

## 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](mailto: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](mailto:nccoe@nist.gov)

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

## ABSTRACT

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

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

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

Technology Partner/Collaborator	Build Involvement
<a href="#"><u>Splunk</u></a>	Splunk Enterprise
<a href="#"><u>TDi Technologies</u></a>	ConsoleWorks

## 1 **Contents**

2	<b>1</b>	<b>Introduction .....</b>	<b>1</b>
3	1.1	Practice Guide Structure .....	1
4	1.2	Build Overview .....	2
5	1.3	Typographic Conventions.....	3
6	<b>2</b>	<b>Product Installation Guides.....</b>	<b>3</b>
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	<b>Appendix A List of Acronyms .....</b>	<b>103</b>

## 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](mailto: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> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on-screen computer output, sample code examples, and status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b>service sshd start</b>
<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 <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a> .

## 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  
215    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()
```

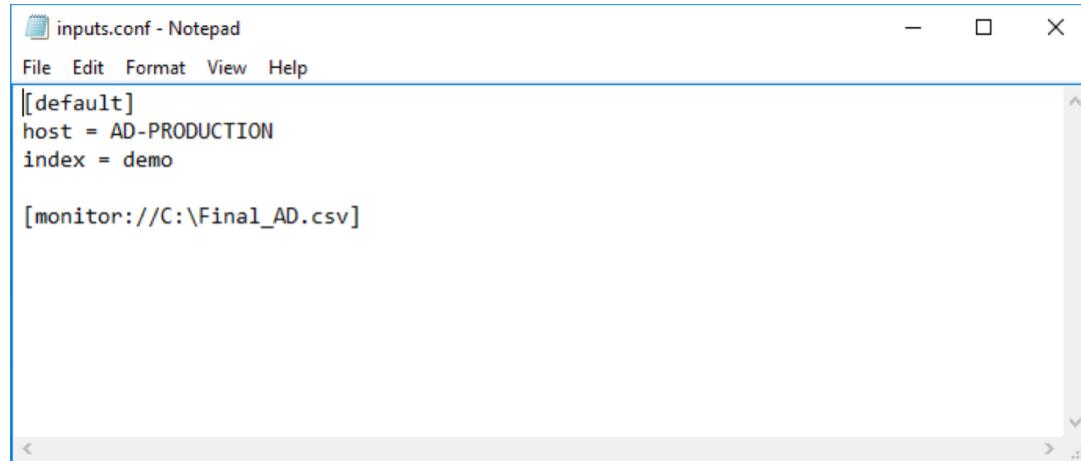
258 The following PowerShell script extracts data from the Windows security event log and executes the  
259 Python script above:

```
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)

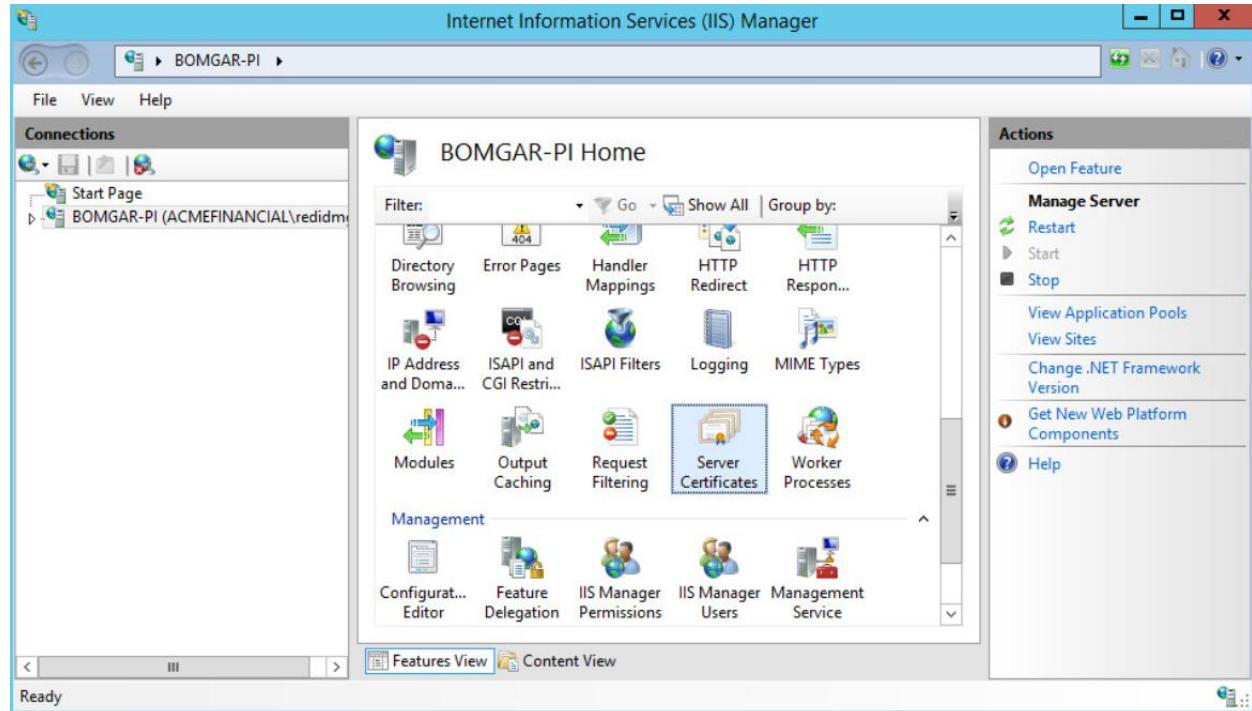
308   **2.2.3 Prerequisites**

- 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**

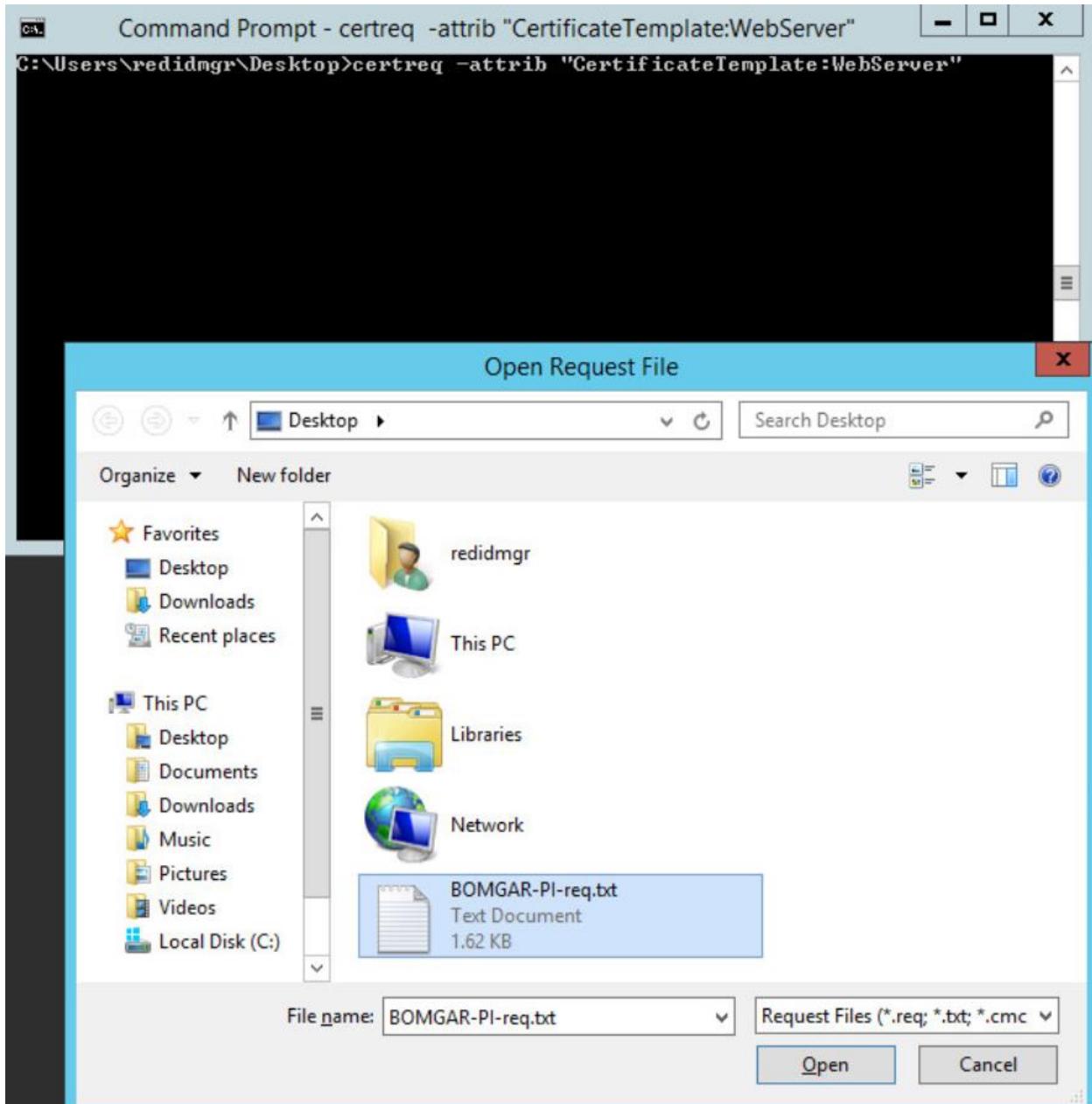
315   To configure IIS for use with Bomgar's web application server, a certificate signed by AD Certificate  
316   Services was created.

- 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**.



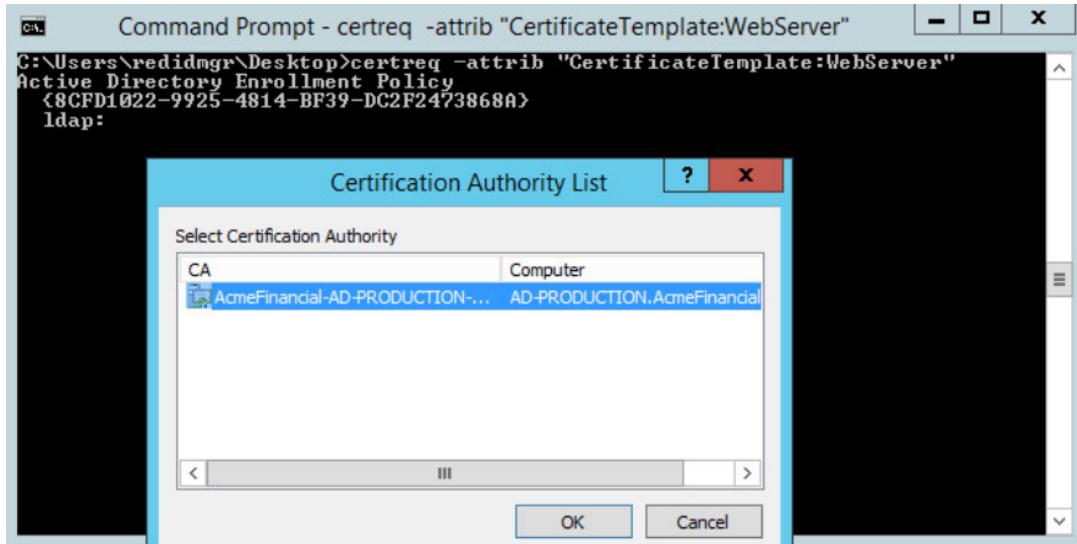
320

- 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**.



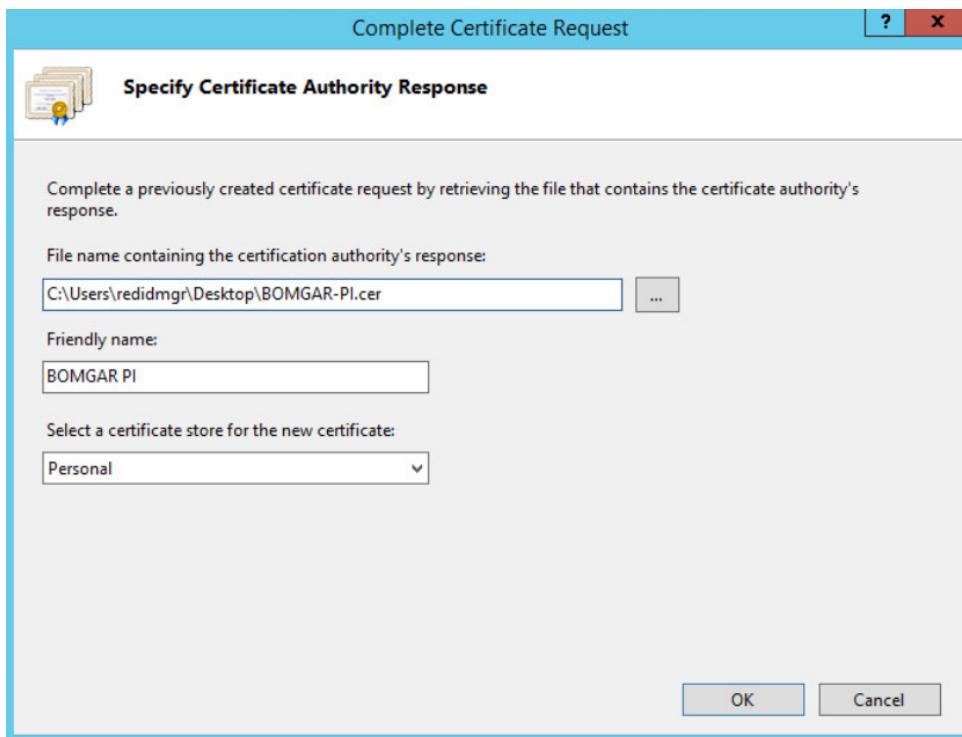
328

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

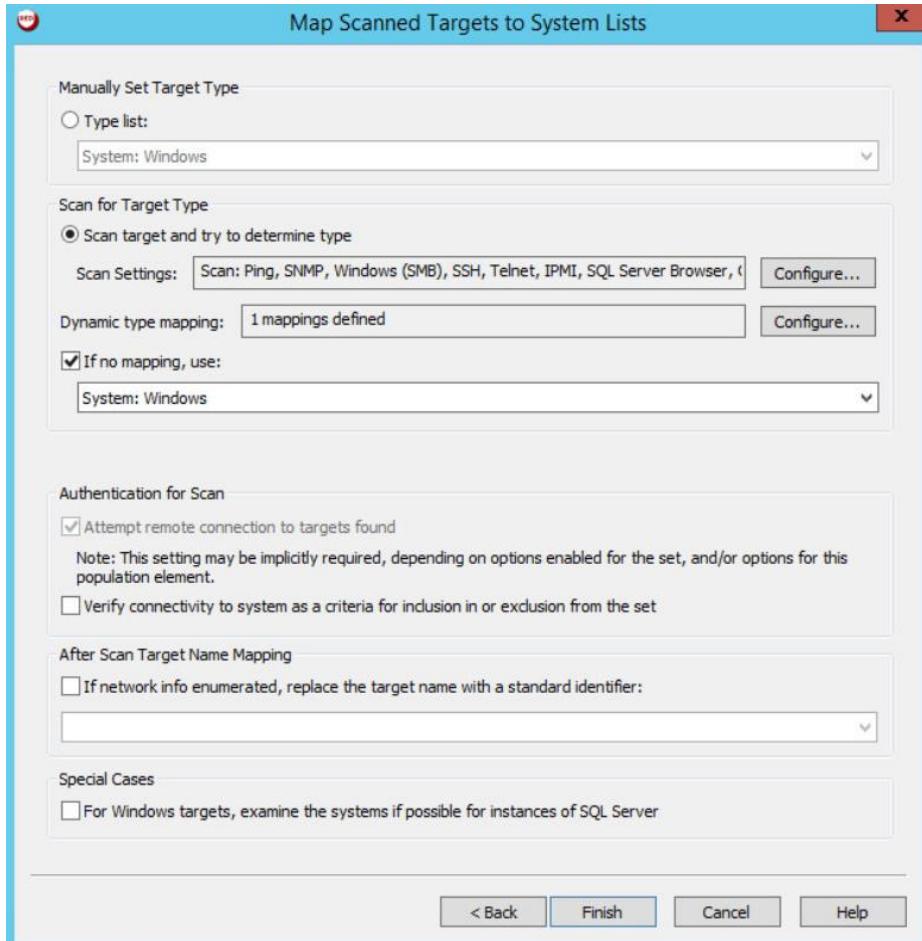
- 336        14. Click **OK**
- 337        15. Create a Secure Sockets Layer (SSL) binding with that certificate by following [documentation from Microsoft](#).
- 339        You are now ready to begin following further installation instructions that are publicly available on  
340        Bomgar's [website](#).

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:				
<b>Add targets from:</b>				
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"/>				
<b>Dynamic Update</b>				
<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			
<b>Options</b> <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**.

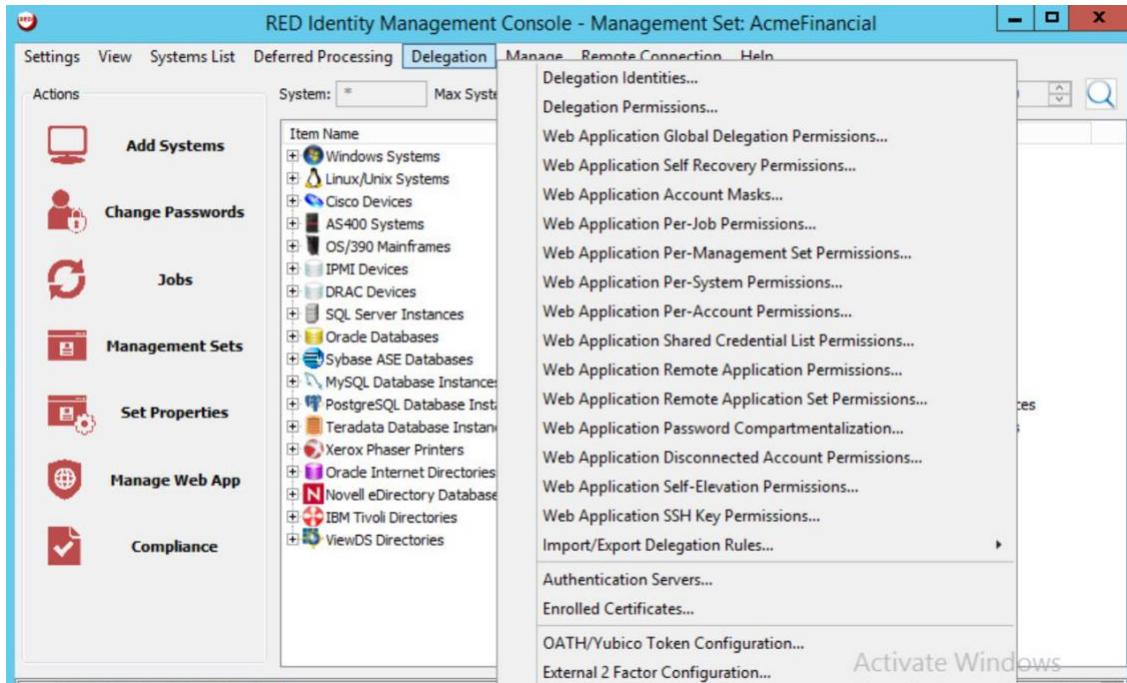
385       6. Configure the web launcher settings in the Bomgar **RED Identity Management Console**.

### 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.

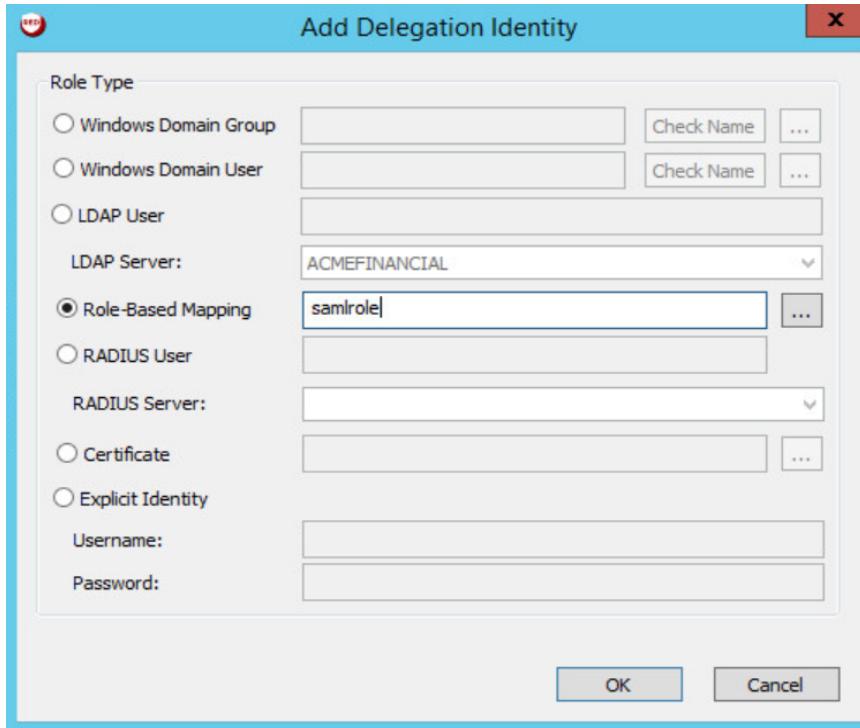
390 2. Navigate to **Delegation > Web Application Global Delegation Permissions**.



391

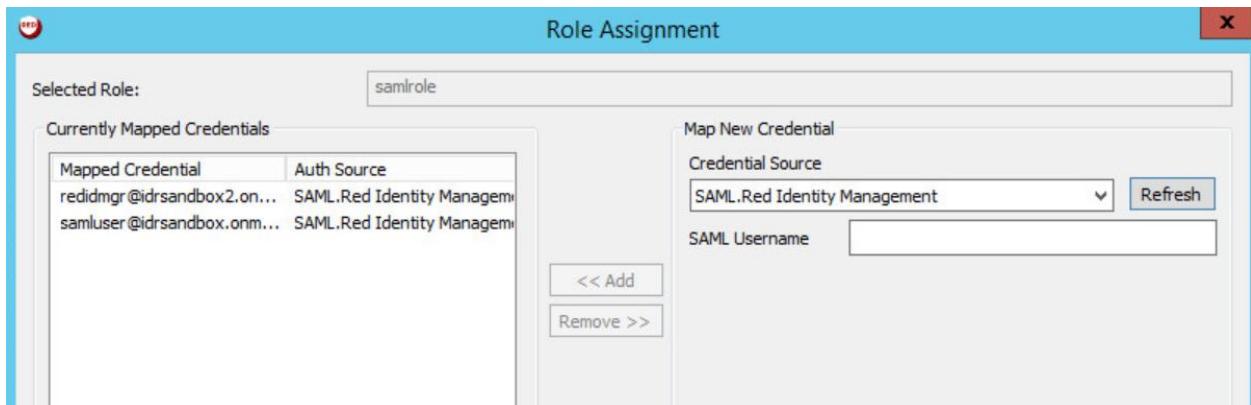
392 3. Click **Add** at the lower left corner.

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\edidmgr	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.

Please log in to access the Web Console

Authenticator

SAML.Red Identity Management

Use Integrated Authentication: ACMEFINANCIAL\edidmgr

Login

408

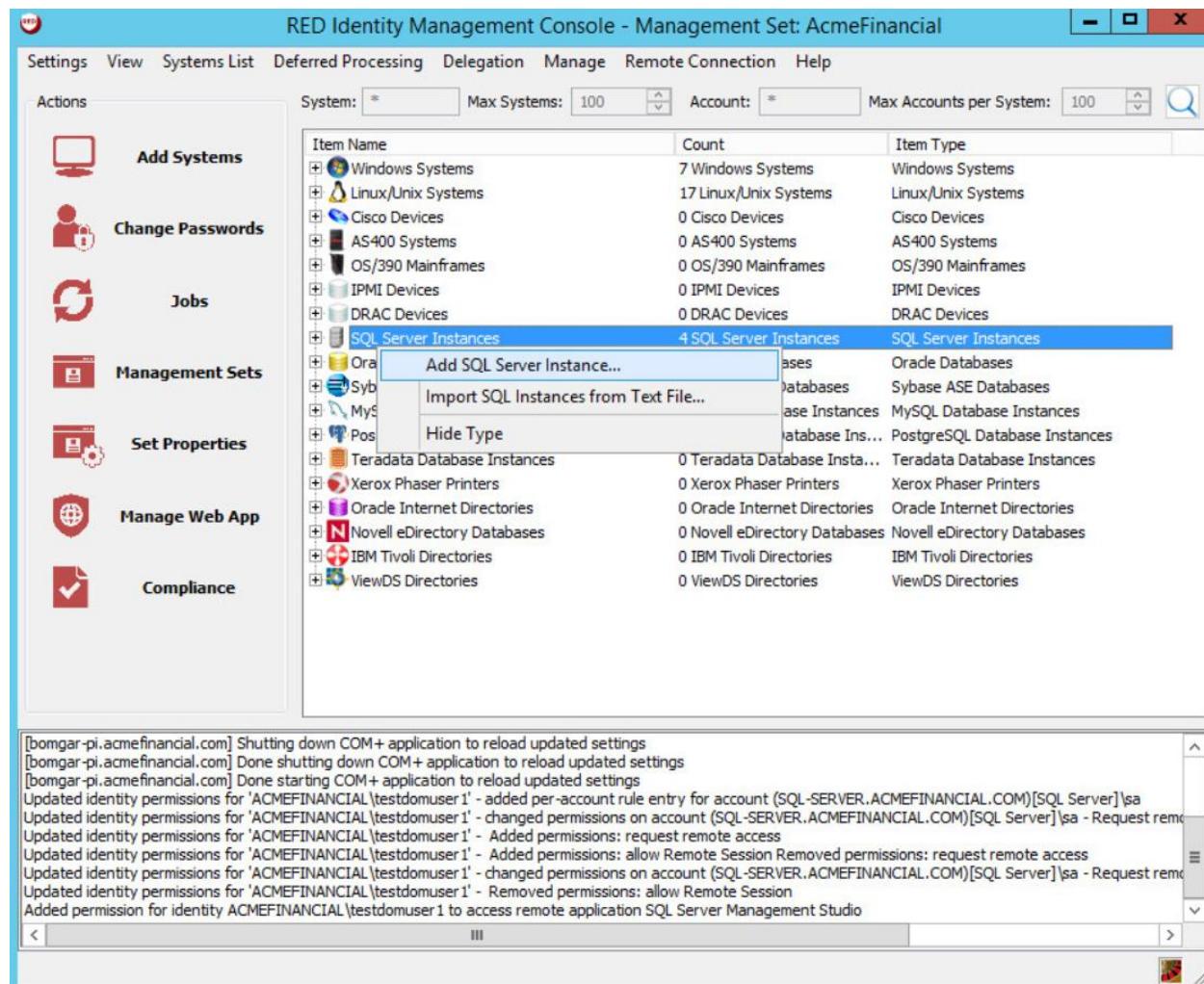
409    **2.2.8 Configuring Microsoft SQL Server Access**

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.

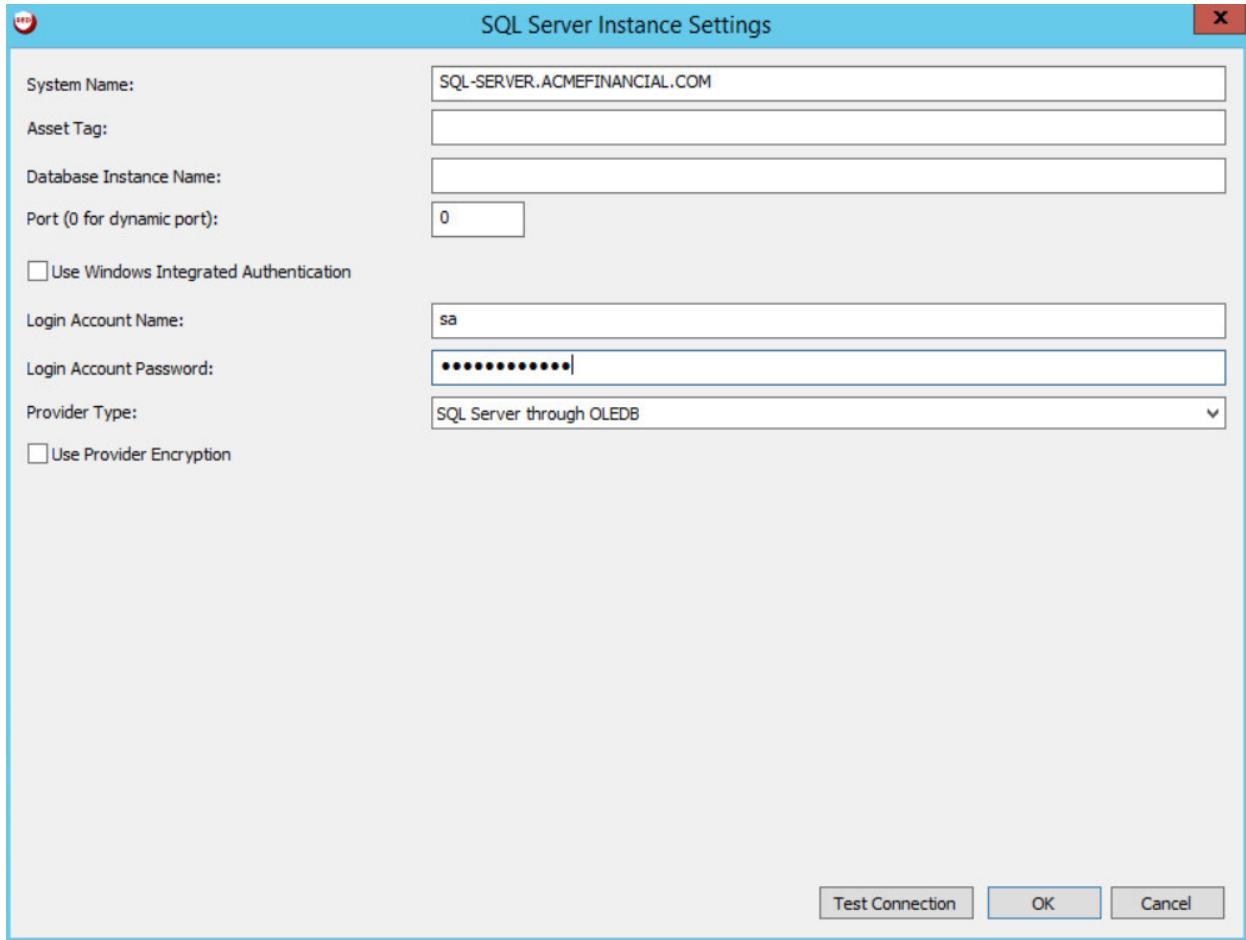
414    The following instructions configure Bomgar Privileged Identity to allow the **edb1** to request permission  
 415    to launch Microsoft SSMS and to log in as the **sa** account on Microsoft SQL Server in the production  
 416    environment.

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

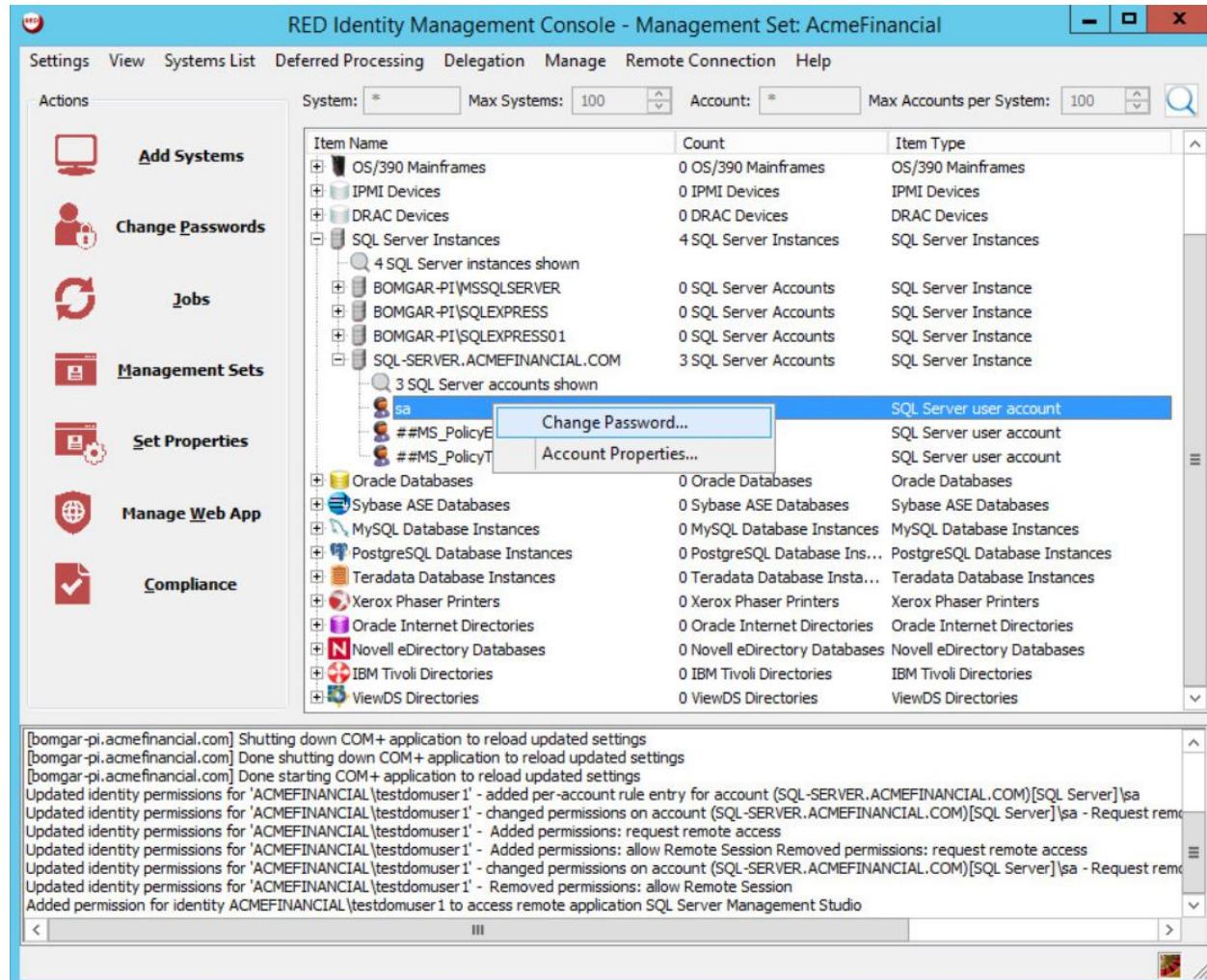


419

- 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.

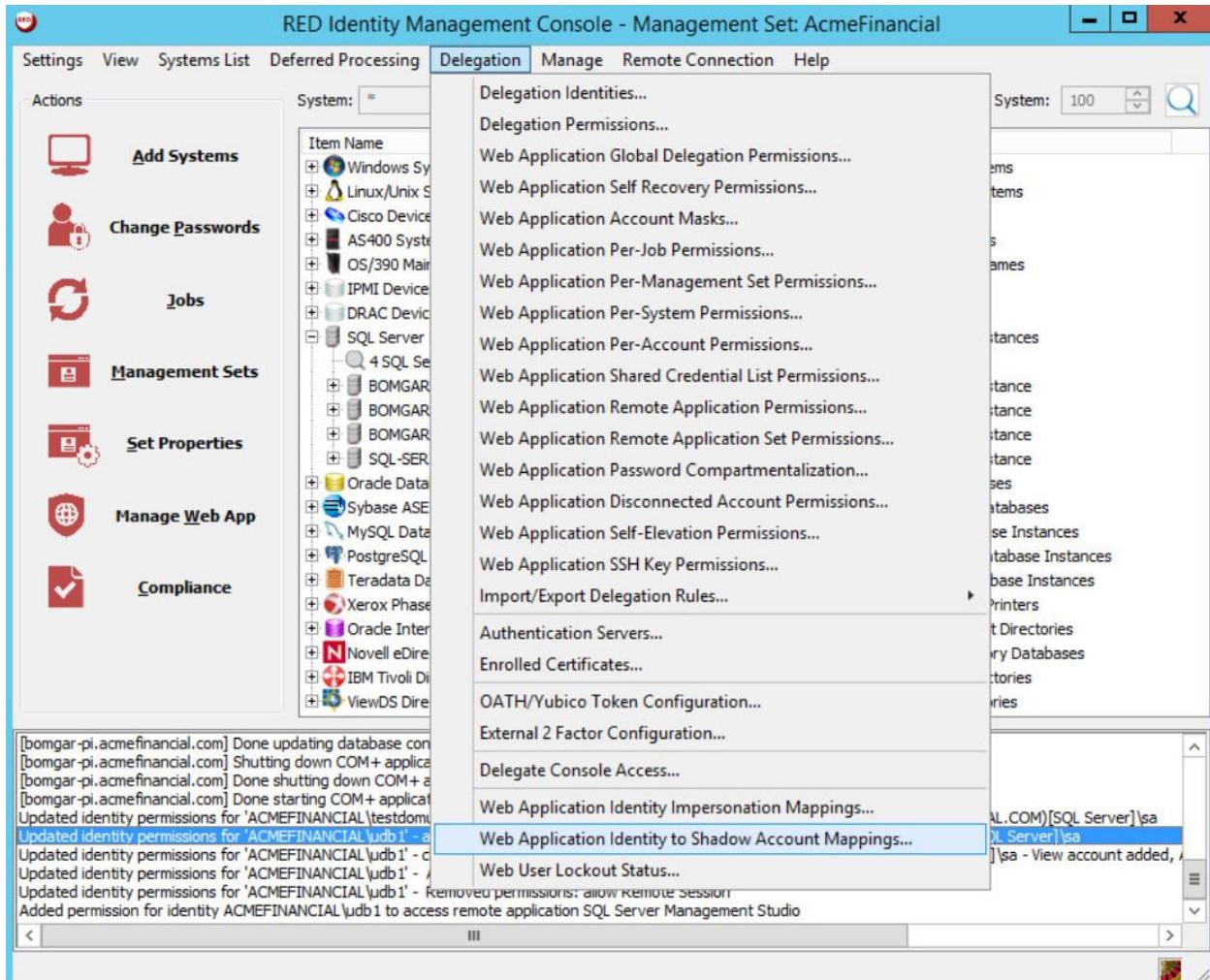


- 424        3. Click **Test Connection**. The connection should be successful. Click **OK**.
- 425        4. Expand **SQL Server Instances** by clicking on the plus sign to the left of the item name, and then expand **SQL-SERVER.ACMEFINANCIAL.COM**. Right-click the **sa** account, and then select **Change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



429

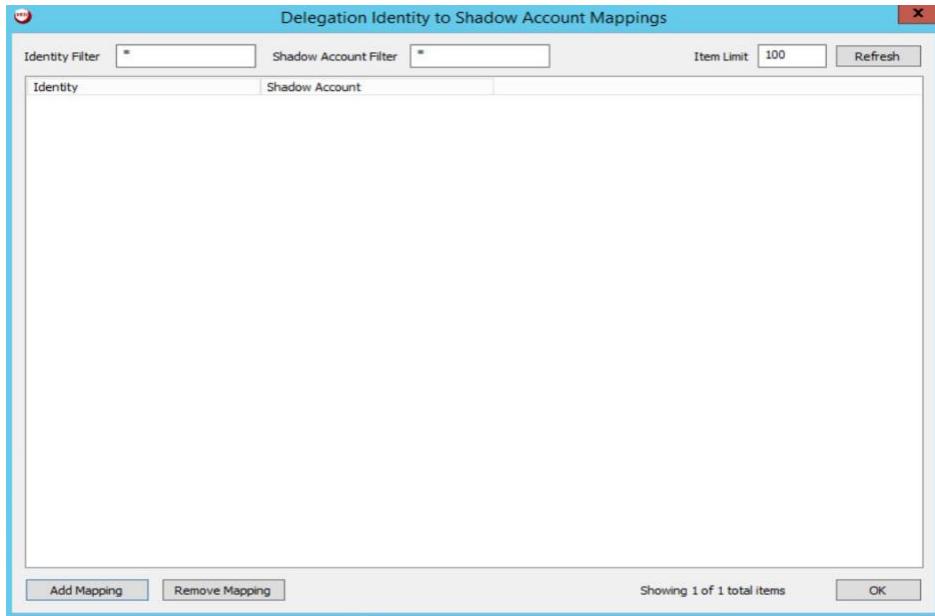
- 430     5. Select strong password policy options, such as increasing both the length of the password and its compliance with password standards.
- 432     6. On the **Schedule** tab, set the **Job Scheduling Period** to **Immediately**, and write a **Job Comment** to describe why this action is being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



436

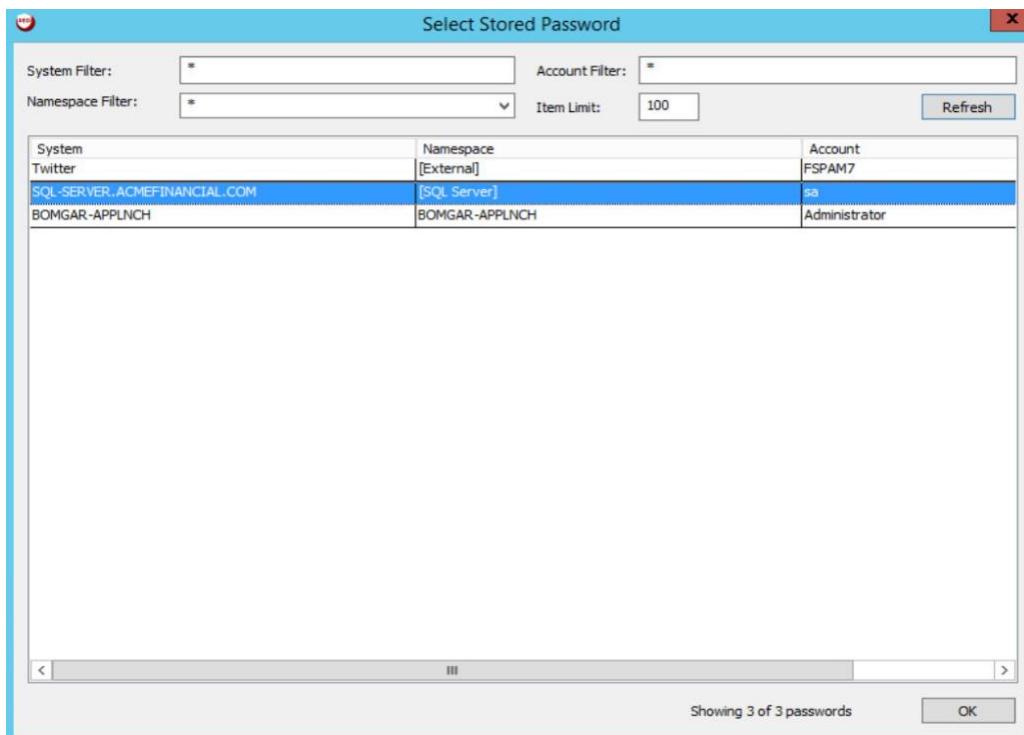
437

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**.

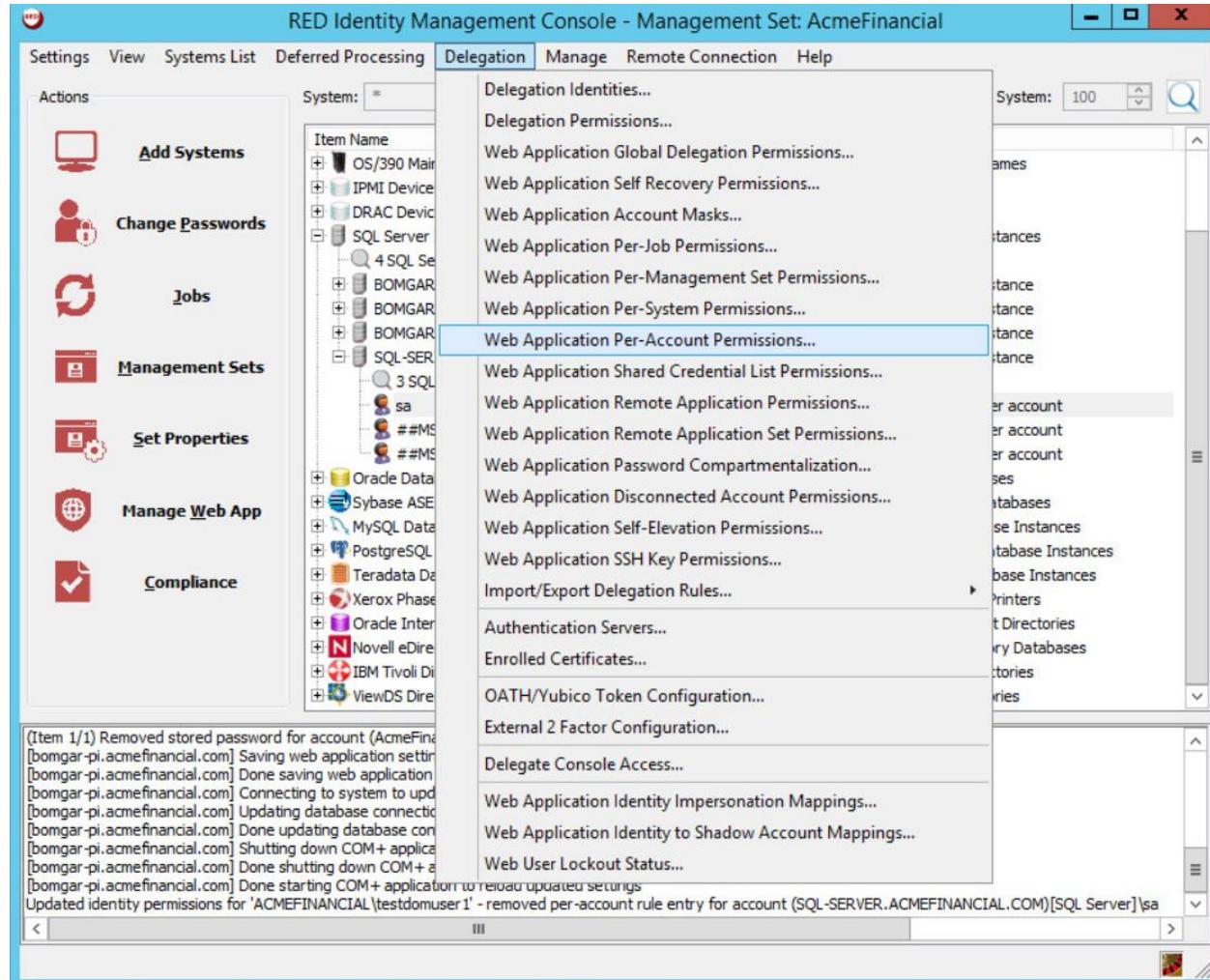


441

- 442    11. Click **OK** again.

443

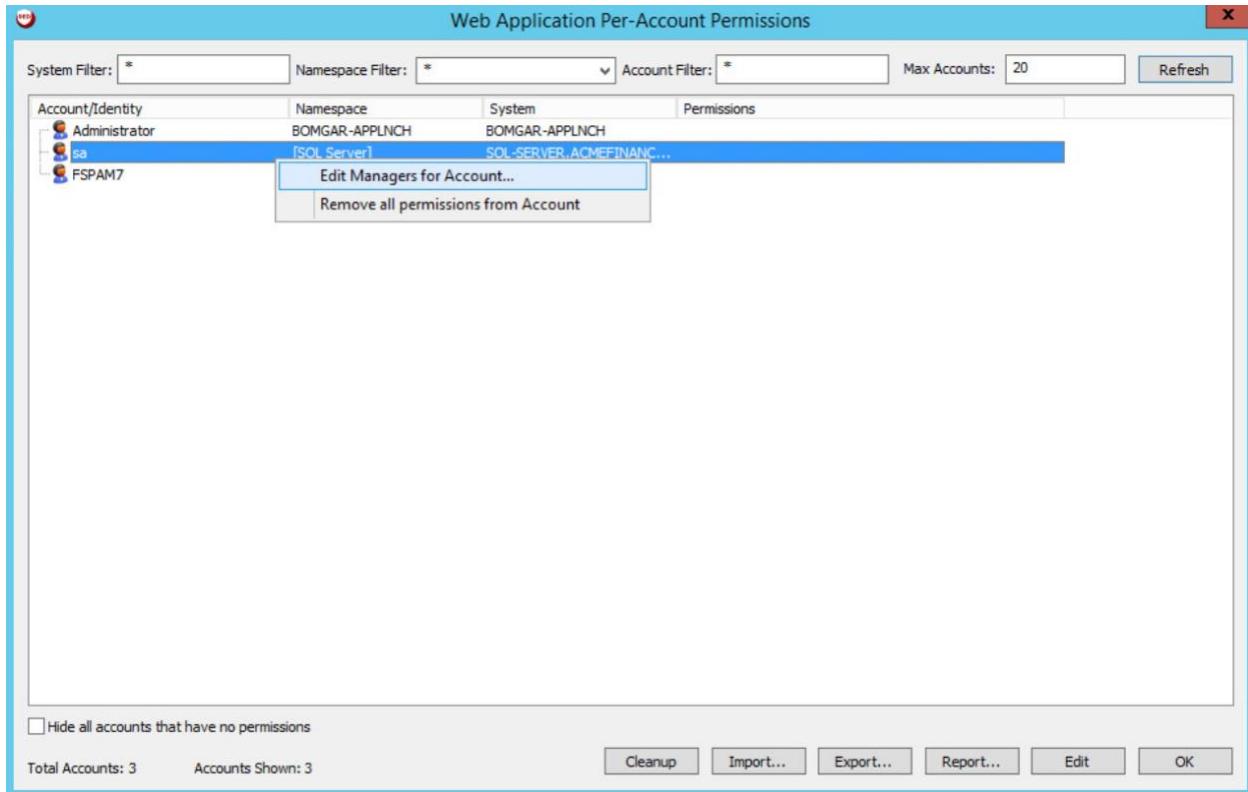
**12. Click Delegation > Web Application Per-Account Permissions.**



444

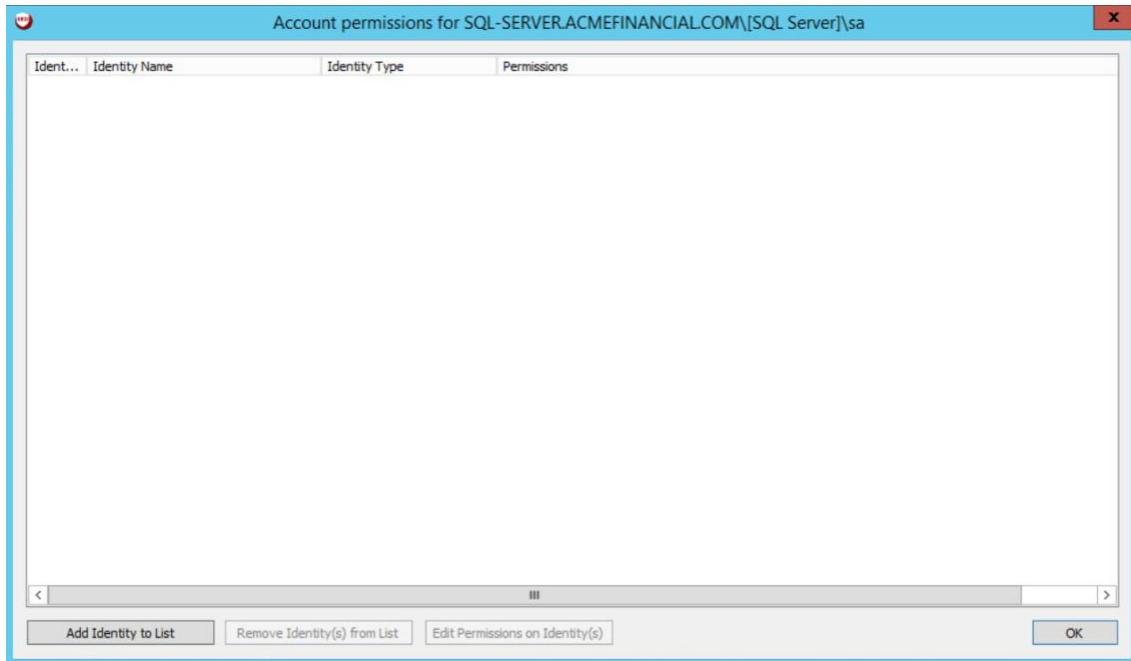
445

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



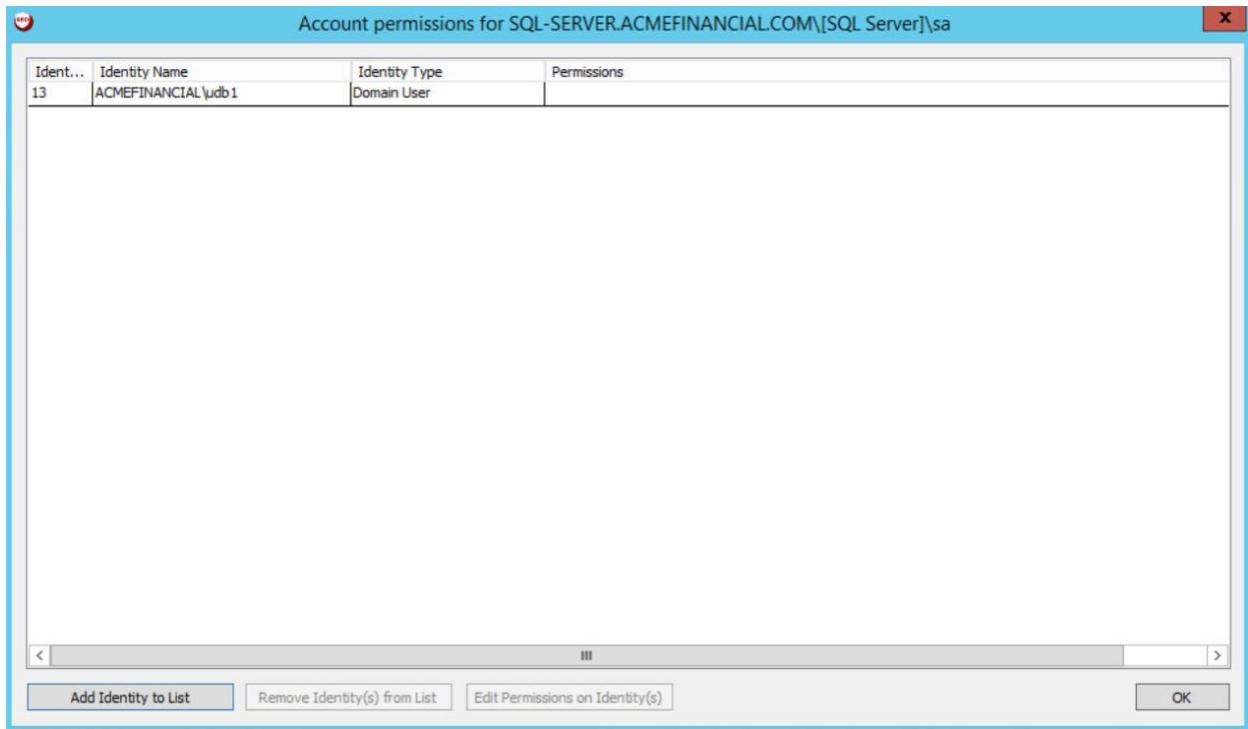
446

447      14. Click Add Identity to List.



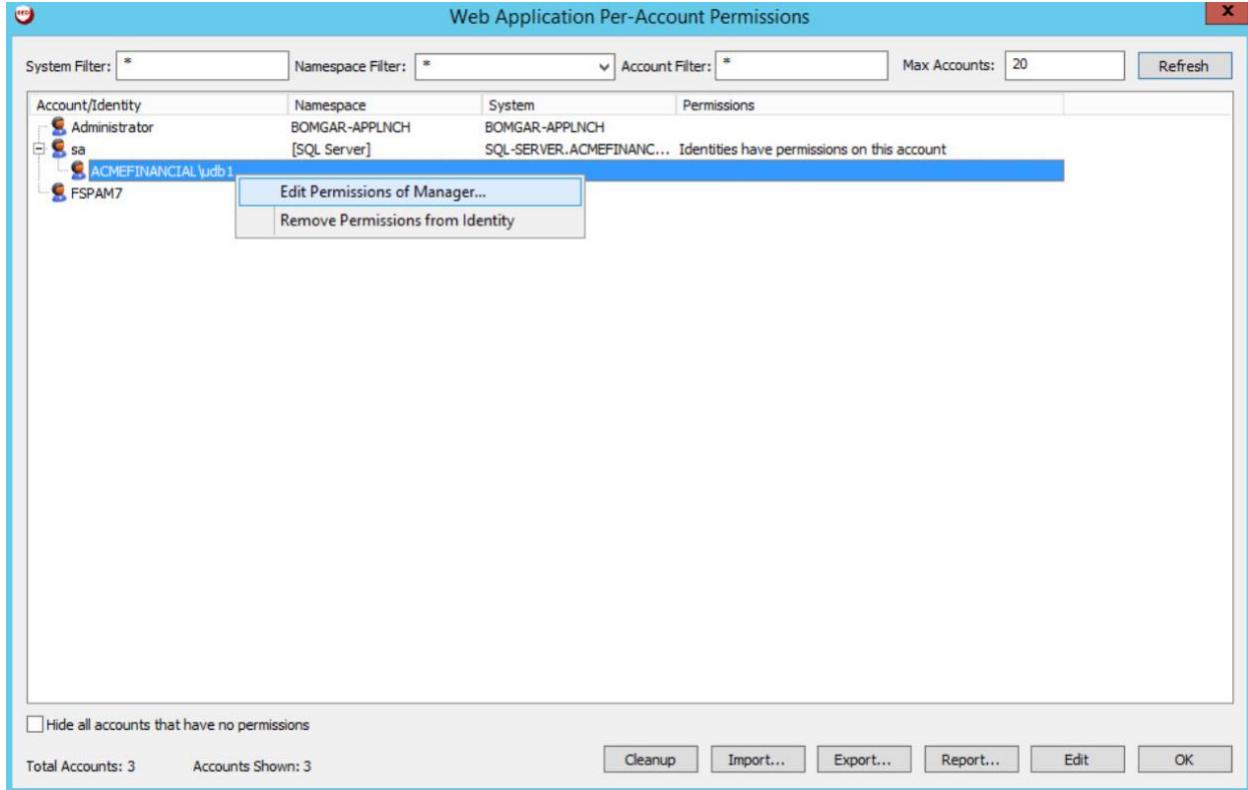
448

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

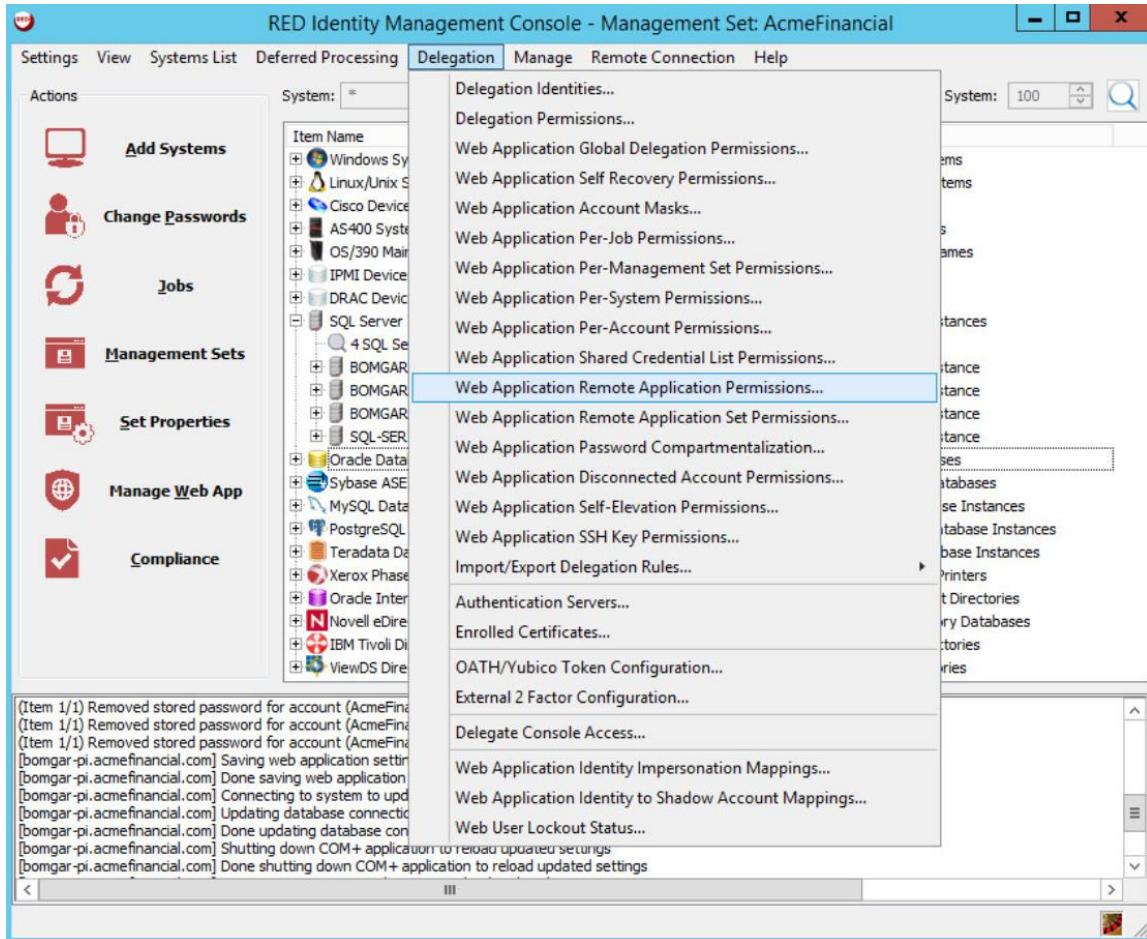


450

- 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



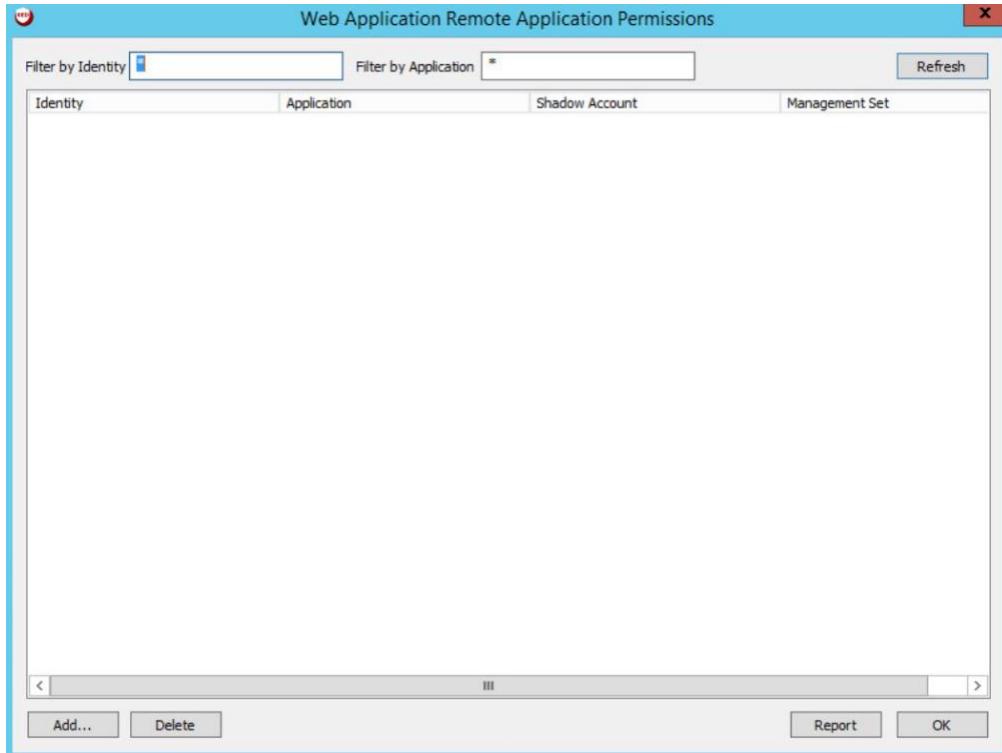
- 453
- 454        17. Give the account the **View Account** and **Request Remote Access** permissions. Click **OK**. Click **OK** again to exit the **Web Application Per-Account Permissions** window.
- 455
- 456        18. Click **Delegation > Web Application Remote Application Permissions**.



457

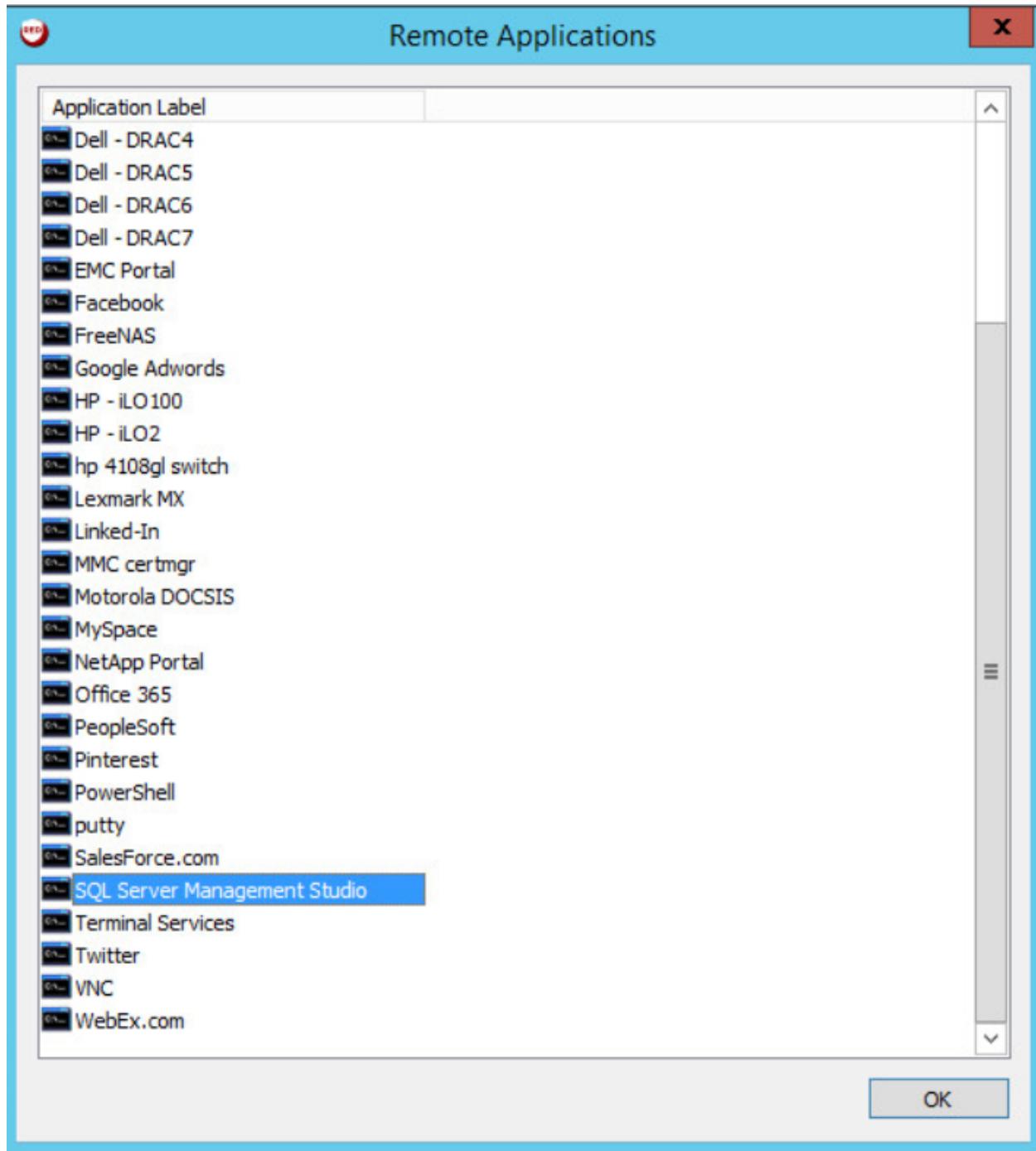
458

19. Click Add.



459

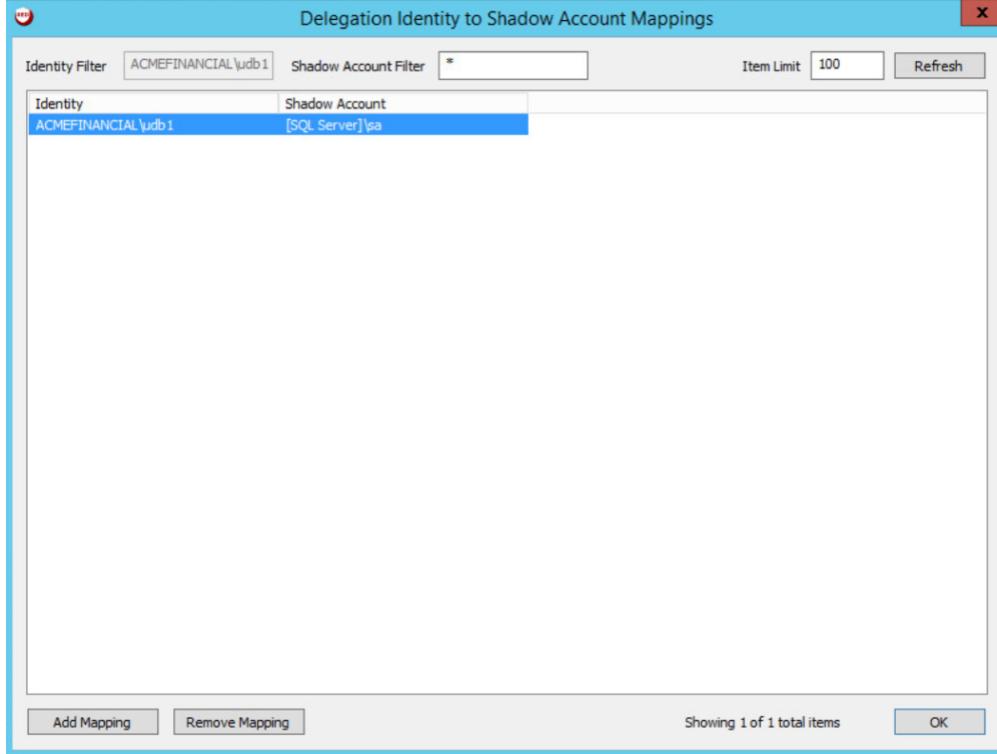
- 460    20. Select the **ACMEFINANCIAL\udb1** account from the list of **Delegation Identities**. Click **OK**. Next,  
461    select **SQL Server Management Studio** from the list of **Remote Applications**.



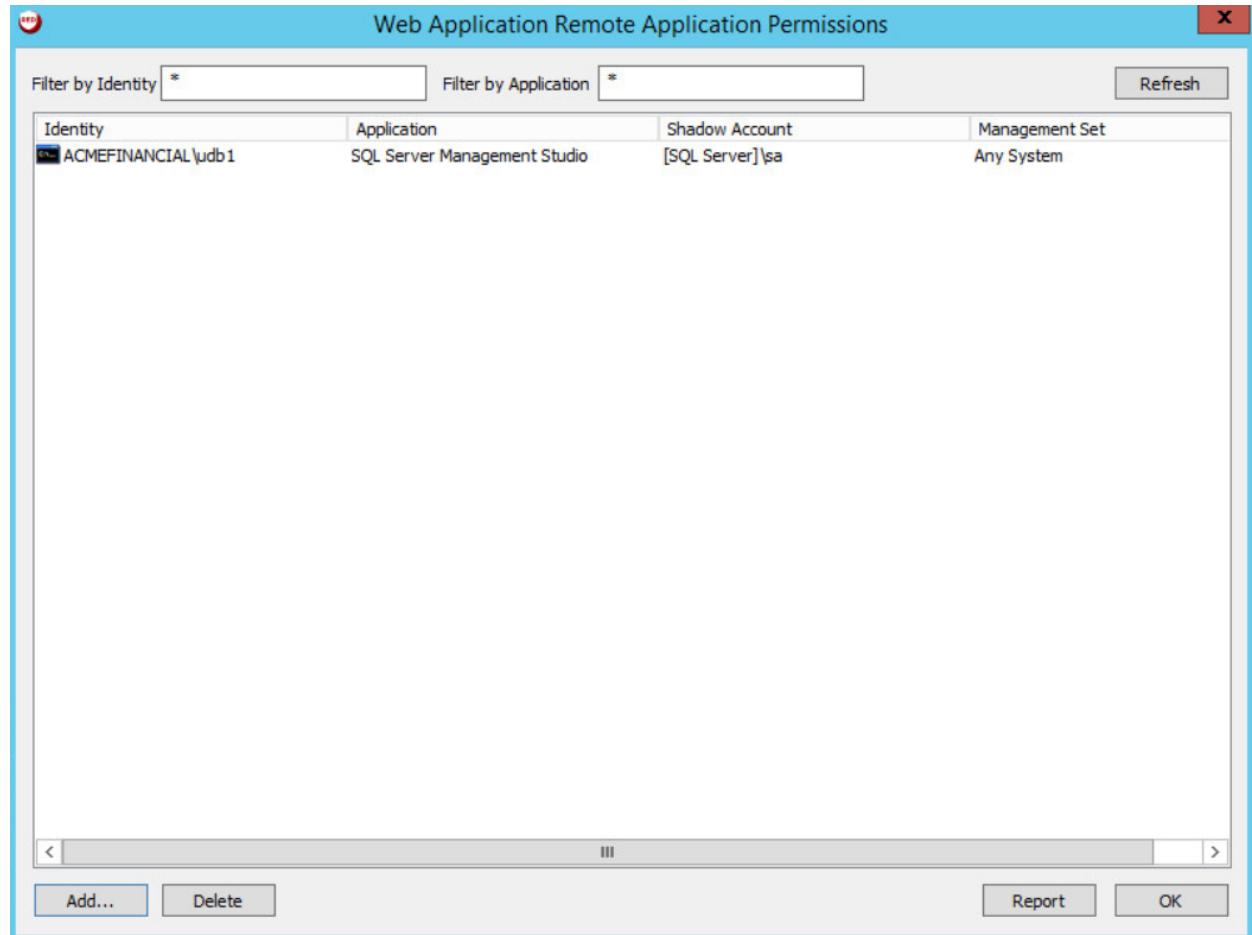
462

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

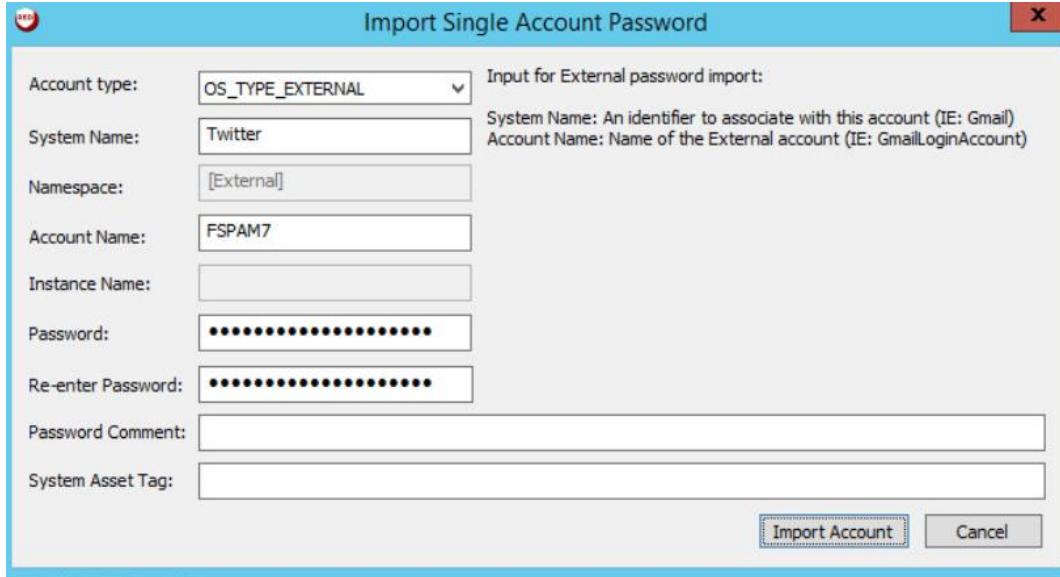
## 2.2.9 Configuring Twitter Account Launching

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.

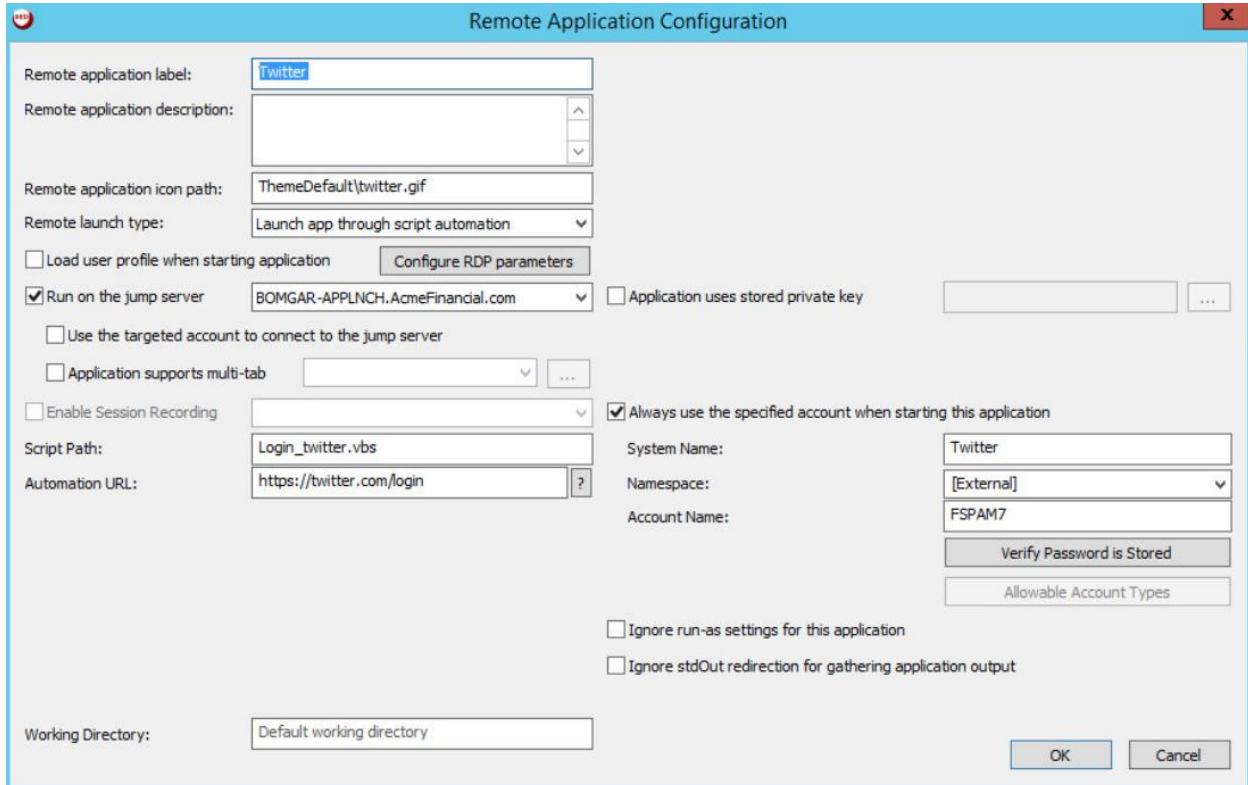
474 To launch Twitter, Bomgar-PI needs the Twitter account password. The following steps detail how to  
475 add an external password to Bomgar-PI:

- 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.

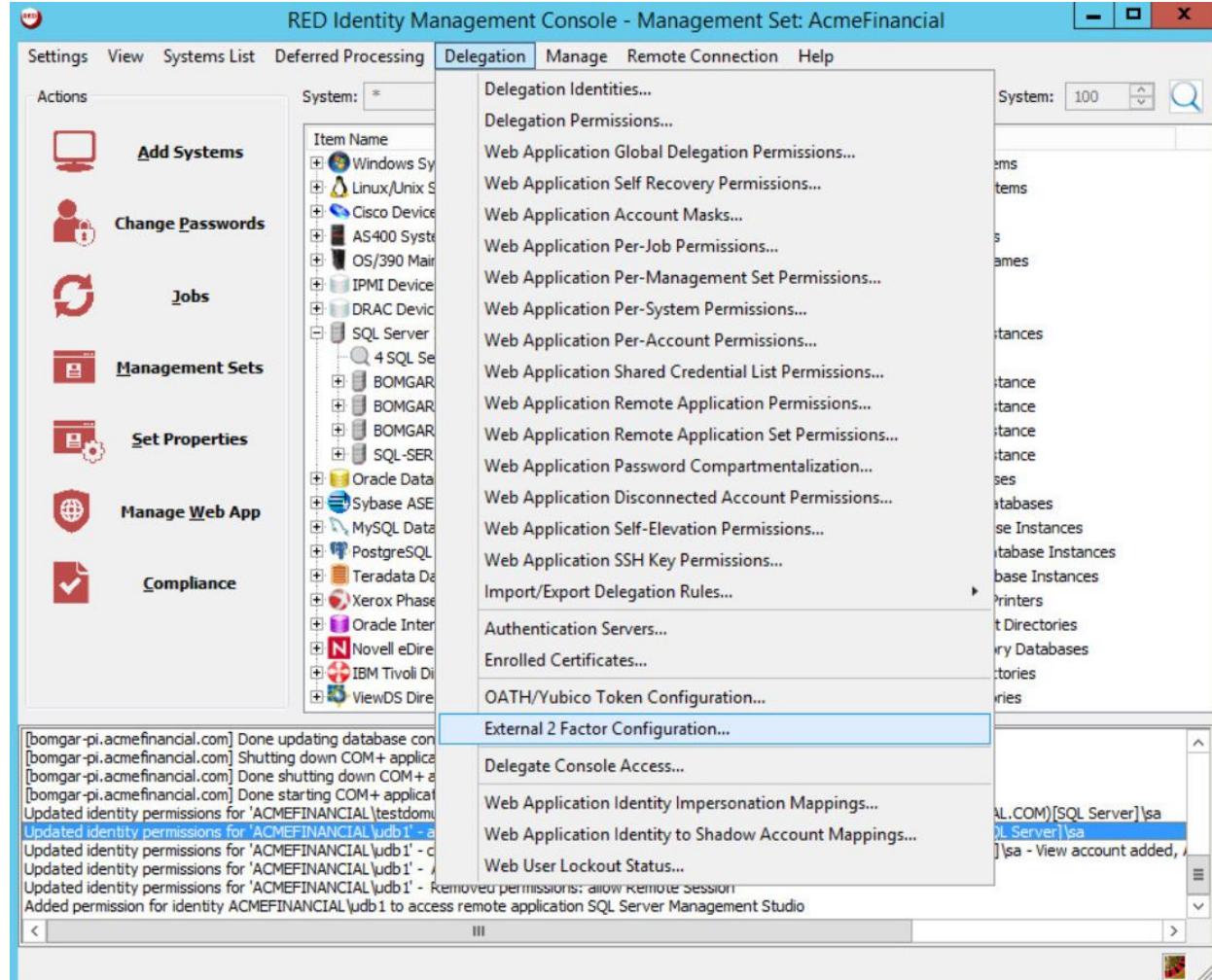
501 To allow users to launch Twitter, follow these steps:

- 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**.

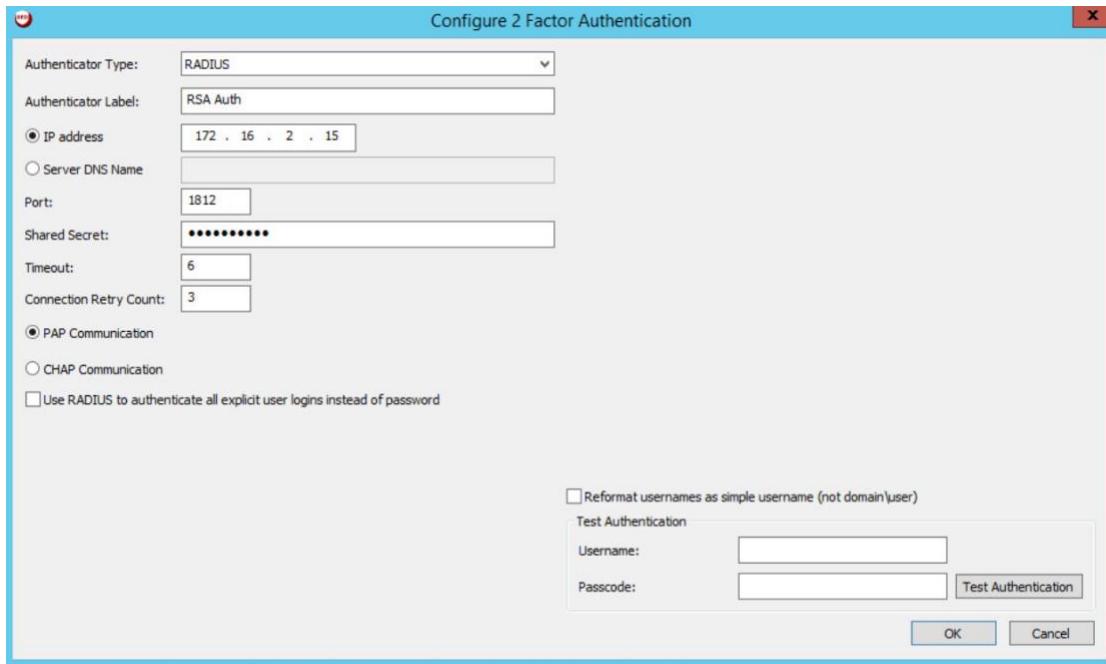


516

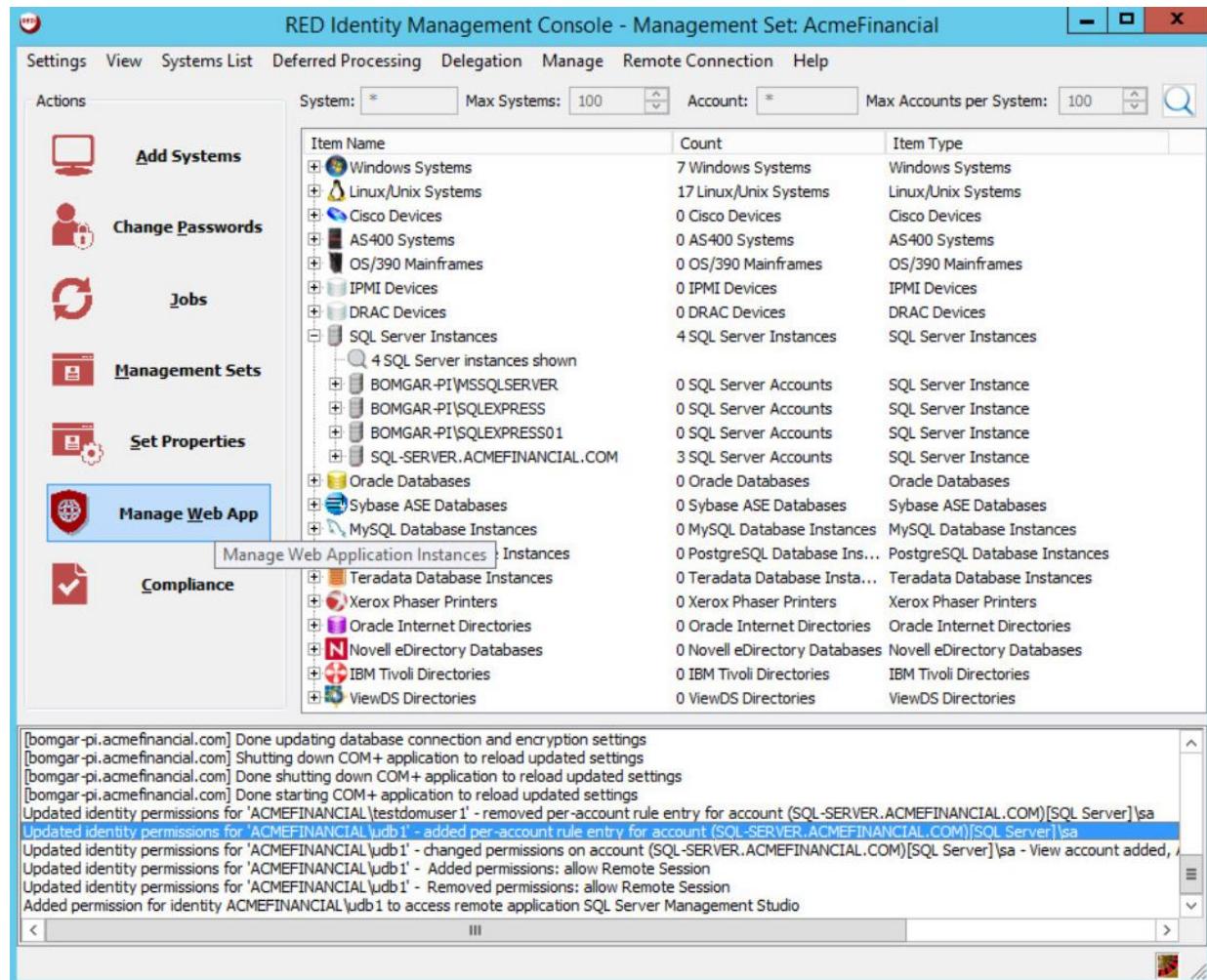
- 517 2. Fill out the **Configure 2 Factor Authentication** window with the following settings:

- 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.

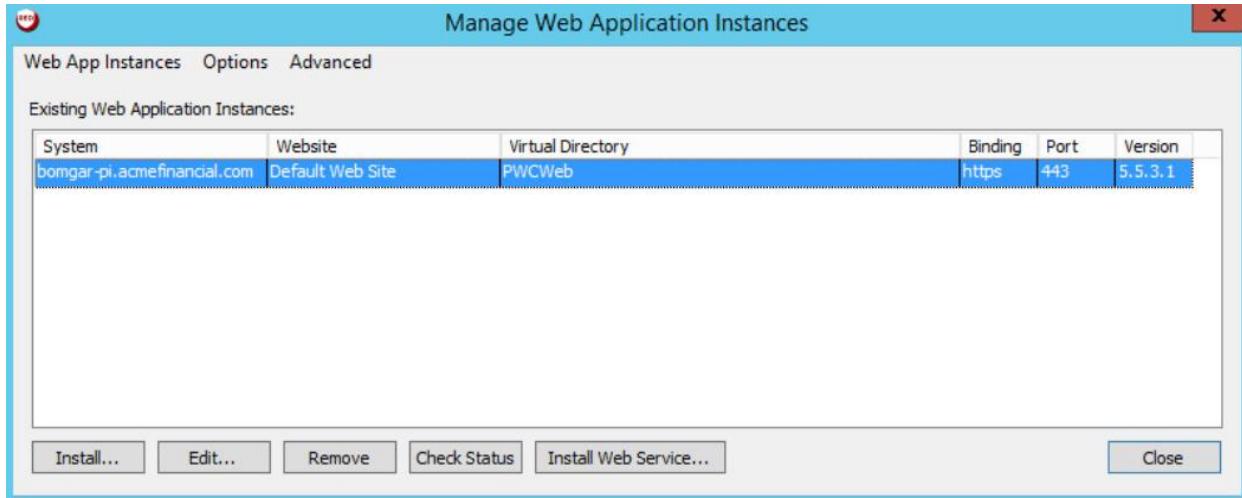


- 526
- 527       3. Click **OK**.
- 528       4. Click **Manage Web App**.

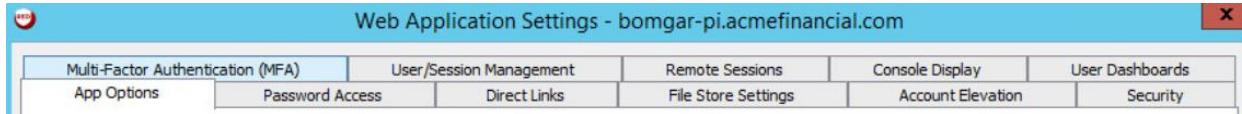


529

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

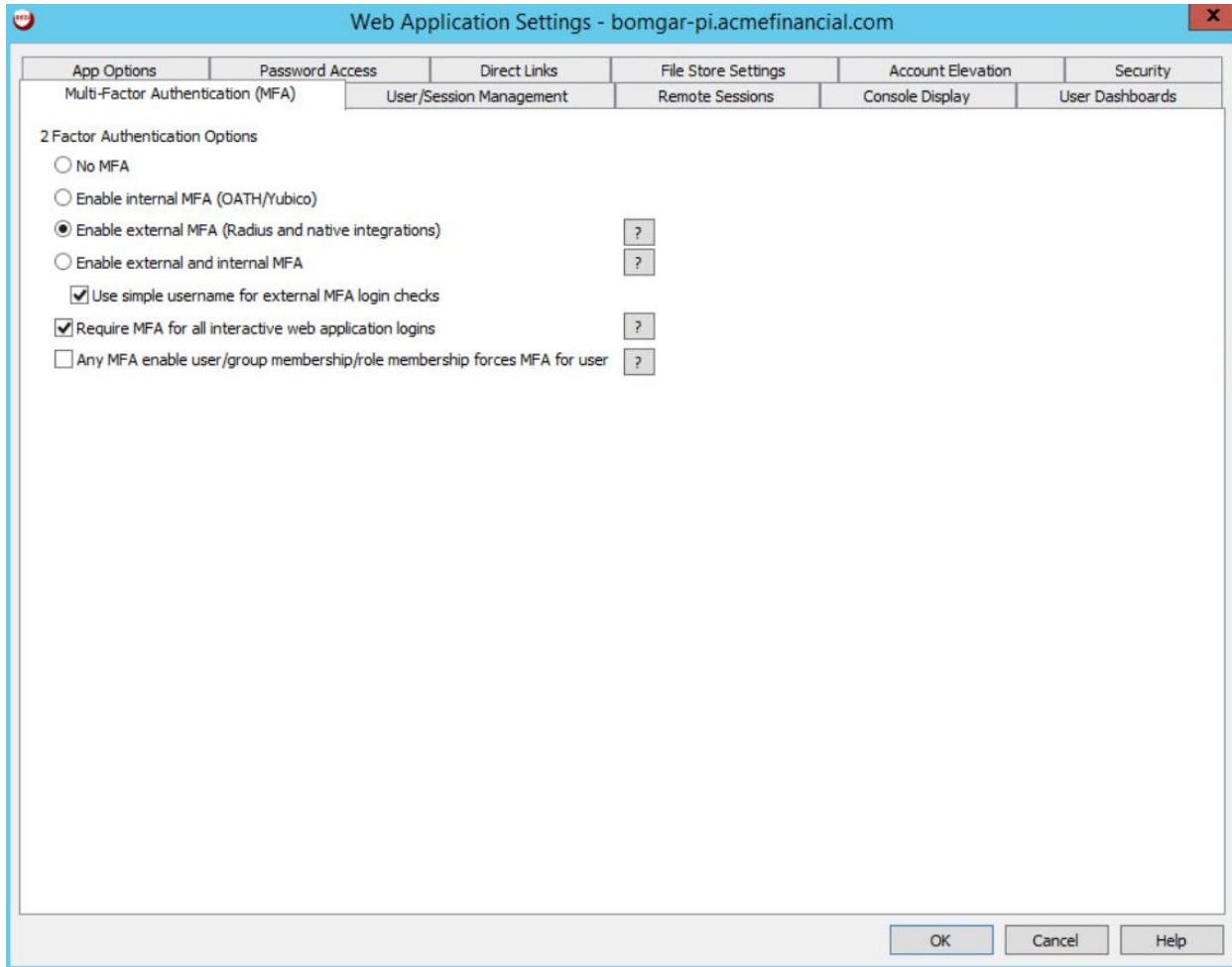


531

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

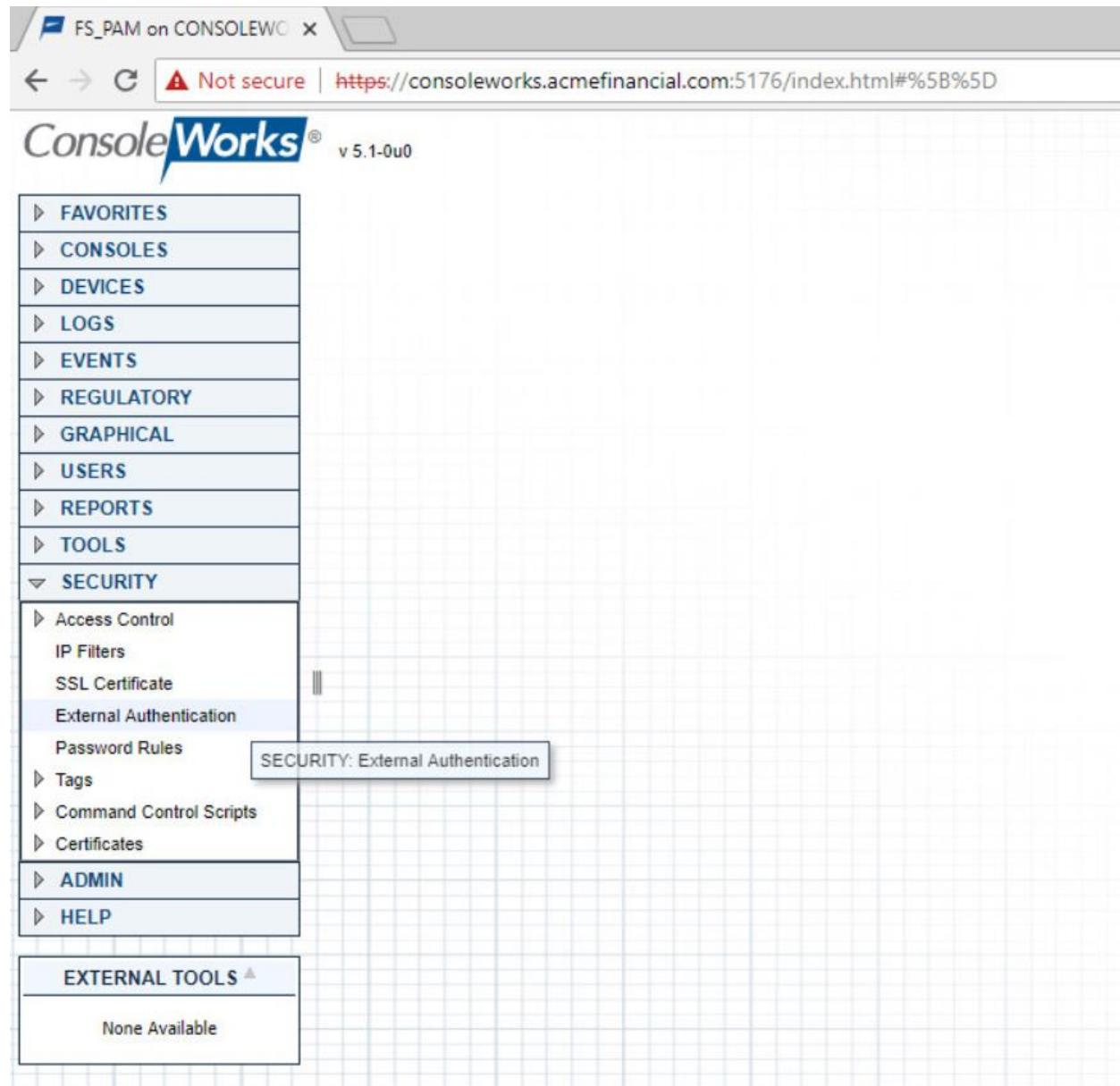
### 567     2.3.3 Installation

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.



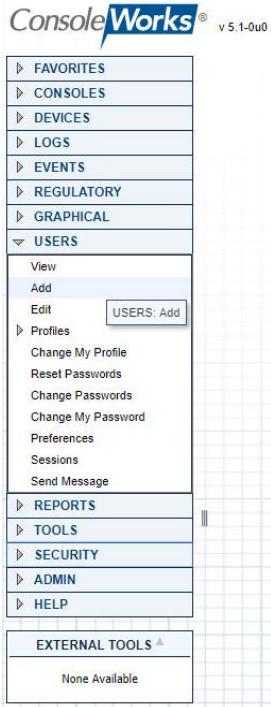
593

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

### 595 2.3.5 Creating Users

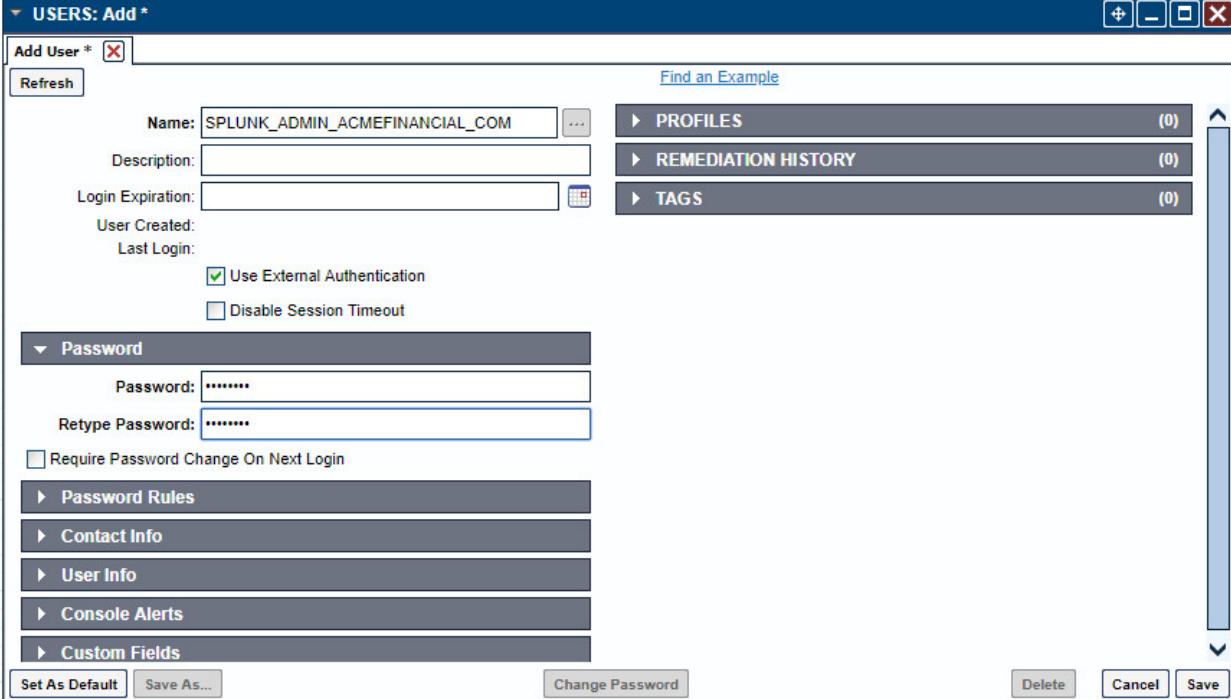
596        Each privileged user must have an account in ConsoleWorks to log into ConsoleWorks. The following  
597        steps detail the process of creating accounts for AD users in ConsoleWorks. For this example, we will  
598        create a ConsoleWorks account for the [splunk\\_admin@acmefinancial.com](mailto:splunk_admin@acmefinancial.com) 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 style="border: 1px solid #ccc; padding: 2px 5px;" type="button" value="..."/> <input style="border: 1px solid #ccc; padding: 2px 5px;" type="button" value="..."/>
Nickname:	<input type="text"/>	
Description:	Web Console for pfSense	
Status:	<input type="radio"/> - <input checked="" type="radio"/> Enable	
Device:	<input type="text"/> <down arrow="" style="font-size: small; vertical-align: middle;"></down>	
Connector:	<input type="text"/> <down arrow="" style="font-size: small; vertical-align: middle;"></down>	
<b>Connection Details</b>		
Bind Name:	<input type="text"/> <down arrow="" style="font-size: small; vertical-align: middle;"></down>	
Host Header:	<input type="text"/> pfsenseweb.acmefinancial.com	
URL:	<input type="text"/> https://172.16.4.1	
Relative URL:	<input type="text"/> <input type="button" value="Open"/> <input type="checkbox"/> Disable Standard Translations	
Log Web Traffic:	<input type="text"/> <down arrow="" style="font-size: small; vertical-align: middle;"></down>	
Profile:	<input type="text"/> <down arrow="" style="font-size: small; vertical-align: middle;"></down>	

Set As Default
Save As...
Delete
Cancel
Save

**▶ GROUPS (0)**  
**▶ SCANS (0)**  
**▶ AUTOMATIC ACTIONS (0)**  
**▶ ACKNOWLEDGE ACTIONS (0)**  
**▶ PURGE ACTIONS (0)**  
**▶ ADDITIONAL BINDS (0)**  
**▶ REMEDIATION HISTORY (0)**  
**▶ SCHEDULES + EVENTS (0)**  
**▶ TAGS (0)**  
**▶ BASELINES + SCHEDULES (0)**  
**▶ BASELINE RUNS (0)**  
**▶ GRAPHICAL CONNECTIONS (0)**

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 main input area, 'Name' is set to 'SPLUNK\_ADMIN' and 'Description' is 'Admins of Splunk's OS'. To the right, a list titled 'USERS' shows one entry: 'SPLUNK\_ADMIN\_ACMEFINANCIAL\_COM'. Below the list are 'Add', 'Remove', and 'View' buttons. At the bottom, there are 'Custom Fields' and 'TAGS' sections, each with '(0)' next to it. Action buttons at the bottom include 'Set As Default', 'Save As...', '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** chosen) to create profiles for each group of users who should have access to a specific set of consoles. In  
700 this case, it was Splunk OS-level consoles. Next, it could be Splunk application-level consoles.  
701

### 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 shown in the following screenshot. Click **Save**.

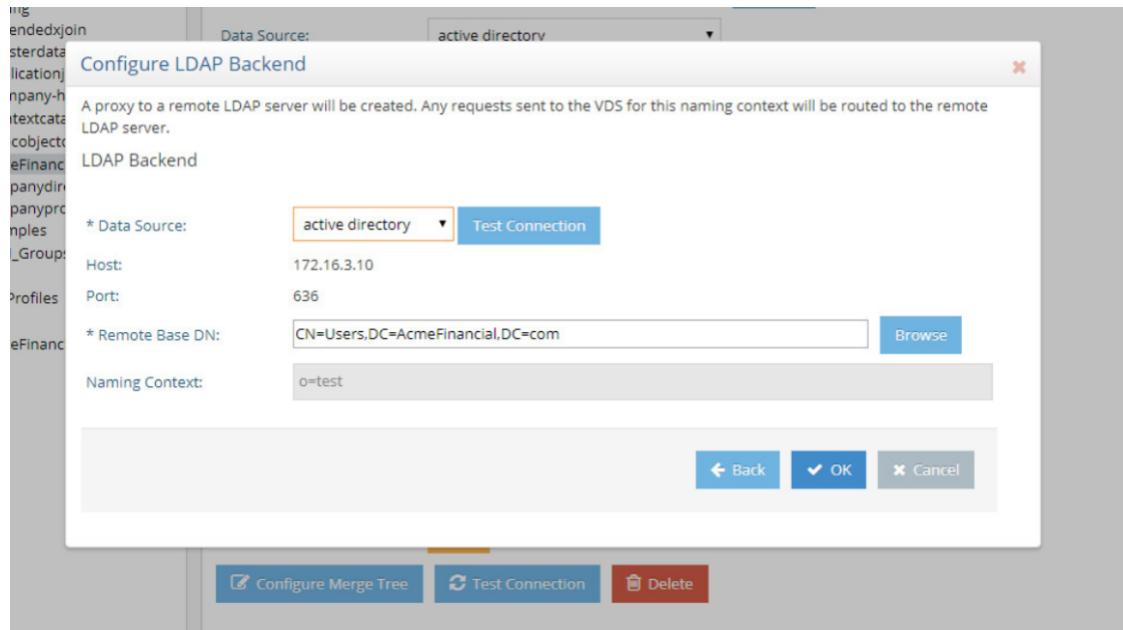
804

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

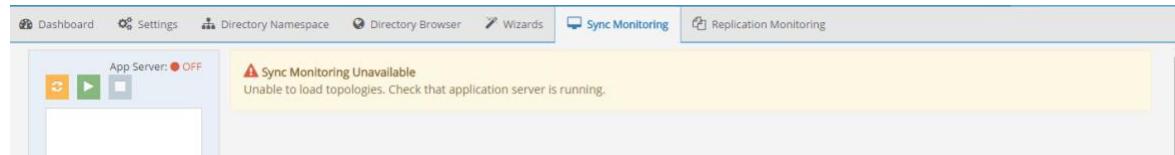


813

## 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.



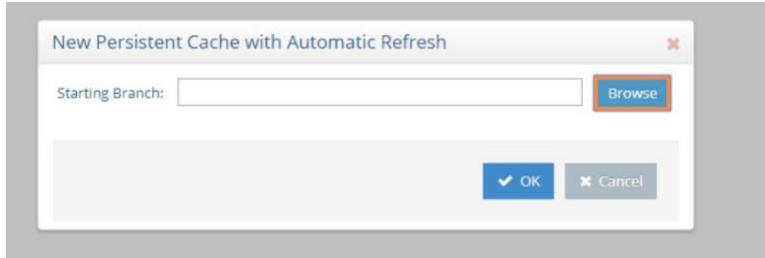
819

- 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.

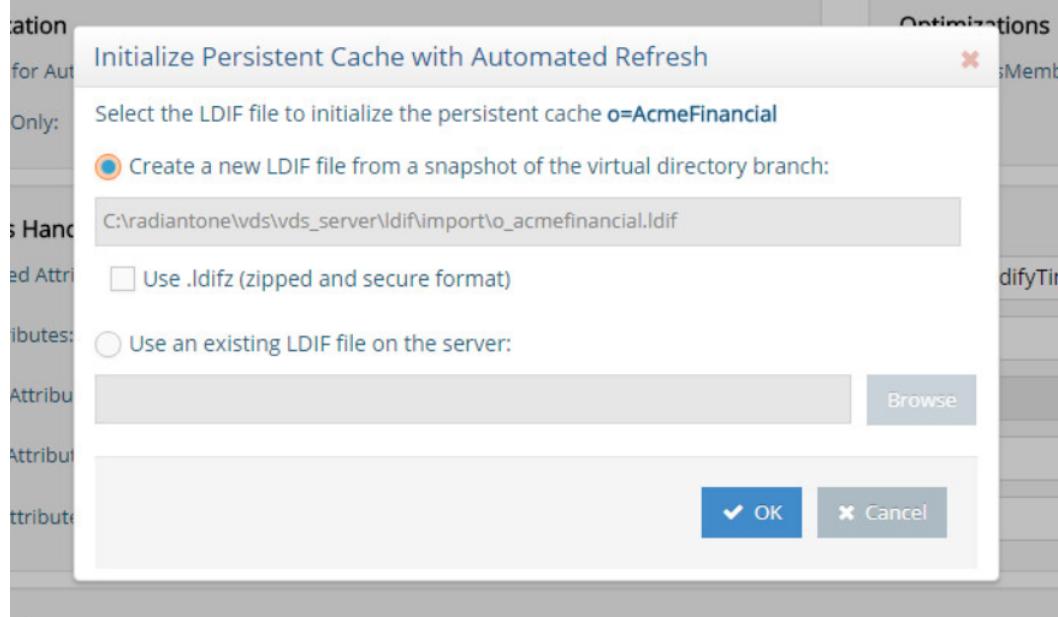
822

- 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.

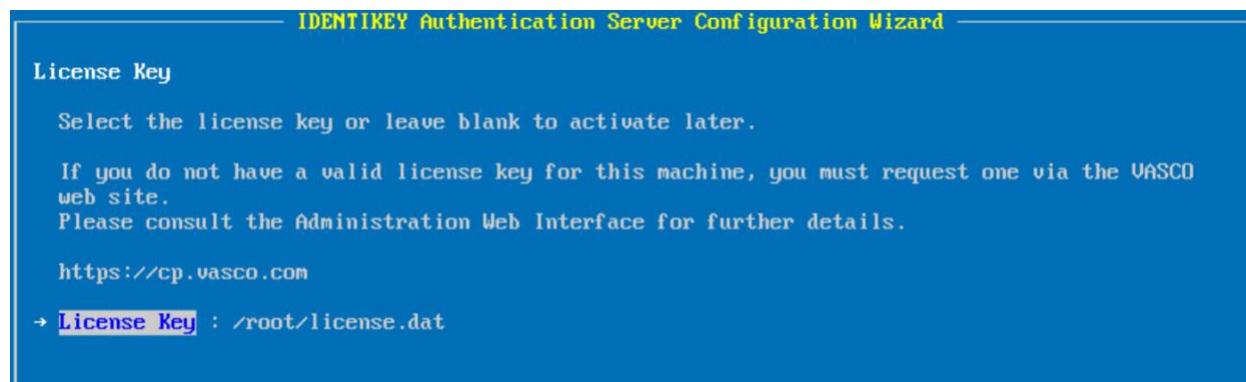
- 948 4. Accept the licenses.

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

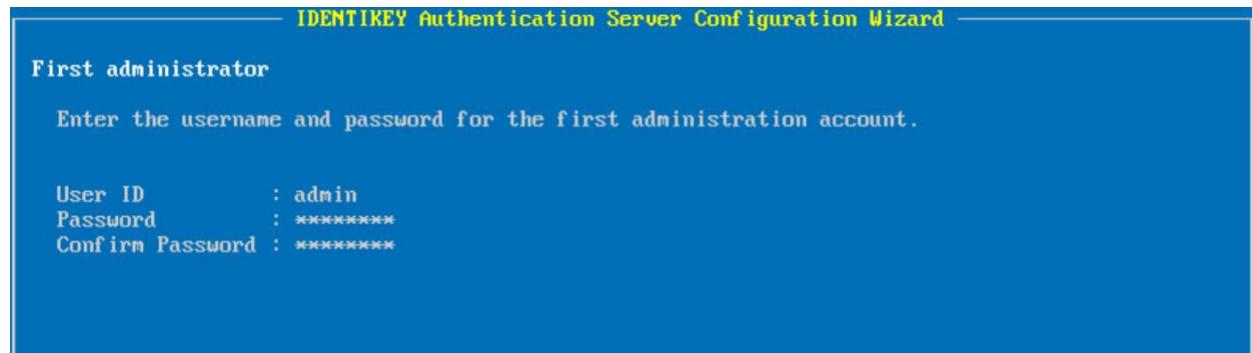
950 **2.7.5 Configuration**

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.

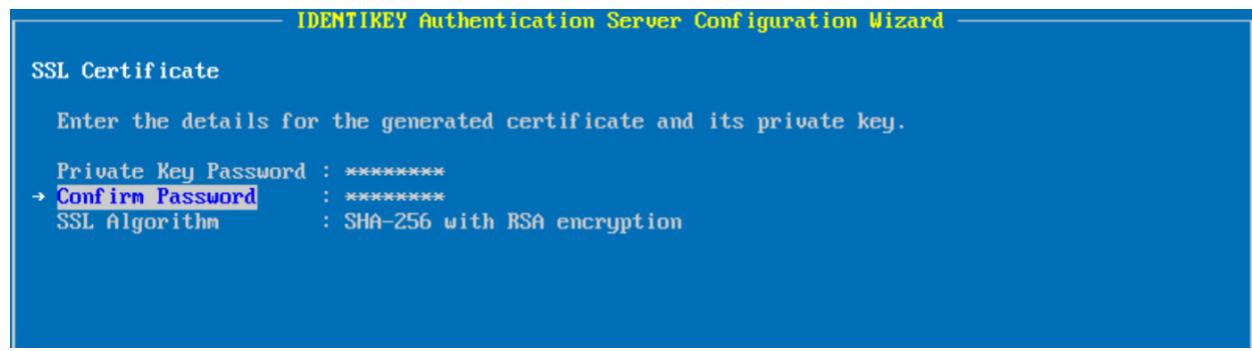


- 955
- 956 4. Accept the server functionality, and then select **Next**.
  - 957 5. Create a username and password for the first admin account, and then select **Next**.



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 labeled 'FIND' with a dropdown menu showing 'Users' and 'DIGIPASS', and a 'SEARCH' button. 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**.
- 985

**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
<b>Edit Policy Settings</b>	<b>Current Effective Settings</b>							
<b>Description</b>	2-Factor Authentication Local Digipass Back-end Active Directory							
<b>Local/Back-End Authentication</b>								
<b>Local Authentication</b>	Digipass Only	(None)						
<b>Back-End Authentication</b>	Always	(Always)						
<b>Back-End Protocol</b>	Microsoft Active Directory							
	<b>SAVE</b>	<b>CANCEL</b>						

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

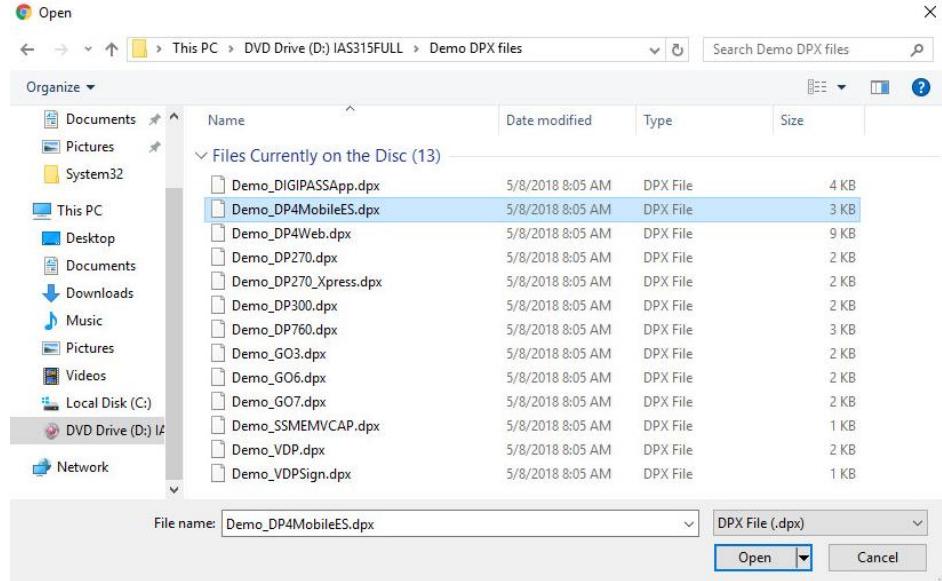
990

### 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    4. Click **UPLOAD**.

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

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

1004    7. Click **IMPORT**.

1005    8. Choose to run the task immediately.

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

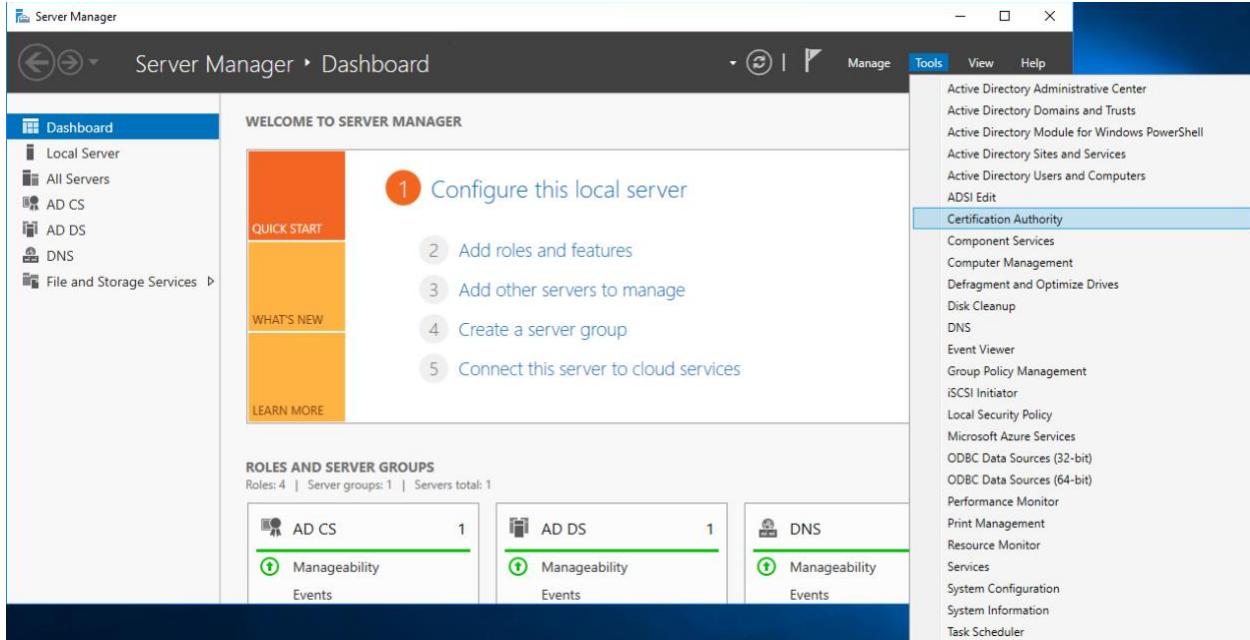
1007   With Radiant Logic configured to replicate users and groups from AD, OneSpan can use Radiant Logic as  
1008   an AD back-end. This works, as OneSpan connects to Radiant by using LDAP over SSL, and Radiant Logic  
1009   contains a virtual directory that presents like AD.

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

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

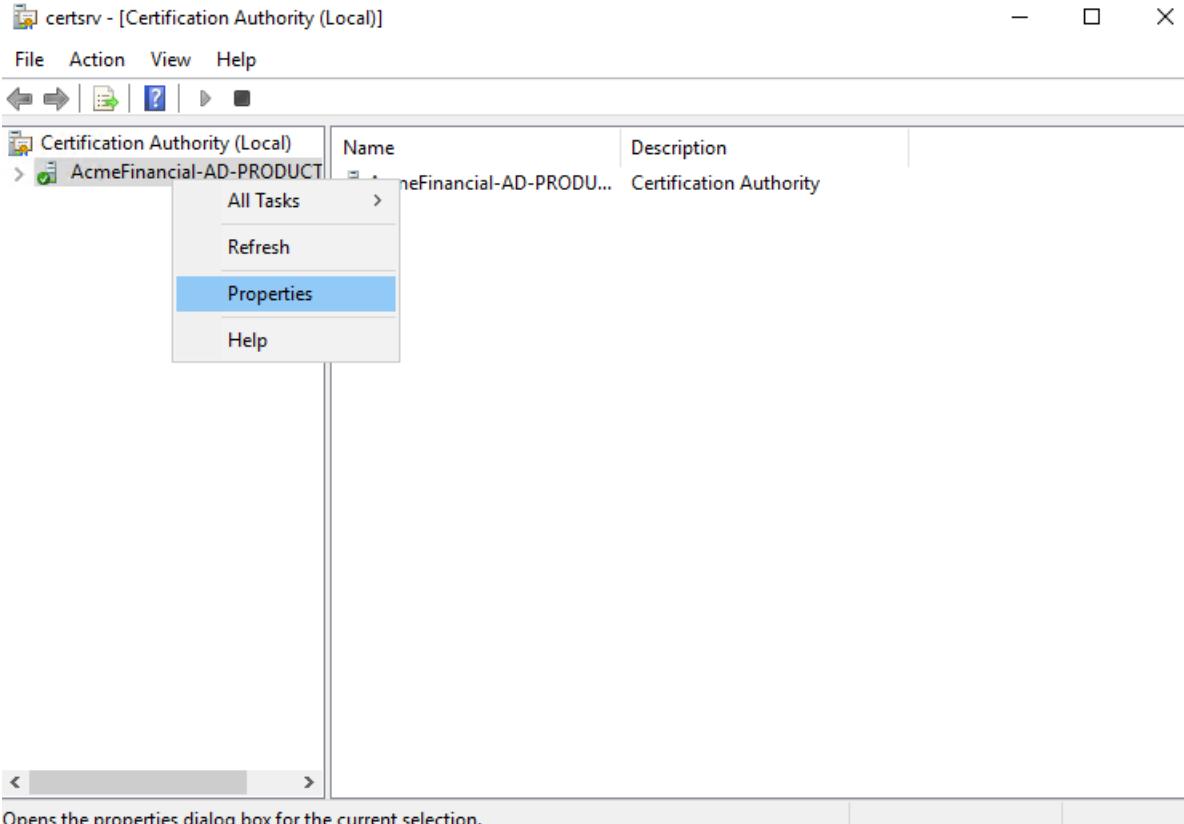
1015    1. On AD-PRODUCTION, the AD Domain Controller, open **Server Manager**.

- 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.

<b>Client Type *</b>	IDENTIKEY User Websites
<b>Location *</b>	172.16.2.208
<b>Policy ID *</b>	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
<b>Protocol ID</b>	SOAP
<b>Shared Secret</b>	
<b>Confirm Shared Secret</b>	
<b>Character Encoding</b>	
<b>Enabled</b>	<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.

<b>Client Type *</b>	<input type="text" value="UWS MDL Provisioning"/>
<b>Location *</b>	<input type="text" value="172.16.2.208"/>
<b>Policy ID *</b>	<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
<b>Protocol ID</b>	<input type="text" value="SOAP"/>
<b>Shared Secret</b>	<input type="text"/>
<b>Confirm Shared Secret</b>	<input type="text"/>
<b>Character Encoding</b>	<input type="text"/>
<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>CREATE</b> <b>CANCEL</b>	

- 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:

1134        **apt-get -y install chrony**

1135        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 is 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        server 172.16.3.10

1138        8. Restart the chrony service as shown below:

1139        **systemctl restart chrony**

1140        9. Request an AD domain join by using a domain admin account or a user with appropriate
1141              privileges. Perform the domain join by running the following commands:

1142              a. kinit administrator@ACMEFINANCIAL.COM

1143              b. Enter the password when prompted.

1144              c. realm -v join acmefinancial.com -user-principal =
1145                          yourlinuxhost.acmefinancial.com/administrator@ACMEFINANCIAL.COM

1146              d. systemctl restart realmd

1147        10. Set fallback-homedir = /home/%u/%d to create Linux home directories for domain users, and
1148              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...
<b>Log on as a service</b>	<b>ACMEFINANCIAL\dbserver1svc...</b>
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
<b>Service Account Credentials</b>	
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**.

1324

## 2.11.6 Adding New Users

- 1325 1. Once logged in, navigate to **Configure > Server > Add User/Group**.
- 1326 2. In the search bar, type the name of the domain user, and then click **Add User/Group**.

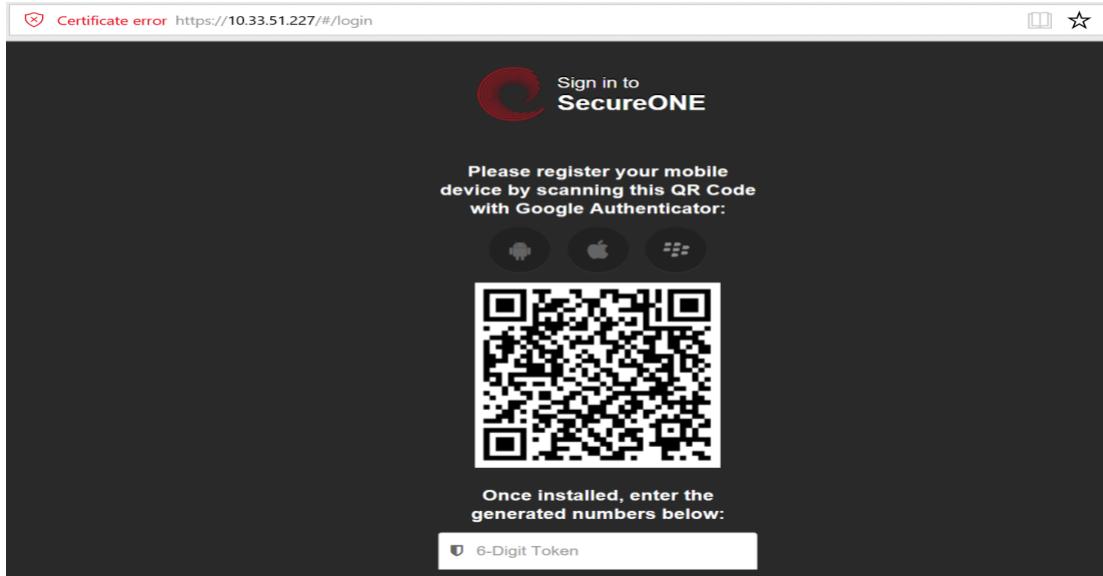
1327

Showing 1 to 4 of 4 entries

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

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 and scan modes 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**.

This screenshot is similar to the previous one but includes additional buttons at the bottom: 'Extend Session' and 'Expire Session'. The rest of the interface and data are identical to the first screenshot, showing the system details for WIN10CLIENT1 and the list of administrator accounts with their respective properties and expiration dates.

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.

The screenshot shows a web browser window with the URL <https://10.33.51.229/login.jsp>. The page title is "RSA Authentication Manager". The main content area is titled "RSA Authentication Manager Quick Setup". It displays a welcome message: "Welcome to RSA Authentication Manager Quick Setup. Use Quick Setup to configure the primary and replica appliances." Below this is a form field labeled "Quick Setup Access Code" with the placeholder "Enter Quick Setup Access Code:" followed by an empty input field and a "What is this?" link. A blue "Next" button is visible. At the bottom right, there is a copyright notice: "Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved."

1361

1362

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

The screenshot shows the "RSA Authentication Manager Quick Setup" page. It features two main sections: "Primary Quick Setup" and "Replica Quick Setup". The "Primary Quick Setup" section contains a link to "Start Primary Quick Setup" and a note: "Configure a primary appliance, unless there is one already configured on your network. A primary appliance is where all authentication and administrative actions occur." The "Replica Quick Setup" section contains a link to "Start Replica Quick Setup" and a note: "If you have already configured a primary appliance, RSA recommends that you configure one or more replica appliances for high availability and load balancing." Both sections include a "What is this?" link.

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, it 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](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.

User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
Administrator	Not Provided	No	No	SystemDomain	AD-PRODUCTION
		Yes	Yes	SystemDomain	Identity Source

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**.

Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	Expires On	Replaced By Token	Security Domain
00000000000006	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000007	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000008	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000009	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000010	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000011	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000012	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
00000000000013	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain

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](https://www.splunk.com/page/sign_up).

1422 Download Splunk Enterprise from [https://www.splunk.com/en\\_us/download/splunk-enterprise.html](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>.
1462

**1463 Appendix A List of Acronyms**

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

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