

Secure Remote Services Policy Manager[™]

Version 6.8

Policy Manager Installation Guide using Active Directory

REV 02



Copyright © 2018 Dell EMC Corporation. All rights reserved. Published in the USA.

Published November 2018

Dell 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. Dell 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 Dell EMC software described in this publication requires an applicable software license.

EMC², EMC, and the Dell and EMC logos are registered trademarks or trademarks of Dell 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 Dell EMC Online Support (https://support.emc.com).

CONTENTS

Preface

Chapter 1	Introduction	
	Policy Manager	8
	Specifications	9
	VMware support	. 11
Chapter 2	Policy Manager Installation - Windows	
	Standard Policy Manager installation using Active Directory	. 14
Appendix A	Implementation of LDAPS/SSL for Windows	
	Procedure	28
Appendix B	Changing the Directory Server Password	
	Changing the Directory Server Password	36
Appendix C	Backing up Policy Manager Database on Windows Server 2012	
	Installer does not configure Automatic Daily Backup for Policy Manager 6.8 Database	. 40

Contents

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

Note: EMC Secure Remote Services (ESRS) is being rebranded to Secure Remote Services (SRS). This change is not reflected in the user interface as of the time of this publication. Consequently, the screen samples in this document does not reflect the rebranding.

Note: This document was accurate at publication time. Go to Dell EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Audience

This guide is part of the Secure Remote Services documentation set and is intended for use by device administrators.

Related Documentation

You can access the documentation section at:

Secure Remote Services Documentation

Conventions used in this document

Dell EMC uses the following conventions for special notices:

ADANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

AWARNING

WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION, used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

Typographical conventions

Dell EMC uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text and for variables in body text.
Monospace	 Use for: System output, such as an error message or script System code Pathnames, file names, prompts, and syntax Commands and options
Monospace italic	Use for variables.
Monospace bold	Use for user input.
[]	Square brackets enclose optional values
	Vertical bar indicates alternate selections — the bar means "or"
{}	Braces enclose content that the user must specify, such as x or y or z
	Ellipses indicate nonessential information omitted from the example

Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

Product information — For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at:

https://support.emc.com

Technical support — Go to Dell EMC Online Support and click Service Center. You will see several options for contacting Dell EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

techpubcomments@emc.com

CHAPTER 1 Introduction

This chapter introduces the Secure Remote Services (SRS) Policy Manager, version 6.8, which enforces the rules for customer-controlled SRS site access and activity.

٠	Policy Manager	, 8
٠	Specifications	. 9
٠	VMware support	11

Policy Manager

The Policy Manager allows you to set permissions for devices that are being managed by the SRS Clients. The SRS Client polls the Policy Manager every 5 minutes and receives the current policies, which it then caches locally. (Because of this polling time interval, policy updates may take up to 5 minutes before being applied.)

During the periodic poll, the SRS Client posts all requests and actions that have occurred which are then written to local log files and the Policy Manager database. When a remote access request arrives at the SRS Client for device access, the access is controlled by the SRS Client enforcing the policy set by the Policy Manager.

The Policy Manager software may be on another application server (for example, a Dell EMC Navisphere[®] Management station) or co-located on a non-high-availability SRS Client server.

Note: Once installed on your server, the Policy Manager application is inaccessible by third parties, including Dell EMC.

What is New, Fixed, and Improved with SRS Policy Manager 6.8 over SRS Policy Manager 6.6

The following describes what is new, fixed, and improved with SRS Policy Manager 6.8 over SRS Policy Manager 6.6:

1. Issue: Policy Manager does not show more than first 25 users.

Status: Resolved

2. Issue: Using roles/profiles with Active Directory required write access to AD.

Status - Active Directory integration no longer requires write access to AD; roles are managed in the PM database.

- 3. Security hardening processes (ciphers/default permissions, LDAP injection, etc.) rolled up.
- 4. The following CVEs were addressed in this release:
 - CVE-2017-4976
 - CVE-2014-3566
- 5. Updates to the underlying application (Tomcat and Java) have closed security vulnerabilities that were native to the older versions PLUS addressing a number of additional vulnerabilities.
- 6. Local OpenDS does not respond to NULL queries.
- 7. Policy Manager code has been enhanced to assure that policies are consistent across ALL managed Gateways.
- 8. We have simplified implementation with External Directory services.
- 9. We have simplified Windows Active Directory implementation.
- 10. Customers can now use Customer defined groups to replace the required groups of **ESRSUsers/ESRSAdmins** during the install.
- 11. Improved stability and scalability.

Specifications

Table 1 on page 9 shows the minimum configuration of the required hardware and the application software.

Table 1	Specifications	for Policy	/ Manager	server
---------	----------------	------------	-----------	--------

Туре	Requirements	Dell EMC provided software	Notes
Policy Manager server (optional)	 Processor — One or more processors, each 2.1 GHz or better. Free Memory—Minimum 2 GB RAM, preferred 3 GB RAM. (If the Gateway Client and Policy Manager are on the same server, the minimum RAM is 3 GB.) Minimum 4 GB recommend for 64-bit operating systems. Network Interface Cards (NIC) — One 10/100 Ethernet adapters (NIC cards) are recommended (1 GB preferred). You may choose to use a third NIC card for data backups. Free Disk Space — Minimum 2 GB available (preferably on a storage device of 80 GB or larger) Microsoft .NET Framework — Version 2.0 SP1 (minimum) Microsoft.NET Framework A.5 is required if you are using the Customer Environment Check Tool (CECT) to validate that the Policy Manager server is setup correctly to install the PM software. Microsoft.NET Framework 3.5 SP1 in Windows 2012 Note: Microsoft.NET Framework 4.0 is not compatible at this time. Operating System — US English only supported, as follows: Red Hat 6.x 64bit SuSE 11 64bit Windows 8 64bit Windows 2018 R2 Windows 2012 R2 Windows 2012 R2 Windows 2012 R2 Windows 2016 Web Browser: Microsoft Internet Explorer 10+ Google Chrome Mozilla Firefox 	Policy Manager	A Policy Manager is optional, but highly recommended. Policy Manager requires a site-supplied server. Policy Manager supports up to three Gateway Client servers or pairs. One Policy Manager server can support up to 750 devices. Note: Support for Policy Manager on Windows Server 2003 will be deprecated in the near future due to declaration of End of Life/End of Service Life by Microsoft. Note: Policy Manager 6.8 requires Adobe Flash Player 11.2 or later to run in supported browser.
Managed devices	Secure Remote Services products — Support products — You must provide required networking (or VLAN) from the managed devices to the SRS Clients (Gateway and Embedded device Clients) and the Policy Manager servers. Refer to the Secure Remote Services Site Planning Guide.		

Note: Policy Manager REQUIRES that Adobe Flash Player 11.2 or later be installed on any host that will access the Policy Manager with a web browser. This application is NOT included in the Policy Manager software package and must be download from the internet. Packages for redistribution to hosts that do not have internet access are available at http://www.adobe.com/products/flashplayer/distribution3.html.

Note: Windows Server 2012 Foundation or Standard requires that the .NET3.5 SP1 feature be enabled in order to comply with the Microsoft .NET Framework Version 2.0 SP1 (minimum). It is NOT enabled by default. Microsoft .NET.Framework 3.5 is required if you are using the Customer Environment Check Tool (CECT) to validate that the Policy Manager server is setup correctly to install the PM software.

VMware support

SRS is qualified to run on a VMware or Hyper-V virtual machine. VMware/Hyper-V support allows customers to leverage their existing VMware/Hyper-V infrastructure to benefit from the security features of SRS without adding hardware. VMware VMotion functionality also allows the Policy Manager, when installed on a virtual machine, to be moved from one physical server to another with no impact to remote support.

The following are the absolute minimum requirements for VMware support:

- VMware ESX 2.5.2 or later
- 15 GB partition
- 2.2 GHz virtual CPU
- 1 GB memory allocated minimum 2 GB preferred
- SMB modules optional
- VMotion functionality optional is supported for the Policy Manager components
- Operating Systems are the same as for physical hardware

Do not place VMware or Hyper-V images or storage files on Dell EMC devices managed and monitored by SRS. Loss of connectivity to the storage will result in SRS components becoming unavailable and impact the ability to support the deployed devices.

Note: Installation and configuration of the VM or Hyper-V instance and operating system are the customer's responsibility.

Note: It is strongly recommended that the VM/Hyper-V instance be configured to meet or exceed physical hardware requirements.

Note: Virtual environments other than those defined above that fully support the qualified operating systems are permitted but have NOT been tested. The Customer is entirely responsible for the virtual environment, it's maintenance, security, compatibility, and operation.

Introduction

CHAPTER 2 Policy Manager Installation - Windows

This chapter describes how to install the Policy Manager on Windows Server 2008 and above. Topics include:

• Standard Policy Manager installation using Active Directory 14

Standard Policy Manager installation using Active Directory

To install using Active Directory:

1. Right-click on the EMC ESRS Policy Manager installer, and select **Run as administrator**.

Name		Date modified
EMCPoli	cyManager64.exe	2/7/2017 4:12 PM
	Open	
	💡 Run as administrator	
	Troubleshoot compatible Pin to Start Restore previous version Send to	ility 15
	Cut Copy	
	Create shortcut Delete Rename	
	Properties	

Figure 1 Running Installer as administrator

Note: Installation of Policy Manager on Microsoft Windows Server 2012 and above requires that the backup be configured manually and the AT command has been deprecated from Windows Server 2012.

The InstallAnywhere box appears.

	InstallAnywhere	
ئ	InstallAnywhere is preparing to install	
	28%	
		Cancel
(C) 2012 Flexer	ra Software LLC	

Figure 2 InstallAnywhere box

2. The Information Needed for the Installation screen appears. Review the summary and click **Next**.

Information Needed for th		
License Agreement	this installation:	
Choose Install Folder EMC ESRS-IP Policy Man	A. Location where you wish to install the software	^
Database Server Configur Directory Server Configur E-mail Server	 B. EMC Policy Manager Components 1) Database Server - Connection Configuration a) External or internal database 	=
	 b) Database host name c) Database port number d) Database schema name e) Database user name f) Database user password 	
SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary	 2) Directory Server - Configuration a) External (Active Directory) or internal directory server (OpenDS) b) Directory Server Host name (if external) 	

Figure 3 Information Needed for the Installation

3. In the License Agreement screen, read through the agreement, click the option button next to "I accept the terms of the License Agreement," and then click **Next**.

3	EMC ESRS-IP Policy Manager
EMC ² after information from	License Agreement
✓ Information Needed for th ➡ License Agreement	Installation and Use of EMC ESRS-IP Policy Manager Requires Acceptance of the Following License Agreement:
 Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation 	EMC Secure Remote Support (ESRS) Software License Agreement IMPORTANT - PLEASE READ CAREFULLY This EMC Secure Remote Support Software contains computer programs and other proprietary material and information, the use of which is subject to and expressly conditioned upon acceptance of this EMC Secure Remote Support Software License Agreement. This EMC Secure Remote Support Software License Agreement (the "Agreement") is a legal agreement between EMC Corporation, with a principal office at 176 South Street. Honkinton. MA 01748 USA ("EMC").
InstallAnywhere Cancel	Previous Next

Figure 4 License Agreement

- 4. In the Choose Install Folder screen, you can:
 - a. Keep the default folder and click **Next**.
 - b. Use a different folder by clicking **Choose** to browse for the folder in which you want to install the software; when ready, click **Next**.

3	EMC ESRS-IP Policy Manager	- • ×
EMC ² eter information liter	Choo	se Install Folder
Information Needed for th	Where would you like to install?	
License Agreement	C:\EMC\ESRS\PolicyManager	
Choose Install Folder	Restore Default Folde	r Choose
EMC ESRS-IP Policy Man		
Database Server Configur		
Directory Server Configur		
E-mail Server		
Default Notification Templ		
System Error Notification		
EMC ESRS-IP Policy Man		
Non SSL Configuration		
SSL Configuration		
EMC ESRS-IP Policy Man		
Pre-Installation Summary		
Repair Installation		
Instananywhere		
Cancel	Previor	us Next

Figure 5 Choose Install Folder

5. To use Active Directory LDAP services, uncheck Directory Server, and then click **Next**.

2	EMC ESRS-IP Policy Manager
EMC ²	EMC ESRS-IP Policy Manager Components
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur 	Select the Policy Manager components you wish to install on this machine. EMC ESRS-IP Policy Manager and Database Server are required and will be installed by deafult.
 Directory Server Configur E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation 	Required: EMC ESRS-IP Policy Manager Database Server Optional: Directory Server
Cancel	Previous

Figure 6 Policy Manager Components

6. Fill in the appropriate fields for the Policy Manager Database (scroll down for additional fields). It is recommended to use the defaults. Review the content, and then click **Next**.

3	EMC ESRS-IP Policy Manager	x
EMC ² where information little	Database Server Configuration Set	tings
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur. 	Enter the information to use for database installation.	
E-mail Server Default Notification Templ	Database Host Name: localhost	^
System Error Notification EMC ESRS-IP Policy Man	Database Port Number: 9001	=
SSL Configuration SSL Configuration	Database Schema Name:	
Pre-Installation Summary Repair Installation	Database User Name:	~
InstallAnywhere Cancel	Previous	xt

Figure 7 Database Server Configuration Settings

Note: If you change the user name or password, then make sure to record them and keep them for reference. Loss of the user name or password WILL require the uninstall and reinstallation of the Policy Manager as there is **NO** recovery process.

Note: It is strongly recommended to accept the defaults by clicking **Next**; otherwise, be sure to document any changes and make sure to retain them.

7. Scroll down and review the content (This is NOT the login information for the Policy Manager application). Click **Next**.

The screens below are pre-populated with examples. These fields will need to be edited with the proper information relative to the customers Windows AD implementation. It is critical to understand that syntax, punctuation, whitespace and the "paths" are correct for the solution to work and be able to communicate with AD. It is also important to be aware that the application can only follow down the "Tree" so the path defined by the statement MUST be at or one level above the location of the level where the Users and Groups are located. The OU windows uses CN to start the path definition.

The following fields are required:

Note: It is the customer's responsibility to configure these features and is outside the scope of a standard Policy Manager installation.

- Host name for the Directory Server: Host name for the AD server
- Listening Port for Directory Server: If LDAPS is required, best practice is to first configure LDAP then change it over to LDAPS. For details on how to configure Policy Manager to use LDAPS Protocol for Windows Active Directory over SSL, see Appendix A, "Implementation of LDAPS/SSL for Windows,".
- Directory Server Principal DN: Full DN of AD bind account user.
- Directory Server Principal Password: Password for the bind account user.

3	EMC ESRS-IP Policy Manager	x
EMC ² where sufformation bare	Directory Server Configura	ation
Information Needed for th		
✓ License Agreement	Enter the information for the Active Directory Server.	
Choose Install Folder		
EMC ESRS-IP Policy Man		
Database Server Configur		
Directory Server Configur		
E-mail Server	Host name for the Directory Server	
🔁 Default Notification Templ	esrs3dc.esrsdomain.local	
System Error Notification	Listening Dect for Directory Con pr	=
EMC ESRS-IP Policy Man		
Non SSL Configuration		
SSL Configuration	Directory Server Principal DN	
EMC ESRS-IP Policy Man	cn=joebindadmin,ou=Staff,ou=IT,dc=esrsdomain,dc=local	
Pre-Installation Summary	Directory Server Principal Password	-
Repair Installation		¥
InstallAnywhere		
Cancel	Previous Nex	t

Figure 8 Directory Server Configuration

Note: The Password will **not** be stored in clear text in the server.xml file. It will be encrypted. If the Password needs to be changed, then follow the special instructions in Appendix C, "Backing up Policy Manager Database on Windows Server 2012".

- User Base DN = Enter the OU to start searching for users.
- Group Base DN = Enter the OU where the ESRSUsers and ESRSAdmins groups are stored.

	EMC ESRS-IP Policy Manager	x
EMC ² where information firm	Directory Server Configu	ration
Information Needed for th		
Choose Install Folder	Enter the information for the Active Directory Server.	
 EMC ESRS-IP Policy Man Database Server Configur 		
Directory Server Configur E-mail Server		
Default Notification Templ	······	^
System Error Notification EMC ESRS-IP Policy Man	Confirm Directory Server Principal Password	=
Non SSL Configuration SSL Configuration	User Base DN	
EMC ESRS-IP Policy Man	ou=Staff,ou=IT,dc=esrsdomain,dc=local	
Pre-Installation Summary Repair Installation	ou=ESRS,ou=IT,dc=esrsdomain,dc=local	~
InstallAnywhere	Previous N	ext

Figure 9 Directory Server Configuration - continued

Note: Active Directory implementations can vary. Best Practice for User and Group Base DN's are to define them directly to the OU's that contain the users and groups. It is possible to define only the DC = portion of the DN but success will depend on the configuration of the customer's AD environment.

- Username Attribute: Leave default value unless directed by your AD admin.
- Static Group Name Attribute: Leave default value unless directed by your AD admin.
- User from Name Filter: Leave default value unless directed by your AD admin.
- Group from Name Filter: Leave default value unless directed by your AD admin.

3	EMC ESRS-IP Policy Manager	x
EMC ² where information liner	Directory Server Configu	ration
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur 	Enter the information for the Active Directory Server.	
E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man	Username Attribute uid Static Group Name Attribute	<
Non SSL Configuration SSL Configuration EMC ESBS-IP Policy Man	User from Name Filter (sAMAccountName = (0))	=
Pre-Installation Summary Repair Installation	Group from Name Filter (member = {0})	4
Cancel	Previous	ext

Figure 10 Directory Server Configuration - continued

- Policy Manager Users Group: Group that contains users to be managed by Roles/Profiles.
- Policy Manager Administrators Group: Group that contains users that have administrative access to the Policy Manager.

U	EMC ESRS-IP Policy Manager
EMC ² where information there	Directory Server Configuration
Information Needed for th	
✓ License Agreement	Enter the information for the Active Directory Server.
Choose Install Folder	
EMC ESRS-IP Policy Man	
Database Server Configur	
Directory Server Configur	
E-mail Server	Group from Name Hitter
Default Notification Templ	(member = {0})
System Error Notification	Policy Manager Users Group
EMC ESRS-IP Policy Man	ESRSUsers
Non SSL Configuration	Policy Manager Administrators Group
SSL Configuration	ESRSAdmins
EMC ESRS-IP Policy Man	Please consult your Directory Server administrator for the
Pre-installation Summary Repair Installation	correct information to insert here.
InstallAnwhere	
Cancal	Provinue
Calicer	Previous Next

Figure 11 Directory Server Configuration - continued

8. Provide the Customer's mail server and port (25 by default) and/or Protocol (SMTP by default). Click **Next**.

2	EMC ESRS-IP Policy Manager
EMC ² where television here	E-mail Server
Information Needed for th	
✓ License Agreement	Enter the information for outgoing e-mail server.
Choose Install Folder	
EMC ESRS-IP Policy Man	
Database Server Configur	
Directory Server Configur	
E-mail Server	E-mail Server Hostname
Default Notification Templ	mail.example.com
System Error Notification	E-mail Server Port
EMC ESRS-IP Policy Man	25
SSI Configuration	E-mail Server Protocol
EMC ESRS-IP Policy Man	SMTP 🗸
Pre-Installation Summary	
Repair Installation	
InstallAnywhere	
Cancel	Previous Next

Figure 12 E-mail Server

9. Scroll down to view the default notification template. This template is the default template that will be used to send Access Request notification if using the Ask For Approval permission for Remote Connections that is configured in the Policy Manager 6.8 Operations Guide. This can be edited post install.

2	EMC ESRS-IP Policy Manager	x
EMC ² where information from	Default Notification Temp	olate
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man 	Below is the default notification template: If you wish to change it please visit the configuration page within the EMC Policy Server. Hello, Your current authorization Policy Manager rules require your approval for the following EMC support action: Date: <\$TMST> Description: <\$ACTD> Device Model: <\$A_MN> Device Serial Number: <\$A_SN> EMC User Name: <\$USRN> Please click the URL link listed below to approve or deny this request. <\$BURL>/aps/index.html#Requests=Requests	
Pre-Installation Summary Repair Installation	This email was automatically generated by the EMC Secure	~
InstallAnywhere Cancel	Previous	t

Figure 13 Default Notification Template

10. Configure the email address that the Policy Manager will use to send notification of system errors that may occur on the Policy Manager application itself. The addressee is/may be different from the email address that is used to send notification for Support Access Request if the customer has set **Ask For Approval permission for Remote Connections** that is configured in the Policy Manager 6.8 Operations Guide. Click **Next**.

2	EMC ESRS-IP Policy Manager
EMC ²	System Error Notification Settings
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur 	Enter the requested settings for System Error notifications.
 Directory Server Conligur E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation 	E-mail To address someone@example.com E-mail From address esrssupport@emc.com Frequency (in minutes) of e-mails 60 Subject for System Error E-mails EMC Policy Manager System Error
InstallAnywhere Cancel	Previous Next

Figure 14 System Error Notification Settings

Note: Best Practice recommends that the IP address or host name be included in the "Subject for System Error E-mails" field so as to identify which Policy Manager is having an issue. This is especially important in a large enterprise with multiple Policy Managers.

11. The selection in the figure example below is for communication between the Gateways and the Policy Manager and/or users logging on to the Policy Manager with a browser. The recommended selection is **Yes**. The Policy Manager will then use HTTPS on port 8443. The Policy Manager installer will generate and install a self-signed certificate.

3	EMC ESRS-IP Policy Manager
EMC ²	EMC ESRS-IP Policy Manager Communication
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation 	To ensure that internal and external communications are secure between Policy Manager and its clients, EMC recommends that you use SSL. If you do not want to use SSL (HTTPS), please select "No". • Yes • No
InstallAnywhere Cancel	Previous Next

Figure 15 EMC ESRS-IP Policy Manager Communication

12. Enter the hostname or FQDN of the server in the host name field.

U	EMC ESRS-IP Policy Manager	×
EMC ²	SSL Configu	ration
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur 	Enter the SSL information	
E-mail Server Default Notification Templ System Error Notification	Enter the EMC ESRS-IP Policy Manager host name servername.example.com	^
EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration	8443 Keystore esrskeystore.iks	=
EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation	Key Passphrase	~
InstallAnywhere Cancel	Previous	ext

Figure 16 SSL Configuration

Note: The default passphrase is **tomcat**. Enter a different passphrase if desired, ensuring that it is documented. There is no recovery process if the password is lost.

13. If you are performing a new install, select **Install as a service** and **Start the service after installation.**

3	EMC ESRS-IP Policy Manager
EMC	EMC ESRS-IP Policy Manager Service
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur E-mail Server Default Notification Templ System Error Notification System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation 	The components selected for installation are: Database Server - Yes Directory Server - Yes Policy Manager Application - Yes Please check this checkbox if you want to install selected Policy Manager components as a service: ☑ Install as a service ☐ Start the service after installation The selected Policy Manager component's services will be started automatically every time your machine is restarted.
Cancel	Previous Next

Figure 17 Policy Manager Service

14. Select the option in the figure example below if you wish to enable daily backups of the Policy Manager database. If this is a reinstall of the Policy Manager 6.x., do not check this feature as it will already be present and may result in multiple backup jobs being triggered at the same time or successively, and thus may result in stability issues for the Policy Manager or the Policy Manager becoming unavailable.

2	EMC ESRS-IP Policy Manager
EMC	Backup
Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur	Schedule Policy Manger Backup at 3am?
 E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Non SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary 	Backup ESRS-IP Policy Manager Database
InstallAnywhere Cancel	Previous Next

Figure 18 Backup

Note: On Windows Server 2012, this scheduled task is not configured. See Appendix D, "Backing up Policy Manager Database on Windows Server 2012" to correct this issue.

15. Review the planned install, and click **Previous** to correct any errors. Scroll down to view multiple pages of the summary. If satisfied with the information in the summary, click **Install**.



Figure 19 Pre-Installation Summary

16. View progress as the installation and initial configuration of the Policy Manager proceeds.



Figure 20 Installation and initial configuration of the Policy Manager



Figure 21 Installing directory server configuration

17. After the installation completes, click Done.

2	EMC ESRS-IP Policy Manager
 Information Needed for th License Agreement Choose Install Folder EMC ESRS-IP Policy Man Database Server Configur Directory Server Configur E-mail Server Default Notification Templ System Error Notification EMC ESRS-IP Policy Man Mon SSL Configuration SSL Configuration SSL Configuration EMC ESRS-IP Policy Man Pre-Installation Summary Repair Installation InstallAnywhere Cancel 	Installation Complete Congratulations! EMC ESRS-IP Policy Manager has been successfully installed. Click "Done" to quit the installer. Previous Done

Figure 22 Installation Complete

18. Verify that the Policy Manager is available. Open a browser and browse to the Policy Manager:

http://<IP_Addressof the host >:8090/aps

19. If https was selected during the install, then you will be redirected to:

```
https://<IP_Address of the host >:8443/aps
```

Note: If using Windows Firewall or Windows Active Directory Advanced Firewall, you will need to configure access on ports 8090 and 8443 or the server will reject the connection.

20. To log on, enter the credentials of a user that was placed in the ESRSAdmins group.

Sign in To Your Accou	ıt	EMC ²
Username:	admin	
Password:	*****	
Copyright © 2001 - 2013 EM	IC Corporation.	Sign In

Figure 23 Log on page

21. Click Sign In. The Policy Manager interface opens.

APPENDIX A Implementation of LDAPS/SSL for Windows

This appendix describes how to configure Policy Manager to use LDAPS Protocol for Windows Active Directory over SSL.

٠	Procedure	2	8	3
---	-----------	---	---	---

Procedure

This section describes the process to configure Policy Manager to use LDAPS Protocol for Windows Active Directory over SSL. It is based on using the default port of 636, and that standard LDAP is functioning. If the Customer is using a different port, then those changes will need to be implemented where appropriate. The management of the certificate requires the use of the Java Keytool from the command line. There is **no** GUI for this feature/functionality.

Note: It is recommended that the Policy Manager and Policy Manager Database be stopped and that the entire Policy Manager directory structure be copied to another location before attempting to configure LDAPS/Windows Active Directory Integration over SSL to permit easier recovery if necessary without having to perform a full uninstall; reboot, reinstall, and configuration. This backup copy may be deleted when configuration is complete. It is also recommended to perform this procedure before any major changes to the configuration to permit easier recovery in the event of unexpected behaviors as a result of those changes.

- 1. The Host must have a certificate from the domain in order to do the LDAPS/SSL bind as indicated below.
- 2. If this is a server that is not part of the domain, then you can request and install a certificate from your Enterprise CA, depending on your corporate policies. This is beyond the scope of this document or Dell.
- 3. Configuration of the Windows Active Directory for SSL and/or the Certificate Authorities is outside the scope of this documentation and is the Customer's responsibility.
- 4. In order to establish an SSL Tunnel, the Policy Manager MUST have a copy of the Root Certificate Authority's root certificate and the root certificates of all the Certificate Authorities in the chain to the Root CA installed in the cacerts keystore, which is located as follows:

<install_drive>:\EMC\ESRS\PolicyManager\jre\lib\security\cacerts

- 5. Stop the Policy Manager and Policy Manager Database services in the services.msc.
- 6. Change to the location of the keytool directory in the Policy Manager.

C:\Users\Administrator> cd C:\EMC\ESRS\PolicyManager\jre\bin

7. Get a copy of the Root CA Certificate and copy it to a directory on the hard drive.



Figure 24 Copying Root CA Certificate

8. Execute the following command in the command window (RunAsAdministrator mode on Windows Server 2008 or above):

Note: The following command is a single line entry. It is word wrapped here. For LDAPS/Windows AD over SSL to work correctly, the full path to the keystore **must** be supplied. You will be prompted for the password. The password for the cacerts keystore is **changeit**. The certificate will be displayed. Verify the signature and information before importing the certificate.

Command example and explanation

```
keytool -importcert -file C:\0\cacert.cer -keystore
C:\EMC\ESRS\PolicyManager\jre\lib\security\cacerts -alias
esrs20.esrs2kad.local
where:
  - file is the certificate file including full path to be imported
-file C:\0\cacert.cer
-alias is the FQDN of the CA issuing /providing the certificate
-alias esrs20.esrs2K8AD.local
```

-keystore cacerts is the keystore including the full path that the certificate is being installed in

C:\EMC\ESRS\PolicyManager\jre\lib\security\cacerts

Note: Failure to use the full path will result in the creation of a new keystore that will not be in the proper path for the Policy Manager to use for the SSL communication.

You will be prompted for the keystore password - it is changeit

C:\EMC\ESRS\PolicyManager\jre\bin>dir c:\0 Volume in drive C has no label. Volume Serial Number is 1019-DC4B

Directory of c:\0

12/05/2013 01:10 PM <DIR> . 12/05/2013 01:10 PM <DIR> . 11/22/2013 12:39 PM 895 cacert.cer 1 File(s) 895 bytes 2 Dir(s) 20,788,678,656 bytes free

Note: The following command is a single line entry, which is word wrapped here. For LDAPS / WindowsAD over SSL to work correctly the full path to the keystore MUST be supplied. You will be prompted for the password. The password for the cacerts keystore is changeit. The Certificate will be displayed verify the signature and information.

C:\EMC\ESRS\PolicyManager\jre\bin>keytool -importcert -file C:\0\cacert.cer -keystore C:\EMC\ESRS\PolicyManager\jre\lib\security\cacerts -alias esrs20.esrs2k8ad.local Enter keystore password: Owner: CN=ESRS2K8AD-ESRS20-CA, DC=ESRS2K8AD, DC=local Issuer: CN=ESRS2K8AD-ESRS20-CA, DC=ESRS2K8AD, DC=local Serial number: 54ef258e300f6ca340f3cac49c8aff93 Valid from: Tue Nov 19 10:50:26 EST 2013 until: Sun Nov 19 11:00:24 EST 2023 Certificate fingerprints: MD5: 2E:FF:E8:F8:3C:F3:CB:D2:62:40:71:A9:E3:33:3A:E4 SHA1: 77:FC:DD:C2:5D:4A:EC:45:9B:74:8E:32:B4:4C:58:B8:A5:A7:E8:0F SHA256: C8:F6:C0:0D:AE:25:54:1B:6F:05:15:82:27:82:2E:08:35:0D:2C:37:1 E3:5D:81:2B:17:59:00:40:51:15:86 Signature algorithm name: SHA1withRSA Version: 3 Extensions: #1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 0000: 02 01 00 . . . #2: ObjectId: 2.5.29.19 Criticality=true BasicConstraints:[CA:true PathLen:2147483647 1 #3: ObjectId: 2.5.29.15 Criticality=false KeyUsage [DigitalSignature Key_CertSign Crl_Sign 1 #4: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [

```
0000: 94 12 7D 97 5E 57 62 C2 B3 64 66 A6 61 6C 0A D8
....^Wb..df.al..
0010: 60 E4 63 67
                                                          `.cg
1
]
Trust this certificate? [no]: y
                                          <<<<<<type y <ente>r>
to import the Certificate
Certificate was added to keystore
C:\EMC\ESRS\PolicyManager\jre\bin>
Verify the certificate is installed in the keystore:
Note: The following command is a single line entry which is word
wrapped here. For LDAPS/Windows AD over SSL to work correctly the
full path to the keystore MUST be supplied. You will be prompted for
the password. The password for the cacert keystore is changeit. The
Certificate will be displayed verify the signature and information.
C:\EMC\ESRS\PolicyManager\jre\bin>keytool -list -keystore
C:\EMC\ESRS\PolicyManager\jre\lib\security\cacerts -alias
esrs20.esrs2k8ad.local -v
Enter keystore password:
Alias name: esrs20.esrs2k8-ad.local
Creation date: Dec 5, 2013
Entry type: trustedCertEntry
Owner: CN=ESRS2K8AD-ESRS20-CA, DC=ESRS2K8AD, DC=local
Issuer: CN=ESRS2K8AD-ESRS20-CA, DC=ESRS2K8AD, DC=local
Serial number: 54ef258e300f6ca340f3cac49c8aff93
Valid from: Tue Nov 19 10:50:26 EST 2013 until: Sun Nov 19 11:00:24
EST 2023
Certificate fingerprints:
         MD5: 2E:FF:E8:F8:3C:F3:CB:D2:62:40:71:A9:E3:33:3A:E4
         SHA1:
77:FC:DD:C2:5D:4A:EC:45:9B:74:8E:32:B4:4C:58:B8:A5:A7:E8:0F
         SHA256:
C8:F6:C0:0D:AE:25:54:1B:6F:05:15:82:27:82:2E:08:35:0D:2C:37:10:E3:5
D:81:2B:17:59:
40:51:15:86
         Signature algorithm name: SHA1withRSA
         Version: 3
Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
                                                          . . .
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA.true
  PathLen:2147483647
1
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
1
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
```

```
0000: 94 12 7D 97 5E 57 62 C2 B3 64 66 A6 61 6C 0A D8
....^Wb..df.al..
0010: 60 E4 63 67
                                                          `.cg
1
]
C:\EMC\ESRS\PolicyManager\jre\bin>
After importing the certificate, make a copy of the
C:\EMC\ESRS\PolicyManager\Tomcat7\aps\conf\server.xml to permit
recovery if there are issues with the LDAPS configuration.
With Notepad, edit
C:\EMC\ESRS\PolicyManager\Tomcat7\aps\conf\server.xml
~
~
<!-- Directory Server configuration -->
      <Realm className="com.emc.apm.user.CustomJNDIRealm"
              connectionName="APMDSAdmin2"
connectionPassword="MCoCAQECAQEEELGwecrlWl6ptjtV619QsZ0EE0xC0VQ+f06
VVRTLDEig6Zs="
               connectionURL="ldap://10.241.172.20:389"
               alternateURL="ldap://10.241.172.20:389"
               userSearch="(sAMAccountName={0})"
               userBase="CN=Users,dc=ESRS2K8AD,dc=local"
               roleBase="CN=Users,dc=ESRS2k8AD,dc=local"
               roleName="cn"
               roleSearch="(member={0})"
               userSubtree="true"
               roleSubtree="true"/>
     <!-- Define the default virtual host
~
# Edit the ConnectionURL and the AlternateURL to indicate that you
are using LDAPS and the Port used in your environment (Default port
is 636).
<!-- Directory Server configuration -->
      <Realm className="com.emc.apm.user.CustomJNDIRealm"
               connectionName="APMDSAdmin2"
connectionPassword="MCoCAQECAQEEELGwecrlWl6ptjtV619QsZ0EEOxCOVQ+f06
VVRTLDEiq6Zs="
               connectionURL="ldaps://10.241.172.20:636"
               alternateURL="ldaps://10.241.172.20:636"
               userSearch="(sAMAccountName={0})"
               userBase="CN=Users,dc=ESRS2K8AD,dc=local"
               roleBase="CN=Users,dc=ESRS2k8AD,dc=local"
               roleName="cn"
               roleSearch="(member={0})"
               userSubtree="true"
               roleSubtree="true"/>
      <!-- Define the default virtual host
~
~
```

- 9. Save the file.
- 10. Stop and restart the Policy Manager Service.
- 11. Verify that you can log on to the Policy Manager with a user that is a member of the Policy Manager Admin (APSAdmins) Windows Active Directory Group.
- 12. Click **Continue to this website**.

		n ★ ¤
Eile Edit View Favorites Iools Help	💩 🛪 🖾 🛪 🖂 🚔 🛪 Page 🛪 Safety	• Tools • 👰 • 🕅
Commence we draw of the second of the s	in on is the code of South	· 1 <u>0</u> 03 · • • •
The security certificate presented by this website was not issued by a trusted certificate authority.		
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.		
We recommend that you close this webpage and do not continue to this website.		
Click here to close this webpage.		
 Commute to this website (not recommended). More information 		
		~
		🔍 100% 🔻

Figure 25 Continue to this website

13. The user in this case is ampuser8. Sign in as ampuser8.



Figure 26 Login page

14. If the Policy Manager interface appears, you have successfully configured the Policy Manager for Windows Active Directory Integration.

EMC ² Dashboard		Policies Pen	ding Requests Assets	Audit Log	Remote Sessions	Users		0
	ERS			•				
All Groups	1	Policies for the group: Globa			Policies 1 to 33 of 33	on Pages: 1	- 8 8	ana) 💽 💽
▼ GROUPS		Action Name	Permission Name/Description	Filters/Parameters	Inheritance	Acc	ess Right	
Global		Set Data Item Values	Permission for All Data Items No Description	0 Filters Data Item Name:*	Global		Assign Filters	LOCK
		Gateway Provisioning	Default Gateway provisioning per No Description	0 Filters Action:*	Global	✓ ¥ ×	Assign Filters	LOCK
		File Download	Default file download permission No Description	0 Filters File:*	Global	✓ ¥ ×	Assign Filters	LOCK
		File Download	ESRS Device Registration No Description	0 Filters File:worki*	Global	✓ ↓ ×	Assign Filters	LOCK
		File Upload	Default file upload permission No Description	0 Filters File:*	Global	✓ ♥ ×	Assign Filters	LOCK
			Assign Filters 🧹 🖐 🗴	Group Settings Set All Permissions	0 Filte	rs	Show Hidden 🗹	Lock All

Figure 27 Policy Manager interface

15. You must now configure Profiles and Roles in the Policy Manager to permit User Access. Refer to the Policy Manager 6.8 Operations Guide for information about security and administration.

APPENDIX B Changing the Directory Server Password

This appendix describes how to change the Directory Server password.

Changing the Directory Server Password

The password provided in the connectionPassword property in the Tomcat server.xml file must be encrypted. To obtain an encrypted version of a password, you need to use the CryptoUtils tool provided with Policy Server. Follow these steps to change the directory server password, including encrypting the password (Windows paths shown):

- 1. Open the command prompt in administrator mode.
- 2. Run the following command:

Note: Text below needs to be on 1 line - it is wordwrapped below. You MUST enter the full paths as the environment variable {APS_HOME} is not configured.

```
C:\Users\Administrator>C:\EMC\ESRS\PolicyManager\jre\bin\java -cp
C:\EMC\ESRS\PolicyManager\Tomcat7\aps\common\lib\cryptoutils-1.0.2.jar
com.axeda.security.encryption.Encrypt -home
C:\EMC\ESRS\PolicyManager\Tomcat7\aps\conf -?
Usage: java com.axeda.security.encryption.Encrypt [OPTION] ...
        -? -help Print this help message
        -home Pathname of the directory with key
        -echo Do not disable console echo during input
        -stdin Read text from stdin
        -text <text> Encrypt specified <text>
C:\Users\Administrator>C:\EMC\ESRS\PolicyManager\jre\bin\java -cp
C:\EMC\ESRS\PolicyManager\Tomcat7\aps\common\lib\cryptoutils-1.0.2.jar
com.axeda.security.encryption.Encrypt -home
C:\EMC\ESRS\PolicyManager\Tomcat7\aps\conf
Enter text:
                 <<<<<enter the text for the password
MCoCAQECAQEEEJbDTu1IHja7ePIt/zVilhIEEBzfpCIYWuT0p+I8elxlvzs=
```

C:\Users\Administrator>

3. When prompted, enter the password that you want to encrypt.

4. When the utility returns the encrypted version of the password, copy it.

5. As long as you are logged in with administrator rights, open the server.xml file from the directory,

C:\EMC\ESRS\PolicyManager\Tomcat7\aps\conf. 6. Paste the encrypted password in the connectionPassword field of the server.xml file.

7. Save and close the file.

Note: Since the tool's Java classes are packaged in cryptoutils-1.0.2.jar, the cryptoutils-1.0.2.jar (and its dependencies) must exist on the Java class path. For example, assuming that the Policy Server instance is installed in \${APS_HOME}, the CryptoUtils tool should be invoked using the APS home directory.

When run without arguments, the CryptoUtils tool prompts you to enter the text to be Entered.

Note: The \${APS_HOME} variable is NOT set as environment variable the full path MUST be supplied

In addition, this tool supports the following command line options:

Table 2 CryptoUtils tool command line options

Option	Description
-?, -help	Print the help message. Do not disable console echo during input. Read the text from the standard input (instead of the console). Encrypt the specified text (instead of console or standard input).
-echo	Do not disable console echo during input.
-stdin	Read the text from the standard input (instead of the console).
-text text	Encrypt the specified text (instead of console or standard input).

Note: Encrypted passwords produced by the CryptoUtils tool can be used only with the Policy Server instance for which they were created.

Note: Since the tool's Java classes are packaged in cryptoutils-1.0.2.jar, the cryptoutils-1.0.2.jar (and its dependencies) must exist on the Java class path. For example, assuming that the Policy Server instance is installed in \${APS_HOME}, the CryptoUtils tool should be invoked using the APS home directory.

Changing the Directory Server Password

APPENDIX C Backing up Policy Manager Database on Windows Server 2012

This appendix describes the steps you must take to back up the Policy Manager database on Windows Server 2012.

 Installer does not configure Automatic Daily Backup for Policy Manager 6.8 Database 40

Installer does not configure Automatic Daily Backup for Policy Manager 6.8 Database

This issue is caused because Microsoft has deprecated the AT command in Windows 2012 all versions. The Policy Manager Installer calls a script that uses the AT command to configure the scheduled task that performs a daily backup of the Policy Manager Database every day at 3:00 AM local time.

The following is a manually process to accomplish this task. If it is not performed the Policy Manager Database will not be backed up on Windows 2012 and therefore recovery of the Policy Manager. Database if it were to become corrupted will NOT be possible and will require an uninstall, reboot, reinstall, and complete re-configuration of Permissions, Filters, Users, Profiles, Roles and Notifications.

- 1. After the Install completes, log on to the Policy Manager host.
- 2. Open Control Panel.

9	Control Panel\All Con	trol Panel Items
💿 💿 🕤 🛧 骡 🕨 Control P	anel 🔸 All Control Panel Items	マ C Search Control Panel の
ile Edit View Tools Help		
Adjust your computer's se	ttings	View by: Small icons 👻
🏲 Action Center	administrative Tools	🛃 AutoPlay
📮 Color Management	Credential Manager	🔐 Date and Time
🛃 Default Programs	🚔 Device Manager	na Devices and Printers
📮 Display	🕒 Ease of Access Center	Flash Player (32-bit)
F Folder Options	🗼 Fonts	😥 Internet Options
🍓 iSCSI Initiator	🕮 Keyboard	🗫 Language
Interview Mouse	👯 Network and Sharing Center	🛄 Notification Area Icons
Personalization	📰 Phone and Modem	Power Options
Programs and Features	🔗 Region	🐻 RemoteApp and Desktop Connections
🛋 Sound	Sync Center	1 System
Taskbar	🐏 Text to Speech	I Troubleshooting
12	Windows Firewall	Windows Update

Figure 28 Control Panel

3. Open Administrative Tools.

🖄 l 🗋 🔝 = l	Shortcut Tools Control Panel\All Control	Panel Items\Adminis	trative Tools	- • ×
File Home Share View	Manage			v 😮
🍥 💿 👻 🕇 협 🕨 Control Panel 🕨	All Control Panel Items + Administrative Tools	~ C	Search Administrat	tive Tools 🛛 🔎
🔶 Exvorites	Name *	Date modified	Туре	Size
Deskton	🗿 desktop.ini	12/20/2013 11:19	Configuration sett	4 KB
Downloads	💦 Disk Cleanup	7/25/2012 1:22 PM	Shortcut	2 KB
Secent places	Event Viewer	7/25/2012 1:20 PM	Shortcut	2 KB
2 receive process	Internet Information Services (IIS) 6.0 M	a 7/25/2012 1:15 PM	Shortcut	2 KB
🦰 Libraries	Internet Information Services (IIS) Mana	ger 7/25/2012 1:15 PM	Shortcut	2 KB
Documents	🔗 iSCSI Initiator	7/25/2012 1:22 PM	Shortcut	2 KB
-) Music	📩 Local Security Policy	7/25/2012 1:19 PM	Shortcut	2 KB
 Pictures 	B ODBC Data Sources (32-bit)	7/25/2012 1:29 PM	Shortcut	2 KB
Videos	B ODBC Data Sources (64-bit)	7/25/2012 1:25 PM	Shortcut	2 KB
	Performance Monitor	7/25/2012 1:17 PM	Shortcut	2 KB
Computer	Resource Monitor	7/25/2012 1:17 PM	Shortcut	2 KB =
Local Disk (Ct)	👼 Security Configuration Wizard	7/25/2012 1:30 PM	Shortcut	2 KB
2nddrive (Dr)	🛼 Server Manager	7/25/2012 1:19 PM	Shortcut	2 KB
errs 2.0 (\\10.241.172.13) (7)	Services	7/25/2012 1:19 PM	Shortcut	2 KB
C on USCSGUSTALD1CW7	🔝 System Configuration	7/25/2012 1:18 PM	Shortcut	2 KB
D on USCSGUSTALD1CW7	🔁 System Information	7/25/2012 1:18 PM	Shortcut	2 KB
E on USC SOUSTALD1CW7	😥 Task Scheduler	7/25/2012 1:20 PM	Shortcut	2 KB
G on USCSGUSTALD1CW7	🔗 Windows Firewall with Advanced Securi	ty 7/25/2012 1:29 PM	Shortcut	2 KB
S on USCSGUSTALD1CW7	😹 Windows Memory Diagnostic	7/25/2012 1:17 PM	Shortcut	2 KB
	😸 Windows PowerShell (x86)	7/26/2012 1:03 AM	Shortcut	3 KB
👊 Network	Windows PowerShell ISE (x86)	7/25/2012 1:20 PM	Shortcut	2 KB ¥
27 items 1 item selected 1.10 KB			Activa	ate Wingeby

Figure 29 Administrative Tools

- 4. Open Task Scheduler.
- 5. In the Actions pane, click Enable All Tasks History. This will permit troubleshooting of scheduled task issues. It is disabled by default.

•	Task Scheduler	I
File Action View Help		
 Task Scheduler (Local) Task Scheduler Library Task Scheduler Library Task Scheduler Library 	Name Status Triggers Next Run Time Last Run Time Last Run Result Optimize Sta Ready When computer is idle Never III III III IIII 	Actions Task Scheduler Lite © Create Basic Task Import Task Import Task © Display All Runnin Import Task Wew Folder View Refresh Import Help
) A (in all account

Figure 30 Task Scheduler

6. Then click Create Task. You are presented with a blank template.

Θ	Create Task	x
General Trig	gers Actions Conditions Settings	
Name:]
Location:	/	
Author:	W2K12-STD-100\Administrator	
Description:		
Security opt When runni	ions	
W2K12-STD	-100\Administrator Change User or Group	
Run only	/ when user is logged on	
O Run whe	ther user is logged on or not	
🗌 Don	ot store password. The task will only have access to local computer resources.	
🗌 Run with) highest privileges	
🗌 Hidden	Configure for: Windows Vista™, Windows Server™ 2008 ✓	
	OK Cancel	

Figure 31 Create Task

7. Fill in the necessary information as below. Then select Triggers.

	Create Task	¢
General Trig	gers Actions Conditions Settings	
Name:	Daily policy Manager Database Backup	
Location:	\ \	
Author:	W2K12-STD-100\Administrator	
Description:	Daily policy Manager Database Backup @ 0300 hours local time	
- Security opt	ions	
When runn	ing the task, use the following user account:	
W2K12-STL	-100\4dministrator Change User or Group	
O Run only	/ when user is logged on	
Run whe	ther user is logged on or not	
🗹 Don	ot store password. The task will only have access to local computer resources.	
🗹 Run with	n highest privileges	
🗌 Hidden	Configure for: Windows Vista™, Windows Server™ 2008 ✓	
	OK Cancel]

Figure 32 General tab

- 8. Fill in the information needed:
 - a. Leave **On a schedule**.
 - b. Select **Daily** radio button.
 - c. Check Stop task if running longer than and select 2 hours in the drop-down.
 - d. Click OK.

	New Trigger	x
Begin the task: C)n a schedule 🗸	
 One time Daily Weekly Monthly 	Start: 1/31/2014 🔍 3:00:01 AM 🏠 Synchronize across time zones Recur every: 1 days	
-Advanced setting	15	
🗌 Delay task for	r up to (random delay): 1 hour 💗	
📃 Repeat task e	very: 1 hour v for a duration of: 1 day v	
🗌 Stop all	running tasks at end of repetition duration	
🗹 Stop task if it	runs longer than: 🛛 🖌 🗸	
Expire: 1/3	1/2015 🗐 🔻 2:24:04 PM 🔪 🗌 Synchronize across time zones	
🗹 Enabled		
	OK Cancel	

Figure 33 New Trigger

9. Select the Actions tab, and click New.

G	Create Task	X
General Trigge When you cre	rs Actions Conditions Settings ate a task, you must specify the action that will occur when your task starts.	
Action	Details Edit Delete	•
	ОК	Cancel

Figure 34 Actions tab

10. On the Edit Action template:

- a. Leave Action at Start a program.
- b. In the Program/script field the drive and path to the location of the backup_database.bat file.

(Default path C:\EMC\ESRS\PolicyManager\hsqldb\bin\ backup_database.bat)

- c. Add Arguments enter 30 (this is the maximum number of backups maintained).
- d. Leave the Start in field blank.
- e. Click OK.

You must specify what action this task will perform.					
~					
_databa Browse					
30					
OK Cancel					

Figure 35 Edit Action

11. Select the Conditions tab, and configure as below. Click OK.

Create	e Task	×
General Triggers Actions Conditions Settings		
Specify the conditions that, along with the trigger, dete run if any condition specified here is not true. Idle	rmine whether the task shou	ld run. The task will not
Start the task only if the computer is idle for:	10 minutes	¥
Wait for idle for:	1 hour	~
Stop if the computer ceases to be idle		
Restart if the idle state resumes		
Power Start the task only if the computer is on AC power		
Stop if the computer switches to battery power		
Wake the computer to run this task		
Network —	ilable:	
Any connection		~
		OK Cancel

Figure 36 Conditions tab

12. Select the **Settings** tab.

- a. Configure as below:
- b. After checking Stop the task if ...
- c. Select 2 hours from the drop-down.
- d. Click OK.

Create Task	X
General Triggers Actions Conditions Settings	
Specify additional settings that affect the behavior of the task.	
Allow task to be run on demand	
Run task as soon as possible after a scheduled start is missed	
If the task fails, restart every:	10 minut 🗸
Attempt to restart up to:	3 times
Stop the task if it runs longer than:	2 hours 🗸
✓ If the running task does not end when requested, force it to	stop
If the task is not scheduled to run again, delete it after:	30 days 🗸 🗸
If the task is already running, then the following rule applies:	
Do not start a new instance 🗸 🗸	
	OK Cancel

Figure 37 Settings Task

The Scheduled Task is now configured.

0	Task Scheduler	_ 0
File Action View Help		
 Task Scheduler (Local) Task Scheduler Library Microsoft 	Name Status Triggers Next Run Time Last Run Time Last Run Time Last Run Result • Daily policy • Optimize Sta Ready At 3:00 AM every day 2/1/2014 3:00:01 AM Never • Optimize Sta Ready When computer is idle Never	Actions Task Scheduler Libr Create Basic Task Create Task Import Task
	III Orditions Conditions Settings History	Disable All Tasks Hi Disable All Tasks Hi New Folder View
	Location: \ Author: W2K12-STD-100\Administrator	 Refresh Help
	Description: Daily policy Manager Database Backup @ 0300 hours local time	Run End Disable
	Security options When running the task, use the following user account	Export B Properties Delete

Figure 38 Task Scheduler

- 13. Verify the Policy Manager Database backup task executes successfully.
- 14. In the center pane select the newly created Backup Task.
- 15. In the Action Pane, click the Run button. The Task will be queued and will Run. The Center Pane will indicate success or failure.

•	Task Scheduler	
File Action View Help		
🏟 🖄 🖬 👔 🖬		
🕑 Task Scheduler (Local)	Name Status Triggers Next Run Time Last Run Time Last Run Result	Actions
▷ 🛅 Task Scheduler Library	(B) Optimize Sta Ready When computer is idle Never	Task Sch
	Policy Mana Ready At 3:00 AM every day 2/1/2014 3:00:00 AM 1/31/2014 3:00:00 AM The operation cor	🕑 Creat
		🕭 Creat
		Impo
		Displa
		🗐 Enabl
		Merec New 1
	General Inggers Actions Conditions Settings History (disabled)	16
	Name: Policy Manager BU	View
	Location: \	Refre:
	Author: W2K12-STD-100\Administrator	👔 Help
	Description: Backup Policy Manager @ 0300 each day	Selected
		🕨 Run
		End
		🐥 Disab
		Expor
	security options	🕒 Prope
	When running the task, use the following user account:	🗙 Deleti
	C Acțiva	te Winc

Figure 39 Backup Directory before Scheduled Task was executed



Figure 40 Directory after the Scheduled task completed

Issue resolved.