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The electric power industry is upgrading older, outdated infrastructure to take advantage of emerging technologies that will create “a platform [that] efficiently [integrates] new energy resources, new technologies,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.

---


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
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
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jasvir Gill</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Srini Kakkera</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Srinivas Adepu</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Pan Kamal</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Mike Dullea</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Ted Short</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Alan Zhu</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Peter Romness</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Name</td>
<td>Company</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Lila Kee</td>
<td>GlobalSign</td>
</tr>
<tr>
<td>Sid Desai</td>
<td>GlobalSign</td>
</tr>
<tr>
<td>Paul Townsend</td>
<td>Mount Airey Group (MAG)</td>
</tr>
<tr>
<td>Joe Lloyd</td>
<td>Mount Airey Group (MAG)</td>
</tr>
<tr>
<td>Ayal Vogel</td>
<td>Radiflow</td>
</tr>
<tr>
<td>Dario Lobozzo</td>
<td>Radiflow</td>
</tr>
<tr>
<td>Steve Schmalz</td>
<td>RSA</td>
</tr>
<tr>
<td>Tony Kroukamp (The SCE Group)</td>
<td>RSA</td>
</tr>
<tr>
<td>Kala Kinyon (The SCE Group)</td>
<td>RSA</td>
</tr>
<tr>
<td>Dave Barnard</td>
<td>RS2 Technologies</td>
</tr>
<tr>
<td>David Bensky</td>
<td>RS2 Technologies</td>
</tr>
<tr>
<td>Rich Gillespie (IACS Inc.)</td>
<td>RS2 Technologies</td>
</tr>
<tr>
<td>George Wrenn</td>
<td>Schneider Electric</td>
</tr>
<tr>
<td>Michael Pyle</td>
<td>Schneider Electric</td>
</tr>
<tr>
<td>Bill Johnson</td>
<td>TDi Technologies</td>
</tr>
<tr>
<td>Pam Johnson</td>
<td>TDi Technologies</td>
</tr>
<tr>
<td>Clyde Poole</td>
<td>TDi Technologies</td>
</tr>
<tr>
<td>Danny Vital</td>
<td>XTe</td>
</tr>
<tr>
<td>Mari Devitte</td>
<td>XTe</td>
</tr>
<tr>
<td>David Hellbock</td>
<td>XTe</td>
</tr>
<tr>
<td>John Schiefer</td>
<td>XTe</td>
</tr>
</tbody>
</table>
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 Application94

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 SUMMARY

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

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

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

1.1 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.”1 The ever greater numbers of technologies, devices, and systems connected to utilities’ grid networks need protection from physical and cybersecurity attacks.2

IdAM implementations in the electricity subsector are often decentralized and controlled by numerous departments within an energy 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, energy companies need to be able to control physical and logical access to their networked resources, including buildings, equipment, information technology, and industrial control systems (ICS)—all of which have unique technical and political challenges.3 Identity and access management (IdAM) systems for these assets often exist in silos, and employees who manage access to these systems lack methods to effectively coordinate access to devices and facilities in these silos. This drives inefficiency and creates security risks, according to our electric utility stakeholders.

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

---

3 Protect Critical Infrastructure, McAfee, 2012.
matters require the technician to move out of the region, so she terminates her employment at the company. Without a centralized IdAM system, managing routine events like this one can become cumbersome and time-consuming. How can energy companies be confident that access to the appropriate physical and technological resources across the enterprise is granted or revoked correctly, and in a timely fashion?

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

1.2 The Solution

The example solution we propose demonstrates the following capabilities:

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

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

- an IdAM workflow to manage the overall process and to require explicit approval of requests to access certain resources
- 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

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

The guide:

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

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

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

This guide lists all the necessary components and provides installation, configuration, and integration information so that an energy company can replicate what we have built. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your utility’s 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.

1.3 Risks

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

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

At the strategic level, you might consider the cost of mitigating these risks and the potential return on your investment in implementing a product (or multiple products). You may also want to assess if a centralized IdAM system can help enhance the productivity of employees and speed delivery of services, and explore if it can help support oversight of resources, including information technology, personnel, and data. This example solution addresses imminent operational security risks and incorporates strategic risk considerations, too.
Adopting any new technology can introduce new risks to your enterprise. We understand that this example solution to mitigate the risks of decentralized IdAM may, in turn, introduce new risks. By centralizing IdAM functions, we decrease the risk that multiple IdAM platforms can be infiltrated to gain unauthorized access to networked devices. We recognize, however, that centralizing IdAM functions may provide a point of single infiltration of multiple critical systems (OT, PACS, and IT). We address this key risk in detail in Section 5.9.5.1 Threats, Vulnerabilities and Assumptions, and provide a comprehensive list of mitigations in Section 5.9.6, Security Recommendations.

1.4 Benefits

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

- products and capabilities can be adopted on a component-by-component basis, or as a whole
- minimizes impact to the enterprise and existing infrastructure
- reduces opportunities for attack or error, and impact of identity and access incidents on energy delivery, 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

1.5 Technology Partners

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

- AlertEnterprise
- CA Technologies
- Cisco Systems, Inc.
- GlobalSign
- Mount Airey Group
- RS2 Technologies
- RSA Security, LLC
- RADiFlow
1.6 Feedback

You can improve this guide 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 example solution by contacting us at energy_nccoe@nist.gov.
2 How to Use This Guide

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

This guide contains three volumes:

- NIST SP 1800-2a: Executive Summary
- NIST SP 1800-2c: How To Guides – instructions for building the example solution

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

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

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

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

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

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

This guide assumes that IT professionals have experience implementing security products in energy industry organizations. While we have used a suite of commercial products to address
this challenge, this guide does not endorse these particular products. Your organization’s security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your organization 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 for operational technology systems (OT), physical access control systems (PACS), and IT systems (IT). If you use other products, we hope you will seek those that are congruent with applicable standards and best practices.

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

3 INTRODUCTION

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

The individuals we consulted told us that they need to control physical and logical access to their resources, including buildings, equipment, IT, and industrial control systems. They need to authenticate only designated individuals and devices 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. Current IdAM implementations are often not centralized and are controlled by numerous departments within an energy company. Several negative outcomes can result from this situation: 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. Another key consideration is the need for companies to demonstrate compliance with industry standards and/or government regulations.

We constructed two versions of an end-to-end identity management solution that provides access control capabilities across the OT, PACS, and IT networks. We used the same approach 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.
functionality and capability. Sections 5.3.1 and 5.3.2 detail these two example solutions. The end result is that a user’s access to facilities and devices can be provisioned from a single console. Access privileges can be modified by adding new users and assigning access for the first time, modifying existing user access privileges, or disabling user access privileges. Our goal was to provide the electricity subsector with a solution that addresses the key tenet of cybersecurity—access management/rights—based on the principle of least privilege.\(^5\)

**4 APPROACH**

**4.1 Audience**

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

**4.2 Scope**

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

In response, the NCCoE drafted a use case that identified numerous desired solution characteristics. After an open call in the Federal Register, we chose technology partners on the basis of their ability to provide these characteristics. We initially thought it would be feasible to include federation of identity management\(^6\) services in the scope. As we progressed through the initial stages of solution development, we realized that access, authentication, and authorization through federated identity means would vastly increase the amount of time needed to complete a build. We narrowed the scope to providing identity management of energy company employees including a centralized provisioning capability to the OT, PACS, and IT networks. The scope became successful execution of the following provisioning functions:

1. enabling access for a new employee
2. modifying access for an existing employee
3. disabling access for a former employee

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

---


\(^6\) “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](http://searchsecurity.techtarget.com/definition/federated-identity-management)
4.2.1 Assumptions

4.2.1.1 Security

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

4.2.1.2 Modularity

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

4.2.1.3 Human Resources Database/Identity Vetting

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

4.2.1.4 Identity Federation

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

4.2.1.5 Technical Implementation

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

4.2.1.6 Limited Scalability Testing

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

4.2.1.7 Replication of Enterprise Network

We were able to replicate the three silos: 1) physical access control systems, 2) information technology or corporate networks, and 3) the operational technology network, in a limited
The goal was to demonstrate both logically and physically that provisioning functions could be performed from a centralized IdAM system regardless of its location in the enterprise. In a real-world environment, the interconnections between the OT, PACS, and IT silos depend on the business needs and compliance requirements of the enterprise. We did not attempt to replicate these interconnections. Rather, we acknowledge that implementing our build or its components creates new interfaces across silos. We focused on providing general information on how to remain within the bounds of compliance should you adopt this example solution. In addition, we provide guidance on how to mitigate any new risks introduced to the environment.

4.3 Risk Assessment and Mitigation

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

4.3.1 Assessing Risk Posture

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

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

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

---

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

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

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

Undertaking these activities in accordance with the NIST RMF guidance yielded the necessary operational and strategic risk information, which we subsequently translated to security characteristics. We mapped these characteristics to NIST’s SP 800-53 Rev.4 controls where applicable, along with other applicable industry and mainstream security standards.

4.3.2 Managing IdAM Risk

A foundation of cybersecurity is the principle of least privilege, defined as providing the least amount of access (to systems) necessary for the user to complete his or her job. To enforce this principle, the access control system needs to know the appropriate privileges for each user and system. An analysis of the IdAM solution reveals two components that need to be 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
store, and the authorization workflow management system. The authorization workflow management system is trusted to make changes to the central identity and authorization store. Therefore, any inappropriate or unauthorized use of these systems could change authorization levels for anyone in the enterprise. If that occurred, the enterprise would experience a lack of integrity of the identity and authentication stores. The central identity and authorization store is the authoritative source for the enterprise and holds the hash for each user password, as well as the authorizations associated with each user. Access to this information would enable an unauthorized user to impersonate anyone in the organization. In this situation, the enterprise would lose the confidentiality of its users.\(^\text{12}\)

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

4.3.3 Security Characteristics and Controls Mapping

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

<table>
<thead>
<tr>
<th>Example Characteristic</th>
<th>Cybersecurity Standards and Best Practices</th>
<th>Specific Related and Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Characteristics</strong></td>
<td><strong>Example Capability</strong></td>
<td><strong>CSF Function</strong></td>
</tr>
<tr>
<td>Authentication for OT</td>
<td>Authentication mechanisms</td>
<td>Protect</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Example Characteristic</th>
<th>Cybersecurity Standards and Best Practices</th>
<th>Specific Related and Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example Characteristic</td>
<td>Cybersecurity Standards and Best Practices</td>
<td>Specific Related and Best Practices</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Security Characteristics</strong></td>
<td><strong>Example Capability</strong></td>
<td><strong>CSF</strong></td>
</tr>
<tr>
<td>Centrally monitor use of accounts</td>
<td>Log account activity</td>
<td>Detect</td>
</tr>
<tr>
<td>Example Characteristic</td>
<td>Cybersecurity Standards and Best Practices</td>
<td>Specific Related and Best Practices</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Provision, modify or revoke access throughout all federated entities</td>
<td>Mechanisms for centrally managed provisioning of access</td>
<td>Protect</td>
</tr>
</tbody>
</table>

**CSF Function:** 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.

**CSF Category:** Access Control

**CSF Subcategory:** NIST 800-53 rev4

**NIST 800-53 rev4:**
- AC-2, AC-3, AC-5, AC-6, AC-16, IA Family

**IEC/ISO27001:**

**SANS CAG20:**
- CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12

**NERC CIP v3/5:**
- 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
### Table 2. Products and Technologies Used to Satisfy Security Control Requirements

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

---

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
<table>
<thead>
<tr>
<th>Security Characteristics</th>
<th>Example Capability</th>
<th>CSF Subcategory</th>
<th>Application</th>
<th>Company</th>
<th>Product</th>
<th>Version</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>federated entities</td>
<td>access</td>
<td></td>
<td>Credential Management</td>
<td>GlobalSign</td>
<td>Enterprise PKI</td>
<td>N/A</td>
<td>Provides NAESB-compliant X.509 certificates to OT personnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Credential Management / Physical Access Control</td>
<td>XTeC</td>
<td>Credential Issuance Solutions</td>
<td>N/A</td>
<td>Provides PIV-I smartcard credentials and physical access control capability using the smartcard.</td>
</tr>
<tr>
<td>Access Control for OT</td>
<td>Access control mechanisms</td>
<td>PR.AC-2: Physical access to assets is managed and protected</td>
<td>Credential Management / Physical Access Control</td>
<td>XTeC</td>
<td>Physical Access Control Logical Access Control Authentication and Validation</td>
<td>N/A</td>
<td>Provides PIV-I smartcard credentials and physical access control capability using the smartcard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Physical Access Control Enforcement</td>
<td>RS2 Technologies</td>
<td>AccessIT!</td>
<td>4.1.15</td>
<td>Controls physical access to power facilities, buildings, etc.</td>
</tr>
<tr>
<td>Authorization (provisioning) OT</td>
<td>Access policy management mechanisms</td>
<td>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</td>
<td>Provisioning</td>
<td>AlertEnterprise</td>
<td>Guardian</td>
<td>4.0 SP04 HF3</td>
<td>Provisions access authorizations from the IdAM workflow to Access It Universal</td>
</tr>
<tr>
<td>Provision, modify or revoke access throughout all federated entities</td>
<td>Mechanisms for centrally managed provisioning of access</td>
<td>Provisioning</td>
<td>AlertEnterprise</td>
<td>Guardian</td>
<td>4.0 SP04 HF3</td>
<td>Provisions access authorizations from the IdAM workflow to Access It Universal</td>
<td></td>
</tr>
<tr>
<td>Security Characteristics</td>
<td>Example Capability</td>
<td>CSF Subcategory</td>
<td>Application</td>
<td>Company</td>
<td>Product</td>
<td>Version</td>
<td>Use</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------</td>
<td>----------------------------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Provenion, modify or revoke access throughout all federated entities</td>
<td>Mechanisms for centrally managed provisioning of access</td>
<td>RSA</td>
<td>RSA IMG 16</td>
<td>Ozone Console and Ozone Authority Secure Attribute Management Public Key Enablement Ozone Mobile</td>
<td>6.9.74968</td>
<td>Manages attributes that control access to high-value transactions.</td>
<td></td>
</tr>
<tr>
<td>Centrally monitor use of accounts</td>
<td>Log account activity</td>
<td>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</td>
<td>Mount Airey Group</td>
<td>TDi Technologies</td>
<td>Ozone Console 4.0.1, Ozone Server 2.1.301, Ozone Envoy 4.1.0, Ozone Console 2.0.2</td>
<td>Controls access to industrial control system (ICS) devices by people (ICS engineers and technicians).</td>
<td></td>
</tr>
</tbody>
</table>

16 RSA IMG is now known as RSA VIA Governance and RSA VIA Lifecycle
<table>
<thead>
<tr>
<th>Security Characteristics</th>
<th>Example Capability</th>
<th>CSF Subcategory</th>
<th>Application</th>
<th>Company</th>
<th>Product</th>
<th>Version</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control for OT</td>
<td>Access control</td>
<td>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</td>
<td>Industrial Control System (ICS) User Access Management</td>
<td>TDi Technologies</td>
<td>Console Works</td>
<td>4.9-0u0</td>
<td>Creates an audit trail of access to ICS devices by people.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Access Gateway</td>
<td>Cisco</td>
<td>Identity Service Engine (ISE)</td>
<td>1.4.0.253</td>
<td>Controls access to resources in OT by users in IT based on both user identity and device identity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Access Gateway</td>
<td>Schneider Electric</td>
<td>ConneXium Tofino Ethernet Firewall</td>
<td>2.10</td>
<td>Controls access to devices in the ICS/SCADA network</td>
</tr>
</tbody>
</table>
5 ARCHITECTURE

5.1 Example Solution Description

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

1. **User registration** determines that a reason exists to give a person access to resources, verifies the person’s identity, and creates one or more digital identities for the person.

2. **Credential issuance and management**\(^\text{17}\) provides life-cycle management of credentials such as employee badges or digital certificates.

3. **Access rights management** determines the resources a digital identity is allowed to use.

4. **Provisioning** populates digital identity, credential, and access rights information for use in authentication, access control, and audit.

5. **Authentication** establishes confidence in a person’s digital identity.

6. **Access control**\(^\text{18}\) allows or denies a digital identity access to a resource.

7. **Audit** maintains a record of resource access attempts by a digital identity.

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

\(^\text{17}\) NIST SP 800-63-2, Electronic Authentication Guideline, provides additional information on credential issuance and management, as well as authentication.

\(^\text{18}\) NIST IR 7316, Assessment of Access Control Systems, explains commonly used access control policies, models, and mechanisms.
invoked when an employee is hired, changes jobs, leaves the company, loses a credential, or when a credential expires.

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

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

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

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

- 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

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

The example solution implements three basic transactions:

- 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
destroying credentials and removing accesses for a terminated employee

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

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

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

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

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

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

---

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

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

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

5.1.1 The Physical Access Control System Silo

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

Figure 3 shows the architecture of the PACS silo.

---

20 Workflow actions are programmable and can be customized to meet organization-specific needs.
An instance of Microsoft Active Directory contains identities and access control information for the people who operate the badging systems and the people who manage the access control systems. This access control information is provisioned into the PACS Active Directory instance from the centralized IdAM system.

The PACS Active Directory instance may also store authorized physical access information used by the access control systems. If the access control systems are integrated with Active Directory, then the IdAM system will provision authorization information to PACS Active Directory. If the access control systems are not integrated with Active Directory, then authorization information will be provisioned directly to the access control system.\(^{21}\)

### 5.1.2 The Operational Technology Silo

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

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

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

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

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

Figure 5 shows the notional architecture of the IT silo.

![Figure 5. Notional IT silo architecture](image)

### 5.2 Example Solution Relationship to Use Case

When we first defined this challenge\(^22\) in collaboration with industry members, we wrote the following scenario:

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

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

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

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

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

5.3 Core Components of the Reference Architecture

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

- AlertEnterprise Guardian implements provisioning to an RS2 Technologies (RS2) AccessIT! Physical Access Control System (PACS).
TDi Technologies ConsoleWorks and a Schneider Electric Tofino firewall serve as an EACMS.

A RADiFlow ICS/SCADA firewall controls interactions between two Modbus-speaking RTUs—a Schweitzer Engineering Laboratories (SEL) RTU and an RTU emulated by a Raspberry Pi single-board computer.

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

5.3.1 Build #1

Figure 6 illustrates Build #1.

CA Identity Manager implements the IdAM workflow. It receives input from an HR system in the form of comma-separated value (.csv) files. We simulated the HR system using manually produced .csv files. Identity Manager also provisions information to Microsoft Active Directory.
instances in business systems (IT), and the operational system (OT). No relationship among these Active Directory instances is assumed.

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

AlertEnterprise Guardian\(^{23}\) provisions physical access authorizations into the RS2 PACS. CA Identity Minder supports call-outs within a workflow that can be used to invoke external programs. A call-out is used to connect with AlertEnterprise Guardian and provide information to be provisioned to the RS2 PACS.

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

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

\(^{23}\) Guardian is also capable of implementing workflow and provisioning ICS devices. However, those capabilities were not used in this build.
RSA IMG implements the IdAM workflow. It receives input from an HR system in the form of .csv files. RSA IMG also has the capability to provision information to systems. In Build #2, RSA IMG stores information in RSA Adaptive Directory, which subsequently provisions the information to its associated Active Directory instances.

RSA Adaptive Directory implements the identity store and provisioning portions of the example solution. RSA Adaptive Directory is a virtual directory that acts as a proxy in front of multiple back-end directories. The build assumes that each silo—OT, PACS, and IT—hosts a Microsoft Active Directory instance. No relationship among these Active Directory instances is assumed. When an IMG workflow stores information in Adaptive Directory, that information is actually stored in one or more of the underlying Active Directory instances. In this way, storing information in Adaptive Directory provisions that information into one or more Active Directory instances.
AlertEnterprise Guardian provisions physical access authorizations into the RS2 PACS. RSA IMG writes these authorizations into Adaptive Directory, which stores them in the PACS Active Directory instance. AlertEnterprise Guardian monitors the Active Directory PACS instance for updates such as changed physical access authorizations for an existing user, addition of a new user with physical access authorizations, or removal of an existing user and associated access authorizations. When changes are detected, Guardian provisions them into the RS2 PACS.

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

5.3.3 Implementation of the Use Case Illustrative Scenario
This section explains how each of the two builds implements the scenario in Section 5.2

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

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

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

In Build #2, IMG removes the authorizations from Adaptive Directory. This removes the authorizations from the PACS and OT Active Directory instances. AlertEnterprise Guardian detects the change in the PACS Active Directory instance and de-provisions the technician’s substation physical access. ConsoleWorks detects the change in the OT Active Directory instance and de-provisions the technician’s access to the RTU.
Without an active assigned work order, the technician has no physical or logical access to the substation.  

5.4 Supporting Components of the Reference Architecture

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

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

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

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

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

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.

The description of the XTec product and its role supporting the implementation of the example solution was provided to NCCoE by XTec.
GlobalSign operates a North American Energy Standards Board (NAESB)-accredited Software as a Service Certificate Authority. It illustrates an outsourced credential issuance and management capability that provides NAESB-compliant X.509 digital certificates. NAESB-compliant digital certificates are required credentials for authenticating Open Access Same-Time Information Systems (OASIS) transactions and access to the Electronic Industry Registry—the central repository for information related to energy scheduling and management activities in North America.  

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

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

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

---

27 NIST Special Publication 800-162, Guide to Attributed Based Access Control (ABAC) Definition and Considerations.
Ozone Server uses these attributes, in either the OT or IT silo, to decide if a user is allowed to perform a transaction. Ozone Server provides its decision to the policy enforcement point associated with the application.

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

Cisco ISE controls the ability of devices to connect over the network. ISE expands on basic network address-based control to include the identity of the person using a device. ISE is used in the builds to provide a gateway function between OT and IT, limiting which users and devices 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
5.5 Build #3 - An Alternative Core Component Build of the Example Solution

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

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

IT applications are assumed to be integrated with Active Directory and use credential information and authorization information in the IT Active Directory instance. If there are IT
applications that are not integrated with Active Directory, the provisioning capabilities of Guardian would be used to directly provision the applications.

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

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


5.6 Build Implementation Description

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

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

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

<table>
<thead>
<tr>
<th>Product Vendor</th>
<th>Component Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell</td>
<td>PowerEdge R620</td>
<td>Physical server hardware</td>
</tr>
<tr>
<td>Dell</td>
<td>PowerConnect 7024</td>
<td>Physical network switch</td>
</tr>
<tr>
<td>Dell</td>
<td>EqualLogic</td>
<td>Network attached storage</td>
</tr>
<tr>
<td>VMware</td>
<td>vSphere vCenter Server version 5.5</td>
<td>Virtual server and workstation environment</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2012 r2 Active Directory Server</td>
<td>Authentication and authority</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows 7</td>
<td>Information management</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows Server 2012 r2 DNS Server</td>
<td>Domain name system</td>
</tr>
<tr>
<td>Windows</td>
<td>SQL Server</td>
<td>Database</td>
</tr>
<tr>
<td>AlertEnterprise</td>
<td>Enterprise Guardian</td>
<td>Interface and translation between IdAM central store and the PACS management server</td>
</tr>
<tr>
<td>CA Technologies</td>
<td>Identity Manager Rel 12.6.05 Build 06109.28</td>
<td>Identity and access automation management application, IdAM provisioning</td>
</tr>
<tr>
<td>Cisco</td>
<td>ISE Network Server 3415</td>
<td>Network access controller</td>
</tr>
<tr>
<td>Cisco</td>
<td>Catalyst Model 3650</td>
<td>TrustSec-enabled physical network switch</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>Digital Certificates</td>
<td>Cloud certificate authority</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Authority</td>
<td>Central attribute management system</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Console</td>
<td>Ozone administrative management console</td>
</tr>
<tr>
<td>Product Vendor</td>
<td>Component Name</td>
<td>Function</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Envoy</td>
<td>Enterprise identity store interface</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Server</td>
<td>Ozone centralized attribute based authorization server</td>
</tr>
<tr>
<td>RADiFlow</td>
<td>(iSIM) Industrial Service Management Tool</td>
<td>Supervisory control and data acquisition (SCADA) router management application</td>
</tr>
<tr>
<td>RADiFlow</td>
<td>SCADA Router RF-3180S</td>
<td>Router/firewall for SCADA network</td>
</tr>
<tr>
<td>RSA</td>
<td>Adaptive Directory Version 7.1.5</td>
<td>Central identity store, IdAM provisioning</td>
</tr>
<tr>
<td>RSA</td>
<td>IMG Version 6.9 Build 74968</td>
<td>Central IdAM system (workflow management)</td>
</tr>
<tr>
<td>TDi Technologies</td>
<td>ConsoleWorks</td>
<td>Privileged user access controller, monitor, and logging system</td>
</tr>
<tr>
<td>RS2 Technologies</td>
<td>AccessIT! Universal Release 4.1.15 Physical access control components</td>
<td>Configures and monitors the PACS devices (e.g., card readers, keypads, etc.)</td>
</tr>
<tr>
<td>Schweitzer Electronics Laboratory</td>
<td>SEL-2411</td>
<td>Programmable automation controller</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Tofino Firewall model number TCSEFEA23F3F20</td>
<td>Industrial Ethernet firewall</td>
</tr>
<tr>
<td>XTEC</td>
<td>XNode</td>
<td>Remote access control and management</td>
</tr>
</tbody>
</table>

5.6.1 Build Architecture Components Overview

The build architecture consists of multiple networks that mirror the infrastructure of a typical energy industry corporation. The networks are a management network and a production
network (Figure 10). The management network was implemented to facilitate the
implementation, configuration, and management of the underlying infrastructure, including the
physical servers, vSphere infrastructure, and monitoring. The production network, Figure 11
consists of:

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

These networks were implemented separately to match a typical electricity subsector
enterprise infrastructure. Firewalls block all traffic except required internetwork
communications. The primary internetwork communications are the user access and
authorization updates from the central IdAM systems between the directories and OT, PACS,
and IT networks.
Figure 10. Management and production networks
The IdAM network represents the proposed centralized/converged IdAM network/system. This network was separated into OT, PACS, and IT to highlight the unique IdAM components proposed to address the use case requirements.

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

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

The PACS network represents the network that supports the physical access control systems across the enterprise. Typically, this network uses the enterprise IT network and is segmented from the user networks by virtual local area networks (VLANs). In our architecture, a firewall...
allows limited access to and from the PACS network to facilitate the communication of access
and authorization information. Technically, this communication consists of user role and
responsibility directory updates originating in the IdAM system.

5.6.2 Build Network Components

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

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

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

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

5.6.3 Operational Technology Network

The builds include the following OT network components:

- directory instance
- OT management workstation
- RTU with IP interface
- RTU with serial interface
- ICS/SCADA router
- router management workstation
- ICS/SCADA gateway/access control system

This network emulates an energy enterprise OT network and systems. The specific vendor
products used in this network are identified in Table 3 and Figure 12. OT network.
In the OT network, the RADiFlow router performs the ICS/SCADA network firewall function. The ConsoleWorks product provides the access control/gateway function. The build used the gateway function to manage access to the OT router and RTU management/console interface. The interface can be used to configure the RTU as well as issue real-time function commands (e.g., open/close relays). The access control/gateway uses the OT directory to obtain access authority for each user requesting access to an RTU.

5.6.4 Information Technology Network

The builds include the following IT network components:

- Active Directory
- Cisco ISE
- TrustSec switch
- Workstation

A typical enterprise includes information-sharing systems, email, and application servers. We did not include these systems in the architecture because they are not needed to demonstrate
the effectiveness of the IdAM example solution. The specific vendor products used in this network are identified in Table 3 and Figure 13.

Figure 13. IT network

5.6.5 Physical Access and Control System Network

The builds include the following PACS network components:

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

This network emulates a typical enterprise PACS. The specific vendor products used in this network are identified in Table 3 and Figure 14.
Two technologies are demonstrated in the PACS network: XTEC XNode and RS2 Technologies AccessIT!. XTEC XNode is a physical access system using smart card readers, pin pads, and an Internet cloud-based authorization service. The cloud service can federate (interoperate) with corporate identity and access stores or can be operated as a fully outsourced PACS IdAM solution. The RS2 Technologies system includes card readers, pin pads, and the AccessIT! local management server. The local management server is integrated with the central identity and access store via the AlertEnterprise Guardian product. In Build #1, Guardian receives IdAM data directly from Identity Manager. Once the information is received, Guardian provisions the information to the PACS management server. In Build #2, Guardian monitors the PACS directory for IdAM changes. Once changes are identified, Guardian collects the information and provisions the IdAM information to the PACS management server.

5.6.6 Identity and Access Management Network

5.6.6.1 Build #1

Build #1 includes the following IdAM network components:
The IdAM was separated to highlight the unique IdAM components proposed to address the use case requirements. The implementation is not a recommendation to separate IdAM functions on their own network. The products used in this build are identified in Table 3 and Figure 15. Central IdAM network.

Identity and Access Management Area

![Central IdAM network, Build #1](image)

The central IdAM system is the authoritative central store for identity and access authorization data. CA Identity Manager provides central identity and access store as well as workflow management capability in Build #1 (see Figure 15). The central IdAM system takes over control of the directory instances in each silo. The control is implemented by providing an administrative account credential for each managed directory to the IdAM system. This is an important aspect of the implementation. When the administrative credential is issued, the organization must limit access to the managed directories of the IdAM system to a reduced...
number of administrative users. The security of the solution partially depends on limited access to the managed directories, as discussed in Section 5.9.6, Security Recommendations.

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

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

5.6.6.2 Build #2

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

Central IdAM network, Build #2.
The central IdAM systems are the authoritative central store for identity and access authorization data. RSA IdAM products and AlertEnterprise provide central identity and access stores as well as workflow management capability. The central IdAM system takes over control of the directory instances in each silo. The control is implemented by providing an administrative account credential for each managed directory to the IdAM system. This is an important aspect of the implementation. When the administrative credential is issued, the organization must limit the access to the managed directories of the IdAM system to a reduced number of administrative users. The security of the solution partially depends on limited access to the managed directories, as discussed in Sections 5.9.6.

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

In this build, Guardian was used to integrate the IdAM system with the PACS access management system (AccessIT!). Guardian includes integration and translation capabilities to transfer the IdAM data to AccessIT! Guardian monitors the PACS directory for IdAM updates.
The MAG Ozone product provides secure attribute distribution within the enterprise. Section 5.4 describes its use.

5.6.7 Access Authorization Information Flow and Control Points

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

5.6.7.1 OT Access and Authorization Information Flow

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

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

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

PACS Access and Authorization Information Flow

The PACS access and authorization information flows in each build are described below.
Figure 18. Access and authorization information flow for the PACS network, Build #1

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

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

IT Network Identity Access and Management

All messages traverse the DMZ between networks

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

5.7 Data

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

The example solution both impacts and is impacted by the requirement to conform to NERC-CIP standards.\(^\text{29}\)

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

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

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

<table>
<thead>
<tr>
<th>NERC-CIP Requirement</th>
<th>IdAM Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP 004-3a Maintain a list of individuals with logical or unescorted physical access to Critical Cyber Assets.</td>
<td>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.</td>
</tr>
<tr>
<td>CIP 004-3a Conduct a cybersecurity training program for individuals with logical or unescorted physical access to Critical Cyber Assets.</td>
<td>The IdAM workflow can be configured to check a training system before granting access to critical cyber assets.</td>
</tr>
<tr>
<td>CIP 004-3a Conduct personnel risk</td>
<td>The IdAM workflow can be configured to</td>
</tr>
</tbody>
</table>

\(^{29}\) 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.

<table>
<thead>
<tr>
<th>NERC-CIP Requirement</th>
<th>IdAM Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment. Individuals must have an acceptable risk assessment before being granted access to Critical Cyber Assets.</td>
<td>verify that individuals have an acceptable risk assessment before granting access to critical cyber assets.</td>
</tr>
<tr>
<td><strong>CIP 004-3a</strong> A list of all personnel with logical or unescorted physical access to Critical Cyber Assets must be maintained.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>CIP 004-3a</strong> Personnel with logical or physical access to Critical Cyber Assets must have that access removed within 24 hours if terminated for cause and within 7 days otherwise.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>CIP 005-3</strong> requires documentation of the process for authorizing access in accordance with NERC CIP 004-3.</td>
<td>The IdAM workflow is the process for authorizing access. The workflow design and implementation documents the process.</td>
</tr>
</tbody>
</table>

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

5.9 Evaluation of Security Characteristics

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

5.9.1 Scope

The evaluation included analysis of the example solution to identify weaknesses, discuss mitigations, and understand benefits and trade-offs.
We considered the following elements of the IdAM example solution:

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

The following elements of the example solution were not considered:

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

This security characteristic evaluation has the following limitations:
• The evaluation examines the security claims made by the example solution; however, it is not a comprehensive test of all security components.

• The evaluation cannot identify all weaknesses. Its purpose is to verify that the example solution meets its security claims, and to understand the trade-offs involved in doing so.

• This is not a red team exercise. The intent was to verify the security claims, not to break hardware or software involved in the example solution.

• The lab routers and firewalls were not included in the evaluation. It is assumed that they are hardened. Testing these devices would reveal only weaknesses in implementation that would not be of value to those adopting this example solution.

5.9.3 Example Solution Analysis

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

Table 5. IdAM Components and Security Capability Mapping

<table>
<thead>
<tr>
<th>Component</th>
<th>Specific Product</th>
<th>Function</th>
<th>Security Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity, Authorization, and Workflow Manager</td>
<td>RSA IMG</td>
<td>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.</td>
<td>Authentication and authorization</td>
</tr>
<tr>
<td></td>
<td>Or CA Identity Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Store</td>
<td>RSA Adaptive Directory (identity Store), which is used with RSA IMG Or Windows SQL 2012, which is used with CA Identity Manager</td>
<td>Database of user identities</td>
<td>Authentication and authorization</td>
</tr>
<tr>
<td>High Assurance Attribute Service (AAS)</td>
<td>MAG Ozone System</td>
<td>Access control solution with ABAC architecture; provides increased assurance by signing attributes with private key infrastructure (PKI) and requiring users to authenticate with PKI</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Specific Product</td>
<td>Function</td>
<td>Security Characteristic</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>----------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Translator between Active Directory and PACS and OT Access Management Systems (AMS)</td>
<td>AlertEnterprise Guardian</td>
<td>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</td>
<td>Authorization, access control</td>
</tr>
<tr>
<td>Directory Service</td>
<td>MS Active Directory (for IT devices) Or RS2 PACS Server (for PACS devices)</td>
<td>Database of PACS or IT resource and user identifiers and their associated security policies</td>
<td>Authentication and authorization</td>
</tr>
<tr>
<td>SCADA Router and Remote Manager (RM) of SCADA Router</td>
<td>RADiFlow</td>
<td>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</td>
<td>Access control</td>
</tr>
<tr>
<td>Network Access Control (AC) and Policy Enforcement System (PES)</td>
<td>Cisco ISE</td>
<td>Allows access policies for network endpoints to be controlled centrally</td>
<td>Network security</td>
</tr>
<tr>
<td>Stand-alone Smartcard Provisioning (SP) and Access System (AS)</td>
<td>XTEC</td>
<td>Smartcard-based physical access control</td>
<td>Authentication, authorization, access control</td>
</tr>
</tbody>
</table>

5.9.4 Security Characteristics Addressed

One aspect of our security evaluation involved assessing how well the IdAM example solution addresses the security characteristics that it was intended to support. These security characteristics are listed in a security control map published in the appendix of the IdAM use case description (http://nccoe.nist.gov/sites/default/files/ncco/NCCoE_ES_Identity_Access_Management.pdf). Six security characteristics are listed, each of which is further classified by the Cybersecurity Framework (CSF) categories and subcategories to which they map. The CSF subcategories further map to specific sections of each standard and best practice cited in the CSF in reference to that subcategory. Figure 21 depicts an example of the process.
We used the CSF subcategories to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to that subcategory. The cited sections provide example solution validation points by listing specific traits that a solution that supports the desired security characteristics should exhibit. Using the CSF subcategories as a basis for organizing our analysis and consulting the specific sections of the security standards that are cited with respect to each subcategory allowed us to systematically consider how well the example solution supports the security characteristics identified in the use case description.

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

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

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

5.9.4.1 Authentication, Access Control, and Authorization for OT

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

5.9.4.2 Centrally Monitor Use of Accounts

The example solution supports centralized accountability and tracking of user accounts, with the IdAM identity, authorization, and workflow manager acting as the locus of this capability. On the OT network, the console access manager, which acts as the gatekeeper to all ICS/SCADA devices, monitors and logs all ICS/SCADA access requests and responses, as well as all user interactions with the ICS/SCADA OT devices. These logs should be centrally monitored along with other ICS/SCADA OT monitoring within the enterprise.

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

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

5.9.4.3 Protect Exchange of Identity and Access Information

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

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

Because of time constraints, the laboratory builds of the example solution did not include encryption or integrity assurance for every IdAM information exchange. Nevertheless, such protection is strongly recommended when deploying the example solution.
5.9.4.4 Provision, Modify, or Revoke Access

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

5.9.5 Assessment of Reference Architecture

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

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

5.9.5.1 Threats, Vulnerabilities, and Assumptions

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

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

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

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

_______________________________

35 Section 4.3.2 describes the risks associated with access to the IdAM workflow.
5.9.5.1.2. Logging Activity on IdAM Components

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

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

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

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

Access to the identity store on the IdAM network must also be strictly controlled, and the identity store should be configured so that it will only perform addition, modification, and deletion requests received from the identity, authorization, and workflow manager. If the identity store were to accept updates or edits from another entity, the result could be catastrophic. Any updates made by an administrator would have to be made via machine
console, so at least these would be logged. Updates made by a super-administrator could escape detection if the super-administrator were to defy organization policy and access the identity store console without going through the console access manager. We acknowledge insider threats but feel that mitigating the risk of insider threats presently relies more on organizational policy decisions rather than technology. Therefore, addressing insider threat is outside the scope of this project.

5.9.5.1.3. Unauthorized Modification of Access and Authorization Information

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

5.9.5.2 Mitigations: Essentials for Securing the IdAM Example Solution

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

- securing access to the
  - identity, authorization, and workflow manager, identity store, and network access control components on the IdAM network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)
  - directory service and console access manager components on the OT network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)
  - IT network access control switch that serves as a gateway to the OT network

- protecting the integrity of the information exchanged between the
  - identity manager and the identity stores
  - identity store and the directory service on the OT network
  - directory service and the console access manager components on the OT network, as well as the network access control and policy enforcement system within the IT network
  - network access control component identity stores
  - network access control component on the IT network and the IT network access control switch that serves as a gateway to the OT network
Based on the information flows for supporting PACS authentication, PACS access control, and PACS authorization described in Section 5.6.7 securing the part of the IdAM example solution that supports PACS access control requires:

- securing access to the
  - identity, authorization, and workflow manager; identity store; and IdAM translator components on the IdAM network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)
  - IdAM identity store and PACS directory service components on the PACS network (i.e., ensuring that only authorized users can access and add, modify, or delete information on these components)

- protecting the integrity of the information exchanged between the
  - identity manager and identity stores
  - identity store on the IdAM network and the PACS directory service on the PACS network
  - IdAM translator component on the IdAM network and the IdAM directory service on the PACS network
  - IdAM translator component on the IdAM network and the PACS management server on the PACS network

5.9.5.3 Trade-offs

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

5.9.5.3.1 Benefits

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

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

- Conduct their own evaluations of their example solution implementation.
- Deploy all components on securely configured operating systems that use multifactor authentication and are configured according to best practices.  
- Ensure that all operating systems on which example solution implementation components are running are hardened, maintained, and kept up-to-date in terms of patching, version control, and virus and malware detection.
- Put into place a security infrastructure that will protect the example solution itself and secure the communications among the components on the IdAM network and between these components and the IdAM components on the other three networks, as described in Section 5.9.5.2. Many of the remaining recommendations relate to providing such a security infrastructure.
- Design the authorization and workflow policies that are enforced by the identity, authorization, and workflow manager component to enforce the principle of least privilege and separation of duties.
- Design the authorization and access control policies that govern user access to the IdAM components themselves to enforce the principle of least privilege and separation of duties.
- Segregate IdAM components onto their own network, either physically or using private VLANs and port-based authentication or similar mechanisms.  
- Deploy a security infrastructure to secure the IdAM network and the IdAM platforms themselves. This infrastructure must consist of a holistic set of components that work together to prevent the IdAM network, components, and workflow from being used as an attack vector.
- Protect the IdAM network using security components such as firewalls and intrusion 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.
• 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:
  o Perform all information exchange to/from the directory services in each of the OT, PACS, and IT, networks in protected mode.
  o 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.
  o 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.
  o 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
when accessing the console of all devices on the IdAM network and never to access any console directly. Use of a console access manager ensures that all activity performed via the console is logged.

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

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

5.9.7 Security Characteristics Evaluation Summary

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

6 Functional Evaluation

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

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

Section 6.1 explains the functional test plan in more detail and lists the procedures used for each of the functional tests.
6.1 IdAM Functional Test Plan

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

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

<table>
<thead>
<tr>
<th>Test Case Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent requirement</td>
<td>Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.</td>
</tr>
<tr>
<td>Testable requirement</td>
<td>Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.</td>
</tr>
<tr>
<td>Associated Security Controls</td>
<td>The NIST SP 800-53 rev 4 controls addressed by the test case.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the objective of the test case.</td>
</tr>
<tr>
<td>Associated test cases</td>
<td>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.</td>
</tr>
<tr>
<td>Preconditions</td>
<td>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</td>
</tr>
<tr>
<td>Procedure</td>
<td>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.</td>
</tr>
<tr>
<td>Expected results</td>
<td>The specific expected results for each variation in the test procedure.</td>
</tr>
<tr>
<td>Actual results</td>
<td>The actual observed results in comparison with the documented expected results.</td>
</tr>
</tbody>
</table>
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.

6.2 IdAM Use Case Requirements

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

Table 7. IdAM Functional Requirements

<table>
<thead>
<tr>
<th>Capability Requirement (CR) ID</th>
<th>Parent Requirement</th>
<th>Sub-requirement 1</th>
<th>Sub-requirement 2</th>
<th>Test Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR 1</td>
<td>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:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 1.a</td>
<td>IT</td>
<td>Allow access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.a.1</td>
<td></td>
<td>Allow access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.a.2</td>
<td></td>
<td>Deny access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.b</td>
<td>OT</td>
<td>Allow access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.b.1</td>
<td></td>
<td>Allow access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.b.2</td>
<td></td>
<td>Deny access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.c</td>
<td>PACS</td>
<td>Allow access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.c.1</td>
<td></td>
<td>Allow access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 1.c.2</td>
<td></td>
<td>Deny access</td>
<td></td>
<td>IdAM-1</td>
</tr>
<tr>
<td>CR 2</td>
<td>The IdAM system shall include an IdAM workflow capability that can create and activate new users in the following networks and systems:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 2.a</td>
<td>IT</td>
<td></td>
<td></td>
<td>IdAM-2</td>
</tr>
<tr>
<td>CR 2.b</td>
<td>OT</td>
<td></td>
<td></td>
<td>IdAM-2</td>
</tr>
<tr>
<td>CR 2.c</td>
<td>PACS</td>
<td></td>
<td></td>
<td>IdAM-2</td>
</tr>
<tr>
<td>CR 3</td>
<td>The IdAM system shall include an IdAM workflow capability that can de-activate users in the following networks and systems:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 3.a</td>
<td>IT</td>
<td>IdAM-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 3.b</td>
<td>OT</td>
<td>IdAM-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 3.c</td>
<td>PACS</td>
<td>IdAM-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4</td>
<td>The IdAM system shall include a workflow capability that can change an existing user access to the various networks and systems.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.a</td>
<td>IT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.a.1</td>
<td>Allow to deny</td>
<td>IdAM-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.a.2</td>
<td>Deny to allow</td>
<td>IdAM-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.b</td>
<td>OT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.b.1</td>
<td>Allow to deny</td>
<td>IdAM-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.b.2</td>
<td>Deny to allow</td>
<td>IdAM-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.c</td>
<td>PACS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.c.1</td>
<td>Allow to deny</td>
<td>IdAM-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR 4.c.2</td>
<td>Deny to allow</td>
<td>IdAM-3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 6.3 Test Case: 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**

AC-2, AC-3, IA-2, PE-2, PE-3

**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)

<table>
<thead>
<tr>
<th>Network Access Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users with allowed access are able to log into a workstation on the IT network.</td>
</tr>
<tr>
<td>Users with allowed access are able to log into a workstation on the OT network as well as the SEL RTU and RTU emulator.</td>
</tr>
<tr>
<td>Users with allowed access are able to log into a workstation on the PACS network.</td>
</tr>
<tr>
<td>Users with allowed access are authorized and allowed access by the PACS card reader and door access demonstration system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Access Denied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users who are denied access to the IT network are unable to log into a workstation on the IT network.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Users who are denied access PACS network are unable to log into a workstation on the PACS network.</td>
</tr>
<tr>
<td>Users without access are not authorized and not allowed access by the PACS</td>
</tr>
</tbody>
</table>
card reader and door access demonstration system.

<table>
<thead>
<tr>
<th>Actual results</th>
<th>This test functioned appropriately and provided the expected results. Users 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall result</td>
<td>Pass</td>
</tr>
</tbody>
</table>
## Test Case 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)

<table>
<thead>
<tr>
<th>Testable requirement</th>
<th>(CR 2.a) IT, (CR 2.b) OT, (CR 2.c) PACS</th>
<th>(CR 3.a) IT, (CR 3.b) OT, (CR 3.c) PACS</th>
</tr>
</thead>
</table>

**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**

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...
At a PACS card reader, attempt an “access” with a card for a new user known to have access allowed.

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.

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.

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.

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.

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.

<table>
<thead>
<tr>
<th>Expected results (pass)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(CR 2) Create and activate a new user.</td>
</tr>
<tr>
<td>New users are created and access to the three networks and systems is confirmed.</td>
</tr>
<tr>
<td>(CR 2.a) IT</td>
</tr>
<tr>
<td>(CR 2.b) OT network, SEL RTU and RTU emulator</td>
</tr>
<tr>
<td>(CR 2.c) PACS network and demonstration card reader access system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actual results</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
</tr>
</tbody>
</table>
access was deactivated and the deactivation approved. The users were no longer able to access the OT, PACS, or IT.

| Overall result | Pass |

### 6.5 Test Case 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.

<table>
<thead>
<tr>
<th>Expected results (pass)</th>
<th>(CR 4.) Change user access.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(CR 4.a) IT</td>
</tr>
<tr>
<td></td>
<td>(CR 4.a.1) Allow-to-deny changes are successfully provisioned.</td>
</tr>
<tr>
<td></td>
<td>(CR 4.a.2) Deny-to-allow changes are successfully provisioned.</td>
</tr>
<tr>
<td></td>
<td>(CR 4.b) OT</td>
</tr>
</tbody>
</table>
(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
# APPENDIX A: ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Literal Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAC</td>
<td>Attribute-Based Access Control</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>CA</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>CR</td>
<td>Capability Requirement</td>
</tr>
<tr>
<td>CSF</td>
<td>Cybersecurity Framework</td>
</tr>
<tr>
<td>.csv</td>
<td>Comma-Separated Value</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>EACMS</td>
<td>Electronic Access Control and Monitoring System</td>
</tr>
<tr>
<td>EAP</td>
<td>Electronic Access Point</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>ESP</td>
<td>Electronic Security Perimeter</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>ID</td>
<td>Identity</td>
</tr>
<tr>
<td>IdAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IMG</td>
<td>Identity Management and Governance</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISE</td>
<td>Identity Services Engine</td>
</tr>
<tr>
<td>LDAPS</td>
<td>Lightweight Directory Access Protocol Secure</td>
</tr>
<tr>
<td>MAG</td>
<td>Mount Airey Group</td>
</tr>
<tr>
<td>Acronym</td>
<td>Literal Translation</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>NAESB</td>
<td>North American Energy Standards Board</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NCCoE</td>
<td>National Cybersecurity Center of Excellence</td>
</tr>
<tr>
<td>NERC</td>
<td>North American Electric Reliability Corporation</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control System</td>
</tr>
<tr>
<td>PIV-I</td>
<td>Personal Identity Verification Interoperable</td>
</tr>
<tr>
<td>PKI</td>
<td>Private Key Infrastructure</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>STIG</td>
<td>Security Technical Implementation Guideline</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>

**APPENDIX B: REFERENCES**


The Personal Profile Application (PPA) was developed by Mount Airey Group, Inc. in order to demonstrate the functionality of the Ozone® Suite of products. Ozone® implements atomic authorization for the protection of critical resources by cryptographically binding credentials to specific authorizations, access rights, and/or explicit privileges; as well as provides a privacy protecting mechanism that allows these authorizations to be distributed across the enterprise — as close to the protected resource as necessary — without concern for tampering, data mining, or compromise; and is meant to protect an organizations most sensitive or highest risk resources. If an application relies on PKI-based smart cards and/or biometrics for authentication, then that system should implement the congruent security for the authorization of users for access to that resource as is provided by Ozone®.

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

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

In order to bring up the demonstration application, the user must present a digital certificate to the application. Upon inspection of the authorizations provisioned within Ozone® for the
selected certificate, the application dynamically populates the table at the bottom of the first screen with the results of the authorization queries. If the certificate has been authorized for a specific action, then the results table will display “true” for that specific action. The information identifying the certificate that was selected is also displayed above the table.

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

- View Personal Information – View the personal information of the selected person.
- Edit Personal Information – Add or edit the personal information of people in the application.
- View Criminal History – View the criminal history of the selected person.
- Edit Criminal History – Add or edit the criminal history of people in the application.
- View Credit Report – View the credit report of the selected person.
- Request a New Credit Report – Request an updated credit report for the selected person.

**Sample First Page Table:**

<table>
<thead>
<tr>
<th>PPA Proof</th>
<th>Authorized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Criminal History</td>
<td>true</td>
</tr>
<tr>
<td>Edit Personal Information</td>
<td>false</td>
</tr>
<tr>
<td>Request Credit Report</td>
<td>false</td>
</tr>
<tr>
<td>View Credit Report</td>
<td>false</td>
</tr>
<tr>
<td>View Criminal History</td>
<td>true</td>
</tr>
<tr>
<td>View Personal Information</td>
<td>false</td>
</tr>
</tbody>
</table>

**Sample Search Results Page Table:**
Search Results:

<table>
<thead>
<tr>
<th>Name</th>
<th>View CH</th>
<th>Add CH</th>
<th>View CR</th>
<th>Request CR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hicks, Chick</td>
<td>View</td>
<td>Add</td>
<td>View</td>
<td>Request</td>
</tr>
<tr>
<td>McQueen, Lightning</td>
<td>View</td>
<td>Add</td>
<td>View</td>
<td>Request</td>
</tr>
<tr>
<td>Sullivan, James P</td>
<td>View</td>
<td>Add</td>
<td>View</td>
<td>Request</td>
</tr>
<tr>
<td>Waternoose, Henry J</td>
<td>View</td>
<td>Add</td>
<td>View</td>
<td>Request</td>
</tr>
</tbody>
</table>

Add a new entry...[editPie.jsp]

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

**Jim McCarthy**

Email Address = james.mccarthy@nist.gov, CN = James McCarthy, OU = GSUS, OU = NCCoE NIST
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

**Donald Faatz**

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

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

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

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
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 (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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jasvir Gill</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Srini Kakkera</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Srinivas Adepu</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Pan Kamal</td>
<td>AlertEnterprise</td>
</tr>
<tr>
<td>Mike Dullea</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Ted Short</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Alan Zhu</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Name</td>
<td>Company</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Peter Romness</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Lila Kee</td>
<td>GlobalSign</td>
</tr>
<tr>
<td>Sid Desai</td>
<td>GlobalSign</td>
</tr>
<tr>
<td>Paul Townsend</td>
<td>Mount Airey Group (MAG)</td>
</tr>
<tr>
<td>Joe Lloyd</td>
<td>Mount Airey Group (MAG)</td>
</tr>
<tr>
<td>Ayal Vogel</td>
<td>RADiFlow</td>
</tr>
<tr>
<td>Dario Lobozzo</td>
<td>RADiFlow</td>
</tr>
<tr>
<td>Steve Schmalz</td>
<td>RSA</td>
</tr>
<tr>
<td>Tony Kroukamp (The SCE Group)</td>
<td>RSA</td>
</tr>
<tr>
<td>Kala Kinyon (The SCE Group)</td>
<td>RSA</td>
</tr>
<tr>
<td>Dave Barnard</td>
<td>RS2 Technologies</td>
</tr>
<tr>
<td>David Bensky</td>
<td>RS2 Technologies</td>
</tr>
<tr>
<td>Rich Gillespie (IACS Inc.)</td>
<td>RS2 Technologies</td>
</tr>
<tr>
<td>George Wrenn</td>
<td>Schneider Electric</td>
</tr>
<tr>
<td>Michael Pyle</td>
<td>Schneider Electric</td>
</tr>
<tr>
<td>Bill Johnson</td>
<td>TDi Technologies</td>
</tr>
<tr>
<td>Pam Johnson</td>
<td>TDi Technologies</td>
</tr>
<tr>
<td>Clyde Poole</td>
<td>TDi Technologies</td>
</tr>
<tr>
<td>Danny Vital</td>
<td>XTeC</td>
</tr>
</tbody>
</table>
# 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
1 | NIST Cybersecurity Practice Guide SP 1800-2c

1 INTRODUCTION

1.1 PRACTICE GUIDE STRUCTURE

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

This guide contains three volumes:

- NIST SP 1800-2a: Executive Summary
- NIST SP 1800-2c: How To Guides – instructions for building the example solution

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

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

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

These guides assume that the people using this document have experience implementing information technology security products (including systems integration and administration of networked Windows and Linux systems, firewalls, routers, etc.) in an electricity subsector organization. While we have used the commercially available products described here, we assume that you have the knowledge and expertise to choose other products that might better 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.
products that are congruent with standards and best practices, as we have. Refer to NIST SP 1800-2b: Approach, Architecture, and Security Characteristics, Section 4.5, Table 2, for a list of the products that we used, mapped to the cybersecurity controls provided by this example solution, to understand the characteristics you should seek in alternate products. Section 4.4 Security Characteristics and Controls Mapping, of that document describes how we arrived at this list of controls.

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. In addition, this document was reviewed by the NERC ES-ISAC to ensure that the approach was informed by standards and NERC regulations.

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. This NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a draft version. We are seeking feedback on its contents and welcome your input. Comments and suggestions will improve subsequent versions of this guide. Please contribute your thoughts to energy_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/energy.

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

1.2 CONVENTIONS

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

   filename.conf

http://nccoe.nist.gov

Commands and status codes are in Courier:

   mkdir

Code that a user inputs is in Garamond bold:

   service sshd start
2 BUILD OVERVIEW

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

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

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

<table>
<thead>
<tr>
<th>Product Vendor</th>
<th>Component</th>
<th>Function</th>
<th>Implementation (physical device or virtual environment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell</td>
<td>PowerEdge R620</td>
<td>Server hardware</td>
<td>Physical device</td>
</tr>
<tr>
<td>Dell</td>
<td>PowerConnect 7024</td>
<td>Network switch</td>
<td>Physical device</td>
</tr>
<tr>
<td>Dell</td>
<td>EqualLogic</td>
<td>Network attached storage</td>
<td>Physical device</td>
</tr>
<tr>
<td>VMware</td>
<td>vSphere vCenter Server version 5.5</td>
<td>Virtual server and workstation environment</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2012 r2 Active Directory Server</td>
<td>Authentication and authority</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows 7</td>
<td>Information management</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows Server 2012 r2 DNS Server</td>
<td>Domain name system</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Windows</td>
<td>SQL Server</td>
<td>Database</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Product Vendor</td>
<td>Component</td>
<td>Function</td>
<td>Implementation (physical device or virtual environment)</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>AlertEnterprise</td>
<td>Enterprise Guardian</td>
<td>Interface and translation between IdAM central store and the PACS management server</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>CA Technologies</td>
<td>Identity Manager Rel 12.6.05 Build 06109.28</td>
<td>Identity and access automation management application, IdAM provisioning</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Cisco</td>
<td>ISE Network Server 3415</td>
<td>Network access controller</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Cisco</td>
<td>Catalyst 3550</td>
<td>Network switch</td>
<td>Physical device</td>
</tr>
<tr>
<td>Cisco</td>
<td>Catalyst 3650</td>
<td>TrustSec-enabled physical network switch</td>
<td>Physical device</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>SSL Certificate</td>
<td>Cloud certificate and registration authority</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Authority</td>
<td>Central attribute management system</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Console</td>
<td>Ozone administrative management console</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Envoy</td>
<td>Enterprise identity store interface</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>Mount Airey Group</td>
<td>Ozone Server</td>
<td>Ozone centralized attribute based authorization server</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>RADiFlow</td>
<td>Industrial Service Management Tool (iSIM)</td>
<td>Supervisory control and data acquisition (SCADA) router management application</td>
<td>Physical device</td>
</tr>
<tr>
<td>Product Vendor</td>
<td>Component</td>
<td>Function</td>
<td>Implementation (physical device or virtual environment)</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>RADiFlow</td>
<td>SCADA Router RF-3180S</td>
<td>Router/firewall for SCADA network</td>
<td>Physical device</td>
</tr>
<tr>
<td>RSA</td>
<td>Adaptive Directory Version 7.1.5</td>
<td>Central identity store, IdAM provisioning</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>RSA</td>
<td>IMG Version 6.9 Build 74968</td>
<td>Central IdAM system (workflow management)</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>TDi Technologies</td>
<td>ConsoleWorks</td>
<td>User access controller, monitor, and logging system</td>
<td>Virtual environment</td>
</tr>
<tr>
<td>RS2 Technologies</td>
<td>AccessIT! Universal Release 4.1.15</td>
<td>Configures and monitors the PACS devices (e.g., card readers, keypads)</td>
<td>Virtual environment server and physical device card reader</td>
</tr>
<tr>
<td>Schweitzer Electronics Laboratory</td>
<td>SEL-2411</td>
<td>Remote Terminal Unit (RTU)</td>
<td>Physical device</td>
</tr>
<tr>
<td>Schneider Electric</td>
<td>Tofino Firewall model number TCSEFEA23F3F20</td>
<td>Ethernet/IP firewall</td>
<td>Physical device</td>
</tr>
<tr>
<td>XTEC</td>
<td>Xnode</td>
<td>Remote access control and management</td>
<td>Physical device</td>
</tr>
</tbody>
</table>

2.1 BUILD IMPLEMENTATION OVERVIEW

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

- the demilitarized zone (DMZ)
• Identity and Access Management - IdAM
• IT - business management system
• OT - ICS/SCADA industrial control system and energy management system (EMS)
• PACS – physical access control system networks

These networks were implemented separately to match a typical electric utility enterprise infrastructure. Firewalls are configured to route traffic and limit access among the production networks to block all traffic except required inter-network communications. The primary inter-network communications are the user access and authorization updates from the central IdAM systems to and from the directories and PACS, IT, and OT networks. The DMZ provides a protected neutral network space that the other networks of the production network can use to route traffic to and from the Internet or each other.
Figure 1. Management and production networks
The IdAM network represents the proposed centralized/converged IdAM network/system. This network was separated to highlight the unique IdAM components proposed to address the use case requirements.

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

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

The PACS network represents the network used to support the physical access control systems across the enterprise. Typically, this network uses the enterprise IT network and is segmented.
from the user networks via virtual local area networks (VLANs). In our architecture, a firewall is configured to allow limited access to and from the PACS network to facilitate the communication of access and authorization information. Technically, this communication consists of user role and responsibility directory updates originating in the IdAM system.

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

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

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

2.2 BUILD IMPLEMENTATION DESCRIPTIONS

Figure 3 depicts the build network comprising the management, VendorNet, IdAM, DMZ, IT, OT, and PACS subnetworks. VendorNet provides remote access for vendors to access, configure, demonstrate, and provide training for each of the implemented products. The IdAM network contains the central IdAM components of the build (described below). The IT, OT, and PACS networks contain the representative components of a typical electric utility enterprise, as described below.
The IdAM network (Figure 4 and Figure 5) contains the central IdAM components for Build #1 and Build #2. The IdAM components are placed into a separate network to highlight the importance of protecting these assets and to simplify the demonstration of their capabilities.
Build #1 uses the CA Identity Manager product for the IdAM system and identity store.
Figure 5. Build #2 IdAM Network
Build #2 uses the RSA IMG and Adaptive Directory products for the IdAM system and identity store.

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

The OT network (Figure 7) contains the OT components, which include representative components found in electric utility OT networks/systems. These components were chosen to demonstrate the integration capabilities of the central IdAM capability. The lab did not attempt to replicate a fully operational OT network or set of systems. Because we had a limited number of remote terminal units (RTUs) available, we used Raspberry Pi on the network to emulate an RTU.
Figure 7 OT Network
The PACS network (Figure 8) contains the PACS components, which include representative components found in electric utility physical access control systems. These components were chosen to demonstrate the integration capabilities of the central IdAM capability.

Physical Access Control Area

Figure 8 PACS Network
### 2.3 IP NETWORK ADDRESS ASSIGNMENTS

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

**Table 2 Build IP Address Assignments**

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

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

### 3 BUILD INFRASTRUCTURE

#### 3.1 OPERATING SYSTEMS

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

- Windows 7 enterprise
- Windows server 2008 R2
- Windows server 2012 R2
- MicroFocus SUSE Linux Enterprise Server 11
- CentOS 7.

#### 3.1.1 Windows Installation and Hardening Details

The NCCoE Windows OS images are derived from the Department of Defense (DoD) Security Technical Implementation Guide (STIG) images. The Windows systems were installed using installation files provided by the Defense Information Systems Agency (DISA). These images were chosen because they are standardized, hardened, and fully documented. The STIG guidelines are available on-line at [http://iase.disa.mil/stigs/os/Pages/index.aspx](http://iase.disa.mil/stigs/os/Pages/index.aspx).
Modifications to the STIG compliant OS configurations were required for each product to enable its operation. The compliance results in Section 17 identify the specific OS configuration modifications (noncompliant configuration items) needed in each case.

### 3.1.2 SUSE Linux Enterprise Server 11 Installation and Hardening Details
The SUSE OS was included as part of the virtual appliance image provided by RSA for the IMG product. The center did not make any OS configuration changes. The OS was not configured to meet the DoD CentOS 6 STIG. The STIG guidelines are available on-line at [http://iase.disa.mil/stigs/os/Pages/index.aspx](http://iase.disa.mil/stigs/os/Pages/index.aspx). The OS configurations for SUSE Linux implementation are listed in Section 17. The compliance results report for SUSE Linux is included for illustration purposes, Section 20.2.

### 3.1.3 Base Linux Installation and Hardening Details
The NCCoE base Linux OS used in the build is CentOS 7. This OS is available as an open source image. The OS was configured to meet the DoD CentOS 6 STIG, because no CentOS 7 STIG was available at the time the build was implemented. The STIG guidelines are available on-line at [http://iase.disa.mil/stigs/os/Pages/index.aspx](http://iase.disa.mil/stigs/os/Pages/index.aspx). The OS configurations for each Linux implementation are listed in section 17. The compliance results reports identify the configuration items that do not conform to the STIG configuration guide.

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

The following firewall configurations include the rules that were implemented in each of the firewalls for the build implementation. These configurations are provided to enable the reader to reproduce the traffic filtering/blocking that was achieved in the build implementation.
### Table 3. Border Firewall Rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualInfra</td>
<td>10.32.2.10-12</td>
<td>Virtualization Systems for Build</td>
</tr>
<tr>
<td>VPNserver</td>
<td>172.16.7.253</td>
<td>VPN Server</td>
</tr>
</tbody>
</table>

#### WAN Interface

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>10.32.2.0/25</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow all management network traffic</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>10.255.2.0/25</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Center VPN to all systems</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>WAN Address</td>
<td>80</td>
<td>Allow access to WebGUI pfSense</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>10.255.2.0/25</td>
<td>Any</td>
<td>172.16.4.8</td>
<td>5176</td>
<td>Center VPN to Consoleworks</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>10.255.2.0/25</td>
<td>Any</td>
<td>172.16.4.8</td>
<td>443</td>
<td>Center VPN to Consoleworks HTTPS</td>
</tr>
<tr>
<td>Deny</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>WAN Address</td>
<td>Any</td>
<td>Block All access to pfSense</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>172.16.7.110</td>
<td>3389</td>
<td>RDP to Lab-PC on PACS (Backups)</td>
</tr>
</tbody>
</table>
**Table 4. Border Firewall Rules (continued)**

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>172.16.7.135</td>
<td>Any</td>
<td>VirtualInfra</td>
<td>Any</td>
<td>Lab laptop to Virtualization</td>
</tr>
<tr>
<td>Deny</td>
<td>IPv4 – All</td>
<td>Any</td>
<td>Any</td>
<td>VirtualInfra</td>
<td>Any</td>
<td>Block all to Virtualization</td>
</tr>
<tr>
<td>Deny</td>
<td>IPv4 – TCP</td>
<td>172.16.8.0/24</td>
<td>Any</td>
<td>10.32.2.0/25</td>
<td>Any</td>
<td>Block Vendor VPN from Management</td>
</tr>
<tr>
<td>Deny</td>
<td>IPv4 – TCP</td>
<td>10.32.2.128/25</td>
<td>Any</td>
<td>10.32.2.0/25</td>
<td>Any</td>
<td>Block Vendor VPN from Management</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv6 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>172.16.7.128/25</td>
<td>Any</td>
<td>10.32.2.117</td>
<td>3389</td>
<td>RDP to 117</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – UDP</td>
<td>172.16.7.128/25</td>
<td>Any</td>
<td>10.32.2.117</td>
<td>3389</td>
<td>RDP to 117</td>
</tr>
<tr>
<td>Deny</td>
<td>IPv4 – All</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Block IPv4</td>
</tr>
<tr>
<td>Deny</td>
<td>IPv6 – All</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Block IPv6</td>
</tr>
</tbody>
</table>
### Table 5. IdAM Firewall Rules

<table>
<thead>
<tr>
<th>Aliases</th>
<th>Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AD_DCs_All</td>
<td>172.16.{5,6,7,2}</td>
<td>All DCs in Infrastructure</td>
</tr>
<tr>
<td></td>
<td>LinuxSystems</td>
<td>172.16.4.{2,3,8,10,11,12,253}</td>
<td>Used for SSH</td>
</tr>
<tr>
<td></td>
<td>MAG_Linux</td>
<td>172.16.4.{10,11,12}</td>
<td>Systems for MAG</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>10.32.2.0/25</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow all management network traffic</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>10.255.2.0/25</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Center VPN to all systems</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>172.16.7.133</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>IT to IdAm</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>LinuxSystems</td>
<td>IMG</td>
<td>Allow SSH to Linux</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>Any</td>
<td>Any</td>
<td>172.16.4.8</td>
<td>161,162,514,5176</td>
<td>Allow SNMP, Syslog, default to TDi</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>AD_DCs_All</td>
<td>Any</td>
<td>172.16.4.15</td>
<td>Any</td>
<td>AD DCs to IdAM-CA</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>172.16.8.50</td>
<td>Any</td>
<td>172.16.4.15,22</td>
<td>Any</td>
<td>CA to CA_srv12, CA_SQL_srv12</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>172.16.4.2</td>
<td>5900-5910</td>
<td>VNC to IMG</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>172.16.7.2</td>
<td>Any</td>
<td>172.16.4.2</td>
<td>Any</td>
<td>PACS AD to IMG</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>172.16.7.2</td>
<td>Any</td>
<td>172.16.4.3</td>
<td>Any</td>
<td>PACS AD to Adaptive Directory</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>10.32.2.0/25</td>
<td>Any</td>
<td>172.16.4.8</td>
<td>517,6443</td>
<td>MGMT to TDi Consoleworks</td>
</tr>
</tbody>
</table>

### Table 6. IT Firewall Rules

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv6 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Name</td>
<td>Values</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------</td>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert_Enterprise</td>
<td>172.16.4.5</td>
<td>AlertEnterprise</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td>172.16.4.15</td>
<td>CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA_RSA_Alert</td>
<td>172.16.4.{2,3,5,15}, 172.16.7.132</td>
<td>CA, RSA, Alert</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConsoleWorks</td>
<td>172.15.4.8</td>
<td>Console Works</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT_Network</td>
<td>172.16.7.132</td>
<td>IT network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinuxSystems</td>
<td>172.16.5.4</td>
<td>All Linux on IT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ozone</td>
<td>172.16.4.10-12</td>
<td>Ozone products</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td>172.16.4.2-3</td>
<td>IMG, Adaptive Dir</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**WAN Interface**

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

**LAN Interface**

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv6 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
</tbody>
</table>

**Aliases**

<table>
<thead>
<tr>
<th>Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
</table>

Table 7. OT Firewall Rules
<table>
<thead>
<tr>
<th>System</th>
<th>IP Address</th>
<th>OT Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinuxSystems</td>
<td>172.16.6.7</td>
<td>All Linux on OT</td>
</tr>
<tr>
<td>RADiFlow</td>
<td>172.16.6.{4,6,202}</td>
<td>All RADiFlow IPs</td>
</tr>
</tbody>
</table>

### WAN Interface

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>10.32.0/25</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow all management network traffic</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>172.16.6.10</td>
<td>22</td>
<td>SSH to RPi RTU</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>LinuxSystems</td>
<td>22</td>
<td>Allow SSH to Linux</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>Any</td>
<td>Any</td>
<td>172.16.6.2</td>
<td>53</td>
<td>Allow DNS</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>172.16.4.8</td>
<td>Any</td>
<td>LAN net</td>
<td>22,161-162</td>
<td>TDI to OT-Net</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>172.16.6.2</td>
<td>389,636</td>
<td>Any LDAP to AD</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>172.16.4.{2,3,15}</td>
<td>Any</td>
<td>172.16.6.2</td>
<td>Any</td>
<td>AdaptiveDir, IMG, CA IM to AD</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv4 – TCP</td>
<td>Any</td>
<td>Any</td>
<td>172.16.6.100</td>
<td>2001-2101</td>
<td>Telnet Access through RADiFlow</td>
</tr>
</tbody>
</table>

### LAN Interface

<table>
<thead>
<tr>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv6 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
</tbody>
</table>
Table 8. PACS Firewall Rules

<table>
<thead>
<tr>
<th>Aliases</th>
<th>Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VirtualInfra</td>
<td>10.32.2.10-12</td>
<td>Virtualization Systems for Build</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>LAN Interface</th>
<th>Allow/Deny</th>
<th>Protocol</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>IPv4 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
<tr>
<td>Allow</td>
<td>IPv6 – All</td>
<td>LAN Net</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Default Allow Any LAN</td>
</tr>
</tbody>
</table>
Microsoft Active Directory was used to provide directory services in each silo networks (OT, PACS, IT). Linux CentOS 7 was used to provide DNS services in the IdAM network. Microsoft Windows Server was used to provide certificate authority services in each network.

### 3.3.1 IT Network — Network Services (AD and Certificate Authority) Installation and Configuration Settings

#### 3.3.1.1 Active Directory

Use these basic domain controller configuration settings:

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

**Step-by-step instructions:**

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

#### 3.3.1.2 Certificate Authority Role
Use these basic certificate authority configuration settings:

- CA Setup Type: Enterprise CA
- CA Type: Root CA
- Cryptographic options: RSA 2048 and SHA1
- CN: IT-ES-IDAM-B1-IDAM-ITDC
- DN suffix: DC=IT-ES-IDAM-B1, DC=TEST

Step-by-step instructions:

1. From the Server Manager dashboard, select Option 2, Add Roles and Features.
2. Select Role-based or Feature-based installation (this is a single option to choose).
3. From the server pool, select the local server named OTDC.
5. When prompted to add features, select Add Features.
6. When prompted to select roles services, check Certificate Authority.
7. After the Server Manager finishes installing, select Post-deployment Configuration for Certificate Services from the Task menu.
8. When prompted to specify setup type, select Enterprise CA.
9. When prompted to specify CA type, select Root CA.
10. When prompted to specify private key, select Create a new private key.
11. When prompted to specify cryptographic options, select RSA with a key length of 2048 and select SHA1 for the hash algorithm.
12. Leave the CN and DN suffix, which should be based on the computers hostname and domain.
13. Select 5 years for certificate validity period.
14. Leave the default options for the certificate database and log location.
15. After configuration is complete, restart the server.
2. From the dashboard, select Option 2, Add Roles and Features.
3. Select Role-based or Feature-based installation.
4. From the server pool, select the local server named OTDC.
5. Select Active Directory Domain Service and DNS Server.
6. When prompted to add features, select Add Features for each role.
7. After the Server Manager finishes installing, select Post-deployment Configuration for Active Directory from the Task menu.
8. The Active Directory Domain Services Configuration Wizard launches:
   - For the deployment operation, select Add a New Forest.
   - For the root domain, specify OT-ES-IDAM-B1.TEST, then select Next >.
   - For both the Forest Functional Level and the Domain Functional Level, select Windows Server 2012 R2.
   - Under Domain Controller Capabilities:
     - Check both DNS server and Global Catalog.
     - Uncheck read-only domain controller.
     - Specify a password for DSRM and select Next >.
   - Continue through the wizard without modifying any options.
   - On the last page, select Install. After installation, the server automatically reboots.

3.3.2.2 Certificate Authority Role

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

Step-by-step instructions:

1. Ensure the domain controller installation has been completed before proceeding.
2. From the Server Manager dashboard, select Option 2, Add Roles and Features.
3. Select Role-based or Feature-based installation (this is a single option to choose)
4. From the server pool, select the local server named OTDC.
6. When prompted to add features, select Add Features.
7. When prompted to select roles services, check Certificate Authority.

8. After the Server Manager finishes installing, select Post-deployment Configuration for Certificate Services from the Task menu.

9. When prompted to specify setup type, select Enterprise CA.

10. When prompted to specify CA type, select Root CA.

11. When prompted to specify a private key, select Create a new private key.

12. When prompted to specify cryptographic options, select RSA with a key length of 2048 and select SHA1 for the hash algorithm.

13. Leave the CN and DN suffix, which should be based on the computer’s hostname and domain.

14. Select 5 years for certificate validity period.

15. Leave the default options for the certificate database and log location.

16. After configuration is complete, restart the server.

3.3.3 PACS Network – Network Services: AD, DNS Server, and Certificate Authority Installation and Configuration Setting

3.3.3.1 Active Directory Domain Services and DNS Server

Use these basic domain controller configuration settings:

- Hostname: PACSDC
- Domain: PACS-ES-IDAM-B1.TEST
- IP: 172.16.7.2

Step-by-step instructions:

1. Launch Server Manager.

2. From the dashboard, select Option 2, Add Roles and Features.

3. Select Role-based or Feature-based installation (this is a single option to choose).

4. From the server pools, select the local server named PACSDC.

5. Select Active Directory Domain Service and DNS Server.

6. When prompted to add features, select Add Features for each role.

7. After the Server Manager finishes installing, select Post-deployment Configuration for Active Directory from the Task menu.

8. The Active Directory Domain Services Configuration Wizard launches:

   - Select Add a new forest for the deployment operation. Specify PACS-ES-IDAM-B1.TEST for the root domain, then select Next.
Select Windows Server 2012 R2 for both the forest functional level and the domain functional level.

Under domain controller capabilities:
- Check both DNS server and Global Catalog.
- Uncheck read-only domain controller.
- Specify a password for DSRM and select Next >.

Continue through the Wizard without modifying any options.

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

### Installation of Certificate Authority Role on the PACS network

Use these basic domain controller configuration settings:
- **CA Setup Type:** Enterprise CA
- **CA Type:** Root CA
- **Cryptographic options:** RSA 2048 and SHA1
- **CN:** PACS-ES-IDAM-B1-IDAM-PACSDC
- **DN suffix:** DC=PACS-ES-IDAM-B1, DC=TEST

#### Step-by-step instructions:

1. From the Server Manager dashboard, select the Option 2, Add Roles and Features.
2. Select Role-based or Feature-based installation.
3. From the server pools, select the local server named OTDC.
5. When prompted to add features, select Add Features.
6. When prompted to select roles services, check Certificate Authority.
7. After the Server Manager finishes installing, select Post-deployment Configuration for Certificate Services from the Task menu.
8. When prompted to specify setup type, select Enterprise CA.
9. When prompted to specify CA type, select Root CA.
10. When prompted to specify private key, select Create a new private key.
11. When prompted to specify cryptographic options, select RSA with a key length of 2048 and select SHA1 for the hash algorithm.
12. Leave the CN and DN suffix, which should be based on the computer’s hostname and domain.
13. Select 5 years for certificate validity period.
14. Leave the default options for the certificate database and log location.

15. After configuration is complete, restart the server.

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

Custom attribute details:

- **Common Name**: pacsAllDoors
- **X.500 OID**: 1.3.6.1.4.1.4203.666.1
- **Syntax**: Boolean

- **Common Name**: pacsHomeAccess
- **X.500 OID**: 1.3.6.1.4.1.4203.666.2
- **Syntax**: Boolean

- **Common Name**: pacsWorkAccess
- **X.500 OID**: 1.3.6.1.4.1.4203.666.3
- **Syntax**: Boolean

Step-by-step instructions:

1. Launch Command Prompt as an administrator.
2. Run the command: `regsvr32 schmgmt.dll`
3. Launch the Microsoft Management Console.
4. Select File > Add/Remove Snap-in.
5. From the Snap-in menu, select Active Directory Schema, then select OK.
6. Expand the Active Directory Schema, then select Attributes.
7. To create an attribute for the all doors access level, right-click on Attributes, then select Create Attribute.
8. Select OK when prompted with the Schema Object Creation Warning.
9. Enter the following fields:
   - **Common Name**: pacsAllDoors
   - **LDAP Display Name**: pacsAllDoors
   - **Unique X500 Object ID**: 1.3.6.1.4.1.4203.666.1
   - **Syntax**: Boolean
10. Select OK when finished.
11. Create an attribute for the home access level by entering the following fields:
   - **Common Name**: pacsHomeAccess
   - **LDAP Display Name**: pacsHomeAccess
12. Create an attribute for the work access level by entering the following fields:

- **Common Name:** pacsWorkAccess
- **LDAP Display Name:** pacsWorkAccess
- **Unique X500 Object ID:** 1.3.6.1.4.1.4203.666.3
- **Syntax:** Boolean

13. After creating custom attributes, add the attributes to the user class so that every user contains the attribute:

- Select the Classes drop-down under Active Directory Schema.
- Right-click on User, then select Properties.
- Select the Attributes tab, then select Add.
- Select the attribute you want to add to the user class. Then select OK. Do this for the pacsAllDoors, pacsHomeAccess and pacsWorkAccess attributes.
- Then select Apply and OK.
- Restart the server.

### 3.3.4 IdAM Network – Network Services (DNS Server) Installation and Configuration Settings

A Linux CentOS 7 DNS server was established on the IdAM network to provide DNS services to the IdAM components. No other network service was installed in the IdAM network.

#### System Environment Settings

- CentOS 7
- VM with 4 CPU Quad Core 2.199GHz.
- VM with 16384MB of memory.
- Virtual Hard Disk containing 98GB of storage.

#### Linux CentOS DNS Configuration

Basic DNS configuration settings are specified using three different system files that are located in the /etc and /var subdirectories of the root directory as follows.

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

```
//
// named.conf
//
```
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).

// See /usr/share/doc/bind*/sample/ for example named configuration files.

options {
    listen-on port 53 { 127.0.0.1; 172.16.4.253; };
    #listen-on-v6 port 53 { ::1; };
    #listen-on-v6 { none; };
    directory "/var/named";
    forwarders { 8.8.8.8; 8.8.4.4; };
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query { localhost; 172.16.4.0/22; };
    allow-transfer { localhost; 172.16.4.0/22; };

    /*
     - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
     - If you are building a RECURSIVE (caching) DNS server, you need to enable recursion.
     - If your recursive DNS server has a public IP address, you MUST enable access control to limit queries to your legitimate users. Failing to do so will cause your server to become part of large scale DNS amplification attacks. Implementing BCP38 within your network would greatly reduce such attack surface
     */
    recursion yes;

dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;

/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";

managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
};
logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "idam-es-idam-b1.test" IN {
    type master;
    file "idam-es-idam-b1.test";
    allow-update { none; };
};

zone "4.16.172.in-addr.arpa" IN {
    type master;
    file "4.16.172.db";
    allow-update { none; };
}
zone "ot-es-idam-b1.test" IN {
  type slave;
  masters {
    172.16.6.2;
  }
  forwarders {};
};

zone "pacs-es-idam-b1.test" IN {
  type slave;
  masters {
    172.16.7.2;
  }
  forwarders {};
};

zone "es-idam-b1.test" IN {
  type slave;
  masters {
    172.16.5.2;
  }
  forwarders {};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

3.3.4.2 System file 2 – 4.16.172.db in the /var subdirectory
$TTL 86400
@ IN SOA idam-dns.idam-es-idam-b1.test. root.idam-es-idam-b1.test. ( 
    2011071001 ;Serial
@ IN NS idam-dns.idam-es-idam-b1.test.
@ IN PTR idam-es-idam-b1.test.
idam-dns IN A 172.16.4.253

101 IN PTR idam-dns.idam-es-idam-b1.test.

System file – idam-es-idam-b1.test in the /etc subdirectory

$TTL 86400
@ IN SOA idam-dns.idam-es-idam-b1.test. root.idam-es-idam-b1.test. ( 
2011071001 ;Serial
3600 ;Refresh
1800 ;Retry
604800 ;Expire
86400 ;Minimum TTL
)

@ IN NS idam-dns.idam-es-idam-b1.test.
@ IN A 172.16.4.253
idam-dns IN A 172.16.4.253
idam-ca IN A 172.16.4.15
idam-sql IN A 172.16.4.22
adaptivedir IN A 172.16.4.3
img IN A 172.16.4.2
consoleworks IN A 172.16.4.8
 ozoneserver IN A 172.16.4.10
 ozoneenvoy IN A 172.16.4.12
 ozoneauthority IN A 172.16.4.11
alertent IN A 172.16.4.5
WIN-IPERGL2ELUD IN A 172.16.4.5
4  Remote Terminal Units (RTUs)

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

4.1 TCP/IP RTU

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

4.2 Serial RTU

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

5  Identity Services Engine (ISE) and TrustSec Enabled Switch: Cisco

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

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

5.1 Security Characteristics

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

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

5.2 Pre-Installation Task

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

   - This is the Cisco Identity Services Engine Hardware Installation Guide, Release 1.4, section on Installing ISE on a VMware Virtual Machine.
   - To deploy the OVA file, follow the instructions at the heading “Installing Cisco ISE on Virtual Machines.”
   - After OVA is deployed, follow instructions at heading “Installing Cisco ISE Software on a VMware System.”

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

3. The following are prompts and build responses:
   - Enter hostname: `ise`
   - Enter IP address: `172.16.4.77`
   - Enter IP netmask: `255.255.255.0`
   - Enter IP default gateway: `172.16.4.1`
   - Enter default DNS domain: `idam-es-idam-b1.test`
   - Enter primary nameserver: `172.16.4.253`
   - Add secondary nameserver? Y/N [N]: <blank>
   - Enter NTP server: `time.nist.gov`: `172.16.4.1`
   - Add another NTP server? Y/N [N]: <blank>
   - Enter system time zone: `EST`
   - Enable SSH service? Y/N [N]: Y
   - Enter username [admin]: `admin`
   - Enter password: <password>
   - Enter password again: <password>

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

5. Begin the Setup Assistant.

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

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

8. Select Yes for authenticate users using Cisco ISE, select Join the Active Directory domain, and add domain credentials (in build, we used `es-idam-b1.test` for domain and the domain admin credentials to connect). Fill in the Employee Switched VLAN Interface box with: `172.16.5.0 /24`. Press Next.
9. Select switch (build used Cisco Catalyst 3560 Series Switches), fill in pertinent information for switch. For Employee VLAN ID, build used 104. Select a RADIUS Shared Secret (build used password). Press Next.

10. Confirm all settings are correct, then select Confirm Configuration Settings.

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

```
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting delay-start all
aaa accounting auth-proxy default start-stop group radius
aaa accounting dot1x default start-stop group radius
aaa accounting network default start-stop group radius
aaa server radius dynamic-author
   client 172.16.4.77 server-key 7 15020A1F173D24362C
!
aaa session-id common
switch 1 provision ws-c3650-48ps
authentication mac-move permit
ip routing
!
ip device tracking
ip dhcp snooping vlan 102
no ip dhcp snooping information option
ip dhcp snooping
dot1x system-auth-control
!
diagnostic bootup level minimal
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
   mode sso
!
ip ssh version 2
```
class-map match-any non-client-nrt-class
  match non-client-nrt
!

policy-map port_child_policy
  class non-client-nrt-class
  bandwidth remaining ratio 10

snmp trap mac-notification change added
  spanning-tree portfast
!

ip access-list extended ACL-DEFAULT
  remark Allow DHCP
  permit udp any eq bootpc any eq bootps
  remark Allow DNS
  permit udp any any eq domain
  permit icmp any any
  permit tcp any any host 172.16.4.77 eq 8443
  permit tcp any any host 172.16.4.77 eq 443
  permit tcp any any host 172.16.4.77 eq www
  permit tcp any any host 172.16.4.77 eq 8905
  permit tcp any any host 172.16.4.77 eq 8909
  permit udp any any host 172.16.4.77 eq 8905
  permit udp any any host 172.16.4.77 eq 8909
  deny ip any any

ip access-list extended ACL-WEBAUTH-REDIRECT
  permit tcp any any eq www
  permit tcp any any eq 443
  deny ip any any
!

logging origin-id ip
logging source-interface GigabitEthernet1/0/48
!

radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 172.16.4.77 auth-port 1812 acct-port 1813 key 7
140713181F13253920
!
radius server host
!
wsma agent exec

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

```
interface GigabitEthernet1/0/10
switchport access vlan 101
switchport mode access
switchport block unicast
switchport voice vlan 105
ip arp inspection limit rate 2000
ip access-group ACL-DEFAULT in
authentication event fail action next-method
authentication event server dead action authorize vlan 101
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity 180
authentication violation restrict
mab
```
dot1x pae authenticator

dot1x timeout tx-period 10

spanning-tree portfast

spanning-tree bpduguard enable

ip dhcp snooping limit rate 2048

11. Go to the top tabs and click Administration > System > Deployment. (If a warning that
says “This node is standby mode. To register other...Role to Primary” click OK.) Under
the Deployment Nodes – Hostnames click on the ise link. Then click Profiling
Configuration, and ensure that Netflow, Radius, DNS, SNMPQUERY, and SNMPTRAP are
selected. If they are not selected, select them. Then click Save.

12. Select Administration > Identity Management > External Identity Sources. In the frame
on the left choose Active Directory, then choose ise.idam-es-idam-b1.test. Click
Connections tab, select the checkbox next to the domain es-idam-b1.test. Check
to see if there is a green check in the Status column. If yes click Save.
If not, Click Join, and type in the AD Credentials and click Save. A green check
should appear in the Status column.

13. Select Administration > Identity Management > External Identity Sources > Groups tab.
Click Add > Select Group From Directory. Click retrieve groups. Check the es-idam-
b1.test/Users/Domain Users box and the es-idam-b1.test/Builtin/Users box and the es-
idam-b1.test/Users/OTAccess box. These items are specified for protected access (the
build used OTAccess). Then Click OK. Then click Save. Relogin as directed.

14. Select Administration > System > Settings. Click on Policy Sets in the frame at the left of
the screen, and click enabled (if it is not already clicked). Click Save if needed.

15. Select Policy > Policy Elements > Results. In the frame at the left of the screen, left
column, click Authorization, then Downloadable ACL List. Create the following (all IP
addresses are pertinent to the current build.; these addresses will need to be replaced
with IP addressing that is appropriate to the target environment):

- All_But_OT-Access-DACL
  - Name: All_But_OT-Access-DACL
  - DACL Content:
    - deny ip any 172.16.6.0 0.0.0.255
    - permit ip any any

Click Save

16. In the left column, select Authorization Profiles and click Add to create the
following:

- All_and_OT
  - Name: All_and_OT
  - Access Type: ACCESS_ACCEPT
  - Check DACL Name: PERMIT_ALL_TRAFFIC

Click Submit
17. Select Policy > Policy Elements > Conditions. In the left column, select Authorization, then Simple Conditions. Click Add to create the following:

- **NotOTAccess**
  - **Name:** NotOTAccess
  - **Attribute:** Select the domain (build uses es-idam-b1.test) > ExternalGroups
  - **Operator:** Not Equals
  - **Value:** Select the Security Group (build uses es-idam-b1.test/Users/OTAccess)

Click Submit

- **IT_DomainUsers**
  - **Name:** IT_DomainUsers
  - **Attribute:** Select the domain (build uses es-idam-b1.test) > ExternalGroups
  - **Operator:** Equals
  - **Value:** Select domain users group (build uses es-idam-b1.test/Users/Domain Users)

Click Submit

18. Select Policy > Policy Sets. Select Default and configure policies. Choose the arrow next to Authorization to expand the section. Choose the top rule and click the option arrow to the right of the Edit link within the policy. Click New rule above.

- **Rule 1:** Click the plus sign in the Conditions box. Select Create New Condition (Advanced Option). Select Attribute > es.idam-b1.test > External Groups. Leave equals Select Attributes > es-idam-b1.test/Users/OTAccess. Click the plus sign in the Permissions box. Select item drop down choose Standard > All_and_OT. Click Done button on right. Click the arrow to the right of the Edit link within the top policy (new policy created above) Click Insert Below.

- **Rule 2:** Click the plus sign in the Conditions box. Select Existing Condition from Library. Select arrow to choose simple conditions > NotOTAccess. Select arrow next to the gear icon (on right). Select Add Condition from Library. Select Arrow
to choose Simple conditions > IT_DomainUsers. Click on the Permissions input box. Click the plus sign in the Permissions box. Click the arrow and choose standard > All_But_OT_Access. Click Done. Click Save.

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

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

6.1  SECURITY CHARACTERISTICS

Cybersecurity Framework Categories:

- 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

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

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

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

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

6.2  INSTALLATION PREREQUISITES

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

1. Use a server with a supported OS (e.g., Windows 2012 R2).
2. Install a supported version of the JDK. (e.g., 1.7.0_71).
3. Install a supported version of JBoss. (e.g., jboss-eap-6.3).

4. To install JBoss as a Windows service, follow the instructions at the following link:

5. Create a Database and associated user with DBA permissions on a supported database (e.g., MSQL 2012).

6. Download and unzip CA Identity Manager software from https://support.ca.com.

6.3 INSTALL CA DIRECTORY

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

6.4 INSTALL CA IDENTITY MANAGER

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

16. Review Settings: Click Install

17. After the installation completes, start JBoss by executing `jboss-eap-6.3\bin\standalone.bat`.

18. Review the log file to verify that JBoss started without error: `jboss-eap-6.3\standalone\log\server.log`

19. If you receive a timeout error such as “Timeout after [300] seconds waiting for service container stability…”, increase the timeout by modifying standalone.bat, adding the following attribute to the startup script:

   `-Djboss.as.management.blocking.timeout=900`

6.5 **CREATE THE SAMPLE NeteAuto DIRECTORY**

1. Open a command prompt as the administrator user

2. cd to “C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\NeteAuto\Organization”

   o You will see several sample files. For this example, we will use neteauto.ldif

3. Execute the following commands:

   ```
   dxnewdsa -s500 neteauto 3895 "dc=security,dc=com"
dxserver install neteauto
dxserver stop neteauto
dxloaddb -v -s neteauto neteauto.ldif
dxserver start neteauto
   ```

4. To log in to the IM Management Console, navigate to `http://<ServerName>:8080/iam/immanage` and log in using the credentials you supplied in Login Information above.

5. From Directories, select “Create or Update from XML”.

6. Browse to `C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\NeteAuto\Organization`.

7. Select directory.xml. Click Next.

8. Supply values for the fields in this window as follows:

   - **Name** - NeteAuto
   - **Description** - (Optional)
   - **Connection Object Name** - neteauto
   - **Host** - the machine name where you ran the dxserver commands above
   - **Port** - 3895
   - **Username/User DN** - `uid=NeteAuto,Administrator,ou=People,ou=Employee,ou=NeteAuto,dc=security,dc=com`
   - **Password/Confirm Password** - test
   - **Secure Connection** - Unchecked
9. Click Next, then Finish.

6.6 CREATE THE PROVISIONING DIRECTORY

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

6.7 CREATE THE NETEAUTO ENVIRONMENT

1. From Environments, select “New”.
2. Supply the following information:
   • Environment name - NeteAuto
   • Description - (Optional)
   • URL alias - neteauto
   • Base URL – accept the default (make sure it is a fully qualified host name in the URL)
3. Click Next.
4. Select the “NeteAuto” directory. Click Next.
5. Select the “Provisioning” directory. Click Next.
   • URL alias used to reference public tasks – neteauto_pub
   • User for anonomous authentication – SelfRegUser
6. Click Validate. Then click Next.
7. Select “Create Default Roles”. Click Next.
8. Select the Checkbox for Active Directory.
9. Scroll down and click the Browse button.
10. Select the NIST_PXPolicies.xml file provided with this guide. (Download the file from https://nccoe.nist.gov/sites/default/files/nccoe/NIST_PXPolicies.zipx and unzip it.)
11. Click Next.
12. Click Add. Then click Next.
13. Click Next.
14. Click Next.
15. Review the settings, then click Finish.
16. Allow a few minutes for the Environment to deploy.
17. When finished with “0 error(s)”, click Continue.
18. Click “NeteAuto”.
19. Click “Advanced Settings”, then “Workflow”. Enable both check boxes and click Save.
20. Click the “Restart Environment” button.
21. Verify that you can login to the environment by going to the environment URL and logging in:

- http://<FullyQualifiedServerName>:8080/iam/im/<ProtectedAlias>
- Username: SuperAdmin
- Password: test

6.8 Configure Connection to Alert Enterprises Database

Generate the encrypted password for the Alert Database as follows:

1. From a command prompt, cd to C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool
2. Execute the following command: pwdtools -JSAFE -p
   <AlertDBPassword>
3. The result displays the Encrypted value with a prefix of {PBES}.
4. Copy this encrypted password to be used below for EncryptedALERTDBPassword.

2. From the JBoss installation directory, create the following folder structure:
   jboss-eap-6.3\modules\com\mysql\main
   - Select Platform Independent, Compressed Zip Archive. Download.
   - Unzip and copy the mysql-connector-java-5.1.35-bin.jar to the mysql\main folder you created above.
   - Under the same folder, create a text file named module.xml. Paste the following text into the file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="com.mysql">
  <resources>
    <resource-root path="mysql-connector-java-5.1.35-"
3. From jboss-eap-6.3\standalone\configuration edit standalone-full.xml

4. In the “<drivers>” section, add:
   <driver name="mysql" module="com.mysql">
   <driver-class>com.mysql.jdbc.Driver</driver-class>
   </driver>

5. Just above the “<drivers>” section, add a new data source:
   <datasource jndi-name="java:/iam/im/jdbc/jdbc/AlertDB"
     pool-name="MySQLPool" use-java-context="true">
     <connection-url>
       jdbc:mysql://ALERTDBServerName:3306/ALERTDBName
     </connection-url>
     <driver>
       mysql
     </driver>
     <pool>
       <max-pool-size>30</max-pool-size>
     </pool>
     <security>
       <security-domain>mysqldb</security-domain>
     </security>
   </datasource>

6. In the “<security-domains>” section, add the following security domain:
   <security-domain name="mysqldb">
     <authentication>
       <login-module
         code="com.netegrity.jboss.datasource.PicketBoxPasswordEncryptedLogin"
         flag="required" module="com.ca.iam.idmutils">
         <module-option name="userName" value="ALERTDBUserName"/>
         <module-option name="password" value="EncryptedALERTDBPassword"/>
         <module-option name="managedConnectionFactoryName"
           value="jboss.jca:name=iam/im/jdbc/jdbc/WPDS,service=LocalTxCM"/>
       </login-module>
     </authentication>
   </security-domain>
7. Restart the JBoss service
8. Review the log file to verify that JBoss started without error: `jboss-eap-6.3\standalone\log\server.log`

### POLICY XPRESS POLICY REVIEW

1. Log in to the NeteAuto Environment that you created above by navigating to `http://<FullyQualifiedServerName>:8080/iam/im/<ProtectedAlias>`
2. For NeteAuto the username/password is `superadmin/test`.
4. Select the desired Policy to review and modify as desired.
   - Check for Duplicates on Create: Stops the task with a message to the user if duplicates are detected for the CardNumber or the UserID on the Alert Database
   - Check for Duplicates on Modify: Stops the task with a message to the user if the CardNumber is already used by another user on the Alert Database.
   - Check for Numeric on Create and Modify: Stops the task with a message to the user if the PIN, FacilityCode, or CardNumber is not an integer.
   - Check PACs fields on Create and Modify: Stops the task with a message to the user if none of the PACs checkboxes are selected. At least one must be selected.
   - Disable AE User: Disables User on the Alert Database, by setting the UserStatus to “Inactive”
   - Enable AE User: Enables User on the Alert Database, by setting the UserStatus to “Active”
   - Modify AE User: Modifies User on the Alert Database if all above checks pass.

### UPDATE CREATE USER AND MODIFY USER SCREENS

1. From Roles and Tasks > Admin Tasks > Modify Admin Task, search and select Create User.
2. Go to the Tabs tab and click the edit pencil next to Profile.
3. Click Browse Next to the Create User Profile.
4. Select the Default User Profile, and click the Edit button.
5. Click the edit pencil next to each of the following fields:
   - Office: Change Name to PIN
   - Postal Code: Change Name to Facility Code. Change Permission to Read/Write Required.
   - Cell Phone: Change Name to Home Phone.
• Business Phone: Change Name to Work Phone.
• State: Change Name to Pacs All Door. Change Style to Checkbox. Set Check value to 1. Set Unchecked Value to 0.
• City: Change Name to Pacs Work Access. Change Style to Checkbox. Set Check value to 1. Set Unchecked Value to 0.
• Address: Change Name to Pacs Home Access. Change Style to Checkbox. Set Check value to 1. Set Unchecked Value to 0.
• Employee Number: Change Name to Card Number. Change Permission to Read/Write Required.
• For any non-required fields that you don’t want to display: Change Style to Hidden.

6. Click OK.
7. Select the Create User Profile, and click the Edit button.
8. Repeat Step 5 for this profile. When finished, click OK.
9. Navigate to Users > Manage Users > Create User, and click “Yes” for the warning message about losing changes.
10. Select Create New User, and click OK.
11. Verify that the fields you updated are changed as desired.
12. Navigate to Users > Manage Users > Modify User, and click “Yes” for the warning message about losing changes.
13. Select Create Modify User, and click OK.
14. Verify that the fields you updated are changed as desired.

6.11 INSTALL ACTIVITY DIRECTORY CERTIFICATE

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.
2. Double-click on the certificate, and click Install Certificate.
3. Select Local Machine, then Place all Certificates in the following store. Click Browse.
4. Select Trusted Root Certification Authorities. Click OK twice.

6.12 ACQUIRE ACTIVITY DIRECTORY ENDPOINT

1. From Endpoints > Manage Endpoints > Create Endpoint, select Create a new endpoint of Endpoint type ActiveDirectory. Click OK.

• Endpoint: Give your endpoint a name
• Hostname: Fully qualified host name for the Active Directory Domain Controller
• **User ID:** Fully qualified User ID, for example: domain\userid.
• **Password/Confirm Password:** Password for the AD User

2. Click the Security tab. Check the “Use LDAP – SSL Encryption” checkbox.
3. Click Submit.

### 6.13 **EXPLORE AND CORRELATE ACTIVE DIRECTORY**

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

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

1. From Endpoints > Account Templates > Create Account Template, select Create a new Account Template of Endpoint Type “Active Directory”. Click OK.
2. Give the Account Template a name, such as “<domain controller name> Account Template”.
3. From the Endpoints tab, add the Active Directory Endpoint you created above.
4. From the Groups tab, add the Active Directory groups you want to provision to the user.
5. When finished, click Submit.
6. From Roles > Provisioning Roles > Create Provisioning Role, select Create a new provisioning role, click OK.

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

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

9. From the Administrators tab, select a user, or group of users that you want to be the Administrators of this role. For example, to make the members of a certain Admin role the administrators of this provisioning role:
   - Click Add.
   - From the Users drop-down select a group of users, such as Users who are members of <role-rule>, then admin role.
   - Browse, search, and select the Admin Role you want to add.
   - From the Owners tab, select a user, or group of users that you want to be the Owners of this role, using the same process as used for the Administrators tab.
   - Click Submit.

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

1. From Policies > Policy Xpress > Modify Policy Xpress Policy, search and select the Create AE User policy.

2. From the Action Rules tab, click the edit pencil next to Create User

3. Click the edit pencil next to Add otdc. Click the Browse “…” button next to the Provisioning Role Name. Select the Provisioning Role you just created.

4. Click Select, OK, OK, Submit.

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

1. From Roles and Tasks > Admin Tasks > Modify Admin Task, search and select Create User.

2. From the Events tab, click the edit pencil next to the CreateUserEvent workflow process.

3. Select the Non-Policy Based workflow process “SingleStepApproval.”

4. For the approval, select “Approve Create User” *

5. For the Participant resolver select the type of members you want to assign. For example, Admin Role Members. *

6. Click Add Admin Roles. Search and select the Admin Roles you want to have approve this workflow. *

7. Repeat the above 3 steps with * for the Primary Approver.

8. When finished with both approvers, click OK, then Submit.
The above steps can be used for the Modify User and Enable/Disable User tasks (or any other task).

### 6.17 Test Creation of a User Manually

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

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

### 6.18 Test Creation of a User with a CSV File

2. Modify the CSV file to enter the desired values for the new users to be created. Keep in mind the policy rules that must be followed as described above.
3. From System > Bulk Loader, Browse for the CSV file.
4. What field represents the action to perform on the object: `action`.
5. What field will be used to uniquely identify the object: `uid`.
6. Click Next.
7. What is the Primary Object: `USER`.
8. Select a task to execute for action 'create': Create User
9. Click Finish.

Repeat the steps from Section 9.17 (above) with an asterisk (*) to approve the users and verify that they were successfully created.
7  **IDENTITY MANAGEMENT AND GOVERNANCE (IMG): RSA (BUILD #2)**

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

7.1  **SECURITY CHARACTERISTICS**

Cybersecurity Framework Categories:

- 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

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

7.2  **IMG INSTALLATION**

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

7.3  **IMG CONFIGURATION AND INTEGRATION WITH DIRECTORIES**

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

Log in with the default credentials:

- **Username:** AveksaAdmin (case sensitive)
- **Password:** aveksa123

Change the password when prompted to change.

7.3.1  **Set Up Custom Attributes**

1. Navigate to ‘Admin’ then ‘Attributes’:
1. Click on ‘User’ then ‘Edit’ as shown in Figure 10.

![Attribute Configuration - User](image)

*Figure 11. IMG Attributes Examples*
3. Click on OK.

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

5. Modify your attributes to match those shown in Figure 15. IMG Attribute Example.
6. Click on ‘OK’.

7.3.2 **Set up Organization Users**

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

1. Once the CSV file is copied to the server, perform the following actions:
2. Navigate to ‘Resources’ and under resources, select ‘Directories’ as shown in Figure 16.
3. Click ‘Create Directory’ as shown in Figure 17.

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

5. Enter ‘HR’ in the ‘Directory Raw Name’ field. Click ‘Finish’ as shown in Figure 19.
You have now created your first directory which will serve as a repository for all the HR Data for the organization.

6. Repeat the above steps, creating a second directory. This one will be named ‘RSA Adaptive Directory’. This container will be used to pull AD accounts from the Adaptive Directory server. In this case be sure to select the two options as shown in Figure 20.
Figure 20. IMG Create Directory
7.3.3 *Populate the HR Directory*

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

1. Click on ‘Resources’ and ‘Directories’ again as shown in Figure 21.

*Figure 21. IMG Directories*

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

*Figure 22. IMG Directories*
3. Click on ‘Collectors’ then click ‘Create Identity Collector’ as shown in Figure 23.

4. Enter details as below as shown in Figure 24.
5. Click ‘Next’, and enter details as below as shown in Figure 25.

**Figure 25. IMG HR Identities (cont.)**

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

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

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

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

7. Click ‘Next’.

8. Leave ‘Users’ selected and click ‘Next’ as shown in Figure 26.
1. Enter details as shown in Figure 27 and Figure 28, below. The full text of the ‘User Data Query’ is as follows:

```sql
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 fullname, is_manager, email as UniqueID from HR_Data_Move
```

The highlighted section is specific to this example, based off of our sample data, the OU that the user needs to be provisioned in is based off of the last name. Basically, when the 1st two letters of the last name = IT, the user will have ‘it’ set to the OU attribute, if it’s OT, then ‘ot’ is set as the OU attribute, any other scenario the OU attribute is set to ‘pacs’.
Figure 27. IMG HR Identities
9. Click ‘Finish’

7.3.4 Configure Adaptive Directory Container

The next step is to configure the Adaptive Directory Container with Identity and Account collectors.

1. Navigate to the Adaptive Directory Container as shown in Figure 29.
This identity collector will tie together user identities in Adaptive Directory to user identities in the HR CSV file.

2. Click on ‘Collectors’ and ‘Create Identity Collector’ as shown in Figure 30.
3. Create the ID collector as follows, clicking ‘Next’ between each screen shown in Figure 31, Figure 32, Figure 33, Figure 34 and Figure 35.
Figure 32. IMG AD Identity Collector

Figure 33. IMG AD Identity Collector
Figure 34. IMG AD Identity Collector
4. Click Finish

7.3.5 Create an Account Collector

The next step is to create an account collector which pulls all relevant attributes from Adaptive Directory.

1. Click on ‘Collectors’ and ‘Create Account Collector’ as shown in Figure 36.
2. Create the Account collector as follows, clicking ‘Next’ between each screenshot, Figure 37 through Figure 46 below.
Figure 37. IMG Edit Collector

Figure 38. IMG Edit Collector

Figure 39. IMG Edit Collector
### Search Configuration for Accounts

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

<table>
<thead>
<tr>
<th>Account Base DN</th>
<th>dc=master,dc=test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Search Scope</td>
<td>Subtree</td>
</tr>
<tr>
<td>Account Search Filter</td>
<td><code>(objectCategory=person)(objectClass=user)(sAMAccountName=*)</code></td>
</tr>
<tr>
<td>Account ID</td>
<td>distinguishedName</td>
</tr>
<tr>
<td>Account Attribute</td>
<td>Attribute in LDAP schema</td>
</tr>
<tr>
<td>Last Login Date</td>
<td>lastLogon</td>
</tr>
<tr>
<td>Account Disabled</td>
<td></td>
</tr>
<tr>
<td>Account Locked</td>
<td></td>
</tr>
<tr>
<td>Account email</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>Account expiration date</td>
<td>accountExpires</td>
</tr>
<tr>
<td>Account full name</td>
<td>displayName</td>
</tr>
<tr>
<td>Account status</td>
<td>userAccountControl</td>
</tr>
<tr>
<td>Account technical name</td>
<td>sAMAccountName</td>
</tr>
</tbody>
</table>

**Figure 40. IMG Edit Collector**

<table>
<thead>
<tr>
<th>DN</th>
<th>dn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login ID</td>
<td></td>
</tr>
<tr>
<td>PACS All Doors</td>
<td>pacsAllDoors</td>
</tr>
<tr>
<td>PACS Home Access</td>
<td>pacsHomeAccess</td>
</tr>
<tr>
<td>PACS Work Access</td>
<td>pacsWorkAccess</td>
</tr>
</tbody>
</table>

**Figure 41. IMG Edit Collector**

**User Account Mapping Attribute**

<table>
<thead>
<tr>
<th>User ID</th>
<th>userPrincipalName</th>
<th>Attribute in LDAP schema</th>
</tr>
</thead>
</table>
Figure 42. IMG Edit Collector

Edit Collector: RSA AD Directory Accounts
Mapping for group attributes

Group Data

<table>
<thead>
<tr>
<th>Group attribute</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Base DN*</td>
<td>DC=master,DC=test</td>
</tr>
<tr>
<td>Group Search Scope*</td>
<td>Subtree</td>
</tr>
<tr>
<td>Group Search Filter*</td>
<td>(objectclass=group)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group ID/Name*</th>
<th>distinguishedName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member of Group*</td>
<td>member</td>
</tr>
<tr>
<td>DN</td>
<td>on</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td>Domain</td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td>value is User User ID</td>
</tr>
<tr>
<td>Owner</td>
<td>managedBy</td>
</tr>
<tr>
<td>Resource type</td>
<td></td>
</tr>
</tbody>
</table>

Edit Collector: RSA AD Directory Accounts
Edit User Resolution Rules

Target Collector

Users

User Attribute

User Id
3. Click ‘Finish’

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

4. Test each account collector you created using the test button. This action verifies that IMG can retrieve the account information for each directory added as shown in Figure 47 below.
A successful test will look something like Figure 48.

![Test Collector: RSA AD Directory Accounts](image)

You can see valid data in an XML format. A failed test will generate an error message that can help you isolate the problem.
7.3.6 Edit the Unification Configuration Participating Collectors
The next step is to configure Unification – this is the process of joining Identities from the HR CSV and the Adaptive Directory collectors.

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

![Figure 49. IMG Unification Configuration](image)

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

![Figure 50. IMG Participating Collectors](image)

3. Configure as shown in Figure 51 and Figure 52. Click Next on each screen.
In the above example, we have HR Identities at the top. This indicates that HR Identities is authoritative source – if there are any discrepancies between the data between the two, then the one at the top will win by default, but this can be overridden, which we will see later.

4. Click Finish.

7.3.7 **Edit Unification Configuration Attribute Source**

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

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

![Edit User Attribute Mapping]

Figure 53. IMG Unification Configuration Attribute Sources
3. Click on OK.

7.3.8 **Edit Unification Configuration Attribute Source**

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

1. Choose the Joins tab. Click on Edit as shown in Figure 56.
2. Choose the HR Identities from the Primary Identity Collector dropdown box as shown in Figure 57.

3. Click ‘Finish’.

7.3.9 **Start Data Collection**

The next step is to start collecting identity data.

1. From the home page choose the Resources > Directories tab. Click Collect Data (all) button as shown in Figure 58.
2. Click OK on the next window as shown in Figure 59.

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.
You will see all the processes change to ‘Complete’ when done.

7.3.10 **Review Data Collected**

Now you can look at this data by going to ‘Users’ then ‘Users’ and ‘Groups’.

1. From the home page choose the Users > Groups tab as shown in Figure 61 to review the data collected.
7.3.11  **Configure Business Rules**

The next step is to configure Business Roles.

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

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

---

*Figure 61. IMG Data Collection Review*

*Figure 62. IMG Roles*
3. Configure as follows as shown in Figure 64 through Figure 66.

Figure 63. IMG Discover Roles
4. Notice how there are some duplicates – the job codes are the same, but the descriptions are slightly different. You can combine these roles into one as shown in Figure 67:
5. When you are done combining duplicates, click Finish.

7.3.12 Create Automated Rules

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

1. Click on ‘Rules’ and ‘Definitions’ as shown in Figure 68.
2. Click on ‘Create Rule’ and configure as shown in Figure 69 and Figure 70 for New Users.

![Edit Rule: New User](image)

**Figure 69. IMG New User**
Click on ‘Create Rule’ and configure as shown in Figure 71 and Figure 72 for User Terminations.
Edit Rule: Termination

Rule Name*: Termination

Description:

Owner*: AveksaAdmin

Control URL:

Control Description:

Type*: Provisioning - Termination

Status*: Active

Rule Set*: Existing rule set Default Rule Set

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)
- [x] Delete accounts (excludes shared and service accounts)

For particular accounts All

Perform this action

- [ ] Immediately
- [ ] After ___ days

Processing Schedule/Trigger

- [ ] Use global configuration
- [ ] Define for this rule

Scheduled: Yes

Triggered: Run after identity unification

Figure 71. IMG User Termination
4. Click ‘OK’.

7.3.13 Create Provisioning Template

The next step is to create a template that IMG uses when provisioning accounts in Adaptive Directory:

1. Click on ‘Requests’, ‘Configuration’, ‘Account Template’ tab, then ‘Create Account Template’ as shown in Figure 73.

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

3. Click on the name of the account template you just created and add parameters as shown in Figure 75.
Next configure the IMG AFX module which will allow IMG to provision to Adaptive Directory:

4. Click on ‘AFX’ and ‘Connectors’ as shown in Figure 76.

5. Click on ‘Create Connector’ as shown in Figure 77.
6. Configure the ‘General’ tab as shown in Figure 78.

7. Configure the ‘Settings’ tab as shown in Figure 79 through Figure 81.
Edit Connector: RSA Adaptive Directory Connector IT

Connection Details

- Host*: 172.16.4.3
- Port*: 1635
- Use Secure Connection: checked
- 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: 
Edit Connector: RSA Adaptive Directory Connector IT

Connection Details

- **Host**: 172.16.4.3
- **Port**: 1635
- **Use Secure Connection**: Checkmark
- **Login Distinguished Name**: `cn=Directory Manager`
- **Password**: Hiding
- **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**: None
8. Configure the ‘Capabilities’ tab as shown in Figure 82.
9. Check all capabilities needed for the connector. Once all are selected, click on the capability name one by one and configure as shown in Figure 83 through Figure 96.
Figure 83. IMG AD Connector IT Capability Configuration
Figure 84. IMG AD Connector IT Capability Configuration

Figure 85. IMG AD Connector IT Capability Configuration
Figure 86. IMG AD Connector IT Capability Configuration
Figure 87. IMG AD Connector IT Capability Configuration

Figure 88. IMG AD Connector IT Capability Configuration

Figure 89. IMG AD Connector IT Capability Configuration
Figure 90. IMG AD Connector IT Capability Configuration

Figure 91. IMG AD Connector IT Capability Configuration
Figure 92. IMG AD Connector IT Capability Configuration

Figure 93. IMG AD Connector IT Capability Configuration
Figure 94. IMG AD Connector IT Capability Configuration
Figure 95. IMG AD Connector IT Capability Configuration

Figure 96. IMG AD Connector IT Capability Configuration

10. Click OK.
7.3.14  **Configure Adaptive Directory to Use AFX Connector**

The next step is to configure the RSA Adaptive Directory ‘Directory’ to use the new AFX Connector.

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

   ![Figure 97. IMG Resources Directories](image)

2. Then in the next window choose the AFX Connector Binding tab as shown in Figure 98.

3. Click the Edit Connector Binding as shown in Figure 98.
4. Click OK as shown in Figure 99.

Now the system is ready.

7.4 USING RSA IMG

7.4.1 Adding a New User
1. Open the HR CSV file and add a user.
2. Go to ‘Resources’, ‘Directories’ and click ‘Collect Data (all)’ as shown in Figure 100.
1. Click ‘OK’ as shown in Figure 101.

![Figure 100. IMG Resources Directories](image)

This will collect data from all directories.

Collection will run as a background process. Total execution time will depend on the volume of data.

- Collect Identity And Run Unification
- Collect Accounts
- Collect Entitlements (No active entitlement collectors)

![Figure 101. IMG Collect Data](image)

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

![Figure 102. IMG Activities](image)
3. Select a group you would like to add the user to, Click ‘Next’, then ‘Accepted’ as shown in Figure 103.

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

5. Go to ‘Requests’, and click ‘Requests’. Click the name of the request as shown in Figure 104.
6. After about 30 seconds, your new user will be provisioned to AD and added to the group you selected as shown in Figure 105.
Note: The state of the group add will remain pending, and the overall status will remain at 50% until you recollect data from the Directories page so that IMG can detect that the user has been added to the group successfully as shown in Figure 106.

7.4.2 Moving a User
1. Open your CSV file and change the attribute that defines the OU that the user is in to a different OU.
2. Collect data again.
3. The OU change is detected, and IMG deletes the user from the original OU and adds the user to the new OU.
4. Go to ‘Requests’ and ‘Activities’ and click ‘Perform’ as shown in Figure 107.
5. Select the group you would like the moved user to have access to, click ‘Next’ and ‘Accepted’, then ‘Finish’ on the final screen. As you did before for adding a new user.

6. Collect data again so IMG can confirm that the user is added to the appropriate group in the new OU.

7. Terminating a user

8. Delete the user from the HR CSV file.

9. Collect data again.

10. The user is automatically removed.

11. Collect data again, so IMG can confirm the user is no longer in Adaptive Directory.

12. Check the Status in ‘Requests’, and ‘Requests’ as shown in Figure 108.
RSA Adaptive Directory implements the central IdAM ID store in Build #2. It receives input from the central IdAM system (RSA IMG). The central ID store contains the distribution mechanism for updating the various downstream (synchronized) directories with user access and authorization data. This process applies to new users, terminated users (disabled or deleted users), and any changes to a user profile. Changes include promotions, job responsibility changes, and any other change that would affect the systems a user needs to access.

8.1 Security Characteristics

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

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

The following lines detail the command line installation procedure for RSA Adaptive Directory, including displayed responses:
[root@localhost ~]# ls
anaconda-ks.cfg reports xml
[root@localhost ~]# cd ..
[root@localhost /]# ls
bin dev home lib64 mnt proc run srv tmp var
boot etc lib media opt root sbin sys usr
[root@localhost /]# cd media
[root@localhost media]# ls
cdrom
[root@localhost media]# cd cdrom
[root@localhost cdrom]# ls
Documentation rsa_7.1.5_linux_64.bin rsa_7.1.5_windows_64.exe
[root@localhost cdrom]# su root ./rsa_7.1.5_linux_64.bin
Preparing to install...
WARNING: /tmp does not have enough disk space!
Attempting to use /root for install base and tmp dir.
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
Graphical installers are not supported by the VM. The console mode will be used instead...
=======================================================================
RSA Adaptive Directory 7.1.5      (created with InstallAnywhere)
-------------------------------------------------------------------------------
Preparing CONSOLE Mode Installation...

=======================================================================
License Agreement
-----------------
Please read the following License Agreement carefully.
LICENSE AGREEMENT
*** IMPORTANT INFORMATION - PLEASE READ CAREFULLY ***
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y

Choose Install Folder

Please choose a destination folder for this installation

Where would you like to install?

Default Install Folder: /root/rsa/adaptivedirectory

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

Choose Install Set

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

>1- RSA Adaptive Directory New Cluster / Standalone

2- RSA Adaptive Directory Cluster Node

3- Customize...

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

New Cluster settings

Enter information below about the new cluster to create:

- The cluster name

Cluster name: (DEFAULT: cluster1): cluster1

- The ZooKeeper ports that will be used

ZooKeeper Ensemble Port: (DEFAULT: 2888): 2888

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

ZooKeeper Client Port: (DEFAULT: 2181): 2181

Administrator name

Please provide the administrator name:

Admin User Name (DEFAULT: cn=Directory Manager): Directory Manager
Server administrator password

Please provide a password for the administrator user:

Password (DEFAULT: ): secretsecret

Confirm Password (DEFAULT: ): secretsecret

Adaptive Directory port numbers

Please enter port numbers for Adaptive Directory:

Adaptive Directory Port (DEFAULT: 2389): 2389
Scheduler Port (DEFAULT: 1099): 1099
Adaptive Directory SSL Port: (DEFAULT: 1636): 1636

TLS Configuration

Enable TLS (Y/N)? (DEFAULT: N): N

Adaptive Directory HTTP port numbers

Please enter port numbers for Adaptive Directory HTTP services:

Adaptive Directory HTTP Port (DEFAULT: 8089): 8089
Adaptive Directory HTTPS Port (DEFAULT: 8090): 8090

Certificate configuration

Use an existing certificate (Y/N)? (DEFAULT: N): N
Application Server Configuration

Enter information below to configure the Application Server

- Administrator user name for initial server instance.
- Administrator password for initial server instance (must be at least 8 characters in length).
- Administration server port number for initial server instance.
- HTTP/HTTPS port number for initial server instance.
- JMX port number for initial server instance.

Admin User (DEFAULT: admin): admin
Password (DEFAULT: ): secretsecret
Confirm Password (DEFAULT: ): secretsecret
Admin Port (DEFAULT: 4848): 4848
HTTP Port (DEFAULT: 9090): 9090
HTTPS Port (DEFAULT: 9191): 9191
JMX Port (DEFAULT: 8686): 8686

Control Panel Configuration

These are the settings for the Web Server hosting the Control Panel.
Enter the HTTP/HTTPS ports to configure the Web Server on the main instance:

HTTP Port (DEFAULT: 7070): 7070
HTTPS Port (DEFAULT: 7171): 7171

Port validation failed
Control Panel HTTP port These are the settings for the Web Server hosting the Control Panel. is invalid.
Please select a new one.
PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK): Enter
Control Panel Configuration

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

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

HTTP Port (DEFAULT: 7070): 7070
HTTPS Port (DEFAULT: 7171): 7171

Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name: RSA Adaptive Directory 7.1.5
Install Folder: /root/rsa/adaptivedirectory
Install Set: RSA Adaptive Directory New Cluster / Standalone
Product Features: Application, Sample Data
Java VM Installation Folder: /root/rsa/adaptivedirectory/jdk
Administrator User: cn=Directory Manager
Adaptive Directory Ports: 2389 8089 8090
Scheduler Port: 1099
SSL Configuration: 1636
Start TLS Configuration: TLS is disabled.
Certificate Configuration: Self signed certificate.
App Server Configuration: 4848 9090 9191 8686
Web Server Configuration: 7070 7171
Disk Space Information (for Installation Target):
Required: 1,164.03 MegaBytes
Available: 49,030.86 MegaBytes

PRESS <ENTER> TO CONTINUE: Enter

Installing...

[================================|==================|==================]
[------------------|------------------|------------------|------------------]
Installation Complete

Congratulations. RSA Adaptive Directory 7.1.5 has been successfully installed to:
/root/rsa/adaptivedirectory In order to start working with RSA Adaptive Directory 7.1.5, please follow these steps:
- LOG OFF
Then
- LOG IN
- Copy and paste your license key when prompted after running RSA Adaptive Directory 7.1.5
- Run /root/rsa/adaptivedirectory/bin/openControlPanel.sh

PRESS <ENTER> TO EXIT THE INSTALLER:

---

8.3 ADDITIONAL STEPS REQUIRED AFTER INSTALLATION IS COMPLETE

Then you need to install netstat: yum install net-tools
Copy the license.lic file to: /root/rsa/adaptivedirectory/vds_server
Open all relevant firewall ports on the CentOS server
Run /root/rsa/adaptivedirectory/bin/openControlPanel.sh
Run /root/rsa/adaptivedirectory/bin/runContextBuilder.sh
From a web browser go to: http://IPADDRESS:7070
Start the server by clicking the Start button.
Click on Tools menu item, and start the Application Server.

Configuration Procedure:
From a web browser, connect to the Adaptive Directory server and log in (Note the URL with port number) using the following credentials: (Default credentials) See Figure 109.
Username: cn=Directory Manager
Password: secretsecret
On the main page, Figure 110, start the Adaptive Directory server:

On the Tools tab, Figure 111, click Start it to start the Persistent Cache service:
Now go to the Settings tab, Figure 112 and click Server Backend Settings and then click LDAP Data Sources.

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

Now click on Directory, click on Configuration, right-click on Root Naming Contexts, and select Naming context as shown in Figure 114.
You are presented with this screen, Figure 115:

Enter the “name” you would like your new Virtual LDAP directory to be configured with. Select Virtual Tree and click Next.
Leave the defaults selected as shown in Figure 116, and click OK. You will see the following screen, Figure 117.

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

Right-click on your newly created Virtual Directory and select New Level as shown in Figure 118:
Enter a “name” for this LDAP backend mapping. This name will be an OU in the Virtual Directory as shown in Figure 119.

Right-click this new OU in your Virtual Directory and select Backend Mapping as shown in Figure 120.
Leave LDAP Backend selected and click Next as shown in Figure 121.
Now select one of your backend AD clusters we configured earlier and click OK as shown in Figure 122. Repeat this procedure for all your backend AD clusters (i.e., for the backend ADs on the IT, OT, and PACS networks). By default, the Adaptive Directory server will return default AD attributes.
8.4 CUSTOM ATTRIBUTE CONFIGURATION

Custom attributes are required and are configured as follows:

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

![Figure 123. Adaptive Directory Addition Attributes](image)

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

![Figure 124. Adaptive Directory Add/Edit Main Attribute](image)

Complete this procedure for any additional custom attributes that are required and for any additional AD backends to which you may need to add attributes.
Your Adaptive Directory virtual directory is now complete and can be accessed from RSA IMG / Aveksa or any other application that can access LDAP directories.

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

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

![Edit Collector: RSA AD Directory Account](image)

**Figure 125. Adaptive Directory Edit Collector**

![Search Configuration for Accounts](image)

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

### 8.5 RSA AD OPTIMIZATION AND TUNING

#### 8.5.1 Disable Referral Chasing

Referral chasing should be disabled for performance reasons. Check the Disable Referral Chasing option when you define the LDAP data source.
8.5.2 Limit Attributes Requested from the LDAP Backend

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

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

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

8.5.3 Process Joins and Computed Attributes Only When Necessary

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

8.5.4 Use the Client Sizelimit Value to Query the Backend

Whenever Adaptive Directory queries a backend LDAP, the default behavior is to ask for all entries (sizelimit=0) even if the client to Adaptive Directory indicates a sizelimit. This is the default behavior because the entries returned by the backend are possible candidates but may not be retained for the final result that is sent to the client. For example, if an ACL has been defined in Adaptive Directory, not all entries from the backend may be authorized for the user (who is connected to Adaptive Directory) to access. As another example, when joins or interception scripts are involved with the virtual view, they may also alter the entries that match the client's search. To limit the number of entries from the backend, using paging is the
recommended approach. If the backend supports paging, Adaptive Directory will not get all the results at once; rather, it will get only one page at a time (pagesize is indicated in the configuration). In this case, if Adaptive Directory has returned to the client the sizelimit required, Adaptive Directory will not go to the next page.

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

9 PRIVILEGED USER ACCESS CONTROL: ALERTENTERPRISE GUARDIAN INSTALLATION

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

9.1 SECURITY CHARACTERISTICS

Cybersecurity Framework Categories: PR.AC-1: Identities and credentials are managed for authorized devices and users
NIST 800-53 rev 4 Security Controls: AC-2, IA Family

9.2 INSTALLATION ON TOMCAT AND WINDOWS

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

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

Installation Prerequisites

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

Pre-Installation Verification
Before you start installing AlertEnterprise product, verify the proper functioning of the underlying software systems. Verify that:

- Your system meets all the software and hardware prerequisites as described in Systems Requirement Specification document.
- Compatible version of Java Runtime Environment (JRE) is installed and working on the system.
- Compatible version of the web server is installed and running.
- Compatible version of the database server is installed and running.
- Supported Internet Browser (for example, Microsoft Internet Explorer) is working properly.


Installing Mandatory Software Applications

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

Installing JRE

To install JRE:

1. Download the application server-compatible JRE.
2. Double-click the setup launcher to start the installation process.

Setting Java Home

1. Make sure that JAVA_HOME variable is set to the folder where Java is installed and %JAVA_HOME%/bin is in the system’s path.
2. Open the Command Prompt in Administrator Mode (Right Click > Run As Administrator) and issue:

   Set JAVA_HOME=<PATH OF JDK/JRE>

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

3. Setting Path:

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

4. Checking JAVA_HOME and PATH:

   Echo %JAVA_HOME%
   Echo %PATH%
Checking JAVA Version: Java -version

Running ActiveMQ as Windows Service

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

1. Go to the folder apache-activemq and move to bin/win32 in Windows Explorer and right-click on InstallService.bat file and select Run as Administrator. Refer to .

2. Once the above batch file gets executed, verify that the ActiveMQ is added as Windows Services.

3. Go to Run command and enter services.msc. The Services window appears. Refer to the following screen shot.

![Services (Local)]( servicios.png)

Figure 127. Adaptive Directory Search Configuration for Accounts

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

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

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

   - Search for the URL that starts with TCP ://<IP Address>:61616 in activemq.log located in Apache ActiveMQ home directory/data folder.

Refer to the following screen shot:
• 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>`.

**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.

```bash
: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:

```bash
# Java Application
```
wrapper.java.command=java

to this:

# Java Application

wrapper.java.command=%JAVA_HOME%\bin\java.exe

After you have performed these steps, you should be able to run the InstallService.bat successfully.

5. To also use the UninstallService.bat file, open it and hard-code the path to the wrapper:

rem
rem Uninstall the Wrapper as an NT service.
rem
:startup
"%ACTIVEMQ_HOME%/bin/win32/wrapper.exe" -r %_WRAPPER_CONF%
if not error level 1 goto : eof
pause

After executing the InstallService.bat file, you can see the ActiveMQ in Services.

6. If the ActiveMQ server is not up and the system throws the following error:

| WARN | tmpdir | org.eclipse.jetty.util.log | WrapperSimpleAppMainjava.io.IOException: The system cannot find the path specified

at java.io.WinNTFileSystem.create File Exclusively (Native Method)
at java.io.File.check And Create (File.java:1343)
at java.io.File.create Temp File (File.java:1431)

Solution:

You must manually create two folders: <ActiveMQ home directory>/work and <ActiveMQ home directory>/temp.

To check whether ActiveMQ is started, access the following link as shown in Figure 129.

http://<Server IP Address>:8161/admin/
Installing Apache Tomcat

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

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

Apache Tomcat Configuration

You need to specify Tomcat configuration as specified in the following steps:
1. Click Start > Programs > Apache Tomcat > Configure Tomcat option.
2. Click Java tab in the Apache Tomcat Properties dialog box.
3. Enter the following settings:
   - Initial memory pool: 1024
   - Maximum memory pool: 1024
   - Thread stack size: 300

   *Note:* These settings may vary with the volume of random access memory (RAM) in the server.
4. Click Apply and OK to close the dialog box.

**Configuring Database Server**

You need to perform some configurations in the database server to install AlertEnterprise applications. You must perform these configurations through the database administrator login.

The current version of AlertEnterprise products supports Oracle and MS SQL Server databases. The NCCoE build also supports MySQL server database.

To configure the database server:

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

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

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

Follow these steps to avoid case-sensitivity issues:

1. Create a trigger to support case insensitiveness.

```sql
/*************/
create or replace
trigger set_nls_onlogon
AFTER LOGON ON SCHEMA
DECLARE
```
BEGIN
EXECUTE IMMEDIATE 'ALTER SESSION SET NLS_SORT="BINARY_CI"';
EXECUTE IMMEDIATE 'ALTER SESSION SET NLS_COMP="LINGUISTIC"';
END set_nls_onlogon;
/*******************/
  2. Restart the AlertEnterprise Application server.

The effect may not be visible in some client tools like SQL Developer. To see the effect in the
SQL Developer tool:
  1. Open SQL Developer and click Tools > Preferences.
  2. Click Database > NLS and do the following:
     • Set the Sort option to BINARY_CI.
     • Set the Comparison option to LINGUISTIC.

Enabling Support for International Characters
Storage of character data is controlled by character-set setting at database level. It is
recommended to have the following database settings to support international characters:

For Oracle:
NLS_CHARACTERSET = AL32UTF8
NLS_NCHAR_CHARACTERSET = AL16UTF16

For SQL Server:
• Server Collation = SQL_Latin1_General_CP1_CI_AS

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

  1. Stop the Tomcat server from the Windows services if it is already running. Click Start >
     Run and type services.msc then click OK. Select the Apache Tomcat and click the
     Stop Service icon to stop the service.
  2. Copy the AlertEnterprise.war, AccessMap.war (if you possess AlertInsight
     license), and AlertEnterpriseHelp.war, and jasperserver-pro.war files
to <Tomcat installation folder>\webapps\ path.
  3. You need to copy password management war file AIPM.war to <Tomcat
     installation folder>/webapps if you possess license for the Password
     Management application.
  4. Create a new folder AlertCommonLib and AlertExternalLib under
     <Tomcat Installation Folder>.
5. Extract `AlertCommonLib.zip` under `AlertCommonLib` folder. You will see many new files in this folder.

6. Edit the `<Tomcat Installation Folder>\conf\catalina.properties` using any editor and add append the following to the common.loader as described below:
   ```properties
   common.loader=${catalina.base}/lib,${catalina.base}/lib/*,${catalina.home}/lib,${catalina.home}/lib/*,${catalina.home}/AlertCommonLib/*,${catalina.home}/AlertExternalLib/* (bold path added). Save the file and close the editor.
   ```

7. Add Database Connection. Add a new <resource> entry as below with name "jdbc/alntdb" in `<Tomcat installation folder>\conf\context.xml`. Replace the code in <> with relevant information.

   For MY-SQL Server:
   ```xml
   <Resource description="DB Connection" name="jdbc/alntdb" auth="Container" type="com.mchange.v2.c3p0.ComboPooledDataSource" factory="org.apache.naming.factory.BeanFactory" user="username" password="password" jdbcUrl="jdbc:mysql://<IP of DB Server>:3306/<DB Instance Name>" driverClass="com.mysql.jdbc.Driver" maxPoolSize="100" minPoolSize="5" acquireIncrement="5" numHelperThreads="20" maxIdleTime="600" maxIdleTimeExcessConnections="300" debugUnreturnedConnectionStackTraces="true" unreturnedConnectionTimeout="900"/>
   ```

For repository setting in same `context.xml`, add the following entry:
   ```xml
   <ResourceLink name="AlertEnterpriseRepo" global="AlertEnterpriseRepo" type="javax.jcr.Repository" />
   ```

For ActiveMQ settings in same context.xml, add the following entry:
   ```xml
   ```
brokerName="LocalActiveMQBroker"
useEmbeddedBroker="false"/>

<Resource name="jms/requestSubmissionQueue"
    auth="Container"
    type="org.apache.activemq.command.ActiveMQQueue"
    description="JMS Queue requestSubmissionQueue"
    factory="org.apache.activemq.jndi.JNDIReferenceFactory"
    physicalName="requestSubmissionQueue"/>

<Resource name="jms/requestApprovalQueue"
    auth="Container"
    type="org.apache.activemq.command.ActiveMQQueue"
    description="JMS Queue requestApprovalQueue"
    factory="org.apache.activemq.jndi.JNDIReferenceFactory"
    physicalName="requestApprovalQueue"/>

<Resource name="jms/autoApprovalQueue"
    auth="Container"
    type="org.apache.activemq.command.ActiveMQQueue"
    description="JMS Queue autoApprovalQueue"
    factory="org.apache.activemq.jndi.JNDIReferenceFactory"
    physicalName="autoApprovalQueue"/>

<Resource name="jms/queue/taskSubmissionQueue"
    auth="Container"
    type="org.apache.activemq.command.ActiveMQQueue"
    description="JMS Queue taskSubmissionQueue"
    factory="org.apache.activemq.jndi.JNDIReferenceFactory"
    physicalName="taskSubmissionQueue"/>

<Resource name="jms/queue/taskRejectionQueue"
    auth="Container"
    type="org.apache.activemq.command.ActiveMQQueue"
    description="JMS Queue taskRejectionQueue"
    factory="org.apache.activemq.jndi.JNDIReferenceFactory"
    physicalName="taskRejectionQueue"/>

<Resource name="jms/queue/projectCancelQueue"
    auth="Container"
    type="org.apache.activemq.command.ActiveMQQueue"
    description="JMS Queue projectCancelQueue"
factory="org.apache.activemq.jndi.JNDIReferenceFactory"
physicalName="projectCancelQueue"/>

<Resource name="jms/queue/projectCompleteQueue"
   auth="Container"
type="org.apache.activemq.command.ActiveMQQueue"
description="JMS Queue projectCompleteQueue"
   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
physicalName="projectCompleteQueue"/>

<Resource name="jms/eventRequestQueue"
   auth="Container"
type="org.apache.activemq.command.ActiveMQQueue"
description="JMS Queue eventRequestQueue"
   factory="org.apache.activemq.jndi.JNDIReferenceFactory"
physicalName="eventRequestQueue"/>

<Resource auth="Container" description="my Queue"
factory="org.apache.activemq.jndi.JNDIReferenceFactory"
name="jms/reqQueue" physicalName="requestQueue"
type="org.apache.activemq.command.ActiveMQQueue"/>

<Resource auth="Container" description="my Queue"
factory="org.apache.activemq.jndi.JNDIReferenceFactory"
name="jms/resQueue" physicalName="responseQueue"
type="org.apache.activemq.command.ActiveMQQueue"/>

8. Edit <Tomcat installation folder>\conf\server.xml. Replace the code in <> with relevant information:

<GlobalNamingResources>
</GlobalNamingResources>
<! -- Editable user database that can also be used by UserDatabaseRealm to authenticate users -->
<Resource auth="Container"
configFile="/AlertEnterpriseRepo/repository.xml"
description="AlertEnterprise Repository"
factory="com.alnt.repository.jndi.JackrabbitRepositoryFactory"
homeDir="/AlertEnterpriseRepo" name="AlertEnterpriseRepo"
type="javax.jcr.Repository"/>

<Resource auth="Container" description="Rule Engine Service"
factory="com.sae.ruleengine.jndi.RuleEngineFactory"
9. Open `<Webserver installation folder>\bin` location and double-click `tomcat5w.exe`. Click Java tab and under Java options add the following lines at the end:

- `-XX:PermSize=512m`
- `-XX:MaxPermSize=512m`
- `-Xms1024m`
- `-Xmx1024m`
- `-Djs.license.directory=C:\AlertApplication\Tomcat 6.0\webapps\jasperserver-pro`
- `-Dcom.alnt.fabric.loadInitData=force`
- `-Dalert.db.update=update`

*Note:* These settings may vary with the volume of RAM in the server.

10. Start the Tomcat server.

11. Start the AlertEnterprise application by using the address, which is of the form `http://<Server IP Address>:8080/AlertEnterprise`.

*Note:* The name and contents of the init script will vary depending on the database management system of the organization. 8080 is the default port on local host. If you want to change it, then change it in the `server.xml`.

12. Log on to the application by using admin credentials. You should be able to view Home screen of the application.

### 9.3 ALERTENTERPRISE APPLICATION CONFIGURATIONS FOR THE RSA BUILD

#### Systems/Connectors

9.3.1 **System Type Import of DB Connector:**

1. Log in to Application.

2. Go to Setup tab > Manual Configuration > Import/Export.

3. Check System Types and click on Import.
4. Select the .csv files, which are there in the software build package under connector ALNTDbconnector\InitDataFiles folder.

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

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

7. Restart the server if required.

9.3.2 System Types Param of DB Connector:

1. Log in to Application.

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

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

4. Click on Next button.

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

   The following fields need to be provided under Name field and Label can be any user-friendly name see Figure 130.

<table>
<thead>
<tr>
<th>Name</th>
<th>Label</th>
<th>Parameter Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>jndiName</td>
<td>Jndi Name</td>
<td>Mandatory</td>
</tr>
<tr>
<td>DATE_TIME_FORMAT</td>
<td>Date and Time Format</td>
<td>Mandatory</td>
</tr>
<tr>
<td>DATE_TIME</td>
<td>Date Format</td>
<td>Mandatory</td>
</tr>
<tr>
<td>passwordColumnName</td>
<td>Password Column Name</td>
<td>Mandatory</td>
</tr>
<tr>
<td>useridColumnName</td>
<td>UserId Column Name</td>
<td>Mandatory</td>
</tr>
<tr>
<td>EXTERNAL_USER_ID_ATT</td>
<td>External UserId Att</td>
<td>Mandatory</td>
</tr>
<tr>
<td>MODIFIED_ENTITLEMENT</td>
<td>Fetch User Entitlement</td>
<td>Mandatory</td>
</tr>
<tr>
<td>GET_ALL_USERS0</td>
<td>GET_ALL_USERS0</td>
<td>Mandatory</td>
</tr>
<tr>
<td>GET_INCREMENTAL_USE</td>
<td>GET_INCREMENTAL_USE</td>
<td>Mandatory</td>
</tr>
<tr>
<td>CREATE_USER0</td>
<td>Create Cardholder Q.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>UPDATE_USER0</td>
<td>Update Cardholder Q.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>LOCK_USER0</td>
<td>Lock Cardholder Que</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
Figure 130. Guardian DB Connector Attributes

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

2. Click on New to create a new system.
3. Definition...Enter the following:
   - **System Type** – LDAP from drop-down
   - **Connector Name** – PACS AD
   - **Connector Description** - PACS AD
   - **Connector Long Description** - PACS AD
   - **Connector Type** – LDAP (default)
4. Click on Next.
5. Parameters...Enter the following:

<table>
<thead>
<tr>
<th>System Param Name</th>
<th>System Param Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bindPass</td>
<td>o60ypIUQT3IOqHmbuRWeuw==</td>
</tr>
<tr>
<td>useSSL</td>
<td>FALSE</td>
</tr>
<tr>
<td>baseDns</td>
<td>DC=pacs-es-idam-b1,DC=test</td>
</tr>
<tr>
<td>groupBaseDn</td>
<td>DC=pacs-es-idam-b1,DC=test</td>
</tr>
<tr>
<td>reconBaseDN</td>
<td></td>
</tr>
<tr>
<td>getIncrementGrpChanges</td>
<td>FALSE</td>
</tr>
<tr>
<td>System Param Name</td>
<td>System Param Value</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>wsdlURL</td>
<td></td>
</tr>
<tr>
<td>wsUserName</td>
<td></td>
</tr>
<tr>
<td>wsPwd</td>
<td></td>
</tr>
<tr>
<td>rootLevelDomain</td>
<td></td>
</tr>
<tr>
<td>cookieLocation</td>
<td></td>
</tr>
<tr>
<td>adUserName</td>
<td></td>
</tr>
<tr>
<td>SYS_CON_ATTR_POST_CREATE_SCRIPT</td>
<td></td>
</tr>
<tr>
<td>SYS_CON_ATTR_POST_CREATE_SCRIPT_PARAMS</td>
<td></td>
</tr>
<tr>
<td>objectClass</td>
<td>User</td>
</tr>
<tr>
<td>Skipprovisioning</td>
<td>Yes</td>
</tr>
<tr>
<td>lastModifiedColumnRole</td>
<td>whenChanged</td>
</tr>
<tr>
<td>lastModifiedColumn</td>
<td>whenChanged</td>
</tr>
<tr>
<td>host</td>
<td>172.16.7.2</td>
</tr>
<tr>
<td>port</td>
<td>389</td>
</tr>
<tr>
<td>bindDn</td>
<td>CN=AlertEnterprise, CN=Users,DC=pacs-es-idam-b1,DC=test</td>
</tr>
</tbody>
</table>

6. Click on Next.

7. Attributes...Enter the following:
   - Application – Alert Access
   - Check the following boxes – Provisioning, Role Management, Offline System.
   - Leave Connector Category as Production.
   - Time Zone – Greenwich Mean Time from drop-down

8. Click on Next.

9. Click on Save.

**CONFIGURATION: Create “Identity DB” System**
2. Click on New to create a new system.
3. Definition...Enter the following:
   • System Type – Database (JDBC J2EE) from drop-down
   • Connector Name – IDENTITYDB
   • Connector Description - IDENTITYDB
   • Connector Long Description - IDENTITYDB
   • Connector Type – Database (JDBC J2EE) (default)
4. Click on Next.
5. Parameters...Enter the following:

<table>
<thead>
<tr>
<th>System Param Name</th>
<th>System Param Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>driverName</td>
<td></td>
</tr>
<tr>
<td>url</td>
<td></td>
</tr>
<tr>
<td>userName</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td></td>
</tr>
<tr>
<td>whereClause</td>
<td></td>
</tr>
<tr>
<td>jndiName</td>
<td>java:comp/env/jdbc/alntdb</td>
</tr>
</tbody>
</table>
6. Click on Next.
7. Attributes...Enter the following:
   • Application – All
   • Check the following boxes – Provisioning, Certification, Identity Provider, Allow Modify Role and Allow Time Change.
   • Leave Connector Category as Production.
   • Time Zone – Eastern Daylight Time from drop-down
8. Click on Next.
9. Click on Save.

CONFIGURATION: Create “ACCESSIT PACS” System
2. Click on New to create a new system.
3. Definition...Enter the following:
   - System Type – DBCConnector from drop-down
   - Connector Name – ACCESSIT PACS
   - Connector Description - ACCESSIT PACS
   - Connector Long Description - ACCESSIT PACS
   - Connector Type – DBCConnector (default)
4. Click on Next.
5. Parameters...Enter the following:

<table>
<thead>
<tr>
<th>System Param Name</th>
<th>System Param Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>driverName</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>jdbc:sqlserver://&lt;HOST_NAME&gt;:&lt;PORT&gt;;databaseName=AI Universal</td>
</tr>
<tr>
<td>userName</td>
<td>DB User Name</td>
</tr>
<tr>
<td>password</td>
<td>DB User Password</td>
</tr>
<tr>
<td>Date and Time Format</td>
<td>CardholderID</td>
</tr>
<tr>
<td>External UserId Attribute</td>
<td>CardholderID</td>
</tr>
<tr>
<td>Create CardHolder Query</td>
<td>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(), ‘alerten’, ‘1’, $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, ‘1’, $CardholderActiveDate, $CardholderExpireDate)</td>
</tr>
<tr>
<td>Update CardHolder Query</td>
<td>update [dbo].[Cardholders] set LastModified=GetUTCDate() where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>System Param Name</td>
<td>System Param Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lock CardHolder Query</td>
<td>update [dbo].[Cardholders] set CardholderStatus='0' where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>Unlock Card Holder Query</td>
<td>update [dbo].[Cardholders] set CardholderStatus='1' where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>Check Card Holder Provisioned Query</td>
<td>select CardholderID from [dbo].[Cardholders] where CardholderID = $CardholderID</td>
</tr>
<tr>
<td>Assign Roles to Card Holder Query</td>
<td>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)</td>
</tr>
<tr>
<td>Remove Roles From Card Holder Query</td>
<td>delete from [dbo].[CardholderAccessLevels] where CardholderID=$CardholderID and AccessLevelID=(select AccessLevelID from [dbo].[AccessLevels] where AccessLevelName=$ROLE_NAME)</td>
</tr>
<tr>
<td>Retrieve User Id Query</td>
<td>select CardholderID from [dbo].[Cardholders] where UserText1=$UserText1</td>
</tr>
<tr>
<td>CREATE_USER1</td>
<td>INSERT INTO [AllUniversal].[dbo].[Cards] ([CardID],[CardholderID],[CardNumber],[FacilityCode],[PINNumber],[PINExempt],[APBExempt],[UseExtendedAccessTimes],[CardStatus],[ActiveDate],[ExpireDate],[UserLevel],[UseCustomReporting],[EventInfo],[Notes],[LastModified],[LastModifiedByUser],[DateCreated],[CreatedByUser],[IssueLevel],[DeactivateExempt],[VacationDate],[VacationDuration],[UseCount],[TempDeactivateStart],[TempDeactivateEnd],[Classification],[IPLocksetAccessMode],[IPLocksetCredentialFormat],[IPLocksetAccessAlways],[RawPrimaryCredential],[LargeEncodedCardID],[EmbossedNumber]) VALUES (NEWID(),(select CardholderID from [dbo].[Cardholders] where UseText1=$UserText1),$CardNumber,$FacilityCode,$PIN,'0','0','0','1',NULL,NULL,'0','0',NULL,NULL,'alertent',SYSDATETIME(),'alertent',SYSDATETIME(),'alertent','0','0','255','Active',NULL,NULL,NULL,NULL,NULL,NULL,&quot;&quot;)</td>
</tr>
<tr>
<td>LOCK_USER1</td>
<td>update [AllUniversal].[dbo].[Cards] set CardStatus='0',Classification='InActive' where [CardNumber]=$CardNumber</td>
</tr>
</tbody>
</table>

6. Click on Next.
7. Attributes...Enter the following:
   - 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
8. Click on Next.
9. Click on Save.

Identity & Access – Enable Identity

2. Enable the following for “Identity DB” system, see Figure 131.
9.3.3 **Identity & Access—User Field Mapping**

2. Select User = Identity (from drop-down) and click on Go.
3. Click the Create New button.
   Select values for respective fields and hit on save (Refer to below sheet for values selection.)
4. Repeat Steps 1–4 for all fields in the sheet.

Follow the steps above to configure the User Field mappings manually. You can match the 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).

**Identity & Access > Recon Authoritative Fields**

2. Click on Create.
3. Enter the following shown in Figure 132.

```
<table>
<thead>
<tr>
<th>Recon Authoritative Fields</th>
<th>Authoritative Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>System: DBCONNECTOR</td>
<td>FirstName</td>
</tr>
<tr>
<td>System: DBCONNECTOR</td>
<td>LastName</td>
</tr>
<tr>
<td>System: PACS AD</td>
<td>PacsAllDoors</td>
</tr>
<tr>
<td>System: PACS AD</td>
<td>PacsHomeAccess</td>
</tr>
<tr>
<td>System: PACS AD</td>
<td>PacsWorkAccess</td>
</tr>
<tr>
<td>System: PACS AD</td>
<td>FirstName</td>
</tr>
<tr>
<td>System: PACS AD</td>
<td>LastName</td>
</tr>
</tbody>
</table>
```

**Identity & Access > Request Categories**

2. Click on New.
3. Enter following at define Request Category screen:
   - Name – New Hire
   - Description – New Hire
4. Click on Save.

5. Repeat similar to above for following Request Categories:

**Termination**

- Name – Change Access
- Description – Change of Access
- Visible – Yes
- Hover Text –
- Provisioning Actions – Create User, Change Roles, Change User
- Display the following in USS – Resources
- Add Existing – Systems and Remove Roles

6. Click on Save.

**ChangeAccess**

- Name – Terminate
- Description – Terminate User
- Visible – Yes
- Hover Text –
- Provisioning Actions – Lock User, Change Roles
- Display the following in USS – Resources
- Add Existing – Systems

7. Click on Save.

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


2. On the next screen select System and click Next.
3. Follow the mapping shown in Figure 133 to Create/Update provisioning mappings for the ACCESS IT PACS system.

![Figure 133. Guardian DB Connector Attribute Mapping]

<table>
<thead>
<tr>
<th>User Data&gt; User Data Source</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>User Data&gt; User Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Select “Identity DB” system from the list and click on Save button.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Engine&gt; Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Click on New and add the following:</td>
</tr>
</tbody>
</table>

**Table 12. Guardian Policy Engine Rules**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Entity Type</th>
<th>Rule Type</th>
<th>Description</th>
<th>Applicable to</th>
<th>Attributes</th>
<th>Drop down value</th>
<th>Selection Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Door Access New</td>
<td>Workflow</td>
<td>AlertAccess</td>
<td>All Door Access New</td>
<td>Suggest/Default</td>
<td>PacsAllDoors AND Request Category</td>
<td>Equals</td>
<td>2. True and New Hire</td>
</tr>
</tbody>
</table>
Policy Engine> Suggest/Default Access

2. Click on New and enter the following:

Table 13. Guardian Policy Engine Suggest/Default Access

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Rule Name</th>
<th>Search By</th>
<th>Default System</th>
<th>Selected Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Door Access</td>
<td>Default</td>
<td>All Door Access NEW Systems</td>
<td>ACCESSIT PACS</td>
<td>ALL DOORS</td>
<td></td>
</tr>
<tr>
<td>Home Access Level</td>
<td>Default</td>
<td>Home Access Level Systems</td>
<td>ACCESSIT PACS</td>
<td>Home Access Level</td>
<td></td>
</tr>
<tr>
<td>WO Access Level</td>
<td>Default</td>
<td>Home Access Level Systems</td>
<td>ACCESSIT PACS</td>
<td>WO Access Level</td>
<td></td>
</tr>
<tr>
<td>NewHireDefaultSystems</td>
<td>Default</td>
<td>NewHireDefaultSystems Systems</td>
<td>ACCESSIT PACS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Policy Engine> Rule Action Handler

2 – Click New and create the following Action Handlers:

Table 14. Guardian Policy Engine Rule Action Handler

<table>
<thead>
<tr>
<th>Action Handler Name</th>
<th>Workflow</th>
<th>Task Type</th>
<th>Value</th>
<th>Priority</th>
<th>Update Identity Info</th>
<th>Evaluate Enterprise Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon New Hire</td>
<td>AlertAccess</td>
<td>Recon Create Request</td>
<td>New Hire</td>
<td>0</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Recon terminate Handler</td>
<td>AlertAccess</td>
<td>Recon Create Request</td>
<td>Terminate</td>
<td>0</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Recon Error Handler</td>
<td>AlertAccess</td>
<td>Recon Exception Record Task</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ReconChangeHandler | AlertAccess | Recon Create Request | Change Access | 0 | Yes | No

1. Policy Engine > Policy Designer
   2. Select New to create new Policy designer as:

   **User Policy New**
   1. Name – User Policy New
   2. Rule Type – AlertAccess
   3. Description – User Policy
   4. Priority – 29
   5. Active – Yes
   6. Default Process – No

   Figure 134 depicts the new policy interface to create the User Policy described above.
The following table describes User Policy New.

**Table 15. Guardian User Policy**

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

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.
Table 16. Guardian Job Scheduler Triggers Field Map

<table>
<thead>
<tr>
<th>AE Attribute</th>
<th>Mapped Key</th>
<th>userType</th>
<th>roleType</th>
<th>userRole</th>
<th>userBadge</th>
<th>userEnt RoleType</th>
<th>User Training Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sAMAccountName</td>
<td>Userld</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>accountExpires</td>
<td>ValidTo</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>givenName</td>
<td>FirstName</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>sn</td>
<td>LastName</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>userAccountControl</td>
<td>statusLDAP</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>pacsAllDoors</td>
<td>PacsAllDoors</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>pacsHomeAccess</td>
<td>PacsHomeAccess</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>pacsWorkAccess</td>
<td>PacsWorkAccess</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

**Job Scheduler>Triggers**

1. Setup > Manual Configuration > Job Scheduler > Triggers
2. Click New and create the following Triggers:

**AlertDbConnectorTrigger**

Table 17. Guardian Job Scheduler Triggers

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Batch Size</th>
<th>Number of Attempts</th>
<th>Policy Designer for</th>
</tr>
</thead>
<tbody>
<tr>
<td>PACSAD Trigger</td>
<td>PACSAD Trigger</td>
<td>Reconciliation</td>
<td>100</td>
<td>3</td>
<td>User policy New</td>
</tr>
<tr>
<td>Users/Roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:</td>
<td>PACS AD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconciliation From</td>
<td>PACS AD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconciliation System</td>
<td>PACS AD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field Mapping Group</td>
<td>PACSAD Field Map</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Type</td>
<td>True</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Role</td>
<td>True</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Click New and enter the following as shown in Figure 135:
   - Job Type – Reconciliation Job
   - Job Name - <Job Name>
   - Reconciliation for – User
   - Reconciliation Type – Incremental Reconciliation
   - Reconciliation Triggers – PACSAD Trigger
   - Select the schedule as Immediate, Once, periodic or Advance. For Periodic Job, specify the Job Start date, End date, and duration of job frequency.
3. Click Save.

9.4 SECTION 3. ALERT ENTERPRISE APPLICATION CONFIGURATIONS FOR THE CA BUILD

9.4.1 System Type Import of DB Connector:

1. Log in to Application.
2. Go to Setup tab > Manual Configuration > Import/Export
3. Check System Types and click on Import.
4. Select the .csv files, which are there in software build package under Connector \ALNTDbconnector\InitDataFiles folder.
5. After selecting all the files, click on Upload button.
6. Refresh page until it shows as success or failed.
7. Restart the server if required.

9.4.2 **System Types Param of DB Connector:**
1. Log in to Application.
2. Go to Setup tab > Manual Configuration _> Systems > System Types
3. Search for Connector named “DBConnector” and click on Modify button.
4. Click on Next.
5. Add the following attributes one by one and click on the ADD button.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>jndiName</td>
<td>Jndi Name</td>
</tr>
<tr>
<td>DATE_TIME_FORMAT</td>
<td>Date and Time Format</td>
</tr>
<tr>
<td>DATE_TIME</td>
<td>Date Format</td>
</tr>
<tr>
<td>passwordColumnName</td>
<td>Passwrpd Column Name</td>
</tr>
<tr>
<td>userIdColumnName</td>
<td>Userld Column Name</td>
</tr>
<tr>
<td>EXTERNAL_USER_ID_ATTRIBUTE</td>
<td>External Userld Attribute</td>
</tr>
<tr>
<td>MODIFIED_ENTITLEMENTS</td>
<td>Fetch User Entitlement based on last modified date(not by user)</td>
</tr>
<tr>
<td>GET_ALL_USERS0</td>
<td>GET_ALL_USERS0</td>
</tr>
<tr>
<td>GET_INCREMENTAL_USERS0</td>
<td>GET_INCREMENTAL_USERS0</td>
</tr>
<tr>
<td>CREATE_USER0</td>
<td>Create CardHolder Q...</td>
</tr>
<tr>
<td>UPDATE_USER0</td>
<td>Update CardHolder Q...</td>
</tr>
<tr>
<td>LOCK_USER0</td>
<td>Lock CardHolder Q...</td>
</tr>
</tbody>
</table>

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

Table 18. Guardian Name and Label Fields
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATE_USER0</td>
<td>Create CardHolder Query</td>
</tr>
<tr>
<td>UPDATE_USER0</td>
<td>Update CardHolder Query</td>
</tr>
<tr>
<td>LOCK_USER0</td>
<td>Lock CardHolder Query</td>
</tr>
<tr>
<td>UNLOCK_USER0</td>
<td>Unlock Card Holder Query</td>
</tr>
<tr>
<td>DELIMIT_USER0</td>
<td>Change CardHolder Validity Query</td>
</tr>
<tr>
<td>USER_PROVISIONED0</td>
<td>Check Card Holder Provisioned Query</td>
</tr>
<tr>
<td>ADD_ROLES0</td>
<td>Assign Roles to Card Holder Query</td>
</tr>
<tr>
<td>DEPROVE_ROLES0</td>
<td>Remove Roles From Card Holder Query</td>
</tr>
<tr>
<td>GET_GENERATED_USERID0</td>
<td>Retrieve User Id Query</td>
</tr>
<tr>
<td>driverName</td>
<td>driverName</td>
</tr>
<tr>
<td>url</td>
<td>URL</td>
</tr>
<tr>
<td>userName</td>
<td>userName</td>
</tr>
<tr>
<td>password</td>
<td>password</td>
</tr>
<tr>
<td>CREATE_USER1</td>
<td>CREATE_USER1</td>
</tr>
<tr>
<td>LOCK_USER1</td>
<td>LOCK_USER1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Label</th>
<th>Parameter Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>jndiName</td>
<td>Jndi Name</td>
<td>Mandatory</td>
</tr>
<tr>
<td>DATE_TIME_FORMAT</td>
<td>Date and Time Format</td>
<td>Mandatory</td>
</tr>
<tr>
<td>DATE_TIME</td>
<td>Date Format</td>
<td>Mandatory</td>
</tr>
<tr>
<td>passwordColumnName</td>
<td>Password Column Name</td>
<td>Mandatory</td>
</tr>
<tr>
<td>userIdColumnName</td>
<td>User Id Column Name</td>
<td>Mandatory</td>
</tr>
<tr>
<td>EXTERNAL_USER_ID_AT</td>
<td>External User Id At</td>
<td>Mandatory</td>
</tr>
<tr>
<td>MODIFIED_ENTITLEMENT...</td>
<td>Fetch User Entitlement...</td>
<td>Mandatory</td>
</tr>
<tr>
<td>GET_ALL_USERED</td>
<td>GET_ALL_USERED</td>
<td>Mandatory</td>
</tr>
<tr>
<td>GET_INCREMENTAL_USE...</td>
<td>GET_INCREMENTAL_USE...</td>
<td>Mandatory</td>
</tr>
<tr>
<td>CREATE_USERED</td>
<td>Create CardHolder Query</td>
<td>Mandatory</td>
</tr>
<tr>
<td>UPDATE_USERED</td>
<td>Update CardHolder Query</td>
<td>Mandatory</td>
</tr>
<tr>
<td>LOCK_USERED</td>
<td>Lock CardHolder Query</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>
Create System Connectors for all Target Systems

1. CONFIGURATION: Create connector for “Alert User Database (External)”

This connector is required to connect the Alert user table exposed to third-party systems (CA in this case) and get the data.

Steps to create this connector:

2. Click New to create a new system.
3. Definition...Enter the following:
   - System Type – DBConnector
   - Connector Name – ALERTDBCONNECTOR
   - Connector Description – ALERT DB CONNECTOR
   - Connector Long Description – ALERT DB CONNECTOR
   - Connector Type – DbConnector (Label)
4. Click on Next.
5. Parameters...Enter the following:

<table>
<thead>
<tr>
<th>System Param Name</th>
<th>System Param Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jndi Name</td>
<td>java:comp/env/jdbc/alertdb</td>
</tr>
<tr>
<td>Date and Time Format</td>
<td>MM/dd/yyyy HH:mm:ss</td>
</tr>
<tr>
<td>GET_ALL_USERS0</td>
<td>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</td>
</tr>
<tr>
<td>System Param Name</td>
<td>System Param Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>GET_INCREMENTAL_USERS@0</strong></td>
<td>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_dtl where LastModifiedDate&gt; STR_TO_DATE($LAST_RUN_DATE,'%m/%e/%Y %H:%I:%S') and UserStatus='Active'</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External UserId Attribute</th>
<th>UserId</th>
</tr>
</thead>
<tbody>
<tr>
<td>Userld Column Name</td>
<td>UserId</td>
</tr>
</tbody>
</table>

6. Click on Next.

7. Attributes...Enter the following:
   - Application – Alert Access
   - Check the following boxes – Provisioning, Role Management, Offline System.
   - Leave Connector Category as Production
   - Time Zone – Eastern Daylight Time from drop-down

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

8. Click on Next.

9. Click on Save.

2. **CONFIGURATION: Create “Identity DB” System**

This is connector is required for internal purposes. Ignore this step if **Identity DB Connector** already setup

Steps to create this connector:


2. Click New to create a new system.

3. Definition...Enter the following:
   - System Type – Database (JDBC J2EE) from drop-down
   - Connector Name – IDENTITYDB
   - Connector Description - IDENTITYDB
4. Click on Next.
5. Parameters...Enter the following:
Table 20. Guardian Identity DB Parameters

<table>
<thead>
<tr>
<th>System Param Name</th>
<th>System Param Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>driverName</td>
<td>(use default)</td>
</tr>
<tr>
<td>url</td>
<td>(use default)</td>
</tr>
<tr>
<td>userName</td>
<td>(use default)</td>
</tr>
<tr>
<td>password</td>
<td>(use default)</td>
</tr>
<tr>
<td>whereClause</td>
<td>(use default)</td>
</tr>
<tr>
<td>jndiName</td>
<td>java:comp/env/jdbc/alntdb</td>
</tr>
</tbody>
</table>

6. Click on Next.
7. Attributes...Enter the following:
   - Application – All
   - Check the following boxes – Provisioning, Certification, Identity Provider, Allow Modify Role and Allow Time Change.
   - Leave Connector Category as Production
   - Time Zone – Eastern Daylight Time from drop-down
8. Click on Next.
9. Click on Save.

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

This connector is required for integrating with RS2 PACS system and performing various provisioning operations.

Steps to create this connector:

2. Click New to create a new system.
3. Definition...Enter the following:
   - System Type – DBConnector from drop-down
   - Connector Name – ACCESSIT PACS
   - Connector Description - ACCESSIT PACS
   - Connector Long Description - ACCESSIT PACS
4. Click on Next.
5. Parameters...Enter the following:

---

**Table 21. Guardian PACS DBConnector Parameters**

<table>
<thead>
<tr>
<th>System Param Name</th>
<th>System Param Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>driverName</td>
<td>com.microsoft.sqlserver.jdbc.SQLServerDriver</td>
</tr>
<tr>
<td>URL</td>
<td>jdbc:sqlserver://&lt;HOST_NAME&gt;:&lt;PORT&gt;;databaseName=AI Universal</td>
</tr>
<tr>
<td></td>
<td>&lt;HOST_NAME&gt; should be replaced with the hostname of the RS2 PACS system</td>
</tr>
<tr>
<td>username</td>
<td>Login User Name to connect to RS2 PACS database</td>
</tr>
<tr>
<td>Password</td>
<td>Login password to connect to RS2 PACS database</td>
</tr>
<tr>
<td>Date and Time Format</td>
<td>MM/dd/yyyy HH:mm:ss</td>
</tr>
<tr>
<td>External UserId Attribute</td>
<td>CardholderID</td>
</tr>
<tr>
<td>Create CardHolder Query</td>
<td>INSERT INTO [AIUniversal].[dbo].<a href="CardholderID,LastName,FirstName,MiddleInitial,CompanyID,Notes,LastModified,LastModifiedByUser,DateCreated,CardholderActiveDate,CardholderExpireDate">Cardholders</a> VALUES (NEWID(),$LastName,$FirstName,$MiddleInitial,$CompanyID,$Notes,GetUTCDate(),'alertent',GetUTCDate(),'alertent','1',$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,$UserDate5,$UserDate6,$UserDate7,$UserDate8,$UserDate9,$UserDate10,$UserDate11,$UserDate12,$UserDate13,$UserDate14,$UserDate15,$UserDate16,$UserDate17,$UserDate18,$UserDate19,$UserDate20,$UserDate21,$UserDate22,$UserDate23,$UserDate24,$UserDate25,$UserDate26,$UserDate27,$UserDate28,$UserDate29,$UserDate30,$UserDate31,$UserDate32,$UserDate33,$UserDate34,$UserDate35,$UserDate36,$UserDate37,$UserDate38,$UserDate39,$UserDate40,$UserDate41,$UserDate42,$UserDate43,$UserDate44,$UserDate45,$UserDate46,$UserDate47,$UserDate48,$UserDate49,$UserDate50,$UserDate51,$UserDate52,$UserDate53,$UserDate54,$UserDate55,$UserDate56,$UserDate57,$UserDate58,$UserDate59,$UserDate60,$UserDate61,$UserDate62,$UserDate63,$UserDate64,$UserDate65,$UserDate66,$UserDate67,$UserDate68,$UserDate69,$UserDate70,$UserDate71,$UserDate72,$UserDate73,$UserDate74,$UserDate75,$UserDate76,$UserDate77,$UserDate78,$UserDate79,$UserDate80,$UserDate81,$UserDate82,$UserDate83,$UserDate84,$UserDate85,$UserDate86,$UserDate87,$UserDate88,$UserDate89,$UserDate90,$UserDate91,$UserDate92,$UserDate93,$UserDate94,$UserDate95,$UserDate96,$UserDate97,$UserDate98,$UserDate99,$UserDate100,$UserDate101,$UserDate102,$UserDate103,$UserDate104,$UserDate105,$UserDate106,$UserDate107,$UserDate108,$UserDate109,$UserDate110,$UserDate111,$UserDate112,$UserDate113,$UserDate114,$UserDate115,$UserDate116,$UserDate117,$UserDate118,$UserDate119,$UserDate120,$UserDate121,$UserDate122,$UserDate123,$UserDate124,$UserDate125,$UserDate126,$UserDate127,$UserDate128,$UserDate129,$UserDate130,$UserDate131,$UserDate132,$UserDate133,$UserDate134,$UserDate135,$UserDate136,$UserDate137,$UserDate138,$UserDate139,$UserDate140,$UserDate141,$UserDate142,$UserDate143,$UserDate144,$UserDate145,$UserDate146,$UserDate147,$UserDate148,$UserDate149,$UserDate150,$UserDate151,$UserDate152,$UserDate153,$UserDate154,$UserDate155,$UserDate156,$UserDate157,$UserDate158,$UserDate159,$UserDate160,$UserDate161,$UserDate162,$UserDate163,$UserDate164,$UserDate165,$UserDate166,$UserDate167,$UserDate168,$UserDate169,$UserDate170,$UserDate171,$UserDate172,$UserDate173,$UserDate174,$UserDate175,$UserDate176,$UserDate177,$UserDate178,$UserDate179,$UserDate180,$UserDate181,$UserDate182,$UserDate183,$UserDate184,$UserDate185,$UserDate186,$UserDate187,$UserDate188,$UserDate189,$UserDate190,$UserDate191,$UserDate192,$UserDate193,$UserDate194,$UserDate195,$UserDate196,$UserDate197,$UserDate198,$UserDate199,$UserDate200,$UserDate201,$UserDate202,$UserDate203,$UserDate204,$UserDate205,$UserDate206,$UserDate207,$UserDate208,$UserDate209,$UserDate210,$UserDate211,$UserDate212,$UserDate213,$UserDate214,$UserDate215,$UserDate216,$UserDate217,$UserDate218,$UserDate219,$UserDate220,$UserDate221,$UserDate222,$UserDate223,$UserDate224,$UserDate225,$UserDate226,$UserDate227,$UserDate228,$UserDate229,$UserDate230,$UserDate231,$UserDate232,$UserDate233,$UserDate234,$UserDate235,$UserDate236,$UserDate237,$UserDate238,$UserDate239,$UserDate240,$UserDate241,$UserDate242,$UserDate243,$UserDate244,$UserDate245,$UserDate246,$UserDate247,$UserDate248,$UserDate249,$UserDate250,$UserDate251,$UserDate252,$UserDate253,$UserDate254,$UserDate255,$UserDate256,$UserDate257,$UserDate258,$UserDate259,$UserDate260,$UserDate261,$UserDate262,$UserDate263,$UserDate264,$UserDate265,$UserDate266,$UserDate267,$UserDate268,$UserDate269,$UserDate270,$UserDate271,$UserDate272,$UserDate273,$UserDate274,$UserDate275,$UserDate276,$UserDate277,$UserDate278,$UserDate279,$UserDate280,$UserDate281,$UserDate282,$UserDate283,$UserDate284,$UserDate285,$UserDate286,$UserDate287,$UserDate288,$UserDate289,$UserDate290,$UserDate291,$UserDate292,$UserDate293,$UserDate294,$UserDate295,$UserDate296,$UserDate297,$UserDate298,$UserDate299,$UserDate300)</td>
</tr>
<tr>
<td>Update CardHolder Query</td>
<td>update [dbo].[Cardholders] set LastModified=GetUTCDate() where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>Lock CardHolder Query</td>
<td>update [dbo].[Cardholders] set CardholderStatus='0' where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>Unlock Card Holder Query</td>
<td>update [dbo].[Cardholders] set CardholderStatus='1' where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>System Param Name</td>
<td>System Param Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Check Card Holder Provisioned Query</td>
<td>select CardholderID from [dbo].[Cardholders] where CardholderID=$CardholderID</td>
</tr>
<tr>
<td>Assign Roles to Card Holder Query</td>
<td>INSERT INTO [dbo].[CardholderAccessLevels] (CardholderID, [dbo].[AccessLevels] where AccessLevelName=$ROLE_NAME)</td>
</tr>
<tr>
<td>Remove Roles From Card Holder Query</td>
<td>delete from [dbo].[CardholderAccessLevels] where CardholderID=$CardholderID and AccessLevelID=(select AccessLevelID from [dbo].[AccessLevels] where AccessLevelName=$ROLE_NAME)</td>
</tr>
<tr>
<td>Retrieve User Id Query</td>
<td>select CardholderID from [dbo].[Cardholders] where UserText1=$UserText1</td>
</tr>
</tbody>
</table>

CREATE_USER1

INSERT INTO [AIUniversal].[dbo].[Cards] (CardID,CardholderID,CardNumber,FacilityCode,PINNumber,PINExempt,APBExempt,UseExtendedAccessTimes,CardStatus,ActiveDate,ExpireDate,UserLevel,UseCustomReporting,EventInfo,Notes,LastModifiedByUser,DateCreated,[CreatedByUser],[IssueLevel],[DeactivateExempt],[VacationDate],[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

6. Click on Next.

7. Attributes...Enter the following:
   - 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

8. Click on Next.

9. Click on Save.

Form customization – Attributes

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

### Table 22. **PacsAllDoors Attributes**

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

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

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

### Table 24. *PacsWorkAccess Attributes*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>PacsWorkAccess</td>
</tr>
<tr>
<td>Label</td>
<td>PacsWorkAccess</td>
</tr>
<tr>
<td>Description</td>
<td>PacsWorkAccess</td>
</tr>
</tbody>
</table>
3. Create **FacilityCode** Attributes as shown in Table 25.

### Table 25. FacilityCode Attributes

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>FacilityCode</td>
</tr>
<tr>
<td>Label</td>
<td>Facility Code</td>
</tr>
<tr>
<td>Description</td>
<td>Facility Code</td>
</tr>
<tr>
<td>Visible</td>
<td>Yes</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Yes</td>
</tr>
<tr>
<td>Read Only</td>
<td>No</td>
</tr>
<tr>
<td>Field Type</td>
<td>TextField (Select this value from drop down)</td>
</tr>
</tbody>
</table>
4. Create **PIN** Attributes as shown in Table 26.

**Table 26. PIN Attributes**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>PIN</td>
</tr>
<tr>
<td>Label</td>
<td>PIN</td>
</tr>
<tr>
<td>Description</td>
<td>PIN</td>
</tr>
<tr>
<td>Visible</td>
<td>Yes</td>
</tr>
<tr>
<td>Mandatory</td>
<td>No</td>
</tr>
<tr>
<td>Read Only</td>
<td>No</td>
</tr>
<tr>
<td>Field Type</td>
<td>TextField (Select this value from drop down)</td>
</tr>
<tr>
<td>USS Create Request</td>
<td>Yes(Select Check Box)</td>
</tr>
<tr>
<td>USS User Information</td>
<td>No(Select Check Box)</td>
</tr>
<tr>
<td>Approver View</td>
<td>No(Select Check Box)</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Yes(Select Check Box)</td>
</tr>
<tr>
<td>Create Request</td>
<td>12</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Value</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Sequence</td>
<td></td>
</tr>
<tr>
<td>User Info Sequence</td>
<td></td>
</tr>
<tr>
<td>Approver Sequence</td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>Personnel Information (Select this value from drop down)</td>
</tr>
</tbody>
</table>

2814

**Modify Employee Type Attribute**

2815

1. Setup > Manual Configuration > Form customization > Attributes
2816
2. Select Employee Type Field from list of Attributes and Click **Modify**
2817
3. **Click on DropDown Values Icon**
2818
4. On the popup window, Click on New and Provide Employee in both Name and Label fields, Figure 137.

![Create DropDownValues](image)

*Figure 137. Create DropDownValues*

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

![DropDown Values](image)

*Figure 138. Contractor Field*

6. Click **Save** and then Click **Save** to save the configuration
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 fields, Figure 139.
5. Similarly configure values for InActive field, Figure 140
6. Click Save and then Click Save to save the configuration
7. Ignore this step if these values already exists for Status field

Identity & Access– Enable Identity

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

Identity & Access– User Field Mapping

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

<table>
<thead>
<tr>
<th>Custom Field</th>
<th>Primary Key</th>
<th>Visible In List</th>
<th>IsSsearchable</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserId</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ValidFrom</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ValidTo</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FirstName</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LastName</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Email</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Building</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ManagerId</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BadgeStatus</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BadgeType</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BadgeValidFrom</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BadgeValidTo</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Location</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Badgeld</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>EmployeeType</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Department</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Password</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Groups</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ManagerName</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ManagerLN</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Manager</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ManagerId</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Status</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Telephone</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ImageUpload</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Password_AD</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PacsAllDoors</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PacsHomeAccess</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PacsWorkAccess</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Identity & Access > Recon Authoritative Fields**

2. Click on New.
3. Select ALERTDBCONNECTOR from Systems Drop down and select Authoritative field as PacsAllDoors as shown in

![Figure 142. Authoritative Fields]

4. Click Save button to save the mapping.

5. Repeat Steps 1-4 to configure mapping other fields PacsWorksAccess and PacsHomeAccess as listed in the screenshot shown in Figure 139.

![Figure 143. Guardian Recon Authoritative Fields]

Identity & Access > Request Categories

2. Select ChangeAccess Category name and Click Modify
3. On the Modify screen make following changes
   a. In the Provisioning Actions section Un select Delimit user and Change Validity Dates check boxes if they are selected
   b. Go to Add Existing section and select System and Remove Role option for Resources/Roles Drop down field
4. Click Save Button to save the configuration

Identity & Access>Provisioning>External Provisioning Attributes

2. Select ACCESSIT PACS system from the list and Click **Configure**

3. On the Next screen, Click on **New** Button and provide “LastName” in both Name and description fields

4. Click **Save** to save the configurations as shown in Figure 144.

![Create External Provisioning Attribute](image)

**Figure 144. External Provisioning Attribute**

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

![Attribute Fields](image)

**Figure 145. Attribute Fields**

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


2. Select ACCESSIT PACS and click on **Configure**.

3. On the Next Screen, Figure 146, Click **New** Button and select UserText1 from
Click on Save button to save the mapping.

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

Policy Engine > Rules

2. Click New Button
3. On the Next screen provide following information. See Figure 148.
4. Click Next Button

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

6. Repeat the step 5 to define rule condition for other request categories Remove User Access and ChangeAccess as shown in Figure 150.
7. Repeat Step 1-6 to configure Other Rules Home Access Level New and WO Access Level New as shown in following Table 21.

Table 28. Guardian Manual Configuration Policy Engine Rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Entity Type</th>
<th>Rule Type</th>
<th>Description</th>
<th>Applicable to</th>
<th>Attributes</th>
<th>Drop down value</th>
<th>Selection Value</th>
</tr>
</thead>
</table>
| 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 |
2. True and Remove User Access  
3. True and ChangeAccess |
2. True and Remove User Access  
3. True and ChangeAccess |

Policy Engine> Suggest/Default Access

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

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

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

6. Click Next Button

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

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

9. Click Save button to save the configuration

10. Repeat the steps 1-9 to configure other criteria for Home Access Level,


Table 29. Manual Configuration Policy Engine Suggest/Default Access

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Condition</th>
<th>Search By System</th>
<th>Selected System</th>
<th>Selected Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Door Access</td>
<td>Default</td>
<td>All Door Access</td>
<td>Yes</td>
<td>ACCESSIT PACS</td>
<td>ALL DOORS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NEW</td>
<td>(Select check box)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11. Select all existing Suggest Default Access criterias other than the one listed in Table 22 and Click **Delete** button to delete them.

**Policy Engine>Rule Action Handler**


2. In Action Handlers List page select ReconChangeHandler and Click **Modify**

3. On the next screen Select **Recon Create Request** Task Type and Click **Update Task**

4. On the popup window Click on **Value** drop down field and select **ChangeAccess** from the list as shown in Figure 152.

![Modify Task](image)

*Figure 152. Modify Task*

5. Click on **Save Task** and then Click **Save** Button
Policy Engine>Policy Designer

2. Select New to create new Policy designer as shown in Figure 153.
   Name – User Policy New
   Rule Type – AlertAccess
   Description – User Policy

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

   **Figure 153. Policy Designer**

   **Figure 154. Toolbar**

   *Stop* represents Start button
   *Stop* represents End Button
   *UserID Check* represents Decision
5. Guidelines to configure the policy

a. To place an element/node on the layout page, drag it from the toolbar and place it.

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)

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.
6. Click on Step 1 decision box and it will open popup window with some fields. See Figure 156.

7. Enter `$masterUser[UserId].size='0'` in the Condition text box and hit Enter.

8. Similarly, click on other Steps (2 to 7) and configure the data based on Table 30.

9. For decision nodes provide Condition value and for Task nodes like Create User, Terminate User, Change Handler, Error Handler provide IsTaskHandler and Task Handler fields.
### Table 30. Condition Decision Values

<table>
<thead>
<tr>
<th>Step</th>
<th>Name</th>
<th>Type</th>
<th>Condition</th>
<th>Is Task Handler</th>
<th>Task Handler</th>
<th>Update Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User ID Check</td>
<td>Decision</td>
<td>$masterUser[UserId].size='0'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Create User</td>
<td>Task Handler</td>
<td></td>
<td>Yes</td>
<td>Recon New Hire</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Terminate Check</td>
<td>Decision</td>
<td>$checkStatus[UserStatus,Active,Inactive].action='LOCK'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Terminate</td>
<td>Task Handler</td>
<td></td>
<td>Yes</td>
<td>Recon Terminate Handler</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Remove Access Check</td>
<td>Decision</td>
<td>$checkAuthFields[].status='Yes'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Error Handler</td>
<td>Task Handler</td>
<td></td>
<td>Yes</td>
<td>Recon Error Handler</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Change Handler</td>
<td>Task Handler</td>
<td></td>
<td>Yes</td>
<td>Recon Change Handler</td>
<td></td>
</tr>
</tbody>
</table>

#### Job Scheduler>Triggers Field Map

2. Click New
3. Enter Group Name – Alert DbConnector Field Mapping
4. Description – Alert DbConnector Field Mapping
5. Select Type – Reconciliation
6. After creating Field Map, select the newly created map and select Configure
7. Click New and create mapping per below, Table 31
Table 31. Guardian Job Scheduler Triggers Field Map

<table>
<thead>
<tr>
<th>AE Attribute</th>
<th>mappedKey</th>
<th>userType</th>
<th>roleType</th>
<th>userRole</th>
<th>userBadge</th>
<th>userEnrollRoleType</th>
<th>userTrainingType</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserId</td>
<td>UserId</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>FirstName</td>
<td>FirstName</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>LastName</td>
<td>LastName</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Email</td>
<td>Email</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Telephone</td>
<td>WorkPhone</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Mobile</td>
<td>HomePhone</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>EmployeeType</td>
<td>EmployeeType</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>PacsAllDoors</td>
<td>PacsAllDoor</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>PacsHomeAccess</td>
<td>PacsHomeAccess</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>PacsWorkAccess</td>
<td>PacsWorkAccess</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>BadgedId</td>
<td>CardNumber</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Format</td>
<td>FacilityCode</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>ValidFrom</td>
<td>ValidFrom</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>ValidTo</td>
<td>ValidTo</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Title</td>
<td>Title</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Status</td>
<td>UserStatus</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>PIN</td>
<td>PIN</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>AlertDepartment</td>
<td>Department</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

Job Scheduler>Triggers

1. Setup > Manual Configuration > Job Scheduler > Triggers
2. Click New and create the following Triggers in Table 32.

AlertDbConnectorTrigger

Table 32. Guardian AlertEnterprise DB Trigger

<table>
<thead>
<tr>
<th>Name</th>
<th>AlertDbConnectorTrigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>AlertDbConnectorTrigger</td>
</tr>
<tr>
<td>Type</td>
<td>Reconciliation</td>
</tr>
<tr>
<td>Batch size</td>
<td>100</td>
</tr>
<tr>
<td>Number of Attempts</td>
<td>3</td>
</tr>
<tr>
<td>Policy Designer for Users/ Roles</td>
<td>User policy New</td>
</tr>
<tr>
<td>System: Reconciliation From</td>
<td>ALERTDBCONNECTOR</td>
</tr>
<tr>
<td>Reconciliation System</td>
<td>ALERTDBCONNECTOR</td>
</tr>
<tr>
<td>Field Mapping Group</td>
<td>ALERTDBCONNECTOR Field Mapping</td>
</tr>
<tr>
<td>User Type</td>
<td>True</td>
</tr>
<tr>
<td>User Role</td>
<td>True</td>
</tr>
</tbody>
</table>

Job Scheduler>Scheduler

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

3. Click Save.

- Job Type – Reconciliation Job
- Job Name - <Job Name>
- Select Global check box
- Reconciliation for – User
- Reconciliation Type – Incremental Reconciliation
- Reconciliation Triggers – AlertDbConnectorTrigger
- Select the schedule as Immediate, Once, periodic or Advance.
- For a periodic job, specify the job start date, end date, and duration of job frequency.
1. Click Save.

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

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

10.1 **SECURITY CHARACTERISTICS**

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

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

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

- Windows Server 2012 R2
- VM with CPU Quad Core 2.199GHz
- VM with 8192MB of memory
- Virtual Hard Disk containing 240 GB of storage.

10.3 AIUNIVERSAL INSTALLATION

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

10.4 POST INSTALLATION

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

10.4.1 Connect Access It! Universal to Door Controller

1. Under the Main > Hardware tab, select Channels.
2. Create a new Channel.
3. For Channel Type select IP Server.
4. Ensure Protocol Type is SCP.
5. Select Save.

6. Create a new SCP.


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

9. TCP/IP Settings:
   - IP Address: 172.16.7.101
   - Port Number: 3001

10. Encryption Settings: None.

11. Under the Card Formats tab:
   - Format Name: 26 Bit Wiegand Facility code: 20
   - Format Name: 26 Bit Wiegand Facility code: 219

12. Save changes to SCP 000.

13. Under SIOs

14. Edit SCP 000 – SIO 00


16. Edit SCP 000 – SIO 01

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

18. Under Main > Hardware select Installed Readers

19. Create SCP 000 – SIO 00-Reader 1

20. Create SCP 000 – SIO 01-Card Reader

21. Create SCP 000 – SIO 01-MRDT Keypad


23. Create new access levels.
   - Access Level Name: All Doors.
   - Assigned Readers for All Doors: SCP 000 – SIO 01-Card Reader and SCP 000 – SIO 01-MRDT Keypad.

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

   - Assigned Reader for Work Order Access Level: SCP 000 – SIO-Card Reader
10.4.2 Enable TCP/IP to SQL 2008 R2 Server

1. Launch Microsoft SQL Server Configuration Manager.
2. Expand SQL Server Network Configuration (32-bit).
3. Select Protocols for AIUNIVERSAL.
4. Right-click on TCP/IP and then select Properties.
5. Select tab IP Addresses.
6. Under IP1 ensure IP Address is set to 0.0.0.0 and TCP Port is set to 1433.
7. Under IPALL ensure TCP Dynamic Ports is set to 52839 and TCP Port is set to 1433.
8. Restart the SQL server by selecting SQL Server Services then right click on SQL Server (AIUNIVERSAL) and select Restart.

11 Privileged User Access Control: TDi ConsoleWorks Server Installation

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

11.1 Security Characteristics

Cybersecurity Framework Categories:

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

11.2 ConsoleWorks Server Installation

ConsoleWorks was installed on the OT network to control and monitor access between OT technicians and physical devices such as the RTUs and the RADiFlow ICS firewall. ConsoleWorks uses the OT directory to authenticate users requesting access to these devices. It also establishes a permanent SSH or telnet connection to each of the RTUs and ICS firewall using pre-established usernames and passwords. As users request access and are authenticated, ConsoleWorks makes the cross-connection from the user to the specific SSH or telnet session to allow access. Once the cross-connection is established the user has access to the device to make any changes needed. When the user completes their task they log-off of the connection and ConsoleWorks removes the cross-connect between the user and the SSH or telnet session.
ConsoleWorks logs all user access requests, all of the traffic on the session, and can alert on any pre-defined aspect of the traffic. Directory based authentication is used to manage the user access in near real time.

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

11.2.1 System Environment
The system for the OT Network ConsoleWorks Server configured by the NCCoE contains the following configuration settings and environmental constraints:

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

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

11.2.3 Post-installation Configuration of ConsoleWorks on the OT Network
1. Copy TDi Technologies license key files into C:\ProgramData\ConsoleWorks\Server\LMF\TDI_Licenses
2. Go to Start > Run > services.msc.
3. Right-click on the ConsoleWorks Server Service, then select Properties.
4. Select Start to start the service. Then change the Startup Type from Manual to Automatic.

5. Select Apply to save changes. Both the ConsoleWorks Server and ConsoleWorks LMF Server services should be running.

6. Test browser connectivity by going to http://localhost:5176. The default account is CONSOLE_MANAGER. The default password is: Setup

11.2.4 Configuring External Authentication for the OT Network ConsoleWorks Server

1. From the left menu, select the SECURITY tab.
2. Select External Authentication.
3. Ensure the Enable External Authentication checkbox has been selected.
4. Select Add.
   - Parameter 1: OT-ES-IDAM-B1
   - Parameter 2: CW_
   - Required Profile: CONSOLE_WORKS
   - Template User: CONSOLE_MANAGER
   - Leave all other fields blank.
5. Then select Next.
6. Enter a Username and Password to test External Authentication settings.
7. Then select Next.
8. Then select Save.

12 ICS/SCADA Firewall: RADiFlow

A RADiFlow switch is installed on the physical network that represents the industrial control system component that can be accessed and controlled via the OT network. A RADiFlow management workstation is installed on the OT network. The RADiFlow Management Workstation is installed on a VM that is running the Windows 7 Enterprise OS.

12.1 Security Characteristics

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

NIST 800-53 rev 4 Security Controls: AC-3, CM-7
12.2 OT Network RADiFlow Management Workstation INSTALLATION

12.2.1 Installing iSIM
1. Launch the iSIM installer as an administrator
2. Set the Destination Directory to C:\Program Files (x86).
3. Leave default settings for all other options

12.2.2 iEMS
1. Launch iEMS from the Start menu.
2. From the menu items, select System > Switch Initialization > Force Switch Model > 3180.
3. In the main windows dialog box, enter the switches IP address 172.16.6.4 and then select Refresh.
4. From the menu items, select Configuration > Interfaces > Serial Ports...
5. Select the Terminal Server tab and ensure Service 1 and Service 2 dialog boxes are checked.
6. Under Service 1, enter these settings:
   - Service ID: 1
   - Local IP Address: 172.16.6.100
   - Telnet Port: 2050
   - Null CR Bit Mode: OFF
7. Under Service 2, enter these settings:
   - Service ID: 2
   - Local IP Address: 172.16.6.100
   - Telnet Port: 2051
   - Null CR Bit Mode: OFF
8. Then Select Create/Update.
9. Select the Serial Ports tab ensure Port-1 and Port-2 dialog boxes are checked.
10. Under Port 1 enter these settings:
    - Application: Terminal Server
    - Local Position: Slave
    - Service-id: 1
    - Operation Mode: Transparent
    - Buffer Mode: byte
    - Protocol: any
    - Baudrate: 9600
11. Under Port 2 enter these settings:

- Databits: 8
- Stopbits: 1
- Parity: no
- Allowed-latency: 6
- Bus-idle-time: 30
- Dtr-dsr: enable
- Rts-cts: enable
- Local-dsr-delay: 0
- Local-cts-delay: 0
- Tx-delay: 10
- Bits-for-sync1: 28
- Bits-for-sync2: 1
- Unit-id length: 2
- Iec101-link-address-len: 2

12. Then Select Create/Update.

13 **OZONE: MAG INSTALLATION**

Four Ozone components are installed on the IdAM network: Console, Authority, Server, and Envoy. These components are installed on VMs running the CentOS 7 image.
13.1 Security Characteristics

Cybersecurity Framework Categories: PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

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

13.2 Ozone Console Installation and Authority Configuration

1. Install CA Certificate into trusted root store (MAG_DEV_CA.crt).
2. Install Ozone Authority Certificate into Trusted People store (ozoneauthority.crt).
3. Install Administrator keys into Personal store (admin1.crt and admin2.crt).
4. Run Setup Ozone Console.exe
   • Run Ozone Console.
   • Go to Configuration> Ozone Authority> New... see Figure 158.
   • In the Proof Settings tab:
     o Select SHA256 for the Entity Digest Algorithm.
     o Select SHA256withRSA for the Proof Signature Algorithm.

5. In the Authority Web Service tab, Figure 159.
• Set the HTTPS Port to 443.

• Select SHA1withRSA for the Message Signature Algorithm.

Figure 159. Ozone Authority Web Service

• Click Save.

6. Select a certificate to be used to digitally sign the configuration (Admin 1).

7. Save the file as AuthorityConfiguration.xml.

8. SCP the file to Ozone Authority machine.

13.3 OZONE AUTHORITY INSTALLATION

Create keys and certificates and store in Java Keystore (JKS)

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

Install mariDB
[root@ozone ~]# yum install mariadb-server
[root@ozone ~]# reboot
[root@ozone ~]# systemctl start mariadb
[root@ozone ~]# systemctl enable mariadb

Secure the mysql installation
[root@ozone ~]# mysql_secure_installation
Create the Ozone Authority database and user
[root@ozone ~]# mysql -u root –p
MariaDB> create database ozone;
Query OK, 1 row affected (0.02 sec)
MariaDB> create user 'ozone'@'localhost' identified by 'password';
Query OK, 0 rows affected (0.00 sec)
MariaDB> grant all privileges on ozone.* to 'ozone'@'localhost';
Query OK, 0 rows affected (0.00 sec)
MariaDB> flush privileges;
Query OK, 0 rows affected (0.00 sec)

Install the Ozone Authority
[root@ozone local]# cd /usr/local/
[root@ozone local]# tar -xzf ~/Ozone\ Authority-2014.tar.gz
Copy AuthorityConfiguration.xml to conf directory
[root@ozone local]# mv ~/AuthorityConfiguration.xml authority/conf/
Copy AuthorityLicense.xml to conf directory
[root@ozone local]# mv ~/AuthorityLicense.xml authority/conf/
Copy JKS to keystores directory
[root@ozone local]# mv ~/authority.jks authority/keystores/
Copy administrator certificates to bin directory
[root@ozone local]# mv ~/admin1.cer authority/bin/
[root@ozone local]# mv ~/admin2.cer authority/bin/
Run the Ozone Authority script
[root@ozone local]# cd authority/bin/
[root@ozone bin]# ./startAuthority.sh
Configuration file not found, would you like to create a new
installation? [Y] Y
***WARNING*** This product MUST be installed by an Ozone Certified
Engineer. Pericore, Inc. cannot be held liable for damages resulting
from negligent or fraudulent actions of unauthorized or unqualified
administrators. Please review all documentation thoroughly before
continuing. Continuation of this configuration process represents an
agreement to abide by the Pericore EULA.
Do you wish to continue? [N] : y
Please select the license file for this Ozone Authority.: 
1: /usr/local/authority/conf/AuthorityLicense.xml
2: Other...
Choice [1] : 1
Please select the configuration file for this Ozone Authority:
1: /usr/local/authority/conf/AuthorityConfiguration.xml
2: Other...
Choice [1] : 1

Do you wish to set any passphrase complexity requirements? [N] : N
Note: If you require passphrase at start, you will not be able to
restart this Ozone Authority without user intervention.
Do you wish to require a passphrase to start this Ozone Authority? [N] N

Using keystore type: RSA
Do you have an existing keystore you wish to use for this Ozone Authority? [Y] :
Please select the keystore file for this Ozone Authority:
1: /usr/local/authority/keystores/authority.jks
2: Other...
Choice [1] : 1
Please enter the passphrase. : 123456
POST: [FIPS] FIPS-140 compliance self-test passed.

What type of database do you wish to use?:
1: SQLSERVER
2: ORACLE
3: MYSQL
Choice [1] : 3
Please enter the hostname or IP address of the database server: [ozone] :
localhost
Please enter the port number for the database: [3306] 3306
Please enter the username for the database: [] :
ozone
Please enter the database password: password
Using only available database: ozone

How many initial administrators would you like to create? [2] : 2

Please select the file containing the administrators certificate: [ # ] : 2

Please enter distinguished name(DN) of the starting Organizational
Unit (OU) for this proof tree: [OU=Ozone] : ou=Ozone, dc=NCCOE, dc=test
Please enter the minimum number of administrators required to approve
changes to the initial proofs: [1] : 1
Please enter a name for the initial publication schedule: [Primary Schedule]  
**Daily**

Please enter the publication interval: [12] : **12**

Please select the time unit:
1: Minute  
2: Hour  
3: Day  
Choice [1] : **2**

Please enter the validity period after publication: [12] : **12**

Please select the validity period time unit:
1: Minute  
2: Hour  
3: Day  
Choice [1] : **2**

Please enter a name for the initial distribution point for proofs. [File Distribution Point] : **LDAP Distribution Point**

Please enter the initial distribution point for proofs. This may be changed later. [file:///usr/local/authority/proofs/] : **ldap://ozoneauthority/**

Configuration File: /usr/local/authority/conf/AuthorityConfiguration.xml

May 15, 2015 1:25:16 PM  
com.pericore.util.ObjectIdentifierFactory$OIDDataLoader debug  
INFO: ObjectIdentifierFactory Read 240.165 kb in 2.511 ms; Indexed 2,415 Arcs in 51.731 ms; 2,310(1,054:5) keys => 2.003 kb  
Created proof ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in the database.  
Created proof ou=Applications, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in the database.  
Created proof ou=Groups, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in the database.  
Created proof ou=Attribute Types, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in the database.

Allowing a user certificate to be associated with a directory GUID allows for a migration path from username and password to a PKI based authentication and authorization mechanism. However, this method lowers the initial security settings by relying on a directory for the association. Please be sure you understand the risks associated with this method before allowing this mechanism to be used.

Would you like to allow users certificates to be associated with a directory GUID? [N] : **N**

Do you wish to display a logon message? [N] : **N**

Ozone Authority  
Version: 2014 - 4.0.1 (Build: 475)  
Copyright Pericore, Inc. 2014  
-----------------------------------  
Started at: May 15, 2015 1:24:13 PM EDT  
Licensed to: NCCOE  
-----------------------------------  
Built: ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in 0:00:00.304.  
Built: ou=Applications, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test in 0:00:00.243.  
Built: ou=Groups, ou=Master Authorization Group, ou=Ozone, dc=NCCOE, dc=test
Install LDAP (389) directory server

[root@ozone ~]# yum install 389-ds-base
[root@ozone ~]# vi /etc/hosts

Modify the first line of hosts file so that it is the same as below:
```
127.0.0.1 ozoneauthority.nccoe.test localhost localhost.localdomain
localhost4 localhost4.localdomain4
```

Configure the directory server

[root@ozone ~]# setup-ds.pl

Would you like to continue with set up? [yes]: yes

Your system has been scanned for potential problems, missing patches, etc. The following output is a report of the items found that need to be addressed before running this software in a production environment.


NOTICE : System is x86_64-unknown-linux3.8.13-68.2.2.el7uek.x86_64 (1 processor).

NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds (120 minutes). This may cause temporary server congestion from lost client connections.

WARNING: There are only 1024 file descriptors (soft limit) available, which limit the number of simultaneous connections.

WARNING : The warning messages above should be reviewed before proceeding.

Would you like to continue? [no]: yes
Choose a setup type:

1. Express
   Allows you to quickly set up the servers using the most
   common options and pre-defined defaults. Useful for quick
   evaluation of the products.

2. Typical
   Allows you to specify common defaults and options.

3. Custom
   Allows you to specify more advanced options. This is
   recommended for experienced server administrators only.

To accept the default shown in brackets, press the Enter key.

Choose a setup type [2]: 2

Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: eros.example.com.

To accept the default shown in brackets, press the Enter key.

Warning: This step may take a few minutes if your DNS servers
cannot be reached or if DNS is not configured correctly. If
you would rather not wait, hit Ctrl-C and run this program again
with the following command line option to specify the hostname:

General.FullMachineName=your.hostname.domain.name

Computer name [ozone.mountaireygroup.com]: ozoneauthority.nccoe.test

The server must run as a specific user in a specific group.
It is strongly recommended that this user should have no privileges
on the computer (i.e. a non-root user). The setup procedure
will give this user/group some permissions in specific paths/files
to perform server-specific operations.

If you have not yet created a user and group for the server,
create this user and group using your native operating
system utilities.

System User [nobody]: nobody
System Group [nobody]: nobody

The standard directory server network port number is 389. However, if
you are not logged as the superuser, or port 389 is in use, the
default value will be a random unused port number greater than 1024.
If you want to use port 389, make sure that you are logged in as the superuser, that port 389 is not in use.

Directory server network port [389]: 389

Each instance of a directory server requires a unique identifier. This identifier is used to name the various instance specific files and directories in the file system, as well as for other uses as a server instance identifier.

Directory server identifier [ozoneauthority]: ozoneauthority

The suffix is the root of your directory tree. The suffix must be a valid DN. It is recommended that you use the dc=domaincomponent suffix convention. For example, if your domain is example.com, you should use dc=example,dc=com for your suffix. Setup will create this initial suffix for you, but you may have more than one suffix. Use the directory server utilities to create additional suffixes.

Suffix [dc=nccoe, dc=test]: dc=nccoe, dc=test

Certain directory server operations require an administrative user. This user is referred to as the Directory Manager and typically has a bind Distinguished Name (DN) of cn=Directory Manager. You will also be prompted for the password for this user. The password must be at least 8 characters long, and contain no spaces. Press Control-B or type the word "back", then Enter to back up and start over.

Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
Password: password
Password (confirm): password

Your new DS instance 'ozoneauthority' was successfully created.

Exiting . . .
Log file is '/tmp/setup_C4mdK.log'

Setup the directory structure
Modify the file /usr/local/authority/bin/389SetupDirectory.ldif

Set the correct DN structure and passwords for the ozone authority user and tree

#Create the User for Ozone Authority
dn: uid=ozone, ou=Special Users, dc=nccoe, dc=test

changeType: add
objectClass: inetorgperson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Ozone Authority
sn: Authority
givenName: Ozone
uid: ozone
userPassword: P@$$word

#make the people writable by ozone
dn: ou=People, dc=nccoe, dc=test
changeType: modify
add: aci
aci: (targetAttr="*")(version 3.0; acl "ozone authority"; allow (all)(userdn = "ldap:///uid=ozone, ou=Special Users, dc=nccoe, dc=test");)

#Create the Ozone OU
dn: ou=Ozone, dc=nccoe, dc=test
changeType: add
objectClass: organizationalUnit
objectClass: top
ou: Ozone
aci: (targetAttr="*")(version 3.0; acl "ozone authority"; allow (all)(userdn = "ldap:///uid=ozone, ou=Special Users, dc=nccoe, dc=test");)

#Create required Attributes and Object Classes
dn: cn=schema
changeType: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.26135.1.1.1.2 NAME 'authorizationProof' DESC 'Ozone Authorization Proof' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 SINGLE-VALUE X-ORIGIN 'user defined'
attributetypes: ( 2.23.136.1.1.2 NAME 'cscaMasterList' DESC 'CSCA Master List' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 SINGLE-VALUE X-ORIGIN 'user defined'

Modify the directory using the LDIF
[root@ozone bin]# ldapmodify -x -D "cn=Directory Manager" -W -f /usr/local/authority/bin/389SetupDirectory.ldif
Enter LDAP Password:
adding new entry "uid=ozone, ou=Special Users, dc=nccoe, dc=test"
modifying entry "ou=People, dc=nccoe, dc=test"
adding new entry "ou=Ozone, dc=nccoe, dc=test"
modifying entry "cn=schema"
modifying entry "cn=schema"
13.4 **OZONE CONSOLE SERVER CONFIGURATION**

Before proceeding ensure that OzoneAuthority has been started by running startauthority.sh on the OzoneAuthority machine.

1. Open Ozone Console.
2. Go to File > Properties, Figure 160, below.
3. Enter the Ozone Authority URL.
4. Click Select Certificate and select the Ozone Authority Certificate.
5. Select SHA1withRSA as the Message Signature Algorithm.
6. Click Save to the connection information.

![Figure 160. Ozone Authority Connection Information](image)

**Create the publication point for the proofs**

1. Select Publication > Add Publication Point > Add LDAP Publication Point, Figure 161
2. Enter a name for the publication point.
3. Enter the hostname or IP address of the directory server.
4. Enter a base context, if any.
5. Select the port.
6. Enter the name of the user who has permissions to write to the directory.
7. Enter the password for the user.
8. Confirm the password.
Import the desired groups from the RSA Adaptive directory

1. Right-click on the Groups proof.
2. Select Import Group from Active Directory, Figure 162.
3. Enter the directory connection information.
4. Select a group to import, see Figure 163.
5. Check the box to Import New Entities.
6. Check the box to Import Associated Groups.

7. Then select Import

![Image of Import Group from Directory](image)

*Figure 163. Ozone Import Group from Directory*

8. Select the publication schedule as shown in Figure 164.

9. Select the publication point as shown in Figure 164.

10. Select the distribution point as shown in Figure 164.
11. Click the Administrators tab as shown in Figure 165
12. Click the Add Administrators button.
13. Select the users who will administer the proof.
14. Then select Add Entities
15. Click the Save button.

**Create the Ozone Server Configuration**

1. Select Configuration > Ozone Server > New...
2. Click the Add proof from tree... button.
3. Select a proof Ozone Server should use for authorizations as shown in Figure 166.
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.
6. Click the Save button.

7. Repeat Steps 2–6 until you have selected all of the proofs Ozone Server should initially retrieve for Authorizations.
8. Click the Save configuration button as shown in Figure 168.
9. Select a certificate to be used to digitally sign the configuration.
10. Save the file as ServerConfiguration.xml.
11. SCP the file to the Ozone Server machine.

13.5 OZONE SERVER INSTALLATION

Create keys and certificates and store in Java Keystore (JKS)

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

Install Ozone Server
[root@ozone ~]# cd /usr/local/
[root@ozoneserver local]# tar -xzf ~/Ozone\ Server-2014.tar.gz

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/

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/
Run the Ozone Server

[root@ozoneserver bin]# ./startServer.sh

POST [MAIN] v2.1.301

```
_______ __________ _______ __ _ ________
[___/___]_____ // ___ \\ | \\ | | ______| (R)
[___/___]_____ // ___ \\ | \\ | | |
[___/___]_____ // ___ \\ | \\ | | |
[___/___]_____ // ___ \\ | \\ | | |
[___/___]_____ // ___ \\ | \\ | | |
[___/___]_____ // ___ \\ | \\ | | |
```

Ozone(R) Server copyright (c) Pericore, Inc. 2007-2011

---

Fri May 15 14:31:33 EDT 2015


POST: [FIPS] FIPS-140 compliance self-test passed.

Found Java version: 1.8.0_31

Working in: /usr/local/server/bin

/env/work/usr/local/server/bin/conf/server.cfg not found. Run setup [Y] : y

Found Java Version: 1.8.0_31

Ozone Server Setup Utility

***WARNING***

This product MUST be installed by a Pericore Certified Engineer. Pericore, Inc. cannot be held liable for damages resulting from negligent or fraudulent actions of unauthorized or unqualified administrators. Please review all documentation thoroughly before concluding. Continuation of this configuration process represents an agreement to abide by the Pericore EULA.

I agree to all terms and conditions set forth by Pericore, Inc. [N] : n

Enable Startup Password? [N] : n

Server Configuration Directory:

1: /usr/local/server/bin/conf

Select the XML License File:

1: /usr/local/server/bin/conf/ServerLicense.xml

Server Configuration Directory:

1: /usr/local/server/bin/conf

Choice [1] : 1

Select the XML License File:

1: /usr/local/server/bin/conf/ServerLicense.xml

Choice [1] : 1
Select the XML Configuration File:
1: /usr/local/server/bin/conf/ServerConfiguration.xml
2: Other...
Choice [1] : 1

Page 1 | Current Directory: /usr/local/server/bin
[00] ..
[01] lib/
[02] conf/
Select Server Identity Keystore [ # ] : 2
Page 1 | Current Directory: /usr/local/server/bin/conf
[00] ..
[01] server.jks
Select Server Identity Keystore [ # ] : 1
Enter password for server.jks : 123456
Is the Private Key Alias 'server' correct? [Y] : Y
Enable logging? [Y] : Y
Log File Roll Size (Kb) [512] : 512
Configured Client Services: 0
Choose an option:
1: Configure Authorization Service
2: Configure a Proof Proxy
3: Configure an Info Page
4: Configure a Push Service
5: Done Configuring Web Services
Choice [1] : 1
Configuring XACML Authorization Service
Service Port [8080] : 443
SOAP Signature Method:
1: RSA_SHA1
2: RSA_SHA256
3: RSA_SHA384
4: RSA_SHA512
Choice [1] : 2
Enable WS-Security Client Authentication? [N] : N
Configured Client Services: 1
Choose an option:
1: Configure Authorization Service
2: Configure a Proof Proxy
3: Configure an Info Page
4: Configure a Push Service
5: Done Configuring Web Services
Choice [1] : 5
Enable SSL? [N] : Y
Service Port [8080] : 443
Enable SSL Client Authentication? [N] : N
Enable SSL? [N] : N
Modify Advanced Performance Options? [N] : N

Writing server configuration...
Thank you for choosing Ozone Server
Goodbye.

[root@ozoneserver local]# /usr/local/server/bin/startServer.sh

13.6 OZONE ENVOY INSTALLATION

Ozone Envoy was installed and not utilized in the builds. The functions it provides, automated CRLs and certificate collection, were not required in the solution.

Create keys and certificates and store in Java Keystore (JKS)

Install java
[root@ozoneenvoy ~]# yum install java

Install Ozone Envoy
[root@ozoneenvoy ~]# cd /usr/local/
[root@ozoneenvoy local]# tar -xzf ~/Ozone Envoy-2014.tar.gz

Copy the keystore to the bin directory
[root@ozoneenvoy local]# cp ~/envoy.jks envoy/bin/

Edit the envoy.txt file to set configuration options
### Ozone Suite (c) Pericore, Inc. 2007-2014.
### All rights reserved.

#############################################################################
### envoy.txt - Ozone Envoy 2014 Configuration File ###
### Author: Jacob Dilles <jdilles@mountaireygroup.com> ###
### Date: 1 Jan 2014   ###
### Notes: This is a sample Ozone Envoy 4.1.0 Setup Configuration File ###
### demonstrating configuration options for Mobile Enrollment. ###
### After installation is complete, this file should be deleted ###
### or 'chown root; chgrp 0; chmod 000' to secure it. ###
#############################################################################
### General Envoy Configuration

### Identity Keystore Configuration

### This keystore is used for:
### Authenticating with Ozone Authority

### Secure log signing

system/identity/store=envoy.jks

#### Authority Listener Configuration

This web service endpoint listens for push configuration and fetch requests from Ozone Authority. It should match what you entered in Ozone Console.

```
#authority/host.name=
authority/port=4242
authority/path=/
authority/mode=ANY
```

#### Authority Web Service Endpoint Logging

```
authority/log/enable=true
authority/log/path=var/log
authority/log/rollsize=10485760
authority/log/format=CLF
```

### Enrollment Configuration

```
### Enable enrollment
enroll/enable=false
```

Run Ozone Envoy to complete the setup

```
[root@ozoneenvoy bin]# ./startEnvoy.sh
```

```
INFO: ObjectIdentifierFactory Read 240.165 kb in 14.366 ms; Indexed 2,415 Arcs in 63.198 ms; 2,310 (1,054:5) keys => 2.003 kb
```
***WARNING***
This product MUST be installed by a Pericore Certified Engineer.
Improper configuration of Ozone Envoy Tool may cause security vulnerabilities.

I agree to all terms and conditions set forth by Pericore, Inc. [N] : y

envoy.jks

system/identity/store [/usr/local/envoy/bin/envoy.jks] :
Enter password for envoy.jks :
Is the Private Key Alias 'envoy' correct? [Y] : Y


Return to Ozone Console to complete Ozone Envoy Configuration

13.7 OZONE CONSOLE ENVOY CONFIGURATION

Create a proof to store the certificates retrieved by Ozone Envoy

1. Open Ozone Console.
2. Select an administrator certificate to log in as shown in Figure 169.
3. Select Proof>New Proof..
4. Enter a name for the proof.
5. Select the publication schedule.
6. Select the publication point(s).
7. Select the distribution point(s).
8. Click the Administrators tab.

9. Select the administrators to manage the proof.

10. Click the Authentication tab.

11. Click the Add from file… button.

12. Select the CA and intermediate CA certificates to be used to authenticate certificates retrieved.

13. Select the Certificate Revocation Lists tab as shown in Figure 170.

14. Enter a CRL grace period, the number of hours a CRL can be considered valid after its next update time.

15. Click the Add... button to add a CRL.
16. Select the Source Configuration tab as shown in Figure 171.

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

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

19. Check the box for LDAPS.

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

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

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

23. Enter the attributeName for the CRLs, typically certificateRevocationList shown in Figure 156.

24. Enter the connection information:
   - If connecting anonymously, check the box for anonymous connections.
   - If a username/password is required for the connection, enter them.

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

Configure Ozone Authority to connect to Ozone Envoy

1. Select Enrollment>Envoy Configuration.
2. Enter the hostname or IP address of the Ozone Envoy. See Figure 172.
3. Enter the port number Ozone Envoy is listening on.
4. Enter the number of hours that should elapse between connections to Ozone Envoy to check for new information.
5. Enter the number of minutes to before attempting to reconnect to Ozone Envoy if the connection fails.
6. Click Save.
PHYSICAL ACCESS CONTROL: XTEC XNODE

The XNode was installed in the DMZ network. The Xnode is a standalone IdAM demonstration capability including a personal identification verification (PIV) card reader, PIV Interoperability (PIV-I) cards, keypad and electric door strike. The XNode was preconfigured to poll the IP address of the cloud based IdAM system at the Xtec control center. No additional configuration information is required. The identities on the PIV cards included access allowed and access denied status for demonstration purposes.

14.1 SECURITY CHARACTERISTICS

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

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

ENTERPRISE PKI PLATFORM: GLOBALSIGN

15.1 OVERVIEW

The NCCoE used the GlobalSign Enterprise PKI platform to issue and manage North American Energy Standards Board (NAESB) WEQ-12 digital certificates used for secure network access of for both internal and external users, see Figure 173. The certificates were used in conjunction with the MAG Ozone product to provide high assurance attributes for the Personal Profile Application (PPA). The application has three main information groups for which actions can be authorized: Personal Information, Credit Reports, and Criminal History. Based on the authorizations associated with a credential, results pages are dynamically populated.
The North American Energy Standards Board (NAESB) serves as an industry forum for the development and promotion of business process standards which can lead to a seamless marketplace for wholesale and retail natural gas and electricity, as recognized by its customers, business community, participants, and regulatory entities. GlobalSign is an active participant of the NAESB Cyber-Security standards committee and is a NAESB-authorized Certificate Authority (CA). For more information about NAESB, go to https://www.naesb.org/.

GlobalSign’s NAESB-compliant certificate-based authentication solution is managed through a SaaS service accessed through a web-based portal. The web portal gives organizations control of Digital IDs issued to individuals using one of four NIST defined assurance levels. Set-up usually takes less than three days. Another advantage of the web-portal is that all of the lifecycle functions including issuance, re-issuance, renewal, and revocation are available to the administrator.
15.1.1 Managing the Account
Managing the account is accomplished using the GlobalSign Certificate Management Center (GCC). GCC is a web-based interface allowing you to access your certificates anywhere with an Internet connection. Within the platform, administrators may add additional users and delegate some or all certificate management functions.

15.1.2 What Is a Profile? / Profile Management
A profile, or certificate profile, contains the organization’s identity information that will be used for all NAESB WEQ-12 digital certificates issued from the account. Organization identity information includes the organization legal name, country code, and optionally locality, state, and up to three fixed organization units as well as assurance level.

15.1.3 What Is a License?
GlobalSign NAESB digital certificates are valid for either (1) or (2) years and must be issued within (12) months of license ordering.

GlobalSign NAESB digital certificates are sold in “license packs” (i.e., in quantities of 5, 10, 25, 50, etc.) Certificates are issued with either (1) or (2) year validities and must be issued within (12) months of license ordering.

15.2 Security Characteristics
Cybersecurity Framework Categories: PR.AC-1: Identities and credentials are managed for authorized devices and users
NIST 800-53 rev 4 Security Controls: AC-2, IA Family

15.3 How To Order Certificates

15.3.1 Step 1: Get a GlobalSign Gcc Account

15.3.2 Step 2: Order Certificate License Pack
Once you have your GCC account credentials, use the following link to login – www.globalsign.com/en/login/. See Figure 174.
Click on the “Enterprise PKI” tab as shown in Figure 175.

Choose the “Enterprise PKI Pro For Personal Digital ID” license pack you intend to purchase and click next as shown in Figure 177.
Choose your validity period (1 or 2 year certificate), see Figure 178.

Provide payment details as shown in Figure 179.
Confirm your order details and check the box confirming you understand that the license pack will expire 12 months from the order date, Figure 180.

Step 3: Set Up Organization Profile

Click “Order Additional Profiles” from the left navigation menu as shown in Figure 181.

Enter your Organization Profile details. Please note the details you enter will be vetted and included as the certificate identity within your issued certificate, see Figure 182.
Additionally select the Assurance level appropriate for the risk associated with the transaction.
Contact GlobalSign NAESB experts for additional guidance on this topic.

Confirm your profile details (Figure 183) and then review and accept the EPKI Service Agreement that includes important NAESB WEQ-012 obligations. Note the EPKI Service Agreement binds you to obligations as outlined in the GlobalSign Certificate Policy and Certificate Practice Statements, including Local Registration Authority, end user, and relying party, as defined in the NAESB Public Key Infrastructure (PKI) Standards – WEQ-012.

Certificate Practice Statements can be found at [http://www.globalsign.com/repository/](http://www.globalsign.com/repository/)
15.3.4 **Step 4: Vetting**

Once you have placed your order, all of your information will be sent to GlobalSign’s vetting department. The organization details you provided for your profile will be vetted by GlobalSign using third party checks.

15.3.5 **Step 5: Register for Your EPKI Administrator Certificate**

Once your company profile has been approved, you will need to register for what is known as an “EPKI Administrator Certificate.” An EPKI Administrator Certificate is required to authenticate to secure areas of the EPKI service to register and manage end user certificates.

1. Login into GCC
2. Select “View Admin Menu Options” in the left hand menu to start the enrollment process, see Figure 184.

3. Choose a certificate password. It is very important to remember this password.
4. Download your administrator certificate and follow the on screen prompts to install your certificate.

CAUTION: If you need to access the EPKI administrator menu options from multiple machines, you can copy your .pfx file to other computers and repeat the import process. Instructions for importing your certificate can be found here - https://support.globalsign.com/customer/portal/articles/1211387.

15.3.6 Step 6: Register and Issue Certificates to Individual Users

Click “Order Certificates” in the left navigation menu as shown in Figure 185.

NOTE: If you haven’t already authenticated to the secure section of the portal with your Administrator Certificate, you may see “View Admin Menu Options” instead of the menu options included in the image below. Simply click the “View Admin Menu Options” link and select the appropriate certificate to gain access to this section of the portal.

Select the profile and license you want to use and click Next, see Figure 186.

Complete the certificate identity details (Figure 187) for the end user of the certificate, including the common name (i.e., the individual’s first and last name) and the email addresses. Organization name, and other fields will be pre-populated from the profile you selected.
You will also need to choose a “pick up password”. The pick up password is a unique password that you will give to the end user of the certificate. After you have completed the registration process, the end user will receive an email invitation to pick up their certificate and at that time they will be prompted for the pick up password (you gave them in an out-of-band method) along with details of how to install their new certificate.

Finally, confirm the details of your certificate request as shown in Figure 188.
Repeat this process until you have requested certificates for all of your end users.

For further information on the features available in your GlobalSign Certificate Center please visit: http://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf

15.4 GLOBALSIGN’S IDENTITY AND ACCESS MANAGEMENT SOLUTION FOR MANAGING EXTERNAL USERS

For use cases involving external users (e.g. Independent System Operators (ISOs) operating wholesale electric marketplaces), GlobalSign PKI can provide an identity and access management (IAM) solution that enables management of external user (customer and partner) identities and the online services and applications they can access.

15.5 GETTING HELP

GlobalSign provides technical support through our Client Service departments around the world. Visit https://www.support.globalsign.com for detailed instructions on installing and managing certificates, or contact support@globalsign.com or 1-877-467-7543 with specific questions.

16 INDUSTRIAL FIREWALL: SCHNEIDER ELECTRIC

A Schneider Electric (SE) industrial firewall is installed on the physical network that contains the industrial control system/SCADA components that can be accessed and controlled via the OT network. The firewall is configured to monitor the data passing between the RADiFlow SCADA...
The SE industrial firewall will alert if out-of-policy traffic is detected on the network segment connecting the OT network and the SCADA network of devices.

Install and Configure Schneider Tofino Firewall

1. Download the ConneXium software from the Schneider site as stated in the instructions accompanying the firewall, start the ConneXium Tofino Configurator.

2. At the startup screen, click ‘Create New Project…’, Figure 189.

3. In Project name, enter the name you would like to use for the project, as shown in Figure 190. Also fill in the Company field. When finished, click Next.
4. In the Project Protection screen, Figure 191, choose a password to protect the project. Then click Next.
In the Administrator Password screen,

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

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.
8. Right click on the ‘Assets’ icon in the Project Explorer frame, Figure 195, and click ‘New Asset.’
9. In the New Asset window, Figure 196, set the name of the device, as well as the type and all other fields as necessary. Then click Next.

*Figure 196. New Asset*
10. Fill in the IP address and/or the MAC address fields, Figure 197, then click Finish.

11. Repeat steps 8-10 for all devices on the network. When they are configured, click on the ‘Assets’ icon, Figure 197, in the Project Explorer frame (if it isn’t already selected) and there should be a list of all the configured Assets.

12. Under the Project Explorer frame, click the dropdown arrow next to ‘Tofino SAs’, then choose the SA created earlier, Figure 198. From there, click on ‘Firewall’ in the Project Explorer frame to display current firewall rules. This should be empty currently.
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.
14. On the next screen, Figure 200, there are 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. In the Lab Build, Asset 1 is the OT Workstation, which is connected to a network that is connect to the External interface on the firewall. Select the ‘Select an asset from the list below’ radio button for both Asset 1 and Asset 2, and select the systems to create a rule between. Also, select the direction of the traffic using the arrow buttons in the middle. When finished, select Next.

![New Firewall Rule Wizard](image)

Figure 200. Firewall Rule Wizard
15. On the Asset Rule Profiles, Figure 201, select the ‘Manually create the firewall rules for the selected assets’ radio button. Click Next.

Figure 201. Asset Rule Profiles

16. On the Protocol screen, Figure 202, choose the protocol to be checked against. There are drop down menus for ‘Common Industrial’, ‘Common IT’, and ‘Vendor Specific.’ For this example, we are choosing SSH and Telnet (by holding the CTRL key, you can select multiple protocols). Then choose the Permission on the right side of the screen, as well as whether to log or not. Then click Finish.
Note: By default, any traffic that does not match the rules in the firewall will automatically be denied.

17. After that is completed, the firewall rule should be listed in the Rule Table, Figure 203.
18. Repeat steps 13 through 17 for the remainder of the rules needed.

19. Finally, press the save button on the menu bar. Circled in red below in Figure 204.

20. Place a FAT/FAT32 formatted USB device into the computer running the ConneXium Tofino Configurator, then right click ‘Tofino SAs’ in the Project Explorer pane and select ‘Apply.’ If the project asks you to save, press ‘OK’.
21. In the Apply Configuration pane, Figure 205, ensure that your SA is selected in the table at the top, and the ‘USB Drive’ radio button is selected. Then browse to the top-level directory of your USB drive. Then click Finish.

Figure 205. Apply Configuration Pane

22. A popup, Figure 206, will notify you of successful completion.
23. Ensure the firewall has been powered on and has been running for at least one minute, then plug the USB device used to copy the Tofino configuration to into the USB port on the back of the firewall.

24. Press the Save/Load/Reset button twice, setting it to the Load setting (Pressing once should turn the indicator light to green, pressing it again will change it from green to amber). After a few seconds, the device will begin displaying lights that move from right to left across the LEDs on the back, indicating the configuration is being loaded.

25. Once the lights stop moving right to left, wait a few seconds, and ensure the Fault LED does not light up. Then remove the USB drive and place it back into the computer running the ConneXium Tofino Configurator software.

26. Right click ‘Tofino SAs’ in the Project Explorer pane and select ‘Verify’.

27. At the Verify Loaded Configuration window, select the Tofino SA in the table, and select the ‘USB Drive’ radio button. Then select the USB drive using the Browse button. Finally, press Finish.

28. A popup will notify you of successful verification, and configuration is complete.

17 Operating System STIG Compliance Reports

STIG compliance reports were generated for the STIG-compliant OS installations that were used in the build. The reports for each installation are provided in the following subsections. Neither the Windows 7 Console on the IT network nor the OT Management Windows 7 Workstation on the OT network were STIG-compliant installations, so compliance reports for those OSs are not provided.

The Linux implementations (except SUSE Linux) were configured to meet the DoD CentOS 6 STIG, because no CentOS 7 STIG was available at the time the build was implemented. The STIG guidelines are available on-line at http://iase.disa.mil/stigs/os/Pages/index.aspx. The OS configurations for each Linux implementation are listed below. The compliance results reports identify the configuration items that do not conform to the STIG configuration guide.

Compliance reports are provided for the following OSs:

- SQL Server on IdAM Network STIG Compliance Report
- RSA IMG SUSE Linux Server STIG Compliance Report
- RSA Adaptive Directory Centos 7 Server STIG Compliance Report
- AlertEnterprise Microsoft Server STIG Compliance Report
- IT Domain Controller STIG Compliance Report
### 17.1 SQL Server on IDAM Network STIG Compliance Report

<table>
<thead>
<tr>
<th>Status</th>
<th>STIG ID</th>
<th>Rule ID</th>
<th>Vuln ID</th>
<th>Severity</th>
<th>Rule Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>SQL2-00-000300</td>
<td>SV-53912r1_rule</td>
<td>V-41389</td>
<td>CAT II</td>
<td>SQL Server must maintain and support organization-defined security labels on stored information.</td>
</tr>
<tr>
<td>N/A</td>
<td>SQL2-00-000400</td>
<td>SV-53914r1_rule</td>
<td>V-41391</td>
<td>CAT II</td>
<td>SQL Server must maintain and support organization-defined security labels on information in process.</td>
</tr>
<tr>
<td>N/A</td>
<td>SQL2-00-000500</td>
<td>SV-53916r1_rule</td>
<td>V-41392</td>
<td>CAT II</td>
<td>SQL Server must maintain and support organization-defined security labels on data in transmission.</td>
</tr>
<tr>
<td>N/A</td>
<td>SQL2-00-000900</td>
<td>SV-53917r1_rule</td>
<td>V-41393</td>
<td>CAT II</td>
<td>SQL Server must allow authorized users to associate security labels to information in the database.</td>
</tr>
<tr>
<td>N/A</td>
<td>SQL2-00-00920</td>
<td>SV-53920r1_rule</td>
<td>V-41395</td>
<td>CAT II</td>
<td>SQL Server must be protected from unauthorized access by developers.</td>
</tr>
<tr>
<td>N/A</td>
<td>SQL2-00-009300</td>
<td>SV-53921r1_rule</td>
<td>V-41396</td>
<td>CAT II</td>
<td>SQL Server must be protected from unauthorized access by developers on shared production/development host systems.</td>
</tr>
<tr>
<td>PASS</td>
<td>SQL2-00-00950</td>
<td>SV-53922r2_rule</td>
<td>V-41397</td>
<td>CAT II</td>
<td>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.</td>
</tr>
<tr>
<td>PASS</td>
<td>SQL2-00-011050</td>
<td>SV-53918r2_rule</td>
<td>V-41394</td>
<td>CAT II</td>
<td>SQL Server utilizing Discretionary Access Control (DAC) must enforce a policy that limits propagation of access rights.</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>SQL2-00-011200</td>
<td>SV-53928r2_rule</td>
<td>V-41402</td>
<td>CAT II</td>
<td>SQL Server must provide audit record generation capability for organization-defined auditable events within the database.</td>
</tr>
</tbody>
</table>

What is considered auditable?

### 17.2 RSA IMG SUSE Linux Server STIG Compliance Report

OpenSCAP Evaluation Report

#### 17.2.1 Evaluation Characteristics

- **Target machine:** dvd-acm
- **Benchmark URL:** U_RedHat_6_V1R6_STIG_SCAP_1-1_Benchmark-xccdf.xml
17.2.2 Compliance and Scoring

The target system did not satisfy the conditions of 107 rules! Furthermore, the results of 12 rules were inconclusive. Please review rule results and consider applying remediation.

17.2.3 Rule Results

<table>
<thead>
<tr>
<th>Rule</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>passed</td>
</tr>
<tr>
<td>107</td>
<td>failed</td>
</tr>
<tr>
<td>12</td>
<td>other</td>
</tr>
</tbody>
</table>

17.2.4 Severity of Failed Rules

<table>
<thead>
<tr>
<th>Severity</th>
<th>Failed Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 other</td>
<td></td>
</tr>
<tr>
<td>53 low</td>
<td></td>
</tr>
<tr>
<td>53 medium</td>
<td></td>
</tr>
<tr>
<td>1 high</td>
<td></td>
</tr>
</tbody>
</table>

17.2.5 Score

<table>
<thead>
<tr>
<th>Scoring system</th>
<th>Score</th>
<th>Maximum</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>33.519554</td>
<td>100.000000</td>
<td>33.52%</td>
</tr>
</tbody>
</table>

Search Title Severity Result

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated file system mounting tools must not be enabled unless needed.</td>
<td>low</td>
<td>error</td>
</tr>
<tr>
<td>Auditing must be enabled at boot by setting a kernel parameter.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The /etc/gshadow file must be owned by root.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The /etc/gshadow file must be group-owned by root.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The /etc/gshadow file must have mode 0000.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The system must use a separate file system for /tmp.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must use a separate file system for /var.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must use a separate file system for /var/log.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Library files must be owned by root.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The system must use a separate file system for the system audit data path.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The audit system must alert designated staff members when the audit storage volume approaches capacity.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>All system command files must be owned by root.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The system must use a separate file system for user</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Title</td>
<td>Severity</td>
<td>Result</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>home directories.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000078 1x fail</td>
<td>The system must require passwords to contain a minimum of 14 characters.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000075 1x fail</td>
<td>Users must not be able to change passwords more than once every 24 hours.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000076 1x fail</td>
<td>User passwords must be changed at least every 60 days.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000071 1x fail</td>
<td>The system must require passwords to contain at least one numeric character.</td>
<td>low</td>
</tr>
<tr>
<td>SRG-OS-000103 1x fail</td>
<td>The system package management tool must cryptographically verify the authenticity of system software packages during installation.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000232 1x fail</td>
<td>A file integrity tool must be installed.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000273 1x fail</td>
<td>The operating system must enforce requirements for the connection of mobile devices to operating systems.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000248 1x fail</td>
<td>There must be no .rhosts or hosts.equiv files on the system.</td>
<td>high</td>
</tr>
<tr>
<td>SRG-OS-000249 1x fail</td>
<td>The system must disable accounts after excessive login failures within a 15-minute interval.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td>The /etc/shadow file must be group-owned by root.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td>The /etc/shadow file must have mode 0000.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td>IP forwarding for IPv4 must not be enabled, unless the system is a router.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000146 1x error</td>
<td>The operating system must prevent public IPv4 access into an organizations internal networks, except as appropriately mediated by managed interfaces employing boundary protection devices.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000231 1x fail</td>
<td>The systems local IPv4 firewall must implement a deny-all, allow-by-exception policy for inbound packets.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000096 1x fail</td>
<td>The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000096 1x fail</td>
<td>The Stream Control Transmission Protocol (SCTP) must be disabled unless required.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000096 1x fail</td>
<td>The Reliable Datagram Sockets (RDS) protocol must be disabled unless required.</td>
<td>low</td>
</tr>
<tr>
<td>SRG-OS-000096 1x fail</td>
<td>The Transparent Inter-Process Communication (TIPC) protocol must be disabled unless required.</td>
<td>medium</td>
</tr>
<tr>
<td>SRG-OS-000215 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Severity</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>The operating system must back up audit records on an organization defined frequency onto a different system or media than the system being audited.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The operating system must support the requirement to centrally manage the content of audit records generated by organization defined information system components.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The audit system must be configured to audit all attempts to alter system time through settimeofday.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must not accept IPv4 source-routed packets on any interface.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The system must not accept ICMPv4 redirect packets on any interface.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The system must not accept ICMPv4 secure redirect packets on any interface.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The audit system must be configured to audit all attempts to alter system time through clock_settime.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must log Martian packets.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must not accept IPv4 source-routed packets by default.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The audit system must be configured to audit all attempts to alter system time through /etc/localtime.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The operating system must automatically audit account creation.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must not accept ICMPv4 secure redirect packets by default.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>The system must ignore ICMPv4 redirect messages by default.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The operating system must automatically audit account modification.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must not respond to ICMPv4 sent to a broadcast address.</td>
<td>low</td>
<td>pass</td>
</tr>
<tr>
<td>The operating system must automatically audit account disabling actions.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must ignore ICMPv4 bogus error responses.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The operating system must automatically audit account termination.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>The system must be configured to use TCP syncookies.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>Title</td>
<td>Severity</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>SRG-OS-999999 [1x fail] The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using chmod.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 [1x fail] The system must use a reverse-path filter for IPv4 network traffic when possible by default.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using chown.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 [1x fail] The IPv6 protocol handler must not be bound to the network stack unless needed.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using chmodat.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The system must ignore ICMPv6 redirects by default.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using fchown.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using fchownat.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The system must employ a local IPv4 firewall.</td>
<td>medium</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using fremovexattr.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using fsetxattr.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using lchown.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using lremovexattr.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using fremovexattr.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 [1x fail] The audit system must be configured to audit all discretionary access control permission modifications using fsetxattr.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>Title</td>
<td>Severity</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>The audit system must be configured to audit all discretionary access control permission modifications using <code>setxattr</code>.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must be configured to audit all discretionary access control permission modifications using <code>removexattr</code>.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must be configured to audit successful file system mounts.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000069 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must require passwords to contain at least one uppercase alphabetic character.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000266 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must require passwords to contain at least one special character.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000070 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must require passwords to contain at least one lowercase alphabetic character.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000072 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must require at least four characters be changed between the old and new passwords during a password change.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000021 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must disable accounts after three consecutive unsuccessful logon attempts.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000120 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (system-auth).</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must be configured to audit user deletions of files and programs.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000120 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (login.defs).</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000120 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes (libuser.conf).</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must be configured to audit changes to the <code>/etc/sudoers</code> file.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be owned by root.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000064 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must be configured to audit the loading and unloading of dynamic kernel modules.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Severity</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>The system boot loader configuration file(s) must be group-owned by root.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000096 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The xinetd service must be disabled if no network services utilizing it are enabled.</strong></td>
<td>medium</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system boot loader configuration file(s) must have mode 0600 or less permissive.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000096 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The xinetd service must be uninstalled if no network services utilizing it are enabled.</strong></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000080 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system boot loader must require authentication.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000080 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must require authentication upon booting into single-user and maintenance modes.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000080 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must not permit interactive boot.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000022 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must require administrator action to unlock an account locked by excessive failed login attempts.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must not send ICMPv4 redirects by default.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must not send ICMPv4 redirects from any interface.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000096 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The ypbind service must not be running.</strong></td>
<td>medium</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-999999 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The cron service must be running.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The avahi service must be disabled.</strong></td>
<td>low</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-000056 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system clock must be synchronized continuously, or at least daily.</strong></td>
<td>medium</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must set a maximum audit log file size.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000062 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The audit system must be configured to audit all attempts to alter system time through adjtimex.</strong></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system must retain enough rotated audit logs to cover the required log retention period.</strong></td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000096 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The atd service must be disabled.</strong></td>
<td>low</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system default umask for daemons must be 027 or 022.</strong></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system default umask in /etc/login.defs must be 077.</strong></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system default umask in /etc/profile must be 077.</strong></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The system default umask for the csh shell must be 077.</strong></td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000096 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Severity</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>The rdisc service must not be running.</td>
<td>low</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system default umask for the bash shell must be 077.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The postfix service must be enabled for mail delivery.</td>
<td>low</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-000096 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The netconsole service must be disabled unless required.</td>
<td>low</td>
<td>error</td>
</tr>
<tr>
<td>SRG-OS-000248 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X Windows must not be enabled unless required.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process core dumps must be disabled unless needed.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000027 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must limit users to 10 simultaneous system logins, or a site-defined number, in accordance with operational requirements.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000160 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must provide VPN connectivity for communications over untrusted networks.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000024 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000034 1x error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Bluetooth service must be disabled.</td>
<td>medium</td>
<td>error</td>
</tr>
<tr>
<td>GEN006660 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts must be locked upon 35 days of inactivity.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-000118 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All public directories must be owned by a system account.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must use a Linux Security Module configured to enforce limits on system services.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must use a Linux Security Module configured to limit the privileges of system services.</td>
<td>low</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>medium</td>
<td>fail</td>
</tr>
<tr>
<td>SRG-OS-999999 1x fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must switch the system to single-user mode when available audit storage volume becomes dangerously low.</td>
<td>medium</td>
<td>fail</td>
</tr>
</tbody>
</table>
Test Result

<table>
<thead>
<tr>
<th>Result ID</th>
<th>Profile</th>
<th>Start time</th>
<th>End time</th>
<th>Benchmark</th>
<th>Benchmark version</th>
</tr>
</thead>
<tbody>
<tr>
<td>xccdf_org.open-scap_testresult_default-profile</td>
<td>(Default profile)</td>
<td>2015-04-08 08:16</td>
<td>2015-04-08 08:17</td>
<td>embedded</td>
<td>1</td>
</tr>
</tbody>
</table>

Target info

Targets
- adaptivedir

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

Platforms
- cpe:/o:redhat:enterprise_linux:6

Score

<table>
<thead>
<tr>
<th>system</th>
<th>score</th>
<th>max</th>
<th>%</th>
<th>bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>96.65</td>
<td>100</td>
<td>96.65%</td>
<td></td>
</tr>
</tbody>
</table>

Rule Results Summary

<table>
<thead>
<tr>
<th>pass</th>
<th>fixed</th>
<th>fail</th>
<th>error</th>
<th>not selected</th>
<th>not checked</th>
<th>not applicable</th>
<th>informational</th>
<th>unknown</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>173</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>179</td>
</tr>
</tbody>
</table>

Title

Auditing must be enabled at boot by setting a kernel parameter.

Result: fail

The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).

Result: fail

The system boot loader configuration file(s) must be owned by root.

Result: fail

The system boot loader configuration file(s) must be group-owned by root.

Result: fail

The system boot loader configuration file(s) must have mode 0600 or less permissive.

Result: fail

The system boot loader must require authentication.

Result: fail

17.4 AlertEnterprise Microsoft Server STIG Compliance Report

Non-Compliance Report - U_Windows_2008_R2_MS_V1R15_STIG_SCAP_1-0_Benchmark

Score

30.04%

Adjusted Score: 30.04%
Original Score: 30.04%
Compliance Status: RED

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
System Information

<table>
<thead>
<tr>
<th>Target</th>
<th>WIN-IPERGL2ELUD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 R2 Standard</td>
</tr>
<tr>
<td>OS Service Pack</td>
<td></td>
</tr>
</tbody>
</table>

Results

- **Unsupported Service Packs**
  - Systems must be at supported service pack (SP) or release levels. - Fail

- **Legal Notice Display**
  - The required legal notice will be configured to display before console logon. - (CCE-10673-2) - Fail

- **Caching of logon credentials**
  - Caching of logon credentials will be limited. - (CCE-10926-4) - Fail

- **Anonymous shares are not restricted**
  - Anonymous enumeration of shares will be restricted. - (CCE-10557-7) - Fail

- **Bad Logon Attempts**
  - The number of allowed bad-logon attempts will meet minimum requirements. - (CCE-11046-0) - Fail

- **Bad Logon Counter Reset**
  - The time before the bad-logon counter is reset will meet minimum requirements. - (CCE-11059-3) - Fail

- **Lockout Duration**
  - The lockout duration will meet minimum requirements. - (CCE-10399-4) - Fail

- **Rename Built-in Guest Account**
  - The built-in guest account will be renamed. - (CCE-10747-4) - Fail

- **Rename Built-in Administrator Account**
  - The built-in administrator account will be renamed. - (CCE-10976-9) - Fail

- **LanMan Authentication Level**
  - The LanMan authentication level will be set to Send NTLMv2 response only\refuse LM & NTLM. - (CCE-10984-3) - Fail

- **Deny Access from the Network**
  - The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-10733-4) - Fail

- **Smart Card Removal Option**
  - The Smart Card removal option will be configured to Force Logoff or Lock Workstation. - (CCE-10573-4) - Fail

- **Format and Eject Removable Media**
  - Ejection of removable NTFS media is not restricted to Administrators. - (CCE-10637-7) - Fail

- **Password Expiration Warning**
  - Users will be warned in advance that their passwords will expire. - (CCE-10930-6) - Fail

- **Disable Media Autoplay**
  - Autoplay will be disabled for all drives. - (CCE-11126-0) - Fail

- **Anonymous Access to Named Pipes**
  - Named pipes that can be accessed anonymously will be configured to contain no values. - (CCE-10944-7) - Fail

- **Remote Assistance - Solicit Remote Assistance**
  - Solicited Remote Assistance will not be allowed. - (CCE-11723-4) - Fail

- **Undock Without Logging On**
  - A system must be logged on to before removing from a docking station. - (CCE-10883-7) - Fail

- **Storage of Passwords and Credentials**
  - The system will be configured to prevent the storage of passwords and credentials - (CCE-10292-1) - Fail

- **Force Logoff When Logon Hours Expire**
  - The system will be configured to force users to log off when their allowed logon hours expire. - (CCE-10588-2) - Fail
• Session Security for NTLM SSP Based Clients
  o The system will be configured to meet the minimum session security requirement for NTLM SSP based clients. - (CCE-10035-4) - Fail

• FIPS Compliant Algorithms
  o The system will be configured to use FIPS-compliant algorithms for encryption, hashing, and signing. - (CCE-10789-6) - Fail

• TS/RDS - Session Limit
  o Remote Desktop Services will limit users to one remote session. - (CCE-12016-2) - Fail

• TS/RDS - Password Prompting
  o Remote Desktop Services will always prompt a client for passwords upon connection. - (CCE-11299-5) - Fail

• TS/RDS - Set Encryption Level
  o Remote Desktop Services will be configured with the client connection encryption set to the required level. - (CCE-11677-2) - Fail

• TS/RDS - Do Not Use Temp Folders
  o Remote Desktop Services will be configured to use session-specific temporary folders. - (CCE-10669-0) - Fail

• TS/RDS - Delete Temp Folders
  o Remote Desktop Services will delete temporary folders when a session is terminated. - (CCE-12046-9) - Fail

• TS/RDS - Time Limit for Disc. Session
  o Remote Desktop Services will be configured to set a time limit for disconnected sessions. - (CCE-11117-9) - Fail

• TS/RDS - Time Limit for Idle Session
  o Remote Desktop Services will be configured to disconnect an idle session after the specified time period. - (CCE-11506-3) - Fail

• Remote Assistance - Offer Remote Assistance
  o The system will be configured to prevent unsolicited remote assistance offers. - (CCE-11625-1) - Fail

• Error Reporting - Report Errors
  o The system will be configured to prevent automatic forwarding of error information. - (CCE-11750-7) - Fail

• Safe DLL Search Mode
  o The system will be configured to use Safe DLL Search Mode. - (CCE-10772-2) - Fail

• Media Player - Disable Automatic Updates
  o Media Player must be configured to prevent automatic checking for updates. - (CCE-11298-7) - Fail

• Session Security for NTLM SSP based Servers
  o The system will be configured to meet the minimum session security requirement for NTLM SSP based servers. - (CCE-10040-4) - Fail

• Audit Log Warning Level
  o The system will generate an audit event when the audit log reaches a percent full threshold. - (CCE-11011-4) - Fail

• Disable IP Source Routing
  o The system will be configured to prevent IP source routing. - (CCE-10732-6) - Fail

• Disable ICMP Redirect
  o The system will be configured to prevent ICMP redirects from overriding OSPF generated routes. - (CCE-10518-9) - Fail

• Disable Router Discovery
  o The system will be configured to disable the Internet Router Discover Protocol (IRDP). - (CCE-10768-0) - Fail

• TCP Connection Keep-Alive Time
  o The system will be configured to limit how often keep-alive packets are sent. - (CCE-10381-2) - Fail

• Name-Release Attacks
  o The system will be configured to ignore NetBIOS name release requests except from WINS servers. - (CCE-10653-4) - Fail

• TCP Data Retransmissions
  o The system will limit how many times unacknowledged TCP data is retransmitted. - (CCE-10941-3) - Fail

• Screen Saver Grace Period
  o 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

• Remotely Accessible Registry Paths and Sub-Paths
  o Unauthorized remotely accessible registry paths and sub-paths will not be configured. - (CCE-10935-5) - Fail
• Strong Key Protection
  o Users will be required to enter a password to access private keys. - (CCE-11035-3) - Fail
• Optional Subsystems
  o Optional Subsystems will not be permitted to operate on the system. - (CCE-10913-2) - Fail
• Software Restriction Policies
  o Software certificate restriction policies will be enforced. - (CCE-10900-9) - Fail
• TS/RDS - Secure RPC Connection.
  o The Remote Desktop Session Host will require secure RPC communications. - (CCE-11368-8) - Fail
• Group Policy - Registry Policy Processing
  o Group Policy objects will be reprocessed even if they have not changed. - (CCE-12754-8) - Fail
• SMB Client Packet Signing (Always)
  o The Windows SMB client will be enabled to always perform SMB packet signing. - (CCE-10970-2) - Fail
• Minimum Password Length
  o For systems utilizing a logon ID as the individual identifier, passwords will, at a minimum, be 14 characters. - (CCE-10372-1) - Fail
• Display of Last User Name
  o The system will be configured to prevent the display of the last user name on the logon screen. - (CCE-10788-8) - Fail
• Audit Policy Subcategory Setting
  o Audit policy using subcategories will be enabled. - (CCE-10112-1) - Fail
• IPSec Exemptions
  o IPSec Exemptions will be limited. - (CCE-10018-0) - Fail
• UAC - Admin Approval Mode
  o User Account Control approval mode for the built-in Administrator will be enabled. - (CCE-11028-8) - Fail
• UAC - Admin Elevation Prompt
  o User Account Control will, at a minimum, prompt administrators for consent. - (CCE-11023-9) - Fail
• UAC - User Elevation Prompt
  o User Account Control will automatically deny standard user requests for elevation. - (CCE-10807-6) - Fail
• Enumerate Administrator Accounts on Elevation
  o The system will require username and password to elevate a running application. - (CCE-11450-4) - Fail
• TS/RDS - Prevent Password Saving
  o Passwords will not be saved in the Remote Desktop Client. - (CCE-11905-7) - Fail
• TS/RDS - Drive Redirection
  o Local drives will be prevented from sharing with Remote Desktop Session Hosts (Remote Desktop Services Role). - (CCE-11709-3) - Fail
• RPC - Unauthenticated RPC Clients
  o Unauthenticated RPC clients will be restricted from connecting to the RPC server. - (CCE-10881-1) - Fail
• RPC - Endpoint Mapper Authentication
  o Client computers will be required to authenticate for RPC communication. - (CCE-10715-1) - Fail
• Internet Download / Online Ordering
  o Web publishing and online ordering wizards will be prevented from downloading a list of providers. - (CCE-11136-9) - Fail
• Printing Over HTTP
  o Printing over HTTP will be prevented. - (CCE-11360-5) - Fail
• HTTP Printer Drivers
  o Downloading print driver packages over HTTP will be prevented. - (CCE-11563-4) - Fail
• Windows Update Device Drive Searching
  o Windows will be prevented from using Windows Update to search for drivers. - (CCE-10357-2) - Fail
• IPv6 Transition
  o IPv6 will be disabled until a deliberate transition strategy has been implemented. - Fail
• Windows Peer to Peer Networking
  o Windows Peer-to-Peer networking services will be turned off. - (CCE-11604-6) - Fail
• Prohibit Network Bridge
  o Network Bridges will be prohibited in Windows. - (CCE-12074-1) - Fail
• Root Certificates Update
• Root Certificates will not be updated automatically from the Microsoft site. - (CCE-11264-9) - Fail

• Event Viewer Events.asp Links
  o Event Viewer Events.asp links will be turned off. - (CCE-10693-0) - Fail

• Internet File Association Service
  o The Internet File Association service will be turned off. - (CCE-10697-1) - Fail

• Order Prints Online
  o The Order Prints Online wizard will be turned off. - (CCE-11243-3) - Fail

• Classic Logon
  o The classic logon screen will be required for user logons. - (CCE-11256-5) - Fail

• RSS Attachment Downloads
  o Attachments will be prevented from being downloaded from RSS feeds. - Fail

• Windows Explorer – Shell Protocol Protected Mode
  o Windows Explorer shell protocol will run in protected mode. - (CCE-11530-3) - Fail

• Windows Installer – IE Security Prompt
  o Users will be notified if a web-based program attempts to install software. - (CCE-10343-2) - Fail

• Windows Installer – User Control
  o Users will be prevented from changing installation options. - (CCE-10906-6) - Fail

• Windows Installer – Vendor Signed Updates
  o Non-administrators will be prevented from applying vendor signed updates. - (CCE-11468-6) - Fail

• Media Player – First Use Dialog Boxes
  o Users will not be presented with Privacy and Installation options on first use of Windows Media Player. - (CCE-11155-9) - Fail

• Network – Mapper I/O Driver
  o The Mapper I/O network protocol driver will be disabled. - (CCE-10484-4) - Fail

• Network – Responder Driver
  o The Responder network protocol driver will be disabled. - (CCE-11304-3) - Fail

• Network – WCN Wireless Configuration
  o The configuration of wireless devices using Windows Connect Now will be disabled. - (CCE-11242-5) - Fail

• Network – Windows Connect Now Wizards
  o The Windows Connect Now wizards will be disabled. - (CCE-11155-9) - Fail

• Device Install – PnP Interface Remote Access
  o Remote access to the Plug and Play interface will be disabled for device installation. - (CCE-11248-2) - Fail

• Device Install – Drivers System Restore Point
  o A system restore point will be created when a new device driver is installed. - (CCE-10546-0) - Fail

• Device Install – Generic Driver Error Report
  o An Error Report will not be sent when a generic device driver is installed. - (CCE-12274-7) - Fail

• Driver Install – Device Driver Search Prompt
  o Users will not be prompted to search Windows Update for device drivers. - (CCE-11319-1) - Fail

• Handwriting Recognition Error Reporting
  o Errors in handwriting recognition on Tablet PCs will not be reported to Microsoft. - (CCE-11030-4) - Fail

• Power Mgmt – Password Wake on Battery
  o 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

• Power Mgmt – Password Wake When Plugged In
  o 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

• Remote Assistance – Session Logging
  o Remote Assistance log files will be generated. - (CCE-11263-1) - Fail

• Game Explorer Information Downloads
  o Game explorer information will not be downloaded from Windows Metadata Services. - (CCE-11739-0) - Fail

• Error Reporting – Logging
  o Error Reporting events will be logged in the system event log. - (CCE-11621-0) - Fail

• Error Reporting – Windows Error Reporting
  o Windows Error Reporting to Microsoft will be disabled. - (CCE-11708-5) - Fail

• Error Reporting – Additional Data
Additional data requests in response to Error Reporting will be declined. - (CCE-11584-0) - Fail

- Windows Explorer – Heap Termination
  - Windows Explorer heap termination on corruption will be disabled. - (CCE-10981-9) - Fail

- Logon – Report Logon Server
  - Users will be notified if the logon server was inaccessible and cached credentials were used. - (CCE-12260-6) - Fail

- Media DRM – Internet Access
  - Windows Media Digital Rights Management will be prevented from accessing the Internet. - (CCE-11052-8) - Fail

- TS/RDS – COM Port Redirection
  - 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

- TS/RDS – LPT Port Redirection
  - 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

- TS/RDS – PNP Device Redirection
  - 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

- TS/RDS – Smart Card Device Redirection
  - 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

- TS/RDS – Printer Redirection
  - 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

- TS/RDS – Remove Disconnect Option
  - 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

- Windows Customer Experience Improvement Program
  - The Windows Customer Experience Improvement Program will be disabled. - (CCE-11354-8) - Fail

- SPN Target Name Validation Level
  - The service principal name (SPN) target name validation level will be turned off. - (CCE-10617-9) - Fail

- Computer Identity Authentication for NTLM
  - Services using Local System that use negotiate when reverting to NTLM authentication will use the computer identity vs. authenticating anonymously. - (CCE-10817-5) - Fail

- NTLM NULL Session Fallback
  - NTLM will be prevented from falling back to a Null session. - (CCE-10812-6) - Fail

- PKU2U Online Identities Authentication
  - PKU2U authentication using online identities will be prevented. - (CCE-10839-9) - Fail

- Kerberos Encryption Types
  - Kerberos encryption types will be configured to prevent the use of DES encryption suites. - (CCE-10843-1) - Fail

- IPv6 Source Routing
  - IPv6 source routing will be configured to highest protection. - (CCE-10888-6) - Fail

- IPv6 TCP Data Retransmissions
  - IPv6 TCP data retransmissions will be configured to prevent resources from becoming exhausted. - (CCE-10804-3) - Fail

- Elevate when setting a network’s location
  - Domain users will be required to elevate when setting a network’s location. - (CCE-11610-3) - Fail

- Direct Access – Route Through Internal Network
  - All Direct Access traffic will be routed through the internal network. - (CCE-11300-1) - Fail

- Windows Update Point and Print Driver Search
  - Windows Update will be prevented from searching for point and print drivers. - (CCE-11976-8) - Fail

- Prevent device metadata retrieval from Internet
  - Device metadata retrieval from the Internet will be prevented. - (CCE-11589-9) - Fail

- Prevent Windows Update for device driver search
  - Device driver searches using Windows Update will be prevented. - (CCE-11787-9) - Fail
• MSDT Interactive Communication
  o Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft will be prevented. - (CCE-10855-5) - Fail

• Windows Online Troubleshooting Service
  o Access to Windows Online Troubleshooting Service (WOTS) will be prevented. - (CCE-11161-7) - Fail

• Disable PerfTrack
  o Responsiveness events will be prevented from being aggregated and sent to Microsoft. - (CCE-11889-3) - Fail

• Application Compatibility Program Inventory
  o The Application Compatibility Program Inventory will be prevented from collecting data and sending the information to Microsoft. - (CCE-11043-7) - Fail

• Autoplay for non-volume devices
  o Autoplay will be turned off for non-volume devices. - (CCE-11375-3) - Fail

• Turn Off Game Updates
  o Downloading of game update information will be turned off. - (CCE-11807-5) - Fail

• Prevent Joining Homegroup
  o The system will be prevented from joining a homegroup. - (CCE-10691-4) - Fail

• Windows Anytime Upgrade
  o Windows Anytime Upgrade will be disabled. - (CCE-10544-5) - Fail

• Explorer Data Execution Prevention
  o Explorer Data Execution Prevention will be enabled. - (CCE-12161-6) - Fail

• Default Autorun Behavior
  o The default autorun behavior will be configured to prevent autorun commands. - (CCE-11431-4) - Fail

• Legal Banner Dialog Box Title
  o The Windows dialog box title for the legal banner will be configured. - (CCE-10010-7) - Fail

• Access this computer from the network
  o Unauthorized accounts will not have the "Access this computer from the network" user right. - (CCE-10086-7) - Fail

• Adjust memory quotas for a process
  o Unauthorized accounts will not have the "Adjust memory quotas for a process" user right. - (CCE-10849-8) - Fail

• Allow log on locally
  o Unauthorized accounts will not have the "Allow log on locally" user right. - (CCE-10853-0) - Fail

• Back up files and directories
  o Unauthorized accounts will not have the "Back up files and directories" user right. - (CCE-10880-3) - Fail

• Bypass traverse checking
  o Unauthorized accounts will not have the "Bypass traverse checking" user right. - (CCE-10369-7) - Fail

• Change the system time
  o Unauthorized accounts will not have the "Change the system time" user right. - (CCE-10122-0) - Fail

• Change the time zone
  o Unauthorized accounts will not have the "Change the time zone" user right. - (CCE-10897-7) - Fail

• Deny log on as a batch job
  o 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

• Deny log on as a service
  o 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

• Deny log on locally
  o 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

• Deny log on through Remote Desktop \ Terminal Services
  o 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
• Force shutdown from a remote system
  o Unauthorized accounts will not have the "Force shutdown from a remote system" user right. - (CCE-10785-4) - Fail
• Generate security audits
  o Unauthorized accounts will not have the "Generate security audits" user right. - (CCE-10274-9) - Fail
• Impersonate a client after authentication
  o Unauthorized accounts will not have the "Impersonate a client after authentication" user right. - (CCE-9946-5) - Fail
• Increase a process working set
  o Unauthorized accounts will not have the "Increase a process working set" user right. - (CCE-10548-6) - Fail
• Load and unload device drivers
  o Unauthorized accounts will not have the "Load and unload device drivers" user right. - (CCE-10202-0) - Fail
• Log on as a batch job
  o Unauthorized accounts will not have the "Log on as a batch job" user right. - (CCE-10549-4) - Fail
• Replace a process level token
  o Unauthorized accounts will not have the "Replace a process level token" user right. - (CCE-10599-9) - Fail
• Restore files and directories
  o Unauthorized accounts will not have the "Restore files and directories" user right. - (CCE-10805-0) - Fail
• Shut down the system
  o Unauthorized accounts will not have the "Shut down the system" user right. - (CCE-10439-8) - Fail
• Audit - Credential Validation - Failure
  o The system will be configured to audit "Account Logon > Credential Validation" failures. - Fail
• Audit - Computer Account Management - Failure
  o The system will be configured to audit "Account Management > Computer Account Management" failures. - Fail
• Audit - Other Account Management Events - Success
  o The system will be configured to audit "Account Management > Other Account Management Events" successes. - Fail
• Audit - Other Account Management Events - Failure
  o The system will be configured to audit "Account Management > Other Account Management Events" failures. - Fail
• Audit - Security Group Management - Failure
  o The system will be configured to audit "Account Management > Security Group Management" failures. - Fail
• Audit - User Account Management - Success
• Audit - User Account Management - Failure
  o The system will be configured to audit "Account Management > User Account Management" failures. - Fail
• Audit - Process Creation - Success
  o The system will be configured to audit "Detailed Tracking > Process Creation" successes. - Fail
• Audit - File System - Failure
  o The system will be configured to audit "Object Access > File System" failures. - Fail
• Audit - Registry - Failure
  o The system will be configured to audit "Object Access > Registry" failures. - Fail
• Audit - Audit Policy Change - Failure
  o The system will be configured to audit "Policy Change > Audit Policy Change" failures. - Fail
• Audit - Sensitive Privilege Use - Success
  o The system will be configured to audit "Privilege Use > Sensitive Privilege Use" successes. - Fail
• Audit - Sensitive Privilege Use - Failure
  o The system will be configured to audit "Privilege Use > Sensitive Privilege Use" failures. - Fail
• Audit - IPSec Driver - Success
  o The system will be configured to audit "System > IPSec Driver" successes. - Fail
• Audit - IPSec Driver - Failure
  o The system will be configured to audit "System > IPSec Driver" failures. - Fail
• Audit - Security State Change - Failure
  o The system will be configured to audit "System > Security State Change" failures. - Fail
• Audit - Security System Extension - Success
  o The system will be configured to audit "System > Security System Extension" successes. - Fail
• Audit - Security System Extension - Failure
  o The system will be configured to audit "System > Security System Extension" failures. - Fail
• 6to4 State
  o The 6to4 IPv6 transition technology will be disabled. - (CCE-11356-3) - Fail
• IP-HTTPS State
  o The IP-HTTPS IPv6 transition technology will be disabled. - (CCE-10832-4) - Fail
• ISATAP State
  o The ISATAP IPv6 transition technology will be disabled. - (CCE-11141-9) - Fail
• Teredo State
  o The Teredo IPv6 transition technology will be disabled. - (CCE-11865-3) - Fail
• Maximum Log Size - Application
  o The Application event log will be configured to a minimum size requirement. - (CCE-11143-5) - Fail
• Maximum Log Size - Security
  o The Security event log will be configured to a minimum size requirement. - (CCE-11033-8) - Fail
• Maximum Log Size - Setup
  o The Setup event log will be configured to a minimum size requirement. - (CCE-11717-6) - Fail
• Maximum Log Size - System
  o The System event log will be configured to a minimum size requirement. - (CCE-11174-0) - Fail
• Device Install Software Request Error Report
  o Windows will be prevented from sending an error report when a device driver requests additional software during installation. - (CCE-11336-5) - Fail
• Always Install with Elevated Privileges Disabled
  o The Windows Installer Always install with elevated privileges must be disabled. - (CCE-12401-6) - Fail
• Local admin accounts filtered token policy enabled on domain systems.
  o Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems. - Fail
• WINCC-000078
  o The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomization (ASLR) must be enabled and configured to Application Opt In. - Fail
• WINCC-000079
  o The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer must be enabled. - Fail
• WINCC-000080
  o The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Recommended Software must be enabled. - Fail
• WINCC-000081
  o The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software must be enabled. - Fail
• WINCC-000082
  o The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) must be enabled and configured to at least Application Opt Out. - Fail
• WINCC-000083
  o The Enhanced Mitigation Experience Toolkit (EMET) system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be configured to Application Opt Out. - Fail
• WINGE-000100
  o The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
• WINGE-000200
  o A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail
17.5 IT Domain Controller STIG Compliance Report

Non-Compliance Report - U_Windows2012_DC_V1R3_STIG_SCAP_1-1_Benchmark

SCAP Compliance Checker - 3.1.2

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

Score 91.13%

Adjusted Score: 91.13%
Original Score: 91.13%
Compliance Status: GREEN

Pass: 267 Not Applicable: 0
Fail: 26 Not Checked: 0
Error: 0 Not Selected: 0
Unknown: 0 Total: 293
BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

System Information

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

Results

• Bad Logon Attempts
  o The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
• Force Logoff When Logon Hours Expire
  o The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4)
  - Fail
• LDAP Signing Requirements
  o Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
• Computer Account Password Change
  o Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6)
  - Fail
• Remotely Accessible Registry Paths and Sub-Paths
  o Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
• Minimum Password Length
  o Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
• Media DRM – Internet Access
• Software Certificate Installation Files
  o Software certificate installation files must be removed from a system. - Fail
• Legal Banner Dialog Box Title
  o The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
• Access this computer from the network
  o Unauthorized accounts must not have the Access this computer from the network user right on domain controllers. - Fail
• Allow log on locally
Unauthorized accounts must not have the Allow log on locally user right. - (CCE-25228-8) - Fail

Back up files and directories

Unauthorized accounts must not have the Back up files and directories user right. - (CCE-25380-7) - Fail

Bypass traverse checking

Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail

Change the system time

Unauthorized accounts must not have the Change the system time user right. - (CCE-24185-1) - Fail

Change the time zone

Unauthorized accounts must not have the Change the time zone user right. - (CCE-24632-2) - Fail

Force shutdown from a remote system

Unauthorized accounts must not have the Force shutdown from a remote system user right. - (CCE-24734-6) - Fail

Increase a process working set

Unauthorized accounts must not have the Increase a process working set user right. - (CCE-24162-0) - Fail

Increase scheduling priority

Unauthorized accounts must not have the Load and unload device drivers user right. - (CCE-24779-1) - Fail

Log on as a batch job

Unauthorized accounts must not have the Log on as a batch job user right. - (CCE-23386-6) - Fail

Restore files and directories

Unauthorized accounts must not have the Restore files and directories user right. - (CCE-25518-2) - Fail

Shut down the system

Unauthorized accounts must not have the Shut down the system user right. - (CCE-23500-2) - Fail

Add workstations to domain

Unauthorized accounts must not have the Add workstations to domain user right. - (CCE-23271-0) - Fail

Audit Directory Service Access - Success

The system must be configured to audit DS Access - Directory Service Access successes. - Fail

Audit Directory Service Access - Failure

The system must be configured to audit DS Access - Directory Service Access failures. - Fail

Audit Directory Service Changes - Success

The system must be configured to audit DS Access - Directory Service Changes successes. - Fail

Audit Directory Service Changes - Failure

The system must be configured to audit DS Access - Directory Service Changes failures. - Fail

WINGE-000100

The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

17.6 IT WINDOWS 7 WORKSTATIONS STIG COMPLIANCE REPORT

Non-Compliance Report - U_Windows_7_V1R23_STIG_SCAP_1-0_Benchmark

SCAP Compliance Checker - 3.1.2

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

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

<table>
<thead>
<tr>
<th>Target:</th>
<th>ITWORKS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System:</td>
<td>Windows 7 Enterprise</td>
</tr>
<tr>
<td>OS Service Pack:</td>
<td>Service Pack 1</td>
</tr>
<tr>
<td>Domain:</td>
<td>ES-IDAM-B1</td>
</tr>
<tr>
<td>Processor:</td>
<td>Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz</td>
</tr>
<tr>
<td>Processor Architecture:</td>
<td>Intel64 Family 6 Model 45 Stepping 7</td>
</tr>
<tr>
<td>Processor Speed:</td>
<td>2200 MHz</td>
</tr>
<tr>
<td>Physical Memory:</td>
<td>6144 mb</td>
</tr>
<tr>
<td>Manufacturer:</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>Model:</td>
<td>VMware Virtual Platform</td>
</tr>
<tr>
<td>Serial Number:</td>
<td>VMware-42 09 b3 57 32 50 16 c6-cb 47 45 dd e3 a9 68 f1</td>
</tr>
<tr>
<td>BIOS Version:</td>
<td>6.00</td>
</tr>
<tr>
<td>Interfaces:</td>
<td>[00000007] Intel(R) PRO/1000 MT Network Connection</td>
</tr>
<tr>
<td></td>
<td>o 172.16.5.6</td>
</tr>
<tr>
<td></td>
<td>o 00:50:56:89:A2:29</td>
</tr>
</tbody>
</table>

4932 Results

- **Legal Notice Display**
  - The required legal notice must be configured to display before console logon. - (CCE-8973-0) - Fail

- **Bad Logon Attempts**
  - Number of allowed bad-logon attempts does not meet minimum requirements. - (CCE-9136-3) - Fail

- **Secure Print Driver Installation**
  - Print driver installation privilege is not restricted to administrators. - (CCE-9026-6) - Fail

- **Deny Access from the Network**
  - The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-9244-5) - Fail

- **Force Logoff When Logon Hours Expire**
  - The system is not configured to force users to log off when their allowed logon hours expire. - (CCE-9704-8) - Fail

- **Minimum Password Length**
  - For systems utilizing a logon ID as the individual identifier, passwords must be a minimum of 14 characters in length. - (CCE-9357-5) - Fail

- **TS/RDS - Remote User Connections**
  - Terminal Services / Remote Desktop Services - Prevent users from connecting using Terminal Services or Remote Desktop. - (CCE-9985-3) - Fail

- **Unnecessary Features Installed**
  - Unnecessary features are installed. - Fail
• Deny log on as a batch job
  o 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

• Deny log on as service
  o 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

• Deny log on locally
  o 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

• Deny log on through Remote Desktop \ Terminal Services
  o 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

• Enable accounts to be trusted for delegation

• WINGE-000100
  o The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. -
    Fail

• WINGE-000200
  o A group named DenyNetworkAccess must be defined on domain systems to include all local administrator
    accounts. - Fail

17.7 OZONE AUTHORITY AND OZONE SERVER CENTOS 6 SERVER STIG COMPLIANCE REPORT

XCCDF Test Result

17.7.1 Introduction

Test Result

<table>
<thead>
<tr>
<th>Result ID</th>
<th>Profile</th>
<th>Start time</th>
<th>End time</th>
<th>Benchmark</th>
<th>Benchmark version</th>
</tr>
</thead>
<tbody>
<tr>
<td>xccdf_org.open-scap_testresult_default-profile</td>
<td>(Default profile)</td>
<td>2015-04-08 07:58</td>
<td>2015-04-08 07:59</td>
<td>embedded</td>
<td>1</td>
</tr>
</tbody>
</table>

Target info

<table>
<thead>
<tr>
<th>Targets</th>
<th>Addresses</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost.localdomain</td>
<td>127.0.0.1</td>
<td>epe:o:redhat:enterprise_linux</td>
</tr>
<tr>
<td></td>
<td>172.16.4.11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0:0:0:0:0:0:0:0:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fe80:0:0:0:250:56ff:fe89:76dd</td>
<td></td>
</tr>
</tbody>
</table>

Score

<table>
<thead>
<tr>
<th>system</th>
<th>score</th>
<th>max</th>
<th>%</th>
<th>bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>95.53</td>
<td>100.00</td>
<td>95.53%</td>
<td></td>
</tr>
</tbody>
</table>

17.7.2 Rule Results Summary

<table>
<thead>
<tr>
<th>pass</th>
<th>fixed</th>
<th>fail</th>
<th>error</th>
<th>not selected</th>
<th>not checked</th>
<th>not applicable</th>
<th>informational</th>
<th>unknown</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>171</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>179</td>
</tr>
<tr>
<td>Title</td>
<td>Result</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditing must be enabled at boot by setting a kernel parameter.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Library files must be owned by root.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be owned by root.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be group-owned by root.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must have mode 0600 or less permissive.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system boot loader must require authentication.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system must provide VPN connectivity for communications over untrusted networks.</td>
<td>fail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 17.8 OZONE Envoy CentOS 6 Server STIG Compliance Report

#### XCCDF Test Result

#### Test Result

<table>
<thead>
<tr>
<th>Result ID</th>
<th>Profile</th>
<th>Start time</th>
<th>End time</th>
<th>Benchmark</th>
<th>Benchmark version</th>
</tr>
</thead>
<tbody>
<tr>
<td>xccdf_org.open-scap_testresult_default-profile</td>
<td>(Default profile)</td>
<td>2015-04-08 08:02</td>
<td>2015-04-08 08:03</td>
<td>embedded</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Target info

**Targets**
- localhost.localdomain

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

#### Score

<table>
<thead>
<tr>
<th>system</th>
<th>score</th>
<th>max</th>
<th>%</th>
<th>bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>96.09</td>
<td>100.00</td>
<td>96.09%</td>
<td></td>
</tr>
</tbody>
</table>

#### 17.8.2 Rule Results Summary

<table>
<thead>
<tr>
<th>pass</th>
<th>fixed</th>
<th>fail</th>
<th>error</th>
<th>not selected</th>
<th>not checked</th>
<th>not applicable</th>
<th>informational</th>
<th>unknown</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>172</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>179</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing must be enabled at boot by setting a kernel parameter.</td>
<td>fail</td>
</tr>
<tr>
<td>The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be owned by root.</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be group-owned by root.</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must have mode 0600 or less permissive.</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader must require authentication.</td>
<td>fail</td>
</tr>
<tr>
<td>The system must provide VPN connectivity for communications over untrusted networks.</td>
<td>fail</td>
</tr>
</tbody>
</table>
17.9 OT DOMAIN CONTROLLER STIG COMPLIANCE REPORT

Non-Compliance Report - U_Windows2012_DC_V1R3_STIG_SCAP_1-1_Benchmark

SCAP Compliance Checker - 3.1.2

Score | System Information | Stream Information | Results | Detailed Results
---|---|---|---|---
91.13% | | | | |

Adjusted Score: 91.13%
Original Score: 91.13%
Compliance Status: GREEN

Pass: 267 Not Applicable: 0
Fail: 26 Not Checked: 0
Error: 0 Not Selected: 0
Unknown: 0 Total: 293

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

System Information

<table>
<thead>
<tr>
<th>Target</th>
<th>OTDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012 R2 Standard</td>
</tr>
<tr>
<td>OS Service Pack</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>OT-ES-IDAM-B1</td>
</tr>
</tbody>
</table>

Results

- Bad Logon Attempts
  - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
- Force Logoff When Logon Hours Expire
  - The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail
- LDAP Signing Requirements
  - Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
- Computer Account Password Change
  - Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6) - Fail
- Remotely Accessible Registry Paths and Sub-Paths
  - Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
- Minimum Password Length
  - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
- Software Certificate Installation Files
  - Software certificate installation files must be removed from a system. - Fail
- Legal Banner Dialog Box Title
  - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
- Access this computer from the network
  - Unauthorized accounts must not have the Access this computer from the network user right on domain controllers. - Fail
- Adjust memory quotas for a process
- Allow log on locally
17.10 OT CONSOLEWORKS WINDOWS SERVER 2012 STIG COMPLIANCE REPORT

Non-Compliance Report - U_Windows2012_MS_V1R3_STIG_SCAP_1-1_Benchmark

<table>
<thead>
<tr>
<th>SCAP Compliance Checker - 3.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>Score</td>
</tr>
<tr>
<td>Adjusted Score: 97.13%</td>
</tr>
<tr>
<td>Original Score: 97.13%</td>
</tr>
<tr>
<td>Compliance Status: GREEN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pass: 271</th>
<th>Not Applicable: 0</th>
<th>Fail: 8</th>
<th>Not Checked: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLUE: Score equals 100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GREEN: Score is greater than or equal to 90</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Information

<table>
<thead>
<tr>
<th>Target</th>
<th>OT-CONSOLEWORKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012 R2 Standard</td>
</tr>
<tr>
<td>OS Service Pack</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>OT-ES-IDAM-B1</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz</td>
</tr>
<tr>
<td>Processor Architecture</td>
<td>Intel64 Family 6 Model 45 Stepping 7</td>
</tr>
<tr>
<td>Processor Speed</td>
<td>2200 MHz</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>8192 mb</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>Model</td>
<td>VMware Virtual Platform</td>
</tr>
<tr>
<td>Serial Number</td>
<td>VMware-42 09 c2 cc c1 37 31 5c-2d 94 63 96 80 d2 05 fe</td>
</tr>
<tr>
<td>BIOS Version</td>
<td>6.00</td>
</tr>
<tr>
<td>Interfaces</td>
<td>• [00000010] Intel(R) 82574L Gigabit Network Connection</td>
</tr>
<tr>
<td></td>
<td>o 172.16.6.8</td>
</tr>
<tr>
<td></td>
<td>o 00:50:56:89:56:86</td>
</tr>
</tbody>
</table>

Results

- **Bad Logon Attempts**
  - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail

- **Force Logoff When Logon Hours Expire**
  - The system must be configured to force users to log off when their allowed logon hours expire. - (CCE-25367-4) - Fail

- **Minimum Password Length**
  - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail

- **Legal Banner Dialog Box Title**
  - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail

- **Deny log on as a batch job**
  - The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-25215-5) - Fail

- **Deny log on as service**
  - The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-23117-5) - Fail

- **Deny log on locally**
  - The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-24460-8) - Fail

- **WINGE-000100**
  - The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail
17.11 OT WINDOWS 7 WORKSTATIONS STIG COMPLIANCE REPORT

Non-Compliance Report - U_Windows_7_V1R23_STIG_SCAP_1-0_Benchmark

SCAP Compliance Checker - 3.1.2

<table>
<thead>
<tr>
<th>Score</th>
<th>System Information</th>
<th>Stream Information</th>
<th>Results</th>
<th>Detailed Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>95.47%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Adjusted Score: 95.47%
Original Score: 95.47%
Compliance Status: GREEN

Score

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

System Information

<table>
<thead>
<tr>
<th>Target:</th>
<th>OTWORKS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System:</td>
<td>Windows 7 Enterprise</td>
</tr>
<tr>
<td>OS Service Pack:</td>
<td>Service Pack 1</td>
</tr>
<tr>
<td>Domain:</td>
<td>OT-ES-IDAM-B1</td>
</tr>
<tr>
<td>Processor:</td>
<td>Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz</td>
</tr>
<tr>
<td>Processor Architecture:</td>
<td>Intel64 Family 6 Model 45 Stepping 7</td>
</tr>
<tr>
<td>Processor Speed:</td>
<td>2200 MHz</td>
</tr>
<tr>
<td>Physical Memory:</td>
<td>4096 mb</td>
</tr>
<tr>
<td>Manufacturer:</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>Model:</td>
<td>VMware Virtual Platform</td>
</tr>
<tr>
<td>Serial Number:</td>
<td>VMware-42 09 49 1e 0a 42 38 8e-03 d2 8f e6 31 25 5a 63</td>
</tr>
<tr>
<td>BIOS Version:</td>
<td>6.00</td>
</tr>
<tr>
<td>Interfaces:</td>
<td>[00000007] Intel(R) PRO/1000 MT Network Connection</td>
</tr>
<tr>
<td></td>
<td>o 172.16.6.6</td>
</tr>
<tr>
<td></td>
<td>o 00:50:56:89:08:7A</td>
</tr>
</tbody>
</table>

Results

- Legal Notice Display
  - The required legal notice must be configured to display before console logon. - (CCE-8973-0) - Fail
- Bad Logon Attempts
  - Number of allowed bad-logon attempts does not meet minimum requirements. - (CCE-9136-3) - Fail
- Secure Print Driver Installation
o Print driver installation privilege is not restricted to administrators. - (CCE-9026-6) - Fail

• Deny Access from the Network
  o The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems. - (CCE-9244-5) - Fail

• Force Logoff When Logon Hours Expire
  o The system is not configured to force users to log off when their allowed logon hours expire. - (CCE-9704-8) - Fail

• Minimum Password Length
  o For systems utilizing a logon ID as the individual identifier, passwords must be a minimum of 14 characters in length. - (CCE-9357-5) - Fail

• Deny log on as a batch job
  o 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

• Deny log on as service
  o 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

• Deny log on locally
  o 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

• Deny log on through Remote Desktop \ Terminal Services
  o 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

• WINGE-000100
  o The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

• WINGE-000200
  o A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - Fail

17.12 PACS DOMAIN CONTROLLER STIG COMPLIANCE REPORT
**Score**

91.47 %

<table>
<thead>
<tr>
<th>Adjusted Score:</th>
<th>91.47 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Score:</td>
<td>91.47 %</td>
</tr>
<tr>
<td>Compliance Status:</td>
<td>GREEN</td>
</tr>
</tbody>
</table>

- **Pass:** 268
- **Fail:** 25
- **Not Applicable:** 0
- **Not Checked:** 0
- **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
- **BLUE:** Score equals 100

**System Information**

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

**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

**Detailed Results**

1. **Bad Logon Attempts** - The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
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
3. LDAP Signing Requirements - Domain controllers must require LDAP access signing. - (CCE-23587-9) - Fail
4. Computer Account Password Change - Domain controllers must be configured to allow reset of machine account passwords. - (CCE-24692-6) - Fail
5. Remotely Accessible Registry Paths and Sub-Paths - Unauthorized remotely accessible registry paths and sub-paths must not be configured. - (CCE-25426-8) - Fail
6. Minimum Password Length - Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
7. Legal Banner Dialog Box Title - The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
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
9. Allow log on locally - Unauthorized accounts must not have the Allow log on locally user right. - (CCE-25228-8) - Fail
10. Back up files and directories - Unauthorized accounts must not have the Back up files and directories user right. - (CCE-25380-7) - Fail
11. Bypass traverse checking - Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail
12. Change the system time - Unauthorized accounts must not have the Change the system time user right. - (CCE-24185-1) - Fail
13. Change the time zone - Unauthorized accounts must not have the Change the time zone user right. - (CCE-24632-2) - Fail
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
15. Increase a process working set - Unauthorized accounts must not have the Increase a process working set user right. - (CCE-24162-0) - Fail
16. Load and unload device drivers - Unauthorized accounts must not have the Load and unload device drivers user right. - (CCE-24779-1) - Fail
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
18. Restore files and directories - Unauthorized accounts must not have the Restore files and directories user right. - (CCE-25518-2) - Fail
19. Shut down the system - Unauthorized accounts must not have the Shut down the system user right. - (CCE-23500-2) - Fail
20. Add workstations to domain - Unauthorized accounts must not have the Add workstations to domain user right. - (CCE-23271-0) - Fail
21. Audit Directory Service Access - Success - The system must be configured to audit DS Access - Directory Service Access successes. - Fail
22. Audit - Directory Service Access - Failure - The system must be configured to audit DS Access - Directory Service Access failures. - Fail
23. Audit - Directory Service Changes - Success - The system must be configured to audit DS Access - Directory Service Changes successes. - Fail
24. Audit - Directory Service Changes - Failure - The system must be configured to audit DS Access - Directory Service Changes failures. - Fail
25. WINGE-000100 - The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

17.13 PACS CONSOLE WINDOWS SERVER 2012 STIG COMPLIANCE REPORT

Non-Compliance Report - U_Windows2012_MS_V1R3_STIG_SCAP_1-1_Benchmark

SCAP Compliance Checker - 3.1.2
Score | System Information | Stream Information | Results | Detailed Results
Score

96.06%

Adjusted Score: 96.06%
Original Score: 96.06%
Compliance Status: GREEN

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

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: • [00000010] Intel(R) 82574L Gigabit Network Connection
  o 172.16.7.11
  o 00:50:56:89:F8:E0

5186 Results

5187 • Bad Logon Attempts
5188  o The number of allowed bad logon attempts must meet minimum requirements. - (CCE-23909-5) - Fail
5189 • Force Logoff When Logon Hours Expire
5190  o 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  o Passwords must, at a minimum, be 14 characters. - (CCE-25317-9) - Fail
5194 • Legal Banner Dialog Box Title
5195  o The Windows dialog box title for the legal banner must be configured. - (CCE-24020-0) - Fail
5196 • Adjust memory quotas for a process
5197  o Unauthorized accounts must not have the Adjust memory quotas for a process user right. - (CCE-25112-4) - Fail
5198 • Bypass traverse checking
5199  o Unauthorized accounts must not have the Bypass traverse checking user right. - (CCE-25271-8) - Fail
5200 • Deny log on as a batch job
5201  o 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-25215-5) - Fail
5203 • Deny log on as service
5204  o The Deny log on as a service user right on member servers must be configured to prevent access from highly
5205  privileged domain accounts on domain systems. No other groups or accounts must be assigned this right. - (CCE-23117-5) - Fail
5206 • Deny log on locally
5207  o The Deny log on locally user right on member servers must be configured to prevent access from highly
5208  privileged domain accounts on domain systems, and from unauthenticated access on all systems. - (CCE-24460-8) - Fail
5209 • Replace a process level token
5210  o Unauthorized accounts must not have the Replace a process level token user right. - (CCE-24555-5) - Fail
5211 • WINGE-000100
The Enhanced Mitigation Experience Toolkit (EMET) V4.1 Update 1 or later must be installed on the system. - Fail

17.14 BASELINE CENTOS 7 LINUX CONFIGURATION

How To STIG/Configure Centos 7
Install fresh Centos 7 server image, using Minimal Install. The following are assumptions in the installation:

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

```
yum update -y
yum install wget openscap-utils aide libreswan iptables-service ntp
mkdir {reports,xml}
cd xml
wget http://iase.disa.mil/stigs/Documents/u_RedHat_6_V1R6_STIG_SCAP_1-1_Benchmark.zip
unzip u_RedHat*
```

-----------------------------------------   Run Initial Test   -----------------------------------------

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

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

1. Next add the following files to the following locations:
   - rules_d-audit.rules > /etc/audit/rules.d/audit.rules
   - audit.rules > /etc/audit/audit.rules
   - audit.conf > /etc/audit/audit.conf
   - system-auth > /etc/pam.d/system-auth
   - system-aur 0 * * * root /sbin/aide -checkth-ac > /etc/pam.d/system-auth-ac
   - syslog.conf > /etc/sysctl.conf
   - password-auth-ac > /etc/pam.d/password-auth-ac
   - iptables > /etc/sysconfig/iptables

2. Next edit the following files:
   1. In /etc/logindefs add/change variables to:
      PASS_MIN_LEN 14
      PASS_MIN_DAYS 1
      PASS_MAX_DAYS 60
   2. Add the following to /etc/crontab:
3. In `/etc/modprobe.d/disabled.conf` (create if doesn't exist), add:

   ```
   install usb-storage /bin/false
   install dccp /bin/false
   install sctp /bin/false
   install rds /bin/false
   install tipc /bin/false
   install ipv6 /bin/false
   ```

4. Remove any line in `/etc/securetty` that starts with 'vc' or 'ttyS'

5. Add to `/etc/rsyslog.conf`

   ```
   *.* @@<any remote syslog server IP address>:514
   ```

6. Add to `/etc/sysconfig/init`

   ```
   SINGLE=/sbin/sulogin
   PROMPT=no
   ```

7. Edit `/etc/ntp.conf`

   ```
   ◦ place '#' in front of any line that starts with 'server'
   ◦ Add 'server tick.usno.navy.mil'
   ```

8. For all files `/etc/csh.cshrc`, `/etc/profile`, `/etc/login.defs`, and `/etc/bashrc`

   ```
   ◦ Change any 'umask' line to 'umask 077' and any 'UMASK' line to 'UMASK 077'
   ```

9. Add to `/etc/inittab`

   ```
   id:3:initdefault:
   ```

10. Add to `/etc/security/limits.conf`

   ```
   * hard core 0
   * hard maxlogins 0
   ```

11. Edit `/etc/default/useradd`

   ```
   ◦ Change 'INACTIVE=-1' to 'INACTIVE=35'
   ```

12. `yum remove firewalld`

13. `chkconfig ntpd on`

14. `service ntpd start`

15. `ln -sf /lib/systemd/system/multi-user.target /etc/systemd/system/default.target`

17.14.1 **Baseline CentOS 7 Configuration Files**

1. Audit.rules file contents:

2. Audit.conf file contents:

3. iptables file contents:

4. Password_auth-ac file contents

5. rules_d-audi.rules file contents

6. Sysct1.conf files contents

7. system-auth file contents

8. system-auth-ac file contents
### 17.14.2 Audit.rules File Contents

```bash
# This file controls the configuration of the audit daemon
#
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_gos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 6
max_log_file_action = ROTATE
space_left = 75
space_left_action = email
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SINGLE
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

### 17.14.3 Audit.conf File Contents

```bash
# This file controls the configuration of the audit daemon
#
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_gos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 6
max_log_file_action = ROTATE
space_left = 75
```

space_left_action = email
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SINGLE
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
#krb5_key_file = /etc/audit/audit.key

17.14.4 iptables File Contents
# Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
*nat
:PREROUTING ACCEPT [219:23061]
:INPUT ACCEPT [2:120]
:OUTPUT ACCEPT [125:7804]
:POSTROUTING ACCEPT [125:7804]
:OUTPUT_direct - [0:0]
:POSTROUTING_ZONES - [0:0]
:POSTROUTING_ZONES_SOURCE - [0:0]
:POSTROUTING_direct - [0:0]
:POST_public - [0:0]
:POST_public_allow - [0:0]
:POST_public_deny - [0:0]
:POST_public_log - [0:0]
:PREROUTING_ZONES - [0:0]
:PREROUTING_ZONES_SOURCE - [0:0]
:PREROUTING_direct - [0:0]
:PRE_public - [0:0]
:PRE_public_allow - [0:0]
:PRE_public_deny - [0:0]
:PRE_public_log - [0:0]
-A PREROUTING -j PREROUTING_direct
-A PREROUTING -j PREROUTING_ZONES_SOURCE
-A PREROUTING -j PREROUTING_ZONES
-A OUTPUT -j OUTPUT_direct
-A POSTROUTING -j POSTROUTING_direct
-A POSTROUTING -j POSTROUTING_ZONES_SOURCE
-A POSTROUTING -j POSTROUTING_ZONES
-A POSTROUTING_ZONES -o ens160 -g POST_public
-A POSTROUTING_ZONES -g POST_public
-A POST_public -j POST_public_log
-A POST_public -j POST_public_deny
-A POST_public -j POST_public_allow
-A PREROUTING_ZONES -i ens160 -g PRE_public
-A PREROUTING_ZONES -g PRE_public
-A PRE_public -j PRE_public_log
-A PRE_public -j PRE_public_deny
# Completed on Tue Jan 27 13:28:25 2015
# Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
*mangle
:PREROUTING ACCEPT [94235:148159541]
:INPUT ACCEPT [94155:148151187]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [43012:2796100]
:POSTROUTING ACCEPT [43027:2798919]
:FORWARD_direct - [0:0]
:INPUT_direct - [0:0]
:OUTPUT_direct - [0:0]
:POSTROUTING_direct - [0:0]
:PREROUTING_ZONES - [0:0]
:PREROUTING_ZONES_SOURCE - [0:0]
:PREROUTING_direct - [0:0]
:PRE_public - [0:0]
:PRE_public_allow - [0:0]
:PRE_public_deny - [0:0]
:PRE_public_log - [0:0]
-A PREROUTING -j PREROUTING_direct
-A PREROUTING -j PREROUTING_ZONES_SOURCE
-A PREROUTING -j PREROUTING_ZONES
-A INPUT -j INPUT_direct
-A FORWARD -j FORWARD_direct
-A OUTPUT -j OUTPUT_direct
-A POSTROUTING -j POSTROUTING_direct
-A PREROUTING_ZONES -i ens160 -g PRE_public
-A PREROUTING_ZONES -g PRE_public
-A PRE_public -j PRE_public_log
-A PRE_public -j PRE_public_deny
-A PRE_public -j PRE_public_allow
COMMIT
# Completed on Tue Jan 27 13:28:25 2015
# Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
*security
:INPUT ACCEPT [94003:148133781]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [43012:2796100]
:FORWARD_direct - [0:0]
:INPUT_direct - [0:0]
:OUTPUT_direct - [0:0]
-A INPUT -j INPUT_direct
-A FORWARD -j FORWARD_direct
-A OUTPUT -j OUTPUT_direct
COMMIT
# Completed on Tue Jan 27 13:28:25 2015
# Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
*raw
:PREROUTING ACCEPT [94236:148159577]
:OUTPUT ACCEPT [43012:2796100]
:OUTPUT_direct - [0:0]
:PREROUTING_direct - [0:0]
-A PREROUTING -j PREROUTING_direct
-A OUTPUT -j OUTPUT_direct

# Completed on Tue Jan 27 13:28:25 2015
# Generated by iptables-save v1.4.21 on Tue Jan 27 13:28:25 2015
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:FORWARD_IN_ZONES - [0:0]
:FORWARD_IN_ZONES_SOURCE - [0:0]
:FORWARD_OUT_ZONES - [0:0]
:FORWARD_OUT_ZONES_SOURCE - [0:0]
:FORWARD_direct - [0:0]
:FWDI_public - [0:0]
:FWDI_public_allow - [0:0]
:FWDI_public_deny - [0:0]
:FWDI_public_log - [0:0]
:FWDO_public - [0:0]
:FWDO_public_allow - [0:0]
:FWDO_public_deny - [0:0]
:FWDO_public_log - [0:0]
:INPUT_ZONES - [0:0]
:INPUT_ZONES_SOURCE - [0:0]
:INPUT_direct - [0:0]
:IN_public - [0:0]
:IN_public_allow - [0:0]
:IN_public_deny - [0:0]
:IN_public_log - [0:0]
:OUTPUT_direct - [0:0]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -j INPUT_direct
-A INPUT -j INPUT_ZONES_SOURCE
-A INPUT -j INPUT_ZONES
-A INPUT -p icmp -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i lo -j ACCEPT
-A FORWARD -j FORWARD_direct
-A FORWARD -j FORWARD_IN_ZONES_SOURCE
-A FORWARD -j FORWARD_IN_ZONES
-A FORWARD -j FORWARD_OUT_ZONES_SOURCE
-A FORWARD -j FORWARD_OUT_ZONES
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -j OUTPUT_direct
-A FORWARD_IN_ZONES -i ens160 -g FWDI_public
-A FORWARD_IN_ZONES -o ens160 -g FWDO_public
-A FORWARD_OUT_ZONES -g FWDO_public
-A FWDI_public -j FWDI_public_log
-A FWDI_public -j FWDI_public_deny
-A FWDI_public -j FWDI_public_allow
-A FWDO_public -j FWDO_public_log
-A FWDO_public -j FWDO_public_deny
-A FWDO_public -j FWDO_public_allow
-A INPUT_ZONES -i ens160 -g IN_public
-A INPUT_ZONES -g IN_public
-A IN_public -j IN_public_log
-A IN_public -j IN_public_deny
-A IN_public -j IN_public_allow
-A IN_public_allow -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
COMMIT

# Completed on Tue Jan 27 13:28:25 2015

17.14.5 Password_auth-ac File Contents

```plaintext
#$PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth sufficient pam_unix.so nullok try_first_pass
auth [default=die] pam_faillock.so authfail deny=3 unlock_time=604800 fail_interval=900
auth required pam_faillock.so authsucceed deny=3 unlock_time=604800 fail_interval=900
auth requisite pam_succeed_if.so uid >= 1000 quiet_success
auth required pam_deny.so
account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 1000 quiet
account required pam_permit.so
password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authok_type=
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authok
password required pam_deny.so
session optional pam_keyinit.so revoke
session required pam_limits.so
session optional pam_systemd.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
```

17.14.6 rules_d-audi.rules File Contents

```
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
# The rules are simply the parameters that would be passed
# to auditctl.

-D
```
# Increase the buffers to survive stress events.
# Make this bigger for busy systems
-b 320

# Feel free to add below this line. See auditctl man page
# STIG Stuff Below
# audit_time_rules
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock_settime -k audit_time_rules
-w /etc/localtime -p wa -k audit_time_rules

# audit_account_changes
-w /etc/group -p wa -k audit_account_changes
-w /etc/passwd -p wa -k audit_account_changes
-w /etc/gshadow -p wa -k audit_account_changes
-w /etc/shadow -p wa -k audit_account_changes
-w /etc/security/opasswd -p wa -k audit_account_changes

# MAC-policy
-w /etc/selinux -p wa -k MAC-policy

# export
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k export
-a always,exit -F arch=b64 -S mount -F auid=0 -k export

# delete
-a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid=0 -k delete

# actions
-w /etc/sudoers -p wa -k actions

# modules
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules

# perm_mod
-a always,exit -F arch=b32 -S chmod -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -F auid=0 -k perm_mod
-a always,exit -F arch=b32 -S fchmod -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S fchown -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S chmod -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S chown -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S fchown -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S chmod -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S chmod -F auid=0 -k perm_mod
- a always, exit -F arch=b32 -S chmodat -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b32 -S chmodat -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S chmodat -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S chmodat -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S chown -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S chown -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S chownat -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S chownat -F auid=0 -k perm_mod
- a always, exit -F arch=b32 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b32 -S fremovexattr -F auid=0 -k perm_mod
- a always, exit -F arch=b32 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b32 -S fremovexattr -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S fremovexattr -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S fsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S fsetxattr -F auid=0 -k perm_mod
- a always, exit -F arch=b32 -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b32 -S lchown -F auid=0 -k perm_mod
- a always, exit -F arch=b64 -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod
- a always, exit -F arch=b64 -S lchown -F auid=0 -k perm_mod
-a always,exit -F arch=b32 -S lremovexattr -F auid>=500 -F
  auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S lremovexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=500 -F
  auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b32 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S lsetxattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid=0 -k perm_mod
-a always,exit -F arch=b32 -S removexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S removexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid=0 -k perm_mod

17.14.7 Sysctl.conf Files Contents
# System default settings live in /usr/lib/sysctl.d/00-system.conf.
# To override those settings, enter new settings here, or in an
# /etc/sysctl.d/<name>.conf file
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv6.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.send_redirects = 0
17.14.8 system-auth File Contents

`#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth  required  pam_env.so
auth  sufficient pam_unix.so try_first_pass
auth  [default=die] pam_faillock.so authfail deny=3 unlock_time=604800
    fail_interval=900
auth  required  pam_faillock.so authsucc deny=3 unlock_time=604800
    fail_interval=900
auth  requisite  pam_succeed_if.so uid >= 1000 quiet_success
auth  required  pam_deny.so

account  required  pam_unix.so
account  sufficient pam_localuser.so
account  sufficient pam_succeed_if.so uid < 1000 quiet
account  required  pam_permit.so

password required  pam_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1
    ocredit=-1 lcredit=-1 difok=4
password requisite  pam_pwquality.so try_first_pass local_users_only
    retry=3 authtok_type=
password sufficient pam_unix.so sha512 shadow try_first_pass use_authtok
password required  pam_deny.so

session  optional  pam_keyinit.so revoke
session  required  pam_limits.so
session  [success=1 default=ignore] pam_succeed_if.so service in crond
    quiet use_uid
session  required  pam_unix.so
session  required  pam_lastlog.so showfailed
session  required  pam_limits.so`

17.14.9 system-auth-ac File Contents

`#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth  required  pam_env.so
auth  sufficient pam_unix.so try_first_pass
auth  [default=die] pam_faillock.so authfail deny=3 unlock_time=604800
    fail_interval=900
auth  required  pam_faillock.so authsucc deny=3 unlock_time=604800
    fail_interval=900
auth  requisite  pam_succeed_if.so uid >= 1000 quiet_success
auth  required  pam_deny.so

account  required  pam_unix.so
account  sufficient pam_localuser.so
account  sufficient pam_succeed_if.so uid < 1000 quiet
account  required  pam_permit.so
account  required  pam_deny.so

password required  pam_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1
    ocredit=-1 lcredit=-1 difok=4
password requisite  pam_pwquality.so try_first_pass local_users_only
    retry=3 authtok_type=
password sufficient pam_unix.so sha512 shadow try_first_pass use_authtok
password required  pam_deny.so

session  optional  pam_keyinit.so revoke
session  required  pam_limits.so
session  optional  pam_systemd.so
session  [success=1 default=ignore] pam_succeed_if.so service in crond
    quiet use_uid
session  required  pam_unix.so
session  required  pam_lastlog.so showfailed
session  required  pam_limits.so`
password required pam_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1
ocredit=-1 lcredit=-1 difok=4
password requisite pam_pwquality.so try_first_pass local_users_only
retry=3 authtok_type=
password sufficient pam_unix.so sha512 shadow try_first_pass use_authtok
password required pam_deny.so

session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
session [success=1 default=ignore] pam_succeed_if.so service in crond
quiet use_uid
session required pam_unix.so
session required pam_lastlog.so showfailed
session required pam_limits.so

17.15 BASELINE CENTOS 7 STIG COMPLIANCE

Note the STIG compliance test is based on the CentOS 6 STIG compliance analysis. At the time this testing was completed the CentOS 7 STIG had not been published.

Introduction

Test Result

<table>
<thead>
<tr>
<th>Result ID</th>
<th>Profile</th>
<th>Start time</th>
<th>End time</th>
<th>Benchmark</th>
<th>Benchmark version</th>
</tr>
</thead>
<tbody>
<tr>
<td>xccdf_org.open-scap_testresult_default-profile</td>
<td>(Default profile)</td>
<td>2015-03-11 12:25</td>
<td>2015-03-11 12:26</td>
<td>embedded</td>
<td>1</td>
</tr>
</tbody>
</table>

Target info

Targets

Addresses

Platform

localhost.localdomain

• 127.0.0.1
• 10.32.2.59
• 0:0:0:0:0:0:1
• fe80:0:0:0:250:56ff:fe89:5cab

Score

<table>
<thead>
<tr>
<th>system</th>
<th>score</th>
<th>max</th>
<th>%</th>
<th>bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:xccdf:scoring:default</td>
<td>96.65</td>
<td>100.00</td>
<td>96.65%</td>
<td></td>
</tr>
</tbody>
</table>
Rule Results Summary

<table>
<thead>
<tr>
<th>pass</th>
<th>fixed</th>
<th>fail</th>
<th>error</th>
<th>not selected</th>
<th>not checked</th>
<th>not applicable</th>
<th>informational</th>
<th>unknown</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>173</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>179</td>
</tr>
</tbody>
</table>

17.15.1 Rule Results Summary

<table>
<thead>
<tr>
<th>Title</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing must be enabled at boot by setting a kernel parameter.</td>
<td>fail</td>
</tr>
<tr>
<td>The audit system must be configured to audit modifications to the systems Mandatory Access Control (MAC) configuration (SELinux).</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be owned by root.</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must be group-owned by root.</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader configuration file(s) must have mode 0600 or less permissive.</td>
<td>fail</td>
</tr>
<tr>
<td>The system boot loader must require authentication.</td>
<td>fail</td>
</tr>
</tbody>
</table>
## 18 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Literal Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate authority (also used as shorthand for the name of the company “CA Technologies”)</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>.csv</td>
<td>Comma-Separated Value</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>IdAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>iEMS</td>
<td>RADiFlow ICS/SCADA router configuration management software</td>
</tr>
<tr>
<td>ISE</td>
<td>Identity Services Engine</td>
</tr>
<tr>
<td>iSIM</td>
<td>Industrial Service Management Tool</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>JRE</td>
<td>Java Runtime Environment</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NCCoE</td>
<td>National Cybersecurity Center of Excellence</td>
</tr>
<tr>
<td>NERC</td>
<td>North American Electric Reliability Corporation</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control System</td>
</tr>
<tr>
<td>Acronym</td>
<td>Literal Translation</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>STIG</td>
<td>Security Technical Implementation Guideline</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAR</td>
<td>Web Application Archive</td>
</tr>
</tbody>
</table>

**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 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 ....................................................... 236
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 30. Condition Decision Values ........................................................................................... 186
Table 31. Guardian Job Scheduler Triggers Field Map ................................................................ 187
Table 32. Guardian AlertEnterprise DB Trigger ................................................................. 187