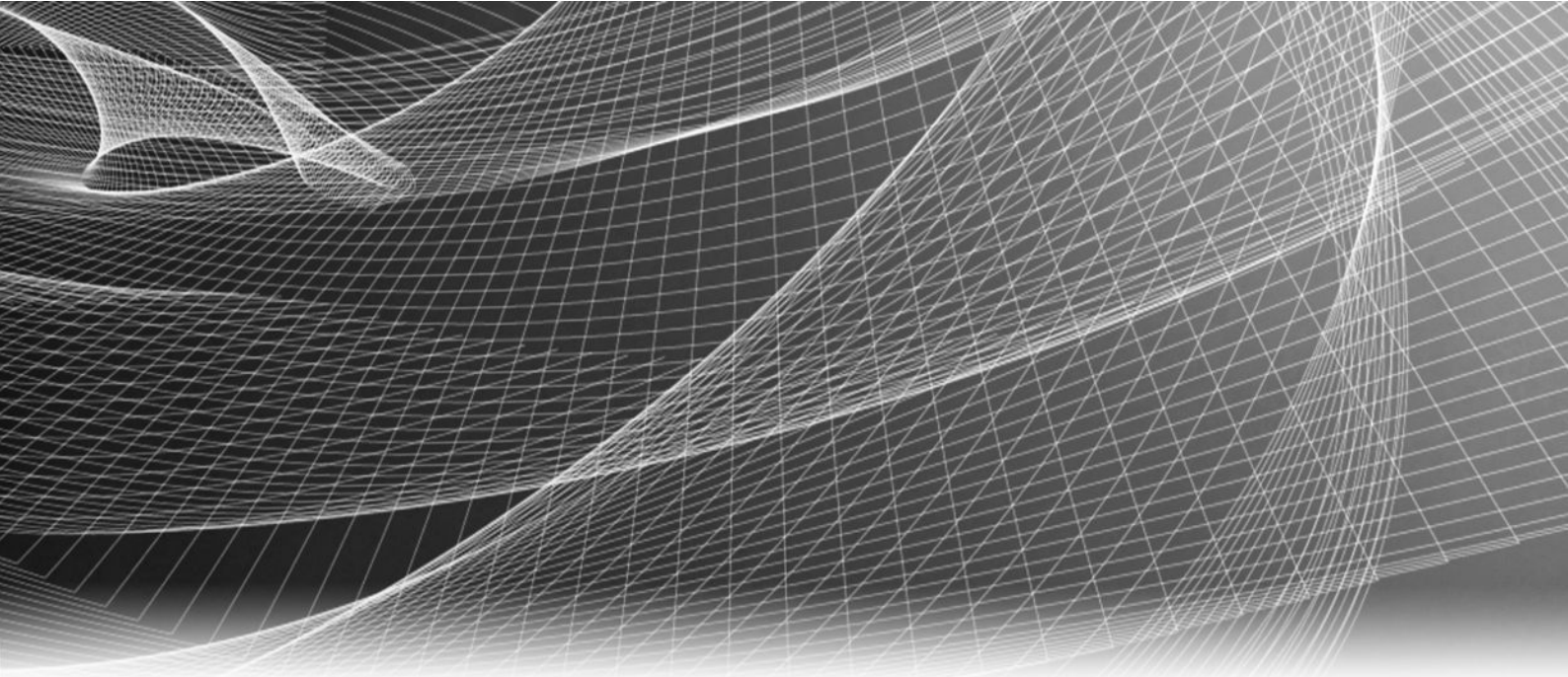




EMC[®] SolutionPack for Avaya Aura

Version 1.0

Installation and Configuration Guide

302-000-331

REV 02

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 for Avaya VoIP	7
	Workflow	8
	Support	8
	Set up Avaya CDR and RTCP.....	9
	Enabling Call Detail Records (CDR).....	9
	Adding node names for CDR monitoring.....	9
	Adding IP CDR Service for CDR Monitoring.....	10
	Setting CDR System Parameters for CDR Monitoring.....	11
	Enabling Intra-switch CDRs.....	12
	Enabling trunk groups for CDR monitoring.....	12
	CDR monitoring for 10 Digit Plus dial plans.....	13
	Configuring RTCP Monitoring.....	15
	License management.....	17
Chapter 2	Installation and Configuration	19
	Installation.....	20
	Logging in to Centralized Management.....	20
	Installing the SolutionPack.....	20
	Starting the CDR and RTCP Listeners.....	22
	Log files.....	23
	Configuring the user process limits for the Linux installation.....	23
	Installing a SolutionPack Center Upgrade.....	24
	Uninstalling a SolutionPack.....	25
Chapter 3	Reports	27
	Viewing SolutionPack reports.....	28
	Avaya Reports.....	28
Appendix A	Metrics	31
	Metrics for Avaya VoIP.....	32
Appendix B	Troubleshooting	37
	SSL certificates.....	38
	SSL certificate error examples.....	38
	Troubleshooting an SSL certificate error: Accepting the exception....	39
	Installing a self-signed SSL certificate from an Internet Explorer browser.....	39
	Importing an SSL certificate into your truststore	39
	Exporting an SSL certificate from an Internet Explorer browser.....	40
	Contacting EMC Support.....	41

TABLES

1	Report metrics.....	32
---	---------------------	----

CHAPTER 1

SolutionPack for Avaya VoIP

This chapter includes the following topics:

◆	Workflow	8
◆	Support	8
◆	Set up Avaya CDR and RTCP	9
◆	License management	17

Workflow

The SolutionPack for Avaya Aura reports on health statistics for the Avaya Aura Communication Manager call servers. Metrics are Collected via SNMP for host statistics, and call services.

In additon this SolutionPack:

- ◆ Reports on health statistics for the Avaya Aura Communication Manager call servers. Metrics are Collected via SNMP for host statistics, and call services.
- ◆ Provides inventory views for Network Regions, and phone end points, as well as registration status. This information is collected via SSH/SAT connections to the ACM <Perl>.
- ◆ Provides reports for MOS per phone call. This is collected via CDR (Call Detail Records). You must configure ACM CDR destination to W4N Text Collector, and RTCP (Real Time Communication Protocol) (Perl- based listener, IIRC).

Use these guidelines to prepare your environment for installation of the SolutionPack for Avaya VoIP.

- ◆ Verify that prerequisite software is installed in your environment. [Support information on page 8](#)
- ◆ Check that your Watch4net network configuration has the minimum requirements to run reports.
- ◆ [Set up your Avaya Aura environment on page 9.](#)
 - [Enable Call Detail Records \(CDR\) on page 9](#)
 - [Configure RTCP monitoring on page 15](#)

After setting up your environment:

- ◆ [Manage SolutionPack licenses on page 17.](#)
- ◆ [Install the SolutionPack for Avaya VoIP on page 20](#) (first-time installations), or
- ◆ [Update a SolutionPack from the SolutionPack Center](#) to uprade an existing version of the SolutionPack.

Support

Before installing this SolutionPack, review version support information.

Verify that prerequisite software is installed in your environment.

Software	Version
Watch4net	6.3 or higher installed on Red Hat LINUX or Windows
Perl (Linux)	5.8.8 or higher
Strawberry Perl (Windows)	5.18.2
Net-SSH (Linux only)	Net-SSH2-0.48

Set up Avaya CDR and RTCP

Before installing your SolutionPack you must configure your Avaya Aura environment to work with Watch4net.

Avaya Aura CDR and RTCP monitoring must be configured so that Watch4net can communicate with your environment and generate Avaya Aura SolutionPackreports.

Enabling Call Detail Records (CDR)

In order for the SolutionPack for Avaya Aura to provide a full range of call metrics, you must configure the Avaya PBX so that Call Detail Records (CDRs) are sent to the IP address of the Watch4net Server.

Follow the steps in the following sections to configure CDR for Avaya Aura.

Procedure

1. [Add node names. on page 9](#)
2. [Add an IP CDR service. on page 10](#)
3. [Set CDR system parameters. on page 11](#)
4. [Enable intra-switch CDRs. on page 12](#)
5. [Enable trunk groups. on page 12](#)
6. [Configure 10-Digit Plus dial plans. on page 13.](#)

After you finish

For additional details on performing any of these procedures, refer to *Configure CDR Monitoring*, Avaya document 100059519, available on the Avaya website: <http://www.avaya.com>.

Adding node names for CDR monitoring

With this procedure, you can configure the AVAYA device to send data to the Watch4net instance where the SolutionPack is installed.

Follow these steps to add a new node for CDR monitoring. Make sure you have login credentials with proper administrative rights to make this configuration.

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
 - a. Type: `ssh <username>@<ACM FQDN>` and then press **Enter**.
 - b. Enter password.
 - c. Enter terminal type: `vt100`.
 - d. At the prompt, enter `sat`.
 - e. Enter terminal type: `w2ktt`.
2. Execute this command: `change node-names ip`.

```
change node-names ip
1 of 2
```

Page

		IP NODE NAMES	
Name	IP Address	Name	IP
Address			

```

clan1          10.1.10.21
clan2          10.1.10.22
default        0.0.0.0
medpro1        10.1.10.31
medpro2        10.1.10.32
procr          10.1.10.9
vall           10.1.10.41
prognosis      10.1.10.105

```

3. Complete the following fields: **Name**: Add a name, then **IP Address**: Add the IP address of the host where Watch4net is running.

4. Press **Esc + e** to save and exit.

NAT Environment: In the case of a NAT environment the IP Address should be set to the Public IP address assigned to the IP Telephony Manager Monitoring server.

Note

If the PBX has an S85xx or S87xx series Media Server, then ensure that a valid node name for the CLAN board exists as well. If it has an S8300 series Media Server, then ensure that a valid node name for the PROCR also exists.

Adding IP CDR Service for CDR Monitoring

Use this procedure to define the CDR link.

Procedure

1. Execute the command: **change ip-services**.

```

change ip-services
Page 1 of 4

```

		IP SERVICES			
Service	Enabled	Local	Local	Remote	
Remote					
Type		Node	Port	Node	Port
CDR1		clan1	0	prognosis	
50000					

2. To define a primary CDR link, enter the following details:

- **Service Type:** CDR1 - If CDR1 already exists, add a new destination by defining the Service Type to CDR2 (or as appropriate).
- **Local Node:** clan1 - Add the node name for the CLAN (S85xx or S87xx series) or PROCR (S8300 series).

Note

Execute `list node-names ip all` command to view the node name that refers to the ACM IP Address.

- **Local Port:** 0 - The Local Port is fixed to 0 as Avaya Communication Manager initiates the CDR link.
- **Remote Node:** - This is the name you specified in `change node-names ip` step 3 in the previous section (Adding node names for CDR monitoring).
- **Remote Port:** - Set port to 5001. This is the port where the SolutionPack listens for the CDR data. With multiple Avaya hosts, all send data to the same port on the SP host.

3. Disable the Reliable Session Protocol (RSP) from the CDR link by setting the **Reliable Protocol** field to *n*.

4. Use **Esc n** to get to the **SESSION LAYER TIMERS** page. Set the value for the CDR you used in the previous screen for the Reliable Protocol to **n**. For example:

SESSION LAYER TIMERS				
Service Connectivity Cntr	Reliable Type Timer	Packet Resp Protocol	Session Connect Timer	SPDU Message Cntr
CDR1	n	30	3	3
60				

5. Press **Esc + e** to save and exit.

Setting CDR System Parameters for CDR Monitoring

The CDR SYSTEM PARAMETERS form of the Avaya SAT program should be set up with the required parameters for the type of calls to track and format the CDR data.

Procedure

1. Execute the command: **change system-parameters cdr**

```
change system-parameters cdr
Page 1 of 1
```

CDR SYSTEM PARAMETERS	
Node Number: (Local PBX ID)	CDR Date Format:
month/day	
Primary Output Format: unformatted	Primary Output Endpoint:
CDR1	
Secondary Output Format:	Secondary Output Endpoint:
Use ISDN Layouts? n	Enable CDR Storage
on Disk? n	
Use Enhanced Formats? n	Condition Code 'T' For
Redirected Calls: n	
Use Legacy CDR Formats? y	Remove # From Called
Number? n	
Modified Circuit ID Display? n	Intra-
switch CDR? y	
Record Outgoing Calls Only? n	Outg Trk Call
Splitting? y	
Suppress CDR for ineffective Call Attempts? y	Outg Attd Call
Record? y	
Disconnect Information in Place of FRL? n	Interworking
Feat-flag? n	
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n	
	Calls to Hunt Group - Record:
member-ext	
Record Called Vector Directory Number Instead of Group or Member? n	
Record Agent ID on Incoming? n	Record Agent ID on Outgoing? y
Inc Trk Call Splitting? n	
Record Non-Call Assoc TSC? n	Call Record Handling
Option: warning	
Record Call-Assoc TSC? n	Digits to Record for Outgoing
Calls: dialed	
Privacy - Digits to Hide: 0	CDR Account Code
Length: 15	

2. Edit the information. The following settings are recommended:

- CDR Date Format: month/day
- Primary Output Format: unformatted
- Primary Output Endpoint: CDR1

The following parameters define the type of calls that will be recorded and what data will be included in the record.

- ◆ **Use Legacy CDR Formats? y** Specifies the use of the Avaya Communication Manager 3.x (legacy) formats in the CDR records produced by the system.

- ◆ **Intra-switch CDR: y** If CDRs are required for intra-PBX calls, then the `Intra-switch CDR?` option must be set to `y`. This setting allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form.
- ◆ **Record Outgoing Calls Only? n** Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
- ◆ **Outg Trk Call Splitting? y** Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.
- ◆ **Inc Trk Call Splitting? n** Disallows a separate call record for any portion of an incoming call that is transferred or conferenced.

This is the recommended PBX setting, although setting `n` to all options is also possible. By using these recommended settings CDRs will be sent for most types of calls (conference calls, transfers, attendant) and intra-switch. Unless there is a requirement for any other particular option, the default should be `n`.

Enabling Intra-switch CDRs

CDRs are usually only sent when calls are made through a trunk. In the case of an Intra-switch call (for example, a call that goes to another phone directly connected to the PBX), a CDR will not be sent unless Intra-switch CDR has been enabled. Intra-switch CDRs are only available if enabled for specific extensions.

Before you begin

If the Intra-switch CDR field is set to `y` on Page 1 of the CDR SYSTEM PARAMETERS form, then the INTRA-SWITCH CDR form also needs to be updated to define the extensions that will be subjected to call detail recording.

Procedure

1. Execute the command: `change intra-switch-cdr.`

```
change intra-switch-cdr
```

```
Page 1 of 3
```

```
INTRA-SWITCH CDR
```

```
Assigned Members: 6 of 4000
```

```
administered
```

```
Extension
```

```
Extension
```

```
Extension
```

```
Extension
```

```
3001
```

```
3002
```

```
3003
```

```
3004
```

```
3005
```

```
3006
```

2. In the `Assigned Members` field, enter the individual extensions for usage tracking with the CDR records.

Enabling trunk groups for CDR monitoring

Enabling trunk groups is not required for configuring the SolutionPack, however if you do not configure them you will not get trunk group-related traffic statistics.

For each trunk group where CDR records are required, verify that CDR reporting is enabled.

Procedure

1. Execute the command: `change trunk-group <n>` (where <n> is the trunk group number).

```
change trunk-group 1
Page 1 of 21

Group Number: 1                      TRUNK GROUP
Reports: y                          Group Type: isdn                      CDR
  Group Name: Bondi H.323              COR: 1      TN: 1
TAC: 501
  Direction: two-way      Outgoing Display? y      Carrier
Medium: H.323
  Dial Access? n          Busy Threshold: 255      Night Service:
Queue Length: 0
Service Type: tie         Auth Code? n            TestCall ITC:
rest
                                Far End Test Line No:
TestCall BCC: 4
```

2. Make sure that the CDR Reports field is set to `y`.
3. Repeat for all trunk groups to be reported.

CDR monitoring for 10 Digit Plus dial plans

You can optionally configure 10 Digit Plus dial plans for CDR.

Options include:

- ◆ Configure the Avaya PBX Custom Fields. Use this procedure when no other customized CDR system parameters have been specified for any other purposes on the Avaya PBX
- ◆ Including with other customized formats. Use this procedure if existing customized CDR system parameters are already configured on the Avaya PBX for the Billing Server or other CDR applications.

Configuring Avaya PBX custom fields

There are two options when configuring 10 Digit Plus dial plans for CDR.

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
 - a. Type: `ssh <username>@<ACM FQDN>` and then press **Enter**.
 - b. At the prompt, type: `sat` and then press **Enter**.
 - c. Select terminal type, and press **Enter** to generate a command prompt.
2. Execute the command: `change system-parameters cdr`
3. Set the Output Format to **customized**. For example:

```
change system-parameters cdr
Page 1 of 1

                                CDR SYSTEM PARAMETERS
Node Number: (Local PBX ID)      CDR Date Format:
month/day
  Primary Output Format: customized      Primary Output Endpoint:
CDR1
Secondary Output Format:          Secondary Output Endpoint:
  Use ISDN Layouts? n            Enable CDR Storage
on Disk? n
  Use Enhanced Formats? n      Condition Code 'T' For
```

Redirected Calls: n
...

4. Go to page 2 of the CDR System Parameters form (Esc - n) and specify the customized CDR parameters as shown in the following code.

Data Item - Length		CDR SYSTEM PARAMETERS		Data Item
- Length		Data Item - Length		
1: time	- 4	17: ins	- 3	
33: duration	- 4	18: ixc-code	- 4	
34: cond-code	- 1	19: bcc	- 1	
35: code-dial	- 4	20: ma-uui	- 1	
36: code-used	- 4	21: res_flag	- 1	
37: dialed-num	- 15	22: tsc_flag	- 1	
38: calling-num	- 15	23: null	- 1	
39: acct-code	- 15	24:	-	
40: auth-code	- 13	25:	-	
41: frl	- 1	26:	-	
42: in-crt-id	- 3	27:	-	
43: out-crt-id	- 3	28:	-	
44: feat-flag	- 1	29:	-	
45: attd-console	- 2	30:	-	
46: in-trk-code	- 4	31:	-	
47: node-num	- 2	32:	-	
48:	-			

Record length = 103

Configuring other customized formats

Follow the procedure to configure the Avaya PBX and for other customized formats .

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
 - a. Type: **ssh <username>@<ACM FQDN>** and then press **Enter**.
 - b. At the prompt, type: **sat** and then press **Enter**.
 - c. Select terminal type, and press **Enter** to generate a command prompt.
2. Execute the command: **change system-parameters cdr**
3. Set the Output Format related to IP Telephony Manager to **customized**. For example:

```
change system-parameters cdr
Page 1 of 1
```

CDR SYSTEM PARAMETERS	
Node Number: (Local PBX ID)	CDR Date Format:
month/day	
Primary Output Format: customized	Primary Output Endpoint:
CDR1	
Secondary Output Format:	Secondary Output Endpoint:
Use ISDN Layouts? n	Enable CDR Storage

```

on Disk? n
      Use Enhanced Formats? n      Condition Code 'T' For
Redirected Calls: n
...

```

Go to page 2 of the form (Esc - n) and specify at least the following parameters:

- time (4)
- duration (4) or sec-dur (4)
- cond-code (1)
- code-used (4)
- dialed-num (15)
- calling-num (15), plus in-trk-code (4), or calling-num (15), plus in-trk-code (4), plus in-crt-id (3)

These minimum parameters are required and must be added to the custom settings page along with the minimum field lengths as specified. You can also include additional parameters as shown in [Standard Custom Format on page 13](#).

Configuring RTCP Monitoring

In order for the SolutionPack for Avaya Aura to receive RTCP data necessary to create SolutionPack reports, the Avaya PBX needs to be configured to send the reporting data to the IP address of the VoIP Monitor server

Procedure to set up RTCP.

Procedure

1. [Set up the PBX on page 15](#)
2. [Set up network regions on page 16](#)
3. [Set up monitoring for SIP voice streams](#)
4. [After configuring RTCP on page 16](#)

Setting up the PBX

Perform these tasks to setup your PBX to work with the SolutionPack software.

Before you begin

Make sure you have login credentials with proper administrative rights to make this configuration.

Procedure

1. Use an SSH client to open a terminal and connect to the ACM (Aura Communication Manager).
 - a. Type: `ssh <username>@<ACM FQDN>` and then press **Enter**.
 - b. At the prompt, type: `sat` and then press **Enter**.
 - c. Select terminal type, and press **Enter** to generate a command prompt.
2. Execute the command: `change system-parameters ip-options`
3. In the RTCP MONITOR SERVER section of the code, input the following values:
 - Set the **Default Server IP Address** to the IP address of the VoIP Monitor server.
 - Set the **Default Server Port** to 5005.
 - Set the **Default RTCP Report Period** (secs) to 5.

4. When finished press **Esc+e** to submit the changes.

Setting up network regions

After you set up the VoIP Monitor IP address on the Avaya PBX, configure the associated network regions IP addresses. You can configure either a default setting or add individual IP addresses for each region.

Procedure

1. Execute the command: **change ip-network-region <n>**, where **<n>** is the IP network region number to be monitored.
2. Set the **RTCP Reporting Enabled?** field to **y (yes)** and the **Use Default Server Parameters?** field to **y (yes)**.

Only one RTCP MONITOR SERVER can be configured per IP network region.

3. Repeat Step 2 for all IP network regions that are required to be monitored, and then press **Esc+e** to submit the changes.

Results

The RTCP changes are implemented immediately for all calls, including those already in progress.

Setting up Avaya voice stream monitoring

Voice stream data settings direct voice stream RTCP information to VoIP Monitor.

To monitor voice stream data for Avaya SIP Phones, edit these settings in the Avaya `46xxsettings.txt` file.

Procedure

1. Edit **SET RTCPMON <ip_address>** and insert the **<ip_address>** of the VoIP Monitor server.
2. Edit **SET RTCPMONPORT <port_number>** and set the port number of the port used to send RTCP information to the IP address of the VoIP Monitor server, as specified in the **RTCPMON** statement. When possible use the default setting **5005**.
3. Edit **SET RTCPMONPERIOD <n>** where **<n>** specifies the time interval in seconds when the system sends RTCP monitoring reports (5-30 seconds, with the default of 5). Use the default.

After configuring RTCP Monitoring

After you set the default RTCP monitoring, make sure that you set all phone network regions to use the default RTCP server.

Procedure

1. To set all phone network regions to use the default RTCP server use the **change ip-network-region <n>** command (n = network region) from the Avaya CM command console, and make sure that all phone network regions use the default RTCP server.
2. Use the these Avaya CM Native console commands to display and configure additional phones, IP addresses and network regions as needed.

Command	Result
list ip-interface all	Lists IP interfaces/network regions

Command	Result
<code>display ip-network-region <n></code>	Displays ip network region configuration.
<code>change ip-network-region <n></code>	Change configuration for network region <n>
<code>list registered-ip-stations</code>	List of registered ip stations
<code>list station</code>	Avaya stations list

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.

- ◆ Permanent licenses do not have expiration dates and may be associated with a host ID.
- ◆ Temporary licenses 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 front-end module fails, you cannot access the User Interface.

The SolutionPack license name is either SolutionPack for Avaya or ReportPack for Avaya. The system will use either license.

CHAPTER 2

Installation and Configuration

This chapter includes the following topics:

◆	Installation	20
◆	Logging in to Centralized Management	20
◆	Installing the SolutionPack	20
◆	Starting the CDR and RTCP Listeners	22
◆	Log files	23
◆	Configuring the user process limits for the Linux installation	23
◆	Installing a SolutionPack Center Upgrade	24
◆	Uninstalling a SolutionPack	25

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

Using the Watch4net console, install the SolutionPack.

Before you begin

Make sure you review requirements and complete relevant procedures described in [Installation Workflow on page 7](#), and have your credentials for Avaya Aura Communication Manager and Watch4net on hand.

Procedure

1. Log in to Watch4net with root privileges.
For example, `http://Frontend-hostname:58080/APG`
2. Select **Administration**.
3. Select **Centralized Management** in the **Administration** tree.
4. Select **SolutionPack Center**.
5. Select **Avaya Aura Communication Manager** in the **Browse and Install SolutionPacks** screen.
6. Read the summary information and click **Install**.
7. Select the components to install.
 - a. Accept the default name, **avaya-voip-acm**, in the **Instance name** field.

- b. Select the Watch4netserver that will host the data collector in the **Data collection** list box.
 - c. Select the Watch4net server to host the reports in the **Reports** list box.
 - d. Click **Next**.
8. Accept the default values for the **Data Collection** and **Alerting on Data Collection** panes.
 9. Enter the server addresses, root credentials, and path to the Perl executable directory for the Avaya VoIP-specific configuration. The default Perl path for Windows: C:\strawberry\perl\bin and for Linux: /usr/bin

After installing the SolutionPack, you can click the Device Discovery link in the post install message window, and follow this link to configure SNMP monitoring for the Avaya Call Managers you provided during SolutionPack installation. Alternatively you can add the devices later by accessing the Device Discovery module from Administration window. Follow these steps:

- a. Create a collector (if you have not already created one). Navigate to **Device Discovery > Collectors > Add New Collector**.
- b. Add a device to Watch4net: Navigate to **Administration > Modules > Device Discovery > Devices > Add New Device**, and then configure the name of the device and IP address as part of Main parameters.

Note

Make the **Device Type** `CallManager`, otherwise data for Avaya Health reports will not be displayed in the console.

- c. Configure SNMP Credentials.
- d. Add the previously created collector.
- e. Select appropriate Avaya capabilities for AVAYA-SERVER, GENERIC-INTERFACES, GENERIC-SYSUPTIME.
- f. Distribute: navigate to **Device Discovery > Dashboard** and then click `distribute all approved devices with Capabilities on all enabled collectors`.

After you finish

Allow four to five polling cycles to pass before viewing reports.

Note

If data for CDR reports does not appear, verify whether the CDR Link established successfully by executing the `status cdr-link` command from SAT terminal. Link state should be up.

sample output :

	Primary	CDR LINK STATUS	Secondary
Link State:	up		down
Number of Retries:			ÿÿÿÿ
Date & Time:	2014/02/06 03:46:08		2014/01/16 10:08:20
Forward Seq. No:	0		0
Backward Seq. No:	0		0
CDR Buffer % Full:	0.00		0.00
Reason Code:	OK		Maintenance busy

2. If Link state is down, then execute "test cdr-link primary long" command from SAT terminal to test primary cdr link. Test 215 should PASS.

Sample Output :

TEST RESULTS				
Port Error Code	Mtce Name	Alt. Name	Test No.	Result
	PRI-CDR		213	PASS
	PRI-CDR		215	PASS

If the Test 215 = fail, verify:

- ◆ Watch4Net server is reachable from ACM
- ◆ CDR Listener is running on Watch4Net Server on port 5001(default)

Starting the CDR and RTCP Listeners

After Installing the Solution Pack, start the CDR and RTCP listeners.

Procedure

1. For LINUX, go to <APG_HOME>/Collecting/Text-Collector/avaya-voip-acm/conf/scripts.
 - ./avayaListeners.sh start – This option starts both RTCP and CDR listener
 - ./avayaListeners.sh status - This option shows the status of the listeners in the system.
 - ./avayaListeners.sh stop - This option stops the listeners.
 - ./avayaListeners.sh install – This option runs the listeners as a start option mentioned above addition to install the listeners into System startup so that it starts automatically when the system gets restarted / rebooted.

Note

As you run the above script with parameter start and install, two additional script files are generated. They are `runAvayaCDRListener.sh` and `runAvayaRTCPListener.sh`. These are actual files to start the listeners created by this script.

2. For Windows: Goto <APG_HOME>/Collecting/Text-Collector/avaya-voip-acm/conf/scripts, and run `avayaListeners.bat` to start the listeners using the command: **Cmd> avayaListeners.bat .**

Note

As you run the batch file, two additional batch files are generated. They are `runAvayaCDRListener.bat` and `runAvayaRTCPListener.bat`. Use these files to start the listeners created by this batch file.

To start the listeners automatically on the system restart, add these scripts separately as 2 tasks in Task Scheduler. This step is carried out after running the `avayaListeners.bat`. The procedure follows:

- a. Go to Start->All Programs -> Accessories -> System Tools -> Task Scheduler
- b. Select Action-> Create Task
- c. Add the name of the task to be created under General Tab.

- d. Select Run whether or not the user is logged on.
- e. Select Run with highest privileges.
- f. Go to the Triggers tab.
- g. Add New Trigger.
- h. Select Begin the Task as **At Startup**.
- i. In advanced settings, select **Enabled**.
- j. Go to the **Actions** tab.
- k. Select **New** action.
- l. Select Action as **Start a Program**.
- m. In Settings section below in the same tab, Select **Program Script** – select the `runAvayaRTCPLListener.bat` from `conf/scripts` folder
- n. Go to last tab Settings and deselect Stop the task if it runs longer than option.
- o. Click **OK**.

Repeat these steps to create a task with different name for the `runAvayaCDRListener.bat` script. With **Step m**, you need to select the `runAvayaCDRListener.bat` file.

Log files

Information on the log files for this SolutionPack follow.

Log files for the SolutionPack for Avaya Aura are located in: `<APG_installdir>/Collecting/Collector-Manager/avaya-voip-acm/logs`.

Since this SolutionPack also uses Generic SNMP collector, the log files for this collector appear in `<APG_install>/Collecting/Collector-Manager/Generic-SNMP/logs`.

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.
- ◆ 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
```

After restarting, check the status of services, enter: `./manage-modules.sh service status 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](#)..... 28
- ◆ [Avaya Reports](#)..... 28

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*.

Avaya Reports

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

Some top-level reports include additional sub-level reports with specific metrics related to the top-level report.

- ◆ CPU Utilization for System %
- ◆ CPU Utilization for Calls %
- ◆ CPU Utilization %
- ◆ Avaya Health
- ◆ Busy Calls
 - Data
 - Media
 - Service
 - Total
 - Voice
- ◆ Calls completed
 - Data
 - Media
 - Service
 - Total
 - Voice
- ◆ Other Reports
 - Alarm Occurrences
 - Number of Connections to Switch
 - More Reports
 - Registered Phone Summary
 - Port Network Summary
 - Avaya CDR Reports - Call Data Records (Call Detail and Duration)

- Avaya RTCP Reports - RTCP Summary Report (all network with Source of the call)
- Media Gateways
- Network Region Report
- Occupancy Summary Report
 - Occupancy - Reports time 000 till 2300 - for last 24 hours
 - Calls Summary Report
 - Connections Summary Report
 - Idle Occupancy Report
- Trunk Group Report
 - Trunk Group Inventory Report
 - Trunk Group Member Report

APPENDIX A

Metrics

- ◆ [Metrics for Avaya VoIP](#)..... 32

Metrics for Avaya VoIP

Report metrics are used to create various reports within the SolutionPack. Metrics gather information on values such as switch name, product ID, RTP Monitoring IPV4 address, Trunk Group number, and many more listed in this table.

Table 1 Report metrics

Group Metrics	Details of the Metric	Mode of Collection in APG
IP Phones		
extension	Extension	Text-Collector
set_type	Model /Type	Text-Collector
product_id	Product ID	Text-Collector
station_ip	IP Address	Text-Collector
product_release	Software Release Version of the Phone	Text-Collector
gatekeeper_ip	Gatekeeper's IP Address	Text-Collector
ACM Processor Occupancy Summary		
meas_hour	Measurement Hour (0000, 0100, 0200,0300...2300)	Text-Collector
switch_name	Switch Name	Text-Collector
date	Date of the collected information	Text-Collector
static_occ	Static Occurrence	Text-Collector
cm_occ	CM Occurrence	Text-Collector
sm_occ	SM Occurrence	Text-Collector
idle_occ	Idle Occurrence	Text-Collector
total_calls	Total no of calls	Text-Collector
tandem_calls	Total no of tandem calls	Text-Collector
total_conn	Total Connections	Text-Collector
intcom_atmpts	Internal Communication attempts	Text-Collector
inc_atmpts	Incoming attempts	Text-Collector
out_atmpts	Outgoing attempts	Text-Collector
pnet_atmpts	Port Networking attempts	Text-Collector
Network Region Information		
Region	Network Region number	Text-Collector
Name	Name of the NR	Text-Collector
ipv4PortNum	IPV4 Port Number	Text-Collector

Table 1 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
rtcpMonIPv4	RTCP Monitoring IPV4 address	Text-Collector
rptPeriod	Report Period	Text-Collector
udpMinPort	UDP port allocated Minimum	Text-Collector
udpMaxPort	UDP port allocated Maximum	Text-Collector
codecStatus	CODEC Status	Text-Collector
Port Network Data		
portnetwork	Port Network Number	Text-Collector
major	No of Major alarms	Text-Collector
minor	No of Minor alarms	Text-Collector
Warning	No of Warning alarms	Text-Collector
CarrierlocA	Carrier Location A	Text-Collector
CarrierlocB	Carrier Location B	Text-Collector
pnctrlActive	Port Network Controller Active	Text-Collector
pncontrolStdby	Port Network Controller Standby Status	Text-Collector
Trunk Group Status and Monitoring		
TrunkGroupNo	Trunk Group Number	Text-Collector
Size	Size of the TG	Text-Collector
Active	Status of the TG	Text-Collector
QueueSize	Queue Size	Text-Collector
Waiting	No of waiting calls in that TG	Text-Collector
tac	Trunk Access Code	Text-Collector
tgtype	TG Type	Text-Collector
group_name	TG Name	Text-Collector
mem_numbers	Number of members in that TG	Text-Collector
cor	COR (Class of Restriction)	Text-Collector
cdr	CDR (Call Data Record)	Text-Collector
CDRData		
Date	Date of the call monitored	Text-Collector
Time	Time of the call monitored	Text-Collector
To	Extension To	Text-Collector
From	Extension From	Text-Collector
Duration	Duration of the call	Text-Collector

Table 1 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
MediaGatewayInfo		
number	Media Gateway Number	Text-Collector
gwname	Gateway Name	Text-Collector
gwserial	GW Serial Number	Text-Collector
gwtype	GW Type	Text-Collector
gwip	GW IP address	Text-Collector
gwnrnet_region	Network Region to which the Gateway belongs	Text-Collector
gwregd	GW Registration Status	Text-Collector
firmware_ver	Firmware Version of the GW	Text-Collector
hardware_vintage	Hardware Vintage Version	Text-Collector
clan_ipaddress	CLAN IP Address	Text-Collector
RTCPData		
station-ip	IP Address	Text-Collector
packet-type	Packet Type (SR, RR, SDES etc.)	Text-Collector
ssrc	SSRC - Source of the call	Text-Collector
lastseq	Last Sequence Number	Text-Collector
lsr	Last SR Received	Text-Collector
dlsr	Delay value from the Last SR received	Text-Collector
time	Time of the monitoring data	Text-Collector
jitter	Jitter	Text-Collector
frlost	Fraction Lost	Text-Collector
packlost	Packet Lost	Text-Collector
MoS	Computed based on Latency, PacketLost,Jitter	Formula
R-Factor	Computed based on Latency, PacketLost,Jitter	Formula
OtherACMDatacollectedatACMlevel		
sysUpTime	Uptime	SNMP-Collector
g3connectState	Availability	SNMP-Collector
g3connectTimeUp	Uptime	SNMP-Collector
g3connectAttempts	Attempts	SNMP-Collector
g3connectSuccess	Success	SNMP-Collector

Table 1 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
g3connectRequests	DataRequests	SNMP-Collector
g3connectResponses	DataResponses	SNMP-Collector
g3connectErrors	DataErrors	SNMP-Collector
g3connectQueued	DataQueued	SNMP-Collector
g3healthMajor	AlarmsMajor	SNMP-Collector
g3healthMinor	AlarmsMinor	SNMP-Collector
g3healthWarning	AlarmsWarning	SNMP-Collector
g3healthTrkBusy	TrunksBusy	SNMP-Collector
g3healthStnBusy	StationsBusy	SNMP-Collector
g3healthOthBusy	OthersBusy	SNMP-Collector
g3healthLogins	ActiveLogins	SNMP-Collector
g3healthStaticOcc	CurrentUtilization	SNMP-Collector
g3healthCallpOcc	CurrentUtilization	SNMP-Collector
g3healthSysMgmtOcc	CurrentUtilization	SNMP-Collector
g3healthIdleOcc	Cpuidle	SNMP-Collector
g3pnchealthPncAMajor	AlarmsMajor Port Network Controller A	SNMP-Collector
g3pnchealthPncAMinor	AlarmsMinor Port Network Controller A	SNMP-Collector
g3pnchealthPncAWarning	AlarmsWarning Port Network Controller A	SNMP-Collector
g3pnchealthPncBMajor	AlarmsMajor Port Network Controller B	SNMP-Collector
g3pnchealthPncBMinor	AlarmsMinor Port Network Controller B	SNMP-Collector
g3pnchealthPncBWarning	AlarmsWarning Port Network Controller B	SNMP-Collector
g3stamediaAlarmMajor	AlarmsMajor	SNMP-Collector
g3stamediaAlarmMinor	AlarmsMinor	SNMP-Collector
g3stamediaAlarmWarning	AlarmsWarning	SNMP-Collector
g3stamediaBusyOutTrunks	TrunksBusy	SNMP-Collector
g3stamediaBusyOutStations	StationsBusy	SNMP-Collector
g3stamediaH248LinksDown	H248LinksDown	SNMP-Collector
g3stamediaH248LinksUp	H248LinksUp	SNMP-Collector

Table 1 Report metrics (continued)

Group Metrics	Details of the Metric	Mode of Collection in APG
g3stamediaNbrLogins	ActiveLogins	SNMP-Collector
g3callratedataNumCalls	CallCompleted	SNMP-Collector
g3callratedataBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratevoiceNumCalls	CallCompleted	SNMP-Collector
g3callratevoiceBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratesrvNumCalls	CallCompleted	SNMP-Collector
g3callratesrvBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratemediNumCalls	CallCompleted	SNMP-Collector
g3callratemediBsyCalCmpl	BusyCallCompleted	SNMP-Collector
g3callratetotalNumCalls	CallCompleted	SNMP-Collector
g3callratetotalBsyCalCmpl	BusyCallCompleted	SNMP-Collector

APPENDIX B

Troubleshooting

- ◆ [SSL certificates](#) 38
- ◆ [Contacting EMC Support](#).....41

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

Temporary resolution

Accept the certificate exception temporarily: [Troubleshooting an SSL certificate error: Accepting the exception on page 39](#).

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 39
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 40 2. Importing an SSL certificate into your truststore on page 39
Import an exported SSL certificate that you or another administrator prepared.	Importing an SSL certificate into your truststore on page 39

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 40](#).

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 39](#)
 - [Importing an SSL certificate in Firefox on page 40](#)
 - [Importing an SSL certificate in Internet Explorer on page 40](#)

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.

