NIST SPECIAL PUBLICATION 1800-18

Privileged Account Management for the Financial Services Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Karen Waltermire
Tom Conroy
Marisa Harriston
Chinedum Irrechukwu
Navaneeth Krishnan
James Memole-Doodson
Benjamin Nkrumah
Harry Perper
Susan Prince
Devin Wynne

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

NIST SPECIAL PUBLICATION 1800-18

Privileged Account Management for the Financial Services Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Karen Waltermire
National Cybersecurity Center of Excellence
Information Technology Laboratory

Tom Conroy
Marisa Harriston
Chinedum Irrechukwu
Navaneeth Krishnan
James Memole-Doodson
Benjamin Nkrumah
Harry Perper
Susan Prince
Devin Wynne
The MITRE Corporation
McLean, VA

DRAFT

September 2018

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-18A

Privileged Account Management for the Financial Services Sector

Volume A:
Executive Summary

Karen Waltermire
National Cybersecurity Center of Excellence
Information Technology Laboratory

Tom Conroy
Marisa Harriston
Chinedum Irrechukwu
Navaneeth Krishnan
James Memole-Doodson
Benjamin Nkrumah
Harry Perper
Susan Prince
Devin Wynne
The MITRE Corporation
McLean, VA

September 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

Executive Summary

- Privileged accounts are used to access and manage an organization's information assets and systems. Often described as the "keys to the kingdom," these accounts are used by trusted users who perform tasks that ordinary users are not authorized to perform.
- Controlling these accounts is challenging, as the very nature of the functions that they perform requires broad access and authority. Additionally, this broad access makes privileged accounts a tempting target for external and internal malicious actors and increases the impact of accidental mistakes.
- Malicious actors can inflict substantial harm, often without notice. Industry reports have identified that privilege misuse is a major component of reported cyber incidents, with estimates up to 80 percent of all data breaches (Forrester 2016).
- To address this challenge, the National Cybersecurity Center of Excellence (NCCoE) has developed a reference design that illustrates how financial institutions can implement a privileged account management (PAM) system to secure, manage, control, and audit the use of privileged accounts.
- This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide describes how financial-services companies can use commercially available technology to implement PAM to reduce the risk associated with privileged accounts.

CHALLENGE

Financial organizations rely on privileged accounts to enable authorized users to perform their duties with little to no direct oversight or technical control of their actions. Companies have difficulty managing these accounts, which, in turn, opens a significant risk to the business. If used improperly, these accounts can cause substantial operational damage, including data theft, espionage, sabotage, or ransom. Malicious external actors can gain unauthorized access to privileged accounts through a variety of techniques, such as leveraging stolen credentials or social engineering schemes. In addition, there are rare instances of disgruntled employees who abuse their accounts, as well as honest employees who make mistakes. Misuse and mistakes can affect both high-value applications (e.g., payment systems) and core systems (e.g., human resources, database access, access control).

Managing privileged accounts is an important, yet complicated, task. Financial institutions often operate highly complex infrastructure and disparate systems that run on multiple operating systems. Managing and controlling access to these privileged accounts is further complicated by the significant pace of workforce and responsibility changes over time. Lastly, changes made at a system level can be used to bypass controls, to hide activity, and to cause financial institutions to breach their stringent reporting and compliance requirements.

SOLUTION

The NCCoE, in collaboration with experts from the financial services sector and technology vendors, developed a PAM system that controls, monitors, logs, and alerts on the use of privileged accounts. The example implementation highlights how organizations can add a security layer between users and the privileged accounts they access. This guide outlines the practical steps to secure privileged accounts in

your organization. We developed representative use-case scenarios to address specific challenges that the financial services sector faces during normal day-to-day business operations.

This guide references NIST guidance and industry standards, including the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool.

The NCCoE sought existing technologies that provided the following capabilities:

- privileged account control
- privileged account command filtering (allow or deny specific commands, such as disk formatting)
- multifactor authentication capability
- access logging/database system
- password management, including storage (vault)
- separation of duties management
- support least privileged policies
- password obfuscation (hiding passwords from PAM users)
- temporary access management
- automated logging and log management (analytics, storage, alerting)
- secure communications between components, where applicable
- ad hoc reporting to answer management, performance, and security questions
- support for multiple access levels for the PAM system (e.g., administrator, operator, viewer)
- protection from the introduction of new attack vectors into existing systems
- a complement to, rather than the replacement of, the existing security infrastructure

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and information-technology 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.

BENEFITS

Implementing a PAM system is an essential way for financial institutions to effectively secure, manage, control, and audit the activities of privileged accounts. A properly implemented and administered PAM system can help your organization meet compliance requirements, limit opportunity for and reduce the damage that a privileged user can cause, and improve the enforcement of access policies. The NCCoE's practice guide to address PAM for the financial services sector can help your organization:

- identify vulnerabilities and risk factors within your organization
- limit opportunity for a successful attack by improving control over privileged accounts

- improve efficiencies by reducing the complexity associated with managing privileged accounts, which leads to the following results:
  - minimized damage that results from misuse and mistakes by internal/external actors
  - automated enforcement of existing access policies
- simplify compliance by producing automated reports and documentation

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at financial_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

BOMGAR EKRAN IdRamp OneSpan RADIANT LOGIC Remediant RSA splunk> tdi technologies

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

Learn More
Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200

NIST SPECIAL PUBLICATION 1800-18B

Privileged Account Management for the Financial Services Sector

Volume B:
Approach, Architecture, and Security Characteristics

Karen Waltermire
National Cybersecurity Center of Excellence
Information Technology Laboratory

Tom Conroy
Marisa Harriston
Chinedum Irrechukwu
Navaneeth Krishnan
James Memole-Doodson
Benjamin Nkrumah
Harry Perper
Susan Prince
Devin Wynne
The MITRE Corporation
McLean, VA

September 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

DISCLAIMER

Certain commercial entities, equipment, products, 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, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-18B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-18B, 83 pages, September 2018, CODEN: NSPUE2

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.

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

Public comment period: September 28, 2018 through November 30, 2018

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology (IT) security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://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, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Privileged account management (PAM) is a domain within identity and access management (IdAM) that focuses on monitoring and controlling the use of privileged accounts. Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and service accounts. These powerful accounts provide elevated, often nonrestricted, access to the underlying IT resources and technology, which is why external and internal malicious actors seek to gain access to them. Hence, it is critical to monitor, audit, control, and manage privileged account usage. Many organizations, including financial sector companies, face challenges in managing privileged accounts.

The goal of this project is to demonstrate a PAM capability that effectively protects, monitors, and manages privileged account access, including life-cycle management, authentication, authorization, auditing, and access controls.

KEYWORDS

Access control, auditing, authentication, authorization, life-cycle management, multifactor authentication, PAM, privileged account management, provisioning management

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Dan Morgan	Bomgar (formerly Lieberman Software)
David Weller	Bomgar (formerly Lieberman Software)
Oleksiy Bidniak	Ekran System
Oleg Shomonko	Ekran System
Karl Kneiss	IdRamp
Eric Vinton	IdRamp
Michael Fagan	NIST
Will LaSala	OneSpan (formerly VASCO)
Michael Magrath	OneSpan (formerly VASCO)
Jim Chmura	Radiant Logic
Don Graham	Radiant Logic
Timothy Keeler	Remediant
Paul Lanzi	Remediant

Name	Organization
Michael Dalton	RSA
Timothy Shea	RSA
Adam Cohn	Splunk
Pam Johnson	TDi Technologies
Clyde Poole	TDi Technologies
Sallie Edwards	The MITRE Corporation
Sarah Kinling	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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:

Technology Partner/Collaborator	Build Involvement
Bomgar (formerly Lieberman Software)	Red Identity Suite
Ekran System	Ekran System Client
IdRamp	Secure Access
OneSpan (formerly VASCO)	DIGIPASS
Radiant Logic	RadiantOne FID
Remediant	SecureONE
RSA	SecureID Access

Technology Partner/Collaborator	Build Involvement
Splunk	Splunk Enterprise
TDi Technologies	ConsoleWorks

Contents

68 # List of Figures

76 # List of Tables

1 Summary

Financial organizations rely on privileged accounts to enable authorized users, such as systems administrators, to perform essential duties that ordinary users are not authorized to perform [1]. For example, system administrators use privileged "super user" accounts to manage information technology (IT) infrastructures and resources or to access high-value applications (e.g., payment systems, accounting systems) and core systems (e.g., human resources, database access, access control).

Despite being the "keys to the kingdom," these privileged accounts rarely receive direct oversight or technical control of how they are used. The lack of oversight and technical control poses a substantial operational and financial risk for organizations. If used improperly, privileged accounts can cause much damage, including data theft, espionage, sabotage, or ransom—often without notice. Privilege misuse is a major contributor of reported cyber incidents, with estimates as much as 80 percent of all data breaches [2]. Malicious external actors can gain unauthorized access to privileged accounts through various techniques, including leveraging stolen credentials, malware, social engineering schemes, or default passwords. In addition, there are occasional instances of disgruntled employees who abuse their accounts, even after they have left the company. Honest employees or contractors can also cause damage and downtime by making accidental mistakes with privileged accounts, even though that access was unnecessary for them to perform their work.

Organizations must harden themselves against these operational and reputational risks by implementing policies and technologies that **detect** and **prevent** the misuse of privileged accounts by external and internal actors. This combination of detection and prevention technologies and policies is referred to as privileged account management (PAM). PAM systems typically use one of two techniques for controlling account access and use: account escalation or account sharing. The account escalation technique escalates the privileged/authorized activity for each user's personal account for the duration of the session with the target system, based on the organizational policies. The account sharing technique utilizes a set of privileged accounts that are shared among the authorized privileged users via the PAM system.

Managing the access and use of privileged accounts is difficult without proper planning and tools. The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore methods to **manage and monitor the use of privileged accounts by authorized users** as they perform their normal activities, as well as techniques to **protect against and detect the unauthorized use of privileged accounts.** NIST Special Publication (SP) 800-171 [1], *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, defines a privileged user as "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." Privileged accounts are utilized in managing IT infrastructures, resources, and applications, as well as access to, and the use of, high-value applications like payment systems, accounting systems, and social media accounts.

The reference design and example solutions outlined in this guide describe example solutions built in the NCCoE lab. After reading this NIST Cybersecurity Practice Guide, an organization should be able to implement a PAM system that effectively monitors and manages privileged accounts. The solutions built in the NCCoE lab are not the only combination of technologies that can address this issue. They are examples demonstrating that off-the-shelf and open-source technologies are available to implement PAM.

The goals of this NIST Cybersecurity Practice Guide are to help organizations confidently:

- control access to, and the use of, privileged accounts (both on-premises and in the cloud)
- manage and monitor the activity of privileged accounts
- audit the activity of privileged accounts
- receive alerts or notifications when privileged accounts are used for unauthorized or out-of-policy activities
- encourage personal accountability among the users of privileged accounts
- enforce stringent policies for "least privilege" and separation of duties

For ease of use, a short description of the different sections of this volume is provided below:

- Section 1, Summary, presents the challenges addressed by the NCCoE project, with a look at the solution demonstrated to address the challenge, as well as benefits of the solution. This section also explains how to provide feedback on this guide.
- Section 2, How to Use This Guide, explains how readers—business decision makers, program managers, cybersecurity practitioners, and IT professionals (e.g., systems administrators)—might use each volume of this guide.
- Section 3, Approach, offers a detailed treatment of the scope of the project. This section also describes the assumptions on which the security architecture development was based; the risk assessment that informed architecture development; and NIST Cybersecurity Framework [3] functions supported by each component of the architecture and reference design, which industry collaborators contributed to support in building, demonstrating, and documenting the solution. This section also includes a mapping of the Cybersecurity Framework subcategories to other industry guidance, and identifies the products used to address each subcategory.
- Section 4, Architecture, describes the usage scenarios supported by the project architecture and reference design, as well as the capability descriptions, including a description of the relationship among the capabilities.
- Section 5, Example Implementations, provides in-depth descriptions of the implementations developed in the NCCoE's lab environment.

- Section 6, Security Characteristics Analysis, analyzes how to secure the components within the solution and minimize any vulnerabilities that they might have. This section also explains how the architecture addresses the security goals of the project.
- Section 7, Functional Evaluation, summarizes the test cases that we employed to demonstrate the example implementations' functionality and the Cybersecurity Framework functions to which each test case is relevant.

1.1 Challenge

In modern financial organizations, employees need access to a variety of applications, resources, and systems to ensure efficient business operations and meaningful customer experiences. Employees often access those systems through user accounts—commonly secured by usernames and passwords. Not all accounts are created equal, however. Some accounts—known as privileged accounts—are authorized to perform actions that ordinary accounts do not have authorization to perform. These privileged accounts provide elevated, often unrestricted, access to corporate resources and critical systems (e.g., crown jewels) beyond what a regular user would have. IT administrators and managers use these privileged accounts to perform system-critical actions, including maintenance, system management, and access control.

Privileged accounts pose significant operational, legal, and reputational risk to organizations if not secured effectively. The accounts become the virtual "keys to the kingdom," permitting unfettered access to many, if not all, systems within an organization.

The core risk of privileged accounts is that an organization faces significant damage to business operations if the accounts are misused for malicious or erroneous purposes. Malicious external attackers understand the value of privileged accounts and target them to maximize their access to the data, applications, and infrastructure of an organization, putting the organization at risk of data breach, espionage, sabotage, or ransom. Further, malicious actors may also be able to leverage privileged accounts to bypass, defeat, or otherwise render inoperable, other cybersecurity or legal compliance protections that protect critical systems or data.

The risk of privileged accounts is not limited to malicious external actors. Though relatively infrequent, there are instances of disgruntled employees leveraging their own or colleagues' privileged accounts for malicious purposes, including exfiltrating sensitive data, industrial sabotage, or creating technical backdoors that they or others can abuse after leaving the organization. Although less malicious, there are also instances in which well-meaning employees make mistakes while using their privileged accounts; these unintentional mistakes can cause significant disruption, which can influence business operations and customer satisfaction.

Managing access to, and the use of, privileged accounts is difficult without planning and tools. This practice guide provides the much-needed guidance and examples that financial institutions can use to reduce the risk of privileged accounts in their organization.

1.2 Solution

Organizations require a PAM solution that appropriately secures privileged accounts and enforces organizational policies for privileged account use. The NCCoE developed a PAM reference design that addresses these issues, providing control, oversight, and management of privileged accounts. The reference design outlines how monitoring, auditing, and authentication controls can combine to prevent unauthorized access to, and allow rapid detection of unapproved use, of privileged accounts.

The NCCoE developed example solutions, based on the reference design, that incorporate appropriate, commercially available technologies to manage and control the use of privileged accounts. The solutions are composed of multiple systems working together to enforce organizational access policies and to protect privileged accounts from misuse. These example solutions illustrate the various technical approaches available for PAM and the multiple areas of an organization (e.g., infrastructure, applications, cloud services, security monitoring), that can be considered for policy enforcement. This guide will also explain the importance of implementing policies, such as least privilege and separation of duties, for accounts that provide access to the data, applications, and infrastructure across an organization.

The NCCoE sought existing technologies that provided the following capabilities:

- privileged account control (password management and privilege escalation techniques)
- multifactor authentication (MFA)
- support both on-premises and cloud business systems
- event logging (e.g., access requests, logins, users)
- password management (including hiding passwords from users)
- policy management
- emergency/break-glass access
- log management (analytics, storage, alerting)
- user behavior analytics (UBA)

While the NCCoE used a suite of commercial products to address this cybersecurity challenge, this guide does not endorse these particular, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the 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 the design to the needs of your organization and its risk management decisions.

In developing our reference design, we used portions of the following standards and guidance, which can also provide your organization with relevant standards and best practices:

- NIST SP 800-171 Rev. 1: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [1]
- *NIST Framework for Improving Critical Infrastructure Cybersecurity* (commonly known as the NIST Cybersecurity Framework) [3]
- NIST SP 800-30 Rev. 1: *Guide for Conducting Risk Assessments* [4]
- NIST SP 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [5]
- NIST SP 800-39: *Managing Information Security Risk* [6]
- NIST SP 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and Organizations* [7]
- Federal Information Processing Standards (FIPS) 140-2: *Security Requirements for Cryptographic Modules* [8]
- NIST SP 800-92: *Guide to Computer Security Log Management* [9]
- NIST SP 800-100: *Information Security Handbook: A Guide for Managers* [10]
- Office of Management and Budget (OMB), Circular Number A-130: *Managing Information as a Strategic Resource* [11]
- Federal Financial Institutions Examination Council (FFIEC), *Cybersecurity Assessment Tool* (CAT) [12]
- NIST SP 800-63B: *Digital Identity Guidelines: Authentication and Lifecycle Management* [13]

1.3 Benefits

Implementing a PAM system is an essential way for financial institutions to effectively secure, manage, control, and audit the activities of privileged accounts. A properly implemented and administered PAM system can help an organization meet compliance requirements; limit opportunity for and reduce the damage that users of privileged accounts—whether authorized or unauthorized—can cause; and improve the enforcement of an organization's access policies.

The NCCoE's practice guide can help an organization:

- identify vulnerabilities and manage enterprise risk factors within the organization (consistent with the foundations of the NIST Cybersecurity Framework) [3]
- reduce the opportunity for a successful attack by improving control over privileged accounts
- improve efficiencies by reducing complexity associated with managing privileged accounts

- maintain the integrity and availability of data and systems that are critical to supporting business operations and revenue-generating activities
- reduce the impact of insider and external threats and other malicious or unintentional activity utilizing privileged accounts and accessing business-critical systems
- develop an implementation plan for PAM
- automate the enforcement of existing access policies

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate a solution for managing privileged accounts. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-18A: *Executive Summary*
- NIST SP 1800-18B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-18C: *How-To Guides* – instructions for building the example solution

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-18A*, which describes the following topics:

- challenges enterprises face in managing privileged accounts
- example solutions built at the NCCoE
- benefits of adopting an example solution

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 SP 1800-18B,* which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-18A,* with your leadership team members to help them understand the importance of adopting a standards-based PAM reference design that provides the control, oversight, and management of privileged accounts.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-18C*, to replicate all or parts of the build created in our lab. The How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally 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 within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. 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 PAM solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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 financial_nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**

Typeface/Symbol	Meaning	Example
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

Based on discussions with cybersecurity practitioners in the financial sector, the NCCoE pursued a PAM project to illustrate the broad set of capabilities available to manage privileged accounts. NCCoE engineers further worked to define the requirements for the PAM project by collaborating with the NCCoE Financial Sector Community of Interest (COI).

Members of the COI, which include participating vendors referenced in this document, contributed to developing a reference design and example implementations. Vendors provided technologies that met the project requirements, and assisted in installing and configuring those technologies. This practice guide highlights the approach that was used to develop the NCCoE reference design. Elements include risk assessment and analysis, logical design, example implementation development, test and evaluation, and security control mapping. This guide is intended to provide practical guidance to any organization interested in implementing a solution for managing and controlling the use of privileged accounts and for accessing business-critical/high-value systems and applications.

3.1 Audience

This guide is intended for individuals responsible for securing an organization's IT infrastructure, business systems, and applications (including cloud services). Current IT systems, particularly in the private sector, often lack PAM. The reference design and example solutions demonstrated by this project, and the implementation information provided in this practice guide, permit the integration of products to implement a PAM system and to protect current IT systems. The technical components will appeal to system administrators, IT managers, IT security managers, cybersecurity practitioners, and others directly involved in the secure and safe operation of the IT systems on which businesses rely.

3.2 Scope

This PAM practice guide includes a high-level architecture, reference design, and example implementations that depict approaches to manage and control the use of privileged accounts that use off-the-shelf and open-source technologies. This guide provides practical, real-world general guidance for developing and implementing a PAM solution consistent with the principles in the *NIST Framework for Improving Critical Infrastructure Cybersecurity Volume 1* (Cybersecurity Framework) [3]. The PAM reference design addresses subcategories within each of the Cybersecurity Framework core functions, as shown in the mapping of the reference design capabilities to the Cybersecurity Framework. Example

implementations (demonstrable lab implementations) include a broad range of technologies that provide organizations with various methods to control, monitor, audit, and enforce policies for the use of privileged accounts by privileged users. The architecture and technologies demonstrated by this project, and the implementation information provided in this practice guide, can inform the implementation of a PAM system by the integration of standards-based products. In addition, this guide describes how to monitor for unauthorized privilege escalation changes. Unauthorized-privilege-escalation monitoring is described in Section 4.1.2, Reference Design.

The following items were determined to be out of scope for this practice guide:

- specific PAM policy recommendations, other than following best-practice policies for least privilege and separation of duties
- specific PAM implementation guidance: The example solutions illustrated in this practice guide are intended to offer a broad set of examples of PAM deployments.
- specific security controls appropriate to secure the PAM system: General guidance is provided in Section 6.

In addition, the NCCoE is not recommending any one example solution as the approach to implement PAM. The example solutions illustrated in this practice guide are intended to offer a broad set of examples of PAM deployments. An organization implementing PAM should consider an implementation that is consistent with its risk management decisions.

3.3 Assumptions

This project is guided by the following assumptions:

- The solutions were developed in a lab environment. The environment is based on a typical organization's IT enterprise. The environment does not reflect the complexity of a production environment.
- An organization can access the skills and resources required to implement a PAM solution.

3.4 Risk Assessment

NIST SP 800-30 [4], *Guide for Conducting Risk Assessments*, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputations), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of NIST 800-37 [5], *Guide for Applying the Risk Management Framework to Federal Information Systems*—material that is available to the public. The risk management framework guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

We performed two types of risk assessment:

- initial analysis of the risk factors that were discussed with financial institutions: This analysis led to the creation of the PAM project and the desired security posture.
- analysis of how to secure the components within a solution and minimize any vulnerabilities that they might introduce (see Section 6, Security Characteristics Analysis)

3.4.1 Assessing Risk Posture

Using the guidance in NIST's series of publications concerning risk, we worked with financial institutions and the Financial Sector Information Sharing and Analysis Center to identify the most-compelling risk factors encountered by this business group. We participated in conferences and met with members of the financial sector to define the main security risks to business operations. These discussions gave us an understanding of strategic (mission) risks for organizations, with respect to PAM. NIST SP 800-39, *Managing Information Security Risk* [6], focuses on the business aspect of risk, namely at the enterprise level. This understanding is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. A summary of the strategic risk areas that we identified, and their mitigations, is provided below:

- Impact on system function: Ensuring the acceptable system availability, PAM reduces the risk of systems being compromised due to insiders and external malicious actors.
- Compliance with industry regulations: PAM complies with industry regulatory compliance requirements for access control for privileged accounts and corporate resources (e.g., data, applications).
- Maintenance of reputation and public image: PAM helps reduce the level of impact of insiders and external malicious actors, in turn helping maintain image.

These discussions also resulted in identifying a technical (operational) area of concern: the inability to adequately control the use of privileged accounts. We then identified the core operational risks, resulting from a privileged account compromise:

- data theft
- malicious/unauthorized/out-of-policy use of corporate resources (e.g., applications, computing resources)

- system unavailability
- data manipulation

We subsequently translated the identified operational risk factors to security functions and subcategories within the NIST Cybersecurity Framework.

3.4.2 Security Control Map

As explained in Section 3.4.1, we used a risk analysis process to identify the Cybersecurity Framework security functions and subcategories that we wanted the reference design to support. This was a critical first step in designing the reference design and example implementations to mitigate the risk factors. Table 3-1 lists the addressed Cybersecurity Framework functions and subcategories, and maps them to relevant NIST standards, industry standards, and controls and best practices. In Table 3-1, we mapped the categories to NIST's SP 800-53 Rev. 4 [7] controls, to International Electrotechnical Commission (IEC) / International Organization for Standardization (ISO) controls, and to FFIEC CAT [12], for additional guidance. The references provide solution validation points, as they list specific security capabilities that a solution addressing the Cybersecurity Framework subcategories would be expected to exhibit. Additionally, from NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [14], work roles are identified so that organizations may understand the work roles that are typically used by those implementing the capabilities contained in this practice guide.

Note: Not all of the Cybersecurity Framework subcategory guidance can be implemented by using technology. Any organization executing a PAM solution would need to adopt processes and organizational policies that address organization risk management. Many of the subcategories require that processes and policies be developed prior to implementing the technical recommendations within this practice guide.

428 **Table 3-1 PAM Reference Design Cybersecurity Framework Core Components Map**

Function	Category	Subcategory	Informative References			NIST SP 800-181 NICE Framework Work Roles
			FFIEC CAT	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-3:** Organizational communication and data flows are mapped.	D4.C.Co.B.4 D4.C.Co.Int.1	A.13.2.1	AC-4, CA-9, PL-8	PR-CDA-001
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	D1.R.St.B.1 D1.TC.Cu.B.1	A.6.1.1	PM-11	OV-SPP-001
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established.	D4.C.Co.B.1 D1.G.IT.B.2	Not applicable (N/A)	PM-8, SA-14	OV-MGT-001
		ID.BE-5: Resilience requirements to support delivery of critical services are established.	D5.IR.Pl.B.5 D5.IR.Pl.E.3	A.17.1.1, A.17.1.2, A.17.2.1	CP-2, SA-14	OV-MGT-001

Function	Category	Subcategory	Informative References			NIST SP 800-181 NICE Framework Work Roles
			FFIEC CAT	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established.	D1.G.SP.B.4	A.5.1.1	-1 controls from all families	OV-SPP-002
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners.	D1.G.SP.B.7	A.6.1.1, A.7.2.1	PM-1, PS-7	OV-SPP-001
		ID.GV-4: Governance and risk management processes address cybersecurity risks.	D1.G.SP.E.1	N/A	PM-9, PM-11	SP-RSK-002
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users.	D3.PC.Im.B.7 D3.PC.Am.B.6	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3	AC-2, IA Family	SP-DEV-001 OV-PMA-003

Function	Category	Subcategory	Informative References			NIST SP 800-181 NICE Framework Work Roles
			FFIEC CAT	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	D3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.4	AC-2, AC-3, AC-5, AC-6, AC-16	OM-STS-001
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.	D3.DC.Im.B.1 D3.DC.Im.Int.1	A.13.1.1, A.13.1.3, A.13.2.1	AC-4, SC-7	OM-NET-001
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected.	D1.G.IT.B.13 D3.PC.Am.A.1	N/A	SC-28	OM-DTA-002
		PR.DS-2: Data-in-transit is protected.	D3.PC.Am.B.13 D3.PC.Am.E.5 D3.PC.Am.Int.7	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8	OM-DTA-002 PR-CDA-001

Function	Category	Subcategory	Informative References			NIST SP 800-181 NICE Framework Work Roles
			FFIEC CAT	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	
		PR.DS-5: Protections against data leaks are implemented.	D3.PC.Am.B.15 D3.PC.Am.Int.1 D3.PC.De.Int.1 D3.DC.Ev.Int.1	A.6.1.2, A.9.1.1, A.9.1.2, A.9.2.3, A.9.2.4, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.13.1.3, A.13.2.1, A.13.2.3	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	SP-SYS-001
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	D1.G.SP.B.3 D2.MA.Ma.B.1 D2.MA.Ma.B.2	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	AU Family	OV-LGA-002
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	D3.PC.Am.B.3 D3.PC.Am.B.4 D3.PC.Am.B.7 D4.RM.Om.Int.1	A.9.1.2	AC-3	OM-ANA-001 PR-CDA-001

Function	Category	Subcategory	Informative References			NIST SP 800-181 NICE Framework Work Roles
			FFIEC CAT	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	
		PR.PT-4: Communications and control networks are protected.	D3.PC.Im.B.1 D3.PC.Im.Int.1	A.13.1.1, A.13.1.2, A.13.2.1	AC-4, SC-7	SP-ARC-002
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	D4.C.Co.B.4	N/A	AC-4, CA-3, CM-2, SI-4	SP-ARC-001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	D5.IR.Pl.Int.4	A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.7	AU family, CA-7, IR-4, SI-4	PR-CDA-001
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	D3.DC.Ev.E.1	A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.7	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	PR-CIR-001 CO-OPS-001
		DE.AE-5: Incident alert thresholds are established.	D3.DC.An.E.4 D3.DC.An.Int.3 D5.DR.De.B.1	A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.7	IR-4, IR-5, IR-8	PR-CIR-001

Function	Category	Subcategory	Informative References			NIST SP 800-181 NICE Framework Work Roles
			FFIEC CAT	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events.	D3.DC.An.A.3	A.12.4.1, A.12.4.3	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	AN-TWA-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	D3.DC.Ev.B.3	A.12.4.1, A.14.2.7, A.15.2.1	AU-12, CA-7, CM-3, SI-4	AN-TWA-001
RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-2:** Events are reported consistent with established criteria.	D5.ER.Es.B.4 D5.DR.Re.B.4 D5.IR.Pl.B.2	A.16.1.2	AU family, IR-6	IN-FOR-002
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-3:** Forensics are performed.	D3.CC.Re.Int.3 D3.CC.Re.Int.4	A.16.1.7	AU-7	PR-CDA-001

429

3.5 Security Functions and Subcategories Related to FFIEC

The example implementations are responsive to the desire to support compliance with the FFIEC CAT [12] guidance and with the NIST standards and best practices, as detailed in Table 3-1.

One example implementation is informed by FFIEC CAT guidance and may contribute to CAT-aligned implementations by providing PAM capabilities efficiently and cost-effectively. With this solution in place, privileged users have access to the only resources that they are authorized to maintain/administer or operate.

Table 3-2 describes how the PAM solution supports compliance with FFIEC CAT guidance.

Table 3-2 FFIEC CAT Guidance

FFIEC CAT Guidance	PAM Solution Characteristics
D4.C.Co.B.4: Data flow diagrams are in place and document information flows to external parties.	The solutions utilize data flows to determine the implementation approach.
D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	Data flows within the PAM solutions are documented and enforced because of the asset value to the organization.
D1.R.St.B.1: Information security roles and responsibilities have been identified. **D1.TC.Cu.B.1:** Management holds employees accountable for complying with the information security program. **D1.G.SP.B.4:** The institution has board-approved policies commensurate with its risk and complexity that address information security. **D1.G.SP.B.7:** All elements of the information security program are coordinated enterprise-wide. **D1.G.SP.E.1:** The institution augmented its information security strategy to incorporate cybersecurity and resilience. **D5.IR.P1.E.1:** The remediation plan and process outline the mitigating actions, resources, and time parameters.	The PAM solutions provide policy enforcement for privileged account access by using automation to ensure access policy compliance.
D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	A PAM solution may be classified as a critical asset that needs to be protected.

FFIEC CAT Guidance	PAM Solution Characteristics
D5.IR.Pl.B.5: A formal backup and recovery plan exists for all critical business lines. **D5.IR.Pl.E.3:** Alternative processes have been established to continue critical activity within a reasonable time.	The solutions include emergency access and can be implemented with high-availability components.
D3.PC.Im.B.7: Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. **D3.PC.Am.B.6:** Identification and authentication are required and managed for access to systems, applications, and hardware.	The solutions provide automated account access control for privileged users and for MFA authentication.
D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. **D3.PC.Am.B.2:** Employee access to systems and confidential data provides for separation of duties. **D3.PC.Am.B.5:** Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	The solutions provide automated policy enforcement for account access control for privileged users.
D3.DC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used. **D3.DC.Im.Int.1:** The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.	The solutions are implemented by using network defense tools and network segmentation to illustrate support for this guidance.
D1.G.IT.B.13: Confidential data is identified on the institution's network. **D3.PC.Am.A.1:** Encryption of select data at rest is determined by the institution's data classification and risk assessment.	The solutions protect confidential data by using encryption of data-at-rest (PAM passwords) and can support this guidance.
D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., internet). **D3.PC.Am.E.5:** Controls are in place to prevent unauthorized access to cryptographic keys.	The solutions include encryption capabilities and can be implemented to support this guidance.

FFIEC CAT Guidance	PAM Solution Characteristics
D3.PC.Am.Int.7: Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.	
D3.DC.Ev.Int.1: Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data. **D3.PC.Am.B.15:** Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. **D3.PC.Am.Int.1:** The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data. **D3.PC.De.Int.1:** Data-loss prevention controls or devices are implemented for inbound and outbound communications (e.g., email, file transfer protocol, Telnet, prevention of large file transfers).	The solutions provide automated account access control, including MFA for privileged users. Account access to confidential data is controlled to support this guidance.
D1.G.SP.B.3: The institution has policies commensurate with its risk and complexity that address the concept of threat information sharing. **D2.MA.Ma.B.1:** Audit log records and other security event logs are reviewed and retained in a secure manner. **D2.MA.Ma.B.2:** Computer event logs are used for investigations once an event has occurred.	The solutions provide automated log collection and analysis to support this guidance.
D3.PC.Am.B.3: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). **D3.PC.Am.B.4:** User access reviews are performed periodically for all systems and applications based on the risk to the application or system. **D3.PC.Am.B.7:** Access controls include password complexity and limits to password attempts and reuse. **D4.RM.Om.Int.1:** Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.	The solutions provide automated account access control and access reporting/logging for privileged users. The solutions include policies that can be audited and reported.

FFIEC CAT Guidance	PAM Solution Characteristics
D5.IR.P1.Int.4: Lessons learned from real-life cyber risk incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.	The solutions implemented are reconfigurable to support this guidance.
D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	The solutions are designed by using automated log collection and analysis to support this guidance.
D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response. **D3.DC.An.Int.3:** Tools actively monitor security logs for anomalous behavior and alert within established parameters. **D5.DR.De.B.1:** Alert parameters are set for detecting information security incidents that prompt mitigating actions.	The solutions are designed by using automated log collection and analysis to support this guidance.
D3.DC.Ev.B.3: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	The solutions are configured to block and log all unauthorized PAM system-use attempts, as well as to automatically discover new accounts/users, to support this guidance.
D5.ER.Re.B.4: Incidents are classified, logged, and tracked. **D5.ER.Es.B.4:** Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond. **D5.IR.Pl.B.2:** Communication channels exist to provide employees a means for reporting information security events in a timely manner.	The solutions are designed by using automated log collection and analysis to support this guidance.
D3.CC.Re.Int.3: Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties. **D3.CC.Re.Int.4:** Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.	The solutions can be implemented to support this guidance.

3.6 Technologies

Table 3-3 lists all of the technologies used in this project and provides a mapping between the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 3-1 for an explanation of the Cybersecurity Framework subcategory codes. Table 3-3 describes only the product capabilities that were used in our example solutions. Many of the products have additional security capabilities that were not used.

Table 3-3 Products and Technologies

Component ID	Specific Product	Function	Cybersecurity Framework Subcategories
1. Identity Store Lightweight Directory Access Protocol (LDAP)	Radiant Logic RadiantOne Federated Identity (FID)	1. An identity repository specifically reserved for the privileged users of the organization 2. Account change monitoring and reporting	ID.AM-6, ID.GV-1, ID.GV-2, PR.AC-1, PR.AC-4
2. MFA	RSA SecureID Access IdRamp Secure Access combined with Microsoft Authenticator and Azure Active Directory services OneSpan DIGIPASS (formerly VASCO) Remediant SecureOne	3. Add-on MFA capabilities for PAM system user login authentication 4. Logs of each authentication attempt	PR.AC-1

Component ID	Specific Product	Function	Cybersecurity Framework Subcategories
3. User Interface	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE TDi Technologies ConsoleWorks	5. Login authentication and a user-to-PAM-system interactive interface through which users interact to establish work sessions for each system that they administer or access to perform their work functions	N/A
4. Policy Management	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE TDi Technologies ConsoleWorks	6. The enterprise privileged-user access and control policies, such as privileged user sessions, are limited to four hours.	ID.AM-6, ID.GV-1, ID.GV-2, ID.GV-4, PR.AC-1, PR.AC-4
5. Password Management	Bomgar (formerly Lieberman Software) Red Identity Suite	7. Management and enforcement of the enterprise password policies	ID.GV-4, PR.AC-1

Component ID	Specific Product	Function	Cybersecurity Framework Subcategories
6. Session ID Management	Bomgar (formerly Lieberman Software) Red Identity Suite TDi Technologies ConsoleWorks	8. The session start and stop functionality 9. Enforces the enterprise access and control policies within each work session, such as limiting sessions to Secure Shell (SSH) or Remote Desktop Protocol (RDP) or limiting allowed application use on the target system	PR.AC-1, PR.DS-2, PR.PT-3, PR.PT-4
7. Password Vault	Bomgar (formerly Lieberman Software) Red Identity Suite TDi Technologies ConsoleWorks	10. Provides secure storage of the current password for each privileged account managed by the PAM system	PR.DS-1
8. Emergency Access	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE TDi Technologies ConsoleWorks	11. PAM use in unpredicted or emergency situations when access to privileged accounts is required by unanticipated users (privileged or nonprivileged)	ID.BE-5, ID.GV-1, ID.GV-2, ID.GV-4, PR.AC-1, PR.AC-4

Component ID	Specific Product	Function	Cybersecurity Framework Subcategories
9. Automated Account Discovery	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE	12. Automated search of the enterprise for evidence and identification of privileged accounts, such as domain administrators or accounts that directly or indirectly (through inheritance of privileges) have privileged-account-level authority	ID.GV-4, PR.AC-1, PR.AC-4, DE.CM-7
10. Session Monitoring	Ekran System Client TDi Technologies ConsoleWorks	13. A mechanism to identify, log, and alert on anomalous privileged-account activity	DE.CM-3
11. Session Replay	Ekran System Client TDi Technologies ConsoleWorks	14. Session review for training and event review and investigations	RS.AN-3
12. Security Monitoring	Splunk Enterprise Radiant Logic RadiantOne FID	15. Logging and auditing provide log storage, analysis, and alerting components	DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-3, DE.CM-7, PR.PT-1, RS.CO-2
13. Lab Environment	Miscellaneous	16. Virtual machines, networking, routing, firewalls, etc.	PR.AC-5, PR.DS-5

4 Architecture

PAM is a domain within identity and access management (IdAM) that focuses on monitoring and controlling the access rights assigned to privileged users for their privileged accounts. Privileged accounts include local, domain, and system administrative accounts, and application, application management, and service accounts. These accounts can also be used to gain access and conduct

transactions that use business-critical/high-value applications, such as payroll, social media, cloud services, and human resources.

The PAM architecture and reference design identify the set of capabilities and their relationships that, when combined, can be used to control and monitor the use of privileged accounts by privileged users, for both on-premises and cloud implementations. This section presents a high-level architecture and reference design for implementing such a solution. The reference design includes a broad set of capabilities available in the marketplace, to illustrate the full breadth of PAM capabilities that an organization may implement. The NCCoE understands that an organization may not need all of these capabilities. An organization may choose to implement a subset of the depicted capabilities, depending on its risk management decisions.

4.1 Architecture Description

4.1.1 High-Level Architecture

The PAM solution is designed to address the security functions and subcategories described in Table 3-1 and is composed of the capabilities illustrated in Figure 4-1 and Figure 4-2.

Figure 4-1 High-Level Architecture

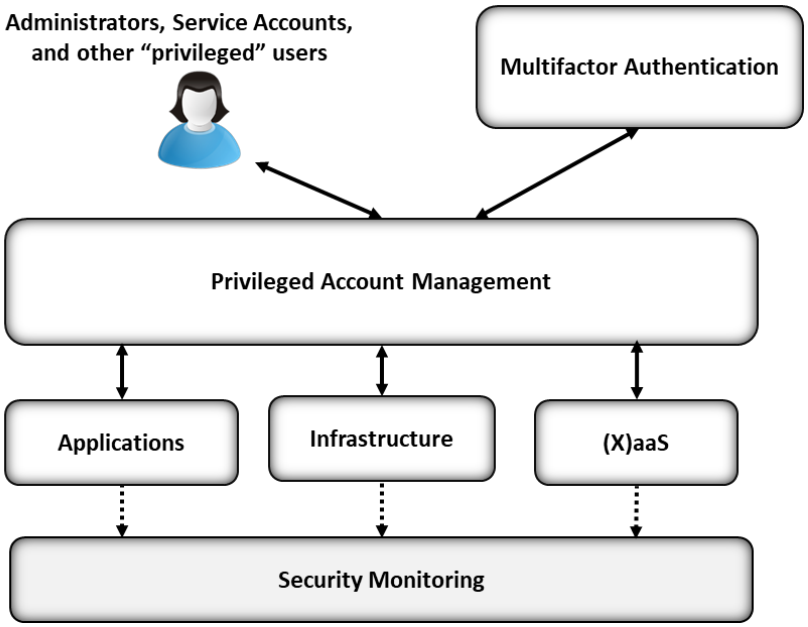


Figure 4-1 depicts the PAM architecture within the context of an enterprise. A PAM system is designed to mediate/control access to, and the use of, privileged accounts between enterprise systems and services and authorized "privileged" users. In Figure 4-1, "(X)aaS" stands for "[fill in the blank] as a

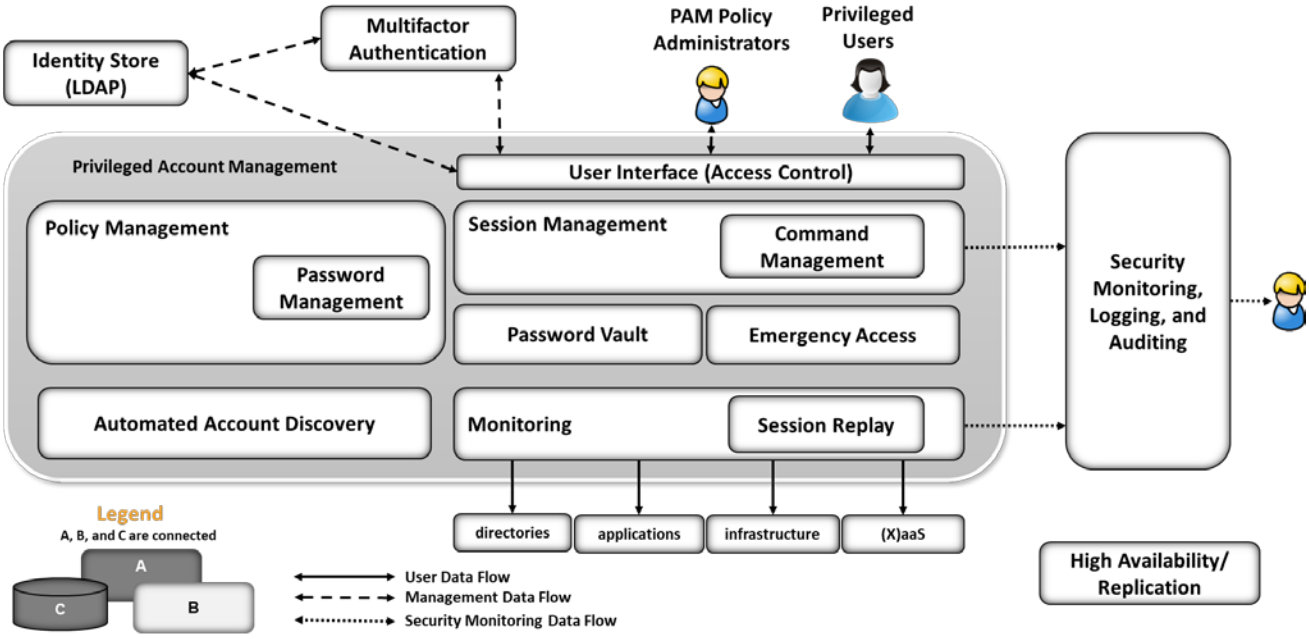
service," such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud services. Examples of each of these cloud services are as follows:

- SaaS: email, customer relationship management software
- PaaS: application development, streaming services
- IaaS: caching, storage, networking

4.1.2 Reference Design

The reference design shown in Figure 4-2 depicts the detailed PAM design, including the relationships among the capabilities that compose the design.

Figure 4-2 PAM Reference Design



The solid lines in Figure 4-2 represent the user data flow between privileged users and systems within the enterprise. The dashed lines represent the management data flow among PAM architecture components. The dotted lines represent the security monitoring data flow (logs). The PAM capabilities/components are briefly described below:

1. The identity store (LDAP) provides an identity repository specifically reserved for the privileged users of the organization.
2. MFA enables two or three authentication factors to improve the authentication level for privileged users (see NIST 800-63B [13] for a more detailed description of authentication factor requirements).

3. The user interface provides login authentication and a user-to-PAM-system interactive interface through which users interact to establish or request work sessions for each system that they administer or access to perform their work functions.
4. Policy management maintains the enterprise privileged-user access and control policies, such as limiting privileged user sessions to four hours.
5. Password management maintains and enforces the enterprise password policies.
6. Session management enforces the enterprise access and control policies within each work session, such as limiting sessions to SSH or RDP or limiting allowed application use on the target system.
7. The password vault provides secure storage of the current password for each privileged account managed by the PAM system.
8. Emergency access provides PAM use in unpredicted or emergency situations when access to privileged accounts is required by unanticipated users (privileged or nonprivileged).
9. Automated account discovery searches the enterprise for evidence and identification of privileged accounts, such as domain administrators or accounts that directly or indirectly (through inheritance of privileges) have privileged-account-level authority.
10. Session monitoring provides a mechanism to identify, log, and alert on anomalous activity as well as for real-time training for privileged account use.
11. Session replay provides session review for training and event review and investigations.
12. Security monitoring, logging, and auditing provides log storage, analysis, and alerting components, generally referred to as security information and event management (SIEM).
13. UBA monitors the activity of the privileged users for activity or actions that are considered to be unexpected or outside a recognized pattern of activity.
14. High availability/replication ensures the availability of the PAM solution.

PAM systems typically use one of two techniques for controlling account access and use: account escalation or account sharing. The account escalation technique escalates the privileged/authorized activity for each user's personal account for the duration of the session with the target system, based on the organizational policies. When each session is completed, the user's account is returned to its "normal"/nonprivileged authorization level. The account sharing technique utilizes a set of privileged accounts that are shared among the authorized privileged users. The passwords for these accounts are typically changed automatically, based on usage or time. For example, account-sharing PAM systems may be set up to change the password for each account after every session in which it is used, or, if unused, after a specific amount of time. Some organizations may choose to utilize an account-sharing PAM system with unique user-specific PAM accounts. This approach may provide simplified log analysis for forensic and training purposes, as the target system will record each unique user in its logs.

The components listed above work together to provide the PAM functionality. The user interface utilizes the identity store and MFA to authenticate privileged users and is the interface through which users interact with the PAM system. PAM users may be human or systems, such as applications. In PAM systems that implement privileged account sharing, session management establishes a session for each user to the system that they choose, based on the policies within the policy management system. Session management also utilizes the password vault to obtain passwords for the target systems. Each session is established via the monitoring and session replay systems, according to enterprise policies for session monitoring and recording. The target system and PAM system log the activity of each privileged user and send logs to the SIEM for analysis and alerting for anomalous events and conditions.

In PAM systems that implement account escalation techniques to manage privileged users, the session management system escalates the privilege of each user for the duration of the session with the target system, based on the policies within the policy management system. Session management monitors the session to return the account privilege level to its normal state after the user ends the session. Session management also logs the user account requests and the session request details according to enterprise policies. The target systems log the activity of each privileged user and send logs to the SIEM. NIST SP 800-92, *Guide to Computer Security Log Management* [9], was utilized for SIEM implementation and configuration guidance. The SIEM stores logs generated by each system and performs analytics to identify anomalous activity. Anomalous activity is reported to security analysts.

Automated account discovery provides the enterprise with continuous monitoring for accounts that may be considered privileged, and with changes to those accounts. Based on enterprise policies, the PAM administrators may include these newly identified privileged accounts in the PAM system. Automated account discovery can also be used to alert security analysts when account changes occur among the privileged accounts or if a nonprivileged account escalation attempt occurs. The high-availability/replication components are identified in the architecture to highlight the need to ensure high availability of a PAM system. An enterprise may find that a subset of the components is sufficient to address its risk mitigation needs.

UBA and high-availability/replication components were not included in the example solutions implemented in the NCCoE lab. The high-availability/replication component was not included due to the limited implementation scope of the NCCoE lab representative enterprise instance.

UBA solutions are designed to detect behaviors of concern by combining all relevant data (e.g., network and client/host-based activity, human resource systems, employee reports, public records, travel records), and to then look for meaningful patterns of behavior. For example, a UBA solution can detect that an attack, such as a privilege escalation attack, has been launched (ideally during the early formative stages of that attack). UBA was not included in the example implementations due to the lack of relevant data needed for effective pattern-of-behavior analysis. Because UBA techniques vary widely, UBA for PAM may be considered by organizations that can identify the specific dimensions of behavior and analysis important in their environment and risk management decisions.

5 Example Implementations

Multiple PAM implementations are included in this guide to illustrate the varied PAM techniques available and the various use cases where PAM provides value. Each example implementation illustrates a different PAM technique or implementation approach. An organization may consider implementing the PAM technique that best addresses its security needs. The implementations include PAM for IT infrastructure, business-critical/high-value applications, cloud services, privileged user workstations, and SIEM. The example implementations are constructed on the NCCoE lab's infrastructure and consist of several products to compose each implementation.

The lab infrastructure consists of a VMware vSphere virtualization operating environment. We used network-attached storage and virtual switches, as well as internet access, to interconnect the solution components. Both commercially available and open-source technologies are included in the lab infrastructure. The lab network is not connected to the NIST enterprise network.

Table 5-1 lists (alphabetically) the specific components/capabilities that the NCCoE utilized in the example implementations to create the desired functionality of PAM. Each component's functions are identified by the Component ID number from Table 3-3 in Section 3.6. For example, in Table 5-1, the Component ID 6 indicates Session Management. Note that many of the products offer capabilities other than those used in the NCCoE example implementations. The example implementations focus on the capabilities, rather than the products. The NCCoE is not recommending, assessing, or certifying the products included in the example implementations.

Table 5-1 Example Implementation Component List

Product Vendor	Component (product) Name	Component ID
Bomgar (formerly Lieberman Software)	Red Identity Suite	3, 4, 5, 6, 7, 8
Ekran System	System Client	9, 10
IdRamp	Secure Access	2
Radiant Logic	RadiantOne FID	1, 11
Remediant	SecureONE	3, 4, 8
RSA	SecureID Access	2
Splunk	Splunk Enterprise	11
TDi Technologies	ConsoleWorks	3, 4, 6, 7, 9, 10
OneSpan (formerly VASCO)	DIGIPASS	2

The example implementations described in the following sections are built around typical enterprise infrastructure components: SAMBA file server, Apache web server, Microsoft Structured Query Language (SQL) server, and a Microsoft Active Directory server that also runs Microsoft Domain Name System service, as well as an array of client machines, primarily running Windows 10 and Ubuntu 16.04.

Open-source router and firewall technologies were used as well. The implementation also included the Microsoft Azure Active Directory cloud service. The details of the implementations are included in Volume C of this practice guide.

The NCCoE built three example solutions in its lab. We built these examples to illustrate our modular approach and the wide variety of PAM techniques and approaches to the organizational management of privileged accounts. Organizations may identify techniques and or approaches for implementation (in part or in whole), based on their risk management decisions, regulatory/compliance requirements, and other resource constraints. The example solutions are described in the following subsections. Each subsection includes a diagram depicting the example solution implementation and the data flows. In the example implementations, management networks were implemented to highlight the need to segment networks for management, and event-log and production traffic as a best practice. Organizations may choose to segment traffic, based on their risk management decisions. The management network is described in Volume C.

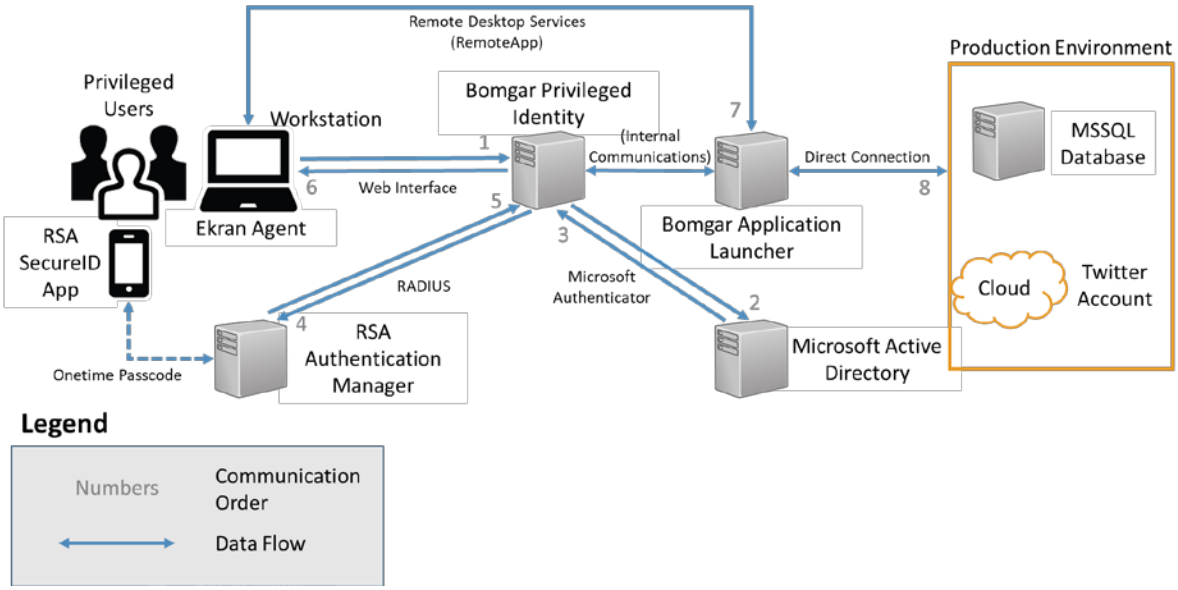
5.1 Example Implementation 1: Application Layer PAM

Example Implementation 1 was designed and implemented to illustrate PAM for the application-layer (including high-value applications) privileged accounts. These accounts are used by accounts payable administrators and specialists, social media administrators, writers/editors, human resources administrators, personnel managers, etc. These types of users are authorized to administer or use applications (including high-value applications) that can have significant (positive or negative) impacts on an organization. In this example, privileged user workstations have additional monitoring to illustrate local-workstation PAM capabilities. Where possible, all data-at-rest and data-in-transit are encrypted.

In Example Implementation 1 (Figure 5-1 and Figure 5-2), the NCCoE utilized these products to monitor and control privileged user access:

- Bomgar (formerly Lieberman) Privileged Identity and Application Launcher provides PAM capabilities.
- The Ekran agent provides PAM monitoring capabilities for the privileged user workstations.
- RSA Authentication Manager provides onetime-passcode synchronization and authentication (Option 1, Figure 5-1).
- IdRamp Secure Access, combined with Microsoft Authenticator and Azure Active Directory services, provides onetime-passcode synchronization and authentication (Option 2, Figure 5-2).
- Microsoft Active Directory provides the enterprise privileged-user identity store (source for privileged user identity information).
- Splunk Enterprise provides the security monitoring, logging, and auditing component (SIEM) (see Section 5.5 for a description of the security monitoring component).

619 **Figure 5-1 Example Implementation 1: Application Layer PAM Architecture (Option 1)**



620

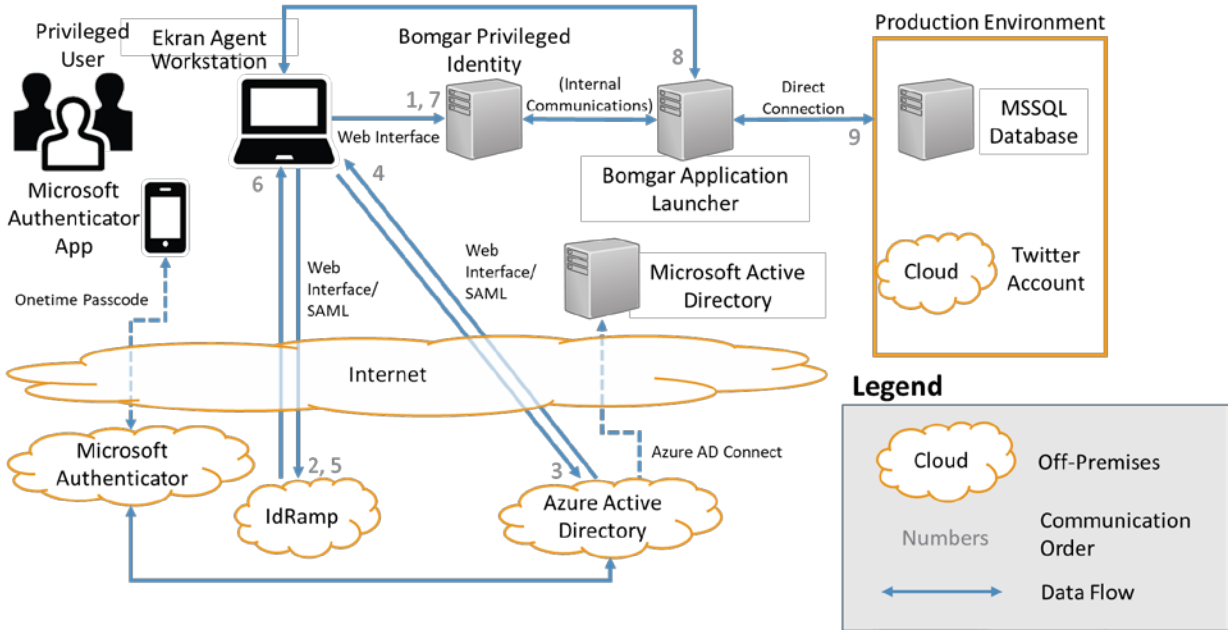
621 In this example implementation, the Ekran Agent monitors the privileged user activity on their
622 workstation. A best practice is that privileged users perform their work from dedicated workstations.
623 That workstation should not be used for nonprivileged user activities like email, web browsing, and
624 other organizational activities. The Bomgar Privileged Identity server provides the privileged-user-access
625 control interface. The user is authenticated based on their user account information within the
626 privileged user identity store that is implemented by using Microsoft Active Directory. Once the
627 privileged user authenticates with their username, password, and second authentication factor (a
628 onetime passcode via a phone application), the user is forwarded to the application launcher. Multiple
629 onetime-passcode products are utilized to highlight seamless modular implementation approaches to
630 implementing onetime passcodes for use in PAM implementations. Both RSA and IdRamp utilize a
631 onetime-passcode mobile application to provide the onetime-passcode second authentication factor.

632 In this example implementation, the NCCoE chose to integrate IdRamp with the Microsoft Authenticator
633 service to provide the onetime passcode. Both RSA Authentication Manager and the Microsoft
634 Authenticator service provide synchronization and authentication of the onetime passcode. The
635 application launcher gives the user a proxied access to the target system application. This PAM
636 implementation has used the account sharing PAM technique described in Section 4. The privileged
637 account required to access this application is used by the application launcher. The username is stored
638 in the application launcher, and the current password is pulled from a password vault. In this
639 implementation, we chose to have the password change after each application session is closed. The
640 session information is optionally monitored and recorded by the application launcher server for one or
641 more of the following purposes: security, forensics, and training. Logs of the session details are reported

to a security monitoring system for the detection of anomalous activity. The following list describes the authentication and access-control steps referenced in Figure 5-1:

1. The user connects to the Bomgar Privileged Identity web interface from their workstation and enters their username, password, and RSA token from the SecureID Access (Option 1) or Microsoft Authenticator (Option 2) application on their phone.
2. Bomgar authenticates the user by querying Active Directory to check the username and password. Active Directory returns an authentication response.
3. Bomgar sends the RSA token to the RSA Authentication Manager by using RADIUS (Option 1), or the Microsoft token to the Azure Active Directory services using Security Assertion Markup Language (SAML) via the IdRamp product (Option 2).
4. RSA Authentication Manager (Option 1) or Azure Active Directory services (Option 2) via the IdRamp product verifies the token and returns the allow/deny response to Bomgar.
5. Bomgar gives the user access to the full web interface, which allows the user to access the application launcher server.
6. The application launcher provides access to the target system either directly or via a remote desktop application.

Figure 5-2 Example Implementation 1: Application Layer PAM Architecture (Option 2)



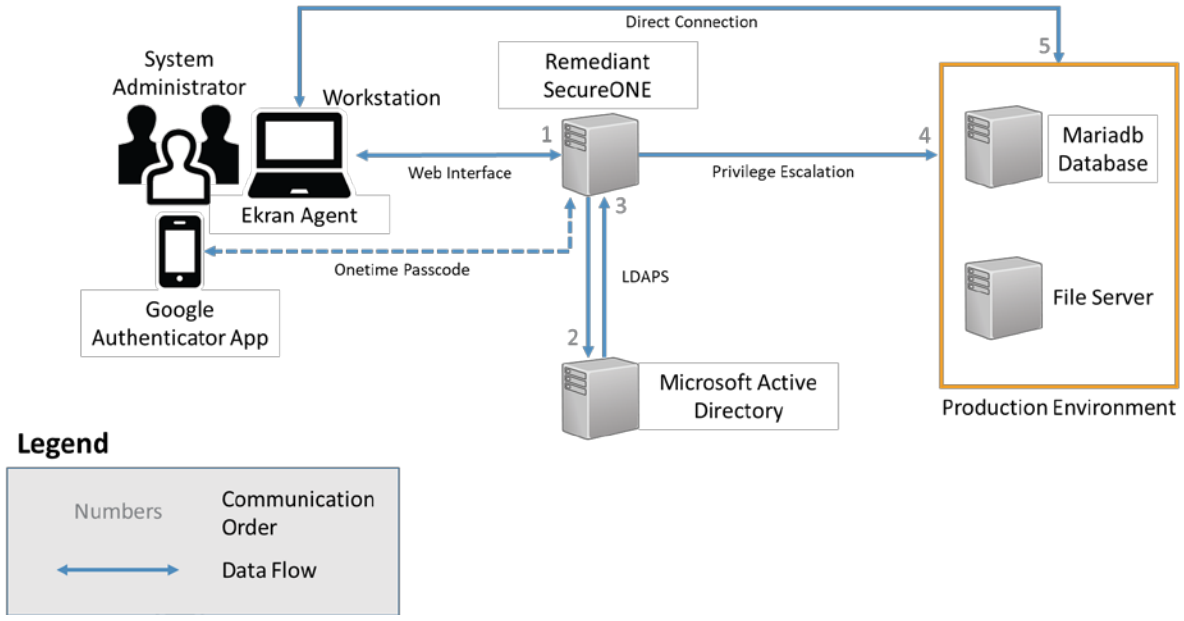
5.2 Example Implementation 2: Organization Infrastructure PAM

Example Implementation 2 was designed and implemented to illustrate PAM for the infrastructure of an organization (e.g., networking devices, servers, workstations, databases, applications). Typical infrastructure users are configuring network devices, updating server operating systems (OSs) and application software, among other tasks. These users are the typical system administrators. In this example, privileged user workstations have additional monitoring to illustrate local-workstation PAM capabilities. Where possible, all data-at-rest and data-in-transit are encrypted.

In Example Implementation 2 (Figure 5-3), the NCCoE utilized the following products to monitor and control privileged user access:

- Remediant SecureONE provides PAM for the organization infrastructure and utilizes Google Authenticator for the MFA second factor for authentication.
- Ekran Agent provides the session monitoring/replay for the privileged user workstations.
- Microsoft Active Directory provides the enterprise privileged-user identity store (source for privileged user identity information).
- Splunk Enterprise provides the security monitoring, logging, and auditing component (SIEM).

Figure 5-3 Example Implementation 2: Organization Infrastructure PAM Architecture



In this example implementation, the Ekran Agent monitors the privileged user's activity on their workstation. A best practice is that privileged users perform their work from dedicated workstations. Those workstations should not be used for nonprivileged user activities like email, web browsing, and

other organizational activities. The Remediant SecureONE server provides the privileged-user-access control interface. The user is authenticated based on their user account information, which is authenticated by the user identity store implemented by using Microsoft Active Directory. In this example implementation, Google Authenticator is used to provide the second authentication factor via mobile Google Authenticator application. SecureONE includes a Google Authenticator server application, but can also be configured to utilize other existing MFA solutions. Once the privileged user authenticates with their username, password, and second authentication factor (a onetime passcode via Google Authenticator), SecureONE completes a temporary (policy-based time limit) user account escalation on the target system to enable that user to perform user activities. Once SecureONE completes the privilege escalation, the user is instructed to connect directly to the target system. When the user completes their activities on the target system, they disconnect or close the session. After the policy-based time limit expires, or if manually requested by the user, SecureONE de-escalates the user account privilege on the target system.

This PAM implementation uses the account escalation PAM technique described in Section 4. In this technique, the target system user account is temporarily escalated to a privileged user status for a policy-based time limit. The target system must be configured to log all of the activity needed to monitor the user activity for normal, privileged, and anomalous activity. The session information is optionally monitored and recorded by the SIEM and the SecureONE server for one or more of the following purposes: security monitoring, forensics, and training. Logs from the target system and SecureONE server are reported to a security monitoring system for detecting anomalous activity. The following list describes the authentication and access-control steps referenced in Figure 5-2:

1. The user connects to the Remediant SecureONE web interface by using their username, password, and Google Authenticator onetime passcode.
2. Remediant authenticates the user by querying Active Directory to check the username and password.
3. Active Directory returns an authentication response.
4. If the user is authenticated, then Remediant SecureONE validates the onetime passcode.
5. Remediant SecureONE confirms that the user is authorized to escalate privileges on the target system.
6. If the user is authorized, then Remediant SecureONE escalates the user's privileges on the user-requested target system for a policy-based time-limited duration.
7. The user directly logs into the requested target by using their username and password.
8. The access is automatically de-escalated after the prespecified period of time, or as manually commanded by the user.

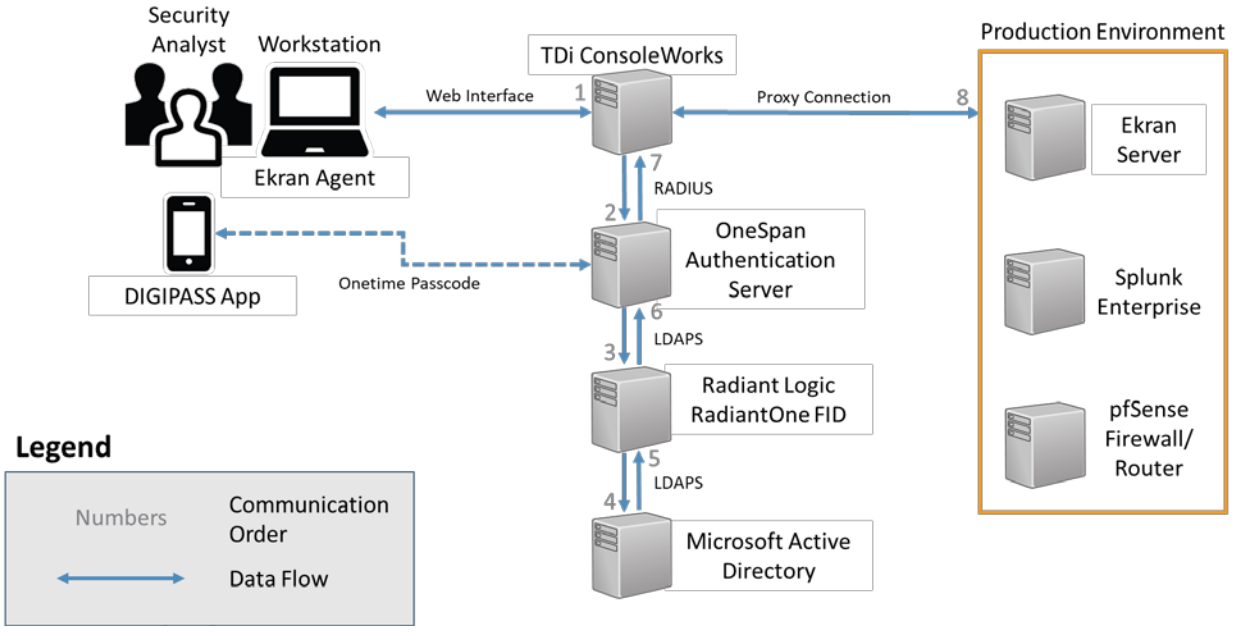
5.3 Example Implementation 3: SIEM

Example Implementation 3 was designed and implemented to illustrate PAM for the SIEM of an organization. The SIEM platform is a critical component of any cybersecurity architecture. The SIEM, provided by Splunk, typically operates and is accessed via the management network within an enterprise. The privileged accounts that are used to access the SIEM are used by the privileged users who perform their work functions on the SIEM. Those functions include administering and operating the SIEM as well as security operations activities. In Example Implementation 3, privileged user workstations have additional monitors to illustrate additional PAM capabilities. Where possible, all data-at-rest and data-in-transit are encrypted.

In Example Implementation 3 (Figure 5-4), the NCCoE utilized the following products to monitor and control privileged user access:

- TDi Consoleworks provides PAM for the security monitoring system.
- Ekran System provides PAM for the privileged user workstations.
- OneSpan (formerly VASCO) Authentication Server provides an interface between the PAM components and the MFA second factor for authentication (via mobile application).
- Radiant Logic RadiantOne FID provides the privileged user identity store.
- Microsoft Active Directory provides the enterprise standard-user identity store (source for privileged user identity information).
- Splunk Enterprise provides the security monitoring, logging, and auditing component.

733 **Figure 5-4 Example Implementation 3: SIEM Architecture**



734

735 In this example implementation, the Ekran Agent monitors the privileged user's activity on their
736 workstation. A best practice is that privileged users perform their work from dedicated workstations.
737 Those workstations should not be used for nonprivileged user activities like email, web browsing, and
738 other organizational activities.

739 The TDi Technologies ConsoleWorks server provides the privileged-user-access control interface. The
740 user is authenticated based on their user account information, which is authenticated via the
741 RadiantOne FID privileged-user identity store. RadiantOne FID forwards the authentication request to
742 the Microsoft Active Directory for an authentication response. Once the privileged user authenticates
743 with their username, password, and second authentication factor (a onetime passcode via a phone
744 application), the user is presented with only their authorized set of target systems. The OneSpan server
745 provides the second-authentication-factor synchronization and authentication. DIGIPASS is the mobile
746 device application providing the user with the second-factor onetime passcode. ConsoleWorks provides
747 the user with proxied access to the target system application.

748 This PAM implementation uses the account sharing PAM technique described in Section 4. In this
749 example implementation, the privileged accounts required to access the SIEM and Ekran management
750 applications are reused by ConsoleWorks. The username and current password are securely stored in
751 ConsoleWorks. In this implementation, we chose not to have the password change after each session.
752 The session information is optionally monitored and recorded by ConsoleWorks for one or more of the
753 following purposes: security, forensics, and training. Logs of the session details are reported to a security

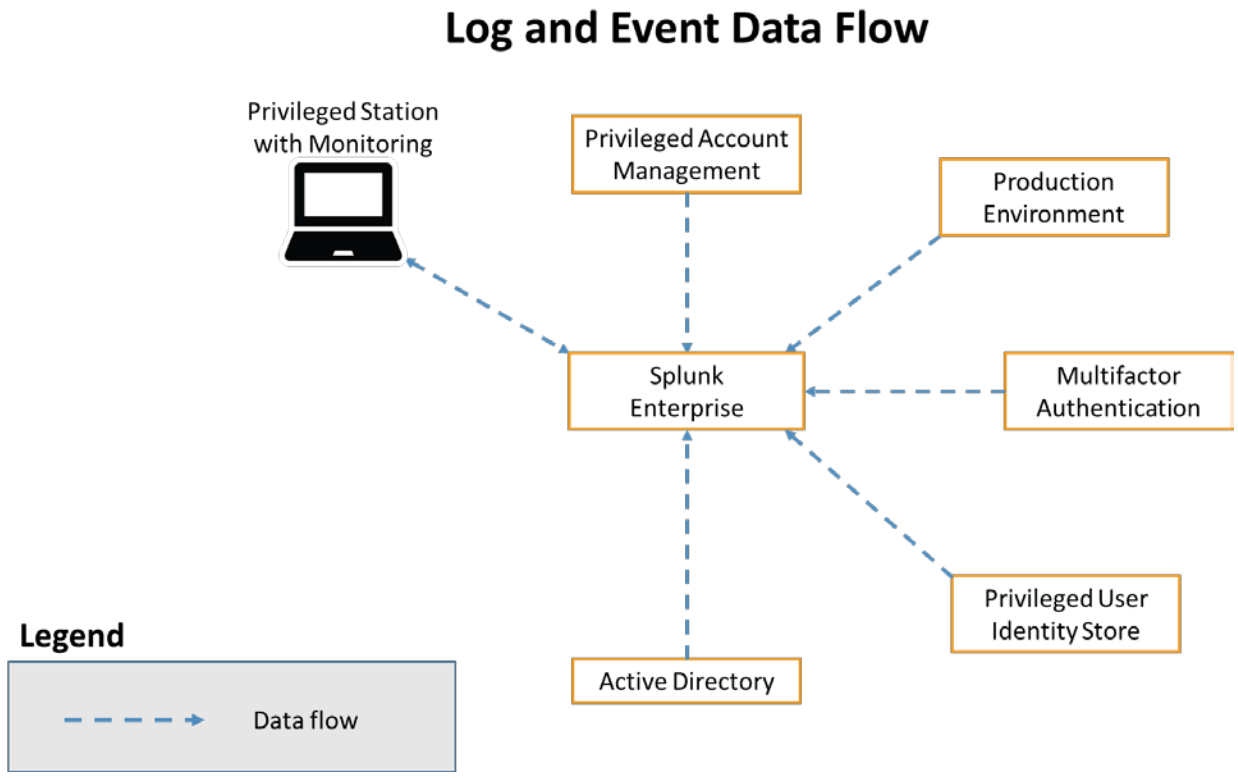
monitoring system for detecting anomalous activity. The following list describes the authentication and access-control steps referenced in Figure 5-3:

1. The user connects to the ConsoleWorks web interface by using their username, password, and OneSpan Authentication Server and DIGIPASS onetime-passcode mobile application.
2. ConsoleWorks authenticates the user by querying the OneSpan server to check the username, password, and onetime passcode.
3. OneSpan passes the username and password authentication query to RadiantOne FID.
4. RadiantOne FID passes the authentication query to Active Directory, which returns an authentication response.
5. RadiantOne FID passes the response from Active Directory to OneSpan.
6. OneSpan passes an allow/deny response to ConsoleWorks, based on the response from RadiantOne FID and the onetime-passcode validation.
7. If authenticated, the user is presented with their authorized target system choices by ConsoleWorks (the choices are based on pre-established policies).
8. After choosing the target system, ConsoleWorks creates a proxied connection to the target system.

5.4 Security Monitoring Implementation

Security monitoring is an important aspect of any cybersecurity implementation. The NCCoE based the security monitoring implementation on the guidance found in the Architecture section of NIST SP 800-92, *Guide to Computer Security Log Management* [9]. The NCCoE implemented the network segmentation recommendation from NIST SP 800-92 in the solutions described above for management/PAM network use by PAM systems for access to the target systems, excluding the application PAM use. The same management/PAM network would also be used to collect logs from each of the target systems and PAM systems. Figure 5-5 illustrates the data flow across the management/PAM network. Where possible, all data-at-rest and data-in-transit are encrypted.

779 **Figure 5-5 Security Monitoring Implementation Architecture**



780

781 ## 5.5 Use Cases

782 ### 5.5.1 Typical Administrator (Directory, Cloud Service, Etc.)

783 From time to time, directories, cloud services, and other systems need to be updated or reconfigured.
784 For example, a new application account may need to be added to support a new or modified
785 application.

786 #### *5.5.1.1 Scenario*

787 A new application (on-premises or in the cloud) is developed that requires a new system account to gain
788 access to an existing database. A directory administrator is assigned to add the account. In this scenario,
789 the administrator may log into the directory by using a shared privileged account. The password may be
790 shared among other accounts or administrators. This change may be reported to a SIEM for monitoring
791 purposes. The report should consist of all of the information necessary to identify the administrator, the
792 time that the change occurred, the account used to make the change, and a description of the change.

In this scenario, without PAM, there is no evidence of who made the change, as shared accounts/passwords are used, and there is no evidence of what actions were taken to create the change. If a mistake was made, then the investigator (probably an administration manager) would have to sift through logs and interview the various administrators to understand who made the change and how it was done. Shared accounts/passwords limit the data available to determine who made a change. If an inadvertent or purposeful incorrect change occurs, then the change may be difficult to remediate because a full description of the user's actions may be difficult to determine.

5.5.1.2 Resolution

The use of a PAM system enables the manager to conclude an investigation without relying on the administrator's memories of the event or sifting through logs. MFA ensures that each PAM user is authorized through strong authentication techniques. Password management ensures that a unique password is used for each system accessed. Password management provides the password to log into each system for each new session and can automatically change the password after each session or other configured aspect. Policy management dictates which systems a user is authorized to access. Session management controls access to the systems that users are authorized to access. Session management logs the user activities in each session and can optionally record each session to allow the manager to review the method or set of commands used to make the change. In addition, session monitoring provides logs of the event to the security monitoring system or SIEM for correlation with other enterprise events. If the SIEM is configured to alert on specific PAM events or combinations of events, then the manager can be proactively notified to review the specific type of changes that are concerning. In that way, a manager can react as needed versus using their time for monitoring.

5.5.1.3 Other Considerations

A PAM system can offer additional controls and protections such as automated discovery and MFA. Automated discovery identifies new privileged accounts immediately after they are created. This function provides an additional layer of monitoring for the enterprise to identify privileged accounts that are created both pre and post implementation of the PAM system.

5.5.2 Security Analyst

The security analyst accesses the system logs as part of a server-outage investigation.

5.5.2.1 Scenario

In response to an incident or alert, a security analyst requires access to the recorded logs associated with the incident or alert. The analyst opens the SIEM to review the incident/alert data and identify the directly and indirectly affected components. Once the components are identified, the analyst must gain access and review the log data for each component. At this time, the analyst may assess the data that generated the alert, including interpolating the data relationships and the order of events. The

assessment includes identifying the users involved, the accounts that they accessed, and the systems involved.

In this scenario, there is no direct evidence of who caused the incident or what set of actions were taken that created the outage. To determine who (if a person is responsible) was involved in the incident, the analyst would have to interview the various administrators to understand who made the change and how it was done. Shared accounts/passwords limit the data available to determine who made a change. If an inadvertent or purposeful incorrect change occurs, then the individual involved may be difficult to identify because a full description of the user's actions may be difficult to determine.

5.5.2.2 Resolution

The use of a PAM system enables the security analyst to conclude an investigation without relying on the administrator's memories of the event, or on sifting through logs if a privileged user is responsible for the alert/incident. PAM systems log the user activities in each session and can optionally record each session to allow the manager to review the method or set of commands used to make the change. In addition, the PAM system provides logs of the event to the security monitoring system or SIEM for correlation with other enterprise events. If the SIEM is configured to alert on particular PAM events or combinations of events, then the manager can be proactively notified to review specific changes that are concerning. In that way, a manager can react as needed versus using their time for monitoring.

5.5.2.3 Other Considerations

PAM systems can also incorporate session recording. The session recording can be useful for determining the most expedient course of action to reverse/remediate the undesirable system changes that caused the incident.

5.5.3 Business-Critical/High-Value Application Access

Social media accounts are high-value applications due to the potential impact of misuse. Other examples of high-value applications are accounts-payable and human-resources systems or any other application that could significantly impact an organization's operations.

5.5.3.1 Scenario

A marketing manager decides to manipulate the organization's brand loyalty by posting a negative report in the company Twitter account. The marketing manager's plan includes using the shared account password to ensure that there is no direct indication of the manager logging into the account. The manager knows that the password has previously been used by at least four other people in the organization. The marketing manager posts the negative report by using the shared account. After the post becomes public, the company posts a retraction and begins an investigation into the negative post. Where does the enterprise look for the chain of events that led to the "mistaken" announcement?

5.5.3.2 Resolution

A PAM system can enable the enterprise to control and manage users of social media accounts. Any approved user can use the PAM system to access the social media accounts. The PAM system can log user activity in each session and can optionally record each session to allow the organization to review the set of commands (including all entries) used to create social media posts. In addition, the PAM system provides logs of the event to the security monitoring system or SIEM for correlation with other enterprise events.

If the organization used a PAM system to manage access to social media accounts, then all activity could be recorded for after-action reporting and forensic investigations. In the scenario described above, the PAM system could have recorded the activity that led to the negative post and could have enabled the organization to quickly identify the rogue employee.

5.5.3.3 Other Considerations

A PAM system can offer additional controls and protections, such as two-person control. Two-person control can enforce review policies that might require a second person (possibly the social media manager) to review all changes prior to posting. This type of control can occur in real time.

6 Security Characteristic Analysis

This section discusses the results of a comprehensive security evaluation of the reference design shown in Figure 4-2. This evaluation focuses on the security of the reference design itself. In addition, it explains the security benefits and drawbacks of the example solutions. The analysis, and the results documented herein, supports the program goals, efforts, and activities necessary to protect, and to achieve compliance with, organizational security requirements for PAM. The security characteristic analysis of the PAM reference design is organized as follows:

- Section 6.4, Analysis of the Reference Design's Support for Cybersecurity Framework Subcategories, analyzes the reference architecture in terms of the specific subcategories of the Cybersecurity Framework that it supports. This section identifies the security benefits of each of the reference design capabilities and discusses how the reference architecture supports specific cybersecurity activities, as specified in terms of Cybersecurity Framework subcategories.
- Section 6.5, Security of the Reference Design, reviews vulnerabilities and attack vectors that the reference design might introduce, as well as ways to mitigate them.
- Section 6.6, Deployment Recommendations, highlights the policies and best practices that an organization may consider when initiating or implementing any part or all of the reference architecture. This section includes references to NIST best practices that may help secure the implementation and the greater infrastructure.

6.1 Assumptions and Limitations

The security characteristic evaluation has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that an organization's infrastructure is hardened against known threats. Security testing of the lab example implementations would not be relevant to those adopting the reference design.

6.2 Build Testing

The purpose of the security characteristic analysis is to examine the extent to which the example solution meets its objective of demonstrating PAM functionality as defined in Section 3.2. In addition, it is intended to explain the security benefits and drawbacks of the reference design.

6.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework subcategories were used to provide structure to the security assessment. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

6.4 Analysis of the Reference Design's Support for Cybersecurity Framework Subcategories

Table 6-1 lists reference design capabilities, their functions, and the addressed subcategories, along with the products that we used to instantiate each capability in the example implementation. The focus of the security evaluation is not on these specific products, but on the Cybersecurity Framework subcategories, because, in theory, any number of commercially available products could be substituted to provide the Cybersecurity Framework support represented by a given reference design capability.

The "Cybersecurity Framework Subcategories" column of Table 6-1 lists the Cybersecurity Framework subcategories that each capability of the reference design supports. The references provide solution validation, listing specific security functions and controls that a solution supporting the desired Cybersecurity Framework would include. Using the Cybersecurity Framework subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports specific security activities and provides structure to our security analysis. The remainder of this

924 subsection describes how the reference design and implemented products support each of the
925 identified Cybersecurity Framework subcategories.

926 **Table 6-1 PAM Reference Design Capabilities and Supported Cybersecurity Framework Subcategories**

Component	Specific Product	Function	Cybersecurity Framework Subcategories
1. Identity Store LDAP	Radiant Logic RadiantOne FID	1. An identity repository specifically reserved for the privileged users of the organization 2. Account change monitoring and reporting	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. **ID.GV-1:** Organizational information security policy is established. **ID.GV-2:** Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. **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.
2. MFA	RSA SecureID Access IdRamp Secure Access combined with Microsoft Authenticator and Azure Active Directory services	3. Add-on MFA capabilities for PAM system user login authentication 4. Logs of each authentication attempt	**PR.AC-1:** Identities and credentials are managed for authorized devices and users.

Component	Specific Product	Function	Cybersecurity Framework Subcategories
	OneSpan (Formerly VASCO) DIGIPASS		
3. User Interface	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE TDi Technologies ConsoleWorks	5. Login authentication and a user-to-PAM-system interactive interface through which users interact to establish work sessions for each system that they administer or access to perform their work functions	N/A
4. Policy Management	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE TDi Technologies ConsoleWorks	6. The enterprise privileged-user access and control policies, such as privileged user sessions, are limited to four hours.	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. **ID.GV-1:** Organizational information security policy is established. **ID.GV-2:** Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. **ID.GV-4:** Governance and risk management processes address cybersecurity risks. **PR.AC-1:** Identities and credentials are managed for authorized devices and users. **PR.AC-4:** Access permissions are managed, incorporating

Component	Specific Product	Function	Cybersecurity Framework Subcategories
			the principles of least privilege and separation of duties.
5. Password Management	Bomgar (formerly Lieberman Software) Red Identity Suite	7. Management and enforcement of the enterprise password policies	**ID.GV-4:** Governance and risk management processes address cybersecurity risks. **PR.AC-1:** Identities and credentials are managed for authorized devices and users.
6. Session Management	Bomgar (formerly Lieberman Software) Red Identity Suite TDi Technologies ConsoleWorks	8. The session start and stop functionality 9. Enforces the enterprise access and control policies within each work session, such as limiting sessions to Secure Shell (SSH) or Remote Desktop Protocol (RDP) or limiting allowed application use on the target system	**PR.AC-1:** Identities and credentials are managed for authorized devices and users. **PR.DS-2:** Data in transit is protected. **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality. **PR.PT-4:** Communications and control networks are protected.
7. Password Vault	Bomgar (formerly Lieberman Software) Red Identity Suite TDi Technologies ConsoleWorks	10. Provides secure storage of the current password for each privileged account managed by the PAM system	**PR.DS-1:** Data at rest is protected.
8. Emergency Access	Bomgar (formerly Lieberman Software) Red Identity Suite	11. PAM use in unpredicted or emergency situations when access to privileged accounts is required by unanticipated	**ID.BE-5:** Resilience requirements to support delivery of critical services are established.

Component	Specific Product	Function	Cybersecurity Framework Subcategories
	Remediant SecureONE TDi Technologies ConsoleWorks	users (privileged or nonprivileged)required by unanticipated users (privileged or nonprivileged)	**ID.GV-1:** Organizational information security policy is established. **ID.GV-2:** Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. **ID.GV-4:** Governance and risk management processes address cybersecurity risks. **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.
9. Automated Account Discovery	Bomgar (formerly Lieberman Software) Red Identity Suite Remediant SecureONE	12. Automated search of the enterprise for evidence and identification of privileged accounts, such as domain administrators or accounts that directly or indirectly (through inheritance of privileges) have privileged-account-level authority	**ID.GV-4:** Governance and risk management processes address cybersecurity risks. **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. **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed.

Component	Specific Product	Function	Cybersecurity Framework Subcategories
10. Session Monitoring	Ekran System Client TDi Technologies ConsoleWorks	13. A mechanism to identify, log, and alert on anomalous privileged-account activity	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events.
11. Session Replay	Ekran System Client TDi Technologies ConsoleWorks	14. Session review for training and event review and investigations	**RS.AN-3:** Forensics are performed.
12. Security Monitoring	Splunk Enterprise Radiant Logic RadiantOne FID	15. Logging and auditing provide log storage, analysis, and alerting components	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods. **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors. **DE.AE-5:** Incident alert thresholds are established. **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events. **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed. **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. **RS.CO-2:** Events are reported consistent with established criteria.
13. Lab Environment	Miscellaneous	16. Virtual machines, networking, routing, firewalls, etc.	**PR.AC-5:** Network integrity is protected, incorporating

Component	Specific Product	Function	Cybersecurity Framework Subcategories
			network segregation where appropriate. **PR.DS-5:** Protections against data leaks are implemented.

Note: Table 6-1 describes only the product capabilities and the Cybersecurity Framework subcategory support that the reference architecture addresses. Many of the products have additional security capabilities that are not listed in this table.

6.4.1 Supported Cybersecurity Framework Subcategories

The reference design is created to identify a set of capabilities and their relationship to provide a PAM solution. These capabilities ensure that privileged accounts are protected from potential cyber attacks and breaches. The Cybersecurity Framework (i.e., functions, categories, and subcategories) defines the capabilities and processes needed to implement a cybersecurity program. Within this practice guide (Table 3-1), the NCCoE has identified the Cybersecurity Framework subcategory capabilities and processes that are desirable to implement a PAM solution. In the following subsections, we review how the PAM reference design addresses the Cybersecurity Framework subcategories included in Table 3-1 with technical capabilities. The following subsections also include the Cybersecurity Framework subcategory processes from Table 3-1 that are beyond the scope of the PAM solution, but important for organizations to address. Some Cybersecurity Framework subcategories are supported by individual components of the reference design, and other subcategories are supported by the reference design as a whole. Still, other Cybersecurity Framework subcategories are relevant as long as the reference design is predicated upon them being addressed by the enterprise-wide security architecture, policies, and programs.

6.4.1.1 ID.AM-3: Organizational Communication and Data Flows Are Mapped

All communication paths, flows of data, directories, and connectivity between the directories and other components that are within the reference design are clearly defined and identified. This supports the ability to determine and control information flows, data sources, where the data is stored, who is responsible for the data, and who is authorized to access the data throughout the organization. It also allows policy administrators and managers to conduct risk assessments when data or the flow of data is modified. In addition, the reference design ensures that all resources are properly classified and mapped according to the needs of the organization. The reference design can support Cybersecurity Framework Subcategory ID.AM-3 with respect to managing data flows associated with the use of privileged accounts and the authentication of privileged users.

6.4.1.2 ID.AM-6: Cybersecurity Roles and Responsibilities for the Entire Workforce and Third-Party Stakeholders Are Established

The reference design is predicated on there being a clearly defined set of roles and responsibilities for each privileged user that determines that user's required access. The organization's policy administrators define the roles and responsibilities of the privileged users within the workforce and describe these roles and responsibilities in terms of authorized privileged account use (and at what level). Once these roles and responsibilities have been established and described within the reference design, the design then serves as the mechanism for enforcing the privileged-access-control-related aspects of these roles and responsibilities. The policy management, user interface, and session management capabilities enforce policies for privileged users and ensure access-policy compliance.

6.4.1.3 ID.BE-5: Resilience Requirements to Support Delivery of Critical Services Are Established

The reference design supports resilience by identifying system capabilities and processes that maintain the functionality of the design in degraded environments, including emergency access, security monitoring, detecting and preventing malicious activity, generating alerts and sending incident notifications, etc. Emergency access allows the use of the PAM system in unpredicted or emergency situations when access to privileged accounts is required by unanticipated users (privileged or nonprivileged). These capabilities support the resilience requirements to deliver critical services for most operating states (e.g., under duress/attack, during recovery, during normal operations).

6.4.1.4 ID.GV-1: Organizational Cybersecurity Policy Is Established and Communicated

Policy administrators and managers are responsible for establishing policy requirements for privileged accounts and for the interactions between these accounts and their users. The reference design has implemented policy enforcement and automated account discovery capabilities to support best practices, processes, and structures that ensure privileged access policy compliance. It also ensures the flow of information to all components to prevent and detect any unauthorized access.

6.4.1.5 ID.GV-2: Cybersecurity Roles and Responsibilities Are Coordinated and Aligned with Internal Roles and External Partners

The reference design is predicated on there being a clearly defined set of roles and responsibilities for each privileged user that determines that user's required access. It is expected that roles and responsibilities are established within the organization's information security policies, procedures, standards, or guidelines for internal employees and contractors. This determines the level of responsibilities or the functions that are assigned to an individual (including contractors) and at what level of privilege they are assigned. Within the reference design, this is supported by the policy management, user interface, and automated account discovery components, which ensure that privileged users are authorized to perform privileged functions based on their roles and responsibilities and that any attempts to bypass those roles are detected. It is important that the policy requirements are communicated to all employees. Organizations adopting the reference design may ensure that contractors clearly understand their roles and responsibilities as defined by the organization.

6.4.1.6 ID.GV-4: Governance and Risk Management Processes Address Cybersecurity Risks

Senior management is responsible for the organization's risk assessment processes. An organization's risk management program should include strategies that ensure that risks are identified, registered, and mitigated. The reference design is based on a risk assessment in Section 3.4. The reference design capabilities support the risk analysis, risk response/mitigation, and risk monitoring process that address the cyber risk factors that privileged accounts represent.

6.4.1.7 PR.AC-1: Identities and Credentials Are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes

Organizations establish privileged-account access control policies to ensure that privileged account use is limited to authorized personnel, least privilege is implemented, and separation of duties is maintained. Access control policies determine the authentication method and authorization processes, roles, and responsibilities of the users. The privileged identity store capability deployed within the reference design provides a unique repository for privileged users' identities and credentials. This is fundamental to the reference design to segregate the privileged-user community and account information from the production components of the organization. This Cybersecurity Framework element primarily considers the implementation of privileged access controls via the account sharing technique.

6.4.1.8 PR.AC-4: Access Permissions and Authorizations Are Managed, Incorporating the Principles of Least Privilege and Separation of Duties

A key strength of the reference design is the ability to enforce policies for privileged accounts, including the principles of least privilege and separation of duties. By enforcing these principles, the reference design allows limiting unauthorized access to data and systems.

The policy management capability is the repository for approved-use policies for use by the session management and user interface capabilities. The session management capability enforces the access policies. The session management and password capabilities ensure the control of privileged sessions and of usage of the password vault, through request and approval workflows and (optionally) time-bound access. Automated account discovery is an important consideration as well, as that functionality will detect any attempts to bypass or ignore the principles of least privilege and separation of duties. All privileged user activities in the reference design are logged and sent to the monitoring component for further analysis. Policy administrators and managers are responsible for setting up, making changes to, and managing, all privileged accounts and functions. This Cybersecurity Framework element primarily considers the implementation of privileged access controls via the account escalation technique.

6.4.1.9 PR.AC-5: Network Integrity Is Protected (e.g., Network Segregation, Network Segmentation)

Network segmentation is a key function of this reference design. Segregating the PAM system from the production network reduces the risk of session information interception and exposure of privileged account information to nonprivileged users and systems, and reduces the risk of being negatively impacted from malware or an exploit. The PAM system was implemented on a management network to accomplish the network segmentation. Using firewalls and routers to segregate the zones also limits the risk to the enterprise, should a vulnerability be exploited within the production network.

6.4.1.10 PR.DS-1: Data at Rest Is Protected

Privileged user account information is not encrypted while stored at rest. However, this data is limited to the privileged user identity store within the reference design and is situated in its own security enclave or subnetwork. The security enclave consists of the physical directory only, without any other reference design components, and is separated from the rest of the reference design by a firewall.

Furthermore, although this information is not encrypted while at rest, its integrity is monitored by the security monitoring capability. The security monitoring capability receives logs of privileged account information changes from the privileged user identity store and from the underlying enterprise-wide identity store and PAM activity log. The monitoring capability correlates and compares the log information that it receives from each of the components, to ensure that the information is consistent across all sources. In this way, it is possible to verify that each change made to the privileged identity store and/or enterprise-wide identity store is the result of an authorized change by an authorized

privileged user or system. If a change to an identity store is detected and cannot be correlated with logs from other components, then the system generates an alert to signal that this change might be unauthorized. File integrity tools are available to monitor for the loss of event integrity within systems like an identity store. These tools are not addressed in the reference design.

6.4.1.11 PR.DS-2: Data in Transit Is Protected

Privileged user access information is encrypted while it is in transit within the reference design components, where possible. In the example implementation, multiple applications are used to implement the policy management and user interface (access control) components over secure protocols (e.g., Transport Layer Security [TLS]) so that all information that flows between the components is not transmitted over a network where it would be vulnerable to eavesdropping or tampering. If the reference design were built using separate physical components to instantiate the policy management and user interface components, then messages exchanged among these components would need to be provided with at least data integrity, and preferably confidentiality, protections.

In the current example implementation (Request for Comments 2830), LDAP over SSL [Secure Sockets Layer] (LDAPS) is used to perform read-and-write access to the identity store component, ensuring that privileged user account information sent across a network to these other components is encrypted. Also, when log information is sent to the monitoring component, it is encrypted, resulting in protection from disclosure and from unauthorized modification.

6.4.1.12 PR.DS-5: Protections Against Data Leaks Are Implemented

The reference design itself, through its focus on managing access permissions, protects the enterprise in general against data leaks that might occur. By preventing unauthorized access to information, the reference design protects against leaks of that information. The reference design, however, is not intended to protect against the exfiltration of information by an authorized user; such an insider threat is not addressed. The fact that data flows within the reference design are encrypted serves to ensure that, even if data-in-transit within the reference design was exfiltrated, this information would not be in plaintext form. For example, administrators may have access to administration and configuration directories, but not to directories that contain sensitive data files. The reference design allows logging all privileged user access, ensuring that, if a privileged user misuses their privileges and leaks data, this activity would be recorded in log files and would generate alerts.

Within the reference design, a management network is implemented to segment network access and can increase the effort needed to exfiltrate data. Automated account discovery is an important consideration as well, as that functionality will detect any attempts to bypass these other protections in an attempt to leak data by using privileged access.

6.4.1.13 PR.PT-1: Audit/Log Records Are Determined, Documented, Implemented, and Reviewed in Accordance with Policy

The reference design ensures the real-time monitoring of privileged sessions and optionally can record every session for a detailed audit trail in accordance with requirements defined by an organization's policies and compliance requirements. The security monitoring capability ensures that all session activity and access-related change activity can be centrally logged, tracked, and managed. All relevant information (e.g., about, what, when, who) at each design component is monitored and logged. The design leverages automation to collect, protect, and analyze logs; produce log-based reports; and retain log data to support investigations. Given that access to the logs in the monitoring capability would enable an adversary to delete or modify logs that document adversarial activity, the ability to delete or modify such logs should, by policy, require the cooperation of multiple individuals.

6.4.1.14 PR.PT-3: Access to Systems and Assets Is Controlled, Incorporating the Principle of Least Functionality

Please refer to Section 6.4.1.8 for an explanation of the how the reference design supports this Cybersecurity Framework subcategory.

6.4.1.15 PR.PT-4: Communications and Control Networks Are Protected

Please refer to Section 6.4.1.9, Section 6.4.1.11, and Section 6.4.1.12 for an explanation of the how the reference design supports this Cybersecurity Framework subcategory.

6.4.1.16 DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods

The reference design provides comprehensive-log and advanced-threat analytics to detect malicious activity that is near-real-time, accurate, comprehensive, and scalable. These capabilities include analyzing logs from the PAM system capabilities and related activities of privileged accounts. Comprehensive logs and advanced threat analytics allows analysts and administrators to detect and correlate anomalous events in a timely, structured, and constant way. Unauthorized operation/activity attempts are detected and analyzed through these capabilities. They also automate the processes required to understand suspicious privileged-account access or use attempts.

6.4.1.17 DE.AE-3: Event Data Are Collected and Correlated from Multiple Sources and Sensors

The security monitoring capability provides real-time monitoring and aggregates and correlates privileged-account or privileged-user logs from the following sources:

- user interface (access control)
- password vault
- identity store (LDAP)

- automated account discovery
- emergency access
- session management

6.4.1.18 DE.AE-5: Incident Alert Thresholds Are Established

The alert thresholds are binary. If the user-access information logs that the security monitoring capability receives from each of its sources are not consistent with each other, then an alert is generated. If the user-access information logs received from the various components are consistent with one another, then no alert will be generated, but the information will be logged. The reference design provides capabilities to define thresholds and to log and audit user access information within each directory that is consistent with established policies. All incidents and events in the reference design are clearly communicated. Policy managers define and categorize the incident reporting process (e.g., a user logging into an account, a web server receiving a request for a specific web page, a user accessing files on network share, a firewall blocking a connection attempt). For additional information, please refer to NIST SP 800-61, *Computer Security Incident Handling Guide* [15].

In addition, the monitoring capability of the reference design ensures that logs received from any privileged operation are consistent with each another. If any inconsistences in the logs are detected, then an alert is generated based on the threshold defined by policy managers. This analysis may help identify unauthorized access attempts and can be supplemented to detect some Kerberos-based attacks.

6.4.1.19 DE.CM-3: Personnel Activity Is Monitored to Detect Potential Cybersecurity Events

All activity associated with privileged accounts in the reference design is monitored on a continuous basis. This includes all activity that administrators, policy administrators, and other privileged users perform. It also includes alerts when an anomalous activity of an individual is detected. User-interface and session monitoring allow configuring and recording proxy-level sessions. The logs are forwarded to the monitoring components. For example, a malicious insider or malware attempting (successful or not) to access an asset outside defined policies can be detected. Additionally, these capabilities can create an unalterable audit trail of privileged account activity; improve incident response times; and provide a rich data set from which to understand how, when, and why a security incident occurred.

6.4.1.20 DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software Is Performed

The reference design continuously monitors all unauthorized activity and access to restricted resources and generates alerts when a potential incident or event is detected. The user interface (access control) and configuration components also allow configuring and recording proxy-level sessions. This ensures the tracking and detection of suspicious activities of individuals associated with a privileged account or system (including the secret mounting of unauthorized drives or devices). The logs are forwarded to the monitoring components (SIEM) for proper notification. Automated account discovery is an important consideration as well, as that functionality will detect any attempts to disable protections against unauthorized access.

6.4.1.21 RS.CO-2: Incidents Are Reported Consistent with Established Criteria

The reference design provides the ability to collect logs from multiple sources. Any security incidents associated with unauthorized account activity that are consistent with established policies will be detected and reported (see Section 6.4.1.22 for more details). It is important to develop a structured incident response program by implementing incident response strategies that can detect and resolve security incidents. An effective incident response program should include the following stages:

- incident response process
- incident investigation life cycle
- incident remediation
- incident response

6.4.1.22 RS.AN-3: Forensics Are Performed

The reference design incorporates monitoring capabilities for complete visibility and control and consolidates identity across all privileged systems, which improves reporting and reduces the audit time as well as forensics investigations. This allows all privileged sessions and privileged user activities to be recorded. The recording provides details on the user and their activities. This creates accountability to support forensic investigations, troubleshoot system failures, and audit reports. For additional information, please refer to NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* [16].

6.5 Security of the Reference Design

The purpose of the security characteristic analysis is to understand the extent to which the use case meets its objective of demonstrating PAM. In addition, the analysis seeks to understand the security benefits and drawbacks of the reference design. The list of reference design capabilities in Table 3-1

focuses on the capabilities needed to ensure the integrity of system data and to manage and secure the reference design. To this end, this section focuses on the security of the reference design itself.

The following measures were implemented to protect the reference design from outside attack:

- installed an MFA system to provide an additional layer of security
- installed session management capabilities to track and manage all privileged user sessions, integrated with the password manager
- installed policy management
- installed a management network to isolate log and PAM-system traffic from the production (business operations) networks
- limited the use of, and access to, privileged accounts
- monitored identity stores to detect unapproved insertion, modification, or deletion
- monitored individual endpoints to detect unapproved privileged access allocation
- recorded and logged all privileged-account use and access activities
- used encryption and integrity protection of identity-store-access and system logs while this information was in transit

The security evaluation focuses on the capabilities, rather than the products. The NCCoE is not assessing or certifying the security of the products included in the example implementations. We assume that an organization already deploys network security, such as firewalls and intrusion detection devices, that are configured using best practices. The focus of this section is securing capabilities introduced by the reference design and minimizing their exposure to threats. The list in Table 3-2 also includes capabilities for managing and securing the PAM reference design.

6.5.1 Securing New Attack Surfaces

The reference design introduces new capabilities into an organization, and with any new capability comes the potential for new attack surfaces. Hence, it is imperative that reference design capabilities and their contents be secured to minimize their potential to introduce new vulnerabilities into the enterprise. The threat landscape is dynamic. Therefore, maintaining the security of the reference design requires establishing and maintaining privileged account control and control of security events from multiple sources, while being responsive to perceived threats and malicious activities. However, if an organization deploys the reference design, then the organization will also have additional capabilities that must be safeguarded—namely, the policy management, user interface (access control), session management, password vault, monitoring, and emergency access. Each capability must be protected from unauthorized access so that the information that they contain is safeguarded from unauthorized modification. One method that assists with this protection is automated account discovery, as that function detects attempts to bypass or otherwise defeat existing information security protections.

Points of entry. The user interface provides the primary point of entry for a PAM system. Therefore, the protection of the user interface and authentication method for PAM users is critically important. The reference design addresses the user authentication by implementing MFA to reduce the chance of a successful impersonation of an authorized PAM user. The user interface system must be protected within the organization by limiting access to the underlying support systems (e.g., OS, physical hardware). A successful attack on the user interface system could allow an attacker to compromise any of the PAM system capabilities. For example, if an adversary could compromise the policy management, password vault, or user interface (access control) capabilities, then the attacker would be able to access the PAM system for unauthorized use. Inappropriate or unauthorized use of these capabilities could change the authorization levels for anyone in the enterprise.

Disabling monitoring. Continuous monitoring is critical to detect anomalous system changes or activities. The monitoring capability must be protected from physical and logical access. Example Implementation 3 provides an example of logical access control for the monitoring capability. Further, automated account discovery is an important consideration to protect the fidelity of the monitoring and to ensure that no attempts to bypass, redirect, or disable the continuous monitoring facility have been made.

Sabotaging detection. Unauthorized access to the PAM user interface, password vault, and security monitoring capabilities must be prevented because of the value of the information that they maintain and store. The monitoring capability forms the locus of the reference design's analytic capabilities for detecting access control security events. The aggregation of privileged-account information and logs in the monitoring capability provides enormous potential in terms of anomaly detection. If an adversary could access the password vault and the monitoring capabilities to modify or delete information or to alter the rules used to analyze information, then the ability to monitor and detect access control anomalies could be severely impaired. The example solution illustrates one of the techniques for protecting the PAM and security monitoring capability through a network segmentation technique. With network segmentation, attackers are required to identify the management network, and to cross over the network boundaries undetected, before unauthorized access to the PAM system and security monitoring capabilities can be achieved. Network segmentation is an important defense-in-depth tactic.

Safeguarding the enterprise. The following sections discuss mechanisms that are used to secure these reference design capabilities and to safeguard user access and policy information. In all cases, restricting logical and physical access to these capabilities is key to protecting them. Standard users are never given accounts on, or given authorization to access, any reference design capabilities. Each reference design capability should permit access by only one or two privileged users who have the authority and responsibility to administer that (and only that) reference design capability, or, by policy, the cooperation of multiple individuals should be required to access any single reference design capability, thereby decreasing the probability that any capability could be subverted by a single inside adversary. No administrative users should reuse the same workstation or administrative activities account that they use for other business use, such as email, word processing, or other business applications.

Furthermore, access to the consoles/management interfaces of the machines and applications on which the reference design capabilities reside must be protected. The PAM implementation can be used to administer portions of the implementation, or another PAM system might be considered to administer the primary PAM system, based on the needs and risk management decisions of the organization. Any passwords needed for PAM system administration should be stored separately in a manner consistent with the organization's risk management decisions. This helps ensure that all access to any reference design capability must be performed via the PAM (rather than directly via the machine console) or in another secure manner.

6.5.2 Securing Access to the LDAP Directory

The identity store (LDAP) is the authoritative source for privileged account information. The security of the identity store can be maximized by ensuring that direct connection to consoles of the machines on which these capabilities reside is physically secured and that console passwords are secure according to organization risk management decisions. This approach will minimize the possibility that any reference design machine could be accessed directly, rather than via the PAM. In addition, the reference design implements the MFA capability to ensure that all privileged access requests can be authenticated using a strong method.

6.5.3 Securing Access to the Policy Management Capability

The ability to create and modify privileged account policies within the policy management capability must also be carefully controlled. By policy, workflows should be established to ensure that no single administrator can create or modify policies in isolation. Workflows based on the principles of least privilege and separation of duties should be defined to ensure that multiple administrators and/or multiple administrative approvals are received before updates are performed. It should not be possible to submit policies that have not been properly vetted and approved by using an approved workflow.

6.5.4 Securing Access to the User Interface (Access Control) Capability

The user interface capability provides login authentication and an interactive interface through which users interact to establish work sessions for each target system that they administer or access to perform their privileged functions. This establishes the single entry point into the reference design. The reference design should not accept direct input from any source other than the user interface (or an associated and equally well-authenticated application programming interface [API]). The identity store and MFA capabilities provide additional layers of security to ensure the use of a strong authentication method.

6.5.5 Securing Password Vault Capability

The password vault capability of the reference design stores and manages all passwords for every privileged user, according to the account sharing technique. Because the vault stores sensitive data, it becomes a target for attackers. Therefore, it is critical to protect the password vault from unauthorized access. Access to the password vault should require two-person control to increase the resistance to a single malicious actor acting independently. MFA should also be incorporated to further increase the resistance to an attack that is performed via the impersonation of an authorized user.

6.5.6 Securing Emergency Access Capability

The emergency access capability provides additional privileged account access to the PAM components when normal access control to the password vault is broken down or when outages and failure happen in the enterprise infrastructure. This may be the only access point to restore the PAM system to normal operation or to use the PAM system when the unanticipated or unauthorized personnel require access to privileged accounts. For example, if privileged users are locked out of the password vault, then the senior administrator can log into the password vault and get the credentials for the privileged users in all cases, even if (for example) the LDAP infrastructure is down and no one can log into the PAM system in the usual manner. Policy administrators and managers may write down and store the emergency access passwords in a physical vault. In such cases, the physical vault is placed in a secure location with limited access.

6.5.7 Securing Access to the Security Monitoring and Analytics Capability

The security monitoring capability, which provides complete management and visibility within the reference design, collects and tracks all privileged user activity in real time. Therefore, if an adversary could modify the contents of the monitoring capability without detection, then that would negatively impact the ability of the reference design to monitor all privileged account changes. By policy, only security analysts, whose role is to be notified of alerts and to examine the logs pertinent to those alerts to determine if there is a genuine security event, should be able to view logs, and the logs should be accessible only via read-only access. Workflows based on the principles of least privilege and separation of duties should be defined to ensure that multiple administrators and/or multiple administrative approvals are received before any changes to the monitoring analytics are performed. It should not be possible to create or modify analytics that have not been properly vetted and approved. Example Implementation 3 illustrates one approach to secure a security monitoring capability.

6.5.8 Ensuring Information Integrity

Within the reference design, multiple capabilities have been implemented to prevent unauthorized modification or deletion of access policies, privileged account information, and analytics information stored in these capabilities. In addition to preventing access to information while it is stored in these

capabilities, the information must be protected from modification while it is in transit between reference design capabilities. If privileged accounts or policy information were to be deleted, modified, or falsified while in transit between capabilities, then the result would be a loss of confidence in the access authorization and authentication of users. It is essential that the user-access and policy information have integrity protection, and ideally confidentiality protection, when in transit between capabilities. Securing communications among all capabilities is essential to securing the reference design. To provide this protection, all information sent to and from LDAP is encrypted using the TLS protocol.

All logs sent within the reference design are encrypted in transit to ensure confidentiality and integrity from the reference design capability to the monitoring capability. Once the log file is transmitted to the monitoring capability, it is stored in the clear (i.e., in plaintext form), where it would be vulnerable to modification or deletion if an adversary were able to gain unauthorized access to the monitoring capability.

6.5.9 Protecting Privileged Accounts

In any organization that adopts the reference design, we would expect there to be several classes of privileged users who are authorized to access reference design capabilities or the machines on which they are running, for administering those capabilities and machines. It is important to limit privileged users and accounts by enforcing the principle of least-privilege access controls. The reference design implements the automatic account discovery capability, which ensures the detection of all privileged account changes within the privileged identity store and of the assets administered or otherwise accessed by using privileged accounts.

6.5.10 Preventing Insider Threats

Insider threats are difficult to detect. The attacks perpetuated by insiders, and the consequences resulting from such attacks, can be very costly. The reference design supports the principles of least privilege and separation of duties. These principles restrict privileged users to only those resources to which their role gives them access, and limit privileged users in what they are authorized to do with those resources. The implementation of these policies does not prevent inside attacks; however, it can reduce the scope of the damage that an insider can cause. The privileged account identity store and MFA capabilities in the reference design prevent an unauthorized user from using privileged accounts. These measures ensure that the reference design itself is secure from any nonprivileged user insider threat. Any organization adopting the reference design should ensure the integration of these protective mechanisms and other solutions that it may see fit in its implementation against insider threats.

6.5.11 Addressing Attacks

The specific challenge of the reference design is the abuse of privileged account credentials. Once these accounts are compromised, an adversary can create additional accounts to avoid detection, escalate their privileges, and disrupt critical services. To address these and other related challenges in a comprehensive way, we used the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) model and framework developed by The MITRE Corporation, to identify the following adversary tactics and techniques against which the reference design protects:

- Privilege escalation and credential access result when an adversary obtains or modifies a higher level of permissions on a system or network than they are authorized to have.
  - An adversary employing the tactic of privilege escalation might use the technique to modify their privilege information attributes that are stored in LDAP, so that these attributes permit the adversary to have more access authority than entitled. In this attack technique, the adversary tries to circumvent the principle of least privilege. The reference design protects against circumventing the principle of least privilege, through MFA, password managers, session management, automated account discovery, logging, and security monitoring, which enables it to detect changes in privileged account information that is stored in LDAP.
  - Alternatively, an adversary attempting to abuse privileges could use the technique of creating a secret account in one of the enterprise's directories and giving that new account the desired higher level of privilege for malicious purposes. This means that the adversary is not using the PAM user interface. The monitoring and logging system is designed to detect and generate an alert when an unauthorized new account is created.
  - Similarly, an adversary could create a local account (outside the scope of the enterprise directory) and grant it privileged access. The unauthorized new account will be detected only if the automated account discovery capability has been deployed and includes in its scan scope such local accounts.
  - Credential access results when an adversary obtains unauthorized privileged access to enterprise resources or when an adversary modifies credential information in unapproved ways. An adversary employing the tactic of privileged credential access abuse could use the technique of trying to obtain legitimate privileged user credentials that belong to another user by eavesdropping on these credentials as they are sent to and from directories in the network. The reference design protects against such privileged credential access abuse through its use of LDAPS (SSL-based encrypted traffic between LDAP servers and clients) and MFA, which prevents the network sniffing of another privileged user's credentials. Further, use of the account escalation (rather than account sharing) design pattern can mitigate the risk of credential access by minimizing the value of stolen credentials.

6.5.12 User Behavior Analytics

UBA tracks a system's user and their interactions with the system, rather than security events or devices. UBA solutions detect behaviors of concern by combining all relevant data (e.g., network and client/host-based activity, human resource systems, employee reports, public records, travel records) and then looking for meaningful patterns of behavior. UBA offers the potential for organizations to improve their security posture by detecting that an attack—such as a privilege escalation attack—has been launched or is to be imminently launched, allowing the organization to take preventive, corrective, and investigative action as appropriate. Detection ideally occurs during the early formative stages of an attack or before the technical implementation of an attack has been launched, but can also extend until after the primary phase of an attack has been launched.

Various analytic approaches exist that UBA solutions can leverage to detect privilege escalation attacks, including static event and threshold analysis, whereby specific patterns of network and client activity are deemed to signify behaviors of concern. Other approaches include anomaly detection that identifies an attack based on deviations from a baseline at the organizational, job-role, or individual-employee level. These baselines can be generated with or without machine learning algorithms, though the level of computational power required increases with system complexity.

For this build, a UBA capability was not implemented. The low volume of user, client, and network data transmitted across the example implementations would have been insufficient for a UBA capability to meaningfully identify patterns or develop a baseline. Furthermore, the selection of a UBA should be tailored to the business operations and technical infrastructure of an organization. Our test build did not have the wider set of system operations and connectivity to adequately simulate a financial institution.

Nonetheless, there are some UBA considerations that will be consistent across financial institutions that wish to select a UBA capability as part of the defense against privilege escalation attacks and other forms of cyber attacks. Organizations should consider the following issues when contemplating adding UBA to their security architecture:

- Can the UBA detect or enable other types of attacks? Privilege escalation attacks are only one attack of many that financial organizations face. Organizations may consider UBA for the detection of alternative avenues of attack or for obscuring alternative types of attack from detection.
- Organizations should consider how UBA can most effectively and efficiently add to the situational awareness that a privilege escalation attack (or any attack) is underway. Good situational awareness can involve a combination of notifications, visualizations, administration and automated system actions, and business processes that are regularly drilled, trained, evaluated, and based on best practices from the fields of behavioral sciences and human factors. Failure to act quickly—whether through prevention, mitigation, or investigation—can generate significant reputational, financial, productivity, legal, and cultural risks that UBA solutions would be unable to remedy.

6.6 Deployment Recommendations

When deploying the reference design in an operational environment, organizations should follow security best practices to address potential vulnerabilities and to ensure that all assumptions upon which the solution relies are valid, to minimize any risk to the production network. Organizations leveraging the reference design should adhere to the recommended best practices that are designed to reduce risk (see the subsections below). Please note that the example implementations of the reference design did not implement every security recommendation. Organizations should not consider this list of recommended best practices to be comprehensive; merely following this list will not guarantee a secure environment. Planning for the deployment of the design gives an organization the opportunity to go back and audit the privileged account information in their directories and get a more global, correlated, disambiguated view of the user access roles and attributes.

6.6.1 Patch, Harden, Scan, and Test

Vulnerability assessment programs establish controls and processes to help identify weaknesses within the organization's information system components, which could be exploited by attackers to gain unauthorized access, to disrupt business operations, and to steal or leak sensitive data. The vulnerability assessment focuses on identifying controls and processes that will provide appropriate protection against threats that could adversely affect the security of the information system or data entrusted on the information system. The controls implemented need to be consistent with established policy requirements to secure against known vulnerabilities in OSs and application software. The following activities provide additional steps to the IT infrastructure:

- Keep OSs up-to-date by patching, version control, and monitoring indicators of compromise (e.g., performing virus and malware detection, keeping antivirus signatures up-to-date).
- Harden all capabilities by deploying on securely configured OSs that use long and complex passwords and are configured per best practices. Built-in accounts with privileged access rights should be disabled or closely monitored.
- Scan OSs for vulnerabilities and unexpected changes in privileged access.
- Test individual capabilities to ensure that they provide the expected Cybersecurity Framework subcategory support and that they do not introduce unintended vulnerabilities.
- Evaluate reference design implementations before going operational with them.

It is also recommended that additional network security strategies are implemented that utilize secure protocols and processes. However unlikely a targeted attack is for the reference design, the most potent area of risk remains from within the network itself. Pushing audit log capabilities beyond system log (syslog) and auditing services into a security monitoring platform increases the likelihood that exploited trust relationships would be detected quickly. Such deployments would support a defense-in-depth strategy and assist in transitioning the reference design toward a more resilient state. Specifically, check

external accounting logs, external syslog logs, booting information (periodically) for information about the last time that the firewall was reloaded, and the configuration checksum (on a regular basis), and periodically verify the integrity of other software loaded on the firewall.

6.6.2 Other Security Best Practices

- Install, configure, and use each capability of the reference design per the security guidance provided by the capability vendor.
- Change the default password when installing software.
- Identify and understand which predefined administrative and other accounts each capability comes with by default, to eliminate any inadvertent backdoors into these capabilities. Disable all unnecessary predefined accounts, and, even though they are disabled, change the default passwords in case a future patch enables these accounts.
- Segregate reference design capabilities on their own subnetwork, separate from the production network, either physically or by using virtual private networks and port-based authentication or similar mechanisms.
- Protect the various reference design subnetworks from each other and from the production network by using security capabilities, such as firewalls and intrusion detection devices, that are configured per best practices.
- Configure firewalls to limit connections between the reference design network and the production network, except for the connections needed to support required internetwork communications to specific internet protocol (IP) address and port combinations in certain directions.
- Configure and verify firewall configurations to ensure that data transmission to and from reference design capabilities is limited to interactions that are needed. Restrict all permitted communications to specific protocols and IP address and port combinations in specific directions.
- Monitor the firewalls that separate the various reference design subnetworks from each another.
- Volume C, *How-To Guides*, contains the firewall configurations that show the rules implemented in each of the firewalls for an example implementation. These configurations are provided to enable the reader to reproduce the traffic filtering/blocking that was achieved in the implementation.
- Apply encryption or integrity-checking mechanisms to all information exchanged between reference design capabilities (i.e., to all user access, policy, and log information exchanged), so that tampering can be detected. Use only encryption and integrity mechanisms that conform to the most-recent industry best practices. Note that, in the case of directory reads and writes, the protected mode is defined as the use of Lightweight Directory Access.

- Strictly control physical access to all assets.
- Deploy a configuration management system to serve as a "monitor of monitors" to ensure that any changes made to the list of information are logged and reported to the monitoring system or to the analytics in the monitoring system, and that notifications are generated. Such a system could also monitor whether reference design monitoring capabilities, such as log integrity capabilities or the monitoring system itself, go offline or stop functioning, and could generate alerts when these capabilities become unresponsive.
- Deploy a system that audits and analyzes directory content to create a description of who has access to what resources, and to validate that these access permissions correctly implement the enterprise's intended business process and access policies.

6.6.3 Deployment Phases

The key to effective PAM solution implementation is to develop and adopt a comprehensive deployment plan to align security components in the existing infrastructure with and around the PAM efforts. It is recommended that a phased approach be developed to deploy the PAM solution and that ensures that short-term and long-term goals can be addressed. It is usually a good practice to develop a maintenance structure that can address additional and future implementations as well as operational and security requirements. The following key activities should be considered when adopting the reference design:

- Phase 0: Define the business and technical objectives for the PAM deployment.
- Phase I: initial setup and infrastructure preparation to ensure that all of the resources needed to deploy, operate, and maintain the PAM solution are available. This includes identifying and documenting privileged users, accounts, critical assets, etc. to management, as well as their functions. The results of automated account discovery are often useful in this preparation.
- Phase II: Deploy the solutions in the reference design to a test set of systems, and tune the configuration for the desired performance and feature functionality to ensure that appropriate security events can be identified and logged, that privileged account information and functions are clearly defined, etc. Measure achievement against the objectives defined in Phase 0; make rollout or objective changes as needed.
- Phase III: broad deployment with use-cases-based testing. It is a good practice to test the adopted solution and test, based on use cases. Measure achievement against the objectives defined in Phase 0.
- Phase IV: Evaluate the performance of the reference design, and perform a risk assessment to assess performance and to identify any weaknesses that can compromise the overall security objectives, based on the identified needs and the defined use case. Measure achievement against the objectives defined in Phase 0.
- Phase V: Manage logs and ensure continuous monitoring. Log management and ongoing events tuning can be complicated by a large volume of security data. It is important to create processes

and procedures for collecting, storing, and analyzing security logs from multiple sources and to prioritize security activities. Integrate with other information security tools in the ecosystem in ways that support the achievement of the objectives defined in Phase 0.

Each of the phases described above should be designed to fit the needs of the organization.

6.6.4 Policy Recommendations

- Define the access policies to enforce the principles of least privilege and separation of duties.
- Configure the monitoring capability with comprehensive analytics to identify anomalous situations that can signal a cyber event. Define enterprise-level workflows that include business and security rules, to determine each user's access control authorizations and to ensure that enterprise access control policy is enforced as completely and accurately as possible.
- Develop an attack model to help determine the types of events that should generate alerts.
- Ensure that the reference design, when adopted, supports flexible data collection.
- Grant only a few users (e.g., human resource administrators) the authority to modify (e.g., initiate, change, delete) employee access information. Require the approval of more than one individual to update employee access information. Log all employee access information modifications. Define workflows to enforce these requirements.
- Define applicable doctrine and guidance for feedback processes, monitoring capabilities, and expected outcome, and develop alternative operational methods to ensure resiliency.

7 Functional Evaluation

A functional evaluation of the PAM example implementation, as constructed in our laboratory, was conducted to verify that it meets its objective of demonstrating the ability to manage and control access to the myriad privileged accounts across an enterprise. The evaluation verified that the example implementation could perform the following functions:

- enforce privileged-account-access and privileged-account-use policies
- protect against unauthorized access to, and/or use of, privileged accounts

Section 7.1 describes the format and components of the functional test cases. Each functional test case is designed to assess the capability of the example implementation to perform the functions listed above and is detailed in Section 7.1.1.

7.1 PAM Functional Test Plan

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework subcategories were used 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 validation points that the example solution is expected to exhibit. Using the Cybersecurity Framework subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

This plan includes the test cases necessary to conduct the functional evaluation of the PAM example implementation, which is currently deployed in a lab at the NCCoE. The implementation tested is described in Section 5.

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 7-1 describes each field in the test case.

Table 7-1 Test Case Fields

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

7.1.1 PAM Use Case Requirements

Table 7-2 identifies the PAM functional evaluation requirements that are addressed in the test plan, and the associated test cases.

Table 7-2 PAM Functional Requirements

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 1	The PAM example implementation shall enforce access and use policies.	N/A	N/A
CR 1.a	N/A	Access denied	PAM-1
CR 1.b	N/A	Access allowed	PAM-1
CR 2	The PAM example implementation shall hide passwords from users.	Verify password is not displayed to users	PAM-2 (not applicable to PAM systems utilizing privilege escalation)
CR 3	The PAM example implementation shall provide replay of user actions.	Replay a user session	PAM-3
CR 4	The PAM example implementation shall support two-factor authentication of users.	N/A	N/A
CR 4.a	N/A	Verify two-factor authentication is operational by using RSA token and that it fails without the token	PAM-4
CR 4.b	N/A	Verify two-factor authentication is operational by using OneSpan (formerly VASCO) token and that it fails without the token	PAM-4
CR 4.c	N/A	Verify two-factor authentication is operational by using IdRamp (Microsoft Authenticator) and that it fails without the token	PAM-4

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 5	The PAM example implementation shall log activity, including failed login attempts.	N/A	N/A
CR 5.a	N/A	Verify logs are collected by the security monitoring system	PAM-5
CR 5.b	N/A	Alert is generated for failed login attempt	PAM-5
CR 6	The PAM example implementation shall include the capability to change account passwords automatically.	N/A	N/A
CR 6.a	N/A	Password change policy can be set to change the password automatically for an account	PAM-6
CR 6.b	N/A	Password changes after each session	PAM-6
CR 7	The PAM example implementation shall include an emergency access (also called break glass) capability.	Use of the emergency access allows access to any privileged account within policy	PAM-7
CR 8	The PAM example implementation shall include automated privileged account discovery.	Verify that accounts known to be privileged are discovered and reported	PAM-8

7.1.2 Test Case: PAM-1

Table 7-3 describes each field in the PAM-1 test case.

Table 7-3 Test Case ID: PAM-1

Parent Requirement	**(CR 1) The PAM example implementation shall enforce access policies and use policies.**
Testable Requirement	(CR 1.a) Access denied (CR 1.b) Access allowed
Description	Show that the PAM solution can enforce access and use policies

Associated Test Cases	N/A
Associated Cybersecurity Framework Subcategories	ID.AM-6, ID.GV-1, ID.GV.2, ID.GV-4, PR.AC-4, PR.PT-3
Preconditions	Access policies and user accounts are configured with the policy management system. The systems to be managed/administered are configured and operational.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM system user interface. 2. Identify a system (A) known to be unavailable (access outside policy) to the PAM user. 3. Identify a system (B) known to be available (access within policy) to the PAM user. 4. Request access to System A. (In some PAM systems, these systems may not be an option.) 5. Request access to System B. 6. Attempt to perform a common action on System A if access is allowed. 7. Attempt to perform a common action on System B if access is allowed.
Expected Results (Pass)	Access is denied to System A (CR 1.a). Access is allowed to System B (CR 1.b).
Actual Results	PAM Build 1 results: ▪ CR 1.a – Access is denied to System A. ▪ CR 1.b – Access is allowed to System B. PAM Build 2 results: ▪ CR 1.a – Access is denied to System A. ▪ CR 1.b – Access is allowed to System B. PAM Build 3 results: ▪ CR 1.a – Access is denied to System A. ▪ CR 1.b – Access is allowed to System B.
Overall Result	Pass

7.1.3 Test Case: PAM-2

Table 7-4 describes each field in the PAM-2 test case.

Table 7-4 Test Case ID: PAM-2

Parent Requirement	**(CR 2) The PAM example implementation shall hide passwords from users.**
Testable Requirement	(CR 2) Verify password is not displayed to users
Description	Show that the PAM solution can hide passwords from users
Associated test cases	PAM-1
Associated Cybersecurity Framework Ssubcategories	ID.AM-3, ID.GV-4, PR.AC-1, PR.PT-4
Preconditions	The systems are established as configured for CR 1.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM system user interface. 2. Identify a system (B) known to be available (access within policy) to the PAM user. 3. Request access to System B. 4. Attempt to perform a common action on System B if access is allowed.
Expected Results (Pass)	The password used for authentication to System B is used and is not displayed to the PAM user (CR 2).
Actual Results	PAM Build 1 results: ▪ CR 2 – The password used for authentication to System B is used and is not displayed to the PAM user. PAM Build 2 results: ▪ CR 2 – The password used for authentication to System B is used and is not displayed to the PAM user. PAM Build 3 results: ▪ CR 2 – The password used for authentication to System B is used and is not displayed to the PAM user.
Overall Result	Pass

7.1.4 Test Case: PAM-3

Table 7-5 describes each field in the PAM-3 test case.

Table 7-5 Test Case ID: PAM-3

Parent Requirement	**(CR 3) The PAM example implementation shall provide session replay capabilities.**
Testable Requirement	(CR 3) Replay a user session
Description	Show that the PAM solution can provide session replay functionality for use in training or forensic activities
Associated Test Cases	PAM-2
Associated Cybersecurity Subcategories	PR.PT-1, RS.AN-3
Preconditions	This test can be run after CR 1 or CR 2.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM system user interface. 2. Request replay of a session known to have occurred. Any session established in CR 1 or CR 2 is sufficient. 3. Replay the session.
Expected Results (Pass)	The session replay is successful (CR 3). The details of the activity during the session are replayed (CR 3).
Actual Results	PAM Build 1 results: ▪ CR 3 – The session replay is successful. The details of the activity during the session are replayed. PAM Build 2 results: ▪ CR 3 – The session replay is successful. The details of the activity during the session are replayed. PAM Build 3 results: ▪ CR 3 – The session replay is successful. The details of the activity during the session are replayed.
Overall Result	Pass

7.1.5 Test Case: PAM-4

Table 7-6 describes each field in the PAM-4 test case.

Table 7-6 Test Case ID: PAM-4

Parent Requirement	**(CR 4) The PAM example implementation shall support two-factor authentication.**
Testable Requirement	(CR 4.a) Two-factor authentication is operational using a RSA token (CR 4.b) Two-factor authentication is operational using the OneSpan token mobile solution (CR 4.c) Two-factor authentication is operational using the IdRamp (Microsoft Authenticator) mobile solution
Description	Show that the PAM solution can enforce the use of MFA
Associated Test Cases	PAM-2
Associated Cybersecurity Framework Subcategories	ID.GV-4, PR.AC-1, PR.PT-3
Preconditions	This test can be run after CR 1 or CR 2.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM system user interface. 2. Log into the PAM system (two-factor authentication must be enabled). 3. Log in by using the correct second factor. 4. Attempt login with an incorrect second factor.
Expected Results (Pass)	Two-factor authentication is operational (CR 4.a, CR 4.b, CR 4.c). Login is prevented without a proper second factor (CR 4.a, CR 4.b, CR 4.c).
Actual Results	PAM Build 1 results: ▪ CR 4.a, CR 4.b, CR 4.c – Two-factor authentication is operational. Login is prevented without a proper second factor. PAM Build 2 results: ▪ CR 4.a, CR 4.b, CR 4.c – Two-factor authentication is operational. Login is prevented without a proper second factor. PAM Build 3 results: ▪ CR 4.a, CR 4.b, CR 4.c – Two-factor authentication is operational. Login is prevented without a proper second factor.
Overall Result	Pass

7.1.6 Test Case: PAM-5

Table 7-7 describes each field in the PAM-5 test case.

Table 7-7 Test Case ID: PAM-5

Parent Requirement	**(CR 5) The PAM example implementation shall log activity, including failed login attempts.**
Testable Requirement	(CR 5.a) Verify logs are collected by the security monitoring system (CR 5.b) Alert is generated for failed login attempts
Description	Show that the PAM solution can record event logs and integrates with the security monitoring system (both normal and anomalous events)
Associated Test Cases	PAM-4
Associated Cybersecurity Framework Subcategories	DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-3, DE.CM-7, RS.CO-2
Preconditions	CR 4
Procedure	Perform the following procedures on each PAM build instance: 1. Access the security monitoring system. 2. View collected logs. 3. Set up alerts for anomalous events that need to be identified.
Expected Results (Pass)	The security monitoring system records events for each component (CR 5.a). The security monitoring system provides alerts when a predefined anomalous activity is detected (failed login attempt) (CR 5.b).
Actual Results	PAM Build 1 results: ▪ CR 5.a – The security monitoring system records events for each component. ▪ CR 5.b – The security monitoring system provides alerts when a predefined anomalous activity is detected (failed login attempt). PAM Build 2 results: ▪ CR 5.a – The security monitoring system records events for each component. ▪ CR 5.b – The security monitoring system provides alerts when a predefined anomalous activity is detected (failed login attempt). PAM Build 3 results: ▪ CR 5.a – The security monitoring system records events for each component. ▪ CR 5.b – The security monitoring system provides alerts when a predefined anomalous activity is detected (failed login attempt).

Overall Result	Pass

7.1.7 Test Case: PAM-6

Table 7-8 describes each field in the PAM-6 test case.

Table 7-8 Test Case ID: PAM-6

Parent Requirement	**(CR 6) The PAM example implementation shall include the capability to change account passwords automatically.**
Testable Requirement	(CR 6.a) Password change policy can be set to change the password automatically for an account (CR 6.b) Password changes after each session
Description	Show that the PAM solution can be configured to automatically change account passwords
Associated Test Cases	PAM-1
Associated Cybersecurity Framework Subcategories	ID.GV-4, PR.AC-1, PR.PT-3
Preconditions	CR 4: The packet capture is set up to capture the login username and password from the PAM system.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM policy management system. 2. Create a password change policy to change the password after each session. 3. Access the PAM system user interface. 4. Identify a system (B) known to be available (access within policy) to the PAM user. 5. Activate the packet capture for the sessions with System B. 6. Request access to System B. 7. Attempt to perform a common action on System B if access is allowed. 8. Close the session. 9. Request access to System B (second time). 10. Close the session.
Expected Results (Pass)	The PAM password management system can be configured to change passwords after each session (CR 6.a). Passwords are changed after each session (CR 6.b).

Actual Results	PAM Build 1 results: ▪ CR 6.a – The PAM password management system can be configured to change passwords after each session. ▪ CR 6.b – Passwords are changed after each session. PAM Build 2 results: ▪ CR 6.a – The PAM password management system can be configured to change passwords after each session. ▪ CR 6.b – Passwords are changed after each session. PAM Build 3 results: ▪ CR 6.a – The PAM password management system can be configured to change passwords after each session. ▪ CR 6.b – Passwords are changed after each session.
Overall Result	Pass

7.1.8 Test Case: PAM-7

Table 7-9 describes each field in the PAM-7 test case.

Table 7-9 Test Case ID: PAM-7

Parent Requirement	**(CR 7) The PAM example implementation shall include an emergency access (also called break glass) capability.**
Testable Requirement	(CR 7) Use of the emergency access allows access to any privileged account within policy
Description	Show that the PAM solution can provide emergency access to any privileged account within policy
Associated Test Cases	PAM-2
Associated Cybersecurity Framework Subcategories	ID.BE-4
Preconditions	This test can be run after CR 1 or CR 2.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM system user interface. 2. Request an emergency session using a predefined emergency credential. 3. Request access to System B. 4. Attempt to perform a common action on System B if access is allowed. 5. Close the emergency session.

	6. Request an emergency session using an incorrect emergency credential. 7. Request access to System B. 8. Attempt to perform a common action on System B if access is allowed.
Expected Results (Pass)	Emergency access using the predefined emergency credential results in access to the desired system (B) (CR 7). Emergency access without the predefined emergency credential results in no access allowed (CR 7).
Actual Results	PAM Build 1 results: ▪ CR 7 – Emergency access using the predefined emergency credential results in access to the desired system (B). Emergency access without the predefined emergency credential results in no access allowed. PAM Build 2 results: ▪ CR 7 – Emergency access using the predefined emergency credential results in access to the desired system (B). Emergency access without the predefined emergency credential results in no access allowed. PAM Build 3 results: ▪ CR 7 – Emergency access using the predefined emergency credential results in access to the desired system (B). Emergency access without the predefined emergency credential results in no access allowed.
Overall Result	Pass

7.1.9 Test Case: PAM-8

Table 7-10 describes each field in the PAM-8 test case.

Table 7-10 Test Case ID: PAM-8

Parent Requirement	**(CR 8) The PAM example implementation shall include automated privileged account discovery.**
Testable Requirement	(CR 8) Verify that accounts known to be privileged are discovered and reported
Description	Show that the PAM solution can automatically discover privileged accounts
Associated Test Cases	PAM-2

Associated Cybersecurity Framework Subcategories	PR.AC-1, DE-AE-2, RS.CO-2
Preconditions	This test can be run after CR 1 or CR 2.
Procedure	Perform the following procedures on each PAM build instance: 1. Access the PAM system user interface. 2. Request an automated privileged account discovery process for a selected directory. 3. Review the results of the process. 4. Add a privileged account to a directory. 5. Request an automated privileged account discovery process for the selected directory. 6. Review the results of the process.
Expected Results (Pass)	Automated privileged account discovery should identify the newly created account (CR 8).
Actual Results	PAM Build 1 results: ▪ CR 8 – Automated privileged account discovery should identify the newly created account. PAM Build 2 results: ▪ CR 8 – Automated privileged account discovery should identify the newly created account. PAM Build 3 results: ▪ CR 8 – Automated privileged account discovery should identify the newly created account.
Overall Result	Pass

Appendix A List of Acronyms

API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CAT	Cybersecurity Assessment Tool
COI	Community of Interest
CR	Capability Requirement
DE	Detect
FFIEC	Federal Financial Institutions Examination Council
FID	Federated Identity
FIPS	Federal Information Processing Standards
IaaS	Infrastructure as a Service
ID	Identify
IdAM	Identity and Access Management
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
MFA	Multifactor Authentication
N/A	Not Applicable
NCCoE	National Cybersecurity Center of Excellence
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OS	Operating System

PaaS	Platform as a Service
PAM	Privileged Account Management
PR	Protect
RDP	Remote Desktop Protocol
RS	Respond
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
Syslog	System Log
TLS	Transport Layer Security
UBA	User Behavior Analytics

Appendix B References

[1] R. Ross et al., "Protecting controlled unclassified information in nonfederal systems and organizations," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-171, Dec. 2016, Revision 1, p. 125. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[2] A. Cser et al. (2016, Jul. 8). *The Forrester Wave™: Privileged Identity Management, Q3 2016* [Online].
Available: https://www.forrester.com/report/The+Forrester+Wave+Privileged+Identity+Management+Q3+2016/-/E-RES123903.

[3] A. Sedgewick, "Framework for improving critical infrastructure cybersecurity," NIST, Gaithersburg, Maryland, Feb. 2014, Version 1.0, p. 41.
Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[4] G. Stoneburner et al., "Guide for conducting risk assessments," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-30, Sep. 2012, Revision 1, p. 95.
Available: http://dx.doi.org/10.6028/NIST.SP.800-30r1.

[5] R. Ross et al., "Guide for applying the risk management framework to federal information systems," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-37, Feb. 2010, p. 101.
Available: http://dx.doi.org/10.6028/NIST.SP.800-37r1.

[6] R. Ross et al., "Managing information security risk," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-39, Mar. 2011, p. 87. Available: http://dx.doi.org/10.6028/NIST.SP.800-39.

[7] R. Ross et al., "Security and privacy controls for federal information systems and organizations," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-53, Apr. 2013, Revision 4, p. 461. Available: https://doi.org/10.6028/NIST.SP.800-53r4.

[8] U.S. Department of Commerce, "Security requirements for cryptographic modules," NIST, Gaithersburg, MD, Federal Information Processing Standards (FIPS) Publication 140-2, May 2001, p. 69. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

[9] K. Kent and M. Souppaya, "Guide to computer security log management," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-92, Sep. 2006, p. 72.
Available: http://dx.doi.org/10.6028/NIST.SP.800-92.

[10] P. Bowen et al., "Information security handbook: A guide for managers," NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-100, Oct. 2006, p. 178.
Available: http://dx.doi.org/10.6028/NIST.SP.800-100.

[11] OMB, “Managing information as a strategic resource,” OMB, Washington, DC, OMB Circular No. A-130, Nov. 2000. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

[12] “FFIEC Cybersecurity Assessment Tool,” FFIEC, Washington, DC, May 2017, p. 59. Available: https://www.ffiec.gov/%5C/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

[13] P. Grassi et al., “Digital identity guidelines: Authentication and lifecycle management,” NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-63B, Jun. 2017, p. 79. Available: https://doi.org/10.6028/NIST.SP.800-63b.

[14] W. Newhouse et al., “National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework,” NIST, Gaithersburg, MD, NIST Special Publication (SP) 800-181, Aug. 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[15] Paul Cichonski et al., “Computer security incident handling guide,” NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-61, Aug. 2012, Revision 2, p. 79. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[16] Karen Kent et al., “Guide to integrating forensic techniques into incident response,” NIST, Gaithersburg, Maryland, NIST Special Publication (SP) 800-86, Aug. 2006, p. 121. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

NIST SPECIAL PUBLICATION 1800-18C

Privileged Account Management for the Financial Services Sector

Volume C:
How-To Guides

Karen Waltermire
National Cybersecurity Center of Excellence
Information Technology Laboratory

Tom Conroy
Marisa Harriston
Chinedum Irrechukwu
Navaneeth Krishnan
James Memole-Doodson
Benjamin Nkrumah
Harry Perper
Susan Prince
Devin Wynne
The MITRE Corporation
McLean, VA

September 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

DISCLAIMER

Certain commercial entities, equipment, products, 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, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-18C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-18C, 104 pages, September 2018, CODEN: NSPUE2

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.

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

Public comment period: September 28, 2018 through November 30, 2018

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology (IT) security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://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, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Privileged account management (PAM) is a domain within identity and access management (IdAM) that focuses on monitoring and controlling the use of privileged accounts. Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and service accounts. These powerful accounts provide elevated, often nonrestricted, access to the underlying IT resources and technology, which is why external and internal malicious actors seek to gain access to them. Hence, it is critical to monitor, audit, control, and manage privileged account usage. Many organizations, including financial sector companies, face challenges in managing privileged accounts.

The goal of this project is to demonstrate a PAM capability that effectively protects, monitors, and manages privileged account access, including life-cycle management, authentication, authorization, auditing, and access controls.

KEYWORDS

Access control, auditing, authentication, authorization, life-cycle management, multifactor authentication, PAM, privileged account management, provisioning management

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Dan Morgan	Bomgar (formerly Lieberman Software)
David Weller	Bomgar (formerly Lieberman Software)
Oleksiy Bidniak	Ekran System
Oleg Shomonko	Ekran System
Karl Kneiss	IdRamp
Eric Vinton	IdRamp
Michael Fagan	NIST
Will LaSala	OneSpan (formerly VASCO)
Michael Magrath	OneSpan (formerly VASCO)
Jim Chmura	Radiant Logic
Don Graham	Radiant Logic
Timothy Keeler	Remediant
Paul Lanzi	Remediant

Name	Organization
Michael Dalton	RSA
Timothy Shea	RSA
Adam Cohn	Splunk
Pam Johnson	TDi Technologies
Clyde Poole	TDi Technologies
Sallie Edwards	The MITRE Corporation
Sarah Kinling	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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:

Technology Partner/Collaborator	Build Involvement
Bomgar (formerly Lieberman Software)	Red Identity Suite
Ekran System	Ekran System Client
IdRamp	Secure Access
OneSpan (formerly VASCO)	DIGIPASS
Radiant Logic	RadiantOne FID
Remediant	SecureONE
RSA	SecureID Access

Technology Partner/Collaborator	Build Involvement
Splunk	Splunk Enterprise
TDi Technologies	ConsoleWorks

Contents

1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not recreate the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the privileged account management (PAM) example solution. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST Special Publication (SP) 1800-18A: *Executive Summary*
- NIST SP 1800-18B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-18C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-18A, which describes the following topics:

- challenges enterprises face in managing privileged accounts
- example solution built at the National Cybersecurity Center of Excellence (NCCoE)
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-18B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk, provides a description of the risk analysis we performed
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-18A,* with your leadership team members to help them understand the importance of adopting standards-based PAM.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-18C,* to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally 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 within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. 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 PAM system to manage and monitor the use of privileged accounts. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, of Volume B lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

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 financial_nccoe@nist.gov.

1.2 Build Overview

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively manage and monitor the authorized use of privileged accounts and to explore techniques to protect against and detect the unauthorized use of these accounts. The NCCoE also explored the issues of auditing and reporting that IT systems use to support incident recovery and investigations. The servers in the virtual environment were built to the hardware specifications of their specific software components.

The NCCoE worked with members of the Financial Sector Community of Interest to develop a diverse (but noncomprehensive) set of use-case scenarios against which to test the reference implementation. These use-case scenarios are detailed in Volume B, Section 5.5. For a detailed description of our architecture, see Volume B, Section 4.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*.
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, on-screen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

2.1 Microsoft Active Directory

2.1.1 How It's Used

Microsoft Active Directory (AD) serves as the privileged account identity repository, the Domain Name System (DNS) server, and the certificate authority (CA).

2.1.2 Virtual Machine Configuration

The Microsoft AD virtual machine is configured as follows:

- 4 central processing unit (CPU) cores
- 16 gigabytes (GB) of random-access memory (RAM)

- 120 GB hard disk drive (HDD)
- 1 network adapter

Network Configuration (Interface 1):

- Internet protocol version 4 (IPv4): manual
- Internet protocol version 6 (IPv6): disabled
- Internet protocol (IP) address: 172.16.3.10
- Netmask: 255.255.255.0
- Gateway: 172.16.3.1
- DNS name servers: 172.16.3.10
- DNS-search domains: AcmeFinancial.com

2.1.3 Installation

Install the AD domain services and CA according to the instructions provided at the following links:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-

https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority

2.1.4 DNS Configuration

1. Create the host records and reverse entries in the AcmeFinancial.com DNS service for the following servers:
    a. Bomgar Privileged Identity
    b. TDi ConsoleWorks
    c. Splunk Enterprise
    d. Radiant Logic Federated Identity (FID)
    e. Ekran System
    f. Remediant SecureONE
    g. RSA Authentication Manager
    h. OneSpan IDENTIKEY

2.1.5 Group Policy Object Configuration

1. Open **Group Policy Management.**
2. Under the **Default Domain Policy**, make the following changes under **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration:**

Advanced Audit Configuration	
Account Management	
Policy	**Setting**
Audit Application Group Management	Success, Failure
Audit Computer Account Management	Success, Failure
Audit Distribution Group Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure
Logon/Logoff	
Policy	**Setting**
Audit Group Membership	Success, Failure
Audit Logon	Success, Failure
Audit Other Logon/Logoff Events	Success, Failure
Audit Special Logon	Success, Failure
Policy Change	
Policy	**Setting**
Audit Audit Policy Change	Success, Failure
Privilege Use	
Policy	**Setting**
Audit Non Sensitive Privilege Use	Success, Failure
Audit Sensitive Privilege Use	Failure

2.1.6 Scripts

The following scripts were created to easily import and correlate data once forwarded to Splunk Enterprise.

The following Python script parses data extracted from the Windows security event log. The script is located at **c:**.

```
import csv
import re
from subprocess import check_output
```

```
csvfile = open('Final_AD.csv', 'w+')
wr = csv.writer(csvfile, quoting=csv.QUOTE_ALL)
csvlist = ["Event", "UserSubject", "UserObject", "Timestamp"]
wr.writerow(csvlist)
with open('ADLOG.csv', 'r') as f:
	reader = csv.reader(f)
	zerothrow = 1
	for row in reader:
		csvlist = []
		if zerothrow == 1:
			zerothrow = 0
		else:
			parse_list =  row[1].split('\n')
			#print parse_list
			#break
			csvlist.append(parse_list[0].replace('\t', '').replace('\r', ''))
			csvlist.append(parse_list[4].replace('\t', '').replace('\r',
			'').replace('Account Name:', ''))
			if row[4] == "4728":
			win_command = parse_list[10].replace('\t', '').replace('\r',
			'').replace('Account Name:', '')
			win_command = win_command[:3] + '"' + win_command[3:]
			sec_index = win_command.index(",CN=")
			win_command = win_command[:sec_index] + '"' +
			win_command[sec_index:]
			win_command = "dsquery * " + win_command + " -scope base -attr
			sAMAccountName"
			account = check_output(win_command, shell  = True).decode()
			account = account.replace('sAMAccountName', '').replace('\n',
			'').replace(' ', '')
			csvlist.append(account)
		else:
```

```
                    csvlist.append(parse_list[10].replace('\t', '').replace('\r',
'').replace('Account Name:', ''))
                    csvlist.append(row[2].replace('\t', '').replace('\r', ''))
                    wr.writerow(csvlist)
#temp = check_output("dir C:", shell=True).decode()
#print(temp)
csvfile.close()
```

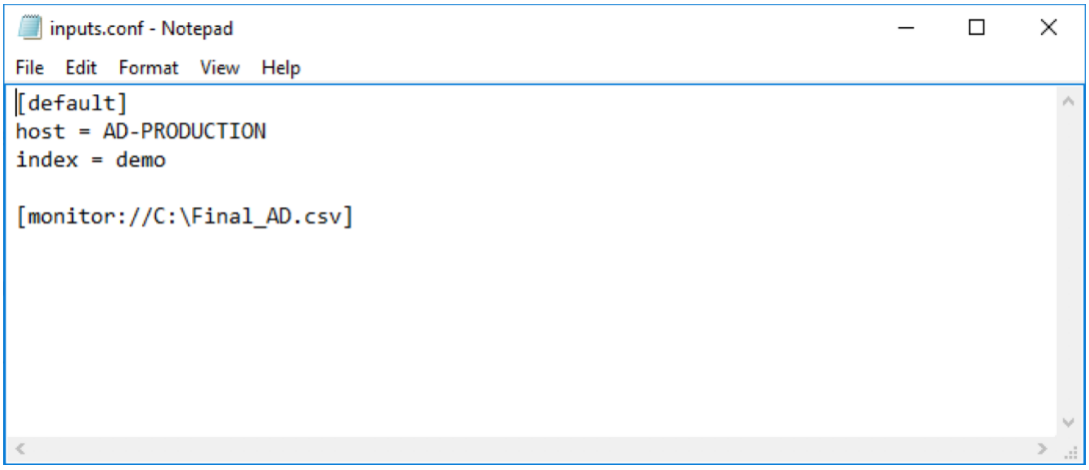
The following PowerShell script extracts data from the Windows security event log and executes the Python script above:

```
Set-Variable -Name EventAgeDays -Value 2    #we will take events for the latest 2 days
Set-Variable -Name Computer -Value "AD-Production"   # replace it with your server
names
Set-Variable -Name LogNames -Value "Security"  # Checking app and system logs
Set-Variable -Name EventTypes -Value @(7001, 7002, 4720, 4722, 4725, 4726, 4728, 4738)
# Loading only Errors and Warnings
Set-Variable -Name ExportFolder -Value "C:\"
$el_c = @()   #consolidated error log
$now=get-date
$startdate=$now.adddays(-$EventAgeDays)
$ExportFile=$ExportFolder + "ADLOG.csv"  # we cannot use standard delimiteds like ":"
Write-Host Processing $Computer\$LogNames
$el = get-eventlog -ComputerName $Computer -log $Lognames -After $startdate -
InstanceId $EventTypes
$el_c += $el  #consolidating
$el_sorted = $el_c | Sort-Object TimeGenerated    #sort by time
Write-Host Exporting to $ExportFile
$el_sorted|Select EntryType, Message, TimeGenerated, Source, EventID, MachineName |
Export-CSV $ExportFile -NoTypeInfo  #EXPORT
Write-Host Done!
python adparse.py
```

2.1.7 Splunk Universal Forwarder

Install Splunk Universal Forwarder by following the instructions provided at http://docs.splunk.com/Documentation/Forwarder/7.1.3/Forwarder/Abouttheuniversalforwarder.

Edit the *inputs.conf* file to monitor the *Final_AD.csv* file created from the Python script above and to forward logs to the **demo** index at Splunk Enterprise.



2.2 Bomgar Privileged Identity

Bomgar Privileged Identity is a PAM solution that manages account passwords in Microsoft AD.

2.2.1 How It's Used

Privileged Identity is used as a PAM provider in the example implementation. It provides a web application server that users log into with unprivileged accounts. These users are then allowed to launch applications as privileged users, based on the policy and configuration in Privileged Identity.

2.2.2 Virtual Machine Configuration

The Privileged Identity virtual machine is configured as follows:

- Windows Server 2012 R2
- 4 CPU cores
- 16 GB of RAM
- 60 GB of storage
- 1 network interface controller/card (NIC)

Network Configuration (Interface 1):

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.1.10
- Netmask: 255.255.255.0
- Gateway: 172.16.1.1
- DNS name servers: 172.16.3.10
- DNS-search domains: not applicable (N/A)

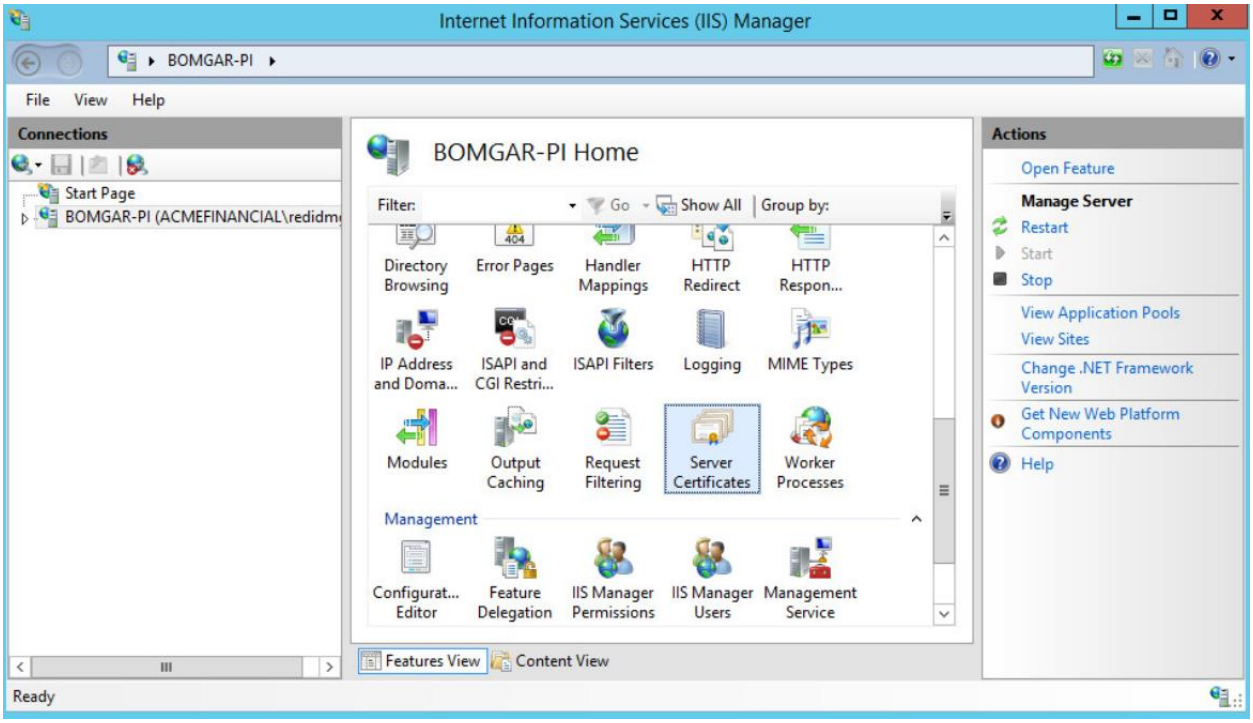
2.2.3 Prerequisites

- Before Privileged Identity can be installed, Microsoft Structured Query Language (SQL) Server must be installed. In a test environment, Microsoft SQL Server Express also is acceptable.
- The web application server's requirements include Internet Information Services (IIS) and Microsoft .NET Framework 4.5.2 or later.
- A full list of requirements can be found in the Installation Guide on Bomgar's website.

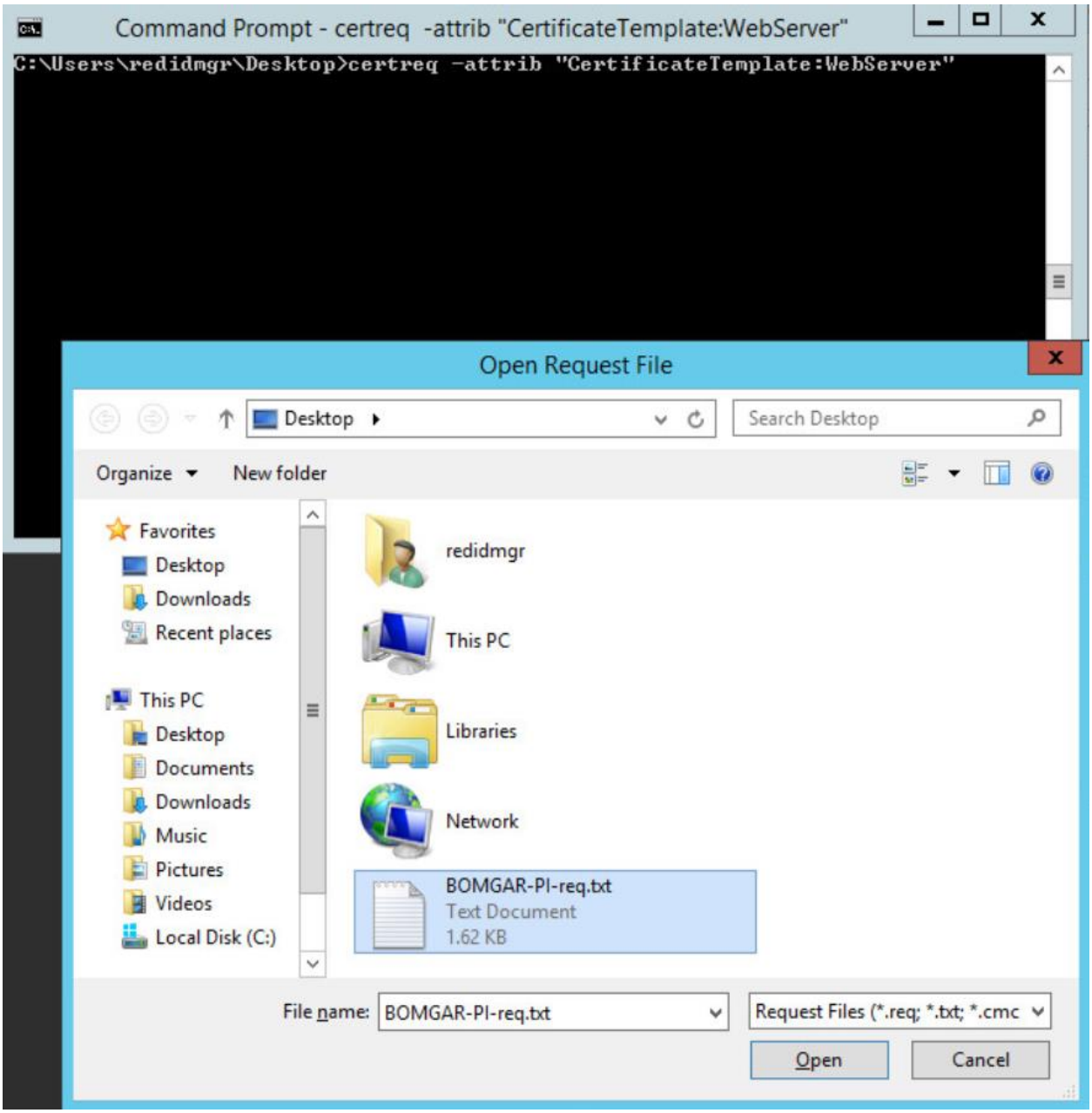
2.2.4 Installing Privileged Identity

To configure IIS for use with Bomgar's web application server, a certificate signed by AD Certificate Services was created.

1. Open **Server Manager.**
2. Click **Tools > Internet Information Services (IIS) Manager.**
3. Click on the name of the server (in this case, **Bomgar-PI**), and select **Server Certificates.**

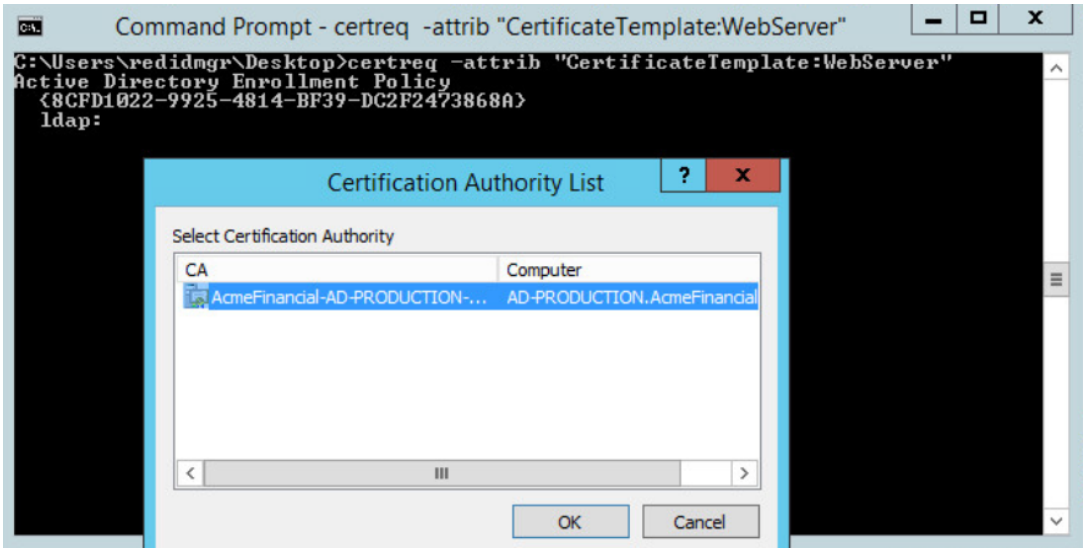


4. On the right, click **Create Certificate Request.**
5. Fill out the **Distinguished Name Properties,** and then click **Next.**
6. Select a bit length of **2048,** and then click **Next.**
7. Give the certificate a file name, and then click **Finish.**
8. Using the certreq command in the **Command Prompt,** enter `certreq -attrib "CertificateTemplate:WebServer"`.
9. Select the certificate file that was created in Step 7, and then click **Open.**



328

329 10. Choose the Domain Controller CA from the **Certification Authority List,** and then click **OK.**

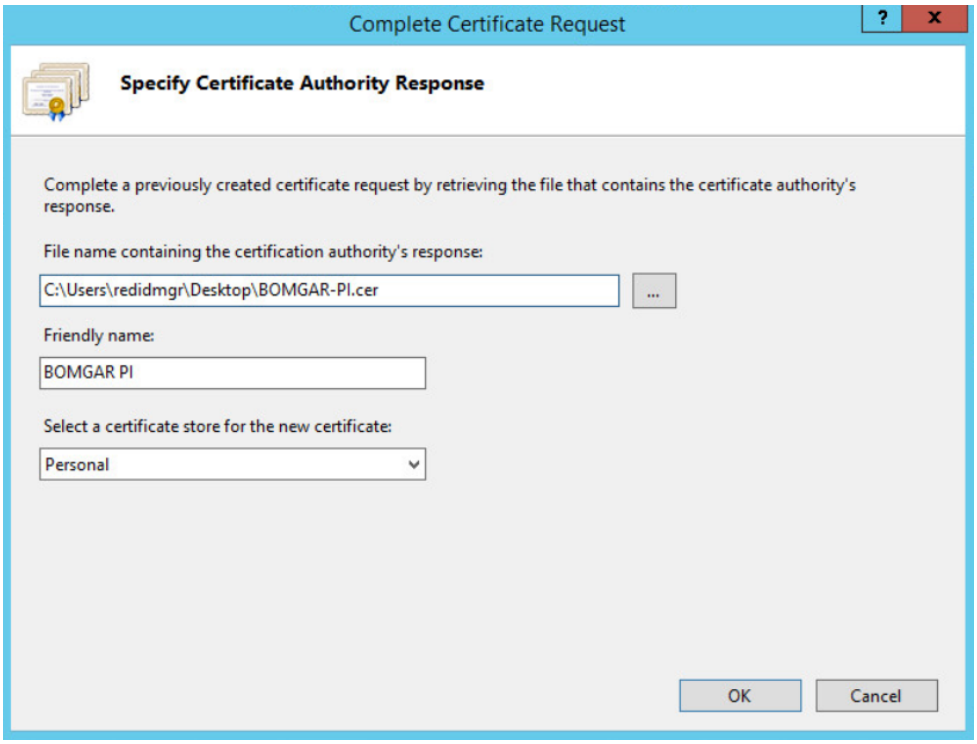


330

331 11. Go back to the **IIS Manager,** and click **Bomgar-PI.** Select **Server Certificates.**

332 12. On the right, click **Complete Certificate Request.**

333 13. Fill out the pop-up window with the signed-certificate file name and a friendly name (e.g.,
334 Bomgar-PI), and store it in the **Personal** certificate store.



335

14. Click **OK**
15. Create a Secure Sockets Layer (SSL) binding with that certificate by following documentation from Microsoft.

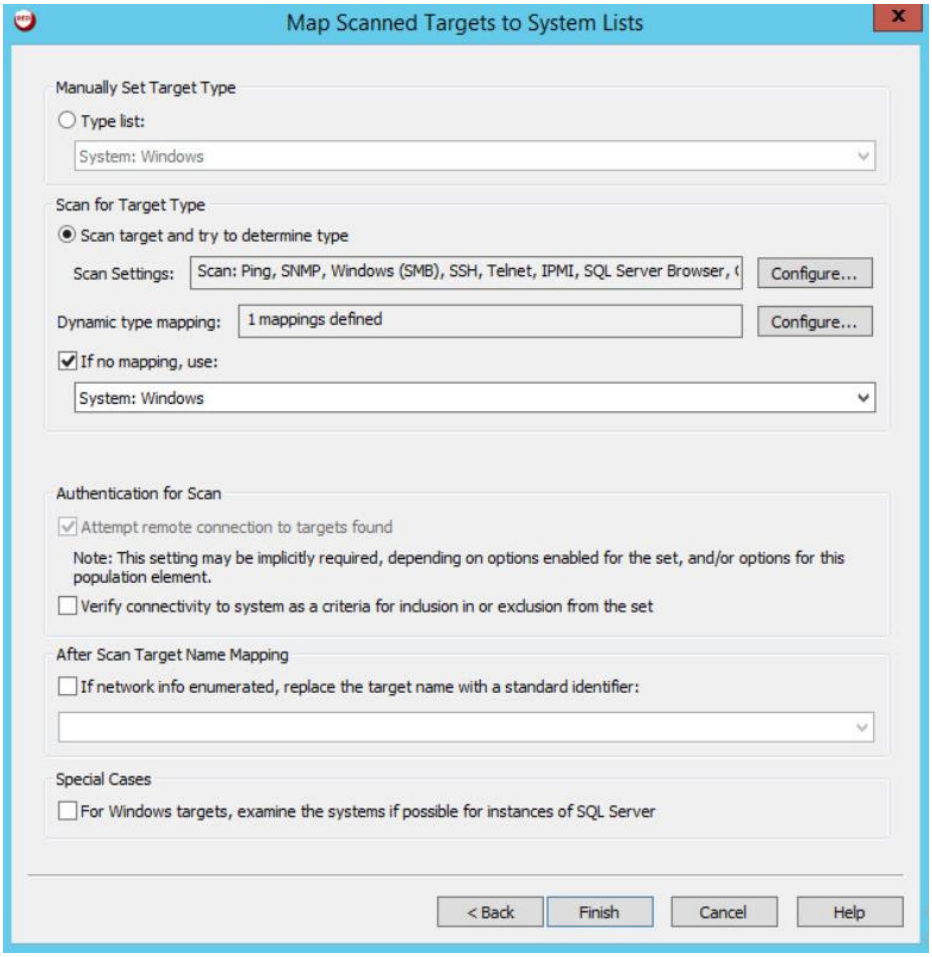
You are now ready to begin following further installation instructions that are publicly available on Bomgar's website.

2.2.5 Configuration

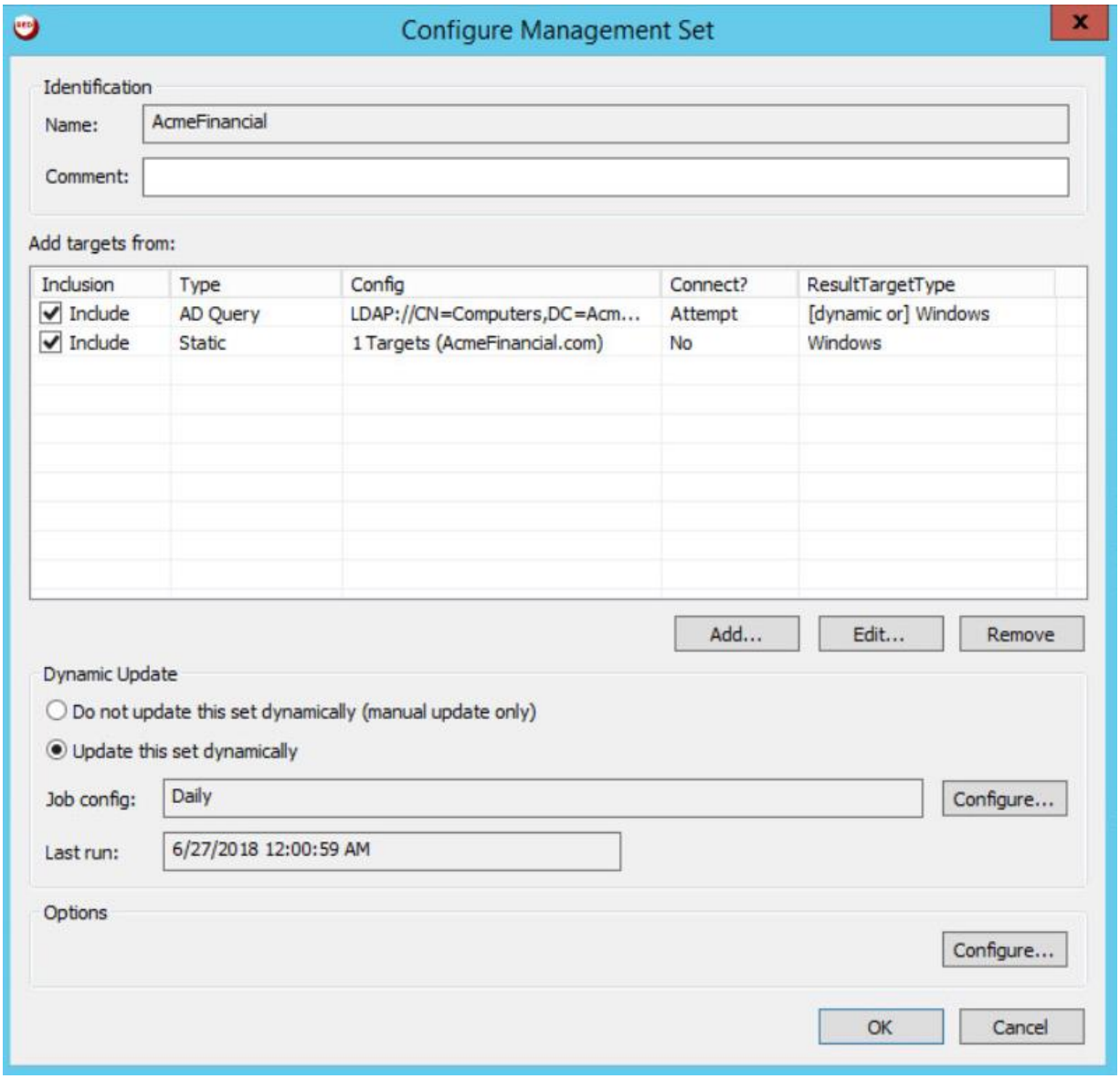
Using the Bomgar Privileged Identity Admin Guide, complete the configuration steps provided in the following subsections.

2.2.5.1 Management Set

1. Create a new management set for the AD domain.
2. Configure the management set to include systems by querying AD.
3. Configure the management set to scan for the target type by scanning for a Secure Shell (SSH) server. Set the default to Windows if there is no match.



4. Configure the management set to have a second inclusion from a **Static list of targets,** and include the domain name **(AcmeFinancial.com).** Manually set the target type to Windows.
5. Set the management set to update dynamically each day.



2.2.5.2 Delegation Identities

To allow a user to have access to the web console, a Delegation Identity must be created for that user.

Add the following users as Delegation Identities by following the steps provided below:

1. Add the following regular user accounts as Delegation Identities by selecting **Delegation > Delegation Identities** and then clicking **Add.**
    a. ACMEFINANCIAL\udb1

b. ACMEFINANCIAL\twitteruser

2. For the **Role Type,** select **Windows Domain User,** and then enter the username in the field next to it.
3. Click **OK.**

2.2.6 Installing Privileged Identity Application Launcher

To allow users to proxy connections as privileged users, the Privileged Identity application launcher must be installed on another server. Detailed prerequisite and installation instructions are available on Bomgar's website.

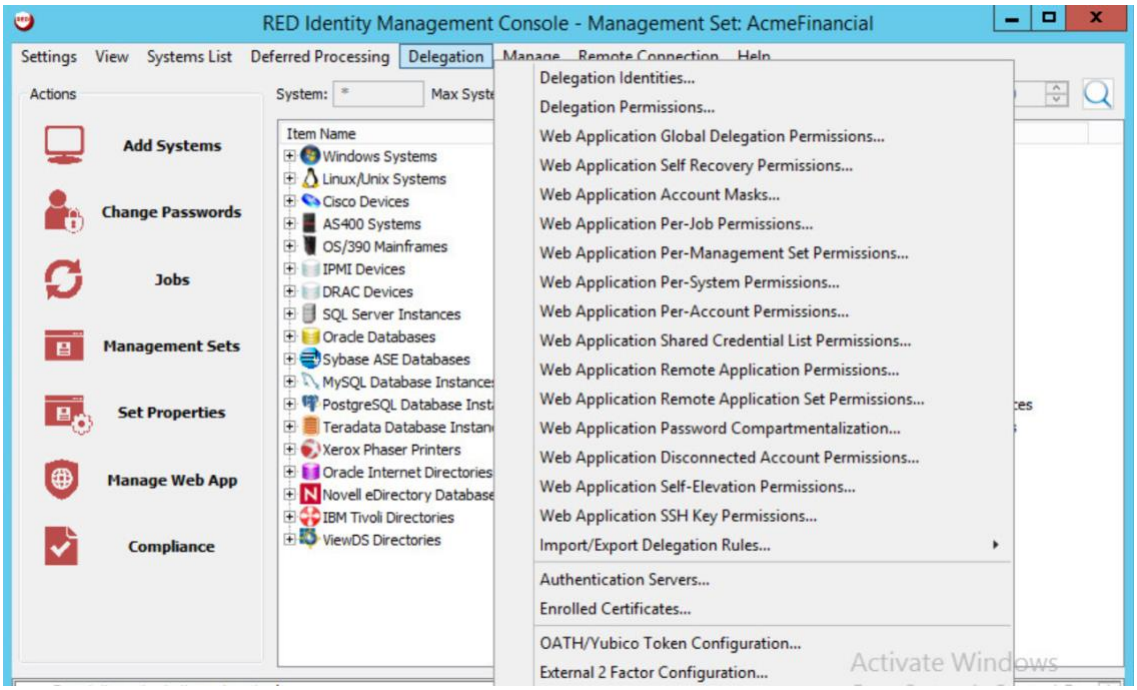
Using the Bomgar documentation, complete the following steps:

1. Create a new virtual machine:
    a. Windows Server 2012 R2
    b. 1 CPU core
    c. 4 GB of RAM
    d. 60 GB of storage
    e. 1 NIC
        i. IPv4: manual
        ii. IPv6: disabled
        iii. IPv4 address: 172.16.1.31
        iv. Netmask: 255.255.255.0
        v. Gateway: 172.16.1.1
        vi. DNS-search domains: N/A
2. Install Remote Desktop Services.
3. DO NOT install Desktop Experience.
4. Install Application Launcher without Session Recording.
5. Configure Remote Desktop Services to publish **LiebsoftLauncher.exe** and **ssms.exe.**
6. Configure the web launcher settings in the Bomgar **RED Identity Management Console.**

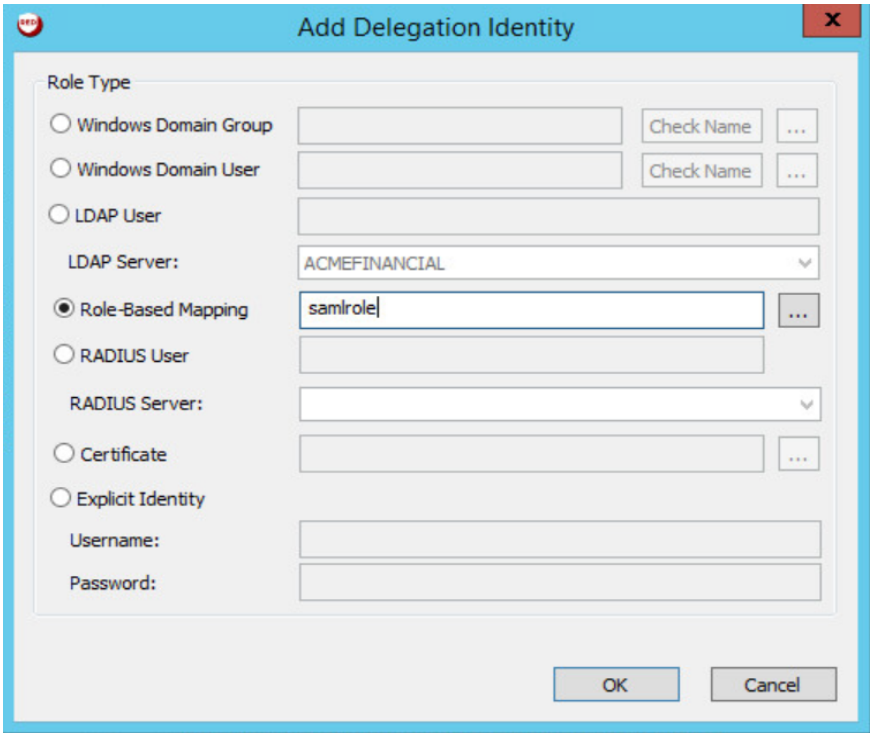
2.2.7 Configure Bomgar Privileged Identity with IdRamp SAML Authentication

Use the following steps to configure the Security Assertion Markup Language (SAML) authentication for the Bomgar Privileged Identity Manager, using IdRamp as an identity provider and broker to Azure AD.

1. Open the Bomgar **RED Identity Management Console** desktop application.
2. Navigate to **Delegation > Web Application Global Delegation Permissions.**



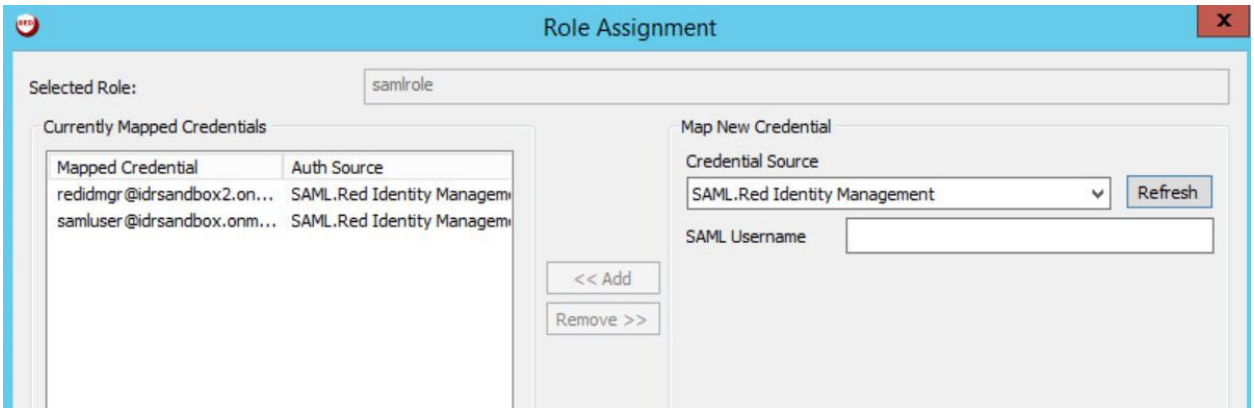
3. Click **Add** at the lower left corner.
4. Select **Role-Based Mapping,** enter a friendly name in the field, and then click **OK.**



394

395 5. Select the role that you just created, and then click **Assign Role.**

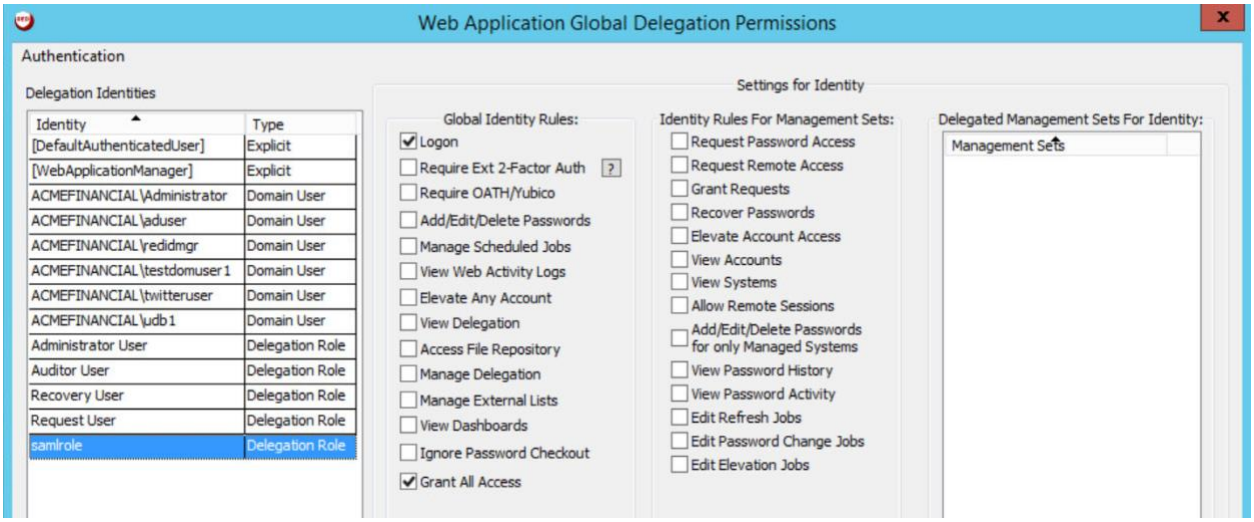
396 6. In the **SAML Username** field, enter the identities or usernames of the users to whom you would
397 like to assign this role. Click **Add** after each username that you enter.



398

399 7. Click **OK.**

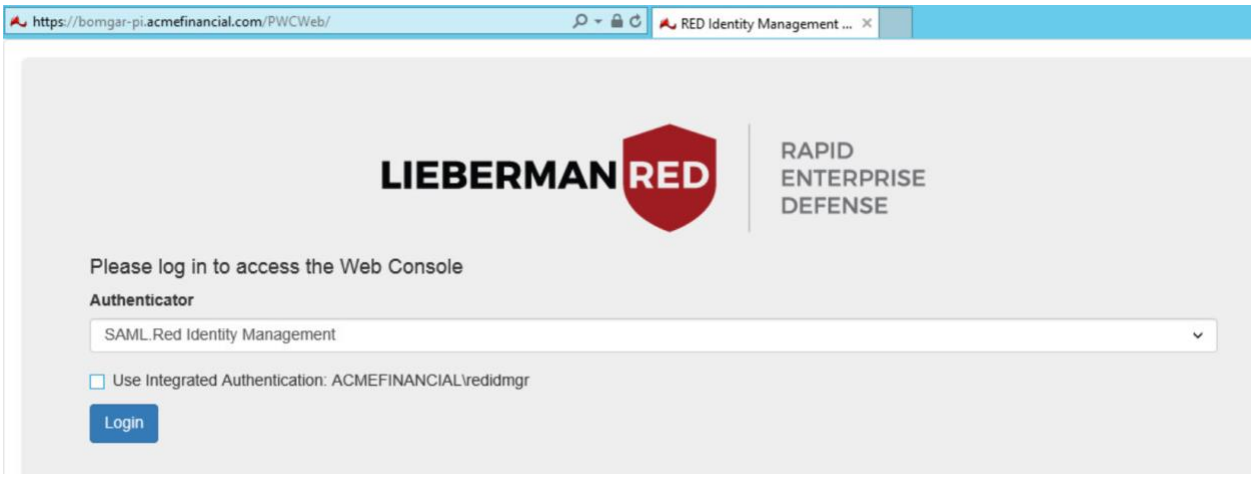
400 8. Make sure that the role that you created is selected, and then select the **Logon** and **Grant All**
401 **Access** check boxes.



9. Click **OK.**

10. To log onto the Bomgar Privileged Identity Manager by using SAML authentication, navigate your web browser to https://<serverhostname>/PWCWeb/.

11. Select SAML authentication on the login page, click **Login,** and then follow the authentication prompts.



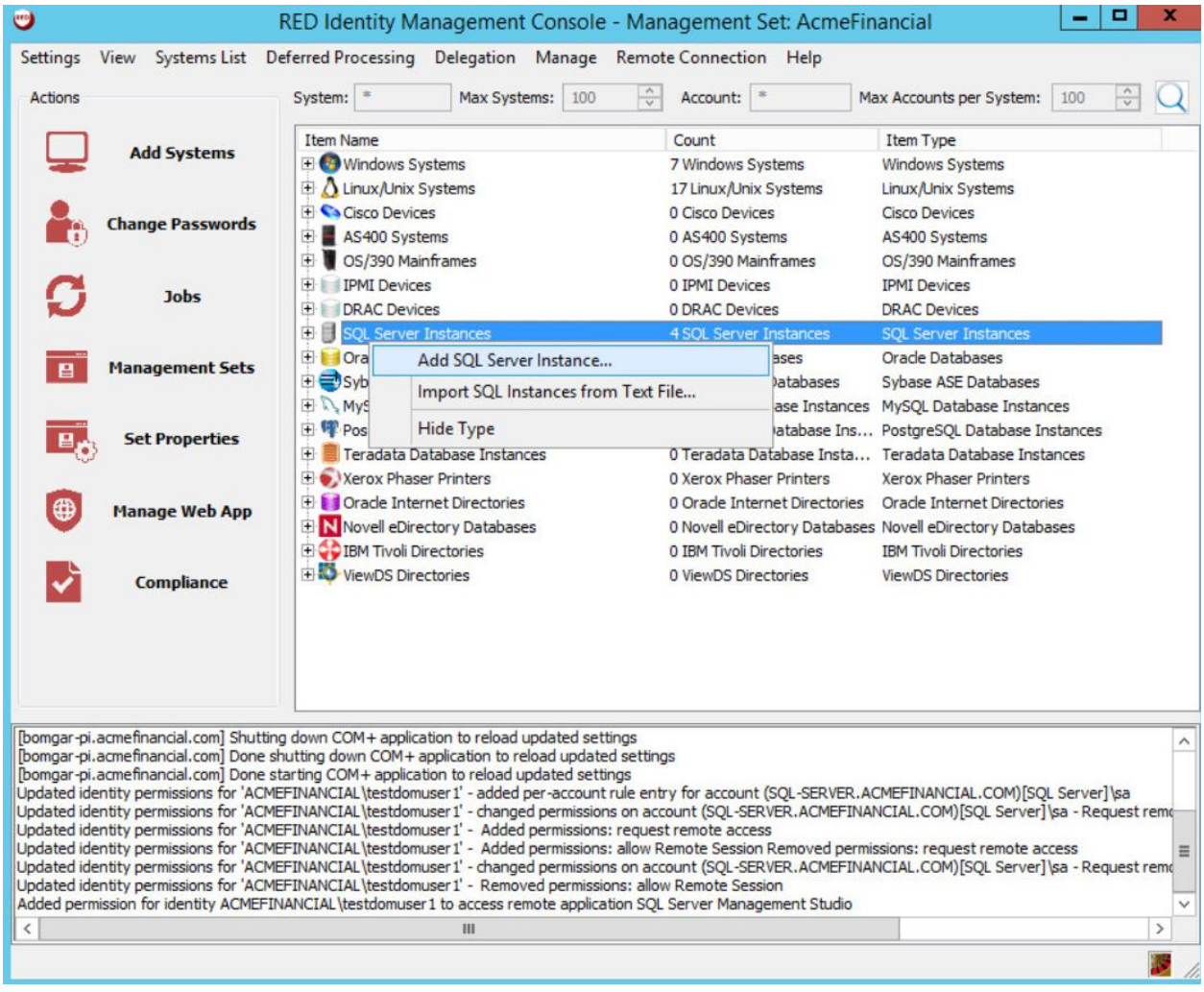
2.2.8 Configuring Microsoft SQL Server Access

Prerequisites:

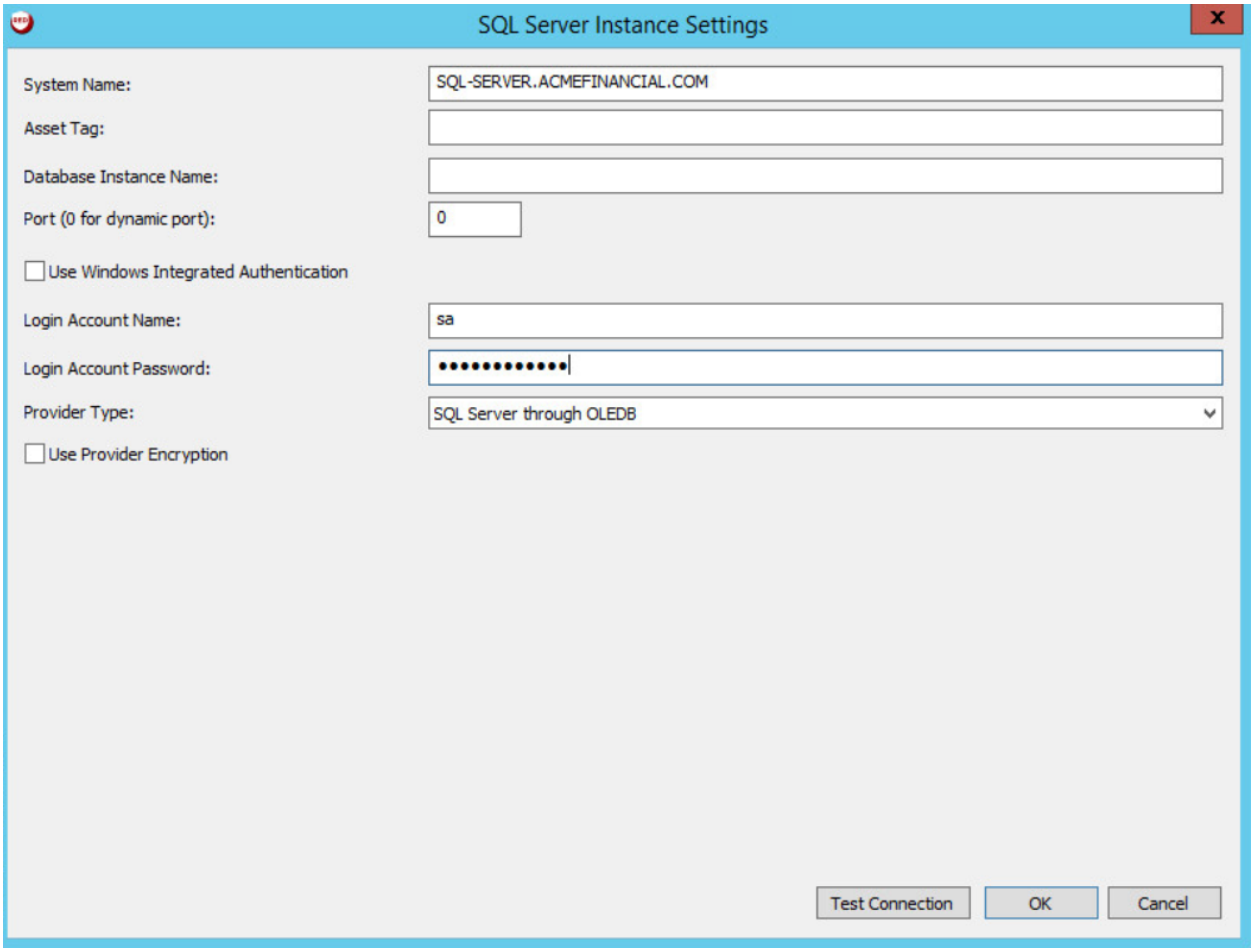
- Microsoft SQL Server has hybrid authentication.
- Microsoft SQL Server Management Studio (SSMS) has already been added as an application in the application launcher.

The following instructions configure Bomgar Privileged Identity to allow the **udb1** to request permission to launch Microsoft SSMS and to log in as the **sa** account on Microsoft SQL Server in the production environment.

1. Open the **Bomgar RED Identity Management Console** on Bomgar-PI. Right-click **SQL Server Instances,** and then select **Add SQL Server Instance.**

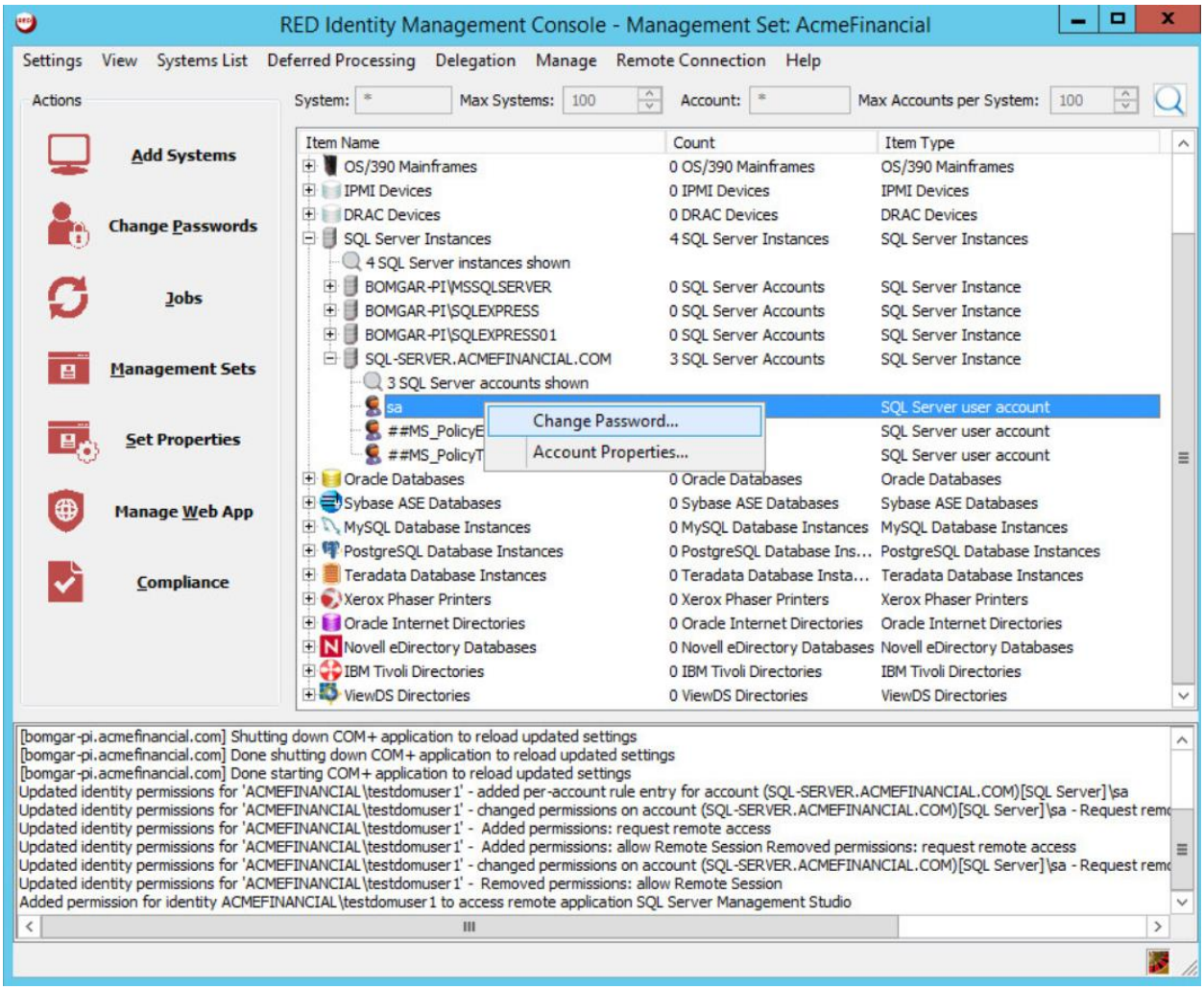


2. Fill out the **SQL Server Instance Settings.** Enter the host name of the SQL Server in the **System Name** field. Populate the **Login Account Name** and **Login Account Password** fields with the username and password of the **sa** account. Note: This will work only if hybrid authentication is enabled on the SQL Server.



3. Click **Test Connection.** The connection should be successful. Click **OK.**

4. Expand **SQL Server Instances** by clicking on the plus sign to the left of the item name, and then expand **SQL-SERVER.ACMEFINANCIAL.COM.** Right-click the **sa** account, and then select **Change Password.**

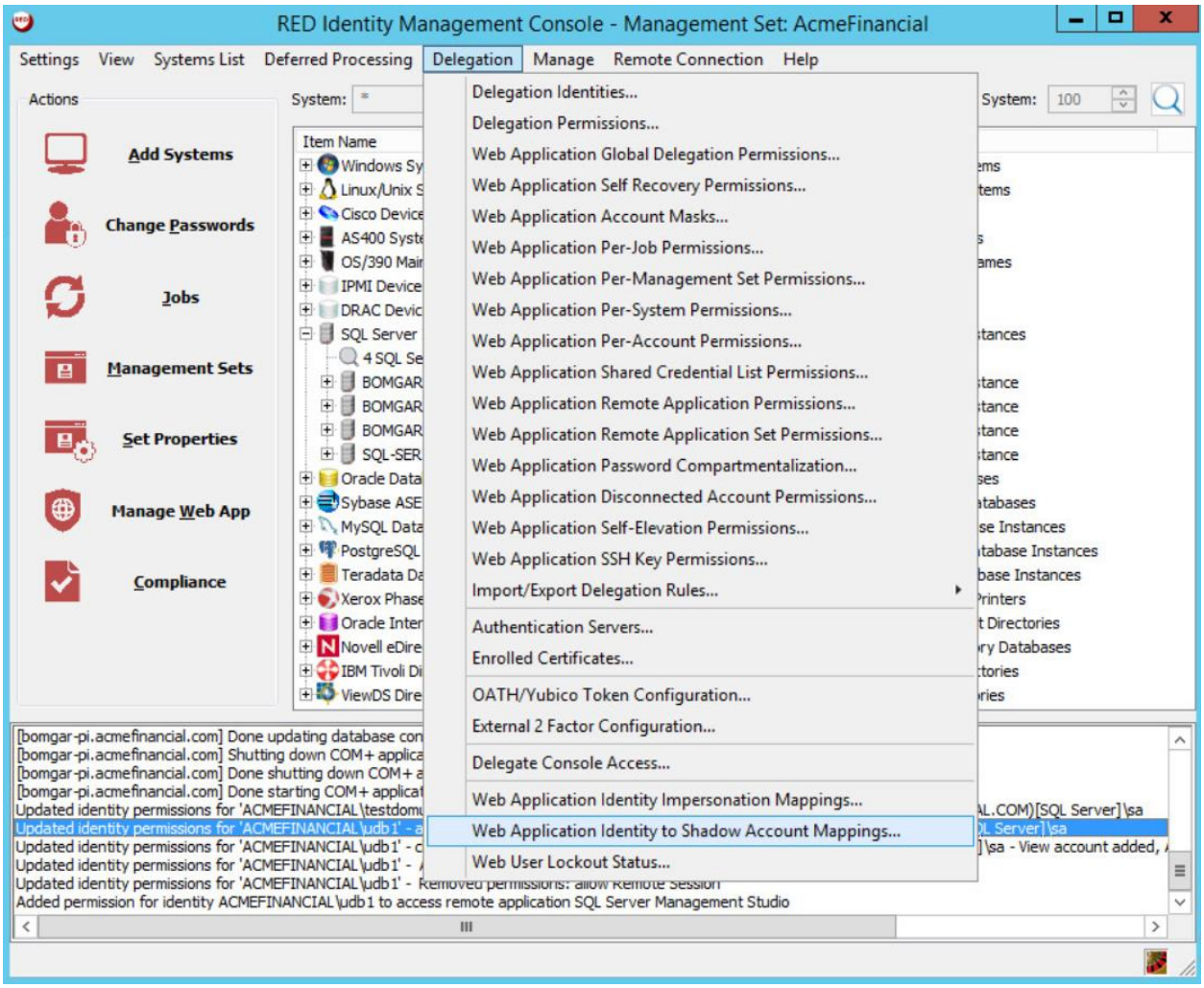


5. Select strong password policy options, such as increasing both the length of the password and its compliance with password standards.

6. On the **Schedule** tab, set the **Job Scheduling Period** to **Immediately,** and write a **Job Comment** to describe why this action is being taken.

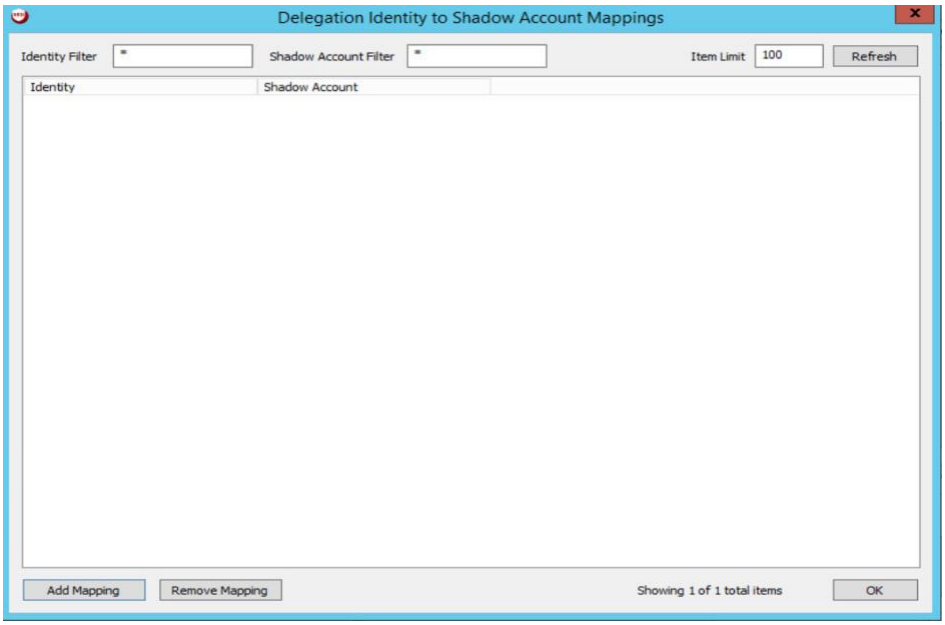
7. Click **OK,** and then let the operation complete.

8. Click **Delegation > Web Application Identity to Shadow Account Mappings.**



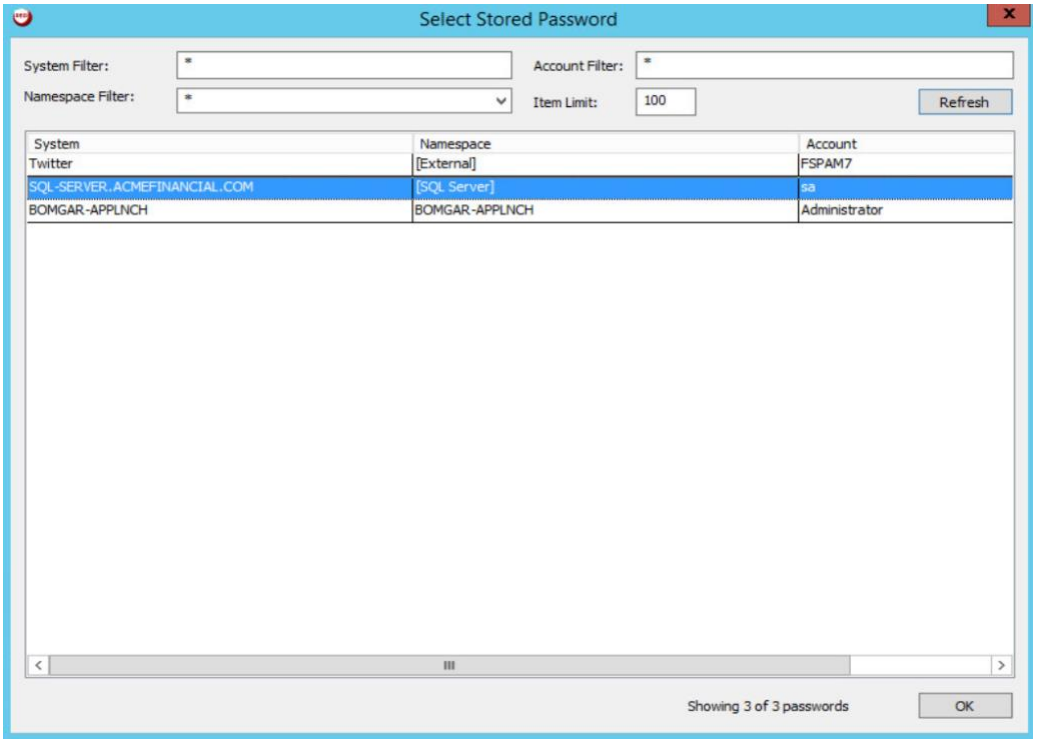
436

437 9. Click **Add Mapping.**



438

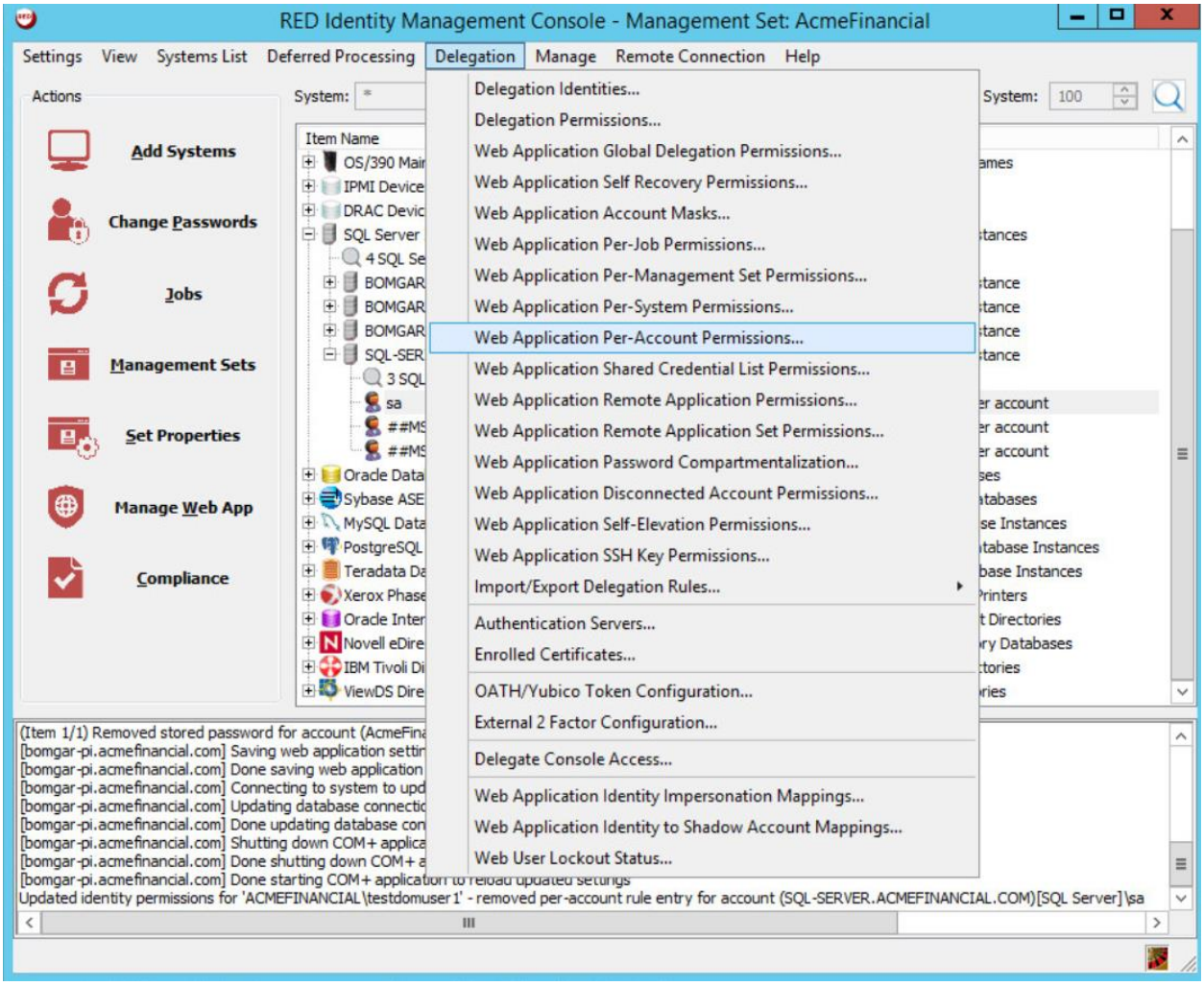
439 10. Choose the **ACMEFINANCIAL\udb1** account, and then click **OK.** Choose the **sa** account from the
440 list on the next screen, and then click **OK.**



441

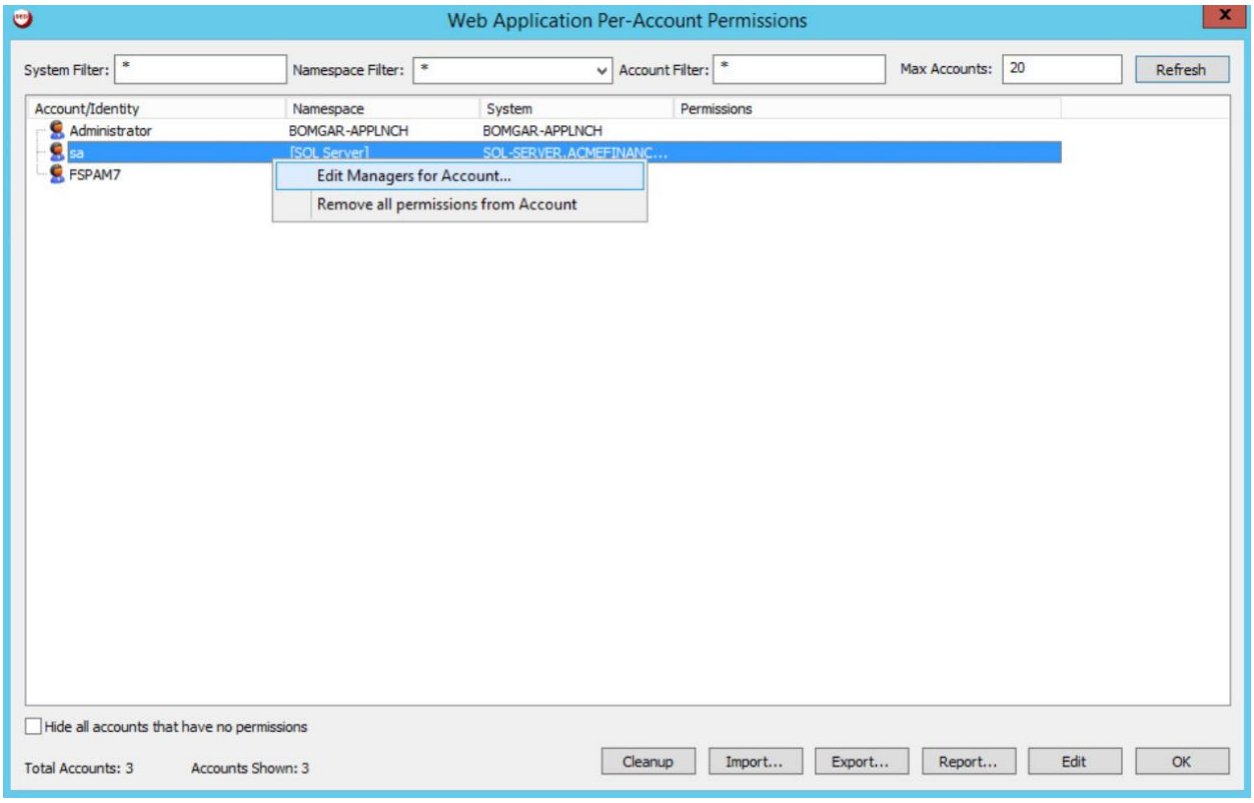
442 11. Click **OK** again.

443 12. Click **Delegation > Web Application Per-Account Permissions.**

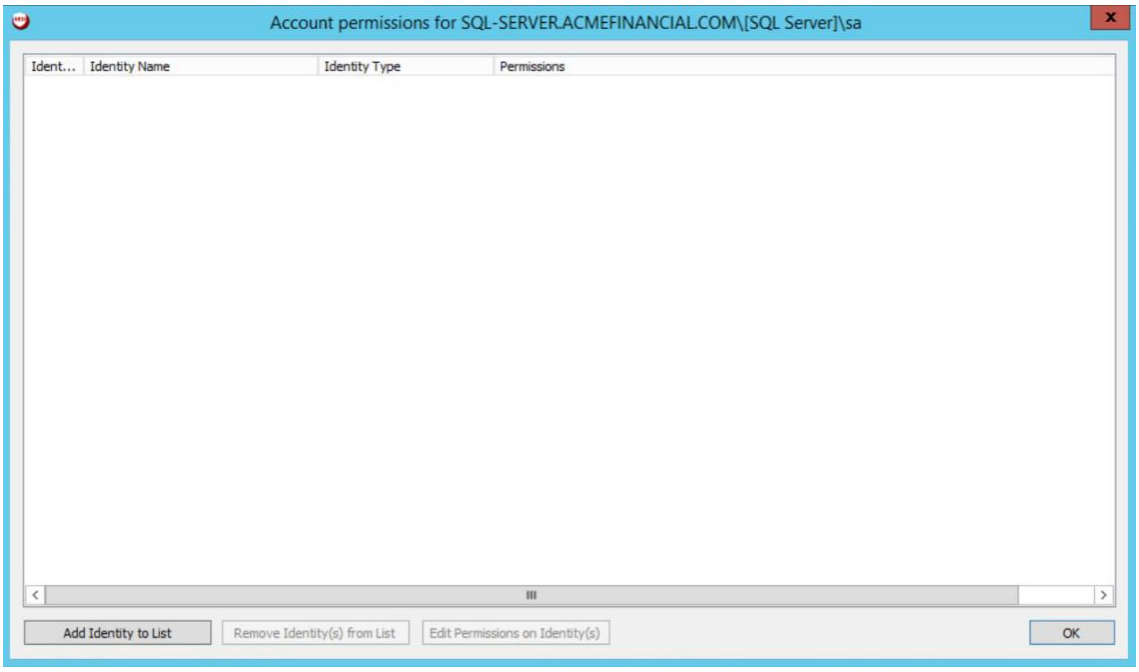


444

445 13. Right-click the **sa** account, and then select **Edit Managers for Account.**

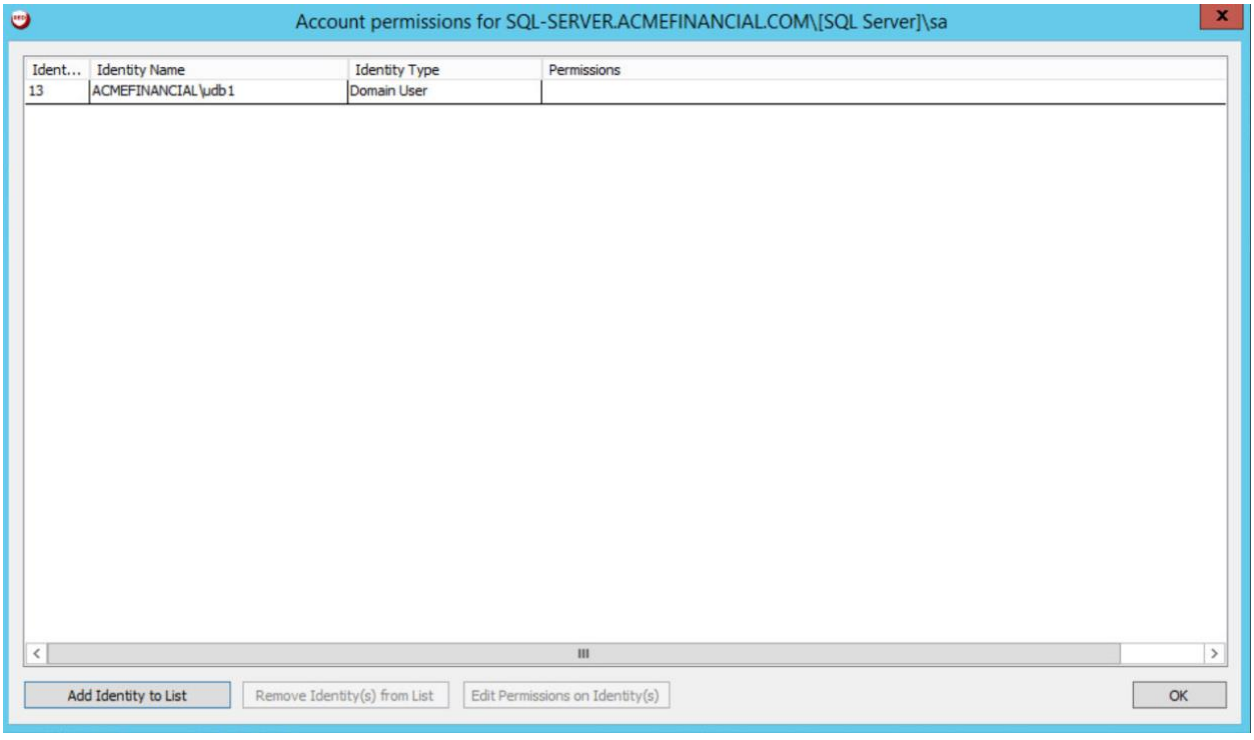


14. Click **Add Identity to List.**



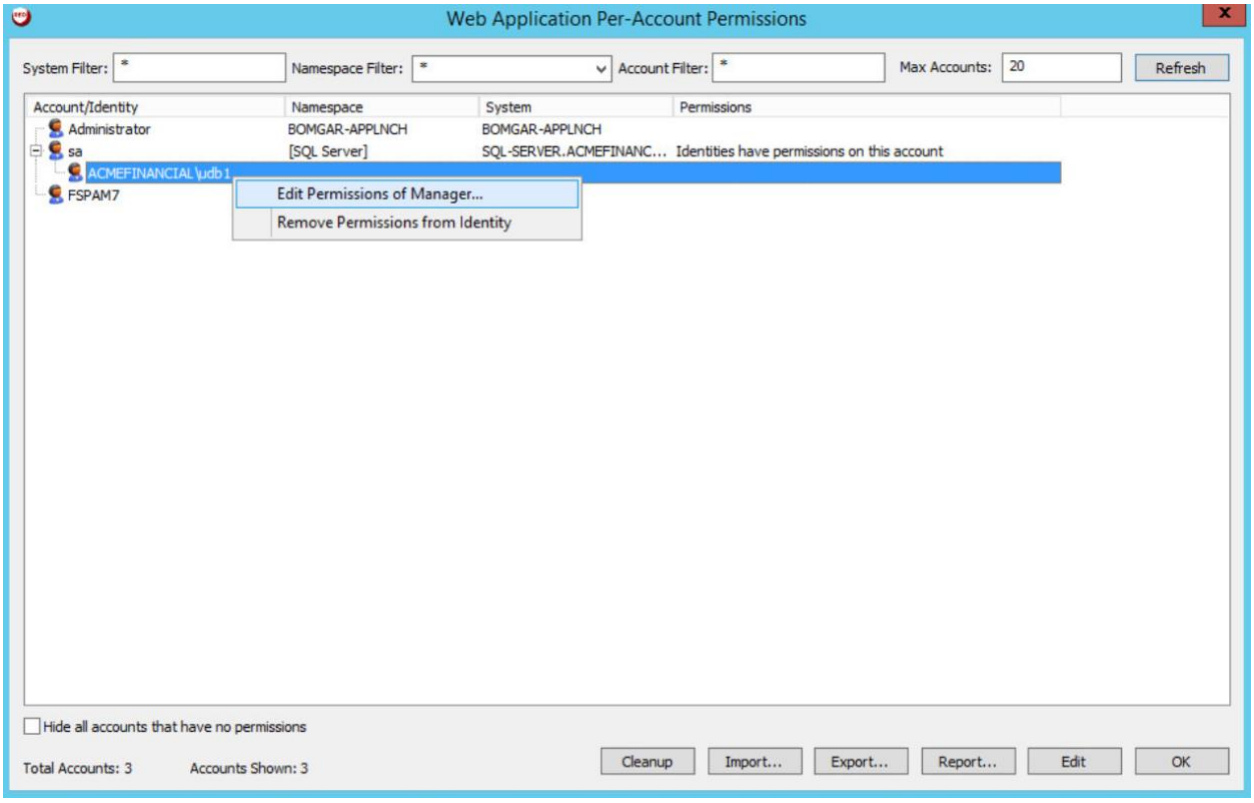
448

449 15. Select the **ACMEFINANCIAL\udb1** account. You should see it appear in the list. Click **OK.**



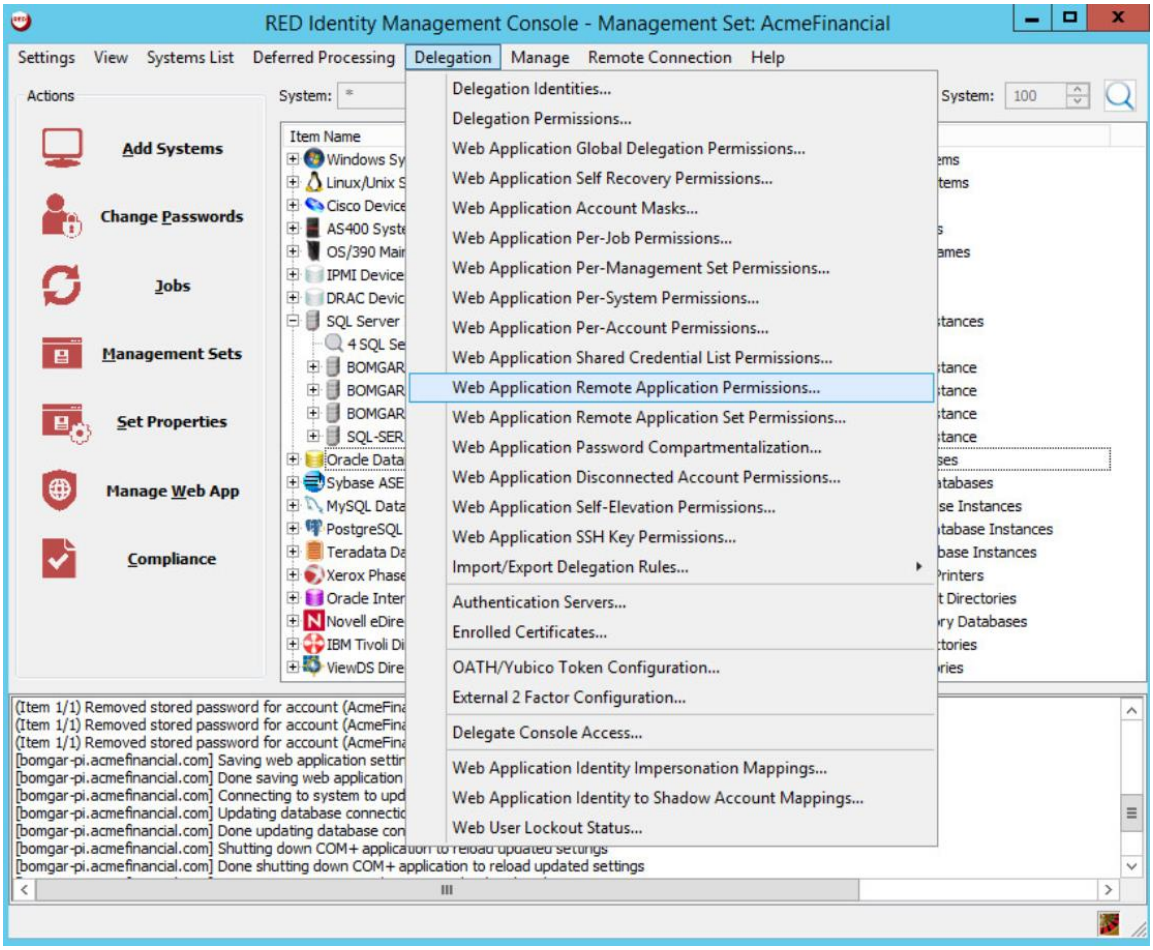
450

16. Expand the **sa** account by clicking the plus sign to the left, right-click the **ACMEFINANCIAL\udb1** account, and then select **Edit Permissions of Manager.**

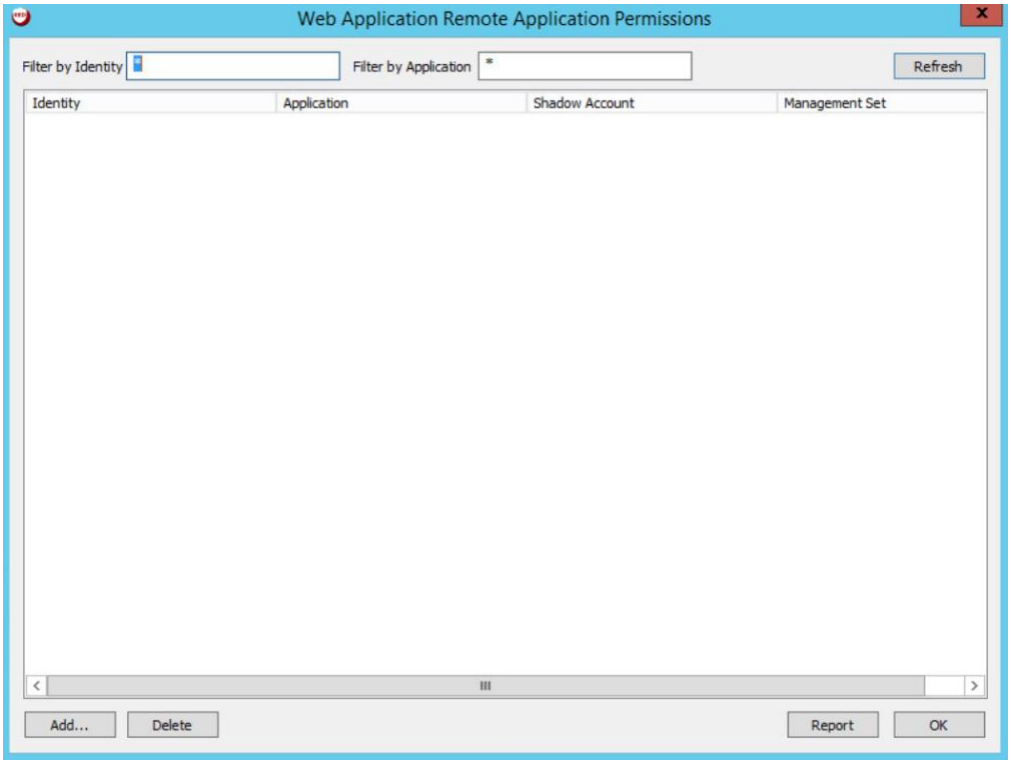


17. Give the account the **View Account** and **Request Remote Access** permissions. Click **OK**. Click **OK** again to exit the **Web Application Per-Account Permissions** window.

18. Click **Delegation > Web Application Remote Application Permissions.**

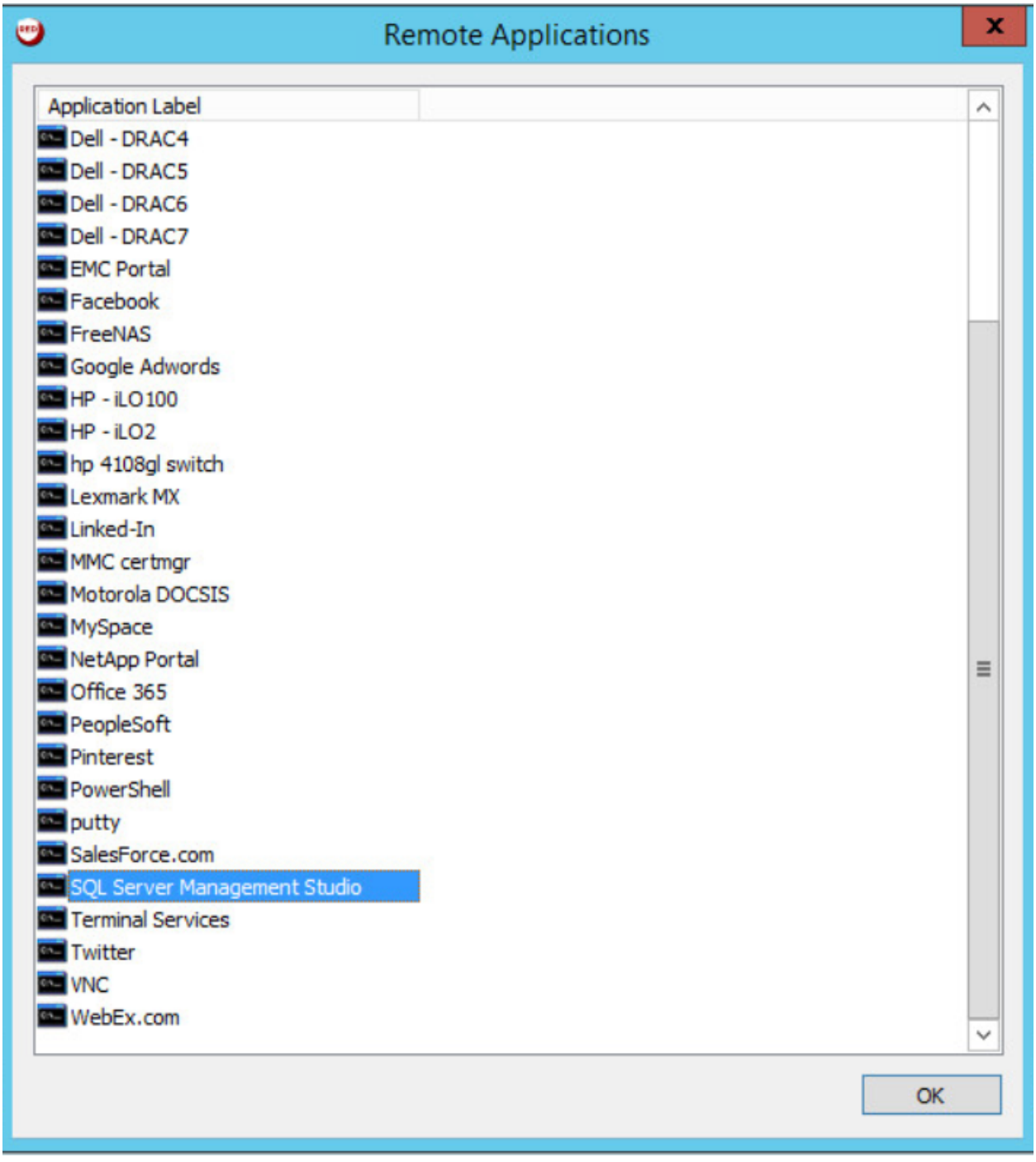

RED Identity Management Console - Management Set: AcmeFinancial
Settings
View
Systems List
Deferred Processing
Delegation
Manage
Remote Connection
Help
Actions
Add Systems
Change Passwords
Jobs
Management Sets
Set Properties
Manage Web App
Compliance
System:
Item Name
Delegation Identities...
Delegation Permissions...
Web Application Global Delegation Permissions...
Web Application Self Recovery Permissions...
Web Application Account Masks...
Web Application Per-Job Permissions...
Web Application Per-Management Set Permissions...
Web Application Per-System Permissions...
Web Application Per-Account Permissions...
Web Application Shared Credential List Permissions...
Web Application Remote Application Permissions...
Web Application Remote Application Set Permissions...
Web Application Password Compartmentalization...
Web Application Disconnected Account Permissions...
Web Application Self-Elevation Permissions...
Web Application SSH Key Permissions...
Import/Export Delegation Rules...
Authentication Servers...
Enrolled Certificates...
OATH/Yubico Token Configuration...
External 2 Factor Configuration...
Delegate Console Access...
Web Application Identity Impersonation Mappings...
Web Application Identity to Shadow Account Mappings...
Web User Lockout Status...
[bomgar-pi.acmefinancial.com] Done shutting down COM+ application to reload updated settings

19. Click **Add.**



459

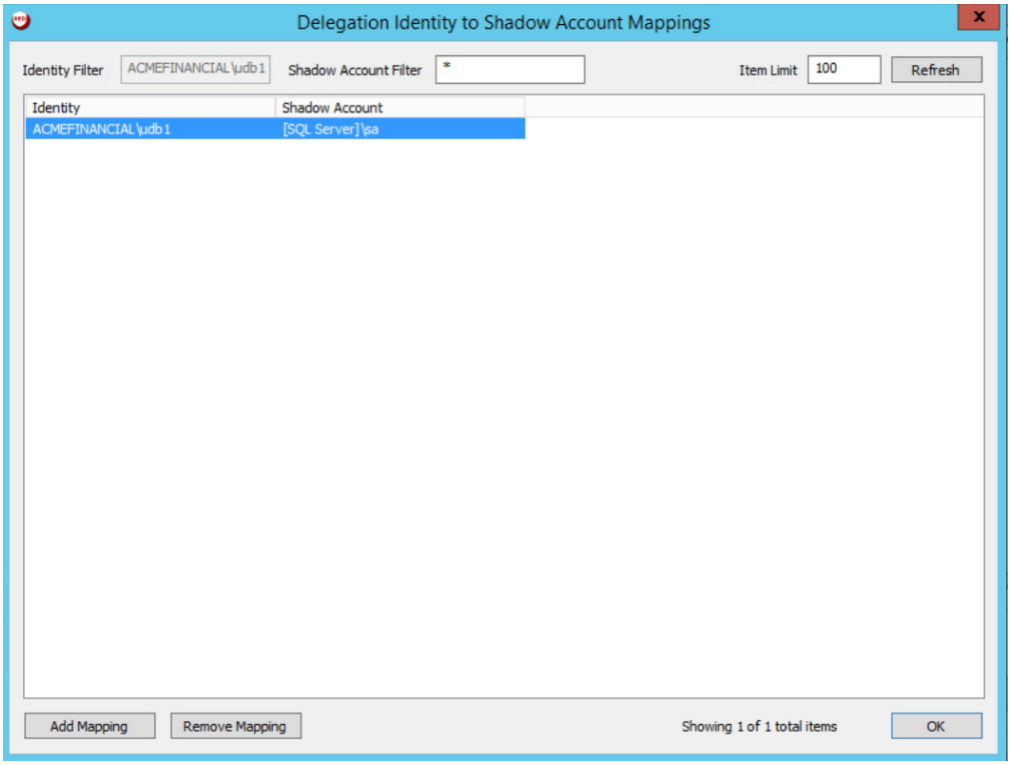
460 20. Select the **ACMEFINANCIAL\udb1** account from the list of **Delegation Identities.** Click **OK.** Next,
461 select **SQL Server Management Studio** from the list of **Remote Applications.**



462

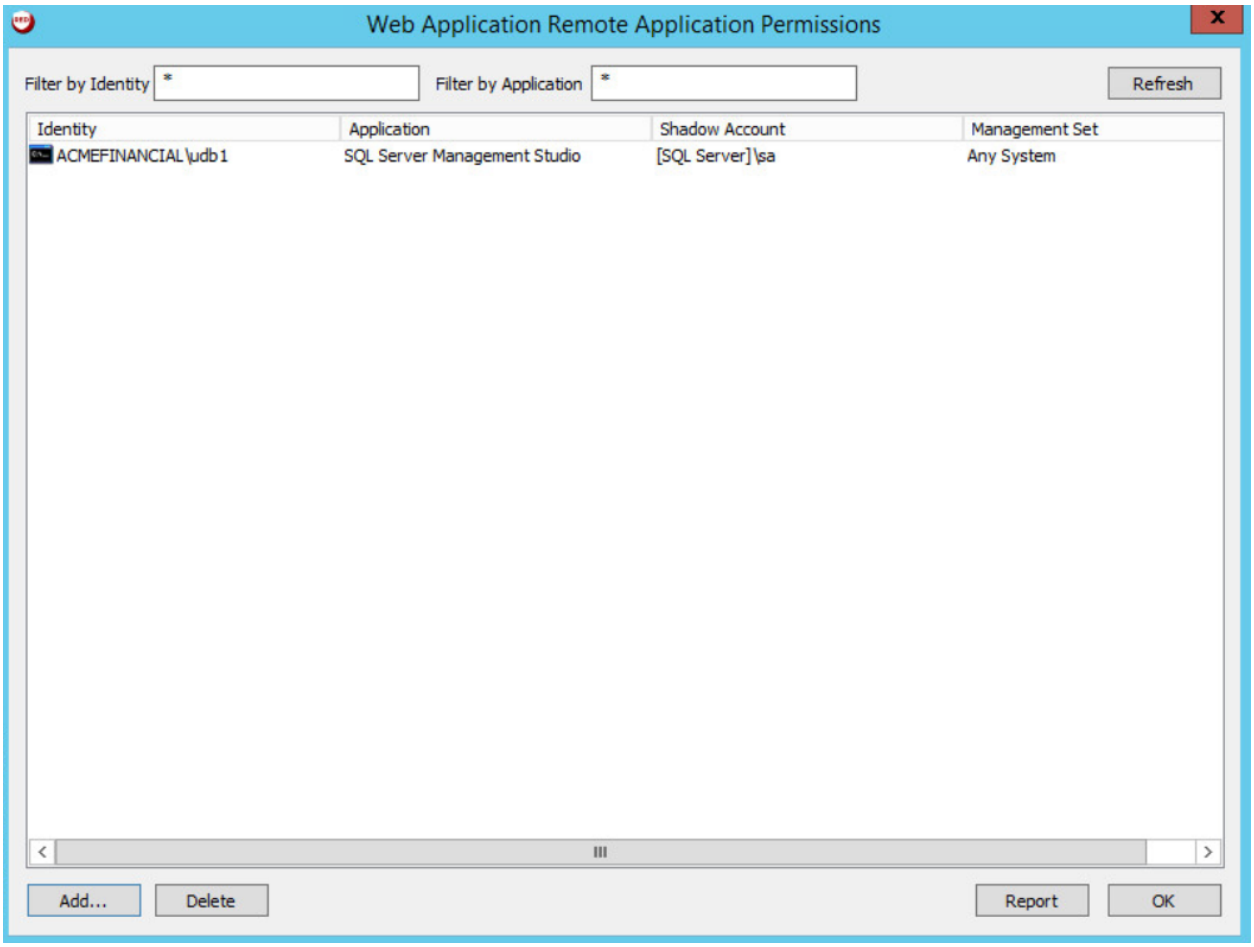
463 21. Select **Yes** for the pop-up about **Shadow Account Restriction.**

22. Select the **ACMEFINANCIAL\udb1** to **[SQL Server]\sa** shadow account mapping, and then click **OK.**



23. Select **No** for pop-up about the **System Target Restriction.**

24. You should see that the **ACMEFINANCIAL\udb1** user now has access to **SQL Server Management Studio** with the **[SQL Server]\sa** shadow account. Click **OK.**



2.2.9 Configuring Twitter Account Launching

The Bomgar application launcher comes with some premade scripts to launch various applications. One of these scripts launches Internet Explorer and automatically signs the user into a Twitter account. The following steps detail the process of configuring the script.

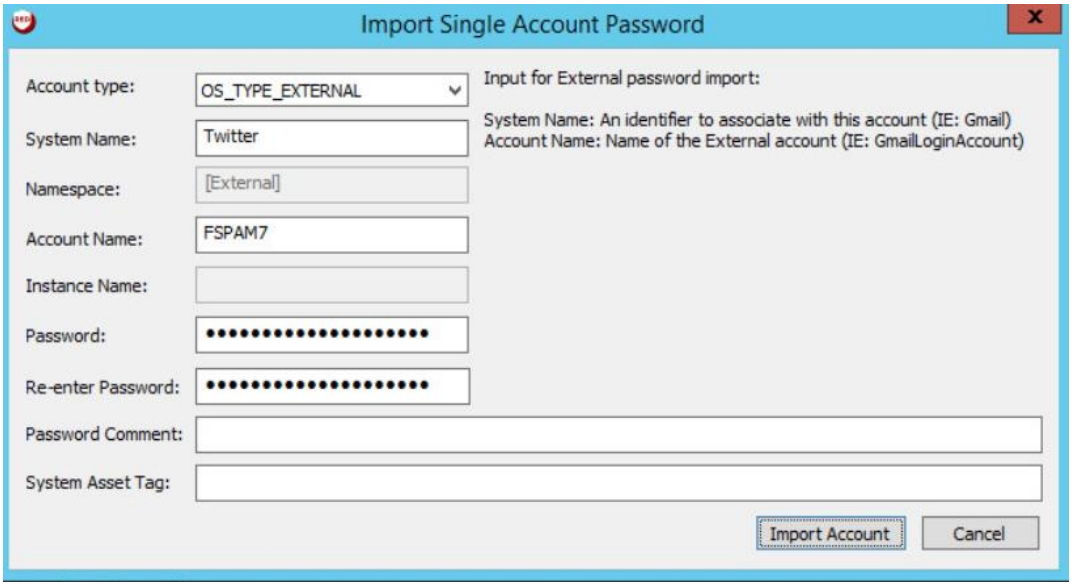
To launch Twitter, Bomgar-PI needs the Twitter account password. The following steps detail how to add an external password to Bomgar-PI:

1. In the **RED Identity Management Console,** select **Manage > Import Password Information > Import Password into Password Store.**
2. In the **Import Single Account Password** window, enter the following configuration:
    a. **Account type:** OS_TYPE_EXTERNAL
    b. **System Name:** Twitter

c. **Account Name:** <the Twitter account username>

d. **Password:** <the Twitter account password>

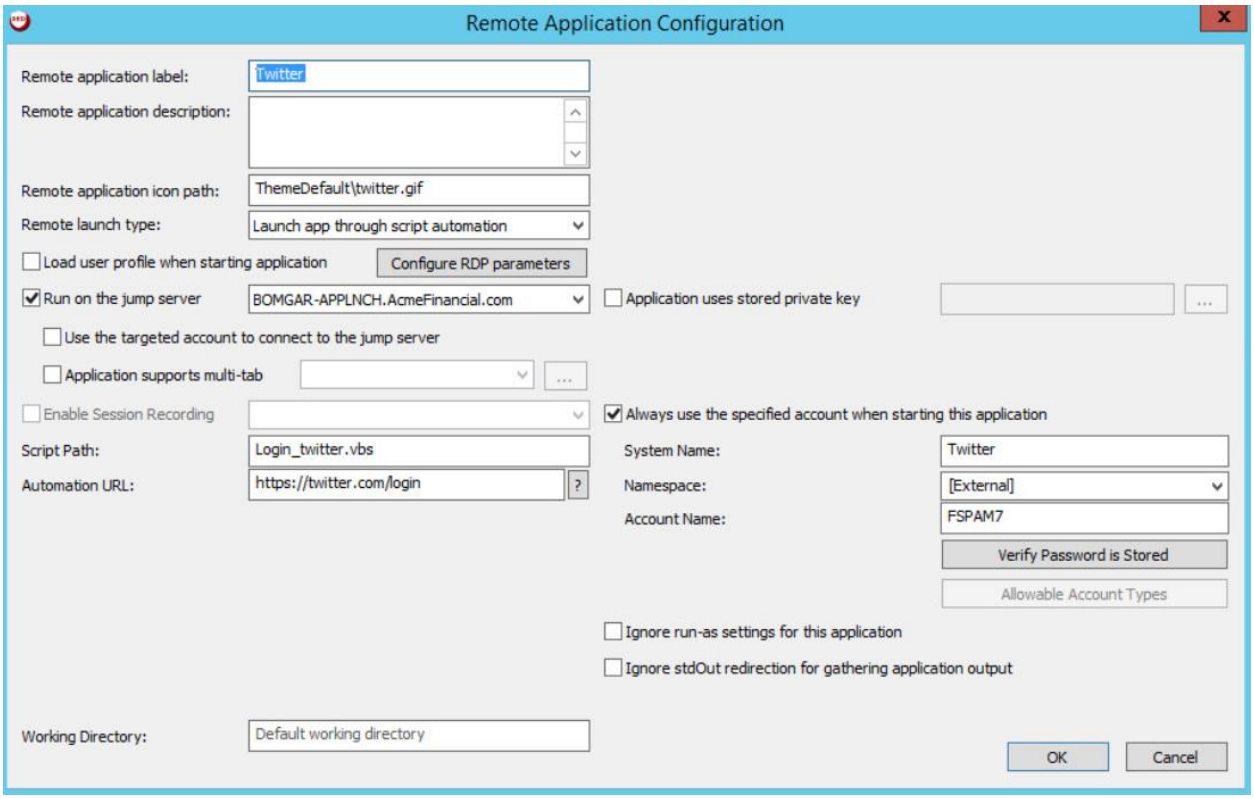
e. **Re-enter Password:** <the Twitter account password>



3. Click **Import Account.**

We can now configure Bomgar-PI to use that account to launch Twitter:

1. Go to **Settings > Manage Web Application > Application Launch.**
2. Scroll down, and double-click **Twitter.**
3. In the **Remote Application Configuration** window, enter the following information:
   a. **Run on the jump server:** BOMGAR-APPLNCH.AcmeFinancial.com
      i. This check box should be selected.
   b. **Automation URL:** https://twitter.com/login
   c. **Always use the specified account when starting this application:** This check box should be selected.
   d. **System Name:** Twitter
   e. **Namespace:** [External]
   f. **Account Name:** <the Twitter account username>



4. Click **OK,** then **OK,** and then **OK** again.

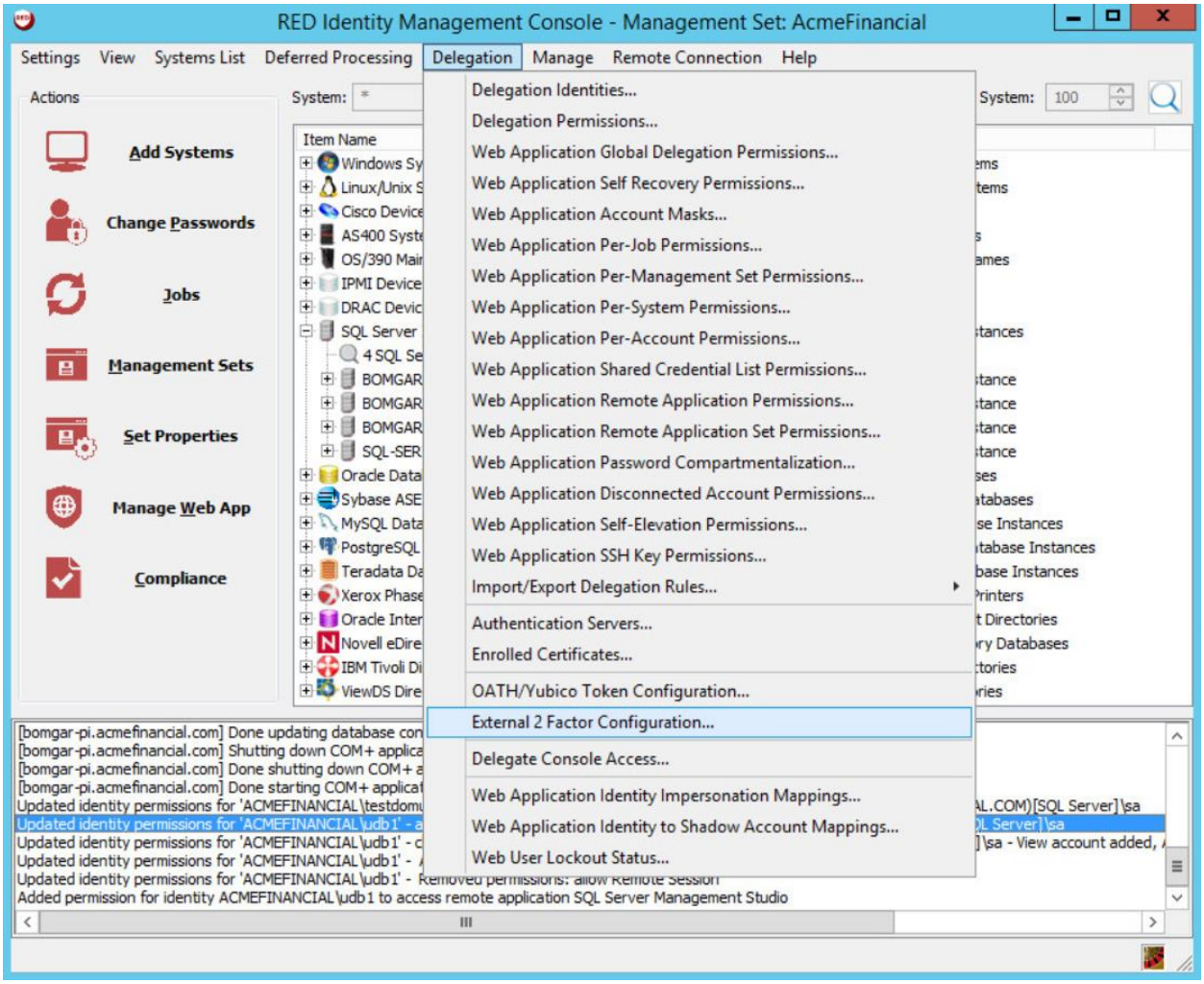
To allow users to launch Twitter, follow these steps:

1. Open **Delegation > Web Application Remote Application Permissions.**
2. Click **Add.**
3. Select the identity that should be allowed to launch Twitter. More identities can be added by clicking **Add Identity.**
4. Click **OK.**
5. Select the Remote Application **Twitter,** and then click **OK.**
6. Select **No** for the pop-up about **Shadow Account Restriction.**
7. Select **No** for the pop-up about **System Target Restriction.**
8. Click **OK.**

2.2.10 Configuring Multifactor Authentication with RSA

The following steps detail how Bomgar Privileged Identity was configured to authenticate users by using a SecurID from RSA. In summary, Bomgar acts as a RADIUS client to an RSA Authentication Manager. Bomgar is configured to prompt for a onetime passcode after authenticating the user with AD.

1. In the **RED Identity Management Console,** select **Delegation > External 2 Factor Configuration.**



2. Fill out the **Configure 2 Factor Authentication** window with the following settings:
    a. **Authenticator Type:** RADIUS
    b. **Authenticator Label:** RSA Auth
    c. **IP address:** 172.16.2.15 (the IP address of the RSA Authentication Manager)

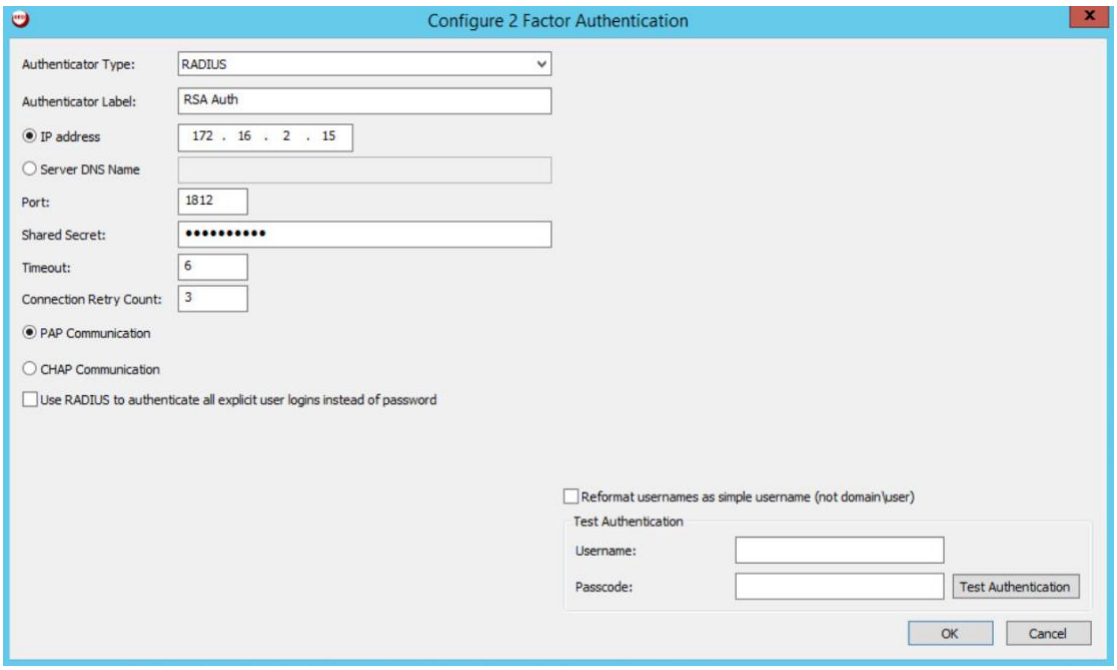
d. **Port:** 1812

e. **Shared Secret:** <the shared secret from RSA for RADIUS clients>

f. **Timeout:** 6

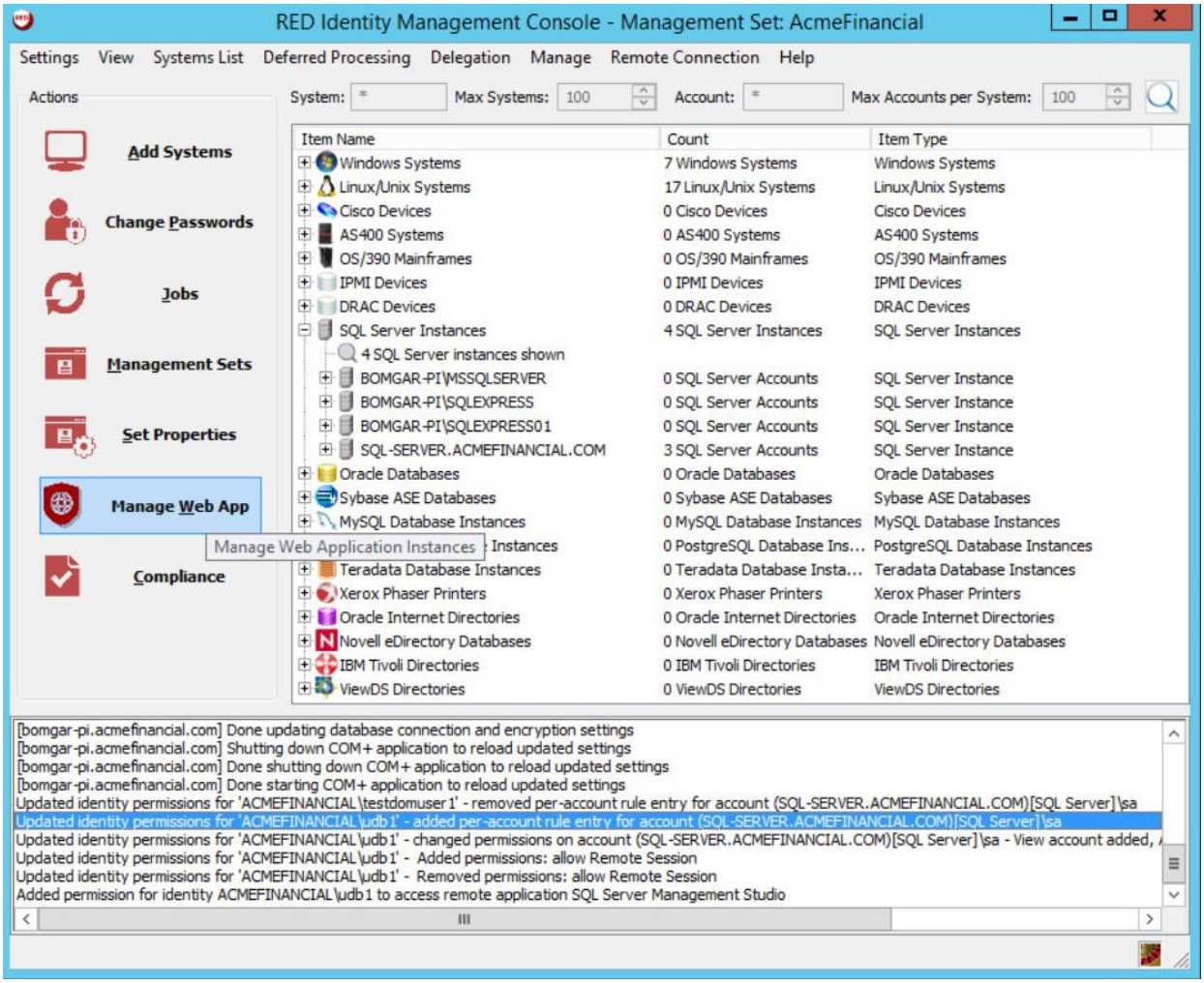
g. **Connection Retry Count:** 3

h. **PAP Communication:** This check box should be selected.



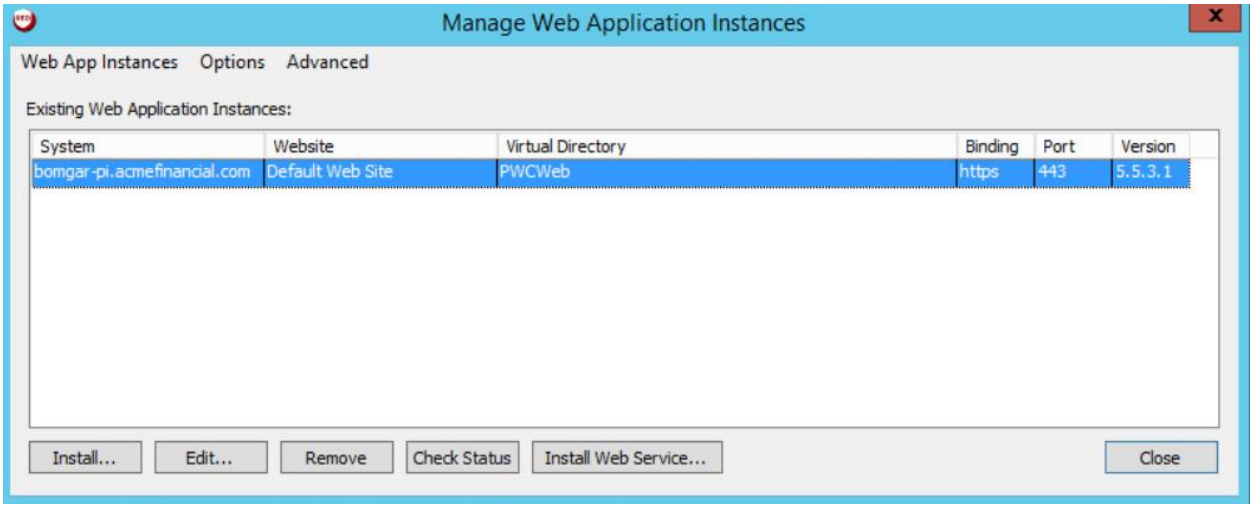
3. Click **OK.**

4. Click **Manage Web App.**



529

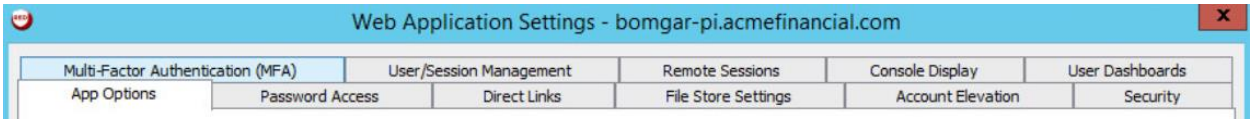
530 5. In the **Manage Web Application Instances** window, double-click the Web Application Instance.



531

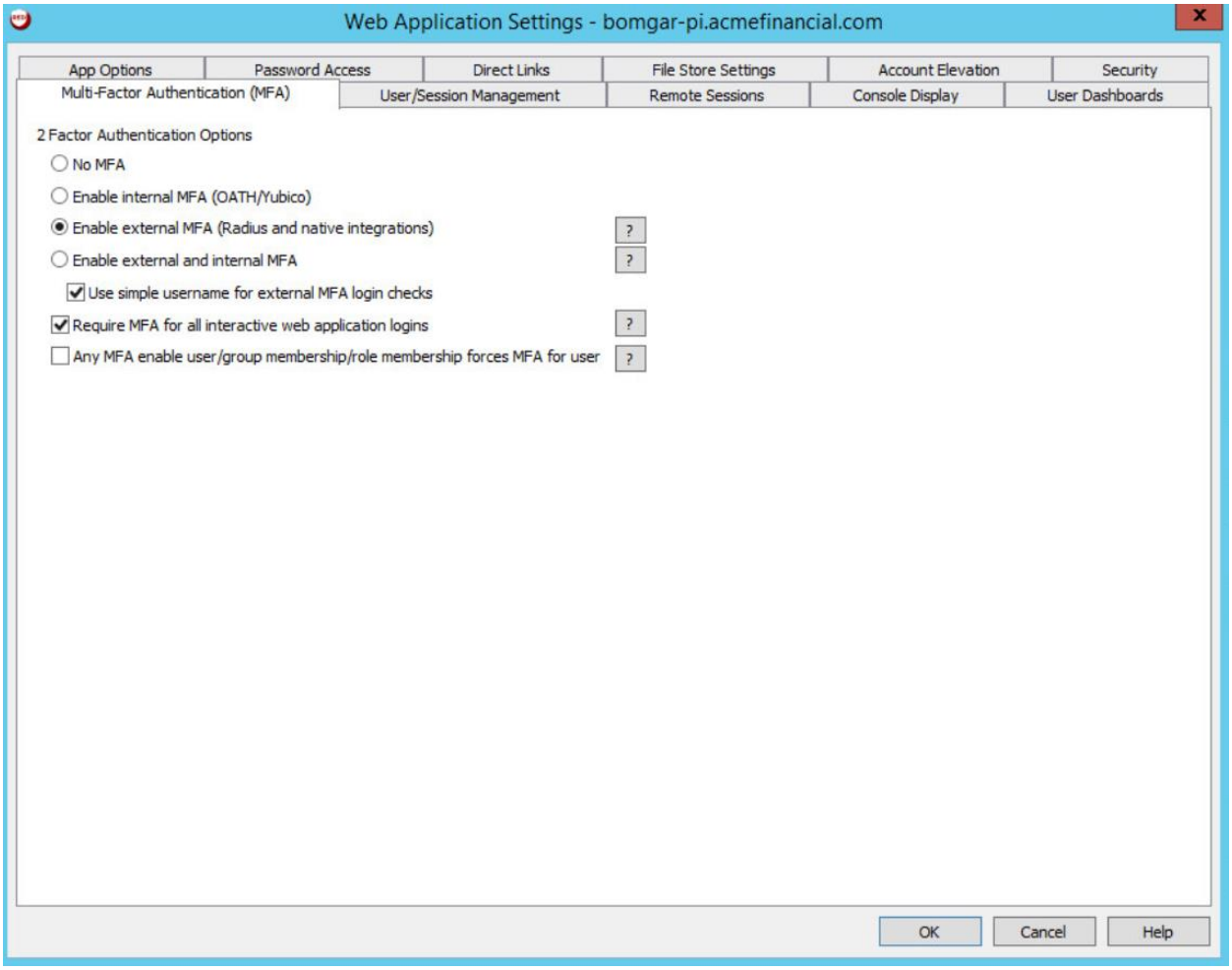
532 6. Click **Yes.**

533 7. Click the tab labeled **Multi-Factor Authentication (MFA).**



534

535 8. Select **Enable external MFA (RADIUS and native integrations), Use simple username for**
536 **external MFA login checks,** and **Require MFA for all interactive web application logins.**



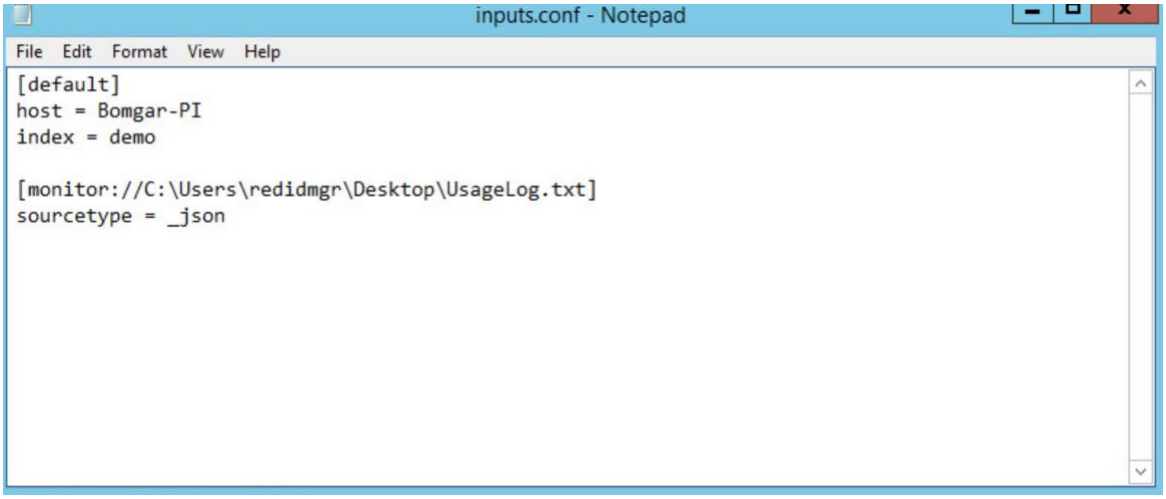
9. Click **OK.** Click **OK** again in the pop-up window.

10. Click **Close.**

2.2.11 Splunk Universal Forwarder

Install Splunk Universal Forwarder by following the instructions provided at http://docs.splunk.com/Documentation/Forwarder/7.1.3/Forwarder/Abouttheuniversalforwarder.

Edit the *inputs.conf* file to monitor and forward logs from the *UsageLog.txt* file to the **demo** index at Splunk Enterprise. Use the built-in **_json sourcetype.**



2.3 TDi ConsoleWorks

TDi ConsoleWorks is a PAM solution that allows for proxying terminal and web connections through a web interface.

2.3.1 How It's Used

TDi ConsoleWorks provides PAM for accounts accessing Splunk and the router/firewall configuration web page.

2.3.2 Virtual Machine Configuration

The TDi ConsoleWorks virtual machine is configured as follows:

- CentOS 7
- 2 CPU cores
- 8 GB of RAM
- 75 GB of storage
- 1 NIC

Network Interface Configuration:

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.4.11
- Netmask: 255.255.225.0

- Gateway: 172.16.4.1
- DNS servers: 172.16.3.10
- DNS-search domain: N/A

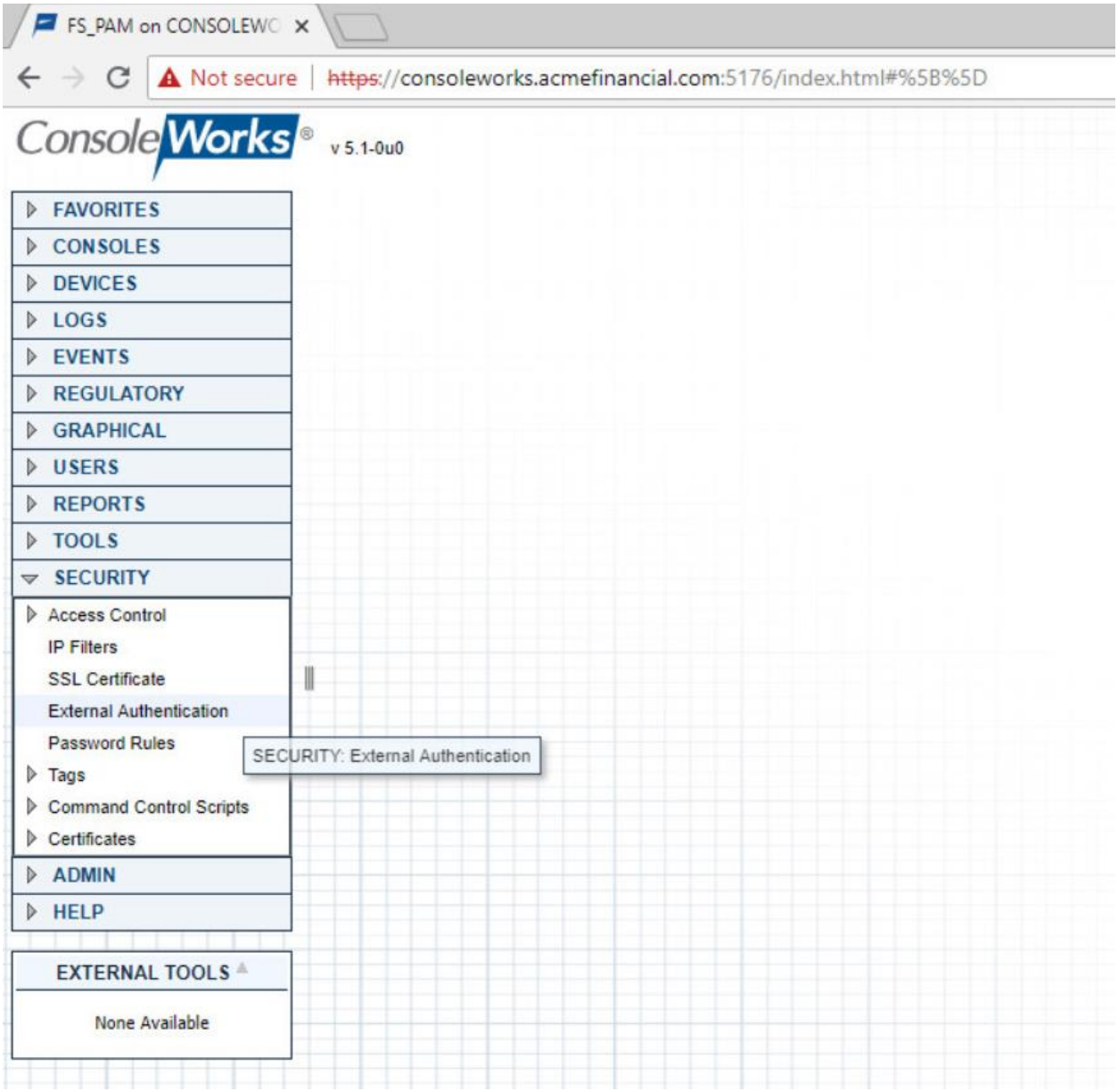
2.3.3 Installation

Installation documentation is provided on TDi's website, but an account with TDi Technologies is necessary to access it. A basic installation was used in this project.

2.3.4 Configuration of Back-End Authentication

The following steps describe how ConsoleWorks was configured to authenticate users with the IDENTIKEY Authentication Server.

1. Log in as a user with the CONSOLE_MANAGER role.
2. Click **SECURITY > External Authentication.**



3. Click **Add.**

4. Fill out the **External Authentication Record** with the following information for the IDENTIKEY Authentication Server:

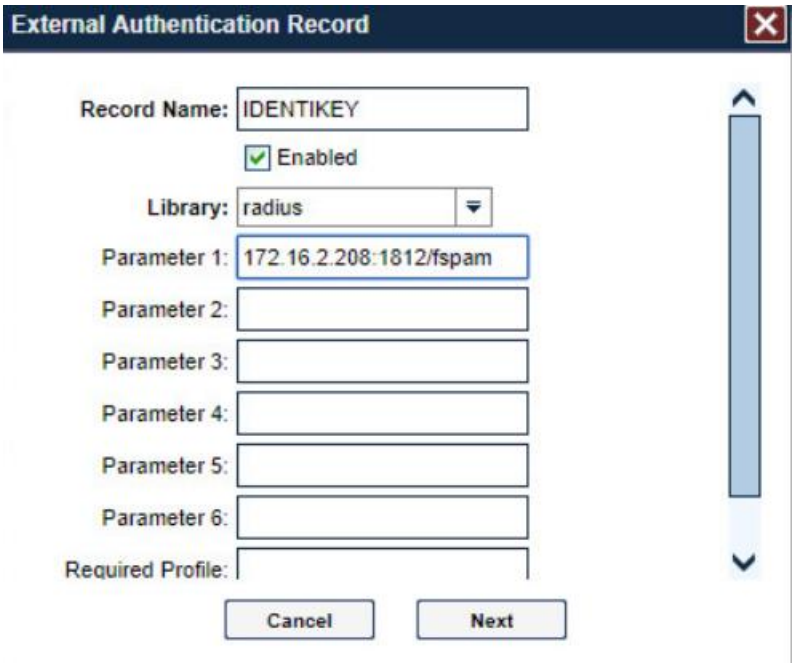
    a. **Record Name:** IDENTIKEY

    b. **Enabled:** This check box should be selected.

c. **Library:** radius

d. **Parameter 1:** 172.16.2.208:1812/fspam

Note: Parameter 1 specifies the IP address (or host name) of the RADIUS server, followed by the port and then the shared secret in the format [ip address]:[port]/[shared secret].

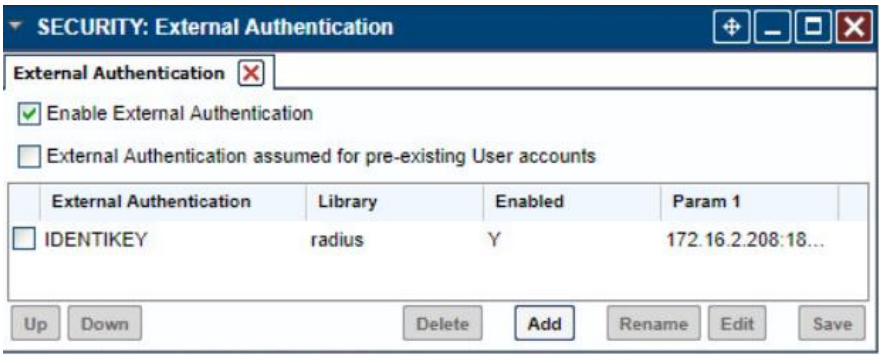


5. Click **Next,** and then click **Next** again.

6. Check that the verification passed. The user should be denied. Click **Next.**

7. Click **Save.**

8. Make sure that the **Enable External Authentication** check box is selected in the **SECURITY: External Authentication** window.

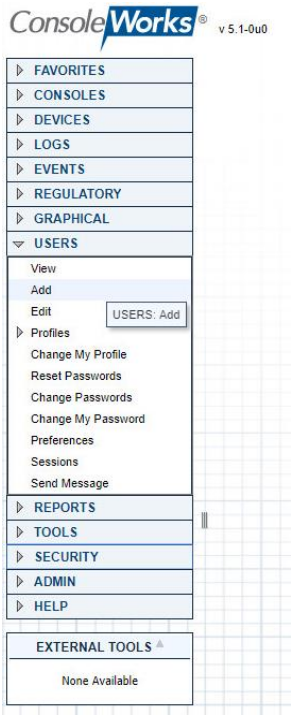


9. Click **Save** if available.

2.3.5 Creating Users

Each privileged user must have an account in ConsoleWorks to log into ConsoleWorks. The following steps detail the process of creating accounts for AD users in ConsoleWorks. For this example, we will create a ConsoleWorks account for the splunk_admin@acmefinancial.com AD account. This user will manage the Splunk virtual-machine OS.

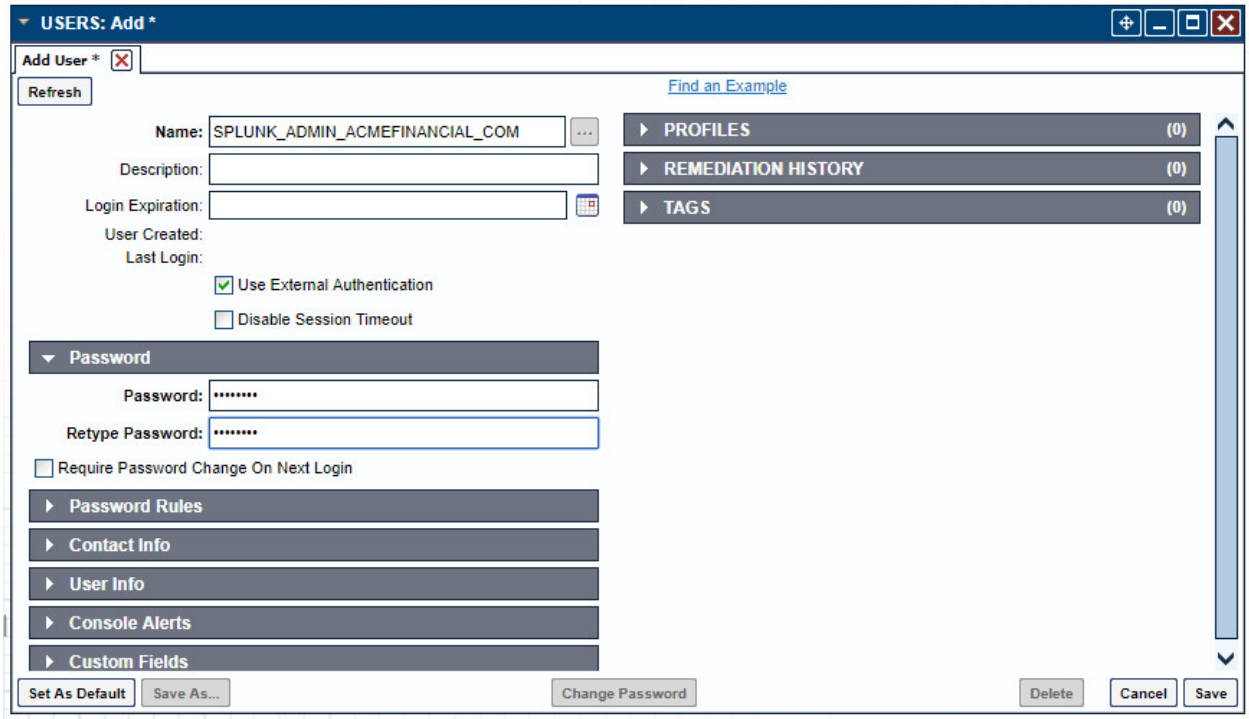
1. In ConsoleWorks, click **USERS > Add** as a CONSOLE_MANAGER account.



2. Fill out the pop-up window with the following information:
    a. **Name:** SPLUNK_ADMIN_ACMEFINANCIAL_COM
    b. **Use External Authentication:** This check box should be selected.
    c. Enter a dummy password in the **Password** field, and then retype it in the **Retype Password** field.
    d. **Require Password Change on Next Login:** This check box should not be selected.

    Note: The format USERNAME_DOMAIN_NAME is important. This is how ConsoleWorks expects a user with the fully qualified domain name (FQDN) **username@domain.name** to be named in the product.

3. Click **Save.**



612

613 2.3.6 Creating Tags

614 Tags in ConsoleWorks allow consoles to be easily identified as part of a certain group. We will create a
615 tag for the consoles that should be accessible to users who need OS-level access to the Splunk virtual
616 machine.

617 1. Click **SECURITY > Tags > Add.**

618 2. Fill out the pop-up window with the following information:

619 a. **Name:** SPLUNK_OS

620 b. (optional) **Description:** Splunk OS Consoles

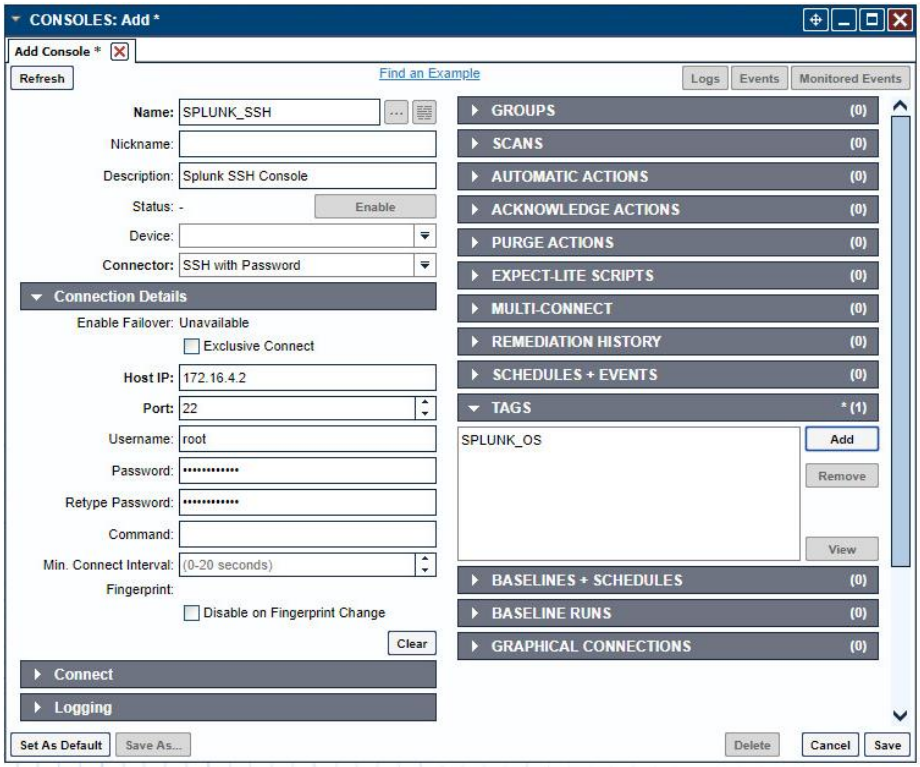
621 3. Click **Save.**

622 2.3.7 Creating SSH Consoles

623 Managed assets must have a “console” entry in ConsoleWorks for privileged users to connect to them.
624 The following steps detail how to create a console for SSH access to the Splunk virtual machine that an
625 administrator (admin) (e.g., splunk_admin) would use.

626 1. Click **CONSOLES > Add.**

2. Fill out the pop-up window with the following information:
    a. **Name:** SPLUNK_SSH
    b. (optional) **Description:** Splunk SSH Console
    c. **Connector:** SSH with Password
    d. **Connection Details:**
        i. **Host IP:** 172.16.4.2
        ii. **Port:** 22
        iii. **Username:** root
        iv. **Password:** fspam@nccoe1
        v. **Retype Password:** fspam@nccoe1
    e. **TAGS:** Add the tag **SPLUNK_OS,** which we created earlier, to this console by clicking **Add** and then entering SPLUNK_OS.

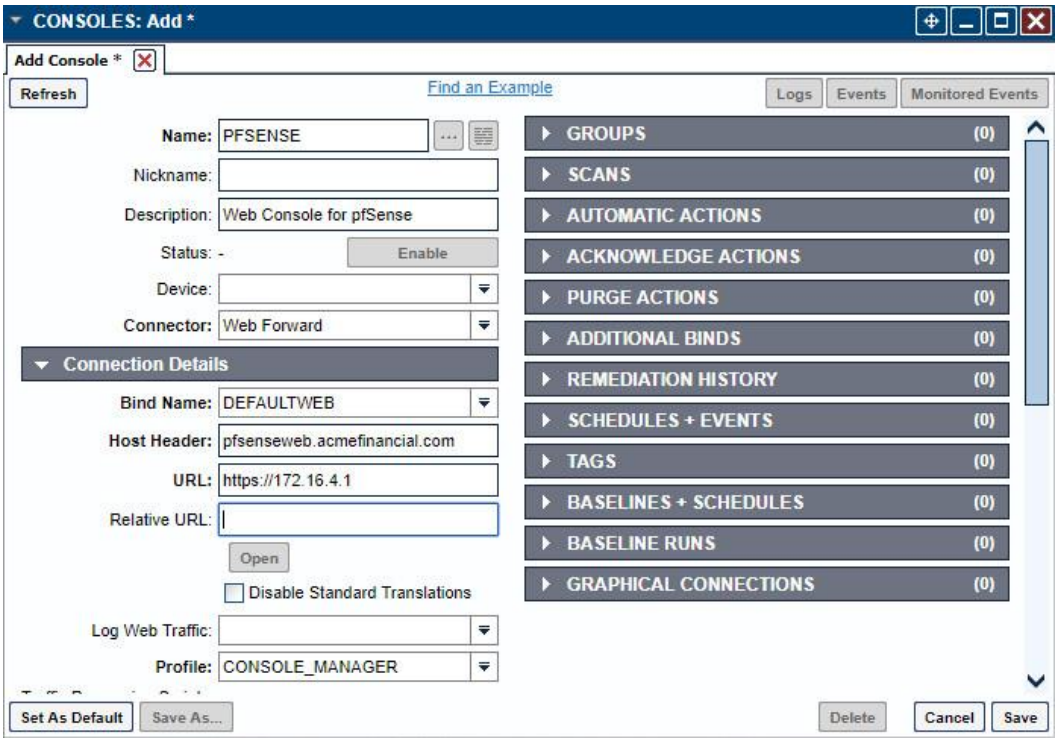


3. Click **Save.**

2.3.8 Creating Web Consoles

The following steps describe how to create a console for a web application. ConsoleWorks will proxy a connection to the managed asset, allowing for monitoring of user activity on the managed asset. These steps were completed twice: once for the Splunk web interface and again for a pfSense router/firewall. The following steps describe the configuration for pfSense:

1. On the AD Domain Controller, which acts as a DNS server, open **DNS Manager.**
2. Double-click the **AcmeFinancial.com** object.
3. Double-click the **Forward Lookup Zone** object.
4. Right-click in the area with DNS records, and select **New Host (A or AAAA).**
5. In the **Name** field, enter pfsenseweb.
6. In the **IP address** field, enter the IP address of the ConsoleWorks virtual machine. In this case, it is 172.16.4.11.
7. Click **Add Host.**
8. In ConsoleWorks' web interface, log in as a CONSOLE_MANAGER.
9. Click **CONSOLES > Add.**
10. Fill out the window **CONSOLES: Add** window with the following information:
    a. **Name:** PFSENSE
    b. **Description:** Web Console for pfSense
    c. **Connector:** Web Forward
    d. **Connection Details:**
        i. **Bind Name:** DEFAULTWEB
        ii. **Host Header:** pfsenseweb.acmefinancial.com
        iii. **URL:** https://172.16.4.1
        iv. **Profile:** CONSOLE_MANAGER



Note: In the case where the URL is not just the host name, the rest of the URL after the forward slash should be put in **Relative URL.**

11. Click **Save.**

2.3.9 Assigning Tags to Consoles

We created a unique tag to identify each group of consoles. Specifically, we created tags for the following console groups:

- pfSense consoles
- Splunk application-level consoles
- Splunk OS-level consoles
- Ekran Server consoles

Even though each of these groups has only one console in it, organizing the consoles this way makes it easy to add more consoles to the groups later.

The following steps describe the process for assigning a tag to a console:

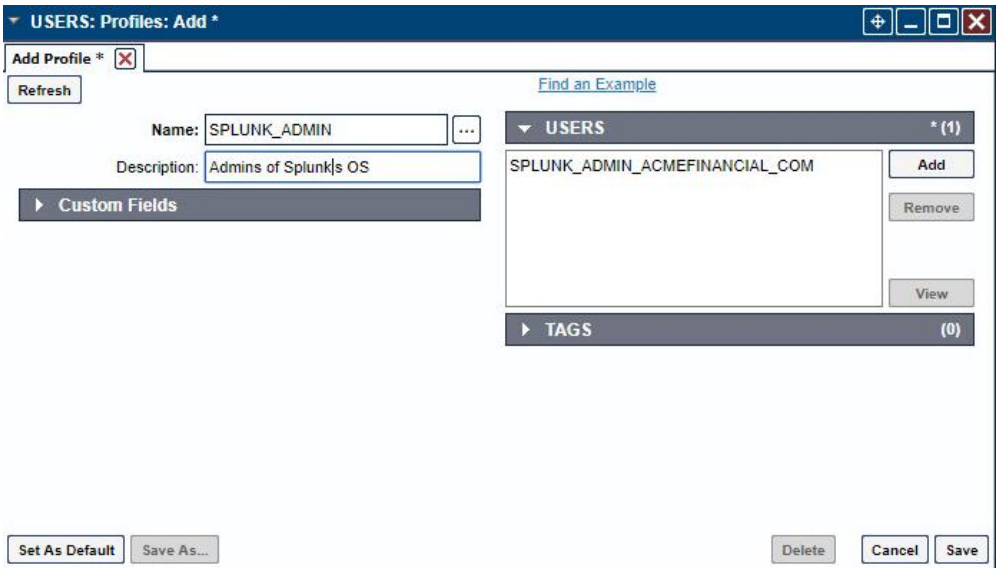
1. In ConsoleWorks, click **CONSOLES > View.**
2. Select a console (e.g., **PFSENSE**).
3. Click **Edit.**
4. Open the **TAGS** menu, and then click **Add.**
5. Move the pfSense consoles' tag to the list on the right, and then click **OK.**
6. Click **Save.**

2.3.10 Creating Profiles for Users

Profiles in ConsoleWorks are like groups in Windows. Users can be added to profiles, and those profiles can be assigned permissions, such as access to a specific set of consoles.

The following steps describe creating a SPLUNK_ADMIN profile that will eventually allow users who have access to this profile to access the Splunk OS-level console:

1. Click **USERS > Profiles > Add.**
2. Fill out the **USERS: Profiles: Add** pop-up window with the following information:
    a. **Name:** SPLUNK_ADMIN
    b. **Description:** Admins of Splunk's OS
3. Under **USERS,** click **Add.**
4. Move the **SPLUNK_ADMIN_ACMEFINANCIAL_COM** user to the list on the right, and then click **OK.**
5. Click **Save.**



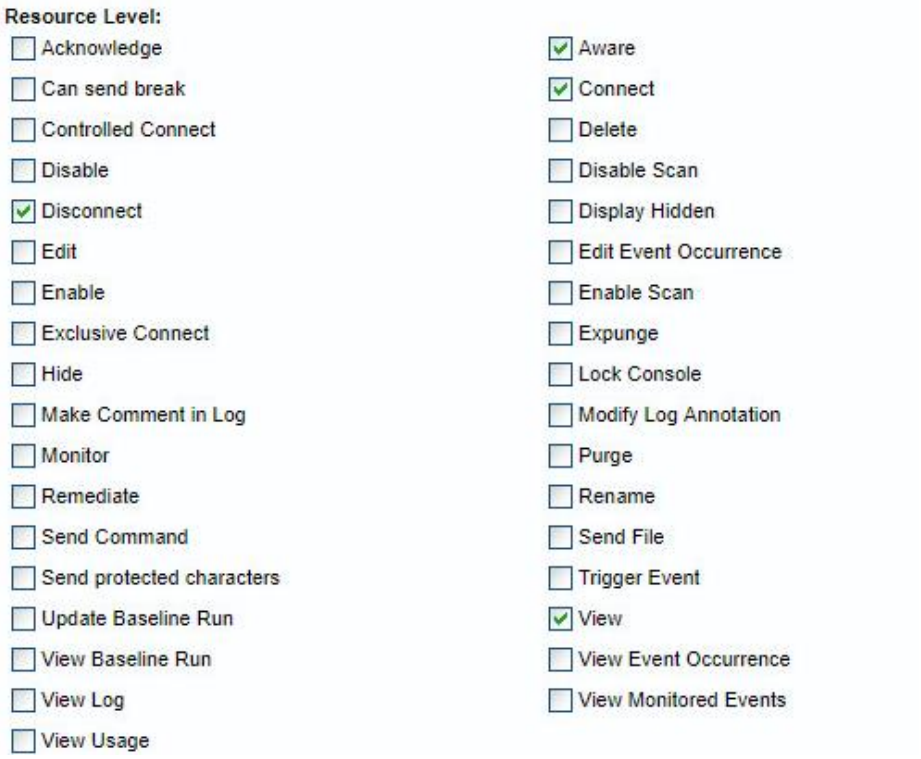
Use the same procedure provided above (while just changing the **Name, Description,** and **USERS** chosen) to create profiles for each group of users who should have access to a specific set of consoles. In this case, it was Splunk OS-level consoles. Next, it could be Splunk application-level consoles.

2.3.11 Assigning Permissions to Profiles

Profiles were given access to the consoles through Access Control Rules in ConsoleWorks. The following steps create an Access Control Rule for Splunk OS-level admins:

1. In ConsoleWorks, click **SECURITY > Access Control > Add.**
2. Fill out the **SECURITY: Access Control: Add** window with the following information:
    a. **Name:** SPLUNK_OS_CONSOLES
    b. **Description:** Access to Splunk OS consoles
    c. **Order:** 10
    d. **Allow or Deny:** ALLOW
    e. **Component Type:** Console
3. Open **Profile Selection,** and select the **Simple** tab.
4. Move the **SPLUNK_ADMIN** profile to the list on the right.
5. Open **Resource Selection,** and select the **Simple** tab.
6. Change the drop-down from **Is one of these Consoles** to **Has one of these Tags.**

7. Move the **SPLUNK_OS** tag to the list on the right.
8. Open **Privileges,** and select the following privileges (these are the same for both SSH and web consoles):
    a. **Aware**
    b. **Connect**
    c. **Disconnect**
    d. **View**



9. Click **Save.**

2.4 Ekran System

Ekran System is a monitoring solution that provides session recording and playback. A server records the actions of users on multiple clients.

2.4.1 How It's Used

Ekran System is used to create "privileged stations" that privileged users use to access their privileged accounts. Ekran monitors the actions taken by privileged users, and reports to Splunk.

2.4.2 Virtual Machine Configuration

The Ekran System server is installed on one virtual machine, while the client is on another virtual machine. Ekran recommends increasing the storage of the virtual machine based on how many clients are being monitored.

The Ekran System server virtual machine is configured as follows:

- Windows Server 2016
- 1 CPU core
- 8 GB of RAM
- 150 GB of storage
- 1 NIC

Network Configuration (Interface 1):

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.1.20
- Netmask: 255.255.255.0
- Gateway: 172.16.1.1
- DNS name servers: 172.16.3.10
- DNS-search domains: N/A

2.4.3 Prerequisites

Ekran System requires Microsoft SQL Server, although, in the lab environment, Microsoft SQL Server Express was used. Ekran System also requires IIS to be installed. A full list of requirements can be found on Ekran's website.

2.4.4 Installing Ekran System

Full installation instructions are available on Ekran's website.

The Ekran System server and agent are installed in the privileged user station and are used to monitor privileged users.

2.5 Radiant Logic

Radiant Logic FID is a virtual directory that performs a federated identity service.

2.5.1 How It's Used

Radiant Logic FID is used in two capacities in this example implementation. First, FID acts as the identity provider for users accessing TDi ConsoleWorks to view security dashboards within Splunk. Users are forced to use MFA with VASCO IDENTIKEY. Second, FID acts as a monitoring service where privileged user accounts are monitored for changes, logged, and forwarded to Splunk.

2.5.2 Virtual Machine

The Radiant Logic virtual machine is configured as follows:

- Windows Server 2016
- 3 CPU cores
- 20 GB of RAM
- 120 GB of storage
- 1 NIC

Network Configuration (Interface 1):

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.3.218
- Netmask: 255.255.255.0
- Gateway: 172.16.1.1
- DNS name servers: 172.16.3.10
- DNS-search domains: N/A

2.5.3 Prerequisites

The minimum system requirements are as follows:

- Hardware
  - Cluster nodes must be deployed on hardware that is configured for optimal redundancy and highly reliable connectivity between the cluster nodes/machines.
  - Processor: Intel Pentium or AMD Opteron, minimum dual core

- Processor speed: 2 gigahertz or higher
- Memory: 16 GB minimum. For most production deployments, more than 16 GB of memory is required.
- Hard drive: 100 GB of disk space. The hard-disk usage will vary depending on the log types/levels that are enabled and the desired log history to maintain.

- Software
  - OS: Windows 2008 R2 Server, Windows Server 2012 R2, Windows Server 2016

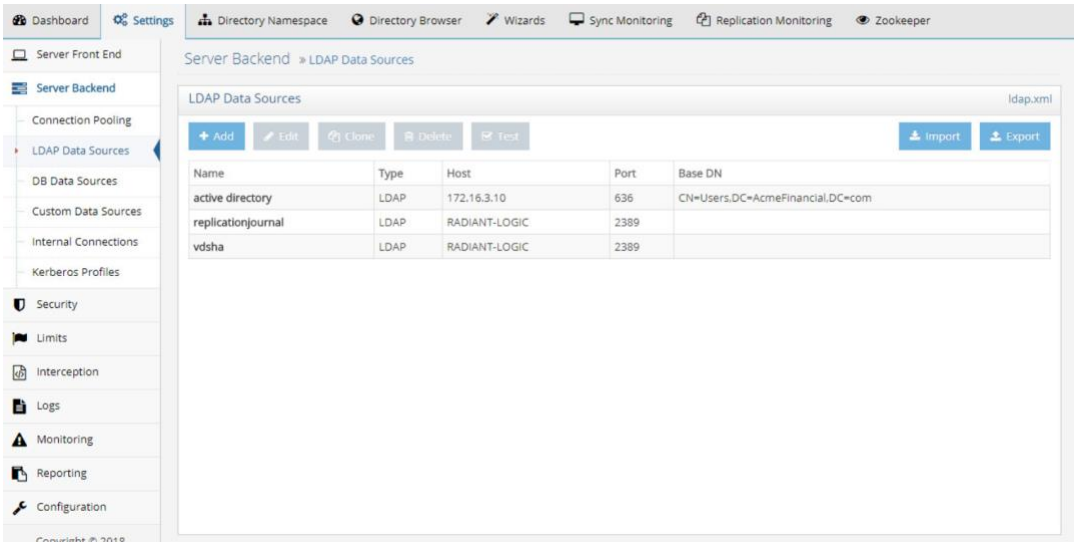
2.5.4 Installation

To install FID, see the documentation provided with the software. The FID installation guide can also be found on the Radiant Logic support website. A support account is required.

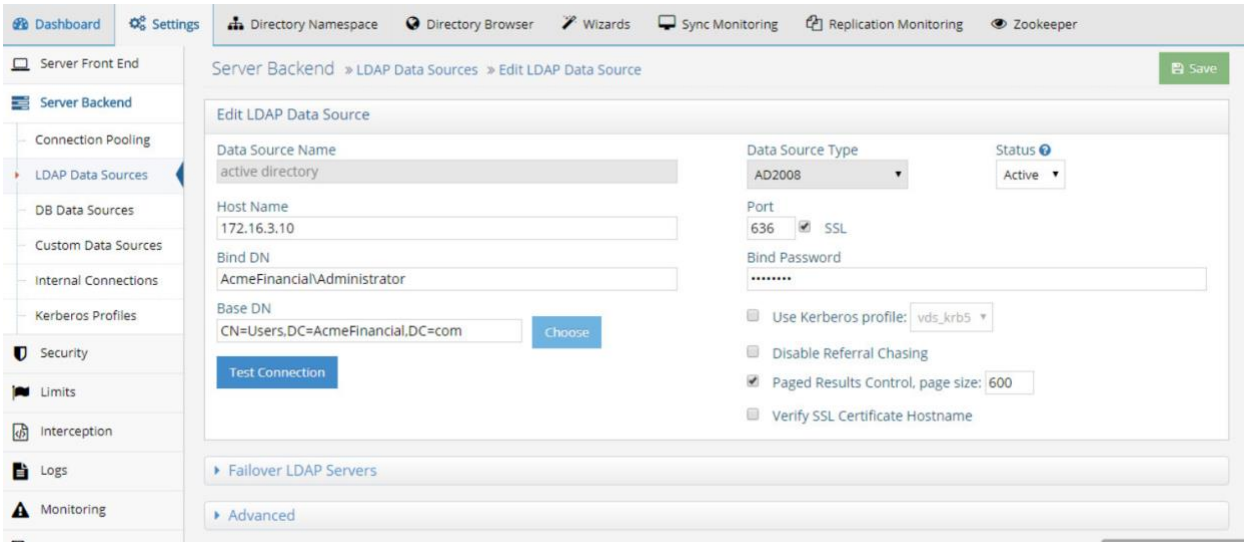
2.5.5 Configure FID

The steps for configuring FID are as follows:

1. Add server back-ends:
   a. While logged in as the Directory Manager, navigate to **Settings > Server Backend > LDAP Data Sources.**
   b. Click **Add.**



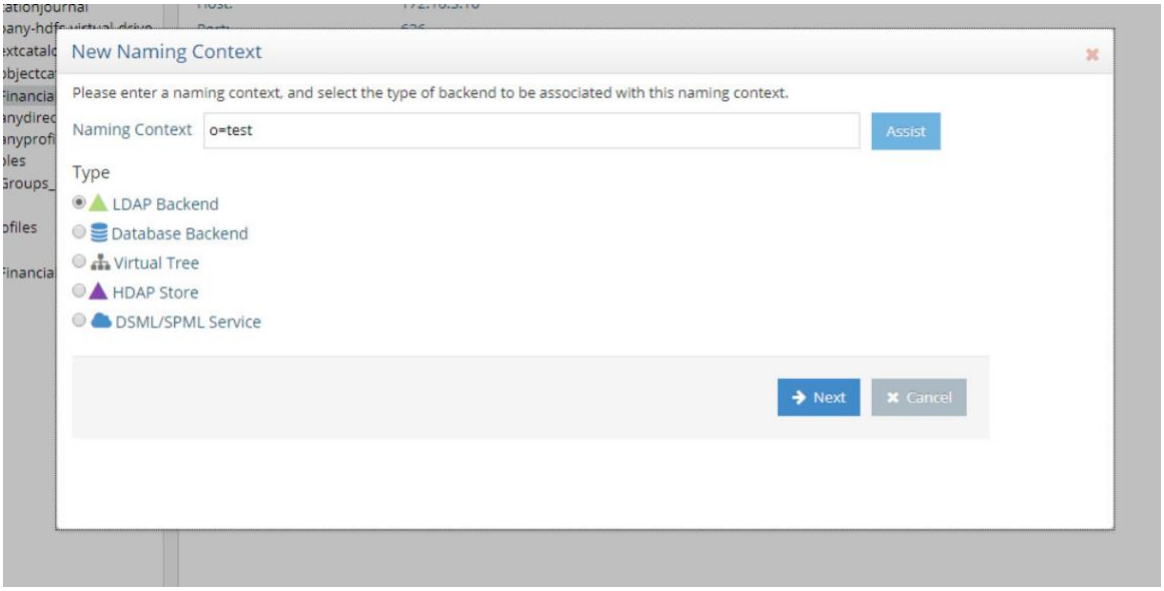
   c. Name the data source, and then enter the parameters. For AD, the parameters used are shown in the following screenshot. Click **Save.**



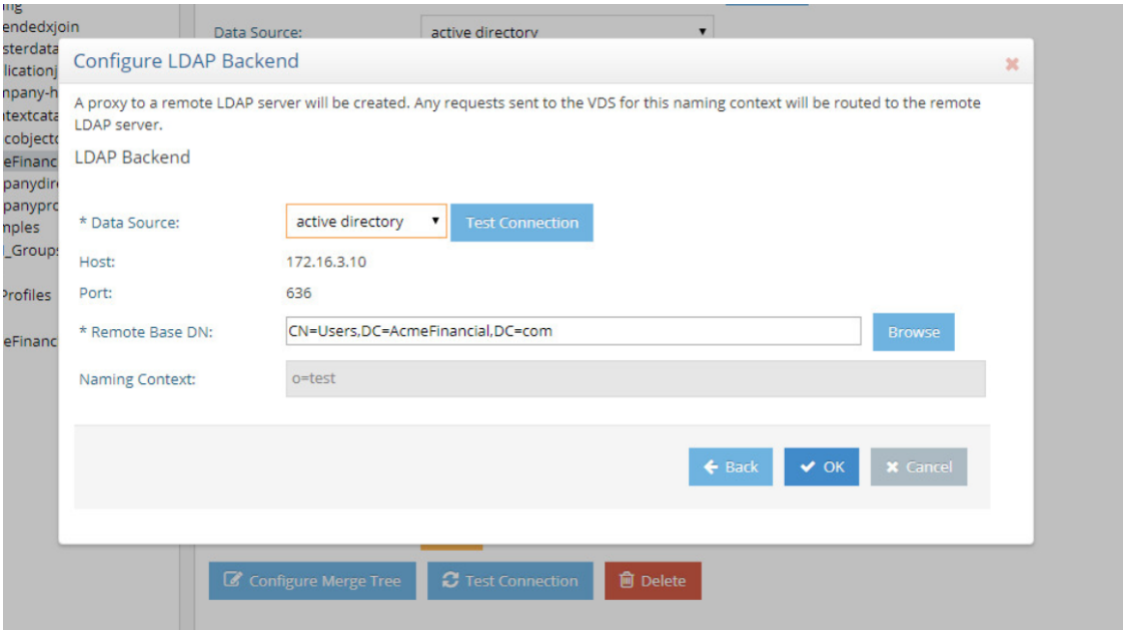
2. Create a proxy view to the back-end directories:

   a. On the **Directory Namespace** tab, select **New Naming Context** (the plus sign) at the top left of the screen.

   b. Select the **LDAP Backend** radio button, and enter the naming context, such as o=test. Click **Next.**



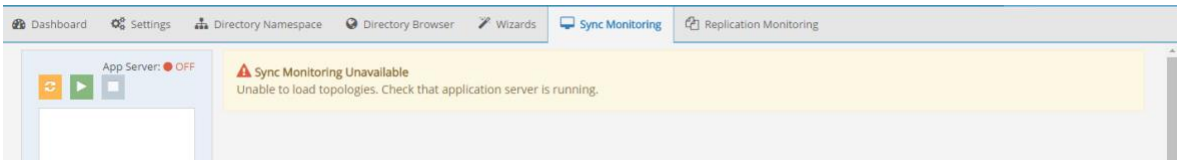
   c. For the **Data Source,** select the name of the AD back-end created earlier. Browse and select the **Remote Base DN** of the domain. Click **OK.**



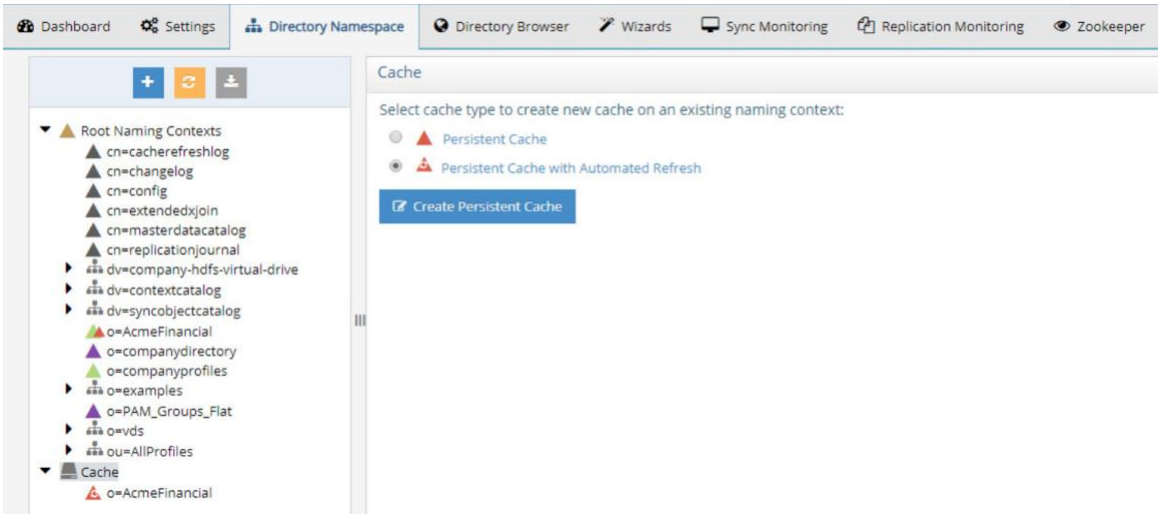
2.5.6 Configure Logging

To log changes to each directory object, you must create a cache for the proxy view created in the previous section. To create the cache and to log changes made to the back-end directories, complete the following steps:

1. Navigate to the **Sync Monitoring** tab. Press the play (▷)button to start the glassfish server.

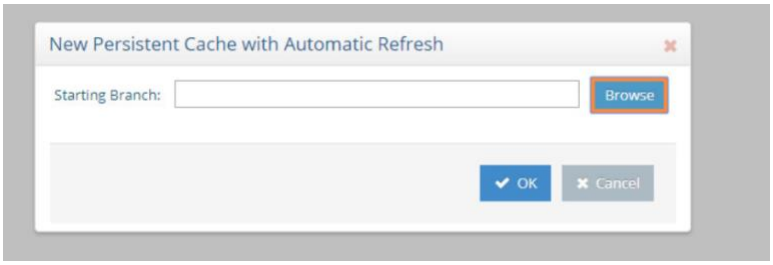


2. In the **Directory Namespace** tab, highlight **Cache** in the left window pane. Select **Persistent Cache with Automated Refresh.** Click **Create Persistent Cache.**



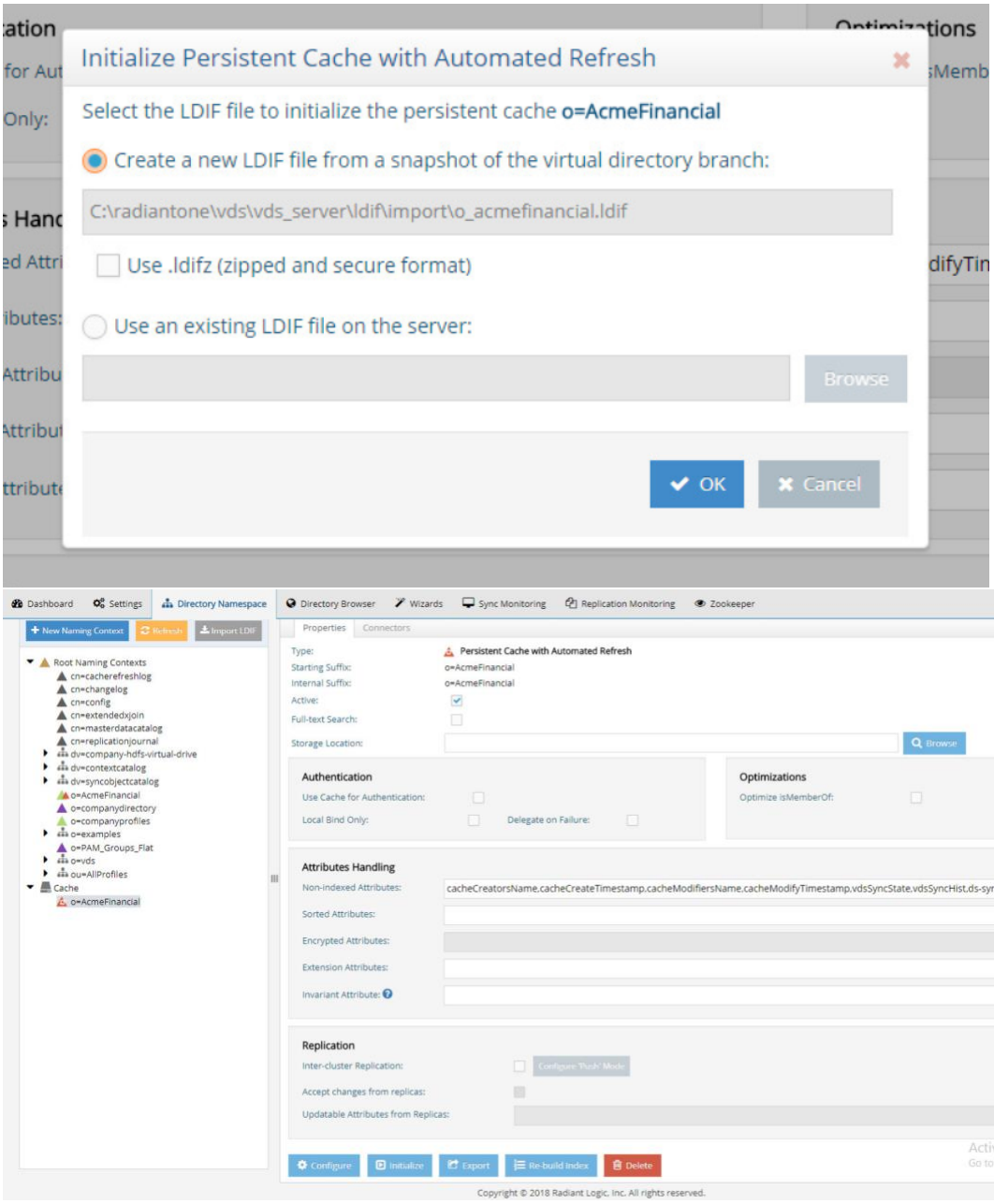
822

823 3. Browse and select the Lightweight Directory Access Protocol (LDAP) proxy created in the
824 previous steps. Click **OK**. FID creates the cache.



825

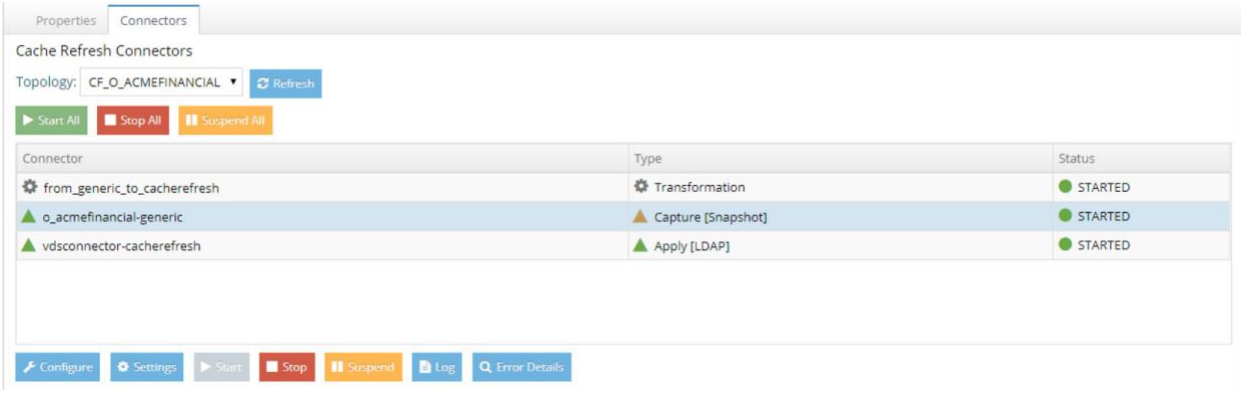
826 4. Under **Cache** in the lower left window, select the cache that you created. Click **Initialize** to make
827 the cache active.



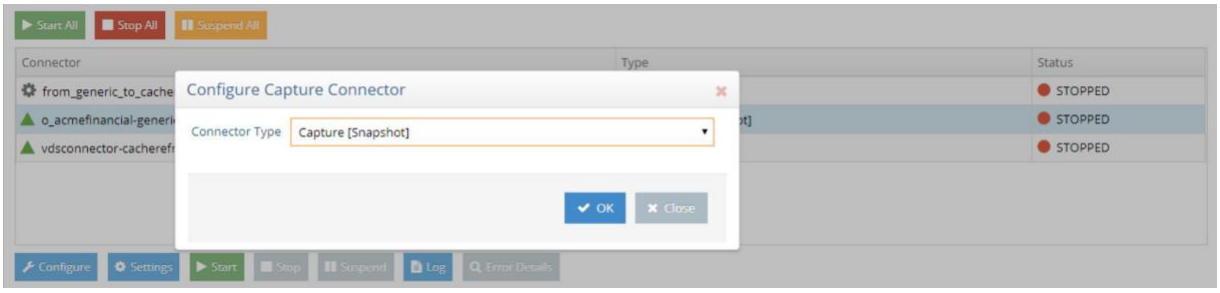
5. Select **Create a new LDIF file from a snapshot of the virtual directory branch.** Click **OK.** This step may take a few minutes.

6. Once complete, click **Save.**

7. Select the **Connectors** tab.



8. There will be a connector for the back-end directory and for the connector itself. Highlight the AD connector. Click **Configure.** Change the connector type to **Capture [Snapshot].** Click **OK.**



9. Install Splunk Universal Forwarder to monitor the file at *C:\radiantone\vds\r1syncsvcs\log\cf_o_acmefinancial\object_generic_dv_so_o_acmefinancial_capture.log*

2.5.7 Configure SSL

In this implementation, AD serves as the CA.

1. Create the initial FID private key:

   Navigate to *c:\radiantone\vds\jdk\jre\bin*, and run `keytool -genkey -alias rli -keyalg RSA -keystore C:\radiantone\vds\vds_server\conf\rli.keystore -dname "cn=radiant-logic, dc=acmefinancial,dc=com"`.

2. Download the certificate from the CA.

3. Create the certificate signing request:

   Navigate to *c:\radiantone\vds\jdk\jre\bin*, and run `keytool -certreq -alias rli -keystore C:\radiantone\vds_server\conf\rli.keystore -file C:\radiantone\vds_server\conf\vdsserver.csr.`

4. Submit the request to the CA.

5. Import the trusted CA certificate into the keystore and cacerts database on FID:

   a. Navigate to *c:\radiantone\vds\jdk\jre\bin*, and run `keytool -import -trustcacerts -file C:\radiantone\vds\vds_server\conf\certca.cer -keystore C:\radiantone\vds\vds_server\conf\rli.keystore.`

   b. Run `keytool -import -trustcacerts -file C:\radiantone\vds\vds_server\conf\certca.cer -keystore C:\radiantone\vds\jdk\jre\lib\security\cacerts.`

6. Import the signed server certificate from the request into FID:

   Navigate to *c:\radiantone\vds\jdk\jre\bin*, and run `keytool -import -file C:\radiantone\vds\vds_server\conf\rli.cer -keystore C:\radiantone\vds\vds_server\conf\rli.keystore -v -alias rli.`

7. Restart FID.

2.5.8 Splunk Universal Forwarder

Install Splunk Universal Forwarder by following the instructions provided at http://docs.splunk.com/Documentation/Forwarder/7.1.3/Forwarder/Abouttheuniversalforwarder.

Edit the *inputs.conf* file to monitor the *object_generic_dv_so_o_acmefinancial_capture.txt* file created by Radiant Logic FID and to forward logs to the **demo** index at Splunk Enterprise.

2.6 IdRamp

2.6.1 How It's Used

IdRamp is used for MFA in this build. The majority of the IdRamp configuration is performed by the IdRamp team.

2.6.2 Prerequisites

- premium Azure account
- AD installed

2.6.3 Installation

1. Set up Azure AD sync with password hash synchronization:

   https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-get-started-express

2. Enable MFA in Azure for certain privileged users:

   a. In the Azure AD admin center at https://aad.portal.azure.com, click **Azure Active Directory.**

   b. Click **SECURITY > Conditional access.**

   c. Click **New policy.**

d. Give the policy a name, such as Privileged 2FA.

e. Click **Users and groups.** Under **Include,** click **users and groups,** and select **Users and groups** check box.

f. Click the region labeled as **Select.**

g. Select the privileged users from the list.

h. Once all of those users are selected, click **Done.**

i. Click **Cloud apps,** and then select **All cloud apps.** Click **Done.**

j. Under **Access Controls,** click **Grant.**

k. Make sure that the **Grant access** check box is selected, and select the check box labeled as **Require multi-factor authentication.**

l. Click **Select.**

m. Click **On** under **Enable policy,** and then click **Create.**

3. Disable logins of all other accounts:

   a. For each user that you do not want to allow to sign in with Azure AD at all, click their user account under **All users** in the Azure AD admin center.

   b. Click **Yes** next to **Block sign in.**

4. Configure sign-in to block incoming requests, except from your organization's network:

   a. Under **SECURITY > Conditional access** in the Azure AD admin center, select **Named locations.**

   b. Click **New location,** and then give the location a name.

   c. Select the check box labeled as **Mark as trusted location.**

   d. Enter the IP range of the network to which you want to restrict access.

   e. Click **Create.**

   f. Complete steps 2a–2c above.

   g. Give the policy a name, such as Block Remote Access.

   h. For users of this policy, select the privileged users.

   i. Select all cloud apps for the **Cloud apps assignment.**

j. Under **Conditions,** select **Locations.**

k. Select **Yes** under **Configure,** and select **Any location** under **Include.**

l. Click **Exclude,** and then click **Select.**

m. Select the **Named location** that we just created, and then click **Select.**

n. Click **Done.**

o. Click **Grant** under **Access controls,** and then click **Block access.**

p. Click **Select.**

q. Click **On** under **Enable policy,** and then click **Create.**

2.7 OneSpan IDENTIKEY Authentication Server

OneSpan IDENTIKEY Authentication Server, now known as OneSpan Authentication Server, is a two-factor authentication (2FA) solution with user, policy, and token management. DIGIPASS is the name of their two-factor token, and it can be hardware-based or software-based.

2.7.1 How It's Used

IDENTIKEY Authentication Server provides 2FA to TDi ConsoleWorks. The Authentication Server acts as a RADIUS server, which allows a variety of clients to authenticate through it. The Authentication Server, based on a user-defined policy, checks the onetime passcode from a DIGIPASS. Additionally, the server binds to Radiant Logic by using LDAPS to authenticate the user's password.

2.7.2 Virtual Machine Configuration

The IDENTIKEY Authentication Server virtual machine is configured with Ubuntu Server 16.04 LTS.

The text `search acmefinancial.com` should be saved in *resolv.conf* file.

2.7.3 Prerequisites

The product can be installed on both Windows and Linux. This project used Linux.

The prerequisite software for a basic installation could be installed with the following command:

```
sudo apt install unixodbc libaio1 libdbi-perl socat openjdk-8-jre-headless
```

The license key should be located on the server where the Authentication Server is going to be installed.

2.7.4 Installation

The following instructions lead through a basic installation of IDENTIKEY Authentication Server:

1. Mount the *.iso* file with the server installer:

```
mkdir /mnt/dvd
mount /dev/dvd /mnt/dvd
```

2. Run the installation script:

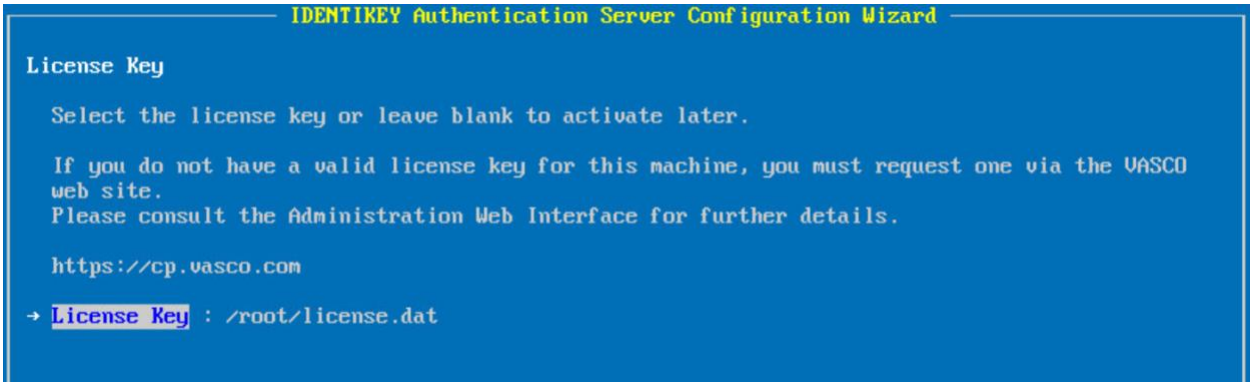
```
cd /mnt/dvd
sudo ./install.sh
```

3. Begin following the installation wizard, and choose basic installation.
4. Accept the licenses.
5. Select **Yes** to encrypt the embedded database.

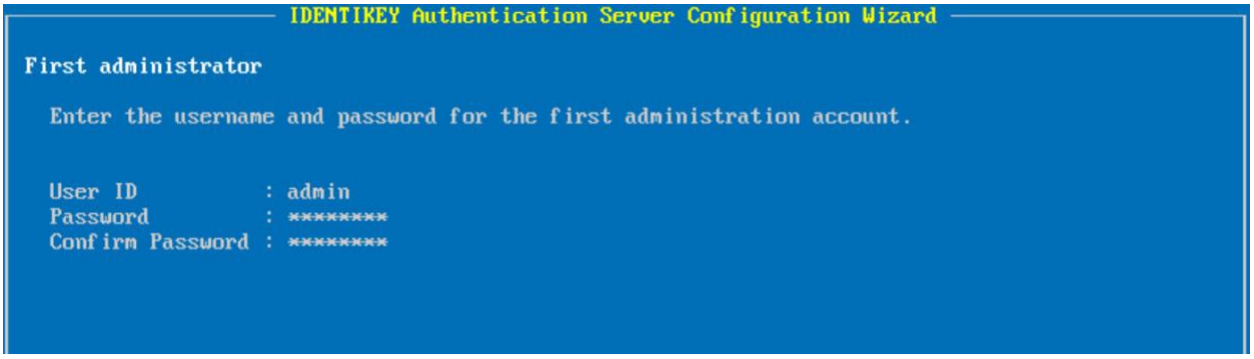
2.7.5 Configuration

After completing the installation, configuration happens immediately:

1. Press Enter to choose **Next.**
2. Enter the IP address of the server (in this case, 172.16.2.208).
3. Enter the location of the license key on the server.

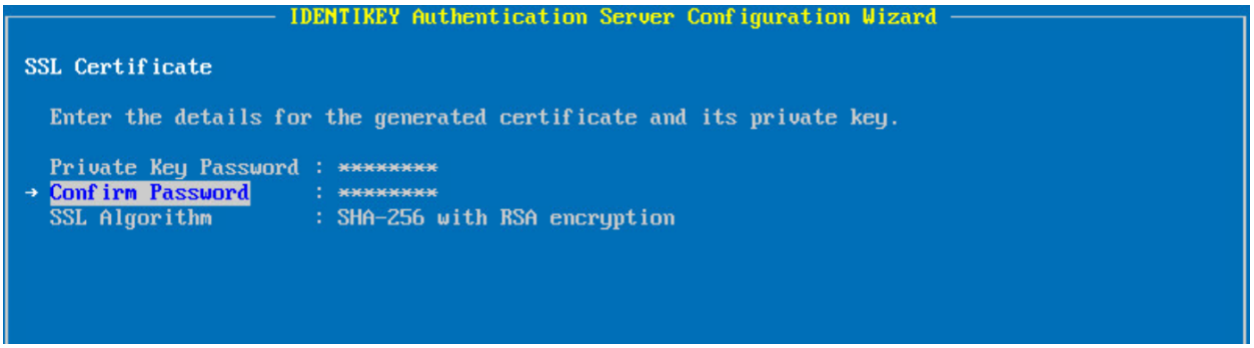


4. Accept the server functionality, and then select **Next.**
5. Create a username and password for the first admin account, and then select **Next.**



958

959 6. Create a password for the certificate, and then select **Next.**



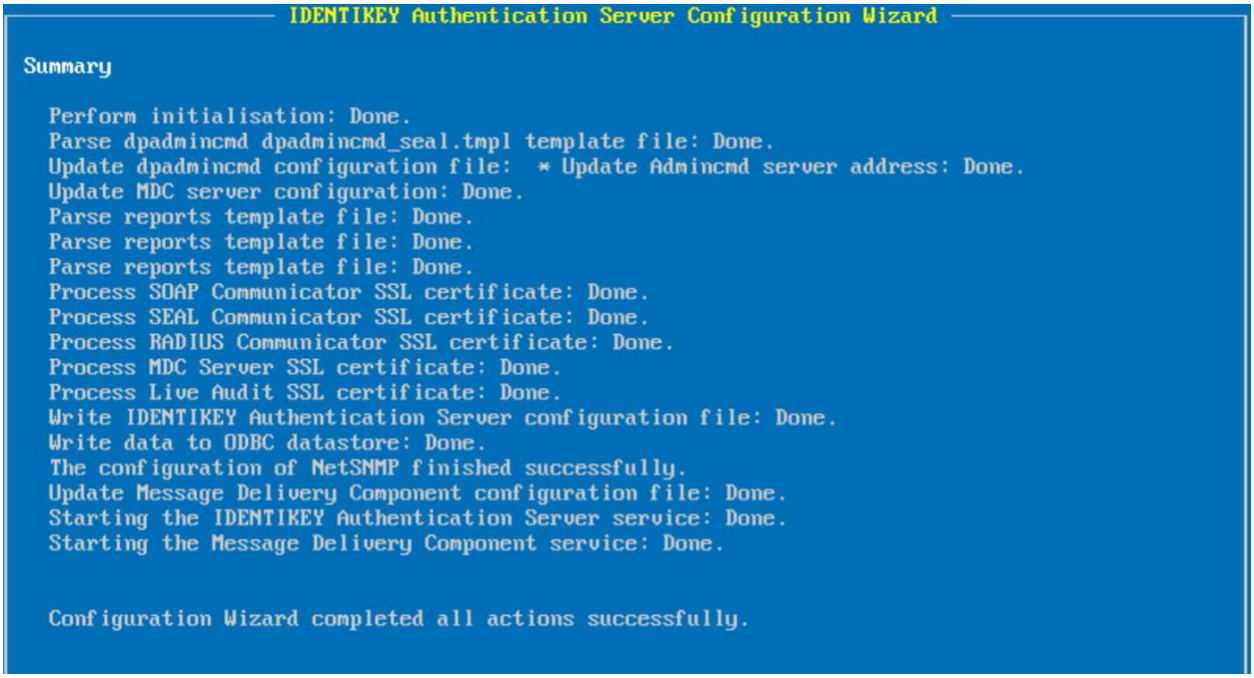
960

961 7. Set up the server to act as a stand-alone RADIUS server, and then select **Next.**

962 8. Create the first RADIUS client, with the IP address and a shared secret. The first client will be
963 ConsoleWorks. Select **Next.**

964 9. Verify that all of the options shown on the screen are consistent with the above instructions.
965 Select **Proceed.**

966 10. Verify that the configuration succeeded as shown below.



967

968 11. Respond **No** to the question “Do you want to import a DIGIPASS file? (yes/no)” as you will do
969 this later.

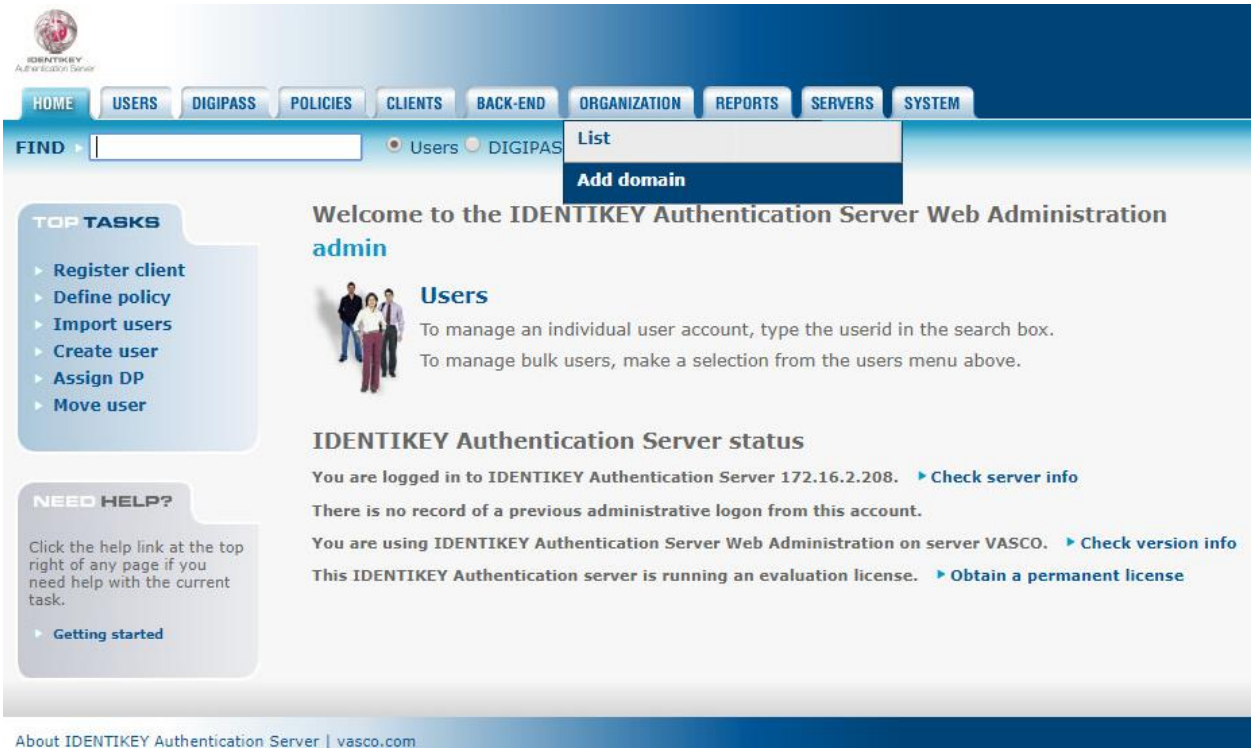
970 2.7.6 Creating a Domain and Policies

971 After completing installation and basic configuration with the terminal, the following steps are
972 completed with the web interface:

973 1. Open the web interface at https://172.16.2.208:8443.

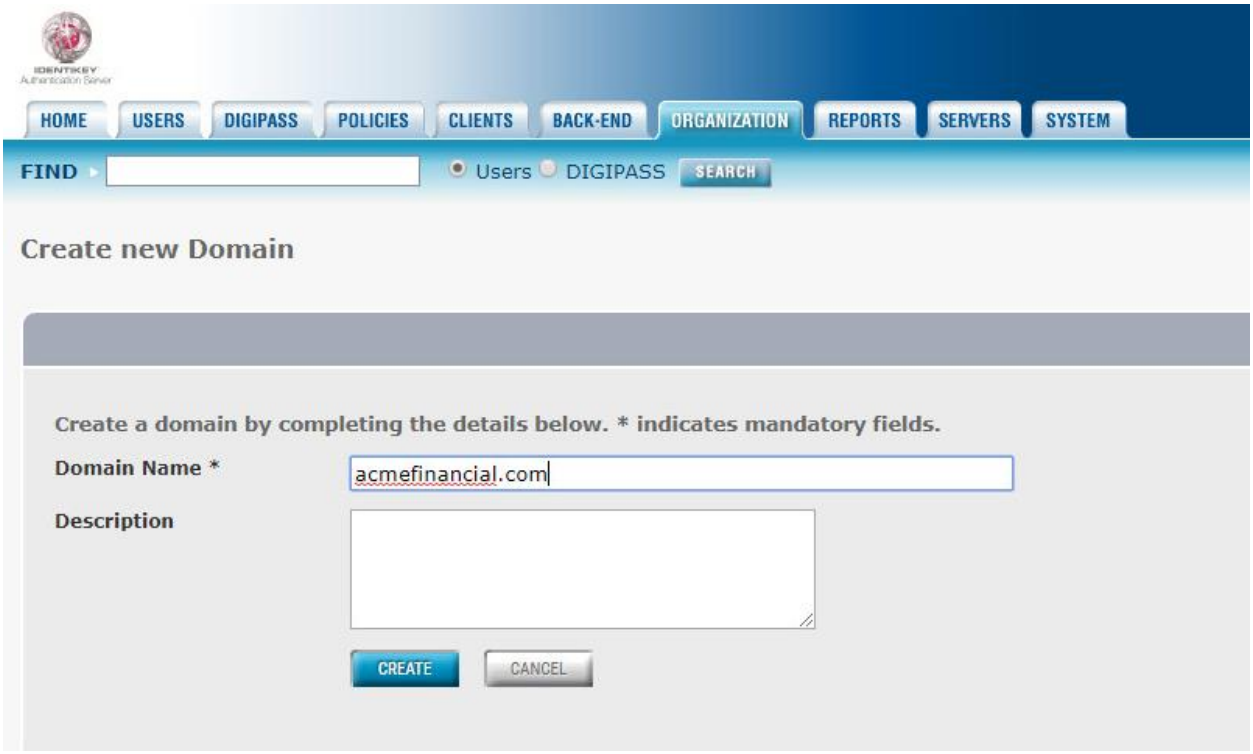
974 2. Log in by using the admin account that was created during configuration.

975 3. Click **ORGANIZATION > Add domain.**



976

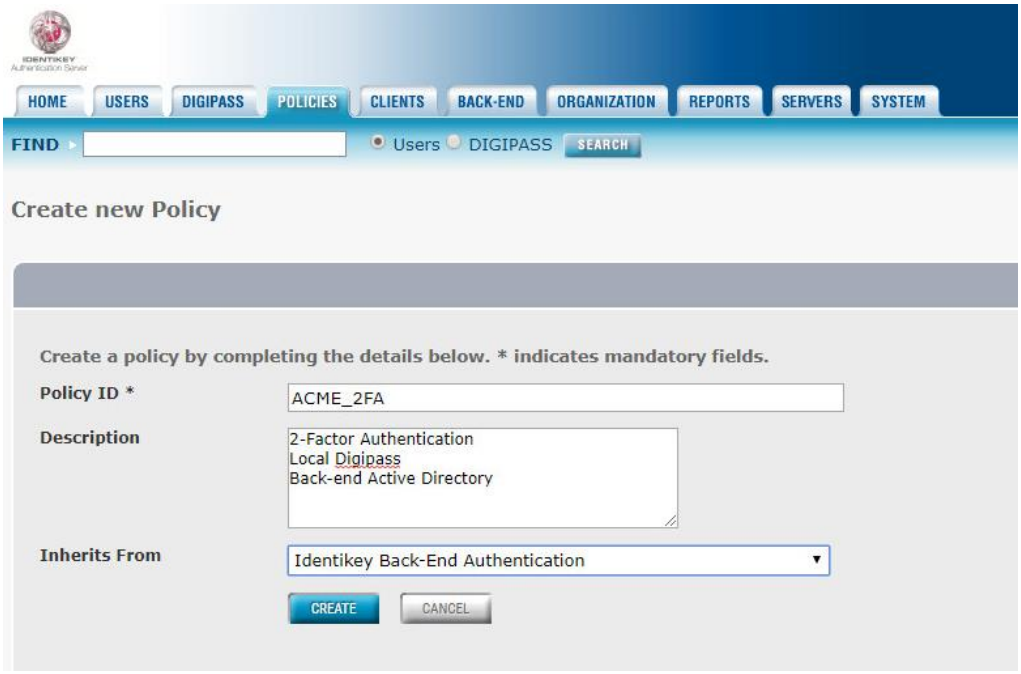
977 4. Enter the **Domain Name** acmefinancial.com and then click **CREATE.**



978

979 5. Click **POLICIES > Create.**

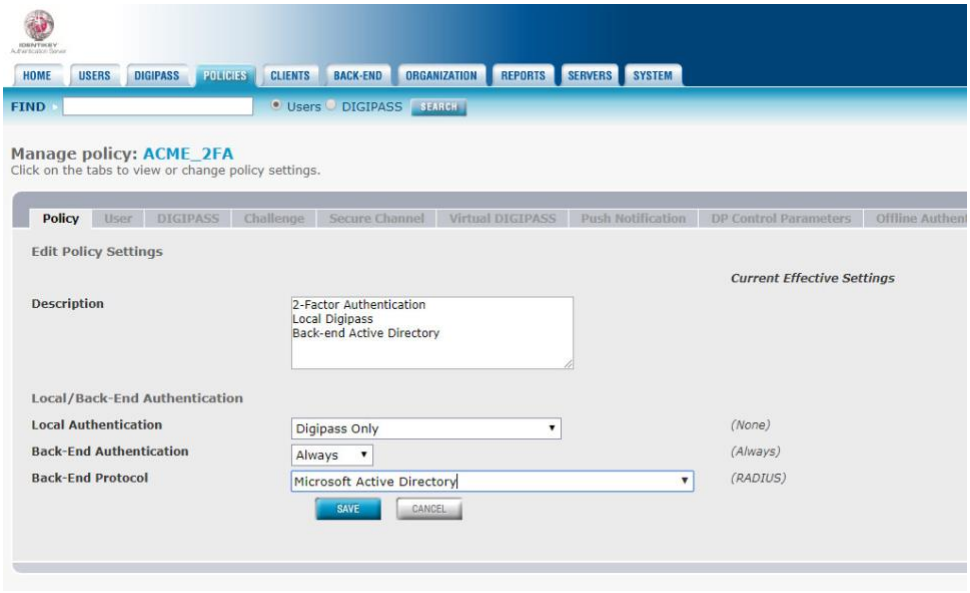
980 6. Enter the **Policy ID** ACME_2FA, write a short **Description,** and choose for it to inherit from
981 **Identikey Back-End Authentication.** Click **CREATE.**



982

983 7. Choose to manage the policy, and click **EDIT.**

984 8. Select **Digipass Only** for **Local Authentication, Always** for **Back-End Authentication,** and
985 **Microsoft Active Directory** for **Back-End Protocol.** Click **SAVE.**



986

987 9. Click **CLIENTS > List.**

988 10. Click the **RADIUS client.**

989 11. Select ACME_2FA for the **Policy ID,** which was just created. Click **SAVE.**

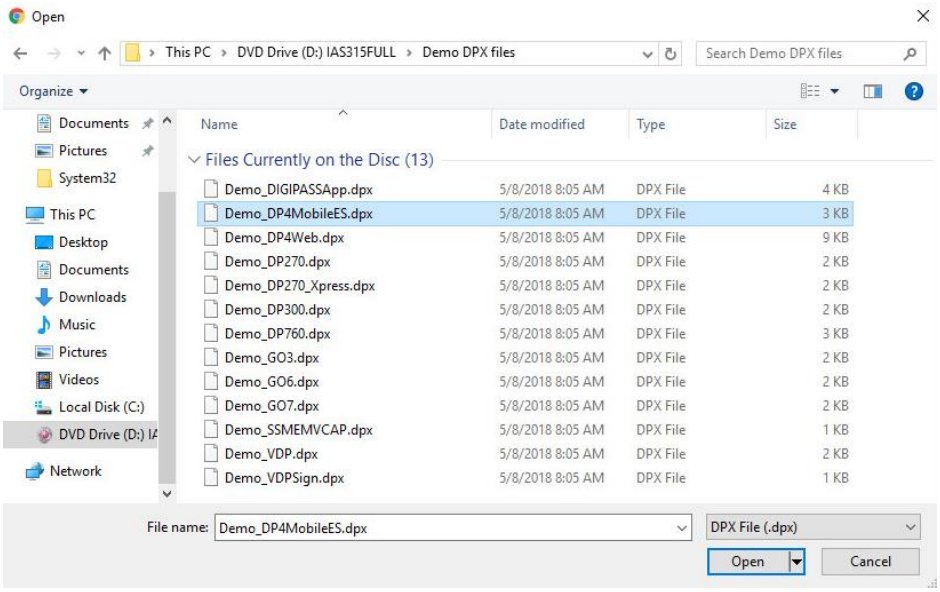
990

991 2.7.7 Importing DIGIPASSes

992 The following steps import demo DIGIPASSes that were included in the installation *.iso* file:

993 1. In the web interface, click **DIGIPASS > Import.**

994 2. Click **Choose File** next to **Get DPX file,** and select the demo DIGPASSApp.dpx file, which came in
995 the *.iso* file. Within the *DIGPASSApp.dpx* file is a set of mobile-application DIGIPASSes. Click
996 **Open.**



997

998 3. Enter the transport key for that file. For the demo files, the transport key is
999 11111111111111111111111111111111 (32 1s).

1000 4. Click **UPLOAD.**

1001 5. Select **ACTIVATION** as the application name. Click **NEXT.**

1002 6. On the next screen, import the DIGIPASSes as **ACTIVE,** and set the **Domain** to be
1003 acmefinancial.com.

1004 7. Click **IMPORT.**

1005 8. Choose to run the task immediately.

1006 2.7.8 Configuring to Use Radiant Logic as a Back-End Authentication Server

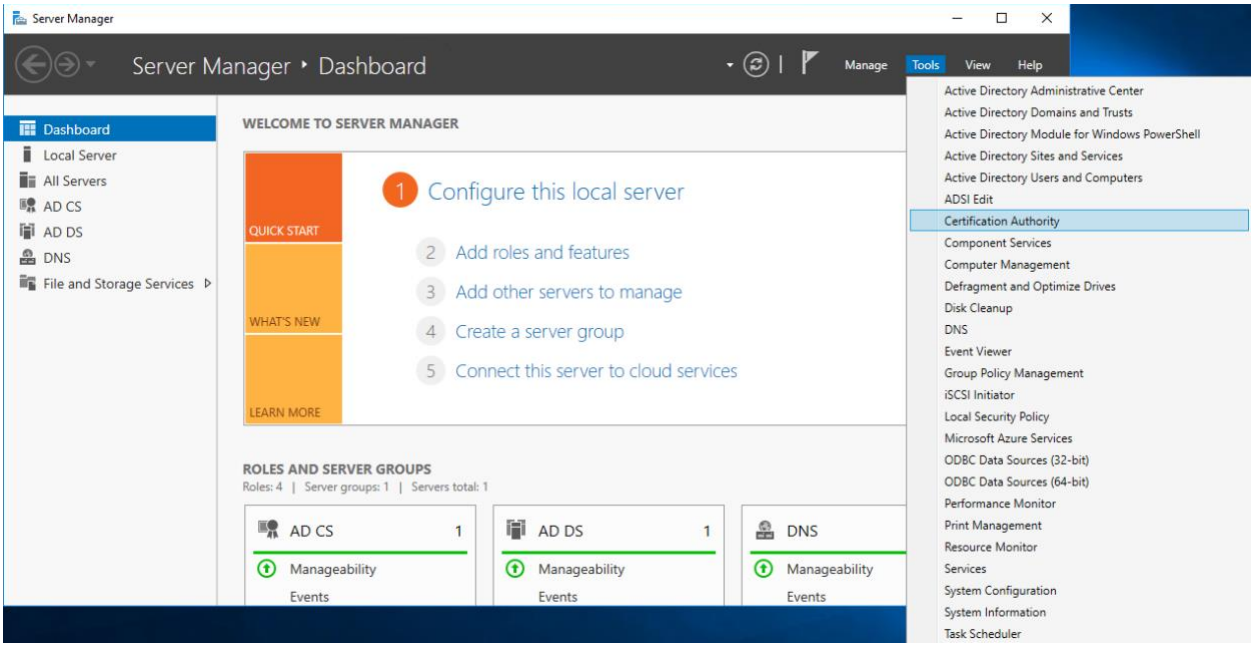
1007 With Radiant Logic configured to replicate users and groups from AD, OneSpan can use Radiant Logic as
1008 an AD back-end. This works, as OneSpan connects to Radiant by using LDAP over SSL, and Radiant Logic
1009 contains a virtual directory that presents like AD.

1010 *2.7.8.1 Installing the AD CA Certificate in the OneSpan Server OS*

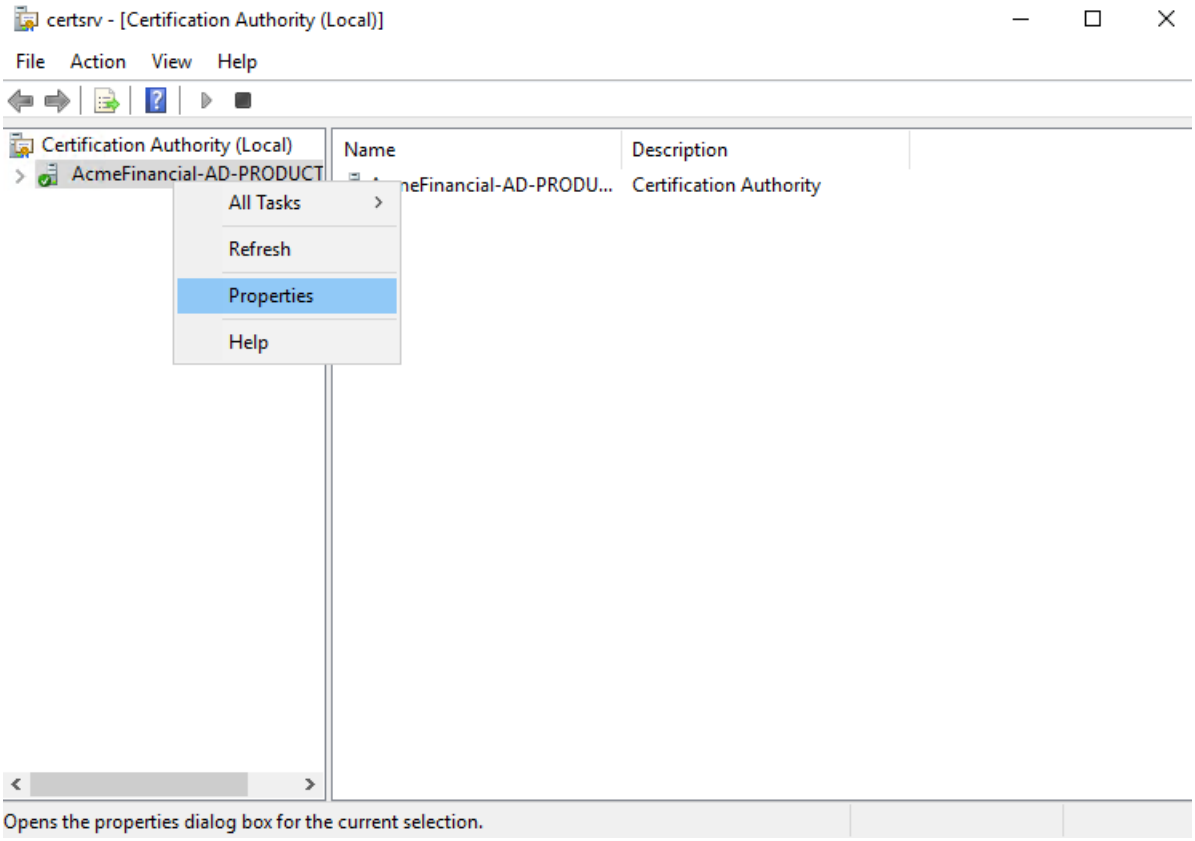
1011 For OneSpan to trust the certificate used by Radiant Logic during the SSL handshake, the AD CA
1012 certificate needs to be installed. Because the Radiant Logic certificate was signed by the AD CA, once
1013 OneSpan trusts the CA, it trusts Radiant Logic. The following instructions detail how to export the AD CA
1014 certificate and how to install it in Ubuntu:

1015 1. On AD-PRODUCTION, the AD Domain Controller, open **Server Manager.**

2. In the top right corner, click **Tools > Certification Authority.**



3. **Under Certification Authority (Local),** right-click **AcmeFinancial-AD-PRODUCTION-CA,** and then select **Properties.**



4. Click **Certificate #0,** and then click **View Certificate.**
5. Tab over to **Details,** and then click **Copy to File.**
6. Click **Next.**
7. Select the format option **Base-64 encoded X.509 (.CER),** and then click **Next.**
8. Select a location and file name for saving the certificate. For example, *C:\Users\Administrator\Desktop\AD-PRODUCTION-CA-PEM.cer.*
9. Click **Next,** and then click **Finish.**
10. Copy the file over to the OneSpan server.
11. On the OneSpan server, copy the file to the */usr/local/share/ca-certificates* directory, and give it a *.crt* file extension.
12. Update the trusted CA certificates with the following command:

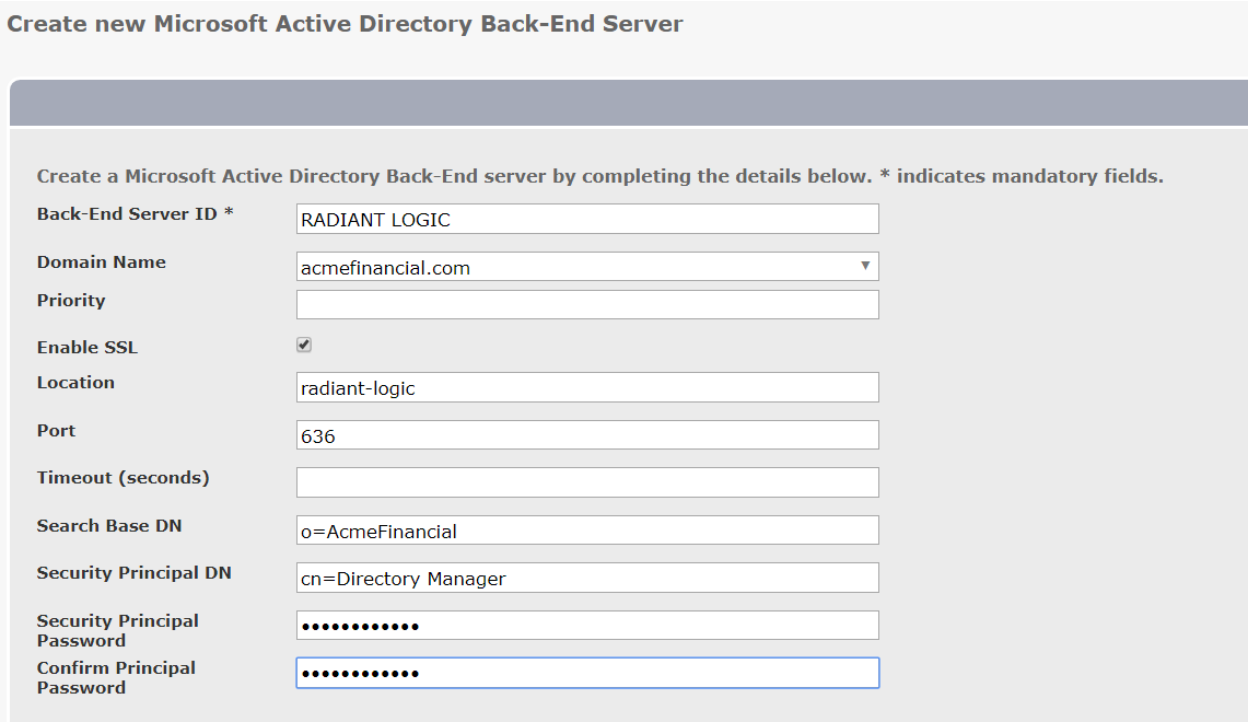
```
sudo update-ca-certificates --fresh
```

13. Reboot the OneSpan server machine.

2.7.8.2 Configuring OneSpan to Use Radiant Logic

Once the certificate for Radiant Logic will be trusted, the final step (before OneSpan will authenticate with Radiant Logic as a back-end) is to add a back-end server entry in OneSpan. The following procedure completes this step:

1. In the **IAS Web Administration** interface, click **BACK-END > Register Active Directory Back-End.**
2. Fill out the pop-up window with the following information:
    a. **Back-End Server ID:** RADIANT LOGIC
    b. **Domain Name:** acmefinancial.com
    c. **Enable SSL:** This check box should be selected.
    d. **Location:** radiant-logic
    e. **Port:** 636
    f. **Search Base DN:** o=AcmeFinancial
    g. **Security Principal DN:** cn=Directory Manager
    h. **Security Principle Password:** <the Security Principal Password from Radiant Logic>
    i. **Confirm Principle Password:** <the Security Principal Password from Radiant Logic>



3. Click **CREATE.**

2.7.9 Integration with TDi ConsoleWorks

Integrating TDi ConsoleWorks with OneSpan required disabling the NAS-IP-Address RADIUS attribute. Instructions for completing this step are available online from OneSpan.

2.7.10 Installing User Websites

To allow users to register their own DIGIPASS device without the need of an admin being present, User Websites must be installed and then configured with a corresponding license. The following steps detail how to install the User Websites on the same server as the Authentication Server:

1. Mount the *.iso* file with the server installer:

```
mkdir /mnt/dvd
sudo mount /dev/dvd /mnt/dvd
```

2. Run the installation script:

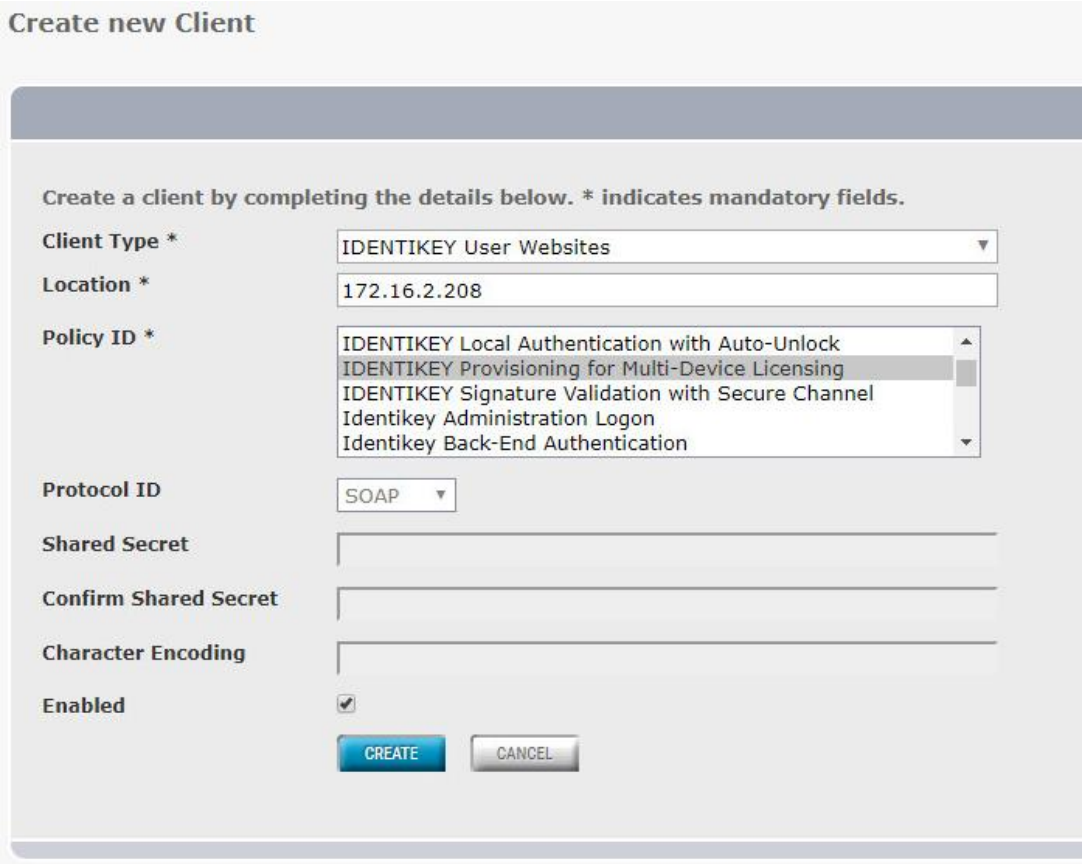
```
cd /mnt/dvd/IDENTIKEY\ User\ Websites/
sudo ./install-uws.sh
```

3. Accept the licenses for the server.

2.7.11 Creating Component Records in IDENTIKEY Authentication Server

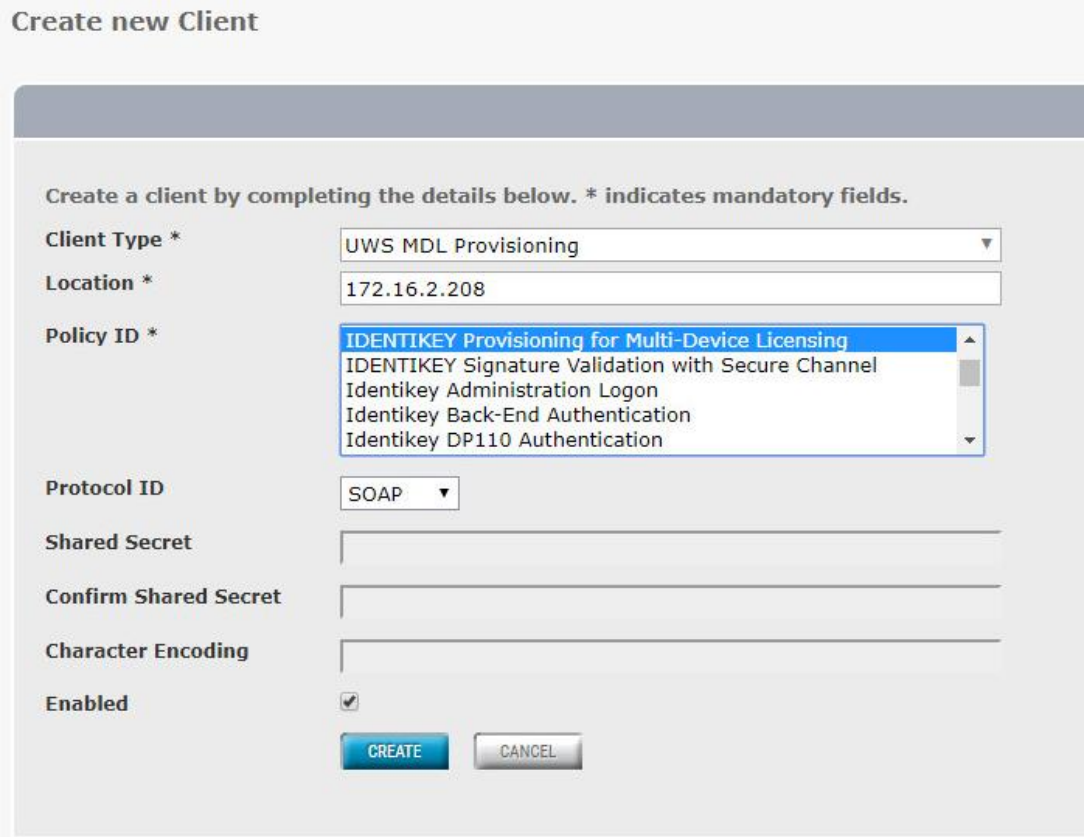
Before User Websites can be used to assign a user a DIGIPASS, the IDENTIKEY Authentication Server must be configured to accept connections from the User Websites. We will create two component records for the websites: one general User Websites client record and another UWS MDL Provisioning client record for provisioning DIGIPASSes.

1. In **IAS Web Administration,** click **CLIENTS > Register.**
2. Fill out the **Create new Client** page with the following information:
    a. **Client Type: IDENTIKEY User Websites**
    b. **Location:** 172.16.2.208
    c. **Policy ID: IDENTIKEY Provisioning for Multi-Device Licensing**



3. Click **CREATE.**

4. Click **Click here to manage IDENTIKEY User Websites.**
5. Tab over to **License.**
6. Click **LOAD LICENSE KEY.**
7. Click **Choose File,** and then provide it with the User Websites license.
8. Click **FINISH.**
9. Click **CLIENTS > Register** again.
10. Fill out the **Create new Client** page with the following information:
    a. **Client Type:** UWS MDL Provisioning (type it in)
    b. **Location:** 172.16.2.208
    c. **Policy ID: IDENTIKEY Provisioning for Multi-Device Licensing**



11. Click **CREATE.**

12. Click **POLICIES > List.**
13. Find the policy **IDENTIKEY Provisioning for Multi-Device Licensing,** and then click it.
14. Click **EDIT.**
15. Change the **Back-End Protocol** from **RADIUS** to **Microsoft AD.**
16. Click **SAVE.**
17. Tab over to **User.**
18. Click **EDIT,** and change **Dynamic User Registration** to **No.** This way, only users added by admins in IDENTIKEY Authentication Server will be assigned DIGIPASSes.
19. Click **SAVE.**

Users are now able to go to https://vasco.acmefinancial.com:9443/selfmgmt to assign themselves DIGIPASSes. Details about and instructions for using the DIGIPASS application are available from OneSpan.

2.8 Base Linux OS

The base Linux image used in this project is an Ubuntu 16.04 Server OS. It is open-source and freely available.

2.8.1 Virtual Machine Configuration

The base Linux virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 1 CPU core
- 8 GB of RAM
- 40 GB of storage
- 1 NIC

Network Configuration:

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.x.x
- Netmask: 255.255.255.0
- Gateway: 172.16.x.1

- DNS name servers: 172.16.3.10
- DNS-search domain: acmefinancial.com

2.8.2 Domain Join Configuration

The base system used was configured to be a part of the project's AD domain, as demonstrated by the following steps:

1. Ensure that the system has the DNS IP address pointing to the AD server IP address.

```
root@ssh-server:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 172.16.3.100
netmask 255.255.255.0
gateway 172.16.3.1
dns-nameservers 172.16.3.10
dns-search acmefinancial.com
```

2. Restart the networking by entering the following command:

   `systemctl restart networking`

3. Verify changes by checking the */etc/resolv.conf* file. Enter the following command:

   `cat /etc/resolv.conf`

4. Install the packages required for the AD domain join as described above, using the following command:

```
apt-get -y install realmd sssd sssd-tools samba-common krb5-usr
packagekit samba-common-bin samba-libs adcli
```

5. If prompted to enter your Kerberos 5 realm name, enter your domain name in capital letters. The Kerberos 5 default realm is **ACMEFINANCIAL.COM**.

6. Install the chrony ntp client by entering the following command:

```
apt-get -y install chrony
```

7. Add the following line, which points to the NTP server:

```
server 172.16.3.10
```

```
 GNU nano 2.5.3                File: /etc/chrony/chrony.conf

# This the default chrony.conf file for the Debian chrony package.  After
# editing this file use the command 'invoke-rc.d chrony restart' to make
# your changes take effect.  John Hasler <jhasler@debian.org> 1998-2008

# See www.pool.ntp.org for an explanation of these servers.  Please
# consider joining the project if possible.  If you can't or don't want to
# use these servers I suggest that you try your ISP's nameservers.  We mark
# the servers 'offline' so that chronyd won't try to connect when the link
# is down.  Scripts in /etc/ppp/ip-up.d and /etc/ppp/ip-down.d use chronyc
# commands to switch it on when a dialup link comes up and off when it goes
# down.  Code in /etc/init.d/chrony attempts to determine whether or not
# the link is up at boot time and set the online status accordingly.  If
# you have an always-on connection such as cable omit the 'offline'
# directive and chronyd will default to online.
#
# Note that if Chrony tries to go "online" and dns lookup of the servers
# fails they will be discarded.  Thus under some circumstances it is
# better to use IP numbers than host names.

server 172.16.3.10
```

8. Restart the chrony service as shown below:

```
systemctl restart chrony
```

9. Request an AD domain join by using a domain admin account or a user with appropriate privileges. Perform the domain join by running the following commands:

    a. `kinit administrator@ACMEFINANCIAL.COM`

    b. Enter the password when prompted.

    c. `realm -v join acmefinancial.com –user-principal = yourlinuxhost.acmefinancial.com/administrator@ACMEFINANCIAL.COM`

    d. `systemctl restart realmd`

10. Set `fallback-homedir = /home/%u/%d` to create Linux home directories for domain users, and `access_provider = ad` to allow domain users to log into Linux end points via SSH:

```
 GNU nano 2.5.3                    File: /etc/sssd/sssd.conf

[sssd]
domains = AcmeFinancial.com
config_file_version = 2
services = nss, pam

[domain/AcmeFinancial.com]
ad_domain = AcmeFinancial.com
krb5_realm = ACMEFINANCIAL.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

2.9 Microsoft SQL Server Installation on Ubuntu Linux

Microsoft SQL Server is a relational database management system developed and provided by the Microsoft Corporation. Microsoft SQL Server has different editions that target different audiences. The Express edition, which is freely available, was used in this build.

2.9.1 How It's Used

Microsoft SQL Server is used in the example implementation as a managed asset. It represents a critical asset that would naturally exist in most enterprises. Access to the server by privileged users is controlled by the policies configured on the PAM system.

2.9.2 Virtual Machine Configuration

The Microsoft SQL Server virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 1 CPU core
- 4 GB of RAM
- 40 GB of storage
- 1 NIC

Network Configuration:

- IPv4: manual
- IPv6: disabled

- IPv4 address: 172.16.3.12
- Netmask: 255.255.255.0
- Gateway: 172.16.3.1
- DNS name servers: 172.16.3.10
- DNS-search domain: acmefinancial.com

2.9.3 Firewall Configuration

```
ufw allow 1433/tcp
ufw allow 22/tcp
ufw default deny incoming
```

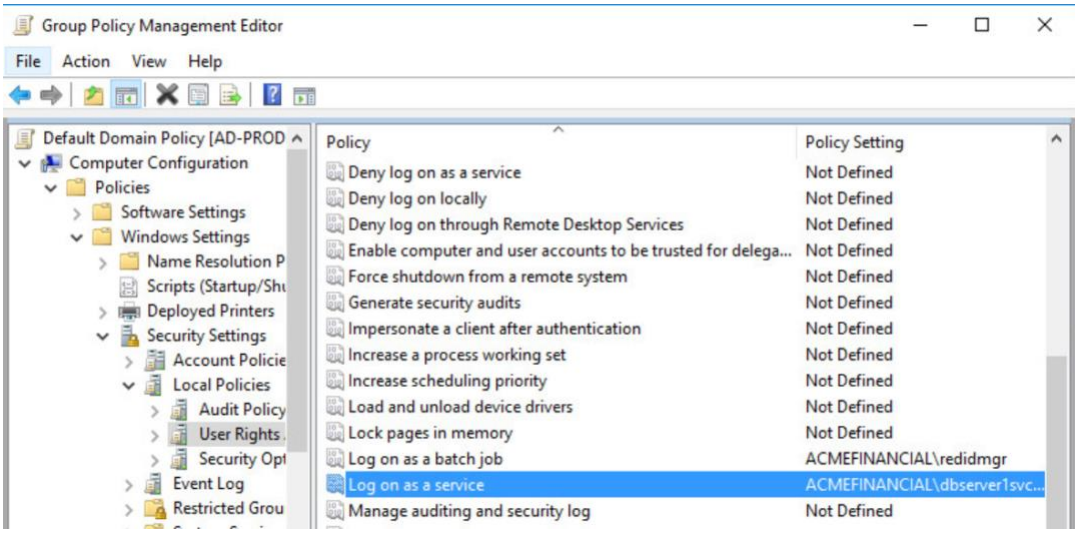
2.9.4 Installation and Initial Configuration

Use the following steps to install Microsoft SQL Server Express 2017 and to configure it to authenticate to AD:

1. Install Microsoft SQL Server on Ubuntu Linux by using the instructions provided at https://docs.microsoft.com/en-us/sql/linux/quickstart-install-connect-ubuntu?view=sql-server-linux-2017.
2. Create a service account by entering the following Powershell command:

   ```
   New-ADuser mssql -AccountPassword (Read_host -AsSecureString "Enter password")
   -PasswordNeverExpires $true -Enabled $true.
   ```

   a. Enter the password when prompted.
3. Give the account the **Log on as a service** right by going to **Server Manager > Group Policy Management > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.**



4. Create a Service Principal Name by entering the following command:

```
setspn -A MSSQLSvc/sql-server.acmefinancial.com:1433 mssql
```

5. Request the information needed to create a keytab file by entering the following commands:

    a. Enter the following command:

    ```
    kinit mssql@ACMEFINANCIAL.COM
    ```

        i. Enter the account password when prompted.

    b. Retrieve the kvno value by entering the following command:

    ```
    kvno MSSQLSvc/sql-server.acmefinancial.com:1433
    ```

```
root@sql-server:~# kinit mssql@ACMEFINANCIAL.COM
Password for mssql@ACMEFINANCIAL.COM:
root@sql-server:~# kvno MSSQLSvc/sql-server.acmefinancial.com:1433
MSSQLSvc/sql-server.acmefinancial.com:1433@ACMEFINANCIAL.COM: kvno = 2
```

6. Create a keytab file by entering the commands shown below:

```
root@sql-server:~# ktutil
ktutil:  addent -password -p MSSQLSvc/sql-server.ACMEFINANCIAL.COM -k 2 -e aes256-cts-hmac-sha1-96
Password for MSSQLSvc/sql-server.ACMEFINANCIAL.COM@ACMEFINANCIAL.COM:
ktutil:  addent -password -p MSSQLSvc/sql-server.ACMEFINANCIAL.COM -k 2 -e rc4-hmac
Password for MSSQLSvc/sql-server.ACMEFINANCIAL.COM@ACMEFINANCIAL.COM:
ktutil:  write_kt /var/opt/mssql/secrets/mssql.keytab
```

7. Exit the ktutil tool by entering the following command:

```
quit
```

8. Restart SQL Server by entering the following command:

```
systemctl restart mssql-server
```

9. Install SQL Server command-line tools by using the instructions provided at https://docs.microsoft.com/en-us/sql/linux/quickstart-install-connect-ubuntu?view=sql-server-linux-2017#tools.

10. Log into the database by entering the following command:

```
./sqlcmd -S localhost -U sa
```

11. To enable AD-based logins to the database, use the instructions provided at https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-active-directory-authentication?view=sql-server-linux-2017#createsqllogins.

2.10 Samba File Server

Samba is an open-source tool that provides file and print services by using the Server Message Block (SMB) / Common Internet File System protocol. Samba can also be used to emulate Windows domain controllers and member servers in AD environments.

2.10.1 How It's Used

Samba was used in this example implementation to provide file services for AD domain clients. As a file server potentially holding confidential information, it was also used as a managed asset for which privileged user access was controlled by policies configured on the PAM system.

2.10.2 Virtual Machine Configuration

The Samba virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 1 CPU core
- 8 GB of RAM
- 40 GB of storage
- 1 NIC

Network Configuration:

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.3.21

- Netmask: 255.255.255.0
- Gateway: 172.16.3.1
- DNS name servers: 172.16.3.10
- DNS-search domain: acmefinancial.com

2.10.3 Firewall Configuration

```
ufw allow 137
ufw allow 138
ufw allow 139
ufw allow 445
ufw allow 22/tcp
ufw default deny incoming
```

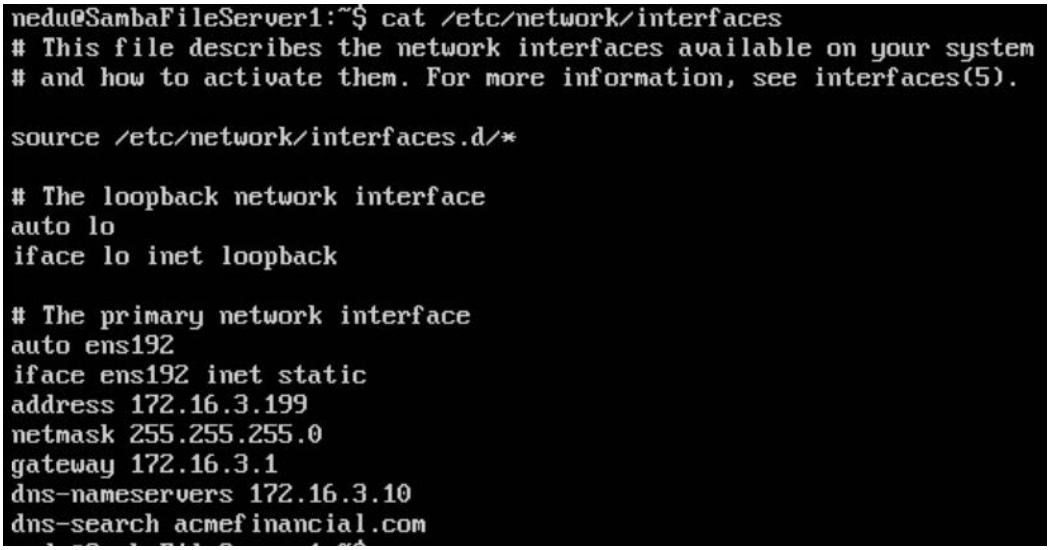
2.10.4 Installation and Configuration

1. Ensure that the DNS server is set to the AD domain controller IP address. Enter the following command to verify:

   ```
   cat /etc/resolv.conf
   ```

2. Ensure that the search domain is set to your domain (e.g., acmefinancial.com). Enter the following command to verify:

   ```
   cat /etc/resolv.conf
   ```



3. Install the chrony ntp client by entering the following command:

```
sudo apt-get install chrony
```

4. Add the following line to the */etc/chrony/chrony.conf* file so that chrony points to the NTP server:

```
server 172.16.3.10
```

5. Restart the chrony service by entering the following command:

```
systemctl restart chrony
```

6. Install the Samba, Kerberos, and winbind packages by entering the following command at the terminal:

```
apt-get install samba krb5-user krb5-config winbind libpam-winbind libnss-
winbind
```

7. Edit the */etc/samba/smb.conf* file with the values as shown below:

```
#======================= Global Settings =======================

[global]
security = ADS
workgroup = ACMEFINANCIAL
realm = ACMEFINANCIAL.COM

logfile = /var/log/samba/%m.log
log level = 1
idmap config * :backend = tdb
idmap config * : range = 10000-120000
template shell = /bin/bash
template homedir = /home/%D/%U
winbind use default domain = true
winbind offline logon = false
winbind nss info = rfc2307
winbind enum users = yes
vfs objects = acl_xattr
map acl inherit = Yes
store dos attributes = Yes
dns forwarder = 172.16.3.10
```

8. Restart these services by entering the following command:

```
systemctl restart smbd winbind
```

9. Join the domain by entering the following command:

```
net ads join -U administrator
```

10. Enter the domain admin password when prompted.
11. Enter the following command at the terminal to create a folder to be shared via Samba:

```
mkdir /PII2
```

12. Enter the following command to change the owning group to domain users:

```
chgrp "domain users" /PII2
```

13. Enter the following command to ensure that only domain admins have access to the folder:

```
chmod 660 /PII2
```

14. Edit the */etc/samba/smb.conf* file with the information shown below:

```
[PII2]
path = /PII2
read only = no
directory mask = 0775
guest ok = yes
```

15. Restart these services by entering the following command:

```
systemctl restart smbd winbind
```

2.11 Remediant SecureONE

SecureONE is a PAM system that controls privileged access to managed assets by adding accounts to or removing accounts from administrative groups on the asset's OSes. SecureONE does not require an agent on the managed asset but instead uses Windows Remote Procedure Call and SSH to make privilege escalation and de-escalation changes on the end point.

2.11.1 How It's Used

In the example implementation, SecureONE was used as a PAM system that controls administrative access to the managed asset's OS. SecureONE was not used for managing administrative access to any application.

2.11.2 Virtual Machine Configuration

The Remediant SecureONE virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 4 CPU cores

- 16 GB of RAM
- 100 GB of storage
- 1 NIC

Network Configuration:

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.2.10
- Netmask: 255.255.255.0
- Gateway: 172.16.2.1
- DNS name servers: 172.16.3.10
- DNS-search domain: acmefinancial.com

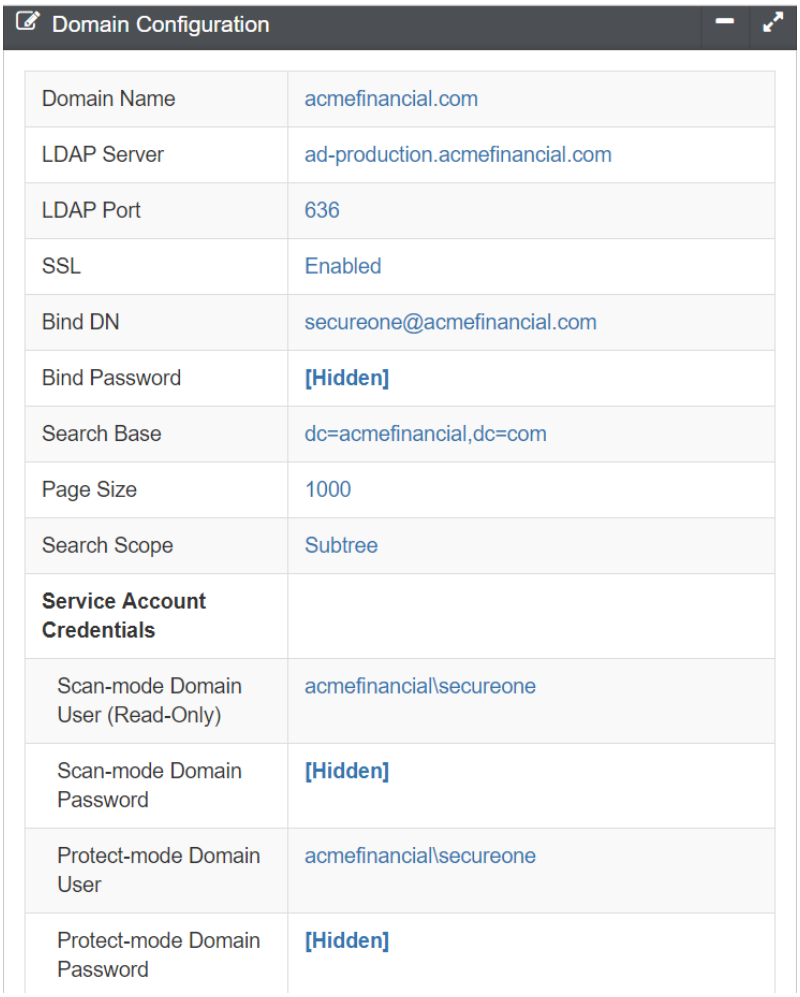
2.11.3 Installation and Initial Configuration

In the example implementation, SecureONE was deployed as a prebuilt virtual-machine appliance from the vendor. The appliance was still configured with parameters necessary for our environment. You can connect to the SecureONE appliance by navigating your web browser to https://10.33.51.227. Replace the IP address with your appliance's IP address.

2.11.4 Domain Configuration

SecureONE needs to be configured to manage systems in an AD environment. The configuration details are provided in the following steps:

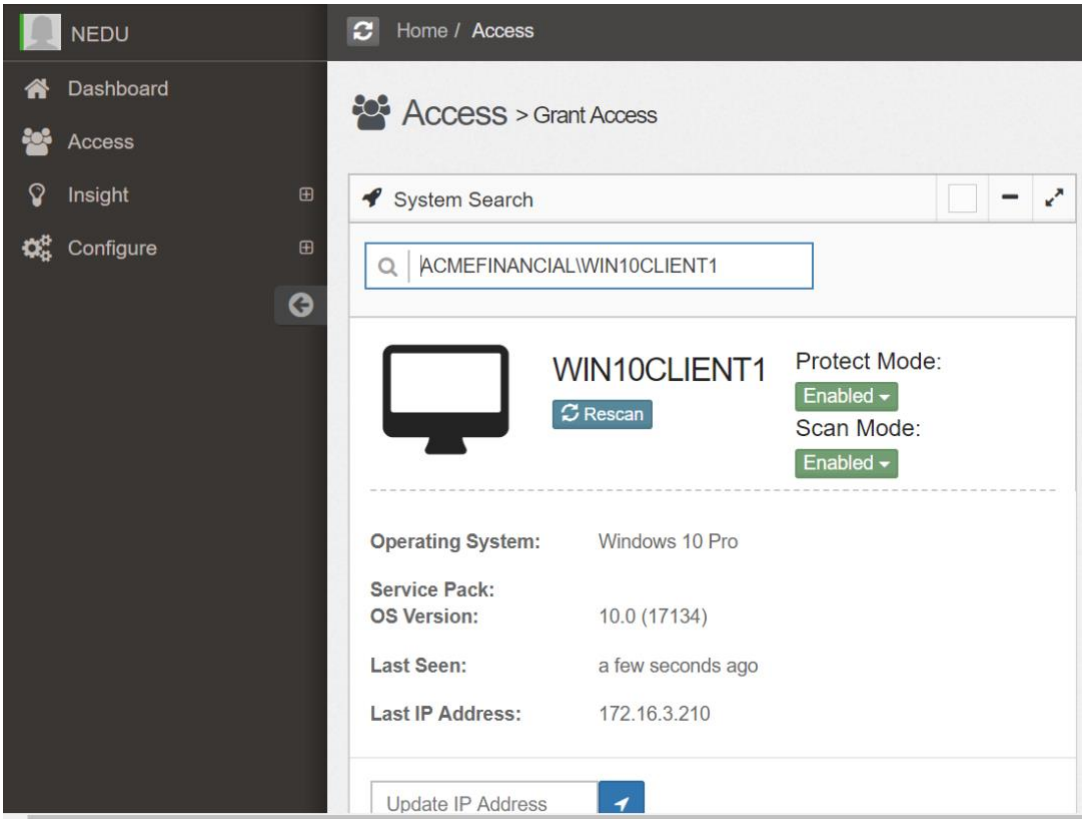
1. Create a service account in AD. Name the service account as secureone, and add it to the domain admins group. This account will be used by the SecureONE appliance.
2. Click **Configure > Server > Edit Configuration,** and fill out the pop-up window with the relevant information:



2.11.5 Managing Systems

SecureONE manages systems by enrolling them into protected mode. Once a system is enrolled, SecureONE can change a user's group memberships. SecureONE can add or remove users from the local admins group or the local sudoers group. Use the following steps to enroll a domain computer:

1. Navigate to **Access > System Search.**
2. In the search bar, enter the host name of the system to be managed.
3. Change the setting under **Protect Mode** to **Enabled.**

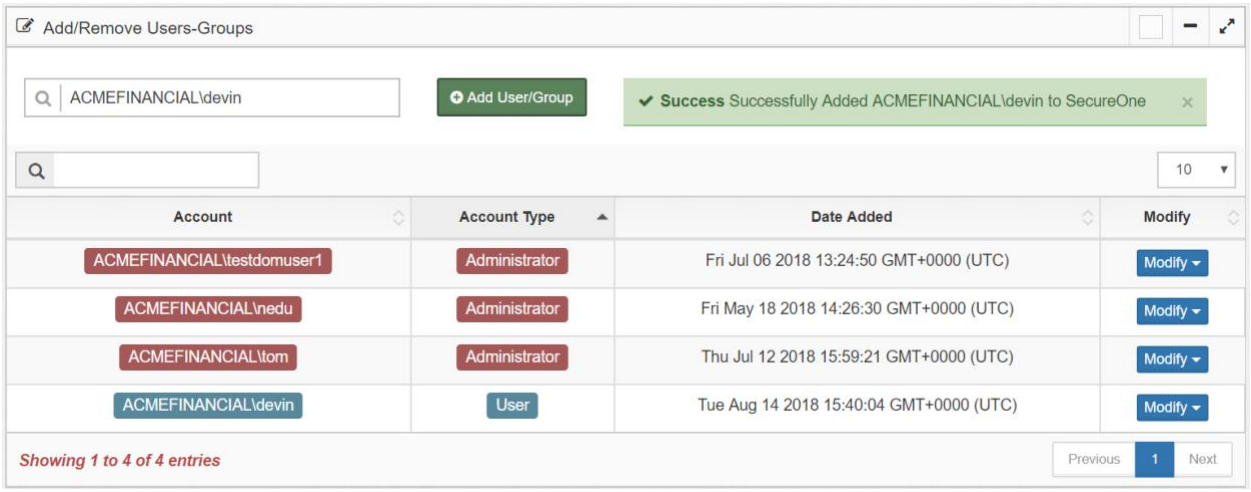


1324

1325 2.11.6 Adding New Users

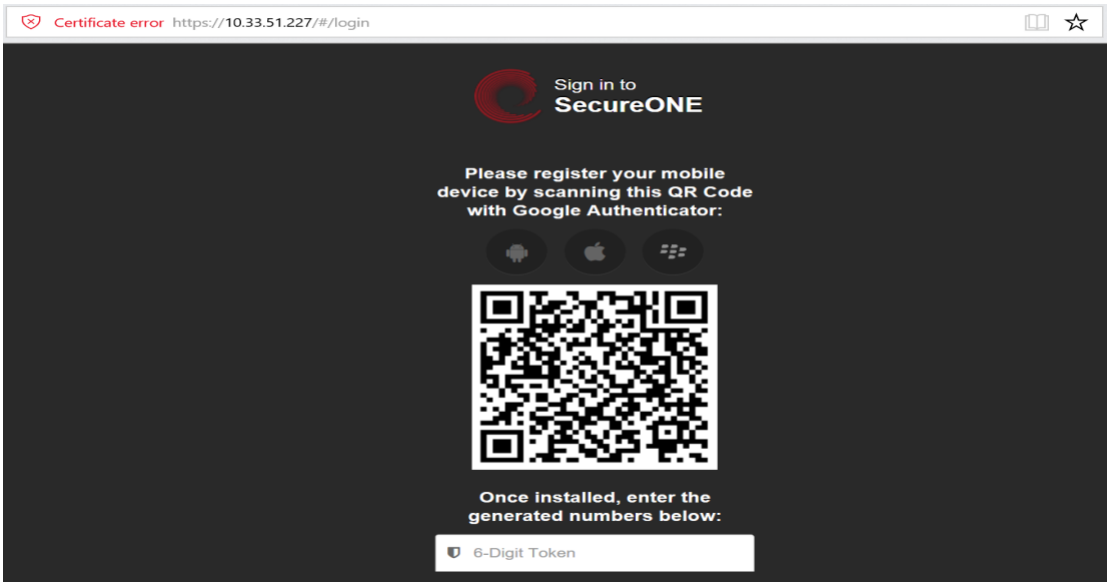
1326 1. Once logged in, navigate to **Configure > Server > Add User/Group.**

1327 2. In the search bar, type the name of the domain user, and then click **Add User/Group.**



1328

3. SecureONE uses a built-in Google Authenticator for 2FA. Once the new user attempts to log in with their domain password, a Quick Response (QR) code is presented.



4. Scan the QR code with the Google Authenticator mobile application to receive your onetime passcode, which changes every 60 seconds.

5. Enter your onetime passcode in the **6-Digit Token** field below the QR code.

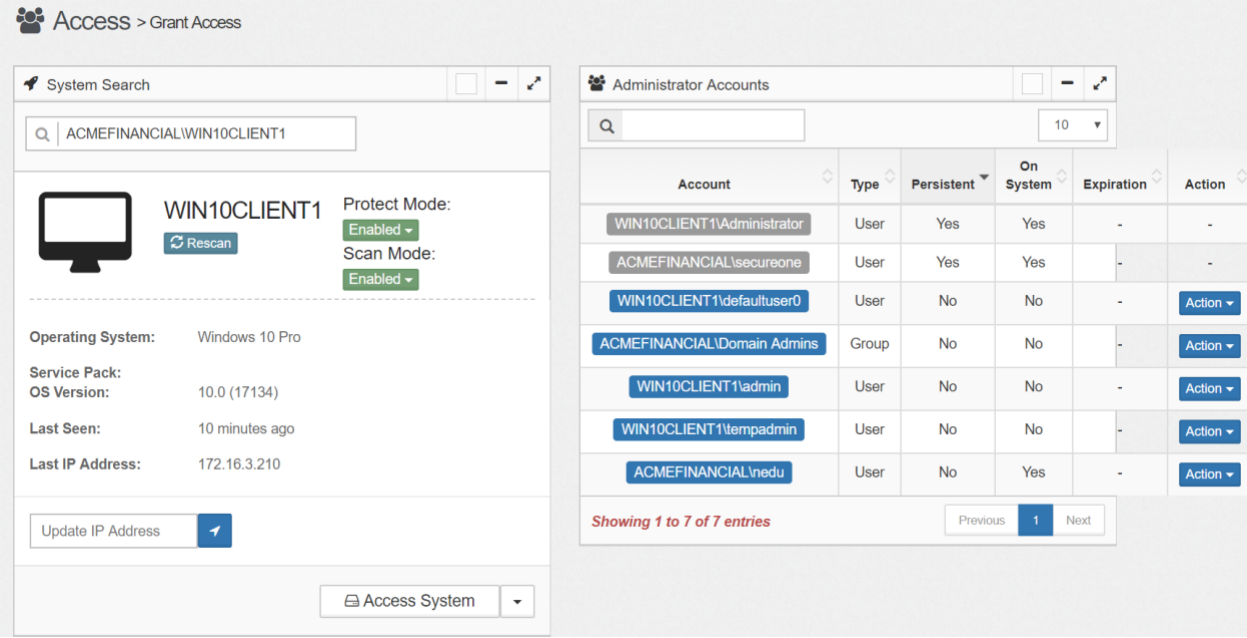
2.11.7 Requesting Privileged Access to Protected System

A user can request privileged access to a system by using the following steps:

1. Navigate to **Access > System Search.**

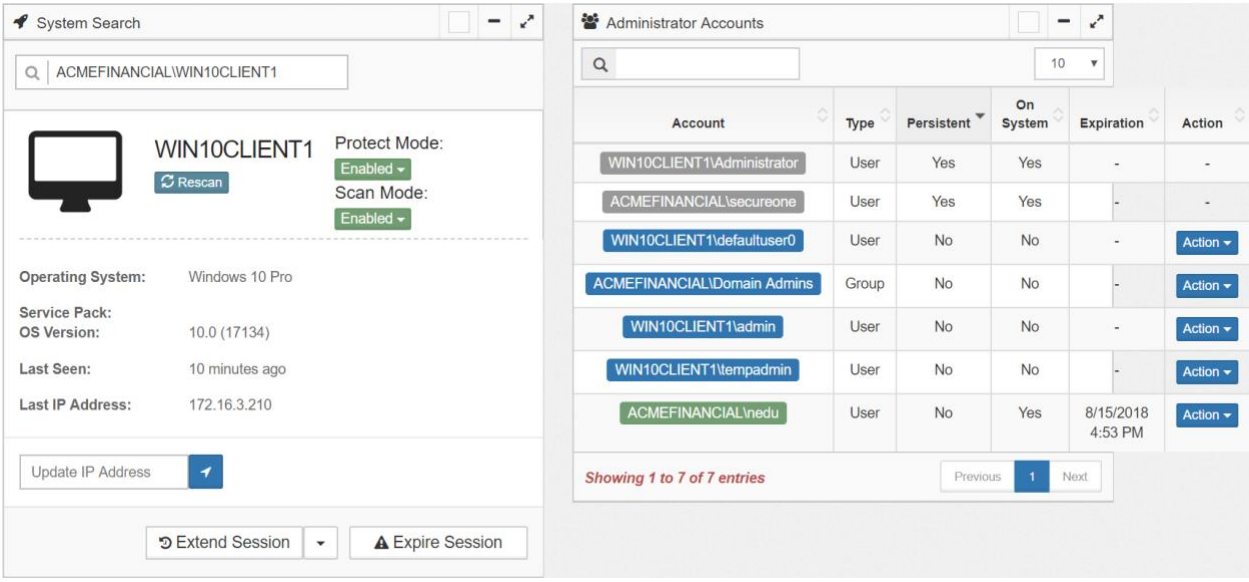
2. In the search bar, enter the host name of the protected system.

3. Click **Access System.**



1340

1341 4. Once access is granted, the session expiration time will be displayed under **Expiration.**



1342

1343 5. At this point, the user can log onto the protected system with administrative privileges.

2.12 RSA Authentication Manager

RSA Authentication Manager is responsible for maintaining and managing user profiles, personal identification numbers (PINs), and tokens. Using its web interface, users can be activated or deactivated, PINs can be configured, and tokens can be assigned to users. Users can be created locally or retrieved from identity repositories.

2.12.1 How It's Used

In the example implementation, RSA Authentication Manager was configured to retrieve user account information from AD. Only accounts for privileged users were retrieved and configured. Tokens that had time-sensitive onetime passcodes were assigned to these user accounts, providing 2FA.

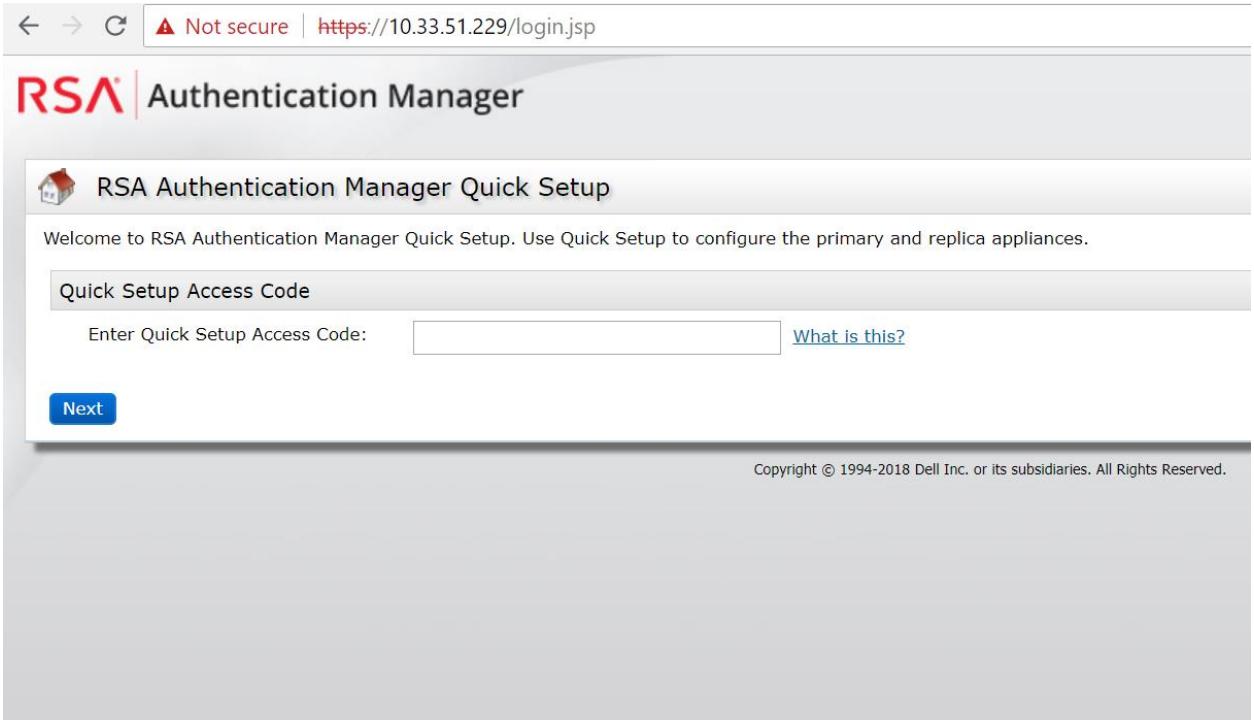
2.12.2 Installation and Initial Configuration

Authentication Manager was deployed as an appliance in the example implementation. Once the appliance boots successfully, the operator will have the opportunity to change or verify the IP address settings. Use the following steps to complete the initial configuration:

1. To log into the system, use the link and the **Quick Setup Access Code** that are displayed after boot:

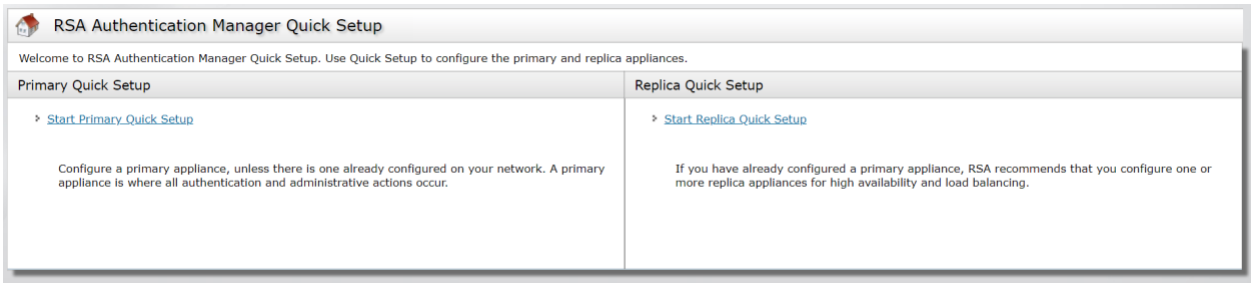
```
RSA Authentication Manager 8.2.0.0.0-build1386271
The appliance network settings have been configured.

Fully qualified hostname: rsa-authmgr.acmefinancial.com
IP address: 172.16.4.15
Subnet mask: 255.255.255.0
Default gateway: 172.16.4.1
DNS servers: 172.16.3.10

To complete the appliance configuration, access Quick Setup at:

    https://172.16.4.15/
    Quick Setup Access Code: 0LfVaE6a
```

2. Enter the **Quick Setup Access Code,** click **Next,** and then accept the license agreement.



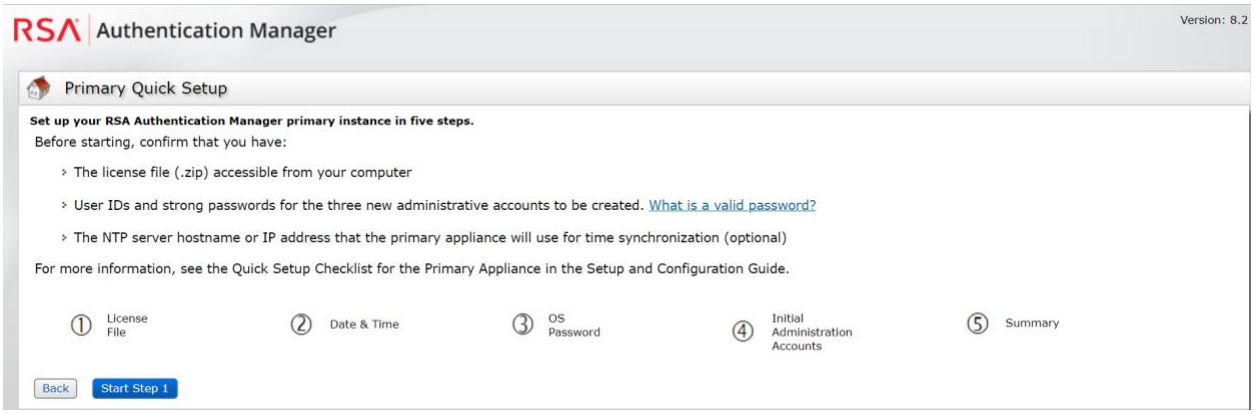
1361

1362 3. Click **Start Primary Quick Setup.**



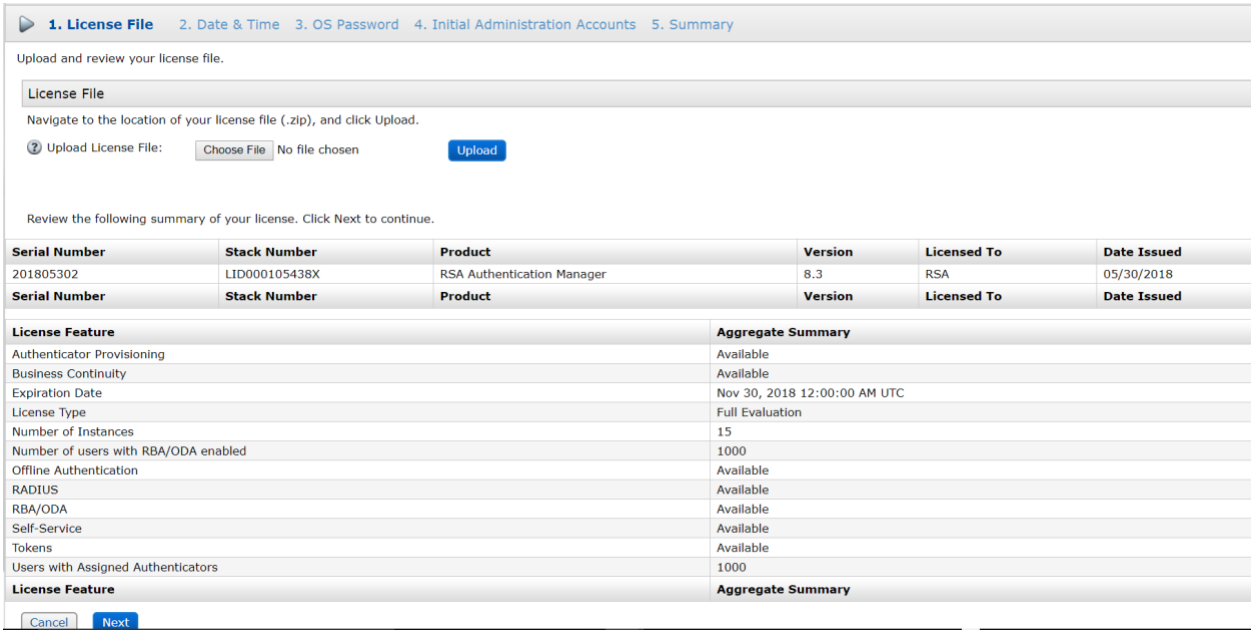
1363

1364 4. Review the information, and then click **Start Step 1.**



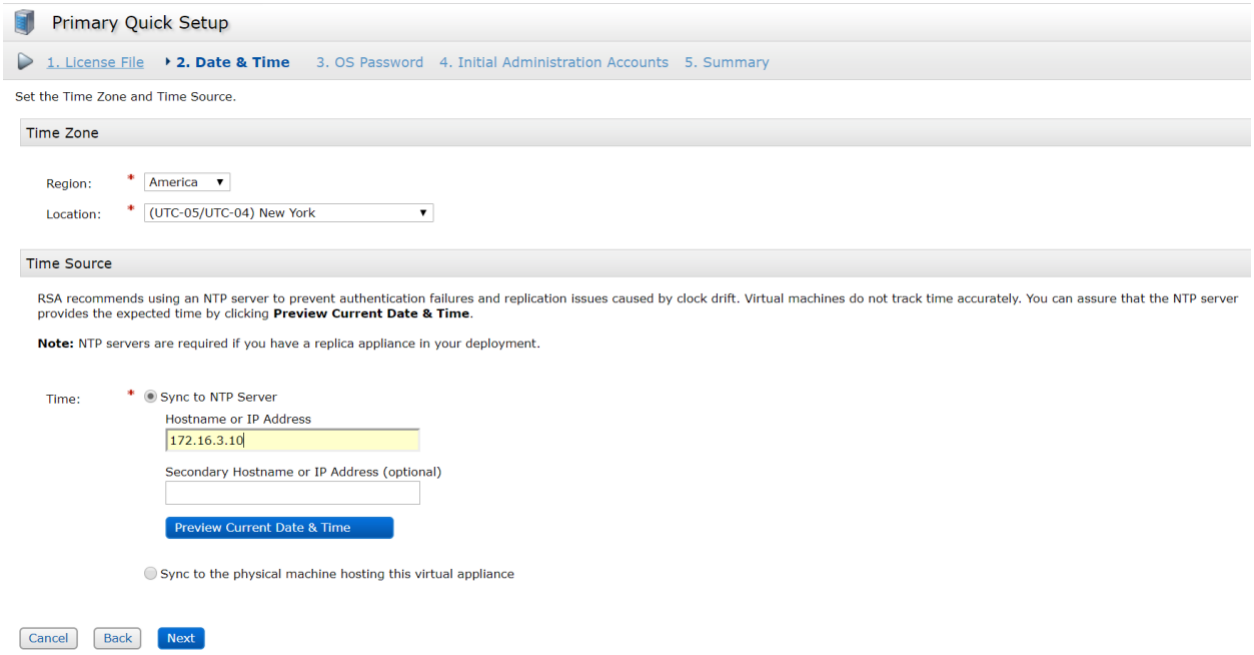
1365

1366 5. Upload the License File by clicking **Choose File,** selecting the appropriate file and clicking **Open,**
1367 and then clicking **Upload.**



1368

1369 6. Enter the **Hostname or IP Address** of the NTP server in your environment, and then click **Next.**



7. Enter the credentials for the Authentication Manager's OS, and then click **Next.**

8. On the following screen, enter the credentials for the **Operations Console admin** and the **Security Console admin.**

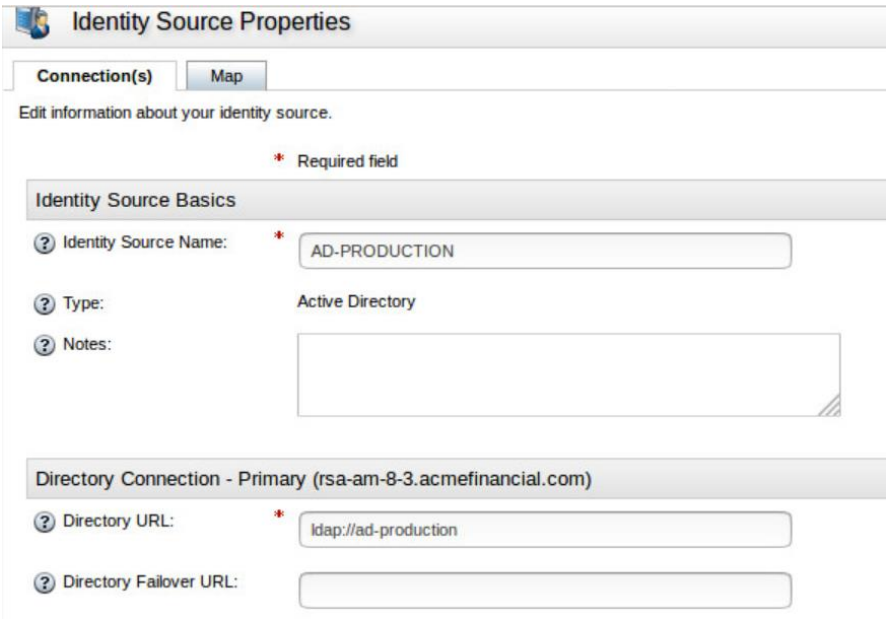
2.12.3 LDAP Integration

Authentication Manager can be configured to connect to LDAP sources and to retrieve user profiles for easy management. The following steps are used to connect to LDAP repositories, to retrieve user account information, and to manage tokens assigned to users:

1. Go to the operations console by navigating your web browser to https://<appliance_IP_address>/oc.

2. Enter the credentials to log into the operations console.

3. Navigate to **Deployment Configuration > Identity Sources > Add New.** On the **Connection(s)** tab in the appropriate fields, add the values necessary for your environment:

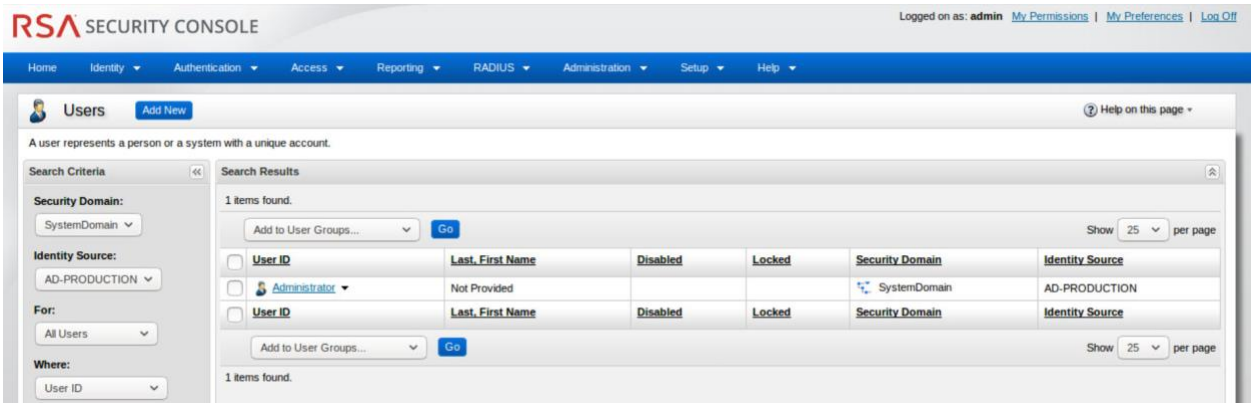


4. Enter the value of a domain admin, such as `administrator@acmefinancial.com`, in the **Directory User ID** field.
5. Click **Test Connection.**

2.12.4 Token Assignment

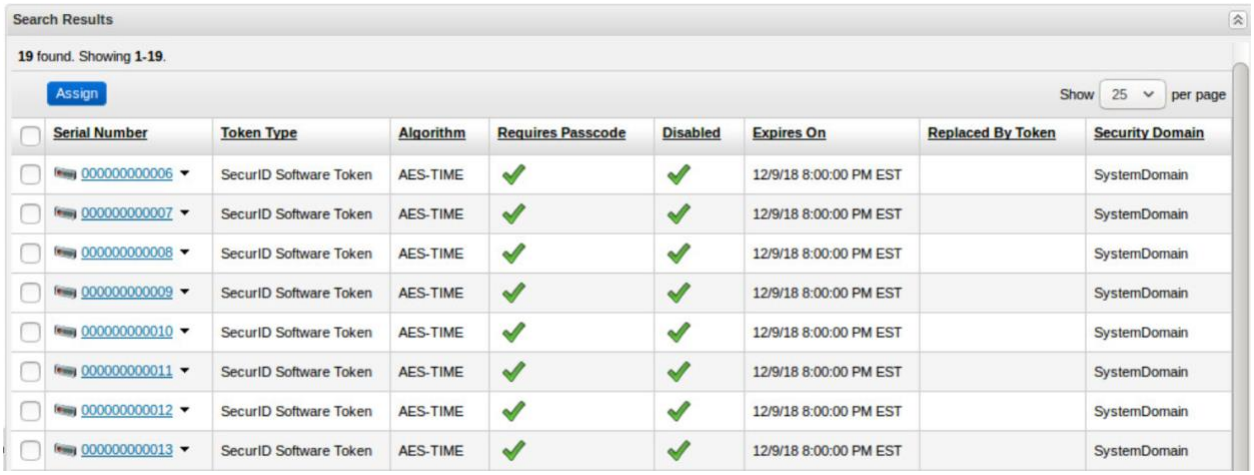
To assign a token to a user, use the following steps:

1. Go to the security console by navigating your web browser to https://<appliance_IP_address>/sc.
2. Enter the credentials to log into the security console.
3. Navigate to **Identity > Users > Manage Existing.**
4. Ensure that the **Identity Source** field points to your AD server, identified by its unique name given in the operations console.
5. In the **Where** field, select **User ID.**
6. In the search bar, enter the User ID for which you would like to search.
7. The user account will be retrieved and displayed.



8. Click on the User ID (by selecting the check box to the left of the User ID), and then click **SecurID Tokens.**

9. Click **Assign Token.**



10. Select a serial number (by selecting the check box to the left of the serial number), and then click **Assign.**

2.12.5 Software Token Profiles and Token Distribution

Software Token Profiles specify parameters that enable the secure distribution of assigned tokens to users. Use the information provided at https://community.rsa.com/docs/DOC-77084 to create a software token profile. To distribute an assigned token to a user, follow the instructions provided at https://community.rsa.com/docs/DOC-77090.

2.13 Splunk

Splunk is a security information and event management system that allows collecting and parsing logs and data from multiple systems.

2.13.1 How It's Used

Splunk can receive data from a plethora of different sources. The most reliable option is installing Splunk's Universal Forwarder on each system from which you want to collect data. Other options include syslogs, file and directory monitoring, and network events. Once data has been collected by Splunk, it can then be parsed and displayed by using prebuilt rules or custom criteria. Splunk is used to report and alert on unauthorized activity.

2.13.2 Installation

Note: You will need a Splunk account to download Splunk Enterprise. The account is free and can be set up at https://www.splunk.com/page/sign_up.

Download Splunk Enterprise from https://www.splunk.com/en_us/download/splunk-enterprise.html. This build uses Version 7.0.3. Splunk can be installed on Windows, Linux, Solaris, and Mac OS X. Each of these installation instructions is provided at http://docs.splunk.com/Documentation/Splunk/7.1.3/Installation/Beforeyouinstall.

2.13.3 Queries

Two Splunk reports were created for this build. One of the reports is named **DemoBomgar-AD-Auth-UnauthV1,** which captures activities that are authorized or activities that violate the workflow. The other report is named **DemoRadiant-AD-Event-Details,** which captures more details of those events and can be used as a secondary monitor for AD.

2.13.4 DemoBomgar-AD-Auth-UnauthV1

```
index="demo" sourcetype=_json OR sourcetype="csv" NOT host="radiant-logic" NOT ("A
user account was changed" OR "A user account was enabled")|where NOT like(UserObject,
"UserObject%")|eval BomgarUserSubject=substr('Event.@sOriginatingAccount',15)|table
_time host Event.@sEventID Event.@sLoginName Event.@sMessage BomgarUserSubject
UserSubject UserObject Event|eval
UserSubject=if(isnotnull(BomgarUserSubject),BomgarUserSubject,UserSubject)|transaction
UserSubject maxspan=240s|eval
Policy=if((BomgarUserSubject==UserSubject),"Authorized","Unauthorized")|table _time
host Policy Event.@sEventID Event.@sLoginName UserSubject UserObject Event
```

2.13.5 DemoRadiant-AD-Event-Details

```
index="demo"
source="C:\\radiantone\\vds\\r1syncsvcs\\log\\cf_o_acmefinancial\\object_generic_dv_so
_o_acmefinancial_capture.log" OR source="c:\\final_ad.csv" NOT ("A user account was
changed" OR "A user account was enabled") |rex
"\<sAMAccountName\>(?P<LDAPObject>.+)\<\/sAMAccountName\>" |rex
"\<RLICHANGETYPE\>(?P<RLICHANGETYPE>\w+)"|rex
"<RLICHANGES>(?P<RLICHANGES>.+)\<\/RLICHANGES\>"|rex
"\<userPrincipalName\>(?P<UserObject>\w+)\@"|table _time host UserSubject LDAPObject
UserObject Event RLICHANGETYPE RLICHANGES|where isnotnull(UserSubject) OR
isnotnull(UserObject)| where NOT like(UserObject, "MSOL%")|where NOT like(UserObject,
"UserObject%")|table _time host UserSubject LDAPObject UserObject Event RLICHANGETYPE
RLICHANGES|where NOT like(RLICHANGES, "replace: logonCount%")|eval
RLICHANGETYPE=if(LIKE(Event,"%added%"),"update",RLICHANGETYPE)|eval
RLICHANGETYPE=if(LIKE(Event,"%created%"),"insert",RLICHANGETYPE)|table _time host
UserSubject UserObject LDAPObject Event RLICHANGETYPE RLICHANGES|eval
UserObject=if(LIKE(LDAPObject,"%Admin%"),"",UserObject)
```

2.13.6 SSL Forwarding

We took advantage of Splunk's built-in SSL forwarding capability and configured SSL encryption between forwarders and the indexer. Instructions to enable SSL forwarding are provided at http://docs.splunk.com/Documentation/Splunk/7.1.3/Security/ConfigureSplunkforwardingtousesignedcertificates.

Appendix A List of Acronyms

2FA	Two-Factor Authentication
AD	Active Directory
CA	Certificate Authority
CPU	Central Processing Unit
DNS	Domain Name System
FID	Federated Identity
FQDN	Fully Qualified Domain Name
GB	Gigabyte(s)
HDD	Hard Disk Drive
IIS	Internet Information Services
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
N/A	Not Applicable
NCCoE	National Cybersecurity Center of Excellence
NIC	Network Interface Controller/Card
NIST	National Institute of Standards and Technology
OS	Operating System
PAM	Privileged Account Management
PIN	Personal Identification Number
QR	Quick Response
RAM	Random-Access Memory

SAML	Security Assertion Markup Language
SMB	Server Message Block
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
URL	Uniform Resource Locator