

Identity and Access Management for Electric Utilities

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE) developed an example solution that electric sector businesses can use to more securely and efficiently manage access to the networked devices and facilities upon which power generation, transmission, and distribution depend.
- The security characteristics in our access management platform are informed by guidance and best practices from standards organizations, including the North American Electric Reliability Corporation’s (NERC) Critical Infrastructure Protection (CIP) standards.
- The NCCoE’s approach uses commercially available products that can be included alongside your current products in your existing infrastructure. They provide a centralized system with a comprehensive view of all users within the enterprise and across the IT, operational, and access control silos often found in electric companies.
- The example solution is packaged as a “How To” guide that demonstrates implementation of standards-based cybersecurity technologies in the real world, based on risk analysis. The guide helps organizations gain efficiencies in access management, while saving them research and proof of concept costs.

THE CHALLENGE

The electric power industry is upgrading older, outdated infrastructure to take advantage of emerging technologies that will create “a platform [that] efficiently [integrates] new energy resources, new technologies, and new devices into the system.”* The ever greater numbers of technologies, devices, and systems connected to utilities’ grid networks need protection from physical and cybersecurity attacks.†

Our conversations with utility company employees confirmed that current identity and access management (IdAM) implementations are often decentralized and controlled by numerous departments within a company. Several negative outcomes can result from this: an increased risk of attack and service disruption, inability to identify potential sources of a problem or attack, and a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets.

To better protect power generation, transmission, and distribution, electric companies need to be able to control access to their networked resources, including buildings, equipment, information technology, and industrial control systems—all of which have unique technical and political challenges.‡ Identity and access management (IdAM) systems for these assets often exist in silos, and employees who manage these systems lack methods to effectively coordinate access to devices and facilities in these silos. This drives inefficiency and can result in security risks for utilities, according to our electric sector stakeholders.

* Thought Leaders Speak Out: The Evolving Electric Power Industry, The Edison Foundation Institute, June 2015.

† State of the Electric Utility 2015, Utility Dive, January 2015.

‡ Protect Critical Infrastructure, McAfee, 2012.

Imagine that a technician has access to several substations and remote terminal units connected to the company's network in those substations. The technician moves out of the region, so she quits her job. Without a centralized IdAM system, managing her access to various facilities and systems can be cumbersome and time-consuming, even error-prone. Electric utilities need the ability to provide the right person with the right degree of access to the right resources at the right time, and quickly.

THE SOLUTION

The NIST Cybersecurity Practice Guide "Identity and Access Management" demonstrates how commercially available technologies can meet your utility's need to control access to resources across the enterprise.

In our lab at the NCCoE, part of the National Institute of Standards and Technology (NIST), we built an environment that simulates an electric company's IT architecture, including the typical technology silos found in a utility (such as IT, operational technology, and physical access control systems).

We show how an electric utility can implement a centralized IdAM platform to provide a comprehensive view of all users within the enterprise across all silos, and the access rights they have been granted, by using multiple commercially available products.

The guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations, and to NERC CIP standards
- provides
 - a detailed example solution with capabilities that address security controls
 - a demonstrated approach using multiple products that achieve the same result
 - instructions for implementers and security engineers, including examples of all the necessary components and installation, configuration, and integration
- uses products that are readily available and interoperable with your existing information technology infrastructure and investments
- is modular and suitable for organizations of all sizes, including corporate and regional business offices, power generation plants, and substations

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee regulatory compliance. Your utility's information security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your company can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Our example solution has the following benefits:

- products and capabilities can be adopted on a component-by-component basis, or as a whole, thereby minimizing impact to the enterprise and existing infrastructure
- can reduce the risk of malicious or untrained people gaining unauthorized access to critical infrastructure components and interfering with their operation, thereby lowering overall business risk
- allows rapid provisioning and de-provisioning of access from a centralized platform, so IT personnel can spend more time on other critical tasks

- improves situational awareness: proper access and authorization can be confirmed via the use of a single, centralized solution
- improves security posture by tracking and auditing access requests and other IdAM activity across all networks
- can enhance the productivity of employees and speed delivery of services, and support oversight of resources, including information technology, personnel, and data

SHARE YOUR FEEDBACK

You can get the guide at <http://nccoe.nist.gov> and help improve it by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email energy_nccoe@nist.gov
- participate in our forums at <http://nccoe.nist.gov/forums/energy>

Or learn more by arranging a demonstration of this reference solution by contacting us at energy_nccoe@nist.gov.

TECHNOLOGY PARTNERS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution.



IDENTITY AND ACCESS MANAGEMENT FOR ELECTRIC UTILITIES

Approach, Architecture, and Security Characteristics

For CIOs, CISOs, and Security Managers

Jim McCarthy

Don Faatz

Harry Perper

Chris Peloquin

John Wiltberger

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-2b

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 1800-2b
Natl. Inst. Stand. Technol. Spec. Publ. 1800-2b, 98 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

The NCCoE wishes to acknowledge the special contributions of Nadya Bartol, Senior Cybersecurity Strategist, Utilities Telecom Council; Jonathan Margulies, formerly with NCCoE and now with Qmulos; and Victoria Pillitteri of NIST, who were instrumental in the initial definition and development of the Identity and Access Management use case. Paul Timmel, formerly detailed to NCCoE from the National Security Agency, helped with these stages and also helped to get the project build started.

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 Lobo	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 Vital	XTec
Mari Devitte	XTec
David Hellbock	XTec
John Schiefer	XTec

Table of Contents

Disclaimer.....	i
National Cybersecurity Center of Excellence.....	iii
NIST Cybersecurity Practice Guides.....	iii
Abstract.....	iii
Keywords.....	iv
List of Figures.....	vii
List of Tables.....	viii
1 Summary.....	9
1.1 The Challenge.....	9
1.2 The Solution.....	10
1.3 Risks.....	11
1.4 Benefits.....	12
1.5 Technology Partners.....	12
1.6 Feedback.....	13
2 How to Use This Guide.....	14
3 Introduction.....	15
4 Approach.....	16
4.1 Audience.....	16
4.2 Scope.....	16
4.3 Risk Assessment and Mitigation.....	18
4.4 Technologies.....	25
5 Architecture.....	29
5.1 Example Solution Description.....	29
5.2 Example Solution Relationship to Use Case.....	36
5.3 Core Components of the Reference Architecture.....	37
5.4 Supporting Components of the Reference Architecture.....	42
5.5 Build #3 - An Alternative Core Component Build of the Example Solution.....	45
5.6 Build Implementation Description.....	46
5.7 Data.....	64
5.8 Security Characteristics Related to NERC-CIP.....	65
5.9 Evaluation of Security Characteristics.....	66

6	Functional Evaluation	79
6.1	IdAM Functional Test Plan	80
6.2	IdAM Use Case Requirements	81
6.3	Test Case: IdAM-1	83
6.4	Test Case IdAM-2	86
6.5	Test Case IdAM-3	88
	Appendix A: Acronyms.....	91
	Appendix B: References	92
	Appendix C: Mount Airey Group, Inc. Personal Profile Applications Demonstration Application	94
	Search Results:	96

LIST OF FIGURES

Figure 1. IdAM capabilities.....	29
Figure 2. IdAM example solution	31
Figure 3. Notional PACS architecture	34
Figure 4. Notional OT silo architecture	35
Figure 5. Notional IT silo architecture.....	36
Figure 6. Build #1	38
Figure 7. Build #2	40
Figure 8. Supporting components.....	44
Figure 9. Build #3	45
Figure 10. Management and production networks	50
Figure 11. IdAM build architecture production network.....	51
Figure 12. OT network.....	53
Figure 13. IT network	54
Figure 14. PACS network	55
Figure 15. Central IdAM network, Build #1.....	56
Figure 16. Central IdAM network, Build #2.....	58

Figure 17. Access and authorization information flow for OT ICS/SCADA devices.....	60
Figure 18. Access and authorization information flow for the PACS network, Build #1.....	62
Figure 19. Access and authorization information flow for the PACS network, Build #2.....	63
Figure 20. Access and authorization information flow for the IT network.....	64
Figure 21. Example process for determining the security standards-based attributes for the example solution.....	70

LIST OF TABLES

Table 1. Use Case Security Characteristics Mapped to Relevant Standards and Controls.....	21
Table 2. Products and Technologies Used to Satisfy Security Control Requirements	25
Table 3. Build Architecture Component List	47
Table 4. NERC-CIP Requirements	65
Table 5. IdAM Components and Security Capability Mapping	68
Table 6. Test Case Fields	80
Table 7. IdAM Functional Requirements.....	81
Table 8. Test Case ID: IdAM-1.....	83
Table 9. Test Case ID: IdAM-2.....	86
Table 10. Test Case ID: IdAM-3.....	88

1 1 SUMMARY

2 When the National Cybersecurity Center of Excellence (NCCoE) met with electricity subsector
3 stakeholders, they told us they need a more secure and efficient way to protect access to
4 networked devices and facilities. The NCCoE developed an example solution to this problem
5 using commercially available products.

6 The NCCoE's approach provides a centralized access management system that reduces risk of
7 disruption of service by reducing opportunities for cyberattack or human error.

8 This example solution is packaged as a "How To" guide that demonstrates how to implement
9 standards-based cybersecurity technologies in the real world, based on risk analysis and
10 regulatory requirements. The guide helps organizations gain efficiencies in identity and access
11 management, while saving them research and proof of concept costs.

12 1.1 The Challenge

13 The electric power industry is upgrading older, outdated infrastructure to take advantage of
14 emerging technologies that will create "a platform [that] efficiently [integrates] new energy
15 resources, new technologies, and new devices into the system."¹ The ever greater numbers of
16 technologies, devices, and systems connected to utilities' grid networks need protection from
17 physical and cybersecurity attacks.²

18 IdAM implementations in the electricity subsector are often decentralized and controlled by
19 numerous departments within an energy company. Several negative outcomes can result from
20 this: an increased risk of attack and service disruption, inability to identify potential sources of a
21 problem or attack, and a lack of overall traceability and accountability regarding who has access
22 to both critical and noncritical assets.

23 To better protect power generation, transmission, and distribution, energy companies need to
24 be able to control physical and logical access to their networked resources, including buildings,
25 equipment, information technology, and industrial control systems (ICS)—all of which have
26 unique technical and political challenges.³ Identity and access management (IdAM) systems for
27 these assets often exist in silos, and employees who manage access to these systems lack
28 methods to effectively coordinate access to devices and facilities in these silos. This drives
29 inefficiency and creates security risks, according to our electric utility stakeholders.

30 We considered a scenario in which a utility technician has access to several physical substations
31 and remote terminal units connected to the company's network in those substations. Personal

¹ Thought Leaders Speak Out: The Evolving Electric Power Industry, The Edison Foundation Institute, June 2015.

² State of the Electric Utility 2015, Utility Dive, January 2015.

³ Protect Critical Infrastructure, McAfee, 2012.

32 matters require the technician to move out of the region, so she terminates her employment at
33 the company. Without a centralized IdAM system, managing routine events like this one can
34 become cumbersome and time-consuming. How can energy companies be confident that
35 access to the appropriate physical and technological resources across the enterprise is granted
36 or revoked correctly, and in a timely fashion?

37 As this scenario shows, energy companies need to be able to authenticate the individuals and
38 systems to which they are giving access rights with a high degree of certainty. In addition,
39 energy companies need to be able to enforce access control policies (e.g., allow, deny, inquire
40 further) consistently, uniformly and quickly across resources.

41 1.2 The Solution

42 The example solution we propose demonstrates the following capabilities:

- 43 • centrally assigns and provisions access privileges to users based on a set of programmed
44 business rules for IT, OT, and physical resources
- 45 • creates, activates, and deactivates users for IT, OT, and physical resources
- 46 • provides a view of all user accounts within the enterprise and the access rights they have
47 been granted
- 48 • can change an existing user's access to one or more resources

49 We accomplished this solution through deployment of a single centralized IdAM platform that
50 implements:

- 51 • an IdAM workflow to manage the overall process and to require explicit approval of
52 requests to access certain resources
- 53 • an identity store, which is the authoritative source for digital identities and their
54 associated access rights to resources
- 55 • a provisioning capability to populate information from the workflow and identity store
56 into the run-time capabilities

57 These combined capabilities can greatly reduce the time to update access to IT, OT, and
58 physical resources. They reduce opportunities for attack or error and lower the impact of
59 identity and access incidents on energy delivery, thereby lowering overall business risk. They
60 also improve a company's security posture by integrating all the IdAM-related audit logs into
61 one, greatly improving visibility into authentication and authorization activities. Another benefit
62 of this example solution is that it supports use of multiple digital identities by a single person. A
63 current employee is likely to have several distinct digital identities because of independent
64 management of digital identities across IT, OT, and physical resources.

65 The guide:

- 66 • maps security characteristics to guidance and best practices from standards
67 organizations, including the North American Electric Reliability Corporation's (NERC)

68 Critical Infrastructure Protection (CIP) standards and NIST SP 800-53, Rev.4, " *Security*
69 *and Privacy Controls for Federal Information Systems and Organizations* "

- 70 • provides a
 - 71 ○ detailed example solution and capabilities that address security controls
 - 72 ○ demonstrated approach using multiple products to achieve the same result
 - 73 ○ how-to for implementers and security engineers with instructions on how the
 - 74 example solution can be integrated and configured into their enterprises in a
 - 75 manner that achieves security goals, with minimum impact on operational
 - 76 efficiency and expense

77 Commercial, standards-based products, like the ones we used, are readily available and
78 interoperable with existing information technology infrastructure and investments. While our
79 simulated environment may be most similar in breadth and diversity to the widely distributed
80 networks of large organizations, this guide is modular and provides guidance on
81 implementation of unified IdAM capabilities to organizations of all sizes. These include, but are
82 not limited to, corporate and regional business offices, power generation plants, and
83 substations.

84 This guide lists all the necessary components and provides installation, configuration, and
85 integration information so that an energy company can replicate what we have built. While we
86 have used a suite of commercial products to address this challenge, this guide does not endorse
87 these particular products. Your utility's security experts should identify the standards-based
88 products that will best integrate with your existing tools and IT system infrastructure. Your
89 company can adopt this solution or one that adheres to these guidelines in whole, or you can
90 use this guide as a starting point for tailoring and implementing parts of a solution.

91 **1.3 Risks**

92 While risk is addressed in current industry standards, such as NERC CIP, our sector partners told
93 us about additional risk considerations at both the operational and strategic levels.

94 Operationally, a lack of a centralized IdAM platform can increase the risk of people gaining
95 unauthorized access to critical infrastructure components. Once unauthorized access is gained,
96 the risk surface increases and the opportunity for introduction of additional threats to the
97 environment, such as malware and denial of service (especially oriented towards OT) is
98 realized.

99 At the strategic level, you might consider the cost of mitigating these risks and the potential
100 return on your investment in implementing a product (or multiple products). You may also
101 want to assess if a centralized IdAM system can help enhance the productivity of employees
102 and speed delivery of services, and explore if it can help support oversight of resources,
103 including information technology, personnel, and data. This example solution addresses
104 imminent operational security risks and incorporates strategic risk considerations, too.

105 Adopting any new technology can introduce new risks to your enterprise. We understand that
106 this example solution to mitigate the risks of decentralized IdAM may, in turn, introduce new
107 risks. By centralizing IdAM functions, we decrease the risk that multiple IdAM platforms can be
108 infiltrated to gain unauthorized access to networked devices. We recognize, however, that
109 centralizing IdAM functions may provide a point of single infiltration of multiple critical systems
110 (OT, PACS, and IT). We address this key risk in detail in Section 5.9.5.1 Threats, Vulnerabilities
111 and Assumptions, and provide a comprehensive list of mitigations in Section 5.9.6, Security
112 Recommendations.

113 1.4 Benefits

114 The example solution described in this guide has the following benefits:

- 115 • products and capabilities can be adopted on a component-by-component basis, or as a
116 whole
- 117 • minimizes impact to the enterprise and existing infrastructure
- 118 • reduces opportunities for attack or error, and impact of identity and access incidents on
119 energy delivery, thereby lowering overall business risk
- 120 • allows rapid provisioning and de-provisioning of access from a centralized platform, so IT
121 personnel can spend more time on other critical tasks
- 122 • improves situational awareness: proper access and authorization can be confirmed via
123 the use of a single, centralized solution
- 124 • improves security posture by tracking and auditing access requests and other IdAM
125 activity across all networks

126 1.5 Technology Partners

127 The technology vendors who participated in this build submitted their capabilities in response
128 to a notice in the Federal Register. Companies with relevant products were invited to sign a
129 Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to
130 participate in a consortium to build this example solution. We worked with:

- 131 • AlertEnterprise
- 132 • CA Technologies
- 133 • Cisco Systems, Inc.
- 134 • GlobalSign
- 135 • Mount Airey Group
- 136 • RS2 Technologies
- 137 • RSA Security, LLC
- 138 • RADiFlow

-
- 139 • Schneider Electric
 - 140 • TDi Technologies
 - 141 • XTec, Inc.

142 **1.6 Feedback**

143 You can improve this guide by contributing feedback. As you review and adopt this solution for
144 your own organization, we ask you and your colleagues to share your experience and advice
145 with us.

- 146 • email energy_nccoe@nist.gov
- 147 • participate in our forums at <http://nccoe.nist.gov/forums/energy>

148 Or learn more by arranging a demonstration of this example solution by contacting us at
149 energy_nccoe@nist.gov.

150

151 2 HOW TO USE THIS GUIDE

152 This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and
153 provides users with the information they need to replicate this approach to identity and access
154 management. The example solution is modular and can be deployed in whole or in part.

155 This guide contains three volumes:

- 156 • NIST SP 1800-2a: Executive Summary
- 157 • **NIST SP 1800-2b: Approach, Architecture, and** ← **YOU ARE HERE**
158 **Security Characteristics – what we built and why**
- 159 • NIST SP 1800-2c: How To Guides – instructions for building the example solution

160 Depending on your role in your organization, you might use this guide in different ways:

161 **Energy utility leaders, including chief security and technology officers** will be interested in the
162 Executive Summary (NIST SP 1800-2a), which describes the:

- 163 • challenges electricity subsector organizations face in implementing and using IdAM
164 systems
- 165 • example solution built at the NCCoE
- 166 • benefits of adopting a secure, centralized IdAM system, and the risks of isolated,
167 decentralized systems

168 **Technology or security program managers** who are concerned with how to identify,
169 understand, assess, and mitigate risk, will be interested in this part of the guide, NIST SP1800-
170 2b, which describes what we did and why. The following sections will be of particular interest:

- 171 • Section 4.3, Risk Assessment and Mitigation, provides a detailed description of two
172 types of risk analysis we performed
- 173 • Table 1, Use Case Security Characteristics Mapped to Relevant Standards and Controls, in
174 Section 4.3, Risk Assessment and Mitigation, maps the security characteristics of this
175 example solution to cybersecurity standards and best practices, including NERC-CIP v.3
176 and v.5

177 IT professionals who want to implement an approach this like this will find the whole practice
178 guide useful. You can use the How-To portion of the guide, NIST Special Publication Series 1800-
179 2c, to replicate all or parts of the build created in our lab. The How-To guide provides specific
180 product installation, configuration, and integration instructions for implementing the example
181 solution. We do not recreate the product manufacturers' documentation, which is widely
182 available. Rather, we show how we incorporated the products together in our environment to
183 create an example solution.

184 This guide assumes that IT professionals have experience implementing security products in
185 energy industry organizations. While we have used a suite of commercial products to address

186 this challenge, this guide does not endorse these particular products.⁴ Your organization’s
187 security experts should identify the standards-based products that will best integrate with your
188 existing tools and IT system infrastructure. Your organization can adopt this solution or one that
189 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring
190 and implementing parts of a solution for operational technology systems (OT), physical access
191 control systems (PACS), and IT systems (IT). If you use other products, we hope you will seek
192 those that are congruent with applicable standards and best practices.

193 A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution.
194 This is a draft guide. We seek feedback on its contents and welcome your input. Comments,
195 suggestions, and success stories will improve subsequent versions of this guide. Please
196 contribute your thoughts to energy_nccoe@nist.gov, and join the discussion at
197 <http://nccoe.nist.gov/forums/energy>.

198 3 INTRODUCTION

199 The NCCoE initiated this project because IT security leaders in the electricity subsector told us
200 that IdAM was a concern to them. As we developed the original problem statement, or use
201 case, on which this project is based, we consulted with electric company chief information
202 officers, chief information security officers, security management personnel, and others with
203 financial decision-making responsibility (particularly for security).

204 The individuals we consulted told us that they need to control physical and logical access to
205 their resources, including buildings, equipment, IT, and industrial control systems. They need to
206 authenticate only designated individuals and devices to which they are giving access rights with
207 a high degree of certainty. In addition, they need to enforce access control policies (e.g., allow,
208 deny, inquire further) consistently, uniformly, and quickly across all of their resources. Current
209 IdAM implementations are often not centralized and are controlled by numerous departments
210 within an energy company. Several negative outcomes can result from this situation: an
211 increased risk of attack and service disruption, inability to identify potential sources of a
212 problem or attack, and a lack of overall traceability and accountability regarding who has access
213 to both critical and noncritical assets. Another key consideration is the need for companies to
214 demonstrate compliance with industry standards and/or government regulations.

215 We constructed two versions of an end-to-end identity management solution that provides
216 access control capabilities across the OT, PACS, and IT networks. We used the same approach
217 for each build in that we only interchanged two core products that contained the same

⁴ Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept. Such identification is not intended to imply recommendation or endorsement by NIST or the NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

218 functionality and capability. Sections 5.3.1 and 5.3.2 detail these two example solutions. The
219 end result is that a user’s access to facilities and devices can be provisioned from a single
220 console. Access privileges can be modified by adding new users and assigning access for the
221 first time, modifying existing user access privileges, or disabling user access privileges. Our goal
222 was to provide the electricity subsector with a solution that addresses the key tenet of
223 cybersecurity—access management/rights—based on the principle of least privilege.⁵

224 4 APPROACH

225 4.1 Audience

226 This guide is intended for individuals responsible for implementing IT security solutions in
227 electricity subsector organizations.

228 4.2 Scope

229 This project began with a detailed discussion between NCCoE and members of the electricity
230 subsector community of their main security challenges. The risk of unauthorized access to
231 facilities and devices and the inability to verify if user access had been properly established,
232 modified, or revoked quickly became the focus.

233 In response, the NCCoE drafted a use case that identified numerous desired solution
234 characteristics. After an open call in the Federal Register, we chose technology partners on the
235 basis of their ability to provide these characteristics. We initially thought it would be feasible to
236 include federation of identity management⁶ services in the scope. As we progressed through
237 the initial stages of solution development, we realized that access, authentication, and
238 authorization through federated identity means would vastly increase the amount of time
239 needed to complete a build. We narrowed the scope to providing identity management of
240 energy company employees including a centralized provisioning capability to the OT, PACS, and
241 IT networks. The scope became successful execution of the following provisioning functions:

- 242 1. enabling access for a new employee
- 243 2. modifying access for an existing employee
- 244 3. disabling access for a former employee

245 The objective is to perform all three actions from a single interface that can serve as the
246 authoritative source for all access managed within an energy provider’s facilities, networks, and
247 systems.

⁵ J. Saltzer, Protection and the control of information sharing in multics, Communication of the ACM, 17 (7), 388-402 (1974)

⁶ “Federated identity management (FIM) is an arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group.”
<http://searchsecurity.techtarget.com/definition/federated-identity-management>

248 4.2.1 Assumptions

249 4.2.1.1 Security

250 All network and system changes have the potential to increase the attack surface within an
251 enterprise. In Section 4.3, Risk Assessment and Mitigation, we provide detailed
252 recommendations on how to secure this reference solution.

253 4.2.1.2 Modularity

254 This example solution is made of many commercially available parts. You might swap one of the
255 products we used for one that is better suited for your environment. We also assume that you
256 already have some IdAM solutions in place. A combination of some of the components
257 described here, or a single component, can improve your identity and access/authorization
258 functions, without requiring you to remove or replace your existing infrastructure. This guide
259 provides both a complete end-to-end solution and options you can implement based on your
260 needs.

261 4.2.1.3 Human Resources Database/Identity Vetting

262 This build is based on a simulated environment. Rather than recreate a human resources (HR)
263 database and the entire identity vetting process in our lab, we assumed that your organization
264 has the processes, databases, and other components necessary to establish a valid identity.

265 4.2.1.4 Identity Federation

266 We initially intended to work with energy providers to demonstrate a means for sharing
267 selected identity information across organizational boundaries. While we assumed the NCCoE
268 could implement some type of identity federation mechanism to authenticate and authorize
269 individuals both internal and external to the organization, this capability exceeded the scope of
270 the build.

271 4.2.1.5 Technical Implementation

272 The guide is written from a “how-to” perspective. Its foremost purpose is to provide details on
273 how to install, configure, and integrate components. We assume that an energy provider has
274 the technical resources to implement all or parts of the build, or has access to companies that
275 can perform the implementation on its behalf.

276 4.2.1.6 Limited Scalability Testing

277 We experienced a major constraint in terms of replicating the user base size that would be
278 found at medium and large energy providers. We do not identify scalability thresholds in our
279 builds, as those depend on the type and size of the implementation and are particular to the
280 individual enterprise.

281 4.2.1.7 Replication of Enterprise Network

282 We were able to replicate the three silos: 1) physical access control systems, 2) information
283 technology or corporate networks, and 3) the operational technology network, in a limited

284 manner. The goal was to demonstrate both logically and physically that provisioning functions
285 could be performed from a centralized IdAM system regardless of its location in the enterprise.
286 In a real-world environment, the interconnections between the OT, PACS, and IT silos depend
287 on the business needs and compliance requirements of the enterprise. We did not attempt to
288 replicate these interconnections. Rather, we acknowledge that implementing our build or its
289 components creates new interfaces across silos. We focused on providing general information
290 on how to remain within the bounds of compliance should you adopt this example solution. In
291 addition, we provide guidance on how to mitigate any new risks introduced to the
292 environment.

293 4.3 Risk Assessment and Mitigation

294 We performed two types of risk assessment: the initial analysis of the risk posed to the
295 electricity subsector as a whole, which led to the creation of the use case and the desired
296 security characteristics, and an analysis to show users how to manage the risk to the
297 components introduced by adoption of the solution.

298 4.3.1 Assessing Risk Posture

299 According to NIST Special Publication (SP) 800-30, Risk Management Guide for Information
300 Technology Systems,⁷ “Risk is the net negative impact of the exercise of a vulnerability,
301 considering both the probability and the impact of occurrence. Risk management is the process
302 of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.” The
303 NCCoE recommends that any discussion of risk management, particularly at the enterprise
304 level, begin with a comprehensive review of the Risk Management Framework (RMF)⁸ material
305 available to the public.

306 Using the guidance in NIST’s series of publications concerning the RMF, we performed two key
307 activities to identify the most compelling risks encountered by energy providers. The first was a
308 face-to-face meeting with members of the energy community to define the main security risks
309 to business operations. This meeting identified a primary risk concern—the lack of centralized
310 IdAM services, particularly on OT networks. We then identified the core risk area, IdAM, and
311 established the core operational risks encountered daily in this area. We deemed these the
312 tactical risks:

- 313 • lack of authentication, authorization, and access control requirements for all OT in the
314 electricity subsector
- 315 • inability to manage and log authentication, authorization, and access control
316 information for all OT using centralized or federated controls

⁷ Guide for Conducting Risk Assessments, National Institute of Standards and Technology Special Publication 800-30, Rev. 1, September 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

⁸ National Institute of Standards and Technology (NIST), Risk Management Framework (RMF) <http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/>

- 317 • inability to centrally monitor authorized and unauthorized use of all OT and user
318 accounts
- 319 • inability to provision, modify, or revoke access throughout the enterprise (including OT)
320 in a timely manner

321 Our second key activity was conducting phone interviews with members of the electricity
322 subsector. These interviews gave us a better understanding of the actual business risks as they
323 relate to the potential cost and business value. NIST SP 800-39, Managing Information Security
324 Risk,⁹ focuses particularly on the business aspect of risk, namely at the enterprise level. This
325 foundation is essential for any further risk analysis, risk response/mitigation, and risk
326 monitoring activities. Below is a summary of the strategic risks:

- 327 • impact on service delivery
- 328 • cost of implementation
- 329 • budget expenditure as they relate to investment in security technologies
- 330 • projected cost savings and operational efficiencies to be gained as a result of new
331 investment in security
- 332 • compliance with existing industry standards
- 333 • high-quality reputation or public image
- 334 • risk of alternative or no action
- 335 • successful precedents

336 Undertaking these activities in accordance with the NIST RMF guidance yielded the necessary
337 operational and strategic risk information, which we subsequently translated to security
338 characteristics. We mapped these characteristics to NIST's SP 800-53 Rev.4¹⁰ controls where
339 applicable, along with other applicable industry and mainstream security standards.

340 4.3.2 Managing IdAM Risk

341 A foundation of cybersecurity is the principle of least privilege, defined as providing the least
342 amount of access (to systems) necessary for the user to complete his or her job.¹¹ To enforce
343 this principle, the access control system needs to know the appropriate privileges for each user
344 and system. An analysis of the IdAM solution reveals two components that need to be
345 protected from both external and internal threat actors: the central identity and authorization

⁹ Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology Special Publication 800-53, Rev. 4, April 2013, <http://dx.doi.org/10.6028/NIST.SP.800-53r4>

¹⁰ Managing Information Security Risk, National Institute of Standards and Technology Special Publication 800-39, March 2011, <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

¹¹ J. Saltzer, Protection and the control of information sharing in multics, Communication of the ACM, 17 (7), 388-402 (1974)

346 store, and the authorization workflow management system. The authorization workflow
347 management system is trusted to make changes to the central identity and authorization store.
348 Therefore, any inappropriate or unauthorized use of these systems could change authorization
349 levels for anyone in the enterprise. If that occurred, the enterprise would experience a lack of
350 integrity of the identity and authentication stores. The central identity and authorization store
351 is the authoritative source for the enterprise and holds the hash for each user password, as well
352 as the authorizations associated with each user. Access to this information would enable an
353 unauthorized user to impersonate anyone in the organization. In this situation, the enterprise
354 would lose the confidentiality of its users.¹²

355 To protect the build components, we implemented the following requirements in our lab
356 environment: access control, data security, and protective technology. Section 5.9, Evaluation
357 of Security Characteristics, provides a security evaluation of the example solution and a list of
358 the security characteristics. Please note that we addressed only the core requirements
359 appropriate for the IdAM build.

360 4.3.3 Security Characteristics and Controls Mapping

361 As explained in Section 4.3.1, we derived the security characteristics through a risk analysis
362 process conducted in collaboration with our electricity subsector stakeholders. This is a critical
363 first step in acquiring or developing the capability necessary to mitigate the risks as identified
364 by our stakeholders. Table 1 maps the desired security characteristics and example capabilities
365 of the use case to the Framework for Improving Critical Infrastructure Cybersecurity, relevant
366 NIST standards, industry standards, and controls and best practices.

¹² Section 5.9.5.1.1 describes the security controls in place to mitigate this risk.

Table 1. Use Case Security Characteristics Mapped to Relevant Standards and Controls

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27001	SANS CAG20	NERC CIP v3/5 ¹³
Authentication for OT	Authentication mechanisms	Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2, IA Family	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-007-5 R2, CIP-007-5 R5

¹³ The relationship of NERC CIP requirements to the Security Characteristics is derived from a mapping between NIST 800-53 rev4 security controls and NERC CIP requirements. It is provided for reference only. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27001	SANS CAG20	NERC CIP v3/5 ¹³
Access Control for OT	Access control mechanisms	Protect	Access Control and Protective Technology	PR.AC-2: Physical access to assets is managed and protected PR.AC-3: Remote access is managed PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, AC-17, AC-19, AC-20, CM-7, PE-2, PE-3, PE-4, PE5, PE-6, PE-9	ISO/IEC 27001:2013 A.6.2.2, A.9.1.2A, 11.1.1,A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	CIP-003-5 R1, CIP-004-5 R2, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R1,
Authorization (provisioning) OT	Access policy management mechanisms	Protect	Access Control	PR.AC-4 Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-007-5 R5

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27001	SANS CAG20	NERC CIP v3/5 ¹³
Centrally monitor use of accounts	Log account activity	Detect, Protect	Continuous Monitoring & Protective Technology	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events PR.PT-1: Audit/log records are determined, documented, implemented...	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 AU family	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	CSC 4-2, CSC 12-10, CSC 14-2, CSC 14-3,	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R4, CIP-007-5 R5, CIP-008-5 R2, CIP-010-5 R1, CIP-011-5 R2
Protect exchange of identity and access information	Encryption	Protect	Data Security	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected	SC-8, SC-28	ISO/IEC 27001:2013 A.8.2, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	CSC 16-16, CSC 17-7	CIP-011-5 R1

Example Characteristic		Cybersecurity Standards and Best Practices						Specific Related and Best Practices
Security Characteristics	Example Capability	CSF Function	CSF Category	CSF Subcategory	NIST 800-53 rev4	IEC/ISO27001	SANS CAG20	NERC CIP v3/5 ¹³
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access	Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users PR.AC-4 : Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16, IA Family	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3 ,A.9.4.4	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-007-5 R4, CIP-007-5 R5

368

369 **4.4 Technologies**

370 Table 2 provides information about the products and technologies that we implemented in order to satisfy the security control
 371 requirements.¹⁴

372

Table 2. Products and Technologies Used to Satisfy Security Control Requirements

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Authentication for OT	Authentication mechanisms	PR.AC-1: Identities and credentials are managed for authorized devices and users	Identity Management Platform	CA	Identity Manager	R12.0 SP14 Build 9140	Implements workflows for creating digital identities and authorizing them access to physical and logical resources, including authoritative source
				RSA	IMG¹⁵ Governance Lifecycle	6.9.74968	Implements workflows for creating digital identities and authorizing them access to physical and logical resources.
Provision, modify or revoke access throughout all	Mechanisms for centrally managed provisioning of		Virtual Directory			Adaptive Directory	7.1.5 R29692

¹⁴ This table describes only the product capabilities used in our builds. Many of the products have significant additional security capabilities that were not used in our builds. The product column of the table contains links to vendor product information that describes the full capabilities.

¹⁵ RSA IMG is now known as RSA VIA Governance and RSA VIA Lifecycle

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
federated entities	access		Credential Management	GlobalSign	Enterprise PKI	N/A	Provides NAESB-compliant X.509 certificates to OT personnel.
			Credential Management / Physical Access Control	XTec	Credential Issuance Solutions	N/A	Provides PIV-I smartcard credentials and physical access control capability using the smartcard.
Access Control for OT	Access control mechanisms	PR.AC-2: Physical access to assets is managed and protected	Credential Management / Physical Access Control	XTec	Physical Access Control Logical Access Control Authentication and Validation	N/A	Provides PIV-I smartcard credentials and physical access control capability using the smartcard.
			Physical Access Control Enforcement	RS2 Technologies	AccessIT!	4.1.15	Controls physical access to power facilities, buildings, etc.
Authorization (provisioning) OT	Access policy management mechanisms	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Provisioning	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the IdAM workflow to Access It Universal
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access						

Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Authorization (provisioning) OT	Access policy management mechanisms		Identity Management Platform	CA	Identity Manager	R12.0 SP14 Build 9140	Provisions identities and authorizations to Active Directory.
Provision, modify or revoke access throughout all federated entities	Mechanisms for centrally managed provisioning of access		Secure Attribute Management	RSA	IMG ¹⁶	6.9.74968	
			Mount Airey Group	Ozone Console and Ozone Authority Secure Attribute Management Public Key Enablement Ozone Mobile	Ozone Authority 4.0.1, Ozone Server 2.1.301, Ozone Envoy 4.1.0, Ozone Console 2.0.2	Manages attributes that control access to high-value transactions.	
Centrally monitor use of accounts	Log account activity	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Industrial Control System (ICS) User Access Management	TDi Technologies	Console Works	4.9-0u0	Controls access to industrial control system (ICS) devices by people (ICS engineers and technicians).

¹⁶ RSA IMG is now known as RSA VIA Governance and RSA VIA Lifecycle

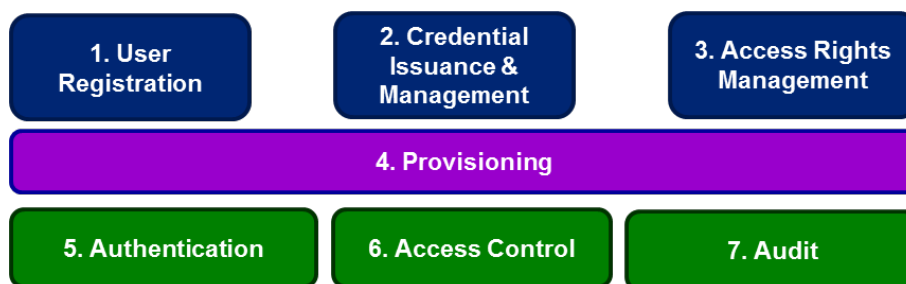
Security Characteristics	Example Capability	CSF Subcategory	Application	Company	Product	Version	Use
Access Control for OT	Access control mechanisms	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Industrial Control System (ICS) User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access to ICS devices by people.
			ICS Device-to-Device Access Management	Radiflow	Industrial Control System Firewall and iSIM Software OT Security Substation Security	iSIM 3.6.07	Controls communication among ICS devices.
			Access Gateway	Cisco	Identity Service Engine (ISE)	1.4.0.253	Controls access to resources in OT by users in IT based on both user identity and device identity.
			Access Gateway	Schneider Electric	ConneXium Tofino Ethernet Firewall	2.10	Controls access to devices in the ICS/SCADA network

373 5 ARCHITECTURE

374 5.1 Example Solution Description

375 IdAM is the discipline of managing the relationship between a person and the resources the
 376 person needs to access to perform a job. It encompasses the processes and technologies by
 377 which individuals are identified, vetted, credentialed, and authorized access to and held
 378 accountable for their use of resources. These processes and technologies create digital identity
 379 representations of people, bind those identities to credentials, and use those credentials to
 380 control access to resources. IdAM is composed of the capabilities illustrated in Figure 1.

381



382

383

Figure 1. IdAM capabilities

- 384 1. **User registration** determines that a reason exists to give a person access to resources,
 385 verifies the person’s identity, and creates one or more digital identities for the person.
- 386 2. **Credential issuance and management**¹⁷ provides life-cycle management of credentials
 387 such as employee badges or digital certificates.
- 388 3. **Access rights management** determines the resources a digital identity is allowed to use.
- 389 4. **Provisioning** populates digital identity, credential, and access rights information for use
 390 in authentication, access control, and audit.
- 391 5. **Authentication** establishes confidence in a person’s digital identity.
- 392 6. **Access control**¹⁸ allows or denies a digital identity access to a resource.
- 393 7. **Audit** maintains a record of resource access attempts by a digital identity.

394 The top three capabilities are administrative capabilities in that they involve human actions or
 395 are used infrequently. For example, verifying identity typically involves physically reviewing
 396 documents such as a driver’s license or passport. Credential issuance and management is

¹⁷ NIST SP 800-63-2, Electronic Authentication Guideline, provides additional information on credential issuance and management, as well as authentication.

¹⁸ NIST IR 7316, Assessment of Access Control Systems, explains commonly used access control policies, models, and mechanisms.

397 invoked when an employee is hired, changes jobs, leaves the company, loses a credential, or
398 when a credential expires.

399 The bottom three capabilities are “run-time” capabilities in that they happen whenever a
400 person accesses a resource. Authentication, access control, and audit are typically automated
401 activities that occur every time a person enters a facility using a badge, or logs into a computer
402 system. A directory, such as Microsoft Active Directory (AD), is often used in the
403 implementation of run-time functions.

404 Provisioning is the “glue” that connects the administrative activities to the run-time activities by
405 providing the run-time capabilities with the information needed from the administrative
406 activities.

407 In the electricity subsector today, all of these IdAM capabilities are frequently replicated at
408 least three times—once for a person’s access to OT, again for access to PACS, and then to
409 access IT. Additionally, these capabilities may be independently replicated for each system
410 within OT or IT. This replication makes it difficult to ensure that employees have access to the
411 resources they need to perform their jobs, and only those resources. Newly hired employees
412 may not have access to all the resources they need. Employees who change jobs may retain
413 access to resources they no longer need. Terminated employees may retain access long after
414 they have left. Further, multiple, independent IdAM processes make it difficult to periodically
415 review who has access to what resources.

416 The example solution described here addresses these problems by centralizing some of the
417 administrative capabilities into a core IdAM capability used across OT, PACS, and IT, while
418 leaving the run-time capabilities replicated and distributed. Figure 2 illustrates the example
419 solution.

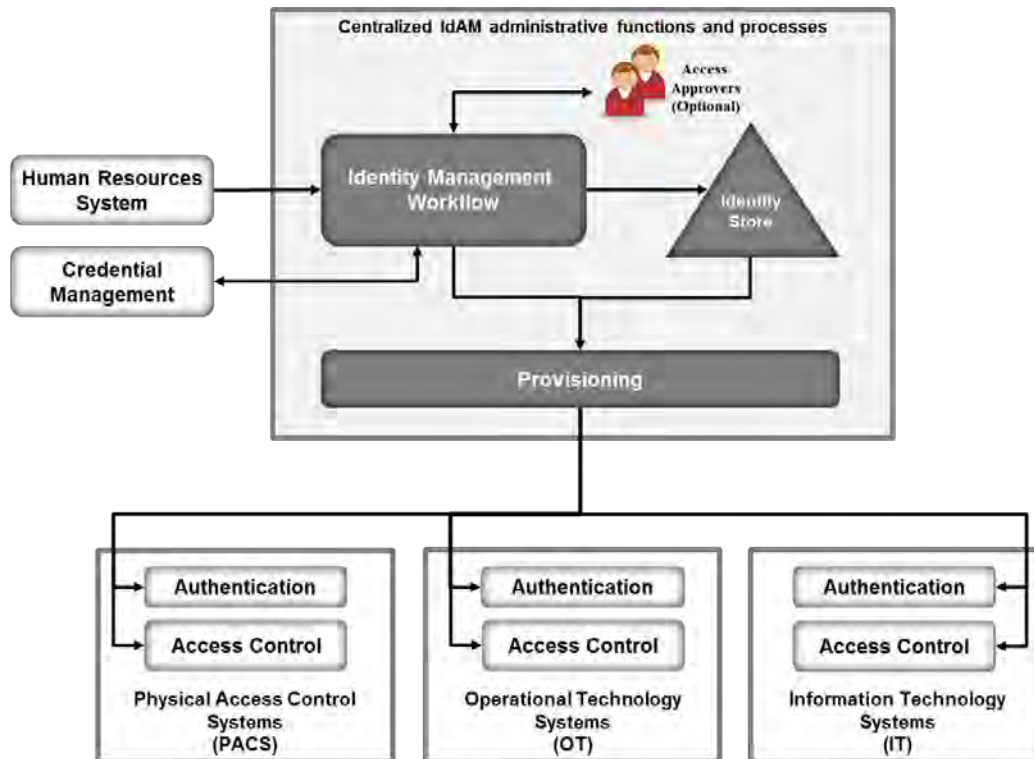


Figure 2. IdAM example solution

420

421

422 The centralized IdAM capability implements:

423

- an IdAM workflow to manage the overall process
- an identity store, which is the authoritative source for digital identities and their associated access rights to resources
- a provisioning capability to populate information from the workflow and identity store into the run-time capabilities

424

425

426

427

428 The combined capabilities can reduce the time to update access in the OT, PACS, and IT systems
 429 from days to minutes. They also improve the audit trail capture by integrating the three audit
 430 logs into one. Provisioning may also verify that authorizations stored locally in the run-time
 431 capabilities are consistent with those in the identity store. If locally stored authorizations are
 432 inconsistent with authoritative values in the identity store, provisioning may raise an alarm or
 433 change locally stored authorizations to be consistent with the identity store.

434 The example solution implements three basic transactions:

435

436

437

438

- creating all required credentials, authorizing access, and provisioning access for a new employee
- updating credentials and access for an existing employee who is changing jobs or requires a temporary access change

- 439 • destroying credentials and removing accesses for a terminated employee

440 The IdAM workflow receives information about employees and their jobs from the HR system.
441 For a new employee, HR is responsible for performing initial identity verification. Based on a
442 new employee's assigned job, the IdAM workflow creates one or more digital identities and
443 determines the credentials and resource accesses required. The workflow triggers credential
444 management capabilities to create physical identification badges, physical access cards, and any
445 logical access credentials such as X.509 public key certificates that may be needed. The
446 workflow records information about these credentials in the identity store.

447 The example solution does not assume that each person will have a single digital identity. A
448 current employee is likely to have several distinct digital identities because of independent
449 management of digital identities in physical security, business systems, and operational
450 systems. Requiring a single digital identity would create a significant challenge to adoption of
451 the example solution.

452 Instead, the identity store associates all of an employee's digital identifiers so all of that
453 person's accesses can be managed together. Once the example solution is in place, an
454 organization can continue issuing multiple digital identifiers to new employees or can assign a
455 single digital identifier that is common to physical security, business systems, and operational
456 systems.

457 The workflow automatically authorizes some physical and logical accesses that either are
458 needed by all employees or for an employee's job. The workflow stores information about
459 credentials and authorized accesses in the identity store. The workflow can then invoke
460 provisioning to populate run-time functions with credential information and access
461 authorizations. This allows the employee to access facilities and systems.

462 Access to some resources, both logical and physical, will require explicit approval before being
463 authorized. For these, the workflow notifies one or more access approvers for each such
464 resource and waits for responses. When the workflow receives approvals, it stores the
465 authorized accesses in the identity store and provisions them to the run-time functions. All
466 information about approved, pending,¹⁹ and provisioned physical and logical access
467 authorizations is maintained in the identity store.

468 When the HR system notifies the workflow that an employee is changing jobs, the workflow
469 performs similar actions. First, it identifies resource accesses and credentials associated only
470 with the employee's former job. It revokes those resource accesses in the identity store and de-
471 provisions them from the run-time functions. It directs that associated credentials be
472 invalidated and destroyed. It removes information about those credentials from the identity

¹⁹ Pending access authorizations may be either authorizations that have been approved but not yet provisioned or time-bounded authorizations to be provisioned/deprovisioned at a future time.

473 store and de-provisions credential information from the run-time functions.²⁰ It then identifies
474 resource accesses needed for the employee's new job, authorizes them in the identity store,
475 and provisions them to the run-time functions. The workflow identifies any new credentials
476 that will be needed in the new job, triggers creation and issuance of those credentials, waits for
477 them to be created, updates the identity store, and provisions new credential information to
478 the run-time functions.

479 When the HR system notifies the workflow that an employee has been terminated, the
480 workflow removes all the employee's resource accesses from the identity store and de-
481 provisions them from the run-time functions. It triggers invalidation and destruction of the
482 employee's credentials, removes credential information from the identity store, and de-
483 provisions credential information from the run-time functions.

484 In addition to input from the HR system to process personnel actions, the workflow can provide
485 a portal for employees to request access to resources, which can be reviewed and approved.
486 Also, systems other than HR can be integrated with the workflow to initiate resource access
487 requests. These capabilities reduce overhead and administrative downtime.

488 5.1.1 [The Physical Access Control System Silo](#)

489 The PACS silo hosts both access control and badging systems. The badging systems implement a
490 credential issuance capability that creates the badges employees use to gain access to facilities
491 and other physical resources. The access control systems read information from badges and
492 check authorization information provided by the centralized IdAM capability to determine if a
493 person should be allowed access. If access is allowed, the access control system unlocks a door,
494 allowing the person to enter the facility.

495 Figure 3 shows the architecture of the PACS silo.

²⁰ Workflow actions are programmable and can be customized to meet organization-specific needs.

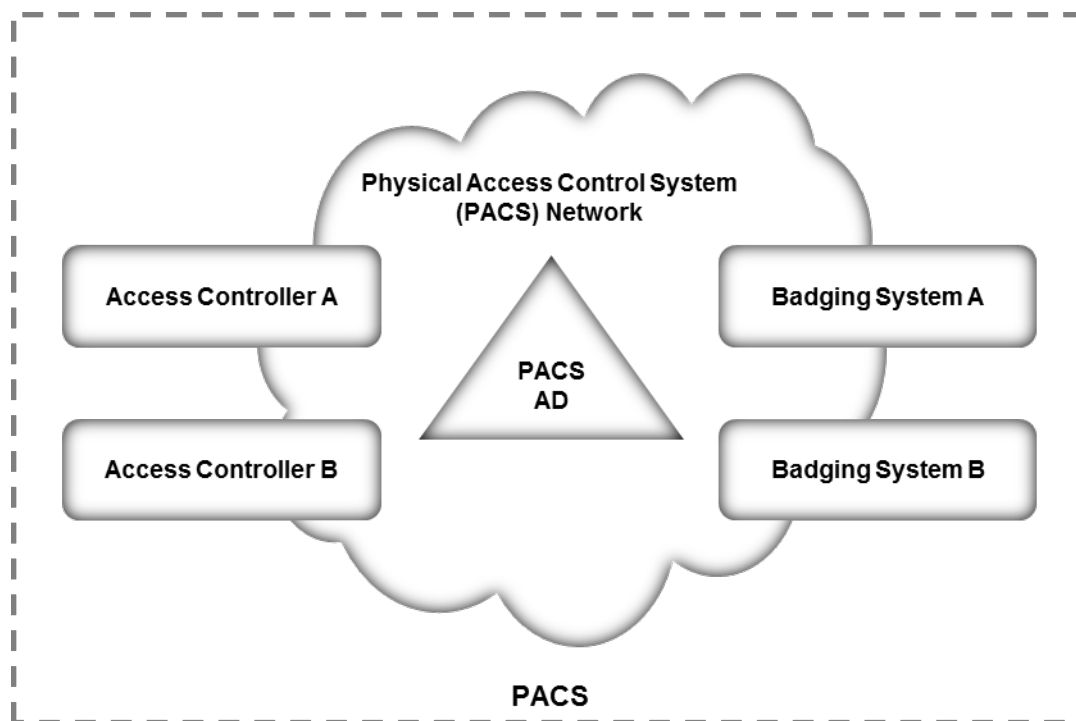


Figure 3. Notional PACS architecture

496 An instance of Microsoft Active Directory contains identities and access control information for
 497 the people who operate the badging systems and the people who manage the access control
 498 systems. This access control information is provisioned into the PACS Active Directory instance
 499 from the centralized IdAM system.

500 The PACS Active Directory instance may also store authorized physical access information used
 501 by the access control systems. If the access control systems are integrated with Active
 502 Directory, then the IdAM system will provision authorization information to PACS Active
 503 Directory. If the access control systems are not integrated with Active Directory, then
 504 authorization information will be provisioned directly to the access control system.²¹

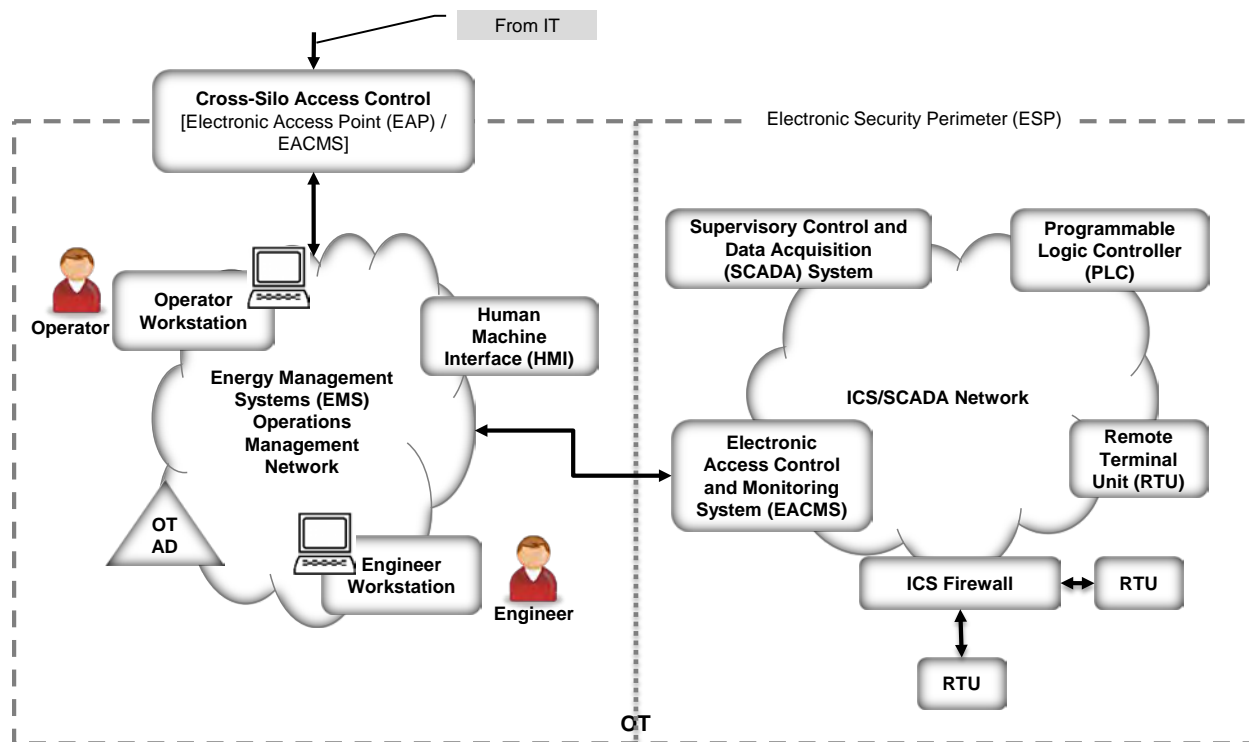
505 5.1.2 The Operational Technology Silo

506 The OT silo is composed of two types of systems—operational management systems that
 507 operators and engineers use to monitor and manage the generation and delivery electric
 508 energy to customers, and industrial control systems (ICSs) and supervisory control and data
 509 acquisition (SCADA) systems that provide real-time and near real-time control of the equipment
 510 that produces and delivers electric energy.

511 Figure 4 shows the notional architecture of the OT silo.

²¹ Build #1 provisions directly to the access control system. Build #2 provisions to the PACS AD.

512



513

514

Figure 4. Notional OT silo architecture

515 The operations and management network within the OT silo has an Active Directory instance
 516 that contains identities and access authorizations for operational management systems. These
 517 identities and authorizations are provisioned from the centralized IdAM system. A cross-silo
 518 access control capability allows some access to operational management systems from the IT
 519 silo. The centralized IdAM system provisions authorizations to access OT resources from the IT
 520 silo into the OT Active Directory.

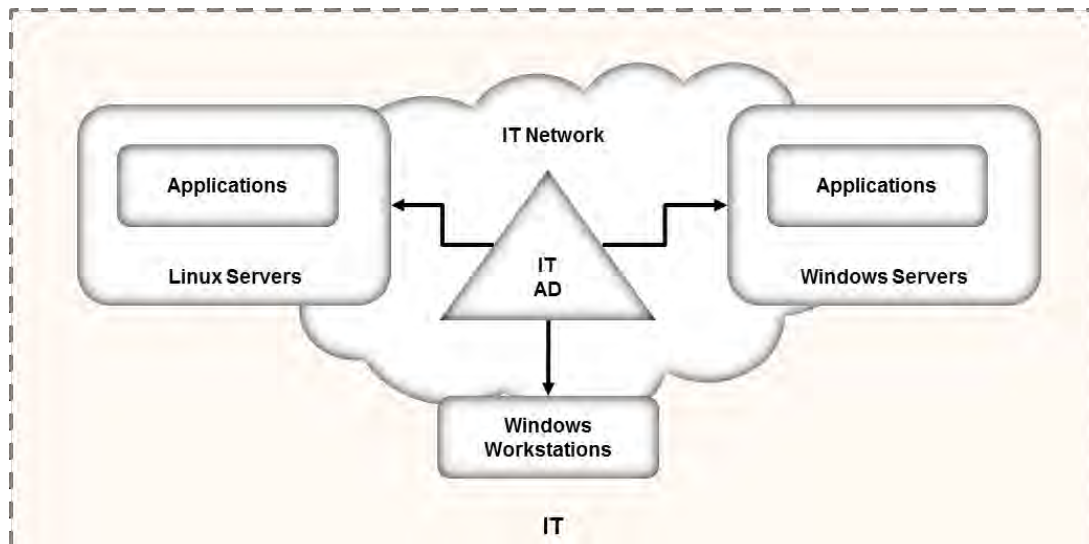
521 An electronic access control and monitoring system (EACMS) controls access to ICS/SCADA
 522 devices on the ICS/SCADA network from the operations management network. The EACMS
 523 allows operators and engineers terminal access to the programmable logic controllers (PLCs)
 524 and remote terminal units (RTUs) that provide real-time control of energy production and
 525 delivery. Authorizations allowing access via the EACMS may be provisioned into the OT Active
 526 Directory instance or directly into the EACMS by the centralized IdAM system. The centralized
 527 IdAM system can provide time-bounded authorizations that will allow access during a limited
 528 time period. When the period expires, a workflow is triggered that revokes the authorization in
 529 the identity store and de-provisions the authorization from the OT Active Directory instance.

530 An ICS/SCADA firewall controls communication among ICS/SCADA devices. The centralized
 531 IdAM system does not currently manage or provision authorizations that control device-to-
 532 device communication. Authorizations for device-to-device communications are either learned
 533 by the firewall in training mode, or configured using a vendor-supplied application. This
 534 capability could be added in a future version of the centralized IdAM system.

535 5.1.3 The Information Technology Silo

536 The IT silo hosts business systems. These systems consist of user workstations and business
 537 applications running on Microsoft Windows or Linux servers. An IT Active Directory instance
 538 contains identities and access authorizations for both business system users and system
 539 administrators who manage the applications and servers. These authorizations are provisioned
 540 from the centralized IdAM system. Applications that are not integrated with Active Directory
 541 can be provisioned directly by the centralized IdAM system.

542 Figure 5 shows the notional architecture of the IT silo.



543

544

Figure 5. Notional IT silo architecture

545 **5.2 Example Solution Relationship to Use Case**

546 When we first defined this challenge²² in collaboration with industry members, we wrote the
 547 following scenario:

548 “An energy company technician attempts to enter a substation. She is challenged to prove her
 549 identity in a way that provides a high degree of confidence and is not onerous (i.e., does not
 550 require a significant behavior change). Her attempt at entry initiates an authentication request
 551 that, if possible, connects to the company’s authentication and authorization services to
 552 validate her identity, ensure that she is authorized to access the substation, and confirm that a
 553 work order is on file for that substation and that worker at that time.

554 Once she gains access to the substation, she focuses on the reason for her visit: She needs to
 555 diagnose a remote terminal unit (RTU) that has lost its network connectivity. She identifies the
 556 cause of the failure as a frayed Ethernet cable and replaces the cable with a spare. She then

²² http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Identity_Access_Management.pdf

557 uses her company-issued mobile device, along with the same electronic credential she used for
558 physical access, to log into the RTU’s Web interface to test connectivity. The RTU queries the
559 central authentication service to ensure the authenticity and authority of both the technician
560 and her device, then logs the login attempt, the successful authentication, and the commands
561 the technician sends during her session.”

562 The first portion of the scenario deals with physical access to a substation. Unlike the
563 description in this scenario, the example solution provides centralized management of
564 identities and authorizations, but assumes the decision to allow a particular technician access
565 to a particular facility at a particular time may be distributed. Distributing the access decision-
566 making capability helps ensure that access control continues to function in the event of
567 communication failures. Utilities have indicated that communication failures with substations
568 are common. Therefore, authorization to allow the technician access to the substation will be
569 created centrally by the IdAM workflow, placed in the identity store, and then provisioned to
570 the PACS responsible for the substation. Accomplishing this requires integrating the work order
571 management system with the IdAM workflow. Assigning the technician a work order that
572 requires access to a substation triggers actions within the IdAM workflow to authorize access to
573 the substation and provision that authorization to the substation PACS. When the technician
574 presents her physical access credential at the substation, the PACS uses the provisioned
575 authorization to determine if she should be allowed access. Likewise, while not explicitly stated
576 in the example, completion of the work order triggers the IdAM workflow to remove the
577 technician’s substation access authorization and de-provision it from the substation PACS.

578 The second portion of the scenario deals with logical access to ICS/SCADA devices within the
579 substation. Again, unlike the description in the scenario, the example solution centralizes
580 management of identities and authorizations but assumes that run-time functions such as
581 authenticating a user and granting her access to specific ICS/SCADA devices are distributed
582 functions. In this case, the example solution assumes that the substation contains an EACMS to
583 which the technician connects her mobile device. The EACMS authenticates the technician and
584 controls her access to ICS/SCADA devices within the substation. Assigning the technician to this
585 work order triggers an IdAM workflow that authorizes her access to ICS/SCADA devices in the
586 substation, stores these authorizations in the identity store, and provisions both the
587 authorizations and any needed authentication credentials to the substation’s EACMS.
588 Completion of the work order triggers removal of the access authorization and de-provisioning
589 of authorizations and credentials from the substation EACMS.

590 **5.3 Core Components of the Reference Architecture**

591 To verify the modularity of the example solution and to demonstrate alternative provisioning
592 methods, we created two builds of the centralized IdAM capability. Both builds used the
593 following products:

- 594 • AlertEnterprise Guardian implements provisioning to an RS2 Technologies (RS2)
595 AccessIT! Physical Access Control System (PACS).

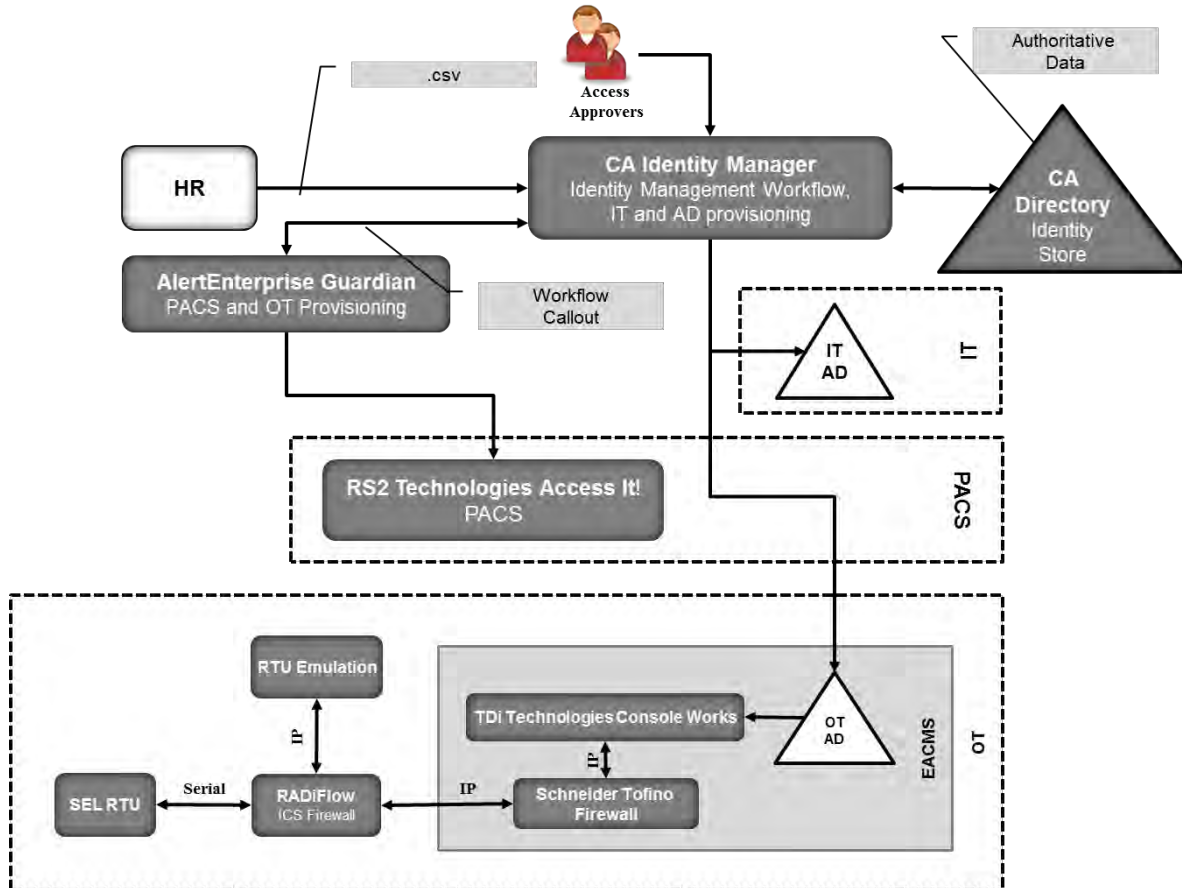
- 596 • TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall serve as an
597 EACMS.
- 598 • A RADiFlow ICS/SCADA firewall controls interactions between two Modbus-speaking
599 RTUs—a Schweitzer Engineering Laboratories (SEL) RTU and an RTU emulated by a
600 Raspberry Pi single-board computer.

601 Build #1 used CA Technologies (CA) Identity Manager to implement the IdAM workflow and
602 aspects of provisioning, and CA Directory to implement the identity store. Build #2 used the RSA
603 Identity Management and Governance (IMG) [now known as RSA VIA Governance and RSA VIA
604 Lifecycle] to implement the IdAM workflow and the RSA Adaptive Directory to implement the
605 identity store and aspects of provisioning.

606 5.3.1 Build #1

607 Figure 6 illustrates Build #1.

608



609

610

Figure 6. Build #1

611 CA Identity Manager implements the IdAM workflow. It receives input from an HR system in the
612 form of comma-separated value (.csv) files. We simulated the HR system using manually
613 produced .csv files. Identity Manager also provisions information to Microsoft Active Directory

614 instances in business systems (IT), and the operational system (OT). No relationship among
615 these Active Directory instances is assumed.

616 IT applications are assumed to be integrated with Active Directory and use credential
617 information and authorization information in the IT Active Directory instance. If there are IT
618 applications that are not integrated with Active Directory, the provisioning capabilities of CA
619 Identity Manager would be used to directly provision the applications.

620 AlertEnterprise Guardian²³ provisions physical access authorizations into the RS2 PACS. CA
621 Identity Minder supports call-outs within a workflow that can be used to invoke external
622 programs. A call-out is used to connect with AlertEnterprise Guardian and provide information
623 to be provisioned to the RS2 PACS.

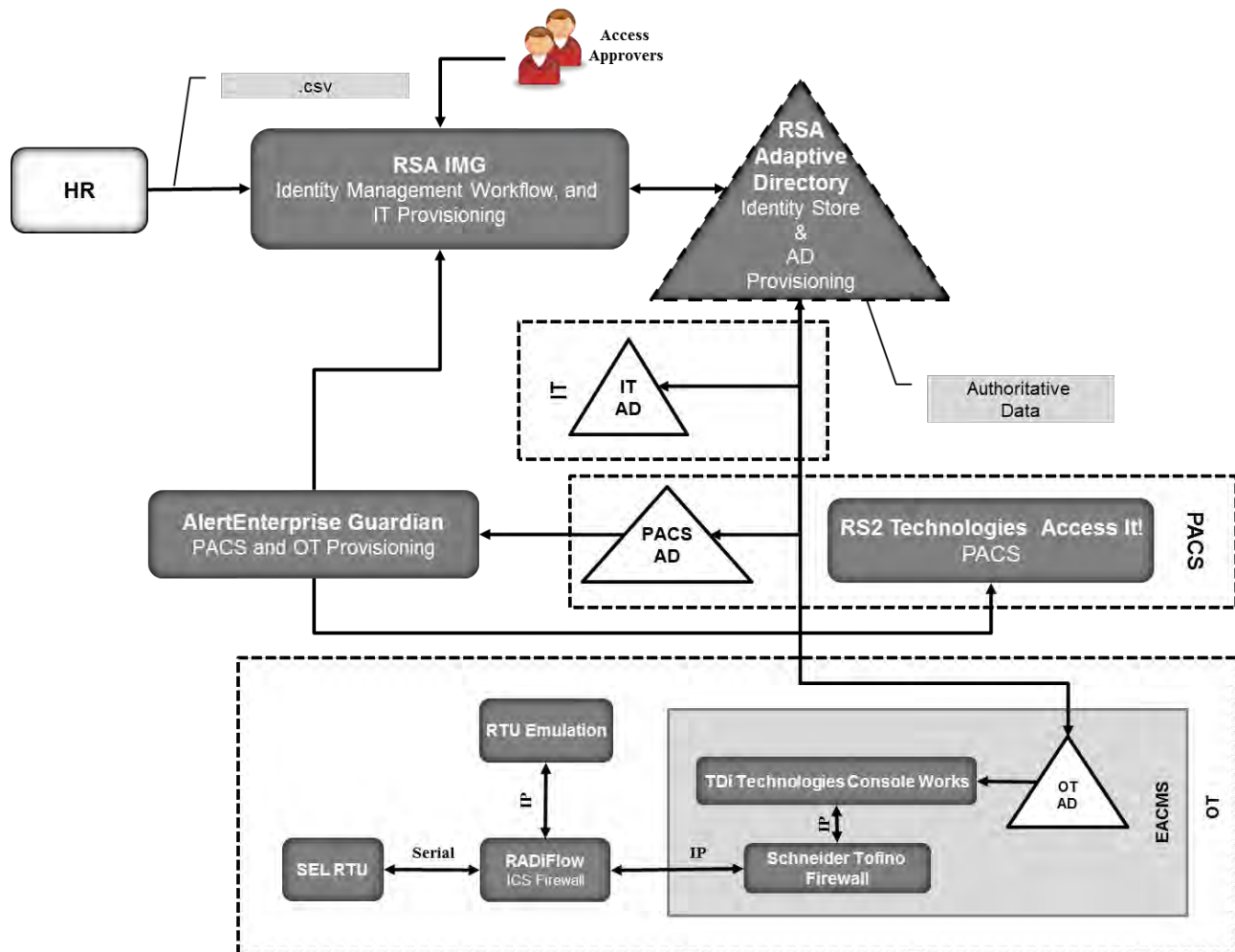
624 An instance of TDi Technologies ConsoleWorks is installed in the OT silo and integrated with the
625 OT Active Directory instance. Identity Manager provisions ICS/SCADA access authorizations in
626 the OT Active Directory instance. ConsoleWorks uses the access authorizations in OT Active
627 Directory to control user access to ICS/SCADA devices. Console Works also captures an audit
628 trail of all user access to the ICS/SCADA network.

629 A Schneider Electric Tofino firewall is installed between Console \Works and the ICS/SCADA
630 network. The firewall determines which IP addresses within the ICS/SCADA network are
631 accessible through ConsoleWorks and which network protocols can be used when accessing
632 those addresses. The combination of Console Works and the Tofino firewall implement an
633 Electronic Access Control and Monitoring System (EACMS) between the Energy Management
634 System / Operations Management Network and the ICS/SCADA network.

635 5.3.2 Build #2
636 Figure 7 illustrates Build #2.

²³ Guardian is also capable of implementing workflow and provisioning ICS devices. However, those capabilities were not used in this build.

637



638

639

Figure 7. Build #2

640 RSA IMG implements the IdAM workflow. It receives input from an HR system in the form of
 641 .csv files. RSA IMG also has the capability to provision information to systems. In Build #2, RSA
 642 IMG stores information in RSA Adaptive Directory, which subsequently provisions the
 643 information to its associated Active Directory instances.

644 RSA Adaptive Directory implements the identity store and provisioning portions of the example
 645 solution. RSA Adaptive Directory is a virtual directory that acts as a proxy in front of multiple
 646 back-end directories. The build assumes that each silo—OT, PACS, and IT—hosts a Microsoft
 647 Active Directory instance. No relationship among these Active Directory instances is assumed.
 648 When an IMG workflow stores information in Adaptive Directory, that information is actually
 649 stored in one or more of the underlying Active Directory instances. In this way, storing
 650 information in Adaptive Directory provisions that information into one or more Active Directory
 651 instances.

652 AlertEnterprise Guardian provisions physical access authorizations into the RS2 PACS. RSA IMG
653 writes these authorizations into Adaptive Directory, which stores them in the PACS Active
654 Directory instance. AlertEnterprise Guardian monitors the Active Directory PACS instance for
655 updates such as changed physical access authorizations for an existing user, addition of a new
656 user with physical access authorizations, or removal of an existing user and associated access
657 authorizations. When changes are detected, Guardian provisions them into the RS2 PACS.

658 As in Build #1, TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall are used
659 is used in the OT silo to provide an EACMS between the EMS/Operations Management Network
660 and the ICS/SCADA network. ConsoleWorks utilizes the OT Active Directory for authorization of
661 users in this build as well.

662 5.3.3 Implementation of the Use Case Illustrative Scenario

663 This section explains how each of the two builds implements the scenario in Section 5.2

664 A work order management system assigns a technician to resolve an issue with an RTU at a
665 substation. The system initiates a workflow in either CA Identity Manager or RSA IMG that
666 authorizes the technician physical access to the substation. In Build #1, this authorization is sent
667 to AlertEnterprise Guardian via a call-out in the workflow in CA Identity Manager. Guardian
668 provisions the authorization into the RS2 PACS. The authorization is also stored in the CA
669 directory. In Build #2, this authorization is written to Adaptive Directory and stored in the PACS
670 Active Directory instance. AlertEnterprise Guardian detects the authorization change for the
671 technician and provisions it to RS2. When the technician arrives at the substation and scans her
672 credentials at the door, RS2 allows her entry.

673 The workflow also authorizes access to ICS/SCADA devices in the substation. In Build #1,
674 Identity Manger stores this authorization in the CA directory and provisions it to the OT Active
675 Directory instance. In Build #2, IMG writes this authorization to Adaptive Directory, which
676 stores it in the OT Active Directory instance. When the technician connects her mobile device to
677 ConsoleWorks in the substation, she is authenticated, and ConsoleWorks checks the OT Active
678 Directory instance, sees that she is authorized, and allows her to access the ICS/SCADA devices
679 in the substation.

680 When the work order is closed, the work order management system triggers another workflow
681 that removes the technician's access authorizations. In Build #1, the authorizations are
682 removed from the CA directory. Substation physical access is de-provisioned from RS2 via a call-
683 out from the workflow to AlertEnterprise Guardian. Identity Manager de-provisions ICS/SCADA
684 access from the OT Active Directory. ConsoleWorks detects the change in the OT Active
685 Directory instance and de-provisions the technician's access to the RTU.

686 In Build #2, IMG removes the authorizations from Adaptive Directory. This removes the
687 authorizations from the PACS and OT Active Directory instances. AlertEnterprise Guardian
688 detects the change in the PACS Active Directory instance and de-provisions the technician's
689 substation physical access. ConsoleWorks detects the change in the OT Active Directory
690 instance and de-provisions the technician's access to the RTU.

691 Without an active assigned work order, the technician has no physical or logical access to the
692 substation.²⁴

693 **5.4 Supporting Components of the Reference Architecture**

694 In addition to the products used to build an instance of the core example solution (the build),
695 several products provide supporting components to the build as show in Figure 8. These
696 products implement IdAM capabilities that, while necessary to completely implement IdAM
697 within an organization, are not an integral part of the centralized IdAM capability.

698 XTec AuthentX and GlobalSign demonstrate outsourcing some credential issuance and
699 management capabilities. XTec AuthentX also demonstrates outsourcing of some physical
700 access control capabilities.

701 XTec AuthentX Identity and Credential Management System²⁵ provides a personal identity
702 verification interoperable (PIV-I) smartcard credential based on NIST standards that can be used
703 for logical and physical access. AuthentX demonstrates outsourcing of some aspects of user
704 registration, credential issuance and management, authentication, and access control
705 capabilities. These capabilities are provided using a cloud-hosted solution with identity vetting
706 workflows, credential issuance stations, and full life-cycle maintenance tools. AuthentX
707 produces Homeland Security Presidential Directive 12-compliant smart cards that are
708 interoperable with and trusted by federal counterparts.

709 XTec demonstrates a cloud-based implementation of the XTec physical access control (PACS)
710 product. The components of the XTec solution in our lab included XNode, card readers, and
711 compliant PIV-I cards. The XTec product places the XNode, an IP addressable RS232/RS485
712 controller within close range of the reader and door strike, as opposed to a typical central
713 control panel deployment. The XNode can also control SCADA devices and send them
714 encrypted instructions.

715 AuthentX IDMS/CMS can also provide a Web-based implementation of the IdAM workflow in
716 the example solution, as well as credential management and provisioning. AuthentX IDMS/CMS
717 can control, log, and account for identity vetting, credential issuance, and credential usage with
718 AuthentX PACS and logical access controls, as well as control credential revocation to all
719 interoperable resources immediately.

²⁴ The reference architecture requires substations to have power and communications to receive provisioned authorizations. The reference architecture does not address crisis / emergency situations where this requirement is not met. The reference architecture assumes existing energy company procedures for crisis / emergency response will be used / updated to address this challenge.

²⁵ The description of the XTec product and its role supporting the implementation of the example solution was provided to NCCoE by XTec.

720 GlobalSign operates a North American Energy Standards Board (NAESB)-accredited Software as
721 a Service Certificate Authority. It illustrates an outsourced credential issuance and management
722 capability that provides NAESB-compliant X.509 digital certificates. NAESB-compliant digital
723 certificates are required credentials for authenticating Open Access Same-Time Information
724 Systems (OASIS) transactions and access to the Electronic Industry Registry—the central
725 repository for information related to energy scheduling and management activities in North
726 America.²⁶

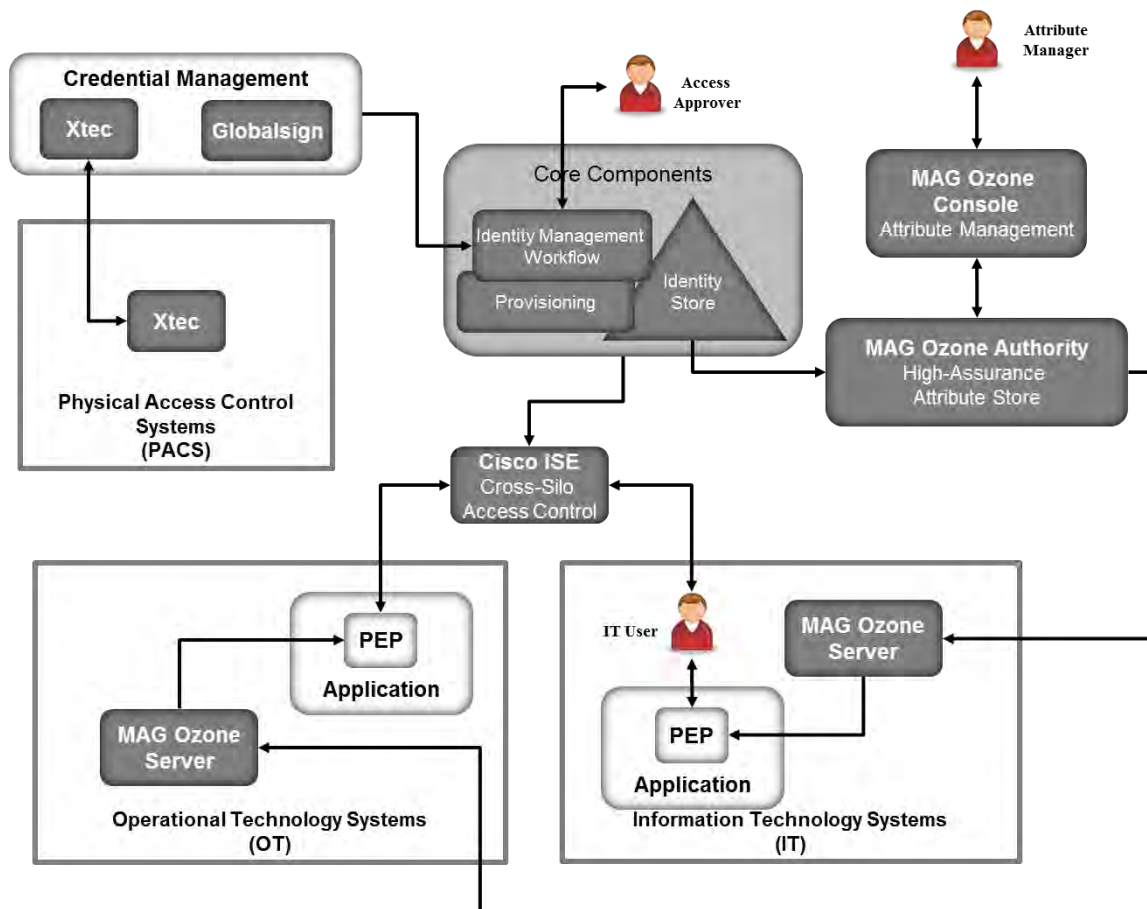
727 Mount Airey Group (MAG) Ozone and Cisco Identity Services Engine (ISE) demonstrate access
728 control decision and enforcement capabilities that the centralized IdAM capability can
729 provision. MAG Ozone can also provide authorization management capabilities.

730 The MAG Ozone product provides a high-assurance attribute-based access control²⁷ (ABAC)
731 implementation. ABAC controls access to resources by evaluating access rules using attributes
732 associated with the resource being accessed, the person accessing the resource, and the
733 environment. Ozone Authority provides a high-assurance attribute store. Attributes stored in
734 Ozone Authority are managed using Ozone Console. Ozone manages attributes that control
735 access to high-value transactions such as high-dollar-value financial transactions.

736 Ozone Authority pulls attributes either from Adaptive Directory in Build #2 or from an AD
737 instance in Build #1. Once Ozone Authority pulls the attributes, their values are managed
738 through Ozone Console.

²⁶ <https://www.GlobalSign.com/en/digital-certificates-for-naesb/>

²⁷ NIST Special Publication 800-162, Guide to Attributed Based Access Control (ABAC) Definition and Considerations.



739

740

Figure 8. Supporting components

741 Ozone Server uses these attributes, in either the OT or IT silo, to decide if a user is allowed to
 742 perform a transaction. Ozone Server provides its decision to the policy enforcement point
 743 associated with the application.

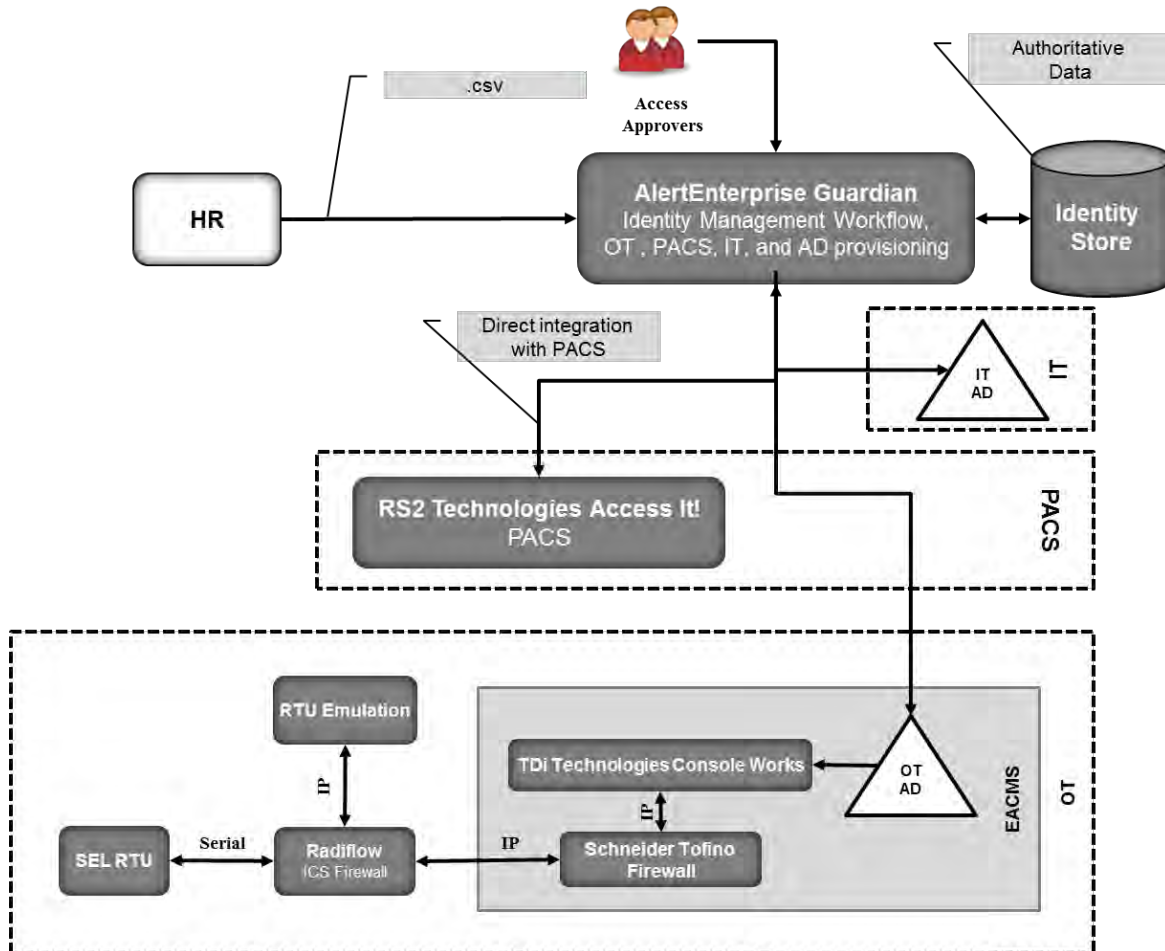
744 MAG provided an application for the IT silo to demonstrate some of Ozone’s capabilities. The
 745 application is described in Appendix C.²⁸

746 Cisco ISE controls the ability of devices to connect over the network. ISE expands on basic
 747 network address-based control to include the identity of the person using a device. ISE is used
 748 in the builds to provide a gateway function between OT and IT, limiting which users and devices
 749 are allowed to connect from IT to resources in OT.

²⁸ Other than the MAG demonstration application, a full ABAC capability was not included in the architecture. A separate NCCoE project is creating an ABAC building block that could be used in IT or OT.
<http://nccoe.nist.gov/content/attribute-based-access-control>

750 5.5 Build #3 - An Alternative Core Component Build of the Example Solution

751 RSA, CA, and AlertEnterprise all provide products that can implement the IdAM workflow,
 752 identity store, and provisioning. Our initial builds of the example solution used RSA and CA
 753 products to implement the IdAM workflow, the identity store, and Active Directory
 754 provisioning. AlertEnterprise Guardian was used to provision the RS2 PACS; however, Guardian
 755 can also implement the IdAM workflow, identity store, and both OT and IT provisioning. To
 756 illustrate Guardian's full capabilities, AlertEnterprise created this independent build of the
 757 example solution in their labs using the Guardian product.



758

759

Figure 9. Build #3

760 AlertEnterprise Guardian implements the IdAM workflow. It receives input from an HR system
 761 in the form of comma-separated value (.csv) files. We simulated the HR system using manually
 762 produced .csv files. Guardian provisions information to Microsoft Active Directory instances in
 763 OT and IT. No relationship among these Active Directory instances is assumed.

764 IT applications are assumed to be integrated with Active Directory and use credential
 765 information and authorization information in the IT Active Directory instance. If there are IT

766 applications that are not integrated with Active Directory, the provisioning capabilities of
767 Guardian would be used to directly provision the applications.

768 Guardian provisions physical access authorizations into the RS2 PACS. Physical Access and
769 Cardholder life cycle functions are supported through Guardian workflow to ensure right level
770 of access is granted to the right people based on training, compliance and security
771 requirements.

772 An instance of TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall are
773 installed in the OT silo to implement an EACMS between the EMS/Operations Management
774 network and the ICS/SCADA network. ConsoleWorks is integrated with the OT Active Directory
775 instance. Guardian provisions ICS/SCADA access authorizations in the OT Active Directory
776 instance. ConsoleWorks uses the access authorizations in OT Active Directory to control user
777 access to ICS/SCADA devices.

778 Additional information about Build #3 is available from the AlertEnterprise Web site at
779 <http://www.alertenterprise.com/resources-standards-nistcoe.php> .

780 **5.6 Build Implementation Description**

781 The infrastructure was built on Dell model PowerEdge R620 server hardware. The server
782 operating system was VMware vSphere virtualization operating environment. In addition, we
783 used a 6-terabyte Dell EqualLogic network attached storage (NAS) product, and Dell model
784 PowerConnect 7024, and Cisco 3650 physical switches to interconnect the server hardware,
785 external network components, and the NAS.

786 The NCCoE built two instantiations of the example solution to illustrate the modularity of the
787 technologies. Build #1 uses the CA Technologies Identity Manager product. Build #2 uses the
788 RSA Identity Management and Governance (IMG) [now known as RSA VIA Governance and RSA
789 VIA Lifecycle] and RSA Adaptive Directory products.

790 The lab network is connected to the public Internet via a virtual private network (VPN)
791 appliance and firewall to enable secure Internet and remote access. The lab network is not
792 connected to the NIST enterprise network. Table 3 lists the software and hardware components
793 we used in the build, as well the specific function each component contributes.

794

Table 3. Build Architecture Component List

Product Vendor	Component Name	Function
Dell	PowerEdge R620	Physical server hardware
Dell	PowerConnect 7024	Physical network switch
Dell	EqualLogic	Network attached storage
VMware	vSphere vCenter Server version 5.5	Virtual server and workstation environment
Microsoft	Windows Server 2012 r2 Active Directory Server	Authentication and authority
Microsoft	Windows 7	Information management
Windows	Windows Server 2012 r2 DNS Server	Domain name system
Windows	SQL Server	Database
AlertEnterprise	Enterprise Guardian	Interface and translation between IdAM central store and the PACS management server
CA Technologies	Identity Manager Rel 12.6.05 Build 06109.28	Identity and access automation management application, IdAM provisioning
Cisco	ISE Network Server 3415	Network access controller
Cisco	Catalyst Model 3650	TrustSec-enabled physical network switch
GlobalSign	Digital Certificates	Cloud certificate authority
Mount Airey Group	Ozone Authority	Central attribute management system
Mount Airey Group	Ozone Console	Ozone administrative management console

Product Vendor	Component Name	Function
Mount Airey Group	Ozone Envoy	Enterprise identity store interface
Mount Airey Group	Ozone Server	Ozone centralized attribute based authorization server
RADiFlow	(iSIM) Industrial Service Management Tool	Supervisory control and data acquisition (SCADA) router management application
RADiFlow	SCADA Router RF-3180S	Router/firewall for SCADA network
RSA	Adaptive Directory Version 7.1.5	Central identity store, IdAM provisioning
RSA	IMG Version 6.9 Build 74968	Central IdAM system (workflow management)
TDi Technologies	ConsoleWorks	Privileged user access controller, monitor, and logging system
RS2 Technologies	AccessIT! Universal Release 4.1.15 Physical access control components	Configures and monitors the PACS devices (e.g., card readers, keypads, etc.)
Schweitzer Electronics Laboratory	SEL-2411	Programmable automation controller
Schneider Electric	Tofino Firewall model number TCSEFEA23F3F20	Industrial Ethernet firewall
XTEC	XNode	Remote access control and management

796

797 5.6.1 [Build Architecture Components Overview](#)

798 The build architecture consists of multiple networks that mirror the infrastructure of a typical

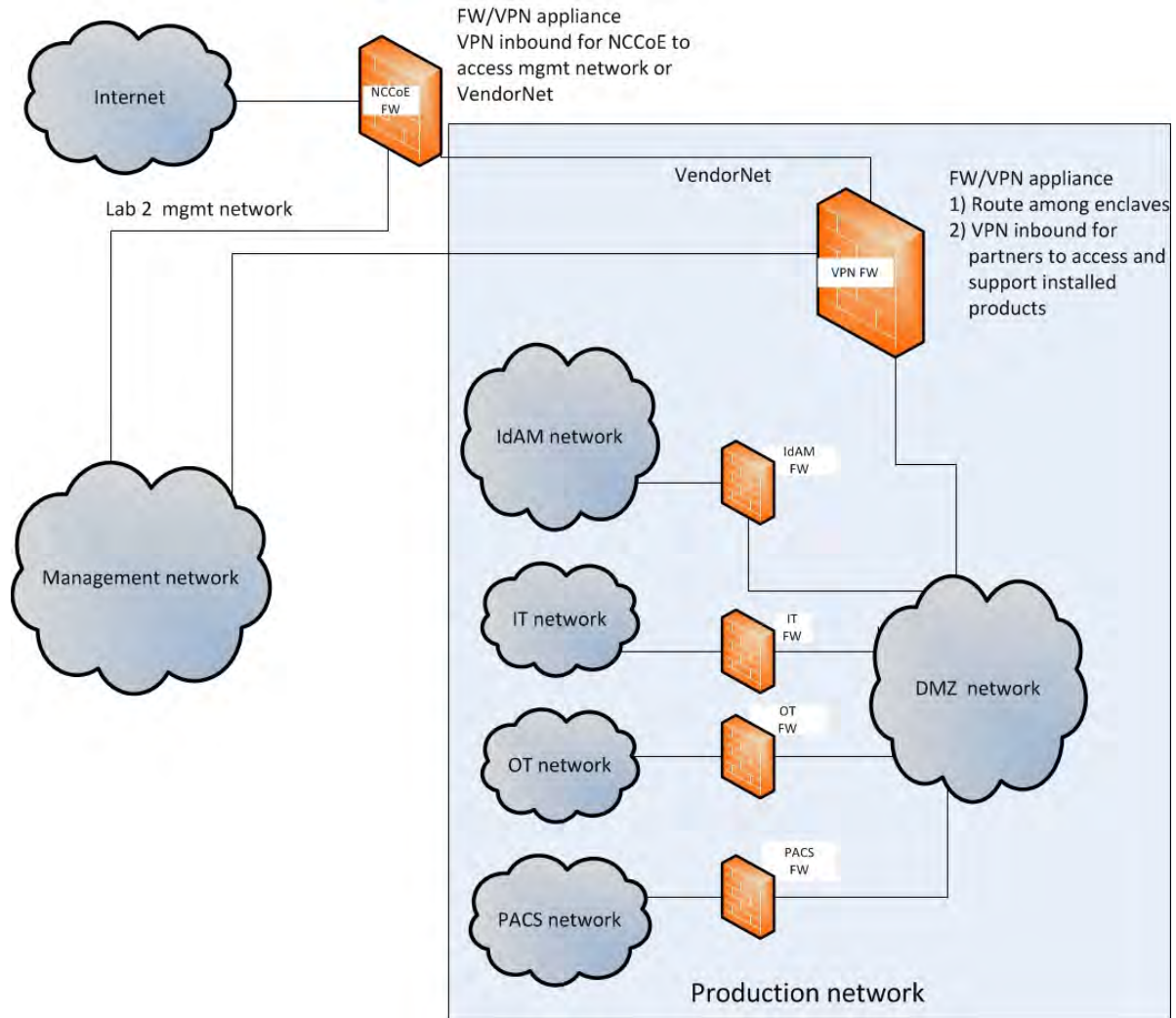
799 energy industry corporation. The networks are a management network and a production

800 network (Figure 10). The management network was implemented to facilitate the
801 implementation, configuration, and management of the underlying infrastructure, including the
802 physical servers, vSphere infrastructure, and monitoring. The production network, Figure 11
803 consists of:

- 804 • the demilitarized zone (DMZ)
- 805 • IdAM
- 806 • OT—ICS/SCADA industrial control system and energy management system (EMS)
- 807 • PACS—physical access control system network
- 808 • IT—business management systems

809 These networks were implemented separately to match a typical electricity subsector
810 enterprise infrastructure. Firewalls block all traffic except required internetwork
811 communications. The primary internetwork communications are the user access and
812 authorization updates from the central IdAM systems between the directories and OT, PACS,
813 and IT networks.

814

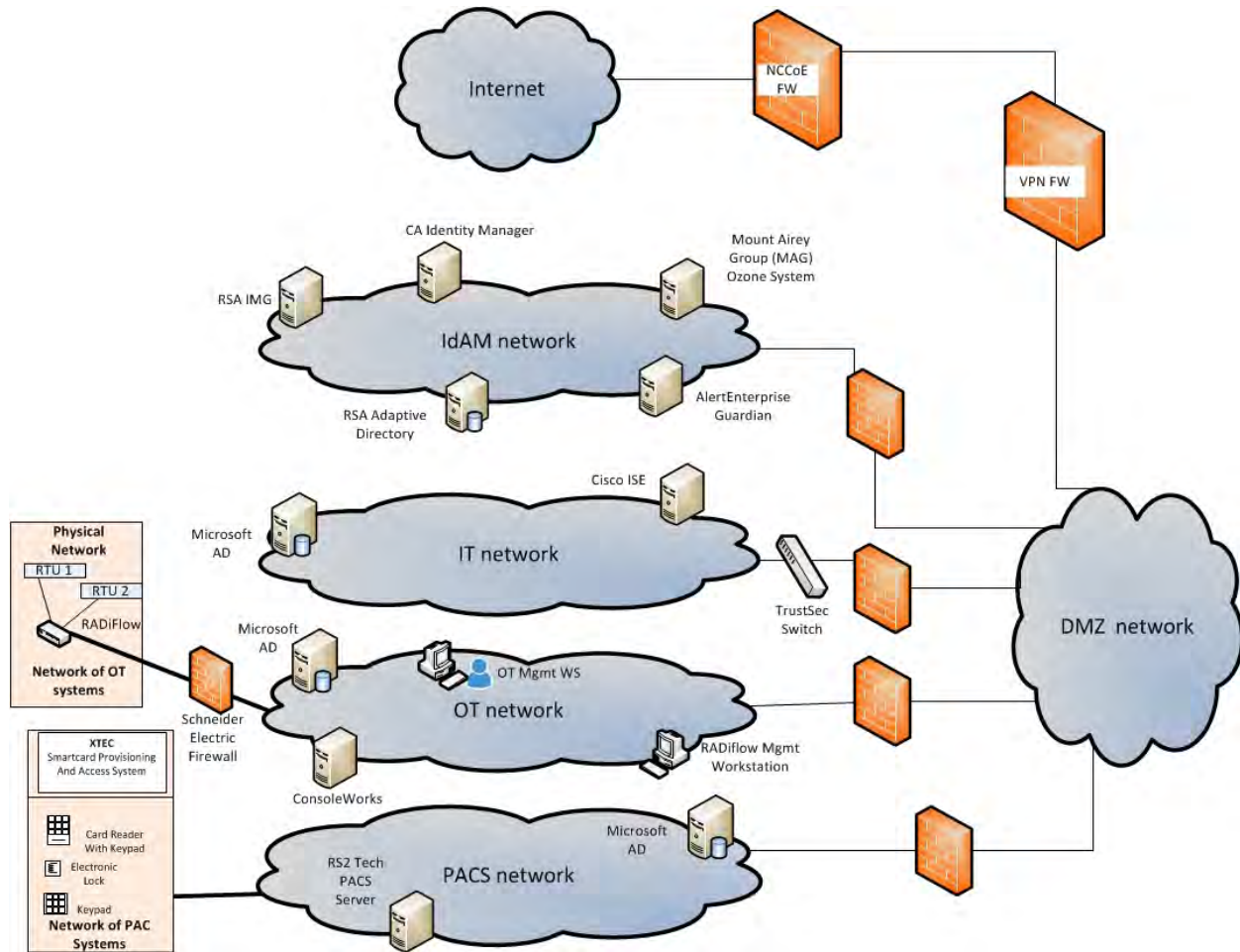


815

816

Figure 10. Management and production networks

817



818

819

Figure 11. IdAM build architecture production network

820 The IdAM network represents the proposed centralized/converged IdAM network/system. This
 821 network was separated into OT, PACS, and IT to highlight the unique IdAM components
 822 proposed to address the use case requirements.

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

826 The OT network represents the network used to support the EMSs and ICS/SCADA systems.
 827 Typically, this network is either not connected to the enterprise IT network or is connected with
 828 a data diode (a one-way communication device from the OT network to the IT network). Two-
 829 way traffic is allowed per NERC-CIP and is enabled via the OT firewall only for specific ports and
 830 protocols between specific systems identified by IP address.

831 The PACS network represents the network that supports the physical access control systems
 832 across the enterprise. Typically, this network uses the enterprise IT network and is segmented
 833 from the user networks by virtual local area networks (VLANs). In our architecture, a firewall

834 allows limited access to and from the PACS network to facilitate the communication of access
835 and authorization information. Technically, this communication consists of user role and
836 responsibility directory updates originating in the IdAM system.

837 5.6.2 Build Network Components

838 **Internet** – The public Internet is accessible by the lab environment to facilitate both cloud
839 services and access for vendors and NCCoE administrators.

840 **VPN Firewall** – The VPN firewall is the access control point for vendors to support the
841 installation and configuration of their components of the architecture. We used this access to
842 facilitate product training and implementation support. This firewall also blocks unauthorized
843 traffic from the public Internet to the production networks. We used additional firewalls to
844 secure the multiple domain networks (OT, PACS, IT, and IdAM).

845 **Switching and Routing** – Switching in the architecture is executed using a series of physical and
846 hypervisor soft switches. VLANs are implemented to segment the networks shown in Figures 9
847 and 10. VLAN switching functions are handled by physical Dell switches and the virtual
848 environment. Routing was accomplished using the firewall.

849 **Demilitarized Zone** – The DMZ provides a protected neutral network space that the other
850 networks of the production network can use to route traffic to/from the Internet or each other.

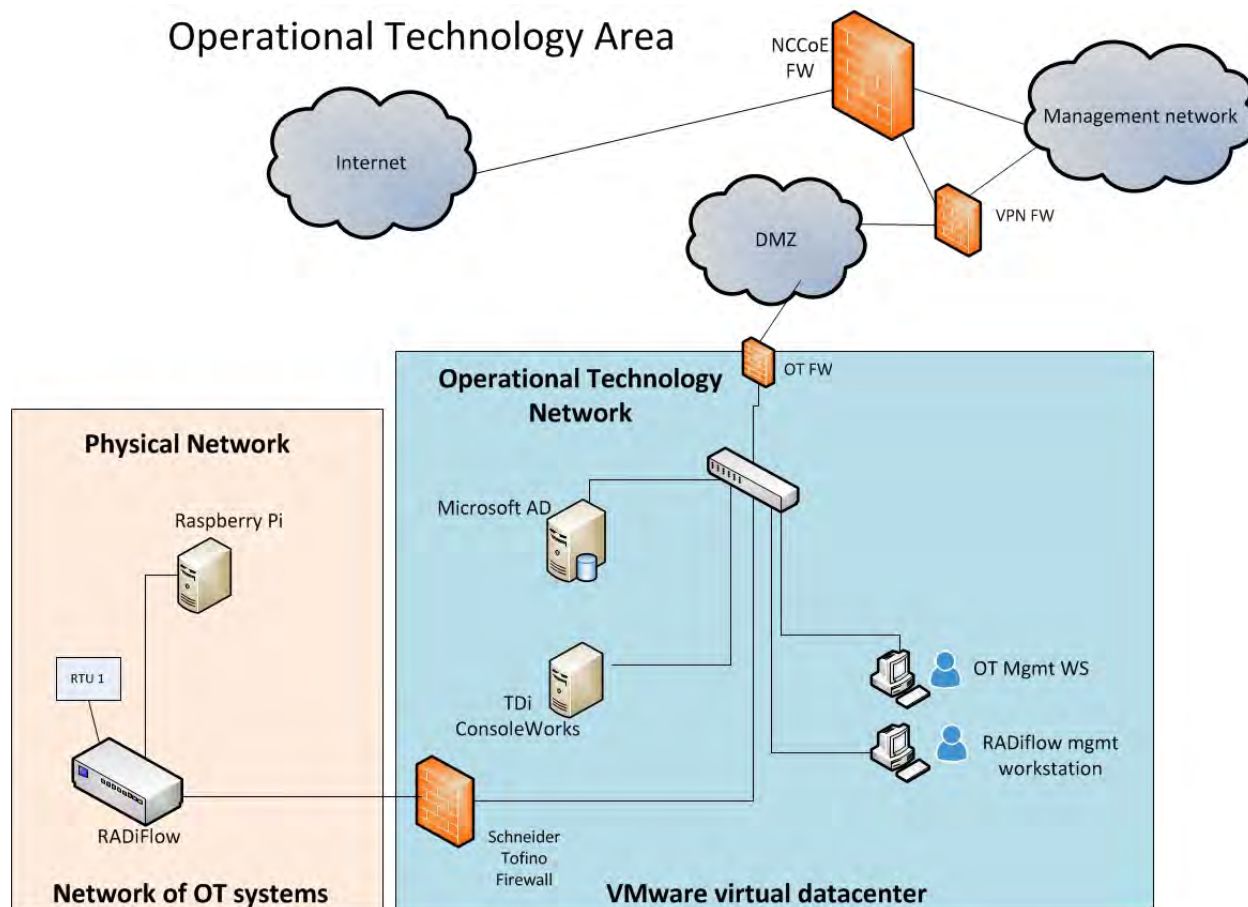
851 5.6.3 Operational Technology Network

852 The builds include the following OT network components:

- 853 • directory instance
- 854 • OT management workstation
- 855 • RTU with IP interface
- 856 • RTU with serial interface
- 857 • ICS/SCADA router
- 858 • router management workstation
- 859 • ICS/SCADA gateway/access control system

860 This network emulates an energy enterprise OT network and systems. The specific vendor
861 products used in this network are identified in Table 3 and Figure 12. OT network.

862



863

864

Figure 12. OT network

865 In the OT network, the RADiFlow router performs the ICS/SCADA network firewall function. The
 866 ConsoleWorks product provides the access control/gateway function. The build used the
 867 gateway function to manage access to the OT router and RTU management/console interface.
 868 The interface can be used to configure the RTU as well as issue real-time function commands
 869 (e.g., open/close relays). The access control/gateway uses the OT directory to obtain access
 870 authority for each user requesting access to an RTU.

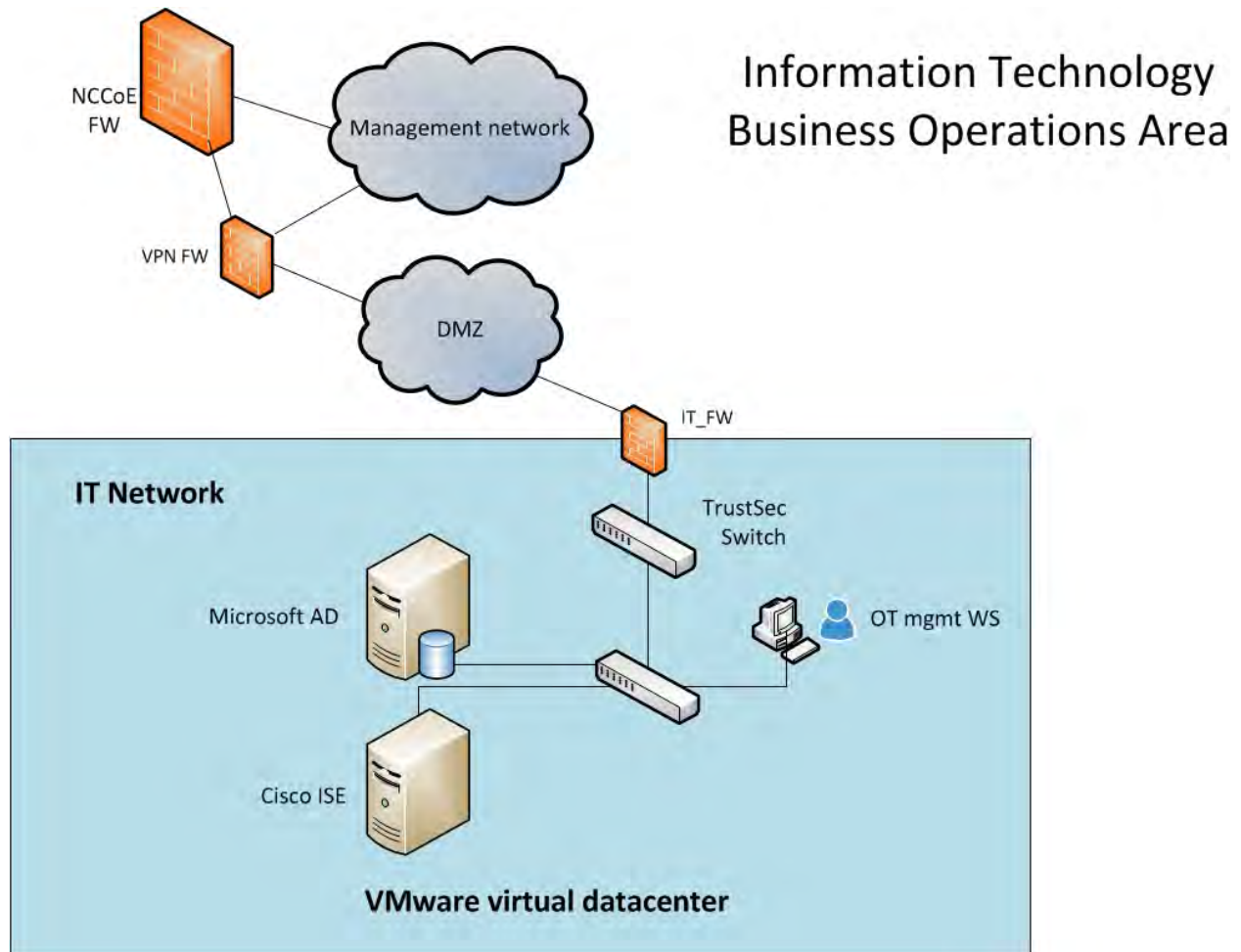
871 5.6.4 Information Technology Network

872 The builds include the following IT network components:

- 873 • Active Directory
- 874 • Cisco ISE
- 875 • TrustSec switch
- 876 • workstation

877 A typical enterprise includes information-sharing systems, email, and application servers. We
 878 did not include these systems in the architecture because they are not needed to demonstrate

879 the effectiveness of the IdAM example solution. The specific vendor products used in this
 880 network are identified in Table 3 and Figure 13.



881

882

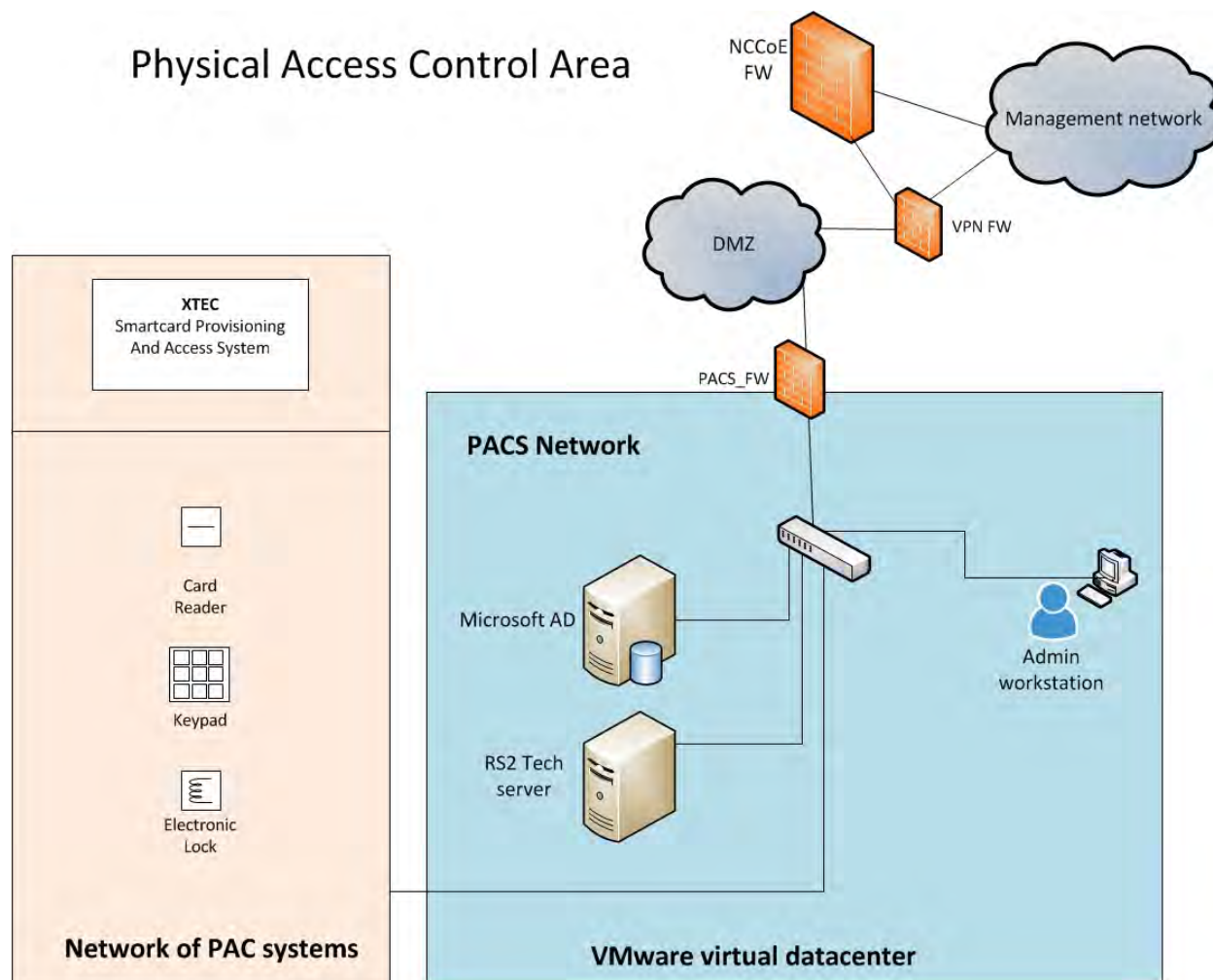
Figure 13. IT network

883 5.6.5 Physical Access and Control System Network

884 The builds include the following PACS network components:

- 885
- 886 • Active Directory
 - 887 • PACS control server – Access IT!
 - 888 • integrated access control unit (including a card reader, keypad, and door strike)—RS2 Technologies
 - 889 • workstation

890 This network emulates a typical enterprise PACS. The specific vendor products used in this
 891 network are identified in Table 3 and Figure 14.



892

893

Figure 14. PACS network

894 Two technologies are demonstrated in the PACS network: XTEC XNode and RS2 Technologies
 895 AccessIT!. XTEC XNode is a physical access system using smart card readers, pin pads, and an
 896 Internet cloud-based authorization service. The cloud service can federate (interoperate) with
 897 corporate identity and access stores or can be operated as a fully outsourced PACS IdAM
 898 solution. The RS2 Technologies system includes card readers, pin pads, and the AccessIT! local
 899 management server. The local management server is integrated with the central identity and
 900 access store via the AlertEnterprise Guardian product. In Build #1, Guardian receives IdAM data
 901 directly from Identity Manager. Once the information is received, Guardian provisions the
 902 information to the PACS management server. In Build #2, Guardian monitors the PACS directory
 903 for IdAM changes. Once changes are identified, Guardian collects the information and
 904 provisions the IdAM information to the PACS management server.

905 5.6.6 Identity and Access Management Network

906 5.6.6.1 Build #1

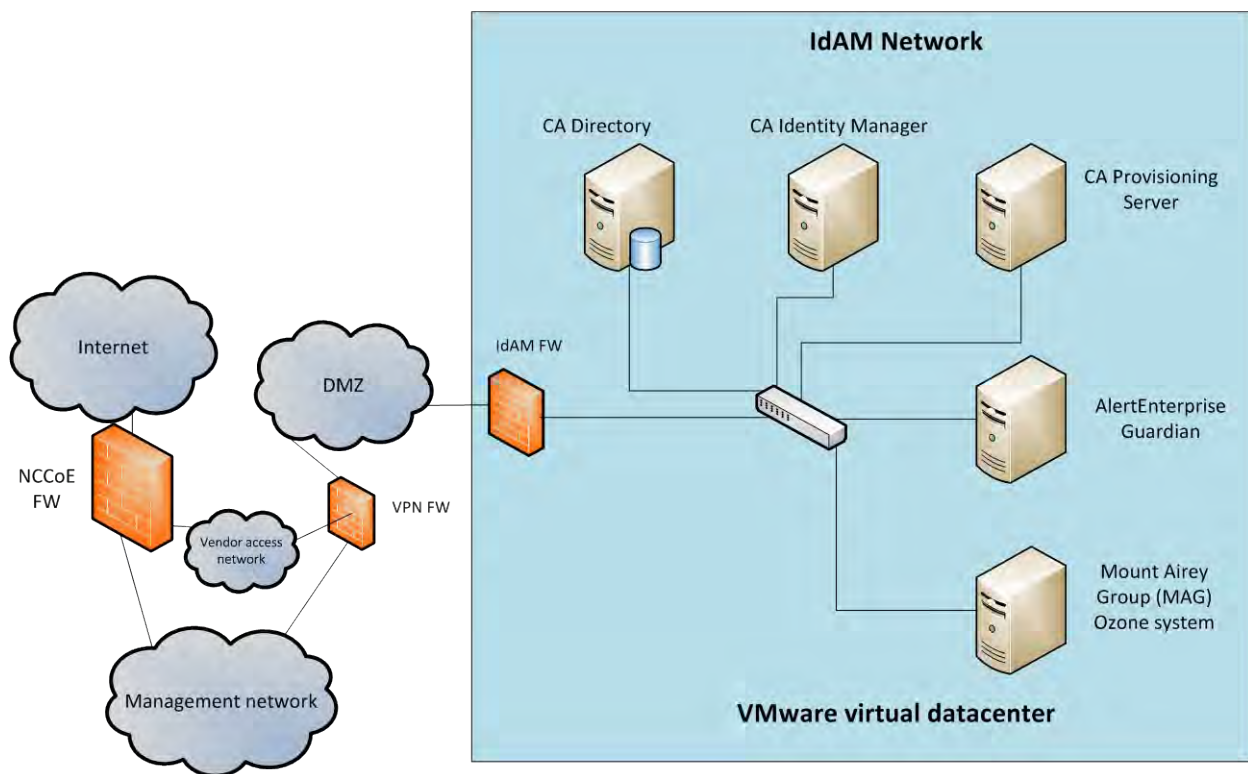
907 Build #1 includes the following IdAM network components:

- 908 • central IdAM system
- 909 • PACS IdAM interface system
- 910 • Structured Query Language (SQL) server
- 911 • MAG Ozone components

912 The IdAM was separated to highlight the unique IdAM components proposed to address the
 913 use case requirements. The implementation is not a recommendation to separate IdAM
 914 functions on their own network. The products used in this build are identified in Table 3 and
 915 Figure 15. Central IdAM network.

916

Identity and Access Management Area



917

918

Figure 15. Central IdAM network, Build #1

919 The central IdAM system is the authoritative central store for identity and access authorization
 920 data. CA Identity Manager provides central identity and access store as well as workflow
 921 management capability in Build #1 (see Figure 15). The central IdAM system takes over control
 922 of the directory instances in each silo. The control is implemented by providing an
 923 administrative account credential for each managed directory to the IdAM system. This is an
 924 important aspect of the implementation. When the administrative credential is issued, the
 925 organization must limit access to the managed directories of the IdAM system to a reduced

926 number of administrative users. The security of the solution partially depends on limited access
927 to the managed directories, as discussed in Section 5.9.6, Security Recommendations.

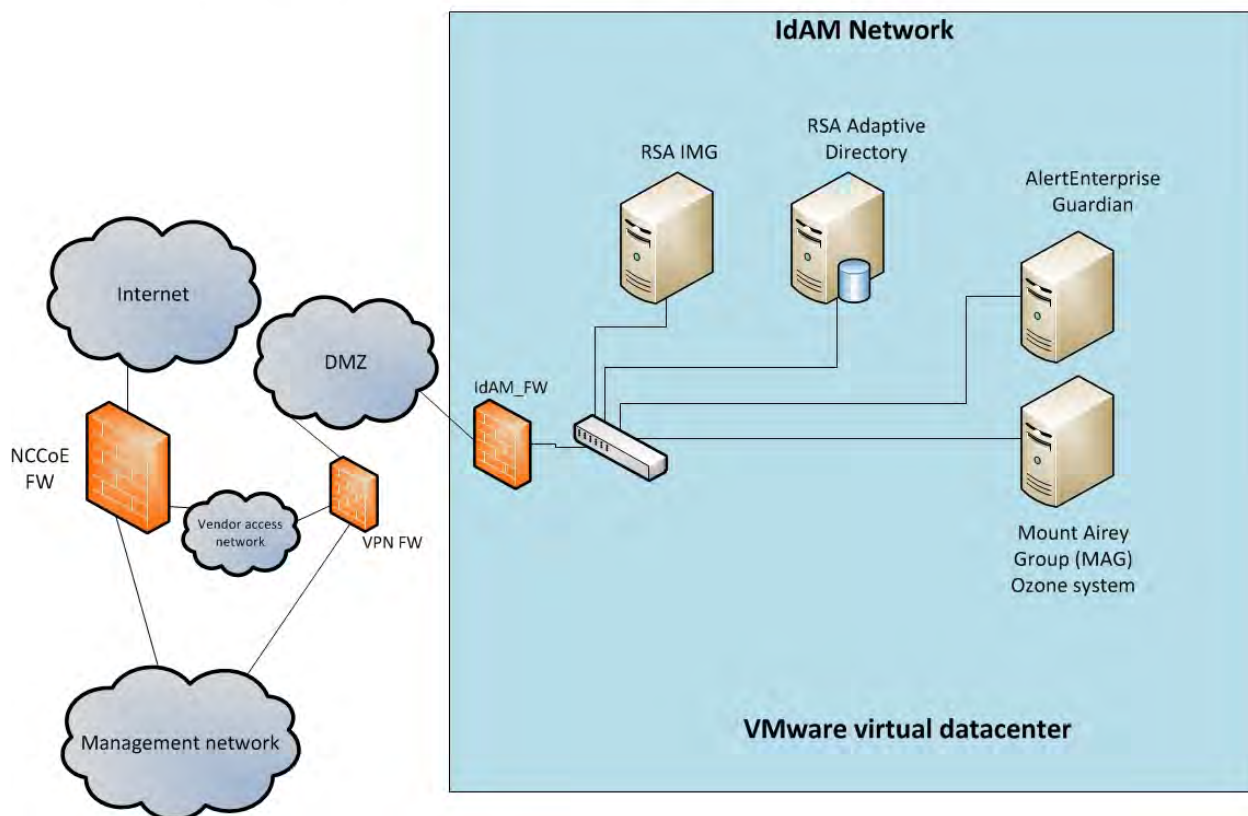
928 In this build, the OT, PACS, and IT directories synchronize (sync) with the central IdAM system
929 using Lightweight Directory Access Protocol Secure (LDAPS). This synchronization is set up to
930 sync changes immediately from the IdAM system to each directory. In addition, an automated
931 sync function can be implemented to check for unauthorized changes in each directory to
932 increase the security of the implementation. Automated sync was not implemented in this
933 build.

934 AlertEnterprise Guardian integrates the IdAM central store with the PACS access management
935 system (AccessIT!). Guardian includes integration and translation capabilities to transfer the
936 IdAM data to the AccessIT! management server database. In this build, Guardian is integrated
937 with Identity Manager for IdAM synchronization.

938 5.6.6.2 Build #2

939 The IdAM network components include a central IdAM system, PACS IdAM interface system,
940 and the MAG Ozone components. The IdAM network represents the proposed
941 centralized/converged identity and access management network/system. This network was
942 separated to highlight the unique IdAM components proposed to address the use case
943 requirements. The implementation is not a recommendation to separate IdAM functions own
944 their own network. The products used in this build are identified in Table 3 and Figure 16.
945 Central IdAM network, Build #2.

Identity and Access Management Area



946

947

Figure 16. Central IdAM network, Build #2

948 The central IdAM systems are the authoritative central store for identity and access
 949 authorization data. RSA IdAM products and AlertEnterprise provide central identity and access
 950 stores as well as workflow management capability. The central IdAM system takes over control
 951 of the directory instances in each silo. The control is implemented by providing an
 952 administrative account credential for each managed directory to the IdAM system. This is an
 953 important aspect of the implementation. When the administrative credential is issued, the
 954 organization must limit the access to the managed directories of the IdAM system to a reduced
 955 number of administrative users. The security of the solution partially depends on limited access
 956 to the managed directories, as discussed in Sections 5.9.6

957 In this build, the OT, PACS, and IT directories sync with the central IdAM system using LDAPS.
 958 This synchronization is set up to sync changes immediately from the IdAM system to each
 959 directory. The IdAM system automatically syncs with each directory to check for unauthorized
 960 changes to increase the security of the implementation.

961 In this build, Guardian was used to integrate the IdAM system with the PACS access
 962 management system (AccessIT!). Guardian includes integration and translation capabilities to
 963 transfer the IdAM data to AccessIT! Guardian monitors the PACS directory for IdAM updates.

964 The MAG Ozone product provides secure attribute distribution within the enterprise. Section
965 5.4 describes its use.

966 5.6.7 [Access Authorization Information Flow and Control Points](#)

967 The access and authorization for each user is based on the business and security rules
968 implemented in workflows within the central IdAM system products (RSA IMG, CA Identity
969 Manager). The workflows include management approval chains as well as approval/denial data
970 logging. Once the central IdAM system has processed the access and authority request, the
971 updated user access and authorization data is pushed to the central ID store. The central ID
972 store contains the distribution mechanism for updating the various downstream (synchronized)
973 directories with user access and authorization data. This process applies to new users,
974 terminated users (disabled or deleted users), and any changes to a user profile. Changes include
975 promotions, job responsibility changes, and anything else that would affect the systems a user
976 needs to access.

977 5.6.7.1 *OT Access and Authorization Information Flow*

978 This section describes the OT ICS/SCADA access and authorization information flow for both
979 builds.

OT Network Identity Access and Management

All messages traverse the DMZ between networks

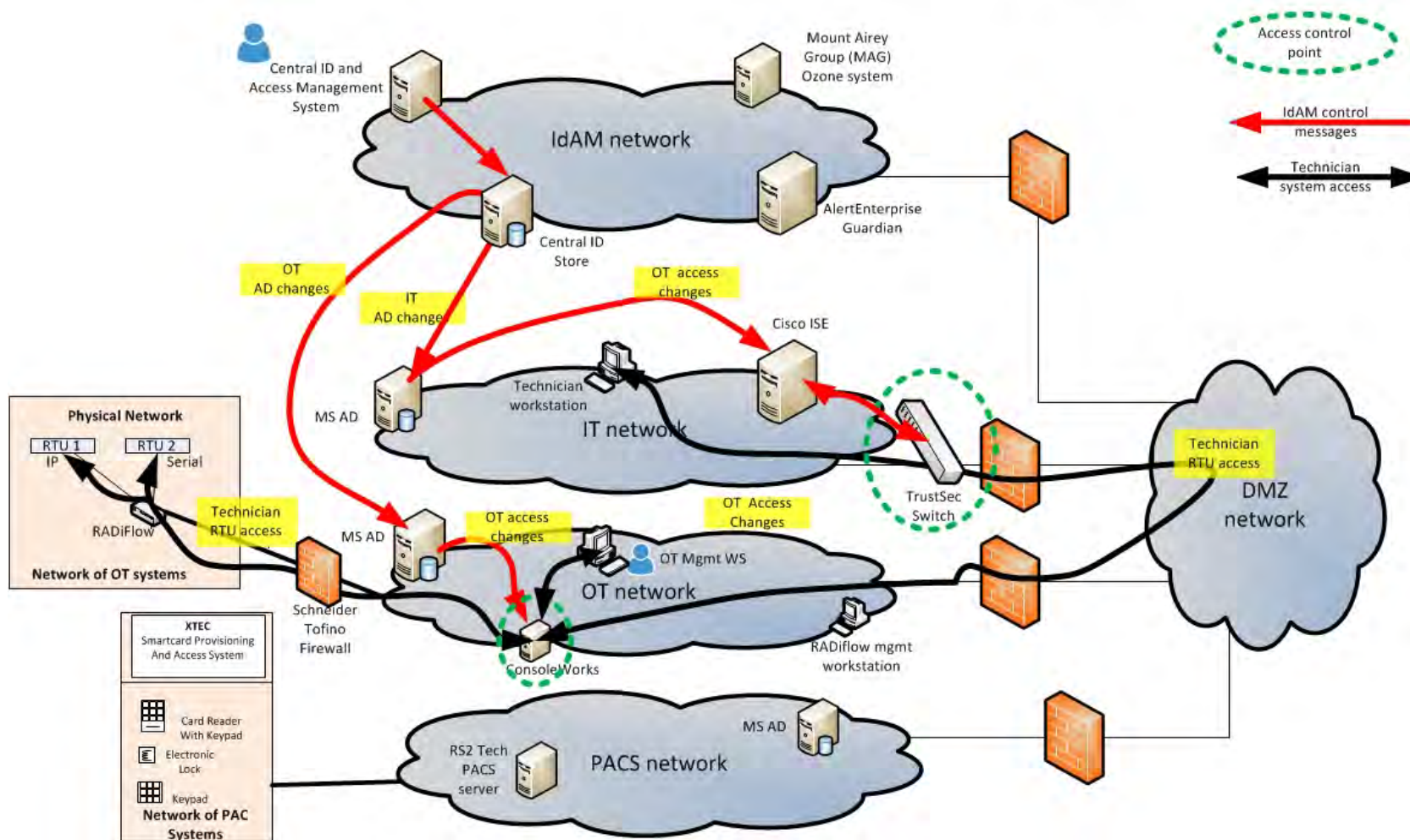


Figure 17. Access and authorization information flow for OT ICS/SCADA devices

DRAFT

1004 Figure 17 depicts the access and authorization information flow for OT ICS/SCADA devices. The
1005 red lines indicate the access and authorization data exchanges. The black lines depict the data
1006 paths of two OT ICS/SCADA technicians accessing RTUs in the SCADA network (one from the IT
1007 network and one from the OT network). Note that all data routed between networks flows
1008 through the DMZ and network firewalls.

1009 In the OT network, ConsoleWorks controls access to the OT ICS/SCADA devices. ConsoleWorks
1010 uses the OT directory to determine which users are authorized to access OT ICS/SCADA devices.
1011 It is the control point for users accessing OT network devices. ConsoleWorks stores profiles for
1012 groups and specific users. The profiles define which OT devices each user is authorized to
1013 access. In addition, ConsoleWorks monitors and logs each user session. This feature allows an
1014 organization to monitor user activity, block undesired activities, and generate alerts for
1015 suspicious or undesired activities.

1016 In the IT network, a TrustSec switch controls which users have access to the OT network. ISE
1017 controls the TrustSec switch. This meets the NERC CIP-005 requirement to maintain an
1018 electronic security perimeter between the ICS/SCADA network and the rest of the corporate
1019 networks. ISE uses the IT directory identity store to determine user access authority and limit
1020 access to the ICS/SCADA network to authorized users. This capability enhances the enterprise's
1021 ability to follow NERC CIP-005. ConsoleWorks also authorizes users to access OT devices.

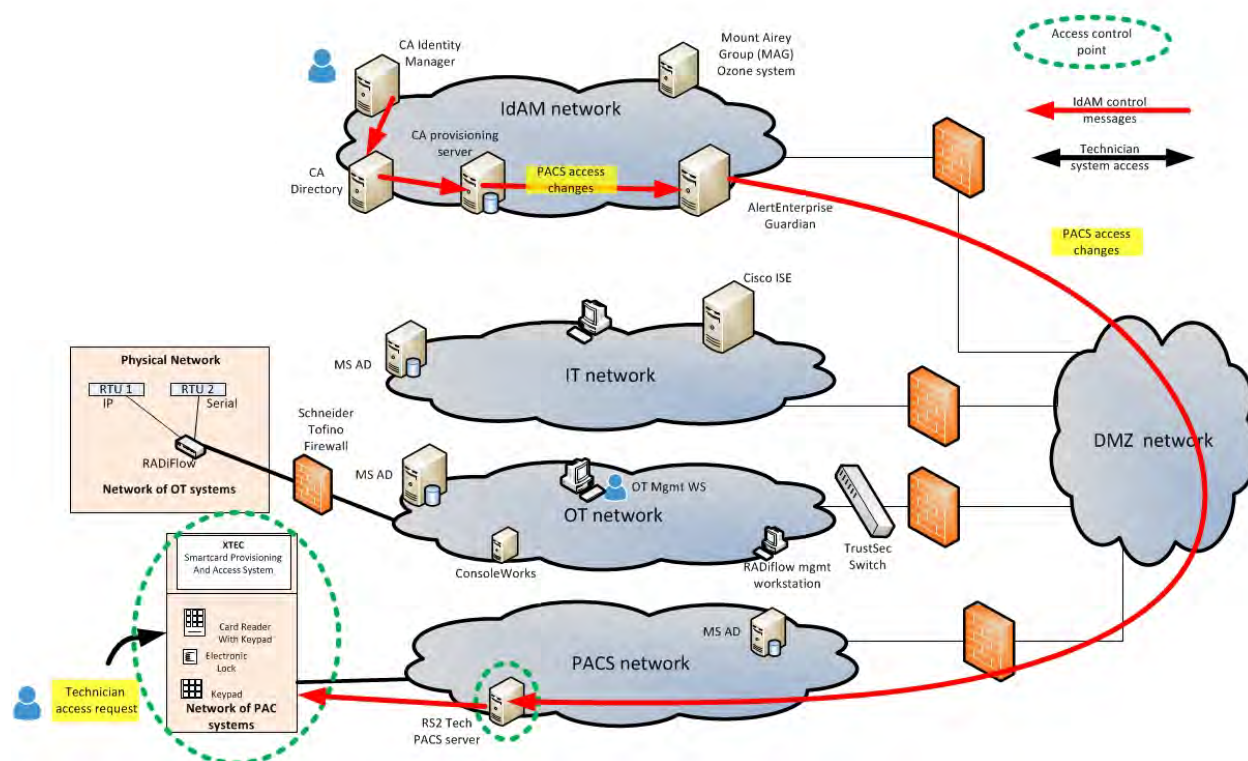
1022 *5.6.7.2 PACS Access and Authorization Information Flow*

1023 The PACS access and authorization information flows in each build are described below.

1024

PACS Network Identity Access and Management

All messages traverse the DMZ between networks



1026

1027

Figure 18. Access and authorization information flow for the PACS network, Build #1

1028 The PACS network includes devices such as door locks and keypads. In Figure 18, the red lines
 1029 indicate the access and authorization data exchanges. Note that all data routed between
 1030 networks flows through the DMZ and network firewalls.

1031 In the PACS network, the AccessIT! management server controls physical access to facilities,
 1032 rooms, and the like. AccessIT! updates the PACS devices as needed. The devices also report/log
 1033 user accesses to this server for logging/auditing purposes. In most environments, the PACS
 1034 network is segregated from other networks, typically using VLANs. Guardian provides the
 1035 access and authorization data that it collects from the Identity Manager provisioning server to
 1036 AccessIT!.

1037

PACS Network Identity Access and Management

All messages traverse the DMZ between networks

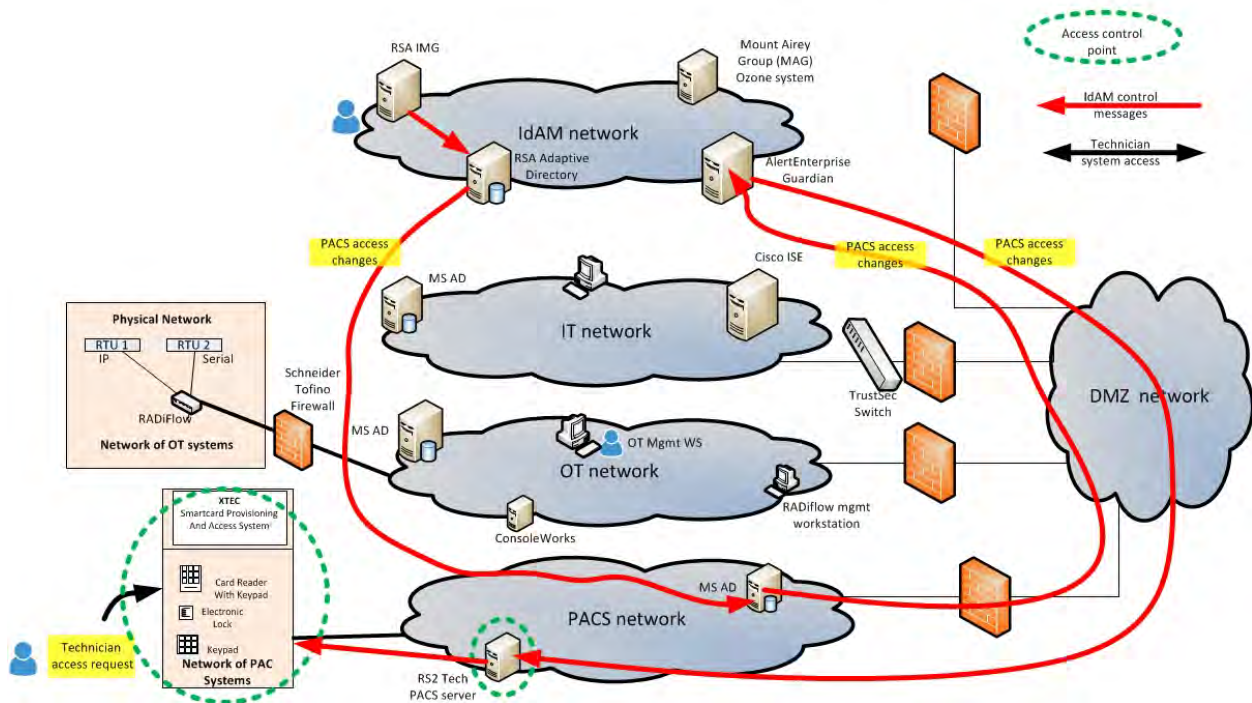


Figure 19. Access and authorization information flow for the PACS network, Build #2

The red lines in Figure 19 indicate the access and authorization data exchanges or PACS access in Build #2. In this build, IMG provisions all PACS IdAM data to the PACS directory.

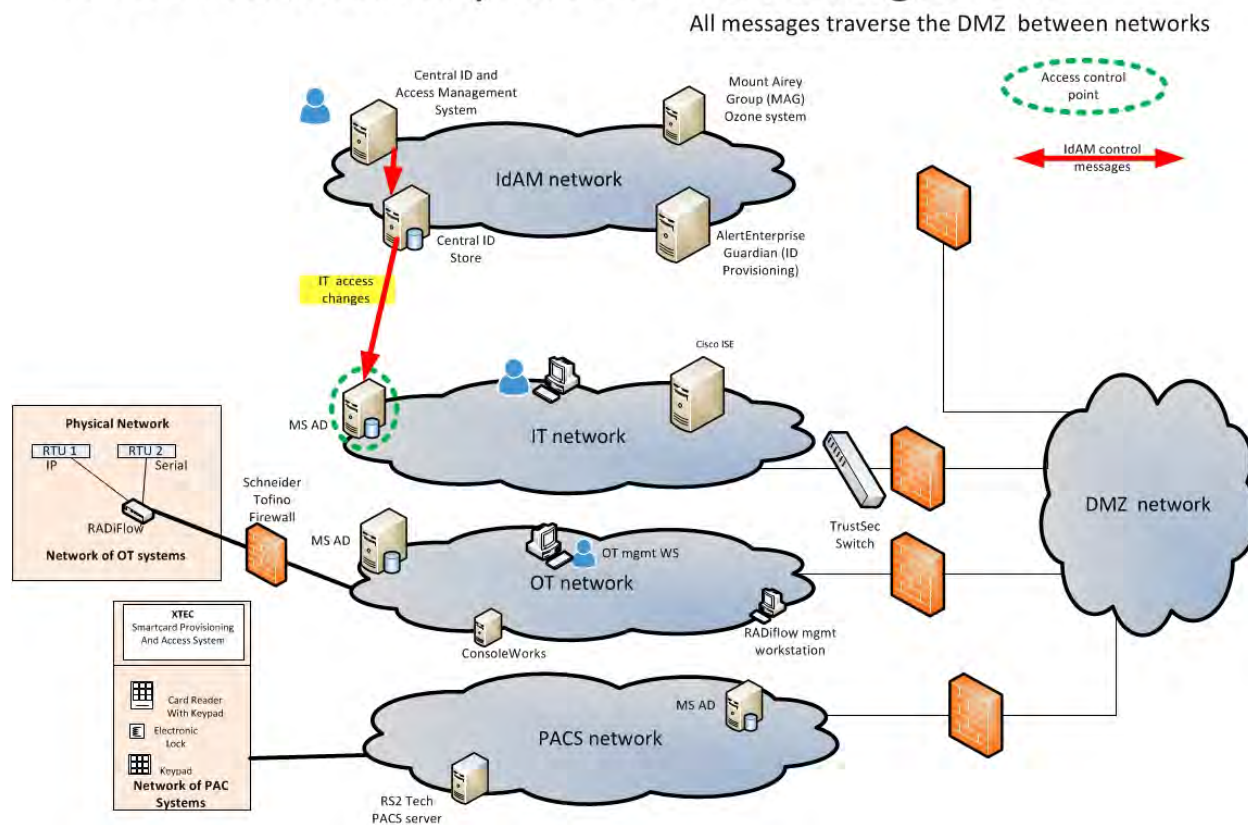
AlertEnterprise provides the access and authorization data that it collects from the PACS

directory to AccessIT!.

1046 5.6.7.3 IT Access and Authorization Information Flow

1047

IT Network Identity Access and Management



1048

1049

Figure 20. Access and authorization information flow for the IT network

1050 The red lines in Figure 20 indicate the access and authorization data exchanges in both builds.
 1051 Note that all data is routed among the OT, PACS, IT, and IdAM networks through the DMZ. In
 1052 the IT network, the hosts and other systems access the IT directory to determine which users
 1053 are authorized to access devices on the IT network. Active Directory provides the typical
 1054 identity store function of storing the access permissions.

1055 5.7 Data

1056 The builds required a user dataset to populate the central IdAM system. In both builds, the
 1057 IdAM system was initially populated with user data from a synthetic dataset. The dataset was
 1058 designed to mirror a typical HR system dataset export file. A .csv file was used, which is a typical
 1059 HR system export file type. The data included user names, titles, access assignments, unique
 1060 identifiers, and other details required to complete valid directory entries. Once the set of user
 1061 data was loaded into the IdAM system, each silo directory was provisioned with the appropriate
 1062 user data. Each silo directory was pre-configured with the group and attribute fields needed to
 1063 support the builds. For example, the OT network directory had user groups corresponding to
 1064 the ConsoleWorks user groups. The details are included in the How-To guide.

1065 **5.8 Security Characteristics Related to NERC-CIP**

1066 The example solution both impacts and is impacted by the requirement to conform to NERC-CIP
 1067 standards.²⁹

1068 Because the example solution uses routed protocols, by definition, it falls within the security
 1069 perimeter of the adopting electricity subsector organization.³⁰ According to NERC-CIP, there
 1070 must be a well-defined process for controlling access to all components within the
 1071 organization’s security perimeter.³¹ So, access to the IdAM network must be controlled.

1072 The example solution is informed by NERC-CIP requirements and may contribute to CIP-aligned
 1073 implementations by providing mechanisms for centralizing logging and auditing of all IdAM
 1074 activity efficiently and cost-effectively.³² With this solution in place, information regarding
 1075 which users have access to what components is easily available via the central identity store.
 1076 Without the solution, this information would have to be gathered separately from each of the
 1077 IT, OT, and PACS network access control/directory components.

1078 Table 4 describes how the centralized IdAM solution relates to NERC-CIP requirements.

1079 *Table 4. NERC-CIP Requirements*

NERC-CIP Requirement	IdAM Role
CIP 004-3a Maintain a list of individuals with logical or unescorted physical access to Critical Cyber Assets.	IdAM maintains, in the identity store, a record of all logical and physical access to resources. If critical cyber assets are identified as such, IdAM inherently maintains such a list.
CIP 004-3a Conduct a cybersecurity training program for individuals with logical or unescorted physical access to Critical Cyber Assets.	The IdAM workflow can be configured to check a training system before granting access to critical cyber assets.
CIP 004-3a Conduct personnel risk	The IdAM workflow can be configured to

²⁹ The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity standards provide specific requirements that apply to the bulk power system and were used as a reference by the development team. The proposed solution is designed to be CIP-informed. This document attempts to capture some of the key areas where CIP standards are relevant to elements of the solution and its implementation, for reference purposes. Please consult your NERC-CIP compliance authority for any questions on NERC-CIP compliance.

³⁰ NERC Standard CIP-002-3 Cyber Security – Critical Cyber Asset Identification, Requirements section R3.

³¹ NERC Standard CIP-005-3a Cyber Security – Electronic Security Perimeter(s), Requirements section R2.

³² NERC Standard CIP-007-3a Cyber Security – Systems Security Management, Requirements section R6.

NERC-CIP Requirement	IdAM Role
assessment. Individuals must have an acceptable risk assessment before being granted access to Critical Cyber Assets.	verify that individuals have an acceptable risk assessment before granting access to critical cyber assets.
CIP 004-3a A list of all personnel with logical or unescorted physical access to Critical Cyber Assets must be maintained.	The identity store maintains authoritative information on all logical and physical access to resources. The identity store is a list of all personnel with logical or unescorted physical access to critical cyber assets.
CIP 004-3a Personnel with logical of physical access to Critical Cyber Assets must have that access removed within 24 hours if terminated for cause and within 7 days otherwise.	The IdAM workflow receives information from the HR system on terminations and can immediately de-provision access for terminated employees. Information from the HR system will need to be provided to the IdAM workflow at least daily to meet the 24-hour constraint.
CIP 005-3 requires documentation of the process for authorizing access in accordance with NERC CIP 004-3.	The IdAM workflow is the process for authorizing access. The workflow design and implementation documents the process.

1080

1081 NERC CIP 005-3 requires cyber assets used in access control and/or monitoring of an electronic
1082 security perimeter to be protected per CIP requirements. In both builds, the IdAM workflow,
1083 the identity store, and the provisioning capability control the information used to make access
1084 control decisions. They are considered inside the electronic security perimeter and must be
1085 protected according to NERC-CIP requirements. Connections from the IdAM components to IT,
1086 OT, and PACS must be considered access points to the electronic security perimeter.

1087 **5.9 Evaluation of Security Characteristics**

1088 The security characteristic evaluation seeks to understand the extent to which the IdAM
1089 example solution provides a more secure, centralized, uniform, and efficient solution for
1090 managing authentication and authorization services and access control across three
1091 independent electricity subsector networks. In addition, it seeks to understand the security
1092 benefits and drawbacks of the example solution.

1093 5.9.1 *Scope*

1094 The evaluation included analysis of the example solution to identify weaknesses, discuss
1095 mitigations, and understand benefits and trade-offs.

DRAFT

1096 We considered the following elements of the IdAM example solution:

- 1097 • security functionality of components depicted within the OT, PACS, IT, and IdAM
1098 networks in Figure 2, and their interactions with each other, with the exception of the
1099 XTEC stand-alone access control system
- 1100 • analysis of the capabilities and overall workflow process for centralizing the
1101 management of authentication and authorization services on and access control to the
1102 IT, OT, and PACS networks, including assumptions, threats, vulnerabilities, mitigations,
1103 benefits, drawbacks, trade-offs, and risks related to the following characteristics:
 - 1104 ○ centralization
 - 1105 ○ automation
 - 1106 ○ audit (accountability and tracking)
 - 1107 ○ authentication
 - 1108 ○ authorization
 - 1109 ○ access control
 - 1110 ○ provisioning
- 1111 • new “cross-silo” attacks that would not have been possible without the centralized IdAM
1112 capability
- 1113 • how the example solution addresses the security characteristics listed in the use case
1114 description <https://nccoe.nist.gov/content/energy>
- 1115 • security recommendations that should be addressed when deploying the IdAM design in
1116 a real-world, operational environment
- 1117 • hands-on evaluation of the laboratory build as appropriate to support analysis and
1118 demonstrate value
- 1119 • security-related aspects of the OT, PACS, and IT networks as they potentially impact the
1120 solution posed by the example solution

1121 The following elements of the example solution were **not** considered:

- 1122 • evaluation of any specific vendor product or its implementation
- 1123 • considerations regarding how to secure direct access to each of the three energy
1124 networks (OT, PACS, and IT)
- 1125 • aspects of the build that are specific to the laboratory setting in which the build is
1126 implemented

1127 5.9.2 [Security Characteristics Evaluation Assumptions and Limitations](#)

1128 This security characteristic evaluation has the following limitations:

- 1129 • The evaluation examines the security claims made by the example solution; however, it
1130 is not a comprehensive test of all security components.
- 1131 • The evaluation cannot identify all weaknesses. Its purpose is to verify that the example
1132 solution meets its security claims, and to understand the trade-offs involved in doing so.
- 1133 • This is not a red team exercise. The intent was to verify the security claims, not to break
1134 hardware or software involved in the example solution.
- 1135 • The lab routers and firewalls were not included in the evaluation. It is assumed that they
1136 are hardened. Testing these devices would reveal only weaknesses in implementation
1137 that would not be of value to those adopting this example solution.

1138 5.9.3 Example Solution Analysis

1139 Table 5 lists the example solution components, their functions, and the security characteristics
1140 they provide. This analysis focuses on these security capabilities rather than on the vendor-
1141 specific components. In theory, any number of commercially available components can provide
1142 these security capabilities. Some of these components are in Build #1 of the IdAM example
1143 solution and others are in Build #2. We discuss them as generic components providing a specific
1144 security functionality rather than as vendor products. One vendor product could be substituted
1145 for another that provides the same security functionality without affecting the results of the
1146 evaluation.

1147 *Table 5. IdAM Components and Security Capability Mapping*

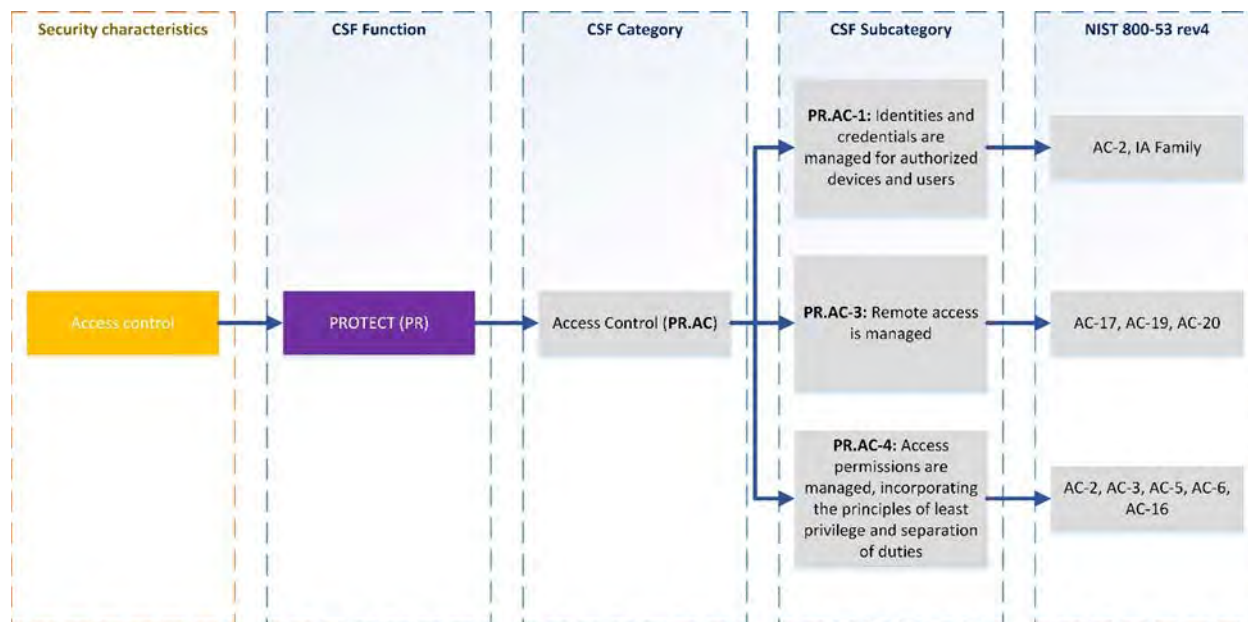
Component	Specific Product	Function	Security Characteristic
Identity, Authorization, and Workflow Manager	RSA IMG Or CA Identity Manager	IdAM workflow engine; manages identities, credentials, and authorization for all other network components in the use case. Enforces workflows to ensure that access control policies are enforced.	Authentication and authorization
Identity Store	RSA Adaptive Directory (identity Store), which is used with RSA IMG Or Windows SQL 2012, which is used with CA Identity Manager	Database of user identities	Authentication and authorization
High Assurance Attribute Service (AAS)	MAG Ozone System	Access control solution with ABAC architecture; provides increased assurance by signing attributes with private key infrastructure (PKI) and requiring users to authenticate with PKI	

Component	Specific Product	Function	Security Characteristic
Translator between Active Directory and PACS and OT Access Management Systems (AMS)	AlertEnterprise Guardian	Translates from RSA/CA IdAM stores on IdAM network to OT and PACS access management systems, enabling access management devices in the OT and PACS networks to be provisioned from the IdAM network	Authorization, access control
Directory Service	MS Active Directory (for IT devices) Or RS2 PACS Server (for PACS devices)	Database of PACS or IT resource and user identifiers and their associated security policies	Authentication and authorization
SCADA Router and Remote Manager (RM) of SCADA Router	RADiFlow	IP-addressable industrial control system gateway that enables remote control of physical devices: Management workstation enables remote management of physical SCADA router; SCADA router serves as firewall, terminal server, IP-to-serial connectivity	Access control
Network Access Control (AC) and Policy Enforcement System (PES)	Cisco ISE	Allows access policies for network endpoints to be controlled centrally	Network security
Stand-alone Smartcard Provisioning (SP) and Access System (AS)	XTEC	Smartcard-based physical access control	Authentication, authorization, access control

1148

1149 5.9.4 Security Characteristics Addressed

1150 One aspect of our security evaluation involved assessing how well the IdAM example solution
1151 addresses the security characteristics that it was intended to support. These security
1152 characteristics are listed in a security control map published in the appendix of the IdAM use
1153 case description
1154 (http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Identity_Access_Management.pdf).
1155 Six security characteristics are listed, each of which is further classified by the Cybersecurity
1156 Framework (CSF) categories and subcategories to which they map. The CSF subcategories
1157 further map to specific sections of each standard and best practice cited in the CSF in reference
1158 to that subcategory. Figure 21 depicts an example of the process.



1159

1160 *Figure 21. Example process for determining the security standards-based attributes for the example solution*

1161 We used the CSF subcategories to provide structure to the security assessment by consulting
 1162 the specific sections of each standard that are cited in reference to that subcategory. The cited
 1163 sections provide example solution validation points by listing specific traits that a solution that
 1164 supports the desired security characteristics should exhibit. Using the CSF subcategories as a
 1165 basis for organizing our analysis and consulting the specific sections of the security standards
 1166 that are cited with respect to each subcategory allowed us to systematically consider how well
 1167 the example solution supports the security characteristics identified in the use case description.

1168 The remainder of this subsection discusses how the example solution addresses the six desired
 1169 security characteristics that are listed in the use case description appendix:³³

- 1170 • authentication for OT
- 1171 • access control for OT
- 1172 • authorization (provisioning) OT
- 1173 • centrally monitor use of accounts
- 1174 • protect exchange of identity and access information
- 1175 • provision, modify or revoke access throughout all federated entities

1176 This section also discusses how the authentication, access control, and authorization
 1177 (provisioning) security characteristics are addressed for PACS.

³³ http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Identity_Access_Management.pdf

DRAFT

1178 5.9.4.1 *Authentication, Access Control, and Authorization for OT*

1179 The implementation includes the capabilities that support these security characteristics. Section
1180 5.6.7.1 describes the information flows for supporting authentication, access control, and
1181 authorization (provisioning) on the OT network.

1182 5.9.4.2 *Centrally Monitor Use of Accounts*

1183 The example solution supports centralized accountability and tracking of user accounts, with
1184 the IdAM identity, authorization, and workflow manager acting as the locus of this capability.

1185 On the OT network, the console access manager, which acts as the gatekeeper to all ICS/SCADA
1186 devices, monitors and logs all ICS/SCADA access requests and responses, as well as all user
1187 interactions with the ICS/SCADA OT devices. These logs should be centrally monitored along
1188 with other ICS/SCADA OT monitoring within the enterprise.

1189 The network access control component also logs all access requests and responses received at
1190 and generated by the IT network switch that controls access to the OT network from the IT
1191 network. These logs should be centrally monitored along with other ICS/SCADA OT monitoring
1192 within the enterprise.

1193 On the PACS network, the PACS devices also report/log user access requests and responses to
1194 the PACS server. These logs should be centrally monitored along with other ICS/SCADA OT
1195 monitoring within the enterprise. In addition, the IdAM identity, authorization, and workflow
1196 manager and the translator component log the PACS access change (add, delete, or change)
1197 requests.

1198 5.9.4.3 *Protect Exchange of Identity and Access Information*

1199 All IdAM-related information exchange between IdAM components (as shown by the red lines
1200 in Figures 17 – 20) should be performed in protected mode. In other words, at the least,
1201 integrity checking mechanisms are performed on this communication so that tampering can be
1202 detected. Preferably, these communications are encrypted. In particular, the following should
1203 be in protected mode:

- 1204 • all information exchange to/from the directory services in the IT, OT, and PACS networks
- 1205 • all information exchanges between the console access manager (e.g., the ConsoleWorks
1206 component in Figure 17) and the OT directory service
- 1207 • all information exchange between the PACS server and the PACS translator component
1208 (e.g., the AlertEnterprise component in Figures 18 and 19)

1209 Because of time constraints, the laboratory builds of the example solution did not include
1210 encryption or integrity assurance for every IdAM information exchange. Nevertheless, such
1211 protection is strongly recommended when deploying the example solution.

DRAFT

1212 5.9.4.4 *Provision, Modify, or Revoke Access*

1213 User authorizations for use of all IT, OT, and PACS network account assets, for ICS/SCADA
1214 devices, and for physical access to rooms, facilities, and the like are provisioned, modified, and
1215 revoked by modifying user authorization information in the central IdAM identity,
1216 authorization, and workflow manager (CA Identity Manager or RSA IMG). These components, in
1217 turn, propagate the changes to all entities used to make local authorization and access
1218 determinations. Such information propagation ensures that all attempts to access IT, OT, and
1219 PACS network assets, SCADA devices, and rooms and facilities are handled uniformly because
1220 they are subject to the same updated access and authorization information when the silo
1221 directory, console manager, PACS server, or other IdAM device is consulted in response to the
1222 access attempt.

1223 5.9.5 *Assessment of Reference Architecture*

1224 The IdAM example solution is not intended to encompass all aspects of electricity subsector
1225 organization operations. It was designed to centralize management of authorization and access
1226 in three disparate IdAM silos. Thus, our assessment considers the solution itself, not the
1227 broader problem of providing general security to all aspects of electricity subsector
1228 organization operations.

1229 The example solution includes three network silos (OT, PACS, and IT,), plus an IdAM network
1230 with numerous components that provide centralization, uniformity, and efficiency through the
1231 use of IdAM workflows. All threats and vulnerabilities that are present on the IT, OT, and PACS
1232 networks are also present in the example solution, so they will need to be addressed during
1233 solution deployment. This evaluation assumes that the OT, PACS, and IT, networks are already
1234 protected using physical access control and network security components such as firewalls and
1235 intrusion detection devices that are configured according to best practices.

1236 5.9.5.1 *Threats, Vulnerabilities, and Assumptions*

1237 This evaluation concerns the IdAM network itself, its components, and their interaction with
1238 IdAM components on the IT, OT, and PACS networks, which both provide the benefits afforded
1239 by the example solution and introduce new attack surfaces and potential threats. For example,
1240 each of the IT, OT, and PACS networks has directory services components that must be secured.
1241 If the information in these directories is not safeguarded against tampering, the organization is
1242 at risk. These directories must be safeguarded in both the existing three-silo architecture and
1243 the example solution. The example solution, however, includes additional, related directory
1244 components that must also be protected.³⁴

1245 The identity, authorization, and workflow manager and the identity store on the IdAM network
1246 must be protected from unauthorized access and their information safeguarded. All of the data

³⁴ Section 5.6 describes the components and products in each build of the reference solution.

1247 in the directory service components in the OT, PACS, and IT networks is accessible by the
1248 identity, authorization, and workflow manager and the identity store. The ability to propagate
1249 data from the IdAM network to the OT, PACS, and IT networks is the main strength as well as
1250 the greatest vulnerability of the example solution. If the IdAM identity store or the identity,
1251 authorization, and workflow manager that has access to it were compromised, this would
1252 equate to a compromise of each of the directory services in the IT, OT, and PACS networks. As a
1253 result, controlling access to the IdAM network, controlling access to each IdAM component,
1254 and securing communications among IdAM components is essential to securing the example
1255 solution. Therefore, analysis of the security of the IdAM network, its components, and the
1256 communications among IdAM components is central to the evaluation of the IdAM example
1257 solution.

1258 5.9.5.1.1. Controlling Access to the Identity, Authorization, and Workflow Manager³⁵

1259 The identity, authorization, and workflow manager on the IdAM network contains information
1260 regarding actual users and accounts for the OT, PACS, and IT. It manages the identities and
1261 credentials for the rest of the use case, but it does not manage them for itself. In other words,
1262 the identity, authorization, and workflow manager component itself does not control user
1263 access to the identity, authorization, and workflow manager. It has a separate set of user
1264 accounts and passwords that are specific to this component and that IdAM administrators use
1265 to log into it. This access must be strictly controlled so that only authorized IdAM
1266 administrators can log into the identity, authorization, and workflow manager. Users or
1267 authorized systems (such as HR or a work order management system) must log into the
1268 identity, authorization, and workflow manager to provision all electricity subsector systems
1269 (i.e., add identity information and authorization rules for new users, delete information for
1270 former users, and modify information as user authorizations change).

1271 There is no Active Directory running on the IdAM network. In the builds, access to the identity,
1272 authorization, and workflow manager and to all other components of the IdAM network is
1273 granted by the use of username and credential, presented either via Web interface or via each
1274 machine's operating system (OS) console. An organization deploying the example solution
1275 operationally would of course be free to implement alternative access control mechanisms.
1276 While both privileged and unprivileged users may access the identity, authorization, and
1277 workflow manager and other IdAM components, only highly privileged users should be
1278 permitted to create, delete, or modify accounts. Monitoring, logging, and auditing all activity
1279 performed directly on IdAM components such as the identity, authorization, and workflow
1280 manager or the identity store is essential to ensure that authorized users are not performing
1281 unauthorized activities.

³⁵ Section 4.3.2 describes the risks associated with access to the IdAM workflow.

1282 5.9.5.1.2. Logging Activity on IdAM Components

1283 Logging all activity performed on IdAM components is crucial for securing the example solution.
1284 Ideally, access to all components on the IdAM network should be logged for the purpose of
1285 auditing and accountability. The example solution is designed to allow logging of all user activity
1286 on IdAM systems (e.g., identity, access, and authorization changes). The example solution
1287 should also log all activity performed by administrators so that no activity is exempt from
1288 monitoring, logging, and audit. Here is a closer look at three different types of IdAM system
1289 users (in terms of the amount of privilege they have) and whether or not their activity should
1290 be logged.

1291 **Unprivileged users**, by definition, are not authorized to interact with any IdAM system. They
1292 cannot create an account on the identity, authorization, and workflow manager or modify the
1293 privileges of a user who already has an account. A user who works for HR, for example, who
1294 needs to add a user identity or modify a user's authorizations, would have an account on the
1295 identity, authorization, and workflow manager (that was set up by a privileged user) that allows
1296 him/her to add to or modify the information in the identity, authorization, and workflow
1297 manager component via Web interface. Such a user would never be able to access the identity,
1298 authorization, and workflow manager via its machine's OS console. Console access would
1299 enable the user to manage the operating system on which the component is running. All the
1300 unprivileged user needs is the ability to use his/her own, unprivileged, user-level account on
1301 the identity, authorization, and workflow manager's machine. Because the example solution is
1302 designed to monitor and log all activity that occurs over a Web interface, it will log all
1303 unprivileged user activity.

1304 **Administrators**, by definition, can access OS consoles and create user accounts on IdAM
1305 machines such as the identity, authorization, and workflow manager. However, they are not
1306 authorized to change the access control policies within the console access manager. As a result,
1307 when administrators access the consoles of an IdAM system operating system, they must do so
1308 via the console access manager. The console access manager will log and monitor all
1309 administrator activity at any OS console.

1310 **Super-administrators**, by definition, can not only access machine consoles and create user
1311 accounts on IdAM machine operating systems; they can change the access control policies
1312 within the console access manager. Therefore, the example solution cannot force them to use
1313 the console access manager when accessing the consoles of IdAM system machine operating
1314 systems. If super-administrators do access the consoles of IdAM system's OS without doing so
1315 via the console manager, their activity will not be logged or monitored. So, while super-
1316 administrators should be strongly encouraged by policy to use the console access manager,
1317 IdAM does not provide a technical mechanism to ensure that they will.

1318 Access to the identity store on the IdAM network must also be strictly controlled, and the
1319 identity store should be configured so that it will only perform addition, modification, and
1320 deletion requests received from the identity, authorization, and workflow manager. If the
1321 identity store were to accept updates or edits from another entity, the result could be
1322 catastrophic. Any updates made by an administrator would have to be made via machine

1323 console, so at least these would be logged. Updates made by a super-administrator could
1324 escape detection if the super-administrator were to defy organization policy and access the
1325 identity store console without going through the console access manager. We acknowledge
1326 insider threats but feel that mitigating the risk of insider threats presently relies more on
1327 organizational policy decisions rather than technology. Therefore, addressing insider threat is
1328 outside the scope of this project.

1329 5.9.5.1.3. Unauthorized Modification of Access and Authorization Information

1330 User identity and credential information is input into the identity, authorization, and workflow
1331 manager and then propagated to other IdAM components. If this information were deleted,
1332 modified, or falsified while in transit between components or while stored in a component, the
1333 result could be catastrophic. It is essential to protect access to each IdAM component so that
1334 adversaries cannot modify IdAM information stored in the components, and so IdAM
1335 information has at least its integrity and ideally its confidentiality protected when in transit
1336 between IdAM components.

1337 5.9.5.2 Mitigations: Essentials for Securing the IdAM Example Solution

1338 Based on the information flows for supporting OT authentication, OT access control, and OT
1339 authorization described in Section 5.6.7 securing the part of the IdAM example solution that
1340 supports OT access control requires:

- 1341 • securing access to the
 - 1342 ○ identity, authorization, and workflow manager, identity store, and network
 - 1343 access control components on the IdAM network (i.e., ensuring that only
 - 1344 authorized users can access and add, modify, or delete information on these
 - 1345 components)
 - 1346 ○ directory service and console access manager components on the OT network
 - 1347 (i.e., ensuring that only authorized users can access and add, modify, or delete
 - 1348 information on these components)
 - 1349 ○ IT network access control switch that serves as a gateway to the OT network
 - 1350 from the IT network
- 1351 • protecting the integrity of the information exchanged between the
 - 1352 ○ identity manager and the identity stores
 - 1353 ○ identity store and the directory service on the OT network
 - 1354 ○ directory service and the console access manager components on the OT
 - 1355 network, as well as the network access control and policy enforcement system
 - 1356 within the IT network
 - 1357 ○ network access control component identity stores
 - 1358 ○ network access control component on the IT network and the IT network access
 - 1359 control switch that serves as a gateway to the OT network

DRAFT

1360 Based on the information flows for supporting PACS authentication, PACS access control, and
1361 PACS authorization described in Section 5.6.7 securing the part of the IdAM example solution
1362 that supports PACS access control requires:

- 1363 • securing access to the
 - 1364 ○ identity, authorization, and workflow manager; identity store; and IdAM
 - 1365 translator components on the IdAM network (i.e., ensuring that only authorized
 - 1366 users can access and add, modify, or delete information on these components)
 - 1367 ○ IdAM identity store and PACS directory service components on the PACS network
 - 1368 (i.e., ensuring that only authorized users can access and add, modify, or delete
 - 1369 information on these components)
- 1370 • protecting the integrity of the information exchanged between the
 - 1371 ○ identity manager and identity stores
 - 1372 ○ identity store on the IdAM network and the PACS directory service on the PACS
 - 1373 network
 - 1374 ○ IdAM translator component on the IdAM network and the IdAM directory service
 - 1375 on the PACS network
 - 1376 ○ IdAM translator component on the IdAM network and the PACS management
 - 1377 server on the PACS network

1378 5.9.5.3 Trade-offs

1379 As mentioned earlier, the very characteristics that are the main objectives of the example
1380 solution, namely centralization and uniformity of the management of authorization and access,
1381 are also its main vulnerabilities. A successful attack on the IdAM network or its components
1382 could result in a compromise of one or all of the OT, PACS, and IT networks. Organizations that
1383 implement the example solution may incur additional costs to secure the IdAM network and its
1384 components.

1385 5.9.5.3.1 Benefits

1386 The benefits of the IdAM example solution include consolidated management of identity and
1387 access audit data; documented and repeatable business and security access decision processes
1388 (workflows); approval/denial data logging; rapid provisioning and de-provisioning using
1389 consistent, efficient, and automated processes; and better situational awareness through the
1390 ability to track and audit all access requests and other IdAM activity across all four networks.
1391 Other important benefits include greatly reduced time to implement access control changes
1392 and highly automated identity synchronization across silos. For example, an OT, PACS, and/or IT
1393 access change request can be implemented in minutes. These benefits directly reduce the cost
1394 of the regulatory audit requirements imposed on the energy industry. They enable IdAM
1395 processes to be handled efficiently, and with more granular, prompt, and cost-effective control.

1396 5.9.6 Security Recommendations

1397 While the example solution provides a centralized IdAM security solution, the solution itself
1398 provides a single attack vector that, if compromised, could have devastating consequences.
1399 Therefore, an organization that implements the example solution must take great care to
1400 secure the IdAM example solution itself. When deploying their own implementations,
1401 organizations should adhere to the following security recommendations:

- 1402 • Conduct their own evaluations of their example solution implementation.
- 1403 • Deploy all components on securely configured operating systems that use multifactor
1404 authentication and are configured according to best practices.³⁶
- 1405 • Ensure that all operating systems on which example solution implementation
1406 components are running are hardened, maintained, and kept up-to-date in terms of
1407 patching, version control, and virus and malware detection.
- 1408 • Put into place a security infrastructure that will protect the example solution itself and
1409 secure the communications among the components on the IdAM network and between
1410 these components and the IdAM components on the other three networks, as described
1411 in Section 5.9.5.2. Many of the remaining recommendations relate to providing such a
1412 security infrastructure.
- 1413 • Design the authorization and workflow policies that are enforced by the identity,
1414 authorization, and workflow manager component to enforce the principle of least
1415 privilege and separation of duties.
- 1416 • Design the authorization and access control policies that govern user access to the IdAM
1417 components themselves to enforce the principle of least privilege and separation of
1418 duties.
- 1419 • Segregate IdAM components onto their own network, either physically or using private
1420 VLANs and port-based authentication or similar mechanisms.³⁷
- 1421 • Deploy a security infrastructure to secure the IdAM network and the IdAM platforms
1422 themselves. This infrastructure must consist of a holistic set of components that work
1423 together to prevent the IdAM network, components, and workflow from being used as
1424 an attack vector.
- 1425 • Protect the IdAM network using security components such as firewalls and intrusion
1426 detection devices that are configured according to best practices.

³⁶ The laboratory instantiation of the example solution builds did not implement every rule or guide in the STIGs upon which the builds installations were based. Exceptions were made to allow for only the needed operation of the solution. See the How-To section for details.

³⁷ IEEE 802.1X is a standard for Port-based Network Access Control that provides an authentication mechanism to devices that are to be attached to a local area network.

- 1427
- 1428
- 1429
- 1430
- 1431
- 1432
- 1433
- 1434
- 1435
- 1436
- 1437
- 1438
- 1439
- 1440
- 1441
- 1442
- 1443
- 1444
- 1445
- 1446
- 1447
- 1448
- 1449
- 1450
- 1451
- 1452
- 1453
- 1454
- 1455
- 1456
- 1457
- 1458
- 1459
- 1460
- 1461
- 1462
- 1463
- 1464
- 1465
- 1466
- Protect each of the OT, PACS, and IT, networks using security components such as firewalls and intrusion detection devices that are configured according to best practices.
 - Strictly control physical access to the OT, PACS, IT, and IdAM networks.
 - Configure firewalls to limit connections between the IdAM network and the production (IT, OT, and PACS) networks, except for connections needed to support required internetwork communications to specific IP address and port combinations in certain directions. The primary required, authorized internetwork communications are user authorization updates from the identity, authorization, and workflow manager component to the directory services on the production networks, the OT console access manager, and the PACS server, and logging information in the reverse direction. Firewalls should block all incoming connections from the Internet and to limit outgoing connections to the Internet, if any, to specific systems and required ports.
 - Perform all IdAM-related information exchanged between IdAM components (as shown by the red lines in Figures 17 - 20) in protected mode, meaning that, at the least, integrity checking mechanisms are performed on this communication so that tampering can be detected. Preferably, these communications should be encrypted. In particular:
 - Perform all information exchange to/from the directory services in each of the OT, PACS, and IT, networks in protected mode.
 - Perform all information exchange between the console access manager (i.e., the ConsoleWorks component in Figure 17) and the OT directory service in protected mode.
 - Perform all information exchange between the network access control manager (i.e., the Cisco ISE component in Figure 17) and the switch in the IT network that controls access to the OT network in protected mode.
 - Perform all information exchange between the PACS server and the PACS translator component (e.g., the AlertEnterprise component in Figure 18 and 19 in protected mode.
- In the case of IdAM exchanges with the silo directories, protected mode is defined as the use of Start Transport Layer Security (TLS) (RFC 2830) rather than LDAPS, which uses Secure Socket Layer and has been deprecated in favor of Start TLS.
- Install, configure, and use each component of the example solution (e.g., the identity, authorization, and workflow manager or the PAC server) according to the security guidance provided by the component vendor.
 - Configure all IdAM components on the IdAM network so that it is impossible to access them remotely.
 - Log all IdAM activity, for example direct access to IdAM components on the IdAM network and all messages exchanged between IdAM components. Limit the number of users able to control whether or not activity performed is logged.
 - Require super-administrators (i.e., users who are authorized to change the access control policies within the console access manager) to use a console access manager

1467 when accessing the console of all devices on the IdAM network and never to access any
1468 console directly. Use of a console access manger ensures that all activity performed via
1469 the console is logged.

1470 • Configure the console access manager to have an always-on connection to all devices on
1471 the IdAM network so that it can monitor each device’s console port. This configuration
1472 ensures that all activity performed over the console port will be logged. Configure the
1473 console access manager to generate an alert if the always-on connection to any device is
1474 disconnected. This configuration ensures that security auditors can be aware of any
1475 times during which the console port of a device may have been accessed without the
1476 activity being logged or monitored.

1477 • Configure all devices on the IdAM network so that they have only one console port (the
1478 port to which the console access manager has an always-on connection). Alternatively
1479 (where applicable), configure the devices on the IdAM network to allow only one
1480 console connection or login at a time. This will ensure that the console access manager
1481 will log all activity performed via the console of any of these devices.

1482 5.9.7 [Security Characteristics Evaluation Summary](#)

1483 Overall, the example solution and the workflow processes that it enforces succeed in
1484 centralizing IdAM functions across the OT, PACS, and IT networks to provide an efficient,
1485 uniform, and secure solution for authenticating and authorizing access across all systems and
1486 facilities. The solution enables access control policies across all three networks to be enforced
1487 consistently, quickly, and with a high degree of granularity, so that users are granted only
1488 enough privilege necessary to complete their work for only the necessary amount of time. It
1489 also enables a centralized, simplified audit capability for accountability and tracking. Such
1490 benefits come with a cost. This cost is the requirement to secure and log all access to the IdAM
1491 network, its components, and the information exchanged between these components and
1492 IdAM components on the OT, PACS, and IT, networks.

1493 **6 FUNCTIONAL EVALUATION**

1494 We conducted a functional evaluation of the IdAM example solution to verify that several
1495 common key provisioning functions of the example solution, as implemented in our laboratory
1496 build, worked as expected. The IdAM workflow capability demonstrated the ability to centrally

- 1497 • assign and provision access privileges to users based on a set of programmed business
1498 rules in the OT, PACS, and IT, networks and systems
- 1499 • create, activate, and deactivate users in the OT, PACS, and IT, networks and systems
- 1500 • change an existing user’s access to the various networks and systems

1501 Section 6.1 explains the functional test plan in more detail and lists the procedures used for
1502 each of the functional tests.

1503 **6.1 IdAM Functional Test Plan**

1504 This test plan includes the test cases necessary to conduct the functional evaluation of the
 1505 IdAM use case. The IdAM implementation is currently deployed in a lab at the NCCoE. Section 5
 1506 describes the test environment.

1507 Each test case consists of multiple fields that collectively identify the goal of the test, the
 1508 specifics required to implement the test, and how to assess the results of the test. Table 6
 1509 provides a template of a test case, including a description of each field in the test case.

1510

Table 6. Test Case Fields

Test Case Field	Description
Parent requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
Associated Security Controls	The NIST SP 800-53 rev 4 controls addressed by the test case.
Description	Describes the objective of the test case.
Associated test cases	In some instances a test case may be based on the outcome of another test case(s). For example, analysis-based test cases produce a result that is verifiable through various means such as log entries, reports, and alerts.
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected results	The specific expected results for each variation in the test procedure.
Actual results	The actual observed results in comparison with the documented expected results.

Overall result	The overall result of the test as pass/fail. In some test case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.
----------------	---

1511

1512 **6.2 IdAM Use Case Requirements**

1513 This section identifies the ES IdAM functional evaluation requirements that are addressed using
 1514 this test plan. Table 7 lists those requirements and associated test cases.

1515 *Table 7. IdAM Functional Requirements*

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 1	The IdAM system shall include an IdAM workflow capability that assigns and provisions access privileges to users based on a set of programmed business rules in the following networks:			
CR 1.a		IT		
CR 1.a.1			Allow access	IdAM-1
CR 1.a.2			Deny access	IdAM-1
CR 1.b		OT		
CR 1.b.1			Allow access	IdAM-1
CR 1.b.2			Deny access	IdAM-1
CR 1.c		PACS		
CR 1.c.1			Allow access	IdAM-1
CR 1.c.2			Deny access	IdAM-1
CR 2	The IdAM system shall include an IdAM workflow capability that can create and activate new users in the following networks and systems:			
CR 2.a		IT		IdAM-2
CR 2.b		OT		IdAM-2
CR 2.c		PACS		IdAM-2

DRAFT

CR 3	The IdAM system shall include an IdAM workflow capability that can de-activate users in the following networks and systems:			
CR 3.a		IT		IdAM-2
CR 3.b		OT		IdAM-2
CR 3.c		PACS		IdAM-2
CR 4	The IdAM system shall include a workflow capability that can change an existing user access to the various networks and systems.			
CR 4.a		IT		
CR 4.a.1			Allow to deny	IdAM-3
CR 4.a.2			Deny to allow	IdAM-3
CR 4.b		OT		
CR 4.b.1			Allow to deny	IdAM-3
CR 4.b.2			Deny to allow	IdAM-3
CR 4.c		PACS		
CR 4.c.1			Allow to deny	IdAM-3
CR 4.c.2			Deny to allow	IdAM-3

1516

1517

1518 **6.3 Test Case: IdAM-1**

1519

Table 8. Test Case ID: IdAM-1

Parent requirement (CR 1) The IdAM system shall include an IdAM workflow capability that assigns and provisions access privileges to users based on a set of programmed business rules in the following networks and systems:

(CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS

Testable requirement (CR 1.a.1-2) IT, (CR 1.b.1-2) OT, (CR 1.c.1-2) PACS

Description Show that the IdAM solution can assign and provision access in the OT and IT networks as well as in the PACS network and system, including allowing and denying access.

Associated test cases

Associated Security Controls AC-2, AC-3, IA-2, PE-2, PE-3

Preconditions

1. HR representative .csv file is available.
2. IdAM example solution is implemented and operational in the lab environment
3. Standard and privileged user sets are known to the testers.
4. A PACS system with a card reader and simulated door access demonstration system is operational in the lab.
5. A simulated OT network with an RTU and RTU emulator (Raspberry Pi) is implemented in the lab.

Procedure

1. Activate IdAM workflow engine and run command to ingest the HR .csv file.
2. At a workstation on the IT network, attempt to log in as a user known to have access in the IT network.
3. At a workstation on the IT network, attempt to log in as a user known to be denied in the IT network.
4. At a workstation on the OT network, attempt to log in as a user known to have access in the OT network.
5. At a workstation on the IT network, attempt to access the Schweitzer Engineering Laboratories (SEL) RTU administrative interface as a user

known to have access to the SEL RTU.

6. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user known to have access to the RTU emulator.
7. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a user known to be denied access to the SEL RTU.
8. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user known to be denied access to the RTU emulator.
9. At a workstation on the OT network, attempt to log in as a user known to be denied access in the OT network.
10. At the demonstration PACS card reader, attempt an “access” with a card for a user known to have access allowed.
11. At the demonstration PACS card reader, attempt an “access” with a card for a user known to not have access allowed.

**Expected results
(pass)**

Network Access Allowed

Users with allowed access are able to log into a workstation on the IT network.

Users with allowed access are able to log into a workstation on the OT network as well as the SEL RTU and RTU emulator.

Users with allowed access are able to log into a workstation on the PACS network.

Users with allowed access are authorized and allowed access by the PACS card reader and door access demonstration system.

Network Access Denied

Users who are denied access to the IT network are unable to log into a workstation on the IT network.

Users who are denied access to the OT network are unable to log into a workstation on the OT network as well as the SEL RTU and RTU emulator.

Users who are denied access PACS network are unable to log into a workstation on the PACS network.

Users without access are not authorized and not allowed access by the PACS

card reader and door access demonstration system.

Actual results

This test functioned appropriately and provided the expected results. User that were denied access were unable to login to the OT and IT networks, and denied access to PACS. Users granted access to each system were able to access the OT and IT networks and granted access via PACS.

Overall result

Pass

1520

1521

1522 **6.4 Test Case IdAM-2**

1523

Table 9. Test Case ID: IdAM-2

Parent requirement	(CR 2) The IdAM system shall include an IdAM workflow capability that can create and activate new users in the following networks and systems: (OT, PACS, IT,) (CR 3) The IdAM system shall include an IdAM workflow capability that can de-activate users in the following networks and systems: (IT, OT, PACS)
Testable requirement	(CR 2.a) IT, (CR 2.b) OT, (CR 2.c) PACS (CR 3.a) IT, (CR 3.b) OT, (CR 3.c) PACS
Description	Show that the IdAM solution can create new users, assign access based on business rules, and provision those users to the appropriate network and system access control systems. New users are users without entries in the authoritative identity store.
Associated test cases	CR 1
Associated security controls	AC-2, AC-3, AC-5, AC-16, AU-12, IA-2, IA-4, IA-5, IA-6, PE-2, PE-3, PE-6
Preconditions	New HR .csv file created with new users included.
Procedure	<ol style="list-style-type: none"> 1. Demonstrate that the new users in the HR .csv file do not have access in the OT, PACS, or IT, networks or systems using Test Case IdAM-1. 2. Perform procedure 1 of CR 1 with the new HR .csv file. 3. At a workstation on the IT network, attempt to log in as a new user known to have access in the IT network. 4. At a workstation on the OT network, attempt to log in as a new user known to have access in the OT network. 5. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a new user known to have access to the SEL RTU. 6. At a workstation on the IT network, attempt to access the RADiFlow router administrative interface as a new user known to have access to the RADiFlow router administrative interface. 7. At a workstation on the PACS network and system, attempt to log in as a new user known to have access in the PACS network and demonstration

system.

8. At a PACS card reader, attempt an “access” with a card for a new user known to have access allowed.
9. Using the IdAM system, deactivate access for one or more users with access to the OT, PACS, and IT, networks and systems. If one user has access to all three, deactivating that user is sufficient.
10. At a workstation on the IT network, attempt to log in as a recently deactivated user known to previously have access in the IT network.
11. At a workstation on the OT network, attempt to log in as a recently deactivated user known to previously have access in the OT network.
12. At a workstation on the IT network, attempt to access the SEL RTU administrative interface as a user known to previously have access to the SEL RTU.
13. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user known to previously have access to the RTU emulator.

**Expected results
(pass)**

(CR 2) Create and activate a new user.

New users are created and access to the three networks and systems is confirmed.

(CR 2.a) IT

(CR 2.b) OT network, SEL RTU and RTU emulator

(CR 2.c) PACS network and demonstration card reader access system

(CR 3) Deactivate a user.

User is deactivated and access is denied to the network(s) and systems that the user previously had allowed access.

(CR 3.a) IT

(CR 3.b) OT network, SEL TRU, and RTU emulator

(CR 3.c) PACS network and demonstration card reader access system

Actual results

This test was conducted with the expected results received. A CSV file with users was successfully uploaded. Upon approval of the user access stated in the file, the user accounts successfully logged into OT, PACS, and IT. User

access was deactivated and the deactivation approved. The users were no longer able to access the OT, PACS, or IT.

Overall result Pass

1524 6.5 Test Case IdAM-3

1525

Table 10. Test Case ID: IdAM-3

Parent requirement (CR 4) The IdAM system shall include a workflow capability that can change an existing user's access to the various networks and systems.

(CR 4.a) IT, (CR 4.b) OT, (CR 4.c) PACS

Testable requirement (CR 4.a.1, CR 4.b.1, CR 4.c.1) Allow to deny
(CR 4.a.2, CR 4.b.2, CR 4.c.2) Deny to allow

Description Show that the IdAM solution can change user access for any network or system.

Associated test cases CR 2

Associated security controls AC-2, AC-3, AC-5, AC-6, AC-16, AU-12, CM-7, IA-2, IA-4, IA-5, IA-6, PE-2, PE-3, PE-6

Preconditions Reuse IdAM system in the state after IdAM-2 is completed.

Procedure

1. Choose a set of users with known access and a set of users without access for each of the OT, PACS, and IT networks and systems.
2. Use the IdAM workflow to deny access for the set of users with known access chosen in 1 above.
3. Use the IdAM workflow to allow access for the set of users without access chosen in 1 above.
4. At a workstation on the IT network, attempt to log in as a user whose access had been changed from "allowed" to "denied".
5. At a workstation on the IT network, attempt to log in as a user whose access had been changed from denied to allowed.
6. At a workstation on the OT network, attempt to log in as a user whose access had been changed from allowed to denied.
7. At a workstation on the OT network, attempt to log in as a user whose access had been changed from denied to allowed.

8. At a workstation on the PACS network, attempt to log in as a user whose access had been changed from allowed to denied.
9. At a workstation on the PACS network, attempt to log in as a user whose access had been changed from denied to allowed.
10. At a PACS card reader, attempt an “access” with a card for a user whose access had been changed from allowed to denied (card access denied in the demo system).
11. At a PACS card reader, attempt an “access” with a card for a user whose access had been changed from denied to allowed (card access allowed in the demo system).
12. At a workstation on the IT network, attempt to access the RADiFlow router administrative interface as a user whose access had been changed from allowed to denied.
13. At a workstation on the IT network, attempt to access the RADiFlow router administrative interface as a user whose access had been changed from denied to allowed.
14. At a workstation on the OT network, attempt to access the SEL RTU administrative interface as a user whose access had been changed from allowed to denied.
15. At a workstation on the OT network, attempt to access the SEL RTU administrative interface as a user whose access had been changed from denied to allowed.
16. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user whose access had been changed from allowed to denied.
17. At a workstation on the OT network, attempt to access the RTU emulator administrative interface as a user whose access had been changed from denied to allowed.

**Expected results
(pass)**

(CR 4.) Change user access.

(CR 4.a) IT

(CR 4.a.1) Allow-to-deny changes are successfully provisioned.

(CR 4.a.2) Deny-to-allow changes are successfully provisioned.

(CR 4.b) OT

(CR 4.b.1) Allow-to-deny changes are successfully provisioned.

(CR 4.b.2) Deny-to-allow changes are successfully provisioned.

(CR 4.c) PACS

(CR 4.c.1) Allow-to-deny changes are successfully provisioned.

(CR 4.c.2) Deny-to-allow changes are successfully provisioned.

Actual results

The test provided the expected results with the impact of changes to user access (allow to deny, deny to allow) and privilege levels (privileged to non-privileged, non-privileged to privileged) verified.

Overall result

Pass

1526

1527

1528 **APPENDIX A: ACRONYMS**

Acronym	Literal Translation
ABAC	Attribute-Based Access Control
AD	Active Directory
CA	CA Technologies
CIP	Critical Infrastructure Protection
CR	Capability Requirement
CSF	Cybersecurity Framework
.csv	Comma-Separated Value
DMZ	Demilitarized Zone
EACMS	Electronic Access Control and Monitoring System
EAP	Electronic Access Point
EMS	Energy Management System
ESP	Electronic Security Perimeter
HR	Human Resources
ICS	Industrial Control System
ID	Identity
IdAM	Identity and Access Management
IDS	Intrusion Detection System
IMG	Identity Management and Governance
IP	Internet Protocol
ISE	Identity Services Engine
LDAPS	Lightweight Directory Access Protocol Secure
MAG	Mount Airey Group

Acronym	Literal Translation
NAESB	North American Energy Standards Board
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
PIV-I	Personal Identity Verification Interoperable
PKI	Private Key Infrastructure
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guideline
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1529 APPENDIX B: REFERENCES

- [1] Cybersecurity Framework, National Institute of Standards and Technology [Web site], <http://www.nist.gov/cyberframework/> [accessed 2/25/14].
- [2] Designation of Public Trust Positions and Investigative Requirements, 5 C.F.R. § 731.106 (2013). <http://www.gpo.gov/fdsys/granule/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-106/content-detail.html>.

DRAFT

- [3] Office of Management and Budget (OMB), E-Authentication Guidance for Federal Agencies, OMB Memorandum 04-04, December 16, 2003. <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf> [accessed 2/20/14].
- [4] E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.
- [5] “Establishment of NIST Smart Grid Advisory Committee and Solicitation of Nominations for Members,” 75 Federal Register 7 (January 12, 2010), pp. 1595-1596. <https://federalregister.gov/a/2010-344>.
- [6] Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.
- [7] J. Boyar, M. Find, and R. Peralta, “Four Measures of Nonlinearity,” Eighth International Conference on Algorithms and Complexity (CIAC 2013), Barcelona, Spain, May 22-24, 2013, Lecture Notes in Computer Science 7878, pp. 61-72. http://dx.doi.org/10.1007/978-3-642-38233-8_6.
- [8] NISTIR 7298 Revision 2, Glossary of Key Information Security Terms, Richard Kissel, Editor.
- [9] V. C. Hu and K. Scarfone, Guidelines for Access Control System Evaluation Metrics, NISTIR 7874, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 48pp. <http://dx.doi.org/10.6028/NIST.IR.7874>.
- [10] M. Souppaya and K. Scarfone, Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication (SP) 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013, 29pp. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf> [accessed 2/25/14].
- [11] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
- [12] International Organization for Standardization/International Electrotechnical Commission, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, 2011. http://www.iso.org/iso/catalogue_detail?csnumber=56742 [accessed 2/25/14].
- [13] Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5280, May 2008 <http://www.ietf.org/rfc/rfc5280.txt> [accessed

2/20/14].

- [14] Internet Security Threat Report 2013, Volume 18, Symantec Corporation, Mountain View, CA, 2013, 58pp.
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf [accessed 2/25/14].
- [15] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile,
- [16] U.S. Department of Commerce. Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standards (FIPS) Publication 201-2, August 2013, 87pp.
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf> [accessed 2/25/14].

1530

1531 **APPENDIX C: MOUNT AIREY GROUP, INC. PERSONAL PROFILE APPLICATIONS**
1532 **DEMONSTRATION APPLICATION**

1533 The Personal Profile Application (PPA) was developed by Mount Airey Group, Inc. in order to
1534 demonstrate the functionality of the Ozone[®] Suite of products.

1535 Ozone[®] implements atomic authorization for the protection of critical resources by
1536 cryptographically binding credentials to specific authorizations, access rights, and/or explicit
1537 privileges; as well as provides a privacy protecting mechanism that allows these authorizations
1538 to be distributed across the enterprise – as close to the protected resource as necessary –
1539 without concern for tampering, data mining, or compromise; and is meant to protect an
1540 organizations most sensitive or highest risk resources. If an application relies on PKI-based
1541 smart cards and/or biometrics for authentication, then that system should implement the
1542 congruent security for the authorization of users for access to that resource as is provided by
1543 Ozone[®].

1544 In support of the National Cybersecurity Center of Excellence (NCCoE) Electricity Subsector
1545 Identity & Access Management (IDAM) Use Case, the PPA was configured to incorporate digital
1546 certificates that were generated by GlobalSign, Inc., to be compliant with the North American
1547 Energy Standards Board (NAESB) certificate profile. Each certificate was provisioned within
1548 Ozone[®] to have specific authorizations related to the PPA demonstration application.

1549 This application has three main information groups for which actions can be authorized:
1550 Personal Information, Credit Reports, and Criminal History. Based on the authorizations
1551 associated with a credential, results pages are dynamically populated.

1552 In order to bring up the demonstration application, the user must present a digital certificate to
1553 the application. Upon inspection of the authorizations provisioned within Ozone[®] for the

DRAFT

1554 selected certificate, the application dynamically populates the table at the bottom of the first
1555 screen with the results of the authorization queries. If the certificate has been authorized for a
1556 specific action, then the results table will display “true” for that specific action. The information
1557 identifying the certificate that was selected is also displayed above the table.

1558 At that point, the user may either enter a name to search for in the search box on the right, or
1559 simply hit the search button to display the Search Results page of the application. The search
1560 will return a list of names as well as links to additional information about the people listed. The
1561 links listed will vary depending upon the authorizations for which the user was authorized at
1562 logon to the PPA. The available authorizations are:

- 1563 • View Personal Information – View the personal information of the selected person.
- 1564 • Edit Personal Information – Add or edit the personal information of people in the
1565 application.
- 1566 • View Criminal History – View the criminal history of the selected person.
- 1567 • Edit Criminal History – Add or edit the criminal history of people in the application.
- 1568 • View Credit Report – View the credit report of the selected person.
- 1569 • Request a New Credit Report – Request an updated credit report for the selected
1570 person.

1571 **Sample First Page Table:**

1572 Authorizations for: C=US, O=Blue Corp, OU=People, CN=Criminal History Editor

PPA Proof	Authorized
Edit Criminal History	true
Edit Personal Information	false
Request Credit Report	false
View Credit Report	false
View Criminal History	true
View Personal Information	false

1573

1574 **Sample Search Results Page Table:**

1575 **Search Results:**

Name	View CH	Add CH	View CR	Request CR
Hicks, Chick	View	Add	View	Request
McQueen, Lightning	View	Add	View	Request
Sullivan, James P	View	Add	View	Request
Waternoose, Henry J	View	Add	View	Request
Add a new entry... editPI.jsp				

1576

1577 For the NCCoE Electricity Subsector IDAM Use Case, the following authorizations have been
1578 configured for the NAESB certificates:

1579 **Jim McCarthy**

1580 Email Address = james.mccarthy@nist.gov, CN = James McCarthy, OU = GSUS, OU = NCCoE NIST
1581 Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

View Personal
Information
Edit Personal Information
View Criminal History
Edit Criminal History
View Credit Report
Request Credit Report

1582

1583 **Donald Faatz**

1584 Email Address = donald.faatz@nist.gov, CN = Donald Faatz, OU = GSUS, OU = NCCoE NIST
1585 Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

View Criminal History
Edit Criminal History

1586

DRAFT

1587 **Harry Perper**

1588 Email Address = harry.perper@nist.gov, CN = Harry Perper, OU = GSUS, OU = NCCoE NIST
1589 Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

- View Personal Information
- Edit Personal Information
- View Criminal History
- View Credit Report

1590

1591 **John Wiltberger**

1592 Email Address = jwiltberger@mitre.org, CN=Johnathan Wiltberger, OU = GSUS, OU = NCCoE
1593 NIST Energy IdAM test account, O = GMO GlobalSign Inc., L = Portsmouth, ST = NH, C = US

- View Personal Information
- View Criminal History
- View Credit Report
- Request Credit Report

1594

1595

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

The NCCoE wishes to acknowledge the special contributions of Nadya Bartol, Senior Cybersecurity Strategist, Utilities Telecom Council; Jonathan Margulies, formerly with NCCoE and now with Qmulos; and Victoria Pillitteri of NIST. All were instrumental in the initial definition and development of the Identity and Access Management use case. Paul Timmel, formerly detailed to NCCoE from the National Security Agency, helped with these stages and also helped to get the project build started.

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 Kakker	AlertEnterprise
Srinivas Adep	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 Lobo	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 Vital	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 ConSOLEWorks 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 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** ← **YOU ARE HERE**
12 **for building the example solution**

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

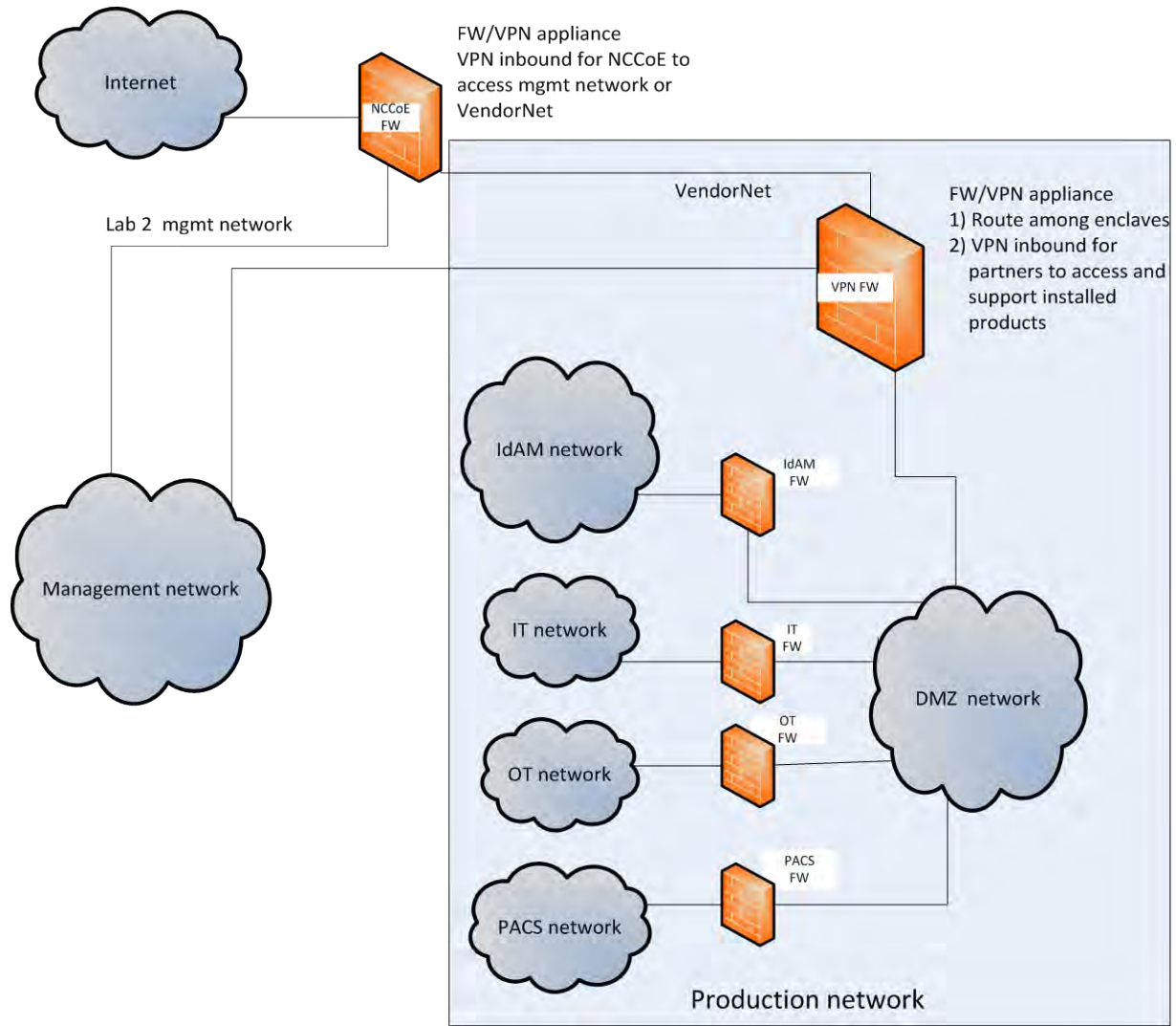
78 2.1 BUILD IMPLEMENTATION OVERVIEW

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)

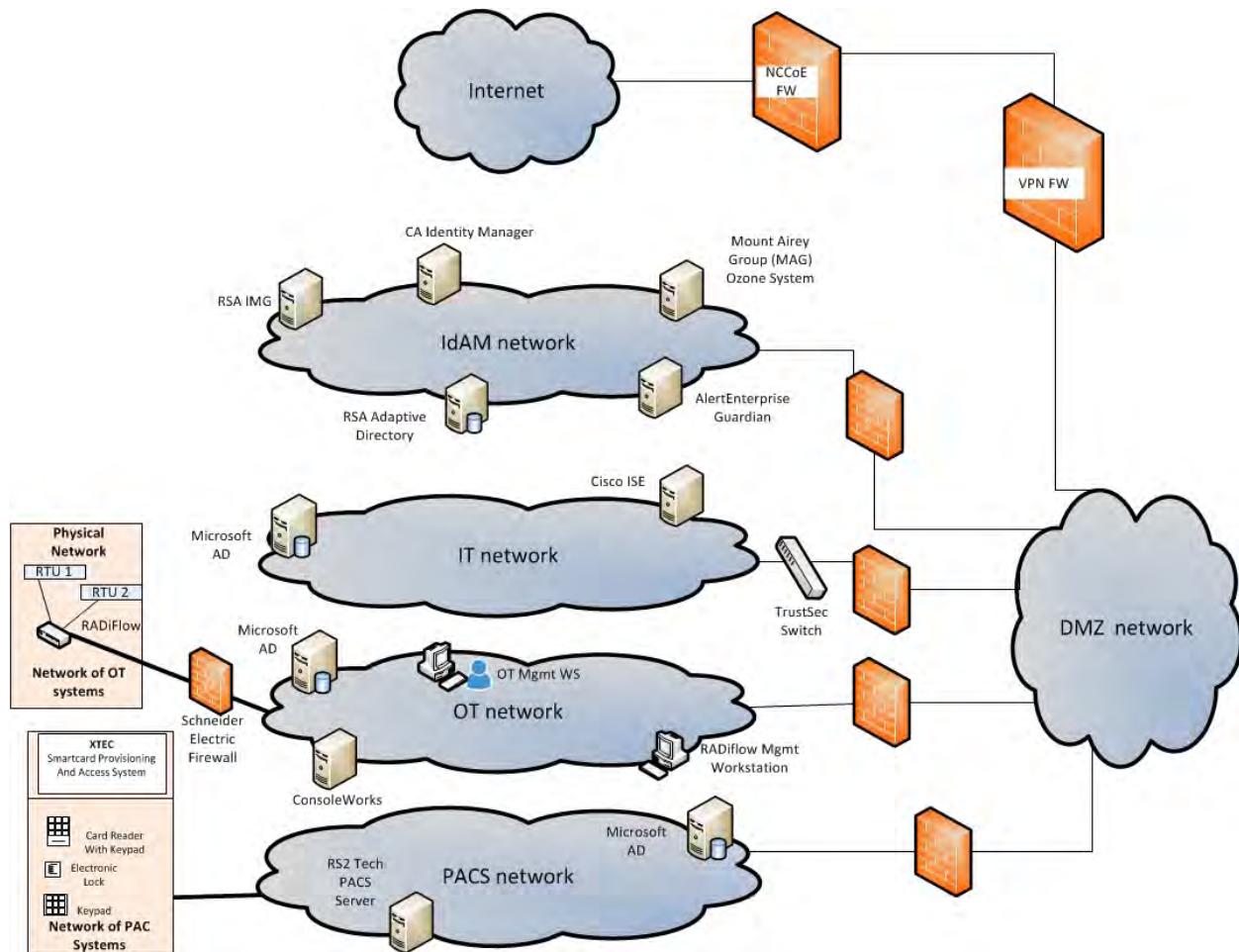
-
- 86 • Identity and Access Management - IdAM
 - 87 • IT - business management system
 - 88 • OT - ICS/SCADA industrial control system and energy management system (EMS)
 - 89 • PACS – physical access control system networks

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



100

101

Figure 2. IdAM build implementation production network

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.

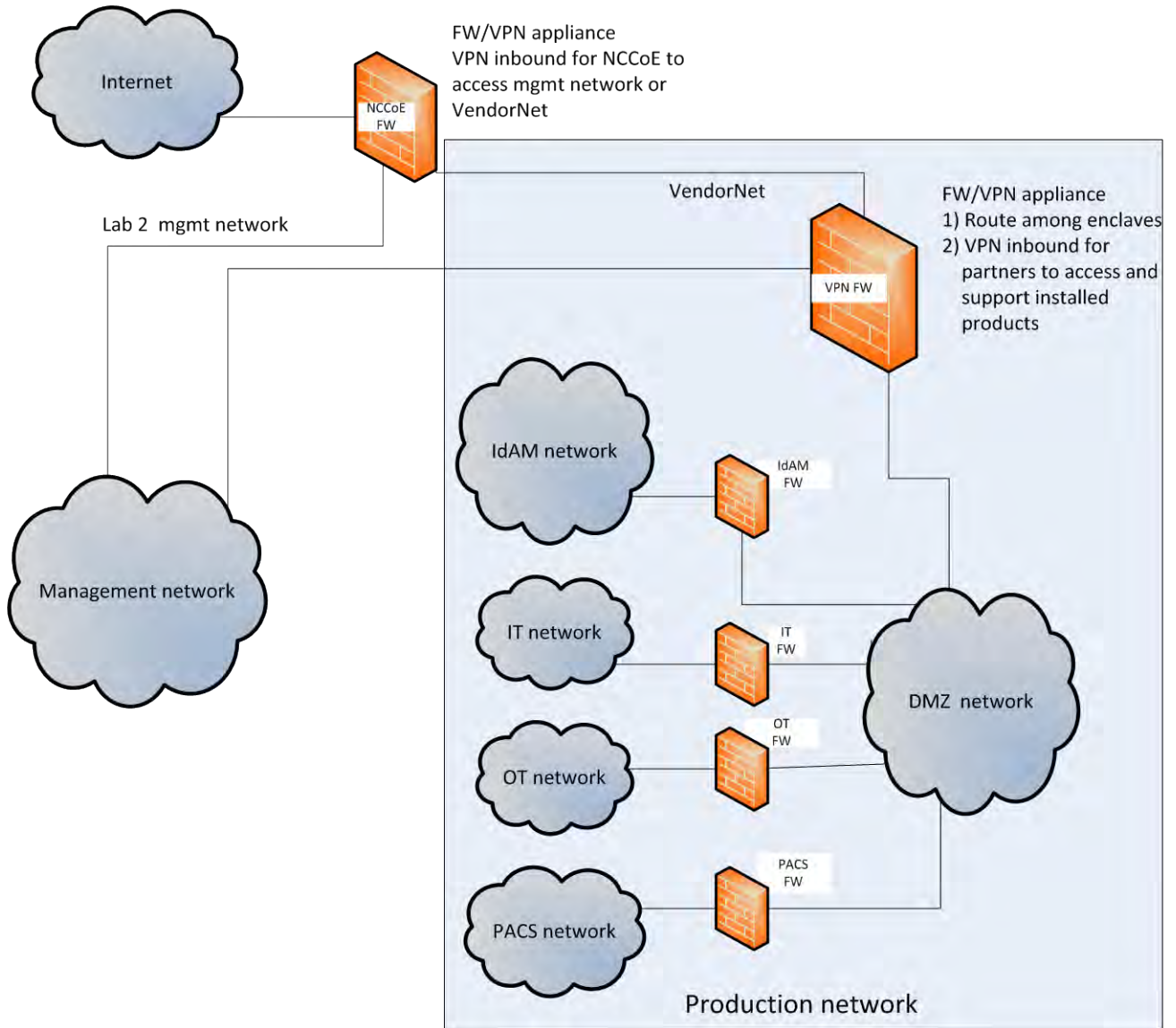
122 The VPN firewall was the access control point for vendors to support the installation and
123 configuration of their components of the architecture. The NCCoE also used this access to
124 facilitate product training. This firewall also blocked unauthorized traffic from the public
125 Internet to 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.

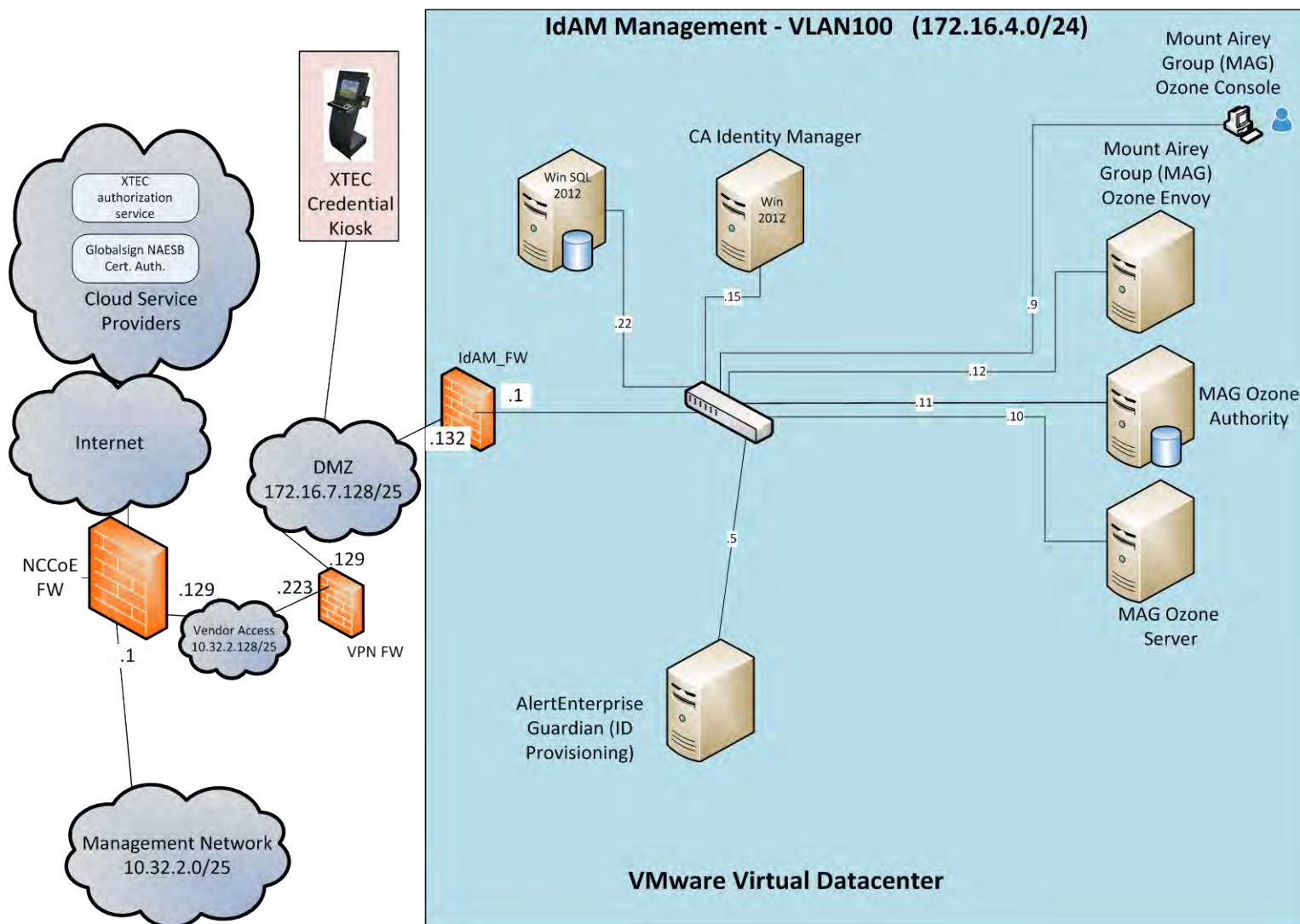
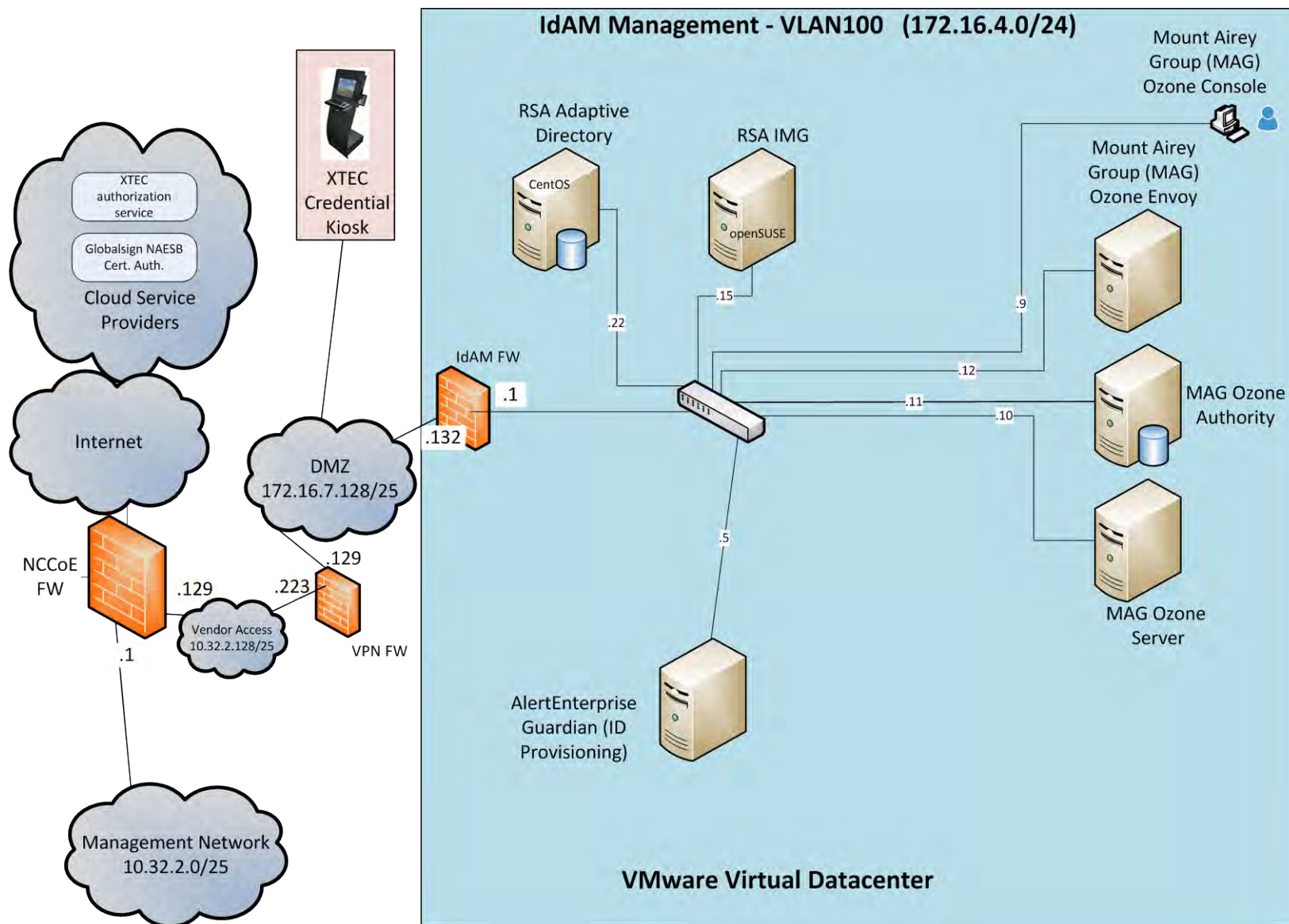


Figure 4. Build #1 IdAM Network

- 144
- 145
- 146 Build #1 uses the CA Identity Manager product for the IdAM system and identity store.



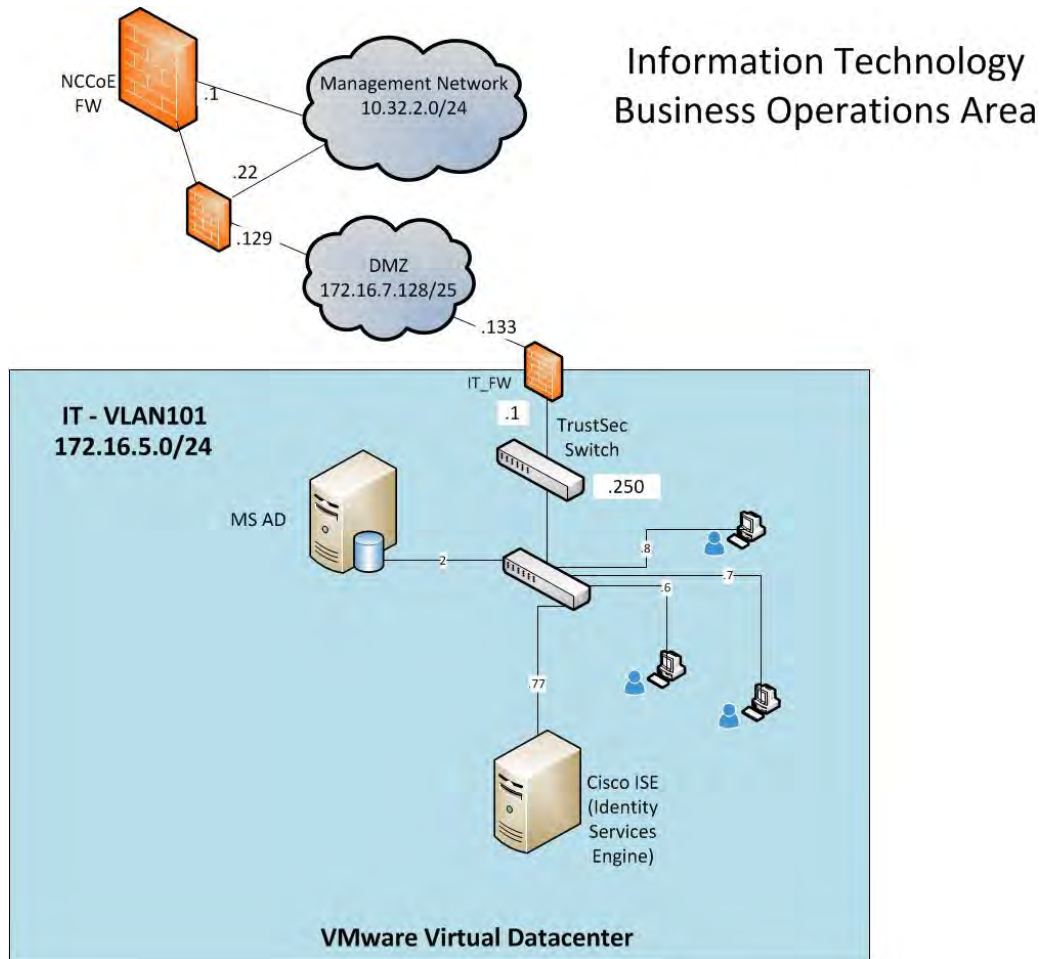
147

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

154

Figure 6. IT Network

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.

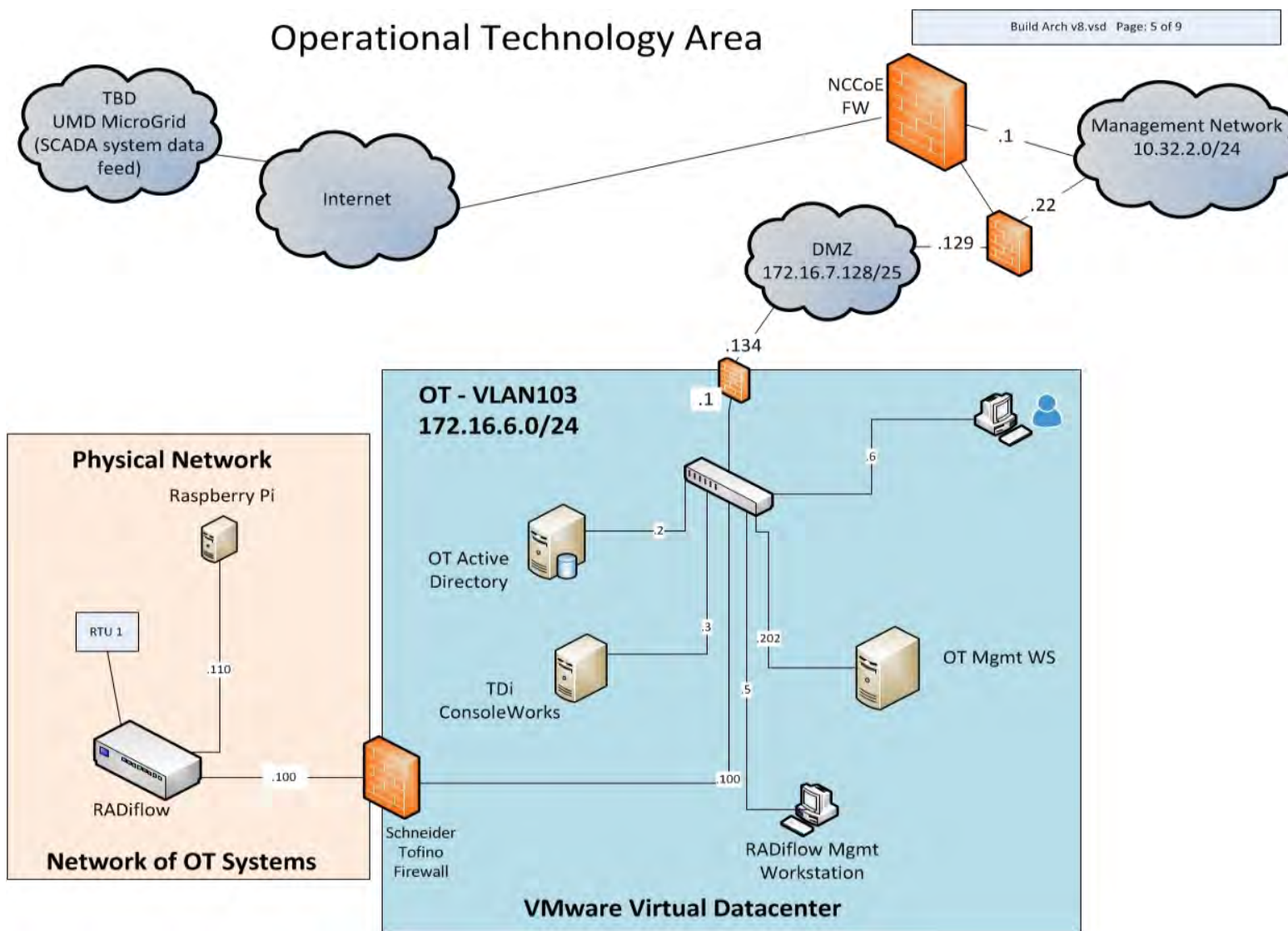
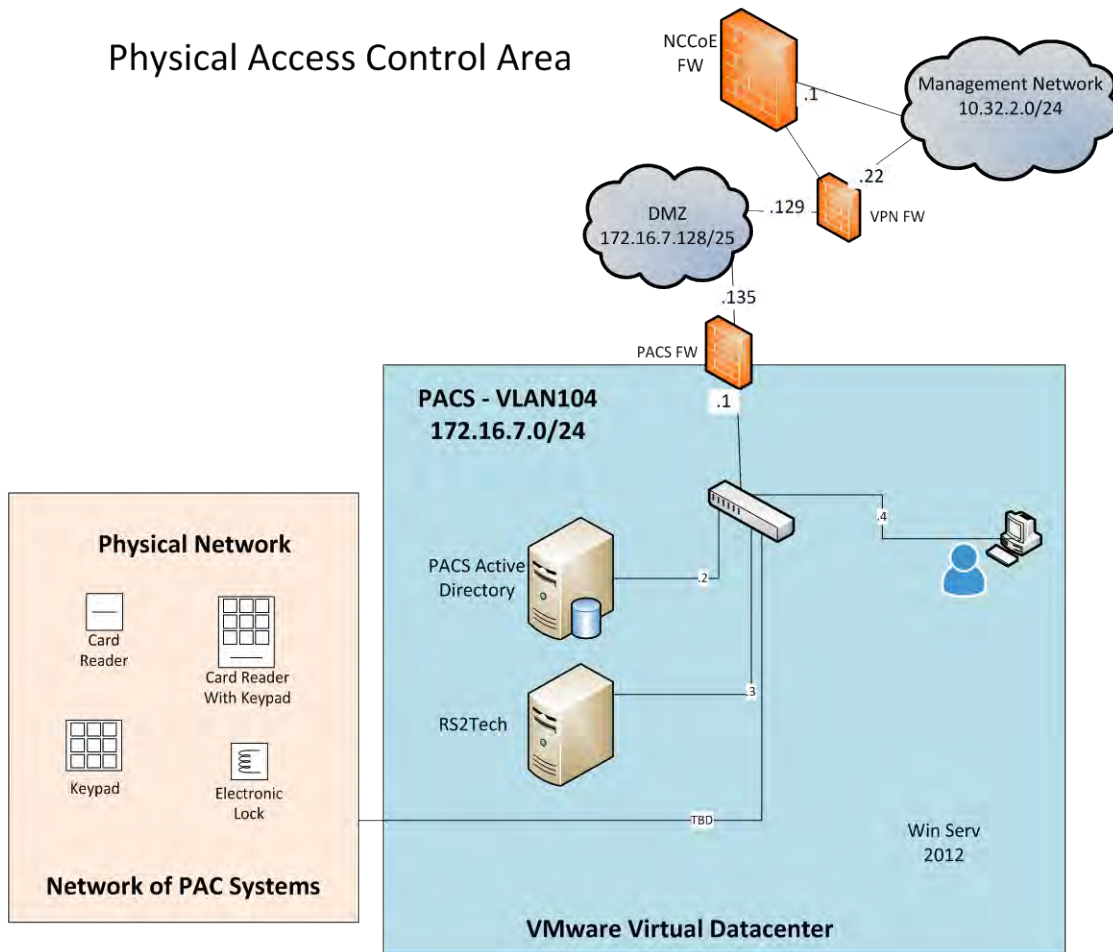


Figure 7 OT Network

161

162

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.

213

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)

214

215

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

216

217

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

218

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 ITEMAIL
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

223

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

224

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:

- 232 • Hostname: ITDC
- 233 • Domain: ES-IDAM-B1.TEST
- 234 • IP: 172.16.5.2

235 Step-by-step instructions:

- 236 1. Launch Server Manager.
- 237 2. From the dashboard, select Option 2, Add Roles and Features.
- 238 3. Select Role-based or Feature-based installation.
- 239 4. From the server pool, select the local server named ITDC.
- 240 5. Select Active Directory Domain Service and DNS Server.
- 241 6. When prompted to add features, select Add Features for each role.
- 242 7. Wait for Server Manager to finishes installing,
- 243 8. Select Post-Deployment Configuration for Active Directory from the Task menu.
- 244 9. After Active Directory Domain Services Configuration Wizard automatically launches.
 - 245 • Select Add a New Forest deployment operation.
 - 246 • Specify ES-IDAM-B1.TEST root domain, then select Next >.
 - 247 • Select Windows Server 2012 R2 for both the Forest Functional Level and the
248 Domain Functional Level,
 - 249 • Under Domain Controller Capabilities:
 - 250 ○ Check both DNS server and Global Catalog.
 - 251 ○ Uncheck read-only domain controller.
 - 252 ○ Specify a password for DSRM and select Next >.
 - 253 • Continue through the Wizard without modifying any options.
 - 254 • Select Install on the next window. After installation, the server automatically
255 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: CA Setup Type:
311 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](#) 337 [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-
354 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     logging {
498         channel default_debug {
499             file "data/named.run";
500             severity dynamic;
501         };
502     };
503
504     zone "." IN {
505         type hint;
506         file "named.ca";
507     };
508
509     zone "idam-es-idam-b1.test" IN {
510         type master;
511         file "idam-es-idam-b1.test";
512         allow-update { none; };
513     };
514
515     zone "4.16.172.in-addr.arpa" IN {
516         type master;
517         file "4.16.172.db";
518         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   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.
- 613 2. Place OVA file in Datastore for vSphere installation.
- 614 3. Ensure that the user domain has a security group (the build used *OTAccess*) for
615 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-](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)
618 [4/installation guide/b_ise_InstallationGuide14/b_ise_InstallationGuide14_chapter_010](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)
619 [0.html](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 ○ 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 ○ 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-](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 [US/JBoss Enterprise Application Platform/6.3/html/Installation Guide/Install JBoss En-](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)
- 896 [terprise Application Platform 6 Microsoft Windows Service.html](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)
- 897 5. Create a Database and associated user with DBA permissions on a supported database
- 898 (e.g., MSSQL 2012).
- 899 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-*
- 928 *6.3\bin\standalone.bat*.
- 929 18. Review the log file to verify that JBoss started without error: *jboss-eap-*
- 930 *6.3\standalone\log\server.log*
- 931 19. If you receive a timeout error such as “Timeout after [300] seconds waiting for service
- 932 container stability...”, increase the timeout by modifying *standalone.bat*, adding the
- 933 following attribute to the startup script:
- 934 **-Djboss.as.management.blocking.timeout=900**

935 6.5 CREATE THE SAMPLE NETEAUTO DIRECTORY

- 936 1. Open a command prompt as the administrator user
- 937 2. cd to “C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity
- 938 Manager\tools\samples\NeteAuto\Organization”
- 939 o You will see several sample files. For this example, we will use *neteauto.ldif*
- 940 3. Execute the following commands:
- ```
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**  
977 above
- 978 5. Click Next, then Finish.

## 979 6.7 CREATE THE NETE AUTO 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  
986 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 anomomous 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\_PXPolicies.xml* file provided with this guide. (Download the file from  
997 [https://nccoe.nist.gov/sites/default/files/nccoe/NIST\\_PXPolicies.zipx](https://nccoe.nist.gov/sites/default/files/nccoe/NIST_PXPolicies.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`
- 1022        `<AlertDBPassword>`
- 1023       • The result displays the Encrypted value with a prefix of {PBES}.
- 1024       • Copy this encrypted password to be used below for EncryptedALERTDBPassword.
- 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       

```
<?xml version="1.0" encoding="UTF-8"?>
```
- 1034       

```
<module xmlns="urn:jboss:module:1.1" name="com.mysql">
```
- 1035       

```
 <resources>
```
- 1036       

```
 <resource-root path="mysql-connector-java-5.1.35-
```
- 1037       

```
 </resource-root>
```

```
1038 bin.jar"/>
1039 </resources>
1040 <dependencies>
1041 <module name="javax.api"/>
1042 </dependencies>
1043 </module>
```

1044 3. From `jboss-eap-6.3\standalone\configuration edit standalone-full.xml`

1045 4. In the “<drivers>” section, add:

```
1046 <driver name="mysql" module="com.mysql">
1047 <driver-class>com.mysql.jdbc.Driver</driver-class>
1048 </driver>
```

1049 5. Just above the “<drivers>” section, add a new data source:

```
1050 <datasource jndi-name="java:/iam/im/jdbc/jdbc/AlertDB"
1051 pool-name="MySQLPool" use-java-context="true">
1052 <connection-url>
1053 jdbc:mysql://ALERTDBServerName:3306/ALERTDBName
1054 </connection-url>
1055 <driver>
1056 mysql
1057 </driver>
1058 <pool>
1059 <max-pool-size>30</max-pool-size>
1060 </pool>
1061 <security>
1062 <security-domain>mysqlldb</security-domain>
1063 </security>
1064 </datasource>
```

1065 6. In the “<security-domains>” section, add the following security domain:

```
1066 <security-domain name="mysqlldb">
1067 <authentication>
1068 <login-module
1069 code="com.netegrity.jboss.datasources.PicketBoxPasswordEncry
1070 ptedLogin" flag="required" module="com.ca.iam.idmutils">
1071 <module-option name="userName"
1072 value="ALERTDBUserName"/>
1073 <module-option name="password" value="
1074 EncryptedALERTDBPassword "/>
1075 <module-option name="managedConnectionFactoryName"
1076 value="jboss.jca:name=iam/im/jdbc/jdbc/WPDS,service=LocalTx
1077 CM"/>
1078 </login-module>
1079 </authentication>
1080 </security-domain>
```

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

## 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 value to 1. Set Unchecked Value to 0.
- 1117
- 1118
- City: Change Name to `Pacs Work Access`. Change Style to Checkbox. Set Check value to 1. Set Unchecked Value to 0.
- 1119
- 1120
- Address: Change Name to `Pacs Home Access`. Change Style to Checkbox. Set Check value to 1. Set Unchecked Value to 0.
- 1121
- 1122
- Employee Number: Change Name to `Card Number`. Change Permission to Read/Write Required.
- 1123
- For any non-required fields that you don't want to display: Change Style to Hidden.
- 1124
- 1125
- 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 about losing changes.
- 1130
- 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 about losing changes.
- 1134
- 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 connect to and copy them to the Identity Manager server.
- 1139
2. Double-click on the certificate, and click Install Certificate.
- 1140
3. Select Local Machine, then Place all Certificates in the following store. Click Browse.
- 1141
4. Select Trusted Root Certification Authorities. Click OK twice.
- 1142

### 1143 6.12 ACQUIRE ACTIVITY DIRECTORY ENDPOINT

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



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

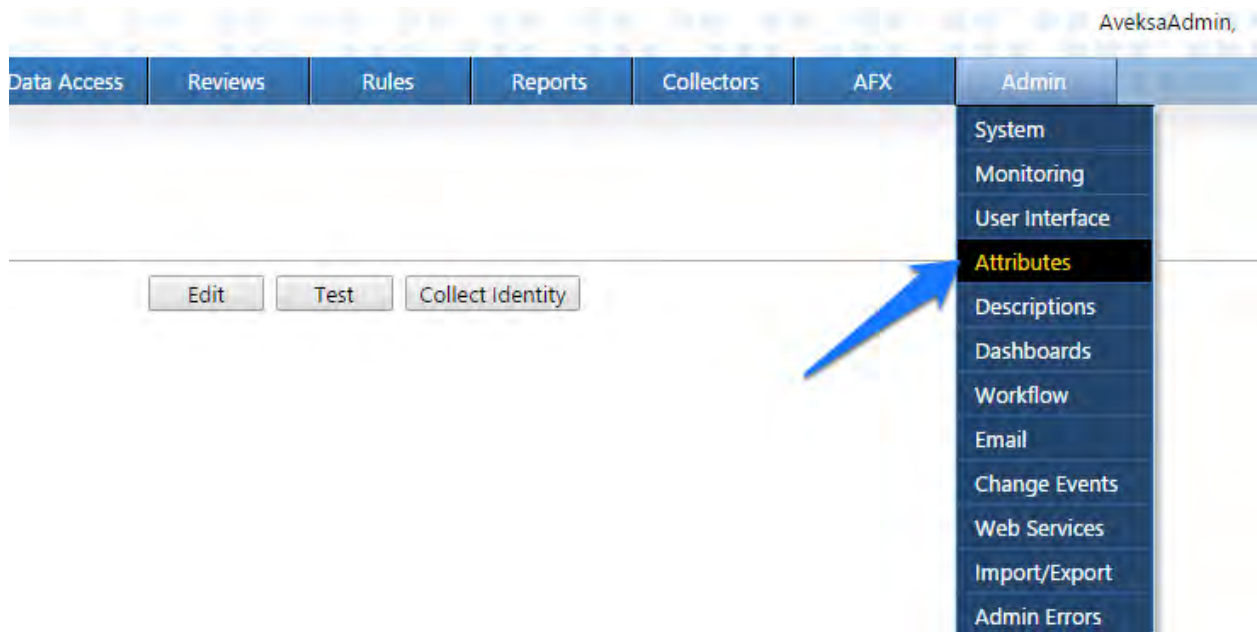
1269 Username: AveksaAdmin (case sensitive)

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':



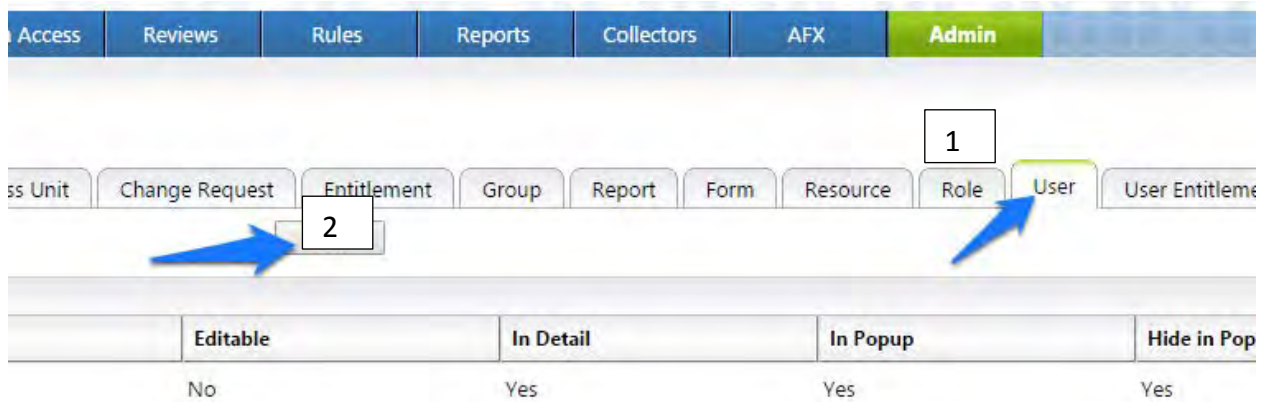
1274

1275

Figure 9. IMG Attributes Window

1276

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



1277

1278

Figure 10. IMG Edit User

1279

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

Attribute Configuration - User										
Once an attribute is configured, it can not be deleted. The option selected for <i>Data Source</i> is a one-time change and cannot be edited later. The <i>Editable</i> option for Collected attributes will be available only for attributes that were mapped in an identity collector.										
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"/>	<input checked="" type="checkbox"/>
Job Family	String	256	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
Job Status	String	256	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
Location	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Other	User		Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
PACS Home Access	String	256	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
Previous Supervisor	User		Managed	<input checked="" type="checkbox"/>	<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"/>	<input checked="" type="checkbox"/>
Supervisor	String	256	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
Title	String	256	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
Unique Id	String	2000	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
User Risk Level	String	256	Managed	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
Login ID	String	256	Collected	<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>
OU	String	256	Collected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Attribute   Add Separator

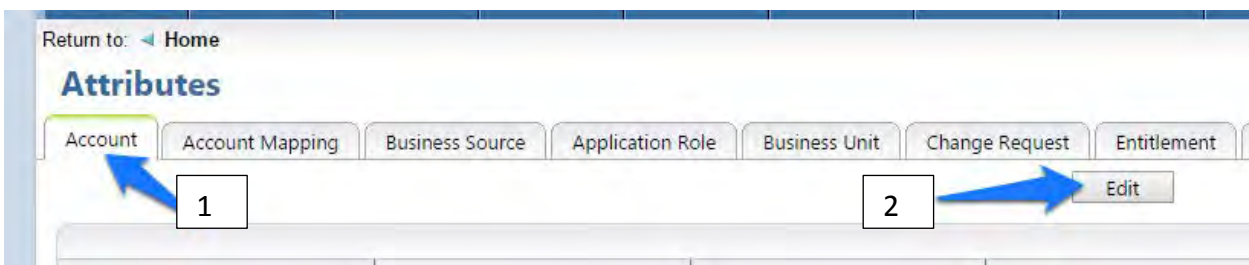
1283

1284

Figure 13. IMG Attributes Examples

1285 3. Click on OK.

1286 4. Click on 'Account' then 'Edit' as shown in Figure 14.



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**

Once an attribute is configured, it can not be deleted. The option selected for *Data Source* is a one-time change and cannot be edited later. The *Editable* option for Collected attributes will be available only for attributes that were mapped in an identity collector.

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	CA11	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

Figure 15. IMG Attribute Example

1290

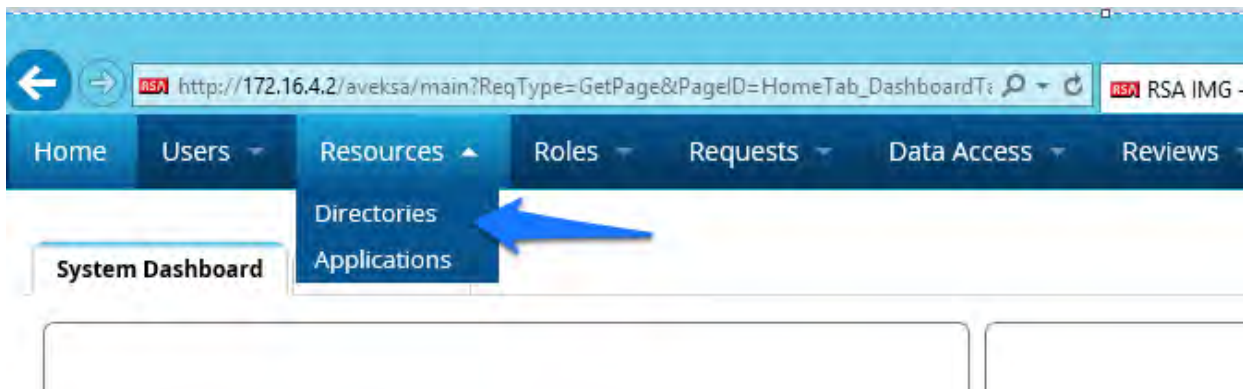
1291

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](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

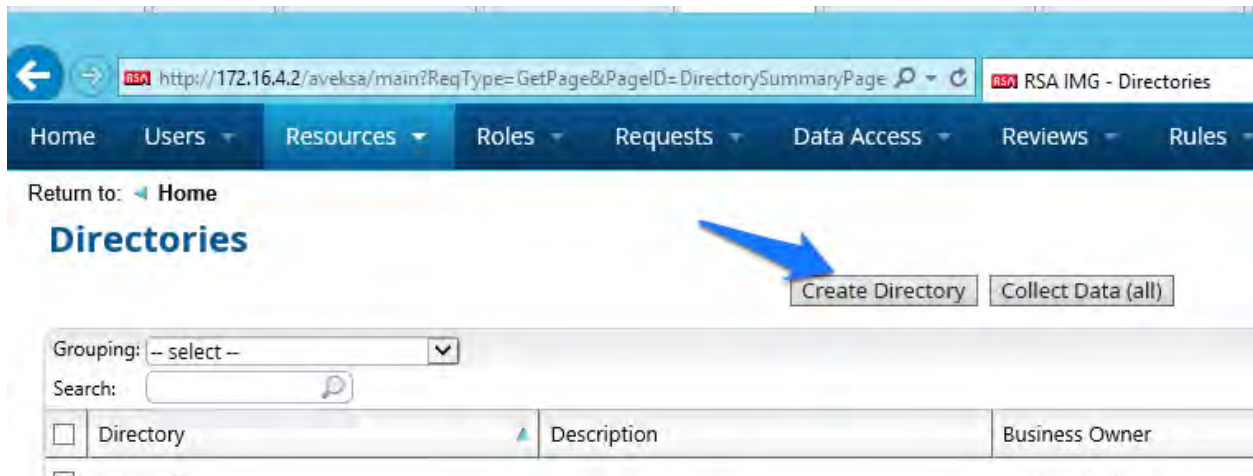


1301

Figure 16. IMG Resources Directories

1302

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



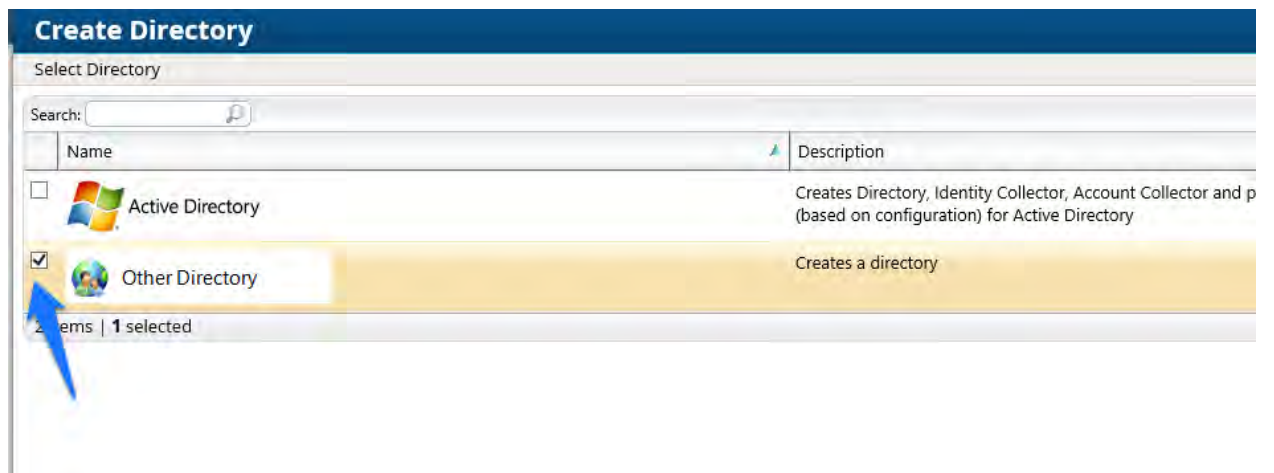
1303

1304

Figure 17. IMG Create Directory

1305

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



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:

1318

1319

1320

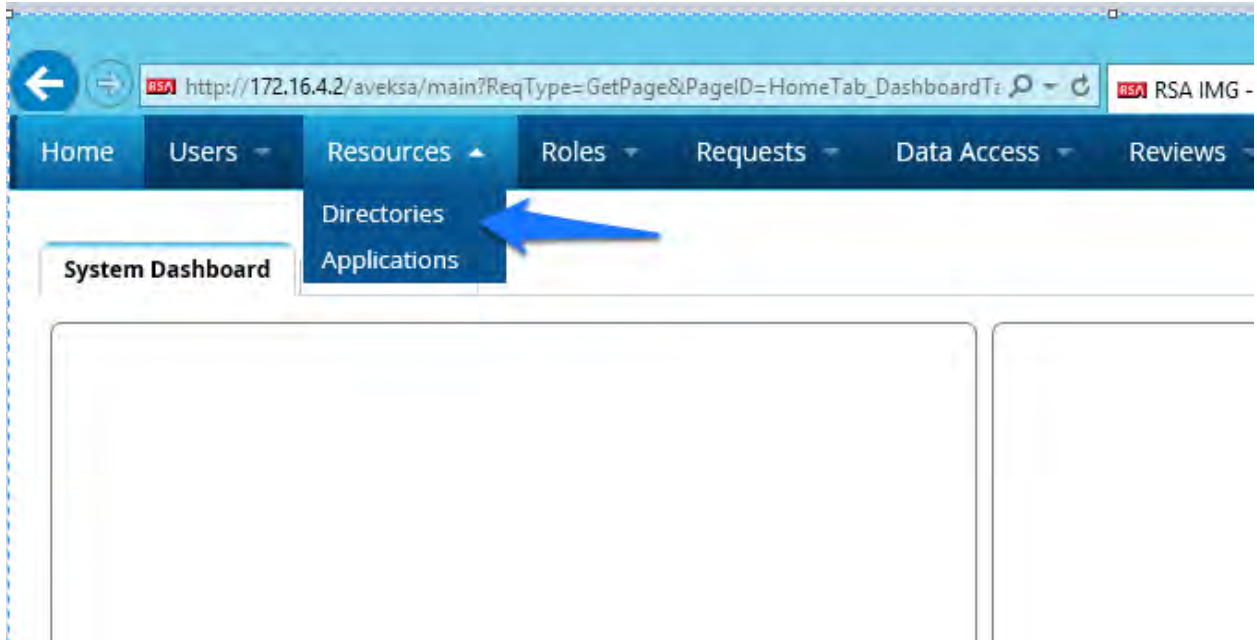
1321

Figure 20. IMG Create Directory

## 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.

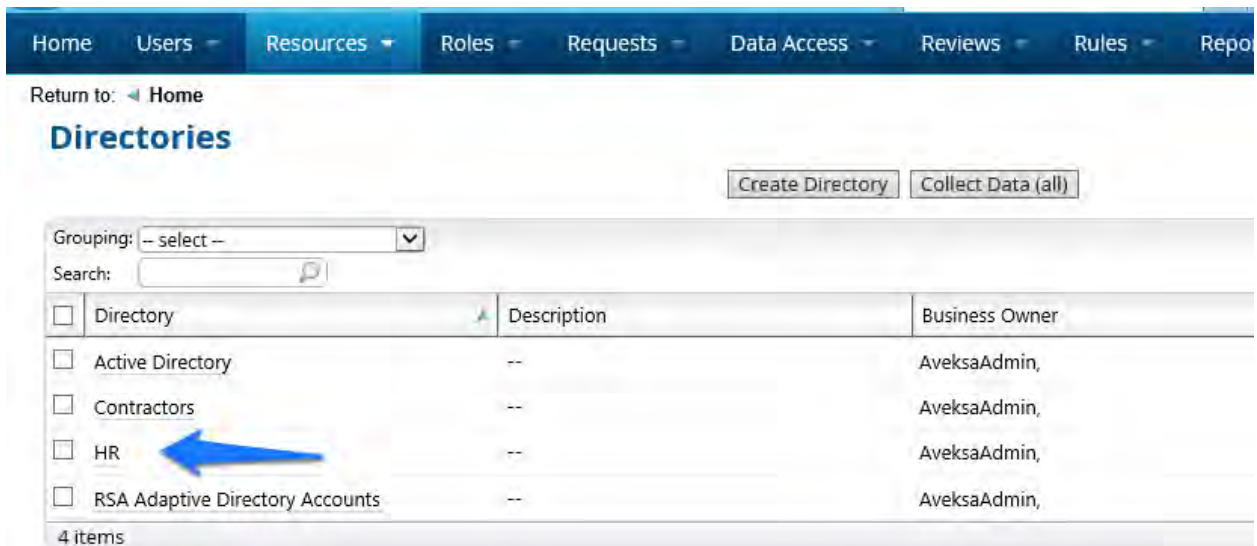


1325

1326

Figure 21. IMG Directories

- 1327 2. Click on your new HR directory you just created as shown in Figure 22.



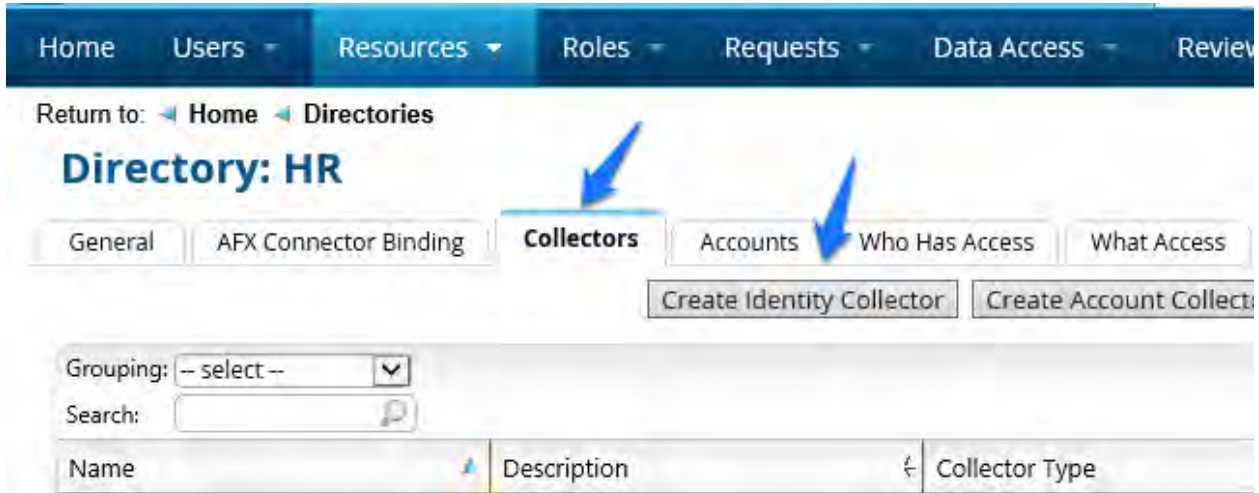
1328

1329

Figure 22. IMG Directories

1330

- 1331 3. Click on 'Collectors' then click 'Create Identity Collector' as shown in Figure 23  
1332 IMG Create Identity Collector.



1333

1334

Figure 23. IMG Create Identity Collector

- 1335 4. Enter details as below as shown in Figure 24.



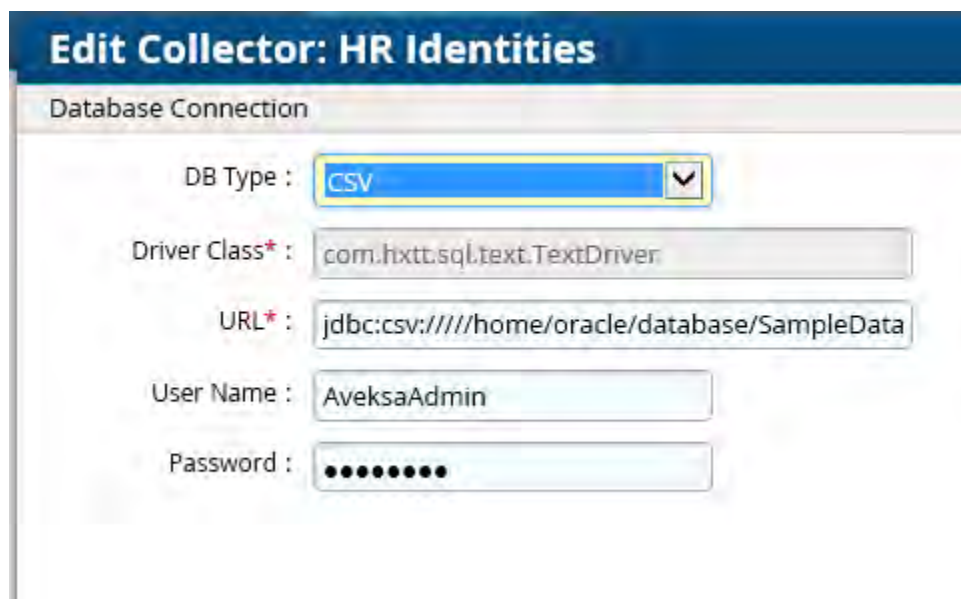
1336

1337

Figure 24. IMG HR Identities

1338

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



The screenshot shows a web form titled "Edit Collector: HR Identities" with a sub-section "Database Connection". The form contains the following fields:

- DB Type: A dropdown menu with "CSV" selected.
- Driver Class\*: A text input field containing "com.hxtt.sql.text.TextDriver".
- URL\*: A text input field containing "jdbc:csv:////home/oracle/database/SampleData".
- User Name: A text input field containing "AvekasaAdmin".
- Password: A password input field with 10 dots.

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 page.

1342

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=/home/oracle`

1345

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

1347

7. Click 'Next'.

1348

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



The screenshot shows a web form titled "Edit Collector: HR Identities" with a sub-section "Select types of identity data to collect". The form contains the following field:

- Users: A checkbox that 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 1<sup>st</sup> 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*	<input type="text" value="sAMAccountName"/>
Business Unit Id :	<input type="text" value="bu"/> 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"/>
Department :	<input type="text" value="department"/>
Email Address :	<input type="text" value="email"/>
Expiration Date :	<input type="text"/>
Expiration Value :	<input type="text"/>
First Name :	<input type="text" value="fname"/>
Full Name :	<input type="text" value="fullname"/>
Is Manager :	<input type="text" value="is_manager"/>
Is Terminated :	<input type="text" value="is_terminated"/>
Job Code :	<input type="text" value="jobcode"/>

Figure 27. IMG HR Identities

1365

1366

1367



Job Family :

Job Level :

Job Status :

Last Name :

Location :

Login ID :

OU :

Other :  value is User

PACS All Doors :

PACS Home AAccess :

PACS Work Access :

Self Reviewer :  value is User

Supervisor :

Termination Date :

Title :

Unique Id :

1368

1369

*Figure 28. IMG HR Identities (cont.)*

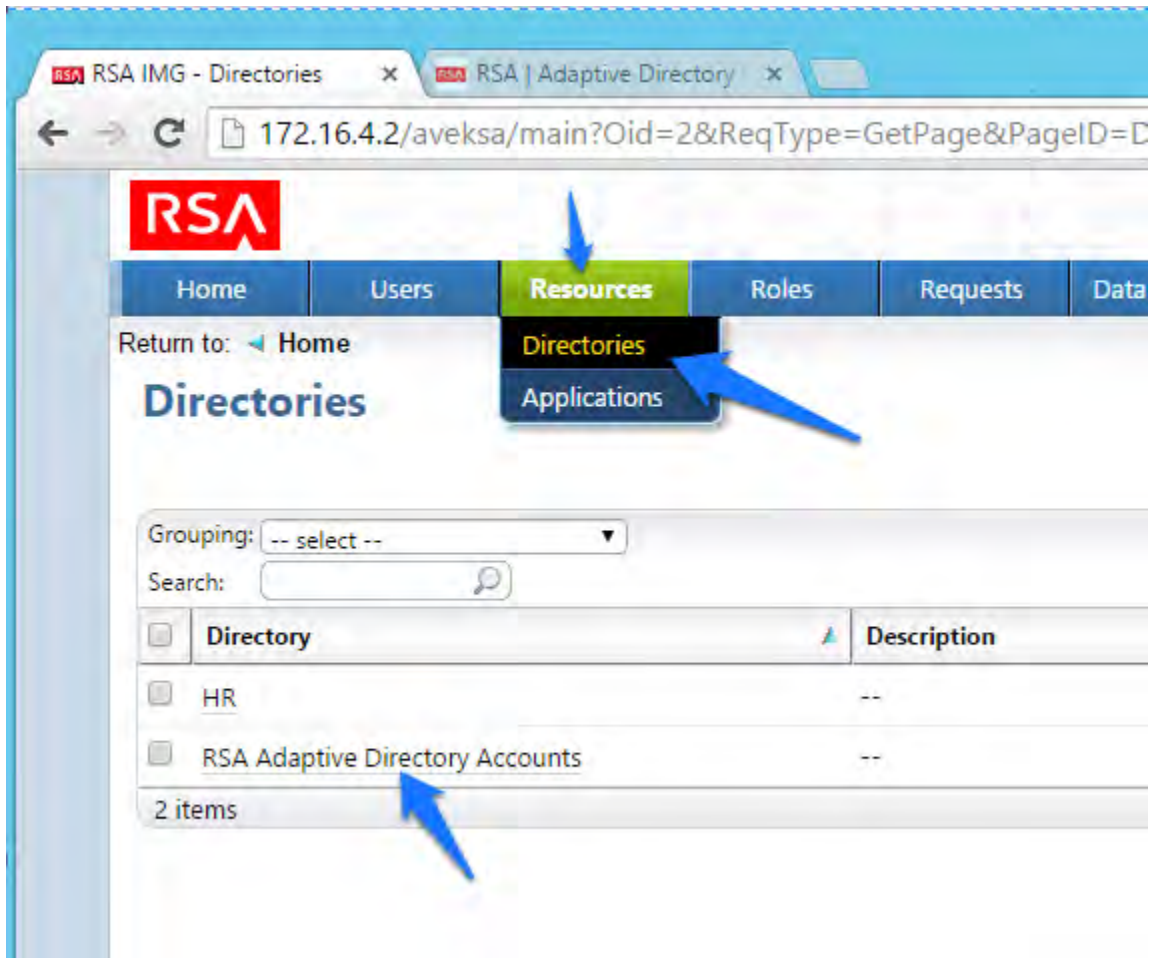
1370 9. Click 'Finish'

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

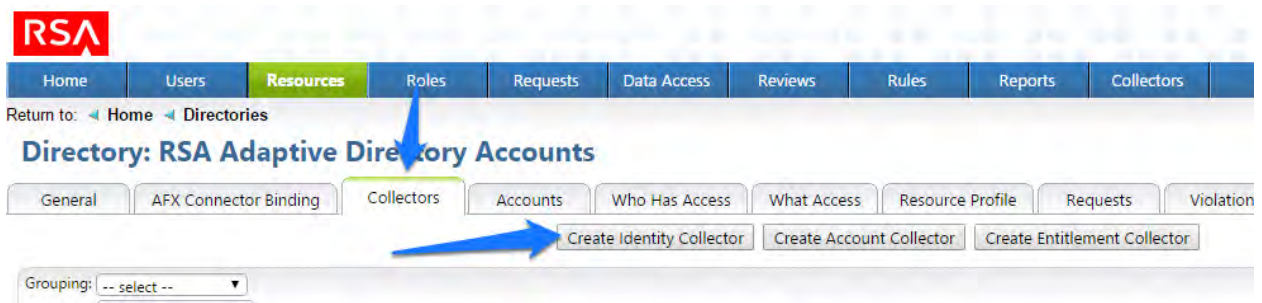
1377

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 : AvekxaAgent

Directory : RSA Adaptive Directory Acco

Status : Active

Schedule

Scheduled :  Yes  No

1386

1387

Figure 31. IMG AD Identity Collector

1388

The screenshot shows a web-based configuration interface for an identity collector. The title bar reads "Edit Collector: RSA Adaptive Directory Identity Collector". Below the title bar is a section labeled "Connection". The form contains the following fields and options:

- Host\*: 172.16.4.3
- Port\*: 2389
- Bind DN\*: cn=Directory Manager
- Bind Password\*: [masked with dots]
- Use SSL:
- Disable Paging:

1389  
1390  
1391

Figure 32. IMG AD Identity Collector

The screenshot shows the same web-based configuration interface, but now the "Select types of identity data to collect" section is visible. It contains a single option:

- Users

1392  
1393  
1394

Figure 33. IMG AD Identity Collector

### Edit Collector: RSA Adaptive Directory Identity Collectr

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="{&amp;(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"/>

1395

1396

1397

Figure 34. IMG AD Identity Collector

Is Terminated :

Job Code :

Job Family :

Job Level :

Job Status :

Last Name :

Location :

Login ID :

OU :

Other :  value is User

PACS All Doors :

PACS Home ACcess :

PACS Work Access :

Self Reviewer :  value is User

Supervisor :

Termination Date :

Title :

Unique Id :

1398

1399 *Figure 35. IMG AD Identity Collector*

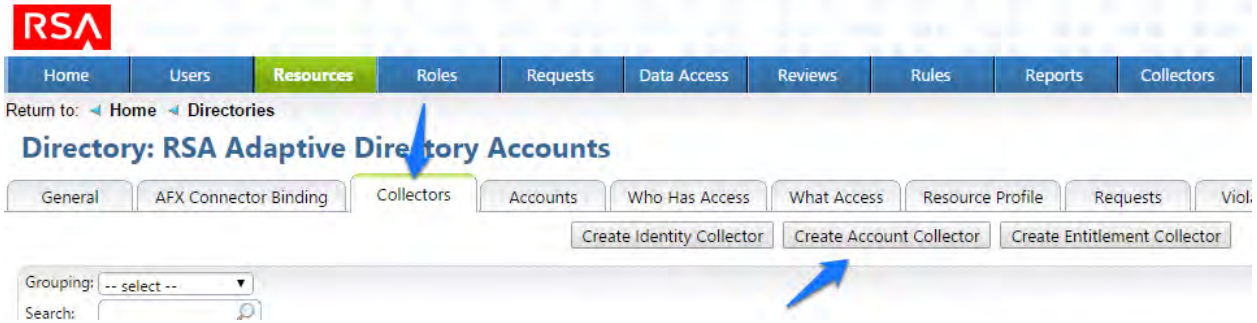
1400

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.



1406

1407

Figure 36. IMG AD Create Account Collector

1408

1409

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



1410

1411

Figure 37. IMG Edit Collector

The screenshot shows a web-based configuration interface titled "Edit Collector: RSA AD Directory Accounts". Under the "Connection" section, there are several input fields and checkboxes:

- Host\*: 172.16.4.3
- Port\*: 2389
- Bind DN\*: cn=Directory Manager
- Bind Password\*: [masked with dots]
- Use SSL:
- Disable Paging:

1412

1413

Figure 38. IMG Edit Collector

1414

The screenshot shows the same web-based configuration interface, but now under the "Select types of account data to collect" section. It includes a list of checkboxes and a "Case Sensitivity" section:

- 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 Scope\* :

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

1425

Figure 42. IMG Edit Collector

### 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="Add More..."/>	

1426

1427

Figure 43. IMG Edit Collector

The screenshot shows a web interface titled "Edit Collector: RSA AD Directory Accounts". Below the title is a sub-header "Edit Member Account Resolution Rules". There are two columns: "Target Collector" and "Account Attribute". Under "Target Collector", a dropdown menu is set to "RSA AD Directory Accounts". Under "Account Attribute", a dropdown menu is set to "DN". To the right of the "Account Attribute" dropdown is a small "x" icon. Below these fields is an "Add More..." button.

1428

1429

Figure 44. IMG Edit Collector

The screenshot shows a web interface titled "Edit Collector: RSA AD Directory Accounts". Below the title is a sub-header "Edit Sub-group Resolution Rules". There are two columns: "Target Collector" and "Group Attribute". Under "Target Collector", a dropdown menu is set to "RSA AD Directory Accounts". Under "Group Attribute", a dropdown menu is set to "Name". To the right of the "Group Attribute" dropdown is a small "x" icon. Below these fields is an "Add More..." button.

1430

1431

Figure 45. IMG Edit Collector

The screenshot shows a web interface titled "Edit Collector: RSA AD Directory Accounts". Below the title is a sub-header "Edit Group Owner Resolution Rules". There are two columns: "Target Collector" and "User Attribute". Under "Target Collector", a dropdown menu is set to "Users". Under "User Attribute", a dropdown menu is set to "User Id". To the right of the "User Attribute" dropdown is a small "x" icon. Below these fields is an "Add More..." button.

1432

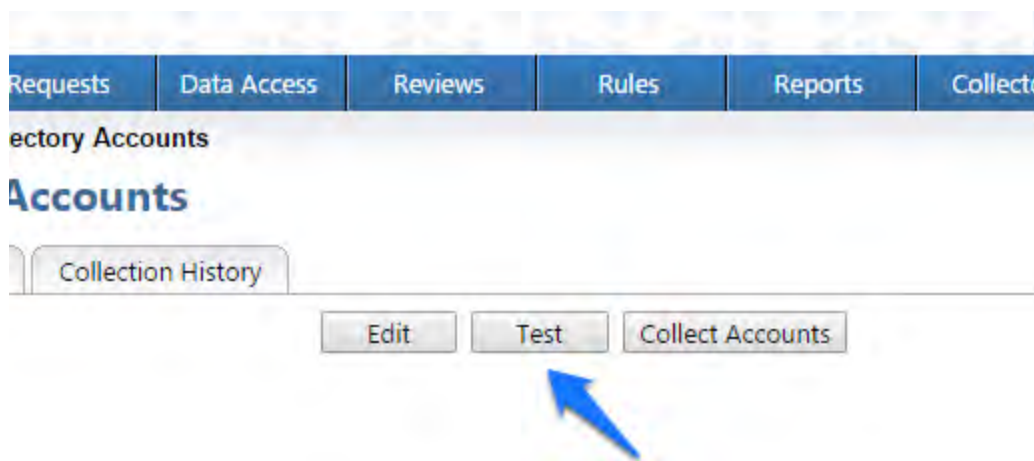
1433

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.

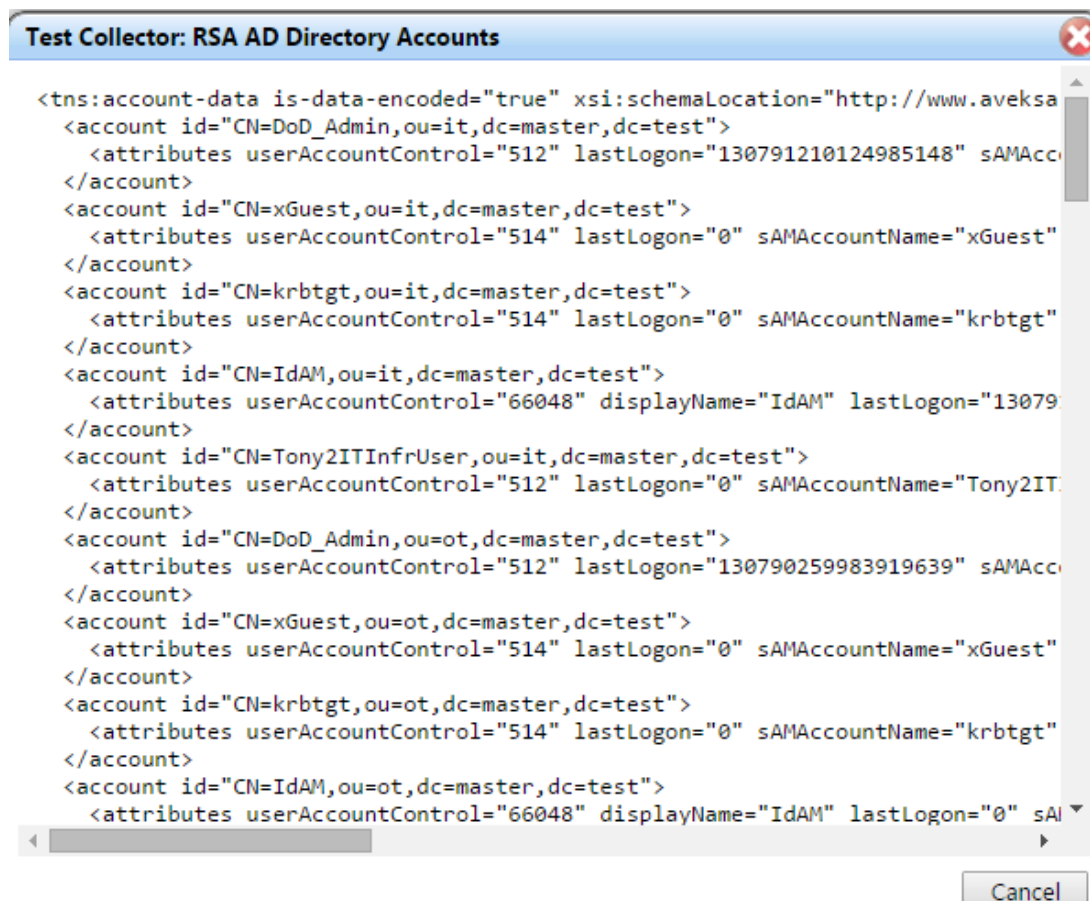


1439

1440

Figure 47. IMG Account Test

1441 A successful test will look something like Figure 48.



1442

1443

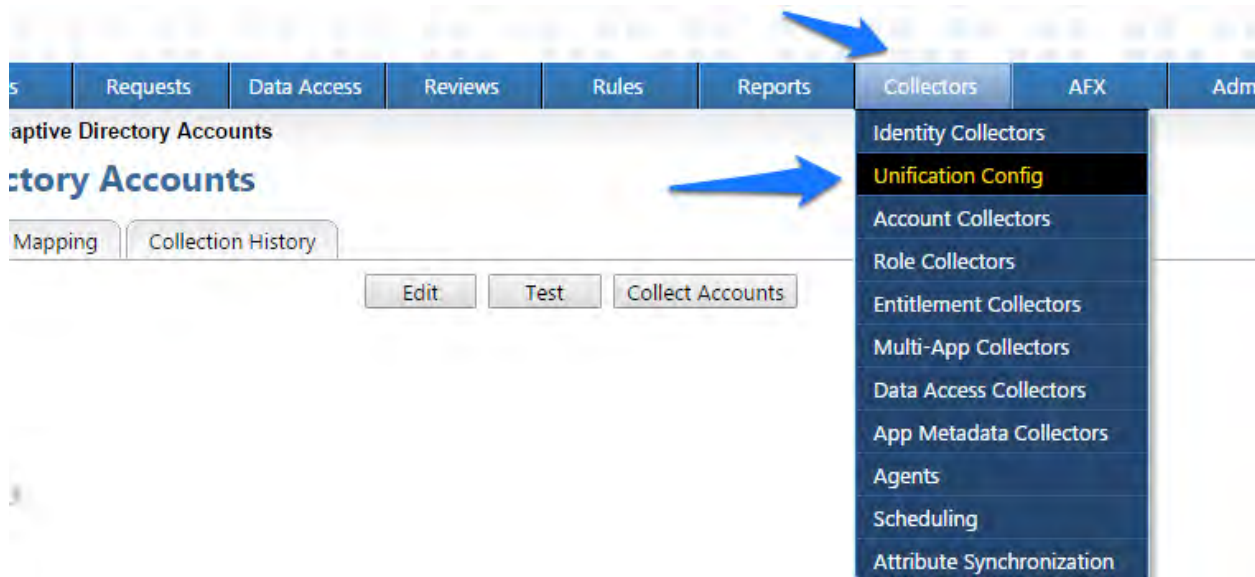
Figure 48. IMG Successful Test Example

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.

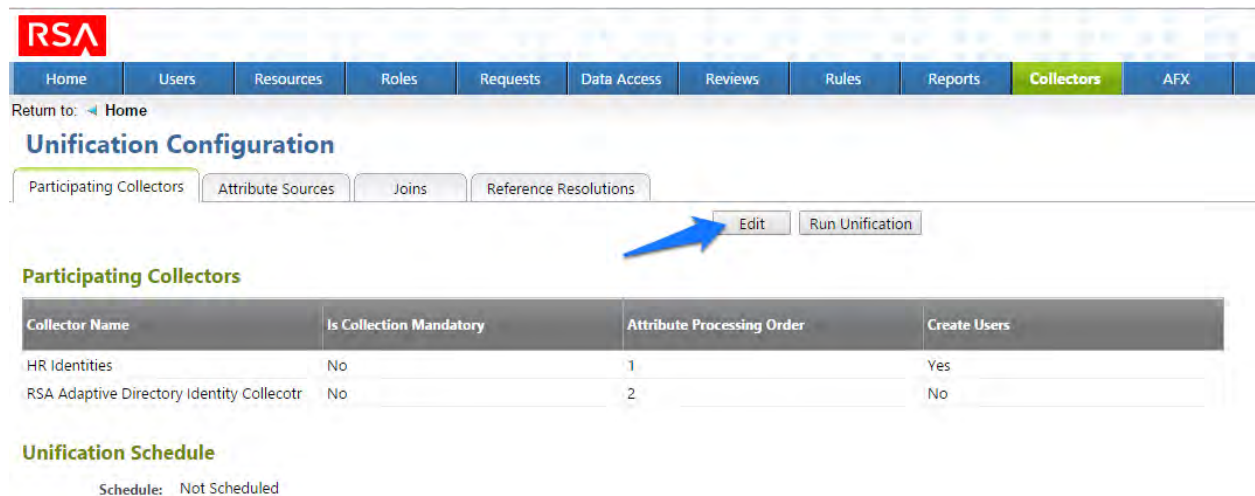


1450

1451

Figure 49. IMG Unification Configuration

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

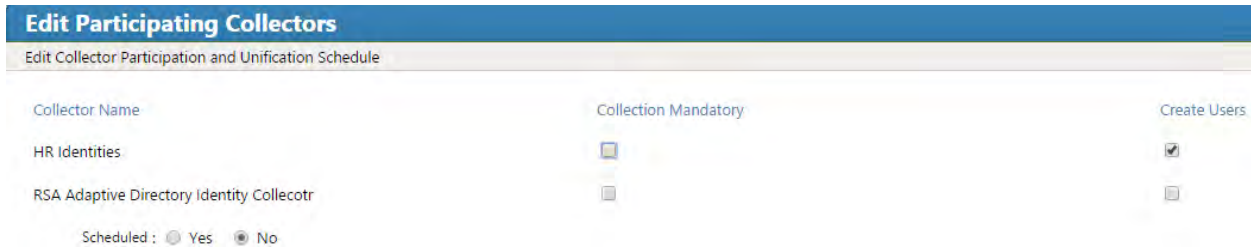


1453

1454

Figure 50. IMG Participating Collectors

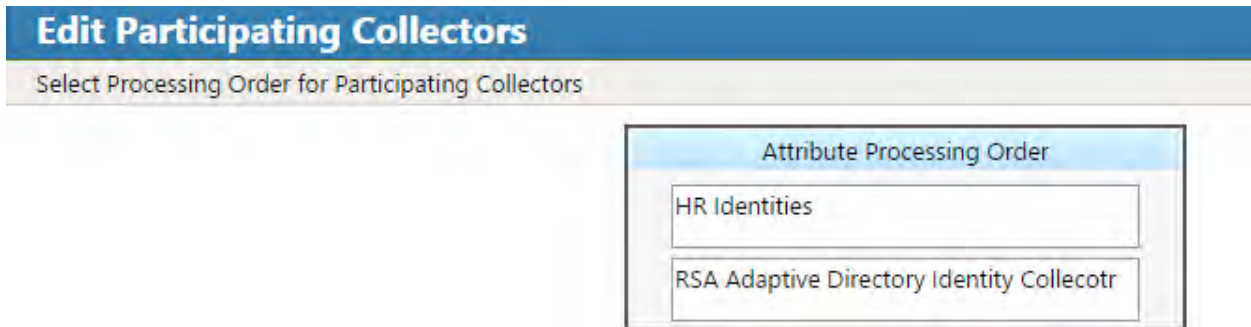
1455 3. Configure as shown in Figure 51 and Figure 52. Click Next on each screen.



1456

1457

Figure 51. IMG Edit Participating Collectors



1458

1459

Figure 52. IMG Edit Participating Collectors

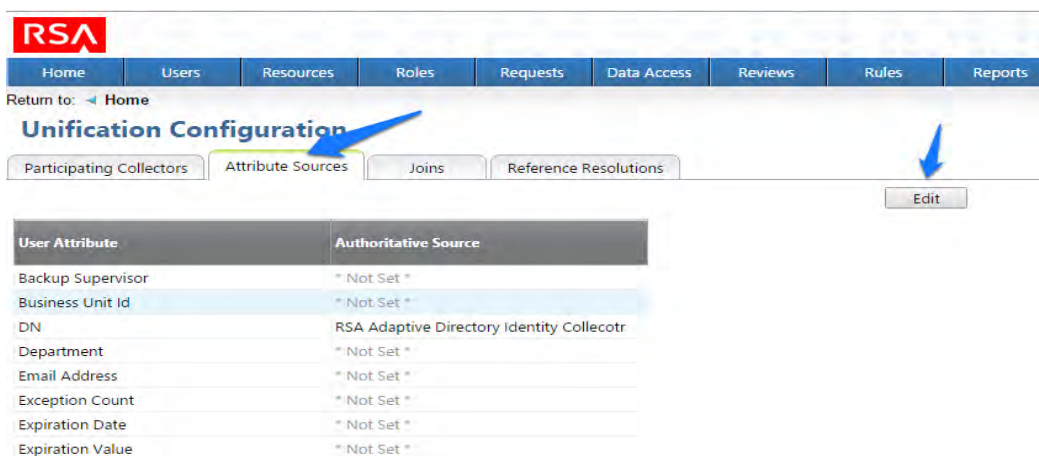
1460 In the above example, we have HR Identities at the top. This indicates that HR Identities is  
 1461 authoritative source – if there are any discrepancies between the data between the two, then  
 1462 the one at the top will win by default, but this can be overridden, which we will see later.

1463 4. Click Finish.

1464 7.3.7 [Edit Unification Configuration Attribute Source](#)

1465 The next step is to change the default behavior of the authoritative source for the necessary  
 1466 attributes.

1467 1. Choose the Attribute Sources tab. Click on Edit as shown in Figure 53.



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 'Not Set'. These attributes will use the default behavior:

1471

### Edit User Attribute Mapping

User Attribute	Authoritative Source
Backup Supervisor :	(not collected)
Business Unit Id :	* Not Set *
DN :	RSA Adaptive Directory Identity Collec
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 : \* Not Set \*

Location : \* Not Set \*

Login ID : \* Not Set \*

OU : \* Not Set \*

Other : \* Not Set \*

PACS All Doors : RSA Adaptive Directory Identity Colle

PACS Home ACcess : RSA Adaptive Directory Identity Colle

PACS Work Access : RSA Adaptive Directory Identity Colle

Previous Supervisor : (not collected)

Self Reviewer : \* Not Set \*

Termination Date : (not collected)

Title : \* Not Set \*

Transfer Date : (not collected)

Unique Id : \* Not Set \*

User Risk Level : (not collected)

Violation Count : (not collected)

1474

1475

Figure 55. IMG Edit User Attribute Mapping

1476 3. Click on OK.

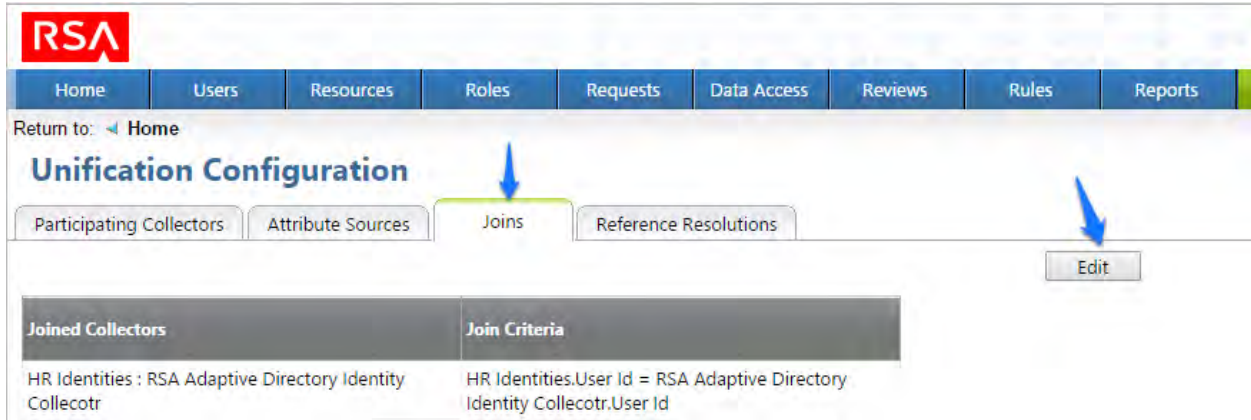
1477 7.3.8 [Edit Unification Configuration Attribute Source](#)

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





1482

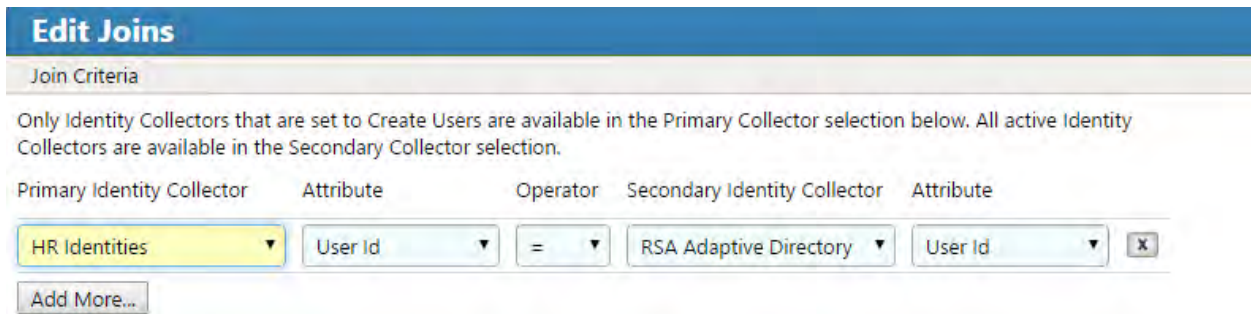
1483

Figure 56. IMG Unification Configuration Joins

1484

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

1485



1486

1487

Figure 57. IMG Edit Joins

1488

3. Click 'Finish'.

1489

### 7.3.9 Start Data Collection

1490

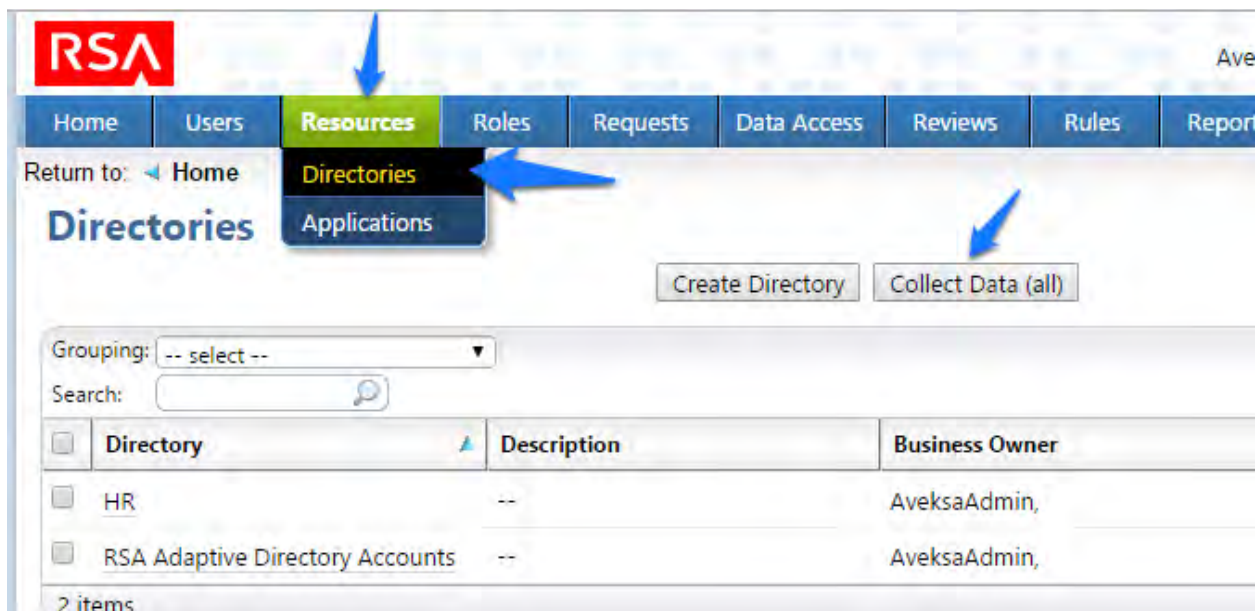
The next step is to start collecting identity data.

1491

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

1492

1493



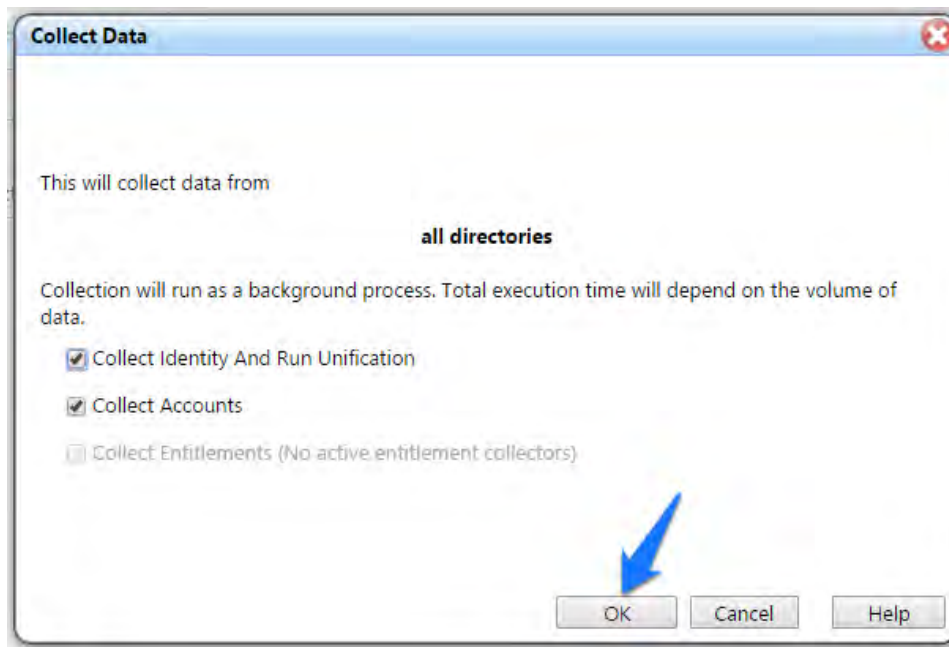
1494

1495

Figure 58. IMG Start Data Collection

1496

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



1497

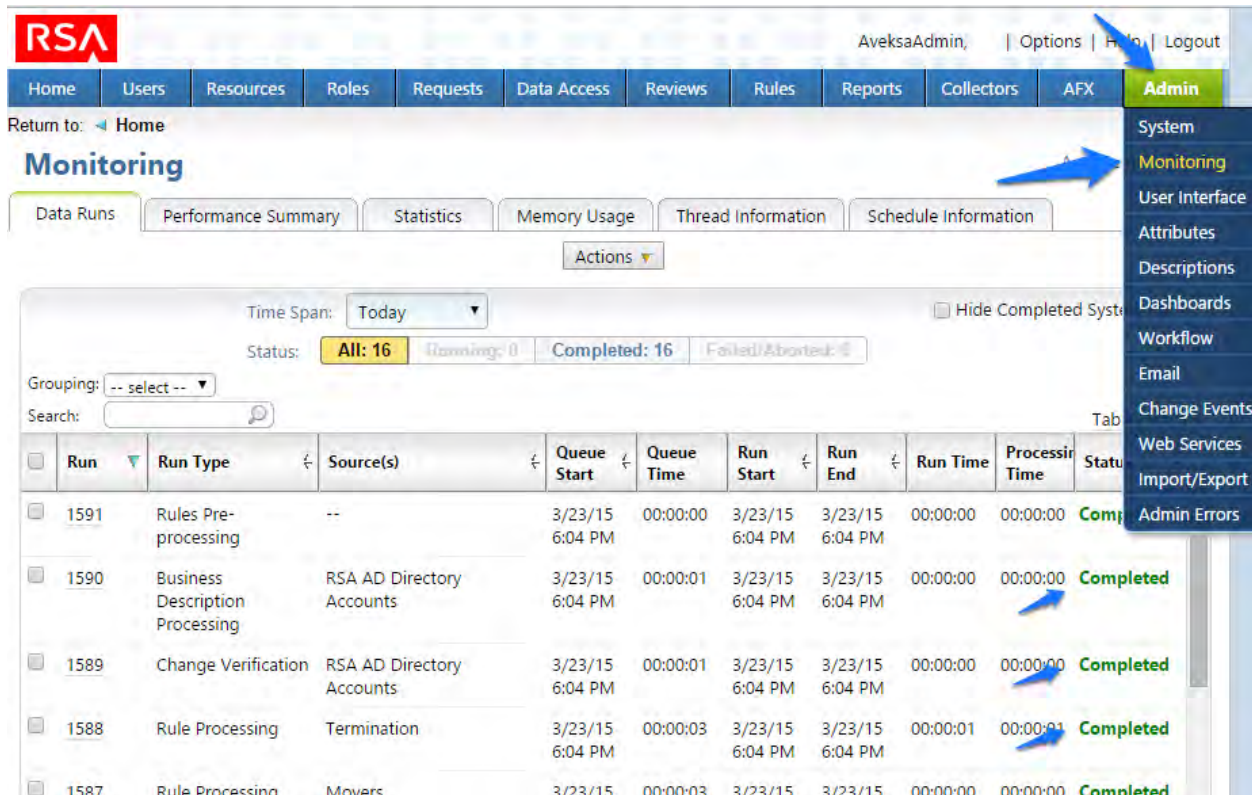
1498

Figure 59. IMG Collect Data

1499

1500

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



1501

1502

Figure 60. IMG Data Collection Monitoring

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
- 1507 data collected.

1508

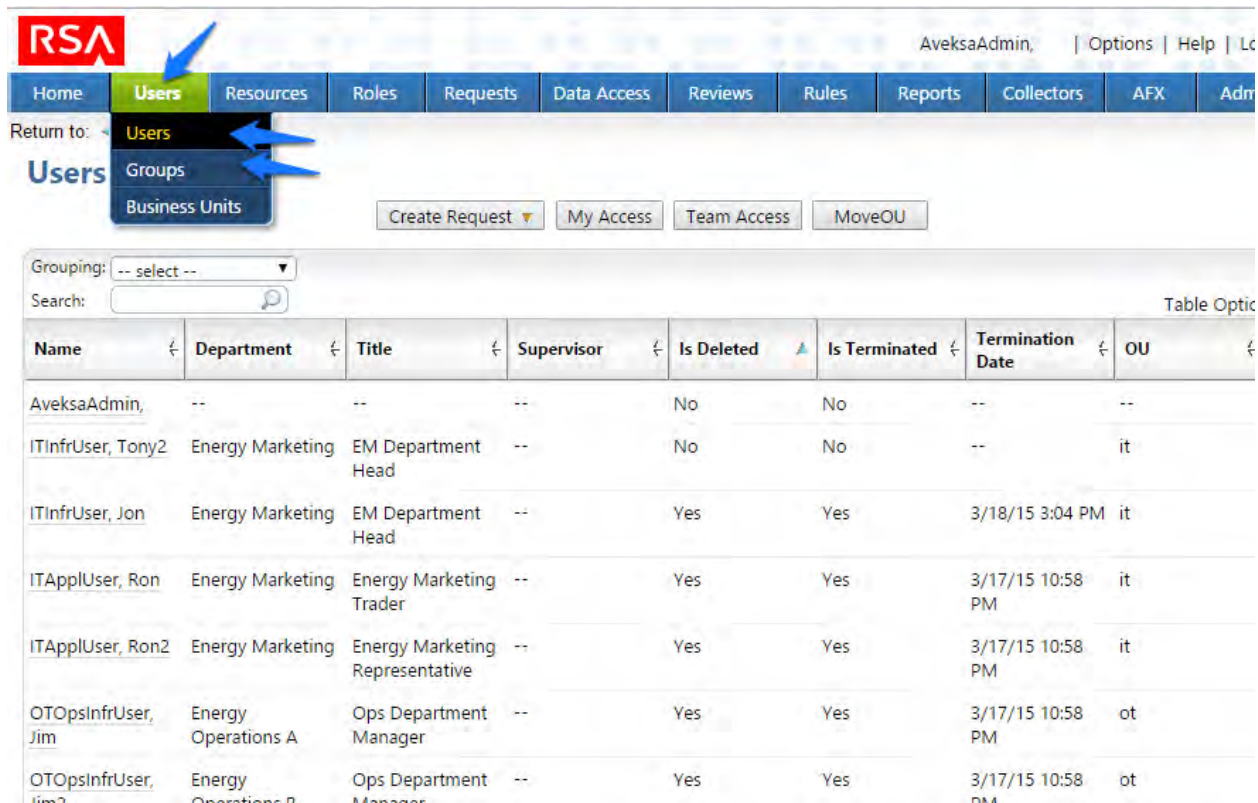


Figure 61. IMG Data Collection Review

1509

1510

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.

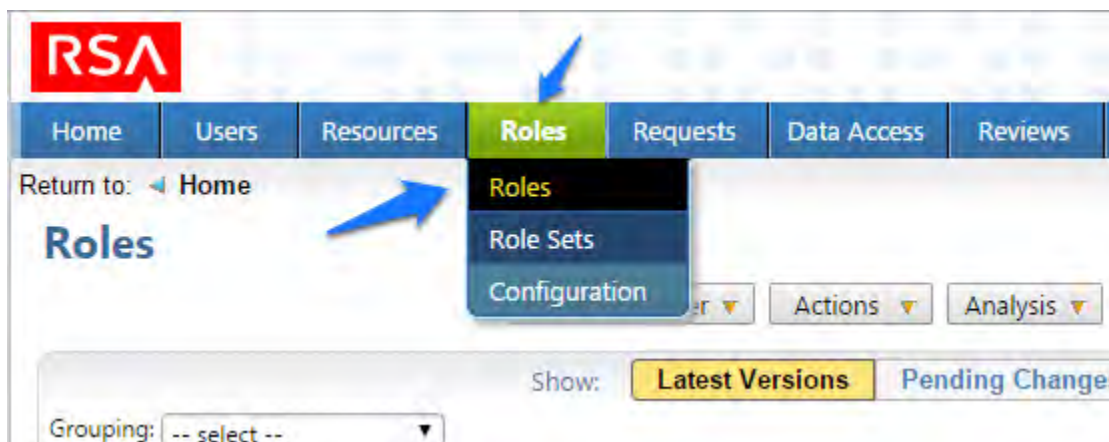


Figure 62. IMG Roles

1514

1515

- 1516 2. Click on 'Create / Discover' and 'Discover Roles' as shown in Figure 63.

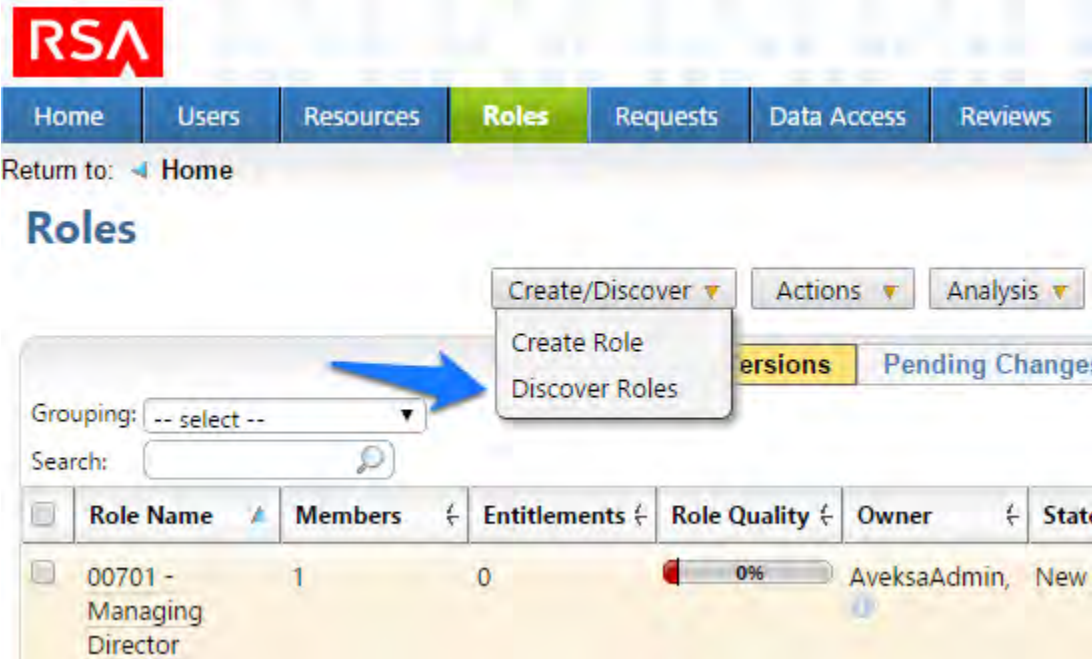


Figure 63. IMG Discover Roles

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

### Discover Roles

Role Creation

How do you want to create the roles?

- from users
- from user-entitlement clusters
- from entitlements

Where do you want to put these new roles?

- Existing role set [Job Roles](#)
- New role set named  with roles of type [Business](#)

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 65. IMG Discover Roles

**Discover Roles**

Role Information Expressions

What expressions should be used to generate role information?

Name  ▼

Last Reviewed Date  ▼

Risk  ▼

1524

1525

Figure 66. IMG Discover Roles

1526

1527

- 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:

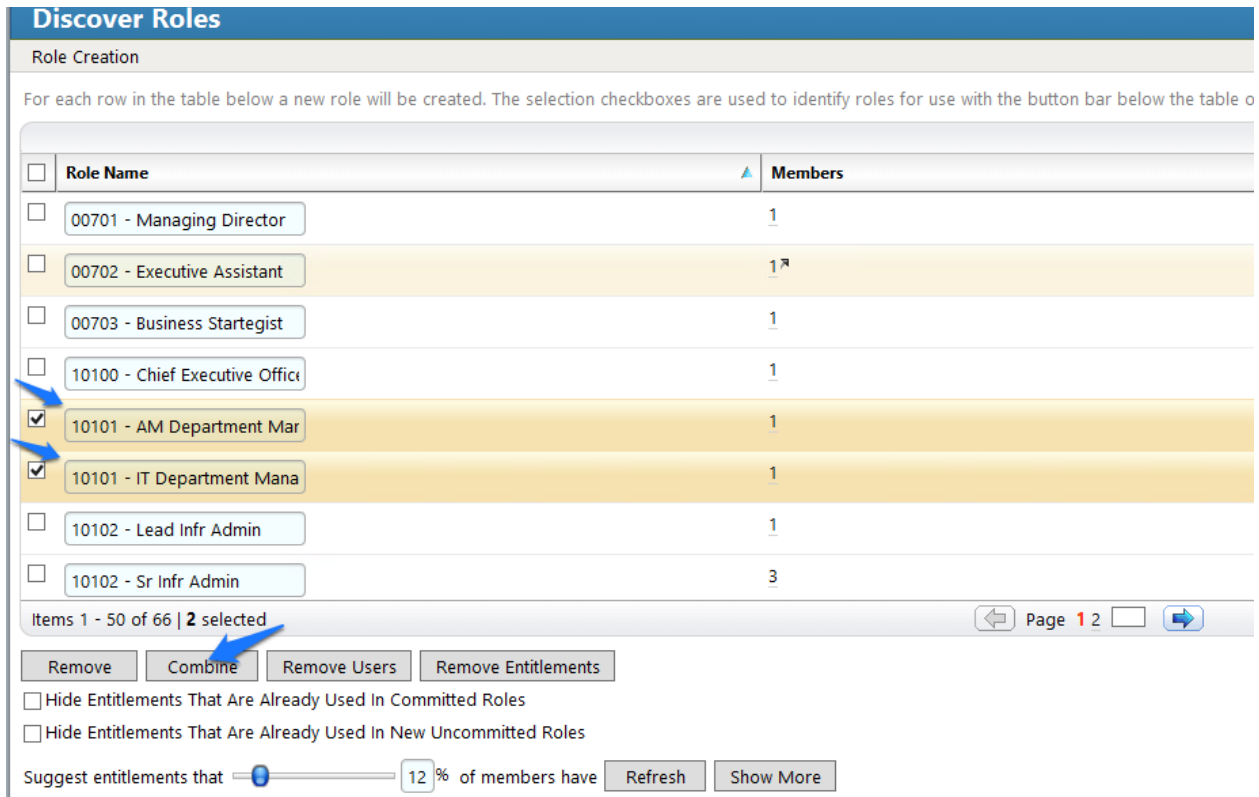


Figure 67. IMG Discover Roles

1528

1529

1530 5. When you are done combining duplicates, click Finish.

1531 7.3.12 Create Automated Rules

1532 The next step is to create rules for automatically detecting and invoking work flows for new  
 1533 users and terminations.

1534 1. Click on 'Rules' and 'Definitions' as shown in Figure 68.



1535

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\* :

Description :

Owner\* : AveksaAdmin, <sup>ⓘ</sup>

Control URL :

Control Description :

Type\* : Provisioning - Joiner/Mover ▼

Status\* : Active ▼

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

**Condition**

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

**Actions**

Assign provisioning request form Default Provisioning Form <sup>ⓘ</sup>

Provisioned entitlements\*:  
Entitlement Suggestion Modeling <sup>ⓘ</sup>  
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<sup>Ⓜ</sup>

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

*Figure 70. IMG New User*

1543

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

1544

Terminations.

### Edit Rule: Termination

Rule Name\* :

Description :

Owner\* : AveksaAdmin, ⓘ

Control URL :

Control Description :

Type\* :

Status\* :

Rule Set\* :  Existing 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

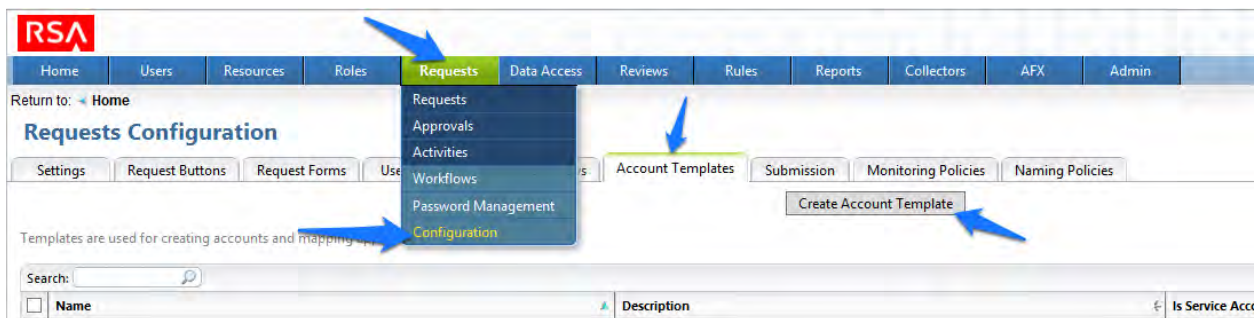
1549

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

Edit



Name: IT Account Template  
Is Service Account: No

#### Template Parameters

Add Parameter

<input type="checkbox"/>	Action	Name	Default Value	Submission Field	Table Options
<input type="checkbox"/>	Edit	CN	\$(User.Login_ID)		^
<input type="checkbox"/>	Edit	sn	\$(User.Last_Name)		
<input type="checkbox"/>	Edit	sAMAccountName	\$(User.Login_ID)		
<input type="checkbox"/>	Edit	mail	\$(User.Email_Address)		
<input type="checkbox"/>	Edit	Account	\$(User.Login_ID)		
<input type="checkbox"/>	Edit	userPrincipalName	\$(User.Email_Address)		
<input type="checkbox"/>	Edit	Password	\$(GeneratedPassword)		
<input type="checkbox"/>	Edit	givenName	\$(User.First_Name)		v

8 items  
Delete

#### Pending Account Parameters

Add Pending Account Parameter

<input type="checkbox"/>	Action	Name	Default Value	Submission Field	Table Options
<input type="checkbox"/>	Edit	Name	CN=\${User.Login_ID};ou=\${User.OU};dc=master;dc=test		^

1 item  
Delete

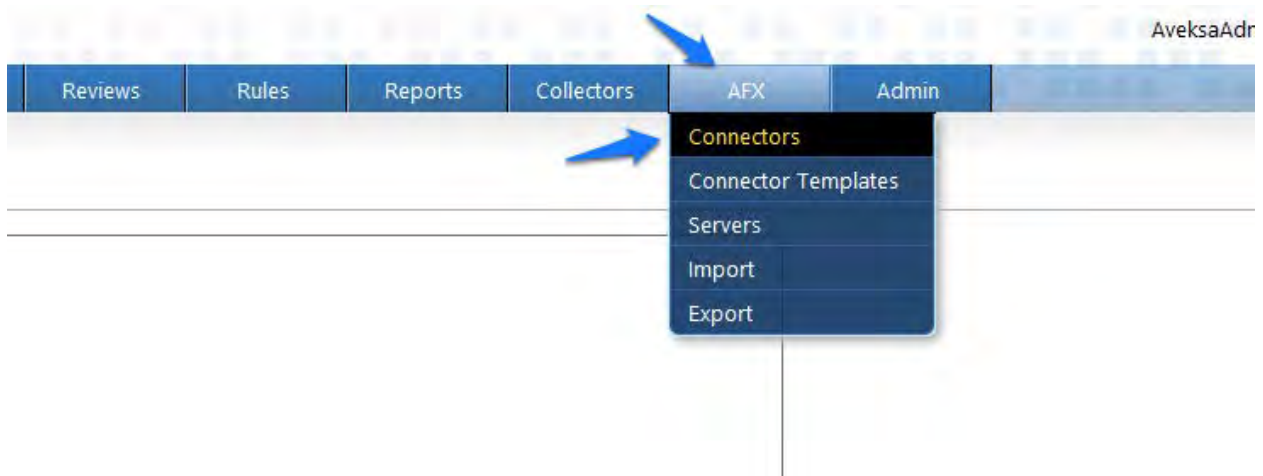
1563

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.

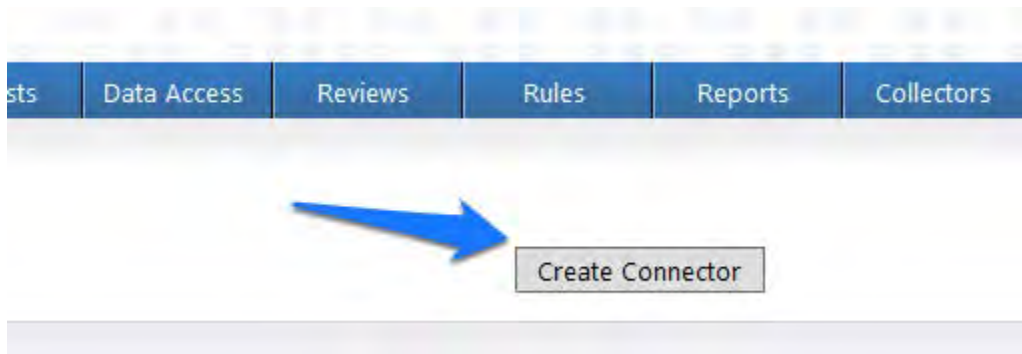


1567

1568

Figure 76. IMG AFX Connectors

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



1570

1571

Figure 77. IMG Create Connector

1572

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



1573

1574

Figure 78. IMG AD Connector AFX Server

1575

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 :

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 : cn=Directory Manager  
Name\*

Password\* : [Redacted]

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\*

LDAP object classes to :  
create group\*

### Group

User membership :  
attribute for Group\*

### AccountLockUnlock

Account Lockout :  
Threshold attribute  
value\*

### Miscellaneous

Dependent Exchange :  
Connector

1580

1581

Figure 81. IMG AD Connector AFX Server

1582 8. Configure the 'Capabilities' tab as shown in Figure 82.

**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

1583



1584

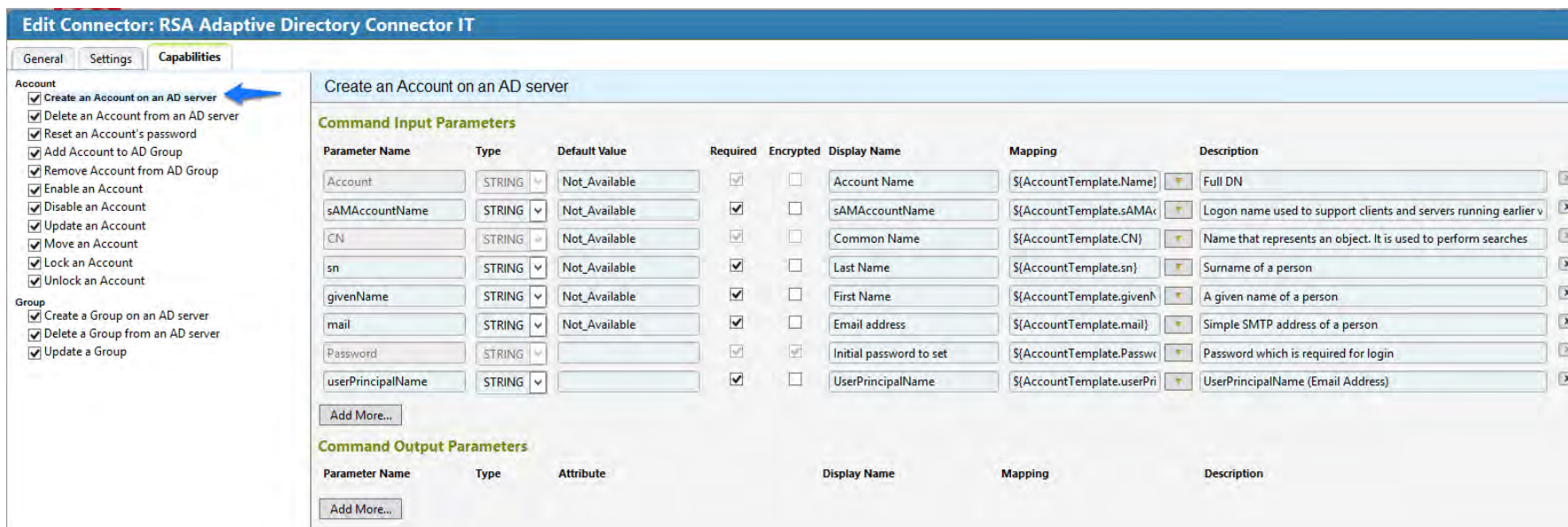
*Figure 82. IMG AD Connector IT*

1585

1586

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

1587



1588

1589

1590

Figure 83. IMG AD Connector IT Capability Configuration

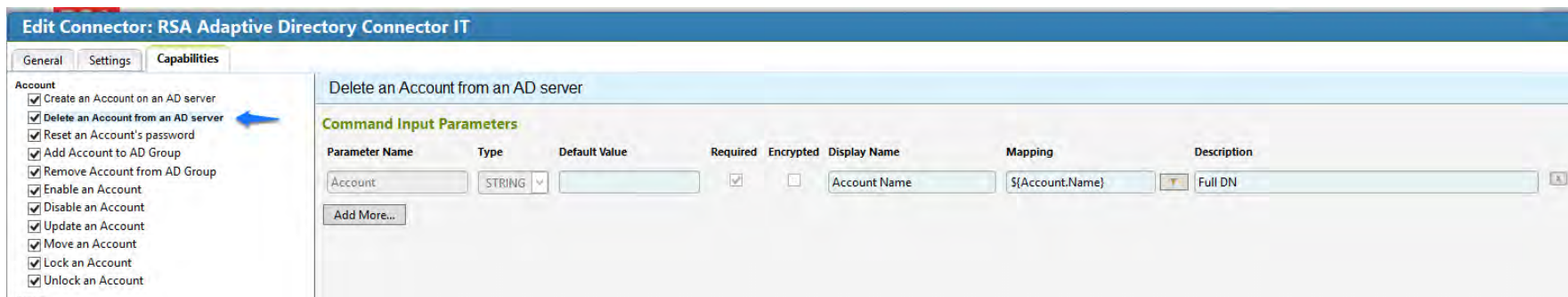
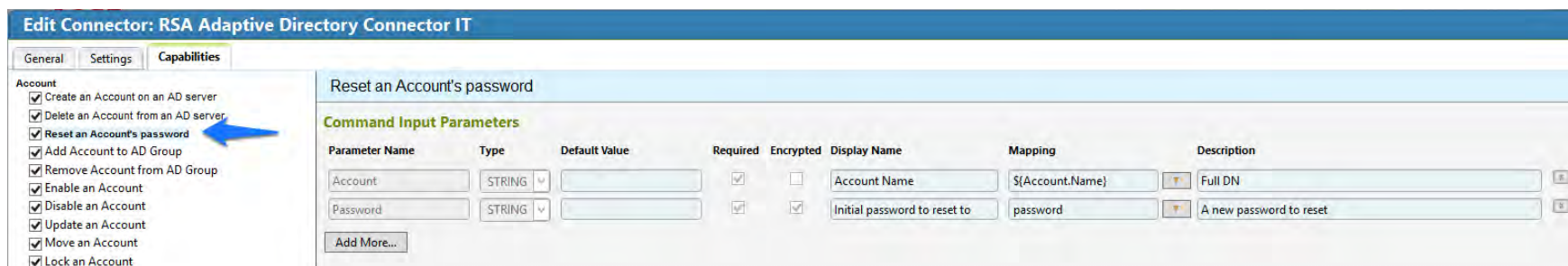


Figure 84. IMG AD Connector IT Capability Configuration

1591



1592

1593

Figure 85. IMG AD Connector IT Capability Configuration

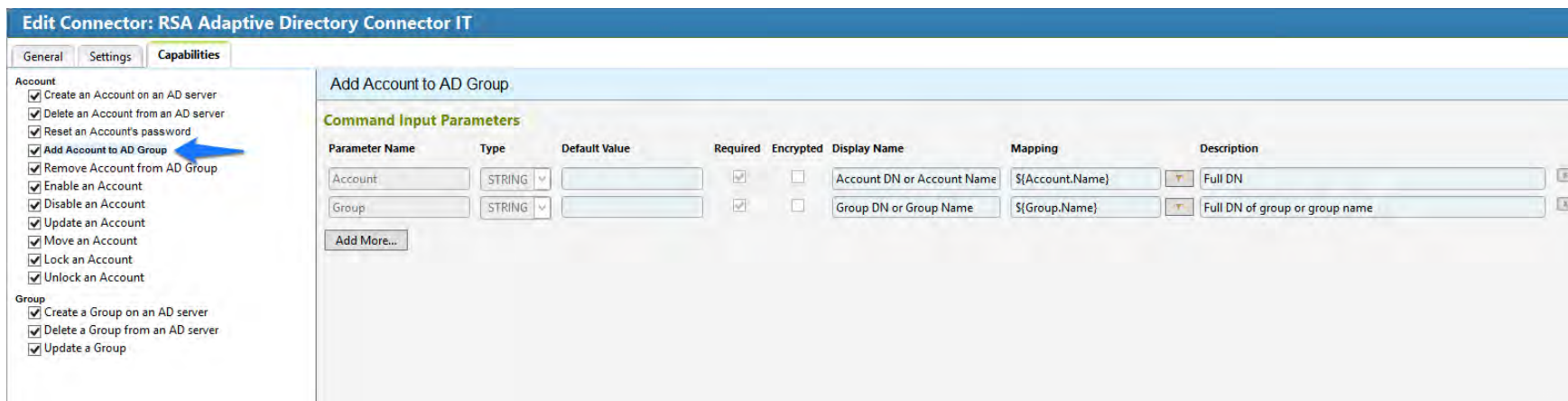


Figure 86. IMG AD Connector IT Capability Configuration

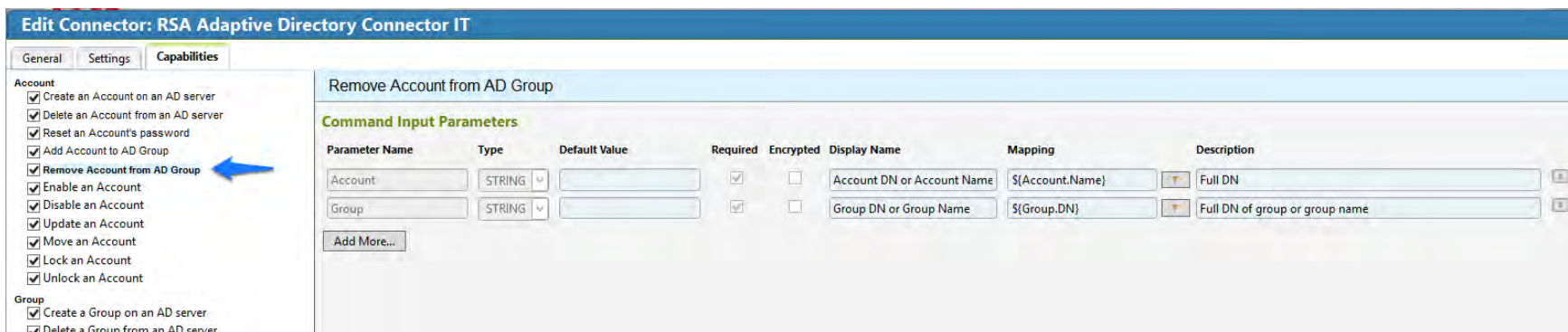


Figure 87. IMG AD Connector IT Capability Configuration

1595  
1596

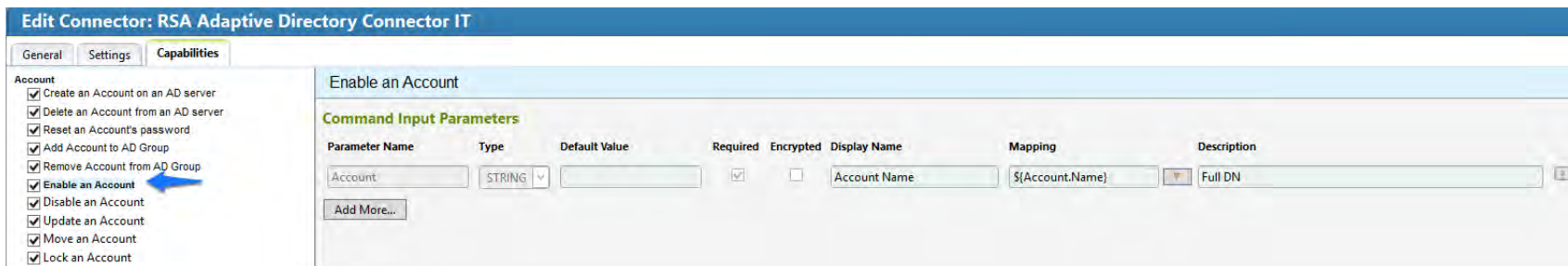


Figure 88. IMG AD Connector IT Capability Configuration

1597  
1598

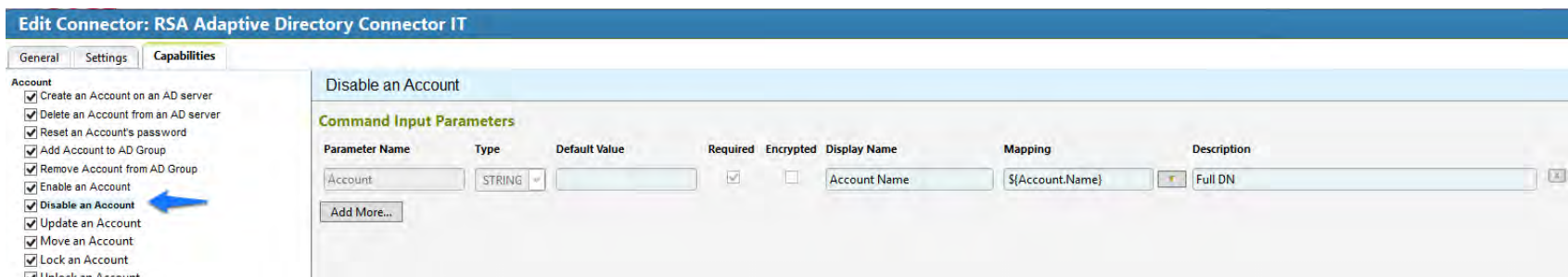
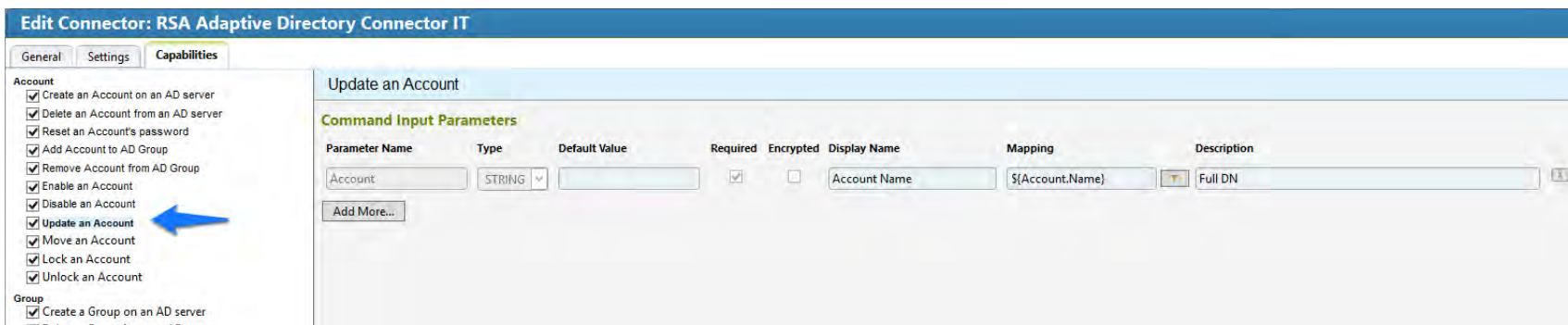


Figure 89. IMG AD Connector IT Capability Configuration

1599  
1600

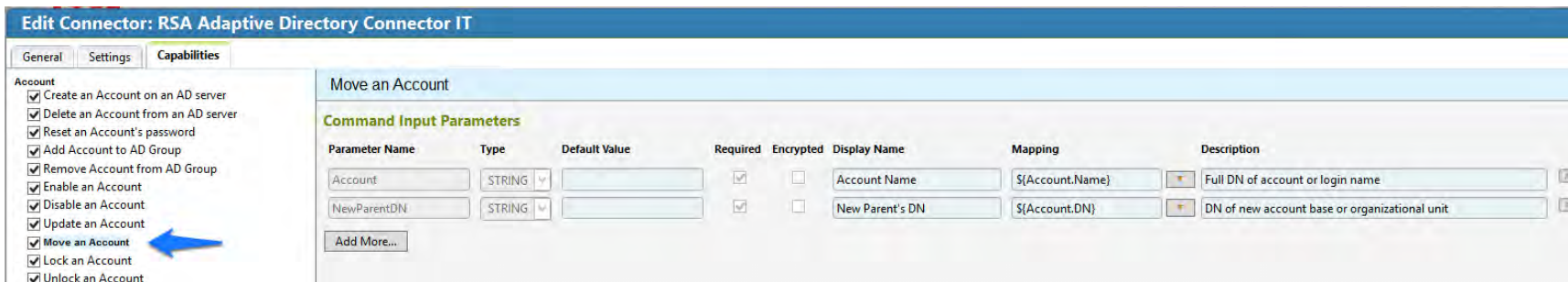
1601



1602

1603

Figure 90. IMG AD Connector IT Capability Configuration



1604

1605

1606

Figure 91. IMG AD Connector IT Capability Configuration

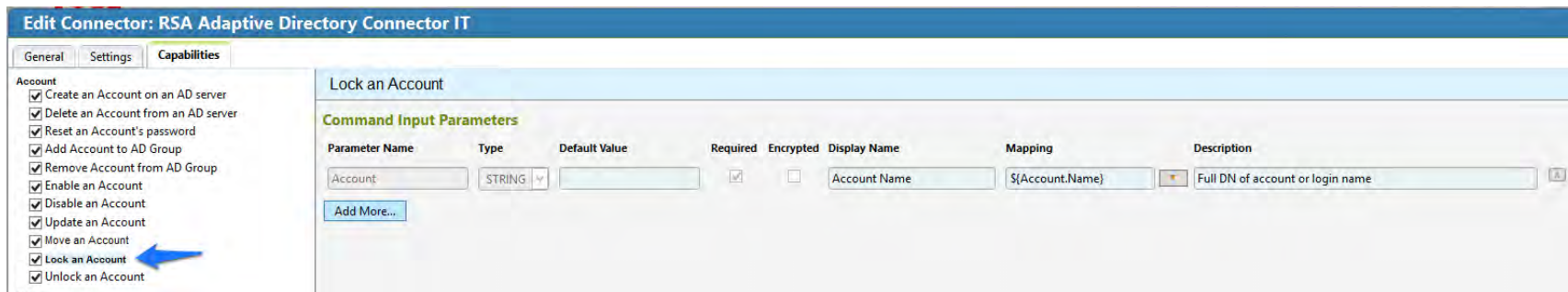


Figure 92. IMG AD Connector IT Capability Configuration

1607

1608

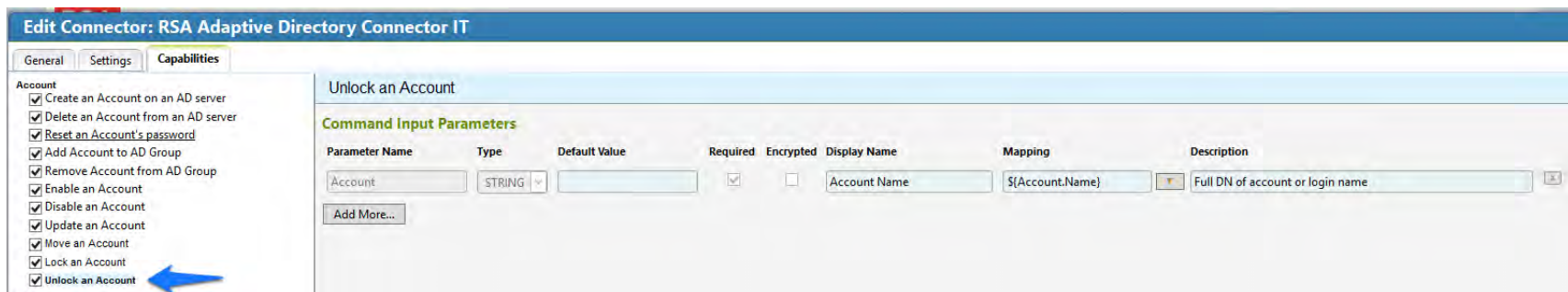
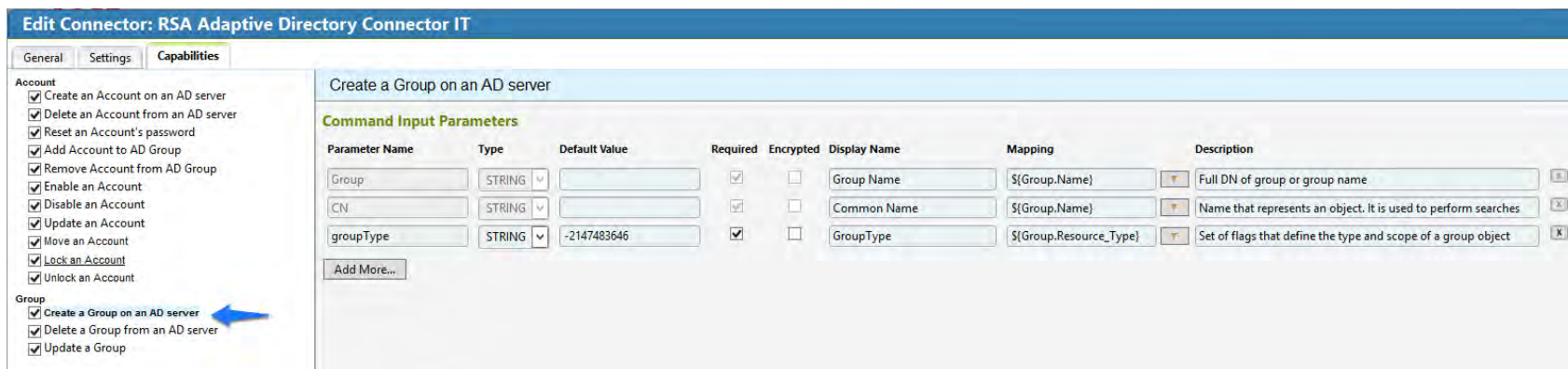


Figure 93. IMG AD Connector IT Capability Configuration

1609

1610

1611



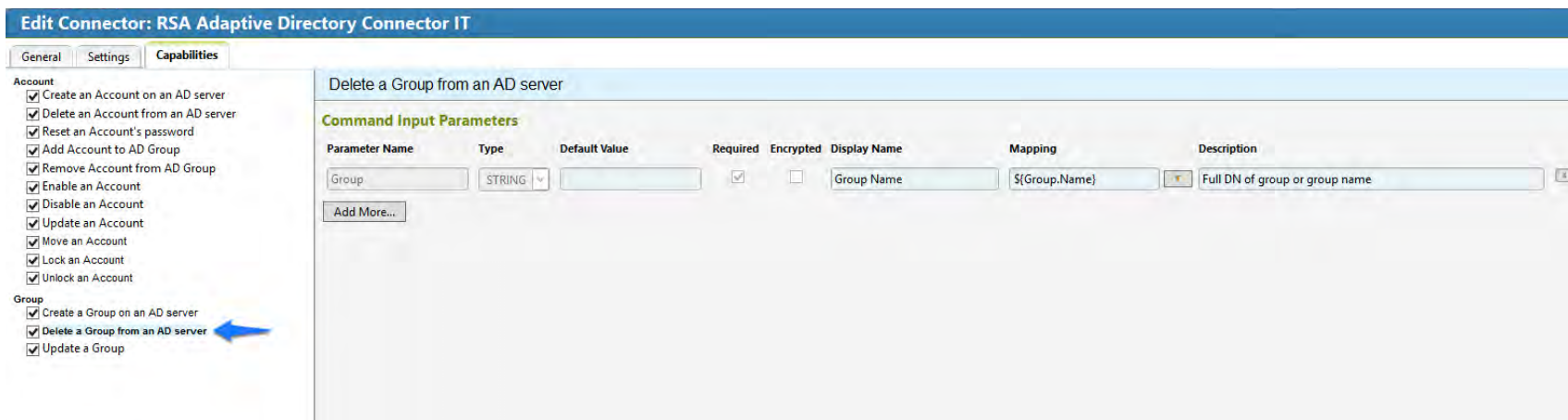
1612

1613

1614

Figure 94. IMG AD Connector IT Capability Configuration

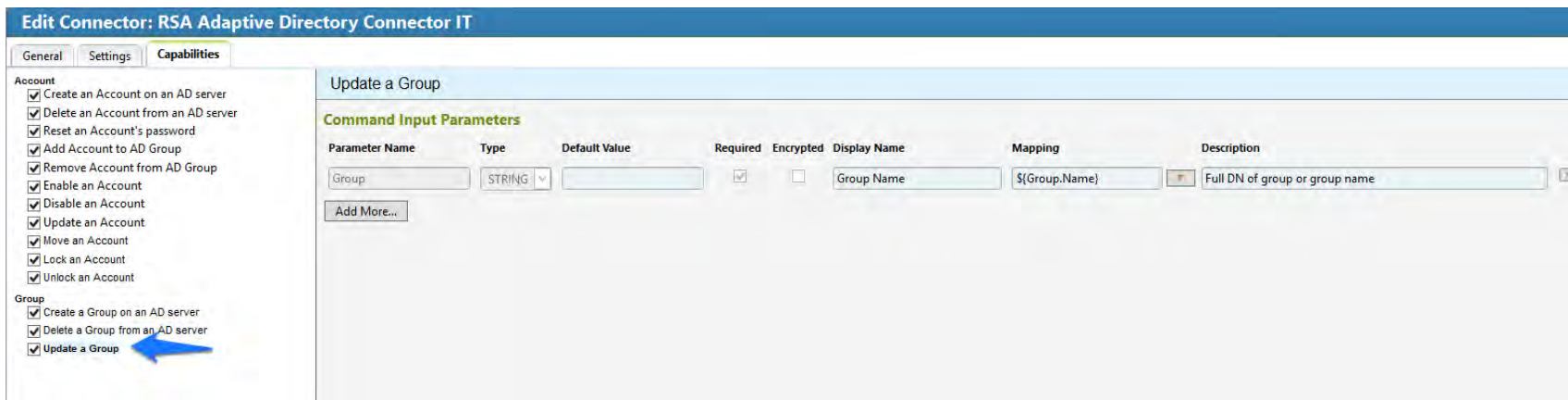




1615  
1616

1617

Figure 95. IMG AD Connector IT Capability Configuration



1618

1619

1620

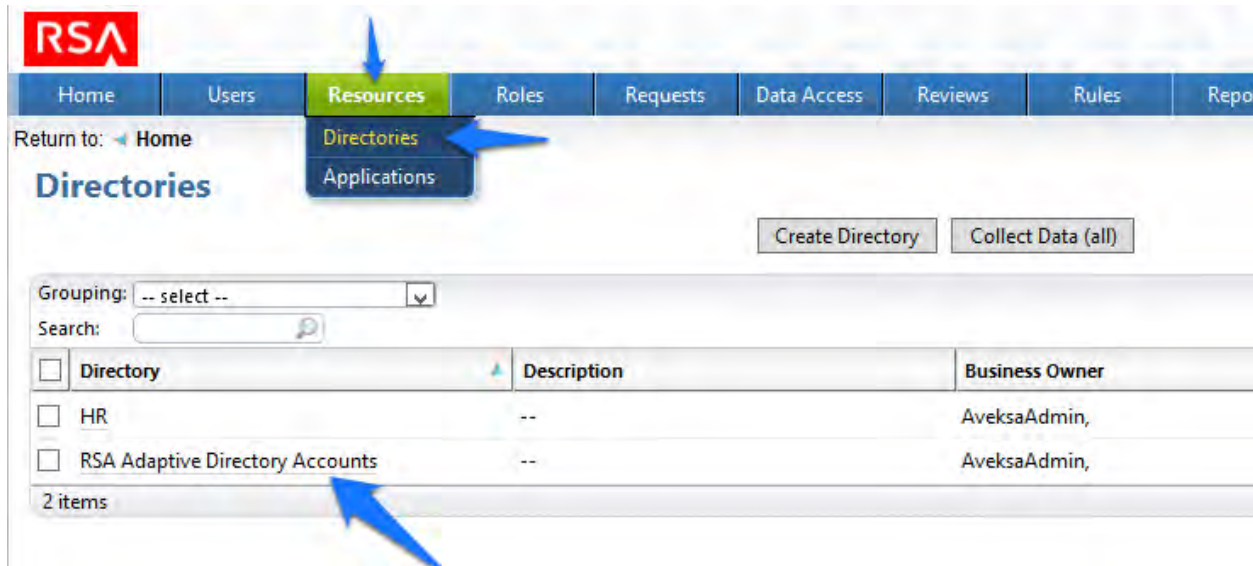
10. Click OK.

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.



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.

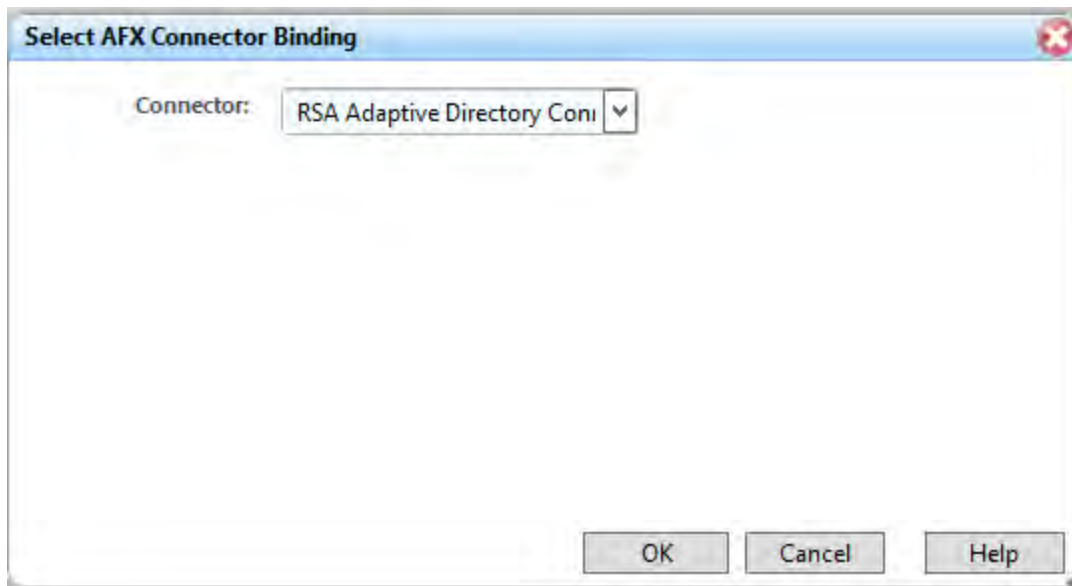
- 1628 3. Click the Edit Connector Binding as shown in Figure 98.



1629

1630

Figure 98. IMG AD Accounts



1631

1632

Figure 99. IMG AD AFX Connector Binding

1633 4. Click OK as shown in Figure 99.

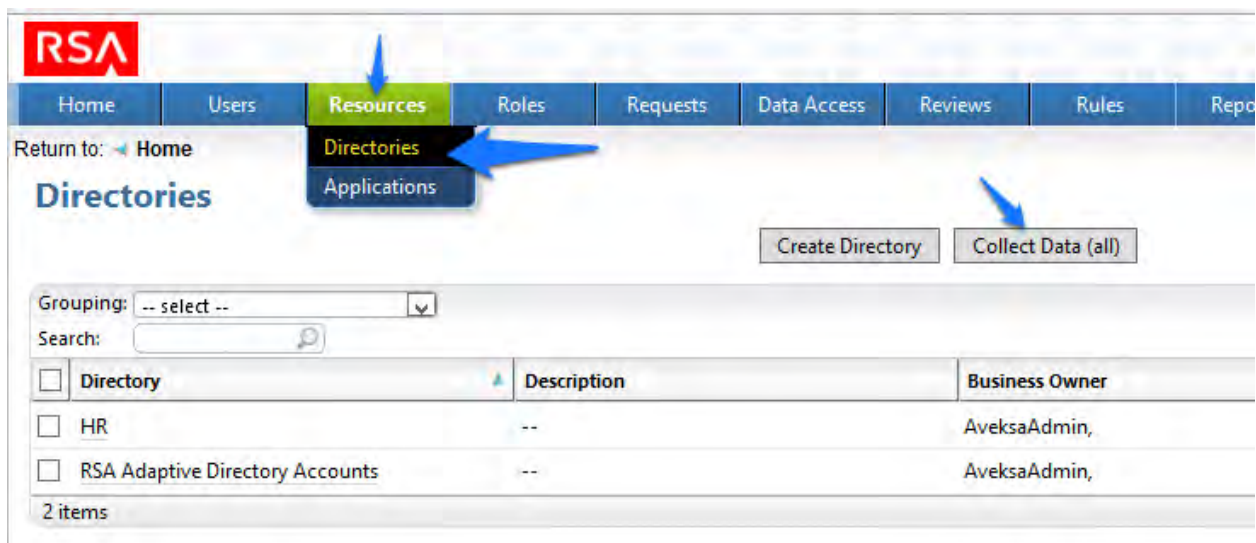
1634 Now the system is ready.

## 1635 7.4 USING RSA IMG

### 1636 7.4.1 Adding a New User

1637 1. Open the HR CSV file and add a user.

1638 2. Go to 'Resources', 'Directories' and click 'Collect Data (all)' as shown in Figure 100.



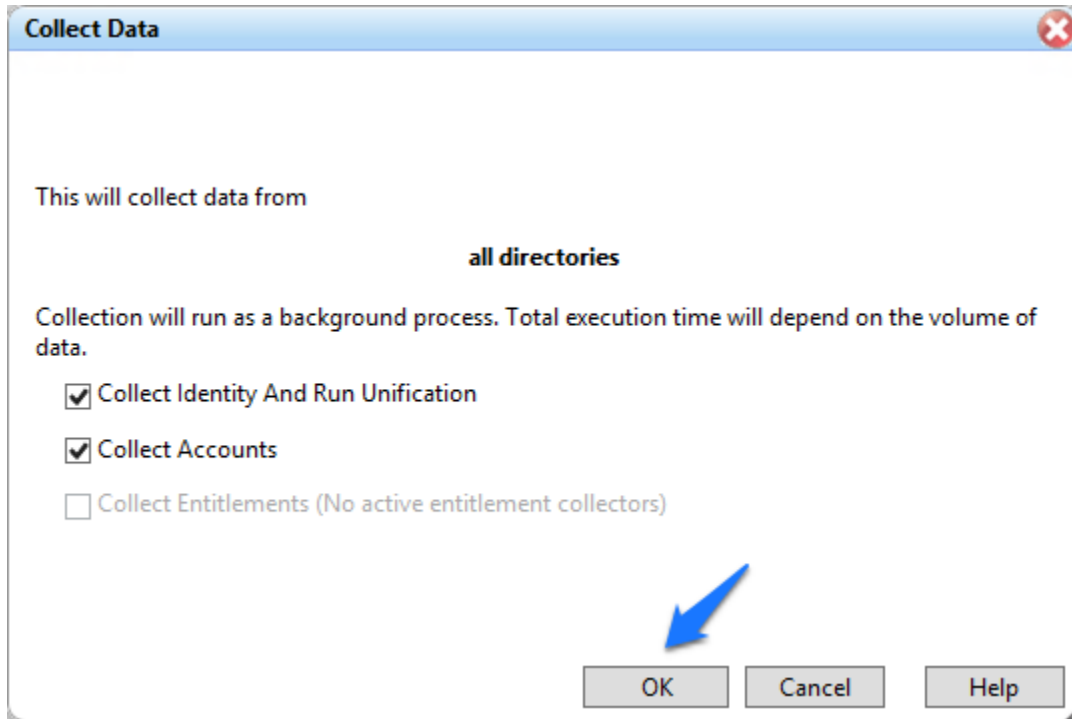
1639

1640

Figure 100. IMG Resources Directories

1641

1642 1. Click 'OK' as shown in Figure 101.

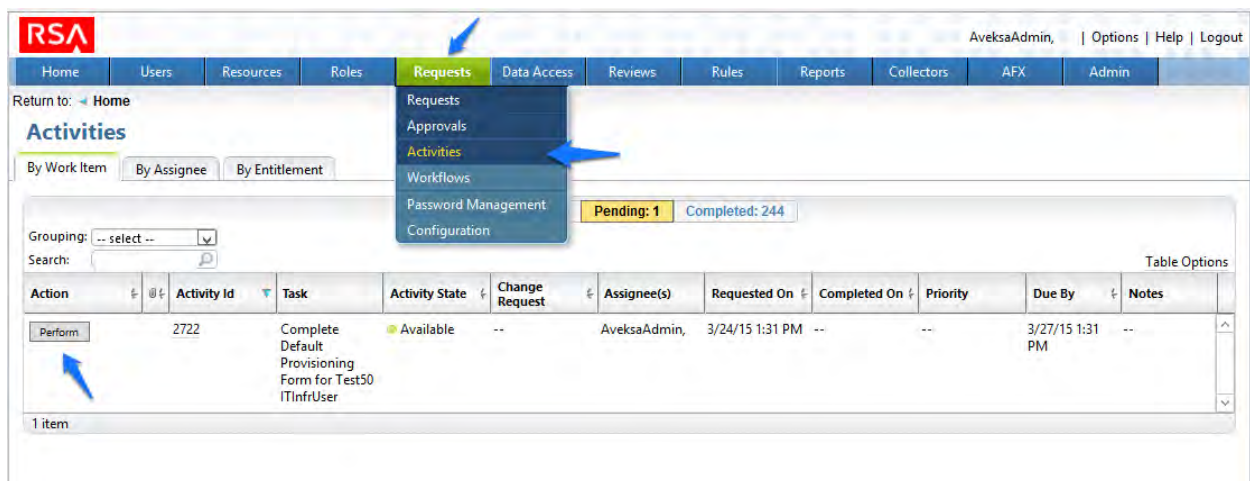


1643

Figure 101. IMG Collect Data

1644

1645 2. After about 30 seconds go to 'Requests', 'Activities' and click 'Perform' next to the  
 1646 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 Figure 103.

1650

**Access Request: ITInfrUser, Test50**

Default Provisioning Form Page 1 of ?

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

Search:

<input checked="" type="checkbox"/>	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?

1651

1652

Figure 103. IMG Accepted Access Request

1653

4. Enter a description if you wish, and click 'Finish'.

1654

5. Go to 'Requests', and click 'Requests'. Click the name of the request as shown in Figure 104.

1655

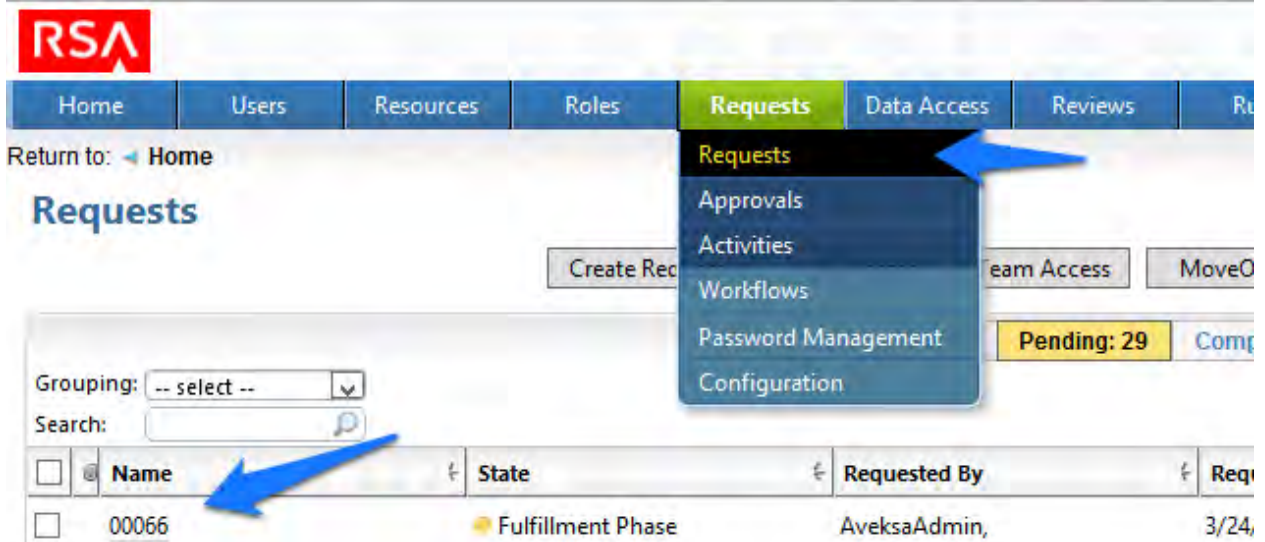
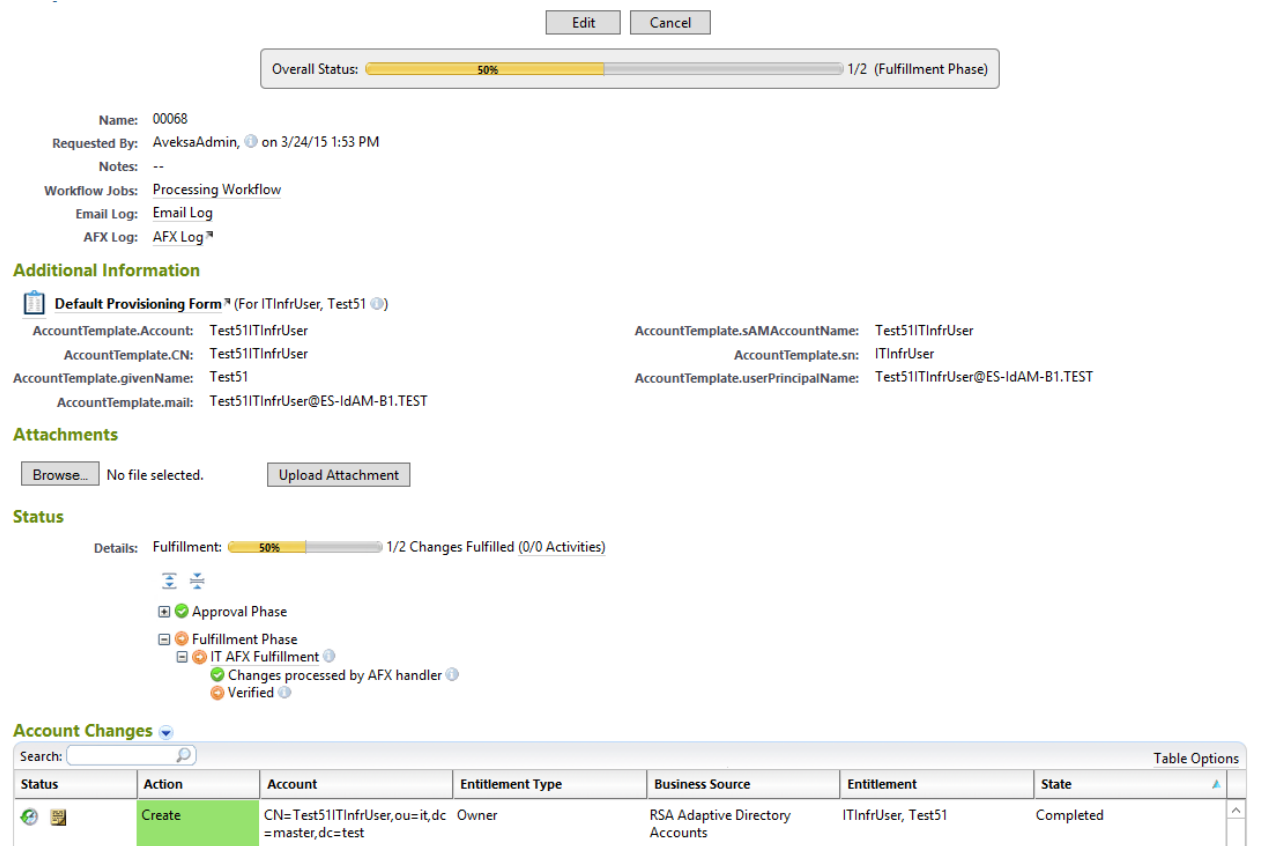


Figure 104. IMG Requests

1656  
1657  
1658  
1659  
1660

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



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

**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

- 1669 1. Open your CSV file and change the attribute that defines the OU that the user is in to a  
 1670 different OU.
- 1671 2. Collect data again.
- 1672 3. The OU change is detected, and IMG deletes the user from the original OU and adds the  
 1673 user to the new OU.
- 1674 4. Go to 'Requests' and 'Activities' and click 'Perform' as shown in Figure 107.

Return to: [Home](#)

## Activities

By Work Item | By Assignee | By Entitlement

Show: All: 253 Pending: 1 Completed: 252

Grouping: -- select --

Search:

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,	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.



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

**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**

No file selected.

**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**

Search:

Status	Action	Account	Entitlement Type	Business Source	Entitlement	State
	Delete	CN=Test52OTInfrUser,ou=ot,dc=master,dc=test	Account		OTInfrUser, Test52	Completed

1 item

Figure 108. IMG Request Status

1687

1688

## 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

#### 1701 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 &lt;ENTER&gt; TO ACCEPT THE FOLLOWING (OK): Enter

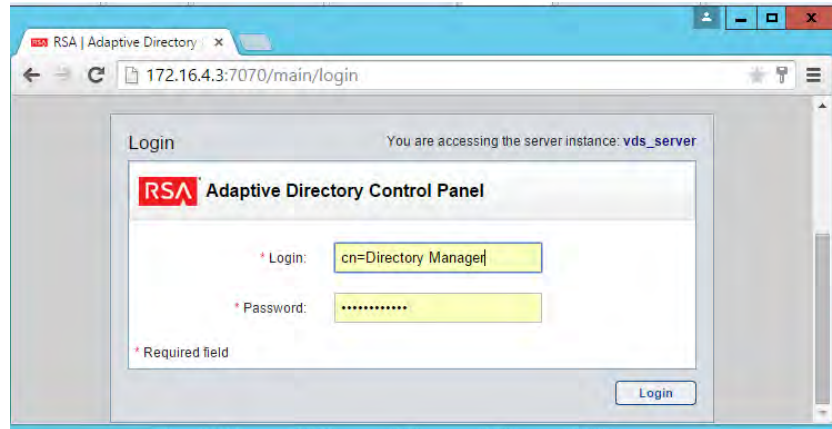
1843

```
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/adaptivedirectory 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/adaptivedirectory/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/adaptivedirectory/vds_server`  
1896 Open all relevant firewall ports on the CentOS server  
1897 Run `/root/rsa/adaptivedirectory/bin/openControlPanel.sh`  
1898 Run `/root/rsa/adaptivedirectory/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

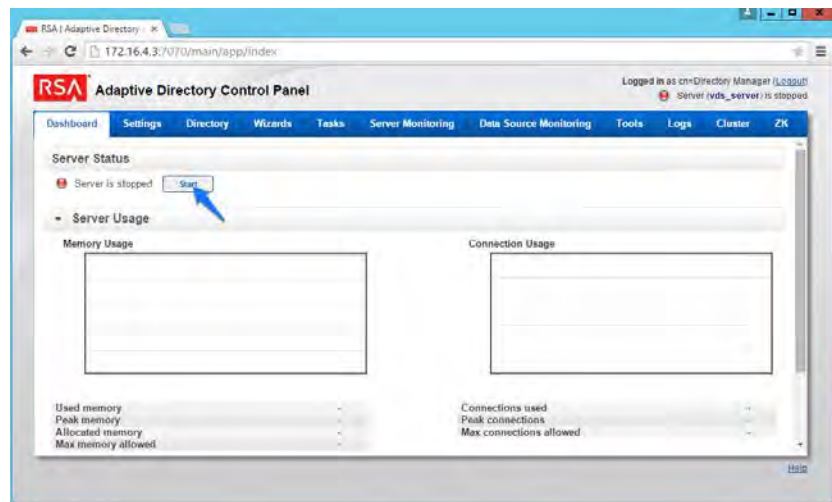


1909

1910

Figure 109. Adaptive Directory Login Page

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



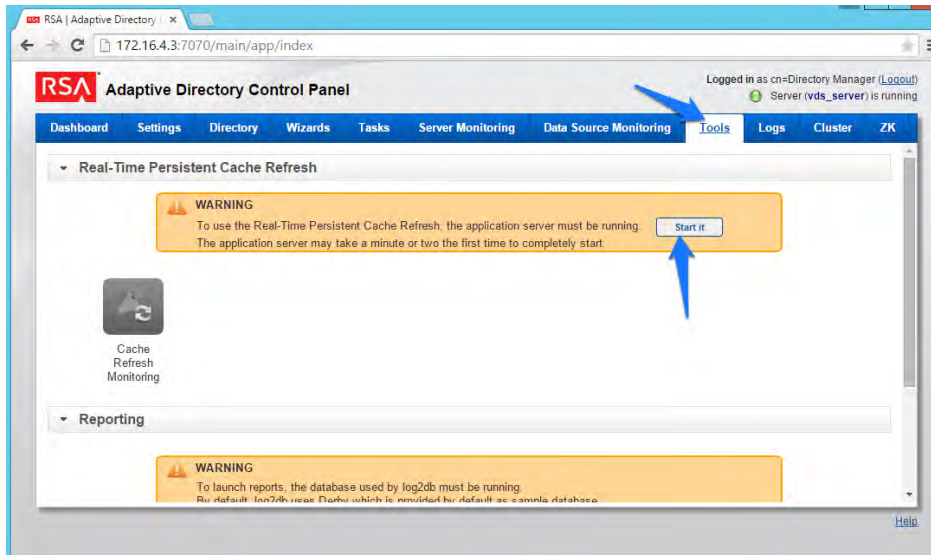
1912

1913

Figure 110. Adaptive Directory Main Page

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



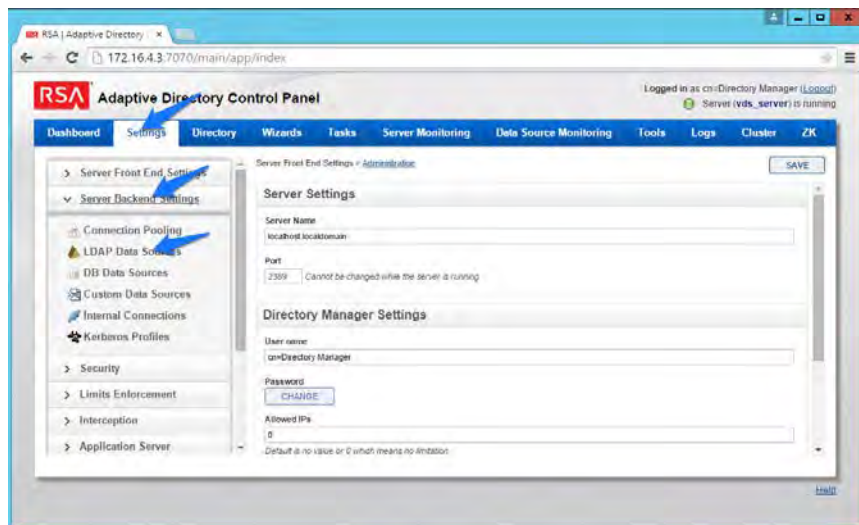


1915

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  
1918 Data Sources.

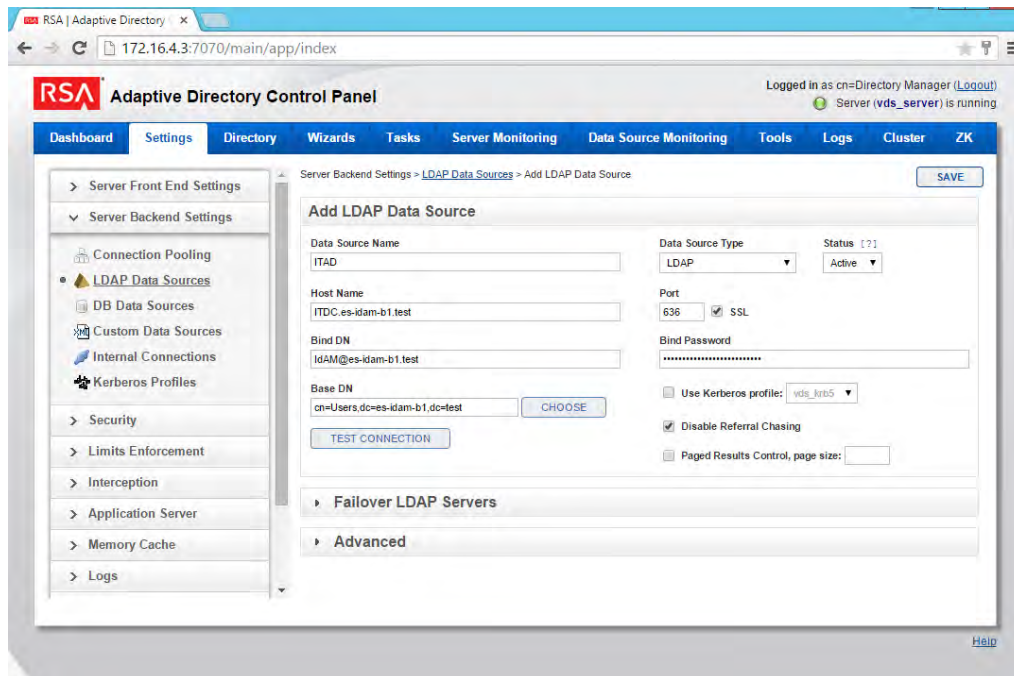


1919

1920

Figure 112. Adaptive Directory Server Backend Settings

1921 Click Add.



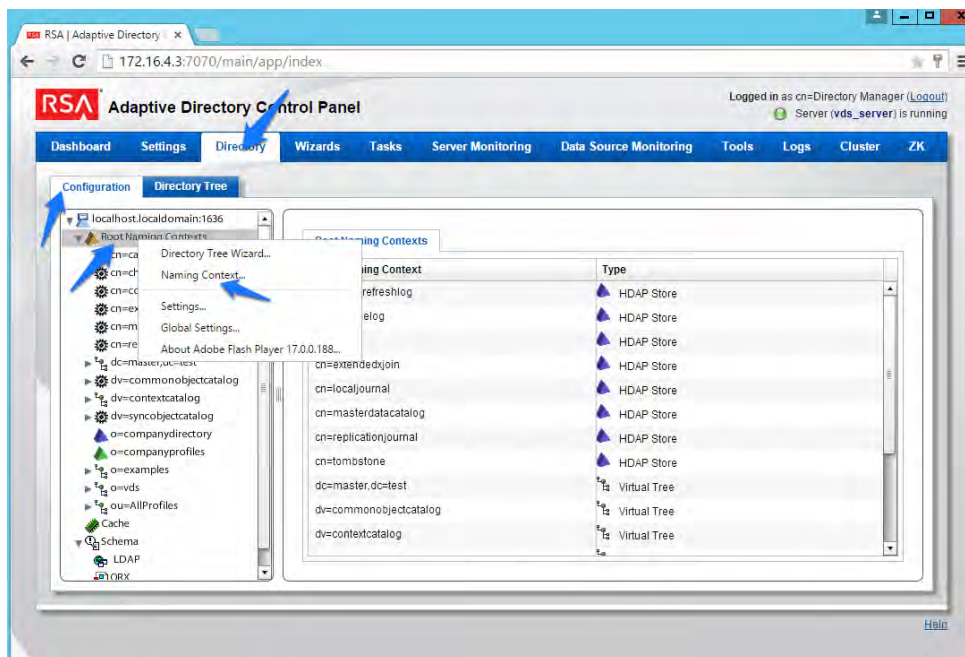
1922

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.

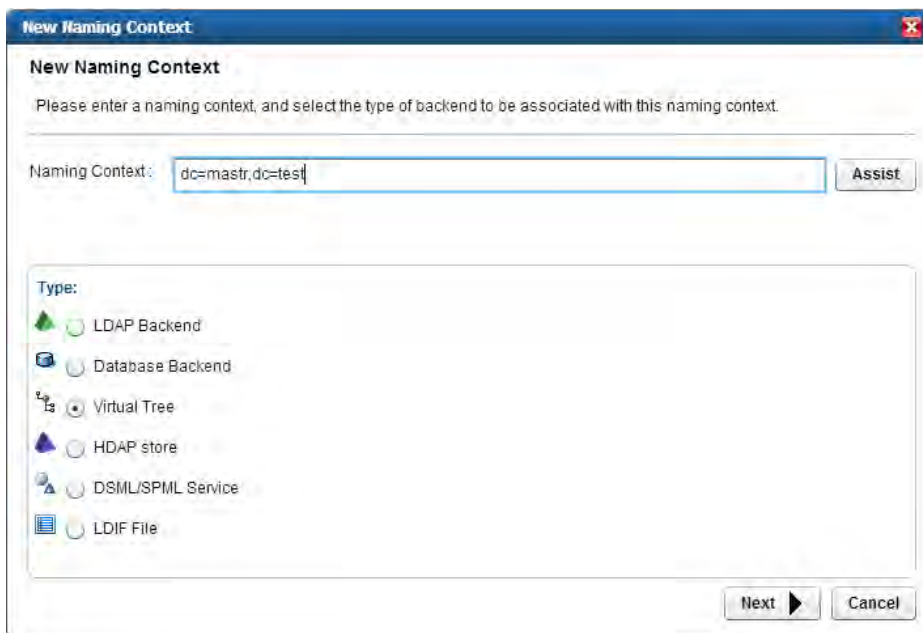


1930

1931

Figure 114. Adaptive Directory Configuration of Naming Context

1932 You are presented with this screen, Figure 115:

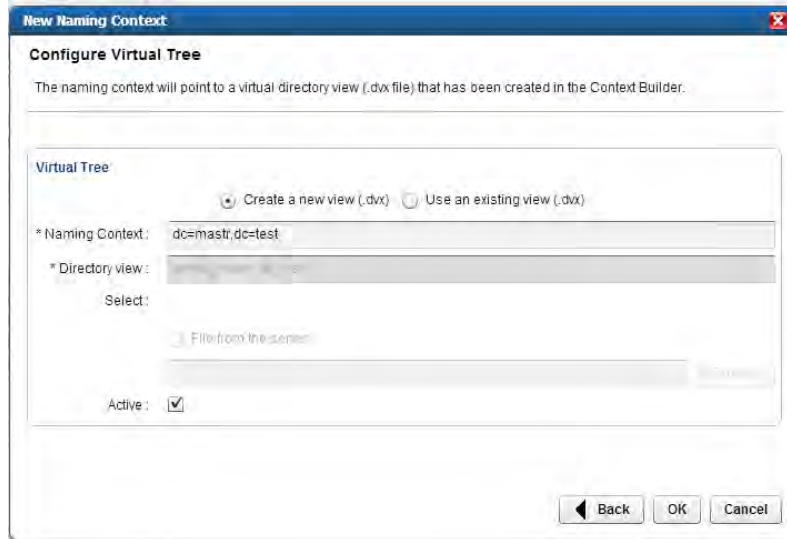


1933

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  
 1936 Virtual Tree and click Next.



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  
1940 screen, Figure 117.



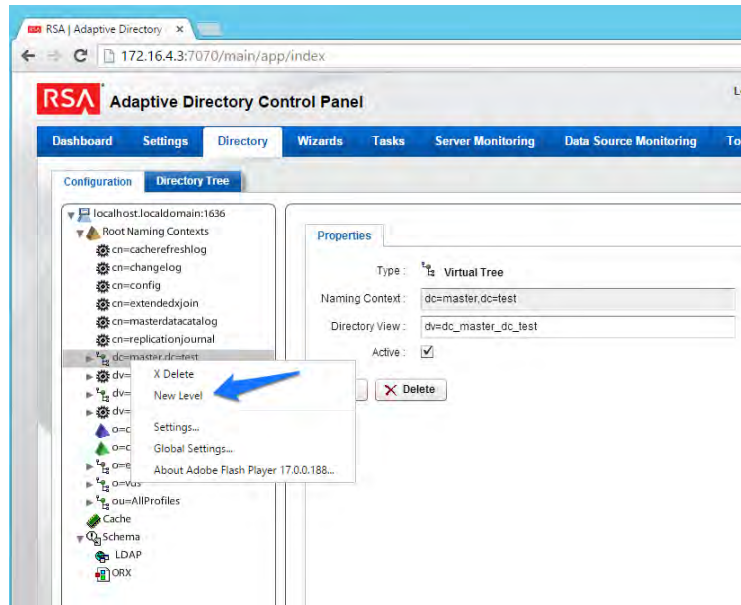
1941

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:

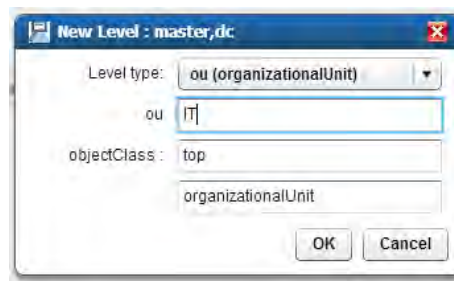


1946

1947

Figure 118. Adaptive Directory Create New Level

1948 Enter a “name” for this LDAP backend mapping. This name will be an OU in the Virtual  
 1949 Directory as shown in Figure 119.

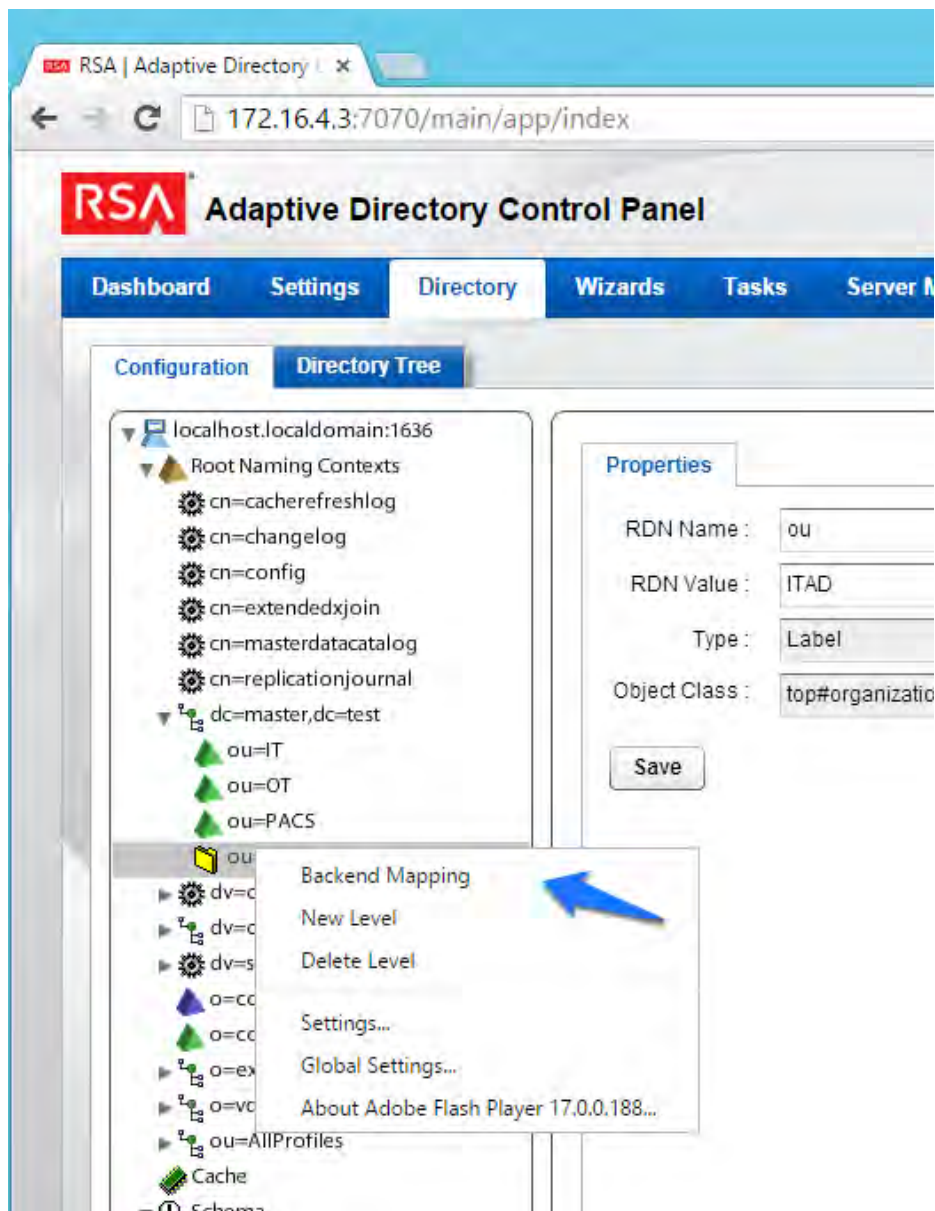


1950

1951

Figure 119. Adaptive Directory New Level Name

1952 Right-click this new OU in your Virtual Directory and select Backend Mapping as shown in Figure  
 1953 120.

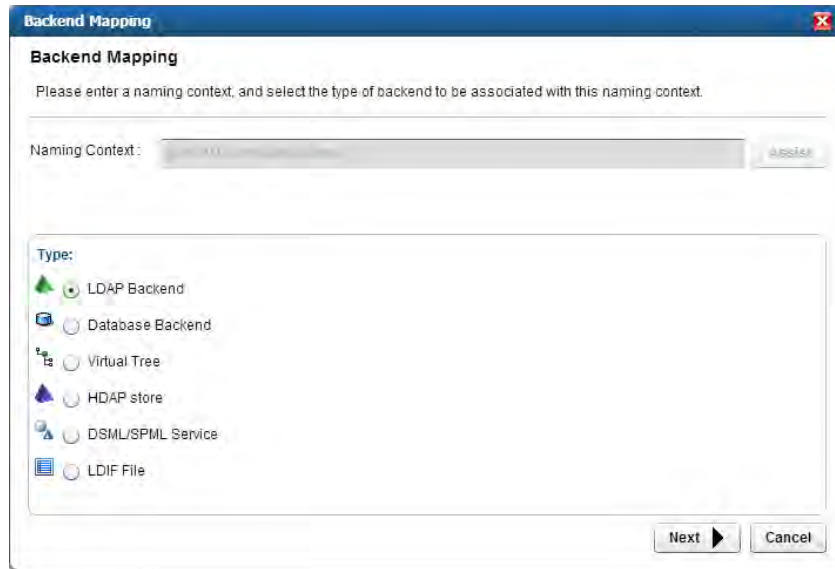


1954

1955

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

Figure 120. Adaptive Directory Backend Mapping

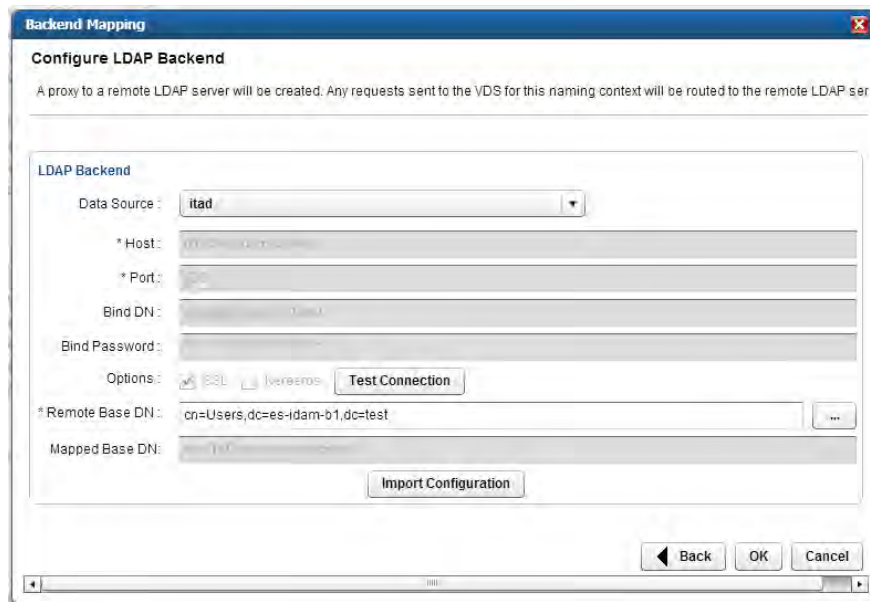


1957

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,  
 1964 and PACS networks).

1965 By default, the Adaptive Directory server will return default AD attributes.

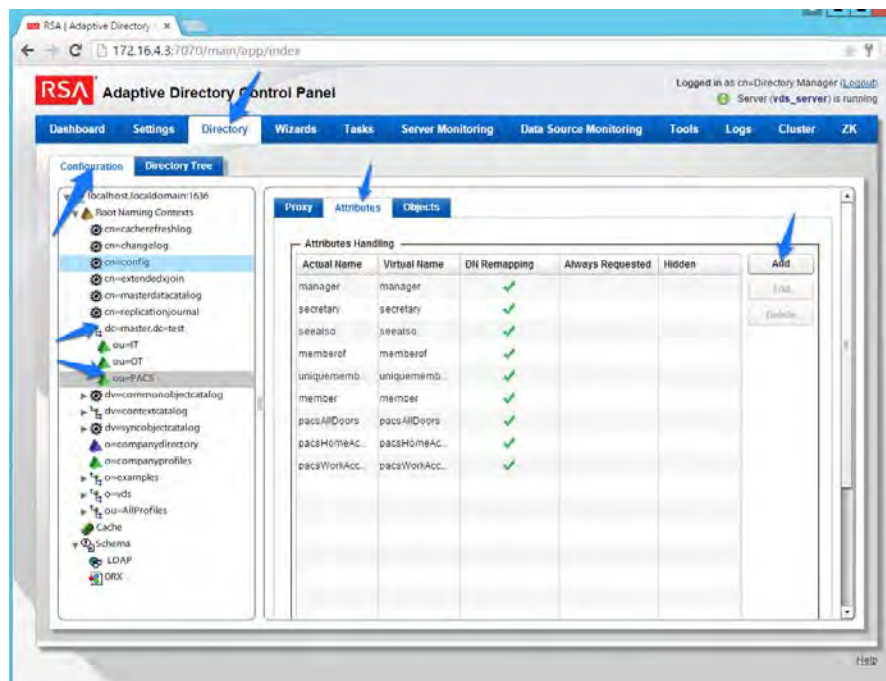
1966 **8.4 CUSTOM ATTRIBUTE CONFIGURATION**

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.



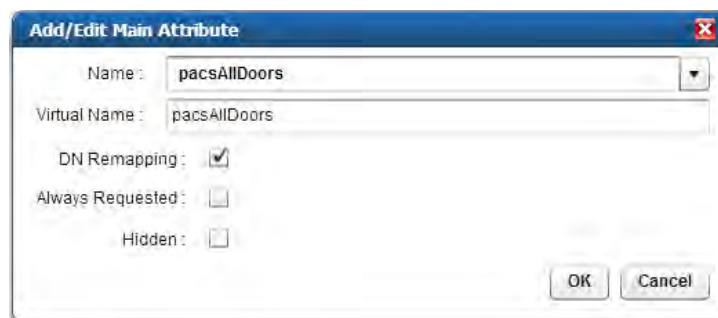
1971

1972 *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

1977 *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.

The screenshot shows a configuration window titled "Edit Collector: RSA AD Directory Account". Under the "Connection" section, the following fields are visible:
 

- Host\*: 172.16.4.3
- Port\*: 2389
- Bind DN\*: cn=Directory Manager
- Bind Password\*: [masked with dots]
- Use SSL:
- Disable Paging:

1989

1990

Figure 125. Adaptive Directory Edit Collector

The screenshot shows a configuration window titled "Search Configuration for Accounts". It includes a note: "Accounts will be created by the User Account Mapping, unless the Accounts option is selected in this collector." The configuration fields are:
 

- Account Base DN\*: dc=master,dc=test
- Account Search Scope\*: Subtree
- Account Search Filter\*: (&(objectCategory=person)(objectClass=user)(sAMAccountName=\*))

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/downloadwz.com](http://www.winzip.com/downloadwz.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:  
2098

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`  
2103

- 2104 3. Setting Path:  
2105

2106 `PATH= C:\Program Files\Java\JDK1.6.0-21\bin;%PATH%`  
2107

- 2108 4. Checking JAVA\_HOME and PATH:  
2109

2110 `Echo %JAVA_HOME%`

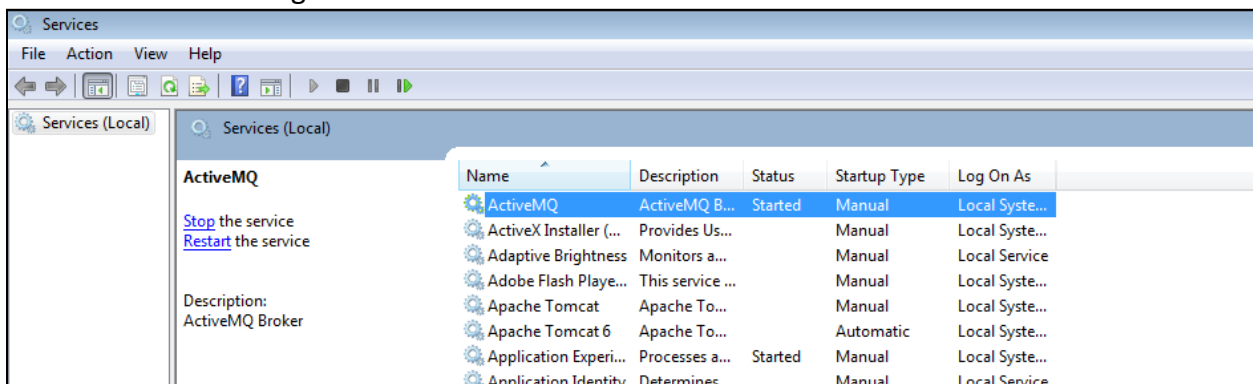
2111 `Echo %PATH%`

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.



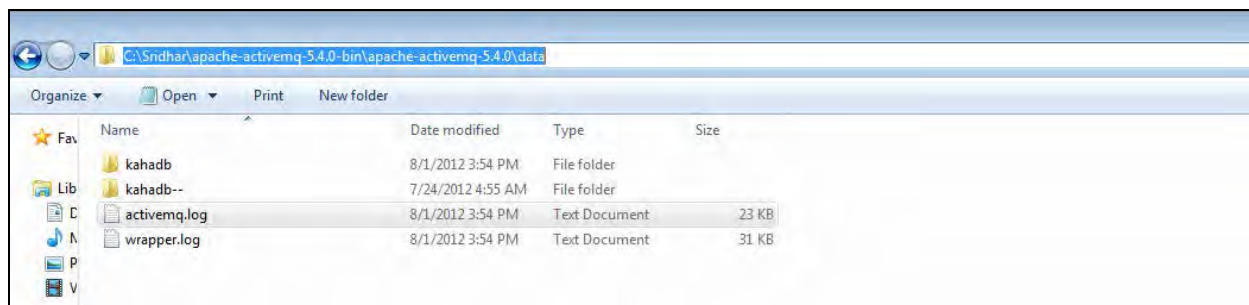
2124

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



2136

2137

Figure 128. Guardian ActiveMQ Home/Data Directory

2138

- 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>`.

2141

2142

### Steps for Failure Case:

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

1. Navigate to the folder `<ActiveMQ home directory>\bin\win32`.
2. Open the `InstallService.bat` file in a local text editor.
3. Modify the bottom part of the script to look like the following. Note that your `JAVA_HOME` environment variable needs to already be set and also need to pass it as a variable to the wrapper.

2146

2147

2148

2149

2150

2151

2152

2153

2154

2155

2156

2157

2158

2159

2160

2161

2162

2163

2164

2165

2166

2167

2168

2169

```
:conf
set WRAPPER_CONF="%ACTIVEMQ_HOME%\bin\win32\wrapper.conf"
set ACTIVEMQ_HOME="set.ACTIVEMQ_HOME=%ACTIVEMQ_HOME%"
set ACTIVEMQ_BASE="set.ACTIVEMQ_BASE=%ACTIVEMQ_BASE%"
set JAVA_HOME="set.JAVA_HOME=%JAVA_HOME%"
rem
rem Install the Wrapper as an NT service.
Rem
:startup
"%ACTIVEMQ_HOME%\bin\win32\wrapper.exe" -i %_WRAPPER_CONF%
%_ACTIVEMQ_HOME% %_ACTIVEMQ_BASE% %_JAVA_HOME%
if not errorlevel 1 goto :eof
pause
```

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

```
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 rem
2181 rem Uninstall the Wrapper as an NT service.
2182 rem
2183 :startup
2184 "%ACTIVEMQ_HOME%\bin\win32\wrapper.exe" -r %_WRAPPER_CONF%
2185 if not error level 1 goto : eof
2186 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

2204

2205

2206

## 2207 Installing Apache Tomcat

2208 You must install hardware and operating system versions specific to Apache Tomcat:

- 2209 1. Double-click the setup launcher to start the setup. It will start the installation process.
- 2210 2. Click Next to start the installation process.
- 2211 3. Click I Agree to accept the license terms. It displays the Choose Components screen.
- 2212 4. Select Custom as install type and uncheck the Examples option.
- 2213 5. Click Next to specify the Destination Folder for installation. We strictly recommend using
- 2214 `D:\AlertEnterprise\Tomcat` location.
- 2215 6. Click Next to specify configuration parameters.
- 2216 7. Enter the desired port in the Connector Port text area. 8080 is the default port.
- 2217 8. Specify the User Name and Password in the respective fields.
- 2218 9. Click Next to select the path of JRE installed on the system.
- 2219 10. Select the path of JDK/JRE you just installed. For example, `C:\Program`
- 2220 `Files\Java\jre1.6`.
- 2221 11. Click Install to start the file copying process. Uncheck Run Apache Tomcat and Show
- 2222 `Readme` options in the final dialog box.
- 2223 12. Click Finish to finish the installation.

2224

## 2225 Apache Tomcat Configuration

2226 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 `/******`

2263 `create or replace`

2264 `trigger set_nls_onlogon`

2265 `AFTER LOGON ON SCHEMA`

2266 `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_CP1_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

2497

<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	Passwrđ Column Name	Mandatory
<input type="checkbox"/>	userIdColumnName	UserId Column Name	Mandatory
<input type="checkbox"/>	EXTERNAL_USER_ID_AT...	External UserId Att...	Mandatory
<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

2498

2499

<input type="checkbox"/>	UNLOCK_USER0	Unlock Card Holder ...	Mandatory
<input type="checkbox"/>	DELIMIT_USER0	Change CardHolder V...	Mandatory
<input type="checkbox"/>	USER_PROVISIONED0	Check Card Holder P...	Mandatory
<input type="checkbox"/>	ADD_ROLES0	Assign Roles to Car...	Mandatory
<input type="checkbox"/>	DEPROVE_ROLES0	Remove Roles From C...	Mandatory
<input type="checkbox"/>	GET_GENERATED_USERI...	Retrieve User Id Qu...	Mandatory
<input type="checkbox"/>	driverName	driverName	Mandatory
<input type="checkbox"/>	url	URL	Mandatory
<input type="checkbox"/>	userName	userName	Mandatory
<input type="checkbox"/>	password	password	Mandatory

2500

2501

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
Skipprovisioning	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:

2533 *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
  - 2538 Modify Role and Allow Time Change.
  - 2539 • Leave Connector Category as Production.
  - 2540 • Time Zone – Eastern Daylight Time from drop-down
- 2541 8. Click on Next.
- 2542 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:

2554 *Table 11. Guardian ACCESSIT PACS Parameters*

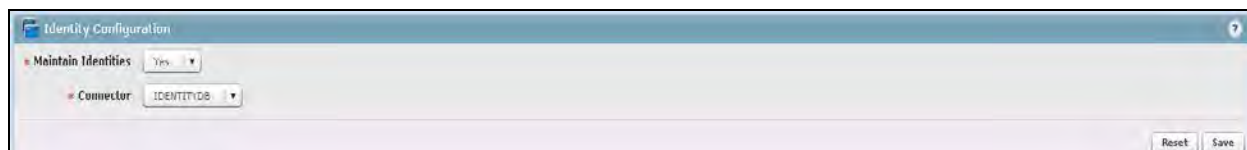
System Param Name	System Param Value
driverName	
URL	jdbc:sqlserver://<HOST_NAME>:<PORT>;databaseName=AI Universal
userName	DB User Name
password	DB User Password
Date and Time Format	CardholderID
External UserId Attribute	CardholderID
Create CardHolder Query	<pre> INSERT INTO [AIUniversal].[dbo].[Cardholders]([CardholderID],[LastName],[FirstName],[MiddleInitial],[C ompanyID],[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],[UserText2 0],[Department],[UserDate1],[UserDate2],[UserDate3],[UserDate4],[UserDate5],[UserNum eric1],[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,\$User Text_19,\$UserText_20,\$Department,\$UserDate1,\$UserDate2,\$UserDate3,\$UserDate4,\$Us erDate5,\$UserNumeric1,\$UserNumeric2,\$UserNumeric3,\$UserNumeric4,\$UserNumeric5,' 1',\$CardholderActiveDate,\$CardholderExpireDate)                     </pre>
Update CardHolder Query	<pre> update [dbo].[Cardholders] set LastModified=GetUTCDate() where CardholderID=\$CardholderID                     </pre>

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','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,")
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
  - Check the following boxes – Provisioning, Role Management, and Offline System.
  - Leave Connector Category as Production.
  - 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

2567

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.
- 2572 Select values for respective fields and hit on save (Refer to below sheet for values
- 2573 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](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	
<input type="checkbox"/>	Authoritative Field
<input type="checkbox"/> Systems	Authoritative Field
<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

2582

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 &gt; Manual Configuration &gt; Policy Engine &gt; 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	NewHireDefaultSyst ems	Systems	ACCESSIT PACS	

2639

2640 **Policy Engine>Rule Action Handler**

2641 1 – Setup &gt; Manual Configuration &gt; Policy Engine &gt; 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		



---

ReconChangeHa ndler	AlertAccess	Recon Create Request	Change Access	0	Yes	No
------------------------	-------------	-------------------------	------------------	---	-----	----

2644

2645 **Policy Engine>Policy Designer**

2646 1. Setup &gt; Manual Configuration &gt; Policy Engine &gt; 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.

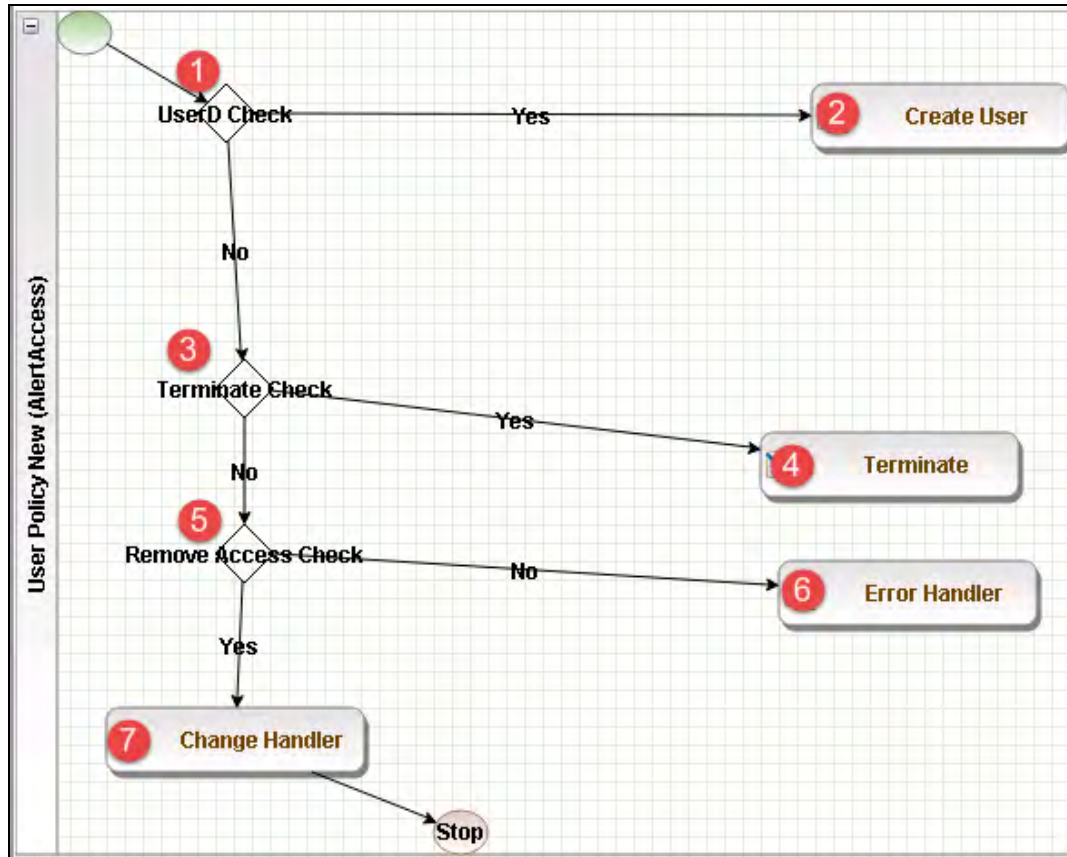


Figure 134. Guardian User Policy

2656

2657

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	userBadg e	userEnt RoleType	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
pacAllDoors	PacsAllDoors	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
pacHomeAccess	PacsHomeAccesses	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
pacWorkAccess	PacsWorkAccess	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE

2670

2671 **Job Scheduler>Triggers**

2672 1. Setup &gt; Manual Configuration &gt; Job Scheduler &gt; 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.

**\* Job Type** Reconciliation Job

**\* Job Name** PACS AD User Reconciliation

**Global**

**Job Visibility** private

**Notification Templates** Choose One

**\* Reconciliation For** Users  
Roles  
User Training

**\* Reconciliation Type** Incremental Reconciliation

**\* Reconciliation Triggers** PACSAD Trigger

**Init Date Load** No

**Create/Update Scheduled Jobs**

Immediate  
 Once  
 Periodically  
 Advance

**Time Zone** (GMT-05:00) America/New\_York

**Start At** 06/08/2015 [date] 20 [hrs] 58 [minutes]

**End At** 06/08/2016 [date] 20 [hrs] 58 [minutes]

**Rerun every** 2 [Repeat Duration] Minutes [Repeat Unit]

Save Cancel

Figure 135. Guardian Reconciliation Job

2688

2689

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
userName	userName
password	password
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	Passwrld Column Name	Mandatory
<input type="checkbox"/>	userIdColumnName	UserId Column Name	Mandatory
<input type="checkbox"/>	EXTERNAL_USER_ID_AT...	External UserId Att...	Mandatory
<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

2713

2714



<input type="checkbox"/>	UNLOCK_USER0	Unlock Card Holder ...	Mandatory
<input type="checkbox"/>	DELIMIT_USER0	Change CardHolder V...	Mandatory
<input type="checkbox"/>	USER_PROVISIONED0	Check Card Holder P...	Mandatory
<input type="checkbox"/>	ADD_ROLES0	Assign Roles to Car...	Mandatory
<input type="checkbox"/>	DEPROVE_ROLES0	Remove Roles From C...	Mandatory
<input type="checkbox"/>	GET_GENERATED_USERI...	Retrieve User Id Qu...	Mandatory

2715

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_USERSO	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 &gt; Manual Configuration &gt; Systems &gt; 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	jdbc:sqlserver://<HOST_NAME>:<PORT>;databaseName=AI Universal  <HOST_NAME> should be replaced with the hostname of the RS2 PACS system
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	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(),'alertnt',GetUTCDate(),'alertnt','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)
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,")
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

2800

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

2803

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

2804

Table 23. PacsHomeAccess Attributes

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

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.

2821

Figure 137. Create DropDownValues

- 2822 5. Similarly configure values for Contractor field, Figure 138.

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

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.

Figure 139. DropDownValues

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

Figure 140. InActive

2832

2833

2834

2835 5. Similarly configure values for **InActive** field, Figure 1402836 6. Click **Save** and then Click **Save** to save the configuration

2837 7. Ignore this step if these values already exists for Status field

2838 **Identity & Access– Enable Identity**

2839 1. Setup &gt; Manual Configuration &gt; Identity &amp; Access &gt; Enable Identity

2840 2. Enable the following for Identity DB system as shown in Figure 141.

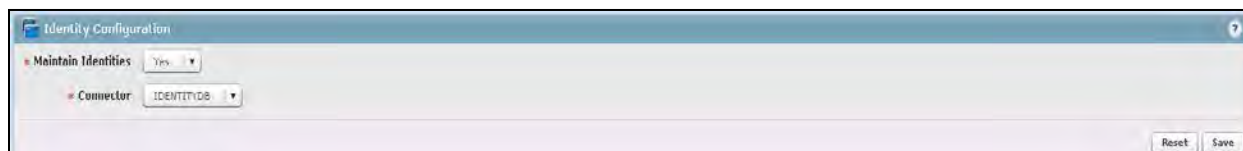


Figure 141. Guardian Identity Configuration

2841

2842

2843 9.4.4 **Identity & Access– User Field Mapping**

2844 1. Setup &gt; Manual Configuration &gt; Identity &amp; Access &gt; User Field Mapping.

2845 2. Select User = Identity (from drop-down) and click Go.

2846 3. Click the Create New button.

2847 4. Select Custom Field, Primary Key, Visible In List, IsSearchable fields based on the table  
2848 listed below. Select checkbox for these fields if it is specified as “Yes” otherwise, keep it  
2849 as unselected.

2850 5. Click on Save button to save the record

2851 6. Repeat Steps 1–5 for all fields in the following table, Table 27. Ignore fields if pre-existing  
2852 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 &gt; Manual Configuration &gt; Identity &amp; Access &gt; 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

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

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  
2871 a. In the Provisioning Actions section Un select Delimit user and Change Validity  
2872 Dates check boxes if they are selected  
2873 b. Go to Add Existing section and select System and Remove Role option for  
2874 Resources/Roles Drop down field  
2875 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 has two input fields: "Name" and "Description", both containing the text "LastName". Below the fields are two buttons: "Cancel" and "Save".

2883

2884 *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**

- 2893 1. Setup > Manual Configuration > Identity & Access > Provisioning > Provisioning Mapping.
- 2894 2. Select ACCESSIT PACS and click on **Configure**.
- 2895 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:

Buttons: Cancel, Save

2896

2897

Figure 146. Provisioning Mapping

2898 4. Click on Save button to save the mapping

2899 5. Repeat the steps 1-4 to configure other fields as shown in Figure 140.

<input type="checkbox"/>	DB Connector Attribute	Mandatory	AlertEnterprise Attrib...	Default Value	Editable	Visible	Validati...	Is User...
<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

Buttons: Cancel, New, Modify, Delete

2900

2901

Figure 147. Guardian DB Connector Attribute Mapping

2902 **Policy Engine> Rules**

2903 1. Setup > Manual Configuration > Policy Engine > Rules

2904 2. Click New Button

2905 3. On the Next screen provide following information. See Figure 148.



**Define Rules**

\* **Rule Name** All Door Access New

**Entity Type**  Workflow  Entity

**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

Next Cancel

2906

2907

Figure 148. Policy Rules

2908

4. Click **Next** Button

2909

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

2910

**Define Condition**

If PacsAllDoors equals True and

Request Category equals NewHire

Add Cancel

2911

2912

Figure 149. Rule Conditions

2913

2914

6. Repeat the step 5 to define rule condition for other request categories Remove User Access and ChangeAccess as shown in Figure 150.

2915

<input type="checkbox"/>	If	<b>PacsAllDoors</b>	and	<b>Request Category</b>
<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

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

2920

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

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

2925

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

2926

The screenshot shows a configuration form with the following fields and values:

- \* Name:** All Door Access
- \* Type:** Default
- Description:** All Door Access
- \* Condition:** All Door Access New
- Use identity old values:**
- Provisioning Action:**
- Search By Role Attributes:**
- Search by Systems:**
- Search by Training Roles:**
- Search by Training Attributes:**
- Search by Enterprise Roles:**

At the bottom of the form are three buttons: **Cancel**, **Back**, and **Next**.

Figure 151. Default Access

- 2927
- 2928
- 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
NewHireDefaultSystems	Default	NewHireDefaultSystems	Yes (Select check box)	ACCESSIT PACS	

2943

2944

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

2945

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 list as shown in Figure 152.

2951

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 &gt; Manual Configuration &gt; Policy Engine &gt; 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

\* Name User Policy New

\* Rule Type AlertAccess

Description User Policy New

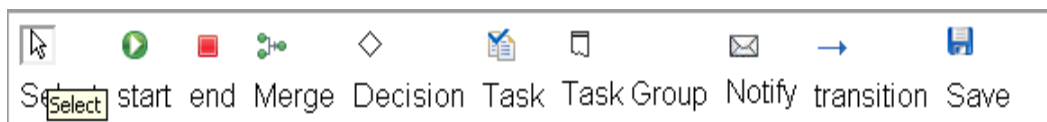
Back Next Cancel

2963

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



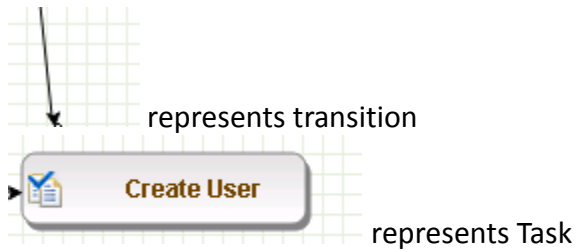
2971

2972 *Figure 154. Toolbar*

2973

2974  represents Start button2975  represents End Button2976  represents Decision

2977



2978

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 it.

2982

2983

- b. To connect two nodes, select transition icon from tool bar and then mouse over to the first node and connect to the other node in the same direction specified in the Figure 23)

2984

2985

2986

- c. To provide text for a Decision or Task or Line, double click on the corresponding node and enter the text. Hit Enter after that to come out of the edit mode.

2987

2988

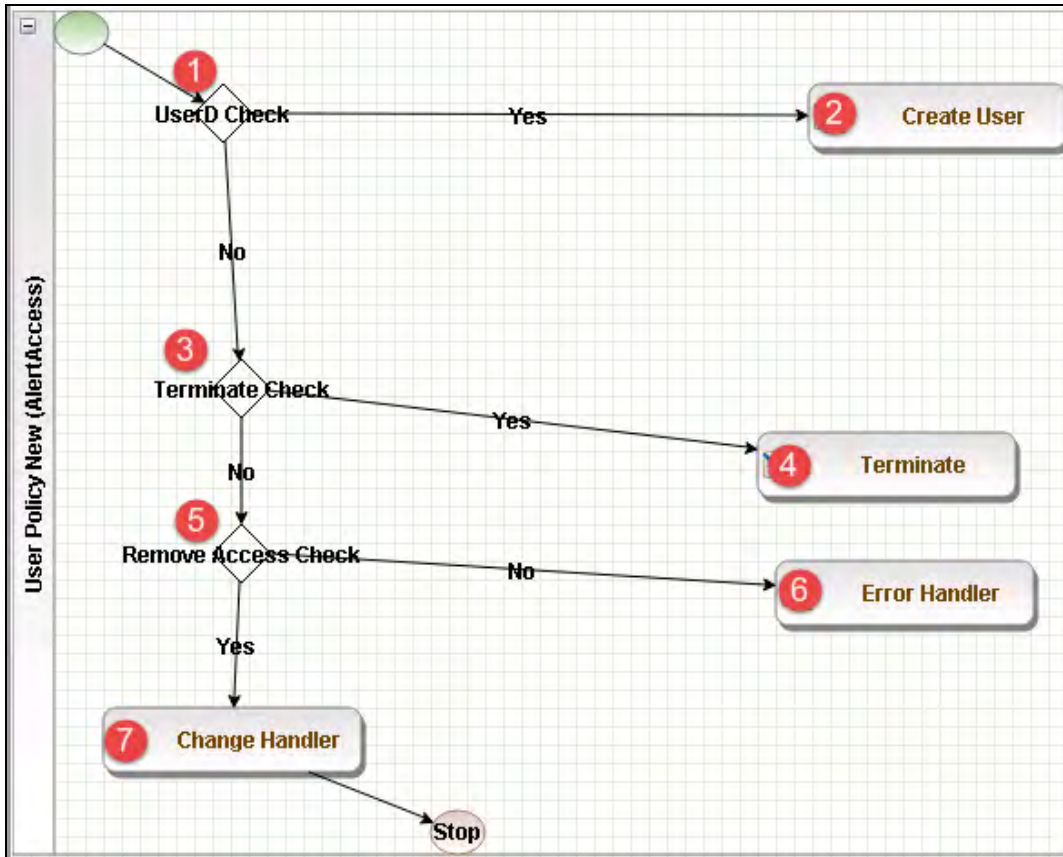


Figure 155. Guardian User Policy

2989

2990

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

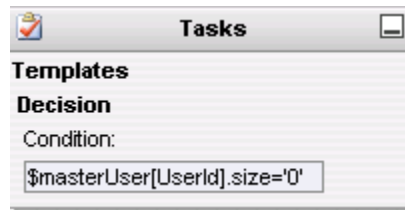


Figure 156. Tasks Popup

2994

2995

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	Terminate Check	Decision	\$checkStatus[UserStatus,Active,Inactive].action='LOCK'			
4	Terminate	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 &gt; Manual Configuration &gt; Job Scheduler &gt; 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
  - 3034 frequency.

**\* Job Type** Reconciliation Job

**\* Job Name** Alert External DB User Reconciliation

**Global**

**Job Visibility** private

**Notification Templates** Choose One

**\* Reconciliation For** Users  
Roles  
User Training

**\* Reconciliation Type** Incremental Reconciliation

**\* Reconciliation Triggers** AlertDbConnectorTrigger

**Init Date Load** No

**Create/Update Scheduled Jobs**

Immediate  
 Once  
 Periodically  
 Advance

**Time Zone** (GMT-05:00) America/New\_York

**Start At** 06/08/2015 [date] 20 [hrs] 58 [minutes]

**End At** 06/08/2016 [date] 20 [hrs] 58 [minutes]

**Rerun every** 2 [Repeat Duration] Minutes [Repeat Unit]

Save Cancel

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 CONSLEWORKS 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](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.

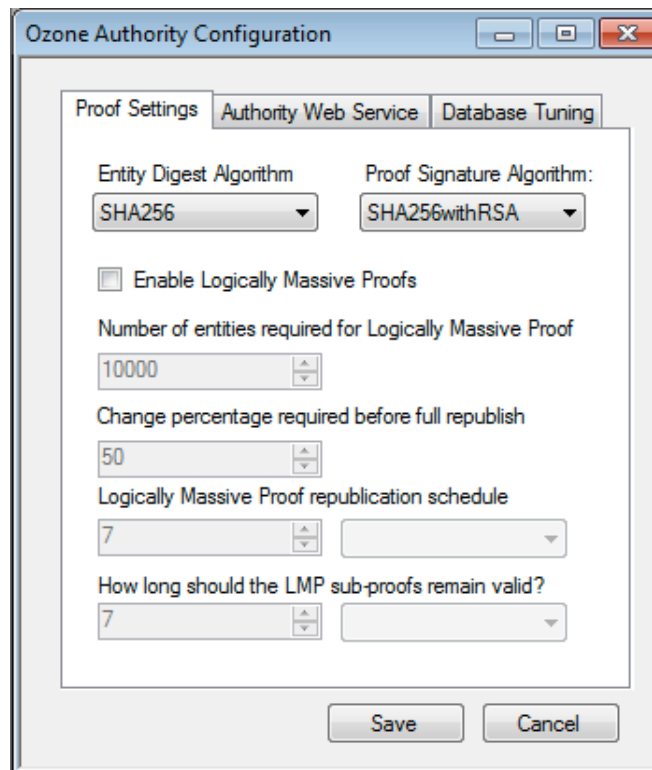


Figure 158. Ozone Proof Settings

- 3291  
 3292  
 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.

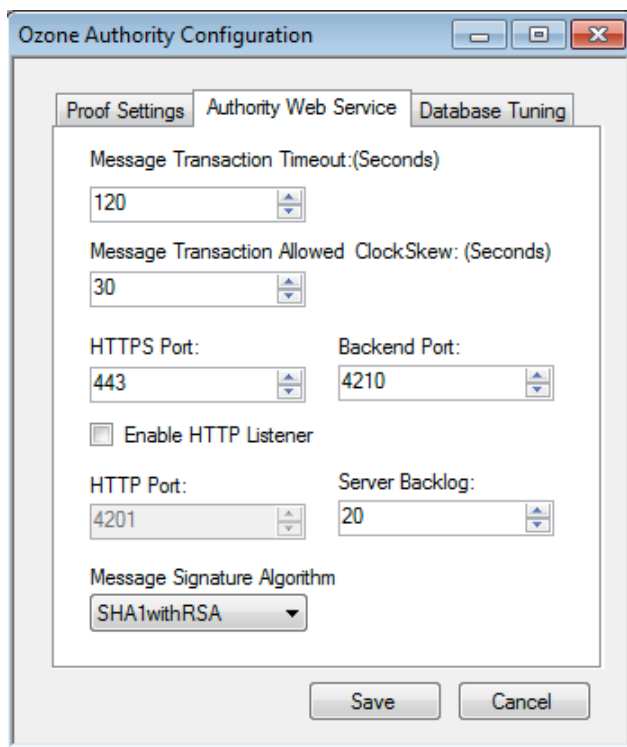


Figure 159. Ozone Authority Web Service

- 3296
- 3297
- 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/kestores/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 localhost.localdomain
3497 localhost4 localhost4.localdomain4
3498
3499 Configure the directory server
3500 [root@ozone ~]# setup-ds.pl
3501
3502 =====
3503 =
3504 This program will set up the 389 Directory Server.
3505
3506 It is recommended that you have "root" privilege to set up the software.
3507 Tips for using this program:
3508 - Press "Enter" to choose the default and go to the next screen
3509 - Type "Control-B" or the word "back" then "Enter" to go back to the
3510 previous screen
3511 - Type "Control-C" to cancel the setup program
3512
3513 Would you like to continue with set up? [yes]: yes
3514
3515 =====
3516 =
3517 Your system has been scanned for potential problems, missing patches,
3518 etc. The following output is a report of the items found that need to
3519 be addressed before running this software in a production
3520 environment.
3521
3522 389 Directory Server system tuning analysis version 23-FEBRUARY-2012.
3523
3524 NOTICE : System is x86_64-unknown-linux3.8.13-68.2.2.el7uek.x86_64 (1
3525 processor).
3526
3527 NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds
3528 (120 minutes). This may cause temporary server congestion from lost
3529 client connections.
3530
3531 WARNING: There are only 1024 file descriptors (soft limit) available, which
3532 limit the number of simultaneous connections.
3533
3534 WARNING : The warning messages above should be reviewed before proceeding.
3535
3536 Would you like to continue? [no]: yes
3537
3538 =====
```



```
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 =
3560 Enter the fully qualified domain name of the computer
3561 on which you're setting up server software. Using the form
3562 <hostname>.<domainname>
3563 Example: eros.example.com.
3564
3565 To accept the default shown in brackets, press the Enter key.
3566
3567 Warning: This step may take a few minutes if your DNS servers
3568 cannot be reached or if DNS is not configured correctly. If
3569 you would rather not wait, hit Ctrl-C and run this program again
3570 with the following command line option to specify the hostname:
3571
3572 General.FullMachineName=your.hostname.domain.name
3573
3574 Computer name [ozone.mountaireygroup.com]: ozoneauthority.nccoe.test
3575
3576 =====
3577 =
3578 The server must run as a specific user in a specific group.
3579 It is strongly recommended that this user should have no privileges
3580 on the computer (i.e. a non-root user). The setup procedure
3581 will give this user/group some permissions in specific paths/files
3582 to perform server-specific operations.
3583
3584 If you have not yet created a user and group for the server,
3585 create this user and group using your native operating
3586 system utilities.
3587
3588 System User [nobody]: nobody
3589 System Group [nobody]: nobody
3590
3591 =====
3592 =
3593 The standard directory server network port number is 389. However, if
3594 you are not logged as the superuser, or port 389 is in use, the
3595 default value will be a random unused port number greater than 1024.
```

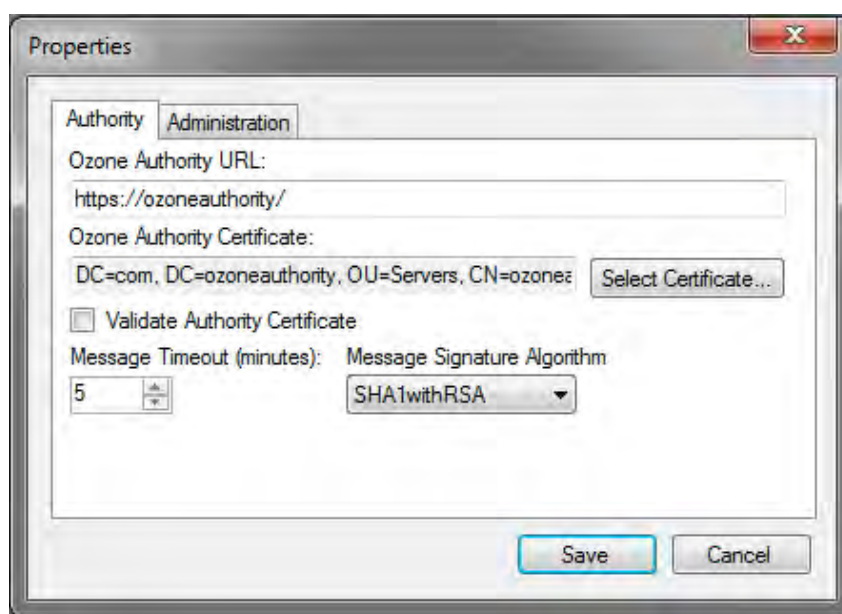
```
3596 If you want to use port 389, make sure that you are logged in as the
3597 superuser, that port 389 is not in use.
3598
3599 Directory server network port [389]: 389
3600
3601 =====
3602 =
3603 Each instance of a directory server requires a unique identifier.
3604 This identifier is used to name the various
3605 instance specific files and directories in the file system,
3606 as well as for other uses as a server instance identifier.
3607
3608 Directory server identifier [ozoneauthority]: ozoneauthority
3609
3610 =====
3611 =
3612 The suffix is the root of your directory tree. The suffix must be a valid DN.
3613 It is recommended that you use the dc=domaincomponent suffix convention.
3614 For example, if your domain is example.com,
3615 you should use dc=example,dc=com for your suffix.
3616 Setup will create this initial suffix for you,
3617 but you may have more than one suffix.
3618 Use the directory server utilities to create additional suffixes.
3619
3620 Suffix [dc=nccoe, dc=test]: dc=nccoe, dc=test
3621
3622 =====
3623 =
3624 Certain directory server operations require an administrative user.
3625 This user is referred to as the Directory Manager and typically has a
3626 bind Distinguished Name (DN) of cn=Directory Manager.
3627 You will also be prompted for the password for this user. The password must
3628 be at least 8 characters long, and contain no spaces.
3629 Press Control-B or type the word "back", then Enter to back up and start
3630 over.
3631
3632 Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
3633 Password: password
3634 Password (confirm): password
3635 Your new DS instance 'ozoneauthority' was successfully created.
3636 Exiting . . .
3637 Log file is '/tmp/setup_C4mdK.log'
3638
3639 Setup the directory structure
3640 Modify the file /usr/local/authority/bin/389SetupDirectory.ldif
3641 Set the correct DN structure and passwords for the ozone authority user and tree
3642 [root@ozone bin]# vi 389SetupDirectory.ldif
3643 [root@ozone bin]# cat 389SetupDirectory.ldif
3644
3645 #Create the User for Ozone Authority
3646 dn: uid=ozone, ou=Special Users, dc=nccoe, dc=test
3647 changetype: add
3648 objectClass: inetorgperson
3649 objectClass: organizationalPerson
3650 objectClass: person
3651 objectClass: top
```

```
3652 cn: Ozone Authority
3653 sn: Authority
3654 givenName: Ozone
3655 uid: ozone
3656 userPassword: P@$sword
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.

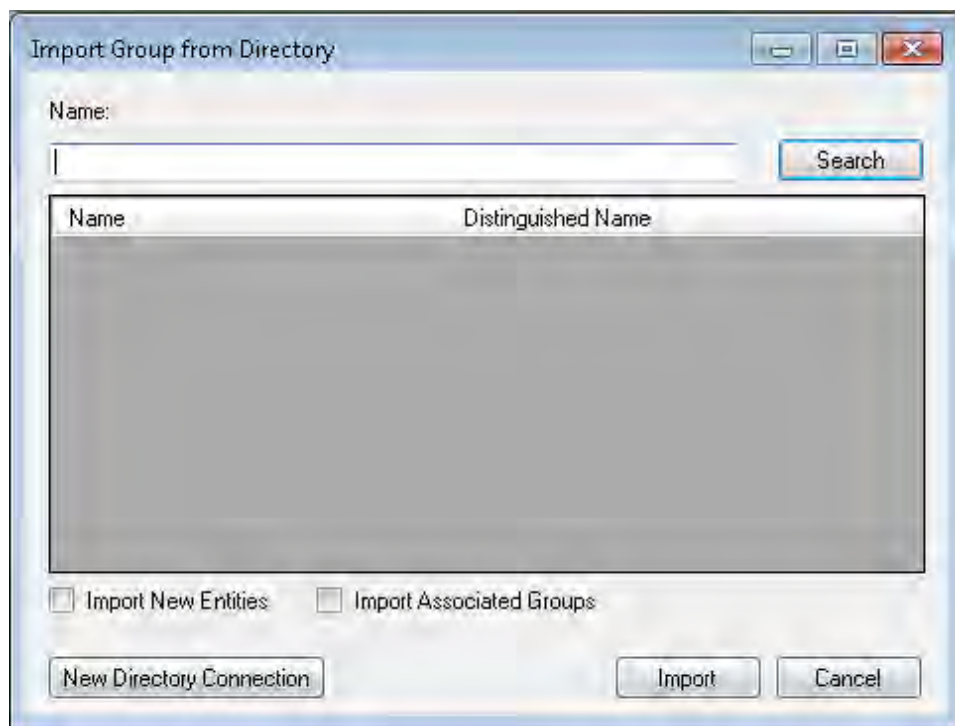
3733

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

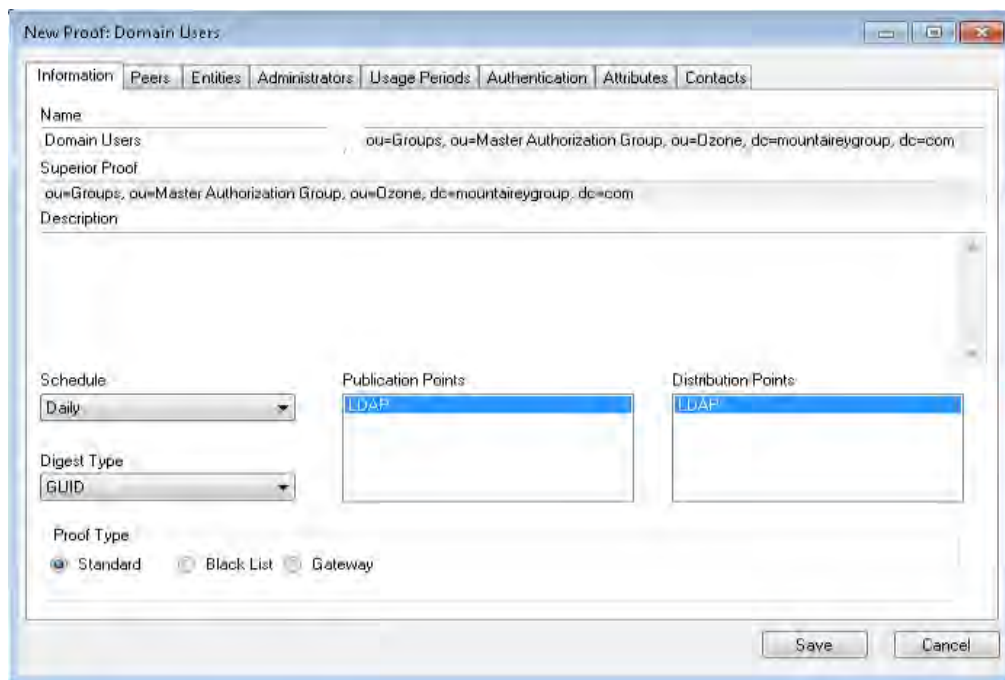


3739

3740

*Figure 163. Ozone Import Group from Directory*

- 3741 8. Select the publication schedule as shown in Figure 164.  
3742 9. Select the publication point as shown in Figure 164.  
3743 10. Select the distribution point as shown in Figure 164.



3744

3745

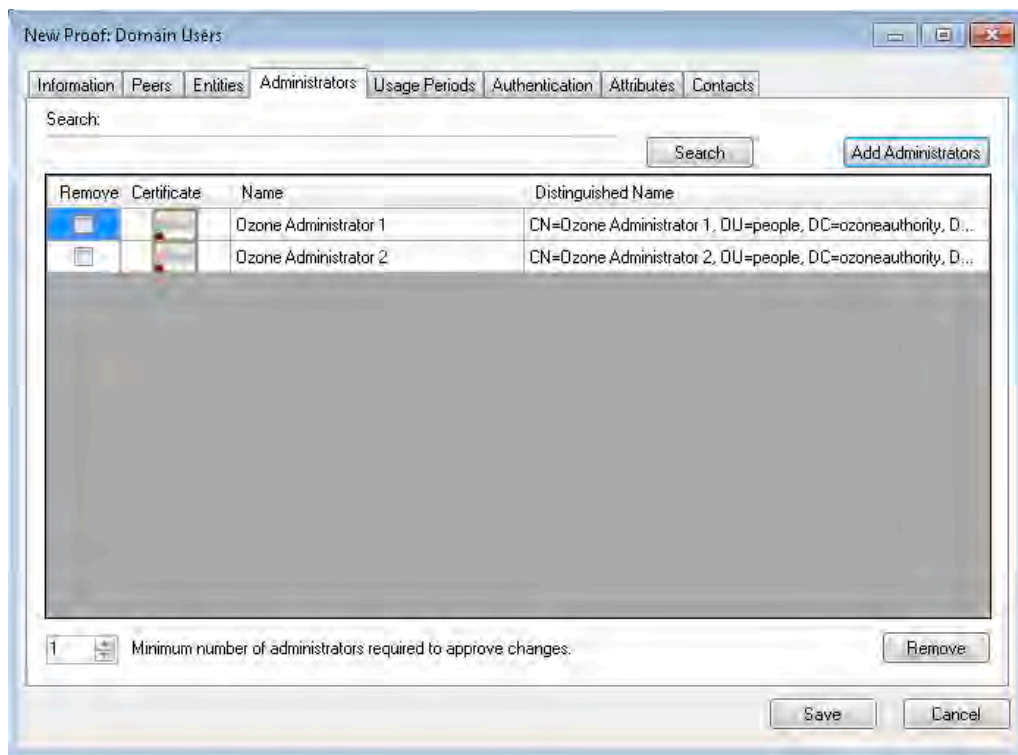
Figure 164. Ozone New Proof Information

3746 11. Click the Administrators tab as shown in Figure 165

3747 12. Click the Add Administrators button.

3748 13. Select the users who will administer the proof.

3749 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.



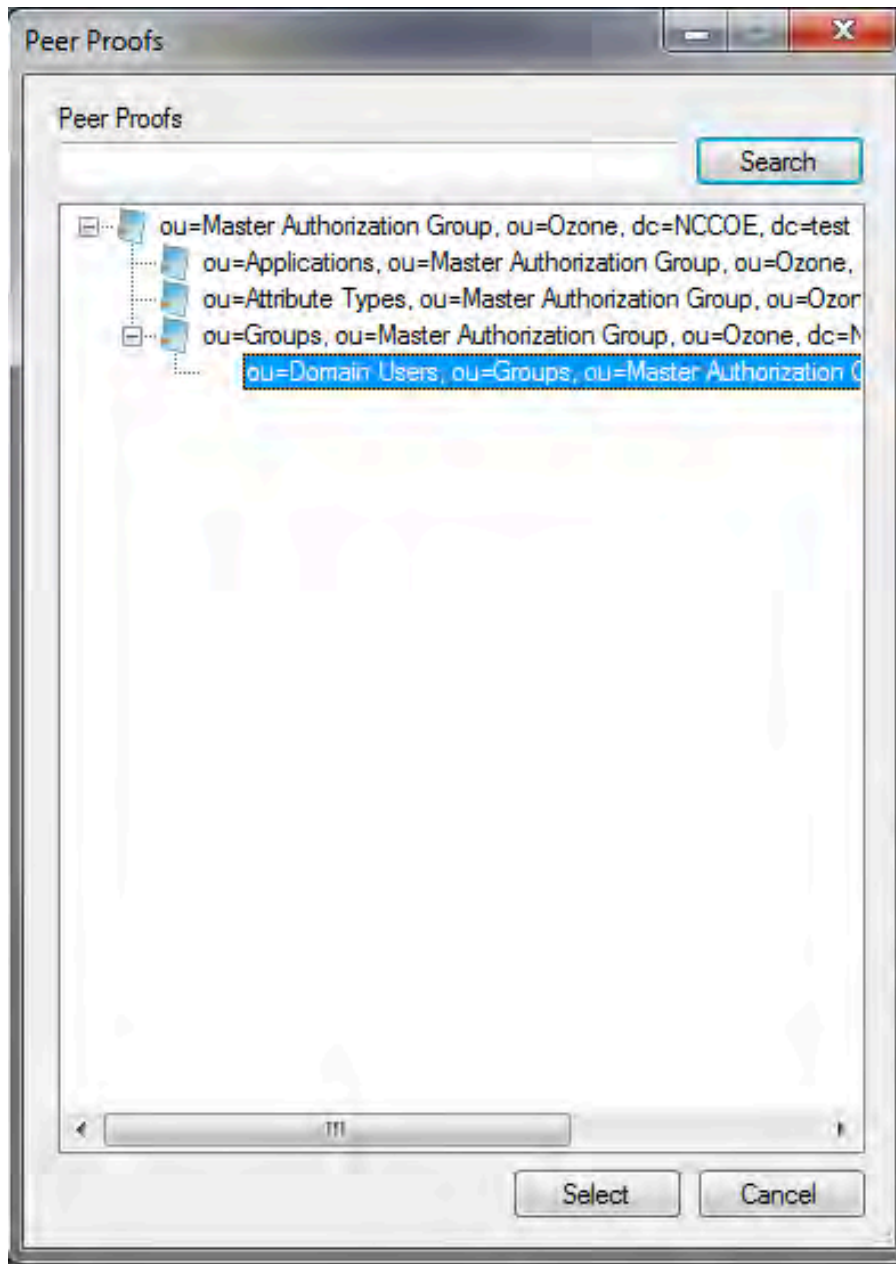


Figure 166. Ozone Peer Proofs

3758

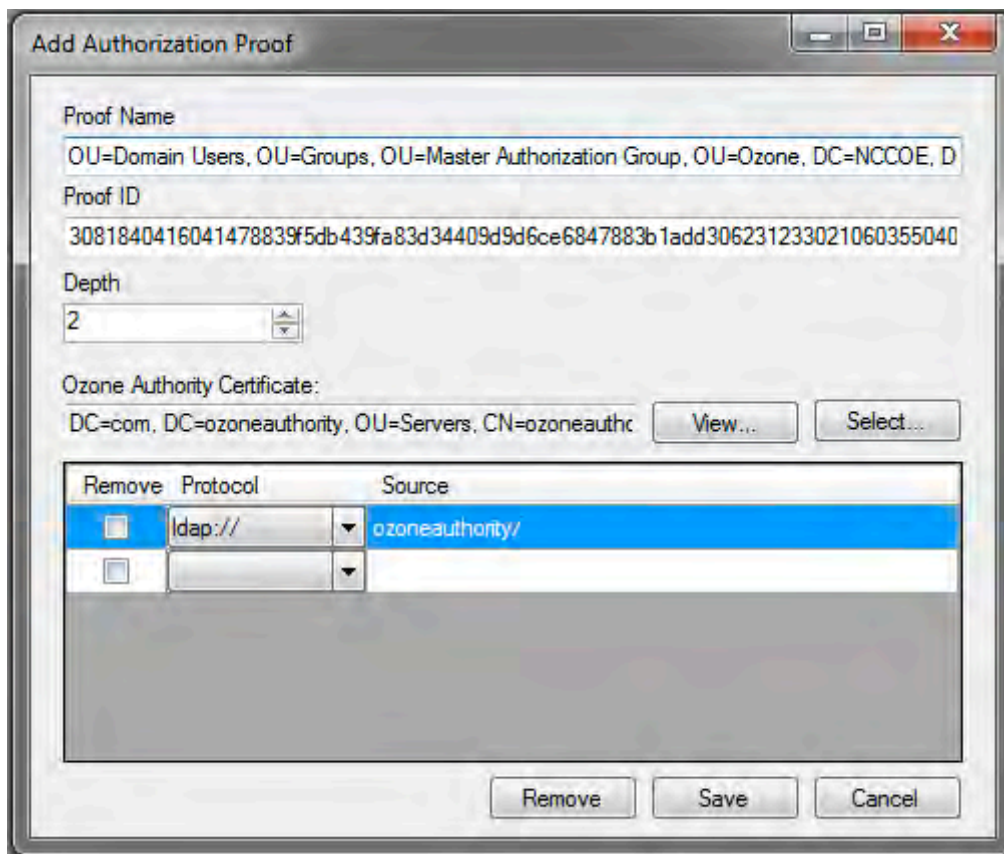
3759

3760

3761

3762

4. Set the number of proof references (Depth) the proof may follow in order to authorize a credential as shown in Figure 167.
5. Ensure that the locations where the Ozone Server will retrieve the proof are correct.



3763

3764

*Figure 167. Ozone Add Authorization Proof*

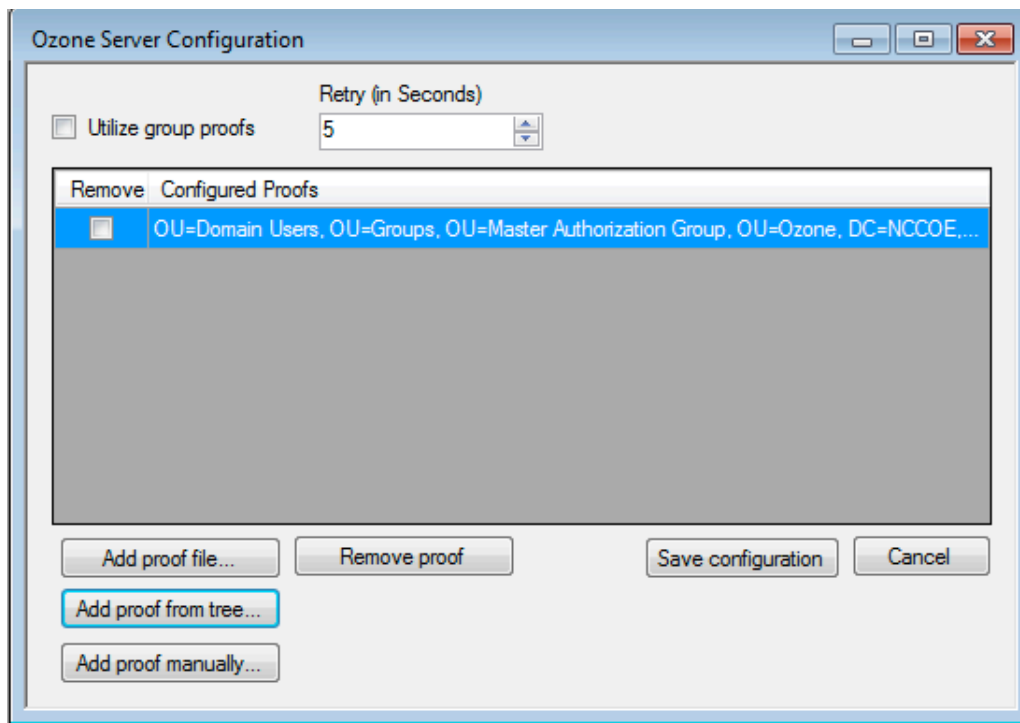
3765

6. Click the Save button.

3766

7. Repeat Steps 2–6 until you have selected all of the proofs Ozone Server should initially retrieve for Authorizations.

3767



3768

3769

Figure 168. Ozone Server Configuration

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

##### Install java

```
[root@ozone ~]# yum install java
```

3779

##### Install Ozone Server

```
[root@ozoneserver ~]# cd /usr/local/
```

```
[root@ozoneserver local]# tar -xzf ~/Ozone\ Server-2014.tar.gz
```

3783

##### Copy the keystore to the conf directory

```
[root@ozoneserver local]# mkdir /usr/local/server/bin/conf/
```

```
[root@ozoneserver local]# cp ~/server.jks server/bin/conf/
```

3787

##### Copy the configuration and license files to the conf directory

```
[root@ozoneserver local]# cp ~/ServerConfiguration.xml server/bin/conf/
```

```
[root@ozoneserver local]# cp ~/ServerLicense.xml server/bin/conf/
```

3791

3792 **Run the Ozone Server**

3793 [root@ozoneserver 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 =&gt; 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 #####
3955 ### This keystore is used for:
```

```

3956 ### - Authenticating with Ozone Authority
3957 ### - Secure log signing
3958 system/identity/store=envoy.jks
3959
3960 ##### Authority Listener Configuration
3961 ### This web service endpoint listens for push configuration and fetch
3962 requests
3963 ### from Ozone Authority. It should match what you entered in Ozone Console
3964
3965 #authority/host.name=
3966 authority/port=4242
3967 authority/path=/
3968 authority/mode=ANY
3969
3970 ### Authority Web Service Endpoint Logging
3971 authority/log/enable=true
3972 authority/log/path=var/log
3973 authority/log/rollsize=10485760
3974 authority/log/format=CLF
3975
3976 #####
3977 ##### Enrollment Configuration #####
3978 #####
3979
3980 ### Enable enrollment
3981 enroll/enable=false
3982
3983 Run Ozone Envoy to complete the setup
3984 [root@ozoneenvoy bin]# ./startEnvoy.sh
3985
3986 May 15, 2015 3:09:04 PM
3987 com.pericore.util.ObjectIdentifierFactory$OIDDataLoader debug
3988 INFO: ObjectIdentifierFactory Read 240.165 kb in 14.366 ms; Indexed 2,415
3989 Arcs in 63.198 ms; 2,310(1,054:5) keys => 2.003 kb
3990 May 15, 2015 3:09:06 PM com.pericore.util.PericoreProvider jsafeJCEinit
3991 POST: [FIPS] FIPS-140 compliance self-test passed.
3992
3993 /_/_ _/_ //_/_ _/_ |_/_ |_/_ |_/_ |_/_ (R)
3994 | / \ | / / | / \ | | \ \ | | |
3995 | | | | / / | | | | | | \ \ | | | |
3996 | | | | / / | | | | | | \ \ | | | |
3997 | | | | / / | | | | | | \ \ | | | |
3998 \ _/_ / // /_/_ \ _/_ / // | \ \ | | |
3999 _/_ //_/_ _/_ / | | _/_ |
4000
4001 |_/_ |
4002 | |_/_ |
4003 | |_/_ | | \ \ / / |_/_ | | | |
4004 | |_/_ | | | \ V / () | | | |
4005 |_/_ | | | | _/_ / _/_ , |
4006 |_/_ / |
4007 2014 Mobile Edition |_/_ /
4008
4009 Ozone(R) Envoy copyright (c) Pericore, Inc. 2007-2014
4010 -----
4011

```

```
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).



The screenshot shows a window titled "New Proof: Domain Certificates" with several tabs: Information, Peers, Entities, Administrators, Usage Periods, Authentication, Attributes, and Contacts. The "Information" tab is selected. The "Name" field contains "Domain Certificates" and the "Superior Proof" field contains "ou=Applications, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test". The "Description" field is empty. The "Schedule" dropdown is set to "Primary Schedule". The "Digest Type" dropdown is set to "Certificate". The "Proof Type" radio buttons are set to "Standard". The "Publication Points" list contains "Ozone Authority LDAP" and the "Distribution Points" list contains "LDAP Distribution Point". "Save" and "Cancel" buttons are at the bottom right.

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.

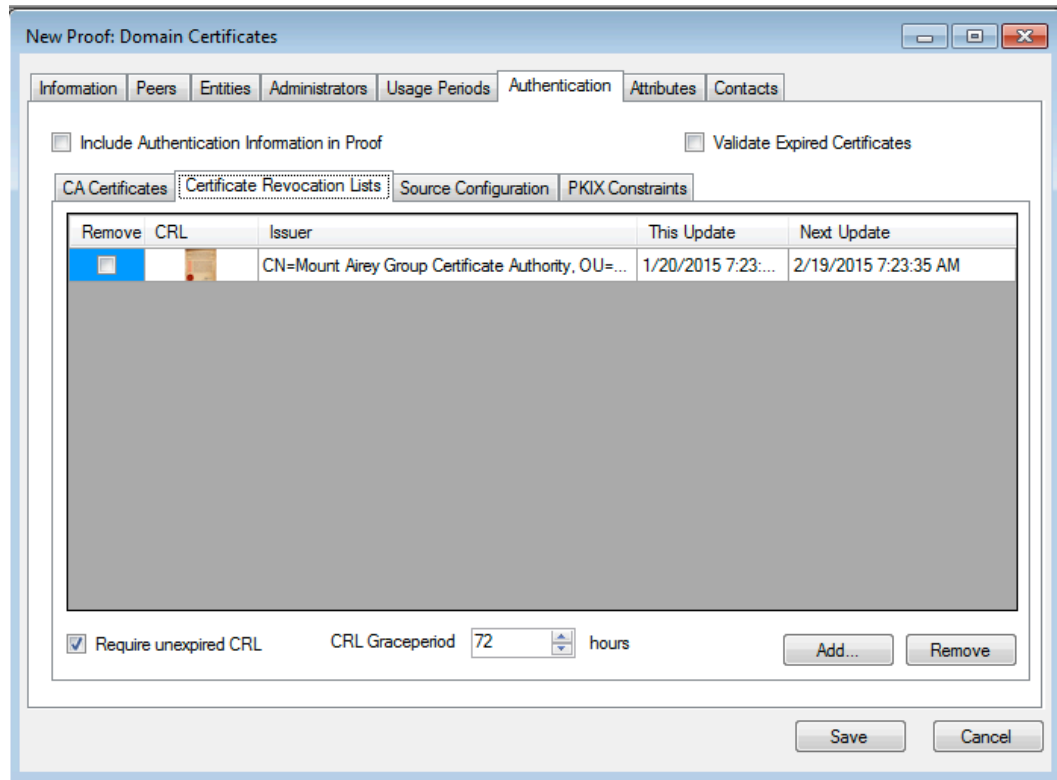
4051

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.



4054

4055

Figure 170. Ozone New Proof Authentication CRLs

4056

16. Select the Source Configuration tab as shown in Figure 171.

4057

17. Enter hostname or IP address of the LDAP server.

4058

18. Enter the port the LDAP server is listening on.

4059

19. Check the box for LDAPS.

4060

20. Enter the base context of where user certificates can be obtained.

4061

21. Enter the attributeName for the certificates, either userCertificate or

4062

userCertificate;binary

4063

22. Enter the base context of where updated CRLs can be obtained.

4064

23. Enter the attributeName for the CRLs, typically certificateRevocationList shown in Figure

4065

156.

4066

24. Enter the connection information:

4067

- If connecting anonymously, check the box for anonymous connections.

4068

- If a username/password is required for the connection, enter them.

4069

25. Enter the number of hours after which Ozone Envoy should check the directory for new

4070

certificates.

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
- 4080 check for new information.
- 4081 5. Enter the number of minutes to before attempting to reconnect to Ozone Envoy if the
- 4082 connection fails.
- 4083 6. Click Save.

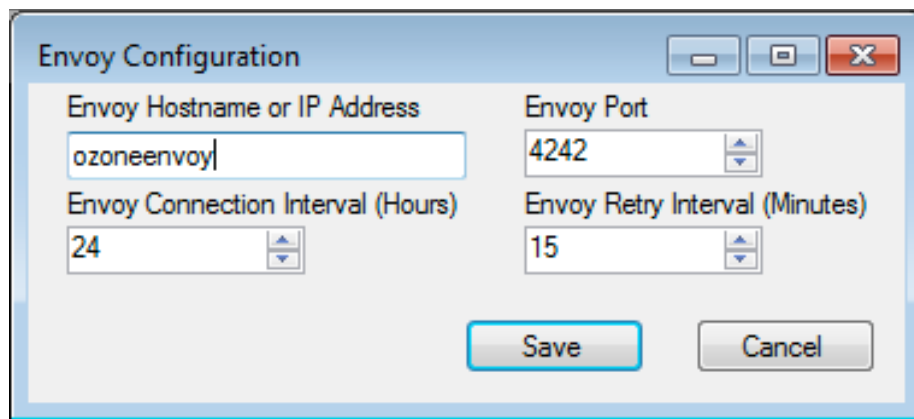


Figure 172. Ozone Envoy Configuration

4084

4085

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.

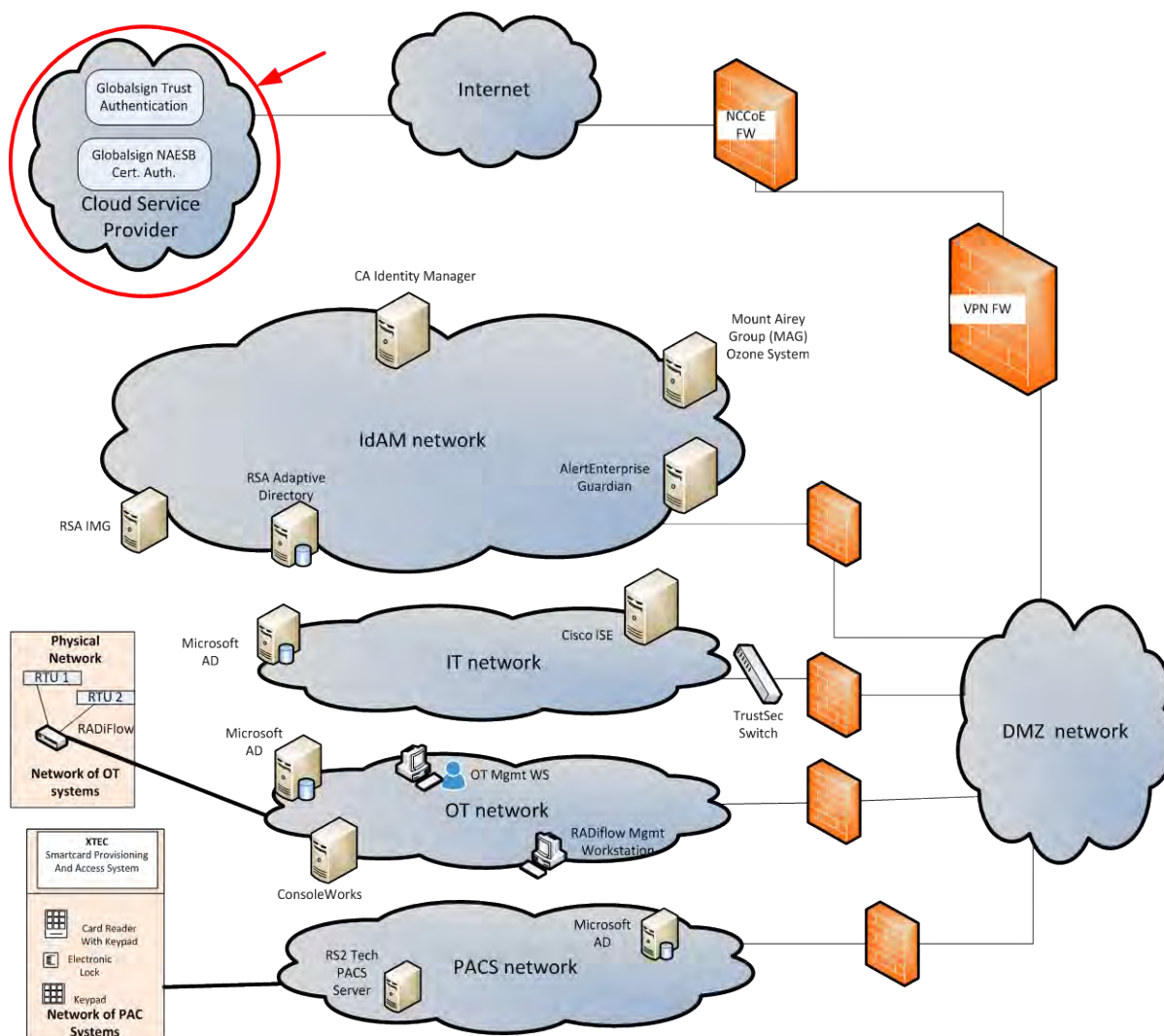


Figure 173. GlobalSign Overview

4107

4108

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 \(CA\)](https://www.naesb.org/).  
 4114 For more information about NAESB, go to <https://www.naesb.org/>.

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.

#### 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

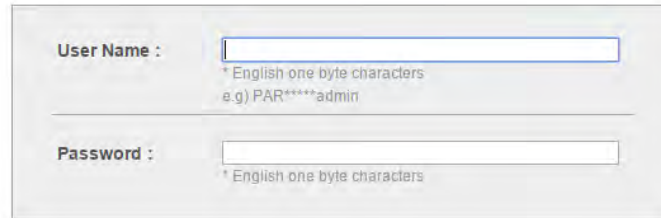
#### 4142 15.3.1 Step 1: Get a GlobalSign Gcc Account

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/](http://www.globalsign.com/en/login/). See Figure 174.

## Ordering Certificates from GlobalSign is Quick & Easy



User Name :   
 \* English one byte characters  
 e.g) PAR\*\*\*\*\*admin

Password :   
 \* English one byte characters

Figure 174. GlobalSign Login Page

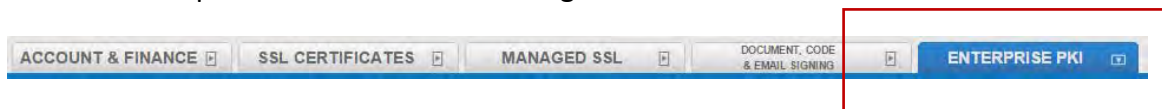
4148

4149

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.



4161

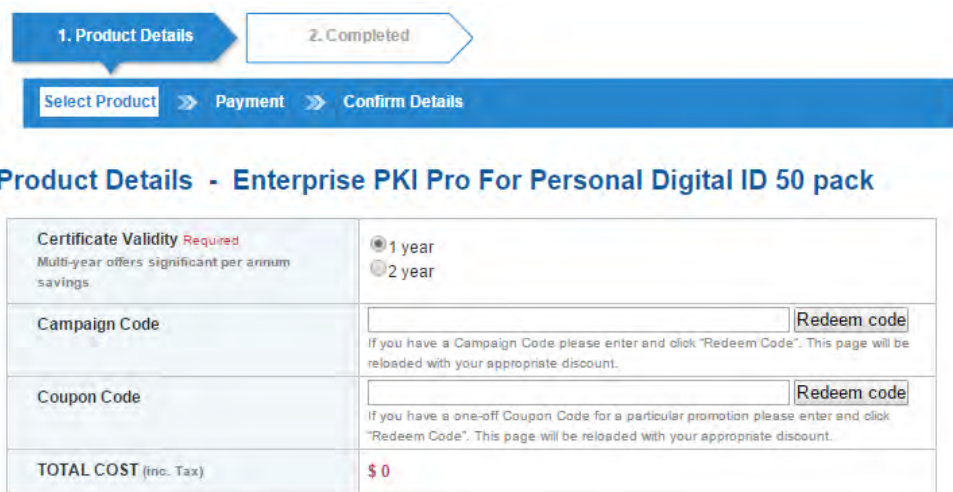
4162

Figure 177. GlobalSign License Selection Page

4163

4164 Choose your validity period (1 or 2 year certificate), see Figure 178.

4165

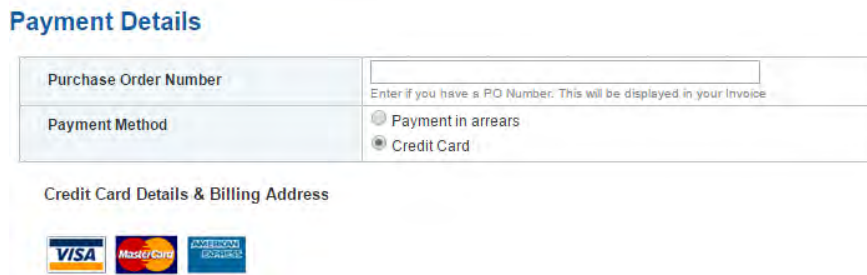


4166

4167

Figure 178. GlobalSign Product Details

4168 Provide payment details as shown in Figure 179.



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.

4174

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 web interface. At the top, there are navigation tabs: ACCOUNT & FINANCE, SSL CERTIFICATES, MANAGED SSL, DOCUMENT, CODE & EMAIL SIGNING, and ENTERPRISE PKI. Below the tabs, the left navigation menu is visible, with 'Order Additional Profiles' highlighted in red. The main content area shows 'Enterprise PKI - Home' with four icons: Find Licenses, Configure Profile, Manage Portal, and Edit Email Templates.

4177

4178

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'.

<b>Organization</b> <small>Required</small>	<input type="text" value="Your company legal name"/>
<b>Organizational Unit</b> <small>Optional unless locked as unique</small>	<input type="text"/> <input type="text"/> <input type="checkbox"/> Lock a unique OU
<b>Locality</b> <small>Optional</small>	<input type="text"/>
<b>State or Province</b> <small>Optional</small>	<input type="text"/>
<b>Country</b> <small>Required</small>	United States - US ▼
<b>Assurance Level</b>	<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

GlobalSign ePKI Service Agreement - Version 2.4

4191

4192

Figure 183. GlobalSign Confirm Details

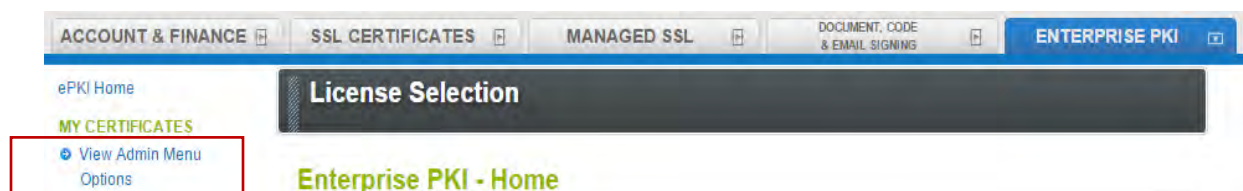
#### 4193 15.3.4 Step 4: Vetting

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

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.

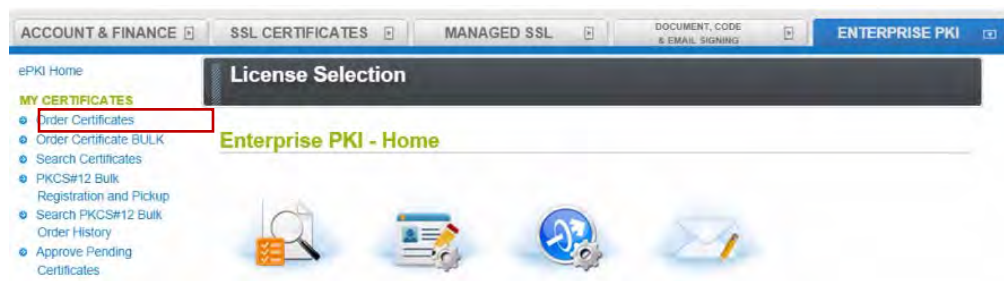
4209 Please follow the guide [http://www.globalsign.com/support/ordering-guides/epki-](http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf)  
4210 [authentication-user-guide.pdf](http://www.globalsign.com/support/ordering-guides/epki-authentication-user-guide.pdf) for 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.

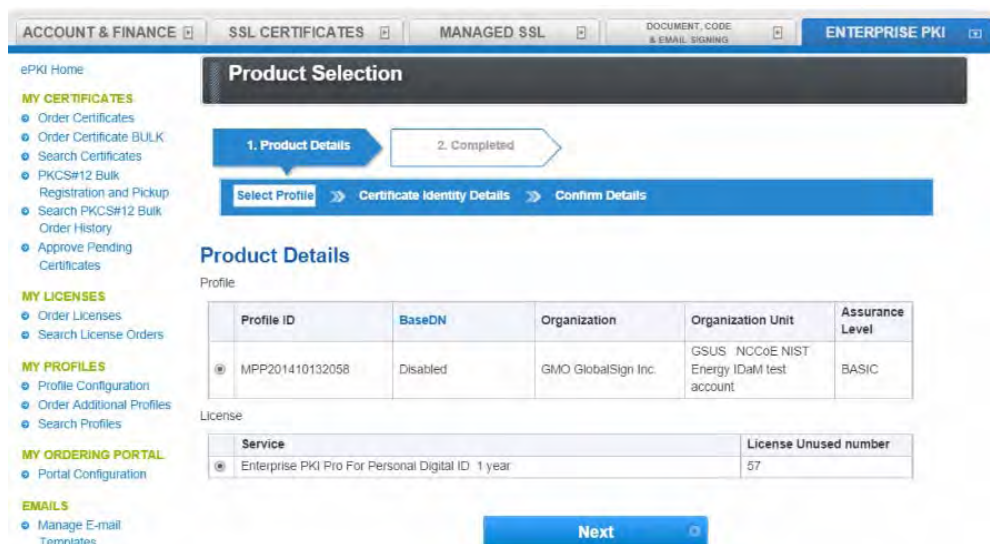


4222

4223

Figure 185. GlobalSign Oder 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

<b>Common Name</b> <small>Required</small>	<input type="text"/>
<b>Organization</b>	GMO GlobalSign Inc.
<b>Organizational Unit (Profile)</b>	GSUS NCCoE NIST Energy IDaM test account
<b>Organizational Unit</b>	<input type="text"/>
<b>Locality</b>	Portsmouth
<b>State or Province</b>	NH
<b>Country</b>	United States - US
<b>Email Address</b> <small>Required</small>	<input type="text"/>

Option certificate delivery method - Select only 1

<b>I have an externally generated CSR</b> Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR)	<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](mailto:support@globalsign.com) or 1-877-467-7543 with specific  
4252 questions.

## 4253 16 INDUSTRIAL FIREWALL: SCHNEIDER ELECTRIC

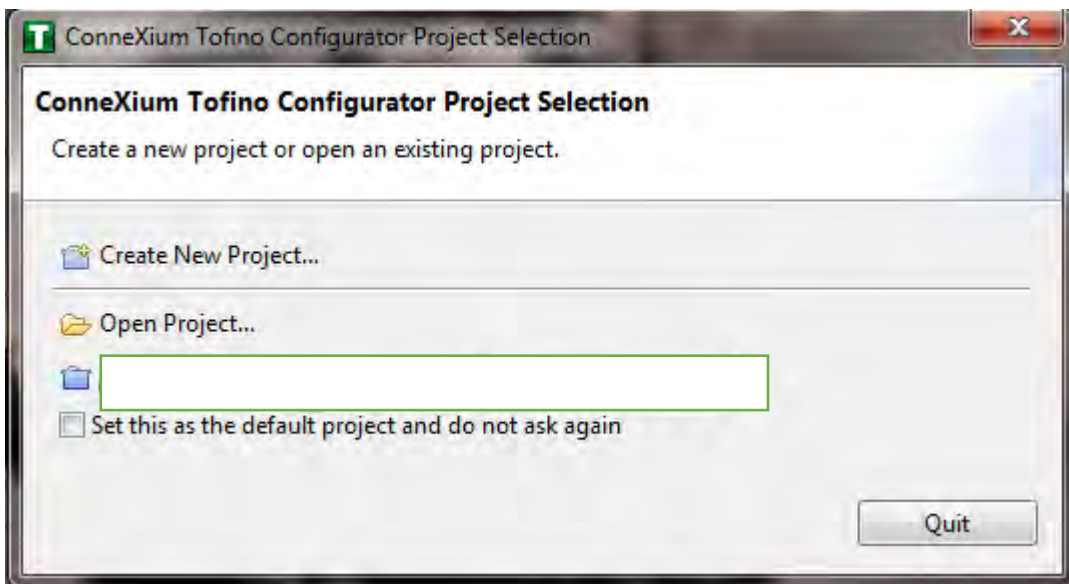
4254 A Schneider Electric (SE) industrial firewall is installed on the physical network that contains the  
4255 industrial control system/SCADA components that can be accessed and controlled via the OT  
4256 network. The firewall is configured to monitor the data passing between the RADiFlow SCADA

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.

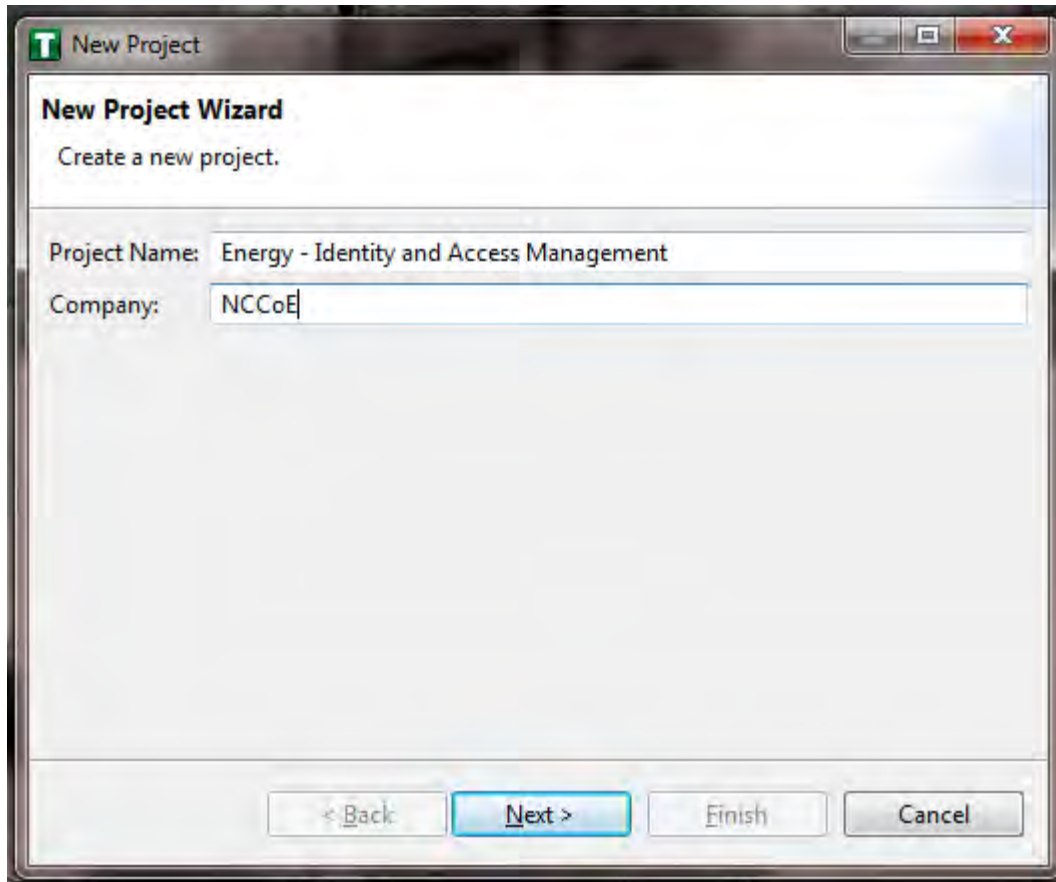


4264

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

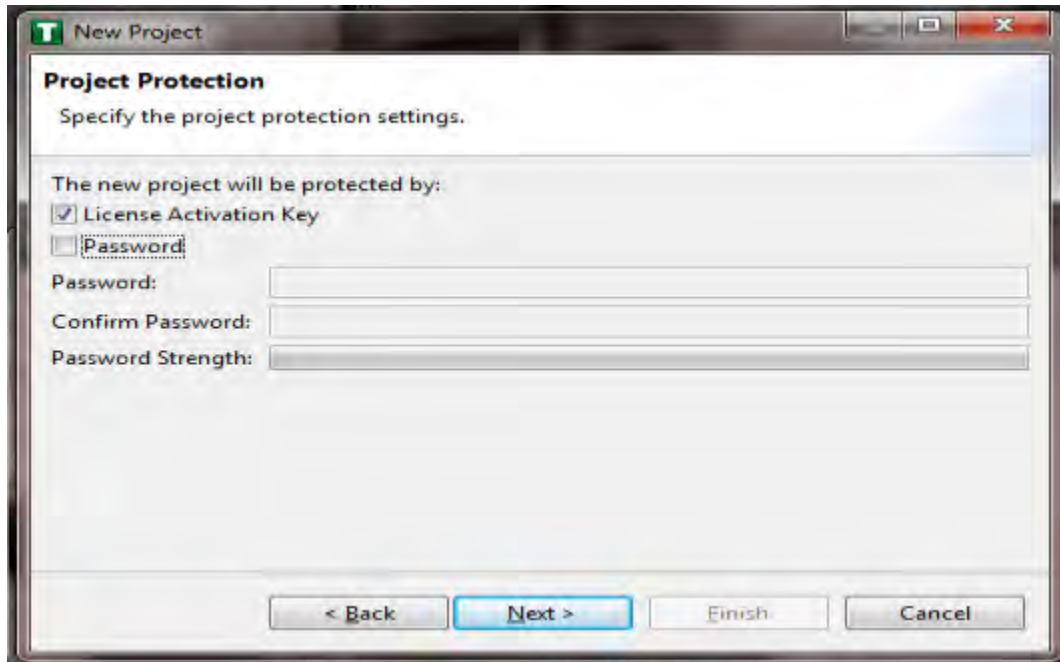
Figure 190. New Project Wizard

4270

4. In the Project Protection screen, Figure 191, choose a password to protect the project. Then click Next.

4271





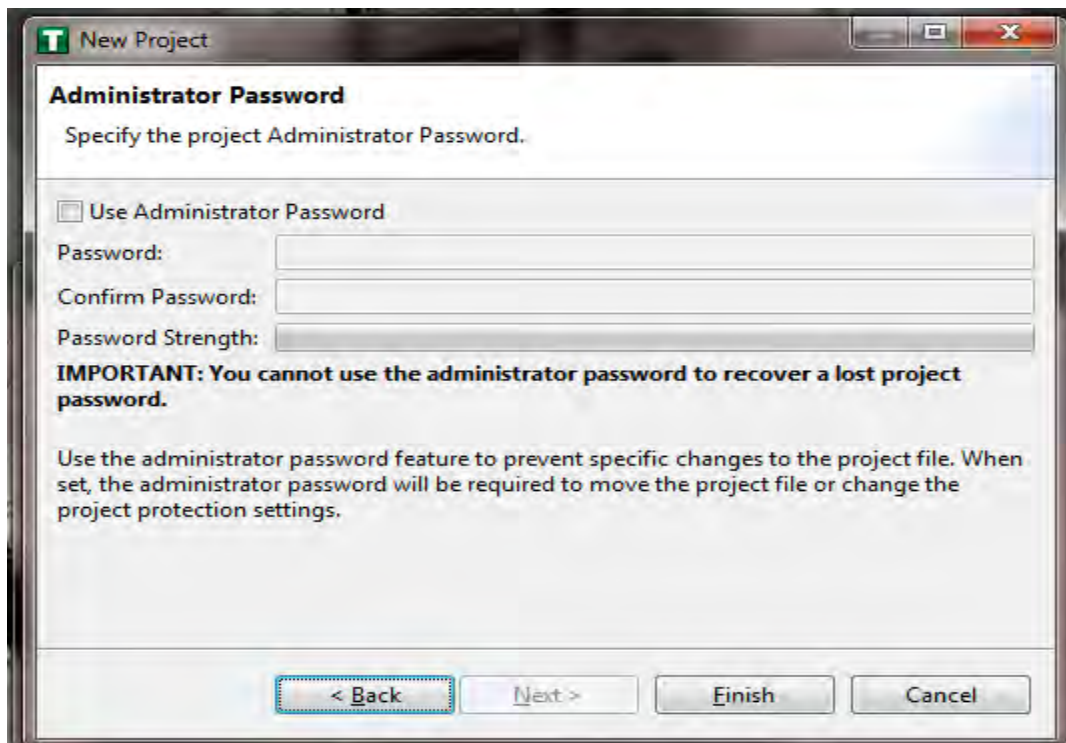
4272

4273

4274

Figure 191. Project Protection

In the Administrator Password screen,



4275

5. Figure 192, choose the administrator password. Then click Finish.

4276

4277

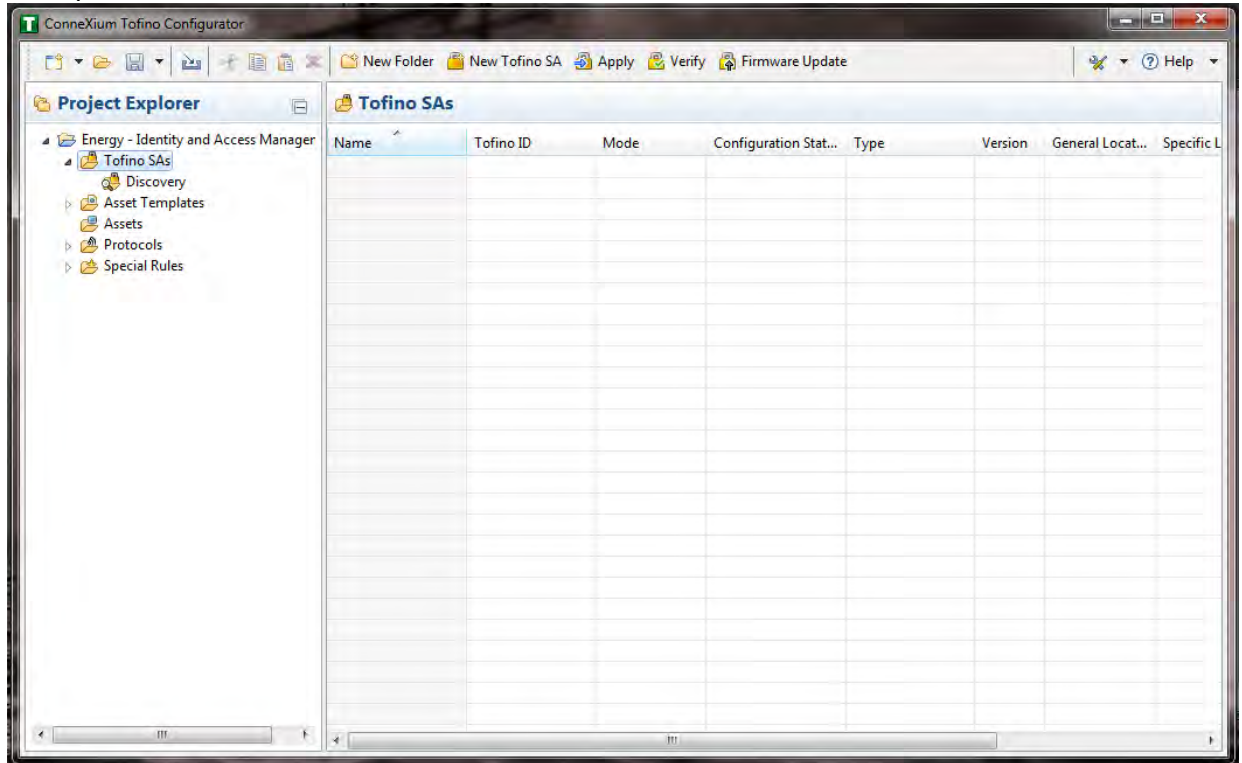
Figure 192. Administrator Password

4278

6. In the Project Explorer Window, Figure 193, right click 'Tofino SAs' and select 'New Tofino SA'. \*Note: You can also chose to create a folder for the SAs to help organize multiple areas.

4279

4280



4281

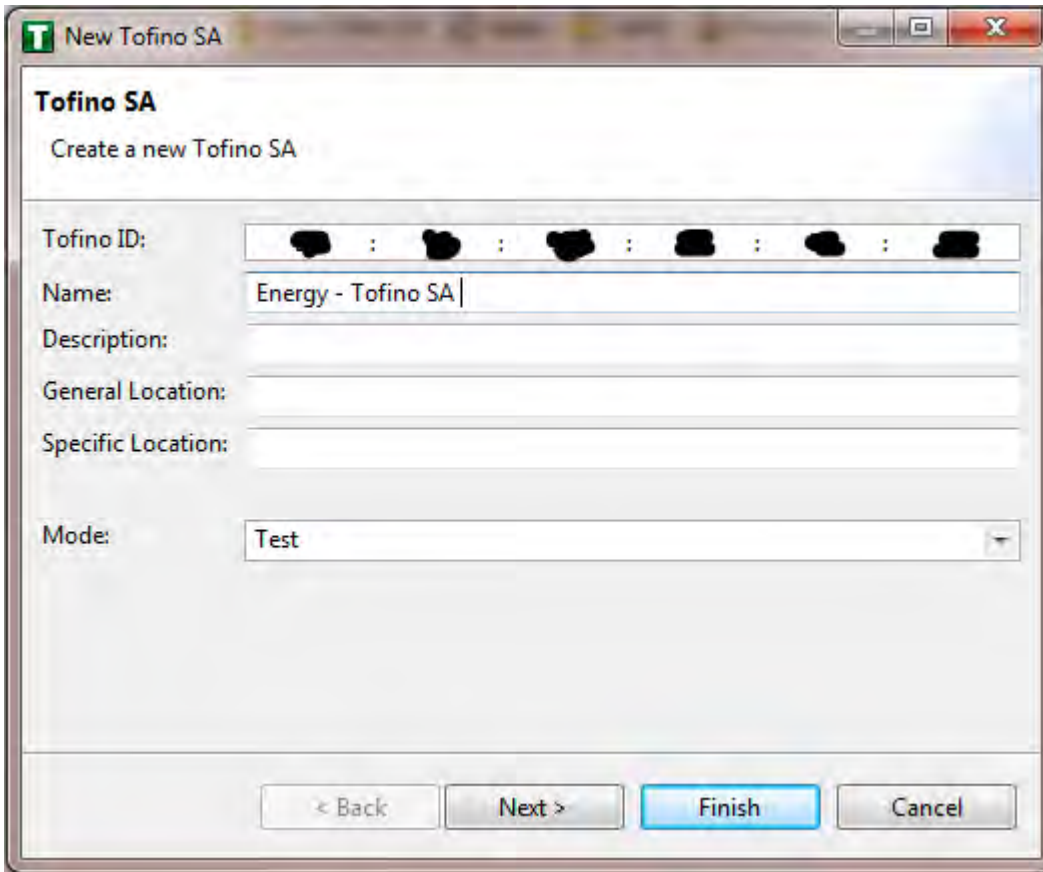
4282

Figure 193. Project Explorer Window

4283

7. In the Tofino ID field, Figure 194, enter the MAC address listed on the firewall hardware 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.'

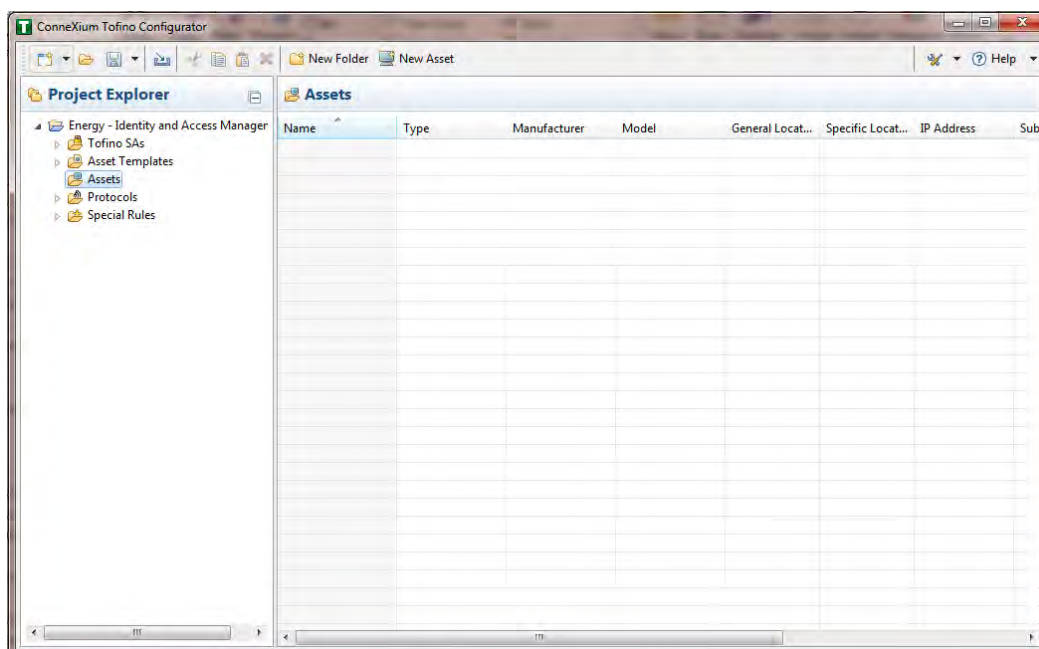
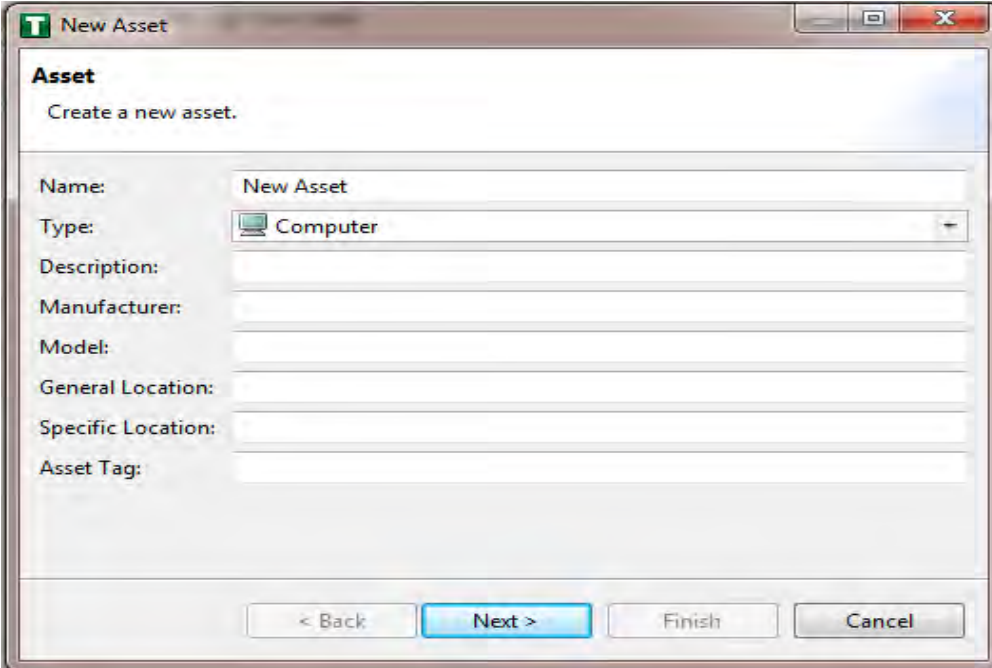


Figure 195.  
Project  
Explorer

- 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.



The image shows a software dialog box titled "New Asset". The dialog has a title bar with standard Windows window controls. Below the title bar, the text "Asset" is displayed in bold, followed by "Create a new asset." The main area of the dialog contains several input fields: "Name:" with the text "New Asset", "Type:" with a dropdown menu showing "Computer", "Description:", "Manufacturer:", "Model:", "General Location:", "Specific Location:", and "Asset Tag:". At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

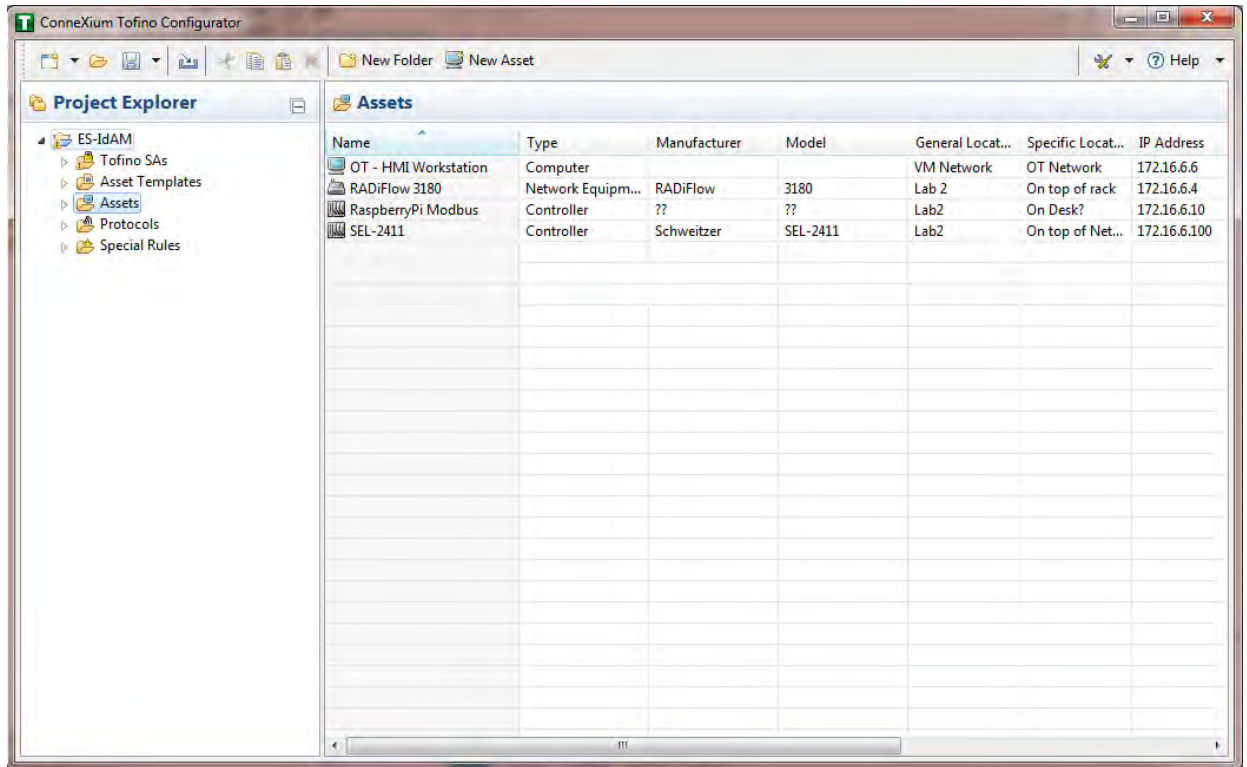
4295

4296

4297

Figure 196. New Asset

- 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.

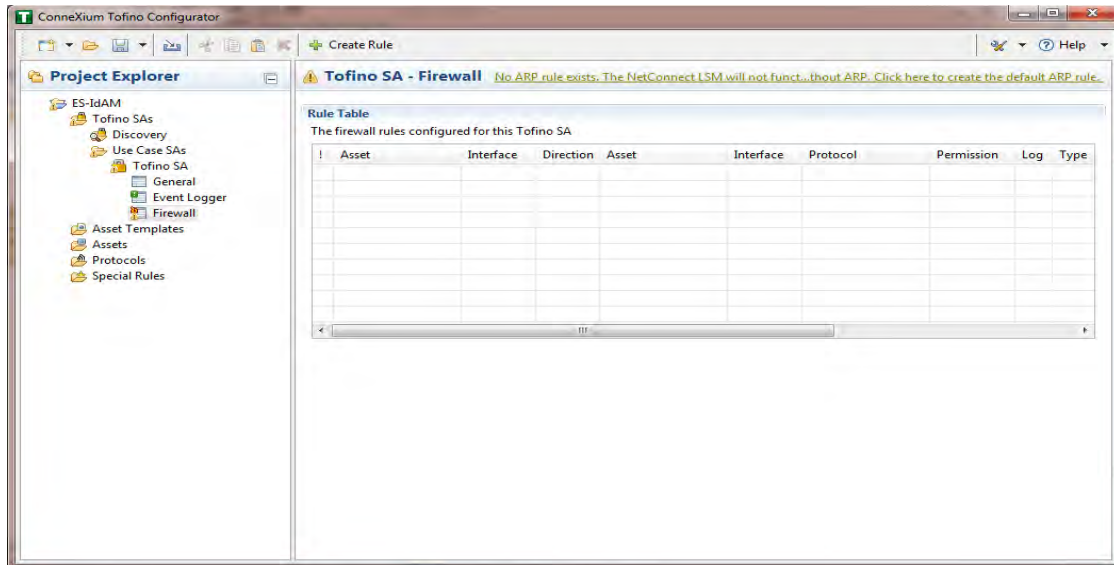


4302

4303

Figure 197. Project Explorer Assets Icon

- 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

4309

4310

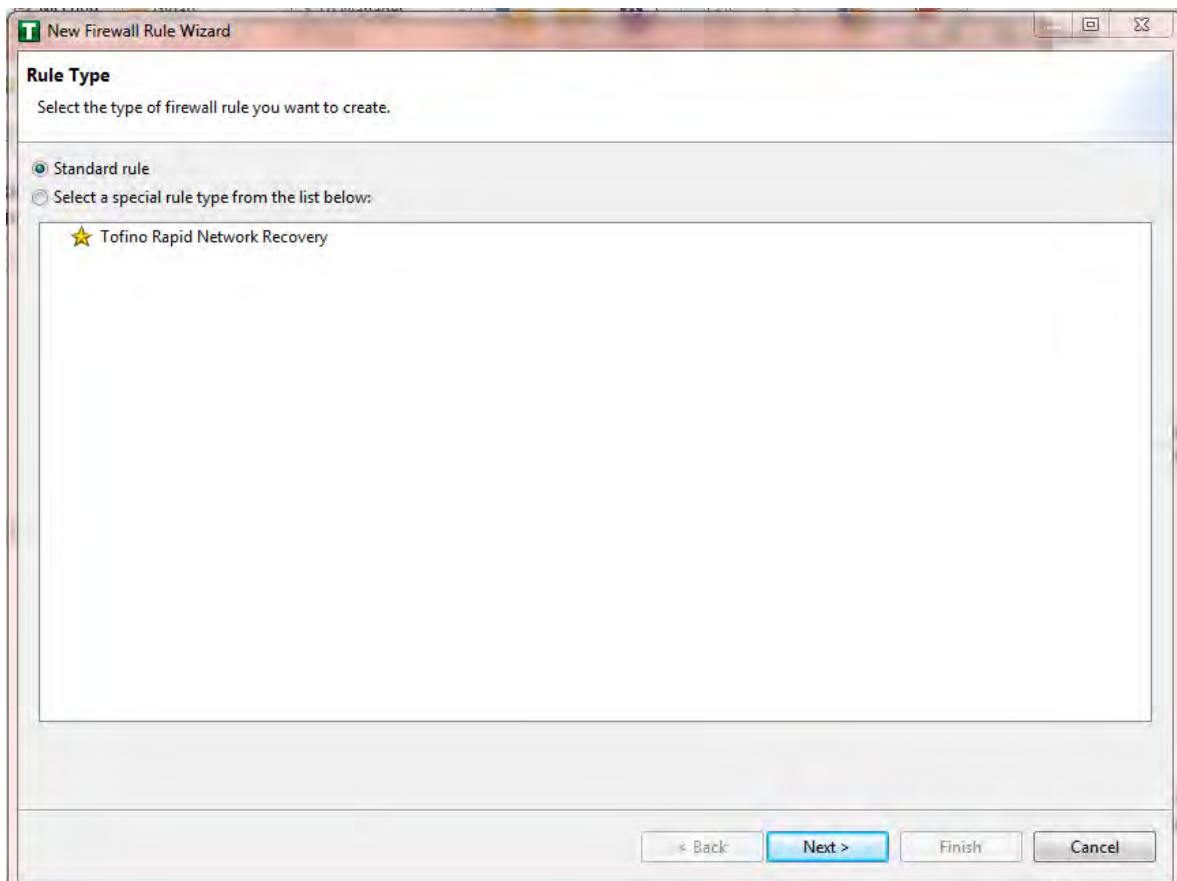
4311

4312

4313

Figure 198. Project Explorer Tofino SA Icon

13. To create the first rule, click on the '+ Create Rule' button above the Tofino SA-Firewall title, Figure 198, above. Then ensure the 'Standard rule' radio button is selected and click 'Next', Figure 199.



4314

Figure 199. Rule Type

4315

14. On the next screen, Figure 200, there a few options to determine. First is Asset 1, you must choose the interface. This will be where the traffic is coming from into the device.

4316

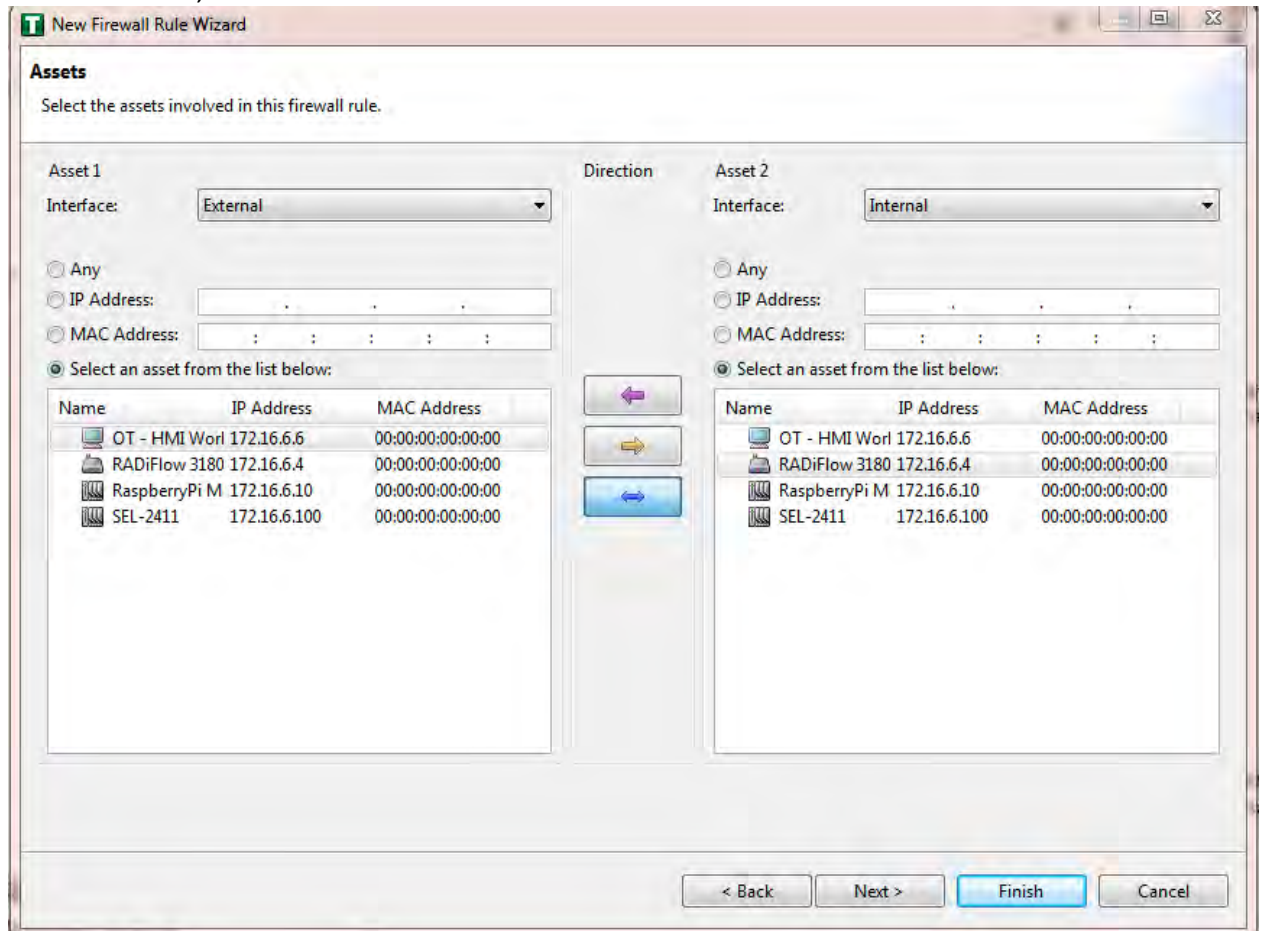
4317

4318

4319

4320

4321

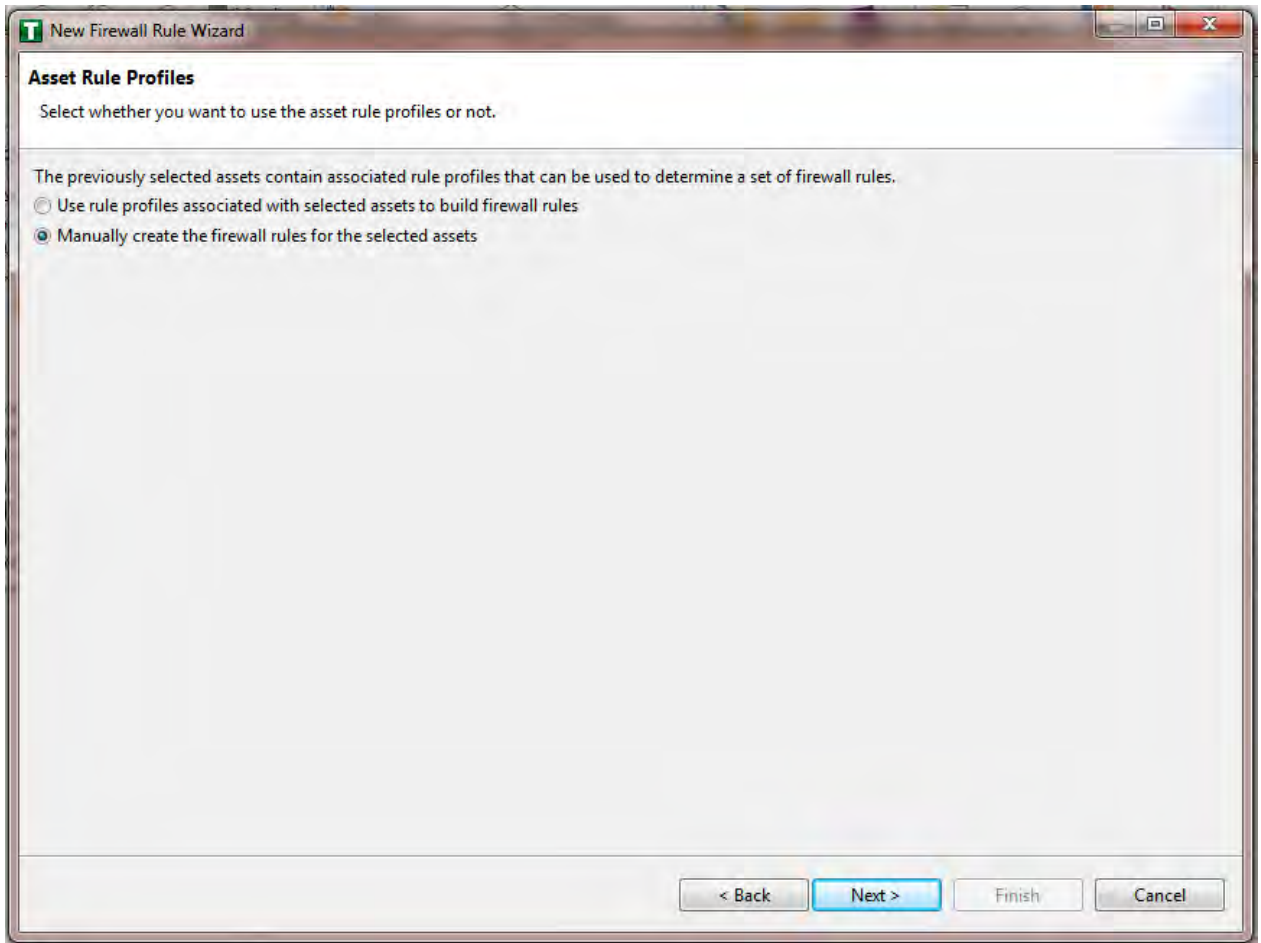


4322

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.*

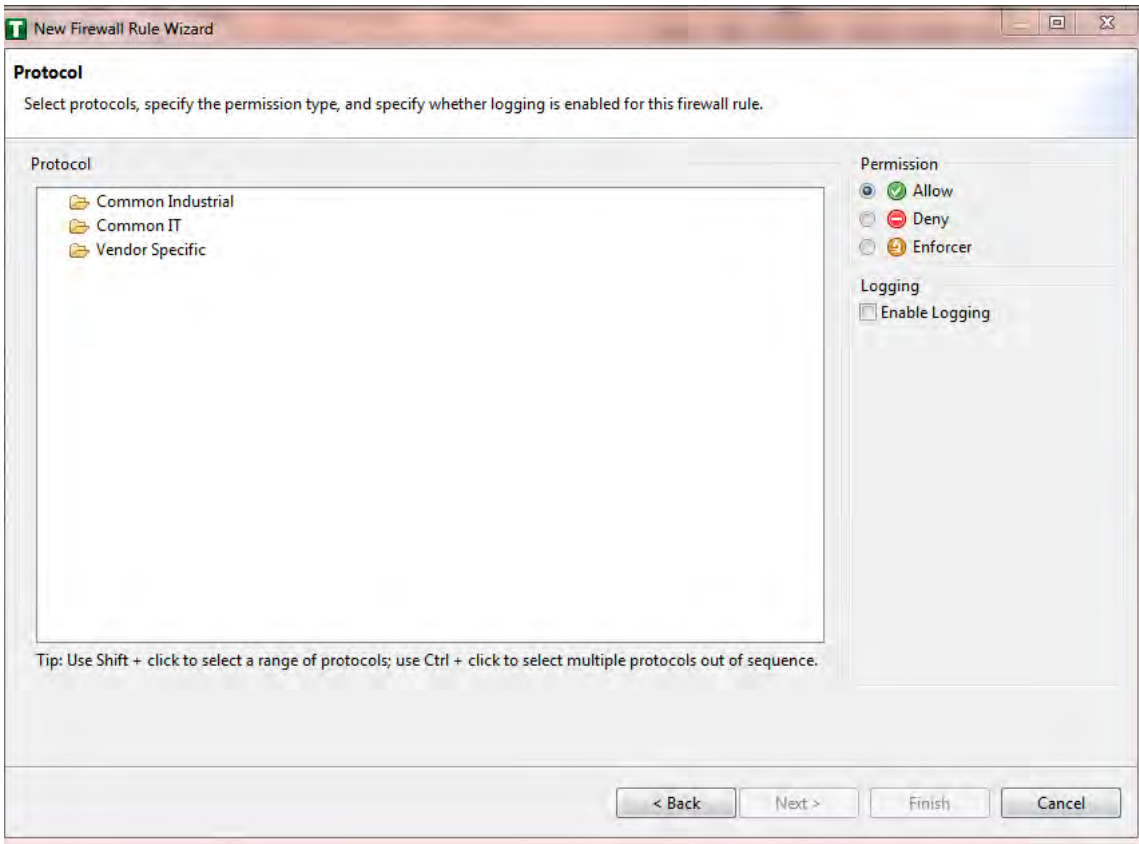
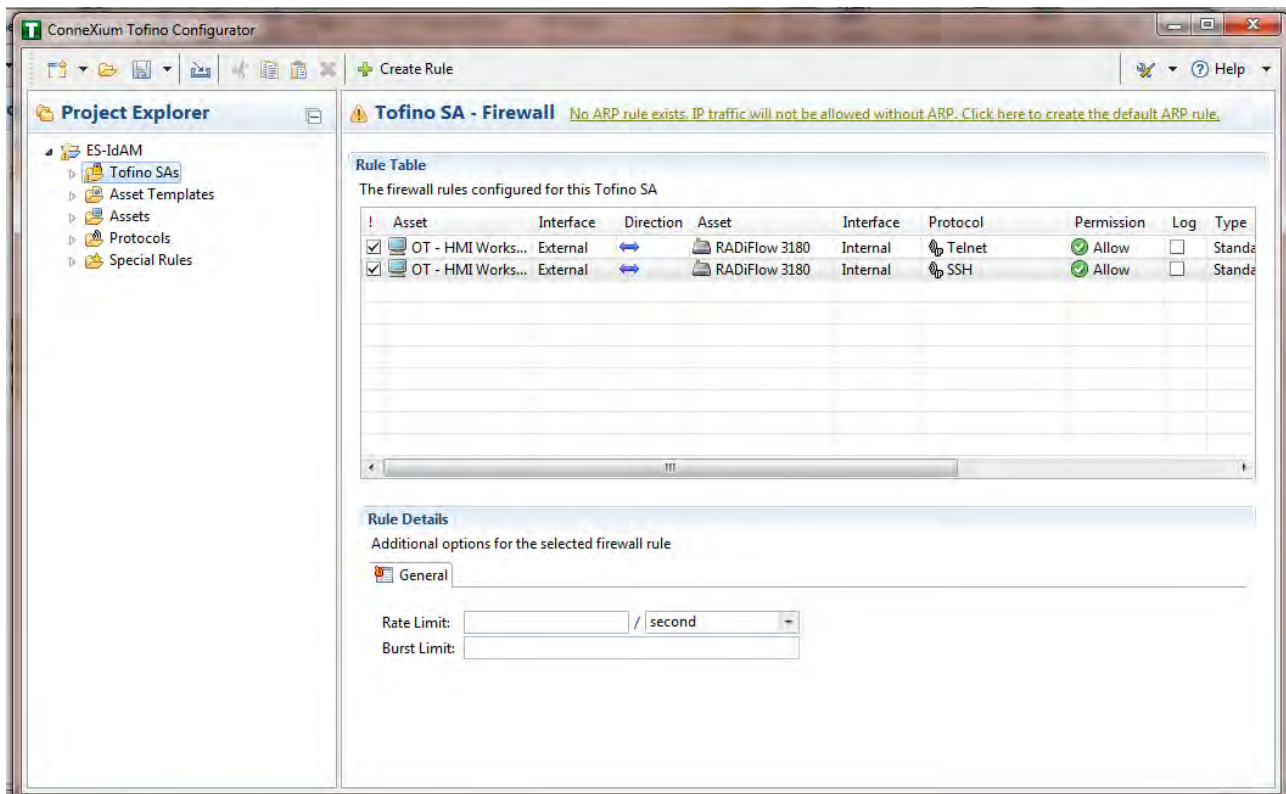


Figure 202. Protocol Window

4335

4336

17. After that is completed, the firewall rule should be listed in the Rule Table, Figure 203.



4337

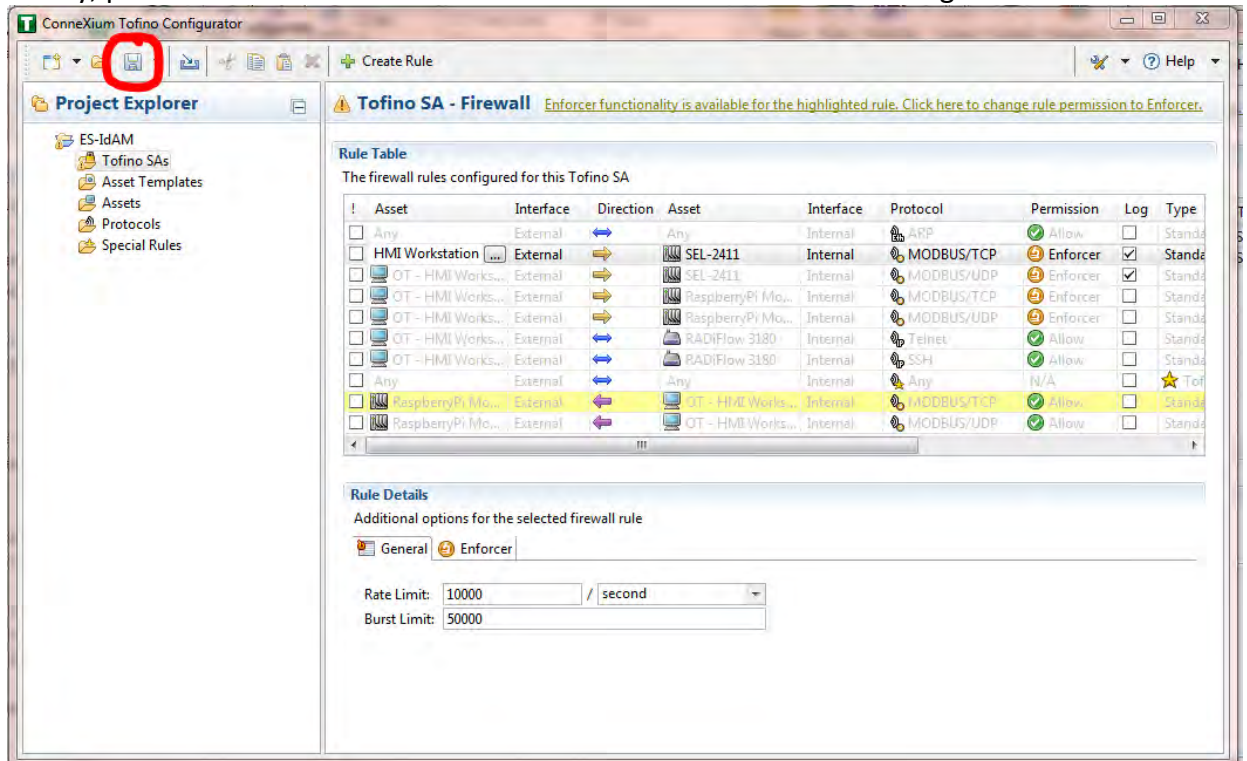
Figure 203. Rule Table

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

4341

Figure 204. Save rules in Project Explorer

4342

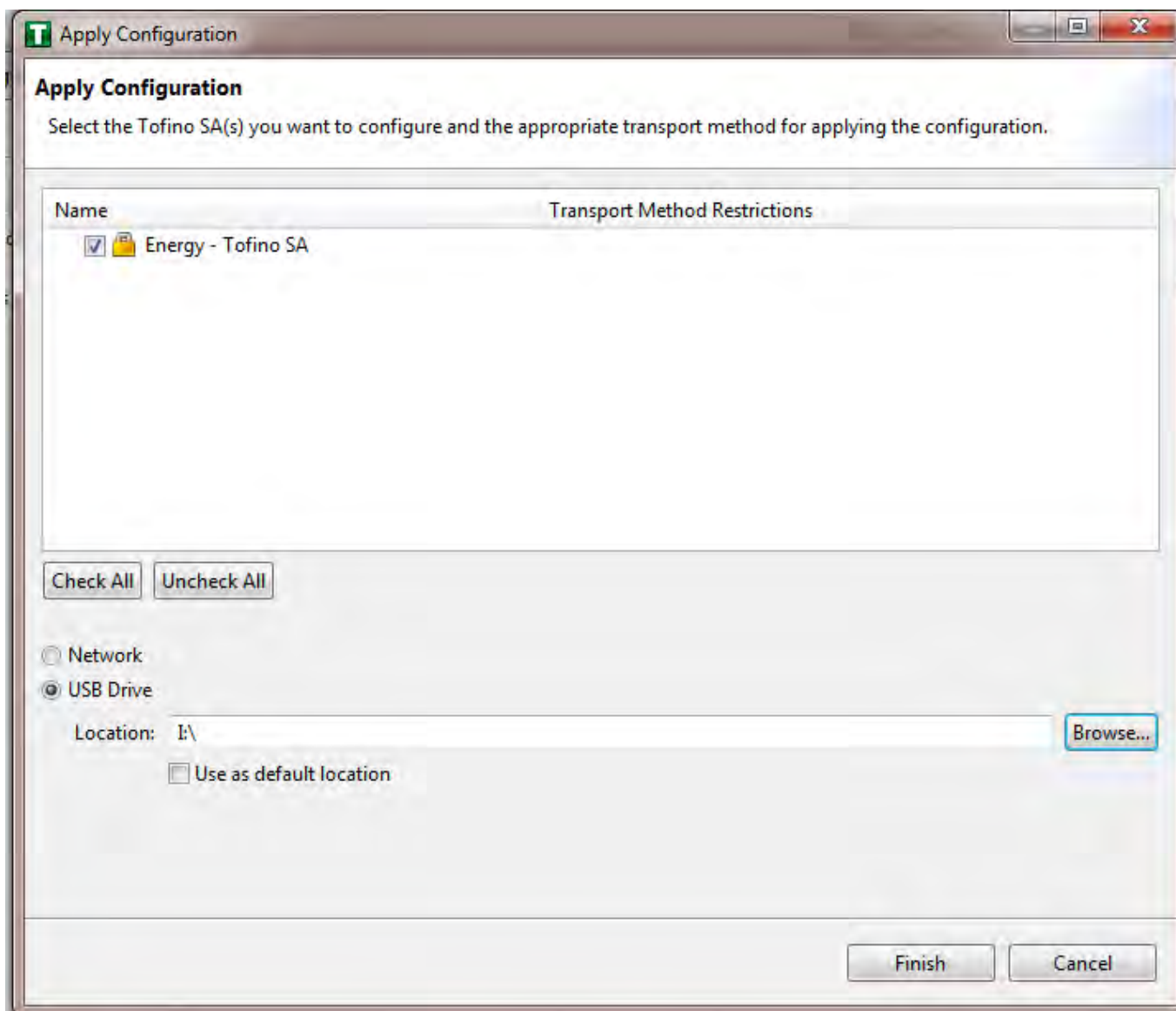
20. Place a FAT/FAT32 formatted USB device into the computer running the ConneXium

4343

Tofino Configurator, then right click 'Tofino SAs' in the Project Explorer pane and select

4344

'Apply.' If the project asks you to save, press 'OK'.

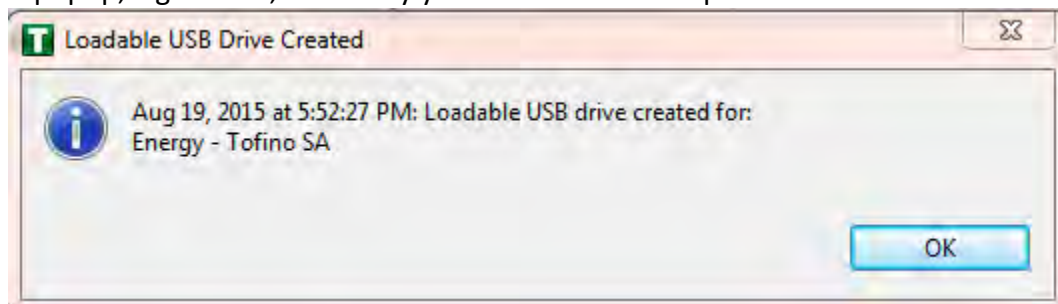


- 4345 21. In the Apply Configuration pane, Figure 205, ensure that your SA is selected in the table  
 4346 at the top, and the 'USB Drive' radio button is selected. Then browse to the top-level  
 4347 directory of your USB drive. Then click Finish.

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
- 4381 • RSA IMG SUSE Linux Server STIG Compliance Report
- 4382 • RSA Adaptive Directory Centos 7 Server STIG Compliance Report
- 4383 • AlertEnterprise Microsoft Server STIG Compliance Report
- 4384 • 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
<b>Red Hat Enterprise Linux 6 Security Technical Implementation Guide</b>	<b>107x fail</b>	<b>12x error</b>
<b>SRG-OS-999999</b> 1x error <a href="#">Automated file system mounting tools must not be enabled unless needed.</a>	low	error
<b>SRG-OS-000062</b> 1x fail <a href="#">Auditing must be enabled at boot by setting a kernel parameter.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The /etc/gshadow file must be owned by root.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The /etc/gshadow file must be group-owned by root.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The /etc/gshadow file must have mode 0000.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a separate file system for /tmp.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a separate file system for /var.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a separate file system for /var/log.</a>	low	fail
<b>SRG-OS-000259</b> 1x fail <a href="#">Library files must be owned by root.</a>	medium	fail
<b>SRG-OS-000044</b> 1x fail <a href="#">The system must use a separate file system for the system audit data path.</a>	low	fail
<b>SRG-OS-000045</b> 1x fail <a href="#">The audit system must alert designated staff members when the audit storage volume approaches capacity.</a>	medium	fail
<b>SRG-OS-000259</b> 1x fail <a href="#">All system command files must be owned by root.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a separate file system for user</a>	low	fail

Title	Severity	Result
<a href="#">home directories.</a>		
<b>SRG-OS-000078</b> 1x fail <a href="#">The system must require passwords to contain a minimum of 14 characters.</a>	medium	fail
<b>SRG-OS-000075</b> 1x fail <a href="#">Users must not be able to change passwords more than once every 24 hours.</a>	medium	fail
<b>SRG-OS-000076</b> 1x fail <a href="#">User passwords must be changed at least every 60 days.</a>	medium	fail
<b>SRG-OS-000071</b> 1x fail <a href="#">The system must require passwords to contain at least one numeric character.</a>	low	fail
<b>SRG-OS-000103</b> 1x fail <a href="#">The system package management tool must cryptographically verify the authenticity of system software packages during installation.</a>	medium	fail
<b>SRG-OS-000232</b> 1x fail <a href="#">A file integrity tool must be installed.</a>	medium	fail
<b>SRG-OS-000273</b> 1x fail <a href="#">The operating system must enforce requirements for the connection of mobile devices to operating systems.</a>	medium	fail
<b>SRG-OS-000248</b> 1x fail <a href="#">There must be no .rhosts or hosts.equiv files on the system.</a>	high	fail
<b>SRG-OS-000249</b> 1x fail <a href="#">The system must disable accounts after excessive login failures within a 15-minute interval.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The /etc/shadow file must be group-owned by root.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The /etc/shadow file must have mode 0000.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">IP forwarding for IPv4 must not be enabled, unless the system is a router.</a>	medium	fail
<b>SRG-OS-000146</b> 1x error <a href="#">The operating system must prevent public IPv4 access into an organizations internal networks, except as appropriately mediated by managed interfaces employing boundary protection devices.</a>	medium	error
<b>SRG-OS-000231</b> 1x fail <a href="#">The systems local IPv4 firewall must implement a deny-all, allow-by-exception policy for inbound packets.</a>	medium	fail
<b>SRG-OS-000096</b> 1x fail <a href="#">The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.</a>	medium	fail
<b>SRG-OS-000096</b> 1x fail <a href="#">The Stream Control Transmission Protocol (SCTP) must be disabled unless required.</a>	medium	fail
<b>SRG-OS-000096</b> 1x fail <a href="#">The Reliable Datagram Sockets (RDS) protocol must be disabled unless required.</a>	low	fail
<b>SRG-OS-000096</b> 1x fail <a href="#">The Transparent Inter-Process Communication (TIPC) protocol must be disabled unless required.</a>	medium	fail
<b>SRG-OS-000215</b> 1x fail		

Title	Severity	Result
<a href="#">The operating system must back up audit records on an organization defined frequency onto a different system or media than the system being audited.</a>	medium	fail
SRG-OS-000043 1x fail		
<a href="#">The operating system must support the requirement to centrally manage the content of audit records generated by organization defined information system components.</a>	medium	fail
SRG-OS-000062 1x fail		
<a href="#">The audit system must be configured to audit all attempts to alter system time through settimeofday.</a>	low	fail
SRG-OS-999999 1x fail		
<a href="#">The system must not accept IPv4 source-routed packets on any interface.</a>	medium	fail
SRG-OS-999999 1x fail		
<a href="#">The system must not accept ICMPv4 redirect packets on any interface.</a>	medium	fail
SRG-OS-999999 1x fail		
<a href="#">The system must not accept ICMPv4 secure redirect packets on any interface.</a>	medium	fail
SRG-OS-000062 1x fail		
<a href="#">The audit system must be configured to audit all attempts to alter system time through clock_settime.</a>	low	fail
SRG-OS-999999 1x fail		
<a href="#">The system must log Martian packets.</a>	low	fail
SRG-OS-999999 1x fail		
<a href="#">The system must not accept IPv4 source-routed packets by default.</a>	medium	fail
SRG-OS-000062 1x fail		
<a href="#">The audit system must be configured to audit all attempts to alter system time through /etc/localtime.</a>	low	fail
SRG-OS-000004 1x fail		
<a href="#">The operating system must automatically audit account creation.</a>	low	fail
SRG-OS-999999 1x fail		
<a href="#">The system must not accept ICMPv4 secure redirect packets by default.</a>	medium	fail
SRG-OS-999999 1x fail		
<a href="#">The system must ignore ICMPv4 redirect messages by default.</a>	low	fail
SRG-OS-000239 1x fail		
<a href="#">The operating system must automatically audit account modification.</a>	low	fail
SRG-OS-999999		
<a href="#">The system must not respond to ICMPv4 sent to a broadcast address.</a>	low	pass
SRG-OS-000240 1x fail		
<a href="#">The operating system must automatically audit account disabling actions.</a>	low	fail
SRG-OS-999999 1x fail		
<a href="#">The system must ignore ICMPv4 bogus error responses.</a>	low	fail
SRG-OS-000241 1x fail		
<a href="#">The operating system must automatically audit account termination.</a>	low	fail
SRG-OS-000142 1x fail		
<a href="#">The system must be configured to use TCP syncookies.</a>	medium	fail



Title	Severity	Result
<b>SRG-OS-999999</b> 1x fail <a href="#">The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</a>	low	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using chmod.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a reverse-path filter for IPv4 network traffic when possible by default.</a>	medium	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using chown.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The IPv6 protocol handler must not be bound to the network stack unless needed.</a>	medium	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using fchmod.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must ignore ICMPv6 redirects by default.</a>	medium	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using fchmodat.</a>	low	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using fchown.</a>	low	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using fchownat.</a>	low	fail
<b>SRG-OS-000152</b> 1x error <a href="#">The system must employ a local IPv4 firewall.</a>	medium	error
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using fremovexattr.</a>	low	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using fsetxattr.</a>	low	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using lchown.</a>	low	fail
<b>SRG-OS-000064</b> 1x fail <a href="#">The audit system must be configured to audit all discretionary access control permission modifications using lremovexattr.</a>	low	fail

Title	Severity	Result
<a href="#">The audit system must be configured to audit all discretionary access control permission modifications using lsetxattr.</a>	low	fail
<b>SRG-OS-000064 1x fail</b>		
<a href="#">The audit system must be configured to audit all discretionary access control permission modifications using removexattr.</a>	low	fail
<b>SRG-OS-000064 1x fail</b>		
<a href="#">The audit system must be configured to audit all discretionary access control permission modifications using setxattr.</a>	low	fail
<b>SRG-OS-000064 1x fail</b>		
<a href="#">The audit system must be configured to audit successful file system mounts.</a>	low	fail
<b>SRG-OS-000069 1x fail</b>		
<a href="#">The system must require passwords to contain at least one uppercase alphabetic character.</a>	low	fail
<b>SRG-OS-000266 1x fail</b>		
<a href="#">The system must require passwords to contain at least one special character.</a>	low	fail
<b>SRG-OS-000070 1x fail</b>		
<a href="#">The system must require passwords to contain at least one lowercase alphabetic character.</a>	low	fail
<b>SRG-OS-000072 1x fail</b>		
<a href="#">The system must require at least four characters be changed between the old and new passwords during a password change.</a>	low	fail
<b>SRG-OS-000021 1x fail</b>		
<a href="#">The system must disable accounts after three consecutive unsuccessful logon attempts.</a>	medium	fail
<b>SRG-OS-000120 1x fail</b>		
<a href="#">The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (system-auth).</a>	medium	fail
<b>SRG-OS-000064 1x fail</b>		
<a href="#">The audit system must be configured to audit user deletions of files and programs.</a>	low	fail
<b>SRG-OS-000120 1x fail</b>		
<a href="#">The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (login.defs).</a>	medium	fail
<b>SRG-OS-000120 1x fail</b>		
<a href="#">The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (libuser.conf).</a>	medium	fail
<b>SRG-OS-000064 1x fail</b>		
<a href="#">The audit system must be configured to audit changes to the /etc/sudoers file.</a>	low	fail
<b>SRG-OS-999999 1x fail</b>		
<a href="#">The system boot loader configuration file(s) must be owned by root.</a>	medium	fail
<b>SRG-OS-000064 1x fail</b>		
<a href="#">The audit system must be configured to audit the loading and unloading of dynamic kernel modules.</a>	medium	fail
<b>SRG-OS-999999 1x fail</b>		

Title	Severity	Result
<a href="#">The system boot loader configuration file(s) must be group-owned by root.</a>	medium	fail
<b>SRG-OS-000096 1x error</b> <a href="#">The xinetd service must be disabled if no network services utilizing it are enabled.</a>	medium	error
<b>SRG-OS-999999 1x fail</b> <a href="#">The system boot loader configuration file(s) must have mode 0600 or less permissive.</a>	medium	fail
<b>SRG-OS-000096 1x fail</b> <a href="#">The xinetd service must be uninstalled if no network services utilizing it are enabled.</a>	low	fail
<b>SRG-OS-000080 1x fail</b> <a href="#">The system boot loader must require authentication.</a>	medium	fail
<b>SRG-OS-000080 1x fail</b> <a href="#">The system must require authentication upon booting into single-user and maintenance modes.</a>	medium	fail
<b>SRG-OS-000080 1x fail</b> <a href="#">The system must not permit interactive boot.</a>	medium	fail
<b>SRG-OS-000022 1x fail</b> <a href="#">The system must require administrator action to unlock an account locked by excessive failed login attempts.</a>	medium	fail
<b>SRG-OS-999999 1x fail</b> <a href="#">The system must not send ICMPv4 redirects by default.</a>	medium	fail
<b>SRG-OS-999999 1x fail</b> <a href="#">The system must not send ICMPv4 redirects from any interface.</a>	medium	fail
<b>SRG-OS-000096 1x error</b> <a href="#">The ybind service must not be running.</a>	medium	error
<b>SRG-OS-999999 1x fail</b> <a href="#">The cron service must be running.</a>	medium	fail
<b>SRG-OS-999999 1x error</b> <a href="#">The avahi service must be disabled.</a>	low	error
<b>SRG-OS-000056 1x error</b> <a href="#">The system clock must be synchronized continuously, or at least daily.</a>	medium	error
<b>SRG-OS-999999 1x fail</b> <a href="#">The system must set a maximum audit log file size.</a>	medium	fail
<b>SRG-OS-000062 1x fail</b> <a href="#">The audit system must be configured to audit all attempts to alter system time through adjtimex.</a>	low	fail
<b>SRG-OS-999999 1x fail</b> <a href="#">The system must retain enough rotated audit logs to cover the required log retention period.</a>	medium	fail
<b>SRG-OS-000096 1x error</b> <a href="#">The atd service must be disabled.</a>	low	error
<b>SRG-OS-999999 1x fail</b> <a href="#">The system default umask for daemons must be 027 or 022.</a>	low	fail
<b>SRG-OS-999999 1x fail</b> <a href="#">The system default umask in /etc/login.defs must be 077.</a>	low	fail
<b>SRG-OS-999999 1x fail</b> <a href="#">The system default umask in /etc/profile must be 077.</a>	low	fail
<b>SRG-OS-999999 1x fail</b> <a href="#">The system default umask for the csh shell must be 077.</a>	low	fail
<b>SRG-OS-000096 1x error</b>		

Title	Severity	Result
<b>SRG-OS-999999</b> 1x fail <a href="#">The rdisc service must not be running.</a>	low	error
<b>SRG-OS-999999</b> 1x error <a href="#">The system default umask for the bash shell must be 077.</a>	low	fail
<b>SRG-OS-000096</b> 1x error <a href="#">The postfix service must be enabled for mail delivery.</a>	low	error
<b>SRG-OS-000248</b> 1x fail <a href="#">The netconsole service must be disabled unless required.</a>	low	error
<b>SRG-OS-999999</b> 1x fail <a href="#">X Windows must not be enabled unless required.</a>	medium	fail
<b>SRG-OS-000027</b> 1x fail <a href="#">Process core dumps must be disabled unless needed.</a>	low	fail
<b>SRG-OS-000160</b> 1x fail <a href="#">The system must limit users to 10 simultaneous system logins, or a site-defined number, in accordance with operational requirements.</a>	low	fail
<b>SRG-OS-000160</b> 1x fail <a href="#">The system must provide VPN connectivity for communications over untrusted networks.</a>	low	fail
<b>SRG-OS-000024</b> 1x fail <a href="#">A login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.</a>	medium	fail
<b>SRG-OS-000034</b> 1x error <a href="#">The Bluetooth service must be disabled.</a>	medium	error
<b>GEN006660</b> 1x fail <a href="#">Accounts must be locked upon 35 days of inactivity.</a>	low	fail
<b>SRG-OS-000118</b> 1x fail <a href="#">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.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">All public directories must be owned by a system account.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a Linux Security Module configured to enforce limits on system services.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The system must use a Linux Security Module configured to limit the privileges of system services.</a>	low	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">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.</a>	medium	fail
<b>SRG-OS-999999</b> 1x fail <a href="#">The audit system must switch the system to single-user mode when available audit storage volume becomes dangerously low.</a>	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**

- adaptivedir

**Addresses**

- 127.0.0.1
- 172.16.4.3
- 0:0:0:0:0:0:1
- fe80:0:0:0:250:56ff:fe89:8965

**Platforms**

- 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									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

4423

4424 17.4 ALERTENTERPRISE 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	BLUE: Score equals 100
Fail: 184	Not Checked: 0	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: 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)
- 4452 - 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
- 4455 prevent access from highly privileged domain accounts and local administrator accounts on domain systems
- 4456 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) -
- 4475 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
- 4479 • **FIPS Compliant Algorithms**
- 4480 ○ The system will be configured to use FIPS-compliant algorithms for encryption, hashing, and signing. - (CCE-10789-6) - Fail
- 4481
- 4482 • **TS/RDS - Session Limit**
- 4483 ○ Remote Desktop Services will limit users to one remote session. - (CCE-12016-2) - Fail
- 4484 • **TS/RDS - Password Prompting**
- 4485 ○ Remote Desktop Services will always prompt a client for passwords upon connection. - (CCE-11299-5) - Fail
- 4486 • **TS/RDS - Set Encryption Level**
- 4487 ○ Remote Desktop Services will be configured with the client connection encryption set to the required level. - (CCE-11677-2) - Fail
- 4488
- 4489 • **TS/RDS - Do Not Use Temp Folders**
- 4490 ○ Remote Desktop Services will be configured to use session-specific temporary folders. - (CCE-10669-0) - Fail
- 4491 • **TS/RDS - Delete Temp Folders**
- 4492 ○ Remote Desktop Services will delete temporary folders when a session is terminated. - (CCE-12046-9) - Fail
- 4493 • **TS/RDS - Time Limit for Disc. Session**
- 4494 ○ Remote Desktop Services will be configured to set a time limit for disconnected sessions. - (CCE-11117-9) - Fail
- 4495 • **TS/RDS - Time Limit for Idle Session**
- 4496 ○ Remote Desktop Services will be configured to disconnect an idle session after the specified time period. - (CCE-11506-3) - Fail
- 4497
- 4498 • **Remote Assistance - Offer Remote Assistance**
- 4499 ○ The system will be configured to prevent unsolicited remote assistance offers. - (CCE-11625-1) - Fail
- 4500 • **Error Reporting - Report Errors**
- 4501 ○ The system will be configured to prevent automatic forwarding of error information. - (CCE-11750-7) - Fail
- 4502 • **Safe DLL Search Mode**
- 4503 ○ The system will be configured to use Safe DLL Search Mode. - (CCE-10772-2) - Fail
- 4504 • **Media Player - Disable Automatic Updates**
- 4505 ○ Media Player must be configured to prevent automatic checking for updates. - (CCE-11298-7) - Fail
- 4506 • **Session Security for NTLM SSP based Servers**
- 4507 ○ The system will be configured to meet the minimum session security requirement for NTLM SSP based servers. - (CCE-10040-4) - Fail
- 4508
- 4509 • **Audit Log Warning Level**
- 4510 ○ The system will generate an audit event when the audit log reaches a percent full threshold. - (CCE-11011-4) - Fail
- 4511
- 4512 • **Disable IP Source Routing**
- 4513 ○ The system will be configured to prevent IP source routing. - (CCE-10732-6) - Fail
- 4514 • **Disable ICMP Redirect**
- 4515 ○ The system will be configured to prevent ICMP redirects from overriding OSPF generated routes. - (CCE-10518-9) - Fail
- 4516
- 4517 • **Disable Router Discovery**
- 4518 ○ The system will be configured to disable the Internet Router Discover Protocol (IRDP). - (CCE-10768-0) - Fail
- 4519 • **TCP Connection Keep-Alive Time**
- 4520 ○ The system will be configured to limit how often keep-alive packets are sent. - (CCE-10381-2) - Fail
- 4521 • **Name-Release Attacks**
- 4522 ○ The system will be configured to ignore NetBIOS name release requests except from WINS servers. - (CCE-10653-4) - Fail
- 4523
- 4524 • **TCP Data Retransmissions**
- 4525 ○ The system will limit how many times unacknowledged TCP data is retransmitted. - (CCE-10941-3) - Fail
- 4526 • **Screen Saver Grace Period**
- 4527 ○ 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
- 4528
- 4529 • **Remotely Accessible Registry Paths and Sub-Paths**
- 4530 ○ 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
- 4546 • **Display of Last User Name**
- 4547 ○ The system will be configured to prevent the display of the last user name on the logon screen. - (CCE-10788-8)
- 4548 - Fail
- 4549 • **Audit Policy Subcategory Setting**
- 4550 ○ Audit policy using subcategories will be enabled. - (CCE-10112-1) - Fail
- 4551 • **IPSec Exemptions**
- 4552 ○ IPSec Exemptions will be limited. - (CCE-10018-0) - Fail
- 4553 • **UAC - Admin Approval Mode**
- 4554 ○ User Account Control approval mode for the built-in Administrator will be enabled. - (CCE-11028-8) - Fail
- 4555 • **UAC - Admin Elevation Prompt**
- 4556 ○ User Account Control will, at a minimum, prompt administrators for consent. - (CCE-11023-9) - Fail
- 4557 • **UAC - User Elevation Prompt**
- 4558 ○ User Account Control will automatically deny standard user requests for elevation. - (CCE-10807-6) - Fail
- 4559 • **Enumerate Administrator Accounts on Elevation**
- 4560 ○ The system will require username and password to elevate a running application. - (CCE-11450-4) - Fail
- 4561 • **TS/RDS - Prevent Password Saving**
- 4562 ○ Passwords will not be saved in the Remote Desktop Client. - (CCE-11905-7) - Fail
- 4563 • **TS/RDS - Drive Redirection**
- 4564 ○ Local drives will be prevented from sharing with Remote Desktop Session Hosts (Remote Desktop Services Role). - (CCE-11709-3) - Fail
- 4565
- 4566 • **RPC - Unauthenticated RPC Clients**
- 4567 ○ Unauthenticated RPC clients will be restricted from connecting to the RPC server. - (CCE-10881-1) - Fail
- 4568 • **RPC - Endpoint Mapper Authentication**
- 4569 ○ Client computers will be required to authenticate for RPC communication. - (CCE-10715-1) - Fail
- 4570 • **Internet Download / Online Ordering**
- 4571 ○ Web publishing and online ordering wizards will be prevented from downloading a list of providers. - (CCE-11136-9) - Fail
- 4572
- 4573 • **Printing Over HTTP**
- 4574 ○ Printing over HTTP will be prevented. - (CCE-11360-5) - Fail
- 4575 • **HTTP Printer Drivers**
- 4576 ○ Downloading print driver packages over HTTP will be prevented. - (CCE-11563-4) - Fail
- 4577 • **Windows Update Device Drive Searching**
- 4578 ○ Windows will be prevented from using Windows Update to search for drivers. - (CCE-10357-2) - Fail
- 4579 • **IPv6 Transition**
- 4580 ○ IPv6 will be disabled until a deliberate transition strategy has been implemented. - Fail
- 4581 • **Windows Peer to Peer Networking**
- 4582 ○ Windows Peer-to-Peer networking services will be turned off. - (CCE-11604-6) - Fail
- 4583 • **Prohibit Network Bridge**
- 4584 ○ Network Bridges will be prohibited in Windows. - (CCE-12074-1) - Fail
- 4585 • **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**
- 4588 ○ Event Viewer Events.asp links will be turned off. - (CCE-10693-0) - Fail
- 4589 ● **Internet File Association Service**
- 4590 ○ The Internet File Association service will be turned off. - (CCE-10697-1) - Fail
- 4591 ● **Order Prints Online**
- 4592 ○ The Order Prints Online wizard will be turned off. - (CCE-11243-3) - Fail
- 4593 ● **Classic Logon**
- 4594 ○ The classic logon screen will be required for user logons. - (CCE-11256-5) - Fail
- 4595 ● **RSS Attachment Downloads**
- 4596 ○ Attachments will be prevented from being downloaded from RSS feeds. - Fail
- 4597 ● **Windows Explorer – Shell Protocol Protected Mode**
- 4598 ○ Windows Explorer shell protocol will run in protected mode. - (CCE-11530-3) - Fail
- 4599 ● **Windows Installer – IE Security Prompt**
- 4600 ○ Users will be notified if a web-based program attempts to install software. - (CCE-10343-2) - Fail
- 4601 ● **Windows Installer – User Control**
- 4602 ○ Users will be prevented from changing installation options. - (CCE-10906-6) - Fail
- 4603 ● **Windows Installer – Vendor Signed Updates**
- 4604 ○ Non-administrators will be prevented from applying vendor signed updates. - (CCE-11468-6) - Fail
- 4605 ● **Media Player – First Use Dialog Boxes**
- 4606 ○ Users will not be presented with Privacy and Installation options on first use of Windows Media Player. - (CCE-11596-4) - Fail
- 4607 ● **Network – Mapper I/O Driver**
- 4608 ○ The Mapper I/O network protocol driver will be disabled. - (CCE-10484-4) - Fail
- 4609 ● **Network – Responder Driver**
- 4610 ○ The Responder network protocol driver will be disabled. - (CCE-11304-3) - Fail
- 4611 ● **Network – WCN Wireless Configuration**
- 4612 ○ The configuration of wireless devices using Windows Connect Now will be disabled. - (CCE-11242-5) - Fail
- 4613 ● **Network – Windows Connect Now Wizards**
- 4614 ○ The Windows Connect Now wizards will be disabled. - (CCE-11155-9) - Fail
- 4615 ● **Device Install – PnP Interface Remote Access**
- 4616 ○ Remote access to the Plug and Play interface will be disabled for device installation. - (CCE-11248-2) - Fail
- 4617 ● **Device Install – Drivers System Restore Point**
- 4618 ○ A system restore point will be created when a new device driver is installed. - (CCE-10546-0) - Fail
- 4619 ● **Device Install – Generic Driver Error Report**
- 4620 ○ An Error Report will not be sent when a generic device driver is installed. - (CCE-12274-7) - Fail
- 4621 ● **Driver Install – Device Driver Search Prompt**
- 4622 ○ Users will not be prompted to search Windows Update for device drivers. - (CCE-11319-1) - Fail
- 4623 ● **Handwriting Recognition Error Reporting**
- 4624 ○ Errors in handwriting recognition on Tablet PCs will not be reported to Microsoft. - (CCE-11030-4) - Fail
- 4625 ● **Power Mgmt – Password Wake on Battery**
- 4626 ○ 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
- 4627 ● **Power Mgmt – Password Wake When Plugged In**
- 4628 ○ 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
- 4629 ● **Remote Assistance – Session Logging**
- 4630 ○ Remote Assistance log files will be generated. - (CCE-11263-1) - Fail
- 4631 ● **Game Explorer Information Downloads**
- 4632 ○ Game explorer information will not be downloaded from Windows Metadata Services. - (CCE-11739-0) - Fail
- 4633 ● **Error Reporting – Logging**
- 4634 ○ Error Reporting events will be logged in the system event log. - (CCE-11621-0) - Fail
- 4635 ● **Error Reporting – Windows Error Reporting**
- 4636 ○ Windows Error Reporting to Microsoft will be disabled. - (CCE-11708-5) - Fail
- 4637 ● **Error Reporting – Additional Data**
- 4638 ○
- 4639 ○
- 4640 ○

- 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
- 4646
- 4647 ● **Media DRM – Internet Access**
- 4648 ○ Windows Media Digital Rights Management will be prevented from accessing the Internet. - (CCE-11052-8) - Fail
- 4649
- 4650 ● **TS/RDS – COM Port Redirection**
- 4651 ○ 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
- 4652
- 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
- 4655
- 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
- 4658
- 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
- 4661
- 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
- 4664
- 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
- 4667
- 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
- 4674
- 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
- 4685
- 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
- 4698
- 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
- 4705
- 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
- 4722
- 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
- 4737
- 4738
- 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
- 4741
- 4742
- 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
- 4745
- 4746
- 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
- 4749
- 4750

- 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) -
- 4753 Fail
- 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) -
- 4758 Fail
- 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 • **Load and unload device drivers**
- 4762 ○ Unauthorized accounts will not have the "Load and unload device drivers" user right. - (CCE-10202-0) - Fail
- 4763 • **Log on as a batch job**
- 4764 ○ Unauthorized accounts will not have the "Log on as a batch job" user right. - (CCE-10549-4) - Fail
- 4765 • **Replace a process level token**
- 4766 ○ Unauthorized accounts will not have the "Replace a process level token" user right. - (CCE-10599-9) - Fail
- 4767 • **Restore files and directories**
- 4768 ○ Unauthorized accounts will not have the "Restore files and directories" user right. - (CCE-10805-0) - Fail
- 4769 • **Shut down the system**
- 4770 ○ Unauthorized accounts will not have the "Shut down the system" user right. - (CCE-10439-8) - Fail
- 4771 • **Audit - Credential Validation - Failure**
- 4772 ○ The system will be configured to audit "Account Logon > Credential Validation" failures. - Fail
- 4773 • **Audit - Computer Account Management - Failure**
- 4774 ○ The system will be configured to audit "Account Management > Computer Account Management" failures. - Fail
- 4775 • **Audit - Other Account Management Events - Success**
- 4776 ○ The system will be configured to audit "Account Management > Other Account Management Events" successes.
- 4777 - Fail
- 4778 • **Audit - Other Account Management Events - Failure**
- 4779 ○ The system will be configured to audit "Account Management > Other Account Management Events" failures. -
- 4780 Fail
- 4781 • **Audit - Security Group Management - Failure**
- 4782 ○ The system will be configured to audit "Account Management > Security Group Management" failures. - Fail
- 4783 • **Audit - User Account Management - Success**
- 4784 • **Audit - User Account Management - Failure**
- 4785 ○ The system will be configured to audit "Account Management > User Account Management" failures. - Fail
- 4786 • **Audit - Process Creation - Success**
- 4787 ○ The system will be configured to audit "Detailed Tracking > Process Creation" successes. - Fail
- 4788 • **Audit - File System - Failure**
- 4789 ○ The system will be configured to audit "Object Access > File System" failures. - Fail
- 4790 • **Audit - Registry - Failure**
- 4791 ○ The system will be configured to audit "Object Access > Registry" failures. - Fail
- 4792 • **Audit - Audit Policy Change - Failure**
- 4793 ○ The system will be configured to audit "Policy Change > Audit Policy Change" failures. - Fail
- 4794 • **Audit - Sensitive Privilege Use - Success**
- 4795 ○ The system will be configured to audit "Privilege Use > Sensitive Privilege Use" successes. - Fail
- 4796 • **Audit - Sensitive Privilege Use - Failure**
- 4797 ○ The system will be configured to audit "Privilege Use > Sensitive Privilege Use" failures. - Fail
- 4798 • **Audit - IPSec Driver - Success**
- 4799 ○ The system will be configured to audit "System > IPSec Driver" successes. - Fail
- 4800 • **Audit - IPSec Driver - Failure**
- 4801 ○ The system will be configured to audit "System > IPSec Driver" failures. - Fail
- 4802 • **Audit - Security State Change - Failure**
- 4803 ○ The system will be configured to audit "System > Security State Change" failures. - Fail
- 4804 • **Audit - Security System Extension - Success**
- 4805 ○ The system will be configured to audit "System > Security System Extension" successes. - Fail

- 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
- 4827 • **Always Install with Elevated Privileges Disabled**
- 4828 ○ The Windows Installer Always install with elevated privileges must be disabled. - (CCE-12401-6) - Fail
- 4829 • **Local admin accounts filtered token policy enabled on domain systems.**
- 4830 ○ Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems. - Fail
- 4831
- 4832 • **WINCC-000078**
- 4833 ○ The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomization (ASLR) must be enabled and configured to Application Opt In. - Fail
- 4834
- 4835 • **WINCC-000079**
- 4836 ○ The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer must be enabled. - Fail
- 4837
- 4838 • **WINCC-000080**
- 4839 ○ The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Recommended Software must be enabled. - Fail
- 4840
- 4841 • **WINCC-000081**
- 4842 ○ The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software must be enabled. - Fail
- 4843
- 4844 • **WINCC-000082**
- 4845 ○ The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) must be enabled and configured to at least Application Opt Out. - Fail
- 4846
- 4847 • **WINCC-000083**
- 4848 ○ The Enhanced Mitigation Experience Toolkit (EMET) system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be configured to Application Opt Out. - Fail
- 4849
- 4850 • **WINGE-000100**
- 4851 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
- 4852
- 4853 • **WINGE-000200**
- 4854 ○ A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail
- 4855
- 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	BLUE: Score equals 100
Fail: 26	Not Checked: 0	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

## 4863 System Information

Target:	ITDC
Operating System:	Windows Server 2012 R2 Standard
OS Service Pack:	
Domain:	ES-IDAM-B1

## 4864 Results

- 4865 • **Bad Logon Attempts**
- 4866 ○ The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- 4867 • **Force Logoff When Logon Hours Expire**
- 4868 ○ The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4)
- 4869 - Fail
- 4870 • **LDAP Signing Requirements**
- 4871 ○ Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
- 4872 • **Computer Account Password Change**
- 4873 ○ Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6)
- 4874 - Fail
- 4875 • **Remotely Accessible Registry Paths and Sub-Paths**
- 4876 ○ Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
- 4877 • **Minimum Password Length**
- 4878 ○ Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- 4879 • **Media DRM – Internet Access**
- 4880 • **Software Certificate Installation Files**
- 4881 ○ Software certificate installation files must be removed from a system. - Fail
- 4882 • **Legal Banner Dialog Box Title**
- 4883 ○ The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- 4884 • **Access this computer from the network**
- 4885 ○ Unauthorized accounts must not have the Access this computer from the network user right on domain
- 4886 controllers. - Fail
- 4887 • **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 ○ Fail
- 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 ○ Fail

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	BLUE: Score equals 100
Fail: 14	Not Checked: 0	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: 265	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"> <li>• [00000007] Intel(R) PRO/1000 MT Network Connection <ul style="list-style-type: none"> <li>○ 172.16.5.6</li> <li>○ 00:50:56:89:A2:29</li> </ul> </li> </ul>

## 4932 Results

- 4933
- **Legal Notice Display**
    - The required legal notice must be configured to display before console logon. - (CCE-8973-0) - Fail
- 4934
- 4935
- **Bad Logon Attempts**
    - Number of allowed bad-logon attempts does not meet minimum requirements. - (CCE-9136-3) - Fail
- 4936
- 4937
- **Secure Print Driver Installation**
    - Print driver installation privilege is not restricted to administrators. - (CCE-9026-6) - Fail
- 4938
- 4939
- **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
- 4940
- 4941
- 4942
- **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
- 4943
- 4944
- 4945
- **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
- 4946
- 4947
- 4948
- **TS/RDS - Remote User Connections**
    - Terminal Services / Remote Desktop Services - Prevent users from connecting using Terminal Services or Remote Desktop. - (CCE-9985-3) - Fail
- 4949
- 4950
- 4951
- **Unnecessary Features Installed**
    - Unnecessary features are installed. - Fail
- 4952
- 4953



- 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 privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9212-2) - Fail
- 4956
- 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 privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-9098-5) - Fail
- 4959
- 4960
- 4961 • **Deny log on locally**
- 4962 ○ 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
- 4963
- 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 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
- 4966
- 4967
- 4968
- 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. - Fail
- 4972
- 4973 • **WINGE-000200**
- 4974 ○ A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail
- 4975

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**

- localhost.localdomain

**Addresses**

- 127.0.0.1
- 172.16.4.11
- 0:0:0:0:0:0:1
- fe80:0:0:0:250:56ff:fe89:76dd

**Platforms**

- cpe:/o:redhat:enterprise\_linu

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**

- localhost.localdomain

**Addresses**

- 127.0.0.1
- 172.16.4.12
- 0:0:0:0:0:0:1
- fe80:0:0:0:250:56ff:fe89:980a

**Platforms**

- cpe:/o:redhat:enterprise\_lin

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	BLUE: Score equals 100
Fail: 26	Not Checked: 0	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

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)
- 5009 - Fail
- 5010 • **LDAP Signing Requirements**
- 5011 ○ Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
- 5012 • **Computer Account Password Change**
- 5013 ○ Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6) - Fail
- 5014 • **Remotely Accessible Registry Paths and Sub-Paths**
- 5015 ○ Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
- 5016 • **Minimum Password Length**
- 5017 ○ Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- 5018 • **Software Certificate Installation Files**
- 5019 ○ Software certificate installation files must be removed from a system. - Fail
- 5020 • **Legal Banner Dialog Box Title**
- 5021 ○ The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- 5022 • **Access this computer from the network**
- 5023 ○ Unauthorized accounts must not have the Access this computer from the network user right on domain
- 5024 controllers. - Fail
- 5025 • **Adjust memory quotas for a process**
- 5026 • **Allow log on locally**

- 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
- 5030 ○ Unauthorized accounts must not have the Back up files and directories user right. - (CCE-25380-7) - Fail
- 5031 ● Bypass traverse checking
- 5032 ○ Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail
- 5033 ● Change the system time
- 5034 ○ Unauthorized accounts must not have the Change the system time user right. - (CCE-24185-1) - Fail
- 5035 ● Change the time zone
- 5036 ○ Unauthorized accounts must not have the Change the time zone user right. - (CCE-24632-2) - Fail
- 5037 ● Force shutdown from a remote system
- 5038 ○ Unauthorized accounts must not have the Force shutdown from a remote system user right. - (CCE-24734-6) - Fail
- 5039 ○ Fail
- 5040 ● Increase a process working set
- 5041 ○ Unauthorized accounts must not have the Increase a process working set user right. - (CCE-24162-0) - Fail
- 5042 ● Load and unload device drivers
- 5043 ○ Unauthorized accounts must not have the Load and unload device drivers user right. - (CCE-24779-1) - Fail
- 5044 ● Log on as a batch job
- 5045 ○ Unauthorized accounts must not have the Log on as a batch job user right. - (CCE-23386-6) - Fail
- 5046 ● Restore files and directories
- 5047 ○ Unauthorized accounts must not have the Restore files and directories user right. - (CCE-25518-2) - Fail
- 5048 ● Shut down the system
- 5049 ○ Unauthorized accounts must not have the Shut down the system user right. - (CCE-23500-2) - Fail
- 5050 ● Add workstations to domain
- 5051 ○ Unauthorized accounts must not have the Add workstations to domain user right. - (CCE-23271-0) - Fail
- 5052 ● Audit Directory Service Access - Success
- 5053 ○ The system must be configured to audit DS Access - Directory Service Access successes. - Fail
- 5054 ● Audit - Directory Service Access - Failure
- 5055 ○ The system must be configured to audit DS Access - Directory Service Access failures. - Fail
- 5056 ● Audit - Directory Service Changes - Success
- 5057 ○ The system must be configured to audit DS Access - Directory Service Changes successes. - Fail
- 5058 ● Audit - Directory Service Changes - Failure
- 5059 ○ The system must be configured to audit DS Access - Directory Service Changes failures. - Fail
- 5060 ● WINGE-000100
- 5061 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
- 5062 ○ 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

5065 SCAP Compliance Checker - 3.1.2

5066 Score | System Information | Stream Information | Results | Detailed Results

5067 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"> <li>• [00000010] Intel(R) 82574L Gigabit Network Connection           <ul style="list-style-type: none"> <li>○ 172.16.6.8</li> <li>○ 00:50:56:89:56:86</li> </ul> </li> </ul>

## 5070 Results

- 5071 • **Bad Logon Attempts**
- 5072 ○ The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- 5073 • **Force Logoff When Logon Hours Expire**
- 5074 ○ The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4)
- 5075 - Fail
- 5076 • **Minimum Password Length**
- 5077 ○ Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- 5078 • **Legal Banner Dialog Box Title**
- 5079 ○ The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- 5080 • **Deny log on as a batch job**
- 5081 ○ The Deny log on as a batch job user right on member servers must be configured to prevent access from highly
- 5082 privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-25215-
- 5083 5) - Fail
- 5084 • **Deny log on as service**
- 5085 ○ The Deny log on as a service user right on member servers must be configured to prevent access from highly
- 5086 privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. -
- 5087 (CCE-23117-5) - Fail
- 5088 • **Deny log on locally**
- 5089 ○ The Deny log on locally user right on member servers must be configured to prevent access from highly
- 5090 privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-24460-
- 5091 8) - Fail
- 5092 • **WINGE-000100**
- 5093 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. -
- 5094 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	BLUE: Score equals 100
Fail: 12	Not Checked: 0	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: 265	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"> <li>• [00000007] Intel(R) PRO/1000 MT Network Connection                             <ul style="list-style-type: none"> <li>○ 172.16.6.6</li> <li>○ 00:50:56:89:0B:7A</li> </ul> </li> </ul>

5102 Results

- 5103 • **Legal Notice Display**
- 5104 ○ The required legal notice must be configured to display before console logon. - (CCE-8973-0) - Fail
- 5105 • **Bad Logon Attempts**
- 5106 ○ Number of allowed bad-logon attempts does not meet minimum requirements. - (CCE-9136-3) - Fail
- 5107 • **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
- 5111 access from highly privileged domain accounts and local administrator accounts on domain systems and
- 5112 unauthenticated access on all systems. - (CCE-9244-5) - Fail
- 5113 ● **Force Logoff When Logon Hours Expire**
- 5114 ○ The system is not configured to force users to log off when their allowed logon hours expire. - (CCE-9704-8) -
- 5115 Fail
- 5116 ● **Minimum Password Length**
- 5117 ○ For systems utilizing a logon ID as the individual identifier, passwords must be a minimum of 14 characters in
- 5118 length. - (CCE-9357-5) - Fail
- 5119 ● **Deny log on as a batch job**
- 5120 ○ The Deny log on as a batch job user right on workstations must be configured to prevent access from highly
- 5121 privileged domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9212-2) - Fail
- 5122 ● **Deny log on as service**
- 5123 ○ The Deny log on as a service user right on workstations must be configured to prevent access from highly
- 5124 privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. -
- 5125 (CCE-9098-5) - Fail
- 5126 ● **Deny log on locally**
- 5127 ○ The Deny log on locally user right on workstations must be configured to prevent access from highly privileged
- 5128 domain accounts on domain systems and unauthenticated access on all systems. - (CCE-9239-5) - Fail
- 5129 ● **Deny log on through Remote Desktop \ Terminal Services**
- 5130 ○ The Deny log on through Remote Desktop Services user right on workstations must prevent all access if RDS is
- 5131 not used by the organization. If RDS is used, it must be configured to prevent access from highly privileged
- 5132 domain accounts and local administrator accounts on domain systems and unauthenticated access on all
- 5133 systems. - (CCE-9274-2) - Fail
- 5134 ● **WINGE-000100**
- 5135 ○ The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. -
- 5136 Fail
- 5137 ● **WINGE-000200**
- 5138 ○ A group named DenyNetworkAccess must be defined on domain systems to include all local administrator
- 5139 accounts. - Fail

## 5140 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**

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	BLUE: Score equals 100
	Fail: 11	Not Checked: 0	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

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"> <li>• [00000010] Intel(R) 82574L Gigabit Network Connection <ul style="list-style-type: none"> <li>○ 172.16.7.11</li> <li>○ 00:50:56:89:F8:E0</li> </ul> </li> </ul>

## 5186 Results

- 5187 • **Bad Logon Attempts**
- 5188 ○ The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- 5189 • **Force Logoff When Logon Hours Expire**
- 5190 ○ The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4)
- 5191 - Fail
- 5192 • **Minimum Password Length**
- 5193 ○ Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- 5194 • **Legal Banner Dialog Box Title**
- 5195 ○ The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- 5196 • **Adjust memory quotas for a process**
- 5197 ○ Unauthorized accounts must not have the Adjust memory quotas for a process user right. - (CCE-25112-4) - Fail
- 5198 • **Bypass traverse checking**
- 5199 ○ Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail
- 5200 • **Deny log on as a batch job**
- 5201 ○ The Deny log on as a batch job user right on member servers must be configured to prevent access from highly
- 5202 privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-25215-
- 5203 5) - Fail
- 5204 • **Deny log on as service**
- 5205 ○ The Deny log on as a service user right on member servers must be configured to prevent access from highly
- 5206 privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. -
- 5207 (CCE-23117-5) - Fail
- 5208 • **Deny log on locally**
- 5209 ○ The Deny log on locally user right on member servers must be configured to prevent access from highly
- 5210 privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-24460-
- 5211 8) - Fail
- 5212 • **Replace a process level token**
- 5213 ○ Unauthorized accounts must not have the Replace a process level token user right. - (CCE-24555-5) - Fail
- 5214 • **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:

- 5221 • Separate partitions for /var, /var/log, /var/log/audit, /tmp, /home
- 5222 • Networking is configured for your network

```
5223
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*
```

```
5231
5232 ----- Run Initial Test -----
5233
```

```
5234 oscap xccdf eval --report ../reports/report.html --cpe *cpe-
5235 dictionary.xml *Benchmark-xccdf.xml
5236 python -m SimpleHTTPServer
```

```
5237
5238 Go to http://<Centos 7 IP Address>:8000/ to view the results of the STIG test
5239
```

5240 1. Next add the following files to the following locations:

- 5241 • rules\_d-audit.rules > /etc/audit/rules.d/audit.rules
- 5242 • audit.rules > /etc/audit/audit.rules
- 5243 • audit.conf > /etc/audit/audit.conf
- 5244 • system-auth > /etc/pam.d/system-auth
- 5245 • system-au0 0 \* \* \* root /sbin/aide -checkth-ac > /etc/pam.d/system-auth-ac
- 5246 • sysctl.conf > /etc/sysctl.conf
- 5247 • password-auth-ac > /etc/pam.d/password-auth-ac
- 5248 • iptables > /etc/sysconfig/iptables

5249 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
```

5254 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. In -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 authsucc 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 settimeofday -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/rmmod -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 -
5654 k 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 -
5657 k 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 -
5675 k 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 -
5678 k 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
5682 -k 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
5685 -k 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 authsucc 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 authsucc 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_authtok
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
<ul style="list-style-type: none"> <li>localhost.localdomain</li> </ul>	<ul style="list-style-type: none"> <li>127.0.0.1</li> <li>10.32.2.59</li> <li>0:0:0:0:0:0:1</li> <li>fe80:0:0:0:250:56ff:fe89:5cab</li> </ul>	<ul style="list-style-type: none"> <li>cpe:/o:redhat:enterprise_linux:6</li> </ul>

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
<a href="#">Auditing must be enabled at boot by setting a kernel parameter.</a>	fail
<a href="#">The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</a>	fail
<a href="#">The system boot loader configuration file(s) must be owned by root.</a>	fail
<a href="#">The system boot loader configuration file(s) must be group-owned by root.</a>	fail
<a href="#">The system boot loader configuration file(s) must have mode 0600 or less permissive.</a>	fail
<a href="#">The system boot loader must require authentication.</a>	fail

5796

5797 **18 ACRONYMS**

Acronym	Literal Translation
<b>AD</b>	Active Directory
<b>CA</b>	Certificate authority (also used as shorthand for the name of the company “CA Technologies”)
<b>CIP</b>	Critical Infrastructure Protection
<b>.csv</b>	Comma-Separated Value
<b>DISA</b>	Defense Information Systems Agency
<b>DMZ</b>	Demilitarized Zone
<b>DoD</b>	Department of Defense
<b>EMS</b>	Energy Management System
<b>ICS</b>	Industrial Control System
<b>IdAM</b>	Identity and Access Management
<b>iEMS</b>	RADiFlow ICS/SCADA router configuration management software
<b>ISE</b>	Identity Services Engine
<b>iSIM</b>	Industrial Service Management Tool
<b>IT</b>	Information Technology
<b>JRE</b>	Java Runtime Environment
<b>NAS</b>	Network Attached Storage
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NERC</b>	North American Electric Reliability Corporation
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>OT</b>	Operational Technology
<b>PACS</b>	Physical Access Control System



Acronym	Literal Translation
<b>PLC</b>	Programmable Logic Controller
<b>RAM</b>	Random Access Memory
<b>RTU</b>	Remote Terminal Unit
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>STIG</b>	Security Technical Implementation Guideline
<b>VLAN</b>	Virtual Local Area Network
<b>VM</b>	Virtual Machine
<b>VPN</b>	Virtual Private Network
<b>WAR</b>	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 Oder 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 Attributes.....	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