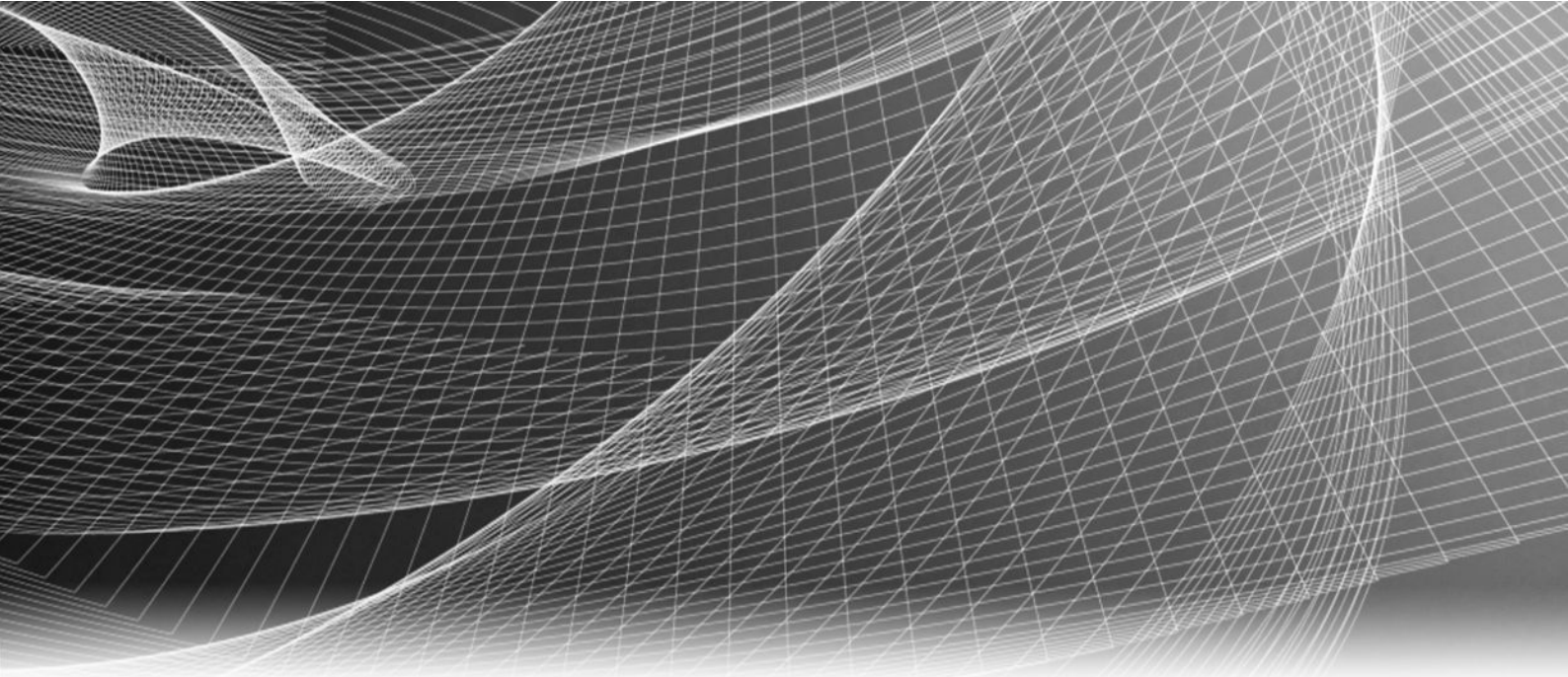




EMC[®] SolutionPack for Cisco VoIP

Version 1.0

Installation and Configuration Guide

302-000-667

01

Copyright © 2014 EMC Corporation. All rights reserved. Published in USA.

Published February, 2014

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		5
Chapter 1	SolutionPack Workflow	7
	SolutionPack for Cisco VoIP workflow.....	8
	Support.....	8
	License management.....	8
	Setting up Cisco CDRs.....	9
	Performing additional prerequisite configuration.....	9
Chapter 2	Installation	11
	Installation.....	12
	Logging in to Centralized Management.....	12
	Installing the SolutionPack.....	12
	Creating CDR database schema.....	13
	Editing Tomcat files.....	13
	Configuring the user process limits for the Linux installation.....	14
	Installing a SolutionPack Center Upgrade.....	14
	Uninstalling a SolutionPack.....	15
Chapter 3	Reports	17
	Viewing SolutionPack reports.....	18
	Reports.....	18
Appendix A	Metrics	19
	Metrics.....	20
Appendix B	Troubleshooting	35
	SSL certificates.....	36
	SSL certificate error examples.....	36
	Troubleshooting an SSL certificate error: Accepting the exception....	37
	Installing a self-signed SSL certificate from an Internet Explorer browser.....	37
	Importing an SSL certificate into your truststore.....	37
	Exporting an SSL certificate from an Internet Explorer browser.....	38
	Contacting EMC Support.....	39

TABLES

1	Metrics group 1	20
2	Metrics group 2	30

CHAPTER 1

SolutionPack Workflow

This chapter includes the following topics:

◆	SolutionPack for Cisco VoIP workflow	8
◆	Support	8
◆	License management	8
◆	Setting up Cisco CDRs	9
◆	Performing additional prerequisite configuration	9

SolutionPack for Cisco VoIP workflow

This SolutionPack reports on voice quality, availability and VoIP performance and provides status and metrics for service level measurement.

The SolutionPack enables administrators to identify and resolve issues and avoid the risk of VoIP service degradation or outages. Additionally the SolutionPack:

- ◆ Measures voice quality-establishes voice quality trends over time and helps troubleshoot VoIP calls for failures and quality deterioration.
- ◆ Helps optimize resources-identifies usage, reduces or increases capacity.
- ◆ Delivers real-time insight-views performance at a glance or in-depth.

Before beginning your installation, review these sections for pre-requisite information:

- ◆ [Device and application version support](#)
- ◆ [Configure Cisco CDRs on page 9](#)
- ◆ [Performing additional prerequisite configurations on page 9](#)
- ◆ [Manage SolutionPack licenses](#)
- ◆ [Upgrading an existing SolutionPack on page 14](#)

Support

Review the prerequisite support information before installing the SolutionPack.

This SolutionPack is supported on Watch4net version 6.3 and above. The following devices are supported:

Product	Version
Cisco Unified Communications Manager (CUCM)	6.0 and above
Cisco Universal Gateways	AS5xxx Series
Cisco Integrated Services Routers	1861 Series, 2800/2900 Series, 3800/3900/3900E Series

License management

You can evaluate features in the SolutionPack Center using 30-day temporary licenses included with Watch4net software. If you install or plan to use the SolutionPack for longer than 30 days, contact EMC Online Support for permanent license files.

If you have an existing permanent license or a temporary license that requires updating, use the license upload feature in Watch4net Centralized Management. Both permanent and temporary licenses are distributed in .zip files.

The Watch4net license name is either Watch4net SolutionPack for Cisco VoIP CUCM or ReportPack for Cisco VoIP. The system will use either license.

Setting up Cisco CDRs

Complete this procedure to configure your Cisco Call Manager device to save CDR/CMR data so that Watch4net can generate your SolutionPack reports.

Before you begin

You need administrator access to Cisco Unified Communications Manager and Cisco Unified Serviceability.

Procedure

1. Log on to your Cisco Unified Communications Manager Administration page with Administrative privileges.
2. From the drop-down menu on the top of the window, select `Cisco Unified Serviceability`, and then click `Go`.
3. On the Service Parameter page, go to **Tools > CDR Management**.
4. Click `Add new`, and provide the FTP details.

For example,

```
FTP Host/Destination (VM host IP) : 10.9.13.175
User (VM host user) : root
Password (VM host password): dangerous
Protocol : SFTP
Directory on ftp server(CUCMs will dump CDR/CMR data in
this directory): /root/w4n/cisco-voip/cdr
Resend on Failure : TRUE

For unix Directory Path would be like /root/w4n/cisco-
voip/cdr/
For windows Directory Path would be like /
cygdrive/c/w4n/cisco-voip/cdr/
(Note: CUCM does not understand C:\ so you need to
provide cygwin path for windows.)
```

5. Make sure you activate the service for Cisco CDR located at **Tools > Control Centre Network Services**.

Performing additional prerequisite configuration

Before installing your SolutionPack perform these additional tasks on your Cisco call managers and gateways that require polling.

Procedure

1. Enable SNMP on all call managers and gateways that require polling.

2. **Note**

Refer to the following Cisco website for information on this step as well as step 3:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/devguide/9_1_1/axl.html#wp1054628

Enable AXL for the call managers that require polling.

3. Obtain the CUCM DB schema version to be used with AXL requests.
4. Enable CDRs to send data to the billing server which can be the same server as Watch4net.

Make sure the user 'apg' has the correct CDR permissions so that it can access the CDR repository on the billing server.

CHAPTER 2

Installation

This chapter includes the following topics:

◆	Installation	12
◆	Logging in to Centralized Management	12
◆	Installing the SolutionPack	12
◆	Creating CDR database schema	13
◆	Editing Tomcat files	13
◆	Configuring the user process limits for the Linux installation	14
◆	Installing a SolutionPack Center Upgrade	14
◆	Uninstalling a SolutionPack	15

Installation

Review this information before beginning the installation.

- ◆ Make sure you review and perform the prerequisites outlined in the first chapter.
- ◆ Perform the installation with administrative privileges on the Watch4net User Interface.

Logging in to Centralized Management

Log in to Centralized Management to perform operations that 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.

Installing the SolutionPack

After you log in as an administrator, you can install this 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). The recommended module update order varies. Refer to the *EMC Watch4net Installation and Configuration Guide* for information on module update order for multiple hosts or single host deployments.

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 Cisco VoIP SolutionPack on 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 **Collector**, and **Reports** 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, verify the SolutionPack version number along with SolutionPackBlock information. Select **Centralized Management** > **SolutionPacks** > **Cisco VoIP**.

Creating CDR database schema

After installation you must manually create the schema for the CDR database.

Procedure

1. Verify that datastore service started. If not start it: `<APG>/bin/manage-modules.sh service status datastore Default`.
2. Copy the content of `voip-setup-db.ddl` under `[APG]/Event-processing/APG-Datastore-Writer/[instance_name]/ddl`.
3. Execute the script `datastore-client.sh` or (cmd for Windows) under `[APG]/bin/` and paste the content of the `ddl` file at the prompt line.
4. Restart the event-processing-manager.

Editing Tomcat files

After editing the schema for the CDR database, edit these Tomcat files and configure the connection to the CDR database.

Procedure

1. Edit following tomcat file: `[APG]/Web-Servers/Tomcat/[instance_name]/conf/server.xml`. Add the following definition to the section where the connections to the DBs are defined. Add it above the following line `Defines the connection to the Events Archive database for APG Datastore`.

```
<Resource name="jdbc/FLOW-TF-VOIP" auth="Container"
type="javax.sql.DataSource" maxActive="10"
                                maxIdle="10"
validationQuery="SELECT 1" testOnBorrow="false"
testWhileIdle="true"

timeBetweenEvictionRunsMillis="10000"
minEvictableIdleTimeMillis="60000" maxWait="10000"
                                username="admin"
```

```
password="changeme"
driverClassName="com.watch4net.x100.jdbc.Driver"
                                removeAbandoned="true"
removeAbandonedTimeout="60" logAbandoned="true"
                                url="jdbc:x100://localhost:48443/
Databases/APG-Datastore" />
```

2. Edit [APG]/Web-Servers/Tomcat/[instance_name]/conf/Catalina/localhost/APG.xml. Add the following definition to the section where the connections to the DBs are defined. Add the definition above the `<!-- emc prosphere -->` line: `<ResourceLink name="jdbc/FLOW-TF-VOIP: { mapping=FLOW-CISCO-CDR.xml, table= CISCO_VOIP_CUCM_CDR}" global="jdbc/FLOW-TF-VOIP" type="javax.sql.DataSource" />`
3. Restart the Tomcat service.

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'
```

Installing a SolutionPack Center Upgrade

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. 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.

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 3

Reports

This chapter includes the following topics:

- ◆ [Viewing SolutionPack reports](#)..... 18
- ◆ [Reports](#)..... 18

Viewing SolutionPack reports

You can view your reports from the Watch4net console.

Before you begin

After installing the SolutionPack, access the Watch4net User Interface.

Procedure

1. Point your web browser to `http://[serverIP:port]/APG`.
An example default URL is `http://localhost:58080/APG`.
2. On the login screen, enter your Watch4net username and password, and click **Sign In**.
3. View SolutionPack reports by expanding **Report Library** > *Your SolutionPack Name*.

Reports

This reports table includes the "out-of-the box" reports available with this SolutionPack.

You can drill-down on some top-level reports to view sub-level reports with specific metrics related to the objects in the top-level report.

Report	Description
Devices Health - All Devices	Includes health information for all gateways and call manager devices per cluster - drill down on a device for metrics such as CPU usage, average used memory, availability, interface usage and statistics.
UC Environment Inventory	Lists all call managers per cluster as well as their availability.
Call Overview	Displays important information per cluster including: • Call overviews • Disconnected calls and their root cause • Calls Quality (Qos and MoS) • Calls statistics and more.
CUCM Reports	Call Manager reports include reports per cluster on licensing, services, cluster health, phones, route pattern, trunks and media resources. Drill down on any device for more metrics and reports.
Gateway Reports	Gateway reports per cluster on gateway trunk utilization, trunk statistics, trunks availability and more.

APPENDIX A

Metrics

- ◆ [Metrics](#).....20

Metrics

Report metrics are used to create SolutionPack reports. Metrics are used to gather information for monitoring or reporting on your Cisco devices.

Table 1 Metrics group 1

Source	Properties	Name
VOIP-CISCO-XML-CCSERVICES	part =>ServiceName	Status =>ServiceStatus (%)
	partdesc =>ReasonCodeString	
	datagrps=ControlCenterServices (hard Coded)	
	devtype=CallManager(hard Coded)	
	entity=ControlCenter(hard Coded)	
	parttype=ControlCenter(hard Coded)	
	type=Services(hard Coded)	
	ip (taken from context file)	
VOIP-CISCO-XML-CCSERVICES	part => ServiceName	Service UpTime=>UpTime(s)
	partdesc =>ReasonCodeString	
	datagrps=ControlCenterServices (hard Coded)	
	devtype=CallManager(hard Coded)	
	entity=ControlCenter(hard Coded)	
	parttype=ControlCenter(hard Coded)	
	type=Services(hard Coded)	
	ip (taken from context file)	
VOIP-CISCO-XML-PERFMON-RT	datagrps=Cisco MGCP Gateways-RT(hard Coded)	Channel Status=>BRChannelsActive(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	part=>Name	
	type=BRI(hard Coded)	
	entity=PSTN Trunk(hard Coded)	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
VOIP-CISCO-XML-PERFMON-RT	datagrp=Cisco MGCP Gateways-RT(hard Coded)	Channel Status=>FXOPortsActive(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	part=>Name	
	type=FXO(hard Coded)	
	entity=Gateway(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagrp=Cisco MGCP Gateways-RT(hard Coded)	Channel Status=>FXSPortsActive(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	part=>Name	
	type=FXS(hard Coded)	
	entity=Gateway(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagrp=Cisco MGCP Gateways-RT(hard Coded)	Channel Status=>PRChannelsActive(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	part=>Name	
	type=PRI(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagrp=Cisco MGCP Gateways-RT(hard Coded)	Channel Status=>T1ChannelsActive(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
	part=>Name	
	type=T1CAS(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagr=Cisco CTIManager-RT(hard Coded)	CTI Active Connections=>CTIConnectionActive(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=CTI Device(hard Coded)	
	part=>Name	
	entity=CallManager(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagr=Cisco Lines-RT(hard Coded)	ActiveLines=>Value(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=Lines(hard Coded)	
	part=>Name	
	entity=CallManager(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagr=Cisco H323-RT(hard Coded)	Calls Active=>CallsActive(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=H323Device(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON-RT	datagr=Cisco H323-RT(hard Coded)	Video Calls Active=>VideoCallsActive(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=H323Device(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON-RT	datagr=Cisco SIP-RT(hard Coded)	Calls Active=>CallsActive(Nb)
	devtype=CallManager(hard Coded)	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
	ip (taken from context file)	
	parttype=SIPDevice(hard Coded)	
	part=>Name	
	type=SIP Trunk(hard Coded)	
	entity=IP Trunk(hard Coded)	
VOIP-CISCO-XML-PERFMON-RT	datagr=Cisco SIP-RT(hard Coded)	Video Calls Active=>VideoCallsActive(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=SIPDevice(hard Coded)	
	part=>Name	
	type=SIP Trunk(hard Coded)	
	entity=IP Trunk(hard Coded)	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP BRI Device(hard Coded)	Calls Attempted=>OutboundBusyAttempts(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=BRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP BRI Device(hard Coded)	Calls Completed=>CallsCompleted(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=BRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP BRI Device(hard Coded)	Signaling Status=>DatalinkInService(%)

Table 1 Metrics group 1 (continued)

Source	Properties	Name
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=BRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP FXO Device(hard Coded)	Calls Attempted=>OutboundBusyAttempts(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=Gateway(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=FXO(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP FXO Device(hard Coded)	Calls Completed=>CallsCompleted(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=Gateway(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=FXO(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP FXO Device(hard Coded)	Port Status=>PortStatus(%)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=Gateway(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=FXO(hard Coded)	
	part=>Name	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP FXS Device(hard Coded)	Calls Attempted=>OutboundBusyAttempts(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=Gateway(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=FXS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP FXS Device(hard Coded)	Calls Completed=>CallsCompleted(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=Gateway(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=FXS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP FXS Device(hard Coded)	Port Status=>PortStatus(%)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=Gateway(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=FXS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP PRI Device(hard Coded)	Calls Attempted=>OutboundBusyAttempts(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
	parttype=MGCPDevice(hard Coded)	
	type=PRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP PRI Device(hard Coded)	Calls Completed=>CallsCompleted(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=PRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP PRI Device(hard Coded)	Signaling Status=>DatalinkInService(%)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=PRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP T1 CAS Device(hard Coded)	Calls Attempted=>OutboundBusyAttempts(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=T1CAS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP T1 CAS Device(hard Coded)	Calls Completed=>CallsCompleted(Nb)

Table 1 Metrics group 1 (continued)

Source	Properties	Name
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	entity=PSTN Trunk(hard Coded)	
	parttype=MGCPDevice(hard Coded)	
	type=T1CAS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco H323(hard Coded)	Calls Attempted=>CallsAttempted(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=H323Device(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco H323(hard Coded)	Calls Completed=>CallsCompleted(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=H323Device(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco H323(hard Coded)	Video Calls Completed=>VideoCallsCompleted(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=H323Device(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco SIP(hard Coded)	Calls Attempted=>CallsAttempted(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=SIPDevice(hard Coded)	
	entity=IP Trunk(hard Coded)	
	part=>Name	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
VOIP-CISCO-XML-PERFMON	datagr=Cisco SIP(hard Coded)	Calls Completed=>CallsCompleted(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=SIPDevice(hard Coded)	
	entity=IP Trunk(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco SIP(hard Coded)	Video Calls Completed=>VideoCallsCompleted(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	parttype=SIPDevice(hard Coded)	
	entity=IP Trunk(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP Gateways(hard Coded)	Channels Count=>BRISpansInService(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
	type=BRI(hard Coded)	
VOIP-CISCO-XML-PERFMON	datagr=Cisco MGCP Gateways(hard Coded)	Channels Count=>FXOPortsInService(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
	type=FXO(hard Coded)	
	part=>Name	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
VOIP-CISCO-XML-PERFMON	datagrp=Cisco MGCP Gateways(hard Coded)	Channels Count=>FXSPortsInService(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
	type=FXS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagrp=Cisco MGCP Gateways(hard Coded)	Channels Count=>PRIspansInService(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
	type=PRI(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagrp=Cisco MGCP Gateways(hard Coded)	Channels Count=>T1SpansInService(Nb)
	devtype=Gateway MGCP(hard Coded)	
	ip (taken from context file)	
	parttype=MGCPDevice(hard Coded)	
	entity=PSTN Trunk(hard Coded)	
	type=T1CAS(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagrp=Cisco CallManager(hard Coded)	HeartBeat=>CallManagerHeartBeat(Nb)
	devtype=Call Manager(hard Coded)	
	ip (taken from context file)	
	entity=CallManager(hard Coded)	

Table 1 Metrics group 1 (continued)

Source	Properties	Name
	parttype=CallManager(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco CallManager System Performance(hard Coded)	Expected Delay=>AverageExpectedDelay(ms)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	entity=CallManager(hard Coded)	
	parttype=CallManager(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco CallManager System Performance(hard Coded)	Calls Rejected Due To ICT Throttling=>CallsRejectedDueToThrottling(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	entity=CallManager(hard Coded)	
	parttype=CallManager(hard Coded)	
	part=>Name	
VOIP-CISCO-XML-PERFMON	datagr=Cisco CallManager System Performance(hard Coded)	Calls Rejected Due To Generic Throttling=>CallThrottlingGenericCounter 3(Nb)
	devtype=CallManager(hard Coded)	
	ip (taken from context file)	
	entity=CallManager(hard Coded)	
	parttype=CallManager(hard Coded)	
	part=>Name	

Table 2 Metrics group 2

Metric name	Unit	Description
ActivePhones	Number (Nb)	Number of phones connected to, and actively in communication with, (via keep-alives), the Call Manager.
InActivePhones	Nb	Number of phones registered with, but has lost contact with the Call Manager. Phones lose contact with the Call Manager if the Call Manager does not receive any keep-alives.

Table 2 Metrics group 2 (continued)

Metric name	Unit	Description
ActiveGateways	Nb	Number of gateways configured with the Call Manager and actively in communication (via keep-alives) with the Call Manager.
InActiveGateways		Number of gateways that are registered with the Call Manager but have lost contact with the Call Manager. The gateways are said to have lost contact with the Call Manager if the Call Manager does not receive any keep-alives.
RegisteredPhones	Nb	Number of phones that are registered and actively in communication with the local Call Manager.
UnregisteredPhones	Nb	Number of phones that are unregistered or have lost contact with the local Call Manager.
RejectedPhones	Nb	Number of phones whose registration requests were rejected by the local Call Manager.
RegisteredMediaDevices	Nb	Number of media devices that are registered and actively in communication with the local Call Manager.
UnregisteredMediaDevices	Nb	Number of media devices that are unregistered or have lost contact with the local Call Manager.
RejectedMediaDevices	Nb	Number of media devices whose registration requests were rejected by the local Call Manager.
RegisteredCTIDevices	Nb	Number of CTI devices that are registered and actively in communication with the local Call Manager.
UnregisteredCTIDevices	Nb	Number of CTI devices that are unregistered or lost contact with the local Call Manager.
RejectedCTIDevices	Nb	Number of CTI devices with registration requests rejected by the local Call Manager.
RegisteredVoiceMailDevices	Nb	Number of voice messaging devices that are registered and actively communicating with the local Call Manager.
UnregisteredVoiceMailDevices	Nb	Number of voice messaging devices that are unregistered or lost contact with the local Call Manager.
RejectedVoiceMailDevices	Nb	Number of voice messaging devices with registration requests rejected by the local Call Manager.
PartiallyRegisteredPhones	Nb	Number of phones that are partially registered with the local Call Manager.
Status (CallManager)		Current status of the Call Manager. A Call Manager is Up if the SNMP Agent received a system Up event from the local CCM - status values include: 1. · Unknown: Current status of the Call Manager is Unknown

Table 2 Metrics group 2 (continued)

Metric name	Unit	Description
		1. · Up: Call Manager is running and able to communicate with other Call Managers 1. · Down: Call Manager is down or the Agent is unable to communicate with the local Call Manager.
Availability (Phone)	%	Availability of the phone. The availability of the phone changes from Unknown to Registered when the phone registers with the local CCM.
Availability (Line Extension)	%	Represents the % availability of the phone line.
Availability (Gateway)	%	Status of the gateway. The Gateway status changes from Unknown to Registered when the Gateway registers with the local CCM.
Status (Gateway)	%	D-Channel status of the gateway. Status values include: active(1): The D-Channel is up inActive(1): The D-Channel is down unknown(3): The D-Channel status is unknown notApplicable(4): The D-channel status is not applicable for this gateway.
Availability (Trunk Gateway)	%	The state of the trunk. The trunk status changes from Unknown to Up when it registers with the local CCM. Status values include: Unknown: state of trunk is unknown up: Up and running. Idle with no calls. busy: Trunk in busy state down: Trunk down
Availability (Media Device)	%	Status of the Media Device. The status changes from unknown to registered after registration with the local CCM.
Availability (CTI Device)	%	The status of the CTI Device. CTI Device status changes from unknown to registered after registration with local CCM.
Availability (Voice Mail)	%	The table containing a list of all voice messaging devices that attempted registration with the local Call Manager (minimum of one attempt).
Availability (H323)	%	The H323 device registration status with the gatekeeper. The status changes from unknown to registered when the H323 device successfully registers with the gatekeeper. Status values include: notApplicable: The registration status is not applicable for this H323 device. unknown: The registration status of the H323 device with the gatekeeper is unknown. registered: H323 device successfully registered with gatekeeper. unregistered: H323 device no longer registered with gatekeeper rejected: Registration request from H323 device rejected by gatekeeper.
CardState	%	DSP subsystem might reset DSP card to recover from fatal error condition. After the DSP card resets

Table 2 Metrics group 2 (continued)

Metric name	Unit	Description
		successfully, the object cdspCardResourceUtilization and cdspCardLastHiWaterUtilization reset to 0. If the fatal error persists in this object after card is reset, card should be replaced. - offLine - DSP card is in off-line maintenance state.
ResourceUtilization	%	Indicates the percentage of current DSP resource utilization of the card. Utilization is a ratio of number of busy DSP resources (for handling calls, transcoding, voice compression, and so on) to the total available DSP resources.
Availability (DSP Module)	%	The current operational state of the DSP. Values include: normal: DSP operates normally. shutdown: DSP shut down due to fatal error. congested: DSP does not accept call because the DSP buffer is full. failed: DSP failed.
TotalChannels (DSP Module)	Nb	Total number of channels in the DSP. Value is predetermined by the DSP functionality upon initialization. Value of 0 indicates Channelized DSP mode is turned off.
ActiveChannels (DSP Module)	Nb	Number of channels that are used by active calls to process media stream. The value is incremented after the reserved DSP channel enters call connection state and is decremented after the call disconnects.
isdnOperStatus	%	The current call control state for the port. Values include: idle(1): B channel is idle. No current call or call attempt. connecting(2): Current connection attempt (outgoing call). connected(3): Incoming call being validated. active(4): Call active on the interface.
isdnSignalingStatus	%	Object used to create and delete rows in the isdnSignalingTable.
VOIPSuccessCalls	Nb	Number of completed calls to this peer.
VOIPFailCalls	Nb	Number of failed call attempts to this peer since system startup.
VOIPAcceptCalls	Nb	Number of calls from this peer accepted since system startup.
VOIPRefuseCalls	Nb	Number of calls from this peer refused since system startup.

APPENDIX B

Troubleshooting

- ◆ [SSL certificates](#) 36
- ◆ [Contacting EMC Support](#).....39

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 36](#) provides a list of sample errors.

Temporary resolution

Accept the certificate exception temporarily: [Troubleshooting an SSL certificate error: Accepting the exception on page 37](#).

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 37
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 38 2. Importing an SSL certificate into your truststore on page 37
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 37

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 38](#).

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 37](#)
 - [Importing an SSL certificate in Firefox on page 38](#)
 - [Importing an SSL certificate in Internet Explorer on page 38](#)

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.

Contacting EMC Support

EMC support, product, and licensing information can be obtained through EMC online support.

Procedure

- ◆ For documentation, videos, release notes, software updates, or information about EMC products, go to EMC Online Support at <https://support.emc.com>.
- ◆ For technical support, go to EMC Online Support and click **Service Center**.
You must have a valid support agreement to open a service request.
- ◆ Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

