

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>



1 Executive Summary

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

19 CHALLENGE

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

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

35 SOLUTION

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

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

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

44 The NCCoE sought existing technologies that provided the following capabilities:

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

61 While the NCCoE used a suite of commercial products to address this challenge, this guide does not
62 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your
63 organization's information security experts should identify the products that will best integrate with
64 your existing tools and information-technology system infrastructure. Your organization can adopt this
65 solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point
66 for tailoring and implementing parts of a solution.

67 **BENEFITS**

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

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

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

80 **SHARE YOUR FEEDBACK**

81 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
 82 read the guide. If you adopt this solution for your own organization, please share your experience and
 83 advice with us. We recognize that technical solutions alone will not fully enable the benefits of our
 84 solution, so we encourage organizations to share lessons learned and best practices for transforming the
 85 processes associated with implementing this guide.

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

90 **TECHNOLOGY PARTNERS/COLLABORATORS**

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



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

1 **Contents**

2	1	Summary	1
3	1.1	Challenge	3
4	1.2	Solution.....	4
5	1.3	Benefits.....	5
6	2	How to Use This Guide	6
7	2.1	Typographic Conventions.....	7
8	3	Approach	8
9	3.1	Audience.....	8
10	3.2	Scope	8
11	3.3	Assumptions	9
12	3.4	Risk Assessment	9
13	3.4.1	Assessing Risk Posture	10
14	3.4.2	Security Control Map	11
15	3.5	Security Functions and Subcategories Related to FFIEC	18
16	3.6	Technologies.....	22
17	4	Architecture	25
18	4.1	Architecture Description	26
19	4.1.1	High-Level Architecture	26
20	4.1.2	Reference Design	27
21	5	Example Implementations.....	30
22	5.1	Example Implementation 1: Application Layer PAM	31
23	5.2	Example Implementation 2: Organization Infrastructure PAM	34
24	5.3	Example Implementation 3: SIEM	36
25	5.4	Security Monitoring Implementation.....	38
26	5.5	Use Cases.....	39
27	5.5.1	Typical Administrator (Directory, Cloud Service, Etc.).....	39
28	5.5.2	Security Analyst.....	40

29	5.5.3 Business-Critical/High-Value Application Access.....	41
30	6 Security Characteristic Analysis	42
31	6.1 Assumptions and Limitations	43
32	6.2 Build Testing	43
33	6.3 Scenarios and Findings	43
34	6.4 Analysis of the Reference Design’s Support for Cybersecurity Framework Subcategories	43
35	6.4.1 Supported Cybersecurity Framework Subcategories	49
36	6.5 Security of the Reference Design	56
37	6.5.1 Securing New Attack Surfaces	57
38	6.5.2 Securing Access to the LDAP Directory	59
39	6.5.3 Securing Access to the Policy Management Capability	59
40	6.5.4 Securing Access to the User Interface (Access Control) Capability	59
41	6.5.5 Securing Password Vault Capability.....	60
42	6.5.6 Securing Emergency Access Capability	60
43	6.5.7 Securing Access to the Security Monitoring and Analytics Capability.....	60
44	6.5.8 Ensuring Information Integrity.....	60
45	6.5.9 Protecting Privileged Accounts	61
46	6.5.10 Preventing Insider Threats.....	61
47	6.5.11 Addressing Attacks.....	62
48	6.5.12 User Behavior Analytics	63
49	6.6 Deployment Recommendations.....	64
50	6.6.1 Patch, Harden, Scan, and Test	64
51	6.6.2 Other Security Best Practices.....	65
52	6.6.3 Deployment Phases	66
53	6.6.4 Policy Recommendations.....	67
54	7 Functional Evaluation.....	67
55	7.1 PAM Functional Test Plan.....	67
56	7.1.1 PAM Use Case Requirements	69
57	7.1.2 Test Case: PAM-1	70

59	7.1.3	Test Case: PAM-2	72
60	7.1.4	Test Case: PAM-3	73
61	7.1.5	Test Case: PAM-4	74
62	7.1.6	Test Case: PAM-5	75
63	7.1.7	Test Case: PAM-6	76
64	7.1.8	Test Case: PAM-7	77
65	7.1.9	Test Case: PAM-8	78
66	Appendix A	List of Acronyms	80
67	Appendix B	References	82

68 **List of Figures**

69	Figure 4-1 High-Level Architecture	26
70	Figure 4-2 PAM Reference Design	27
71	Figure 5-1 Example Implementation 1: Application Layer PAM Architecture (Option 1).....	32
72	Figure 5-2 Example Implementation 1: Application Layer PAM Architecture (Option 2).....	33
73	Figure 5-3 Example Implementation 2: Organization Infrastructure PAM Architecture	34
74	Figure 5-4 Example Implementation 3: SIEM Architecture	37
75	Figure 5-5 Security Monitoring Implementation Architecture.....	39

76 **List of Tables**

77	Table 3-1 PAM Reference Design Cybersecurity Framework Core Components Map	12
78	Table 3-2 FFIEC CAT Guidance	18
79	Table 3-3 Products and Technologies	22
80	Table 5-1 Example Implementation Component List	30
81	Table 6-1 PAM Reference Design Capabilities and Supported Cybersecurity Framework Subcategories	44
83	Table 7-1 Test Case Fields.....	68

84	Table 7-2 PAM Functional Requirements.....	69
85	Table 7-3 Test Case ID: PAM-1.....	70
86	Table 7-4 Test Case ID: PAM-2.....	72
87	Table 7-5 Test Case ID: PAM-3.....	73
88	Table 7-6 Test Case ID: PAM-4.....	74
89	Table 7-7 Test Case ID: PAM-5.....	75
90	Table 7-8 Test Case ID: PAM-6.....	76
91	Table 7-9 Test Case ID: PAM-7.....	77
92	Table 7-10 Test Case ID: PAM-8.....	78

93 1 Summary

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

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

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

119 Managing the access and use of privileged accounts is difficult without proper planning and tools. The
120 National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and
121 Technology (NIST) built a laboratory environment to explore methods to **manage and monitor the use**
122 **of privileged accounts by authorized users** as they perform their normal activities, as well as techniques
123 **to protect against and detect the unauthorized use of privileged accounts**. NIST Special Publication (SP)
124 800-171 [1], *Protecting Controlled Unclassified Information in Nonfederal Information Systems and*
125 *Organizations*, defines a privileged user as “a user that is authorized (and therefore, trusted) to perform
126 security-relevant functions that ordinary users are not authorized to perform.” Privileged accounts are
127 utilized in managing IT infrastructures, resources, and applications, as well as access to, and the use of,
128 high-value applications like payment systems, accounting systems, and social media accounts.

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

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

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

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

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

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

168 1.1 Challenge

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

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

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

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

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

198 **1.2 Solution**

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

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

213 The NCCoE sought existing technologies that provided the following capabilities:

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

223 While the NCCoE used a suite of commercial products to address this cybersecurity challenge, this guide
224 does not endorse these particular, nor does it guarantee compliance with any regulatory initiatives. Your
225 organization's information security experts should identify the products that will best integrate with
226 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that
227 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and
228 implementing parts of the design to the needs of your organization and its risk management decisions.

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

- 231 ■ NIST SP 800-171 Rev. 1: *Protecting Controlled Unclassified Information in Nonfederal Systems*
232 *and Organizations* [\[1\]](#)
- 233 ■ *NIST Framework for Improving Critical Infrastructure Cybersecurity* (commonly known as the
234 NIST Cybersecurity Framework) [\[3\]](#)
- 235 ■ NIST SP 800-30 Rev. 1: *Guide for Conducting Risk Assessments* [\[4\]](#)
- 236 ■ NIST SP 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal*
237 *Information Systems: A Security Life Cycle Approach* [\[5\]](#)
- 238 ■ NIST SP 800-39: *Managing Information Security Risk* [\[6\]](#)
- 239 ■ NIST SP 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and*
240 *Organizations* [\[7\]](#)
- 241 ■ Federal Information Processing Standards (FIPS) 140-2: *Security Requirements for Cryptographic*
242 *Modules* [\[8\]](#)
- 243 ■ NIST SP 800-92: *Guide to Computer Security Log Management* [\[9\]](#)
- 244 ■ NIST SP 800-100: *Information Security Handbook: A Guide for Managers* [\[10\]](#)
- 245 ■ Office of Management and Budget (OMB), Circular Number A-130: *Managing Information as a*
246 *Strategic Resource* [\[11\]](#)
- 247 ■ Federal Financial Institutions Examination Council (FFIEC), *Cybersecurity Assessment Tool* (CAT)
248 [\[12\]](#)
- 249 ■ NIST SP 800-63B: *Digital Identity Guidelines: Authentication and Lifecycle Management* [\[13\]](#)

250 **1.3 Benefits**

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

256 The NCCoE’s practice guide can help an organization:

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

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

2 How to Use This Guide

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

271 This guide contains three volumes:

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

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

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

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

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

- 285 ■ [Section 3.4](#), Risk Assessment, provides a description of the risk analysis we performed
- 286 ■ [Section 3.4.2](#), Security Control Map, maps the security characteristics of this example solution to
287 cybersecurity standards and best practices

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

291 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.
 292 You can use the How-To portion of the guide, *NIST SP 1800-18C*, to replicate all or parts of the build
 293 created in our lab. The How-To portion of the guide provides specific product installation, configuration,
 294 and integration instructions for implementing the example solution. We do not recreate the product
 295 manufacturers' documentation, which is generally widely available. Rather, we show how we
 296 incorporated the products together in our environment to create an example solution.

297 This guide assumes that IT professionals have experience implementing security products within the
 298 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
 299 not endorse these particular products. Your organization can adopt this solution or one that adheres to
 300 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
 301 parts of a PAM solution. Your organization's security experts should identify the products that will best
 302 integrate with your existing tools and IT system infrastructure. We hope that you will seek products that
 303 are congruent with applicable standards and best practices. [Section 3.6](#), Technologies, lists the products
 304 we used and maps them to the cybersecurity controls provided by this reference solution.

305 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
 306 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
 307 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
 308 financial_nccoe@nist.gov.

309 2.1 Typographic Conventions

310 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
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	<code>mkdir</code>
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

311 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).

316 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

324 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

333 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

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

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

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

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

358 **3.3 Assumptions**

359 This project is guided by the following assumptions:

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

364 **3.4 Risk Assessment**

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

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

378 We performed two types of risk assessment:

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

383 **3.4.1 Assessing Risk Posture**

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

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

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

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

406 ■ system unavailability
407 ■ data manipulation
408 We subsequently translated the identified operational risk factors to security functions and
409 subcategories within the NIST Cybersecurity Framework.

410 **3.4.2 Security Control Map**

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

423 Note: Not all of the Cybersecurity Framework subcategory guidance can be implemented by using
424 technology. Any organization executing a PAM solution would need to adopt processes and
425 organizational policies that address organization risk management. Many of the subcategories require
426 that processes and policies be developed prior to implementing the technical recommendations within
427 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.PI.B.5 D5.IR.PI.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	
PROTECT (PR)	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 : Privileged Account Management	PR.AC : Access Control	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
	PR.DS : Data Security	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	
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.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
		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.PI.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.PI.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

430 **3.5 Security Functions and Subcategories Related to FFIEC**

431 The example implementations are responsive to the desire to support compliance with the FFIEC CAT
432 [\[12\]](#) guidance and with the NIST standards and best practices, as detailed in [Table 3-1](#).

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

437 [Table 3-2](#) describes how the PAM solution supports compliance with FFIEC CAT guidance.

438 **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
<p>D5.IR.PI.B.5: A formal backup and recovery plan exists for all critical business lines.</p> <p>D5.IR.PI.E.3: Alternative processes have been established to continue critical activity within a reasonable time.</p>	<p>The solutions include emergency access and can be implemented with high-availability components.</p>
<p>D3.PC.Im.B.7: Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.</p> <p>D3.PC.Am.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware.</p>	<p>The solutions provide automated account access control for privileged users and for MFA authentication.</p>
<p>D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.</p> <p>D3.PC.Am.B.2: Employee access to systems and confidential data provides for separation of duties.</p> <p>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.</p>	<p>The solutions provide automated policy enforcement for account access control for privileged users.</p>
<p>D3.DC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p>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.</p>	<p>The solutions are implemented by using network defense tools and network segmentation to illustrate support for this guidance.</p>
<p>D1.G.IT.B.13: Confidential data is identified on the institution's network.</p> <p>D3.PC.Am.A.1: Encryption of select data at rest is determined by the institution's data classification and risk assessment.</p>	<p>The solutions protect confidential data by using encryption of data-at-rest (PAM passwords) and can support this guidance.</p>
<p>D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., internet).</p> <p>D3.PC.Am.E.5: Controls are in place to prevent unauthorized access to cryptographic keys.</p>	<p>The solutions include encryption capabilities and can be implemented to support this guidance.</p>

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.	
<p>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.</p> <p>D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.</p> <p>D3.PC.Am.Int.1: The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.</p> <p>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).</p>	The solutions provide automated account access control, including MFA for privileged users. Account access to confidential data is controlled to support this guidance.
<p>D1.G.SP.B.3: The institution has policies commensurate with its risk and complexity that address the concept of threat information sharing.</p> <p>D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.</p> <p>D2.MA.Ma.B.2: Computer event logs are used for investigations once an event has occurred.</p>	The solutions provide automated log collection and analysis to support this guidance.
<p>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).</p> <p>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.</p> <p>D3.PC.Am.B.7: Access controls include password complexity and limits to password attempts and reuse.</p> <p>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.</p>	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.
<p>D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response.</p> <p>D3.DC.An.Int.3: Tools actively monitor security logs for anomalous behavior and alert within established parameters.</p> <p>D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions.</p>	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.
<p>D5.ER.Re.B.4: Incidents are classified, logged, and tracked.</p> <p>D5.ER.Es.B.4: Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.</p> <p>D5.IR.PI.B.2: Communication channels exist to provide employees a means for reporting information security events in a timely manner.</p>	The solutions are designed by using automated log collection and analysis to support this guidance.
<p>D3.CC.Re.Int.3: Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties.</p> <p>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.</p>	The solutions can be implemented to support this guidance.

439 **3.6 Technologies**

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

445 **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)	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

446 4 Architecture

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

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

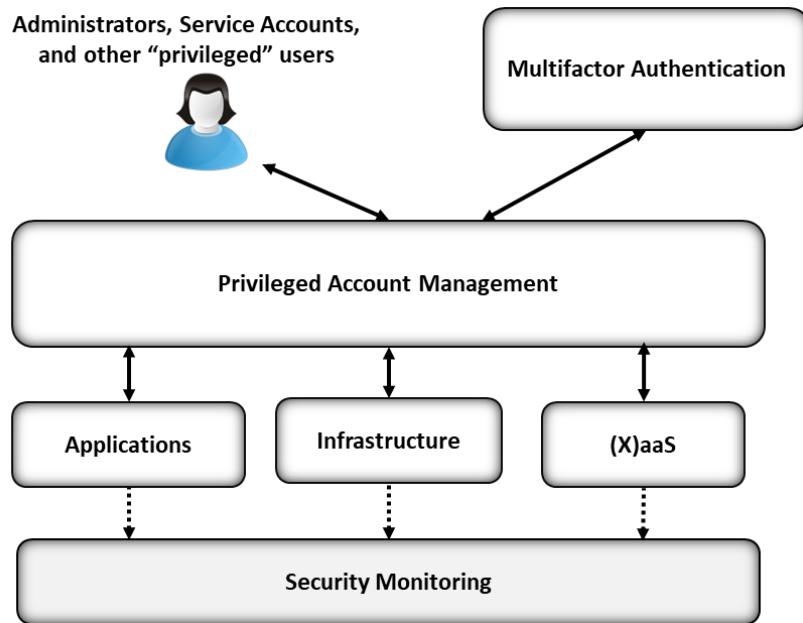
453 The PAM architecture and reference design identify the set of capabilities and their relationships that,
 454 when combined, can be used to control and monitor the use of privileged accounts by privileged users,
 455 for both on-premises and cloud implementations. This section presents a high-level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

461 **4.1 Architecture Description**

462 **4.1.1 High-Level Architecture**

463 The PAM solution is designed to address the security functions and subcategories described in [Table 3-1](#)
 464 and is composed of the capabilities illustrated in [Figure 4-1](#) and [Figure 4-2](#).

465 **Figure 4-1 High-Level Architecture**



466
 467 [Figure 4-1](#) depicts the PAM architecture within the context of an enterprise. A PAM system is designed
 468 to mediate/control access to, and the use of, privileged accounts between enterprise systems and
 469 services and authorized “privileged” users. In [Figure 4-1](#), “[X]aaS” stands for “[fill in the blank] as a

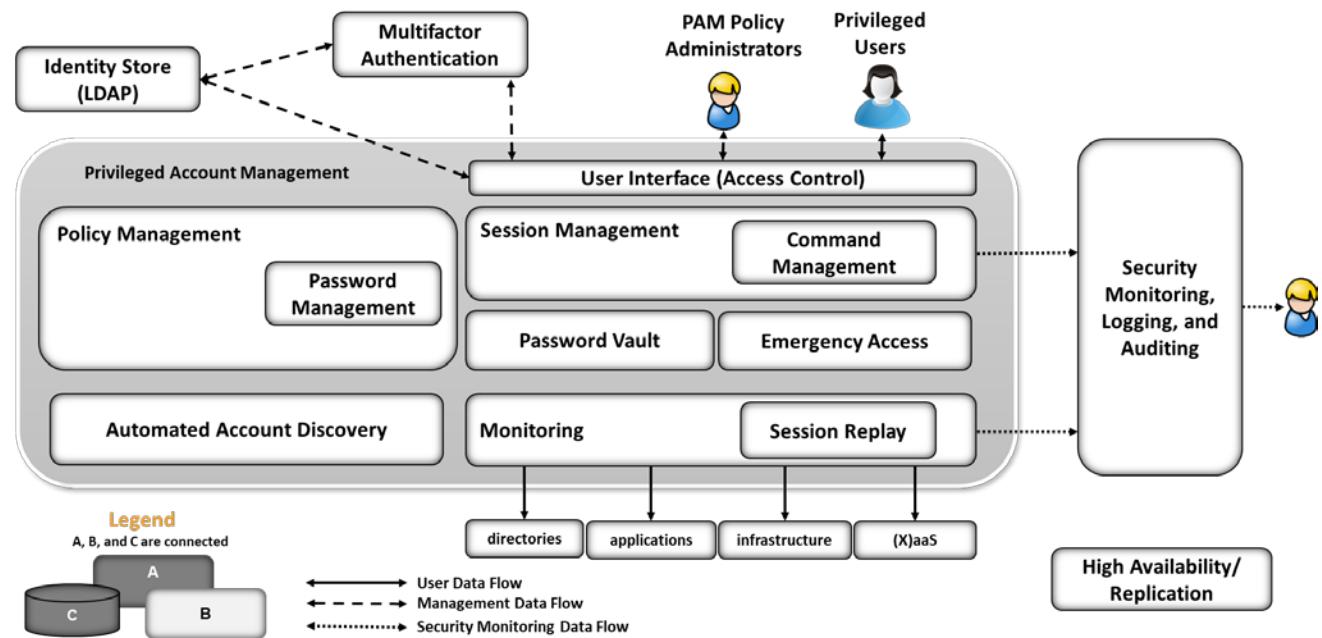
470 service,” such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud services. Examples of each of these cloud services are as follows:

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

475 4.1.2 Reference Design

476 The reference design shown in [Figure 4-2](#) depicts the detailed PAM design, including the relationships
 477 among the capabilities that compose the design.

478 **Figure 4-2 PAM Reference Design**



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

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

- 489 3. The user interface provides login authentication and a user-to-PAM-system interactive interface
490 through which users interact to establish or request work sessions for each system that they
491 administer or access to perform their work functions.
- 492 4. Policy management maintains the enterprise privileged-user access and control policies, such as
493 limiting privileged user sessions to four hours.
- 494 5. Password management maintains and enforces the enterprise password policies.
- 495 6. Session management enforces the enterprise access and control policies within each work
496 session, such as limiting sessions to SSH or RDP or limiting allowed application use on the target
497 system.
- 498 7. The password vault provides secure storage of the current password for each privileged account
499 managed by the PAM system.
- 500 8. Emergency access provides PAM use in unpredicted or emergency situations when access to
501 privileged accounts is required by unanticipated users (privileged or nonprivileged).
- 502 9. Automated account discovery searches the enterprise for evidence and identification of
503 privileged accounts, such as domain administrators or accounts that directly or indirectly
504 (through inheritance of privileges) have privileged-account-level authority.
- 505 10. Session monitoring provides a mechanism to identify, log, and alert on anomalous activity as
506 well as for real-time training for privileged account use.
- 507 11. Session replay provides session review for training and event review and investigations.
- 508 12. Security monitoring, logging, and auditing provides log storage, analysis, and alerting
509 components, generally referred to as security information and event management (SIEM).
- 510 13. UBA monitors the activity of the privileged users for activity or actions that are considered to be
511 unexpected or outside a recognized pattern of activity.
- 512 14. High availability/replication ensures the availability of the PAM solution.
- 513 PAM systems typically use one of two techniques for controlling account access and use: account
514 escalation or account sharing. The account escalation technique escalates the privileged/authorized
515 activity for each user's personal account for the duration of the session with the target system, based on
516 the organizational policies. When each session is completed, the user's account is returned to its
517 "normal"/nonprivileged authorization level. The account sharing technique utilizes a set of privileged
518 accounts that are shared among the authorized privileged users. The passwords for these accounts are
519 typically changed automatically, based on usage or time. For example, account-sharing PAM systems
520 may be set up to change the password for each account after every session in which it is used, or, if
521 unused, after a specific amount of time. Some organizations may choose to utilize an account-sharing
522 PAM system with unique user-specific PAM accounts. This approach may provide simplified log analysis
523 for forensic and training purposes, as the target system will record each unique user in its logs.

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

533 In PAM systems that implement account escalation techniques to manage privileged users, the session
534 management system escalates the privilege of each user for the duration of the session with the target
535 system, based on the policies within the policy management system. Session management monitors the
536 session to return the account privilege level to its normal state after the user ends the session. Session
537 management also logs the user account requests and the session request details according to enterprise
538 policies. The target systems log the activity of each privileged user and send logs to the SIEM. NIST SP
539 800-92, *Guide to Computer Security Log Management* [9], was utilized for SIEM implementation and
540 configuration guidance. The SIEM stores logs generated by each system and performs analytics to
541 identify anomalous activity. Anomalous activity is reported to security analysts.

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

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

553 UBA solutions are designed to detect behaviors of concern by combining all relevant data (e.g., network
554 and client/host-based activity, human resource systems, employee reports, public records, travel
555 records), and to then look for meaningful patterns of behavior. For example, a UBA solution can detect
556 that an attack, such as a privilege escalation attack, has been launched (ideally during the early
557 formative stages of that attack). UBA was not included in the example implementations due to the lack
558 of relevant data needed for effective pattern-of-behavior analysis. Because UBA techniques vary widely,
559 UBA for PAM may be considered by organizations that can identify the specific dimensions of behavior
560 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.

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

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

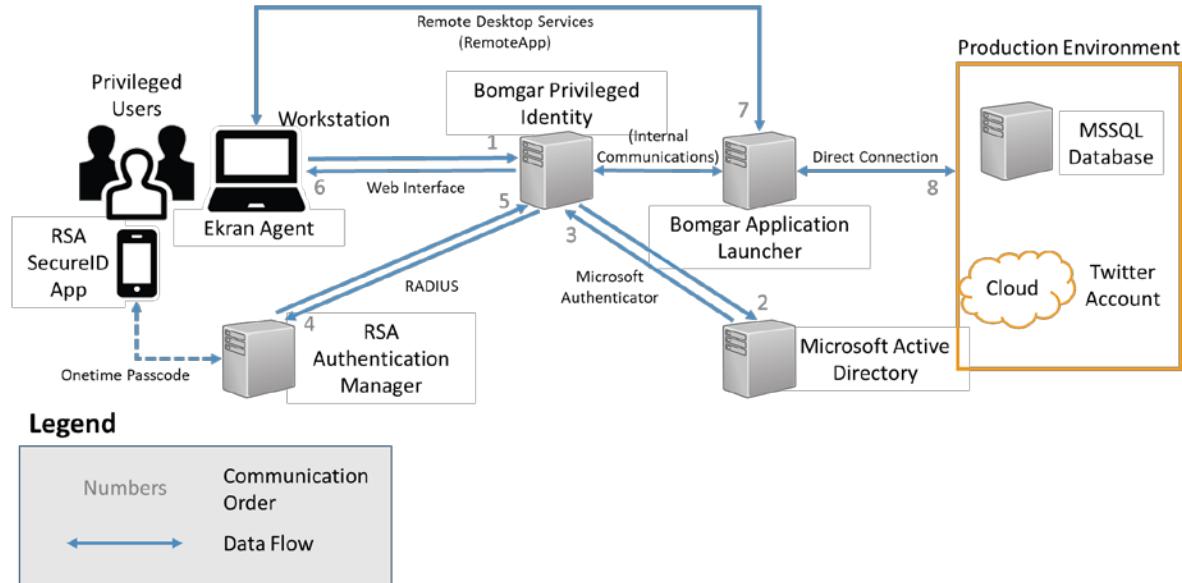
598 5.1 Example Implementation 1: Application Layer PAM

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

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

- 608 ■ Bomgar (formerly Lieberman) Privileged Identity and Application Launcher provides PAM
609 capabilities.
- 610 ■ The Ekran agent provides PAM monitoring capabilities for the privileged user workstations.
- 611 ■ RSA Authentication Manager provides onetime-passcode synchronization and authentication
612 (Option 1, [Figure 5-1](#)).
- 613 ■ IdRamp Secure Access, combined with Microsoft Authenticator and Azure Active Directory
614 services, provides onetime-passcode synchronization and authentication (Option 2, [Figure 5-2](#)).
- 615 ■ Microsoft Active Directory provides the enterprise privileged-user identity store (source for
616 privileged user identity information).
- 617 ■ Splunk Enterprise provides the security monitoring, logging, and auditing component (SIEM)
618 (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)



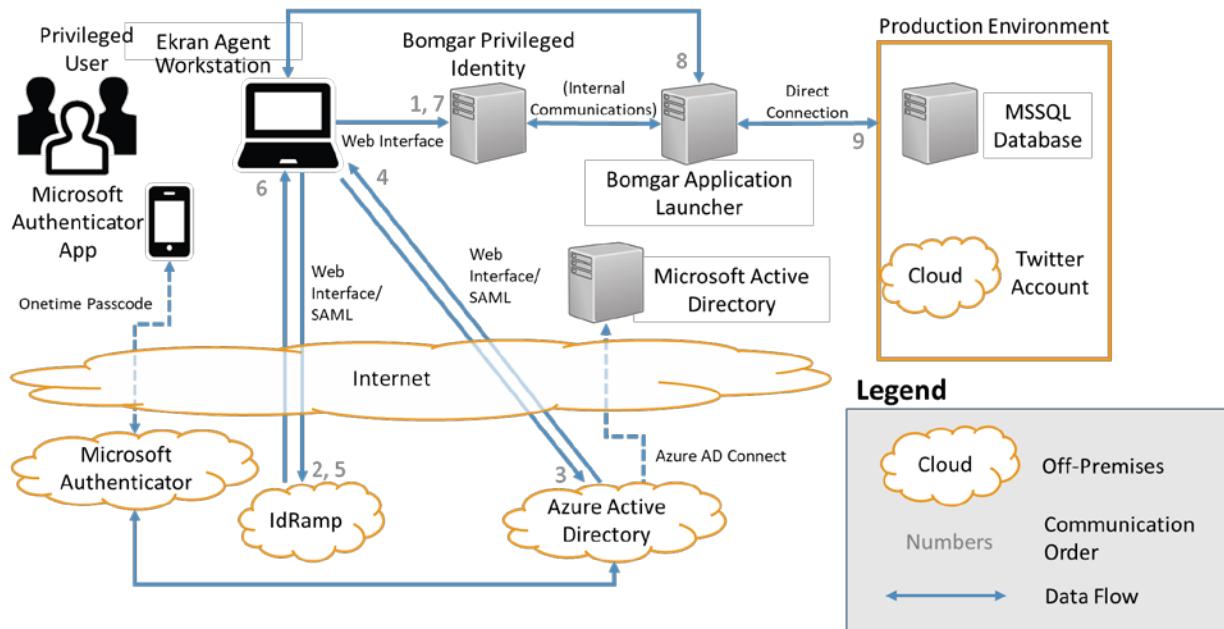
620

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

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

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

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



659

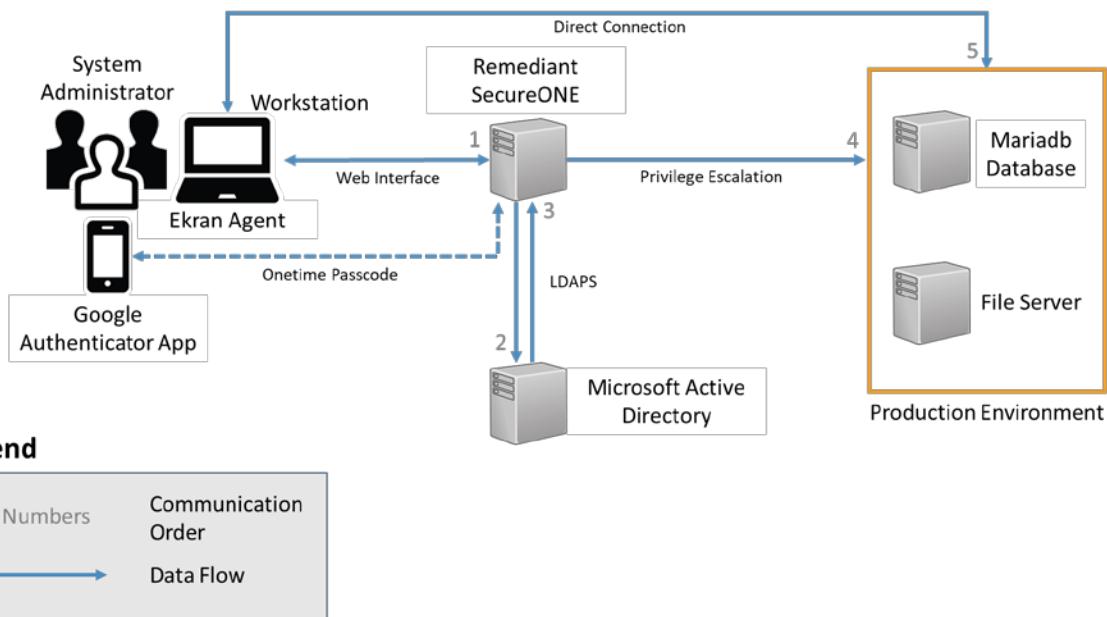
660 5.2 Example Implementation 2: Organization Infrastructure PAM

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

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

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

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



676 677 In this example implementation, the Ekran Agent monitors the privileged user's activity on their
 678 workstations. A best practice is that privileged users perform their work from dedicated workstations.
 679 Those workstations should not be used for nonprivileged user activities like email, web browsing, and

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

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

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

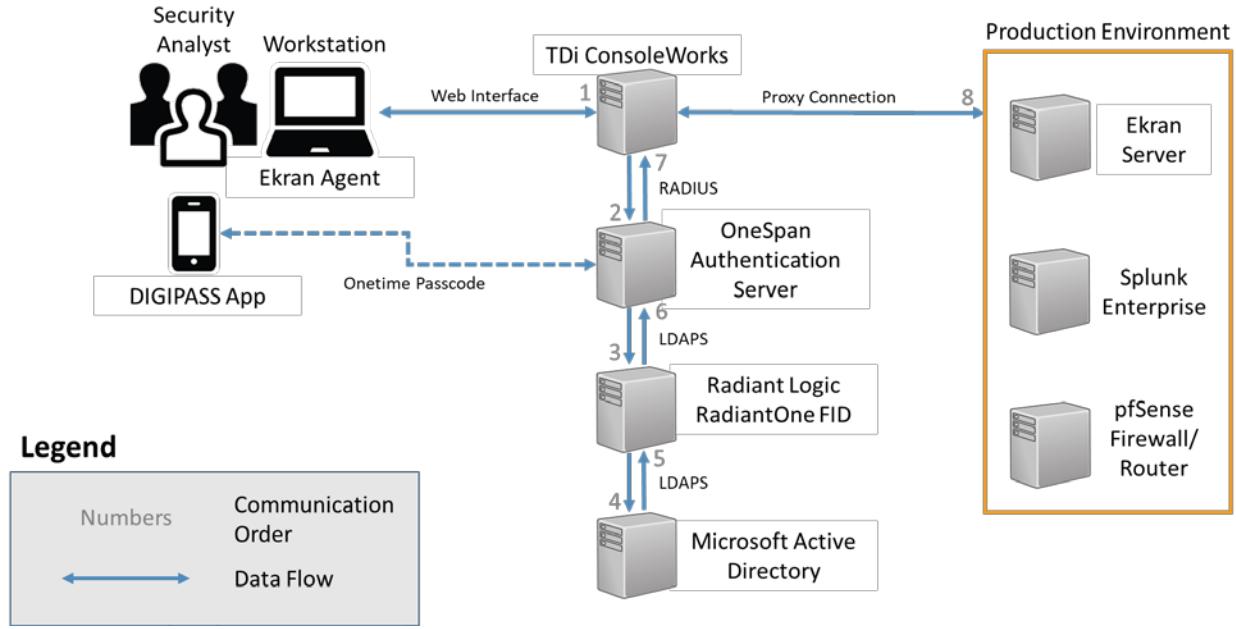
714 **5.3 Example Implementation 3: SIEM**

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

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

- 725 ▪ TDi Consoleworks provides PAM for the security monitoring system.
- 726 ▪ Ekran System provides PAM for the privileged user workstations.
- 727 ▪ OneSpan (formerly VASCO) Authentication Server provides an interface between the PAM
728 components and the MFA second factor for authentication (via mobile application).
- 729 ▪ Radiant Logic RadiantOne FID provides the privileged user identity store.
- 730 ▪ Microsoft Active Directory provides the enterprise standard-user identity store (source for
731 privileged user identity information).
- 732 ▪ 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

754 monitoring system for detecting anomalous activity. The following list describes the authentication and
755 access-control steps referenced in [Figure 5-3](#):

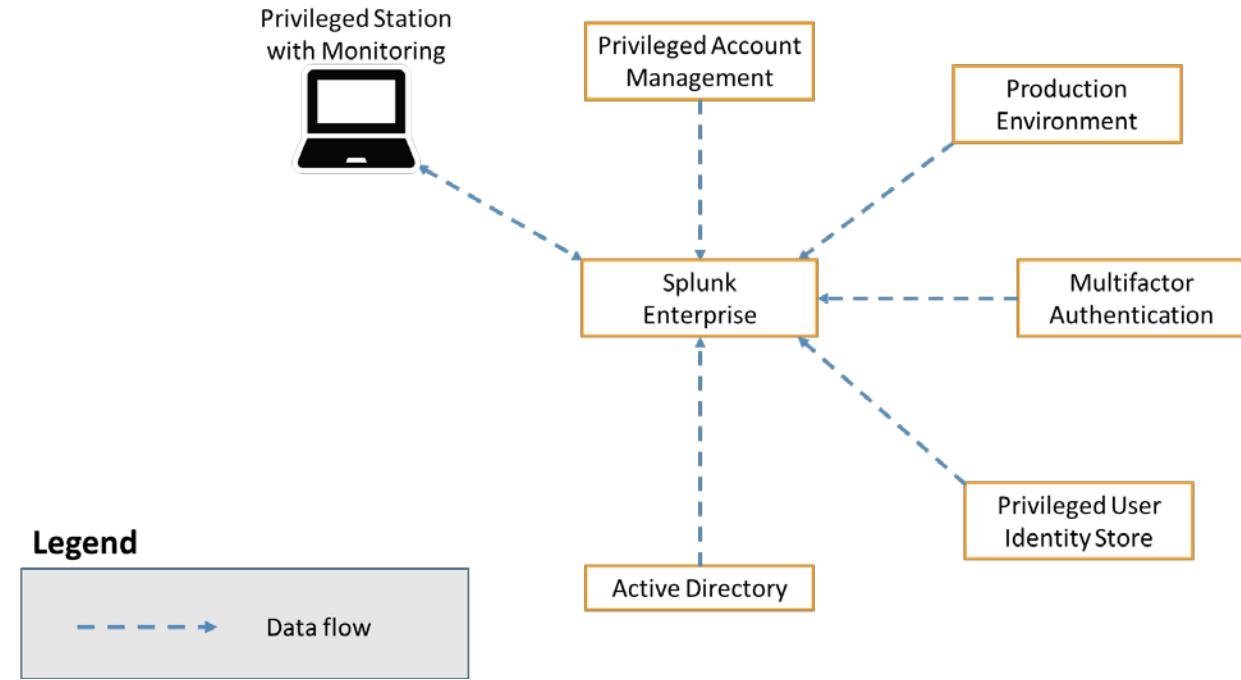
- 756 1. The user connects to the ConsoleWorks web interface by using their username, password, and
757 OneSpan Authentication Server and DIGIPASS onetime-passcode mobile application.
- 758 2. ConsoleWorks authenticates the user by querying the OneSpan server to check the username,
759 password, and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

770 **5.4 Security Monitoring Implementation**

771 Security monitoring is an important aspect of any cybersecurity implementation. The NCCoE based the
772 security monitoring implementation on the guidance found in the Architecture section of NIST SP 800-
773 92, *Guide to Computer Security Log Management* [\[9\]](#). The NCCoE implemented the network
774 segmentation recommendation from NIST SP 800-92 in the solutions described above for
775 management/PAM network use by PAM systems for access to the target systems, excluding the
776 application PAM use. The same management/PAM network would also be used to collect logs from each
777 of the target systems and PAM systems. [Figure 5-5](#) illustrates the data flow across the
778 management/PAM network. Where possible, all data-at-rest and data-in-transit are encrypted.

779 Figure 5-5 Security Monitoring Implementation Architecture

Log and Event Data Flow



780

5.5 Use Cases

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 application.

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

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

800 ***5.5.1.2 Resolution***

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

814 ***5.5.1.3 Other Considerations***

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

819 ***5.5.2 Security Analyst***

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

821 ***5.5.2.1 Scenario***

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

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

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

835 *5.5.2.2 Resolution*

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

844 *5.5.2.3 Other Considerations*

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

848 **5.5.3 Business-Critical/High-Value Application Access**

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

852 *5.5.3.1 Scenario*

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

860 *5.5.3.2 Resolution*

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

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

871 *5.5.3.3 Other Considerations*

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

875

6 Security Characteristic Analysis

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

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

893 6.1 Assumptions and Limitations

894 The security characteristic evaluation has the following limitations:

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

900 6.2 Build Testing

901 The purpose of the security characteristic analysis is to examine the extent to which the example

902 solution meets its objective of demonstrating PAM functionality as defined in [Section 3.2](#). In addition, it

903 is intended to explain the security benefits and drawbacks of the reference design.

904 6.3 Scenarios and Findings

905 One aspect of our security evaluation involved assessing how well the reference design addresses the

906 security characteristics that it was intended to support. The Cybersecurity Framework subcategories

907 were used to provide structure to the security assessment. The cited sections provide validation points

908 that the example solution would be expected to exhibit. Using the Cybersecurity Framework

909 subcategories as a basis for organizing our analysis allowed us to systematically consider how well the

910 reference design supports the intended security characteristics.

911 6.4 Analysis of the Reference Design's Support for Cybersecurity

912 Framework Subcategories

913 [Table 6-1](#) lists reference design capabilities, their functions, and the addressed subcategories, along with

914 the products that we used to instantiate each capability in the example implementation. The focus of

915 the security evaluation is not on these specific products, but on the Cybersecurity Framework

916 subcategories, because, in theory, any number of commercially available products could be substituted

917 to provide the Cybersecurity Framework support represented by a given reference design capability.

918 The "Cybersecurity Framework Subcategories" column of [Table 6-1](#) lists the Cybersecurity Framework

919 subcategories that each capability of the reference design supports. The references provide solution

920 validation, listing specific security functions and controls that a solution supporting the desired

921 Cybersecurity Framework would include. Using the Cybersecurity Framework subcategories as a basis

922 for organizing our analysis allowed us to systematically consider how well the reference design supports

923 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.	<p>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.</p> <p>ID.GV-1: Organizational information security policy is established.</p> <p>ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.</p> <p>ID.GV-4: Governance and risk management processes address cybersecurity risks.</p> <p>PR.AC-1: Identities and credentials are managed for authorized devices and users.</p> <p>PR.AC-4: Access permissions are managed, incorporating</p>

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
	Remiant 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 Remiant 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.

927

928 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
929 capabilities that are not listed in this table.
930

931 [6.4.1 Supported Cybersecurity Framework Subcategories](#)

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

946 [6.4.1.1 ID.AM-3: Organizational Communication and Data Flows Are Mapped](#)

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

956 ***6.4.1.2 ID.AM-6: Cybersecurity Roles and Responsibilities for the Entire Workforce and Third-***
957 ***Party Stakeholders Are Established***

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

966 ***6.4.1.3 ID.BE-5: Resilience Requirements to Support Delivery of Critical Services Are***
967 ***Established***

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

975 ***6.4.1.4 ID.GV-1: Organizational Cybersecurity Policy Is Established and Communicated***

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

981 ***6.4.1.5 ID.GV-2: Cybersecurity Roles and Responsibilities Are Coordinated and Aligned with***
982 ***Internal Roles and External Partners***

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

994 ***6.4.1.6 ID.GV-4: Governance and Risk Management Processes Address Cybersecurity***
995 ***Risks***

996 Senior management is responsible for the organization's risk assessment processes. An organization's
997 risk management program should include strategies that ensure that risks are identified, registered, and
998 mitigated. The reference design is based on a risk assessment in [Section 3.4](#). The reference design
999 capabilities support the risk analysis, risk response/mitigation, and risk monitoring process that address
1000 the cyber risk factors that privileged accounts represent.

1001 ***6.4.1.7 PR.AC-1: Identities and Credentials Are Issued, Managed, Verified, Revoked, and***
1002 ***Audited for Authorized Devices, Users, and Processes***

1003 Organizations establish privileged-account access control policies to ensure that privileged account use
1004 is limited to authorized personnel, least privilege is implemented, and separation of duties is
1005 maintained. Access control policies determine the authentication method and authorization processes,
1006 roles, and responsibilities of the users. The privileged identity store capability deployed within the
1007 reference design provides a unique repository for privileged users' identities and credentials. This is
1008 fundamental to the reference design to segregate the privileged-user community and account
1009 information from the production components of the organization. This Cybersecurity Framework
1010 element primarily considers the implementation of privileged access controls via the account sharing
1011 technique.

1012 ***6.4.1.8 PR.AC-4: Access Permissions and Authorizations Are Managed, Incorporating the***
1013 ***Principles of Least Privilege and Separation of Duties***

1014 A key strength of the reference design is the ability to enforce policies for privileged accounts, including
1015 the principles of least privilege and separation of duties. By enforcing these principles, the reference
1016 design allows limiting unauthorized access to data and systems.

1017 The policy management capability is the repository for approved-use policies for use by the session
1018 management and user interface capabilities. The session management capability enforces the access
1019 policies. The session management and password capabilities ensure the control of privileged sessions
1020 and of usage of the password vault, through request and approval workflows and (optionally) time-
1021 bound access. Automated account discovery is an important consideration as well, as that functionality
1022 will detect any attempts to bypass or ignore the principles of least privilege and separation of duties. All
1023 privileged user activities in the reference design are logged and sent to the monitoring component for
1024 further analysis. Policy administrators and managers are responsible for setting up, making changes to,
1025 and managing, all privileged accounts and functions. This Cybersecurity Framework element primarily
1026 considers the implementation of privileged access controls via the account escalation technique.

1027 ***6.4.1.9 PR.AC-5: Network Integrity Is Protected (e.g., Network Segregation, Network***
1028 ***Segmentation)***

1029 Network segmentation is a key function of this reference design. Segregating the PAM system from the
1030 production network reduces the risk of session information interception and exposure of privileged
1031 account information to nonprivileged users and systems, and reduces the risk of being negatively
1032 impacted from malware or an exploit. The PAM system was implemented on a management network to
1033 accomplish the network segmentation. Using firewalls and routers to segregate the zones also limits the
1034 risk to the enterprise, should a vulnerability be exploited within the production network.

1035 ***6.4.1.10 PR.DS-1: Data at Rest Is Protected***

1036 Privileged user account information is not encrypted while stored at rest. However, this data is limited
1037 to the privileged user identity store within the reference design and is situated in its own security
1038 enclave or subnetwork. The security enclave consists of the physical directory only, without any other
1039 reference design components, and is separated from the rest of the reference design by a firewall.

1040 Furthermore, although this information is not encrypted while at rest, its integrity is monitored by the
1041 security monitoring capability. The security monitoring capability receives logs of privileged account
1042 information changes from the privileged user identity store and from the underlying enterprise-wide
1043 identity store and PAM activity log. The monitoring capability correlates and compares the log
1044 information that it receives from each of the components, to ensure that the information is consistent
1045 across all sources. In this way, it is possible to verify that each change made to the privileged identity
1046 store and/or enterprise-wide identity store is the result of an authorized change by an authorized

1047 privileged user or system. If a change to an identity store is detected and cannot be correlated with logs
1048 from other components, then the system generates an alert to signal that this change might be
1049 unauthorized. File integrity tools are available to monitor for the loss of event integrity within systems
1050 like an identity store. These tools are not addressed in the reference design.

1051 *6.4.1.11 PR.DS-2: Data in Transit Is Protected*

1052 Privileged user access information is encrypted while it is in transit within the reference design
1053 components, where possible. In the example implementation, multiple applications are used to
1054 implement the policy management and user interface (access control) components over secure
1055 protocols (e.g., Transport Layer Security [TLS]) so that all information that flows between the
1056 components is not transmitted over a network where it would be vulnerable to eavesdropping or
1057 tampering. If the reference design were built using separate physical components to instantiate the
1058 policy management and user interface components, then messages exchanged among these
1059 components would need to be provided with at least data integrity, and preferably confidentiality,
1060 protections.

1061 In the current example implementation (Request for Comments 2830), LDAP over SSL [Secure Sockets
1062 Layer] (LDAPS) is used to perform read-and-write access to the identity store component, ensuring that
1063 privileged user account information sent across a network to these other components is encrypted.
1064 Also, when log information is sent to the monitoring component, it is encrypted, resulting in protection
1065 from disclosure and from unauthorized modification.

1066 *6.4.1.12 PR.DS-5: Protections Against Data Leaks Are Implemented*

1067 The reference design itself, through its focus on managing access permissions, protects the enterprise in
1068 general against data leaks that might occur. By preventing unauthorized access to information, the
1069 reference design protects against leaks of that information. The reference design, however, is not
1070 intended to protect against the exfiltration of information by an authorized user; such an insider threat
1071 is not addressed. The fact that data flows within the reference design are encrypted serves to ensure
1072 that, even if data-in-transit within the reference design was exfiltrated, this information would not be in
1073 plaintext form. For example, administrators may have access to administration and configuration
1074 directories, but not to directories that contain sensitive data files. The reference design allows logging all
1075 privileged user access, ensuring that, if a privileged user misuses their privileges and leaks data, this
1076 activity would be recorded in log files and would generate alerts.

1077 Within the reference design, a management network is implemented to segment network access and
1078 can increase the effort needed to exfiltrate data. Automated account discovery is an important
1079 consideration as well, as that functionality will detect any attempts to bypass these other protections in
1080 an attempt to leak data by using privileged access.

1081 *6.4.1.13 PR.PT-1: Audit/Log Records Are Determined, Documented, Implemented, and*
1082 *Reviewed in Accordance with Policy*

1083 The reference design ensures the real-time monitoring of privileged sessions and optionally can record
1084 every session for a detailed audit trail in accordance with requirements defined by an organization's
1085 policies and compliance requirements. The security monitoring capability ensures that all session activity
1086 and access-related change activity can be centrally logged, tracked, and managed. All relevant
1087 information (e.g., about, what, when, who) at each design component is monitored and logged. The
1088 design leverages automation to collect, protect, and analyze logs; produce log-based reports; and retain
1089 log data to support investigations. Given that access to the logs in the monitoring capability would
1090 enable an adversary to delete or modify logs that document adversarial activity, the ability to delete or
1091 modify such logs should, by policy, require the cooperation of multiple individuals.

1092 *6.4.1.14 PR.PT-3: Access to Systems and Assets Is Controlled, Incorporating the Principle of*
1093 *Least Functionality*

1094 Please refer to [Section 6.4.1.8](#) for an explanation of the how the reference design supports this
1095 Cybersecurity Framework subcategory.

1096 *6.4.1.15 PR.PT-4: Communications and Control Networks Are Protected*

1097 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
1098 reference design supports this Cybersecurity Framework subcategory.

1099 *6.4.1.16 DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods*

1100 The reference design provides comprehensive-log and advanced-threat analytics to detect malicious
1101 activity that is near-real-time, accurate, comprehensive, and scalable. These capabilities include
1102 analyzing logs from the PAM system capabilities and related activities of privileged accounts.
1103 Comprehensive logs and advanced threat analytics allows analysts and administrators to detect and
1104 correlate anomalous events in a timely, structured, and constant way. Unauthorized operation/activity
1105 attempts are detected and analyzed through these capabilities. They also automate the processes
1106 required to understand suspicious privileged-account access or use attempts.

1107 *6.4.1.17 DE.AE-3: Event Data Are Collected and Correlated from Multiple Sources and Sensors*

1108 The security monitoring capability provides real-time monitoring and aggregates and correlates
1109 privileged-account or privileged-user logs from the following sources:

- 1110 ▪ user interface (access control)
- 1111 ▪ password vault
- 1112 ▪ identity store (LDAP)

- 1113 ■ automated account discovery
1114 ■ emergency access
1115 ■ session management

1116 ***6.4.1.18 DE.AE-5: Incident Alert Thresholds Are Established***

1117 The alert thresholds are binary. If the user-access information logs that the security monitoring
1118 capability receives from each of its sources are not consistent with each other, then an alert is
1119 generated. If the user-access information logs received from the various components are consistent
1120 with one another, then no alert will be generated, but the information will be logged. The reference
1121 design provides capabilities to define thresholds and to log and audit user access information within
1122 each directory that is consistent with established policies. All incidents and events in the reference
1123 design are clearly communicated. Policy managers define and categorize the incident reporting process
1124 (e.g., a user logging into an account, a web server receiving a request for a specific web page, a user
1125 accessing files on network share, a firewall blocking a connection attempt). For additional information,
1126 please refer to NIST SP 800-61, *Computer Security Incident Handling Guide* [\[15\]](#).

1127 In addition, the monitoring capability of the reference design ensures that logs received from any
1128 privileged operation are consistent with each other. If any inconsistencies in the logs are detected,
1129 then an alert is generated based on the threshold defined by policy managers. This analysis may help
1130 identify unauthorized access attempts and can be supplemented to detect some Kerberos-based
1131 attacks.

1132 ***6.4.1.19 DE.CM-3: Personnel Activity Is Monitored to Detect Potential Cybersecurity Events***

1133 All activity associated with privileged accounts in the reference design is monitored on a continuous
1134 basis. This includes all activity that administrators, policy administrators, and other privileged users
1135 perform. It also includes alerts when an anomalous activity of an individual is detected. User-interface
1136 and session monitoring allow configuring and recording proxy-level sessions. The logs are forwarded to
1137 the monitoring components. For example, a malicious insider or malware attempting (successful or not)
1138 to access an asset outside defined policies can be detected. Additionally, these capabilities can create an
1139 unalterable audit trail of privileged account activity; improve incident response times; and provide a rich
1140 data set from which to understand how, when, and why a security incident occurred.

1141 *6.4.1.20 DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and*
1142 *Software Is Performed*

1143 The reference design continuously monitors all unauthorized activity and access to restricted resources
1144 and generates alerts when a potential incident or event is detected. The user interface (access control)
1145 and configuration components also allow configuring and recording proxy-level sessions. This ensures
1146 the tracking and detection of suspicious activities of individuals associated with a privileged account or
1147 system (including the secret mounting of unauthorized drives or devices). The logs are forwarded to the
1148 monitoring components (SIEM) for proper notification. Automated account discovery is an important
1149 consideration as well, as that functionality will detect any attempts to disable protections against
1150 unauthorized access.

1151 *6.4.1.21 RS.CO-2: Incidents Are Reported Consistent with Established Criteria*

1152 The reference design provides the ability to collect logs from multiple sources. Any security incidents
1153 associated with unauthorized account activity that are consistent with established policies will be
1154 detected and reported (see [Section 6.4.1.22](#) for more details). It is important to develop a structured
1155 incident response program by implementing incident response strategies that can detect and resolve
1156 security incidents. An effective incident response program should include the following stages:

- 1157 ▪ incident response process
- 1158 ▪ incident investigation life cycle
- 1159 ▪ incident remediation
- 1160 ▪ incident response

1161 *6.4.1.22 RS.AN-3: Forensics Are Performed*

1162 The reference design incorporates monitoring capabilities for complete visibility and control and
1163 consolidates identity across all privileged systems, which improves reporting and reduces the audit time
1164 as well as forensics investigations. This allows all privileged sessions and privileged user activities to be
1165 recorded. The recording provides details on the user and their activities. This creates accountability to
1166 support forensic investigations, troubleshoot system failures, and audit reports. For additional
1167 information, please refer to NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident*
1168 *Response* [\[16\]](#).

1169

6.5 Security of the Reference Design

1170 The purpose of the security characteristic analysis is to understand the extent to which the use case
1171 meets its objective of demonstrating PAM. In addition, the analysis seeks to understand the security
1172 benefits and drawbacks of the reference design. The list of reference design capabilities in [Table 3-1](#)

1173 focuses on the capabilities needed to ensure the integrity of system data and to manage and secure the
1174 reference design. To this end, this section focuses on the security of the reference design itself.

1175 The following measures were implemented to protect the reference design from outside attack:

- 1176 ▪ installed an MFA system to provide an additional layer of security
- 1177 ▪ installed session management capabilities to track and manage all privileged user sessions,
1178 integrated with the password manager
- 1179 ▪ installed policy management
- 1180 ▪ installed a management network to isolate log and PAM-system traffic from the production
1181 (business operations) networks
- 1182 ▪ limited the use of, and access to, privileged accounts
- 1183 ▪ monitored identity stores to detect unapproved insertion, modification, or deletion
- 1184 ▪ monitored individual endpoints to detect unapproved privileged access allocation
- 1185 ▪ recorded and logged all privileged-account use and access activities
- 1186 ▪ used encryption and integrity protection of identity-store-access and system logs while this
1187 information was in transit

1188 The security evaluation focuses on the capabilities, rather than the products. The NCCoE is not assessing
1189 or certifying the security of the products included in the example implementations. We assume that an
1190 organization already deploys network security, such as firewalls and intrusion detection devices, that are
1191 configured using best practices. The focus of this section is securing capabilities introduced by the
1192 reference design and minimizing their exposure to threats. The list in [Table 3-2](#) also includes capabilities
1193 for managing and securing the PAM reference design.

1194 [6.5.1 Securing New Attack Surfaces](#)

1195 The reference design introduces new capabilities into an organization, and with any new capability
1196 comes the potential for new attack surfaces. Hence, it is imperative that reference design capabilities
1197 and their contents be secured to minimize their potential to introduce new vulnerabilities into the
1198 enterprise. The threat landscape is dynamic. Therefore, maintaining the security of the reference design
1199 requires establishing and maintaining privileged account control and control of security events from
1200 multiple sources, while being responsive to perceived threats and malicious activities. However, if an
1201 organization deploys the reference design, then the organization will also have additional capabilities
1202 that must be safeguarded—namely, the policy management, user interface (access control), session
1203 management, password vault, monitoring, and emergency access. Each capability must be protected
1204 from unauthorized access so that the information that they contain is safeguarded from unauthorized
1205 modification. One method that assists with this protection is automated account discovery, as that
1206 function detects attempts to bypass or otherwise defeat existing information security protections.

1207 **Points of entry.** The user interface provides the primary point of entry for a PAM system. Therefore, the
1208 protection of the user interface and authentication method for PAM users is critically important. The
1209 reference design addresses the user authentication by implementing MFA to reduce the chance of a
1210 successful impersonation of an authorized PAM user. The user interface system must be protected
1211 within the organization by limiting access to the underlying support systems (e.g., OS, physical
1212 hardware). A successful attack on the user interface system could allow an attacker to compromise any
1213 of the PAM system capabilities. For example, if an adversary could compromise the policy management,
1214 password vault, or user interface (access control) capabilities, then the attacker would be able to access
1215 the PAM system for unauthorized use. Inappropriate or unauthorized use of these capabilities could
1216 change the authorization levels for anyone in the enterprise.

1217 **Disabling monitoring.** Continuous monitoring is critical to detect anomalous system changes or
1218 activities. The monitoring capability must be protected from physical and logical access. Example
1219 Implementation 3 provides an example of logical access control for the monitoring capability. Further,
1220 automated account discovery is an important consideration to protect the fidelity of the monitoring and
1221 to ensure that no attempts to bypass, redirect, or disable the continuous monitoring facility have been
1222 made.

1223 **Sabotaging detection.** Unauthorized access to the PAM user interface, password vault, and security
1224 monitoring capabilities must be prevented because of the value of the information that they maintain
1225 and store. The monitoring capability forms the locus of the reference design's analytic capabilities for
1226 detecting access control security events. The aggregation of privileged-account information and logs in
1227 the monitoring capability provides enormous potential in terms of anomaly detection. If an adversary
1228 could access the password vault and the monitoring capabilities to modify or delete information or to
1229 alter the rules used to analyze information, then the ability to monitor and detect access control
1230 anomalies could be severely impaired. The example solution illustrates one of the techniques for
1231 protecting the PAM and security monitoring capability through a network segmentation technique. With
1232 network segmentation, attackers are required to identify the management network, and to cross over
1233 the network boundaries undetected, before unauthorized access to the PAM system and security
1234 monitoring capabilities can be achieved. Network segmentation is an important defense-in-depth tactic.

1235 **Safeguarding the enterprise.** The following sections discuss mechanisms that are used to secure these
1236 reference design capabilities and to safeguard user access and policy information. In all cases, restricting
1237 logical and physical access to these capabilities is key to protecting them. Standard users are never given
1238 accounts on, or given authorization to access, any reference design capabilities. Each reference design
1239 capability should permit access by only one or two privileged users who have the authority and
1240 responsibility to administer that (and only that) reference design capability, or, by policy, the
1241 cooperation of multiple individuals should be required to access any single reference design capability,
1242 thereby decreasing the probability that any capability could be subverted by a single inside adversary.
1243 No administrative users should reuse the same workstation or administrative activities account that
1244 they use for other business use, such as email, word processing, or other business applications.

1245 Furthermore, access to the consoles/management interfaces of the machines and applications on which
1246 the reference design capabilities reside must be protected. The PAM implementation can be used to
1247 administer portions of the implementation, or another PAM system might be considered to administer
1248 the primary PAM system, based on the needs and risk management decisions of the organization. Any
1249 passwords needed for PAM system administration should be stored separately in a manner consistent
1250 with the organization's risk management decisions. This helps ensure that all access to any reference
1251 design capability must be performed via the PAM (rather than directly via the machine console) or in
1252 another secure manner.

1253 **6.5.2 Securing Access to the LDAP Directory**

1254 The identity store (LDAP) is the authoritative source for privileged account information. The security of
1255 the identity store can be maximized by ensuring that direct connection to consoles of the machines on
1256 which these capabilities reside is physically secured and that console passwords are secure according to
1257 organization risk management decisions. This approach will minimize the possibility that any reference
1258 design machine could be accessed directly, rather than via the PAM. In addition, the reference design
1259 implements the MFA capability to ensure that all privileged access requests can be authenticated using a
1260 strong method.

1261 **6.5.3 Securing Access to the Policy Management Capability**

1262 The ability to create and modify privileged account policies within the policy management capability
1263 must also be carefully controlled. By policy, workflows should be established to ensure that no single
1264 administrator can create or modify policies in isolation. Workflows based on the principles of least
1265 privilege and separation of duties should be defined to ensure that multiple administrators and/or
1266 multiple administrative approvals are received before updates are performed. It should not be possible
1267 to submit policies that have not been properly vetted and approved by using an approved workflow.

1268 **6.5.4 Securing Access to the User Interface (Access Control) Capability**

1269 The user interface capability provides login authentication and an interactive interface through which
1270 users interact to establish work sessions for each target system that they administer or access to
1271 perform their privileged functions. This establishes the single entry point into the reference design. The
1272 reference design should not accept direct input from any source other than the user interface (or an
1273 associated and equally well-authenticated application programming interface [API]). The identity store
1274 and MFA capabilities provide additional layers of security to ensure the use of a strong authentication
1275 method.

1276 **6.5.5 Securing Password Vault Capability**

1277 The password vault capability of the reference design stores and manages all passwords for every
1278 privileged user, according to the account sharing technique. Because the vault stores sensitive data, it
1279 becomes a target for attackers. Therefore, it is critical to protect the password vault from unauthorized
1280 access. Access to the password vault should require two-person control to increase the resistance to a
1281 single malicious actor acting independently. MFA should also be incorporated to further increase the
1282 resistance to an attack that is performed via the impersonation of an authorized user.

1283 **6.5.6 Securing Emergency Access Capability**

1284 The emergency access capability provides additional privileged account access to the PAM components
1285 when normal access control to the password vault is broken down or when outages and failure happen
1286 in the enterprise infrastructure. This may be the only access point to restore the PAM system to normal
1287 operation or to use the PAM system when the unanticipated or unauthorized personnel require access
1288 to privileged accounts. For example, if privileged users are locked out of the password vault, then the
1289 senior administrator can log into the password vault and get the credentials for the privileged users in all
1290 cases, even if (for example) the LDAP infrastructure is down and no one can log into the PAM system in
1291 the usual manner. Policy administrators and managers may write down and store the emergency access
1292 passwords in a physical vault. In such cases, the physical vault is placed in a secure location with limited
1293 access.

1294 **6.5.7 Securing Access to the Security Monitoring and Analytics Capability**

1295 The security monitoring capability, which provides complete management and visibility within the
1296 reference design, collects and tracks all privileged user activity in real time. Therefore, if an adversary
1297 could modify the contents of the monitoring capability without detection, then that would negatively
1298 impact the ability of the reference design to monitor all privileged account changes. By policy, only
1299 security analysts, whose role is to be notified of alerts and to examine the logs pertinent to those alerts
1300 to determine if there is a genuine security event, should be able to view logs, and the logs should be
1301 accessible only via read-only access. Workflows based on the principles of least privilege and separation
1302 of duties should be defined to ensure that multiple administrators and/or multiple administrative
1303 approvals are received before any changes to the monitoring analytics are performed. It should not be
1304 possible to create or modify analytics that have not been properly vetted and approved. Example
1305 Implementation 3 illustrates one approach to secure a security monitoring capability.

1306 **6.5.8 Ensuring Information Integrity**

1307 Within the reference design, multiple capabilities have been implemented to prevent unauthorized
1308 modification or deletion of access policies, privileged account information, and analytics information
1309 stored in these capabilities. In addition to preventing access to information while it is stored in these

1310 capabilities, the information must be protected from modification while it is in transit between
1311 reference design capabilities. If privileged accounts or policy information were to be deleted, modified,
1312 or falsified while in transit between capabilities, then the result would be a loss of confidence in the
1313 access authorization and authentication of users. It is essential that the user-access and policy
1314 information have integrity protection, and ideally confidentiality protection, when in transit between
1315 capabilities. Securing communications among all capabilities is essential to securing the reference
1316 design. To provide this protection, all information sent to and from LDAP is encrypted using the TLS
1317 protocol.

1318 All logs sent within the reference design are encrypted in transit to ensure confidentiality and integrity
1319 from the reference design capability to the monitoring capability. Once the log file is transmitted to the
1320 monitoring capability, it is stored in the clear (i.e., in plaintext form), where it would be vulnerable to
1321 modification or deletion if an adversary were able to gain unauthorized access to the monitoring
1322 capability.

1323 **6.5.9 Protecting Privileged Accounts**

1324 In any organization that adopts the reference design, we would expect there to be several classes of
1325 privileged users who are authorized to access reference design capabilities or the machines on which
1326 they are running, for administering those capabilities and machines. It is important to limit privileged
1327 users and accounts by enforcing the principle of least-privilege access controls. The reference design
1328 implements the automatic account discovery capability, which ensures the detection of all privileged
1329 account changes within the privileged identity store and of the assets administered or otherwise
1330 accessed by using privileged accounts.

1331 **6.5.10 Preventing Insider Threats**

1332 Insider threats are difficult to detect. The attacks perpetuated by insiders, and the consequences
1333 resulting from such attacks, can be very costly. The reference design supports the principles of least
1334 privilege and separation of duties. These principles restrict privileged users to only those resources to
1335 which their role gives them access, and limit privileged users in what they are authorized to do with
1336 those resources. The implementation of these policies does not prevent inside attacks; however, it can
1337 reduce the scope of the damage that an insider can cause. The privileged account identity store and
1338 MFA capabilities in the reference design prevent an unauthorized user from using privileged accounts.
1339 These measures ensure that the reference design itself is secure from any nonprivileged user insider
1340 threat. Any organization adopting the reference design should ensure the integration of these protective
1341 mechanisms and other solutions that it may see fit in its implementation against insider threats.

1342

6.5.11 Addressing Attacks

1343 The specific challenge of the reference design is the abuse of privileged account credentials. Once these
1344 accounts are compromised, an adversary can create additional accounts to avoid detection, escalate
1345 their privileges, and disrupt critical services. To address these and other related challenges in a
1346 comprehensive way, we used the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
1347 model and framework developed by The MITRE Corporation, to identify the following adversary tactics
1348 and techniques against which the reference design protects:

- 1349 ▪ Privilege escalation and credential access result when an adversary obtains or modifies a higher
1350 level of permissions on a system or network than they are authorized to have.
 - 1351 • An adversary employing the tactic of privilege escalation might use the technique to modify
1352 their privilege information attributes that are stored in LDAP, so that these attributes
1353 permit the adversary to have more access authority than entitled. In this attack technique,
1354 the adversary tries to circumvent the principle of least privilege. The reference design
1355 protects against circumventing the principle of least privilege, through MFA, password
1356 managers, session management, automated account discovery, logging, and security
1357 monitoring, which enables it to detect changes in privileged account information that is
1358 stored in LDAP.
 - 1359 • Alternatively, an adversary attempting to abuse privileges could use the technique of
1360 creating a secret account in one of the enterprise's directories and giving that new account
1361 the desired higher level of privilege for malicious purposes. This means that the adversary
1362 is not using the PAM user interface. The monitoring and logging system is designed to
1363 detect and generate an alert when an unauthorized new account is created.
 - 1364 • Similarly, an adversary could create a local account (outside the scope of the enterprise
1365 directory) and grant it privileged access. The unauthorized new account will be detected
1366 only if the automated account discovery capability has been deployed and includes in its
1367 scan scope such local accounts.
 - 1368 • Credential access results when an adversary obtains unauthorized privileged access to
1369 enterprise resources or when an adversary modifies credential information in unapproved
1370 ways. An adversary employing the tactic of privileged credential access abuse could use the
1371 technique of trying to obtain legitimate privileged user credentials that belong to another
1372 user by eavesdropping on these credentials as they are sent to and from directories in the
1373 network. The reference design protects against such privileged credential access abuse
1374 through its use of LDAPS (SSL-based encrypted traffic between LDAP servers and clients)
1375 and MFA, which prevents the network sniffing of another privileged user's credentials.
1376 Further, use of the account escalation (rather than account sharing) design pattern can
1377 mitigate the risk of credential access by minimizing the value of stolen credentials.

1378 [6.5.12 User Behavior Analytics](#)

1379 UBA tracks a system's user and their interactions with the system, rather than security events or
1380 devices. UBA solutions detect behaviors of concern by combining all relevant data (e.g., network and
1381 client/host-based activity, human resource systems, employee reports, public records, travel records)
1382 and then looking for meaningful patterns of behavior. UBA offers the potential for organizations to
1383 improve their security posture by detecting that an attack—such as a privilege escalation attack—has
1384 been launched or is to be imminently launched, allowing the organization to take preventive, corrective,
1385 and investigative action as appropriate. Detection ideally occurs during the early formative stages of an
1386 attack or before the technical implementation of an attack has been launched, but can also extend until
1387 after the primary phase of an attack has been launched.

1388 Various analytic approaches exist that UBA solutions can leverage to detect privilege escalation attacks,
1389 including static event and threshold analysis, whereby specific patterns of network and client activity are
1390 deemed to signify behaviors of concern. Other approaches include anomaly detection that identifies an
1391 attack based on deviations from a baseline at the organizational, job-role, or individual-employee level.
1392 These baselines can be generated with or without machine learning algorithms, though the level of
1393 computational power required increases with system complexity.

1394 For this build, a UBA capability was not implemented. The low volume of user, client, and network data
1395 transmitted across the example implementations would have been insufficient for a UBA capability to
1396 meaningfully identify patterns or develop a baseline. Furthermore, the selection of a UBA should be
1397 tailored to the business operations and technical infrastructure of an organization. Our test build did not
1398 have the wider set of system operations and connectivity to adequately simulate a financial institution.

1399 Nonetheless, there are some UBA considerations that will be consistent across financial institutions that
1400 wish to select a UBA capability as part of the defense against privilege escalation attacks and other
1401 forms of cyber attacks. Organizations should consider the following issues when contemplating adding
1402 UBA to their security architecture:

- 1403 ▪ Can the UBA detect or enable other types of attacks? Privilege escalation attacks are only one
1404 attack of many that financial organizations face. Organizations may consider UBA for the
1405 detection of alternative avenues of attack or for obscuring alternative types of attack from
1406 detection.
- 1407 ▪ Organizations should consider how UBA can most effectively and efficiently add to the
1408 situational awareness that a privilege escalation attack (or any attack) is underway. Good
1409 situational awareness can involve a combination of notifications, visualizations, administration
1410 and automated system actions, and business processes that are regularly drilled, trained,
1411 evaluated, and based on best practices from the fields of behavioral sciences and human
1412 factors. Failure to act quickly—whether through prevention, mitigation, or investigation—can
1413 generate significant reputational, financial, productivity, legal, and cultural risks that UBA
1414 solutions would be unable to remedy.

1415 6.6 Deployment Recommendations

1416 When deploying the reference design in an operational environment, organizations should follow
1417 security best practices to address potential vulnerabilities and to ensure that all assumptions upon
1418 which the solution relies are valid, to minimize any risk to the production network. Organizations
1419 leveraging the reference design should adhere to the recommended best practices that are designed to
1420 reduce risk (see the subsections below). Please note that the example implementations of the reference
1421 design did not implement every security recommendation. Organizations should not consider this list of
1422 recommended best practices to be comprehensive; merely following this list will not guarantee a secure
1423 environment. Planning for the deployment of the design gives an organization the opportunity to go
1424 back and audit the privileged account information in their directories and get a more global, correlated,
1425 disambiguated view of the user access roles and attributes.

1426 6.6.1 Patch, Harden, Scan, and Test

1427 Vulnerability assessment programs establish controls and processes to help identify weaknesses within
1428 the organization's information system components, which could be exploited by attackers to gain
1429 unauthorized access, to disrupt business operations, and to steal or leak sensitive data. The vulnerability
1430 assessment focuses on identifying controls and processes that will provide appropriate protection
1431 against threats that could adversely affect the security of the information system or data entrusted on
1432 the information system. The controls implemented need to be consistent with established policy
1433 requirements to secure against known vulnerabilities in OSs and application software. The following
1434 activities provide additional steps to the IT infrastructure:

- 1435 ■ Keep OSs up-to-date by patching, version control, and monitoring indicators of compromise
1436 (e.g., performing virus and malware detection, keeping antivirus signatures up-to-date).
- 1437 ■ Harden all capabilities by deploying on securely configured OSs that use long and complex
1438 passwords and are configured per best practices. Built-in accounts with privileged access rights
1439 should be disabled or closely monitored.
- 1440 ■ Scan OSs for vulnerabilities and unexpected changes in privileged access.
- 1441 ■ Test individual capabilities to ensure that they provide the expected Cybersecurity Framework
1442 subcategory support and that they do not introduce unintended vulnerabilities.
- 1443 ■ Evaluate reference design implementations before going operational with them.

1444 It is also recommended that additional network security strategies are implemented that utilize secure
1445 protocols and processes. However unlikely a targeted attack is for the reference design, the most potent
1446 area of risk remains from within the network itself. Pushing audit log capabilities beyond system log
1447 (syslog) and auditing services into a security monitoring platform increases the likelihood that exploited
1448 trust relationships would be detected quickly. Such deployments would support a defense-in-depth
1449 strategy and assist in transitioning the reference design toward a more resilient state. Specifically, check

1450 external accounting logs, external syslog logs, booting information (periodically) for information about
1451 the last time that the firewall was reloaded, and the configuration checksum (on a regular basis), and
1452 periodically verify the integrity of other software loaded on the firewall.

1453 6.6.2 Other Security Best Practices

- 1454 ■ Install, configure, and use each capability of the reference design per the security guidance
1455 provided by the capability vendor.
- 1456 ■ Change the default password when installing software.
- 1457 ■ Identify and understand which predefined administrative and other accounts each capability
1458 comes with by default, to eliminate any inadvertent backdoors into these capabilities. Disable all
1459 unnecessary predefined accounts, and, even though they are disabled, change the default
1460 passwords in case a future patch enables these accounts.
- 1461 ■ Segregate reference design capabilities on their own subnetwork, separate from the production
1462 network, either physically or by using virtual private networks and port-based authentication or
1463 similar mechanisms.
- 1464 ■ Protect the various reference design subnetworks from each other and from the production
1465 network by using security capabilities, such as firewalls and intrusion detection devices, that are
1466 configured per best practices.
- 1467 ■ Configure firewalls to limit connections between the reference design network and the
1468 production network, except for the connections needed to support required internetwork
1469 communications to specific internet protocol (IP) address and port combinations in certain
1470 directions.
- 1471 ■ Configure and verify firewall configurations to ensure that data transmission to and from
1472 reference design capabilities is limited to interactions that are needed. Restrict all permitted
1473 communications to specific protocols and IP address and port combinations in specific
1474 directions.
- 1475 ■ Monitor the firewalls that separate the various reference design subnetworks from each
1476 another.
- 1477 ■ Volume C, *How-To Guides*, contains the firewall configurations that show the rules implemented
1478 in each of the firewalls for an example implementation. These configurations are provided to
1479 enable the reader to reproduce the traffic filtering/blocking that was achieved in the
1480 implementation.
- 1481 ■ Apply encryption or integrity-checking mechanisms to all information exchanged between
1482 reference design capabilities (i.e., to all user access, policy, and log information exchanged), so
1483 that tampering can be detected. Use only encryption and integrity mechanisms that conform to
1484 the most-recent industry best practices. Note that, in the case of directory reads and writes, the
1485 protected mode is defined as the use of Lightweight Directory Access.

- 1486 ▪ Strictly control physical access to all assets.
- 1487 ▪ Deploy a configuration management system to serve as a “monitor of monitors” to ensure that
1488 any changes made to the list of information are logged and reported to the monitoring system
1489 or to the analytics in the monitoring system, and that notifications are generated. Such a system
1490 could also monitor whether reference design monitoring capabilities, such as log integrity
1491 capabilities or the monitoring system itself, go offline or stop functioning, and could generate
1492 alerts when these capabilities become unresponsive.
- 1493 ▪ Deploy a system that audits and analyzes directory content to create a description of who has
1494 access to what resources, and to validate that these access permissions correctly implement the
1495 enterprise’s intended business process and access policies.

1496 6.6.3 Deployment Phases

1497 The key to effective PAM solution implementation is to develop and adopt a comprehensive
1498 deployment plan to align security components in the existing infrastructure with and around the PAM
1499 efforts. It is recommended that a phased approach be developed to deploy the PAM solution and that
1500 ensures that short-term and long-term goals can be addressed. It is usually a good practice to develop a
1501 maintenance structure that can address additional and future implementations as well as operational
1502 and security requirements. The following key activities should be considered when adopting the
1503 reference design:

- 1504 ▪ Phase 0: Define the business and technical objectives for the PAM deployment.
- 1505 ▪ Phase I: initial setup and infrastructure preparation to ensure that all of the resources needed to
1506 deploy, operate, and maintain the PAM solution are available. This includes identifying and
1507 documenting privileged users, accounts, critical assets, etc. to management, as well as their
1508 functions. The results of automated account discovery are often useful in this preparation.
- 1509 ▪ Phase II: Deploy the solutions in the reference design to a test set of systems, and tune the
1510 configuration for the desired performance and feature functionality to ensure that appropriate
1511 security events can be identified and logged, that privileged account information and functions
1512 are clearly defined, etc. Measure achievement against the objectives defined in Phase 0; make
1513 rollout or objective changes as needed.
- 1514 ▪ Phase III: broad deployment with use-cases-based testing. It is a good practice to test the
1515 adopted solution and test, based on use cases. Measure achievement against the objectives
1516 defined in Phase 0.
- 1517 ▪ Phase IV: Evaluate the performance of the reference design, and perform a risk assessment to
1518 assess performance and to identify any weaknesses that can compromise the overall security
1519 objectives, based on the identified needs and the defined use case. Measure achievement
1520 against the objectives defined in Phase 0.
- 1521 ▪ Phase V: Manage logs and ensure continuous monitoring. Log management and ongoing events
1522 tuning can be complicated by a large volume of security data. It is important to create processes

1523 and procedures for collecting, storing, and analyzing security logs from multiple sources and to
1524 prioritize security activities. Integrate with other information security tools in the ecosystem in
1525 ways that support the achievement of the objectives defined in Phase 0.

1526 Each of the phases described above should be designed to fit the needs of the organization.

1527 **6.6.4 Policy Recommendations**

- 1528 ▪ Define the access policies to enforce the principles of least privilege and separation of duties.
- 1529 ▪ Configure the monitoring capability with comprehensive analytics to identify anomalous
1530 situations that can signal a cyber event. Define enterprise-level workflows that include business
1531 and security rules, to determine each user's access control authorizations and to ensure that
1532 enterprise access control policy is enforced as completely and accurately as possible.
- 1533 ▪ Develop an attack model to help determine the types of events that should generate alerts.
- 1534 ▪ Ensure that the reference design, when adopted, supports flexible data collection.
- 1535 ▪ Grant only a few users (e.g., human resource administrators) the authority to modify
1536 (e.g., initiate, change, delete) employee access information. Require the approval of more than
1537 one individual to update employee access information. Log all employee access information
1538 modifications. Define workflows to enforce these requirements.
- 1539 ▪ Define applicable doctrine and guidance for feedback processes, monitoring capabilities, and
1540 expected outcome, and develop alternative operational methods to ensure resiliency.

1541 **7 Functional Evaluation**

1542 A functional evaluation of the PAM example implementation, as constructed in our laboratory, was
1543 conducted to verify that it meets its objective of demonstrating the ability to manage and control access
1544 to the myriad privileged accounts across an enterprise. The evaluation verified that the example
1545 implementation could perform the following functions:

- 1546 ▪ enforce privileged-account-access and privileged-account-use policies
- 1547 ▪ protect against unauthorized access to, and/or use of, privileged accounts

1548 [Section 7.1](#) describes the format and components of the functional test cases. Each functional test case
1549 is designed to assess the capability of the example implementation to perform the functions listed
1550 above and is detailed in [Section 7.1.1](#).

1551 **7.1 PAM Functional Test Plan**

1552 One aspect of our security evaluation involved assessing how well the reference design addresses the
1553 security characteristics that it was intended to support. The Cybersecurity Framework subcategories
1554 were used to provide structure to the security assessment by consulting the specific sections of each

1555 standard that are cited in reference to that subcategory. The cited sections provide validation points
 1556 that the example solution is expected to exhibit. Using the Cybersecurity Framework subcategories as a
 1557 basis for organizing our analysis allowed us to systematically consider how well the reference design
 1558 supports the intended security characteristics.

1559 This plan includes the test cases necessary to conduct the functional evaluation of the PAM example
 1560 implementation, which is currently deployed in a lab at the NCCoE. The implementation tested is
 1561 described in [Section 5](#).

1562 Each test case consists of multiple fields that collectively identify the goal of the test, the specifics
 1563 required to implement the test, and how to assess the results of the test. [Table 7-1](#) describes each field
 1564 in the test case.

1565 **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.

1566 **7.1.1 PAM Use Case Requirements**

1567 [Table 7-2](#) identifies the PAM functional evaluation requirements that are addressed in the test plan, and
 1568 the associated test cases.

1569 **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

1570 [**7.1.2 Test Case: PAM-1**](#)

1571 [Table 7-3](#) describes each field in the PAM-1 test case.

1572 [**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	<p>Perform the following procedures on each PAM build instance:</p> <ol style="list-style-type: none"> 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)	<p>Access is denied to System A (CR 1.a).</p> <p>Access is allowed to System B (CR 1.b).</p>
Actual Results	<p>PAM Build 1 results:</p> <ul style="list-style-type: none"> ■ CR 1.a – Access is denied to System A. ■ CR 1.b – Access is allowed to System B. <p>PAM Build 2 results:</p> <ul style="list-style-type: none"> ■ CR 1.a – Access is denied to System A. ■ CR 1.b – Access is allowed to System B. <p>PAM Build 3 results:</p> <ul style="list-style-type: none"> ■ CR 1.a – Access is denied to System A. ■ CR 1.b – Access is allowed to System B.
Overall Result	Pass

1573 **7.1.3 Test Case: PAM-2**1574 [Table 7-4](#) describes each field in the PAM-2 test case.1575 **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 Subcategories	ID.AM-3, ID.GV-4, PR.AC-1, PR.PT-4
Preconditions	The systems are established as configured for CR 1.
Procedure	<p>Perform the following procedures on each PAM build instance:</p> <ol style="list-style-type: none"> 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	<p>PAM Build 1 results:</p> <ul style="list-style-type: none"> ▪ CR 2 – The password used for authentication to System B is used and is not displayed to the PAM user. <p>PAM Build 2 results:</p> <ul style="list-style-type: none"> ▪ CR 2 – The password used for authentication to System B is used and is not displayed to the PAM user. <p>PAM Build 3 results:</p> <ul style="list-style-type: none"> ▪ CR 2 – The password used for authentication to System B is used and is not displayed to the PAM user.
Overall Result	Pass

1576 **7.1.4 Test Case: PAM-3**1577 [Table 7-5](#) describes each field in the PAM-3 test case.1578 **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: <ul style="list-style-type: none">▪ CR 3 – The session replay is successful. The details of the activity during the session are replayed. PAM Build 2 results: <ul style="list-style-type: none">▪ CR 3 – The session replay is successful. The details of the activity during the session are replayed. PAM Build 3 results: <ul style="list-style-type: none">▪ CR 3 – The session replay is successful. The details of the activity during the session are replayed.
Overall Result	Pass

1579 **7.1.5 Test Case: PAM-4**1580 [Table 7-6](#) describes each field in the PAM-4 test case.1581 **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: <ul style="list-style-type: none">▪ 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: <ul style="list-style-type: none">▪ 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: <ul style="list-style-type: none">▪ 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

1582 **7.1.6 Test Case: PAM-5**1583 [Table 7-7](#) describes each field in the PAM-5 test case.1584 **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: <ul style="list-style-type: none">▪ 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: <ul style="list-style-type: none">▪ 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: <ul style="list-style-type: none">▪ 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
----------------	------

1585 **7.1.7 Test Case: PAM-6**

1586 [Table 7-8](#) describes each field in the PAM-6 test case.

1587 **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: <ol style="list-style-type: none"> Access the PAM policy management system. Create a password change policy to change the password after each session. Access the PAM system user interface. Identify a system (B) known to be available (access within policy) to the PAM user. Activate the packet capture for the sessions with System B. Request access to System B. Attempt to perform a common action on System B if access is allowed. Close the session. Request access to System B (second time). 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	<p>PAM Build 1 results:</p> <ul style="list-style-type: none"> ■ 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. <p>PAM Build 2 results:</p> <ul style="list-style-type: none"> ■ 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. <p>PAM Build 3 results:</p> <ul style="list-style-type: none"> ■ 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

1588 [7.1.8 Test Case: PAM-7](#)

1589 [Table 7-9](#) describes each field in the PAM-7 test case.

1590 [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	<p>Perform the following procedures on each PAM build instance:</p> <ol style="list-style-type: none"> 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.

	<p>6. Request an emergency session using an incorrect emergency credential.</p> <p>7. Request access to System B.</p> <p>8. Attempt to perform a common action on System B if access is allowed.</p>
Expected Results (Pass)	<p>Emergency access using the predefined emergency credential results in access to the desired system (B) (CR 7).</p> <p>Emergency access without the predefined emergency credential results in no access allowed (CR 7).</p>
Actual Results	<p>PAM Build 1 results:</p> <ul style="list-style-type: none"> ■ 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. <p>PAM Build 2 results:</p> <ul style="list-style-type: none"> ■ 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. <p>PAM Build 3 results:</p> <ul style="list-style-type: none"> ■ 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

1591 [7.1.9 Test Case: PAM-8](#)

1592 [Table 7-10](#) describes each field in the PAM-8 test case.

1593 [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	<p>Perform the following procedures on each PAM build instance:</p> <ol style="list-style-type: none"> 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	<p>PAM Build 1 results:</p> <ul style="list-style-type: none"> ■ CR 8 – Automated privileged account discovery should identify the newly created account. <p>PAM Build 2 results:</p> <ul style="list-style-type: none"> ■ CR 8 – Automated privileged account discovery should identify the newly created account. <p>PAM Build 3 results:</p> <ul style="list-style-type: none"> ■ 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 Kneis	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
<u>Splunk</u>	Splunk Enterprise
<u>TDi Technologies</u>	ConsoleWorks

1 **Contents**

2	1	Introduction	1
3	1.1	Practice Guide Structure	1
4	1.2	Build Overview	2
5	1.3	Typographic Conventions.....	3
6	2	Product Installation Guides.....	3
7	2.1	Microsoft Active Directory	3
8	2.1.1	How It's Used.....	3
9	2.1.2	Virtual Machine Configuration	3
10	2.1.3	Installation	4
11	2.1.4	DNS Configuration	4
12	2.1.5	Group Policy Object Configuration.....	5
13	2.1.6	Scripts	5
14	2.1.7	Splunk Universal Forwarder	8
15	2.2	Bomgar Privileged Identity.....	8
16	2.2.1	How It's Used.....	8
17	2.2.2	Virtual Machine Configuration	8
18	2.2.3	Prerequisites.....	9
19	2.2.4	Installing Privileged Identity	9
20	2.2.5	Configuration	13
21	2.2.6	Installing Privileged Identity Application Launcher	16
22	2.2.7	Configure Bomgar Privileged Identity with IdRamp SAML Authentication	17
23	2.2.8	Configuring Microsoft SQL Server Access.....	20
24	2.2.9	Configuring Twitter Account Launching	33
25	2.2.10	Configuring Multifactor Authentication with RSA.....	36
26	2.2.11	Splunk Universal Forwarder	40
27	2.3	TDi ConsoleWorks	41
28	2.3.1	How It's Used.....	41
29	2.3.2	Virtual Machine Configuration	41

30	2.3.3	Installation	42
31	2.3.4	Configuration of Back-End Authentication.....	42
32	2.3.5	Creating Users.....	45
33	2.3.6	Creating Tags	47
34	2.3.7	Creating SSH Consoles	47
35	2.3.8	Creating Web Consoles.....	49
36	2.3.9	Assigning Tags to Consoles	50
37	2.3.10	Creating Profiles for Users.....	51
38	2.3.11	Assigning Permissions to Profiles	52
39	2.4	Ekran System	53
40	2.4.1	How It's Used.....	54
41	2.4.2	Virtual Machine Configuration	54
42	2.4.3	Prerequisites.....	54
43	2.4.4	Installing Ekran System.....	54
44	2.5	Radiant Logic	55
45	2.5.1	How It's Used.....	55
46	2.5.2	Virtual Machine	55
47	2.5.3	Prerequisites.....	55
48	2.5.4	Installation	56
49	2.5.5	Configure FID	56
50	2.5.6	Configure Logging.....	58
51	2.5.7	Configure SSL	61
52	2.5.8	Splunk Universal Forwarder	62
53	2.6	IdRamp	63
54	2.6.1	How It's Used.....	63
55	2.6.2	Prerequisites.....	63
56	2.6.3	Installation	63
57	2.7	OneSpan IDENTIKEY Authentication Server	65
58	2.7.1	How It's Used	65
59	2.7.2	Virtual Machine Configuration	65
60	2.7.3	Prerequisites.....	65

61	2.7.4	Installation	66
62	2.7.5	Configuration	66
63	2.7.6	Creating a Domain and Policies	68
64	2.7.7	Importing DIGIPASSes.....	72
65	2.7.8	Configuring to Use Radiant Logic as a Back-End Authentication Server	73
66	2.7.9	Integration with TDi ConsoleWorks	77
67	2.7.10	Installing User Websites	77
68	2.7.11	Creating Component Records in IDENTIKEY Authentication Server	78
69	2.8	Base Linux OS	80
70	2.8.1	Virtual Machine Configuration	80
71	2.8.2	Domain Join Configuration	81
72	2.9	Microsoft SQL Server Installation on Ubuntu Linux	83
73	2.9.1	How It's Used	83
74	2.9.2	Virtual Machine Configuration	83
75	2.9.3	Firewall Configuration	84
76	2.9.4	Installation and Initial Configuration	84
77	2.10	Samba File Server	86
78	2.10.1	How It's Used	86
79	2.10.2	Virtual Machine Configuration	86
80	2.10.3	Firewall Configuration	87
81	2.10.4	Installation and Configuration	87
82	2.11	Remiant SecureONE	89
83	2.11.1	How It's Used	89
84	2.11.2	Virtual Machine Configuration	89
85	2.11.3	Installation and Initial Configuration	90
86	2.11.4	Domain Configuration	90
87	2.11.5	Managing Systems.....	91
88	2.11.6	Adding New Users	92
89	2.11.7	Requesting Privileged Access to Protected System	93
90	2.12	RSA Authentication Manager	95
91	2.12.1	How It's Used	95

92	2.12.2 Installation and Initial Configuration	95
93	2.12.3 LDAP Integration.....	98
94	2.12.4 Token Assignment	99
95	2.12.5 Software Token Profiles and Token Distribution	100
96	2.13 Splunk	101
97	2.13.1 How It's Used.....	101
98	2.13.2 Installation	101
99	2.13.3 Queries.....	101
100	2.13.4 DemoBomgar-AD-Auth-UnauthV1	101
101	2.13.5 DemoRadiant-AD-Event-Details	102
102	2.13.6 SSL Forwarding	102
103	Appendix A List of Acronyms	103

104 1 Introduction

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

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

112 1.1 Practice Guide Structure

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

117 This guide contains three volumes:

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

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

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

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

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

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

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

136 **IT professionals** who want to implement an approach like this will find this whole practice guide useful.
137 You can use this How-To portion of the guide, *NIST SP 1800-18C*, to replicate all or parts of the build
138 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
139 and integration instructions for implementing the example solution. We do not recreate the product
140 manufacturers' documentation, which is generally widely available. Rather, we show how we
141 incorporated the products together in our environment to create an example solution.

142 This guide assumes that IT professionals have experience implementing security products within the
143 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
144 not endorse these particular products. Your organization can adopt this solution or one that adheres to
145 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
146 parts of a PAM system to manage and monitor the use of privileged accounts. Your organization's
147 security experts should identify the products that will best integrate with your existing tools and IT
148 system infrastructure. We hope that you will seek products that are congruent with applicable standards
149 and best practices. Section 3.6, Technologies, of Volume B lists the products that we used and maps
150 them to the cybersecurity controls provided by this reference solution.

151 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
152 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
153 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
154 financial_nccoe@nist.gov.

155 1.2 Build Overview

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

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

166 1.3 Typographic Conventions

167 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
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	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	service sshd start
<u>blue text</u>	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 .

168 2 Product Installation Guides

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

171 2.1 Microsoft Active Directory

172 2.1.1 How It's Used

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

175 2.1.2 Virtual Machine Configuration

176 The Microsoft AD virtual machine is configured as follows:

- 177 ▪ 4 central processing unit (CPU) cores
- 178 ▪ 16 gigabytes (GB) of random-access memory (RAM)

179 ■ 120 GB hard disk drive (HDD)

180 ■ 1 network adapter

181 **Network Configuration (Interface 1):**

182 ■ Internet protocol version 4 (IPv4): manual

183 ■ Internet protocol version 6 (IPv6): disabled

184 ■ Internet protocol (IP) address: 172.16.3.10

185 ■ Netmask: 255.255.255.0

186 ■ Gateway: 172.16.3.1

187 ■ DNS name servers: 172.16.3.10

188 ■ DNS-search domains: AcmeFinancial.com

189 **2.1.3 Installation**

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

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

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

195 **2.1.4 DNS Configuration**

196 1. Create the host records and reverse entries in the AcmeFinancial.com DNS service for the
197 following servers:

198 a. Bomgar Privileged Identity

199 b. TDi ConsoleWorks

200 c. Splunk Enterprise

201 d. Radiant Logic Federated Identity (FID)

202 e. Ekran System

203 f. Remediant SecureONE

204 g. RSA Authentication Manager

205 h. OneSpan IDENTIKEY

206 **2.1.5 Group Policy Object Configuration**

- 207 1. Open **Group Policy Management**.
- 208 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

210

211 **2.1.6 Scripts**

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

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

```
216 import csv
217 import re
218 from subprocess import check_output
```

```
219 csvfile = open('Final_AD.csv', 'w+')
220 wr = csv.writer(csvfile, quoting=csv.QUOTE_ALL)
221 csvlist = ["Event", "UserSubject", "UserObject", "Timestamp"]
222 wr.writerow(csvlist)
223 with open('ADLOG.csv', 'r') as f:
224     reader = csv.reader(f)
225     zerothrow = 1
226     for row in reader:
227         csvlist = []
228         if zerothrow == 1:
229             zerothrow = 0
230         else:
231             parse_list = row[1].split('\n')
232             #print parse_list
233             #break
234             csvlist.append(parse_list[0].replace('\t', '') .replace('\r', ''))
235             csvlist.append(parse_list[4].replace('\t', '') .replace('\r',
236             '') .replace('Account Name:', ''))
237             if row[4] == "4728":
238                 win_command = parse_list[10].replace('\t', '') .replace('\r',
239                 '') .replace('Account Name:', '')
240                 win_command = win_command[:3] + ' "' + win_command[3:]
241                 sec_index = win_command.index(",CN=")
242                 win_command = win_command[:sec_index] + ' "' +
243                 win_command[sec_index:]
244                 win_command = "dsquery * " + win_command + " -scope base -attr
245                 sAMAccountName"
246                 account = check_output(win_command, shell = True).decode()
247                 account = account.replace('sAMAccountName', '') .replace('\n',
248                 '') .replace(' ', '')
249                 csvlist.append(account)
250             else:
```

```

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

```

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

```

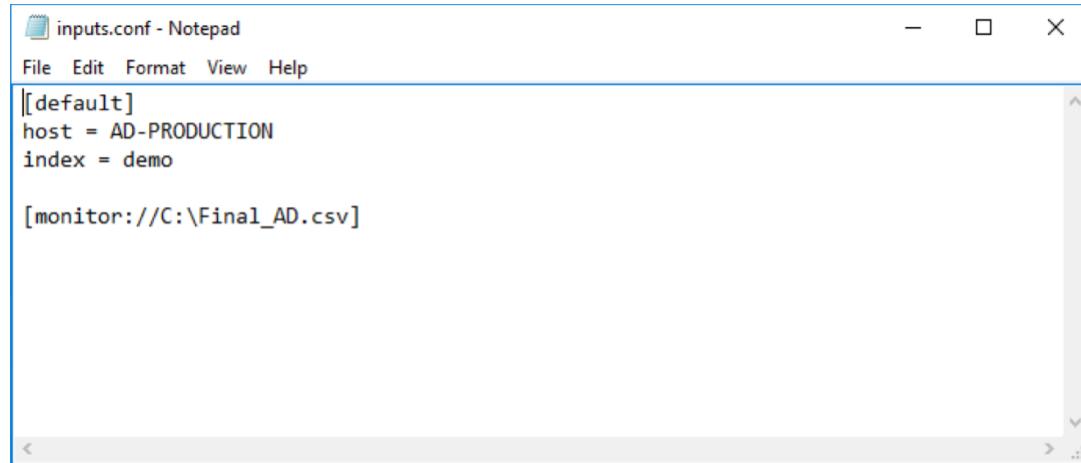
260 Set-Variable -Name EventAgeDays -Value 2      #we will take events for the latest 2 days
261 Set-Variable -Name Computer -Value "AD-Production"  # replace it with your server
262 names
263 Set-Variable -Name LogNames -Value "Security" # Checking app and system logs
264 Set-Variable -Name EventTypes -Value @(7001, 7002, 4720, 4722, 4725, 4726, 4728, 4738)
265 # Loading only Errors and Warnings
266 Set-Variable -Name ExportFolder -Value "C:\"
267 $el_c = @() #consolidated error log
268 $now=get-date
269 $startdate=$now.adddays(-$EventAgeDays)
270 $ExportFile=$ExportFolder + "ADLOG.csv" # we cannot use standard delimiteds like ":"#
271 Write-Host Processing $Computer\$LogNames
272 $el = get-eventlog -ComputerName $Computer -log $LogNames -After $startdate -
273 InstanceId $EventTypes
274 $el_c += $el #consolidating
275 $el_sorted = $el_c | Sort-Object TimeGenerated    #sort by time
276 Write-Host Exporting to $ExportFile
277 $el_sorted|Select EntryType, Message, TimeGenerated, Source, EventID, MachineName |
278 Export-CSV $ExportFile -NoTypeInfo #EXPORT
279 Write-Host Done!
280 python adparse.py

```

281 **2.1.7 Splunk Universal Forwarder**

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

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



```
inputs.conf - Notepad
File Edit Format View Help
[[default]
host = AD-PRODUCTION
index = demo

[monitor://C:\Final_AD.csv]
```

286

287 **2.2 Bomgar Privileged Identity**

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

289 **2.2.1 How It's Used**

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

293 **2.2.2 Virtual Machine Configuration**

294 The Privileged Identity virtual machine is configured as follows:

- 295 □ Windows Server 2012 R2
- 296 □ 4 CPU cores
- 297 □ 16 GB of RAM
- 298 □ 60 GB of storage
- 299 □ 1 network interface controller/card (NIC)

300 **Network Configuration (Interface 1):**

- 301 ■ IPv4: manual
- 302 ■ IPv6: disabled
- 303 ■ IPv4 address: 172.16.1.10
- 304 ■ Netmask: 255.255.255.0
- 305 ■ Gateway: 172.16.1.1
- 306 ■ DNS name servers: 172.16.3.10
- 307 ■ DNS-search domains: not applicable (N/A)

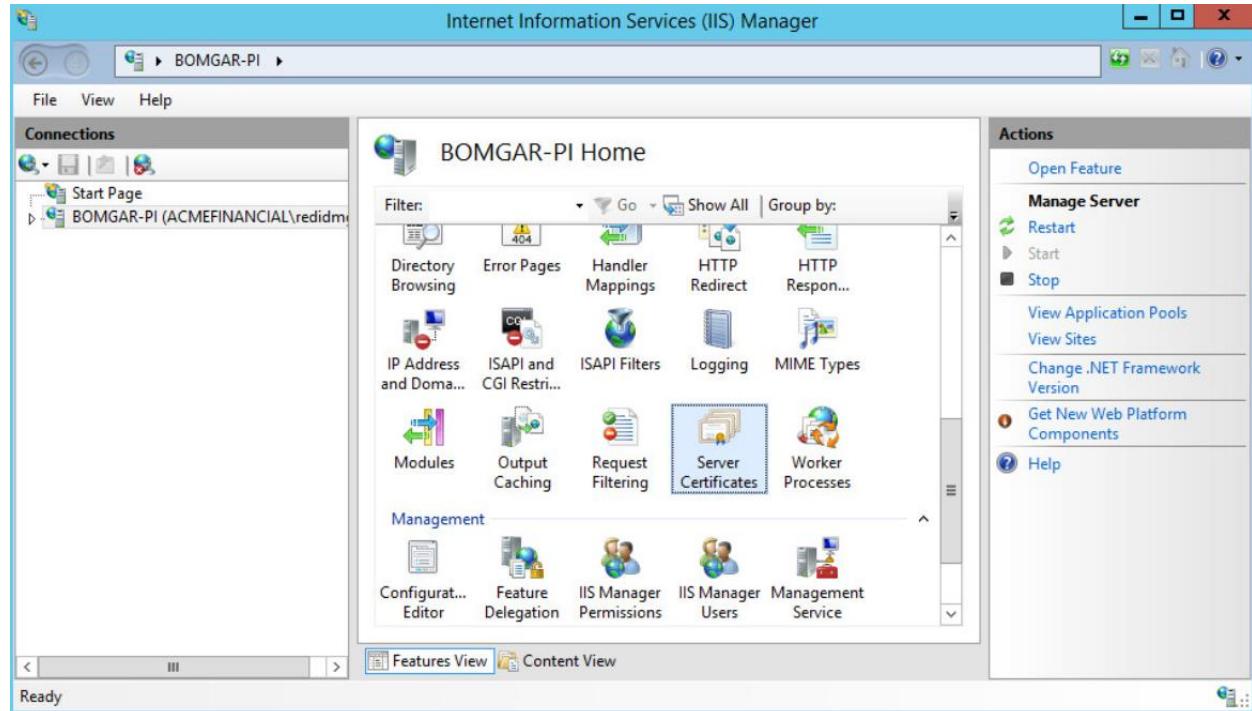
308 **2.2.3 Prerequisites**

- 309 ■ 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.
- 310
- 311 ■ The web application server's requirements include Internet Information Services (IIS) and Microsoft .NET Framework 4.5.2 or later.
- 312
- 313 ■ A full list of requirements can be found in the Installation Guide on Bomgar's [website](#).

314 **2.2.4 Installing Privileged Identity**

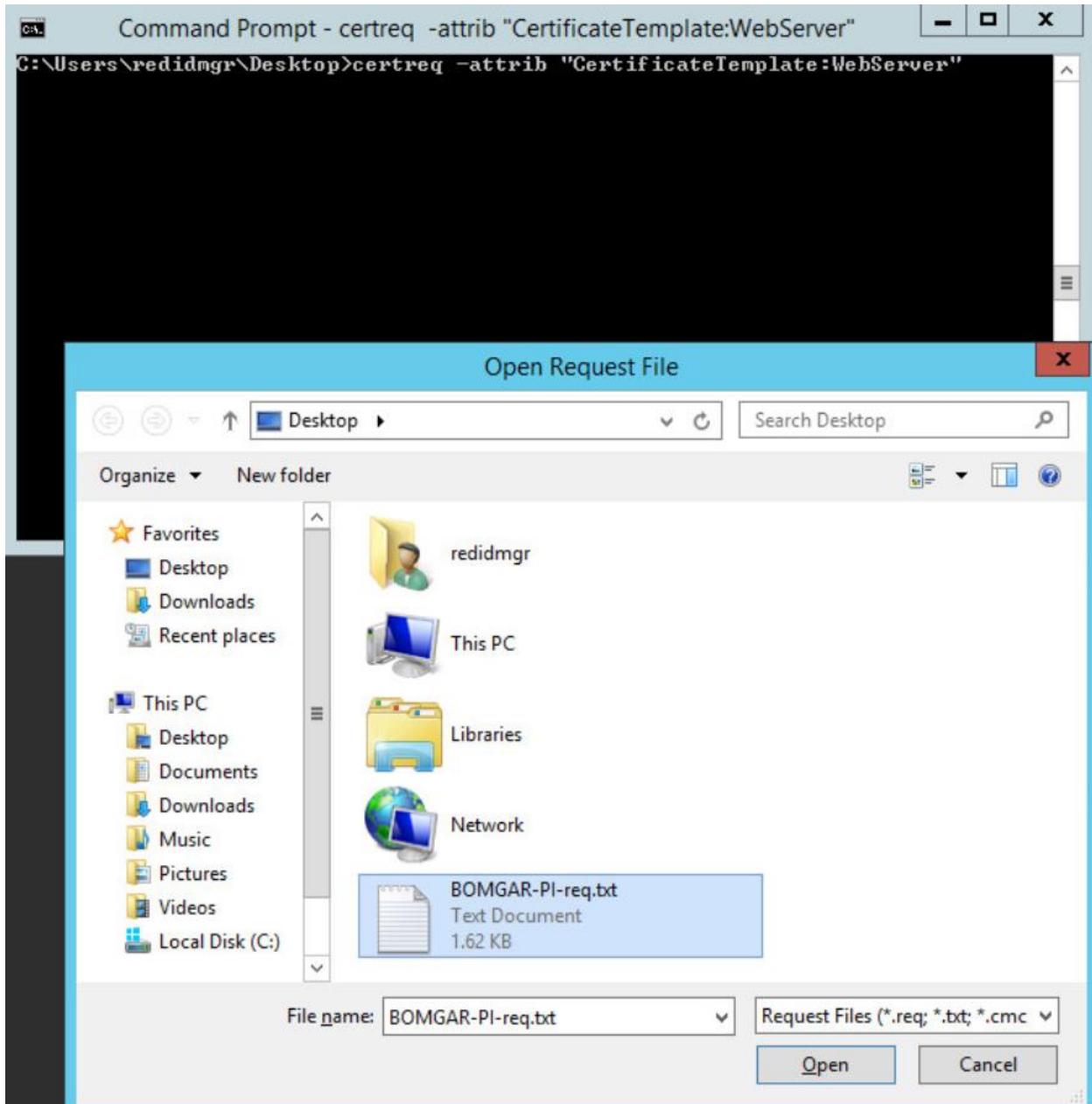
315 To configure IIS for use with Bomgar's web application server, a certificate signed by AD Certificate
316 Services was created.

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



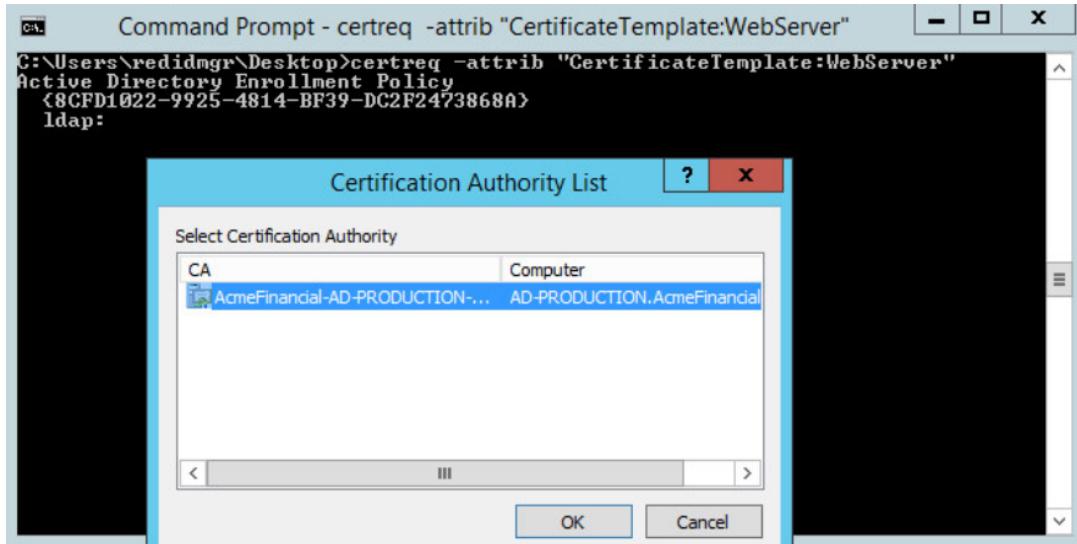
320

- 321 4. On the right, click **Create Certificate Request**.
- 322 5. Fill out the **Distinguished Name Properties**, and then click **Next**.
- 323 6. Select a bit length of **2048**, and then click **Next**.
- 324 7. Give the certificate a file name, and then click **Finish**.
- 325 8. Using the certreq command in the **Command Prompt**, enter `certreq -attrib "CertificateTemplate:WebServer"`.
- 326
- 327 9. Select the certificate file that was created in Step 7, and then click **Open**.



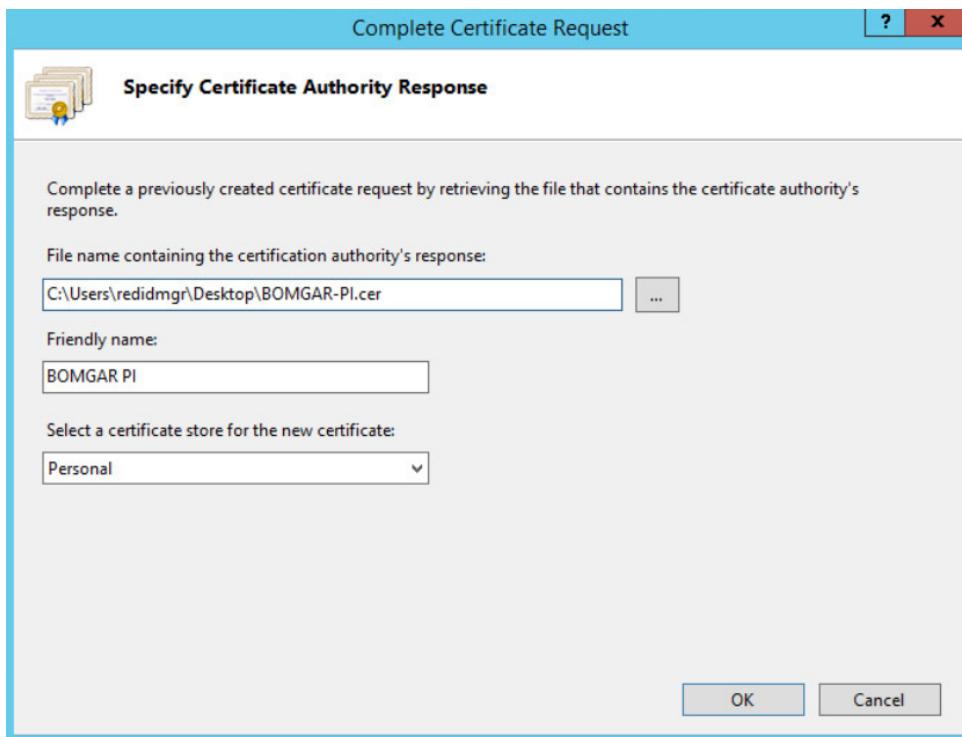
328

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., Bomgar-PI), and store it in the **Personal** certificate store.



335

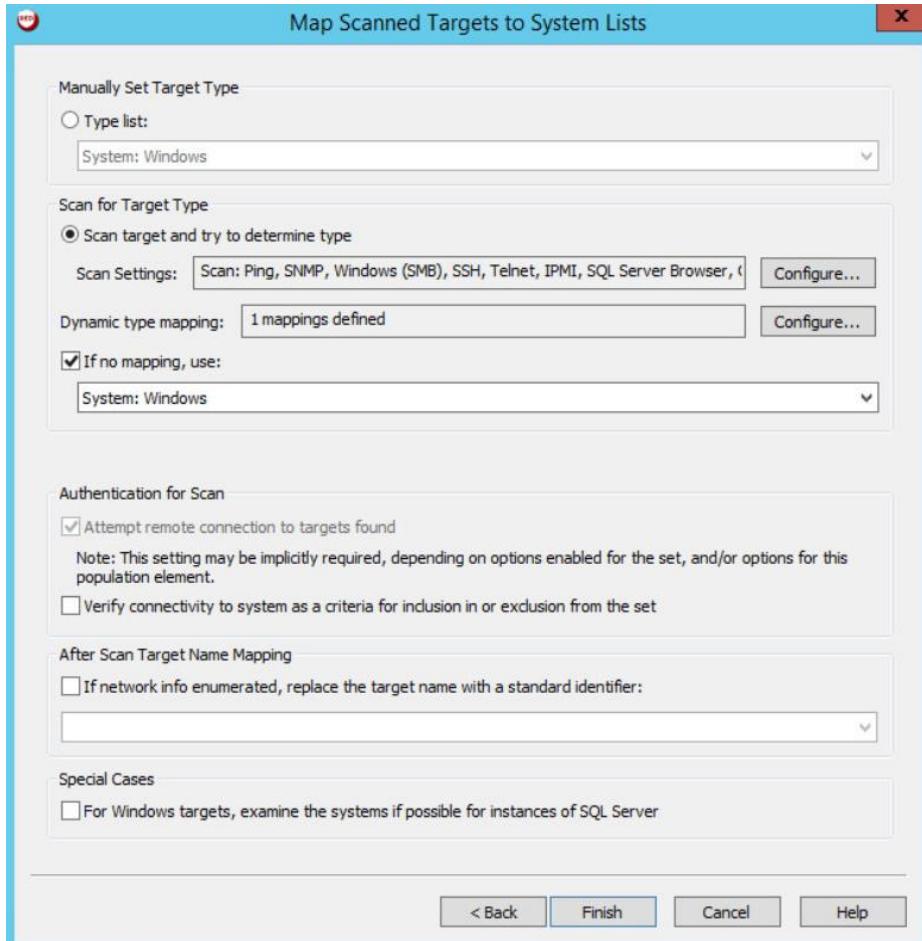
- 336 14. Click **OK**
- 337 15. Create a Secure Sockets Layer (SSL) binding with that certificate by following [documentation from Microsoft](#).
- 339 You are now ready to begin following further installation instructions that are publicly available on
340 Bomgar's [website](#).

341 **2.2.5 Configuration**

342 Using the Bomgar Privileged Identity [Admin Guide](#), complete the configuration steps provided in the
343 following subsections.

344 **2.2.5.1 Management Set**

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



349

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

Configure Management Set

Identification				
Name:	AcmeFinancial			
Comment:				
Add targets from:				
Inclusion	Type	Config	Connect?	ResultTargetType
<input checked="" type="checkbox"/> Include	AD Query	LDAP://CN=Computers,DC=Acm...	Attempt	[dynamic or] Windows
<input checked="" type="checkbox"/> Include	Static	1 Targets (AcmeFinancial.com)	No	Windows
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Remove"/>				
Dynamic Update				
<input type="radio"/> Do not update this set dynamically (manual update only) <input checked="" type="radio"/> Update this set dynamically				
Job config:	Daily			<input type="button" value="Configure..."/>
Last run:	6/27/2018 12:00:59 AM			
Options <input type="button" value="Configure..."/>				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>				

353

354 2.2.5.2 Delegation Identities

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

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

- 357 1. Add the following regular user accounts as Delegation Identities by selecting **Delegation > Delegation Identities** and then clicking **Add**.

- 358 a. ACMEFINANCIAL\udb1

360 b. ACMEFINANCIAL\twitteruser

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

363 3. Click **OK**.

364 2.2.6 Installing Privileged Identity Application Launcher

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

368 Using the Bomgar documentation, complete the following steps:

369 1. Create a new virtual machine:

370 a. Windows Server 2012 R2

371 b. 1 CPU core

372 c. 4 GB of RAM

373 d. 60 GB of storage

374 e. 1 NIC

375 i. IPv4: manual

376 ii. IPv6: disabled

377 iii. IPv4 address: 172.16.1.31

378 iv. Netmask: 255.255.255.0

379 v. Gateway: 172.16.1.1

380 vi. DNS-search domains: N/A

381 2. Install Remote Desktop Services.

382 3. DO NOT install Desktop Experience.

383 4. Install Application Launcher without Session Recording.

384 5. Configure Remote Desktop Services to publish **LiebsoftLauncher.exe** and **ssms.exe**.

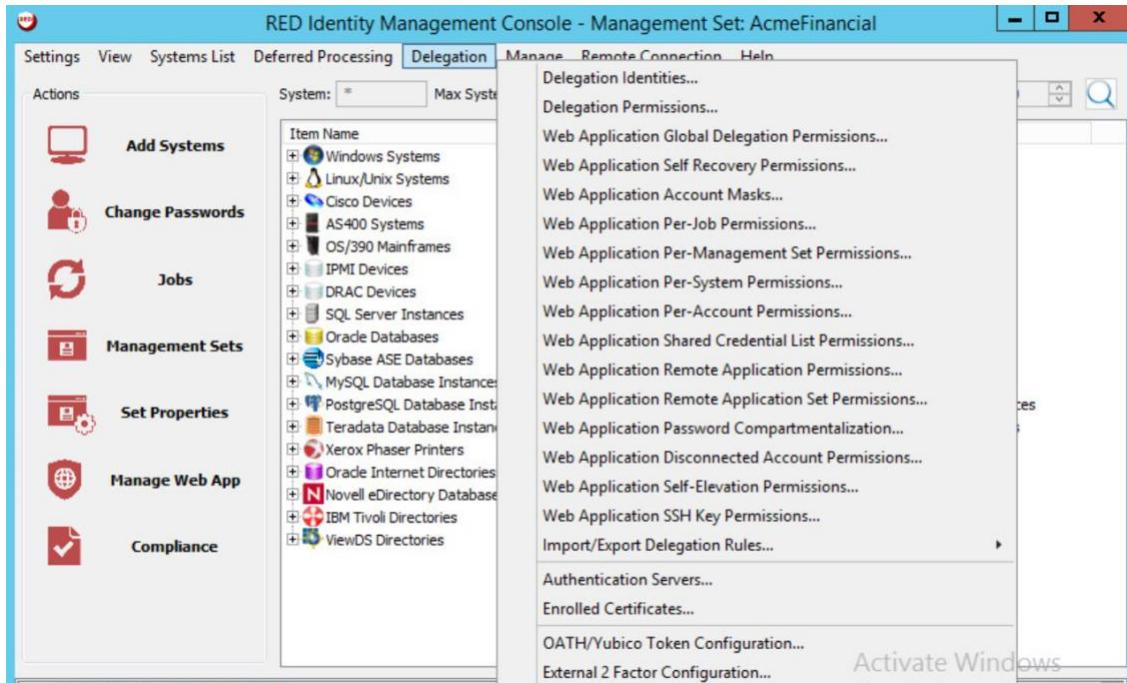
385 6. Configure the web launcher settings in the Bomgar **RED Identity Management Console**.

386 2.2.7 Configure Bomgar Privileged Identity with IdRamp SAML Authentication

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

389 1. Open the Bomgar **RED Identity Management Console** desktop application.

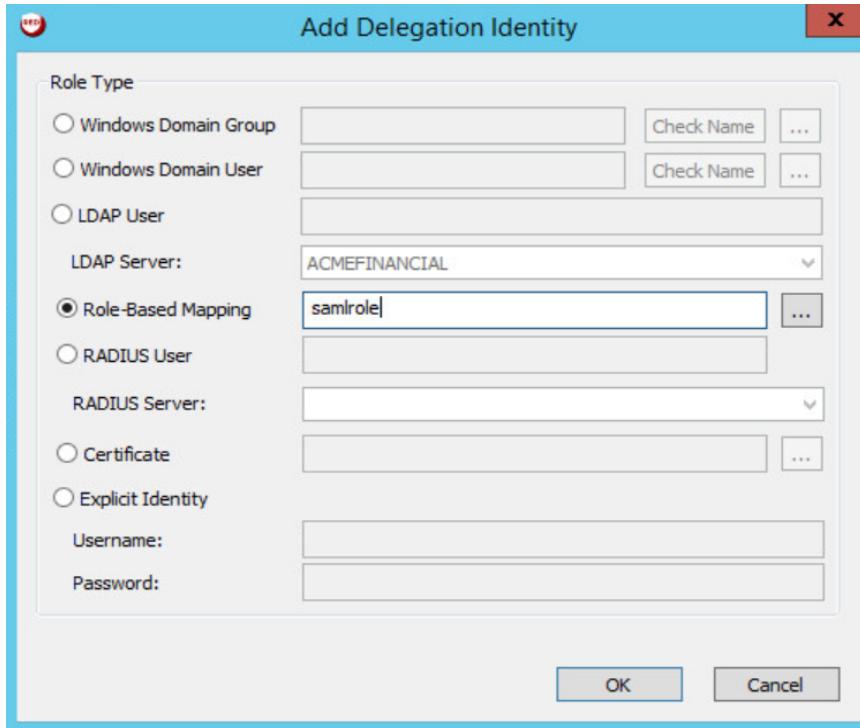
390 2. Navigate to **Delegation > Web Application Global Delegation Permissions**.



391

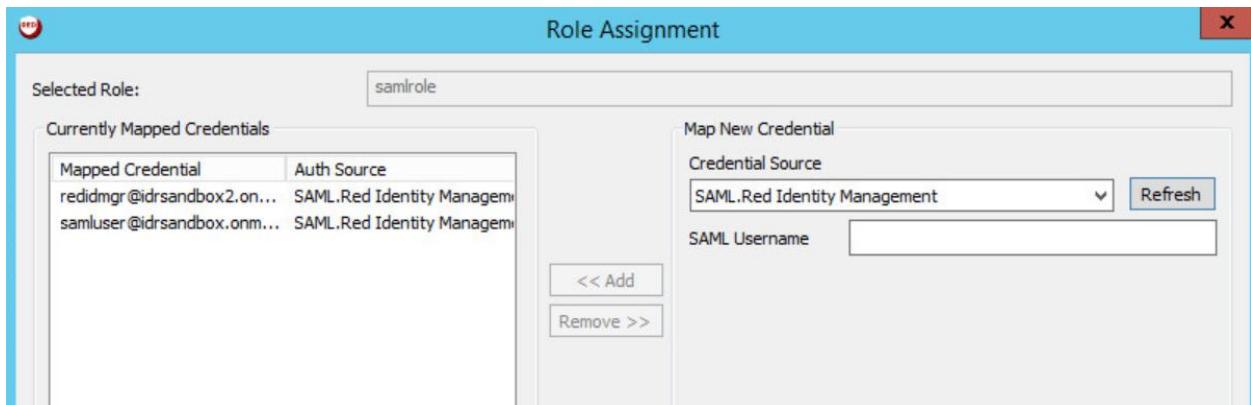
392 3. Click **Add** at the lower left corner.

393 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 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 Access** check boxes.

Web Application Global Delegation Permissions

Authentication

Delegation Identities

Identity	Type
[DefaultAuthenticatedUser]	Explicit
[WebApplicationManager]	Explicit
ACMEFINANCIAL\Administrator	Domain User
ACMEFINANCIAL\aduser	Domain User
ACMEFINANCIAL\redidmgr	Domain User
ACMEFINANCIAL\testdomuser1	Domain User
ACMEFINANCIAL\twitteruser	Domain User
ACMEFINANCIAL\udb1	Domain User
Administrator User	Delegation Role
Auditor User	Delegation Role
Recovery User	Delegation Role
Request User	Delegation Role
samlrole	Delegation Role

Global Identity Rules:

- Logon
- Require Ext 2-Factor Auth
- Require OATH/Yubico
- Add/Edit/Delete Passwords
- Manage Scheduled Jobs
- View Web Activity Logs
- Elevate Any Account
- View Delegation
- Access File Repository
- Manage Delegation
- Manage External Lists
- View Dashboards
- Ignore Password Checkout
- Grant All Access

Identity Rules For Management Sets:

- Request Password Access
- Request Remote Access
- Grant Requests
- Recover Passwords
- Elevate Account Access
- View Accounts
- View Systems
- Allow Remote Sessions
- Add/Edit/Delete Passwords for only Managed Systems
- View Password History
- View Password Activity
- Edit Refresh Jobs
- Edit Password Change Jobs
- Edit Elevation Jobs

Delegated Management Sets For Identity:

Management Sets

402

9. Click **OK**.

403
404
405

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

406
407

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

https://bomgar-pi.acmefinancial.com/PWCWeb/

LIEBERMAN RED

RAPID
ENTERPRISE
DEFENSE

Please log in to access the Web Console

Authenticator

SAML.Red Identity Management

Use Integrated Authentication: ACMEFINANCIAL\redidmgr

Login

408

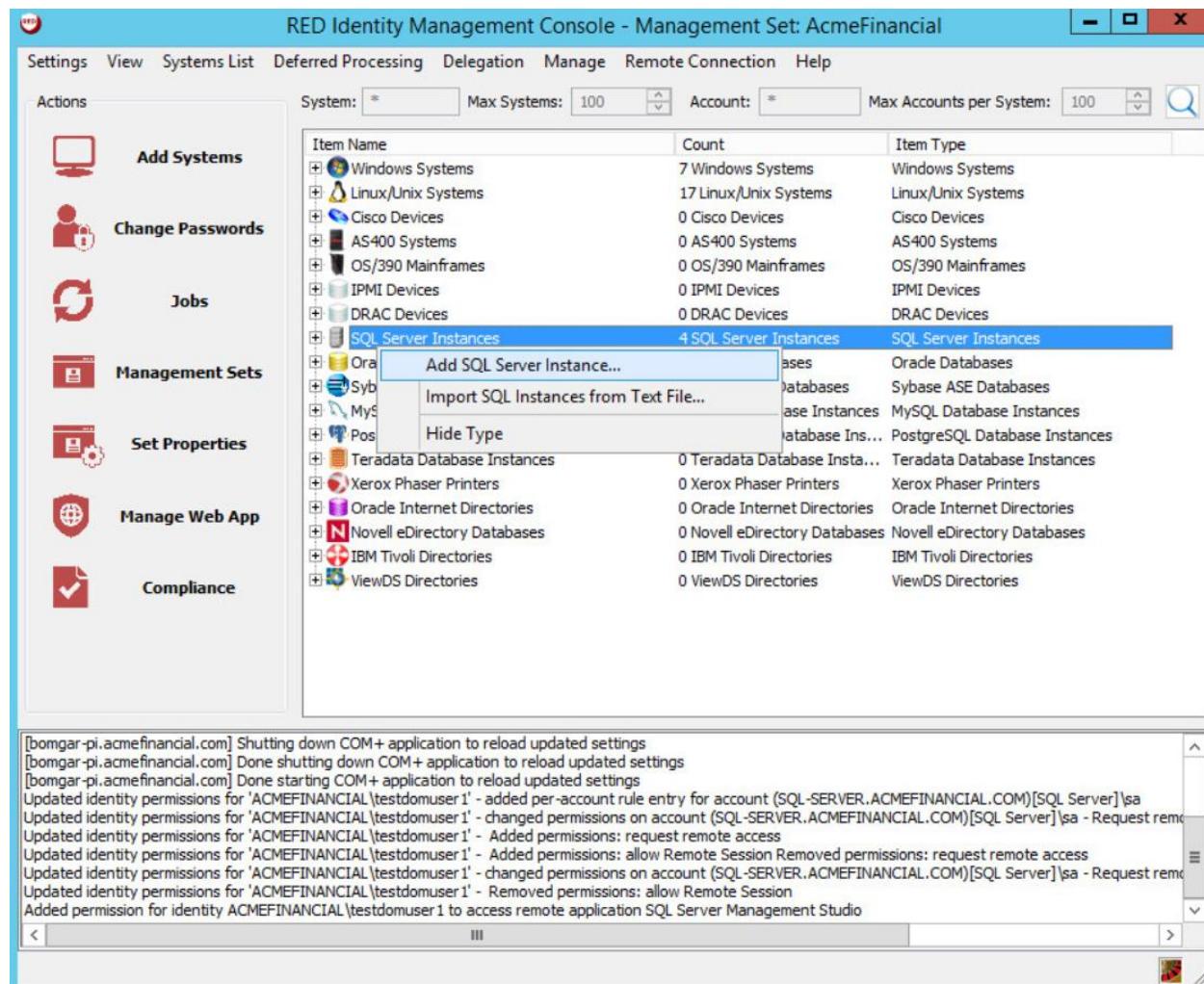
409 **2.2.8 Configuring Microsoft SQL Server Access**

410 Prerequisites:

- 411
 - Microsoft SQL Server has hybrid authentication.
 - Microsoft SQL Server Management Studio (SSMS) has already been added as an application in the application launcher.

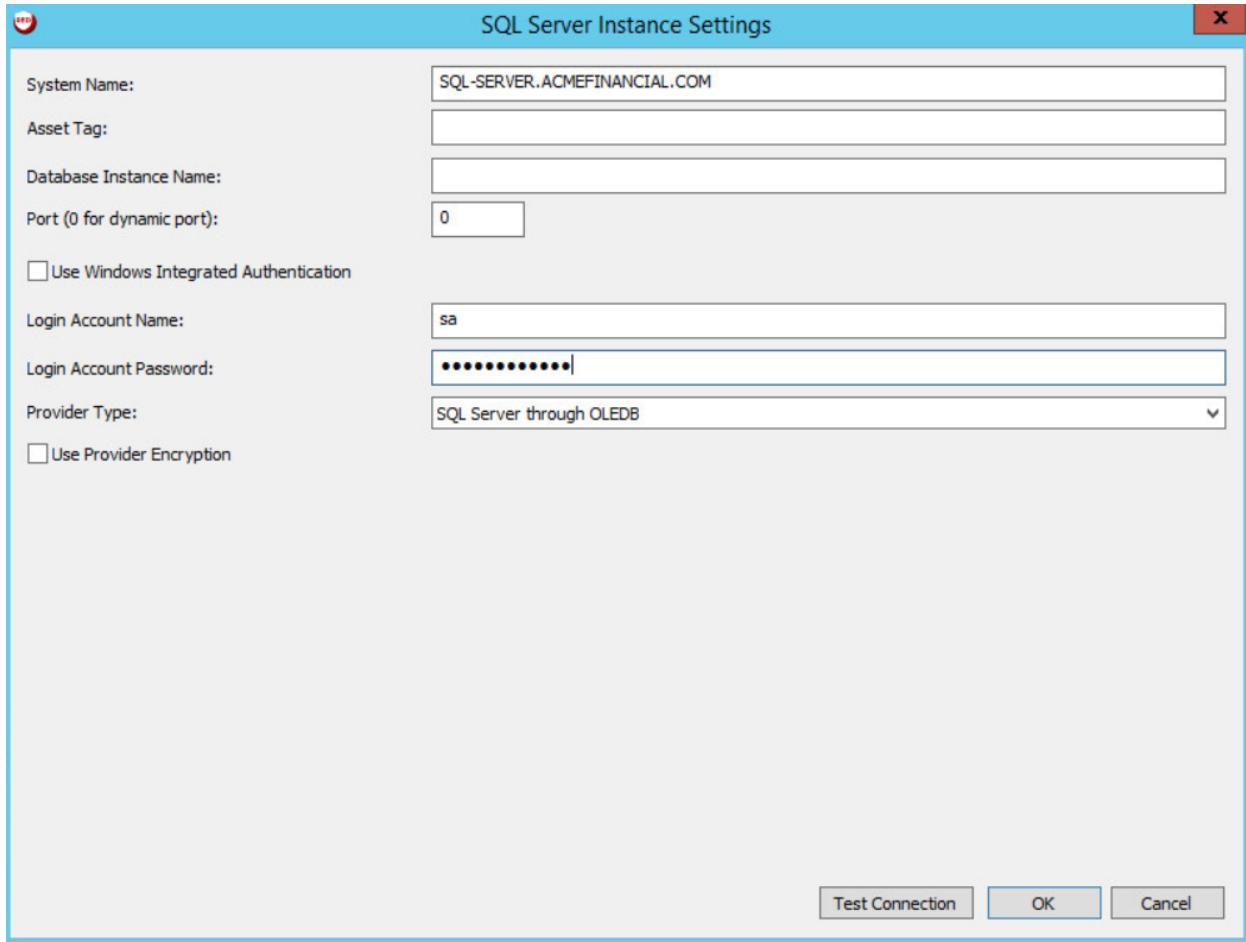
414 The following instructions configure Bomgar Privileged Identity to allow the **edb1** to request permission
 415 to launch Microsoft SSMS and to log in as the **sa** account on Microsoft SQL Server in the production
 416 environment.

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

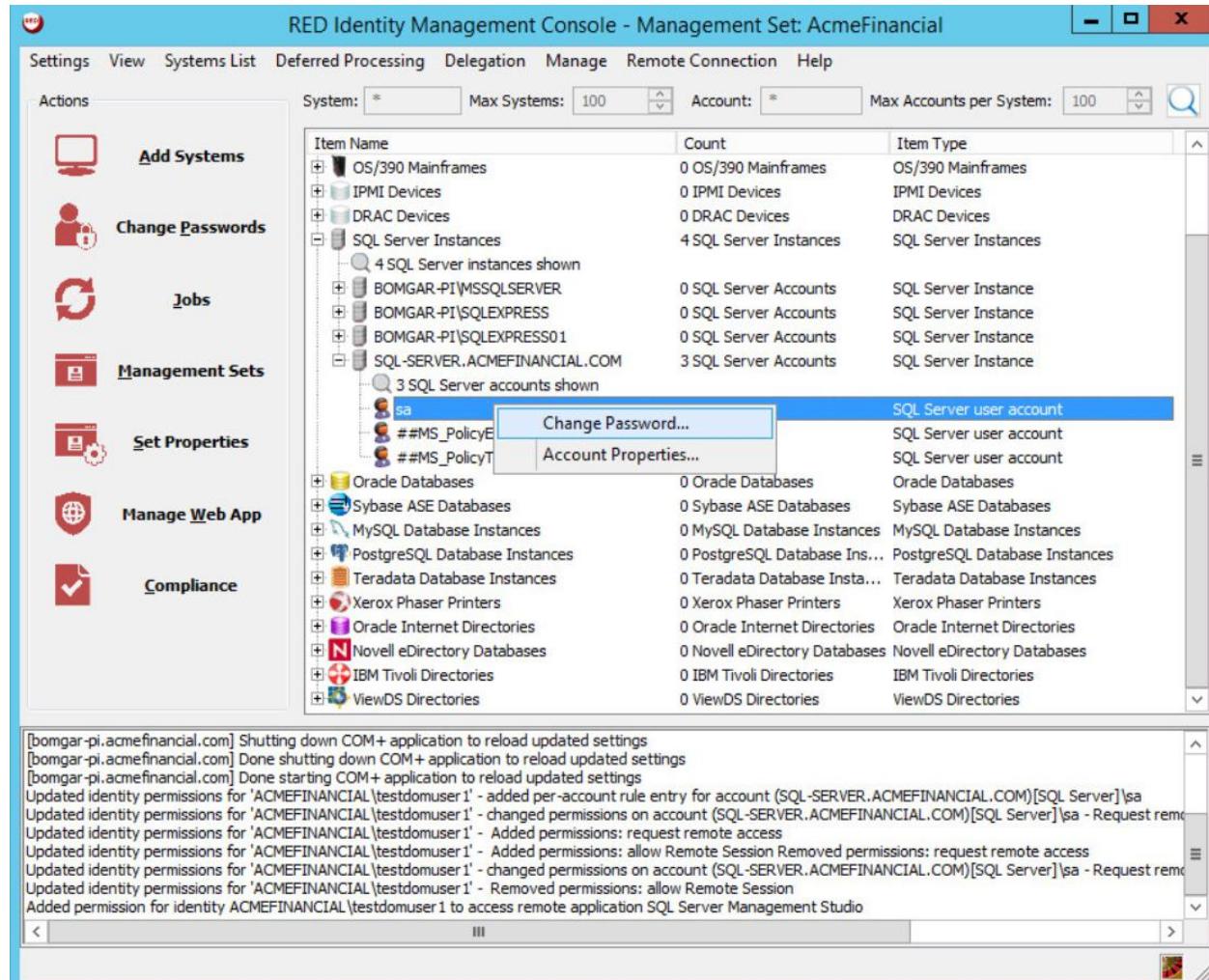


419

- 420 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.

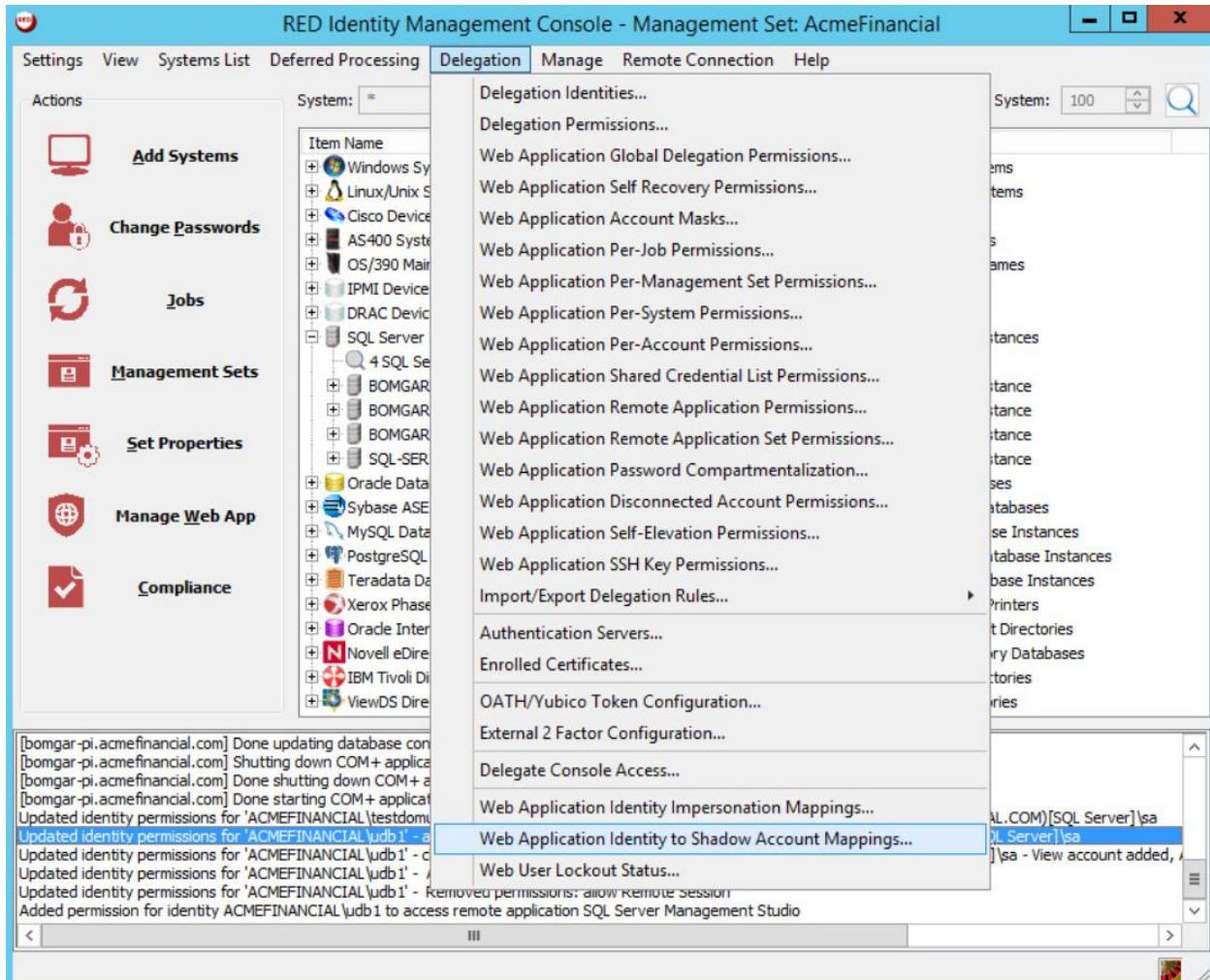


- 424 3. Click **Test Connection**. The connection should be successful. Click **OK**.
- 425 4. Expand **SQL Server Instances** by clicking on the plus sign to the left of the item name, and then expand **SQL-SERVER.ACMEFINANCIAL.COM**. Right-click the **sa** account, and then select **Change Password**.



429

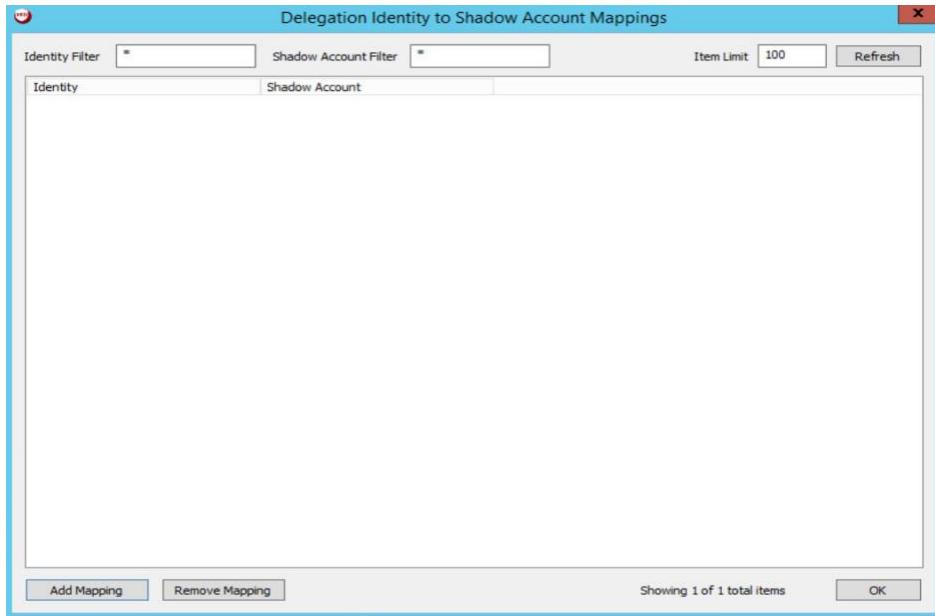
- 430 5. Select strong password policy options, such as increasing both the length of the password and its compliance with password standards.
- 432 6. On the **Schedule** tab, set the **Job Scheduling Period** to **Immediately**, and write a **Job Comment** to describe why this action is being taken.
- 434 7. Click **OK**, and then let the operation complete.
- 435 8. Click **Delegation > Web Application Identity to Shadow Account Mappings**.



436

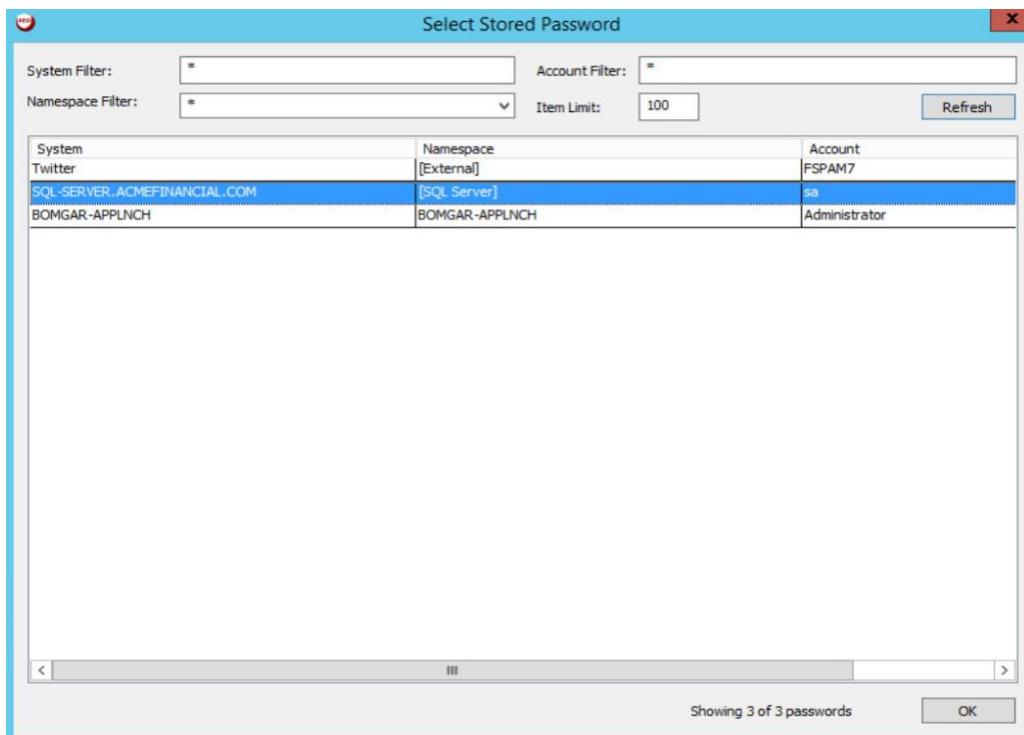
437

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**.

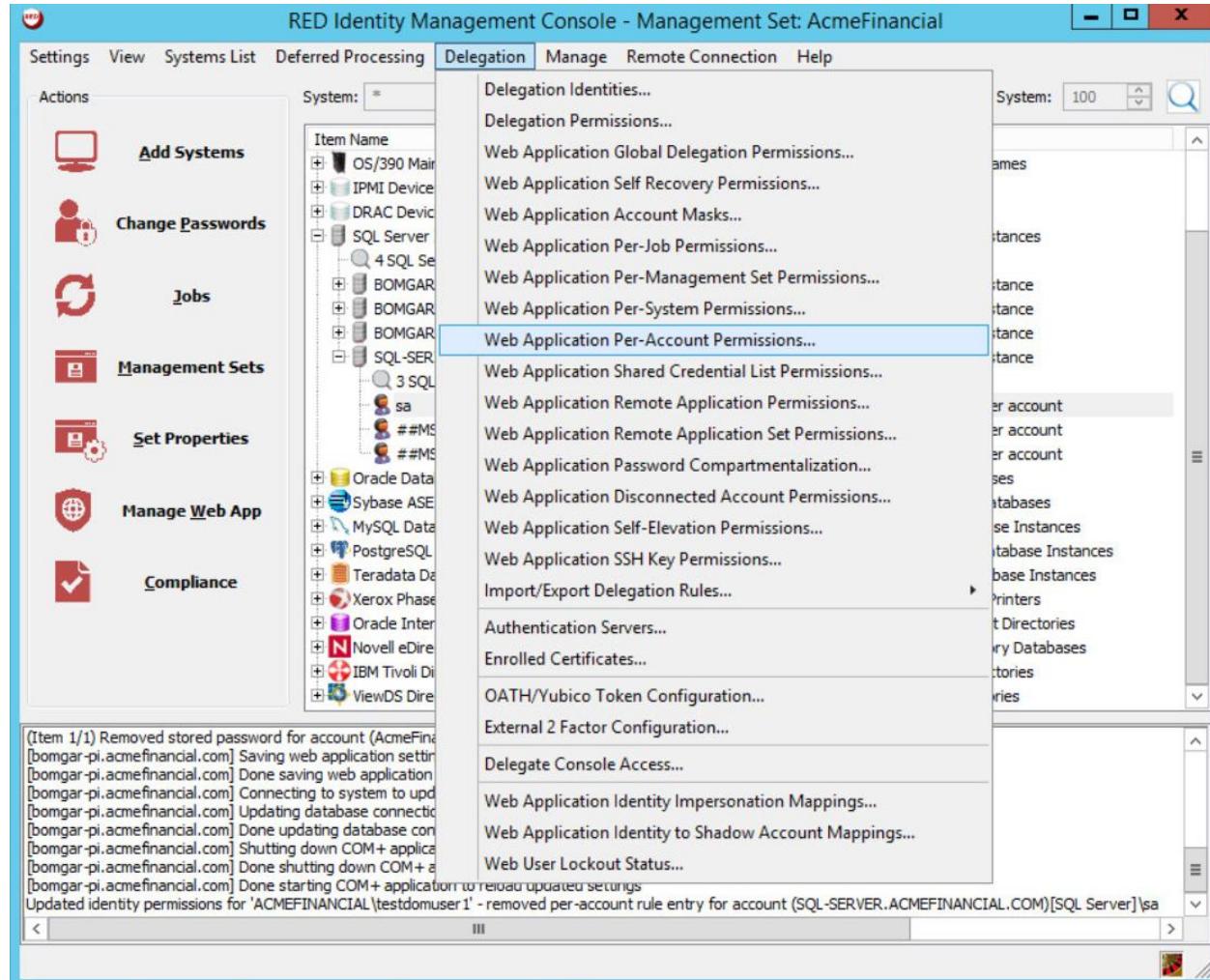


441

- 442 11. Click **OK** again.

443

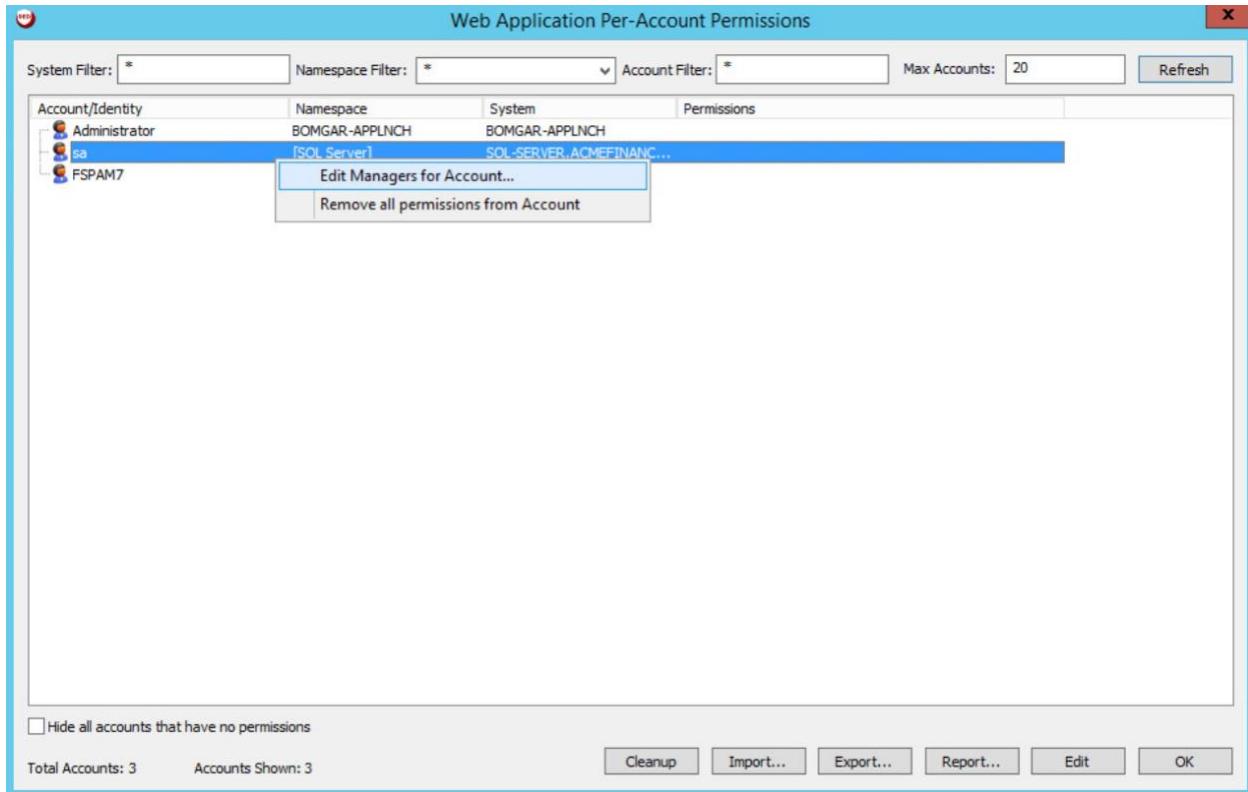
12. Click Delegation > Web Application Per-Account Permissions.



444

445

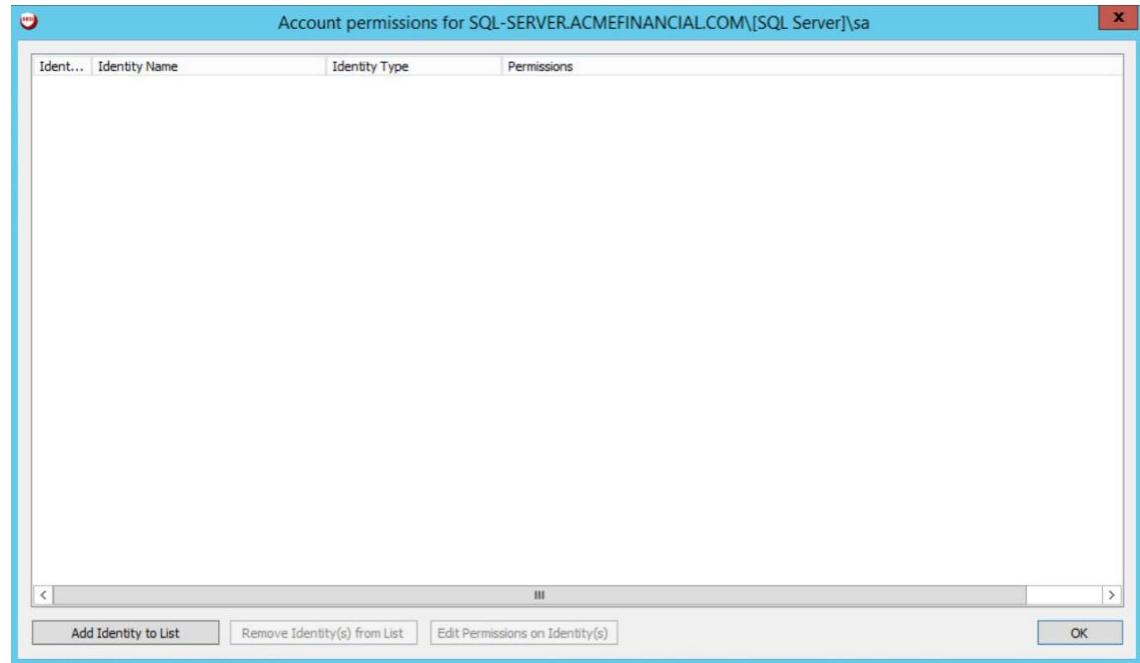
13. Right-click the **sa account, and then select **Edit Managers for Account**.**



446

447 14. Click Add Identity to List.

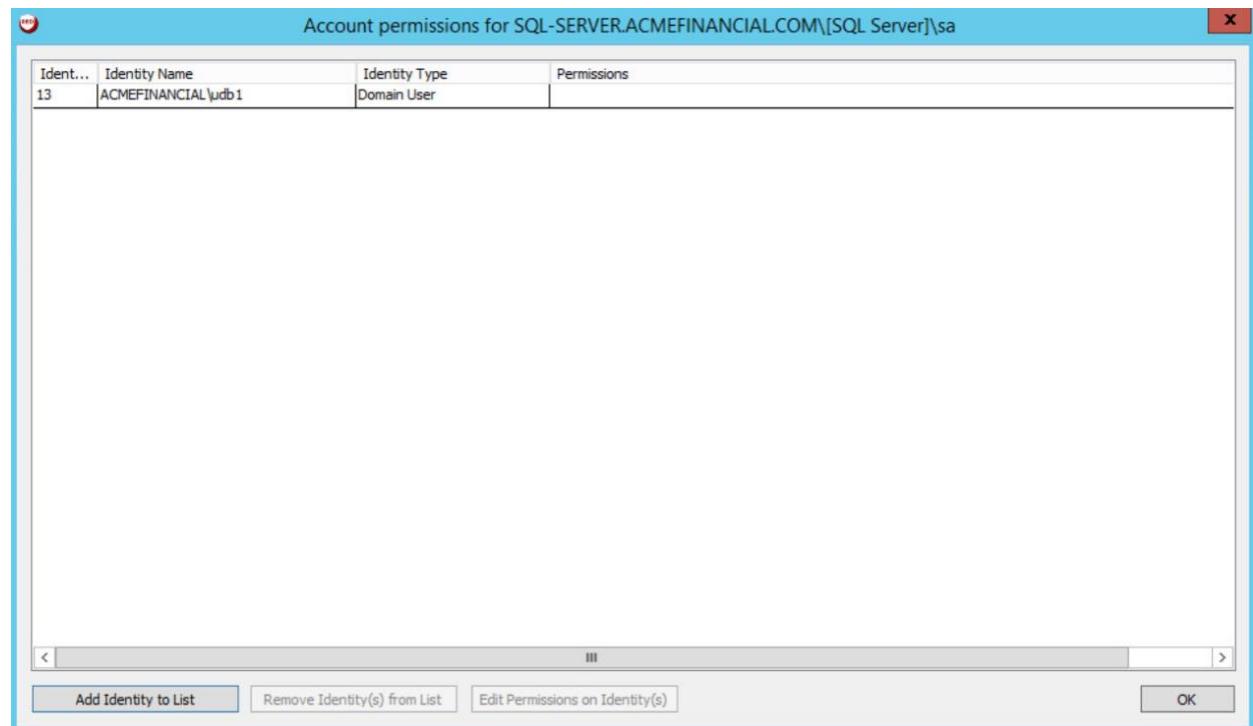
448



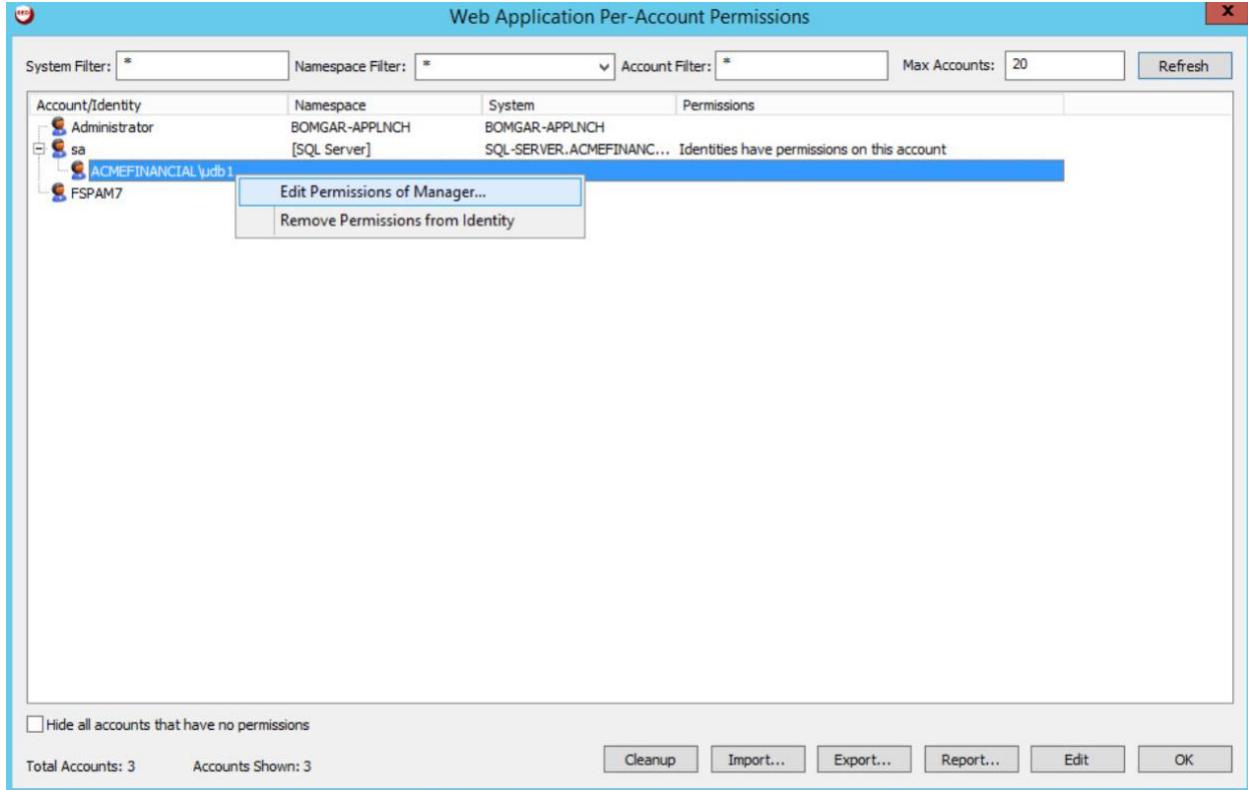
449

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

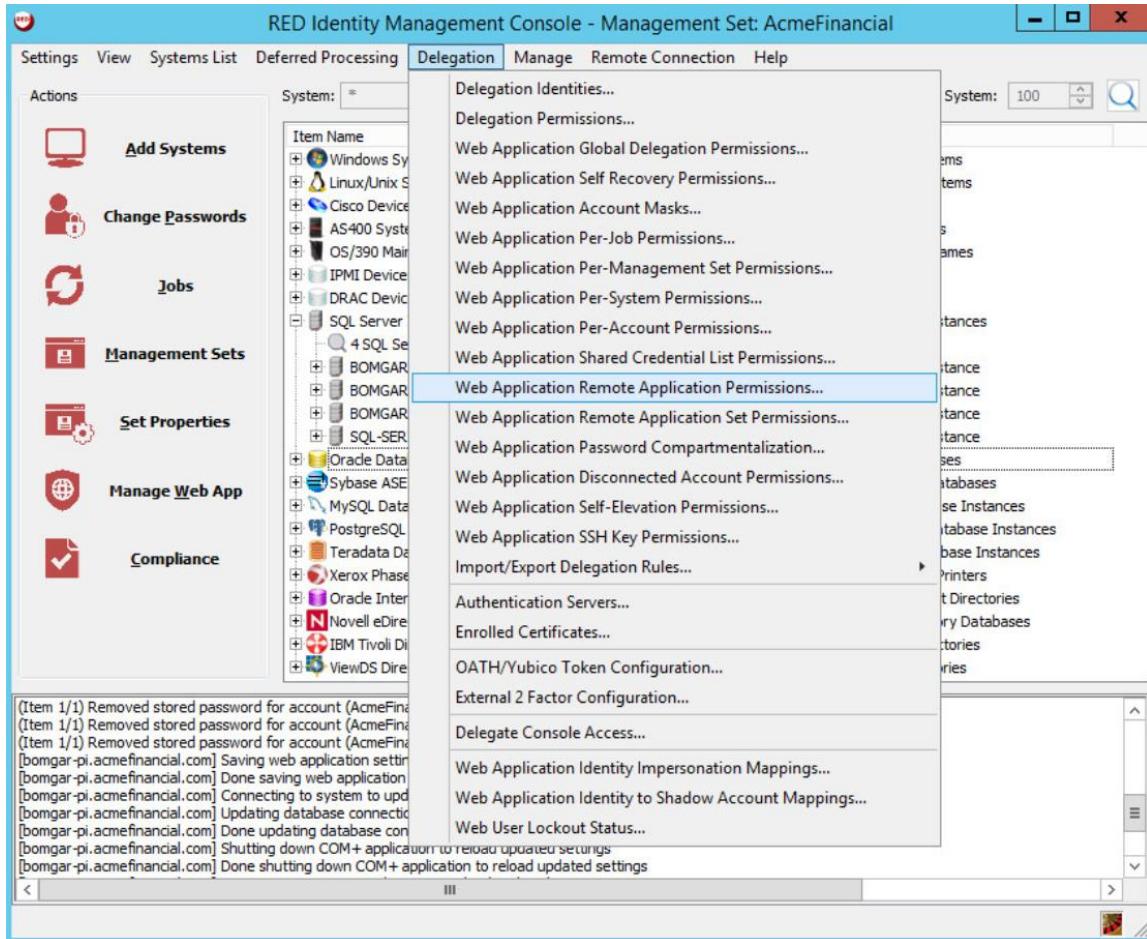
450



- 451 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**.
- 452



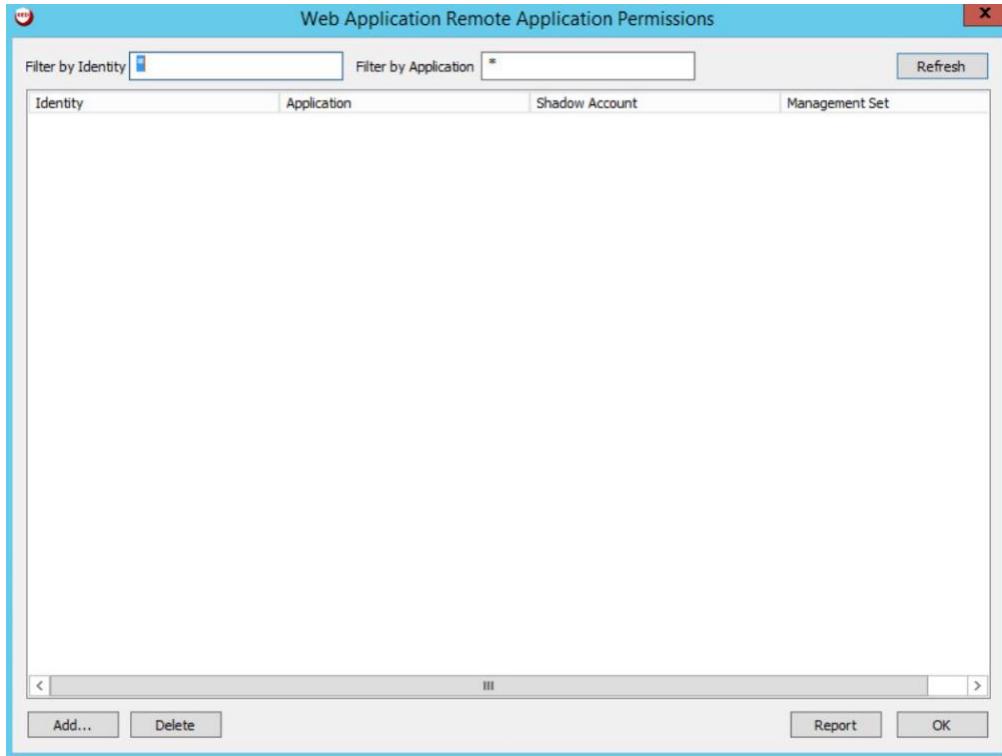
- 453
- 454 17. Give the account the **View Account** and **Request Remote Access** permissions. Click **OK**. Click **OK** again to exit the **Web Application Per-Account Permissions** window.
- 455
- 456 18. Click **Delegation > Web Application Remote Application Permissions**.



457

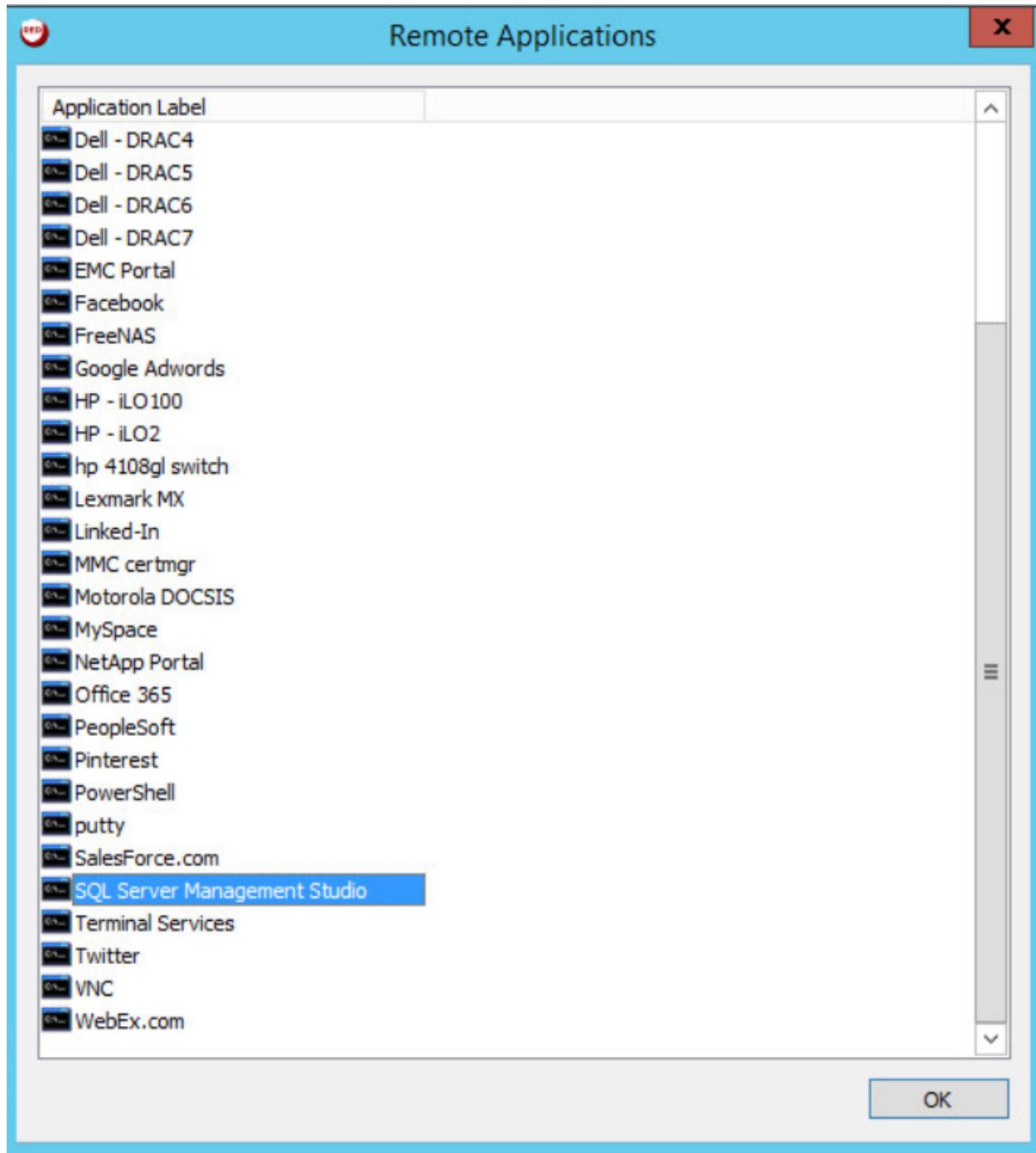
458

19. Click Add.



459

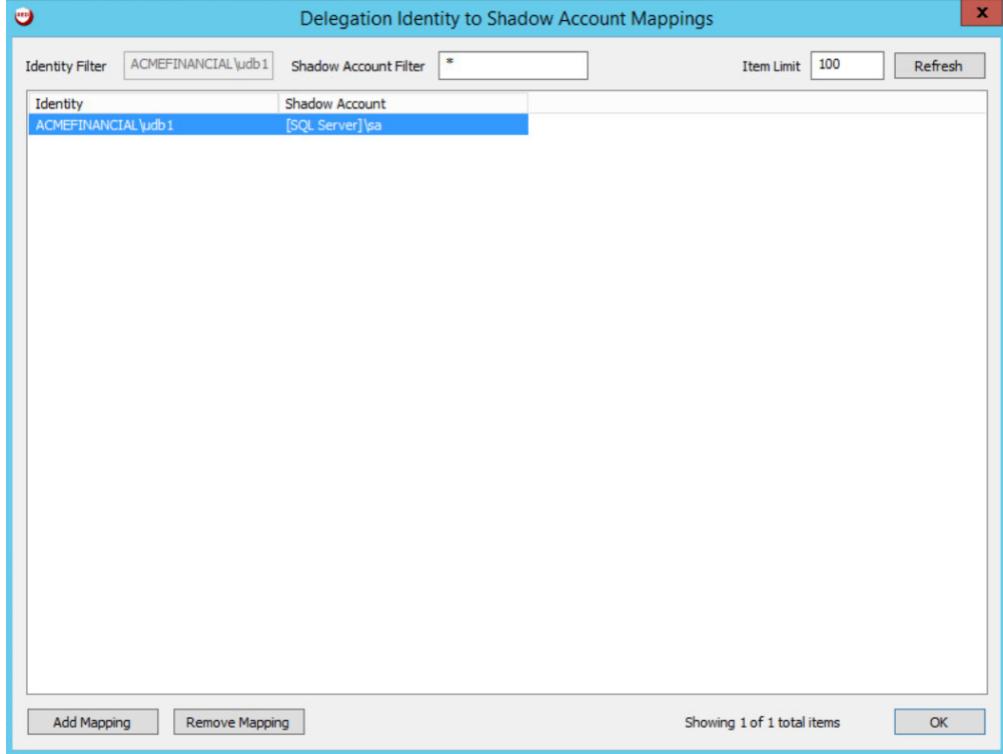
- 460 20. Select the **ACMEFINANCIAL\udb1** account from the list of **Delegation Identities**. Click **OK**. Next,
461 select **SQL Server Management Studio** from the list of **Remote Applications**.



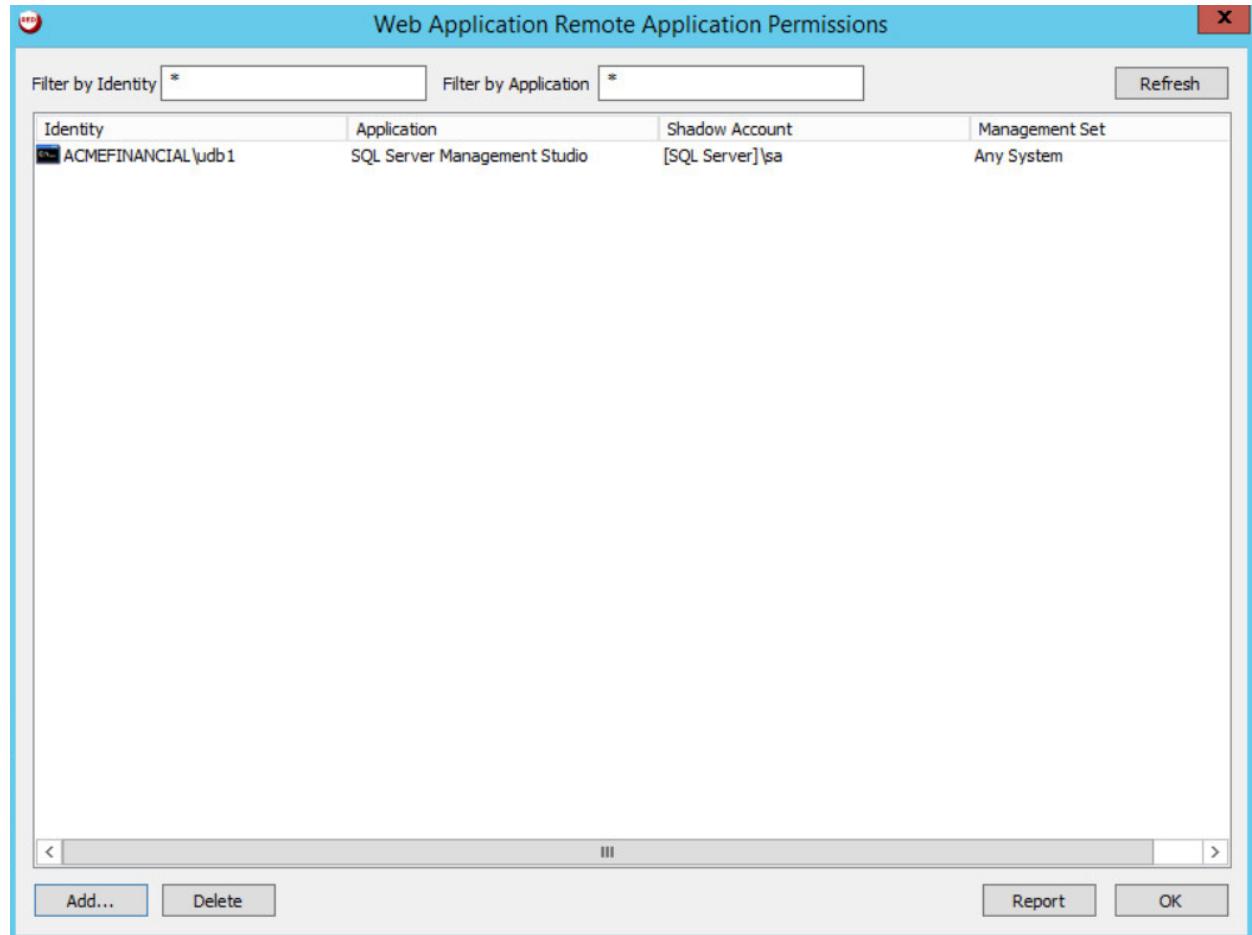
462

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

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



- 466
467 23. Select **No** for pop-up about the **System Target Restriction**.
468 24. You should see that the **ACMEFINANCIAL\udb1** user now has access to **SQL Server**
469 **Management Studio** with the **[SQL Server]\sa** shadow account. Click **OK**.



470

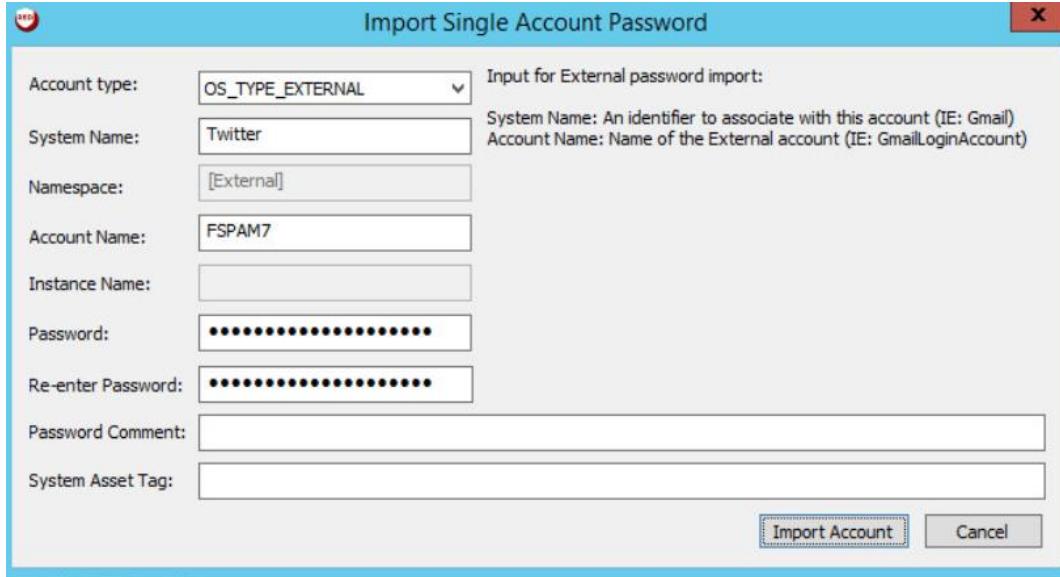
2.2.9 Configuring Twitter Account Launching

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

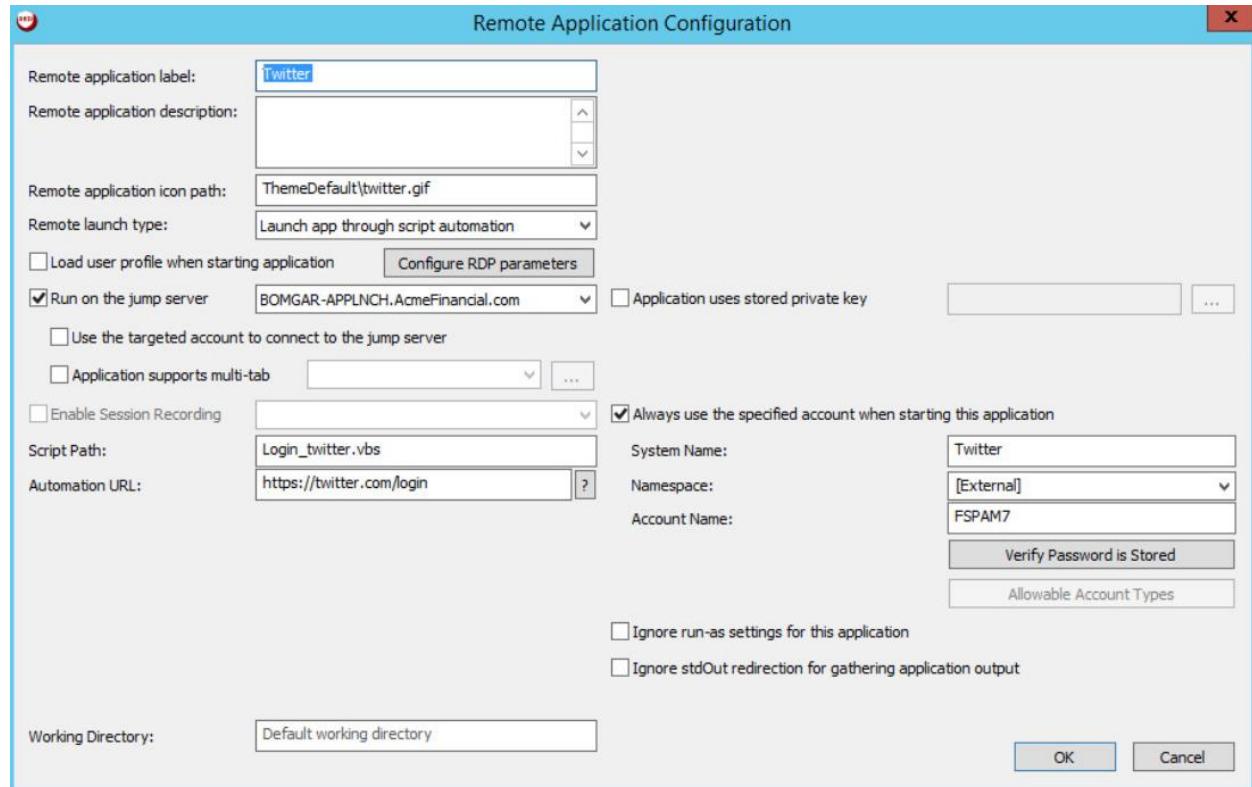
474 To launch Twitter, Bomgar-PI needs the Twitter account password. The following steps detail how to
475 add an external password to Bomgar-PI:

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

- 482 c. **Account Name:** <the Twitter account username>
- 483 d. **Password:** <the Twitter account password>
- 484 e. **Re-enter Password:** <the Twitter account password>



- 485
- 486 3. Click **Import Account**.
- 487 We can now configure Bomgar-PI to use that account to launch Twitter:
- 488 1. Go to **Settings > Manage Web Application > Application Launch**.
- 489 2. Scroll down, and double-click **Twitter**.
- 490 3. In the **Remote Application Configuration** window, enter the following information:
- 491 a. **Run on the jump server:** BOMGAR-APPLNCH.AcmeFinancial.com
- 492 i. This check box should be selected.
- 493 b. **Automation URL:** <https://twitter.com/login>
- 494 c. **Always use the specified account when starting this application:** This check box should be selected.
- 495
- 496 d. **System Name:** Twitter
- 497 e. **Namespace:** [External]
- 498 f. **Account Name:** <the Twitter account username>



499

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

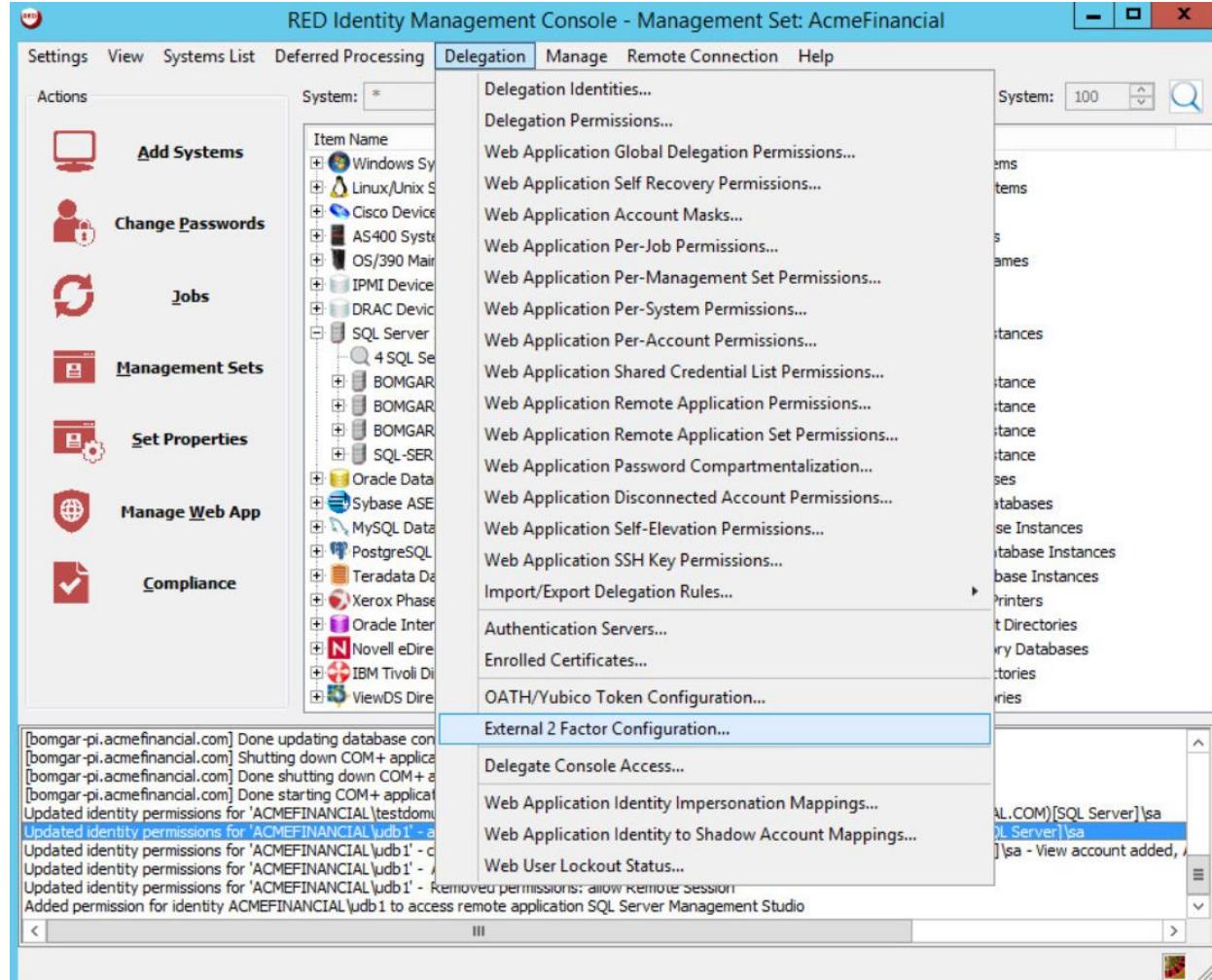
501 To allow users to launch Twitter, follow these steps:

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

511 2.2.10 Configuring Multifactor Authentication with RSA

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

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

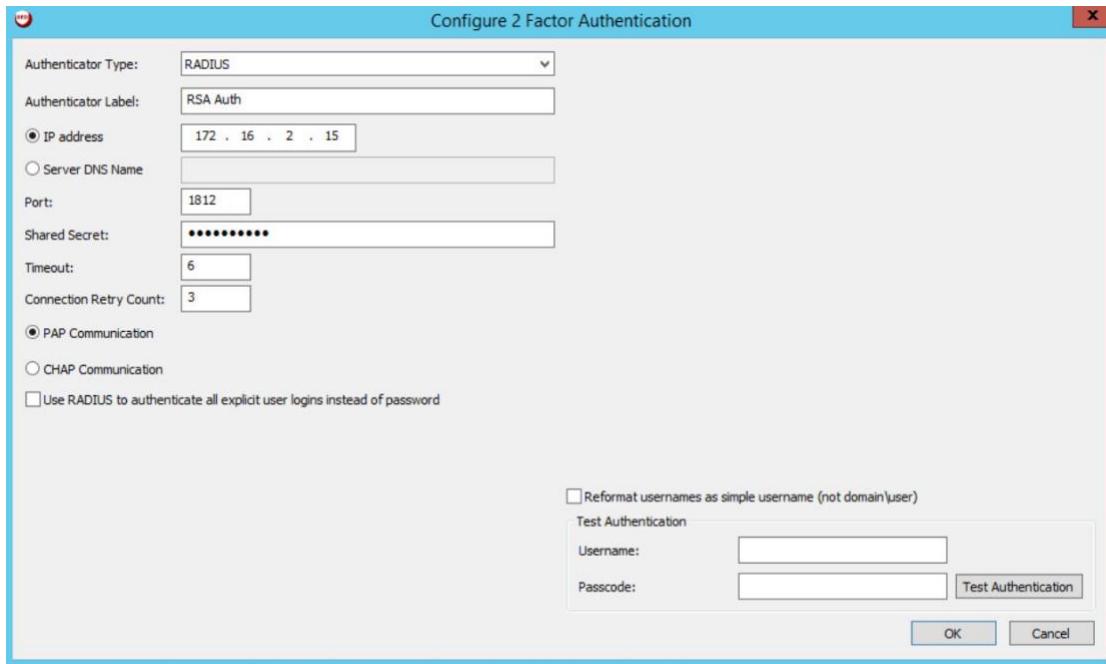


516

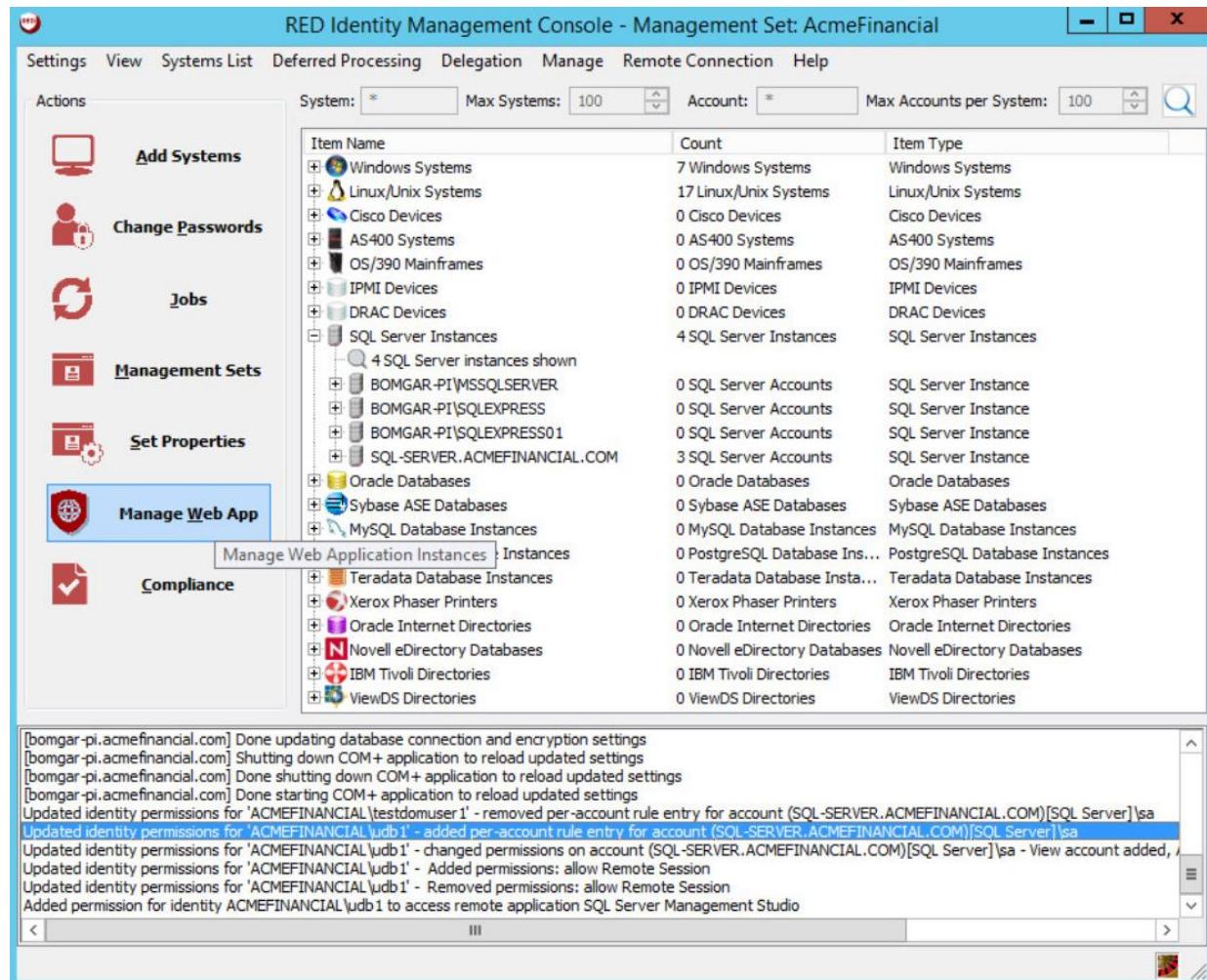
- 517 2. Fill out the **Configure 2 Factor Authentication** window with the following settings:

- 518 a. **Authenticator Type:** RADIUS
- 519 b. **Authenticator Label:** RSA Auth
- 520 c. **IP address:** 172.16.2.15 (the IP address of the RSA Authentication Manager)

- 521 d. **Port:** 1812
- 522 e. **Shared Secret:** <the shared secret from RSA for RADIUS clients>
- 523 f. **Timeout:** 6
- 524 g. **Connection Retry Count:** 3
- 525 h. **PAP Communication:** This check box should be selected.

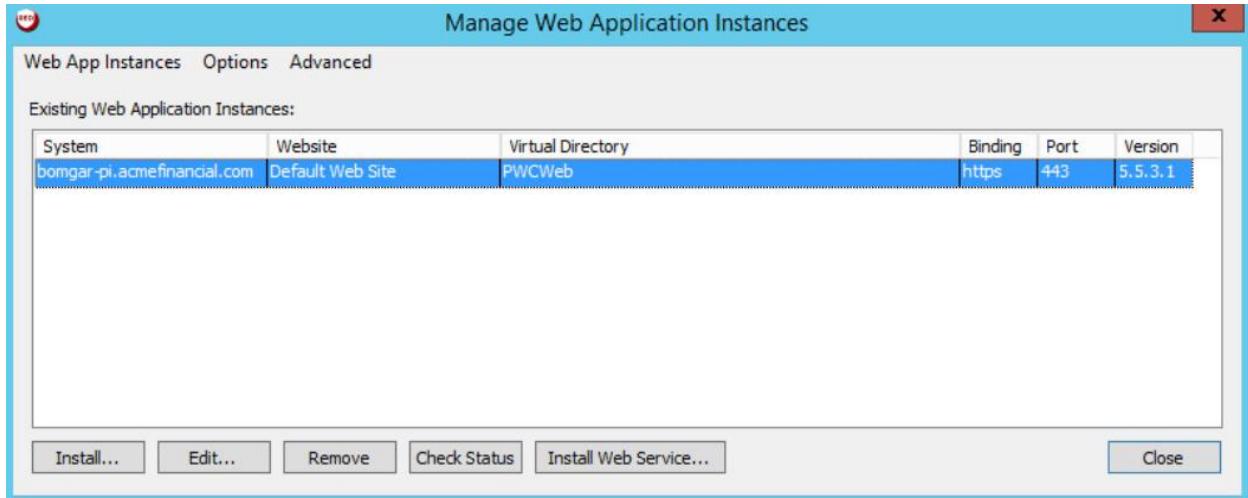


- 526
- 527 3. Click **OK**.
- 528 4. Click **Manage Web App**.

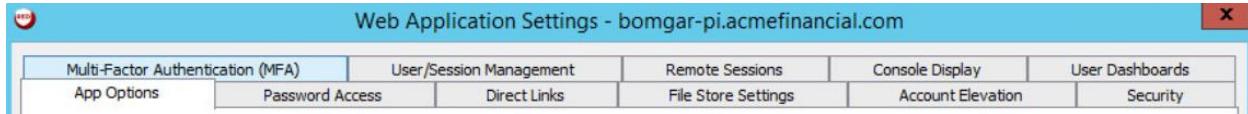


529

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

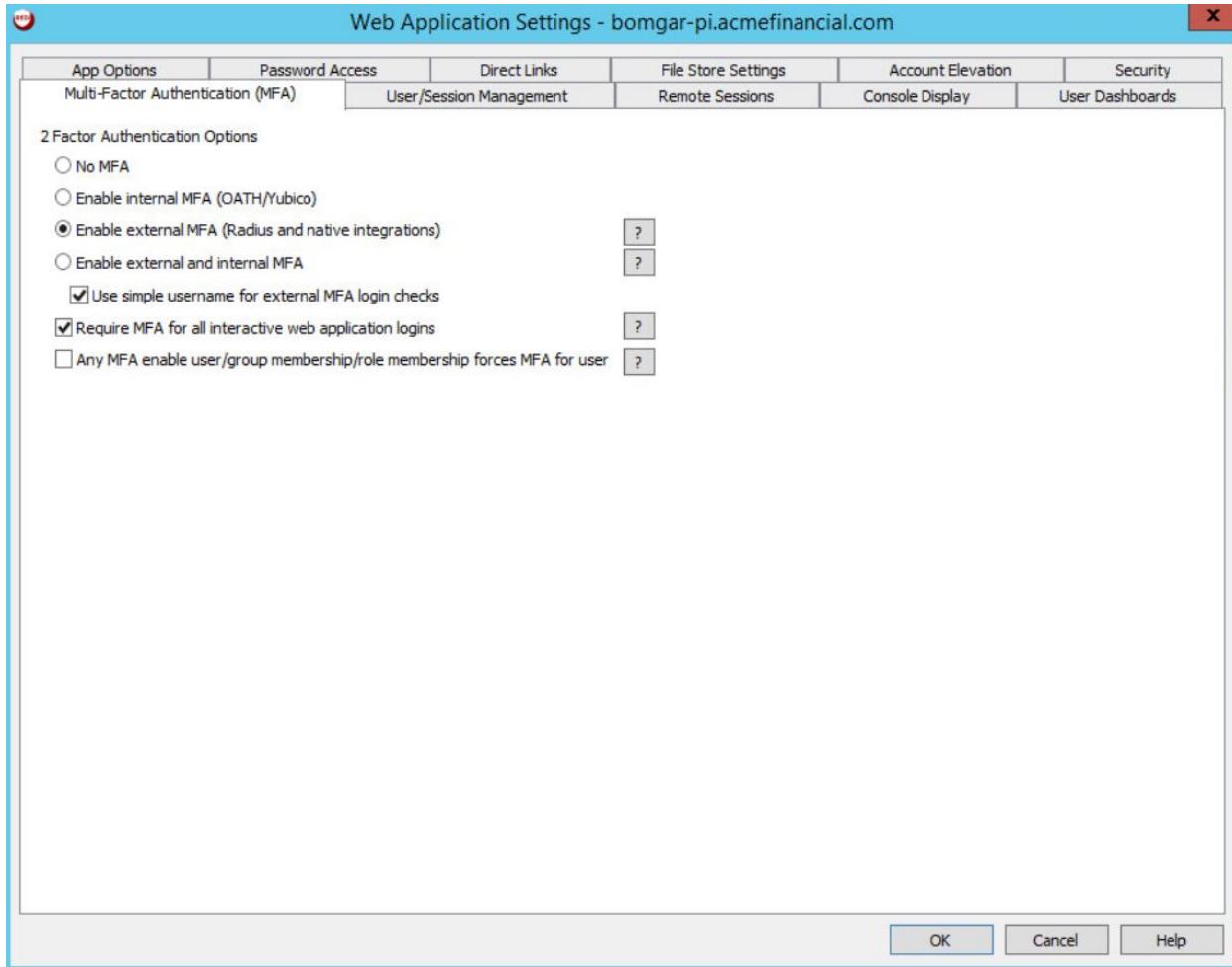


531

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 external MFA login checks**, and **Require MFA for all interactive web application logins**.



537

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

539 10. Click **Close**.

2.2.11 Splunk Universal Forwarder

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

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



The screenshot shows a Windows Notepad window titled "inputs.conf - Notepad". The window contains the following configuration file:

```
[default]
host = Bomgar-PI
index = demo

[monitor://C:\Users\redidmgr\Desktop\UsageLog.txt]
sourcetype = _json
```

545

546 **2.3 TDi ConsoleWorks**

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

549 **2.3.1 How It's Used**

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

552 **2.3.2 Virtual Machine Configuration**

553 The TDi ConsoleWorks virtual machine is configured as follows:

- 554 ■ CentOS 7
- 555 ■ 2 CPU cores
- 556 ■ 8 GB of RAM
- 557 ■ 75 GB of storage
- 558 ■ 1 NIC

559 **Network Interface Configuration:**

- 560 ■ IPv4: manual
- 561 ■ IPv6: disabled
- 562 ■ IPv4 address: 172.16.4.11
- 563 ■ Netmask: 255.255.225.0

- 564 ■ Gateway: 172.16.4.1
565 ■ DNS servers: 172.16.3.10
566 ■ DNS-search domain: N/A

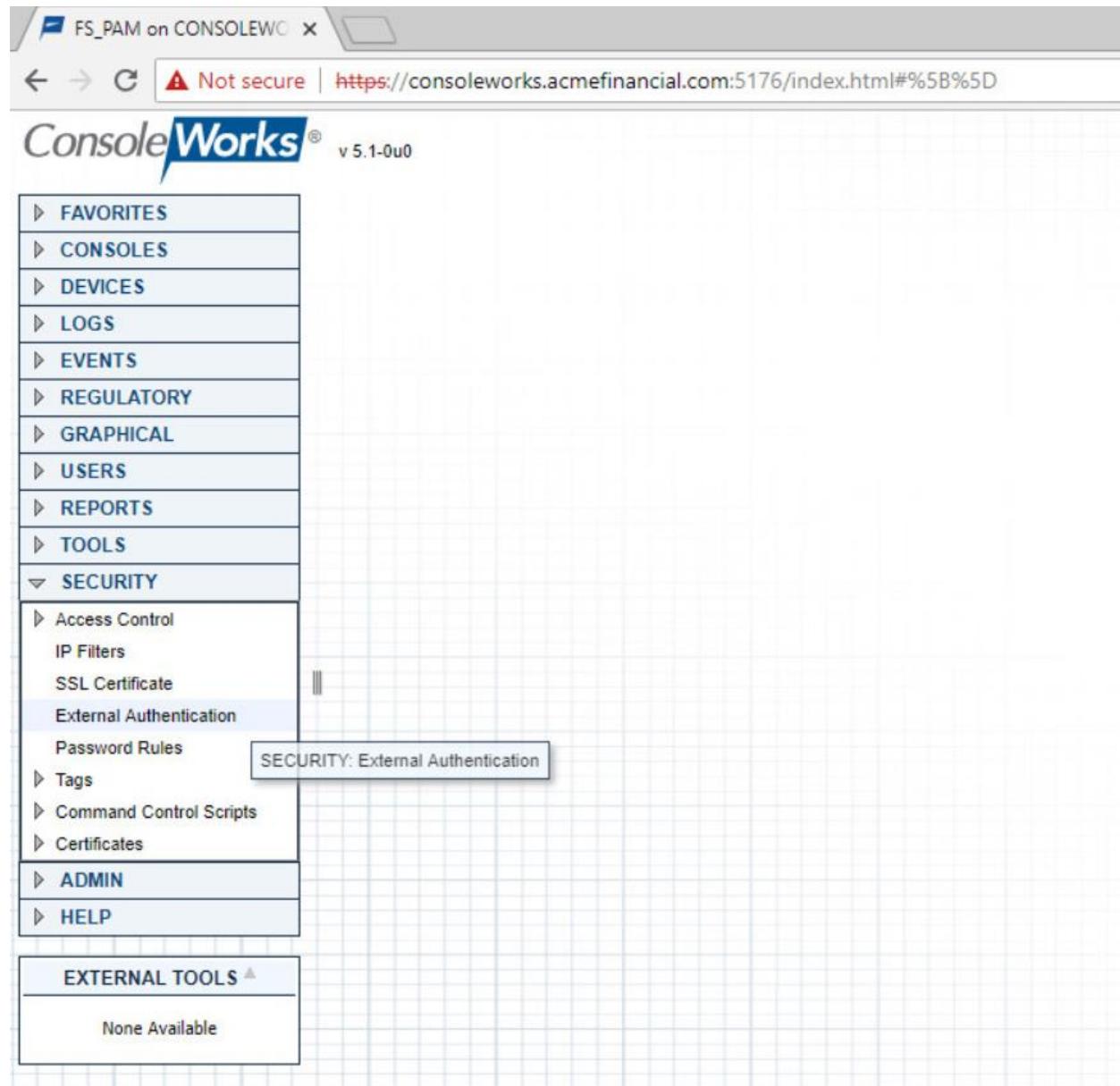
567 2.3.3 Installation

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

570 2.3.4 Configuration of Back-End Authentication

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

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



575

576 3. Click **Add**.577 4. Fill out the **External Authentication Record** with the following information for the IDENTIKEY
578 Authentication Server:579 a. **Record Name:** IDENTIKEY580 b. **Enabled:** This check box should be selected.

581 c. **Library:** radius

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

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

External Authentication Record

Record Name: IDENTIKEY

Enabled

Library: radius

Parameter 1: 172.16.2.208:1812/fspam

Parameter 2:

Parameter 3:

Parameter 4:

Parameter 5:

Parameter 6:

Required Profile:

Cancel Next

586

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

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

External Authentication Record

Verification Passed

User Is Denied

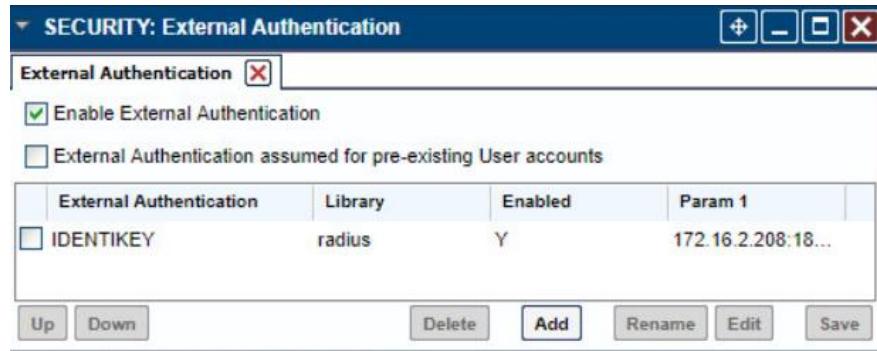
Flags: :

Cancel Prev Next

589

590 7. Click **Save**.

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



593

594 9. Click **Save** if available.

595 2.3.5 Creating Users

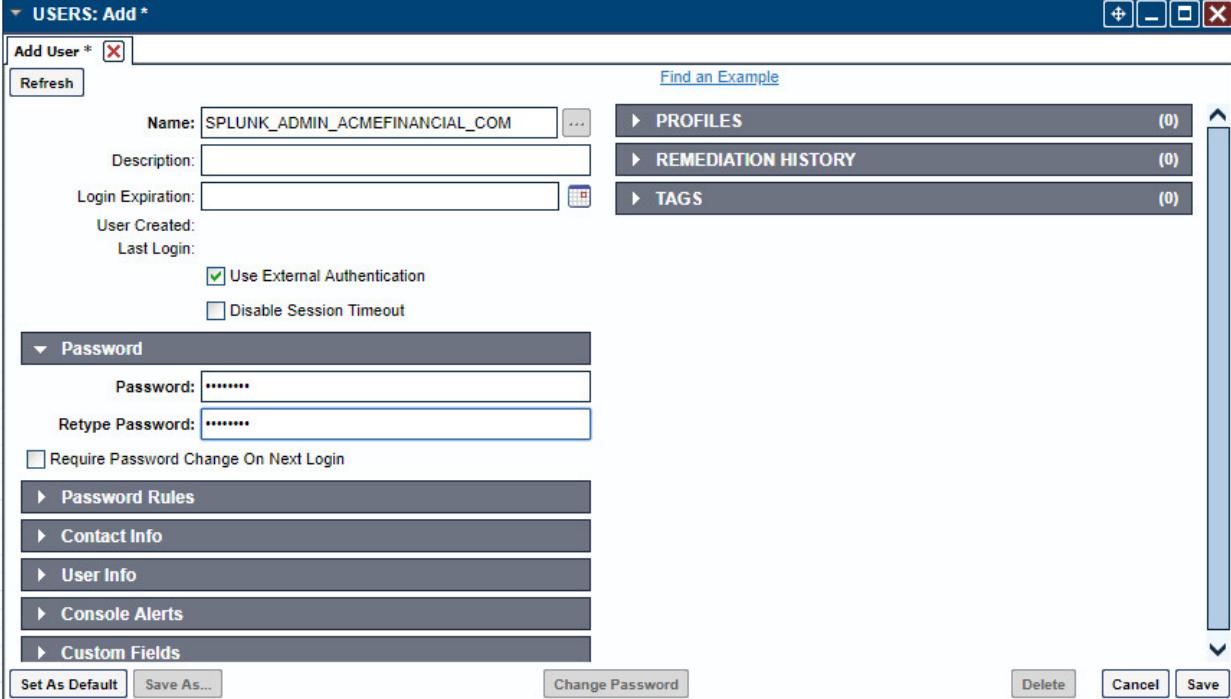
596 Each privileged user must have an account in ConsoleWorks to log into ConsoleWorks. The following
597 steps detail the process of creating accounts for AD users in ConsoleWorks. For this example, we will
598 create a ConsoleWorks account for the splunk_admin@acmefinancial.com AD account. This user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

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



601

- 602 2. Fill out the pop-up window with the following information:
 - 603 a. **Name:** SPLUNK_ADMIN_ACMEFINANCIAL_COM
 - 604 b. **Use External Authentication:** This check box should be selected.
 - 605 c. Enter a dummy password in the **Password** field, and then retype it in the **Retype Password** field.
 - 606 d. **Require Password Change on Next Login:** This check box should not be selected.
- 608 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.
- 611 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**.

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

The screenshot shows the 'CONSOLES: Add*' dialog box. In the 'Connection Details' section, the 'Host IP' is set to 172.16.4.2, 'Port' is 22, 'Username' is root, and 'Password' is fspam@nccoe1. Under the 'Tags' section, there is one tag listed: SPLUNK_OS. The 'Add' button is visible next to the tag input field.

639

- 640 3. Click **Save**.

641 **2.3.8 Creating Web Consoles**

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

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

CONSOLES: Add *

Add Console * X

Refresh Find an Example Logs Events Monitored Events

Name:	PFSENSE	<input type="button" value="..."/>	<input type="button" value=""/>
Nickname:			
Description:	Web Console for pfSense		
Status:	-	Enable	<input type="button" value=""/>
Device:	<input type="button" value=""/>		
Connector:	Web Forward		
Connection Details			
Bind Name:	DEFAULTWEB		
Host Header:	pfSenseweb.acmefinancial.com		
URL:	https://172.16.4.1		
Relative URL:	<input type="button" value="Open"/> <input type="checkbox"/> Disable Standard Translations		
Log Web Traffic:	<input type="button" value=""/>		
Profile:	CONSOLE_MANAGER		

665

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

668 11. Click **Save**.

669 2.3.9 Assigning Tags to Consoles

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

- 672 ▪ pfSense consoles
- 673 ▪ Splunk application-level consoles
- 674 ▪ Splunk OS-level consoles
- 675 ▪ Ekran Server consoles

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

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

679 1. In ConsoleWorks, click **CONSOLES > View**.

680 2. Select a console (e.g., **PFSENSE**).

681 3. Click **Edit**.

682 4. Open the **TAGS** menu, and then click **Add**.

683 5. Move the pfSense consoles' tag to the list on the right, and then click **OK**.

684 6. Click **Save**.

685 2.3.10 Creating Profiles for Users

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

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

690 1. Click **USERS > Profiles > Add**.

691 2. Fill out the **USERS: Profiles: Add** pop-up window with the following information:

692 a. **Name:** SPLUNK_ADMIN

693 b. **Description:** Admins of Splunk's OS

694 3. Under **USERS**, click **Add**.

695 4. Move the **SPLUNK_ADMIN_ACMEFINANCIAL_COM** user to the list on the right, and then click
696 **OK**.

697 5. Click **Save**.

The screenshot shows the 'Users: Profiles: Add' interface. In the top left, there's a 'Find an Example' link. Below it, the 'Name' field contains 'SPLUNK_ADMIN' and the 'Description' field contains 'Admins of Splunk's OS'. On the right, a list titled 'USERS' shows one entry: 'SPLUNK_ADMIN_ACMEFINANCIAL_COM'. There are 'Add', 'Remove', and 'View' buttons next to the list. At the bottom, there are 'Custom Fields' and 'TAGS' sections, both currently empty. The bottom right corner has buttons for 'Delete', 'Cancel', and 'Save'.

698

Set As Default **Save As...****Delete** **Cancel** **Save**

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

2.3.11 Assigning Permissions to Profiles

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

- 705 1. In ConsoleWorks, click **SECURITY > Access Control > Add**.
- 706 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
- 712 3. Open **Profile Selection**, and select the **Simple** tab.
- 713 4. Move the **SPLUNK_ADMIN** profile to the list on the right.
- 714 5. Open **Resource Selection**, and select the **Simple** tab.
- 715 6. Change the drop-down from **Is one of these Consoles** to **Has one of these Tags**.

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

Resource Level:

<input type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Aware
<input type="checkbox"/> Can send break	<input checked="" type="checkbox"/> Connect
<input type="checkbox"/> Controlled Connect	<input type="checkbox"/> Delete
<input type="checkbox"/> Disable	<input type="checkbox"/> Disable Scan
<input checked="" type="checkbox"/> Disconnect	<input type="checkbox"/> Display Hidden
<input type="checkbox"/> Edit	<input type="checkbox"/> Edit Event Occurrence
<input type="checkbox"/> Enable	<input type="checkbox"/> Enable Scan
<input type="checkbox"/> Exclusive Connect	<input type="checkbox"/> Expunge
<input type="checkbox"/> Hide	<input type="checkbox"/> Lock Console
<input type="checkbox"/> Make Comment in Log	<input type="checkbox"/> Modify Log Annotation
<input type="checkbox"/> Monitor	<input type="checkbox"/> Purge
<input type="checkbox"/> Remediate	<input type="checkbox"/> Rename
<input type="checkbox"/> Send Command	<input type="checkbox"/> Send File
<input type="checkbox"/> Send protected characters	<input type="checkbox"/> Trigger Event
<input type="checkbox"/> Update Baseline Run	<input checked="" type="checkbox"/> View
<input type="checkbox"/> View Baseline Run	<input type="checkbox"/> View Event Occurrence
<input type="checkbox"/> View Log	<input type="checkbox"/> View Monitored Events
<input type="checkbox"/> View Usage	

- 723
- 724 9. Click **Save**.

725 **2.4 Ekran System**

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

728 **2.4.1 How It's Used**

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

731 **2.4.2 Virtual Machine Configuration**

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

735 The Ekran System server virtual machine is configured as follows:

- 736 □ Windows Server 2016
- 737 □ 1 CPU core
- 738 □ 8 GB of RAM
- 739 □ 150 GB of storage
- 740 □ 1 NIC

741 **Network Configuration (Interface 1):**

- 742 □ IPv4: manual
- 743 □ IPv6: disabled
- 744 □ IPv4 address: 172.16.1.20
- 745 □ Netmask: 255.255.255.0
- 746 □ Gateway: 172.16.1.1
- 747 □ DNS name servers: 172.16.3.10
- 748 □ DNS-search domains: N/A

749 **2.4.3 Prerequisites**

750 Ekran System requires Microsoft SQL Server, although, in the lab environment, Microsoft SQL Server
751 Express was used. Ekran System also requires IIS to be installed. A full list of requirements can be found
752 on Ekran’s [website](#).

753 **2.4.4 Installing Ekran System**

754 Full installation instructions are available on Ekran’s [website](#).

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

757 **2.5 Radiant Logic**

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

759 **2.5.1 How It's Used**

760 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.

764 **2.5.2 Virtual Machine**

765 The Radiant Logic virtual machine is configured as follows:

- 766 ■ Windows Server 2016
- 767 ■ 3 CPU cores
- 768 ■ 20 GB of RAM
- 769 ■ 120 GB of storage
- 770 ■ 1 NIC

771 **Network Configuration (Interface 1):**

- 772 ■ IPv4: manual
- 773 ■ IPv6: disabled
- 774 ■ IPv4 address: 172.16.3.218
- 775 ■ Netmask: 255.255.255.0
- 776 ■ Gateway: 172.16.1.1
- 777 ■ DNS name servers: 172.16.3.10
- 778 ■ DNS-search domains: N/A

779 **2.5.3 Prerequisites**

780 The minimum system requirements are as follows:

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

- 785
 - Processor speed: 2 gigahertz or higher
- 786
 - Memory: 16 GB minimum. For most production deployments, more than 16 GB of memory is required.
- 788
 - 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.
- 790 ■ Software
 - OS: Windows 2008 R2 Server, Windows Server 2012 R2, Windows Server 2016

792 2.5.4 Installation

793 To install FID, see the documentation provided with the software. The FID installation guide can also be
 794 found on the Radiant Logic support [website](#). A support account is required.

795 2.5.5 Configure FID

796 The steps for configuring FID are as follows:

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

Name	Type	Host	Port	Base DN
active directory	LDAP	172.16.3.10	636	CN=Users,DC=AcmeFinancial,DC=com
replicationjournal	LDAP	RADIANT-LOGIC	2389	
vdsha	LDAP	RADIANT-LOGIC	2389	

- 801

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

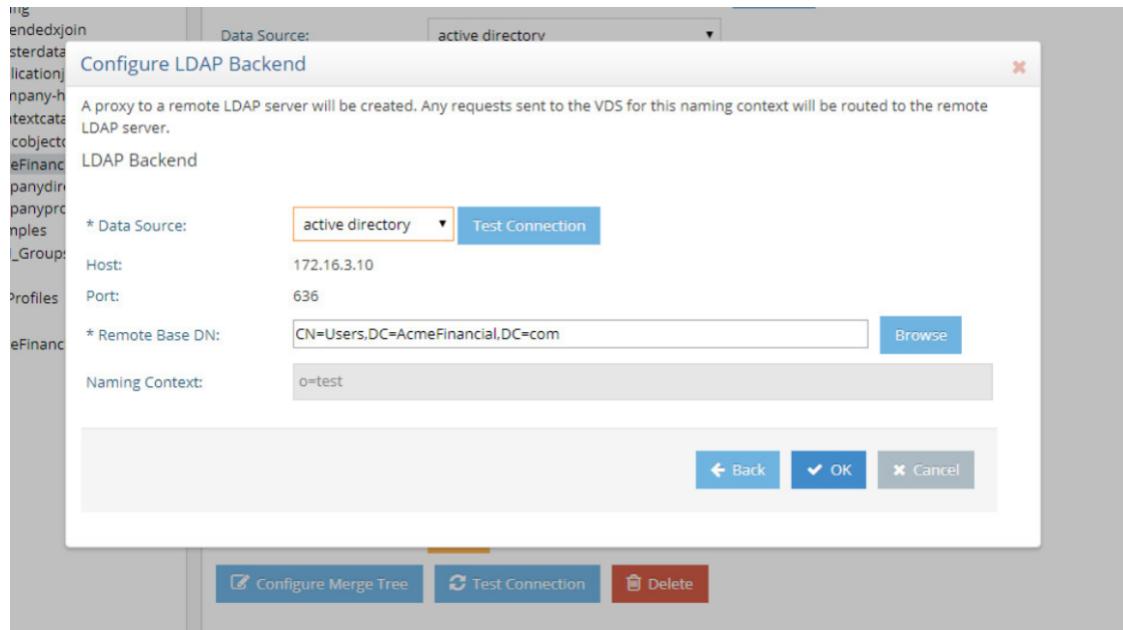
804

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

- 806 a. On the **Directory Namespace** tab, select **New Naming Context** (the plus sign) at the top left of the screen.
- 807
- 808 b. Select the **LDAP Backend** radio button, and enter the naming context, such as o=test. Click **Next**.
- 809

810

- 811 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**.
- 812

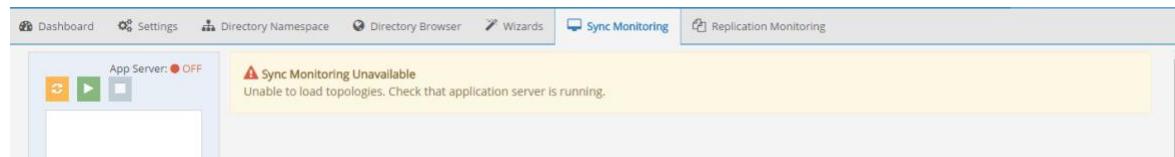


813

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:

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



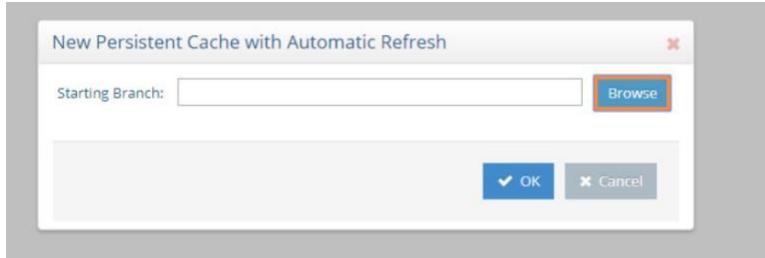
819

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

The screenshot shows the FID interface with the 'Cache' tab selected. On the left, there's a tree view of naming contexts under 'Root Naming Contexts'. A 'Create Persistent Cache' button is visible. The interface includes tabs for Dashboard, Settings, Directory Namespace, Directory Browser, Wizards, Sync Monitoring, Replication Monitoring, and Zookeeper.

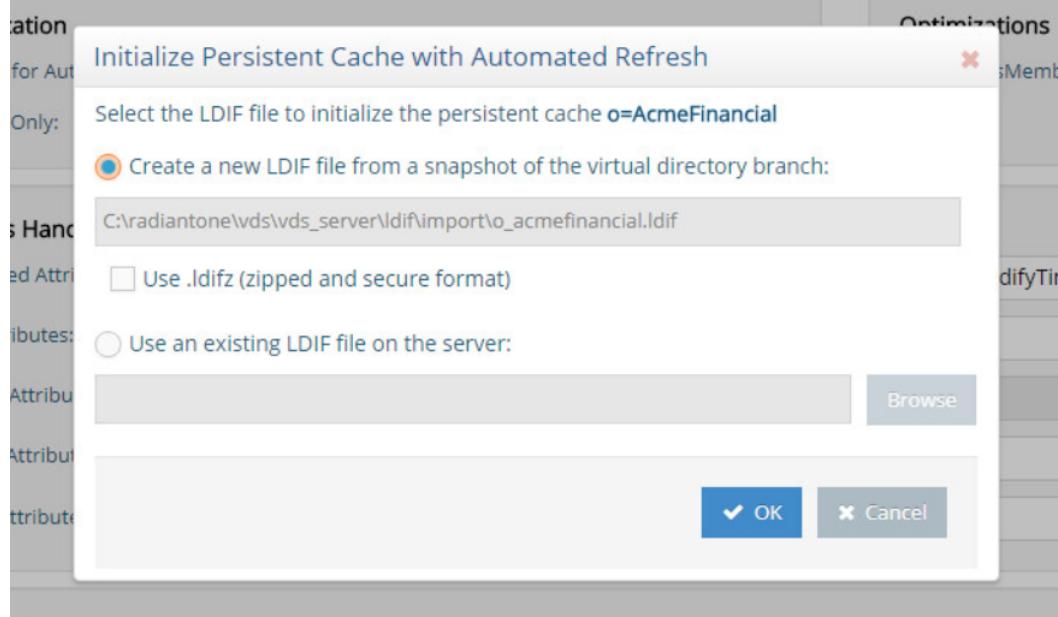
822

- 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.



828

Type: Persistent Cache with Automated Refresh
 Starting Suffix: o=AcmeFinancial
 Internal Suffix: o=AcmeFinancial
 Active:
 Full-text Search:
 Storage Location:
 Authentication
 Use Cache for Authentication:
 Local Bind Only: Delegate on Failure:
 Optimizations
 Optimize isMemberOf:
 Attributes Handling
 Non-indexed Attributes: cacheCreatorsName.cacheCreateTimestamp.cacheModifiersName.cacheModifyTimestamp.vdsSyncState.vdsSyncHist.ds-sync-generation-id.ds-sync-st
 Sorted Attributes:
 Encrypted Attributes:
 Extension Attributes:
 Invariant Attribute:
 Replication
 Inter-cluster Replication: Configure 'Push' Mode
 Accept changes from replicas:
 Updatable Attributes from Replicas:
 Configuration Buttons: Configure, Initialize, Export, Re-build Index, Delete
 Copyright © 2018 Radiant Logic, Inc. All rights reserved.
 Activate Windows
 Go to Settings to activate Windows.

829

- 830 5. Select **Create a new LDIF file from a snapshot of the virtual directory branch**. Click **OK**. This
 831 step may take a few minutes.
- 832 6. Once complete, click **Save**.

833 7. Select the **Connectors** tab.

Connector	Type	Status
from_generic_to_cacherefresh	Transformation	STARTED
o_acmefinancial-generic	Capture [Snapshot]	STARTED
vdsconnector-cacherefresh	Apply [LDAP]	STARTED

834

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

837

838 9. Install Splunk Universal Forwarder to monitor the file at
839 C:\radiantone\vds\r1syncsvcs\log\cf_o_acmefinancial\object_generic_dv_so_o_acmefinancial_c
840 apture.log

841 2.5.7 Configure SSL

842 In this implementation, AD serves as the CA.

843 1. Create the initial FID private key:

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

847 2. Download the certificate from the CA.

- 848 3. Create the certificate signing request:
- 849 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.`
- 852 4. Submit the request to the CA.
- 853 5. Import the trusted CA certificate into the keystore and cacerts database on FID:
- 854 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.`
- 857 b. Run `keytool -import -trustcacerts -file C:\radiantone\vds\vds_server\conf\certca.cer -keystore C:\radiantone\vds\jdk\jre\lib\security\cacerts.`
- 860 6. Import the signed server certificate from the request into FID:
- 861 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.`
- 864 7. Restart FID.
- 865

2.5.8 Splunk Universal Forwarder
- 866 Install Splunk Universal Forwarder by following the instructions provided at <http://docs.splunk.com/Documentation/Forwarder/7.1.3/Forwarder/Abouttheuniversalforwarder>.
- 868 Edit the `inputs.conf` file to monitor the `object_generic_kv_so_o_acmefinancial_capture.txt` file created by Radiant Logic FID and to forward logs to the **demo** index at Splunk Enterprise.



```
[default]
host = RADIANT-LOGIC
index = demo

[monitor://C:\radiantone\vds\r1syncsvcs\log\cf_o_acmefinancial\object_generic_dv_so_o_acmefinancial_capture.log]
```

870

871 2.6 IdRamp

872 2.6.1 How It's Used

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

875 2.6.2 Prerequisites

- 876 ■ premium Azure account
- 877 ■ AD installed

878 2.6.3 Installation

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

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

- 882 2. Enable MFA in Azure for certain privileged users:

- 883 a. In the Azure AD admin center at <https://aad.portal.azure.com>, click **Azure Active Directory**.
- 885 b. Click **SECURITY > Conditional access**.
- 886 c. Click **New policy**.

- 887 d. Give the policy a name, such as Privileged 2FA.
- 888 e. Click **Users and groups**. Under **Include**, click **users and groups**, and select **Users and**
889 **groups** check box.
- 890 f. Click the region labeled as **Select**.
- 891 g. Select the privileged users from the list.
- 892 h. Once all of those users are selected, click **Done**.
- 893 i. Click **Cloud apps**, and then select **All cloud apps**. Click **Done**.
- 894 j. Under **Access Controls**, click **Grant**.
- 895 k. Make sure that the **Grant access** check box is selected, and select the check box labeled
896 as **Require multi-factor authentication**.
- 897 l. Click **Select**.
- 898 m. Click **On** under **Enable policy**, and then click **Create**.
- 899 3. Disable logins of all other accounts:
- 900 a. For each user that you do not want to allow to sign in with Azure AD at all, click their
901 user account under **All users** in the Azure AD admin center.
- 902 b. Click **Yes** next to **Block sign in**.
- 903 4. Configure sign-in to block incoming requests, except from your organization's network:
- 904 a. Under **SECURITY > Conditional access** in the Azure AD admin center, select **Named**
905 **locations**.
- 906 b. Click **New location**, and then give the location a name.
- 907 c. Select the check box labeled as **Mark as trusted location**.
- 908 d. Enter the IP range of the network to which you want to restrict access.
- 909 e. Click **Create**.
- 910 f. Complete steps 2a–2c above.
- 911 g. Give the policy a name, such as Block Remote Access.
- 912 h. For users of this policy, select the privileged users.
- 913 i. Select all cloud apps for the **Cloud apps assignment**.

- 914 j. Under **Conditions**, select **Locations**.
- 915 k. Select **Yes** under **Configure**, and select **Any location** under **Include**.
- 916 l. Click **Exclude**, and then click **Select**.
- 917 m. Select the **Named location** that we just created, and then click **Select**.
- 918 n. Click **Done**.
- 919 o. Click **Grant** under **Access controls**, and then click **Block access**.
- 920 p. Click **Select**.
- 921 q. Click **On** under **Enable policy**, and then click **Create**.

922 2.7 OneSpan IDENTIKEY Authentication Server

923 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
924 their two-factor token, and it can be hardware-based or software-based.

926 2.7.1 How It's Used

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

931 2.7.2 Virtual Machine Configuration

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

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

934 2.7.3 Prerequisites

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

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

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

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

939 **2.7.4 Installation**

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

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

```
942        mkdir /mnt/dvd  
943        mount /dev/dvd /mnt/dvd
```

- 944 2. Run the installation script:

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

- 947 3. Begin following the installation wizard, and choose basic installation.

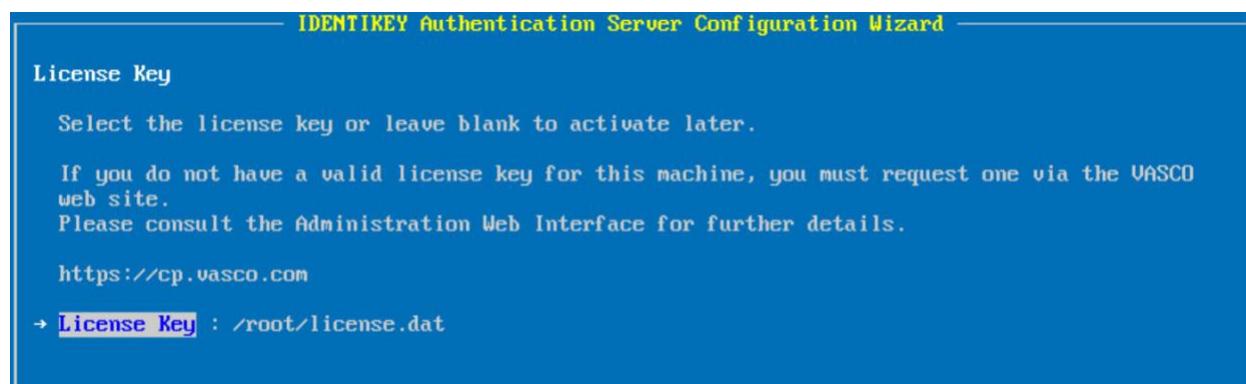
- 948 4. Accept the licenses.

- 949 5. Select **Yes** to encrypt the embedded database.

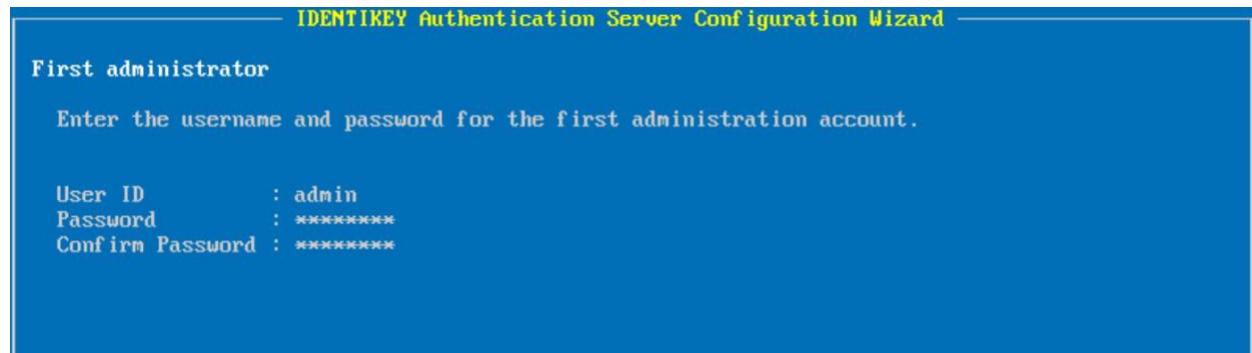
950 **2.7.5 Configuration**

951 After completing the installation, configuration happens immediately:

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

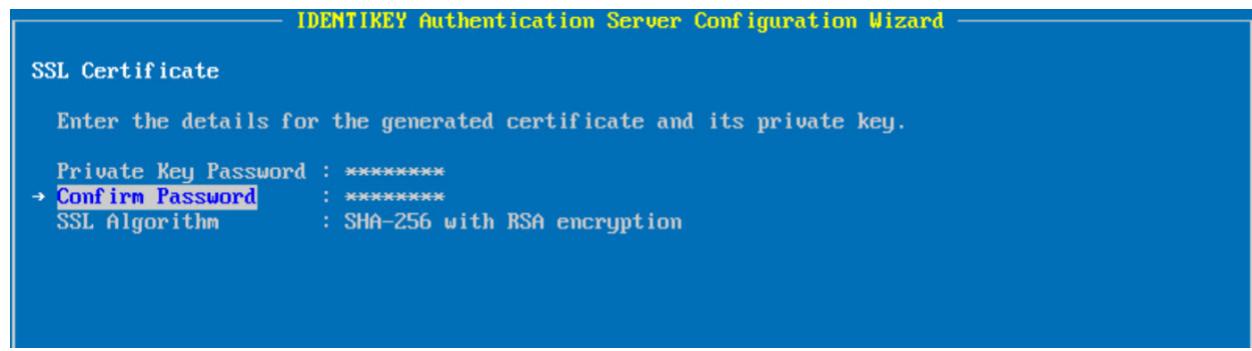


- 955
- 956 4. Accept the server functionality, and then select **Next**.
- 957 5. Create a username and password for the first admin account, and then select **Next**.



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.

```
IDENTIKEY Authentication Server Configuration Wizard

Summary

Perform initialisation: Done.
Parse dpadmincmd dpadmincmd_seal.tpl template file: Done.
Update dpadmincmd configuration file: * Update Admincmd server address: Done.
Update MDC server configuration: Done.
Parse reports template file: Done.
Parse reports template file: Done.
Parse reports template file: Done.
Process SOAP Communicator SSL certificate: Done.
Process SEAL Communicator SSL certificate: Done.
Process RADIUS Communicator SSL certificate: Done.
Process MDC Server SSL certificate: Done.
Process Live Audit SSL certificate: Done.
Write IDENTIKEY Authentication Server configuration file: Done.
Write data to ODBC datastore: Done.
The configuration of NetSNMP finished successfully.
Update Message Delivery Component configuration file: Done.
Starting the IDENTIKEY Authentication Server service: Done.
Starting the Message Delivery Component service: Done.

Configuration Wizard completed all actions successfully.
```

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**.

Welcome to the IDENTIKEY Authentication Server Web Administration
admin

Users

To manage an individual user account, type the userid in the search box.
To manage bulk users, make a selection from the users menu above.

IDENTIKEY Authentication Server status

You are logged in to IDENTIKEY Authentication Server 172.16.2.208. [► Check server info](#)
There is no record of a previous administrative logon from this account.
You are using IDENTIKEY Authentication Server Web Administration on server VASCO. [► Check version info](#)
This IDENTIKEY Authentication server is running an evaluation license. [► Obtain a permanent license](#)

TOP TASKS

- Register client
- Define policy
- Import users
- Create user
- Assign DP
- Move user

NEED HELP?

Click the help link at the top right of any page if you need help with the current task.

- Getting started

976

[About IDENTIKEY Authentication Server | vasco.com](#)

977

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

The screenshot shows the IDENTIKEY Authorization Server interface. At the top, there is a navigation bar with tabs: HOME, USERS, DIGIPASS, POLICIES, CLIENTS, BACK-END, ORGANIZATION, REPORTS, SERVERS, and SYSTEM. The 'ORGANIZATION' tab is currently selected. Below the navigation bar is a search bar with the text 'FIND' and a dropdown menu set to 'Users'. There are also buttons for 'DIGIPASS' and 'SEARCH'. The main content area has a title 'Create new Domain'. A sub-instruction reads: 'Create a domain by completing the details below. * indicates mandatory fields.' There are two input fields: 'Domain Name *' containing 'acmefinancial.com' and 'Description' which is empty. At the bottom are two buttons: 'CREATE' (blue) and 'CANCEL' (grey).

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 **Identikit Back-End Authentication**. Click **CREATE**.
- 981

Create a policy by completing the details below. * indicates mandatory fields.

Policy ID * ACME_2FA

Description 2-Factor Authentication
Local Digipass
Back-end Active Directory

Inherits From Identify Back-End Authentication

CREATE **CANCEL**

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 **Microsoft Active Directory** for **Back-End Protocol**. Click **SAVE**.

Manage policy: ACME_2FA
Click on the tabs to view or change policy settings.

Policy	User	DIGIPASS	Challenge	Secure Channel	Virtual DIGIPASS	Push Notification	DP Control Parameters	Offline Authen
Edit Policy Settings								
<i>Current Effective Settings</i>								
Description	2-Factor Authentication Local Digipass Back-end Active Directory							
Local/Back-End Authentication								
Local Authentication	Digipass Only	(None)						
Back-End Authentication	Always	(Always)						
Back-End Protocol	Microsoft Active Directory							
(RADIUS)								
SAVE CANCEL								

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**.

Manage client: RADIUS Client
Click on the tabs to view or change client settings.

Client RADIUS

Edit Client Settings

Enabled

Protocol ID RADIUS

Policy ID

ACME_2FA
Base Policy
IDENTIKEY Administration for Multi-Device Activation
IDENTIKEY Authentication with Secure Channel
IDENTIKEY Local Authentication with Auto-Unlock

SAVE CANCEL

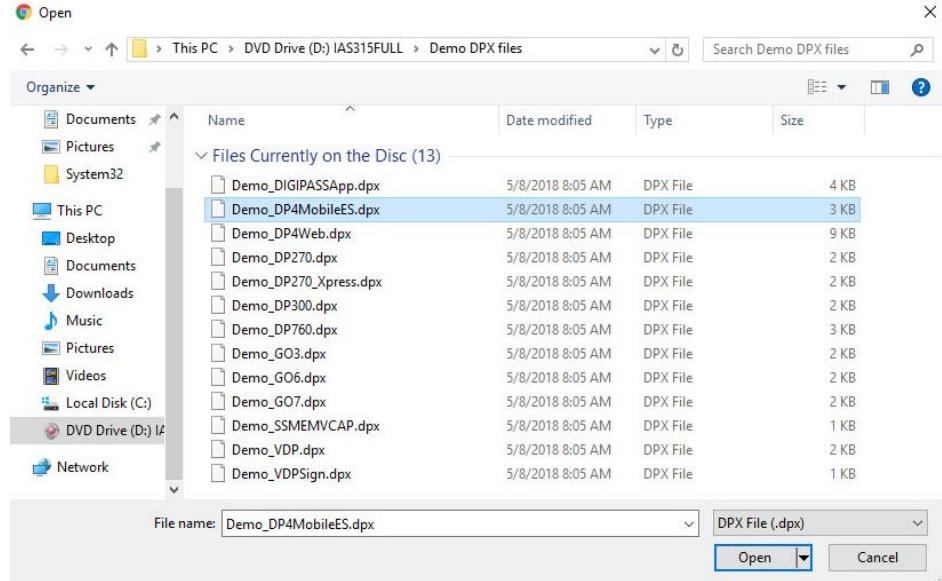
990

2.7.7 Importing DIGIPASSes

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

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

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



997

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

1000

1000 4. Click **UPLOAD**.

1001

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

1002
1003

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

1004

1004 7. Click **IMPORT**.

1005

1005 8. Choose to run the task immediately.

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

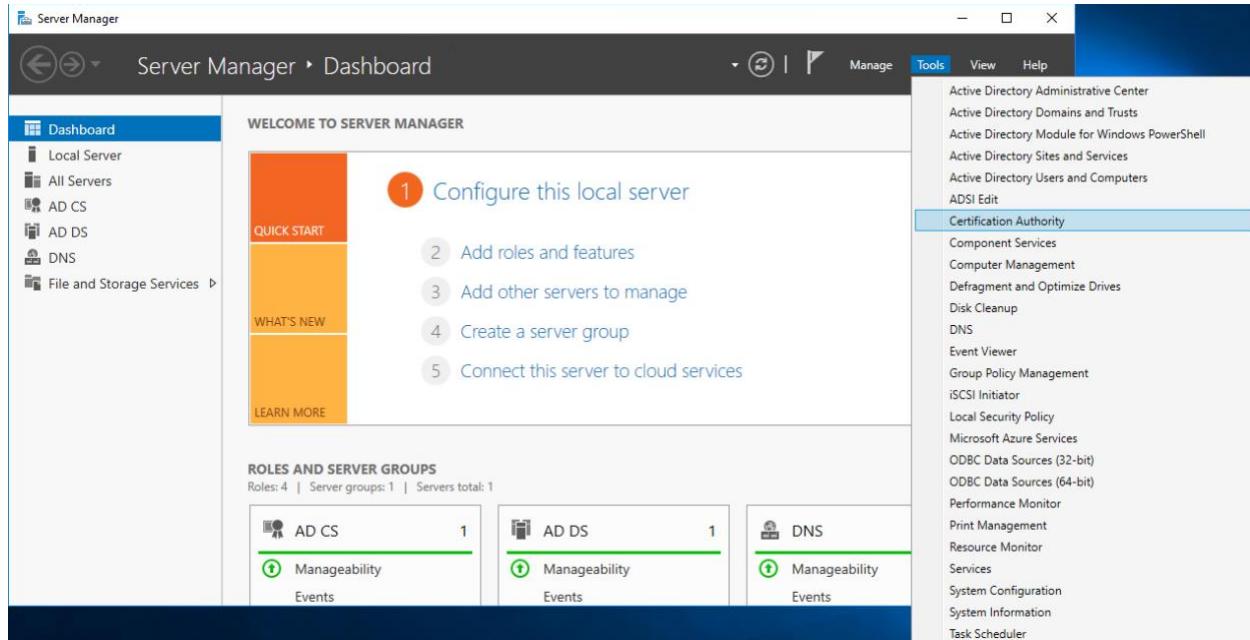
1007 With Radiant Logic configured to replicate users and groups from AD, OneSpan can use Radiant Logic as
 1008 an AD back-end. This works, as OneSpan connects to Radiant by using LDAP over SSL, and Radiant Logic
 1009 contains a virtual directory that presents like AD.

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:

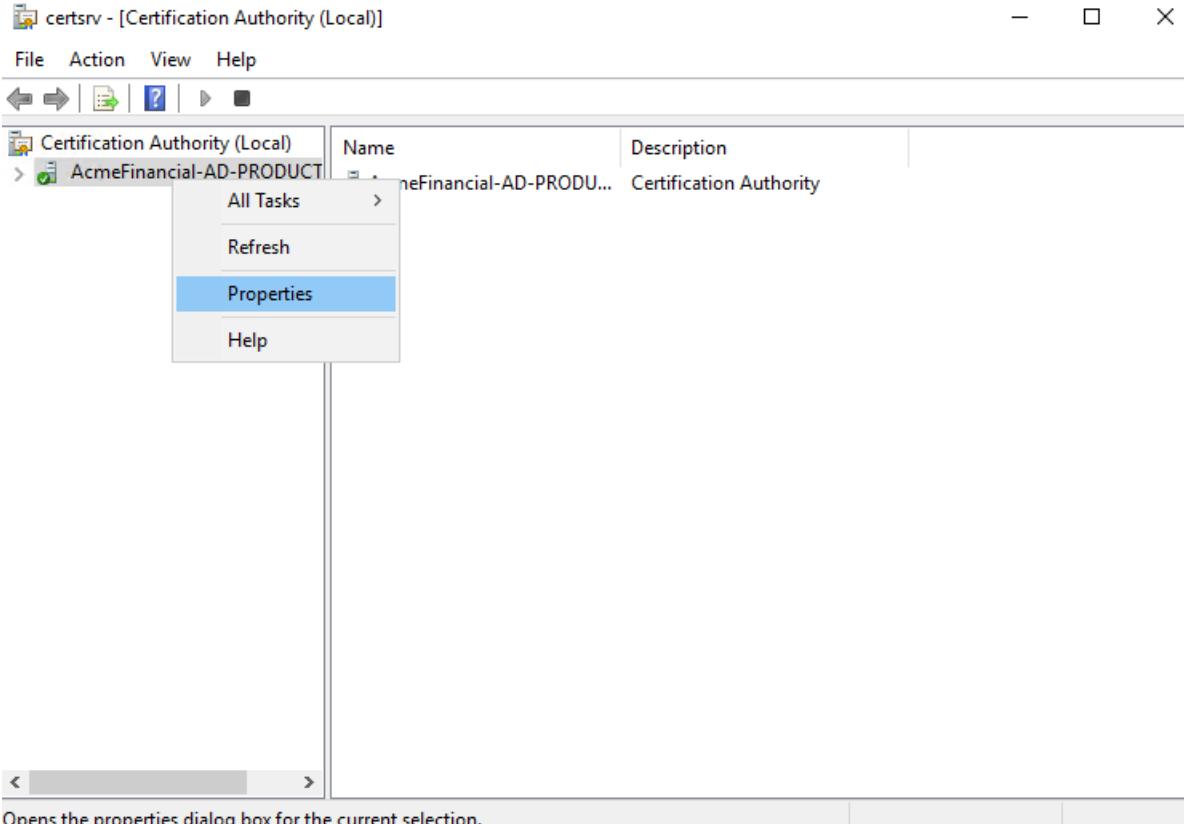
1015 1. On AD-PRODUCTION, the AD Domain Controller, open **Server Manager**.

- 1016 2. In the top right corner, click **Tools > Certification Authority**.



1017

- 1018 3. Under **Certification Authority (Local)**, right-click **AcmeFinancial-AD-PRODUCTION-CA**, and then
1019 select **Properties**.



1020

Opens the properties dialog box for the current selection.

1021

4. Click **Certificate #0**, and then click **View Certificate**.

1022

5. Tab over to **Details**, and then click **Copy to File**.

1023

6. Click **Next**.

1024

7. Select the format option **Base-64 encoded X.509 (.CER)**, and then click **Next**.

1025

8. Select a location and file name for saving the certificate. For example,

1026

C:\Users\Administrator\Desktop\AD-PRODUCTION-CA-PEM.cer.

1027

9. Click **Next**, and then click **Finish**.

1028

10. Copy the file over to the OneSpan server.

1029

11. On the OneSpan server, copy the file to the */usr/local/share/ca-certificates* directory, and give it a *.crt* file extension.

1031

12. Update the trusted CA certificates with the following command:

1032

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

1033 13. Reboot the OneSpan server machine.

1034 *2.7.8.2 Configuring OneSpan to Use Radiant Logic*

1035 Once the certificate for Radiant Logic will be trusted, the final step (before OneSpan will authenticate
1036 with Radiant Logic as a back-end) is to add a back-end server entry in OneSpan. The following procedure
1037 completes this step:

1038 1. In the **IAS Web Administration** interface, click **BACK-END > Register Active Directory Back-End**.

1039 2. Fill out the pop-up window with the following information:

1040 a. **Back-End Server ID:** RADIANT LOGIC

1041 b. **Domain Name:** acmefinancial.com

1042 c. **Enable SSL:** This check box should be selected.

1043 d. **Location:** radiant-logic

1044 e. **Port:** 636

1045 f. **Search Base DN:** o=AcmeFinancial

1046 g. **Security Principal DN:** cn=Directory Manager

1047 h. **Security Principle Password:** <the Security Principal Password from Radiant Logic>

1048 i. **Confirm Principle Password:** <the Security Principal Password from Radiant Logic>

Create new Microsoft Active Directory Back-End Server

Create a Microsoft Active Directory Back-End server by completing the details below. * indicates mandatory fields.

Back-End Server ID *	RADIANT LOGIC
Domain Name	acmefinancial.com
Priority	
Enable SSL	<input checked="" type="checkbox"/>
Location	radiant-logic
Port	636
Timeout (seconds)	
Search Base DN	o=AcmeFinancial
Security Principal DN	cn=Directory Manager
Security Principal Password	*****
Confirm Principal Password	*****

1049

1050 3. Click **CREATE**.1051 **2.7.9 Integration with TDi ConsoleWorks**1052 Integrating TDi ConsoleWorks with OneSpan required disabling the NAS-IP-Address RADIUS attribute.
1053 Instructions for completing this step are available [online](#) from OneSpan.1054 **2.7.10 Installing User Websites**1055 To allow users to register their own DIGIPASS device without the need of an admin being present, User
1056 Websites must be installed and then configured with a corresponding license. The following steps detail
1057 how to install the User Websites on the same server as the Authentication Server:

1058 1. Mount the .iso file with the server installer:

1059

```
mkdir /mnt/dvd
```

1060

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

1061 2. Run the installation script:

1062

```
cd /mnt/dvd/IDENTIKEY\ User\ Websites\
```

1063

```
sudo ./install-uws.sh
```

1064 3. Accept the licenses for the server.

1065 2.7.11 Creating Component Records in IDENTIKEY Authentication Server

1066 Before User Websites can be used to assign a user a DIGIPASS, the IDENTIKEY Authentication Server
1067 must be configured to accept connections from the User Websites. We will create two component
1068 records for the websites: one general User Websites client record and another UWS MDL Provisioning
1069 client record for provisioning DIGIPASSes.

1070 1. In IAS Web Administration, click **CLIENTS > Register**.

1071 2. Fill out the **Create new Client** page with the following information:

1072 a. **Client Type: IDENTIKEY User Websites**

1073 b. **Location: 172.16.2.208**

1074 c. **Policy ID: IDENTIKEY Provisioning for Multi-Device Licensing**

Create new Client

Create a client by completing the details below. * indicates mandatory fields.

Client Type *	IDENTIKEY User Websites
Location *	172.16.2.208
Policy ID *	IDENTIKEY Local Authentication with Auto-Unlock IDENTIKEY Provisioning for Multi-Device Licensing IDENTIKEY Signature Validation with Secure Channel Identikit Administration Logon Identikit Back-End Authentication
Protocol ID	SOAP
Shared Secret	
Confirm Shared Secret	
Character Encoding	
Enabled	<input checked="" type="checkbox"/>

CREATE **CANCEL**

1075

1076 3. Click **CREATE**.

- 1077 4. Click **Click here to manage IDENTIKEY User Websites.**
- 1078 5. Tab over to **License**.
- 1079 6. Click **LOAD LICENSE KEY**.
- 1080 7. Click **Choose File**, and then provide it with the User Websites license.
- 1081 8. Click **FINISH**.
- 1082 9. Click **CLIENTS > Register** again.
- 1083 10. Fill out the **Create new Client** page with the following information:
- 1084 a. **Client Type:** UWS MDL Provisioning (type it in)
- 1085 b. **Location:** 172.16.2.208
- 1086 c. **Policy ID: IDENTIKEY Provisioning for Multi-Device Licensing**

Create new Client

Create a client by completing the details below. * indicates mandatory fields.

Client Type *	<input type="text" value="UWS MDL Provisioning"/>
Location *	<input type="text" value="172.16.2.208"/>
Policy ID *	<input type="text" value="IDENTIKEY Provisioning for Multi-Device Licensing"/> IDENTIKEY Signature Validation with Secure Channel Identikit Administration Logon Identikit Back-End Authentication Identikit DP110 Authentication
Protocol ID	<input type="text" value="SOAP"/>
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Character Encoding	<input type="text"/>
Enabled	<input checked="" type="checkbox"/>
CREATE CANCEL	

- 1087
- 1088 11. Click **CREATE**.

- 1089 12. Click **POLICIES > List**.
- 1090 13. Find the policy **IDENTIKEY Provisioning for Multi-Device Licensing**, and then click it.
- 1091 14. Click **EDIT**.
- 1092 15. Change the **Back-End Protocol** from **RADIUS** to **Microsoft AD**.
- 1093 16. Click **SAVE**.
- 1094 17. Tab over to **User**.
- 1095 18. Click **EDIT**, and change **Dynamic User Registration** to **No**. This way, only users added by admins
1096 in IDENTIKEY Authentication Server will be assigned DIGIPASSes.
- 1097 19. Click **SAVE**.
- 1098 Users are now able to go to <https://vasco.acmefinancial.com:9443/selfmgmt> to assign themselves
1099 DIGIPASSes. Details about and instructions for using the DIGIPASS application are available from
1100 OneSpan.

1101 **2.8 Base Linux OS**

1102 The base Linux image used in this project is an Ubuntu 16.04 Server OS. It is open-source and freely
1103 available.

1104 **2.8.1 Virtual Machine Configuration**

1105 The base Linux virtual machine is configured as follows:

- 1106 ▪ Ubuntu Linux 16.04 LTS
- 1107 ▪ 1 CPU core
- 1108 ▪ 8 GB of RAM
- 1109 ▪ 40 GB of storage
- 1110 ▪ 1 NIC

1111 **Network Configuration:**

- 1112 ▪ IPv4: manual
- 1113 ▪ IPv6: disabled
- 1114 ▪ IPv4 address: 172.16.x.x
- 1115 ▪ Netmask: 255.255.255.0
- 1116 ▪ Gateway: 172.16.x.1

- 1117 ▪ DNS name servers: 172.16.3.10
 1118 ▪ DNS-search domain: acmefinancial.com

1119 **2.8.2 Domain Join Configuration**

1120 The base system used was configured to be a part of the project's AD domain, as demonstrated by the
 1121 following steps:

- 1122 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
```

- 1123
 1124 2. Restart the networking by entering the following command:
 1125 **systemctl restart networking**
 1126 3. Verify changes by checking the */etc/resolv.conf* file. Enter the following command:
 1127 **cat /etc/resolv.conf**
 1128 4. Install the packages required for the AD domain join as described above, using the following
 1129 command:

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

- 1130
 1131 5. If prompted to enter your Kerberos 5 realm name, enter your domain name in capital letters.
 1132 The Kerberos 5 default realm is **ACMEFINANCIAL.COM**.

1133 6. Install the chrony ntp client by entering the following command:

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

1134

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

1136 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.
```

1137

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:

1112

3. Limitación administrativa y acuerdo financiero. COM

1142

b. Enter the password when prompted.

1144

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

1146

d `systemctl restart realmd`

1147
1148

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
realm_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

```

1149

2.9 Microsoft SQL Server Installation on Ubuntu Linux

1151 Microsoft SQL Server is a relational database management system developed and provided by the
 1152 Microsoft Corporation. Microsoft SQL Server has different editions that target different audiences. The
 1153 Express edition, which is freely available, was used in this build.

2.9.1 How It's Used

1155 Microsoft SQL Server is used in the example implementation as a managed asset. It represents a critical
 1156 asset that would naturally exist in most enterprises. Access to the server by privileged users is controlled
 1157 by the policies configured on the PAM system.

2.9.2 Virtual Machine Configuration

1159 The Microsoft SQL Server virtual machine is configured as follows:

- 1160 ■ Ubuntu Linux 16.04 LTS
- 1161 ■ 1 CPU core
- 1162 ■ 4 GB of RAM
- 1163 ■ 40 GB of storage
- 1164 ■ 1 NIC

1165 Network Configuration:

- 1166 ■ IPv4: manual
- 1167 ■ IPv6: disabled

- 1168 ■ IPv4 address: 172.16.3.12
1169 ■ Netmask: 255.255.255.0
1170 ■ Gateway: 172.16.3.1
1171 ■ DNS name servers: 172.16.3.10
1172 ■ DNS-search domain: acmefinancial.com

1173 2.9.3 Firewall Configuration

1174 `ufw allow 1433/tcp`
1175 `ufw allow 22/tcp`
1176 `ufw default deny incoming`

1177 2.9.4 Installation and Initial Configuration

1178 Use the following steps to install Microsoft SQL Server Express 2017 and to configure it to authenticate
1179 to AD:

- 1180 1. Install Microsoft SQL Server on Ubuntu Linux by using the instructions provided at
1181 <https://docs.microsoft.com/en-us/sql/linux/quickstart-install-connect-ubuntu?view=sql-server-linux-2017>.
- 1183 2. Create a service account by entering the following Powershell command:

1184 `New-ADUser mssql -AccountPassword (Read_host -AsSecureString "Enter password")`
1185 `-PasswordNeverExpires $true -Enabled $true.`

1186 a. Enter the password when prompted.
- 1187 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**.

Policy	Policy Setting
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	ACMEFINANCIAL\dbserver1svc...
Log on as a service	ACMEFINANCIAL\dbserver1svc...
Manage auditing and security log	Not Defined

1190 4. Create a Service Principal Name by entering the following command:

1191 setspn -A MSSQLSvc/sql-server.acmefinancial.com:1433 mssql

1192 5. Request the information needed to create a keytab file by entering the following commands:

1193 a. Enter the following command:

1194 kinit mssql@ACMEFINANCIAL.COM

1195 i. Enter the account password when prompted.

1196 b. Retrieve the kvno value by entering the following command:

1197 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
```

1198 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
```

1199 7. Exit the ktutil tool by entering the following command:

1200 quit

1204 8. Restart SQL Server by entering the following command:

1205 systemctl restart mssql-server

1206 9. Install SQL Server command-line tools by using the instructions provided at

1207 <https://docs.microsoft.com/en-us/sql/linux/quickstart-install-connect-ubuntu?view=sql-server-linux-2017#tools>.

1209 10. Log into the database by entering the following command:

1210 ./sqlcmd -S localhost -U sa

1211 11. To enable AD-based logins to the database, use the instructions provided at

1212 <https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-active-directory-authentication?view=sql-server-linux-2017#createsqllogins>.

1214 **2.10 Samba File Server**

1215 Samba is an open-source tool that provides file and print services by using the Server Message Block
1216 (SMB) / Common Internet File System protocol. Samba can also be used to emulate Windows domain
1217 controllers and member servers in AD environments.

1218 **2.10.1 How It's Used**

1219 Samba was used in this example implementation to provide file services for AD domain clients. As a file
1220 server potentially holding confidential information, it was also used as a managed asset for which
1221 privileged user access was controlled by policies configured on the PAM system.

1222 **2.10.2 Virtual Machine Configuration**

1223 The Samba virtual machine is configured as follows:

1224 ▪ Ubuntu Linux 16.04 LTS

1225 ▪ 1 CPU core

1226 ▪ 8 GB of RAM

1227 ▪ 40 GB of storage

1228 ▪ 1 NIC

1229 **Network Configuration:**

1230 ▪ IPv4: manual

1231 ▪ IPv6: disabled

1232 ▪ IPv4 address: 172.16.3.21

- 1233 ■ Netmask: 255.255.255.0
1234 ■ Gateway: 172.16.3.1
1235 ■ DNS name servers: 172.16.3.10
1236 ■ DNS-search domain: acmefinancial.com

1237 **2.10.3 Firewall Configuration**

1238 `ufw allow 137`
1239 `ufw allow 138`
1240 `ufw allow 139`
1241 `ufw allow 445`
1242 `ufw allow 22/tcp`
1243 `ufw default deny incoming`

1244 **2.10.4 Installation and Configuration**

- 1245 1. Ensure that the DNS server is set to the AD domain controller IP address. Enter the following command to verify:
1246 `cat /etc/resolv.conf`
- 1248 2. Ensure that the search domain is set to your domain (e.g., acmefinancial.com). Enter the following command to verify:
1249 `cat /etc/resolv.conf`

```
nedu@SambaFileServer1:~$ 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).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet static
address 172.16.3.199
netmask 255.255.255.0
gateway 172.16.3.1
dns-nameservers 172.16.3.10
dns-search acmefinancial.com
```

1251

- 1252 3. Install the chrony ntp client by entering the following command:
- 1253 sudo apt-get install chrony
- 1254 4. Add the following line to the */etc/chrony/chrony.conf* file so that chrony points to the NTP server:
- 1255 server 172.16.3.10
- 1256 5. Restart the chrony service by entering the following command:
- 1257 systemctl restart chrony
- 1259 6. Install the Samba, Kerberos, and winbind packages by entering the following command at the terminal:
- 1261 apt-get install samba krb5-user krb5-config winbind libpam-winbind libnss-winbind
- 1262
- 1263 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
```

- 1264
- 1265 8. Restart these services by entering the following command:
- 1266 systemctl restart smbd winbind
- 1267 9. Join the domain by entering the following command:
- 1268 net ads join -U administrator

- 1269 10. Enter the domain admin password when prompted.
- 1270 11. Enter the following command at the terminal to create a folder to be shared via Samba:
- 1271 mkdir /PII2
- 1272 12. Enter the following command to change the owning group to domain users:
- 1273 chgrp "domain users" /PII2
- 1274 13. Enter the following command to ensure that only domain admins have access to the folder:
- 1275 chmod 660 /PII2
- 1276 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
```

- 1277
- 1278 15. Restart these services by entering the following command:
- 1279 systemctl restart smbd winbind

1280 **2.11 Remidian SecureONE**

1281 SecureONE is a PAM system that controls privileged access to managed assets by adding accounts to or
1282 removing accounts from administrative groups on the asset's OSes. SecureONE does not require an
1283 agent on the managed asset but instead uses Windows Remote Procedure Call and SSH to make
1284 privilege escalation and de-escalation changes on the end point.

1285 **2.11.1 How It's Used**

1286 In the example implementation, SecureONE was used as a PAM system that controls administrative
1287 access to the managed asset's OS. SecureONE was not used for managing administrative access to any
1288 application.

1289 **2.11.2 Virtual Machine Configuration**

1290 The Remidian SecureONE virtual machine is configured as follows:

- 1291 ▪ Ubuntu Linux 16.04 LTS
- 1292 ▪ 4 CPU cores

1293 ■ 16 GB of RAM

1294 ■ 100 GB of storage

1295 ■ 1 NIC

1296 **Network Configuration:**

1297 ■ IPv4: manual

1298 ■ IPv6: disabled

1299 ■ IPv4 address: 172.16.2.10

1300 ■ Netmask: 255.255.255.0

1301 ■ Gateway: 172.16.2.1

1302 ■ DNS name servers: 172.16.3.10

1303 ■ DNS-search domain: acmefinancial.com

1304 **2.11.3 Installation and Initial Configuration**

1305 In the example implementation, SecureONE was deployed as a prebuilt virtual-machine appliance from
1306 the vendor. The appliance was still configured with parameters necessary for our environment. You can
1307 connect to the SecureONE appliance by navigating your web browser to <https://10.33.51.227>. Replace
1308 the IP address with your appliance's IP address.

1309 **2.11.4 Domain Configuration**

1310 SecureONE needs to be configured to manage systems in an AD environment. The configuration details
1311 are provided in the following steps:

1312 1. Create a service account in AD. Name the service account as secureone, and add it to the
1313 domain admins group. This account will be used by the SecureONE appliance.

1314 2. Click **Configure > Server > Edit Configuration**, and fill out the pop-up window with the relevant
1315 information:

Domain Configuration	
Domain Name	acmefinancial.com
LDAP Server	ad-production.acmefinancial.com
LDAP Port	636
SSL	Enabled
Bind DN	secureone@acmefinancial.com
Bind Password	[Hidden]
Search Base	dc=acmefinancial,dc=com
Page Size	1000
Search Scope	Subtree
Service Account Credentials	
Scan-mode Domain User (Read-Only)	acmefinancial\secureone
Scan-mode Domain Password	[Hidden]
Protect-mode Domain User	acmefinancial\secureone
Protect-mode Domain Password	[Hidden]

1316

1317 2.11.5 Managing Systems

1318 SecureONE manages systems by enrolling them into protected mode. Once a system is enrolled,
 1319 SecureONE can change a user's group memberships. SecureONE can add or remove users from the local
 1320 admins group or the local sudoers group. Use the following steps to enroll a domain computer:

- 1321 1. Navigate to **Access > System Search**.
- 1322 2. In the search bar, enter the host name of the system to be managed.
- 1323 3. Change the setting under **Protect Mode** to **Enabled**.

The screenshot shows the NEDU Access interface. On the left is a dark sidebar with icons for Dashboard, Access, Insight, and Configure. The main area has a title 'Access > Grant Access'. A search bar at the top contains the text 'ACMEFINANCIAL\WIN10CLIENT1'. Below it is a card for 'WIN10CLIENT1' showing a monitor icon, 'Protect Mode: Enabled', and 'Scan Mode: Enabled'. Below the card are details: Operating System: Windows 10 Pro, Service Pack: 10.0 (17134), OS Version: 10.0 (17134), Last Seen: a few seconds ago, and Last IP Address: 172.16.3.210. At the bottom is a button labeled 'Update IP Address'.

1324

2.11.6 Adding New Users

1. Once logged in, navigate to **Configure > Server > Add User/Group**.
2. In the search bar, type the name of the domain user, and then click **Add User/Group**.

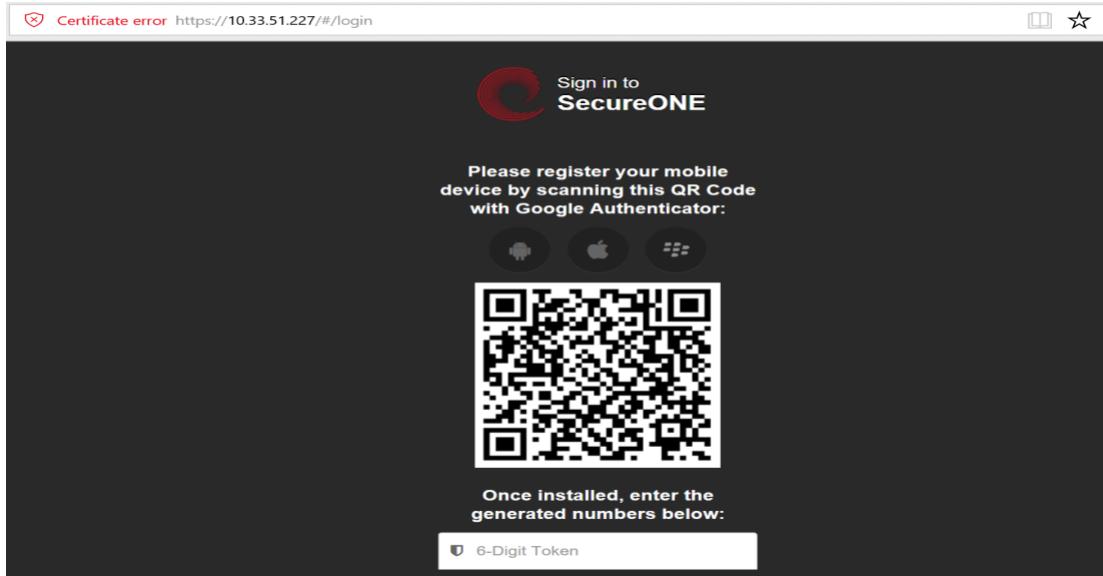
The screenshot shows the 'Add/Remove Users-Groups' interface. A search bar at the top contains 'ACMEFINANCIAL\devin'. A green success message says 'Successfully Added ACMEFINANCIAL\devin to SecureOne'. Below is a table of users:

Account	Account Type	Date Added	Modify
ACMEFINANCIAL\testdomuser1	Administrator	Fri Jul 06 2018 13:24:50 GMT+0000 (UTC)	Modify
ACMEFINANCIAL\nedu	Administrator	Fri May 18 2018 14:26:30 GMT+0000 (UTC)	Modify
ACMEFINANCIAL\tom	Administrator	Thu Jul 12 2018 15:59:21 GMT+0000 (UTC)	Modify
ACMEFINANCIAL\devin	User	Tue Aug 14 2018 15:40:04 GMT+0000 (UTC)	Modify

At the bottom, a red note says 'Showing 1 to 4 of 4 entries' and there are navigation buttons for 'Previous', '1', and 'Next'.

1328

- 1329 3. SecureONE uses a built-in Google Authenticator for 2FA. Once the new user attempts to log in
1330 with their domain password, a Quick Response (QR) code is presented.



- 1331
- 1332 4. Scan the QR code with the Google Authenticator mobile application to receive your onetime
1333 passcode, which changes every 60 seconds.
- 1334 5. Enter your onetime passcode in the **6-Digit Token** field below the QR code.

1335 [2.11.7 Requesting Privileged Access to Protected System](#)

- 1336 A user can request privileged access to a system by using the following steps:
- 1337 1. Navigate to **Access > System Search**.
- 1338 2. In the search bar, enter the host name of the protected system.
- 1339 3. Click **Access System**.

The screenshot shows the 'Access' interface with a search bar for 'ACMEFINANCIAL\WIN10CLIENT1'. On the left, a detailed view of the system 'WIN10CLIENT1' is shown, including its operating system (Windows 10 Pro), service pack (10.0 (17134)), last seen (10 minutes ago), and last IP address (172.16.3.210). It also shows protect mode and scan mode as enabled. On the right, a table lists administrator accounts with columns for Account, Type, Persistent, On System, Expiration, and Action. The accounts listed are WIN10CLIENT1\Administrator, ACMEFINANCIAL\secureone, WIN10CLIENT1\defaultuser0, ACMEFINANCIAL\Domain Admins, WIN10CLIENT1\admin, WIN10CLIENT1\tempadmin, and ACMEFINANCIAL\nedu. The 'Expiration' column for the 'ACMEFINANCIAL\nedu' account shows a date and time: 8/15/2018 4:53 PM.

1340

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

The screenshot shows the 'Access' interface with a search bar for 'ACMEFINANCIAL\WIN10CLIENT1'. On the left, a detailed view of the system 'WIN10CLIENT1' is shown, including its operating system (Windows 10 Pro), service pack (10.0 (17134)), last seen (10 minutes ago), and last IP address (172.16.3.210). It also shows protect mode and scan mode as enabled. On the right, a table lists administrator accounts with columns for Account, Type, Persistent, On System, Expiration, and Action. The accounts listed are WIN10CLIENT1\Administrator, ACMEFINANCIAL\secureone, WIN10CLIENT1\defaultuser0, ACMEFINANCIAL\Domain Admins, WIN10CLIENT1\admin, WIN10CLIENT1\tempadmin, and ACMEFINANCIAL\nedu. The 'Expiration' column for the 'ACMEFINANCIAL\nedu' account shows a date and time: 8/15/2018 4:53 PM.

1342

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

1344 **2.12 RSA Authentication Manager**

1345 RSA Authentication Manager is responsible for maintaining and managing user profiles, personal
1346 identification numbers (PINs), and tokens. Using its web interface, users can be activated or deactivated,
1347 PINs can be configured, and tokens can be assigned to users. Users can be created locally or retrieved
1348 from identity repositories.

1349 **2.12.1 How It's Used**

1350 In the example implementation, RSA Authentication Manager was configured to retrieve user account
1351 information from AD. Only accounts for privileged users were retrieved and configured. Tokens that had
1352 time-sensitive onetime passcodes were assigned to these user accounts, providing 2FA.

1353 **2.12.2 Installation and Initial Configuration**

1354 Authentication Manager was deployed as an appliance in the example implementation. Once the
1355 appliance boots successfully, the operator will have the opportunity to change or verify the IP address
1356 settings. Use the following steps to complete the initial configuration:

- 1357 1. To log into the system, use the link and the **Quick Setup Access Code** that are displayed after
1358 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
```

- 1359
1360 2. Enter the **Quick Setup Access Code**, click **Next**, and then accept the license agreement.

Not secure | <https://10.33.51.229/login.jsp>

RSA Authentication Manager

RSA Authentication Manager Quick Setup

Welcome to RSA Authentication Manager Quick Setup. Use Quick Setup to configure the primary and replica appliances.

Quick Setup Access Code

Enter Quick Setup Access Code: [What is this?](#)

Next

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

1361

1362

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

Primary Quick Setup	Replica Quick Setup
> Start Primary Quick Setup Configure a primary appliance, unless there is one already configured on your network. A primary appliance is where all authentication and administrative actions occur.	> Start Replica Quick Setup If you have already configured a primary appliance, RSA recommends that you configure one or more replica appliances for high availability and load balancing.

1363

1364

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

The screenshot shows the RSA Authentication Manager Primary Quick Setup interface. At the top, it says "RSA | Authentication Manager" and "Version: 8.2". Below that, the title "Primary Quick Setup" is displayed with a gear icon. A sub-section titled "Set up your RSA Authentication Manager primary instance in five steps." is shown. It lists requirements: "Before starting, confirm that you have:" followed by three bullet points: "The license file (.zip) accessible from your computer", "User IDs and strong passwords for the three new administrative accounts to be created. [What is a valid password?](#)", and "The NTP server hostname or IP address that the primary appliance will use for time synchronization (optional)". A note below says "For more information, see the Quick Setup Checklist for the Primary Appliance in the Setup and Configuration Guide." At the bottom of the step, there are five numbered tabs: ① License File, ② Date & Time, ③ OS Password, ④ Initial Administration Accounts, and ⑤ Summary. Below the tabs are "Back" and "Start Step 1" buttons.

1365

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

The screenshot shows the "1. License File" step of the Primary Quick Setup wizard. At the top, it shows the navigation tabs: 1. License File, 2. Date & Time, 3. OS Password, 4. Initial Administration Accounts, and 5. Summary. Below the tabs, a message says "Upload and review your license file." A "License File" section has a "Choose File" button with "No file chosen" and an "Upload" button. Below this, a summary table shows license details:

Serial Number	Stack Number	Product	Version	Licensed To	Date Issued
201805302	LID000105438X	RSA Authentication Manager	8.3	RSA	05/30/2018

Review the following summary of your license. Click Next to continue.

License Feature		Aggregate Summary
Authenticator Provisioning		Available
Business Continuity		Available
Expiration Date		Nov 30, 2018 12:00:00 AM UTC
License Type		Full Evaluation
Number of Instances		15
Number of users with RBA/ODA enabled		1000
Offline Authentication		Available
RADIUS		Available
RBA/ODA		Available
Self-Service		Available
Tokens		Available
Users with Assigned Authenticators		1000

Cancel **Next**

1368

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

Primary Quick Setup

1. License File 2. Date & Time 3. OS Password 4. Initial Administration Accounts 5. Summary

Set the Time Zone and Time Source.

Time Zone

Region: * America ▾

Location: * (UTC-05/UTC-04) New York ▾

Time Source

RSA recommends using an NTP server to prevent authentication failures and replication issues caused by clock drift. Virtual machines do not track time accurately. You can assure that the NTP server provides the expected time by clicking **Preview Current Date & Time**.

Note: NTP servers are required if you have a replica appliance in your deployment.

Time: * Sync to NTP Server
Hostname or IP Address
172.16.3.10
Secondary Hostname or IP Address (optional)

 Sync to the physical machine hosting this virtual appliance

1370

- 1371 7. Enter the credentials for the Authentication Manager's OS, and then click **Next**.
- 1372 8. On the following screen, enter the credentials for the **Operations Console admin** and the **Security Console admin**.

1374 2.12.3 LDAP Integration

1375 Authentication Manager can be configured to connect to LDAP sources and to retrieve user profiles for
1376 easy management. The following steps are used to connect to LDAP repositories, to retrieve user
1377 account information, and to manage tokens assigned to users:

- 1378 1. Go to the operations console by navigating your web browser to
1379 https://<appliance_IP_address>/oc.
- 1380 2. Enter the credentials to log into the operations console.
- 1381 3. Navigate to **Deployment Configuration > Identity Sources > Add New**. On the **Connection(s)** tab
1382 in the appropriate fields, add the values necessary for your environment:

The screenshot shows the 'Identity Source Properties' interface. At the top, there are tabs for 'Connection(s)' and 'Map'. Below them, a message says 'Edit information about your identity source.' A note indicates that the 'Identity Source Name' field is required. The 'Identity Source Basics' section contains fields for 'Identity Source Name' (set to 'AD-PRODUCTION'), 'Type' (set to 'Active Directory'), and 'Notes' (an empty text area). The 'Directory Connection - Primary' section shows a 'Directory URL' field containing 'ldap://ad-production'.

1383

1384 4. Enter the value of a domain admin, such as `administrator@acmefinancial.com`, in the
1385 **Directory User ID** field.

1386 5. Click **Test Connection**.

1387 2.12.4 Token Assignment

1388 To assign a token to a user, use the following steps:

- 1389 1. Go to the security console by navigating your web browser to
1390 `https://<appliance_IP_address>/sc`.
- 1391 2. Enter the credentials to log into the security console.
- 1392 3. Navigate to **Identity > Users > Manage Existing**.
- 1393 4. Ensure that the **Identity Source** field points to your AD server, identified by its unique name
1394 given in the operations console.
- 1395 5. In the **Where** field, select **User ID**.
- 1396 6. In the search bar, enter the User ID for which you would like to search.
- 1397 7. The user account will be retrieved and displayed.

1398

1399 8. Click on the User ID (by selecting the check box to the left of the User ID), and then click **SecurID Tokens**.

1400

1401 9. Click **Assign Token**.

1402

1403 10. Select a serial number (by selecting the check box to the left of the serial number), and then click **Assign**.

1405 2.12.5 Software Token Profiles and Token Distribution

1406 Software Token Profiles specify parameters that enable the secure distribution of assigned tokens to
 1407 users. Use the information provided at <https://community.rsa.com/docs/DOC-77084> to create a
 1408 software token profile. To distribute an assigned token to a user, follow the instructions provided at
 1409 <https://community.rsa.com/docs/DOC-77090>.

1410 2.13 Splunk

1411 Splunk is a security information and event management system that allows collecting and parsing logs
1412 and data from multiple systems.

1413 2.13.1 How It's Used

1414 Splunk can receive data from a plethora of different sources. The most reliable option is installing
1415 Splunk's Universal Forwarder on each system from which you want to collect data. Other options
1416 include syslogs, file and directory monitoring, and network events. Once data has been collected by
1417 Splunk, it can then be parsed and displayed by using prebuilt rules or custom criteria. Splunk is used to
1418 report and alert on unauthorized activity.

1419 2.13.2 Installation

1420 Note: You will need a Splunk account to download Splunk Enterprise. The account is free and can be set
1421 up at https://www.splunk.com/page/sign_up.

1422 Download Splunk Enterprise from https://www.splunk.com/en_us/download/splunk-enterprise.html.
1423 This build uses Version 7.0.3. Splunk can be installed on Windows, Linux, Solaris, and Mac OS X. Each of
1424 these installation instructions is provided at
1425 <http://docs.splunk.com/Documentation/Splunk/7.1.3/Installation/Beforeyouinstall>.

1426 2.13.3 Queries

1427 Two Splunk reports were created for this build. One of the reports is named **DemoBomgar-AD-Auth-**
1428 **UnauthV1**, which captures activities that are authorized or activities that violate the workflow. The
1429 other report is named **DemoRadiant-AD-Event-Details**, which captures more details of those events and
1430 can be used as a secondary monitor for AD.

1431 2.13.4 DemoBomgar-AD-Auth-UnauthV1

```
1432 index="demo" sourcetype=_json OR sourcetype="csv" NOT host="radiant-logic" NOT ("A  
1433 user account was changed" OR "A user account was enabled") |where NOT like(UserObject,  
1434 "UserObject%") |eval BomgarUserSubject=substr('Event.@sOriginatingAccount',15) |table  
1435 _time host Event.@sEventID Event.@sLoginName Event.@sMessage BomgarUserSubject  
1436 UserSubject UserObject Event|eval  
1437 UserSubject=if(isnotnull(BomgarUserSubject),BomgarUserSubject,UserSubject) |transaction  
1438 UserSubject maxspan=240s|eval  
1439 Policy=if((BomgarUserSubject==UserSubject),"Authorized","Unauthorized") |table _time  
1440 host Policy Event.@sEventID Event.@sLoginName UserSubject UserObject Event
```

1441 2.13.5 DemoRadiant-AD-Event-Details

```
1442 index="demo"
1443 source="C:\\\\radiantone\\\\vds\\\\r1syncsvcs\\\\log\\\\cf_o_acmefinancial\\\\object_generic_dv_so
1444 _o_acmefinancial_capture.log" OR source="c:\\\\final_ad.csv" NOT ("A user account was
1445 changed" OR "A user account was enabled") |rex
1446 "\\<sAMAccountName\\> (?P<LDAPObject>.+) \\</sAMAccountName\\>" |rex
1447 "\\<RLICHANGETYPE\\> (?P<RLICHANGETYPE>\\w+)" |rex
1448 "\\<RLICHANGES\\> (?P<RLICHANGES>.+) \\</RLICHANGES\\>" |rex
1449 "\\<userPrincipalName\\> (?P<UserObject>\\w+) @" |table _time host UserSubject LDAPObject
1450 UserObject Event RLICHANGETYPE RLICHANGES |where isnotnull(UserSubject) OR
1451 isnotnull(UserObject) | where NOT like(UserObject, "MSOL%") |where NOT like(UserObject,
1452 "UserObject%") |table _time host UserSubject LDAPObject UserObject Event RLICHANGETYPE
1453 RLICHANGES |where NOT like(RLICHANGES, "replace: logonCount%") |eval
1454 RLICHANGETYPE=if(LIKE(Event, "%added%"), "update", RLICHANGETYPE) |eval
1455 RLICHANGETYPE=if(LIKE(Event, "%created%"), "insert", RLICHANGETYPE) |table _time host
1456 UserSubject UserObject LDAPObject Event RLICHANGETYPE RLICHANGES |eval
1457 UserObject=if(LIKE(LDAPObject, "%Admin%"), "", UserObject)
```

1458 2.13.6 SSL Forwarding

1459 We took advantage of Splunk's built-in SSL forwarding capability and configured SSL encryption between
1460 forwarders and the indexer. Instructions to enable SSL forwarding are provided at
1461 <http://docs.splunk.com/Documentation/Splunk/7.1.3/Security/ConfigureSplunkforwardingtousesignedcertificates>.

1463 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