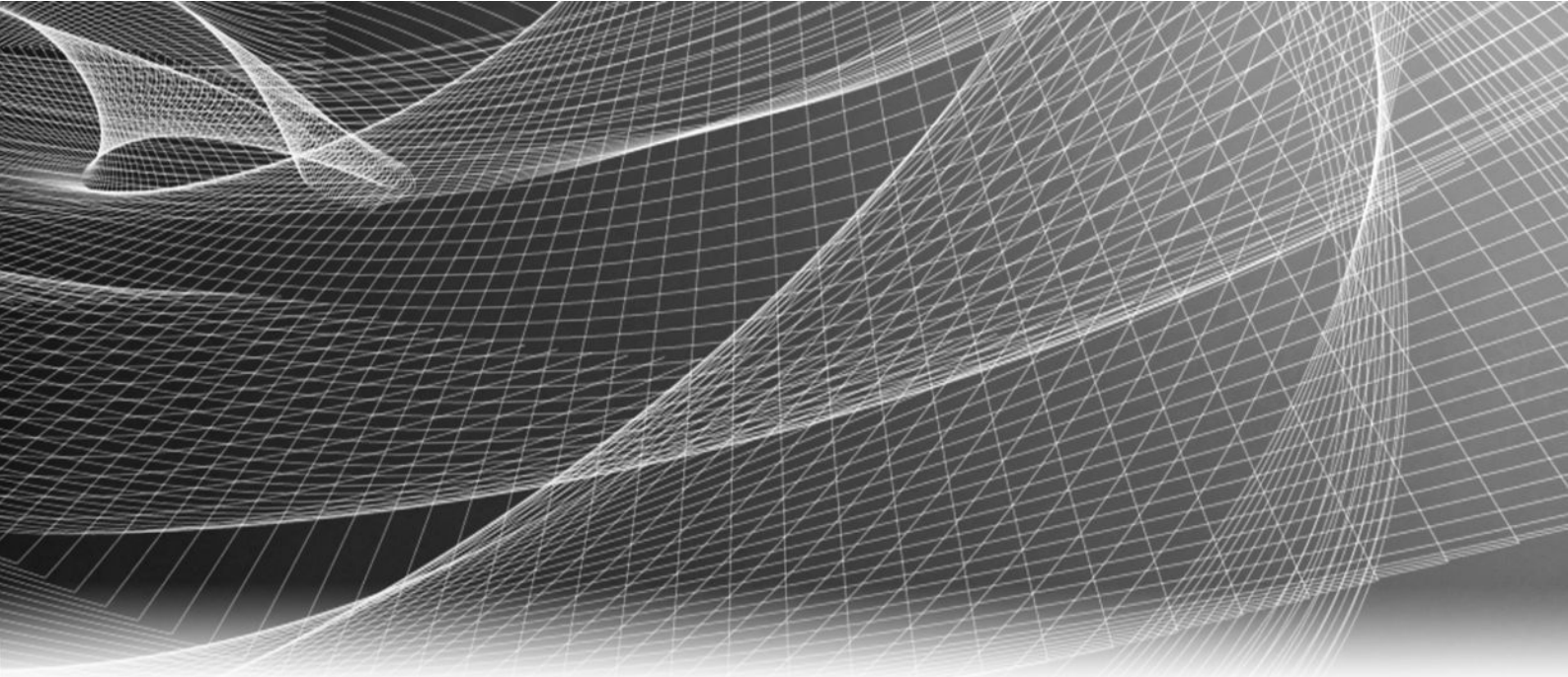




EMC[®] Watch4net[®]

Version 6.3

Installation and Configuration Guide

P/N 302-000-451

REV 01

Copyright © 2012-2013 EMC Corporation. All rights reserved. Published in USA.

Published December, 2013

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>). For documentation on EMC Data Domain products, go to the EMC Data Domain Support Portal (<https://my.datadomain.com>).

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Tables		7
Chapter 1	System Requirements for Watch4net	9
	Operating system requirements.....	10
	Database requirements for Watch4net.....	10
	Browser requirements.....	10
	Supported mobile devices.....	11
Chapter 2	Installation	13
	Standard installation options.....	14
	Installing core software on UNIX.....	14
	Installing core software on Windows Server.....	15
Chapter 3	Configuration	17
	Configuring the user process limits for the Linux installation.....	18
	Starting the core software services from the command line.....	18
	Starting the core software services on Windows.....	19
	Verifying if the core software services are running.....	19
	Troubleshooting service start-up problems on UNIX.....	20
	Troubleshooting service start-up problems on Windows.....	20
	Logging in to the User Interface.....	21
	Confirming settings for the first time.....	21
	License management.....	21
	Obtaining a permanent license.....	21
	Obtaining a temporary license.....	22
	Installing licenses.....	22
	Adding licenses.....	23
	Verifying core software licenses from Centralized Management.....	23
	Obtaining a new license after host reconfiguration.....	24
	Installing a SolutionPack.....	24
	Reviewing reports.....	25
Chapter 4	Migration for Multiple Hosts	27
	Migration workflow.....	28
	Migration for multiple hosts with installed SolutionPacks.....	28
	Migrating core software on a UNIX server.....	31
	Migrating core software on a Windows server.....	31
	Identifying which modules to update.....	32
	Module update order for multiple hosts.....	32
	Updating modules.....	35
	Recommendations for answering module update questions.....	36
	manage-modules.sh update command.....	37
	Updating all core software services from the command line.....	38
	Starting the core software services from the command line.....	38
	Logging in to Centralized Management.....	39
	Confirming settings for the first time.....	39

	Retrieving the list of modules from remote host servers using Centralized Management.....	40
	Updating modules from Centralized Management.....	40
	Recommendations for answering module update questions.....	41
	Installing the generic-rsc package.....	42
	Installing the generic-topology package.....	42
	Installing the Maps-Service package.....	43
	Updating the SolutionPackBlocks.....	43
	Controlling services from Centralized Management.....	44
	Default ReportPack migration.....	44
	Exporting a ReportPack.....	45
	Updating the Default ReportPack.....	45
	Deleting a ReportPack.....	46
	Installing a SolutionPack.....	46
	Reviewing reports.....	47
Chapter 5	Migration for Single Host	49
	Migration workflow.....	50
	Migration for single host with installed SolutionPacks.....	50
	Migrating core software on a UNIX server.....	52
	Migrating core software on a Windows server.....	52
	Identifying which modules to update.....	53
	Module update order for single hosts.....	53
	Updating modules	55
	Recommendations for answering module update questions.....	56
	Updating all core software services from the command line.....	57
	Starting the core software services from the command line.....	57
	Logging in to Centralized Management.....	58
	Confirming settings for the first time.....	58
	Updating modules from Centralized Management.....	59
	Recommendations for answering module update questions.....	59
	Installing the generic-rsc package.....	60
	Installing the generic-topology package.....	61
	Installing the Maps-Service package.....	61
	Updating the SolutionPackBlocks.....	62
	Controlling services from Centralized Management.....	63
	Default ReportPack migration.....	63
	Exporting a ReportPack.....	63
	Updating the Default ReportPack.....	64
	Deleting a ReportPack.....	64
	Installing a SolutionPack.....	65
	Reviewing reports.....	66
Chapter 6	Uninstallation	67
	Overview.....	68
	Stopping core software services on a UNIX server.....	68
	Uninstalling core software from a UNIX server.....	68
	Stopping core software services on a Windows server.....	68
	Uninstalling core software from a Windows server.....	69
	Uninstalling a SolutionPack.....	69
Chapter 7	Software Updates	71
	Product updates.....	72

	Updating the core software installation.....	72
	Installing a SolutionPack Center Update.....	77
	Updating an existing SolutionPack.....	80
	ReportPack Installation.....	81
Chapter 8	Troubleshooting	83
	Troubleshooting service start-up problems on UNIX.....	84
	Troubleshooting service start-up problems on Windows.....	84
	SSL certificates.....	84
	SSL certificate error examples.....	85
	Troubleshooting an SSL certificate error: Accepting the exception....	85
	Installing a self-signed SSL certificate from an Internet Explorer	
	browser.....	85
	Importing an SSL certificate into your truststore.....	86
	Exporting an SSL certificate from an Internet Explorer browser.....	87
Appendix A	Available Modules	89
	Available modules.....	90
Appendix B	Virtual Appliance Installation	95
	Virtual Appliance installation for Watch4net.....	96
	Deploying an appliance.....	96
	Starting the appliance	98
	Verifying the appliance deployment	98
	Log onto the appliance	98
	Passwords.....	98
	Installing a SolutionPack.....	99
	Reviewing reports.....	100
Appendix C	Restoring Modules to their Previous Version	101
	Restoring modules workflow.....	102
	Listing restorable modules.....	102
	Restoring modules.....	103
	manage-modules.sh restore command.....	104
	Starting the core software services from the command line.....	105
	Starting the core software services on Windows.....	105

TABLES

1	Supported operating systems	10
2	Supported relational database management systems.....	10
3	Supported browsers.....	10
4	Supported mobile devices.....	11
5	Group A: Core modules for CLI update.....	33
6	Group B: Launch the update from Centralized Management › Logical Overview.....	33
7	Group A: Core modules for CLI update.....	54
8	Group B: Core modules to update from Centralized Management.....	54
9	Group A: Core modules for CLI update.....	74
10	Group B: Launch the update from Centralized Management › Logical Overview.....	74
11	Version 6.3 available modules.....	90

CHAPTER 1

System Requirements for Watch4net

This chapter includes the following topics:

◆ Operating system requirements	10
◆ Database requirements for Watch4net	10
◆ Browser requirements	10
◆ Supported mobile devices	11

Operating system requirements

The following operating systems are supported for production.

Table 1 Supported operating systems

Operating system	Version
Red Hat Enterprise Linux	5, 64-bit 6, 64-bit
CentOS Linux	5, 64-bit 6, 64-bit
SUSE Linux Enterprise Server (SLES)	11, 64-bit
Microsoft Windows	- Server 2008 R2 - Server 2012 - Server 2012 R2

Database requirements for Watch4net

EMC Watch4net supports these relational database management systems.

Table 2 Supported relational database management systems

Relational database management systems	Version	Notes
MySQL	5.5	Watch4net ships with MySQL 5.5. Existing customers may continue to use MySQL 5.0 in their Watch4net installations.
Oracle Database Enterprise Edition	10G or later	Ensure that the Watch4net server and its operating system satisfy the database engine requirements. Consult the Oracle website for more information. For a distributed Watch4net scenario, the server with the Watch4net back-end components must satisfy the database engine requirements.
Watch4net Datastore	N/A	Watch4net Datastore is an internal database.

Browser requirements

For the following browsers, support varies.

Table 3 Supported browsers

Browser	Version	Operating system	Notes
Google Chrome	Latest	Windows, Linux	Full support
Internet Explorer	8	Windows	Minimal Browse mode

Table 3 Supported browsers (continued)

Browser	Version	Operating system	Notes
Internet Explorer	9 and 10	Windows	Full support
Mozilla Firefox	Latest	Windows, Linux	Full support
Apple Safari	Latest	Mac OS X and iOS	Full support

Minimal Browse mode is for report viewing and browsing. It can display tables, including interactive tables, and graphs that are not interactive. Topology maps are not supported.

Full support includes report viewing and browsing, plus support for interactive tables and graphs, topology maps, and administration tasks (user management, enrichment GUI, alerting GUI, and so on).

Supported mobile devices

To manage the application and view reports, you can use any of the supported mobile devices.

Table 4 Supported mobile devices

Device	Version	Operating system	Notes
Apple iPhone	Latest	Mac iOS	Using APG iPhone client from AppStore
Apple iPad	Latest	Mac iOS	Using APG iPad client from AppStore

CHAPTER 2

Installation

This chapter includes the following topics:

- ◆ [Standard installation options](#)..... 14
- ◆ [Installing core software on UNIX](#)..... 14
- ◆ [Installing core software on Windows Server](#)..... 15

Standard installation options

You have several available options when performing a standard, or binary, installation of the core software.

There are three types of host that make up the core software infrastructure:

- ◆ Frontend host
- ◆ Backend host (Primary and Additional)
- ◆ Collector host

Note

You can have only one Primary Backend host. You can add Additional Backend hosts to scale out your configuration. Additional Backend hosts do not include the main database and exclude a subset of modules.

The components that collectively differentiate the host types are called modules. The core software installation binary supports the following installation options.

Default (UNIX) or Recommended Modules (Windows) installation

Use this option to install all modules available in the core software binary installation package. You can use this option on a single host, enabling it to serve as a Frontend, Backend, and Collector host. You can further customize this host by manually adding or removing specific modules.

Host-specific installations

For a host which requires a specific set of modules to perform its intended function (Frontend, Backend or Collector host), you can use the same core software binary installation and select the specific installation type.

Minimal (UNIX) or Base Installation (Windows)

Use this option to install the minimal modules required for any host type. You can further customize this host by manually adding specific modules.

Installing core software on UNIX

You can install the core software on supported UNIX hosts. This procedure specifically uses the Linux installation procedure as an example.

Before you begin

- ◆ When installing core software on a UNIX server, you must assign executable permissions to the installation script.
- ◆ Make sure you have a login with root privileges to run the installer.
- ◆ Download the installation package to a directory on the server, such as `/temp`.

Procedure

1. Locate the installation package.
2. Navigate to the location where the core software is located.
3. Change the permissions of the installer so you can run it.

For example, for the Linux 64-bit executable, type:

```
chmod +x setup-linux-x86_64-v63.sh
```

4. Run the installer from the directory.

For example:

```
./setup-linux-x86_64-v63.sh
```

5. Read and accept the End User License Agreement. Use the **space bar** to scroll through the agreement. Press **y** to accept it.
6. Press **Enter** to accept the default installation directory of `/opt/APG`. Or, enter another location and press **y**.
7. Press **Enter** to accept the default user account name of `apg` or enter another name.
8. Press **Enter** to accept the default location of service scripts of `/etc/init.d` or enter another location.
9. Press **Enter** to accept the default base directory of `/etc` for runlevels scripts or type another location.
10. Depending on the host purpose, select one of the following:

Option	Description
Default	Installs all recommended modules available in the binary installation package. You can use this option on a single host, enabling it to serve as a Frontend, Backend and Collector host. You can further customize this host by manually adding or removing specific modules.
Frontend	Installs web services and front end applications.
Backend	Installs the database and backend services.
Collector	Installs base modules to perform data collection and enrichment.
Minimal	Installs the minimal modules required for any host type. You can further customize this host by manually adding specific modules.

After you finish

[Available modules on page 90](#) provides the list of modules included with the core software.

Installing core software on Windows Server

You can install the core software on supported Windows Server hosts.

Before you begin

- ◆ Make sure you have a login with system administrator privileges to run the installer.
- ◆ Download the installation package to a folder on the server, such as `\temp`.

Procedure

1. Locate the installation package.
2. Double-click the setup file. For example: `setup-win64-v63.exe`
3. Click **Next** in the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Select the Destination Folder:
 - a. Change the drive to a Windows non-root drive.
 - b. Maintain the default folder structure (`Program Files\APG`).
 - c. Click **Next**.
6. Depending on the host purpose, select one of the following:

Option	Description
Recommended Modules	Installs all recommended modules available in the binary installation package. You can use this option on a single host, enabling it to serve as a Frontend, Backend and Collector host. You can further customize this host by manually adding or removing specific modules.
Frontend Modules	Installs web services and front end applications.
Backend Modules	Installs the database and backend services.
Collector Modules	Installs base modules to perform data collection and enrichment.
Base Installation	Installs the minimal modules required for any host type. You can further customize this host by manually adding specific modules.

7. Click **Install**.
8. On completion, click **Next**.
9. Click **Finish** to close the installer.

[Available modules on page 90](#) provides the list of modules included with core software.

CHAPTER 3

Configuration

This chapter includes the following topics:

◆	Configuring the user process limits for the Linux installation	18
◆	Starting the core software services from the command line	18
◆	Starting the core software services on Windows	19
◆	Verifying if the core software services are running	19
◆	Logging in to the User Interface	21
◆	Confirming settings for the first time	21
◆	License management	21
◆	Installing a SolutionPack	24
◆	Reviewing reports	25

Configuring the user process limits for the Linux installation

Increase the user process limits for the user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed.

Before you begin

- ◆ Make sure you have a login with root privileges.
- ◆ The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, or SUSE Linux Enterprise Server (SLES) 11.
- ◆ The name specified for the user account during the installation.

Procedure

1. Open the `/etc/security/limits.conf` file.
2. Add the following lines for the user.

In this example, the user is `apg`.

```
apg    hard    nofile   65534
apg    soft    nofile   65534
apg    hard    nproc    65534
apg    soft    nproc    65534
```

3. Save the file.
4. Type the following commands from the `bin` directory of the installation to restart the services:

```
./manage-modules.sh service stop all
./manage-modules.sh service start all
```

5. Type the following command to verify the changes:

```
su apg -c 'ulimit -n -u'
```

Starting the core software services from the command line

After installing core software, you must start all required services.

Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the `libaio` package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

Results

A list of services appears. For example:

```
* Starting 'topology-mapping-service Default'... [ OK ]
* Starting 'webservice-gateway Default'... [ OK ]
```

```
* Starting 'mysql Default'... [ OK ]
* Starting 'alerting-backend Default'... [ OK ]
* Starting 'backend Default'... [ OK ]
* Starting 'collector-manager Default'... [ OK ]
* Starting 'collector-manager Generic-SNMP'... [ OK ]
* Starting 'collector-manager Load-Balancer'... [ OK ]
* Starting 'collector-manager emc smarts'... [ OK ]
* Starting 'event-processing-manager emc smarts'... [ OK ]
* Starting 'tomcat Default'... [ OK ]
* Starting 'task-scheduler Default'... [ OK ]
```

Starting the core software services on Windows

After installing core software on Windows, you can start all required services from a Windows desktop.

Before you begin

Make sure you have logged in with system administrator credentials to manage services.

Procedure

1. From the application server's desktop, select **Start > Administrative Tools > Services**.
2. Right-click each service and click **Start**, in this order:
 - APG Topology Mapping Service
 - APG Topology Service
 - APG Webservice Gateway
 - APG MySQL
 - APG Alerting Backend
 - APG Backend
 - APG Collector Manager (Generic RSC)
 - APG Collector Manager (Generic-SNMP)
 - APG Collector Manager (Load-Balancer)
 - APG Event Processing Manager (Alert-Consolidation)
 - APG Tomcat
 - APG Task Scheduler

Verifying if the core software services are running

Verify the core software services are running by obtaining the status.

Before you begin

Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

1. Type the command for your operating system from the `bin` directory of the core software installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service status all</code>

Operating system	Command
Windows	manage-modules.cmd service status all

2. Verify that each service has a status of running in the output:

Results

```
* Checking 'topology-mapping-service Default'... [ running ]
* Checking 'webservice-gateway Default'... [ running ]
* Checking 'mysql Default'... [ running ]
* Checking 'alerting-backend Default'... [ running ]
* Checking 'backend Default'... [ running ]
* Checking 'collector-manager Default'... [ running ]
* Checking 'collector-manager Generic-SNMP'... [ running ]
* Checking 'collector-manager Load-Balancer'... [ running ]
* Checking 'collector-manager emc smarts'... [ running ]
* Checking 'event-processing-manager emc smarts'... [ running ]
* Checking 'tomcat Default'... [ running ]
* Checking 'task-scheduler Default'... [ running ]
```

Troubleshooting service start-up problems on UNIX

Check the log files when services do not start.

Before you begin

Make sure you have logged in with root or APG privileges to check the log files.

Procedure

- ◆ Check these logs in the /opt/APG/ directory to troubleshoot start-up problems:

```
Databases/MySQL/Default/data/[SERVER NAME].err
Backends/Alerting-Backend/Default/logs/alerting-0-0.log
Backends/APG-Backend/Default/logs/cache-0-0.log
Collecting/Collector-Manager/Default/logs/collecting-0-0.log
Web-Servers/Tomcat/Default/logs/service.log
Tools/Task-Scheduler/Default/logs/scheduler-0-0.log
Tools/Webservice-Gateway/Default/logs/gateway-0-0.log
```

Troubleshooting service start-up problems on Windows

Check the log files when services do not start.

Before you begin

Make sure you have logged in with system administrator credentials to check the log files.

Procedure

- ◆ Check these logs in the C:\Program Files\APG directory to troubleshoot start-up problems:

```
Databases\MySQL\Default\data\[SERVER NAME].err.
Backends\Alerting-Backend\Default\logs>alerting-0-0.log
Backends\APG-Backend\Default\logs\cache-0-0.log
Collecting\Collector-Manager\Default\logs\collecting-0-0.log
Web-Servers\Tomcat\Default\logs\service.log
Tools\Task-Scheduler\Default\logs\scheduler-0-0.log
Tools\Webservice-Gateway\Default\logs\gateway-0-0.log
```

Logging in to the User Interface

Log in to continue to view reports or to test user access by specifying operator credentials.

Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/APG`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Confirming settings for the first time

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the server.

Procedure

- ◆ Click **Save** to accept the predefined values for the server.

Fields that are blank must remain blank.

License management

You may evaluate features in SolutionPack Center using the 30-day temporary licenses included with version 6.3.x software. If you install ReportPacks or plan to use SolutionPacks longer than 30 days, contact EMC Online Support for permanent license files.

To install licenses, use the `manage-licenses.sh` command. If you have an existing permanent license or a temporary license that requires updating, use the license upload feature in Centralized Management. Both permanent and temporary licenses are distributed in `.zip` files.

- ◆ Permanent licenses do not have expiration dates and may be associated with a host ID.
- ◆ Temporary licenses do have expiration dates and are not associated with a host ID. When temporary licenses expire, the module license checks fail and the modules stop working. For example, the collector modules stop collecting new information and, if the frontend module fails, you cannot access the User Interface.

Obtaining a permanent license

Obtain a permanent license by creating a Service Request (SR).

Before you begin

Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the application uses instead of root.

Procedure

1. Type the command for your operating system to obtain the host ID:

Operating system	Command
UNIX	<code>/opt/APG/bin/manage-licenses.sh host-id</code>
Windows	<code>C:\Program Files\APG\bin\manage-licenses.cmd host-id</code>

2. Copy the host ID information to a clipboard or to a text file.
3. For product licenses, go to EMC Online Support, support.emc.com.
4. Browse to **Service Center > Product Registration & Licenses**.
5. Paste the host ID information into the Service Request.

Obtaining a temporary license

Obtain a temporary license by creating a Service Request (SR).

Procedure

1. For product licenses, go to EMC Online Support, support.emc.com.
2. Browse to **Service Center > Product Registration & Licenses**.
3. Create the Service Request.

Installing licenses

Before the 30-day trial licenses expire, contact EMC Online Support to obtain and install new license files.

Before you begin

- ◆ Obtain the required license file by creating a Service Request on EMC Online Support.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the Watch4net application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory:

Operating system	Command
UNIX	<code>./manage-licenses.sh install <download_path>/<license.zip></code>
Windows	<code>manage-licenses.cmd install <download_path>\<license.zip></code>

Linux example:

```
./manage-licenses.sh install /opt/APG/licenses/license.zip
```

A `.zip` file can contain any number of license files.

Adding licenses

You must upload a license file whenever you install a new SolutionPack or ReportPack. The license enables views and reports to display.

Before you begin

- ◆ Obtain the required license file by creating a Service Request on EMC Online Support.

Procedure

1. Log in to the host with administrator credentials.

For example, `http://Frontend-hostname:58080/APG`

2. Click **Administration**.
3. In the **Centralized Management** pane, select **Licenses**.
4. In the Physical Overview tree, select **Licenses Management**.
5. In the **Licenses Listing** pane, click **Upload**.
6. In the **License Upload** dialog box, browse to your license file. Click **OK**.
Licenses in a .zip file are extracted and appear in the **Licenses Listing** pane.
7. When **License Upload Complete** appears, click **OK**, then click **Continue**.
8. If you have remote servers in a distributed environment, click **Synchronize** to add the licenses to the remote servers.

Deleting licenses from core software

You can select and delete specific licenses or delete all existing licenses from the core software server.

Procedure

1. Log in to with administrator credentials.
For example, `http://Frontend-hostname:58080/APG`
2. Click **Administration**.
3. In the **Centralized Management** pane, select **Licenses**.
4. In the Physical Overview tree, select **Licenses Management**.
5. In the **Licenses Listing** pane, select one or more license checkboxes.
6. Click **Delete**.
7. If you have remote servers in a distributed environment, click **Synchronize** to remove the licenses from the remote servers.

Verifying core software licenses from Centralized Management

Verify whether core software licenses are valid or expired for all servers in your environment from Centralized Management. The local and remote servers listed in this view are registered with Centralized Management.

Procedure

1. Log in with administrator credentials.

For example, `http://Frontend-hostname:58080/centralized-management`

2. Select **Licenses Management**.
3. In the **Licenses Listing** pane, read the **Expiration** column.

The *EMC Watch4net Centralized Management Guide* provides information about using Centralized Management and server registration.

Obtaining a new license after host reconfiguration

If you change the configuration of the host, for example, by adding interfaces, removing them, or by changing the operating system, your Watch4net permanent license may no longer work. In that case, obtain the host ID and request a new permanent license.

Before you begin

Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the application uses instead of root.

Procedure

1. Type the command for your operating system to obtain the host ID:

Operating system	Command
UNIX	<code>/opt/APG/bin/manage-licenses.sh host-id</code>
Windows	<code>C:\Program Files\APG\bin\manage-licenses.cmd host-id</code>

2. Copy the host ID information to a clipboard or to a text file.
3. For product licenses, go to `support.emc.com`.
4. Browse to **Service Center > Product Registration & Licenses**.
5. Paste the host ID information into the Service Request (SR) for a new permanent license.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- ◆ Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.

5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
 - a. Type the instance name.
 - b. Select the server in one or more list boxes. For example, select the server in the **Data collection, Reports, and Events** list boxes.
 - c. Click **Next**.
8. For each list box you select, a screen appears.
 - a. Click **Next** after you complete each screen.
 - b. Click **Install** after you complete the last screen.

The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

When the installation successfully completes, green checkmarks appear.
10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Install the SolutionPack for EMC Watch4net Health if you have not already done so. This is available from **Centralized Management** > **SolutionPack Center**.

Reviewing reports

After you install a new release or migrate to a new release, check the reports to ensure that the data appears properly.

Before you begin

If the collector configuration changed, you can manually run the scheduled tasks in **Administration** > **Centralized-Management** > **Scheduled Tasks** > **Database** to speed up the report generation process. Wait at least two polling cycles before manually running the scheduled tasks.

To view your report:

Procedure

1. Navigate to **User Interface** > **SolutionPacks** or **User Interface** > **ReportPacks** depending upon which features you have installed.
2. Click the SolutionPack or ReportPack you want to view.

Results

It may take several polling cycles to display all relevant information.

CHAPTER 4

Migration for Multiple Hosts

This chapter includes the following topics:

◆ Migration workflow.....	28
◆ Migrating core software on a UNIX server.....	31
◆ Migrating core software on a Windows server.....	31
◆ Identifying which modules to update.....	32
◆ Module update order for multiple hosts.....	32
◆ Updating modules	35
◆ Updating all core software services from the command line.....	38
◆ Starting the core software services from the command line.....	38
◆ Logging in to Centralized Management.....	39
◆ Confirming settings for the first time.....	39
◆ Retrieving the list of modules from remote host servers using Centralized Management.....	40
◆ Updating modules from Centralized Management.....	40
◆ Installing the generic-rsc package.....	42
◆ Installing the generic-topology package.....	42
◆ Installing the Maps-Service package.....	43
◆ Updating the SolutionPackBlocks.....	43
◆ Controlling services from Centralized Management.....	44
◆ Default ReportPack migration.....	44
◆ Installing a SolutionPack.....	46
◆ Reviewing reports.....	47

Migration workflow

If you have existing core software installed, you need to migrate to the latest software version.

Depending on your existing core software version, do one of the following procedures.

If you have:	Perform:
Legacy core software such as version 6.1 or 6.1ux.	1. Migrate to version 6.2 as described in the <i>EMC Watch4net Migration Guide</i> available from EMC Online Support. Note You must migrate any older Watch4net releases to version 6.2.x before using the procedures in this guide to migrate to version 6.3. The Migration Guides for each release describe how to update from one version to the next. 2. Migrate from version 6.2 to version 6.3.
Core software version 6.2 or 6.2ux.	Migrate to version 6.3: ◆ Migration for multiple hosts with installed SolutionPacks on page 28 ◆ Migration for single host with installed SolutionPacks on page 50

Migration for multiple hosts with installed SolutionPacks

In this migration scenario, version 6.2.x software is already installed on multiple hosts and you wish to migrate to version 6.3.x.

Prerequisites

- ◆ Ensure each host server to be migrated meets system requirements for version 6.3.x.
- ◆ Identify the server hosting Centralized Management. Use this server to launch the setup script or executable first (`setup-linux-x86_64-v63.sh` or `setup-win64-v63.exe`).
- ◆ Ensure each host server is listed in the **Physical Overview** section of the Centralized Management server.
- ◆ Version 6.2.x must be installed and running on all host servers.
- ◆ Version 6.3.x software installs with temporary licenses for each feature. Ensure you obtain permanent licenses for any SolutionPacks you plan to use for longer than 30 days.
- ◆ Ensure each host server has 2 GB free disk space.
- ◆ Ensure you have a login with root or system administrator privileges.
- ◆ Back up the existing installation before starting the migration tasks.
- ◆ Review the workflow before starting and refer back to it as needed during the migration process.

Workflow

Migration for multiple hosts consists of two phases:

- ◆ Updating the host server designated for Centralized Management

◆ Updating the remote servers from the Centralized Management server

You will use CLI commands to migrate specific core modules on the server designated for Centralized Management. Then log into Centralized Management and retrieve all module packages from the remote host servers. After this step, you can update most modules on the remote host servers from the Logical Overview and SolutionPack nodes in Centralized Management. A small number of core module updates require you to log into the remote servers and issue CLI commands. It is very important to follow the recommended order of module updates.

1. Log into the server designated for Centralized Management and run the setup script or executable. This step copies version 6.3.x modules into the Module Repository folder in the existing APG directory path. [Migrating core software on a UNIX server on page 31](#) or [Migrating core software on a Windows server on page 31](#)
2. If you have host servers using different architectures (Windows versus Linux for example), choose one server with an architecture different from the Centralized Management server and run the setup script or executable there as well. Run the script on only one host server per type of architecture.
3. On the server designated for Centralized Management, issue the `manage-modules list installed` command to determine which modules require updating. The Status column identifies modules available for update. [Identifying which modules to update on page 32](#)
4. Review the order in which modules must be updated. [Module update order for multiple hosts on page 32](#)
5. Use the `manage-modules update <module name>` CLI command to update a subset of core modules before proceeding to update modules in Centralized Management. [Updating modules on page 35](#)
6. Update services. [Updating all core software services from the command line on page 38](#)
7. Start services. [Starting the core software services from the command line on page 18](#)
8. Log on to the server designated for Centralized Management. [Logging in to Centralized Management on page 39](#)
9. If you added or updated servers, confirm the settings.
10. Retrieve module packages from remote host servers in order to update them from the Centralized Management server. [Retrieving the list of modules from remote host servers using Centralized Management on page 40](#)
11. Update a second subset of core modules from Centralized Management. Ensure you follow the recommended update order and restart any services that are stopped by the update process.

Note

After you retrieve modules from the remote servers, you may find another set of modules similar to the ones you updated earlier with CLI commands. After you retrieve modules from the remote servers, launch all updates from Centralized Management in the correct order. For `module-manager`, `java`, and `webservice-gateway` modules, you must also log in to the remote host servers and complete the update process using CLI commands. [Module update order for multiple hosts on page 32](#)

[Updating modules from Centralized Management on page 40](#)

12. Install new package files to enable topology features. [Installing the generic-rsc package on page 42](#), [Installing the generic-topology package on page 42](#) and [Installing the Maps-Service package on page 43](#)

13. Update Independent SolutionPackBlocks followed by SolutionPackBlocks.

Note

After this step, there will still be a small number of modules (Collectors and Event Processors) that are marked as available for update with the yellow star icon. Do not update these modules.

14. Ensure that all services stopped during the update process have restarted. [Controlling services from Centralized Management on page 44](#)
15. Update the default ReportPack to ensure the latest SolutionPack template is in use. [Updating the Default ReportPack on page 45](#)
16. Install new SolutionPacks to add new features available in version 6.3. [Installing a SolutionPack on page 24](#)
-

Note

Some SolutionPacks require additional steps such as creation of database schemas or updates to the APG.xml file. Check the SolutionPack documentation for details.

17. Review reports. [Reviewing reports on page 25](#)

Conventions for defaults

During the migration, the multiple choice questions show the default answer with an uppercase letter (for example, **Y/n** means Yes is the default answer). Press **Enter** to accept the default. Press **Enter** to accept the default. If you enter **A** for All, the all actions will be performed. If you enter **N** for None, none of the actions will be performed.

Default directory paths are:

Operating system	Default installation directory
UNIX	/opt/APG/
Windows	C:\Program Files\APG\

Operating system	Default module repository directory
UNIX	<INSTALL_DIR>/Tools/Module-Repository
Windows	<INSTALL_DIR>\Tools\Module-Repository

Note

Install the 6.3 core software into the same directory where the 6.2 core software exists. If you do not specify the same directory, the setup script or executable may overwrite the services configurations since the setup script or executable does not detect the existing 6.2 installation.

Migrating core software on a UNIX server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup script.

Before you begin

- ◆ Make sure you have a login with root privileges to run the setup script.
- ◆ Download the installation package to a directory on the server, such as `/temp`.

Procedure

1. Locate the installation package.
2. Change the permissions of the setup script so you can run it.

For example, for the Linux 64-bit executable, type:

```
chmod +x setup-linux-x86_64-v63.sh
```

3. Run the setup script from the directory.

For example:

```
./setup-linux-x86_64-v63.sh
```

4. Read and accept the End User License Agreement. Use the **space bar** to scroll through the agreement. Press **y** and **Enter** to accept it.

5. Press **Enter** to accept the default installation directory of `/opt/APG`.

Or, if your existing core software resides in another location, specify the other location and press **Enter**.

6. Press **y** and **Enter** to install the new packages in the `/opt/APG/Tools/Module-Repository` directory.

After you finish

Identify which modules to update.

Migrating core software on a Windows server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup executable.

Before you begin

- ◆ Make sure you have a login with system administrator privileges to run the setup executable.
- ◆ Download the installation package to a folder on the server, such as `\temp`.

Procedure

1. Locate the installation package.
2. Double-click the setup executable.

For example: `setup-win64-v63.exe`

3. Click **Next** in the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Press **Enter** to accept the default installation directory of `C:\Program Files\APG`.

Or, if your existing core software resides in another location, specify the other location and press **OK**.

6. Press **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory.

After you finish

Identify which modules to update.

Identifying which modules to update

After you update a core software installation, run the `manage-modules.sh list installed` command to view the installed modules and to determine which modules to update. Update the modules with the status of `can be updated`.

Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh list installed</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd list installed</code>

When you view the output, record the identifier value of each module that needs to be updated. You will need to specify the identifier later when you update the module.

This sample output indicates to update the Module-Manager first, then to update the Alerting-Backend and the Alerting-Frontend modules to version 3.5. For other lines, pay attention to the status recommendations.

```
! WARNING: A more recent version of the module-manager is available. It is strongly
recommended to upgrade it before anything else.
Installed Modules:
```

Identifier Revision OS-Arch	Instance Status	:Category	Module Name	Version
-----	-----	-----	-----	-----
* alerting-backend r4123 linux-x64	Default can be updated to	:Backends	Alerting-Backend	v3.1u2 v3.5
* alerting-frontend r4123 linux-x64	alerting-frontend can be updated to	:Web-Applications	Alerting-Frontend	v3.1u2 v3.5

Module update order for multiple hosts

Update modules in a specific order to avoid issues involving software dependencies and redundant files. Modules that are available for update are marked with a yellow star icon in Centralized Management. If a Module-Manager update is available, always update this module first. Refer to the release notes or the workflow for your deployment scenario for additional recommendations.

Depending on your installed SolutionPacks, the list of modules needing to be updated will vary. When updating modules in a multiple host deployment, follow these recommendations:

- ◆ Update a subset of core modules (Group A) on the Centralized Management server first using the CLI command, `manage-modules.sh update` or `manage-modules.cmd update`.

- ◆ After updating the last core module in Group A, update the services and then start the services.
- ◆ After retrieving modules from the remote host servers, launch the update of a second subset of modules (Group B) from **Centralized Management > Logical Overview**. A few modules require an additional manual CLI update step on the remote host servers.
- ◆ Update Independent SolutionPackBlocks.
- ◆ Update SolutionPackBlocks.

Note

Do not update any other modules, even if they display in **Centralized Management > Logical Overview** with the yellow star update icon.

Table 5 Group A: Core modules for CLI update

Update these core modules using CLI commands.
module-manager
java
license-manager
mysql (optional, but recommended)
jdbc-drivers
tomcat
WebApps, includes one or more of these modules if marked for update: • alerting-frontend • centralized-management • device-discovery • frontend • frontend-ws • mib-browser • ip-sla-probes • transaction-collector-gui
webapps-resources
webservice-gateway

Table 6 Group B: Launch the update from Centralized Management > Logical Overview

Core module update order	Node in Logical Overview	Notes
module-manager	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, <code>(manage-modules.sh update module-manager</code> or

Table 6 Group B: Launch the update from Centralized Management › Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
		<code>manage-modules.cmd update module-manager</code>) on the remote host to apply the update.
java	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, <code>(manage-modules.sh update java or manage-modules.cmd update java)</code> on the remote host to apply the update. Ensure all services are restarted after updating java. <code>(manage-modules.sh service start all or manage-modules.cmd service start all</code>
license-manager	Miscellaneous	
mysql	Databases	
jdbc-drivers	Databases	
tomcat	Miscellaneous	The update stops the service. If the display indicates the service failed to stop, retry the update.
alerting-frontend	Frontends	
centralized-management	Frontends	
device-discovery	Frontends	
frontend	Frontends	
frontend-ws	Frontends	
mib-browser	Frontends	
ip-sla-probes	Frontends	
transaction-collector-gui	Frontends	
webapps-resources	Miscellaneous	
webservice-gateway	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, <code>(manage-modules.sh update webservice-gateway or manage-modules.cmd update webservice-gateway)</code> on the remote host to apply the update.
alerting-backend	Backends	
apg-backend	Backends	

Table 6 Group B: Launch the update from Centralized Management › Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
apg-property-store	Databases	
administration-tool	Miscellaneous	
diagnostic-tools	Miscellaneous	
frontend-report-generator	Miscellaneous	
frontend-search	Miscellaneous	
task-scheduler	Miscellaneous	
topology-cli	Miscellaneous	

When updating multiple modules, update first by Category and then by Module Name.

The Frontend and SNMP module families are not used in all deployments.

Since modules belonging to the Frontend family have logical interdependencies, the modules must be updated to the same version or problems may occur.

Modules belonging to the SNMP family also have logical interdependencies and must be updated to the same version.

You can view the Category and Module Name values by using the `manage-modules.sh list installed` command or by viewing the nodes in **Centralized Management › Logical Overview**.

Updating modules

Run the `manage-modules.sh update <identifier>` command to update the modules and their managers. Some modules may request information from you during an update. For example, you may be prompted for a module instance name if there are multiple instances, whether you want to continue the update, and whether you want to keep the original copy of a file that is updated.

Before you begin

- ◆ Obtain the identifier by using the `manage-modules.sh list installed` command.
- ◆ Make sure you have a login with root or system administrator privileges to update modules.

Update the manager of the module first before updating the module. Use the same command and substitute the appropriate identifier.

Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh update <module_identifier> [<module_instance>]</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd update <module_identifier> [<module_instance>]</code>

2. Answer any questions.

Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter [y]es. When prompted to keep the old version as a backup, enter [y]es.

The task file `scheduled-reports/user1/daily_health_report.task` is already installed in the task scheduler but with different content. Replace the current task which is enabled by the updated one? [y]es
[n]o [A]ll [N]one > y

manage-modules.sh update command

Use the `manage-modules.sh update` command to update modules and their managers. Type the command for your operating system from the `bin` directory of your core software installation directory.

Description

The `manage-modules.sh update` command updates installed modules and their managers. For UNIX, specify `manage-modules.sh update`. For Windows, specify `manage-modules.cmd update`.

Update the manager of the module first before updating the module.

To look up the identifier and module instance name, use the `manage-modules.sh list installed` command.

Syntax

```
manage-modules.sh update <module_identifier> [ <module_instance> ]
```

Options

module_identifier

The identifier value of the installed module or manager.

module_instance

The unique name of the module or manager. Omit this value if only one instance is installed since the command will use it as the default. If multiple instances exist, specify the instance you want to update or the command will prompt you for the instance name. The identifier and instance values form a unique key to refer to the module or manager.

Example # 1

In this Linux example, the following commands update the manager, Collector-Manager, and a corresponding module, XML-Collector.

```
<INSTALL_DIR>/bin/manage-modules.sh update collector-manager
<INSTALL_DIR>/bin/manage-modules.sh update xml-collector
```

Example # 2

In this Windows example, the following commands update the Tomcat Web server and a corresponding module, MIB-Browser.

```
<INSTALL_DIR>\bin\manage-modules.cmd update tomcat
<INSTALL_DIR>\bin\manage-modules.cmd update mib-browser
```

Example # 3

In this Linux example, the following commands update specific instances.

```
./manage-modules.sh update tomcat instance3
./manage-modules.sh update mib-browser mymib_browser2
```

Updating all core software services from the command line

After migrating core software, you must update all required services.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service update all</code>
Windows	<code>manage-modules.cmd service update all</code>

Results

A list of services appears. For example:

```
* Stopping 'collector-manager Generic-SNMP'... [ OK ]
* Stopping 'topology-mapping-service Default'... [ OK ]
* Updating service 'topology-mapping-service Default'... [ updated ]
* Updating service 'webservice-gateway Default'... [ updated ]
* Updating service 'mysql Default'... [ updated ]
* Updating service 'alerting-backend Default'... [ updated ]
* Updating service 'backend Default'... [ updated ]
* Updating service 'collector-manager Default'... [ updated ]
* Updating service 'collector-manager Generic-SNMP'... [ updated ]
* Updating service 'collector-manager Load-Balancer'... [ updated ]
* Updating service 'collector-manager emc smarts'... [ updated ]
* Updating service 'event-processing-manager emc smarts'...
[ updated ]
* Updating service 'tomcat Default'... [ updated ]
* Updating service 'task-scheduler Default'... [ updated ]
```

Starting the core software services from the command line

After installing core software, you must start all required services.

Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the libaio package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

Results

A list of services appears. For example:

```
* Starting 'topology-mapping-service Default'... [ OK ]
* Starting 'webservice-gateway Default'... [ OK ]
* Starting 'mysql Default'... [ OK ]
* Starting 'alerting-backend Default'... [ OK ]
* Starting 'backend Default'... [ OK ]
* Starting 'collector-manager Default'... [ OK ]
* Starting 'collector-manager Generic-SNMP'... [ OK ]
* Starting 'collector-manager Load-Balancer'... [ OK ]
* Starting 'collector-manager emc smarts'... [ OK ]
* Starting 'event-processing-manager emc smarts'... [ OK ]
* Starting 'tomcat Default'... [ OK ]
* Starting 'task-scheduler Default'... [ OK ]
```

Logging in to Centralized Management

Log in to Centralized Management to perform operations affect all servers.

Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/centralized-management`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Confirming settings for the first time

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the server.

Procedure

- ◆ Click **Save** to accept the predefined values for the server.

Fields that are blank must remain blank.

Retrieving the list of modules from remote host servers using Centralized Management

If you have remote servers in a distributed environment, during migration, you need to copy the list of modules in use on remote host servers into the Centralized Management server.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Make sure the Centralized Management server has remote access to the remote servers and that their webservice-gateway service is running.

Procedure

1. Navigate to **Centralized Management > Packages Management**.
2. In **Packages Listing**, select **Synchronization**.
3. Select the checkbox for **Retrieve the latest packages from the remote servers** and click **OK**.

Updating modules from Centralized Management

Use Centralized Management as one of the methods to update a module.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Check the required update order for your scenario.

Procedure

1. Navigate to **Centralized Management**.
2. Select **Logical Overview**.

In the pane, notice that the nodes are listed in the **Logical Group** column.

3. Scroll through the pane in the required update order for your scenario to locate nodes with modules that are marked with the yellow star icon.
4. Update each module marked with the yellow star icon.
 - a. Click the **yellow star icon**.
 - b. Click **Update to Latest Version**.
 - c. Click **Update**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

- d. Close the window when the update process is finished.
- e. Repeat for each module marked with the yellow star icon.

After each module is updated, the yellow star icon disappears.

Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter `[y]es`. When prompted to keep the old version as a backup, enter `[y]es`.

The task file `scheduled-reports/user1/daily_health_report.task` is already installed in the task scheduler but with different content. Replace the current task which is enabled by the updated one? `[y]es [n]o [A]ll [N]one > y`

Installing the generic-rsc package

Manually install the `generic-rsc` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the collector host is installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-rsc** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:
 - Topology-Mapping-Service
 - Collector-Manager
 - FailOver-Filter
 - Inline-Calculation-Filter
 - Variable-Handling-Filter
 - Property-Tagging-Filter
 - Remote-Shell-Collector
 - generic-rsc

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Installing the generic-topology package

Manually install the `generic-topology` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Backend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.

5. Select the **Block** category and select the **generic-topology** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:

- Topology-Service
- generic-topology

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Installing the Maps-Service package

Manually install the `Maps-Service` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Frontend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Tools** category and select the **Maps-Service** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Updating the SolutionPackBlocks

After installing a software update or migrating from an older release, you must update SolutionPackBlocks in order to use the latest module configurations and report templates. This block update may trigger the update of an associated module.

Before you begin

- ◆ Be sure you have updated core modules (except for blocks, collectors, and event processors) in all of the servers before you update SolutionPackBlocks.

Procedure

1. Click the **SolutionPacks** node on the left panel to access **Installed SolutionPacks**.

Two panes appear: Independent SolutionPackBlocks and SolutionPacks. Update the Independent SolutionPackBlocks first before you update the SolutionPackBlocks that belong to the SolutionPacks.

2. Do the following to locate the block that you want to update:

In the pane for	Perform:
Independent SolutionPackBlocks	Locate the block.
SolutionPacks	a. Select the specific SolutionPack. b. Locate the block in the Properties page.

3. Click the **yellow star icon**.

The **SolutionPack Update** page appears.

4. Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

5. Click **Update**.

The update process begins. The **SolutionPack Update** page provides information on the progress of the update.

6. Select the maximize arrow next to view the update progress.

When the update successfully completes, a green checkmark appears above this information.

Controlling services from Centralized Management

You can start, stop, or restart services from the Centralized Management.

Before you begin

Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

1. Log in and select **Administration > Centralized Management**.
2. Select the server in **Physical Overview**.
3. In the **Services** tab, select the module.
4. Click one of the following buttons.

Operation	Description
Start	Starts the service.
Stop	Stops the service.
Restart	Restarts the service.

Read the status message.

Default ReportPack migration

Update the Default ReportPack to ensure you use the latest SolutionPack template.

Update the Default ReportPack from the Administration menu after logging in to the User Interface URL, for example, `http://<Frontend-hostname>:58080/APG`

The Default ReportPack contains the default reports. To access all of the new report features available in a software release, update the Default ReportPack during the migration process.

1. Back up the existing Default ReportPack by exporting the `.arp` file.
2. Upload the Default ReportPack.
3. Delete the old ReportPack.

Note

Scheduled reports, pre-generated reports and template restrictions are lost when you delete the old Default ReportPack. The online help describes methods for exporting ReportPack templates so you can save them.

Exporting a ReportPack

You can export a ReportPack to back up the `<ReportPack>.arp` file or for use in another system.

Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.
4. Click **Export** to download the `<ReportPack>.arp` file that contains the required information and templates.
5. Click **Save** to navigate to the download location.

Updating the Default ReportPack

Update your existing Default ReportPack by replacing it completely with a new Default ReportPack.

Before you begin

- ◆ Ensure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.
- ◆ Locate the new `Default ReportPack.arp` file. The file is located on the server in `<INSTALL_DIR>/Web-Servers/Tomcat/Default/webapps/APG`. If you are accessing the server remotely, you will need to download the `.arp` file to your local directory first.

Procedure

1. Log in and select **Administration > ReportPacks** to access **ReportPacks Management**.
Available ReportPacks are listed in a pane.
2. Rename the existing Default ReportPack to distinguish between the existing one and the new one.
 - a. Select **Default ReportPack** in the pane.
 - b. Type **(original 6.2)** in the **Name** field.
The **Name** field value reads: Default ReportPack (original 6.2)
 - c. Click **Save**.

You are returned to **ReportPacks Management**.

3. Click **Upload a ReportPack**.
4. Select the `Default ReportPack.arp` file from your local directory.
5. Click **Save**.

After you finish

If you are satisfied with the resulting reports , you can delete the old Default ReportPack.

Note

Scheduled reports, pre-generated reports and template restrictions will be lost if you remove it.

Deleting a ReportPack

When a ReportPack is no longer needed, you can remove it and its report templates.

Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.
4. Click **Delete** to remove the ReportPack and its templates.
5. Click **Ok** at the warning message.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- ◆ Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
 - a. Type the instance name.
 - b. Select the server in one or more list boxes. For example, select the server in the **Data collection, Reports, and Events** list boxes.

- c. Click **Next**.
- 8. For each list box you select, a screen appears.
 - a. Click **Next** after you complete each screen.
 - b. Click **Install** after you complete the last screen.

The installation process begins.

- 9. Select the maximize arrow next to each component to view the installation process.
When the installation successfully completes, green checkmarks appear.
- 10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Install the SolutionPack for EMC Watch4net Health if you have not already done so. This is available from **Centralized Management** > **SolutionPack Center**.

Reviewing reports

After you install a new release or migrate to a new release, check the reports to ensure that the data appears properly.

Before you begin

If the collector configuration changed, you can manually run the scheduled tasks in **Administration** > **Centralized-Management** > **Scheduled Tasks** > **Database** to speed up the report generation process. Wait at least two polling cycles before manually running the scheduled tasks.

To view your report:

Procedure

- 1. Navigate to **User Interface** > **SolutionPacks** or **User Interface** > **ReportPacks** depending upon which features you have installed.
- 2. Click the SolutionPack or ReportPack you want to view.

Results

It may take several polling cycles to display all relevant information.

CHAPTER 5

Migration for Single Host

This chapter includes the following topics:

◆ Migration workflow.....	50
◆ Migrating core software on a UNIX server.....	52
◆ Migrating core software on a Windows server.....	52
◆ Identifying which modules to update.....	53
◆ Module update order for single hosts.....	53
◆ Updating modules	55
◆ Updating all core software services from the command line.....	57
◆ Starting the core software services from the command line.....	57
◆ Logging in to Centralized Management.....	58
◆ Confirming settings for the first time.....	58
◆ Updating modules from Centralized Management.....	59
◆ Installing the generic-rsc package.....	60
◆ Installing the generic-topology package.....	61
◆ Installing the Maps-Service package.....	61
◆ Updating the SolutionPackBlocks.....	62
◆ Controlling services from Centralized Management.....	63
◆ Default ReportPack migration.....	63
◆ Installing a SolutionPack.....	65
◆ Reviewing reports.....	66

Migration workflow

If you have existing core software installed, you need to migrate to the latest software version.

Depending on your existing core software version, do one of the following procedures.

If you have:	Perform:
Legacy core software such as version 6.1 or 6.1ux.	1. Migrate to version 6.2 as described in the <i>EMC Watch4net Migration Guide</i> available from EMC Online Support. Note You must migrate any older Watch4net releases to version 6.2.x before using the procedures in this guide to migrate to version 6.3. The Migration Guides for each release describe how to update from one version to the next. 2. Migrate from version 6.2 to version 6.3.
Core software version 6.2 or 6.2ux.	Migrate to version 6.3: ◆ Migration for multiple hosts with installed SolutionPacks on page 28 ◆ Migration for single host with installed SolutionPacks on page 50

Migration for single host with installed SolutionPacks

In this migration scenario, version 6.2.x software is already installed and you wish to migrate to version 6.3.x on the same host. Launch the setup script or executable to copy the latest version of modules into the existing APG module repository.

Prerequisites

- ◆ Ensure the host server meets system requirements for version 6.3.x.
- ◆ Version 6.2.x must be installed and running before migrating to version 6.3.x.
- ◆ Version 6.3.x software installs with temporary licenses for each feature. Ensure you obtain permanent licenses for any SolutionPacks you plan to use for longer than 30 days.
- ◆ Ensure the host server has 2 GB free disk space.
- ◆ Ensure you have a login with root or system administrator privileges.
- ◆ Back up the existing installation before starting the migration tasks.
- ◆ Review this workflow before starting. The specific procedures mentioned in the workflow follow this topic in the chapter.

Workflow

You will use CLI commands to migrate specific core modules on the server designated for Centralized Management. Then log into Centralized Management and update remaining modules from the Logical Overview and SolutionPack nodes. It is very important to follow the recommended order of module updates.

1. Log in to the host server with root or administrator credentials and run the setup script or executable to copy the new module packages into the existing APG directory path. For example, `setup-linux-x86_64-v63.sh` or `setup-win64-v63.exe`.

2. Issue the `manage-modules list installed` command to determine which modules require updating. The Status column identifies modules available for update.
3. Review the order in which modules must be updated. [Module update order for single hosts on page 53](#)
4. Use the `manage-modules update <module name>` CLI command to update a subset of core modules before logging in to Centralized Management.
5. Update services.
6. Start services.
7. Log in to Centralized Management.
8. If you updated the server, you may be prompted to confirm the server settings.
9. Update a second subset of core modules from Centralized Management. Ensure you follow the recommended update order and restart any services that are stopped by the update process.
10. Install new package files to enable topology features.
11. Update Independent SolutionPacks followed by SolutionPacks.

Note

After this step, there will still be a small number of modules that are marked as available for update with the yellow star icon. Do not update these modules.

12. Ensure that all services stopped during the update process have restarted.
13. Update the default ReportPack to ensure the latest SolutionPack template is in use.
14. Install new SolutionPacks to add new features available in version 6.3.

Note

Some SolutionPacks require additional steps such as creation of database schemas or updates to the `APG.xml` file. Check the SolutionPack documentation for details.

15. Review reports.

Conventions for defaults

During the migration, the multiple choice questions show the default answer with an uppercase letter (for example, **Y/n** means Yes is the default answer). Press **Enter** to accept the default. If you enter **A** for All, the all actions will be performed. If you enter **N** for None, none of the actions will be performed.

Default directory paths are:

Operating system	Default installation directory
UNIX	<code>/opt/APG/</code>
Windows	<code>C:\Program Files\APG\</code>

Operating system	Default module repository directory
UNIX	<code><INSTALL_DIR>/Tools/Module-Repository</code>
Windows	<code><INSTALL_DIR>\Tools\Module-Repository</code>

Note

Install the 6.3.x software into the directory where 6.2.x software is installed. If you do not specify the same directory, the setup script or executable may overwrite the services configurations because the setup script or executable does not detect the existing 6.2.x installation.

Migrating core software on a UNIX server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup script.

Before you begin

- ◆ Make sure you have a login with root privileges to run the setup script.
- ◆ Download the installation package to a directory on the server, such as `/temp`.

Procedure

1. Locate the installation package.
2. Change the permissions of the setup script so you can run it.

For example, for the Linux 64-bit executable, type:

```
chmod +x setup-linux-x86_64-v63.sh
```

3. Run the setup script from the directory.

For example:

```
./setup-linux-x86_64-v63.sh
```

4. Read and accept the End User License Agreement. Use the **space bar** to scroll through the agreement. Press **y** and **Enter** to accept it.
5. Press **Enter** to accept the default installation directory of `/opt/APG`.

Or, if your existing core software resides in another location, specify the other location and press **Enter**.

6. Press **y** and **Enter** to install the new packages in the `/opt/APG/Tools/Module-Repository` directory.

After you finish

Identify which modules to update.

Migrating core software on a Windows server

Perform this procedure on a single host where version 6.2.x software is already installed. Typically, the host has core software with installed SolutionPacks. During the procedure, you must assign executable permissions to the setup executable.

Before you begin

- ◆ Make sure you have a login with system administrator privileges to run the setup executable.
- ◆ Download the installation package to a folder on the server, such as `\temp`.

Procedure

1. Locate the installation package.
2. Double-click the setup executable.

For example: `setup-win64-v63.exe`

3. Click **Next** in the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Press **Enter** to accept the default installation directory of `C:\Program Files\APG`.
Or, if your existing core software resides in another location, specify the other location and press **OK**.
6. Press **OK** to install the new packages in the `C:\Program Files\APG\Tools\Module-Repository` directory.

After you finish

Identify which modules to update.

Identifying which modules to update

After you update a core software installation, run the `manage-modules.sh list installed` command to view the installed modules and to determine which modules to update. Update the modules with the status of `can be updated`.

Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh list installed</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd list installed</code>

When you view the output, record the identifier value of each module that needs to be updated. You will need to specify the identifier later when you update the module.

This sample output indicates to update the Module-Manager first, then to update the Alerting-Backend and the Alerting-Frontend modules to version 3.5. For other lines, pay attention to the status recommendations.

```
! WARNING: A more recent version of the module-manager is available. It is strongly
recommended to upgrade it before anything else.
Installed Modules:
```

Identifier Revision OS-Arch	Instance Status	:Category	Module Name	Version
-----	-----	-----	-----	-----
* alerting-backend r4123 linux-x64	Default can be updated to v3.5	:Backends	Alerting-Backend	v3.1u2
* alerting-frontend r4123 linux-x64	alerting-frontend can be updated to v3.5	:Web-Applications	Alerting-Frontend	v3.1u2

Module update order for single hosts

Update modules in a specific order to avoid issues involving software dependencies and redundant files. Modules that are available for update are marked with an yellow star icon in Centralized Management. If a Module-Manager update is available, always update this module first. Refer to the release notes or the workflow for your deployment scenario for additional recommendations.

Depending on your installed SolutionPacks, the list of modules needing to be updated will vary. When updating modules in a single host deployment, follow these guidelines:

- ◆ Update a subset of core modules (Group A) using the CLI command, `manage-modules.sh update` or `manage-modules.cmd update`.
- ◆ After updating the last core module in Group A, update the services and then start the services.
- ◆ Update a second subset of modules (Group B) after logging in to **Centralized Management** › **Logical Overview**.
- ◆ Update Independent SolutionPackBlocks.
- ◆ Update SolutionPackBlocks.

Note

Do not update any other modules, even if they display in **Centralized Management** › **Logical Overview** with the yellow star update icon.

Table 7 Group A: Core modules for CLI update

Update these core modules for a single host using CLI commands
module-manager
java
license-manager
mysql (optional, but recommended)
jdbc-drivers
tomcat
WebApps, includes one or more of these modules if marked for update: • alerting-frontend • centralized-management • device-discovery • frontend • frontend-ws • mib-browser • ip-sla-probes • transaction-collector-gui
webapps-resources
webservice-gateway

Table 8 Group B: Core modules to update from Centralized Management

Core module update order	Node in Logical Overview
alerting-backend	Backends
apg-backend	Backends

Table 8 Group B: Core modules to update from Centralized Management (continued)

Core module update order	Node in Logical Overview
apg-property-store	Databases
administration-tool	Miscellaneous
diagnostic-tools	Miscellaneous
frontend-report-generator	Miscellaneous
frontend-search	Miscellaneous
task-scheduler	Miscellaneous
topology-cli	Miscellaneous

When updating modules, update first by Category and then by Module Name.

The Frontend and SNMP module families are not used in all deployments.

Since modules belonging to the Frontend family have logical interdependencies, the modules must be updated to the same version or problems may occur.

Modules belonging to the SNMP family also have logical interdependencies and must be updated to the same version.

View the Category and Module Name values by using the `manage-modules.sh list installed` command or by viewing the nodes in **Centralized Management > Logical Overview**.

Updating modules

Run the `manage-modules.sh update <identifier>` command to update the modules and their managers. Some modules may request information from you during an update. For example, you may be prompted for a module instance name if there are multiple instances, whether you want to continue the update, and whether you want to keep the original copy of a file that is updated.

Before you begin

- ◆ Obtain the identifier by using the `manage-modules.sh list installed` command.
- ◆ Make sure you have a login with root or system administrator privileges to update modules.

Update the manager of the module first before updating the module. Use the same command and substitute the appropriate identifier.

Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh update <module_identifier> [<module_instance>]</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd update <module_identifier> [<module_instance>]</code>

2. Answer any questions.

Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the `daily_health_report`, enter `[y]es`. When prompted to keep the old version as a backup, enter `[y]es`.

The task file `scheduled-reports/user1/daily_health_report.task` is already installed in the task scheduler but with different content. Replace the current task which is enabled by the updated one? `[y]es`
`[n]o [A]ll [N]one > y`

Updating all core software services from the command line

After migrating core software, you must update all required services.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service update all</code>
Windows	<code>manage-modules.cmd service update all</code>

Results

A list of services appears. For example:

```
* Stopping 'collector-manager Generic-SNMP'... [ OK ]
* Stopping 'topology-mapping-service Default'... [ OK ]
* Updating service 'topology-mapping-service Default'... [ updated ]
* Updating service 'webservice-gateway Default'... [ updated ]
* Updating service 'mysql Default'... [ updated ]
* Updating service 'alerting-backend Default'... [ updated ]
* Updating service 'backend Default'... [ updated ]
* Updating service 'collector-manager Default'... [ updated ]
* Updating service 'collector-manager Generic-SNMP'... [ updated ]
* Updating service 'collector-manager Load-Balancer'... [ updated ]
* Updating service 'collector-manager emc smarts'... [ updated ]
* Updating service 'event-processing-manager emc smarts'...
[ updated ]
* Updating service 'tomcat Default'... [ updated ]
* Updating service 'task-scheduler Default'... [ updated ]
```

Starting the core software services from the command line

After installing core software, you must start all required services.

Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the `libaio` package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

Results

A list of services appears. For example:

```
* Starting 'topology-mapping-service Default'... [ OK ]
* Starting 'webservice-gateway Default'... [ OK ]
* Starting 'mysql Default'... [ OK ]
* Starting 'alerting-backend Default'... [ OK ]
* Starting 'backend Default'... [ OK ]
* Starting 'collector-manager Default'... [ OK ]
* Starting 'collector-manager Generic-SNMP'... [ OK ]
* Starting 'collector-manager Load-Balancer'... [ OK ]
* Starting 'collector-manager emc smarts'... [ OK ]
* Starting 'event-processing-manager emc smarts'... [ OK ]
* Starting 'tomcat Default'... [ OK ]
* Starting 'task-scheduler Default'... [ OK ]
```

Logging in to Centralized Management

Log in to Centralized Management to perform operations affect all servers.

Procedure

1. Point your browser to the URL.

For example, `http://<Frontend-hostname>:58080/centralized-management`

2. Log in.

- a. Type the login credentials.

The default username is **admin** and the default password is **changeme**.

- b. Click **Sign In**.

After you finish

Note

You are automatically logged off after four hours.

Confirming settings for the first time

After you first log in with administrator credentials for core software, you must confirm the configuration settings for the server.

Procedure

- ◆ Click **Save** to accept the predefined values for the server.

Fields that are blank must remain blank.

Updating modules from Centralized Management

Use Centralized Management as one of the methods to update a module.

Before you begin

- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.
- ◆ Check the required update order for your scenario.

Procedure

1. Navigate to **Centralized Management**.
2. Select **Logical Overview**.

In the pane, notice that the nodes are listed in the **Logical Group** column.

3. Scroll through the pane in the required update order for your scenario to locate nodes with modules that are marked with the yellow star icon.
4. Update each module marked with the yellow star icon.
 - a. Click the **yellow star icon**.
 - b. Click **Update to Latest Version**.
 - c. Click **Update**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

- d. Close the window when the update process is finished.
- e. Repeat for each module marked with the yellow star icon.

After each module is updated, the yellow star icon disappears.

Recommendations for answering module update questions

During the module update process, there will be questions asked about saving, deleting, or overwriting existing files.

Usually, you should answer no ([n]o) when asked to delete files. You can then compare the old and new files later if there is a problem with the update. However there are exceptions to this recommendation.

centralized-managment module

When updating an older version of the centralized-management module to version 2.2 or higher, you may delete `conf/servers.xml` when prompted during the update process.

```
Starting update of centralized-management centralized-management from
v2.1u2 to v2.2...
* Gathering information...
* Module found in '/opt/APG/Web-Applications/Centralized-Management/
centralized-management'.
* It will now be updated using 'centralized-management-2.2-linux-
x64.pkg'.
* Undeploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' from Tomcat-
Default...
* Unpacking files...
* Configuration file 'conf/servers.xml', which has not changed since
its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 81 files have been updated.
* Finalizing update...
```

```
* Deploying web application '/opt/APG/Web-Applications/Centralized-
Management/centralized-management/webapp/mgmt.war' on Tomcat-
Default...
? Task file online-update-check.task added by module centralized-
management centralized-management. Enable it? [y]es, [n]o, [A]ll,
[N]one > y
```

webapps-resources

You may delete the property-mapping values when updating to webapps-resources version 1.3 or higher.

```
Starting update of webapps-resources Default from v1.2u1 to v1.3...
* Gathering information...
* Module found in '/opt/APG/Custom/WebApps-Resources/Default'.
* It will now be updated using 'webapps-resources-1.3-linux-x64.pkg'.
* Unpacking files...
* Configuration file 'property-mapping/FLOW-TF-SRCADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DATA.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-PROTO.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-DSTADDR.xml', which
has not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Configuration file 'property-mapping/FLOW-TF-APPLI.xml', which has
not changed since its installation, is about to be removed.
? Delete it? [y]es, [n]o, [A]ll, [N]one > y
* Updating files... 100%
* 530 files have been updated.
* Finalizing update...
```

frontend-report-generator

When prompted to replace the v6.2u3 version with the v6.3 version of the daily_health_report, enter [y]es. When prompted to keep the old version as a backup, enter [y]es.

```
The task file scheduled-reports/user1/daily_health_report.task is
already installed in the task scheduler but with different content.
Replace the current task which is enabled by the updated one? [y]es
[n]o [A]ll [N]one > y
```

Installing the generic-rsc package

Manually install the generic-rsc package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the collector host is installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-rsc** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:
 - Topology-Mapping-Service
 - Collector-Manager
 - FailOver-Filter

- Inline-Calculation-Filter
- Variable-Handling-Filter
- Property-Tagging-Filter
- Remote-Shell-Collector
- generic-rsc

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Installing the generic-topology package

Manually install the `generic-topology` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Backend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Block** category and select the **generic-topology** package.
6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install** for each component:

- Topology-Service
- generic-topology

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Installing the Maps-Service package

Manually install the `Maps-Service` package when migrating from 6.2.x to the 6.3.x core software release.

Procedure

1. Navigate to **Centralized Management**.
2. Expand **Physical Overview** and select the server where the Frontend modules are installed.
3. Select the **SolutionPacks and Modules** tab.
4. Click **Install** to access **Packages Installation**.
5. Select the **Tools** category and select the **Maps-Service** package.

6. Click **Launch** to access the **Installation Steps** window.
7. Accept the default values and click **Install**.

If you are prompted for information, press **Enter** to select the default value or type another value appropriate for your deployment.

The component status turns green.

8. Click **Back** to return to **Packages Installation** to continue installing more packages or close the **Installation Steps** window.

Updating the SolutionPackBlocks

After installing a software update or migrating from an older release, you must update SolutionPackBlocks in order to use the latest module configurations and report templates. This block update may trigger the update of an associated module.

Before you begin

- ◆ Be sure you have updated core modules (except for blocks, collectors, and event processors) in all of the servers before you update SolutionPackBlocks.

Procedure

1. Click the **SolutionPacks** node on the left panel to access **Installed SolutionPacks**.

Two panes appear: Independent SolutionPackBlocks and SolutionPacks. Update the Independent SolutionPackBlocks first before you update the SolutionPackBlocks that belong to the SolutionPacks.

2. Do the following to locate the block that you want to update:

In the pane for	Perform:
Independent SolutionPackBlocks	Locate the block.
SolutionPacks	a. Select the specific SolutionPack. b. Locate the block in the Properties page.

3. Click the **yellow star icon**.

The **SolutionPack Update** page appears.

4. Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

5. Click **Update**.

The update process begins. The **SolutionPack Update** page provides information on the progress of the update.

6. Select the maximize arrow next to view the update progress.

When the update successfully completes, a green checkmark appears above this information.

Controlling services from Centralized Management

You can start, stop, or restart services from the Centralized Management.

Before you begin

Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

1. Log in and select **Administration** > **Centralized Management**.
2. Select the server in **Physical Overview**.
3. In the **Services** tab, select the module.
4. Click one of the following buttons.

Operation	Description
Start	Starts the service.
Stop	Stops the service.
Restart	Restarts the service.

Read the status message.

Default ReportPack migration

Update the Default ReportPack to ensure you use the latest SolutionPack template.

Update the Default ReportPack from the Administration menu after logging in to the User Interface URL, for example, `http://<Frontend-hostname>:58080/APG`

The Default ReportPack contains the default reports. To access all of the new report features available in a software release, update the Default ReportPack during the migration process.

1. Back up the existing Default ReportPack by exporting the `.arp` file.
2. Upload the Default ReportPack.
3. Delete the old ReportPack.

Note

Scheduled reports, pre-generated reports and template restrictions are lost when you delete the old Default ReportPack. The online help describes methods for exporting ReportPack templates so you can save them.

Exporting a ReportPack

You can export a ReportPack to back up the `<ReportPack>.arp` file or for use in another system.

Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.

4. Click **Export** to download the `<ReportPack>.arp` file that contains the required information and templates.
5. Click **Save** to navigate to the download location.

Updating the Default ReportPack

Update your existing Default ReportPack by replacing it completely with a new Default ReportPack.

Before you begin

- ◆ Ensure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.
- ◆ Locate the new `Default ReportPack.arp` file. The file is located on the server in `<INSTALL_DIR>/Web-Servers/Tomcat/Default/webapps/APG`. If you are accessing the server remotely, you will need to download the `.arp` file to your local directory first.

Procedure

1. Log in and select **Administration > ReportPacks** to access **ReportPacks Management**.
Available ReportPacks are listed in a pane.
2. Rename the existing Default ReportPack to distinguish between the existing one and the new one.
 - a. Select **Default ReportPack** in the pane.
 - b. Type **(original 6.2)** in the **Name** field.
The **Name** field value reads: Default ReportPack (original 6.2)
 - c. Click **Save**.
You are returned to **ReportPacks Management**.
3. Click **Upload a ReportPack**.
4. Select the `Default ReportPack.arp` file from your local directory.
5. Click **Save**.

After you finish

If you are satisfied with the resulting reports , you can delete the old Default ReportPack.

Note

Scheduled reports, pre-generated reports and template restrictions will be lost if you remove it.

Deleting a ReportPack

When a ReportPack is no longer needed, you can remove it and its report templates.

Procedure

1. Click **Administration**.
2. Under **ReportPacks**, click **List / Import ReportPacks**.
3. Select the ReportPack.

4. Click **Delete** to remove the ReportPack and its templates.
5. Click **Ok** at the warning message.

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- ◆ Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
 - a. Type the instance name.
 - b. Select the server in one or more list boxes. For example, select the server in the **Data collection, Reports, and Events** list boxes.
 - c. Click **Next**.
8. For each list box you select, a screen appears.
 - a. Click **Next** after you complete each screen.
 - b. Click **Install** after you complete the last screen.

The installation process begins.
9. Select the maximize arrow next to each component to view the installation process.

When the installation successfully completes, green checkmarks appear.
10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Install the SolutionPack for EMC Watch4net Health if you have not already done so. This is available from **Centralized Management** > **SolutionPack Center**.

Reviewing reports

After you install a new release or migrate to a new release, check the reports to ensure that the data appears properly.

Before you begin

If the collector configuration changed, you can manually run the scheduled tasks in **Administration > Centralized-Management > Scheduled Tasks > Database** to speed up the report generation process. Wait at least two polling cycles before manually running the scheduled tasks.

To view your report:

Procedure

1. Navigate to **User Interface > SolutionPacks** or **User Interface > ReportPacks** depending upon which features you have installed.
2. Click the SolutionPack or ReportPack you want to view.

Results

It may take several polling cycles to display all relevant information.

CHAPTER 6

Uninstallation

This chapter includes the following topics:

◆ Overview.....	68
◆ Stopping core software services on a UNIX server.....	68
◆ Uninstalling core software from a UNIX server.....	68
◆ Stopping core software services on a Windows server.....	68
◆ Uninstalling core software from a Windows server.....	69
◆ Uninstalling a SolutionPack.....	69

Overview

You can uninstall a SolutionPack and uninstall core software from a UNIX or Windows server.

Stop the core software services before uninstalling core software.

Stopping core software services on a UNIX server

Use the `manage-modules.sh service stop` command to stop a specific core software service or to stop all core software services on a UNIX server.

Before you begin

Make sure you have logged in with root or APG privileges.

Procedure

- ◆ Type `manage-modules.sh service stop <service_name>` from the `bin` directory of the installation to stop a specific core software service.

This example shows how to stop all core software services:

```
./manage-modules.sh service stop all
```

Uninstalling core software from a UNIX server

Use the `manage-modules.sh service remove all` command to uninstall all core software services.

Before you begin

Make sure you have a login with root privileges.

Procedure

1. Type `manage-modules.sh service remove all` from the `/opt/APG/bin` directory to uninstall all core software services.
2. Type `rm -rf /opt/APG` to remove the installation directory.

Stopping core software services on a Windows server

Use this procedure to stop core software services from the Windows desktop.

Before you begin

Make sure you have logged in with system administrator credentials to manage services.

Procedure

1. From the application desktop, select **Start > Administrative Tools > Services**.
2. Right-click each service and click **Stop**, in order:
 - APG MySQL
 - APG Backend
 - APG Alerting Backend
 - APG Collector Manager
 - APG Tomcat
 - APG Task Scheduler
 - APG Webservice Gateway

Uninstalling core software from a Windows server

Use the `manage-modules.cmd service remove all` command to remove all core software services from a Windows server.

Before you begin

Make sure you have logged in with system administrator credentials.

Procedure

1. Type `manage-modules.cmd service remove all` from the `C:\Program Files\APG\bin` folder to uninstall all core software services.
2. Use the **Windows Control Panel** to uninstall core software.
 - a. Click **Start > Control Panel > Programs**.
 - b. Click **Uninstall a program**.
 - c. Select the **Watch4net Solutions APG** and click **Uninstall**.

Uninstalling a SolutionPack

If you no longer want to view the reports of a certain SolutionPack, you can uninstall that SolutionPack from the server.

Procedure

1. Log in with administrator credentials for core software and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select the SolutionPack that you want to uninstall in the **Installed SolutionPacks** screen.
5. In the **Properties** area, click **Trashcan** icon for each instance of the SolutionPackBlock and click **Remove**.

CHAPTER 7

Software Updates

This chapter includes the following topics:

- ◆ [Product updates](#).....72

Product updates

Follow the procedures in this section to update the full core software installation, to update SolutionPack files before installing the SolutionPack for the first time, or to update an existing installed SolutionPack.

To update from software versions prior to this version of core software, use the procedures in the *EMC Watch4net Migration Guide* for legacy core software.

Update core software

- ◆ [Updating the core software installation on page 72](#)

Update SolutionPack software for your core software installation

- ◆ [Module update order for multiple hosts on page 32](#)
- ◆ [Updating modules on page 35](#)
- ◆ [Installing a SolutionPack Center Update on page 77](#)

Update a SolutionPack that is already installed

- ◆ [Module update order for multiple hosts on page 32](#)
- ◆ [Updating modules on page 35](#)
- ◆ [Updating an existing SolutionPack on page 80](#)

Install a ReportPack

- ◆ [Uploading a <ReportPack>.arp file on page 81](#)

Updating the core software installation

Run the installer to update the core software installation. After the installer detects an existing installation, it copies the newer installation into the module repository, which is in `<INSTALL_DIR>/Tools/Module-Repository`.

Before you begin

- ◆ Ensure that the installation update is downloaded from EMC Online Support to the installation directory, such as `/INSTALL_DIR`
- ◆ Ensure you have a login with root or system administrator privileges to perform this task.

Procedure

1. Go to the installation directory.
2. Change the permissions of the installer so you can run it.

For example, for the Linux 64-bit executable, type:

```
chmod +x setup-linux-x86_64-v63u1.sh
```

3. Run the installer for your operating system from the installation directory:

Operating system	Command
UNIX	<code>setup-linux-x86_64-<version_number>.sh</code>
Windows	<code>setup-win64-<version_number>.exe</code>

4. Answer any questions.
5. After the installation update is complete, identify the modules to update.

[Identifying which modules to update on page 32](#)

6. Update the modules.

[Updating modules on page 35](#)

Identifying which modules to update

After you update a core software installation, run the `manage-modules.sh list installed` command to view the installed modules and to determine which modules to update. Update the modules with the status of `can be updated`.

Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh list installed</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd list installed</code>

When you view the output, record the identifier value of each module that needs to be updated. You will need to specify the identifier later when you update the module.

This sample output indicates to update the Module-Manager first, then to update the Alerting-Backend and the Alerting-Frontend modules to version 3.5. For other lines, pay attention to the status recommendations.

```
! WARNING: A more recent version of the module-manager is available. It is strongly
recommended to upgrade it before anything else.
Installed Modules:
```

Identifier Revision OS-Arch	Instance Status	:Category	Module Name	Version
-----	-----	-----	-----	-----
* alerting-backend r4123 linux-x64	Default can be updated to v3.5	:Backends	Alerting-Backend	v3.1u2
* alerting-frontend r4123 linux-x64	alerting-frontend can be updated to v3.5	:Web-Applications	Alerting-Frontend	v3.1u2

Module update order for multiple hosts

Update modules in a specific order to avoid issues involving software dependencies and redundant files. Modules that are available for update are marked with an yellow star icon in Centralized Management. If a Module-Manager update is available, always update this module first. Refer to the release notes or the workflow for your deployment scenario for additional recommendations.

Depending on your installed SolutionPacks, the list of modules needing to be updated will vary. When updating modules in a multiple host deployment, follow these recommendations:

- ◆ Update a subset of core modules (Group A) on the Centralized Management server first using the CLI command, `manage-modules.sh update` or `manage-modules.cmd update`.
- ◆ After updating the last core module in Group A, update the services and then start the services.
- ◆ After retrieving modules from the remote host servers, launch the update of a second subset of modules (Group B) from **Centralized Management > Logical Overview**. A few modules require an additional manual CLI update step on the remote host servers.

- ◆ Update Independent SolutionPackBlocks.
- ◆ Update SolutionPackBlocks.

Note

Do not update any other modules, even if they display in **Centralized Management > Logical Overview** with the yellow star update icon.

Table 9 Group A: Core modules for CLI update

Update these core modules using CLI commands.
module-manager
java
license-manager
mysql (optional, but recommended)
jdbc-drivers
tomcat
WebApps, includes one or more of these modules if marked for update: • alerting-frontend • centralized-management • device-discovery • frontend • frontend-ws • mib-browser • ip-sla-probes • transaction-collector-gui
webapps-resources
webservice-gateway

Table 10 Group B: Launch the update from Centralized Management > Logical Overview

Core module update order	Node in Logical Overview	Notes
module-manager	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, (manage-modules.sh update module-manager or manage-modules.cmd update module-manager) on the remote host to apply the update.
java	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI

Table 10 Group B: Launch the update from Centralized Management > Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
		command, (manage-modules.sh update java or manage-modules.cmd update java) on the remote host to apply the update. Ensure all services are restarted after updating java. (manage-modules.sh service start all or manage-modules.cmd service start all
license-manager	Miscellaneous	
mysql	Databases	
jdbc-drivers	Databases	
tomcat	Miscellaneous	The update stops the service. If the display indicates the service failed to stop, retry the update.
alerting-frontend	Frontends	
centralized-management	Frontends	
device-discovery	Frontends	
frontend	Frontends	
frontend-ws	Frontends	
mib-browser	Frontends	
ip-sla-probes	Frontends	
transaction-collector-gui	Frontends	
webapps-resources	Miscellaneous	
webservice-gateway	Miscellaneous	Launch from Logical Overview to send the module update to the remote host server. You must also issue the CLI command, (manage-modules.sh update webservice-gateway or manage-modules.cmd update webservice-gateway) on the remote host to apply the update.
alerting-backend	Backends	
apg-backend	Backends	
apg-property-store	Databases	
administration-tool	Miscellaneous	
diagnostic-tools	Miscellaneous	
frontend-report-generator	Miscellaneous	

Table 10 Group B: Launch the update from Centralized Management › Logical Overview (continued)

Core module update order	Node in Logical Overview	Notes
frontend-search	Miscellaneous	
task-scheduler	Miscellaneous	
topology-cli	Miscellaneous	

When updating multiple modules, update first by Category and then by Module Name.

The Frontend and SNMP module families are not used in all deployments.

Since modules belonging to the Frontend family have logical interdependencies, the modules must be updated to the same version or problems may occur.

Modules belonging to the SNMP family also have logical interdependencies and must be updated to the same version.

You can view the Category and Module Name values by using the `manage-modules.sh list installed` command or by viewing the nodes in **Centralized Management › Logical Overview**.

Updating modules

Run the `manage-modules.sh update <identifier>` command to update the modules and their managers. Some modules may request information from you during an update. For example, you may be prompted for a module instance name if there are multiple instances, whether you want to continue the update, and whether you want to keep the original copy of a file that is updated.

Before you begin

- ◆ Obtain the identifier by using the `manage-modules.sh list installed` command.
- ◆ Make sure you have a login with root or system administrator privileges to update modules.

Update the manager of the module first before updating the module. Use the same command and substitute the appropriate identifier.

Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh update <module_identifier> [<module_instance>]</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd update <module_identifier> [<module_instance>]</code>

2. Answer any questions.

manage-modules.sh update command

Use the `manage-modules.sh update` command to update modules and their managers. Type the command for your operating system from the `bin` directory of your core software installation directory.

Description

The `manage-modules.sh update` command updates installed modules and their managers. For UNIX, specify `manage-modules.sh update`. For Windows, specify `manage-modules.cmd update`.

Update the manager of the module first before updating the module.

To look up the identifier and module instance name, use the `manage-modules.sh list installed` command.

Syntax

```
manage-modules.sh update <module_identifier> [ <module_instance> ]
```

Options

module_identifier

The identifier value of the installed module or manager.

module_instance

The unique name of the module or manager. Omit this value if only one instance is installed since the command will use it as the default. If multiple instances exist, specify the instance you want to update or the command will prompt you for the instance name. The identifier and instance values form a unique key to refer to the module or manager.

Example # 1

In this Linux example, the following commands update the manager, Collector-Manager, and a corresponding module, XML-Collector.

```
<INSTALL_DIR>/bin/manage-modules.sh update collector-manager
<INSTALL_DIR>/bin/manage-modules.sh update xml-collector
```

Example # 2

In this Windows example, the following commands update the Tomcat Web server and a corresponding module, MIB-Browser.

```
<INSTALL_DIR>\bin\manage-modules.cmd update tomcat
<INSTALL_DIR>\bin\manage-modules.cmd update mib-browser
```

Example # 3

In this Linux example, the following commands update specific instances.

```
./manage-modules.sh update tomcat instance3
./manage-modules.sh update mib-browser mymib_browser2
```

Installing a SolutionPack Center Update

Periodically, updates of the SolutionPacks are available in a .zip file called SolutionPackCenter Update on EMC Online Support. This .zip file contains a README file

that describes the changes made to each SolutionPack and individual `<solution>.pkg` files for installing each update.

Before you begin

- ◆ Install the required license file to enable your SolutionPack.
- ◆ Ensure any Domain Managers that supply data to the SolutionPack are installed and configured.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user `apg` is the account that the core software application uses instead of root.
- ◆ Update the core modules in all servers before you update or install a SolutionPack after upgrading your base installation.

Core modules are modules that are not installed by a SolutionPackBlock. Examples of core modules include `webapps`, `module-manager`, `license-manager`, `java`, `mysql`, `backend`, `tools`, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Examples of modules that are installed with SolutionPackBlocks include `collector-manager`, `event-processing-manager`, and collector or event components.

Procedure

1. Locate the Watch4net downloads area on EMC Online Support.
 - a. Go to `https://support.emc.com`.
 - b. Click **Support by Product**.
 - c. Type **Watch4net** in the **Find a Product** field, and then click the arrow next to it.
 - d. Click **Downloads**.

The **Downloads for Watch4net** page appears.

2. Download the latest SolutionPackCenter Update to a local directory.
For example: SolutionPackCenter Update `<month> <year>`
3. Browse to **Administration > Centralized-Management > Packages Management** and click **Upload**.
4. Browse to the SolutionPackCenter Update .zip file and click **OK**.

After you finish

Update the SolutionPackBlocks after installing the SolutionPack update: [Updating the SolutionPackBlocks on page 43](#).

Browse to **Administration > Centralized Management > SolutionPacks > SolutionPack Center** and install the SolutionPack.

You can confirm the SolutionPack version number by browsing **SolutionPacks** in the left panel.

Updating the SolutionPackBlocks

After installing a software update or migrating from an older release, you must update SolutionPackBlocks in order to use the latest module configurations and report templates. This block update may trigger the update of an associated module.

Before you begin

- ◆ Be sure you have updated core modules (except for blocks, collectors, and event processors) in all of the servers before you update SolutionPackBlocks.

Procedure

1. Click the **SolutionPacks** node on the left panel to access **Installed SolutionPacks**.

Two panes appear: Independent SolutionPackBlocks and SolutionPacks. Update the Independent SolutionPackBlocks first before you update the SolutionPackBlocks that belong to the SolutionPacks.

2. Do the following to locate the block that you want to update:

In the pane for	Perform:
Independent SolutionPackBlocks	Locate the block.
SolutionPacks	a. Select the specific SolutionPack. b. Locate the block in the Properties page.

3. Click the **yellow star icon**.

The **SolutionPack Update** page appears.

4. Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

5. Click **Update**.

The update process begins. The **SolutionPack Update** page provides information on the progress of the update.

6. Select the maximize arrow next to view the update progress.

When the update successfully completes, a green checkmark appears above this information.

Reconfiguring a SolutionPack in Centralized Management

You can reconfigure a SolutionPack by modifying its settings in Centralized Management.

Procedure

1. Navigate to **Centralized Management**.
2. Click the **SolutionPacks** node on the left panel to display the existing installed SolutionPacks.
3. Depending on whether the SolutionPackBlock is an independent block or component of a SolutionPacks, do the following to locate the instance that you want to reconfigure:

In the pane for	Perform:
SolutionPacks	a. Select the SolutionPack.

In the pane for	Perform:
	b. Locate the instance in the Properties page.
Independent SolutionPackBlocks	Locate the instance.

4. Click the **Pencil** icon next to the instance for the SolutionPackBlock.
5. In the **SolutionPack Reconfiguration** screen for each SolutionPackBlock, change one or more settings and click **Reconfigure**.

Updating an existing SolutionPack

Periodically, updates of the SolutionPacks are available in a .zip file called SolutionPackCenter Update on EMC Online Support. This .zip file contains a README file that describes the changes made to each SolutionPack and individual `<solution>.pkg` files for installing each update.

Before you begin

1. Download the SolutionPack from EMC Online Support to a local directory.
2. Upload the SolutionPack to the server where the core software is running.
3. Update the core modules in all of the servers before you update an existing SolutionPack.

The modules used by a SolutionPack are updated with the latest version in the module repository during this process. This may override customizations made to .xml files and reports.

Core modules are modules that are not installed by a SolutionPackBlock. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Examples of modules that are installed with SolutionPackBlocks include collector-manager, event-processing-manager, and collector or event components.

Procedure

1. Log in with administrator credentials for core software.
2. Browse to **Administration > Centralized Management > Packages Management**.
3. Click **SolutionPacks** on the left panel to display the existing installed SolutionPacks.
4. Select the SolutionPack to update.

A **Properties** page appears for the selected SolutionPack, which includes all related SolutionPackBlocks.

5. Select the SolutionPackBlock to update by clicking on its yellow star icon.

The **SolutionPack Update** page appears.

6. Carefully review the settings on this page and make changes as needed.

Most values are from the existing SolutionPack but some may be default values for the new SolutionPack.

7. Click **Update**.

The **SolutionPack Update** page provides information on the progress of the update. When the update successfully completes, a green checkmark appears above this information.

8. Click **SolutionPacks** on the panel to list the existing installed SolutionPacks.

The updated SolutionPack with its new version and updated SolutionPackBlock appear in this list.

ReportPack Installation

Some Watch4net features are distributed as Reportpacks instead of SolutionPacks. If you need to install or update a ReportPack, download the *ReportPack.zip* file from EMC Support Zone and unzip it in any directory on the server where the Collector Manager is installed.

Copy the unzipped ReportPack files to the appropriate folders as explained in the installation instructions that are in each *ReportPack.zip* file. Ensure the ReportPack license file is installed. [Uploading a ReportPack.arp file on page 81](#) explains how to install the *ReportPack.arp* file. For some ReportPacks, you may need to configure filters and wait for completion of two or more polling cycles before data will populate in the reports.

Uploading a *ReportPack.arp* file

You can add a *ReportPack.arp* file that contains required information and report templates. The ReportPack appears as a root node branch in the tree.

Procedure

1. Click **Administration**.
2. Click **ReportPacks**.
3. Click **Upload a ReportPack** and select **Choose File** to browse to the *ReportPack.arp* file.
Upload only .arp file types.
4. Click **OK**.

Results

A message displays,

The file has been uploaded successfully.

Click **Continue**.

CHAPTER 8

Troubleshooting

This chapter includes the following topics:

- ◆ [Troubleshooting service start-up problems on UNIX](#).....84
- ◆ [Troubleshooting service start-up problems on Windows](#)..... 84
- ◆ [SSL certificates](#)..... 84

Troubleshooting service start-up problems on UNIX

Check the log files when services do not start.

Before you begin

Make sure you have logged in with root or APG privileges to check the log files.

Procedure

- ◆ Check these logs in the /opt/APG/ directory to troubleshoot start-up problems:

```
Databases/MySQL/Default/data/[SERVER NAME].err
Backends/Alerting-Backend/Default/logs/alerting-0-0.log
Backends/APG-Backend/Default/logs/cache-0-0.log
Collecting/Collector-Manager/Default/logs/collecting-0-0.log
Web-Servers/Tomcat/Default/logs/service.log
Tools/Task-Scheduler/Default/logs/scheduler-0-0.log
Tools/Webservice-Gateway/Default/logs/gateway-0-0.log
```

Troubleshooting service start-up problems on Windows

Check the log files when services do not start.

Before you begin

Make sure you have logged in with system administrator credentials to check the log files.

Procedure

- ◆ Check these logs in the C:\Program Files\APG directory to troubleshoot start-up problems:

```
Databases\MySQL\Default\data\[SERVER NAME].err.
Backends\Alerting-Backend\Default\logs>alerting-0-0.log
Backends\APG-Backend\Default\logs\cache-0-0.log
Collecting\Collector-Manager\Default\logs\collecting-0-0.log
Web-Servers\Tomcat\Default\logs\service.log
Tools\Task-Scheduler\Default\logs\scheduler-0-0.log
Tools\Webservice-Gateway\Default\logs\gateway-0-0.log
```

SSL certificates

Generally, EMC products are distributed with a self-signed SSL certificate. If you receive an SSL certificate error or a blank pane when you are attempting to access content served by a data source, resolve the issue by doing one of the following procedures.

[SSL certificate error examples on page 85](#) provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: [Troubleshooting an SSL certificate error: Accepting the exception on page 85](#).

Permanent resolution

Add an SSL certificate to your truststore to permanently prevent the exceptions from appearing.

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using an Internet Explorer browser.	Installing a self-signed SSL certificate from an Internet Explorer browser on page 85

You can:	Perform:
Install the self-signed SSL certificate that is provided with the EMC product using a Chrome or Firefox browser.	1. Export the self-signed SSL certificate to save it to the export location: Exporting an SSL certificate from an Internet Explorer browser on page 87 2. Importing an SSL certificate into your truststore on page 86
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 86

If you need to prepare an SSL certificate to share with other users, use: [Exporting an SSL certificate from an Internet Explorer browser on page 87](#).

SSL certificate error examples

The SSL certificate error or a blank pane appears because the certificate is self-signed and it is not added as an exception or into the truststore yet. For example, if you are attempting to access content served by a data source, a blank pane appears when you select views under **SolutionPacks**.

Chrome error examples

This site's security certificate is not trusted!

Or, a blank pane.

Firefox error example

This Connection is Untrusted

Internet Explorer error examples

There is a problem with this website's security certificate.

Content was blocked because it was not signed by a valid security certificate.

Troubleshooting an SSL certificate error: Accepting the exception

An SSL certificate error appears in your browser.

To resolve this issue,

Procedure

- ◆ Accept the exception.

Steps may vary for your browser. For example, for Internet Explorer, click **Continue to this website (not recommended)**.

This temporary solution causes the exception to be ignored for the current browser session, but the exception reappears if you open another browser tab or window.

Installing a self-signed SSL certificate from an Internet Explorer browser

Install the self-signed SSL certificate that is provided with the EMC product to prevent certificate exception errors.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Click **Continue to this website (not recommended)** in the browser window.
2. Click the red **Certificate Error** indicator next to the address bar.
3. In the **Untrusted Certificate** window, select **View certificates**.
4. In the **Certificate** dialog box, in the **General** tab, click **Install Certificate**.
5. Follow the instructions in the **Certificate Import Wizard**.
 - a. Select the **Place all certificates in the following store** setting to add the certificate to your truststore.
6. In the **Certificate** dialog box, in the **General** tab, click **OK**.

After you finish

Refresh the browser window.

Importing an SSL certificate into your truststore

Import an SSL certificate into your truststore to prevent certificate exception errors.

Procedure

- ◆ Import the certificate using one of the following procedures:
 - [Importing an SSL certificate in Chrome on page 86](#)
 - [Importing an SSL certificate in Firefox on page 86](#)
 - [Importing an SSL certificate in Internet Explorer on page 87](#)

Importing an SSL certificate in Chrome

For Chrome, use this procedure to import the certificate into your truststore.

The following procedure is for Chrome version 28.0.1500.95. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Settings > Show advanced settings**.
2. Scroll down and select **HTTP/SSL > Manage Certificates**.
3. In the **Trusted Root Certification Authorities** tab, click **Import**.
4. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
5. Click **OK** in **Internet options**.
6. Refresh the browser window.

Importing an SSL certificate in Firefox

For Firefox, use this procedure to import the certificate into your truststore.

The following procedure is for Firefox version 23.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Firefox > Options > Options**.
2. Click **Advanced**.
3. In the **Certificates** tab, click **View Certificates**.

4. Click **Import**.
5. Locate the certificate file and click **Open**.
6. Click **Save**.
7. Click **OK** in **Certificate Manager**.
8. Refresh the browser window.

Importing an SSL certificate in Internet Explorer

For Internet Explorer, use this procedure to import the certificate into your truststore.

The following procedure is for Internet Explorer version 9.0. The steps may vary slightly depending on your browser version.

Procedure

1. Go to **Tools** > **Internet options**.
2. In the **Content** tab, click **Certificates**.
3. Select the **Trusted Root Certification Authorities** tab.
4. Click **Import**.
5. Follow the instructions in the **Certificate Import Wizard** to import the certificate.
6. Click **OK** in **Internet options**.
7. Refresh the browser window.

Exporting an SSL certificate from an Internet Explorer browser

Use this procedure to export a self-signed SSL certificate, so that you can either import the resulting exported certificate into your truststore or share it with other users.

The following procedure is for Internet Explorer version 10.0. The steps may vary slightly depending on your browser version.

Procedure

1. Access the host for which you want to export the SSL certificate from the browser.
For example: `https://<myHostname>.emc.com`
2. Select **Continue to this website (not recommended)** in the **There is a problem with this website's security certificate** window.
3. Click the red **Certificate Error** indicator next to the address bar.
4. In the **Untrusted Certificate** window, select **View certificates**.
5. In the **Certificate** dialog box, select the **Details** tab and ensure that the Show field is set to All. Click **Copy to File**.
6. In the **Certificate Export Wizard**,
 - a. Click **Next** in the **Welcome** screen.
 - b. Click **Next** to accept the default DER encoded binary X.509 setting in the **Export File Format** screen.
 - c. Browse to the location where you want to save the certificate.
 - d. Specify the certificate file name and click **Save**.
 - e. In the **File name** field, ensure that the location and the certificate file name are correct. Click **Next**.

- f. Click **Finish**.
 - g. Click **OK** when The export was successful appears.
- 7. In the **Certificate** dialog box, click **OK** in the **Details** tab.
- 8. Share the resulting exported SSL certificate with other users to use.

APPENDIX A

Available Modules

This appendix includes the following topics:

- ◆ [Available modules](#).....90

Available modules

These modules are available in the core software version 6.3 installation:

Table 11 Version 6.3 available modules

Module Name	Version	Install type
Active-Cache	v1.0u5	Backend
Administration-Tool	v1.1	Default / Frontend / Backend
alert-consolidation	v0.1	Default / Backend
Alerting-Backend	v3.6	Default / Backend
Alerting-Frontend	v3.6	Default / Frontend
APG-Self-Monitoring-Collector	v1.3u1	Collector
Availability-Filter	v1.3u1	Collector
APG-Backend	v5.6	Default / Backend
APG-Backend-Data-Sender	v1.0u1	Backend
BroadSoft-VolP-Collector	v2.3	Collector
brocade-fc-switch	v1.1u99	Frontend
Centralized-Management	v2.2	Default / Frontend
cisco-ipsla	v1.0	Frontend
cisco-mds-nexus	v1.0u99	Frontend
cisco-qos	v1.0	Frontend
cisco-ucs	v1.0	Frontend
Cisco-VolP-Collector	v2.2	Collector
Collector-Manager	v5.4	Collector
Compliance-Backend	v1.0	Backend
Compliance-Frontend	v1.0	Default / Frontend
Cross-Referencing-Filter	v1.3	Collector
Crossed-Failover-Filter	v1.1u2	Collector
APG-Datastore	v5.0	Database
APG-Datastore-Writer	v2.0	Backend
Delay-Filter	v5.0u2	Collector
Delta-Rate-Filter	v5.0u2	Collector
Device-Discovery	v3.0u4	Default / Frontend
Device-Discovery-CLI	v3.1	Backend
APG-Diagnostic-Tools	v6.0	Default / Frontend / Backend / Collector
emc-centera	v1.2u99	Frontend
emc-data-domain	v1.0	Frontend

Table 11 Version 6.3 available modules (continued)

Module Name	Version	Install type
emc-dpa	v0.6	Frontend
emc-isilon	v1.3u99	Frontend
emc-ncm	v1.1	Frontend
emc-prosphere	v2.1	Frontend
emc-recoverpoint	v0.1u1	Frontend
emc-smarts	v1.3	Frontend
emc-smarts-console	v1.1	Frontend
emc-vipr	v1.1u99	Frontend
emc-vmax	v2.1u99	Frontend
emc-vnx	v1.9u99	Frontend
emc-vplex	v1.4u99	Frontend
emc-watch4net-health	v1.2u99	Frontend
Event-Aggregator	v1.8	Collector
Event-Change-Detector	v1.0u2	Backend
Event-Failover	v1.0u1	Backend
Event-Key-Modifier	v1.1	Backend
Event-Log-Processor	v1.2u3	Backend
Event-Processing-Manager	v1.2u3	Frontend
Event-Processing-Utils	v1.2u1	Backend
Event-Property-Tagger	v2.6	Backend
FailOver-Filter	v5.1	Collector
Flow-Listener	v1.8	Backend
Formulas	v6.2u1	Frontend
APG-Frontend	v6.3	Default / Frontend
Frontend-Report-Generator	v6.3	Default / Frontend
Frontend-Search	v6.3	Default / Frontend
APG-Web-Service	v6.3	Default / Frontend
generic-compliance	v0.1	Frontend
generic-converged-infrastructure	v1.0	Frontend
Generic-Event-Listener	v1.1u1	Backend
Generic-Event-Sender	v1.2	Backend
Generic-Event-Transmitter	v1.0u1	Backend
Generic-Event-Writer	v1.1u1	Backend

Table 11 Version 6.3 available modules (continued)

Module Name	Version	Install type
generic-host	v0.5	Collector
generic-host-agent	v0.4	Backend
Generic-Live-Writer	v1.2	Backend
generic-rsc	v0.5	Default / Collector
generic-snmp	v1.2u99	Default / Collector / Block
generic-topology	v0.1	Default / Backend
Group-Filter	v1.0	Collector
hitachi-device-manager	v1.0	Frontend
hp-eva	v1.0	Frontend
hp3par-storeserv	v1.1u99	Frontend
ibm-ds	v1.0	Frontend
ibm-svc	v1.0	Frontend
ibm-xiv	v1.1u99	Frontend
Index-Generator-Filter	v5.0u2	Frontend
Inline-Calculation-Filter	v6.0	Frontend
IP-SLA-Filter	v5.2u2	Frontend
IP-SLA-Probe-Configuration	v2.3u3	Frontend
IP-SLA-Probe-Configuration-CLI	v2.3u4	Frontend
Sun-JRE	v6.0u45	Default
JDBC-Drivers	v2.0	Database
JMS-Listener	v1.1u1	Backend
JMX-Collector	v1.3u1	Collector
License-Manager	v5.2	Default / Minimal / Frontend / Backend / Collector
Load-Balancer	v1.2	Default / Backend
load-balancer-arbiter	v1.0	Default / Backend
load-balancer-connector	v0.1	Backend
Mapped-Property-Tagged-Filter	v5.0u2	Collector
Maps-Service	v1.0	Default / Frontend
Mib-Browser	v6.3	Default / Frontend
microsoft-hyperv	v1.1	Frontend
Module-Manager	v1.6	Default
MySQL	v5.5u1	Default / Backend / Database

Table 11 Version 6.3 available modules (continued)

Module Name	Version	Install type
MySQL-Maintenance-Tool	v1.3	Default / Backend
Mysql-Resynchronizer	v1.1	Backend
netapp-filer	v2.1u99	Frontend
APG-Notification-View	v2.6u1	Frontend
oracle-database	v1.1	Database
Outage-Manager	v1.1u2	Backend
Property-Concat-Filter	v5.0u2	Backend
APG-Property-Store	v1.2	Default / Frontend / Database
Property-Tagging-Filter	v2.6	Collector
Remote-Shell-Collector	v1.3	Collector
Remote-SNMP-Collector-CLI	v6.3	Backend
Smarts-Collector	v5.3u1	Collector
Smarts-Listener	v1.3u1	Backend
SNMP-Collector	v6.3	Collector
Spatial-Aggregation-Filter	v5.1	Collector
SQL-Collector	v1.4	Collector
Storage-Filter	v2.1	Collector
Task-Scheduler	v1.4	Default / Backend
Text-Collector	v1.10	Collector
Timestamp-Sysuptime-Matching-Filter	v5.0u2	Collector
Tomcat	v6.0u37	Default
Topology	v1.5	Default
Topology-Mapping-Service	v1.0	Backend
Topology-Service	v1.0	Default / Backend
APG-Traceroute-Tool	v1.2u1	Frontend
Transaction-Collector	v1.6	Collector
Transaction-Collector-GUI	v1.5	Frontend
Transaction-Listener	v1.2u2	Backend
Trap-Receiver	v1.1u1	Backend
Value-Offset-Filter	v5.0u1	Collector
Variable-Handling-Filter	v1.9	Collector
VMWare-Collector	v2.3	Collector

Table 11 Version 6.3 available modules (continued)

Module Name	Version	Install type
VMWare-Listener	v1.3u1	Backend
vmware-vcenter	v1.2u99	Frontend
WebApps-Resources	v1.3	Default
Webservice-Gateway	v1.2	Default / Minimal / Frontend / Backend / Collector
WhatIf-Scenario-CLI	v1.0	Backend
XML-Collector	v1.9	Collector

APPENDIX B

Virtual Appliance Installation

This appendix includes the following topics:

- ◆ Virtual Appliance installation for Watch4net.....96
- ◆ Deploying an appliance.....96
- ◆ Starting the appliance 98
- ◆ Verifying the appliance deployment98
- ◆ Log onto the appliance 98
- ◆ Installing a SolutionPack.....99
- ◆ Reviewing reports.....100

Virtual Appliance installation for Watch4net

You can deploy the Watch4net as a virtual appliance (vApp) in a vSphere or vCloud environment, as an alternative to the standard installation.

A virtual appliance (vApp) is a software solution composed of one or more virtual solutions that is packaged by an appliance vendor and can be deployed, managed, and maintained as a unit.

vApps are distributed using Open Virtualization Format (OVF) files. Depending on your environment requirements, two types of OVF installations are available to install the Watch4net core software:

- ◆ Four VM vApp installation - Distributes Watch4net core software components across four VMs (Frontend, Primary Backend, Additional Backend, Collector). The appliances in this installation are pre-configured to communicate with each other, offering an out-of-the-box configuration that can function in smaller environments. You can further scale and extend the environment by installing additional virtual appliances using the one VM vApp installation.
- ◆ One VM vApp installation - Has the potential to install any of the Watch4net core software components in a single VM. This can be used to either install a single, consolidated VM with all components for evaluation purposes, or to add additional Backend or Collector appliances to extend or scale the environment created using the four VM vApp installation.

Note

The vApp deployment should be used only for new installations. If you need to upgrade an existing installation, use the standard binary setup script or executable to migrate to a newer release. The vApp deployment support was not available prior to the Watch4net 6.3 release.

Deploying an appliance

You can deploy an appliance from an OVF file using a vSphere Client.

Before you begin

- ◆ An administrator login with root privileges
- ◆ vCenter location where you are deploying the appliance
- ◆ Data store you can use for deployment
- ◆ Static IP address to assign to your appliance
- ◆ Gateway
- ◆ Netmask
- ◆ DNS Servers

Procedure

1. Open vSphere Client and connect to the vCenter Server that manages your VMware environment.
2. From the **File** menu, select **Deploy OVF Template**.
3. In the **Source** step, browse to the location of the `YourOVFfile.ovf` file.

Example file path: `/opt/ovf/YourOVFfile_OVFxx.ovf`

Example URL: `http://myHost.emc.com/ovf/snapshot/92/YourOVFfile_OVFxx.ovf`

4. Click **Next**.

To minimize the deployment time, deploy the appliance within the same local area network (LAN) shared by your VMware ESX/ESXi servers. The deployment time is approximately 5 to 15 minutes. Deployment across a WAN can take 2 hours or more.

5. In the **OVF Template Details** step, review the details of the loaded .ovf file and click **Next**.6. In the **End User License Agreement** step, review the license agreement. Click **Accept** and then click **Next** to continue.7. In the **Name and Location** step:

- a. Type a **Name** for the appliance.
- b. Specify an **Inventory Location** for the appliance within your VMware environment.
- c. Click **Next**.

8. In the **Host/Cluster** step, select a host or cluster where the appliance will run and click **Next**.9. In the **Resource Pool** step, select a resource pool associated with the host or cluster where the appliance will run and click **Next**.

Note

This step is required only if the host or cluster contains a predefined resource pool.

10. In the **Datastore** step, select a datastore to hold the appliance images and click **Next**.11. In the **Disk Format** step, select the storage space provisioning method and click **Next**.

Option	Description
Thin provisioned format	On-demand expansion of available storage, used for newer data store file systems.
Thick provisioned format	Appliance storage that is allocated immediately and reserved as a block.

Note

The **Thin provisioned format** option is recommended when the vApp is deployed in a high performance environment.

12. In the **Network Mapping** step, select a destination network that has an IP Pool associated with it and click **Next**.13. Provide the values of the properties as defined in the Virtual Appliance Properties table and click **Next**.14. In the **Ready to Complete** step, review the list of properties for the appliance and click **Finish**.

A status bar appears in the vSphere Client showing the deployment progress.

15. After deployment is complete, click **Close** in the **Deployment Completed Successfully** dialog box.

Starting the appliance

Start the appliance using vSphere after deployment. The appliance may take up to 20 minutes to start the first time. You can monitor the progress on the vSphere console.

Procedure

1. In the vSphere Client, right-click the appliance name.
2. Select **Power** > **Power On**.

The status appears in the **Recent Tasks** bar.

Verifying the appliance deployment

After deploying the appliance, verify that it is working.

Procedure

1. In the vSphere client, navigate to the **VMs and Templates** view.
2. From the configured resource pool, find the resource pool you selected for the appliance.

The new appliance is listed under the resource pool.

3. In the console, log in to the appliance with the credentials you defined during the deployment.
4. Verify the services.

Log onto the appliance

Using a browser, you can access the appliance to view and manage your applications as well as develop applications.

Procedure

1. Open a web browser.
2. Browse to the appliance at `https://hostname`.

hostname is the fully qualified domain name of your host.

A security-related dialog box may appear asking you to accept a security certificate from EMC. Accept the certificate or allow a security exception for and continue. To eliminate this message from appearing, install a Certificate Authority-signed SSL certificate.

3. Enter the default username and password.

Passwords

Use passwords to control access to the appliance.

The default usernames and passwords are:

Environment	Username and password
Web-based console accessed via a browser	admin/changeme Make sure you change this password.
Linux guest OS appliance console accessed via SSH or vSphere	root/Changeme1!

If you set the appliance console password while you were deploying the OVF, the password you entered is the default password.

Passwords must conform to the following requirements.

Note

These requirements do not apply to the Linux passwords.

- ◆ Be a minimum of eight characters and a maximum of 40 characters in length
- ◆ Contain at least one numeric character
- ◆ Contain at least one uppercase and one lowercase character
- ◆ Contain at least one non-alphanumeric character such as # or !
- ◆ May not contain the single quote character (') because it is a delimiter for the password string

Installing a SolutionPack

After you log in as an administrator, you can install a SolutionPack from Centralized Management.

Before you begin

- ◆ Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Core modules are modules that are not installed by a SolutionPack. Examples of core modules include webapps, module-manager, license-manager, java, mysql, backend, tools, and so forth. Update these core modules: **Databases, Backends, Frontends, Miscellaneous** (except Blocks). Since the recommended module update order varies, refer to the Module Update Order section for the multiple hosts or single host deployments. Also, the *EMC Watch4net Centralized Management Guide* provides more information.

Procedure

1. Log in and select **Administration**.
2. Select **Centralized Management** in the Administration tree.
3. Select **SolutionPacks** in the tree.
4. Select **SolutionPack Center**.
5. Select the SolutionPack in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
 - a. Type the instance name.
 - b. Select the server in one or more list boxes. For example, select the server in the **Data collection, Reports, and Events** list boxes.
 - c. Click **Next**.
8. For each list box you select, a screen appears.
 - a. Click **Next** after you complete each screen.
 - b. Click **Install** after you complete the last screen.

The installation process begins.

9. Select the maximize arrow next to each component to view the installation process.

When the installation successfully completes, green checkmarks appear.

10. After installation is complete, select **Centralized Management** > **SolutionPack** to verify the installed SolutionPack.

After you finish

Install the SolutionPack for EMC Watch4net Health if you have not already done so. This is available from **Centralized Management** > **SolutionPack Center**.

Reviewing reports

After you install a new release or migrate to a new release, check the reports to ensure that the data appears properly.

Before you begin

If the collector configuration changed, you can manually run the scheduled tasks in **Administration** > **Centralized-Management** > **Scheduled Tasks** > **Database** to speed up the report generation process. Wait at least two polling cycles before manually running the scheduled tasks.

To view your report:

Procedure

1. Navigate to **User Interface** > **SolutionPacks** or **User Interface** > **ReportPacks** depending upon which features you have installed.
2. Click the SolutionPack or ReportPack you want to view.

Results

It may take several polling cycles to display all relevant information.

APPENDIX C

Restoring Modules to their Previous Version

This appendix includes the following topics:

- ◆ [Restoring modules workflow](#)..... 102
- ◆ [Listing restorable modules](#)..... 102
- ◆ [Restoring modules](#)..... 103
- ◆ [Starting the core software services from the command line](#)..... 105
- ◆ [Starting the core software services on Windows](#)..... 105

Restoring modules workflow

If you need to, you can revert to the previous version of core software after an update. For example, an update of version 6.3.x software is completed and you need to revert to version 6.2.x on the same host. If the software is installed on multiple servers, you need to perform the restore process on each server.

Restoring the modules does not restore them to their exact state prior to an upgrade. The reason is that during the update process, some modules may modify their data files to work for newer version. Once the data files are modified, they cannot revert to their previous state.

The Module-Manager cannot be restored to its previous version. The 6.3.x version of Module Manager is fully compatible with version 6.2.x and can be used in its place.

Make sure you have a login with root or system administrator privileges to restore modules.

For single host or multiple host deployments:

1. [Listing restorable modules on page 102](#)
2. [Restoring modules on page 103](#)
3. Start the core software services: [Starting the core software services from the command line on page 18](#) or [Starting the core software services on Windows on page 19](#)

Listing restorable modules

Use the `manage-modules.sh list restorable` command to list all modules that can be restored.

Before you begin

Make sure you have a login with root or system administrator privileges to restore modules.

Procedure

- ◆ Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh list restorable [--match="<module>"]</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd list restorable [--match="<module>"]</code>

To determine if the module has more than one version to restore, specify the `--match` option. For example:

```
/opt/APG/bin/manage-modules.sh list restorable --match="frontend"
```

When you view the output, record the order in which the modules display. You will need to use the order later when you restore the modules.

This partial Linux sample output indicates modules that can be restored.

Available Restore Points:

Identifier	Instance	Version	Date
-----	-----	-----	-----

```

* variable-handling-filter Generic-SNMP v1.8u3
11/26/13 9:00:30 AM
* property-tagging-filter Generic-SNMP v2.5u1
11/26/13 8:57:46 AM
* frontend-report-generator Default v6.2u3
11/26/13 8:38:01 AM
* collector-manager emc-smarts v5.3u2
11/26/13 8:31:29 AM
* event-processing-manager emc-smarts v1.2u3
11/26/13 8:32:29 AM

```

Restoring modules

Restore modules to their previous version.

Before you begin

- ◆ Identify all modules that can be restored by using the `manage-modules.sh list restorable` command.
- ◆ Make sure you have a login with root or system administrator privileges to restore modules.

Restore the modules in the order in which they displayed, starting from first to last. To avoid dependency issues, restore the main components or managers before their sub-components. For example, restore the Event Processing Manager before its sub-component, Event Property Tagger. Refer to the Module Manager documentation for more complete information about module rollback. This document is in the documentation directory of the installation path (for example, `/opt/APG/Doc`).

Procedure

1. Type the command for your operating system from the core software installation directory:

Operating system	Command
UNIX	<code><INSTALL_DIR>/bin/manage-modules.sh restore <module_identifier> [<module_instance>]</code>
Windows	<code><INSTALL_DIR>\bin\manage-modules.cmd restore <module_identifier> [<module_instance>]</code>

2. Answer any questions.

This Linux sample output shows that the administration-tool module has been restored to its previous version.

```

opt/APG/manage-modules.sh restore administration-tool
Starting restoration of administration-tool Default v1.0u2...
* Gathering information...
* Issuing a rollback will overwrite all existing files - except
the data ones - and replace them with their previous versions,
including configuration files.
* The module 'Administration-Tool' will now be restored in
'/opt/APG/Tools/Administration-Tool/Default'.
! WARNING: The targeted directory already exists. This will
overwrite existing files in this directory.
? Continue? [y]es, [n]o > y
* Restoring files...
Restoration complete.

```

manage-modules.sh restore command

Use the `manage-modules.sh restore` command to revert modules to their previous version after an update. Type the command for your operating system from the `bin` directory of your core software installation directory.

Description

The `manage-modules.sh restore` command enables you to revert to the previous version of core software after an update. For UNIX, specify `manage-modules.sh restore`. For Window, specify `manage-modules.cmd restore`.

To look up the identifier and module instance name, use the `manage-modules.sh list restorable` command.

Syntax

```
manage-modules.sh restore <module_identifier> [ <module_instance> ]
[ <version> ]
```

Options

module_identifier

The identifier value of the installed module.

module_instance

The unique name of the module. Omit this value if only one instance is installed since the command will use it as the default. If multiple instances exist, specify the instance you want to restore.

The identifier and instance values form a unique key to refer to the module.

version

The version number to which the module should be restored. Omit this value if only one previous version exists.

Example # 1

In this Linux example, the following command restores the Collector-Manager from 6.3.x to 6.2.x. Since only one previous version exists, the `version` option is omitted.

```
<INSTALL_DIR>/bin/manage-modules.sh update collector-manager
```

Example # 2

In this Windows example, the following command restores the variable-handling-filter from 6.3.x to 6.2.x. Since only one previous version exists, the `version` option is omitted.

```
<INSTALL_DIR>\bin\manage-modules.cmd restore variable-handling-
filter generic-snmp
```

Example # 3

In this Linux example, the following command restores the frontend-ws to version 6.2.

```
./manage-modules.sh restore frontend-ws apg-ws 6.2
./manage-modules.sh update mib-browser mymib_browser2
```

Starting the core software services from the command line

After installing core software, you must start all required services.

Before you begin

- ◆ Before starting core software services, ensure the library search path is correct on the server hosting core software. This requirement applies to the libaio package on Linux.
- ◆ Make sure you have a login with root, APG, or system administrator privileges to perform this task. The user apg is the account that the core software application uses instead of root.

Procedure

- ◆ Type the command for your operating system from the `bin` directory of the installation:

Operating system	Command
UNIX	<code>./manage-modules.sh service start all</code>
Windows	<code>manage-modules.cmd service start all</code>

Results

A list of services appears. For example:

```
* Starting 'topology-mapping-service Default'... [ OK ]
* Starting 'webservice-gateway Default'... [ OK ]
* Starting 'mysql Default'... [ OK ]
* Starting 'alerting-backend Default'... [ OK ]
* Starting 'backend Default'... [ OK ]
* Starting 'collector-manager Default'... [ OK ]
* Starting 'collector-manager Generic-SNMP'... [ OK ]
* Starting 'collector-manager Load-Balancer'... [ OK ]
* Starting 'collector-manager emc smarts'... [ OK ]
* Starting 'event-processing-manager emc smarts'... [ OK ]
* Starting 'tomcat Default'... [ OK ]
* Starting 'task-scheduler Default'... [ OK ]
```

Starting the core software services on Windows

After installing core software on Windows, you can start all required services from a Windows desktop.

Before you begin

Make sure you have logged in with system administrator credentials to manage services.

Procedure

1. From the application server's desktop, select **Start > Administrative Tools > Services**.
2. Right-click each service and click **Start**, in this order:
 - APG Topology Mapping Service
 - APG Topology Service
 - APG Webservice Gateway
 - APG MySQL
 - APG Alerting Backend
 - APG Backend

- APG Collector Manager (Generic RSC)
- APG Collector Manager (Generic-SNMP)
- APG Collector Manager (Load-Balancer)
- APG Event Processing Manager (Alert-Consolidation)
- APG Tomcat
- APG Task Scheduler