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

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

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

FEEDBACK

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

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

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

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

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

Contents

1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

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

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

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

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

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

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

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

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

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

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

1.2 Build Overview

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

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

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

2 Product Installation Guides

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

2.1 Microsoft Active Directory

2.1.1 How It's Used

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

2.1.2 Virtual Machine Configuration

The Microsoft AD virtual machine is configured as follows:

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

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

Network Configuration (Interface 1):

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

2.1.3 Installation

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

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

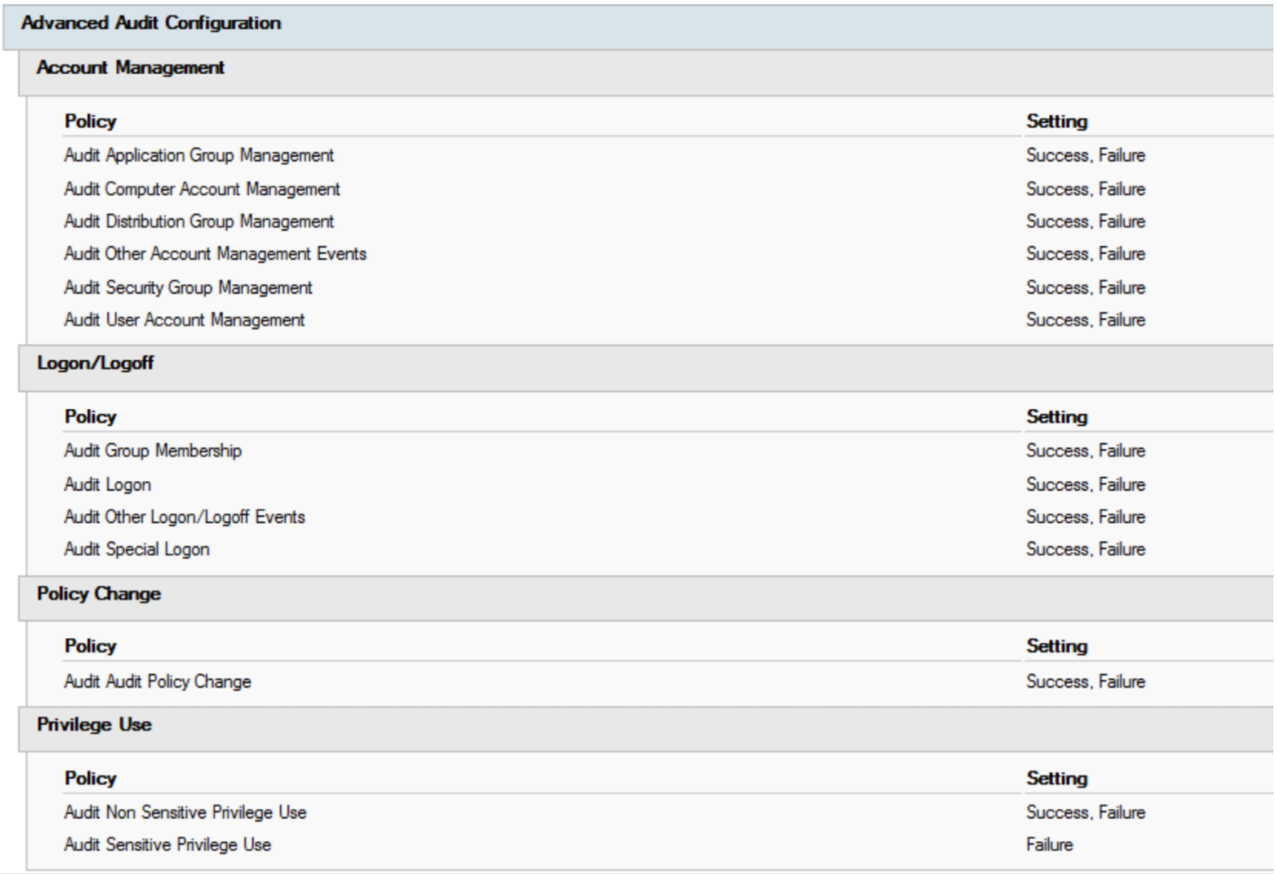
https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority

2.1.4 DNS Configuration

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

2.1.5 Group Policy Object Configuration

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



Advanced Audit Configuration

Account Management

Policy	Setting
Audit Application Group Management	Success, Failure
Audit Computer Account Management	Success, Failure
Audit Distribution Group Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure

Logon/Logoff

Policy	Setting
Audit Group Membership	Success, Failure
Audit Logon	Success, Failure
Audit Other Logon/Logoff Events	Success, Failure
Audit Special Logon	Success, Failure

Policy Change

Policy	Setting
Audit Audit Policy Change	Success, Failure

Privilege Use

Policy	Setting
Audit Non Sensitive Privilege Use	Success, Failure
Audit Sensitive Privilege Use	Failure

2.1.6 Scripts

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

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

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

```
csvfile = open('Final_AD.csv', 'w+')
wr = csv.writer(csvfile, quoting=csv.QUOTE_ALL)
csvlist = ["Event", "UserSubject", "UserObject", "Timestamp"]
wr.writerow(csvlist)
with open('ADLOG.csv', 'r') as f:
        reader = csv.reader(f)
        zerothrow = 1
        for row in reader:
                csvlist = []
                if zerothrow == 1:
                        zerothrow = 0
                else:
                        parse_list =  row[1].split('\n')
                        #print parse_list
                        #break
                        csvlist.append(parse_list[0].replace('\t', '').replace('\r', ''))
                        csvlist.append(parse_list[4].replace('\t', '').replace('\r', '').replace('Account Name:', ''))
                        if row[4] == "4728":
                        win_command = parse_list[10].replace('\t', '').replace('\r', '').replace('Account Name:', '')
                        win_command = win_command[:3] + '"' + win_command[3:]
                        sec_index = win_command.index(",CN=")
                        win_command = win_command[:sec_index] + '"' + win_command[sec_index:]
                        win_command = "dsquery * " + win_command + " -scope base -attr sAMAccountName"
                        account = check_output(win_command, shell  = True).decode()
                        account = account.replace('sAMAccountName', '').replace('\n', '').replace(' ', '')
                        csvlist.append(account)
                else:
                        csvlist.append(parse_list[10].replace('\t', '').replace('\r', 
    '').replace('Account Name:', ''))
                        csvlist.append(row[2].replace('\t', '').replace('\r', ''))
                        wr.writerow(csvlist)
    #temp = check_output("dir C:", shell=True).decode()
    #print(temp)
    csvfile.close()
```

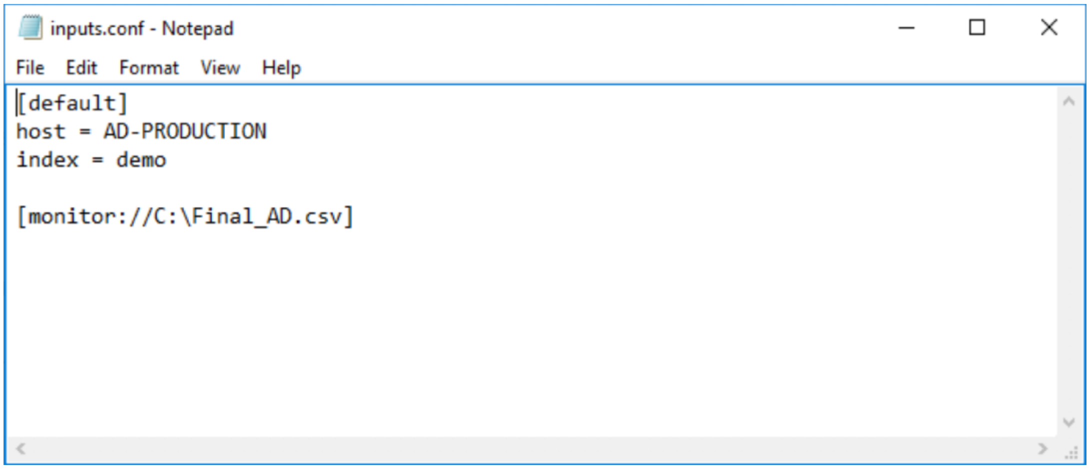
The following PowerShell script extracts data from the Windows security event log and executes the Python script above:

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

2.1.7 Splunk Universal Forwarder

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

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



```
[default]
host = AD-PRODUCTION
index = demo

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

2.2 Bomgar Privileged Identity

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

2.2.1 How It's Used

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

2.2.2 Virtual Machine Configuration

The Privileged Identity virtual machine is configured as follows:

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

Network Configuration (Interface 1):

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

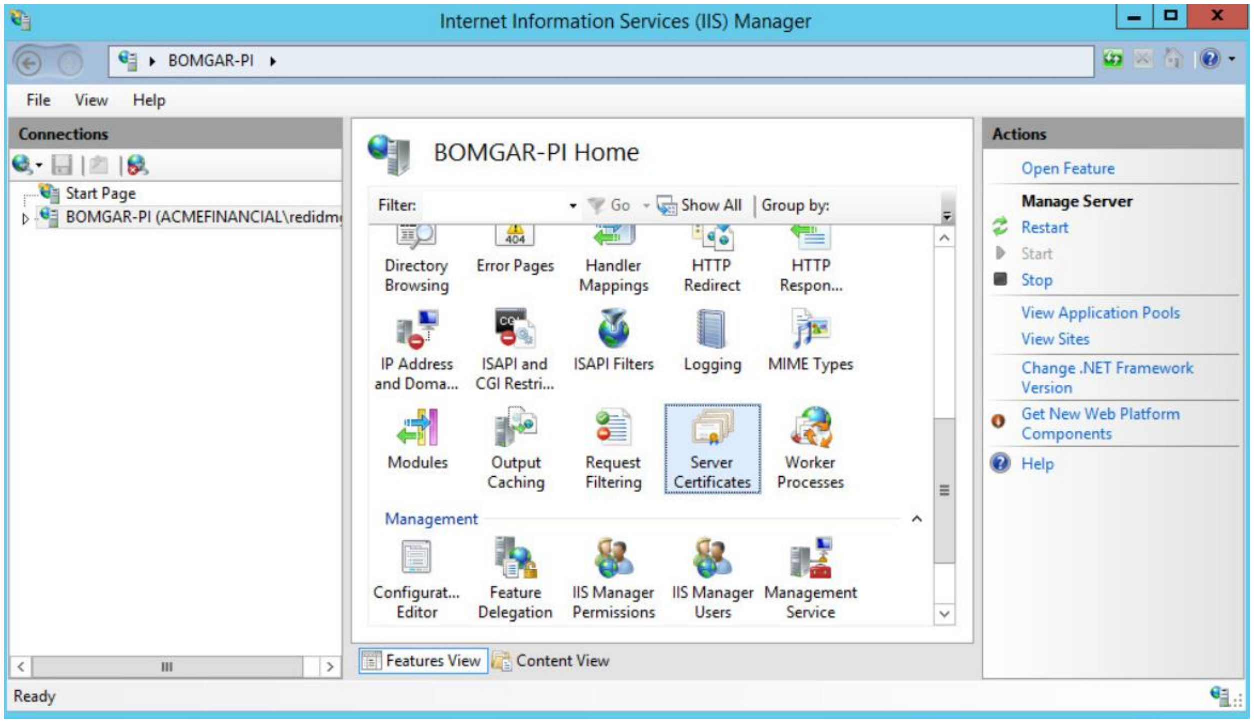
2.2.3 Prerequisites

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

2.2.4 Installing Privileged Identity

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

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



4. On the right, click **Create Certificate Request.**

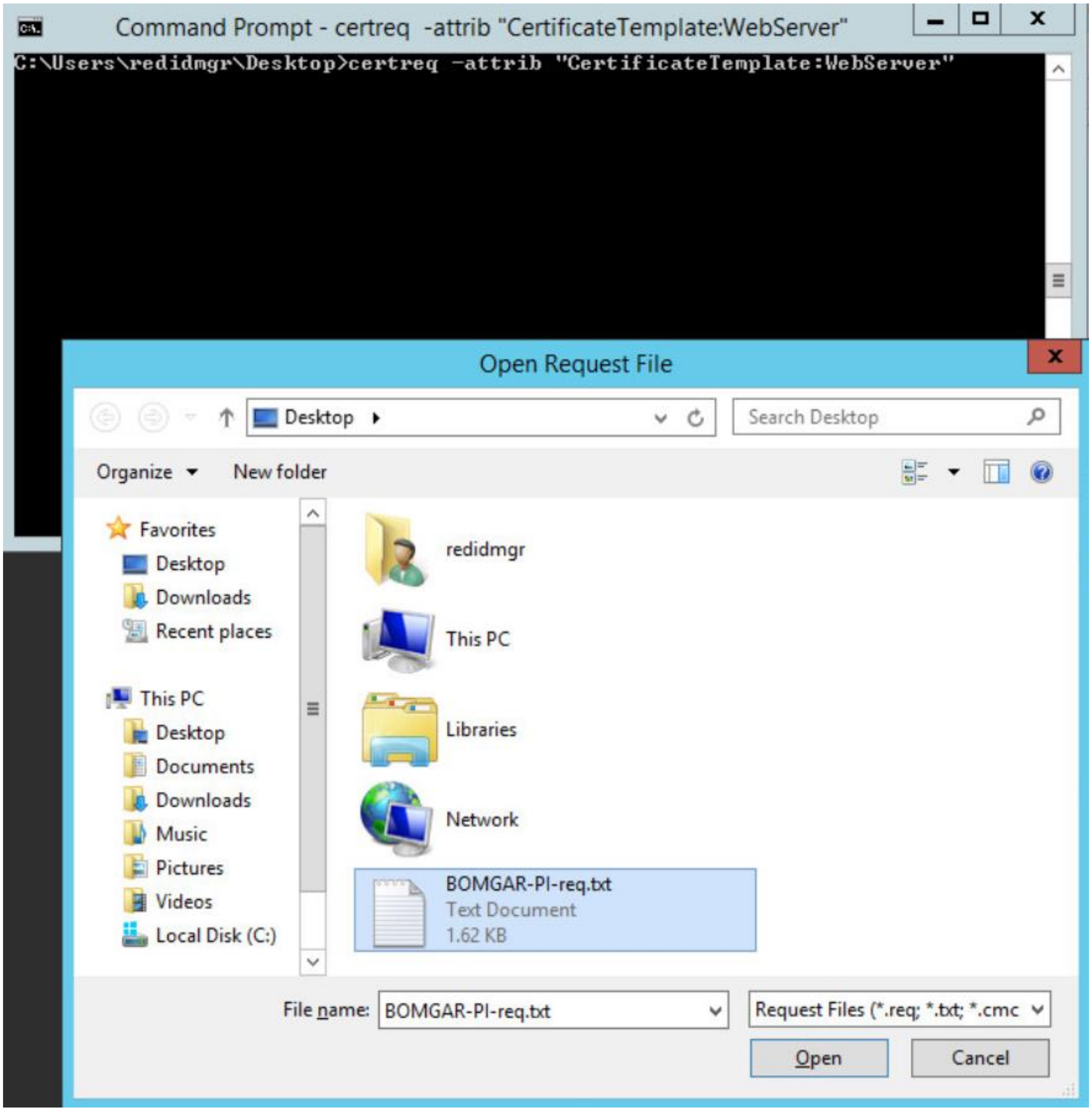
5. Fill out the **Distinguished Name Properties,** and then click **Next.**

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

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

8. Using the certreq command in the **Command Prompt,** enter `certreq -attrib “CertificateTemplate:WebServer”`.

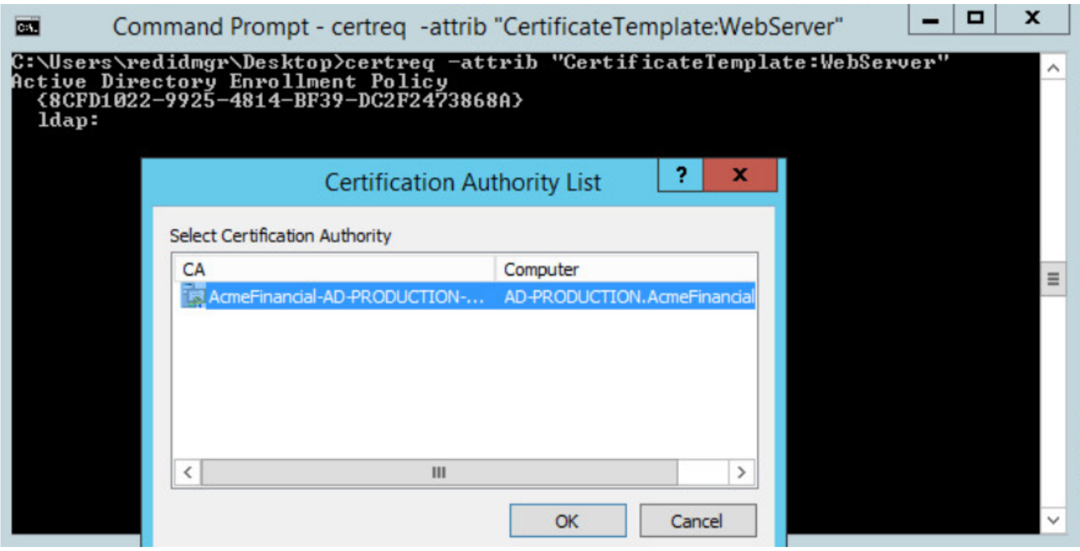
9. Select the certificate file that was created in Step 7, and then click **Open.**



```
C:\Users\redidmgr\Desktop>certreq -attrib "CertificateTemplate:WebServer"
```

328

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



Command Prompt - certreq -attrib "CertificateTemplate:WebServer"

```
C:\Users\redidmgr\Desktop>certreq -attrib "CertificateTemplate:WebServer"
Active Directory Enrollment Policy
  {8CFD1022-9925-4814-BF39-DC2F2473868A}
  ldap:
```

Certification Authority List

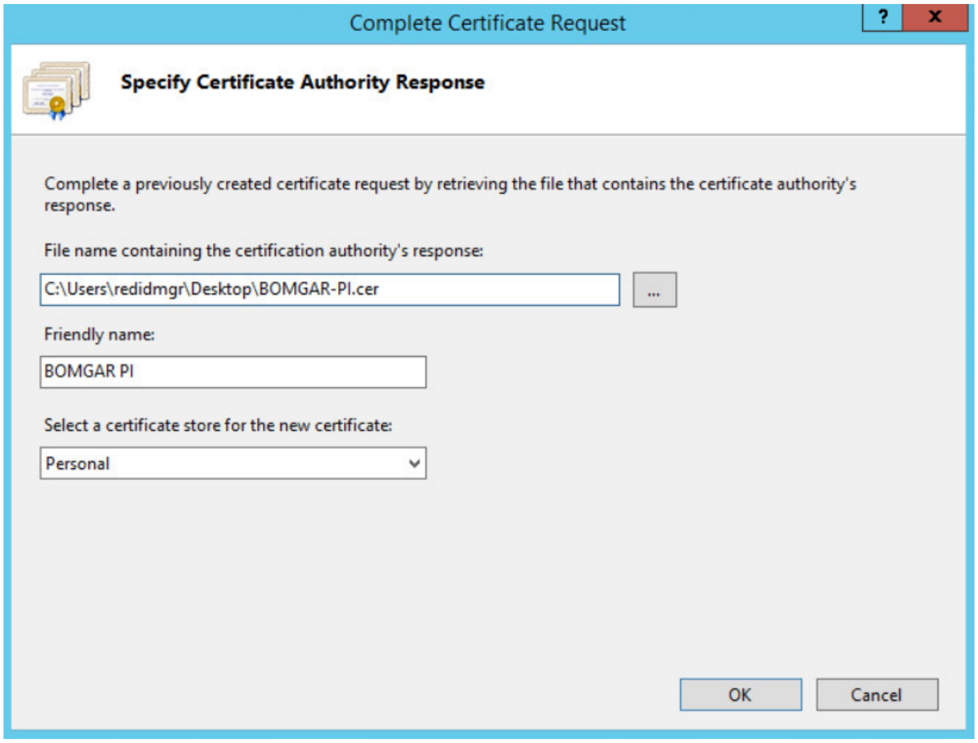
Select Certification Authority

CA	Computer
AcmeFinancial-AD-PRODUCTION-...	AD-PRODUCTION.AcmeFinancial

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.



Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\Users\redidmgr\Desktop\BOMGAR-PI.cer

Friendly name:

BOMGAR PI

Select a certificate store for the new certificate:

Personal

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

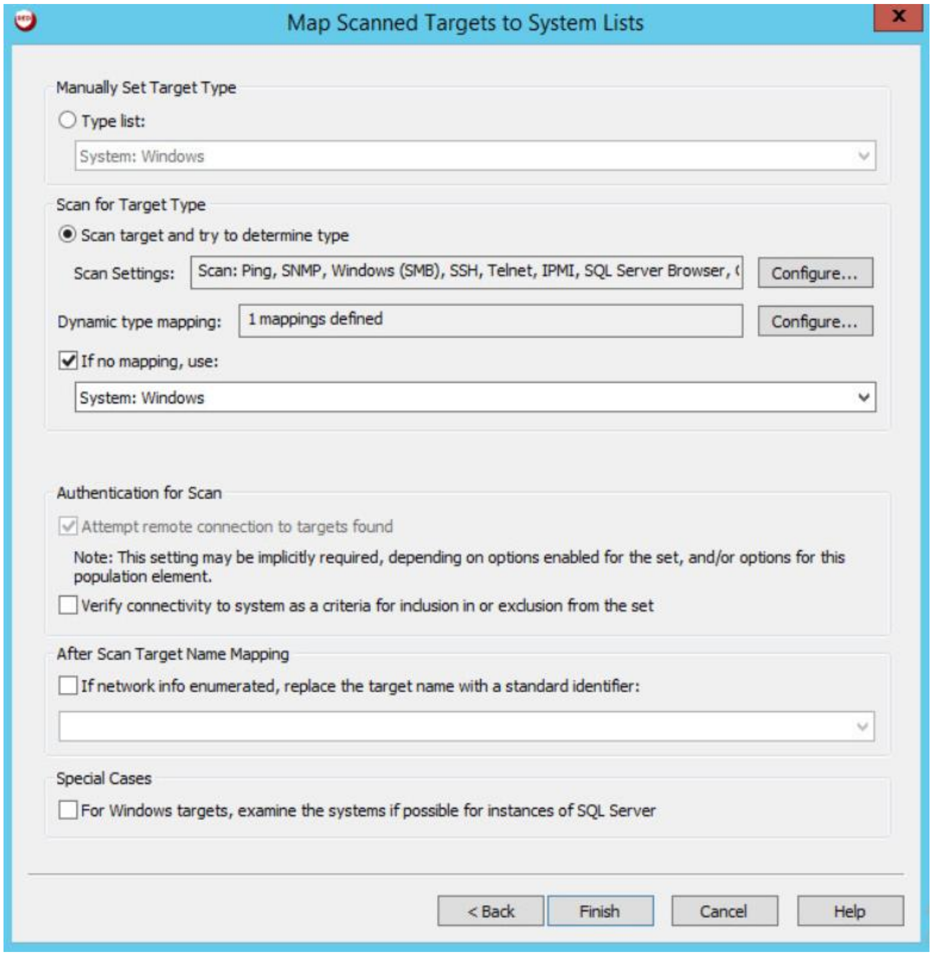
You are now ready to begin following further installation instructions that are publicly available on Bomgar's website.

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.



Map Scanned Targets to System Lists

Manually Set Target Type

○ Type list:

System: Windows

Scan for Target Type

● Scan target and try to determine type

Scan Settings: Scan: Ping, SNMP, Windows (SMB), SSH, Telnet, IPMI, SQL Server Browser, (

Dynamic type mapping: 1 mappings defined

☑ If no mapping, use:

System: Windows

Authentication for Scan

☑ Attempt remote connection to targets found

Note: This setting may be implicitly required, depending on options enabled for the set, and/or options for this population element.

□ Verify connectivity to system as a criteria for inclusion in or exclusion from the set

After Scan Target Name Mapping

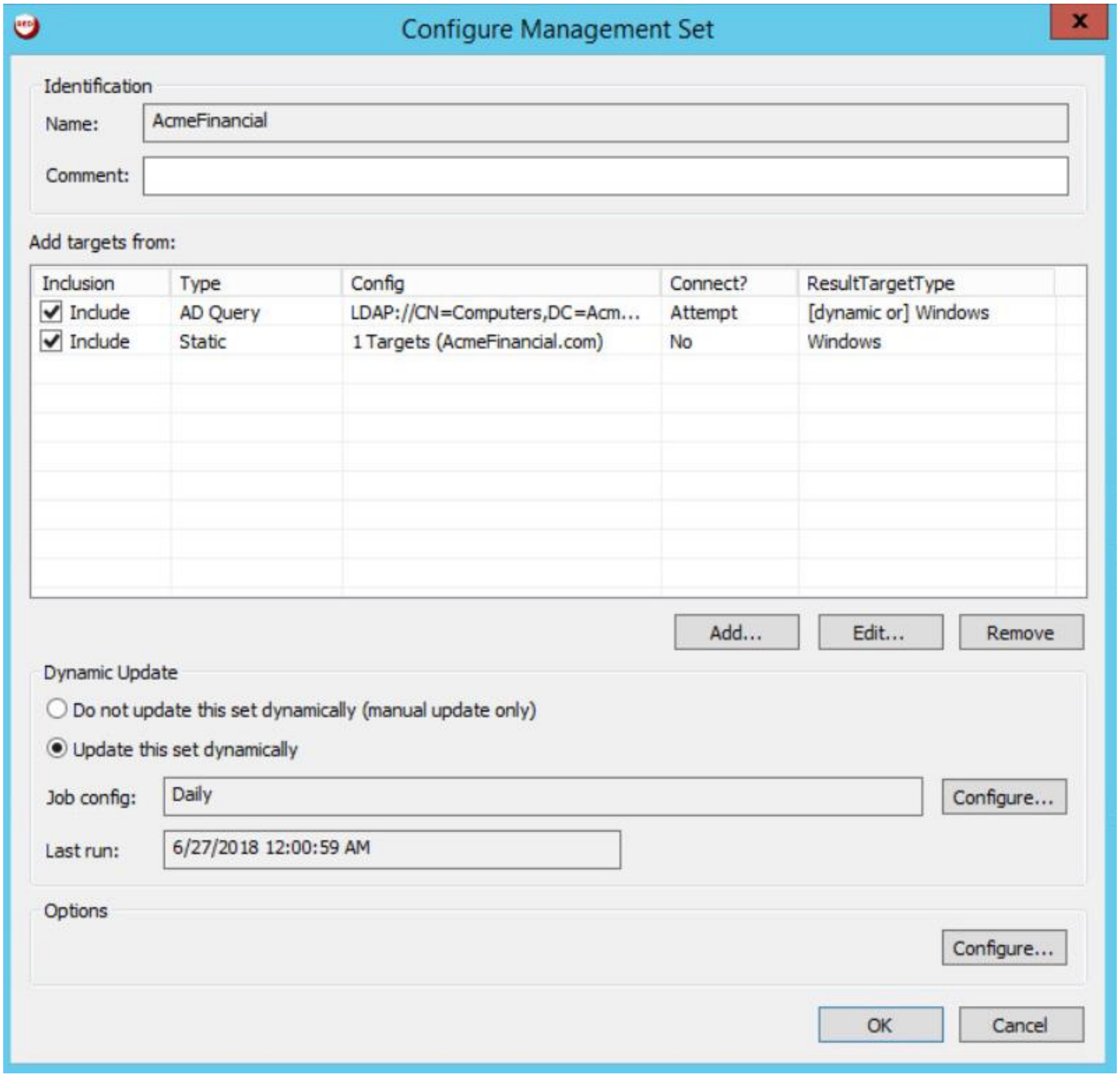
□ If network info enumerated, replace the target name with a standard identifier:

Special Cases

□ For Windows targets, examine the systems if possible for instances of SQL Server

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.



Identification

Name: AcmeFinancial

Comment:

Add targets from:

Inclusion	Type	Config	Connect?	ResultTargetType
☑ Include	AD Query	LDAP://CN=Computers,DC=Acm...	Attempt	[dynamic or] Windows
☑ Include	Static	1 Targets (AcmeFinancial.com)	No	Windows

Dynamic Update

○ Do not update this set dynamically (manual update only)

● Update this set dynamically

Job config: Daily

Last run: 6/27/2018 12:00:59 AM

Options

2.2.5.2 Delegation Identities

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

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

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

   b. ACMEFINANCIAL\twitteruser

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

2.2.6 Installing Privileged Identity Application Launcher

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

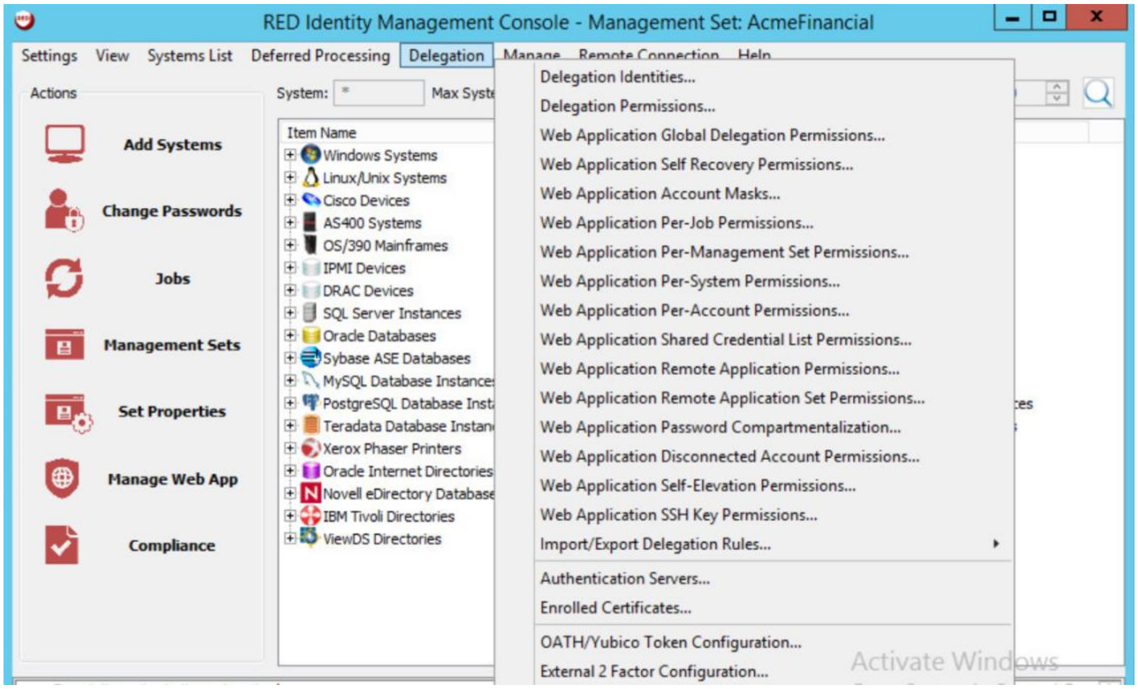
Using the Bomgar documentation, complete the following steps:

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

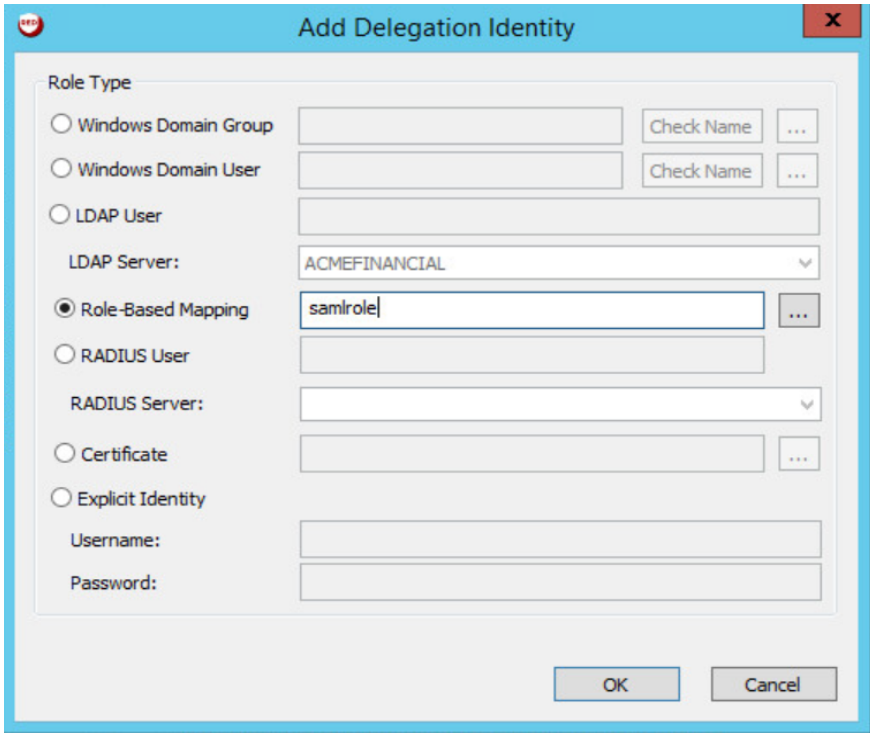
2.2.7 Configure Bomgar Privileged Identity with IdRamp SAML Authentication

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

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


RED Identity Management Console - Management Set: AcmeFinancial
Settings
View
Systems List
Deferred Processing
Delegation
Manage
Remote Connection
Help
Actions
Add Systems
Change Passwords
Jobs
Management Sets
Set Properties
Manage Web App
Compliance
System: *
Max Syste
Item Name
Windows Systems
Linux/Unix Systems
Cisco Devices
AS400 Systems
OS/390 Mainframes
IPMI Devices
DRAC Devices
SQL Server Instances
Oracle Databases
Sybase ASE Databases
MySQL Database Instance
PostgreSQL Database Inst
Teradata Database Instan
Xerox Phaser Printers
Oracle Internet Directories
Novell eDirectory Database
IBM Tivoli Directories
ViewDS Directories
Delegation Identities...
Delegation Permissions...
Web Application Global Delegation Permissions...
Web Application Self Recovery Permissions...
Web Application Account Masks...
Web Application Per-Job Permissions...
Web Application Per-Management Set Permissions...
Web Application Per-System Permissions...
Web Application Per-Account Permissions...
Web Application Shared Credential List Permissions...
Web Application Remote Application Permissions...
Web Application Remote Application Set Permissions...
Web Application Password Compartmentalization...
Web Application Disconnected Account Permissions...
Web Application Self-Elevation Permissions...
Web Application SSH Key Permissions...
Import/Export Delegation Rules...
Authentication Servers...
Enrolled Certificates...
OATH/Yubico Token Configuration...
External 2 Factor Configuration...
Activate Windows

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



Add Delegation Identity

Role Type

○ Windows Domain Group — Check Name ...

○ Windows Domain User — Check Name ...

○ LDAP User

LDAP Server: ACMEFINANCIAL

● Role-Based Mapping: samlrole ...

○ RADIUS User

RADIUS Server:

○ Certificate ...

○ Explicit Identity

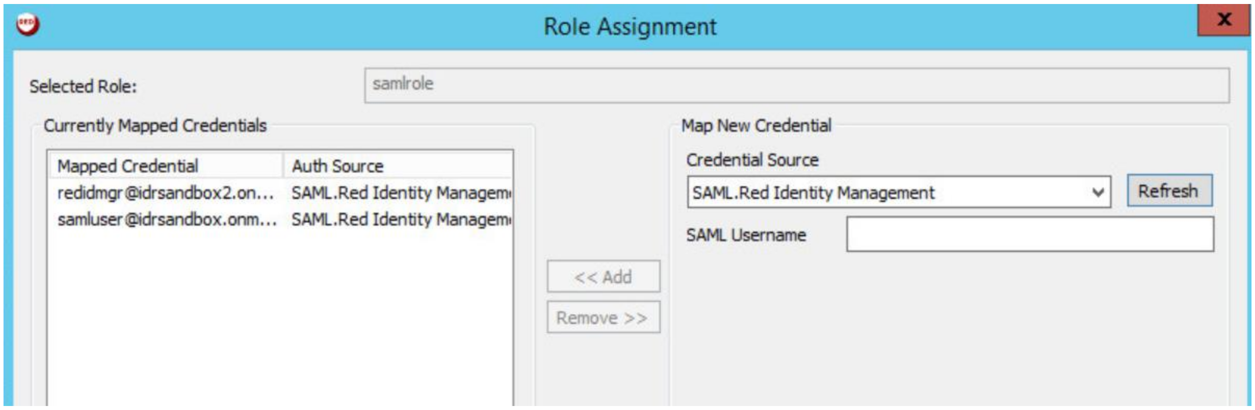
Username:

Password:

OK Cancel

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.



Role Assignment

Selected Role: samlrole

Currently Mapped Credentials

Mapped Credential	Auth Source
redidmgr@idrsandbox2.on...	SAML.Red Identity Managem
samluser@idrsandbox.onm...	SAML.Red Identity Managem

<< Add

Remove >>

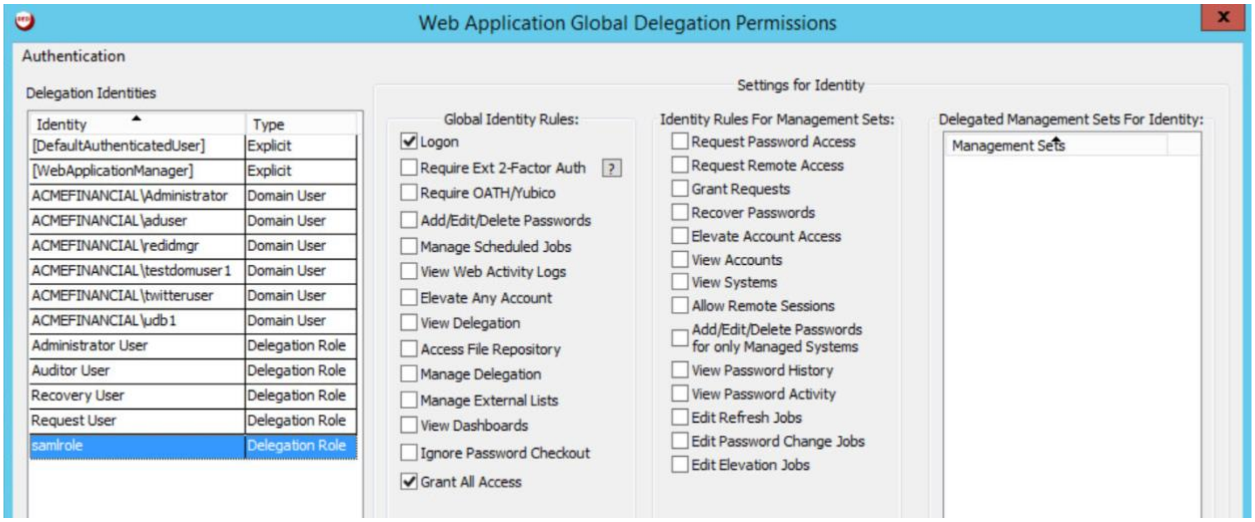
Map New Credential

Credential Source: SAML.Red Identity Management — Refresh

SAML Username:

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.



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

Global Identity Rules:

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

Identity Rules For Management Sets:

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

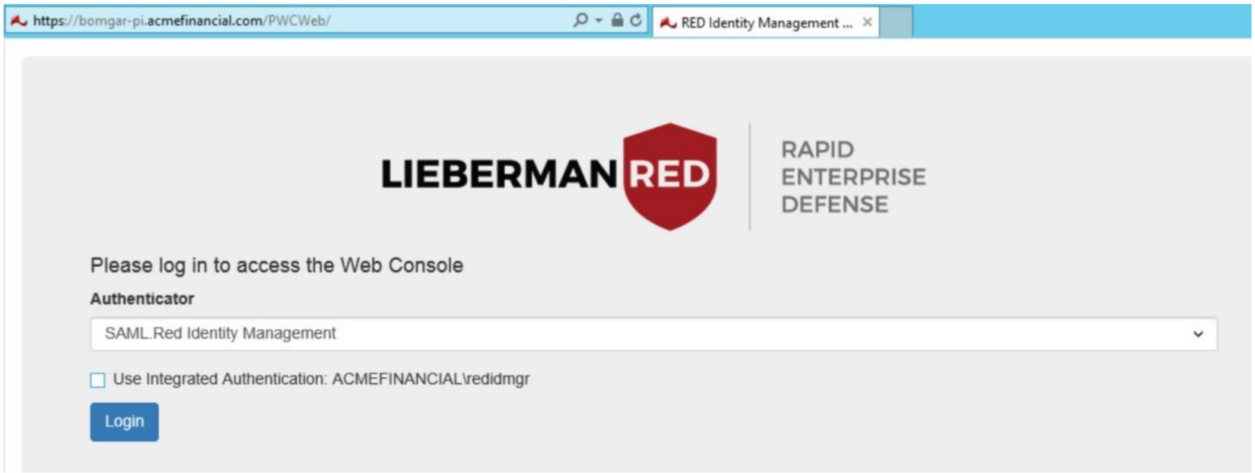
Delegated Management Sets For Identity:

Management Sets

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.



https://bomgar-pi.acmefinancial.com/PWCWeb/
RED Identity Management ...
LIEBERMAN RED
RAPID
ENTERPRISE
DEFENSE

Please log in to access the Web Console

Authenticator

SAML.Red Identity Management

☐ Use Integrated Authentication: ACMEFINANCIAL\redidmgr

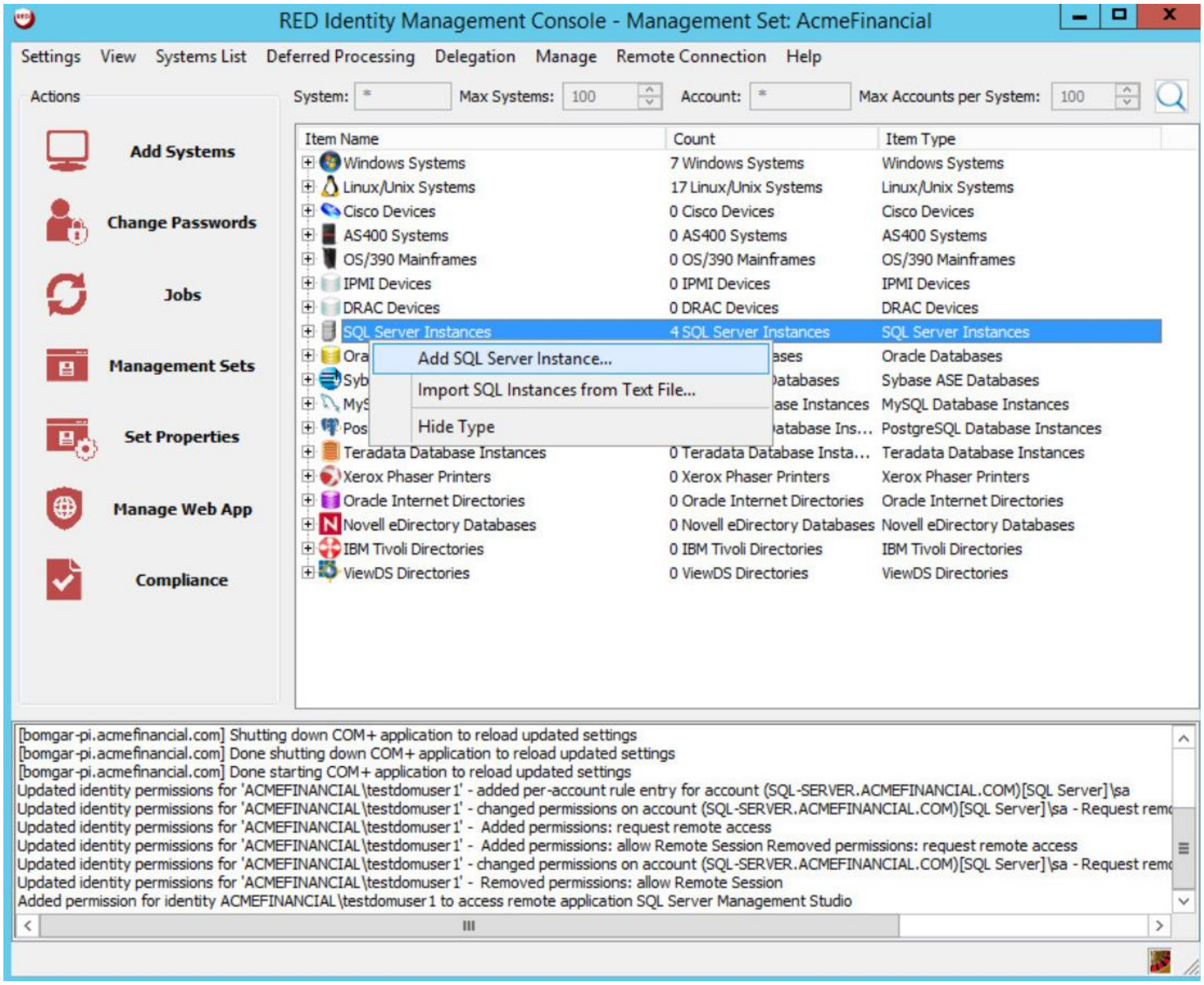
2.2.8 Configuring Microsoft SQL Server Access

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.**

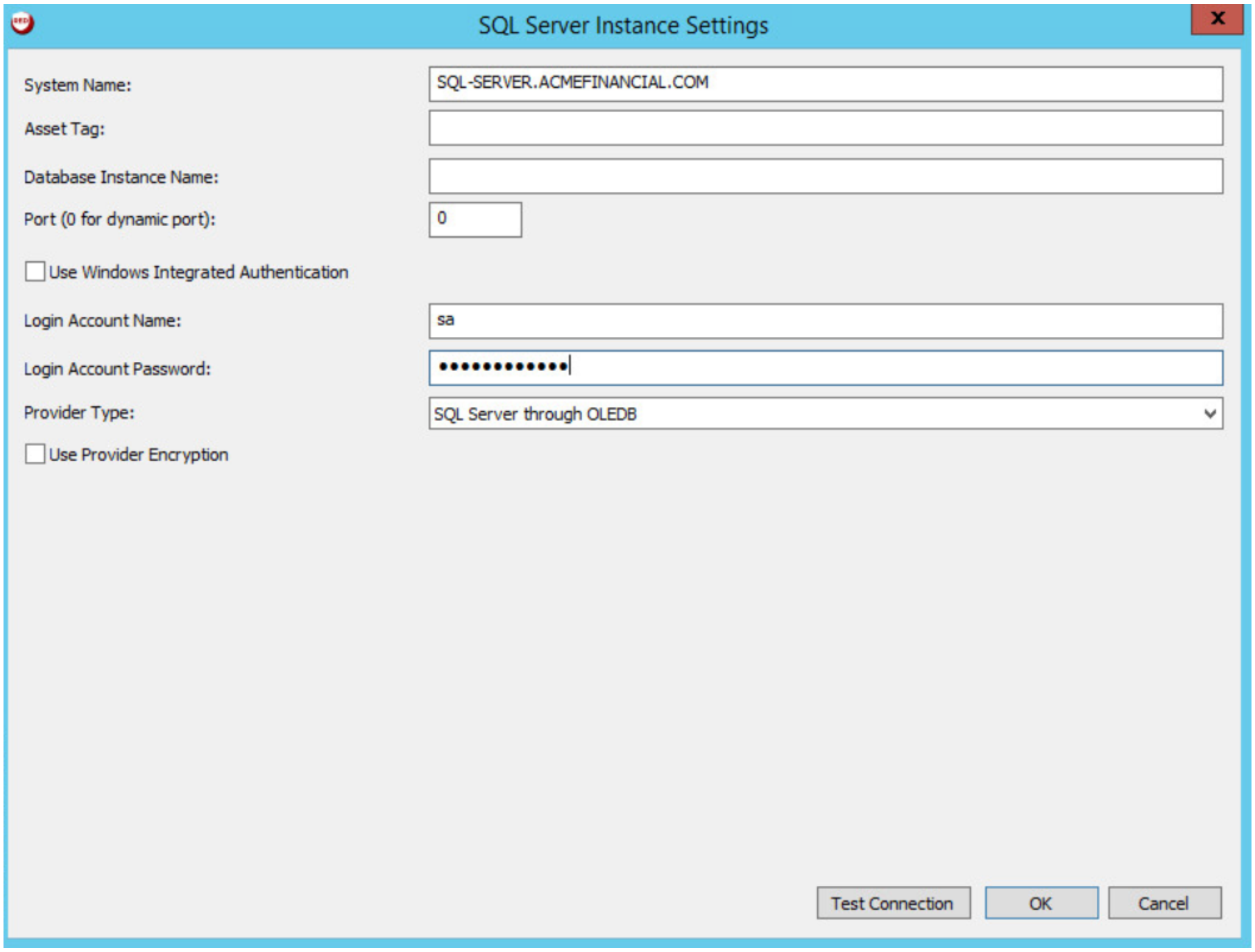


System: * Max Systems: 100 Account: * Max Accounts per System: 100

Item Name	Count	Item Type
Windows Systems	7 Windows Systems	Windows Systems
Linux/Unix Systems	17 Linux/Unix Systems	Linux/Unix Systems
Cisco Devices	0 Cisco Devices	Cisco Devices
AS400 Systems	0 AS400 Systems	AS400 Systems
OS/390 Mainframes	0 OS/390 Mainframes	OS/390 Mainframes
IPMI Devices	0 IPMI Devices	IPMI Devices
DRAC Devices	0 DRAC Devices	DRAC Devices
SQL Server Instances	4 SQL Server Instances	SQL Server Instances
Ora	ases	Oracle Databases
Syb	atabases	Sybase ASE Databases
MyS	ase Instances	MySQL Database Instances
Pos	atabase Ins...	PostgreSQL Database Instances
Teradata Database Instances	0 Teradata Database Insta...	Teradata Database Instances
Xerox Phaser Printers	0 Xerox Phaser Printers	Xerox Phaser Printers
Oracle Internet Directories	0 Oracle Internet Directories	Oracle Internet Directories
Novell eDirectory Databases	0 Novell eDirectory Databases	Novell eDirectory Databases
IBM Tivoli Directories	0 IBM Tivoli Directories	IBM Tivoli Directories
ViewDS Directories	0 ViewDS Directories	ViewDS Directories

```
[bomgar-pi.acmefinancial.com] Shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done starting COM+ application to reload updated settings
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - added per-account rule entry for account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - changed permissions on account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa - Request remo
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' -  Added permissions: request remote access
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' -  Added permissions: allow Remote Session Removed permissions: request remote access
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - changed permissions on account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa - Request remo
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' -  Removed permissions: allow Remote Session
Added permission for identity ACMEFINANCIAL\testdomuser1 to access remote application SQL Server Management Studio
```

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.



System Name: SQL-SERVER.ACMEFINANCIAL.COM

Asset Tag:

Database Instance Name:

Port (0 for dynamic port): 0

□ Use Windows Integrated Authentication

Login Account Name: sa

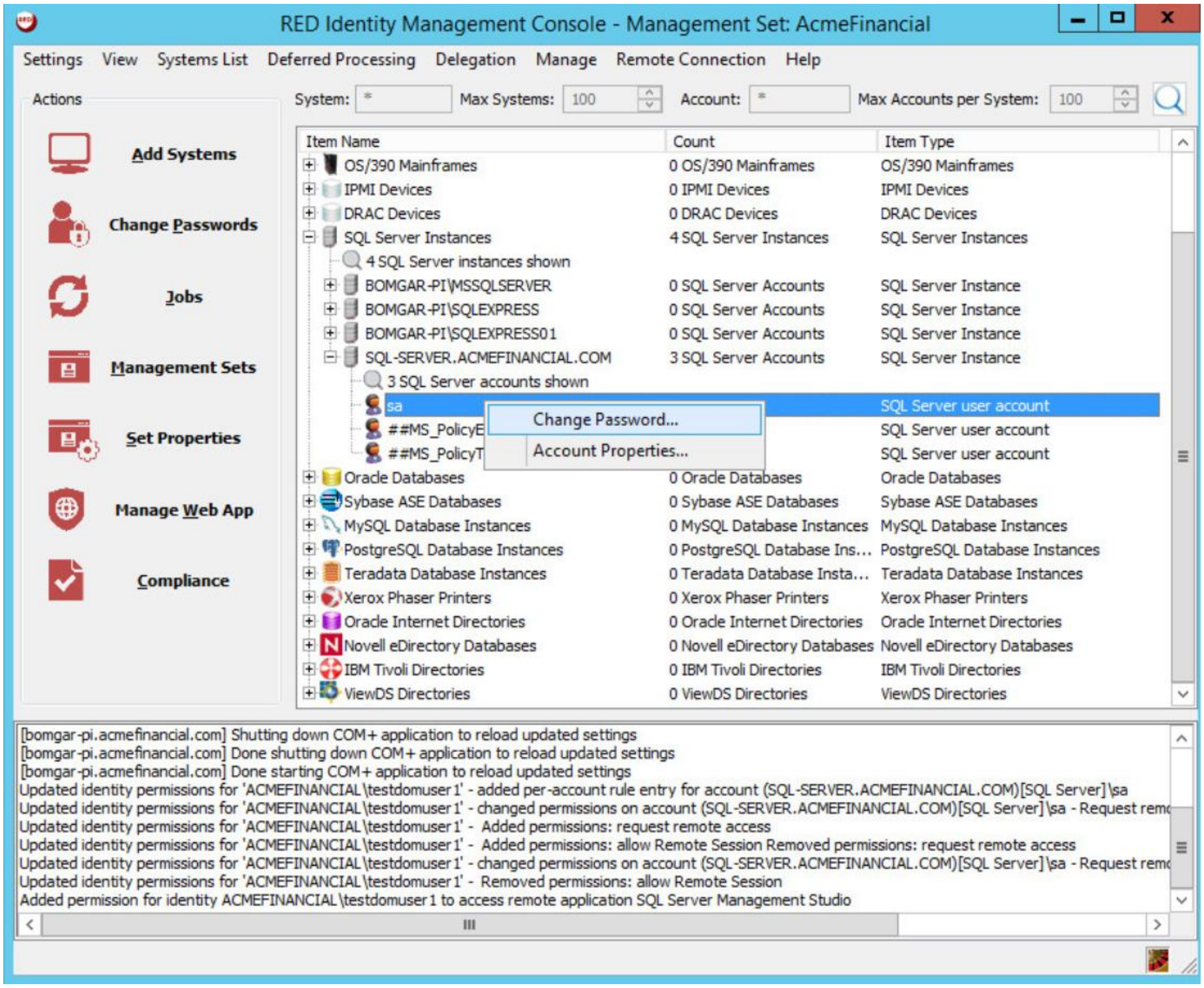
Login Account Password: •••••••••••••

Provider Type: SQL Server through OLEDB

□ Use Provider Encryption

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.**



System: * Max Systems: 100 Account: * Max Accounts per System: 100

Item Name	Count	Item Type
OS/390 Mainframes	0 OS/390 Mainframes	OS/390 Mainframes
IPMI Devices	0 IPMI Devices	IPMI Devices
DRAC Devices	0 DRAC Devices	DRAC Devices
SQL Server Instances	4 SQL Server Instances	SQL Server Instances
4 SQL Server instances shown		
BOMGAR-PI\MSSQLSERVER	0 SQL Server Accounts	SQL Server Instance
BOMGAR-PI\SQLEXPRESS	0 SQL Server Accounts	SQL Server Instance
BOMGAR-PI\SQLEXPRESS01	0 SQL Server Accounts	SQL Server Instance
SQL-SERVER.ACMEFINANCIAL.COM	3 SQL Server Accounts	SQL Server Instance
3 SQL Server accounts shown		
sa		SQL Server user account
##MS_PolicyE		SQL Server user account
##MS_PolicyT		SQL Server user account
Oracle Databases	0 Oracle Databases	Oracle Databases
Sybase ASE Databases	0 Sybase ASE Databases	Sybase ASE Databases
MySQL Database Instances	0 MySQL Database Instances	MySQL Database Instances
PostgreSQL Database Instances	0 PostgreSQL Database Ins...	PostgreSQL Database Instances
Teradata Database Instances	0 Teradata Database Insta...	Teradata Database Instances
Xerox Phaser Printers	0 Xerox Phaser Printers	Xerox Phaser Printers
Oracle Internet Directories	0 Oracle Internet Directories	Oracle Internet Directories
Novell eDirectory Databases	0 Novell eDirectory Databases	Novell eDirectory Databases
IBM Tivoli Directories	0 IBM Tivoli Directories	IBM Tivoli Directories
ViewDS Directories	0 ViewDS Directories	ViewDS Directories

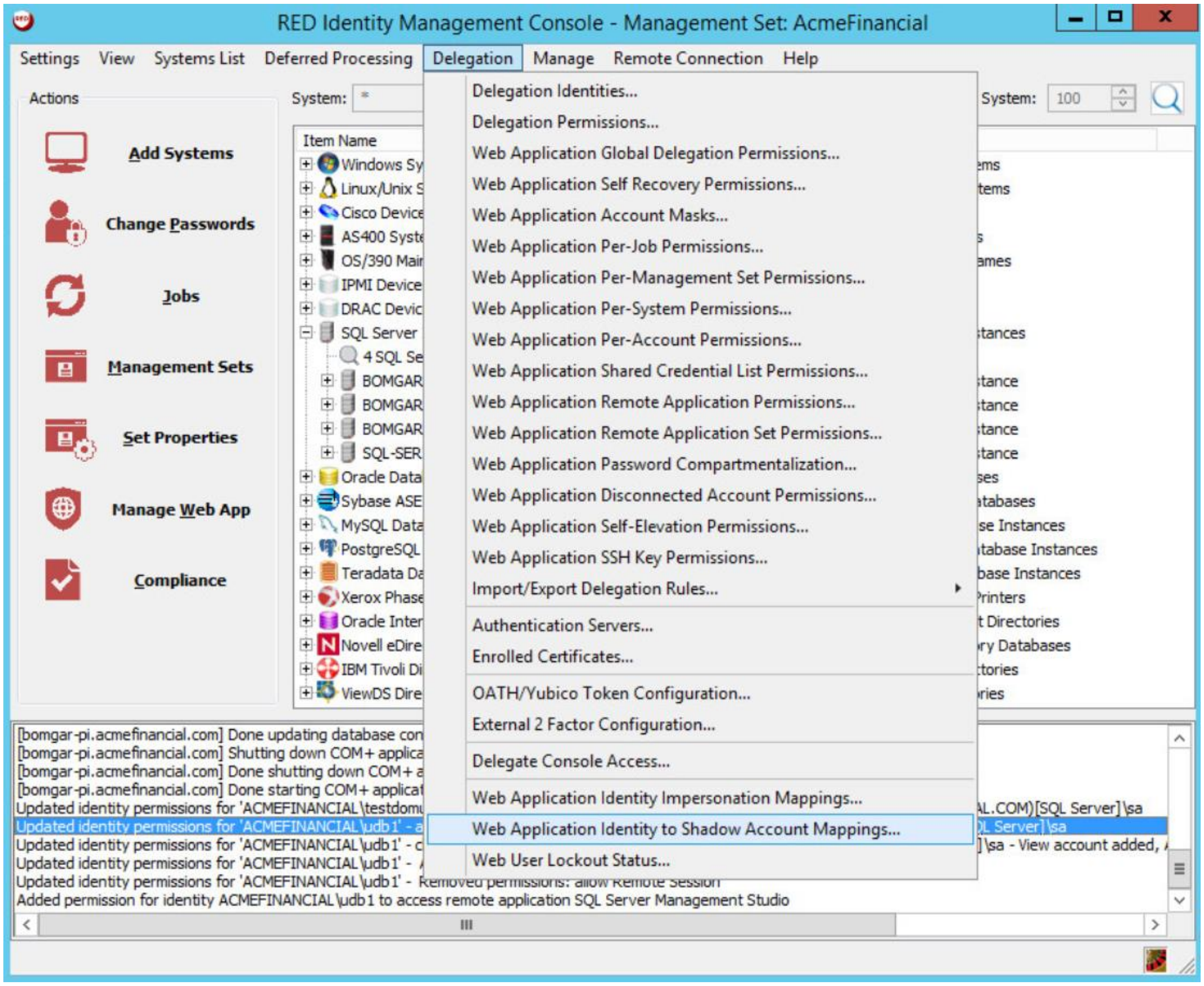
```
[bomgar-pi.acmefinancial.com] Shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done starting COM+ application to reload updated settings
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - added per-account rule entry for account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - changed permissions on account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa - Request rem
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' -  Added permissions: request remote access
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' -  Added permissions: allow Remote Session Removed permissions: request remote access
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - changed permissions on account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa - Request rem
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' -  Removed permissions: allow Remote Session
Added permission for identity ACMEFINANCIAL\testdomuser1 to access remote application SQL Server Management Studio
```

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.

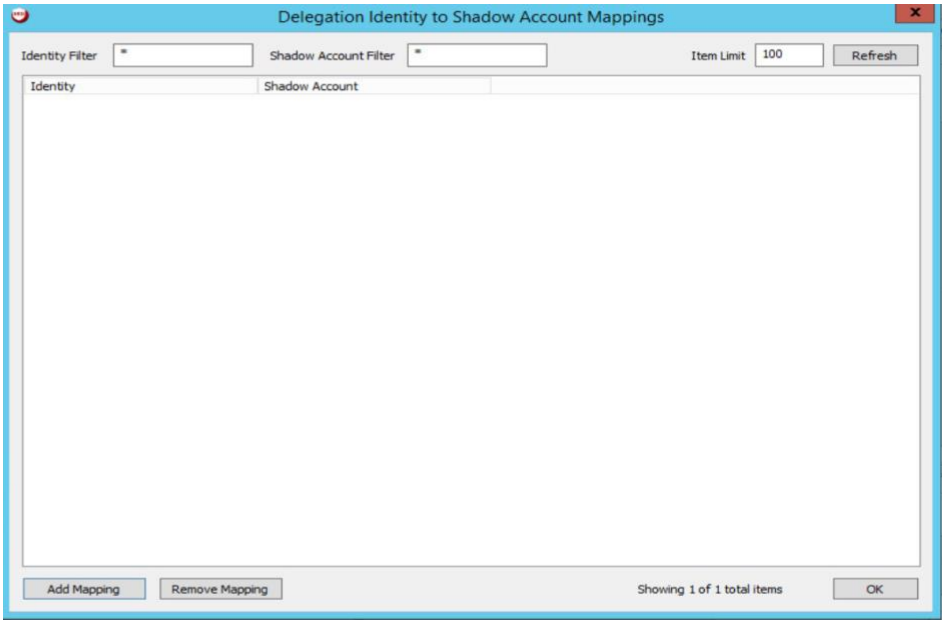
7. Click **OK,** and then let the operation complete.

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


RED Identity Management Console - Management Set: AcmeFinancial
Settings
View
Systems List
Deferred Processing
Delegation
Manage
Remote Connection
Help
Actions
Add Systems
Change Passwords
Jobs
Management Sets
Set Properties
Manage Web App
Compliance
System:
Item Name
Windows Sy
Linux/Unix S
Cisco Device
AS400 Syste
OS/390 Mair
IPMI Device
DRAC Devic
SQL Server
4 SQL Se
BOMGAR
BOMGAR
BOMGAR
SQL-SER
Oracle Data
Sybase ASE
MySQL Data
PostgreSQL
Teradata Da
Xerox Phase
Oracle Inter
Novell eDire
IBM Tivoli Di
ViewDS Dire
Delegation Identities...
Delegation Permissions...
Web Application Global Delegation Permissions...
Web Application Self Recovery Permissions...
Web Application Account Masks...
Web Application Per-Job Permissions...
Web Application Per-Management Set Permissions...
Web Application Per-System Permissions...
Web Application Per-Account Permissions...
Web Application Shared Credential List Permissions...
Web Application Remote Application Permissions...
Web Application Remote Application Set Permissions...
Web Application Password Compartmentalization...
Web Application Disconnected Account Permissions...
Web Application Self-Elevation Permissions...
Web Application SSH Key Permissions...
Import/Export Delegation Rules...
Authentication Servers...
Enrolled Certificates...
OATH/Yubico Token Configuration...
External 2 Factor Configuration...
Delegate Console Access...
Web Application Identity Impersonation Mappings...
Web Application Identity to Shadow Account Mappings...
Web User Lockout Status...
System:
100

```
[bomgar-pi.acmefinancial.com] Done updating database con
[bomgar-pi.acmefinancial.com] Shutting down COM+ applica
[bomgar-pi.acmefinancial.com] Done shutting down COM+ a
[bomgar-pi.acmefinancial.com] Done starting COM+ applicat
Updated identity permissions for 'ACMEFINANCIAL\testdomu                                       L.COM)[SQL Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\udb1' - a                                      L Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\udb1' - c                                      ]\sa - View account added, /
Updated identity permissions for 'ACMEFINANCIAL\udb1' - /
Updated identity permissions for 'ACMEFINANCIAL\udb1' - Removed permissions: allow Remote Session
Added permission for identity ACMEFINANCIAL\udb1 to access remote application SQL Server Management Studio
```

9. Click **Add Mapping.**



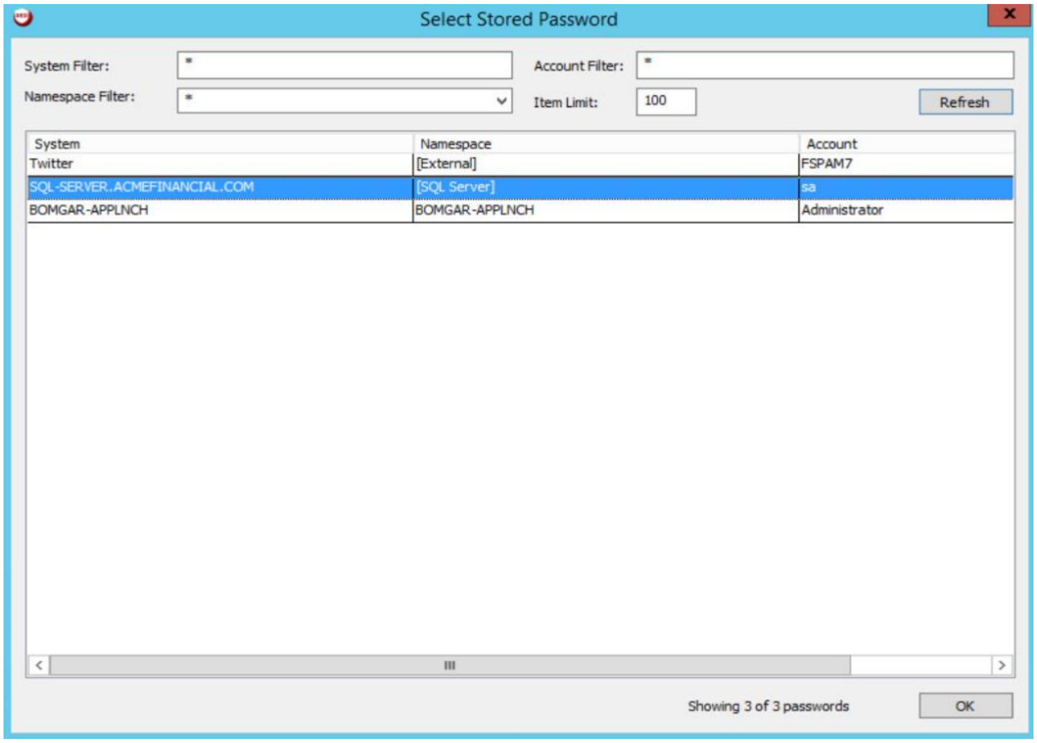
Identity Filter: *

Shadow Account Filter: *

Item Limit: 100

Showing 1 of 1 total items

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.**



System Filter: *

Account Filter: *

Namespace Filter: *

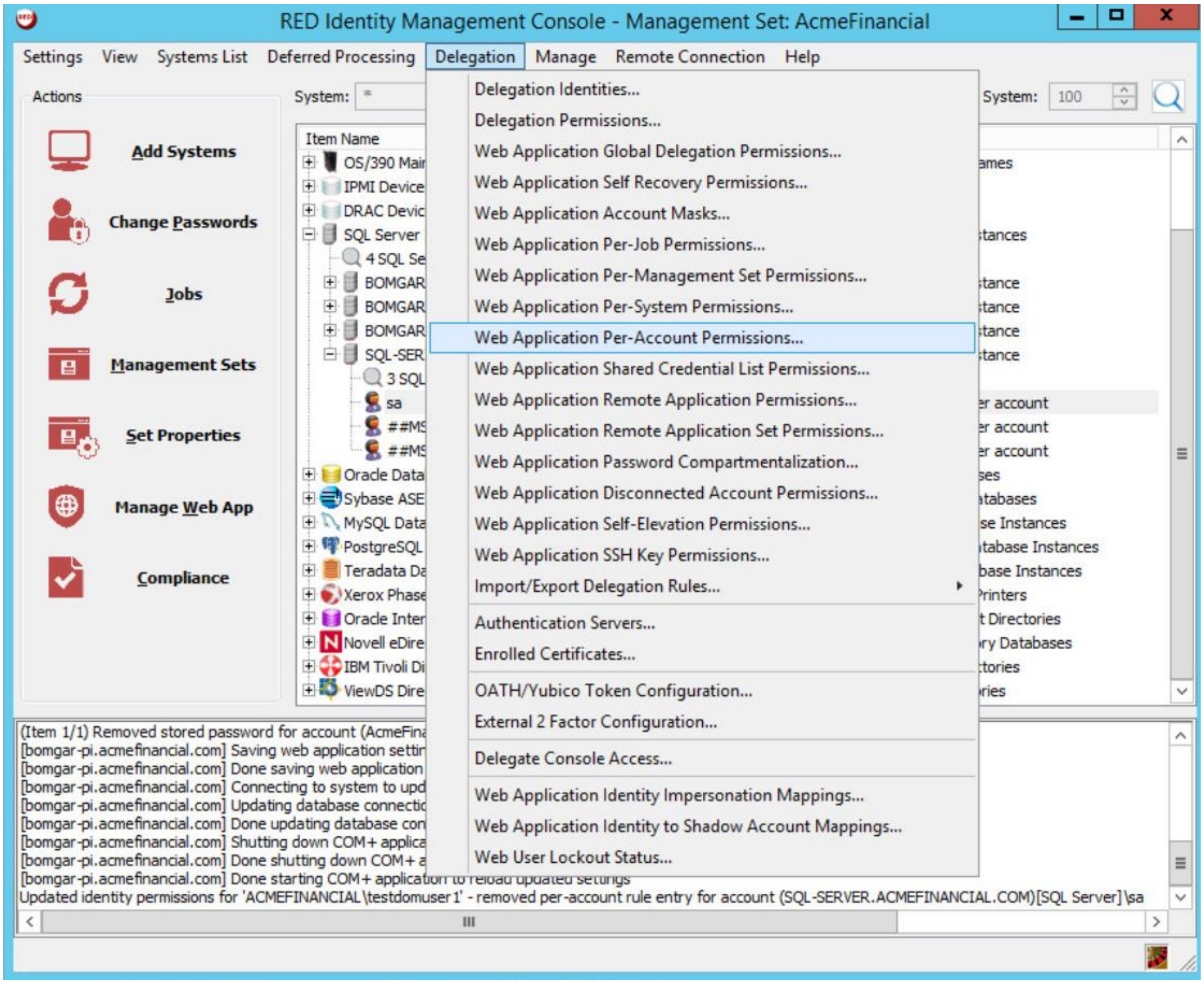
Item Limit: 100

System	Namespace	Account
Twitter	[External]	FSPAM7
SQL-SERVER.ACMEFINANCIAL.COM	[SQL Server]	sa
BOMGAR-APPLNCH	BOMGAR-APPLNCH	Administrator

Showing 3 of 3 passwords

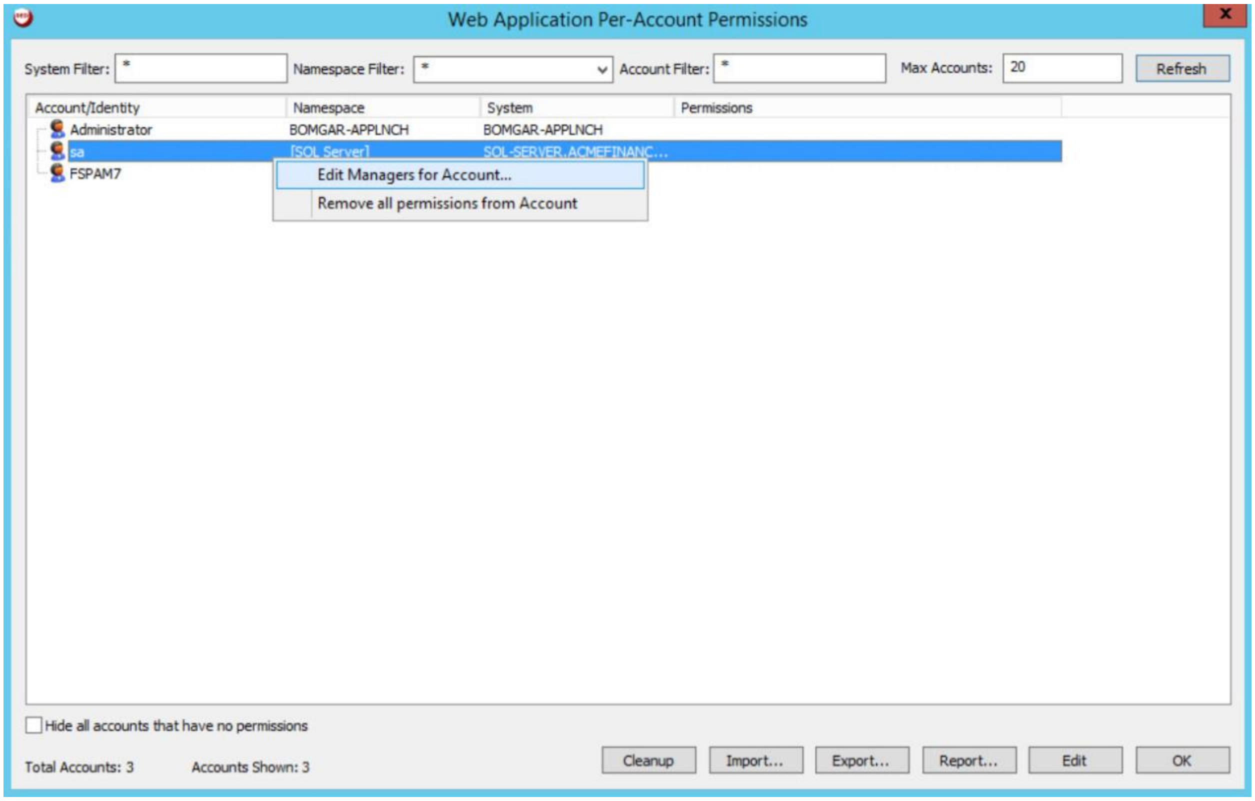
11. Click **OK** again.

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


RED Identity Management Console - Management Set: AcmeFinancial
Settings
View
Systems List
Deferred Processing
Delegation
Manage
Remote Connection
Help
Actions
Add Systems
Change Passwords
Jobs
Management Sets
Set Properties
Manage Web App
Compliance
System:
Item Name
OS/390 Mai
IPMI Device
DRAC Devic
SQL Server
4 SQL Se
BOMGAR
BOMGAR
BOMGAR
SQL-SER
3 SQL
sa
##MS
##MS
Oracle Data
Sybase ASE
MySQL Data
PostgreSQL
Teradata Da
Xerox Phase
Oracle Inter
Novell eDire
IBM Tivoli Di
ViewDS Dire
Delegation Identities...
Delegation Permissions...
Web Application Global Delegation Permissions...
Web Application Self Recovery Permissions...
Web Application Account Masks...
Web Application Per-Job Permissions...
Web Application Per-Management Set Permissions...
Web Application Per-System Permissions...
Web Application Per-Account Permissions...
Web Application Shared Credential List Permissions...
Web Application Remote Application Permissions...
Web Application Remote Application Set Permissions...
Web Application Password Compartmentalization...
Web Application Disconnected Account Permissions...
Web Application Self-Elevation Permissions...
Web Application SSH Key Permissions...
Import/Export Delegation Rules...
Authentication Servers...
Enrolled Certificates...
OATH/Yubico Token Configuration...
External 2 Factor Configuration...
Delegate Console Access...
Web Application Identity Impersonation Mappings...
Web Application Identity to Shadow Account Mappings...
Web User Lockout Status...
System:
100
ames
tances
tance
tance
tance
tance
er account
er account
er account
ses
tabases
se Instances
tabase Instances
base Instances
Printers
t Directories
ry Databases
tories
ries

```
(Item 1/1) Removed stored password for account (AcmeFina
[bomgar-pi.acmefinancial.com] Saving web application settir
[bomgar-pi.acmefinancial.com] Done saving web application
[bomgar-pi.acmefinancial.com] Connecting to system to upd
[bomgar-pi.acmefinancial.com] Updating database connectic
[bomgar-pi.acmefinancial.com] Done updating database con
[bomgar-pi.acmefinancial.com] Shutting down COM+ applica
[bomgar-pi.acmefinancial.com] Done shutting down COM+ a
[bomgar-pi.acmefinancial.com] Done starting COM+ application to reload updated settings
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - removed per-account rule entry for account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa
```

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



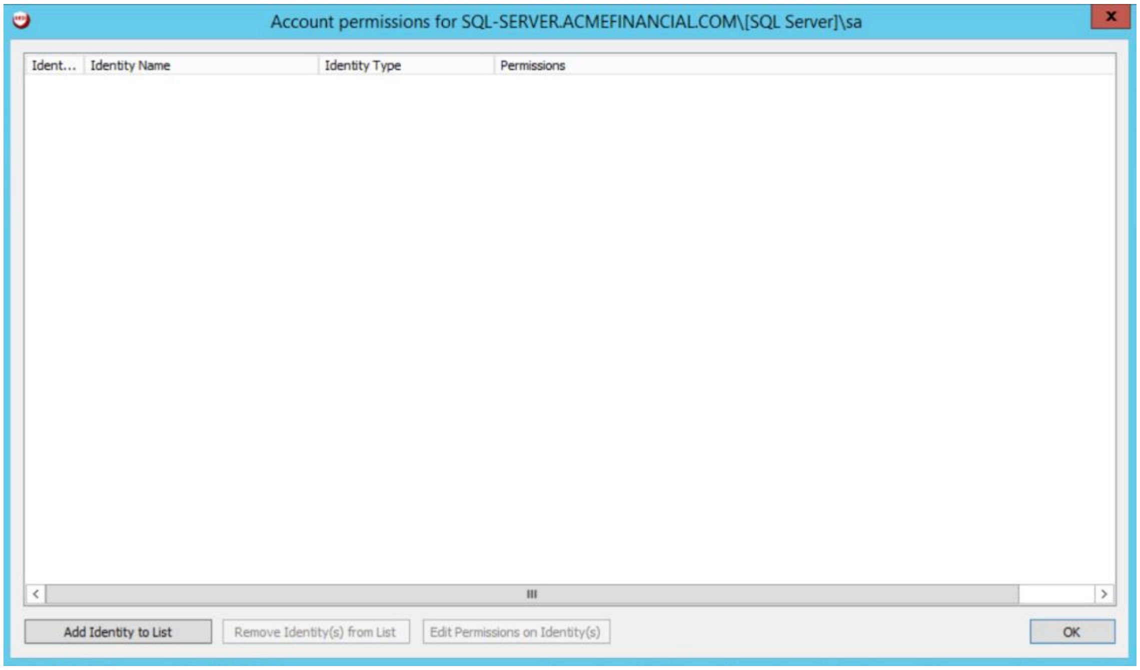
Web Application Per-Account Permissions

System Filter: * Namespace Filter: * Account Filter: * Max Accounts: 20

Account/Identity	Namespace	System	Permissions
Administrator	BOMGAR-APPLNCH	BOMGAR-APPLNCH	
sa	[SQL Server]	SQL-SERVER.ACMEFINANC...	
FSPAM7			

Refresh
Edit Managers for Account...
Remove all permissions from Account
□ Hide all accounts that have no permissions
Total Accounts: 3
Accounts Shown: 3
Cleanup
Import...
Export...
Report...
Edit
OK

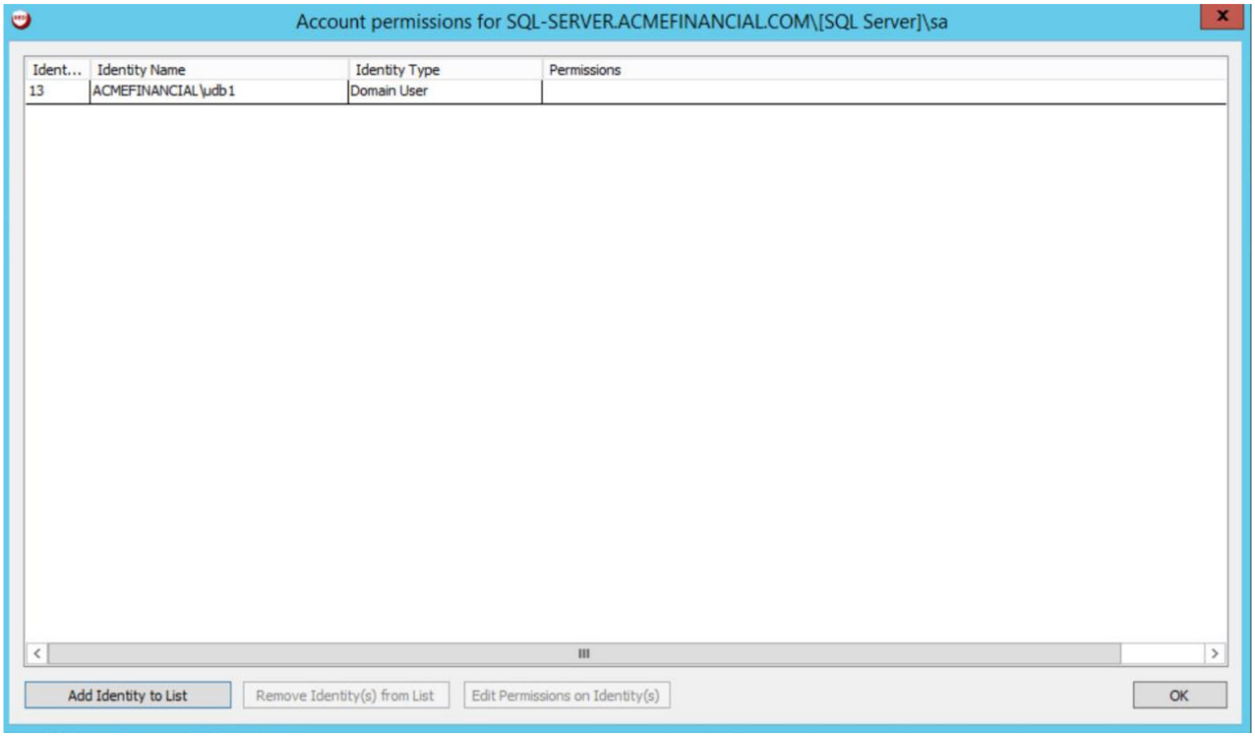
14. Click **Add Identity to List.**



Account permissions for SQL-SERVER.ACMEFINANCIAL.COM\[SQL Server]\sa

Ident...	Identity Name	Identity Type	Permissions

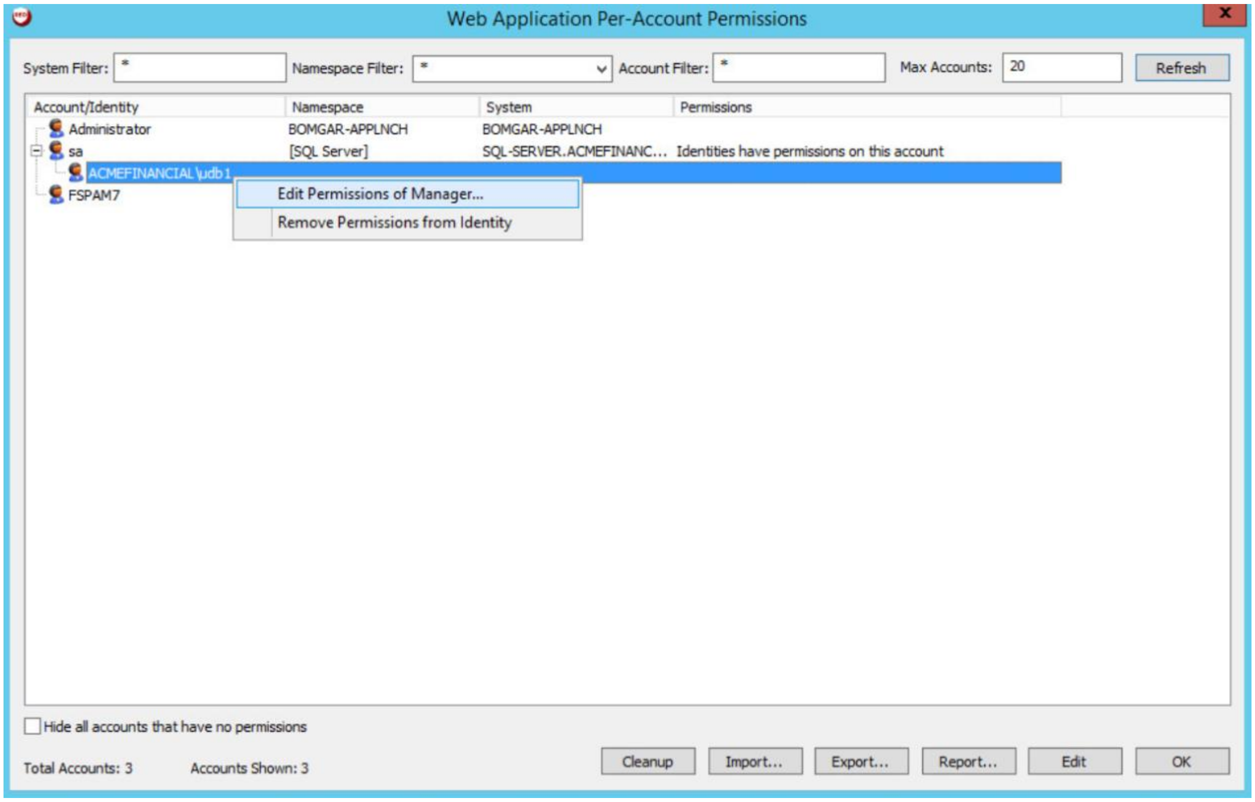
15. Select the **ACMEFINANCIAL\udb1** account. You should see it appear in the list. Click **OK.**



Account permissions for SQL-SERVER.ACMEFINANCIAL.COM\[SQL Server]\sa

Ident...	Identity Name	Identity Type	Permissions
13	ACMEFINANCIAL\udb1	Domain User	

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.**



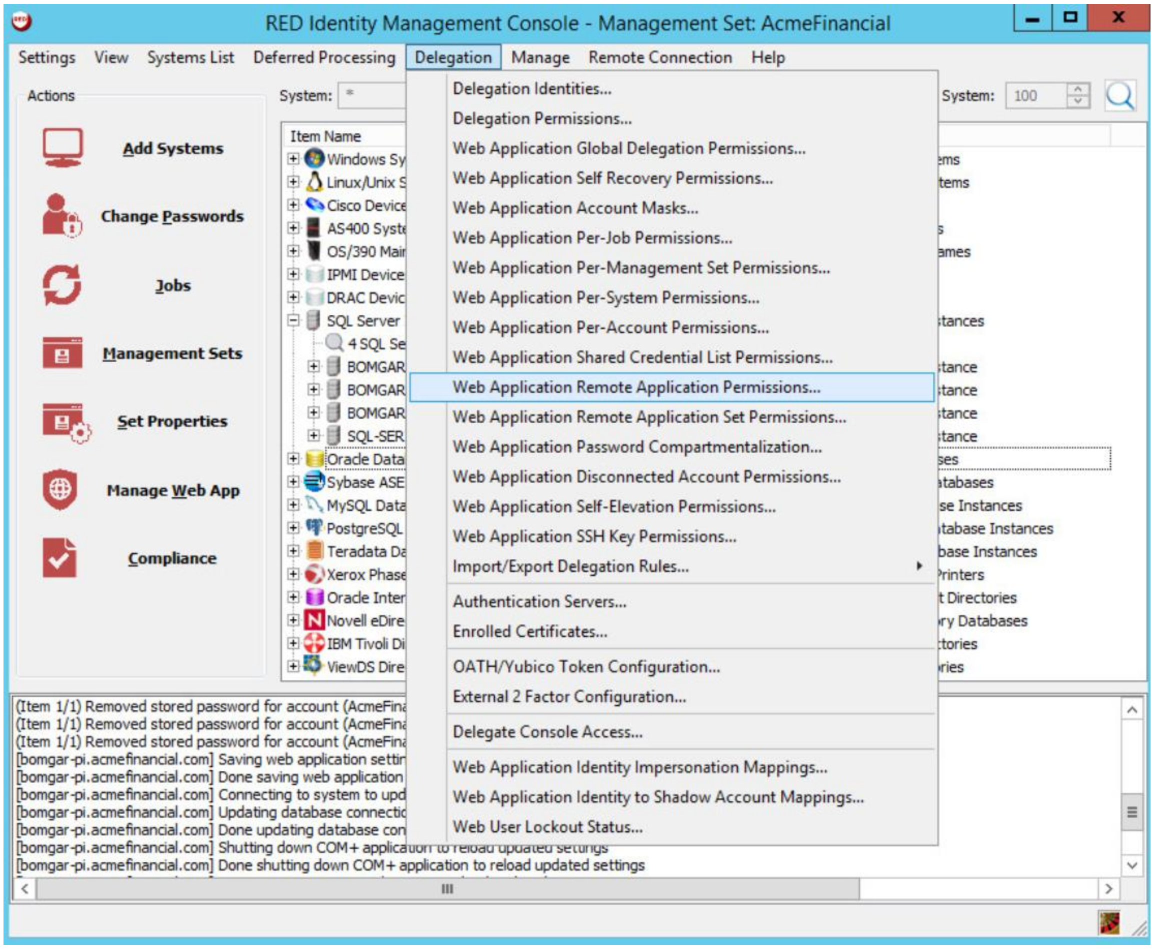
Account/Identity	Namespace	System	Permissions
Administrator	BOMGAR-APPLNCH	BOMGAR-APPLNCH	
sa	[SQL Server]	SQL-SERVER.ACMEFINANC...	Identities have permissions on this account
ACMEFINANCIAL\udb1			
FSPAM7			

□ Hide all accounts that have no permissions

Total Accounts: 3   Accounts Shown: 3

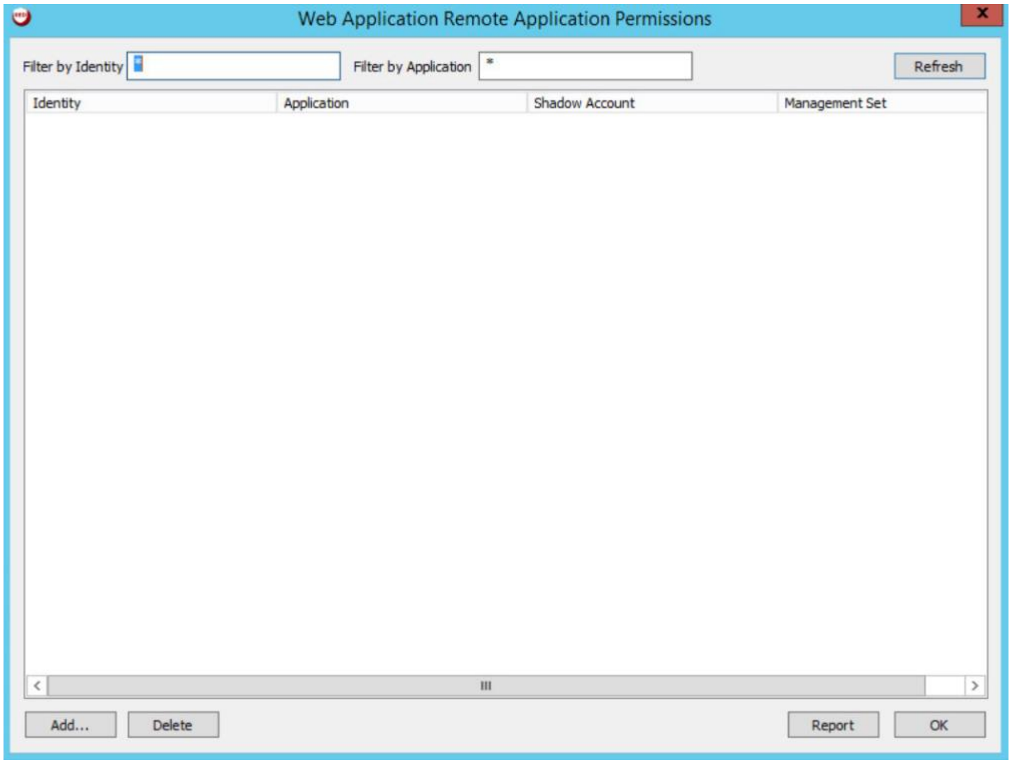
17. Give the account the **View Account** and **Request Remote Access** permissions. Click **OK**. Click **OK** again to exit the **Web Application Per-Account Permissions** window.

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

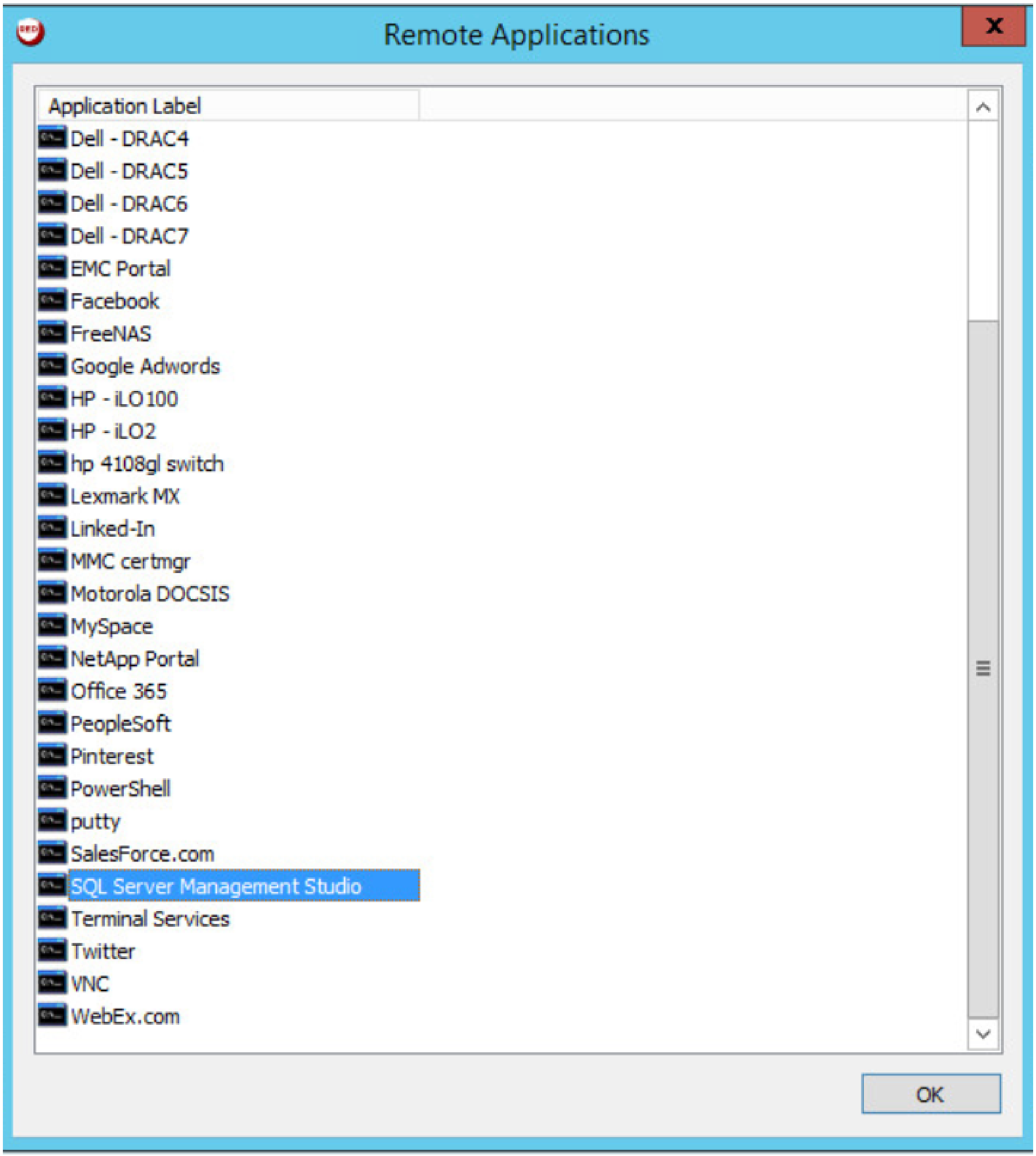

RED Identity Management Console - Management Set: AcmeFinancial
Settings
View
Systems List
Deferred Processing
Delegation
Manage
Remote Connection
Help
Actions
Add Systems
Change Passwords
Jobs
Management Sets
Set Properties
Manage Web App
Compliance
System: *
System: 100
Item Name
Windows Sy
Linux/Unix S
Cisco Device
AS400 Syste
OS/390 Mair
IPMI Device
DRAC Devic
SQL Server
4 SQL Se
BOMGAR
BOMGAR
BOMGAR
SQL-SER
Oracle Data
Sybase ASE
MySQL Data
PostgreSQL
Teradata Da
Xerox Phase
Oracle Inter
Novell eDire
IBM Tivoli Di
ViewDS Dire
Delegation Identities...
Delegation Permissions...
Web Application Global Delegation Permissions...
Web Application Self Recovery Permissions...
Web Application Account Masks...
Web Application Per-Job Permissions...
Web Application Per-Management Set Permissions...
Web Application Per-System Permissions...
Web Application Per-Account Permissions...
Web Application Shared Credential List Permissions...
Web Application Remote Application Permissions...
Web Application Remote Application Set Permissions...
Web Application Password Compartmentalization...
Web Application Disconnected Account Permissions...
Web Application Self-Elevation Permissions...
Web Application SSH Key Permissions...
Import/Export Delegation Rules...
Authentication Servers...
Enrolled Certificates...
OATH/Yubico Token Configuration...
External 2 Factor Configuration...
Delegate Console Access...
Web Application Identity Impersonation Mappings...
Web Application Identity to Shadow Account Mappings...
Web User Lockout Status...
ems
tems
s
ames
tances
tance
tance
tance
tance
ses
atabases
se Instances
atabase Instances
base Instances
Printers
t Directories
ry Databases
ctories
ries

```
(Item 1/1) Removed stored password for account (AcmeFina
(Item 1/1) Removed stored password for account (AcmeFina
(Item 1/1) Removed stored password for account (AcmeFina
[bomgar-pi.acmefinancial.com] Saving web application settin
[bomgar-pi.acmefinancial.com] Done saving web application
[bomgar-pi.acmefinancial.com] Connecting to system to upd
[bomgar-pi.acmefinancial.com] Updating database connectio
[bomgar-pi.acmefinancial.com] Done updating database con
[bomgar-pi.acmefinancial.com] Shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done shutting down COM+ application to reload updated settings
```

19. Click **Add.**



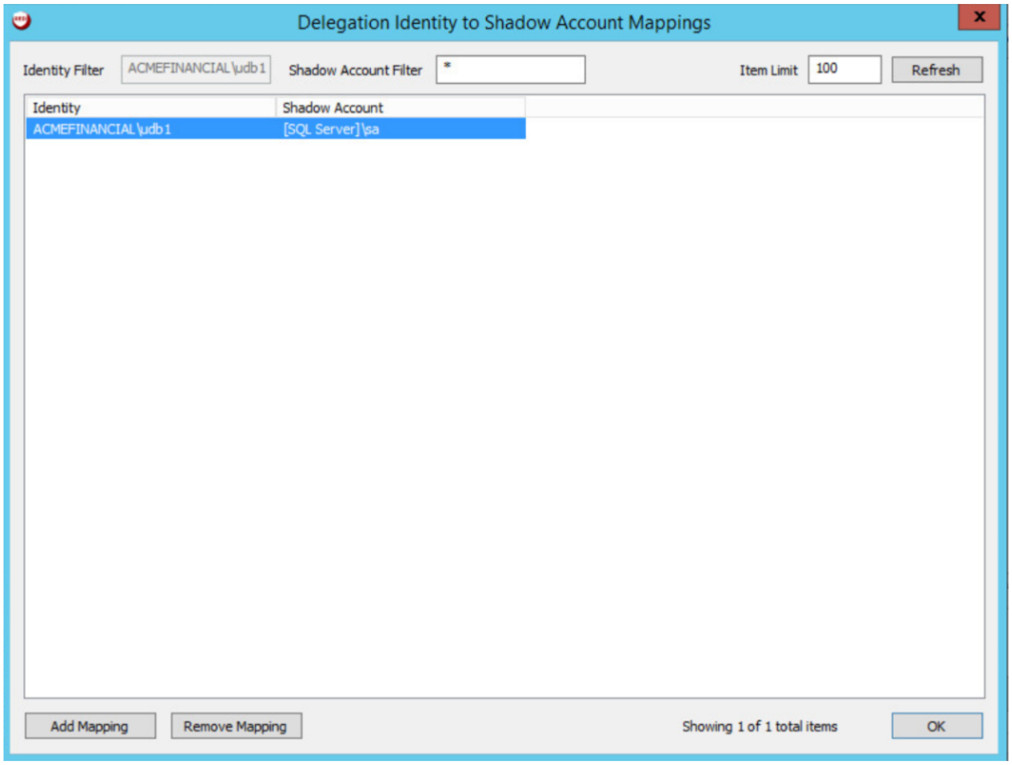
20. Select the **ACMEFINANCIAL\udb1** account from the list of **Delegation Identities.** Click **OK.** Next, select **SQL Server Management Studio** from the list of **Remote Applications.**



Application Label
Dell - DRAC4
Dell - DRAC5
Dell - DRAC6
Dell - DRAC7
EMC Portal
Facebook
FreeNAS
Google Adwords
HP - iLO100
HP - iLO2
hp 4108gl switch
Lexmark MX
Linked-In
MMC certmgr
Motorola DOCSIS
MySpace
NetApp Portal
Office 365
PeopleSoft
Pinterest
PowerShell
putty
SalesForce.com
SQL Server Management Studio
Terminal Services
Twitter
VNC
WebEx.com

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.**



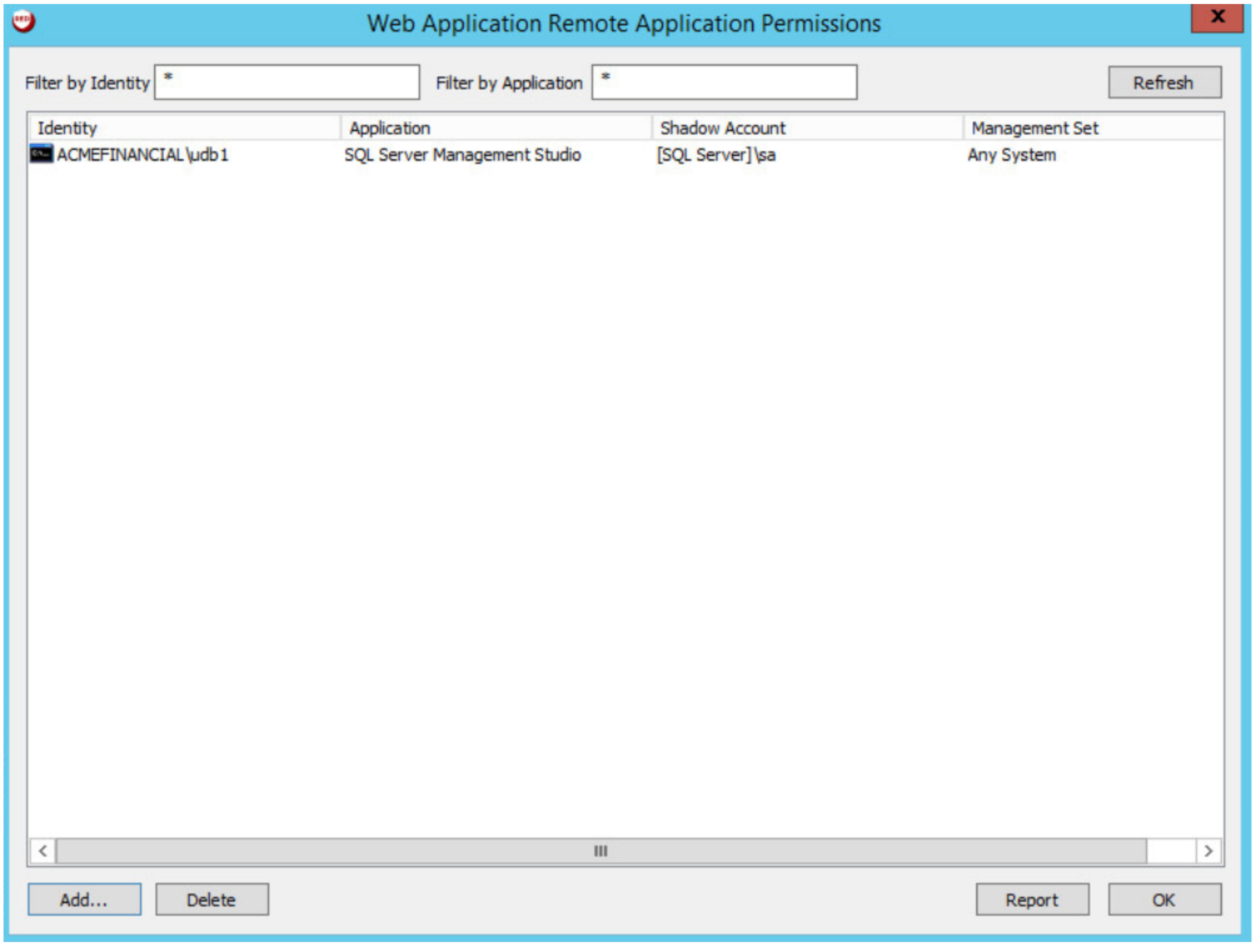
Identity Filter: ACMEFINANCIAL\udb1
Shadow Account Filter: *
Item Limit: 100

Identity	Shadow Account
ACMEFINANCIAL\udb1	[SQL Server]\sa

Showing 1 of 1 total items

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.**



Filter by Identity: *

Filter by Application: *

Identity	Application	Shadow Account	Management Set
ACMEFINANCIAL\udb1	SQL Server Management Studio	[SQL Server]\sa	Any System

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.

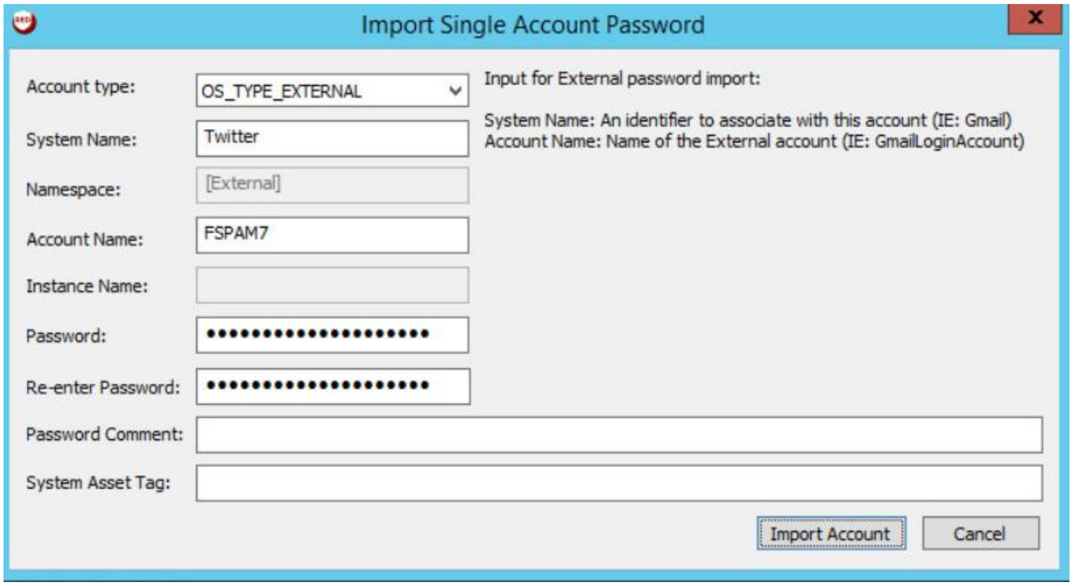
To launch Twitter, Bomgar-PI needs the Twitter account password. The following steps detail how to add an external password to Bomgar-PI:

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>



Account type: OS_TYPE_EXTERNAL

System Name: Twitter

Namespace: [External]

Account Name: FSPAM7

Instance Name:

Password: ••••••••••••••••••••

Re-enter Password: ••••••••••••••••••••

Password Comment:

System Asset Tag:

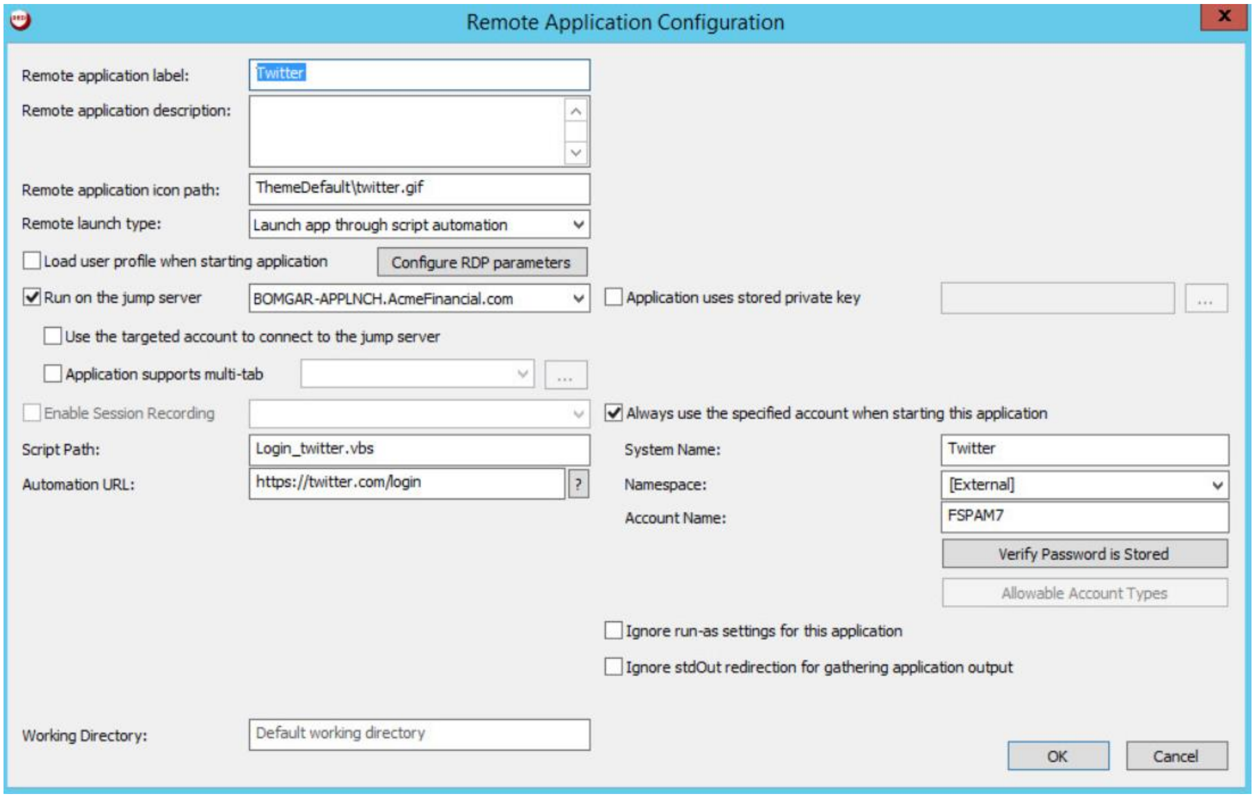
Input for External password import:

System Name: An identifier to associate with this account (IE: Gmail)
Account Name: Name of the External account (IE: GmailLoginAccount)

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>



Remote Application Configuration

Remote application label: Twitter

Remote application description:

Remote application icon path: ThemeDefault\twitter.gif

Remote launch type: Launch app through script automation

□ Load user profile when starting application

☑ Run on the jump server: BOMGAR-APPLNCH.AcmeFinancial.com

□ Application uses stored private key

□ Use the targeted account to connect to the jump server

□ Application supports multi-tab

□ Enable Session Recording

☑ Always use the specified account when starting this application

Script Path: Login_twitter.vbs

Automation URL: https://twitter.com/login

System Name: Twitter

Namespace: [External]

Account Name: FSPAM7

□ Ignore run-as settings for this application

□ Ignore stdOut redirection for gathering application output

Working Directory: Default working directory

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

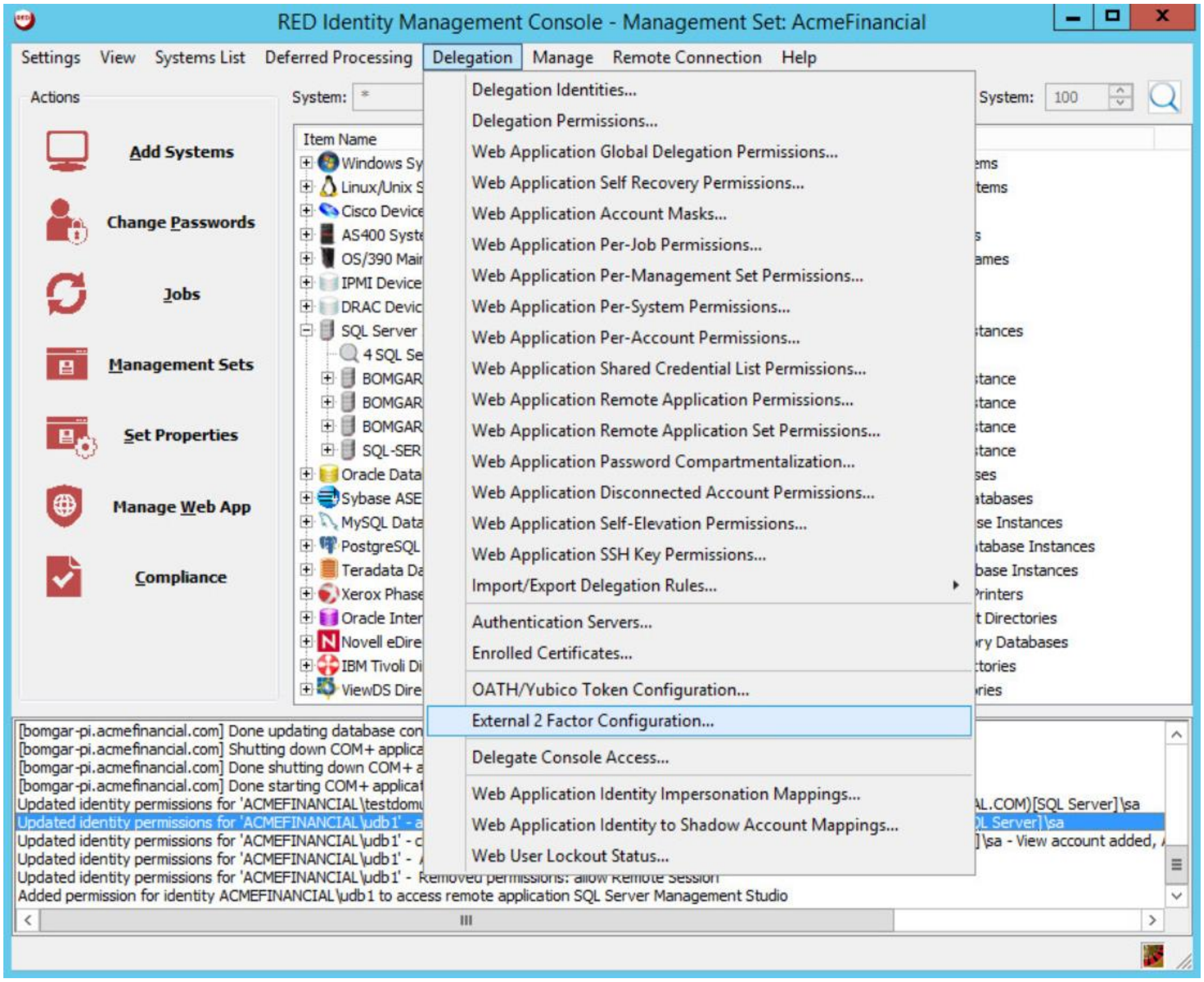
To allow users to launch Twitter, follow these steps:

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

2.2.10 Configuring Multifactor Authentication with RSA

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

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


RED Identity Management Console - Management Set: AcmeFinancial
Settings
View
Systems List
Deferred Processing
Delegation
Manage
Remote Connection
Help
Actions
Add Systems
Change Passwords
Jobs
Management Sets
Set Properties
Manage Web App
Compliance
System:
Item Name
Windows Sy
Linux/Unix S
Cisco Device
AS400 Syste
OS/390 Mair
IPMI Device
DRAC Devic
SQL Server
4 SQL Se
BOMGAR
BOMGAR
BOMGAR
SQL-SER
Oracle Data
Sybase ASE
MySQL Data
PostgreSQL
Teradata Da
Xerox Phase
Oracle Inter
Novell eDire
IBM Tivoli Di
ViewDS Dire
Delegation Identities...
Delegation Permissions...
Web Application Global Delegation Permissions...
Web Application Self Recovery Permissions...
Web Application Account Masks...
Web Application Per-Job Permissions...
Web Application Per-Management Set Permissions...
Web Application Per-System Permissions...
Web Application Per-Account Permissions...
Web Application Shared Credential List Permissions...
Web Application Remote Application Permissions...
Web Application Remote Application Set Permissions...
Web Application Password Compartmentalization...
Web Application Disconnected Account Permissions...
Web Application Self-Elevation Permissions...
Web Application SSH Key Permissions...
Import/Export Delegation Rules...
Authentication Servers...
Enrolled Certificates...
OATH/Yubico Token Configuration...
External 2 Factor Configuration...
Delegate Console Access...
Web Application Identity Impersonation Mappings...
Web Application Identity to Shadow Account Mappings...
Web User Lockout Status...
System:
100
ems
tems
ames
tances
tance
tance
tance
tance
ses
tabases
se Instances
tabase Instances
base Instances
Printers
t Directories
ry Databases
tories
ries

```
[bomgar-pi.acmefinancial.com] Done updating database con
[bomgar-pi.acmefinancial.com] Shutting down COM+ applica
[bomgar-pi.acmefinancial.com] Done shutting down COM+ a
[bomgar-pi.acmefinancial.com] Done starting COM+ applicat
Updated identity permissions for 'ACMEFINANCIAL\testdomu                    AL.COM)[SQL Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\udb1' - a                   L Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\udb1' - c                   ]\sa - View account added, /
Updated identity permissions for 'ACMEFINANCIAL\udb1' - /
Updated identity permissions for 'ACMEFINANCIAL\udb1' - Removed permissions: allow Remote Session
Added permission for identity ACMEFINANCIAL\udb1 to access remote application SQL Server Management Studio
```

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)

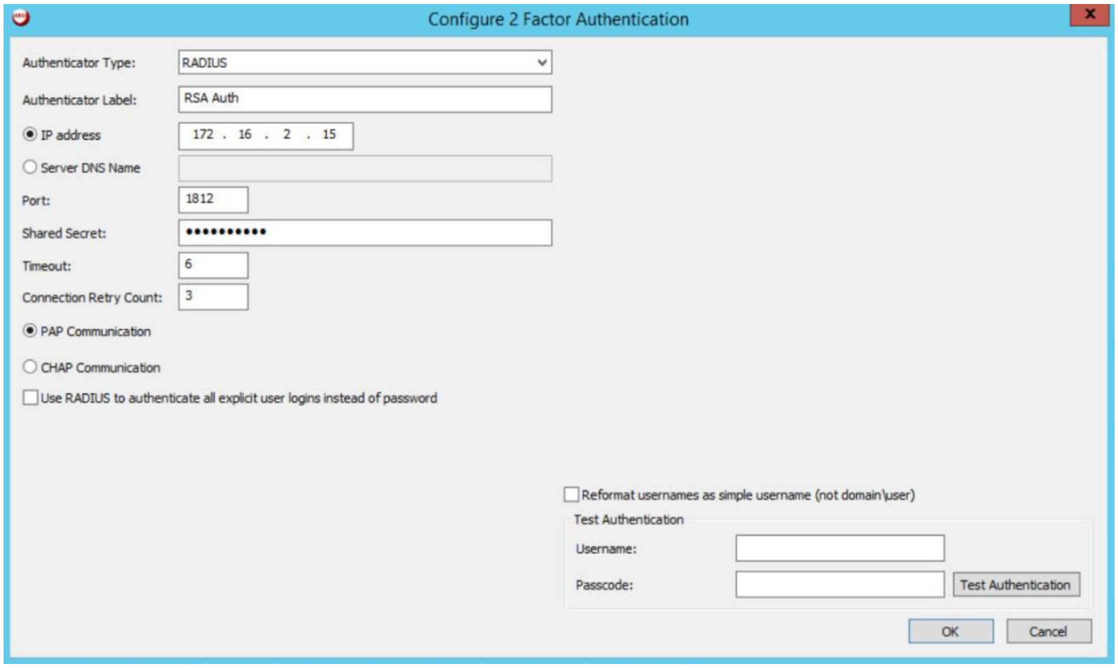
d. **Port:** 1812

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.



Configure 2 Factor Authentication

Authenticator Type: RADIUS

Authenticator Label: RSA Auth

● IP address 172 . 16 . 2 . 15

○ Server DNS Name

Port: 1812

Shared Secret: ••••••••••

Timeout: 6

Connection Retry Count: 3

● PAP Communication

○ CHAP Communication

□ Use RADIUS to authenticate all explicit user logins instead of password

□ Reformat usernames as simple username (not domain\user)

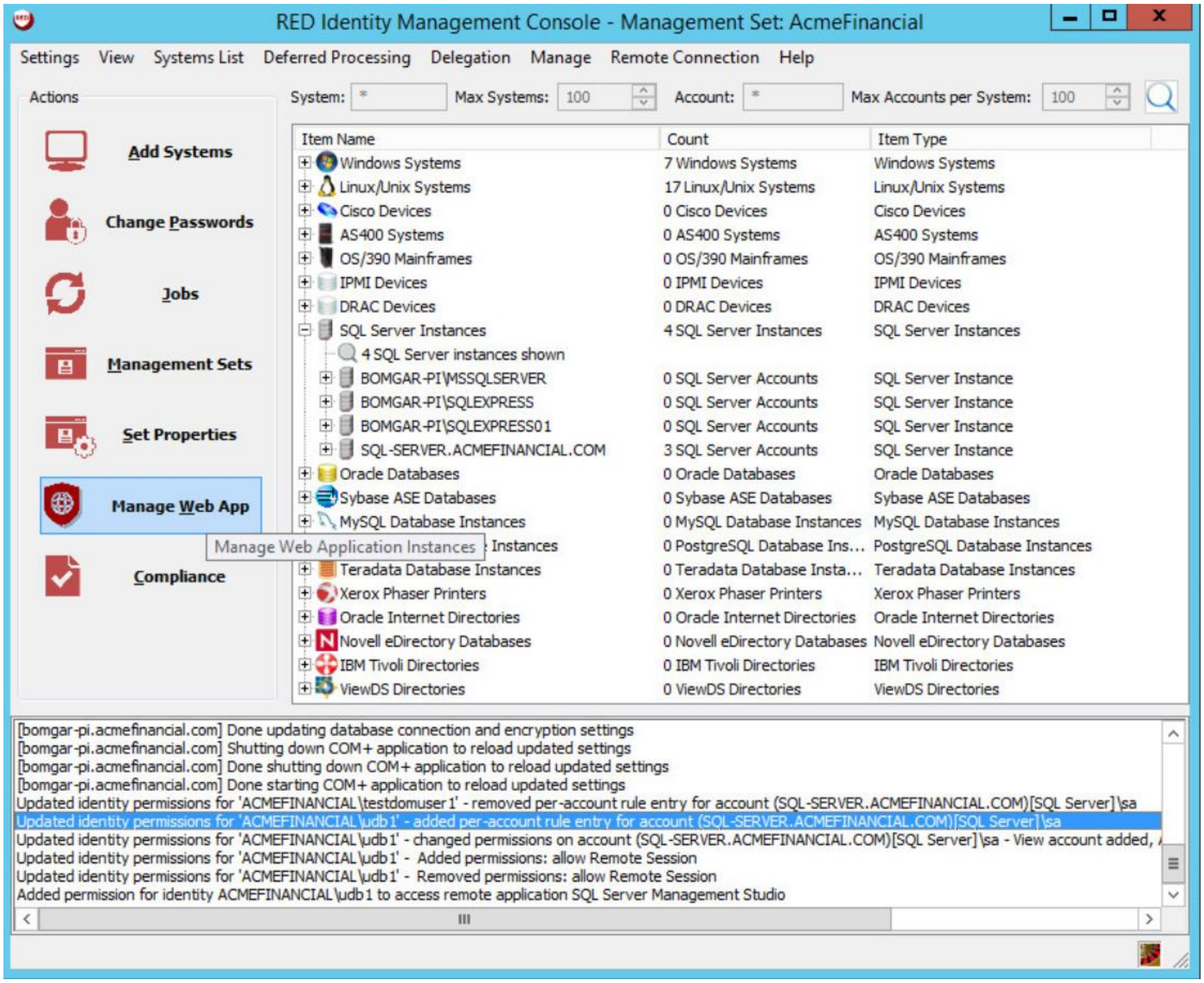
Test Authentication

Username:

Passcode:

3. Click **OK.**

4. Click **Manage Web App.**

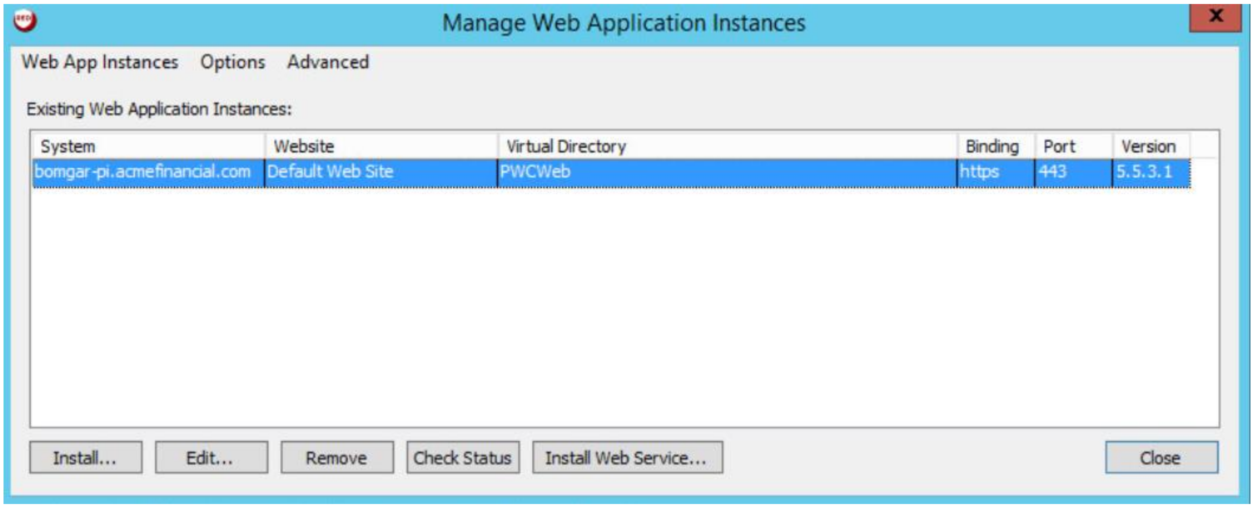


System: * Max Systems: 100 Account: * Max Accounts per System: 100

Item Name	Count	Item Type
Windows Systems	7 Windows Systems	Windows Systems
Linux/Unix Systems	17 Linux/Unix Systems	Linux/Unix Systems
Cisco Devices	0 Cisco Devices	Cisco Devices
AS400 Systems	0 AS400 Systems	AS400 Systems
OS/390 Mainframes	0 OS/390 Mainframes	OS/390 Mainframes
IPMI Devices	0 IPMI Devices	IPMI Devices
DRAC Devices	0 DRAC Devices	DRAC Devices
SQL Server Instances	4 SQL Server Instances	SQL Server Instances
4 SQL Server instances shown		
BOMGAR-PI\MSSQLSERVER	0 SQL Server Accounts	SQL Server Instance
BOMGAR-PI\SQLEXPRESS	0 SQL Server Accounts	SQL Server Instance
BOMGAR-PI\SQLEXPRESS01	0 SQL Server Accounts	SQL Server Instance
SQL-SERVER.ACMEFINANCIAL.COM	3 SQL Server Accounts	SQL Server Instance
Oracle Databases	0 Oracle Databases	Oracle Databases
Sybase ASE Databases	0 Sybase ASE Databases	Sybase ASE Databases
MySQL Database Instances	0 MySQL Database Instances	MySQL Database Instances
Instances	0 PostgreSQL Database Ins…	PostgreSQL Database Instances
Teradata Database Instances	0 Teradata Database Insta…	Teradata Database Instances
Xerox Phaser Printers	0 Xerox Phaser Printers	Xerox Phaser Printers
Oracle Internet Directories	0 Oracle Internet Directories	Oracle Internet Directories
Novell eDirectory Databases	0 Novell eDirectory Databases	Novell eDirectory Databases
IBM Tivoli Directories	0 IBM Tivoli Directories	IBM Tivoli Directories
ViewDS Directories	0 ViewDS Directories	ViewDS Directories

```
[bomgar-pi.acmefinancial.com] Done updating database connection and encryption settings
[bomgar-pi.acmefinancial.com] Shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done shutting down COM+ application to reload updated settings
[bomgar-pi.acmefinancial.com] Done starting COM+ application to reload updated settings
Updated identity permissions for 'ACMEFINANCIAL\testdomuser1' - removed per-account rule entry for account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\udb1' - added per-account rule entry for account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa
Updated identity permissions for 'ACMEFINANCIAL\udb1' - changed permissions on account (SQL-SERVER.ACMEFINANCIAL.COM)[SQL Server]\sa - View account added, /
Updated identity permissions for 'ACMEFINANCIAL\udb1' -  Added permissions: allow Remote Session
Updated identity permissions for 'ACMEFINANCIAL\udb1' -  Removed permissions: allow Remote Session
Added permission for identity ACMEFINANCIAL\udb1 to access remote application SQL Server Management Studio
```

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

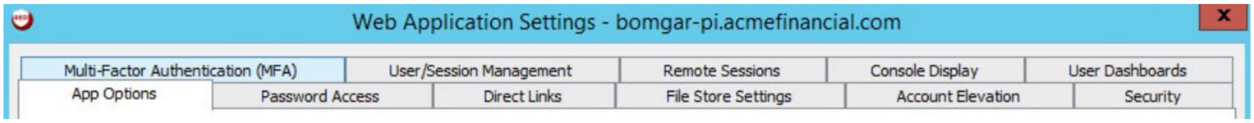


Existing Web Application Instances:

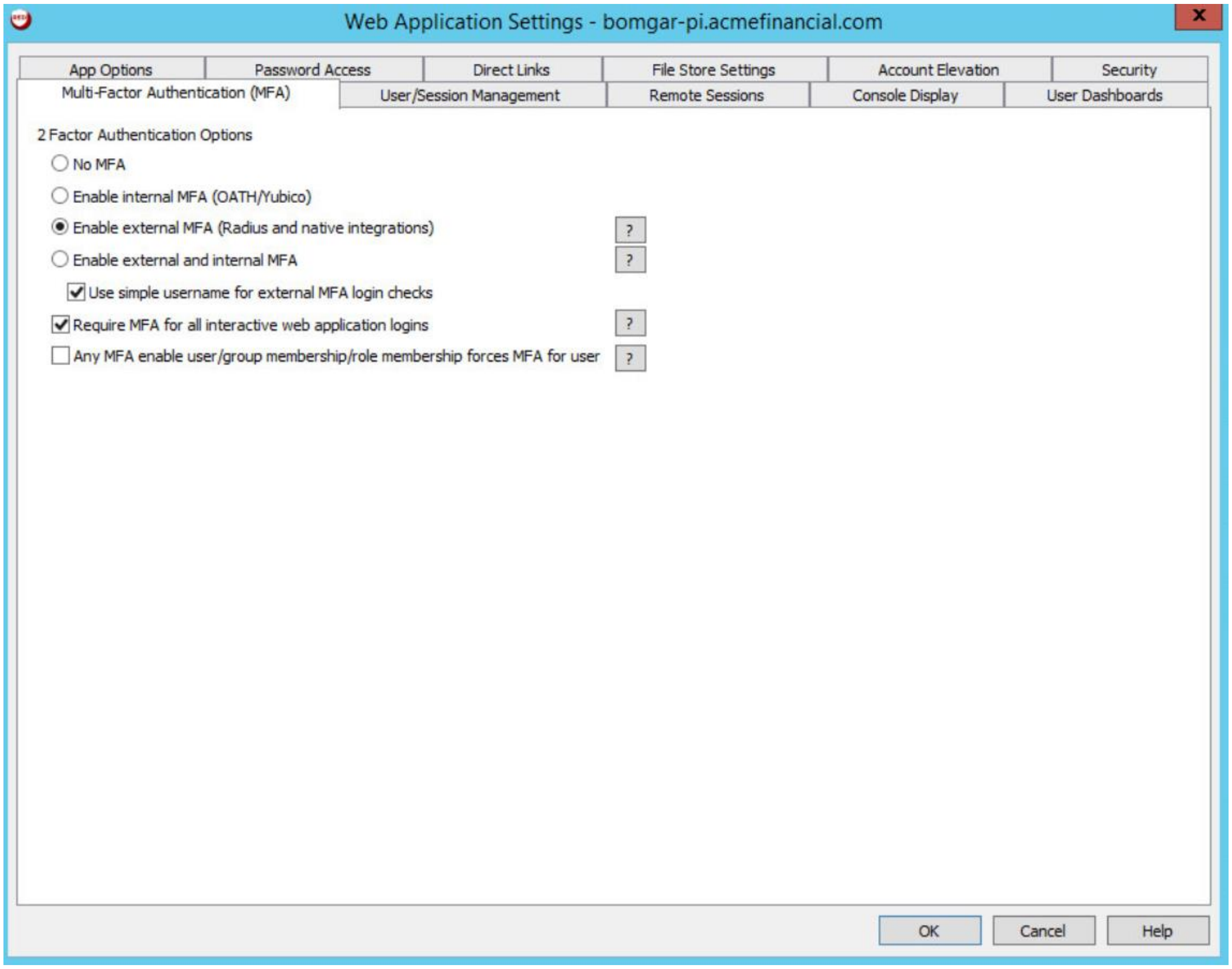
System	Website	Virtual Directory	Binding	Port	Version
bomgar-pi.acmefinancial.com	Default Web Site	PWCWeb	https	443	5.5.3.1

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.**



2 Factor Authentication Options

○ No MFA

○ Enable internal MFA (OATH/Yubico)

● Enable external MFA (Radius and native integrations) ?

○ Enable external and internal MFA ?

☑ Use simple username for external MFA login checks

☑ Require MFA for all interactive web application logins ?

□ Any MFA enable user/group membership/role membership forces MFA for user ?

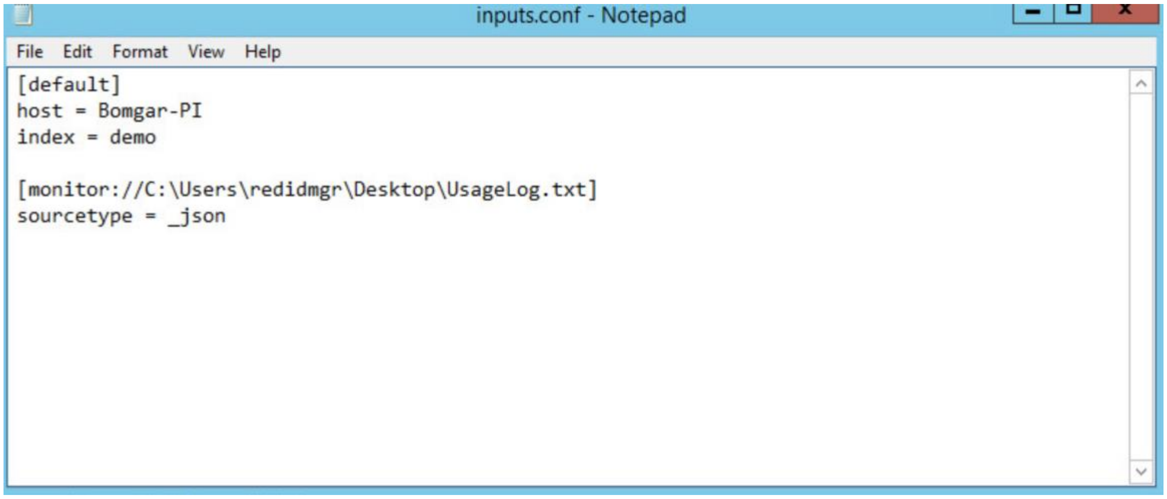
9. Click **OK.** Click **OK** again in the pop-up window.

10. Click **Close.**

2.2.11 Splunk Universal Forwarder

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

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



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

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

2.3 TDi ConsoleWorks

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

2.3.1 How It's Used

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

2.3.2 Virtual Machine Configuration

The TDi ConsoleWorks virtual machine is configured as follows:

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

Network Interface Configuration:

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

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

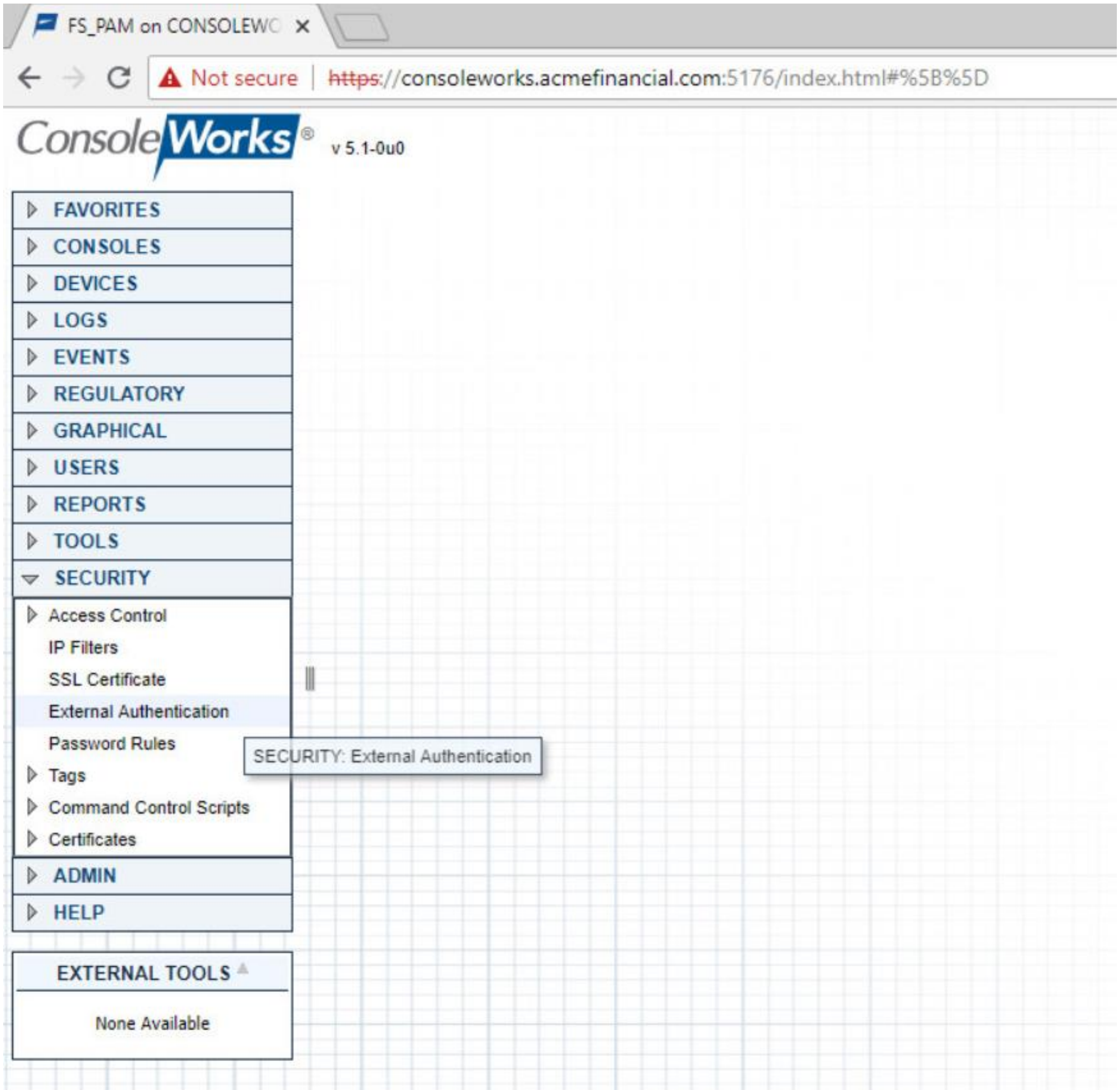
2.3.3 Installation

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

2.3.4 Configuration of Back-End Authentication

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

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

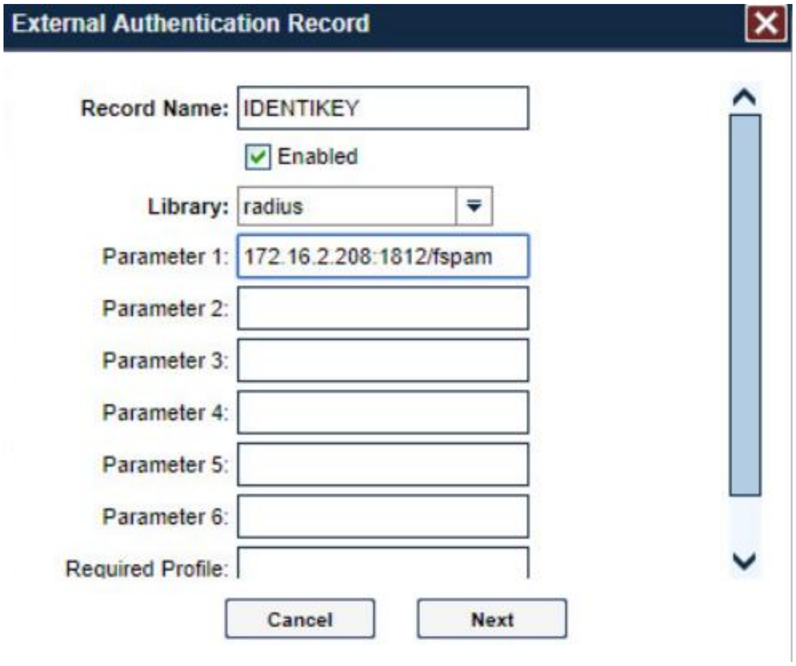


3. Click **Add.**
4. Fill out the **External Authentication Record** with the following information for the IDENTIKEY Authentication Server:
    a. **Record Name:** IDENTIKEY
    b. **Enabled:** This check box should be selected.

c. **Library:** radius

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

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


External Authentication Record

Record Name: IDENTIKEY

☑ Enabled

Library: radius

Parameter 1: 172.16.2.208:1812/fspam

Parameter 2:

Parameter 3:

Parameter 4:

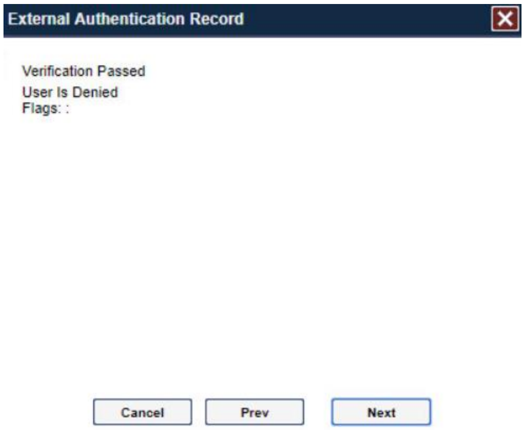
Parameter 5:

Parameter 6:

Required Profile:

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

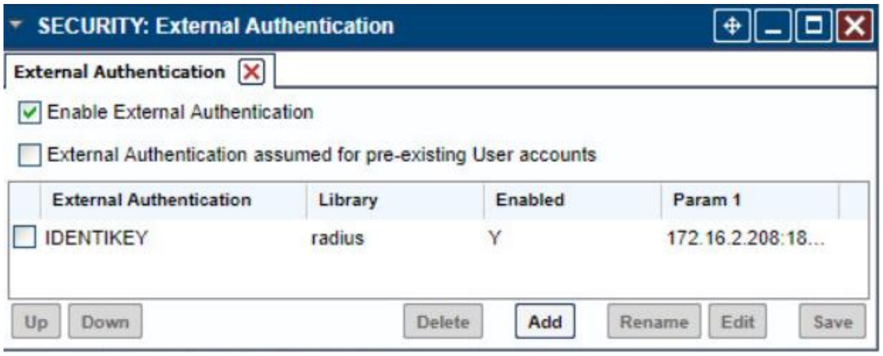
6. Check that the verification passed. The user should be denied. Click **Next.**


External Authentication Record

Verification Passed
User Is Denied
Flags: :

7. Click **Save.**

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



☑ Enable External Authentication

☐ External Authentication assumed for pre-existing User accounts

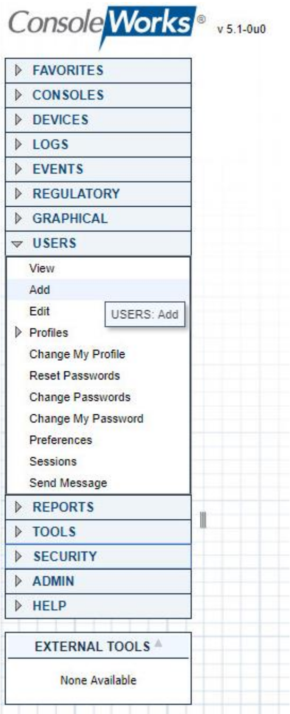
	External Authentication	Library	Enabled	Param 1
☐	IDENTIKEY	radius	Y	172.16.2.208:18...

9. Click **Save** if available.

2.3.5 Creating Users

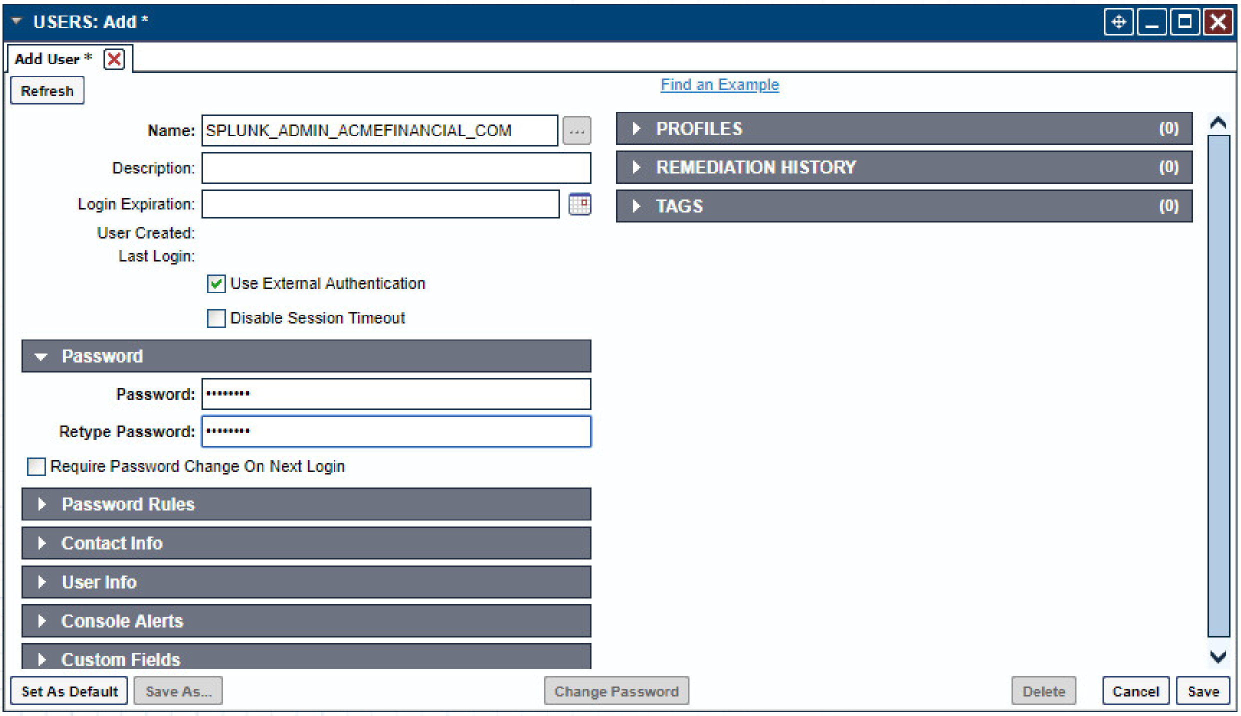
Each privileged user must have an account in ConsoleWorks to log into ConsoleWorks. The following steps detail the process of creating accounts for AD users in ConsoleWorks. For this example, we will create a ConsoleWorks account for the splunk_admin@acmefinancial.com AD account. This user will manage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



USERS: Add *

Add User *

Name: SPLUNK_ADMIN_ACMEFINANCIAL_COM

Description:

Login Expiration:

User Created:

Last Login:

☑ Use External Authentication

□ Disable Session Timeout

Password

Password: ••••••••

Retype Password: ••••••••

□ Require Password Change On Next Login

PROFILES (0)

REMEDIATION HISTORY (0)

TAGS (0)

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.

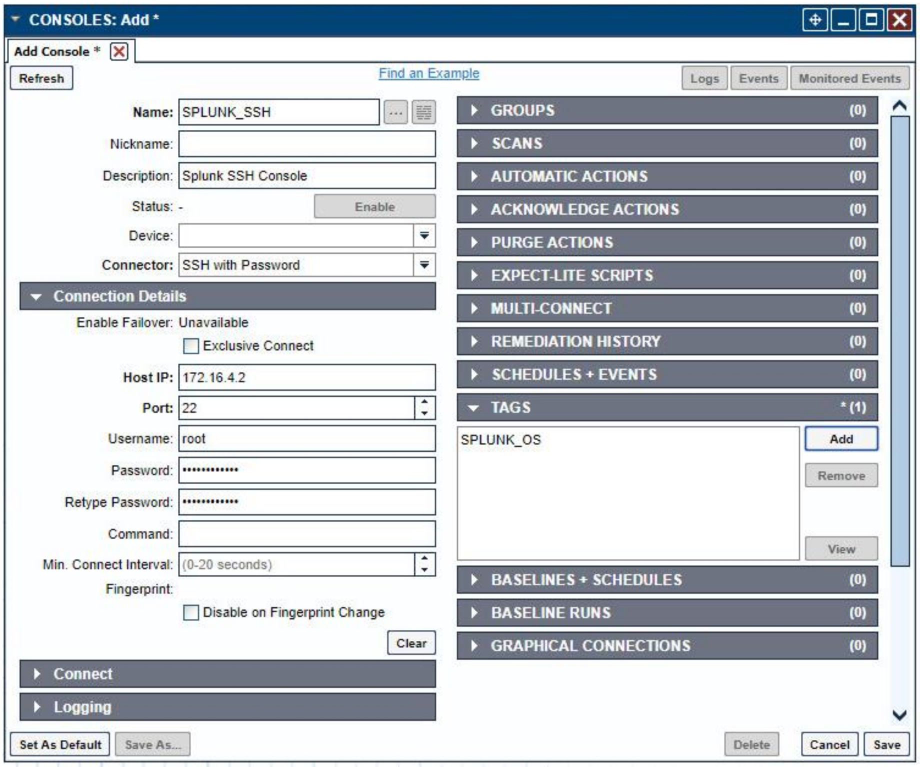
1. Click **SECURITY > Tags > Add.**
2. Fill out the pop-up window with the following information:
    a. **Name:** SPLUNK_OS
    b. (optional) **Description:** Splunk OS Consoles
3. Click **Save.**

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.



CONSOLES: Add *

Add Console *

Name: SPLUNK_SSH
Nickname:
Description: Splunk SSH Console
Status: -
Device:
Connector: SSH with Password

Connection Details
Enable Failover: Unavailable
□ Exclusive Connect
Host IP: 172.16.4.2
Port: 22
Username: root
Password: ••••••••••••
Retype Password: ••••••••••••
Command:
Min. Connect Interval: (0-20 seconds)
Fingerprint:
□ Disable on Fingerprint Change

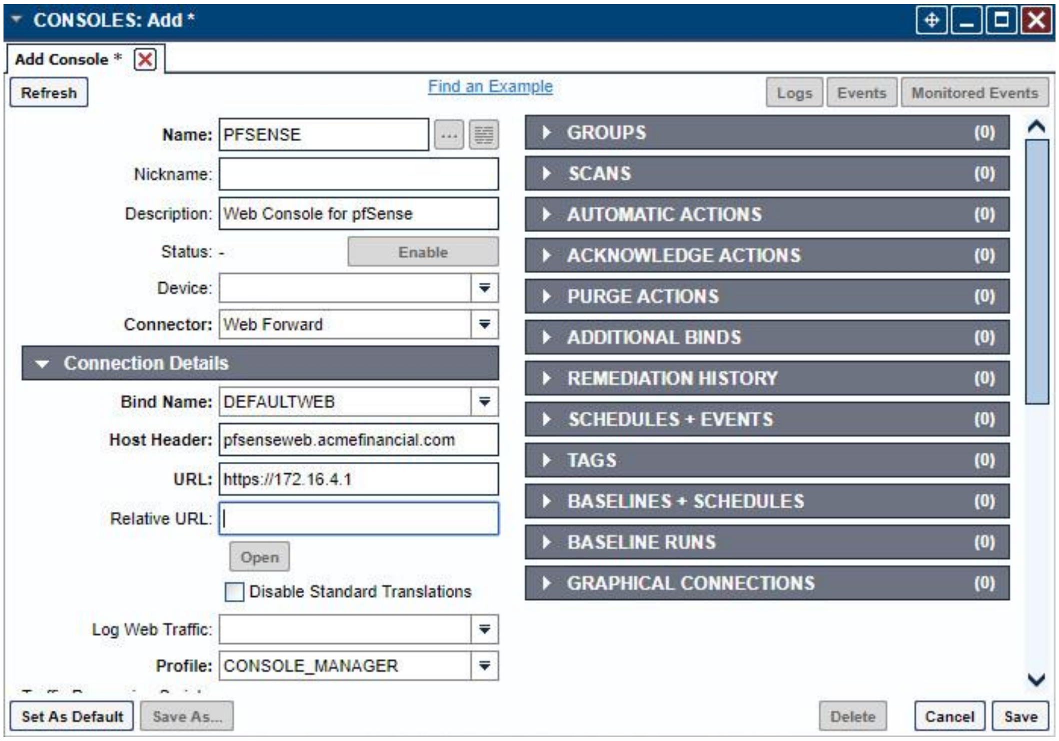
TAGS * (1)
SPLUNK_OS

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



Name: PFSENSE

Nickname:

Description: Web Console for pfSense

Status: -

Device:

Connector: Web Forward

Bind Name: DEFAULTWEB

Host Header: pfsenseweb.acmefinancial.com

URL: https://172.16.4.1

Relative URL:

□ Disable Standard Translations

Log Web Traffic:

Profile: CONSOLE_MANAGER

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

11. Click **Save.**

2.3.9 Assigning Tags to Consoles

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

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

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

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

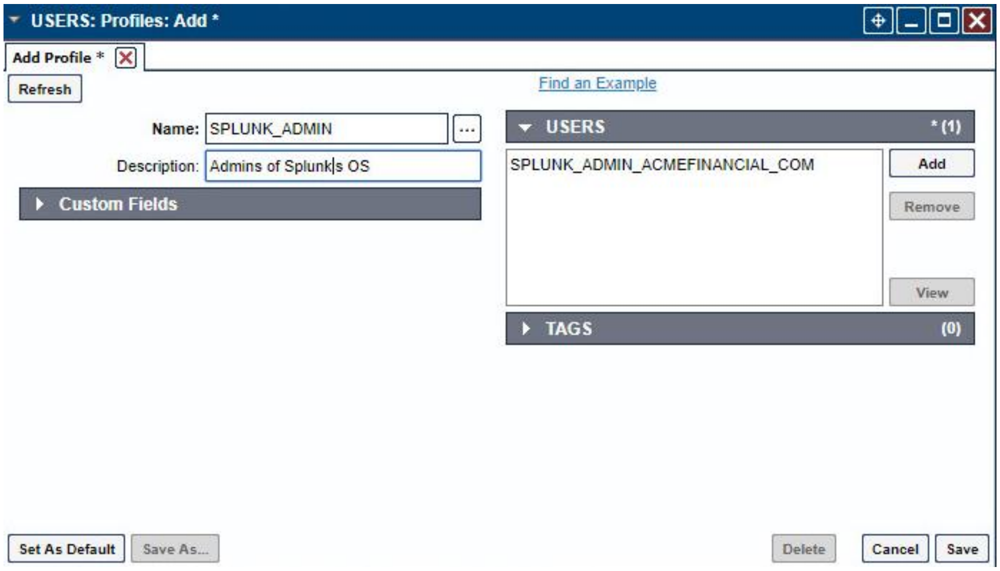
1. In ConsoleWorks, click **CONSOLES > View.**
2. Select a console (e.g., **PFSENSE**).
3. Click **Edit.**
4. Open the **TAGS** menu, and then click **Add.**
5. Move the pfSense consoles' tag to the list on the right, and then click **OK.**
6. Click **Save.**

2.3.10 Creating Profiles for Users

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

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

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



Name: SPLUNK_ADMIN

Description: Admins of Splunks OS

USERS: SPLUNK_ADMIN_ACMEFINANCIAL_COM

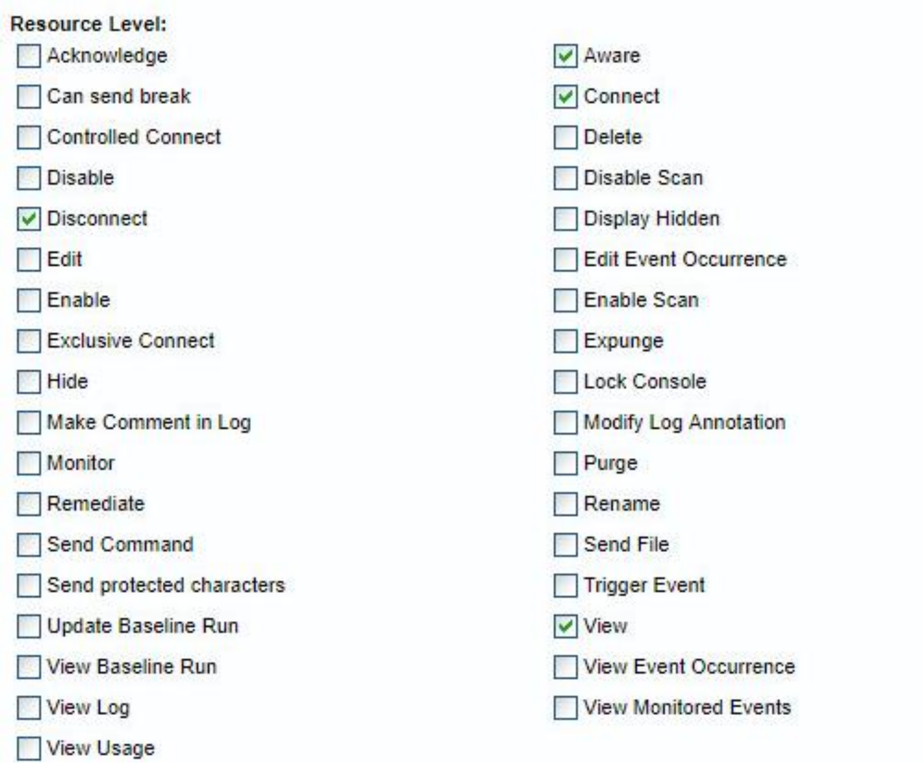
Use the same procedure provided above (while just changing the **Name, Description,** and **USERS** chosen) to create profiles for each group of users who should have access to a specific set of consoles. In this case, it was Splunk OS-level consoles. Next, it could be Splunk application-level consoles.

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**



Resource Level:

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

9. Click **Save.**

2.4 Ekran System

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

2.4.1 How It's Used

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

2.4.2 Virtual Machine Configuration

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

The Ekran System server virtual machine is configured as follows:

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

Network Configuration (Interface 1):

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

2.4.3 Prerequisites

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

2.4.4 Installing Ekran System

Full installation instructions are available on Ekran's website.

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

2.5 Radiant Logic

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

2.5.1 How It's Used

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

2.5.2 Virtual Machine

The Radiant Logic virtual machine is configured as follows:

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

Network Configuration (Interface 1):

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

2.5.3 Prerequisites

The minimum system requirements are as follows:

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

    - Processor speed: 2 gigahertz or higher
    - Memory: 16 GB minimum. For most production deployments, more than 16 GB of memory is required.
    - Hard drive: 100 GB of disk space. The hard-disk usage will vary depending on the log types/levels that are enabled and the desired log history to maintain.
- Software
    - OS: Windows 2008 R2 Server, Windows Server 2012 R2, Windows Server 2016

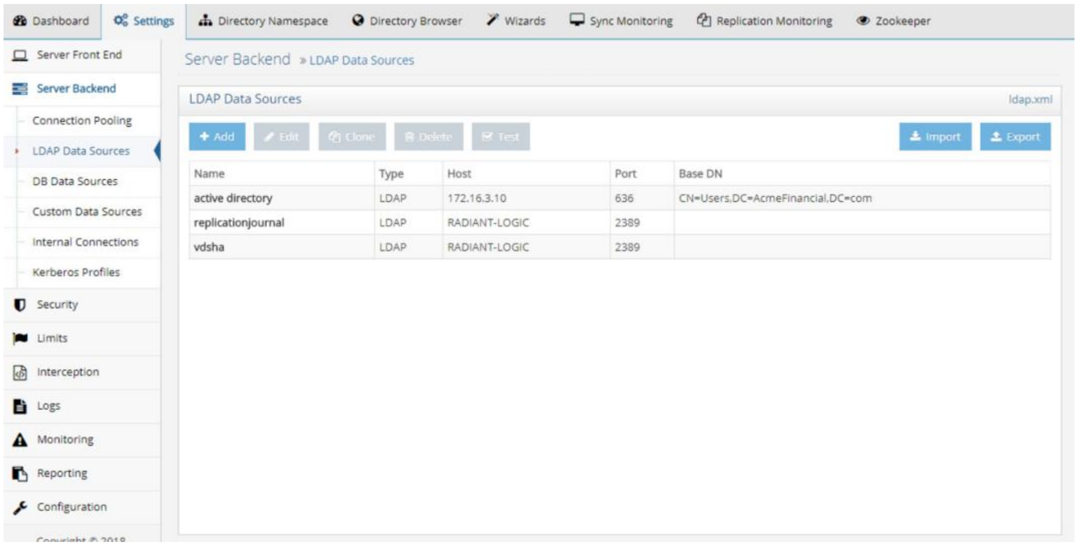
2.5.4 Installation

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

2.5.5 Configure FID

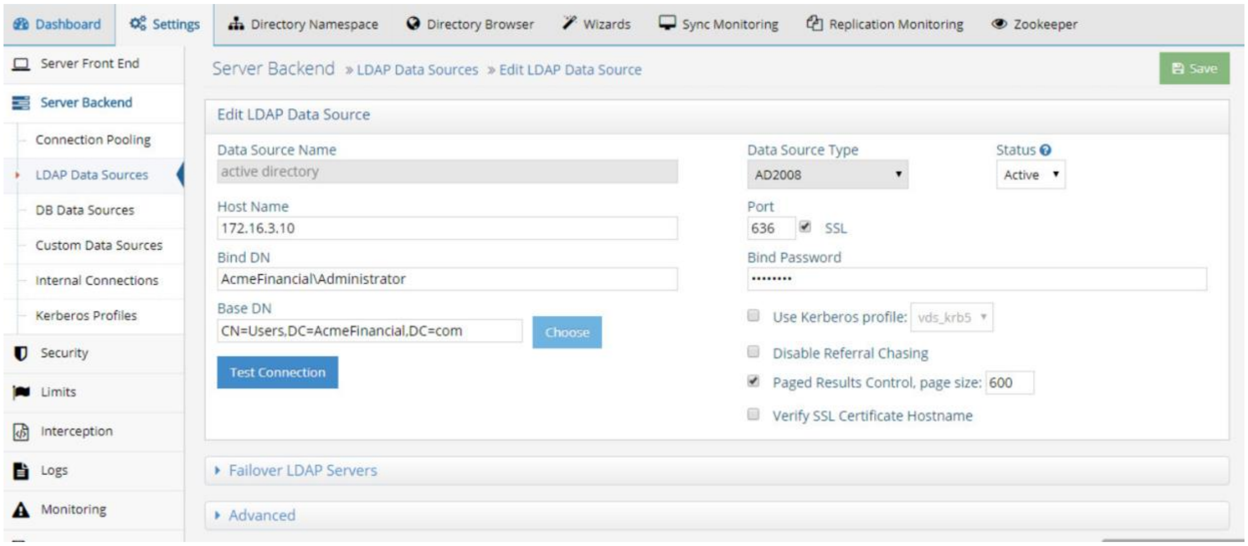
The steps for configuring FID are as follows:

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



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	

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



Edit LDAP Data Source

Data Source Name: active directory

Data Source Type: AD2008

Status: Active

Host Name: 172.16.3.10

Port: 636 ☑ SSL

Bind DN: AcmeFinancial\Administrator

Bind Password: ••••••••

Base DN: CN=Users,DC=AcmeFinancial,DC=com

☐ Use Kerberos profile: vds_krb5

☐ Disable Referral Chasing

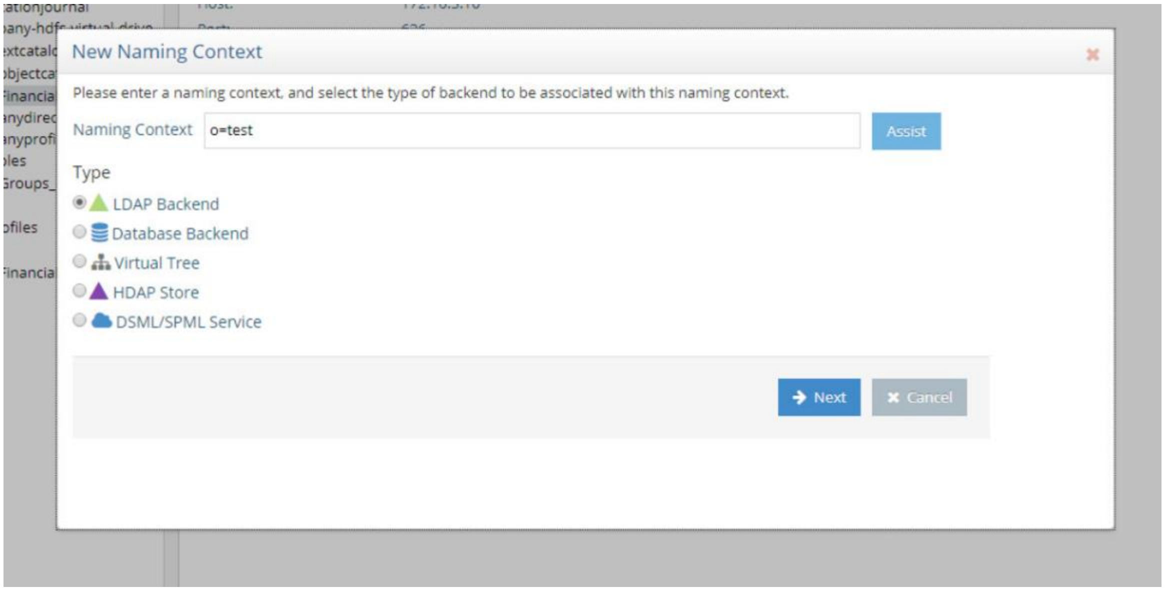
☑ Paged Results Control, page size: 600

☐ Verify SSL Certificate Hostname

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.**



Please enter a naming context, and select the type of backend to be associated with this naming context.

Naming Context: o=test

Type

● LDAP Backend

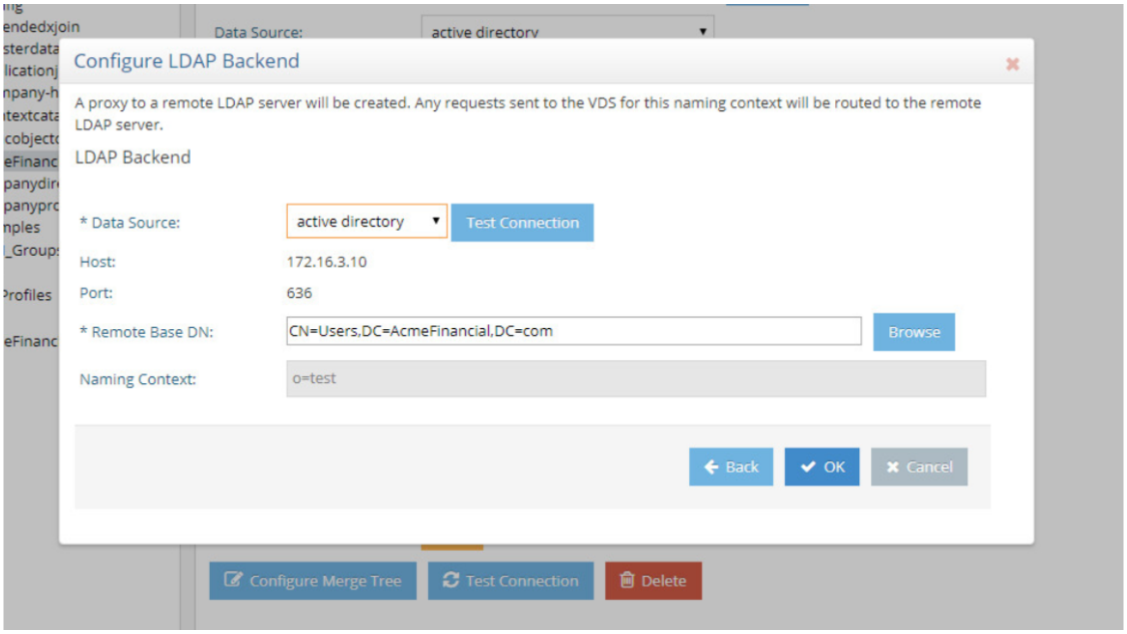
○ Database Backend

○ Virtual Tree

○ HDAP Store

○ DSML/SPML Service

   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.**



Configure LDAP Backend

A proxy to a remote LDAP server will be created. Any requests sent to the VDS for this naming context will be routed to the remote LDAP server.

LDAP Backend

* Data Source: active directory

Host: 172.16.3.10

Port: 636

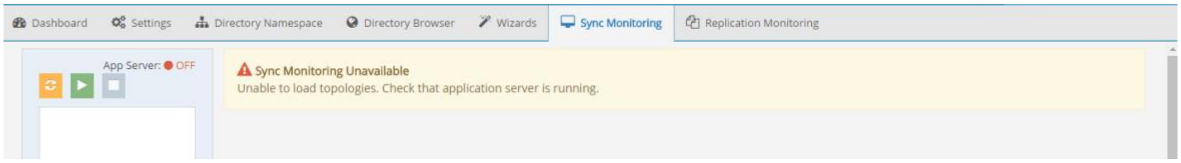
* Remote Base DN: CN=Users,DC=AcmeFinancial,DC=com

Naming Context: o=test

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:

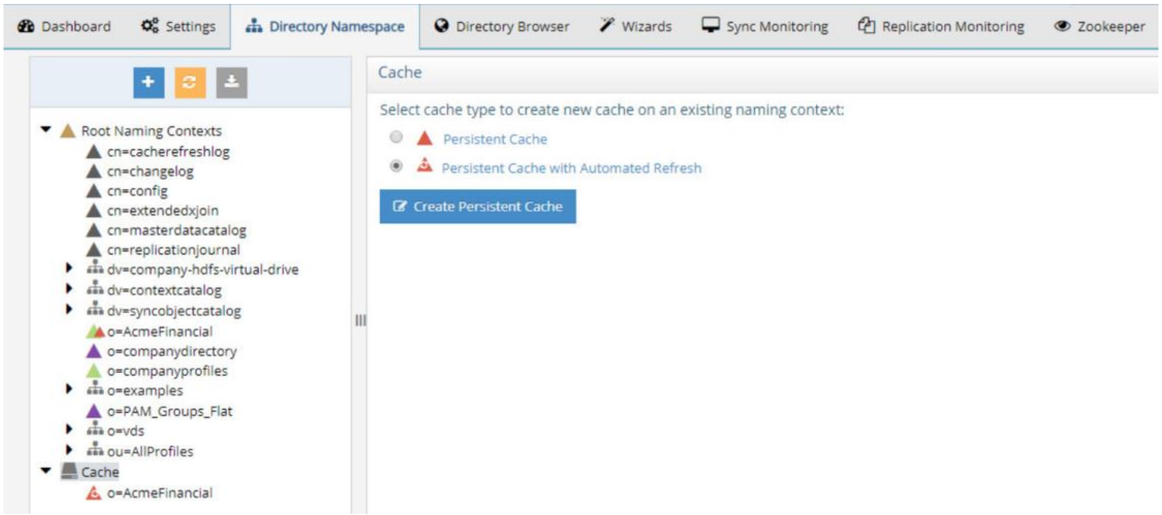
1. Navigate to the **Sync Monitoring** tab. Press the play (▷)button to start the glassfish server.



App Server: ● OFF

Sync Monitoring Unavailable
Unable to load topologies. Check that application server is running.

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

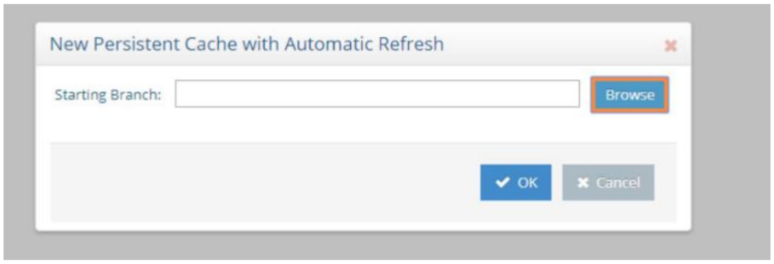


Select cache type to create new cache on an existing naming context:

○ Persistent Cache

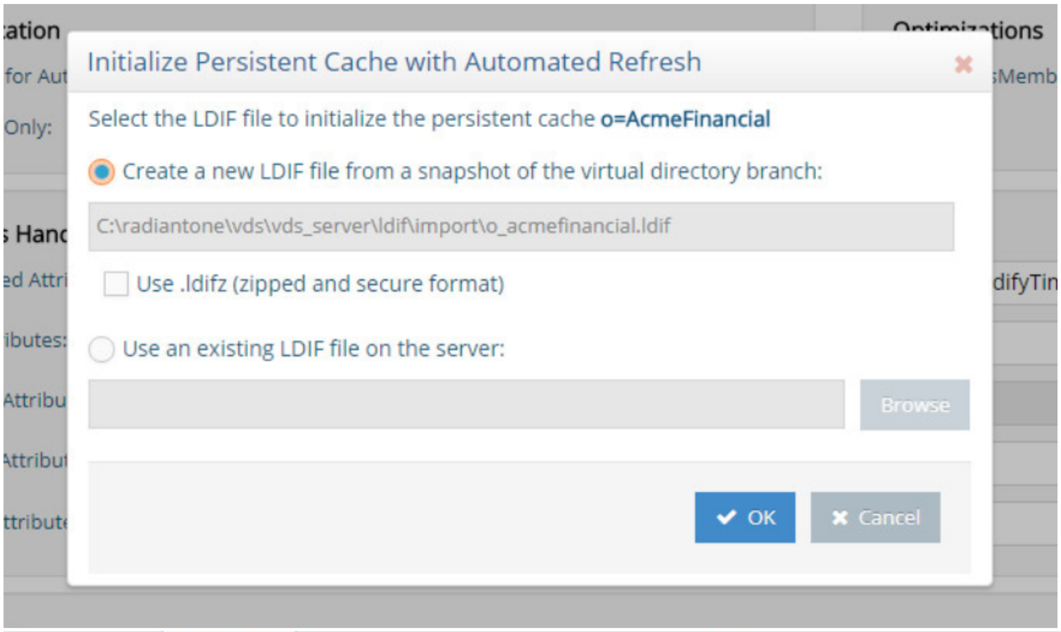
● Persistent Cache with Automated Refresh

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



Starting Branch:

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



Initialize Persistent Cache with Automated Refresh

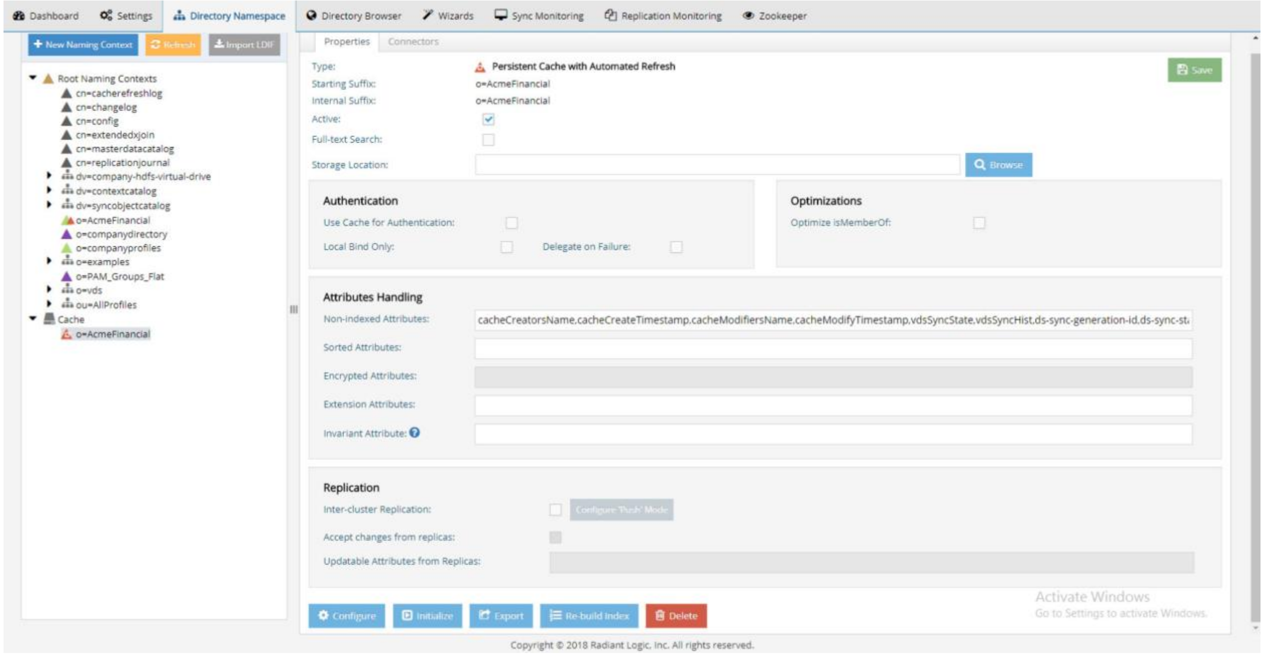
Select the LDIF file to initialize the persistent cache **o=AcmeFinancial**

● Create a new LDIF file from a snapshot of the virtual directory branch:

C:\radiantone\vds\vds_server\ldif\import\o_acmefinancial.ldif

□ Use .ldifz (zipped and secure format)

○ Use an existing LDIF file on the server:



Root Naming Contexts
- cn=cacherefreshlog
- cn=changelog
- cn=config
- cn=extendedxjoin
- cn=masterdatacatalog
- cn=replicationjournal
- dv=company-hdfs-virtual-drive
- dv=contextcatalog
- dv=syncobjectcatalog
- o=AcmeFinancial
- o=companydirectory
- o=companyprofiles
- o=examples
- o=PAM_Groups_Flat
- o=vds
- ou=AllProfiles

Cache
- o=AcmeFinancial

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:

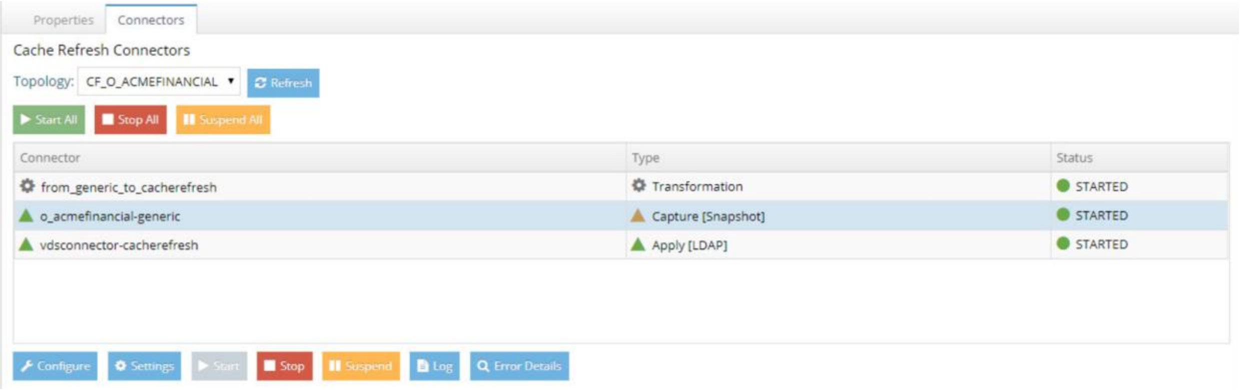
Replication
Inter-cluster Replication: □
Accept changes from replicas: □
Updatable Attributes from Replicas:

Copyright © 2018 Radiant Logic, Inc. All rights reserved.

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.

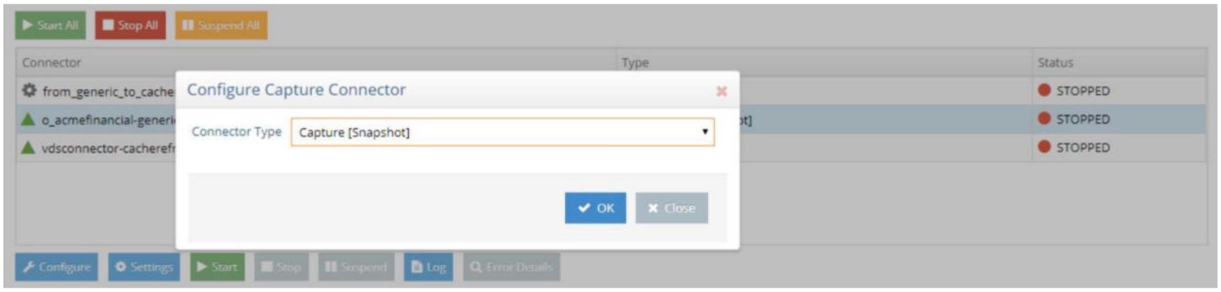


Cache Refresh Connectors

Topology: CF_O_ACMEFINANCIAL

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

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.**



Configure Capture Connector

Connector Type: Capture [Snapshot]

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

2.5.7 Configure SSL

In this implementation, AD serves as the CA.

1. Create the initial FID private key:

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

2. Download the certificate from the CA.

3. Create the certificate signing request:

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

4. Submit the request to the CA.

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

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

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

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

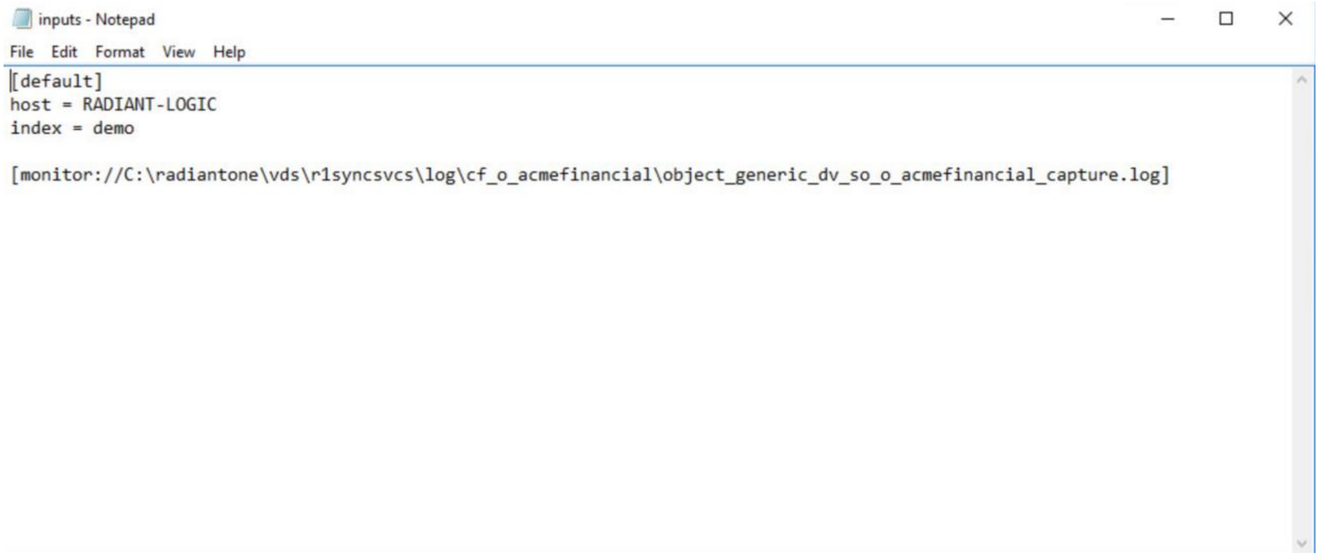
   Navigate to *c:\radiantone\vds\jdk\jre\bin*, and run `keytool -import -file C:\radiantone\vds\vds_server\conf\rli.cer -keystore C:\radiantone\vds\vds_server\conf\rli.keystore -v -alias rli`.

7. Restart FID.

2.5.8 Splunk Universal Forwarder

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

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



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

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

2.6 IdRamp

2.6.1 How It's Used

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

2.6.2 Prerequisites

- premium Azure account
- AD installed

2.6.3 Installation

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

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

2. Enable MFA in Azure for certain privileged users:

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

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

   c. Click **New policy.**

    d. Give the policy a name, such as Privileged 2FA.
    e. Click **Users and groups.** Under **Include,** click **users and groups,** and select **Users and groups** check box.
    f. Click the region labeled as **Select.**
    g. Select the privileged users from the list.
    h. Once all of those users are selected, click **Done.**
    i. Click **Cloud apps,** and then select **All cloud apps.** Click **Done.**
    j. Under **Access Controls,** click **Grant.**
    k. Make sure that the **Grant access** check box is selected, and select the check box labeled as **Require multi-factor authentication.**
    l. Click **Select.**
    m. Click **On** under **Enable policy,** and then click **Create.**

3. Disable logins of all other accounts:
    a. For each user that you do not want to allow to sign in with Azure AD at all, click their user account under **All users** in the Azure AD admin center.
    b. Click **Yes** next to **Block sign in.**
4. Configure sign-in to block incoming requests, except from your organization's network:
    a. Under **SECURITY > Conditional access** in the Azure AD admin center, select **Named locations.**
    b. Click **New location,** and then give the location a name.
    c. Select the check box labeled as **Mark as trusted location.**
    d. Enter the IP range of the network to which you want to restrict access.
    e. Click **Create.**
    f. Complete steps 2a–2c above.
    g. Give the policy a name, such as Block Remote Access.
    h. For users of this policy, select the privileged users.
    i. Select all cloud apps for the **Cloud apps assignment.**

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

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

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

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

n. Click **Done.**

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

p. Click **Select.**

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

2.7 OneSpan IDENTIKEY Authentication Server

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

2.7.1 How It's Used

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

2.7.2 Virtual Machine Configuration

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

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

2.7.3 Prerequisites

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

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

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

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

2.7.4 Installation

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

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

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

2. Run the installation script:

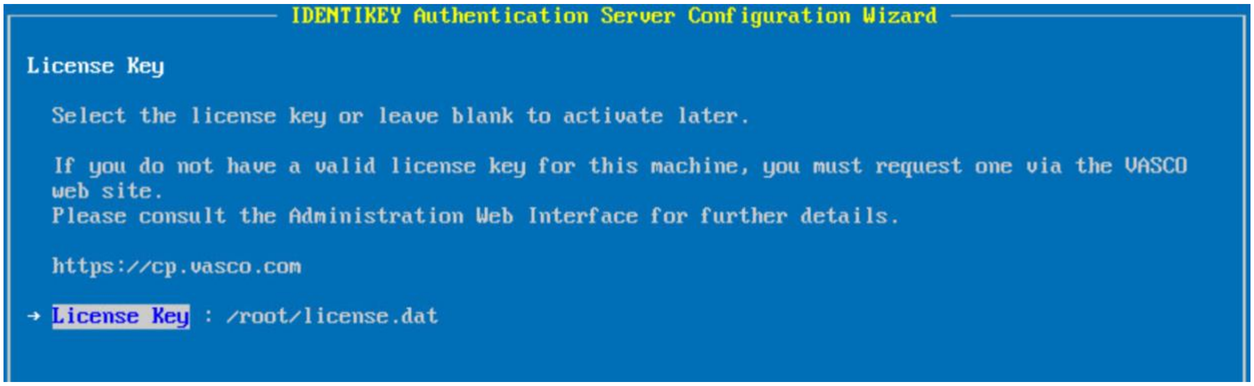
```
cd /mnt/dvd
sudo ./install.sh
```

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

2.7.5 Configuration

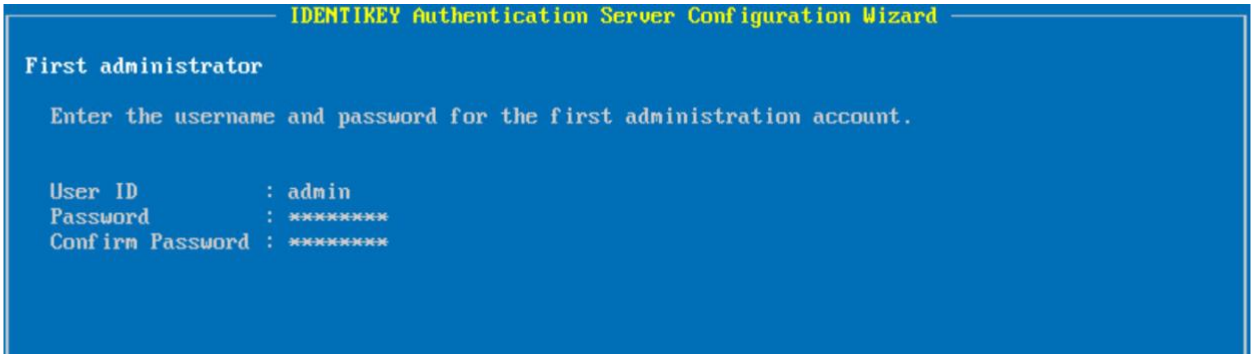
After completing the installation, configuration happens immediately:

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



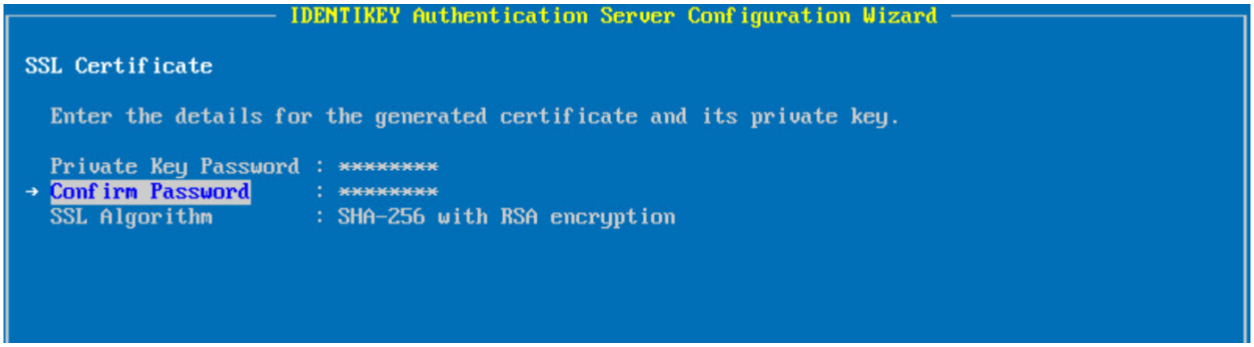
```
IDENTIKEY Authentication Server Configuration Wizard

License Key

  Select the license key or leave blank to activate later.

  If you do not have a valid license key for this machine, you must request one via the VASCO
  web site.
  Please consult the Administration Web Interface for further details.

  https://cp.vasco.com

→ License Key : /root/license.dat
```

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



```
IDENTIKEY Authentication Server Configuration Wizard

First administrator

  Enter the username and password for the first administration account.


  User ID          : admin
  Password         : *********
  Confirm Password : *********
```

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



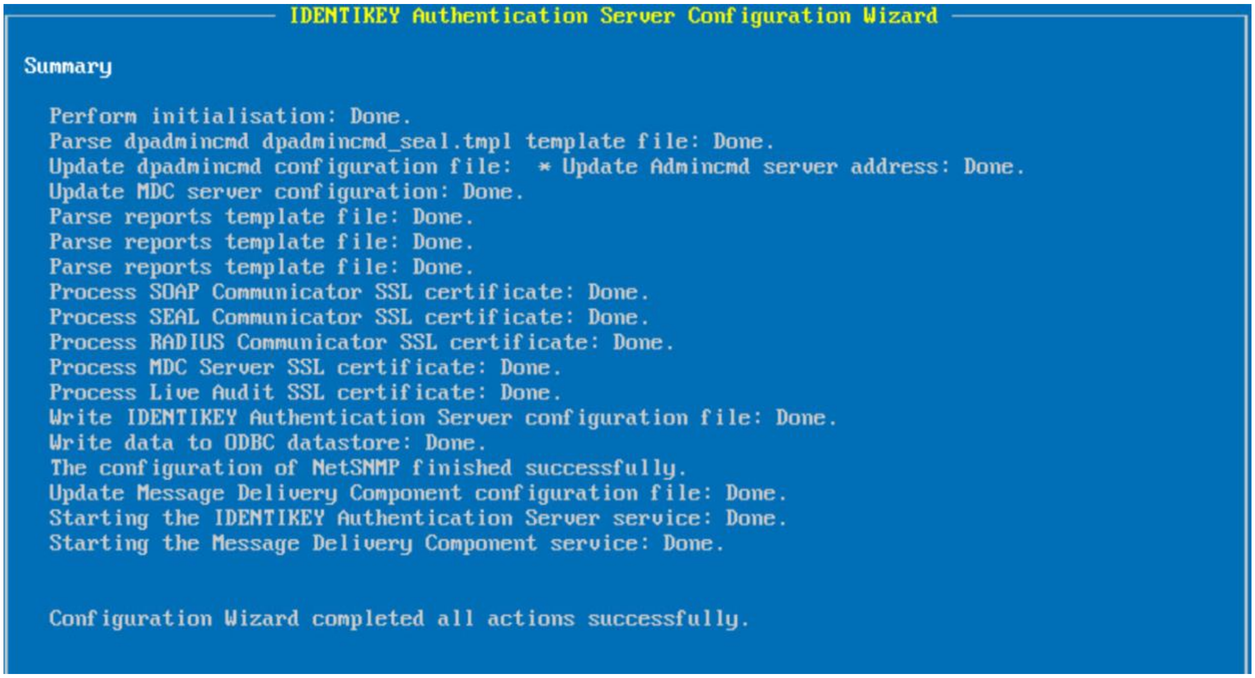
```
IDENTIKEY Authentication Server Configuration Wizard

SSL Certificate

  Enter the details for the generated certificate and its private key.

  Private Key Password : *********
→ Confirm Password     : *********
  SSL Algorithm        : SHA-256 with RSA encryption
```

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.



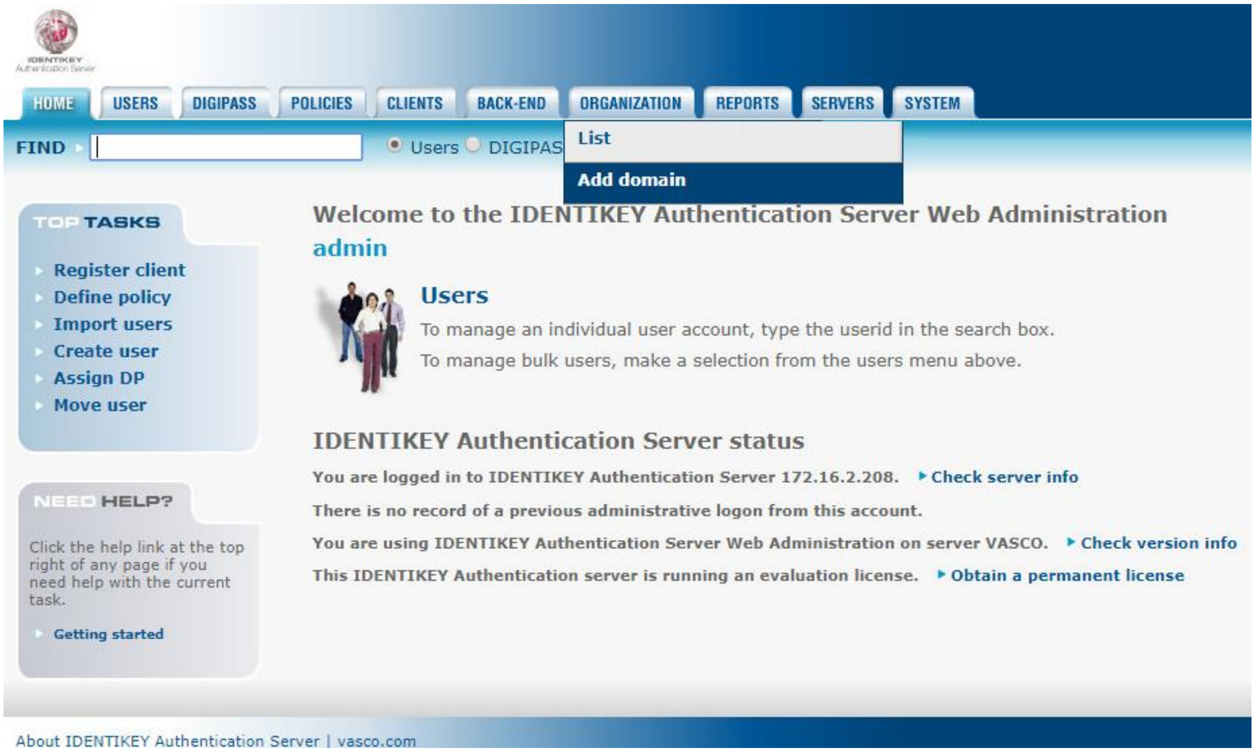
```
IDENTIKEY Authentication Server Configuration Wizard

Summary

  Perform initialisation: Done.
  Parse dpadmincmd dpadmincmd_seal.tmpl 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.
```

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.**



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.

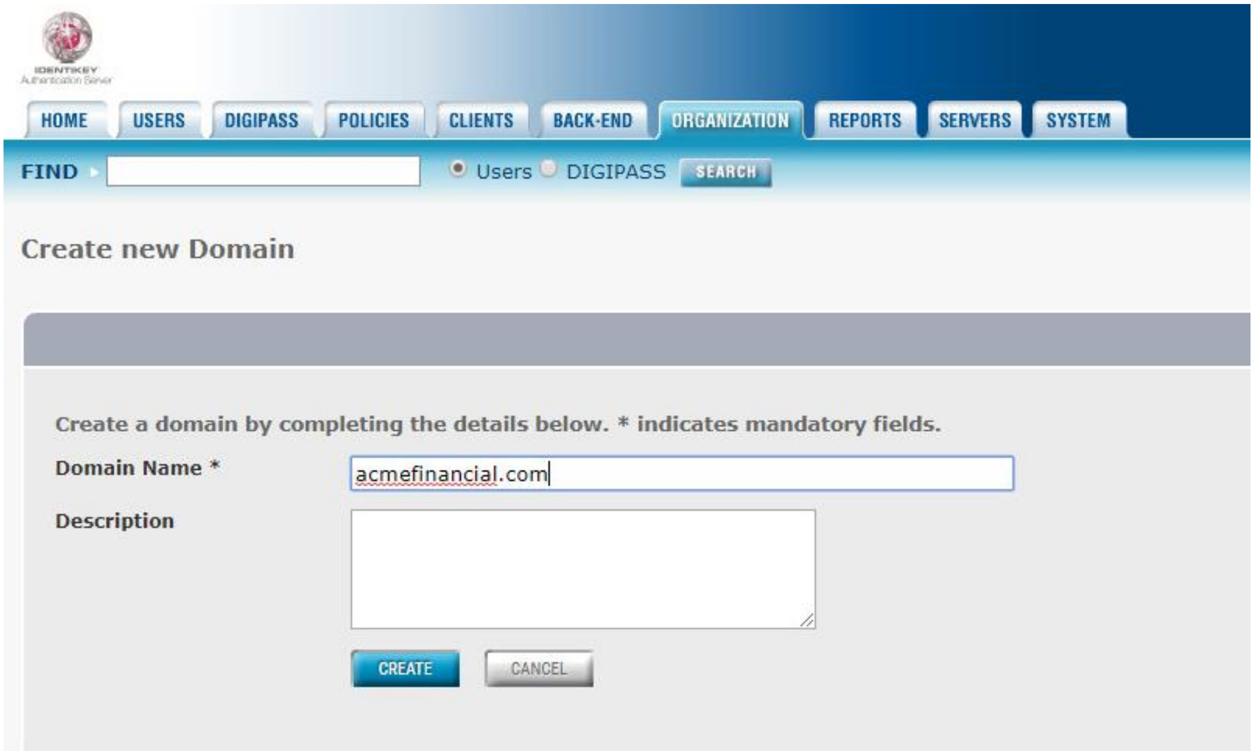
You are using IDENTIKEY Authentication Server Web Administration on server VASCO. ▸ Check version info

This IDENTIKEY Authentication server is running an evaluation license. ▸ Obtain a permanent license

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

976

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



Create new Domain

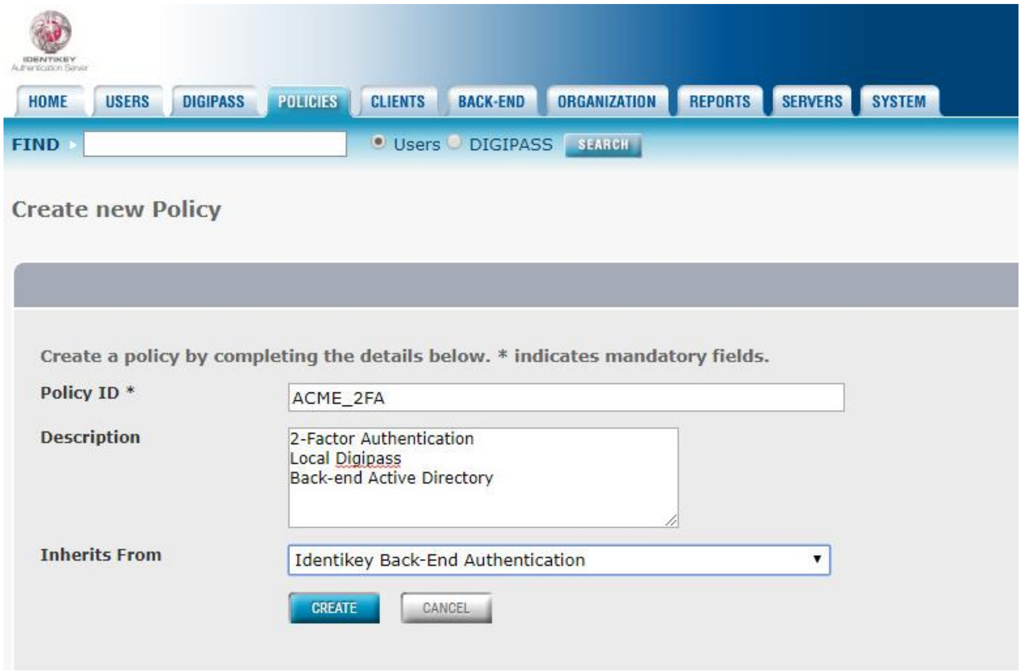
Create a domain by completing the details below. * indicates mandatory fields.

Domain Name * acmefinancial.com

Description

5. Click **POLICIES > Create.**

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



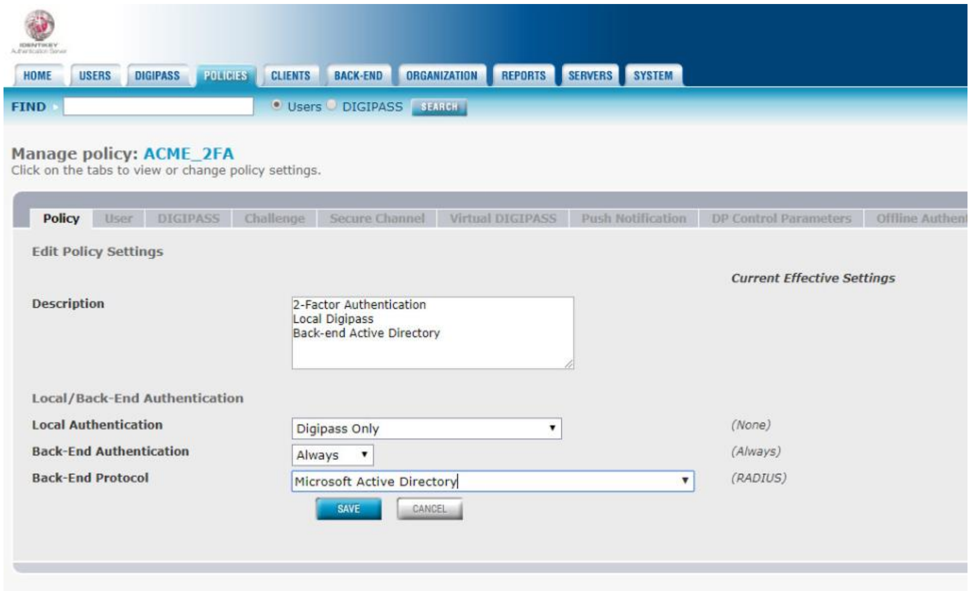
Create new Policy

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	Identikey Back-End Authentication

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.**



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

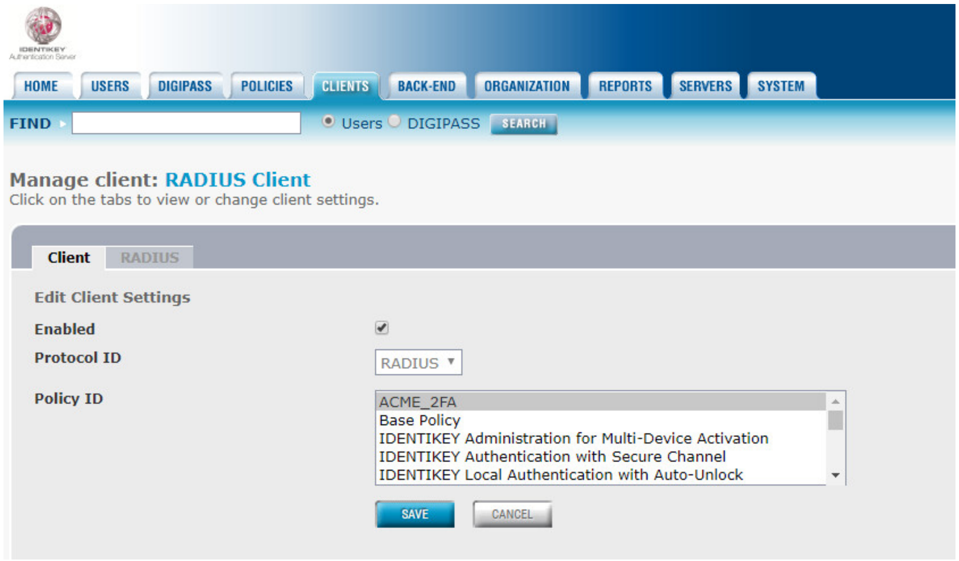
Edit Policy Settings

		Current Effective Settings
Description	2-Factor Authentication Local Digipass Back-end Active Directory	
Local/Back-End Authentication		
Local Authentication	Digipass Only	(None)
Back-End Authentication	Always	(Always)
Back-End Protocol	Microsoft Active Directory	(RADIUS)

9. Click **CLIENTS > List.**

10. Click the **RADIUS client.**

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.

Edit Client Settings

Enabled ☑

Protocol ID RADIUS

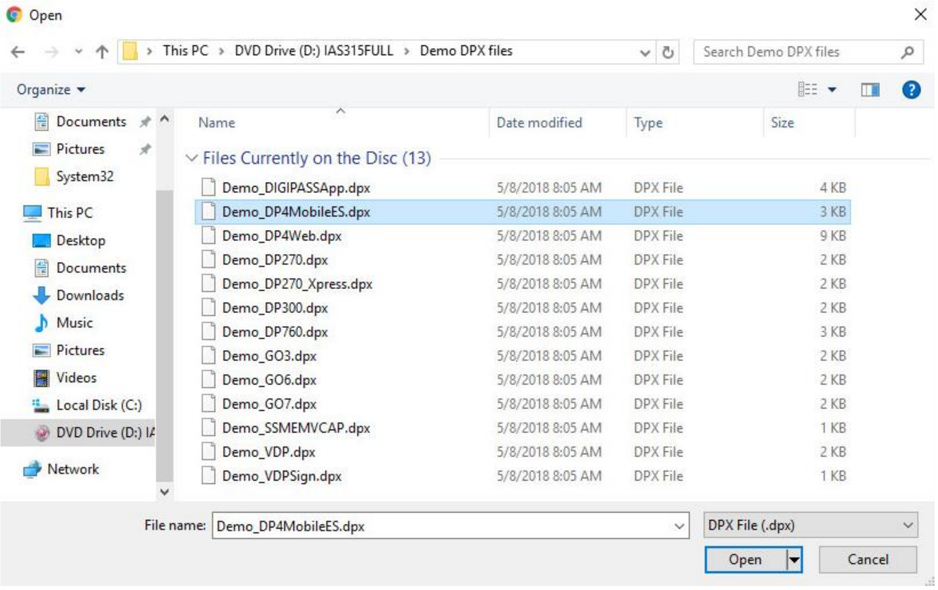
Policy ID
ACME_2FA
Base Policy
IDENTIKEY Administration for Multi-Device Activation
IDENTIKEY Authentication with Secure Channel
IDENTIKEY Local Authentication with Auto-Unlock

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 DIGPASSApp.dpx file, which came in the *.iso* file. Within the *DIGPASSApp.dpx* file is a set of mobile-application DIGIPASSes. Click **Open.**



Files Currently on the Disc (13)

Name	Date modified	Type	Size
Demo_DIGIPASSApp.dpx	5/8/2018 8:05 AM	DPX File	4 KB
Demo_DP4MobileES.dpx	5/8/2018 8:05 AM	DPX File	3 KB
Demo_DP4Web.dpx	5/8/2018 8:05 AM	DPX File	9 KB
Demo_DP270.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_DP270_Xpress.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_DP300.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_DP760.dpx	5/8/2018 8:05 AM	DPX File	3 KB
Demo_GO3.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_GO6.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_GO7.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_SSMEMVCAP.dpx	5/8/2018 8:05 AM	DPX File	1 KB
Demo_VDP.dpx	5/8/2018 8:05 AM	DPX File	2 KB
Demo_VDPSign.dpx	5/8/2018 8:05 AM	DPX File	1 KB

File name: Demo_DP4MobileES.dpx

DPX File (.dpx)

3. Enter the transport key for that file. For the demo files, the transport key is 11111111111111111111111111111111 (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

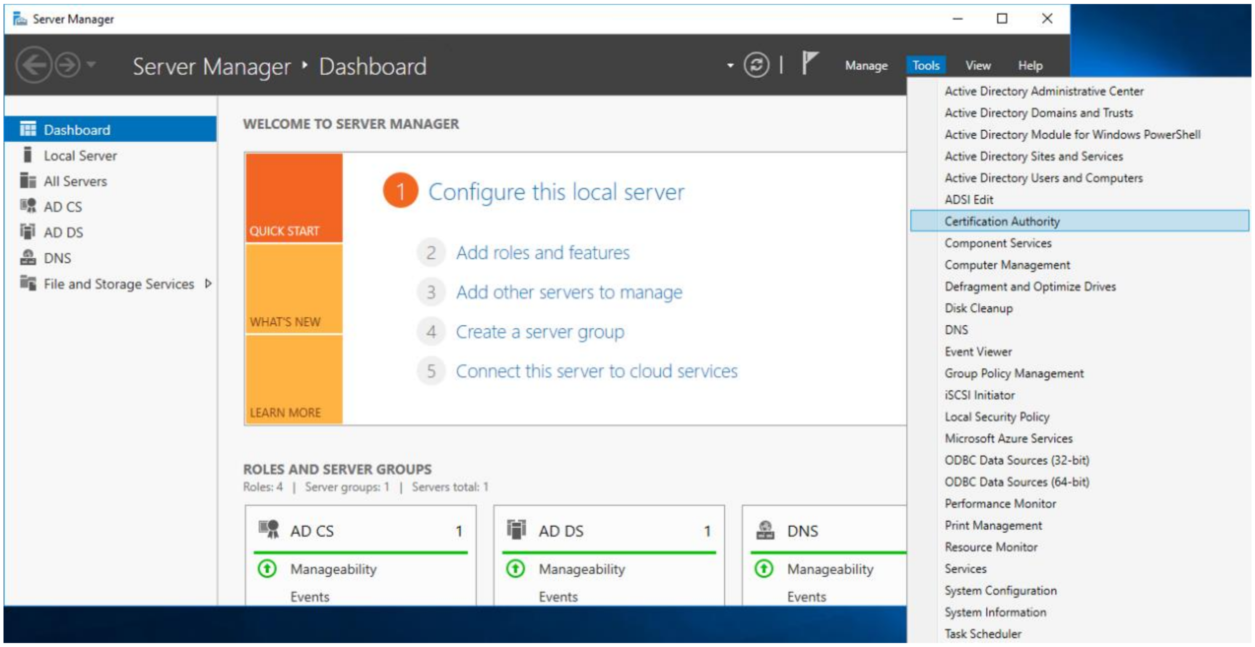
With Radiant Logic configured to replicate users and groups from AD, OneSpan can use Radiant Logic as an AD back-end. This works, as OneSpan connects to Radiant by using LDAP over SSL, and Radiant Logic contains a virtual directory that presents like AD.

2.7.8.1 Installing the AD CA Certificate in the OneSpan Server OS

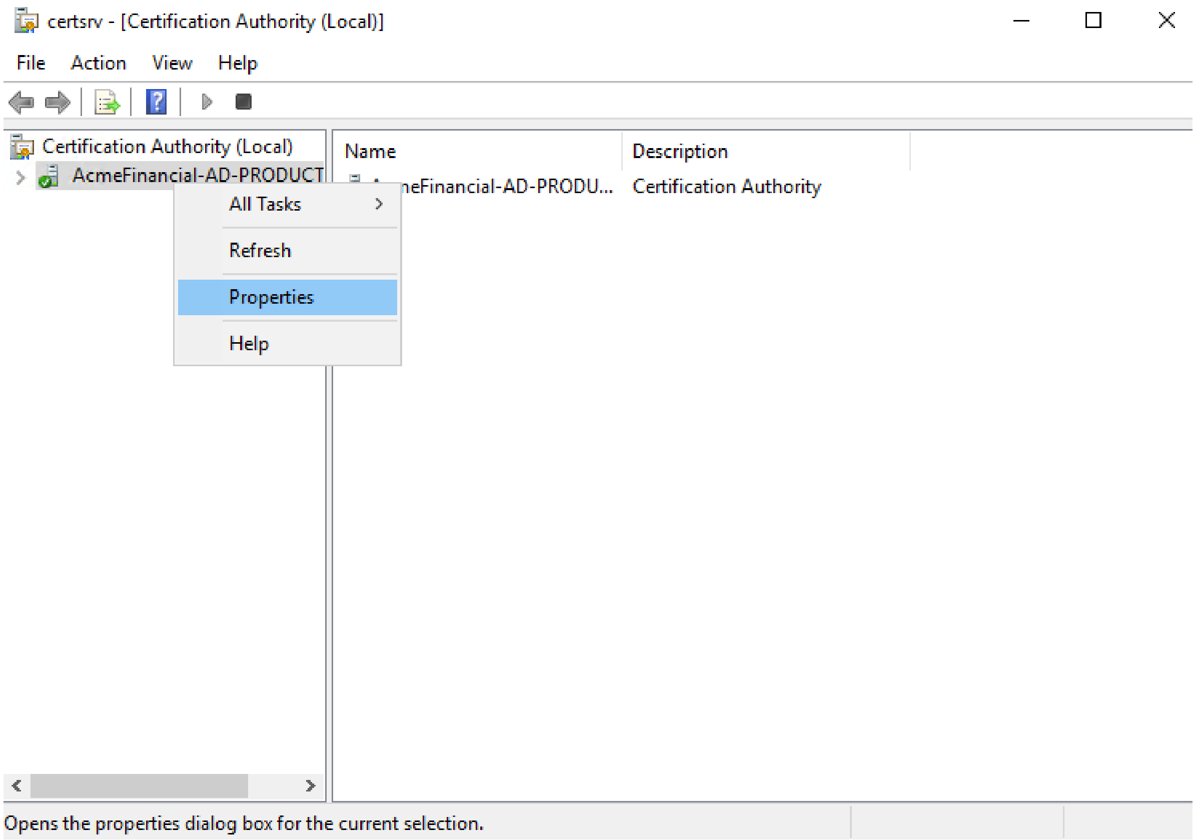
For OneSpan to trust the certificate used by Radiant Logic during the SSL handshake, the AD CA certificate needs to be installed. Because the Radiant Logic certificate was signed by the AD CA, once OneSpan trusts the CA, it trusts Radiant Logic. The following instructions detail how to export the AD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



Opens the properties dialog box for the current selection.

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:

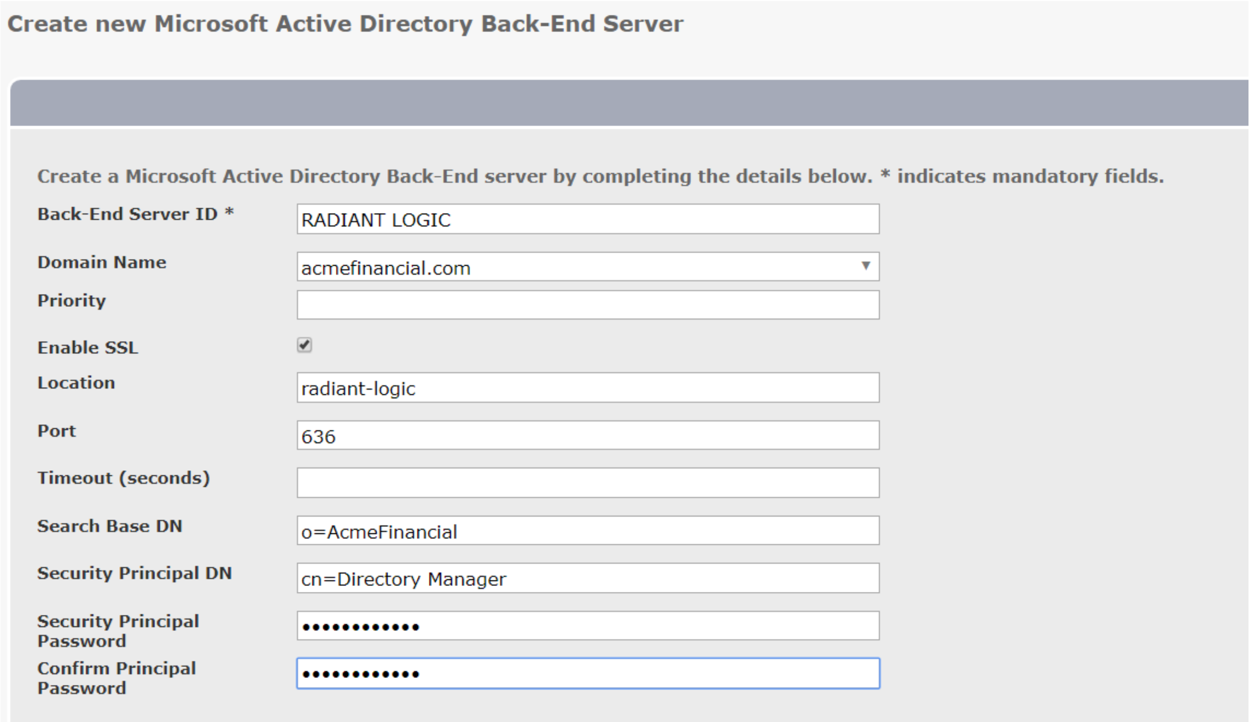
```
sudo update-ca-certificates --fresh
```

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>



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	☑
Location	radiant-logic
Port	636
Timeout (seconds)	
Search Base DN	o=AcmeFinancial
Security Principal DN	cn=Directory Manager
Security Principal Password	●●●●●●●●●●●●
Confirm Principal Password	●●●●●●●●●●●●

3. Click **CREATE.**

2.7.9 Integration with TDi ConsoleWorks

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

2.7.10 Installing User Websites

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

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

```
mkdir /mnt/dvd

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

2. Run the installation script:

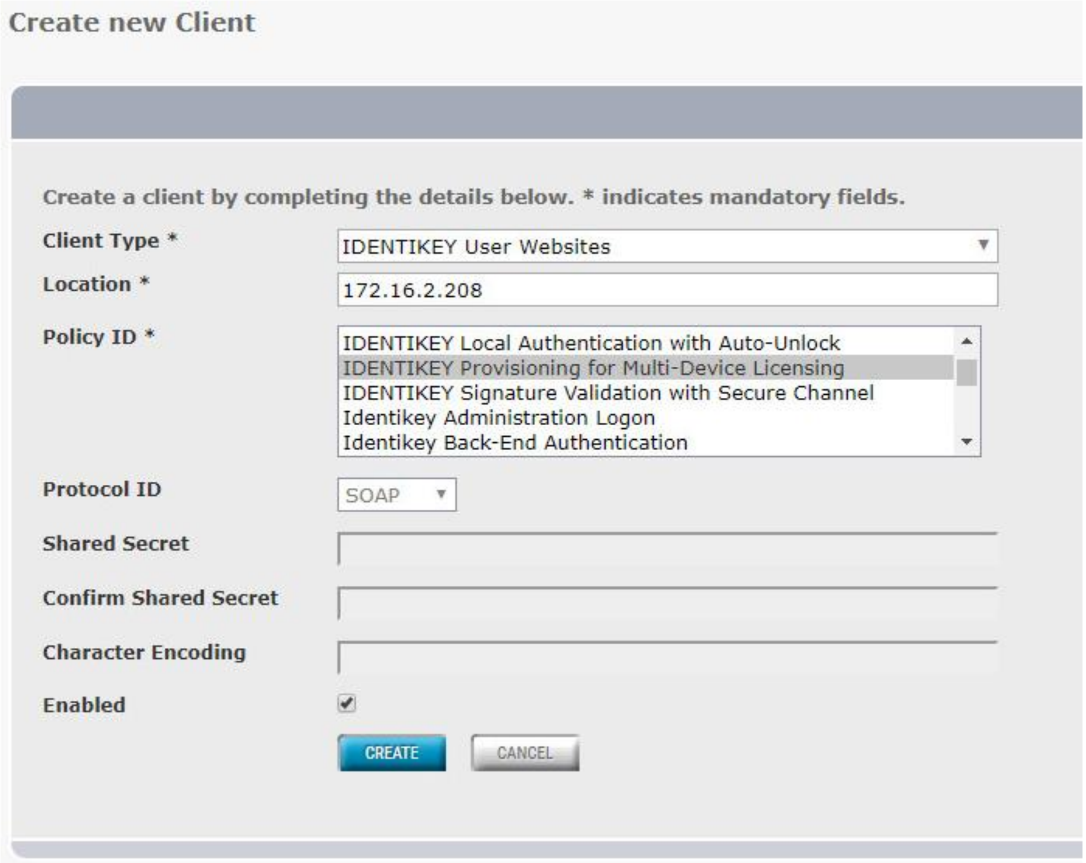
```
cd /mnt/dvd/IDENTIKEY\ User\ Websites/

sudo ./install-uws.sh
```

3. Accept the licenses for the server.

2.7.11 Creating Component Records in IDENTIKEY Authentication Server

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

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



Create new Client

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

Client Type * IDENTIKEY User Websites

Location * 172.16.2.208

Policy ID *
IDENTIKEY Local Authentication with Auto-Unlock
IDENTIKEY Provisioning for Multi-Device Licensing
IDENTIKEY Signature Validation with Secure Channel
Identikey Administration Logon
Identikey Back-End Authentication

Protocol ID SOAP

Shared Secret

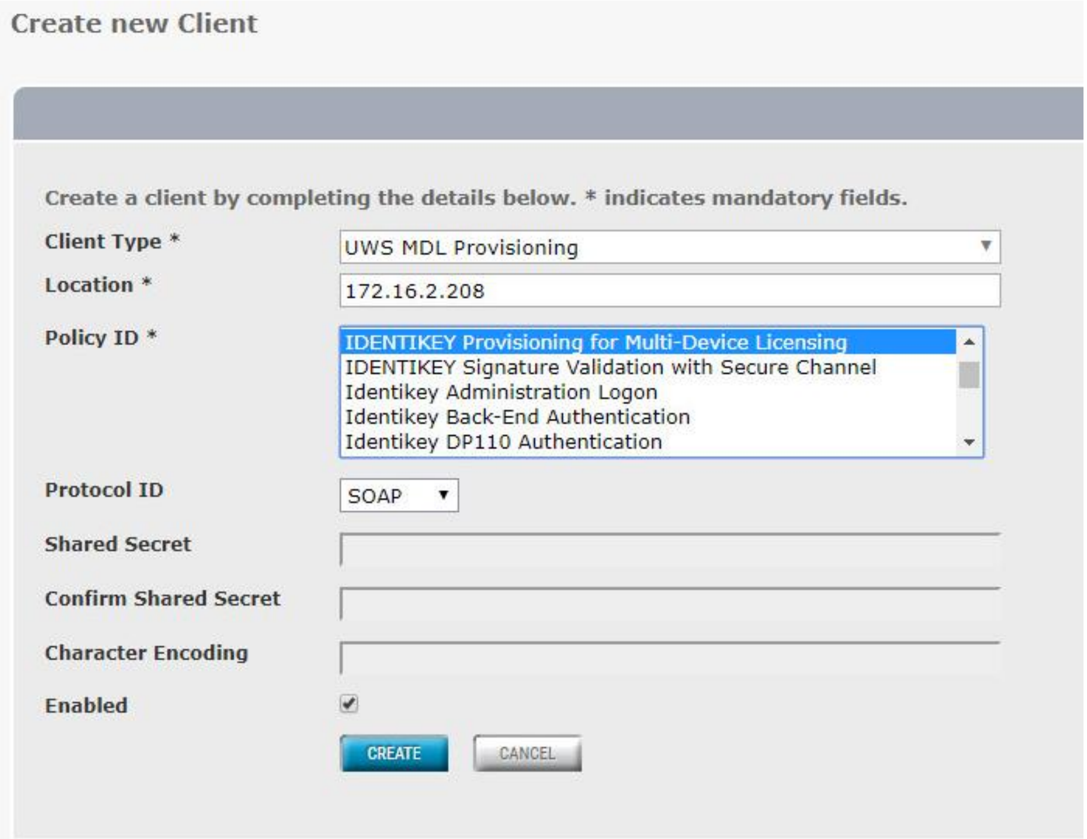
Confirm Shared Secret

Character Encoding

Enabled ☑

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**



Create new Client

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

Client Type *	UWS MDL Provisioning
Location *	172.16.2.208
Policy ID *	IDENTIKEY Provisioning for Multi-Device Licensing IDENTIKEY Signature Validation with Secure Channel Identikey Administration Logon Identikey Back-End Authentication Identikey DP110 Authentication
Protocol ID	SOAP
Shared Secret	
Confirm Shared Secret	
Character Encoding	
Enabled	☑

11. Click **CREATE.**

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

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

2.8 Base Linux OS

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

2.8.1 Virtual Machine Configuration

The base Linux virtual machine is configured as follows:

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

Network Configuration:

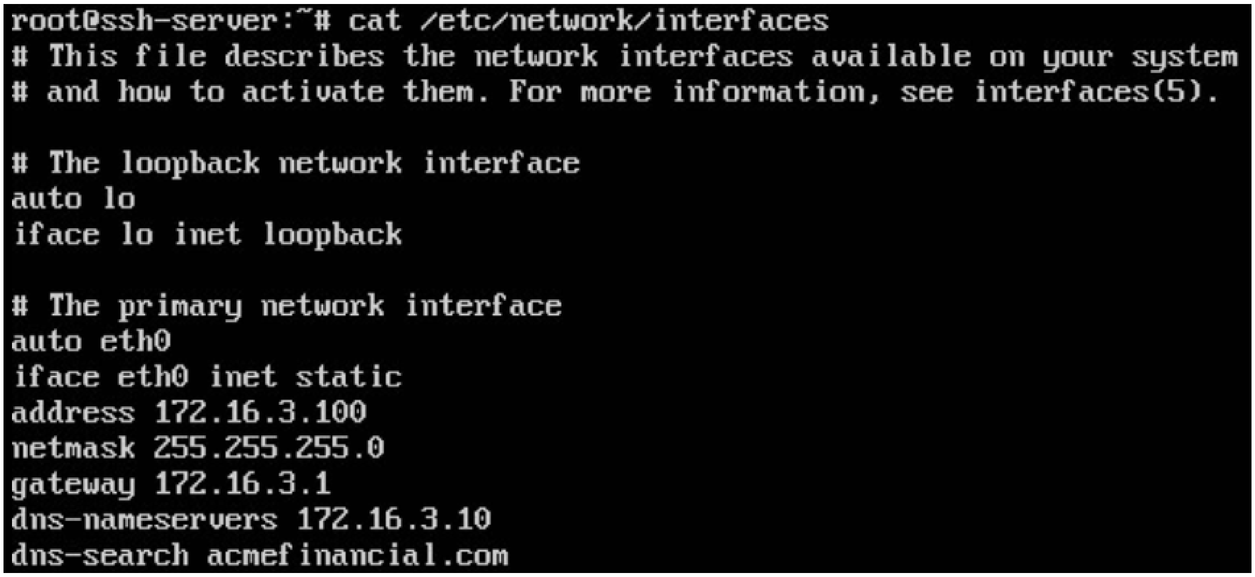
- IPv4: manual
- IPv6: disabled
- IPv4 address: 172.16.x.x
- Netmask: 255.255.255.0
- Gateway: 172.16.x.1

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

2.8.2 Domain Join Configuration

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

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



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

# The loopback network interface
auto lo
iface lo inet loopback

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

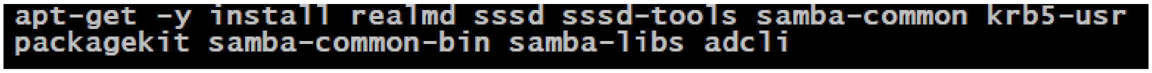
2. Restart the networking by entering the following command:

   `systemctl restart networking`

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

   `cat /etc/resolv.conf`

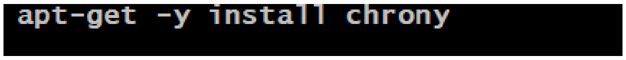
4. Install the packages required for the AD domain join as described above, using the following command:



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

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

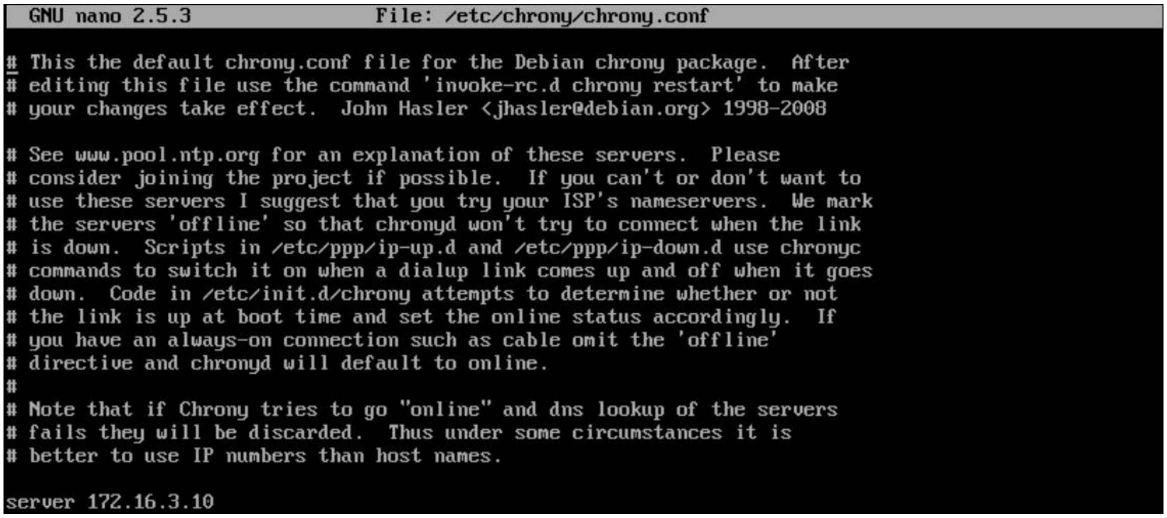
6. Install the chrony ntp client by entering the following command:



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

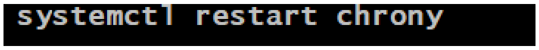
7. Add the following line, which points to the NTP server:

   `server 172.16.3.10`



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

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

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

server 172.16.3.10
```

8. Restart the chrony service as shown below:



```
systemctl restart chrony
```

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

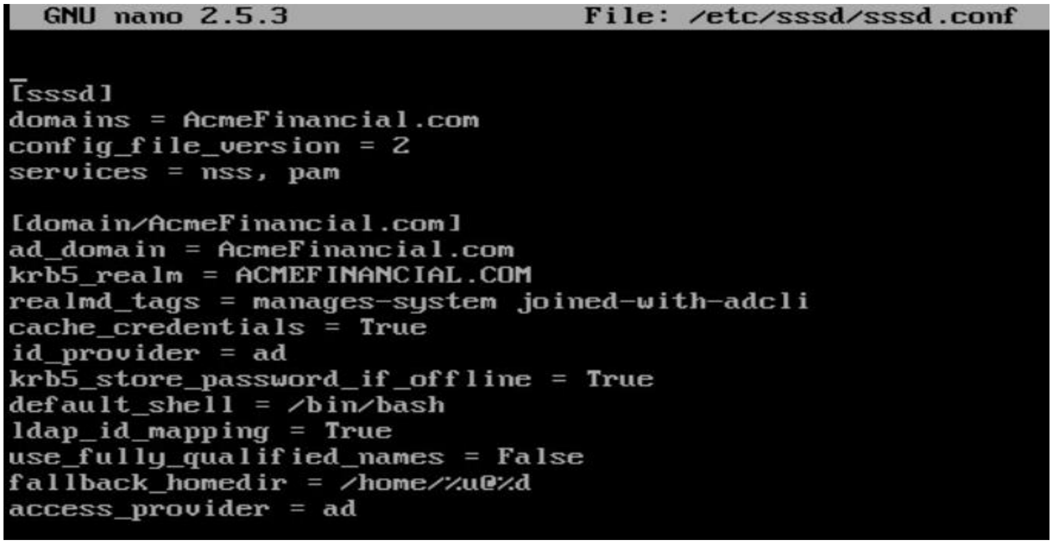
   a. `kinit administrator@ACMEFINANCIAL.COM`

   b. Enter the password when prompted.

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

   d. `systemctl restart realmd`

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



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


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

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

2.9 Microsoft SQL Server Installation on Ubuntu Linux

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

2.9.1 How It’s Used

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

2.9.2 Virtual Machine Configuration

The Microsoft SQL Server virtual machine is configured as follows:

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

Network Configuration:

- IPv4: manual
- IPv6: disabled

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

2.9.3 Firewall Configuration

```
ufw allow 1433/tcp

ufw allow 22/tcp

ufw default deny incoming
```

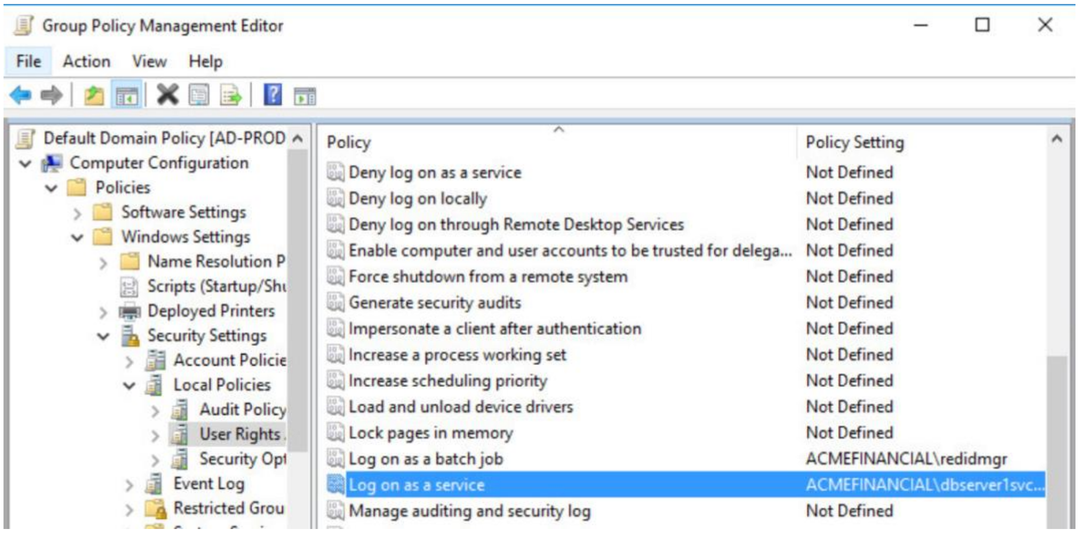
2.9.4 Installation and Initial Configuration

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

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

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

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



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\redidmgr
Log on as a service	ACMEFINANCIAL\dbserver1svc...
Manage auditing and security log	Not Defined

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

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

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

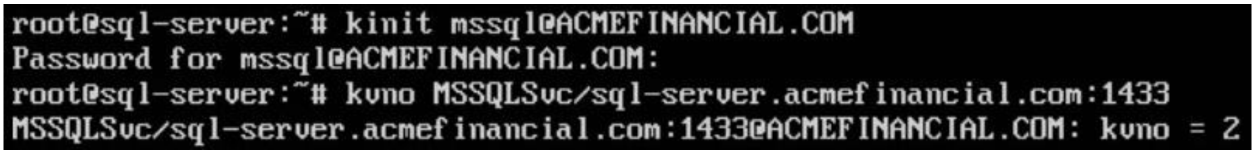
   a. Enter the following command:

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

      i. Enter the account password when prompted.

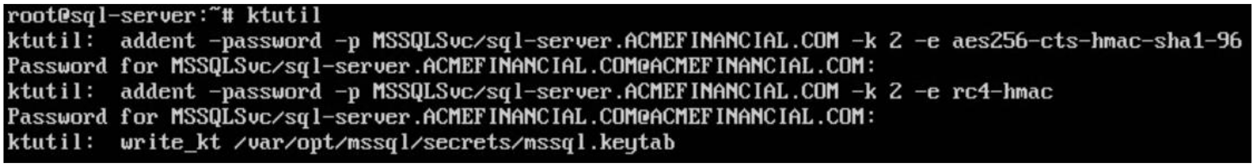
   b. Retrieve the kvno value by entering the following command:

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



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

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



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

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

```
quit
```

8. Restart SQL Server by entering the following command:

```
systemctl restart mssql-server
```

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

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

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

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

2.10 Samba File Server

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

2.10.1 How It's Used

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

2.10.2 Virtual Machine Configuration

The Samba virtual machine is configured as follows:

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

Network Configuration:

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

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

2.10.3 Firewall Configuration

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

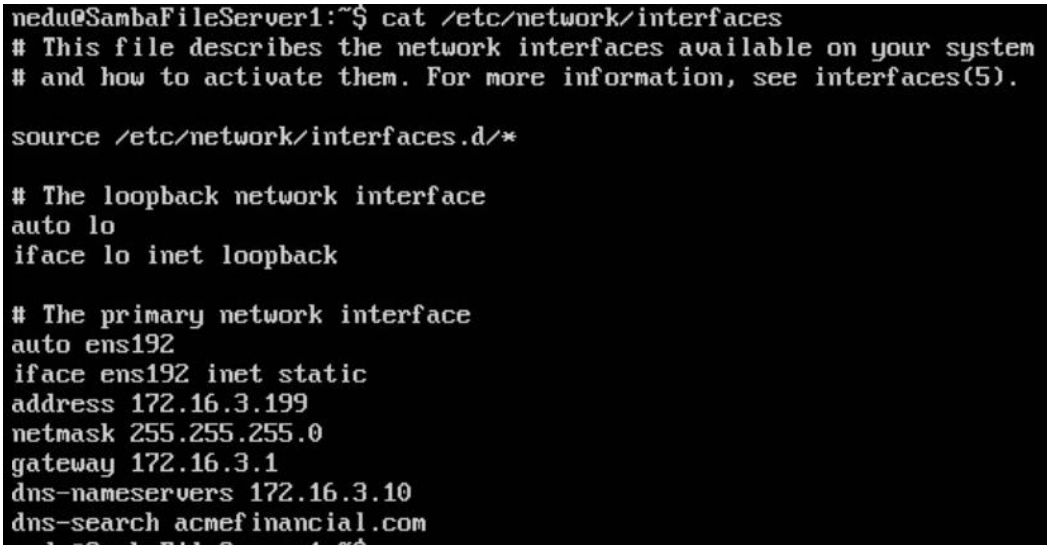
2.10.4 Installation and Configuration

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

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

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

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



```
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
```

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

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

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

```
server 172.16.3.10
```

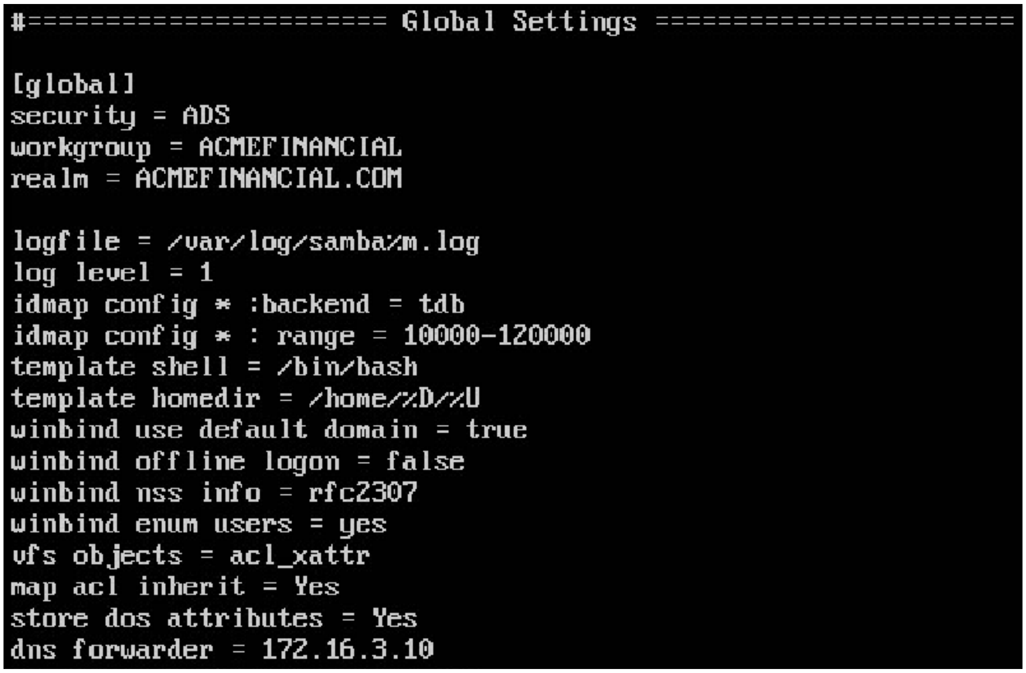
5. Restart the chrony service by entering the following command:

```
systemctl restart chrony
```

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

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

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



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

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

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

8. Restart these services by entering the following command:

```
systemctl restart smbd winbind
```

9. Join the domain by entering the following command:

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

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

    ```
    mkdir /PII2
    ```

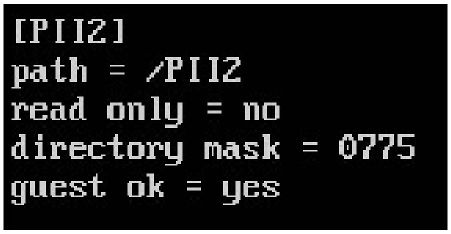
12. Enter the following command to change the owning group to domain users:

    ```
    chgrp “domain users” /PII2
    ```

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

    ```
    chmod 660 /PII2
    ```

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



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

15. Restart these services by entering the following command:

    ```
    systemctl restart smbd winbind
    ```

2.11 Remediant SecureONE

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

2.11.1 How It’s Used

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

2.11.2 Virtual Machine Configuration

The Remediant SecureONE virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 4 CPU cores

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

Network Configuration:

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

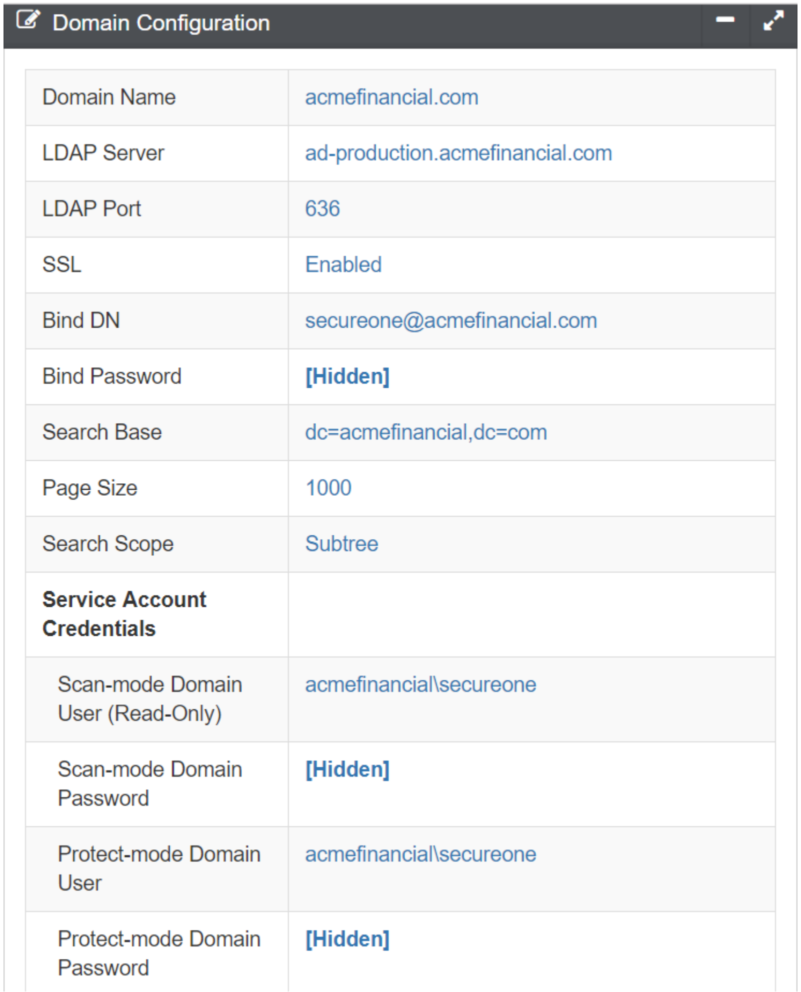
2.11.3 Installation and Initial Configuration

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

2.11.4 Domain Configuration

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

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



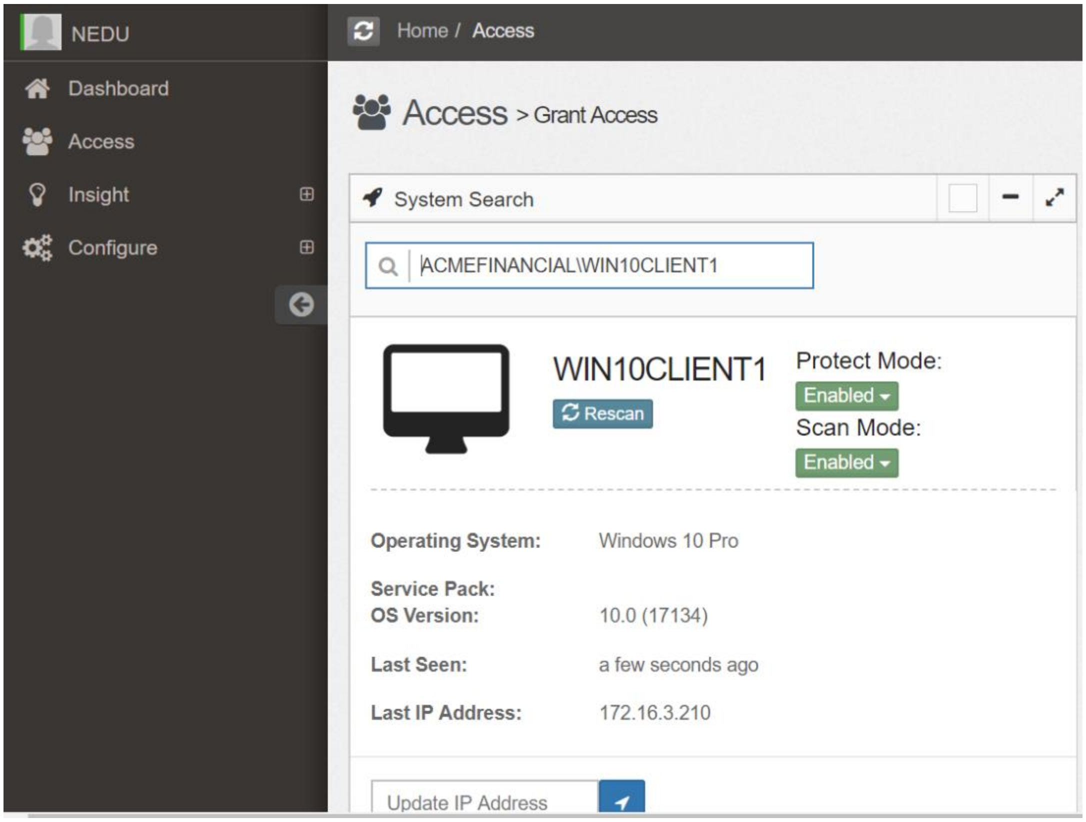
Domain Configuration

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

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.**



ACMEFINANCIAL\WIN10CLIENT1

WIN10CLIENT1

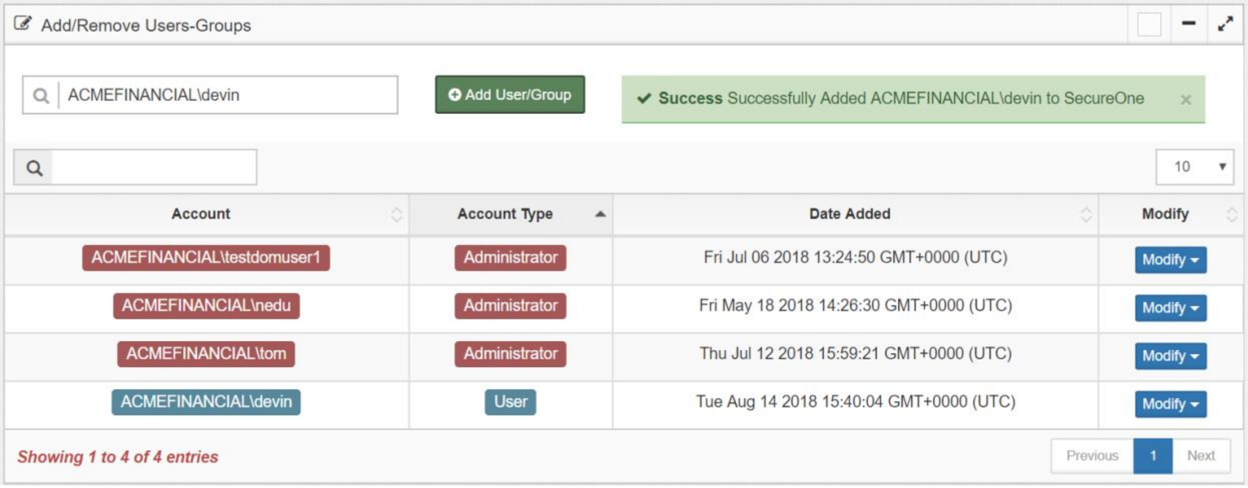
Protect Mode: Enabled

Scan Mode: Enabled

Operating System:	Windows 10 Pro
Service Pack:	
OS Version:	10.0 (17134)
Last Seen:	a few seconds ago
Last IP Address:	172.16.3.210

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.**



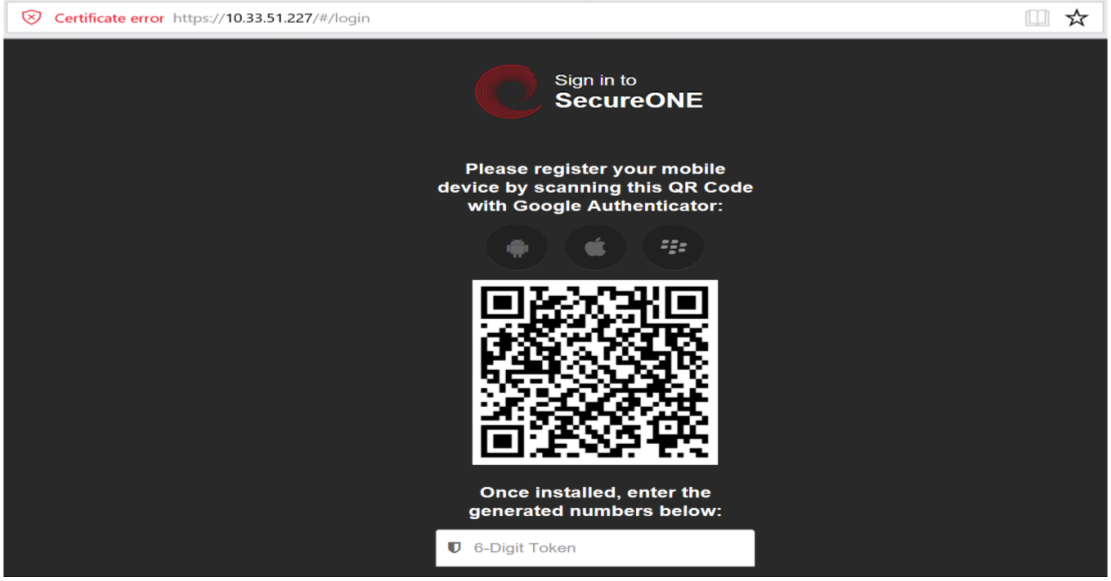
ACMEFINANCIAL\devin

✓ **Success** Successfully Added ACMEFINANCIAL\devin to SecureOne

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

Showing 1 to 4 of 4 entries

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.



Sign in to
SecureONE

Please register your mobile device by scanning this QR Code with Google Authenticator:

Once installed, enter the generated numbers below:

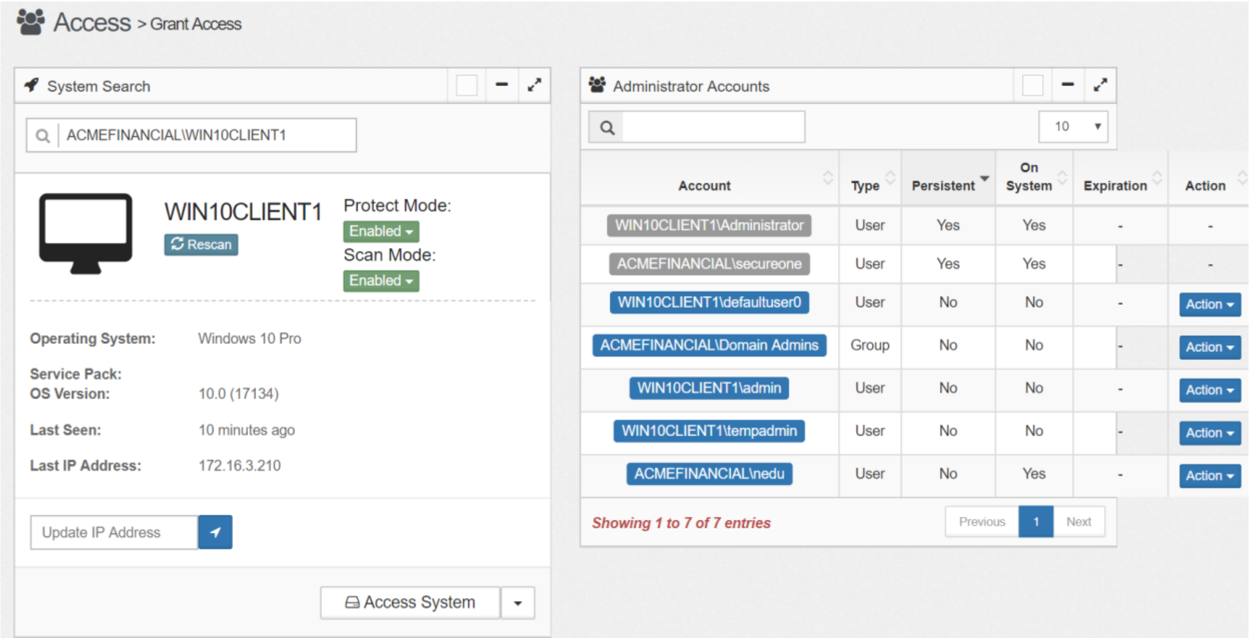
6-Digit Token

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.**



System Search

ACMEFINANCIAL\WIN10CLIENT1

WIN10CLIENT1

Protect Mode: Enabled

Scan Mode: Enabled

Operating System: Windows 10 Pro

Service Pack:

OS Version: 10.0 (17134)

Last Seen: 10 minutes ago

Last IP Address: 172.16.3.210

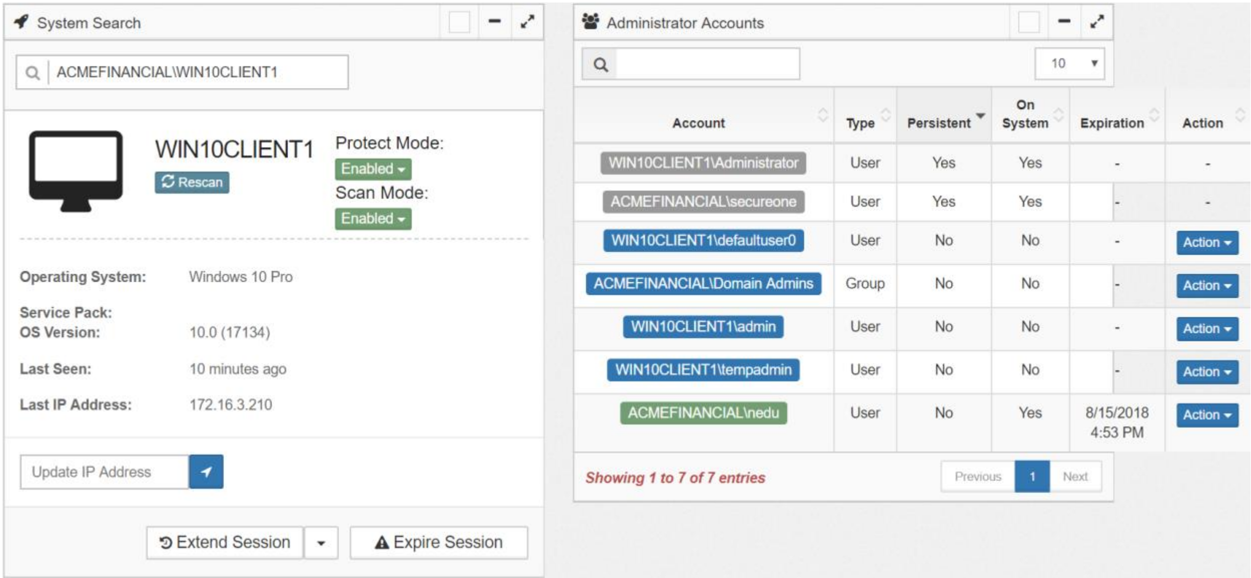
Administrator Accounts

10

Account	Type	Persistent	On System	Expiration	Action
WIN10CLIENT1\Administrator	User	Yes	Yes	-	-
ACMEFINANCIAL\secureone	User	Yes	Yes	-	-
WIN10CLIENT1\defaultuser0	User	No	No	-	Action
ACMEFINANCIAL\Domain Admins	Group	No	No	-	Action
WIN10CLIENT1\admin	User	No	No	-	Action
WIN10CLIENT1\tempadmin	User	No	No	-	Action
ACMEFINANCIAL\nedu	User	No	Yes	-	Action

Showing 1 to 7 of 7 entries

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


System Search

ACMEFINANCIAL\WIN10CLIENT1

WIN10CLIENT1

Protect Mode: Enabled

Scan Mode: Enabled

Operating System: Windows 10 Pro

Service Pack:

OS Version: 10.0 (17134)

Last Seen: 10 minutes ago

Last IP Address: 172.16.3.210

Administrator Accounts

10

Account	Type	Persistent	On System	Expiration	Action
WIN10CLIENT1\Administrator	User	Yes	Yes	-	-
ACMEFINANCIAL\secureone	User	Yes	Yes	-	-
WIN10CLIENT1\defaultuser0	User	No	No	-	Action
ACMEFINANCIAL\Domain Admins	Group	No	No	-	Action
WIN10CLIENT1\admin	User	No	No	-	Action
WIN10CLIENT1\tempadmin	User	No	No	-	Action
ACMEFINANCIAL\nedu	User	No	Yes	8/15/2018 4:53 PM	Action

Showing 1 to 7 of 7 entries

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

2.12 RSA Authentication Manager

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

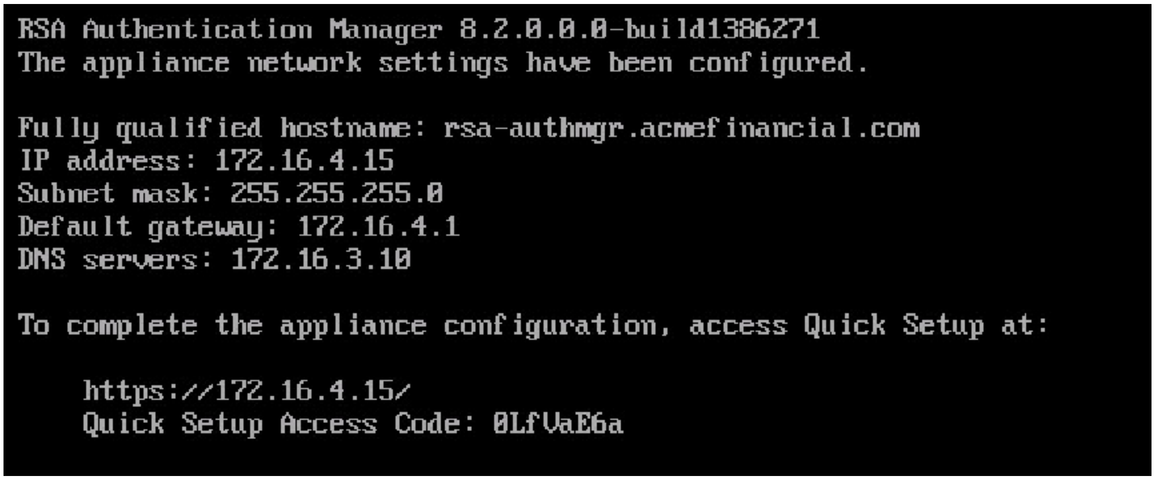
2.12.1 How It's Used

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

2.12.2 Installation and Initial Configuration

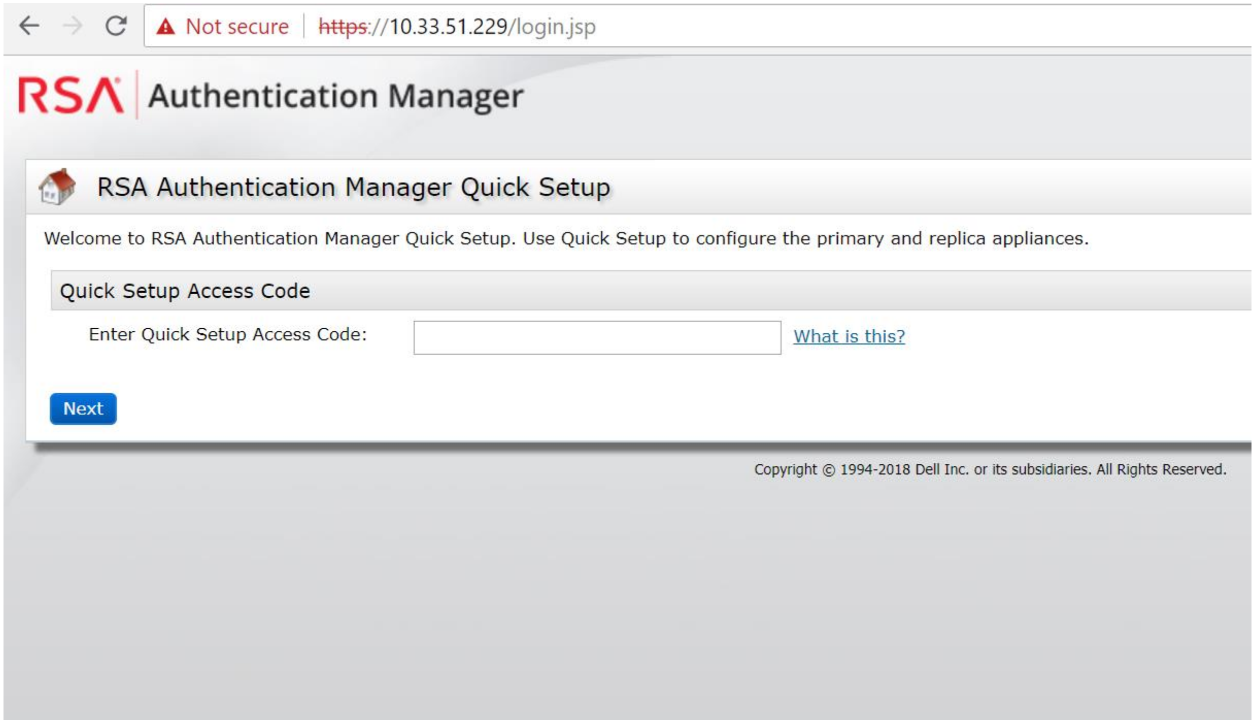
Authentication Manager was deployed as an appliance in the example implementation. Once the appliance boots successfully, the operator will have the opportunity to change or verify the IP address settings. Use the following steps to complete the initial configuration:

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



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

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

To complete the appliance configuration, access Quick Setup at:

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

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


Not secure
~~https~~://10.33.51.229/login.jsp
RSA Authentication Manager

RSA Authentication Manager Quick Setup

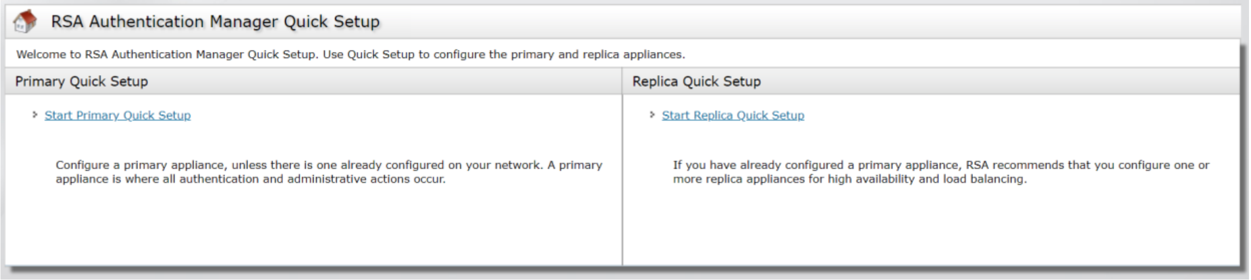
Welcome to RSA Authentication Manager Quick Setup. Use Quick Setup to configure the primary and replica appliances.

Quick Setup Access Code

Enter Quick Setup Access Code:

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

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


RSA Authentication Manager Quick Setup

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

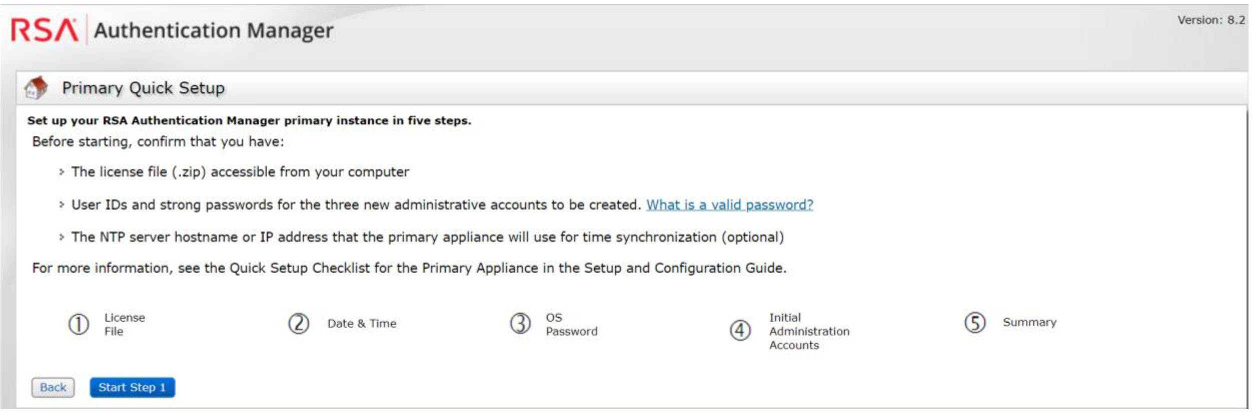
Primary Quick Setup

Configure a primary appliance, unless there is one already configured on your network. A primary appliance is where all authentication and administrative actions occur.

Replica Quick Setup

If you have already configured a primary appliance, RSA recommends that you configure one or more replica appliances for high availability and load balancing.

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



RSA Authentication Manager

Version: 8.2

Primary Quick Setup

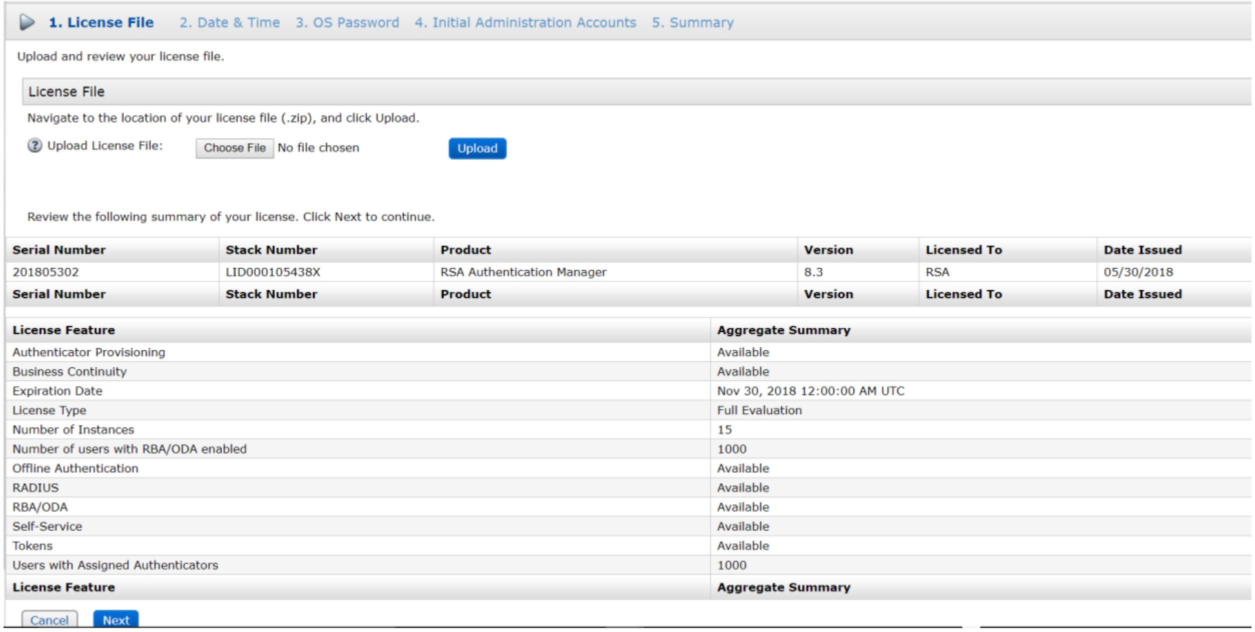
Set up your RSA Authentication Manager primary instance in five steps.

Before starting, confirm that you have:

- 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?
- The NTP server hostname or IP address that the primary appliance will use for time synchronization (optional)

For more information, see the Quick Setup Checklist for the Primary Appliance in the Setup and Configuration Guide.

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



Upload and review your license file.

License File

Navigate to the location of your license file (.zip), and click Upload.

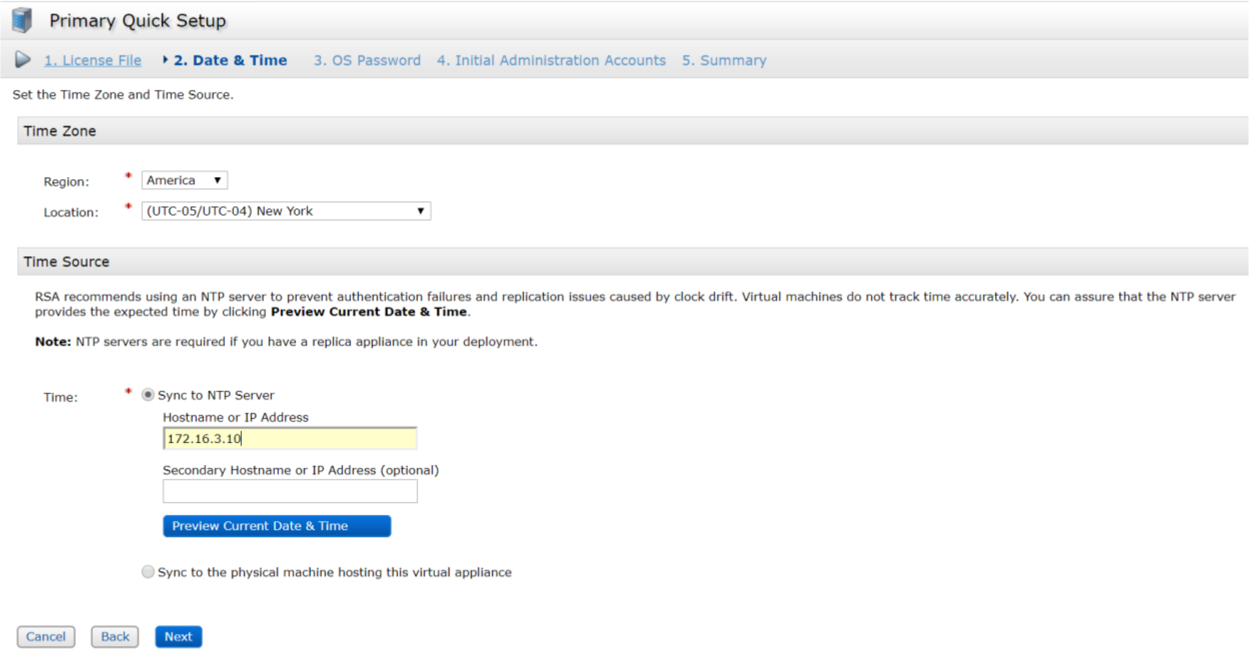
Upload License File: Choose File No file chosen Upload

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

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

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
License Feature	**Aggregate Summary**

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

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.**

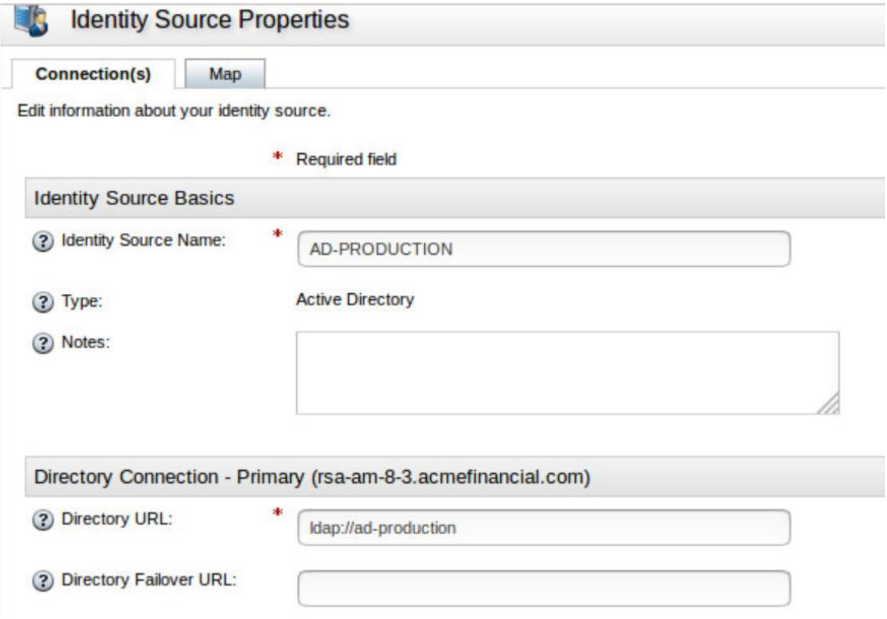
2.12.3 LDAP Integration

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:



Identity Source Properties

Edit information about your identity source.

* Required field

Identity Source Basics

Identity Source Name: * AD-PRODUCTION

Type: Active Directory

Notes:

Directory Connection - Primary (rsa-am-8-3.acmefinancial.com)

Directory URL: * ldap://ad-production

Directory Failover URL:

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.

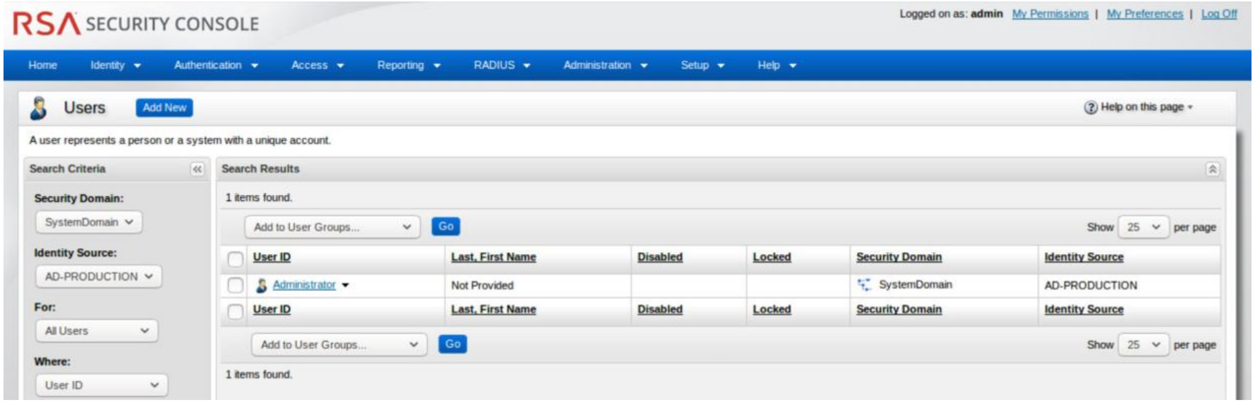
3. Navigate to **Identity > Users > Manage Existing.**

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.



Logged on as: admin | My Permissions | My Preferences | Log Off

Users

A user represents a person or a system with a unique account.

Search Criteria

Security Domain: SystemDomain

Identity Source: AD-PRODUCTION

For: All Users

Where: User ID

Search Results

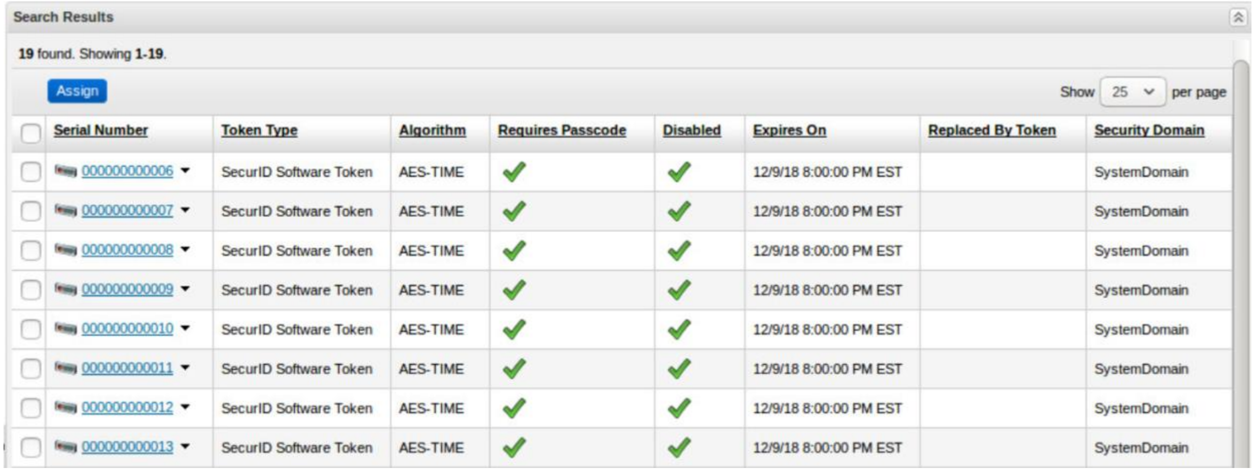
1 items found.

User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
Administrator	Not Provided			SystemDomain	AD-PRODUCTION

1 items found.

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.**



Search Results

19 found. Showing 1-19.

Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	Expires On	Replaced By Token	Security Domain
000000000006	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000007	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000008	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000009	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000010	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000011	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000012	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain
000000000013	SecurID Software Token	AES-TIME	✓	✓	12/9/18 8:00:00 PM EST		SystemDomain

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

2.12.5 Software Token Profiles and Token Distribution

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

2.13 Splunk

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

2.13.1 How It's Used

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

2.13.2 Installation

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

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

2.13.3 Queries

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

2.13.4 DemoBomgar-AD-Auth-UnauthV1

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

2.13.5 DemoRadiant-AD-Event-Details

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

2.13.6 SSL Forwarding

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

Appendix A List of Acronyms

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

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