

IDENTITY AND ACCESS MANAGEMENT FOR ELECTRIC UTILITIES

How-To Guides

For Security Engineers

Jim McCarthy

Don Faatz

Harry Perper

Chris Peloquin

John Wiltberger

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-2c
DRAFT

IDENTITY AND ACCESS MANAGEMENT FOR ELECTRIC UTILITIES

Energy

Draft

Jim McCarthy
*National Cybersecurity Center of Excellence
Information Technology Laboratory*

Don Faatz
Harry Perper
Chris Peloquin
John Wiltberger
*The MITRE Corporation
McLean, VA*

Leah Kauffman, Editor-in-Chief
*National Cybersecurity Center of Excellence
Information Technology Laboratory*



August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-2c
Natl. Inst. Stand. Technol. Spec. Publ. 1800-2c, 306 pages (August 2015)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at <http://nccoe.nist.gov>.

Comments on this publication may be submitted to: Energy_NCCoE@nist.gov

Public comment period: *August 25, 2015 through October 23, 2015*

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002), Rockville, MD 20850
Email: Energy_NCCoE@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit <http://nccoe.nist.gov>. To learn more about NIST, visit <http://www.nist.gov>.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. The documents in this series do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

To protect power generation, transmission, and distribution, energy companies need to control physical and logical access to their resources, including buildings, equipment, information technology, and industrial control systems. They must authenticate authorized individuals to the devices and facilities to which they are giving access rights with a high degree of certainty. In addition, they need to enforce access control policies (e.g., allow, deny, inquire further) consistently, uniformly, and quickly across all of their resources. This project resulted from direct dialogue among NCCoE staff and members of the electricity subsector, mainly from electric power companies and those who provide equipment and/or services to them. The goal of this project is to demonstrate a centralized, standards-based technical approach that unifies identity and access management (IdAM) functions across operational technology (OT) networks, physical access control systems (PACS), and information technology systems (IT). These networks often operate independently, which can result in identity and access information disparity, increased costs, inefficiencies, and loss of capacity and service delivery capability. This guide describes our collaborative efforts with technology providers and electric company stakeholders to address the security challenges energy providers face in the core function of IdAM. It offers a technical approach to meeting the challenge, and also incorporates a business value mind-set by identifying the strategic considerations involved in implementing new

technologies. This NIST Cybersecurity Practice Guide provides a modular, open, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how we met the challenge using open source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case scenario is based on a normal day-to-day business operational scenario that provides the underlying impetus for the functionality presented in the guide. While the reference solution was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with an energy provider's existing tools and infrastructure.

KEYWORDS

Cyber, physical, and operational security; cyber security; electricity subsector; energy sector; identity and access management; information technology

ACKNOWLEDGMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Jasvir Gill	AlertEnterprise
Srini Kakkera	AlertEnterprise
Srinivas Adepu	AlertEnterprise
Pan Kamal	AlertEnterprise
Mike Dullea	CA Technologies
Ted Short	CA Technologies
Alan Zhu	CA Technologies
Peter Romness	Cisco Systems
Lila Kee	GlobalSign
Sid Desai	GlobalSign
Paul Townsend	Mount Airey Group (MAG)

Joe Lloyd	Mount Airey Group (MAG)
Ayal Vogel	RADiFlow
Dario Lobozzo	RADiFlow
Steve Schmalz	RSA
Tony Kroukamp (The SCE Group)	RSA
Kala Kinyon (The SCE Group)	RSA
Dave Barnard	RS2 Technologies
David Bensky	RS2 Technologies
Rich Gillespie (IACS Inc.)	RS2 Technologies
George Wrenn	Schneider Electric
Michael Pyle	Schneider Electric
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Clyde Poole	TDi Technologies
Danny Vitale	XTec

Table of Contents

Disclaimer.....	ii
National Cybersecurity Center of Excellence.....	iii
NIST Cybersecurity Practice Guides.....	iii
Abstract.....	iii
Keywords.....	iv
Acknowledgments.....	iv
1 Introduction.....	1
1.1 Practice Guide Structure	1
1.2 Conventions.....	2
2 Build Overview.....	3
2.1 Build Implementation Overview	5
2.2 Build Implementation Descriptions	9
2.3 IP Network Address Assignments	16
3 Build Infrastructure.....	17
3.1 Operating Systems	17
3.2 Firewall Configurations	18
3.3 Network Services.....	25
4 Remote Terminal Units (RTUs)	36
4.1 TCP/IP RTU	36
4.2 Serial RTU	36
5 Identity Services Engine (ISE) and TrustSec Enabled Switch: Cisco.....	36
5.1 Security Characteristics	36
5.2 Pre-Installation Task.....	36
5.3 Install and Configure	37
6 Identity Manager: CA Technologies (CA) Installation – Build #1.....	43
6.1 Security Characteristics	43
6.2 Installation Prerequisites	43
6.3 Install CA Directory.....	44
6.4 Install CA Identity Manager.....	44
6.5 Create the Sample NeteAuto Directory	45
6.6 Create the Provisioning Directory	46
6.7 Create the NeteAuto Environment	46
6.8 Configure Connection to AlertEnterprises Database.....	47
6.9 Policy Xpress Policy Review.....	49
6.10 Update Create User and Modify User screens.....	49
6.11 Install Activity Directory Certificate	50

6.12	Acquire Activity Directory Endpoint.....	50
6.13	Explore and Correlate Active Directory.....	51
6.14	Create the Active Directory Account Template and Provisioning Role	51
6.15	Modify Create AE User Policy to include the new Provisioning Role	52
6.16	Add Workflow control over Create User and any other task as desired	52
6.17	Test Creation of a User Manually.....	53
6.18	Test Creation of a User with a CSV file.....	53
7	Identity Management and Governance (IMG): RSA (Build #2)	54
7.1	Security Characteristics	54
7.2	IMG Installation.....	54
7.3	IMG Configuration and Integration with Directories.....	54
7.4	Using RSA IMG.....	109
8	Installation of Adaptive Directory: RSA (Build #2).....	115
8.1	Security Characteristics	115
8.2	RSA Adaptive Directory Is Installed on the IdAM Network, on a VM That Is Running CentOS 7	115
8.3	Additional Steps Required After Installation Is Complete	121
8.4	Custom Attribute Configuration	130
8.5	RSA AD Optimization and Tuning.....	131
9	Privileged User Access Control: AlertEnterprise Guardian Installation	133
9.1	Security Characteristics	133
9.2	Installation on Tomcat and Windows	133
9.3	AlertEnterprise Application Configurations for the RSA Build.....	144
9.4	Section 3. AlertEnterprise Application Configurations for the CA build	160
10	PACS Server: RS2 Access It Universal Server Installation	189
10.1	Security Characteristics	189
10.2	System Environment	190
10.3	AIUNIVERSAL Installation	190
10.4	Post Installation.....	190
11	Privileged User Access Control: TDi ConsleWorks Server Installation.....	192
11.1	Security Characteristics	192
11.2	ConsoleWorks Server Installation	192
12	ICS/SCADA Firewall: RADiFlow.....	194
12.1	Security Characteristics	194
12.2	OT Network RADiFlow Management Workstation Installation.....	195
13	Ozone: MAG Installation.....	196
13.1	Security Characteristics	197
13.2	Ozone Console Installation and Authority Configuration	197

13.3	Ozone Authority Installation	198
13.4	Ozone Console Server Configuration	206
13.5	Ozone Server Installation	213
13.6	Ozone Envoy Installation.....	216
13.7	Ozone Console Envoy Configuration.....	218
14	Physical Access Control: XTec XNode	222
14.1	Security Characteristics	222
15	Enterprise PKI Platform: GlobalSign	222
15.1	Overview	222
15.2	Security Characteristics	224
15.3	How To Order Certificates.....	224
15.4	GlobalSign's Identity and Access Management Solution for Managing External Users 232	
15.5	Getting Help	232
16	Industrial Firewall: Schneider Electric.....	232
17	Operating System STIG Compliance Reports.....	246
17.1	SQL Server on IdAM Network STIG Compliance Report	247
17.2	RSA IMG SUSE Linux Server STIG Compliance Report.....	247
17.3	RSA Adaptive Directory Centos 7 Server STIG Compliance Report.....	254
17.4	AlertEnterprise Microsoft Server STIG Compliance Report.....	255
17.5	IT Domain Controller STIG Compliance Report.....	264
17.6	IT Windows 7 Workstations STIG Compliance Report	265
17.7	Ozone Authority and Ozone Server Centos 6 Server STIG Compliance Report.....	267
17.8	Ozone Envoy Centos 6 Server STIG Compliance Report	268
17.9	OT Domain Controller STIG Compliance Report	269
17.10	OT ConsoleWorks Windows Server 2012 STIG Compliance Report.....	270
17.11	OT Windows 7 Workstations STIG Compliance Report.....	272
17.12	PACS Domain Controller STIG Compliance Report.....	273
17.13	PACS Console Windows Server 2012 STIG Compliance Report	275
17.14	Baseline CentOS 7 Linux Configuration	277
17.15	Baseline CentOS 7 STIG Compliance.....	288
18	Acronyms	290
	List of Figures	291
	List of Tables	296

1 **1 INTRODUCTION**

2 **1.1 PRACTICE GUIDE STRUCTURE**

3 This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and
4 provides users with the information they need to replicate this approach to identity and access
5 management (IdAM). The example solution is modular and can be deployed in whole or in
6 parts.

7 This guide contains three volumes:

- 8 • NIST SP 1800-2a: Executive Summary
- 9 • NIST SP 1800-2b: Approach, Architecture, and Security Characteristics – what we built
10 and why
- 11 • **NIST SP 1800-2c: How To Guides – instructions
12 for building the example solution**

 **YOU ARE HERE**

13 The following instructions show IT professionals and security engineers how the National
14 Cybersecurity Center of Excellence (NCCoE) implemented example solutions to the challenge of
15 a centralized IdAM system. We developed two builds that conform to federal standards and best
16 practices, and address the challenge of providing a secure, centralized, uniform, and efficient
17 solution for managing authentication and authorization services, access control, and
18 provisioning across what are currently three independent and disparate corporate silos: IT,
19 operational technology (OT), and physical access control systems (PACS) networks.

20 This example solution is packaged as a “How To” guide. The guide demonstrates how to
21 implement standards-based, commercially available cybersecurity technologies in the real
22 world, based on risk analysis.

23 We cover all the products that we employed in this example solution. We do not recreate the
24 product manufacturer’s documentation, which is presumed to be widely available. Rather, these
25 guides show how we incorporated the products together in our environment.

26 These guides assume that the people using this document have experience implementing
27 information technology security products (including systems integration and administration of
28 networked Windows and Linux systems, firewalls, routers, etc.) in an electricity subsector
29 organization. While we have used the commercially available products described here, we
30 assume that you have the knowledge and expertise to choose other products that might better
31 fit your IT systems and business processes.¹ If you use substitute products, we hope you’ll seek

¹ Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

32 products that are congruent with standards and best practices, as we have. Refer to NIST SP
33 1800-2b: Approach, Architecture, and Security Characteristics, Section 4.5, Table 2, for a list of
34 the products that we used, mapped to the cybersecurity controls provided by this example
35 solution, to understand the characteristics you should seek in alternate products. Section 4.4
36 Security Characteristics and Controls Mapping, of that document describes how we arrived at
37 this list of controls.

38 The security characteristics in our access management platform are informed by guidance and
39 best practices from standards organizations, including the North American Electric Reliability
40 Corporation's (NERC) Critical Infrastructure Protection (CIP) standards. In addition, this
41 document was reviewed by the NERC ES-ISAC to ensure that the approach was informed by
42 standards and NERC regulations.

43 While we have used a suite of commercial products to address this challenge, this guide does
44 not endorse these particular products, nor does it guarantee regulatory compliance. Your
45 utility's information security experts should identify the standards-based products that will best
46 integrate with your existing tools and IT system infrastructure. Your company can adopt this
47 solution or one that adheres to these guidelines in whole, or you can use this guide as a starting
48 point for tailoring and implementing parts of a solution. This NIST Cybersecurity Practice Guide
49 does not describe "the" solution, but a possible solution. This is a draft version. We are seeking
50 feedback on its contents and welcome your input. Comments and suggestions will improve
51 subsequent versions of this guide. Please contribute your thoughts to energy_nccoe@nist.gov,
52 and join the discussion at <http://nccoe.nist.gov/forums/energy>.

53 **NOTE:** These are not comprehensive tutorials. There are many possible service and
54 security configurations for these products that are out of scope for this example
55 solution.

56 **1.2 CONVENTIONS**

57 Filenames, pathnames, partitions, URLs, and program names are in italic text:

58 *filename.conf*

59 *.../folder/filename.conf*

60 *http://nccoe.nist.gov*

61 Commands and status codes are in Courier:

62 `mkdir`

63 Code that a user inputs is in **Garamond bold**:

64 **service sshd start**

65 **2 BUILD OVERVIEW**

66 The NCCoE constructed the IdAM build infrastructure using off-the-shelf hardware and
 67 software. The infrastructure was built on Dell model PowerEdge R620 server hardware. The
 68 server operating system was VMware vSphere virtualization operating environment. In addition,
 69 a 6-terabyte Dell EqualLogic network attached storage (NAS) product was used for storage, Dell
 70 model PowerConnect 7024 and Cisco Catalyst 3650 and 3550 physical switches were used to
 71 interconnect the server hardware, external network components, and the NAS.

72 The lab network was accessible from the public Internet via a virtual private network (VPN)
 73 appliance and firewall to enable secure Internet and remote access. The lab network was not
 74 connected to the NIST enterprise network. Table 1 lists which software and hardware
 75 components were used in the builds, the specific function each component contributes, and
 76 whether the product was installed within the virtual environment or as physical device.

77 *Table 1. Build Implementation Component List (including security controls)*

Product Vendor	Component	Function	Implementation (physical device or virtual environment)
Dell	PowerEdge R620	Server hardware	Physical device
Dell	PowerConnect 7024	Network switch	Physical device
Dell	EqualLogic	Network attached storage	Physical device
VMware	vSphere vCenter Server version 5.5	Virtual server and workstation environment	Virtual environment
Microsoft	Windows Server 2012 r2 Active Directory Server	Authentication and authority	Virtual environment
Microsoft	Windows 7	Information management	Virtual environment
Windows	Windows Server 2012 r2 DNS Server	Domain name system	Virtual environment
Windows	SQL Server	Database	Virtual environment

Product Vendor	Component	Function	Implementation (physical device or virtual environment)
AlertEnterprise	Enterprise Guardian	Interface and translation between IdAM central store and the PACS management server	Virtual environment
CA Technologies	Identity Manager Rel 12.6.05 Build 06109.28	Identity and access automation management application, IdAM provisioning	Virtual environment
Cisco	ISE Network Server 3415	Network access controller	Virtual environment
Cisco	Catalyst 3550	Network switch	Physical device
Cisco	Catalyst 3650	TrustSec-enabled physical network switch	Physical device
GlobalSign	SSL Certificate	Cloud certificate and registration authority	Virtual environment
Mount Airey Group	Ozone Authority	Central attribute management system	Virtual environment
Mount Airey Group	Ozone Console	Ozone administrative management console	Virtual environment
Mount Airey Group	Ozone Envoy	Enterprise identity store interface	Virtual environment
Mount Airey Group	Ozone Server	Ozone centralized attribute based authorization server	Virtual environment
RADiFlow	Industrial Service Management Tool (iSIM)	Supervisory control and data acquisition (SCADA) router management application	Physical device

Product Vendor	Component	Function	Implementation (physical device or virtual environment)
RADiFlow	SCADA Router RF-3180S	Router/firewall for SCADA network	Physical device
RSA	Adaptive Directory Version 7.1.5	Central identity store, IdAM provisioning	Virtual environment
RSA	IMG Version 6.9 Build 74968	Central IdAM system (workflow management)	Virtual environment
TDi Technologies	ConsoleWorks	User access controller, monitor, and logging system	Virtual environment
RS2 Technologies	AccessIT! Universal Release 4.1.15 Physical access control components	Configures and monitors the PACS devices (e.g., card readers, keypads)	Virtual environment server and physical device card reader
Schweitzer Electronics Laboratory	SEL-2411	Remote Terminal Unit (RTU)	Physical device
Schneider Electric	Tofino Firewall model number TCSEFEA23F3F20	Ethernet/IP firewall	Physical device
XTEC	Xnode	Remote access control and management	Physical device

78 [2.1 BUILD IMPLEMENTATION OVERVIEW](#)

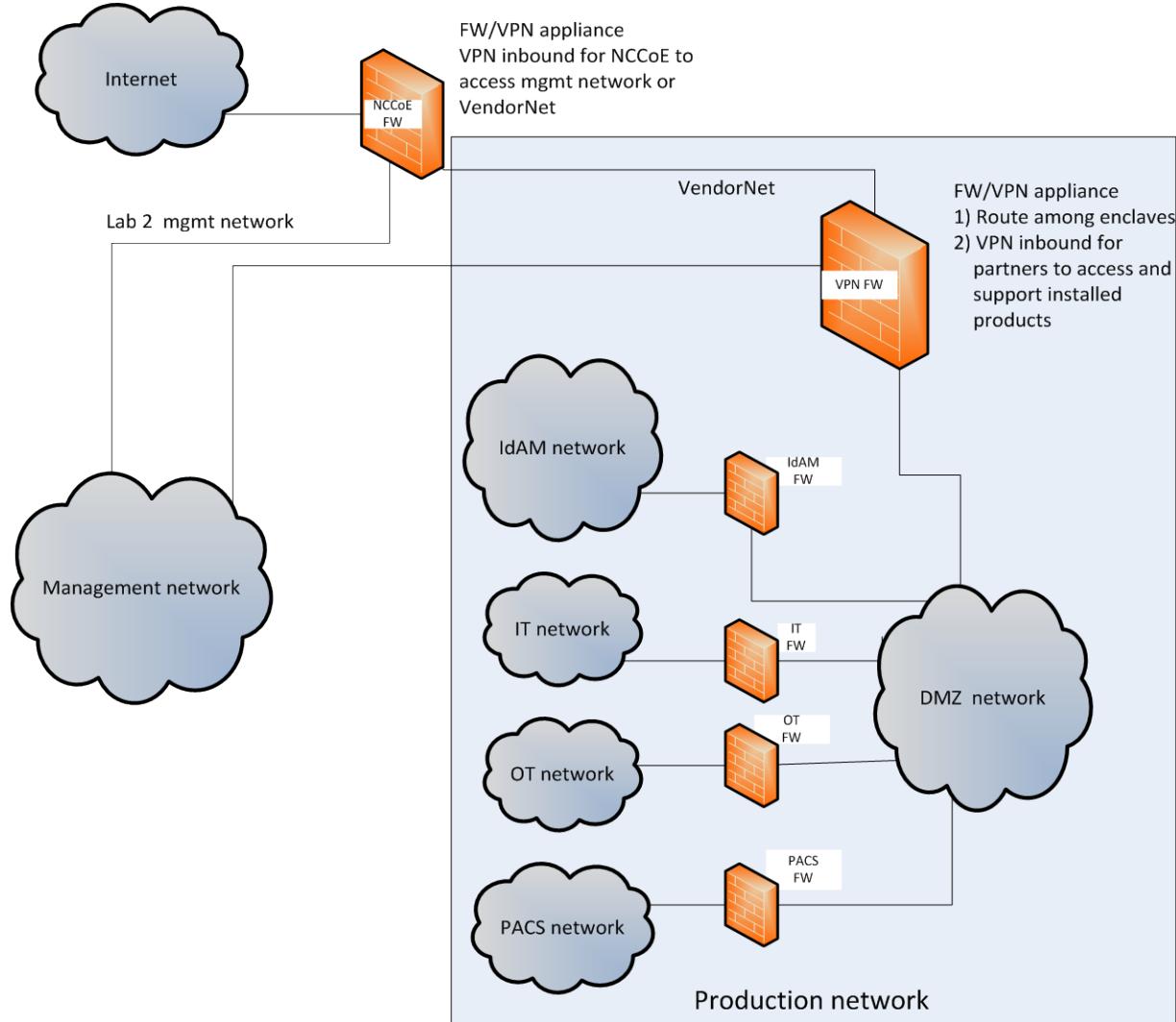
79 The build implementation consists of multiple networks implemented to mirror the
 80 infrastructure of a typical energy industry corporation. The networks include a management
 81 network and a production network, Figure 1. The management network was implemented to
 82 facilitate the implementation, configuration, and management of the underlying infrastructure,
 83 including the physical servers, vSphere infrastructure, and monitoring. The production network,
 84 Figure 1, consists of

85

- the demilitarized zone (DMZ)

86 • Identity and Access Management - IdAM
87 • IT - business management system
88 • OT - ICS/SCADA industrial control system and energy management system (EMS)
89 • PACS – physical access control system networks

90 These networks were implemented separately to match a typical electric utility enterprise
91 infrastructure. Firewalls are configured to route traffic and limit access among the production
92 networks to block all traffic except required inter-network communications. The primary inter-
93 network communications are the user access and authorization updates from the central IdAM
94 systems to and from the directories and PACS, IT, and OT networks. The DMZ provides a
95 protected neutral network space that the other networks of the production network can use to
96 route traffic to and from the Internet or each other.

97
98

99

Figure 1. Management and production networks

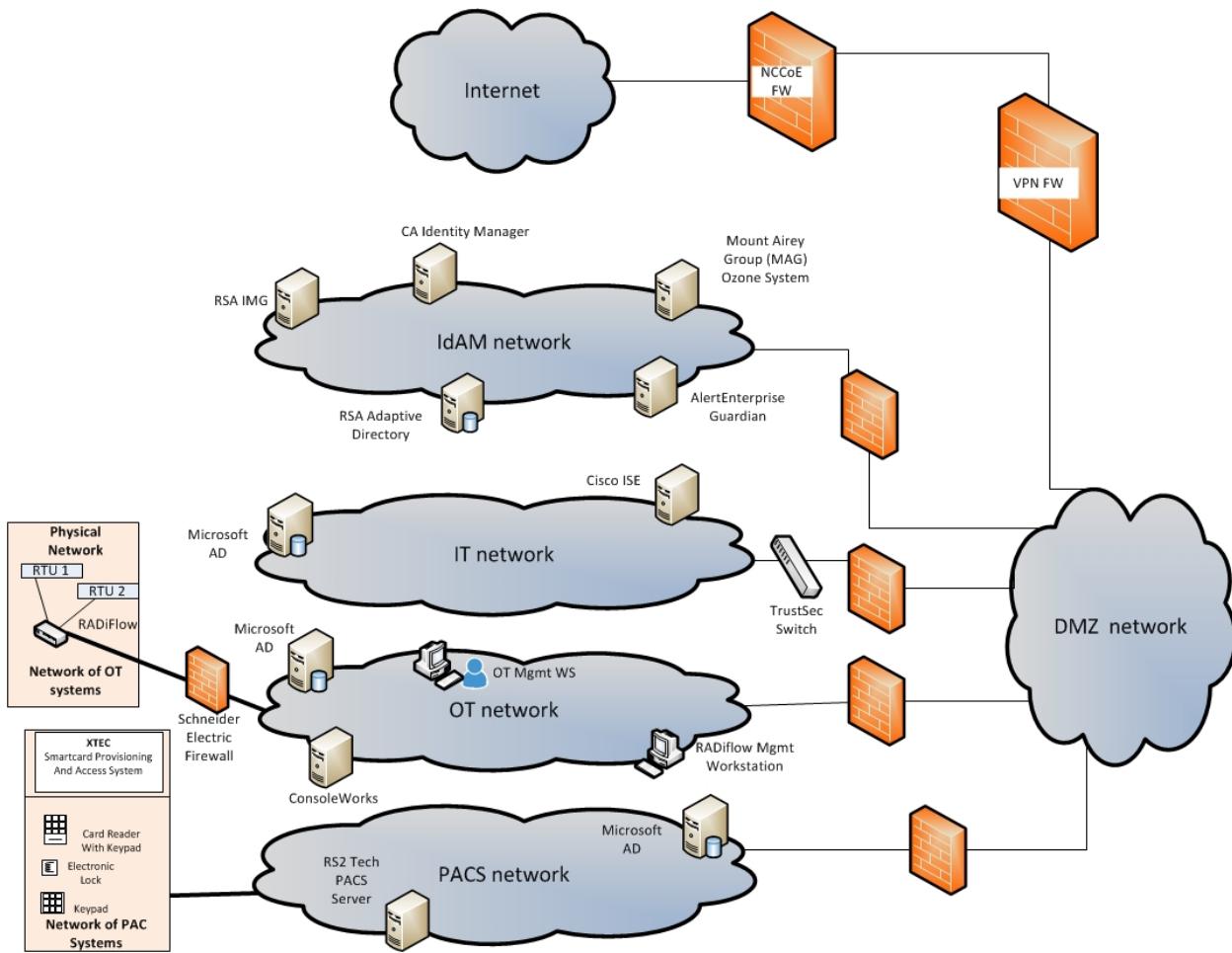


Figure 2. IdAM build implementation production network

100

101

102 The IdAM network represents the proposed centralized/converged IdAM network/system. This
 103 network was separated to highlight the unique IdAM components proposed to address the use
 104 case requirements.

105 The IT network represents the business management network that typically supports corporate
 106 email, file sharing, printing, and Internet access for general business-purpose computing and
 107 communications.

108 The OT network represents the network used to support the energy management systems
 109 (EMS)s and industrial control systems (ICS)/supervisory control and data acquisition (SCADA)
 110 systems. Typically, this network is either not connected to the enterprise IT network or is
 111 connected with a data diode (a one-way communication device from the OT network to the IT
 112 network). Two-way traffic is allowed per NERC-CIP and is enabled via the OT firewall only for
 113 specific ports and protocols between specific systems identified by IP address.

114 The PACS network represents the network used to support the physical access control systems
 115 across the enterprise. Typically, this network uses the enterprise IT network and is segmented

116 from the user networks via virtual local area networks (VLANs). In our architecture, a firewall is
117 configured to allow limited access to and from the PACS network to facilitate the
118 communication of access and authorization information. Technically, this communication
119 consists of user role and responsibility directory updates originating in the IdAM system.

120 The public Internet is accessible by the lab environment to facilitate both cloud services and
121 access for vendors and NCCoE administrators.

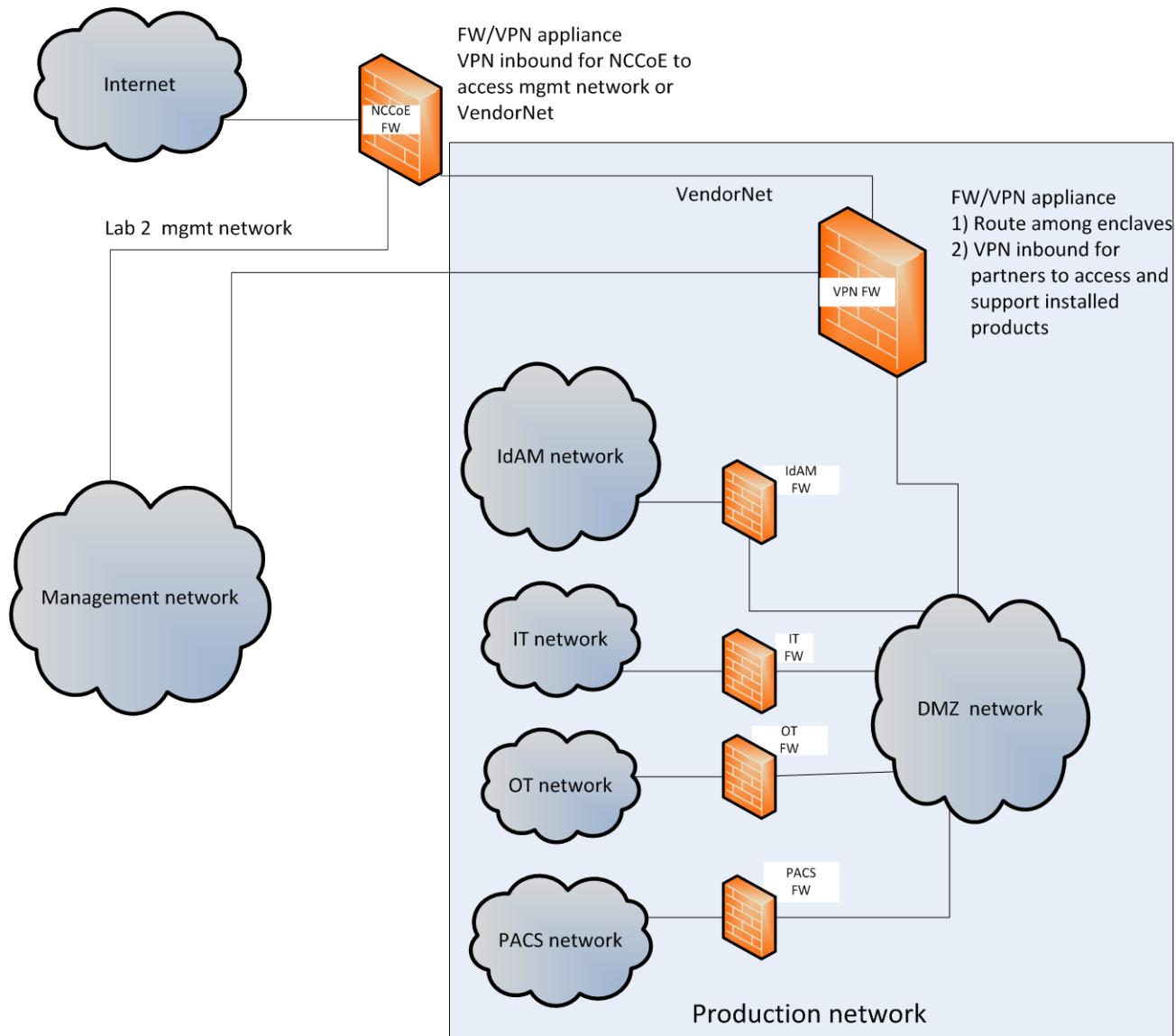
122 The VPN firewall was the access control point for vendors to support the installation and
123 configuration of their components of the architecture. The NCCoE also used this access to
124 facilitate product training. This firewall also blocked unauthorized traffic from the public
125 Internet to the production networks. Additional firewalls are used to secure the multiple
126 domain networks (IT, OT, IdAM, and PACS) explained below.

127 Switching in the implementation is executed using a series of physical and hypervisor soft
128 switches. VLAN switching functions are handled by physical Dell switches and the virtual
129 environment. Routing was accomplished using the firewalls.

130 **2.2 BUILD IMPLEMENTATION DESCRIPTIONS**

131 Figure 3 depicts the build network comprising the management, VendorNet, IdAM, DMZ, IT, OT,
132 and PACS subnetworks. VendorNet provides remote access for vendors to access, configure,
133 demonstrate, and provide training for each of the implemented products. The IdAM network
134 contains the central IdAM components of the build (described below). The IT, OT, and PACS
135 networks contain the representative components of a typical electric utility enterprise, as
136 described below.

137

138
139

140

Figure 3. Build Network

141 The IdAM network (Figure 4 and Figure 5) contains the central IdAM components for Build #1
 142 and Build #2. The IdAM components are placed into a separate network to highlight the
 143 importance of protecting these assets and to simplify the demonstration of their capabilities.

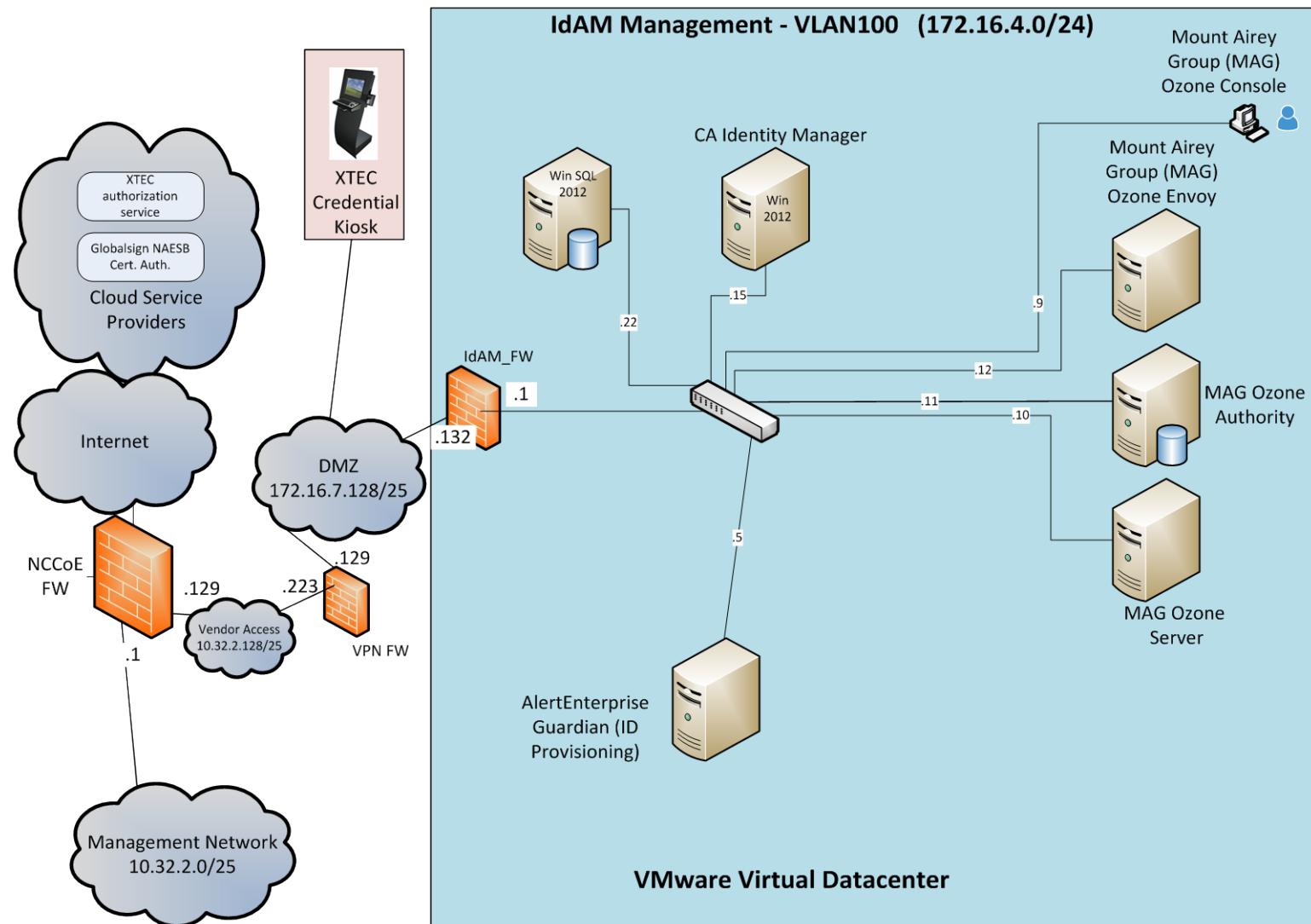
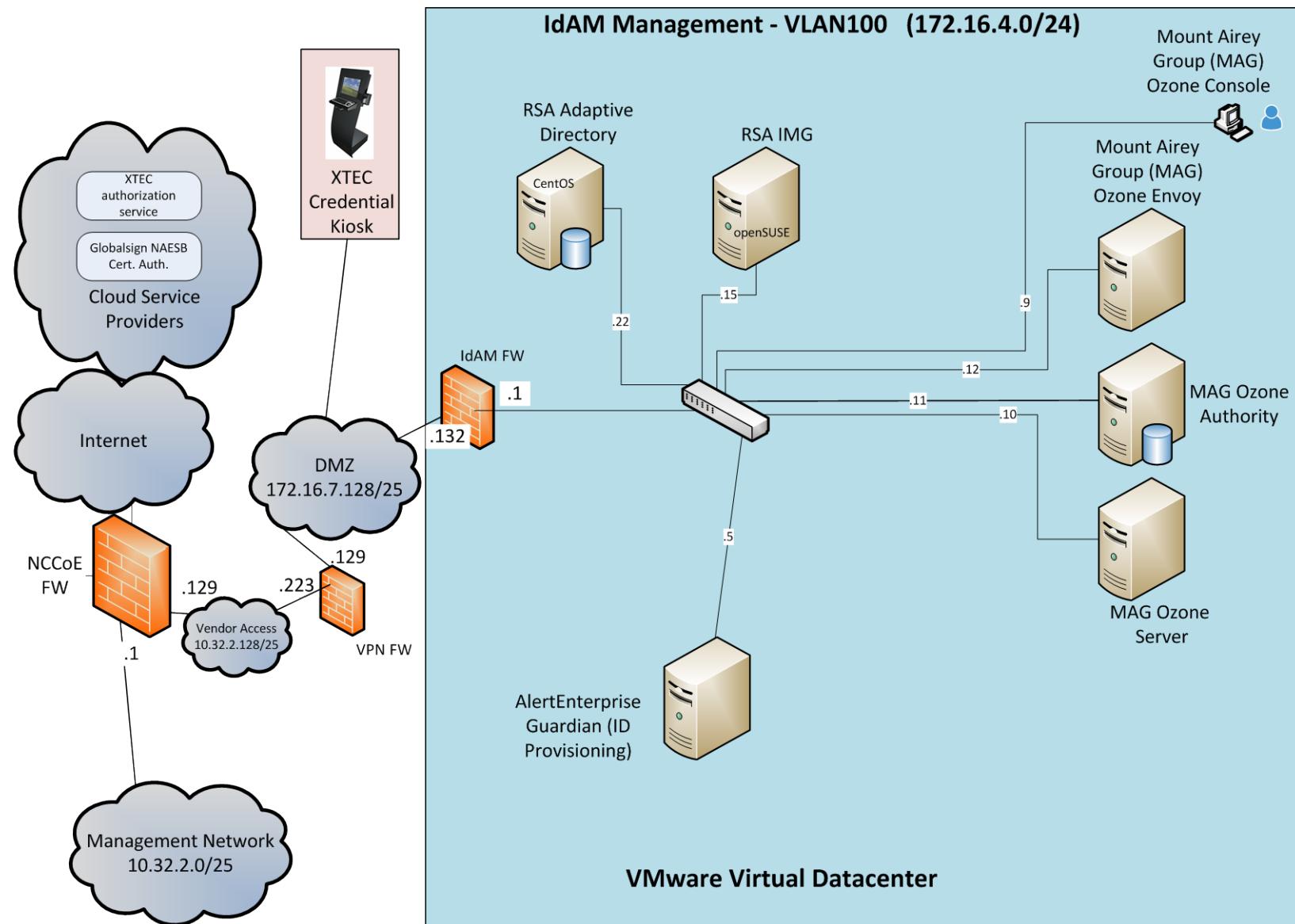


Figure 4. Build #1 IdAM Network

144

145

146 Build #1 uses the CA Identity Manager product for the IdAM system and identity store.



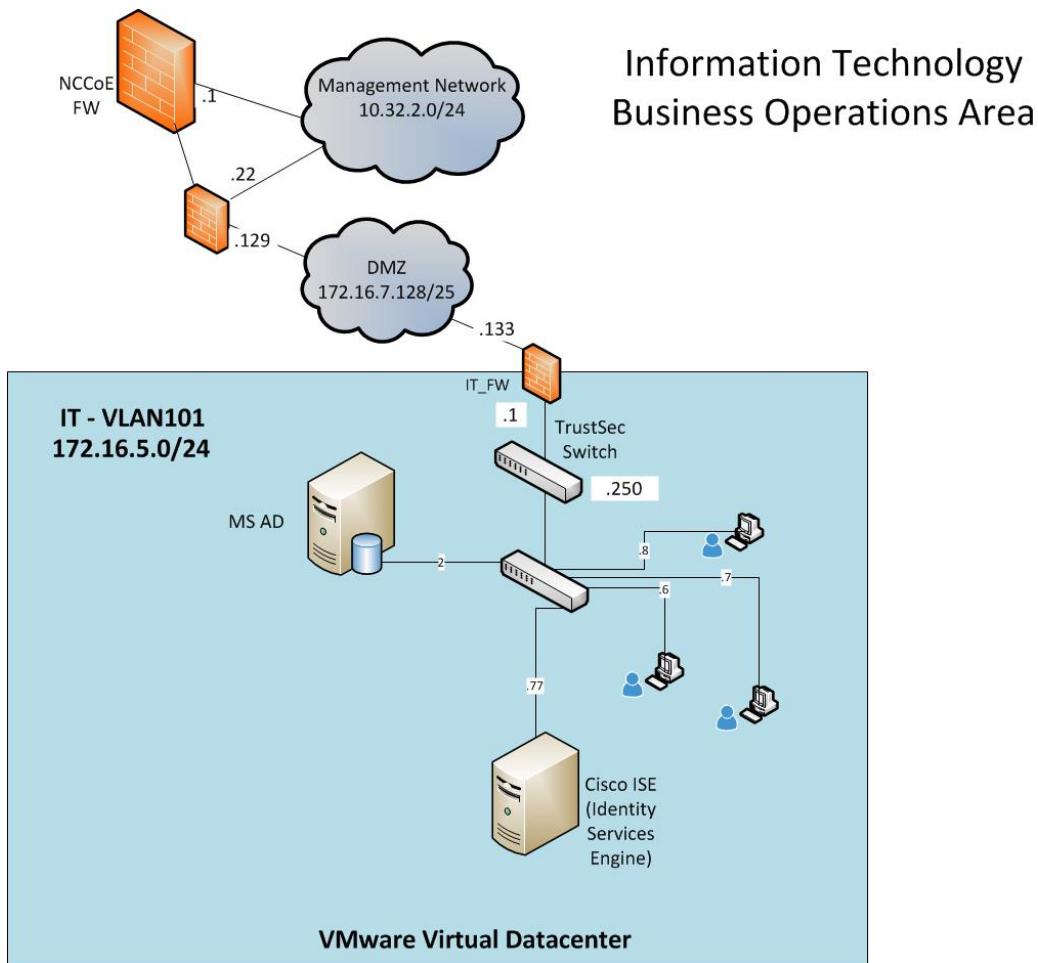
147

148

Figure 5. Build #2 IdAM Network

149 Build #2 uses the RSA IMG and Adaptive Directory products for the IdAM system and identity
 150 store.

151 The IT network (Figure 6) contains the components common in the business operations IT
 152 networks/systems in all organizations.

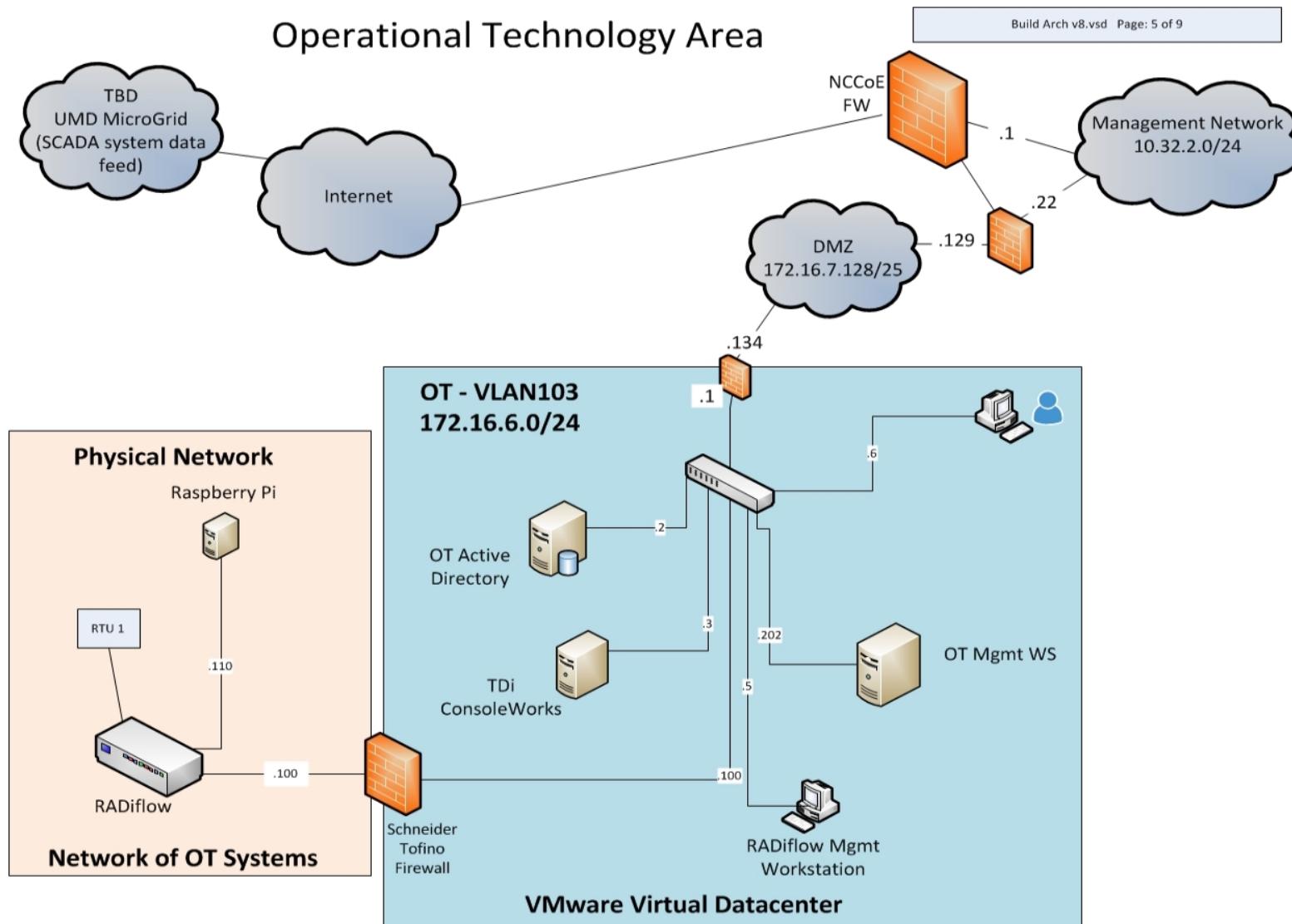


153

Figure 6. IT Network

154

155 The OT network (Figure 7) contains the OT components, which include representative
 156 components found in electric utility OT networks/systems. These components were chosen to
 157 demonstrate the integration capabilities of the central IdAM capability. The lab did not attempt
 158 to replicate a fully operational OT network or set of systems. Because we had a limited number
 159 of remote terminal units (RTUs) available, we used Raspberry Pi on the network to emulate an
 160 RTU.

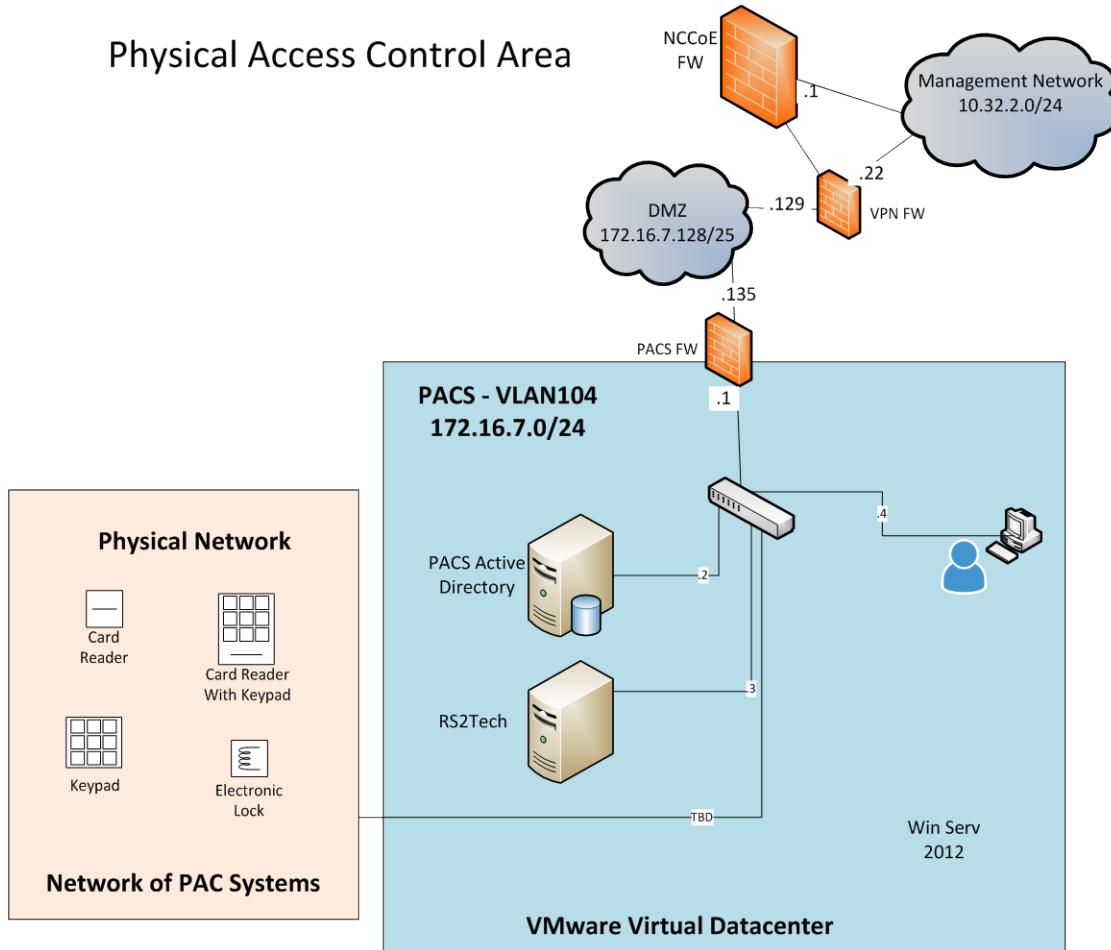


161

162

Figure 7 OT Network

163 The PACS network (Figure 8) contains the PACS components, which include representative
 164 components found in electric utility physical access control systems. These components were
 165 chosen to demonstrate the integration capabilities of the central IdAM capability.



166

167

Figure 8 PACS Network

168 **2.3 IP NETWORK ADDRESS ASSIGNMENTS**

169 Table 2 includes the IP address assignments used for the builds.

170 *Table 2 Build IP Address Assignments*

DMZ Network IP	System	Vendor Access Network	System	IdAM Mgmt IP Network IP	System
10.32.2.0/25	Subnet	10.32.2.128/25	Subnet	172.16.4.0/24	Subnet
10.32.2.1	NCCoE FW/Gateway	10.32.2.129	NCCoE FW/Gateway	172.16.4.1	IdAM FW LAN
10.32.2.10	Vcenter	10.32.2.130	Vendor AD	172.16.4.2	RSA IMG
10.32.2.11	ESXi #1	10.32.2.131	Vendor RDS	172.16.4.3	RSA Adaptive Directory
10.32.2.12	ESXi #2	10.32.2.132	RSA/SCE	172.16.4.5	AlertEnterprise
10.32.2.22	Border FW WAN	10.32.2.133	AlertEnt	172.16.4.9	Ozone Console
10.32.2.50	RS1 FTP Synology	10.32.2.134	CA	172.16.4.10	Ozone Server
10.32.2.X	Veam Backup Server	10.32.2.135	RADiFlow	172.16.4.11	Ozone Authority
		10.32.2.136	MAG	172.16.4.12	Ozone Envoy
		10.32.2.137	TDi	172.16.4.13	Ozone PPA
		10.32.2.232	Border FW OPT1	172.16.4.15	CA IM
				172.16.4.22	Microsoft SQL
				172.16.4.253	CentOS DNS

171

172

173

Table 2. (cont.) Build IP Address Assignments

IT Network IP	System	PAC Network IP	System	OT Network IP	System
172.16.5.0/24	subnet	172.16.7.0/25	Subnet	172.16.6.0/25	Subnet
172.16.5.1	IT FW LAN	172.16.7.1	PACS FW LAN	172.16.6.1	OT FW LAN
172.16.5.2	IT AD, DNS, CA	172.16.7.2	PACS AD, DNS, CA	172.16.6.2	OT AD, DNS, CA
172.16.5.6	Workstation	172.16.7.5	n/a	172.16.6.4	RADiFlow FW/SW
172.16.5.7	Workstation	172.16.7.6	XTEC XNode	172.16.6.5	Schneider Firewall
		172.16.7.11	PACS Console	172.16.6.6	Workstation
		172.16.7.15	PACS Workstation	172.16.6.8	TDi ConsoleWorks
		172.16.7.101	LAB Door Controller	172.16.6.100	RADiFlow Terminal Server for SEL
				172.16.6.202	RADiFlow Vendor Host

174

175 3 BUILD INFRASTRUCTURE

176 3.1 OPERATING SYSTEMS

177 All machines used in the build had one of the following operating systems (OS) installed:

178 • Windows 7 enterprise
 179 • Windows server 2008 R2
 180 • Windows server 2012 R2
 181 • MicroFocus SUSE Linux Enterprise Server 11
 182 • CentOS 7.

183 3.1.1 Windows Installation and Hardening Details

184 The NCCoE Windows OS images are derived from the Department of Defense (DoD) Security
 185 Technical Implementation Guide (STIG) images. The Windows systems were installed using
 186 installation files provided by the Defense Information Systems Agency (DISA). These images
 187 were chosen because they are standardized, hardened, and fully documented. The STIG
 188 guidelines are available on-line at <http://iase.disa.mil/stigs/os/Pages/index.aspx>.

189 Modifications to the STIG compliant OS configurations were required for each product to enable
190 its operation. The compliance results in Section 17 identify the specific OS configuration
191 modifications (noncompliant configuration items) needed in each case.

192 3.1.2 **SUSE Linux Enterprise Server 11 Installation and Hardening Details**

193 The SUSE OS was included as part of the virtual appliance image provided by RSA for the IMG
194 product. The center did not make any OS configuration changes. The OS was not configured to
195 meet the DoD CentOS 6 STIG. The STIG guidelines are available on-line at
196 <http://iase.disa.mil/stigs/os/Pages/index.aspx>. The OS configurations for SUSE Linux
197 implementation are listed in Section 17. The compliance results report for SUSE Linux is
198 included for illustration purposes, Section 20.2.

199 3.1.3 **Base Linux Installation and Hardening Details**

200 The NCCoE base Linux OS used in the build is CentOS 7. This OS is available as an open source
201 image. The OS was configured to meet the DoD CentOS 6 STIG, because no CentOS 7 STIG was
202 available at the time the build was implemented. The STIG guidelines are available on-line at
203 <http://iase.disa.mil/stigs/os/Pages/index.aspx>. The OS configurations for each Linux
204 implementation are listed in section 17. The compliance results reports identify the
205 configuration items that do not conform to the STIG configuration guide.

206 **3.2 FIREWALL CONFIGURATIONS**

207 The firewalls were deployed to minimize the allowed traffic among the silo networks as well as
208 to minimize traffic received from the DMZ and the public Internet. The goal was to limit the
209 cross-network traffic/connections to only those required to support the use case.

210 The following firewall configurations include the rules that were implemented in each of the
211 firewalls for the build implementation. These configurations are provided to enable the reader
212 to reproduce the traffic filtering/blocking that was achieved in the build implementation.

Table 3. Border Firewall Rules

Aliases						
Name	Values	Description				
VirtualInfra	10.32.2.10-12	Virtualization Systems for Build				
VPNserver	172.16.7.253	VPN Server				
WAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	10.32.2.0/25	Any	Any	Any	Allow all management network traffic
Allow	IPv4 – All	10.255.2.0/25	Any	Any	Any	Center VPN to all systems
Allow	IPv4 – TCP	Any	Any	WAN Address	80	Allow access to WebGUI pfSense
Allow	IPv4 – TCP	10.255.2.0/25	Any	172.16.4.8	5176	Center VPN to Consoleworks
Allow	IPv4 – TCP	10.255.2.0/25	Any	172.16.4.8	443	Center VPN to Consoleworks HTTPS
Deny	IPv4 – TCP	Any	Any	WAN Address	Any	Block All access to pfSense
Allow	IPv4 – TCP	Any	Any	172.16.7.110	3389	RDP to Lab-PC on PACS (Backups)

Table 4. Border Firewall Rules (continued)

LAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	172.16.7.135	Any	VirtualInfra	Any	Lab laptop to Virtualization
Deny	IPv4 – All	Any	Any	VirtualInfra	Any	Block all to Virtualization
Deny	IPv4 – TCP	172.16.8.0/24	Any	10.32.2.0/25	Any	Block Vendor VPN from Management
Deny	IPv4 – TCP	10.32.2.128/25	Any	10.32.2.0/25	Any	Block Vendor VPN from Management
Allow	IPv4 – All	LAN Net	Any	Any	Any	Default Allow Any LAN
Allow	IPv6 – All	LAN Net	Any	Any	Any	Default Allow Any LAN
Allow	IPv4 – TCP	172.16.7.128/25	Any	10.32.2.117	3389	RDP to 117
Allow	IPv4 – UDP	172.16.7.128/25	Any	10.32.2.117	3389	RDP to 117
Deny	IPv4 – All	Any	Any	Any	Any	Block IPv4
Deny	IPv6 – All	Any	Any	Any	Any	Block IPv6

Table 5. IdAM Firewall Rules

Aliases						
Name	Values	Description				
AD_DCs_All	172.16.{5,6,7},2	All DCs in Infrastructure				
LinuxSystems	172.16.4.{2,3,8,10,11,12,253}	Used for SSH				
MAG_Linux	172.16.4.{10,11,12}	Systems for MAG				
WAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	10.32.2.0/25	Any	Any	Any	Allow all management network traffic
Allow	IPv4 – All	10.255.2.0/25	Any	Any	Any	Center VPN to all systems
Allow	IPv4 – TCP	172.16.7.133	Any	Any	Any	IT to IdAm
Allow	IPv4 – TCP	Any	Any	LinuxSystems	IMG	Allow SSH to Linux
Allow	IPv4 – All	Any	Any	172.16.4.8	161,162,514,5176	Allow SNMP, Syslog, default to TDi
Allow	IPv4 – All	AD_DCs_All	Any	172.16.4.15	Any	AD DCs to IdAM-CA
Allow	IPv4 – All	172.16.8.50	Any	172.16.4.15,22	Any	CA to CA_srv12, CA_SQL_srv12
Allow	IPv4 – TCP	Any	Any	172.16.4.2	5900-5910	VNC to IMG
Allow	IPv4 – TCP	172.16.7.2	Any	172.16.4.2	Any	PACS AD to IMG
Allow	IPv4 – TCP	172.16.7.2	Any	172.16.4.3	Any	PACS AD to Adaptive Directory
Allow	IPv4 – TCP	10.32.2.0/25	Any	172.16.4.8	517, 6443	MGMT to TDi Consoleworks
LAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	LAN Net	Any	Any	Any	Default Allow Any LAN
Allow	IPv6 – All	LAN Net	Any	Any	Any	Default Allow Any LAN

Table 6. IT Firewall Rules

Aliases

Name	Values	Description
Alert_Enterprise	172.16.4.5	AlertEnterprise
CA	172.16.4.15	CA
CA_RSA_Alert	172.16.4.{2,3,5,15}, 172.16.7.132	CA, RSA, Alert
ConsoleWorks	172.15.4.8	Console Works
IT_Network	172.16.7.132	IT network
LinuxSystems	172.16.5.4	All Linux on IT
Ozone	172.16.4.10-12	Ozone products
RSA	172.16.4.2-3	IMG, Adaptive Dir

WAN Interface

Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	10.32.2.0/25	Any	Any	Any	Allow all management network traffic
Allow	IPv4 – TCP	172.16.7.132	Any	Any	Any	IdAM to IT
Allow	IPv4 – TCP	Any	Any	LinuxSystems	22	Allow SSH to Linux
Allow	IPv4 – All	Any	Any	172.16.5.2	53	Allow DNS
Allow	IPv4 – TCP	IT_Network	Any	172.16.5.4	25443	Alert to IEMAIL
Allow	IPv4 – TCP	ConsoleWorks	Any	LAN net	22,161-162	TDI to IT-Net
Allow	IPv4 – TCP	CA_RSA_Alert	Any	172.16.5.2	389, 636	LDAP/LDAPS to AD

LAN Interface

Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	LAN Net	Any	Any	Any	Default Allow Any LAN
Allow	IPv6 – All	LAN Net	Any	Any	Any	Default Allow Any LAN

219

220

Table 7. OT Firewall Rules

Aliases		
Name	Values	Description

LinuxSystems	172.16.6.7	All Linux on OT
RADiFlow	172.16.6.{4,6,202}	All RADiFlow IPs

WAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	10.32.2.0/25	Any	Any	Any	Allow all management network traffic
Allow	IPv4 – TCP	Any	Any	172.16.6.10	22	SSH to RPi RTU
Allow	IPv4 – TCP	Any	Any	LinuxSystems	22	Allow SSH to Linux
Allow	IPv4 – All	Any	Any	172.16.6.2	53	Allow DNS
Allow	IPv4 – All	172.16.4.8	Any	LAN net	22,161-162	TDI to OT-Net
Allow	IPv4 – TCP	Any	Any	172.16.6.2	389, 636	Any LDAP to AD
Allow	IPv4 – TCP	172.16.4.{2,3,15}	Any	172.16.6.2	Any	AdaptiveDir, IMG, CA IM to AD
Allow	IPv4 – TCP	Any	Any	172.16.6.100	2001-2101	Telnet Access through RADiFlow

LAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	LAN Net	Any	Any	Any	Default Allow Any LAN
Allow	IPv6 – All	LAN Net	Any	Any	Any	Default Allow Any LAN

221

222

Table 8. PACS Firewall Rules

Aliases		
Name	Values	Description
VirtualInfra	10.32.2.10-12	Virtualization Systems for Build

WAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	10.32.2.0/25	Any	Any	Any	Allow all management network traffic
Allow	IPv4 – All	172.16.7.132	Any	172.16.7.{2,11}	Any	IdAM to PACS-Console, PACSDC
Allow	IPv4 – TCP	Any	Any	172.16.7.2	389, 636	Any LDAP to AD
Allow	IPv4 – All	Any	Any	172.16.7.2	53	Allow DNS
Allow	IPv4 – All	172.16.4.8	Any	LAN net	22,161-162	TDI to PACS-Net
Allow	IPv4 – TCP	172.16.4.{2,3,15}	Any	172.16.7.2	Any	AdaptiveDir, IMG, CA IM to AD
Allow	IPv4 – TCP	Any	Any	172.16.7.110	3389	MRDP Nat to LAB Machine PACS

LAN Interface						
Allow/Deny	Protocol	Source	Port	Destination	Port	Description
Allow	IPv4 – All	LAN Net	Any	Any	Any	Default Allow Any LAN
Allow	IPv6 – All	LAN Net	Any	Any	Any	Default Allow Any LAN

225 3.3 NETWORK SERVICES

226 Microsoft Active Directory was used to provide directory services in each silo networks (OT,
227 PACS, IT). Linux CentOS 7 was used to provide DNS services in the IdAM network. Microsoft
228 Windows Server was used to provide certificate authority services in each network.

229 3.3.1 IT Network – Network Services (AD and Certificate Authority) Installation and Configuration Settings

230 3.3.1.1 Active Directory

231 Use these basic domain controller configuration settings:

- Hostname: ITDC
- Domain: ES-IDAM-B1.TEST
- IP: 172.16.5.2

235 Step-by-step instructions:

1. Launch Server Manager.
2. From the dashboard, select Option 2, Add Roles and Features.
3. Select Role-based or Feature-based installation.
4. From the server pool, select the local server named ITDC.
5. Select Active Directory Domain Service and DNS Server.
6. When prompted to add features, select Add Features for each role.
7. Wait for Server Manager to finishes installing,
8. Select Post-Deployment Configuration for Active Directory from the Task menu.
9. After Active Directory Domain Services Configuration Wizard automatically launches.
 - Select Add a New Forest deployment operation.
 - Specify ES-IDAM-B1.TEST root domain, then select Next >.
 - Select Windows Server 2012 R2 for both the Forest Functional Level and the Domain Functional Level,
 - Under Domain Controller Capabilities:
 - Check both DNS server and Global Catalog.
 - Uncheck read-only domain controller.
 - Specify a password for DSRM and select Next >.
 - Continue through the Wizard without modifying any options.
 - Select Install on the next window. After installation, the server automatically reboots.

256 3.3.1.2 Certificate Authority Role

257 • Use these basic certificate authority configuration settings: CA Setup Type:
258 Enterprise CA
259 • CA Type: Root CA
260 • Cryptographic options: RSA 2048 and SHA1
261 • CN: IT-ES-IDAM-B1-IDAM-ITDC
262 • DN suffix: DC=IT-ES-IDAM-B1, DC=TEST

263 Step-by-step instructions:

- 264 1. From the Server Manager dashboard, select Option 2, Add Roles and Features.
- 265 2. Select Role-based or Feature-based installation (this is a single option to choose).
- 266 3. From the server pool, select the local server named OTDC.
- 267 4. Select Active Directory Certificate Services.
- 268 5. When prompted to add features, select Add Features.
- 269 6. When prompted to select roles services, check Certificate Authority.
- 270 7. After the Server Manager finishes installing, select Post-deployment Configuration for
271 Certificate Services from the Task menu.
- 272 8. When prompted to specify setup type, select Enterprise CA.
- 273 9. When prompted to specify CA type, select Root CA.
- 274 10. When prompted to specify private key, select Create a new private key.
- 275 11. When prompted to specify cryptographic options, select RSA with a key length of 2048
276 and select SHA1 for the hash algorithm.
- 277 12. Leave the CN and DN suffix, which should be based on the computers hostname and
278 domain.
- 279 13. Select 5 years for certificate validity period.
- 280 14. Leave the default options for the certificate database and log location.
- 281 15. After configuration is complete, restart the server.

282 3.3.2 OT Network – Network Services (AD, DNS Server, and Certificate Authority) Installation and
283 Configuration Settings

284 3.3.2.1 Active Directory Domain Services and DNS Server

- 285 • Use these basic certificate authority configuration settings: Hostname: OTDC
- 286 • Domain: OT-ES-IDAM-B1.TEST
- 287 • IP: 172.16.6.2

288 Step-by-step instructions:

- 289 1. Launch Server Manager.

290 2. From the dashboard, select Option 2, Add Roles and Features.
291 3. Select Role-based or Feature-based installation.
292 4. From the server pool, select the local server named OTDC.
293 5. Select Active Directory Domain Service and DNS Server.
294 6. When prompted to add features, select Add Features for each role.
295 7. After the Server Manager finishes installing, select Post-deployment Configuration for
296 Active Directory from the Task menu.
297 8. The Active Directory Domain Services Configuration Wizard launches:
298 • For the deployment operation, select Add a New Forest.
299 • For the root domain, specify OT-ES-IDAM-B1.TEST, then select Next >.
300 • For both the Forest Functional Level and the Domain Functional Level, select
301 Windows Server 2012 R2.
302 • Under Domain Controller Capabilities:
303 ○ Check both DNS server and Global Catalog.
304 ○ Uncheck read-only domain controller.
305 ○ Specify a password for DSRM and select Next >.
306 • Continue through the wizard without modifying any options.
307 • On the last page, select Install. After installation, the server automatically
308 reboots.

309 3.3.2.2 Certificate Authority Role

310 • Use these basic certificate authority configuration settings:
311 CA Setup Type: Enterprise CA
312 • CA Type: Root CA
313 • Cryptographic options: RSA 2048 and SHA1
314 • CN: OT-ES-IDAM-B1-IDAM-OTDC
315 • DN suffix: DC=OT-ES-IDAM-B1, DC=TEST

316 Step-by-step instructions:

317 1. Ensure the domain controller installation has been completed before proceeding.
318 2. From the Server Manager dashboard, select Option 2, Add Roles and Features.
319 3. Select Role-based or Feature-based installation (this is a single option to choose)
320 4. From the server pool, select the local server named OTDC.
321 5. Select Active Directory Certificate Services.
322 6. When prompted to add features, select Add Features.

323 7. When prompted to select roles services, check Certificate Authority.
324 8. After the Server Manager finishes installing, select Post-deployment Configuration for
325 Certificate Services from the Task menu.
326 9. When prompted to specify setup type, select Enterprise CA.
327 10. When prompted to specify CA type, select Root CA.
328 11. When prompted to specify a private key, select Create a new private key.
329 12. When prompted to specify cryptographic options, select RSA with a key length of 2048
330 and select SHA1 for the hash algorithm.
331 13. Leave the CN and DN suffix, which should be based on the computer's hostname and
332 domain.
333 14. Select 5 years for certificate validity period.
334 15. Leave the default options for the certificate database and log location.
335 16. After configuration is complete, restart the server.

336 3.3.3 [PACS Network – Network Services: AD, DNS Server, and Certificate Authority Installation and Configuration Setting](#)

338 3.3.3.1 Active Directory Domain Services and DNS Server

339 Use these basic domain controller configuration settings:

- 340 • Hostname: PACSDC
- 341 • Domain: PACS-ES-IDAM-B1.TEST
- 342 • IP: 172.16.7.2

343 Step-by-step instructions:

- 344 1. Launch Server Manager.
- 345 2. From the dashboard, select Option 2, Add Roles and Features.
- 346 3. Select Role-based or Feature-based installation (this is a single option to choose).
- 347 4. From the server pools, select the local server named PACSDC.
- 348 5. Select Active Directory Domain Service and DNS Server.
- 349 6. When prompted to add features, select Add Features for each role.
- 350 7. After the Server Manager finishes installing, select Post-deployment Configuration for
351 Active Directory from the Task menu.
- 352 8. The Active Directory Domain Services Configuration Wizard launches:
 - 353 • Select Add a new forest for the deployment operation. Specify PACS-ES-IDAM-B1.TEST for the root domain, then select Next.

355 • Select Windows Server 2012 R2 for both the forest functional level and the
356 domain functional level.

357 • Under domain controller capabilities:

358 ○ Check both DNS server and Global Catalog.

359 ○ Uncheck read-only domain controller.

360 ○ Specify a password for DSRM and select Next >.

361 • Continue through the Wizard without modifying any options.

362 • On the last page, select Install. After installation, the server automatically
363 reboots.

364 3.3.3.2 Installation of Certificate Authority Role on the PACS network

365 Use these basic domain controller configuration settings:

- 366 • CA Setup Type: Enterprise CA
- 367 • CA Type: Root CA
- 368 • Cryptographic options: RSA 2048 and SHA1
- 369 • CN: PACS-ES-IDAM-B1-IDAM-PACSDC
- 370 • DN suffix: DC=PACS-ES-IDAM-B1, DC=TEST

371 Step-by-step instructions:

- 372 1. From the Server Manager dashboard, select the Option 2, Add Roles and Features.
- 373 2. Select Role-based or Feature-based installation.
- 374 3. From the server pools, select the local server named OTDC.
- 375 4. Select Active Directory Certificate Services.
- 376 5. When prompted to add features, select Add Features.
- 377 6. When prompted to select roles services, check Certificate Authority.
- 378 7. After the Server Manager finishes installing, select Post-deployment Configuration for
379 Certificate Services from the Task menu.
- 380 8. When prompted to specify setup type, select Enterprise CA.
- 381 9. When prompted to specify CA type, select Root CA.
- 382 10. When prompted to specify private key, select Create a new private key.
- 383 11. When prompted to specify cryptographic options, select RSA with a key length of 2048
384 and select SHA1 for the hash algorithm.
- 385 12. Leave the CN and DN suffix, which should be based on the computer's hostname and
386 domain.
- 387 13. Select 5 years for certificate validity period.

388 14. Leave the default options for the certificate database and log location.

389 15. After configuration is complete, restart the server.

390 3.3.3.3 Modify the AD Lightweight Directory Access Protocol (LDAP) schema with custom PACS
391 attributes.

392 Custom attribute details:

393 • Common Name: pacsAllDoors

394 • X.500 OID: 1.3.6.1.4.1.4203.666.1

395 • Syntax: Boolean

396 • Common Name: pacsHomeAccess

397 • X.500 OID: 1.3.6.1.4.1.4203.666.2

398 • Syntax: Boolean

399 • Common Name: pacsWorkAccess

400 • X.500 OID: 1.3.6.1.4.1.4203.666.3

401 • Syntax: Boolean

402 Step-by-step instructions:

403 1. Launch Command Prompt as an administrator.

404 2. Run the command: `regsvr32 schmgmt.dll`

405 3. Launch the Microsoft Management Console.

406 4. Select File > Add/Remove Snap-in.

407 5. From the Snap-in menu, select Active Directory Schema, then select OK.

408 6. Expand the Active Directory Schema, then select Attributes.

409 7. To create an attribute for the all doors access level, right-click on Attributes, then select
410 Create Attribute.

411 8. Select OK when prompted with the Schema Object Creation Warning.

412 9. Enter the following fields:

413 • Common Name: pacsAllDoors

414 • LDAP Display Name: pacsAllDoors

415 • Unique X500 Object ID: 1.3.6.1.4.1.4203.666.1

416 • Syntax: Boolean

417 10. Select OK when finished.

418 11. Create an attribute for the home access level by entering the following fields:

419 • Common Name: pacsHomeAccess

420 • LDAP Display Name: pacsHomeAccess

421 • Unique X500 Object ID: 1.3.6.1.4.1.4203.666.2

422 • Syntax: Boolean

423 12. Create an attribute for the work access level by entering the following fields:

424 • Common Name: pacsWorkAccess

425 • LDAP Display Name: pacsWorkAccess

426 • Unique X500 Object ID: 1.3.6.1.4.1.4203.666.3

427 • Syntax: Boolean

428 13. After creating custom attributes, add the attributes to the user class so that every user

429 contains the attribute:

430 • Select the Classes drop-down under Active Directory Schema.

431 • Right-click on User, then select Properties.

432 • Select the Attributes tab, then select Add.

433 • Select the attribute you want to add to the user class. Then select OK. Do this for

434 the pacsAllDoors, pacsHomeAccess and pacsWorkAccess attributes.

435 • Then select Apply and OK.

436 • Restart the server.

437 3.3.4 [IdAM Network – Network Services \(DNS Server\) Installation and Configuration Settings](#)

438 A Linux CentOS 7 DNS server was established on the IdAM network to provide DNS services to

439 the IdAM components. No other network service was installed in the IdAM network.

440 System Environment Settings

441 • CentOS 7

442 • VM with 4 CPU Quad Core 2.199GHz.

443 • VM with 16384MB of memory.

444 • Virtual Hard Disk containing 98GB of storage.

445 Linux CentOS DNS Configuration

446 Basic DNS configuration settings are specified using three different system files that are located

447 in the /etc and /var subdirectories of the root directory as follows.

448 3.3.4.1 System file 1 – named.conf in the /etc subdirectory

449 //

450 // named.conf

451 //

```
452      // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
453      // server as a caching only nameserver (as a localhost DNS resolver only).
454      //
455      // See /usr/share/doc/bind*/sample/ for example named configuration files.
456      //
457
458      options {
459          listen-on port 53 { 127.0.0.1; 172.16.4.253; };
460          #listen-on-v6 port 53 { ::1; };
461          #listen-on-v6 { none; };
462          directory      "/var/named";
463          forwarders    { 8.8.8.8; 8.8.4.4; };
464          dump-file     "/var/named/data/cache_dump.db";
465          statistics-file "/var/named/data/named_stats.txt";
466          memstatistics-file "/var/named/data/named_mem_stats.txt";
467          allow-query   { localhost; 172.16.4.0/22; };
468          allow-transfer { localhost; 172.16.4.0/22; };
469
470          /*
471          - If you are building an AUTHORITATIVE DNS server, do NOT enable
472            recursion.
473          - If you are building a RECURSIVE (caching) DNS server, you need to
474            enable
475            recursion.
476            - If your recursive DNS server has a public IP address, you MUST enable
477              access
478              control to limit queries to your legitimate users. Failing to do so will
479              cause your server to become part of large scale DNS amplification
480              attacks. Implementing BCP38 within your network would greatly
481              reduce such attack surface
482          */
483          recursion yes;
484
485          dnssec-enable yes;
```

```
486         dnssec-validation yes;
487         dnssec-lookaside auto;
488
489         /* Path to ISC DLV key */
490         bindkeys-file "/etc/named.iscdlv.key";
491
492         managed-keys-directory "/var/named/dynamic";
493
494         pid-file "/run/named/named.pid";
495         session-keyfile "/run/named/session.key";
496     };
497
498     logging {
499         channel default_debug {
500             file "data/named.run";
501             severity dynamic;
502         };
503     };
504
505     zone "." IN {
506         type hint;
507         file "named.ca";
508     };
509
510     zone "idam-es-idam-b1.test" IN {
511         type master;
512         file "idam-es-idam-b1.test";
513         allow-update { none; } ;
514     };
515
516     zone "4.16.172.in-addr.arpa" IN {
517         type master;
518         file "4.16.172.db";
519         allow-update { none; };
```

```
519         };
520
521         zone "ot-es-idam-b1.test" IN {
522             type slave;
523             masters {
524                 172.16.6.2;
525             };
526             forwarders {};
527         };
528
529         zone "pacs-es-idam-b1.test" IN {
530             type slave;
531             masters {
532                 172.16.7.2;
533             };
534             forwarders {};
535         };
536
537         zone "es-idam-b1.test" IN {
538             type slave;
539             masters {
540                 172.16.5.2;
541             };
542             forwarders {};
543         };
544
545
546         include "/etc/named.rfc1912.zones";
547         include "/etc/named.root.key";
548 3.3.4.2 System file 2 – 4.16.172.db in the /var subdirectory
549         $TTL 86400
550         @ IN SOA idam-dns.idam-es-idam-b1.test.      root.idam-es-idam-b1.test. (
551                         2011071001      ;Serial
```

```
552          3600  ;Refresh
553          1800  ;Retry
554          604800 ;Expire
555          86400 ;Minimum TTL
556      )
557      @  IN  NS  idam-dns.idam-es-idam-b1.test.
558      @  IN  PTR  idam-es-idam-b1.test.
559      idam-dns  IN  A  172.16.4.253
560
561
562      101  IN  PTR  idam-dns.idam-es-idam-b1.test.
563      System file – idam-es-idam-b1.test in the /etc subdirectory
564
565      $TTL 86400
566      @  IN  SOA  idam-dns.idam-es-idam-b1.test.  root.idam-es-idam-b1.test. (
567          2011071001  ;Serial
568          3600  ;Refresh
569          1800  ;Retry
570          604800 ;Expire
571          86400 ;Minimum TTL
572      )
573
574      @  IN  NS  idam-dns.idam-es-idam-b1.test.
575      @  IN  A  172.16.4.253
576      idam-dns  IN  A  172.16.4.253
577      idam-ca  IN  A  172.16.4.15
578      idam-sql  IN  A  172.16.4.22
579      adaptivedir  IN  A  172.16.4.3
580      img  IN  A  172.16.4.2
581      consoleworks  IN  A  172.16.4.8
582      ozoneserver  IN  A  172.16.4.10
583      ozoneenvoy  IN  A  172.16.4.12
584      ozoneauthority  IN  A  172.16.4.11
585      alertentIN  IN  A  172.16.4.5
586      WIN-IPERGL2ELUD  IN  A  172.16.4.5
```

587 **4 REMOTE TERMINAL UNITS (RTUs)**

588 Remote terminal units (RTU) provide the cyberspace to physical interface. Remote terminal
589 units are used to collect data such as voltage, current and phase from substation equipment.
590 They are also used to deliver commands via contact closures or output voltage to change device
591 operations such as switches, circuit breakers or capacitors.

592 **4.1 TCP/IP RTU**

593 The TCP/IP RTU in this build is emulated with a RaspberryPi 2 system. The system was
594 developed to simulate a Modbus protocol programmable logic controller (PLC).

595 **4.2 SERIAL RTU**

596 The serial RTU in this build is a Schweitzer Engineering Laboratory SEL-2411 programmable
597 automation controller configured to support the Modbus protocol. It is connected to the
598 RADiFlow ICS Firewall via serial interface.

599 **5 IDENTITY SERVICES ENGINE (ISE) AND TRUSTSEC ENABLED SWITCH: CISCO**

600 Cisco Identity Services Engine (ISE) controls the ability of devices to connect over the network.
601 ISE expands on basic network address-based control to include the identity of the person using
602 a device. ISE is used in the builds to provide a gateway function between IT and OT, limiting
603 which users and devices are allowed to connect from IT to resources in OT.

604 The Cisco ISE component should be installed in a virtual machine (VM) on the IT network. This
605 ISE component will be used in conjunction with the TrustSec switch that is located on the IT
606 network to control access from the IT network to the OT network.

607 **5.1 SECURITY CHARACTERISTICS**

608 Cybersecurity Framework Category: PR.PT-3: Access to systems and assets is controlled,
609 incorporating the principle of least functionality

610 NIST 800-53 rev 4 Security Controls: AC-3, CM-7

611 **5.2 PRE-INSTALLATION TASK**

612

1. Obtain OVA file from Cisco for Cisco ISE 1.4.
2. Place OVA file in Datastore for vSphere installation.
3. Ensure that the user domain has a security group (the build used *OTAccess*) for
determining access to the OT network.

616 **5.3 INSTALL AND CONFIGURE**

617 1. Follow the guide located at: http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/installation_guide/b_ise_InstallationGuide14/b_ise_InstallationGuide14_chapter_010_0.html

620 ● This is the Cisco Identity Services Engine Hardware Installation Guide, Release
621 1.4, section on Installing ISE on a VMware Virtual Machine.

622 ● To deploy the OVA file, follow the instructions at the heading “Installing Cisco ISE
623 on Virtual Machines.”

624 ● After OVA is deployed, follow instructions at heading “Installing Cisco ISE
625 Software on a VMware System.”

626 2. After the system is installed, type `setup` at the prompt.

627 3. The following are prompts and build responses:

628 ● Enter hostname: `ise`

629 ● Enter IP address[]: `172.16.4.77`

630 ● Enter IP netmask[]: `255.255.255.0`

631 ● Enter IP default gateway[]: `172.16.4.1`

632 ● Enter default DNS domain[]: `idam-es-idam-b1.test`

633 ● Enter primary nameserver[]: `172.16.4.253`

634 ● Add secondary nameserver? `Y/N[N]: <blank>`

635 ● Enter NTP server[`time.nist.gov`]: `172.16.4.1`

636 ● Add another NTP server? `Y/N[N]: <blank>`

637 ● Enter system time zone[`UTC`]: `EST`

638 ● Enable SSH service? `Y/N [N]: Y`

639 ● Enter username [`admin`]: `admin`

640 ● Enter password: `<password>`

641 ● Enter password again: `<password>`

642 4. After ISE finishes the installation, connect to ISE through the web browser using the IP
643 address specified during the setup phase.

644 5. Begin the Setup Assistant.

645 6. Select Wired for setup access services, and select the Enforce radio button. For subnets
646 to protect, type the target network (in build, the OT network: `172.16.6.0/24`). Press
647 Next.

648 7. Uncheck Cisco Unified IP Phone box
649 Select AD group : `es-idam-b1.test/Builtin/Users`
650 Leave the default checked boxes as is.

651 8. Select Yes for authenticate users using Cisco ISE, select Join the Active Directory domain,
652 and add domain credentials (in build, we used `es-idam-b1.test` for domain and the
653 domain admin credentials to connect). Fill in the Employee Switched VLAN Interface box
654 with: `172.16.5.0 /24`. Press Next.

655 9. Select switch (build used Cisco Catalyst 3560 Series Switches), fill in pertinent
656 information for switch. For Employee VLAN ID, build used 104. Select a RADIUS Shared
657 Secret (build used password). Press Next.
658 10. Confirm all settings are correct, then select Confirm Configuration Settings.

659 TrustSec switch configuration information: Taken from the Network Device Configuration tab in
660 the Setup Assistant Review section, the recommended configurations to be set globally on the
661 TrustSec-enabled switch are as follows:

```
662 aaa new-model
663 !
664 aaa authentication dot1x default group radius
665 aaa authorization network default group radius
666 aaa authorization auth-proxy default group radius
667 aaa accounting delay-start all
668 aaa accounting auth-proxy default start-stop group radius
669 aaa accounting dot1x default start-stop group radius
670 aaa accounting network default start-stop group radius
671 aaa server radius dynamic-author
672     client 172.16.4.77 server-key 7 15020A1F173D24362C
673 !
674 aaa session-id common
675 switch 1 provision ws-c3650-48ps
676 authentication mac-move permit
677 ip routing
678 !
679 ip device tracking
680 ip dhcp snooping vlan 102
681 no ip dhcp snooping information option
682 ip dhcp snooping
683 dot1x system-auth-control
684 !
685 diagnostic bootup level minimal
686 spanning-tree mode pvst
687 spanning-tree extend system-id
688 !
689 redundancy
690     mode sso
691 !
692 !
693 ip ssh version 2
694 !
```

```
695 class-map match-any non-client-nrt-class
696   match non-client-nrt
697 !
698 policy-map port_child_policy
699   class non-client-nrt-class
700     bandwidth remaining ratio 10
701     snmp trap mac-notification change added
702     spanning-tree portfast
703 !
704 ip access-list extended ACL-DEFAULT
705   remark Allow DHCP
706   permit udp any eq bootpc any eq bootps
707   remark Allow DNS
708   permit udp any any eq domain
709   permit icmp any any
710   permit tcp any host 172.16.4.77 eq 8443
711   permit tcp any host 172.16.4.77 eq 443
712   permit tcp any host 172.16.4.77 eq www
713   permit tcp any host 172.16.4.77 eq 8905
714   permit tcp any host 172.16.4.77 eq 8909
715   permit udp any host 172.16.4.77 eq 8905
716   permit udp any host 172.16.4.77 eq 8909
717   deny ip any any
718 ip access-list extended ACL-WEBAUTH-REDIRECT
719   permit tcp any any eq www
720   permit tcp any any eq 443
721   deny ip any any
722 !
723 logging origin-id ip
724 logging source-interface GigabitEthernet1/0/48
725 !
726 radius-server attribute 6 on-for-login-auth
727 radius-server attribute 6 support-multiple
728 radius-server attribute 8 include-in-access-req
729 radius-server dead-criteria time 5 tries 3
730 radius-server host 172.16.4.77 auth-port 1812 acct-port 1813 key 7
731 140713181F13253920
732 !
733 radius server host
734 !
735 wsma agent exec
736   profile httplistener
```

```
737 profile httpslistener
738 wsma agent config
739 profile httplistener
740 profile httpslistener
741 wsma agent filesys
742 profile httplistener
743 profile httpslistener
744 wsma agent notify
745 profile httplistener
746 profile httpslistener
747 !
748 wsma profile listener httplistener
749 transport http
750 !
751 wsma profile listener httpslistener
752 transport https
753 ap group default-group
754 end
755
```

756 For each interface that is to be controlled, the recommended configurations are as follows:

```
757 interface GigabitEthernet1/0/10
758 switchport access vlan 101
759 switchport mode access
760 switchport block unicast
761 switchport voice vlan 105
762 ip arp inspection limit rate 2000
763 ip access-group ACL-DEFAULT in
764 authentication event fail action next-method
765 authentication event server dead action authorize vlan 101
766 authentication event server alive action reinitialize
767 authentication host-mode multi-auth
768 authentication open
769 authentication order dot1x mab
770 authentication priority dot1x mab
771 authentication port-control auto
772 authentication periodic
773 authentication timer reauthenticate server
774 authentication timer inactivity 180
775 authentication violation restrict
776 mab
```

```
777 dot1x pae authenticator
778 dot1x timeout tx-period 10
779 spanning-tree portfast
780 spanning-tree bpduguard enable
781 ip dhcp snooping limit rate 2048
782
783 11. Go to the top tabs and click Administration > System > Deployment. (If a warning that
784 says “This node is standby mode. To register other...Role to Primary” click OK.) Under
785 the Deployment Nodes – Hostnames click on the ise link. Then click Profiling
786 Configuration, and ensure that Netflow, Radius, DNS, SNMPQUERY, and SNMPTRAP are
787 selected. If they are not selected, select them. Then click Save.
788 12. Select Administration > Identity Management > External Identity Sources. In the frame
789 on the left choose Active Directory, then choose ise.idam-es-idam-b1.test. Click
790 Connections tab, select the checkbox next to the domain es-idam-b1.test. Check
791 to see if there is a green check in the Status column. If yes click Save.
792 If not, Click Join, and type in the AD Credentials and click Save. A green check
793 should appear in the Status column.
794 13. Select Administration > Identity Management > External Identity Sources > Groups tab.
795 Click Add > Select Group From Directory. Click retrieve groups. Check the es-idam-
796 b1.test/Users/Domain Users box and the es-idam-b1.test/Builtin/Users box and the es-
797 idam-b1.test/Users/OTAccess box. These items are specified for protected access (the
798 build used OTAccess). Then Click OK. Then click Save. Relogin as directed.
799 14. Select Administration > System > Settings. Click on Policy Sets in the frame at the left of
800 the screen, and click enabled (if it is not already clicked). Click Save if needed.
801 15. Select Policy > Policy Elements > Results. In the frame at the left of the screen, left
802 column, click Authorization, then Downloadable ACL List. Create the following (all IP
803 addresses are pertinent to the current build.; these addresses will need to be replaced
804 with IP addressing that is appropriate to the target environment):
805     o All_But_OT-Access-DACL
806         ▪ Name: All_But_OT-Access-DACL
807         ▪ DACL Content:
808             deny ip any 172.16.6.0 0.0.0.255
809             permit ip any any
810     Click Save
811 16. In the left column, select Authorization Profiles and click Add to create the
812 following:
813     o All_and_OT
814         ▪ Name: All_and_OT
815         ▪ Access Type: ACCESS_ACCEPT
816         ▪ Check DACL Name: PERMIT_ALL_TRAFFIC
817     Click Submit
```

818 ○ All_But_OT_Access
819 ■ Name: All_But_OT_Access
820 ■ Access Type: ACCESS_ACCEPT
821 ■ Check DACL Name: All_But_OT-Access-DACL
822 Click Submit
823 ○ DenyAccess
824 ■ Name: DenyAccess
825 ■ Access Type: ACCESS_REJECT
826 Click Submit
827 17. Select Policy > Policy Elements > Conditions. In the left column, select Authorization,
828 then Simple Conditions. Click Add to create the following:
829 ○ NotOTAccess
830 ■ Name: NotOTAccess
831 ■ Attribute: Select the domain (build uses es-idam-b1.test) >
832 ExternalGroups
833 ■ Operator: Not Equals
834 ■ Value: Select the Security Group (build uses es-idam-
835 b1.test/Users/OTAccess)
836 Click Submit
837 ○ IT_DomainUsers
838 ■ Name: IT_DomainUsers
839 ■ Attribute: Select the domain (build uses es-idam-b1.test) >
840 ExternalGroups
841 ■ Operator: Equals
842 ■ Value: Select domain users group (build uses es-idam-
843 b1.test/Users/Domain Users)
844 Click Submit
845 18. Select Policy > Policy Sets. Select Default and configure policies. Choose the arrow next
846 to Authorization to expand the section. Choose the top rule and click the option arrow
847 to the right of the Edit link within the policy. Click New rule above.
848 ○ Rule 1: Click the plus sign in the Conditions box. Select Create New Condition
849 (Advanced Option). Select Attribute > es.idam-b1.test > External Groups. Leave
850 equals Select Attributes > es-idam-b1.test/Users/OTAccess. Click the plus sign in
851 the Permissions box. Select item drop down choose Standard > All_and_OT. Click
852 Done button on right.
853 Click the arrow to the right of the Edit link within the top policy (new policy
854 created above) Click Insert Below.
855 ○ Rule 2: Click the plus sign in the Conditions box. Select Existing Condition from
856 Library. Select arrow to choose simple conditions > NotOTAccess. Select arrow
857 next to the gear icon (on right). Select Add Condition from Library. Select Arrow

858 to choose Simple conditions > IT_DomainUsers. Click on the Permissions input
859 box. Click the plus sign in the Permissions box. Click the arrow and choose
860 standard > All_But_OT_Access. Click Done. Click Save.

861 **6 IDENTITY MANAGER: CA TECHNOLOGIES (CA) INSTALLATION – BUILD #1**

862 CA Identity Manager implements the central IdAM workflow in Build #1. It receives input from
863 an HR system in the form of .csv files. The access and authorization for each user is based on the
864 business and security rules implemented in workflows within Identity Manager. The workflows
865 include management approval chains as well as approval/denial data logging. Once Identity
866 Manager has processed the access and authority request, the updated user access and
867 authorization data is pushed to the central ID store. The central ID store contains the
868 distribution mechanism for updating the various downstream (synchronized) directories with
869 user access and authorization data. This process applies to new users, terminated users
870 (disabled or deleted users), and any changes to a user profile. Changes include promotions, job
871 responsibility changes, and any other change that would affect the systems a user needs to
872 access.

873 **6.1 SECURITY CHARACTERISTICS**

874 Cybersecurity Framework Categories:

875 • PR.AC-1: Identities and credentials are managed for authorized devices and users
876 • PR.AC-4: Access permissions are managed, incorporating the principles of least privilege
877 and separation of duties

878 NIST 800-53 rev 4 Security Controls: AC-2, AC-3, AC-5, AC-6, AC-16, IA Family

879 **CA Identity Manager is installed on the IdAM network on a VM running the Windows Server**
880 **2012 R2 OS.**

881 **Important:** The following instructions are for a single server demo environment and are not
882 intended to be used for a production deployment.

883 This guide walks you through a basic installation of CA Identity Manager on JBoss, on a single
884 Windows server. For comprehensive instructions for installing CA Identity Manager, refer to the
885 CA Identity Manager Installation Guide for JBoss at <https://support.ca.com>.

886 **6.2 INSTALLATION PREREQUISITES**

887 The following steps are required prior to the CA Identity Manager installation. (For supported
888 versions of all software, review the CA Identity Manager Support Matrix at
889 <https://support.ca.com>.)

890 1. Use a server with a supported OS (e.g., Windows 2012 R2).
891 2. Install a supported version of the JDK. (e.g., 1.7.0_71).

892 3. Install a supported version of JBoss. (e.g., jboss-eap-6.3).
893 4. To install JBoss as a Windows service, follow the instructions at the following link:
894 https://access.redhat.com/documentation/en-US/JBoss_Enterprise_Application_Platform/6.3/html/Installation_Guide/Install_JBoss_Enterprise_Application_Platform_6_Microsoft_Windows_Service.html
895 5. Create a Database and associated user with DBA permissions on a supported database
896 (e.g., MSSQL 2012).
897 6. Download and unzip CA Identity Manager software from <https://support.ca.com>.

900 **6.3 INSTALL CA DIRECTORY**

901 1. From the unzipped location, go to *CADirectory_x64\dxserver\windows* and execute
902 *dxsetup.exe*.
903 2. Select Typical installation.
904 3. Uncheck “DXmanager will manage...”
905 4. Accept all other defaults.

906 **6.4 INSTALL CA IDENTITY MANAGER**

907 1. From the unzipped location, execute *ca-im-12.6.XX-win32.exe*
908 2. Select Components: deselect “Connect to Existing SiteMinder Policy Server” and
909 “Extensions for Siteminder...”. Leave the rest of the checkboxes checked.
910 3. Deployment Size: compact
911 4. Provisioning Server Hostnames: Just click Next
912 5. Provisioning Directory Information: enter a shared secret and confirmation.
913 6. Destination Location: accept default
914 7. FIPS Information: accept default
915 8. Application Server Information: JBoss
916 9. JBoss Application Server Information: Choose and locate the folder where JBoss is
917 installed. Enter the fully qualified URL and Port for JBoss. Leave the Cluster fields blank.
918 10. Select Java Virtual Machine: Click “Search for Others”. Select *jdk1.7.0_71\bin\java.exe*.
919 11. Key Encryption Information: accept default
920 12. Select Database Type: Select SQL 2005, 2008, or 2012
921 13. Database Connection Information: Enter hostname, database and credentials as created
922 in the prerequisites above.
923 14. Login Information: Enter a username and password to be used for the Management
924 Console. Leave the Enable Secure Login for Management Console checked

925 15. HTTP Proxy Settings: Leave blank
926 16. Review Settings: Click Install
927 17. After the installation completes, start JBoss by executing *jboss-eap-6.3\bin\standalone.bat*.
928 18. Review the log file to verify that JBoss started without error: *jboss-eap-6.3\standalone\log\server.log*
929 19. If you receive a timeout error such as “Timeout after [300] seconds waiting for service
930 container stability...”, increase the timeout by modifying standalone.bat, adding the
931 following attribute to the startup script:
932 **-Djboss.as.management.blocking.timeout=900**
933

934 **6.5 CREATE THE SAMPLE NETEAUTO DIRECTORY**

935 1. Open a command prompt as the administrator user
936 2. cd to “C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity
937 Manager\tools\samples\NeteAuto\Organization”
938 o You will see several sample files. For this example, we will use neteauto.ldif
939 3. Execute the following commands:
940
941 dxnewdsa -s500 neteauto 3895 "dc=security,dc=com"
942 dxserver install neteauto
943 dxserver stop neteauto
944 dxloaddb -v -s neteauto neteauto.ldif
945 dxserver start neteauto
946 4. To log in to the IM Management Console, navigate to
947 <http://<ServerName>:8080/iam/immanage> and log in using the credentials you supplied
948 in Login Information above.
949 5. From Directories, select “Create or Update from XML”.
950 6. Browse to C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity
951 Manager\tools\samples\NeteAuto\Organization.
952 7. Select directory.xml. Click Next.
953 8. Supply values for the fields in this window as follows:
954 • **Name** - NeteAuto
955 • **Description** - (Optional)
956 • **Connection Object Name** - neteauto
957 • **Host** - the machine name where you ran the dxserver commands above
958 • **Port** - 3895
959 • **Username/User DN** - uid=NeteAuto
960 Administrator,ou=People,ou=Employee,ou=NeteAuto,dc=security,dc=com
961 • **Password/Confirm Password** - test
962 • **Secure Connection** - Unchecked

963 9. Click Next, then Finish.

964 **6.6 CREATE THE PROVISIONING DIRECTORY**

- 965 1. From Directories, select “Create or Update from XML”.
- 966 2. Browse to C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity
- 967 Manager\tools\directoryTemplates\ProvisioningServer.
- 968 3. Select directory.xml. Click Next.
- 969 4. Supply values for the fields in this window as follows:
 - 970 • **Name** - Provisioning
 - 971 • **Description** - (Optional)
 - 972 • **Connection Object Name** - provisioning
 - 973 • **Host** - the machine name where IM is installed
 - 974 • **Provisioning Domain** - im
 - 975 • **Username** - the username you supplied in **Login Information** above
 - 976 • **Password/Confirm Password** - the password you supplied in **Login Information** above
- 978 5. Click Next, then Finish.

979 **6.7 CREATE THE NETEAUTO ENVIRONMENT**

- 980 1. From Environments, select “New”.
- 981 2. Supply the following information:
 - 982 • **Environment name** - NeteAuto
 - 983 • **Description** - (Optional)
 - 984 • **URL alias** - neteauto
 - 985 • **Base URL** – accept the default (make sure it is a fully qualified host name in the URL)
- 987 3. Click Next.
- 988 4. Select the “NeteAuto” directory. Click Next.
- 989 5. Select the “Provisioning” directory. Click Next.
 - 990 • **URL alias used to reference public tasks** – neteauto_pub
 - 991 • **User for anonymous authentication** – SelfRegUser
- 992 6. Click Validate. Then click Next.
- 993 7. Select “Create Default Roles”. Click Next.
- 994 8. Select the Checkbox for Active Directory.
- 995 9. Scroll down and click the Browse button.
- 996 10. Select the *NIST_PXPolicy.xml* file provided with this guide. (Download the file from https://nccoe.nist.gov/sites/default/files/nccoe/NIST_PXPolicy.zipx and unzip it.)
- 998 11. Click Next.
 - 999 • **System Manager** – SuperAdmin
- 1000 12. Click Add. Then click Next.

1001 • **Inbound Administrator** – SuperAdmin

1002 13. Click Next.

1003 • **Password/Confirm Password** - the password you supplied in **Login Information**

1004 above

1005 14. Click Next.

1006 15. Review the settings, then click Finish.

1007 16. Allow a few minutes for the Environment to deploy.

1008 17. When finished with “0 error(s)”, click Continue.

1009 18. Click “NeteAuto”.

1010 19. Click “Advanced Settings”, then “Workflow”. Enable both check boxes and click Save.

1011 20. Click the “Restart Environment” button.

1012 21. Verify that you can login to the environment by going to the environment URL and

1013 logging in:

1014 • `http://<FullyQualifiedServerName>:8080/iam/im/<ProtectedAlias>`

1015 • Username: SuperAdmin

1016 • Password: test

1017 6.8 CONFIGURE CONNECTION TO ALERTENTERPRISES DATABASE

1018 Generate the encrypted password for the Alert Database as follows:

1019 1. From a command prompt, cd to `C:\Program Files (x86)\CA\Identity`

1020 Manager\IAM Suite\Identity Manager\tools\PasswordTool

1021 • Execute the following command: `pwdtools -JSafe -p <AlertDBPassword>`

1022 • The result displays the Encrypted value with a prefix of {PBES}.

1023 • Copy this encrypted password to be used below for EncryptedALERTDBPassword.

1024

1025 2. From the JBoss installation directory, create the following folder structure:

1026 `jboss-eap-6.3\modules\com\mysql\main`

1027 • Download Connector/J from <http://dev.mysql.com/downloads/connector/>

1028 • Select Platform Independent, Compressed Zip Archive. Download.

1029 • Unzip and copy the `mysql-connector-java-5.1.35-bin.jar` to the `mysql\main` folder

1030 you created above.

1031 • Under the same folder, create a text file named `module.xml`. Paste the

1032 following text into the file:

1033

```
1034           <?xml version="1.0" encoding="UTF-8"?>
1035           <module xmlns="urn:jboss:module:1.1" name="com.mysql">
1036            <resources>
1037            <resource-root path="mysql-connector-java-5.1.35-"
```

```
1038      bin.jar"/>
1039      </resources>
1040      <dependencies>
1041          <module name="javax.api"/>
1042      </dependencies>
1043  </module>
1044
1045  3. From jboss-eap-6.3\standalone\configuration edit standalone-full.xml
1046
1047  4. In the "<drivers>" section, add:
1048      <driver name="mysql" module="com.mysql">
1049          <driver-class>com.mysql.jdbc.Driver</driver-class>
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
      <connection-url>
      jdbc:mysql://ALERTDBServerName:3306/ALERTDBName
      </connection-url>
      <driver>
          mysql
      </driver>
      <pool>
          <max-pool-size>30</max-pool-size>
      </pool>
      <security>
          <security-domain>mysqlDb</security-domain>
      </security>
  </datasource>
  5. Just above the "<drivers>" section, add a new data source:
      <datasource jndi-name="java:/iam/im/jdbc/jdbc/AlertDB"
      pool-name="MySQLPool" use-java-context="true">
          <connection-url>
          jdbc:mysql://ALERTDBServerName:3306/ALERTDBName
          </connection-url>
          <driver>
              mysql
          </driver>
          <pool>
              <max-pool-size>30</max-pool-size>
          </pool>
          <security>
              <security-domain>mysqlDb</security-domain>
          </security>
      </datasource>
  6. In the "<security-domains>" section, add the following security domain:
      <security-domain name="mysqlDb">
          <authentication>
              <login-module
              code="com.netegrity.jboss.datasource.PicketBoxPasswordEncoder"
              ptedLogin" flag="required" module="com.ca.iam.idmutils">
                  <module-option name="user_name"
                  value="ALERTDBUserName"/>
                  <module-option name="password" value="
                  EncryptedALERTDBPassword "/>
                  <module-option name="managedConnectionFactoryName"
                  value="jboss.jca:name=iam/im/jdbc/jdbc/WPDS,service=LocalTx
                  CM"/>
              </login-module>
          </authentication>
      </security-domain>
```

1081 7. Restart the JBoss service
1082 8. Review the log file to verify that JBoss started without error: *jboss-eap-6.3\standalone\log\server.log*
1083

1084 **6.9 POLICY XPRESS POLICY REVIEW**

1085 1. Log in to the NeteAuto Environment that you created above by navigating to
1086 *http://<FullyQualifiedServerName>:8080/iam/im/<ProtectedAlias>*
1087 2. For NeteAuto the username/password is superadmin/test.
1088 3. Navigate to Policies > Policy Xpress > Modify Policy Xpress Policy, and click Search.
1089 4. Select the desired Policy to review and modify as desired.
1090 • Check for Duplicates on Create: Stops the task with a message to the user if
1091 duplicates are detected for the CardNumber or the UserID on the Alert Database
1092 • Check for Duplicates on Modify: Stops the task with a message to the user if the
1093 CardNumber is already used by another user on the Alert Database.
1094 • Check for Numeric on Create and Modify: Stops the task with a message to the
1095 user if the PIN, FacilityCode, or CardNumber is not an integer.
1096 • Check PACs fields on Create and Modify: Stops the task with a message to the
1097 user if none of the PACs checkboxes are selected. At least one must be selected.
1098 • Create AE User: Creates User on the Alert Database if all above checks pass.
1099 Provisions user to Active Directory.
1100 • Disable AE User: Disables User on the Alert Database, by setting the UserStatus
1101 to “Inactive”
1102 • Enable AE User: Enables User on the Alert Database, by setting the UserStatus to
1103 “Active”
1104 • Modify AE User: Modifies User on the Alert Database if all above checks pass.

1105 **6.10 UPDATE CREATE USER AND MODIFY USER SCREENS**

1106 1. From *Roles and Tasks > Admin Tasks > Modify Admin Task*, search and select Create User.
1107 2. Go to the Tabs tab and click the edit pencil next to Profile.
1108 3. Click Browse Next to the Create User Profile.
1109 4. Select the Default User Profile, and click the Edit button.
1110 5. Click the edit pencil next to each of the following fields:
1111 • Office: Change Name to PIN
1112 • Postal Code: Change Name to Facility Code. Change Permission to
1113 Read/Write Required.
1114 • Cell Phone: Change Name to Home Phone.

1115 • Business Phone: Change Name to Work Phone.

1116 • State: Change Name to Pacs All Door. Change Style to Checkbox. Set Check
1117 value to 1. Set Unchecked Value to 0.

1118 • City: Change Name to Pacs Work Access. Change Style to Checkbox. Set
1119 Check value to 1. Set Unchecked Value to 0.

1120 • Address: Change Name to Pacs Home Access. Change Style to Checkbox. Set
1121 Check value to 1. Set Unchecked Value to 0.

1122 • Employee Number: Change Name to Card Number. Change Permission to
1123 Read/Write Required.

1124 • For any non-required fields that you don't want to display: Change Style to
1125 Hidden.

1126 6. Click OK.

1127 7. Select the Create User Profile, and click the Edit button.

1128 8. Repeat Step 5 for this profile. When finished, click OK.

1129 9. Navigate to Users >Manage Users >Create User, and click "Yes" for the warning message
1130 about losing changes.

1131 10. Select Create New User, and click OK.

1132 11. Verify that the fields you updated are changed as desired.

1133 12. Navigate to Users >Manage Users >Modify User, and click "Yes" for the warning message
1134 about losing changes.

1135 13. Select Create Modify User, and click OK.

1136 14. Verify that the fields you updated are changed as desired.

1137 6.11 INSTALL ACTIVITY DIRECTORY CERTIFICATE

- 1138 1. Obtain the Active Directory certificate(s) from the domain controller(s) you want to
1139 connect to and copy them to the Identity Manager server.
- 1140 2. Double-click on the certificate, and click Install Certificate.
- 1141 3. Select Local Machine, then Place all Certificates in the following store. Click Browse.
- 1142 4. Select Trusted Root Certification Authorities. Click OK twice.

1143 6.12 ACQUIRE ACTIVITY DIRECTORY ENDPOINT

- 1144 1. From Endpoints >Manage Endpoints >Create Endpoint, select Create a new endpoint of
1145 Endpoint type ActiveDirectory. Click OK.
 - 1146 • Endpoint: Give your endpoint a name
 - 1147 • Hostname: Fully qualified host name for the Active
1148 Directory Domain Controller

1149 • User ID: Fully qualified User ID, for example: domain\userid.
1150 • Password/Confirm Password: Password for the AD User
1151 2. Click the Security tab. Check the “Use LDAP – SSL Encryption” checkbox.
1152 3. Click Submit.

1153 **6.13 EXPLORE AND CORRELATE ACTIVE DIRECTORY**

1154 1. From *Endpoints >Explore and Correlate Definitions >Create Explore and Correlate Definition*, select Create a New Object of Type Explore and Correlate and click OK.
1155
1156 2. Explore and Correlate Name: Give it a name such as “Explore AD <domain controller name>”
1157
1158 3. Select the Explore endpoint... checkbox. Uncheck the rest of the checkboxes.
1159
1160 4. Click the Select Container/Endpoint/Explore Method button.
1161
1162 5. Select Active Directory and click Search.
1163
1164 6. Select the endpoint you created above. Click Select.
1165
1166 7. Click Search.
1167
1168 8. Select the containers that you want to be connected to Identity Manager.
1169
1170 9. Click Select, then Submit.
1171
1172 10. From Endpoints > Execute Explore and *Correlate*, select Execute Now and click Next.
1173
1174 11. Browse for the Explore and Correlate Definition you just created, then click Finish.
1175
1176 12. Repeat the steps above to create and execute a Correlate Definition, with only one difference: On the step Explore endpoint step, uncheck Explore endpoint, and check Update User Fields, Correlate Accounts to Users, and Create Users as needed.
1177
1178 13. From System > View Submitted tasks, click Search.
1179 14. Verify that both the Explore and Correlate definitions completed successfully.

1172 **6.14 CREATE THE ACTIVE DIRECTORY ACCOUNT TEMPLATE AND PROVISIONING ROLE**

1173 1. From Endpoints > Account Templates > Create Account Template, select Create a new Account Template of Endpoint Type “Active Directory”. Click OK.
1174
1175 2. Give the Account Template a name, such as “<domain controller name> Account Template”.
1176
1177 3. From the Endpoints tab, add the Active Directory Endpoint you created above.
1178
1179 4. From the Groups tab, add the Active Directory groups you want to provision to the user.
1180
1181 5. When finished, click Submit.

1180 6. From Roles >Provisioning Roles >Create Provisioning Role, select Create a new
1181 provisioning role, click OK.

1182 7. Give the Provisioning Role a name such as “<domain controller name> Provisioning
1183 Role”

1184 8. From the Account Templates tab, add the Account Template you just created above.

1185 9. From the Administrators tab, select a user, or group of users that you want to be the
1186 Administrators of this role. For example, to make the members of a certain Admin role
1187 the administrators of this provisioning role:

- 1188 • Click Add.
- 1189 • From the Users drop-down select a group of users, such as Users who are
1190 members of <role-rule>, then admin role.
- 1191 • Browse, search, and select the Admin Role you want to add.
- 1192 • From the Owners tab, select a user, or group of users that you want to be the
1193 Owners of this role, using the same process as used for the Administrators tab.
- 1194 • Click Submit.

1195 **6.15 MODIFY CREATE AE USER POLICY TO INCLUDE THE NEW PROVISIONING ROLE**

- 1196 1. From Policies >Policy Xpress >Modify Policy Xpress Policy, search and select the Create
1197 AE User policy.
- 1198 2. From the Action Rules tab, click the edit pencil next to Create User
- 1199 3. Click the edit pencil next to Add otdc. Click the Browse “...” button next to the
1200 Provisioning Role Name. Select the Provisioning Role you just created.
- 1201 4. Click Select, OK, OK, Submit.

1202 **6.16 ADD WORKFLOW CONTROL OVER CREATE USER AND ANY OTHER TASK AS DESIRED**

- 1203 1. From Roles and Tasks >Admin Tasks >Modify Admin Task, search and select Create User.
- 1204 2. From the Events tab, click the edit pencil next to the CreateUserEvent workflow process.
- 1205 3. Select the Non-Policy Based workflow process “SingleStepApproval.”
- 1206 4. For the approval, select “Approve Create User” *
- 1207 5. For the Participant resolver select the type of members you want to assign. For example,
1208 Admin Role Members. *
- 1209 6. Click Add Admin Roles. Search and select the Admin Roles you want to have approve this
1210 workflow. *
- 1211 7. Repeat the above 3 steps with * for the Primary Approver.
- 1212 8. When finished with both approvers, click OK, then Submit.

1213 The above steps can be used for the Modify User and Enable/Disable User tasks (or any
1214 other task).

1215 **6.17 TEST CREATION OF A USER MANUALLY**

- 1216 1. From Users >Manage Users > Create User, select Create a New User, click OK.
- 1217 2. Fill out the fields as desired for the new user, keeping in mind the policy rules explained
1218 above. For example, PIN, Facility Code, and Card Number must be integers, and at least
1219 one Pacs access checkbox must be checked.
- 1220 3. Click Submit, then OK.
- 1221 4. From Home > View My Worklist, select and approve the workflow for the Create User
1222 task *
- 1223 5. From System >View Submitted tasks, click Search. Verify that the Create User task
1224 completed successfully. *
- 1225 6. Connect to the AE Database. Verify that the user was created successfully. *
- 1226 7. Connect to the Active Directory Domain Controller. Verify that the user was created
1227 successfully. *

1228 Repeat all the steps above for Modify User, Enable User, and Disable User.

1229 **6.18 TEST CREATION OF A USER WITH A CSV FILE**

- 1230 1. Download the file *HRBulkUsers4.csv* from
1231 <https://nccoe.nist.gov/sites/default/files/nccoe/HRBulkUsers4.csv>.
- 1232 2. Modify the CSV file to enter the desired values for the new users to be created. Keep in
1233 mind the policy rules that must be followed as described above.
- 1234 3. From System > Bulk Loader, Browse for the CSV file.
- 1235 4. What field represents the action to perform on the object: *action*.
- 1236 5. What field will be used to uniquely identify the object: *uid*.
- 1237 6. Click Next.
- 1238 7. What is the Primary Object: *USER*.
- 1239 8. Select a task to execute for action 'create': Create User
- 1240 9. Click Finish.

1241 Repeat the steps from Section 9.17 (above) with an asterisk (*) to approve the users and
1242 verify that they were successfully created.

1243 7 IDENTITY MANAGEMENT AND GOVERNANCE (IMG): RSA (BUILD #2)

1244 RSA IMG implements the central IdAM workflow in Build #2. It receives input from an HR system
1245 in the form of .csv files. The access and authorization for each user is based on the business and
1246 security rules implemented in workflows within RSA IMG. The workflows include management
1247 approval chains as well as approval/denial data logging. Once IMG has processed the access and
1248 authority request, the updated user access and authorization data is pushed to the central ID
1249 store. The central ID store contains the distribution mechanism for updating the various
1250 downstream (synchronized) directories with user access and authorization data. This process
1251 applies to new users, terminated users (disabled or deleted users), and any changes to a user
1252 profile. Changes may include promotions, job responsibility changes, and any other change that
1253 would affect the systems a user needs to access.

1254 7.1 SECURITY CHARACTERISTICS

1255 Cybersecurity Framework Categories:

1256 • PR.AC-1: Identities and credentials are managed for authorized devices and users
1257 • PR.AC-4: Access permissions are managed, incorporating the principles of least privilege
1258 and separation of duties

1259 NIST 800-53 rev 4 Security Controls: AC-2, AC-3, AC-5, AC-6, AC-16, IA Family

1260 7.2 IMG INSTALLATION

1261 Install IMG using the included installation guide on a server running SUSE Linux OS or from an
1262 IMG virtual appliance image. The RSA Installation guide is available for licensed customers at
1263 <http://www.emc.com/domains/rsa/index.htm>.

1264 7.3 IMG CONFIGURATION AND INTEGRATION WITH DIRECTORIES

1265 After install, open a web browser and point it to the IP Address or DNS name of the RSA IMG
1266 server. The following instructions are provided along with screenshots depicting each step.
1267 Unless stated otherwise the settings are included in each screenshot.

1268 Log in with the default credentials:

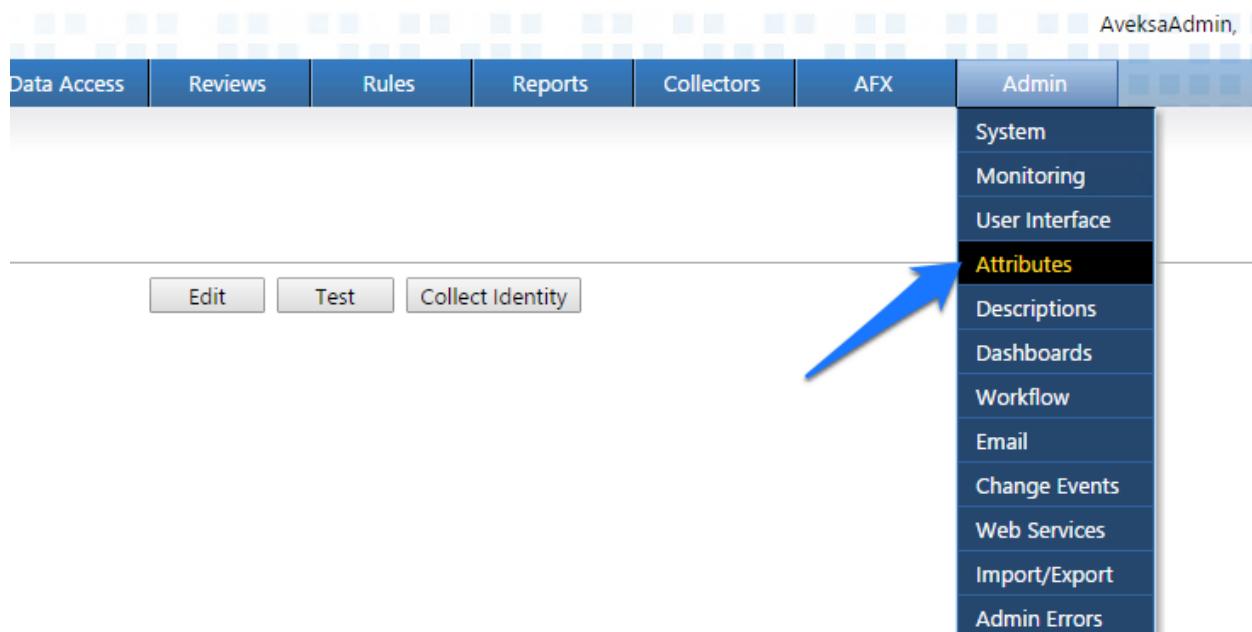
1269 Username: AveksaAdmin (case sensitive)

1270 Password: aveksa123

1271 Change the password when prompted to change.

1272 7.3.1 Set Up Custom Attributes

- 1273 1. Navigate to 'Admin' then 'Attributes':



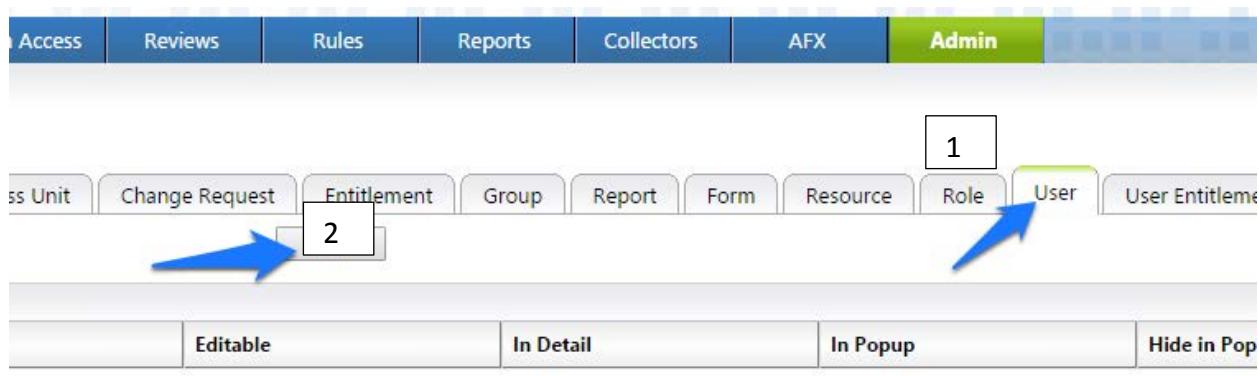
1274

1275

Figure 9. IMG Attributes Window

1276

1. Click on 'User' then 'Edit' as shown in Figure 10.



1277

No

Yes

Yes

Yes

1278

Figure 10. IMG Edit User

1279

2. Modify your attributes to match Figures 11-13.

Attribute Configuration - User									
Attribute Name	Data Type	Length	Data Source	Editable	Custom Value	Directory	In Detail	In Popup	Hide in Popup if Empty
Backup Supervisor	User		Collected				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Creation Date	Date		Collected				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Deletion Date	Date		Collected				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Department	String	256	Collected	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email Address	String	256	Collected	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Exception Count	Integer		Managed	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Expiration Date	Date		Collected				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Expiration Value	String	256	Collected				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
First Name	String	256	Collected	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Full Name	String	256	Collected	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is App Owner	String	256	Managed	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is Deleted	Integer		Collected				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is Manager	String	256	Collected	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is Monitor	String	256	Managed	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is Senior Manager	String	256	Managed	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Is Terminated	Integer		Collected	<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 11. IMG Attributes Examples

1280

Job Code	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Job Family	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Job Level	Integer		Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Job Status	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last Name	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Location	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Other	User		Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PACS All Doors	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PACS Home Access	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PACS Work Access	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Previous Supervisor	User		Managed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Self Reviewer	User		Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Supervisor	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Termination Date	Date		Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Title	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transfer Date	Date		Managed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unique Id	String	2000	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Id	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Risk Level	String	256	Managed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1281

1282

Figure 12. IMG Attributes Examples

Violation Count	Integer	Managed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Login ID	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DN	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OU	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1283

1284

Figure 13. IMG Attributes Examples

1285

3. Click on OK.

1286

4. Click on 'Account' then 'Edit' as shown in Figure 14.

Return to: [Home](#)

Attributes

Account 1 Account Mapping Business Source Application Role Business Unit Change Request Entitlement

2 [Edit](#)

1287

1288

Figure 14. IMG Edit Attributes

1289

5. Modify your attributes to match those shown in Figure 15. IMG Attribute Example.

Attribute Configuration - Account								
Attribute Name	Data Type	Database ID	Data Source	Editable	Custom Value	In Detail	In Popup	Hide in Popup if Empty
Account Email	String	CAS10	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Expiration Date	Date	CAD1	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Full Name	String	CAS2	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Risk Level	String	CAS3	Managed	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Risk Score	Integer	CA1	Managed	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Status	String	CAS8	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Account Technical Name	String	CAS4	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DN	String	CAS7	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last Reviewed Date	Date	LAST_REVIEWED_D	Managed	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PACS All Doors	String	CAS1	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PACS Home Access	String	CAS5	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PACS Work Access	String	CAS6	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Login ID	String	CAS9	Collected			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add Attribute](#) [Add Separator](#)

1290

1291

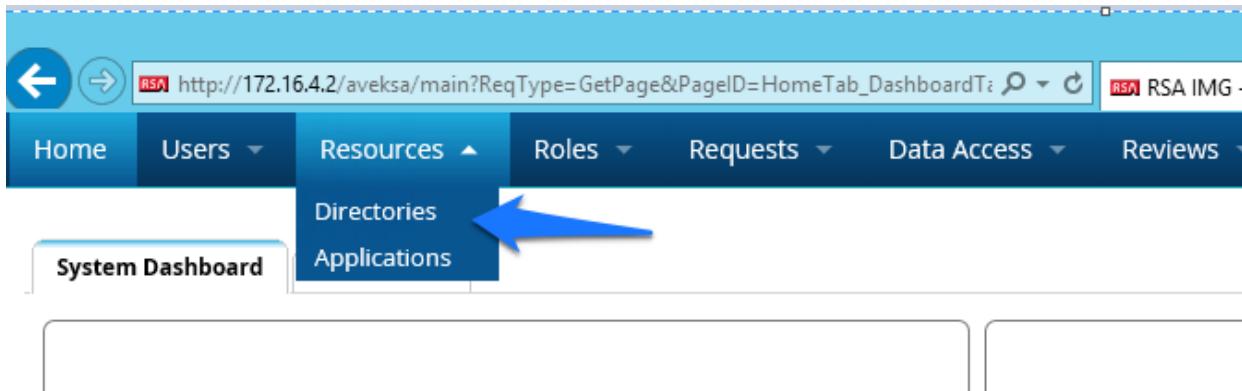
Figure 15. IMG Attribute Example

1292 6. Click on 'OK'.

1293 7.3.2 Set up Organization Users

1294 The next step is to set up the organization's existing users. In the example solution, we used a
 1295 CSV file that contains all the users in the organization. This CSV file needs to be copied to a
 1296 convenient location on the IMG server. You can get a sample CSV file, *HR_Data_Move.csv* at
 1297 https://nccoe.nist.gov/sites/default/files/nccoe/HR_Data_Move.csv.

1298 1. Once the CSV file is copied to the server, perform the following actions:
 1299 2. Navigate to 'Resources' and under resources, select 'Directories' as shown in Figure 16.



1300

1301

Figure 16. IMG Resources Directories

1302

3. Click 'Create Directory' as shown in Figure 17.

The screenshot shows a web-based application interface for managing resources. The top navigation bar includes links for Home, Users, Resources (which is the active tab), Roles, Requests, Data Access, Reviews, and Rules. Below the navigation is a breadcrumb trail 'Return to: Home'. The main content area is titled 'Directories' and displays a table with columns for Directory, Description, and Business Owner. A search bar and grouping dropdown are also present. A blue arrow points to the 'Create Directory' button in the top right of the page.

1303

1304

Figure 17. IMG Create Directory

1305

4. Select 'Other Directory' and click 'Next' as shown in Figure 18.

The screenshot shows a 'Create Directory' dialog box. The left sidebar is titled 'Select Directory' and contains a search bar. The main area lists two items: 'Active Directory' and 'Other Directory'. The 'Other Directory' item is highlighted with a yellow background and has a blue arrow pointing to its checkbox. The status bar at the bottom shows '2 items | 1 selected'.

1306

1307

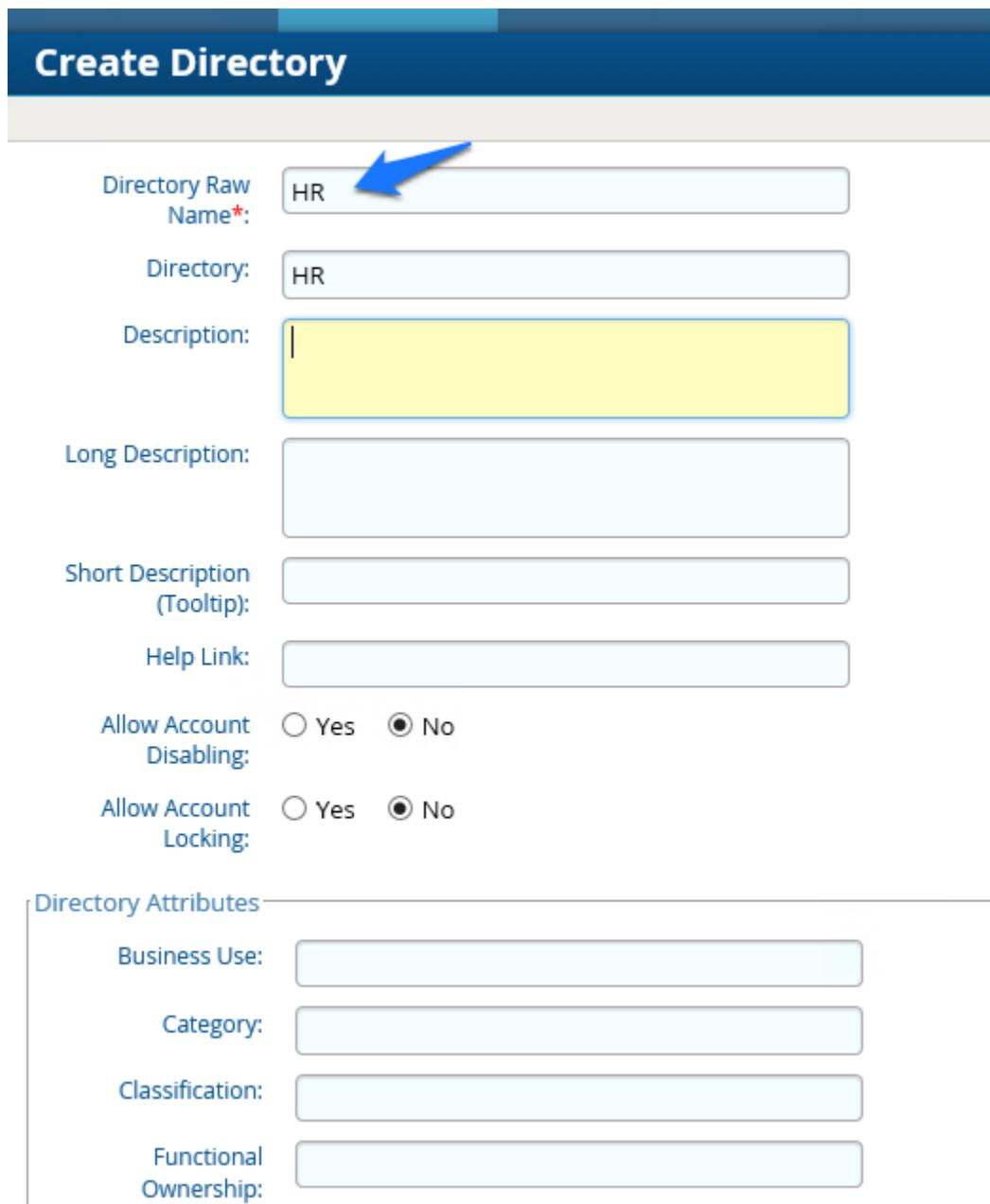
1308

Figure 18. IMG Create Directory

1309

1310

5. Enter 'HR' in the 'Directory Raw Name' field. Click 'Finish' as shown in Figure 19 .



Create Directory

Directory Raw Name*: HR

Directory: HR

Description: |

Long Description:

Short Description (Tooltip):

Help Link:

Allow Account Disabling: Yes No

Allow Account Locking: Yes No

Directory Attributes

Business Use:

Category:

Classification:

Functional Ownership:

1311

1312

Figure 19. IMG Directory Information

1313 You have now created your first directory which will serve as a repository for all the HR Data for
 1314 the organization.

1315 6. Repeat the above steps, creating a second directory. This one will be named 'RSA
 1316 Adaptive Directory'. This container will be used to pull AD accounts from the Adaptive
 1317 Directory server. In this case be sure to select the two options as shown in Figure 20.

Create Directory

Directory Raw Name*: RSA Adaptive Directory Accounts

Directory: RSA Adaptive Directory Accounts

Description:

Long Description:

Short Description (Tooltip):

Help Link:

Allow Account Disabling: Yes No

Allow Account Locking: Yes No

Directory Attributes

Business Use:

Category:

Classification:

Functional Ownership:

Locality:

Sensitivity:

Figure 20. IMG Create Directory

1318

1319

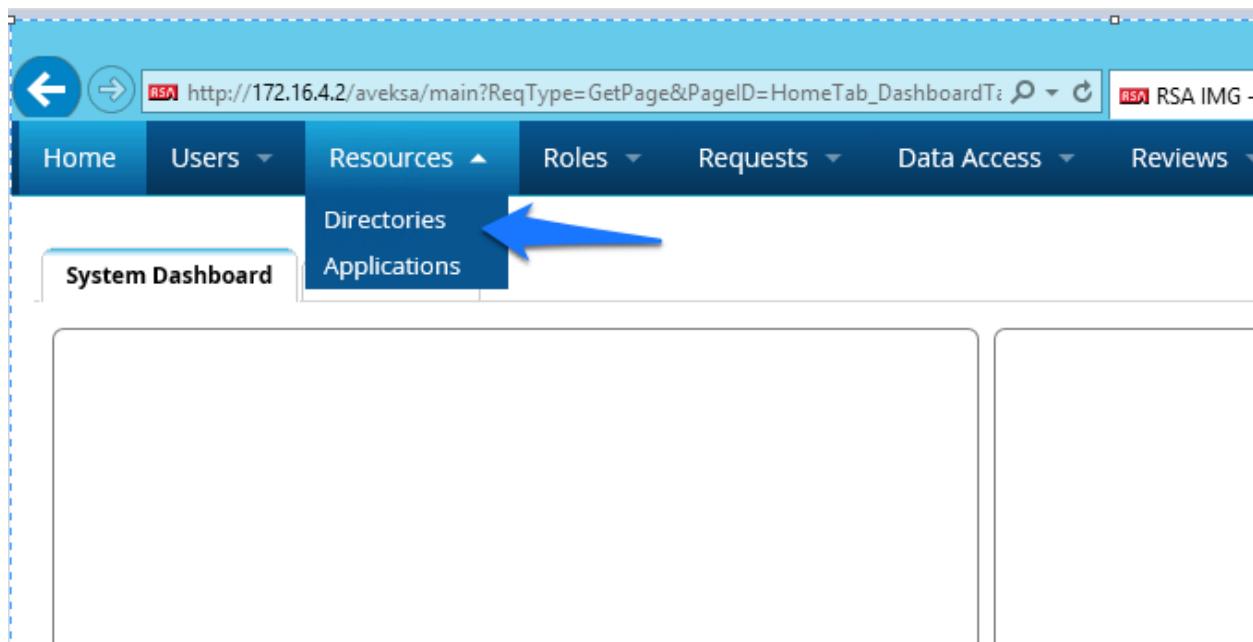
1320

1321

1322 7.3.3 Populate the HR Directory

1323 The next step is to populate the HR directory with users.

1324 1. Click on 'Resources' and 'Directories' again as shown in Figure 21.



1325

1326

Figure 21. IMG Directories

1327

2. Click on your new HR directory you just created as shown in Figure 22.

A screenshot of the 'Directories' page. The top navigation bar is identical to Figure 21. Below it, a 'Return to: Home' link is visible. The main content area is titled 'Directories'. It features a 'Create Directory' and 'Collect Data (all)' button. A search bar and grouping dropdown are also present. A table lists four items: 'Active Directory', 'Contractors', 'HR', and 'RSA Adaptive Directory Accounts'. The 'HR' entry is highlighted with a blue arrow. The table has columns for Directory, Description, and Business Owner.

Directory	Description	Business Owner
Active Directory	--	AveksaAdmin,
Contractors	--	AveksaAdmin,
HR	--	AveksaAdmin,
RSA Adaptive Directory Accounts	--	AveksaAdmin,

1328

1329

Figure 22. IMG Directories

1330

1331 3. Click on 'Collectors' then click 'Create Identity Collector' as shown in Figure 23Figure 23.

1332 IMG Create Identity Collector.

Return to: [Home](#) [Directories](#)

Directory: HR

General AFX Connector Binding **Collectors** Accounts Who Has Access What Access

Create Identity Collector Create Account Collector

Grouping: -- select --

Search:

Name	Description	Collector Type
------	-------------	----------------

1333

1334

Figure 23. IMG Create Identity Collector

1335

4. Enter details as shown in Figure 24.

Edit Collector: HR Identities

Collector Description

Collector Name*:

Description :

Data Source Type :

Agent :

Directory :

Status :

Schedule

Scheduled : Yes No

1336

1337

Figure 24. IMG HR Identities

1338

5. Click 'Next', and enter details as below as shown in Figure 25.

Figure 24 shows the 'Edit Collector: HR Identities' configuration interface. The 'Database Connection' tab is active. The 'DB Type' dropdown is set to 'CSV'. The 'Driver Class*' field contains 'com.hxtt.sql.text.TextDriver'. The 'URL*' field contains 'jdbc:csv:///home/oracle/database/SampleData'. The 'User Name' field contains 'AveksaAdmin'. The 'Password' field is masked with '*****'.

1339

1340

Figure 25. IMG HR Identities (cont.)

1341 6. Use the same username and password you use to log into the IMG management web
1342 page.

1343 The URL will point to the folder that the CSV file is located in. In this example, the full field is:

1344 `jdbc:csv:///home/oracle/database/SampleData/Demo/HR/?_CSV_Header=true;tmpdir=/hom`
1345 `e/oracle`

1346 The CSV file is located in `home/oracle/database/SampleData/Demo/HR`

7. Click 'Next'.
8. Leave 'Users' selected and click 'Next' as shown in Figure 26.

Figure 25 shows the 'Edit Collector: HR Identities' configuration interface. The 'Select types of identity data to collect' tab is active. The 'Users' checkbox is checked.

1349

1350

Figure 26. IMG HR Identities - Users

1351 1. Enter details as shown in Figure 27 and Figure 28 , below. The full text of the 'User Data
1352 Query' is as follows:

```
1353 select fname, lname, case when substr(lname,1,2) = 'IT' then  
1354 'it' when substr(lname,1,2) = 'OT' then 'ot' else 'pacs' end as  
1355 OU, login, email as sAMAccountName, email, location, bu,  
1356 department, title, supervisor, job_level, job_status, login as  
1357 SR, is_terminated, previous_manager, jobcode, previous_manager  
1358 as backjp_supervisor, job_family,concat(lname, ', ', fname) as  
1359 fullname, is_manager, email as UniqueID from HR_Data_Move
```

1360 The highlighted section is specific to this example, based off of our sample data, the OU that the
1361 user needs to be provisioned in is based off of the last name. Basically, when the 1st two letters
1362 of the last name = IT, the user will have 'it' set to the OU attribute, if it's OT, then 'ot' is set as
1363 the OU attribute, any other scenario the OU attribute is set to 'pacs'.

1364

Edit Collector: HR Identities

Mapping for user attributes

User Data

Users Data Query* :

```
select fname, lname, case when substr(lname,1,2) = 'IT' then 'it' when substr(lname,1,2) = 'OT' then 'ot' else 'pacs' end as OU, login, email as sAMAccountName, email, location, bu, department, title, supervisor, job_level, job_status, login as SR, is_terminated, previous_manager, jobcode, previous_manager as backjp_supervisor, job_family,concat(lname, ' ', fname)as
```

User attribute	DB column with value		
User ID* :	sAMAccountName		
Business Unit Id :	bu	value is Business Unit	Name
Backup Supervisor :		value is User	User ID
DN :			
Department :	department		
Email Address :	email		
Expiration Date :			
Expiration Value :			
First Name :	fname		
Full Name :	fullname		
Is Manager :	is_manager		
Is Terminated :	is_terminated		
Job Code :	jobcode		

1365

1366

1367

Figure 27. IMG HR Identities

Job Family :	<input type="text" value="job_family"/>
Job Level :	<input type="text" value="job_level"/>
Job Status :	<input type="text" value="job_status"/>
Last Name :	<input type="text" value="lname"/>
Location :	<input type="text" value="location"/>
Login ID :	<input type="text" value="login"/>
OU :	<input type="text" value="OU"/>
Other :	<input type="text" value="previous_manager"/> value is User <input type="button" value="User ID"/>
PACS All Doors :	<input type="text"/>
PACS Home ACcess :	<input type="text"/>
PACS Work Access :	<input type="text"/>
Self Reviewer :	<input type="text" value="SR"/> value is User <input type="button" value="User ID"/>
Supervisor :	<input type="text" value="supervisor"/>
Termination Date :	<input type="text"/>
Title :	<input type="text" value="title"/>
Unique Id :	<input type="text" value="UniqueID"/>

1368

1369

Figure 28. IMG HR Identities (cont.)

1370 9. Click 'Finish'

1371 7.3.4 **Configure Adaptive Directory Container**1372 The next step is to configure the Adaptive Directory Container with Identity and Account
1373 collectors.

1374

1375 1. Navigate to the Adaptive Directory Container as shown in Figure 29.

1376

1377

Figure 29. IMG Adaptive Directory Container

1378

1379 This identity collector will tie together user identities in Adaptive Directory to user identities in
 1380 the HR CSV file.

1381 2. Click on 'Collectors' and 'Create Identity Collector' as shown in Figure 30.

1382

1383

Figure 30. IMG Identity Collector

1384 3. Create the ID collector as follows, clicking 'Next' between each screen shown in Figure
1385 31, Figure 32, Figure 33, Figure 34 and Figure 35.

Edit Collector: RSA Adaptive Directory Identity Collector

Collector Description

Collector Name* : RSA Adaptive Directory Identity Collector

Description :

Data Source Type : Ldap

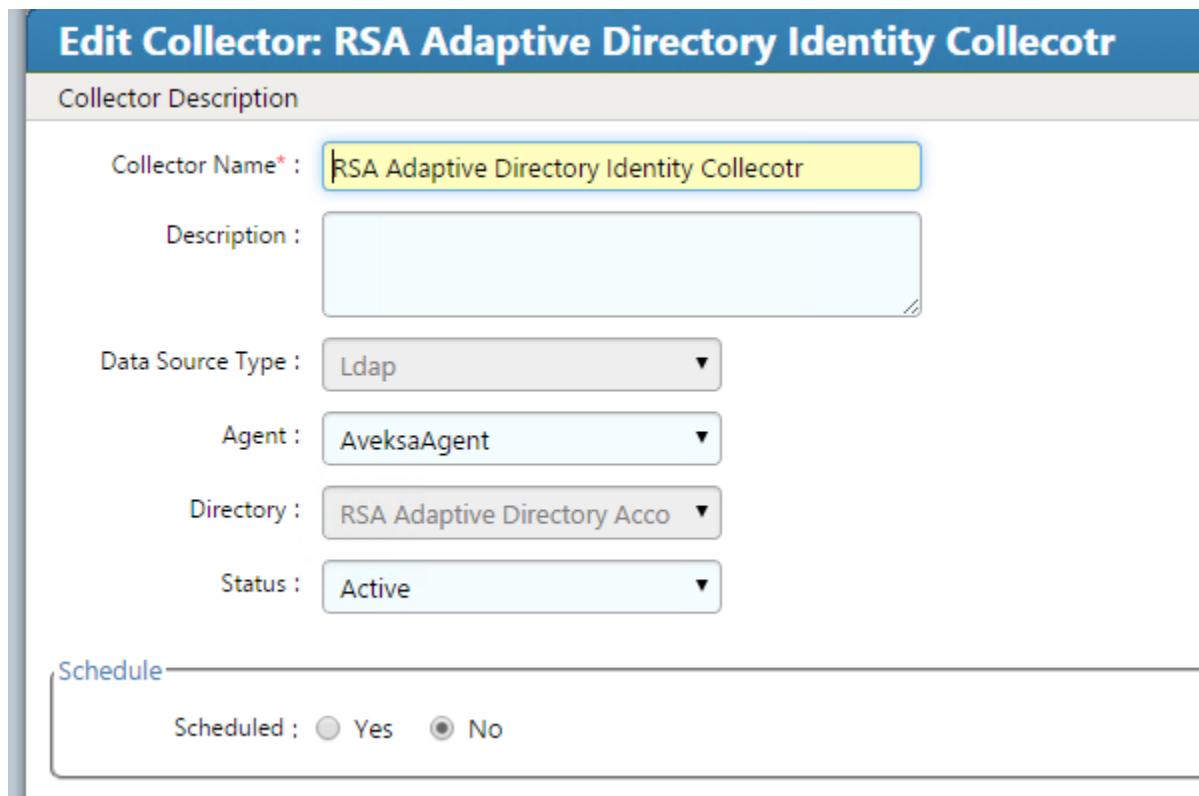
Agent : AveksaAgent

Directory : RSA Adaptive Directory Acco

Status : Active

Schedule

Scheduled : Yes No



1386

1387

Figure 31. IMG AD Identity Collector

1388

1389

1390 *Figure 32. IMG AD Identity Collector*

1391

Edit Collector: RSA Adaptive Directory Identity Collector

Connection

Host*: 172.16.4.3

Port*: 2389

Bind DN*: cn=Directory Manager

Bind Password*:

Use SSL:

Disable Paging:

1392

1393 *Figure 33. IMG AD Identity Collector*

1394

1392

1393 *Figure 33. IMG AD Identity Collector*

1394

Edit Collector: RSA Adaptive Directory Identity Collector

Select types of identity data to collect

Users

Edit Collector: RSA Adaptive Directory Identity Collector

Mapping for user attributes

User Data

User attribute	Mapping
User Base DN* :	<input type="text" value="dc=master,dc=test"/>
User Search Scope* :	<input type="text" value="Subtree"/>
User Search Filter* :	<input type="text" value="(&(objectCategory=person)(objectClass=user)(sAMAccountName=*))"/>
User ID* :	<input type="text" value="userPrincipalName"/>
Business Unit Id :	<input type="text"/> value is Business Unit <input type="text" value="Name"/>
Backup Supervisor :	<input type="text"/> value is User <input type="text" value="User ID"/>
DN :	<input type="text" value="dn"/>
Department :	<input type="text"/>
Email Address :	<input type="text"/>

Figure 34. IMG AD Identity Collector

1395

1396

1397

Is Terminated :	<input type="text"/>
Job Code :	<input type="text"/>
Job Family :	<input type="text"/>
Job Level :	<input type="text"/>
Job Status :	<input type="text"/>
Last Name :	<input type="text"/>
Location :	<input type="text"/>
Login ID :	<input type="text"/>
OU :	<input type="text"/>
Other :	<input type="text"/> value is User <input type="button" value="User ID"/>
PACS All Doors :	<input type="text" value="pacsAllDoors"/>
PACS Home ACcess :	<input type="text" value="pacsHomeAccess"/>
PACS Work Access :	<input type="text" value="pacsWorkAccess"/>
Self Reviewer :	<input type="text"/> value is User <input type="button" value="User ID"/>
Supervisor :	<input type="text"/>
Termination Date :	<input type="text"/>
Title :	<input type="text"/>
Unique Id :	<input type="text"/>

1398

1399

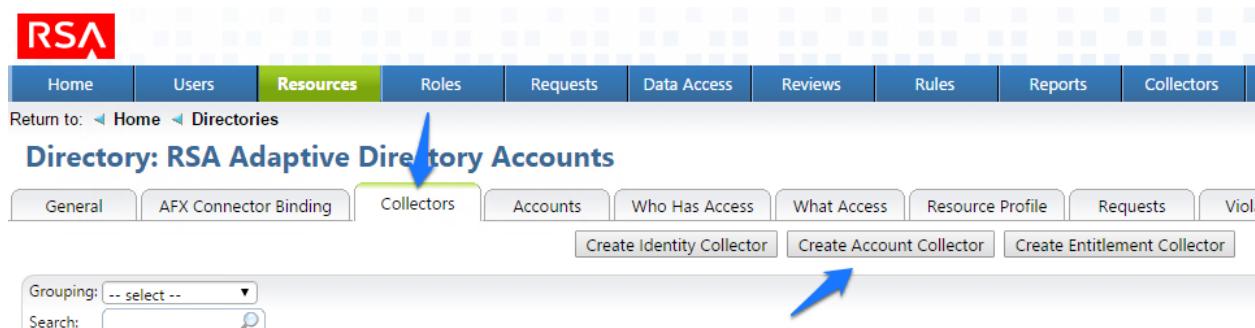
Figure 35. IMG AD Identity Collector

1400

1401 4. Click Finish

1402 7.3.5 [Create an Account Collector](#)1403 The next step is to create an account collector which pulls all relevant attributes from Adaptive
1404 Directory.

1405 1. Click on 'Collectors' and 'Create Account Collector' as shown in Figure 36.



Return to: [Home](#) [Directories](#)

Directory: RSA Adaptive Directory Accounts

General AFX Connector Binding **Collectors** Accounts Who Has Access What Access Resource Profile Requests Violations

Create Identity Collector Create Account Collector Create Entitlement Collector

Grouping: **-- select --** Search:

1406

1407

Figure 36. IMG AD Create Account Collector

1408 2. Create the Account collector as follows, clicking 'Next' between each screenshot, Figure 1409 37 through Figure 46 below.

Edit Collector: RSA AD Directory Accounts

Collector Description

Collector Name*: RSA AD Directory Accounts

Description:

Data Source Type: Ldap

Agent: AveksaAgent

Status: Active

Schedule

1410 Scheduled: Yes No

1411

Figure 37. IMG Edit Collector

Edit Collector: RSA AD Directory Accounts

Connection

Host* :

Port* :

Bind DN* :

Bind Password* :

Use SSL :

Disable Paging :

1412

1413

Figure 38. IMG Edit Collector

1414

Edit Collector: RSA AD Directory Accounts

Select types of account data to collect

Accounts

User Account Mappings

Groups

Case Sensitivity

Data is case sensitive (This option has been disabled as first successful collection has already occurred)

1415

1416

Figure 39. IMG Edit Collector

1417

Edit Collector: RSA AD Directory Accounts

Mapping for account and user account attributes

Search Configuration for Accounts

Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector.

Account Base DN* :

Account Search :

Account Search Filter* :

Account ID* :

Account Attribute	Attribute in Ldap schema
Last Login Date :	<input type="text" value="lastLogon"/>
Account Disabled :	<input type="text"/>
Account Locked :	<input type="text"/>
Account email :	<input type="text" value="userPrincipalName"/>
Account expiration : date	<input type="text" value="accountExpires"/>
Account full name :	<input type="text" value="displayName"/>
Account status :	<input type="text" value="userAccountControl"/>
Account technical : name	<input type="text" value="sAMAccountName"/>

1418

1419

Figure 40. IMG Edit Collector

1420

DN :

Login ID :

PACS All Doors :

PACS Home Access :

PACS Work Access :

User Account Mapping Attribute	Attribute in Ldap schema
User ID* :	<input type="text" value="userPrincipalName"/>

Figure 41. IMG Edit Collector

Edit Collector: RSA AD Directory Accounts

Mapping for group attributes

Group Data

Group attribute	Mapping
Group Base DN* :	<input type="text" value="DC=master,DC=test"/>
Group Search Scope* :	<input type="text" value="Subtree"/>
Group Search Filter* :	<input type="text" value="(objectclass=group)"/>
Group ID/Name* :	<input type="text" value="distinguishedName"/>
Member of Group* :	<input type="text" value="member"/>
DN :	<input type="text" value="cn"/>
Description :	<input type="text" value="description"/>
Domain :	<input type="text"/>
Owner :	<input type="text"/> value is User <input type="text" value="User ID"/>
Owner :	<input type="text" value="managedBy"/>
Resource type :	<input type="text"/>

1423

1424

Figure 42. IMG Edit Collector

1425

Edit Collector: RSA AD Directory Accounts

Edit User Resolution Rules

Target Collector	User Attribute
<input type="text" value="Users"/>	<input type="text" value="User Id"/> <input type="button" value="X"/>
<input type="button" value="Add More..."/>	

1426

1427

Figure 43. IMG Edit Collector

Edit Collector: RSA AD Directory Accounts

Edit Member Account Resolution Rules

Target Collector	Account Attribute	
<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="RSA AD Directory Accounts"/>	<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="DN"/>	<input style="border: 1px solid #ccc; padding: 2px; width: 20px; height: 20px; border-radius: 5px; background-color: #ccc; color: #0070C0; font-weight: bold; font-size: 10px;" type="button" value="X"/>
<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px;" type="button" value="Add More..."/>		

1428

1429

Figure 44. IMG Edit Collector

Edit Collector: RSA AD Directory Accounts

Edit Sub-group Resolution Rules

Target Collector	Group Attribute	
<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="RSA AD Directory Accounts"/>	<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="Name"/>	<input style="border: 1px solid #ccc; padding: 2px; width: 20px; height: 20px; border-radius: 5px; background-color: #ccc; color: #0070C0; font-weight: bold; font-size: 10px;" type="button" value="X"/>
<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px;" type="button" value="Add More..."/>		

1430

1431

Figure 45. IMG Edit Collector

Edit Collector: RSA AD Directory Accounts

Edit Group Owner Resolution Rules

Target Collector	User Attribute	
<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="Users"/>	<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px; margin-right: 10px;" type="button" value="User Id"/>	<input style="border: 1px solid #ccc; padding: 2px; width: 20px; height: 20px; border-radius: 5px; background-color: #ccc; color: #0070C0; font-weight: bold; font-size: 10px;" type="button" value="X"/>
<input style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px; border-radius: 5px; background-color: #fff; color: #0070C0; font-weight: bold; font-size: 10px;" type="button" value="Add More..."/>		

1432

1433

Figure 46. IMG Edit Collector

1434 3. Click 'Finish'

1435 A Test button is provided with each account collector and identity collector.

1436 4. Test each account collector you created using the test button. This action verifies that
1437 IMG can retrieve the account information for each directory added as shown in Figure
1438 47 below.

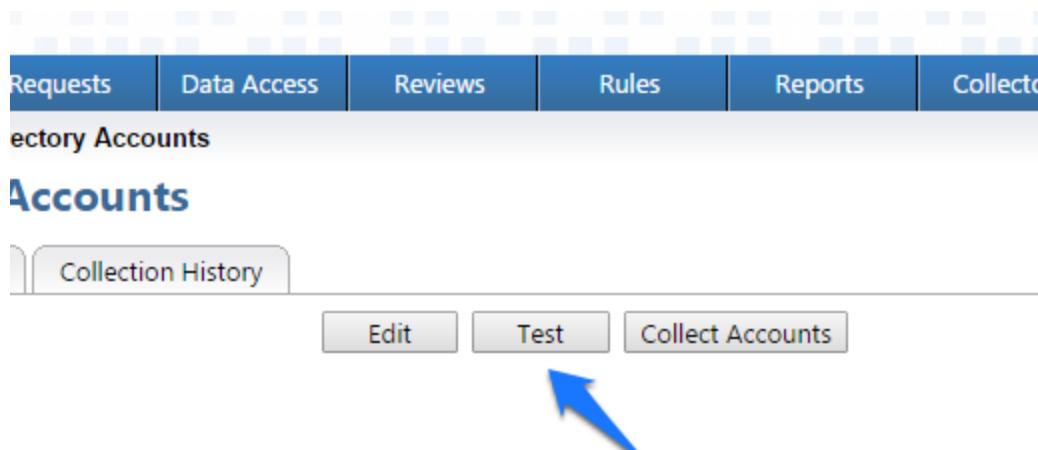


Figure 47. IMG Account Test

1441 A successful test will look something like Figure 48.

1440

1440

1441 A successful test will look something like Figure 48.

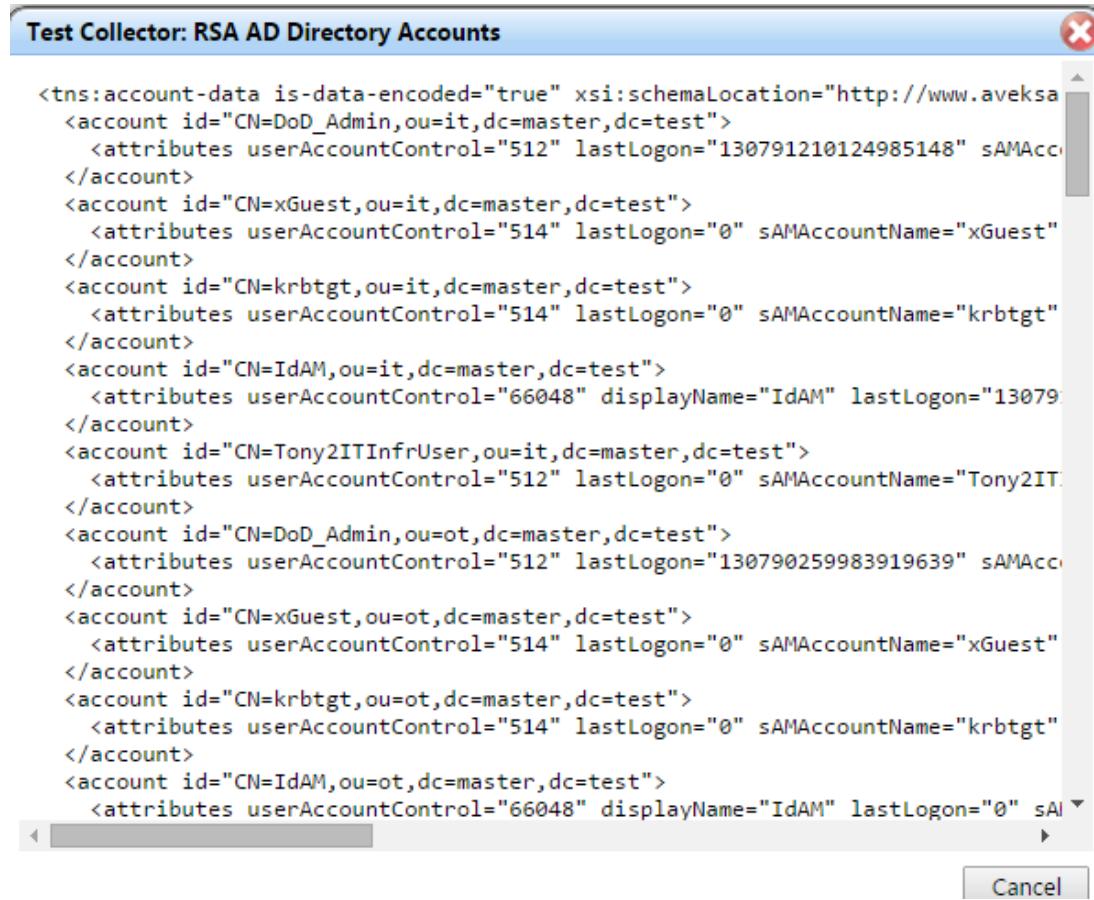


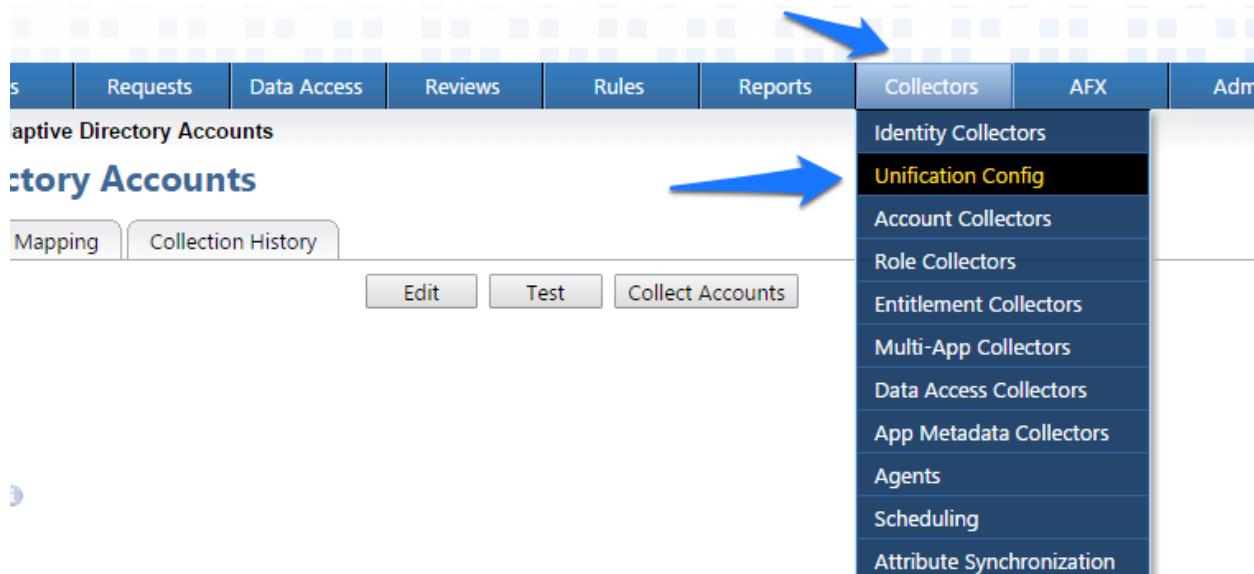
Figure 48. IMG Successful Test Example

1444 You can see valid data in an XML format. A failed test will generate an error message that can
1445 help you isolate the problem.

1446 7.3.6 Edit the Unification Configuration Participating Collectors

1447 The next step is to configure Unification – this is the process of joining Identities from the HR
 1448 CSV and the Adaptive Directory collectors.

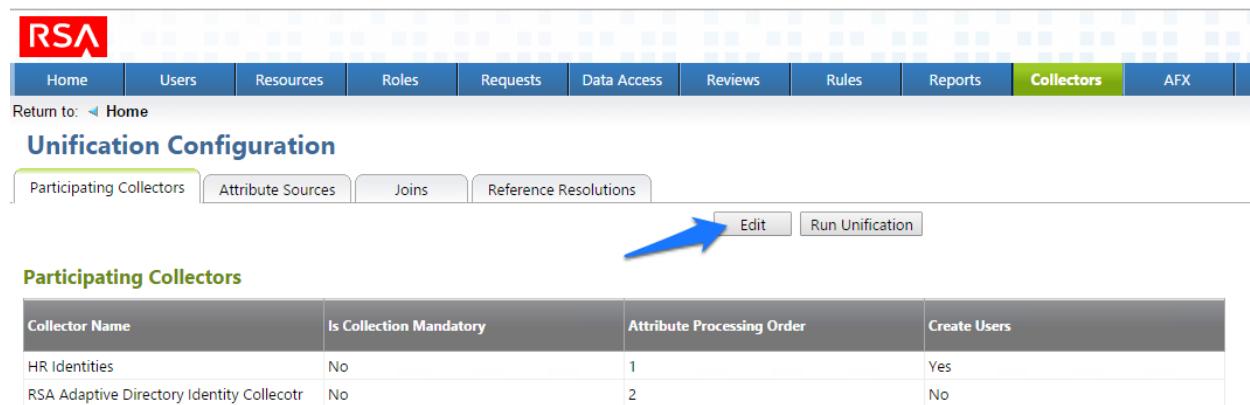
1449 1. Click on ‘Collectors’ and ‘Unification Config’ as shown in Figure 49.



1450

1451 *Figure 49. IMG Unification Configuration*

1452 2. Choose the Participating Collectors tab. Click on Edit as shown in Figure 50.



1453

Schedule: Not Scheduled

1454

Figure 50. IMG Participating Collectors

1455 3. Configure as shown in Figure 51 and Figure 52. Click Next on each screen.

Edit Participating Collectors

Edit Collector Participation and Unification Schedule

Collector Name	Collection Mandatory	Create Users
HR Identities	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RSA Adaptive Directory Identity Collector	<input type="checkbox"/>	<input type="checkbox"/>
Scheduled :	<input type="radio"/> Yes <input checked="" type="radio"/> No	

1456

1457

Figure 51. IMG Edit Participating Collectors

Edit Participating Collectors

Select Processing Order for Participating Collectors

Attribute Processing Order	
HR Identities	
RSA Adaptive Directory Identity Collector	

1458

1459

Figure 52. IMG Edit Participating Collectors

1460 In the above example, we have HR Identities at the top. This indicates that HR Identities is
 1461 authoritative source – if there are any discrepancies between the data between the two, then
 1462 the one at the top will win by default, but this can be overridden, which we will see later.

1463 4. Click Finish.

7.3.7 Edit Unification Configuration Attribute Source

1464 The next step is to change the default behavior of the authoritative source for the necessary
 1465 attributes.

1466 1. Choose the Attribute Sources tab. Click on Edit as shown in Figure 53.

Unification Configuration

Participating Collectors **Attribute Sources** Joins Reference Resolutions

Edit

User Attribute	Authoritative Source
Backup Supervisor	* Not Set *
Business Unit Id	* Not Set *
DN	RSA Adaptive Directory Identity Collector
Department	* Not Set *
Email Address	* Not Set *
Exception Count	* Not Set *
Expiration Date	* Not Set *
Expiration Value	* Not Set *

1468

1469

Figure 53. IMG Unification Configuration Attribute Sources

1470 2. Edit the Attributes shown in Figure 54 and Figure 55. Leave alone any attribute shown as
 1471 'Not Set'. These attributes will use the default behavior:

Edit User Attribute Mapping

User Attribute	Authoritative Source
Backup Supervisor :	(not collected)
Business Unit Id :	* Not Set *
DN :	RSA Adaptive Directory Identity Colle
Department :	* Not Set *
Email Address :	* Not Set *
Exception Count :	(not collected)
Expiration Date :	(not collected)
Expiration Value :	(not collected)
First Name :	* Not Set *
Full Name :	* Not Set *
Is App Owner :	(not collected)
Is Manager :	* Not Set *
Is Monitor :	(not collected)
Is Senior Manager :	(not collected)
Is Terminated :	* Not Set *
Job Code :	* Not Set *
Job Family :	* Not Set *
Job Level :	* Not Set *
Job Status :	* Not Set *

1472

1473

Figure 54. IMG Edit User Attribute Mapping

Last Name :	<input type="text" value="* Not Set *"/>
Location :	<input type="text" value="* Not Set *"/>
Login ID :	<input type="text" value="* Not Set *"/>
OU :	<input type="text" value="* Not Set *"/>
Other :	<input type="text" value="* Not Set *"/>
PACS All Doors :	<input type="text" value="RSA Adaptive Directory Identity Collector"/>
PACS Home Access :	<input type="text" value="RSA Adaptive Directory Identity Collector"/>
PACS Work Access :	<input type="text" value="RSA Adaptive Directory Identity Collector"/>
Previous Supervisor :	(not collected)
Self Reviewer :	<input type="text" value="* Not Set *"/>
Termination Date :	(not collected)
Title :	<input type="text" value="* Not Set *"/>
Transfer Date :	(not collected)
Unique Id :	<input type="text" value="* Not Set *"/>
User Risk Level :	(not collected)

1474

1475

Figure 55. IMG Edit User Attribute Mapping

1476

3. Click on OK.

1477

7.3.8 Edit Unification Configuration Attribute Source

1478 The next step is to configure which attribute to use from each directory so IMG knows how to
 1479 tie users together.

1480

1. Choose the Joins tab. Click on Edit as shown in Figure 56.

1481

Return to: [Home](#)

Unification Configuration

Participating Collectors Attribute Sources **Joins** Reference Resolutions

Joined Collectors

HR Identities : RSA Adaptive Directory Identity Collecotr

Join Criteria

HR Identities.User Id = RSA Adaptive Directory Identity Collecotr.User Id

Edit

1482

1483

Figure 56. IMG Unification Configuration Joins

1484 2. Choose the HR Identities from the Primary Identity Collector dropdown box as shown in
 1485 Figure 57.

Edit Joins

Join Criteria

Only Identity Collectors that are set to Create Users are available in the Primary Collector selection below. All active Identity Collectors are available in the Secondary Collector selection.

Primary Identity Collector Attribute Operator Secondary Identity Collector Attribute

HR Identities User Id = RSA Adaptive Directory User Id

[Add More...](#)

1486

1487

Figure 57. IMG Edit Joins

1488 3. Click 'Finish'.

1489 7.3.9 Start Data Collection

1490 The next step is to start collecting identity data.

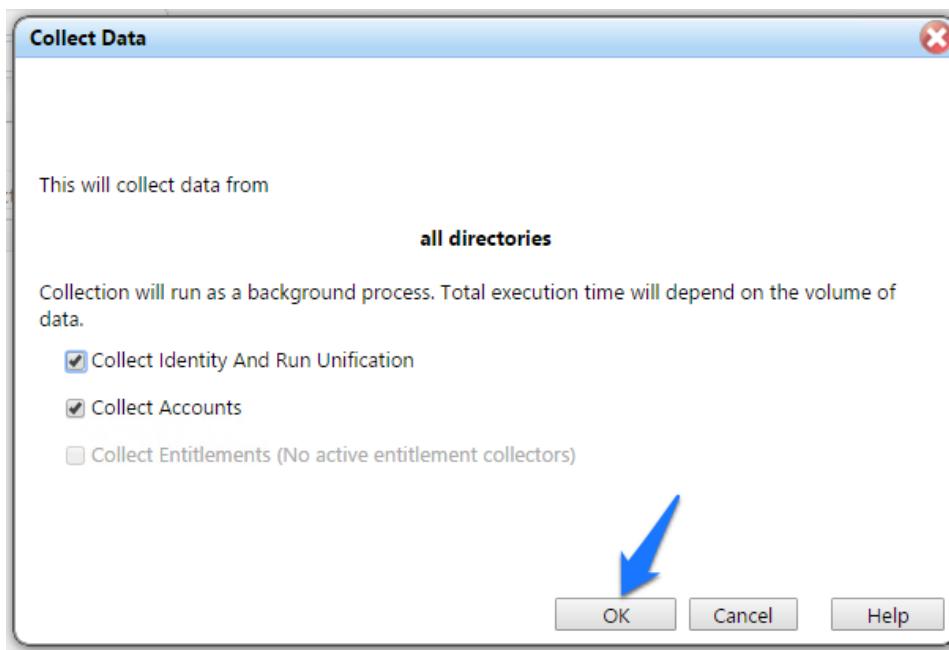
1491 1. From the home page choose the Resources > Directories tab. Click Collect Data (all)
 1492 button as shown in Figure 58.

1493

1494

1495 *Figure 58. IMG Start Data Collection*

1496 2. Click OK on the next window as shown in Figure 59.



1499 3. The process will take 30 seconds or so to complete. You can check the progress under
1500 'Admin' and 'Monitoring' as shown in Figure 60.

The screenshot shows the RSA Monitoring interface. The top navigation bar includes links for Home, Users, Resources, Roles, Requests, Data Access, Reviews, Rules, Reports, Collectors, AFX, and Admin. The Admin link is highlighted with a green background. A blue arrow points from the 'Monitoring' link in the top navigation to the 'Monitoring' tab in the sub-navigation bar. The sub-navigation bar also includes links for System, Monitoring (which is highlighted with a green background), User Interface, Attributes, Descriptions, Dashboards, Workflow, Email, Change Events, Web Services, Import/Export, and Admin Errors. The main content area displays a table of data collection processes. The table columns are: Run, Run Type, Source(s), Queue Start, Queue Time, Run Start, Run End, Run Time, Processing Time, and Status. The table shows five rows of data, all of which are marked as 'Completed' in the Status column. The status bar at the bottom of the interface also shows 'Completed'.

Run	Run Type	Source(s)	Queue Start	Queue Time	Run Start	Run End	Run Time	Processing Time	Status
1591	Rules Pre-processing	--	3/23/15 6:04 PM	00:00:00	3/23/15 6:04 PM	3/23/15 6:04 PM	00:00:00	00:00:00	Completed
1590	Business Description Processing	RSA AD Directory Accounts	3/23/15 6:04 PM	00:00:01	3/23/15 6:04 PM	3/23/15 6:04 PM	00:00:00	00:00:00	Completed
1589	Change Verification	RSA AD Directory Accounts	3/23/15 6:04 PM	00:00:01	3/23/15 6:04 PM	3/23/15 6:04 PM	00:00:00	00:00:00	Completed
1588	Rule Processing	Termination	3/23/15 6:04 PM	00:00:03	3/23/15 6:04 PM	3/23/15 6:04 PM	00:00:01	00:00:01	Completed
1587	Rule Processing	Movers	3/23/15	00:00:03	3/23/15	3/23/15	00:00:00	00:00:00	Completed

Figure 60. IMG Data Collection Monitoring

1501

1502

1503 You will see all the processes change to 'Complete' when done.

1504 7.3.10 Review Data Collected

1505 Now you can look at this data by going to 'Users' then 'Users' and 'Groups'.

1506 1. From the home page choose the Users > Groups tab as shown in Figure 61 to review the data collected.

1507

1508

Name	Department	Title	Supervisor	Is Deleted	Is Terminated	Termination Date	OU
AveksaAdmin,	--	--	--	No	No	--	--
ITInfrUser, Tony2	Energy Marketing	EM Department Head	--	No	No	--	it
ITInfrUser, Jon	Energy Marketing	EM Department Head	--	Yes	Yes	3/18/15 3:04 PM	it
ITApplUser, Ron	Energy Marketing	Energy Marketing Trader	--	Yes	Yes	3/17/15 10:58 PM	it
ITApplUser, Ron2	Energy Marketing	Energy Marketing Representative	--	Yes	Yes	3/17/15 10:58 PM	it
OTOpsInfrUser, Jim	Energy Operations A	Ops Department Manager	--	Yes	Yes	3/17/15 10:58 PM	ot
OTOpsInfrUser, Jim2	Energy Operations B	Ops Department Manager	--	Yes	Yes	3/17/15 10:58 PM	ot

1509

1510

Figure 61. IMG Data Collection Review

1511

7.3.11 Configure Business Rules

1512

The next step is to configure Business Roles.

1513

1. Click on Roles > Roles as shown in Figure.

Show:	Latest Versions	Pending Changes
Grouping: -- select --		

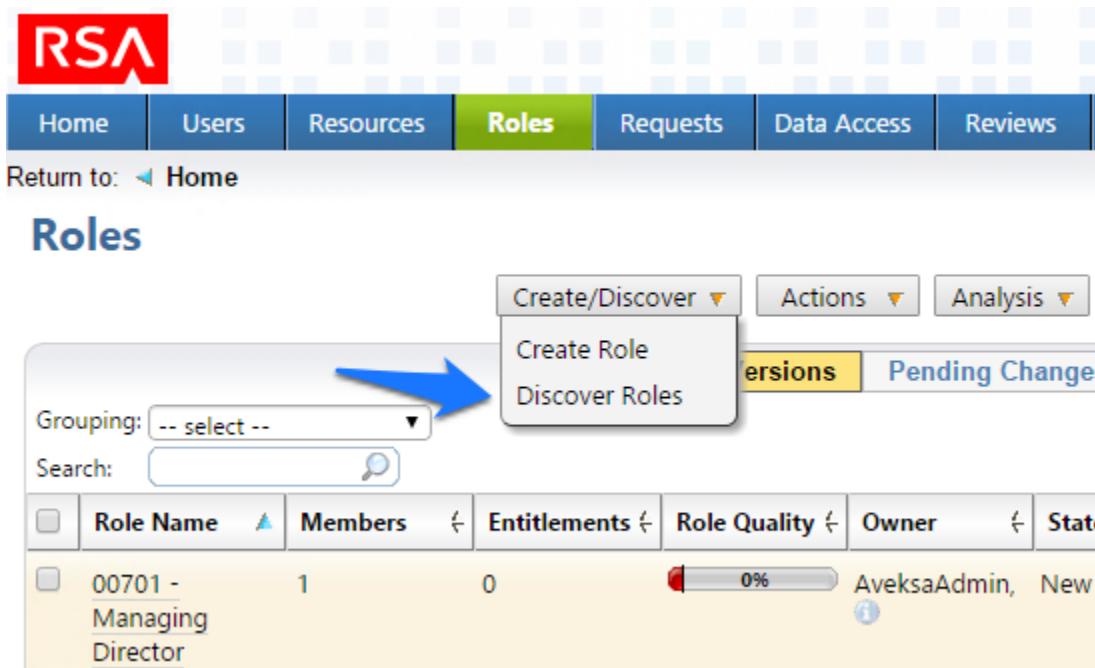
1514

1515

Figure 62. IMG Roles

1516

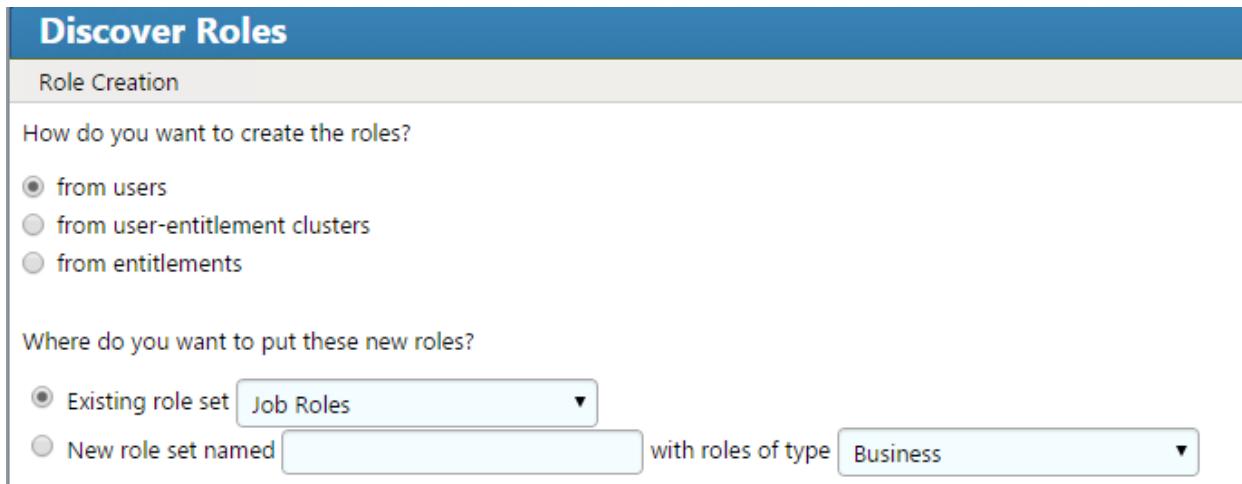
2. Click on 'Create / Discover' and 'Discover Roles' as shown in Figure 63.



The screenshot shows the RSA Roles page. At the top, there is a navigation bar with links: Home, Users, Resources, Roles (highlighted in green), Requests, Data Access, and Reviews. Below the navigation bar, a message says "Return to: Home". The main title is "Roles". On the right side of the page, there is a context menu with options: Create/Discover (with sub-options Create Role and Discover Roles), Actions, and Analysis. A blue arrow points from the "Discover Roles" option in the context menu to the "Discover Roles" link in the "Create/Discover" dropdown. The main content area shows a table with a single row of data. The table columns are: Role Name, Members, Entitlements, Role Quality, Owner, and Status. The data row shows: 00701 - Managing Director, 1, 0, 0%, AveksaAdmin, New.

Figure 63. IMG Discover Roles

1517 3. Configure as follows as shown in Figure 64 through Figure 66.



The screenshot shows the "Discover Roles" configuration page. The title is "Discover Roles". The first section is "Role Creation" with the sub-question "How do you want to create the roles?". There are three radio buttons: "from users" (selected), "from user-entitlement clusters", and "from entitlements". The second section is "Where do you want to put these new roles?". There are two radio buttons: "Existing role set" (selected) with a dropdown menu showing "Job Roles", and "New role set named" with an input field and a dropdown menu showing "Business".

1520

1521

Figure 64. IMG Discover Roles

Discover Roles

Role Creation

Roles will be created for each unique combination of user attributes.

Users matching [All](#) (matches 299 out of 299).

Create Roles Split on these Attributes

User.Job Code ▼ [58 unique values](#)

User.Title ▼ [58 unique values](#)

[Add More...](#)

66 Roles would be created

Suggest Entitlements Add suggested entitlements to roles

Suggest Entitlements Matching [All](#) (matches 397 out of 397)

1522

1523

Figure 64. IMG Discover Roles

Discover Roles

Role Information Expressions

What expressions should be used to generate role information?

Name	<code> \${User.Job Code} - \${User.Title}</code>	▼
Last Reviewed Date		▼
Risk		▼

1524

1525

Figure 66. IMG Discover Roles

1526
1527

4. Notice how there are some duplicates – the job codes are the same, but the descriptions are slightly different. You can combine these rolls into one as shown in Figure 67:

Discover Roles

Role Creation

For each row in the table below a new role will be created. The selection checkboxes are used to identify roles for use with the button bar below the table.

<input type="checkbox"/> Role Name	Members
<input type="checkbox"/> 00701 - Managing Director	1
<input type="checkbox"/> 00702 - Executive Assistant	1
<input type="checkbox"/> 00703 - Business Strategist	1
<input type="checkbox"/> 10100 - Chief Executive Officer	1
<input checked="" type="checkbox"/> 10101 - AM Department Manager	1
<input checked="" type="checkbox"/> 10101 - IT Department Manager	1
<input type="checkbox"/> 10102 - Lead Infr Admin	1
<input type="checkbox"/> 10102 - Sr Infr Admin	3

Items 1 - 50 of 66 | 2 selected

Hide Entitlements That Are Already Used In Committed Roles

Hide Entitlements That Are Already Used In New Uncommitted Roles

Suggest entitlements that of members have

1528

Figure 67. IMG Discover Roles

1529 5. When you are done combining duplicates, click Finish.

1530 7.3.12 **Create Automated Rules**

1531 The next step is to create rules for automatically detecting and invoking work flows for new users and terminations.

1532 1. Click on 'Rules' and 'Definitions' as shown in Figure 68.

1533

1534

1536

Figure 68. IMG Roles Definitions

1537

2. Click on 'Create Rule' and configure as shown in Figure 69 and Figure 70 for New Users.

Edit Rule: New User

Rule Name* :	New User
Description :	
Owner* :	AveksaAdmin, 
Control URL :	
Control Description :	
Type* :	Provisioning - Joiner/Mover
Status* :	Active
Rule Set* :	<input checked="" type="radio"/> Existing rule set <input type="radio"/> New rule set named Default Rule Set

Condition

Trigger when new users are detected (joiners)
 Trigger when users change categories (movers)

Actions

Assign provisioning request form Default Provisioning Form 

Provisioned entitlements*:
Entitlement Suggestion Modeling 
 For these users: All
 Categorize them based on: Job Code
 Consider the following entitlements when making suggestions: All
 Suggested entitlements that 0% of members have

1538

1539

Figure 69. IMG New User

1540

Optional entitlements that 0% of members have

Allow arbitrary entitlements
Allow selection from All 

Allow user comparisons

Assignee*:

Supervisor
 Specified by target user attribute
 Selected user

For movers also generate a review using review definition:

Processing Schedule/Trigger

Use global configuration Define for this rule

Scheduled : Yes No

Triggered : Run after identity unification

1541

1542

1543 3. Click on 'Create Rule' and configure as shown in Figure 71 and Figure 72 for User
1544 Terminations.

Figure 70. IMG New User

Edit Rule: Termination

Rule Name* : **Termination**

Description :

Owner* : AveksaAdmin 

Control URL :

Control Description :

Type* : Provisioning - Termination

Status* : Active

Rule Set* : Existing rule set **Default Rule Set** New rule set named

Condition

Condition* : For terminated users matching the following condition
IT Users 

Actions

Each action will submit a separate change request

Disable accounts (excludes shared and service accounts)

Delete accounts (excludes shared and service accounts)

For particular accounts All 

Perform this action

Immediately After days

1545

1546

Figure 71. IMG User Termination

- Revoke user entitlements (excludes shared and service accounts)
- Shared Accounts
- Service Accounts

Processing Schedule/Trigger

Use global configuration Define for this rule

Scheduled : Yes No

Triggered : Run after identity unification

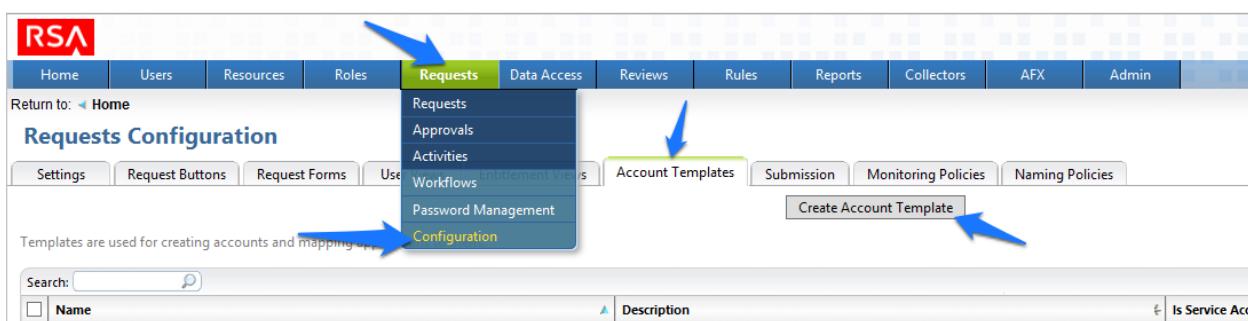
1547

1548

Figure 72. IMG User Termination

1549

1550 4. Click 'OK'.

1551 7.3.13 [Create Provisioning Template](#)1552 The next step is to create a template that IMG uses when provisioning accounts in Adaptive
1553 Directory:1554 1. Click on 'Requests', 'Configuration', 'Account Template' tab, then 'Create Account
1555 Template' as shown in Figure 73 .

1556

1557 Figure 73. IMG Request Configuration

1558 2. Enter a name, and click OK as shown in Figure 74.

1559

1560 Figure 74. IMG Account Template

1561 3. Click on the name of the account template you just created and add parameters as
1562 shown in Figure 75.

Account Template: IT Account Template

Name: IT Account Template
Is Service Account: No

Template Parameters

Pending Account Parameters

Action	Name	Default Value	Submission Field
Edit	CN	<code>\$(User.Login_ID)</code>	
Edit	sn	<code>\$(User.Last_Name)</code>	
Edit	sAMAccountName	<code>\$(User.Login_ID)</code>	
Edit	mail	<code>\$(User.Email_Address)</code>	
Edit	Account	<code>\$(User.Login_ID)</code>	
Edit	userPrincipalName	<code>\$(User.Email_Address)</code>	
Edit	Password	<code>\$(GeneratedPassword)</code>	
Edit	givenName	<code>\$(User.First_Name)</code>	

8 items [Delete](#)

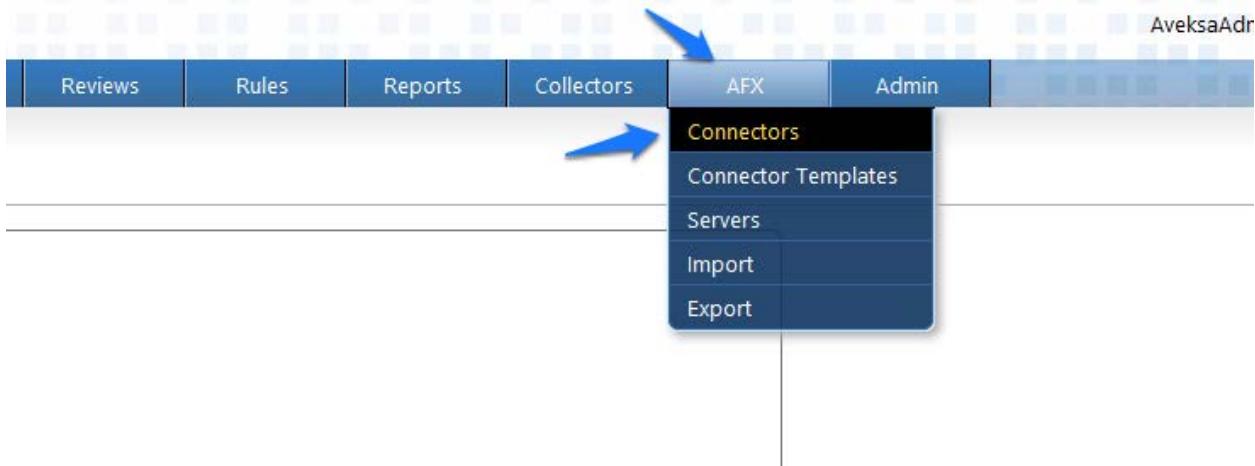
1563

1564

Figure 75. IMG IT Account Template

1565 Next configure the IMG AFX module which will allow IMG to provision to Adaptive Directory:

1566 4. Click on 'AFX' and 'Connectors' as shown in Figure 76.



1567

1568

Figure 76. IMG AFX Connectors

1569 5. Click on 'Create Connector' as shown in Figure 77.



1570

Figure 77. IMG Create Connector

1571

6. Configure the 'General' tab as shown in Figure 78.

A screenshot of the 'Edit Connector: RSA Adaptive Directory Connector' configuration page. The page has a header with three tabs: 'General' (which is selected and highlighted in blue), 'Settings', and 'Capabilities'. Below the tabs, there are several configuration fields:

- 'Name*' input field: 'RSA Adaptive Directory Connector'. A blue arrow points upwards to the left of this field.
- 'Description' input field: An empty text area.
- 'Server*' dropdown menu: 'AFX Server'.
- 'State' dropdown menu: 'Active'.
- 'Export As Template' input field: An empty text area.

1572

1573

Figure 78. IMG AD Connector AFX Server

1574

7. Configure the 'Settings' tab as shown in Figure 79 through Figure 81.

Edit Connector: RSA Adaptive Directory Connector IT

General **Settings** **Capabilities**

Connection Details

Host* : 172.16.4.3

Port* : 1636

Use Secure : Connection

Login Distinguished Name* : cn=Directory Manager

Password* : *****

Timeout (seconds)* : 10

Distinguished Name

Account DN Prefix : CN

Account DN Suffix : dc=master,dc=test

Group DN Prefix : CN

Group DN Suffix : dc=master,dc=test

DN Suffix Mappings : (empty)

1576

1577

Figure 79. IMG AD Connector AFX Server

Edit Connector: RSA Adaptive Directory Connector IT

General **Settings** **Capabilities**

Connection Details

Host* : 172.16.4.3

Port* : 1636

Use Secure : Connection

Login Distinguished Name* : cn=Directory Manager

Password* : XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Timeout (seconds)* : 10

Distinguished Name

Account DN Prefix : CN

Account DN Suffix : dc=master,dc=test

Group DN Prefix : CN

Group DN Suffix : dc=master,dc=test

DN Suffix Mappings :

1578

1579

Figure 80. IMG AD Connector AFX Server

Object Creation

LDAP object classes to : create account*	'top','person','organizationalPerson','user'
LDAP object classes to : create group*	'top','group'

Group

User membership : attribute for Group*	member
---	--------

AccountLockUnlock

Account Lockout : Threshold attribute value*	10
--	----

Miscellaneous

Dependent Exchange : Connector	<input type="button" value="▼"/>
-----------------------------------	----------------------------------

1580

1581

1582

Figure 81. IMG AD Connector AFX Server

8. Configure the 'Capabilities' tab as shown in Figure 82.

Edit Connector: RSA Adaptive Directory Connector IT

General	Settings	Capabilities 
Account <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Create an Account on an AD server <input checked="" type="checkbox"/> Delete an Account from an AD server <input checked="" type="checkbox"/> Reset an Account's password <input checked="" type="checkbox"/> Add Account to AD Group <input checked="" type="checkbox"/> Remove Account from AD Group <input checked="" type="checkbox"/> Enable an Account <input checked="" type="checkbox"/> Disable an Account <input checked="" type="checkbox"/> Update an Account <input checked="" type="checkbox"/> Move an Account <input checked="" type="checkbox"/> Lock an Account <input checked="" type="checkbox"/> Unlock an Account Group <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Create a Group on an AD server <input checked="" type="checkbox"/> Delete a Group from an AD server <input checked="" type="checkbox"/> Update a Group 		

1583

1584

Figure 82. IMG AD Connector IT

1585

1586 9. Check all capabilities needed for to the connector. Once all are selected, click on the
1587 capability name one by one and configure as shown in Figure 83 through Figure 96.

Edit Connector: RSA Adaptive Directory Connector IT

General **Settings** **Capabilities**

Account

- Create an Account on an AD server ←
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account
- Unlock an Account

Group

- Create a Group on an AD server
- Delete a Group from an AD server
- Update a Group

Create an Account on an AD server

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING	Not_Available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(AccountTemplate.Name)</code>	Full DN
sAMAccountName	STRING	Not_Available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	sAMAccountName	<code>\$(AccountTemplate.sAMA</code>	Logon name used to support clients and servers running earlier v
CN	STRING	Not_Available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Common Name	<code>\$(AccountTemplate.CN)</code>	Name that represents an object. It is used to perform searches
sn	STRING	Not_Available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Last Name	<code>\$(AccountTemplate.sn)</code>	Surname of a person
givenName	STRING	Not_Available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	First Name	<code>\$(AccountTemplate.given</code>	A given name of a person
mail	STRING	Not_Available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Email address	<code>\$(AccountTemplate.mail)</code>	Simple SMTP address of a person
Password	STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Initial password to set	<code>\$(AccountTemplate.Passe</code>	Password which is required for login
userPrincipalName	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	UserPrincipalName	<code>\$(AccountTemplate.userPri</code>	UserPrincipalName (Email Address)

Add More...

Command Output Parameters

Parameter Name	Type	Attribute	Display Name	Mapping	Description

Add More...

Figure 83. IMG AD Connector IT Capability Configuration

1588

1589

1590

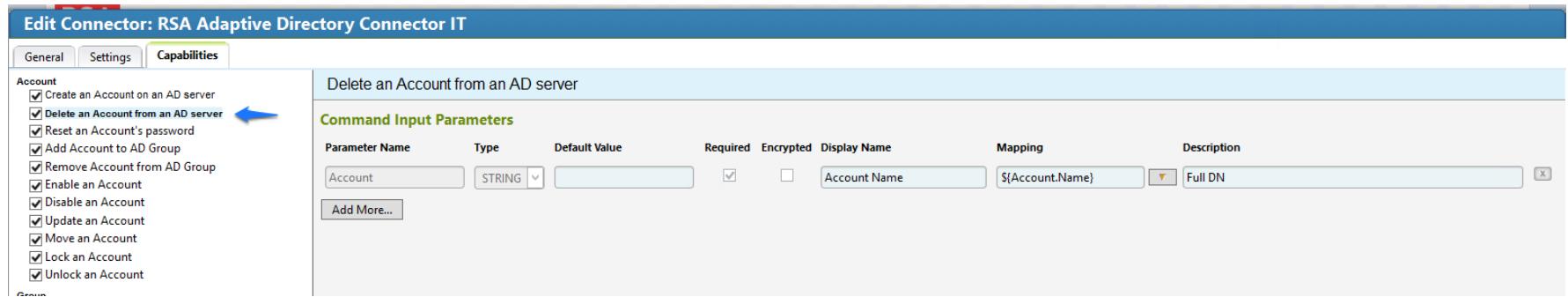
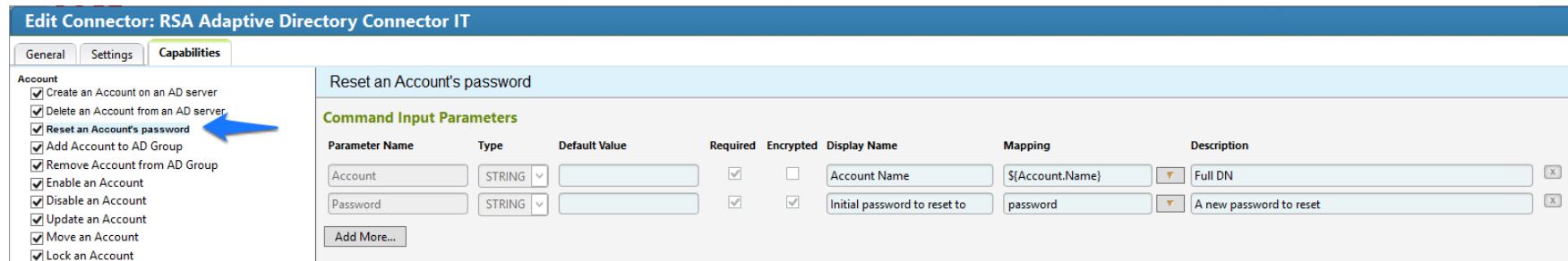


Figure 84. IMG AD Connector IT Capability Configuration

1591



1592

1593

Figure 85. IMG AD Connector IT Capability Configuration

Edit Connector: RSA Adaptive Directory Connector IT

General **Settings** **Capabilities**

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group 
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account
- Unlock an Account

Group

- Create a Group on an AD server
- Delete a Group from an AD server
- Update a Group

Add Account to AD Group

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account DN or Account Name	<code>\$(Account.Name)</code>	Full DN
Group	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Group DN or Group Name	<code>\$(Group.Name)</code>	Full DN of group or group name

Add More...

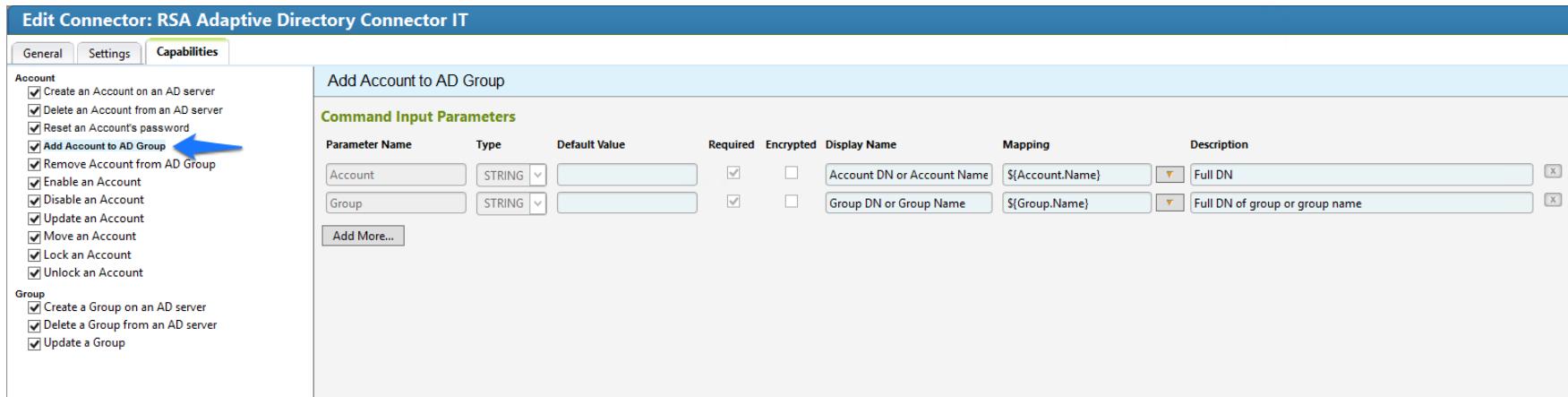


Figure 86. IMG AD Connector IT Capability Configuration

1594

1595
1596

Edit Connector: RSA Adaptive Directory Connector IT

Capabilities

Account	
<input checked="" type="checkbox"/>	Create an Account on an AD server
<input checked="" type="checkbox"/>	Delete an Account from an AD server
<input checked="" type="checkbox"/>	Reset an Account's password
<input checked="" type="checkbox"/>	Add Account to AD Group
<input checked="" type="checkbox"/>	Remove Account from AD Group
<input checked="" type="checkbox"/>	Enable an Account
<input checked="" type="checkbox"/>	Disable an Account
<input checked="" type="checkbox"/>	Update an Account
<input checked="" type="checkbox"/>	Move an Account
<input checked="" type="checkbox"/>	Lock an Account
<input checked="" type="checkbox"/>	Unlock an Account
Group	
<input checked="" type="checkbox"/>	Create a Group on an AD server
<input checked="" type="checkbox"/>	Delete a Group from an AD server

Remove Account from AD Group

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account DN or Account Name	<code>\$(Account.Name)</code>	Full DN
Group	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Group DN or Group Name	<code>\$(Group.DN)</code>	Full DN of group or group name

Add More...

Figure 87. IMG AD Connector IT Capability Configuration

1597
1598

Edit Connector: RSA Adaptive Directory Connector IT

Capabilities

Account	
<input checked="" type="checkbox"/>	Create an Account on an AD server
<input checked="" type="checkbox"/>	Delete an Account from an AD server
<input checked="" type="checkbox"/>	Reset an Account's password
<input checked="" type="checkbox"/>	Add Account to AD Group
<input checked="" type="checkbox"/>	Remove Account from AD Group
<input checked="" type="checkbox"/>	Enable an Account
<input checked="" type="checkbox"/>	Disable an Account
<input checked="" type="checkbox"/>	Update an Account
<input checked="" type="checkbox"/>	Move an Account
<input checked="" type="checkbox"/>	Lock an Account

Enable an Account

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(Account.Name)</code>	Full DN

Add More...

Figure 88. IMG AD Connector IT Capability Configuration

1599
1600

1601

Edit Connector: RSA Adaptive Directory Connector IT

Capabilities

Account	
<input checked="" type="checkbox"/>	Create an Account on an AD server
<input checked="" type="checkbox"/>	Delete an Account from an AD server
<input checked="" type="checkbox"/>	Reset an Account's password
<input checked="" type="checkbox"/>	Add Account to AD Group
<input checked="" type="checkbox"/>	Remove Account from AD Group
<input checked="" type="checkbox"/>	Enable an Account
<input checked="" type="checkbox"/>	Disable an Account
<input checked="" type="checkbox"/>	Update an Account
<input checked="" type="checkbox"/>	Move an Account
<input checked="" type="checkbox"/>	Lock an Account
<input checked="" type="checkbox"/>	Unlock an Account

Disable an Account

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(Account.Name)</code>	Full DN

Add More...

Figure 89. IMG AD Connector IT Capability Configuration

1602

Edit Connector: RSA Adaptive Directory Connector IT

General Settings Capabilities

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account** ←
- Move an Account
- Lock an Account
- Unlock an Account

Group

- Create a Group on an AD server
- Delete a Group from an AD server

Update an Account

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(Account.Name)</code>	Full DN

Add More...

1603

Figure 90. IMG AD Connector IT Capability Configuration

1604

Edit Connector: RSA Adaptive Directory Connector IT

General Settings Capabilities

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account** ←
- Move an Account
- Lock an Account
- Unlock an Account

Move an Account

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(Account.Name)</code>	Full DN of account or login name
NewParentDN	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	New Parent's DN	<code>\$(Account.DN)</code>	DN of new account base or organizational unit

Add More...

1605

Figure 91. IMG AD Connector IT Capability Configuration

1607

1608

1609

1610

1611

Edit Connector: RSA Adaptive Directory Connector IT

General Settings Capabilities

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account ←
- Unlock an Account

Lock an Account

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(Account.Name)</code>	Full DN of account or login name

Add More...

Figure 92. IMG AD Connector IT Capability Configuration

Figure 92. IMG AD Connector IT Capability Configuration

1607

1608

1609

1610

1611

Edit Connector: RSA Adaptive Directory Connector IT

General Settings Capabilities

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account
- Unlock an Account ←

Unlock an Account

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Account	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Account Name	<code>\$(Account.Name)</code>	Full DN of account or login name

Add More...

Figure 93. IMG AD Connector IT Capability Configuration

Figure 93. IMG AD Connector IT Capability Configuration

1612

1613

1614

Edit Connector: RSA Adaptive Directory Connector IT

General **Settings** **Capabilities**

Create a Group on an AD server

Command Input Parameters

Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping	Description
Group	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Group Name	<code>\$(Group.Name)</code>	Full DN of group or group name
CN	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Common Name	<code>\$(Group.Name)</code>	Name that represents an object. It is used to perform searches
groupType	STRING	-2147483646	<input checked="" type="checkbox"/>	<input type="checkbox"/>	GroupType	<code>\$(Group.Resource_Type)</code>	Set of flags that define the type and scope of a group object

Add More...

Group

- Create a Group on an AD server 
- Delete a Group from an AD server
- Update a Group

Figure 94. IMG AD Connector IT Capability Configuration

1615

1616

1617

1618

1619

1620

Edit Connector: RSA Adaptive Directory Connector IT

Capabilities

Delete a Group from an AD server						
Command Input Parameters						
Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping
Group	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Group Name	\$(Group.Name)
<input type="button" value="Add More..."/>						

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account
- Unlock an Account

Group

- Create a Group on an AD server
- Delete a Group from an AD server** 
- Update a Group

1615

1616

1617

1618

1619

1620

Figure 95. IMG AD Connector IT Capability Configuration

Figure 95. IMG AD Connector IT Capability Configuration

1615

1616

1617

1618

1619

1620

Edit Connector: RSA Adaptive Directory Connector IT

Capabilities

Update a Group						
Command Input Parameters						
Parameter Name	Type	Default Value	Required	Encrypted	Display Name	Mapping
Group	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Group Name	\$(Group.Name)
<input type="button" value="Add More..."/>						

Account

- Create an Account on an AD server
- Delete an Account from an AD server
- Reset an Account's password
- Add Account to AD Group
- Remove Account from AD Group
- Enable an Account
- Disable an Account
- Update an Account
- Move an Account
- Lock an Account
- Unlock an Account

Group

- Create a Group on an AD server
- Delete a Group from an AD server** 
- Update a Group

1615

1616

1617

1618

1619

1620

10. Click OK.

Figure 96. IMG AD Connector IT Capability Configuration

1621 7.3.14 Configure Adaptive Directory to Use AFX Connector
 1622 The next step is to configure the RSA Adaptive Directory 'Directory' to use the new AFX
 1623 Connector.

1624 1. Click on Resources > Directories tab as shown in Figure 97 and select HR and click OK.

The screenshot shows the RSA Adaptive Directory interface. The top navigation bar has tabs for Home, Users, Resources (which is highlighted in green), Roles, Requests, Data Access, Reviews, Rules, and Reports. Below the navigation bar, a 'Return to: < Home' link is followed by a 'Directories' link with a blue arrow pointing to it, and an 'Applications' link. A 'Create Directory' and 'Collect Data (all)' button are also present. The main content area is titled 'Directories' and shows a table with two items: 'HR' and 'RSA Adaptive Directory Accounts'. The 'HR' item has a checkbox and a description of '--' with 'AveksaAdmin,' as the Business Owner. The 'RSA Adaptive Directory Accounts' item also has a checkbox and a description of '--' with 'AveksaAdmin,' as the Business Owner. A blue arrow points to the 'HR' entry in the list.

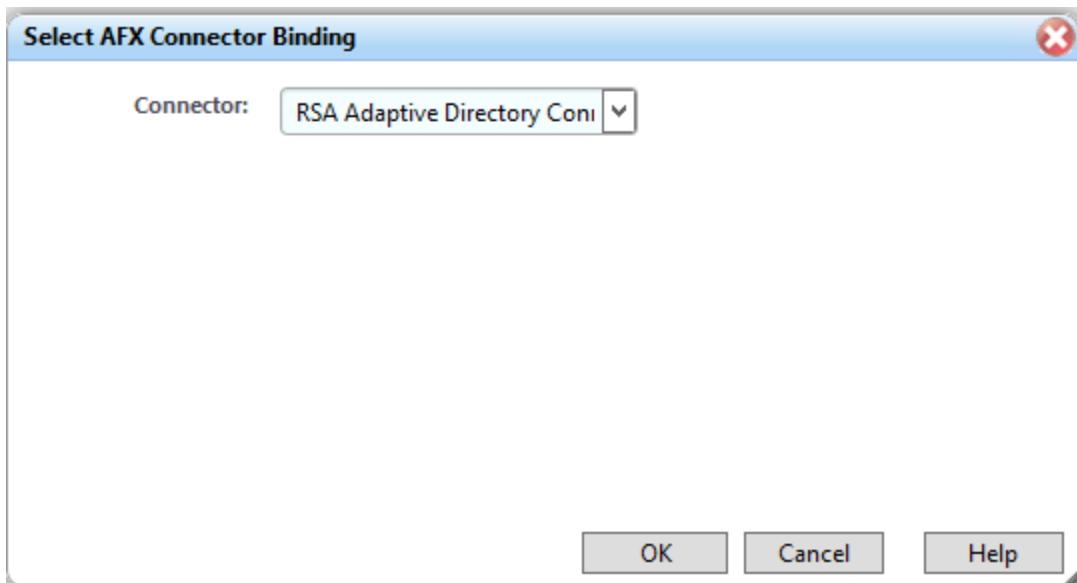
1625
 1626 *Figure 97. IMG Resources Directories*
 1627 2. Then in the next window choose the AFX Connector Binding tab as shown in Figure 98.
 1628 3. Click the Edit Connector Binding as shown in Figure 98.

The screenshot shows the 'Directory: RSA Adaptive Directory Accounts' page. The top navigation bar is identical to Figure 97. The main content area is titled 'Directory: RSA Adaptive Directory Accounts' and shows a tab bar with General, AFX Connector Binding (which is highlighted in green), Collectors, Accounts, Who Has Access, What Access, Resource Profile, and Requests. A blue arrow points to the 'Edit Connector Binding' button. Below the tabs, a message says 'Connector: mapped to AFX Connector RSA Adaptive Directory Connector IT'.

1629

1630

Figure 98. IMG AD Accounts



1631

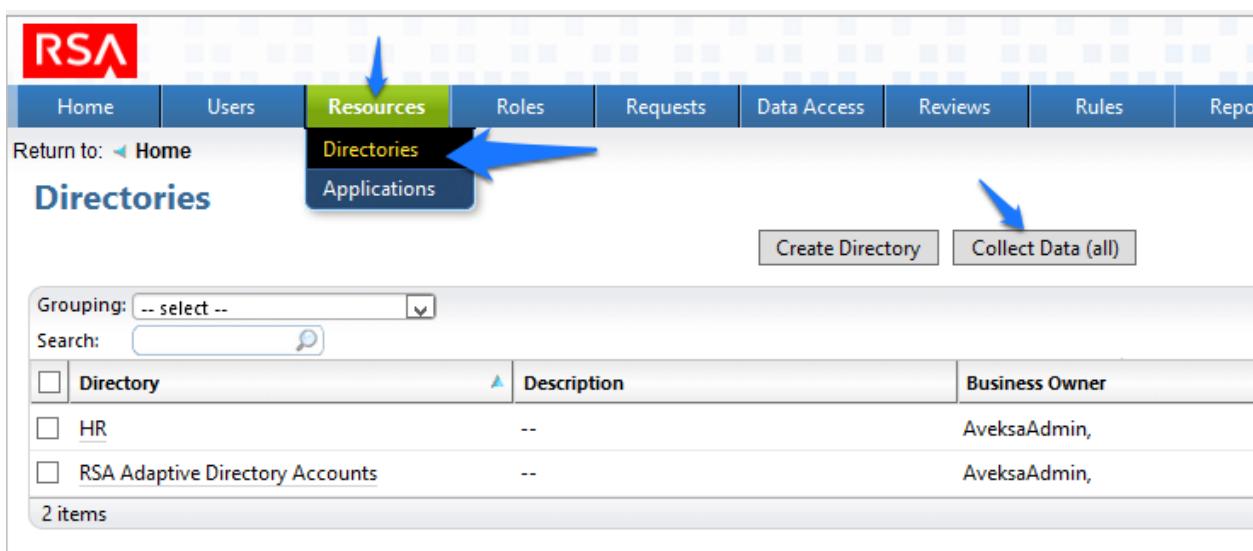
Figure 99. IMG AD AFX Connector Binding

1632 4. Click OK as shown in Figure 99.

1633 Now the system is ready.

1634 **7.4 USING RSA IMG**1635 7.4.1 **Adding a New User**

1. Open the HR CSV file and add a user.
2. Go to 'Resources', 'Directories' and click 'Collect Data (all)' as shown in Figure 100.



1639

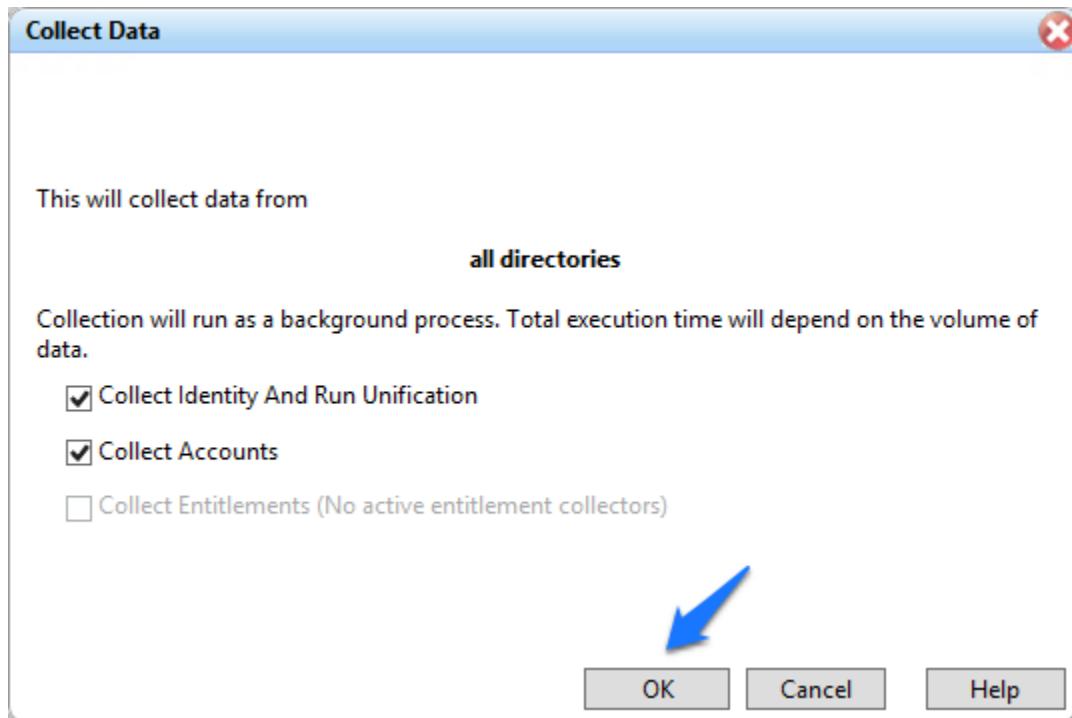
1640

Figure 100. IMG Resources Directories

1641

1642

1. Click 'OK' as shown in Figure 101.



1643

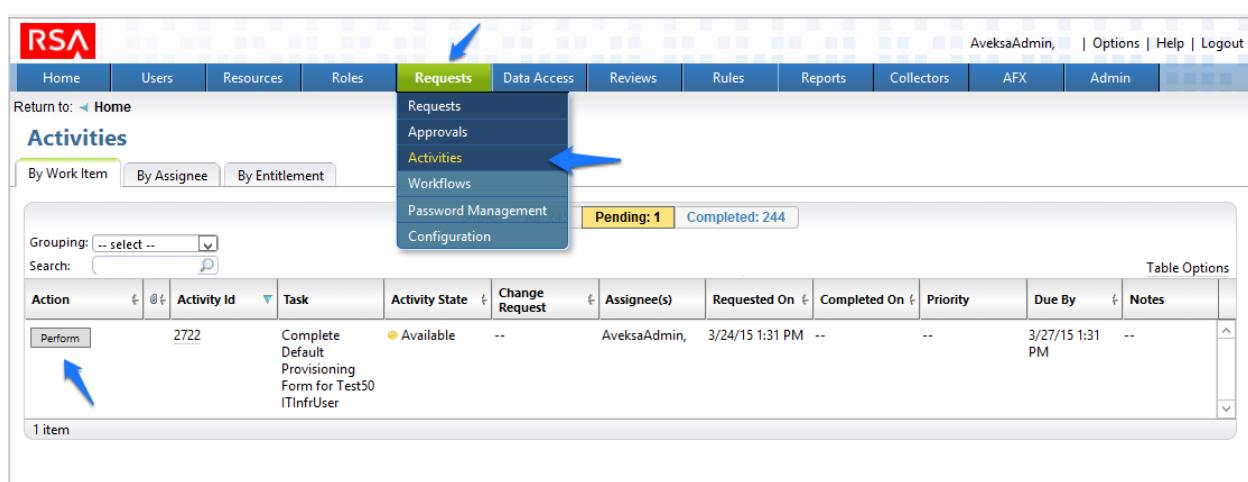
1644

Figure 101. IMG Collect Data

1645

1646

2. After about 30 seconds go to 'Requests', 'Activities' and click 'Perform' next to the request to add a new user as shown in Figure 102.



1647

1648

Figure 102. IMG Requests Activities

1649 3. Select a group you would like to add the user to, Click 'Next', then 'Accepted' as shown in
 1650 Figure 103.

Access Request: ITInfrUser, Test50

Default Provisioning Form

Please select the entitlements Test50 ITInfrUser should have. The suggested entitlements represent the access the system thinks this user should have based on the provisioning rule 'New User'. The optional entitlements represent additional access the system also thinks the user might need.

Suggested Entitlements (At least 0% of the users have these entitlements)

Grouping: Business Source Name ▾

Entitlement Name	Entitlement Type	% of User Have This Entitlement	DN	Description	Domain
<input checked="" type="checkbox"/> RSA Adaptive Directory Accounts (2)					
<input type="checkbox"/> CN=Denied RODC Password Replication Group,ou=it,dc=master,dc=test	group	50	Denied RODC Password Replication Group	Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain	--
<input checked="" type="checkbox"/> CN=Domain Admins,ou=it,dc=master,dc=test	group	50	Domain Admins	Designated administrators of the domain	--

1 Group (2 total items | 1 selected)

Arbitrary Entitlements

Compare with a typical user

< Back Next Finish Cancel Help

Accepted
 Rejected
 Reassign

1651

Figure 103. IMG Accepted Access Request

1652 4. Enter a description if you wish, and click 'Finish'.
 1653 5. Go to 'Requests', and click 'Requests'. Click the name of the request as shown in Figure
 1654 104.

The screenshot shows the RSA Requests module. At the top, there is a navigation bar with tabs: Home, Users, Resources, Roles, Requests (highlighted in green), Data Access, Reviews, and Run. Below the navigation bar, a sub-menu is open under the Requests tab, listing: Requests, Approvals, Activities, Workflows, Password Management, and Configuration. A blue arrow points to the 'Requests' option in the sub-menu. Below the sub-menu, there is a 'Create Request' button and a 'Pending: 29' button. The main area displays a table of requests. The table has columns: Grouping (dropdown), Name, State, Requested By, and Requested On. A blue arrow points to the 'Name' column. The table shows two rows of data:

1656	00066	Fulfillment Phase	AveksaAdmin,	3/24,
------	-------	-------------------	--------------	-------

Figure 104. IMG Requests

1657

1658

1659 6. After about 30 seconds, your new user will be provisioned to AD and added to the group you selected as shown in Figure 105.

1660

The screenshot shows a detailed view of a request. At the top, there are 'Edit' and 'Cancel' buttons. Below them is a progress bar: Overall Status: 50% (1/2 (Fulfillment Phase)). The main area contains the following fields:

- Name: 00066
- Requested By: AveksaAdmin, on 3/24/15 1:53 PM
- Notes: --
- Workflow Jobs: Processing Workflow
- Email Log: Email Log
- AFX Log: AFX Log

Additional Information

Default Provisioning Form (For ITInfrUser, Test51)

AccountTemplate.Account: Test51ITInfrUser	AccountTemplate.sAMAccountName: Test51ITInfrUser
AccountTemplate.CN: Test51ITInfrUser	AccountTemplate.sn: ITInfrUser
AccountTemplate.givenName: Test51	AccountTemplate.userPrincipalName: Test51ITInfrUser@ES-IdAM-B1.TEST
AccountTemplate.mail: Test51ITInfrUser@ES-IdAM-B1.TEST	

Attachments

Browse... No file selected. Upload Attachment

Status

Details: Fulfillment: 50% 1/2 Changes Fulfilled (0/0 Activities)

Approval Phase

Fulfillment Phase

IT AFX Fulfillment

Changes processed by AFX handler

Verified

Account Changes

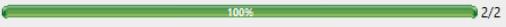
Status	Action	Account	Entitlement Type	Business Source	Entitlement	State
	Create	CN=Test51ITInfrUser,ou=it,dc=master,dc=test		RSA Adaptive Directory Accounts	ITInfrUser, Test51	Completed

1661

1662

Figure 105. IMG New User Provisioned

1663 Note: The state of the group add will remain pending, and the overall status will remain at 50%
 1664 until you recollect data from the Directories page so that IMG can detect that the user has been
 1665 added to the group successfully as shown in Figure 106.

Overall Status:  100% 2/2 (Fulfillment Phase)

Name: 00068	Requested By: AveksaAdmin, @ on 3/24/15 1:53 PM
Notes: --	Workflow Jobs: Processing Workflow
Email Log: Email Log	AFX Log: AFX Log @

Additional Information

 Default Provisioning Form @ (For ITInfrUser, Test51 @)	AccountTemplate.Account: Test51ITInfrUser	AccountTemplate.sAMAccountName: Test51ITInfrUser
	AccountTemplate.CN: Test51ITInfrUser	AccountTemplate.sn: ITInfrUser
	AccountTemplate.givenName: Test51	AccountTemplate.userPrincipalName: Test51ITInfrUser@ES-IdAM-B1.TEST
	AccountTemplate.mail: Test51ITInfrUser@ES-IdAM-B1.TEST	

Attachments

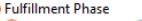
[Browse...](#) No file selected. [Upload Attachment](#)

Status

Details: Fulfillment:  100% 2/2 Changes Fulfilled (0/0 Activities)

  Approval Phase

  Fulfillment Phase



Account Changes

Status	Action	Account	Entitlement Type	Business Source	Entitlement	State
 	Create	CN=Test51ITInfrUser,ou=it,dc=master,dc=test	Owner	RSA Adaptive Directory Accounts	ITInfrUser, Test51	Completed
 	Add	CN=Test51ITInfrUser,ou=it,dc=master,dc=test	Group	RSA Adaptive Directory Accounts	CN=Domain Admins,ou=it,dc=master,dc=test	Completed

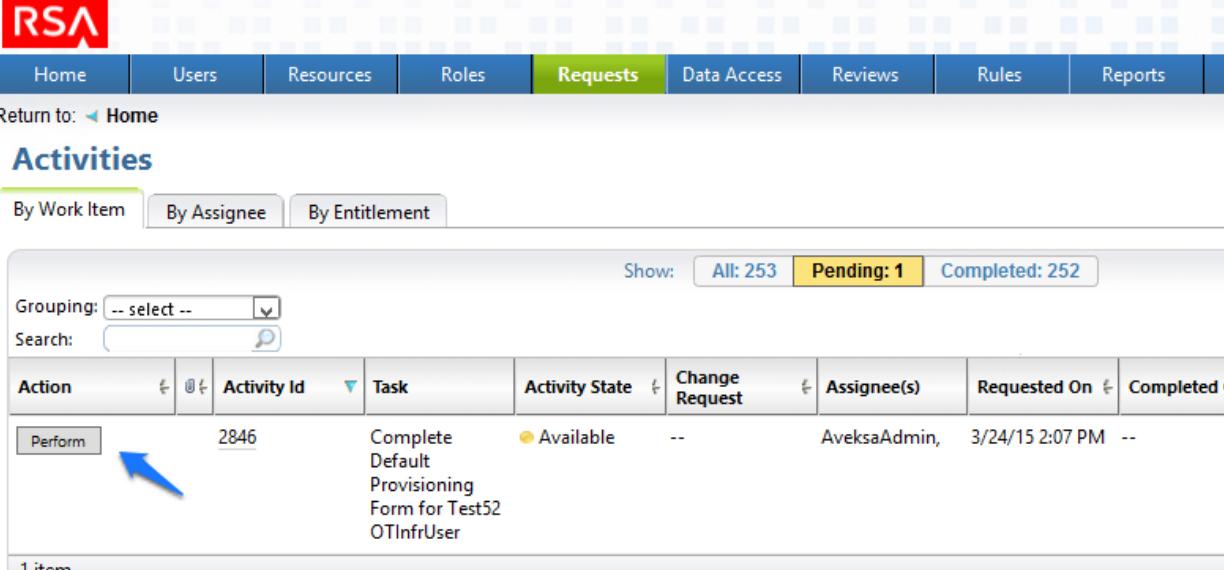
1666

1667

Figure 106. IMG Successful User Add

1668 7.4.2 Moving a User

1. Open your CSV file and change the attribute that defines the OU that the user is in to a different OU.
2. Collect data again.
3. The OU change is detected, and IMG deletes the user from the original OU and adds the user to the new OU.
4. Go to 'Requests' and 'Activities' and click 'Perform' as shown in Figure 107.



The screenshot shows the RSA Requests Activities page. The top navigation bar includes Home, Users, Resources, Roles, Requests (highlighted in green), Data Access, Reviews, Rules, Reports, and a dropdown menu. Below the navigation is a breadcrumb trail: Return to: Home. The main title is Activities, with sub-options: By Work Item (selected), By Assignee, and By Entitlement. A search bar and grouping dropdown are also present. The main content area displays a table of activities. The table columns are: Action, Activity Id, Task, Activity State, Change Request, Assignee(s), Requested On, and Completed On. The first row in the table is highlighted with a blue arrow pointing to the 'Perform' button. The table shows the following data for the first row:

Action	Activity Id	Task	Activity State	Change Request	Assignee(s)	Requested On	Completed On
Perform	2846	Complete Default Provisioning Form for Test52 OTInfrUser	Available	--	AveksaAdmin, OTInfrUser	3/24/15 2:07 PM	--

1 item

1675

1676

Figure 107. IMG Requests Activities

1677 5. Select the group you would like the moved user to have access to, click 'Next' and
 1678 'Accepted', then 'Finish' on the final screen. As you did before for adding a new user.
 1679 6. Collect data again so IMG can confirm that the user is added to the appropriate group in
 1680 the new OU.
 1681 7. Terminating a user
 1682 8. Delete the user from the HR CSV file.
 1683 9. Collect data again.
 1684 10. The user is automatically removed.
 1685 11. Collect data again, so IMG can confirm the user is no longer in Adaptive Directory.
 1686 12. Check the Status in 'Requests', and 'Requests' as shown in Figure 108.

Request: 00077

Overall Status: 100% 1/1 (Fulfillment Phase)

Name: 00077
 Requested By: AveksaAdmin, (through the rule Termination) on 3/24/15 2:12 PM
 Fulfillment Date: 03/23/15
 Notes: Request submitted by the system for the rule Termination on behalf of the rule owner AveksaAdmin.
 Workflow Jobs: Processing Workflow
 Email Log: Email Log
 AFX Log: AFX Log

Attachments

Browse... No file selected. Upload Attachment

Status

Details: Fulfillment: 100% 1/1 Changes Fulfilled (0/0 Activities)

- Approval Phase
- Fulfillment Phase
 - IT AFX Fulfillment
 - Changes processed by AFX handler
 - Verified

Account Changes

Status	Action	Account	Entitlement Type	Business Source	Entitlement	State
	Delete	CN=Test520TInfrUser,ou=ot,dc=master,dc=test	Account	OTInfrUser, Test52	Completed	

1687

1688

Figure 108. IMG Request Status

1689 **8 INSTALLATION OF ADAPTIVE DIRECTORY: RSA (BUILD #2)**

1690 RSA Adaptive Directory implements the central IdAM ID store in Build #2. It receives input from
 1691 central IdAM system (RSA IMG). The central ID store contains the distribution mechanism for
 1692 updating the various downstream (synchronized) directories with user access and authorization
 1693 data. This process applies to new users, terminated users (disabled or deleted users), and any
 1694 changes to a user profile. Changes include promotions, job responsibility changes, and any
 1695 other change that would affect the systems a user needs to access.

1696 **8.1 SECURITY CHARACTERISTICS**

1697 Cybersecurity Framework Categories: PR.AC-1: Identities and credentials are managed for
 1698 authorized devices and users

1699 NIST 800-53 rev 4 Security Controls: AC-2, IA Family

1700 **8.2 RSA ADAPTIVE DIRECTORY IS INSTALLED ON THE IDAM NETWORK, ON A VM THAT IS RUNNING CENTOS 7**

1702 The following lines detail the command line installation procedure for RSA Adaptive Directory,
 1703 including displayed responses:

```
1704 [root@localhost ~]# ls
1705 anaconda-ks.cfg reports xml
1706 [root@localhost ~]# cd ..
1707 [root@localhost /]# ls
1708 bin dev home lib64 mnt proc run srv tmp var
1709 boot etc lib media opt root sbin sys usr
1710 [root@localhost /]# cd media
1711 [root@localhost media]# ls
1712 cdrom
1713 [root@localhost media]# cd cdrom
1714 [root@localhost cdrom]# ls
1715 Documentation rsa_7.1.5_linux_64.bin rsa_7.1.5_windows_64.exe
1716 [root@localhost cdrom]# su root ./rsa_7.1.5_linux_64.bin
1717 Preparing to install...
1718 WARNING: /tmp does not have enough disk space!
1719 Attempting to use /root for install base and tmp dir.
1720 Extracting the JRE from the installer archive...
1721 Unpacking the JRE...
1722 Extracting the installation resources from the installer archive...
1723 Configuring the installer for this system's environment...
1724 Launching installer...
1725
1726 Graphical installers are not supported by the VM. The console mode will be used instead...
1727 =====
1728 RSA Adaptive Directory 7.1.5 (created with InstallAnywhere)
1729 -----
1730 Preparing CONSOLE Mode Installation...
1731
1732
1733 =====
1734 License Agreement
1735 -----
1736 Please read the following License Agreement carefully.
1737 LICENSE AGREEMENT
1738 *** IMPORTANT INFORMATION - PLEASE READ CAREFULLY ***
```

1739 (...Lic agreement text omitted...)

1740 DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y

1741 =====

1742 Choose Install Folder

1743 -----

1744 Please choose a destination folder for this installation

1745 Where would you like to install?

1746 Default Install Folder: /root/rsa/adaptivedirectory

1747 ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT: Enter

1748 =====

1749 Choose Install Set

1750 -----

1751 Please choose the Install Set to be installed by this installer.

1752 >1- RSA Adaptive Directory New Cluster / Standalone

1753 2- RSA Adaptive Directory Cluster Node

1754 3- Customize...

1755 ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:

1756 Enter

1757 =====

1758 New Cluster settings

1759 -----

1760 Enter information below about the new cluster to create:

1761 - The cluster name

1762 - The ZooKeeper ports that will be used

1763 Cluster name: (DEFAULT: cluster1): cluster1

1764 ZooKeeper Ensemble Port: (DEFAULT: 2888): 2888

1765 ZooKeeper Leader Election Port: (DEFAULT: 3888): 3888

1766 ZooKeeper Client Port: (DEFAULT: 2181): 2181

1767

1768

1769 =====

1770 Administrator name

1771 -----

1772 Please provide the administrator name:

1773 Admin User Name (DEFAULT: cn=Directory Manager): Directory Manager

1774
1775 =====
1776 Server administrator password
1777 -----
1778 Please provide a password for the administrator user :
1779 Password (DEFAULT:): secretsecret
1780 Confirm Password (DEFAULT:): secretsecret
1781
1782 =====
1783 Adaptive Directory port numbers
1784 -----
1785 Please enter port numbers for Adaptive Directory:
1786 Adaptive Directory Port (DEFAULT: 2389): 2389
1787 Scheduler Port (DEFAULT: 1099): 1099
1788 Adaptive Directory SSL Port: (DEFAULT: 1636): 1636
1789
1790 =====
1791 TLS Configuration
1792 -----
1793
1794 Enable TLS (Y/N)? (DEFAULT: N): N
1795
1796 =====
1797 Adaptive Directory HTTP port numbers
1798 -----
1799 Please enter port numbers for Adaptive Directory HTTP services:
1800 Adaptive Directory HTTP Port (DEFAULT: 8089): 8089
1801 Adaptive Directory HTTPS Port (DEFAULT: 8090): 8090
1802
1803 =====
1804 Certificate configuration
1805 -----
1806 Use an existing certificate (Y/N)? (DEFAULT: N): N
1807
1808 =====

1809 Application Server Configuration
1810 -----
1811 Enter information below to configure the Application Server
1812 - Administrator user name for initial server instance.
1813 - Administrator password for initial server instance (must be at least 8
1814 characters in length).
1815 - Administration server port number for initial server instance.
1816 - HTTP/HTTPS port number for initial server instance.
1817 - JMX port number for initial server instance.
1818 Admin User (DEFAULT: admin): admin
1819 Password (DEFAULT:): secretsecret
1820 Confirm Password (DEFAULT:): secretsecret
1821 Admin Port (DEFAULT: 4848): 4848
1822 HTTP Port (DEFAULT: 9090): 9090
1823 HTTPS Port (DEFAULT: 9191): 9191
1824 JMX Port (DEFAULT: 8686): 8686
1825
1826 ======
1827 Control Panel Configuration
1828 -----
1829 These are the settings for the Web Server hosting the Control Panel.
1830 Enter the HTTP/HTTPS ports to configure the Web Server on the main instance:
1831 These are the settings for the Web Server hosting the Control Panel.
1832 HTTP Port (DEFAULT: 7070): 7070
1833 Enter the HTTP/HTTPS ports to configure the Web Server on the main instance:
1834 HTTPS Port (DEFAULT: 7171): 7171
1835
1836 ======
1837 Port validation failed
1838 -----
1839 Control Panel HTTP port These are the settings for the Web Server hosting the
1840 Control Panel. is invalid.
1841 Please select a new one.
1842 PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK): Enter
1843

1844 =====

1845 Control Panel Configuration

1846 -----

1847 These are the settings for the Web Server hosting the Control Panel.

1848 Enter the HTTP/HTTPS ports to configure the Web Server on the main instance:

1849 HTTP Port (DEFAULT: 7070): 7070

1850 HTTPS Port (DEFAULT: 7171): 7171

1851

1852 =====

1853 Pre-Installation Summary

1854 -----

1855 Please Review the Following Before Continuing:

1856 Product Name: RSA Adaptive Directory 7.1.5

1857 Install Folder: /root/rsa/adaptivedirectory

1858 Install Set: RSA Adaptive Directory New Cluster / Standalone

1859 Product Features: Application, Sample Data

1860 Java VM Installation Folder: /root/rsa/adaptivedirectory/jdk

1861 Administrator User: cn=Directory Manager

1862 Adaptive Directory Ports: 2389 8089 8090

1863 Scheduler Port: 1099

1864 SSL Configuration: 1636

1865 Start TLS Configuration: TLS is disabled.

1866 Certificate Configuration: Self signed certificate.

1867 App Server Configuration: 4848 9090 9191 8686

1868 Web Server Configuration: 7070 7171

1869 Disk Space Information (for Installation Target):

1870 Required: 1,164.03 MegaBytes

1871 Available: 49,030.86 MegaBytes

1872 PRESS <ENTER> TO CONTINUE: Enter

1873

1874 =====

1875 Installing...

1876 -----

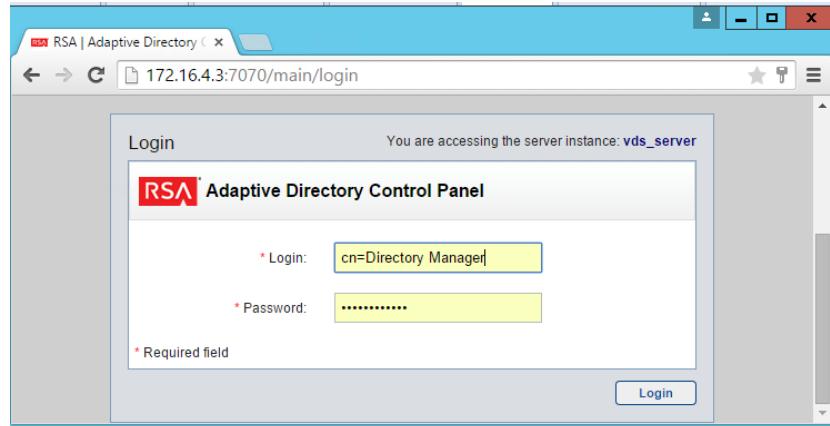
1877 [===== | ===== | =====]

1878 [----- | ----- | ----- | -----]

1879
1880 =====
1881 Installation Complete
1882 -----
1883 Congratulations. RSA Adaptive Directory 7.1.5 has been successfully installed to:
1884 /root/rsa/adaptive directory In order to start working with RSA Adaptive Directory 7.1.5, please
1885 follow these steps:
1886 - LOG OFF
1887 Then
1888 - LOG IN
1889 - Copy and paste your license key when prompted after running RSA Adaptive
1890 Directory 7.1.5
1891 - Run /root/rsa/adaptive directory/bin/openControlPanel.sh
1892 PRESS <ENTER> TO EXIT THE INSTALLER: Enter

1893 **8.3 ADDITIONAL STEPS REQUIRED AFTER INSTALLATION IS COMPLETE**

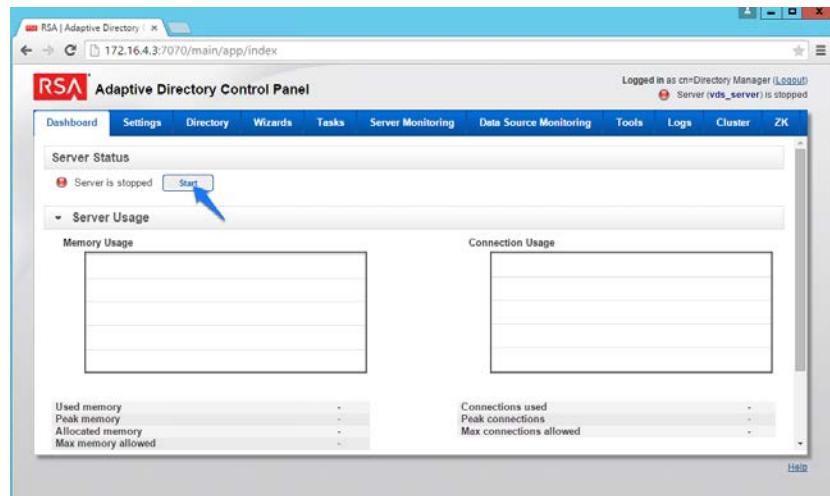
1894 Then you need to install netstat: yum install net-tools
1895 Copy the license.lic file to: /root/rsa/adaptive directory/vds_server
1896 Open all relevant firewall ports on the CentOS server
1897 Run /root/rsa/adaptive directory/bin/openControlPanel.sh
1898 Run /root/rsa/adaptive directory/bin/runContextBuilder.sh
1899 From a web browser go to: *http:IPADDRESS:7070*
1900 Start the server by clicking the Start button.
1901 Click on Tools menu item, and start the Application Server.
1902
1903 Configuration Procedure:
1904 From a web browser, connect to the Adaptive Directory server and log in (Note the URL with
1905 port number) using the following credentials: (Default credentials) See Figure 109.
1906 Username: cn=Directory Manager
1907 Password: secretsecret
1908



1909

Figure 109. Adaptive Directory Login Page

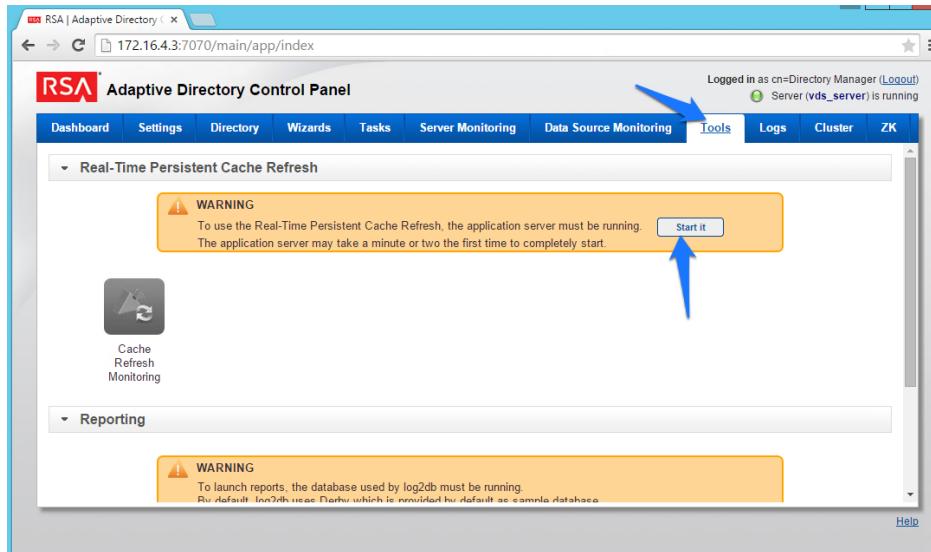
1911 On the main page, Figure 110, start the Adaptive Directory server:



1912

Figure 110. Adaptive Directory Main Page

1914 On the Tools tab, Figure 111, click Start it to start the Persistent Cache service:

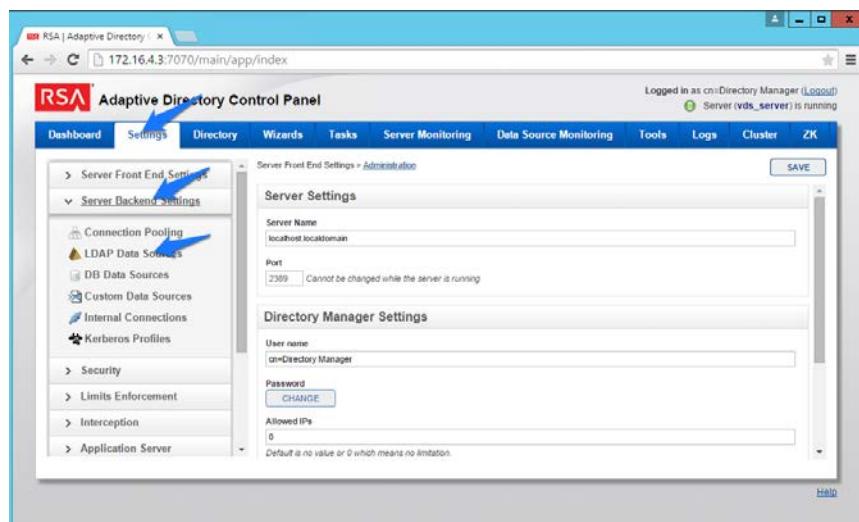


1915

1916

Figure 111. Adaptive Directory Tools Page

1917 Now go to the Settings tab, Figure 112 and click Server Backend Settings and then click LDAP Data Sources.

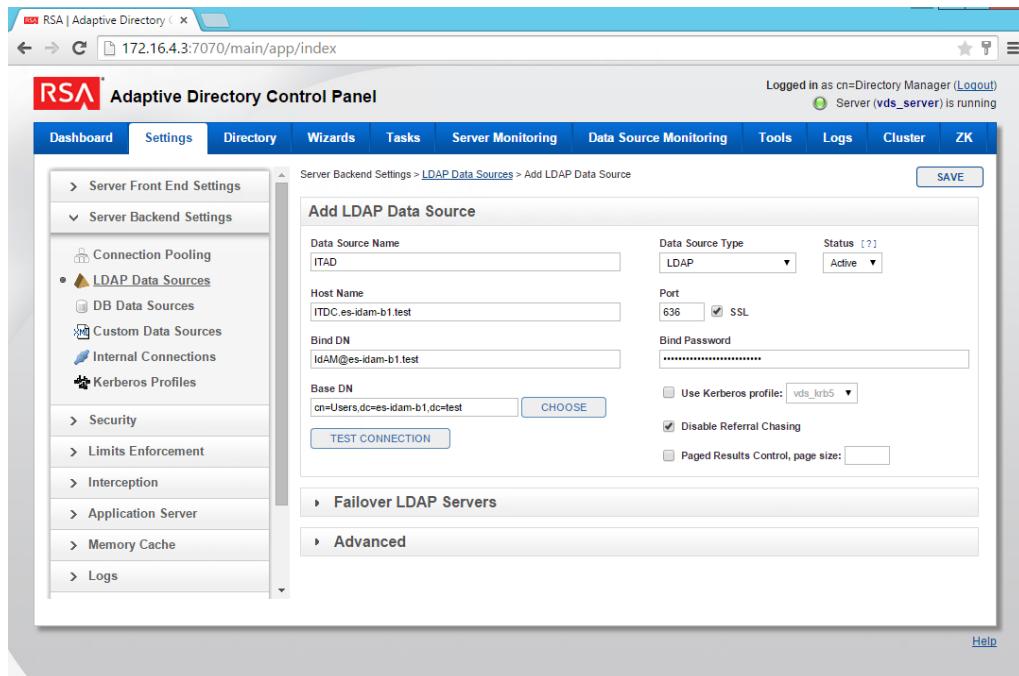


1919

1920

Figure 112. Adaptive Directory Server Backend Settings

1921 Click Add.



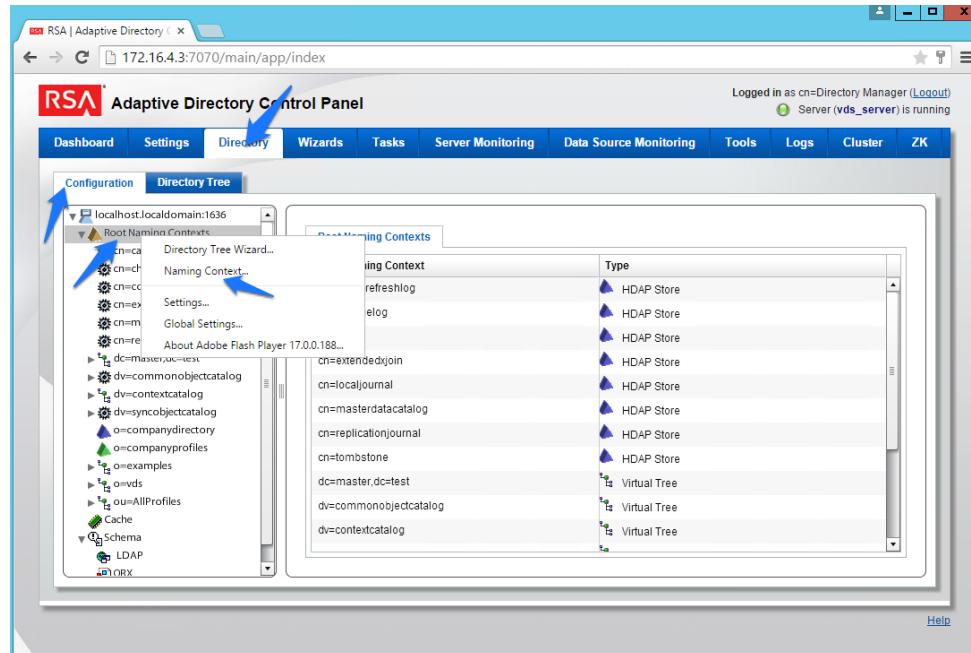
1922

1923

Figure 113. Adaptive Directory LDAP Data Source

1924 Enter details for your “backend AD” as shown in Figure 113. Click the Test Connection button to
 1925 be sure your settings are correct. Repeat this process for all the AD clusters, i.e., for the backend
 1926 ADs on the IT, OT, and PACS networks. You can Clone your first connection to make repeat
 1927 additions easier.

1928 Now click on Directory, click on Configuration, right-click on Root Naming Contexts, and select
 1929 Naming context as shown in Figure 114.



1930

1931

Figure 114. Adaptive Directory Configuration of Naming Context

1932 You are presented with this screen, Figure 115:

New Naming Context

New Naming Context

Please enter a naming context, and select the type of backend to be associated with this naming context.

Naming Context: Assist

Type:

- LDAP Backend
- Database Backend
- Virtual Tree
- HDAP store
- DSML/SPML Service
- LDIF File

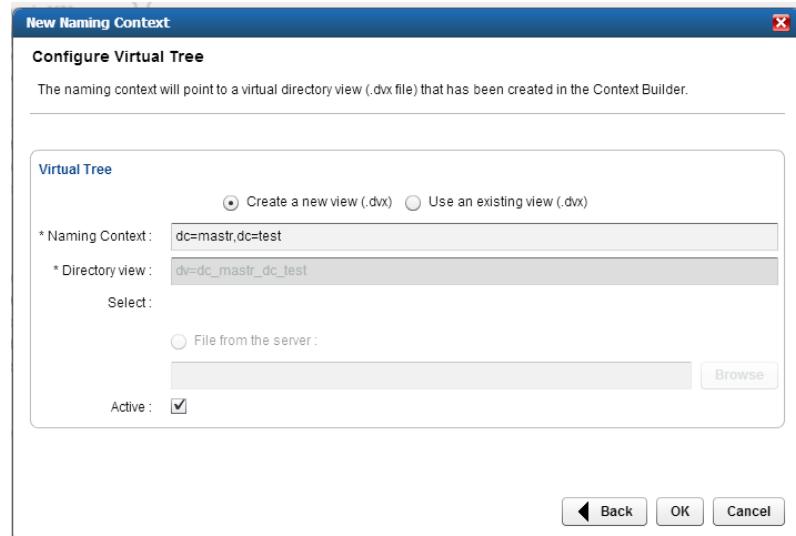
Next ► Cancel

1933

1934

Figure 115. Adaptive Directory New Naming Context

1935 Enter the “name” you would like your new Virtual LDAP directory to be configured with. Select Virtual Tree and click Next.
1936



1937

1938

Figure 116. Adaptive Directory Configure Virtual Tree

1939 Leave the defaults selected as shown in Figure 116, and click OK. You will see the following screen, Figure 117.



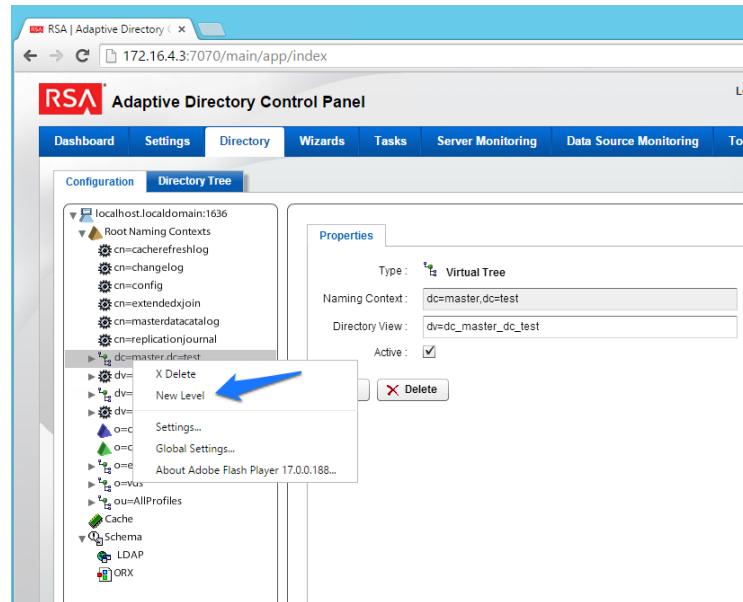
1941

1942

Figure 117. Adaptive Directory Virtual Tree

1943 You now have a virtual directory naming context created, and the next step is to configure this
1944 virtual directory to include all the backend AD clusters.

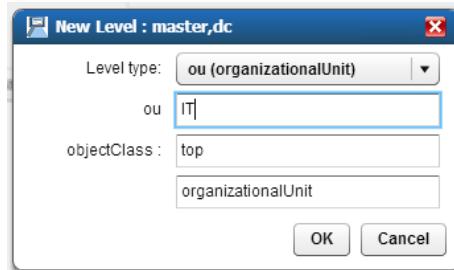
1945 Right-click on your newly created Virtual Directory and select New Level as shown in Figure 118:



1946

Figure 118. Adaptive Directory Create New Level

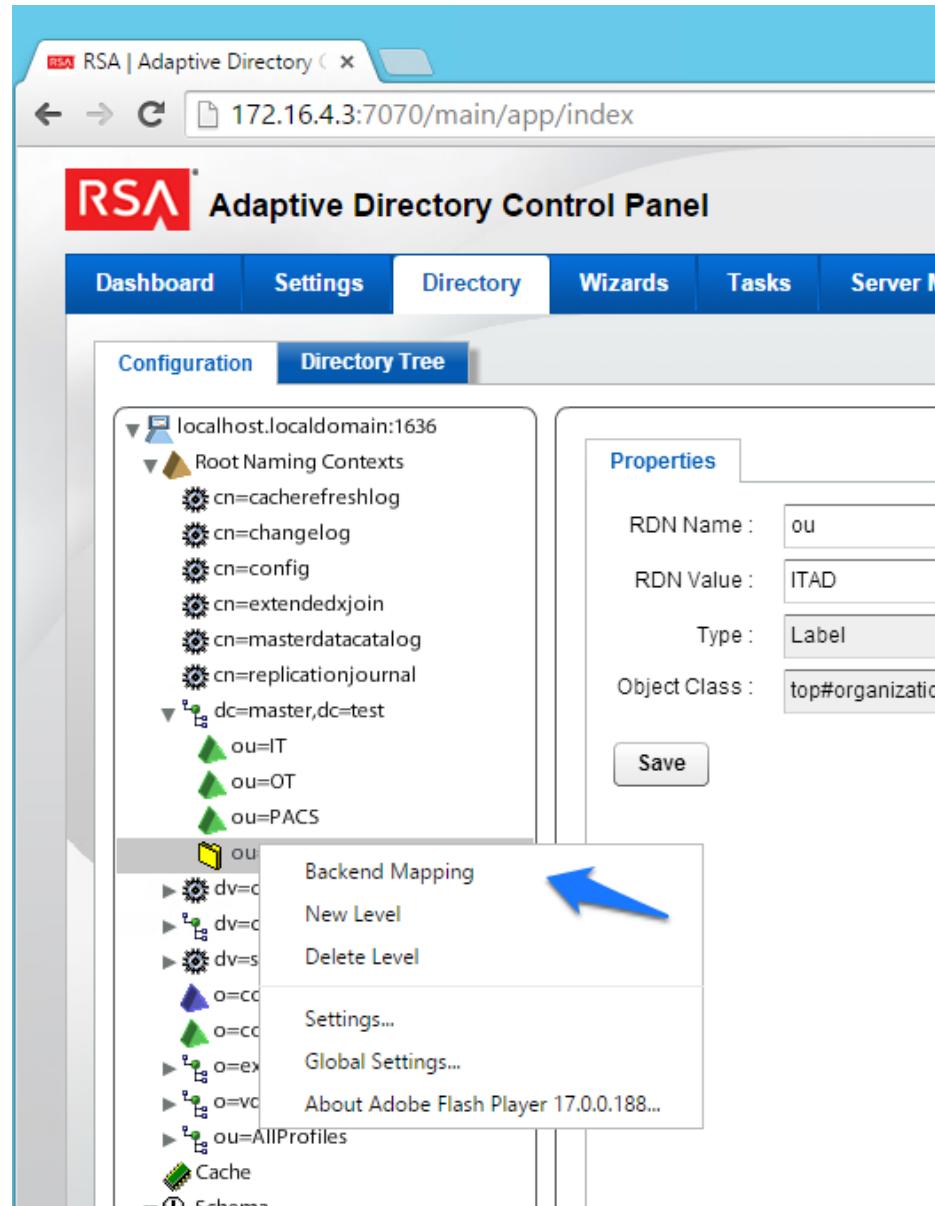
1947 Enter a “name” for this LDAP backend mapping. This name will be an OU in the Virtual
 1948 Directory as shown in Figure 119.



1950

Figure 119. Adaptive Directory New Level Name

1951 Right-click this new OU in your Virtual Directory and select Backend Mapping as shown in Figure
 1952 120.

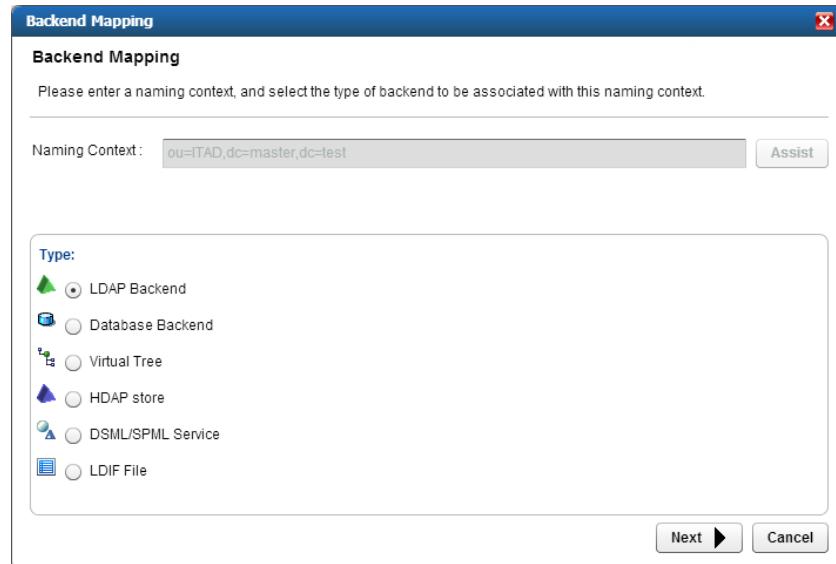


1954

1955

Figure 120. Adaptive Directory Backend Mapping

1956 Leave LDAP Backend selected and click Next as shown in Figure 121.

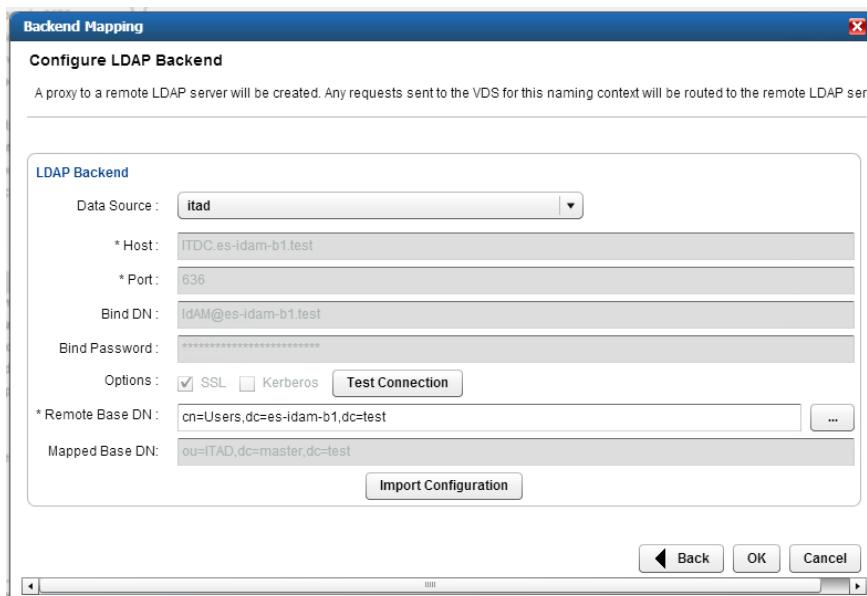


1957

1958

Figure 121. Adaptive Directory Backend Mapping

1959 Now select one of your backend AD clusters we configured earlier and click OK as shown in
 1960 Figure 122.



1961

1962

Figure 122. Adaptive Directory Configure LDAP Backend

1963 Repeat this procedure for all your backend AD clusters (i.e., for the backend ADs on the IT, OT, and PACS networks).
 1964
 1965 By default, the Adaptive Directory server will return default AD attributes.

1966 8.4 CUSTOM ATTRIBUTE CONFIGURATION

1967 Custom attributes are required and are configured as follows:

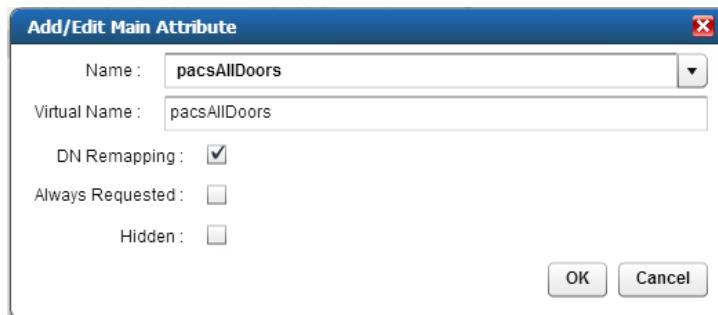
1968 Click on Directory, then Configuration, and then expand the virtual directory you are working
 1969 with and select the backend mapping to AD to which you want to make changes. Then click the
 1970 Attributes tab and Add as shown in Figure 123.

Actual Name	Virtual Name	DN Remapping	Always Requested	Hidden
manager	manager	<input checked="" type="checkbox"/>		
secretary	secretary	<input checked="" type="checkbox"/>		
seealso	seealso	<input checked="" type="checkbox"/>		
memberof	memberof	<input checked="" type="checkbox"/>		
unique memb...	unique memb...	<input checked="" type="checkbox"/>		
member	member	<input checked="" type="checkbox"/>		
pacsAllDoors	pacsAllDoors	<input checked="" type="checkbox"/>		
pacsHomeAcc...	pacsHomeAcc...	<input checked="" type="checkbox"/>		
pacsWorkAcc...	pacsWorkAcc...	<input checked="" type="checkbox"/>		

1971

Figure 123. Adaptive Directory Addition Attributes

1973 Find the attribute you would like to add in the top drop-down list, and enter a “name” (it could
 1974 be the same or different) for the attribute you want Adaptive Directory to return. Then select
 1975 DN Remapping and click OK as shown in Figure 124.



1976

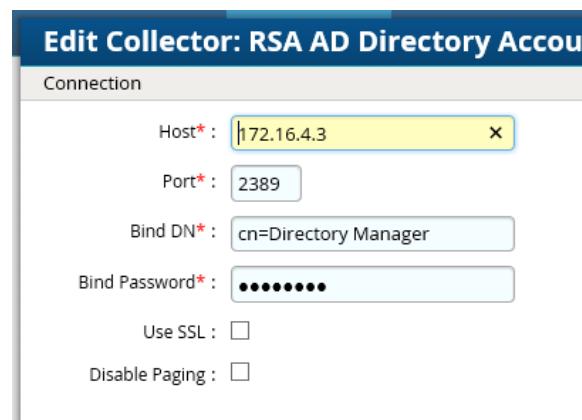
Figure 124. Adaptive Directory Add/Edit Main Attribute

1978 Complete this procedure for any additional custom attributes that are required and for any
 1979 additional AD backends to which you may need to add attributes.

1980 Your Adaptive Directory virtual directory is now complete and can be accessed from RSA IMG /
 1981 Aveksa or any other application that can access LDAP directories.

1982 You can address this virtual directory by configuring the connecting application with the IP
 1983 address or DNS name of the Adaptive Directory server and using port 2389. For the base DN,
 1984 you would use the name of your virtual directory—in the above example, 'dc=master,dc=test'
 1985 and the relevant OU (backend AD cluster) you want to access. You would use the same
 1986 username (cn=Directory Manager) and password you use to log in to the application.

1987 For example, Figure 125 and Figure 126 show the connection information from RSA IMG to
 1988 Adaptive Directory.



1989

1990 *Figure 125. Adaptive Directory Edit Collector*

Search Configuration for Accounts

Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector.

Account Base DN* :	<input type="text" value="dc=master,dc=test"/> <input type="button" value="x"/>
Account Search :	Subtree <input type="button" value="▼"/>
Scope* :	<input type="text"/>
Account Search :	<input type="text" value="(&(objectCategory=person)(objectClass=user)(sAMAccountName=*))"/> <input type="button" value="Filter*"/>

1991

1992 *Figure 126. Adaptive Directory Search Configuration for Accounts*

1993 8.5 RSA AD OPTIMIZATION AND TUNING

1994 8.5.1 Disable Referral Chasing

1995 Referral chasing should be disabled for performance reasons. Check the Disable Referral Chasing
 1996 option when you define the LDAP data source.

1997 8.5.2 Limit Attributes Requested from the LDAP Backend

1998 Whenever RSA Adaptive Directory queries a backend LDAP, the default behavior is to ask for all
1999 attributes (although *only* the attributes requested in the query will be returned to the client).
2000 This default behavior of RSA Adaptive Directory is for the following reasons:

- 2001 • Joins have been configured and the filter in the search request involves attributes from
2002 both the primary and secondary sources (i.e., the query filter contains conditions on
2003 both primary and secondary objects).
- 2004 • Interception scripts may involve logic based on attributes from the backend and so
2005 require these attributes. These attributes may not be specifically requested or searched
2006 for by the client. However, RSA Adaptive Directory must retrieve them from the backend
2007 in order for the script logic to be valid.
- 2008 • Access Control List (ACL) checking. You can set up ACLs based on attribute/values of an
2009 entry (e.g., mystatus=hidden), so RSA Adaptive Directory may need the whole entry to
2010 check the authorization.
- 2011 • For entry caching. The entire entry needs to be in the entry cache.

2012 If your virtual view does not require all attributes to be requested for any of the conditions
2013 mentioned above, you can enable the option to limit the attributes that are requested for
2014 better performance. If this option is enabled, RSA Adaptive Directory will query the backend
2015 server only for attributes requested from the client in addition to attributes set as Always
2016 Requested on the Attributes tab.

2017 8.5.3 Process Joins and Computed Attributes Only When Necessary

2018 The default behavior of RSA Adaptive Directory is to process associated joins and build
2019 computed attributes whenever a virtual object is reached from a query regardless of whether
2020 the attributes requested come from a secondary source or computation. If you enable the
2021 option to process joins and computed attributes only when necessary, RSA Adaptive Directory
2022 will not perform joins or computations when a client requests or searches for attributes from a
2023 primary object only. If a client requests or searches for attributes from secondary objects or
2024 computed attributes, RSA Adaptive Directory will process the join(s) and computations
2025 accordingly. Use caution when enabling this option if you have interception scripts defined on
2026 these objects or if access controls based on filters are being used (both of which may require
2027 other attributes returned from secondary sources or computations regardless of whether or not
2028 the client requested or searched for them).

2029 8.5.4 Use the Client Sizelimit Value to Query the Backend

2030 Whenever Adaptive Directory queries a backend LDAP, the default behavior is to ask for all
2031 entries (sizelimit=0) even if the client to Adaptive Directory indicates a sizelimit. This is the
2032 default behavior because the entries returned by the backend are possible candidates but may
2033 not be retained for the final result that is sent to the client. For example, if an ACL has been
2034 defined in Adaptive Directory, not all entries from the backend may be authorized for the user
2035 (who is connected to Adaptive Directory) to access. As another example, when joins or
2036 interception scripts are involved with the virtual view, they may also alter the entries that match
2037 the client's search. To limit the number of entries from the backend, using paging is the

2038 recommended approach. If the backend supports paging, Adaptive Directory will not get all the
2039 results at once; rather, it will get only one page at a time (pagesize is indicated in the
2040 configuration). In this case, if Adaptive Directory has returned to the client the sizelimit
2041 required, Adaptive Directory will not go to the next page.

2042 If your virtual view does not involve any of the conditions mentioned above (joins,
2043 interceptions, ACL), and using paging between Adaptive Directory and the backend is not
2044 possible, you can enable the Client Sizelimit value option to limit the number of entries
2045 requested from the backend. If this option is enabled, Adaptive Directory will use the sizelimit
2046 specified by the client instead of using sizelimit=0 when querying the backend.

2047 **9 PRIVILEGED USER ACCESS CONTROL: ALERTENTERPRISE GUARDIAN INSTALLATION**

2048 AlertEnterprise Guardian is installed on the IdAM network, in a VM running the Windows Server
2049 2012 R2 OS. Guardian is used to control privileged user access to the components located on
2050 the network OT systems. Guardian collects user authorization information from the AD located
2051 within the OT network. There are three parts to the AlertEnterprise Guardian How-To guide,
2052 each of which is provided in the subsections below: Subsection 12.2 provides general product
2053 installation and set-up information. Subsection 12.3 provides the AlertEnterprise configuration
2054 information as configured in the RSA build. Subsection 12.4 provides the AlertEnterprise
2055 configuration information as configured in the CA build.

2056 **9.1 SECURITY CHARACTERISTICS**

2057 Cybersecurity Framework Categories: PR.AC-1: Identities and credentials are managed for
2058 authorized devices and users

2059 NIST 800-53 rev 4 Security Controls: AC-2, IA Family

2060 **9.2 INSTALLATION ON TOMCAT AND WINDOWS**

2061 This section describes the detailed procedure of installing AlertEnterprise products on Tomcat
2062 on a Windows platform. It lists the hardware and software pre-requisites as well as the steps to
2063 install and use the AlertEnterprise suite of applications.

2064 When copying text from this guide, it is recommended that you first paste text to a Notepad file
2065 and then copy it from there to use it for running scripts. You should use the “Notepad++”
2066 application for this purpose.

2067 **Installation Prerequisites**

2068 The AlertEnterprise Suite is delivered as a WAR (Web application Archive) file that needs to be
2069 deployed on the client’s application server. Before you actually start deploying on your
2070 application server, you must check for the pre-requisites. Refer to AlertEnterprise Systems
2071 Requirements document included in the installation package.

2072 **Pre-Installation Verification**

2073 Before you start installing AlertEnterprise product, verify the proper functioning of the
2074 underlying software systems. Verify that:

2075 • Your system meets all the software and hardware prerequisites as described in Systems
2076 Requirement Specification document.

2077 • Compatible version of Java Runtime Environment (JRE) is installed and working on the
2078 system.

2079 • Compatible version of the web server is installed and running.

2080 • Compatible version of the database server is installed and running.

2081 • Supported Internet Browser (for example, Microsoft Internet Explorer) is working
2082 properly.

2083 Zip extracting software is required. You can download WinZip from
2084 www.winzip.com/downwz.com.

2085 **Installing Mandatory Software Applications**

2086 Before deploying the AlertEnterprise application, install JRE and a Web Application Server (for
2087 example, Tomcat). You must also install the latest version of Adobe Flash Player to enable the
2088 Internet browser you will be using to access the AlertEnterprise application.

2089 **Installing JRE**

2090 To install JRE:

2091 1. Download the application server-compatible JRE.

2092 2. Double-click the setup launcher to start the installation process.

2093 **Setting Java Home**

2094 1. Make sure that JAVA_HOME variable is set to the folder where Java is installed and
2095 %JAVA_HOME%/bin is in the system's path.

2096 2. Open the Command Prompt in Administrator Mode (Right Click > Run As Administrator)
2097 and issue:

2099 **Set JAVA_HOME=<PATH OF JDK/JRE>**

2100
2101 Where <PATH OF JDK/JRE> is the path where Java is installed, for example,
2102 C:\Program Files\Java\JDK1.6

2104 3. Setting Path:

2106 PATH= C:\Program Files\Java\JDK1.6.0-21\bin;%PATH%

2108 4. Checking JAVA_HOME and PATH:

2110 Echo %JAVA_HOME%

2111 Echo %PATH%

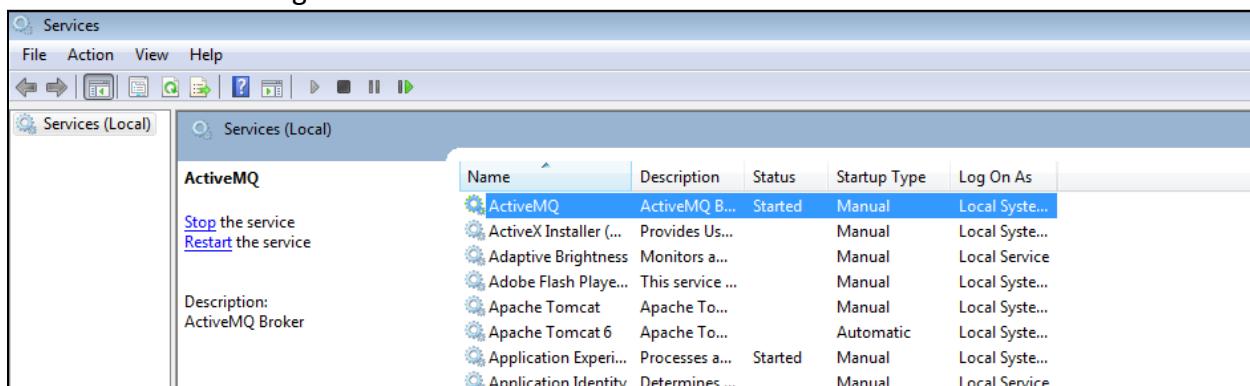
2112 Checking JAVA Version: Java -version

2113 **Running ActiveMQ as Windows Service**

2114 After extracting the folder, the folder name appears as “apache-activemq” at the specified
2115 location.

2116

2117 1. Go to the folder *apache-activemq* and move to *bin/win32* in Windows
2118 Explorer and right-click on *InstallService.bat* file and select Run as
2119 Administrator. Refer to .
2120 2. Once the above batch file gets executed, verify that the ActiveMQ is added as Windows
2121 Services.
2122 3. Go to Run command and enter *services.msc*. The Services window appears. Refer
2123 to the following screen shot.



2124

2125 *Figure 127. Adaptive Directory Search Configuration for Accounts*

2126

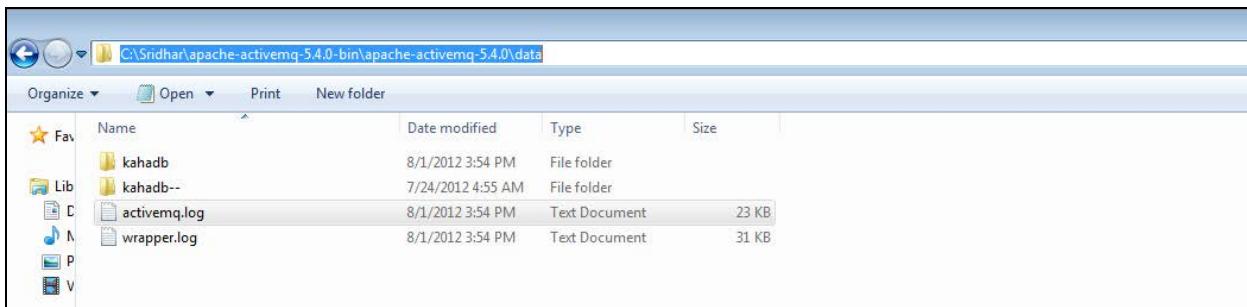
2127 4. The Apache ActiveMQ service has an administrative console. To check if the service is
2128 running correctly, you simply need to connect to the admin console.

2129 URL: <IP address of the server where Active MQ is
2130 installed>:8161/admin

2131

2132 5. Perform the following if Active MQ is on a server other than AlertEnterprise server:

- 2133 • Search for the URL that starts with TCP ://<IP Address>:61616 in
2134 *activemq.log* located in Apache ActiveMQ home directory/data folder.
2135 Refer to the following screen shot:



2136

Figure 128. Guardian ActiveMQ Home/Data Directory

2138

2139 • Copy the URL and update the *context.xml* file in the *<Tomcat Home>/conf* and *appContextDB.properties* file located in *<Tomcat Home/webapps/AlertEnterprise/WEB-INF/classes>*.

2140

2141

2142

2143 **Steps for Failure Case:**

2144 If the system throws an error message while executing the bat file or the ActiveMQ Services
2145 screen does not appear, follow these steps:

2146 1. Navigate to the folder *<ActiveMQ home directory>\bin\win32*.

2147 2. Open the *InstallService.bat* file in a local text editor.

2148 3. Modify the bottom part of the script to look like the following. Note that your
2149 JAVA_HOME environment variable needs to already be set and also need to pass it as a
2150 variable to the wrapper.

2151

```
2152 :conf
2153 set WRAPPER_CONF="%ACTIVEMQ_HOME%\bin\win32\wrapper.conf"
2154 set ACTIVEMQ_HOME="set.ACTIVEMQ_HOME=%ACTIVEMQ_HOME%"
2155 set ACTIVEMQ_BASE="set.ACTIVEMQ_BASE=%ACTIVEMQ_BASE%"
2156 set JAVA_HOME="set.JAVA_HOME=%JAVA_HOME%"
2157 rem
2158 rem Install the Wrapper as an NT service.
2159 Rem
2160 :startup
2161 "%ACTIVEMQ_HOME%\bin\win32\wrapper.exe" -i %_WRAPPER_CONF%
2162 %_ACTIVEMQ_HOME% %_ACTIVEMQ_BASE% %_JAVA_HOME%
2163 if not errorlevel 1 goto :eof
2164 pause
```

2165

2166 4. Open the *<ActiveMQ home directory>\bin\win32\wrapper.conf* in a
2167 local text editor and change this:

2168

```
2169 # Java Application
```

```
2170 wrapper.java.command=java
2171 to this:
2172 # Java Application
2173 wrapper.java.command=%JAVA_HOME%\bin\java.exe
2174
2175 After you have performed these steps, you should be able to run the InstallService.bat
2176 successfully.
2177
2178 5. To also use the UninstallService.bat file, open it and hard-code the path to
2179 the wrapper:
2180
2181 rem
2182 rem Uninstall the Wrapper as an NT service.
2183 rem
2184 :startup
2185 "%ACTIVEMQ_HOME%\bin\win32\wrapper.exe" -r %_WRAPPER_CONF%
2186 if not error level 1 goto :eof
2187 pause
2188 After executing the InstallService.bat file, you can see the ActiveMQ in Services.
2189
2190 6. If the ActiveMQ server is not up and the system throws the following error:
2191
2192 | WARN | tmpdir | org.eclipse.jetty.util.log | WrapperSimpleAppMainjava.io.IOException: The
2193 system cannot find the path specified
2194 at java.io.WinNTFileSystem.create File Exclusively (Native Method)
2195 at java.io.File.check And Create (File.java:1343)
2196 at java.io.File.create Temp File (File.java:1431)
2197
2198 Solution:
2199 You must manually create two folders: <ActiveMQ home directory>/work and
2200 <ActiveMQ home directory>/temp.
2201
2202 To check whether ActiveMQ is started, access the following link as shown in Figure 129.
2203 http://<Server IP Address>:8161/admin/
```

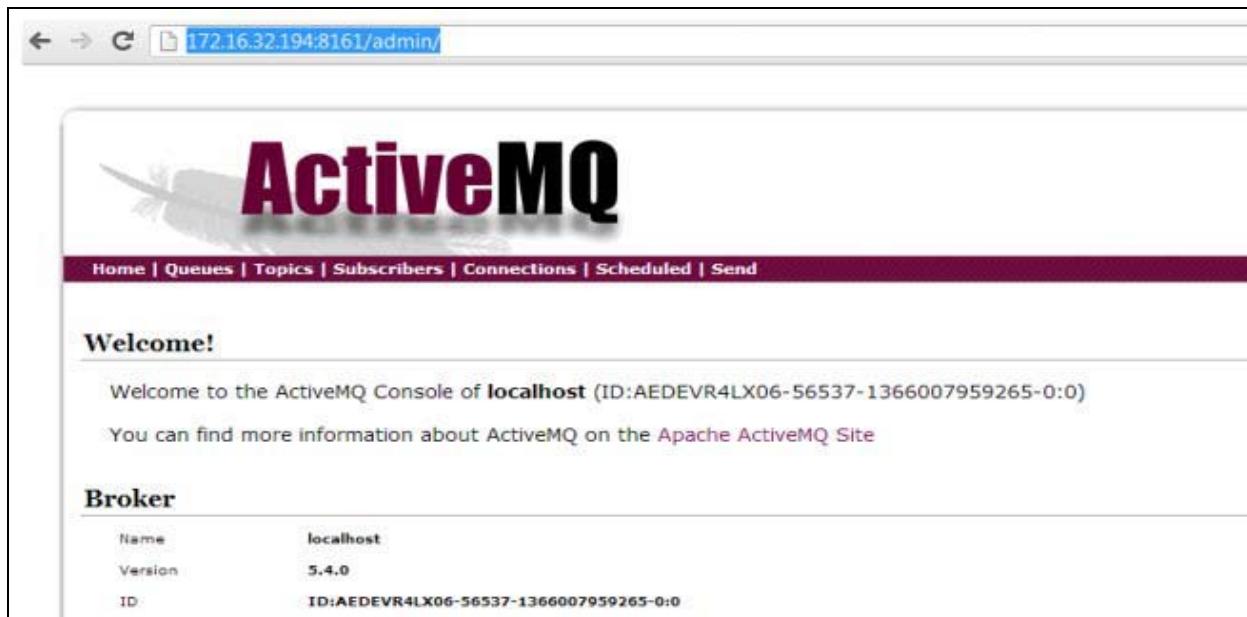


Figure 129. Guardian ActiveMQ

Installing Apache Tomcat

You must install hardware and operating system versions specific to Apache Tomcat:

1. Double-click the setup launcher to start the setup. It will start the installation process.
2. Click Next to start the installation process.
3. Click I Agree to accept the license terms. It displays the Choose Components screen.
4. Select Custom as install type and uncheck the Examples option.
5. Click Next to specify the Destination Folder for installation. We strictly recommend using **D:\AlertEnterprise\Tomcat** location.
6. Click Next to specify configuration parameters.
7. Enter the desired port in the Connector Port text area. 8080 is the default port.
8. Specify the User Name and Password in the respective fields.
9. Click Next to select the path of JRE installed on the system.
10. Select the path of JDK/JRE you just installed. For example, **C:\Program Files\Java\jre1.6**.
11. Click Install to start the file copying process. Uncheck Run Apache Tomcat and Show Readme options in the final dialog box.
12. Click Finish to finish the installation.

Apache Tomcat Configuration

You need to specify Tomcat configuration as specified in the following steps:

2227 1. Click Start > Programs > Apache Tomcat > Configure Tomcat option.
2228 2. Click Java tab in the Apache Tomcat Properties dialog box.
2229 3. Enter the following settings:
2230 • Initial memory pool: 1024
2231 • Maximum memory pool: 1024
2232 • Thread stack size: 300
2233
2234 *Note:* These settings may vary with the volume of random access memory (RAM) in
2235 the server.
2236
2237 4. Click Apply and OK to close the dialog box.
2238

2239 **Configuring Database Server**

2240 You need to perform some configurations in the database server to install AlertEnterprise
2241 applications. You must perform these configurations through the database administrator login.
2242 The current version of AlertEnterprise products supports Oracle and MS SQL Server databases.
2243 The NCCoE build also supports MySQL server database.
2244

2245 To configure the database server:

2246 1. Create a schema/SID as per your naming convention in the database server. The steps to
2247 create schema can be different with different database management systems. Refer to
2248 the administrators guide for the database management system installed at your
2249 landscape.
2250 2. Create a new user with full access to the created schema.
2251 3. Run the included SQL files *AlertReport471.ddl* or *AlertReport471.sql*
2252 and *AlertQuartz.sql* on the new schema created. This step should be performed
2253 while installing the AlertEnterprise application for the first time.

2254 **Avoiding Case-sensitivity Issues in Alert DB**

2255 To avoid case-sensitivity issues while using the search and sort functionalities in the
2256 AlertEnterprise applications, enable “Case Insensitiveness” search in the database. By default, it
2257 is set as case-sensitive.
2258

2259 Follow these steps to avoid case-sensitivity issues:

2260 1. Create a trigger to support case insensitiveness.

```
2261 ******/
2262 create or replace
2263 trigger set_nls_onlogon
2264 AFTER LOGON ON SCHEMA
2265 DECLARE
```

```
2267 BEGIN
2268 EXECUTE IMMEDIATE 'ALTER SESSION SET NLS_SORT="BINARY_CI"';
2269 EXECUTE IMMEDIATE 'ALTER SESSION SET NLS_COMP="LINGUISTIC"';
2270 END set_nls_onlogon;
2271 /*****
```

2272 2. Restart the AlertEnterprise Application server.

2273

2274 The effect may not be visible in some client tools like SQL Developer. To see the effect in the
2275 SQL Developer tool: :

2276 1. Open SQL Developer and click Tools > Preferences.

2277 2. Click Database > NLS and do the following:

2278 • Set the Sort option to BINARY_CI.

2279 • Set the Comparison option to LINGUISTIC.

2280

2281 **Enabling Support for International Characters**

2282 Storage of character data is controlled by character-set setting at database level. It is
2283 recommended to have the following database settings to support international characters:

2284

2285 For Oracle:

2286 NLS_CHARACTERSET = AL32UTF8

2287 NLS_NCHAR_CHARACTERSET = AL16UTF16

2288

2289 For SQL Server:

2290 • Server Collation = SQL_Latin1_General_CI_AS

2291

2292 **Deploying the Application**

2293 After you have successfully configured the database, proceed to deploy the AlertEnterprise
2294 product on your web application server. The following deployment steps are required for the
2295 Tomcat 6.0 version:

2296

2297 1. Stop the Tomcat server from the Windows services if it is already running. Click Start >
2298 Run and type services.msc then click OK. Select the Apache Tomcat and click the
2299 Stop Service icon to stop the service.

2300 2. Copy the *AlertEnterprise.war*, *AccessMap.war* (if you possess AlertInsight
2301 license), and *AlertEnterpriseHelp.war*, and *jasperserver-pro.war* files
2302 to <Tomcat installation folder>\webapps\ path.

2303 3. You need to copy password management war file *AIPM.war* to <Tomcat
2304 installation folder>/webapps if you possess license for the Password
2305 Management application.

2306 4. Create a new folder *AlertCommonLib* and *AlertExternalLib* under
2307 <Tomcat Installation Folder>.

2308 5. Extract *AlertCommonLib.zip* under *AlertCommonLib* folder. You will see
2309 many new files in this folder.
2310 6. Edit the *<Tomcat Installation Folder>\conf\catalina.properties*
2311 using any editor and add append the following to the *common.loader* as described
2312 below:
2313 *common.loader=\${catalina.base}/lib,\${catalina.base}/lib/*.jar,\${catalina.home}/lib,\${cat
2314 alina.home}/lib/*.jar,\${catalina.home}/AlertCommonLib/*.jar,\${catalina.home}/AlertExt
2315 ernalLib/*.jar* (bold path added). Save the file and close the editor.
2316 7. Add Database Connection. Add a new *<resource>* entry as below with name
2317 "jdbc/alntdb" in *< Tomcat installation folder>\conf\context.xml*.
2318 Replace the code in *<>* with relevant information.
2319
2320 For MY-SQL Server:
2321
2322 <Resource
2323 description="DB Connection"
2324 name="jdbc/alntdb" auth="Container"
2325 type="com.mchange.v2.c3p0.ComboPooledDataSource"
2326 factory="org.apache.naming.factory.BeanFactory"
2327 user="username"
2328 password="password"
2329 jdbcUrl="jdbc:mysql://<IP of DB Server>:3306/<DB Instance Name>"
2330 driverClass="com.mysql.jdbc.Driver"
2331 maxPoolSize="100" minPoolSize="5" acquireIncrement="5"
2332 numHelperThreads="20" maxIdleTime="600"
2333 maxIdleTimeExcessConnections="300"
2334 debugUnreturnedConnectionStackTraces="true"
2335 unreturnedConnectionTimeout="900"
2336 />
2337
2338 For repository setting in same *context.xml*, add the following entry:
2339
2340 <ResourceLink name="AlertEnterpriseRepo" global="AlertEnterpriseRepo"
2341 type="javax.jcr.Repository" />
2342
2343 For ActiveMQ settings in same *context.xml*, add the following entry:
2344
2345 <Resource name="jms/ConnectionFactory"
2346 auth="Container"
2347 type="org.apache.activemq.ActiveMQConnectionFactory"
2348 description="JMS Connection Factory"
2349 factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2350 brokerURL="tcp://localhost:61616"

```
2351     brokerName="LocalActiveMQBroker"
2352     useEmbeddedBroker="false"/>
2353
2354 <Resource name="jms/requestSubmissionQueue"
2355   auth="Container"
2356   type="org.apache.activemq.command.ActiveMQQueue"
2357   description="JMS Queue requestSubmissionQueue"
2358   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2359   physicalName="requestSubmissionQueue"/>
2360
2361 <Resource name="jms/requestApprovalQueue"
2362   auth="Container"
2363   type="org.apache.activemq.command.ActiveMQQueue"
2364   description="JMS Queue requestApprovalQueue"
2365   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2366   physicalName="requestApprovalQueue"/>
2367
2368 <Resource name="jms/autoApprovalQueue"
2369   auth="Container"
2370   type="org.apache.activemq.command.ActiveMQQueue"
2371   description="JMS Queue autoApprovalQueue"
2372   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2373   physicalName="autoApprovalQueue"/>
2374
2375 <Resource name="jms/queue/taskSubmissionQueue"
2376   auth="Container"
2377   type="org.apache.activemq.command.ActiveMQQueue"
2378   description="JMS Queue taskSubmissionQueue"
2379   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2380   physicalName="taskSubmissionQueue"/>
2381
2382 <Resource name="jms/queue/taskRejectionQueue"
2383   auth="Container"
2384   type="org.apache.activemq.command.ActiveMQQueue"
2385   description="JMS Queue taskRejectionQueue"
2386   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2387   physicalName="taskRejectionQueue"/>
2388
2389 <Resource name="jms/queue/projectCancelQueue"
2390   auth="Container"
2391   type="org.apache.activemq.command.ActiveMQQueue"
2392   description="JMS Queue projectCancelQueue"
```

```
2393     factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2394     physicalName="projectCancelQueue"/>
2395
2396 <Resource name="jms/queue/projectCompleteQueue"
2397   auth="Container"
2398   type="org.apache.activemq.command.ActiveMQQueue"
2399   description="JMS Queue projectCompleteQueue"
2400   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2401   physicalName="projectCompleteQueue"/>
2402
2403 <Resource name="jms/eventRequestQueue"
2404   auth="Container"
2405   type="org.apache.activemq.command.ActiveMQQueue"
2406   description="JMS Queue eventRequestQueue"
2407   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2408   physicalName="eventRequestQueue"/>
2409
2410 <Resource auth="Container" description="my Queue"
2411   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2412   name="jms/reqQueue" physicalName="requestQueue"
2413   type="org.apache.activemq.command.ActiveMQQueue"/>
2414
2415 <Resource auth="Container" description="my Queue"
2416   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
2417   name="jms/resQueue" physicalName="responseQueue"
2418   type="org.apache.activemq.command.ActiveMQQueue"/>
2419
2420   8. Edit <Tomcat installation folder>\conf\server.xml. Replace the
2421   code in <> with relevant information:
2422
2423 <GlobalNamingResources>
2424   <!-- Editable user database that can also be used by
2425       UserDatabaseRealm to authenticate users
2426   -->
2427 <Resource auth="Container"
2428   configFile="/AlertEnterpriseRepo/repository.xml"
2429   description="AlertEnterprise Repository"
2430   factory="com.alnt.repository.jndi.JackrabbitRepositoryFactory"
2431   homeDir="/AlertEnterpriseRepo" name="AlertEnterpriseRepo"
2432   type="javax.jcr.Repository"/>
2433
2434 <Resource auth="Container" description="Rule Engine Service"
2435   factory="com.sae.ruleengine.jndi.RuleEngineFactory"
```

```
2436 name="Sedna" password="MANAGER" type="com.sae.ruleEngine.RuleEngine"
2437 username="SYSTEM"/>
2438 <Resource name="UserDatabase" auth="Container"
2439 type="org.apache.catalina.UserDatabase"
2440 description="User database that can be updated and saved"
2441 factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
2442 pathname="conf/tomcat-users.xml"/>
2443 </GlobalNamingResources>
2444
2445
2446 9. Open <Webserver installation folder>|bin location and double-click tomcat5w.exe. Click
2447 Java tab and under Java options add the following lines at the end:
2448
2449 -XX:PermSize=512m
2450 -XX:MaxPermSize=512m
2451 -Xms1024m
2452 -Xmx1024m
2453 -Djs.license.directory=C:\AlertApplication\Tomcat
2454 6.0\webapps\jasperserver-pro
2455 -Dcom.alnt.fabric.loadInitData=force
2456 -Dalert.db.update=update
2457
2458 Note: These settings may vary with the volume of RAM in the server.
2459
2460 10. Start the Tomcat server.
2461 11. Start the AlertEnterprise application by using the address, which is of the form
2462 http://<Server IP Address>:8080/AlertEnterprise.
2463 Note: The name and contents of the init script will vary depending on the database
2464 management system of the organization. 8080 is the default port on local host. If you
2465 want to change it, then change it in the sever.xml.
2466 12. Log on to the application by using admin credentials. You should be able to view Home
2467 screen of the application.
2468 9.3 ALERTENTERPRISE APPLICATION CONFIGURATIONS FOR THE RSA BUILD
2469 Systems/Connectors
2470 9.3.1 System Type Import of DB Connector:
2471 1. Log in to Application.
2472 2. Go to Setup tab > Manual Configuration > Import/Export.
2473 3. Check System Types and click on Import.
```

2474 4. Select the .csv files, which are there in the software build package under connector
 2475 \ALNTDbconnector\InitDataFiles folder.

2476 5. After selecting all the files, click on the Upload button.

2477 6. Refresh page until it shows as success or failed.

2478 7. Restart the server if required.

2479 9.3.2 **System Types Param of DB Connector:**

2480 1. Log in to Application.

2481 2. Go to Setup tab >Manual Configuration >Systems > System Types.

2482 3. Search for Connector named “DBConnector” and click on Modify button.

2483 4. Click on Next button.

2484 5. Add the following attributes one by one and click on the ADD button –
 2485 The following fields need to be provided under Name field and Label can be any user-
 2486 friendly name see Figure 130.

2487 CREATE_USER0
 2488 UPDATE_USER0
 2489 LOCK_USER0
 2490 UNLOCK_USER0
 2491 DELIMIT_USER0
 2492 USER_PROVISIONED0
 2493 ADD_ROLES0
 2494 DEPROVE_ROLES0
 2495 CREATE_USER1
 2496 LOCK_USER1

Name	Label	Parameter Level
jndiName	Jndi Name	Mandatory
DATE_TIME_FORMAT	Date and Time Forma...	Mandatory
DATE_TIME	Date Format	Mandatory
passwordColumnName	Passwrd Column Name	Mandatory
userIdColumnName	UserId Column Name	Mandatory
EXTERNAL_USER_ID_AT...	External UserId Att...	Mandatory
MODIFIED_ENTITLEMEN...	Fetch User Entitlem...	Mandatory
GET_ALL_USERS0	GET_ALL_USERS0	Mandatory
GET_INCREMENTAL_USE...	GET_INCREMENTAL_USE...	Mandatory
CREATE_USER0	Create CardHolder Q...	Mandatory
UPDATE_USER0	Update CardHolder Q...	Mandatory
LOCK_USER0	Lock CardHolder Que...	Mandatory

2497

2498

2499	UNLOCK_USER0	Unlock Card Holder ...	Mandatory
	DELIMIT_USER0	Change CardHolder V...	Mandatory
	USER_PROVISIONED0	Check Card Holder P...	Mandatory
	ADD_ROLES0	Assign Roles to Car...	Mandatory
	DEPROVE_ROLES0	Remove Roles From C...	Mandatory
	GET_GENERATED_USERI...	Retrieve User Id Qu...	Mandatory
2500	driverName	driverName	Mandatory
	url	URL	Mandatory
	userName	userName	Mandatory
	password	password	Mandatory

Figure 130. Guardian DB Connector Attributes

2502 **CONFIGURATION: Create “PACS AD” System**

2503 1. Setup > Manual Configuration > Systems > System.

2504 2. Click on New to create a new system.

2505 3. Definition...Enter the following:

2506 • System Type – LDAP from drop-down

2507 • Connector Name – PACS AD

2508 • Connector Description - PACS AD

2509 • Connector Long Description - PACS AD

2510 • Connector Type – LDAP (default)

2511 4. Click on Next.

2512 5. Parameters...Enter the following:

2513 Table 9. Guardian PACS AD Parameters

System Param Name	System Param Value
bindPass	o60ypIUQT3IOqHmbuRWeuw==
useSSL	FALSE
baseDns	DC=pacs-es-idam-b1,DC=test
groupBaseDn	DC=pacs-es-idam-b1,DC=test
reconBaseDN	
getIncrementGrpChanges	FALSE

System Param Name	System Param Value
wsdlURL	
wsUserName	
wsPwd	
rootLevelDomain	
cookieLocation	
adUserName	
SYS_CON_ATTR_POST_CREATE_SCRIPT	
SYS_CON_ATTR_POST_CREATE_SCRIPT_PARAMS	
objectClass	User
Skip provisioning	Yes
lastModifiedColumnRole	whenChanged
lastModifiedColumn	whenChanged
host	172.16.7.2
port	389
bindDn	CN=AlertEnterprise, CN=Users,DC=pacs-es-idam-b1,DC=test

2514 6. Click on Next.

2515 7. Attributes...Enter the following:

2516 • Application – Alert Access

2517 • Check the following boxes – Provisioning, Role Management, Offline System.

2518 • Leave Connector Category as Production.

2519 • Time Zone – Greenwich Mean Time from drop-down

2520 8. Click on Next.

2521 9. Click on Save.

2522 **CONFIGURATION: Create “Identity DB” System**

2523 1. Setup > Manual Configuration > Systems > System.

2524 2. Click on New to create a new system.

2525 3. Definition...Enter the following:

2526 • System Type – Database (JDBC J2EE) from drop-down

2527 • Connector Name – IDENTITYDB

2528 • Connector Description - IDENTITYDB

2529 • Connector Long Description - IDENTITYDB

2530 • Connector Type – Database (JDBC J2EE) (default)

2531 4. Click on Next.

2532 5. Parameters...Enter the following:

Table 10. Guardian Identity DB Parameters

System Param Name	System Param Value
driverName	
url	
userName	
password	
whereClause	
jndiName	java:comp/env/jdbc/alntdb

2534 6. Click on Next.

2535 7. Attributes...Enter the following:

2536 • Application – All

2537 • Check the following boxes – Provisioning, Certification, Identity Provider, Allow Modify Role and Allow Time Change.

2538 • Leave Connector Category as Production.

2539 • Time Zone – Eastern Daylight Time from drop-down

2540 8. Click on Next.

2541 9. Click on Save.

2543 CONFIGURATION: Create “ACCESSIT PACS” System

2544 1. Setup > Manual Configuration > Systems > System.

2545 2. Click on New to create a new system.

2546 3. Definition...Enter the following:

2547 • System Type – DBConnector from drop-down

2548 • Connector Name – ACCESSIT PACS

2549 • Connector Description - ACCESSIT PACS

2550 • Connector Long Description - ACCESSIT PACS

2551 • Connector Type – DBConnector (default)

2552 4. Click on Next.

2553 5. Parameters...Enter the following:

Table 11. Guardian ACCESSIT PACS Parameters

System Param Name	System Param Value
driverName	
URL	jdbc:sqlserver://<HOST_NAME>:<PORT>;databaseName=AI Universal
userName	DB User Name
password	DB User Password
Date and Time Format	CardholderID
External UserId Attribute	CardholderID
Create CardHolder Query	<pre>INSERT INTO [AIUniversal].[dbo].[Cardholders]([CardholderID],[LastName],[FirstName],[MiddleInitial],[CompanyID],[Notes],[LastModified],[LastModifiedByUser],[DateCreated],[CreatedByUser],[MemberOfAllSites],[UserText1],[UserText2],[UserText3],[UserText4],[UserText5],[UserText6],[UserText7],[UserText8],[UserText9],[UserText10],[UserText11],[UserText12],[UserText13],[UserText14],[UserText15],[UserText16],[UserText17],[UserText18],[UserText19],[UserText20],[Department],[UserDate1],[UserDate2],[UserDate3],[UserDate4],[UserDate5],[UserNumeric1],[UserNumeric2],[UserNumeric3],[UserNumeric4],[UserNumeric5],[CardholderStatus],[CardholderActiveDate],[CardholderExpireDate]) VALUES (NEWID(),\$LastName,\$FirstName,\$MiddleInitial,\$CompanyID,\$Notes,GetUTCDate(),'alerte nt',GetUTCDate(),'alertent','1',\$UserText1,\$UserText2,\$UserText3,\$UserText4,\$UserText5,\$UserText6,\$UserText7,\$UserText8,\$UserText9,\$UserText_10,\$UserText_11,\$UserText_12,\$UserText_13,\$UserText_14,\$UserText_15,\$UserText_16,\$UserText_17,\$UserText_18,\$UserText_19,\$UserText_20,\$Department,\$UserDate1,\$UserDate2,\$UserDate3,\$UserDate4,\$UserDate5,\$UserNumeric1,\$UserNumeric2,\$UserNumeric3,\$UserNumeric4,\$UserNumeric5,'1',\$CardholderActiveDate,\$CardholderExpireDate)</pre>
Update CardHolder Query	update [dbo].[Cardholders] set LastModified=GetUTCDate() where CardholderID=\$CardholderID

System Param Name	System Param Value
Lock CardHolder Query	update [dbo].[Cardholders] set CardholderStatus='0' where CardholderID=\$CardholderID
Unlock Card Holder Query	update [dbo].[Cardholders] set CardholderStatus='1' where CardholderID=\$CardholderID
Check Card Holder Provisioned Query	select CardholderID from [dbo].[Cardholders] where CardholderID = \$CardholderID
Assign Roles to Card Holder Query	INSERT INTO [dbo].[CardholderAccessLevels] ([CardholderAccessLevelID], [CardholderID], [AccessLevelID], [LastModified], [ActivateDate], [DeactivateDate]) VALUES (NEWID(), \$CardholderID, (select AccessLevelID from [dbo].[AccessLevels] where AccessLevelName=\$ROLE_NAME), GetUTCDate(), NULL, NULL)
Remove Roles From Card Holder Query	delete from [dbo].[CardholderAccessLevels] where CardholderID=\$CardholderID and AccessLevelID=(select AccessLevelID from [dbo].[AccessLevels] where AccessLevelName=\$ROLE_NAME)
Retrieve User Id Query	select CardholderID from [dbo].[Cardholders] where UserText1=\$UserText1
CREATE_USER1	INSERT INTO [AIUniversal].[dbo].[Cards] ([CardID], [CardholderID], [CardNumber], [FacilityCode], [PINNumber], [PINExempt], [APBExempt], [UseExtendedAccessTimes], [CardStatus], [ActiveDate], [ExpireDate], [UserLevel], [UseCustomReporting], [EventInfo], [Notes], [LastModified], [LastModifiedByUser], [DateCreated], [CreatedByUser], [IssueLevel], [DeactivateExempt], [VacationDate], [VacationDuration], [UseCount], [TempDeactivateStart], [TempDeactivateEnd], [Classification], [IPLocksetUserType], [IPLocksetAccessMode], [IPLocksetCredentialFormat], [IPLocksetAccessAlways], [RawPrimaryCredential], [LargeEncodedCardID], [EmbossedNumber]) VALUES (NEWID(), (select CardholderID from [dbo].[Cardholders] where UserText1=\$UserText1), \$CardNumber, \$FacilityCode, \$PIN, '0', '0', '0', '1', NULL, NULL, '0', '0', NULL, SYSDATETIME(), 'alertent', SYSDATETIME(), 'alertent', '0', '0', NULL, '0', '255', NULL, NULL, 'Active', NULL, NULL, NULL, NULL, NULL, NULL, '')
LOCK_USER1	update [AIUniversal].[dbo].[Cards] set CardStatus='0', Classification='InActive' where [CardNumber]= \$CardNumber

2555 6. Click on Next.

2556 7. Attributes...Enter the following:

- 2557 • Application – All
- 2558 • Check the following boxes – Provisioning, Role Management, and Offline System.
- 2559 • Leave Connector Category as Production.
- 2560 • Time Zone – Eastern Daylight Time from drop-down

2561 8. Click on Next.

2562 9. Click on Save.

2563 **Identity & Access– Enable Identity**

2564 1. Setup > Manual Configuration >Identity & Access>Enable Identity.

2565 2. Enable the following for “Identity DB” system, see Figure 131.



2566

Figure 131. Guardian Identity Configuration

2568 9.3.3 Identity & Access– User Field Mapping

- 2569 1. Setup > Manual Configuration > Identity & Access > User Field Mapping.
- 2570 2. Select User = Identity (from drop-down) and click on Go.
- 2571 3. Click the Create New button.
Select values for respective fields and hit on save (Refer to below sheet for values selection.)
- 2574 4. Repeat Steps 1–4 for all fields in the sheet.

2575 Follow the steps above to configure the User Field mappings manually. You can match the
2576 values in the file at https://nccoe.nist.gov/sites/default/files/nccoe/UserFieldMapping_data.csv.

2577 Identity & Access > Recon Authoritative Fields

- 2578 1. Setup > Manual Configuration > Identity & Access > Recon Authoritative Fields.
- 2579 2. Click on Create.
- 2580 3. Enter the following shown in Figure 132.

Recon Authoritative Fields		Authoritative Field
<input type="checkbox"/>	Systems	
<input type="checkbox"/>	DBCONNECTOR	FirstName
<input type="checkbox"/>	DBCONNECTOR	LastName
<input type="checkbox"/>	PACS AD	PacsAllDoors
<input type="checkbox"/>	PACS AD	PacsHomeAccess
<input type="checkbox"/>	PACS AD	PacsWorkAccess
<input type="checkbox"/>	PACS AD	FirstName
<input type="checkbox"/>	PACS AD	LastName

2581

Figure 132. Guardian Recon Authoritative Fields

2583 Identity & Access > Request Categories

- 2584 1. Setup > Manual Configuration > Identity & Access > Request Categories.
- 2585 2. Click on New.
- 2586 3. Enter following at define Request Category screen:
 - 2587 • Name – New Hire
 - 2588 • Description – New Hire

2589 • Visible – Yes
2590 • Hover Text –
2591 • Provisioning Actions – Create User, Change Roles
2592 • Request Category Type - Resources
2593 • Display the following in USS – Enterprise Roles
2594 4. Click on Save.
2595 5. Repeat similar to above for following Request Categories:

2596 **Termination**

2597 • Name – Change Access
2598 • Description – Change of Access
2599 • Visible – Yes
2600 • Hover Text –
2601 • Provisioning Actions – Create User, Change Roles, Change User
2602 • Display the following in USS – Resources
2603 • Add Existing – Systems and Remove Roles
2604 6. Click on Save.

2605 **ChangeAccess**

2606 ○ Name – Terminate
2607 ○ Description – Terminate User
2608 ○ Visible – Yes
2609 ○ Hover Text –
2610 ○ Provisioning Actions – Lock User, Change Roles
2611 ○ Display the following in USS – Resources
2612 ○ Add Existing – Systems
2613 7. Click on Save.

2614 **Identity & Access>Provisioning>Provisioning Mapping**

2615 1. Setup > Manual Configuration > Identity & Access > Provisioning > Provisioning Mapping.
2616 2. On the next screen select System and click Next.

2617 3. Follow the mapping shown in Figure 133 to Create/Update provisioning mappings for
 2618 the ACCESS IT PACS system.

DB Connector Attribute Mapping								
		DB Connector Connector Name		ACCESSIT PACS				
		Connector Type		DBConnector				
□	DB Connector Attribute	Mandatory	AlertEnterprise Attrib...	Default Value	Editable	Visible	Validati...	Is User...
□	UserText1	No	UserId		No	No	No	No
□	FirstName	Yes	FirstName		Yes	Yes	No	No
□	LastName	Yes	LastName		Yes	Yes	No	No
□	CompanyID	No	Priority		No	No	No	No
□	CardholderID	Yes	UserId		Yes	Yes	No	No

2619

2620 *Figure 133. Guardian DB Connector Attribute Mapping*

2621 **User Data> User Data Source**

2622 1. Setup > Manual Configuration > User Data > User Data Source.

2623 2. Follow the mappings and configurations found in the files at
 2624 <https://nccoe.nist.gov/sites/default/files/nccoe/UserManagement-UserDataSource.zip>.
 2625 Create/Update accordingly.

2626 **User Data> User Mapping**

2627 1. Setup > Manual Configuration > User Data > User Mapping.

2628 2. Select “Identity DB” system from the list and click on Save button.

2629 **Policy Engine> Rules**

2630 1. Setup > Manual Configuration > Policy Engine > Rules.

2631 2. Click on New and add the following:

2632

Table 12. Guardian Policy Engine Rules

Rule Name	Entity Type	Rule Type	Description	Applicable to	Attributes	Drop down value	Selection Value
All Door Access New	Workflow	AlertAccess	All Door Access New	Suggest/Default	PacsALLDoors AND Request Category	Equals	1. True and New Hire 2. True and Remove User Access 3. True and ChangeAccess
Home Access Level New	Workflow	AlertAccess	Home Access Level New	Suggest/Default	PacsALLDoors AND Request Category	Equals	1. True and New Hire 2. True and Remove User Access 3. True and ChangeAccess
WO Access Level New	Workflow	AlertAccess	WO Access Level New	Suggest/Default	PacsALLDoors AND Request Category	Equals	1. True and New Hire 2. True and Remove User Access 3. True and ChangeAccess

2633

2634

2635 **Policy Engine> Suggest/Default Access**

2636 1. Setup > Manual Configuration > Policy Engine > Suggest/Default Access.

2637 2. Click on New and enter the following:

2638 *Table 13. Guardian Policy Engine Suggest/Default Access*

Name	Type	Rule Name	Search By	Default System	Selected Role
All Door Access	Default	All Door Access NEW	Systems	ACCESSIT PACS	ALL DOORS
Home Access Level	Default	Home Access Level	Systems	ACCESSIT PACS	Home Access Level
WO Access Level	Default	Home Access Level	Systems	ACCESSIT PACS	WO Access Level
NewHireDefaultSystems	Default	NewHireDefaultSystems	Systems	ACCESSIT PACS	

2639

2640 **Policy Engine>Rule Action Handler**

2641 1 – Setup > Manual Configuration > Policy Engine > Rule Action Handler.

2642 2 – Click New and create the following Action Handlers:

2643 *Table 14. Guardian Policy Engine Rule Action Handler*

Action Handler Name	Workflow	Task Type	Value	Priority	Update Identity Info	Evaluate Enterprise Role
Recon New Hire	AlertAccess	Recon Create Request	New Hire	0	Yes	No
Recon terminate Handler	AlertAccess	Recon Create Request	Terminate	0	Yes	No
Recon Error Handler	AlertAccess	Recon Exception Record Task		0		

ReconChangeHandler	AlertAccess	Recon Create Request	Change Access	0	Yes	No
--------------------	-------------	----------------------	---------------	---	-----	----

2644

2645 **Policy Engine>Policy Designer**

2646 1. Setup > Manual Configuration > Policy Engine > Policy Designer

2647 2. Select New to create new Policy designer as:

2648 **User Policy New**

2649 1. Name – User Policy New

2650 2. Rule Type – AlertAccess

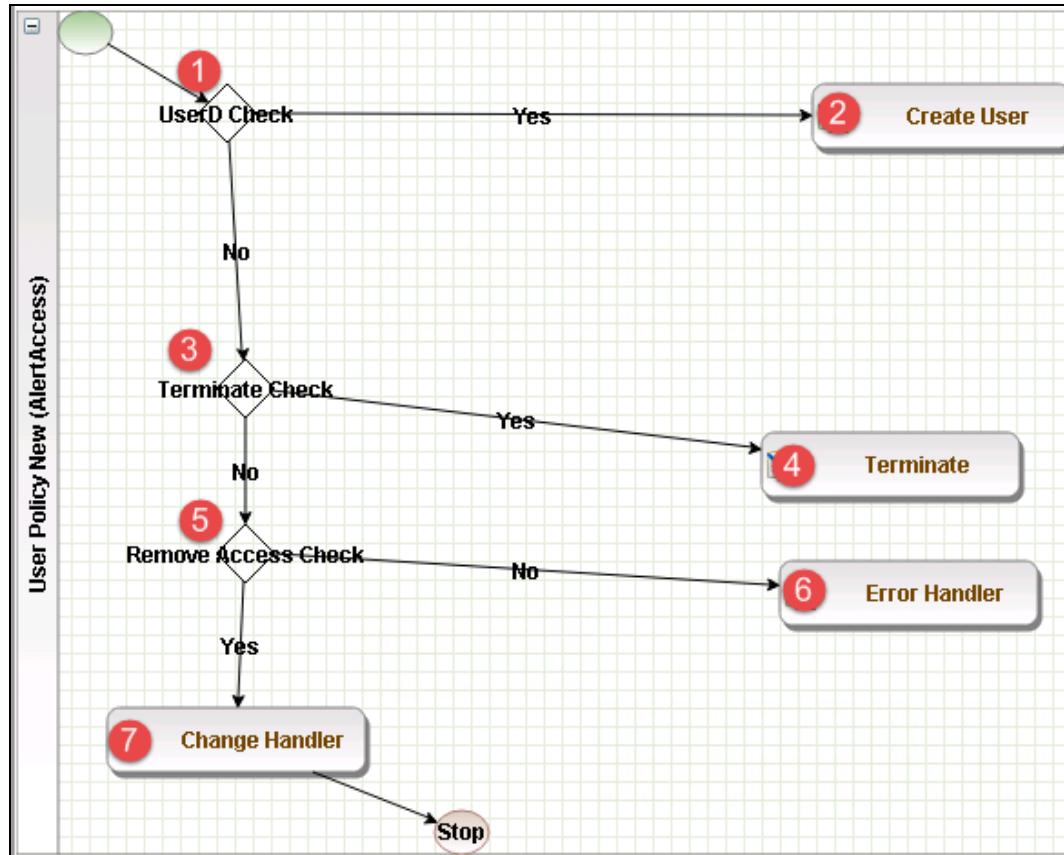
2651 3. Description – User Policy

2652 4. Priority – 29

2653 5. Active – Yes

2654 6. Default Process – No

2655 Figure 134 depicts the new policy interface to create the User Policy described above.



2656

2657

Figure 134. Guardian User Policy

2658 The following table describes User Policy New.

2659

Table 15. Guardian User Policy

Step	Name	Type	Condition	Is Task handler	Task Handler	Update Query
1	User ID Check	Decision	\$masterUser[UserId].size='0'			
2	Create User	Task Handler		Yes	Recon New Hire	
3	Terminate Check	Decision	\$checkStatus[UserStatus,Active,InActive].action='LOCK'			
4	Terminate	Task Handler		Yes	Recon Terminate	

Step	Name	Type	Condition	Is Task handler	Task Handler	Update Query
					Handler	
5	Remove Access Check	Decision	\$checkAuthFields[].[status='Yes'			
6	Error Handler	Task Handler		Yes	Recon Error Handler	
7	Change Handler	Task Handler		Yes	Recon Change Handler	

2660

2661 ***Job Scheduler>Triggers Field Map***

- 2662 1. Setup > Manual Configuration > Job Scheduler > Triggers Field Map
- 2663 2. Click on New.
- 2664 3. Enter Group Name – PACSAD Field Map
- 2665 4. Description – PACSAD Field Mapping
- 2666 5. Select Type – Reconciliation
- 2667 6. After creating Field Map, select the newly created map and select Configure.
- 2668 7. Click New and create mapping per below table.

2669

Table 16. Guardian Job Scheduler Triggers Field Map

AE Attribute	Mapped Key	userType	roleType	userRole	userBadge	userEntRoleType	User Training Type
sAMAccountName	UserId	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
accountExpires	ValidTo	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
givenName	FirstName	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
sn	LastName	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
userAccountControl	statusLDAP	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
pacsAllDoors	PacsAllDoors	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
pacsHomeAccess	PacsHomeAccess	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
pacsWorkAccess	PacsWorkAccess	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE

2670

2671 **Job Scheduler>Triggers**

2672 1. Setup > Manual Configuration > Job Scheduler > Triggers

2673 2. Click New and create the following Triggers:

2674 [AlertDbConnectorTrigger](#)

2675

2676

Table 17. Guardian Job Scheduler Triggers

Name	PACSAD Trigger
Description	PACSAD Trigger
Type	Reconciliation
Batch Size	100
Number of Attempts	3
Policy Designer for	User policy New

Users/Roles	
System: Reconciliation From	PACS AD
Reconciliation System	PACS AD
Field Mapping Group	PACSAD Field Map
User Type	True
User Role	True

2677

2678 **Job Scheduler>Scheduler**

2679 1. Setup > Manual Configuration > Job Scheduler > Scheduler.

2680 2. Click New and enter the following as shown in Figure 135:

2681 • Job Type – Reconciliation Job

2682 • Job Name - <Job Name>

2683 • Reconciliation for – User

2684 • Reconciliation Type – Incremental Reconciliation

2685 • Reconciliation Triggers – PACSAD Trigger

2686 • Select the schedule as Immediate, Once, periodic or Advance. For Periodic Job,
2687 specify the Job Start date, End date, and duration of job frequency.

The screenshot shows a configuration dialog for a 'Reconciliation Job'. The job is named 'PACS AD User Reconciliation' and is set to be 'private'. It is a 'Global' job. The 'Reconciliation For' dropdown shows 'Users', 'Roles', and 'User Training'. The 'Reconciliation Type' is 'Incremental Reconciliation'. The 'Reconciliation Triggers' is 'PACSAD Trigger'. The 'Init Date Load' is 'No'. The 'Create/Update Scheduled Jobs' section shows the job is set to 'Periodically'. The 'Time Zone' is '(GMT-05:00) America/New_York'. The 'Start At' is '06/08/2015' and the 'End At' is '06/08/2016'. The 'Rerun every' is '2'. The scheduling details show '20' [hrs] and '58' [minutes] for the first interval, and '20' [hrs] and '58' [minutes] for the second interval. The 'Repeat Duration' is 'Minutes' and the 'Repeat Unit' is '2'. At the bottom are 'Save' and 'Cancel' buttons.

2688

2689

Figure 135. Guardian Reconciliation Job

2690 3. Click Save.

2691 **9.4 SECTION 3. ALERTENTERPRISE APPLICATION CONFIGURATIONS FOR THE CA BUILD**

2692 9.4.1 System Type Import of DB Connector:

- 2693 1. Log in to Application.
- 2694 2. Go to Setup tab > Manual Configuration > Import/Export
- 2695 3. Check System Types and click on Import.
- 2696 4. Select the .csv files, which are there in software build package under Connector
- 2697 \ALNTDbconnector\InitDataFiles folder.
- 2698 5. After selecting all the files, click on Upload button.

2699 6. Refresh page until it shows as success or failed.

2700 7. Restart the server if required.

2701 9.4.2 **System Types Param of DB Connector:**

2702 1. Log in to Application.

2703 2. Go to Setup tab> Manual Configuration _> Systems > System Types

2704 3. Search for Connector named “DBConnector” and click on Modify button.

2705 4. Click on Next.

2706 5. Add the following attributes one by one and click on the ADD button.

2707 The following fields in Table 18 need to be provided under Name field and Label can
2708 be any user-friendly name as shown in

<input type="checkbox"/>	MODIFIED_ENTITLEMEN...	Fetch User Entitlem...	Mandatory
<input type="checkbox"/>	GET_ALL_USERS0	GET_ALL_USERS0	Mandatory
<input type="checkbox"/>	GET_INCREMENTAL_USE...	GET_INCREMENTAL_USE...	Mandatory
<input type="checkbox"/>	CREATE_USER0	Create CardHolder Q...	Mandatory
<input type="checkbox"/>	UPDATE_USER0	Update CardHolder Q...	Mandatory
<input type="checkbox"/>	LOCK_USER0	Lock CardHolder Que...	Mandatory

2709
2710 and Figure 136: (If the name or label already exists do not add)

2711

Table 18. Guardian Name and Label Fields

Name	Label
jndiName	Jndi Name
DATE_TIME_FORMAT	Date and Time Format
DATE_TIME	Date Format
passwordColumnName	Passwrd Column Name
userIdColumnName	UserId Column Name
EXTERNAL_USER_ID_ATTRIBUTE	External UserId Attribute
MODIFIED_ENTITLEMENTS	Fetch User Entitlement based on last modified date(not by user)
GET_ALL_USERS0	GET_ALL_USERS0
GET_INCREMENTAL_USERS0	GET_INCREMENTAL_USERS0

CREATE_USER0	Create CardHolder Query
UPDATE_USER0	Update CardHolder Query
LOCK_USER0	Lock CardHolder Query
UNLOCK_USER0	Unlock Card Holder Query
DELIMIT_USER0	Change CardHolder Validity Query
USER_PROVISIONED0	Check Card Holder Provisioned Query
ADD_ROLES0	Assign Roles to Card Holder Query
DEPROVE_ROLES0	Remove Roles From Card Holder Query
GET_GENERATED_USERID0	Retrieve User Id Query
driverName	driverName
url	URL
userNames	userNames
passwords	passwords
CREATE_USER1	CREATE_USER1
LOCK_USER1	LOCK_USER1

2712

<input type="checkbox"/>	Name	Label	Parameter Level
<input type="checkbox"/>	jndiName	Jndi Name	Mandatory
<input type="checkbox"/>	DATE_TIME_FORMAT	Date and Time Forma...	Mandatory
<input type="checkbox"/>	DATE_TIME	Date Format	Mandatory
<input type="checkbox"/>	passwordColumnName	Passwrd Column Name	Mandatory
<input type="checkbox"/>	userIdColumnName	UserId Column Name	Mandatory
<input type="checkbox"/>	EXTERNAL_USER_ID_AT...	External UserId Att...	Mandatory

2713

<input type="checkbox"/>	MODIFIED_ENTITLEMEN...	Fetch User Entitelm...	Mandatory
<input type="checkbox"/>	GET_ALL_USERS0	GET_ALL_USERS0	Mandatory
<input type="checkbox"/>	GET_INCREMENTAL_USE...	GET_INCREMENTAL_USE...	Mandatory
<input type="checkbox"/>	CREATE_USER0	Create CardHolder Q...	Mandatory
<input type="checkbox"/>	UPDATE_USER0	Update CardHolder Q...	Mandatory
<input type="checkbox"/>	LOCK_USER0	Lock CardHolder Que...	Mandatory

2714

2715	UNLOCK_USER0	Unlock Card Holder ...	Mandatory
	DELIMIT_USER0	Change CardHolder V...	Mandatory
	USER_PROVISIONED0	Check Card Holder P...	Mandatory
	ADD_ROLES0	Assign Roles to Car...	Mandatory
	DEPROVE_ROLES0	Remove Roles From C...	Mandatory
	GET_GENERATED_USERI...	Retrieve User Id Qu...	Mandatory

2716 *Figure 136. Guardian DB Connector Attributes*2717 9.4.3 **Create System Connectors for all Target Systems**

2718

2719 **1. CONFIGURATION: Create connector for “Alert User Database (External)”**2720 This connector is required to connect the Alert user table exposed to third-party systems (CA in
2721 this case) and get the data.

2722 Steps to create this connector:

2723 1. Setup Tab > Manual Configuration > Systems > System.

2724 2. Click New to create a new system.

2725 3. Definition...Enter the following:

2726 • System Type – DBConnector

2727 • Connector Name – ALERTDBCONNECTOR

2728 • Connector Description – ALERT DB CONNECTOR

2729 • Connector Long Description – ALERT DB CONNECTOR

2730 • Connector Type – DbConnector (Label)

2731 4. Click on Next.

2732 5. Parameters...Enter the following:

2733 *Table 19. Guardian Manual Configuration System Parameters*

System Param Name	System Param Value
Jndi Name	java:comp/env/jdbc/alertdb
Date and Time Format	MM/dd/yyyy HH:mm:ss
GET_ALL_USERS0	select UserId, FirstName,LastName,Email,WorkPhone,HomePhone,Department,EmployeeType,PacsAllDoor,CASE WHEN PacsAllDoor='1' then 'TRUE' Else 'FALSE' END as PacsAllDoor,CASE WHEN PacsHomeAccess='1' then 'TRUE'else 'FALSE' END as PacsHomeAccess , CASE WHEN PacsWorkAccess='1' then 'TRUE' else 'FALSE' END as PacsWorkAccess,CardNumber,FacilityCode,LastModifiedDate,ValidFrom,ValidTo,Title,UserStatus,PIN

System Param Name	System Param Value
	from alnt_idm_user_dtls
GET_INCREMENTAL_USERS0	select UserId, FirstName,LastName,Email,WorkPhone,HomePhone,Department,EmployeeType,PacsAllDoor,CASE WHEN PacsAllDoor='1' then 'TRUE' Else 'FALSE' END as PacsAllDoor,CASE WHEN PacsHomeAccess='1' then 'TRUE' else 'FALSE' END as PacsHomeAccess , CASE WHEN PacsWorkAccess='1' then 'TRUE' else 'FALSE' END as PacsWorkAccess,CardNumber,FacilityCode,LastModifiedDate,ValidFrom,ValidTo,Title,UserStatus,PIN from alnt_idm_user_dtls where LastModifiedDate> STR_TO_DATE(\$LAST_RUN_DATE,'%m/%e/%Y %H:%i:%s') and UserStatus='Active'
External UserId Attribute	UserId
UserId Column Name	UserId

2734

2735 6. Click on Next.

2736 7. Attributes...Enter the following:

- 2737 • Application – Alert Access
- 2738 • Check the following boxes – Provisioning, Role Management, Offline System.
- 2739 • Leave Connector Category as Production
- 2740 • Time Zone – Eastern Daylight Time from drop-down

2741 *Note:* TimeZone should be same as the TimeZone where application is hosted.

2742 8. Click on Next.

2743 9. Click on Save.

2744

2745 **2. CONFIGURATION: Create “Identity DB” System**2746 This is connector is required for internal purposes. Ignore this step if **Identity DB** Connector
2747 already setup

2748 Steps to create this connector:

- 2749 1. Setup Tab > Manual Configuration > Systems > System.
- 2750 2. Click New to create a new system.
- 2751 3. Definition...Enter the following:
 - 2752 • System Type – Database (JDBC J2EE) from drop-down
 - 2753 • Connector Name – IDENTITYDB
 - 2754 • Connector Description - IDENTITYDB

2755 ● Connector Long Description - IDENTITYDB

2756 ● Connector Type – Database (JDBC J2EE) (default)

2757 4. Click on Next.

2758 5. Parameters...Enter the following:

2759

2760

Table 20. Guardian Identity DB Parameters

System Param Name	System Param Value
driverName	(use default)
url	(use default)
userName	(use default)
password	(use default)
whereClause	(use default)
jndiName	java:comp/env/jdbc/alntdb

2761 6. Click on Next.

2762 7. Attributes...Enter the following:

2763 • Application – All

2764 • Check the following boxes – Provisioning, Certification, Identity Provider, Allow

2765 Modify Role and Allow Time Change.

2766 • Leave Connector Category as Production

2767 • Time Zone – Eastern Daylight Time from drop-down

2768 8. Click on Next.

2769 9. Click on Save.

2770 3. **CONFIGURATION: Create “ACCESSIT PACS” System**

2771 This is connector is required for integrating with RS2 PACS system and performing various

2772 provisioning operations.

2773 Steps to create this connector:

2774 1. Setup Tab > Manual Configuration > Systems > System.

2775 2. Click New to create a new system.

2776 3. Definition...Enter the following:

2777 • System Type – DBConnector from drop-down

2778 • Connector Name – ACCESSIT PACS

2779 • Connector Description - ACCESSIT PACS

2780 • Connector Long Description - ACCESSIT PACS

2781 ● Connector Type – DBConnector (default)

2782 4. Click on Next.

2783 5. Parameters...Enter the following:

2784

Table 21. Guardian PACS DBConnector Parameters

System Param Name	System Param Value
driverName	com.microsoft.sqlserver.jdbc.SQLServerDriver
URL	<p>jdbc:sqlserver://<HOST_NAME>:<PORT>;databaseName=AI Universal</p> <p><HOST_NAME> should be replaced with the hostname of the RS2 PACS system</p>
username	Login User Name to connect to RS2 PACS database
Password	Login password to connect to RS2 PACS database
Date and Time Format	MM/dd/yyyy HH:mm:ss
External UserId Attribute	CardholderID
Create CardHolder Query	<pre>INSERT INTO [AIUniversal].[dbo].[Cardholders]([CardholderID],[LastName],[FirstName],[MiddleInitial],[CompanyID],[Notes],[LastModified],[LastModifiedByUser],[DateCreated],[CreatedByUser],[MemberOfAllSites],[UserText1],[UserText2],[UserText3],[UserText4],[UserText5],[UserText6],[UserText7],[UserText8],[UserText9],[UserText10],[UserText11],[UserText12],[UserText13],[UserText14],[UserText15],[UserText16],[UserText17],[UserText18],[UserText19],[UserText20],[Department],[UserDate1],[UserDate2],[UserDate3],[UserDate4],[UserDate5],[UserNumeric1],[UserNumeric2],[UserNumeric3],[UserNumeric4],[UserNumeric5],[CardholderStatus],[CardholderActiveDate],[CardholderExpireDate]) VALUES (NEWID(),\$LastName,\$FirstName,\$MiddleInitial,\$CompanyID,\$Notes,GetUTCDate(),'alertent',GetUTCDate(),'alertent','1',\$UserText1,\$UserText2,\$UserText3,\$UserText4,\$UserText5,\$UserText6,\$UserText7,\$UserText8,\$UserText9,\$UserText_10,\$UserText_11,\$UserText_12,\$UserText_13,\$UserText_14,\$UserText_15,\$UserText_16,\$UserText_17,\$UserText_18,\$UserText_19,\$UserText_20,\$Department,\$UserDate1,\$UserDate2,\$UserDate3,\$UserDate4,\$UserDate5,\$UserNumeric1,\$UserNumeric2,\$UserNumeric3,\$UserNumeric4,\$UserNumeric5,'1',\$CardholderActiveDate,\$CardholderExpireDate)</pre>
Update CardHolder Query	update [dbo].[Cardholders] set LastModified=GetUTCDate() where CardholderID=\$CardholderID
Lock CardHolder Query	update [dbo].[Cardholders] set CardholderStatus='0' where CardholderID=\$CardholderID
Unlock Card Holder Query	update [dbo].[Cardholders] set CardholderStatus='1' where CardholderID=\$CardholderID

System Param Name	System Param Value
Check Card Holder Provisioned Query	select CardholderID from [dbo].[Cardholders] where CardholderID = \$CardholderID
Assign Roles to Card Holder Query	INSERT INTO [dbo].[CardholderAccessLevels] ([CardholderAccessLevelID], [CardholderID], [AccessLevelID], [LastModified], [ActivateDate], [DeactivateDate]) VALUES (NEWID(), \$CardholderID, (select AccessLevelID from [dbo].[AccessLevels] where AccessLevelName=\$ROLE_NAME), GetUTCDate(), NULL, NULL)
Remove Roles From Card Holder Query	delete from [dbo].[CardholderAccessLevels] where CardholderID=\$CardholderID and AccessLevelID=(select AccessLevelID from [dbo].[AccessLevels] where AccessLevelName=\$ROLE_NAME)
Retrieve User Id Query	select CardholderID from [dbo].[Cardholders] where UserText1=\$UserText1
CREATE_USER1	INSERT INTO [AIUniversal].[dbo].[Cards] ([CardID], [CardholderID], [CardNumber], [FacilityCode], [PINNumber], [PINExempt], [APBExempt], [UseExtendedAccessTimes], [CardStatus], [ActiveDate], [ExpireDate], [UserLevel], [UseCustomReporting], [EventInfo], [Notes], [LastModified], [LastModifiedByUser], [DateCreated], [CreatedByUser], [IssueLevel], [DeactivateExempt], [VacationDate], [VacationDuration], [UseCount], [TempDeactivateStart], [TempDeactivateEnd], [Classification], [IPLocksetUserType], [IPLocksetAccessMode], [IPLocksetCredentialFormat], [IPLocksetAccessAlways], [RawPrimaryCredential], [LargeEncodedCardID], [EmbossedNumber]) VALUES (NEWID(), (select CardholderID from [dbo].[Cardholders] where UserText1=\$UserText1), \$CardNumber, \$FacilityCode, \$PIN, '0', '0', '0', '1', NULL, NULL, '0', '0', NULL, NULL, SYSDATETIME(), 'alertent', SYSDATETIME(), 'alertent', '0', '0', NULL, '0', '255', NULL, NULL, 'Active', NULL, NULL, NULL, NULL, NULL, NULL, NULL, '')
LOCK_USER1	update [AIUniversal].[dbo].[Cards] set CardStatus='0', Classification='InActive' where [CardNumber]=\$CardNumber

2785 6. Click on Next.

2786 7. Attributes...Enter the following:

- 2787 • Application – All
- 2788 • Check the following boxes – Provisioning, Role Management, and Offline System.
- 2789 • Leave Connector Category as Production
- 2790 • Time Zone – Eastern Daylight Time from drop-down

2791 8. Click on Next.

2792 9. Click on Save.

2793 **Form customization – Attributes**

2794 **Create New Custom Form Attributes**

2795 1. Setup > Manual Configuration > Form customization > Attributes
2796 2. Click on New Button
2797 3. Create new attribute called **PacsAllDoors** based on the information provided below in
2798 Table 22.
2799 4. Click Save

Table 22. *PacsAllDoors* Attributes

Field Name	Field Value
Name	PacsAllDoors
Label	PacsAllDoors
Description	PacsAllDoors
Visible	Yes
Mandatory	No
Read Only	No
Field Type	TextField (Select this value from drop down)
USS Create Request	Yes(Select CheckBox)
USS User Information	Yes(Select CheckBox)
Approver View	Yes(Select CheckBox)
Provisioning	Yes(Select CheckBox)
Create Request Sequence	10
User Info Sequence	10
Approver Sequence	10
Group Name	Personnel Information (Select this value from drop down)

2801
2802 5. **Repeat Steps 1-4 to create the following custom form attributes**
2803 1. Create **PacsHomeAccess** Attributes (See Table 23)

2804

Table 23. PacsHomeAccess Attributes

Field Name	Field Value
Name	PacsHomeAccess
Label	PacsHomeAccess
Description	PacsHomeAccess
Visible	Yes
Mandatory	No
Read Only	No
Field Type	TextField (Select this value from drop down)
USS Create Request	Yes(Select CheckBox)
USS User Information	Yes(Select CheckBox)
Approver View	Yes(Select CheckBox)
Provisioning	Yes(Select CheckBox)
Create Request Sequence	11
User Info Sequence	11
Approver Sequence	11
Group Name	Personnel Information (Select this value from drop down)

2805

2806

2. Create PacsWorkAccess Attributes (as shown in Table 24)

2807

Table 24. PacsWorkAccess Attributes

Field Name	Field Value
Name	PacsWorkAccess
Label	PacsWorkAccess
Description	PacsWorkAccess

Field Name	Field Value
Visible	Yes
Mandatory	No
Read Only	No
Field Type	TextField (Select this value from drop down)
USS Create Request	Yes(Select CheckBox)
USS User Information	Yes(Select CheckBox)
Approver View	Yes(Select CheckBox)
Provisioning	Yes(Select CheckBox)
Create Request Sequence	12
User Info Sequence	12
Approver Sequence	12
Group Name	Personnel Information (Select this value from drop down)

2808

2809

3. Create FacilityCode Attributes as shown in Table 25.

2810

Table 25. FacilityCode Attributes

Field Name	Field Value
Name	FacilityCode
Label	Facility Code
Description	Facility Code
Visible	Yes
Mandatory	Yes
Read Only	No
Field Type	TextField (Select this value from drop down)

Field Name	Field Value
USS Create Request	No
USS User Information	No
Approver View	No
Provisioning	Yes(Select CheckBox)
Create Request Sequence	
User Info Sequence	
Approver Sequence	
Group Name	Personnel Information (Select this value from drop down)

2811

2812

4. Create PIN Attributes as shown in Table 26.

2813

Table 26. PIN Atributes

Field Name	Field Value
Name	PIN
Label	PIN
Description	PIN
Visible	Yes
Mandatory	No
Read Only	No
Field Type	TextField (Select this value from drop down)
USS Create Request	Yes(Select CheckBox)
USS User Information	No(Select CheckBox)
Approver View	No(Select CheckBox)
Provisioning	Yes(Select CheckBox)
Create Request	12

Field Name	Field Value
Sequence	
User Info Sequence	
Approver Sequence	
Group Name	Personnel Information (Select this value from drop down)

2814

2815 **Modify Employee Type Attribute**

2816 1. Setup > Manual Configuration > Form customization > Attributes

2817 2. Select Employee Type Field from list of Attributes and Click **Modify**

2818 3. **Click on DropDown Values Icon**

2819 4. On the popup window, Click on New and Provide Employee in both Name and Label

2820 fields, Figure 137.

The screenshot shows a dialog box titled 'Create DropDownValues'. It contains two input fields: one for 'Name' (containing 'Employee') and one for 'Label' (containing 'Employee'). Below these fields are two buttons: 'Cancel' and 'Save'. The 'Save' button is highlighted with a blue border.

2821

Figure 137. Create DropDownValues

2822

5. Similarly configure values for Contractor field, Figure 138.

DropDown Values		
	Name	Label
<input type="checkbox"/>	Contractor	Contractor
<input type="checkbox"/>	Employee	Employee

2823

Figure 138. Contractor Field

2824 6. Click **Save** and then Click **Save** to save the configuration

2825 7. Ignore this step if these values already exists

2826 **Modify Status Attribute**

2827 1. Setup > Manual Configuration > Form customization > Attributes

2828 2. Select Status field from list of Attributes and Click **Modify**

2829 3. Click on DropDown Values Icon

2830 4. On the popup window Click on New and provide **Active** in both Name and Label

2831 fields, Figure 139.

2832

Create DropDownValues

*Name	Active	*Label	Active
Cancel	Save		

Figure 139. DropDownValues

2833

DropDown Values

<input type="checkbox"/>	Name	Label
<input type="checkbox"/>	Active	Active
<input type="checkbox"/>	InActive	InActive

Figure 140. InActive

2834

5. Similarly configure values for **InActive** field, Figure 140
 6. Click **Save** and then Click **Save** to save the configuration
 7. Ignore this step if these values already exists for Status field

2835 **Identity & Access– Enable Identity**

2836 1. Setup > Manual Configuration >Identity & Access>Enable Identity
 2837 2. Enable the following for Identity DB system as shown in Figure 141.

2841

Identity Configuration

<input type="checkbox"/>	Maintain Identities	Yes
<input type="checkbox"/>	Connector	IDENTITYDB
Reset Save		

Figure 141. Guardian Identity Configuration

2842 9.4.4 **Identity & Access– User Field Mapping**

2843 1. Setup > Manual Configuration > Identity & Access > User Field Mapping.
 2. Select User = Identity (from drop-down) and click Go.
 3. Click the Create New button.
 4. Select Custom Field, Primary Key, Visible In List, IsSearchable fields based on the table listed below. Select checkbox for these fields if it is specified as “Yes” otherwise, keep it as unselected.
 5. Click on Save button to save the record
 6. Repeat Steps 1–5 for all fields in the following table, Table 27. Ignore fields if pre-existing mapping already exists for a particular field.

2853

Table 27. User Field Mapping Table

Custom Field	Primary Key	Visible In List	IsSearchable
UserId	No	Yes	No
ValidFrom	No	Yes	No
ValidTo	No	Yes	No
FirstName	No	Yes	Yes
LastName	No	Yes	Yes
Email	No	No	No
Building	No	No	No
ManagerId	No	No	No
BadgeStatus	No	No	No
BadgeType	No	No	No
BadgeValidFrom	No	No	No
BadgeValidTo	No	No	No
Location	No	No	No
BadgeId	No	No	No
EmployeeType	No	No	No
Department	No	No	No
Password	No	No	No
Groups	No	No	No
ManagerName	No	No	No
ManagerLN	No	No	No
Manager	No	No	No
ManagerId	No	Yes	No
Status	No	No	No
Telephone	No	No	No
ImageUpload	No	No	No
Password_AD	No	No	No
PacsAllDoors	No	Yes	No
PacsHomeAccess	No	Yes	No
PacsWorkAccess	No	Yes	No

2854

2855 Identity & Access > Recon Authoritative Fields

2856 1. Setup > Manual Configuration > Identity & Access > Recon Authoritative Fields.

2857 2. Click on New.

2858 3. Select ALERTDBCONNECTOR from Systems Drop down and select Authoritative field as
 2859 PacsAllDoors as shown in

Create Recon Authoritative Fields

* Systems	ALERTDBCONNECTOR
* Authoritative Field	PacsAllDoors
Cancel	Save

2860

2861 *Figure 142. Authoritative Fields*

2862 4. Click Save button to save the mapping.
 2863 5. Repeat Steps 1-4 to configure mapping other fields **PacsWorksAccess** and
 2864 **PacsHomeAccess** as listed in the screenshot shown in Figure 139.

<input type="checkbox"/> ALERTDBCONNECTOR	PacsAllDoors
<input type="checkbox"/> ALERTDBCONNECTOR	PacsWorkAccess
<input type="checkbox"/> ALERTDBCONNECTOR	PacsHomeAccess

2865 **New** **Modify** **Delete**

2866 *Figure 143. Guardian Recon Authoritative Fields*

2867 **Identity & Access > Request Categories**

2868 1. Setup > Manual Configuration > Identity & Access > Request Categories
 2869 2. Select ChangeAccess Category name and Click Modify
 2870 3. On the Modify screen make following changes

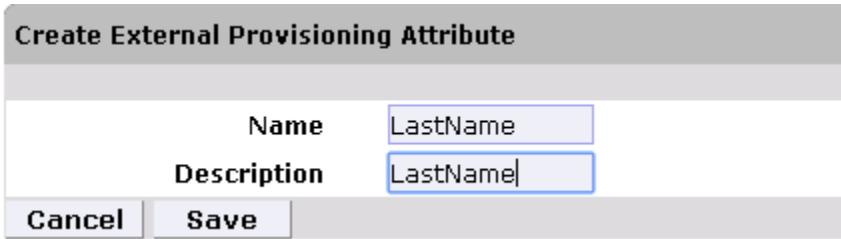
- a. In the Provisioning Actions section Un select Delimit user and Change Validity Dates check boxes if they are selected
- b. Go to Add Existing section and select System and Remove Role option for Resources/Roles Drop down field

 2871 4. Click Save Button to save the configuration

2876 **Identity & Access>Provisioning>External Provisioning Attributes**

2877 1. Setup > Manual Configuration > Identity & Access > Provisioning > External Provisioning
 2878 Attributes

2879 2. Select ACCESSIT PACS system from the list and Click **Configure**
 2880 3. On the Next screen, Click on **New** Button and provide “LastName” in both Name and
 2881 description fields
 2882 4. Click **Save** to save the configurations as shown in Figure 144.



The screenshot shows a dialog box titled "Create External Provisioning Attribute". It contains two input fields: "Name" and "Description", both of which have the value "LastName" entered. Below the fields are two buttons: "Cancel" and "Save".

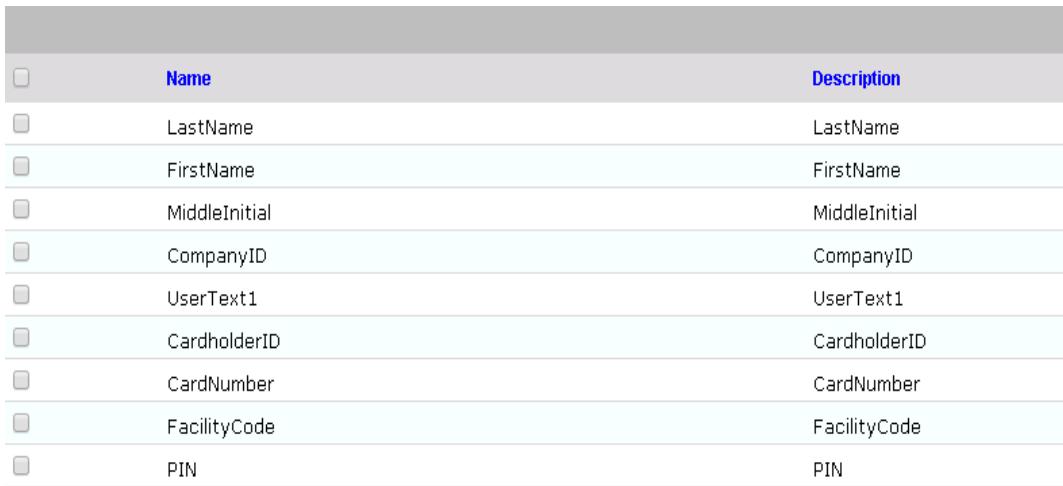
2883

Figure 144. External Provisioning Attribute

2885

2886 Repeat the Steps 1-4 to configure the following fields listed in the following screenshot,
 2887 Figure 145. **Note: The Fields Names are case sensitive.**

2888 5.



<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	LastName	LastName
<input type="checkbox"/>	FirstName	FirstName
<input type="checkbox"/>	MiddleInitial	MiddleInitial
<input type="checkbox"/>	CompanyID	CompanyID
<input type="checkbox"/>	UserText1	UserText1
<input type="checkbox"/>	CardholderID	CardholderID
<input type="checkbox"/>	CardNumber	CardNumber
<input type="checkbox"/>	FacilityCode	FacilityCode
<input type="checkbox"/>	PIN	PIN

2889

2890

Figure 145. Attribute Fields

2891

2892 Identity & Access>Provisioning>Provisioning Mapping

1. Setup > Manual Configuration > Identity & Access > Provisioning > Provisioning Mapping.
2. Select ACCESSIT PACS and click on **Configure**.
3. On the Next Screen, Figure 146, Click **New** Button and select UserText1 from

DB Connector Attribute Name: UserText1

AlertEnterprise Attribute Name: UserId

Derived Attribute Name:

Mandatory: No

Editable: Yes

Visible: Yes

Default Value:

Show Auto Generate:

Validation Flag:

Is User-Id attribute:

Cancel **Save**

2896

2897

2898

2899

Figure 146. Provisioning Mapping

4. Click on Save button to save the mapping
5. Repeat the steps 1-4 to configure other fields as shown in Figure 140.

<input type="checkbox"/> DB Connector Attribute	Mandatory	AlertEnterprise Attribute	Default Value	Editable	Visible	Validation Flag	Is User-Id attribute
<input type="checkbox"/> UserText1	No	UserId		No	No	No	No
<input type="checkbox"/> FirstName	Yes	FirstName		Yes	Yes	No	No
<input type="checkbox"/> LastName	Yes	LastName		Yes	Yes	No	No
<input type="checkbox"/> CompanyID	No	Priority		No	No	No	No
<input type="checkbox"/> CardholderID	Yes	UserId		Yes	Yes	No	No
<input type="checkbox"/> CardNumber	Yes	BadgeId		Yes	Yes	No	No
<input type="checkbox"/> FacilityCode	No	FacilityCode	20	Yes	Yes	No	No
<input type="checkbox"/> PIN	No	PIN		Yes	Yes	No	No

2900

Cancel New Modify Delete

<< < 1 > >>

2901

Figure 147. Guardian DB Connector Attribute Mapping

2902 **Policy Engine> Rules**

1. Setup > Manual Configuration > Policy Engine > Rules
2. Click New Button
3. On the Next screen provide following information. See Figure 148.

Define Rules

* Rule Name: All Door Access New

Entity Type: Workflow

Rule Type: AlertAccess

* Description: All Door Access New

* Applicable To:

- Initiator
- Decision
- Suggest/Default
- Role Model
- Policy
- Master User Search
- Groups
- Role Certification
- unMitigatedRiskAllowed

* Attributes:

And/Or: and or

PacsAllDoors Request Category

2906 **Next** **Cancel**

Figure 148. Policy Rules

2907

2908 4. Click **Next** Button

2909 5. On the next screen, Figure 149, click **New** to define a new Rule Condition for NewHire

2910 request category

Define Condition

If PacsAllDoors equals True and

Request Category equals NewHire

2911 **Add** **Cancel**

Figure 149. Rule Conditions

2912

2913

2914 6. Repeat the step 5 to define rule condition for other request categories Remove User

2915 Access and ChangeAccess as shown in Figure 150.

<input type="checkbox"/>	If	PacsAllDoors	and	Request Category
<input type="checkbox"/>	= True			= NewHire
<input type="checkbox"/>	= True			= Remove User Access
<input type="checkbox"/>	= True			= ChangeAccess
<input type="checkbox"/>	= true			= ChangeAccess

2916

2917

Figure 150. Rule Conditions

2918

2919 7. Repeat Step 1-6 to configure Other Rules **Home Access Level New** and **WO Access Level New** as shown in following *Table 21*.

2921

Table 28. Guardian Manual Configuration Policy Engine Rules

Rule Name	Entity Type	Rule Type	Description	Applicable to	Attributes	Drop down value	Selection Value
All Door Access New	Workflow	AlertAccess	All Door Access New	Suggest/Default	PacsAllDoors AND Request Category	Equals	1. True and New Hire 2. True and Remove User Access 3. True and ChangeAccess
Home Access Level New	Workflow	AlertAccess	Home Access Level New	Suggest/Default	PacsAllDoors AND Request Category	Equals	1. True and New Hire 2. True and Remove User Access 3. True and ChangeAccess
WO Access Level New	Workflow	AlertAccess	WO Access Level New	Suggest/Default	PacsAllDoors AND Request Category	Equals	1. True and New Hire 2. True and Remove User Access 3. True and ChangeAccess

2922

2923 Policy Engine> Suggest/Default Access

2924

1. Setup > Manual Configuration > Policy Engine > Suggest/Default Access.

2925

2. Click New and enter the following information to create **All Door Access** criteria, shown in Figure 151 .

2926

The screenshot shows a configuration interface for 'Default Access'. The 'Name' field is set to 'All Door Access'. The 'Type' field is set to 'Default'. Under 'Search By', the 'Search by Systems' checkbox is checked, while 'Search By Role Attributes', 'Search by Training Roles', and 'Search by Training Attributes' are unchecked. The 'Selected System' dropdown is set to 'ACCESSIT PACS' and the 'Selected Role' dropdown is set to 'ALL DOORS'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

2927

2928

Figure 151. Default Access

2929 3. Click **Next** Button

2930 4. On the Next screen, Enter **ACCESSIT PACS** in System Name Field and hit **Search** button

2931 5. The System will appear in Search Results pane. Click **Add** link under Action column to
2932 add the system to Selected Systems section

2933 6. Click **Next** Button

2934 7. On the next screen, enter **ALL DOORS** in Role Name Field and hit **Search** button

2935 8. The Role will appear in Search Results pane. Click **Add** link under Action column to add
2936 the role to Selected Roles section

2937 9. Click Save button to save the configuration

2938 10. Repeat the steps 1-9 to configure other criteria for **Home Access Level**,
2939 **WO Access Level**, **NewHireDefaultSystems** as listed in Table 29. Manual Configuration
2940 Policy Engine Suggest/Default Access

2941

2942

Table 29. Manual Configuration Policy Engine Suggest/Default Access

Name	Type	Condition	Search By System	Selected System	Selected Role
All Door Access	Default	All Door Access NEW	Yes (Select check box)	ACCESSIT PACS	ALL DOORS

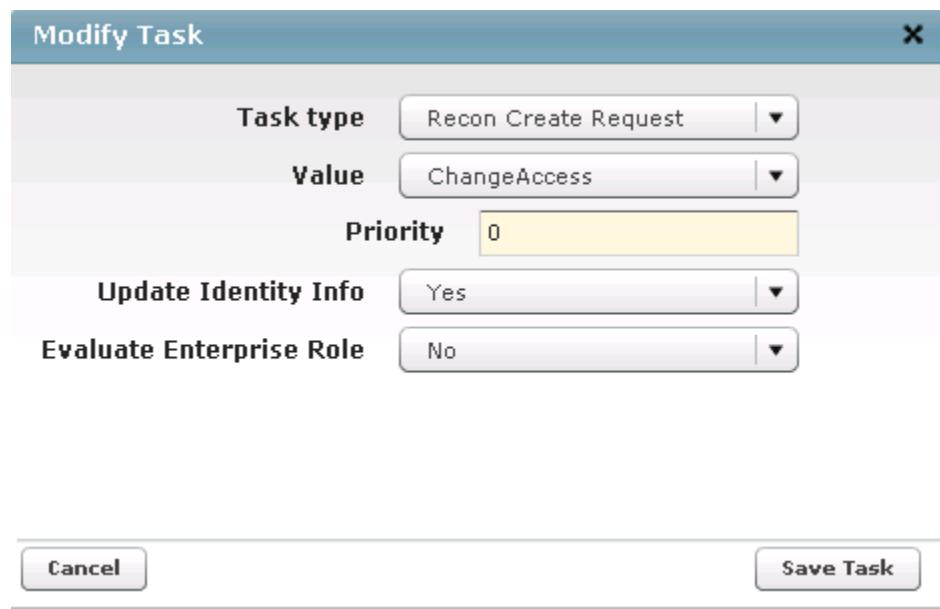
Home Access Level	Default	Work Access Level New	Yes (Select check box)	ACCESSIT PACS	Home Access Level
WO Access Level	Default	Home Access Level New	Yes (Select check box)	ACCESSIT PACS	WO Access Level
NewHireDefaultSy stems	Default	NewHireDefaultSy stems	Yes (Select check box)	ACCESSIT PACS	

2943

2944 11. Select all existing Suggest Default Access criterias other than the one listed in Table 22
2945 and Click **Delete** button to delete them.

2946 **Policy Engine>Rule Action Handler**

2947 1. Setup > Manual Configuration > Policy Engine > Rule Action Handler.
2948 2. In Action Handlers List page select ReconChangeHandler and Click **Modify**
2949 3. On the next screen Select **Recon Create Request** Task Type and Click **Update Task**
2950 4. On the popup window Click on **Value** drop down field and select **ChangeAccess** from the
2951 list as shown in Figure 152.



2952

2953 *Figure 152. Modify Task*

2954 5. Click on **Save Task** and then Click **Save** Button

2955

2956 **Policy Engine>Policy Designer**

2957 1. Setup > Manual Configuration > Policy Engine > Policy Designer

2958 2. Select New to create new Policy designer as shown in Figure 153.

2959 Name – User Policy New

2960 Rule Type – AlertAccess

2961 Description – User Policy

2962

The screenshot shows a configuration dialog box with the following fields:

- * Name: User Policy New
- * Rule Type: AlertAccess
- Description: User Policy New

2963

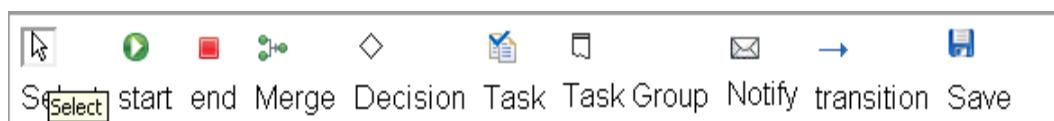
Back **Next** **Cancel**

2964

Figure 153. Policy Designer

2965 3. Click **Next**2966 4. Drag the elements from the tool bar section, available on top of the page and place
2967 them onto the layout page and connect each node as shown in
2968 Figure 154.

2969



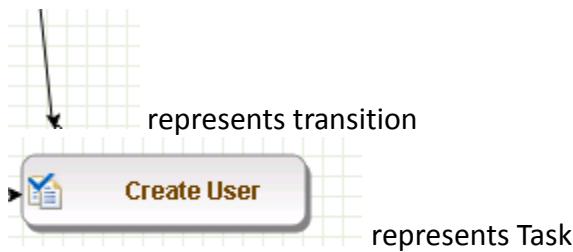
2970

Figure 154. Toolbar

2972

2973

2974  represents Start button2975  represents End Button2976  represents Decision



2977 represents transition

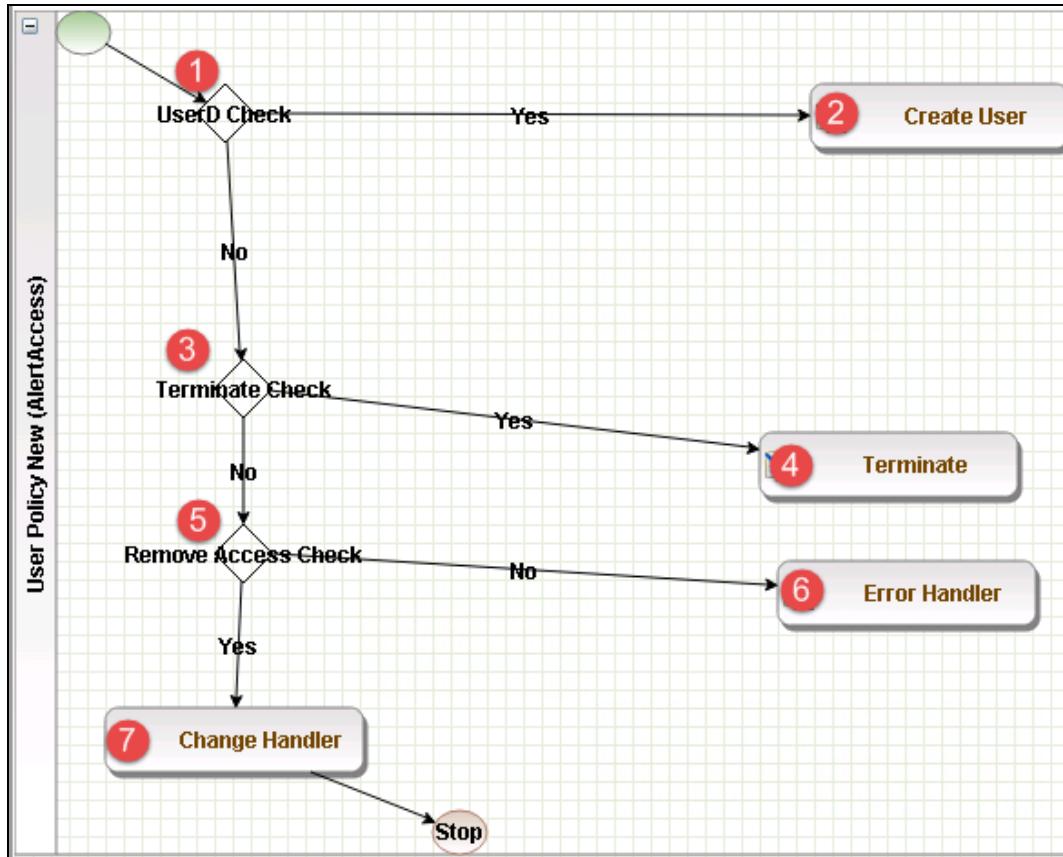
2978 represents Task

2979

2980 5. Guide lines to configure the policy

- 2981 a. To place an element/node on the layout page, drag it from the toolbar and place
2982 it.
- 2983 b. To connect two nodes, select transition icon from tool bar and then mouse over
2984 to the first node and connect to the other node in the same direction specified in
2985 the Figure 23)
- 2986 c. To provide text for a Decision or Task or Line, double click on the corresponding
2987 node and enter the text. Hit Enter after that to come out of the edit mode.

2988



2989

2990

Figure 155. Guardian User Policy

2991 6. Click on Step 1 decision box and it will open popup window with some fields. See Figure
 2992 156
 2993 7. Enter `$masterUser[UserId].size='0'` in the Condition text box and hit Enter

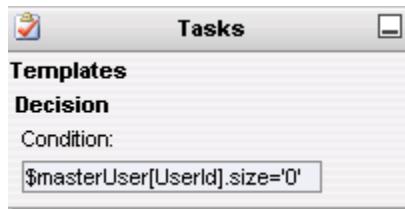
2994

2995

Figure 156. Tasks Popup

2996 8. Similarly, click on other Steps (2 to 7) and configure the data based on Table 30.
 2997 9. For decision nodes provide Condition value and for Task nodes like Create User,
 2998 Terminate User, Change Handler, Error Handler provide IsTaskHandler and Task Handler
 2999 fields

3000



3001

Table 30. Condition Decision Values

Step	Name	Type	Condition	Is Task handler	Task Handler	Update Query
1	User ID Check	Decision	\$masterUser[UserId].size='0'			
2	Create User	Task Handler		Yes	Recon New Hire	
3	Termination Check	Decision	\$checkStatus[UserStatus,Active,InActive].action='LOCK'			
4	Termination	Task Handler		Yes	Recon Terminate Handler	
5	Remove Access Check	Decision	\$checkAuthFields[].status='Yes'			
6	Error Handler	Task Handler		Yes	Recon Error Handler	
7	Change Handler	Task Handler		Yes	Recon Change Handler	

3002

3003 Job Scheduler>Triggers Field Map

- 3004 1. Setup > Manual Configuration > Job Scheduler > Triggers Field Map.
- 3005 2. Click New
- 3006 3. Enter Group Name – Alert DbConnector Field Mapping
- 3007 4. Description – Alert DbConnector Field Mapping
- 3008 5. Select Type – Reconciliation
- 3009 6. After creating Field Map, select the newly created map and select Configure
- 3010 7. Click New and create mapping per below, Table 31

3011

Table 31. Guardian Job Scheduler Triggers Field Map

AE Attribute	mappedKey	userType	roleType	userRole	userBadge	userEntRoleType	userTrainingType
UserId	UserId	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
FirstName	FirstName	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
LastName	LastName	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Email	Email	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Telephone	WorkPhone	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Mobile	HomePhone	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
EmployeeType	EmployeeType	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
PacsAllDoors	PacsAllDoor	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
PacsHomeAccess	PacsHomeAccess	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
PacsWorkAccess	PacsWorkAccess	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
BadgeId	CardNumber	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Format	FacilityCode	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
ValidFrom	ValidFrom	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
ValidTo	ValidTo	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Title	Title	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Status	UserStatus	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
PIN	PIN	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
AlertDepartment	Department	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE

3012

3013

3014 **Job Scheduler>Triggers**

3015 1. Setup > Manual Configuration > Job Scheduler > Triggers

3016 2. Click New and create the following Triggers in Table 32.

3017

3018 AlertDbConnectorTrigger

3019

3020

Table 32. Guardian AlertEnterprise DB Trigger

Name	AlertDbConnectorTrigger
Description	AlertDbConnectorTrigger
Type	Reconciliation
Batch size	100
Number of Attempts	3
Policy Designer for Users/ Roles	User policy New
System: Reconciliation From	ALERTDBCONNECTOR
Reconciliation System	ALERTDBCONNECTOR
Field Mapping Group	ALERTDBCONNECTOR Field Mapping
User Type	True
User Role	True

3021

3022 **Job Scheduler>Scheduler**

3023 1. Setup > Manual Configuration > Job Scheduler > Scheduler.

3024 2. Click New and enter the following, shown in Figure 142.

3025 3. Click Save.

3026 • Job Type – Reconciliation Job

3027 • Job Name - <Job Name>

3028 • Select Global check box

3029 • Reconciliation for – User

3030 • Reconciliation Type – Incremental Reconciliation

3031 • Reconciliation Triggers – AlertDbConnectorTrigger

3032 • Select the schedule as Immediate, Once, periodic or Advance.

3033 • For a periodic job, specify the job start date, end date, and duration of job frequency.

3034

3035

3036 *Figure 157. Guardian Reconciliation Job*

3037 3. Click Save.

3038 **10 PACS SERVER: RS2 ACCESS IT UNIVERSAL SERVER INSTALLATION**

3039 The Access It Universal RS2 Technologies PACS Server is installed on the PACS Network to help
 3040 control physical access to simulated facilities, rooms, etc. RS2 Technologies cards and card
 3041 readers were also included in both builds. The RS2 Technologies PACS Server is installed on a
 3042 VM that is running the Windows Server 2012 R2 OS.

3043 **10.1 SECURITY CHARACTERISTICS**

3044 Cybersecurity Framework Categories: PR.AC-2: Physical access to assets is managed and
 3045 protected

3046 NIST 800-53 rev 4 Security Controls: PE-2, PE-3, PE-4, PE-5, PE-6, PE-9

3047 **10.2 SYSTEM ENVIRONMENT**

3048 The system for the PACS-Console Server configured by the NCCoE contains the following
3049 configuration settings and environmental constraints:

3050 • Windows Server 2012 R2
3051 • VM with CPU Quad Core 2.199GHz
3052 • VM with 8192MB of memory
3053 • Virtual Hard Disk containing 240 GB of storage.

3054 **10.3 AIUNIVERSAL INSTALLATION**

- 3055 1. Insert the AIUNIVERSAL CD into the CD-ROM drive.
- 3056 2. Launch Setup64.exe as Administrator.
- 3057 3. Follow install instructions:
 - 3058 • Select I do not have a SQL Server installed.
 - 3059 • When prompted to install SQL Server 2008 R2 Express Edition select Yes.
 - 3060 • After installation of SQL Server. Select Install Access It! Universal.
 - 3061 • When prompted to install a Stand-Alone Server version of Access It! select OK.
 - 3062 • When prompted by the install wizard select Next >.
 - 3063 • Read the license agreement and select Next > if you agree with the terms of the
3064 agreement.
 - 3065 • Use default installation folder C:\Program Files(x86)\RS2 Technologies\Access It!
3066 Universal\ then select Next >.
 - 3067 • When the installer is ready select Next > to continue.
 - 3068 • Select Close to exit the installer after completion.

3069 **10.4 POST INSTALLATION**

- 3070 1. Launch Access It! by selecting it from the Start menu.
- 3071 2. When prompted to select server, enter the host name of server: PACS-CONSOLE.
- 3072 3. Log in with the default user name and password.

3073 10.4.1 **Connect Access It! Universal to Door Controller**

- 3074 1. Under the Main > Hardware tab, select Channels.
- 3075 2. Create a new Channel.
- 3076 3. For Channel Type select IP Server.
- 3077 4. Ensure Protocol Type is SCP.

3078 5. Select Save.

3079 6. Create a new SCP.

3080 7. Under the General tab ensure that Model is set to EP-1501Plus.

3081 8. Under the Comm tab ensure that Channel is set to Channel 000 (the channel just
3082 created).

3083 9. TCP/IP Settings:

3084 • IP Address: 172.16.7.101

3085 • Port Number: 3001

3086 10. Encryption Settings: None.

3087 11. Under the Card Formats tab:

3088 • Format Name: 26 Bit Wiegand Facility code: 20

3089 • Format Name: 26 Bit Wiegand Facility code: 219

3090 12. Save changes to SCP 000.

3091 13. Under SIOs

3092 14. Edit SCP 000 – SIO 00

3093 15. Under General tab ensure Model is set to EP-1501.

3094 16. Edit SCP 000 – SIO 01

3095 17. Under General tab ensure Model is set to MR-52.

3096 18. Under Main > Hardware select Installed Readers

3097 19. Create SCP 000 – SIO 00-Reader 1

3098 20. Create SCP 000 – SIO 01-Card Reader

3099 21. Create SCP 000 –SIO 01-MRDT Keypad

3100 22. Under Configuration > Access Levels create New Access Level.

3101 23. Create new access levels.

3102 • Access Level Name: All Doors.

3103 • Assigned Readers for All Doors: SCP 000 – SIO 01-Card Reader and SCP 000 – SIO
3104 01-MRDT Keypad.

3105 • Access Level Name: Home Access Level.

3106 • Assigned Reader for Home Access Level: SCP 000 – SIO 01-MRDT Keypad.

3107 • Access Level Name: Work Order Access Level.

3108 • Assigned Reader for Work Order Access Level: SCP 000 – SIO-Card Reader

3109 10.4.2 **Enable TCP/IP to SQL 2008 R2 Server**
3110 1. Launch Microsoft SQL Server Configuration Manager.
3111 2. Expand SQL Server Network Configuration (32-bit).
3112 3. Select Protocols for AIUNIVERSAL.
3113 4. Right-click on TCP/IP and then select Properties.
3114 5. Select tab IP Addresses.
3115 6. Under IP1 ensure IP Address is set to 0.0.0.0 and TCP Port is set to 1433.
3116 7. Under IPALL ensure TCP Dynamic Ports is set to 52839 and TCP Port is set to 1433.
3117 8. Restart the SQL server by selecting SQL Server Services then right click on SQL Server
3118 (AIUNIVERSAL) and select Restart.

3119 **11 PRIVILEGED USER ACCESS CONTROL: TDI CONSOLEWORKS SERVER INSTALLATION**

3120 The TDi ConsoleWorks server was installed in two different locations in the builds. It was
3121 installed on the OT network to control and monitor access between OT technicians and physical
3122 devices such as the RTUs and the RADiFlow ICS firewall. The following two sections provide
3123 details on the steps needed to install and configure each of these servers.

3124 **11.1 SECURITY CHARACTERISTICS**

3125 Cybersecurity Framework Categories:

- 3126 • PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in
3127 accordance with policy
- 3128 • PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least
3129 functionality

3130 NIST 800-53 rev 4 Security Controls: AU Family, AC-3, CM-7

3131 **11.2 CONSOLEWORKS SERVER INSTALLATION**

3132 ConsoleWorks was installed on the OT network to control and monitor access between OT
3133 technicians and physical devices such as the RTUs and the RADiFlow ICS firewall. ConsoleWorks
3134 uses the OT directory to authenticate users requesting access to these devices. It also
3135 establishes a permanent SSH or telnet connection to each of the RTUs and ICS firewall using
3136 pre-established usernames and passwords. As users request access and are authenticated
3137 ConsoleWorks makes the cross-connection from the user to the specific SSH or telnet session to
3138 allow access. Once the cross-connection is established the user has access to the device to
3139 make any changes needed. When the user completes their task they log-off of the connection
3140 and ConsoleWorks removes the cross-connect between the user and the SSh or telnet session.

3141 ConsoleWorks logs all user access requests, all of the traffic on the session, and can alert on any
3142 pre-defined aspect of the traffic. Directory based authentication is used to manage the user
3143 access in near real time.

3144 On the OT network, the ConsoleWorks Server is installed on a VM that is running the Windows
3145 Server 2012 R2 (hardened server OS) image, as explained in Section 1.

3146 11.2.1 **System Environment**

3147 The system for the OT Network ConsoleWorks Server configured by the NCCoE contains the
3148 following configuration settings and environmental constraints:

3149 • Windows Server 2012 R2 OS
3150 • VM with CPU Quad Core 2.199GHz
3151 • VM with 8192MB of memory
3152 • Virtual Hard Disk containing 240 GB of storage.

3153 11.2.2 **ConsoleWorks Server Installation on the OT Network**

- 3154 1. After installing the OS, download the TDi Technologies Installer from
3155 http://support.tditechnologies.com/get_consoleworks.
- 3156 2. Launch the *cw_server_v4.9-0u0.exe* application. The installer requires administrative
3157 privileges to execute.
- 3158 3. When prompted by Windows User Account Control, select Yes to continue.
- 3159 4. The ConsoleWorks Server InstallShield Wizard should display a welcome message. Select
3160 Next > to continue.
- 3161 5. When prompted by the InstallShield Wizard to accept the license agreement, read
3162 carefully. If you agree with the license terms, select Next > to continue with the
3163 installation.
- 3164 6. Enter the User Name and Organization fields, then select Next > to continue.
- 3165 7. Select Complete when prompted for setup type, then select Next > to continue.
- 3166 8. Click Install to begin installation of ConsoleWorks Server.
- 3167 9. After the InstallShield Wizard has completed, ensure that Launch upgrade script (if
3168 upgrading from 32 bit) is unchecked.
- 3169 10. Select Finish.

3170 11.2.3 **Post-installation Configuration of ConsoleWorks on the OT Network**

- 3171 1. Copy TDi Technologies license key files into
3172 *C:\ProgramData\ConsoleWorks\Server\LMF\TDI_Licenses*
- 3173 2. Go to *Start > Run > services.msc*.
- 3174 3. Right-click on the ConsoleWorks Server Service, then select Properties.

3175 4. Select Start to start the service. Then change the Startup Type from Manual to
3176 Automatic.

3177 5. Select Apply to save changes. Both the ConsoleWorks Server and ConsoleWorks LMF
3178 Server services should be running.

3179 6. Test browser connectivity by going to <http://localhost:5176>. The default account is
3180 CONSOLE_MANAGER. The default password is: Setup

3181 11.2.4 [Configuring External Authentication for the OT Network ConsoleWorks Server](#)

3182 1. From the left menu, select the SECURITY tab.

3183 2. Select External Authentication.

3184 3. Ensure the Enable External Authentication checkbox has been selected.

3185 4. Select Add.

3186 • Parameter 1: OT-ES-IDAM-B1

3187 • Parameter 2: CW_

3188 • Required Profile: CONSOLE_WORKS

3189 • Template User: CONSOLE_MANAGER

3190 • Leave all other fields blank.

3191 5. Then select Next.

3192 6. Enter a Username and Password to test External Authentication settings.

3193 7. Then select Next.

3194 8. Then select Save.

3195 **12 ICS/SCADA FIREWALL: RADIFLOW**

3196 A RADiFlow switch is installed on the physical network that represents the industrial control
3197 system component that can be accessed and controlled via the OT network. A RADiFlow
3198 management workstation is installed on the OT network. The RADiFlow Management
3199 Workstation is installed on a VM that is running the Windows 7 Enterprise OS.

3200 **12.1 SECURITY CHARACTERISTICS**

3201 Cybersecurity Framework Categories: PR.PT-3: Access to systems and assets is controlled,
3202 incorporating the principle of least functionality

3203 NIST 800-53 rev 4 Security Controls: AC-3, CM-7

3204 12.2 OT Network RADiFlow Management Workstation **INSTALLATION**3205 12.2.1 **Installing iSIM**

- 3206 1. Launch the iSIM installer as an administrator
- 3207 2. Set the Destination Directory to C:\Program Files (x86).
- 3208 3. Leave default settings for all other options

3209 12.2.2 **iEMS**

- 3210 1. Launch iEMS from the Start menu.
- 3211 2. From the menu items, select *System > Switch Initialization > Force Switch Model > 3180.*
- 3212 3. In the main windows dialog box, enter the switches IP address 172.16.6.4 and then
- 3213 select Refresh.
- 3214 4. From the menu items, select *Configuration > Interfaces > Serial Ports...*
- 3215 5. Select the Terminal Server tab and ensure Service 1 and Service 2 dialog boxes are
- 3216 checked.
- 3217 6. Under Service 1, enter these settings:
 - 3218 • Service ID: 1
 - 3219 • Local IP Address: 172.16.6.100
 - 3220 • Telnet Port: 2050
 - 3221 • Null CR Bit Mode: OFF
- 3222 7. Under Service 2, enter these settings:
 - 3223 • Service ID: 2
 - 3224 • Local IP Address: 172.16.6.100
 - 3225 • Telnet Port: 2051
 - 3226 • Null CR Bit Mode: OFF
- 3227 8. Then Select Create/Update.
- 3228 9. Select the Serial Ports tab ensure Port-1 and Port-2 dialog boxes are checked.
- 3229 10. Under Port 1 enter these settings:
 - 3230 • Application: Terminal Server
 - 3231 • Local Position: Slave
 - 3232 • Service-id: 1
 - 3233 • Operation Mode: Transparent
 - 3234 • Buffer Mode: byte
 - 3235 • Protocol: any
 - 3236 • Baudrate: 9600

3237 • Databits: 8
3238 • Stopbits: 1
3239 • Parity: no
3240 • Allowed-latency: 6
3241 • Bus-idle-time: 30
3242 • Dtr-dsr: enable
3243 • Rts-cts: enable
3244 • Local-dsr-delay: 0
3245 • Local-cts-delay: 0
3246 • Tx-delay: 10
3247 • Bits-for-sync1: 28
3248 • Bits-for-sync2: 1
3249 • Unit-id length: 2
3250 • Iec101-link-address-len: 2

3251 11. Under Port 2 enter these settings:

3252 • Application: Terminal Server
3253 • Local Position: Slave
3254 • Service-id: 2
3255 • Operation Mode: Transparent
3256 • Buffer Mode: byte
3257 • Protocol: any
3258 • Baudrate: 9600
3259 • Databits: 8
3260 • Stopbits: 2
3261 • Parity: no
3262 • Allowed-latency: 6
3263 • Bus-idle-time: 30
3264 • Dtr-dsr: enable
3265 • Rts-cts: enable
3266 • Local-dsr-delay: 0
3267 • Local-cts-delay: 0
3268 • Tx-delay: 10
3269 • Bits-for-sync1: 28
3270 • Bits-for-sync2: 1
3271 • Unit-id length: 2
3272 • Iec101-link-address-len: 2

3273 12. Then Select Create/Update.

3274 **13 OZONE: MAG INSTALLATION**

3275 Four Ozone components are installed on the IdAM network: Console, Authority, Server, and
3276 Envoy. These components are installed on VMs running the CentOS 7 image.

3277 **13.1 SECURITY CHARACTERISTICS**

3278 Cybersecurity Framework Categories: PR.AC-4: Access permissions are managed, incorporating
3279 the principles of least privilege and separation of duties

3280 NIST 800-53 rev 4 Security Controls: AC-2, AC-3, AC-5, AC-6, AC-16

3281 **13.2 OZONE CONSOLE INSTALLATION AND AUTHORITY CONFIGURATION**

3282 1. Install CA Certificate into trusted root store (MAG_DEV_CA.crt).

3283 2. Install Ozone Authority Certificate into Trusted People store (ozoneauthority.crt).

3284 3. Install Administrator keys into Personal store (admin1.crt and admin2.crt).

3285 4. Run Setup Ozone Console.exe

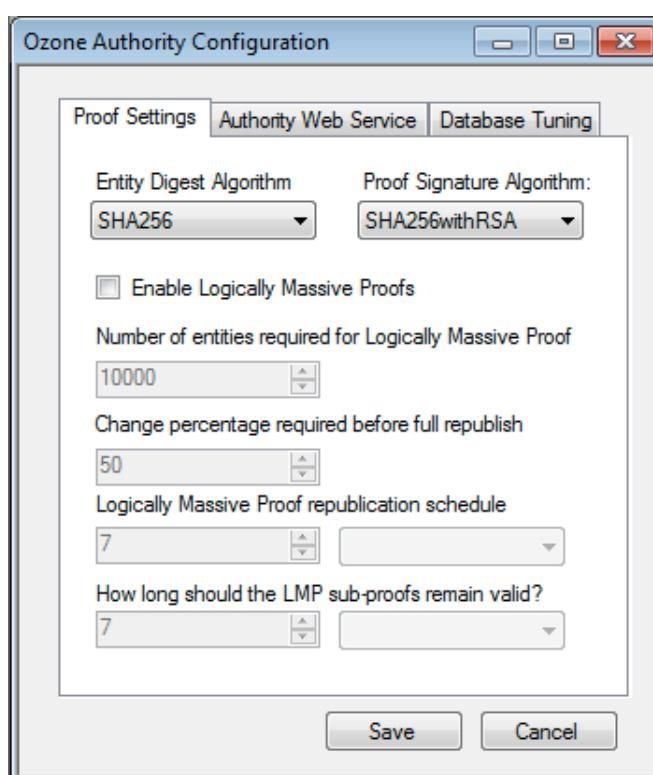
3286 • Run Ozone Console.

3287 • Go to *Configuration>Ozone Authority>New...*...see Figure 158.

3288 • In the Proof Settings tab:

3289 ○ Select SHA256 for the Entity Digest Algorithm.

3290 ○ Select SHA256withRSA for the Proof Signature Algorithm.



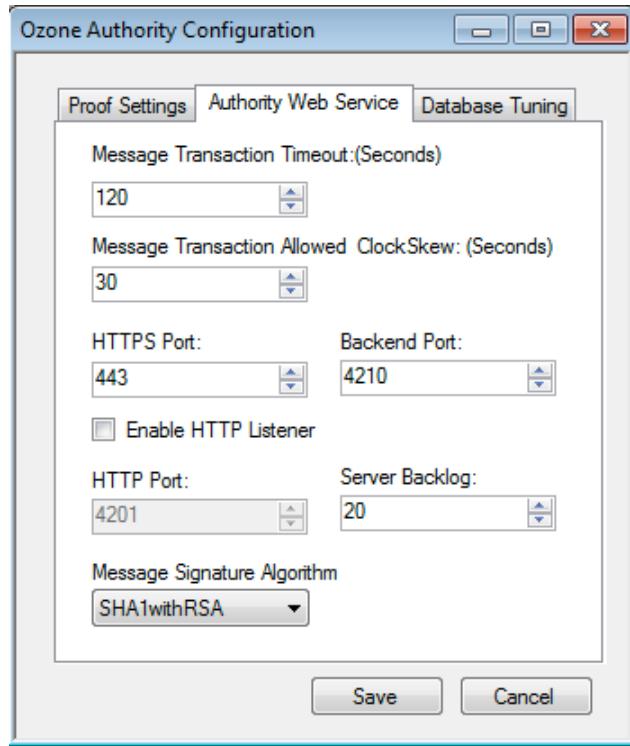
3291

Figure 158. Ozone Proof Settings

3293 5. In the Authority Web Service tab, Figure 159.

3294 • Set the HTTPS Port to 443.

3295 • Select SHA1withRSA for the Message Signature Algorithm.



3296

Figure 159. Ozone Authority Web Service

3298 • Click Save.

3299 6. Select a certificate to be used to digitally sign the configuration (Admin 1).

3300 7. Save the file as AuthorityConfiguration.xml.

3301 8. SCP the file to Ozone Authority machine.

3302 **13.3 OZONE AUTHORITY INSTALLATION**

3303 **Create keys and certificates and store in Java Keystore (JKS)**

3304

3305 **Install java**

3306 [root@ozone ~]# yum install java

3307

3308 **Install mariADB**

3309 [root@ozone ~]# yum install mariadb-server
 3310 [root@ozone ~]# reboot
 3311 [root@ozone ~]# systemctl start mariadb
 3312 [root@ozone ~]# systemctl enable mariadb

3313

3314 **Secure the mysql installation**

3315 [root@ozone ~]# mysql_secure_installation

```
3316
3317 Create the Ozone Authority database and user
3318 [root@ozone ~]# mysql -u root -p
3319
3320 MariaDB> create database ozone;
3321 Query OK, 1 row affected (0.02 sec)
3322
3323 MariaDB> create user 'ozone'@'localhost' identified by 'password';
3324 Query OK, 0 rows affected (0.00 sec)
3325
3326 MariaDB> grant all privileges on ozone.* to 'ozone'@'localhost';
3327 Query OK, 0 rows affected (0.00 sec)
3328
3329 MariaDB> flush privileges;
3330 Query OK, 0 rows affected (0.00 sec)

3331
3332 Install the Ozone Authority
3333 [root@ozone local]# cd /usr/local/
3334 [root@ozone local]# tar -xzf ~/Ozone\ Authority-2014.tar.gz
3335
3336 Copy AuthorityConfiguration.xml to conf directory
3337 [root@ozone local]# mv ~/AuthorityConfiguration.xml authority/conf/
3338
3339 Copy AuthorityLicense.xml to conf directory
3340 [root@ozone local]# mv ~/AuthorityLicense.xml authority/conf/
3341
3342 Copy JKS to keystores directory
3343 [root@ozone local]# mv ~/authority.jks authority/keystores/
3344
3345 Copy administrator certificates to bin directory
3346 [root@ozone local]# mv ~/admin1.cer authority/bin/
3347 [root@ozone local]# mv ~/admin2.cer authority/bin/
3348
3349 Run the Ozone Authority script
3350 [root@ozone local]# cd authority/bin/
3351 [root@ozone bin]# ./startAuthority.sh
3352 Configuration file not found, would you like to create a new
3353 installation? [Y] Y
3354
3355 ***WARNING***
3356 This product MUST be installed by an Ozone Certified
3357 Engineer. Pericore, Inc. cannot be held liable for damages resulting
3358 from negligent or fraudulent actions of unauthorized or unqualified
3359 administrators. Please review all documentation thoroughly before
3360 continuing. Continuation of this configuration process represents an
3361 agreement to abide by the Pericore EULA.
3362 Do you wish to continue? [N] : Y
3363
3364 Please select the license file for this Ozone Authority.:
3365 1: /usr/local/authority/conf/AuthorityLicense.xml
3366 2: Other...
3367 Choice [1] : 1
3368
```

```
3369 Please select the configuration file for this Ozone Authority.:
3370 1: /usr/local/authority/conf/AuthorityConfiguration.xml
3371 2: Other...
3372 Choice [1] : 1
3373
3374 Do you wish to set any passphrase complexity requirements? [N] : N
3375
3376 Note: If you require passphrase at start, you will not be able to
3377 restart this Ozone Authority without user intervention.
3378 Do you wish to require a passphrase to start this Ozone Authority? [N] N
3379
3380 Using keystore type: RSA
3381
3382 Do you have an existing keystore you wish to use for this Ozone Authority?
3383 [Y] : Y
3384
3385 Please select the keystore file for this Ozone Authority.:
3386 1: /usr/local/authority/keystores/authority.jks
3387 2: Other...
3388 Choice [1] : 1
3389 Please enter the passphrase. : 123456
3390 May 15, 2015 1:24:22 PM com.pericore.util.PericoreProvider jsafeJCEinit
3391 POST: [FIPS] FIPS-140 compliance self-test passed.
3392
3393 What type of database do you wish to use.:
3394 1: SQLSERVER
3395 2: ORACLE
3396 3: MYSQL
3397 Choice [1] : 3
3398 Please enter the hostname or IP address of the database server: [ozone] :
3399 localhost
3400 Please enter the port number for the database: [3306] 3306
3401 Please enter the username for the database: [] : ozone
3402 Please enter the database password: password
3403 Using only available database: ozone
3404
3405 How many initial administrators would you like to create? [2] : 2
3406 Page 1 | Current Directory:
3407 [00] ../
3408 [01] lib/
3409 [02] admin1.cer
3410 [03] admin2.cer
3411
3412
3413 Please select the file containing the administrators certificate: [ # ] : 2
3414 3Page 1 | Current Directory:
3415 [00] ../
3416 [01] lib/
3417 [02] admin1.cer
3418 [03] admin2.cer
3419
3420 Please select the file containing the administrators certificate: [ # ] : 1
3421 Please enter distinguished name(DN) of the starting Organizational
3422 Unit (OU) for this proof tree: [OU=Ozone] : ou=Ozone, dc=NCCOE, dc=test
3423 Is: ou=Ozone, dc=NCCOE, dc=test correct? [Y] : Y
3424 Please enter the minimum number of administrators required to approve
3425 changes to the initial proofs: [1] : 1
```

```
3426 Please enter a name for the initial publication schedule: [Primary Schedule]
3427 : Daily
3428 Please enter the publication interval: [12] : 12
3429 Please select the time unit::
3430 1: Minute
3431 2: Hour
3432 3: Day
3433 Choice [1] : 2
3434 Please enter the validity period after publication: [12] : 12
3435 Please select the validity period time unit::
3436 1: Minute
3437 2: Hour
3438 3: Day
3439 Choice [1] : 2
3440
3441 Please enter a name for the initial distribution point for proofs. [File
3442 Distribution Point] : LDAP Distribution Point
3443
3444 Please enter the initial distribution point for proofs. This may be changed
3445 later. [file:///usr/local/authority/proofs/] : ldap://ozoneauthority/
3446 Configuration File: /usr/local/authority/conf/AuthorityConfiguration.xml
3447 May 15, 2015 1:25:16 PM
3448 com.pericore.util.ObjectIdentifierFactory$OIDDataLoader debug
3449 INFO: ObjectIdentifierFactory Read 240.165 kb in 2.511 ms; Indexed 2,415 Arcs
3450 in 51.731 ms; 2,310(1,054:5) keys => 2.003 kb
3451 Created proof ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in
3452 the database.
3453 Created proof ou=Applications, ou=Master Authorization Group, ou=Ozone,
3454 dc=NCCOE, dc=test in the database.
3455 Created proof ou=Groups, ou=Master Authorization Group, ou=Ozone, dc=NCCOE,
3456 dc=test in the database.
3457 Created proof ou=Attribute Types, ou=Master Authorization Group, ou=Ozone,
3458 dc=NCCOE, dc=test in the database.
3459
3460 Allowing a user certificate to be associated with a directory GUID
3461 allows for a migration path from username and password to a PKI based
3462 authentication and authorization mechanism. However, this method
3463 lowers the initial security settings by relying on a directory for the
3464 association. Please be sure you understand the risks associated with
3465 this method before allowing this mechanism to be used.
3466 Would you like to allow users certificates to be associated with a directory
3467 GUID? [N] : N
3468 Do you wish to display a logon message? [N] : N
3469
3470 Ozone Authority
3471 Version: 2014 - 4.0.1 (Build: 475)
3472 Copyright Pericore, Inc. 2014
3473 -----
3474 Started at: May 15, 2015 1:24:13 PM EDT
3475 Licensed to: NCCOE
3476 -----
3477
3478 Built: ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in
3479 0:00:00.304.
3480 Built: ou=Applications, ou=Master Authorization Group, ou=Ozone, dc=NCCOE,
3481 dc=test in 0:00:00.243.
3482 Built: ou=Groups, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test
```

```
3483 in 0:00:00.215.
3484 Built: ou=Attribute Types, ou=Master Authorization Group, ou=Ozone, dc=NCCOE,
3485 dc=test in 0:00:00.214.
3486 Push Certificates loaded with: 0 certificates
3487
3488 Started HTTPS Listener on port: 443
3489 Ozone Authority>
3490
3491
3492 Install LDAP (389) directory server
3493 [root@ozone ~]# yum install 389-ds-base
3494 [root@ozone ~]# vi /etc/hosts
3495 Modify the first line of hosts file so that it is the same as below:
3496 127.0.0.1 ozoneauthority.nccoe.test localhost localdomain
3497 localhost4 localhost4.localdomain4
3498
3499 Configure the directory server
3500 [root@ozone ~]# setup-ds.pl
3501 =====
3502 =
3503 This program will set up the 389 Directory Server.
3504
3505 It is recommended that you have "root" privilege to set up the software.
3506 Tips for using this program:
3507 - Press "Enter" to choose the default and go to the next screen
3508 - Type "Control-B" or the word "back" then "Enter" to go back to the
3509 previous screen
3510 - Type "Control-C" to cancel the setup program
3511
3512 Would you like to continue with set up? [yes]: yes
3513 =====
3514 =
3515 Your system has been scanned for potential problems, missing patches,
3516 etc. The following output is a report of the items found that need to
3517 be addressed before running this software in a production
3518 environment.
3519
3520 389 Directory Server system tuning analysis version 23-FEBRUARY-2012.
3521
3522 NOTICE : System is x86_64-unknown-linux3.8.13-68.2.2.el7uek.x86_64 (1
3523 processor).
3524
3525 NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds
3526 (120 minutes). This may cause temporary server congestion from lost
3527 client connections.
3528
3529 WARNING: There are only 1024 file descriptors (soft limit) available, which
3530 limit the number of simultaneous connections.
3531
3532 WARNING : The warning messages above should be reviewed before proceeding.
3533
3534 Would you like to continue? [no]: yes
3535
3536 =====
```

```
3539 =
3540 Choose a setup type:
3541
3542 1. Express
3543 Allows you to quickly set up the servers using the most
3544 common options and pre-defined defaults. Useful for quick
3545 evaluation of the products.
3546
3547 2. Typical
3548 Allows you to specify common defaults and options.
3549
3550 3. Custom
3551 Allows you to specify more advanced options. This is
3552 recommended for experienced server administrators only.
3553
3554 To accept the default shown in brackets, press the Enter key.
3555
3556 Choose a setup type [2]: 2
3557 =====
3558 =
3559 Enter the fully qualified domain name of the computer
3560 on which you're setting up server software. Using the form
3561 <hostname>.<domainname>
3562 Example: eros.example.com.
3563
3564 To accept the default shown in brackets, press the Enter key.
3565
3566 Warning: This step may take a few minutes if your DNS servers
3567 cannot be reached or if DNS is not configured correctly. If
3568 you would rather not wait, hit Ctrl-C and run this program again
3569 with the following command line option to specify the hostname:
3570
3571
3572 General.FullMachineName=your.hostname.domain.name
3573
3574 Computer name [ozone.mountaireygroup.com]: ozoneauthority.nccoe.test
3575 =====
3576 =
3577 The server must run as a specific user in a specific group.
3578 It is strongly recommended that this user should have no privileges
3579 on the computer (i.e. a non-root user). The setup procedure
3580 will give this user/group some permissions in specific paths/files
3581 to perform server-specific operations.
3582
3583 If you have not yet created a user and group for the server,
3584 create this user and group using your native operating
3585 system utilities.
3586
3587
3588 System User [nobody]: nobody
3589 System Group [nobody]: nobody
3590 =====
3591 =
3592 The standard directory server network port number is 389. However, if
3593 you are not logged as the superuser, or port 389 is in use, the
3594 default value will be a random unused port number greater than 1024.
```

```
3596 If you want to use port 389, make sure that you are logged in as the
3597 superuser, that port 389 is not in use.
3598
3599 Directory server network port [389]: 389
3600 =====
3601 =
3602 Each instance of a directory server requires a unique identifier.
3603 This identifier is used to name the various
3604 instance specific files and directories in the file system,
3605 as well as for other uses as a server instance identifier.
3606
3607 Directory server identifier [ozoneauthority]: ozoneauthority
3608 =====
3609 =
3610 Each instance of a directory server requires a unique identifier.
3611 This identifier is used to name the various
3612 instance specific files and directories in the file system,
3613 as well as for other uses as a server instance identifier.
3614
3615 Directory server identifier [ozoneauthority]: ozoneauthority
3616 =====
3617 =
3618 The suffix is the root of your directory tree. The suffix must be a valid DN.
3619 It is recommended that you use the dc=domaincomponent suffix convention.
3620 For example, if your domain is example.com,
3621 you should use dc=example,dc=com for your suffix.
3622 Setup will create this initial suffix for you,
3623 but you may have more than one suffix.
3624 Use the directory server utilities to create additional suffixes.
3625
3626 Suffix [dc=nccoe, dc=test]: dc=nccoe, dc=test
3627 =====
3628 =
3629 Certain directory server operations require an administrative user.
3630 This user is referred to as the Directory Manager and typically has a
3631 bind Distinguished Name (DN) of cn=Directory Manager.
3632 You will also be prompted for the password for this user. The password must
3633 be at least 8 characters long, and contain no spaces.
3634 Press Control-B or type the word "back", then Enter to back up and start
3635 over.
3636
3637 Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
3638 Password: password
3639 Password (confirm): password
3640 Your new DS instance 'ozoneauthority' was successfully created.
3641 Exiting . . .
3642 Log file is '/tmp/setup_C4mdK.log'
3643
3644 Setup the directory structure
3645 Modify the file /usr/local/authority/bin/389SetupDirectory.ldif
3646 Set the correct DN structure and passwords for the ozone authority user and tree
3647 [root@ozone bin]# vi 389SetupDirectory.ldif
3648 [root@ozone bin]# cat 389SetupDirectory.ldif
3649
3650 #Create the User for Ozone Authority
3651 dn: uid=ozone, ou=Special Users, dc=nccoe, dc=test
3652 changetype: add
3653 objectClass: inetorgperson
3654 objectClass: organizationalPerson
3655 objectClass: person
3656 objectClass: top
```

```

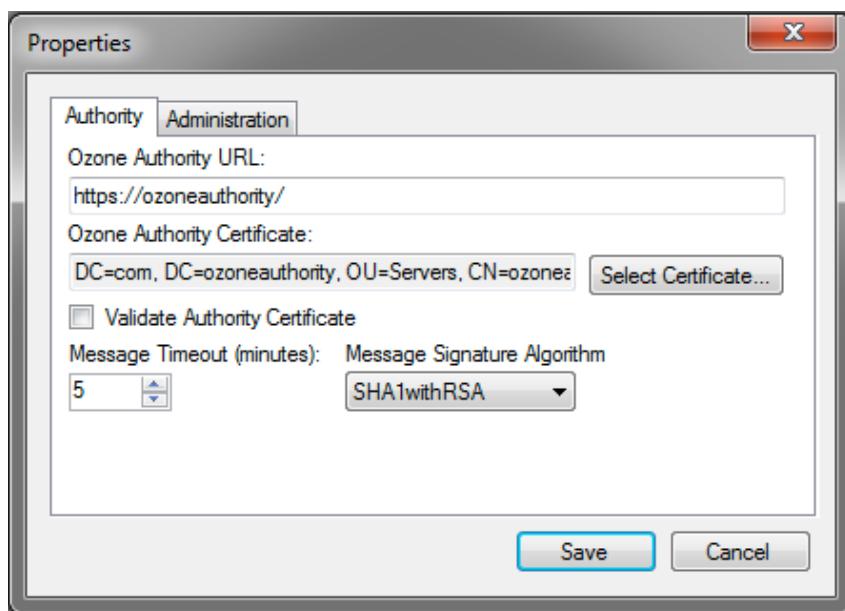
3652 cn: Ozone Authority
3653 sn: Authority
3654 givenName: Ozone
3655 uid: ozone
3656 userPassword: P@$$word
3657
3658 #make the people writable by ozone
3659 dn: ou=People, dc=nccoe, dc=test
3660 changetype: modify
3661 add: aci
3662 aci: (targetattr="*") (version 3.0;acl "ozone authority";allow (all)(userdn =
3663 "ldap:///uid=ozone, ou=Special Users, dc=nccoe, dc=test");)
3664
3665
3666 #Create the Ozone OU
3667 dn: ou=Ozone, dc=nccoe, dc=test
3668 changetype: add
3669 objectClass: organizationalUnit
3670 objectClass: top
3671 ou: Ozone
3672 aci: (targetattr="*") (version 3.0;acl "ozone authority";allow (all)(userdn =
3673 "ldap:///uid=ozone, ou=Special Users, dc=nccoe, dc=test");)
3674
3675 #Create required Attributes and Object Classes
3676 dn: cn=schema
3677 changeType: modify
3678 add: attributetypes
3679 attributetypes: ( 1.3.6.1.4.1.26135.1.1.1.2 NAME 'authorizationProof' DESC
3680 'Ozone Authorization Proof' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 SINGLE-VALUE
3681 X-ORIGIN 'user defined' )
3682 attributetypes: ( 2.23.136.1.1.2 NAME 'cscamasterlist' DESC 'CSCA Master
3683 List' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 SINGLE-VALUE X-ORIGIN 'user
3684 defined' )
3685
3686 dn: cn=schema
3687 changeType: modify
3688 add: objectclasses
3689 objectclasses: ( 1.3.6.1.4.1.26135.1.1.3 NAME 'ozoneAuthority' DESC '' SUP
3690 top STRUCTURAL MAY (authorizationProof $ cscamasterlist) X-ORIGIN 'user
3691 defined' )
3692
3693 Modify the directory using the LDIF
3694 [root@ozone bin]# ldapmodify -x -D "cn=Directory Manager" -W -f
3695 /usr/local/authority/bin/389SetupDirectory.ldif
3696 Enter LDAP Password:
3697 adding new entry "uid=ozone, ou=Special Users, dc=nccoe, dc=test"
3698
3699 modifying entry "ou=People, dc=nccoe, dc=test"
3700
3701 adding new entry "ou=Ozone, dc=nccoe, dc=test"
3702
3703 modifying entry "cn=schema"
3704
3705 modifying entry "cn=schema"
3706

```

3707 **13.4 OZONE CONSOLE SERVER CONFIGURATION**

3708 Before proceeding ensure that OzoneAuthority has been started by running `startauthority.sh` on
 3709 the OzoneAuthority machine.

- 3710 1. Open Ozone Console.
- 3711 2. Go to *File>Properties*, Figure 160, below.
- 3712 3. Enter the Ozone Authority URL.
- 3713 4. Click Select Certificate and select the Ozone Authority Certificate.
- 3714 5. Select SHA1withRSA as the Message Signature Algorithm.
- 3715 6. Click Save to the connection information.

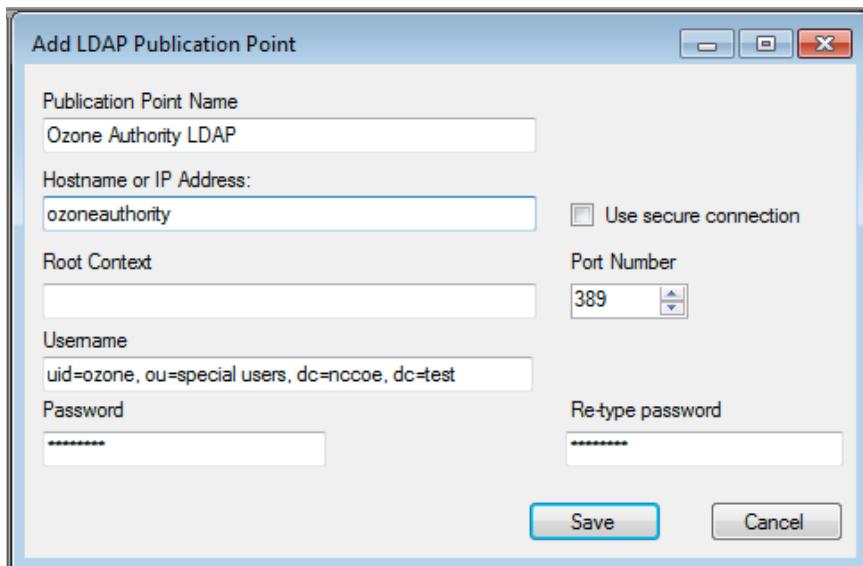


3716

3717 *Figure 160. Ozone Authority Connection Information*

3718 **Create the publication point for the proofs**

- 3719 1. Select Publication > Add Publication Point > Add LDAP Publication Point, Figure 161
- 3720 2. Enter a name for the publication point.
- 3721 3. Enter the hostname or IP address of the directory server.
- 3722 4. Enter a base context, if any.
- 3723 5. Select the port.
- 3724 6. Enter the name of the user who has permissions to write to the directory.
- 3725 7. Enter the password for the user.
- 3726 8. Confirm the password.



3727

3728

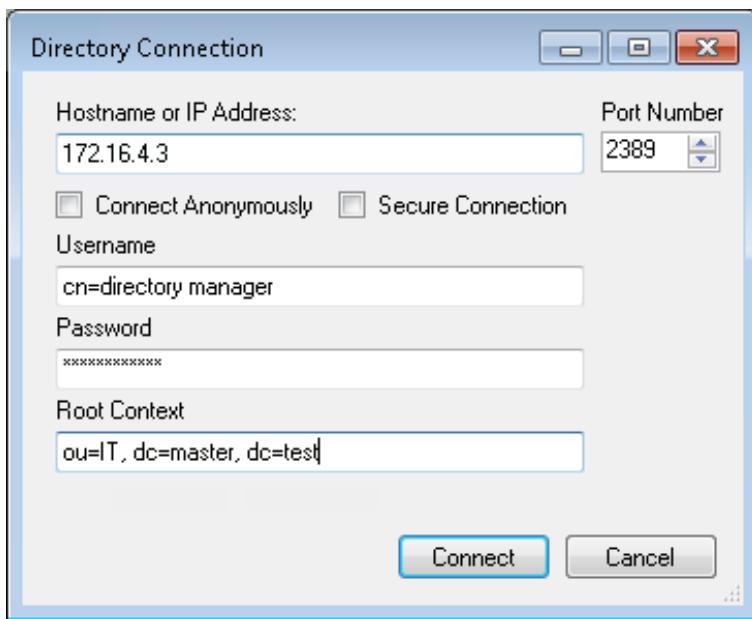
Figure 161. Ozone LDAP Publication Point

3729 **Import the desired groups from the RSA Adaptive directory**

3730 1. Right-click on the Groups proof.

3731 2. Select Import Group from Active Directory, Figure 162.

3732 3. Enter the directory connection information.



3733

3734

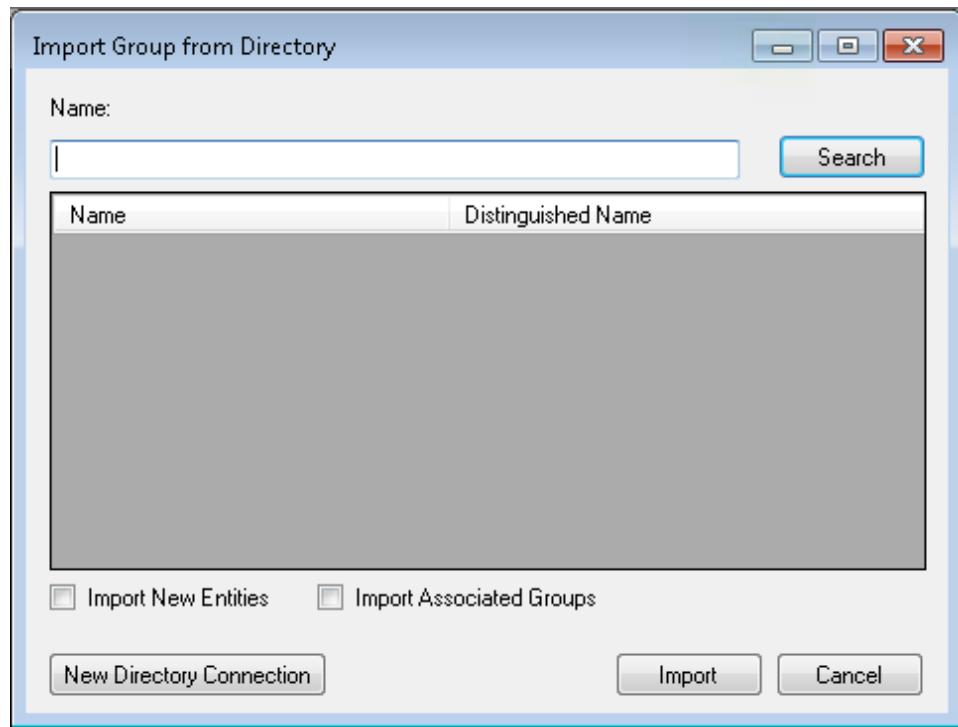
Figure 162. Ozone Directory Connection Information

3735 4. Select a group to import, see Figure 163.

3736 5. Check the box to Import New Entities.

3737 6. Check the box to Import Associated Groups.

3738 7. Then select Import



3739

Figure 163. Ozone Import Group from Directory

3740 8. Select the publication schedule as shown in Figure 164.

3741 9. Select the publication point as shown in Figure 164.

3742 10. Select the distribution point as shown in Figure 164.

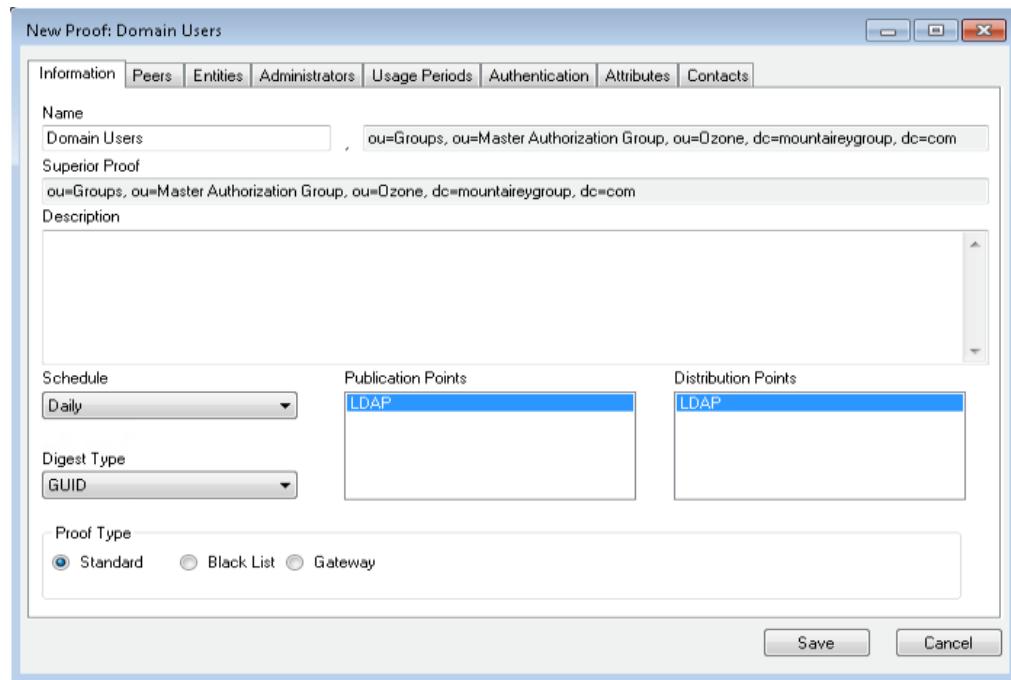
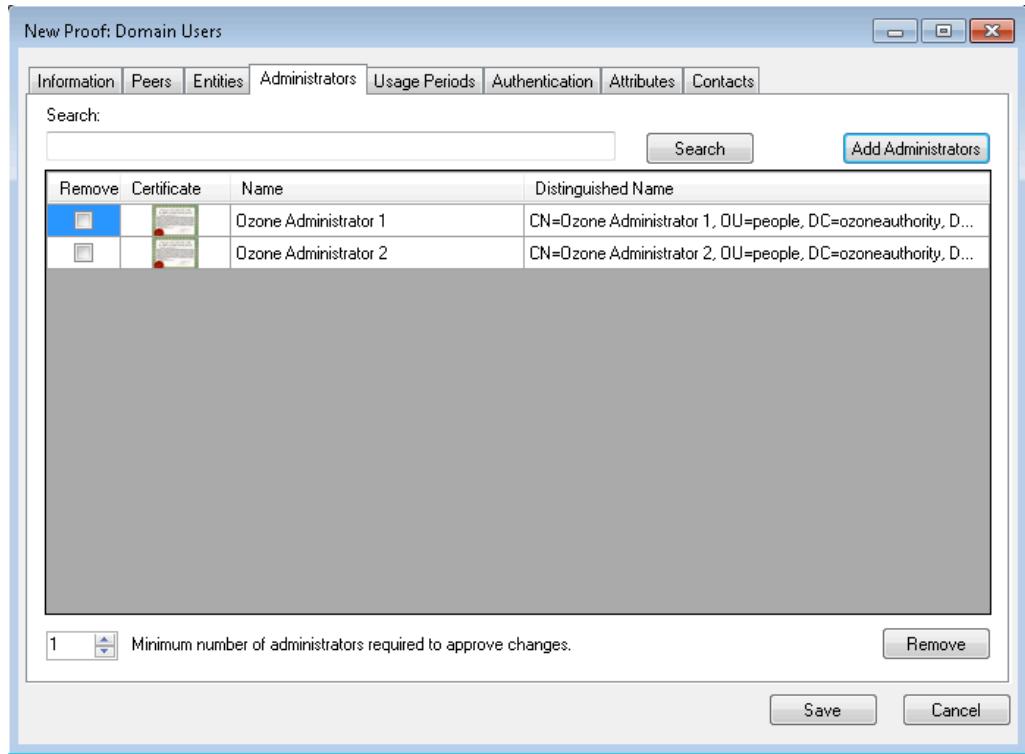


Figure 164. Ozone New Proof Information

- 3744 11. Click the Administrators tab as shown in Figure 165
- 3745 12. Click the Add Administrators button.
- 3746 13. Select the users who will administer the proof.
- 3747 14. Then select Add Entities



3750

3751

Figure 165. Ozone New Proof Administrators

3752 15. Click the Save button.

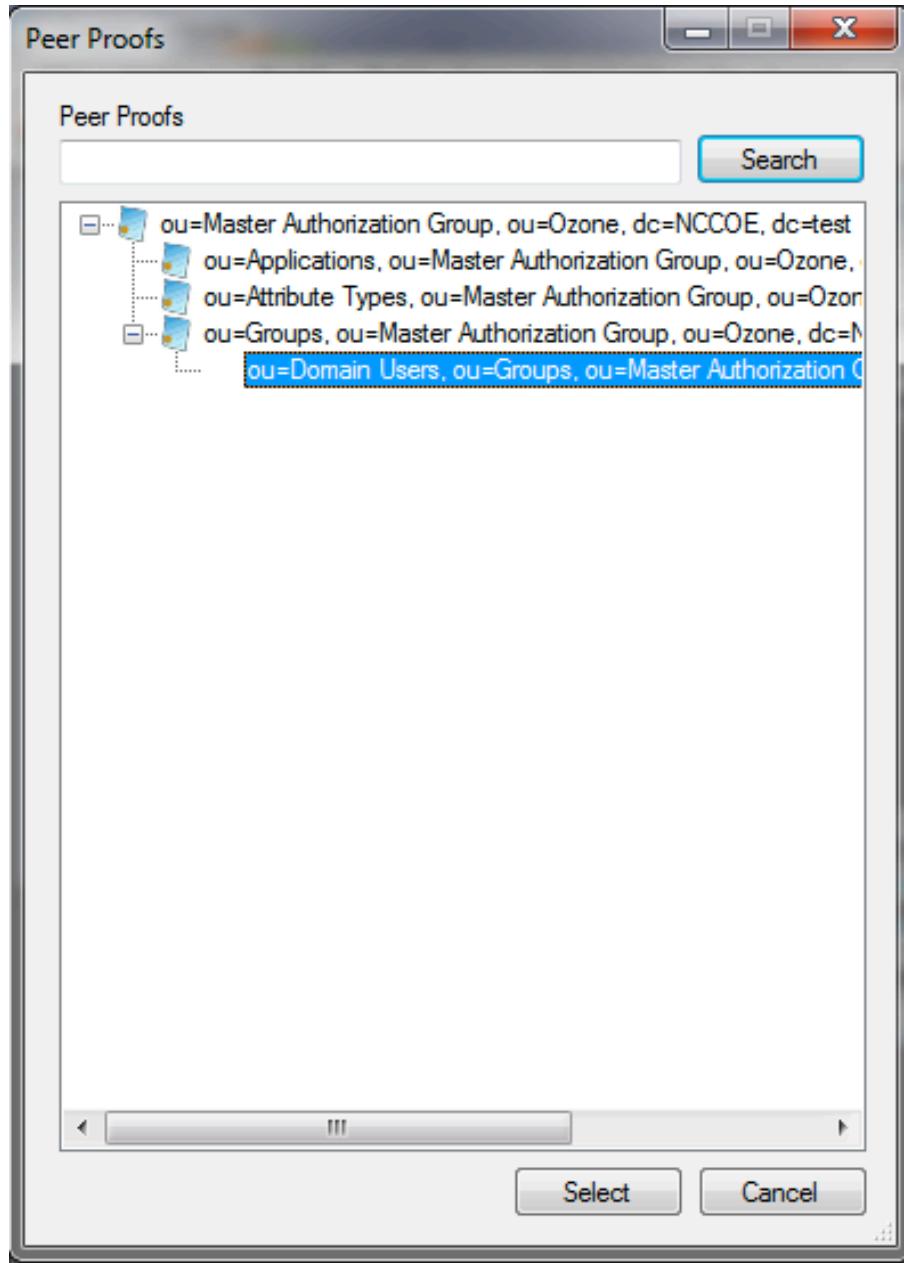
3753

3754 **Create the Ozone Server Configuration**

3755 1. Select Configuration > Ozone Server > New...

3756 2. Click the Add proof from tree... button.

3757 3. Select a proof Ozone Server should use for authorizations as shown in Figure 166.

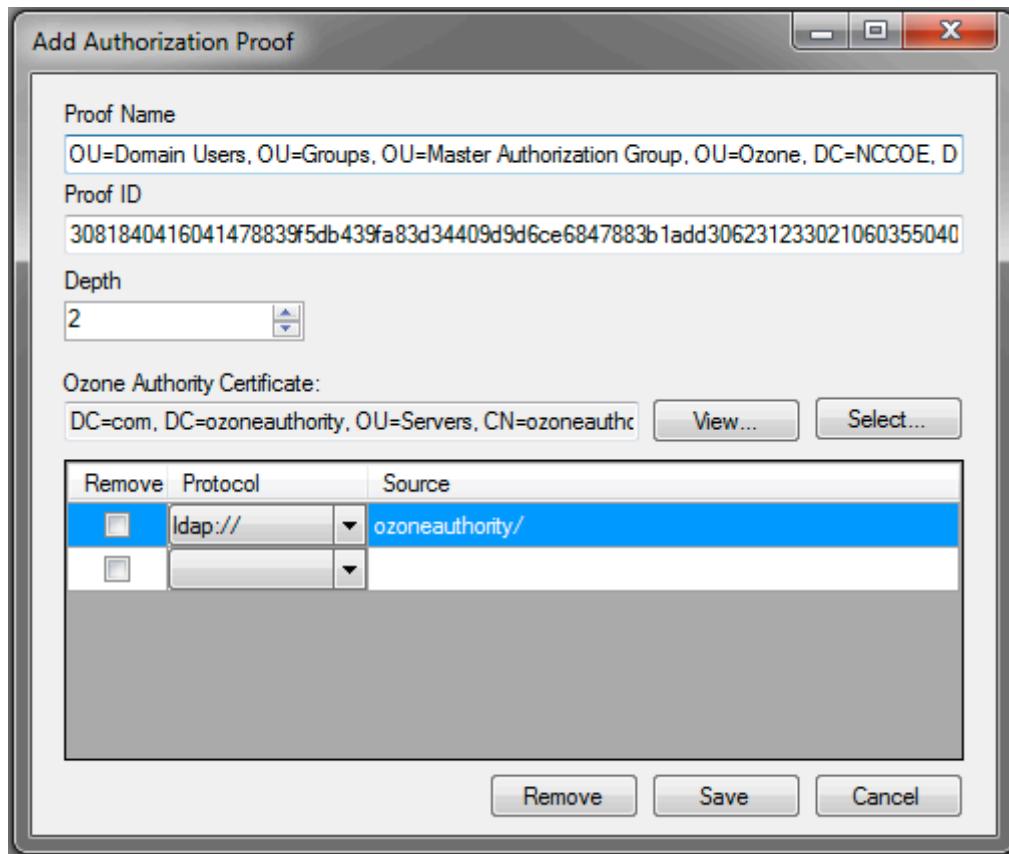


3758

3759

3760 4. Set the number of proof references (Depth) the proof may follow in order to authorize a
3761 credential as shown in Figure 167.

3762 5. Ensure that the locations where the Ozone Server will retrieve the proof are correct.



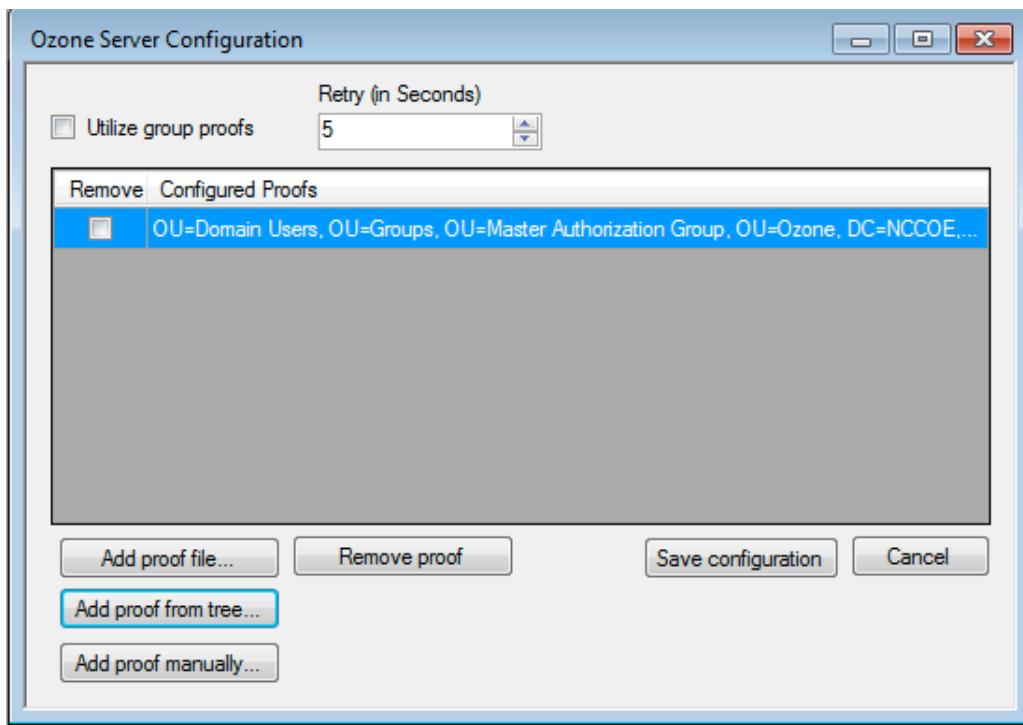
3763

3764

Figure 167. Ozone Add Authorization Proof

3765 6. Click the Save button.

3766 7. Repeat Steps 2–6 until you have selected all of the proofs Ozone Server should initially
3767 retrieve for Authorizations.



3768

Figure 168. Ozone Server Configuration

3769

- 3770 8. Click the Save configuration button as shown in Figure 168.
- 3771 9. Select a certificate to be used to digitally sign the configuration.
- 3772 10. Save the file as ServerConfiguration.xml.
- 3773 11. SCP the file to the Ozone Server machine.

3774 **13.5 OZONE SERVER INSTALLATION**

3775 **Create keys and certificates and store in Java Keystore (JKS)**

3776

3777 **Install java**

```
3778 [root@ozone ~]# yum install java
```

3779

3780 **Install Ozone Server**

```
3781 [root@ozone ~]# cd /usr/local/
3782 [root@ozone local]# tar -xzf ~/Ozone\ Server-2014.tar.gz
```

3783

3784 **Copy the keystore to the conf directory**

```
3785 [root@ozone local]# mkdir /usr/local/server/bin/conf/
3786 [root@ozone local]# cp ~/server.jks server/bin/conf/
```

3787

3788 **Copy the configuration and license files to the conf directory**

```
3789 [root@ozone local]# cp ~/ServerConfiguration.xml server/bin/conf/
3790 [root@ozone local]# cp ~/ServerLicense.xml server/bin/conf/
```

3791

3792 **Run the Ozone Server**

3793 [root@ozone server bin]# ./startServer.sh

3794 POST [MAIN] v2.1.301

3795

3796

3797 / \ // \ | | (R)

3798 | / \ | / / | \ | |

3799 | | | | / | | | | | |

3800 | | | | / | | | | | |

3801 | | | | / | | | | | |

3802 \ \ / / / \ \ / | | | |

3803 \ \ / / \ \ / | | | | |

3804

3805 / |

3806 | (

3807 \ \ / \ \ ' \ / / \ \ , _

3808) | / | \ v / / |

3809 | / \ | \ / \ \ |

3810

3811

3812

3813 Ozone(R) Server copyright (c) Pericore, Inc. 2007-2011

3814 -----

3815 Fri May 15 14:31:33 EDT 2015

3816

3817

3818 May 15, 2015 2:31:35 PM com.pericore.util.PericoreProvider jsafeJCEinit

3819 POST: [FIPS] FIPS-140 compliance self-test passed.

3820 Found Java version: 1.8.0_31

3821 Working in: /usr/local/server/bin

3822 /usr/local/server/bin/conf/server.cfg not found. Run setup [Y] : **y**

3823 env.work/usr/local/server/bin

3824 Found Java Version: 1.8.0_31

3825

3826 Ozone Server Setup Utility

3827 ***WARNING***

3828 This product MUST be installed by a Pericore Certified Engineer. Pericore,

3829 Inc. cannot be held liable for damages resulting from negligent or fraudulent

3830 actions of unauthorized or unqualified administrators. Please review all

3831 documentation thoroughly before continuing. Continuation of this

3832 configuration process represents an agreement to abide by the Pericore EULA.

3833 I agree to all terms and conditions set forth by Pericore, Inc. [N] : **y**

3834 Enable Startup Password? [N] : **n**

3835 May 15, 2015 2:31:37 PM

3836 com.pericore.util.ObjectIdentifierFactory\$OIDDataLoader debug

3837 INFO: ObjectIdentifierFactory Read 240.165 kb in 3.313 ms; Indexed 2,415 Arcs

3838 in 52.438 ms; 2,310(1,054:5) keys => 2.003 kb

3839 Server Configuration Directory:

3840 1: /usr/local/server/bin/conf

3841 2: Other...

3842 Choice [1] : **1**

3843

3844 Select the XML License File:

3845 1: /usr/local/server/bin/conf/ServerLicense.xml

3846 2: Other...

3847 Choice [1] : **1**

```
3848
3849 Select the XML Configuration File:
3850 1: /usr/local/server/bin/conf/ServerConfiguration.xml
3851 2: Other...
3852 Choice [1] : 1
3853
3854 Page 1 | Current Directory: /usr/local/server/bin
3855 [00] ../
3856 [01] lib/
3857 [02] conf/
3858   Select Server Identity Keystore [ # ] : 2
3859 Page 1 | Current Directory: /usr/local/server/bin/conf
3860 [00] ../
3861 [01] server.jks
3862
3863 Select Server Identity Keystore [ # ] : 1
3864 Enter password for server.jks : 123456
3865 Is the Private Key Alias 'server' correct? [Y] : Y
3866
3867 Enable logging? [Y] : Y
3868 Log File Roll Size (Kb) [512] : 512
3869
3870 Configured Client Services: 0
3871 Choose an option:
3872 1: Configure Authorization Service
3873 2: Configure a Proof Proxy
3874 3: Configure an Info Page
3875 4: Configure a Push Service
3876 5: Done Configuring Web Services
3877 Choice [1] : 1
3878
3879 Configuring XACML Authorization Service
3880 Service Port [8080] : 443
3881 Service Context [/AuthorizationService] : /AuthorizationService
3882 Enable WS-Security? [Y] : Y
3883 SOAP Signature Method:
3884 1: RSA_SHA1
3885 2: RSA_SHA256
3886 3: RSA_SHA384
3887 4: RSA_SHA512
3888 Choice [1] : 2
3889 Enable WS-Security Client Authentication? [N] : N
3890 Configured Client Services: 1
3891
3892
3893 Choose an option:
3894 1: Configure Authorization Service
3895 2: Configure a Proof Proxy
3896 3: Configure an Info Page
3897 4: Configure a Push Service
3898 5: Done Configuring Web Services
3899 Choice [1] : 5
3900
3901 Enable SSL? [N] : Y
3902 Service Port [8080] : 443
3903 Enable SSL Client Authentication? [N] : N
3904 Enable SSL? [N] : N
```

```

3905 Modify Advanced Performance Options? [N] : N
3906
3907 Writing server configuration...
3908 Thank you for choosing Ozone Server
3909 Goodbye.
3910
3911 [root@ozoneserver local]# /usr/local/server/bin/startServer.sh

3912 13.6 OZONE ENVOY INSTALLATION

3913 Ozone Envoy was installed and not utilized in the builds. The functions it provides, automated
3914 CRLs and certificate collection, were not required in the solution.
3915
3916 Create keys and certificates and store in Java Keystore (JKS)
3917
3918 Install java
3919 [root@ozoneenvoy ~]# yum install java
3920
3921 Install Ozone Envoy
3922 [root@ozoneenvoy ~]# cd /usr/local/
3923 [root@ozoneenvoy local]# tar -xzf ~/Ozone\ Envoy-2014.tar.gz
3924
3925 Copy the keystore to the bin directory
3926 [root@ozoneenvoy local]# cp ~/envoy.jks envoy/bin/
3927
3928 Edit the envoy.txt file to set configuration options
3929 ### Ozone Suite (c) Pericore, Inc. 2007-2014.
3930 ### All rights reserved.
3931
3932 ######
3933 #####
3934 ### envoy.txt - Ozone Envoy 2014 Configuration File ###
3935 ###
3936 ### Author: Jacob Dilles <jdilles@mountaireygroup.com> ###
3937 ###
3938 ### Date: 1 Jan 2014 ###
3939 ###
3940 ### Notes: This is a sample Ozone Envoy 4.1.0 Setup Configuration File ###
3941 ### demonstrating configuration options for Mobile Enrollment. ###
3942 ###
3943 ### In a production environment, you should exclude the /pass= ###
3944 ### properties and provide them on the command line during setup.###
3945 ### After installation is complete, this file should be deleted ###
3946 ### or 'chown root; chgrp 0; chmod 000' to secure it. ###
3947 ######
3948 #####
3949
3950 ### General Envoy Configuration
3951
3952 ######
3953 ##### Identity Keystore Configuration #####
3954 ##### This keystore is used for:

```

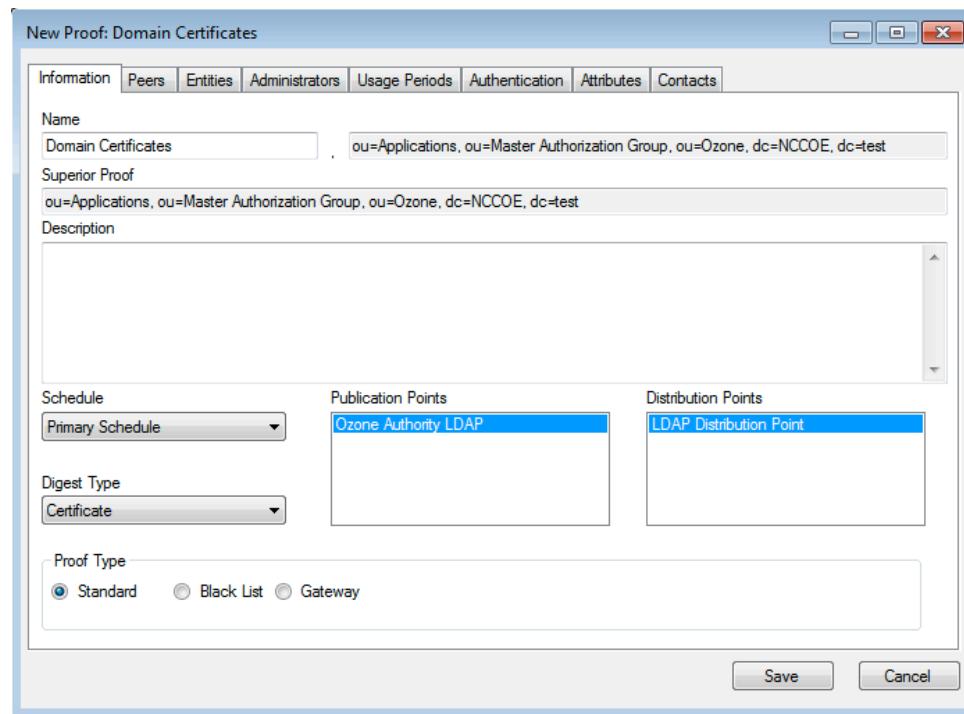


```
4012 Fri May 15 15:09:04 EDT 2015
4013
4014 Ozone Envoy Mobile 2014 Setup Utility
4015 Ozone Suite copyright (c) Pericore, Inc. 2007-2014.
4016 All rights reserved.
4017
4018 ***WARNING***
4019 This product MUST be installed by a Pericore Certified Engineer.
4020 Improper configuration of Ozone Envoy Tool may cause security
4021 vulnerabilities.
4022
4023 I agree to all terms and conditions set forth by Pericore, Inc. [N] : y
4024 envoy.jks
4025 system/identity/store [/usr/local/envoy/bin/envoy.jks] :
4026 Enter password for envoy.jks :
4027 Is the Private Key Alias 'envoy' correct? [Y] : y
4028
4029 [POST] Starting Authority Listener: https://ozoneenvoy:4242/ ..... [ OK ]
4030 > :
4031
4032 Return to Ozone Console to complete Ozone Envoy Configuration
```

4033 [13.7 OZONE CONSOLE ENVOY CONFIGURATION](#)

4034 **Create a proof to store the certificates retrieved by Ozone Envoy**

- 4035 1. Open Ozone Console.
- 4036 2. Select an administrator certificate to log in as shown in Figure 169.
- 4037 3. Select *Proof>New Proof..*
- 4038 4. Enter a name for the proof.
- 4039 5. Select the publication schedule.
- 4040 6. Select the publication point(s).
- 4041 7. Select the distribution point(s).



4042

4043

Figure 169. Ozone New Proof Information

- 4044 8. Click the Administrators tab.
- 4045 9. Select the administrators to manage the proof.
- 4046 10. Click the Authentication tab.
- 4047 11. Click the Add from file... button.
- 4048 12. Select the CA and intermediate CA certificates to be used to authenticate certificates retrieved.
- 4049
- 4050 13. Select the Certificate Revocation Lists tab as shown in Figure 170.
- 4051 14. Enter a CRL grace period, the number of hours a CRL can be considered valid after its next update time.
- 4052
- 4053 15. Click the Add... button to add a CRL.

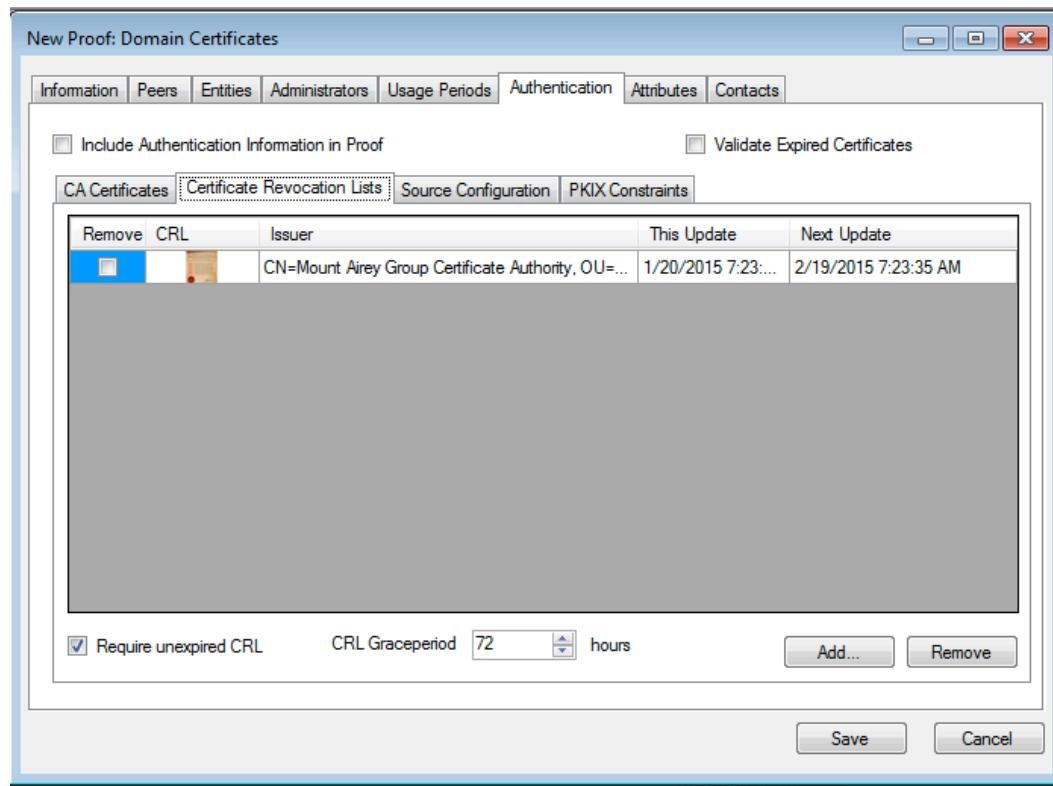


Figure 170. Ozone New Proof Authentication CRLs

4054

4055 16. Select the Source Configuration tab as shown in Figure 171.

4056 17. Enter hostname or IP address of the LDAP server.

4057 18. Enter the port the LDAP server is listening on.

4058 19. Check the box for LDAPS.

4059 20. Enter the base context of where user certificates can be obtained.

4060 21. Enter the attributeName for the certificates, either userCertificate or userCertificate;binary

4061 22. Enter the base context of where updated CRLs can be obtained.

4062 23. Enter the attributeName for the CRLs, typically certificateRevocationList shown in Figure 156.

4063 24. Enter the connection information:

- If connecting anonymously, check the box for anonymous connections.
- If a username/password is required for the connection, enter them.

4064 25. Enter the number of hours after which Ozone Envoy should check the directory for new certificates.

4065

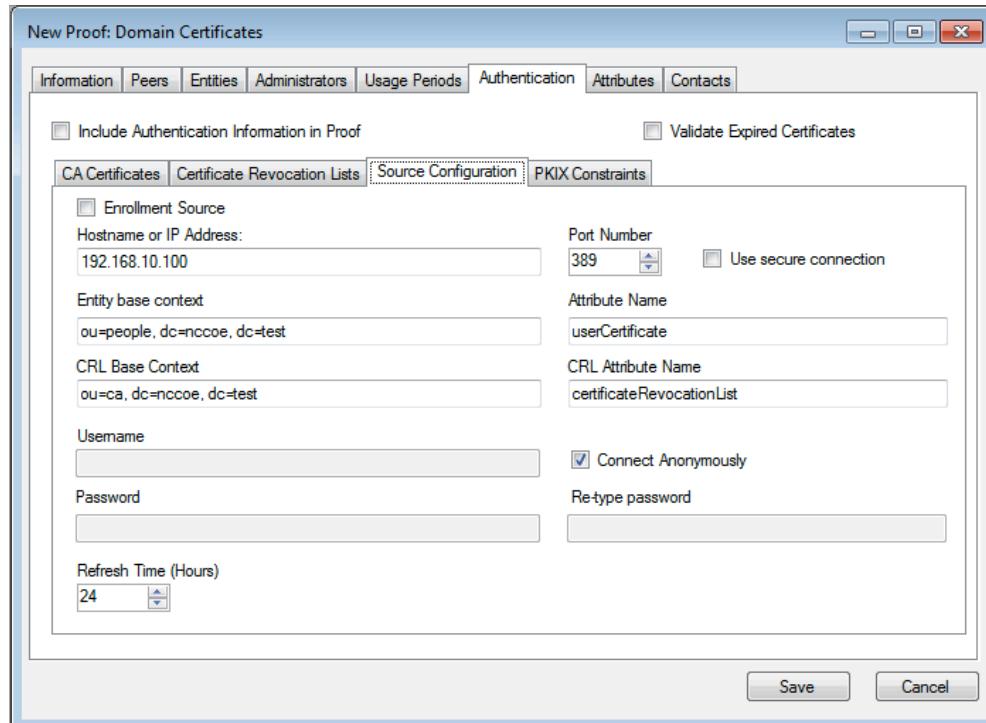
4066

4067

4068

4069

4070



4071

4072

Figure 171. Ozone New Proof Authentication Source Configuration

4073

26. Click Save.

4074

4075 **Configure Ozone Authority to connect to Ozone Envoy**

4076

1. Select Enrollment>Envoy Configuration.

4077

2. Enter the hostname or IP address of the Ozone Envoy. See Figure 172..

4078

3. Enter the port number Ozone Envoy is listening on.

4079

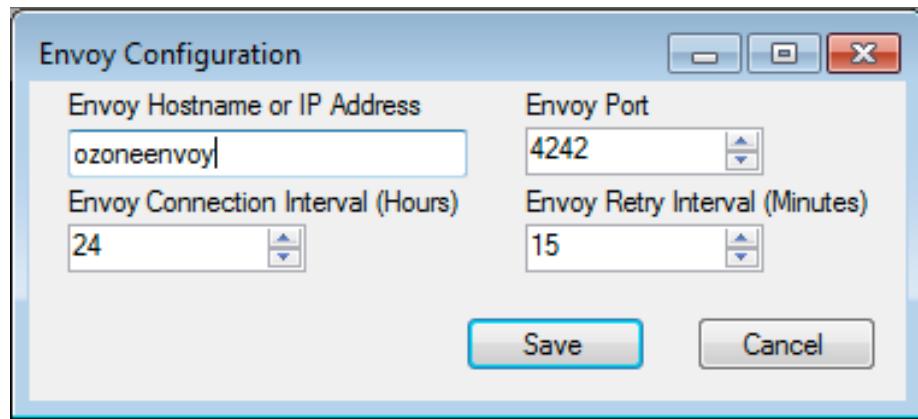
4. Enter the number of hours that should elapse between connections to Ozone Envoy to check for new information.

4080

5. Enter the number of minutes to before attempting to reconnect to Ozone Envoy if the connection fails.

4081

6. Click Save.



4084

4085

Figure 172. Ozone Envoy Configuration

4086

4087 **14 PHYSICAL ACCESS CONTROL: XTEC XNODE**

4088 The XNode was installed in the DMZ network. The Xnode is a standalone IdAM demonstration
 4089 capability including a personal identification verification (PIV) card reader, PIV Interoperability
 4090 (PIV-I) cards, keypad and electric door strike. The XNode was preconfigured to poll the IP
 4091 address of the cloud based IdAM system at the Xtec control center. No additional configuration
 4092 information is required. The identities on the PIV cards included access allowed and access
 4093 denied status for demonstration purposes.

4094 **14.1 SECURITY CHARACTERISTICS**

4095 Cybersecurity Framework Categories: PR.AC-1: Identities and credentials are managed for
 4096 authorized devices and users

4097 NIST 800-53 rev 4 Security Controls: AC-2, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9

4098 **15 ENTERPRISE PKI PLATFORM: GLOBALSIGN**4099 **15.1 OVERVIEW**

4100 The NCCoE used the GlobalSign Enterprise PKI platform to issue and manage North American
 4101 Energy Standards Board (NAESB) WEQ-12 digital certificates used for secure network access of
 4102 for both internal and external users, see Figure 173. The certificates were used in conjunction
 4103 with the MAG Ozone product to provide high assurance attributes for the Personal Profile
 4104 Application (PPA). The application has three main information groups for which actions can be
 4105 authorized: Personal Information, Credit Reports, and Criminal History. Based on the
 4106 authorizations associated with a credential, results pages are dynamically populated.

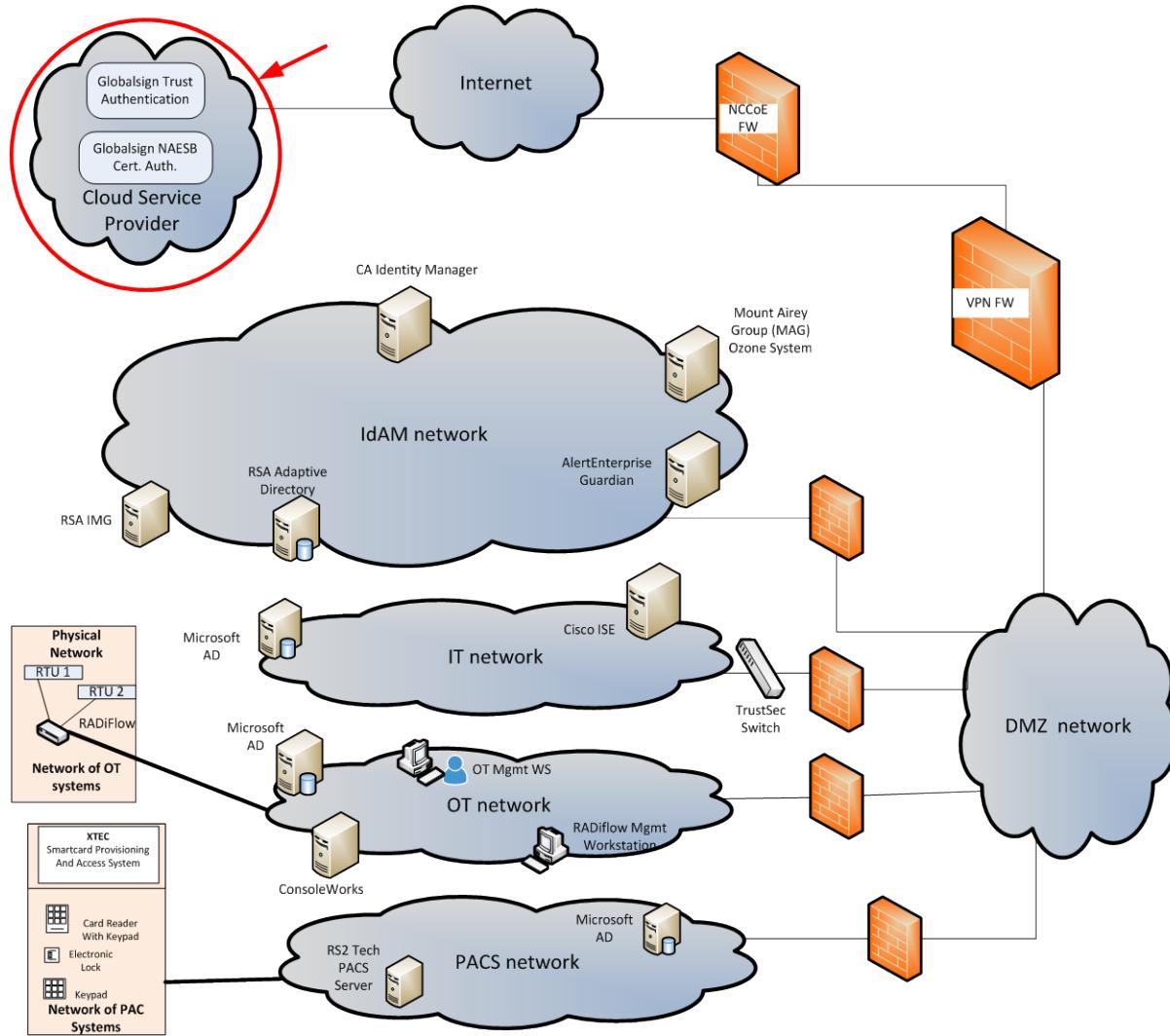


Figure 173. GlobalSign Overview

4109 The North American Energy Standards Board (NAESB) serves as an industry forum for the
 4110 development and promotion of business process standards which can lead to a seamless
 4111 marketplace for wholesale and retail natural gas and electricity, as recognized by its customers,
 4112 business community, participants, and regulatory entities. GlobalSign is an active participant of
 4113 the NAESB Cyber-Security standards committee and is a [NAESB-authorized Certificate Authority
 4114 \(CA\)](#). For more information about NAESB, go to [4115 GlobalSign's NAESB-compliant certificate-based authentication solution is managed through a
 4116 SaaS service accessed through a web-based portal. The web portal gives organizations control of
 4117 Digital IDs issued to individuals using one of four NIST defined assurance levels. Set-up usually
 4118 takes less than three days. Another advantage of the web-portal is that all of the lifecycle
 4119 functions including issuance, re-issuance, renewal, and revocation are available to the
 4120 administrator.](https://www.naesb.org/.</p>
</div>
<div data-bbox=)

4121 15.1.1 **Managing the Account**
4122 Managing the account is accomplished using the GlobalSign [Certificate Management Center](#)
4123 ([GCC](#)). GCC is a web-based interface allowing you to access your certificates anywhere with an
4124 Internet connection. Within the platform, administrators may add additional users and delegate
4125 some or all certificate management functions.

4126 15.1.2 **What Is a Profile? / Profile Management**
4127 A profile, or certificate profile, contains the organization's identity information that will be used
4128 for all NAEsb WEQ-12 digital certificates issued from the account. Organization identity
4129 information includes the organization legal name, country code, and optionally locality, state,
4130 and up to three fixed organization units as well as assurance level.

4131 15.1.3 **What Is a License?**
4132 GlobalSign NAEsb digital certificates are valid for either (1) or (2) years and must be issued
4133 within (12) months of license ordering.

4134 GlobalSign NAEsb digital certificates are sold in "license packs" (i.e., in quantities of 5, 10, 25,
4135 50, etc.) Certificates are issued with either (1) or (2) year validities and must be issued within
4136 (12) months of license ordering.

4137 **15.2 SECURITY CHARACTERISTICS**

4138 Cybersecurity Framework Categories: PR.AC-1: Identities and credentials are managed for
4139 authorized devices and users

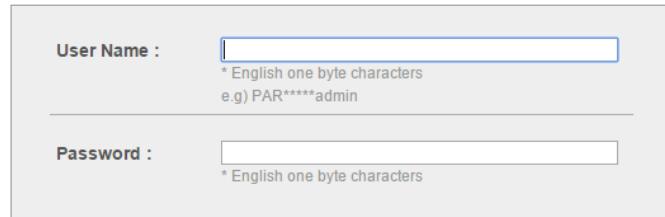
4140 NIST 800-53 rev 4 Security Controls: AC-2, IA Family

4141 **15.3 How To ORDER CERTIFICATES**

4142 15.3.1 **Step 1: Get a GlobalSign Gcc Account**
4143 Request a GlobalSign Certificate Center account here –
4144 <https://www.globalsign.com/en/verticals/energy/>.

4145 15.3.2 **Step 2: Order Certificate License Pack**
4146 Once you have your GCC account credentials, use the following link to login –
4147 www.globalsign.com/en/login/. See Figure 174.

Ordering Certificates from GlobalSign is Quick & Easy



The image shows the GlobalSign login interface. It features a 'User Name' field with a note: '* English one byte characters e.g) PAR*****admin' and a 'Password' field with a note: '* English one byte characters'.

4148

4149

Figure 174. GlobalSign Login Page

4150

4151 Click on the “Enterprise PKI” tab as shown in Figure 175.

4152

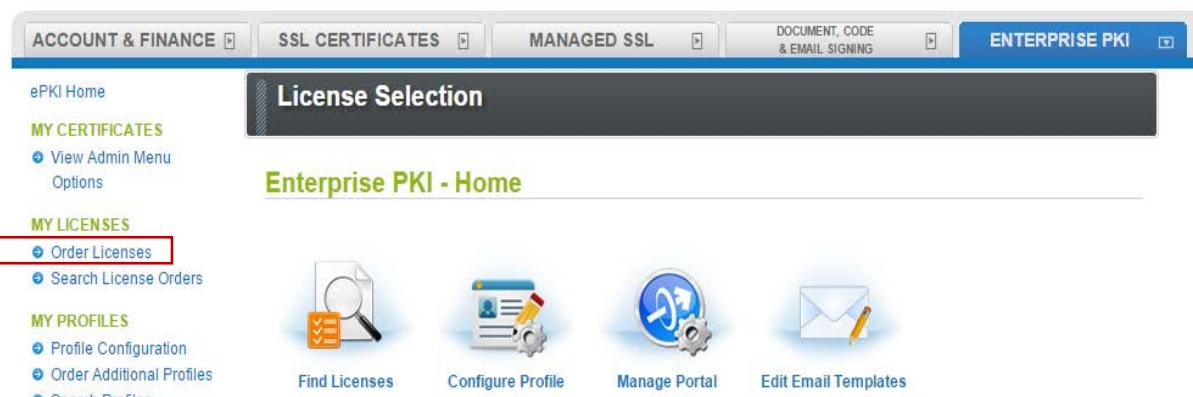


4153

Figure 175. GlobalSign Enterprise PKI Tab

4154

4155 Click “Order Licenses” from the left hand menu as shown in Figure 176.



4156

4157

Figure 176. GlobalSign Order Licenses Page

4158

4159 Choose the “Enterprise PKI Pro For Personal Digital ID” license pack you intend to purchase and
4160 click next as shown in Figure 177.

License Selection

Product Details

Personal Sign

- Enterprise PKI Pro For Personal Digital ID 5 pack
- Enterprise PKI Pro For Personal Digital ID 10 pack
- Enterprise PKI Pro For Personal Digital ID 25 pack
- Enterprise PKI Pro For Personal Digital ID 50 pack

Next

4161

4162

Figure 177. GlobalSign License Selection Page

4163

4164 Choose your validity period (1 or 2 year certificate), see Figure 178.

4165



Product Details - Enterprise PKI Pro For Personal Digital ID 50 pack

Certificate Validity Required Multi-year offers significant per annum savings	<input checked="" type="radio"/> 1 year <input type="radio"/> 2 year
Campaign Code	<input type="text"/> Redeem code If you have a Campaign Code please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.
Coupon Code	<input type="text"/> Redeem code If you have a one-off Coupon Code for a particular promotion please enter and click "Redeem Code". This page will be reloaded with your appropriate discount.
TOTAL COST (inc. Tax)	\$ 0

4166

4167

Figure 178. GlobalSign Product Details

4168

Provide payment details as shown in Figure 179.

Payment Details

Purchase Order Number	<input type="text"/> Enter if you have a PO Number. This will be displayed in your Invoice
Payment Method	<input type="radio"/> Payment in arrears <input checked="" type="radio"/> Credit Card

Credit Card Details & Billing Address



4169

4170

Figure 179. GlobalSign Payment Details

4171 Confirm your order details and check the box confirming you understand that the license pack
 4172 will expire 12 months from the order date, Figure 180.

Confirm Details

License Details

Product	Enterprise PKI Pro For Personal Digital ID 50 pack
Certificate Validity	1 year
Campaign Code	
Coupon Code	
TOTAL COST (inc. Tax)	\$ 0

Payment Details

Purchase Order Number	
-----------------------	--

Others

Special Instructions	
----------------------	--

4173 Required I understand that this license pack will expire 12 months from the order date.

Figure 180. GlobalSign Confirm Details

4175 15.3.3 Step 3: Set Up Organization Profile

4176 Click “Order Additional Profiles” from the left navigation menu as shown in Figure 181.

The screenshot shows the GlobalSign Enterprise PKI interface. The top navigation bar includes 'ACCOUNT & FINANCE', 'SSL CERTIFICATES', 'MANAGED SSL', 'DOCUMENT, CODE & EMAIL SIGNING', and 'ENTERPRISE PKI'. The 'ENTERPRISE PKI' tab is selected. The left sidebar has sections for 'MY CERTIFICATES' (View Admin Menu, Options), 'MY LICENSES' (Order Licenses, Search License Orders), and 'MY PROFILES' (Profile Configuration, Order Additional Profiles, Search Profiles). The 'Order Additional Profiles' link is highlighted with a red box. The main content area is titled 'License Selection' and 'Enterprise PKI - Home'. It features four icons: 'Find Licenses' (document with magnifying glass), 'Configure Profile' (person with gear), 'Manage Portal' (gears), and 'Edit Email Templates' (envelope with pencil).

4177

Figure 181. GlobalSign Order Additional Profiles

4179 Enter your Organization Profile details. Please note the details you enter will be vetted and
 4180 included as the certificate identity within your issued certificate, see Figure 182.

4181 Additionally select the Assurance level appropriate for the risk associated with the transaction.
 4182 Contact GlobalSign NAESB experts for additional guidance on this topic.

Certificate Profile Details

These details will be vetted and included as the certified identity within your issued Certificate. Make sure the details entered are correct - we will vet the details you include. To assist you, some details will be pre-populated from previous pages or from your GCC account details, you may overwrite these if needed.

Note. Within the form below you have the ability to define the certificates DistinguishedName (DN). One optional element is a freeform Organizational Unit (OU) description. The OU field allows you to enter a value that suits your business needs with a description such as "Marketing Team Building 5" for example. It is not mandatory to enter this but please note that if you choose to 'Lock a unique OU' then this means that the description you have chosen cannot be used again and is unique to this profile. An example of where you might choose to do this is for client authentication situations where each certificate needs one or two fixed unique strings to allow access such as 'O' and 'OU'.

Organization Required	Your company legal name
Organizational Unit Optional unless locked as unique	<input type="text"/> <input type="text"/> <input type="text"/>
<input type="checkbox"/> Lock a unique OU	
Locality Optional	<input type="text"/>
State or Province Optional	<input type="text"/>
Country Required	United States - US ▼
Assurance Level	<input type="radio"/> RUDIMENTARY <input checked="" type="radio"/> BASIC <input type="radio"/> MEDIUM <input type="radio"/> HIGH

Next 

4183

4184

Figure 182. GlobalSign Certificate Profile Details

4185 Confirm your profile details (Figure 183) and then review and accept the EPKI Service
 4186 Agreement that includes important NAESB WEQ-012 obligations. Note the EPKI Service
 4187 Agreement binds you to obligations as outlined in the GlobalSign Certificate Policy and
 4188 Certificate Practice Statements, including Local Registration Authority, end user, and relying
 4189 party, as defined in the NAESB Public Key Infrastructure (PKI) Standards – WEQ-012.
 4190 Certificate Practice Statements can be found at <http://www.globalsign.com/repository/>

Confirm Details

Lock a unique OU	
Organization	Your company legal name
Organizational Unit	
State or Province	NH
Locality	Portsmouth
Country	United States - US
Assurance Level	RUDIMENTARY

ePKI Service Agreement

4191

GlobalSign ePKI Service Agreement - Version 2.4

4192

Figure 183. GlobalSign Confirm Details

4193 15.3.4 Step 4: Vetting

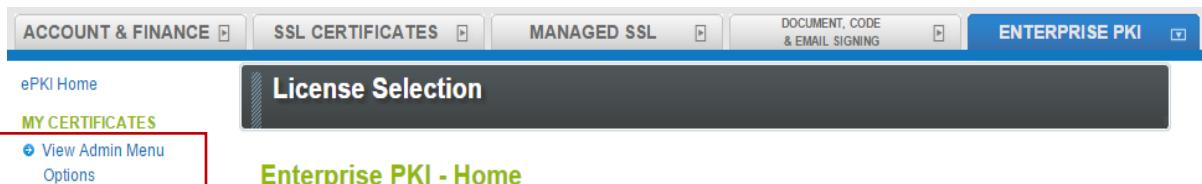
4194 Once you have placed your order, all of your information will be sent to GlobalSign's vetting
4195 department. The organization details you provided for your profile will be vetted by GlobalSign
4196 using third party checks.

4197 15.3.5 Step 5: Register for Your EPKI Administrator Certificate

4198 Once your company profile has been approved, you will need to register for what is known as
4199 an "EPKI Administrator Certificate." An EPKI Administrator Certificate is required to authenticate
4200 to secure areas of the EPKI service to register and manage end user certificates.

4201 1. Login into GCC

4202 2. Select "View Admin Menu Options" in the left hand menu to start the enrollment
4203 process, see Figure 184.



4204

Enterprise PKI - Home

4205

Figure 184. GlobalSign View Admin Menu Options

4206 3. Choose a certificate password. It is very important to remember this password.

4207 4. Download your administrator certificate and follow the on screen prompts to install your
4208 certificate.

4209 Please follow the guide [http://www.globalsign.com/support/ordering-guides/epki-](http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf)

4210 [authentication-user-guide.pdf](http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf) for step-by-step instructions on how to order, install, and use
4211 your Administrator Certificate.

4212 CAUTION: If you need to access the EPKI administrator menu options from multiple machines,
 4213 you can copy your .pfx file to other computers and repeat the import process. Instructions for
 4214 importing your certificate can be found here -
 4215 <https://support.globalsign.com/customer/portal/articles/1211387>.

4216 15.3.6 **Step 6: Register and Issue Certificates to Individual Users**

4217 Click “Order Certificates” in the left navigation menu as shown in Figure 185.

4218 NOTE: If you haven’t already authenticated to the secure section of the portal with your
 4219 Administrator Certificate, you may see “View Admin Menu Options” instead of the menu
 4220 options included in the image below. Simply click the “View Admin Menu Options” link and
 4221 select the appropriate certificate to gain access to this section of the portal.

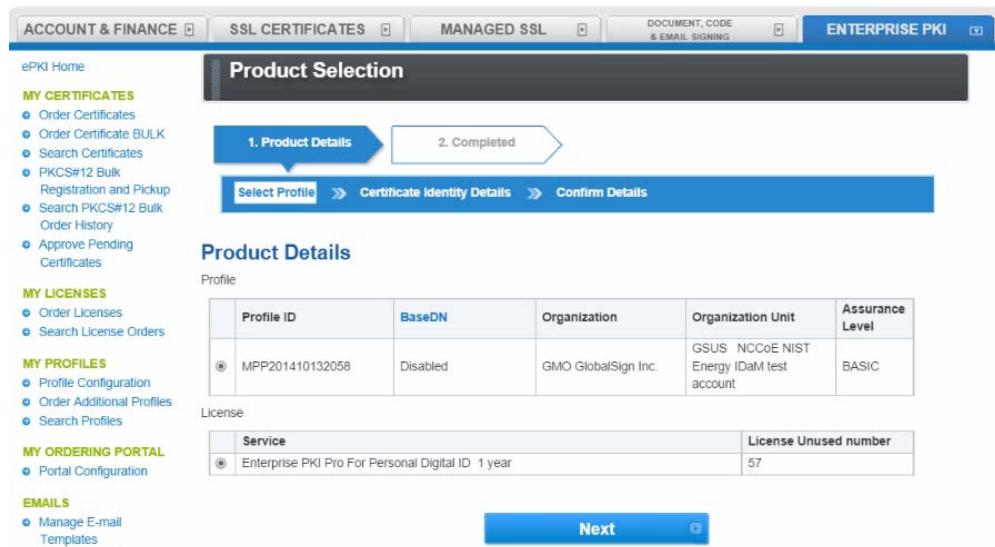


4222

4223

Figure 185. GlobalSign Order Certificates

4224 Select the profile and license you want to use and click Next, see Figure 186.



4225

4226

Figure 186. GlobalSign Product Selection

4227 Complete the certificate identity details (Figure 187) for the end user of the certificate, including
 4228 the common name (i.e., the individual’s first and last name) and the email addresses.
 4229 Organization name, and other fields will be pre-populated from the profile you selected.

Certificate Identity Details

Common Name <small>Required</small>	<input type="text"/>
Organization	GMO GlobalSign Inc.
Organizational Unit [Profile]	GSUS NCCoE NIST Energy IDaM test account
Organizational Unit	<input type="text"/>
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address <small>Required</small>	<input type="text"/>

Option certificate delivery method - Select only 1

I have an externally generated CSR <small>Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR)</small>	<input type="checkbox"/>
---	--------------------------

4230

4231

Figure 187. GlobalSign Certificate Identity Details

4232 You will also need to choose a “pick up password”. The pick up password is a unique password
 4233 that you will give to the end user of the certificate. After you have completed the registration
 4234 process, the end user will receive an email invitation to pick up their certificate and at that time
 4235 they will be prompted for the pick up password (you gave them in an out-of-band method)
 4236 along with details of how to install their new certificate.

4237 Finally, confirm the details of your certificate request as shown in Figure 188.

Confirm Details

Product Details

Profile ID	MPP201410132058
License ID	MPL201410133096

Certificate Identity Details

Common Name	Julie O
Organization	GMO GlobalSign Inc.
Organizational Unit	GSUS NCCoE NIST Energy IDaM test account
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address	julie0@globalsign.com
Encrypting File System	Disabled
MS SmartCard Logon	
I have an externally generated CSR	Disabled
PKCS12 Option	Disabled
Memo	

4238

4239

Figure 188. GlobalSign Confirm Details

4240 Repeat this process until you have requested certificates for all of your end users.

4241 For further information on the features available in your GlobalSign Certificate Center please
4242 visit: <http://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf>

4243 **15.4 GLOBALSIGN'S IDENTITY AND ACCESS MANAGEMENT SOLUTION FOR MANAGING EXTERNAL USERS**

4244 For use cases involving external users (e.g. Independent System Operators (ISOs) operating
4245 wholesale electric marketplaces), GlobalSign PKI can provide an identity and access
4246 management (IAM) solution that enables management of external user (customer and partner)
4247 identities and the online services and applications they can access.

4248 **15.5 GETTING HELP**

4249 GlobalSign provides technical support through our Client Service departments around the
4250 world. Visit <https://www.support.globalsign.com> for detailed instructions on installing and
4251 managing certificates, or contact support@globalsign.com or 1-877-467-7543 with specific
4252 questions.

4253 **16 INDUSTRIAL FIREWALL: SCHNEIDER ELECTRIC**

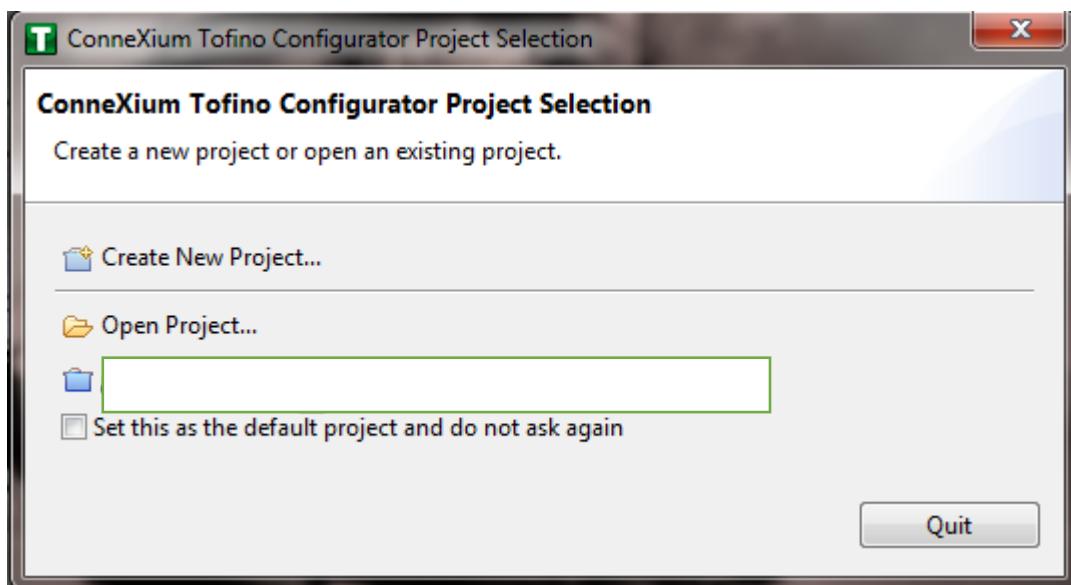
4254 A Schneider Electric (SE) industrial firewall is installed on the physical network that contains the
4255 industrial control system/SCADA components that can be accessed and controlled via the OT
4256 network. The firewall is configured to monitor the data passing between the RADiFlow SCADA

4257 firewall and the OT network. The SE industrial firewall will alert if out-of- policy traffic is
4258 detected on the network segment connecting the OT network and the SCADA network of
4259 devices.

4260 Install and Configure Schneider Tofino Firewall

4261 1. Download the ConneXium software from the Schneider site as stated in the instructions
4262 accompanying the firewall, start the ConneXium Tofino Configurator.

4263 2. At the startup screen, click 'Create New Project...', Figure 189.

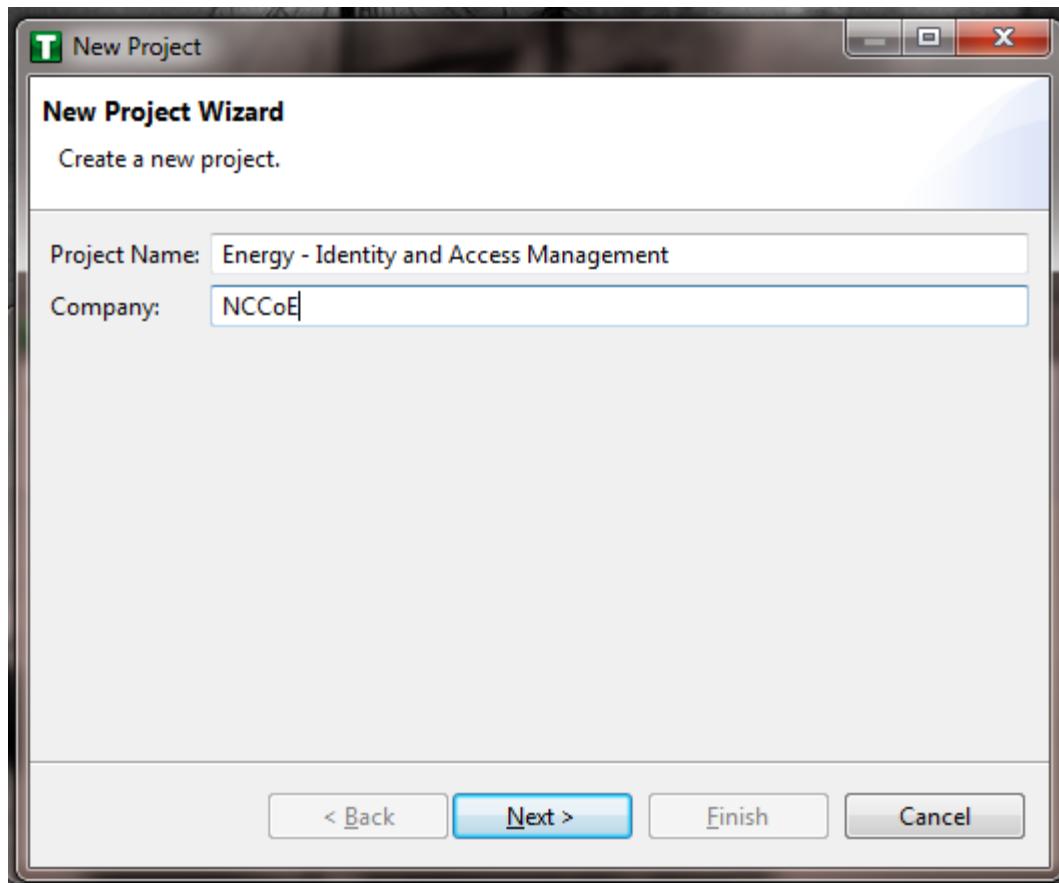


4264

4265

Figure 189. Create New Project

4266 3. In Project name, enter the name you would like to use for the project, as shown in
4267 Figure 190. Also fill in the Company field. When finished, click Next.

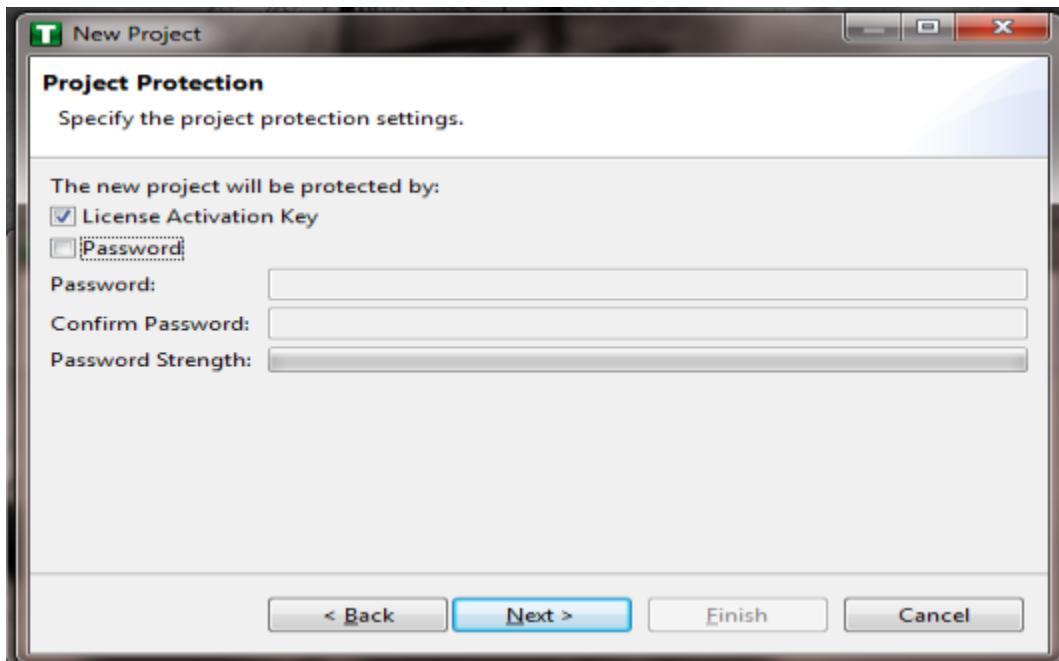


4268

4269

Figure 190. New Project Wizard

4270 4. In the Project Protection screen, Figure 191, choose a password to protect the project.
4271 Then click Next.



4272

4273

4274

Figure 191. Project Protection

In the Administrator Password screen,



4275

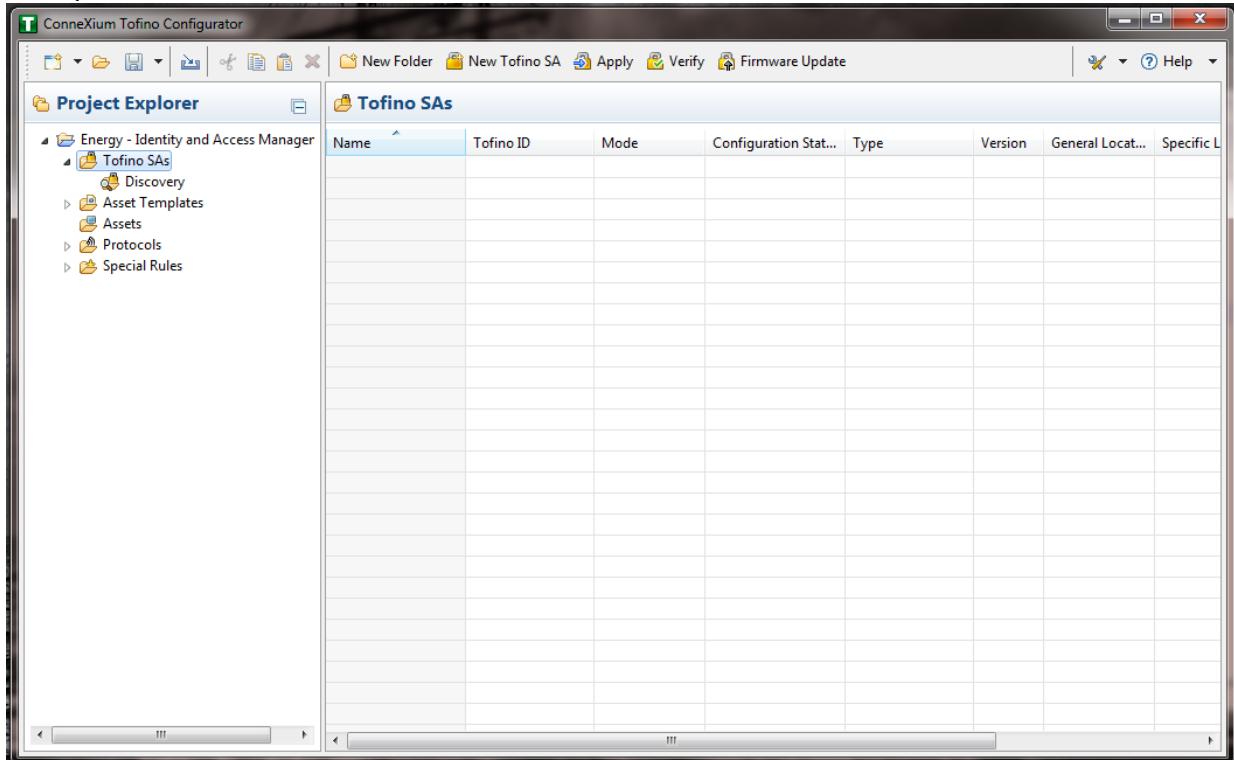
5. Figure 192, choose the administrator password. Then click Finish.

4276

4277

Figure 192. Administrator Password

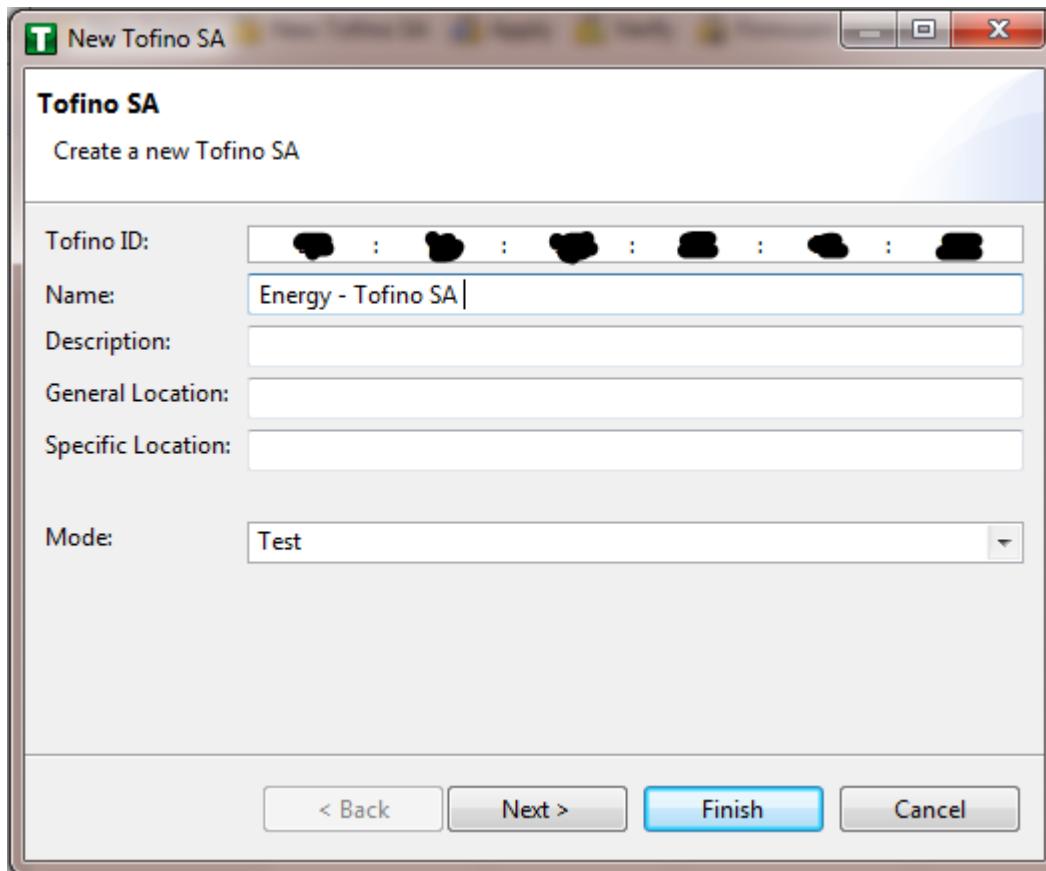
4278 6. In the Project Explorer Window, Figure 193, right click 'Tofino SAs' and select 'New
4279 Tofino SA'. *Note: You can also chose to create a folder for the SAs to help organize
4280 multiple areas.



4281

Figure 193. Project Explorer Window

4282 7. In the Tofino ID field, Figure 194, enter the MAC address listed on the firewall hardware
4283 sticker. Fill out the rest of the fields as necessary. Then click Finish.
4284



4285

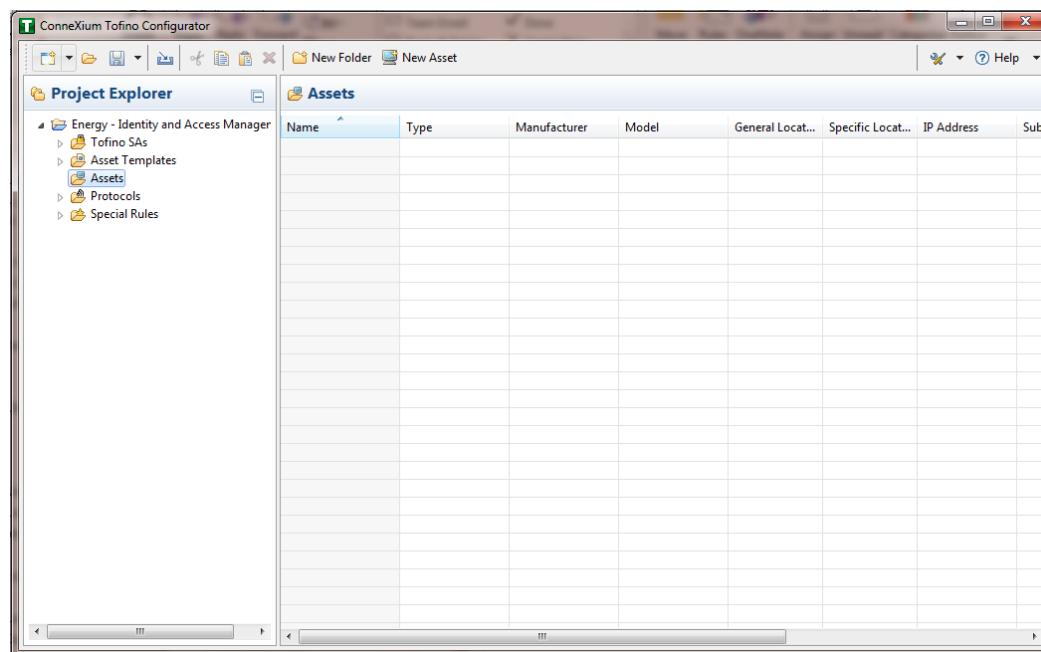
4286

Figure 194. Tofino SA/MAC Address

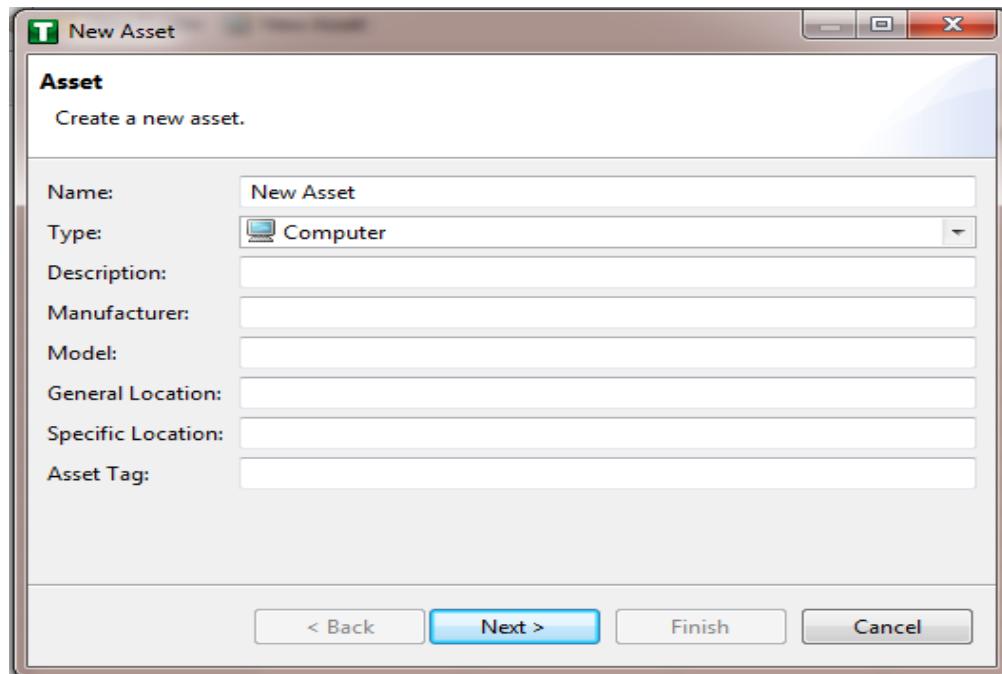
4287

8. Right click on the 'Assets' icon in the Project Explorer frame, Figure 195, and click 'New

4288 Asset.'

Figure 195.
Project
Explorer

4293 9. In the New Asset window, Figure 196, set the name of the device, as well as the type
4294 and all other fields as necessary. Then click Next.



4295

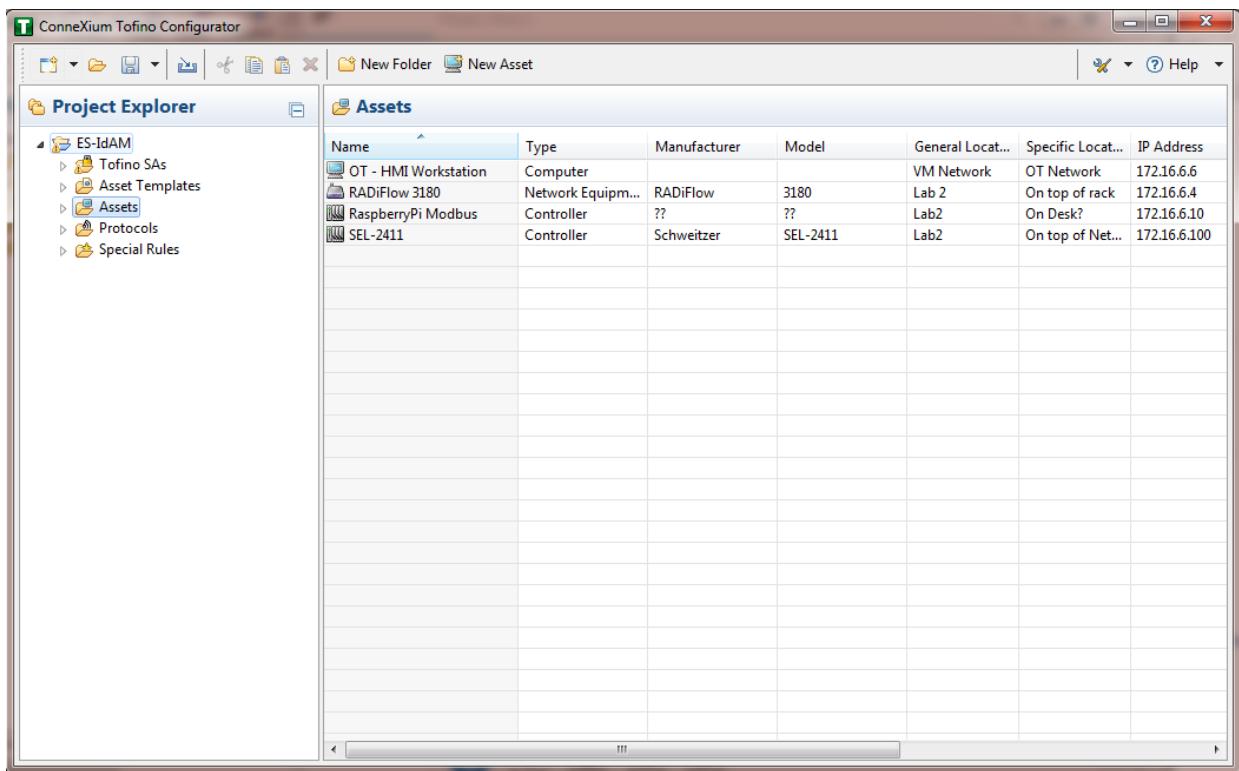
Figure 196. New Asset

4296

4297

4298 10. Fill in the IP address and/or the MAC address fields, Figure 197, then click Finish.

4299 11. Repeat steps 8-10 for all devices on the network. When they are configured, click on the
4300 'Assets' icon, Figure 197, in the Project Explorer frame (if it isn't already selected) and
4301 there should be a list of all the configured Assets.

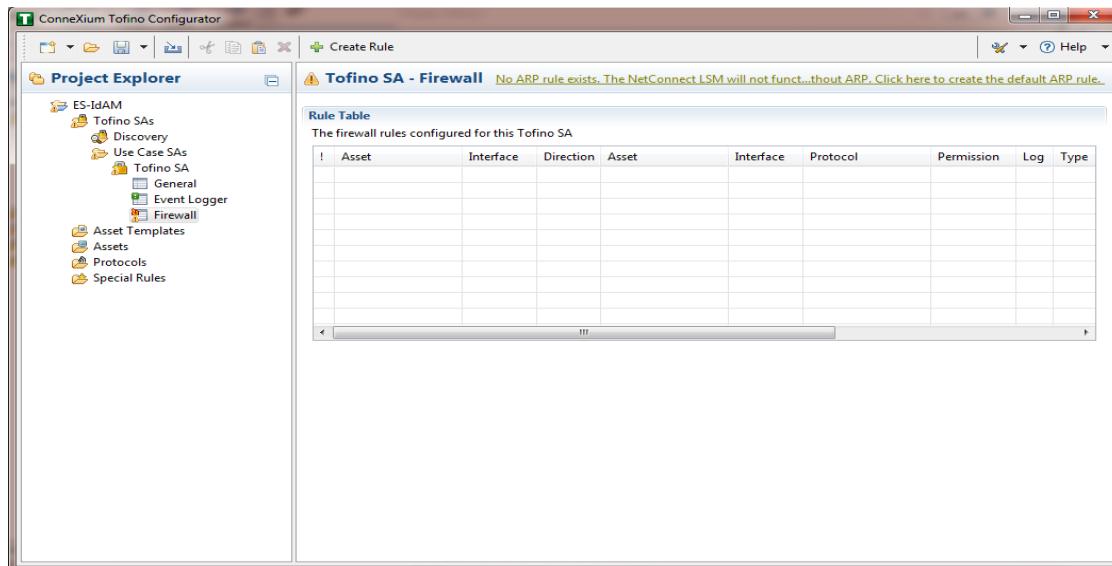


4302

Figure 197. Project Explorer Assets Icon

4303

4304 12. Under the Project Explorer frame, click the dropdown arrow next to 'Tofino SAs', then
4305 choose the SA created earlier, Figure 198. From there, click on 'Firewall' in the Project
4306 Explorer frame to display current firewall rules. This should be empty currently.



4307

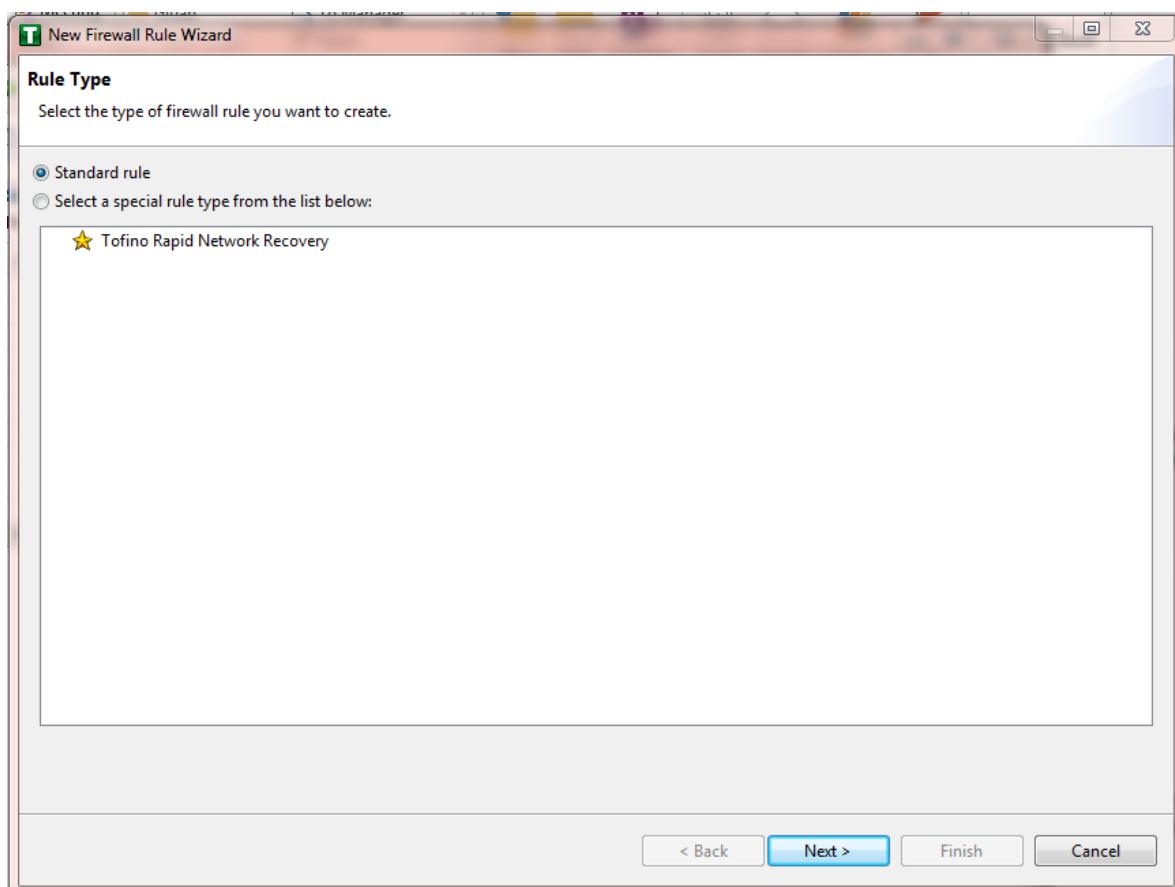
4308

Figure 198. Project Explorer Tofino SA Icon

4309

4310

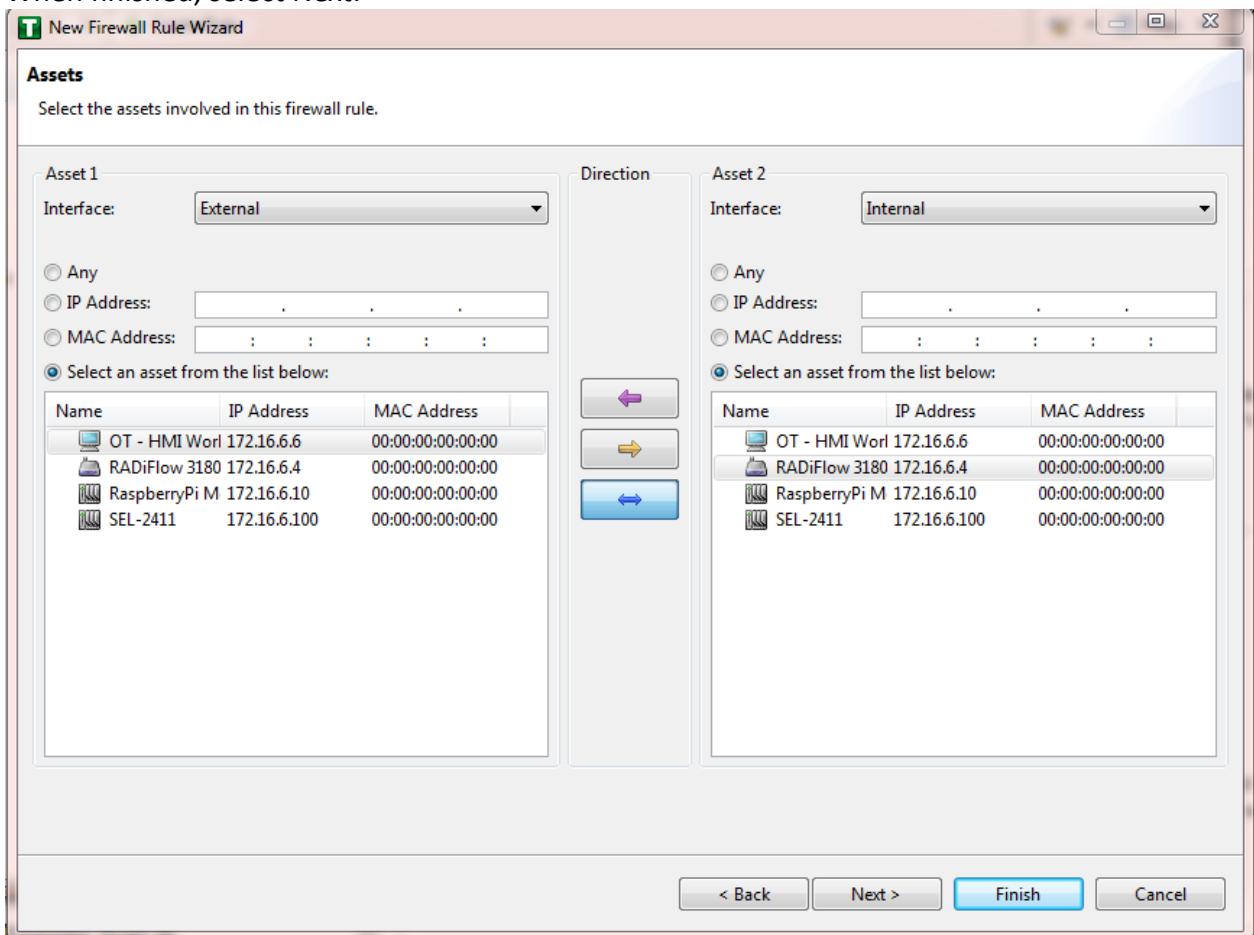
4311 13. To create the first rule, click on the '+ Create Rule' button above the Tofino SA-Firewall
 4312 title, Figure 198, above. Then ensure the 'Standard rule' radio button is selected and
 4313 click 'Next', Figure 199.



4314

Figure 199. Rule Type

4315 14. On the next screen, Figure 200, there are a few options to determine. First is Asset 1, you
 4316 must choose the interface. This will be where the traffic is coming from into the device.
 4317 In the Lab Build, Asset 1 is the OT Workstation, which is connected to a network that is
 4318 connect to the External interface on the firewall. Select the 'Select an asset from the list
 4319 below' radio button for both Asset 1 and Asset 2, and select the systems to create a rule
 4320 between. Also, select the direction of the traffic using the arrow buttons in the middle.
 4321 When finished, select Next.

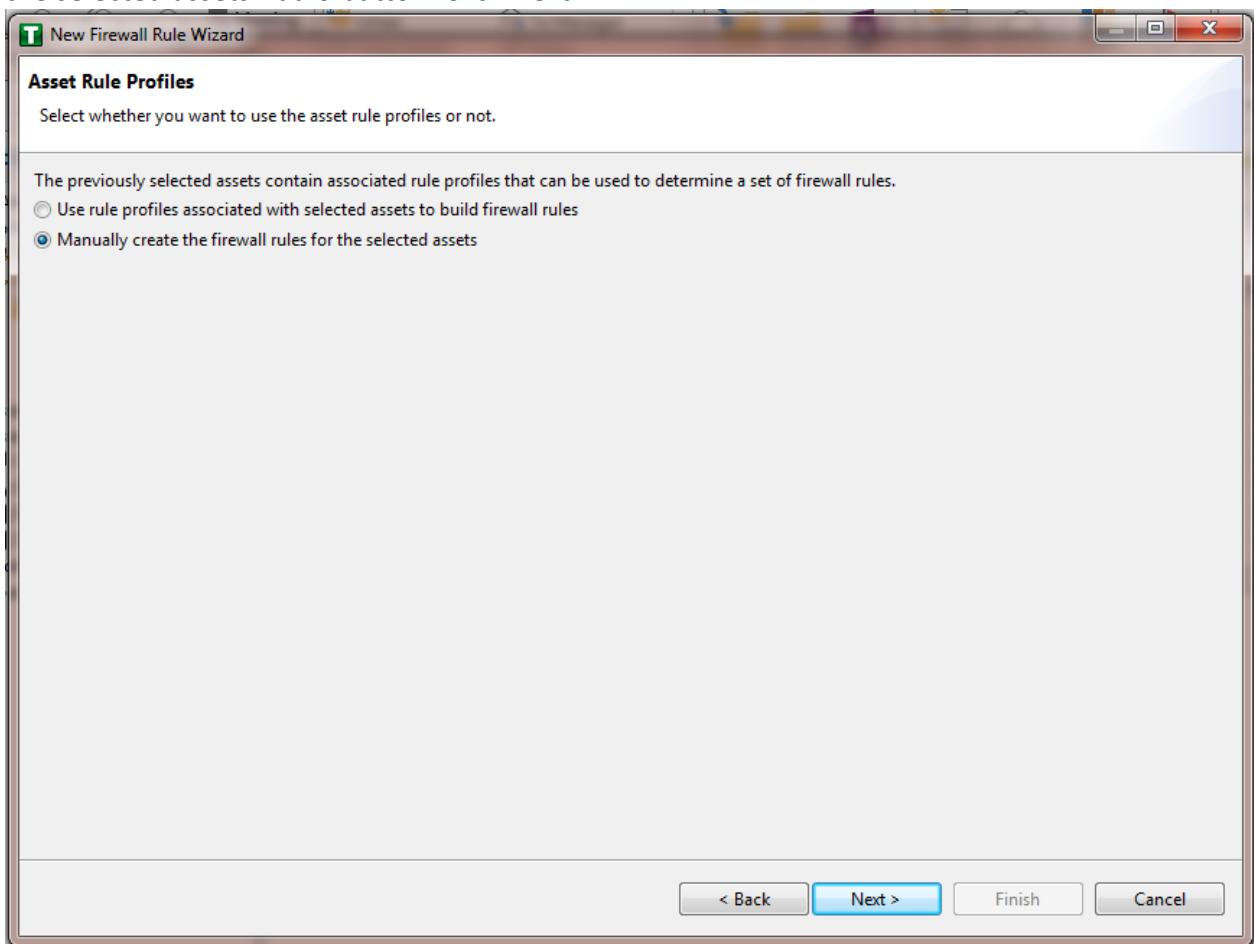


4322

4323

Figure 200. Firewall Rule Wizard

4324 15. On the Asset Rule Profiles, Figure 201, select the 'Manually create the firewall rules for
4325 the selected assets' radio button. Click Next.



4326

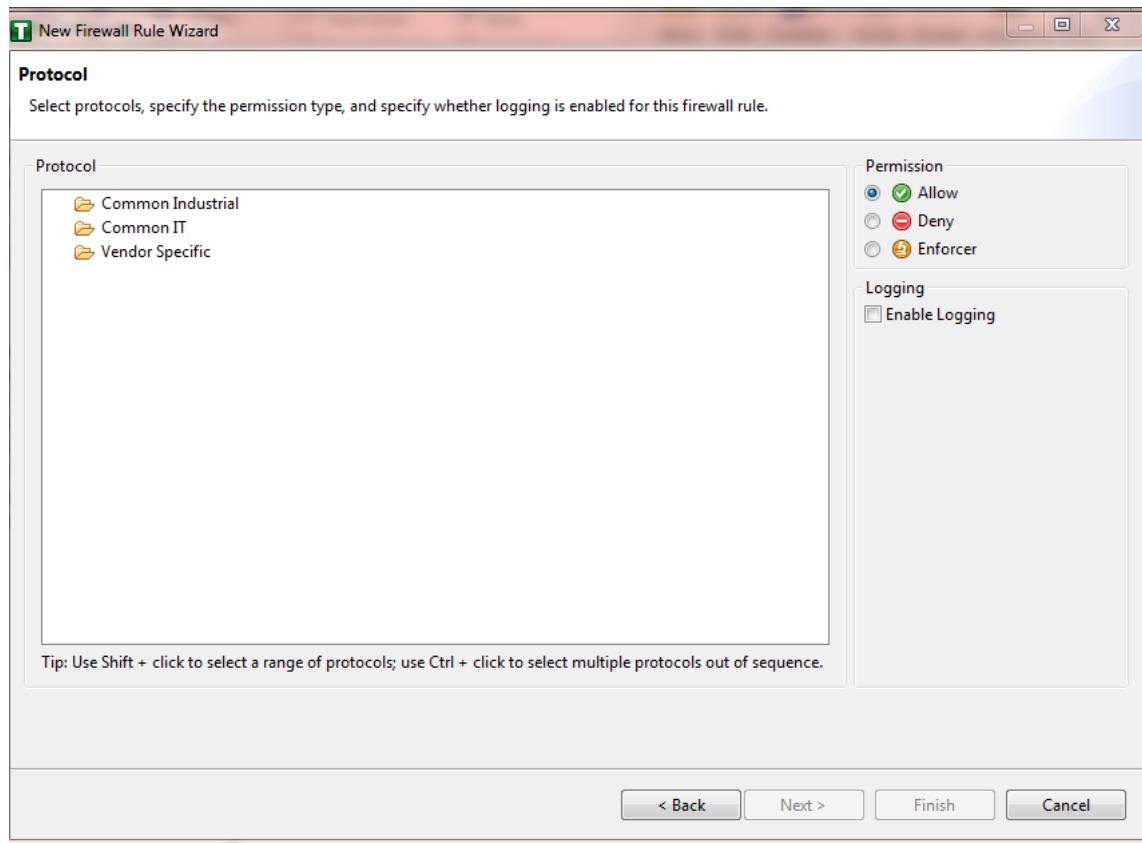
4327

Figure 201. Asset Rule Profiles

4328 16. On the Protocol screen, Figure 202, choose the protocol to be checked against. There are
4329 drop down menus for 'Common Industrial', 'Common IT', and 'Vendor Specific.' For this
4330 example, we are choosing SSH and Telnet (by holding the CTRL key, you can select
4331 multiple protocols). Then choose the Permission on the right side of the screen, as well
4332 as whether to log or not. Then click Finish.

4333
4334

Note: By default, any traffic that does not match the rules in the firewall will automatically be denied.

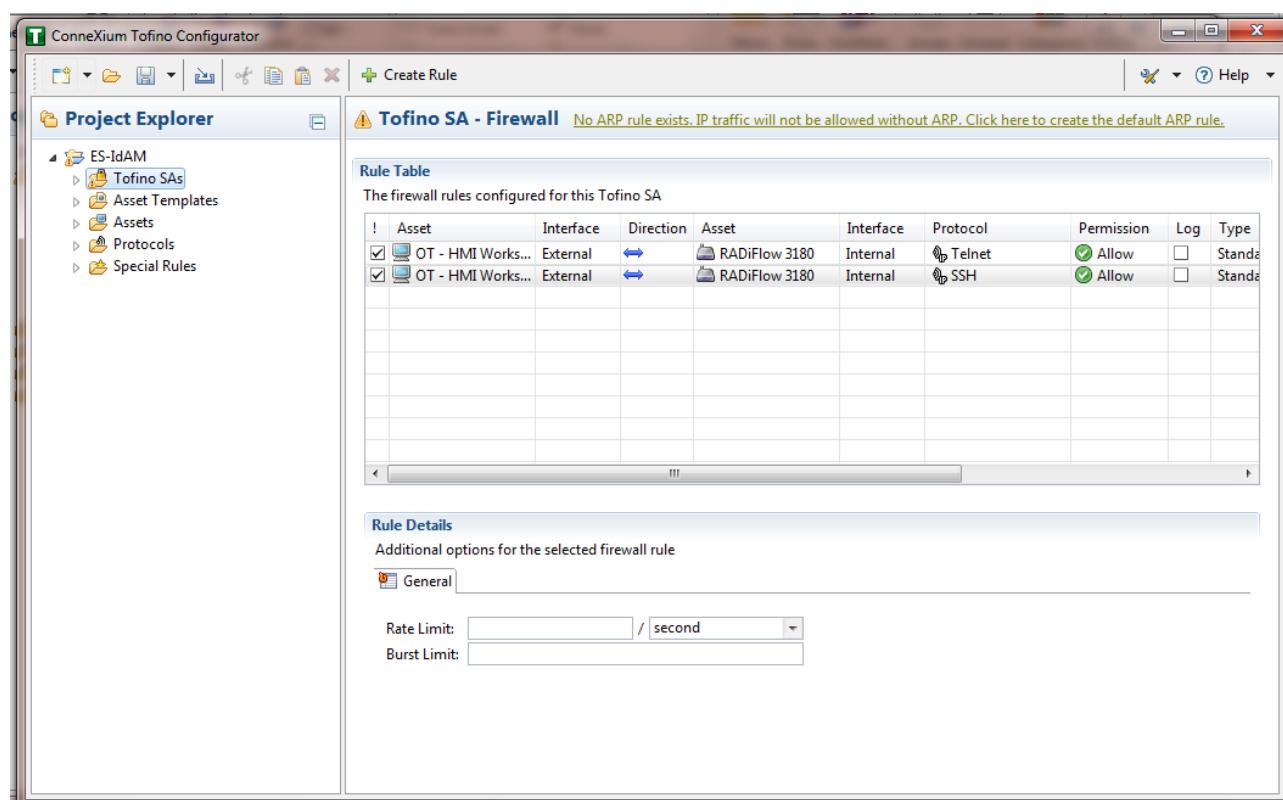


4335

Figure 202. Protocol Window

4336

17. After that is completed, the firewall rule should be listed in the Rule Table, Figure 203.



4337

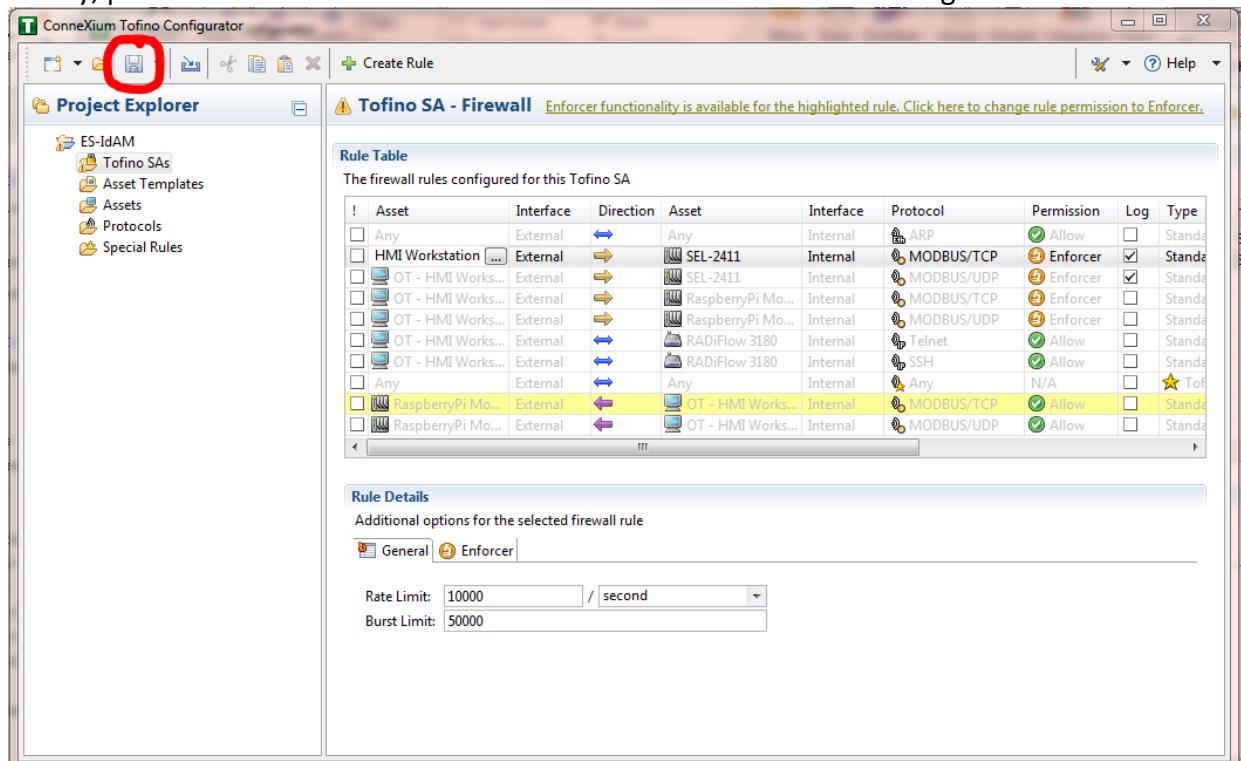
Figure 203. Rule Table

4338

18. Repeat steps 13 through 17 for the remainder of the rules needed.

4339

19. Finally, press the save button on the menu bar. Circled in red below in Figure 204.

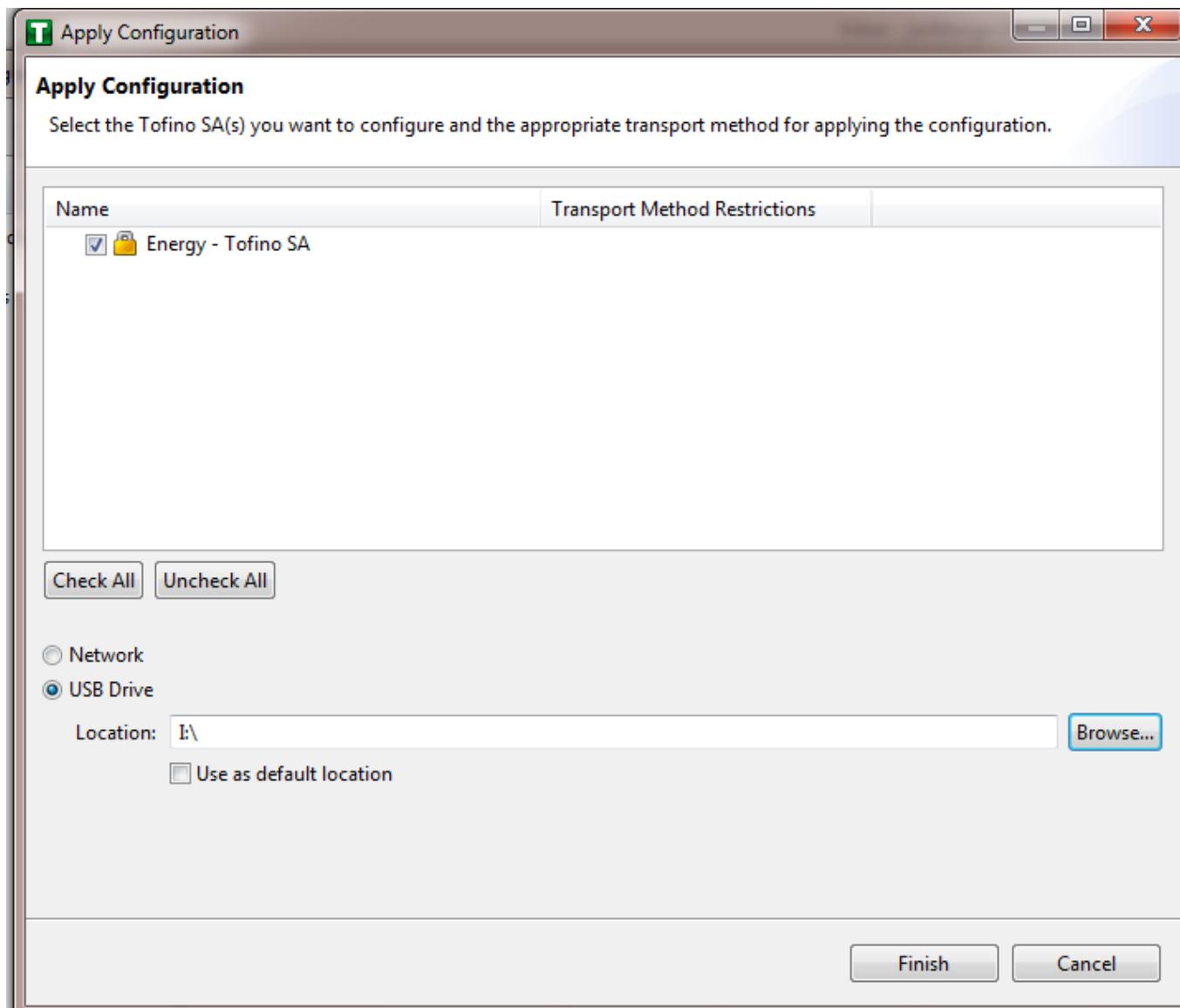


4340

Figure 204. Save rules in Project Explorer

4341

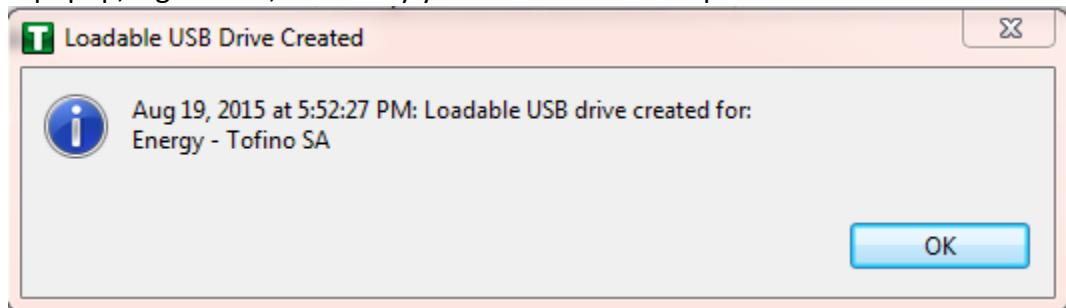
20. Place a FAT/FAT32 formatted USB device into the computer running the ConneXium Tofino Configurator, then right click 'Tofino SAs' in the Project Explorer pane and select 'Apply.' If the project asks you to save, press 'OK'.



4345 21. In the Apply Configuration pane, Figure 205, ensure that your SA is selected in the table
 4346 at the top, and the 'USB Drive' radio button is selected. Then browse to the top-level
 4347 directory of your USB drive. Then click Finish.

4348 *Figure 205. Apply Configuration Pane*

4349 22. A popup, Figure 206, will notify you of successful completion.



4350

4351 *Figure 206. Loadable USB Drive Popup*

4352 23. Ensure the firewall has been powered on and has been running for at least one minute,
4353 then plug the USB device used to copy the Tofino configuration to into the USB port on
4354 the back of the firewall.

4355 24. Press the Save/Load/Reset button twice, setting it to the Load setting (Pressing once
4356 should turn the indicator light to green, pressing it again will change it from green to
4357 amber). After a few seconds, the device will begin displaying lights that move from right
4358 to left across the LEDs on the back, indicating the configuration is being loaded.

4359 25. Once the lights stop moving right to left, wait a few seconds, and ensure the Fault LED
4360 does not light up. Then remove the USB drive and place it back into the computer
4361 running the ConneXium Tofino Configurator software.

4362 26. Right click 'Tofino SAs' in the Project Explorer pane and select 'Verify'.

4363 27. At the Verify Loaded Configuration window, select the Tofino SA in the table, and select
4364 the 'USB Drive' radio button. Then select the USB drive using the Browse button. Finally,
4365 press Finish.

4366 28. A popup will notify you of successful verification, and configuration is complete.

4367

4368 **17 OPERATING SYSTEM STIG COMPLIANCE REPORTS**

4369 STIG compliance reports were generated for the STIG-compliant OS installations that were used
4370 in the build. The reports for each installation are provided in the following subsections. Neither
4371 the Windows 7 Console on the IT network nor the OT Management Windows 7 Workstation on
4372 the OT network were STIG-compliant installations, so compliance reports for those OSs are not
4373 provided.

4374 The Linux implementations (except SUSE Linux) were configured to meet the DoD CentOS 6
4375 STIG, because no CentOS 7 STIG was available at the time the build was implemented. The STIG
4376 guidelines are available on-line at <http://iase.disa.mil/stigs/os/Pages/index.aspx>. The OS
4377 configurations for each Linux implementation are listed below. The compliance results reports
4378 identify the configuration items that do not conform to the STIG configuration guide.

4379 Compliance reports are provided for the following OSs:

4380

- SQL Server on IdAM Network STIG Compliance Report
- RSA IMG SUSE Linux Server STIG Compliance Report
- RSA Adaptive Directory Centos 7 Server STIG Compliance Report
- AlertEnterprise Microsoft Server STIG Compliance Report
- IT Domain Controller STIG Compliance Report

4385 • IT Windows 7 Workstations STIG Compliance Report
 4386 • Ozone Authority and Ozone Server Centos 6 Server STIG Compliance Report
 4387 • Ozone Envoy Centos 6 Server STIG Compliance Report
 4388 • OT Domain Controller STIG Compliance Report
 4389 • OT ConsoleWorks Windows Server 2012 STIG Compliance Report
 4390 • OT Windows 7 Workstations STIG Compliance Report
 4391 • PACS Domain Controller STIG Compliance Report
 4392 • PACS Console Windows Server 2012 STIG Compliance Report
 4393 • Baseline CentOS 7 Linux Configuration
 4394

4395 **17.1 SQL SERVER ON IDAM NETWORK STIG COMPLIANCE REPORT**

Status	STIG ID	Rule ID	Vuln ID	Severity	Rule Title
N/A	SQL2-00-000300	SV-53912r1_rule	V-41389	CAT II	SQL Server must maintain and support organization-defined security labels on stored information.
N/A	SQL2-00-000400	SV-53914r1_rule	V-41391	CAT II	SQL Server must maintain and support organization-defined security labels on information in process.
N/A	SQL2-00-000500	SV-53916r1_rule	V-41392	CAT II	SQL Server must maintain and support organization-defined security labels on data in transmission.
N/A	SQL2-00-000900	SV-53917r1_rule	V-41393	CAT II	SQL Server must allow authorized users to associate security labels to information in the database.
N/A	SQL2-00-00920	SV-53920r1_rule	V-41395	CAT II	SQL Server must be protected from unauthorized access by developers.
N/A	SQL2-00-009300	SV-53921r1_rule	V-41396	CAT II	SQL Server must be protected from unauthorized access by developers on shared production/development host systems.
PASS	SQL2-00-00950	SV-53922r2_rule	V-41397	CAT II	Administrative privileges, built-in server roles and built-in database roles must be assigned to the DBMS login accounts that require them via custom roles, and not directly.
PASS	SQL2-00-011050	SV-53918r2_rule	V-41394	CAT II	SQL Server utilizing Discretionary Access Control (DAC) must enforce a policy that limits propagation of access rights.
UNKNOWN	SQL2-00-011200	SV-53928r2_rule	V-41402	CAT II	SQL Server must provide audit record generation capability for organization-defined auditable events within the database.

What is
considered
auditable?

4396

4397 **17.2 RSA IMG SUSE LINUX SERVER STIG COMPLIANCE REPORT**

4398 OpenSCAP Evaluation Report

4399 17.2.1 Evaluation Characteristics

Target machine dvd-acm

Benchmark URL U_RedHat_6_V1R6_STIG_SCAP_1-1_Benchmark-xccdf.xml

Performed by root

4400 17.2.2 Compliance and Scoring

4401 The target system did not satisfy the conditions of 107 rules! Furthermore, the results of 12 rules
4402 were inconclusive. Please review rule results and consider applying remediation.

4403 17.2.3 Rule Results

4404 60 passed
4405 107 failed
4406 12 other

4407 17.2.4 Severity of Failed Rules

4408 0 other
4409 53 low
4410 53 medium
4411 1 high

4412 17.2.5 Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	33.519554	100.000000	33.52%

4413 Search

Title	Severity	Result
Red Hat Enterprise Linux 6 Security Technical Implementation Guide	107x fail	12x error
SRG-OS-999999 1x error		
Automated file system mounting tools must not be enabled unless needed.	low	error
SRG-OS-000062 1x fail		
Auditing must be enabled at boot by setting a kernel parameter.	low	fail
SRG-OS-999999 1x fail		
The /etc/gshadow file must be owned by root.	medium	fail
SRG-OS-999999 1x fail		
The /etc/gshadow file must be group-owned by root.	medium	fail
SRG-OS-999999 1x fail		
The /etc/gshadow file must have mode 0000.	medium	fail
SRG-OS-999999 1x fail		
The system must use a separate file system for /tmp.	low	fail
SRG-OS-999999 1x fail		
The system must use a separate file system for /var.	low	fail
SRG-OS-999999 1x fail		
The system must use a separate file system for /var/log.	low	fail
SRG-OS-000259 1x fail		
Library files must be owned by root.	medium	fail
SRG-OS-000044 1x fail		
The system must use a separate file system for the system audit data path.	low	fail
SRG-OS-000045 1x fail		
The audit system must alert designated staff members when the audit storage volume approaches capacity.	medium	fail
SRG-OS-000259 1x fail		
All system command files must be owned by root.	medium	fail
SRG-OS-999999 1x fail		
The system must use a separate file system for user	low	fail

Title	Severity	Result
home directories.		
SRG-OS-000078 1x fail		
The system must require passwords to contain a minimum of 14 characters.	medium	fail
SRG-OS-000075 1x fail		
Users must not be able to change passwords more than once every 24 hours.	medium	fail
SRG-OS-000076 1x fail		
User passwords must be changed at least every 60 days.	medium	fail
SRG-OS-000071 1x fail		
The system must require passwords to contain at least one numeric character.	low	fail
SRG-OS-000103 1x fail		
The system package management tool must cryptographically verify the authenticity of system software packages during installation.	medium	fail
SRG-OS-000232 1x fail		
A file integrity tool must be installed.	medium	fail
SRG-OS-000273 1x fail		
The operating system must enforce requirements for the connection of mobile devices to operating systems.	medium	fail
SRG-OS-000248 1x fail		
There must be no .rhosts or hosts.equiv files on the system.	high	fail
SRG-OS-000249 1x fail		
The system must disable accounts after excessive login failures within a 15-minute interval.	medium	fail
SRG-OS-999999 1x fail		
The /etc/shadow file must be group-owned by root.	medium	fail
SRG-OS-999999 1x fail		
The /etc/shadow file must have mode 0000.	medium	fail
SRG-OS-999999 1x fail		
IP forwarding for IPv4 must not be enabled, unless the system is a router.	medium	fail
SRG-OS-000146 1x error		
The operating system must prevent public IPv4 access into an organizations internal networks, except as appropriately mediated by managed interfaces employing boundary protection devices.	medium	error
SRG-OS-000231 1x fail		
The systems local IPv4 firewall must implement a deny-all, allow-by-exception policy for inbound packets.	medium	fail
SRG-OS-000096 1x fail		
The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.	medium	fail
SRG-OS-000096 1x fail		
The Stream Control Transmission Protocol (SCTP) must be disabled unless required.	medium	fail
SRG-OS-000096 1x fail		
The Reliable Datagram Sockets (RDS) protocol must be disabled unless required.	low	fail
SRG-OS-000096 1x fail		
The Transparent Inter-Process Communication (TIPC) protocol must be disabled unless required.	medium	fail
SRG-OS-000215 1x fail		

Title	Severity	Result
The operating system must back up audit records on an organization defined frequency onto a different system or media than the system being audited.	medium	fail
SRG-OS-000043 1x fail		
The operating system must support the requirement to centrally manage the content of audit records generated by organization defined information system components.	medium	fail
SRG-OS-000062 1x fail		
The audit system must be configured to audit all attempts to alter system time through settimeofday.	low	fail
SRG-OS-999999 1x fail		
The system must not accept IPv4 source-routed packets on any interface.	medium	fail
SRG-OS-999999 1x fail		
The system must not accept ICMPv4 redirect packets on any interface.	medium	fail
SRG-OS-999999 1x fail		
The system must not accept ICMPv4 secure redirect packets on any interface.	medium	fail
SRG-OS-000062 1x fail		
The audit system must be configured to audit all attempts to alter system time through clock_settime.	low	fail
SRG-OS-999999 1x fail		
The system must log Martian packets.	low	fail
SRG-OS-999999 1x fail		
The system must not accept IPv4 source-routed packets by default.	medium	fail
SRG-OS-000062 1x fail		
The audit system must be configured to audit all attempts to alter system time through /etc/localtime.	low	fail
SRG-OS-000004 1x fail		
The operating system must automatically audit account creation.	low	fail
SRG-OS-999999 1x fail		
The system must not accept ICMPv4 secure redirect packets by default.	medium	fail
SRG-OS-999999 1x fail		
The system must ignore ICMPv4 redirect messages by default.	low	fail
SRG-OS-000239 1x fail		
The operating system must automatically audit account modification.	low	fail
SRG-OS-999999		
The system must not respond to ICMPv4 sent to a broadcast address.	low	pass
SRG-OS-000240 1x fail		
The operating system must automatically audit account disabling actions.	low	fail
SRG-OS-999999 1x fail		
The system must ignore ICMPv4 bogus error responses.	low	fail
SRG-OS-000241 1x fail		
The operating system must automatically audit account termination.	low	fail
SRG-OS-000142 1x fail		
The system must be configured to use TCP syncookies.	medium	fail

Title	Severity	Result
SRG-OS-999999 1x fail	low	fail
<u>The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using chmod.</u>		
SRG-OS-999999 1x fail	medium	fail
<u>The system must use a reverse-path filter for IPv4 network traffic when possible by default.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using chown.</u>		
SRG-OS-999999 1x fail	medium	fail
<u>The IPv6 protocol handler must not be bound to the network stack unless needed.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using fchmod.</u>		
SRG-OS-999999 1x fail	medium	fail
<u>The system must ignore ICMPv6 redirects by default.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using fchmodat.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using fchown.</u>		
SRG-OS-000064 1x fail	low	fail
SRG-OS-000152 1x error	medium	error
<u>The system must employ a local IPv4 firewall.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using fremovexattr.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using fsetxattr.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using lchown.</u>		
SRG-OS-000064 1x fail	low	fail
<u>The audit system must be configured to audit all discretionary access control permission modifications using iremovexattr.</u>		
SRG-OS-000064 1x fail	low	fail

Title	Severity	Result
The audit system must be configured to audit all discretionary access control permission modifications using <code>isetxattr</code>.	low	fail
SRG-OS-000064 1x fail		
The audit system must be configured to audit all discretionary access control permission modifications using <code>removexattr</code>.	low	fail
SRG-OS-000064 1x fail		
The audit system must be configured to audit all discretionary access control permission modifications using <code>setxattr</code>.	low	fail
SRG-OS-000064 1x fail		
The audit system must be configured to audit successful file system mounts.	low	fail
SRG-OS-000069 1x fail		
The system must require passwords to contain at least one uppercase alphabetic character.	low	fail
SRG-OS-000266 1x fail		
The system must require passwords to contain at least one special character.	low	fail
SRG-OS-000070 1x fail		
The system must require passwords to contain at least one lowercase alphabetic character.	low	fail
SRG-OS-000072 1x fail		
The system must require at least four characters be changed between the old and new passwords during a password change.	low	fail
SRG-OS-000021 1x fail		
The system must disable accounts after three consecutive unsuccessful logon attempts.	medium	fail
SRG-OS-000120 1x fail		
The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (system-auth).	medium	fail
SRG-OS-000064 1x fail		
The audit system must be configured to audit user deletions of files and programs.	low	fail
SRG-OS-000120 1x fail		
The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (login.defs).	medium	fail
SRG-OS-000120 1x fail		
The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (libuser.conf).	medium	fail
SRG-OS-000064 1x fail		
The audit system must be configured to audit changes to the <code>/etc/sudoers</code> file.	low	fail
SRG-OS-999999 1x fail		
The system boot loader configuration file(s) must be owned by root.	medium	fail
SRG-OS-000064 1x fail		
The audit system must be configured to audit the loading and unloading of dynamic kernel modules.	medium	fail
SRG-OS-999999 1x fail		

Title	Severity	Result
The system boot loader configuration file(s) must be group-owned by root.	medium	fail
SRG-OS-000096 1x error		
The xinetd service must be disabled if no network services utilizing it are enabled.	medium	error
SRG-OS-999999 1x fail		
The system boot loader configuration file(s) must have mode 0600 or less permissive.	medium	fail
SRG-OS-000096 1x fail		
The xinetd service must be uninstalled if no network services utilizing it are enabled.	low	fail
SRG-OS-000080 1x fail		
The system boot loader must require authentication.	medium	fail
SRG-OS-000080 1x fail		
The system must require authentication upon booting into single-user and maintenance modes.	medium	fail
SRG-OS-000080 1x fail		
The system must not permit interactive boot.	medium	fail
SRG-OS-000022 1x fail		
The system must require administrator action to unlock an account locked by excessive failed login attempts.	medium	fail
SRG-OS-999999 1x fail		
The system must not send ICMPv4 redirects by default.	medium	fail
SRG-OS-999999 1x fail		
The system must not send ICMPv4 redirects from any interface.	medium	fail
SRG-OS-000096 1x error		
The yppbind service must not be running.	medium	error
SRG-OS-999999 1x fail		
The cron service must be running.	medium	fail
SRG-OS-999999 1x error		
The avahi service must be disabled.	low	error
SRG-OS-000056 1x error		
The system clock must be synchronized continuously, or at least daily.	medium	error
SRG-OS-999999 1x fail		
The system must set a maximum audit log file size.	medium	fail
SRG-OS-000062 1x fail		
The audit system must be configured to audit all attempts to alter system time through adjtimex.	low	fail
SRG-OS-999999 1x fail		
The system must retain enough rotated audit logs to cover the required log retention period.	medium	fail
SRG-OS-000096 1x error		
The atd service must be disabled.	low	error
SRG-OS-999999 1x fail		
The system default umask for daemons must be 027 or 022.	low	fail
SRG-OS-999999 1x fail		
The system default umask in /etc/login.defs must be 077.	low	fail
SRG-OS-999999 1x fail		
The system default umask in /etc/profile must be 077.	low	fail
SRG-OS-999999 1x fail		
The system default umask for the csh shell must be 077.	low	fail
SRG-OS-000096 1x error		

Title	Severity	Result
The rdisc service must not be running.	low	error
SRG-OS-999999 1x fail		
The system default umask for the bash shell must be 077.	low	fail
SRG-OS-999999 1x error		
The postfix service must be enabled for mail delivery.	low	error
SRG-OS-000096 1x error		
The netconsole service must be disabled unless required.	low	error
SRG-OS-000248 1x fail		
X Windows must not be enabled unless required.	medium	fail
SRG-OS-999999 1x fail		
Process core dumps must be disabled unless needed.	low	fail
SRG-OS-000027 1x fail		
The system must limit users to 10 simultaneous system logins, or a site-defined number, in accordance with operational requirements.	low	fail
SRG-OS-000160 1x fail		
The system must provide VPN connectivity for communications over untrusted networks.	low	fail
SRG-OS-000024 1x fail		
A login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.	medium	fail
SRG-OS-000034 1x error		
The Bluetooth service must be disabled.	medium	error
GEN006660 1x fail		
Accounts must be locked upon 35 days of inactivity.	low	fail
SRG-OS-000118 1x fail		
The operating system must manage information system identifiers for users and devices by disabling the user identifier after an organization defined time period of inactivity.	low	fail
SRG-OS-999999 1x fail		
All public directories must be owned by a system account.	low	fail
SRG-OS-999999 1x fail		
The system must use a Linux Security Module configured to enforce limits on system services.	medium	fail
SRG-OS-999999 1x fail		
The system must use a Linux Security Module configured to limit the privileges of system services.	low	fail
SRG-OS-999999 1x fail		
The operating system, upon successful logon/access, must display to the user the number of unsuccessful logon/access attempts since the last successful logon/access.	medium	fail
SRG-OS-999999 1x fail		
The audit system must switch the system to single-user mode when available audit storage volume becomes dangerously low.	medium	fail

4414

4415 17.3 RSA ADAPTIVE DIRECTORY CENTOS 7 SERVER STIG COMPLIANCE REPORT

4416 XCCDF Test Result

4417 Introduction

4418 Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_default-profile	(Default profile)	2015-04-08 08:16	2015-04-08 08:17	embedded	1

4419 Target info

Targets	Addresses	Platforms
<ul style="list-style-type: none"> adaptivedir 	<ul style="list-style-type: none"> 127.0.0.1 172.16.4.3 0:0:0:0:0:0:1 fe80:0:0:0:250:56ff:fe89:8965 	<ul style="list-style-type: none"> cpe:/o:redhat:enterprise_linux:6

4420 Score

system	score	max	%	bar
urn:xccdf:scoring:default	96.65	100.00	96.65%	

4421 17.3.1 Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
173	0	6	0	0	0	0	0	0	179
Title									
Auditing must be enabled at boot by setting a kernel parameter.									
The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).									
The system boot loader configuration file(s) must be owned by root.									
The system boot loader configuration file(s) must be group-owned by root.									
The system boot loader configuration file(s) must have mode 0600 or less permissive.									
The system boot loader must require authentication.									
Result									
fail									
fail									
fail									
fail									
fail									
fail									

4423

4424 17.4 ALERT ENTERPRISE MICROSOFT SERVER STIG COMPLIANCE REPORT

4425 Non-Compliance Report - U_Windows_2008_R2_MS_V1R15_STIG_SCAP_1-0_Benchmark

4426 SCAP Compliance Checker - 3.1.2

4427 Score | System Information | Stream Information | Results | Detailed Results

4428 Score

30.04%

Adjusted Score: 30.04%
 Original Score: 30.04%
 Compliance Status: RED

4429

Pass: 79 Not Applicable: 0
 Fail: 184 Not Checked: 0
 Error: 0 Not Selected: 0

BLUE: Score equals 100
 GREEN: Score is greater than or equal to 90
 YELLOW: Score is greater than or equal to 80

Unknown: 0 Total: 263 RED: Score is greater than or equal to 0

4430 System Information

Target:	WIN-IPERGL2ELUD
Operating System:	Windows Server 2008 R2 Standard
OS Service Pack:	

4431 Results

- 4432 **Unsupported Service Packs**
 - 4433 ○ Systems must be at supported service pack (SP) or release levels. - Fail
- 4434 **Legal Notice Display**
 - 4435 ○ The required legal notice will be configured to display before console logon. - (CCE-10673-2) - Fail
- 4436 **Caching of logon credentials**
 - 4437 ○ Caching of logon credentials will be limited. - (CCE-10926-4) - Fail
- 4438 **Anonymous shares are not restricted**
 - 4439 ○ Anonymous enumeration of shares will be restricted. - (CCE-10557-7) - Fail
- 4440 **Bad Logon Attempts**
 - 4441 ○ The number of allowed bad-logon attempts will meet minimum requirements. - (CCE-11046-0) - Fail
- 4442 **Bad Logon Counter Reset**
 - 4443 ○ The time before the bad-logon counter is reset will meet minimum requirements. - (CCE-11059-3) - Fail
- 4444 **Lockout Duration**
 - 4445 ○ The lockout duration will meet minimum requirements. - (CCE-10399-4) - Fail
- 4446 **Rename Built-in Guest Account**
 - 4447 ○ The built-in guest account will be renamed. - (CCE-10747-4) - Fail
- 4448 **Rename Built-in Administrator Account**
 - 4449 ○ The built-in administrator account will be renamed. - (CCE-10976-9) - Fail
- 4450 **LanMan Authentication Level**
 - 4451 ○ The LanMan authentication level will be set to Send NTLMv2 response only\refuse LM & NTLM. - (CCE-10984-3) - Fail
- 4453 **Deny Access from the Network**
 - 4454 ○ The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-10733-4) - Fail
- 4457 **Smart Card Removal Option**
 - 4458 ○ The Smart Card removal option will be configured to Force Logoff or Lock Workstation. - (CCE-10573-4) - Fail
- 4459 **Format and Eject Removable Media**
 - 4460 ○ Ejection of removable NTFS media is not restricted to Administrators. - (CCE-10637-7) - Fail
- 4461 **Password Expiration Warning**
 - 4462 ○ Users will be warned in advance that their passwords will expire. - (CCE-10930-6) - Fail
- 4463 **Disable Media Autoplay**
 - 4464 ○ Autoplay will be disabled for all drives. - (CCE-11126-0) - Fail
- 4465 **Anonymous Access to Named Pipes**
 - 4466 ○ Named pipes that can be accessed anonymously will be configured to contain no values. - (CCE-10944-7) - Fail
- 4467 **Remote Assistance - Solicit Remote Assistance**
 - 4468 ○ Solicited Remote Assistance will not be allowed. - (CCE-11723-4) - Fail
- 4469 **Undock Without Logging On**
 - 4470 ○ A system must be logged on to before removing from a docking station. - (CCE-10883-7) - Fail
- 4471 **Storage of Passwords and Credentials**
 - 4472 ○ The system will be configured to prevent the storage of passwords and credentials - (CCE-10292-1) - Fail
- 4473 **Force Logoff When Logon Hours Expire**
 - 4474 ○ The system will be configured to force users to log off when their allowed logon hours expire. - (CCE-10588-2) - Fail

- 4476 ● **Session Security for NTLM SSP Based Clients**
 - 4477 ○ The system will be configured to meet the minimum session security requirement for NTLM SSP based clients. - (CCE-10035-4) - Fail
- 4478 ● **FIPS Compliant Algorithms**
 - 4479 ○ The system will be configured to use FIPS-compliant algorithms for encryption, hashing, and signing. - (CCE-10789-6) - Fail
- 4480 ● **TS/RDS - Session Limit**
 - 4481 ○ Remote Desktop Services will limit users to one remote session. - (CCE-12016-2) - Fail
- 4482 ● **TS/RDS - Password Prompting**
 - 4483 ○ Remote Desktop Services will always prompt a client for passwords upon connection. - (CCE-11299-5) - Fail
- 4484 ● **TS/RDS - Set Encryption Level**
 - 4485 ○ Remote Desktop Services will be configured with the client connection encryption set to the required level. - (CCE-11677-2) - Fail
- 4486 ● **TS/RDS - Do Not Use Temp Folders**
 - 4487 ○ Remote Desktop Services will be configured to use session-specific temporary folders. - (CCE-10669-0) - Fail
- 4488 ● **TS/RDS - Delete Temp Folders**
 - 4489 ○ Remote Desktop Services will delete temporary folders when a session is terminated. - (CCE-12046-9) - Fail
- 4490 ● **TS/RDS - Time Limit for Disc. Session**
 - 4491 ○ Remote Desktop Services will be configured to set a time limit for disconnected sessions. - (CCE-11117-9) - Fail
- 4492 ● **TS/RDS - Time Limit for Idle Session**
 - 4493 ○ Remote Desktop Services will be configured to disconnect an idle session after the specified time period. - (CCE-11506-3) - Fail
- 4494 ● **Remote Assistance - Offer Remote Assistance**
 - 4495 ○ The system will be configured to prevent unsolicited remote assistance offers. - (CCE-11625-1) - Fail
- 4496 ● **Error Reporting - Report Errors**
 - 4497 ○ The system will be configured to prevent automatic forwarding of error information. - (CCE-11750-7) - Fail
- 4498 ● **Safe DLL Search Mode**
 - 4499 ○ The system will be configured to use Safe DLL Search Mode. - (CCE-10772-2) - Fail
- 4500 ● **Media Player - Disable Automatic Updates**
 - 4501 ○ Media Player must be configured to prevent automatic checking for updates. - (CCE-11298-7) - Fail
- 4502 ● **Session Security for NTLM SSP based Servers**
 - 4503 ○ The system will be configured to meet the minimum session security requirement for NTLM SSP based servers. - (CCE-10040-4) - Fail
- 4504 ● **Audit Log Warning Level**
 - 4505 ○ The system will generate an audit event when the audit log reaches a percent full threshold. - (CCE-11011-4) - Fail
- 4506 ● **Disable IP Source Routing**
 - 4507 ○ The system will be configured to prevent IP source routing. - (CCE-10732-6) - Fail
- 4508 ● **Disable ICMP Redirect**
 - 4509 ○ The system will be configured to prevent ICMP redirects from overriding OSPF generated routes. - (CCE-10518-9) - Fail
- 4510 ● **Disable Router Discovery**
 - 4511 ○ The system will be configured to disable the Internet Router Discover Protocol (IRDP). - (CCE-10768-0) - Fail
- 4512 ● **TCP Connection Keep-Alive Time**
 - 4513 ○ The system will be configured to limit how often keep-alive packets are sent. - (CCE-10381-2) - Fail
- 4514 ● **Name-Release Attacks**
 - 4515 ○ The system will be configured to ignore NetBIOS name release requests except from WINS servers. - (CCE-10653-4) - Fail
- 4516 ● **TCP Data Retransmissions**
 - 4517 ○ The system will limit how many times unacknowledged TCP data is retransmitted. - (CCE-10941-3) - Fail
- 4518 ● **Screen Saver Grace Period**
 - 4519 ○ The system will be configured to have password protection take effect within a limited time frame when the screen saver becomes active. - (CCE-10019-8) - Fail
- 4520 ● **Remotely Accessible Registry Paths and Sub-Paths**
 - 4521 ○ Unauthorized remotely accessible registry paths and sub-paths will not be configured. - (CCE-10935-5) - Fail

- 4531 ● **Strong Key Protection**
 - 4532 ○ Users will be required to enter a password to access private keys. - (CCE-11035-3) - Fail
- 4533 ● **Optional Subsystems**
 - 4534 ○ Optional Subsystems will not be permitted to operate on the system. - (CCE-10913-2) - Fail
- 4535 ● **Software Restriction Policies**
 - 4536 ○ Software certificate restriction policies will be enforced. - (CCE-10900-9) - Fail
- 4537 ● **TS/RDS - Secure RPC Connection.**
 - 4538 ○ The Remote Desktop Session Host will require secure RPC communications. - (CCE-11368-8) - Fail
- 4539 ● **Group Policy - Registry Policy Processing**
 - 4540 ○ Group Policy objects will be reprocessed even if they have not changed. - (CCE-12754-8) - Fail
- 4541 ● **SMB Client Packet Signing (Always)**
 - 4542 ○ The Windows SMB client will be enabled to always perform SMB packet signing. - (CCE-10970-2) - Fail
- 4543 ● **Minimum Password Length**
 - 4544 ○ For systems utilizing a logon ID as the individual identifier, passwords will, at a minimum, be 14 characters. - (CCE-10372-1) - Fail
- 4545 ● **Display of Last User Name**
 - 4546 ○ The system will be configured to prevent the display of the last user name on the logon screen. - (CCE-10788-8) - Fail
- 4547 ● **Audit Policy Subcategory Setting**
 - 4548 ○ Audit policy using subcategories will be enabled. - (CCE-10112-1) - Fail
- 4549 ● **IPSec Exemptions**
 - 4550 ○ IPSec Exemptions will be limited. - (CCE-10018-0) - Fail
- 4551 ● **UAC - Admin Approval Mode**
 - 4552 ○ User Account Control approval mode for the built-in Administrator will be enabled. - (CCE-11028-8) - Fail
- 4553 ● **UAC - Admin Elevation Prompt**
 - 4554 ○ User Account Control will, at a minimum, prompt administrators for consent. - (CCE-11023-9) - Fail
- 4555 ● **UAC - User Elevation Prompt**
 - 4556 ○ User Account Control will automatically deny standard user requests for elevation. - (CCE-10807-6) - Fail
- 4557 ● **Enumerate Administrator Accounts on Elevation**
 - 4558 ○ The system will require username and password to elevate a running application. - (CCE-11450-4) - Fail
- 4559 ● **TS/RDS - Prevent Password Saving**
 - 4560 ○ Passwords will not be saved in the Remote Desktop Client. - (CCE-11905-7) - Fail
- 4561 ● **TS/RDS - Drive Redirection**
 - 4562 ○ Local drives will be prevented from sharing with Remote Desktop Session Hosts (Remote Desktop Services Role). - (CCE-11709-3) - Fail
- 4563 ● **RPC - Unauthenticated RPC Clients**
 - 4564 ○ Unauthenticated RPC clients will be restricted from connecting to the RPC server. - (CCE-10881-1) - Fail
- 4565 ● **RPC - Endpoint Mapper Authentication**
 - 4566 ○ Client computers will be required to authenticate for RPC communication. - (CCE-10715-1) - Fail
- 4567 ● **Internet Download / Online Ordering**
 - 4568 ○ Web publishing and online ordering wizards will be prevented from downloading a list of providers. - (CCE-11136-9) - Fail
- 4569 ● **Printing Over HTTP**
 - 4570 ○ Printing over HTTP will be prevented. - (CCE-11360-5) - Fail
- 4571 ● **HTTP Printer Drivers**
 - 4572 ○ Downloading print driver packages over HTTP will be prevented. - (CCE-11563-4) - Fail
- 4573 ● **Windows Update Device Drive Searching**
 - 4574 ○ Windows will be prevented from using Windows Update to search for drivers. - (CCE-10357-2) - Fail
- 4575 ● **IPv6 Transition**
 - 4576 ○ IPv6 will be disabled until a deliberate transition strategy has been implemented. - Fail
- 4577 ● **Windows Peer to Peer Networking**
 - 4578 ○ Windows Peer-to-Peer networking services will be turned off. - (CCE-11604-6) - Fail
- 4579 ● **Prohibit Network Bridge**
 - 4580 ○ Network Bridges will be prohibited in Windows. - (CCE-12074-1) - Fail
- 4581 ● **Root Certificates Update**

- 4586 ○ Root Certificates will not be updated automatically from the Microsoft site. - (CCE-11264-9) - Fail
- 4587 ● **Event Viewer Events.asp Links**
 - Event Viewer Events.asp links will be turned off. - (CCE-10693-0) - Fail
- 4588 ● **Internet File Association Service**
 - The Internet File Association service will be turned off. - (CCE-10697-1) - Fail
- 4589 ● **Order Prints Online**
 - The Order Prints Online wizard will be turned off. - (CCE-11243-3) - Fail
- 4590 ● **Classic Logon**
 - The classic logon screen will be required for user logons. - (CCE-11256-5) - Fail
- 4591 ● **RSS Attachment Downloads**
 - Attachments will be prevented from being downloaded from RSS feeds. - Fail
- 4592 ● **Windows Explorer – Shell Protocol Protected Mode**
 - Windows Explorer shell protocol will run in protected mode. - (CCE-11530-3) - Fail
- 4593 ● **Windows Installer – IE Security Prompt**
 - Users will be notified if a web-based program attempts to install software. - (CCE-10343-2) - Fail
- 4594 ● **Windows Installer – User Control**
 - Users will be prevented from changing installation options. - (CCE-10906-6) - Fail
- 4595 ● **Windows Installer – Vendor Signed Updates**
 - Non-administrators will be prevented from applying vendor signed updates. - (CCE-11468-6) - Fail
- 4596 ● **Media Player – First Use Dialog Boxes**
 - Users will not be presented with Privacy and Installation options on first use of Windows Media Player. - (CCE-11596-4) - Fail
- 4597 ● **Network – Mapper I/O Driver**
 - The Mapper I/O network protocol driver will be disabled. - (CCE-10484-4) - Fail
- 4598 ● **Network – Responder Driver**
 - The Responder network protocol driver will be disabled. - (CCE-11304-3) - Fail
- 4599 ● **Network – WCN Wireless Configuration**
 - The configuration of wireless devices using Windows Connect Now will be disabled. - (CCE-11242-5) - Fail
- 4600 ● **Network – Windows Connect Now Wizards**
 - The Windows Connect Now wizards will be disabled. - (CCE-11155-9) - Fail
- 4601 ● **Device Install – PnP Interface Remote Access**
 - Remote access to the Plug and Play interface will be disabled for device installation. - (CCE-11248-2) - Fail
- 4602 ● **Device Install – Drivers System Restore Point**
 - A system restore point will be created when a new device driver is installed. - (CCE-10546-0) - Fail
- 4603 ● **Device Install – Generic Driver Error Report**
 - An Error Report will not be sent when a generic device driver is installed. - (CCE-12274-7) - Fail
- 4604 ● **Driver Install – Device Driver Search Prompt**
 - Users will not be prompted to search Windows Update for device drivers. - (CCE-11319-1) - Fail
- 4605 ● **Handwriting Recognition Error Reporting**
 - Errors in handwriting recognition on Tablet PCs will not be reported to Microsoft. - (CCE-11030-4) - Fail
- 4606 ● **Power Mgmt – Password Wake on Battery**
 - Users will be prompted for a password on resume from sleep (on battery). (Applicable to Server 2008 R2 if the system is configured to sleep.) - (CCE-12088-1) - Fail
- 4607 ● **Power Mgmt – Password Wake When Plugged In**
 - The user will be prompted for a password on resume from sleep (Plugged In). (Applicable on Server 2008 R2 if the system is configured to sleep.) - (CCE-11651-7) - Fail
- 4608 ● **Remote Assistance – Session Logging**
 - Remote Assistance log files will be generated. - (CCE-11263-1) - Fail
- 4609 ● **Game Explorer Information Downloads**
 - Game explorer information will not be downloaded from Windows Metadata Services. - (CCE-11739-0) - Fail
- 4610 ● **Error Reporting – Logging**
 - Error Reporting events will be logged in the system event log. - (CCE-11621-0) - Fail
- 4611 ● **Error Reporting – Windows Error Reporting**
 - Windows Error Reporting to Microsoft will be disabled. - (CCE-11708-5) - Fail
- 4612 ● **Error Reporting – Additional Data**

- 4641 ○ Additional data requests in response to Error Reporting will be declined. - (CCE-11584-0) - Fail
- 4642 ● **Windows Explorer – Heap Termination**
 - 4643 ○ Windows Explorer heap termination on corruption will be disabled. - (CCE-10981-9) - Fail
- 4644 ● **Logon – Report Logon Server**
 - 4645 ○ Users will be notified if the logon server was inaccessible and cached credentials were used. - (CCE-12260-6) - Fail
- 4647 ● **Media DRM – Internet Access**
 - 4648 ○ Windows Media Digital Rights Management will be prevented from accessing the Internet. - (CCE-11052-8) - Fail
- 4649 ● **TS/RDS – COM Port Redirection**
 - 4650 ○ The system will be configured to prevent users from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role) - (CCE-10600-5) - Fail
- 4653 ● **TS/RDS – LPT Port Redirection**
 - 4654 ○ The system will be configured to prevent users from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role) - (CCE-11623-6) - Fail
- 4656 ● **TS/RDS – PNP Device Redirection**
 - 4657 ○ The system will be configured to prevent users from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role) - (CCE-11128-6) - Fail
- 4659 ● **TS/RDS – Smart Card Device Redirection**
 - 4660 ○ The system will be configured to ensure smart card devices can be redirected to the Remote Desktop Session. (Remote Desktop Services Role) - (CCE-11517-0) - Fail
- 4662 ● **TS/RDS – Printer Redirection**
 - 4663 ○ The system will be configured to allow only the default client printer to be redirected in the Remote Desktop session. (Remote Desktop Services Role) - (CCE-10977-7) - Fail
- 4665 ● **TS/RDS – Remove Disconnect Option**
 - 4666 ○ The system will be configured to remove the Disconnect option from the Shut Down Windows dialog box on the Remote Desktop Client. (Remote Desktop Services Role) - (CCE-11997-4) - Fail
- 4668 ● **Windows Customer Experience Improvement Program**
 - 4669 ○ The Windows Customer Experience Improvement Program will be disabled. - (CCE-11354-8) - Fail
- 4670 ● **SPN Target Name Validation Level**
 - 4671 ○ The service principal name (SPN) target name validation level will be turned off. - (CCE-10617-9) - Fail
- 4672 ● **Computer Identity Authentication for NTLM**
 - 4673 ○ Services using Local System that use negotiate when reverting to NTLM authentication will use the computer identity vs. authenticating anonymously. - (CCE-10817-5) - Fail
- 4675 ● **NTLM NULL Session Fallback**
 - 4676 ○ NTLM will be prevented from falling back to a Null session. - (CCE-10812-6) - Fail
- 4677 ● **PKU2U Online Identities Authentication**
 - 4678 ○ PKU2U authentication using online identities will be prevented. - (CCE-10839-9) - Fail
- 4679 ● **Kerberos Encryption Types**
 - 4680 ○ Kerberos encryption types will be configured to prevent the use of DES encryption suites. - (CCE-10843-1) - Fail
- 4681 ● **IPv6 Source Routing**
 - 4682 ○ IPv6 source routing will be configured to highest protection. - (CCE-10888-6) - Fail
- 4683 ● **IPv6 TCP Data Retransmissions**
 - 4684 ○ IPv6 TCP data retransmissions will be configured to prevent resources from becoming exhausted. - (CCE-10804-3) - Fail
- 4686 ● **Elevate when setting a network's location**
 - 4687 ○ Domain users will be required to elevate when setting a network's location. - (CCE-11610-3) - Fail
- 4688 ● **Direct Access – Route Through Internal Network**
 - 4689 ○ All Direct Access traffic will be routed through the internal network. - (CCE-11300-1) - Fail
- 4690 ● **Windows Update Point and Print Driver Search**
 - 4691 ○ Windows Update will be prevented from searching for point and print drivers. - (CCE-11976-8) - Fail
- 4692 ● **Prevent device metadata retrieval from Internet**
 - 4693 ○ Device metadata retrieval from the Internet will be prevented. - (CCE-11589-9) - Fail
- 4694 ● **Prevent Windows Update for device driver search**
 - 4695 ○ Device driver searches using Windows Update will be prevented. - (CCE-11787-9) - Fail

- 4696 ● **MSDT Interactive Communication**
 - 4697 ○ Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft will be prevented. - (CCE-10855-5) - Fail
- 4699 ● **Windows Online Troubleshooting Service**
 - 4700 ○ Access to Windows Online Troubleshooting Service (WOTS) will be prevented. - (CCE-11161-7) - Fail
- 4701 ● **Disable PerfTrack**
 - 4702 ○ Responsiveness events will be prevented from being aggregated and sent to Microsoft. - (CCE-11889-3) - Fail
- 4703 ● **Application Compatibility Program Inventory**
 - 4704 ○ The Application Compatibility Program Inventory will be prevented from collecting data and sending the information to Microsoft. - (CCE-11043-7) - Fail
- 4706 ● **Autoplay for non-volume devices**
 - 4707 ○ Autoplay will be turned off for non-volume devices. - (CCE-11375-3) - Fail
- 4708 ● **Turn Off Game Updates**
 - 4709 ○ Downloading of game update information will be turned off. - (CCE-11807-5) - Fail
- 4710 ● **Prevent Joining Homegroup**
 - 4711 ○ The system will be prevented from joining a homegroup. - (CCE-10691-4) - Fail
- 4712 ● **Windows Anytime Upgrade**
 - 4713 ○ Windows Anytime Upgrade will be disabled. - (CCE-10544-5) - Fail
- 4714 ● **Explorer Data Execution Prevention**
 - 4715 ○ Explorer Data Execution Prevention will be enabled. - (CCE-12161-6) - Fail
- 4716 ● **Default Autorun Behavior**
 - 4717 ○ The default autorun behavior will be configured to prevent autorun commands. - (CCE-11431-4) - Fail
- 4718 ● **Legal Banner Dialog Box Title**
 - 4719 ○ The Windows dialog box title for the legal banner will be configured. - (CCE-10010-7) - Fail
- 4720 ● **Access this computer from the network**
 - 4721 ○ Unauthorized accounts will not have the "Access this computer from the network" user right. - (CCE-10086-7) - Fail
- 4723 ● **Adjust memory quotas for a process**
 - 4724 ○ Unauthorized accounts will not have the "Adjust memory quotas for a process" user right. - (CCE-10849-8) - Fail
- 4725 ● **Allow log on locally**
 - 4726 ○ Unauthorized accounts will not have the "Allow log on locally" user right. - (CCE-10853-0) - Fail
- 4727 ● **Back up files and directories**
 - 4728 ○ Unauthorized accounts will not have the "Back up files and directories" user right. - (CCE-10880-3) - Fail
- 4729 ● **Bypass traverse checking**
 - 4730 ○ Unauthorized accounts will not have the "Bypass traverse checking" user right. - (CCE-10369-7) - Fail
- 4731 ● **Change the system time**
 - 4732 ○ Unauthorized accounts will not have the "Change the system time" user right. - (CCE-10122-0) - Fail
- 4733 ● **Change the time zone**
 - 4734 ○ Unauthorized accounts will not have the "Change the time zone" user right. - (CCE-10897-7) - Fail
- 4735 ● **Deny log on as a batch job**
 - 4736 ○ The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-10596-5) - Fail
- 4739 ● **Deny log on as service**
 - 4740 ○ The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-10226-9) - Fail
- 4743 ● **Deny log on locally**
 - 4744 ○ The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-10750-8) - Fail
- 4747 ● **Deny log on through Remote Desktop \ Terminal Services**
 - 4748 ○ The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-10878-7) - Fail

- 4751 ● **Force shutdown from a remote system**
 - 4752 ○ Unauthorized accounts will not have the "Force shutdown from a remote system" user right. - (CCE-10785-4) - Fail
- 4753
- 4754 ● **Generate security audits**
 - 4755 ○ Unauthorized accounts will not have the "Generate security audits" user right. - (CCE-10274-9) - Fail
- 4756 ● **Impersonate a client after authentication**
 - 4757 ○ Unauthorized accounts will not have the "Impersonate a client after authentication" user right. - (CCE-9946-5) - Fail
- 4758
- 4759 ● **Increase a process working set**
 - 4760 ○ Unauthorized accounts will not have the "Increase a process working set" user right. - (CCE-10548-6) - Fail
- 4761
- 4762 ● **Load and unload device drivers**
 - 4763 ○ Unauthorized accounts will not have the "Load and unload device drivers" user right. - (CCE-10202-0) - Fail
- 4764
- 4765 ● **Log on as a batch job**
 - 4766 ○ Unauthorized accounts will not have the "Log on as a batch job" user right. - (CCE-10549-4) - Fail
- 4767
- 4768 ● **Replace a process level token**
 - 4769 ○ Unauthorized accounts will not have the "Replace a process level token" user right. - (CCE-10599-9) - Fail
- 4770
- 4771 ● **Restore files and directories**
 - 4772 ○ Unauthorized accounts will not have the "Restore files and directories" user right. - (CCE-10805-0) - Fail
- 4773
- 4774 ● **Shut down the system**
 - 4775 ○ Unauthorized accounts will not have the "Shut down the system" user right. - (CCE-10439-8) - Fail
- 4776
- 4777 ● **Audit - Credential Validation - Failure**
 - 4778 ○ The system will be configured to audit "Account Logon > Credential Validation" failures. - Fail
- 4779
- 4780 ● **Audit - Computer Account Management - Failure**
 - 4781 ○ The system will be configured to audit "Account Management > Computer Account Management" failures. - Fail
- 4782
- 4783 ● **Audit - Other Account Management Events - Success**
 - 4784 ○ The system will be configured to audit "Account Management > Other Account Management Events" successes. - Fail
- 4785
- 4786 ● **Audit - Other Account Management Events - Failure**
 - 4787 ○ The system will be configured to audit "Account Management > Other Account Management Events" failures. - Fail
- 4788
- 4789 ● **Audit - Security Group Management - Failure**
 - 4790 ○ The system will be configured to audit "Account Management > Security Group Management" failures. - Fail
- 4791
- 4792 ● **Audit - User Account Management - Success**
 - 4793 ○ The system will be configured to audit "Account Management > User Account Management" failures. - Fail
- 4794
- 4795 ● **Audit - User Account Management - Failure**
 - 4796 ○ The system will be configured to audit "Account Management > User Account Management" failures. - Fail
- 4797
- 4798 ● **Audit - Process Creation - Success**
 - 4799 ○ The system will be configured to audit "Detailed Tracking > Process Creation" successes. - Fail
- 4800
- 4801 ● **Audit - File System - Failure**
 - 4802 ○ The system will be configured to audit "Object Access > File System" failures. - Fail
- 4803
- 4804 ● **Audit - Registry - Failure**
 - 4805 ○ The system will be configured to audit "Object Access > Registry" failures. - Fail
- 4806
- 4807 ● **Audit - Audit Policy Change - Failure**
 - 4808 ○ The system will be configured to audit "Policy Change > Audit Policy Change" failures. - Fail
- 4809
- 4810 ● **Audit - Sensitive Privilege Use - Success**
 - 4811 ○ The system will be configured to audit "Privilege Use > Sensitive Privilege Use" successes. - Fail
- 4812
- 4813 ● **Audit - Sensitive Privilege Use - Failure**
 - 4814 ○ The system will be configured to audit "Privilege Use > Sensitive Privilege Use" failures. - Fail
- 4815
- 4816 ● **Audit - IPSec Driver - Success**
 - 4817 ○ The system will be configured to audit "System > IPSec Driver" successes. - Fail
- 4818
- 4819 ● **Audit - IPSec Driver - Failure**
 - 4820 ○ The system will be configured to audit "System > IPSec Driver" failures. - Fail
- 4821
- 4822 ● **Audit - Security State Change - Failure**
 - 4823 ○ The system will be configured to audit "System > Security State Change" failures. - Fail
- 4824
- 4825 ● **Audit - Security System Extension - Success**
 - 4826 ○ The system will be configured to audit "System > Security System Extension" successes. - Fail
- 4827

- 4806 ● **Audit - Security System Extension - Failure**
 - 4807 ○ The system will be configured to audit "System > Security System Extension" failures. - Fail
- 4808 ● **6to4 State**
 - 4809 ○ The 6to4 IPv6 transition technology will be disabled. - (CCE-11356-3) - Fail
- 4810 ● **IP-HTTPS State**
 - 4811 ○ The IP-HTTPS IPv6 transition technology will be disabled. - (CCE-10832-4) - Fail
- 4812 ● **ISATAP State**
 - 4813 ○ The ISATAP IPv6 transition technology will be disabled. - (CCE-11141-9) - Fail
- 4814 ● **Teredo State**
 - 4815 ○ The Teredo IPv6 transition technology will be disabled. - (CCE-11865-3) - Fail
- 4816 ● **Maximum Log Size - Application**
 - 4817 ○ The Application event log will be configured to a minimum size requirement. - (CCE-11143-5) - Fail
- 4818 ● **Maximum Log Size - Security**
 - 4819 ○ The Security event log will be configured to a minimum size requirement. - (CCE-11033-8) - Fail
- 4820 ● **Maximum Log Size - Setup**
 - 4821 ○ The Setup event log will be configured to a minimum size requirement. - (CCE-11717-6) - Fail
- 4822 ● **Maximum Log Size - System**
 - 4823 ○ The System event log will be configured to a minimum size requirement. - (CCE-11174-0) - Fail
- 4824 ● **Device Install Software Request Error Report**
 - 4825 ○ Windows will be prevented from sending an error report when a device driver requests additional software during installation. - (CCE-11336-5) - Fail
- 4826 ● **Always Install with Elevated Privileges Disabled**
 - 4827 ○ The Windows Installer Always install with elevated privileges must be disabled. - (CCE-12401-6) - Fail
- 4828 ● **Local admin accounts filtered token policy enabled on domain systems.**
 - 4829 ○ Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems. - Fail
- 4830 ● **WINCC-000078**
 - 4831 ○ The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomization (ASLR) must be enabled and configured to Application Opt In. - Fail
- 4832 ● **WINCC-000079**
 - 4833 ○ The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer must be enabled. - Fail
- 4834 ● **WINCC-000080**
 - 4835 ○ The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Recommended Software must be enabled. - Fail
- 4836 ● **WINCC-000081**
 - 4837 ○ The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software must be enabled. - Fail
- 4838 ● **WINCC-000082**
 - 4839 ○ The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) must be enabled and configured to at least Application Opt Out. - Fail
- 4840 ● **WINCC-000083**
 - 4841 ○ The Enhanced Mitigation Experience Toolkit (EMET) system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be configured to Application Opt Out. - Fail
- 4842 ● **WINGE-0000100**
 - 4843 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
- 4844 ● **WINGE-0000200**
 - 4845 ○ A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail

4856

4857 **17.5 IT DOMAIN CONTROLLER STIG COMPLIANCE REPORT**

4858 Non-Compliance Report - U_Windows2012_DC_V1R3_STIG_SCAP_1-1_Benchmark

4859 **SCAP Compliance Checker - 3.1.2**4860 [Score](#) | [System Information](#) | [Stream Information](#) | [Results](#) | [Detailed Results](#)

4861 Score

91.13%

Adjusted Score: 91.13%

Original Score: 91.13%

Compliance Status: GREEN

4862

Pass: 267	Not Applicable: 0
Fail: 26	Not Checked: 0
Error: 0	Not Selected: 0
Unknown: 0	Total: 293

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

4863 **System Information**

Target:	ITDC
Operating System:	Windows Server 2012 R2 Standard
OS Service Pack:	
Domain:	ES-IDAM-B1

4864 **Results**

- **Bad Logon Attempts**
 - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- **Force Logoff When Logon Hours Expire**
 - The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail
- **LDAP Signing Requirements**
 - Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
- **Computer Account Password Change**
 - Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6) - Fail
- **Remotely Accessible Registry Paths and Sub-Paths**
 - Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
- **Minimum Password Length**
 - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- **Media DRM – Internet Access**
- **Software Certificate Installation Files**
 - Software certificate installation files must be removed from a system. - Fail
- **Legal Banner Dialog Box Title**
 - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- **Access this computer from the network**
 - Unauthorized accounts must not have the Access this computer from the network user right on domain controllers. - Fail
- **Allow log on locally**

4888 ○ Unauthorized accounts must not have the Allow log on locally user right. - (CCE-25228-8) - Fail

4889 ● **Back up files and directories**

4890 ○ Unauthorized accounts must not have the Back up files and directories user right. - (CCE-25380-7) - Fail

4891 ● **Bypass traverse checking**

4892 ○ Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail

4893 ● **Change the system time**

4894 ○ Unauthorized accounts must not have the Change the system time user right. - (CCE-24185-1) - Fail

4895 ● **Change the time zone**

4896 ○ Unauthorized accounts must not have the Change the time zone user right. - (CCE-24632-2) - Fail

4897 ● **Force shutdown from a remote system**

4898 ○ Unauthorized accounts must not have the Force shutdown from a remote system user right. - (CCE-24734-6) - Fail

4899

4900 ● **Increase a process working set**

4901 ○ Unauthorized accounts must not have the Increase a process working set user right. - (CCE-24162-0) - Fail

4902 ● **Increase scheduling priority**

4903 ● **Load and unload device drivers**

4904 ○ Unauthorized accounts must not have the Load and unload device drivers user right. - (CCE-24779-1) - Fail

4905 ● **Log on as a batch job**

4906 ○ Unauthorized accounts must not have the Log on as a batch job user right. - (CCE-23386-6) - Fail

4907 ● **Restore files and directories**

4908 ○ Unauthorized accounts must not have the Restore files and directories user right. - (CCE-25518-2) - Fail

4909 ● **Shut down the system**

4910 ○ Unauthorized accounts must not have the Shut down the system user right. - (CCE-23500-2) - Fail

4911 ● **Add workstations to domain**

4912 ○ Unauthorized accounts must not have the Add workstations to domain user right. - (CCE-23271-0) - Fail

4913 ● **Audit Directory Service Access - Success**

4914 ○ The system must be configured to audit DS Access - Directory Service Access successes. - Fail

4915 ● **Audit - Directory Service Access - Failure**

4916 ○ The system must be configured to audit DS Access - Directory Service Access failures. - Fail

4917 ● **Audit - Directory Service Changes - Success**

4918 ○ The system must be configured to audit DS Access - Directory Service Changes successes. - Fail

4919 ● **Audit - Directory Service Changes - Failure**

4920 ○ The system must be configured to audit DS Access - Directory Service Changes failures. - Fail

4921 ● **WINGE-000100**

4922 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

4923

4924

4925 **17.6 IT WINDOWS 7 WORKSTATIONS STIG COMPLIANCE REPORT**

4926 Non-Compliance Report - U_Windows_7_V1R23_STIG_SCAP_1-0_Benchmark

4927 **SCAP Compliance Checker - 3.1.2**4928 [Score](#) | [System Information](#) | [Stream Information](#) | [Results](#) | [Detailed Results](#)

4929 Score

94.72%

Adjusted Score: 94.72%
 Original Score: 94.72%
 Compliance Status: GREEN

4930

Pass: 251	Not Applicable: 0
Fail: 14	Not Checked: 0
Error: 0	Not Selected: 0
Unknown: 0	Total: 265

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

4931 System Information

Target:	ITWORKS1
Operating System:	Windows 7 Enterprise
OS Service Pack:	Service Pack 1
Domain:	ES-IDAM-B1
Processor:	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
Processor Architecture:	Intel64 Family 6 Model 45 Stepping 7
Processor Speed:	2200 MHz
Physical Memory:	6144 mb
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-42 09 b3 57 32 50 16 c6-cb 47 45 dd e3 a9 68 f1
BIOS Version:	6.00
Interfaces:	<ul style="list-style-type: none"> [00000007] Intel(R) PRO/1000 MT Network Connection <ul style="list-style-type: none"> 172.16.5.6 00:50:56:89:A2:29

4932 Results

- **Legal Notice Display**
 - The required legal notice must be configured to display before console logon. - (CCE-8973-0) - Fail
- **Bad Logon Attempts**
 - Number of allowed bad-logon attempts does not meet minimum requirements. - (CCE-9136-3) - Fail
- **Secure Print Driver Installation**
 - Print driver installation privilege is not restricted to administrators. - (CCE-9026-6) - Fail
- **Deny Access from the Network**
 - The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-9244-5) - Fail
- **Force Logoff When Logon Hours Expire**
 - The system is not configured to force users to log off when their allowed logon hours expire. - (CCE-9704-8) - Fail
- **Minimum Password Length**
 - For systems utilizing a logon ID as the individual identifier, passwords must be a minimum of 14 characters in length. - (CCE-9357-5) - Fail
- **TS/RDS - Remote User Connections**
 - Terminal Services / Remote Desktop Services - Prevent users from connecting using Terminal Services or Remote Desktop. - (CCE-9985-3) - Fail
- **Unnecessary Features Installed**
 - Unnecessary features are installed. - Fail

4954 • Deny log on as a batch job
 4955 ○ The Deny log on as a batch job user right on workstations must be configured to prevent access from highly
 4956 privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9212-2) - Fail
 4957 • Deny log on as service
 4958 ○ The Deny log on as a service user right on workstations must be configured to prevent access from highly
 4959 privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. -
 4960 (CCE-9098-5) - Fail
 4961 • Deny log on locally
 4962 ○ The Deny log on locally user right on workstations must be configured to prevent access from highly privileged
 4963 domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9239-5) - Fail
 4964 • Deny log on through Remote Desktop \ Terminal Services
 4965 ○ The Deny log on through Remote Desktop Services user right on workstations must prevent all access if RDS is
 4966 not used by the organization. If RDS is used, it must be configured to prevent access from highly privileged
 4967 domain accounts and local administrator accounts on domain systems and unauthenticated access on all
 4968 systems. - (CCE-9274-2) - Fail
 4969 • Enable accounts to be trusted for delegation
 4970 • WINGE-000100
 4971 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. -
 4972 Fail
 4973 • WINGE-000200
 4974 ○ A group named DenyNetworkAccess must be defined on domain systems to include all local administrator
 4975 accounts. - Fail

4976

4977 **17.7 OZONE AUTHORITY AND OZONE SERVER CENTOS 6 SERVER STIG COMPLIANCE REPORT**

4978 XCCDF Test Result

4979 17.7.1 Introduction

4980 Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_default-profile	(Default profile)	2015-04-08 07:58	2015-04-08 07:59	embedded	1

4981 Target info

Targets	Addresses	Platforms
• localhost.localdomain	• 127.0.0.1 • 172.16.4.11 • 0:0:0:0:0:0:1 • fe80:0:0:0:250:56ff:fe89:76dd	• cpe:/o:redhat:enterprise_linux

4982 Score

system	score	max	%	bar
urn:xccdf:scoring:default	95.53	100.00	95.53%	

4983 17.7.2 Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
171	0	8	0	0	0	0	0	0	179

Title		Result
Auditing must be enabled at boot by setting a kernel parameter.		fail
Library files must be owned by root.		fail
The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).		fail
The system boot loader configuration file(s) must be owned by root.		fail
The system boot loader configuration file(s) must be group-owned by root.		fail
The system boot loader configuration file(s) must have mode 0600 or less permissive.		fail
The system boot loader must require authentication.		fail
The system must provide VPN connectivity for communications over untrusted networks.		fail

4985

4986 17.8 OZONE ENVOY CENTOS 6 SERVER STIG COMPLIANCE REPORT

4987 XCCDF Test Result

4988 17.8.1 Introduction

4989 Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_default-profile	(Default profile)	2015-04-08 08:02	2015-04-08 08:03	embedded	1

4990 Target info

Targets	Addresses	Platforms
• localhost.localdomain	<ul style="list-style-type: none"> 127.0.0.1 172.16.4.12 0:0:0:0:0:0:1 fe80:0:0:0:250:56ff:fe89:980a 	<ul style="list-style-type: none"> cpe:/o:redhat:enterprise_linux

4991 Score

system	score	max	%	bar
urn:xccdf:scoring:default	96.09	100.00	96.09%	

4992 17.8.2 Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
172	0	7	0	0	0	0	0	0	179

Title		Result
Auditing must be enabled at boot by setting a kernel parameter.		fail
The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).		fail
The system boot loader configuration file(s) must be owned by root.		fail
The system boot loader configuration file(s) must be group-owned by root.		fail
The system boot loader configuration file(s) must have mode 0600 or less permissive.		fail
The system boot loader must require authentication.		fail
The system must provide VPN connectivity for communications over untrusted networks.		fail

4994

4995

4996 **17.9 OT DOMAIN CONTROLLER STIG COMPLIANCE REPORT**

4997 Non-Compliance Report - U_Windows2012_DC_V1R3_STIG_SCAP_1-1_Benchmark

4998 **SCAP Compliance Checker - 3.1.2**

4999 Score | System Information | Stream Information | Results | Detailed Results

5000 Score

91.13%

Adjusted Score: 91.13%
 Original Score: 91.13%
Compliance Status: GREEN

5001

Pass: 267	Not Applicable: 0
Fail: 26	Not Checked: 0
Error: 0	Not Selected: 0
Unknown: 0	Total: 293

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

5002 **System Information**

Target:	OTDC
Operating System:	Windows Server 2012 R2 Standard
OS Service Pack:	
Domain:	OT-ES-IDAM-B1

5003 **Results**

- 5004 • **Bad Logon Attempts**
 - 5005 ○ The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
 - 5006 • B
- 5007 • **Force Logoff When Logon Hours Expire**
 - 5008 ○ The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail
 - 5009
- 5010 • **LDAP Signing Requirements**
 - 5011 ○ Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
 - 5012
- 5013 • **Computer Account Password Change**
 - 5014 ○ Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6) - Fail
 - 5015
- 5016 • **Remotely Accessible Registry Paths and Sub-Paths**
 - 5017 ○ Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
 - 5018
- 5019 • **Minimum Password Length**
 - 5020 ○ Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
 - 5021
- 5022 • **Software Certificate Installation Files**
 - 5023 ○ Software certificate installation files must be removed from a system. - Fail
 - 5024
- 5025 • **Legal Banner Dialog Box Title**
 - 5026 ○ The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
 - 5027
- 5028 • **Access this computer from the network**
 - 5029 ○ Unauthorized accounts must not have the Access this computer from the network user right on domain controllers. - Fail
 - 5030
- 5031 • **Adjust memory quotas for a process**
 - 5032
- 5033 • **Allow log on locally**
 - 5034

- 5027 ○ Unauthorized accounts must not have the Allow log on locally user right. - (CCE-25228-8) - Fail
- 5028 ● Allow log on through Remote Desktop Services
- 5029 ● Back up files and directories
 - Unauthorized accounts must not have the Back up files and directories user right. - (CCE-25380-7) - Fail
- 5031 ● Bypass traverse checking
 - Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail
- 5033 ● Change the system time
 - Unauthorized accounts must not have the Change the system time user right. - (CCE-24185-1) - Fail
- 5035 ● Change the time zone
 - Unauthorized accounts must not have the Change the time zone user right. - (CCE-24632-2) - Fail
- 5037 ● Force shutdown from a remote system
 - Unauthorized accounts must not have the Force shutdown from a remote system user right. - (CCE-24734-6) - Fail
- 5040 ● Increase a process working set
 - Unauthorized accounts must not have the Increase a process working set user right. - (CCE-24162-0) - Fail
- 5042 ● Load and unload device drivers
 - Unauthorized accounts must not have the Load and unload device drivers user right. - (CCE-24779-1) - Fail
- 5044 ● Log on as a batch job
 - Unauthorized accounts must not have the Log on as a batch job user right. - (CCE-23386-6) - Fail
- 5046 ● Restore files and directories
 - Unauthorized accounts must not have the Restore files and directories user right. - (CCE-25518-2) - Fail
- 5048 ● Shut down the system
 - Unauthorized accounts must not have the Shut down the system user right. - (CCE-23500-2) - Fail
- 5049 ● Add workstations to domain
 - Unauthorized accounts must not have the Add workstations to domain user right. - (CCE-23271-0) - Fail
- 5052 ● Audit Directory Service Access - Success
 - The system must be configured to audit DS Access - Directory Service Access successes. - Fail
- 5054 ● Audit - Directory Service Access - Failure
 - The system must be configured to audit DS Access - Directory Service Access failures. - Fail
- 5056 ● Audit - Directory Service Changes - Success
 - The system must be configured to audit DS Access - Directory Service Changes successes. - Fail
- 5057 ● Audit - Directory Service Changes - Failure
 - The system must be configured to audit DS Access - Directory Service Changes failures. - Fail
- 5060 ● WINGE-000100
 - The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
- 5061 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
- 5062 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

5063 17.10 OT CONSOLEWORKS WINDOWS SERVER 2012 STIG COMPLIANCE REPORT

5064 Non-Compliance Report - U_Windows2012_MS_V1R3_STIG_SCAP_1-1_Benchmark

SCAP Compliance Checker - 3.1.2				
Score System Information Stream Information Results Detailed Results				
Score				

97.13%

Adjusted Score: 97.13%
 Original Score: 97.13%
 Compliance Status: GREEN

5068

Pass: 271 Not Applicable: 0
 Fail: 8 Not Checked: 0

BLUE: Score equals 100
 GREEN: Score is greater than or equal to 90

Error: 0	Not Selected: 0	YELLOW: Score is greater than or equal to 80
Unknown: 0	Total: 279	RED: Score is greater than or equal to 0

5069 System Information

Target:	OT-CONSOLEWORKS
Operating System:	Windows Server 2012 R2 Standard
OS Service Pack:	
Domain:	OT-ES-IDAM-B1
Processor:	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
Processor Architecture:	Intel64 Family 6 Model 45 Stepping 7
Processor Speed:	2200 MHz
Physical Memory:	8192 mb
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-42 09 c2 cc c1 37 31 5c-2d 94 63 96 80 d2 05 fe
BIOS Version:	6.00
Interfaces:	<ul style="list-style-type: none"> • [00000010] Intel(R) 82574L Gigabit Network Connection <ul style="list-style-type: none"> ○ 172.16.6.8 ○ 00:50:56:89:56:86

5070 Results

- **Bad Logon Attempts**
 - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- **Force Logoff When Logon Hours Expire**
 - The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail
- **Minimum Password Length**
 - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- **Legal Banner Dialog Box Title**
 - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- **Deny log on as a batch job**
 - The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-25215-5) - Fail
- **Deny log on as service**
 - The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-23117-5) - Fail
- **Deny log on locally**
 - The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-24460-8) - Fail
- **WINGE-000100**
 - The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

5095 **17.11 OT WINDOWS 7 WORKSTATIONS STIG COMPLIANCE REPORT**

5096 Non-Compliance Report - U_Windows_7_V1R23_STIG_SCAP_1-0_Benchmark

5097 **SCAP Compliance Checker - 3.1.2**5098 [Score](#) | [System Information](#) | [Stream Information](#) | [Results](#) | [Detailed Results](#)

5099 Score

95.47%

Adjusted Score: 95.47%
 Original Score: 95.47%
Compliance Status: GREEN

5100

Pass: 253	Not Applicable: 0
Fail: 12	Not Checked: 0
Error: 0	Not Selected: 0
Unknown: 0	Total: 265

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

5101 **System Information**

Target:	OTWORKS1
Operating System:	Windows 7 Enterprise
OS Service Pack:	Service Pack 1
Domain:	OT-ES-IDAM-B1
Processor:	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
Processor Architecture:	Intel64 Family 6 Model 45 Stepping 7
Processor Speed:	2200 MHz
Physical Memory:	4096 mb
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-42 09 49 1e 0a 42 38 8e-03 d2 8f e6 31 25 5a 63
BIOS Version:	6.00
Interfaces:	<ul style="list-style-type: none"> • [00000007] Intel(R) PRO/1000 MT Network Connection <ul style="list-style-type: none"> ○ 172.16.6.6 ○ 00:50:56:89:0B:7A

5102 **Results**

- **Legal Notice Display**
 - The required legal notice must be configured to display before console logon. - (CCE-8973-0) - Fail
- **Bad Logon Attempts**
 - Number of allowed bad-logon attempts does not meet minimum requirements. - (CCE-9136-3) - Fail
- **Secure Print Driver Installation**

5108 ○ Print driver installation privilege is not restricted to administrators. - (CCE-9026-6) - Fail

5109 ● **Deny Access from the Network**

5110 ○ The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-9244-5) - Fail

5111 ● **Force Logoff When Logon Hours Expire**

5112 ○ The system is not configured to force users to log off when their allowed logon hours expire. - (CCE-9704-8) - Fail

5113 ● **Minimum Password Length**

5114 ○ For systems utilizing a logon ID as the individual identifier, passwords must be a minimum of 14 characters in length. - (CCE-9357-5) - Fail

5115 ● **Deny log on as a batch job**

5116 ○ The Deny log on as a batch job user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9212-2) - Fail

5117 ● **Deny log on as service**

5118 ○ The Deny log on as a service user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-9098-5) - Fail

5119 ● **Deny log on locally**

5120 ○ The Deny log on locally user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9239-5) - Fail

5121 ● **Deny log on through Remote Desktop \ Terminal Services**

5122 ○ The Deny log on through Remote Desktop Services user right on workstations must prevent all access if RDS is not used by the organization. If RDS is used, it must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-9274-2) - Fail

5123 ● **WINGE-000100**

5124 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

5125 ● **WINGE-000200**

5126 ○ A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail

5127 **17.12 PACS DOMAIN CONTROLLER STIG COMPLIANCE REPORT**

All Settings Report - U_Windows2012_DC_V1R3_STIG_SCAP_11_Benchmark

SCAP Compliance Checker - 3.1.2

Score | System Information | Stream Information | Results | Detailed Results

Score

91.47 %

Adjusted Score: 91.47 %
 Original Score: 91.47 %
 Compliance Status: GREEN

Pass: 268 Not Applicable: 0
 Fail: 25 Not Checked: 0

BLUE: Score equals 100
 GREEN: Score is greater than or equal to 90

Error: 0 Not Selected: 0 YELLOW: Score is greater than or equal to 80

Unknown: 0 Total: 293 RED: Score is greater than or equal to 0

System Information

Target:	PACSDC
Operating System:	Windows Server 2012 R2 Standard
OS Service Pack:	
Domain:	PACS-ES-IDAM-B1

Stream Information

Release Info	• Release: 3 Benchmark Date: 28 Oct 2014
Stream:	U_Windows2012_DC_V1R3_STIG_SCAP_1-1_Benchmark
Title:	Windows Server 2012 / 2012 R2 Domain Controller Security Technical Implementation Guide
Description:	The Windows Server 2012 / 2012 R2 Domain Controller Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. Comments or proposed revisions to this document should be sent via e-mail to the following address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.
Notice:	Developed_by_DISA_for_the_DoD
Target Platforms:	• cpe:/o:microsoft:windows_server_2012:-
Identity Authenticated:	true

5141

5142 Detailed Results

5143

1. Bad Logon Attempts - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail

5144 2. Force Logoff When Logon Hours Expire - The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail

5145 3. LDAP Signing Requirements - Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail

5146 4. Computer Account Password Change - Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6) - Fail

5147 5. Remotely Accessible Registry Paths and Sub-Paths - Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail

5148 6. Minimum Password Length - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail

5149 7. Legal Banner Dialog Box Title - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail

5150 8. Access this computer from the network - Unauthorized accounts must not have the Access this computer from the network user right on domain controllers. - Fail

5151 9. Allow log on locally - Unauthorized accounts must not have the Allow log on locally user right. - (CCE-25228-8) - Fail

5152 10. Back up files and directories - Unauthorized accounts must not have the Back up files and directories user right. - (CCE-25380-7) - Fail

5153 11. Bypass traverse checking - Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail

5154 12. Change the system time - Unauthorized accounts must not have the Change the system time user right. - (CCE-24185-1) - Fail

5155 13. Change the time zone - Unauthorized accounts must not have the Change the time zone user right. - (CCE-24632-2) - Fail

5156 14. Force shutdown from a remote system Unauthorized accounts must not have the Force shutdown from a remote system user right. - (CCE-24734-6) - Fail

5157 15. Increase a process working set - Unauthorized accounts must not have the Increase a process working set user right. - (CCE-24162-0) - Fail

5158 16. Load and unload device drivers - Unauthorized accounts must not have the Load and unload device drivers user right. - (CCE-24779-1) - Fail

5159 17. Log on as a batch job - Unauthorized accounts must not have the Log on as a batch job user right. - (CCE-23386-6) - Fail

5160 18. Restore files and directories - Unauthorized accounts must not have the Restore files and directories user right. - (CCE-25518-2) - Fail

5161 19. Shut down the system - Unauthorized accounts must not have the Shut down the system user right. - (CCE-23500-2) - Fail

5162 20. Add workstations to domain - Unauthorized accounts must not have the Add workstations to domain user right. - (CCE-23271-0) - Fail

5163 21. Audit Directory Service Access - Success - The system must be configured to audit DS Access - Directory Service Access successes. - Fail

5164 22. Audit - Directory Service Access - Failure - The system must be configured to audit DS Access - Directory Service Access failures. - Fail

5165 23. Audit - Directory Service Changes - Success - The system must be configured to audit DS Access - Directory Service Changes successes. - Fail

5166 24. Audit - Directory Service Changes - Failure - The system must be configured to audit DS Access - Directory Service Changes failures. - Fail

5167 25. WINGE-000100 - The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

5168

5169

5170

5171

5172

5173

5174

5175

5176

5177

5178

5179 **17.13 PACS CONSOLE WINDOWS SERVER 2012 STIG COMPLIANCE REPORT**

5180 Non-Compliance Report - U_Windows2012_MS_V1R3_STIG_SCAP_1-1_Benchmark

5181 **SCAP Compliance Checker - 3.1.2**

5182 [Score](#) | [System Information](#) | [Stream Information](#) | [Results](#) | [Detailed Results](#)

5183 Score

96.06%

Adjusted Score: 96.06%
 Original Score: 96.06%
 Compliance Status: GREEN

5184

Pass: 268	Not Applicable: 0
Fail: 11	Not Checked: 0
Error: 0	Not Selected: 0
Unknown: 0	Total: 279

BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

5185 System Information

Target:	PACS-CONSOLE
Operating System:	Windows Server 2012 R2 Standard
OS Service Pack:	
Domain:	PACS-ES-IDAM-B1
Processor:	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
Processor Architecture:	Intel64 Family 6 Model 45 Stepping 7
Processor Speed:	2200 MHz
Physical Memory:	8192 mb
Manufacturer:	VMware, Inc.
Model:	VMware Virtual Platform
Serial Number:	VMware-42 09 dc 00 da 26 44 78-07 ea f5 33 59 b9 af 46
BIOS Version:	6.00
Interfaces:	<ul style="list-style-type: none"> • [00000010] Intel(R) 82574L Gigabit Network Connection <ul style="list-style-type: none"> ○ 172.16.7.11 ○ 00:50:56:89:F8:E0

5186 Results

- **Bad Logon Attempts**
 - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- **Force Logoff When Logon Hours Expire**
 - The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail
- **Minimum Password Length**
 - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- **Legal Banner Dialog Box Title**
 - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- **Adjust memory quotas for a process**
 - Unauthorized accounts must not have the Adjust memory quotas for a process user right. - (CCE-25112-4) - Fail
- **Bypass traverse checking**
 - Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail
- **Deny log on as a batch job**
 - The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-25215-5) - Fail
- **Deny log on as service**
 - The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-23117-5) - Fail
- **Deny log on locally**
 - The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-24460-8) - Fail
- **Replace a process level token**
 - Unauthorized accounts must not have the Replace a process level token user right. - (CCE-24555-5) - Fail
- **WINGE-000100**

5215 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. -
5216 Fail

5217 17.14 BASELINE CENTOS 7 LINUX CONFIGURATION

5218 How To STIG/Configure Centos 7

5219 Install fresh Centos 7 server image, using Minimal Install. The following are assumptions in the
5220 installation:

- Separate partitions for /var, /var/log, /var/log/audit, /tmp, /home
- Networking is configured for your network

```
5224 yum update -y
5225 yum install wget openscap-utiles aide libreswan iptables-service ntp
5226 mkdir {reports,xml}
5227 cd xml
5228 wget http://iase.disa.mil/stigs/Documents/u_RedHat_6_V1R6_STIG_SCAP_1-
5229 1_Benchmark.zip
5230 unzip u_RedHat*
```

Run Initial Test

```
5233
5234 oscap xccdf eval --report ../reports/report.html --cpe *cpe-
5235 dictionary.xml *Benchmark-xccdf.xml
5236 python -m SimpleHTTPServer
```

5238 Go to <http://<Centos 7 IP Address>:8000/> to view the results of the STIG test

1. Next add the following files to the following locations:

- rules_d-audit.rules > `/etc/audit/rules.d/audit.rules`
- audit.rules > `/etc/audit/audit.rules`
- audit.conf > `/etc/audit/audit.conf`
- system-auth > `/etc/pam.d/system-auth`
- system-auth-ac 0 * * * root /sbin/aide -checkth-ac > `/etc/pam.d/system-auth-ac`
- sysctl.conf > `/etc/sysctl.conf`
- password-auth-ac > `/etc/pam.d/password-auth-ac`
- iptables > `/etc/sysconfig/iptables`

2. Next edit the following files:

5250 1. In */etc/logindefs* add/change variables to:

5251 PASS MIN LEN 14

5252 PASS MIN DAYS 1

5253 PASS MAX DAYS 60

2. Add the following to `/etc/crontab`:

```
5255          ◦ 0 0 * * * root /sbin/aide -check
5256      3. In /etc/modprobe.d/disabled.conf (create if doesn't exist), add:
5257 install usb-storage /bin/false
5258 install dccp /bin/false
5259 install sctp /bin/false
5260 install rds /bin/false
5261 install tipc /bin/false
5262 install ipv6 /bin/false
5263      4. Remove any line in /etc/securetty that starts with 'vc' or 'ttyS'
5264      5. Add to /etc/rsyslog.conf
5265 *. * @@<any remote syslog server IP address>:514
5266      6. Add to /etc/sysconfig/init
5267 SINGLE=/sbin/sulogin
5268 PROMPT=no
5269      7. Edit /etc/ntp.conf
5270          ◦ place '#' in front of any line that starts with 'server'
5271          ◦ Add 'server tick.usno.navy.mil'
5272      8. For all files /etc/csh.cshrc, /etc/profile, /etc/login.defs, and /etc/bashrc
5273          ◦ Change any 'umask' line to 'umask 077' and any 'UMASK' line to 'UMASK 077'
5274      9. Add to /etc/inittab
5275 id:3:initdefault:
5276      10. Add to /etc/security/limits.conf
5277 * hard core 0
5278 * hard maxlogins 0
5279      11. Edit /etc/default/useradd
5280          ◦ Change 'INACTIVE=-1' to 'INACTIVE=35'
5281      12. yum remove firewalld
5282      13. chkconfig ntpd on
5283      14. service ntpd start
5284      15. ln -sf /lib/systemd/system/multi-user.target /etc/systemd/system/default.target

5285 17.14.1 Baseline CentOS 7 Configuration Files
5286      1. Audit.rules file contents:
5287      2. Audit.conf file contents:
5288      3. iptables file contents:
5289      4. Password_auth-ac file contents
5290      5. rules_d-audi.rules file contents
5291      6. Sysctl.conf files contents
5292      7. system-auth file contents
5293      8. system-auth-ac file contents
5294
```

```
5295 17.14.2 Audit.rules File Contents
5296 #
5297 # This file controls the configuration of the audit daemon
5298 #
5299
5300 log_file = /var/log/audit/audit.log
5301 log_format = RAW
5302 log_group = root
5303 priority_boost = 4
5304 flush = INCREMENTAL
5305 freq = 20
5306 num_logs = 5
5307 disp_qos = lossy
5308 dispatcher = /sbin/audispd
5309 name_format = NONE
5310 ##name = mydomain
5311 max_log_file = 6
5312 max_log_file_action = ROTATE
5313 space_left = 75
5314 space_left_action = email
5315 action_mail_acct = root
5316 admin_space_left = 50
5317 admin_space_left_action = SINGLE
5318 disk_full_action = SUSPEND
5319 disk_error_action = SUSPEND
5320 ##tcp_listen_port =
5321 tcp_listen_queue = 5
5322 tcp_max_per_addr = 1
5323 ##tcp_client_ports = 1024-65535
5324 tcp_client_max_idle = 0
5325 enable_krb5 = no
5326 krb5_principal = auditd
5327 ##krb5_key_file = /etc/audit/audit.key
5328
```

```
5329 17.14.3 Audit.conf File Contents
5330 #
5331 # This file controls the configuration of the audit daemon
5332 #
5333
5334 log_file = /var/log/audit/audit.log
5335 log_format = RAW
5336 log_group = root
5337 priority_boost = 4
5338 flush = INCREMENTAL
5339 freq = 20
5340 num_logs = 5
5341 disp_qos = lossy
5342 dispatcher = /sbin/audispd
5343 name_format = NONE
5344 ##name = mydomain
5345 max_log_file = 6
5346 max_log_file_action = ROTATE
5347 space_left = 75
```

```

5348 space_left_action = email
5349 action_mail_acct = root
5350 admin_space_left = 50
5351 admin_space_left_action = SINGLE
5352 disk_full_action = SUSPEND
5353 disk_error_action = SUSPEND
5354 ##tcp_listen_port =
5355 tcp_listen_queue = 5
5356 tcp_max_per_addr = 1
5357 ##tcp_client_ports = 1024-65535
5358 tcp_client_max_idle = 0
5359 enable_krb5 = no
5360 krb5_principal = auditd
5361 ##krb5_key_file = /etc/audit/audit.key
5362

```

5363 17.14.4 [iptables](#) File Contents

```

5364 # Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
5365 *nat
5366 :PREROUTING ACCEPT [219:23061]
5367 :INPUT ACCEPT [2:120]
5368 :OUTPUT ACCEPT [125:7804]
5369 :POSTROUTING ACCEPT [125:7804]
5370 :OUTPUT_direct - [0:0]
5371 :POSTROUTING_ZONES - [0:0]
5372 :POSTROUTING_ZONES_SOURCE - [0:0]
5373 :POSTROUTING_direct - [0:0]
5374 :POST_public - [0:0]
5375 :POST_public_allow - [0:0]
5376 :POST_public_deny - [0:0]
5377 :POST_public_log - [0:0]
5378 :PREROUTING_ZONES - [0:0]
5379 :PREROUTING_ZONES_SOURCE - [0:0]
5380 :PREROUTING_direct - [0:0]
5381 :PRE_public - [0:0]
5382 :PRE_public_allow - [0:0]
5383 :PRE_public_deny - [0:0]
5384 :PRE_public_log - [0:0]
5385 -A PREROUTING -j PREROUTING_direct
5386 -A PREROUTING -j PREROUTING_ZONES_SOURCE
5387 -A PREROUTING -j PREROUTING_ZONES
5388 -A OUTPUT -j OUTPUT_direct
5389 -A POSTROUTING -j POSTROUTING_direct
5390 -A POSTROUTING -j POSTROUTING_ZONES_SOURCE
5391 -A POSTROUTING -j POSTROUTING_ZONES
5392 -A POSTROUTING_ZONES -o ens160 -g POST_public
5393 -A POSTROUTING_ZONES -g POST_public
5394 -A POST_public -j POST_public_log
5395 -A POST_public -j POST_public_deny
5396 -A POST_public -j POST_public_allow
5397 -A PREROUTING_ZONES -i ens160 -g PRE_public
5398 -A PREROUTING_ZONES -g PRE_public
5399 -A PRE_public -j PRE_public_log
5400 -A PRE_public -j PRE_public_deny

```

```
5401 -A PRE_public -j PRE_public_allow
5402 COMMIT
5403 # Completed on Tue Jan 27 13:28:25 2015
5404 # Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
5405 *mangle
5406 :PREROUTING ACCEPT [94235:148159541]
5407 :INPUT ACCEPT [94155:148151187]
5408 :FORWARD ACCEPT [0:0]
5409 :OUTPUT ACCEPT [43012:2796100]
5410 :POSTROUTING ACCEPT [43027:2798919]
5411 :FORWARD_direct - [0:0]
5412 :INPUT_direct - [0:0]
5413 :OUTPUT_direct - [0:0]
5414 :POSTROUTING_direct - [0:0]
5415 :PREROUTING_ZONES - [0:0]
5416 :PREROUTING_ZONES_SOURCE - [0:0]
5417 :PREROUTING_direct - [0:0]
5418 :PRE_public - [0:0]
5419 :PRE_public_allow - [0:0]
5420 :PRE_public_deny - [0:0]
5421 :PRE_public_log - [0:0]
5422 -A PREROUTING -j PREROUTING_direct
5423 -A PREROUTING -j PREROUTING_ZONES_SOURCE
5424 -A PREROUTING -j PREROUTING_ZONES
5425 -A INPUT -j INPUT_direct
5426 -A FORWARD -j FORWARD_direct
5427 -A OUTPUT -j OUTPUT_direct
5428 -A POSTROUTING -j POSTROUTING_direct
5429 -A PREROUTING_ZONES -i ens160 -g PRE_public
5430 -A PREROUTING_ZONES -g PRE_public
5431 -A PRE_public -j PRE_public_log
5432 -A PRE_public -j PRE_public_deny
5433 -A PRE_public -j PRE_public_allow
5434 COMMIT
5435 # Completed on Tue Jan 27 13:28:25 2015
5436 # Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
5437 *security
5438 :INPUT ACCEPT [94003:148133781]
5439 :FORWARD ACCEPT [0:0]
5440 :OUTPUT ACCEPT [43012:2796100]
5441 :FORWARD_direct - [0:0]
5442 :INPUT_direct - [0:0]
5443 :OUTPUT_direct - [0:0]
5444 -A INPUT -j INPUT_direct
5445 -A FORWARD -j FORWARD_direct
5446 -A OUTPUT -j OUTPUT_direct
5447 COMMIT
5448 # Completed on Tue Jan 27 13:28:25 2015
5449 # Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
5450 *raw
5451 :PREROUTING ACCEPT [94236:148159577]
5452 :OUTPUT ACCEPT [43012:2796100]
5453 :OUTPUT_direct - [0:0]
5454 :PREROUTING_direct - [0:0]
```

```

5455 -A PREROUTING -j PREROUTING_direct
5456 -A OUTPUT -j OUTPUT_direct
5457 COMMIT
5458 # Completed on Tue Jan 27 13:28:25 2015
5459 # Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
5460 *filter
5461 :INPUT DROP [0:0]
5462 :FORWARD ACCEPT [0:0]
5463 :OUTPUT ACCEPT [0:0]
5464 :FORWARD_IN_ZONES - [0:0]
5465 :FORWARD_IN_ZONES_SOURCE - [0:0]
5466 :FORWARD_OUT_ZONES - [0:0]
5467 :FORWARD_OUT_ZONES_SOURCE - [0:0]
5468 :FORWARD_direct - [0:0]
5469 :FWDI_public - [0:0]
5470 :FWDI_public_allow - [0:0]
5471 :FWDI_public_deny - [0:0]
5472 :FWDI_public_log - [0:0]
5473 :FWDO_public - [0:0]
5474 :FWDO_public_allow - [0:0]
5475 :FWDO_public_deny - [0:0]
5476 :FWDO_public_log - [0:0]
5477 :INPUT_ZONES - [0:0]
5478 :INPUT_ZONES_SOURCE - [0:0]
5479 :INPUT_direct - [0:0]
5480 :IN_public - [0:0]
5481 :IN_public_allow - [0:0]
5482 :IN_public_deny - [0:0]
5483 :IN_public_log - [0:0]
5484 :OUTPUT_direct - [0:0]
5485 -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
5486 -A INPUT -i lo -j ACCEPT
5487 -A INPUT -j INPUT_direct
5488 -A INPUT -j INPUT_ZONES_SOURCE
5489 -A INPUT -j INPUT_ZONES
5490 -A INPUT -p icmp -j ACCEPT
5491 -A INPUT -j REJECT --reject-with icmp-host-prohibited
5492 -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
5493 -A FORWARD -i lo -j ACCEPT
5494 -A FORWARD -j FORWARD_direct
5495 -A FORWARD -j FORWARD_IN_ZONES_SOURCE
5496 -A FORWARD -j FORWARD_IN_ZONES
5497 -A FORWARD -j FORWARD_OUT_ZONES_SOURCE
5498 -A FORWARD -j FORWARD_OUT_ZONES
5499 -A FORWARD -p icmp -j ACCEPT
5500 -A FORWARD -j REJECT --reject-with icmp-host-prohibited
5501 -A OUTPUT -j OUTPUT_direct
5502 -A FORWARD_IN_ZONES -i ens160 -g FWDI_public
5503 -A FORWARD_IN_ZONES -g FWDI_public
5504 -A FORWARD_OUT_ZONES -o ens160 -g FWDO_public
5505 -A FORWARD_OUT_ZONES -g FWDO_public
5506 -A FWDI_public -j FWDI_public_log
5507 -A FWDI_public -j FWDI_public_deny
5508 -A FWDI_public -j FWDI_public_allow

```

```

5509 -A FWDO_public -j FWDO_public_log
5510 -A FWDO_public -j FWDO_public_deny
5511 -A FWDO_public -j FWDO_public_allow
5512 -A INPUT_ZONES -i ens160 -g IN_public
5513 -A INPUT_ZONES -g IN_public
5514 -A IN_public -j IN_public_log
5515 -A IN_public -j IN_public_deny
5516 -A IN_public -j IN_public_allow
5517 -A IN_public_allow -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j
5518 ACCEPT
5519 COMMIT
5520 # Completed on Tue Jan 27 13:28:25 2015
5521

```

```

5522 17.14.5 Password_auth-ac File Contents
5523 #%PAM-1.0
5524 # This file is auto-generated.
5525 # User changes will be destroyed the next time authconfig is run.
5526 auth required pam_env.so
5527 auth sufficient pam_unix.so nullok try_first_pass
5528 auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800
5529 fail_interval=900
5530 auth required pam_faillock.so authsuff deny=3 unlock_time=604800
5531 fail_interval=900
5532 auth requisite pam_succeed_if.so uid >= 1000 quiet_success
5533 auth required pam_deny.so
5534
5535 account required pam_unix.so
5536 account sufficient pam_localuser.so
5537 account sufficient pam_succeed_if.so uid < 1000 quiet
5538 account required pam_permit.so
5539
5540 password requisite pam_pwquality.so try_first_pass local_users_only
5541 retry=3 authtok_type=
5542 password sufficient pam_unix.so sha512 shadow nullok try_first_pass
5543 use_authtok
5544 password required pam_deny.so
5545
5546 session optional pam_keyinit.so revoke
5547 session required pam_limits.so
5548 -session optional pam_systemd.so
5549 session [success=1 default=ignore] pam_succeed_if.so service in crond
5550 quiet use_uid
5551 session required pam_unix.so
5552

```

```

5553 17.14.6 rules_d-audi.rules File Contents
5554 # This file contains the auditctl rules that are loaded
5555 # whenever the audit daemon is started via the initscripts.
5556 # The rules are simply the parameters that would be passed
5557 # to auditctl.
5558
5559 # First rule - delete all
5560 -D

```

```
5561
5562 # Increase the buffers to survive stress events.
5563 # Make this bigger for busy systems
5564 -b 320
5565
5566 # Feel free to add below this line. See auditctl man page
5567 # STIG Stuff Below
5568
5569 # audit_time_rules
5570 -a always,exit -F arch=b64 -S adjtimex -S settimofday -S clock_settime -k
5571 audit_time_rules
5572 -w /etc/localtime -p wa -k audit_time_rules
5573
5574 # audit_account_changes
5575 -w /etc/group -p wa -k audit_account_changes
5576 -w /etc/passwd -p wa -k audit_account_changes
5577 -w /etc/gshadow -p wa -k audit_account_changes
5578 -w /etc/shadow -p wa -k audit_account_changes
5579 -w /etc/security/opasswd -p wa -k audit_account_changes
5580
5581 # MAC-policy
5582 -w /etc/selinux -p wa -k MAC-policy
5583
5584 # export
5585 -a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k
5586 export
5587 -a always,exit -F arch=b64 -S mount -F auid=0 -k export
5588
5589 # delete
5590 -a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S
5591 renameat -F auid>=500 -F auid!=4294967295 -k delete
5592 -a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S
5593 renameat -F auid=0 -k delete
5594
5595 # actions
5596 -w /etc/sudoers -p wa -k actions
5597
5598 # modules
5599 -w /sbin/insmod -p x -k modules
5600 -w /sbin/rmmmod -p x -k modules
5601 -w /sbin/modprobe -p x -k modules
5602 -a always,exit -F arch=b64 -S init_module -S delete_module -k modules
5603
5604 # perm_mod
5605 -a always,exit -F arch=b32 -S chmod -F auid>=500 -F auid!=4294967295 -k
5606 perm_mod
5607 -a always,exit -F arch=b32 -S chmod -F auid=0 -k perm_mod
5608 -a always,exit -F arch=b32 -S fchmod -F auid>=500 -F auid!=4294967295 -k
5609 perm_mod
5610 -a always,exit -F arch=b32 -S fchmod -F auid=0 -k perm_mod
5611 -a always,exit -F arch=b64 -S chmod -F auid>=500 -F auid!=4294967295 -k
5612 perm_mod
5613 -a always,exit -F arch=b64 -S chmod -F auid=0 -k perm_mod
```

```
5614 -a always,exit -F arch=b64 -S fchmod -F auid>=500 -F auid!=4294967295 -k
5615 perm_mod
5616 -a always,exit -F arch=b64 -S fchmod -F auid=0 -k perm_mod
5617
5618 -a always,exit -F arch=b32 -S fchmodat -F auid>=500 -F auid!=4294967295 -k
5619 perm_mod
5620 -a always,exit -F arch=b32 -S fchmodat -F auid=0 -k perm_mod
5621 -a always,exit -F arch=b64 -S fchmodat -F auid>=500 -F auid!=4294967295 -k
5622 perm_mod
5623 -a always,exit -F arch=b64 -S fchmodat -F auid=0 -k perm_mod
5624
5625 -a always,exit -F arch=b32 -S fchown -F auid>=500 -F auid!=4294967295 -k
5626 perm_mod
5627 -a always,exit -F arch=b32 -S fchown -F auid=0 -k perm_mod
5628 -a always,exit -F arch=b64 -S fchown -F auid>=500 -F auid!=4294967295 -k
5629 perm_mod
5630 -a always,exit -F arch=b64 -S fchown -F auid=0 -k perm_mod
5631
5632 -a always,exit -F arch=b32 -S chown -F auid>=500 -F auid!=4294967295 -k
5633 perm_mod
5634 -a always,exit -F arch=b32 -S chown -F auid=0 -k perm_mod
5635 -a always,exit -F arch=b64 -S chown -F auid>=500 -F auid!=4294967295 -k
5636 perm_mod
5637 -a always,exit -F arch=b64 -S chown -F auid=0 -k perm_mod
5638
5639 -a always,exit -F arch=b32 -S fchownat -F auid>=500 -F auid!=4294967295 -k
5640 perm_mod
5641 -a always,exit -F arch=b32 -S fchownat -F auid=0 -k perm_mod
5642 -a always,exit -F arch=b64 -S fchownat -F auid>=500 -F auid!=4294967295 -k
5643 perm_mod
5644 -a always,exit -F arch=b64 -S fchownat -F auid=0 -k perm_mod
5645
5646 -a always,exit -F arch=b32 -S fremovexattr -F auid>=500 -F
5647 auid!=4294967295 -k perm_mod
5648 -a always,exit -F arch=b32 -S fremovexattr -F auid=0 -k perm_mod
5649 -a always,exit -F arch=b64 -S fremovexattr -F auid>=500 -F
5650 auid!=4294967295 -k perm_mod
5651 -a always,exit -F arch=b64 -S fremovexattr -F auid=0 -k perm_mod
5652
5653 -a always,exit -F arch=b32 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k
5654 perm_mod
5655 -a always,exit -F arch=b32 -S fsetxattr -F auid=0 -k perm_mod
5656 -a always,exit -F arch=b64 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k
5657 perm_mod
5658 -a always,exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
5659
5660 -a always,exit -F arch=b32 -S lchown -F auid>=500 -F auid!=4294967295 -k
5661 perm_mod
5662 -a always,exit -F arch=b32 -S lchown -F auid=0 -k perm_mod
5663 -a always,exit -F arch=b64 -S lchown -F auid>=500 -F auid!=4294967295 -k
5664 perm_mod
5665 -a always,exit -F arch=b64 -S lchown -F auid=0 -k perm_mod
5666
```

```

5667 -a always,exit -F arch=b32 -S lremovexattr -F auid>=500 -F
5668 auid!=4294967295 -k perm_mod
5669 -a always,exit -F arch=b32 -S lremovexattr -F auid=0 -k perm_mod
5670 -a always,exit -F arch=b64 -S lremovexattr -F auid>=500 -F
5671 auid!=4294967295 -k perm_mod
5672 -a always,exit -F arch=b64 -S lremovexattr -F auid=0 -k perm_mod
5673
5674 -a always,exit -F arch=b32 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k
5675 perm_mod
5676 -a always,exit -F arch=b32 -S lsetxattr -F auid=0 -k perm_mod
5677 -a always,exit -F arch=b64 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k
5678 perm_mod
5679 -a always,exit -F arch=b64 -S lsetxattr -F auid=0 -k perm_mod
5680
5681 -a always,exit -F arch=b32 -S removexattr -F auid>=500 -F auid!=4294967295 -k
5682 perm_mod
5683 -a always,exit -F arch=b32 -S removexattr -F auid=0 -k perm_mod
5684 -a always,exit -F arch=b64 -S removexattr -F auid>=500 -F auid!=4294967295 -k
5685 perm_mod
5686 -a always,exit -F arch=b64 -S removexattr -F auid=0 -k perm_mod
5687
5688 -a always,exit -F arch=b32 -S setxattr -F auid>=500 -F auid!=4294967295 -k
5689 perm_mod
5690 -a always,exit -F arch=b32 -S setxattr -F auid=0 -k perm_mod
5691 -a always,exit -F arch=b64 -S setxattr -F auid>=500 -F auid!=4294967295 -k
5692 perm_mod
5693 -a always,exit -F arch=b64 -S setxattr -F auid=0 -k perm_mod
5694

```

5695 17.14.7 **Sysctl.conf** Files Contents

```

5696 # System default settings live in /usr/lib/sysctl.d/00-system.conf.
5697 # To override those settings, enter new settings here, or in an
5698 /etc/sysctl.d/<name>.conf file
5699 #
5700 # For more information, see sysctl.conf(5) and sysctl.d(5).
5701 net.ipv4.ip_forward = 0
5702 net.ipv4.conf.all.accept_source_route = 0
5703 net.ipv4.conf.all.accept_redirects = 0
5704 net.ipv4.conf.all.secure_redirects = 0
5705 net.ipv4.conf.all.log_martians = 1
5706 net.ipv4.conf.default.accept_source_route = 0
5707 net.ipv4.conf.default.secure_redirects = 0
5708 net.ipv4.conf.default.accept_redirects = 0
5709 net.ipv4.icmp_echo_ignore_broadcasts = 1
5710 net.ipv4.icmp_ignore_bogus_error_responses = 1
5711 net.ipv4.tcp_syncookies = 1
5712 net.ipv4.conf.all.rp_filter = 1
5713 net.ipv4.conf.default.rp_filter = 1
5714 net.ipv6.conf.default.accept_redirects = 0
5715 net.ipv4.conf.default.send_redirects = 0
5716 net.ipv4.conf.all.send_redirects = 0
5717

```

5718 17.14.8 **system-auth** File Contents

5719 # %PAM-1.0

5720 # This file is auto-generated.

5721 # User changes will be destroyed the next time authconfig is run.

5722 auth required pam_env.so

5723 auth sufficient pam_unix.so try_first_pass

5724 auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800

5725 fail_interval=900

5726 auth required pam_faillock.so authsuc deny=3 unlock_time=604800

5727 fail_interval=900

5728 auth requisite pam_succeed_if.so uid >= 1000 quiet_success

5729 auth required pam_deny.so

5730

5731 account required pam_unix.so

5732 account sufficient pam_localuser.so

5733 account sufficient pam_succeed_if.so uid < 1000 quiet

5734 account required pam_permit.so

5735

5736 password required pam_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1

5737 ocredit=-1 lcredit=-1 difok=4

5738 password requisite pam_pwquality.so try_first_pass local_users_only

5739 retry=3 authtok_type=

5740 password sufficient pam_unix.so sha512 shadow try_first_pass use_authtok

5741 password required pam_deny.so

5742

5743 session optional pam_keyinit.so revoke

5744 session required pam_limits.so

5745 -session optional pam_systemd.so

5746 session [success=1 default=ignore] pam_succeed_if.so service in crond

5747 quiet use_uid

5748 session required pam_unix.so

5749 session required pam_lastlog.so showfailed

5750 session required pam_limits.so

5751

5752 17.14.9 **system-auth-ac** File Contents

5753 # %PAM-1.0

5754 # This file is auto-generated.

5755 # User changes will be destroyed the next time authconfig is run.

5756 auth required pam_env.so

5757 auth sufficient pam_unix.so try_first_pass

5758 auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800

5759 fail_interval=900

5760 auth required pam_faillock.so authsuc deny=3 unlock_time=604800

5761 fail_interval=900

5762 auth requisite pam_succeed_if.so uid >= 1000 quiet_success

5763 auth required pam_deny.so

5764

5765 account required pam_unix.so

5766 account sufficient pam_localuser.so

5767 account sufficient pam_succeed_if.so uid < 1000 quiet

5768 account required pam_permit.so

5769

```

5770 password required pam_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1
5771 ocredit=-1 lcredit=-1 difok=4
5772 password requisite pam_pwquality.so try_first_pass local_users_only
5773 retry=3 authtok_type=
5774 password sufficient pam_unix.so sha512 shadow try_first_pass use_authok
5775 password required pam_deny.so
5776
5777 session optional pam_keyinit.so revoke
5778 session required pam_limits.so
5779 -session optional pam_systemd.so
5780 session [success=1 default=ignore] pam_succeed_if.so service in crond
5781 quiet use_uid
5782 session required pam_unix.so
5783 session required pam_lastlog.so showfailed
5784 session required pam_limits.so
5785

```

5786 [17.15 BASELINE CENTOS 7 STIG COMPLIANCE](#)

5787 Note the STIG compliance test is based on the CentOS 6 STIG compliance analysis. At the time
 5788 this testing was completed the CentOS 7 STIG had not been published.
 5789 Introduction

5790 Test Result

Result ID	Profile	Start time	End time	Benchmark	Benchmark version
xccdf_org.open-scap_testresult_default-profile	(Default profile)	2015-03-11 12:25	2015-03-11 12:26	embedded	1

5791 Target info

Targets	Addresses	Platform
• localhost.localdomain	<ul style="list-style-type: none"> • 127.0.0.1 • 10.32.2.59 • 0:0:0:0:0:0:1 • fe80:0:0:0:250:56ff:fe89:5cab 	<ul style="list-style-type: none"> • cpe:/o:redhat:enterprise_linux:6

5792 Score

system	score	max	%	bar
urn:xccdf:scoring:default	96.65	100.00	96.65%	

5793 Results overview

5794 Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
173	0	6	0	0	0	0	0	0	179

5795 17.15.1 Rule Results Summary

Title	Result
Auditing must be enabled at boot by setting a kernel parameter.	fail
The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).	fail
The system boot loader configuration file(s) must be owned by root.	fail
The system boot loader configuration file(s) must be group-owned by root.	fail
The system boot loader configuration file(s) must have mode 0600 or less permissive.	fail
The system boot loader must require authentication.	fail

5796

18 ACRONYMS

Acronym	Literal Translation
AD	Active Directory
CA	Certificate authority (also used as shorthand for the name of the company “CA Technologies”)
CIP	Critical Infrastructure Protection
.csv	Comma-Separated Value
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
EMS	Energy Management System
ICS	Industrial Control System
IdAM	Identity and Access Management
iEMS	RADiFlow ICS/SCADA router configuration management software
ISE	Identity Services Engine
iSIM	Industrial Service Management Tool
IT	Information Technology
JRE	Java Runtime Environment
NAS	Network Attached Storage
NCCoE	National Cybersecurity Center of Excellence
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OS	Operating System
OT	Operational Technology
PACS	Physical Access Control System

Acronym	Literal Translation
PLC	Programmable Logic Controller
RAM	Random Access Memory
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
STIG	Security Technical Implementation Guideline
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAR	Web Application Archive

LIST OF FIGURES

Figure 1. Management and production networks	7
Figure 2. IdAM build implementation production network.....	8
Figure 3. Build Network	10
Figure 4. Build #1 IdAM Network.....	11
Figure 5. Build #2 IdAM Network.....	12
Figure 6. IT Network.....	13
Figure 7 OT Network	14
Figure 8 PACS Network.....	15
Figure 9. IMG Attributes Window	55
Figure 10. IMG Edit User	55
Figure 11. IMG Attributes Examples	56
Figure 12. IMG Attributes Examples	57
Figure 13. IMG Attributes Examples	57
Figure 14. IMG Edit Attributes	57
Figure 15. IMG Attribute Example	58
Figure 16. IMG Resources Directories.....	59
Figure 17. IMG Create Directory	59
Figure 18. IMG Create Directory	59
Figure 19. IMG Directory Information	60
Figure 20. IMG Create Directory	61
Figure 21. IMG Directories	62
Figure 22. IMG Directories	62

Figure 23. IMG Create Identity Collector	63
Figure 24. IMG HR Identities	64
Figure 25. IMG HR Identities (cont.)	64
Figure 26. IMG HR Identities - Users	65
Figure 27. IMG HR Identities	66
Figure 28. IMG HR Identities (cont.)	67
Figure 29. IMG Adaptive Directory Container	68
Figure 30. IMG Identity Collector	69
Figure 31. IMG AD Identity Collector	69
Figure 32. IMG AD Identity Collector	70
Figure 33. IMG AD Identity Collector	70
Figure 34. IMG AD Identity Collector	71
Figure 35. IMG AD Identity Collector	72
Figure 36. IMG AD Create Account Collector	73
Figure 37. IMG Edit Collector	74
Figure 38. IMG Edit Collector	74
Figure 39. IMG Edit Collector	74
Figure 40. IMG Edit Collector	75
Figure 41. IMG Edit Collector	75
Figure 42. IMG Edit Collector	76
Figure 43. IMG Edit Collector	77
Figure 44. IMG Edit Collector	77
Figure 45. IMG Edit Collector	77
Figure 46. IMG Edit Collector	77
Figure 47. IMG Account Test	78
Figure 48. IMG Successful Test Example	78
Figure 49. IMG Unification Configuration	79
Figure 50. IMG Participating Collectors	79
Figure 51. IMG Edit Participating Collectors	80
Figure 52. IMG Edit Participating Collectors	80
Figure 53. IMG Unification Configuration Attribute Sources	81
Figure 54. IMG Edit User Attribute Mapping	82
Figure 55. IMG Edit User Attribute Mapping	82
Figure 56. IMG Unification Configuration Joins	83
Figure 57. IMG Edit Joins	83
Figure 58. IMG Start Data Collection	84
Figure 59. IMG Collect Data	84
Figure 60. IMG Data Collection Monitoring	85
Figure 61. IMG Data Collection Review	86
Figure 62. IMG Roles	86
Figure 63. IMG Discover Roles	87
Figure 64. IMG Discover Roles	88
Figure 65. IMG Discover Roles	88
Figure 66. IMG Discover Roles	88

Figure 67. IMG Discover Roles	89
Figure 68. IMG Roles Definitions.....	90
Figure 69. IMG New User.....	90
Figure 70. IMG New User.....	91
Figure 71. IMG User Termination.....	92
Figure 72. IMG User Termination.....	93
Figure 73. IMG Request Configuration.....	93
Figure 74. IMG Account Template.....	93
Figure 75. IMG IT Account Template.....	94
Figure 76. IMG AFX Connectors	94
Figure 77. IMG Create Connector	95
Figure 78. IMG AD Connector AFX Server.....	95
Figure 79. IMG AD Connector AFX Server.....	97
Figure 80. IMG AD Connector AFX Server.....	98
Figure 81. IMG AD Connector AFX Server.....	98
Figure 82. IMG AD Connector IT	99
Figure 83. IMG AD Connector IT Capability Configuration	100
Figure 84. IMG AD Connector IT Capability Configuration	101
Figure 85. IMG AD Connector IT Capability Configuration	101
Figure 86. IMG AD Connector IT Capability Configuration	102
Figure 87. IMG AD Connector IT Capability Configuration	103
Figure 88. IMG AD Connector IT Capability Configuration	103
Figure 89. IMG AD Connector IT Capability Configuration	103
Figure 90. IMG AD Connector IT Capability Configuration	104
Figure 91. IMG AD Connector IT Capability Configuration	104
Figure 92. IMG AD Connector IT Capability Configuration	105
Figure 93. IMG AD Connector IT Capability Configuration	105
Figure 94. IMG AD Connector IT Capability Configuration	106
Figure 95. IMG AD Connector IT Capability Configuration	107
Figure 96. IMG AD Connector IT Capability Configuration	107
Figure 97. IMG Resources Directories.....	108
Figure 98. IMG AD Accounts	109
Figure 99. IMG AD AFX Connector Binding.....	109
Figure 100. IMG Resources Directories.....	110
Figure 101. IMG Collect Data	110
Figure 102. IMG Requests Activities	111
Figure 103. IMG Accepted Access Request.....	111
Figure 104. IMG Requests	112
Figure 105. IMG New User Provisioned	113
Figure 106. IMG Successful User Add	113
Figure 107. IMG Requests Activities	114
Figure 108. IMG Request Status.....	115
Figure 109. Adaptive Directory Login Page	122
Figure 110. Adaptive Directory Main Page	122

Figure 111. Adaptive Directory Tools Page	123
Figure 112. Adaptive Directory Server Backend Settings	123
Figure 113. Adaptive Directory LDAP Data Source	124
Figure 114. Adaptive Directory Configuration of Naming Context	125
Figure 115. Adaptive Directory New Naming Context	125
Figure 116. Adaptive Directory Configure Virtual Tree	126
Figure 117. Adaptive Directory Virtual Tree	126
Figure 118. Adaptive Directory Create New Level	127
Figure 119. Adaptive Directory New Level Name	127
Figure 120. Adaptive Directory Backend Mapping	128
Figure 121. Adaptive Directory Backend Mapping	129
Figure 122. Adaptive Directory Configure LDAP Backend	129
Figure 123. Adaptive Directory Addition Attributes	130
Figure 124. Adaptive Directory Add/Edit Main Attribute	130
Figure 125. Adaptive Directory Edit Collector	131
Figure 126. Adaptive Directory Search Configuration for Accounts	131
Figure 127. Adaptive Directory Search Configuration for Accounts	135
Figure 128. Guardian ActiveMQ Home/Data Directory	136
Figure 129. Guardian ActiveMQ	138
Figure 130. Guardian DB Connector Attributes	146
Figure 131. Guardian Identity Configuration	151
Figure 132. Guardian Recon Authoritative Fields	151
Figure 133. Guardian DB Connector Attribute Mapping	153
Figure 134. Guardian User Policy	156
Figure 135. Guardian Reconciliation Job	160
Figure 136. Guardian DB Connector Attributes	163
Figure 137. Create DropDownValues	173
Figure 138. Contractor Field	173
Figure 139. DropDownValues	174
Figure 140. InActive	174
Figure 141. Guardian Identity Configuration	174
Figure 142. Authoritative Fields	176
Figure 143. Guardian Recon Authoritative Fields	176
Figure 144. External Provisioning Attribute	177
Figure 145. Attribute Fields	177
Figure 146. Provisioning Mapping	178
Figure 147. Guardian DB Connector Attribute Mapping	178
Figure 148. Policy Rules	179
Figure 149. Rule Conditions	179
Figure 150. Rule Conditions	180
Figure 151. Default Access	181
Figure 152. Modify Task	182
Figure 153. Policy Designer	183
Figure 154. Toolbar	183

Figure 155. Guardian User Policy	185
Figure 156. Tasks Popup	185
Figure 157. Guardian Reconciliation Job	189
Figure 158. Ozone Proof Settings	197
Figure 159. Ozone Authority Web Service	198
Figure 160. Ozone Authority Connection Information	206
Figure 161. Ozone LDAP Publication Point	207
Figure 162. Ozone Directory Connection Information	207
Figure 163. Ozone Import Group from Directory	208
Figure 164. Ozone New Proof Information	209
Figure 165. Ozone New Proof Administrators	210
Figure 166. Ozone Peer Proofs	211
Figure 167. Ozone Add Authorization Proof	212
Figure 168. Ozone Server Configuration	213
Figure 169. Ozone New Proof Information	219
Figure 170. Ozone New Proof Authentication CRLs	220
Figure 171. Ozone New Proof Authentication Source Configuration	221
Figure 172. Ozone Envoy Configuration	222
Figure 173. GlobalSign Overview	223
Figure 174. GlobalSign Login Page	225
Figure 175. GlobalSign Enterprise PKI Tab	225
Figure 176. GlobalSign Order Licenses Page	225
Figure 177. GlobalSign License Selection Page	226
Figure 178. GlobalSign Product Details	226
Figure 179. GlobalSign Payment Details	227
Figure 180. GlobalSign Confirm Details	227
Figure 181. GlobalSign Order Additional Profiles	227
Figure 182. GlobalSign Certificate Profile Details	228
Figure 183. GlobalSign Confirm Details	229
Figure 184. GlobalSign View Admin Menu Options	229
Figure 185. GlobalSign Order Certificates	230
Figure 186. GlobalSign Product Selection	230
Figure 187. GlobalSign Certificate Identity Details	231
Figure 188. GlobalSign Confirm Details	232
Figure 189. Create New Project	233
Figure 190. New Project Wizard	234
Figure 191. Project Protection	235
Figure 192. Administrator Password	236
Figure 193. Project Explorer Window	236
Figure 194. Tofino SA/MAC Address	237
Figure 195. Project Explorer	237
Figure 196. New Asset	238
Figure 197. Project Explorer Assets Icon	239
Figure 198. Project Explorer Tofino SA Icon	240

Figure 199. Rule Type.....	241
Figure 200. Firewall Rule Wizard.....	241
Figure 201. Asset Rule Profiles.....	242
Figure 202. Protocol Window	243
Figure 203. Rule Table	244
Figure 204. Save rules in Project Explorer	244
Figure 205. Apply Configuration Pane	245
Figure 206. Loadable USB Drive Popup.....	246

LIST OF TABLES

Table 1. Build Implementation Component List (including security controls).....	3
Table 2 Build IP Address Assignments.....	16
Table 3. Border Firewall Rules.....	19
Table 4. Border Firewall Rules (continued)	20
Table 5. IdAM Firewall Rules	21
Table 6. IT Firewall Rules	21
Table 7. OT Firewall Rules	22
Table 8. PACS Firewall Rules.....	24
Table 9. Guardian PACS AD Parameters	146
Table 10. Guardian Identity DB Parameters.....	148
Table 11. Guardian ACCESSIT PACS Parameters.....	149
Table 12. Guardian Policy Engine Rules	153
Table 13. Guardian Policy Engine Suggest/Default Access	154
Table 14. Guardian Policy Engine Rule Action Handler.....	154
Table 15. Guardian User Policy	156
Table 16. Guardian Job Scheduler Triggers Field Map	158
Table 17. Guardian Job Scheduler Triggers	158
Table 18. Guardian Name and Label Fields.....	161
Table 19. Guardian Manual Configuration System Parameters	163
Table 20. Guardian Identity DB Parameters.....	166
Table 21. Guardian PACS DBConnector Parameters	167
Table 22. PacsAllDoors Attributes	169
Table 23. PacsHomeAccess Attributes	170
Table 24. PacsWorkAccess Attributes	170
Table 25. FacilityCode Attributes	171
Table 26. PIN Atributes.....	172
Table 27. User Field Mapping Table	175
Table 28. Guardian Manual Configuration Policy Engine Rules	180
Table 29. Manual Configuration Policy Engine Suggest/Default Access	181
Table 30. Condition Decision Values	186
Table 31. Guardian Job Scheduler Triggers Field Map	187

Table 32. Guardian AlertEnterprise DB Trigger	187
---	-----