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.


FEEDBACK

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

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

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

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

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

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

**KEYWORDS**

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

**ACKNOWLEDGMENTS**

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dan Morgan</td>
<td>Bomgar (formerly Lieberman Software)</td>
</tr>
<tr>
<td>David Weller</td>
<td>Bomgar (formerly Lieberman Software)</td>
</tr>
<tr>
<td>Oleksiy Bidniak</td>
<td>Ekran System</td>
</tr>
<tr>
<td>Oleg Shomonko</td>
<td>Ekran System</td>
</tr>
<tr>
<td>Karl Kneis</td>
<td>IdRamp</td>
</tr>
<tr>
<td>Eric Vinton</td>
<td>IdRamp</td>
</tr>
<tr>
<td>Michael Fagan</td>
<td>NIST</td>
</tr>
<tr>
<td>Will LaSala</td>
<td>OneSpan (formerly VASCO)</td>
</tr>
<tr>
<td>Michael Magrath</td>
<td>OneSpan (formerly VASCO)</td>
</tr>
<tr>
<td>Jim Chmura</td>
<td>Radiant Logic</td>
</tr>
<tr>
<td>Don Graham</td>
<td>Radiant Logic</td>
</tr>
<tr>
<td>Timothy Keeler</td>
<td>Remediant</td>
</tr>
<tr>
<td>Paul Lanzi</td>
<td>Remediant</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Technology Partner/Collaborator</th>
<th>Build Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bomgar</strong> (formerly Lieberman Software)</td>
<td>Red Identity Suite</td>
</tr>
<tr>
<td><strong>Ekran System</strong></td>
<td>Ekran System Client</td>
</tr>
<tr>
<td><strong>IdRamp</strong></td>
<td>Secure Access</td>
</tr>
<tr>
<td><strong>OneSpan</strong> (formerly VASCO)</td>
<td>DIGIPASS</td>
</tr>
<tr>
<td><strong>Radiant Logic</strong></td>
<td>RadiantOne FID</td>
</tr>
<tr>
<td><strong>Remediant</strong></td>
<td>SecureONE</td>
</tr>
<tr>
<td><strong>RSA</strong></td>
<td>SecureID Access</td>
</tr>
<tr>
<td>Technology Partner/Collaborator</td>
<td>Build Involvement</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Splunk</td>
<td>Splunk Enterprise</td>
</tr>
<tr>
<td>TDi Technologies</td>
<td>ConsoleWorks</td>
</tr>
</tbody>
</table>
Contents

1 Introduction ..................................................................................................................1
  1.1 Practice Guide Structure .......................................................................................1
  1.2 Build Overview .......................................................................................................2
  1.3 Typographic Conventions .......................................................................................3

2 Product Installation Guides .........................................................................................3
  2.1 Microsoft Active Directory ....................................................................................3
    2.1.1 How It’s Used ..................................................................................................3
    2.1.2 Virtual Machine Configuration .....................................................................3
    2.1.3 Installation .....................................................................................................4
    2.1.4 DNS Configuration .......................................................................................4
    2.1.5 Group Policy Object Configuration .............................................................5
    2.1.6 Scripts ..........................................................................................................5
    2.1.7 Splunk Universal Forwarder ..........................................................................8
  2.2 Bomgar Privileged Identity ......................................................................................8
    2.2.1 How It’s Used ..................................................................................................8
    2.2.2 Virtual Machine Configuration .....................................................................8
    2.2.3 Prerequisites ..................................................................................................9
    2.2.4 Installing Privileged Identity ........................................................................9
    2.2.5 Configuration ................................................................................................13
    2.2.6 Installing Privileged Identity Application Launcher .....................................16
    2.2.7 Configure Bomgar Privileged Identity with IdRamp SAML Authentication ...17
    2.2.8 Configuring Microsoft SQL Server Access .......................................................20
    2.2.9 Configuring Twitter Account Launching ........................................................33
    2.2.10 Configuring Multifactor Authentication with RSA .....................................36
    2.2.11 Splunk Universal Forwarder ........................................................................40
  2.3 TDi ConsoleWorks ..................................................................................................41
    2.3.1 How It’s Used ..................................................................................................41
    2.3.2 Virtual Machine Configuration .......................................................................41
2.7.4 Installation ........................................................................................................... 66
2.7.5 Configuration ........................................................................................................ 66
2.7.6 Creating a Domain and Policies ............................................................................ 68
2.7.7 Importing DIGIPASSes .......................................................................................... 72
2.7.8 Configuring to Use Radiant Logic as a Back-End Authentication Server ............ 73
2.7.9 Integration with TDi ConsoleWorks ....................................................................... 77
2.7.10 Installing User Websites ..................................................................................... 77
2.7.11 Creating Component Records in IDENTIKEY Authentication Server ............... 78
2.8 Base Linux OS ........................................................................................................ 80
  2.8.1 Virtual Machine Configuration ......................................................................... 80
  2.8.2 Domain Join Configuration ................................................................................. 81
2.9 Microsoft SQL Server Installation on Ubuntu Linux .............................................. 83
  2.9.1 How It’s Used ...................................................................................................... 83
  2.9.2 Virtual Machine Configuration ......................................................................... 83
  2.9.3 Firewall Configuration ....................................................................................... 84
  2.9.4 Installation and Initial Configuration ................................................................. 84
2.10 Samba File Server ................................................................................................ 86
  2.10.1 How It’s Used ................................................................................................... 86
  2.10.2 Virtual Machine Configuration ....................................................................... 86
  2.10.3 Firewall Configuration ..................................................................................... 87
  2.10.4 Installation and Configuration .......................................................................... 87
2.11 Remediant SecureONE .......................................................................................... 89
  2.11.1 How It’s Used ................................................................................................... 89
  2.11.2 Virtual Machine Configuration ....................................................................... 89
  2.11.3 Installation and Initial Configuration ............................................................... 90
  2.11.4 Domain Configuration .................................................................................... 90
  2.11.5 Managing Systems ........................................................................................ 91
  2.11.6 Adding New Users ......................................................................................... 92
  2.11.7 Requesting Privileged Access to Protected System ........................................ 93
2.12 RSA Authentication Manager ................................................................................. 95
  2.12.1 How It’s Used .................................................................................................. 95
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.12.2</td>
<td>Installation and Initial Configuration</td>
<td>95</td>
</tr>
<tr>
<td>2.12.3</td>
<td>LDAP Integration</td>
<td>98</td>
</tr>
<tr>
<td>2.12.4</td>
<td>Token Assignment</td>
<td>99</td>
</tr>
<tr>
<td>2.12.5</td>
<td>Software Token Profiles and Token Distribution</td>
<td>100</td>
</tr>
<tr>
<td>2.13</td>
<td>Splunk</td>
<td>101</td>
</tr>
<tr>
<td>2.13.1</td>
<td>How It’s Used</td>
<td>101</td>
</tr>
<tr>
<td>2.13.2</td>
<td>Installation</td>
<td>101</td>
</tr>
<tr>
<td>2.13.3</td>
<td>Queries</td>
<td>101</td>
</tr>
<tr>
<td>2.13.4</td>
<td>DemoBomgar-AD-Auth-UnauthV1</td>
<td>101</td>
</tr>
<tr>
<td>2.13.5</td>
<td>DemoRadiant-AD-Event-Details</td>
<td>102</td>
</tr>
<tr>
<td>2.13.6</td>
<td>SSL Forwarding</td>
<td>102</td>
</tr>
<tr>
<td>Appendix A</td>
<td>List of Acronyms</td>
<td>103</td>
</tr>
</tbody>
</table>
1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

- NIST Special Publication (SP) 1800-18A: Executive Summary
- NIST SP 1800-18C: How-To Guides – instructions for building the example solution (you are here)

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

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

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

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

- Section 3.4, Risk, provides a description of the risk analysis we performed
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices
You might share the Executive Summary, NIST SP 1800-18A, with your leadership team members to help them understand the importance of adopting standards-based PAM.

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

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

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

### 1.2 Build Overview

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

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

The following table presents typographic conventions used in this volume.

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

2 Product Installation Guides

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

2.1 Microsoft Active Directory

2.1.1 How It’s Used

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

2.1.2 Virtual Machine Configuration

The Microsoft AD virtual machine is configured as follows:

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

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-

2.1.4  **DNS Configuration**
196  1.  Create the host records and reverse entries in the AcmeFinancial.com DNS service for the 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
2.1.5 Group Policy Object Configuration

1. Open Group Policy Management.

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

2.1.6 Scripts

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

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

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

NIST SP 1800-18C: Privileged Account Management for the Financial Services Sector
The following PowerShell script extracts data from the Windows security event log and executes the Python script above:

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

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

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

![inputs.conf](image)

2.2 Bomgar Privileged Identity

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

2.2.1 How It’s Used

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

2.2.2 Virtual Machine Configuration

The Privileged Identity virtual machine is configured as follows:

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

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

2.2.3 Prerequisites

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

2.2.4 Installing Privileged Identity

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

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

5. Fill out the **Distinguished Name Properties**, and then click **Next**.

6. Select a bit length of **2048**, and then click **Next**.

7. Give the certificate a file name, and then click **Finish**.

8. Using the `certreq` command in the **Command Prompt**, enter `certreq -attrib

9. Select the certificate file that was created in Step 7, and then click **Open**.
10. Choose the Domain Controller CA from the **Certification Authority List**, and then click **OK**.
11. Go back to the **IIS Manager**, and click **Bomgar-PI**. Select **Server Certificates**.

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

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.
14. Click OK

15. Create a Secure Sockets Layer (SSL) binding with that certificate by following [documentation from Microsoft](#).

You are now ready to begin following further installation instructions that are publicly available on Bomgar’s [website](#).

### 2.2.5 Configuration

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

#### 2.2.5.1 Management Set

1. Create a new management set for the AD domain.

2. Configure the management set to include systems by querying AD.

3. Configure the management set to scan for the target type by scanning for a Secure Shell (SSH) server. Set the default to Windows if there is no match.
4. Configure the management set to have a second inclusion from a **Static list of targets**, and include the domain name **(AcmeFinancial.com)**. Manually set the target type to Windows.

5. Set the management set to update dynamically each day.
2.2.5.2 Delegation Identities

To allow a user to have access to the web console, a Delegation Identity must be created for that user. Add the following users as Delegation Identities by following the steps provided below:

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

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

3. Click OK.

2.2.6 Installing Privileged Identity Application Launcher

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

Using the Bomgar documentation, complete the following steps:

1. Create a new virtual machine:
   a. Windows Server 2012 R2
   b. 1 CPU core
   c. 4 GB of RAM
   d. 60 GB of storage
   e. 1 NIC
      i. IPv4: manual
      ii. IPv6: disabled
      iii. IPv4 address: 172.16.1.31
      iv. Netmask: 255.255.255.0
      v. Gateway: 172.16.1.1
      vi. DNS-search domains: N/A

2. Install Remote Desktop Services.

3. DO NOT install Desktop Experience.

4. Install Application Launcher without Session Recording.

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

2.2.7 Configure Bomgar Privileged Identity with IdRamp SAML Authentication

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

1. Open the Bomgar RED Identity Management Console desktop application.
2. Navigate to Delegation > Web Application Global Delegation Permissions.
3. Click Add at the lower left corner.
4. Select Role-Based Mapping, enter a friendly name in the field, and then click OK.
5. Select the role that you just created, and then click **Assign Role**.

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.

7. Click **OK**.

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

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

11. Select SAML authentication on the login page, click **Login**, and then follow the authentication prompts.
2.2.8 Configuring Microsoft SQL Server Access

Prerequisites:

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

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

1. Open the Bomgar RED Identity Management Console on Bomgar-PI. Right-click **SQL Server Instances**, and then select **Add SQL Server Instance**.
2. Fill out the **SQL Server Instance Settings**. Enter the host name of the SQL Server in the **System Name** field. Populate the **Login Account Name** and **Login Account Password** fields with the username and password of the *sa* account. Note: This will work only if hybrid authentication is enabled on the SQL Server.

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

4. Expand **SQL Server Instances** by clicking on the plus sign to the left of the item name, and then expand **SQL-SERVER.ACMEFINANCIAL.COM**. Right-click the *sa* account, and then select **Change Password**.
5. Select strong password policy options, such as increasing both the length of the password and its compliance with password standards.

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

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

8. Click Delegation > Web Application Identity to Shadow Account Mappings.
9. Click **Add Mapping**.
10. Choose the ACMEFINANCIAL\udb1 account, and then click OK. Choose the sa account from the list on the next screen, and then click OK.

11. Click OK again.
12. Click Delegation > Web Application Per-Account Permissions.

13. Right-click the sa account, and then select Edit Managers for Account.
14. Click **Add Identity to List**.
15. Select the ACMEFINANCIAL\udb1 account. You should see it appear in the list. Click OK.
16. Expand the sa account by clicking the plus sign to the left, right-click the ACMEFINANCIAL\udb1 account, and then select Edit Permissions of Manager.

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

18. Click Delegation > Web Application Remote Application Permissions.
19. Click **Add**.
20. Select the **ACMEFINANCIAL\udb1** account from the list of **Delegation Identities**. Click **OK**. Next, select **SQL Server Management Studio** from the list of **Remote Applications**.
21. Select Yes for the pop-up about Shadow Account Restriction.
22. Select the **ACMEFINANCIAL\udb1** to **[SQL Server]\sa** shadow account mapping, and then click **OK**.

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

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

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

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

1. In the RED Identity Management Console, select Manage > Import Password Information > Import Password into Password Store.

2. In the Import Single Account Password window, enter the following configuration:
   a. Account type: OS_TYPE_EXTERNAL
   b. System Name: Twitter
c. **Account Name**: <the Twitter account username>

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

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

3. Click **Import Account**.

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

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

To allow users to launch Twitter, follow these steps:

2. Click Add.
3. Select the identity that should be allowed to launch Twitter. More identities can be added by clicking Add Identity.
4. Click OK.
5. Select the Remote Application Twitter, and then click OK.
6. Select No for the pop-up about Shadow Account Restriction.
7. Select No for the pop-up about System Target Restriction.
8. Click OK.
2.2.10 Configuring Multifactor Authentication with RSA

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

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

2. Fill out the Configure 2 Factor Authentication window with the following settings:
   a. Authenticator Type: RADIUS
   b. Authenticator Label: RSA Auth
   c. IP address: 172.16.2.15 (the IP address of the RSA Authentication Manager)
d. **Port:** 1812

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

f. **Timeout:** 6

g. **Connection Retry Count:** 3

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

---

3. Click **OK**.

4. Click **Manage Web App**.
5. In the **Manage Web Application Instances** window, double-click the Web Application Instance.
6. Click Yes.

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

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

10. Click **Close**.

### 2.2.11 Splunk Universal Forwarder

Install Splunk Universal Forwarder by following the instructions provided at


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

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

2.3.1 How It’s Used

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

2.3.2 Virtual Machine Configuration

The TDi ConsoleWorks virtual machine is configured as follows:

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

Network Interface Configuration:

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

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

2.3.4 Configuration of Back-End Authentication

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

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

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

   a. **Record Name**: IDENTIKEY

   b. **Enabled**: This check box should be selected.
c. **Library:** radius

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

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

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

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

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

9. Click **Save** if available.

### 2.3.5 Creating Users

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

1. In ConsoleWorks, click **USERS > Add** as a **CONSOLE_MANAGER** account.
2. Fill out the pop-up window with the following information:

   a. **Name**: SPLUNK_ADMIN_ACMEFINANCIAL_COM

   b. **Use External Authentication**: This check box should be selected.

   c. Enter a dummy password in the **Password** field, and then retype it in the **Retype Password** field.

   d. **Require Password Change on Next Login**: This check box should **not** be selected.

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

3. Click **Save**.
2.3.6 Creating Tags

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

1. Click SECURITY > Tags > Add.

2. Fill out the pop-up window with the following information:
   a. Name: SPLUNK_OS
   b. (optional) Description: Splunk OS Consoles

3. Click Save.

2.3.7 Creating SSH Consoles

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

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

3. Click **Save**.
2.3.8 Creating Web Consoles

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

The following steps describe the configuration for pfSense:

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

### 2.3.9 Assigning Tags to Consoles

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

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

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

Note: In the case where the URL is not just the host name, the rest of the URL after the forward slash should be put in **Relative URL**.
The following steps describe the process for assigning a tag to a console:

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

### 2.3.10 Creating Profiles for Users

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

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

1. Click **USERS > Profiles > Add**.
2. Fill out the **USERS: Profiles: Add** pop-up window with the following information:
   a. **Name**: SPLUNK_ADMIN
   b. **Description**: Admins of Splunk’s OS
3. Under **USERS**, click **Add**.
4. Move the **SPLUNK_ADMIN_ACMEFINANCIAL_COM** user to the list on the right, and then click **OK**.
5. Click **Save**.
Use the same procedure provided above (while just changing the Name, Description, and USERS chosen) to create profiles for each group of users who should have access to a specific set of consoles. In this case, it was Splunk OS-level consoles. Next, it could be Splunk application-level consoles.

2.3.11 Assigning Permissions to Profiles

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

1. In ConsoleWorks, click SECURITY > Access Control > Add.

2. Fill out the SECURITY: Access Control: Add window with the following information:

   a. Name: SPLUNK_OS_CONSOLES
   b. Description: Access to Splunk OS consoles
   c. Order: 10
   d. Allow or Deny: ALLOW
   e. Component Type: Console

3. Open Profile Selection, and select the Simple tab.

4. Move the SPLUNK_ADMIN profile to the list on the right.

5. Open Resource Selection, and select the Simple tab.

6. Change the drop-down from Is one of these Consoles to Has one of these Tags.
7. Move the **SPLUNK_OS** tag to the list on the right.

8. Open **Privileges**, and select the following privileges (these are the same for both SSH and web consoles):
   
   a. **Aware**
   b. **Connect**
   c. **Disconnect**
   d. **View**

<table>
<thead>
<tr>
<th>Resource Level:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledge</td>
<td></td>
</tr>
<tr>
<td>Can send break</td>
<td></td>
</tr>
<tr>
<td>Controlled Connect</td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td></td>
</tr>
<tr>
<td><strong>Connect</strong></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Disable Scan</td>
<td></td>
</tr>
<tr>
<td>Display Hidden</td>
<td></td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Edit Event Occurrence</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Scan</td>
<td></td>
</tr>
<tr>
<td>Expunge</td>
<td></td>
</tr>
<tr>
<td>Hide</td>
<td></td>
</tr>
<tr>
<td><strong>Lock Console</strong></td>
<td></td>
</tr>
<tr>
<td>Make Comment in Log</td>
<td></td>
</tr>
<tr>
<td><strong>Modify Log Annotation</strong></td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td></td>
</tr>
<tr>
<td><strong>Purge</strong></td>
<td></td>
</tr>
<tr>
<td>Remediate</td>
<td></td>
</tr>
<tr>
<td>Rename</td>
<td></td>
</tr>
<tr>
<td>Send Command</td>
<td></td>
</tr>
<tr>
<td>Send File</td>
<td></td>
</tr>
<tr>
<td>Send protected characters</td>
<td></td>
</tr>
<tr>
<td><strong>Send File</strong></td>
<td></td>
</tr>
<tr>
<td>Send protected characters</td>
<td></td>
</tr>
<tr>
<td><strong>Send File</strong></td>
<td></td>
</tr>
<tr>
<td>Update Baseline Run</td>
<td></td>
</tr>
<tr>
<td><strong>Send File</strong></td>
<td></td>
</tr>
<tr>
<td>View Baseline Run</td>
<td></td>
</tr>
<tr>
<td><strong>Trigger Event</strong></td>
<td></td>
</tr>
<tr>
<td>View Log</td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td></td>
</tr>
<tr>
<td>View Event Occurrence</td>
<td></td>
</tr>
<tr>
<td>View Monitored Events</td>
<td></td>
</tr>
<tr>
<td>View Usage</td>
<td></td>
</tr>
</tbody>
</table>

9. Click **Save**.

2.4 **Ekran System**

Ekran System is a monitoring solution that provides session recording and playback. A server records the actions of users on multiple clients.
2.4.1  How It’s Used

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

2.4.2  Virtual Machine Configuration

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

The Ekran System server virtual machine is configured as follows:

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

**Network Configuration (Interface 1):**

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

2.4.3  Prerequisites

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

2.4.4  Installing Ekran System

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

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

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

#### 2.5.1 How It’s Used

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

#### 2.5.2 Virtual Machine

The Radiant Logic virtual machine is configured as follows:

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

**Network Configuration (Interface 1):**

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

#### 2.5.3 Prerequisites

The minimum system requirements are as follows:

- **Hardware**
  - Cluster nodes must be deployed on hardware that is configured for optimal redundancy and highly reliable connectivity between the cluster nodes/machines.
  - Processor: Intel Pentium or AMD Opteron, minimum dual core
• Processor speed: 2 gigahertz or higher
• Memory: 16 GB minimum. For most production deployments, more than 16 GB of memory is required.
• Hard drive: 100 GB of disk space. The hard-disk usage will vary depending on the log types/levels that are enabled and the desired log history to maintain.

 Software

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

2.5.5 Configure FID
The steps for configuring FID are as follows:

1. Add server back-ends:
   a. While logged in as the Directory Manager, navigate to Settings > Server Backend > LDAP Data Sources.
   b. Click Add.
   c. Name the data source, and then enter the parameters. For AD, the parameters used are shown in the following screenshot. Click Save.
2. Create a proxy view to the back-end directories:
   a. On the Directory Namespace tab, select New Naming Context (the plus sign) at the top left of the screen.
   b. Select the LDAP Backend radio button, and enter the naming context, such as o=test. Click Next.
   c. For the Data Source, select the name of the AD back-end created earlier. Browse and select the Remote Base DN of the domain. Click OK.
2.5.6 Configure Logging

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

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

2. In the Directory Namespace tab, highlight Cache in the left window pane. Select Persistent Cache with Automated Refresh. Click Create Persistent Cache.
3. Browse and select the Lightweight Directory Access Protocol (LDAP) proxy created in the previous steps. Click **OK**. FID creates the cache.

4. Under **Cache** in the lower left window, select the cache that you created. Click **Initialize** to make the cache active.
5. Select **Create a new LDIF file from a snapshot of the virtual directory branch**. Click **OK**. This step may take a few minutes.

6. Once complete, click **Save**.
7. Select the **Connectors** tab.

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

9. Install Splunk Universal Forwarder to monitor the file at

   `C:\radiantone\vds\r1syncsvcs\log\cf_o_acmefinancial\object_generic_dv_so_o_acmefinancial_capture.log`

2.5.7 **Configure SSL**

In this implementation, AD serves as the CA.

1. Create the initial FID private key:

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

2. Download the certificate from the CA.
3. Create the certificate signing request:

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

4. Submit the request to the CA.

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

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

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

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

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

7. Restart FID.

2.5.8 Splunk Universal Forwarder

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

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

2.6.1 How It’s Used
IdRamp is used for MFA in this build. The majority of the IdRamp configuration is performed by the IdRamp team.

2.6.2 Prerequisites
- premium Azure account
- AD installed

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

2. Enable MFA in Azure for certain privileged users:
   b. Click SECURITY > Conditional access.
   c. Click New policy.
d. Give the policy a name, such as Privileged 2FA.

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

f. Click the region labeled as Select.

g. Select the privileged users from the list.

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

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

j. Under Access Controls, click Grant.

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

l. Click Select.

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

3. Disable logins of all other accounts:

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

b. Click Yes next to Block sign in.

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

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

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

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

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

e. Click Create.

f. Complete steps 2a–2c above.

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

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

i. Select all cloud apps for the Cloud apps assignment.
j. Under **Conditions**, select **Locations**.

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

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

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

n. Click **Done**.

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

p. Click **Select**.

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

### 2.7 OneSpan IDENTITY Authentication Server

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

#### 2.7.1 How It’s Used

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

#### 2.7.2 Virtual Machine Configuration

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

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

#### 2.7.3 Prerequisites

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

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

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

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

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

1. Mount the .iso file with the server installer:
   ```bash
   mkdir /mnt/dvd
   mount /dev/dvd /mnt/dvd
   ```

2. Run the installation script:
   ```bash
   cd /mnt/dvd
   sudo ./install.sh
   ```

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

4. Accept the licenses.

5. Select Yes to encrypt the embedded database.

2.7.5 Configuration

After completing the installation, configuration happens immediately:

1. Press Enter to choose Next.

2. Enter the IP address of the server (in this case, 172.16.2.208).

3. Enter the location of the license key on the server.

4. Accept the server functionality, and then select Next.

5. Create a username and password for the first admin account, and then select Next.
6. Create a password for the certificate, and then select Next.

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

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

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

10. Verify that the configuration succeeded as shown below.
11. Respond **No** to the question “Do you want to import a DIGIPASS file? (yes/no)” as you will do this later.

### 2.7.6 Creating a Domain and Policies

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

1. Open the web interface at **https://172.16.2.208:8443**.
2. Log in by using the admin account that was created during configuration.
3. Click **ORGANIZATION > Add domain**.
4. Enter the **Domain Name** acmefinancial.com and then click **CREATE**.
5. Click **POLICIES > Create**.

6. Enter the **Policy ID** ACME_2FA, write a short **Description**, and choose for it to inherit from **Identitkey Back-End Authentication**. Click **CREATE**.
7. Choose to manage the policy, and click **EDIT**.

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

9. Click **CLIENTS > List**.
10. Click the **RADIUS client**.

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

### 2.7.7 Importing DIGIPASSes

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

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

2. Click **Choose File** next to **Get DPX file**, and select the demo DIGIPASSApp.dpx file, which came in the .iso file. Within the **DIGIPASSApp.dpx** file is a set of mobile-application DIGIPASSes. Click **Open**.
3. Enter the transport key for that file. For the demo files, the transport key is 11111111111111111111111111111 (32 1s).

4. Click **UPLOAD**.

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

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

7. Click **IMPORT**.

8. Choose to run the task immediately.

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

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

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

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

1. On AD-PRODUCTION, the AD Domain Controller, open **Server Manager**.
2. In the top right corner, click **Tools > Certification Authority**.

3. **Under Certification Authority (Local)**, right-click **AcmeFinancial-AD-PRODUCTION-CA**, and then select **Properties**.
4. Click Certificate #0, and then click View Certificate.

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

6. Click Next.

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

8. Select a location and file name for saving the certificate. For example, C:\Users\Administrator\Desktop\AD-PRODUCTION-CA-PEM.cer.

9. Click Next, and then click Finish.

10. Copy the file over to the OneSpan server.

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

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

    sudo update-ca-certificates --fresh
13. Reboot the OneSpan server machine.

2.7.8.2 Configuring OneSpan to Use Radiant Logic

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

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

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

### 2.7.9 Integration with TDi ConsoleWorks

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

### 2.7.10 Installing User Websites

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

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

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

2. Run the installation script:

   ```bash
   cd /mnt/dvd/IDENTIKEY\ User\ Websites/
   sudo ./install-uws.sh
   ```
3. Accept the licenses for the server.

2.7.11 Creating Component Records in IDENTIKEY Authentication Server

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

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

2. Fill out the Create new Client page with the following information:
   a. Client Type: IDENTIKEY User Websites
   b. Location: 172.16.2.208
   c. Policy ID: IDENTIKEY Provisioning for Multi-Device Licensing

3. Click CREATE.
4. Click **Click here to manage IDENTIKEY User Websites**.

5. Tab over to **License**.

6. Click **LOAD LICENSE KEY**.

7. Click **Choose File**, and then provide it with the User Websites license.

8. Click **FINISH**.

9. Click **CLIENTS > Register** again.

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

    a. **Client Type**: UWS MDL Provisioning (type it in)
    
    b. **Location**: 172.16.2.208
    
    c. **Policy ID**: IDENTIKEY Provisioning for Multi-Device Licensing

11. Click **CREATE**.
12. Click **POLICIES > List**.

13. Find the policy **IDENTIKEY Provisioning for Multi-Device Licensing**, and then click it.

14. Click **EDIT**.

15. Change the **Back-End Protocol** from **RADIUS** to **Microsoft AD**.

16. Click **SAVE**.

17. Tab over to **User**.

18. Click **EDIT**, and change **Dynamic User Registration** to **No**. This way, only users added by admins in IDENTIKEY Authentication Server will be assigned DIGIPASSes.

19. Click **SAVE**.

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

### 2.8 Base Linux OS

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

#### 2.8.1 Virtual Machine Configuration

The base Linux virtual machine is configured as follows:

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

**Network Configuration:**

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.x.x
- Netmask: 255.255.255.0
- Gateway: 172.16.x.1
2.8.2 Domain Join Configuration

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

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

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

# The loopback network interface
auto lo
iface lo inet loopback

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

2. Restart the networking by entering the following command:

```
systemctl restart networking
```

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

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

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

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

5. If prompted to enter your Kerberos 5 realm name, enter your domain name in capital letters. The Kerberos 5 default realm is ACMEFINANCIAL.COM.
6. Install the chrony ntp client by entering the following command:

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

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

```
server 172.16.3.10
```

8. Restart the chrony service as shown below:

```
systemctl restart chrony
```

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

   a. `kinit administrator@ACMEFINANCIAL.COM`
   b. Enter the password when prompted.
   c. `realm -v join acmefinancial.com -user-principal = yourlinuxhost.acmefinancial.com/administrator@ACMEFINANCIAL.COM`
   d. `systemctl restart realmd`

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

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

2.9.1 How It’s Used

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

2.9.2 Virtual Machine Configuration

The Microsoft SQL Server virtual machine is configured as follows:

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

**Network Configuration:**

- IPv4: manual
- IPv6: disabled
IPv4 address: 172.16.3.12
Netmask: 255.255.255.0
Gateway: 172.16.3.1
DNS name servers: 172.16.3.10
DNS-search domain: acmefinancial.com

2.9.3 Firewall Configuration
ufw allow 1433/tcp
ufw allow 22/tcp
ufw default deny incoming

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

1. Install Microsoft SQL Server on Ubuntu Linux by using the instructions provided at

2. Create a service account by entering the following Powershell command:

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

   a. Enter the password when prompted.

3. Give the account the Log on as a service right by going to Server Manager > Group Policy Management > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
4. Create a Service Principal Name by entering the following command:
   
   ```
   setspn -A MSSQLSvc/sql-server.acmefinancial.com:1433 mssql
   ```

5. Request the information needed to create a keytab file by entering the following commands:
   
   a. Enter the following command:
      
      ```
      kinit mssql@ACMEFINANCIAL.COM
      ```
      
      i. Enter the account password when prompted.
   
   b. Retrieve the kvno value by entering the following command:
      
      ```
      kvno MSSQLSvc/sql-server.acmefinancial.com:1433
      ```

6. Create a keytab file by entering the commands shown below:
   
   ```
   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
   root@sql-server:~# ktutil
   Password for MSSQLSvc/sql-server.ACMEFINANCIAL.COM@ACMEFINANCIAL.COM:
   ktutil: addent -password -p MSSQLSvc/sql-server.ACMEFINANCIAL.COM -k 2 -e rc4-hmac
   Password for MSSQLSvc/sql-server.ACMEFINANCIAL.COM@ACMEFINANCIAL.COM:
   ktutil: write_kt /var/opt/mssql/secrets/mssql.keytab
   ```

7. Exit the ktutil tool by entering the following command:
   
   ```
   quit
   ```
8. Restart SQL Server by entering the following command:

   systemctl restart mssql-server

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


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

    ./sqlcmd -S localhost -U sa

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


### 2.10 Samba File Server

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

#### 2.10.1 How It’s Used

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

#### 2.10.2 Virtual Machine Configuration

The Samba virtual machine is configured as follows:

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

**Network Configuration:**

- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.3.21
2.10.3 Firewall Configuration

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

2.10.4 Installation and Configuration

1. Ensure that the DNS server is set to the AD domain controller IP address. Enter the following command to verify:
   ```bash
   cat /etc/resolv.conf
   ```

2. Ensure that the search domain is set to your domain (e.g., acmefinancial.com). Enter the following command to verify:
   ```bash
   cat /etc/resolv.conf
   ```
3. Install the chrony ntp client by entering the following command:
   
   ```bash
   sudo apt-get install chrony
   ```

4. Add the following line to the `/etc/chrony/chrony.conf` file so that chrony points to the NTP server:
   
   ```text
   server 172.16.3.10
   ```

5. Restart the chrony service by entering the following command:
   
   ```bash
   systemctl restart chrony
   ```

6. Install the Samba, Kerberos, and winbind packages by entering the following command at the terminal:
   
   ```bash
   apt-get install samba krb5-user krb5-config winbind libpam-winbind libnss-winbind
   ```

7. Edit the `/etc/samba/smb.conf` file with the values as shown below:
   
   ```ini
   [global]
   security = ADS
   workgroup = ACMFINANCIAL
   realm = ACMFINANCIAL.COM

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

8. Restart these services by entering the following command:
   
   ```bash
   systemctl restart smbd winbind
   ```

9. Join the domain by entering the following command:
   
   ```bash
   net ads join -U administrator
   ```
10. Enter the domain admin password when prompted.

11. Enter the following command at the terminal to create a folder to be shared via Samba:
   ```
   mkdir /PII2
   ```

12. Enter the following command to change the owning group to domain users:
   ```
   chgrp "domain users" /PII2
   ```

13. Enter the following command to ensure that only domain admins have access to the folder:
   ```
   chmod 660 /PII2
   ```

14. Edit the `/etc/samba/smb.conf` file with the information shown below:
   ```
   [PII2]
   path = /PII2
   read only = no
   directory mask = 0775
   guest ok = yes
   ```

15. Restart these services by entering the following command:
   ```
   systemctl restart smbd winbind
   ```

2.11 Remediant SecureONE

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

2.11.1 How It’s Used

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

2.11.2 Virtual Machine Configuration

The Remediant SecureONE virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 4 CPU cores
Network Configuration:

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

2.11.3 Installation and Initial Configuration

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

2.11.4 Domain Configuration

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

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

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

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

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

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

2. In the search bar, type the name of the domain user, and then click Add User/Group.
3. SecureONE uses a built-in Google Authenticator for 2FA. Once the new user attempts to log in with their domain password, a Quick Response (QR) code is presented.

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

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

### 2.11.7 Requesting Privileged Access to Protected System

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

1. Navigate to Access > System Search.
2. In the search bar, enter the host name of the protected system.
3. Click Access System.
4. Once access is granted, the session expiration time will be displayed under **Expiration**.

5. At this point, the user can log onto the protected system with administrative privileges.
2.12 RSA Authentication Manager

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

2.12.1 How It’s Used

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

2.12.2 Installation and Initial Configuration

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

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

   RSA Authentication Manager 8.2.0.0.0-build1366271
   The appliance network settings have been configured.

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

   To complete the appliance configuration, access Quick Setup at:

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

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

4. Review the information, and then click **Start Step 1**.
5. Upload the License File by clicking **Choose File**, selecting the appropriate file and clicking **Open**, and then clicking **Upload**.

6. Enter the **Hostname or IP Address** of the NTP server in your environment, and then click **Next**.
7. Enter the credentials for the Authentication Manager’s OS, and then click Next.

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

2.12.3 LDAP Integration

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

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

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

3. Navigate to Deployment Configuration > Identity Sources > Add New. On the Connection(s) tab in the appropriate fields, add the values necessary for your environment:
4. Enter the value of a domain admin, such as administrator@acmefinancial.com, in the Directory User ID field.

5. Click Test Connection.

### 2.12.4 Token Assignment

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

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

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

3. Navigate to Identity > Users > Manage Existing.

4. Ensure that the Identity Source field points to your AD server, identified by its unique name given in the operations console.

5. In the Where field, select User ID.

6. In the search bar, enter the User ID for which you would like to search.

7. The user account will be retrieved and displayed.
8. Click on the User ID (by selecting the check box to the left of the User ID), and then click SecurID Tokens.

9. Click Assign Token.

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

2.12.5 Software Token Profiles and Token Distribution

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

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

2.13.1 How It’s Used

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

2.13.2 Installation

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

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

2.13.3 Queries

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

2.13.4 DemoBomgar-AD-Auth-UnauthV1

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

2.13.5 DemoRadiant-AD-Event-Details

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

2.13.6 SSL Forwarding

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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA</td>
<td>Two-Factor Authentication</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>FID</td>
<td>Federated Identity</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte(s)</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol Version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>N/A</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>NCCoE</td>
<td>National Cybersecurity Center of Excellence</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Controller/Card</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PAM</td>
<td>Privileged Account Management</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>QR</td>
<td>Quick Response</td>
</tr>
<tr>
<td>RAM</td>
<td>Random-Access Memory</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
</tbody>
</table>