

Data Integrity:

Identifying and Protecting Assets Against Ransomware and Other Destructive Events

Volume C:
How-To Guides

Jennifer Cawthra

National Cybersecurity Center of Excellence
NIST

Michael Ekstrom

Lauren Lusty

Julian Sexton

John Sweetnam

The MITRE Corporation
McLean, Virginia

December 2020

FINAL

This publication is available free of charge from
<https://doi.org/10.6028/NIST.SP.1800-25>.

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect>.



DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-25C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-25C, 489 pages, (December 2020), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at ds-nccoe@nist.gov.

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

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 security—the NCCoE applies standards and best practices to develop modular, 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 Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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 1800 series) 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 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

Ransomware, destructive malware, insider threats, and even honest user mistakes present ongoing threats to organizations. Organizations' data, such as database records, system files, configurations,

user files, applications, and customer data, are all potential targets of data corruption, modification, and destruction. Formulating a defense against these threats requires two things: a thorough knowledge of the assets within the enterprise, and the protection of these assets against the threat of data corruption and destruction. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, has built an example solution to address these data integrity challenges.

Multiple systems need to work together to identify and protect an organization’s assets against the threat of corruption, modification, and destruction. This project explores methods to effectively identify assets (devices, data, and applications) that may become targets of data integrity attacks, as well as the vulnerabilities in the organization’s system that facilitate these attacks. It also explores methods to protect these assets against data integrity attacks using backups, secure storage, integrity checking mechanisms, audit logs, vulnerability management, maintenance, and other potential solutions.

KEYWORDS

attack vector; asset awareness; data integrity; data protection; malicious actor; malware; ransomware

ACKNOWLEDGMENTS

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

Name	Organization
Kyle Black	Bay Dynamics
Sunjeet Randhawa	Broadcom Inc.
Peter Romness	Cisco Systems
Matthew Hyatt	Cisco Systems
Hans Ismirnioglou	Cryptonite
Sapna George	Cryptonite
Justin Yackoski	Cryptonite

Name	Organization
Steve Petruzzo	GreenTec USA
Steve Roberts	Micro Focus
Timothy McBride	NIST
Christopher Lowde	Semperis
Thomas Leduc	Semperis
Darren Mar-Elia	Semperis
Kirk Lashbrook	Semperis
Mickey Bresman	Semperis
Jim Wachhaus	Tripwire
Humphrey Christian	Symantec Corporation
Jon Christmas	Symantec Corporation
Kenneth Durbin	Symantec Corporation
Matthew Giblin	Symantec Corporation
Nancy Correll	The MITRE Corporation
Chelsea Deane	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Milissa McGinnis	The MITRE Corporation
Karri Meldorf	The MITRE Corporation

Name	Organization
Denise Schiavone	The MITRE Corporation
Anne Townsend	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
Symantec Corporation	Symantec Data Loss Prevention v15.1
Cisco Systems	Cisco ISE v2.4, Cisco Web Security Appliance v10.1
GreenTec USA	GreenTec WORMdisk v151228
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7, Tripwire IP360 v9.0.1
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Cryptonite	CryptoniteNXT v2.9.1
Semperis	Semperis Active Directory Forest Recovery v2.5, Semperis Directory Services Protector v2.7

Contents

1	Introduction	1
1.1	How to Use this Guide.....	1
1.2	Build Overview	2
	Typographic Conventions.....	3
2	Product Installation Guides	4
2.1	Active Directory and Domain Name System (DNS Server).....	4
2.1.1	Installing Features.....	4
2.1.2	Creating a Certificate Authority.....	19
2.1.3	Configure Account to Add Computers to Domain	34
2.1.4	Adding Machines to the Domain	41
2.1.5	Configure Active Directory to Audit Account Activity.....	46
2.1.6	Configure Reverse Lookup Zones.....	48
2.2	Microsoft Exchange Server.....	54
2.2.1	Install Microsoft Exchange.....	54
2.3	Windows Server Hyper-V Role	65
2.3.1	Production Installation.....	65
2.4	MS SQL Server	73
2.4.1	Install and Configure MS SQL.....	73
2.4.2	Open Port on Firewall	83
2.4.3	Add a New Login to the Database.....	88
2.5	Microsoft IIS Server	90
2.5.1	Install IIS.....	90
2.5.2	IIS Configuration	98
2.6	GreenTec WORMdisks.....	102
2.6.1	Format GreenTec WORMdisks.....	103

- 2.6.2 Obtain Status Information About GreenTec WORMdisks103
- 2.6.3 Map GreenTec WORMdisks to Drive Letters104
- 2.6.4 Activate Write Protection in GreenTec WORMdisks105
- 2.7 CryptoniteNXT 109
 - 2.7.1 Configure Cryptonite NXT109
 - 2.7.1.1 Verify a New Device.....109
 - 2.7.1.2 Create a New User112
 - 2.7.1.3 Create a New Policy115
 - 2.7.2 Integrate CryptoniteNXT with Active Directory122
 - 2.7.2.1 Generate a Keytab File122
 - 2.7.2.2 Import Keytab File to ACC.....129
- 2.8 Backups..... 136
 - 2.8.1 FileZilla FTPS Server Setup136
 - 2.8.2 FileZilla Configuration139
 - 2.8.3 Add a User to FileZilla144
 - 2.8.4 Duplicati Client Installation (Windows)146
 - 2.8.5 Duplicati Client Installation (Ubuntu)149
 - 2.8.6 Configure Duplicati150
- 2.9 Semperis Active Directory Forest Recovery 155
 - 2.9.1 Install Semperis ADFR155
 - 2.9.2 Create a Backup Schedule for the Domain Controller164
 - 2.9.3 Recover the Active Directory Forest from a Backup.....167
- 2.10 Semperis Directory Services Protector..... 170
 - 2.10.1 Configure Active Directory for Semperis DSP170
 - 2.10.2 Install Semperis DSP.....183
- 2.11 Micro Focus ArcSight Enterprise Security Manager..... 195
 - 2.11.1 Install the ArcSight Console196
 - 2.11.2 Install Individual ArcSight Windows Connectors209

- 2.11.3 Install Individual ArcSight Ubuntu Connectors227
- 2.11.4 Install a Connector Server for ESM on Windows 2012 R2240
- 2.11.5 Install Preconfigured Filters for ArcSight253
 - 2.11.5.1 Install Activate Base.....253
 - 2.11.5.2 Install Packages.....255
- 2.11.6 Apply Filters to a Channel256
- 2.12 Tripwire Enterprise 257
 - 2.12.1 Install Tripwire Enterprise.....257
 - 2.12.2 Install the Axon Bridge270
 - 2.12.3 Install the Axon Agent (Windows)270
 - 2.12.4 Install the Axon Agent (Linux)271
 - 2.12.5 Configure Tripwire Enterprise.....272
 - 2.12.5.1 Terminology.....272
 - 2.12.5.2 Tags.....273
 - 2.12.5.3 Rules275
 - 2.12.5.4 Tasks279
- 2.13 Tripwire Log Center 283
 - 2.13.1 Install Tripwire Log Center Manager283
 - 2.13.2 Configure Tripwire Log Center Manager283
 - 2.13.3 Install Tripwire Log Center Console289
- 2.14 Cisco Web Security Appliance 289
 - 2.14.1 Network Configuration289
 - 2.14.2 System Setup290
 - 2.14.3 Using WSA to Proxy Traffic298

2.14.3.1	Creating a PAC File.....	299
2.14.3.2	Setting Up Web Proxy Auto Discovery (WPAD).....	301
2.14.3.3	Configure Group Policy to Use Explicit Proxy	304
2.14.4	Denylisting	309
2.15	Symantec Data Loss Prevention	316
2.15.1	Install Oracle 12c Enterprise	316
2.15.2	Create an Oracle Database for Symantec DLP	323
2.15.3	Configuring the Oracle Listener	324
2.15.4	Install Symantec DLP	336
2.15.5	Configure Symantec DLP	346
2.16	Cisco Identity Services Engine	347
2.16.1	Initial Setup	347
2.16.2	Inventory: Configure SNMP on Routers/Network Devices.....	347
2.16.3	Inventory: Configure Device Detection.....	347
2.16.4	Policy Enforcement: Configure Active Directory Integration	351
2.16.5	Policy Enforcement: Enable Passive Identity with AD	354
2.16.6	Policy Enforcement: Developing Policy Conditions	359
2.16.7	Policy Enforcement: Developing Policy Results	361
2.16.8	Policy Enforcement: Enforcing a Requirement in Policy.....	362
2.16.9	Policy Enforcement: Configuring a Web Portal	363
2.16.10	Configuring RADIUS with Your Network Device	364
2.16.11	Configuring an Authentication Policy	365
2.16.12	Configuring an Authorization Policy	367
2.17	Tripwire IP360	368
2.17.1	Installation	368
2.17.2	Web Portal	373
2.17.3	Scanning.....	374
2.18	Integration: Tripwire Log Center and Tripwire Enterprise.....	377

- 2.19 Integration: Tripwire Log Center and Tripwire IP360 384
 - 2.19.1 Configure IP360 and Log Center384
 - 2.19.2 Collect Tripwire IP360 Operational Logs.....387
 - 2.19.3 Configure Tripwire IP360 Scan Results Forwarding399
- 2.20 Integration: Tripwire Enterprise and Backups 412
 - 2.20.1 Export Configuration from Tripwire Enterprise413
 - 2.20.2 Back Up the Tripwire Enterprise Configuration413
- 2.21 Integration: Cisco ISE and CryptoniteNXT 413
 - 2.21.1 Requirements for Integrating Cisco ISE and CryptoniteNXT413
 - 2.21.2 Configuring CryptoniteNXT for RADIUS414
- 2.22 Integration: Backups and GreenTec 415
 - 2.22.1 Locate Backups with FileZilla and Duplicati415
 - 2.22.2 Back Up to a GreenTec Disk417
 - 2.22.3 Configure Network-Accessible GreenTec Disk.....418
 - 2.22.4 Secure Storage for Semperis ADFR420
- 2.23 Integration: Micro Focus ArcSight and FileZilla..... 421
 - 2.23.1 Enable Logs in FileZilla421
 - 2.23.2 Install Micro Focus ArcSight.....423
- 2.24 Integration: Micro Focus ArcSight and Tripwire 438
 - 2.24.1 Install Micro Focus ArcSight.....438
- 2.25 Integration: Micro Focus ArcSight and Cisco WSA..... 451
 - 2.25.1 Configure Cisco WSA to Forward Logs.....451
- 2.26 Integration: Micro Focus ArcSight and Cisco ISE..... 454
 - 2.26.1 Configure Cisco ISE to Forward Logs.....454
 - 2.26.2 Select Logs for Forwarding.....457
- 2.27 Integration: Micro Focus ArcSight and Symantec DLP 458
 - 2.27.1 Install Micro Focus ArcSight.....458
 - 2.27.2 Configure Symantec DLP to Forward Logs.....468
- 2.28 Integration: Micro Focus ArcSight and CryptoniteNXT 472

- 2.28.1 Configure CryptoniteNXT to Forward Logs to ArcSight472
- 2.29 Integration: Micro Focus ArcSight and Semperis DSP 473
 - 2.29.1 Configure Semperis DSP to Forward Logs.....473
- 2.30 Integrations: CryptoniteNXT..... 474
 - 2.30.1 Active Directory and DNS.....475
 - 2.30.2 Microsoft Exchange476
 - 2.30.3 FileZilla477
 - 2.30.4 GreenTec.....478
 - 2.30.5 Tripwire Enterprise478
 - 2.30.6 ArcSight ESM479
 - 2.30.7 Cisco ISE479
 - 2.30.8 Semperis DSP480
 - 2.30.9 Symantec DLP481
 - 2.30.10 Cisco WSA481
 - 2.30.11 Tripwire IP360.....482
 - 2.30.11.1 Tripwire Log Center, Tripwire IP360, Tripwire Enterprise, and ArcSight ESM483
 - 2.30.12 FileZilla and ArcSight485
 - 2.30.13 Cisco ISE and ArcSight485
 - 2.30.14 Cisco WSA and ArcSight486
 - 2.30.15 Semperis DSP and ArcSight486
 - 2.30.16 Symantec DLP and ArcSight487
- Appendix A List of Acronyms 488**

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 re-create 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 How to Use this Guide

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 data integrity identify-and protect-solution. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-25A: *Executive Summary*
- NIST SP 1800-25B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-25C: *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 1800-25A), which describes the following topics:

- challenges that enterprises face in identifying assets and protecting them from data integrity events
- example solution built at the 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 1800-25B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, *Assessing Risk Posture*, 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 1800-25A, with your leadership team members to help them understand the importance of adopting standards-based data integrity solutions.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use this How-To portion of the guide, NIST SP 1800-25C, 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 data integrity identify-and-protect solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.5 of Volume B, *Technologies*, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

1.2 Build Overview

The National Cybersecurity Center of Excellence (NCCoE) built a hybrid virtual-physical laboratory environment to explore methods to effectively identify assets and protect them against a data corruption event in various IT enterprise environments. The NCCoE also explored identifying vulnerabilities in advance of an incident. The servers in the virtual environment were built to the hardware specifications of their specific software components.

The NCCoE worked with members of the Data Integrity Community of Interest to develop a diverse but noncomprehensive set of use case scenarios against which to test the reference implementation. These are detailed in Volume B, Section 5.2. For a detailed description of our architecture, see Volume B, Section 4.

Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and pathnames; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, on-screen computer output, sample code examples, and status codes	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
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://nccoe.nist.gov .

2 Product Installation Guides

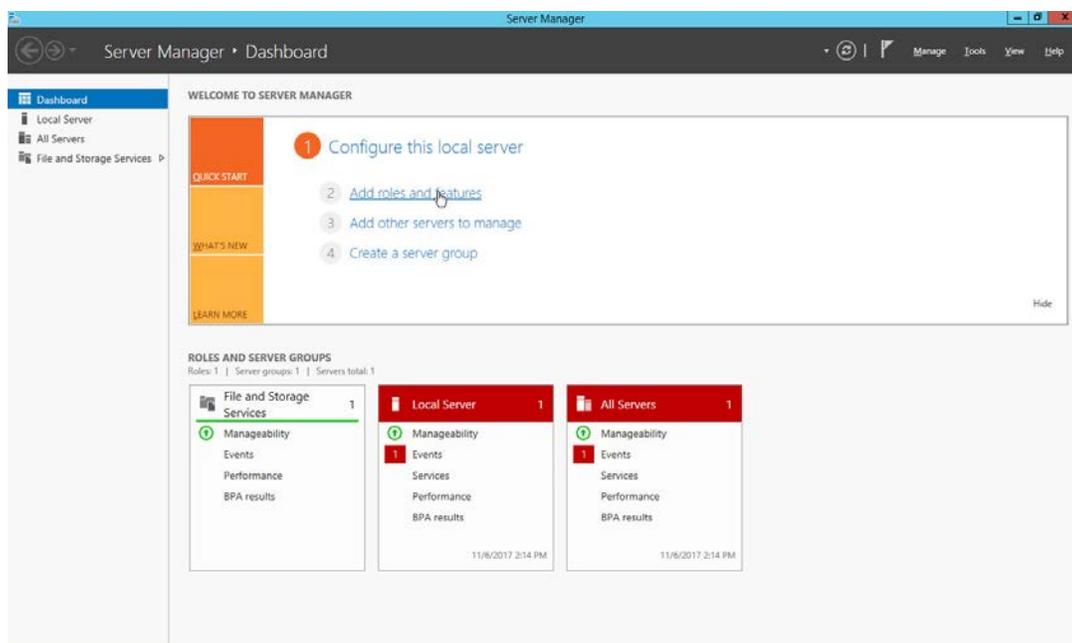
This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

2.1 Active Directory and Domain Name System (DNS Server)

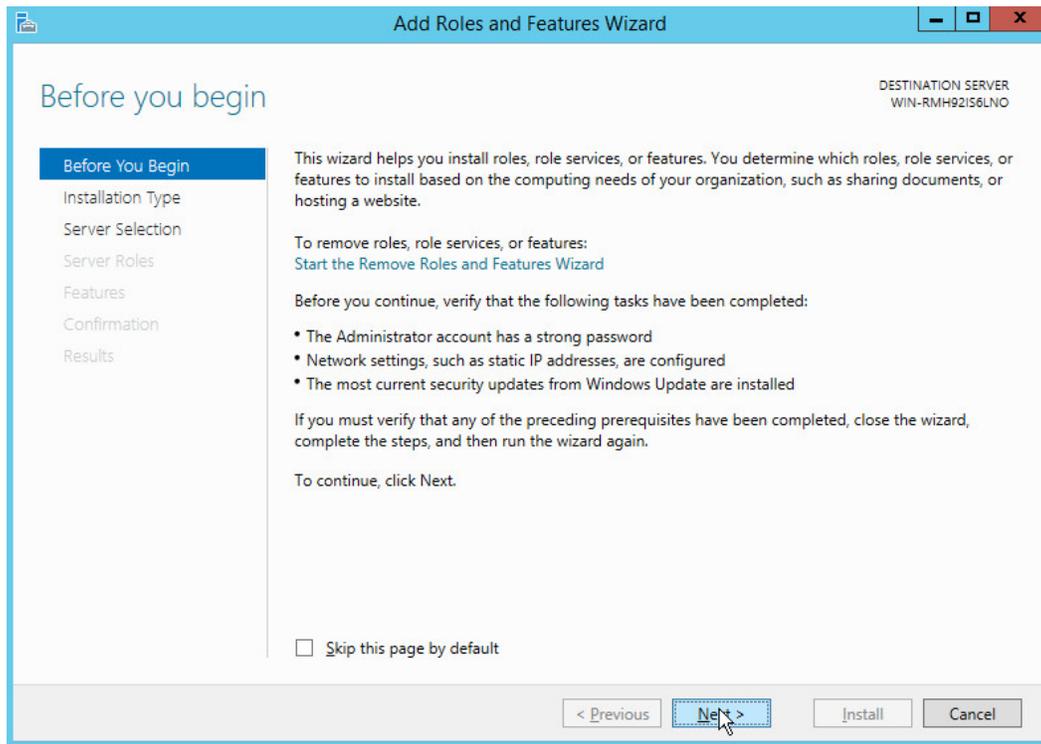
As part of our enterprise emulation, we included an Active Directory server that doubles as a DNS server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

2.1.1 Installing Features

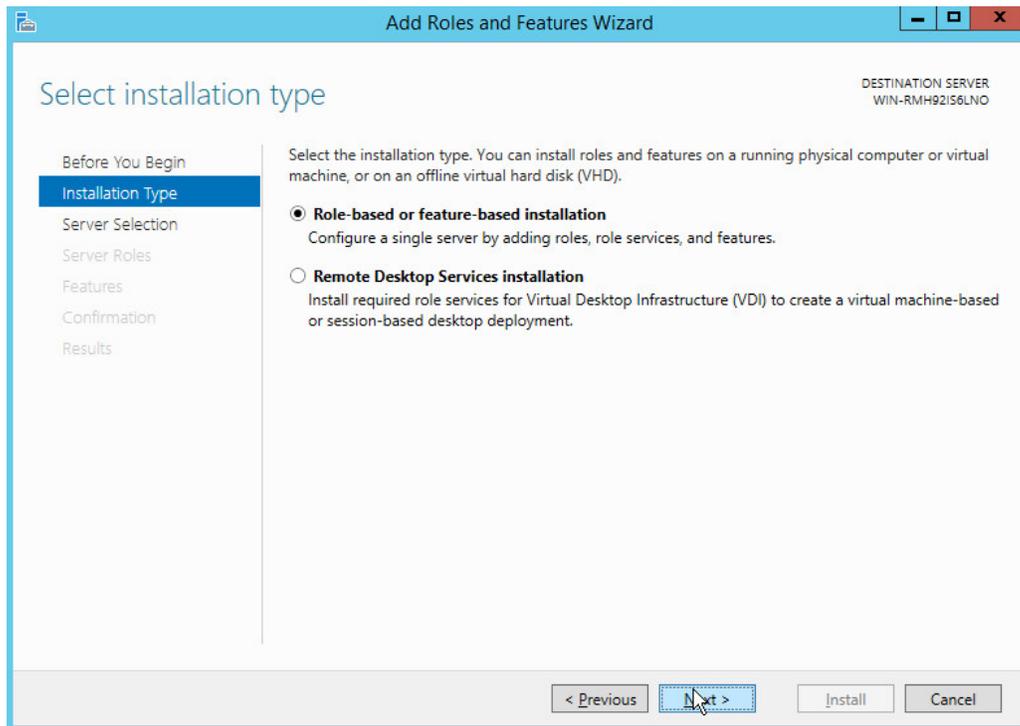
1. Open **Server Manager**.



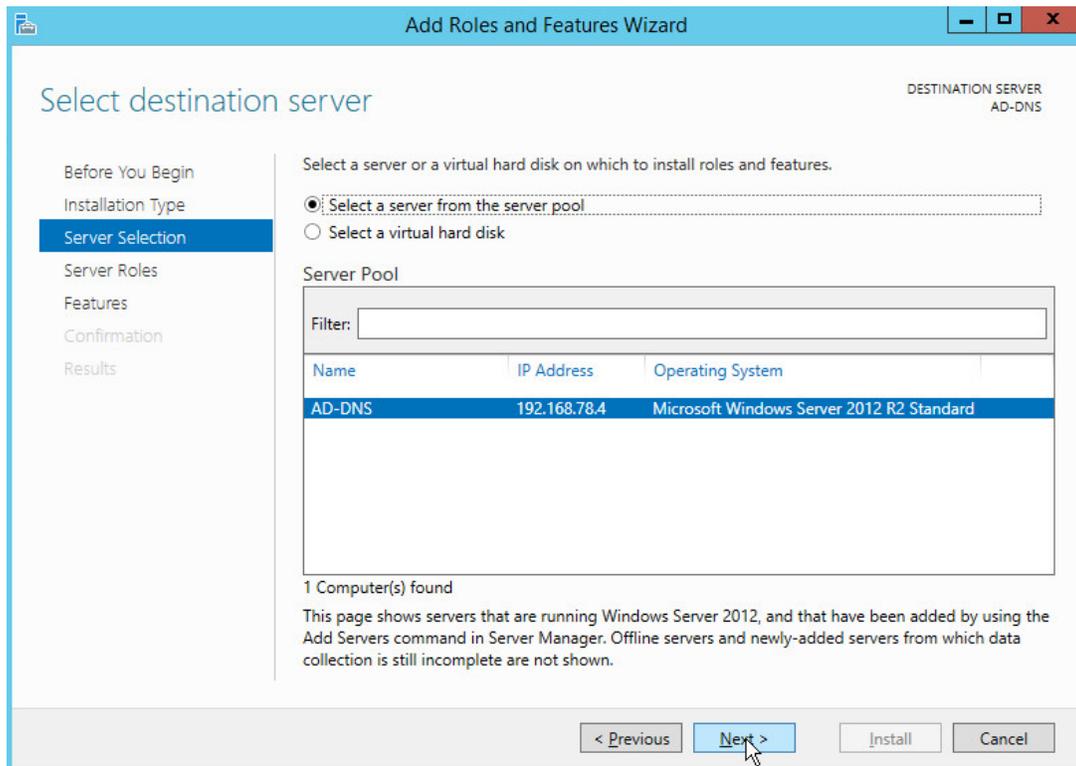
2. Click the link **Add roles and features**.



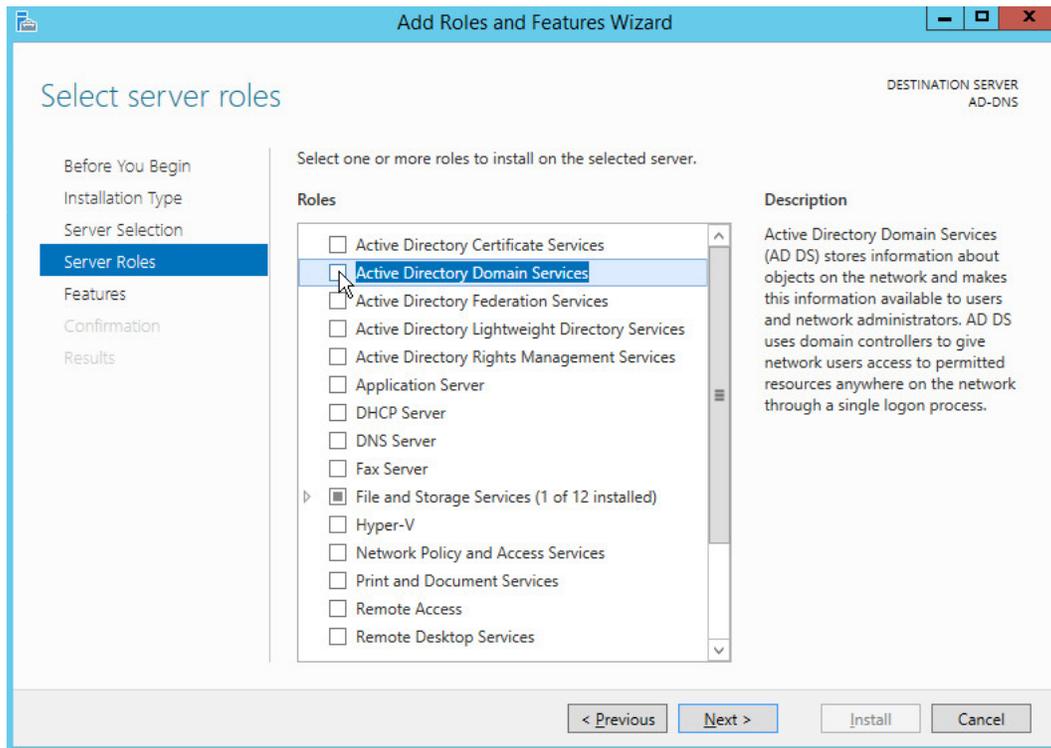
3. Click **Next**.
4. Select **Role-based or feature-based installation**.



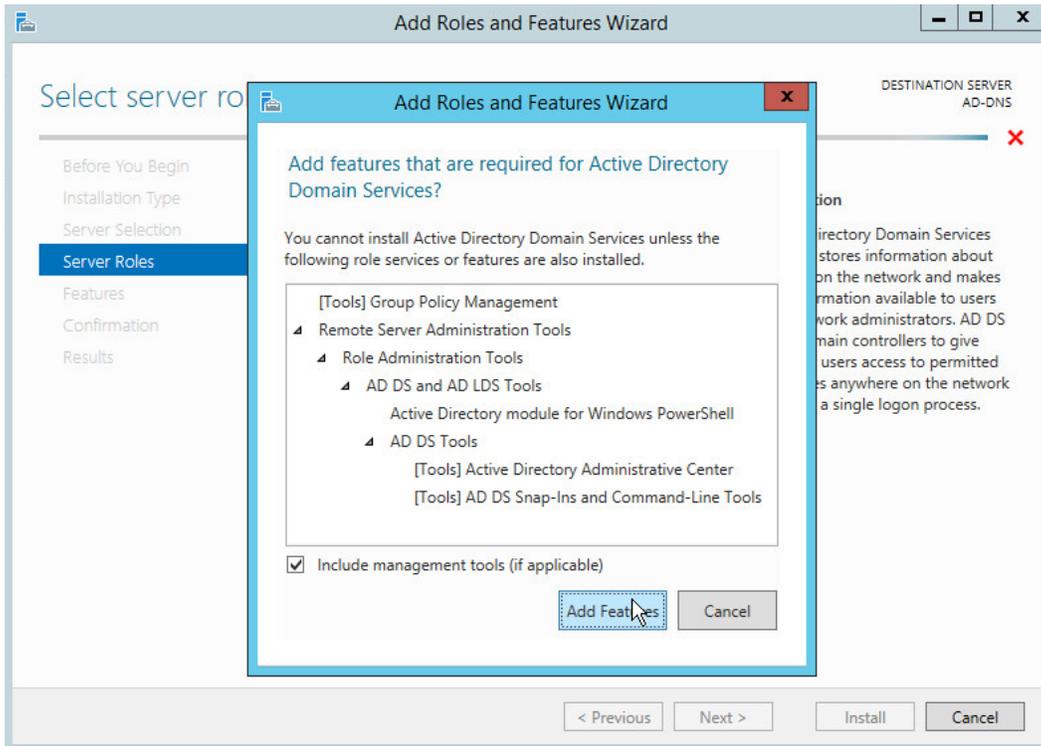
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Select the intended Active Directory server.



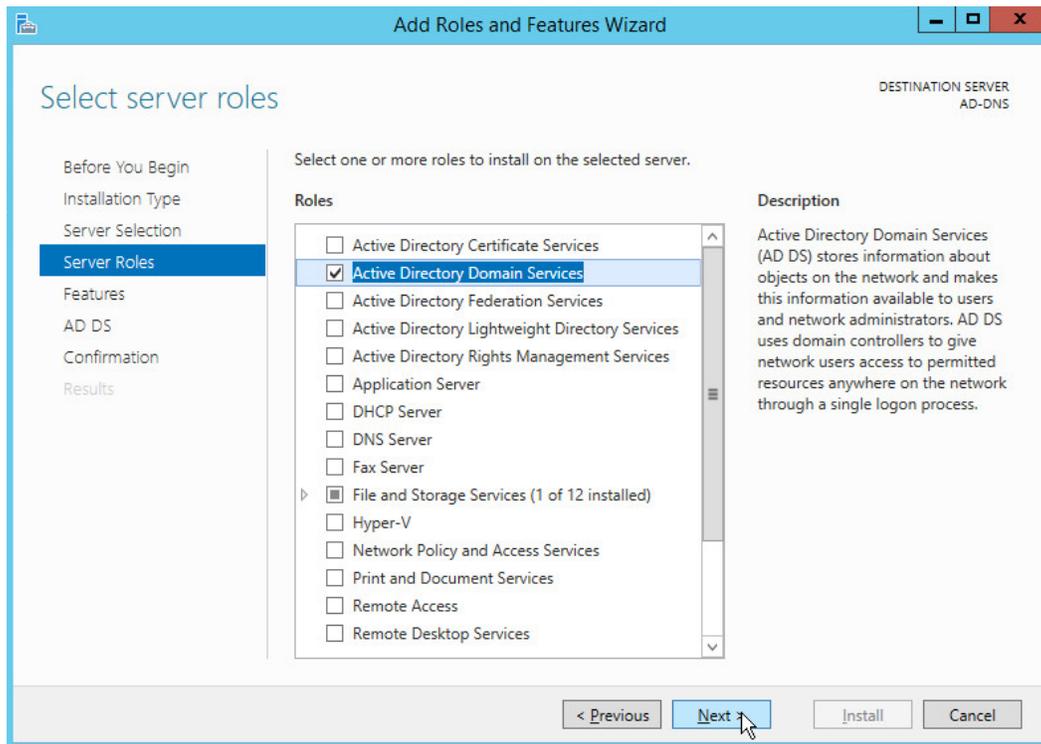
8. Click **Next**.



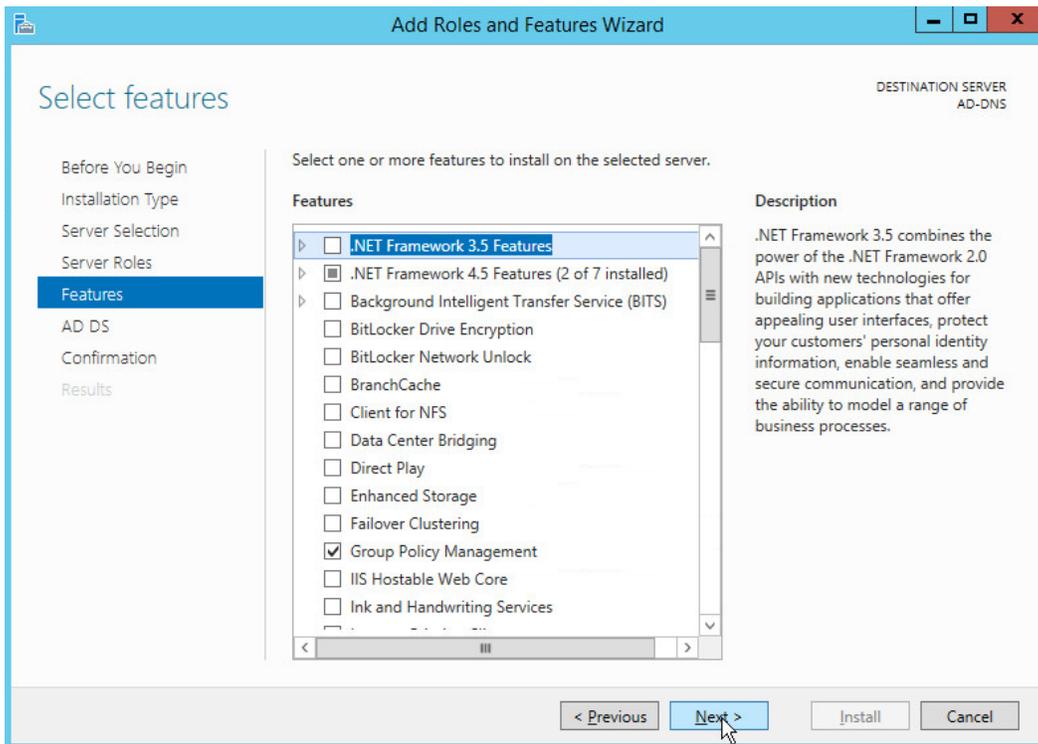
9. Check the box next to **Active Directory Domain Services**.



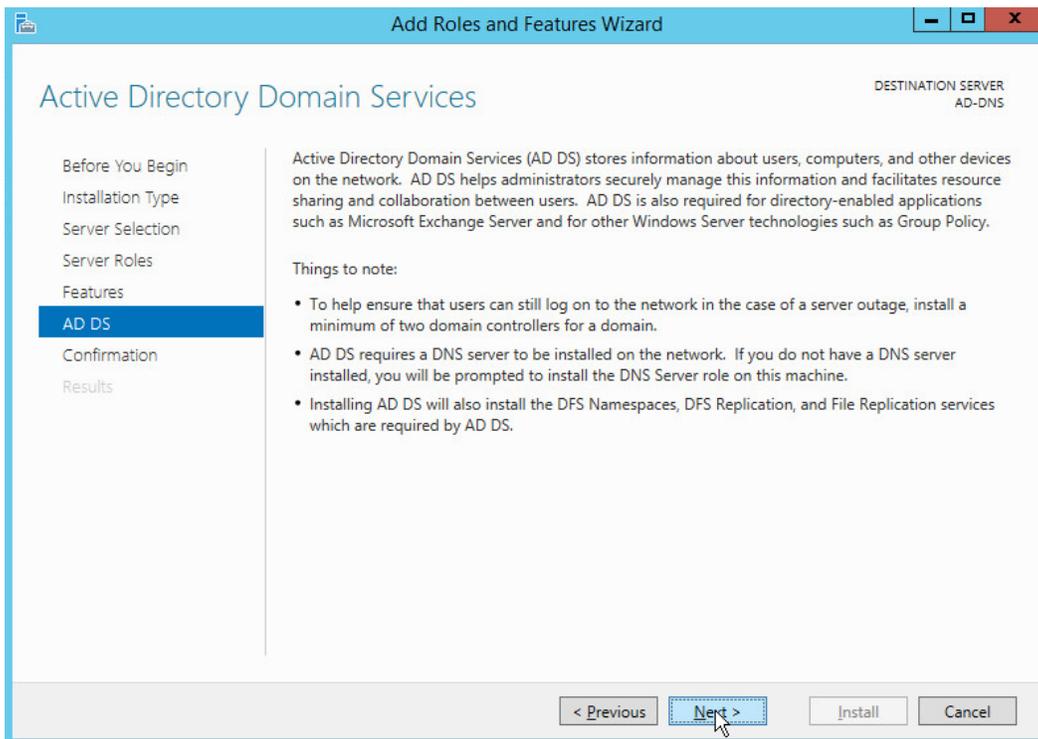
10. Click **Add Features**.



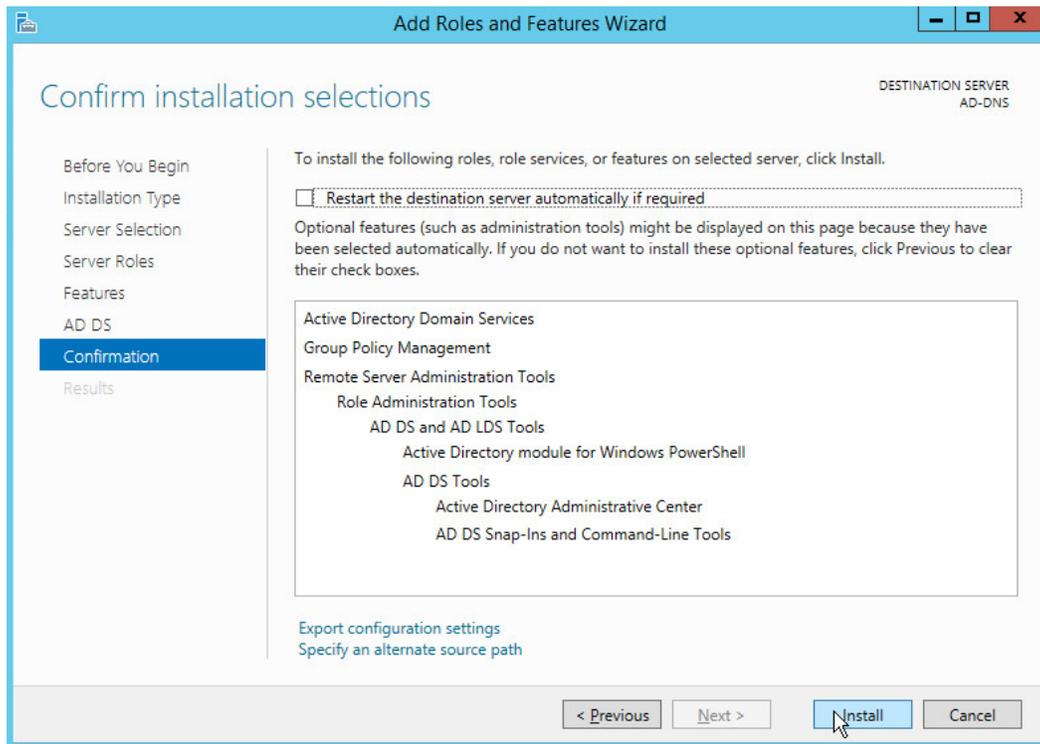
11. Click **Next**.



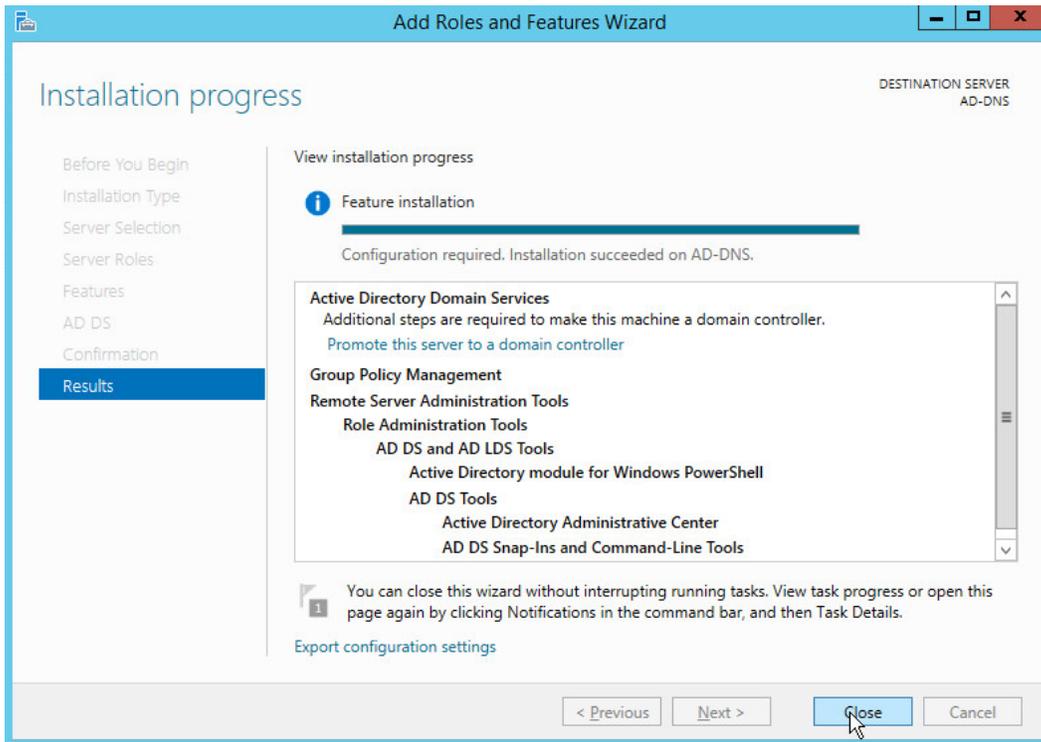
12. Click **Next**.



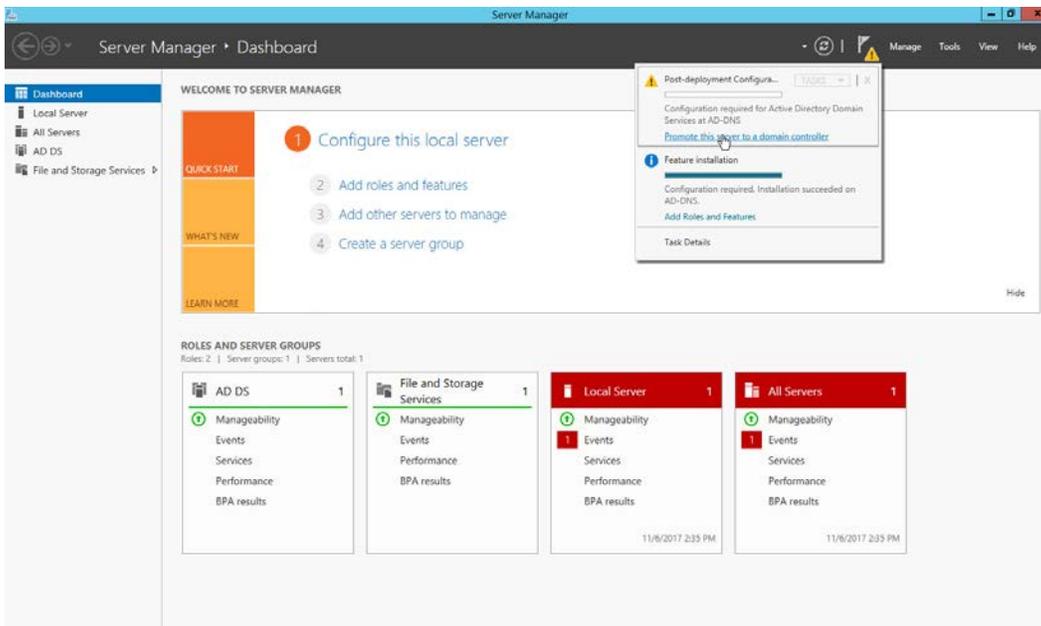
13. Click **Next**.



14. Click **Install**.
15. Wait for the installation to complete.



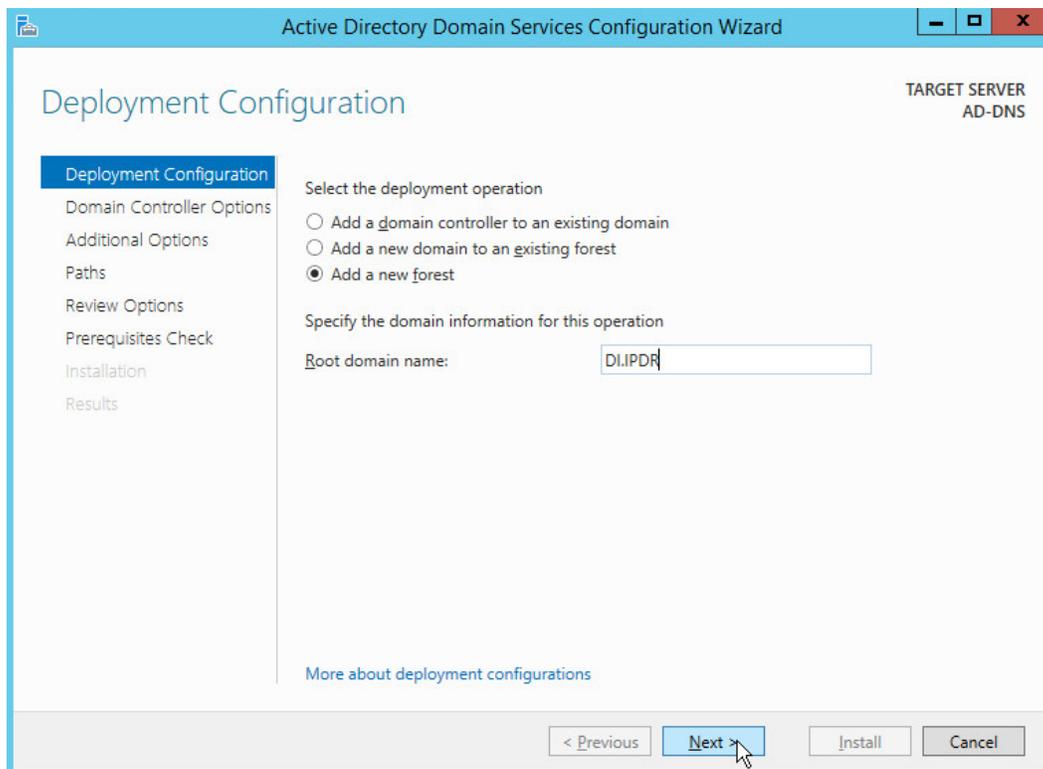
16. Click **Close**.



17. Click **Promote this server to a domain controller**.

18. Select **Add a new forest**.

19. Enter a **Root domain name**.

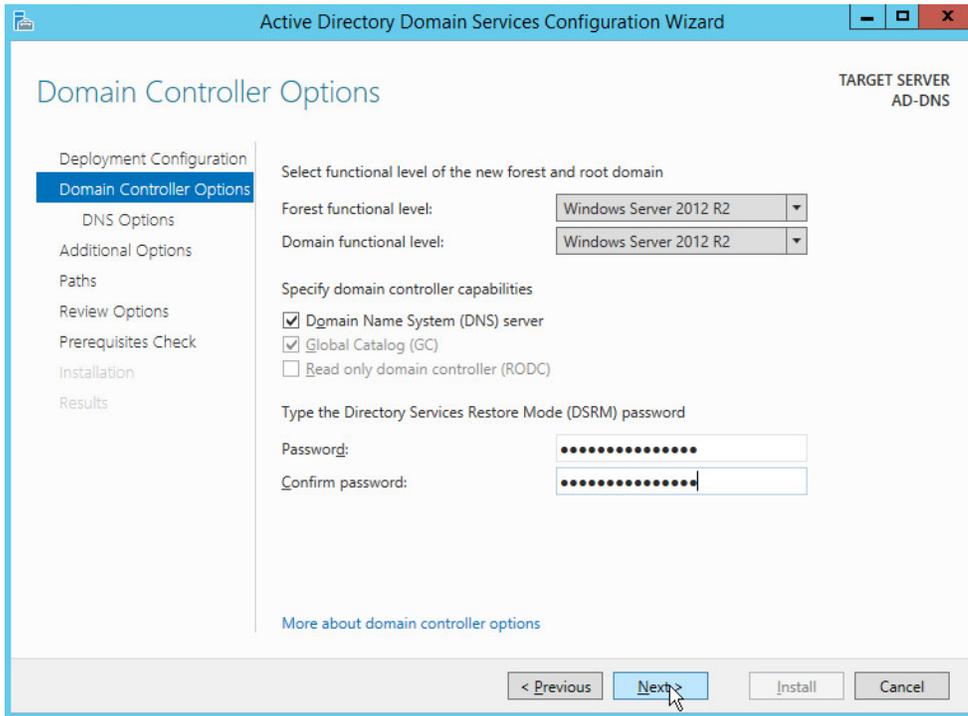


20. Click **Next**.

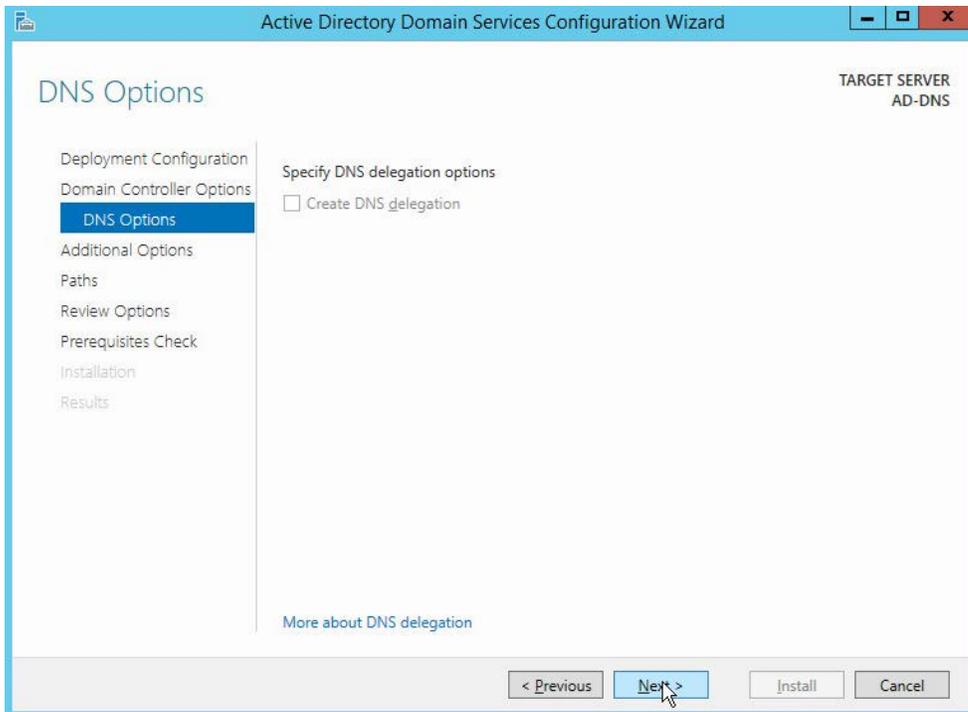
21. Select **Windows Server 2012 R2** for **Forest functional level** and **Domain functional level**.

22. Check the box next to **Domain Name System (DNS) server**.

23. Enter a **password**.

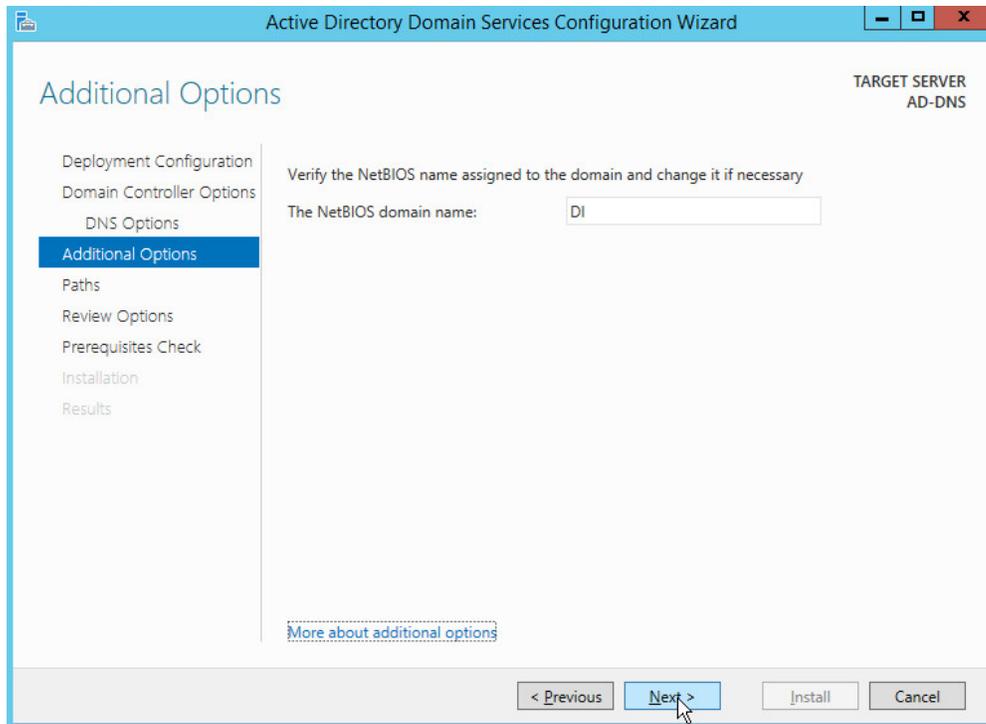


24. Click **Next**.

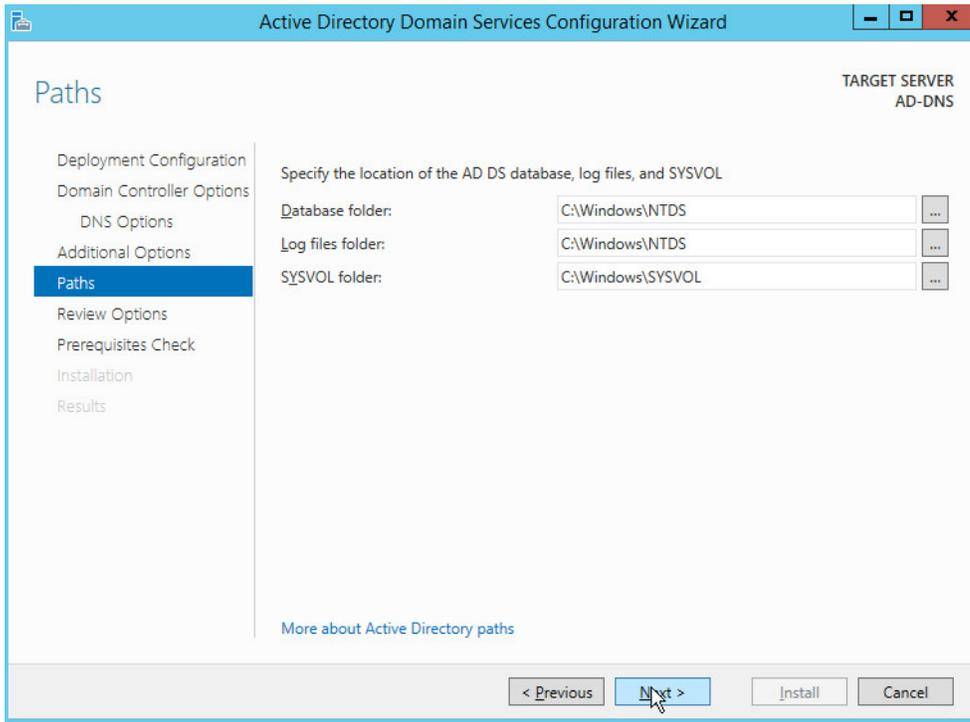


25. Click **Next**.

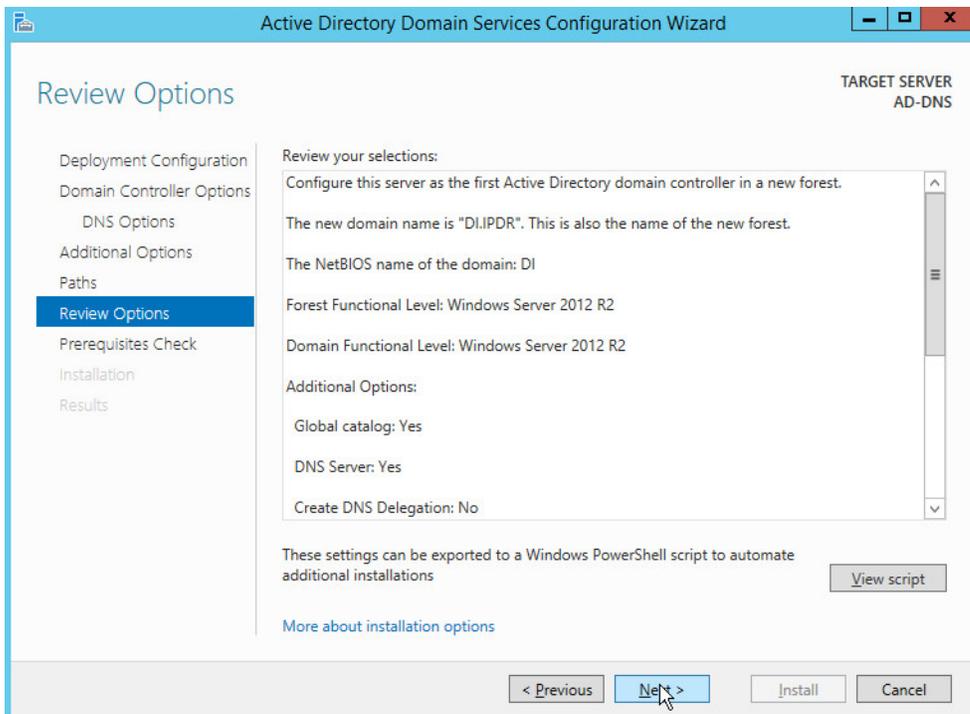
26. Verify the domain name.



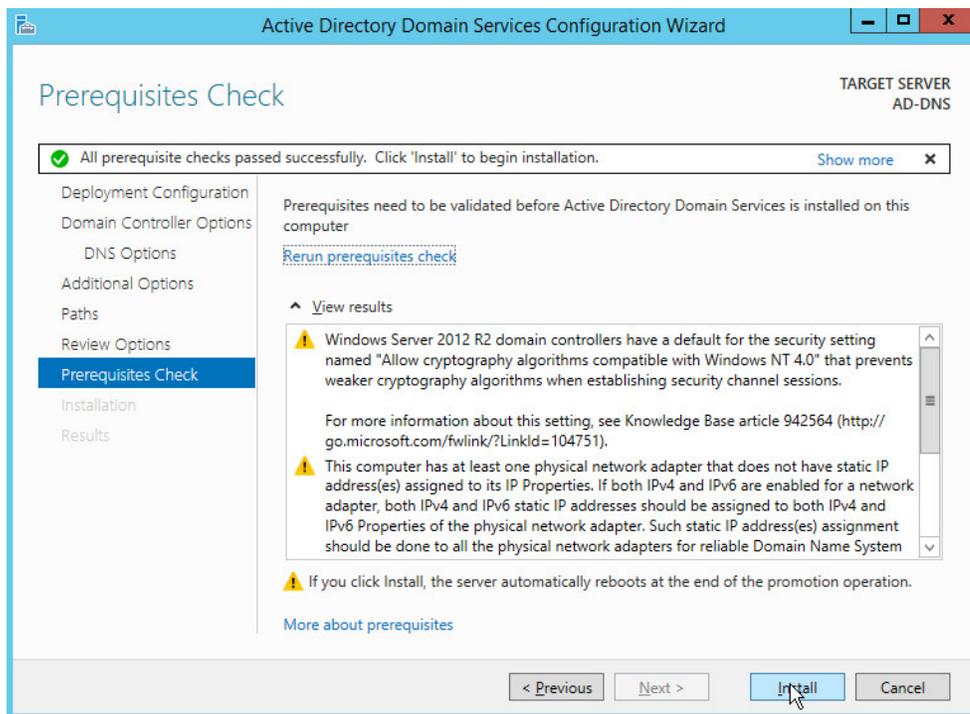
27. Click **Next**.



28. Click **Next**.



29. Click **Next**.



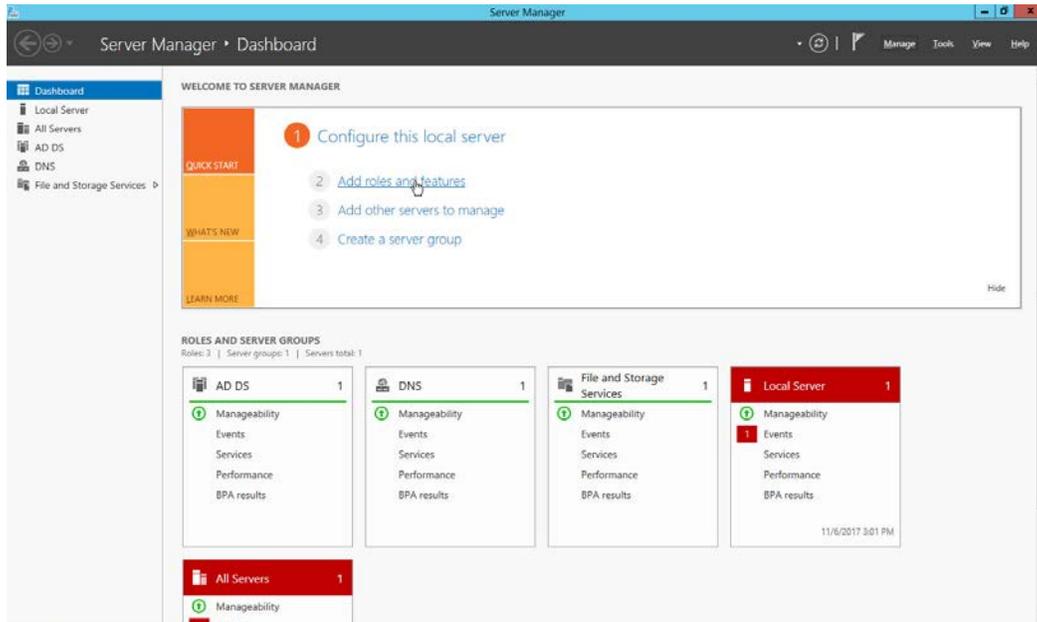
30. Click **Install**.

31. Wait for the installation to complete.

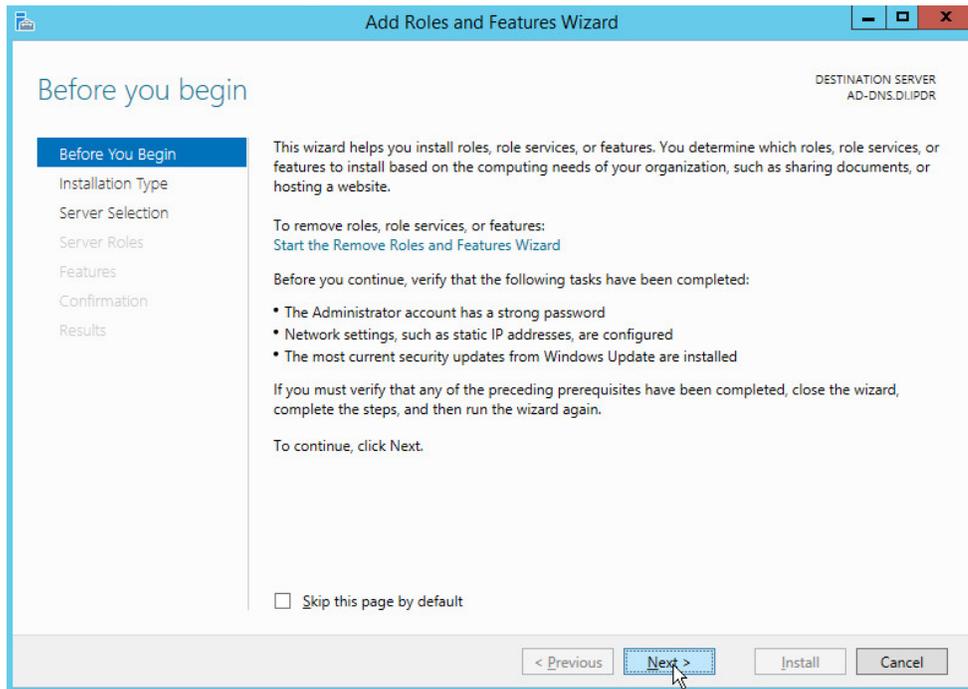
32. The server automatically reboots.

2.1.2 Creating a Certificate Authority

1. Open **Server Manager**.

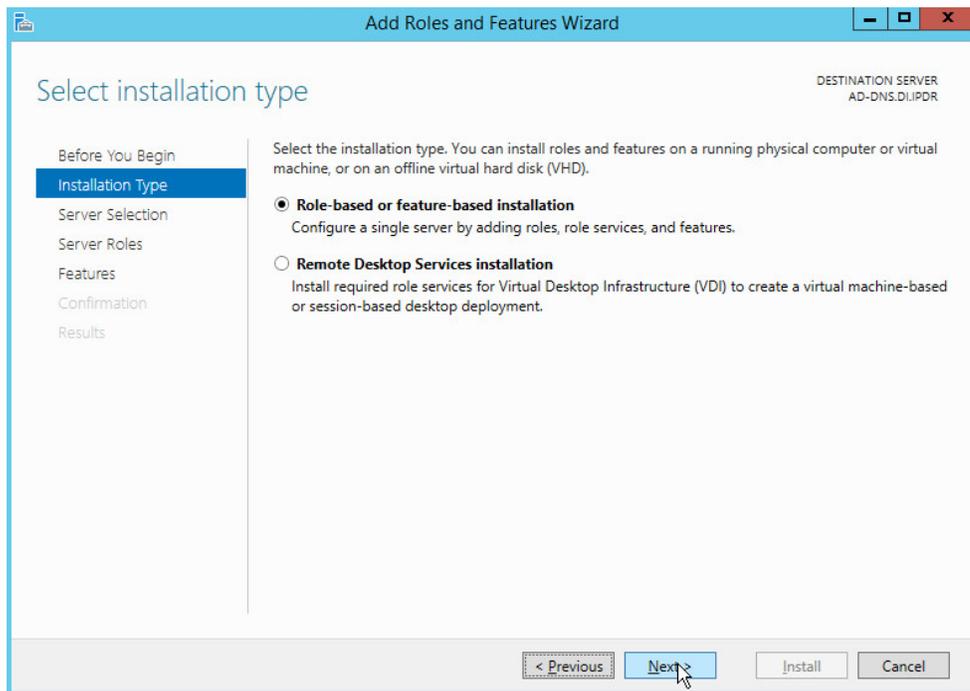


2. Click **Add roles and features**.

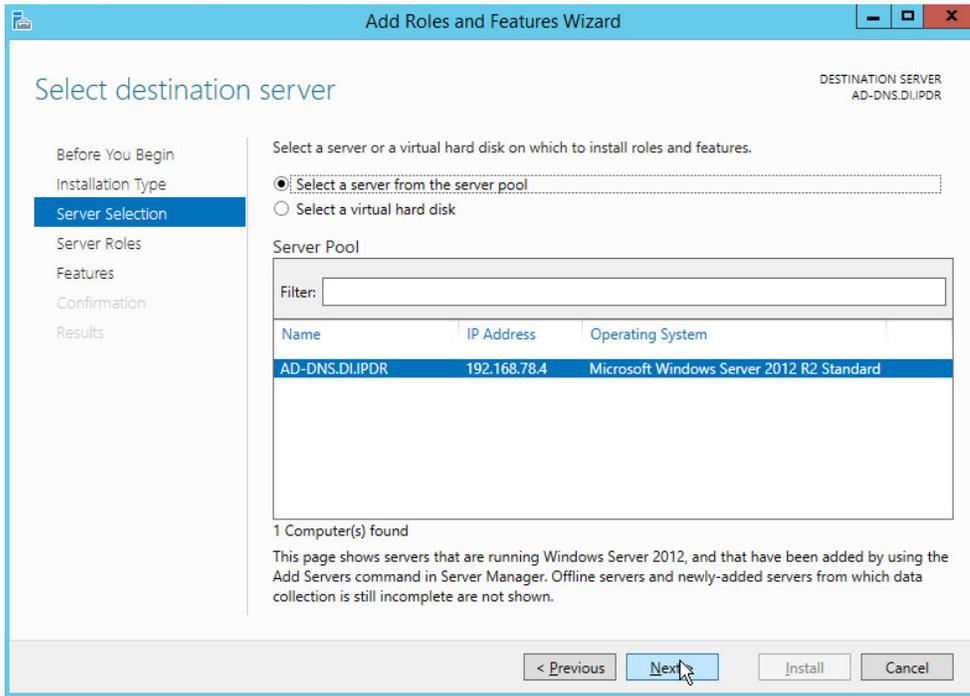


3. Click **Next**.

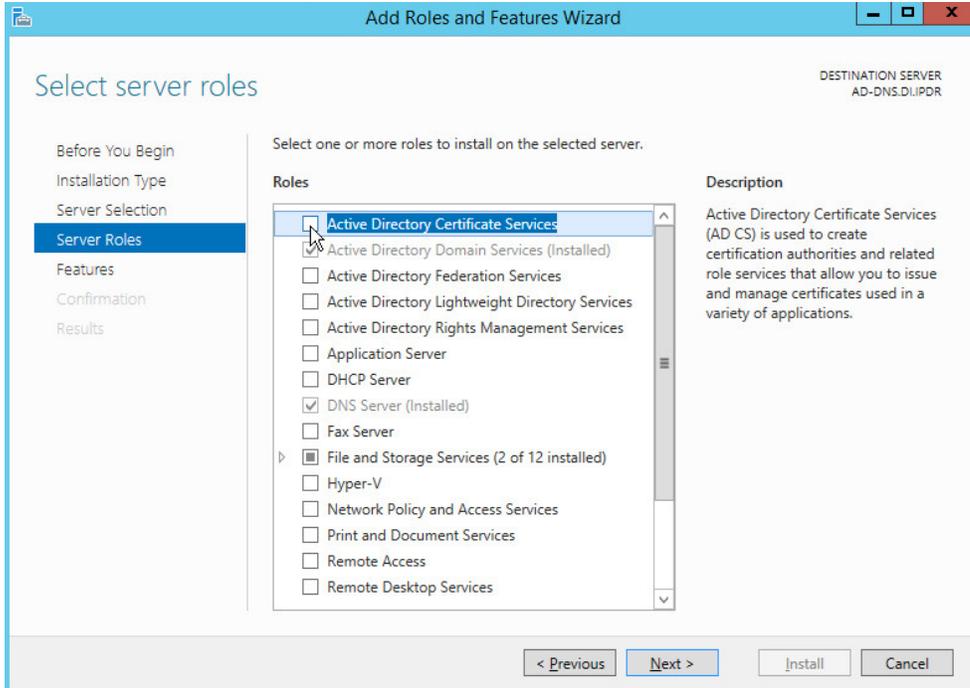
4. Select **Role-based or feature-based installation**.



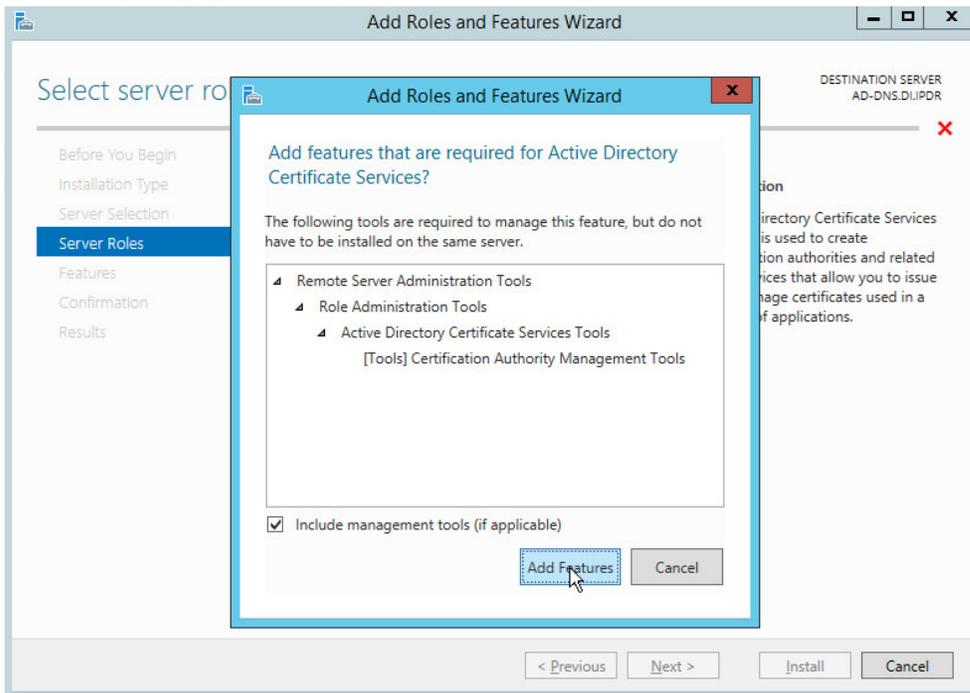
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Select the intended Active Directory server.



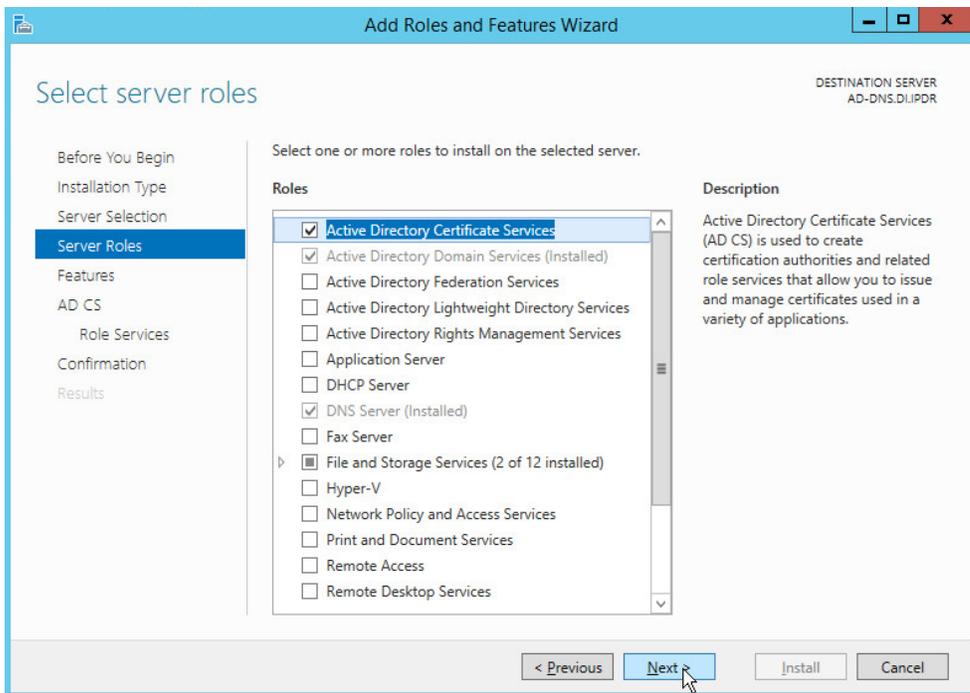
8. Click **Next**.



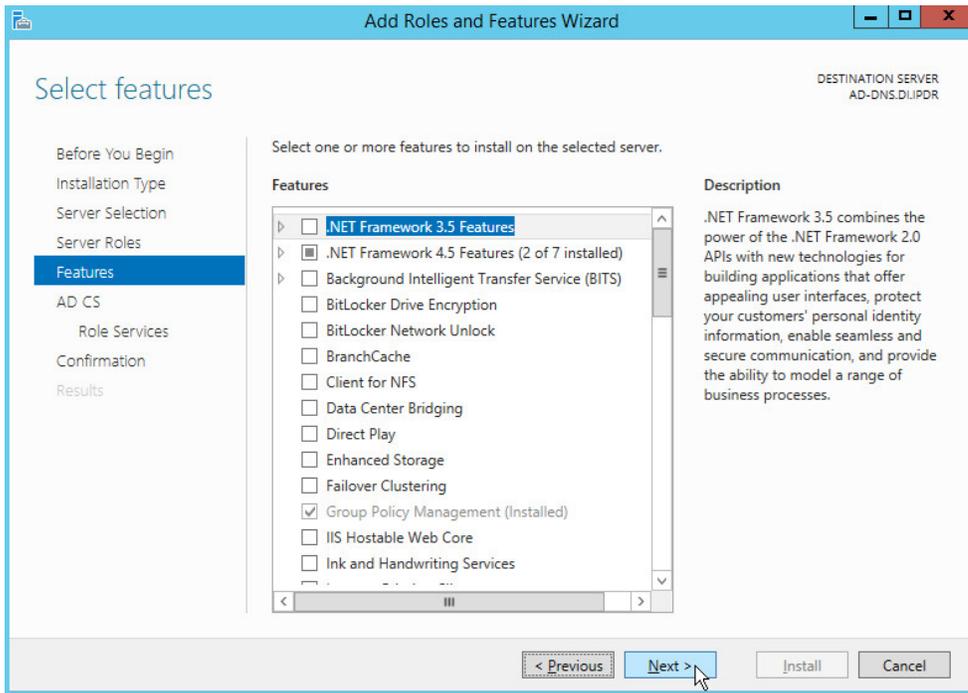
9. Check the box next to **Active Directory Certificate Services**.



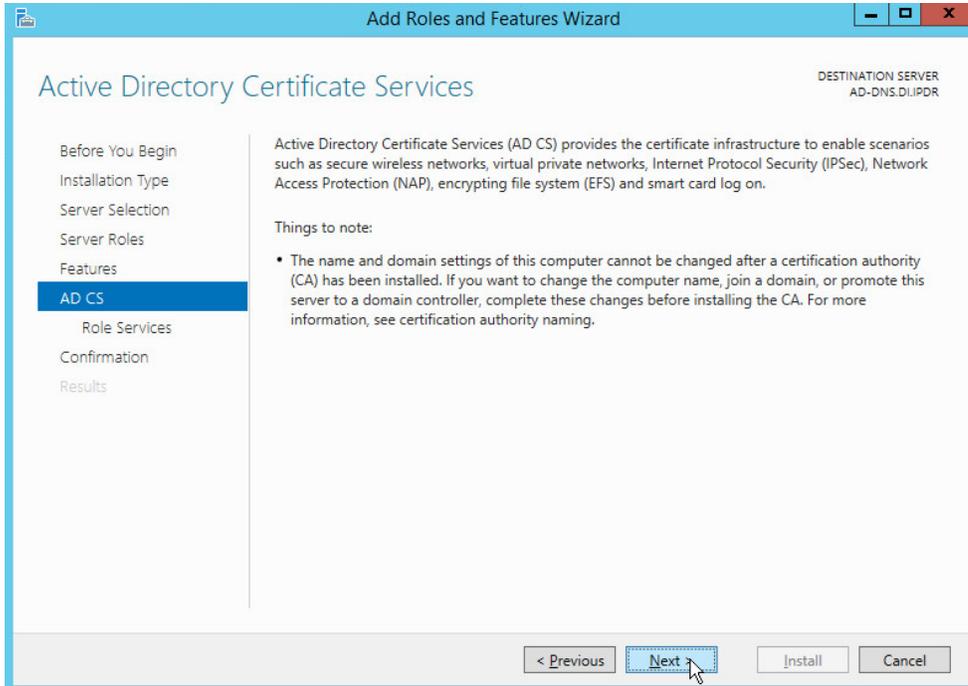
10. Click **Add Features**.



11. Click **Next**.

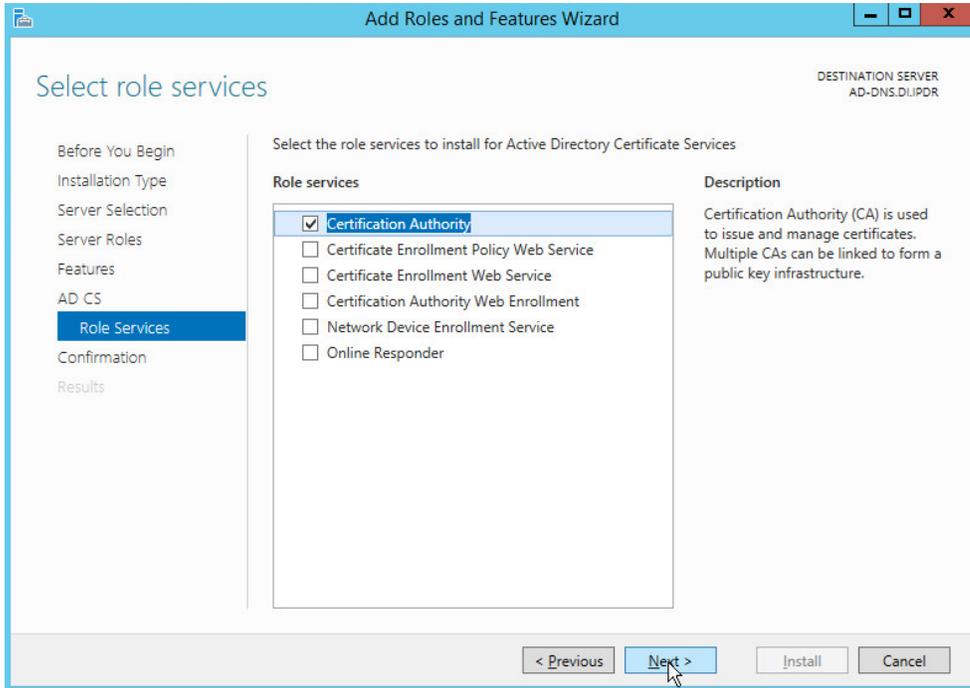


12. Click **Next**.

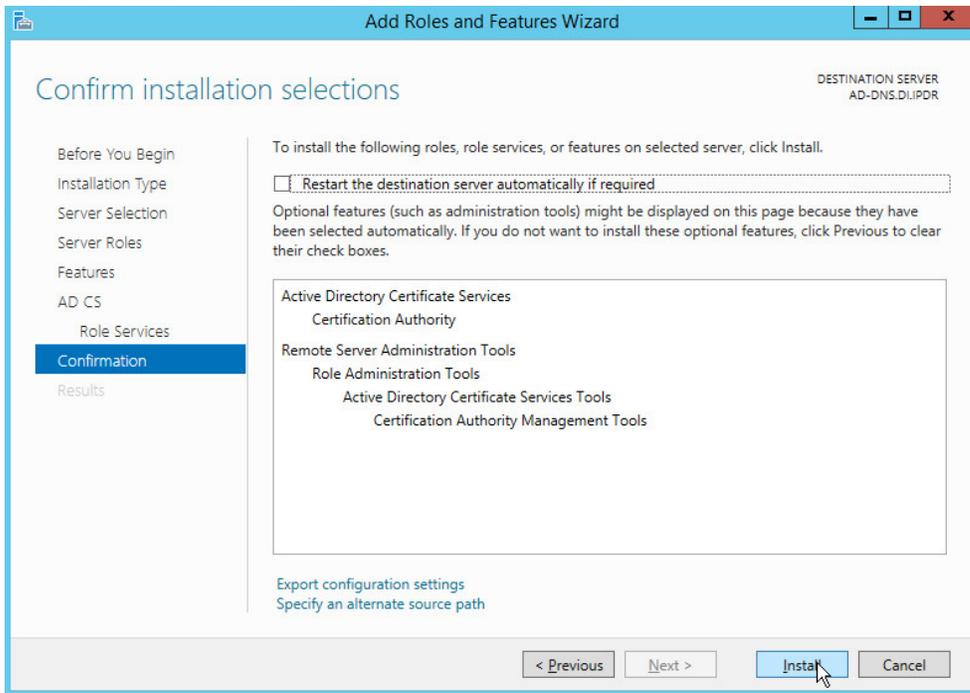


13. Click **Next**.

14. Check the box next to **Certification Authority**.

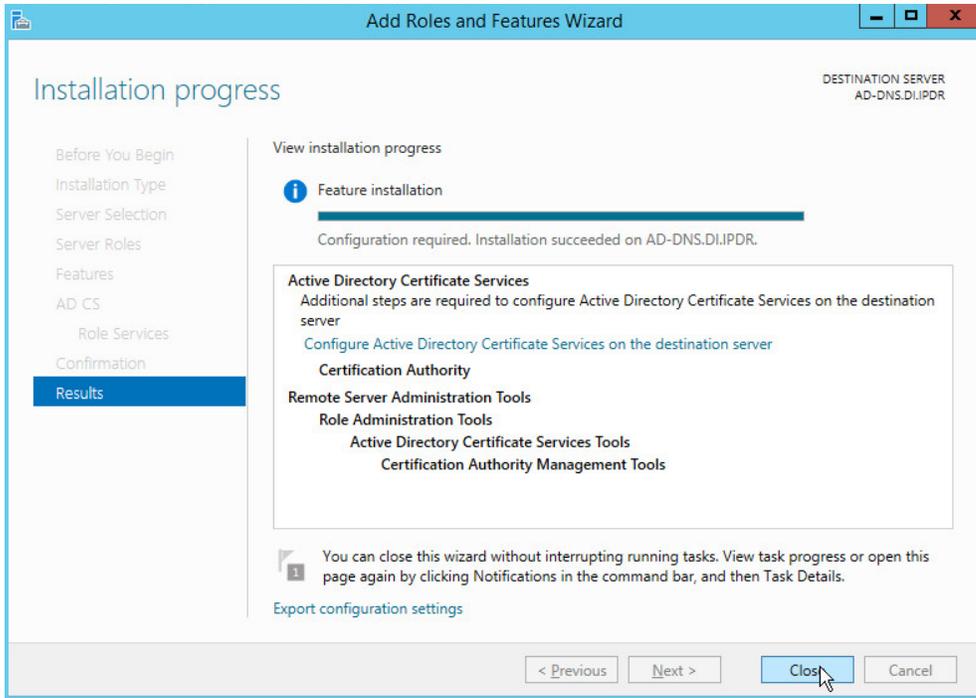


15. Click **Next**.

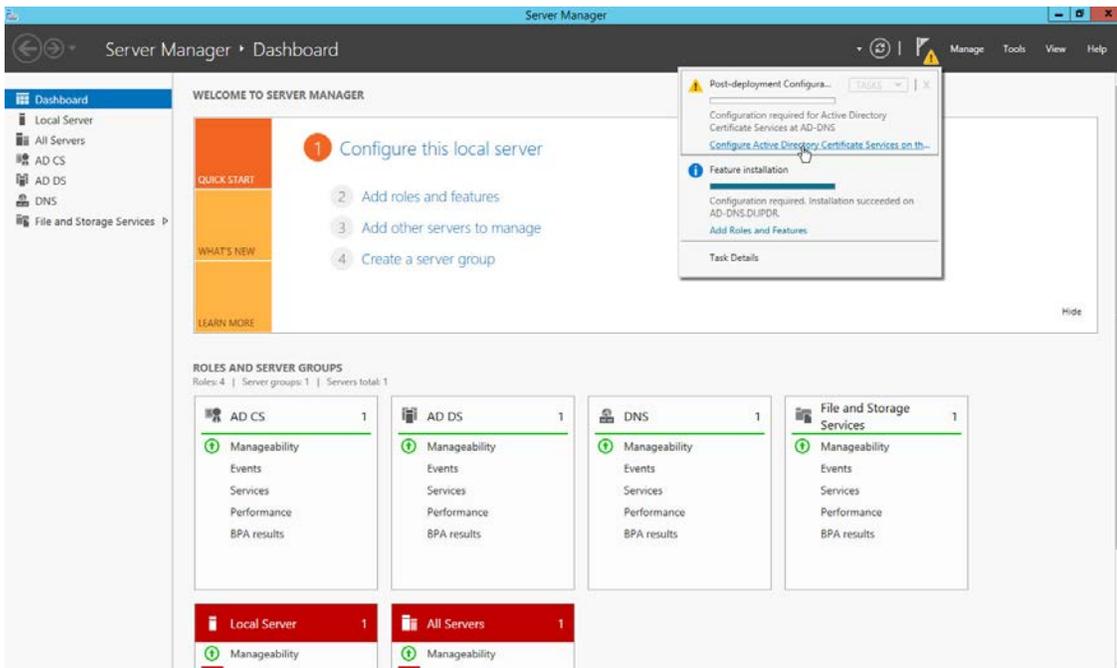


16. Click **Install**.

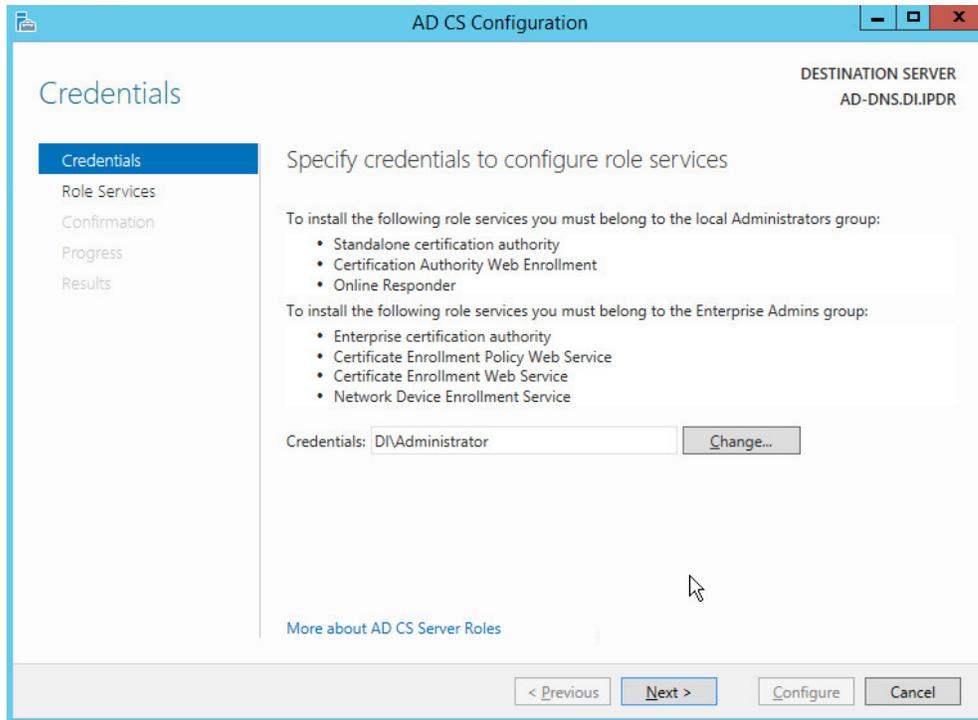
17. Wait for the installation to complete.



18. Click **Close**.

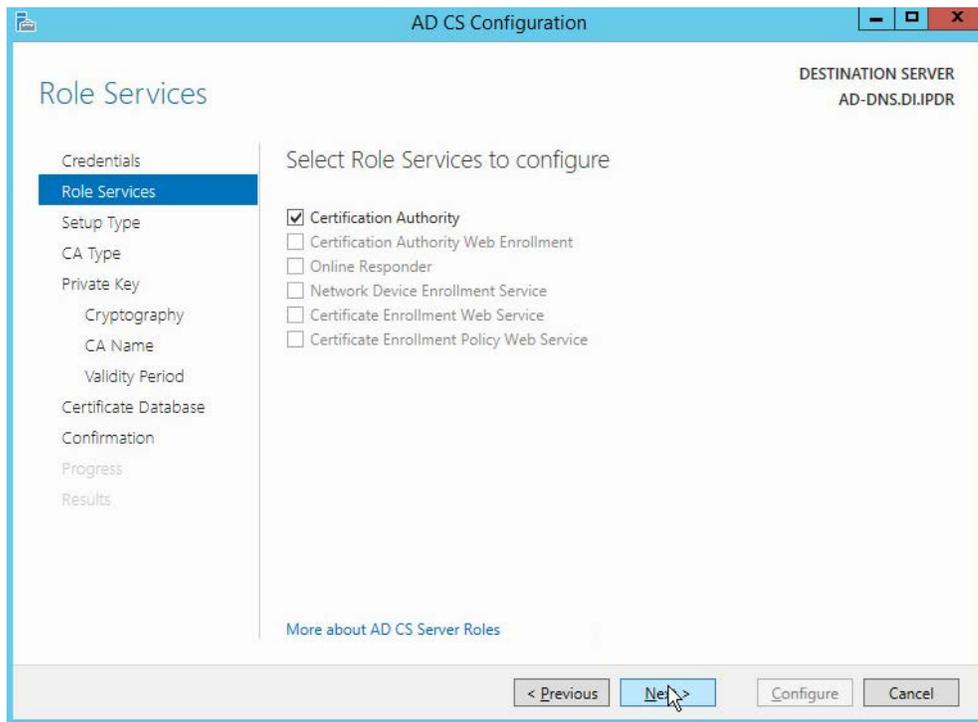


19. Click **Configure Active Directory Certificate Services on the destination server.**



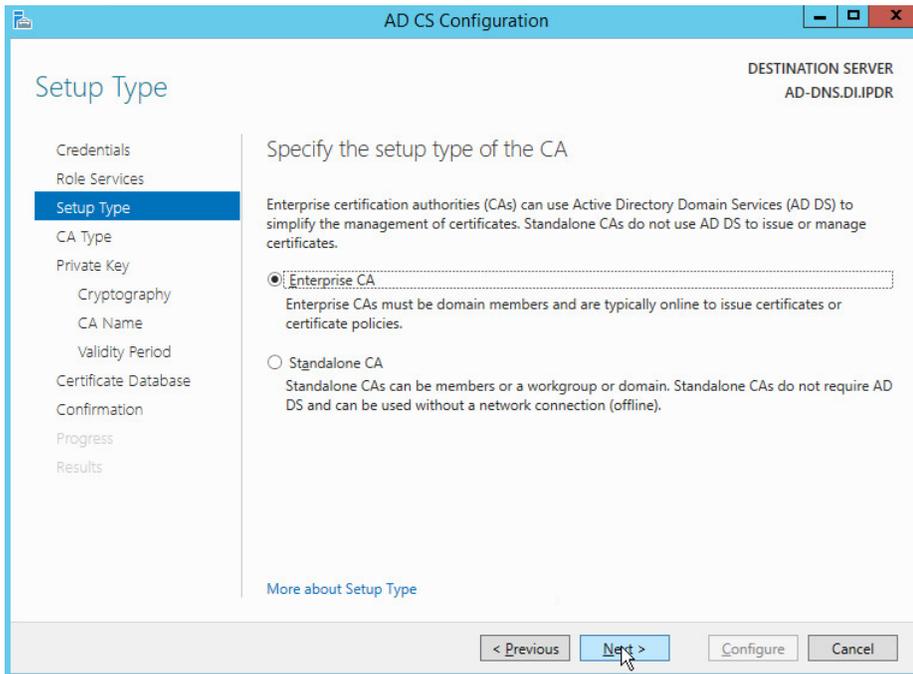
20. Click **Next.**

21. Check the box next to **Certification Authority.**



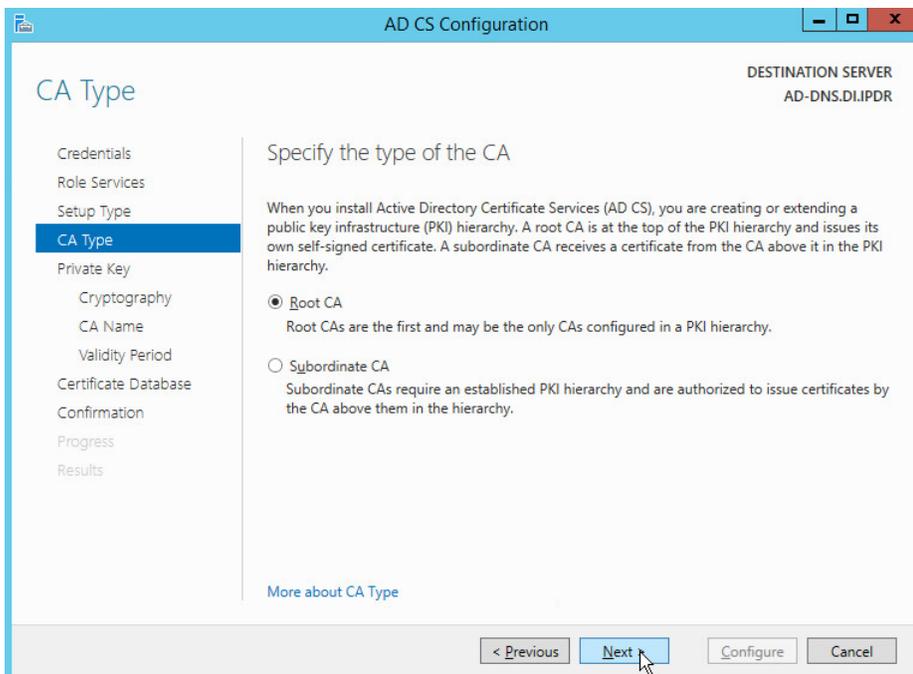
22. Click **Next**.

23. Select **Enterprise CA**.



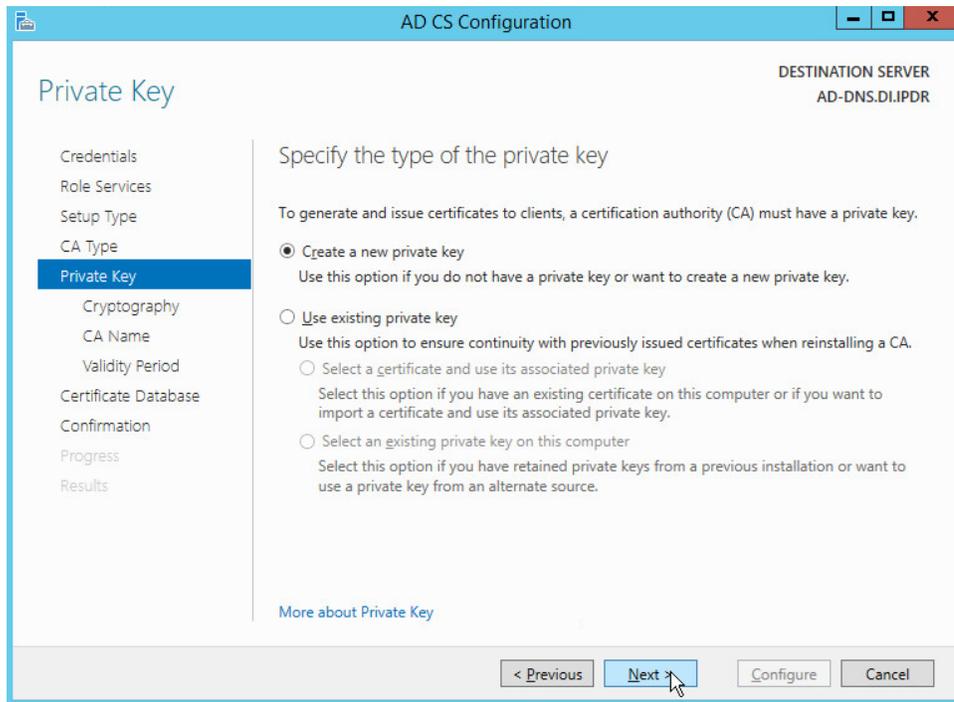
24. Click **Next**.

25. Select **Root CA**.



26. Click **Next**.

27. Select **Create a new private key**.

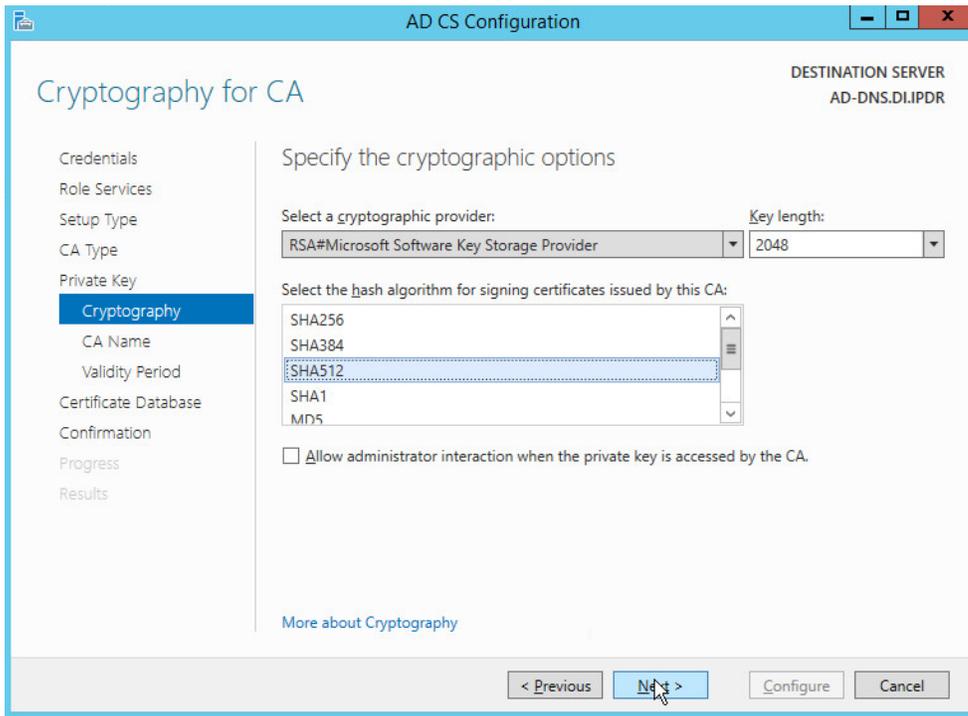


28. Click **Next**.

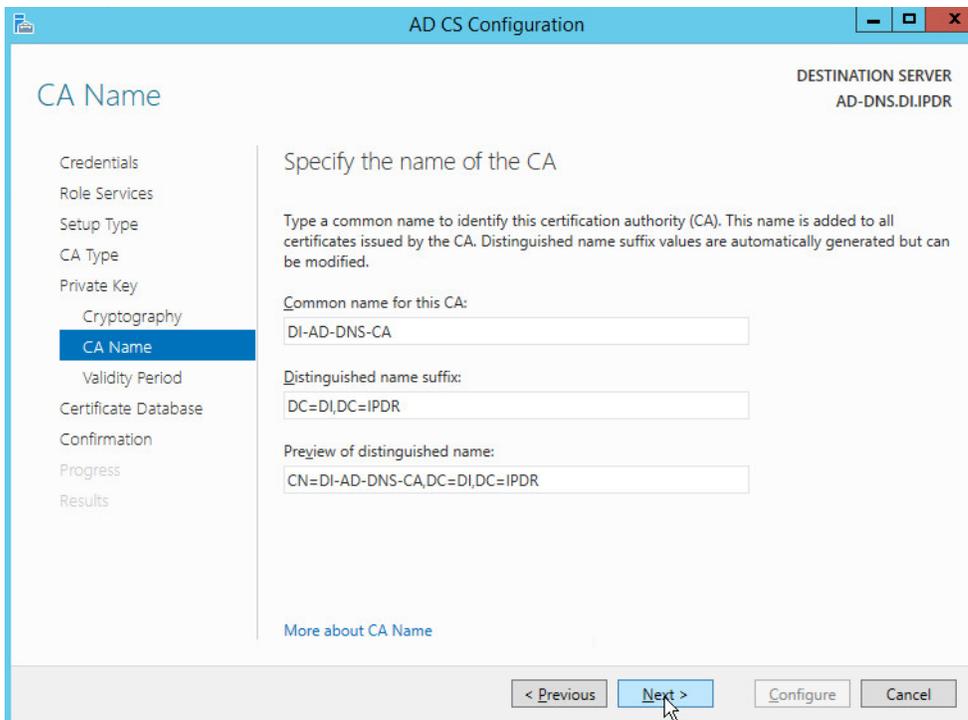
29. Select **RSA#Microsoft Software Key Storage Provider**.

30. Set the **Key length** to **2048**.

31. Select **SHA512** from the list.

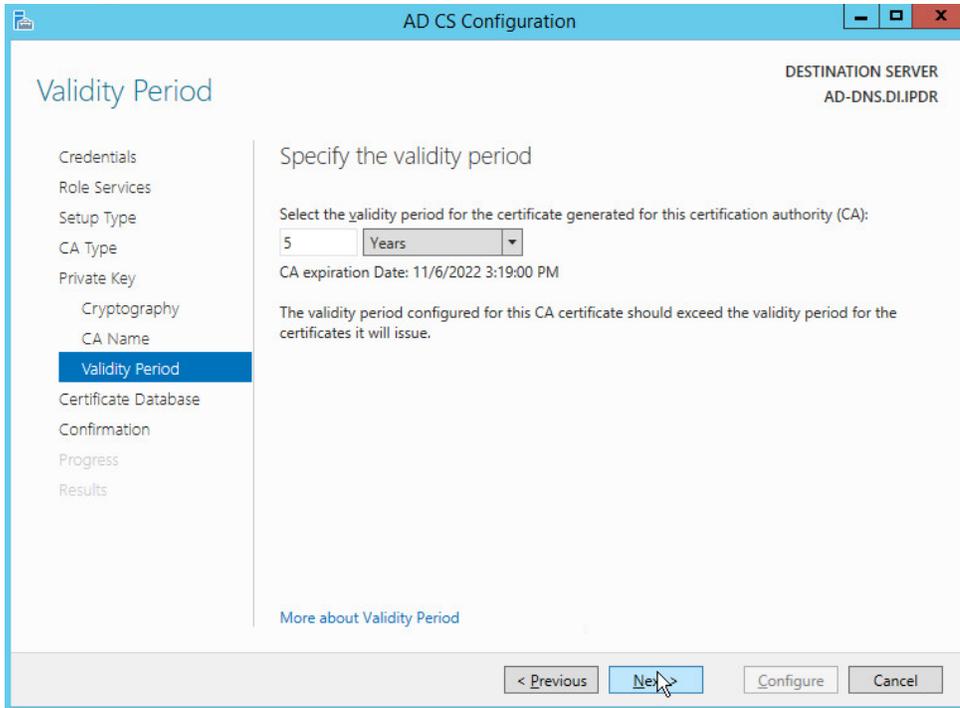


32. Click **Next**.

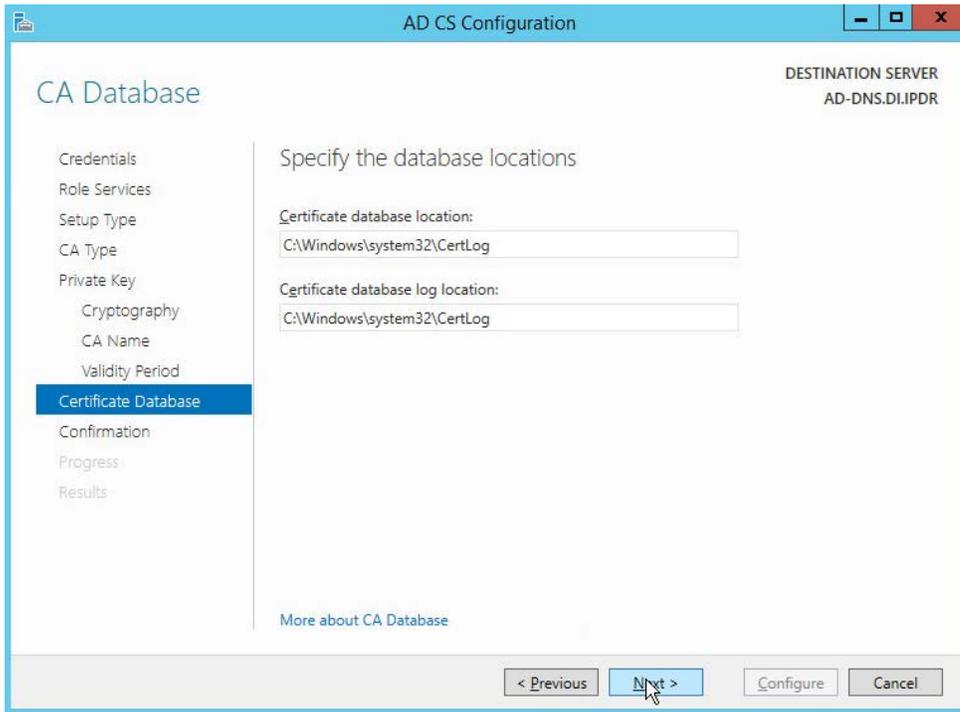


33. Click **Next**.

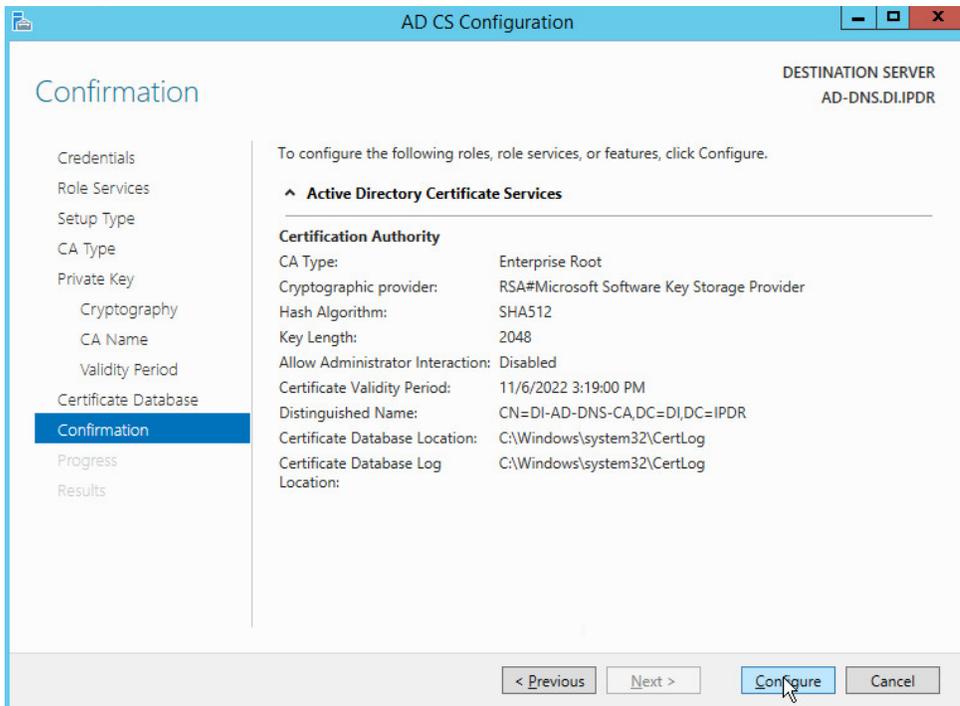
34. Set the time to 5 years.



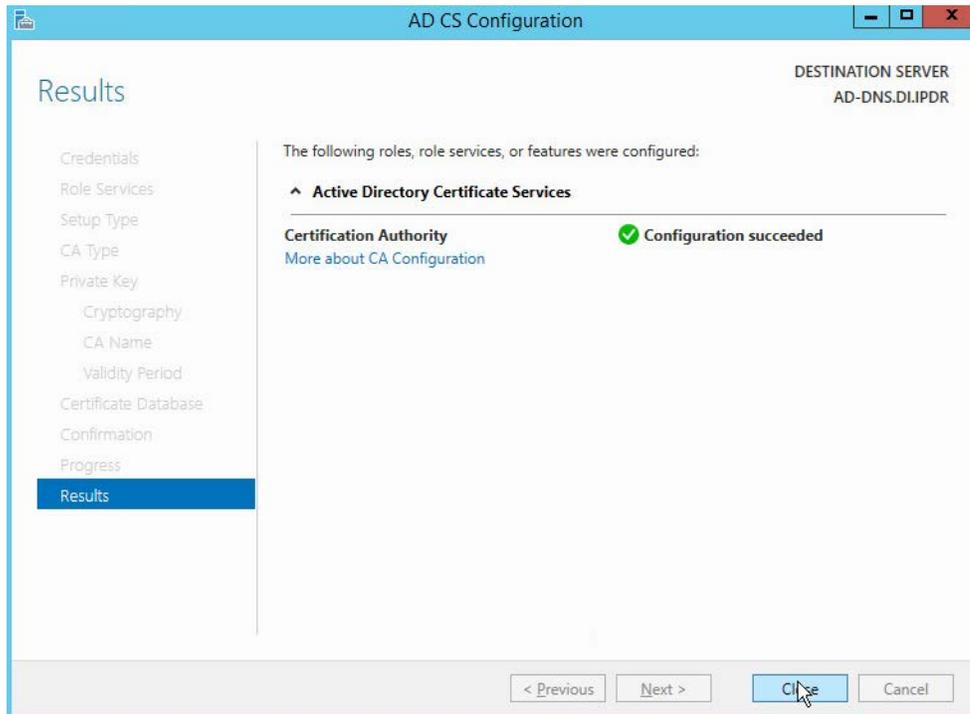
35. Click **Next**.



36. Click **Next**.



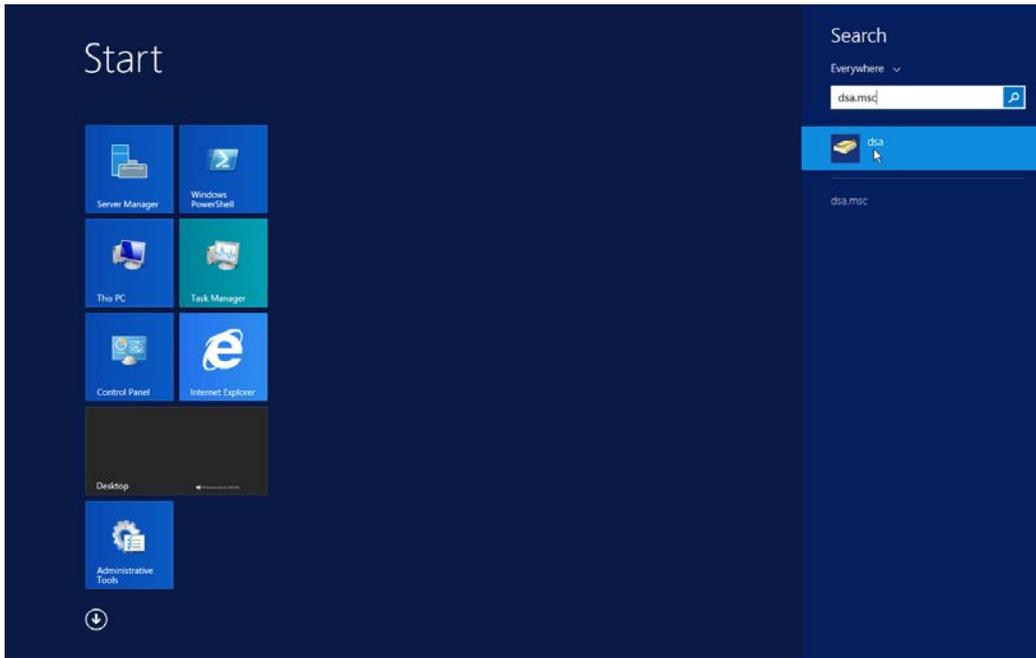
37. Click **Configure**.



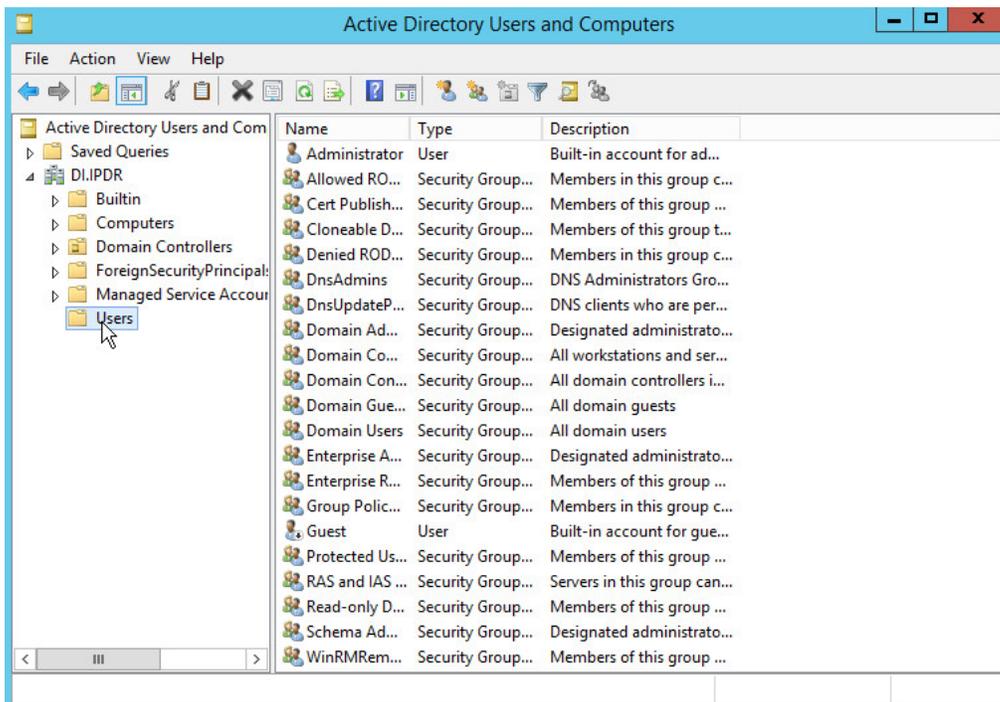
38. Click **Close**.

2.1.3 Configure Account to Add Computers to Domain

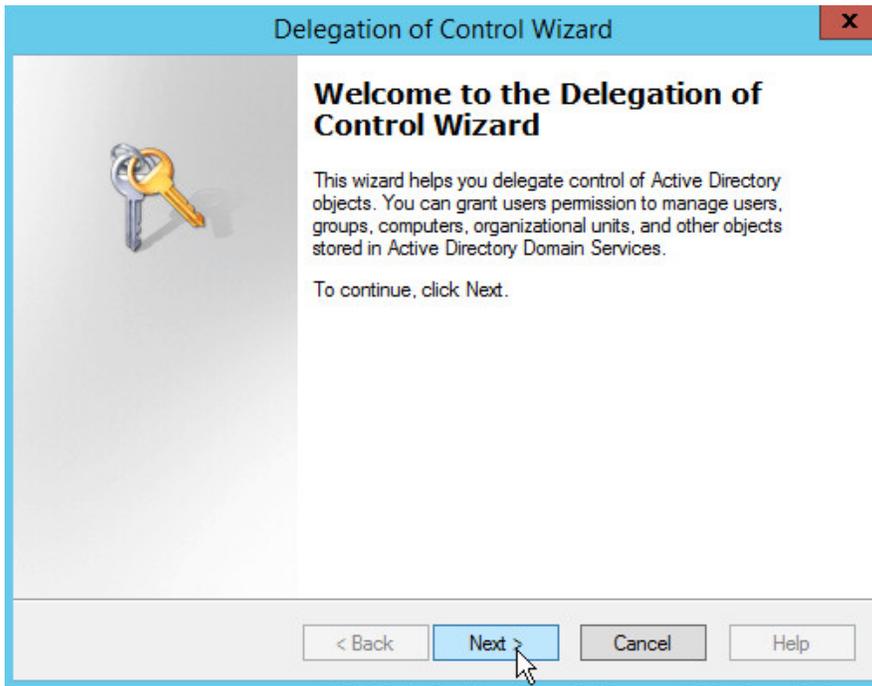
1. Open the Start menu.
2. Enter **dsa.msc** and run the program.



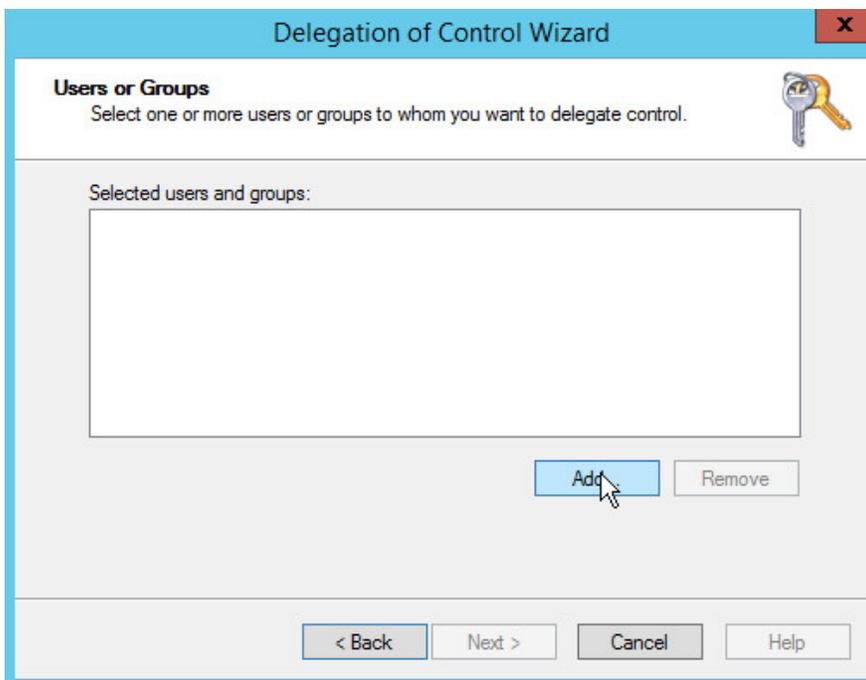
3. Right-click on **Users** in the left panel.



4. Click **Delegate Control**.

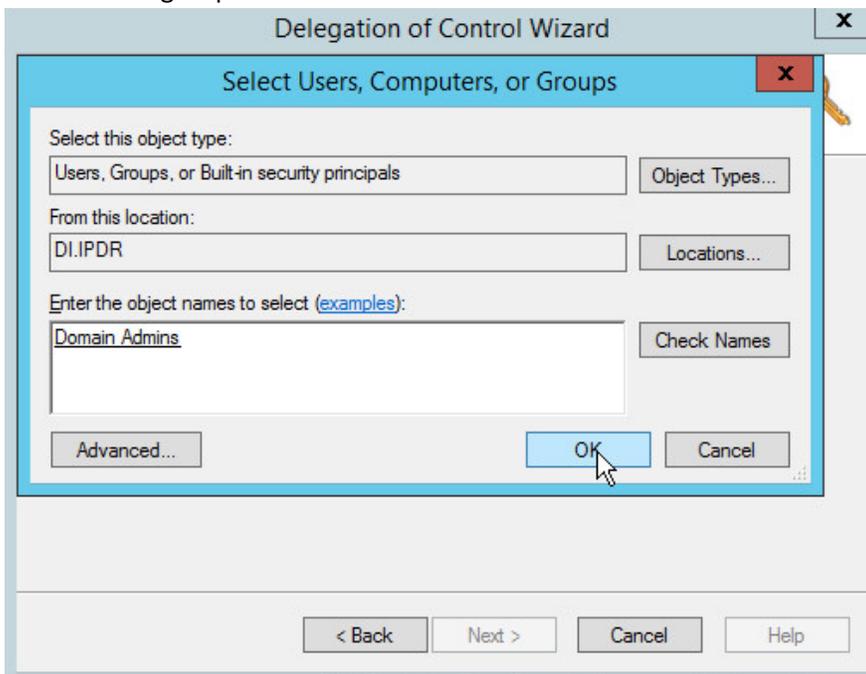


5. Click **Next**.

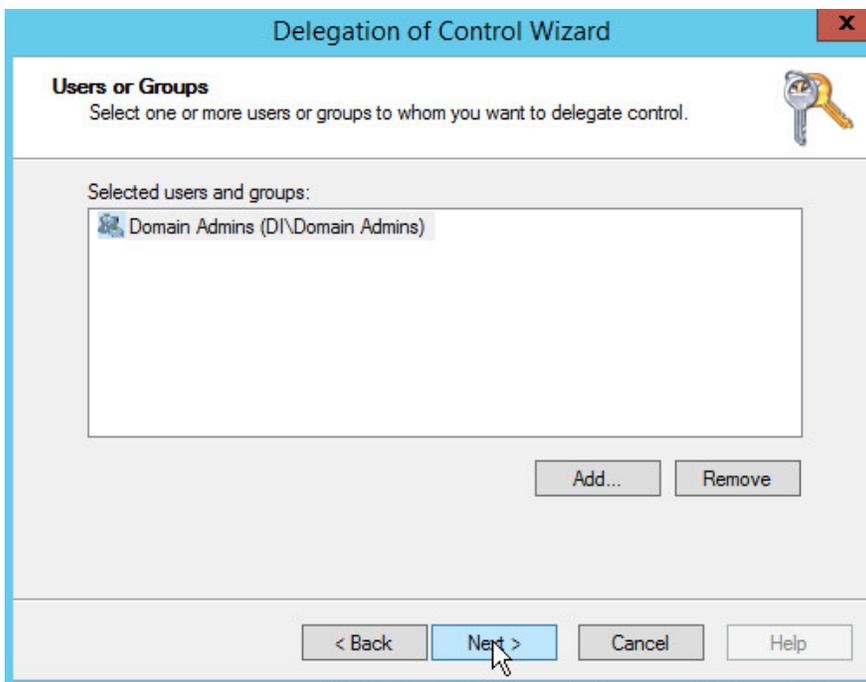


6. Click **Add** to select users or groups.

7. Add users or groups.

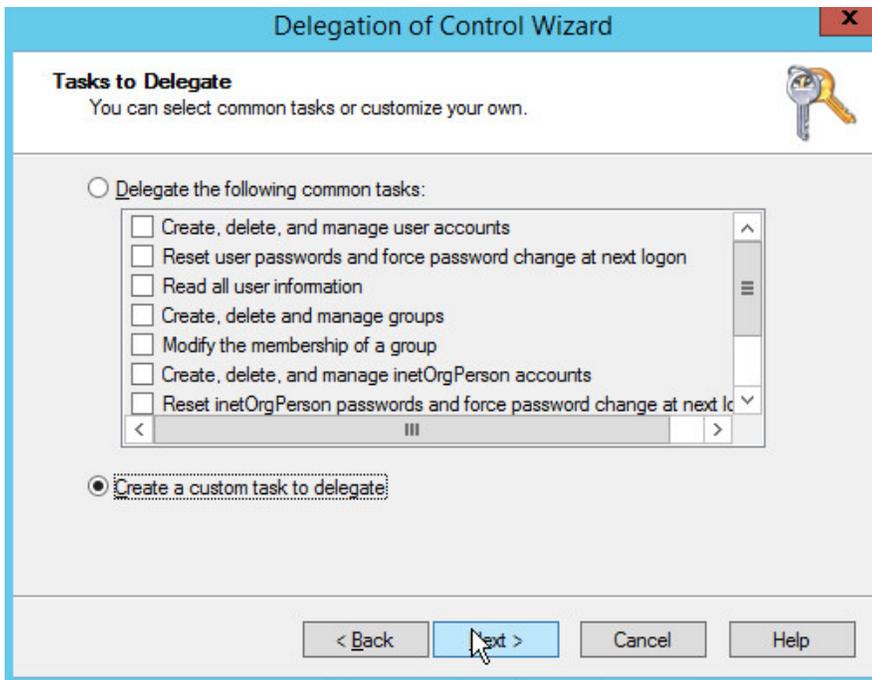


8. Click **OK**.



9. Click **Next**.

10. Choose **Create a custom task to delegate**.



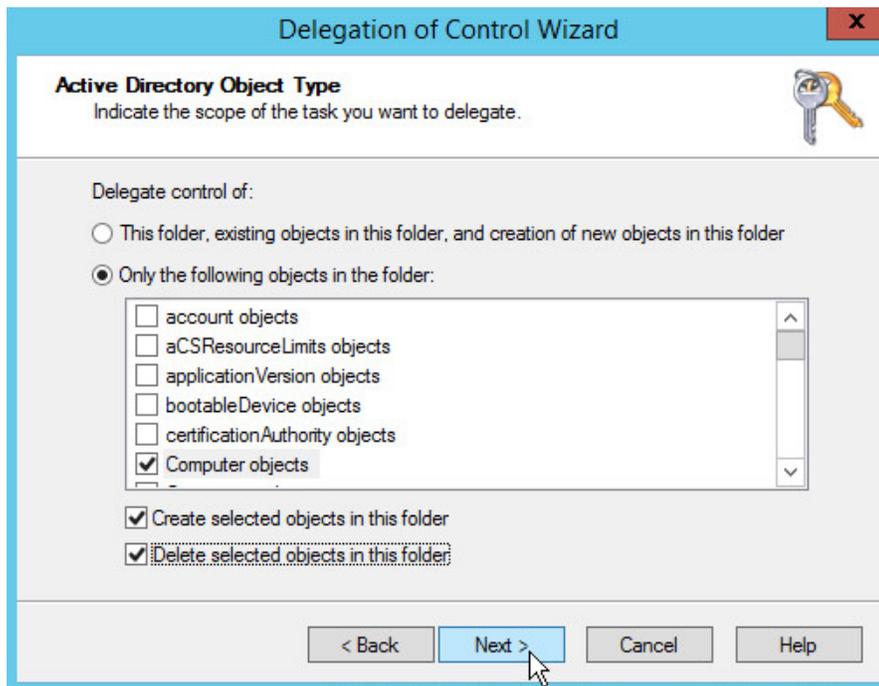
11. Click **Next**.

12. Choose **Only the following objects in the folder**.

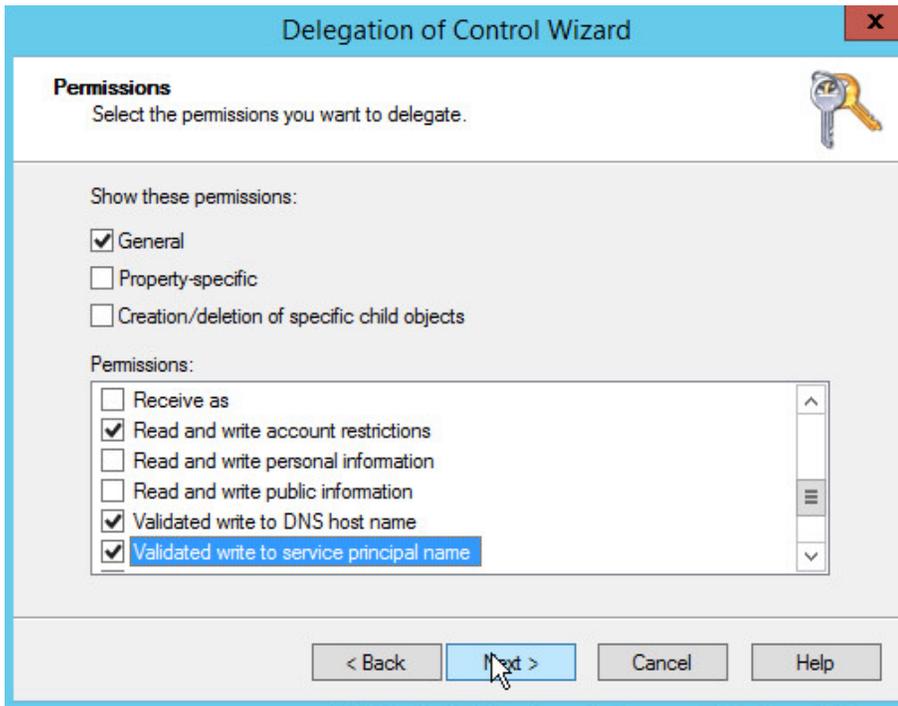
13. Check the box next to **Computer objects**.

14. Check the box next to **Create selected objects in this folder**.

15. Check the box next to **Delete selected objects in this folder**.



16. Click **Next**.
17. Check the boxes next to **Reset password**, **Read and write account restrictions**, **Validated write to DNS host name**, and **Validated write to service principal name**.



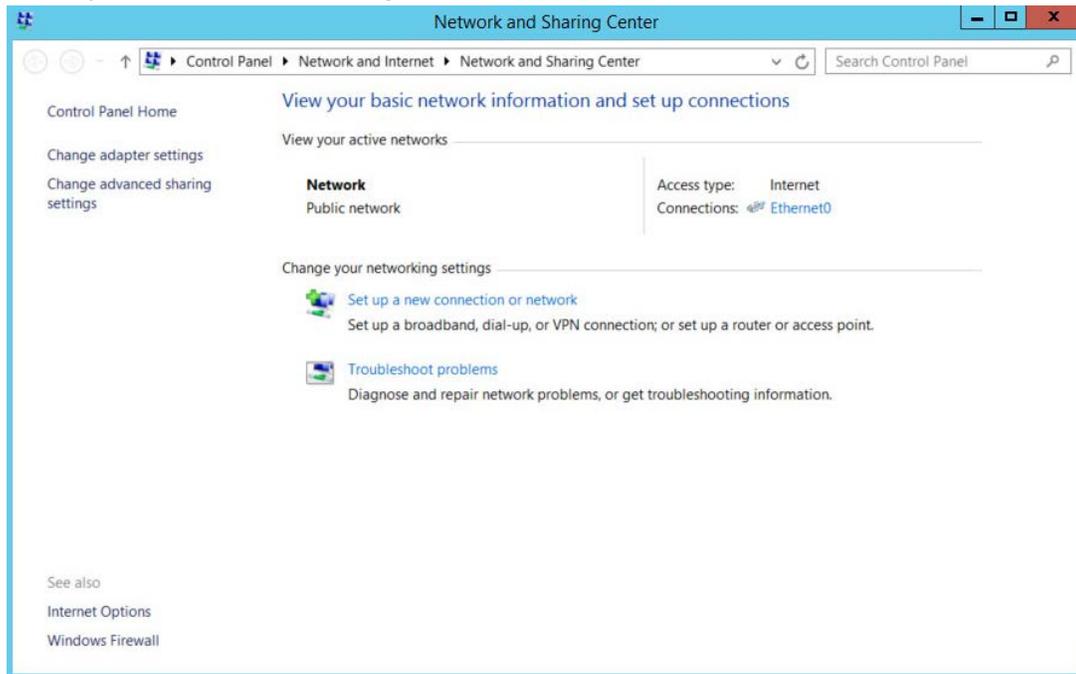
18. Click **Next**.



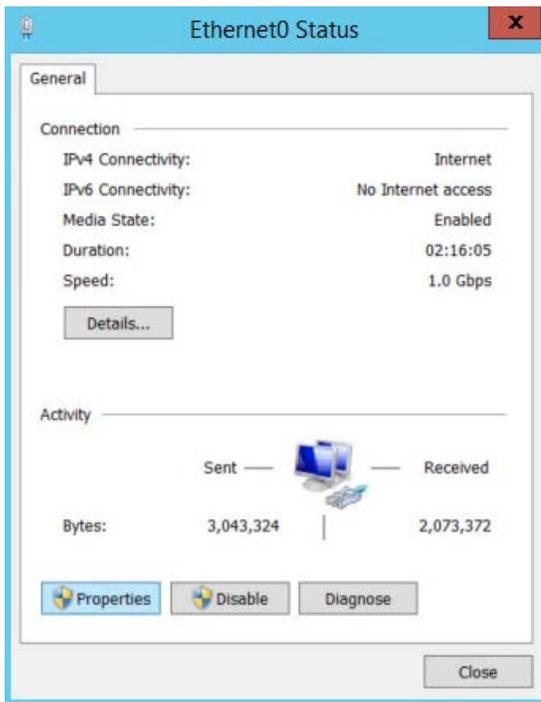
19. Click **Finish**.

2.1.4 Adding Machines to the Domain

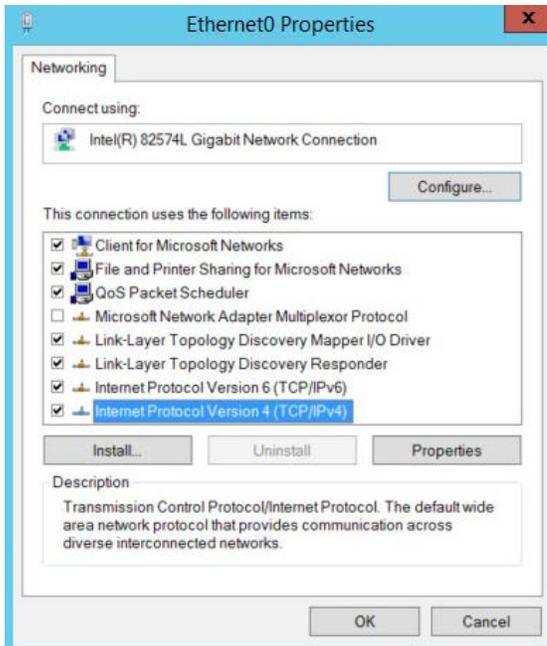
1. Right-click the network icon in the task bar on a computer that you wish to add to the domain.
2. Click **Open Network and Sharing Center**.



3. Click the name of the internet adapter.



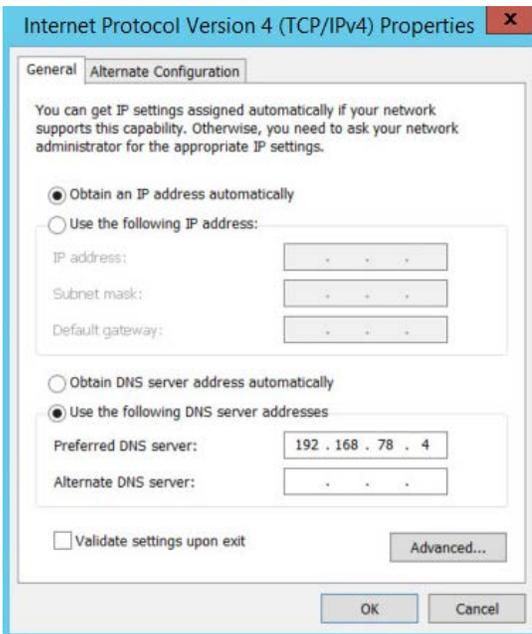
4. Click **Properties**.



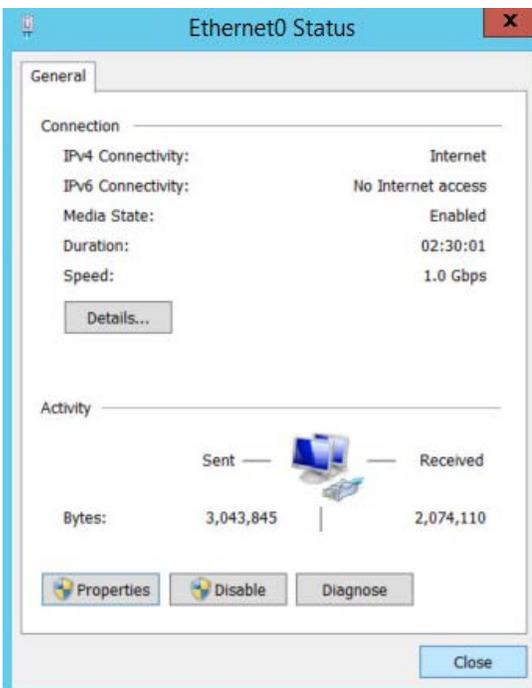
5. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

6. Select **Use the following DNS server addresses**.

- 7. Enter the **IP address** of the DNS server.

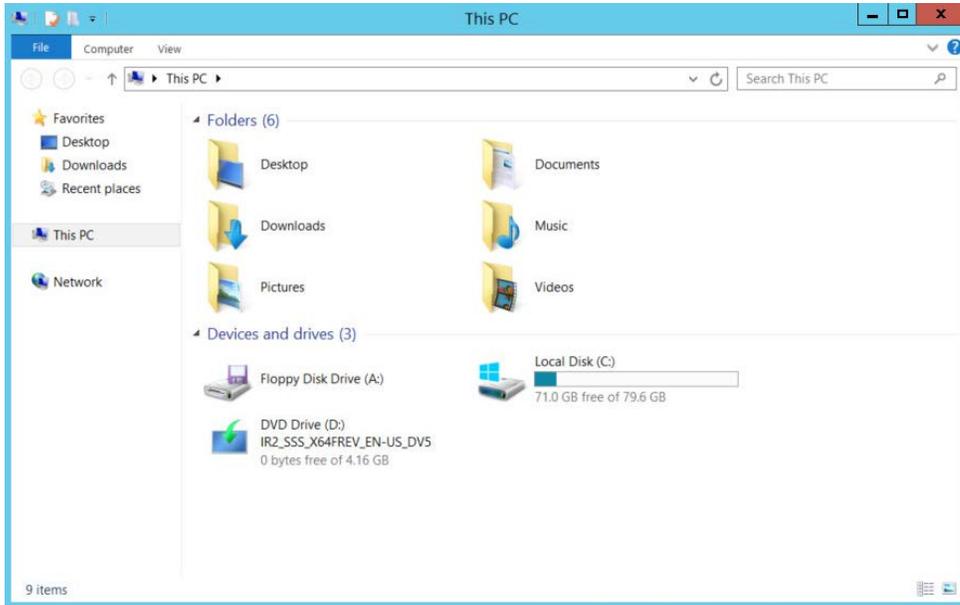


- 8. Click **OK**.
- 9. Click **OK**.

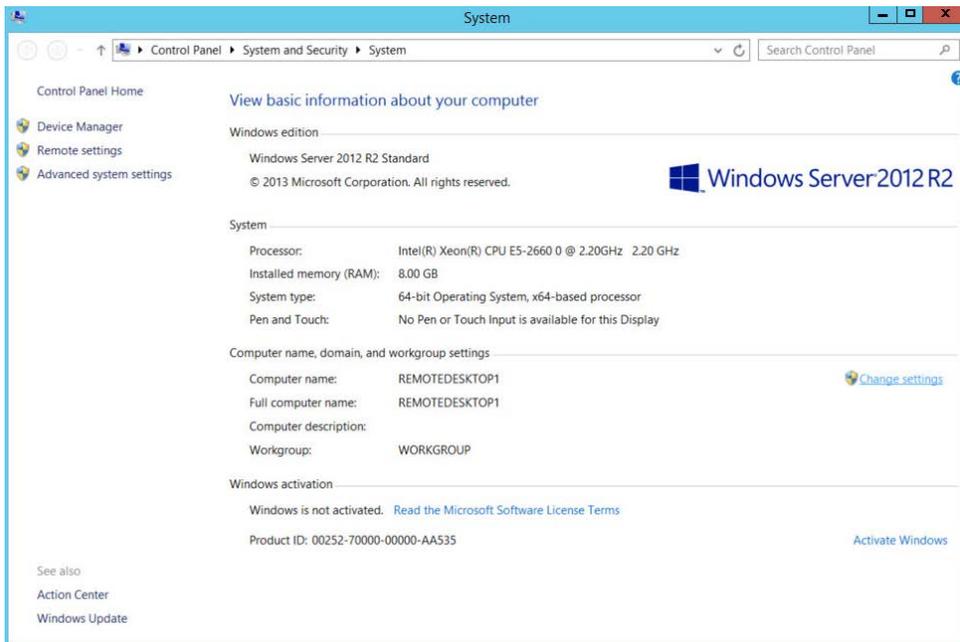


- 10. Click **Close**.

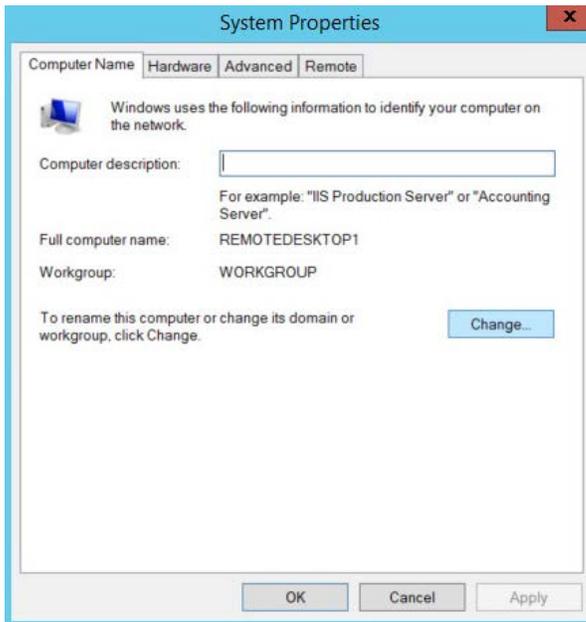
11. Navigate to **This PC**.



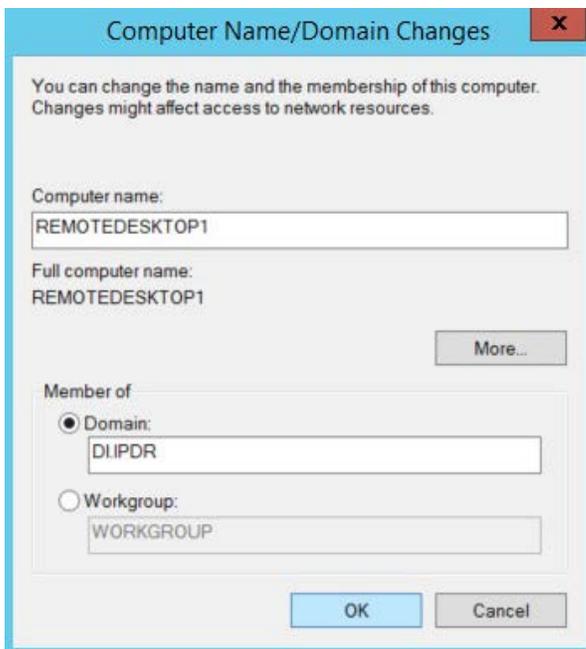
12. Right-click in the window and click **Properties**.



13. Click **Change Settings**.



14. Click **Change**.
15. Select **Domain**.
16. Enter the domain.

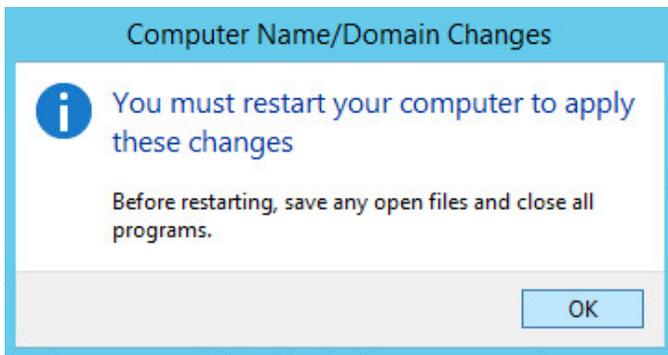


17. Click **OK**.

18. Enter the **username** and **password** of an account with privileges to add computers to the domain.



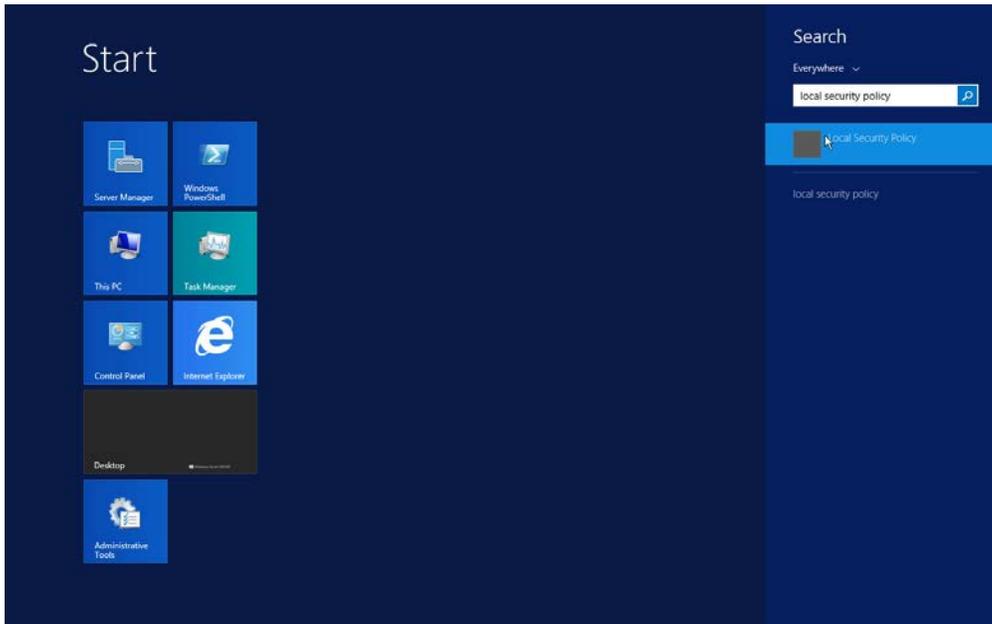
19. Click **OK**.



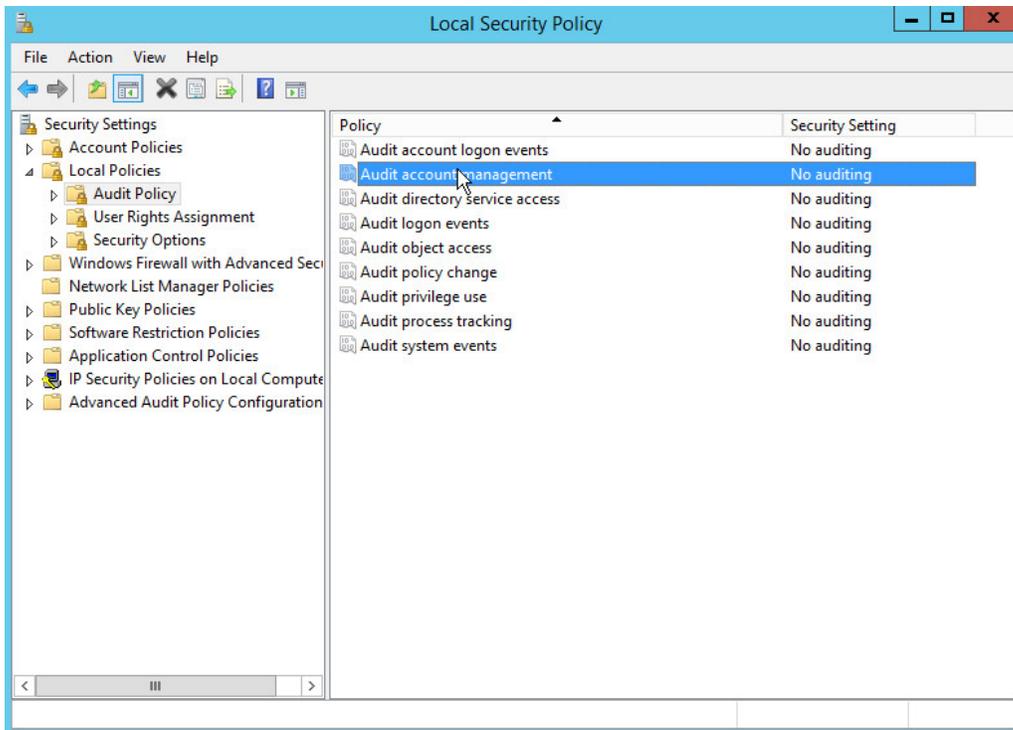
20. Click **OK** when prompted to restart the computer.

2.1.5 Configure Active Directory to Audit Account Activity

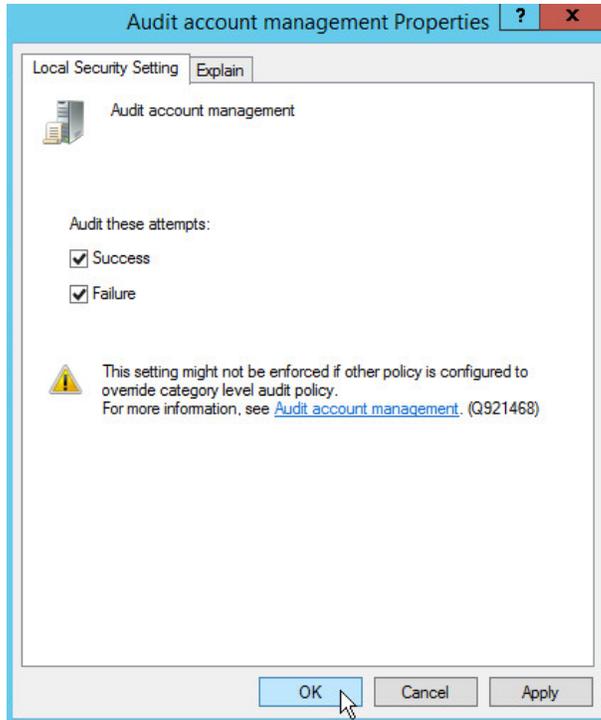
1. Open the Start menu.



2. Enter "Local Security Policy" in the search bar and open the program.
3. Navigate to **Local Policies > Audit Policy**.
4. Right-click **Audit account management**.



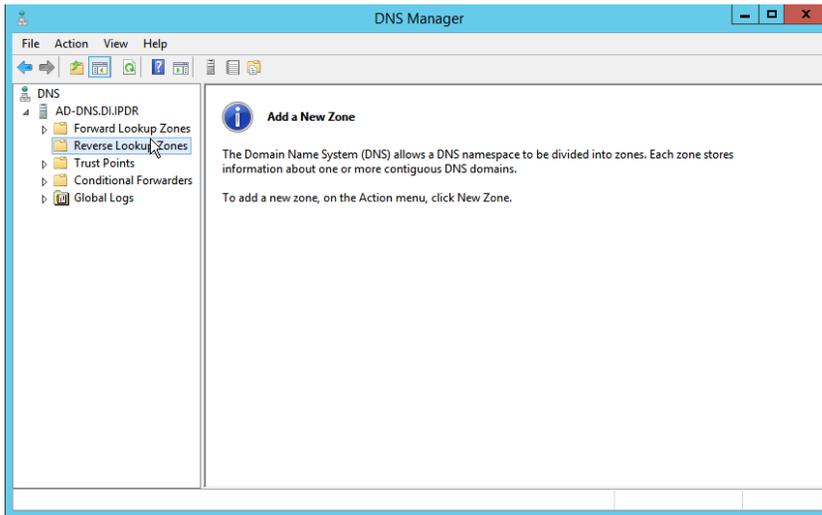
5. Click **Properties**.
6. Check the boxes next to **Success** and **Failure**.



7. Click **OK**.

2.1.6 Configure Reverse Lookup Zones

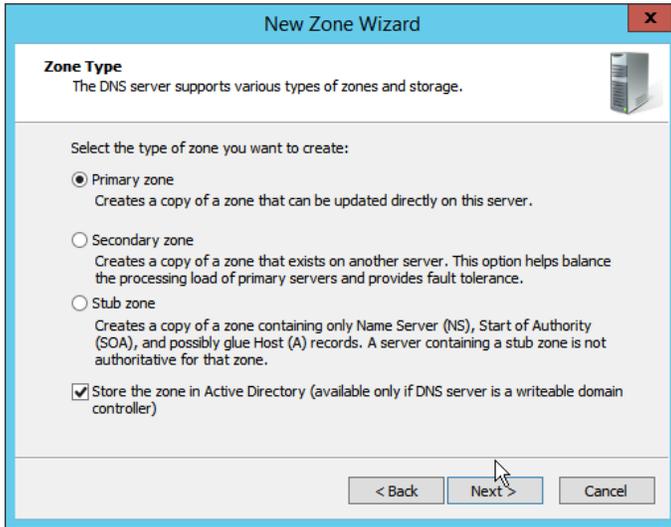
1. Open **DNS Manager** by right-clicking the DNS server in **Server Manager**.
2. Click **Reverse Lookup Zones**.



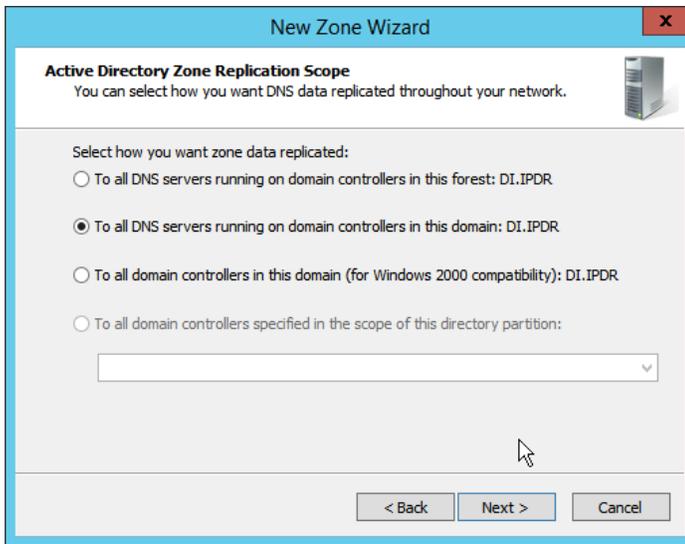
3. Click **Action > New Zone**.



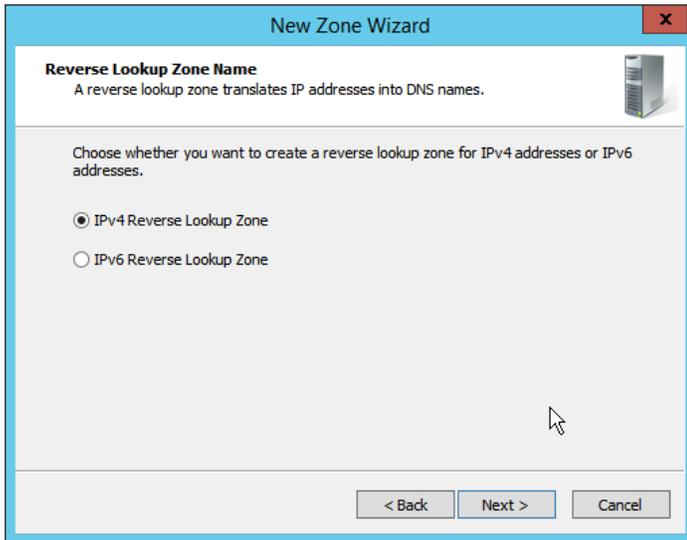
4. Click **Next**.



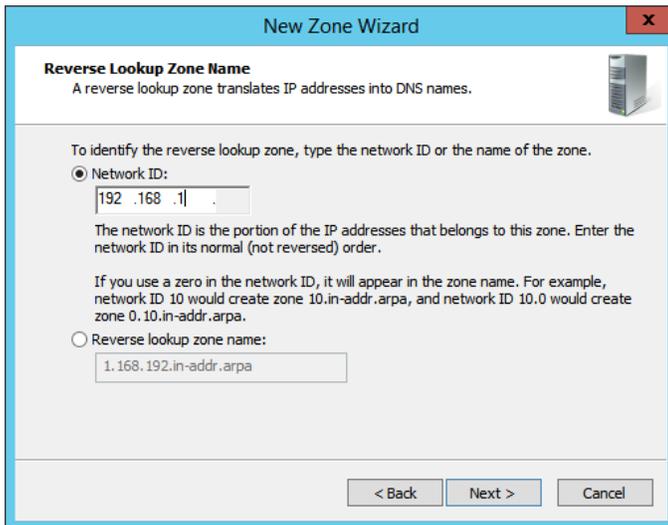
5. Click **Next**.



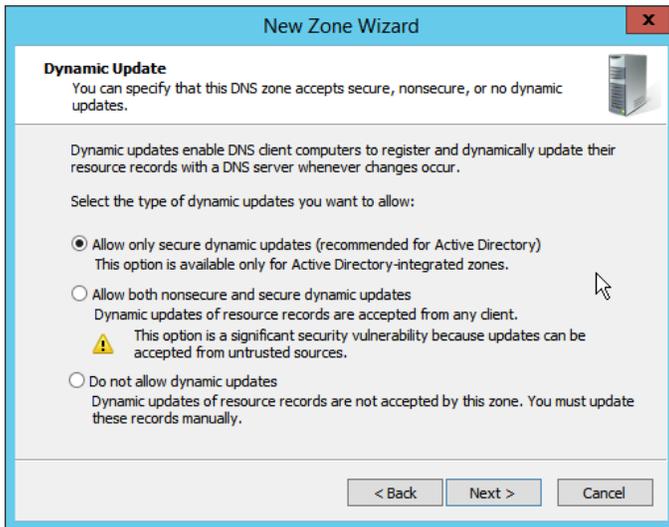
6. Click **Next**.



7. Click **Next**.
8. Enter the first three parts of the IP address of the Active Directory (AD)/DNS server (for example, 192.168.1).



9. Click **Next**.

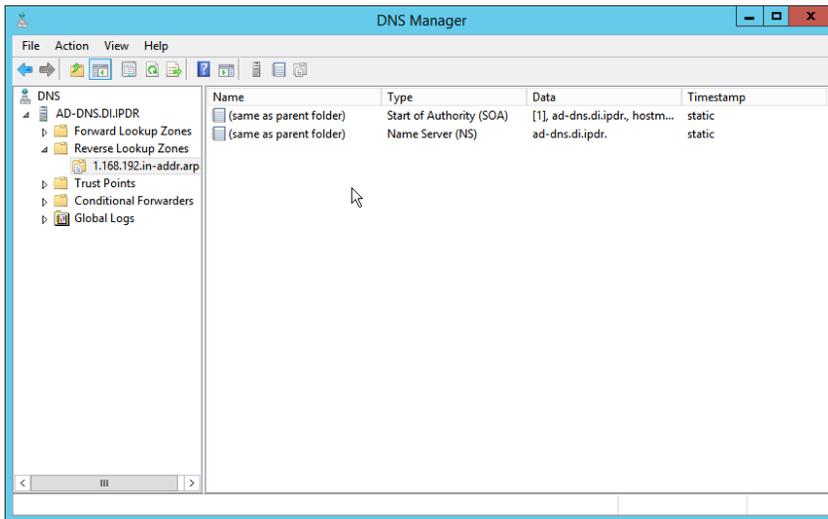


10. Click **Next**.

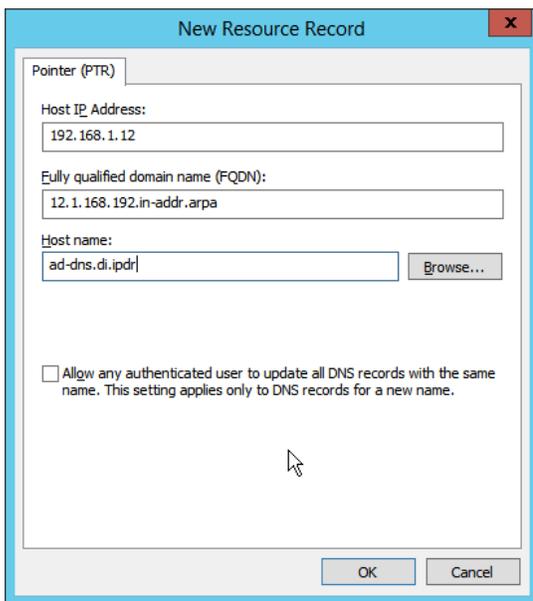


11. Click **Finish**.

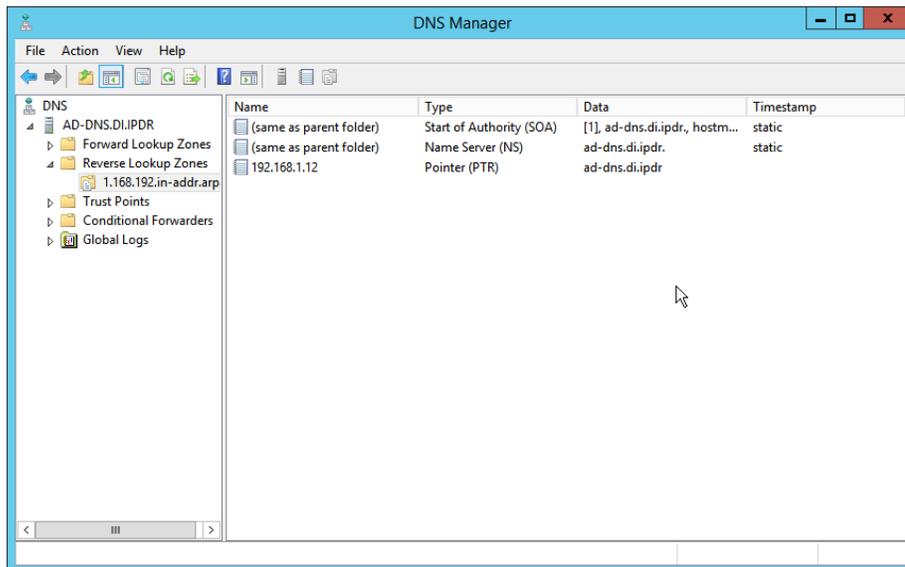
12. Click on the newly created reverse lookup zone.



- 13. Right-click in the window and select **New Pointer (PTR)...**
- 14. Enter the **IP address** of the AD/DNS server.
- 15. Enter the **hostname** of the AD/DNS server.



- 16. Click **OK**.

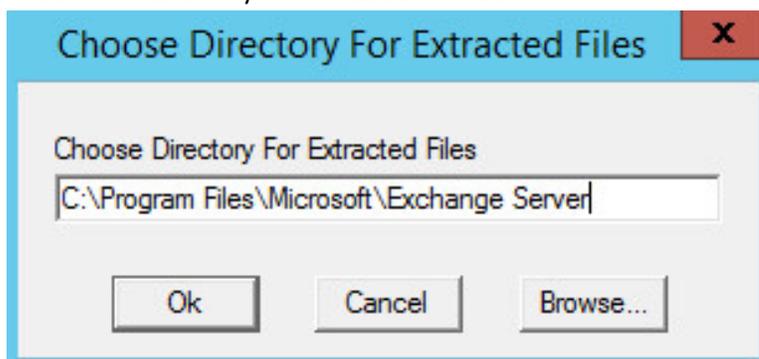


2.2 Microsoft Exchange Server

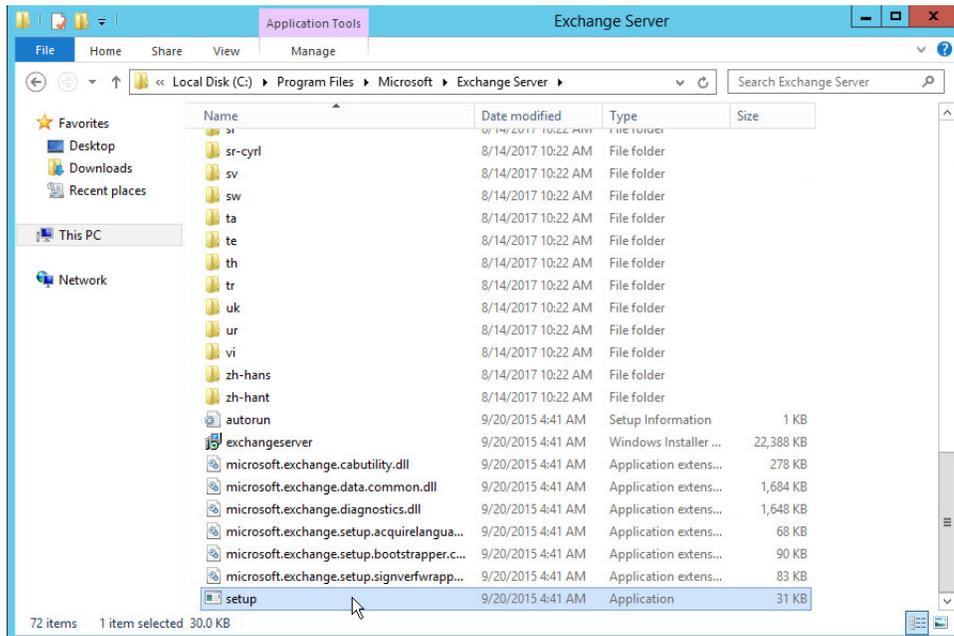
As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

2.2.1 Install Microsoft Exchange

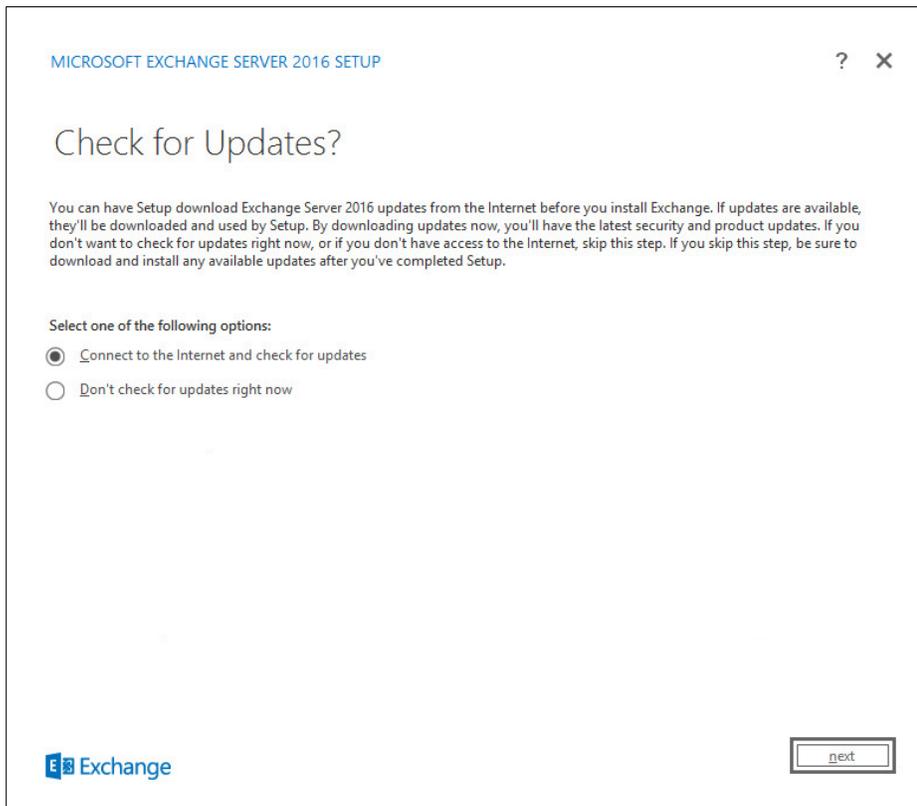
1. Run **Exchange2016-x64.exe**.
2. Choose the directory for the extracted files.



3. Click **OK**.



4. Enter the directory and run **setup.exe**.
5. Select **Connect to the Internet and check for updates**.



6. Click **Next**.
7. Wait for the check to finish.

MICROSOFT EXCHANGE SERVER 2016 SETUP

? X

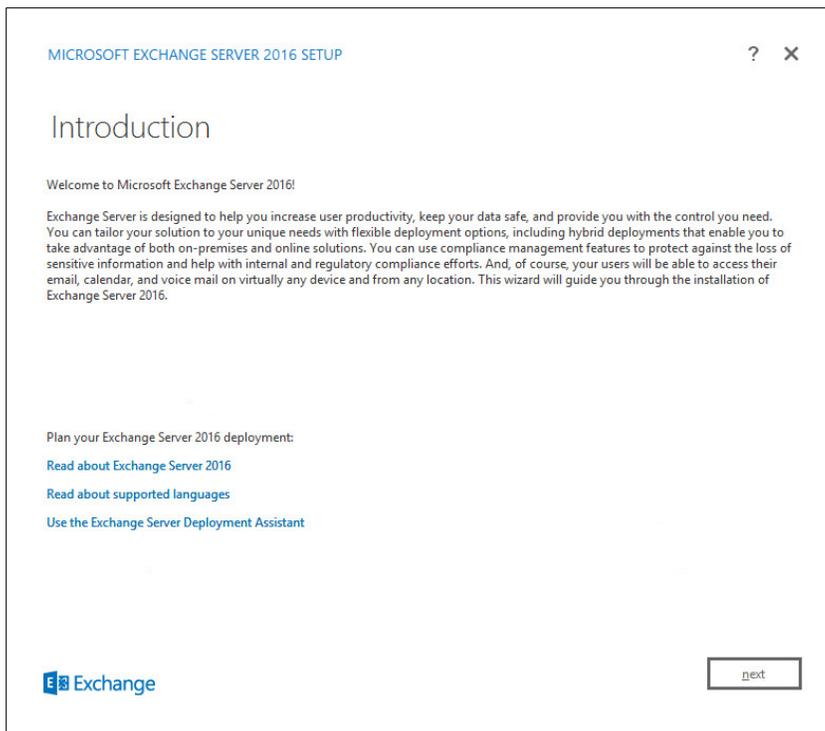
Downloading Updates...

No updates found, click next to continue with setup.

 Exchange

next

8. Click **Next**.
9. Wait for the copying to finish.



10. Click **Next**.
11. Click **I accept the terms in the license agreement**.

License Agreement

Please read and accept the Exchange Server 2016 license agreement.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT EXCHANGE SERVER 2016 STANDARD, ENTERPRISE, TRIAL AND HYBRID

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or the retailer for information about Microsoft's refund policy.

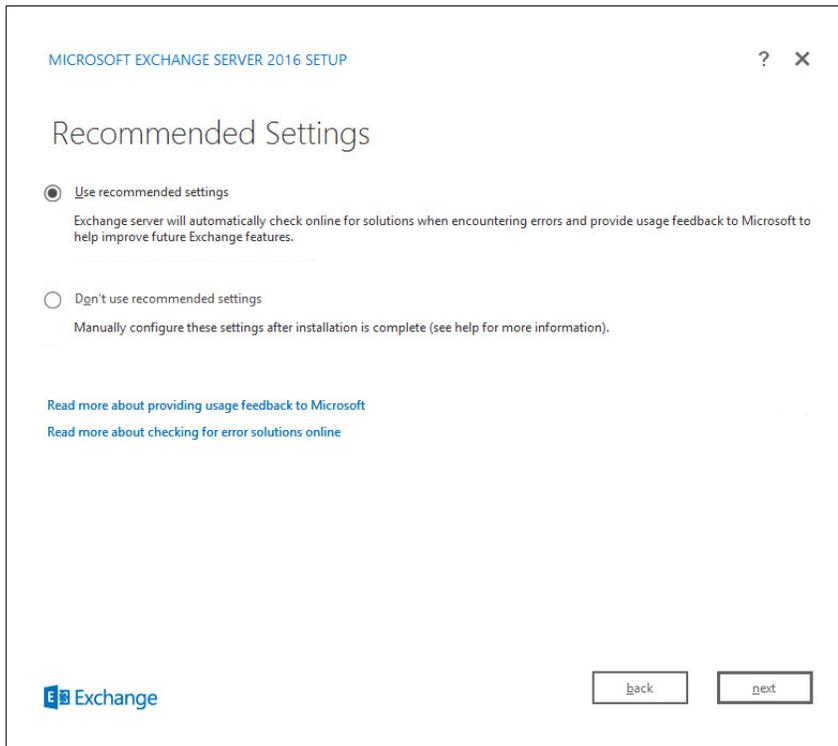
- I accept the terms in the license agreement
- I do not accept the terms in the license agreement.



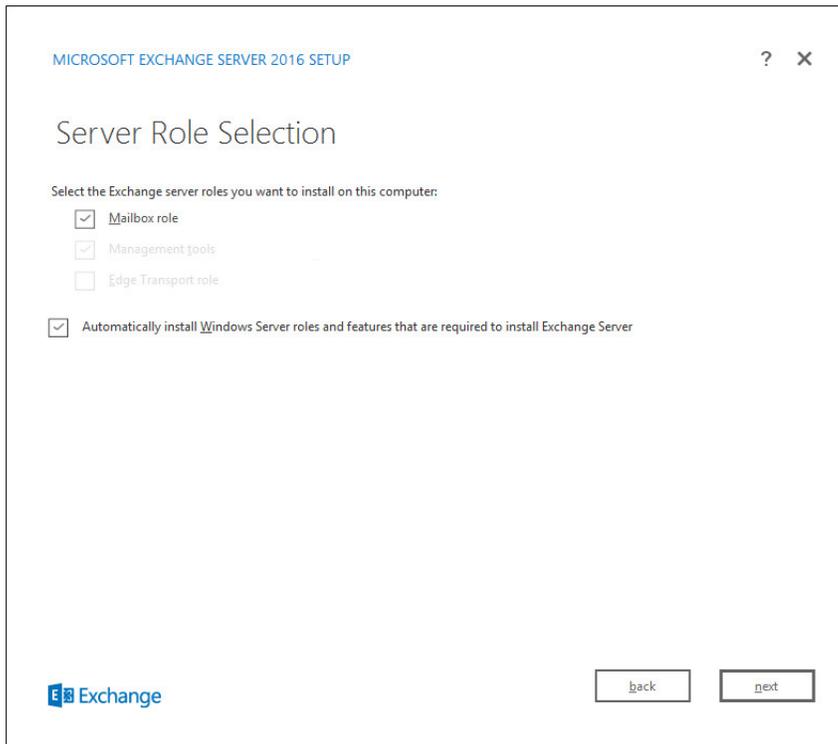
next

12. Click **Next**.

13. Click **Use Recommended Settings**.

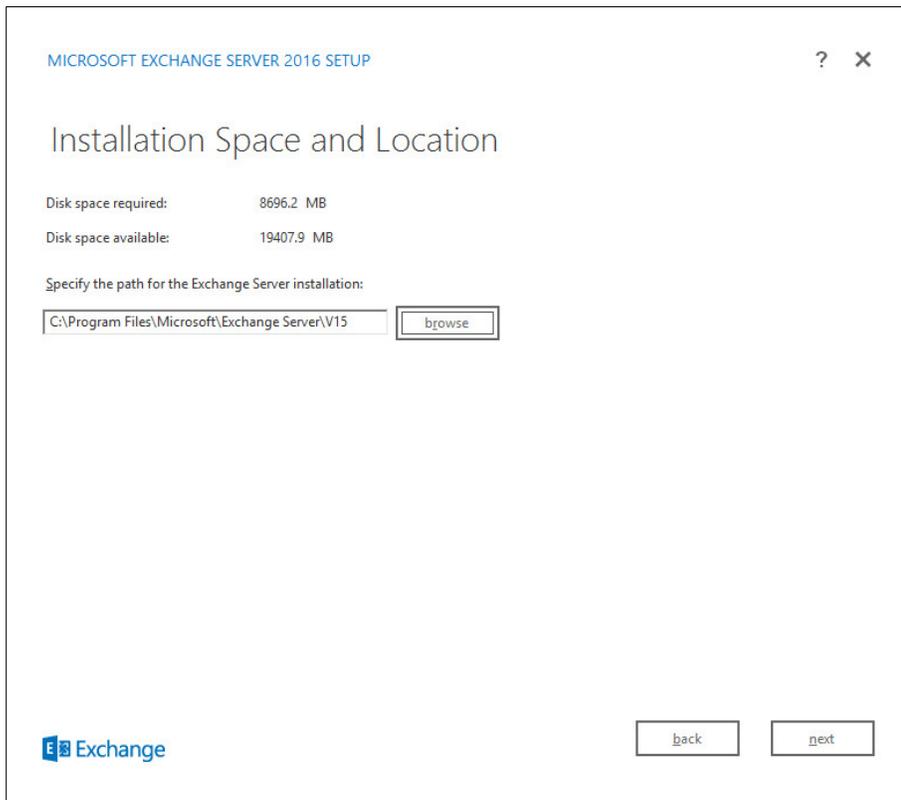


14. Click **Next**.
15. Check **Mailbox role**.
16. Check **Automatically install Windows Server roles and features that are required to install Exchange Server**.



17. Click **Next**.

18. Specify the installation path for MS Exchange.



19. Click **Next**.
20. Specify the name for the Exchange organization, e.g., DI.
21. Decide whether to apply split permissions based on the needs of the enterprise.

Exchange Organization

Specify the name for this Exchange organization:

Apply Active Directory split permissions security model to the Exchange organization

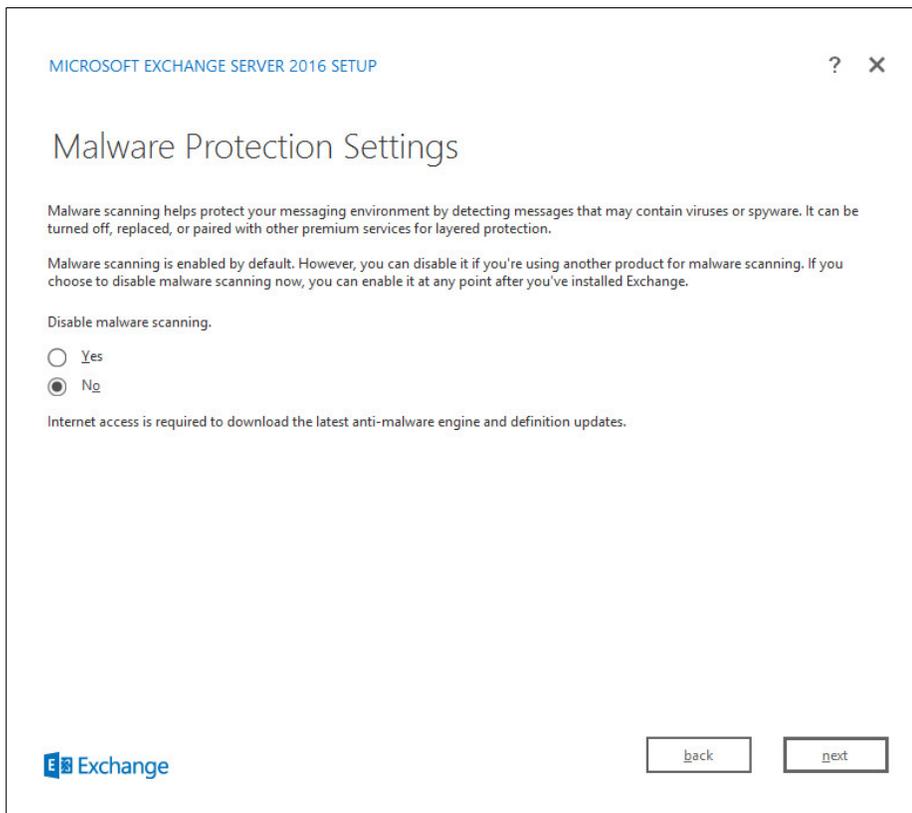
The Active Directory split permissions security model is typically used by large organizations that completely separate the responsibility for the management of Exchange and Active Directory among different groups of people. Applying this security model removes the ability for Exchange servers and administrators to create Active Directory objects such as users, groups, and contacts. The ability to manage non-Exchange attributes on those objects is also removed.

You shouldn't apply this security model if the same person or group manages both Exchange and Active Directory. Click '?' for more information.

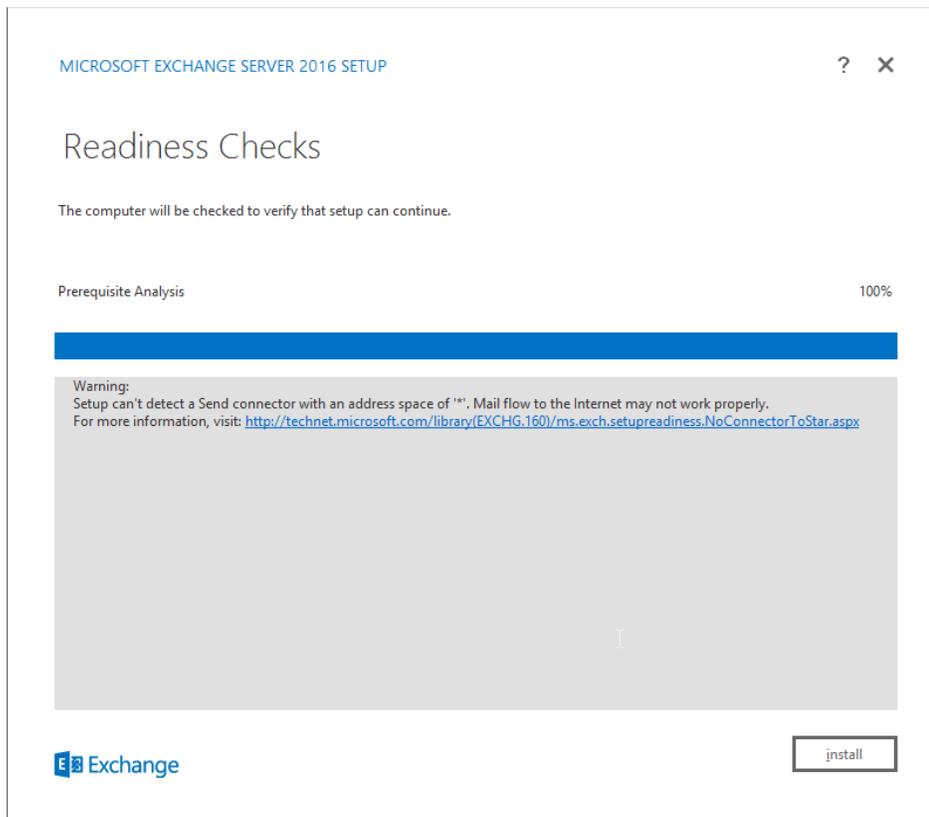


22. Click **Next**.

23. Select **No**.



24. Click **Next**.
25. Install any **prerequisites** listed.
26. If necessary, restart the server and rerun **setup.exe**, following through steps 3–22 again.



27. Click **Install**.

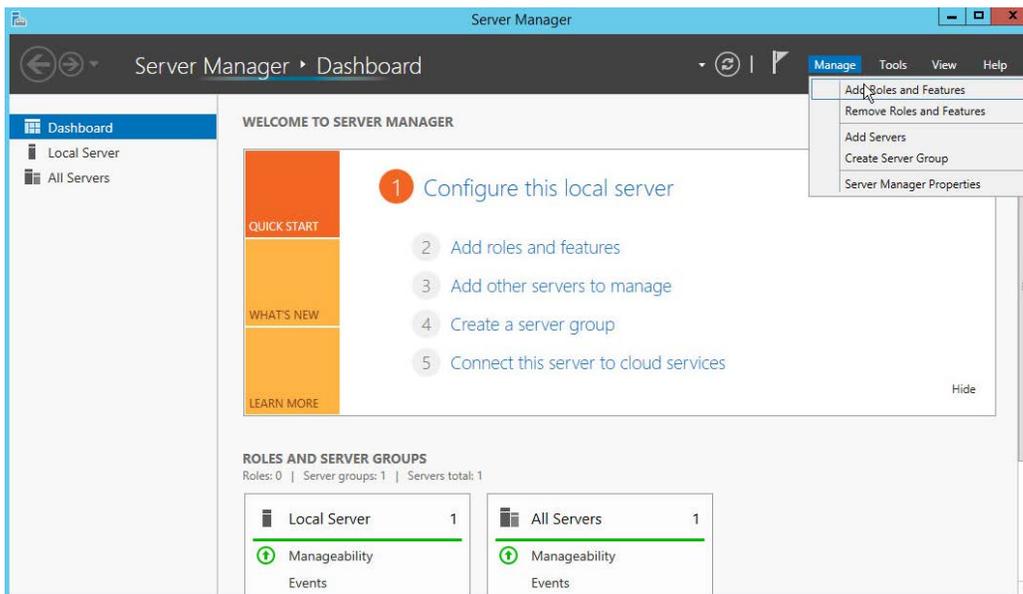
2.3 Windows Server Hyper-V Role

As part of our simulated enterprise, we include a Windows Hyper-V server. This section covers the instructions for installing the Windows Server Hyper-V Role on a Windows Server 2012 R2 machine.

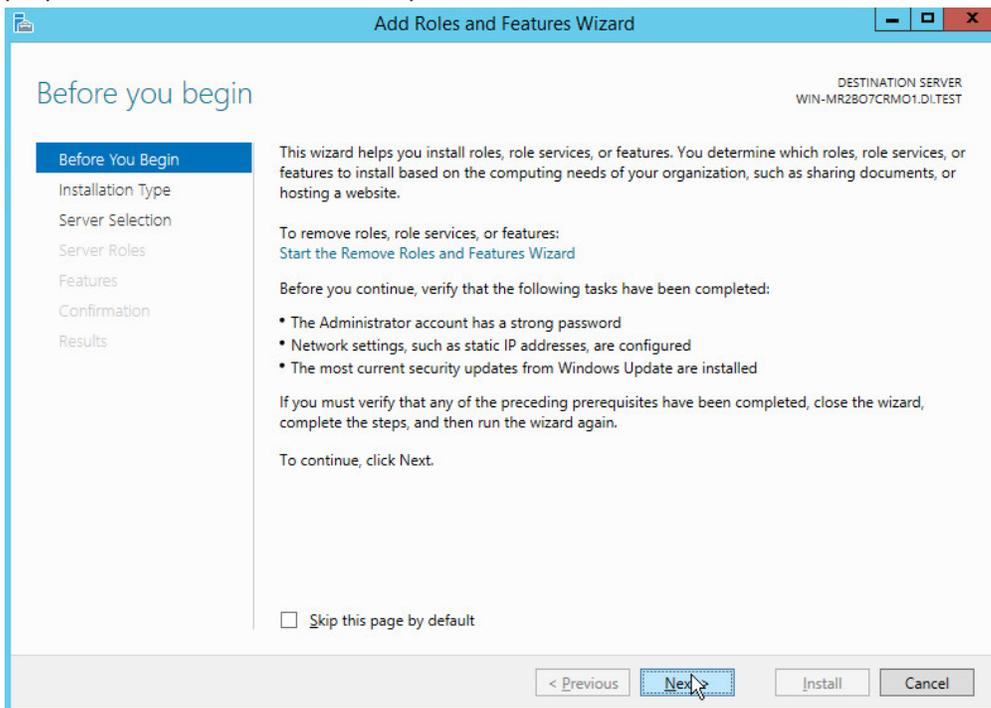
The instructions for enabling the Windows Server Hyper-V Role are retrieved from [https://technet.microsoft.com/en-us/library/hh846766\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx) and are replicated below for preservation and ease of use.

2.3.1 Production Installation

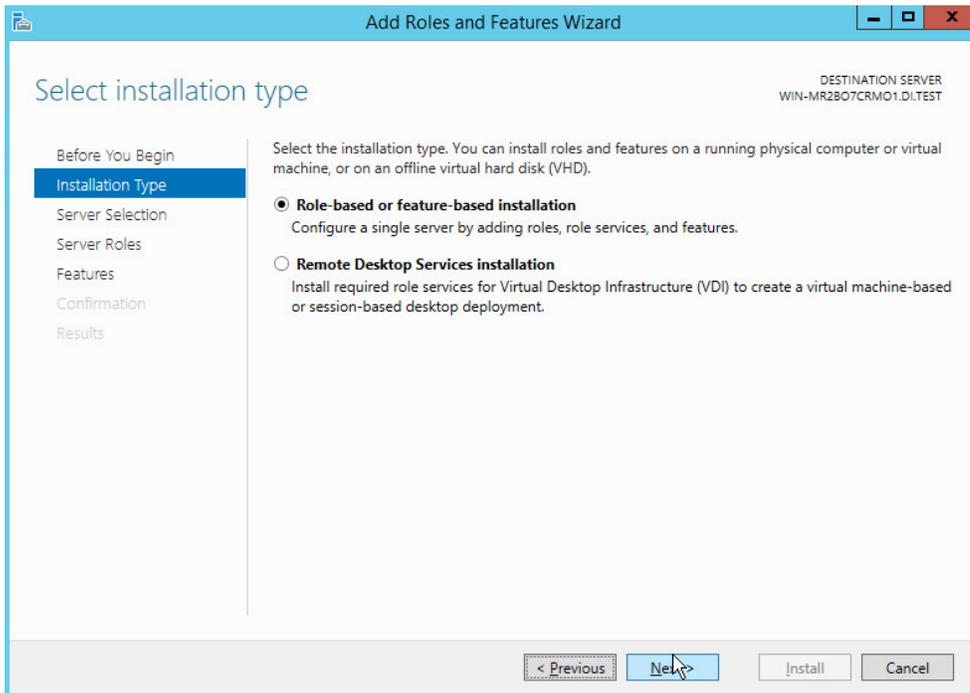
1. In **Server Manager** on the **Manage** menu, click **Add Roles and Features**.



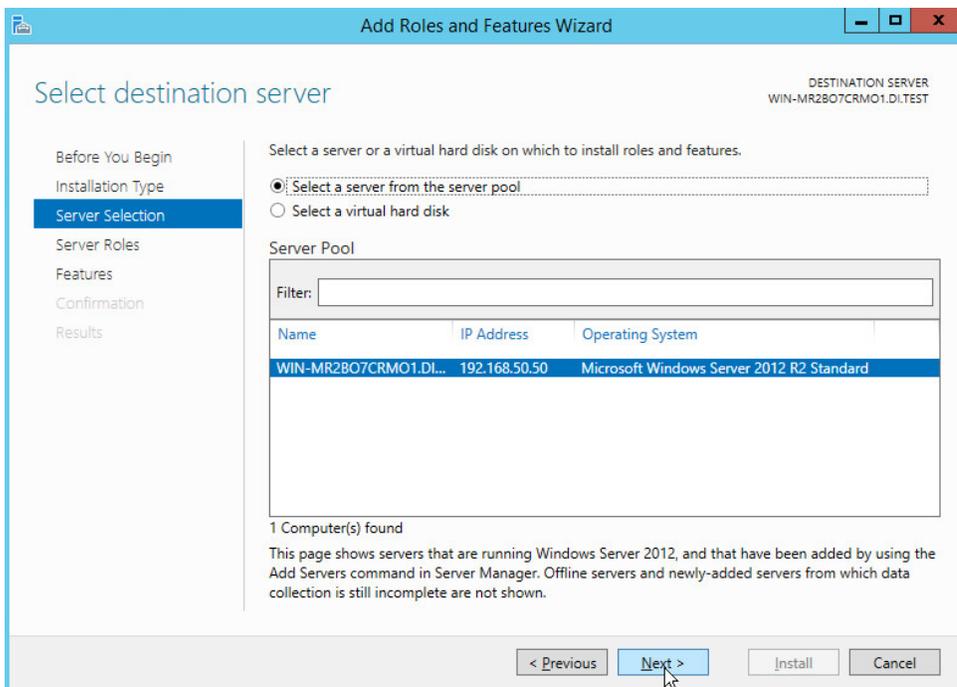
2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.



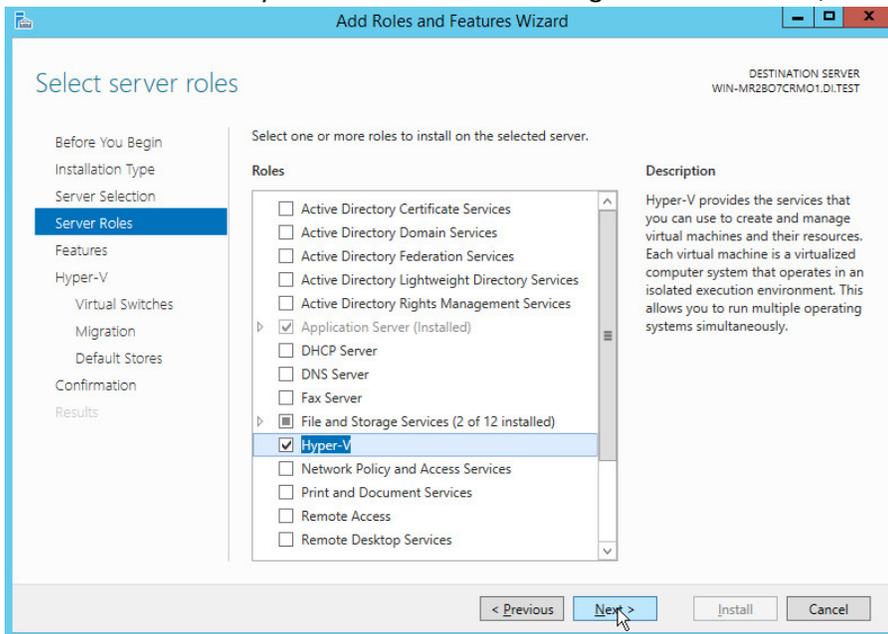
3. Click **Next**.
4. On the **Select installation type** page, select **Role-based or feature-based installation**.



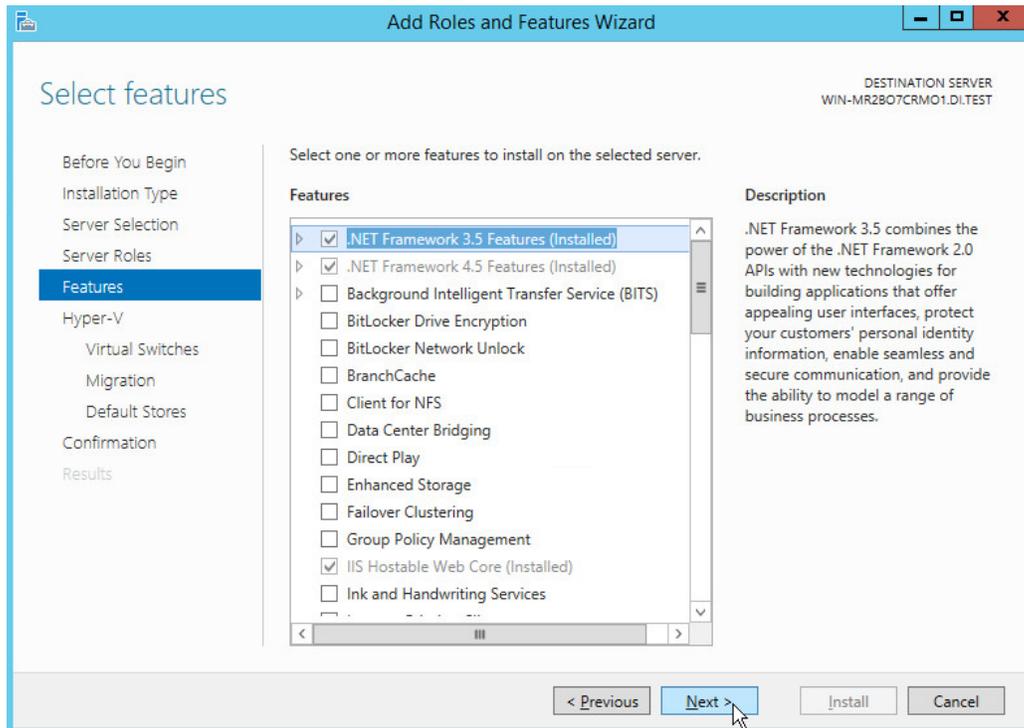
5. Click **Next**.
6. On the **Select destination server** page, select a server from the server pool.



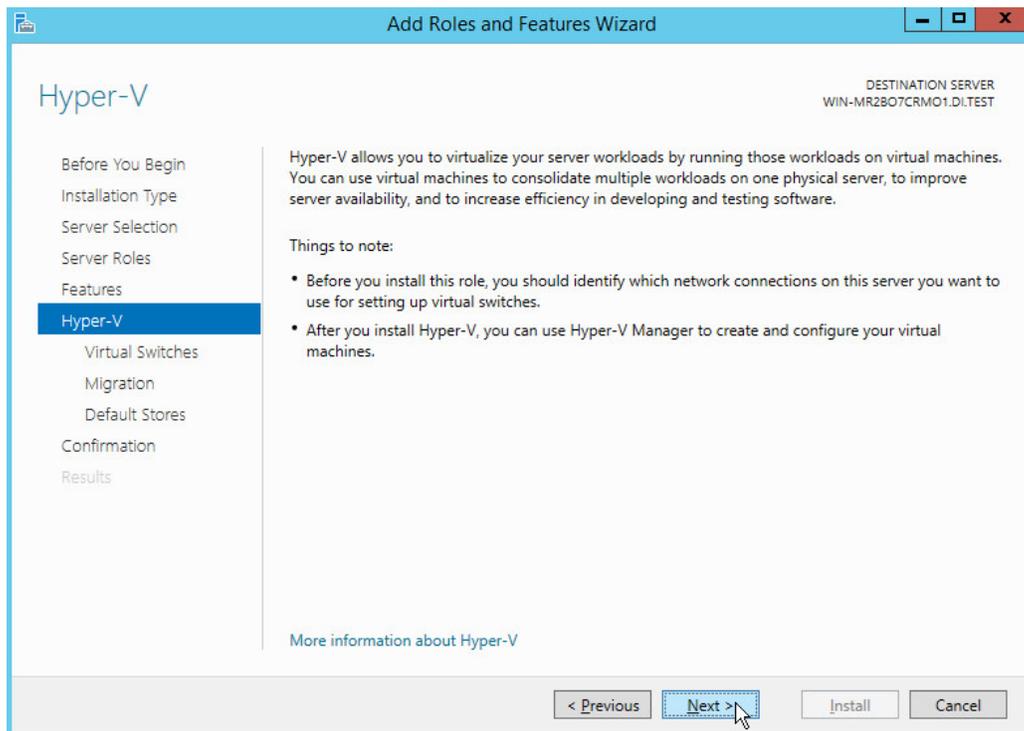
7. Click **Next**.
8. On the **Select server roles** page, select **Hyper-V**.
9. To add the tools that you use to create and manage virtual machines, click **Add Features**.



10. Click **Next**.

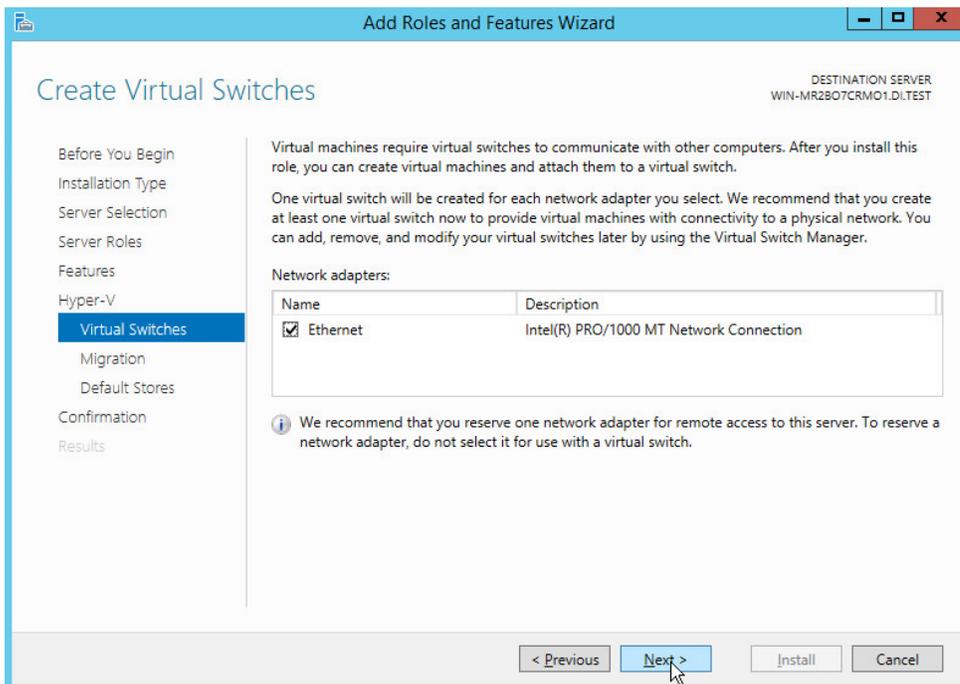


11. Click **Next**.



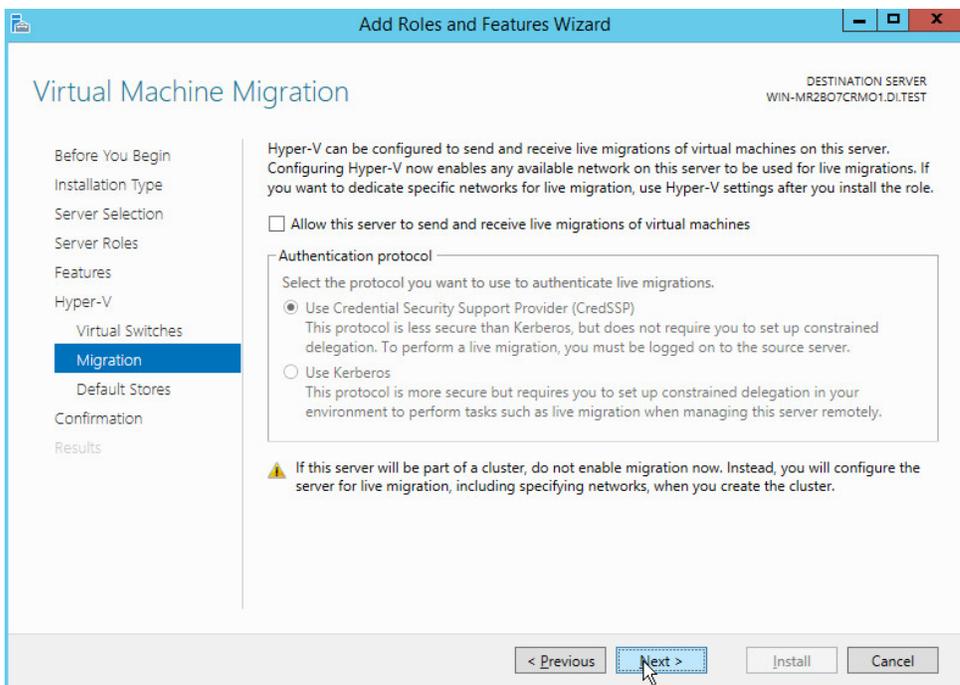
12. Click **Next**.

13. On the **Create Virtual Switches** page, select the appropriate options.



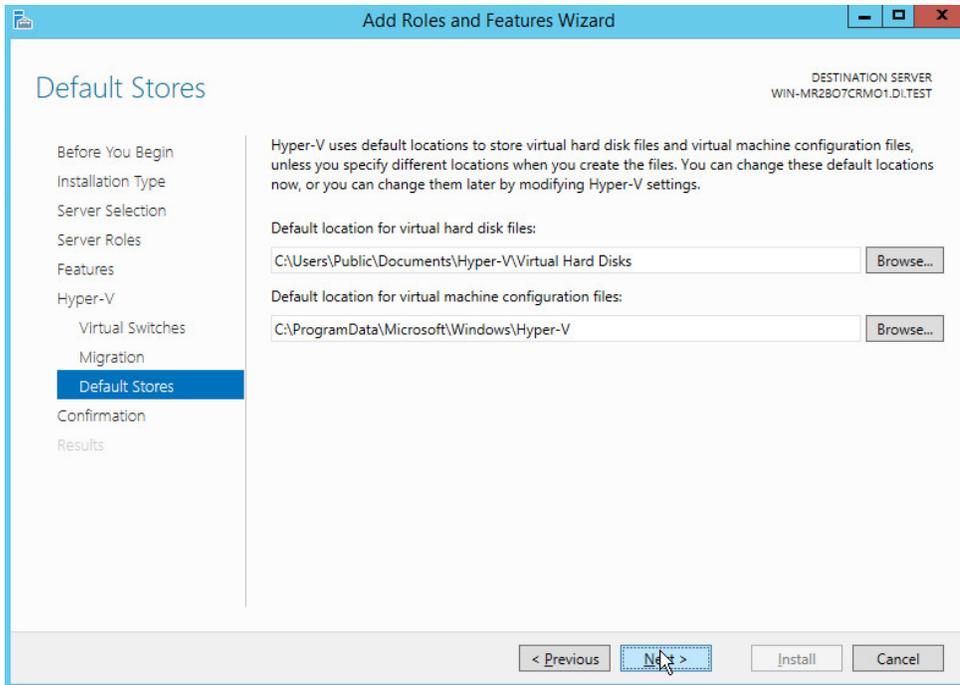
14. Click **Next**.

15. On the **Virtual Machine Migration** page, select the appropriate options.



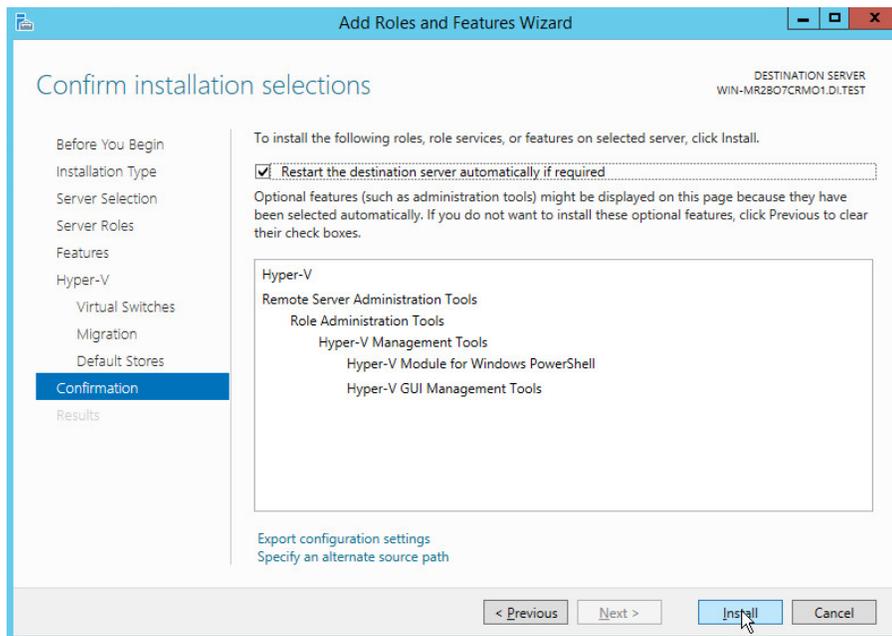
16. Click **Next**.

17. On the **Default Stores** page, select the appropriate options.



18. Click **Next**.

19. On the **Confirm installation selections** page, select **Restart the destination server automatically if required**.



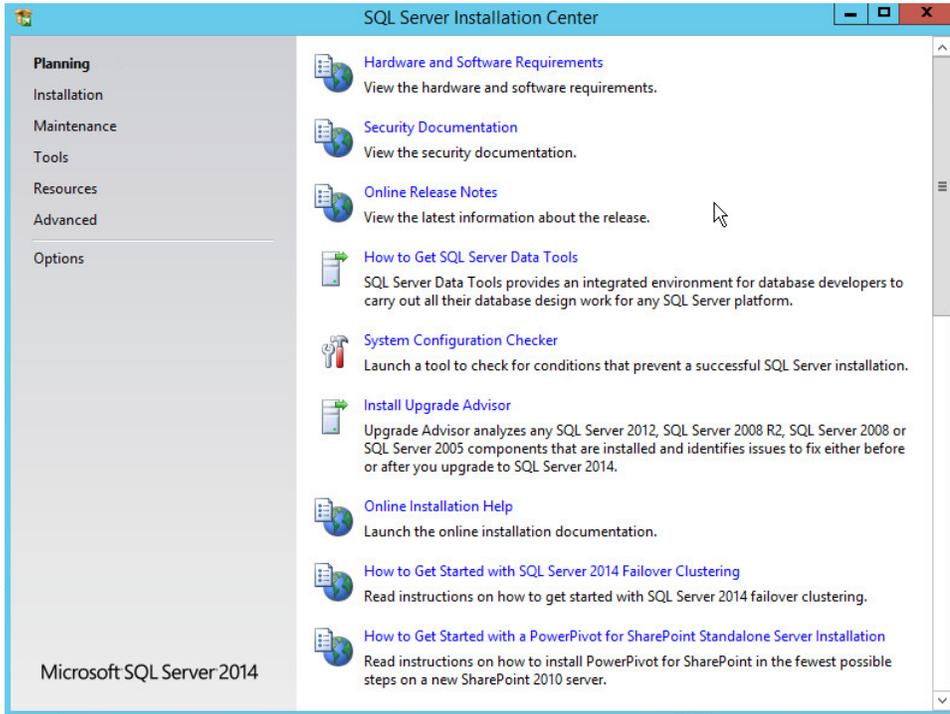
20. Click **Install**.
21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

2.4 MS SQL Server

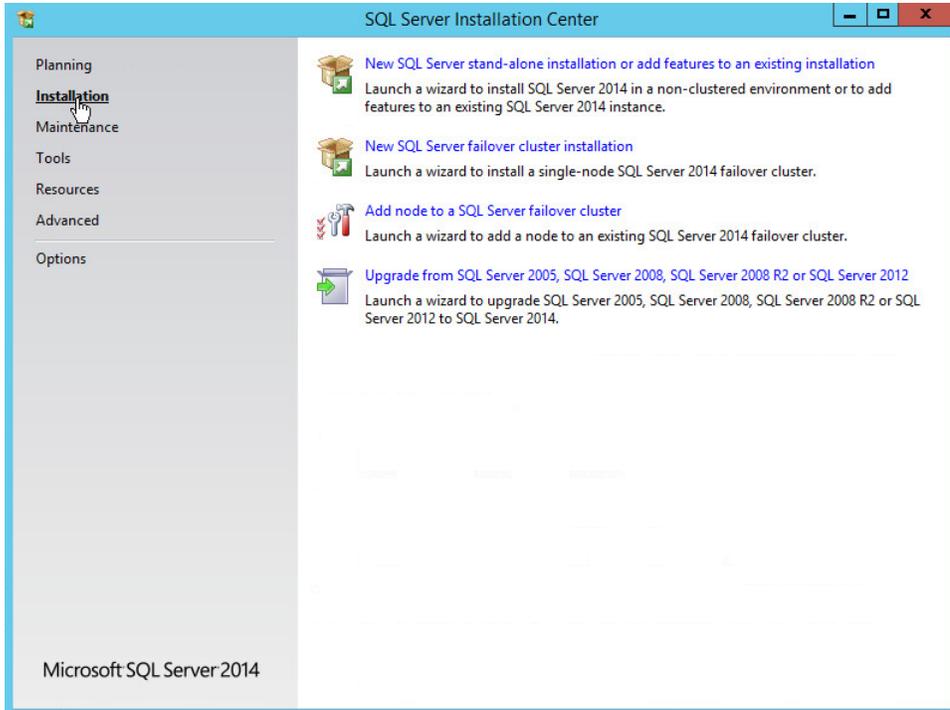
As part of both our enterprise emulation and data integrity solution, we include a Microsoft Structured Query Language (MS SQL) Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

2.4.1 Install and Configure MS SQL

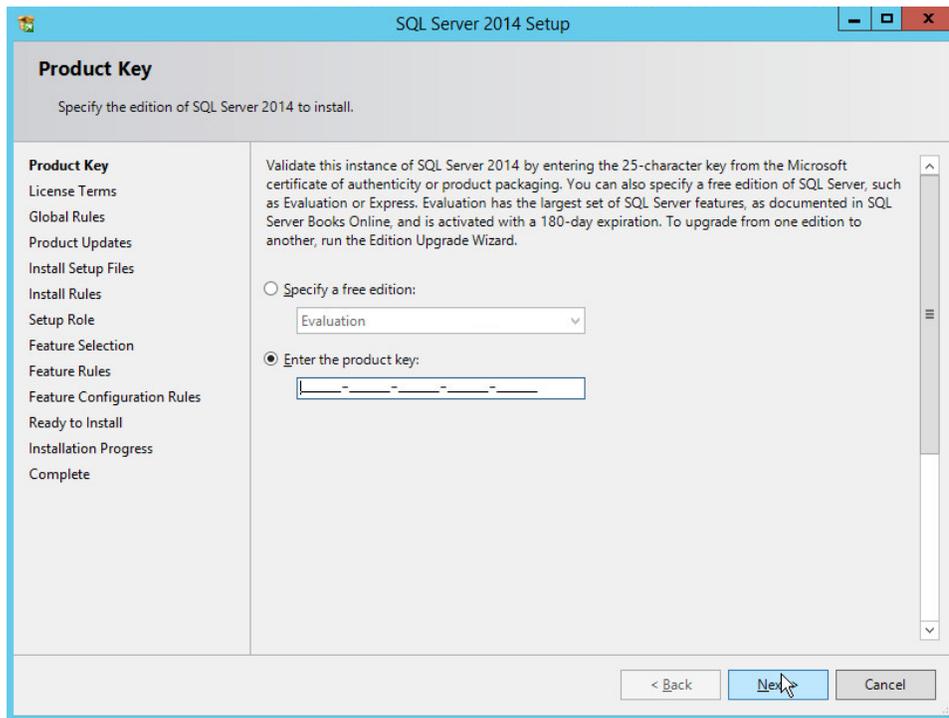
1. Acquire **SQL Server 2014 installation media**.
2. Locate the installation media in the machine and click on **SQL2014_x64_ENU** to launch **SQL Server Installation Center**.



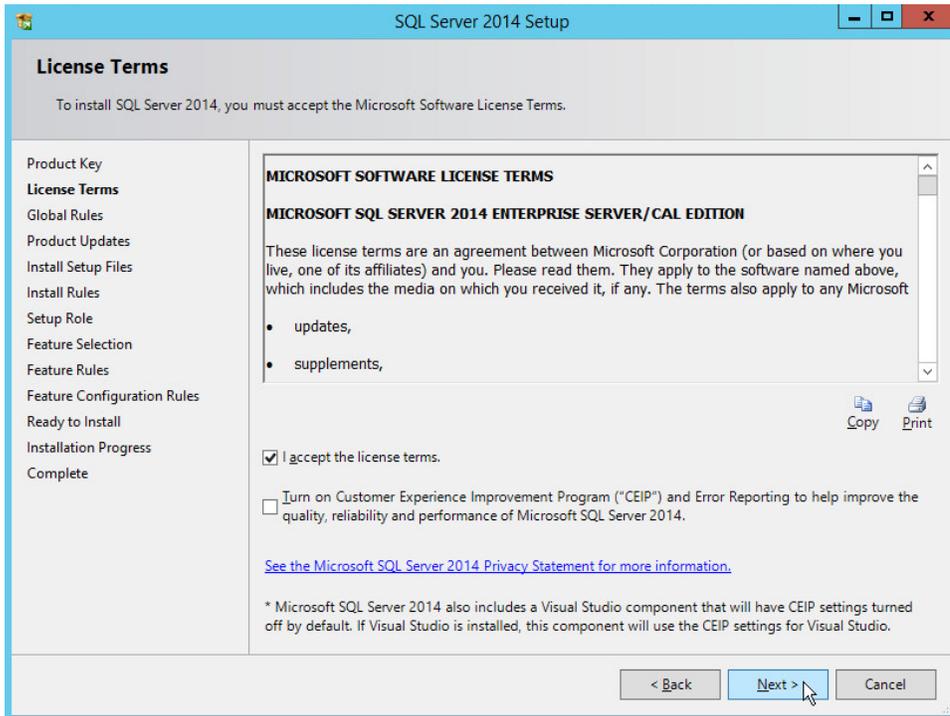
3. On the left menu, select **Installation**.



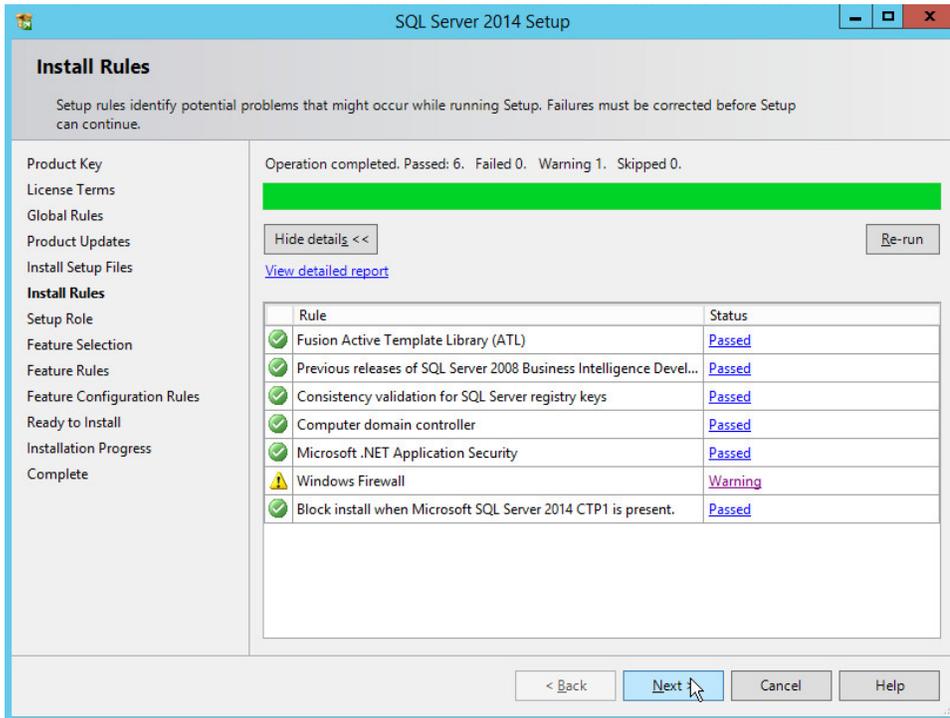
4. Select **New SQL Server stand-alone installation or add features to an existing installation**. This will launch the SQL Server 2014 setup.
5. In the **Product Key** section, enter your product key.



6. Click **Next**.
7. In the **License Terms** section, read and click **I accept the license terms**.

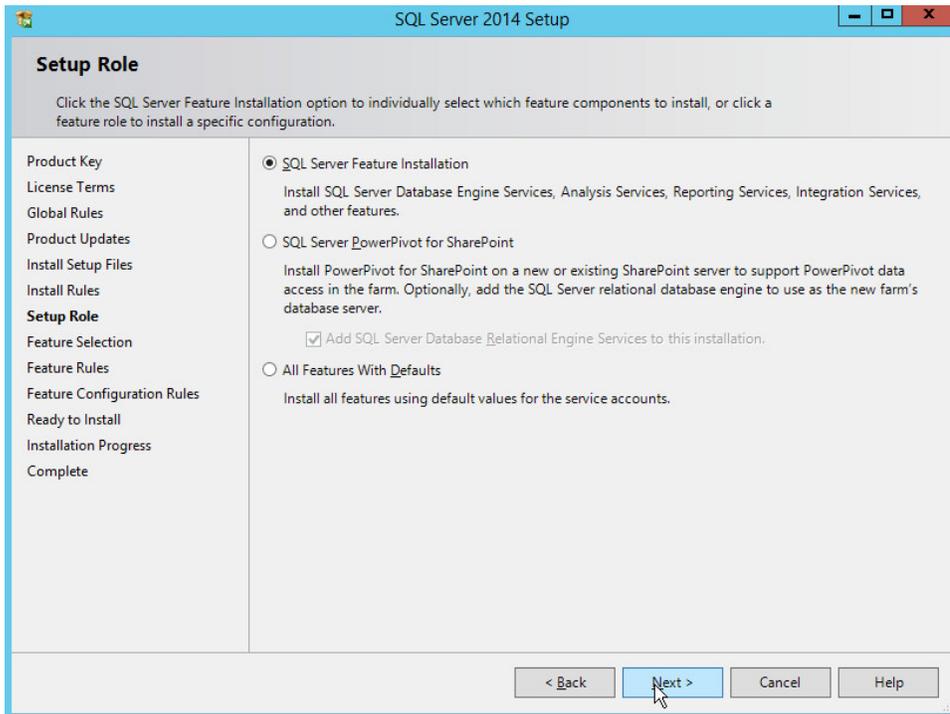


8. Click **Next**.
9. In the **Install Rules** section, note and resolve any further conflicts.



10. Click **Next**.

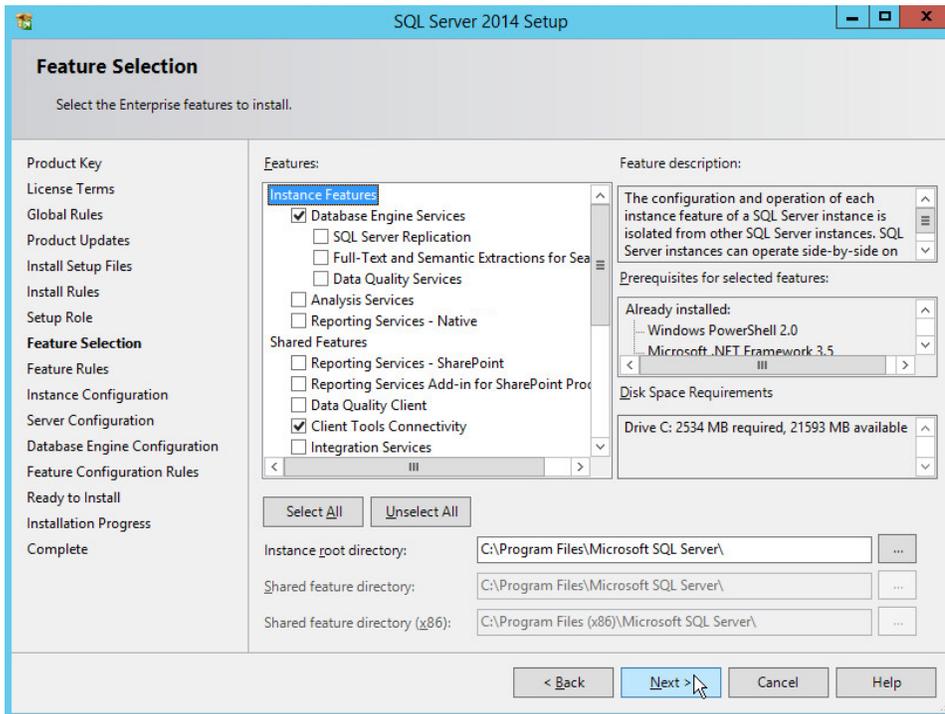
11. In the **Setup Role** section, select **SQL Server Feature Installation**.



12. Click **Next**.

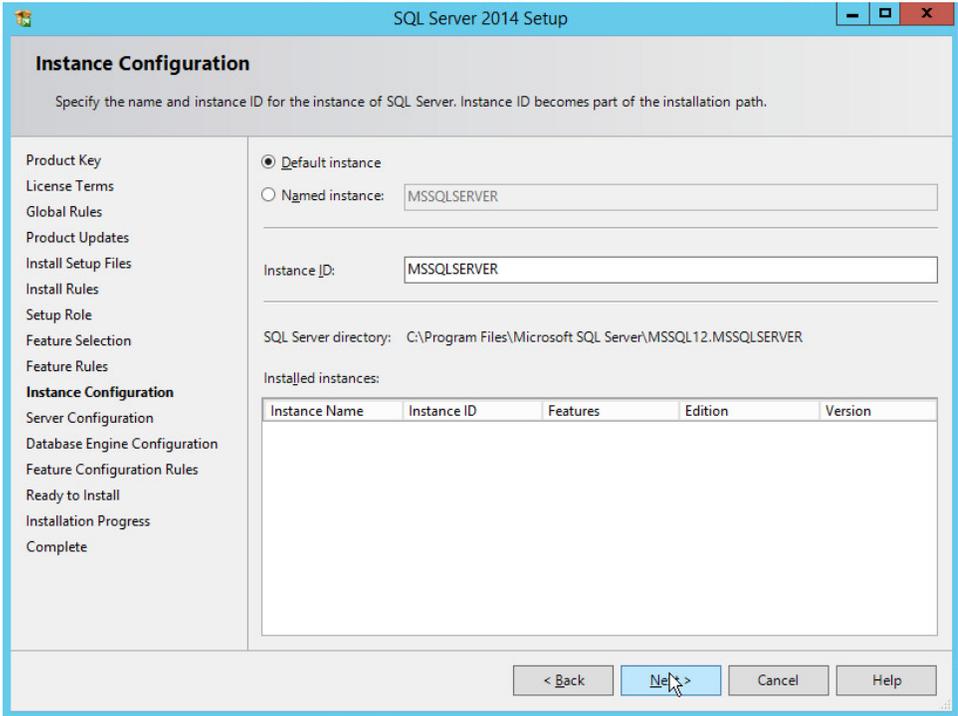
13. In the **Feature Selection** section, select the following options:

- a. **Database Engine Services**
- b. **Client Tools Connectivity**
- c. **Client Tools Backwards Compatibility**
- d. **Client Tools SDK**
- e. **Management Tools – Basic**
- f. **Management Tools – Complete**
- g. **SQL Client Connectivity SDK**
- h. **Any other desired features**

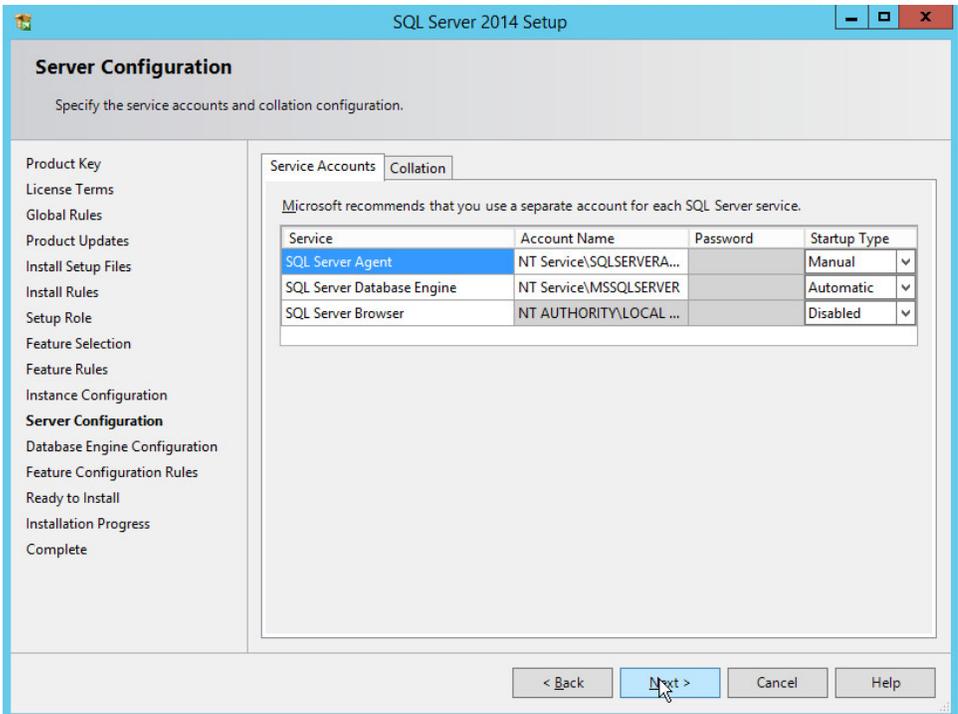


14. Click **Next**.

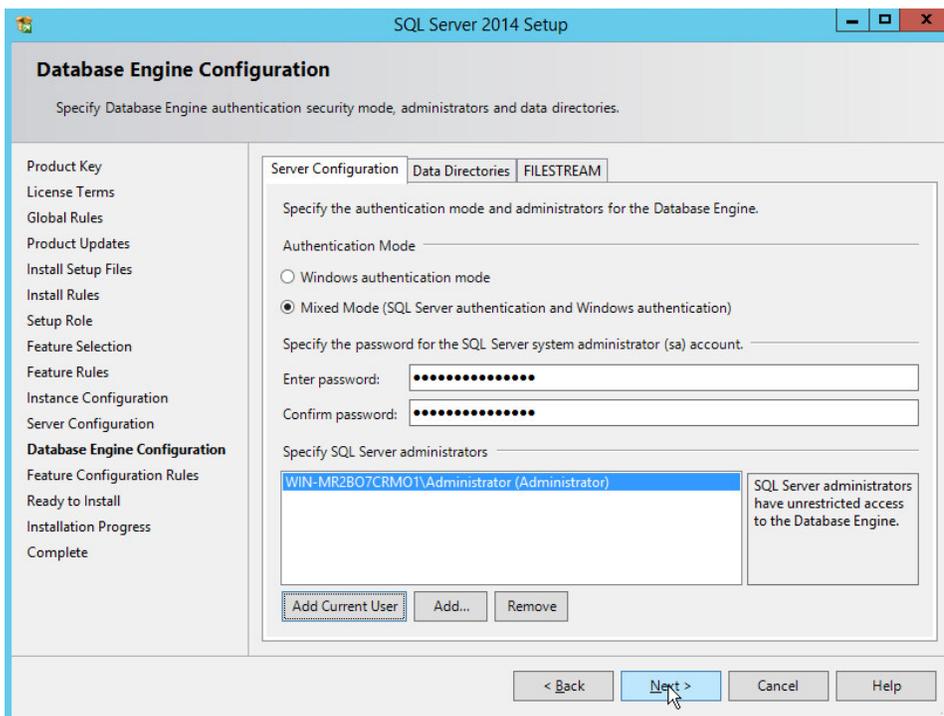
15. In the **Instance Configuration** section, select **Default instance**.



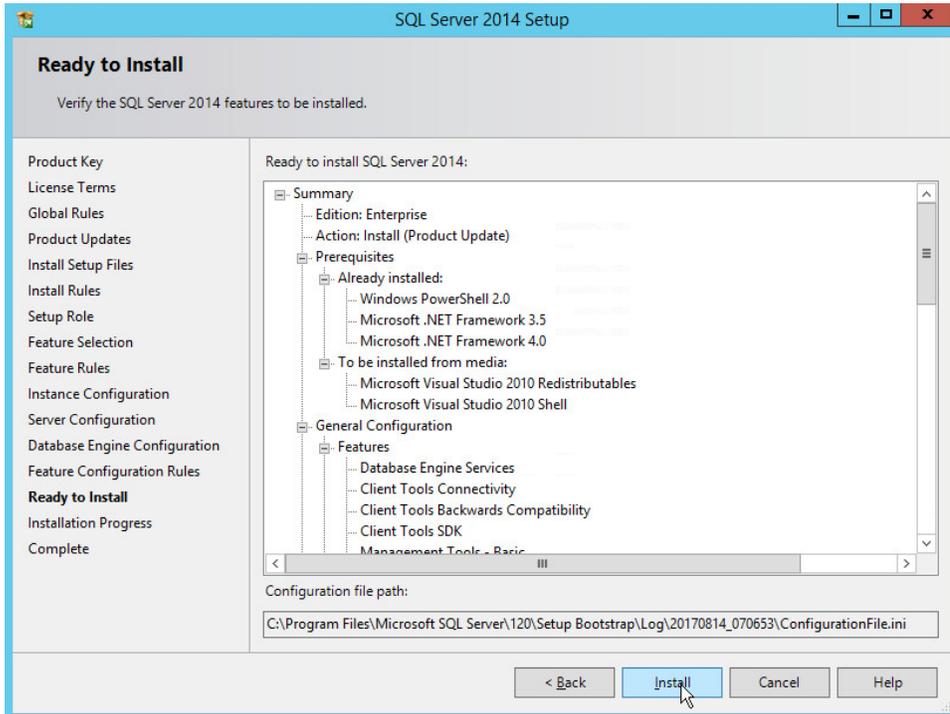
16. Click **Next**.



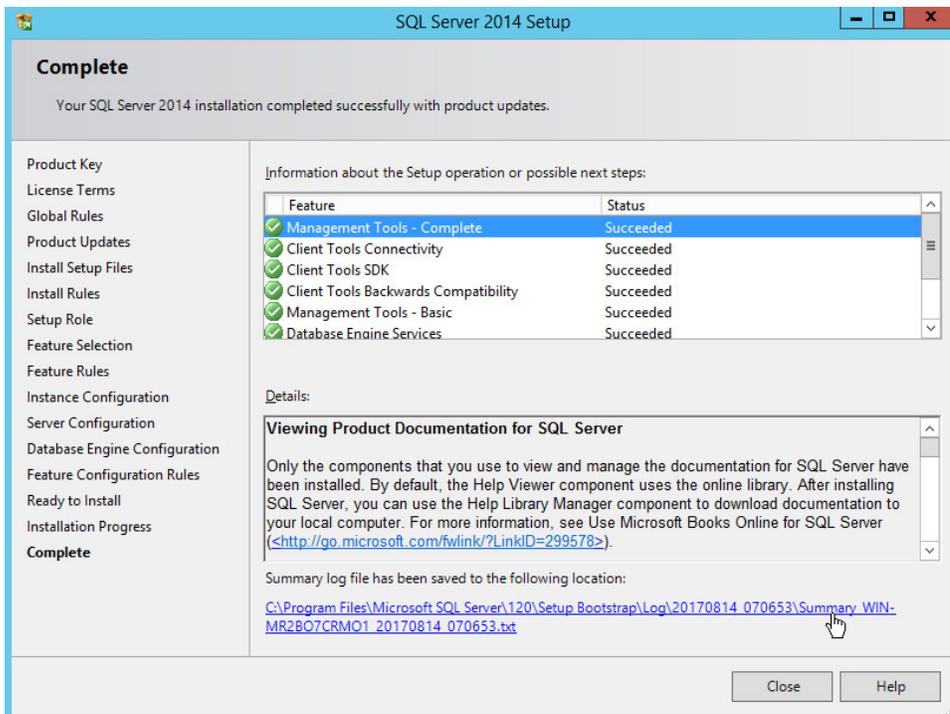
17. In the **Server Configuration** section, click **Next**.
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.
19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User**.
 - a. For Domain accounts, simply type in **\$DOMAINNAME\\$USERNAME** into **Enter the object names to select** text box.
 - b. Click **OK**.
 - c. For local computer accounts, click on **locations** and select the computer's name.
 - d. Click **OK**.
 - e. Type the username into the **Enter the object names to select** text box.
 - f. Once you are finished adding users, click **Next**.



20. In the **Ready to install** section, verify the installation and click **Install**.



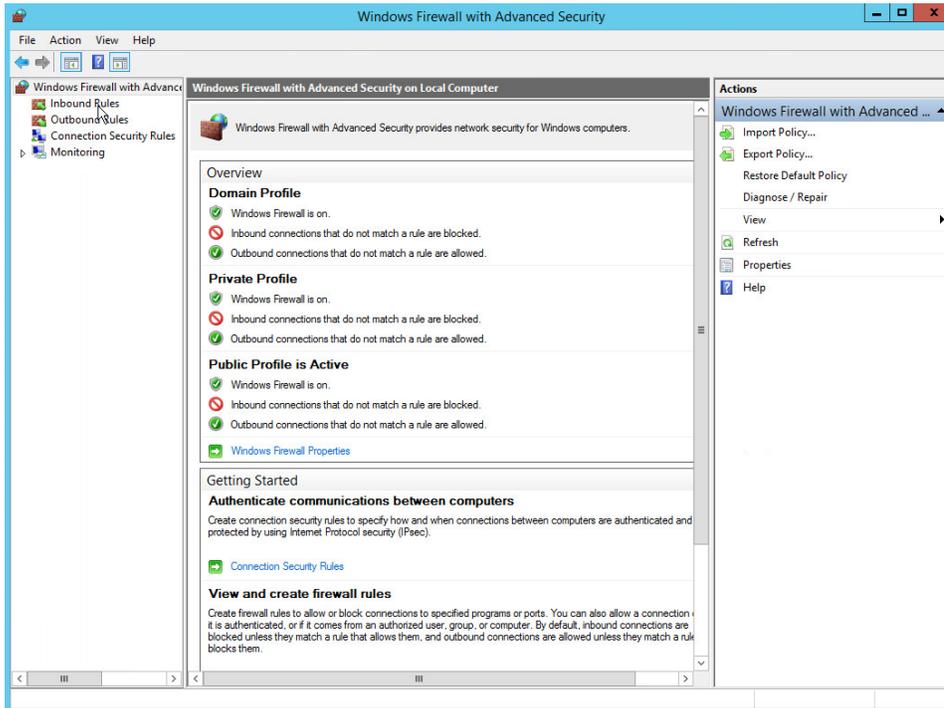
21. Wait for the installation to finish.



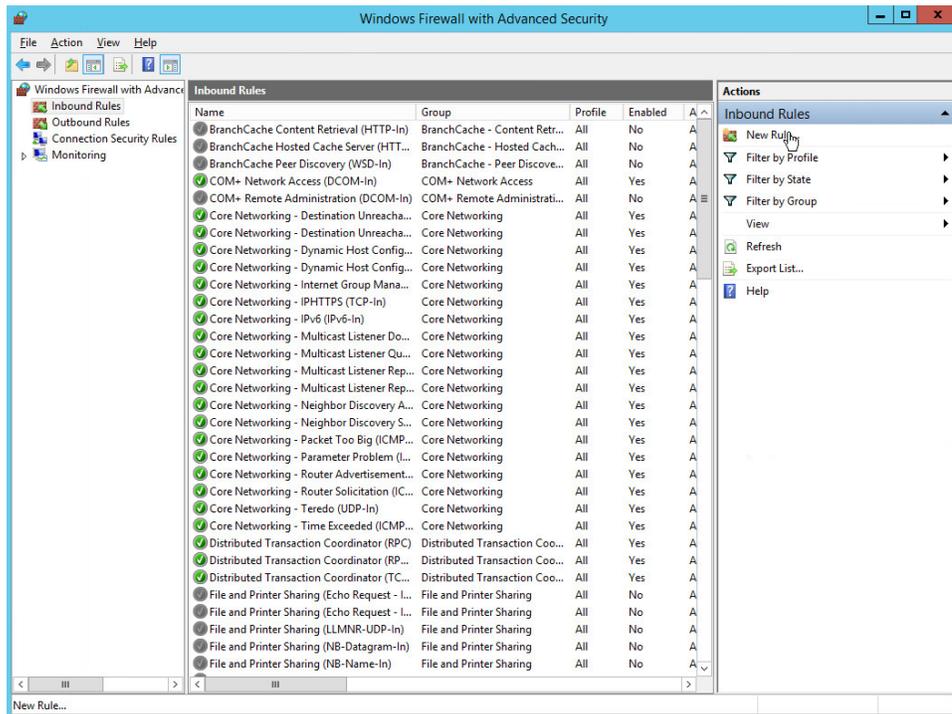
22. Click **Close**.

2.4.2 Open Port on Firewall

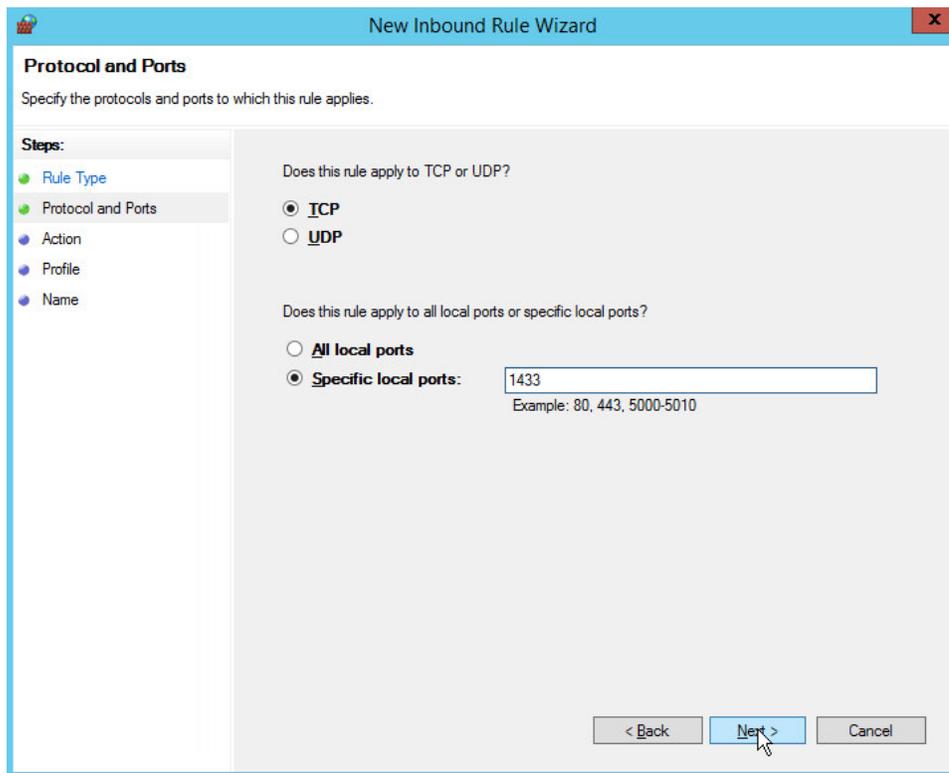
1. Open **Windows Firewall with Advanced Security**.



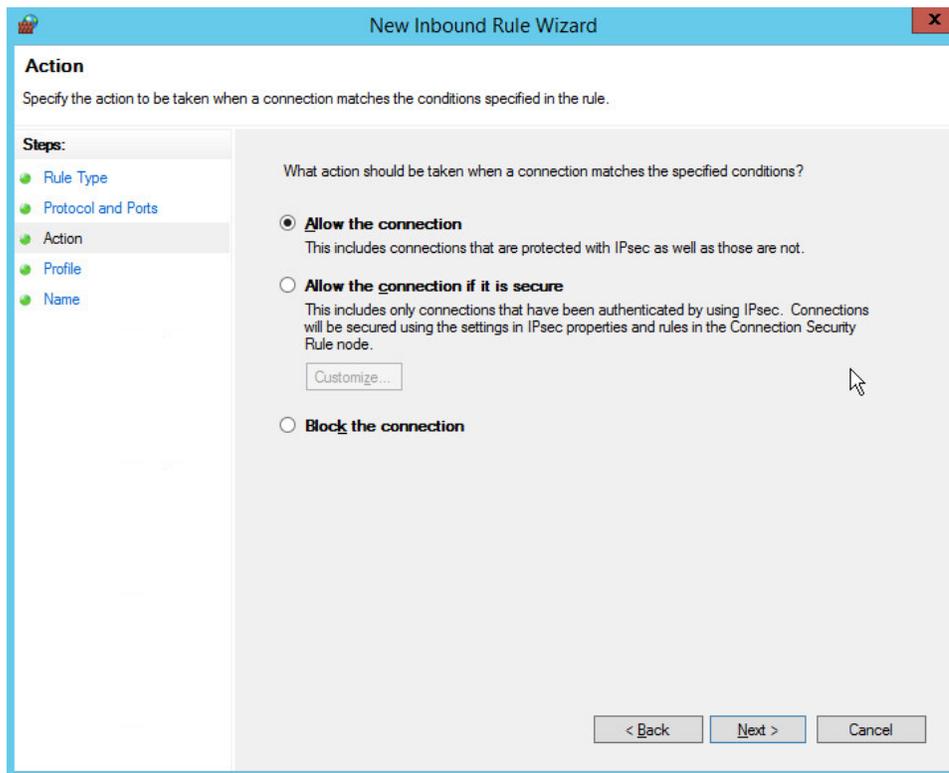
2. Click **Inbound Rules**.



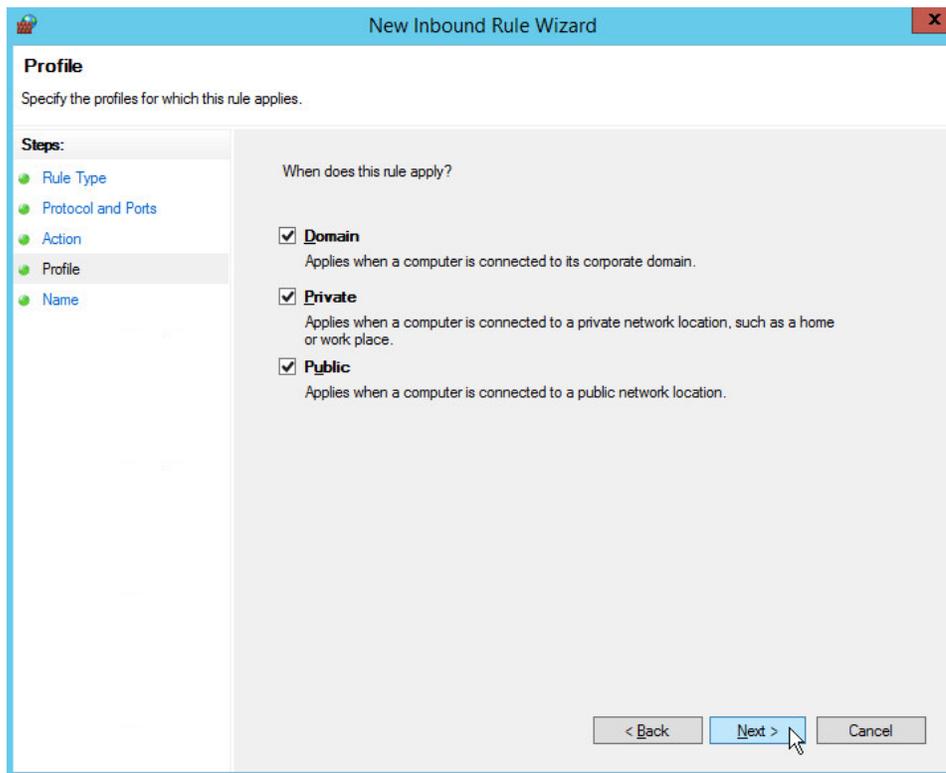
3. Click **New Rule**.
4. Select **Port**.
5. Click **Next**.
6. Select **TCP** and **Specific local ports**.
7. Type **1433** into the text field.



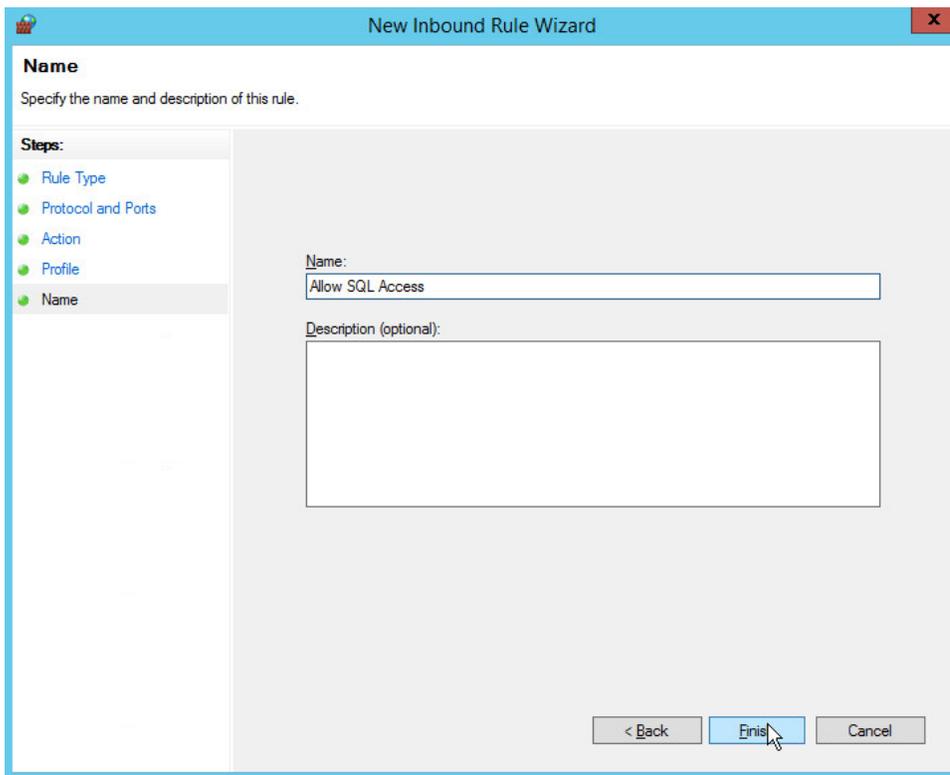
8. Click **Next**.
9. Select **Allow the connection**.



10. Click **Next**.
11. Select all applicable locations.



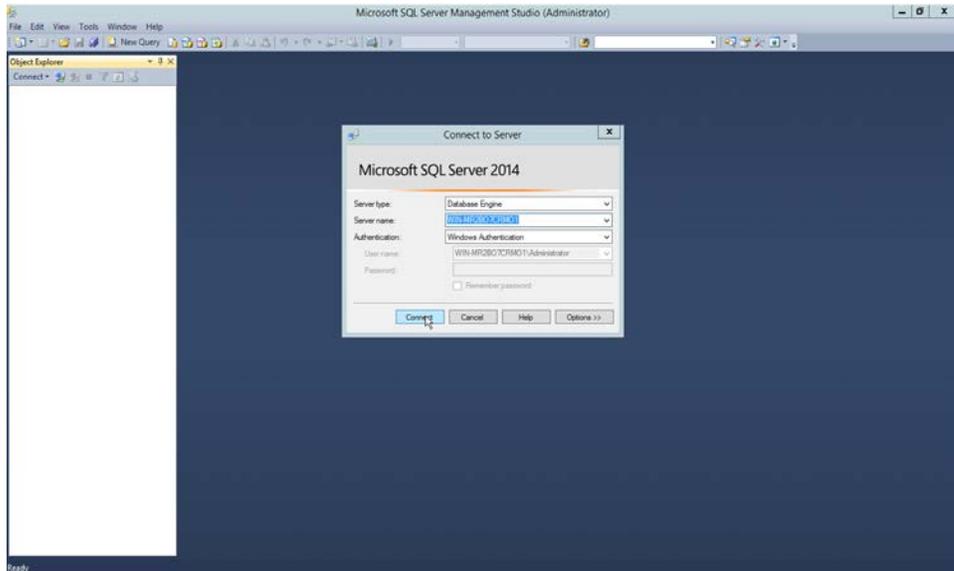
12. Click **Next**.
13. Name the rule **Allow SQL Access**.



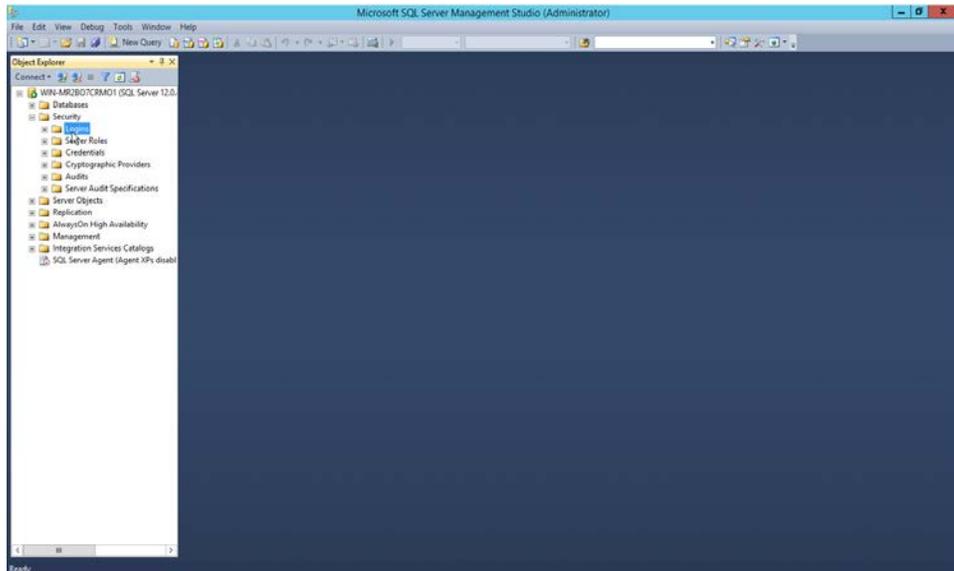
14. Click **Finish**.

2.4.3 Add a New Login to the Database

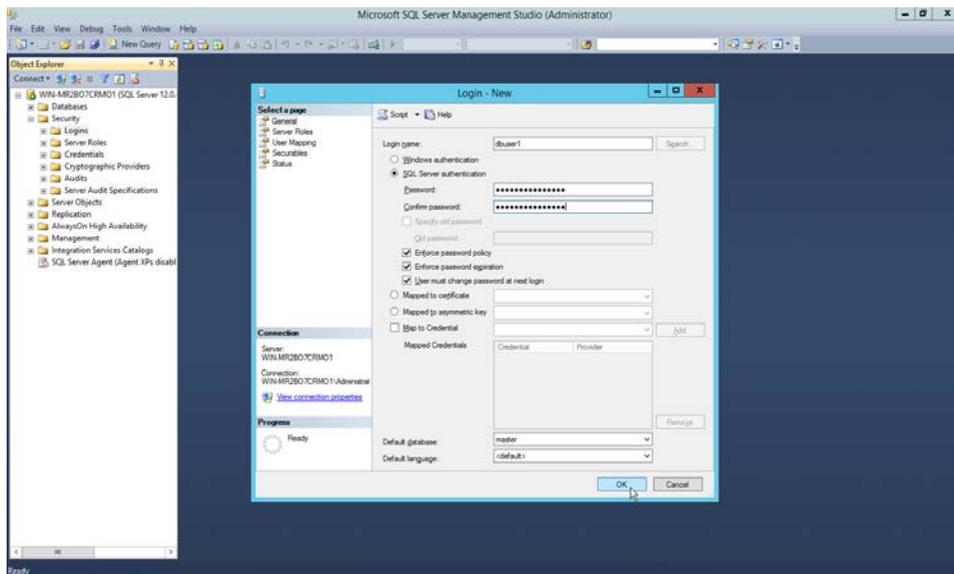
1. Open **SQL Server Management Studio**.



2. Click **Connect** to connect to the database.
3. In the **Object Explorer** window, expand the **Security** folder.



4. Right-click on the **Logins** folder and click **New Login....**
5. Input the desired user.



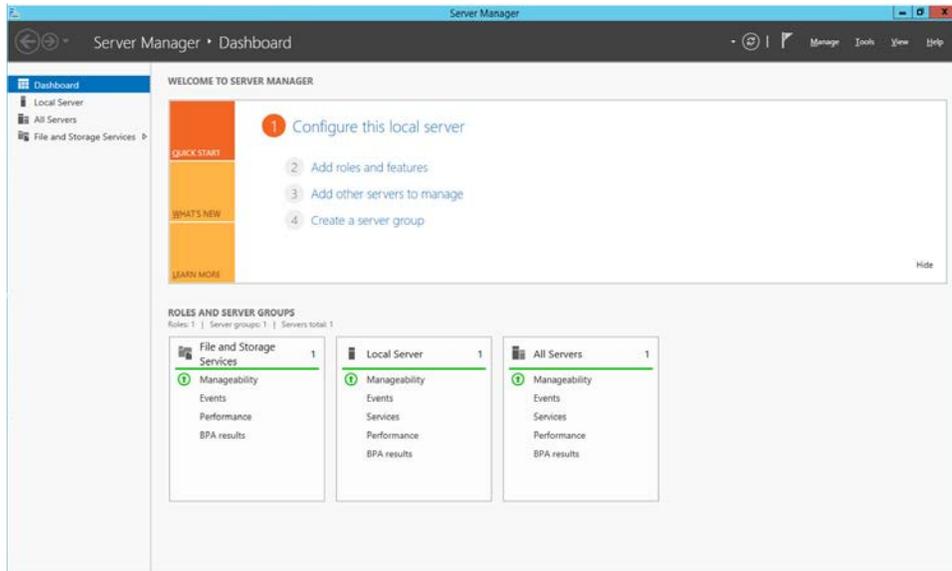
6. Click **OK**.

2.5 Microsoft IIS Server

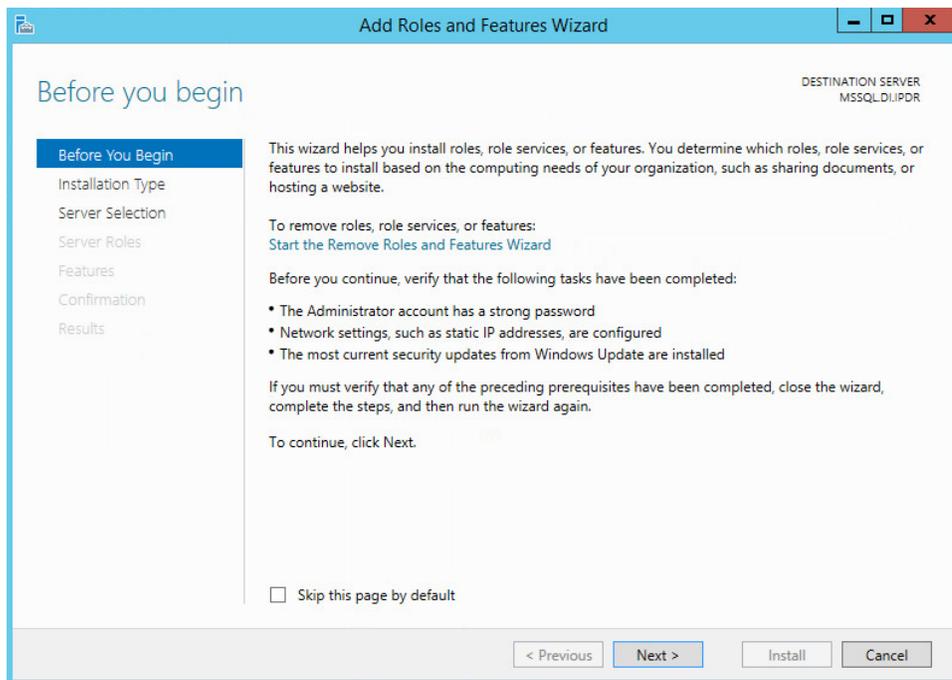
As part of our enterprise emulation, we include a Microsoft Internet Information Services (IIS) server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine. This was conducted on the same machine as in [Section 2.4](#).

2.5.1 Install IIS

1. Open **Server Manager**.

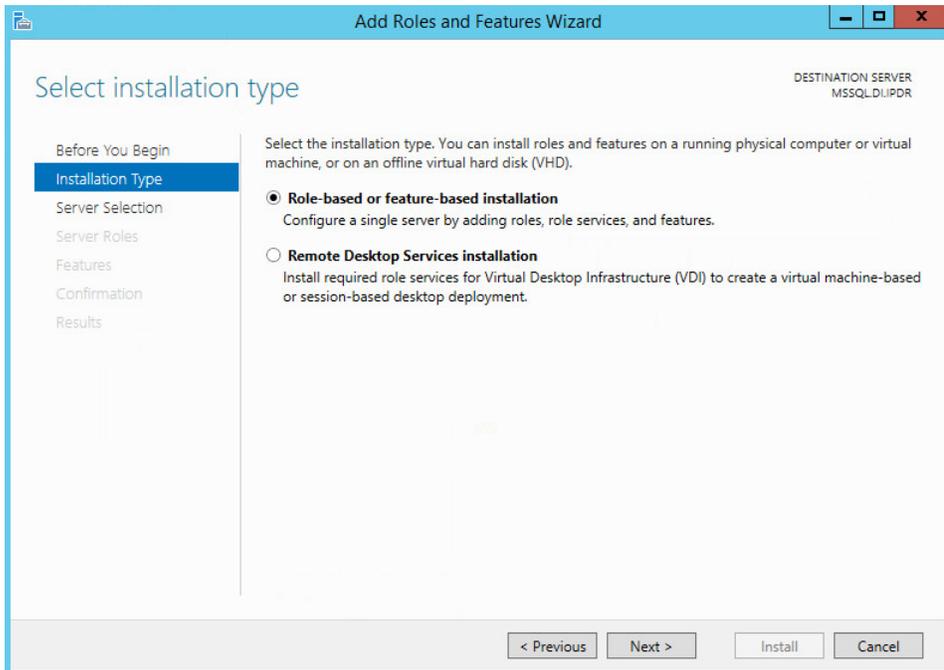


2. Click **Add Roles and Features**.



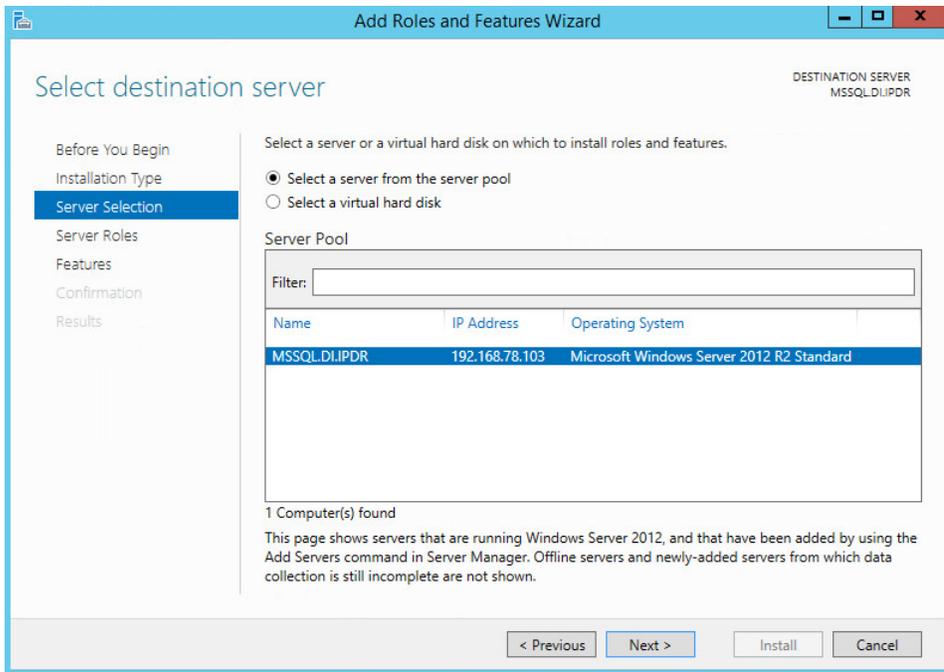
3. Click **Next**.

4. Select **Role-based or feature-based installation**.

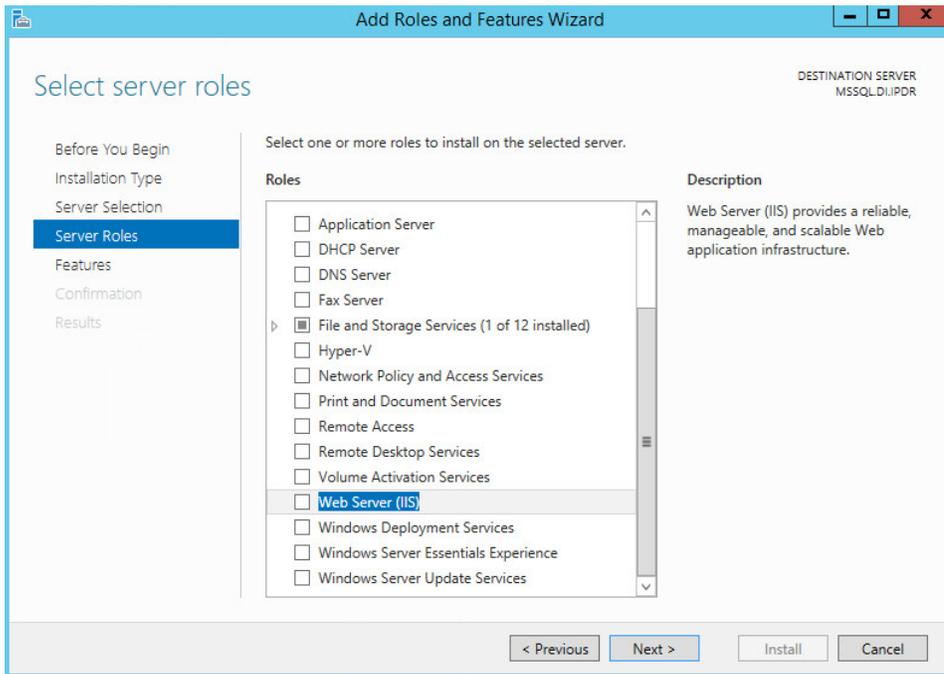


5. Click **Next**.

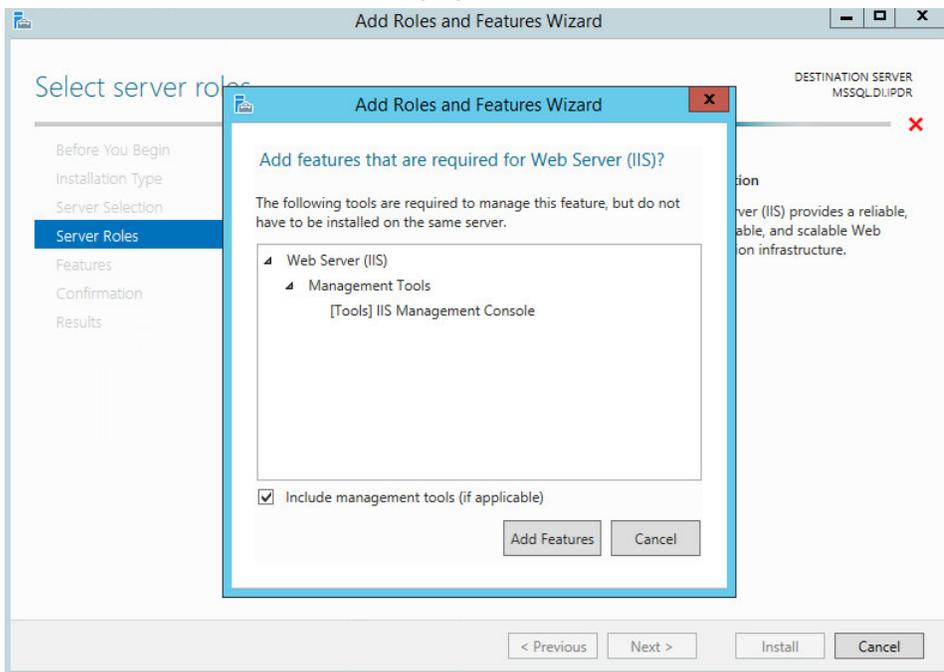
6. Select **MSSQL** (or the correct Windows Server name) from the list.



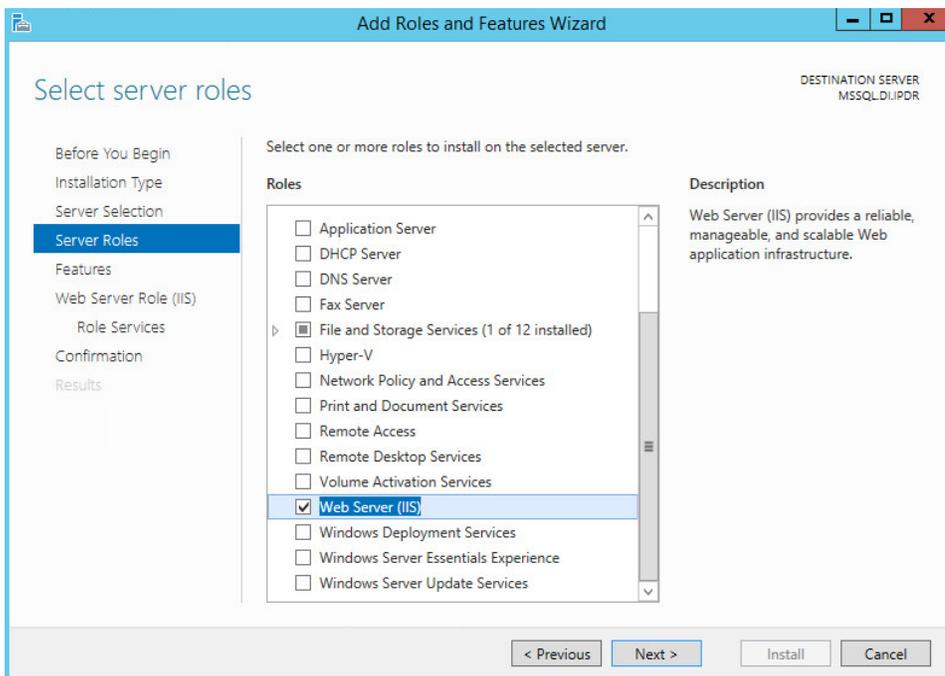
7. Click **Next**.



8. Check the box next to **Web Server (IIS)**.

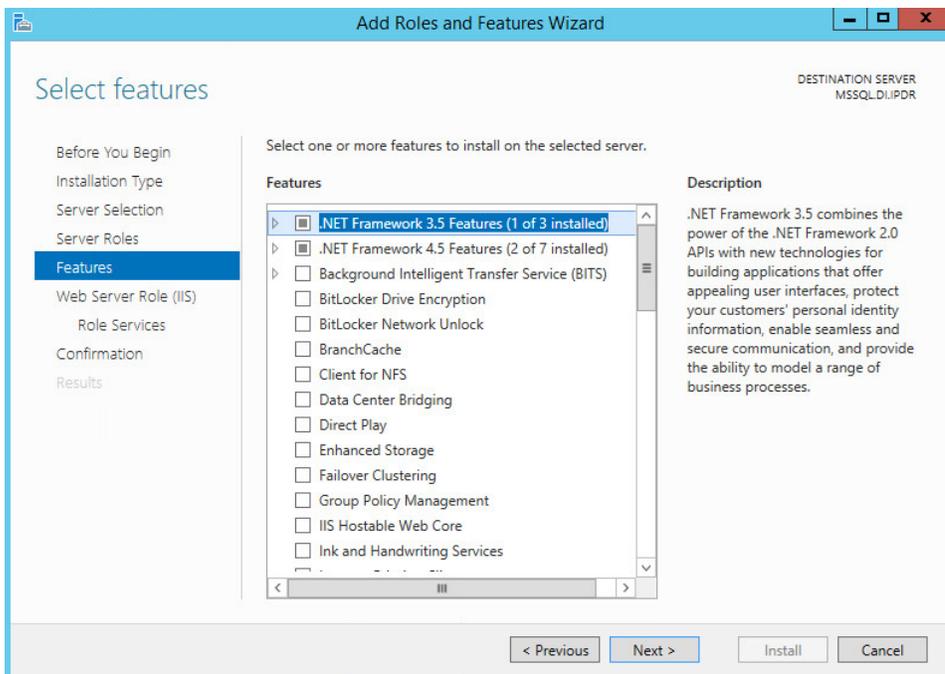


9. Click **Add Features**.

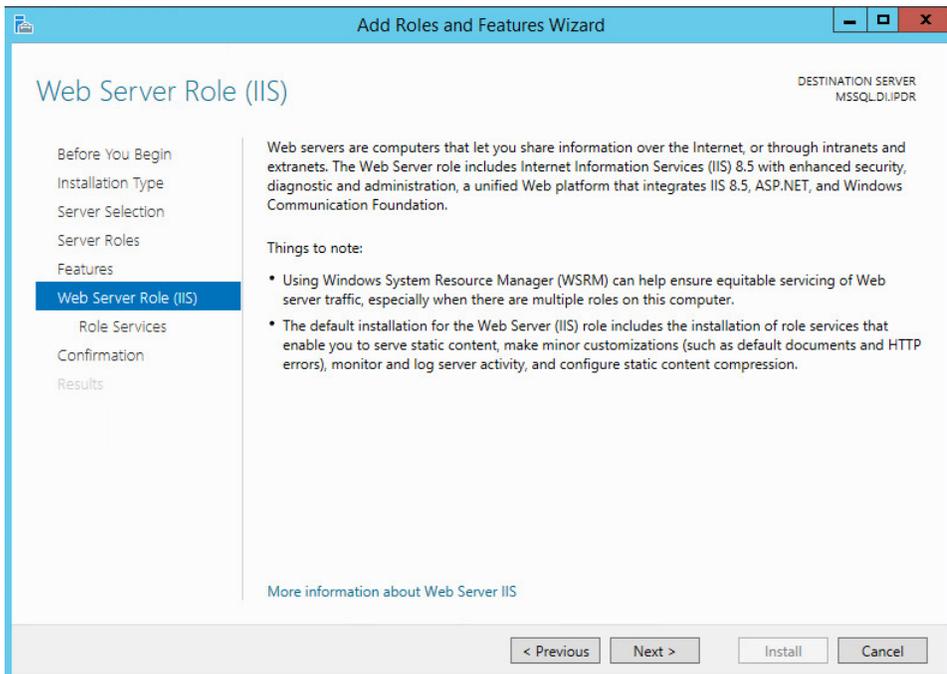


10. Click **Next**.

11. Ensure that all desired features are selected.

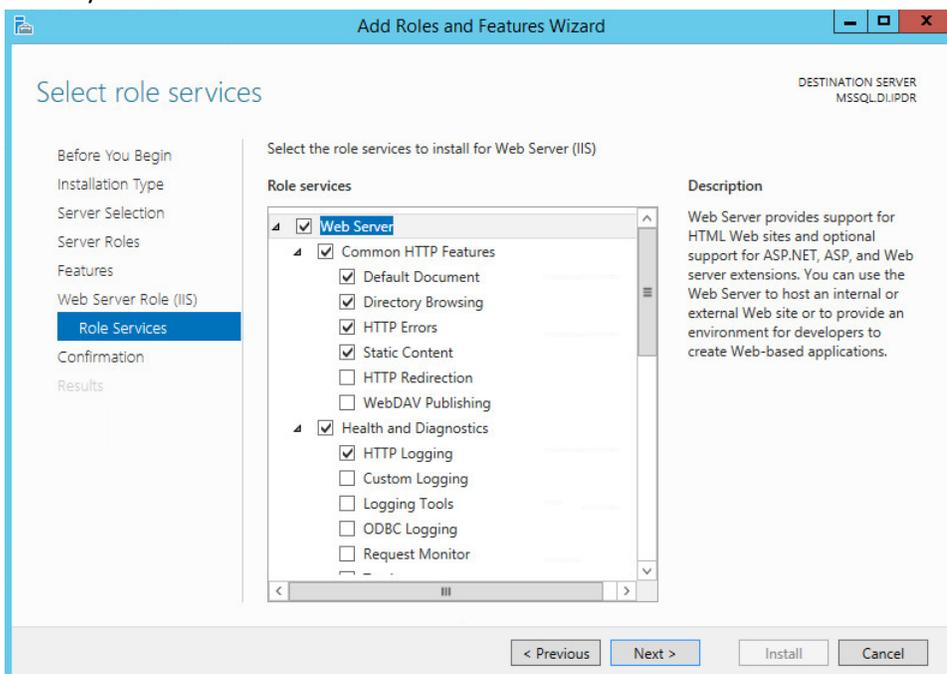


12. Click **Next**.

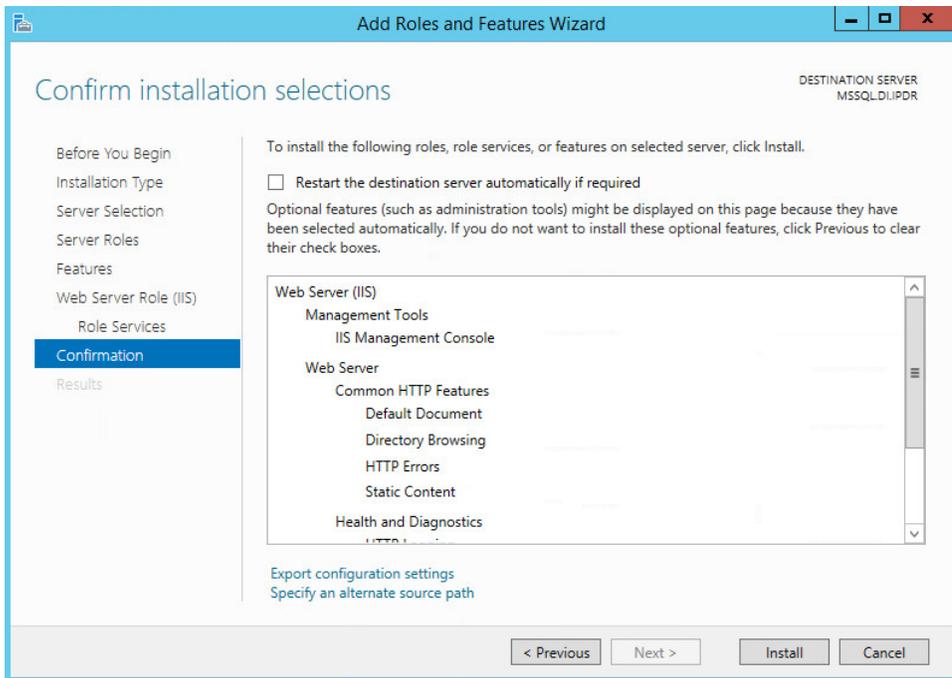


13. Click **Next**.

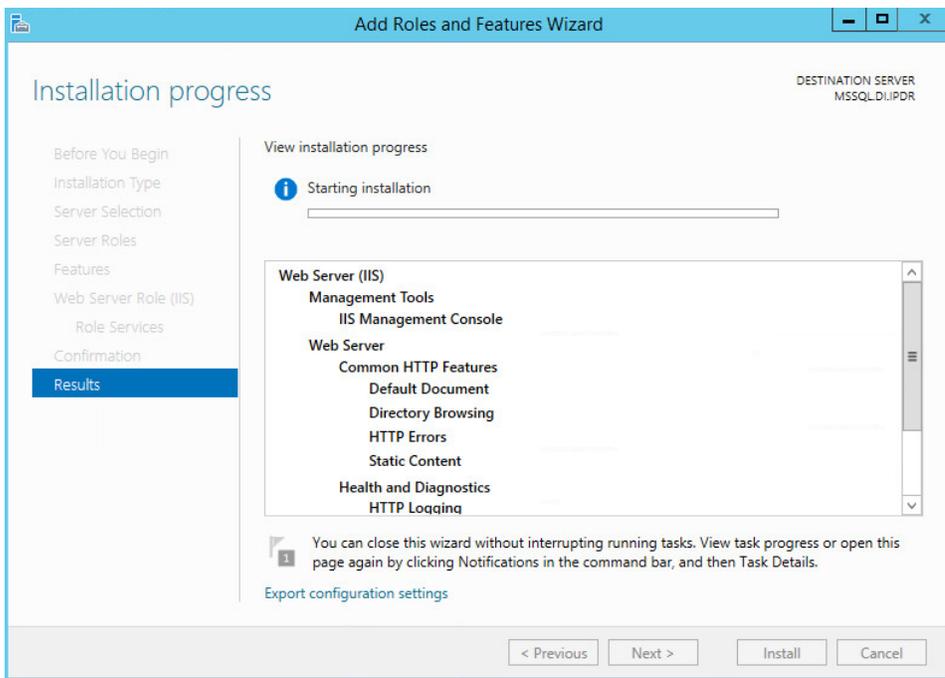
14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging,** and any other desired Role services are selected.



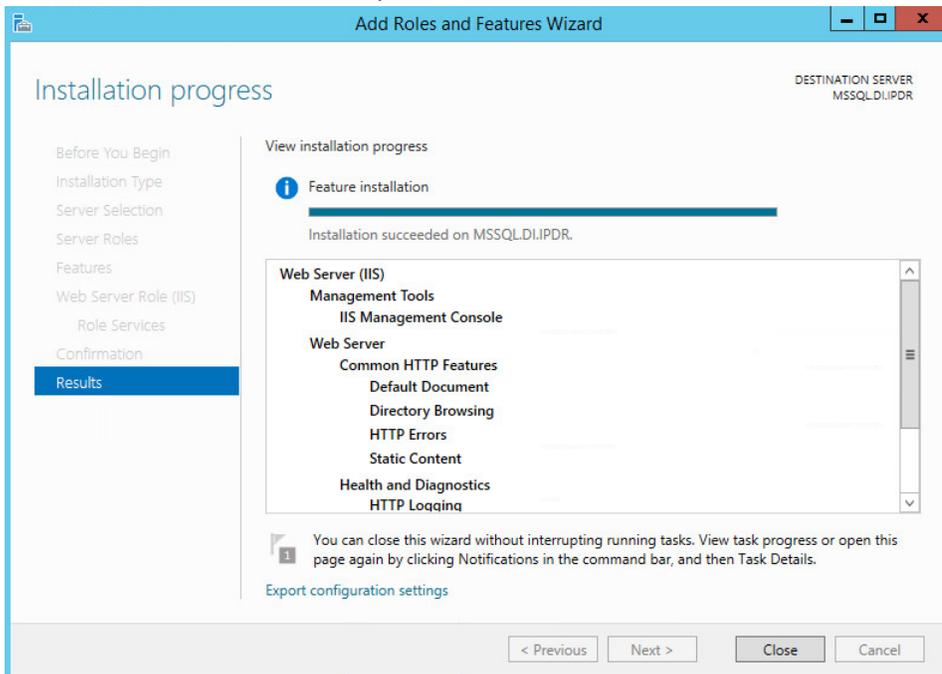
15. Click **Next**.



16. Click **Install**.



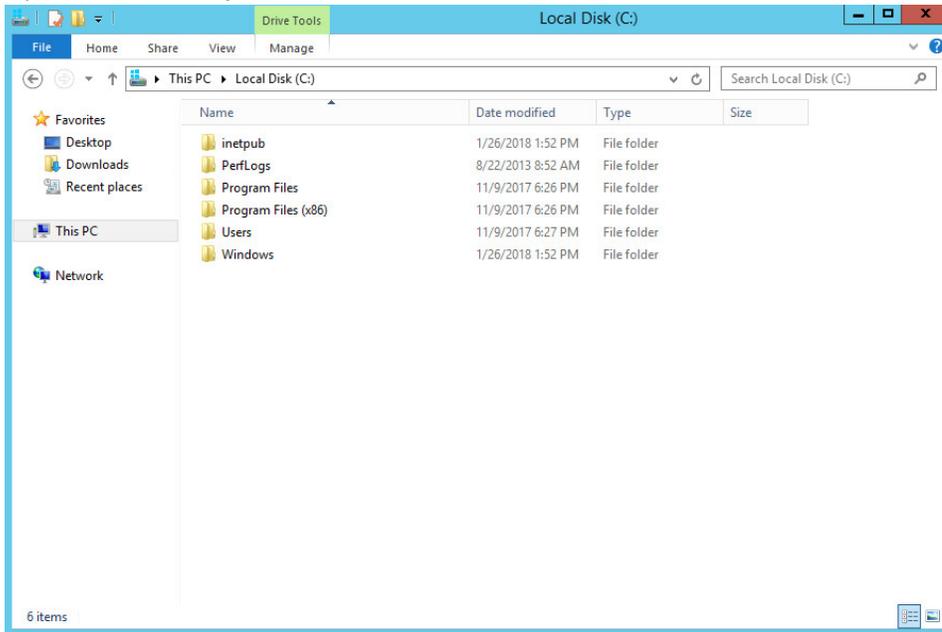
17. Wait for the installation to complete.



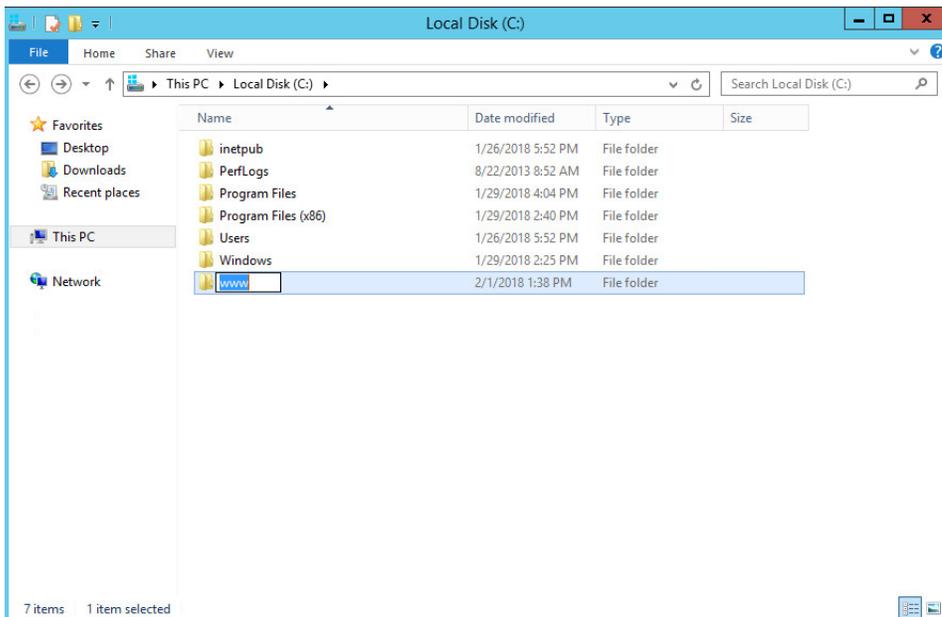
18. Click **Close**.

2.5.2 IIS Configuration

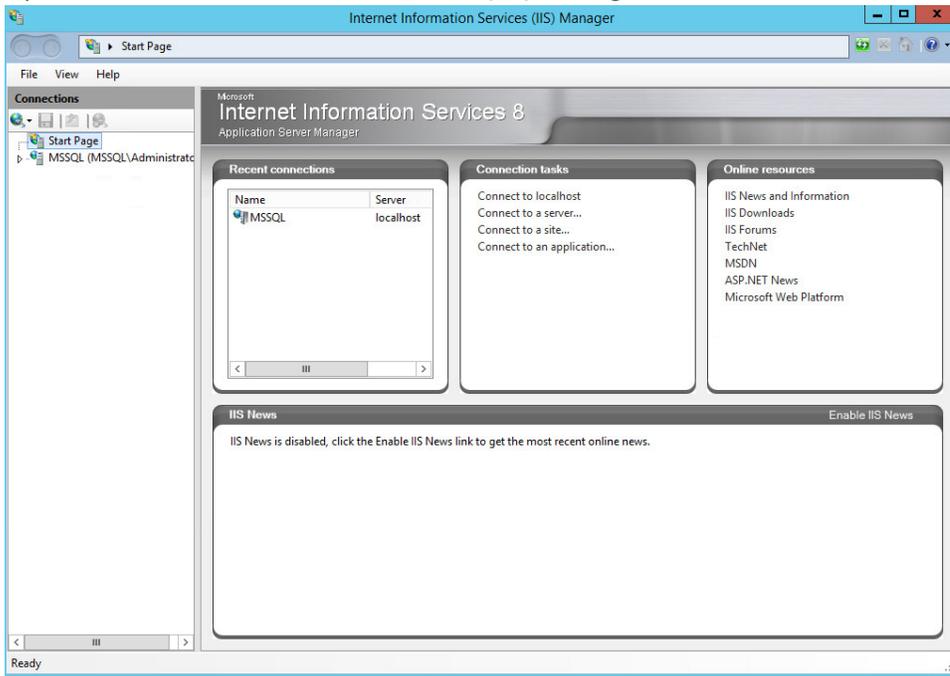
1. Open Windows Explorer and click **This PC**.



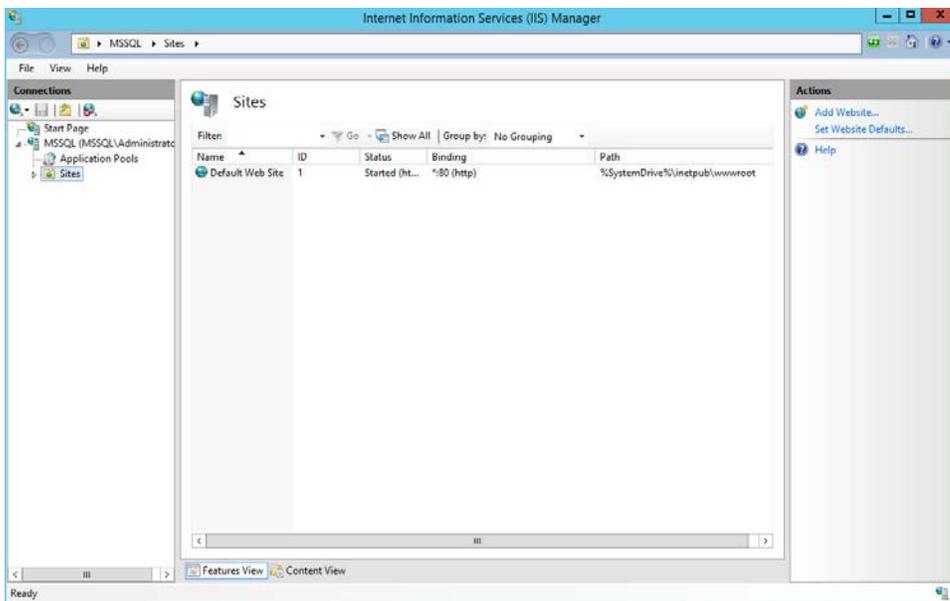
2. Right-click and select **Create Folder**.
3. Name the folder **www**.



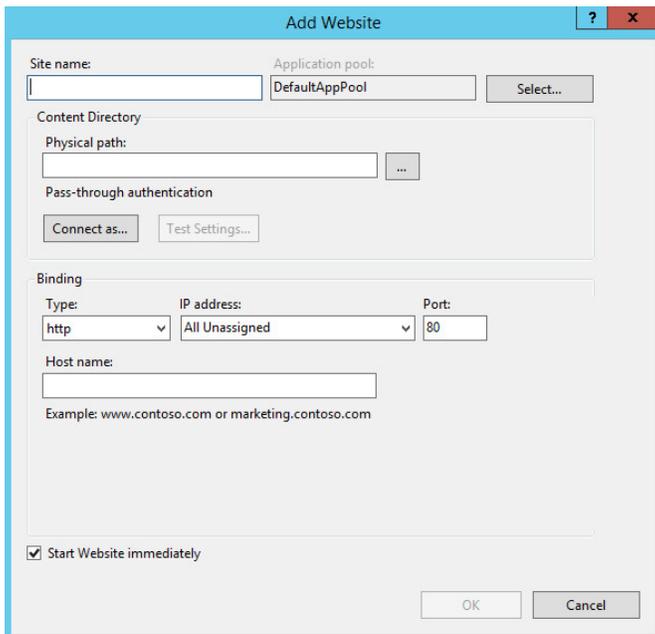
4. Open the **Internet Information Services (IIS) Manager**.



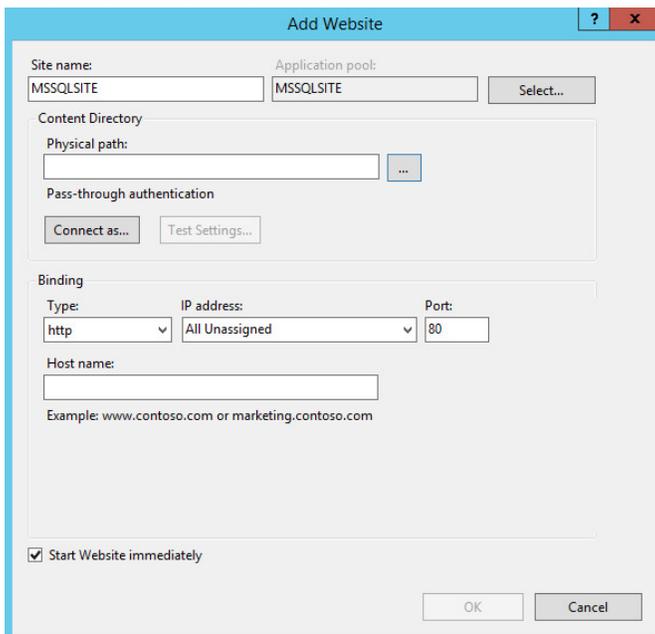
- 5. Click the arrow next to **MSSQL** (or the chosen name of the server).
- 6. Click **Sites**.



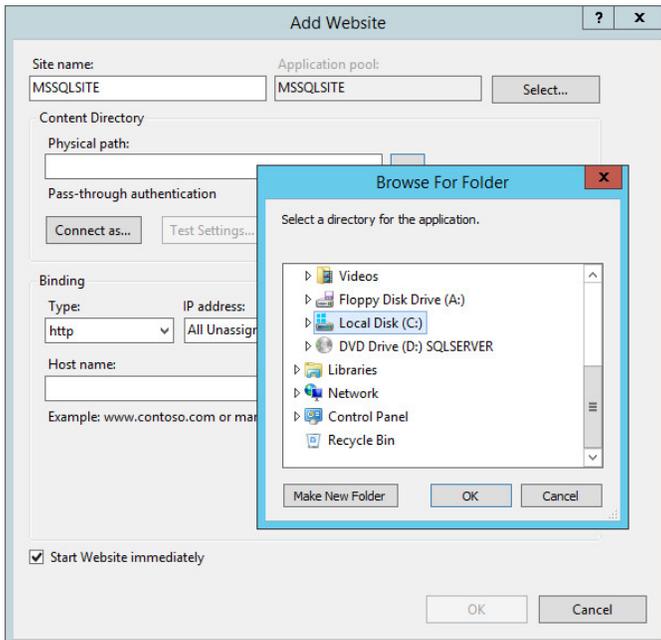
- 7. Click **Add Website....**



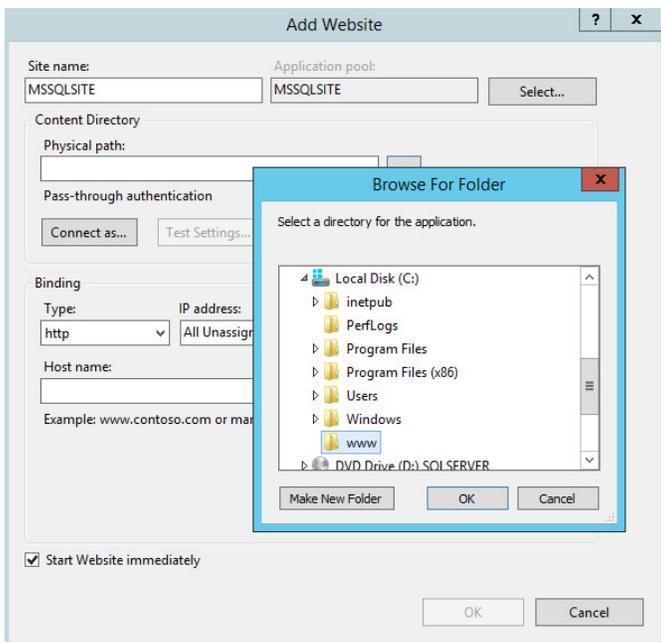
8. Enter the desired site name.



9. Click ... under **Physical path**.



10. Locate and select the folder created in step 3.



11. Click **OK**.

12. Set **Type** to **http** and **Port** to **80**.

13. Ensure that the **IP address** and **Host name** fields are filled in with the correct information for the machine.
14. Ensure that **Start Website immediately** is selected.

The screenshot shows the 'Add Website' dialog box. The 'Site name' field is 'MSSQLSITE'. The 'Application pool' is 'MSSQLSITE'. The 'Physical path' is 'C:\www'. The 'IP address' is '192.168.81.107'. The 'Port' is '80'. The 'Host name' is 'MSSQL.di.ipdr'. The 'Start Website immediately' checkbox is checked.

15. Click **OK**.

2.6 GreenTec WORMdisks

See the *Installation of GreenTec Command Line Utilities* document, which should accompany the installation disk, for a detailed guide on how to install the GreenTec command line utilities.

Furthermore, refer to the *GT_WinStatus User Guide*, which should also accompany the installation disk, for instructions on how to effectively use GreenTec WORMdisks to preserve data. Read these instructions *carefully*, as locking GreenTec WORMdisks can result in making some or all of the disk or the entire disk unusable. Having portions of the disk or the entire disk permanently locked is sometimes desirable, but it is dependent on the needs of your organization, e.g., if you want to store backup information or logs securely.

The *GT_WinStatus User Guide* provides instructions for locking and temporarily locking disk sectors. In this practice guide, we will not include instructions on when to lock GreenTec WORMdisks. However, we will provide instructions detailing how to save data to these disks and various commands used in

manipulating the disks. Below, find descriptions of some commands useful for automation of GreenTec WORMdisks. Actual automation of these disks will vary per organization.

2.6.1 Format GreenTec WORMdisks

To format GreenTec WORMdisks for use, the following command can be used.

```
> gt_format.exe <disk number> /parts:<number of parts> /label:<id>
```

This command can be used to split a disk into a specified number of partitions, with each partition being labeled according to the label id specified.

For example, this command will split drive 1 into four parts, labeled DI001, DI002, DI003, and DI004:

```
> gt_format.exe 1 /parts:4 /label:DI
```

```
Formatting drive 1 partition 1 file system NTFS label "DI001"
```

```
Format successful
```

```
Formatting drive 1 partition 2 file system NTFS label "DI002"
```

```
Format successful
```

```
Formatting drive 1 partition 3 file system NTFS label "DI003"
```

```
Format successful
```

```
Formatting drive 1 partition 4 file system NTFS label "DI004"
```

```
Format successful
```

2.6.2 Obtain Status Information About GreenTec WORMdisks

To verify information about GreenTec WORMdisks, use the following command.

```
> wvlist.exe <drive number>
```

This command can be used to display basic information about a drive, such as the amount of space of each partition, whether it is a WORMdisk, whether they have been locked, and what drive letter to which they are mapped.

For example, this command will list the characteristics of drive 1.

```
> wvlist.exe 1
```

WVLIST: List WORM Volume (WDV) Status on Physical WORMdisks(tm).

Copyright (C) 2015 GreenTec-USA, Inc. All rights reserved.

```
Drive#=1  Type=ATA  F/W=GT5G  Size=500{GB}
```

```
> IS WORM          > IS *NOT* Finalized
```

```
**** WORMdisk Volume (WDV) Info ****
```

WDV #	TB	ENFORCED	GREENTEC	TLOCKED
001	0.125	NO	YES	NO G:\
002	0.125	NO	YES	NO H:\
003	0.125	NO	YES	NO I:\
004	0.125	NO	YES	NO J:\

2.6.3 Map GreenTec WORMdisks to Drive Letters

1. To unmap a partition from a drive letter, use the following command:

```
> wvmap.exe <drive letter>:
```

For example,

```
> wvmap.exe H:
```

will unmap *H:*, making it available for mapping to another partition.

2. To map a partition to a drive letter, use the following command:

```
> wvmap.exe <drive letter>: <drive number>.<partition number>
```

For example,

```
> wvmap.exe H: 1.2
```

will map the second partition of drive 1 to *H:*, making files available through accessing that drive letter.

3. To map the next partition to a drive letter, use the following command:

```
> wvnext.exe <drive letter>:
```

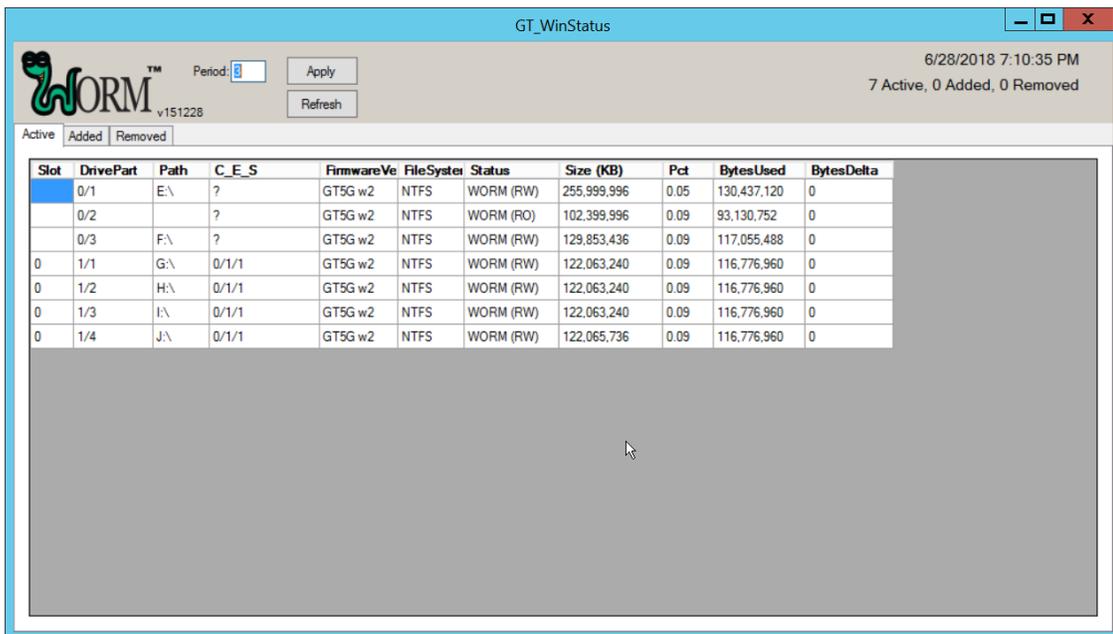
For example, if *H:* is mapped to partition 2 of drive 1 (1.2)

> wvnext.exe H:

will attempt to map *H:* to partition 3 of drive 1 (1.3).

2.6.4 Activate Write Protection in GreenTec WORMdisks

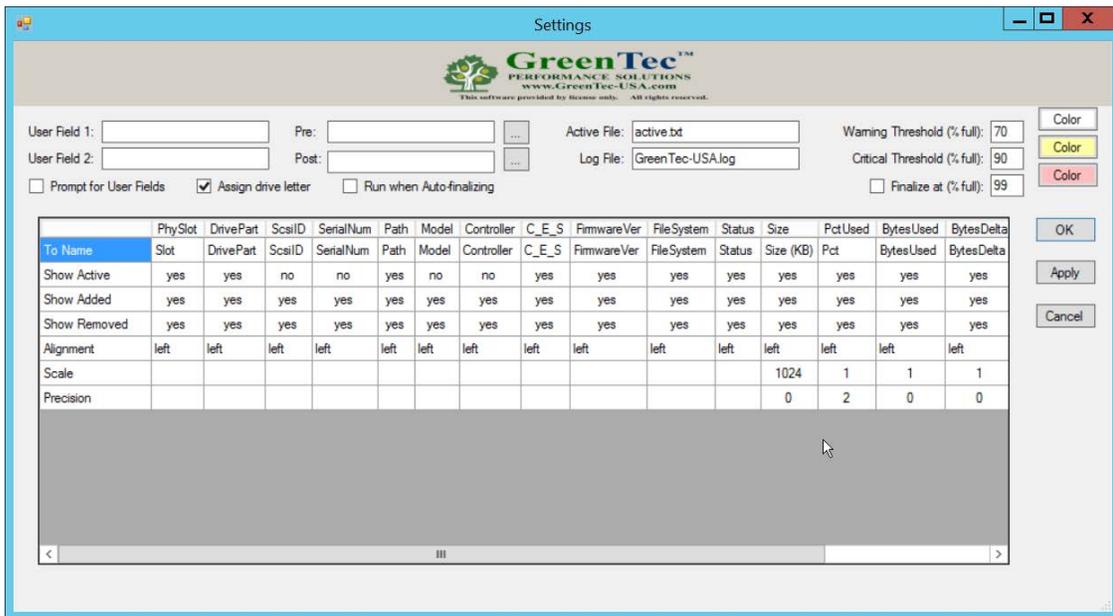
1. Running GT_WinStatus.exe will open the Graphical User Interface (GUI), which displays various information such as drive mappings, partitions, total space, and space used, as well as a range of other options.



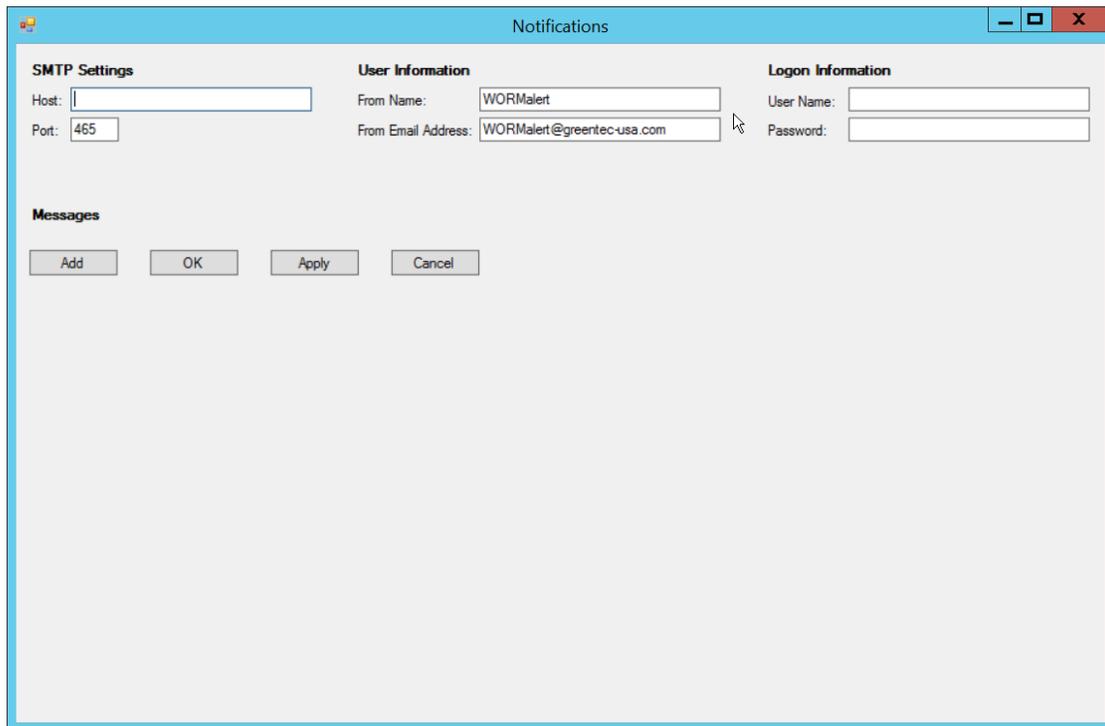
The screenshot shows the GT_WinStatus application window. The title bar reads "GT_WinStatus". The interface includes a logo for "WORM v151228", a "Period:" field with a dropdown menu, and "Apply" and "Refresh" buttons. The top right corner displays the date and time "6/28/2018 7:10:35 PM" and the status "7 Active, 0 Added, 0 Removed". Below this is a tabbed interface with "Active", "Added", and "Removed" tabs. The "Active" tab is selected, showing a table with the following columns: Slot, DrivePart, Path, C_E_S, FirmwareVer, FileSystem, Status, Size (KB), Pct, BytesUsed, and BytesDelta. The table contains 10 rows of data.

Slot	DrivePart	Path	C_E_S	FirmwareVer	FileSystem	Status	Size (KB)	Pct	BytesUsed	BytesDelta
0/1	E:\	?		GT5G w2	NTFS	WORM (RW)	255,999,996	0.05	130,437,120	0
0/2		?		GT5G w2	NTFS	WORM (RO)	102,399,996	0.09	93,130,752	0
0/3	F:\	?		GT5G w2	NTFS	WORM (RW)	129,853,436	0.09	117,055,488	0
0	1/1	G:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0
0	1/2	H:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0
0	1/3	I:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0
0	1/4	J:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,065,736	0.09	116,776,960	0

2. More columns can be added by right-clicking anywhere in the **Active** window, opening the **Settings** window.



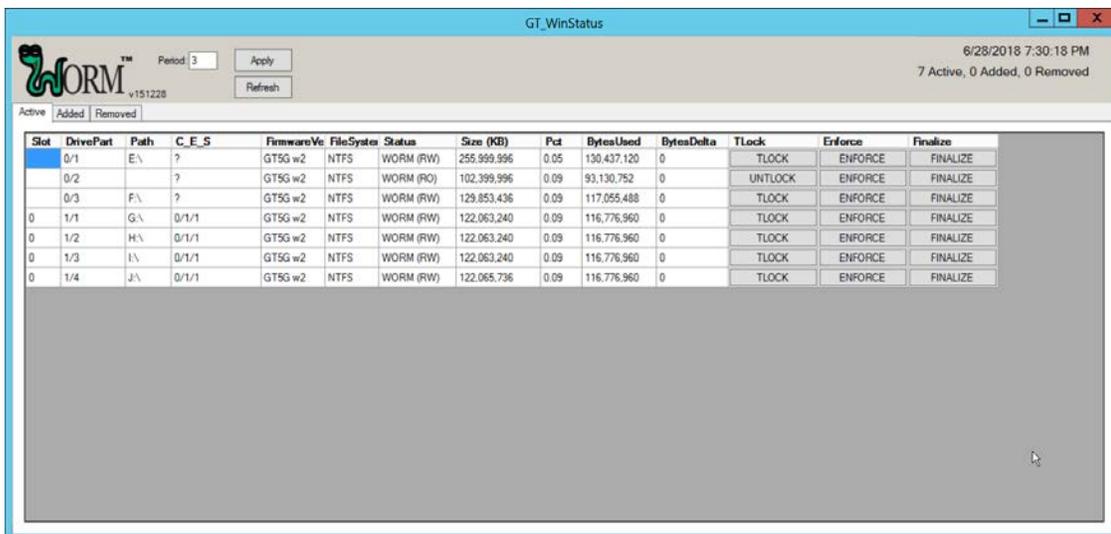
3. In the Settings window, **User Field 1** and **User Field 2** are for any metadata to be stored for a drive. **Pre:** runs a script prior to finalizing a drive, and **Post:** runs a script after finalizing a drive.
4. Also, from the **Settings** window, right-clicking on **Critical Threshold** or **Warning Threshold** will allow the user to set up alert preferences for drives that are nearly full (at a configurable percent value).



5. To display the GUI with options to lock and enforce locks on drives, the following command must be used to start the GUI:

```
> GT_WinStatus.exe /tlock /enf
```

- This will add columns called **TLock** and **Enforce** (as well as the ability to use the **Finalize** column).



- The **TLock** column temporarily locks/unlocks a partition of the drive. This is useful to prevent modification during times when modification should be disallowed.

Important: The following functions in steps 8 and 9 will permanently lock portions of the drive, making them read-only.

The Enforce function permanently locks all volumes up to the enforced volume.

The Finalize function permanently locks the entire drive.

- The **Enforce** column is a *permanent incremental lock*. This means that it permanently prevents modification for the selected volume of a drive as well as all volumes that come before that volume on the drive. Once these sections are enforced, they cannot be written to ever again. This functionality is particularly useful in protecting data or backups that must never be modified, but as the enforce function is permanent, it must be used carefully.
- The **Finalize** column permanently locks the entire drive. This is useful when a drive is full and no longer needs to be written to. Data can still be read and copied from this drive to other places, but no write actions will be possible after this is used, so it also must be used carefully.

2.7 CryptoniteNXT

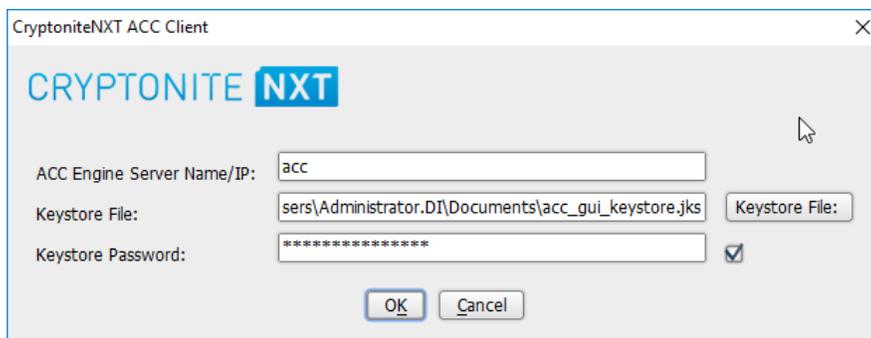
See the *CryptoniteNXT 2.6.2 Unified Installation Guide*, which should accompany the device for a detailed guide on how to install **CryptoniteNXT** on the provided device.

The *CryptoniteNXT 2.6.2 Unified Installation Guide* provides a full installation on both the **CryptoniteNXT** device and the management workstation. When finished, it should be possible to log in on the management workstation and interact with the **CryptoniteNXT ACC GUI**. Instructions are provided below for performing various useful functions, including adding new devices/users, as well as creating policy, but specific recommendations for policy are not provided, as those will be specific to the organization. Some integrations with other security products used in this guide will be provided, as exceptions for those products in CryptoniteNXT are often necessary for their functionality.

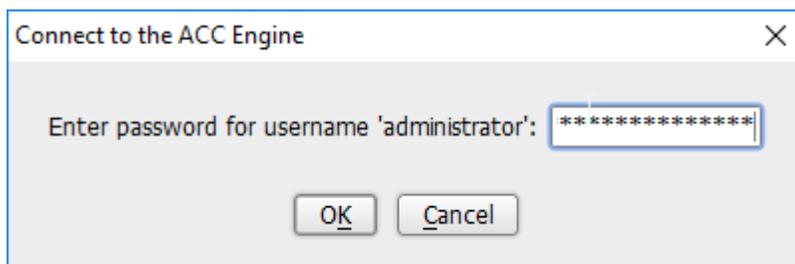
2.7.1 Configure Cryptonite NXT

2.7.1.1 Verify a New Device

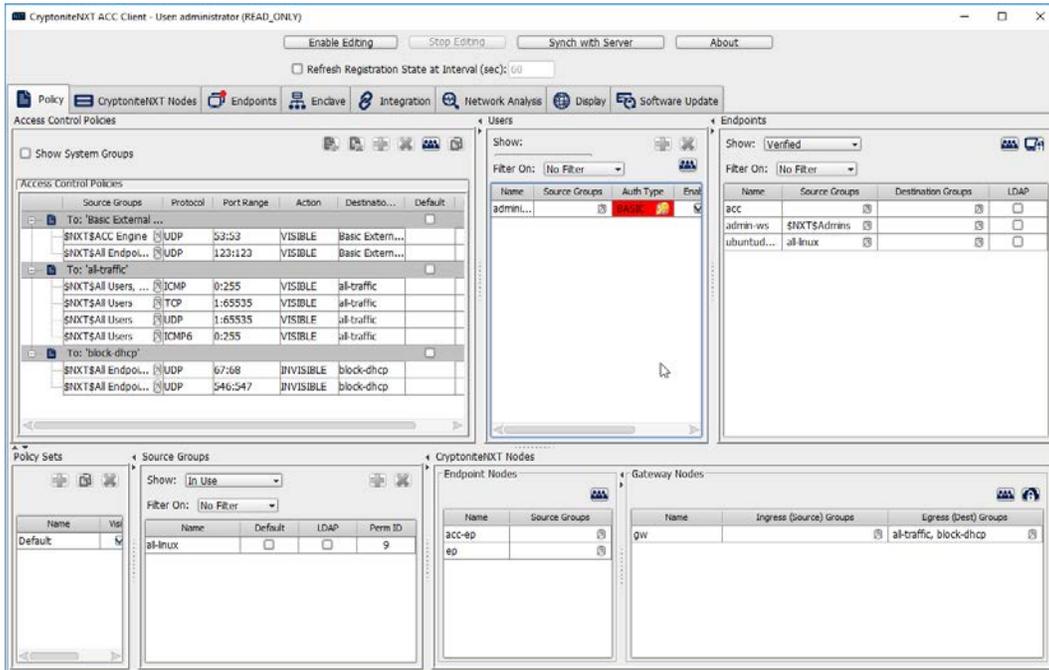
1. Open the **CryptoniteNXT ACC GUI** application.



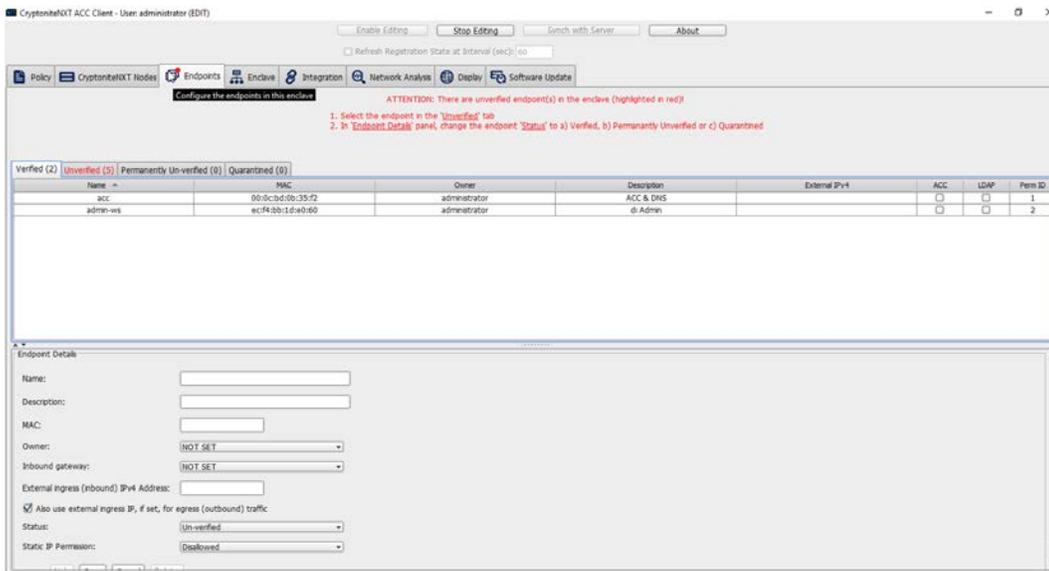
2. Click **OK**.
3. Enter the **password** for the account created during the installation.



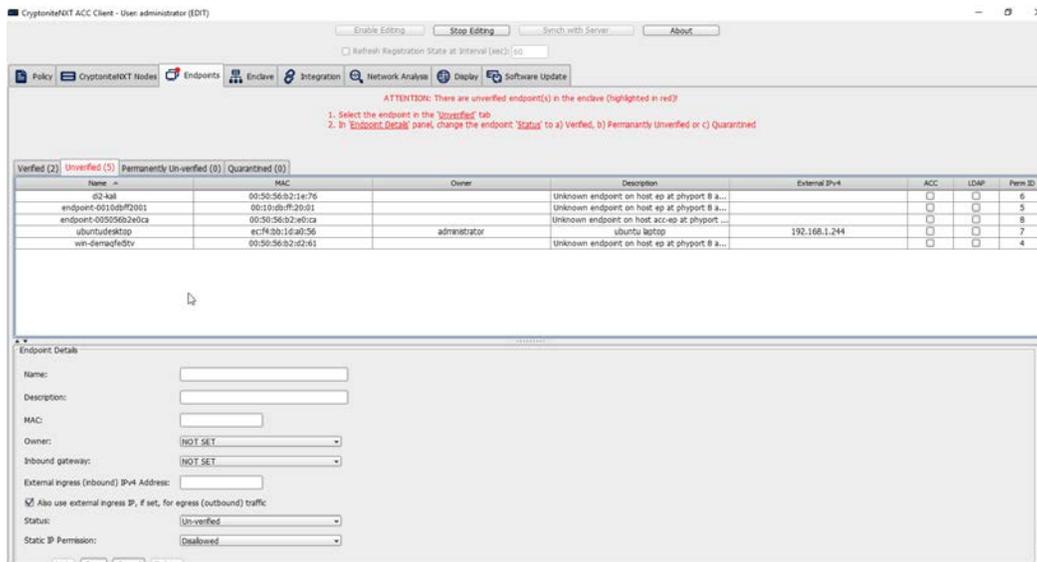
4. Click **OK**.



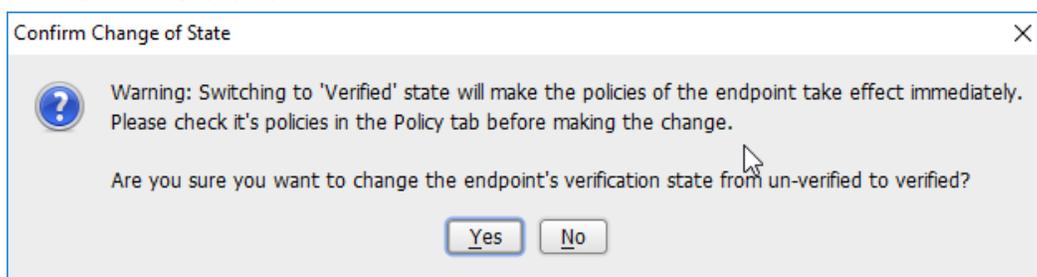
5. Click **Enable Editing** at the top of the application.
6. Click the **Endpoints** tab.



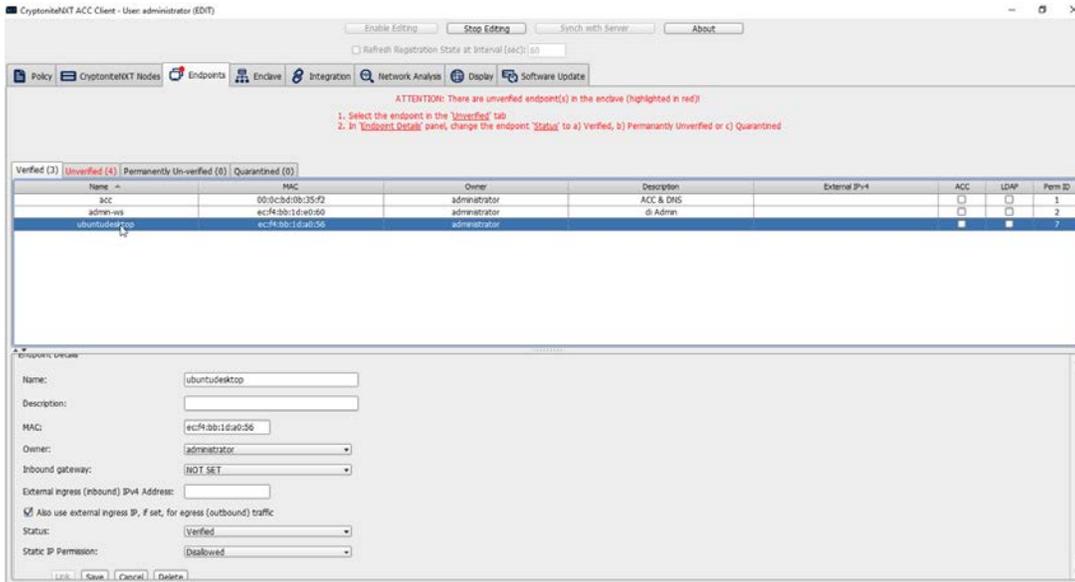
7. Click the **Unverified** tab. Any new devices connected to the network should appear here, if configured to use Dynamic Host Configuration Protocol (DHCP).



8. Click the machine to verify.
9. Enter a **name**.
10. Enter a **description** of the machine.
11. Select an **owner** if desired. If not selected, the owner will be the first user to log in to CryptoniteNXT on the machine.
12. Leave **Inbound gateway**: as **NOT SET** to have it choose a default gateway.
13. Leave **External ingress (inbound) IPv4 Address**: blank.
14. Ensure the box next to **Also use external ingress IP, if set, for egress (outbound) traffic** is checked.
15. Set **Status**: to **Verified**.

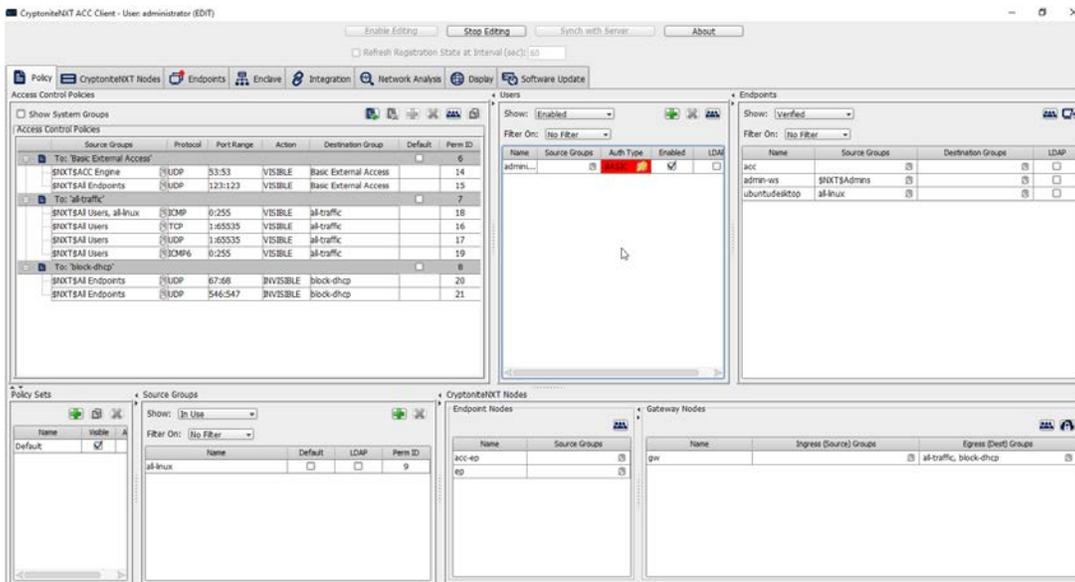


16. Click **Yes**.
17. Click **Save**.
18. The machine should now appear in the **Verified** tab.

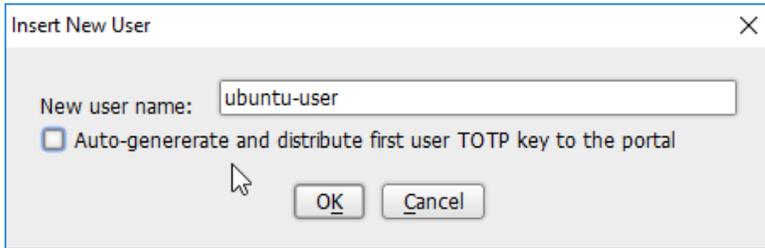


2.7.1.2 Create a New User

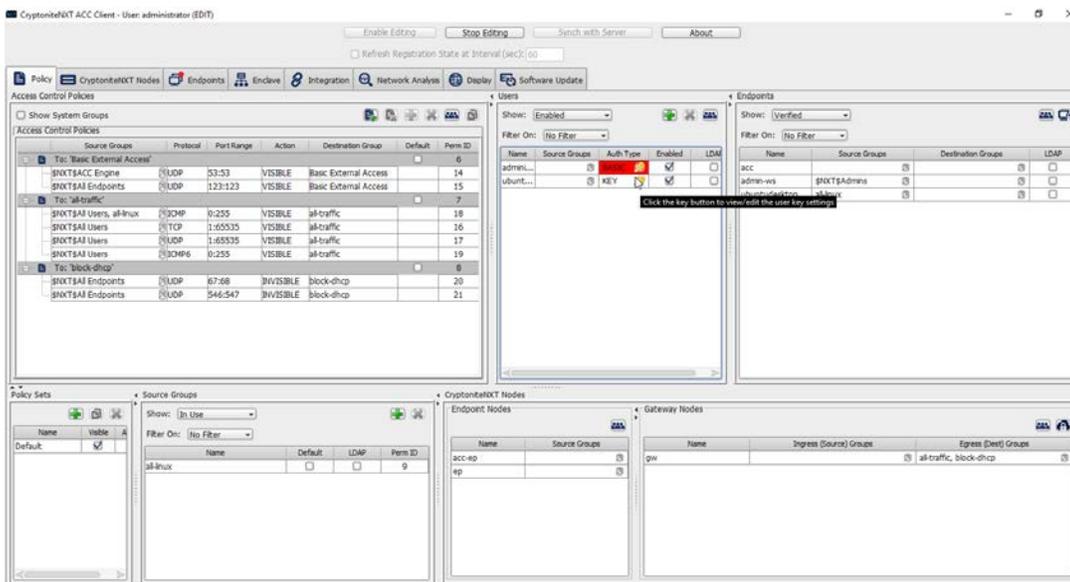
1. Go to the Policy tab.



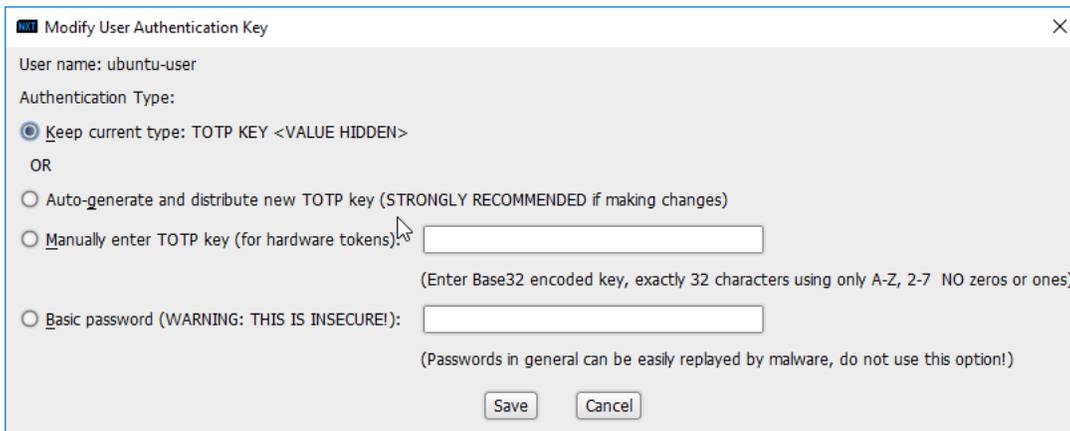
2. Right-click in the **Users** window and select **New User**.
3. Enter the username, and uncheck the box next to **Auto-generate and distribute first user TOTP key to the portal**.



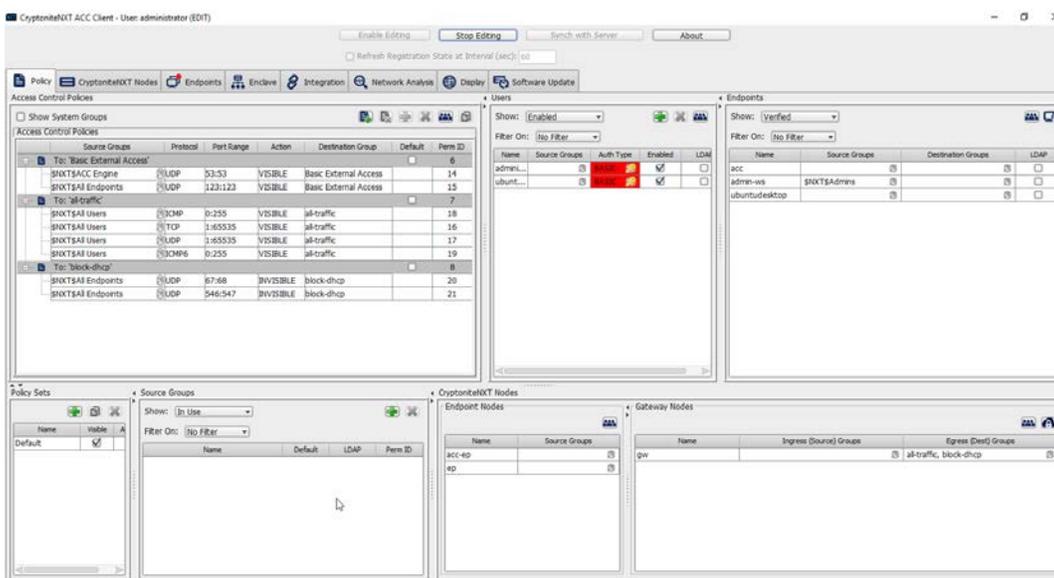
4. Click **OK**.



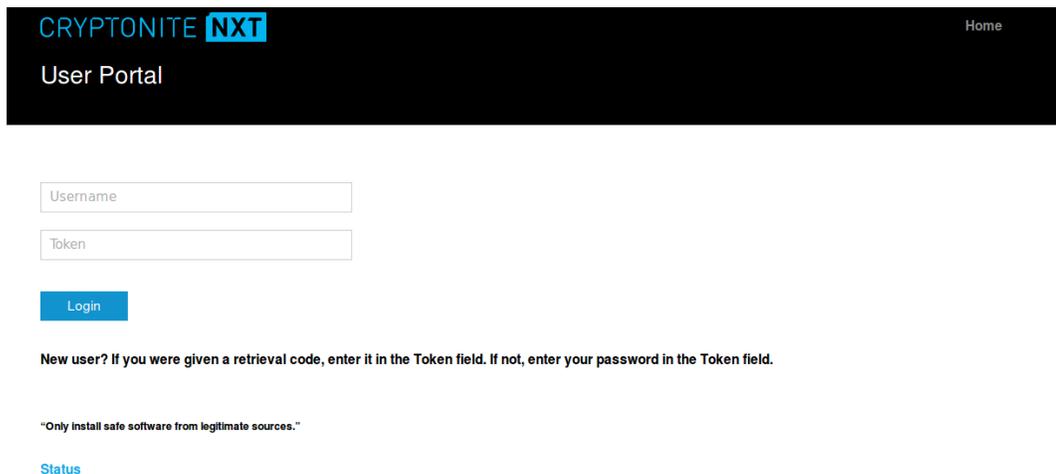
5. The new user should show up in the **Users** window. Click the key icon for the newly created user under **Auth Type**.
6. Decide on an authentication method for the user. (Note: It is not recommended to use passwords, but as this authentication decision depends on the needs of the organization, passwords are used for the purposes of this practice guide.)



7. Click **Save**.



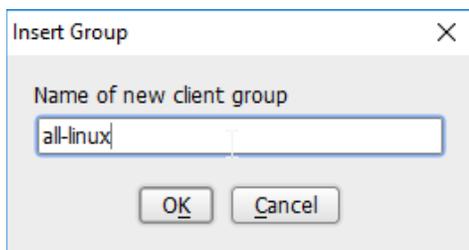
8. On the client machine, the user should be required to sign in on the CryptoniteNXT portal to access the internet. Authenticate using the newly created user.



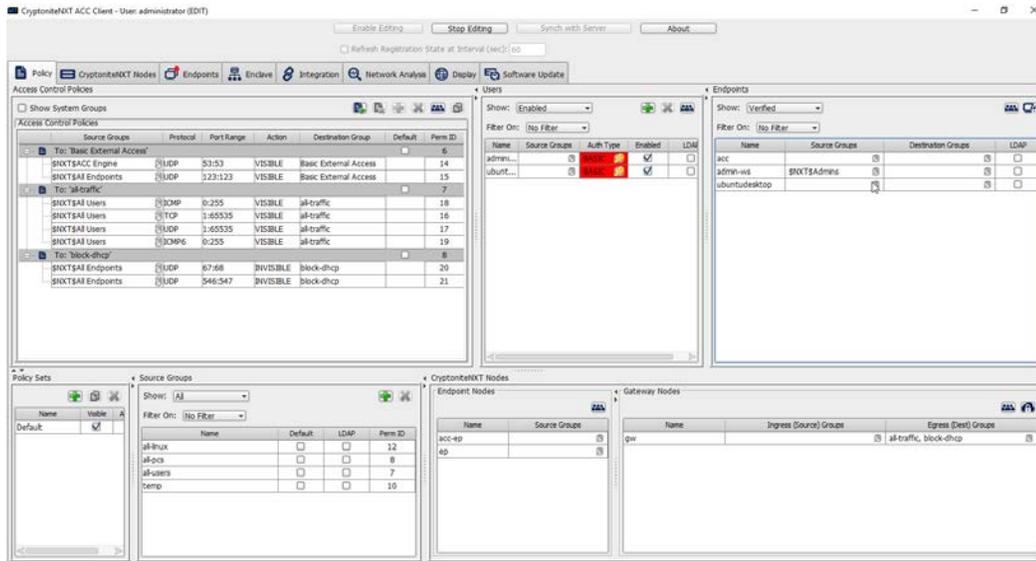
2.7.1.3 Create a New Policy

Creating policy in CryptoniteNXT essentially requires specifying allowed types of traffic. To do this, source groups and destination groups are created.

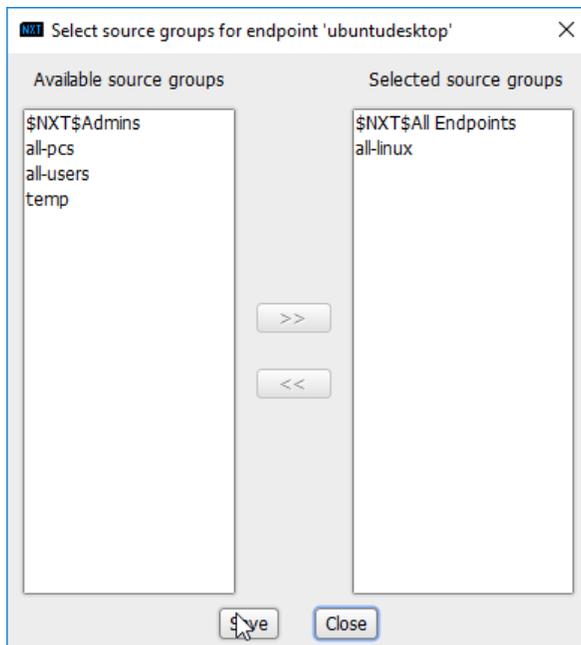
1. To create a source group, right-click in the **Source Groups** window and select **New Source Group**.
2. Enter the name of the group.



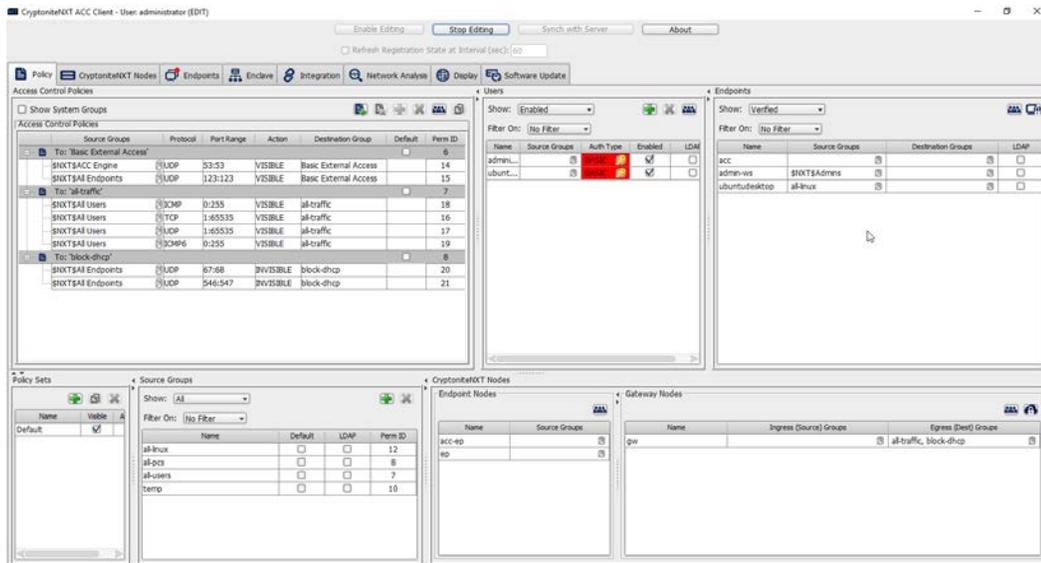
3. Click **OK**.
4. The newly created group should appear in the **Source Groups** window.



5. In the **Endpoints** window, click the arrow button under the **Source Groups** column for any machines to be added to this **Source Group**.
6. Select the newly created group (or groups).
7. Click the >> button to add the endpoint to this group.

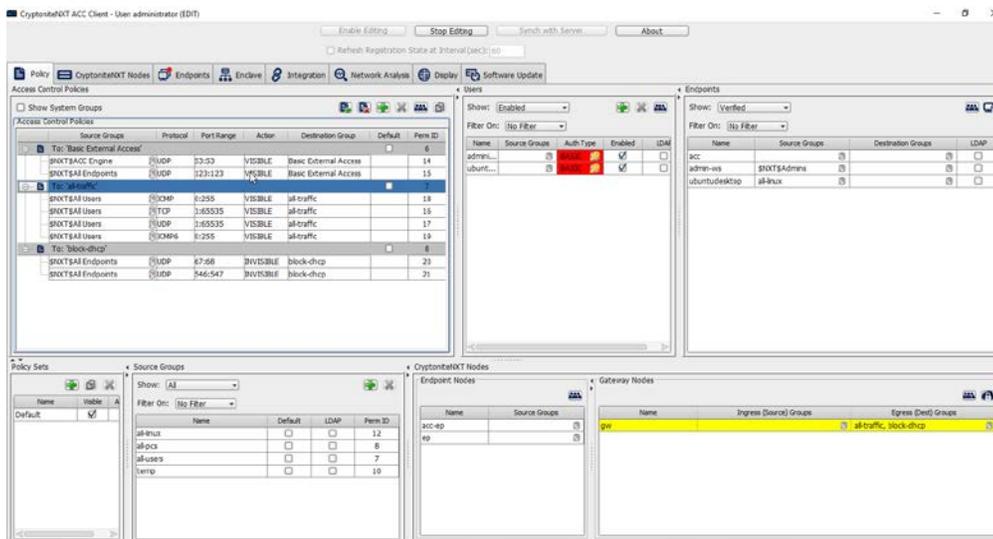


8. Click **Save**.
9. The group should show under the **Source Groups** column for those endpoints.



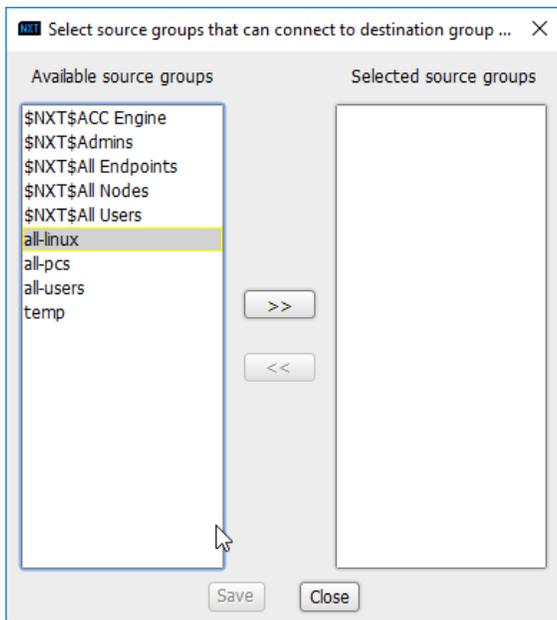
Destination groups are used to govern the allowed destinations of endpoints within certain source groups. While destination groups can be created according to organizational property, this example uses an existing group, **all-traffic**.

1. To allow or prevent the use of ping, we add it to the **all-traffic** group. In the **Access Control Policies** window, right-click on the row labeled **To: 'all-traffic'** and select **New Access Control Policy Entry**.

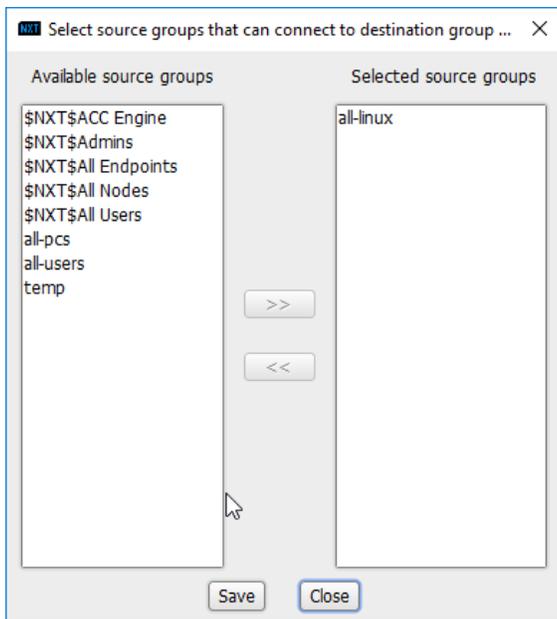


2. Click the arrow button under the **Source Groups** column.

3. Select the newly created source group.

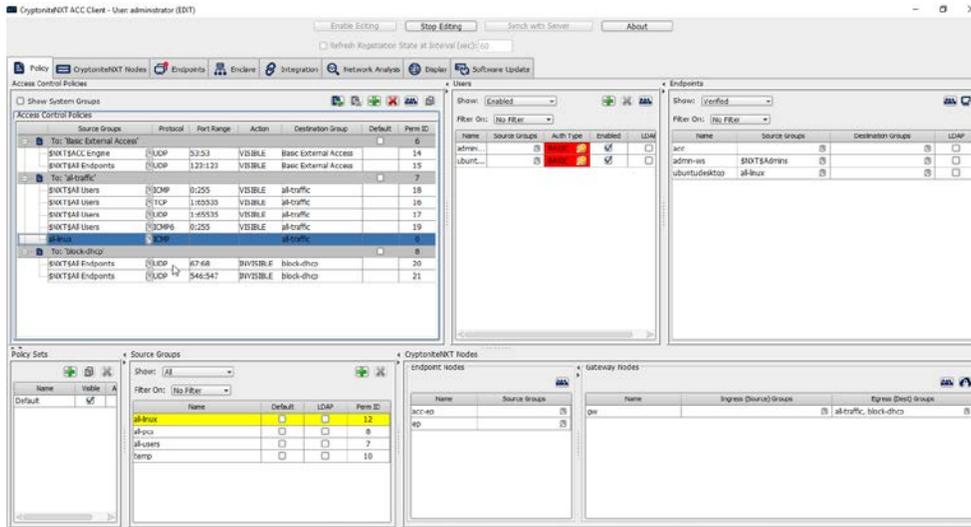


4. Click the >> button.

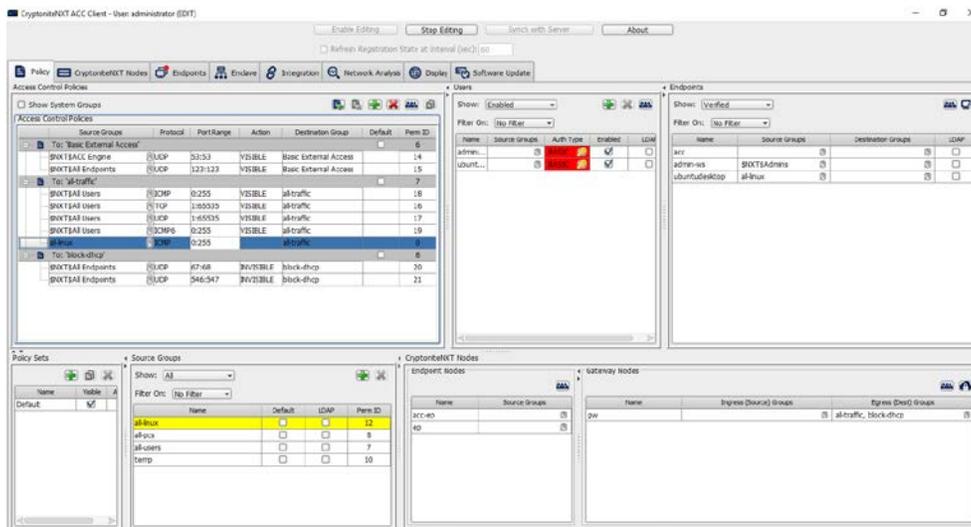


5. Click **Save**.

6. Select the **Protocol**. In this case, to prevent the machine from using ping, we choose **ICMP**.

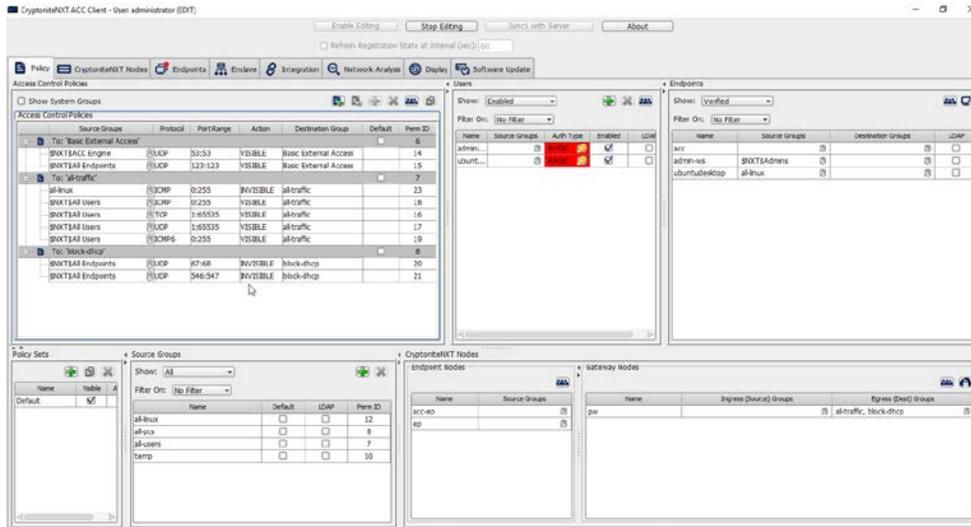


7. Enter the port range that this traffic can operate on.

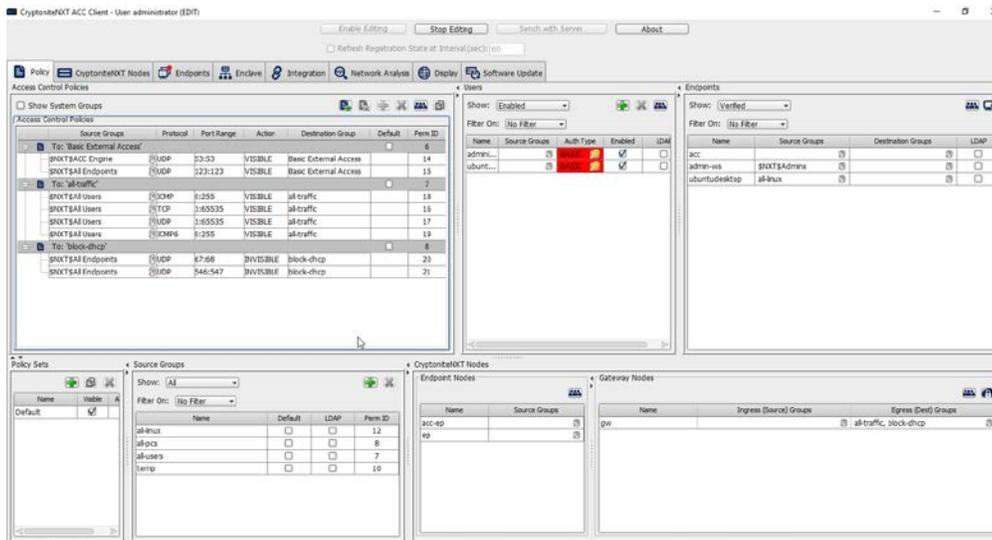


8. Select **INVISIBLE** for the **Action** column.

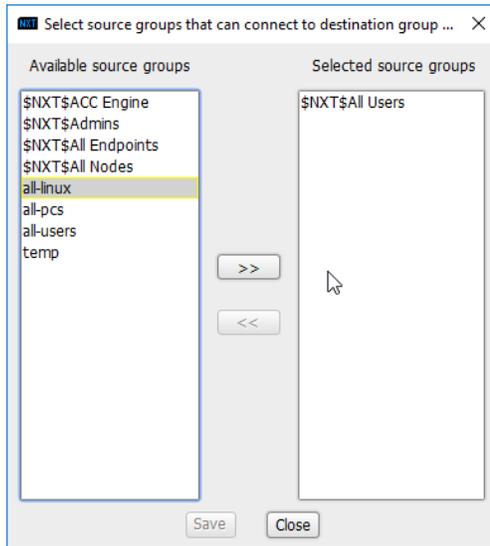




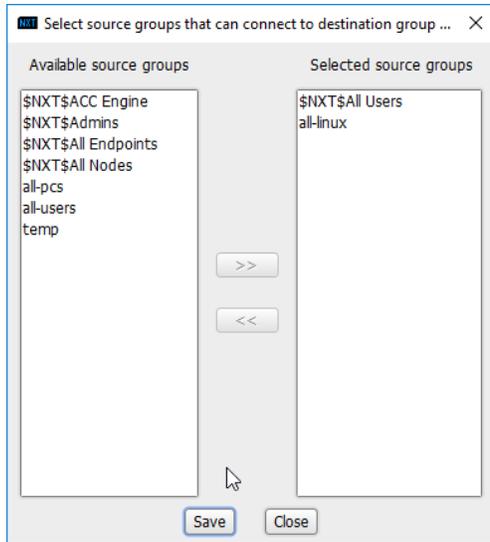
9. This will prevent the members of this group from using ping.
10. To allow the members of this group to use ping, delete this rule. Right-click the entry and select **Delete Access Control Policy Entries**.



11. Add the newly created group to the existing policy entry by clicking the arrow for that entry under **Source Groups**.
12. Select the newly created group.

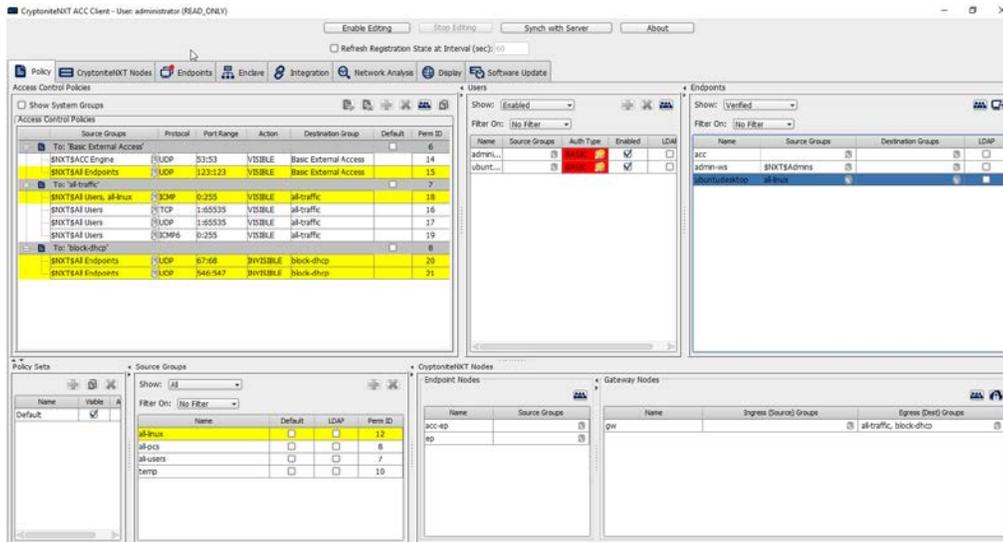


13. Click the >> button.



14. Click **Save**.

15. Click **Stop Editing** when finished.



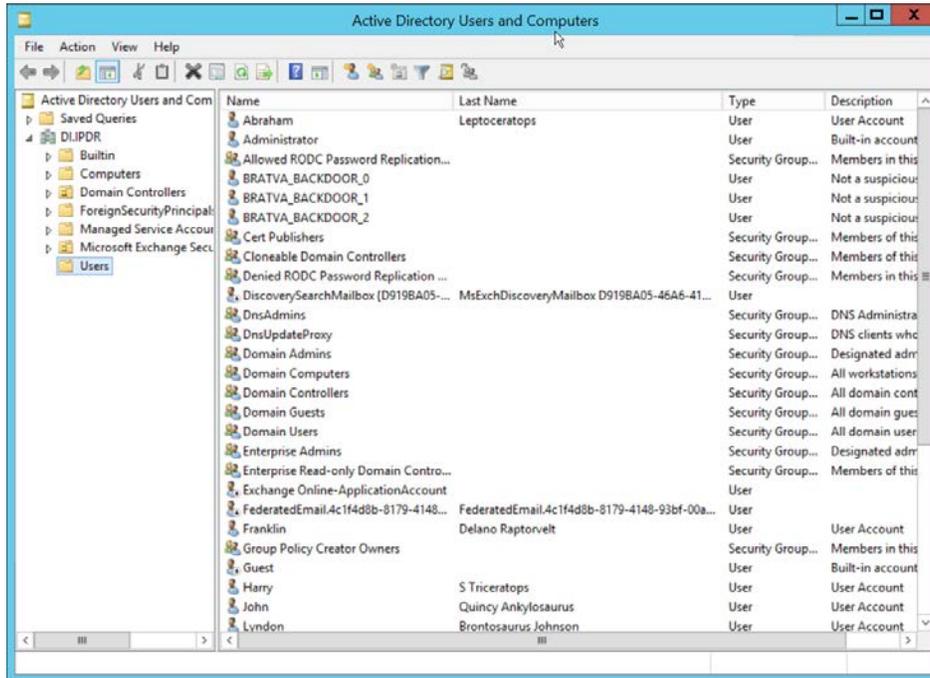
16. Now, the new machine should be allowed to use ping. With these policies it is possible to manage all traffic through the specification of groups, ports, and protocols.

2.7.2 Integrate CryptoniteNXT with Active Directory

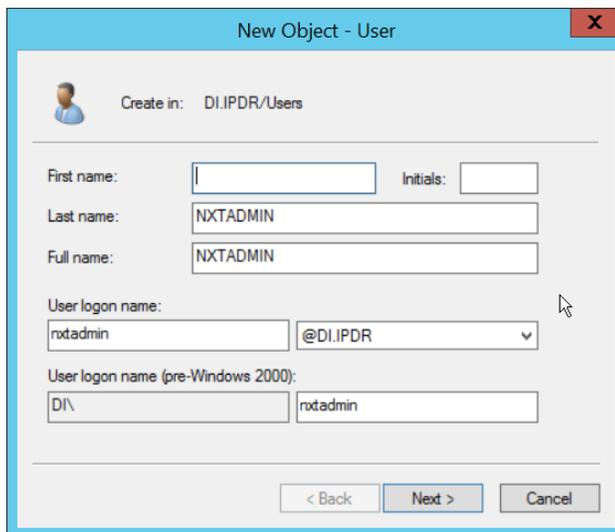
In this section, devices listed in Active Directory will be imported into CryptoniteNXT. For this to be successful, the DNS server must have reverse lookup zones configured for the AD server. Please see [Section 2.1.6](#) for setting up reverse lookup zones on the AD/DNS server.

2.7.2.1 Generate a Keytab File

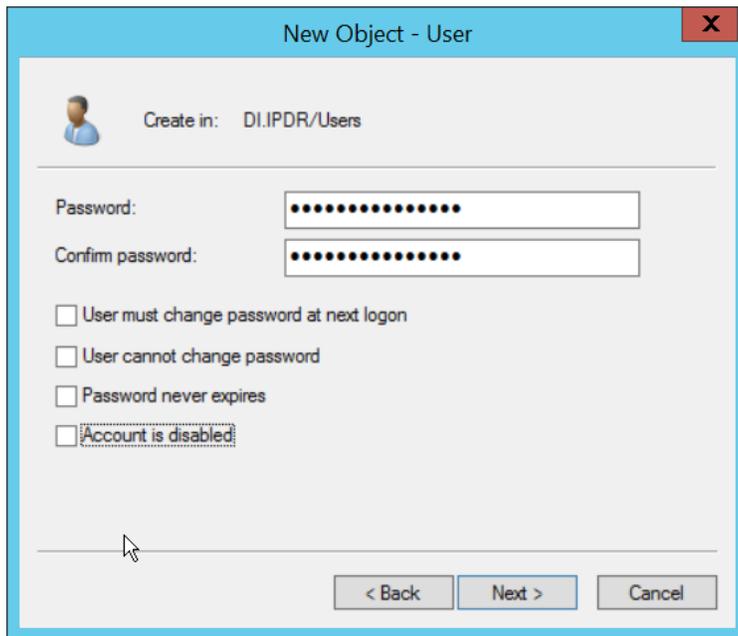
1. Open **Active Directory Users and Computers**.



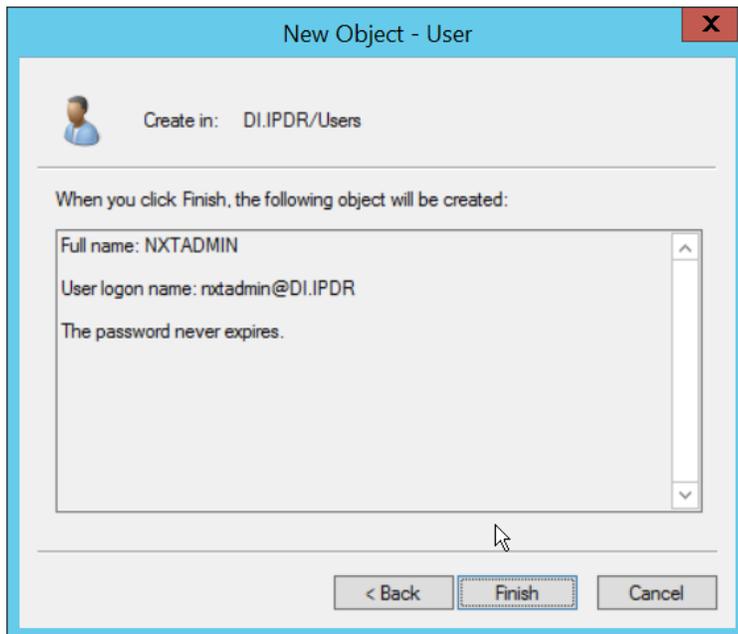
2. Right-click the **Users** folder in the left pane and select **New > User**.
3. Enter a **name** for this user, such as **nxtadmin**.



4. Click **Next**.
5. Enter a **password** for this user, and set the password policy.



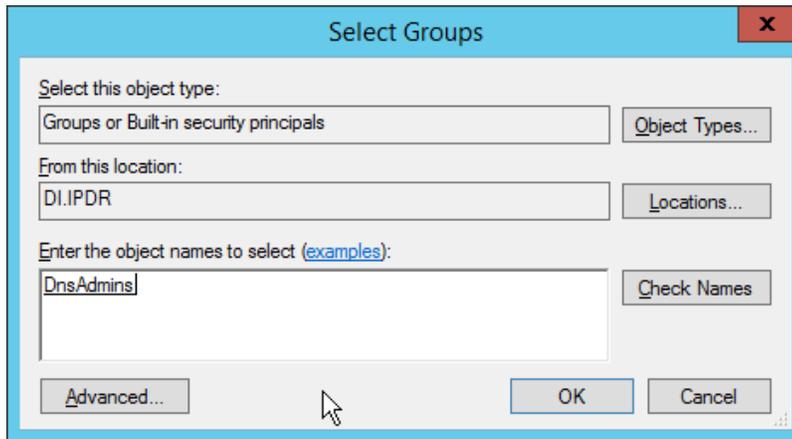
6. Click **Next**.



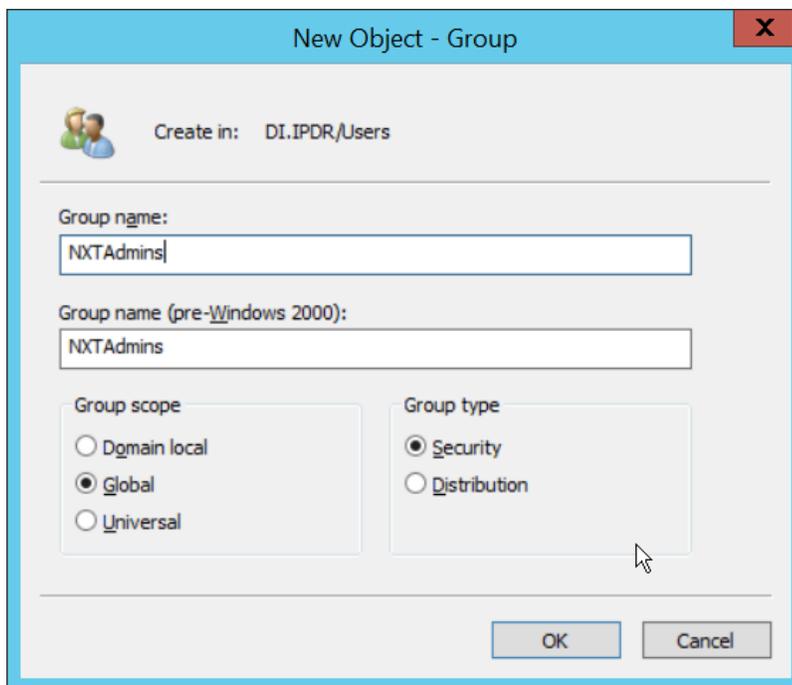
7. Click **Finish**.

8. Right-click the newly created user and select **Add to a group....**

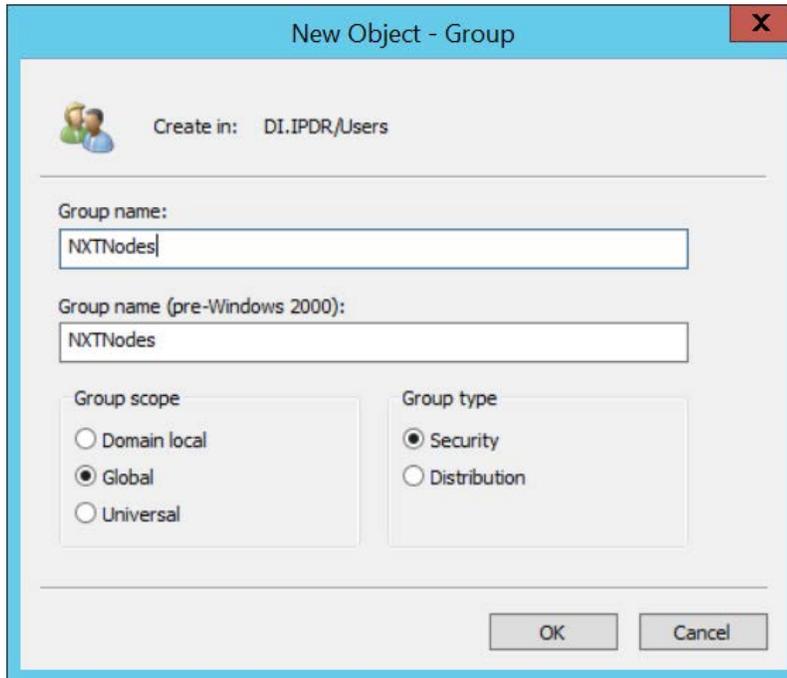
9. Enter **DnsAdmins**.



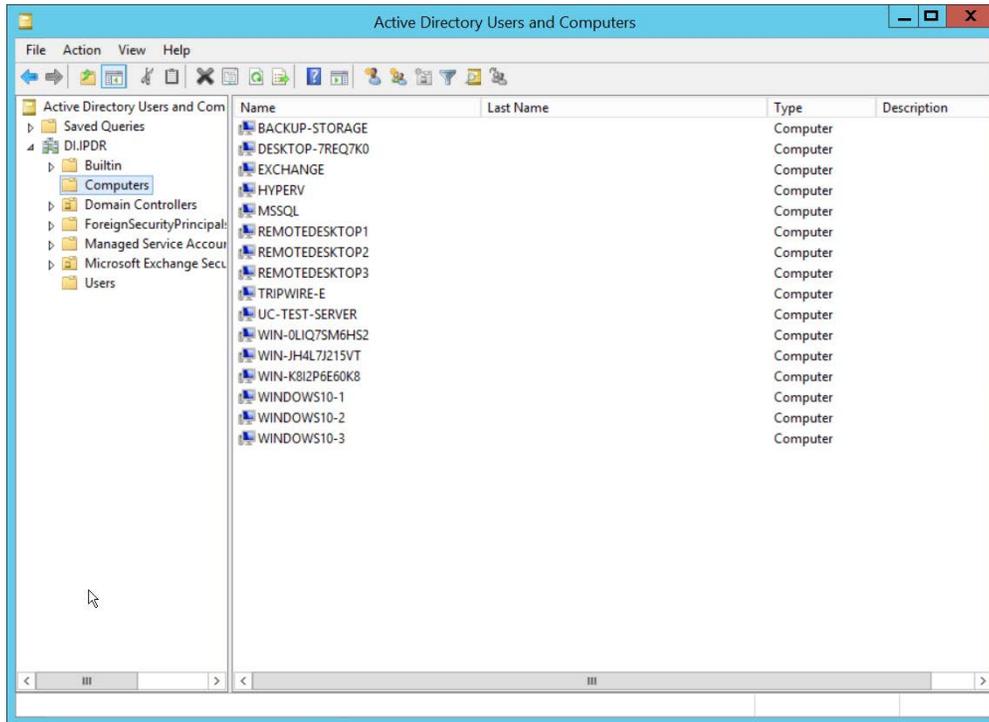
10. Click **OK**.
11. Right-click the **Users** folder in the left pane and select **New > Group**.
12. Enter **NXTAdmins** as the group name.



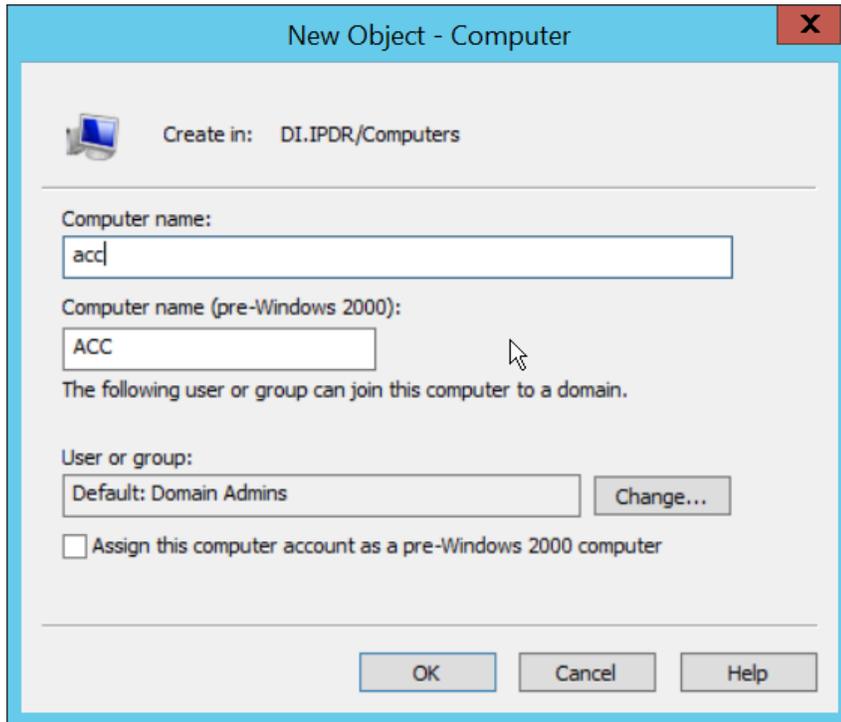
13. Click **OK**.
14. Right-click the **Users** folder in the left pane and select **New > Group**.
15. Enter **NXTNodes** as the group name.



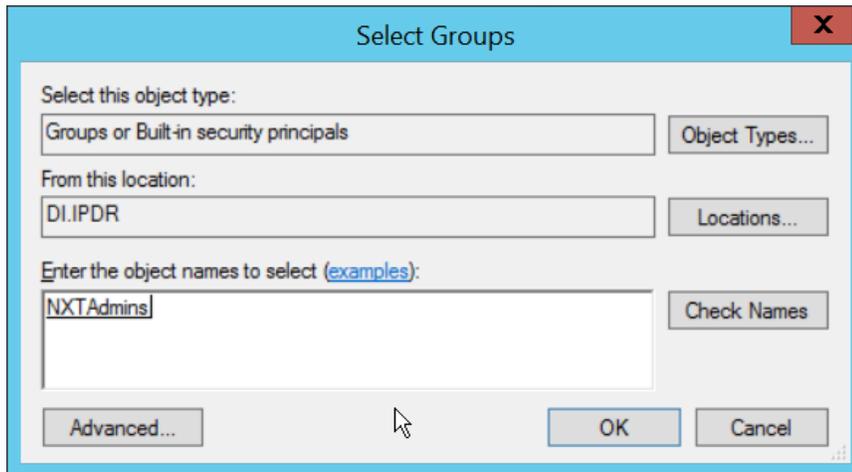
16. Click **OK**.
17. Click **Computers** in the left pane.



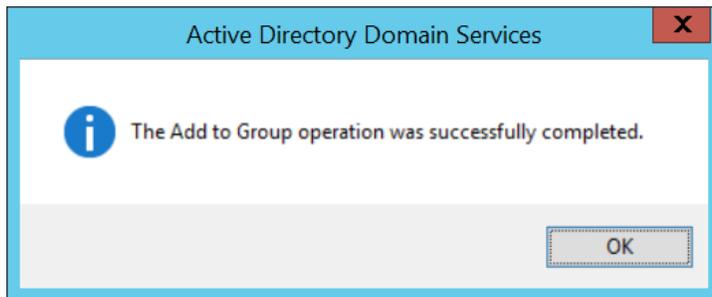
18. Right-click **Computers** in the left pane and select **New > Computer**.
19. Enter the name of the **acc** server for **CryptoniteNXT** (Node A).



20. Click **OK**.
21. Right-click the newly created computer and select **Add to a group....**
22. Enter **NXTAdmins** in the box labeled **Enter the object names to select (examples):**.



23. Click **OK**.



24. Click **OK**.
25. Open a new Administrator **PowerShell** window.
26. Enter the following command, using the newly created user in the **DnsAdmins** group:

```
> ktpass -princ DNS/<user>.<domain>@<DOMAIN> -mapuser  
<user>@<domain> -pass <user password> -out .\<keytab filename>  
-ptype krb5_nt_principal -crypto all
```

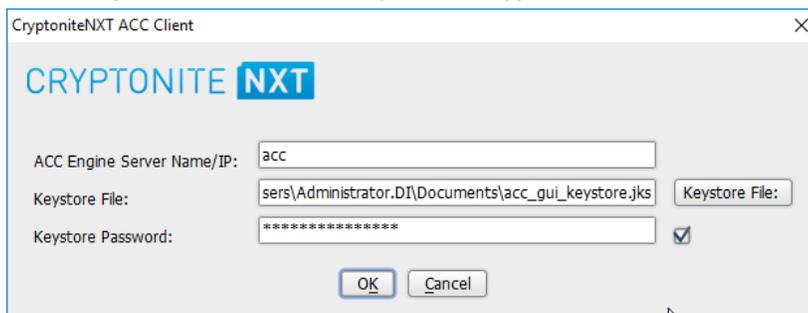
For example:

```
> ktpass -princ DNS/nxtadmin.di.ipdr@DI.IPDR -mapuser  
nxtadmin@di.idpr -pass password123 -out .\keytab.out -ptype  
krb5_nt_principal -crypto all
```

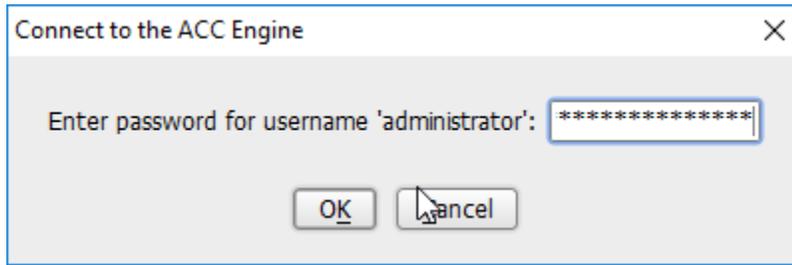
27. This will produce a keytab file. Copy this file to the CryptoniteNXT Management workstation.

2.7.2.2 Import Keytab File to ACC

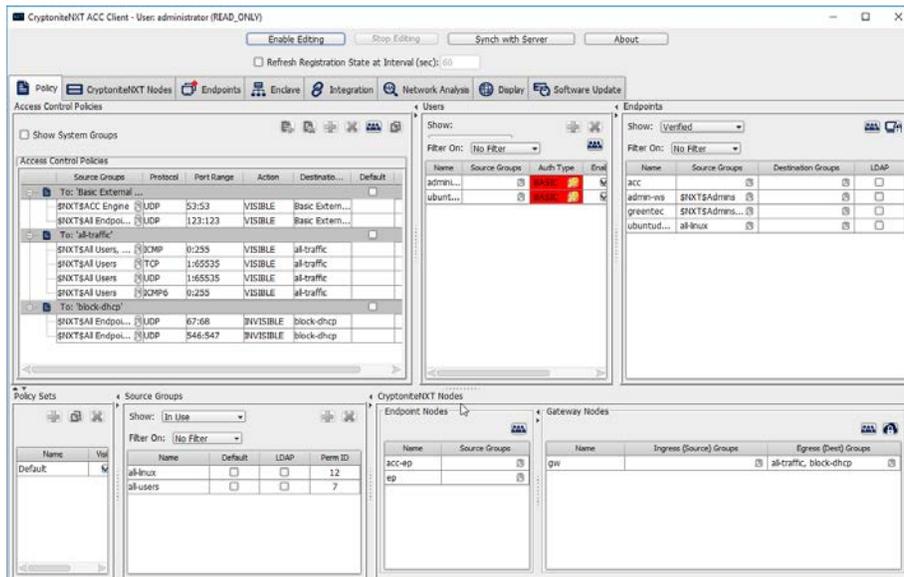
1. On the management workstation, open the **CryptoniteNXT ACC GUI**.



2. Click **OK**.
3. Enter the **password** configured during installation.



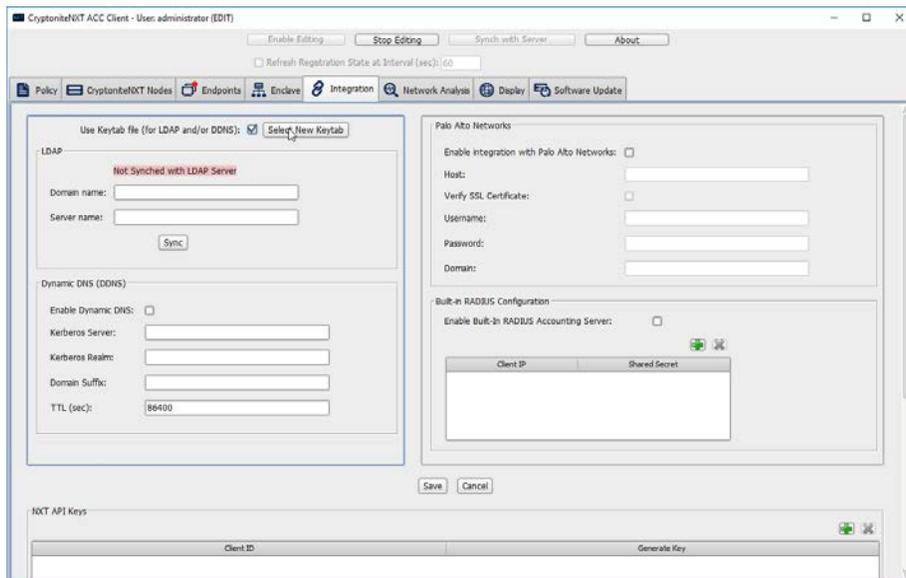
4. Click **OK**.



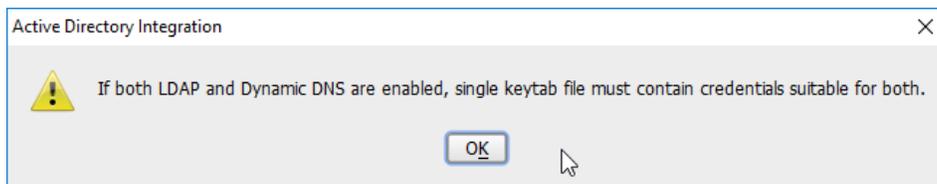
5. Click **Enable Editing**.

6. Click the **Integration** tab.

7. Check the box next to **Use Keytab file (for LDAP and/or DDNS):**.

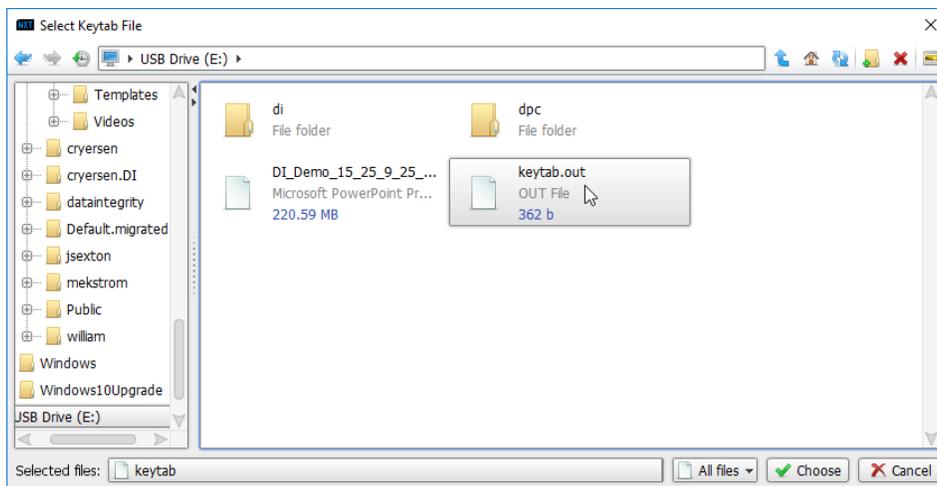


8. Click **Select New Keytab**.



9. Click **OK**.

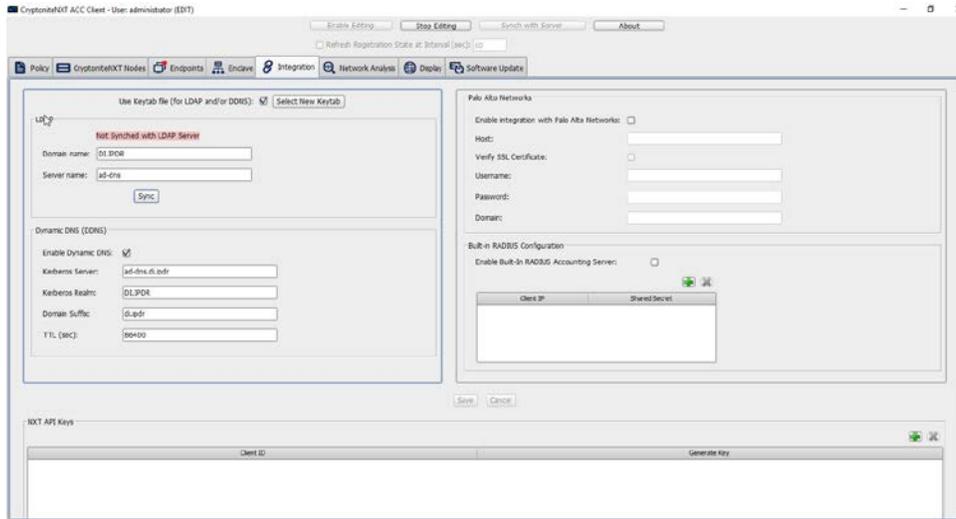
10. Navigate to the keytab file.



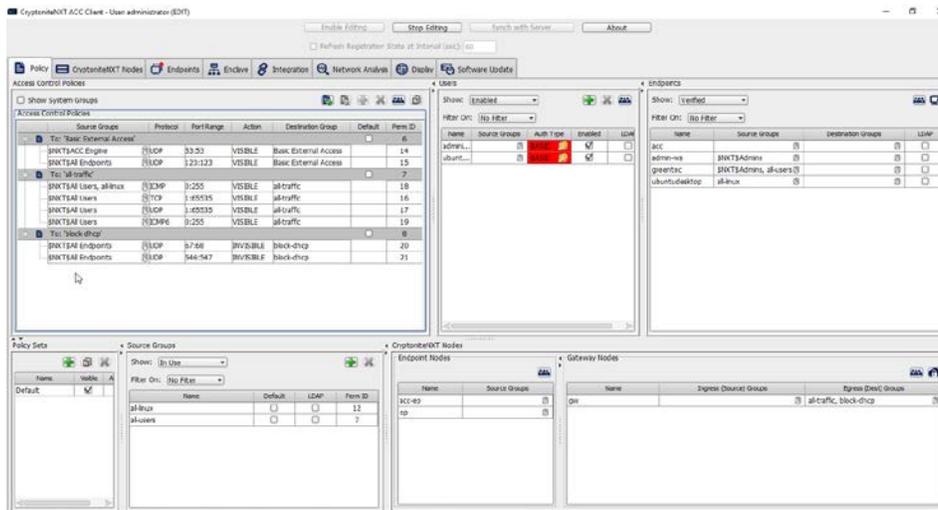
11. Click **Choose**.

12. Click **Save**.

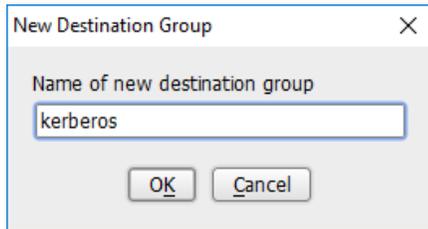
13. Under **LDAP**, enter the **Domain name** (such as DI.IPDR) and the **Server name** (such as ad-dns).
14. Check the box next to **Enable Dynamic DNS:**
15. Enter the **fully qualified domain name** of the DNS server (such as ad-dns.di.ipdr).
16. Enter the **Kerberos realm** (such as DI.IPDR).
17. Enter the **domain suffix** (such as di.ipdr).



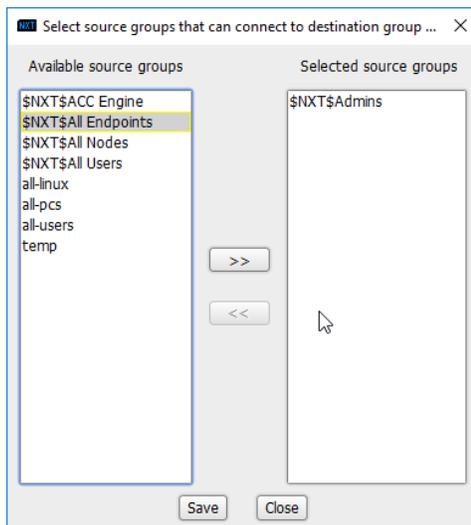
18. Click **Save**.
19. Click the **Policies** tab.



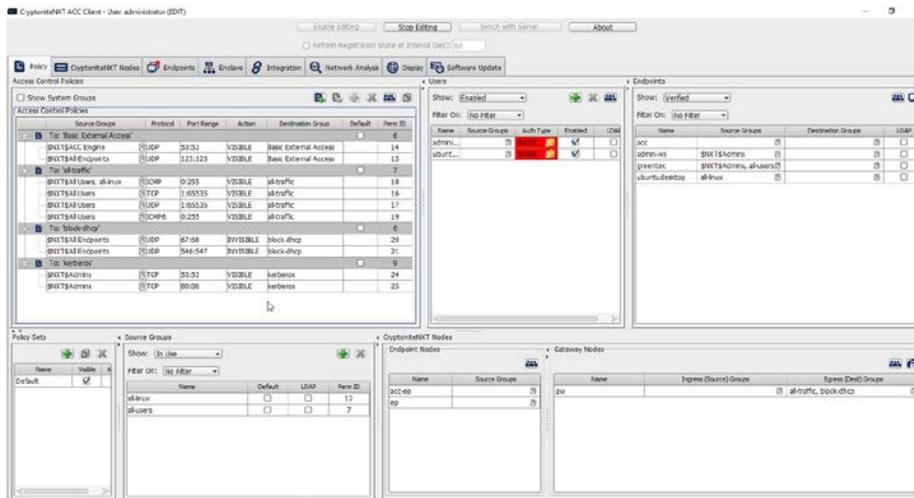
20. Right-click in the **Access Control Policies Window** and select **New Destination Group**.
21. Enter **kerberos**.



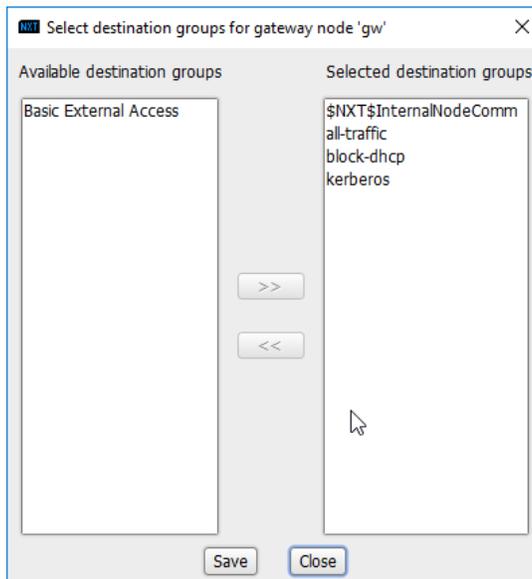
22. Click **OK**.
23. Select **TCP** under **Action**.
24. Enter 53:53 under **Port Range**.
25. Select **VISIBLE** under **Action**.
26. Click the arrow under **Source Groups**.
27. Select **\$NXT\$Admins**.
28. Click the >> button.



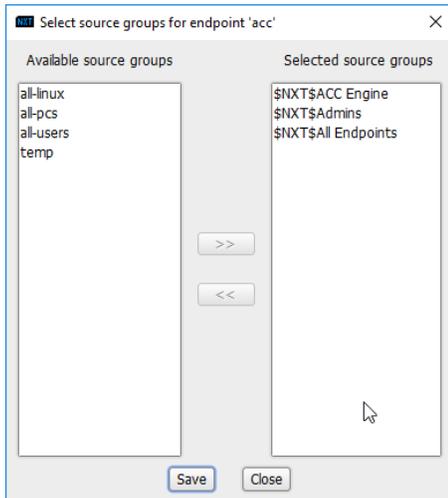
29. Click **Save**.
30. Right-click the **To: 'kerberos'** destination group, and select **New Access Control Policy Entry**.



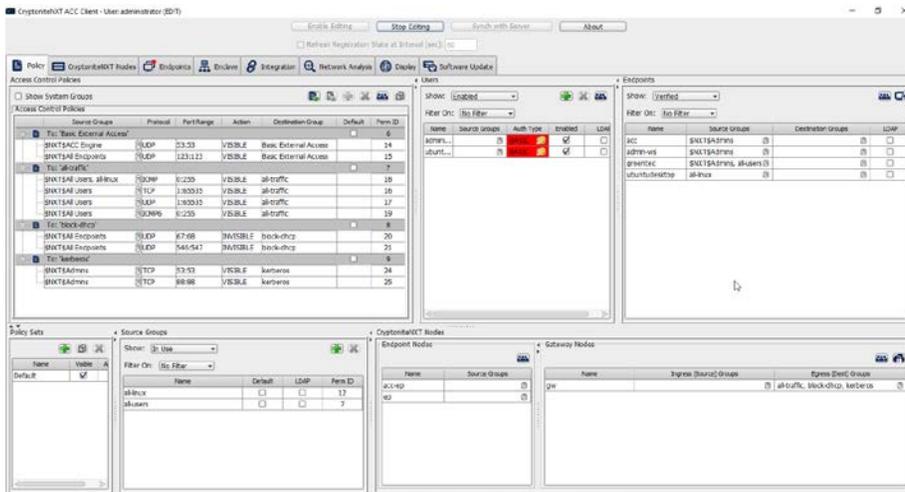
31. Repeat steps 21–29, but replace 53:53 with 88:88.
32. In the **Gateway Nodes** window, click the arrow under **Egress (Dest) Groups**.
33. Select “kerberos”.
34. Click the >> button.



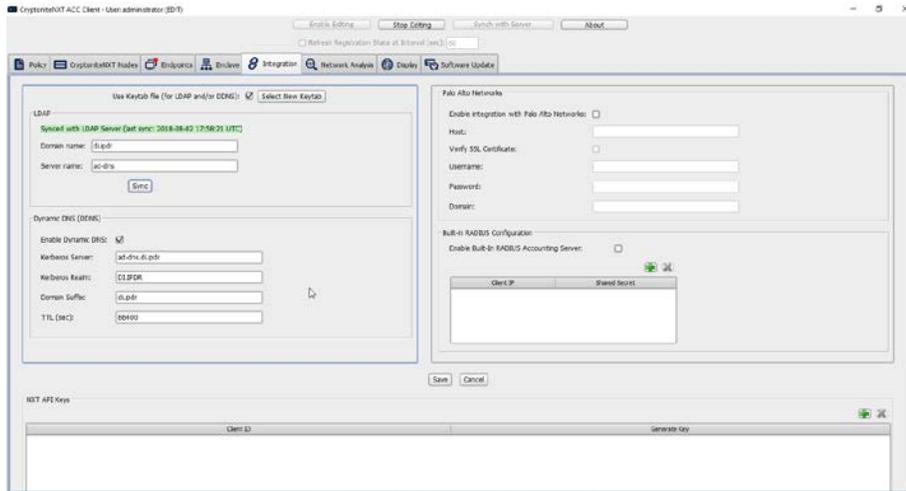
35. Click **Save**.
36. In the **Endpoints** window, click the arrow under **Source Groups** associated with the Administration Control Center (ACC).
37. Select **\$NXT\$Admins**.
38. Click the >> button.



39. Click **Save**.



40. Return to the **Integration** tab.



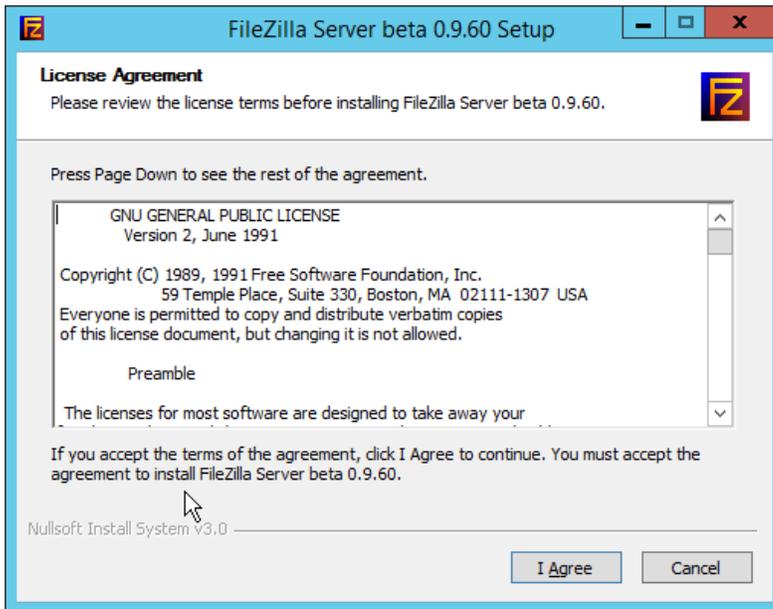
41. Click **Sync**.

2.8 Backups

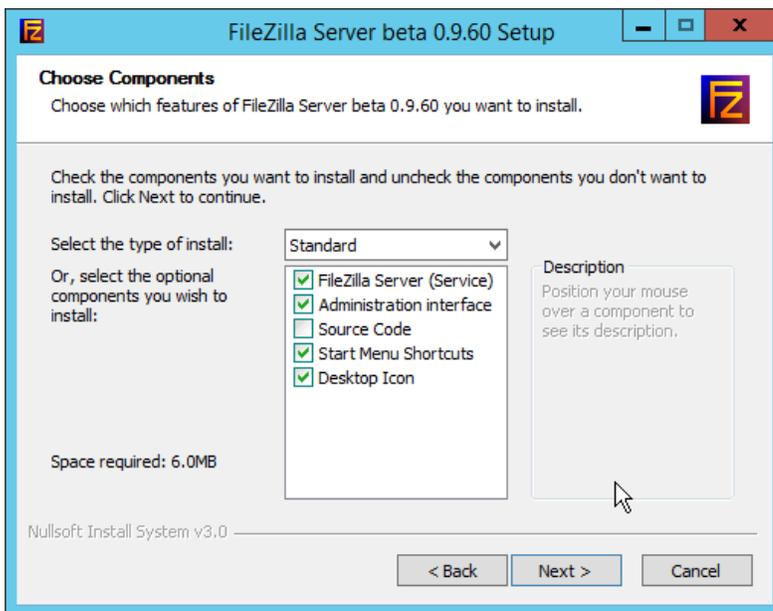
For this capability we use an integration of two open-source tools: **Duplicati** and **FileZilla**. **FileZilla** acts as a File Transfer Protocol (FTP) (over TLS) server component, while **Duplicati** acts as an encrypted backup client. This section details the installation and integration of both tools, as well as the process for creating a backup schedule, but does not provide specific recommendations on backup frequency or backup targets as those are specific to the organization.

2.8.1 FileZilla FTPS Server Setup

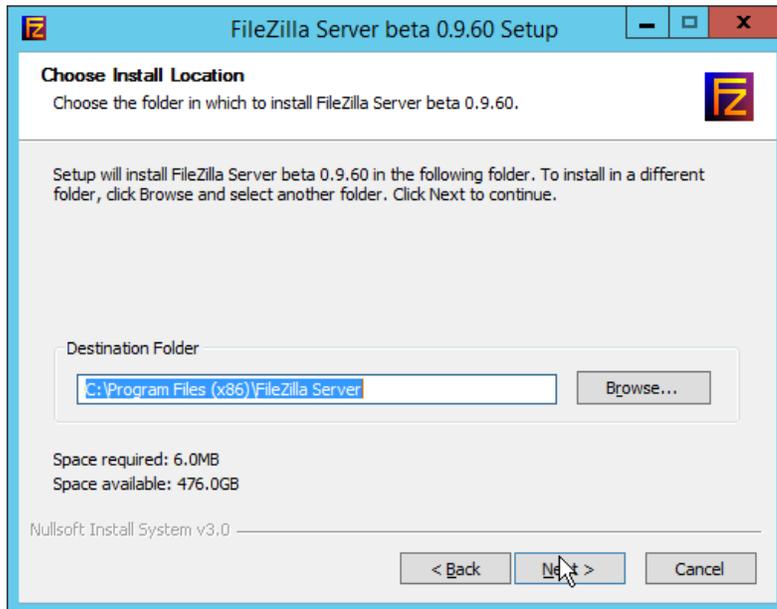
1. Run **FileZilla_Server-0_9_60_2.exe**.



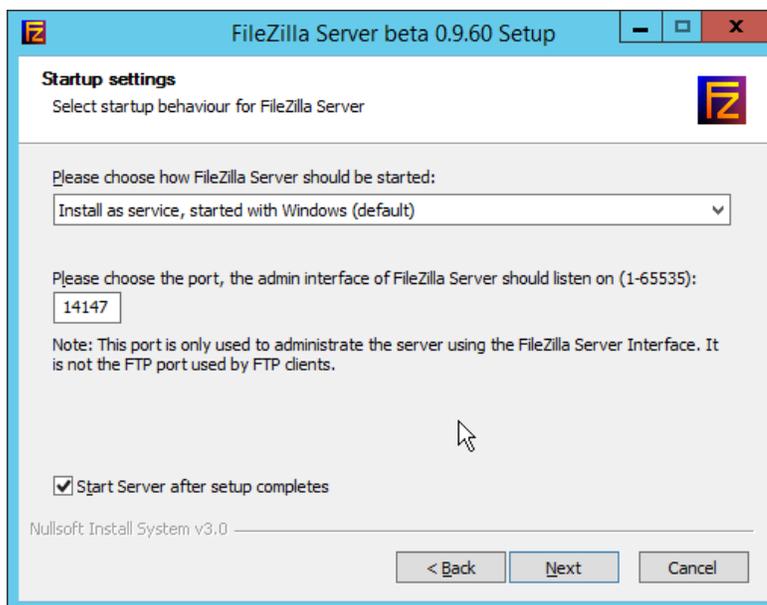
2. Click **I Agree**.
3. Select **Standard** from the drop-down menu.



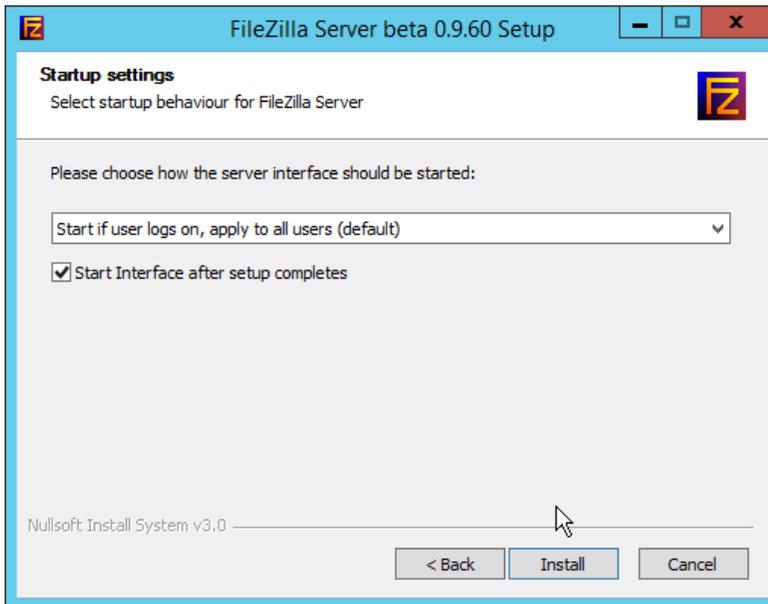
4. Click **Next**.



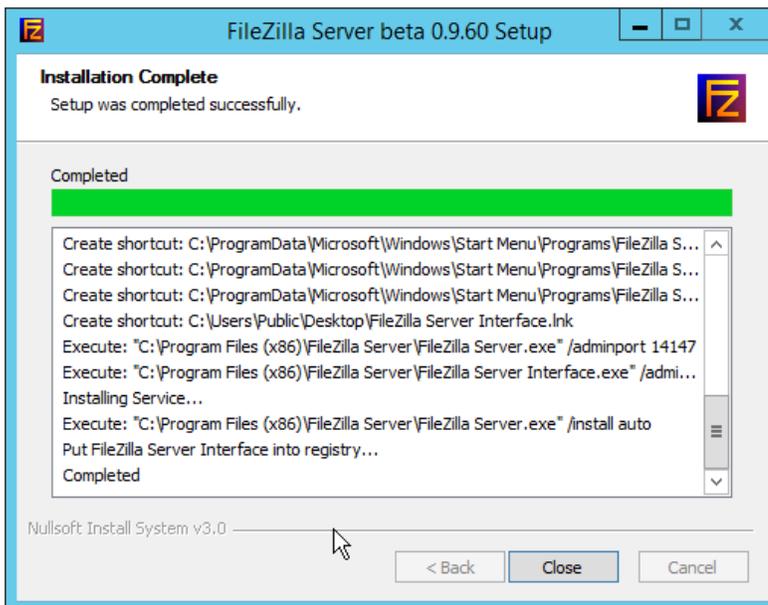
5. Click **Next**.
6. Select **Install as service, started with Windows (default)** from the drop-down.
7. Specify a port (for the administrator interface to run on) if desired (the default is 14147).
8. Ensure the box next to **Start Server after setup completes** is checked.



9. Click **Next**.



10. Click **Install**.

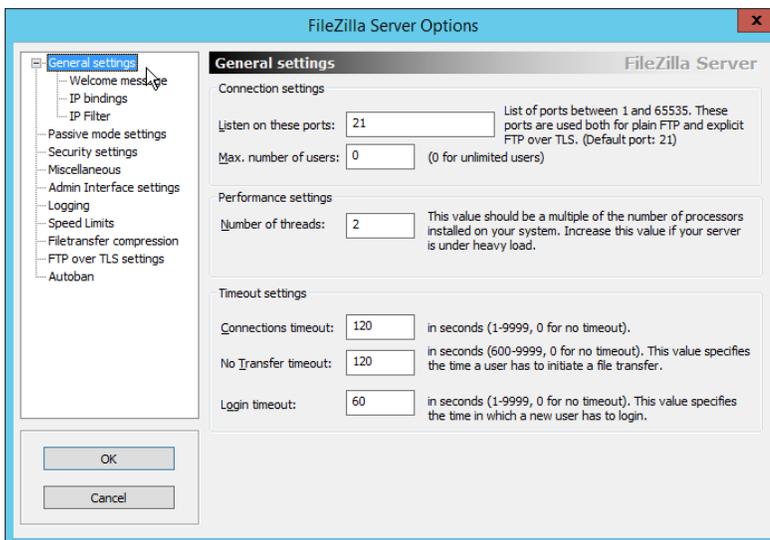


11. Click **Close**.

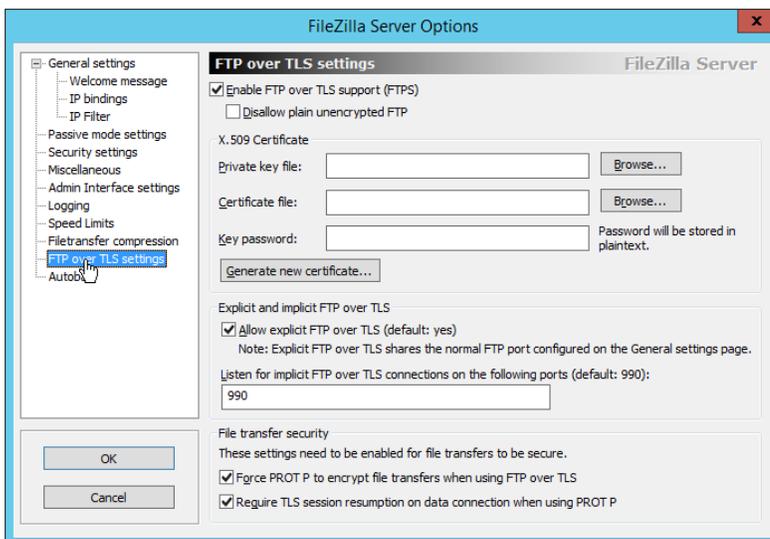
2.8.2 FileZilla Configuration

1. When the administrator interface comes up, ensure that the port is correct and click **Connect**.

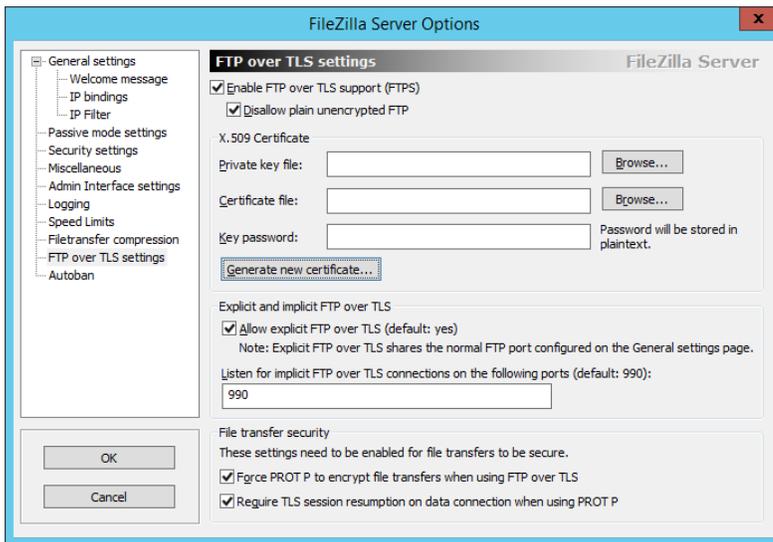
2. Click **Edit > Settings**.



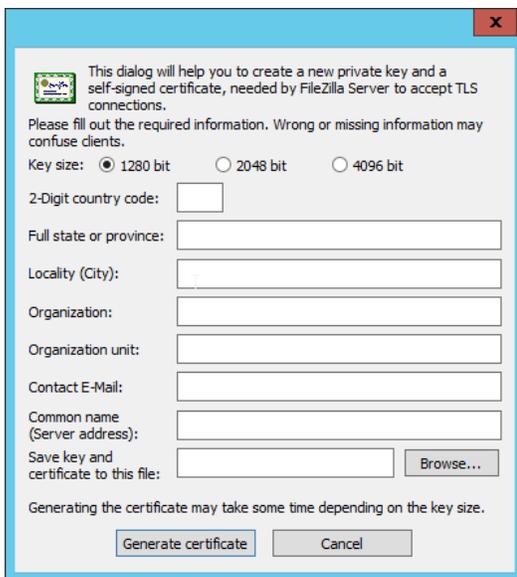
3. Click **FTP over TLS settings**.



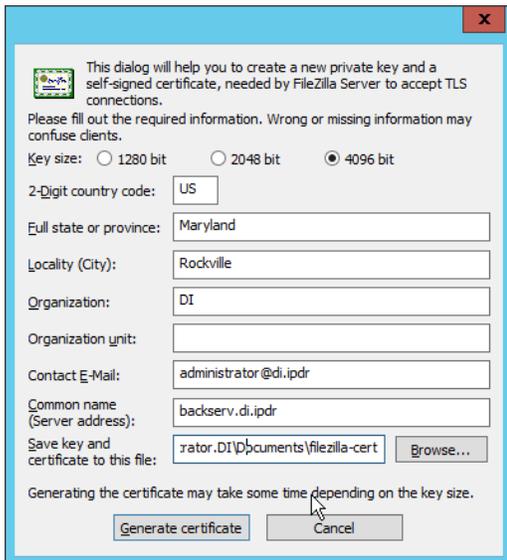
4. Check the box next to **Enable FTP over TLS support (FTPS)**.
5. Check the box next to **Disallow plain unencrypted FTP**.



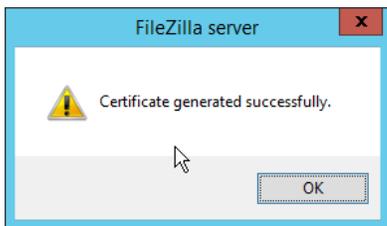
6. Click **Generate new certificate**.



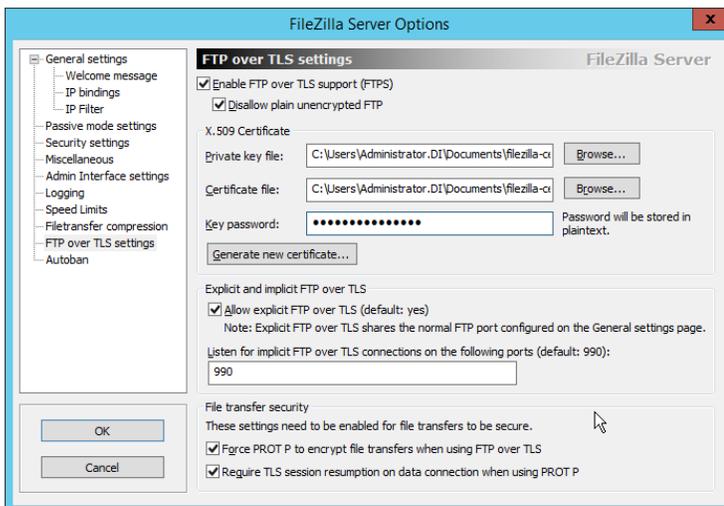
7. Select **4096 bit** for **Key Size**.
8. Enter the information for the certificate specific to your organization.
9. For the **common name**, enter the address of the server on which this is installed.
10. Click **Browse** and specify a file location for the certificate.



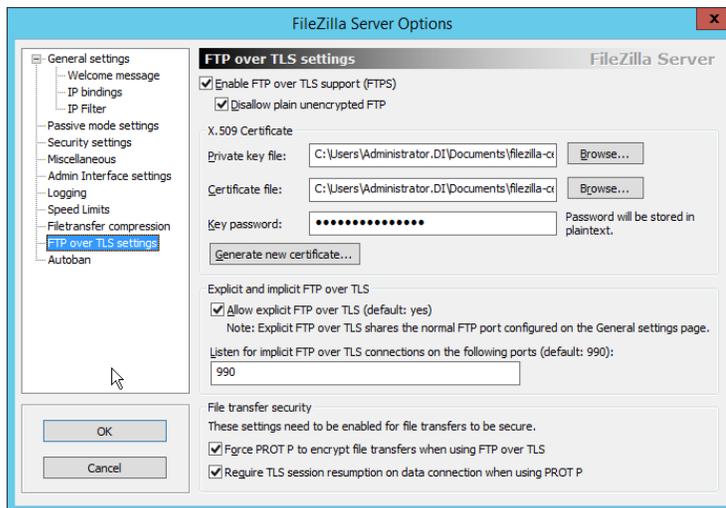
11. Click **Generate certificate**. (The file now contains both the private key and the certificate. These can be separated, for ease of use, as long as the correct file locations are specified in the settings.)



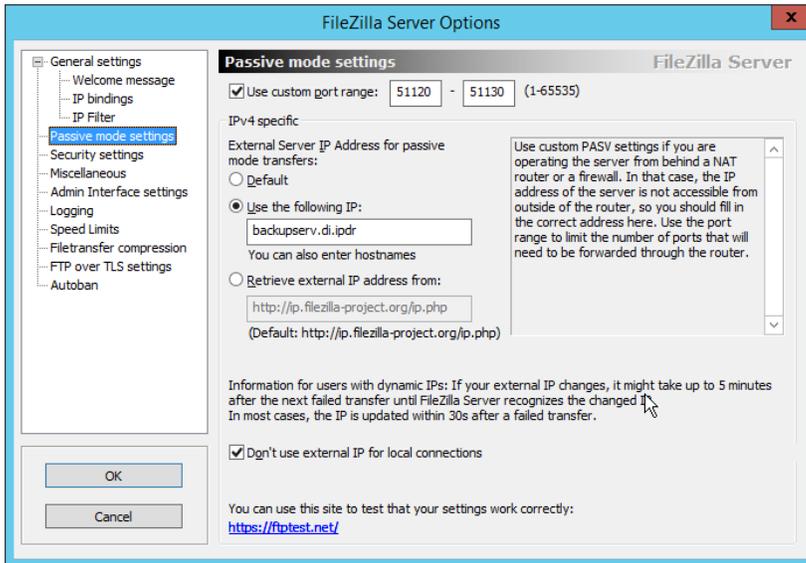
12. Click **OK**.



13. Enter a **password** for the key.
14. Ensure the box next to **Force PROT P to encrypt file transfers when using FTP over TLS** is checked.
15. Ensure the box next to **Require TLS session resumption on data connection when using PROT P** is checked.



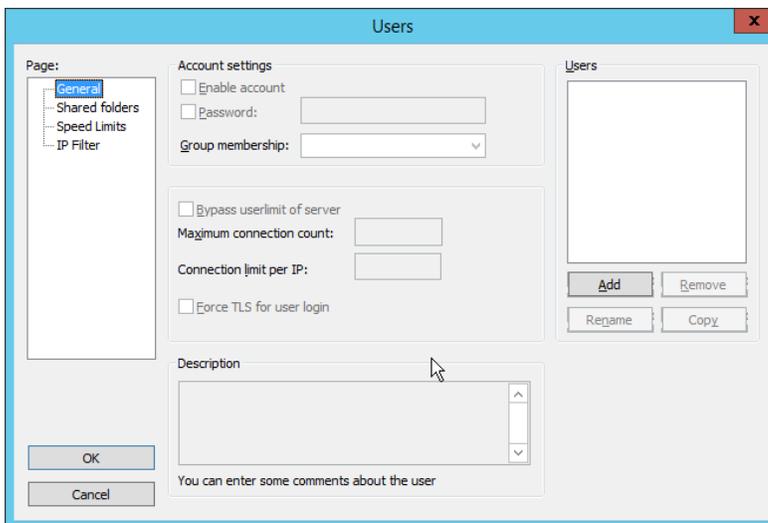
16. Click **Passive mode settings**. Check the box next to **Use custom port range**. (This is necessary in cases of a local server behind Network Address Translation (NAT) or a firewall.)
17. Enter a range of ports for passive mode to use. Ensure that these ports are allowed through the firewall.
18. Select **Use the following IP**.
19. Enter the server address.



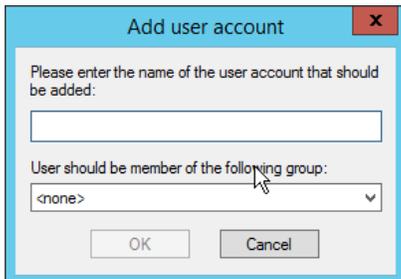
20. Click **OK**.

2.8.3 Add a User to FileZilla

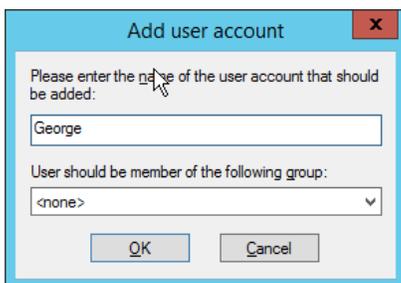
1. In the FileZilla administrator interface, click **Edit > Users**.



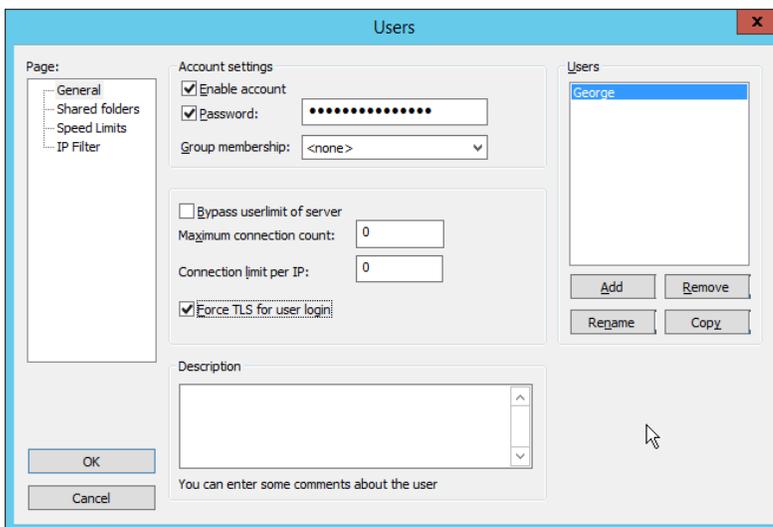
2. Click **Add**.



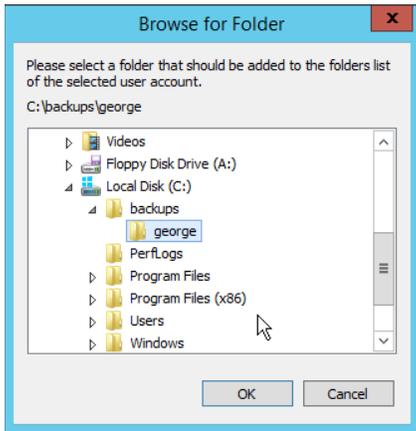
3. Enter a **name** for the user.



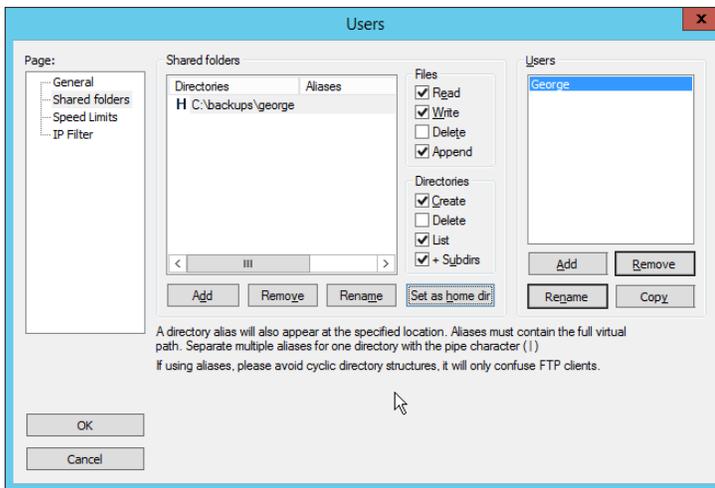
4. Click **OK**.
5. Check the box next to **Password**.
6. Enter a **password** for the user.



7. Check the box next to **Force TLS for user login**.
8. Click **Shared Folders**.
9. Click **Add**, under **Shared Folders**.



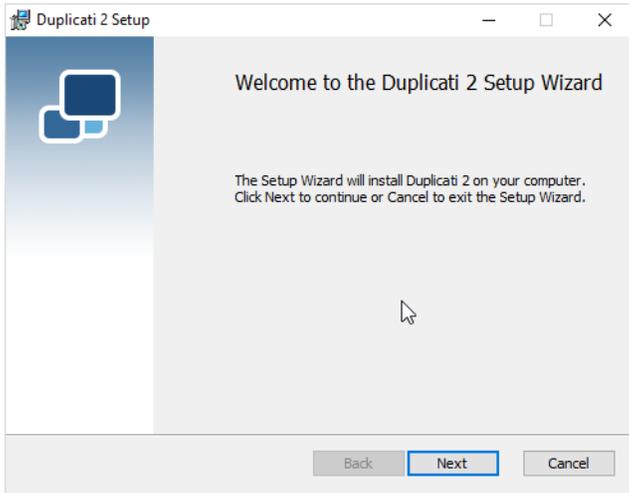
10. Select a place for backups *for this user* to be stored.
11. Check the boxes next to **Write** and **Append**, under **Files**.
12. Check the box next to **Create**, under **Directories**.
13. Select this entry and click **Set as home dir**.



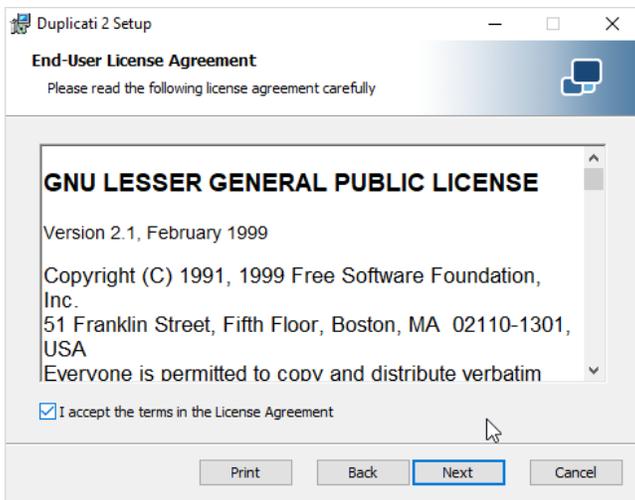
14. Click **OK**.

2.8.4 Duplicati Client Installation (Windows)

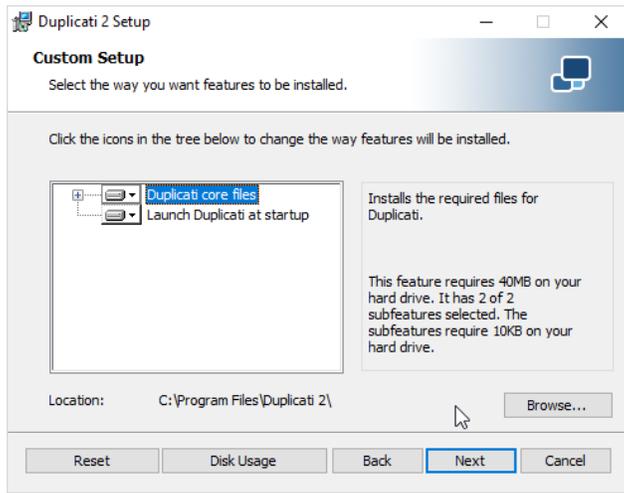
1. On the client machine, run **duplicati-2.0.3.3_beta_2018-04-02-x64.msi**.



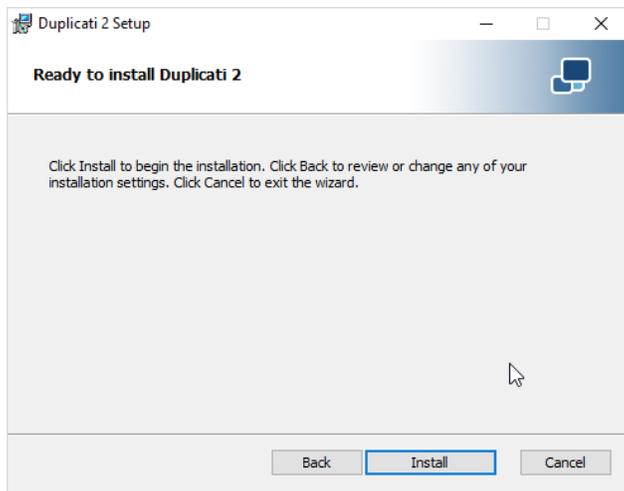
2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



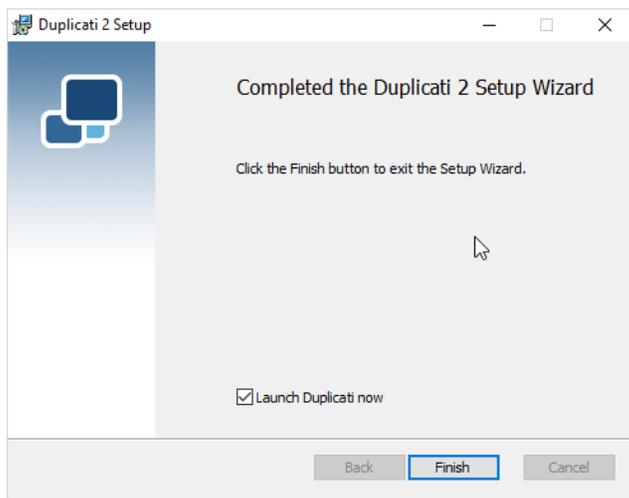
4. Click **Next**.



5. Click **Next**.



6. Click **Install**.



7. Click **Finish**.
8. Start **Duplicati** by going to **localhost:8200**.

2.8.5 Duplicati Client Installation (Ubuntu)

1. Install mono by using the following command:

```
> sudo apt install mono-runtime
```

2. Download the Duplicati package by running the following command:

```
> wget  
https://github.com/duplicati/duplicati/releases/download/v2.0.3.9  
-2.0.3.9_canary_2018-06-30/duplicati_2.0.3.9-1_all.deb
```

3. Install Duplicati by using the following command:

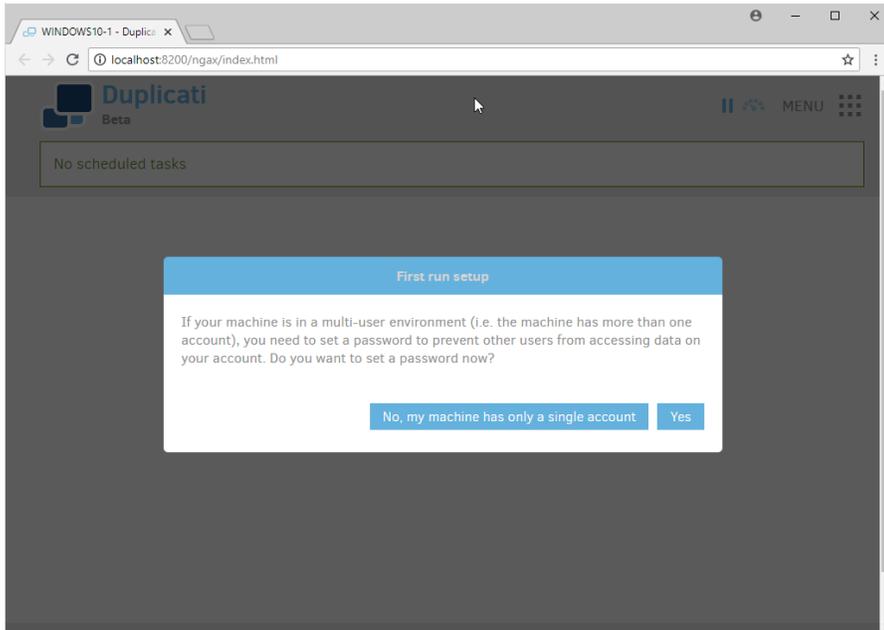
```
> sudo dpkg -i duplicati_2.0.3.9-1_all.deb
```

4. Run Duplicati as a service by running the following command:

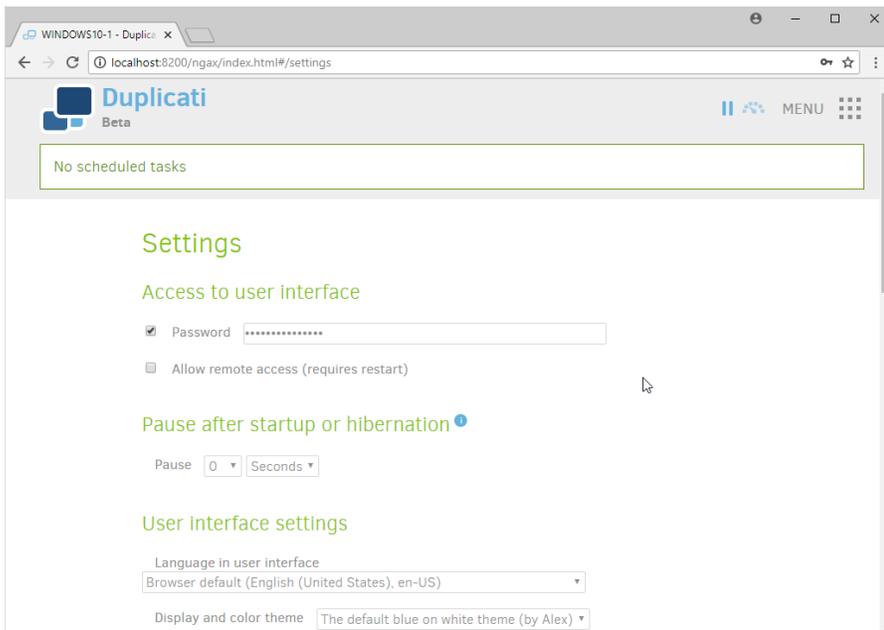
```
> sudo systemctl enable duplicati
```

2.8.6 Configure Duplicati

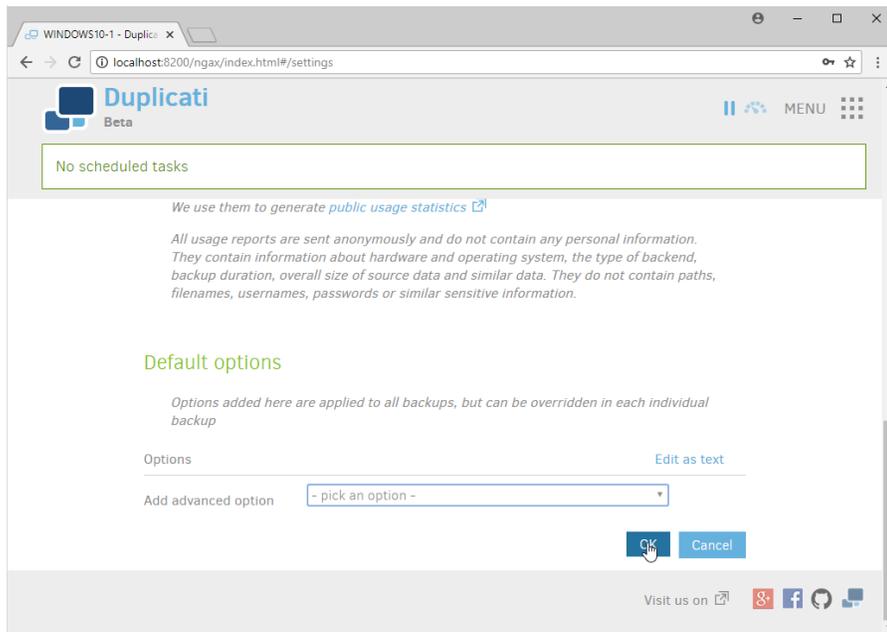
1. When it first starts, **Duplicati** will have a **First run setup**.



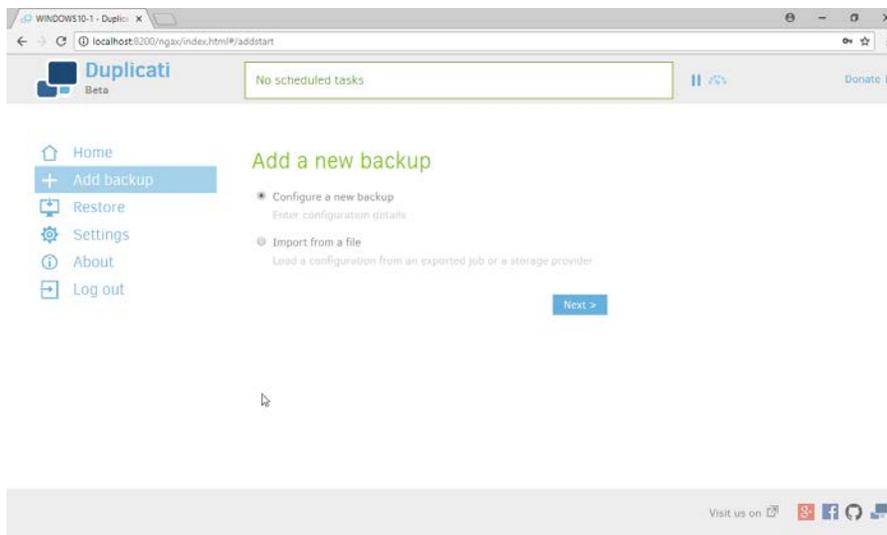
2. Click **Yes**.
3. Check the box next to **Password**.



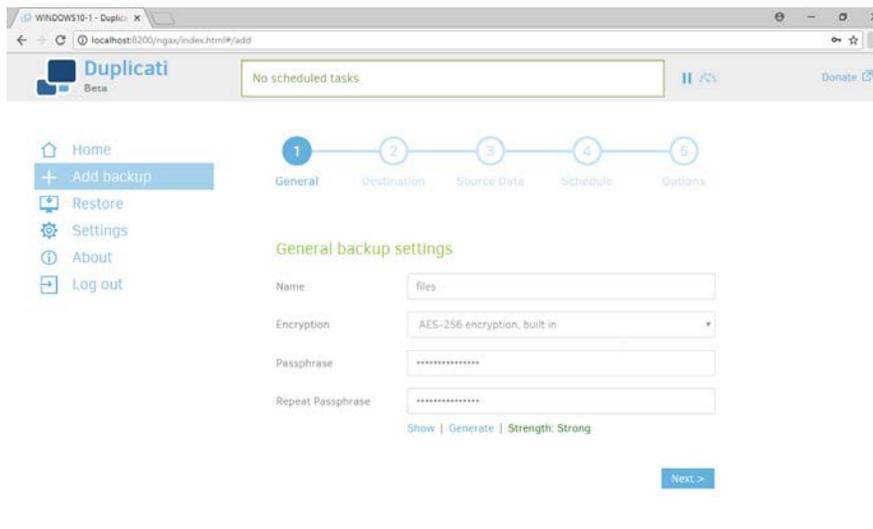
4. Enter a **password**.



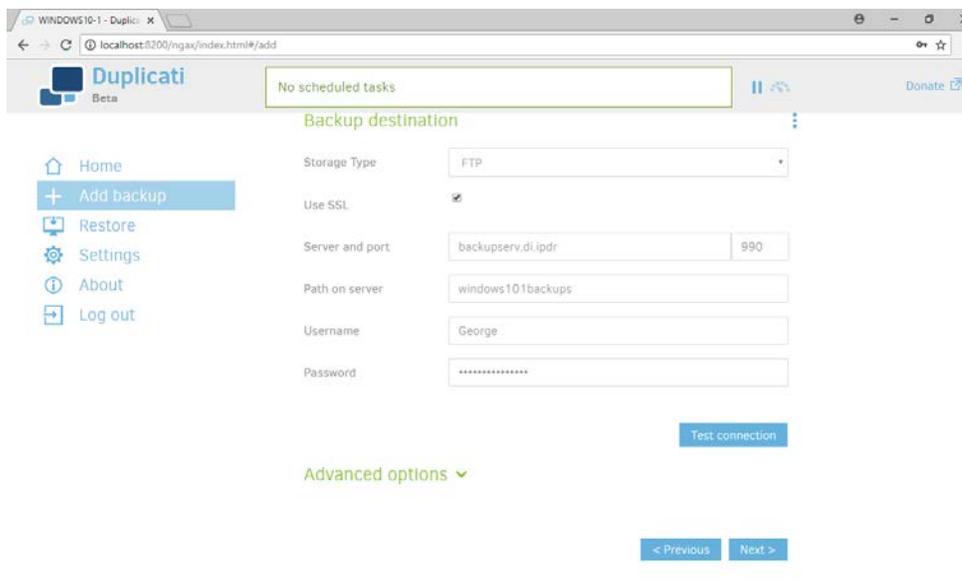
5. Click **OK**.
6. On the home page, click **Add backup**.
7. Select **Configure a new backup**.



8. Click **Next**.
9. Enter a **name** for the backup.
10. Select **AES-256 encryption, built in** from the drop-down menu.
11. Enter a **password**.

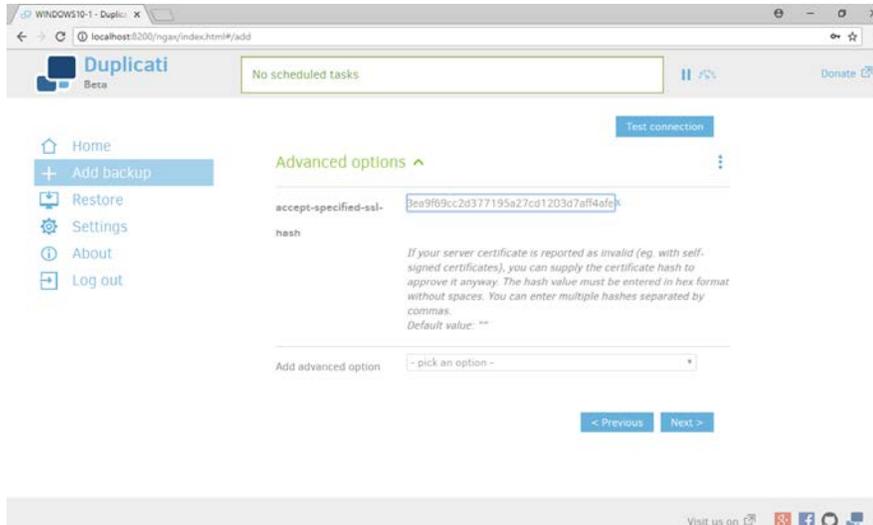


12. Click **Next**.
13. Select **FTP** for **Storage Type**.
14. Check the box next to **Use SSL**.
15. Enter the **server name** and **port** (default: 21) of the server running **FileZilla**.
16. Enter a **path** for the backup to be stored in (within the specified shared directory of the user).
17. Enter the **username** and **password** created for **FileZilla**.

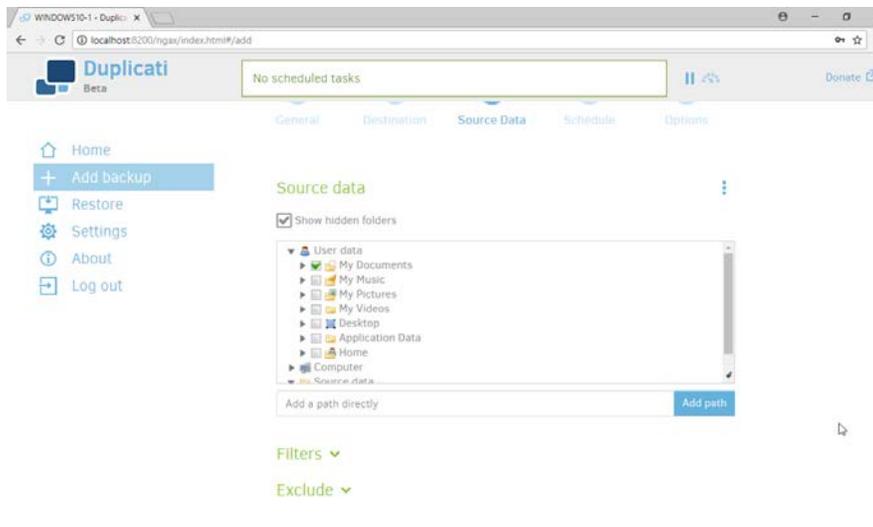


18. Click **Test Connection** (if the connection fails, ensure that the port is allowed in your server's firewall).

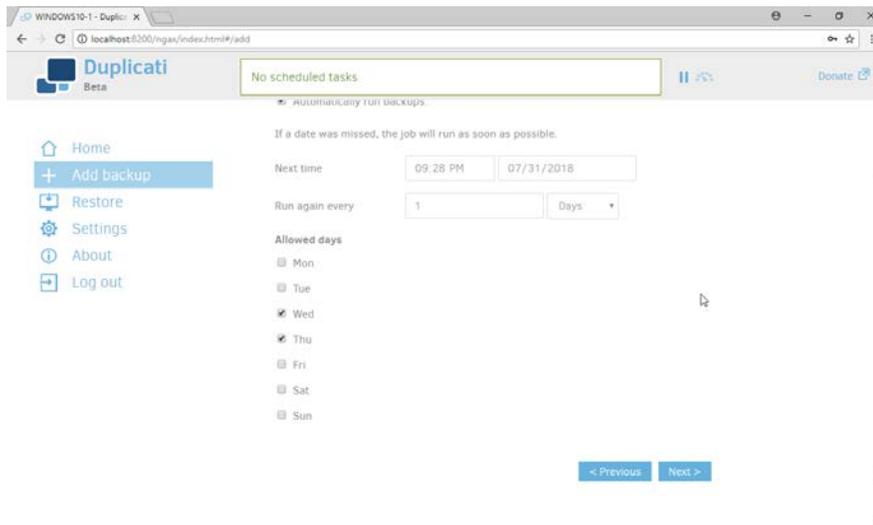
19. If you receive an error about a certificate, you can go to **Advanced Options**, select **accept-specified-ssl-hash**, and enter the **thumbprint** from the server’s certificate.



20. Click **Next**.
21. Select the folders on the local machine to be backed up to the server according to your organization’s needs.

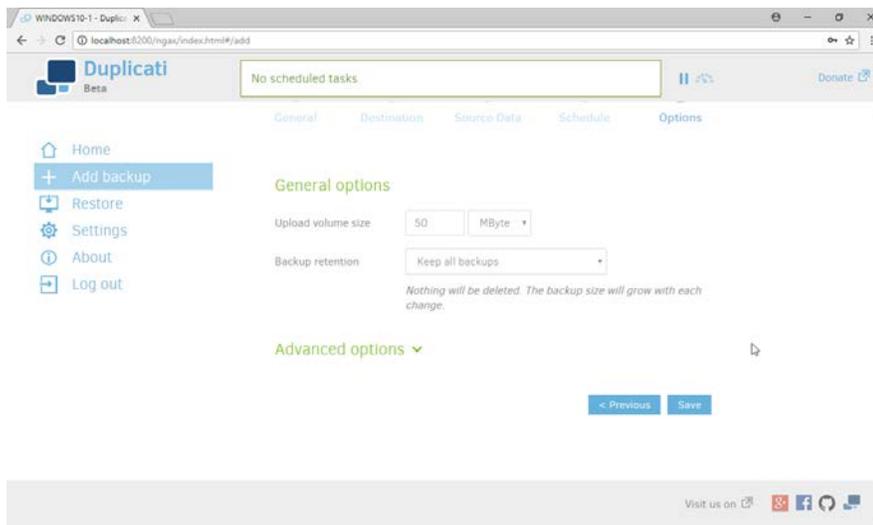


22. Click **Next**.
23. Select a backup schedule according to your organization’s needs.

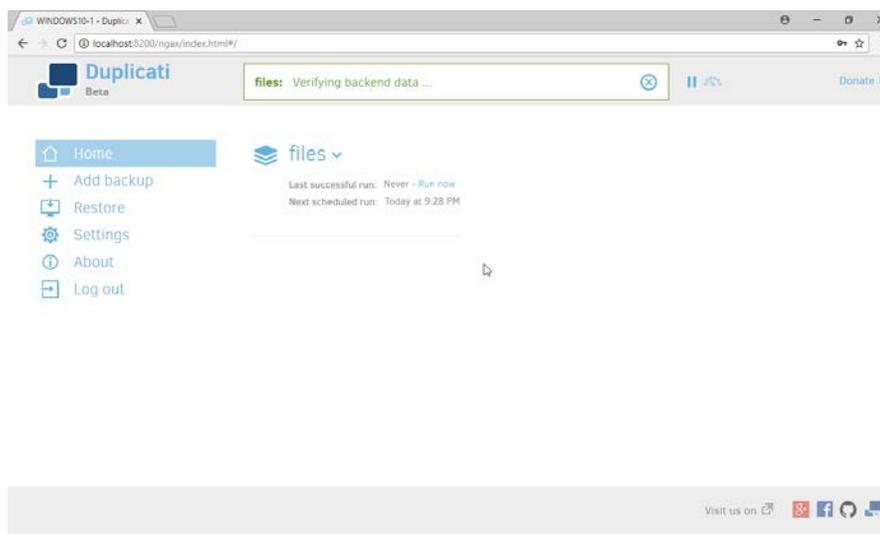


24. Click **Next**.

25. Select any other options according to your organization's needs.



26. Click **Save**.



27. When finished, you can choose to **Run now** to start a backup immediately.

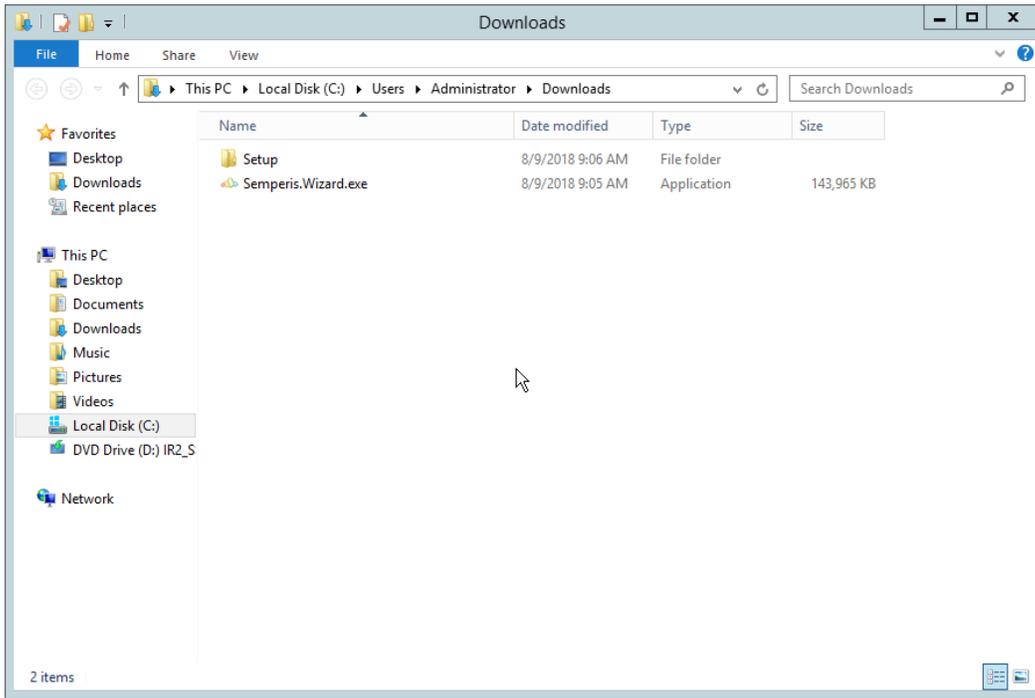
2.9 Semperis Active Directory Forest Recovery

This section details the installation of **Semperis Active Directory Forest Recovery (ADFR)**, a tool used for backing up and restoring Active Directory forests. This installation requires both a copy of SQL Server Express as well as the **Semperis Wizard**. See the **Semperis ADFR v2.5 Technical Requirements** document for specifics on the requirements. For a Windows Server 2012 R2 installation, simply meet the following requirements:

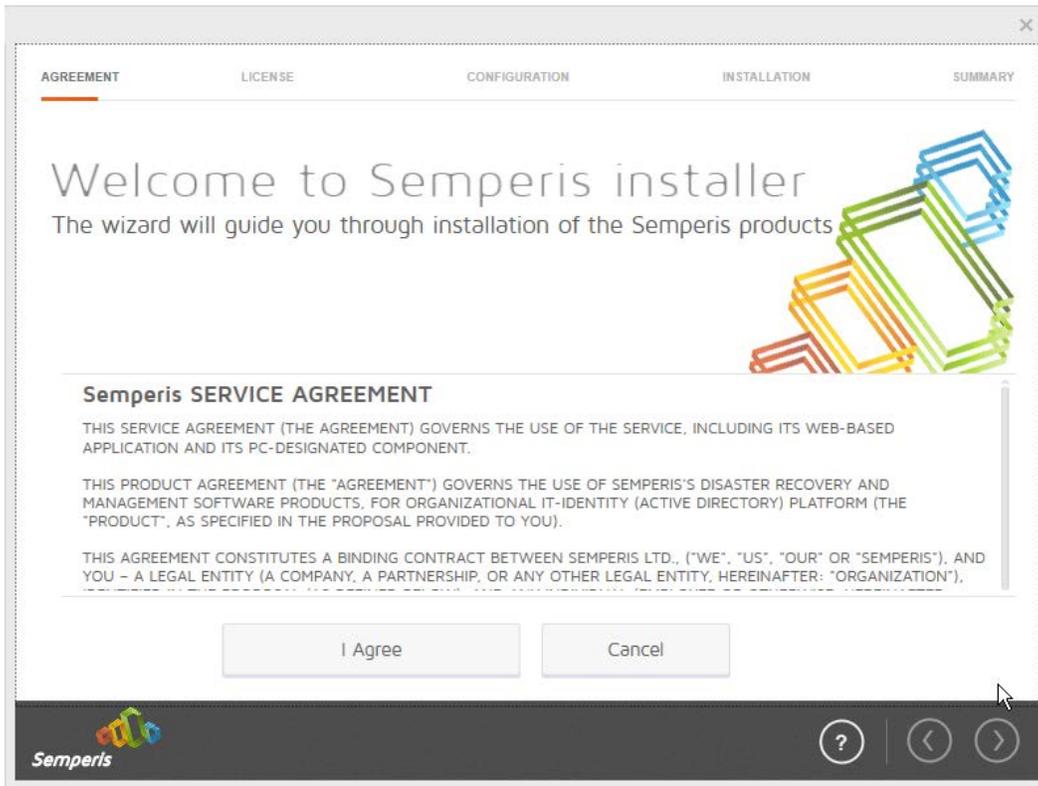
- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- not joined to the Active Directory domain it is protecting
- SQL Express is not installed on the machine, but the installer `SQLEXPRESS_x64_ENU.exe` is downloaded.

2.9.1 Install Semperis ADFR

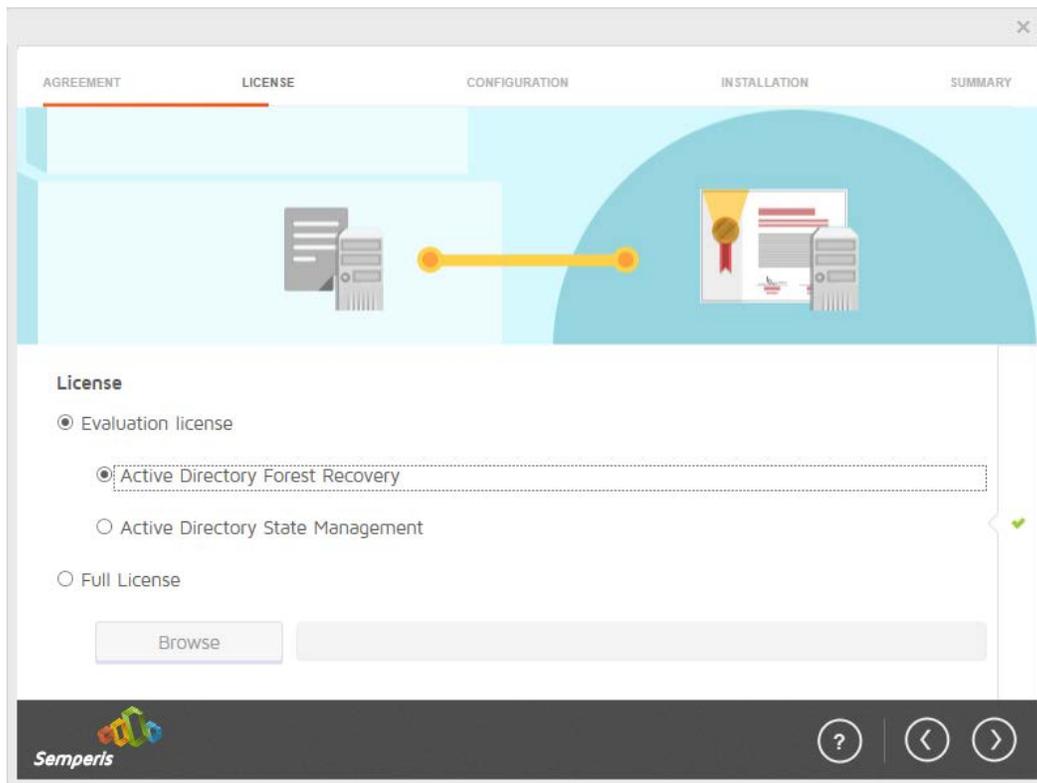
1. Place the **SQLEXPRESS_x64_ENU.exe** installer in a directory called Setup, and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it).



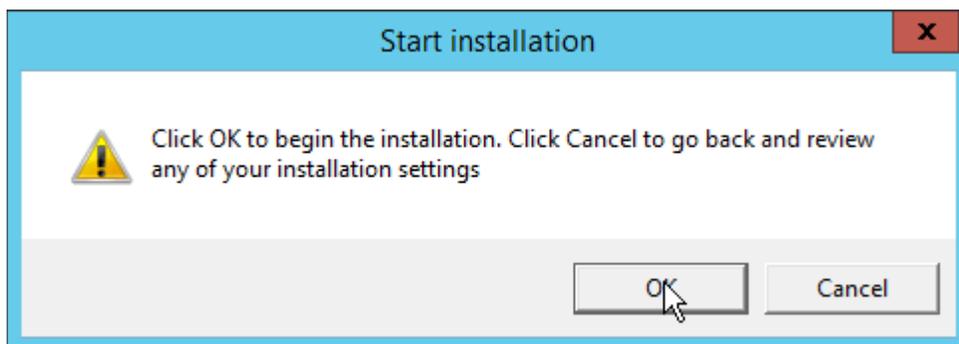
2. If prompted to restart the computer, do so.



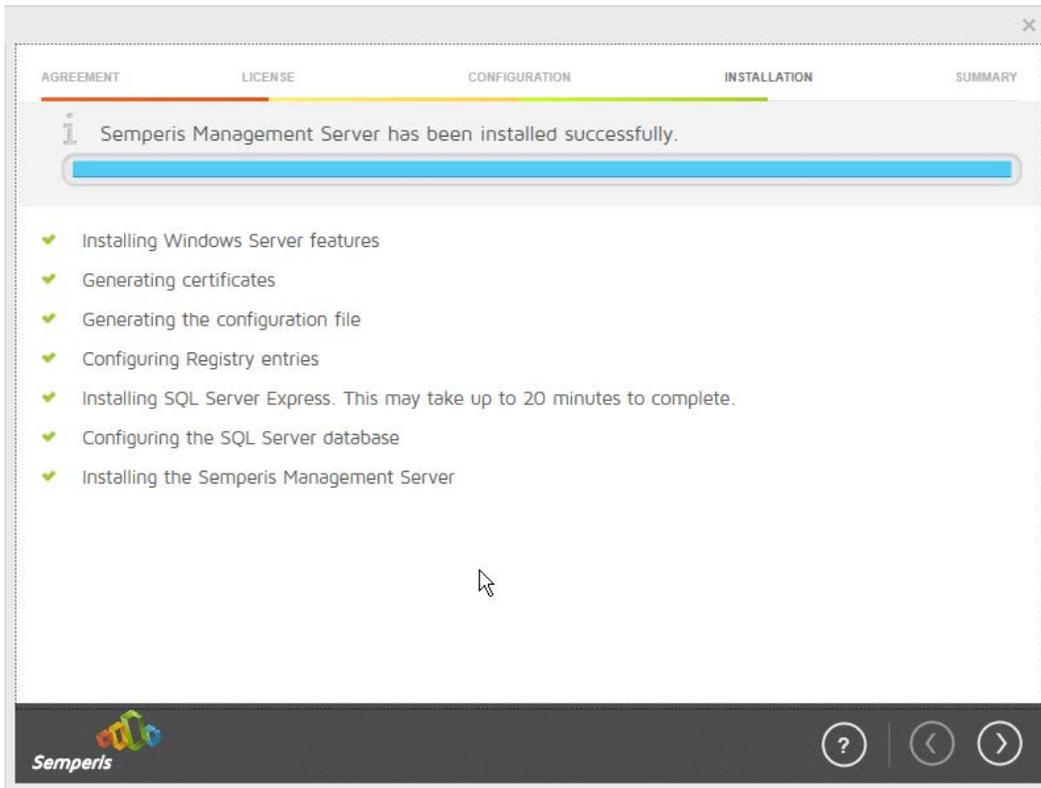
3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory Forest Recovery**.



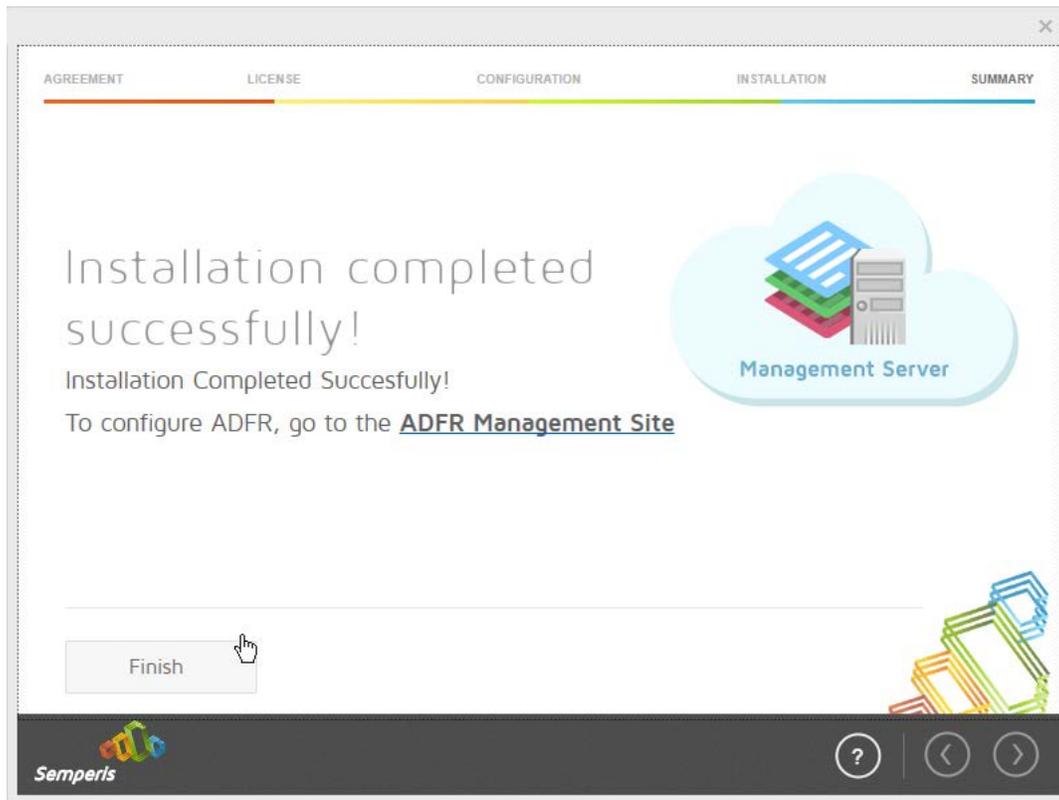
6. Click the > button.



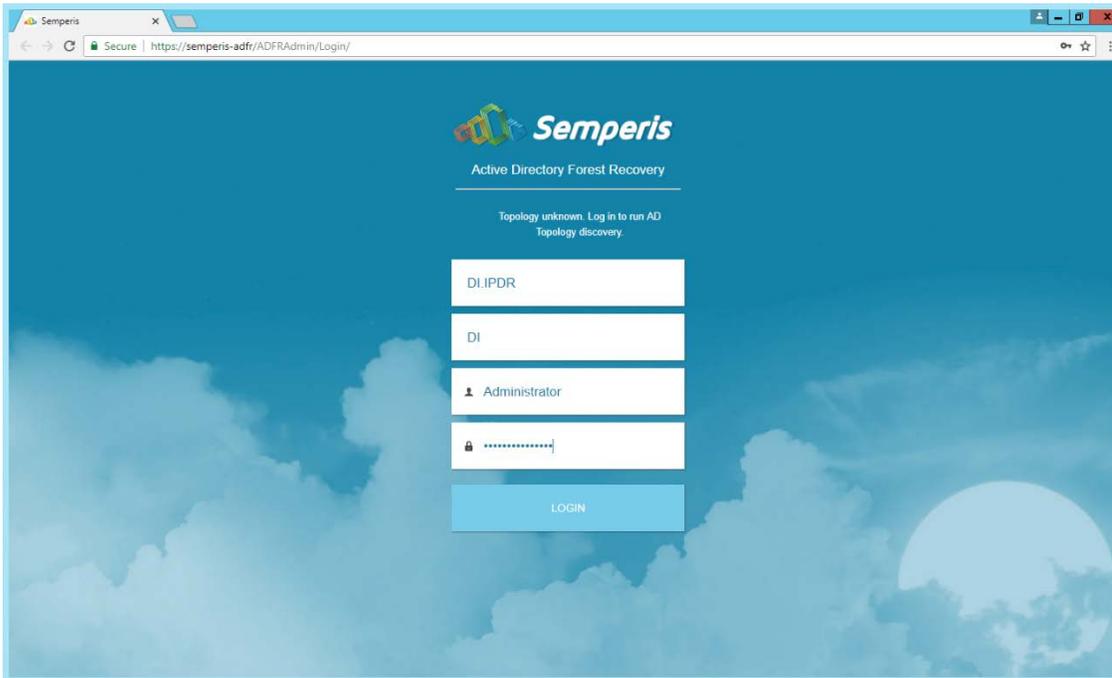
7. Click **OK**.
8. Wait for the installation to complete.



9. Click the > button.

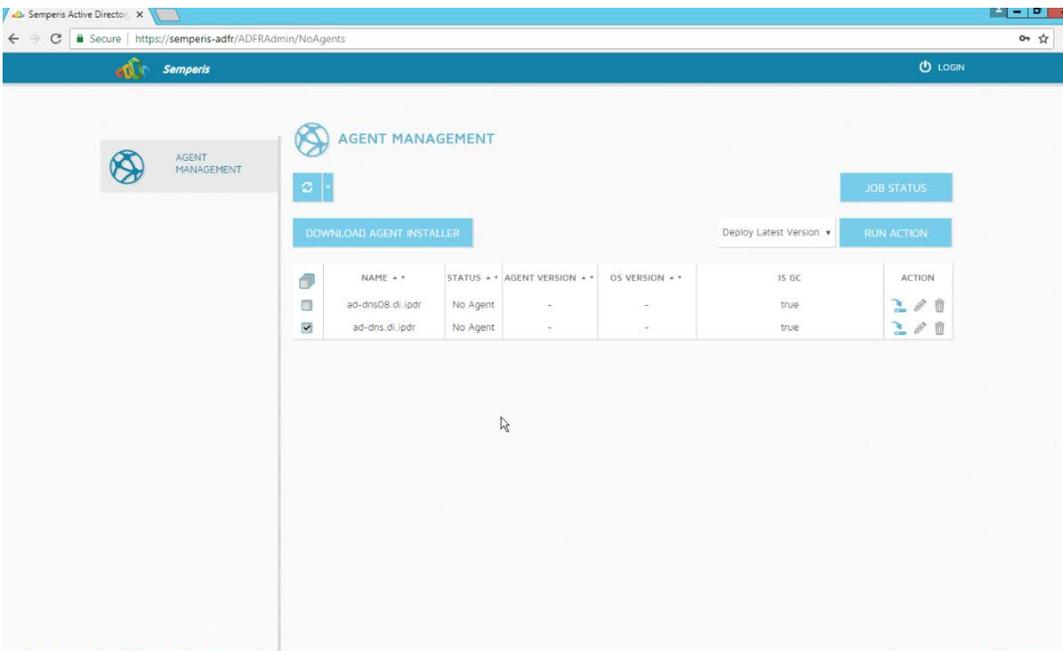


10. Click **Finish**.
11. There should now be a shortcut on the desktop linking to the web console for **Semperis ADFR**.
12. On the login page, enter the full domain as well as the NetBIOS name.
13. Enter the **username** and **password** of an administrator on the domain.



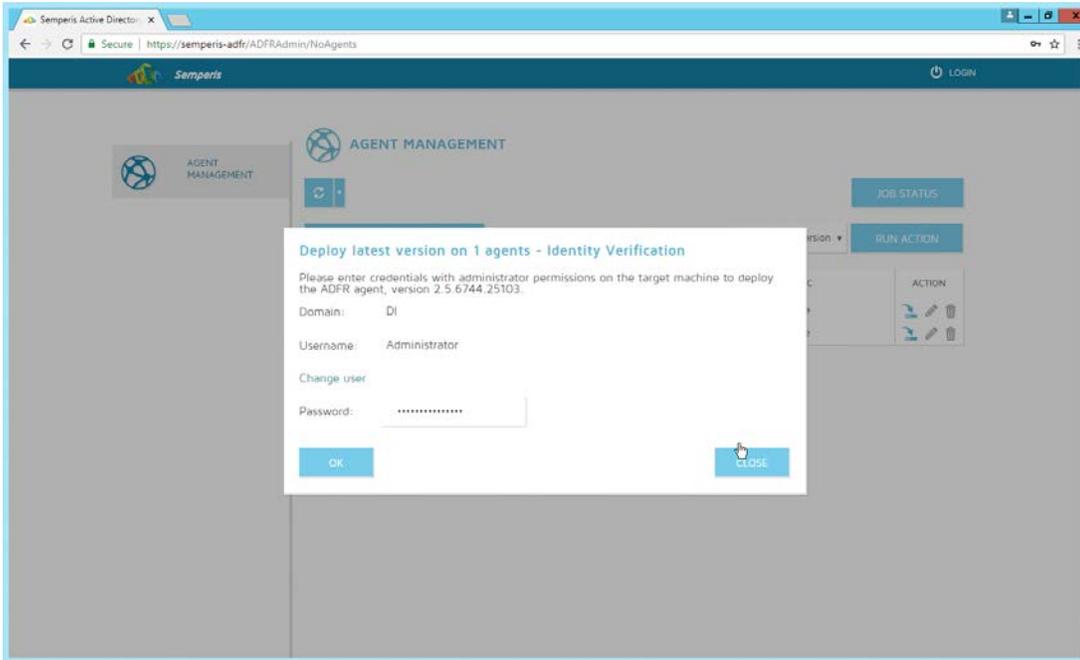
14. Click **Login**.

15. Check the box next to any domain controllers that should be backed up.

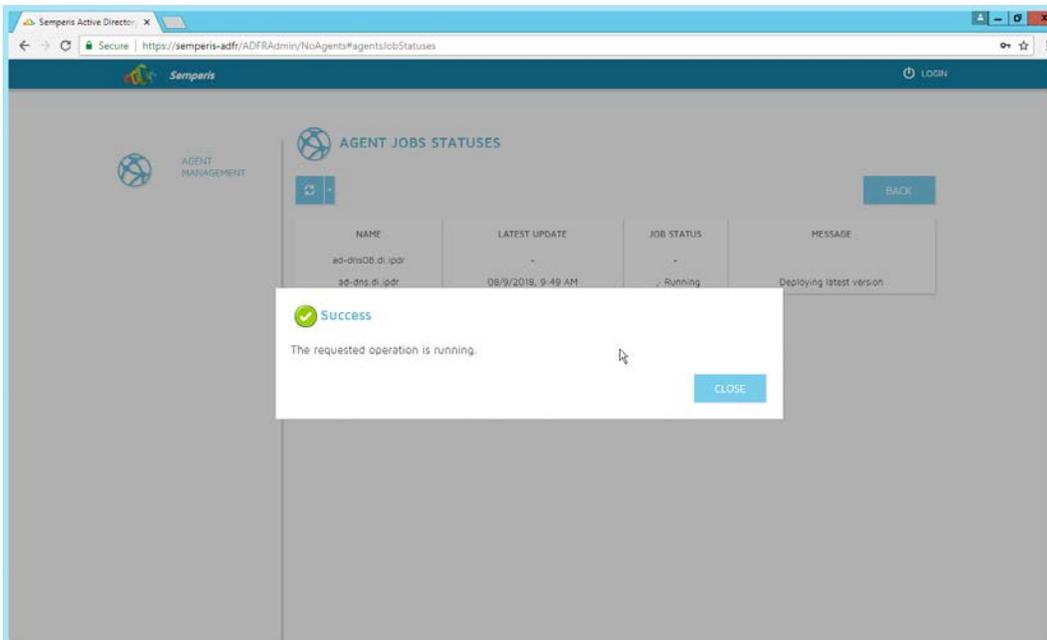


16. Click **Run Action**.

17. Enter the **password** in the prompt.



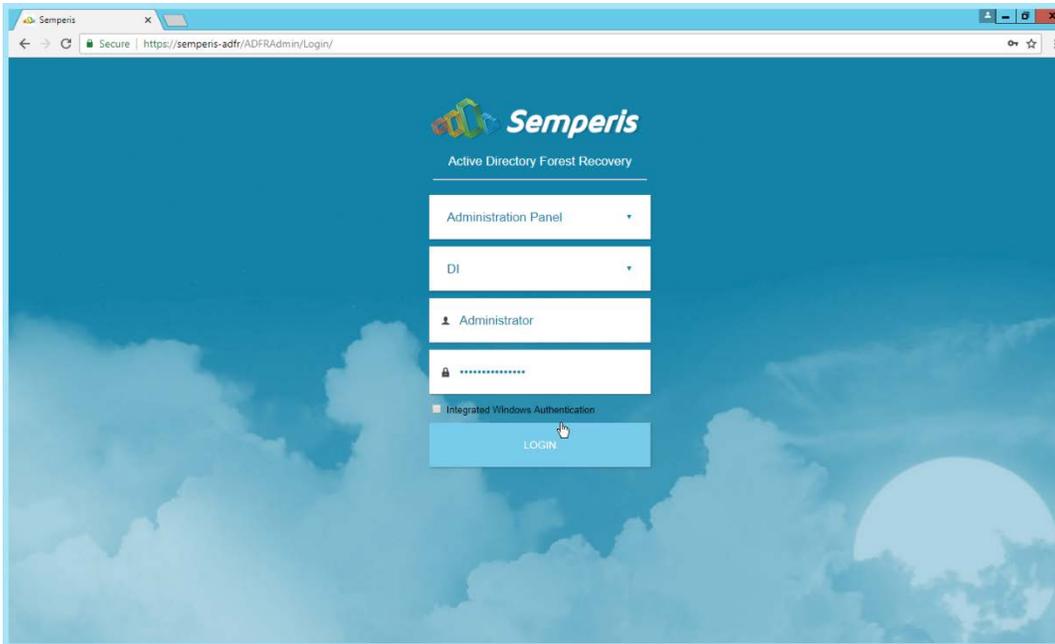
18. Click **OK**.



19. Click **Close**.

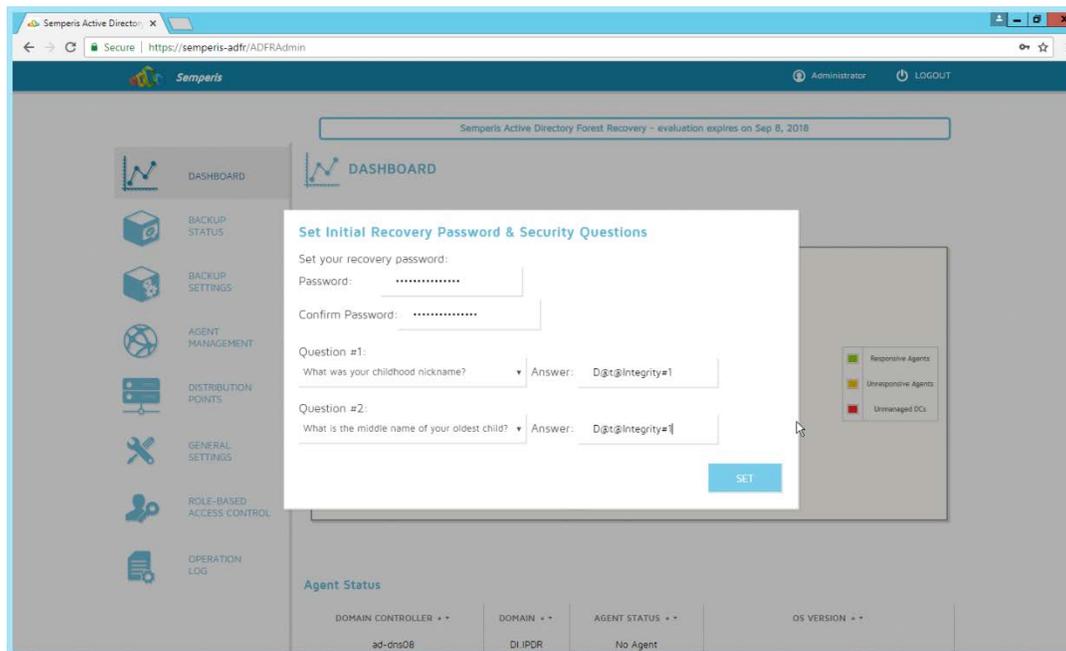
20. After the installation finishes, click **Login** at the top of the page.

21. Enter the login credentials for the domain.



22. Click **Login**.

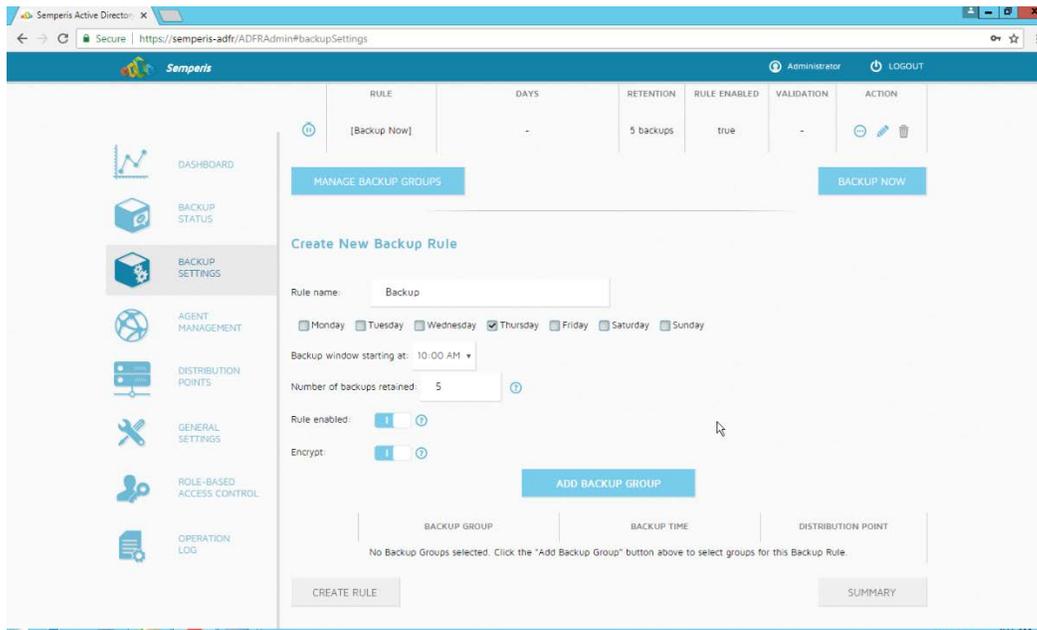
23. Create a recovery **password**. (Note: In the event of a restoration, Active Directory will potentially be unavailable, so a separate password that is not domain-associated is needed here for restorations.)



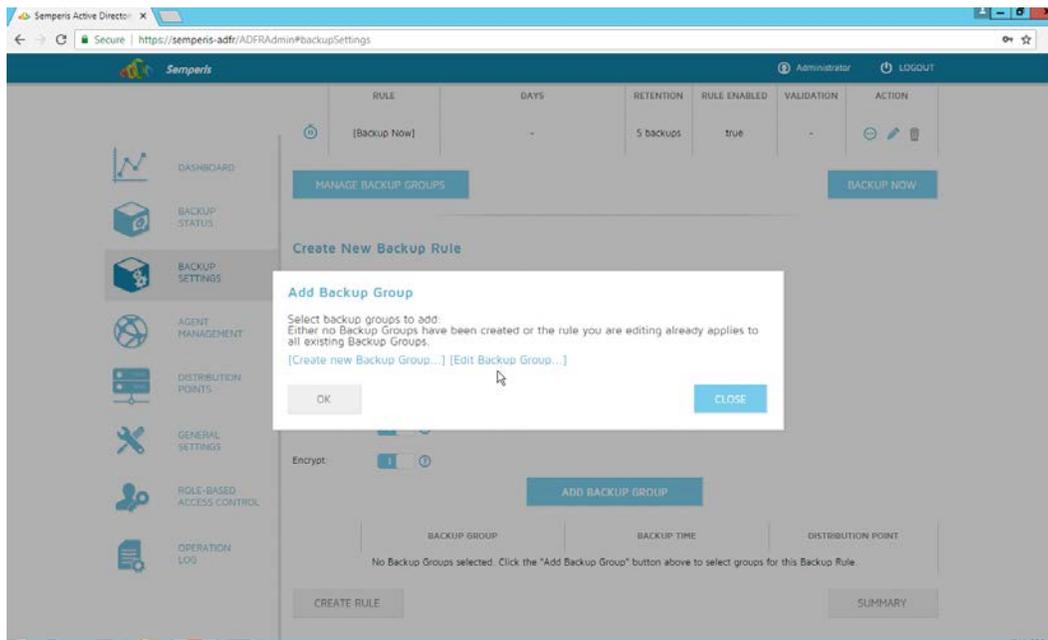
24. Set recovery questions for the password.
25. Click **Set**.

2.9.2 Create a Backup Schedule for the Domain Controller

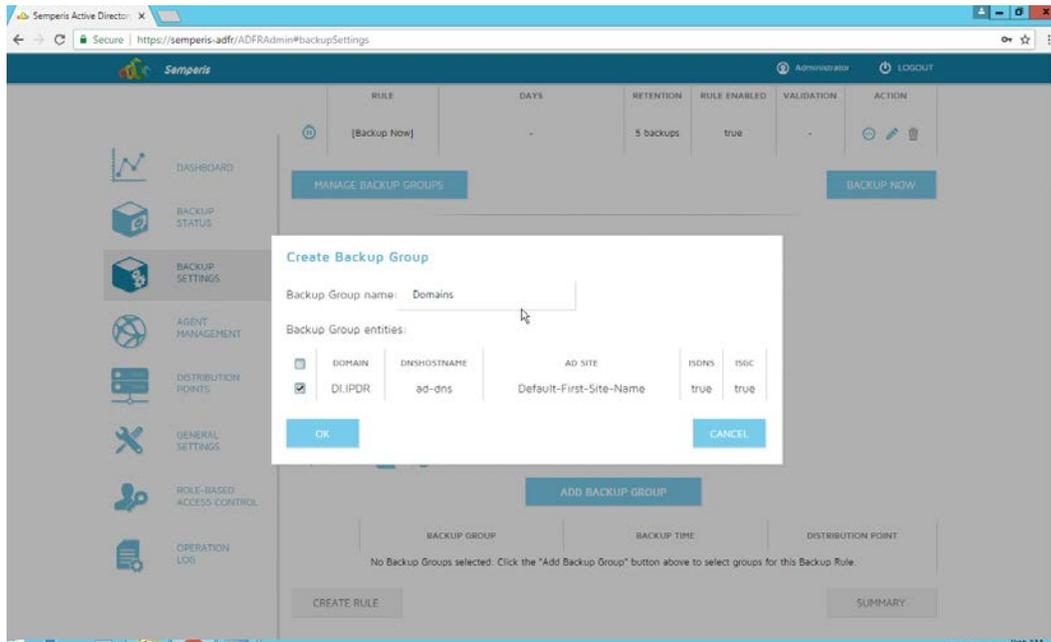
1. Click the **Backup Settings** tab.
2. Enter a **name** for the rule.
3. Select the days and times that the domain controller should be backed up.
4. Enter the maximum number of backups that should be kept. (Note: The oldest backup will be deleted upon creation of a new backup, which would exceed this maximum.)
5. Ensure that **Encrypt** and **Rule enabled** are both turned on.



6. Click **Add Backup Group**.

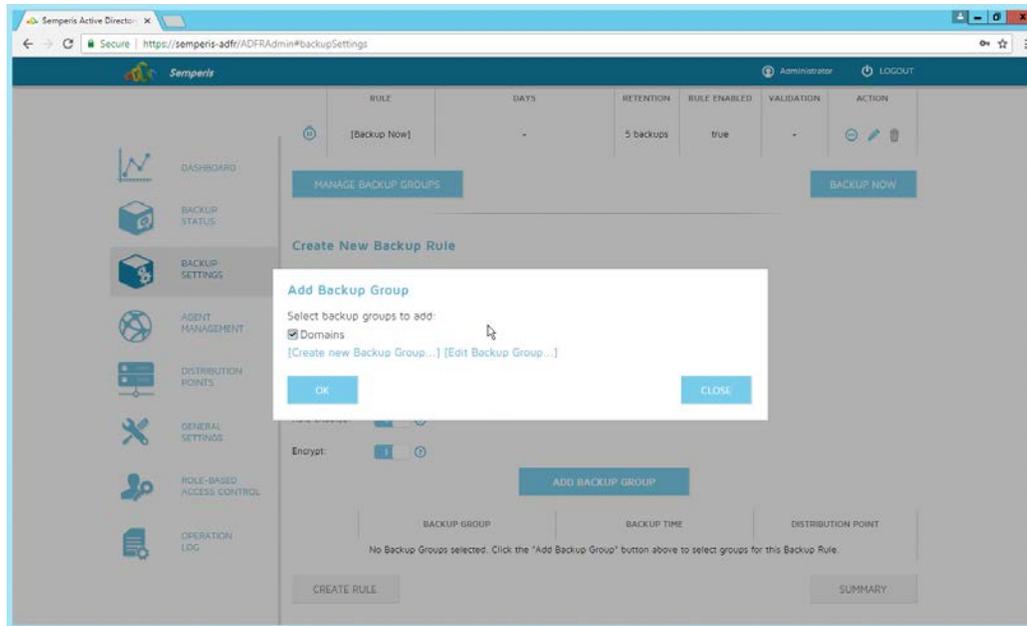


7. Click **Create new Backup Group**.
8. Enter a **name** for the backup group.
9. Select the domain controllers to be part of the backup group.

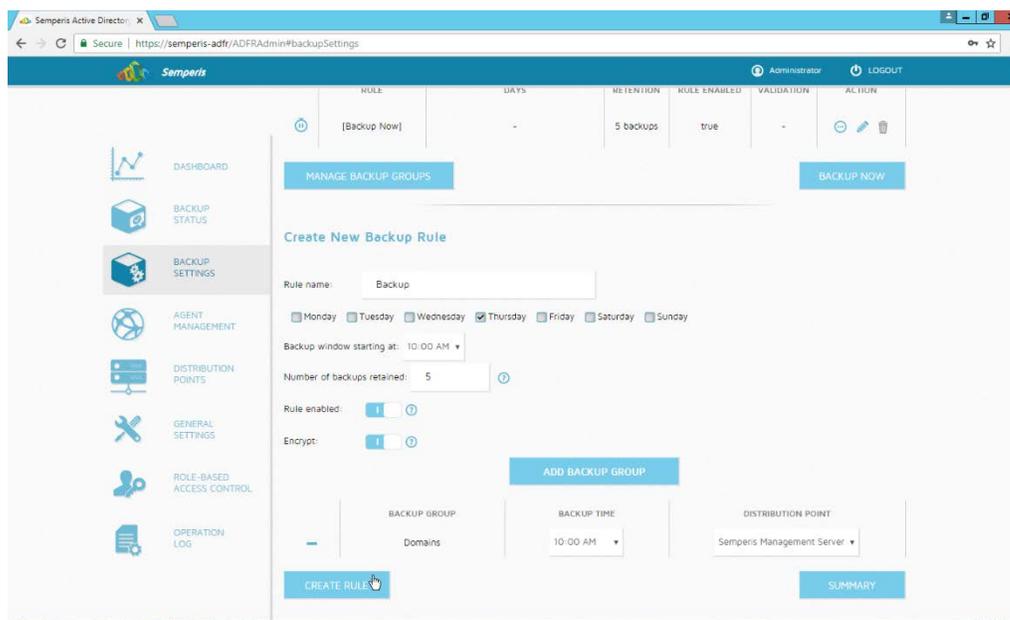


10. Click **OK**.

11. Select the newly created backup group.



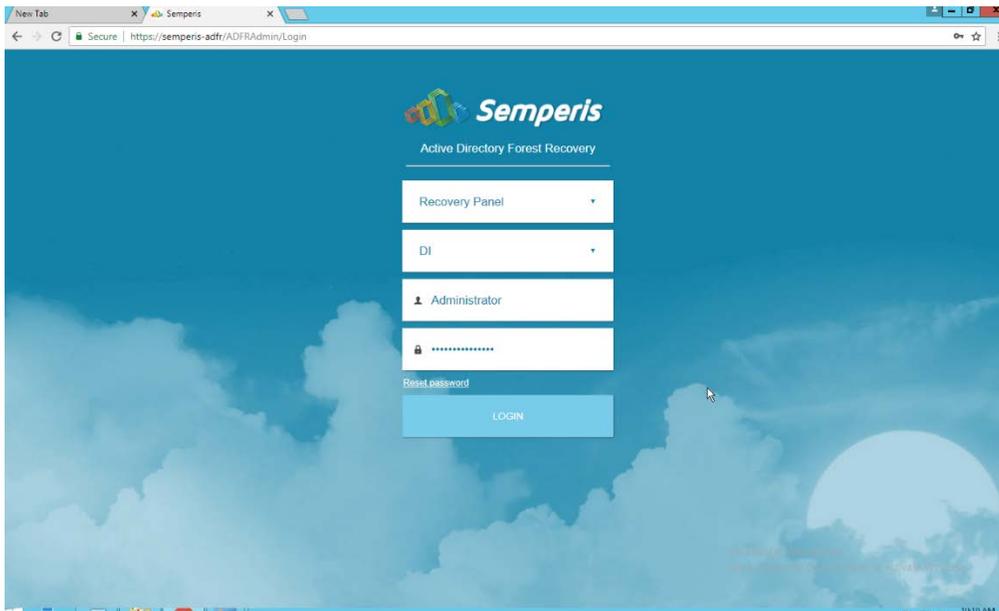
12. Click **OK**.



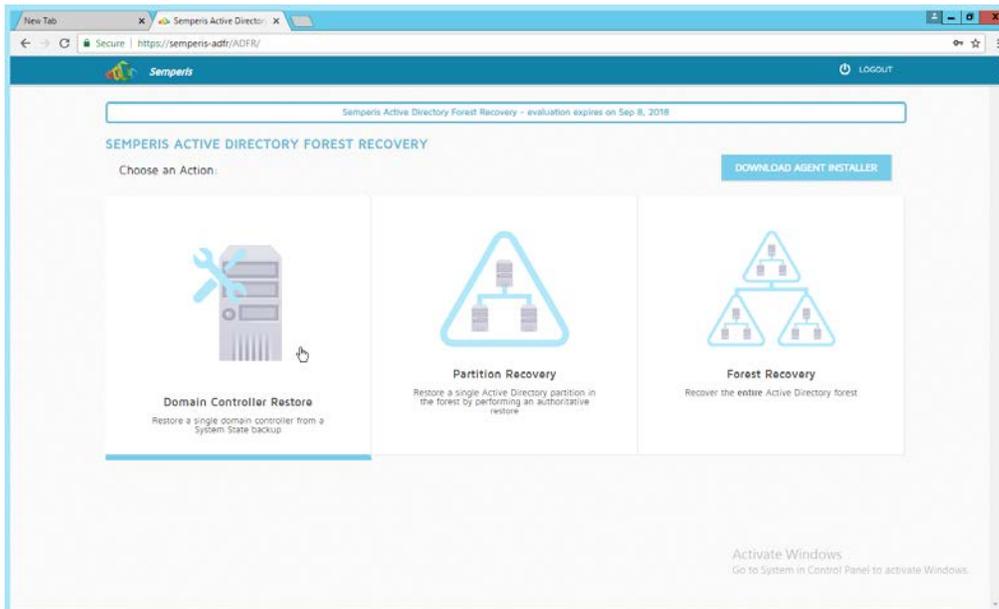
13. Click **Create Rule**.

2.9.3 Recover the Active Directory Forest from a Backup

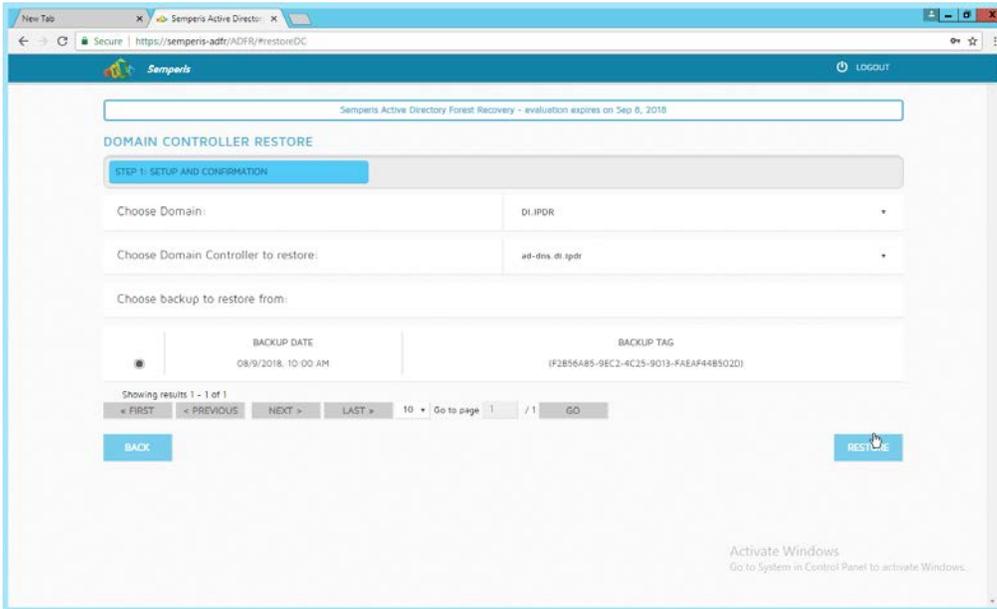
1. Open the **Semperis ADFR** web console.
2. Select **Recovery Panel** from the drop-down.
3. Select the **Domain** that you wish to recover.
4. Enter the **username** and **password**.



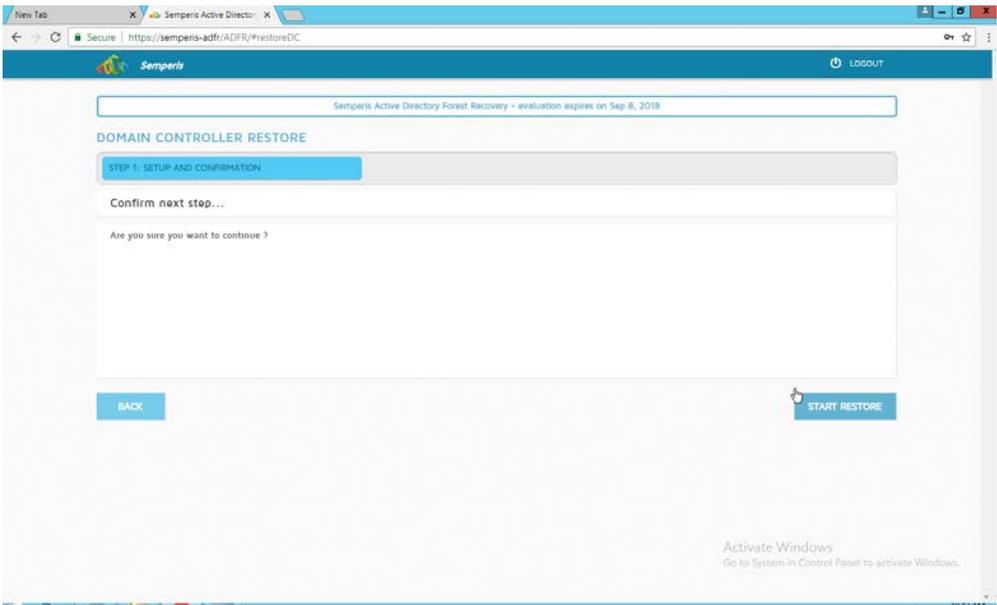
5. Click **Login**.



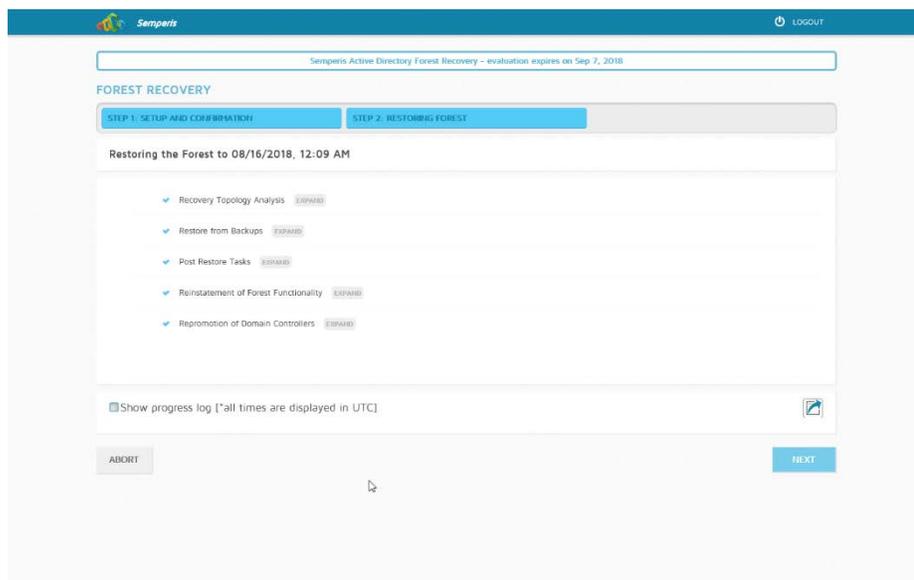
6. Select an action based on the recovery needs of the organization. In this example we select **Domain Controller Restore**.
7. Provide the information for the restoration, namely the **domain**, the **domain controller**, and which backup to use.



8. Click **Restore**.



9. Click **Start Restore** to begin the restoration process.



10. Click **Next** when the restoration finishes.

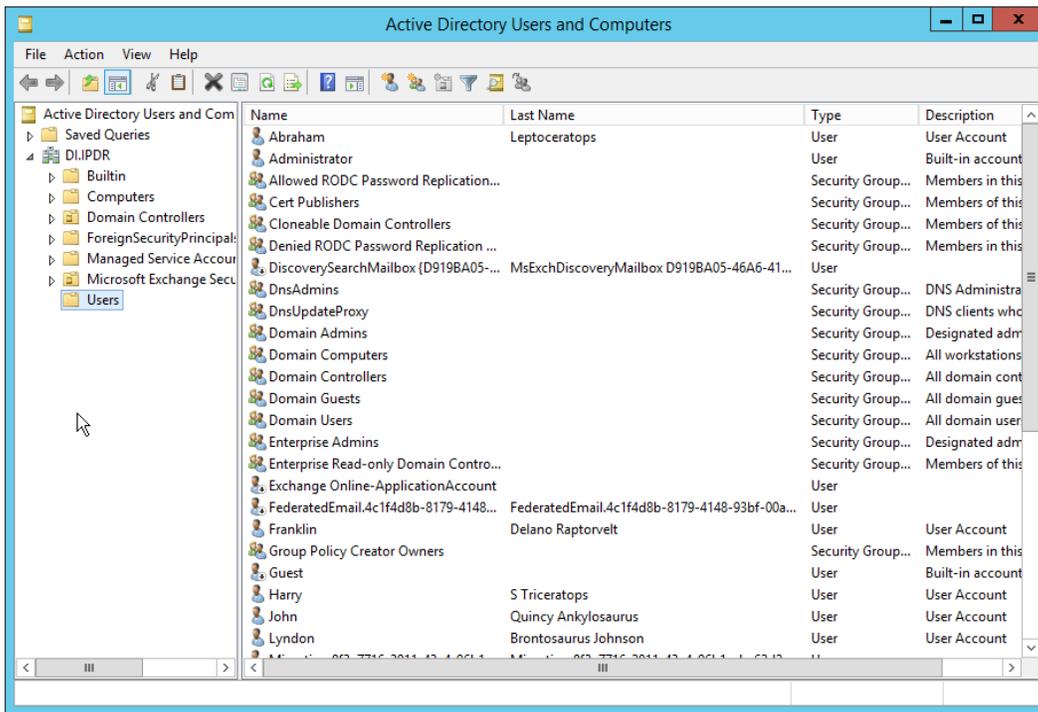
2.10 Semperis Directory Services Protector

This section details the installation of **Semperis Directory Services Protector (DSP)**, a tool used for monitoring Active Directory environments. This installation requires both a copy of SQL Server Express as well as the **Semperis Wizard**. See the **Semperis DS Protector v2.5 Technical Requirements** document for specifics on the requirements. For a Windows Server 2012 R2 installation, simply meet the following requirements:

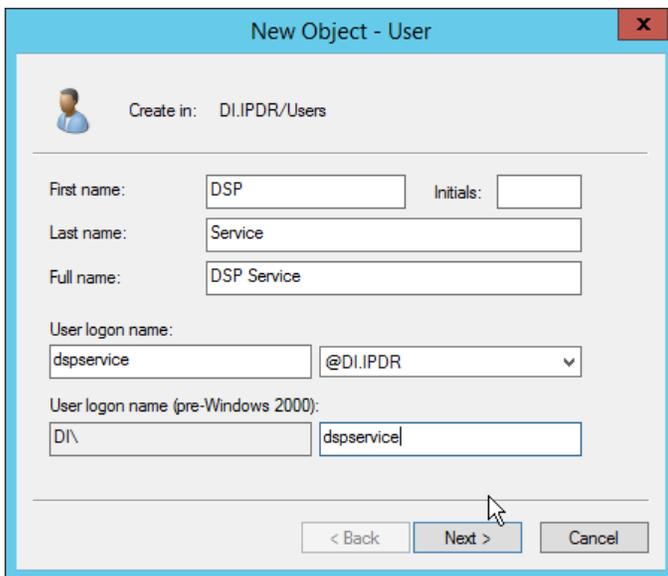
- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- joined to the Active Directory domain it is protecting
- either the installer for SQL Express Advanced or connection information and credentials for a full version of Microsoft SQL (MSSQL)

2.10.1 Configure Active Directory for Semperis DSP

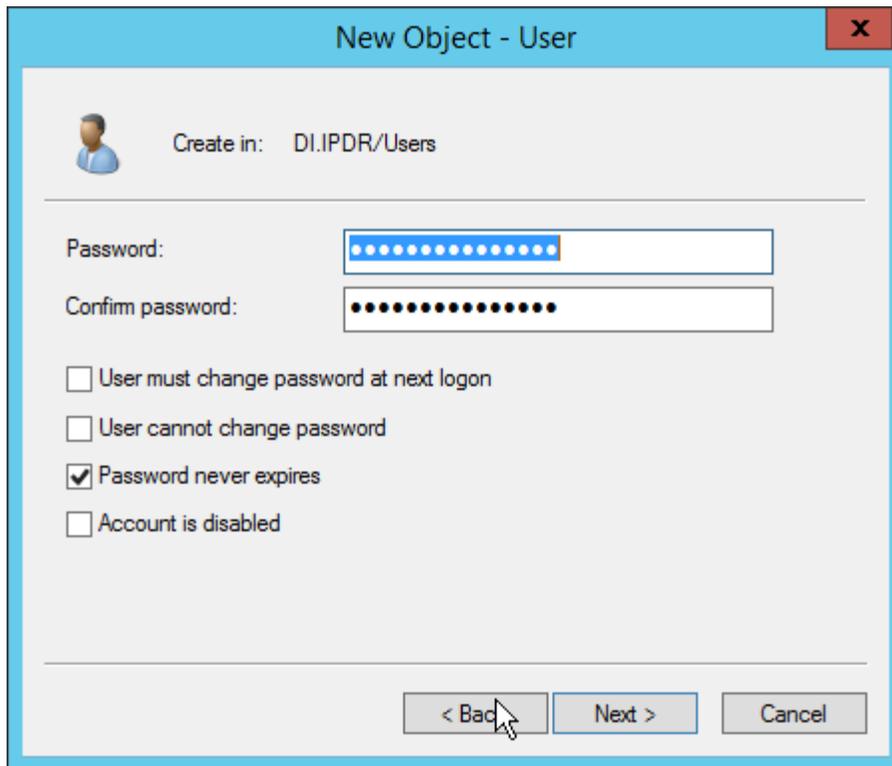
1. Open **Active Directory Users and Computers**.



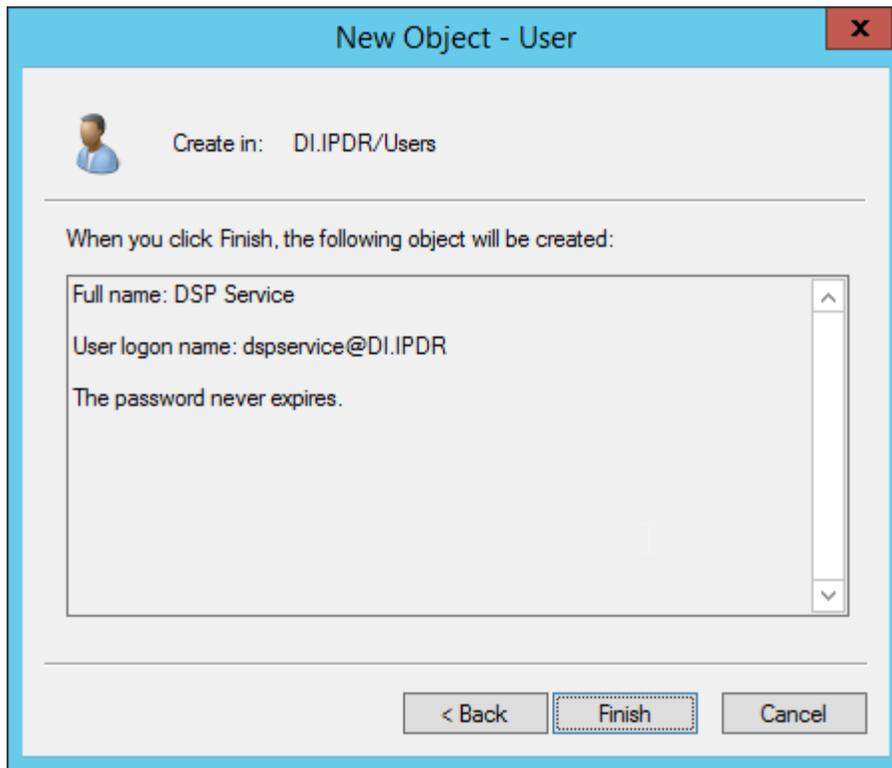
2. Right-click **Users** in the left pane and select **New > User**.
3. Enter the information for a new user for the DSP service.



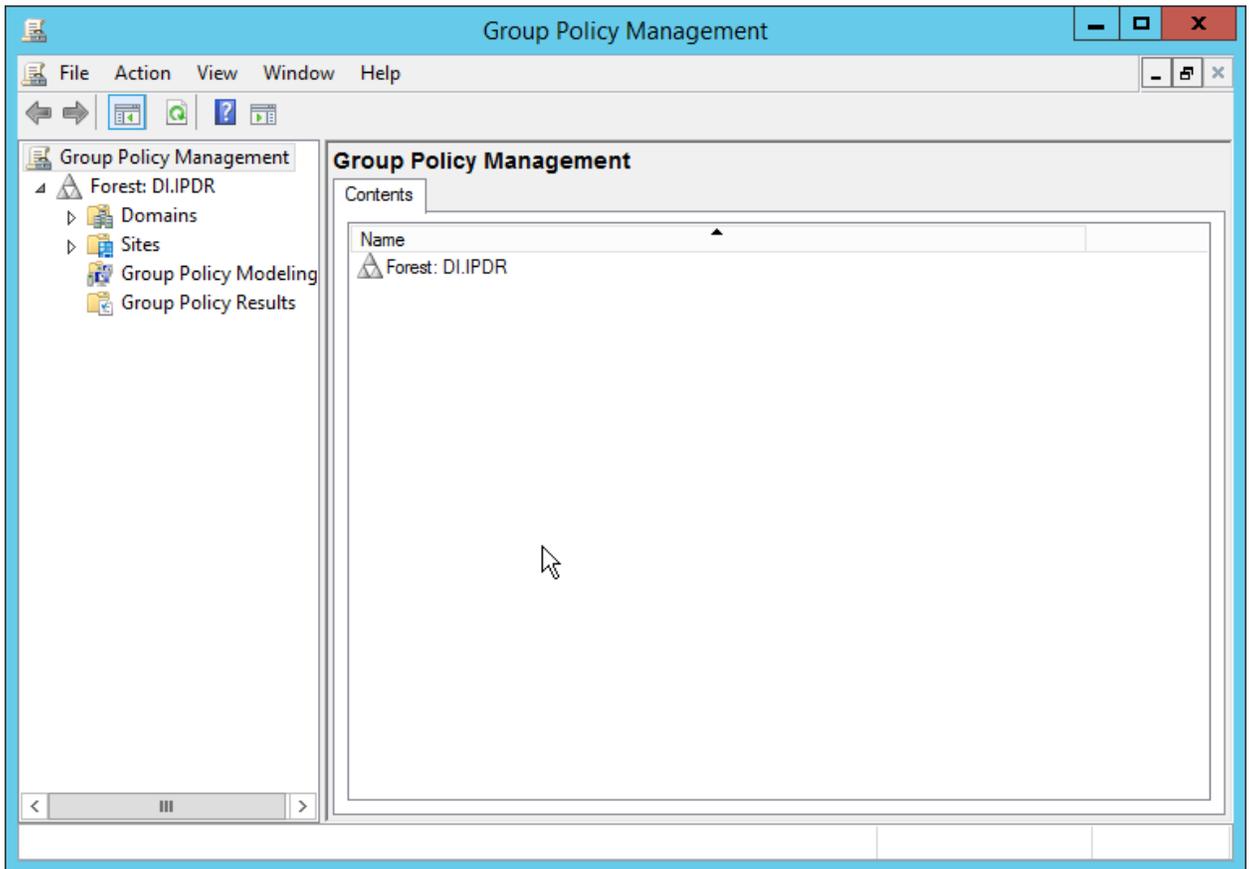
4. Click **Next**.
5. Enter a **password** twice for this user.
6. Set the password policy.



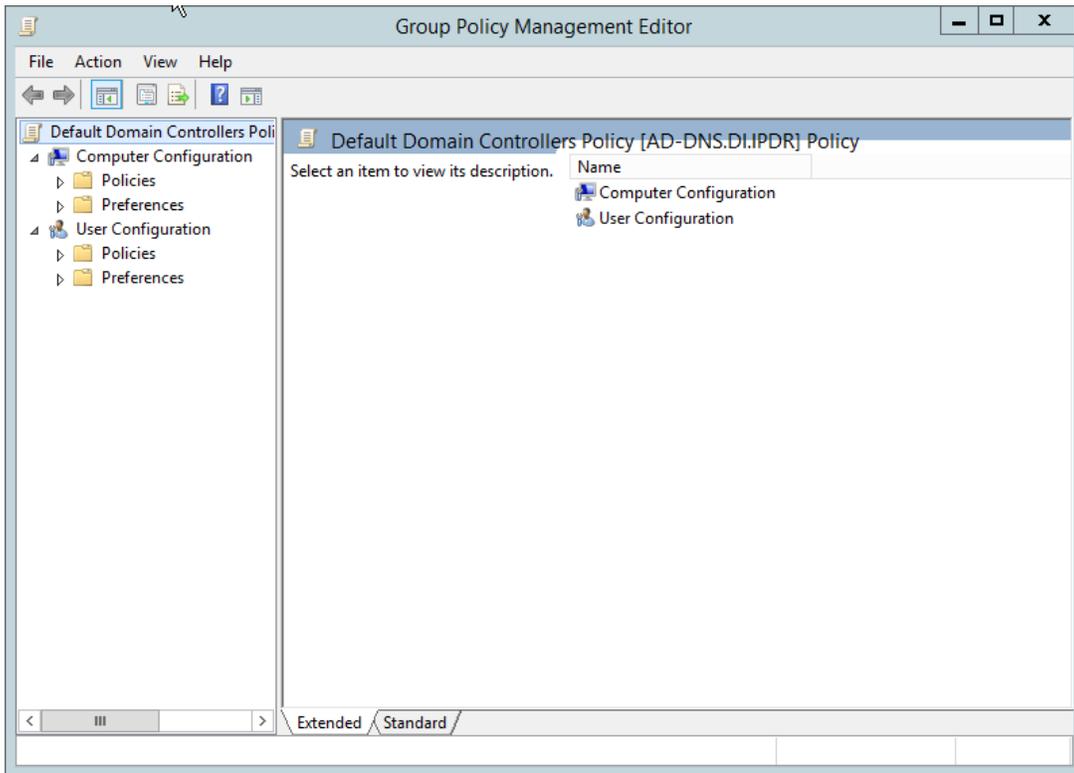
7. Click **Next**.



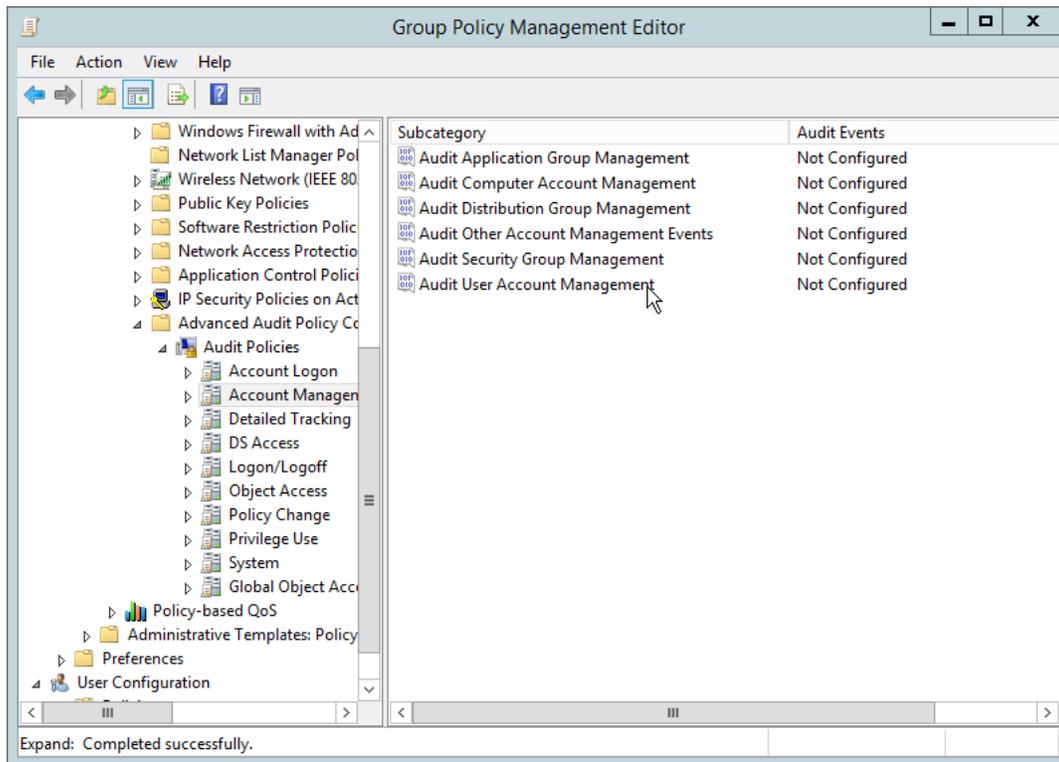
8. Click **Finish**.
9. Open **Group Policy Management**.



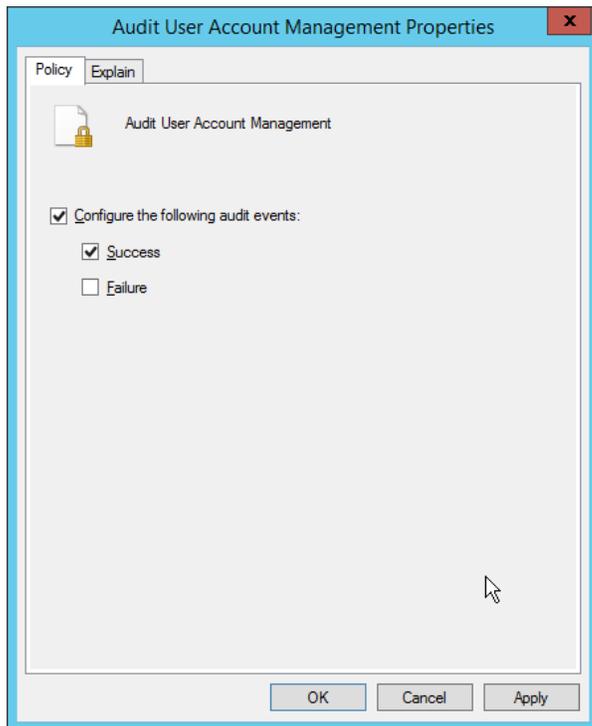
10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy** and click **Edit**.



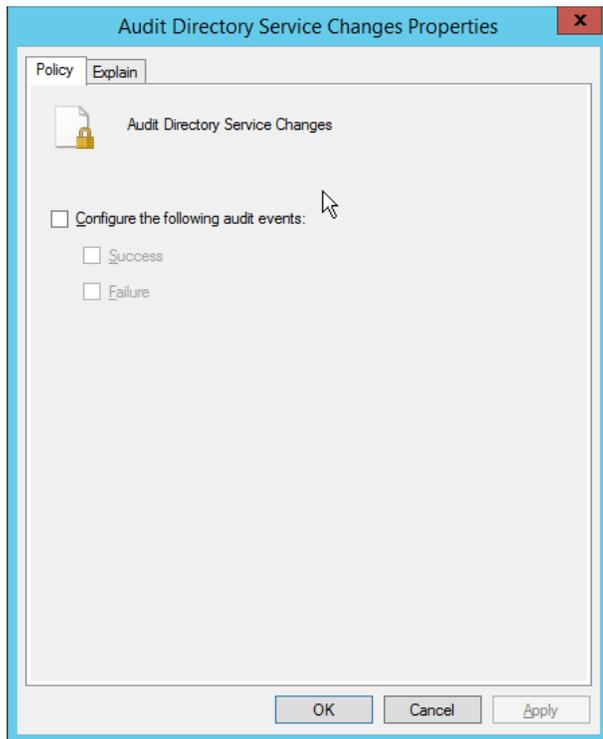
11. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management**.



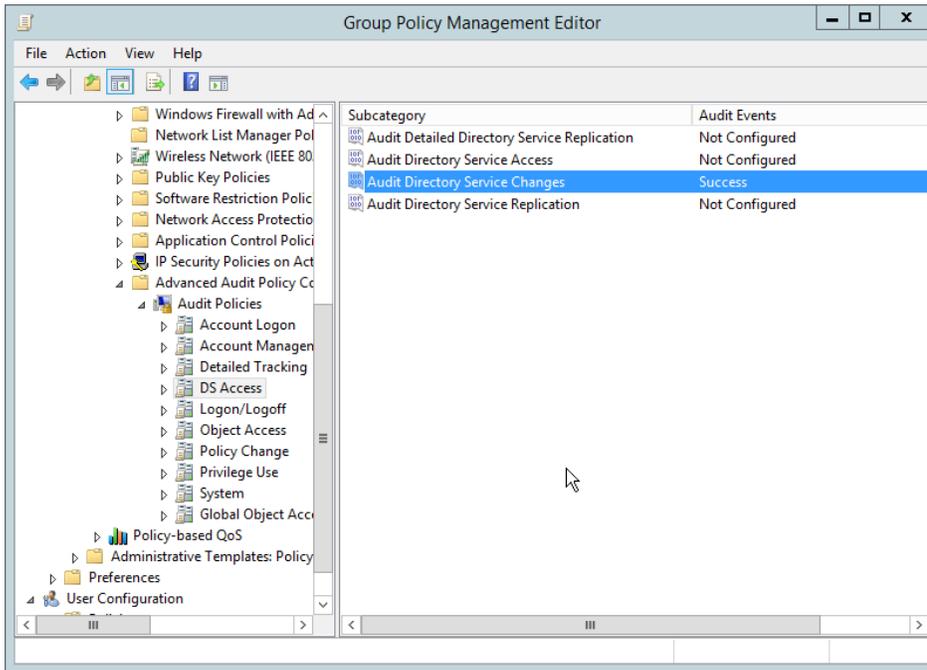
12. Edit the **Audit User Account Management** field by double-clicking it.
13. Check the box next to **Configure the following audit events**.
14. Check the box next to **Success**.



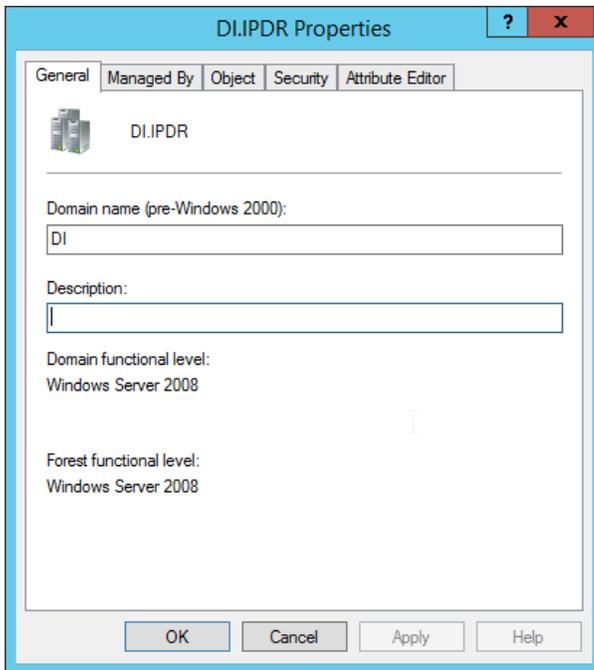
15. Click **OK**.
16. Go to **Audit Policies > DS Access**.
17. Double-click **Audit Directory Service Changes**.



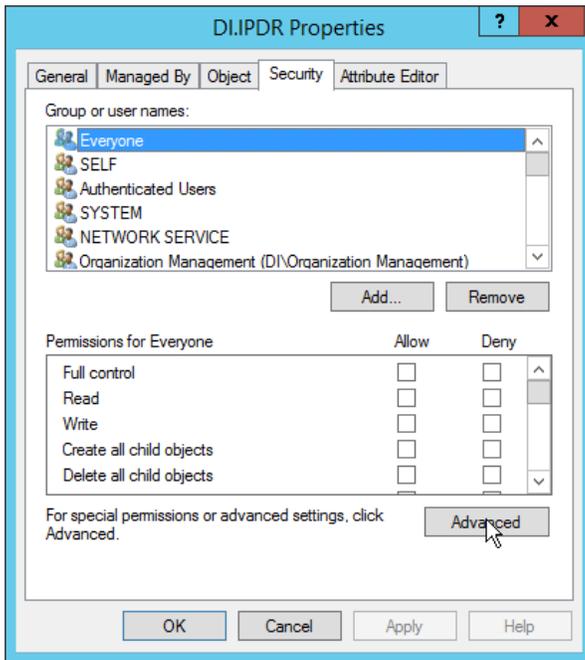
18. Check the box next to **Configure the following audit events**.
19. Check the box next to **Success**.
20. Click **OK**.



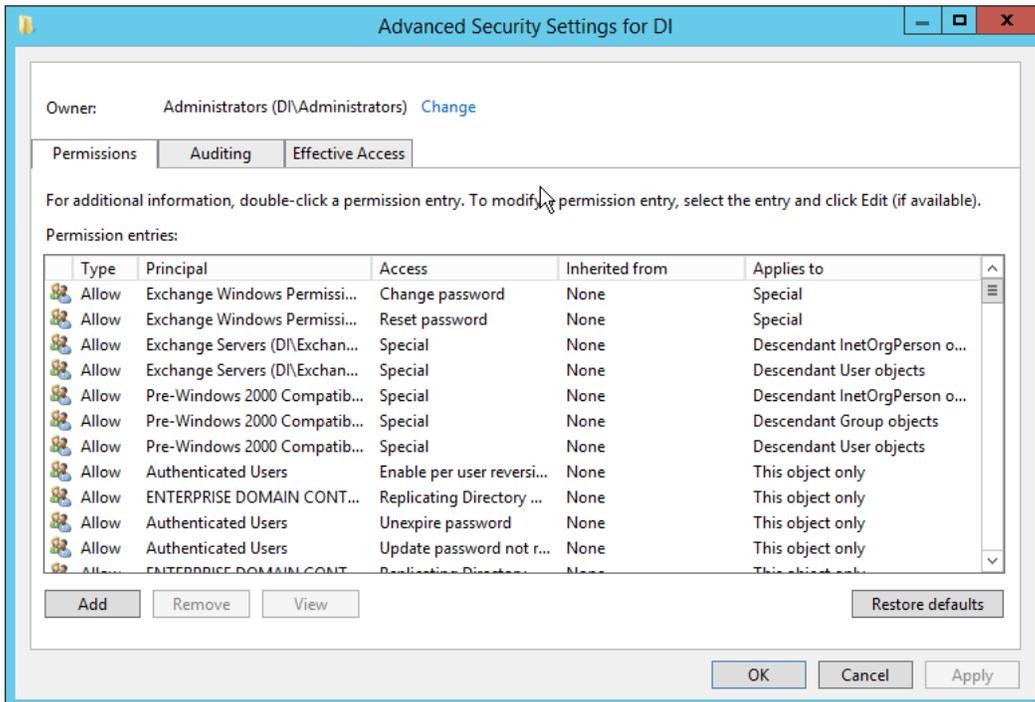
21. Open **Active Directory Users and Computers**.
22. Ensure that **View > Advanced Features** is enabled.
23. Right-click the **domain** (for example, DI.IPDR) created earlier and click **Properties**.



24. Click the **Security** tab.



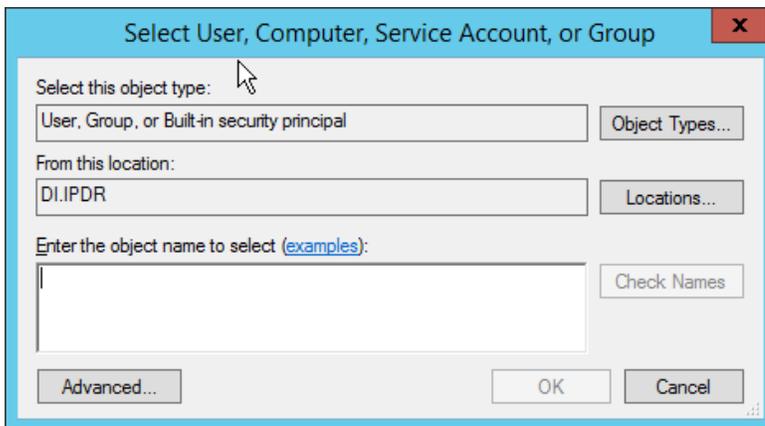
25. Click **Advanced**.



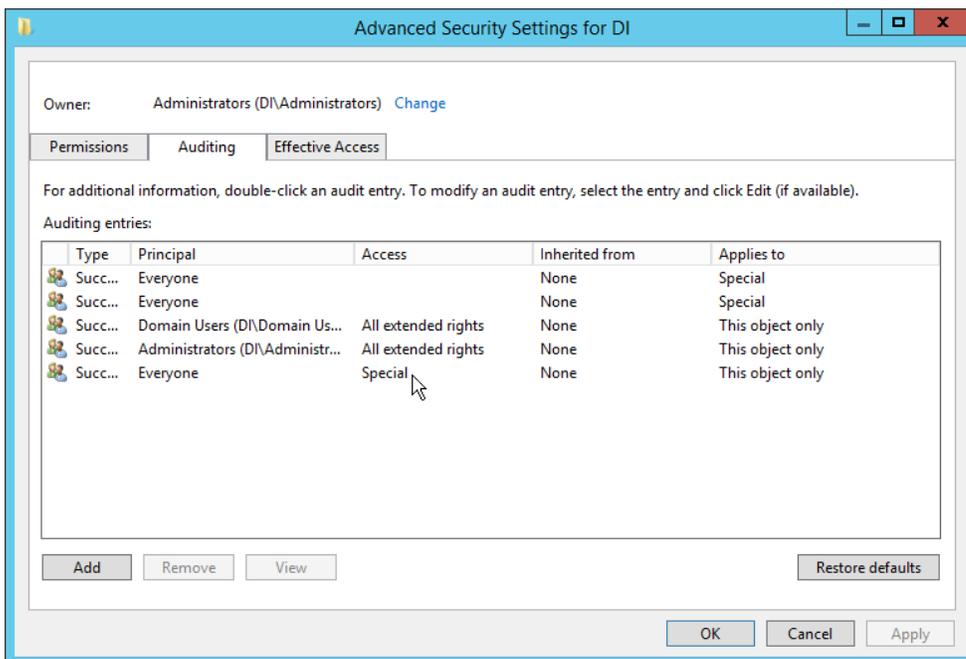
26. Click the **Auditing** tab.

27. Click **Add**.

28. Enter **Everyone**.

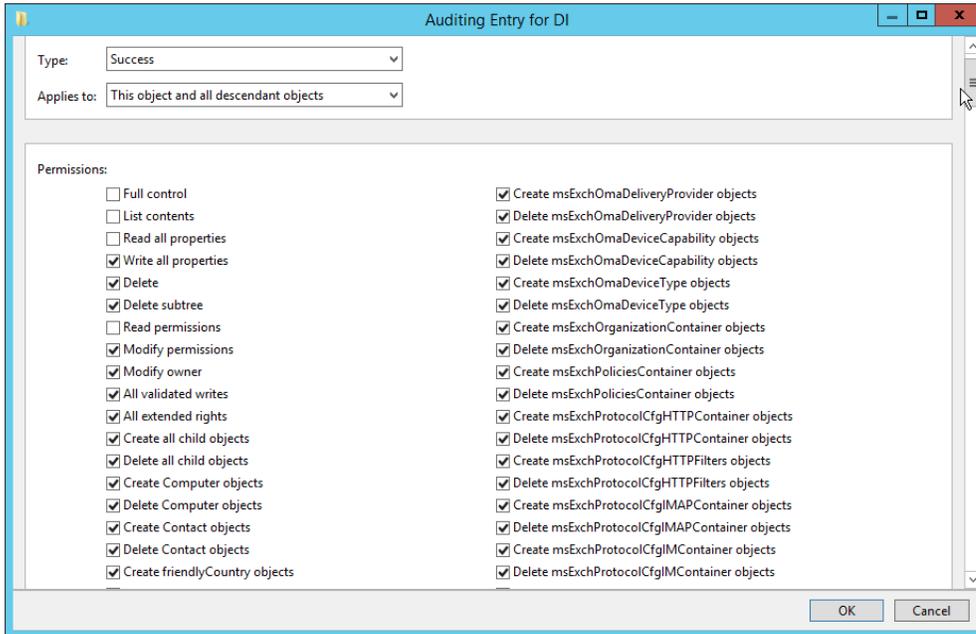


29. Click **OK**.

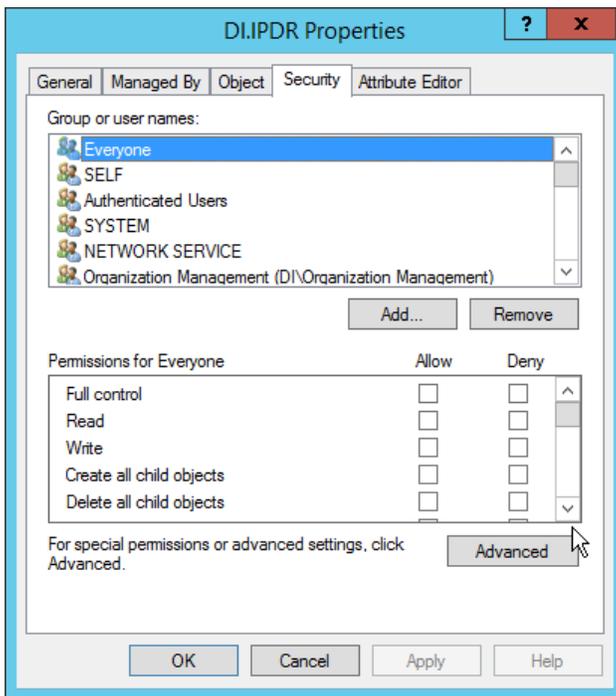


30. Double-click **Everyone**.

31. Check the boxes next to **Write all properties, Delete, Delete subtree, Modify permissions, Modify owner, All validated writes, All extended rights, Create all child objects, Delete all child objects**.



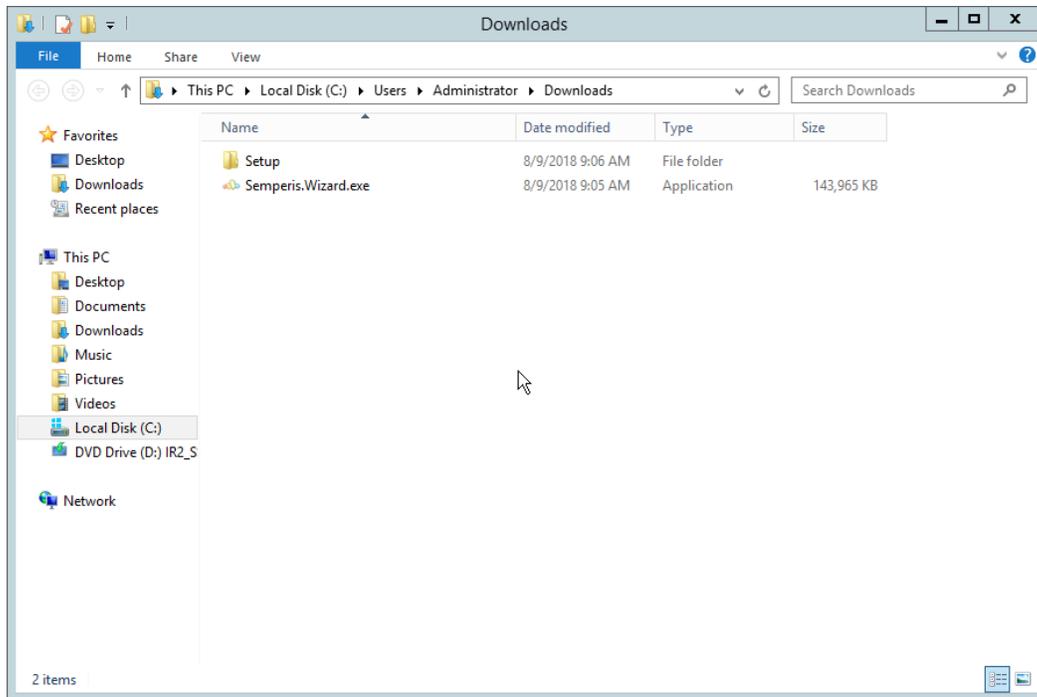
32. Click **OK**.



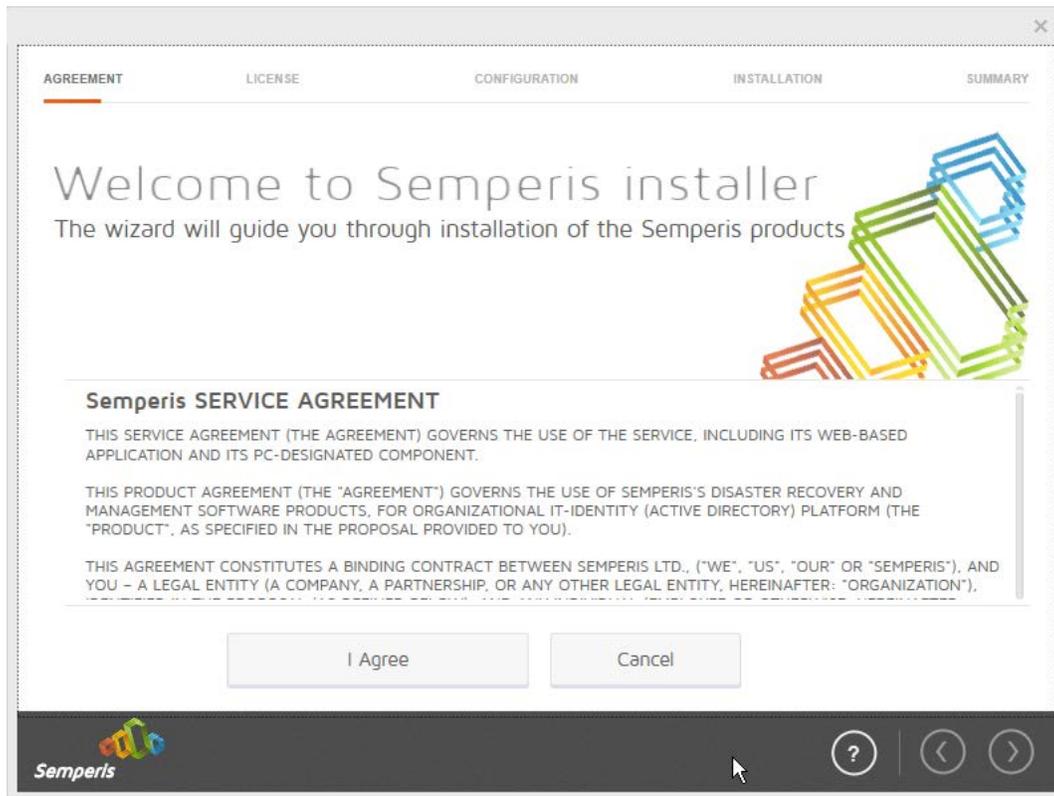
33. Click **OK**.

2.10.2 Install Semperis DSP

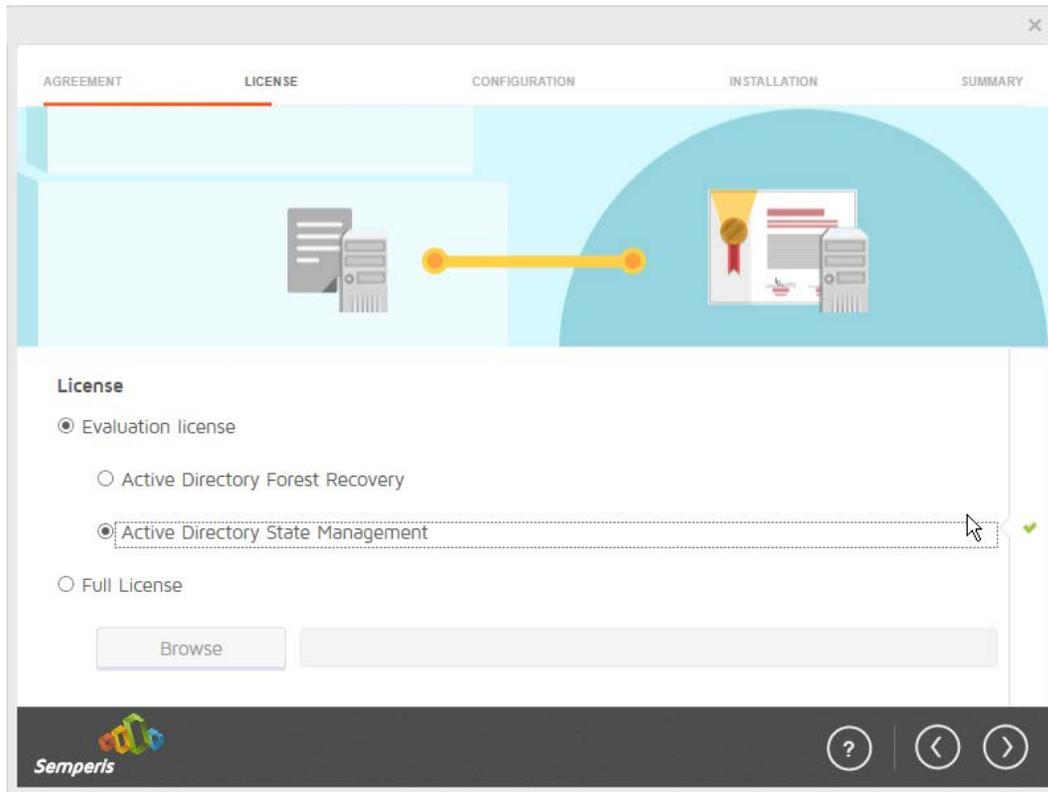
1. If you are using a local SQL Express Advanced server, place the **SQLXPRADV_x64_ENU.exe** installer in a directory called Setup, and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it). If an SQL Express Advanced server is not being used, no **Setup** folder is required.



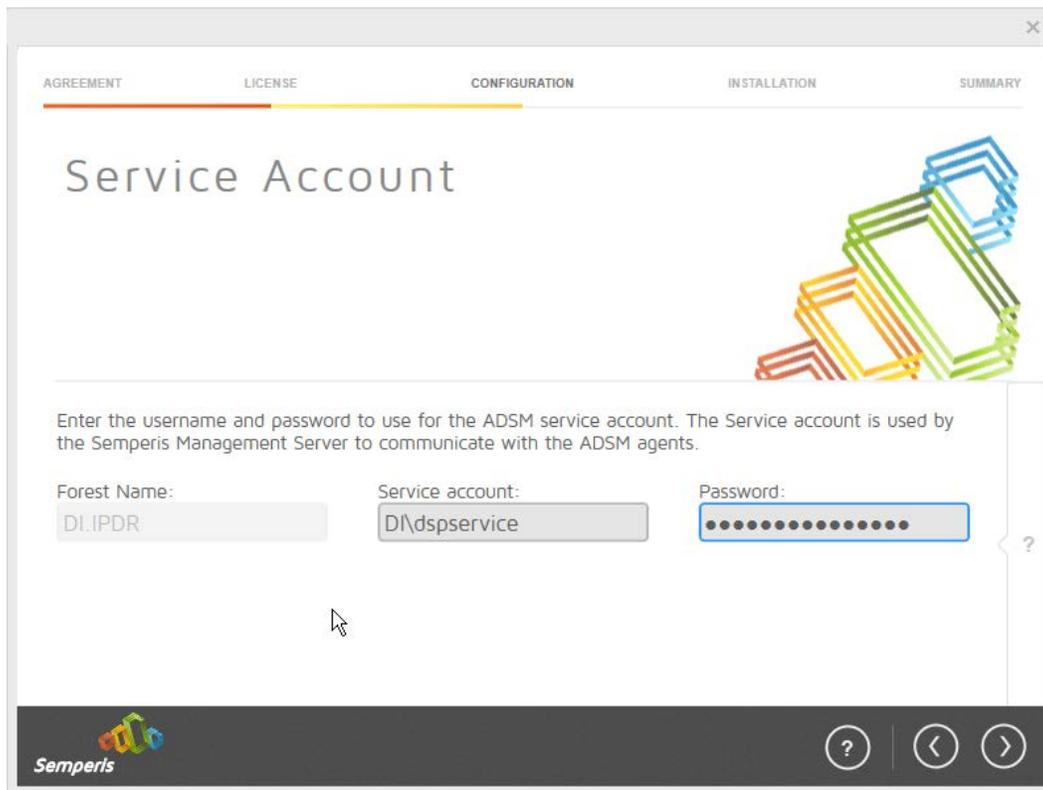
2. If prompted to restart the computer, do so.



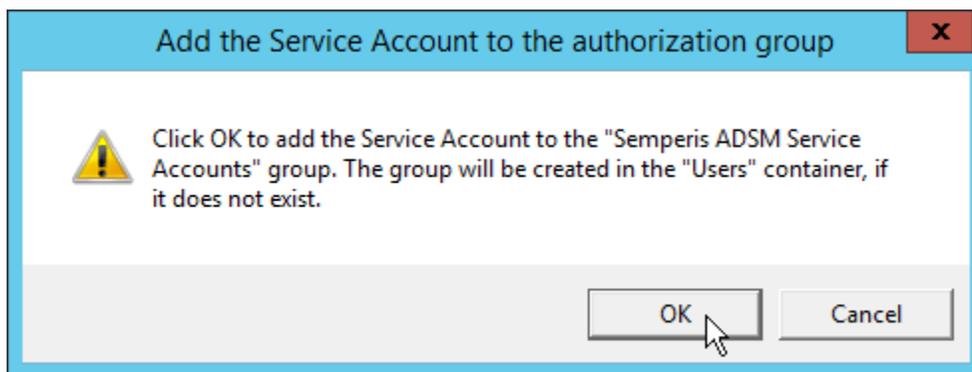
3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory State Management**.



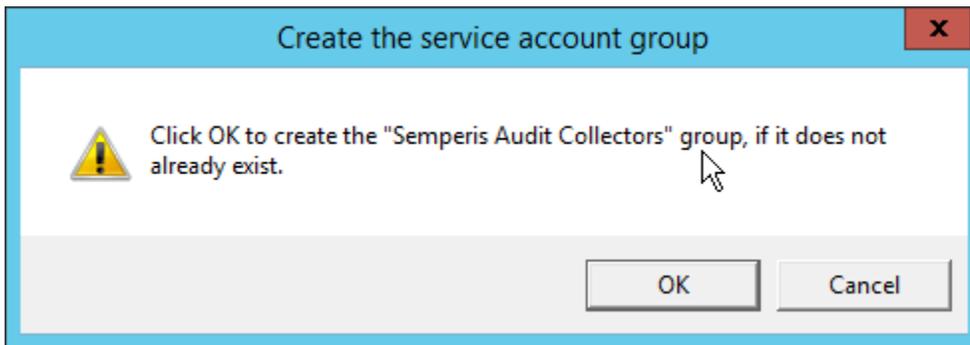
6. Click the > button.
7. Enter the **username** and **password** of the account created earlier.



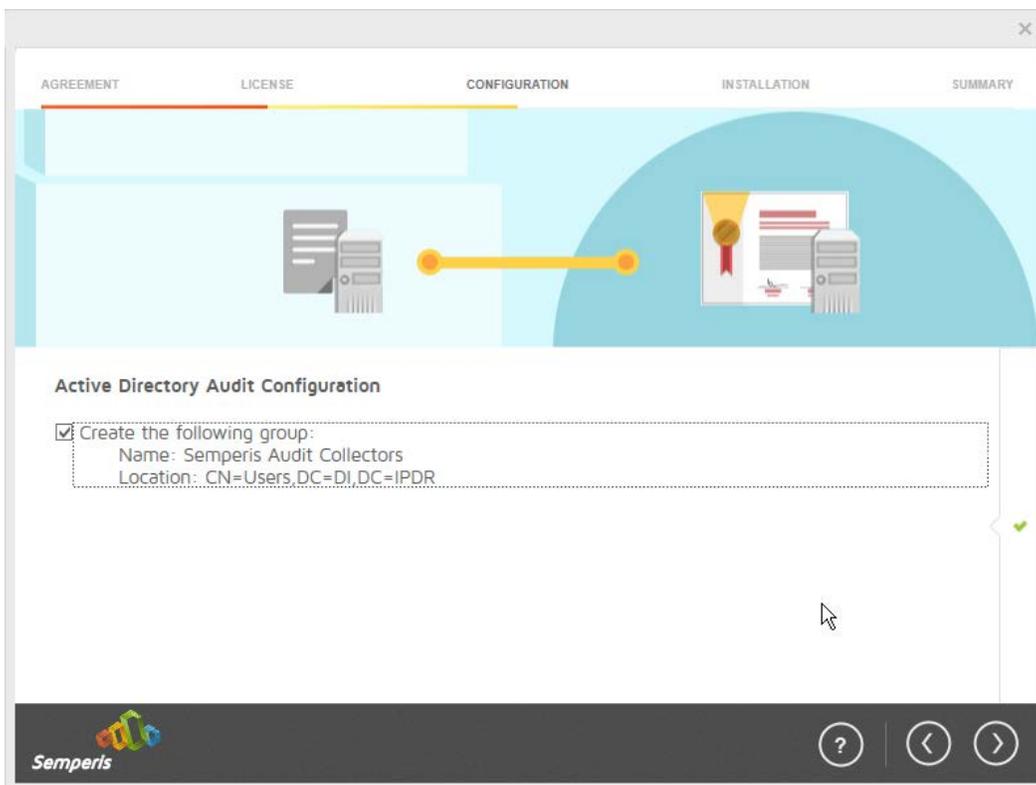
8. Click the > button.



9. Click **OK**.
10. Check the box next to **Create the following group**.

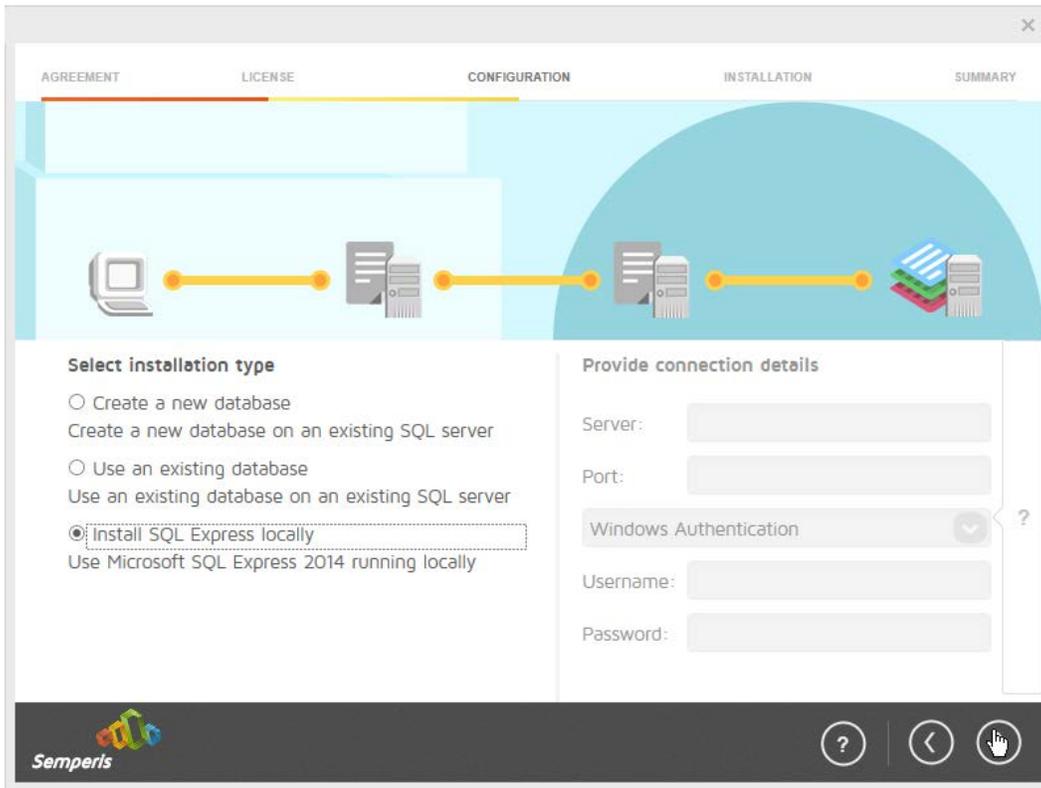


11. Click **OK**.

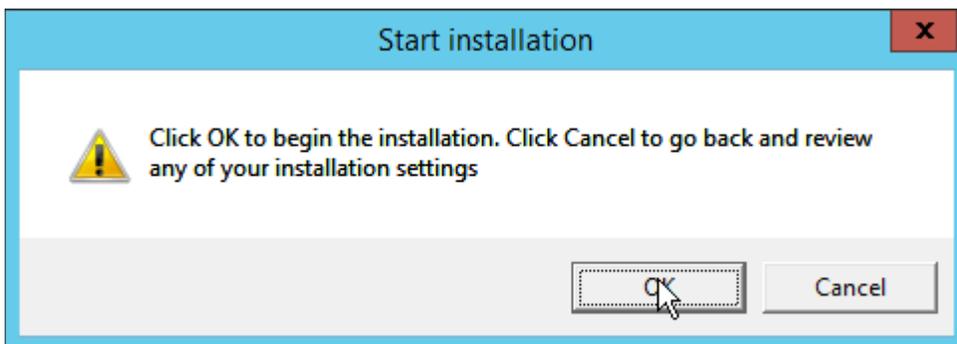


12. Click the > button.

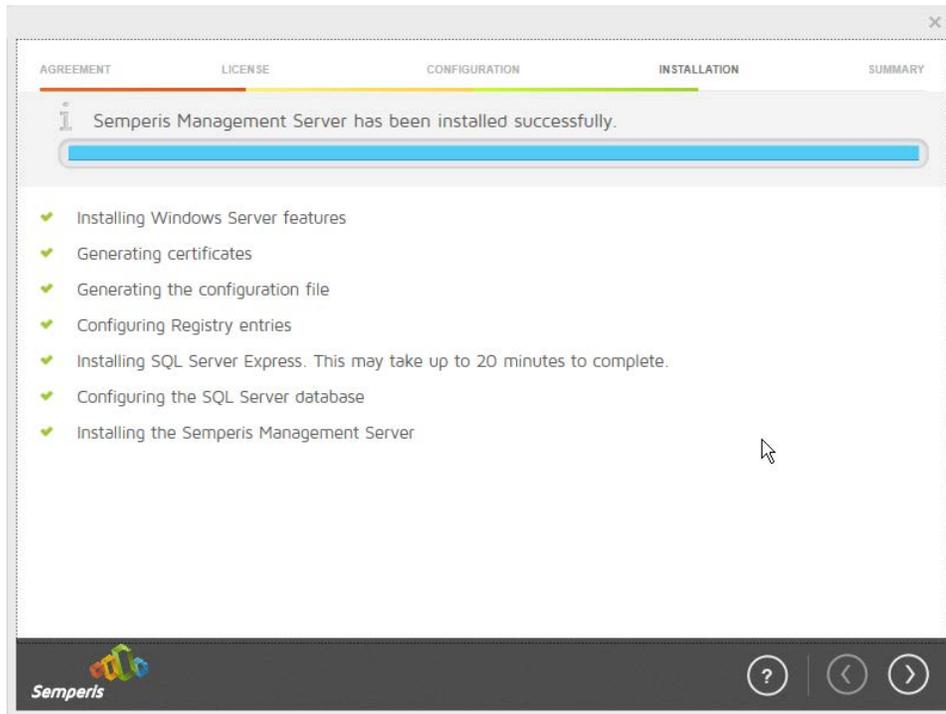
13. Select the appropriate database option, and enter any required information.



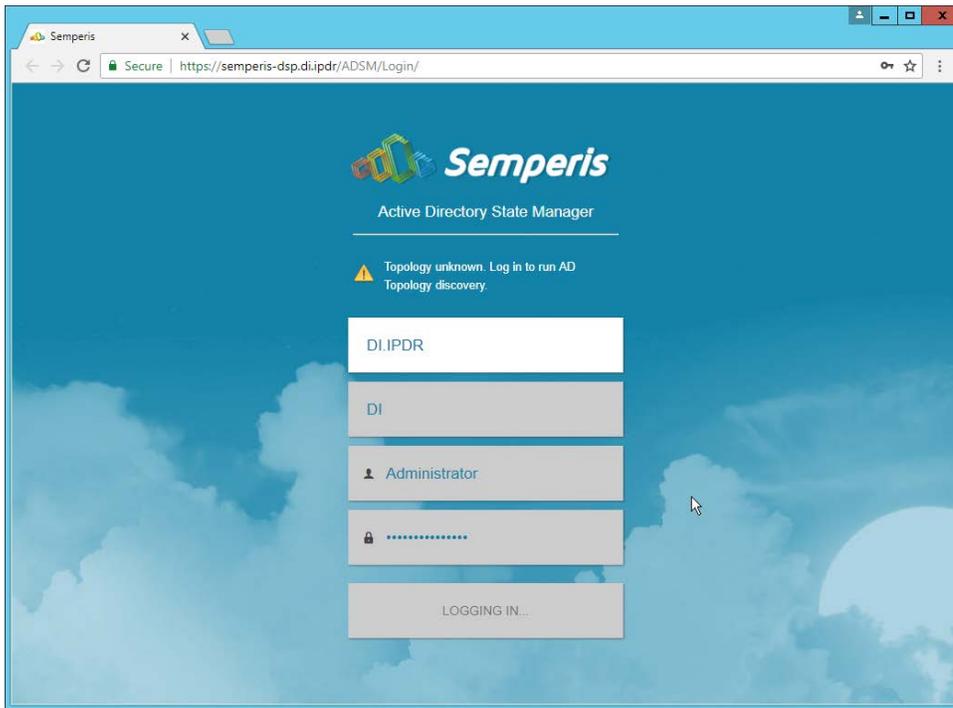
14. Click the > button.



15. Click **OK**.

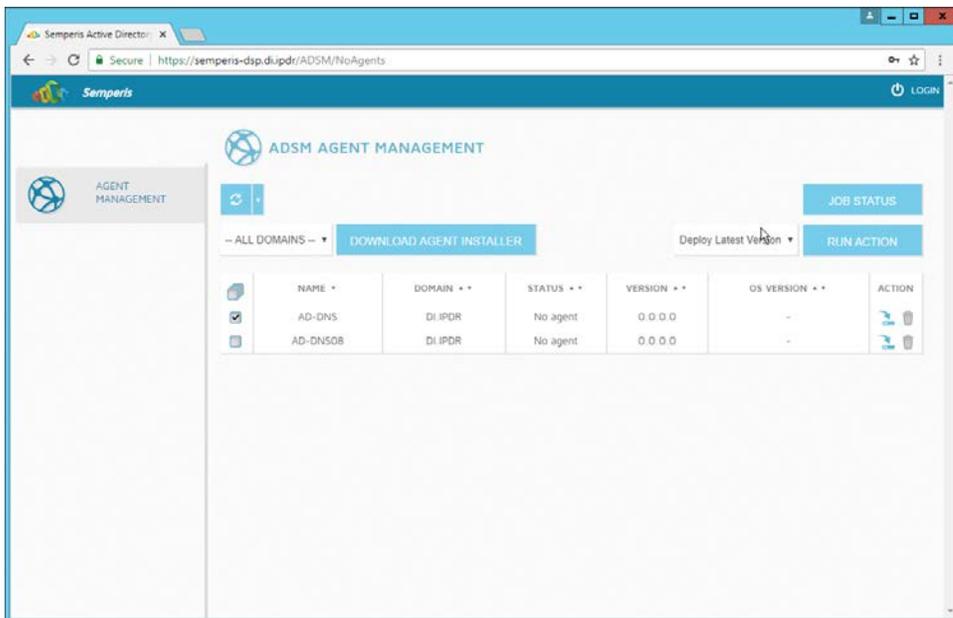


16. Click the > button after the installation completes.
17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector**.
18. On the login page, enter the full domain as well as the NetBIOS name.
19. Enter the **username** and **password** of an administrator on the domain.



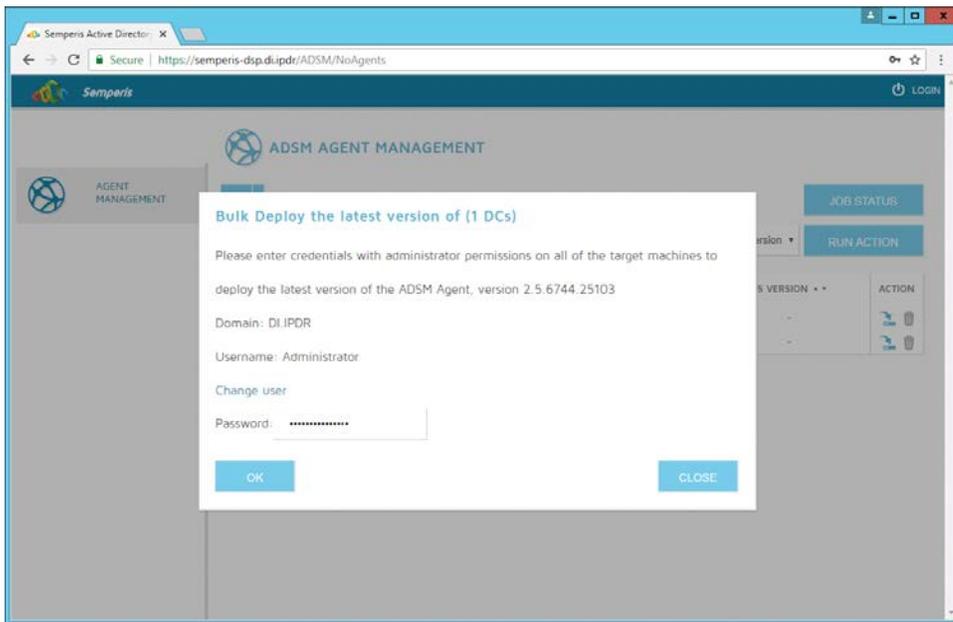
20. Click **Login**.

21. Check the box next to the domain controllers that should be monitored by DSP.

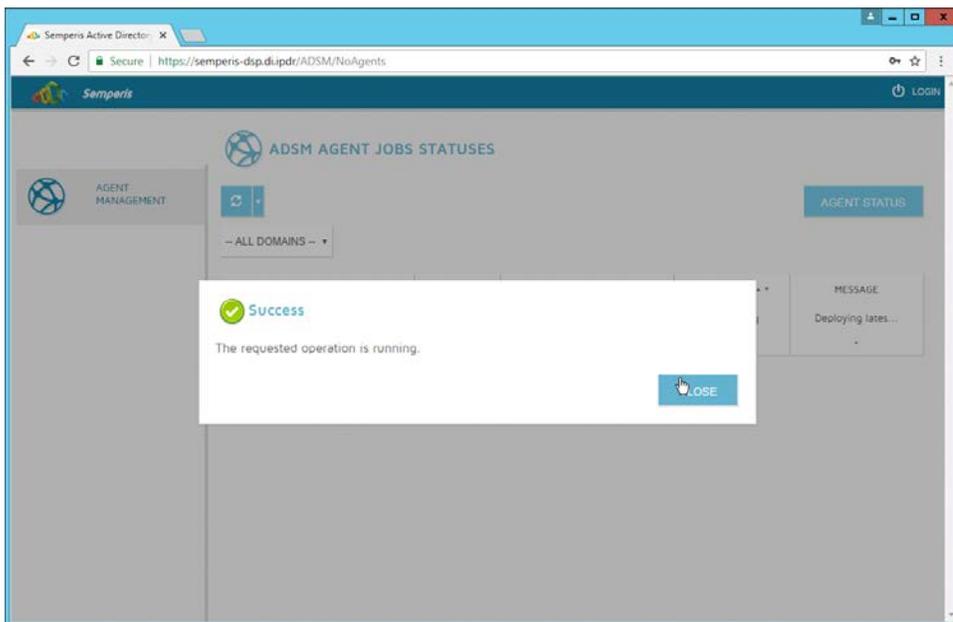


22. Click **Run Action**.

23. Enter the **password** for the account.

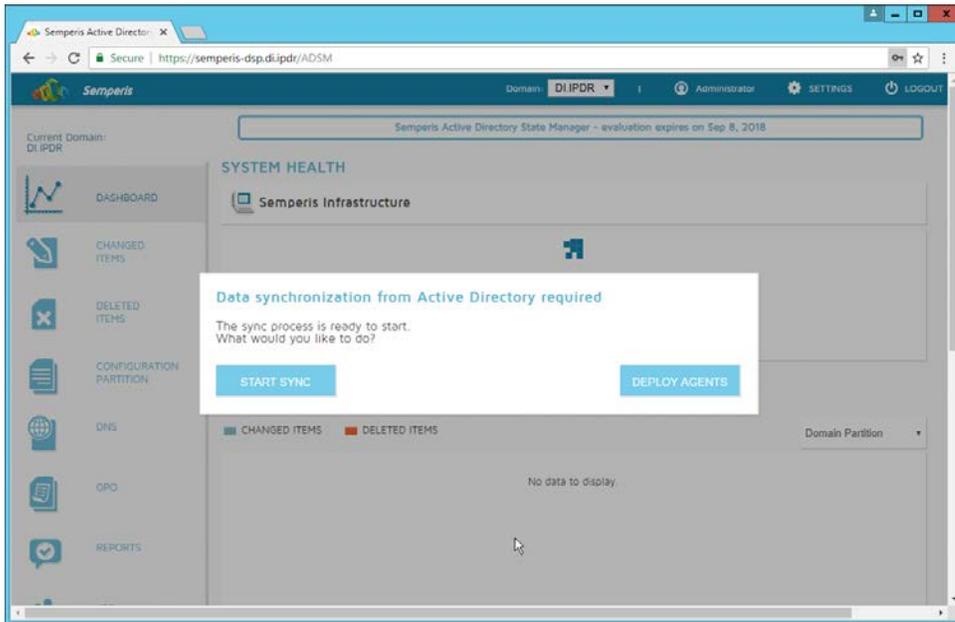


24. Click **OK**.



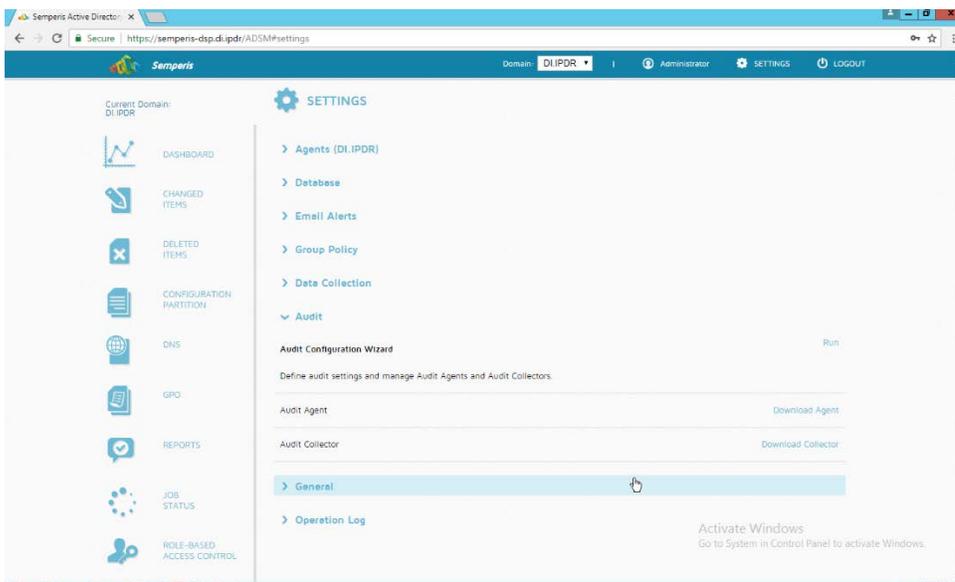
25. Click **Close**.

26. After the agent finishes deploying, click **Login** at the top of the page and log in.



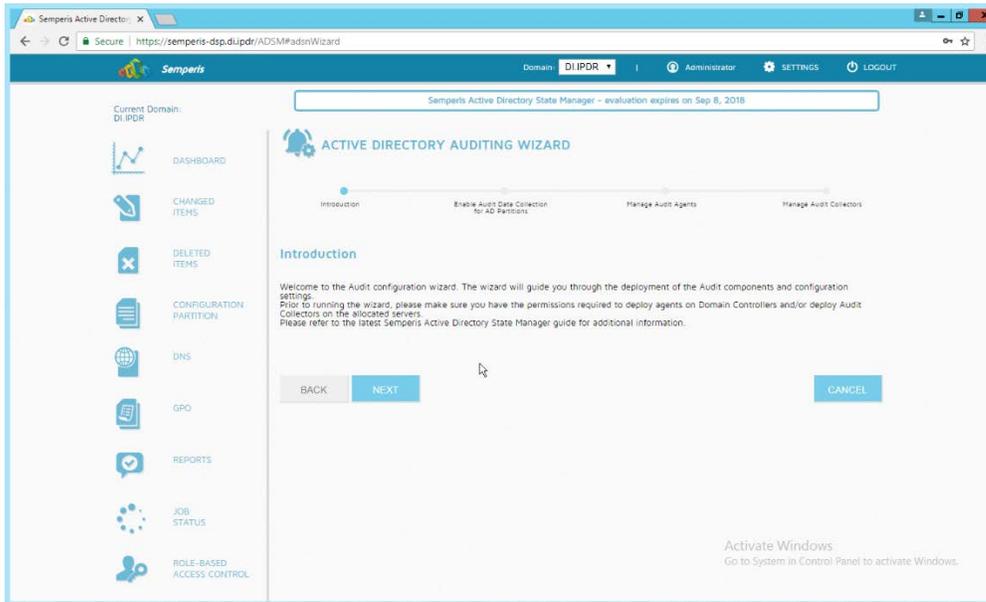
27. Click **Start Sync**.

28. After this completes, click **Settings** at the top of the page.

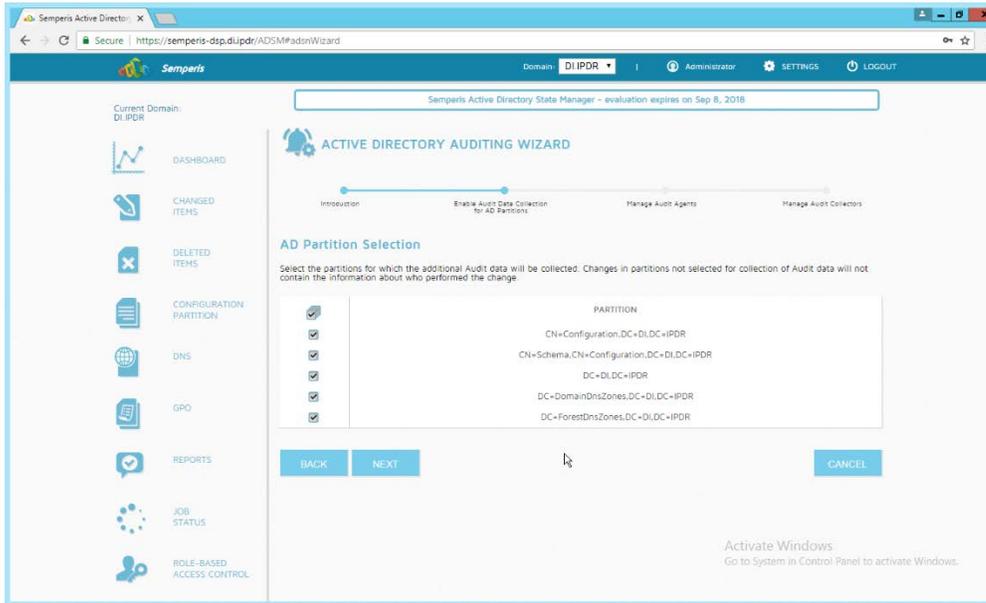


29. Click **Audit**.

30. Click **Run**.

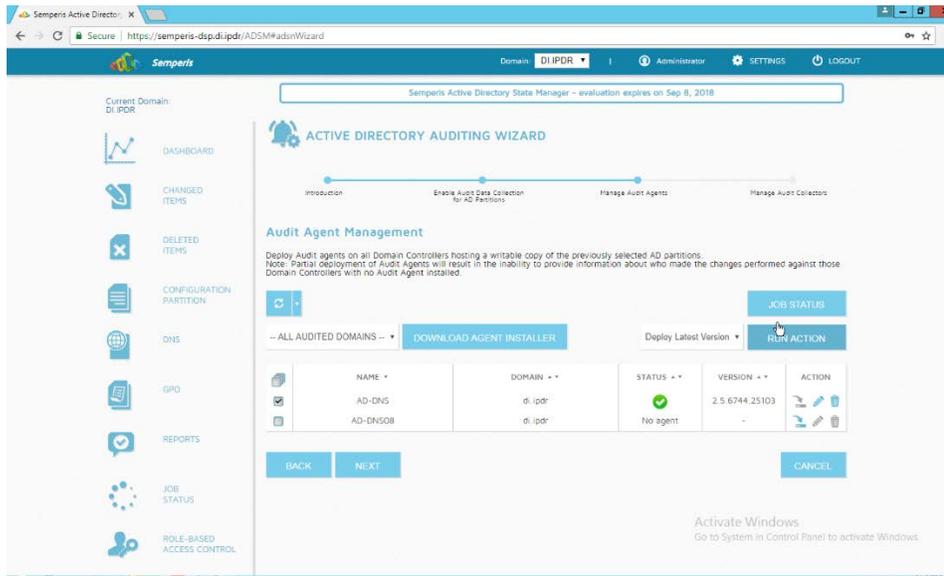


31. Click **Next**.

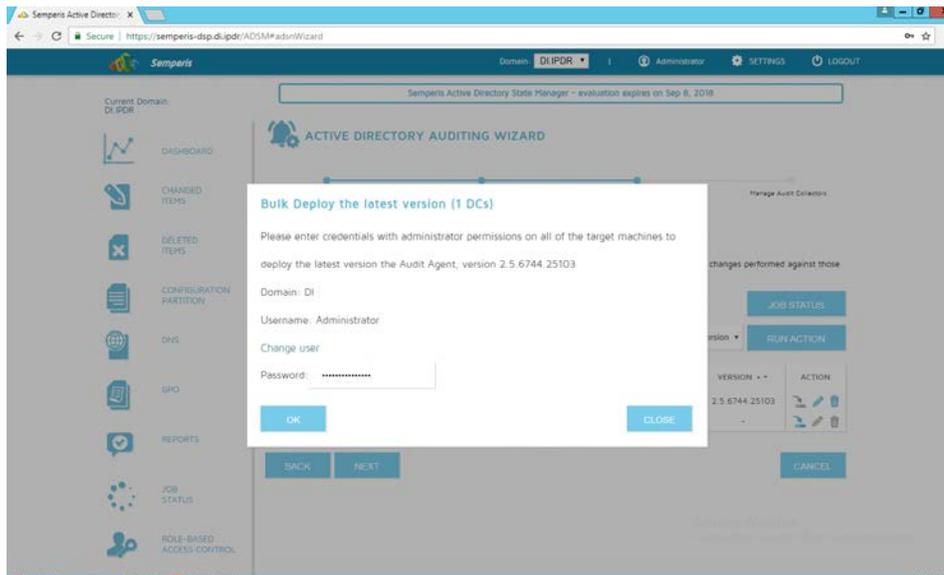


32. Click **Next**.

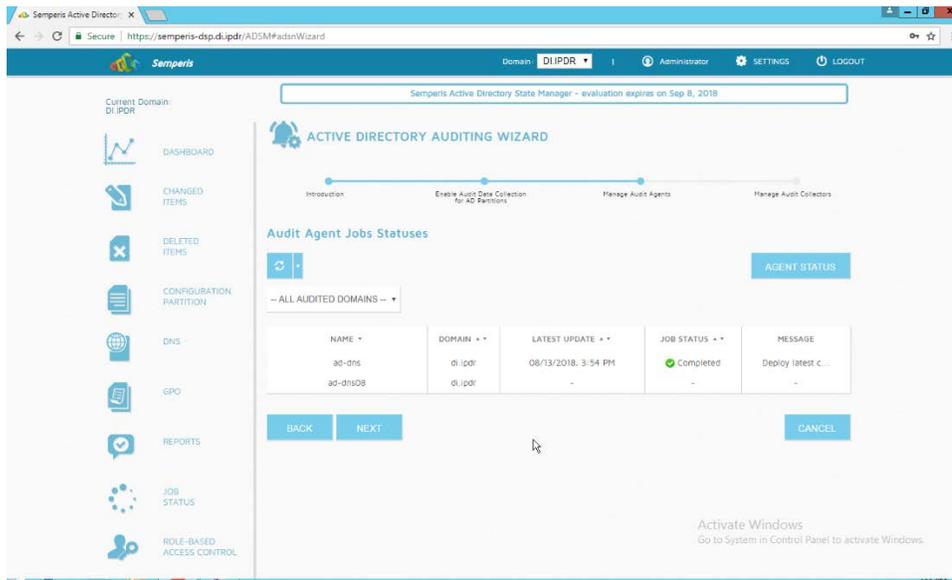
33. Check the boxes next to any Domain Controllers that should be monitored.



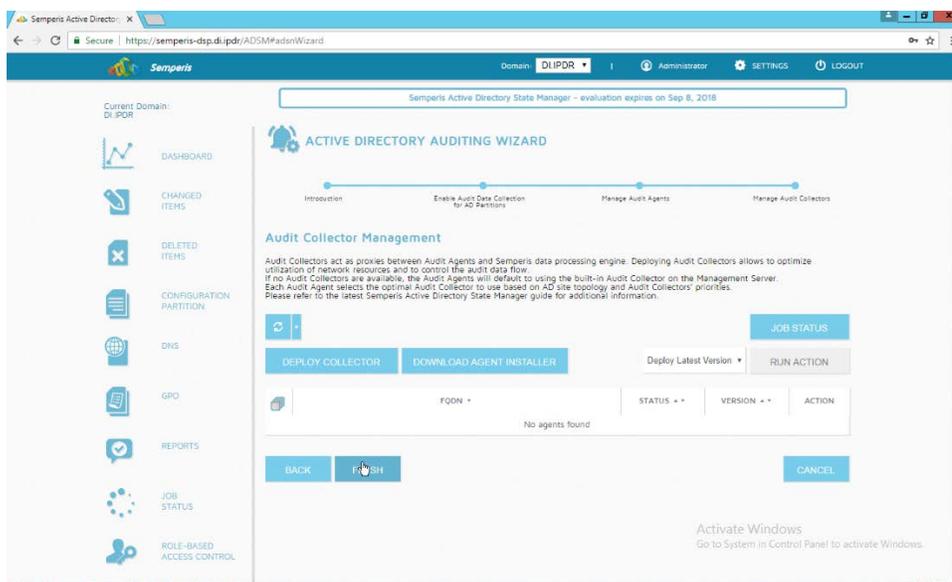
- 34. Click **Run Action**.
- 35. Enter the **password**.



- 36. Click **OK**.
- 37. Wait for the deployment to finish.



38. Click **Next**.



39. Click **Finish**.

2.11 Micro Focus ArcSight Enterprise Security Manager

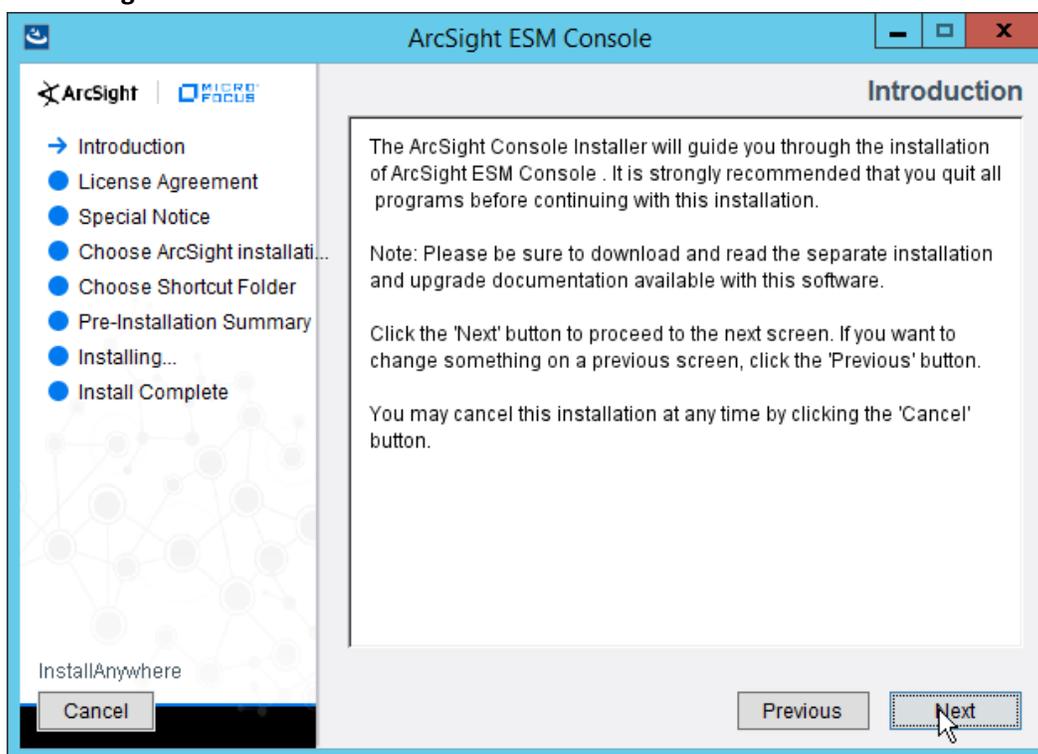
Micro Focus ArcSight Enterprise Security Manager is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

This installation guide assumes a preconfigured CentOS 7 machine with Enterprise Security Manager (ESM) already installed and licensed. This section covers the installation and configuration process used to set up ArcSight agents on various machines, as well as some analysis and reporting capabilities.

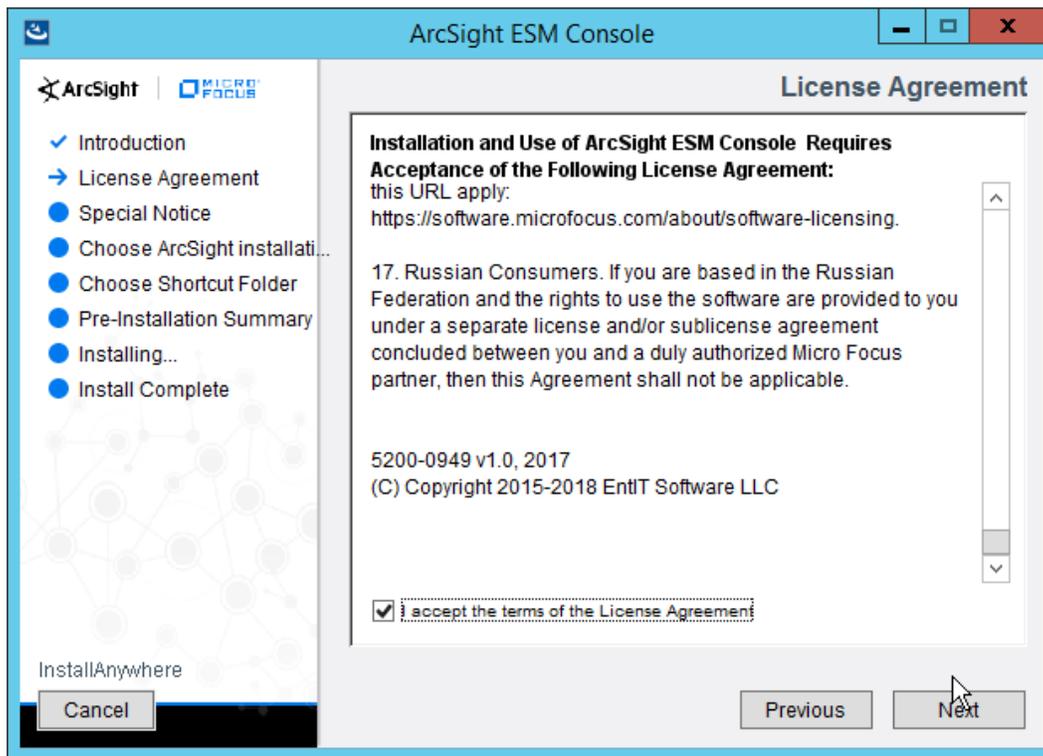
Installation instructions are included for both Windows and UNIX machines, as well as for collecting from multiple machines. Furthermore, integrations with other products in the build are included in later sections.

2.11.1 Install the ArcSight Console

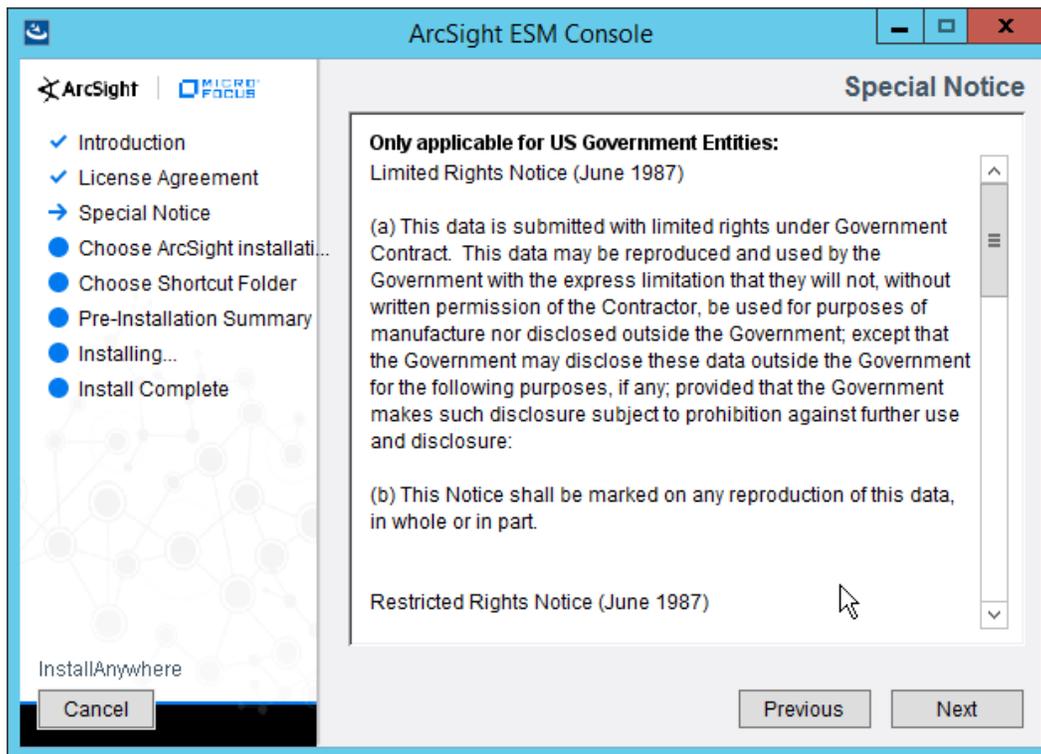
1. Run **ArcSight-7.0.0.2436.1-Console-Win.exe**.



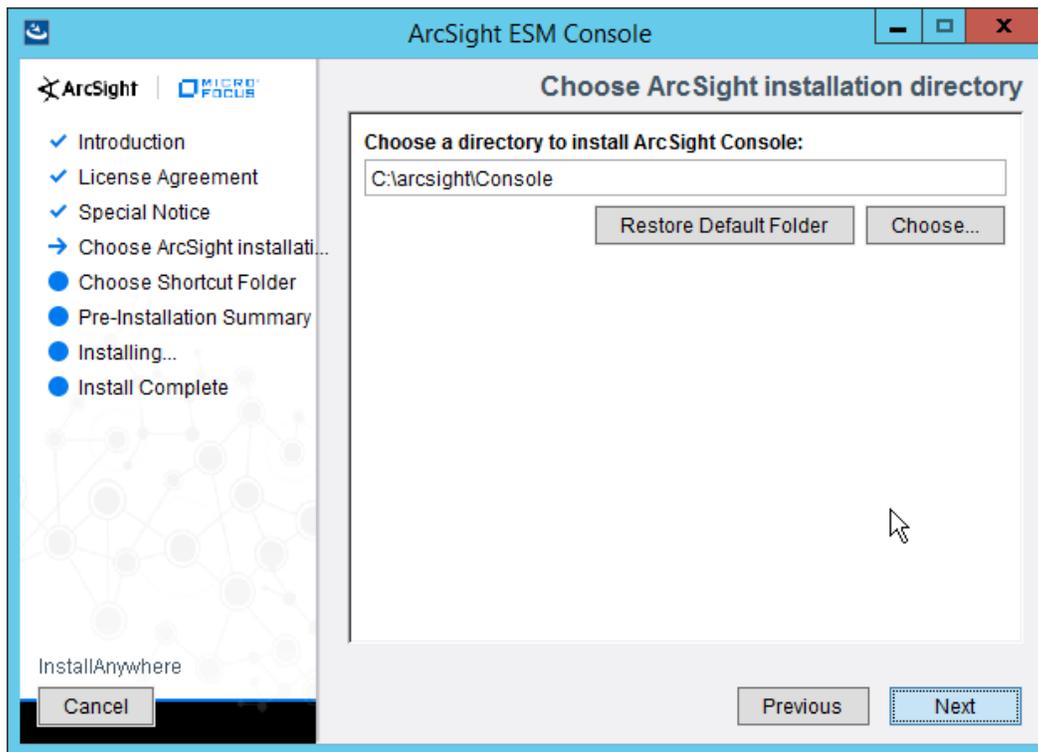
2. Click **Next**.
3. Check the box next to **I accept the License Agreement**.



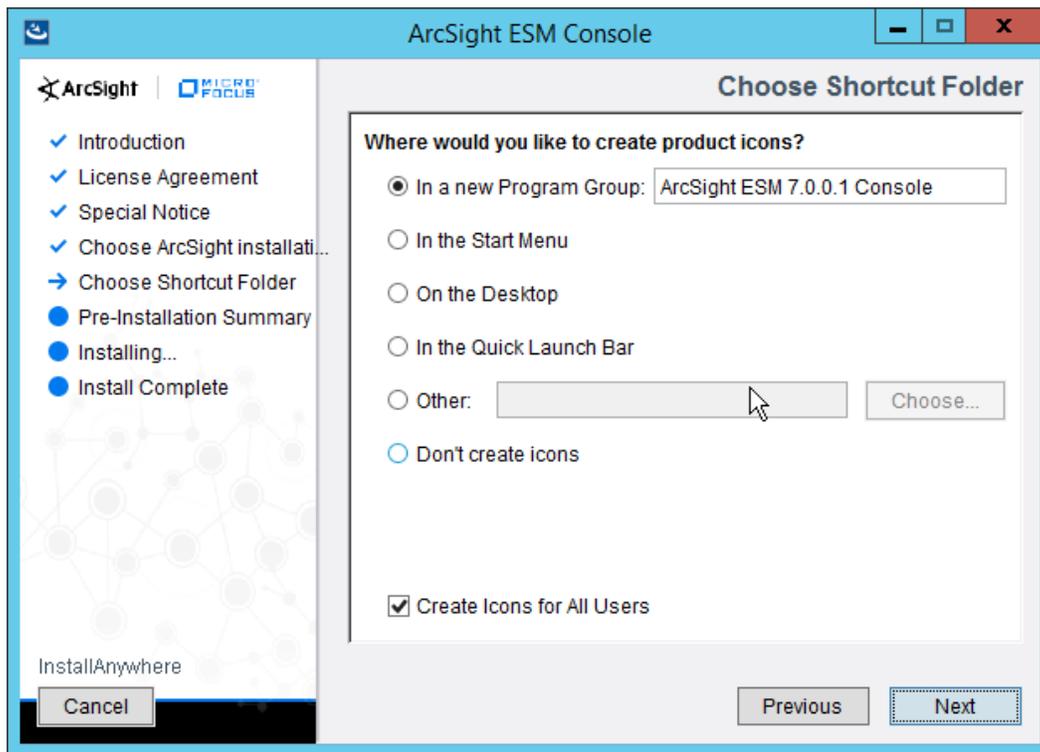
4. Click **Next**.



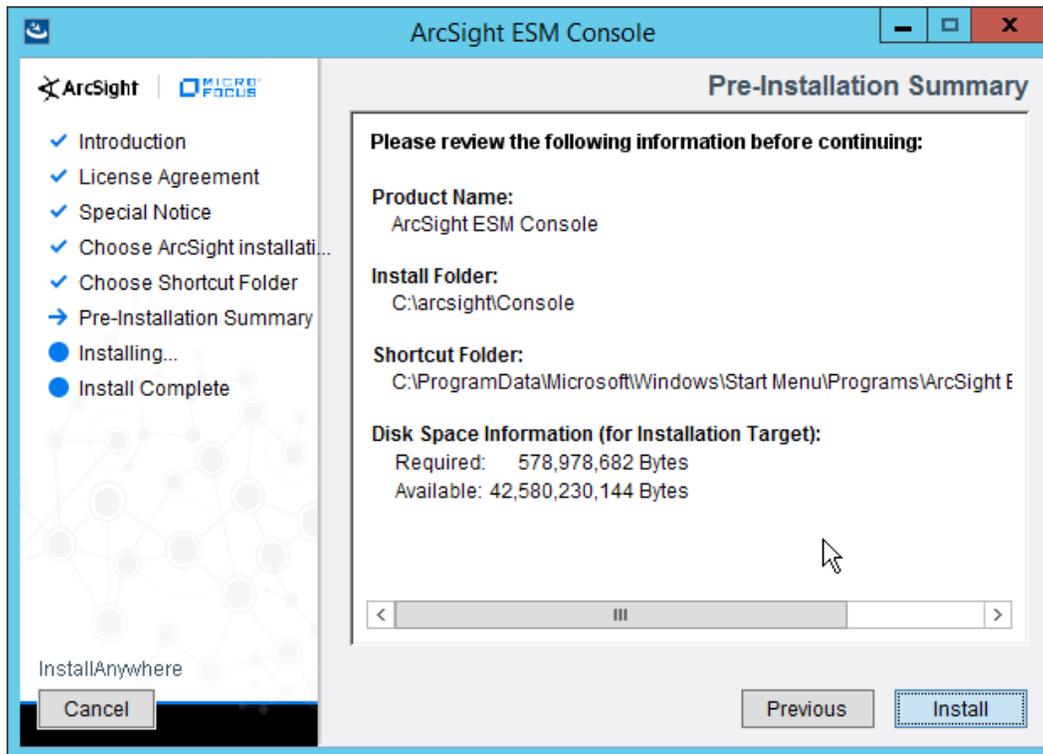
5. Click **Next**.



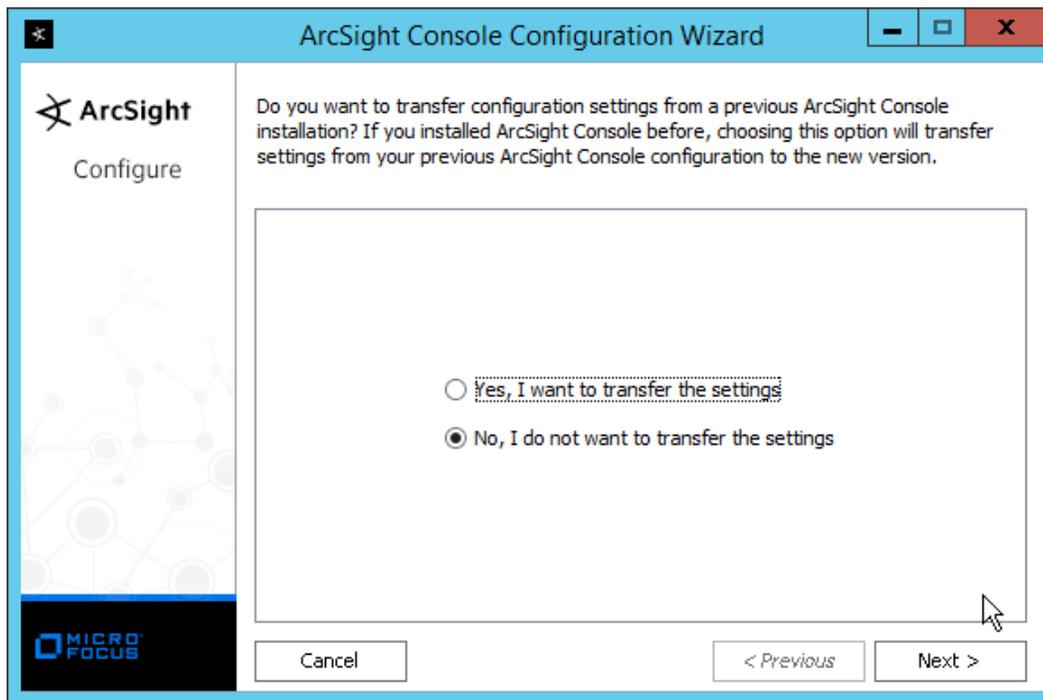
6. Click **Next**.



7. Click **Next**.

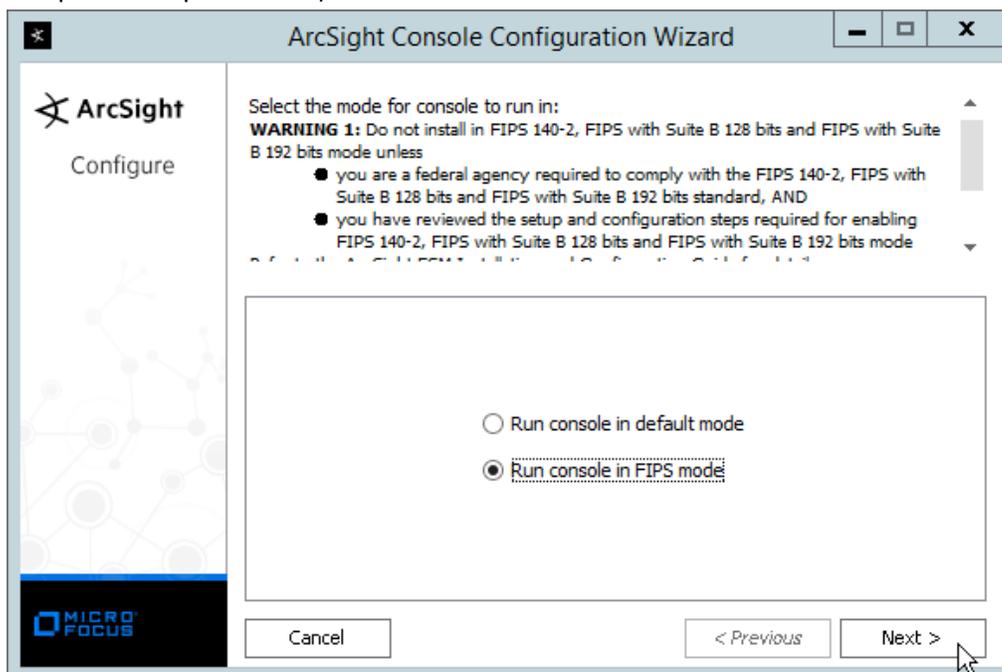


8. Click **Install**.
9. Select **No, I do not want to transfer the settings**.

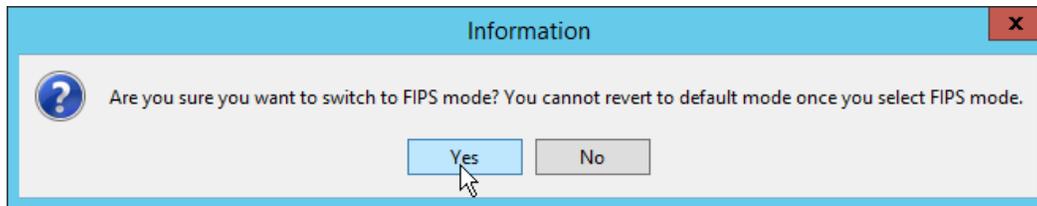


10. Click **Next**.

11. Select **Run console in default mode**. (This can be changed later according to your organization's compliance requirements.)

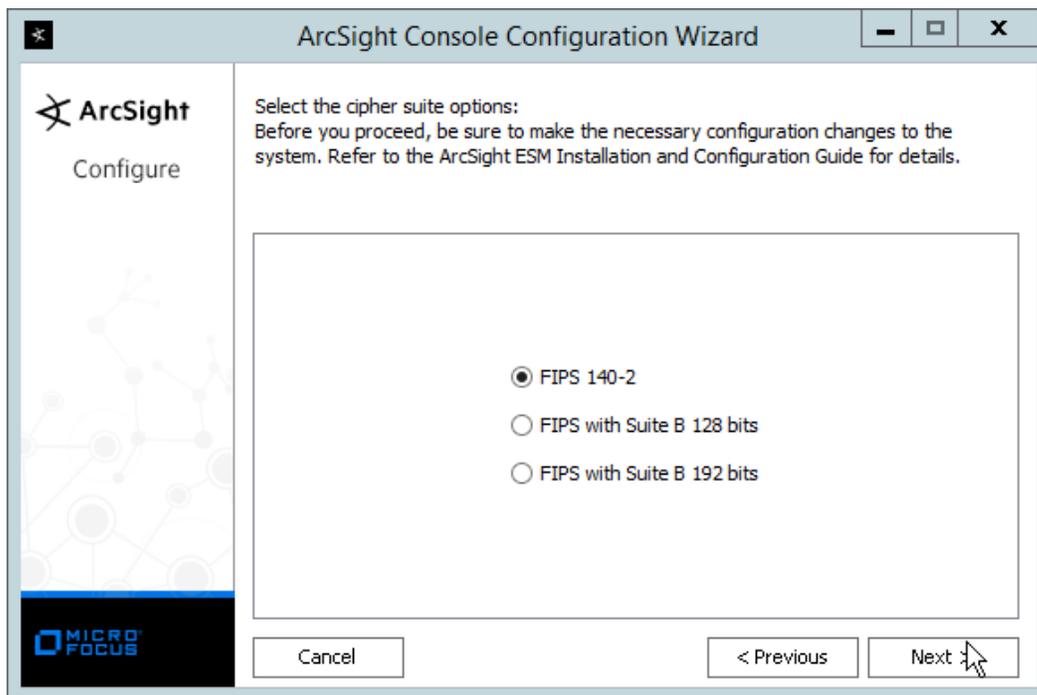


12. Click **Next**.



13. Click **Yes**.

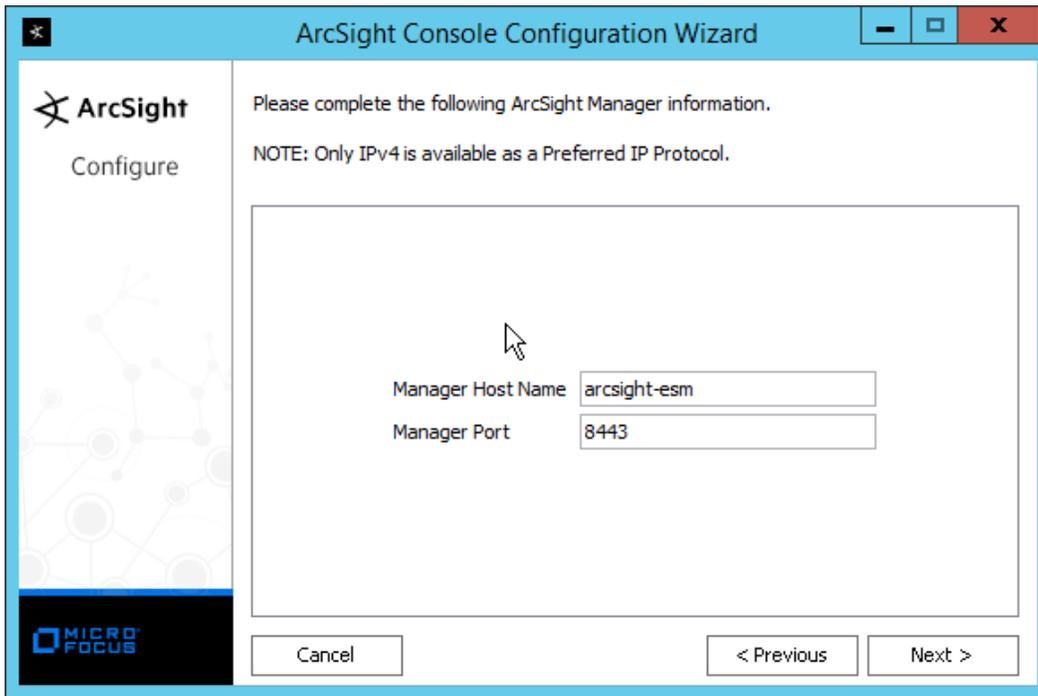
14. Select **FIPS 140-2**.



15. Click **Next**.

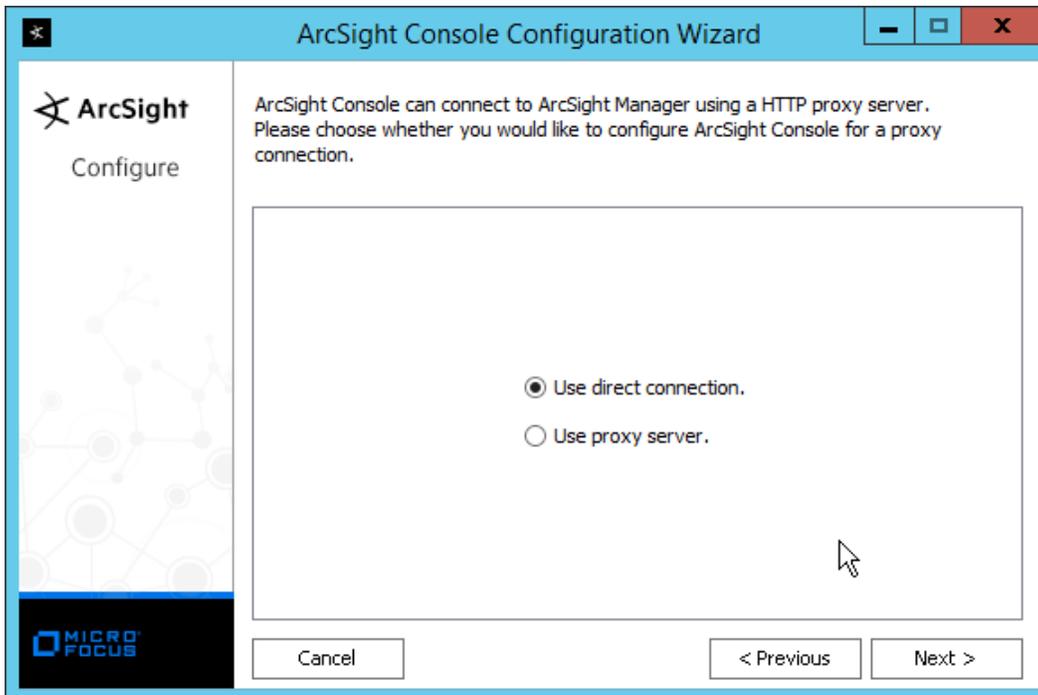
16. Enter the **hostname** of the ESM server for **Manager Host Name**.

17. Enter the **port** that ESM is running on for **Manager Port** (default: 8443).

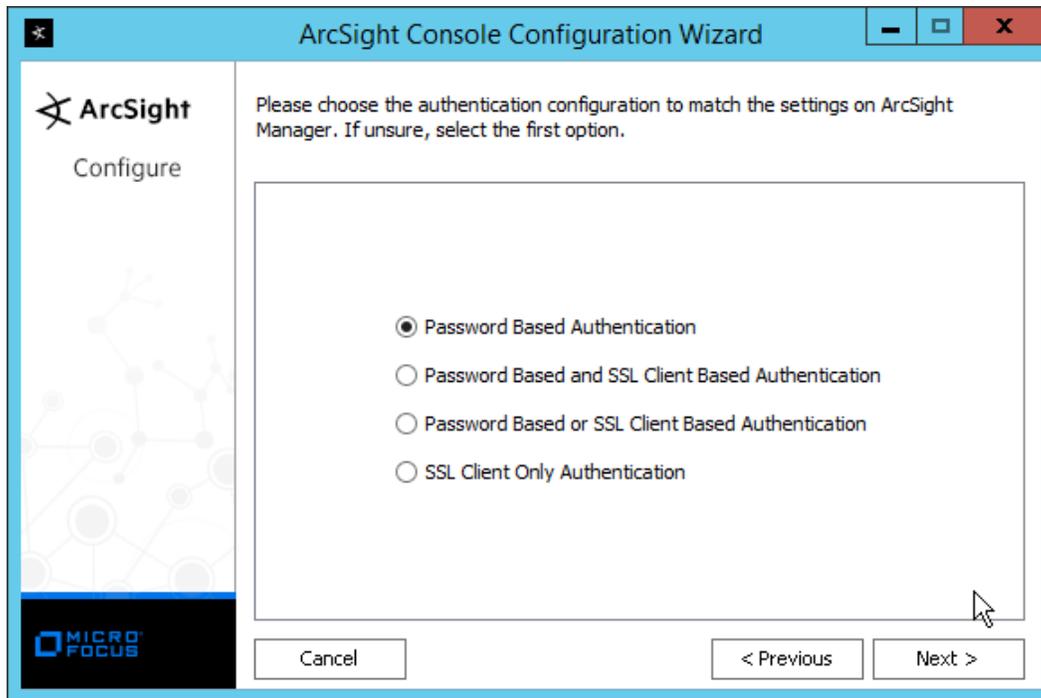


18. Click **Next**.

19. Select **Use direct connection**.

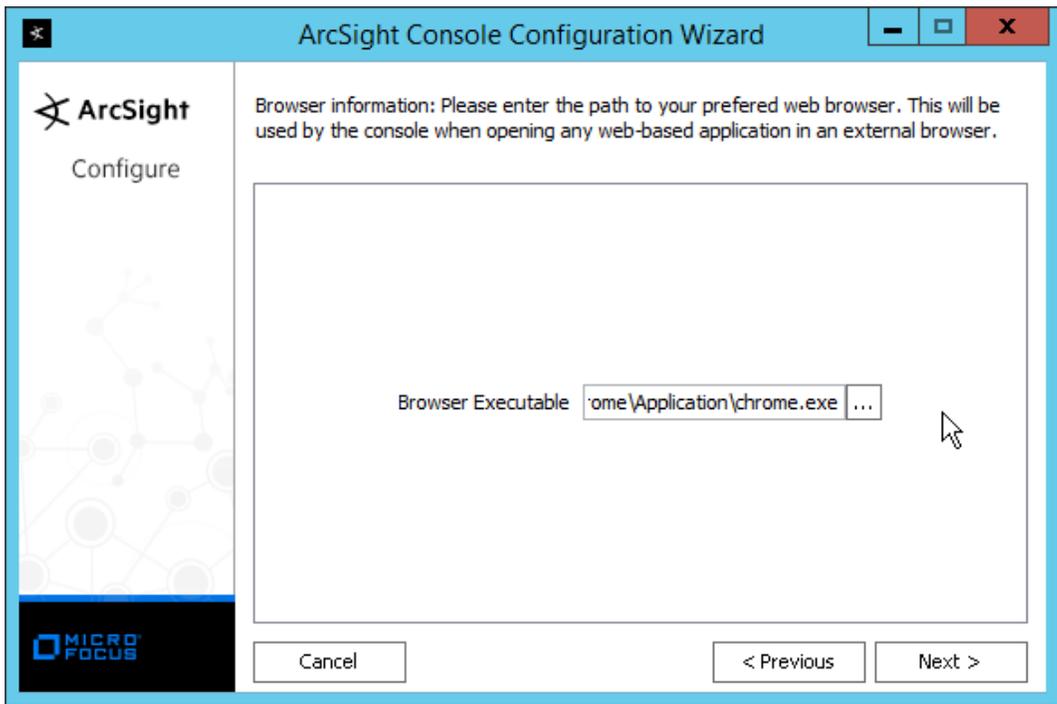


20. Click **Next**.

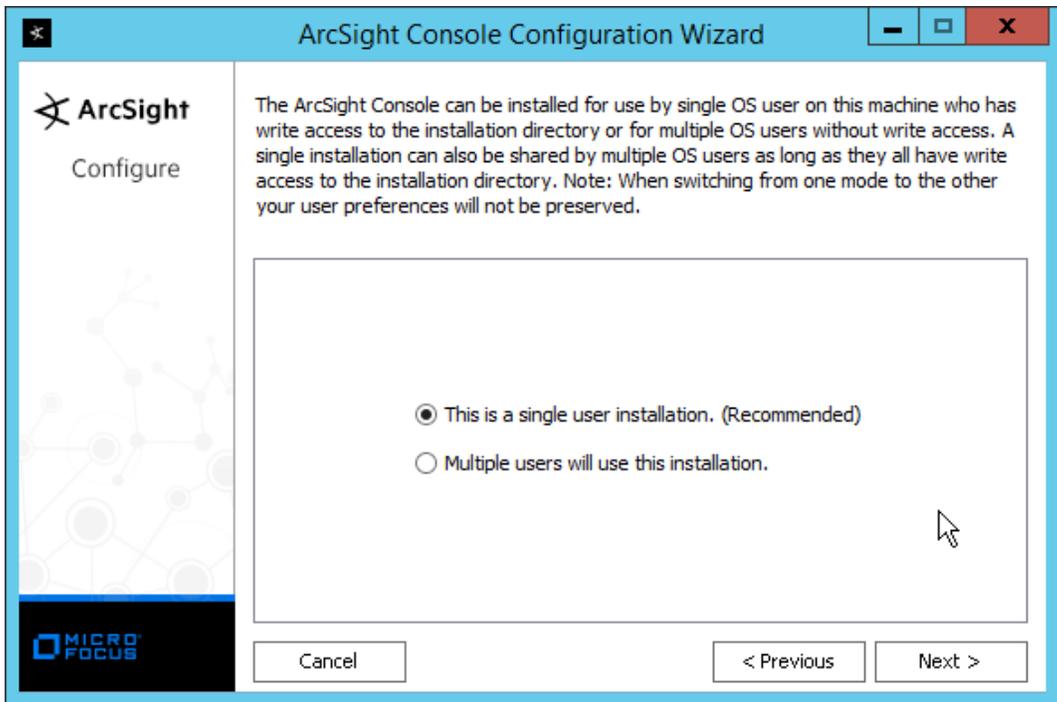


21. Click **Next**.

22. Select your preferred browser.

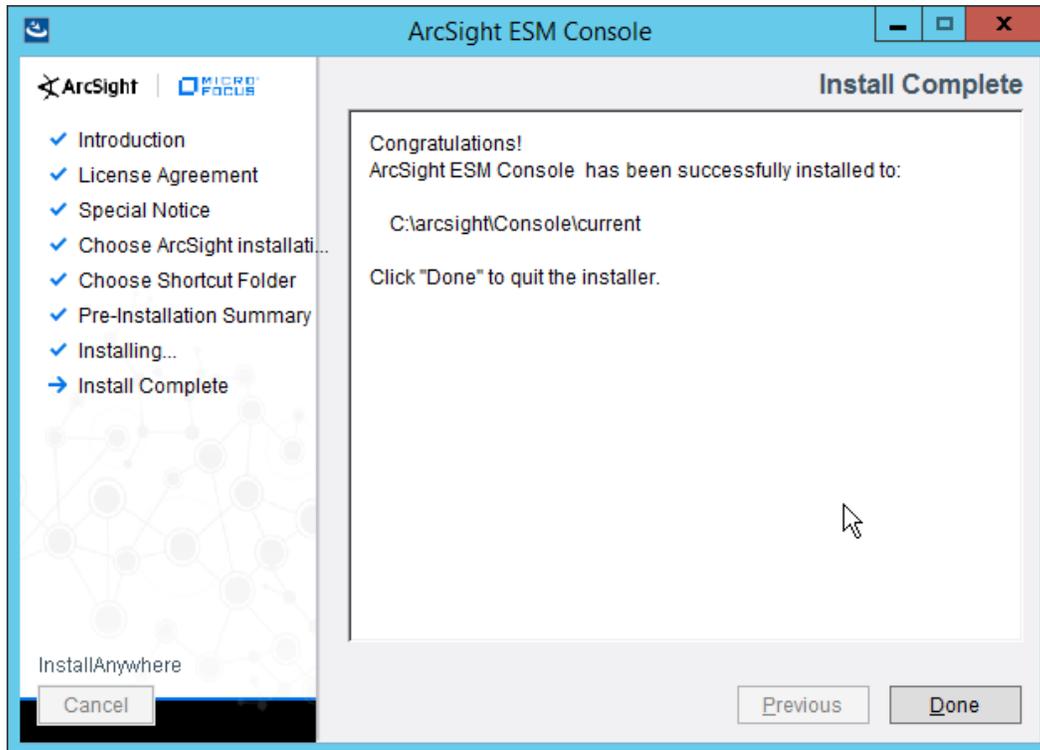


23. Click **Next**.



24. Click **Next**.

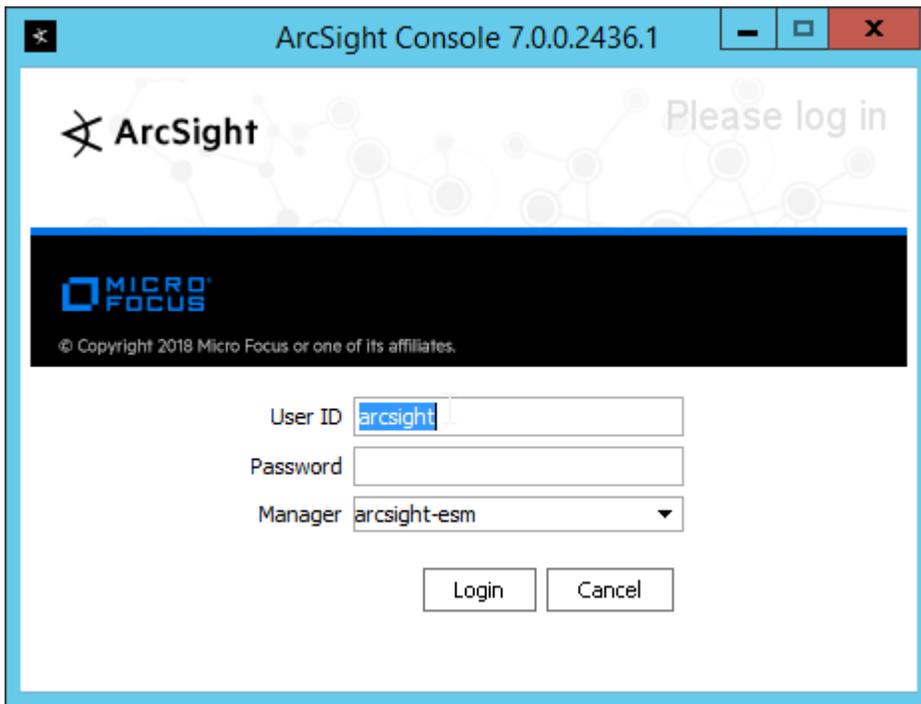
25. Click **Finish**.



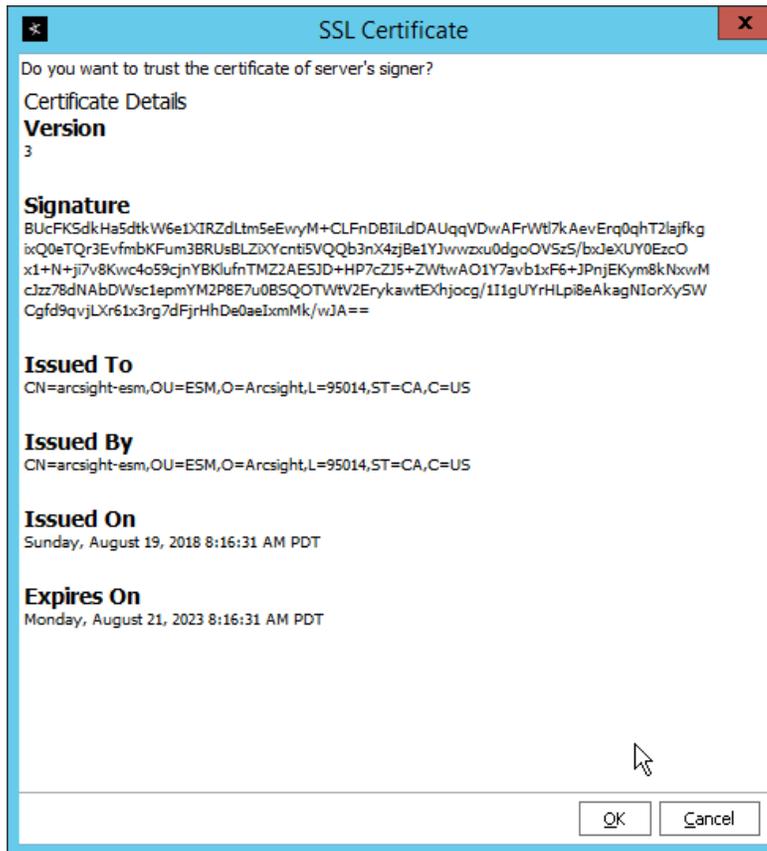
26. Click **Done**.

27. Run **ArcSight Console** from the Start menu.

28. Enter the **username** and **password**.



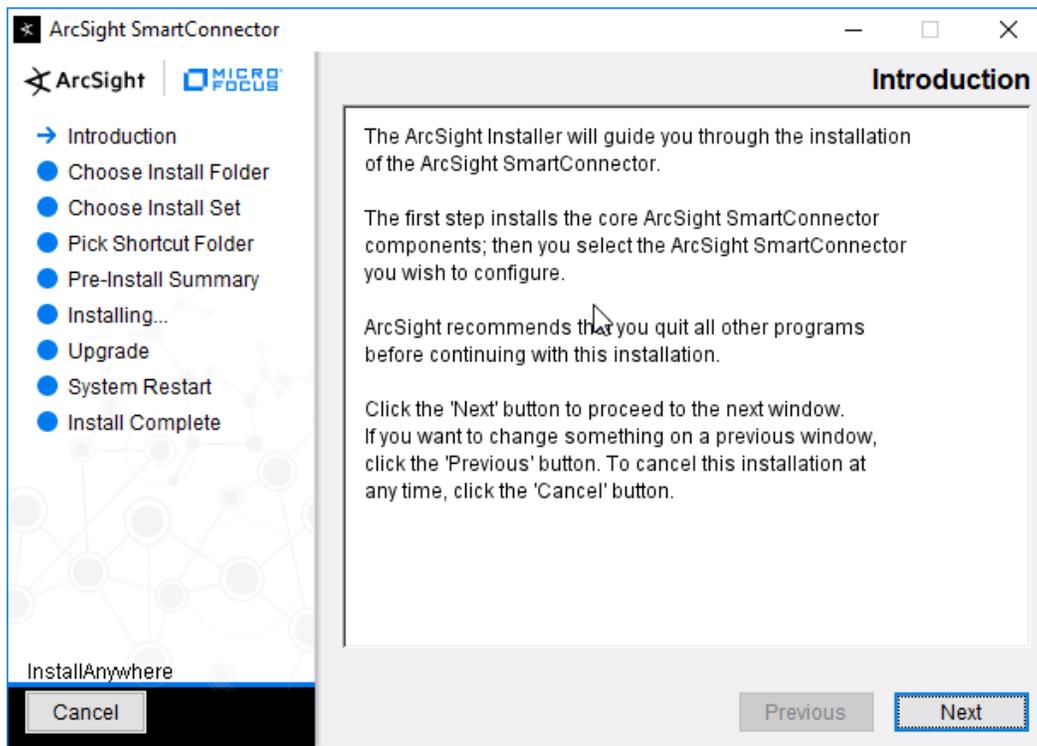
29. Click **Login**. (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)



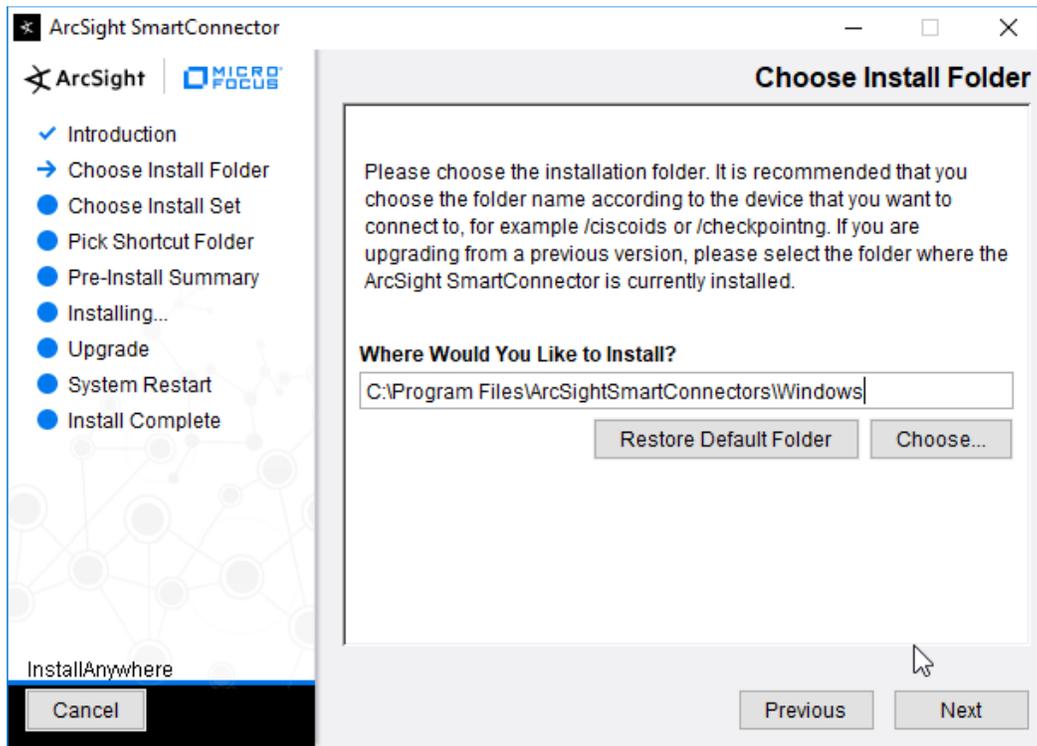
30. Click **OK**.

2.11.2 Install Individual ArcSight Windows Connectors

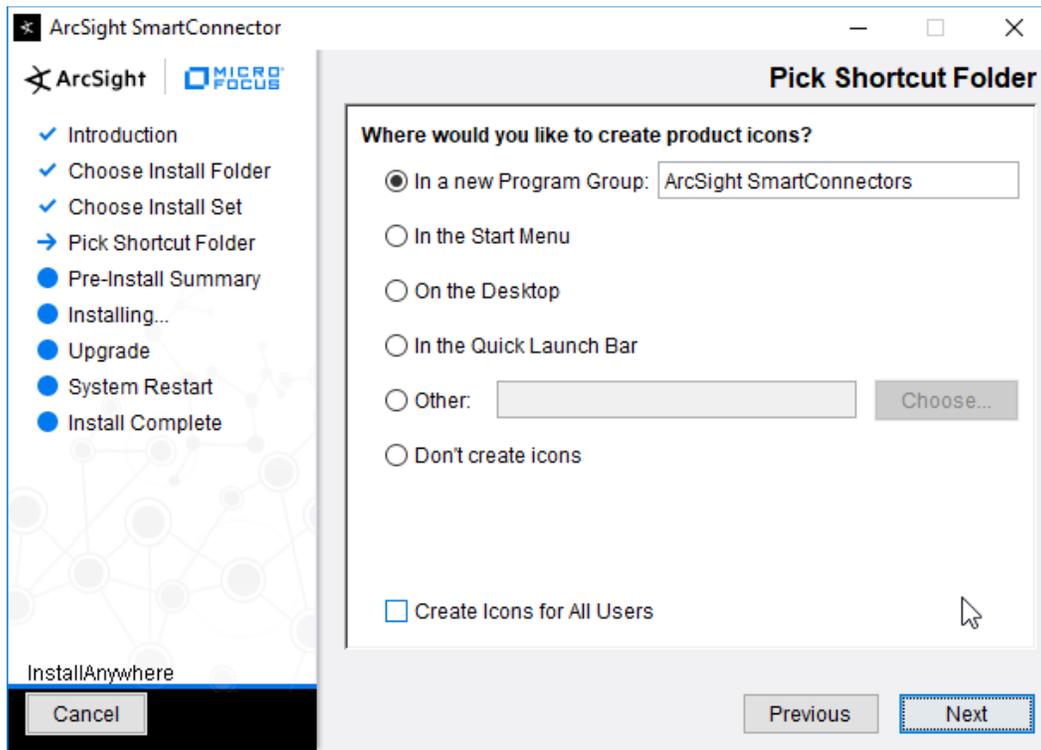
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



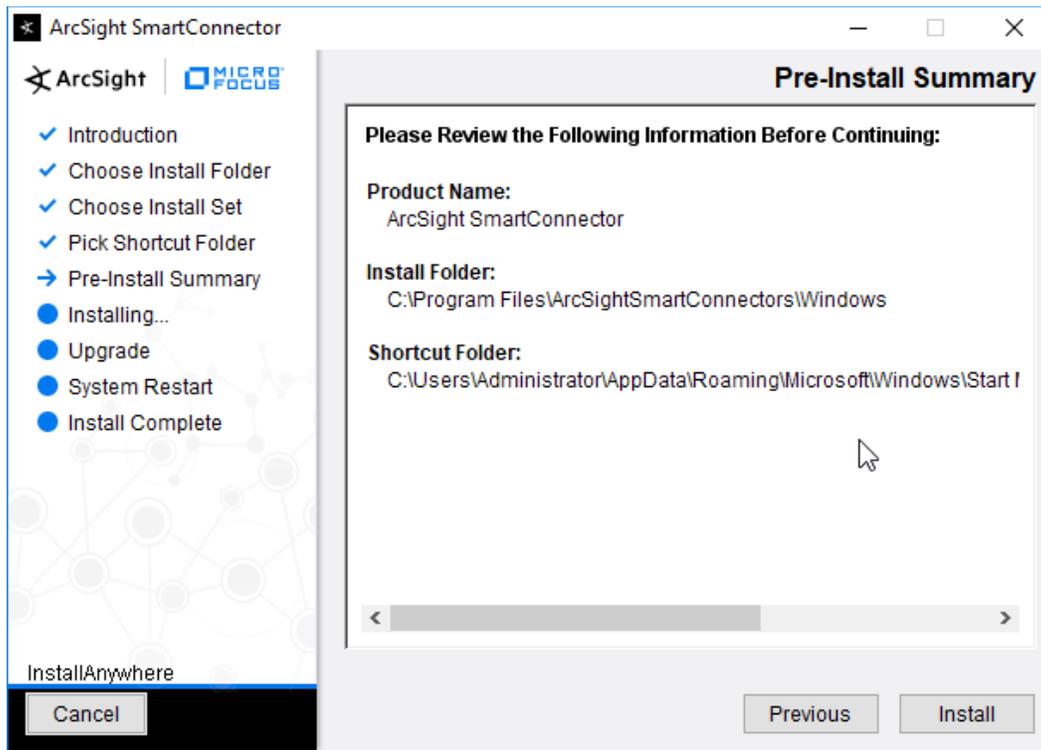
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



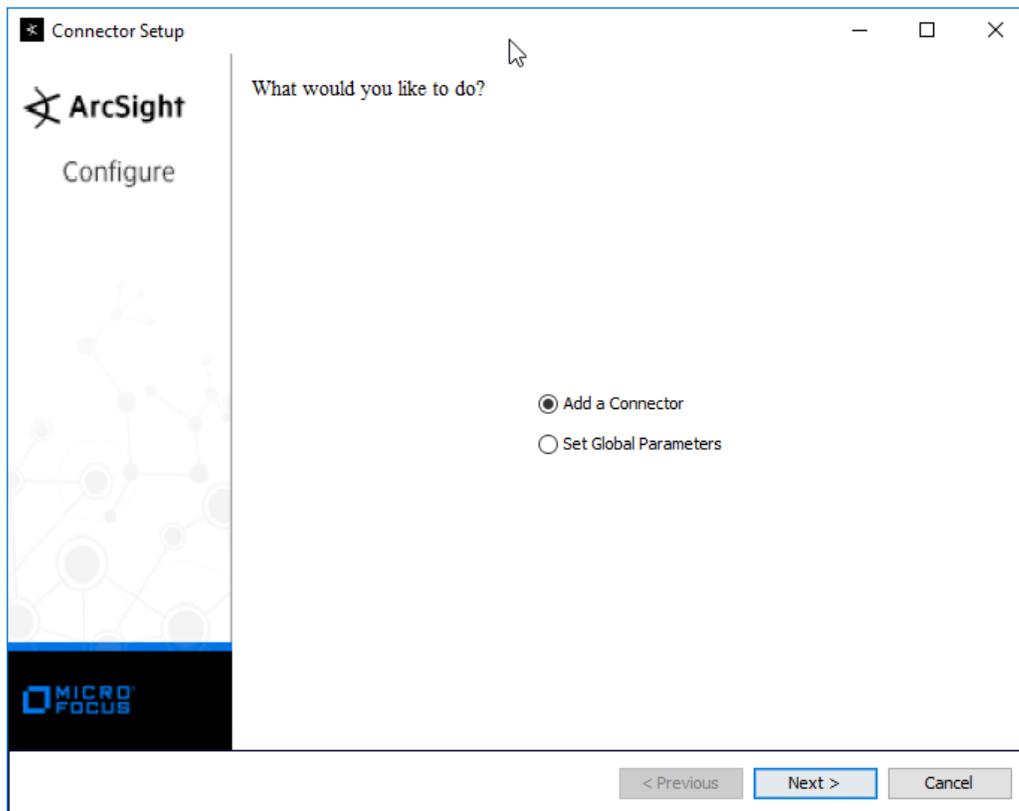
4. Click **Next**.



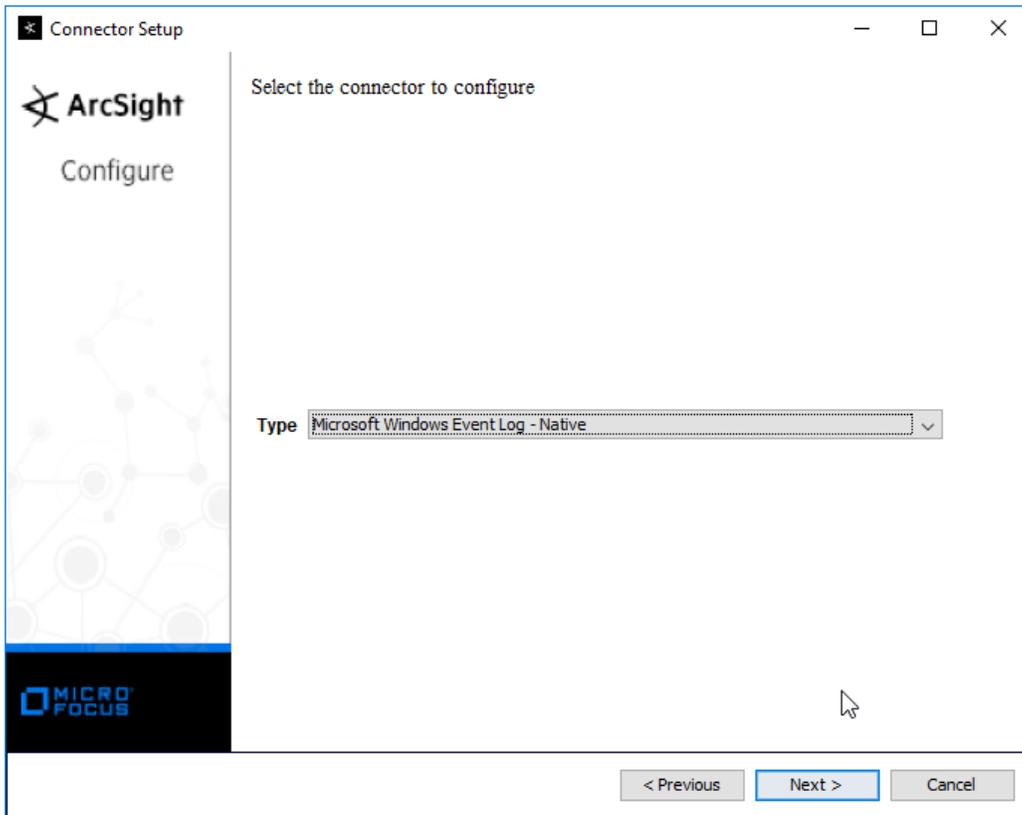
5. Click **Next**.



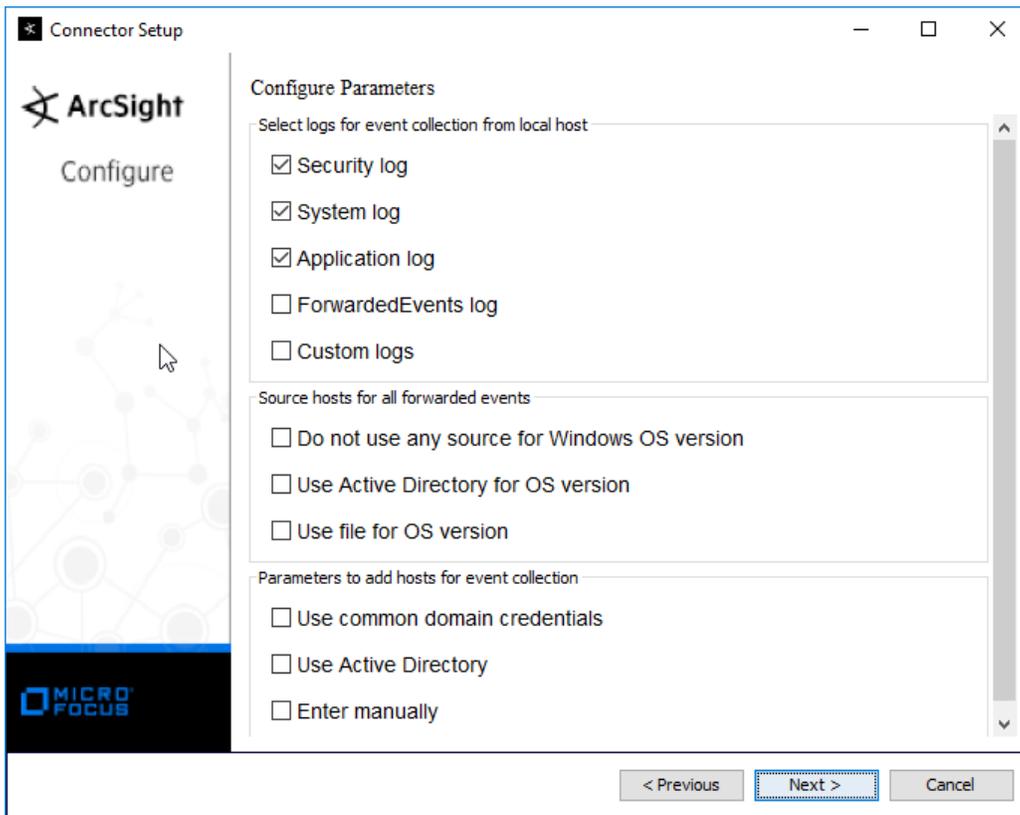
6. Click **Install**.
7. Select **Add a Connector**.



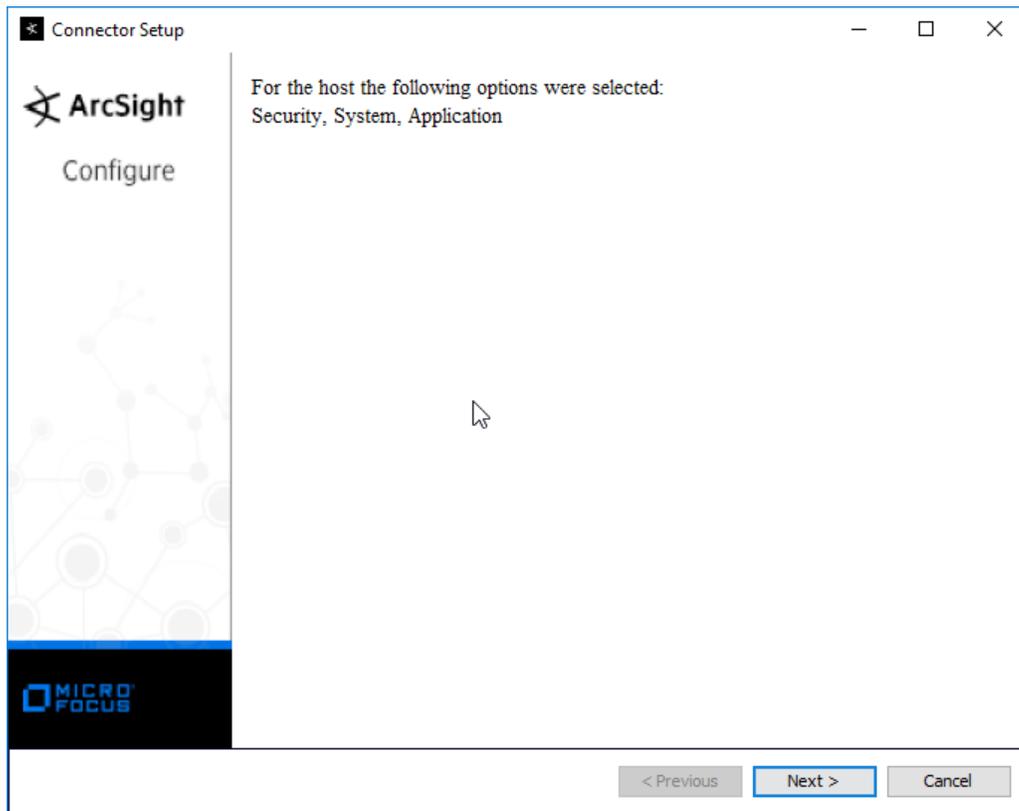
8. Click **Next**.
9. Select **Microsoft Windows Event Log–Native**.



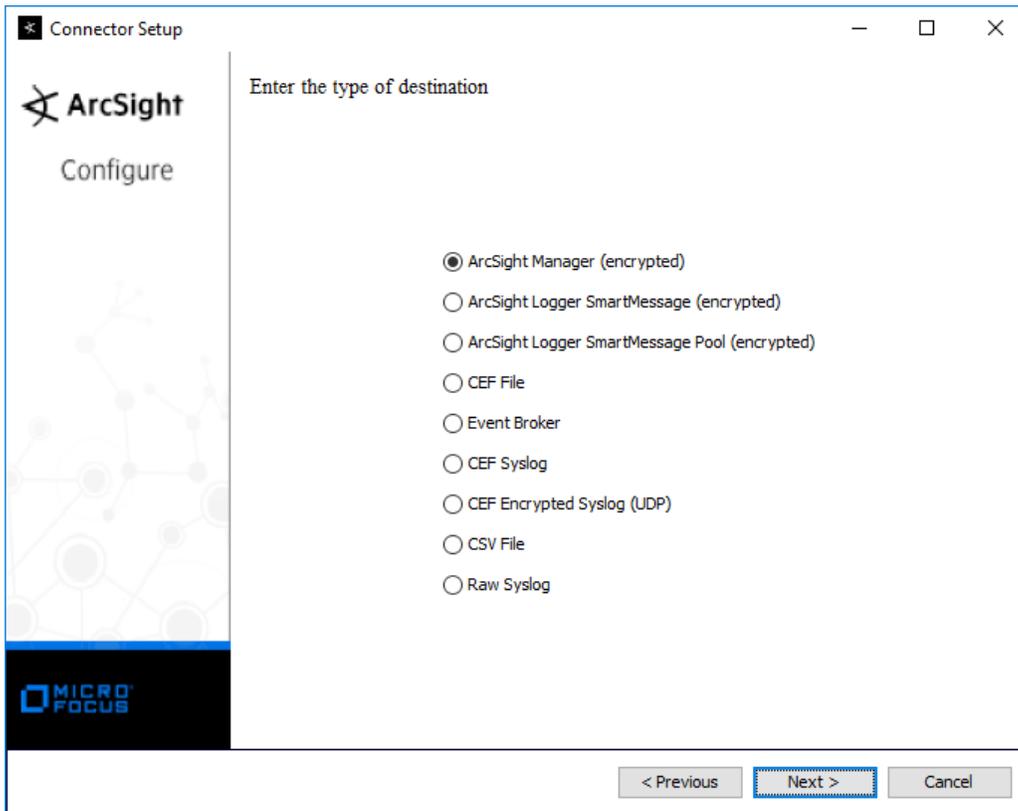
10. Click **Next**.



11. Click **Next**.



12. Click **Next**.
13. Select **ArcSight Manager (encrypted)**.



14. Click **Next**.

15. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.

Connector Setup

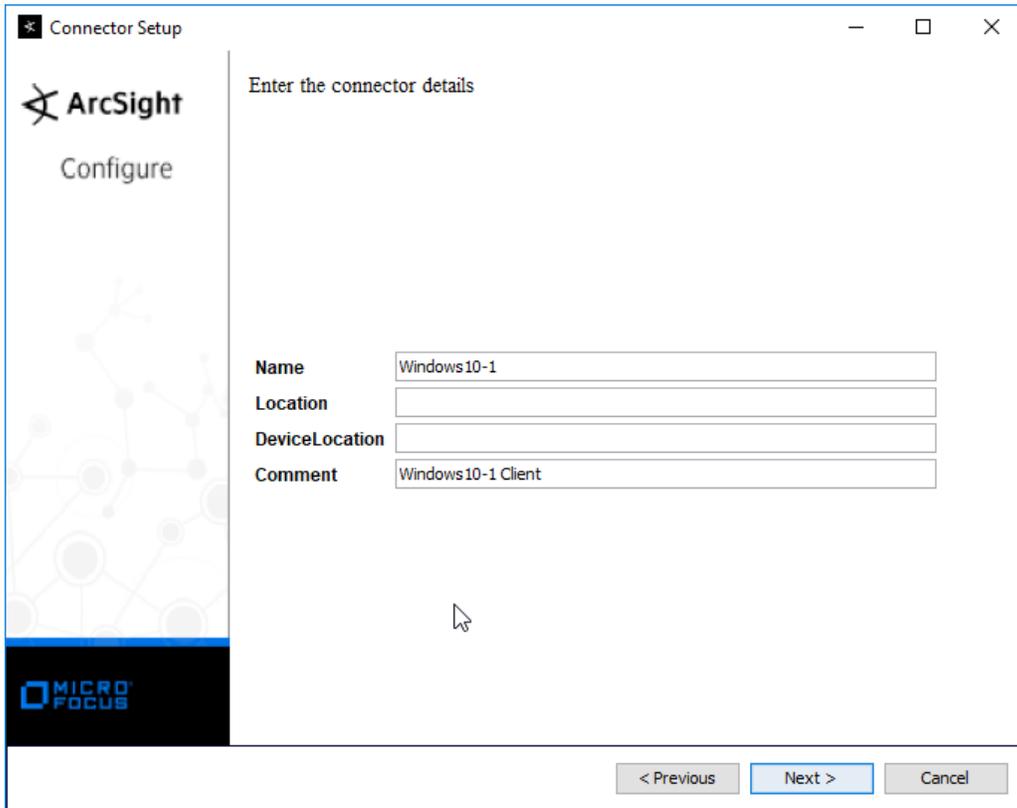
ArcSight
Configure

Enter the destination parameters

Manager Hostname	arcsight-esm
Manager Port	8443
User	administrator
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

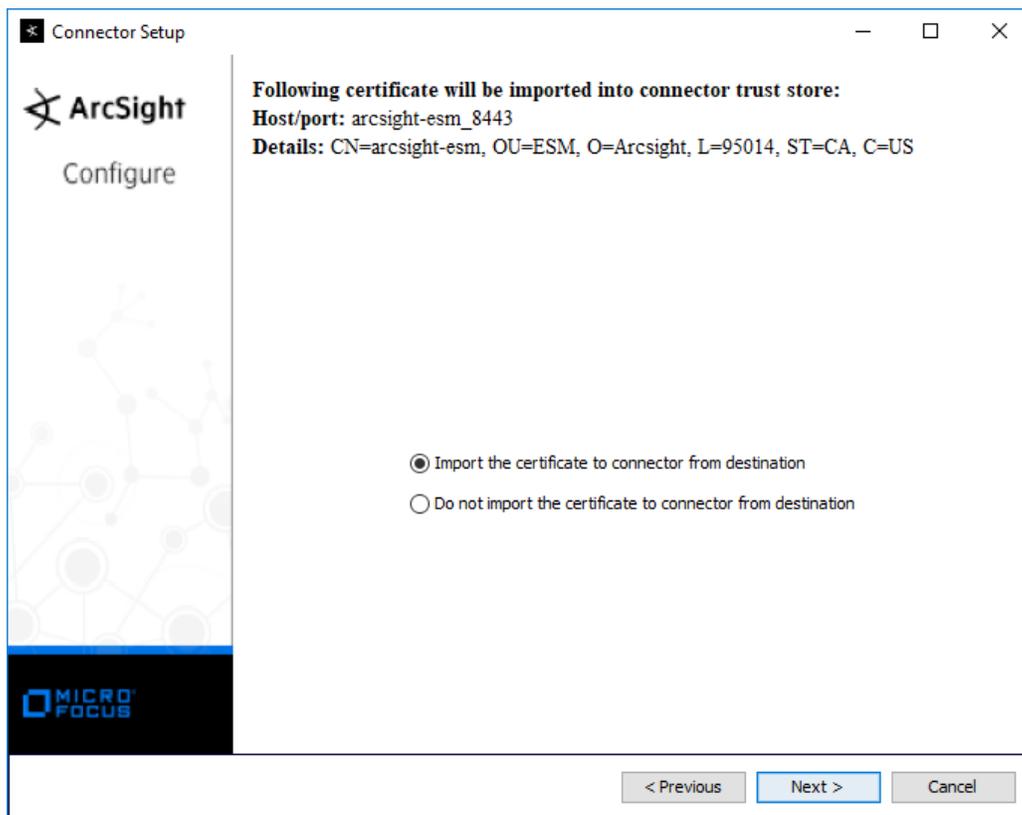
< Previous Next > Cancel

16. Click **Next**.
17. Enter identifying details about the system (only **Name** is required).

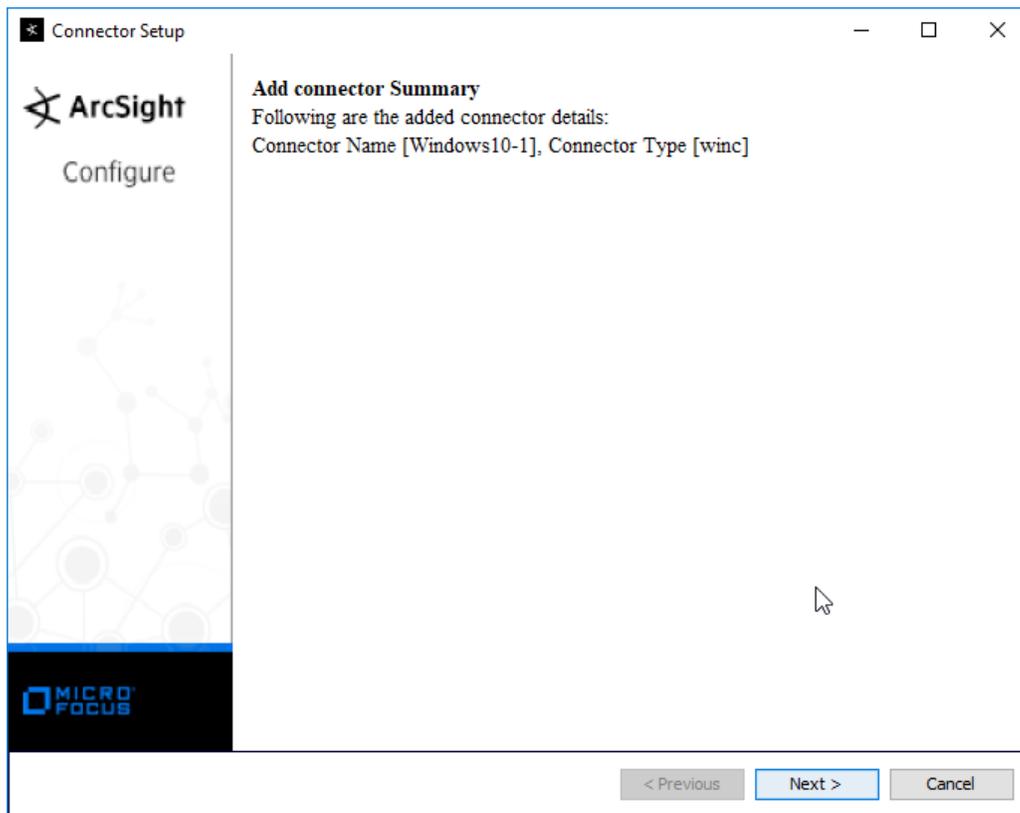


18. Click **Next**.

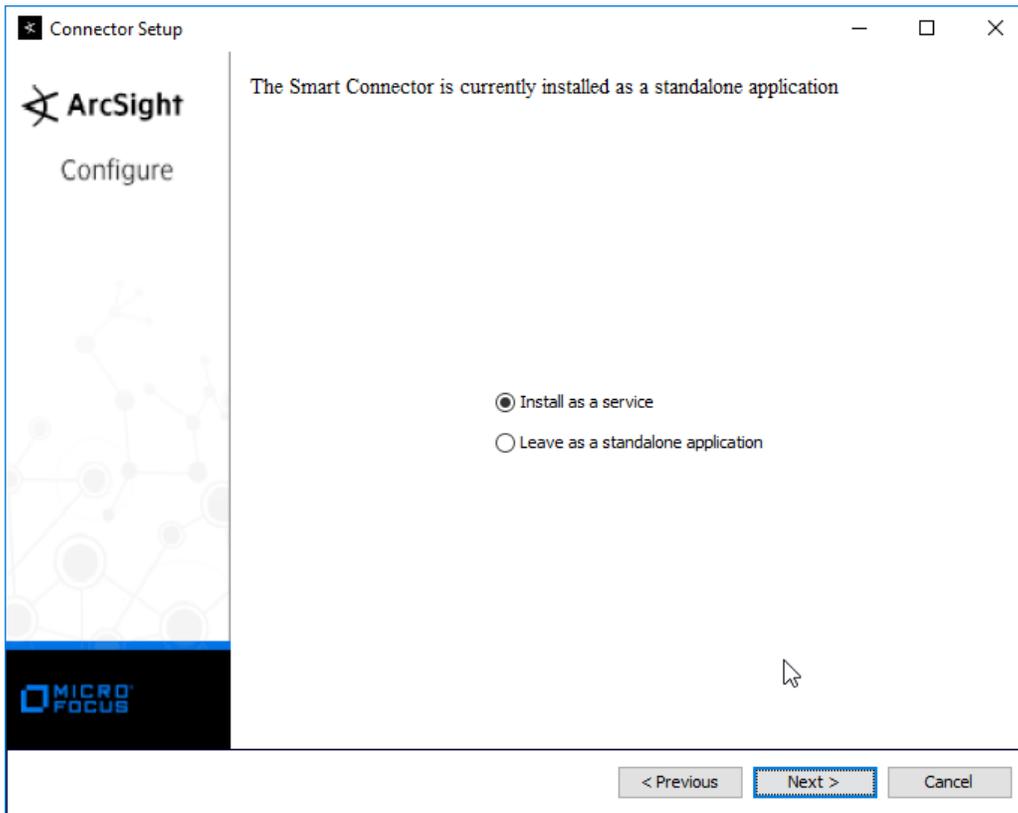
19. Select **Import the certificate to connector from destination**.



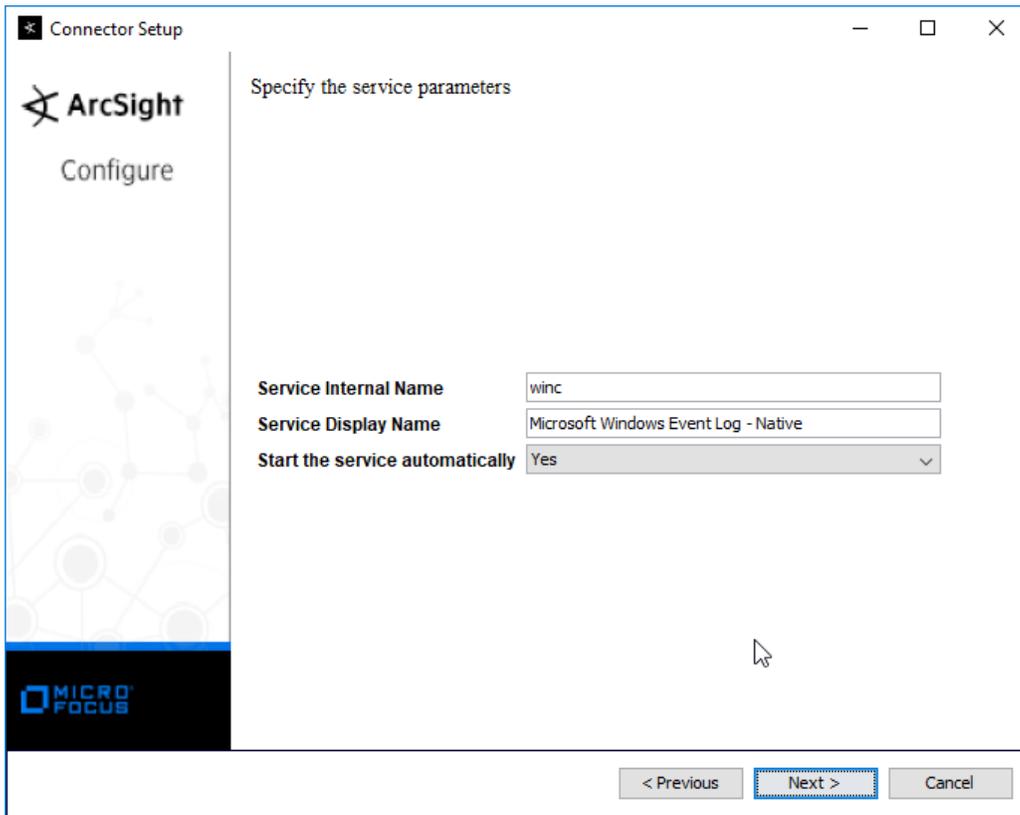
20. Click **Next**.



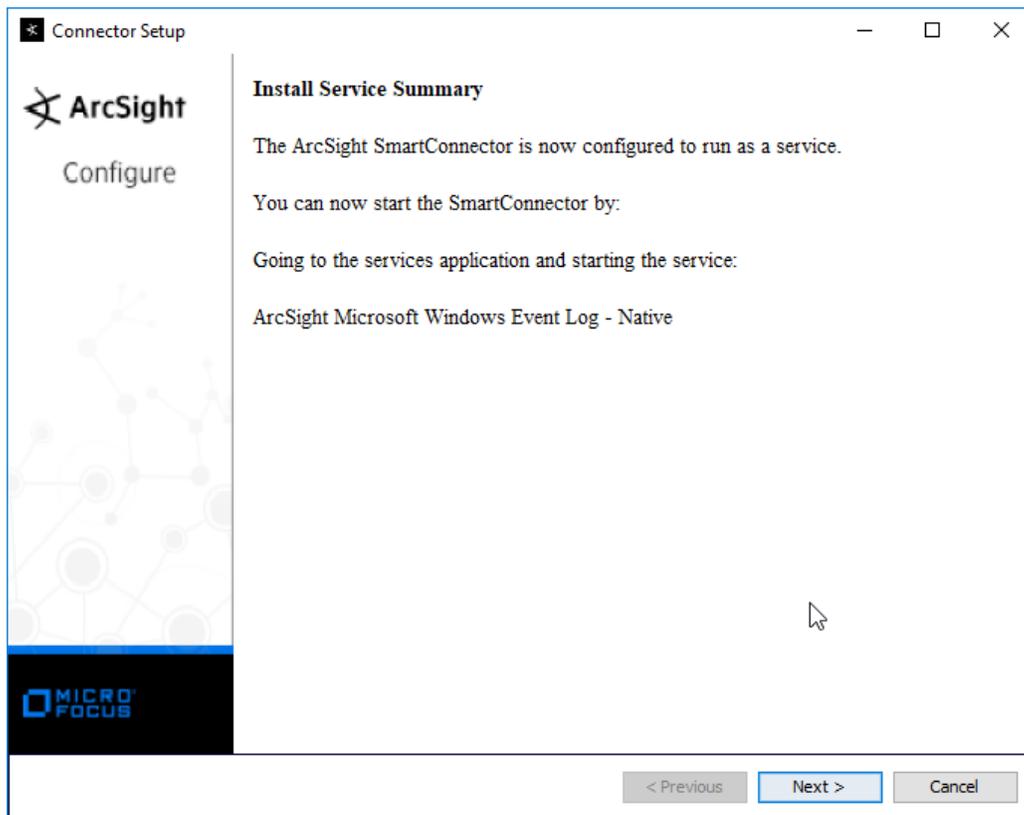
21. Click **Next**.
22. Select **Install as a service**.



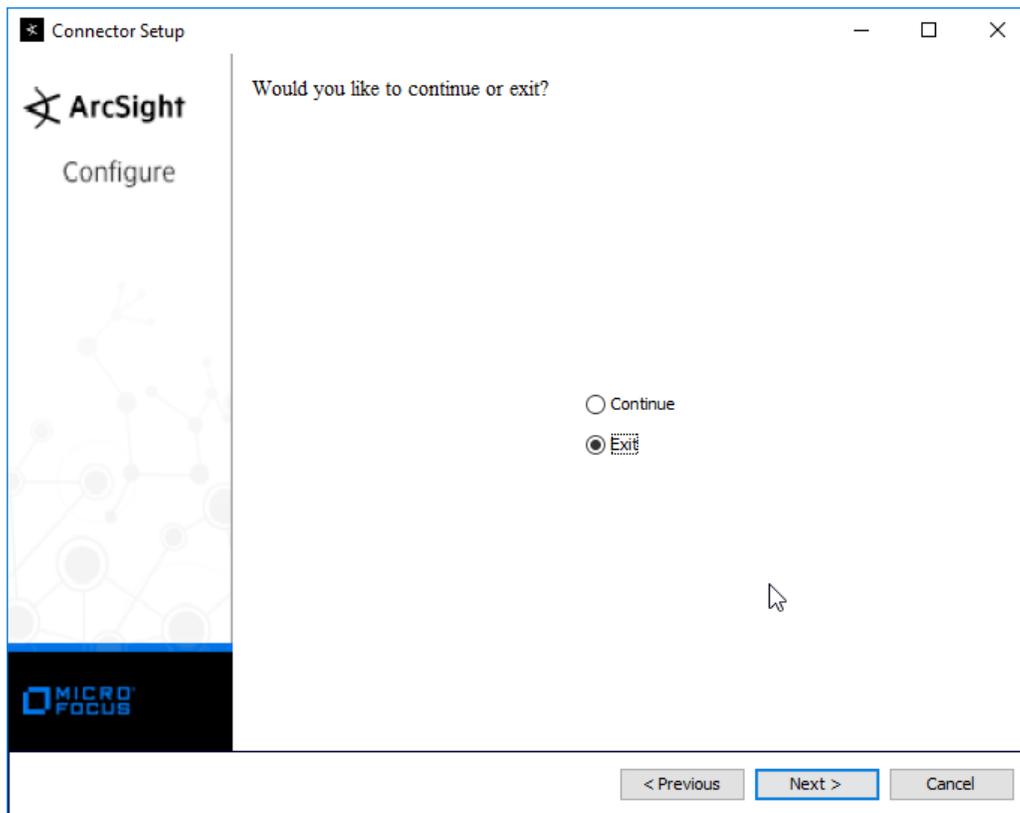
23. Click **Next**.



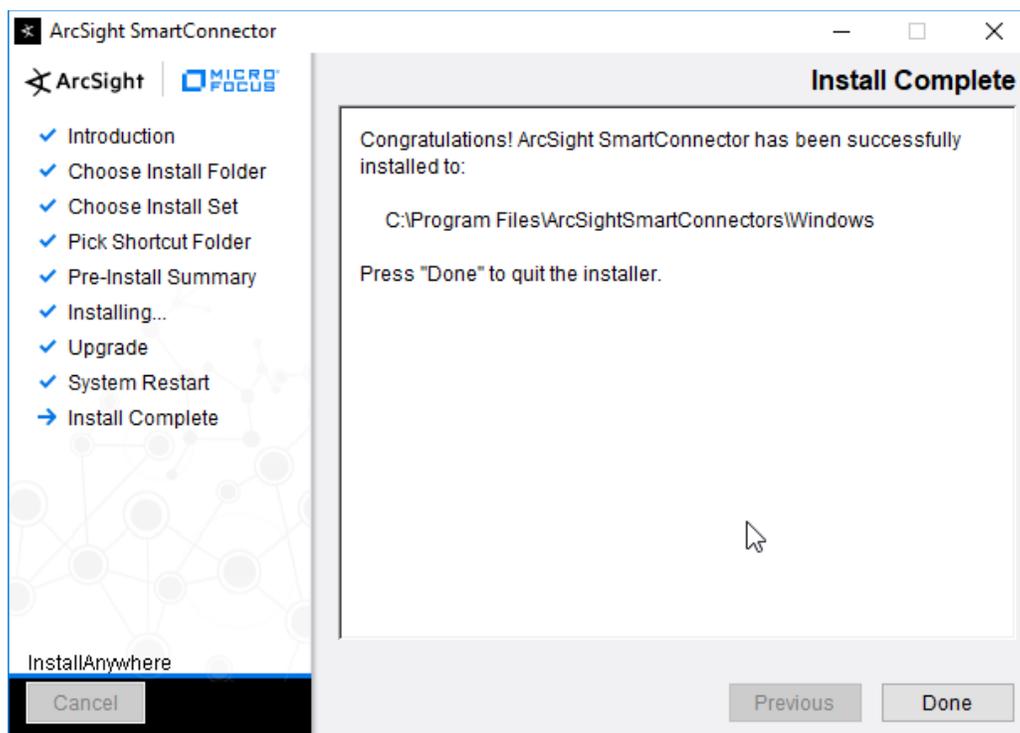
24. Click **Next**.



25. Click **Next**.
26. Select **Exit**.



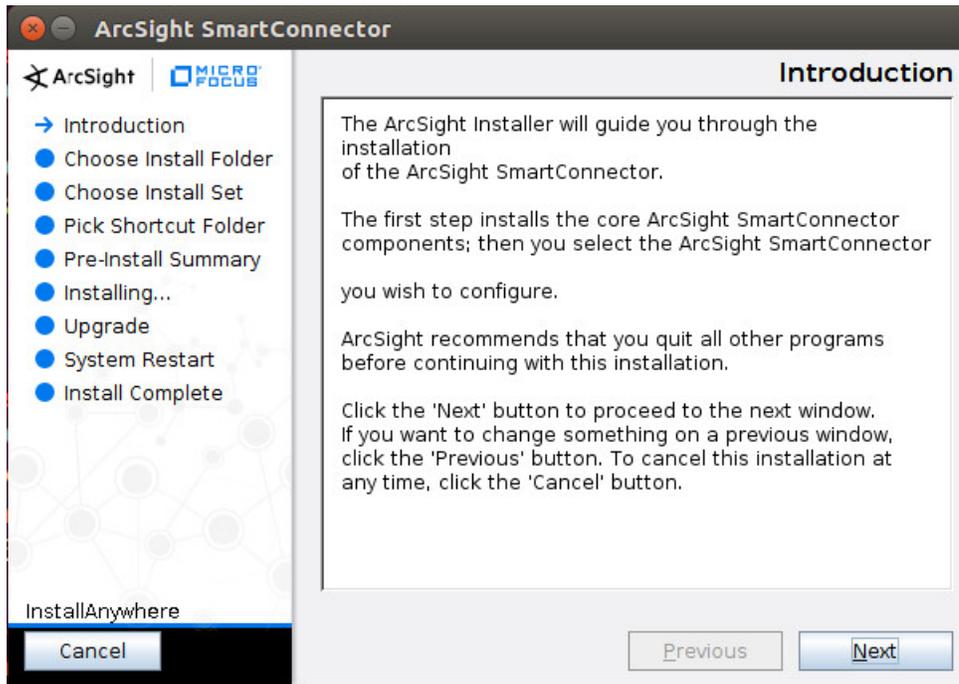
27. Click **Next**.



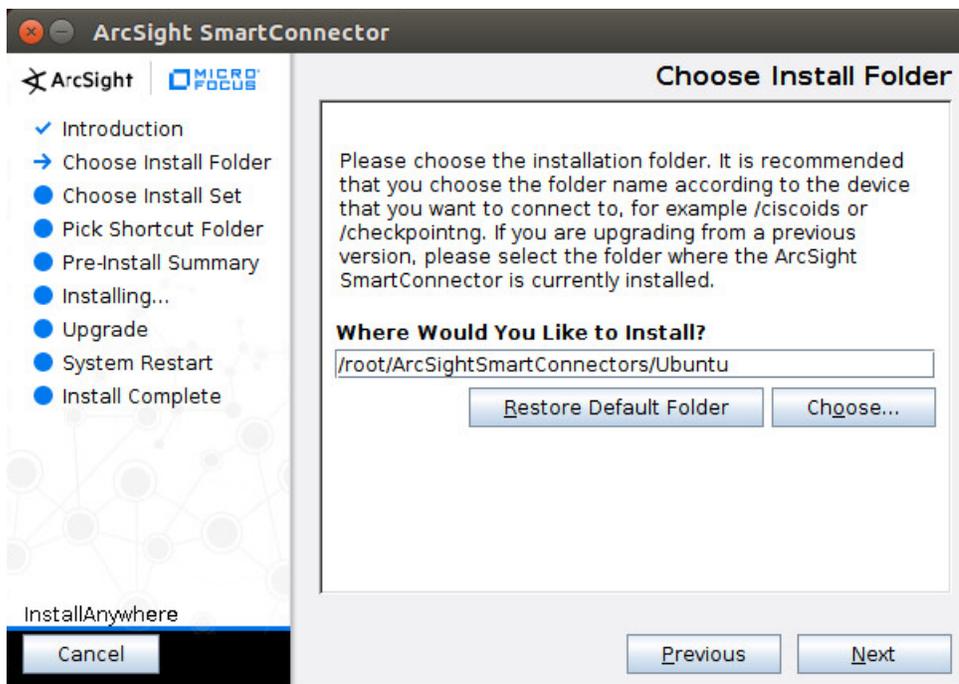
28. Click **Done**.

2.11.3 Install Individual ArcSight Ubuntu Connectors

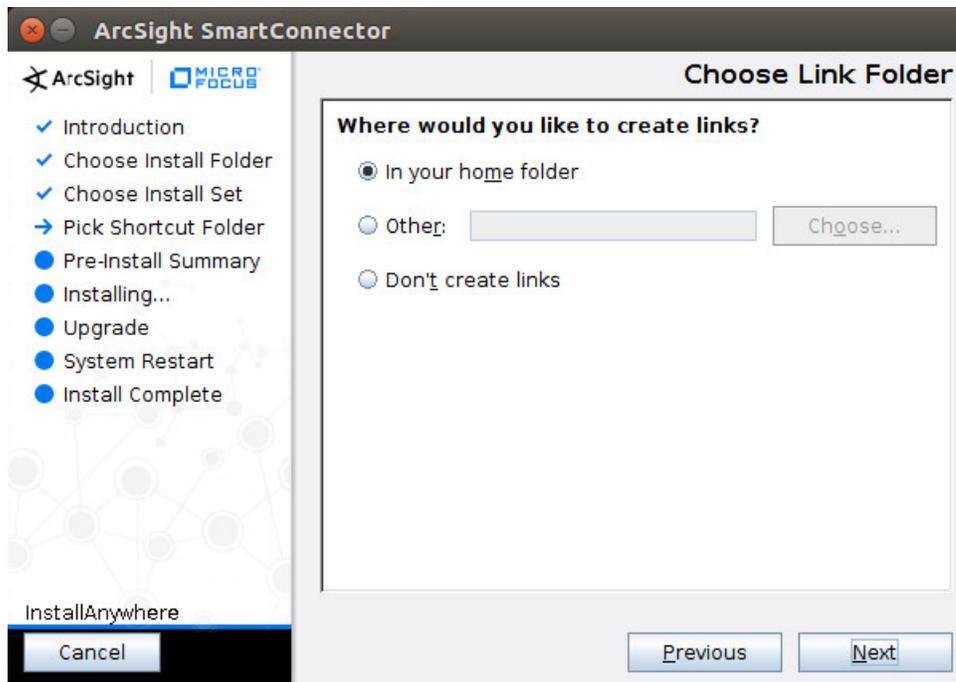
1. From the command line, run:
> sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin
2. Enter the password if prompted.



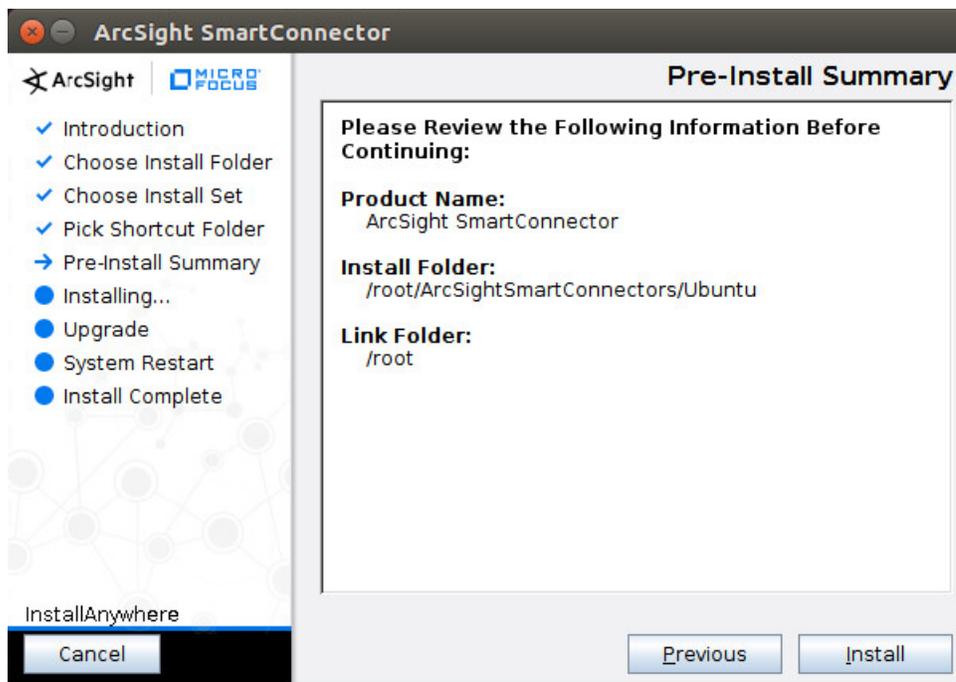
3. Click **Next**.
4. Enter `/root/ArcSightSmartConnectors/Ubuntu`.



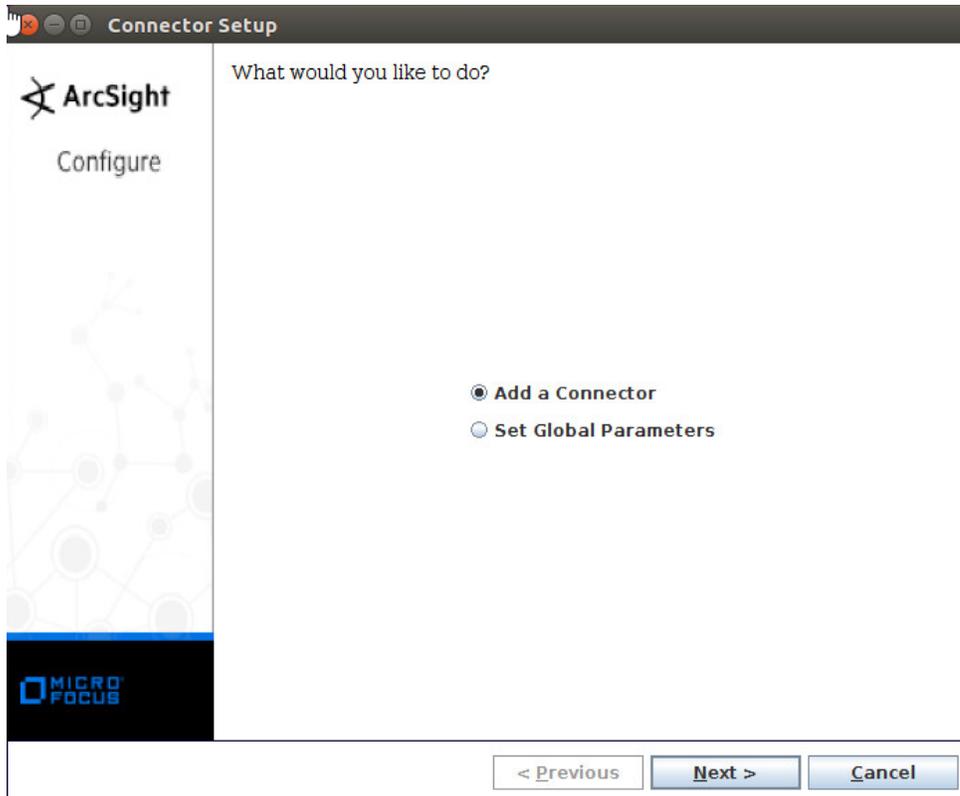
5. Click **Next**.



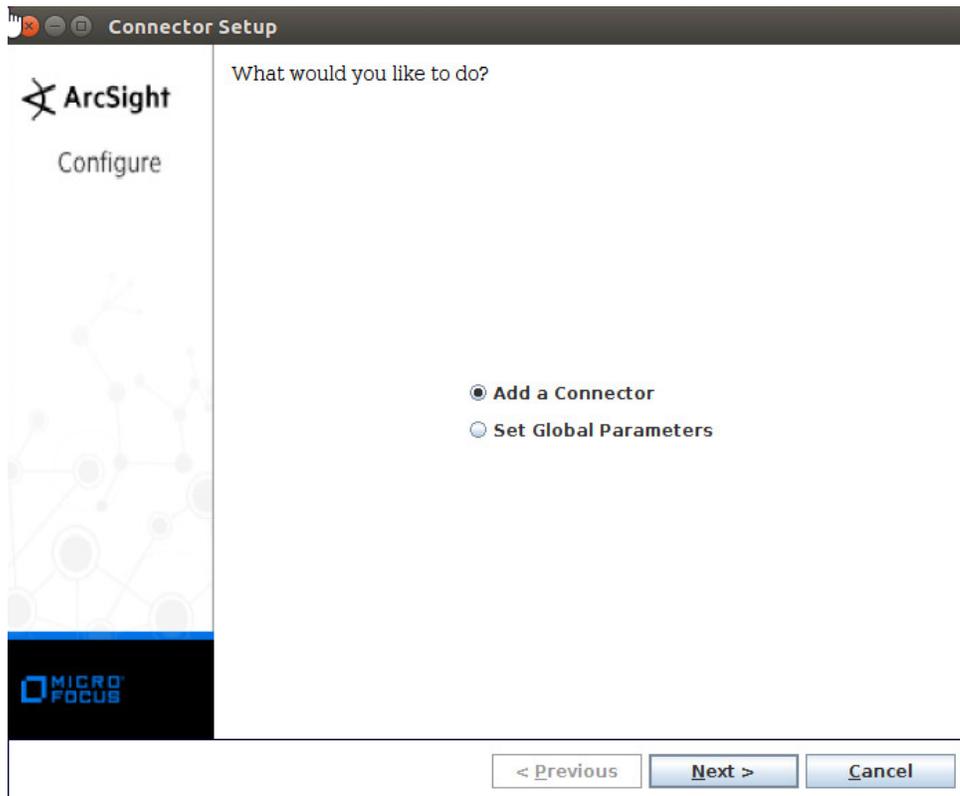
6. Click **Next**.



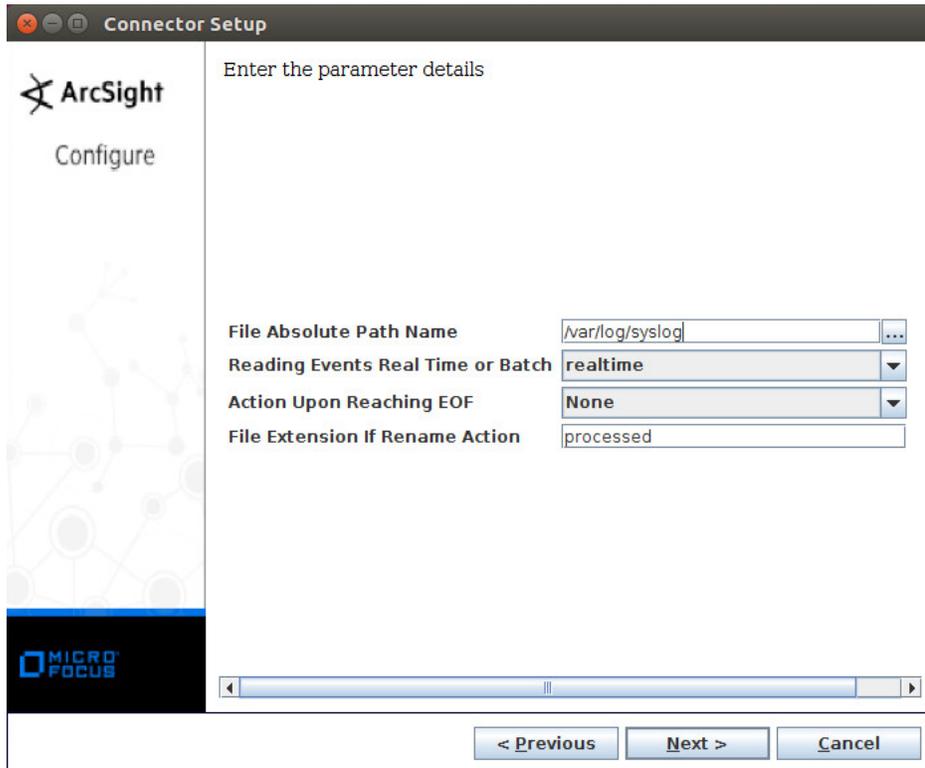
7. Click **Install**.
8. Select **Add a Connector**.



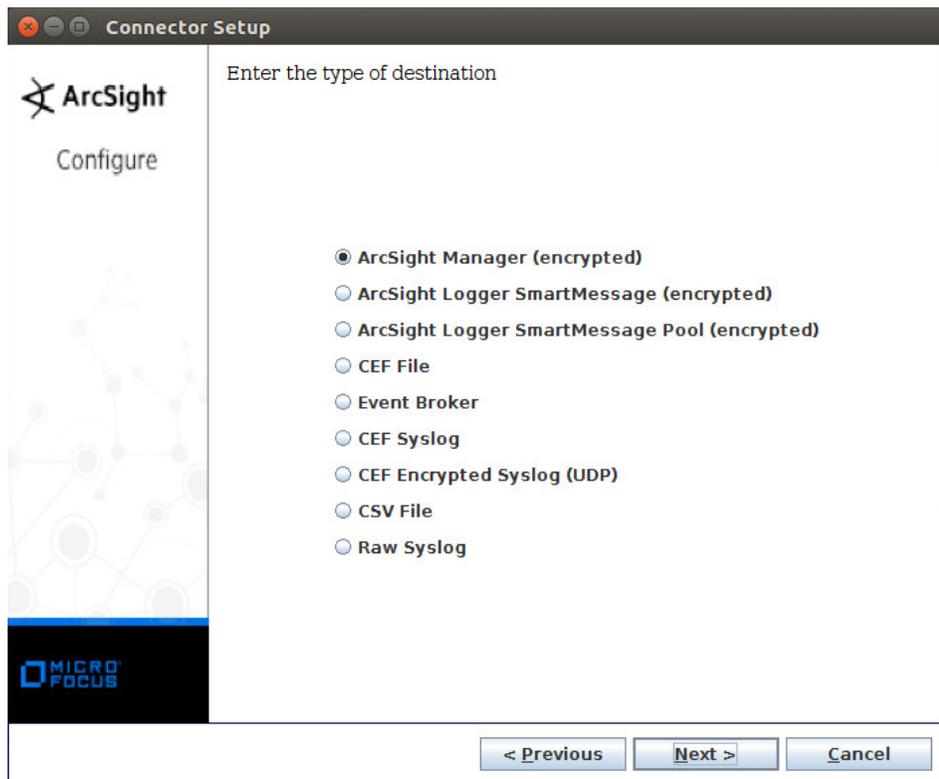
9. Click **Next**.
10. Select **Syslog File**.



11. Click **Next**.
12. Enter `/var/log/syslog` for the File Absolute Path Name.



13. Click **Next**.
14. Select **ArcSight Manager (encrypted)**.



15. Click **Next**.
16. Enter the **hostname**, **port**, **username**, and **password** for ArcSight ESM.

Connector Setup

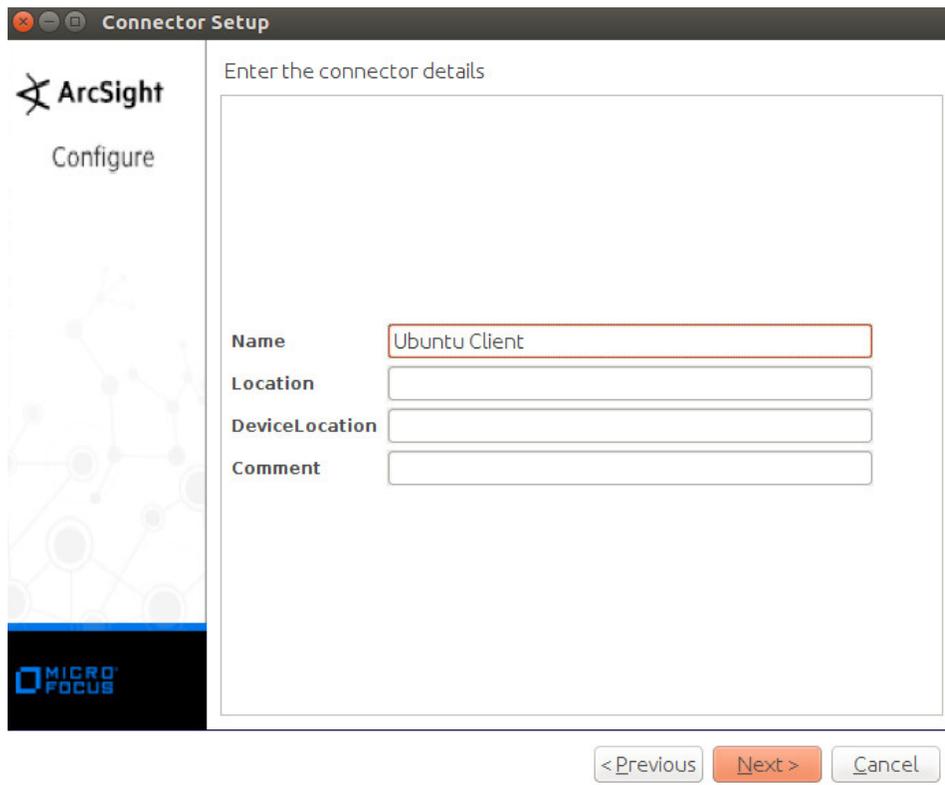
ArcSight
Configure

Enter the destination parameters

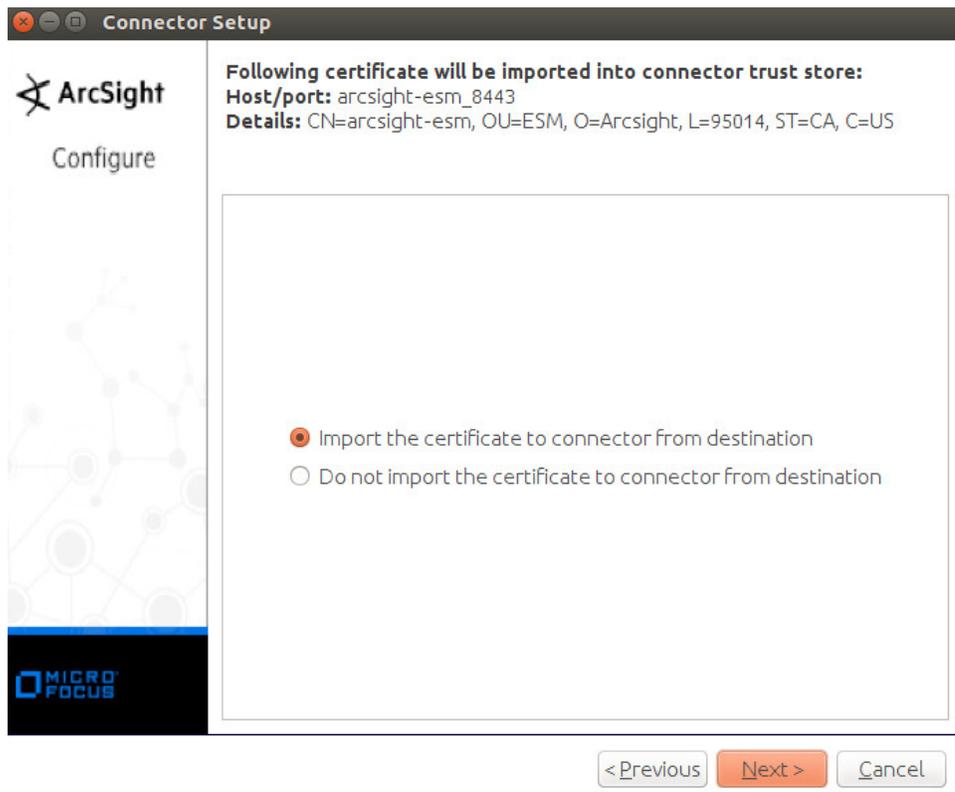
Manager Hostname: arcsight-esm
Manager Port: 8443
User: administrator
Password:
AUP Master Destination: false
Filter Out All Events: false
Enable Demo CA: false

< Previous Next > Cancel

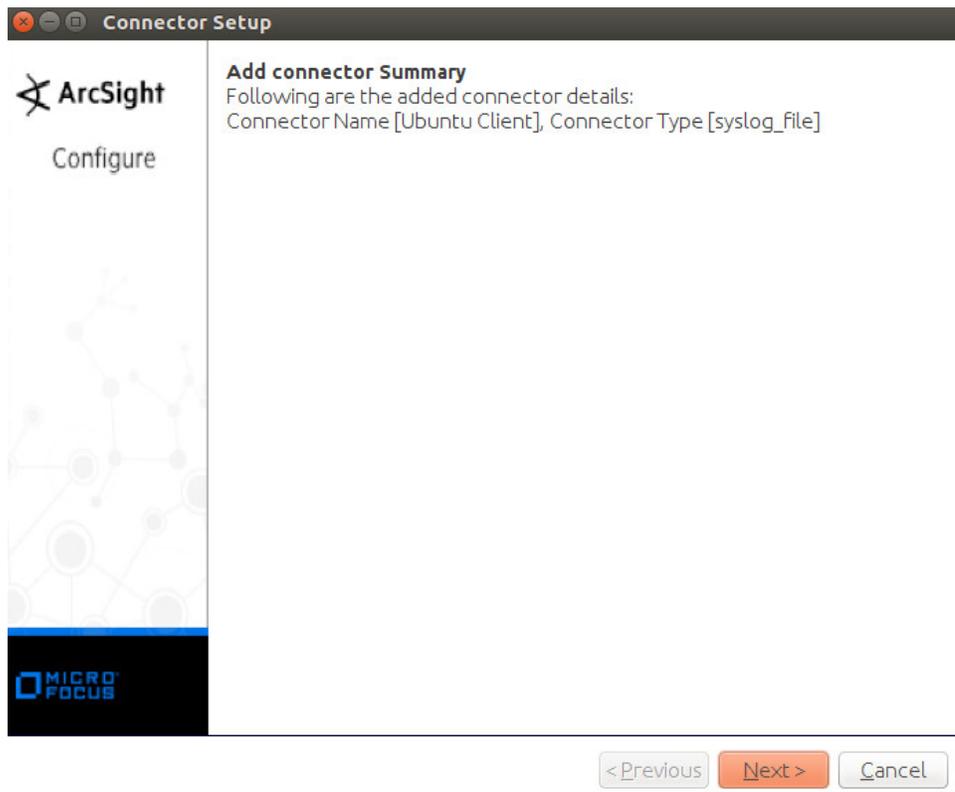
17. Click **Next**.
18. Enter identifying details about the system (only **Name** is required).



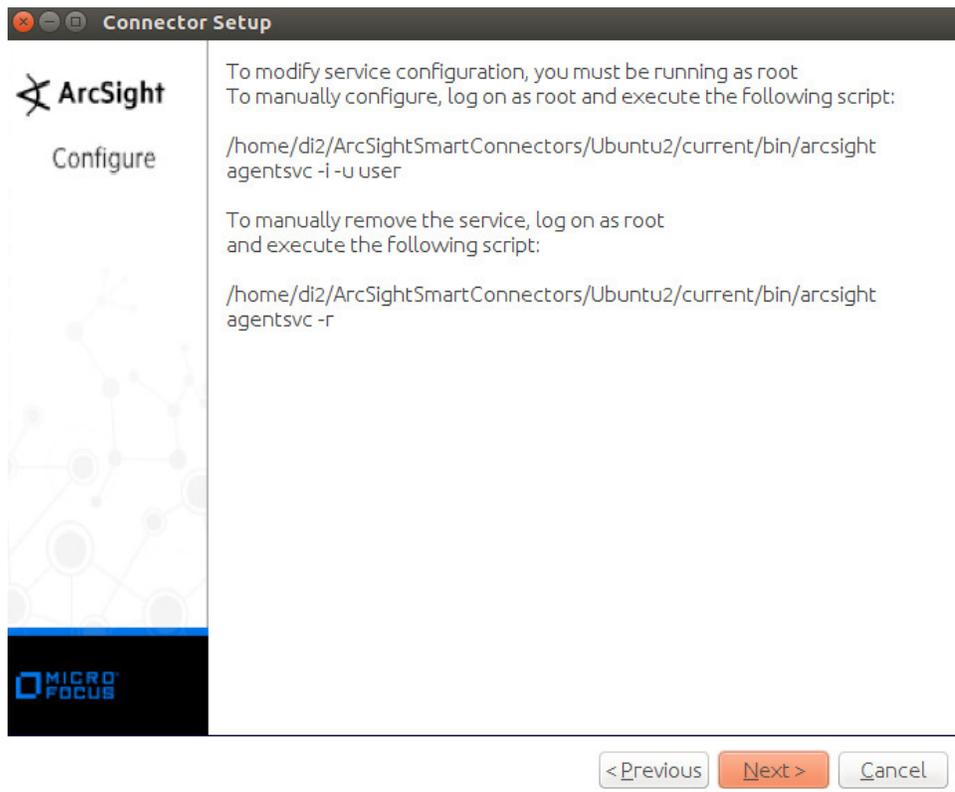
19. Click **Next**.
20. Select **Import the certificate to connector from destination**.



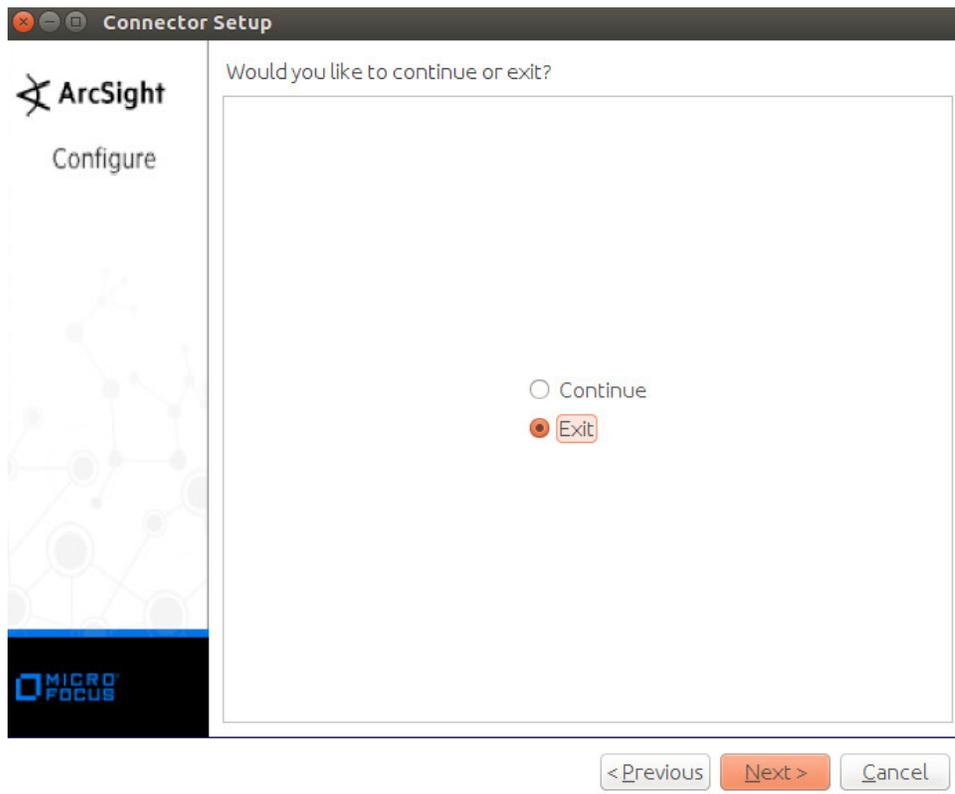
21. Click **Next**.



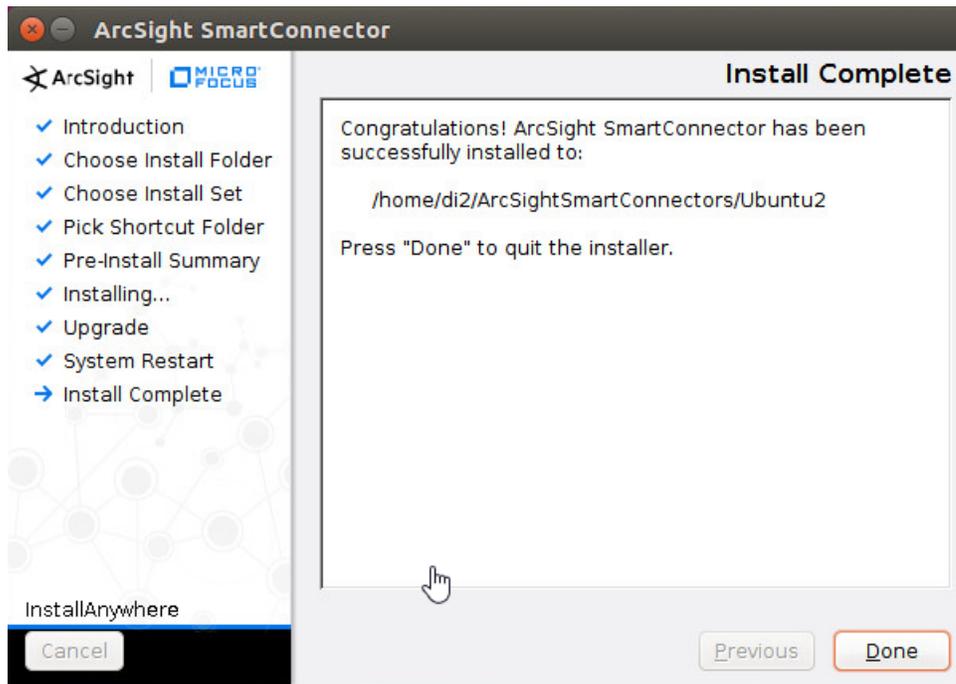
22. Click **Next**.



23. Click **Next**.
24. Select **Exit**.



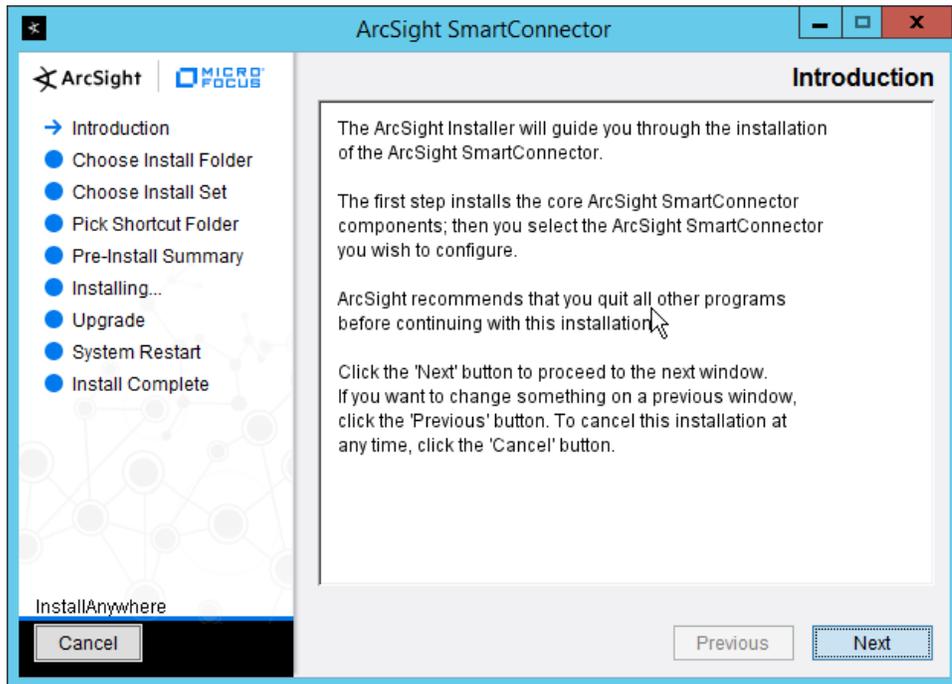
25. Click **Next**.



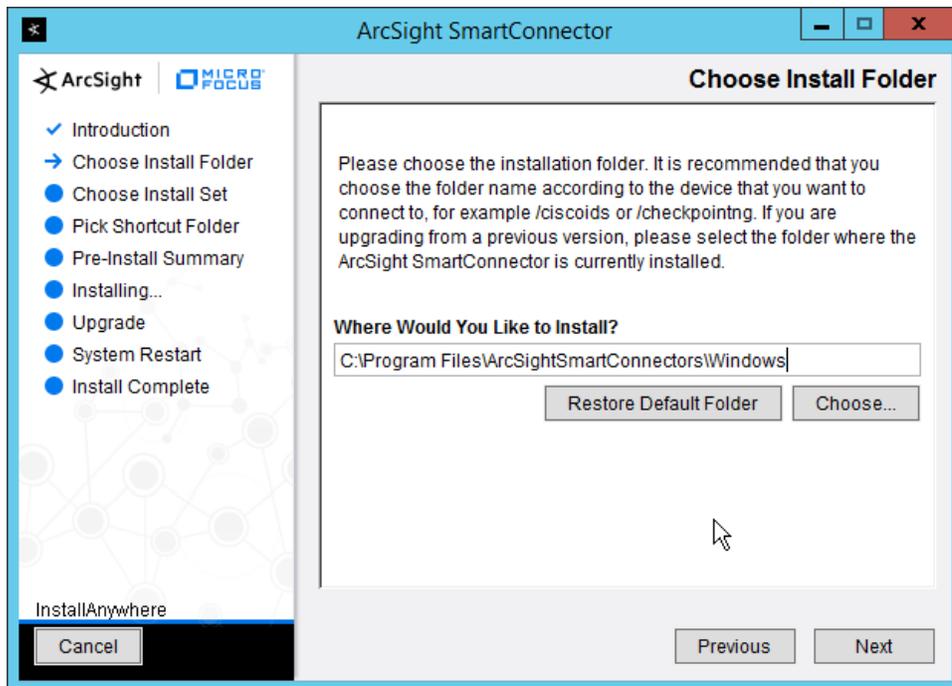
26. Click **Done**.

2.11.4 Install a Connector Server for ESM on Windows 2012 R2

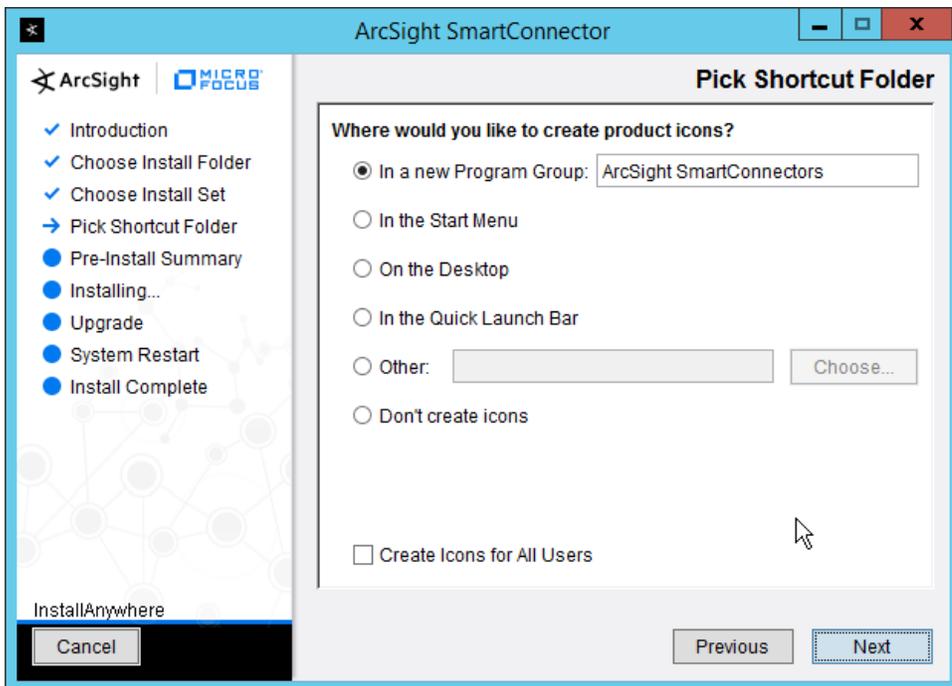
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



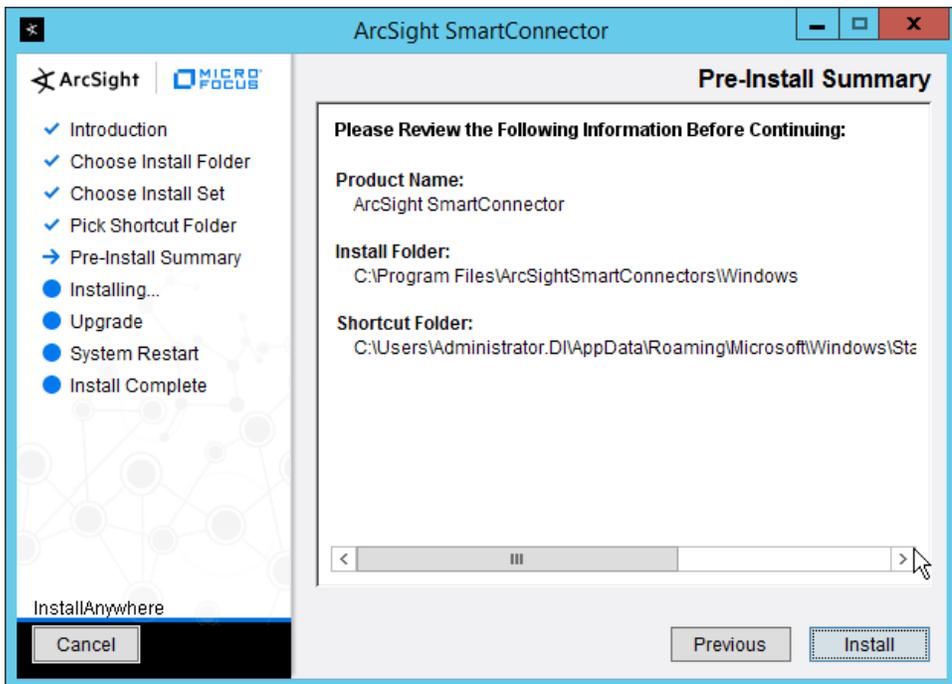
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



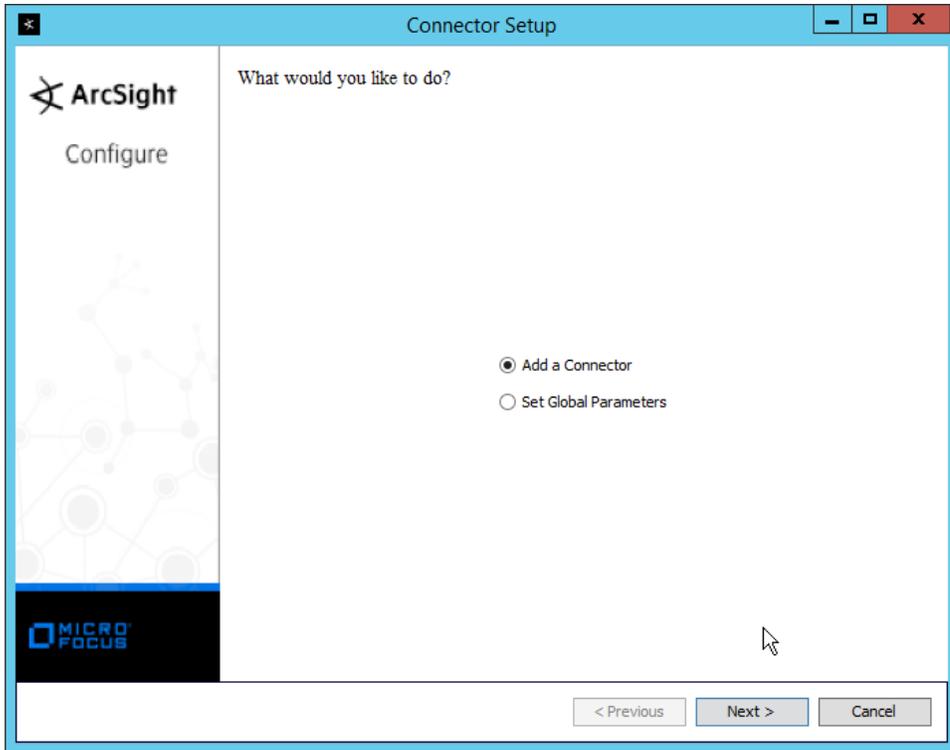
4. Click **Next**.



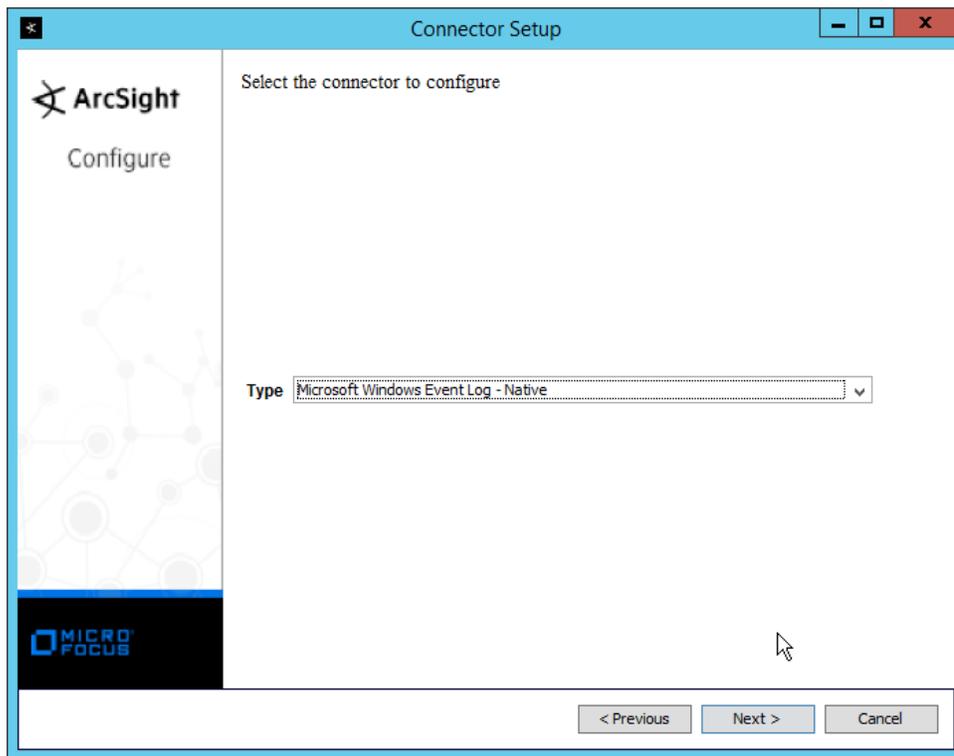
5. Click **Next**.



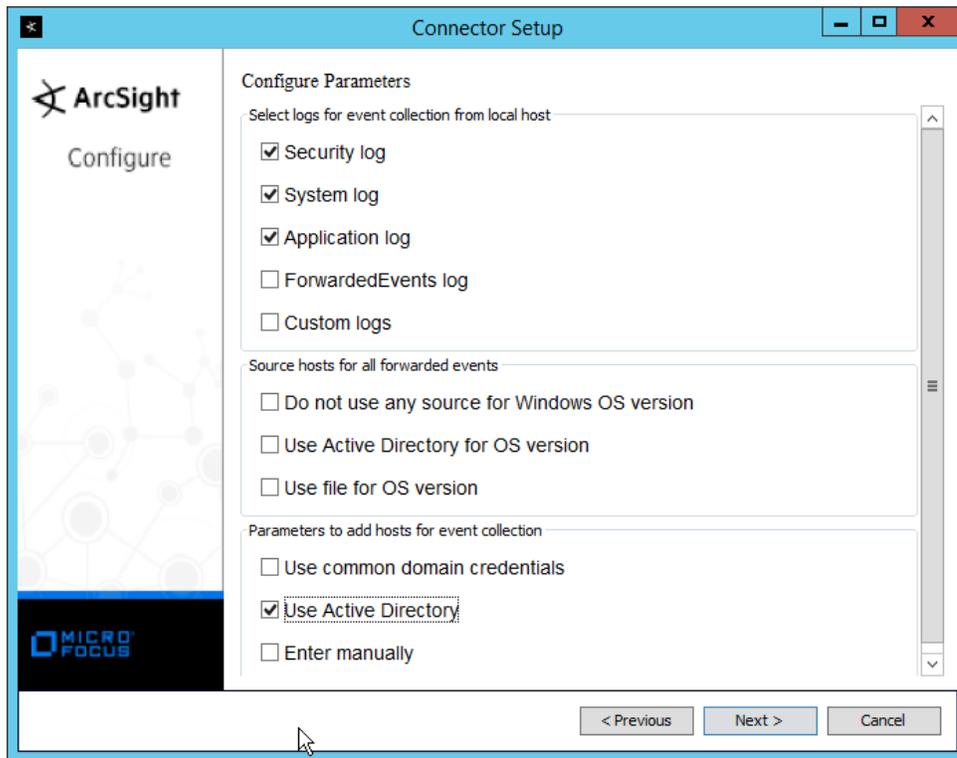
6. Click **Install**.
7. Select **Add a Connector**.



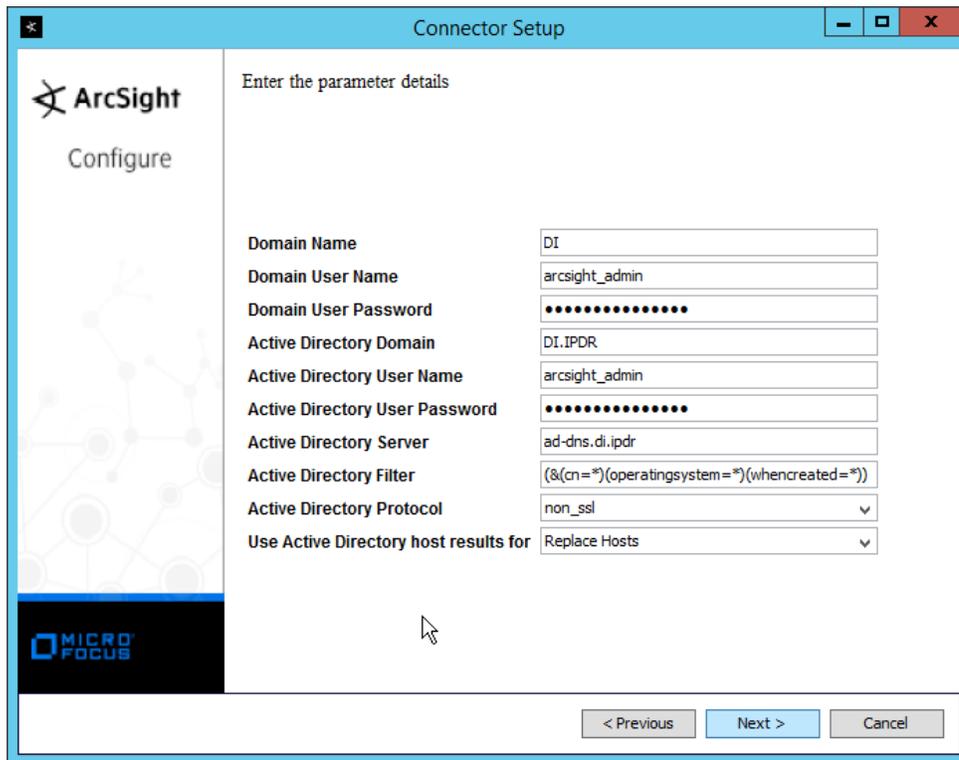
8. Click **Next**.
9. Select **Microsoft Windows Event Log–Native**.



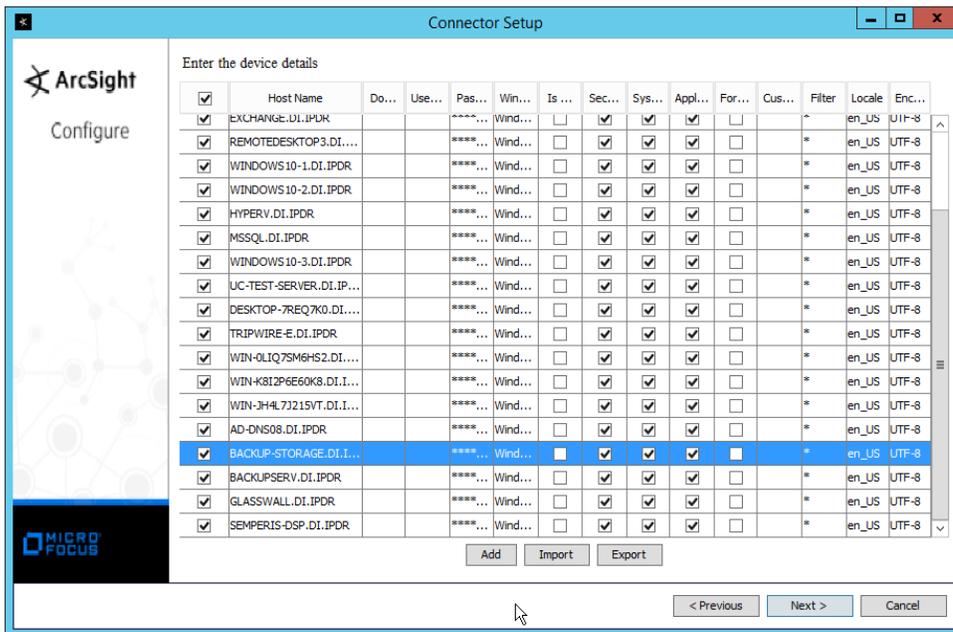
10. Click **Next**.
11. Check the box next to **Use Active Directory**.



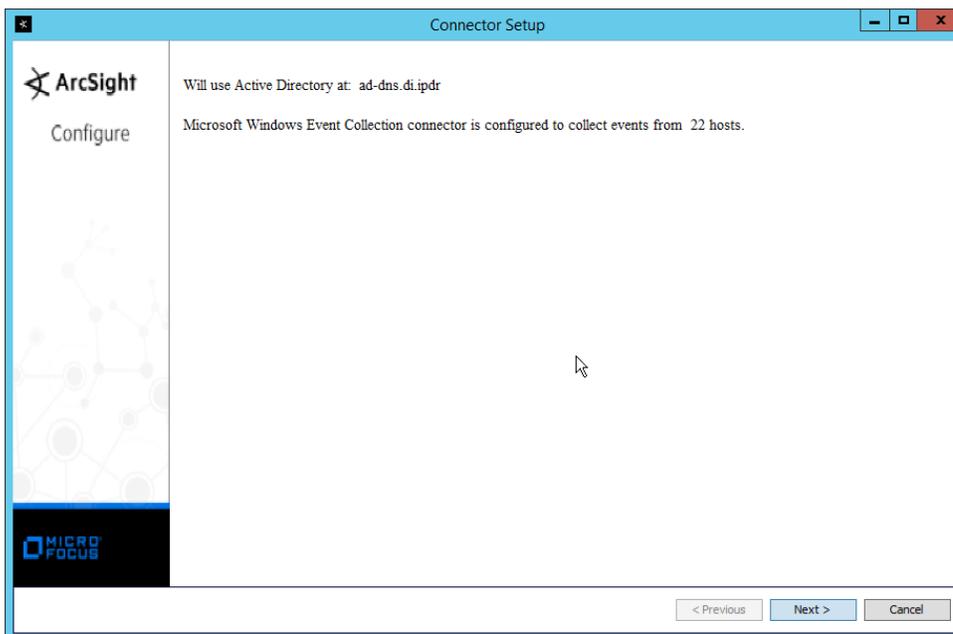
12. Click **Next**.
13. Enter information about your Active Directory server. (It is recommended to create a new administrator account for ArcSight to use.)
14. Set **Use Active Directory host results for** to **Replace Hosts**.



15. Click **Next**.
16. Check the boxes under any event types that should be forwarded to this connector, for each individual host, e.g., **Security, System, Application**.

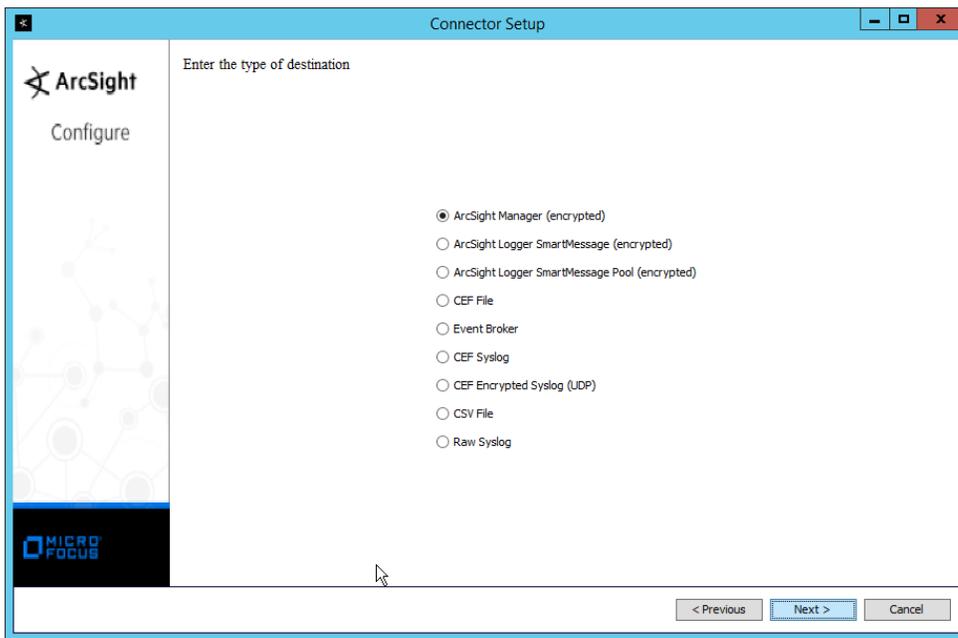


17. Click **Next**.



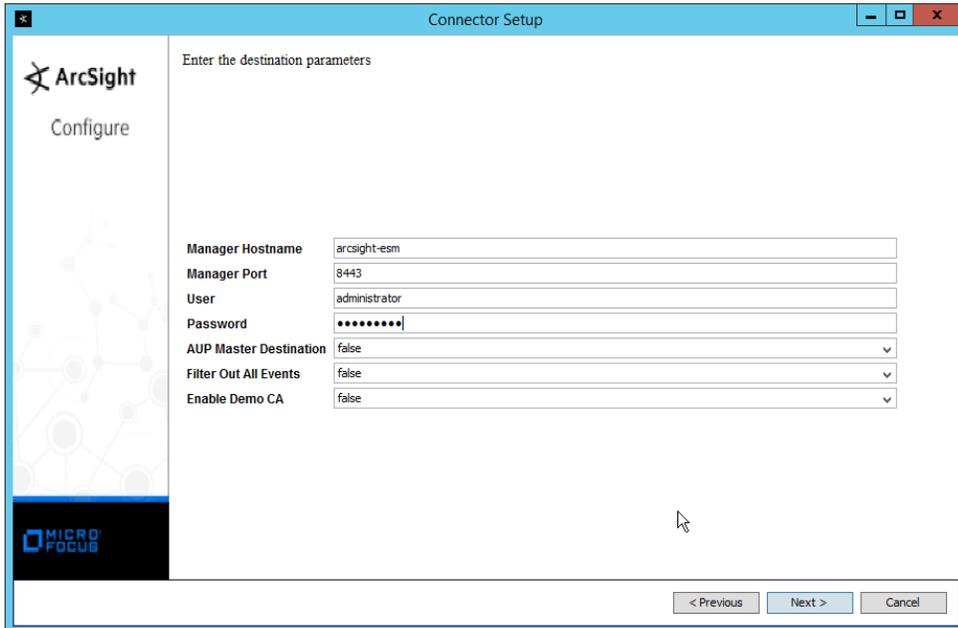
18. Click **Next**.

19. Select **ArcSight Manager (encrypted)**.



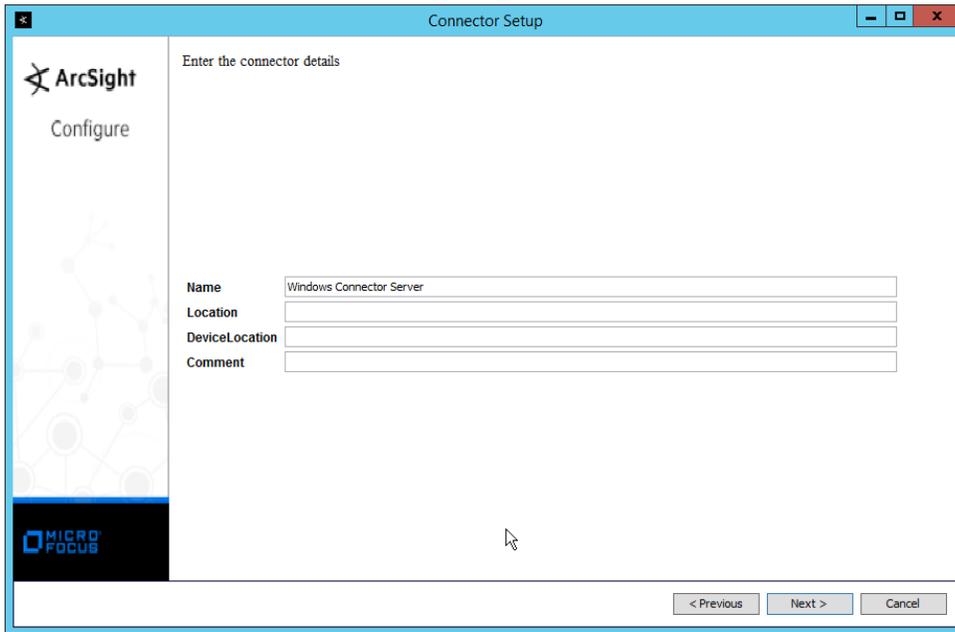
20. Click **Next**.

21. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.



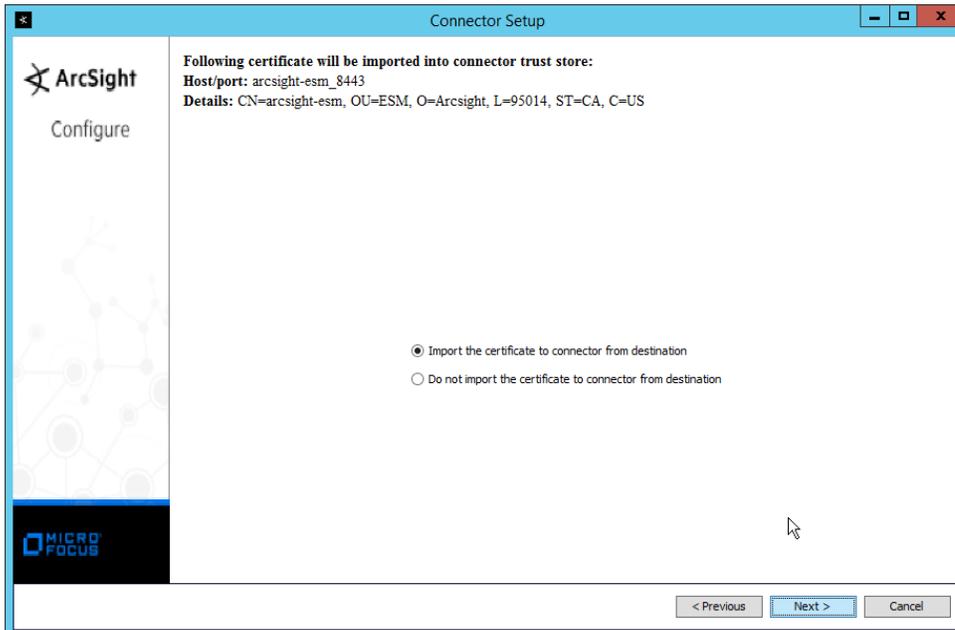
22. Click **Next**.

23. Enter identifying details about the system (only **Name** is required).

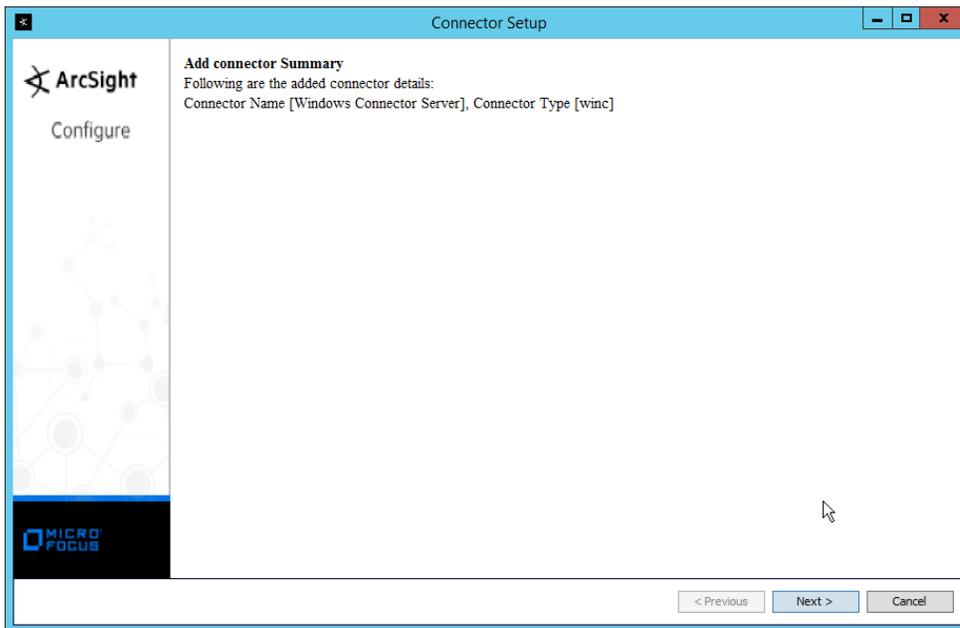


24. Click **Next**.

25. Select **Import the certificate to connector from destination**.

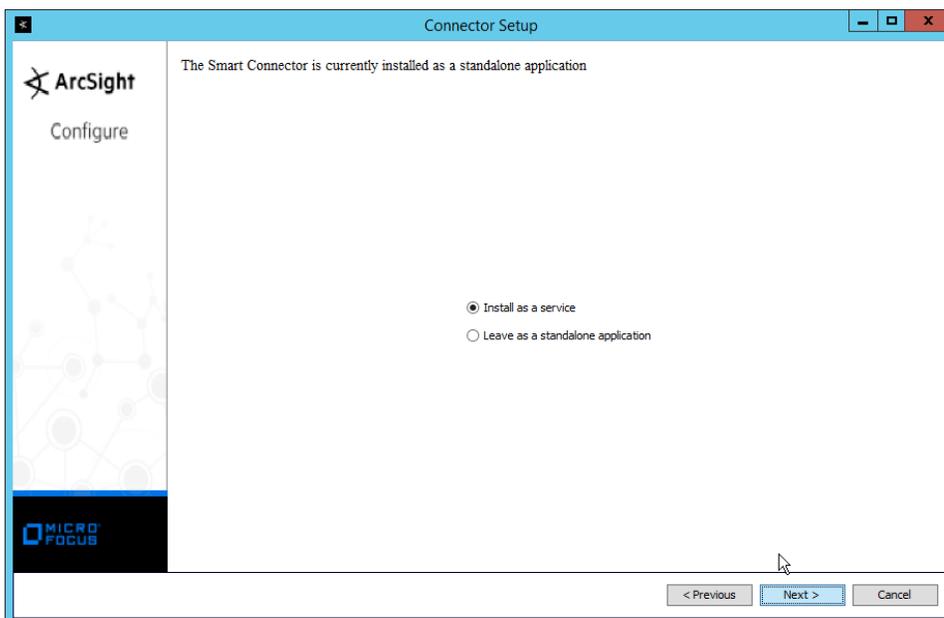


26. Click **Next**.

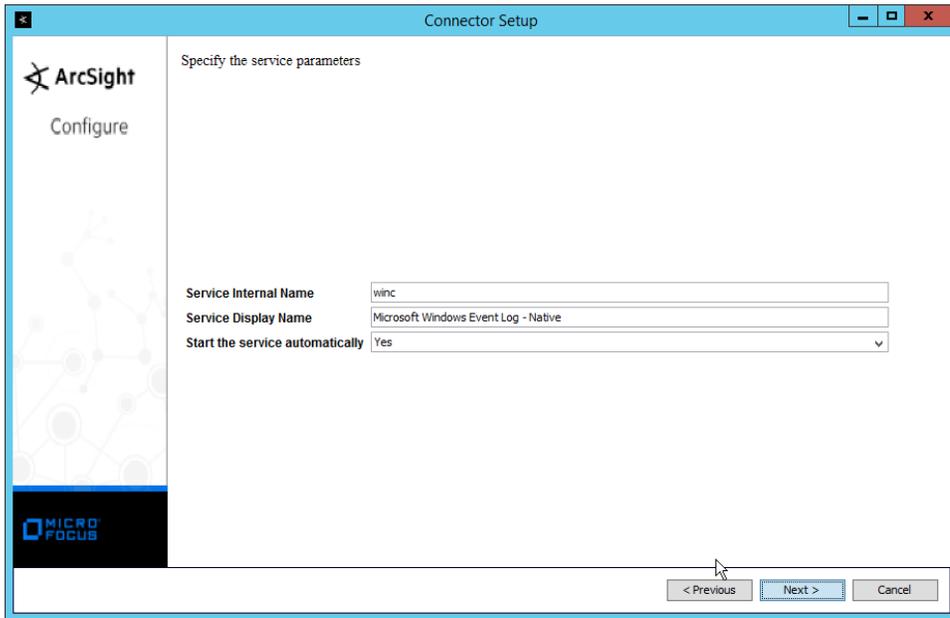


27. Click **Next**.

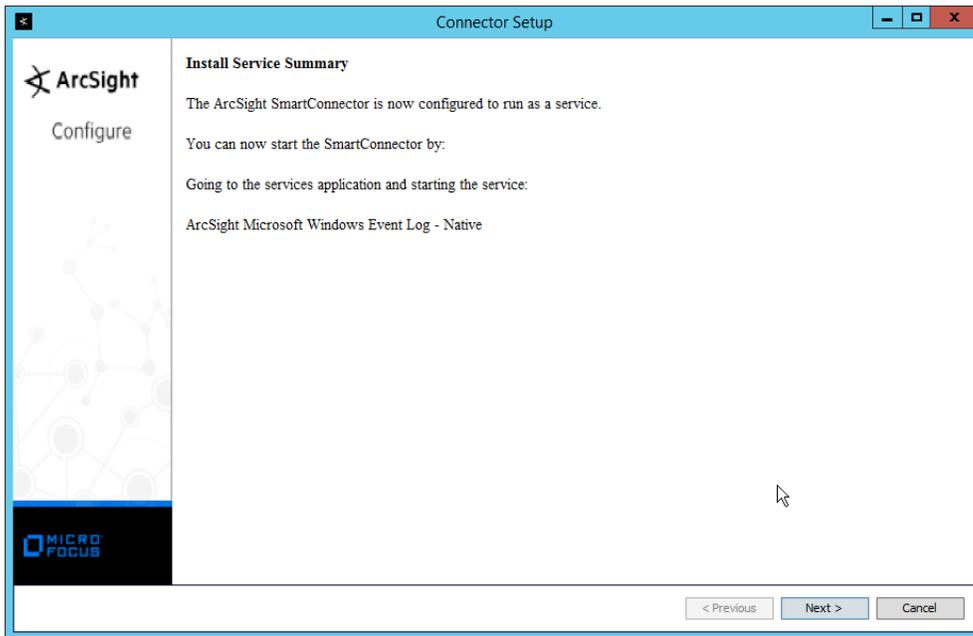
28. Select **Install as a service**.



29. Click **Next**.

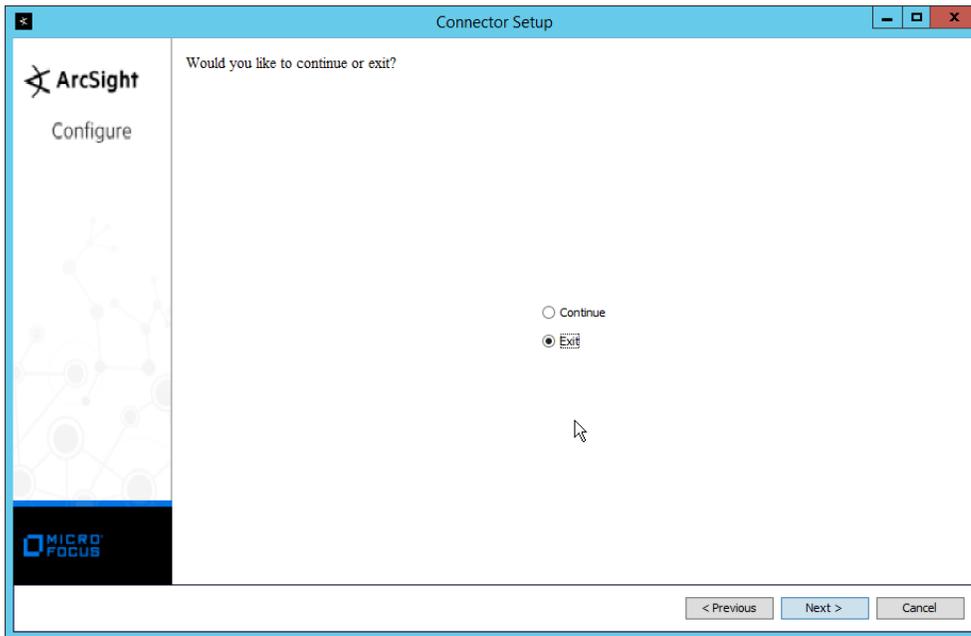


30. Click **Next**.

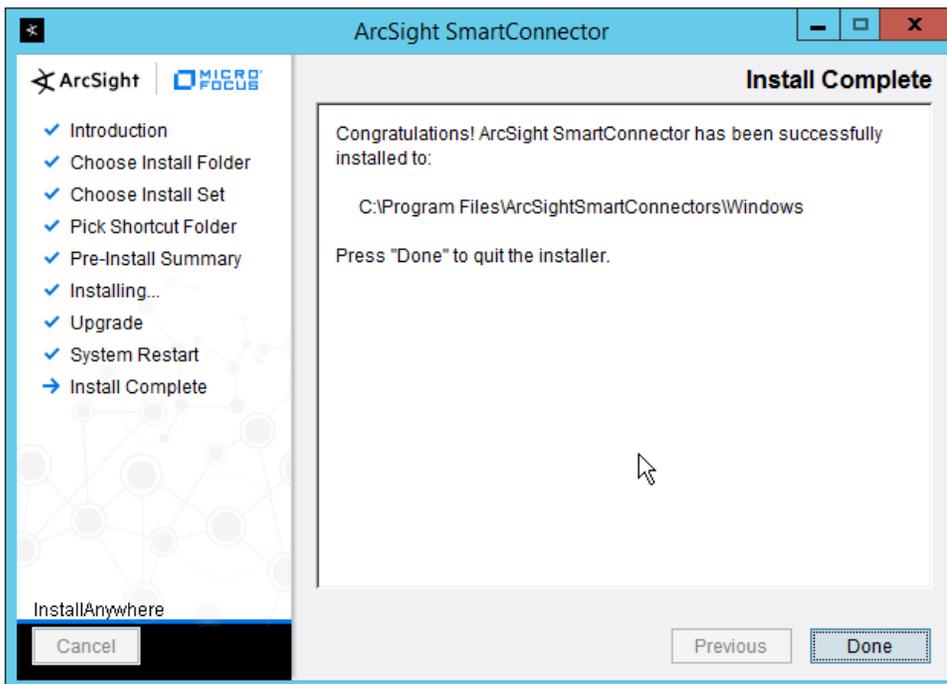


31. Click **Next**.

32. Select **Exit**.



33. Click **Next**.



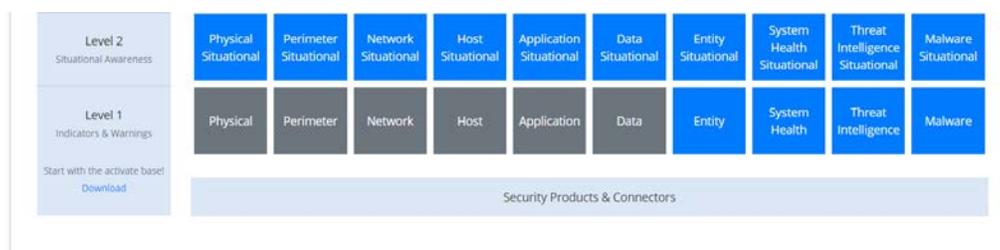
34. Click **Done**.

35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.

2.11.5 Install Preconfigured Filters for ArcSight

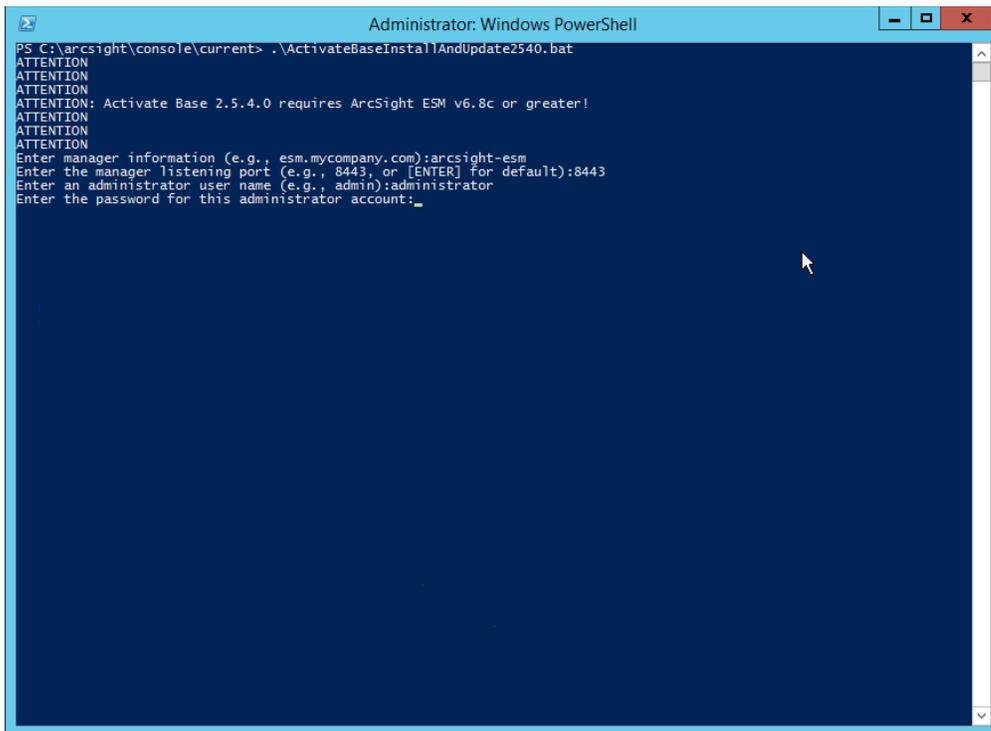
2.11.5.1 Install Activate Base

1. Go to the ArcSight Content Brain web application (<https://arcsightcontentbrain.com/app/>) and log in. This page allows you to keep track of packages to be installed—what packages should be installed depends on the needs of the organization, but the “Activate Base” is required for all products.



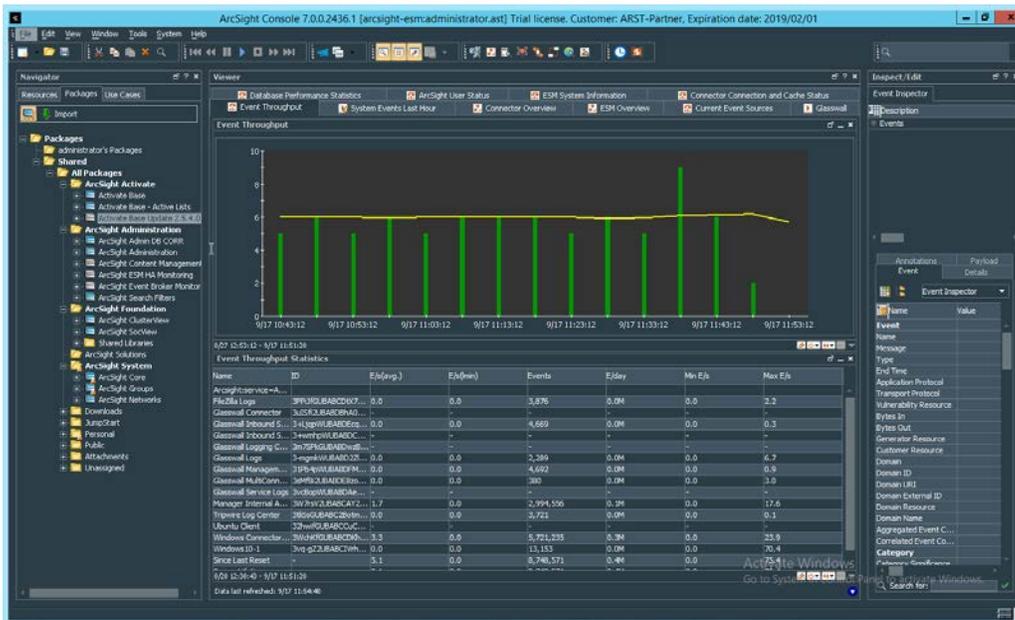
2. Click the **Download** link for the Activate Base. (Note: This package should be installed on the ArcSight Console, not on the ESM.)
3. Copy the contents of the zip file to ARCSIGHT_HOME. The default for this is C:\arcsight\Console\current, assuming a Windows Server.
4. In PowerShell, navigate to the ARCSIGHT_HOME directory (C:\arcsight\Console\current) and run:

```
> .\ActivateBaseInstallAndUpdate2540.bat
```



```
Administrator: Windows PowerShell
PS C:\arcsight\console\current> .\ActivateBaseInstallAndUpdate2540.bat
ATTENTION
ATTENTION
ATTENTION
ATTENTION: Activate Base 2.5.4.0 requires ArcSight ESM v6.8c or greater!
ATTENTION
ATTENTION
ATTENTION
Enter manager information (e.g., esm.mycompany.com):arcsight-esm
Enter the manager listening port (e.g., 8443, or [ENTER] for default):8443
Enter an administrator user name (e.g., admin):administrator
Enter the password for this administrator account:_____
```

5. Enter the **hostname** of the ArcSight machine, the **port** (default: 8443), and the **username** and **password** used to connect to the **ESM**.
6. Delete **Activate_Base_Updated_2.5.4.0.arb** from the ARCSIGHT_HOME directory.
7. Log in to **ArcSight Console**.

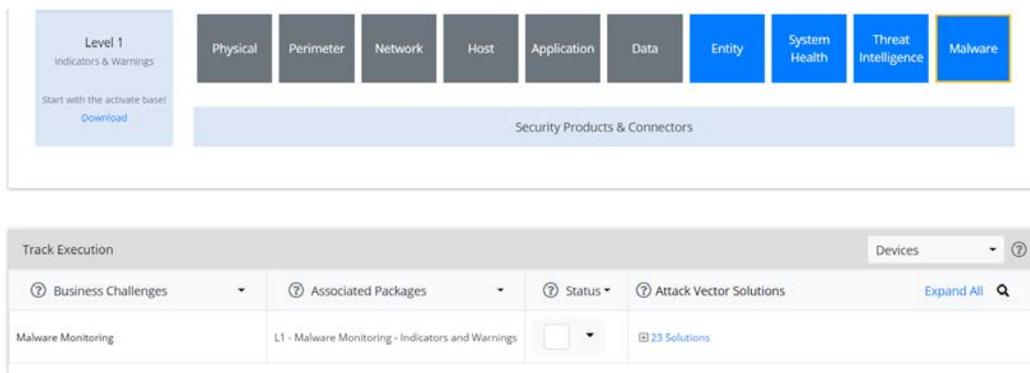


- Under **Packages > Shared > All Packages > ArcSight Activate**, right-click **Activate Base Update 2.5.4.0**, and select **Delete Package**.

2.11.5.2 Install Packages

Once the Activate Base is installed, packages can be installed to monitor for specific types of events. As an example, find below instructions for the Malware Monitoring package.

- Navigate to the **ArcSight Content Brain** web application.
- Select the **Level 1** box labeled **Malware**.



- In the **Track Execution** section, under **Associated Packages**, you can see the list of packages used to address the challenge of **Malware Monitoring**. In this case, there is just one package, **L1–**

Malware Monitoring–Indicators and Warnings. Click the link to be taken to a download page for the package, and download it. (Note: This package should be installed on the ArcSight Console, not on the ESM.)

4. Copy the contents of the zip file to ARCSIGHT_HOME. The default for this is C:\arcsight\Console\current, assuming a Windows Server.
5. In PowerShell, navigate to the ARCSIGHT_HOME directory (C:\arcsight\Console\current) and run:

```
> .\L1-Malware_Monitoring_1.1.0.1.bat
```

```

Administrator: Windows PowerShell

Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre

ArcSight Package Utility starting...

Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)
Configuration initialized: config\console.defaults.properties; config\console.properties

ArcSight
Package Utility Version 7.0.0.2436.1 (8E2436_8-1-2018_12:17:31)

Copyright (c) 2001-2018 Micro Focus or one of its affiliates.
All rights reserved.
Logging in to manager 'arcsight-esm' with username 'administrator'...done.
JVM memory allowed: 455.5 MB
System locale: en_US

will now install:

Installing the following packages:
  /All Packages/ArcSight Activate/Activate Base
-----
Install complete. Elapsed Time:10 mins 28 secs 792 ms
Exiting...

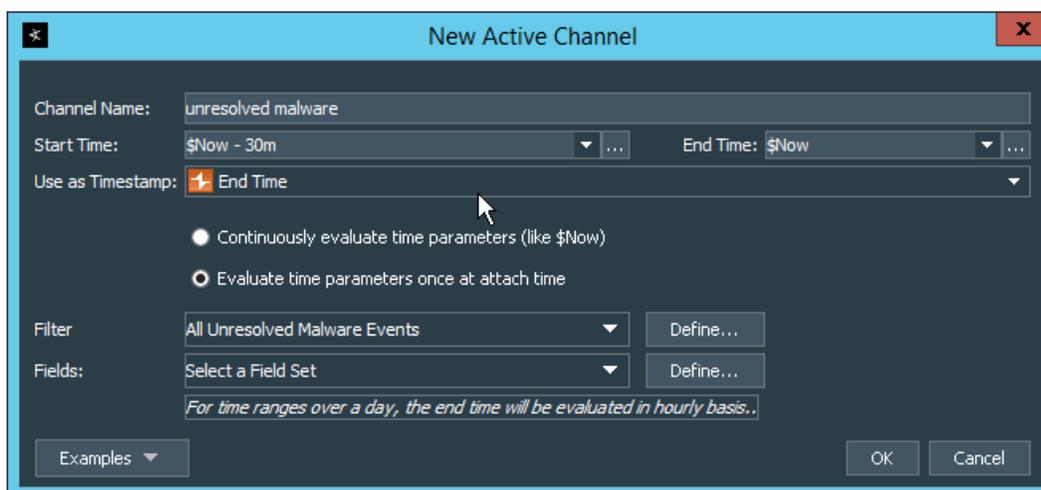
ATTENTION
ATTENTION
ATTENTION: From your ESM console UI:
ATTENTION: Please delete /All Packages/ArcSight Activate/Activate Base Update 2.5.4.0.
ATTENTION:
ATTENTION:
ATTENTION: From your ESM console's file system:
ATTENTION: Please delete Activate_Base_Updated_2.5.4.0.arb
ATTENTION:
ATTENTION:
ATTENTION:
PS C:\arcsight\console\current> .\L1-Malware_Monitoring_1.1.0.1.bat
Enter manager information (e.g., esm.mycompany.com):arcsight-esm
Enter the manager listening port (e.g., 8443, or [ENTER] for default):8443
Enter an administrator user name (e.g., admin):administrator
Enter the password for this administrator account:

```

6. Enter the **hostname** of the ArcSight machine, the **port** (default: 8443), and the **username** and **password** used to connect to the **ESM**.

2.11.6 Apply Filters to a Channel

1. In the **ArcSight Console**, click **File > New > Active Channel**.
2. Enter a **name** for the channel.
3. Select a time frame.
4. For **Filter**, select one the filters that was imported from the packages you installed.



5. Click **OK**. All events that match the filter can be displayed in the newly created channel. Filters from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate > Solutions**.

2.12 Tripwire Enterprise

Notes:

This installation requires MSSQL to be installed on a remote server and configured according to the instructions in the ***Tripwire Enterprise 8.6.2 Installation and Maintenance Guide***.

2.12.1 Install Tripwire Enterprise

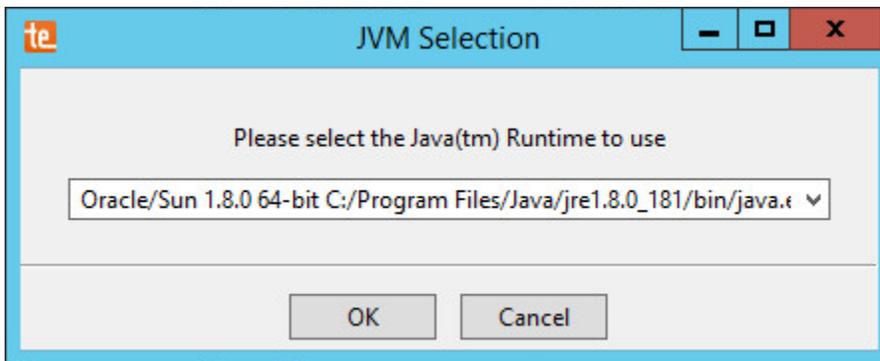
1. Ensure that you have an up-to-date version of Oracle Java. You must install both the Java Runtime Environment (JRE) and the Java Cryptography Extension (JCE).
2. Download and run the **JRE installer**.



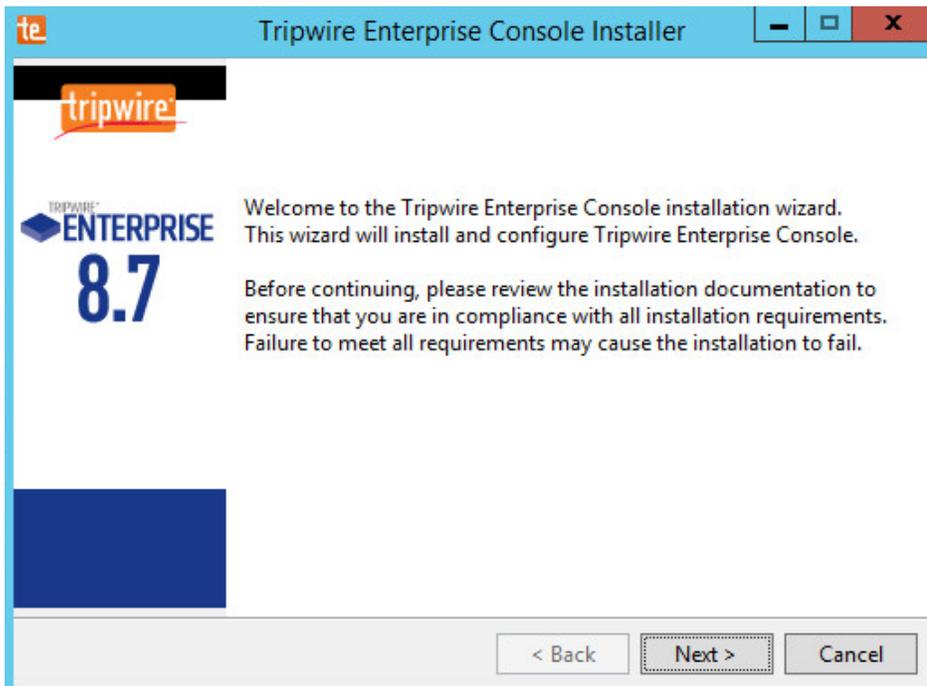
3. Click **Install**.
4. Download the JCE and extract the files.

Name	Date modified	Type	Size
local_policy	12/20/2013 1:54 PM	JAR File	3 KB
README	12/20/2013 1:54 PM	Text Document	8 KB
US_export_policy	12/20/2013 1:54 PM	JAR File	3 KB

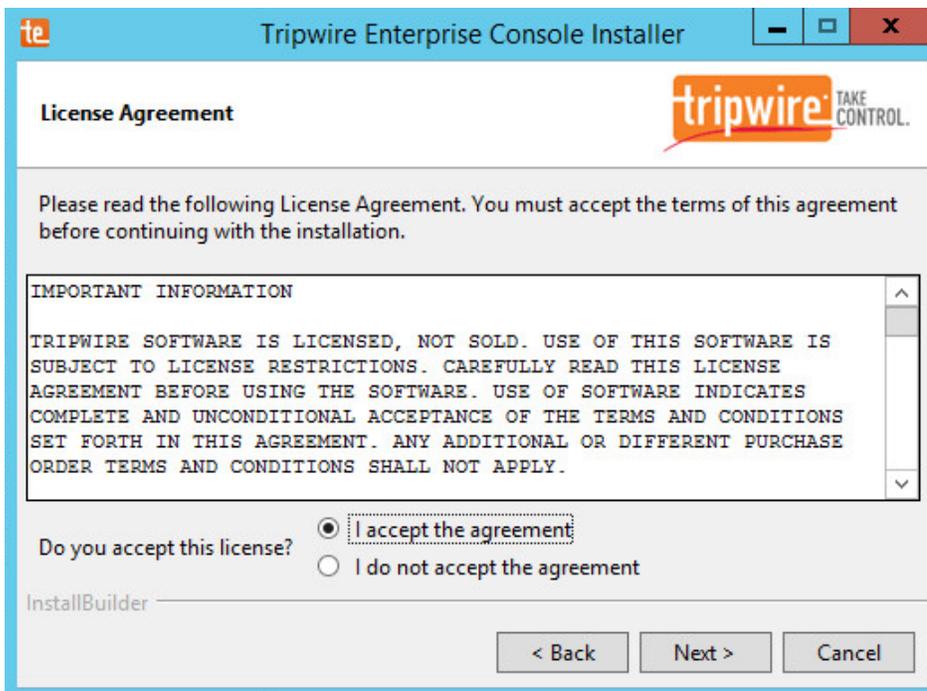
5. Copy the *local_policy.jar* and *US_export_policy.jar* files to `/lib/security/Unlimited/` and `/lib/security/Limited` in the Java installation directory.
6. Run **install-server-windows-amd64**.
7. Select the Java runtime that was just installed.



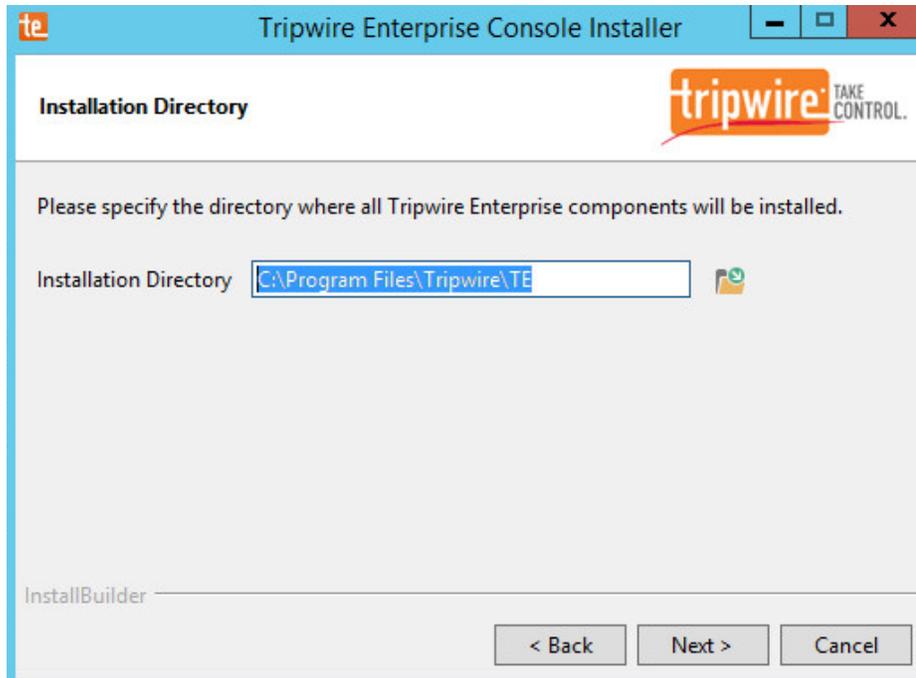
8. Click **OK**.



9. Click **Next**.
10. Select **I accept the agreement**.

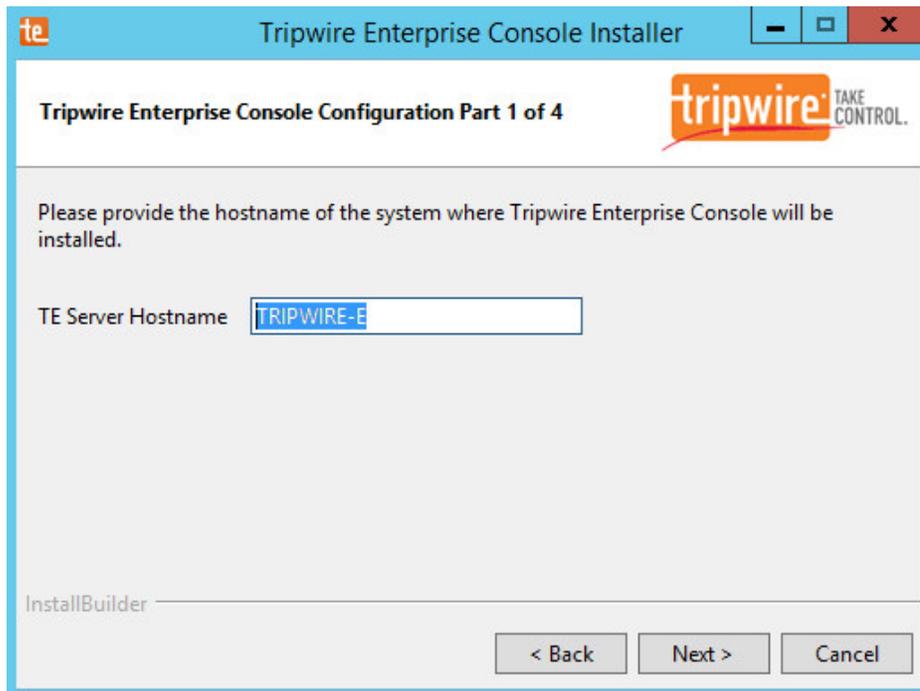


11. Click **Next**.

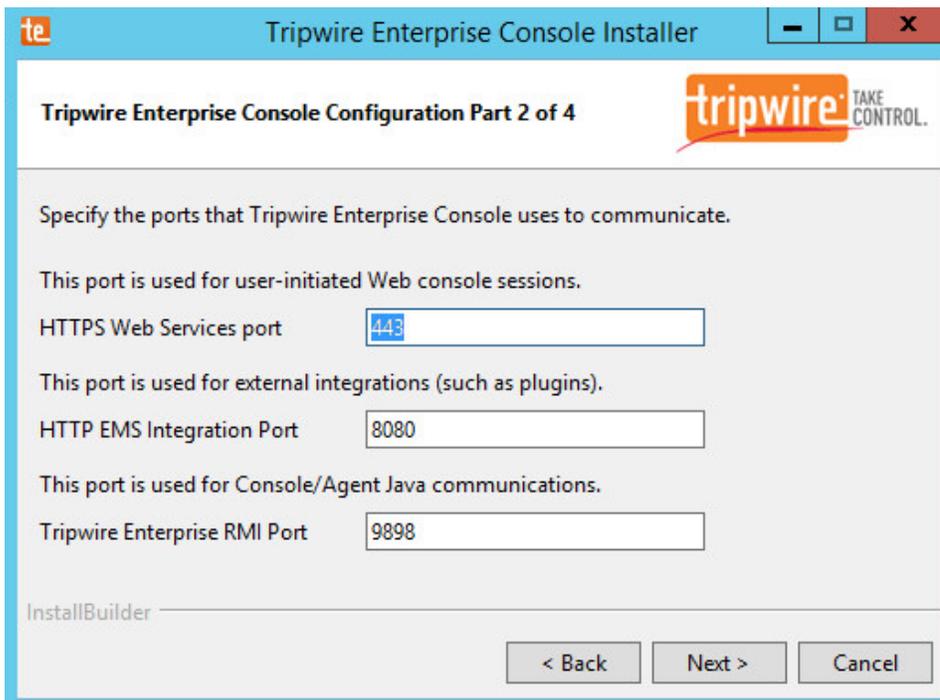


12. Click **Next**.

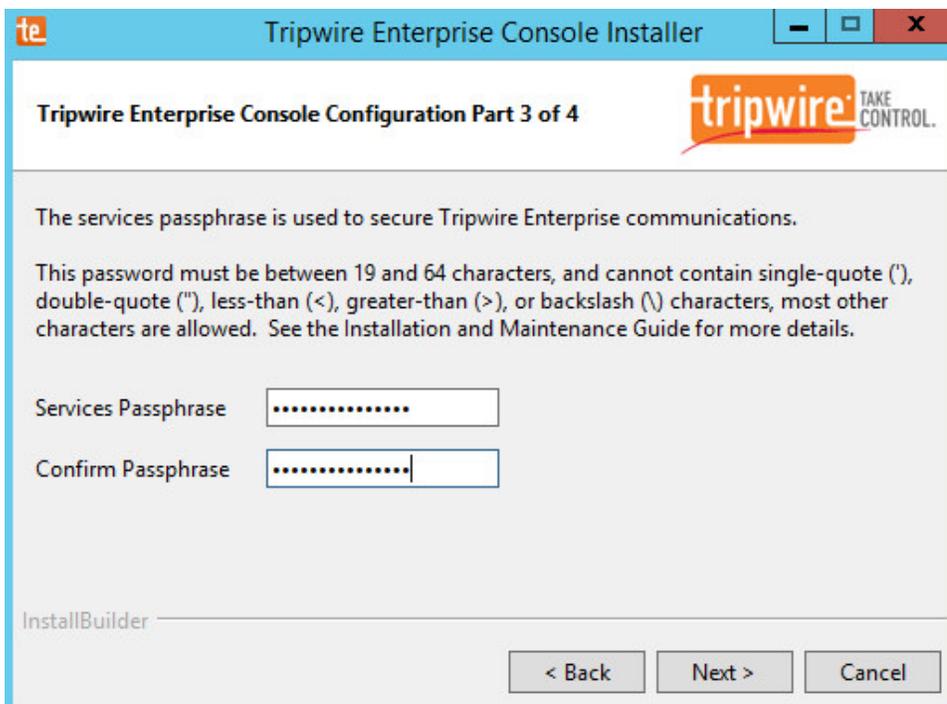
13. The installer should automatically detect the hostname of the system on which Tripwire Enterprise is being installed. If it does not, enter the hostname here.



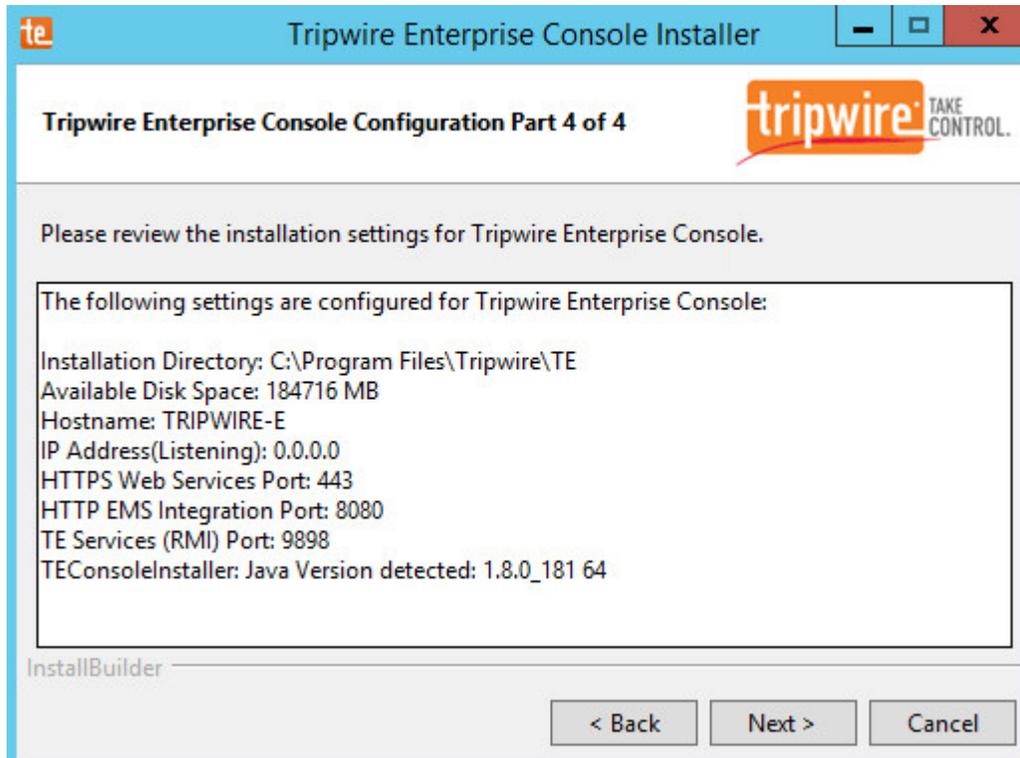
14. Click **Next**.
15. Enter each port number to use for the HTTPS Web Services port, HTTP EMS Integration Port, and Tripwire Enterprise RMI port. The RMI port is used for inbound communication from Tripwire agents to the server, so ensure that it is allowed through the firewall.



16. Click **Next**.
17. Enter a passphrase to use.



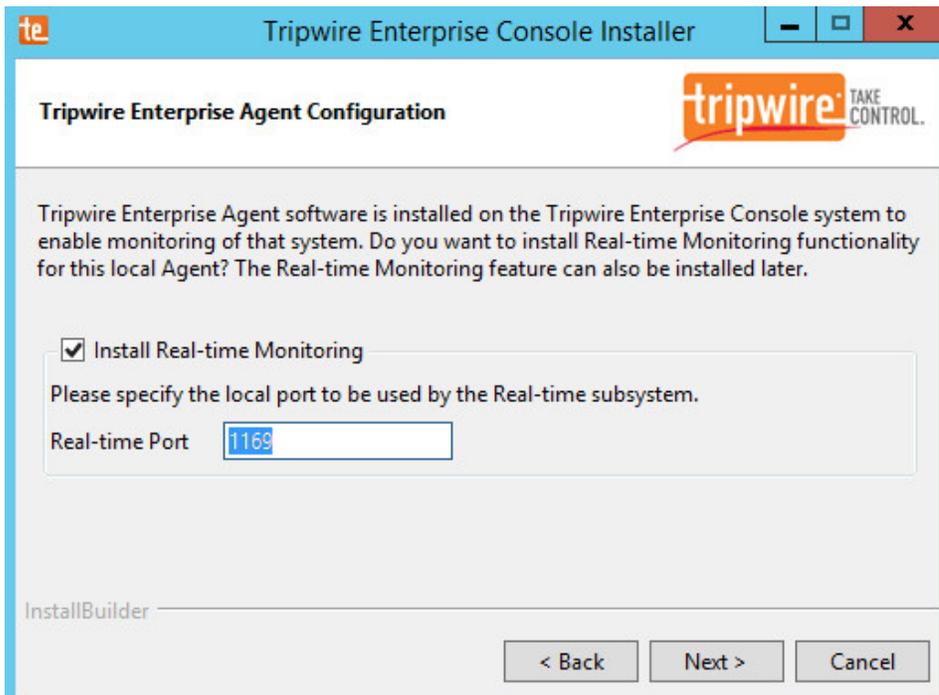
18. Click **Next**.



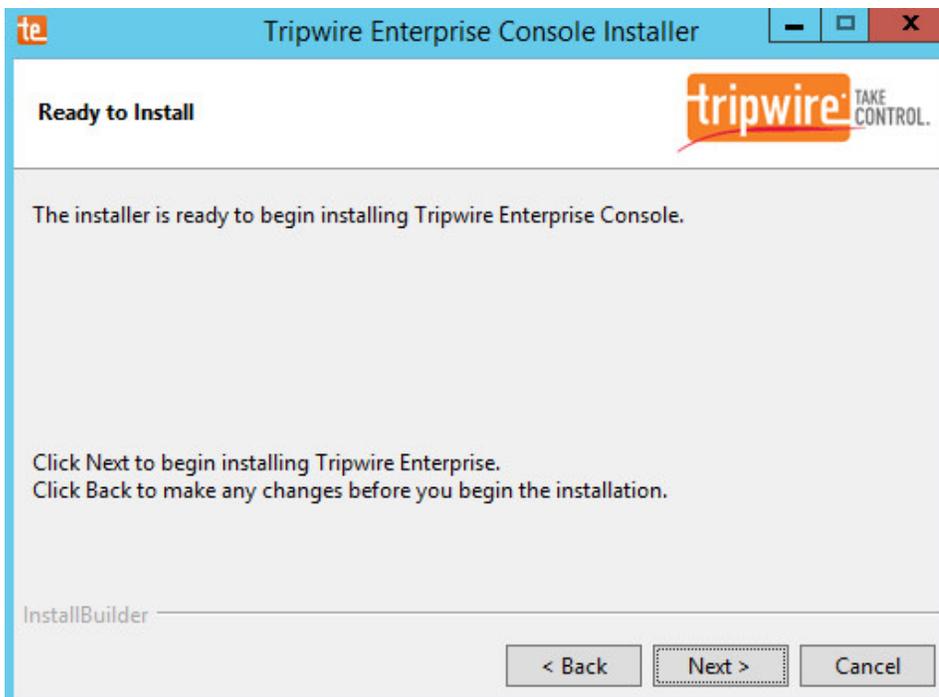
19. Click **Next**.

20. Check the box next to **Install Real-time Monitoring**.

21. Enter **1169** for **Real-time Port**.

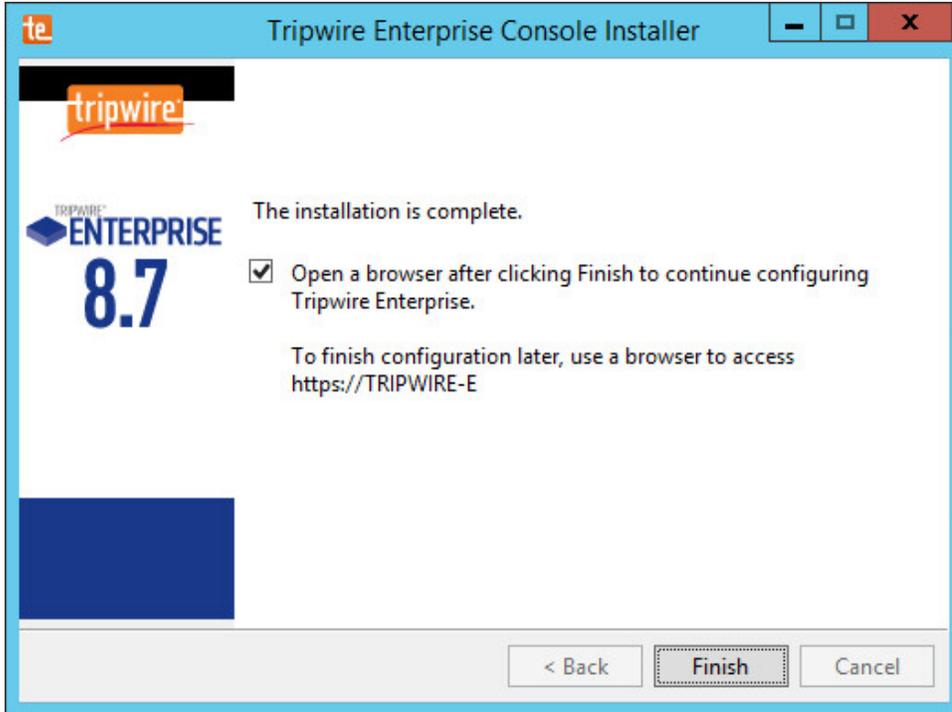


22. Click **Next**.

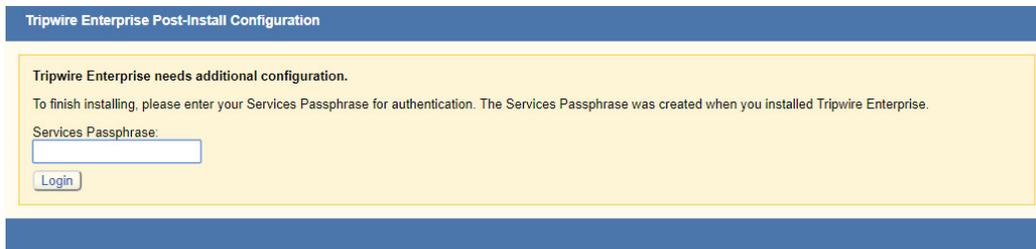


23. Click **Next**.

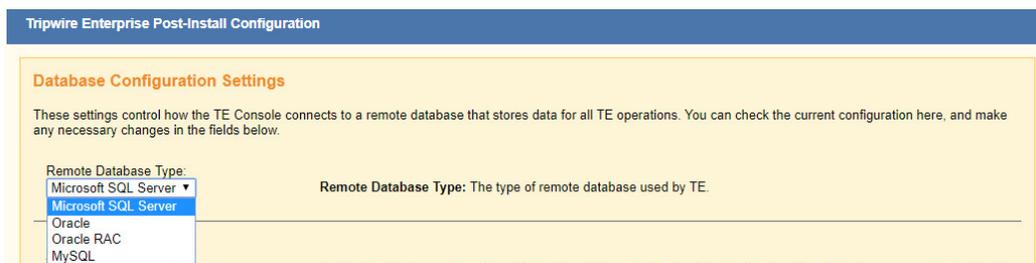
24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise**.



25. Click **Finish**.
26. Once at the web address, enter the **Services passphrase** chosen earlier.



27. Click **Login**.



28. Select **Microsoft SQL Server** for **Remote Database Type**.
29. Select **SQL Server** for **Authentication Type**.
30. Enter login details for the account created during the MSSQL setup.
31. Enter the **hostname** or **IP** of the database server.
32. Enter the **port** on which the database is operating.
33. Enter the **name** of the database to be used for Tripwire Enterprise.
34. Select the appropriate setting for **SSL** according to your organization's needs.

The screenshot shows a configuration window for a remote database connection. It includes the following fields and descriptions:

- Authentication Type:** A dropdown menu set to "SQL Server". Description: Specifies whether the database login should authenticate using a Windows account (typically of the format domain\user), or an SQL Server account (an account defined only in SQL Server). With the Windows authentication type, NTLMv2 should be used, as it is cryptographically superior to the first version of NTLM. However, as NTLMv2 is configured in the operating system, not in the database or application, TE can be used with NTLM to ensure compatibility.
- Login Name:** A text box containing "twadmin". Description: The login name that TE will use to authenticate with the database.
- Password:** A text box with masked characters. Description: The password that TE will use to authenticate with the database.
- Database Host:** A text box containing "192.168.78.125". Description: The fully qualified domain name, hostname or IP address of the system where the database is installed.
- Port (default 1433):** A text box containing "1433". Description: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.
- Database Name:** A text box containing "TE_DB". Description: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.
- Instance Name (Optional):** An empty text box. Description: The location/name of the database instance on the server. Ask your DBA if a non-default instance should be used for TE.
- SSL:** A dropdown menu set to "Off". Description: SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.
 - Request - SSL will be used if available.
 - Require - SSL will always be used, and an error will occur if SSL is not available for the database.
 - Authenticate - SSL will always be used, and an error will occur if SSL is not available for the database. In addition, the certificate chain of the database server's public key will be authenticated using TE's trust store. If the certificate chain does not originate from a trusted source, an error will occur.
 - Off - SSL will never be used. This setting is not recommended.

At the bottom of the form is a "Test Database Login" button with a green checkmark icon.

35. Click **Test Database Login** to ensure the connection is functional.

The screenshot shows the "Test Results" section of the configuration window. It displays a message box that says "Connection Succeeded." Below the message box are three buttons: "Save Configuration and Restart Console" and "Logout".

36. Click **Save Configuration and Restart Console**.
37. After the reboot, enter a new administrator **password**.

Tripwire Enterprise Post-Install Configuration

Configuration Steps Needed:

Tripwire administrator account password needs to be changed from the default.

Create Administrator Password

Passwords must:
Be between 8 and 128 characters in length
Contain at least 1 numeric character
Contain at least 1 uppercase character
Contain at least 1 non-alphanumeric character
Supported characters: ~!@#%&'()*_-+{}|\;:'" < > / ?

Password:

Confirm Password:

Support Information

Still having problems with your installation?
Contact Tripwire Support: <https://secure.tripwire.com/customers/contact-support.cfm>
Or open a Support ticket: <https://secure.tripwire.com/customers/>

For faster assistance from Support, please generate a support bundle to collect information about your system and this installation. Attach the support bundle file to your web ticket or email. [What is a Support Bundle?](#)

Tripwire Enterprise 8.7.0.b8.7.0.r20180606173604-e215728.b40

38. Click **Confirm and Continue**.

Tripwire Enterprise Fast Track

Welcome to Tripwire Enterprise Fast Track!



Fast Track will help you to configure Tripwire Enterprise for Change Auditing, Policy Management, or an integrated Security Configuration Management (SCM) solution. It only takes a few minutes to complete the setup questionnaire. After you do, Fast Track will use your answers to install the components that you need.

Step 1: Add your license file and describe your environment. This includes the platforms you want Tripwire Enterprise to monitor, the policies you want to enforce, and the schedule that Tripwire Enterprise should use.

Step 2: Review the items that will be configured and save the manifest for your records.

Step 3: Apply the configuration and let Fast Track do the rest.

Note: After Fast Track configures Tripwire Enterprise, you can always make changes to your configuration later from the Tripwire Enterprise user interface.

39. Click **Configure Tripwire Enterprise**.

Step 1: Add your Tripwire Enterprise license (*.cert)

Choose File No file chosen

- 40. Click **Choose File** and select the Tripwire Enterprise license file, which should be a **.cert** file.
- 41. Check the boxes next to **Change Auditing** and **Policy Management**.

Step 2: Configure Change Auditing and/or Policy Management

Monitoring Solutions Change Auditing
 Policy Management

Available Policies CIS
 PCI
 DISA
 NIST 800-53 (FISMA)

- 42. Select any available policies desired.

Step 3: Specify the platforms to monitor

Note: You are licensed for the **Highlighted** platforms.
 Available Platforms:

Operating System
<input checked="" type="checkbox"/> Microsoft Windows Server 2008 R2
<input checked="" type="checkbox"/> Microsoft Windows Server 2012 R2
<input checked="" type="checkbox"/> Oracle Solaris 10
<input checked="" type="checkbox"/> Oracle Solaris 11
<input checked="" type="checkbox"/> Red Hat Enterprise Linux 6
<input checked="" type="checkbox"/> Red Hat Enterprise Linux 7

Virtual Infrastructure

<input checked="" type="checkbox"/> VMware ESXi 5.5 Server
--

Selected Platforms:

- × Microsoft Windows Server 2008 R2
- × Microsoft Windows Server 2012 R2
- × Oracle Solaris 10
- × Oracle Solaris 11
- × Red Hat Enterprise Linux 6
- × Red Hat Enterprise Linux 7
- × VMware ESXi 5.5 Server

- 43. Select all the operating systems that you wish to monitor with Tripwire Enterprise.

Step 4: Set up a schedule for running checks and reports

Change Audit Scheduling

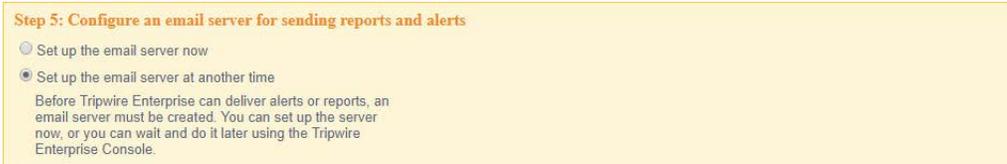
Checks	Reports
How frequently would you like to run checks on your assets? Daily	How frequently would you like to run reports on your assets? Daily
Run the checks at 1:00 AM	Run the reports at 4:00 AM

Checks	Reports
How frequently would you like to run checks on your assets? Weekly on Sundays	How frequently would you like to run reports on your assets? Weekly on Sundays
Run the checks at 1:00 AM	Run the reports at 4:00 AM

Enable Checks and Reports (Optional)

Note: Tripwire does not recommend enabling checks and reports until after you have installed Tripwire Agent software on the systems that you want to monitor.

44. Set up a schedule for running checks and reports according to your organization’s needs. Leave the box next to **Enable Checks and Reports** unchecked for now.



45. Select **Set up the email server at another time**.



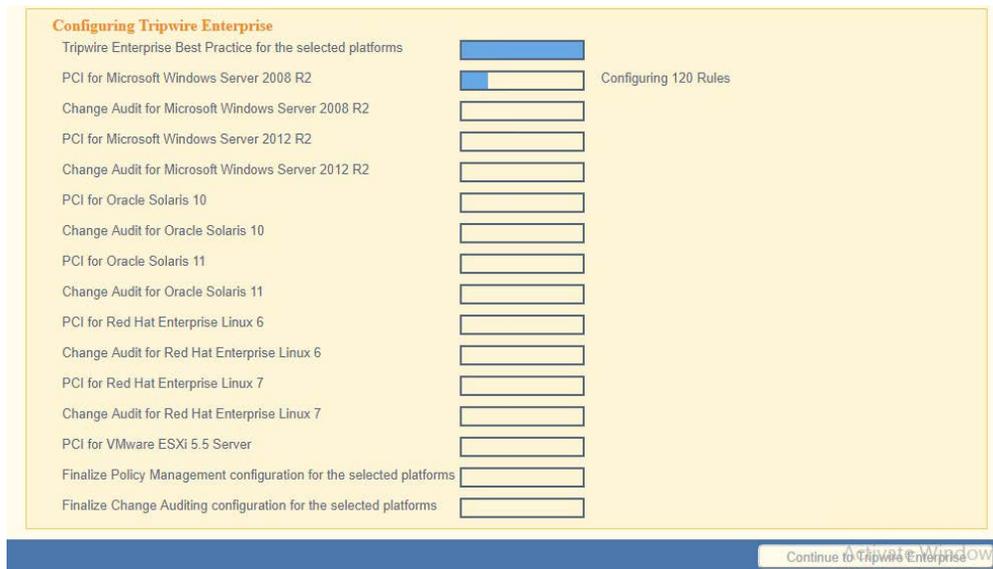
46. Enter a **username** and **password** for a new administrator account for Tripwire Enterprise Console.



47. Click **Preview Configuration**.



48. Click **Apply Configuration**.



49. Click **Continue to Tripwire Enterprise** when the installation finishes.

2.12.2 Install the Axon Bridge

1. Ensure that TCP traffic on port 5670 is allowed through the firewall.
2. Navigate to the Tripwire Enterprise Console installation directory to the `/server/data/config` folder. Copy `bridge_sample.properties` to `bridge.properties`.
3. In the `bridge.properties` file, find the line that says:
`#tw.cap.bridge.registrationPreSharedKey=`
 Remove the “#” character. After the “=” character, enter a **password**. The password has some restrictions, so ensure that it meets the requirements in case the connection fails later.
4. Restart the TE console by running the following command from an administrative command prompt, where `<te_root>` is the TE installation directory:

```
> <te_root>/server/bin/twserver restart
```

2.12.3 Install the Axon Agent (Windows)

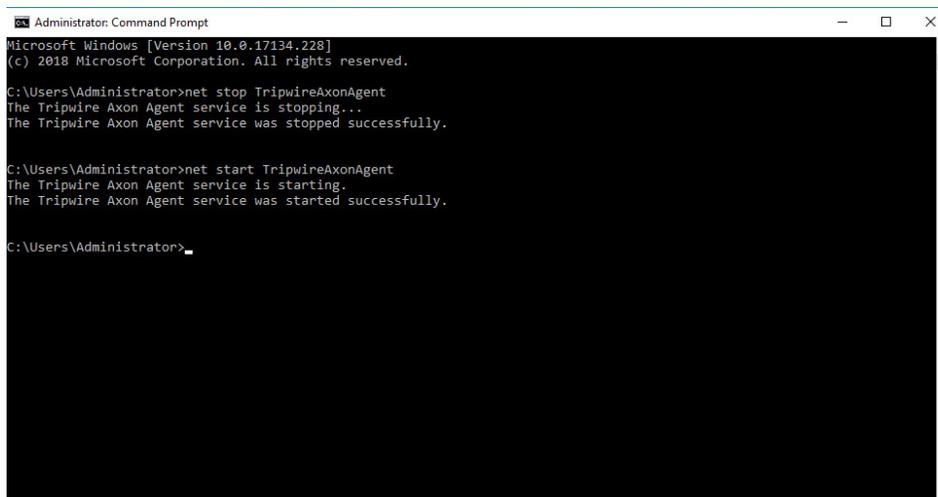
1. Download the Axon Agent zip file from the Tripwire customer website (<https://tripwireinc.force.com/customers>), under the Product Downloads tab.
2. Unzip the file.
3. To begin the installation, double-click the `.msi` file in the extracted folder. Note: No installation wizard will appear; the installation happens automatically.

4. After the Axon Agent is installed, navigate to `C:\ProgramData\Tripwire\agent\config`, and copy `twagent_sample.conf` to `twagent.conf`.

```
#
# HOST based agent configuration:
#   Instead of using a DNS SRV record, the agent may be configured
#   to talk to a specific host, or list of hosts. Lists use a comma separator and
#   can optionally specify a port. The default of port 5670 will be used if a port
#   is not specified.
#
#   Example: host1, host2:5900, 10.123.0.15, [feac:ba80:6fff:93fe]:7582
#
#   The agent may be configured to connect to hosts in a randomized or textual order
#   (default: true)
#
bridge.host=192.168.1.136
#bridge.port=5670
#bridge.randomize.hosts=true
#
```

5. Open `twagent.conf` and find the line that says `bridge.host`. Remove the “#” character, and enter the hostname or IP address of the Axon Bridge server.
6. In a file called `registration_pre_shared_key`, enter the value of the preshared key that was set in the Axon Bridge.
7. Restart the Axon Agent Service by opening a command prompt and running the following commands:

```
> net stop TripwireAxonAgent
> net start TripwireAxonAgent
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net stop TripwireAxonAgent
The Tripwire Axon Agent service is stopping...
The Tripwire Axon Agent service was stopped successfully.

C:\Users\Administrator>net start TripwireAxonAgent
The Tripwire Axon Agent service is starting.
The Tripwire Axon Agent service was started successfully.

C:\Users\Administrator>
```

2.12.4 Install the Axon Agent (Linux)

1. Download the Axon Agent `.tgz` file from the Tripwire customer website (<https://tripwireinc.force.com/customers>), under the Product Downloads tab.
2. To install the software, run the following commands:
RHEL or CentOS: `> rpm -ivh <installer_file>`

Debian or Ubuntu: `> dpkg -i <installer_file>`

3. Navigate to `/etc/tripwire/` and copy **twagent_sample.conf** to **twagent.conf**.
4. Open **twagent.conf** and find the line that says `bridge.host`. Remove the “#” character and enter the hostname or IP address of the Axon Bridge server.
5. In a file called **registration_pre_shared_key.txt**, enter the value of the preshared key that was set in the Axon Bridge.
6. Restart the Axon Agent Service by opening a command prompt and running the following commands:

RHEL or CentOS:

```
> /sbin/service tripwire-axon-agent stop
> /sbin/service tripwire-axon-agent start
```

Debian or Ubuntu:

```
> /usr/sbin/service tripwire-axon-agent stop
> /usr/sbin/service tripwire-axon-agent start
```

2.12.5 Configure Tripwire Enterprise

2.12.5.1 Terminology

Node: a monitored system, such as a file system, directory, network device, database, or virtual infrastructure component

Element: a monitored object, which is a component or property of a node being audited by TE

Element Version: a record of an element’s state at specific points in time. Multiple element versions create a historical archive of changes made to the element.

Rule: A rule identifies one or more elements to the TE Console.

Action: an object that initiates a response to either changes detected by TE or by failures generated from policy tests

Task: a TE operation that runs on a scheduled or manual basis

TE Policy: a measurement of the degree to which elements comply with a policy

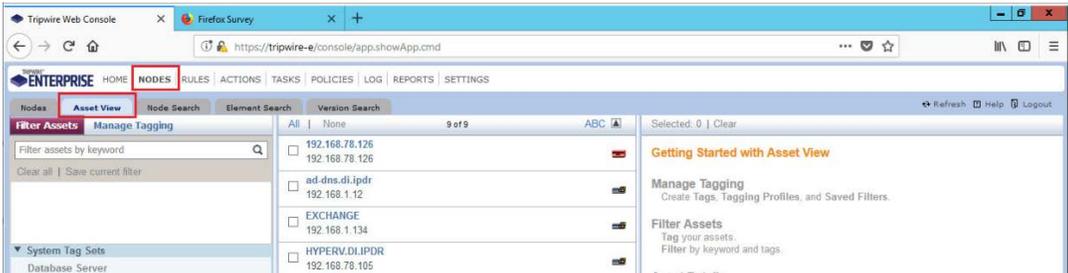
Policy Test: a determination of whether elements comply with the requirements of a policy

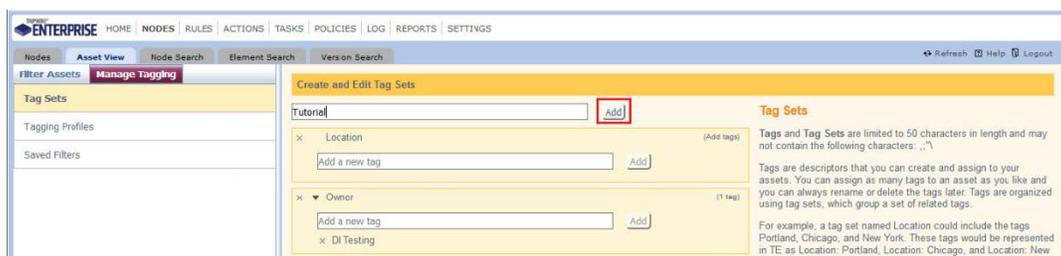
Baseline: the act of creating an element that reflects the current state of a monitored object (also called the **current baseline**). When a node’s baseline is promoted, TE saves the former baseline as a **historic baseline**.

Version Check: a check on monitored objects/elements. It is a comparison of the current state of the element against its already recorded baseline for changes.

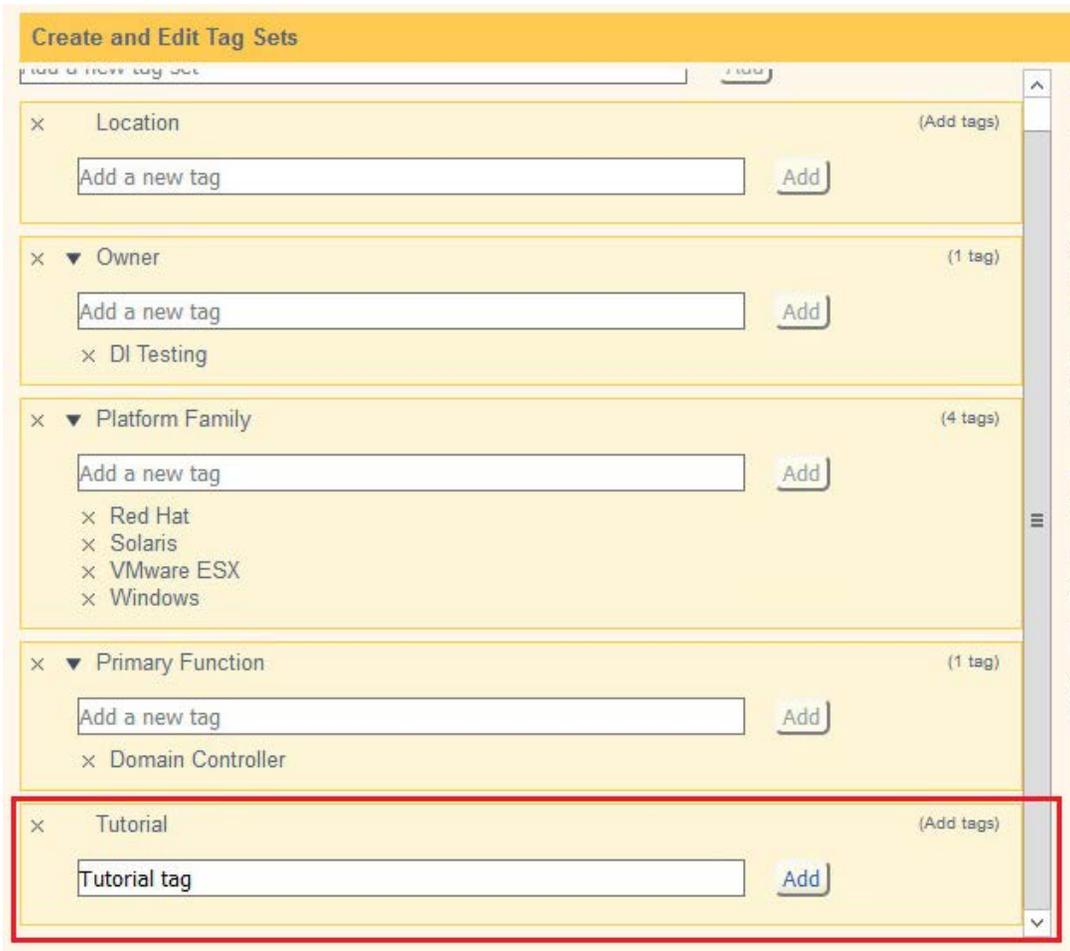
2.12.5.2 Tags

In Tripwire Enterprise, tags can be used to label and target specific nodes. Tags are not required but allow for targeting nodes more granularly than by the operating system. This section describes how to create and assign tags.

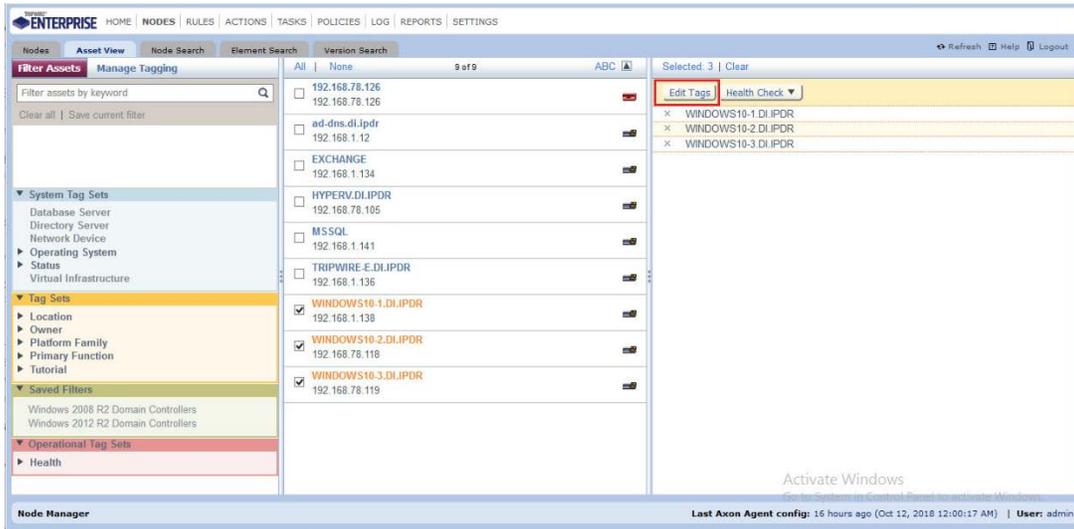
1. Navigate to the TE Console in your browser.
 2. Click **Asset View**.
- 
3. Click the **Manage Tagging** tab.
 4. Enter the name of a tag set, or use one of the four existing ones (Location, Owner, Platform Family, Primary Function). Click **Add** if adding your own tag set.



5. Under the tag set to which you wish to add a tag, enter the name of the tag.

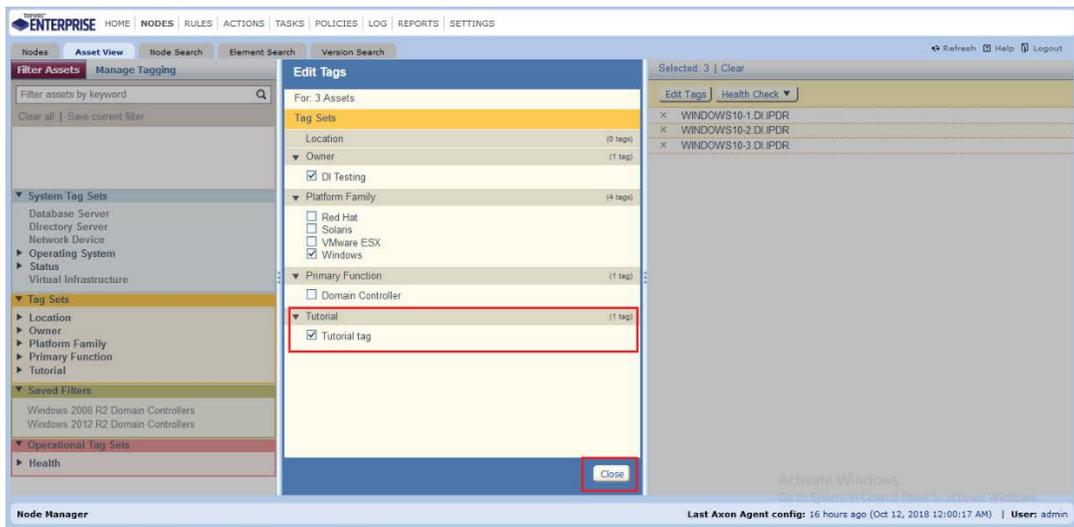


6. Click **Add**.
7. Navigate to **Nodes > Asset View > Filter Assets**.
8. Check the boxes next to the nodes to which you wish to add this tag.



9. Click **Edit Tags**.

10. Check the boxes next to any tags you wish to add to these nodes.



11. Click **Close**.

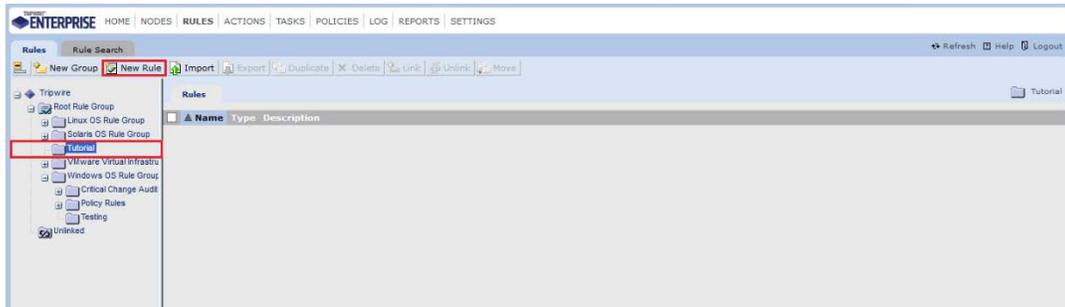
2.12.5.3 Rules

This section describes how to create a rule.

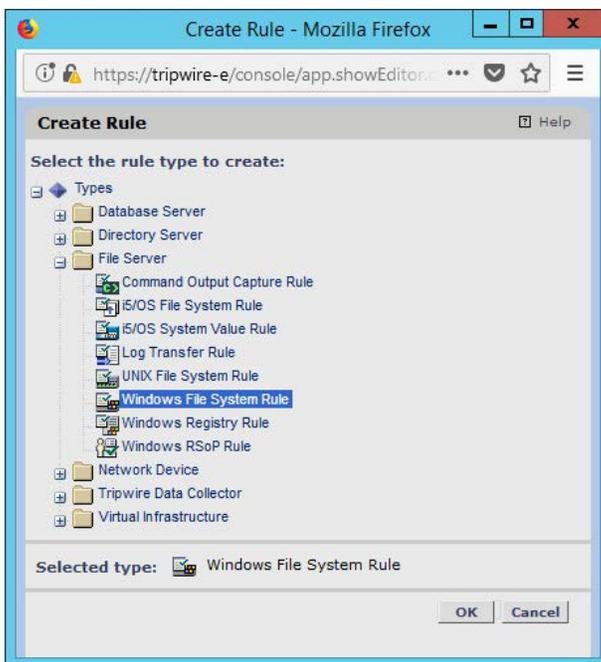
1. Click **Rules**.



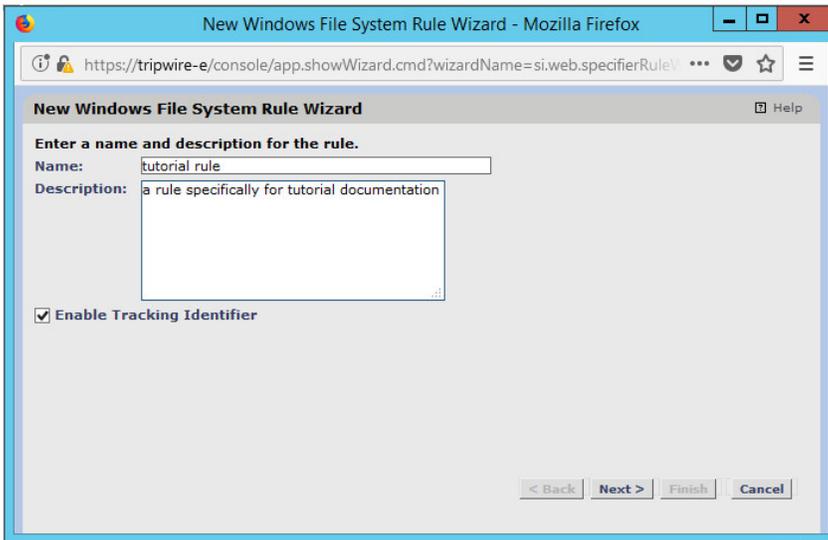
2. Select or create a rule group into which the new rule should be put.



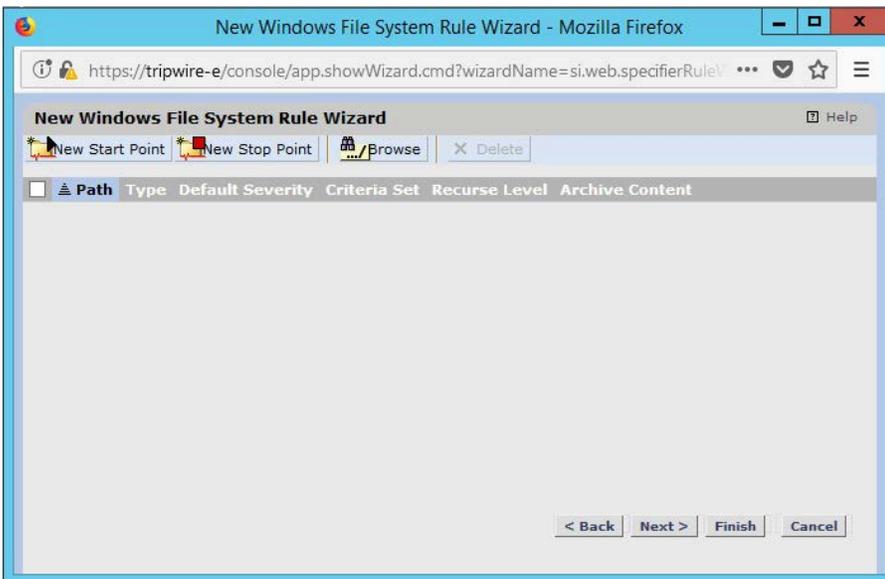
3. Click **New Rule**.
4. Select the type of rule. For monitoring Windows file systems, we choose **Windows File System Rule**.



5. Click **OK**.
6. Enter a **name** and **description** for the rule.



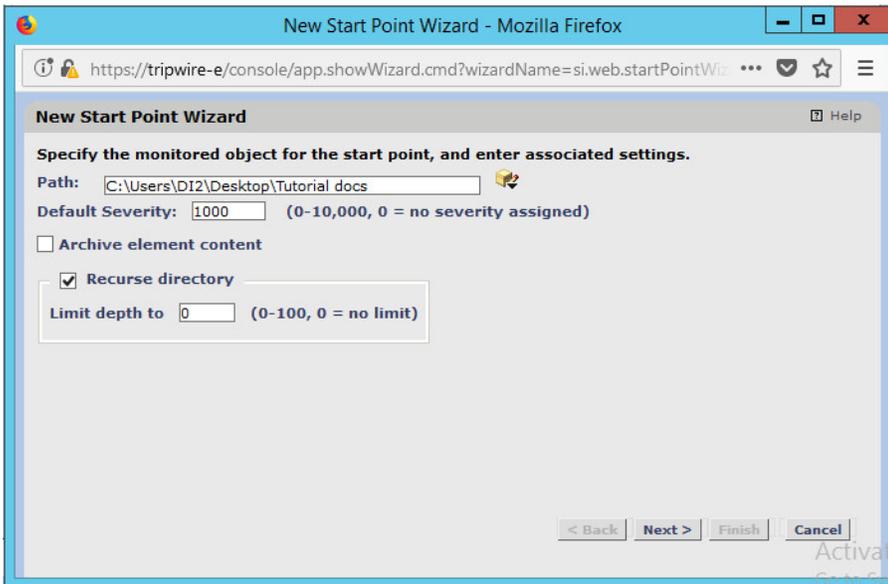
7. Click **Next**.



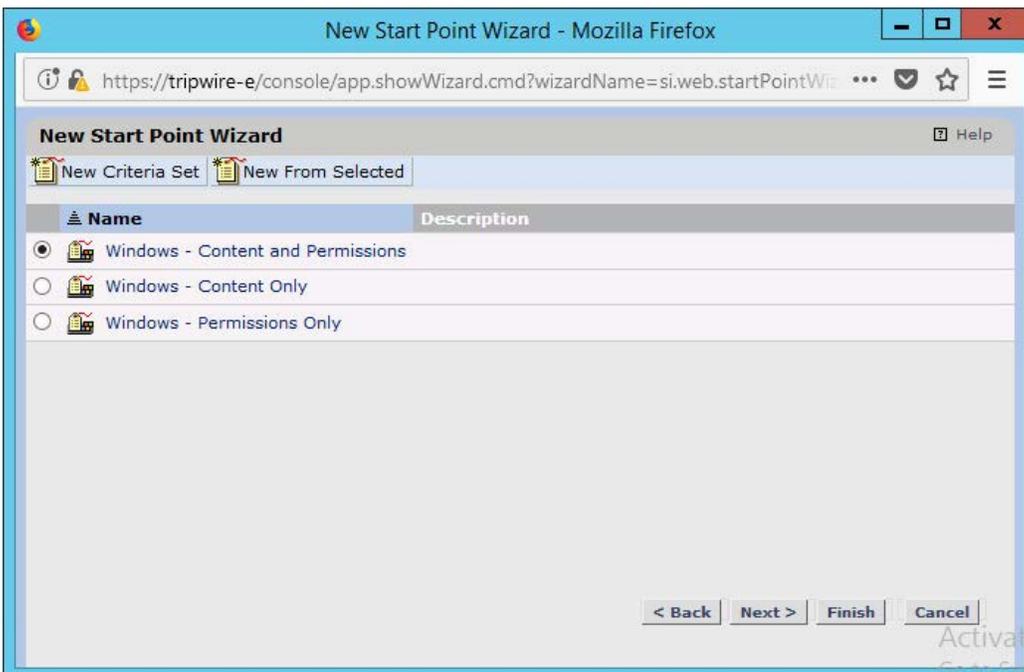
8. Click **New Start Point**.

9. For **Path**, enter a directory that represents the scope of the scan. It can be limited to the documents folder or be wide enough to encompass all the files on a system. Note that the latter will take much longer to scan.

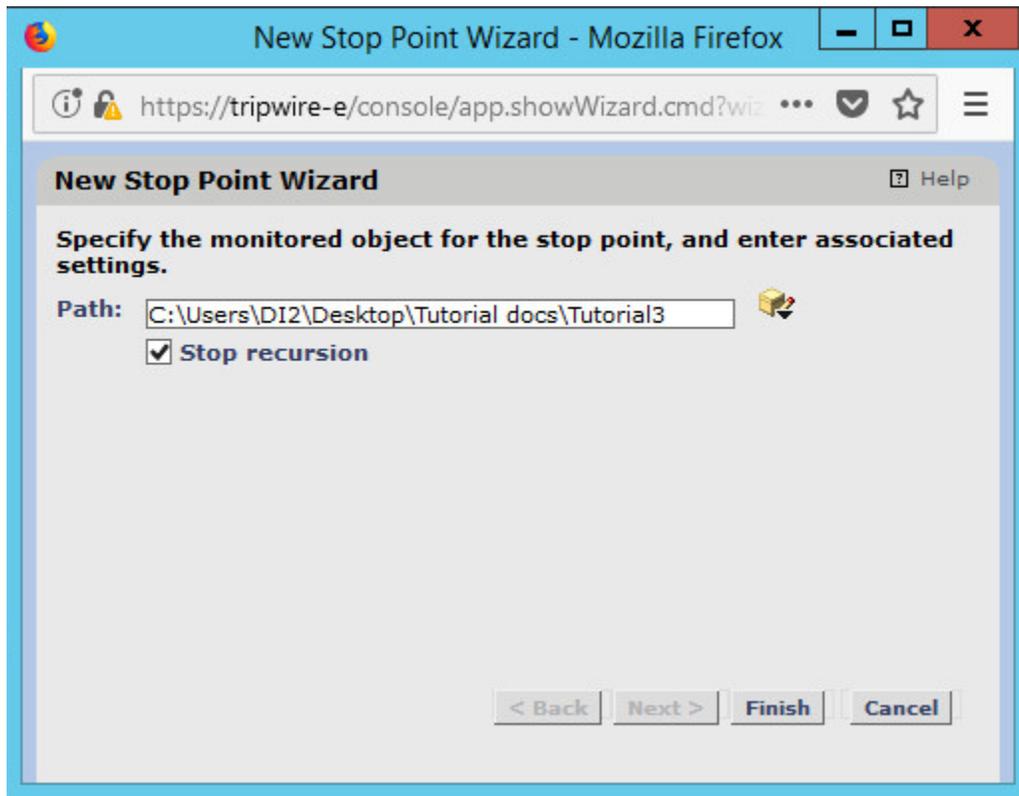
10. Check the box next to **Recurse directory** if you also wish to scan all subfolders.



11. Click **Next**.
12. Select **Windows Content and Permissions**.



13. Click **Finish**.
14. Click **New Stop Point**.
15. Enter the path of any folders or files that should not be included in the scan, and indicate whether they should end the recursion.



16. Click **Finish**.
17. Click **Next**.
18. Click **Next**.
19. Click **Finish**.

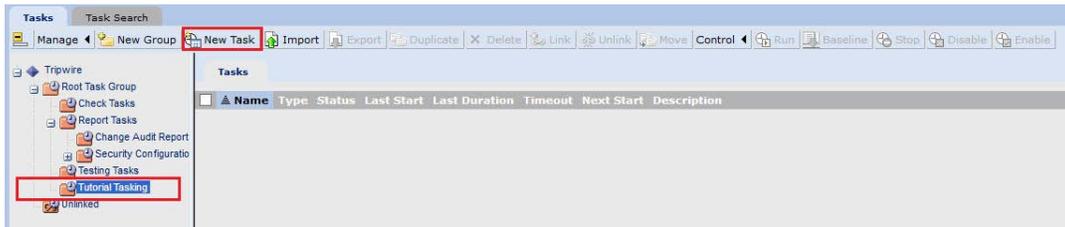
2.12.5.4 Tasks

This section describes how to create a task on a schedule. These tasks can also be run manually if necessary.

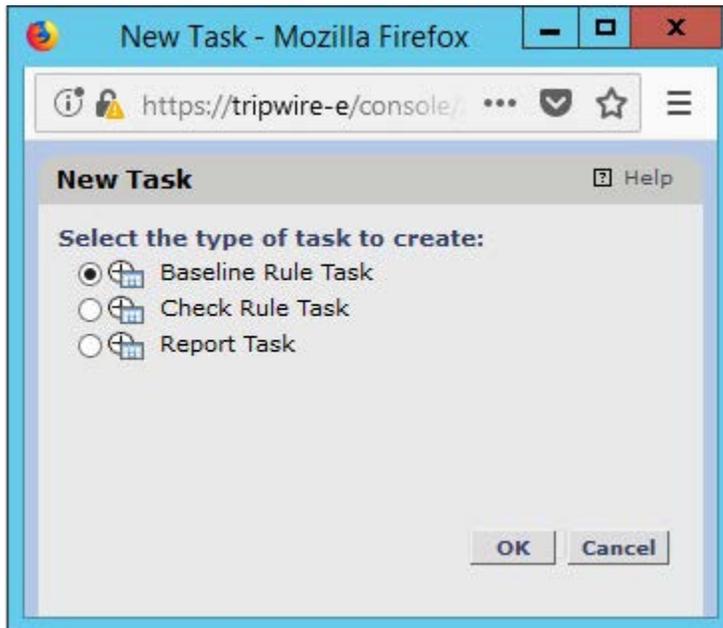
1. Click **Tasks**.



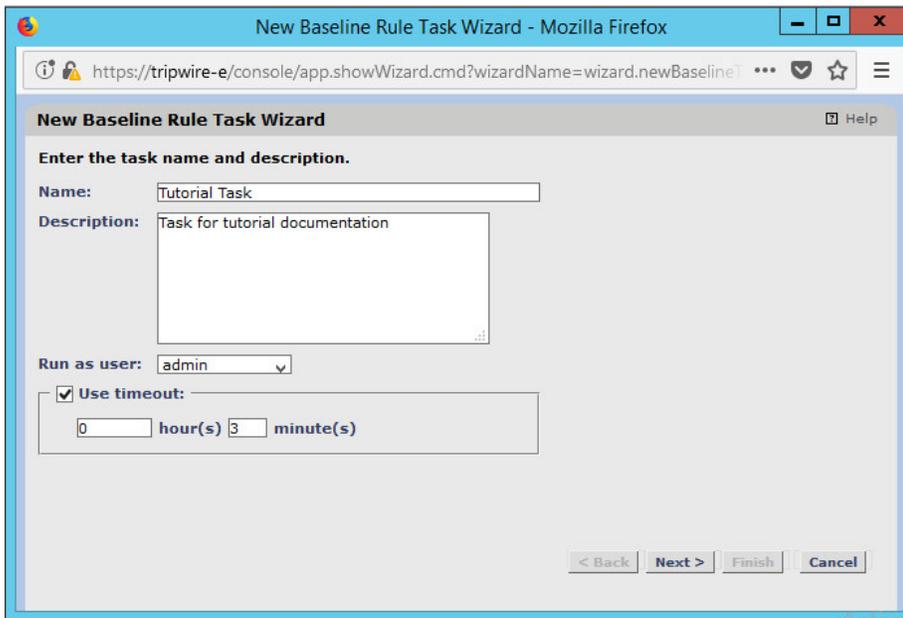
2. Select a folder for a new task, or create one.



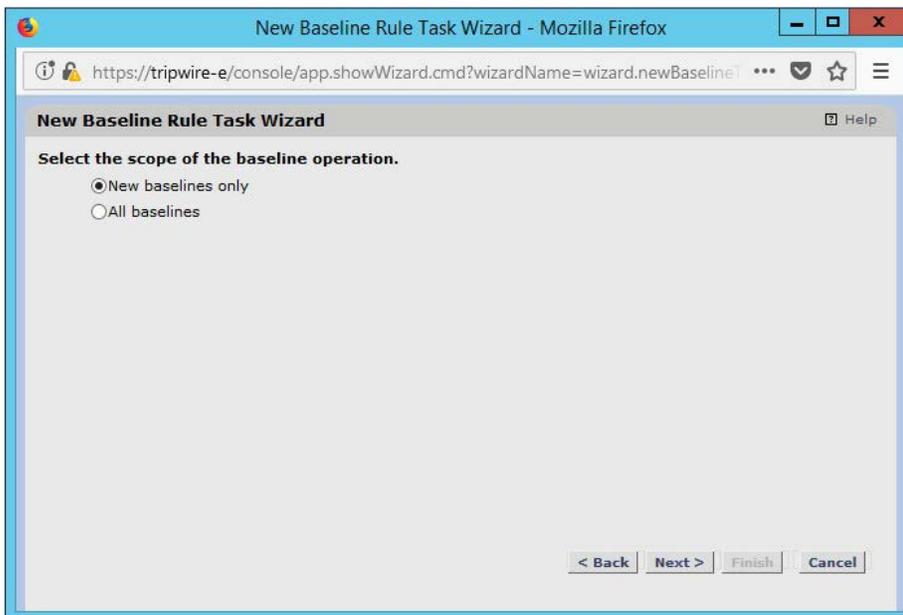
3. Click **New Task**.
4. Select **Baseline Rule Task** or **Check Rule Task**. (Note: Both are needed—baseline creates the initial state of the monitored object, and check updates the state and reports any changes.)



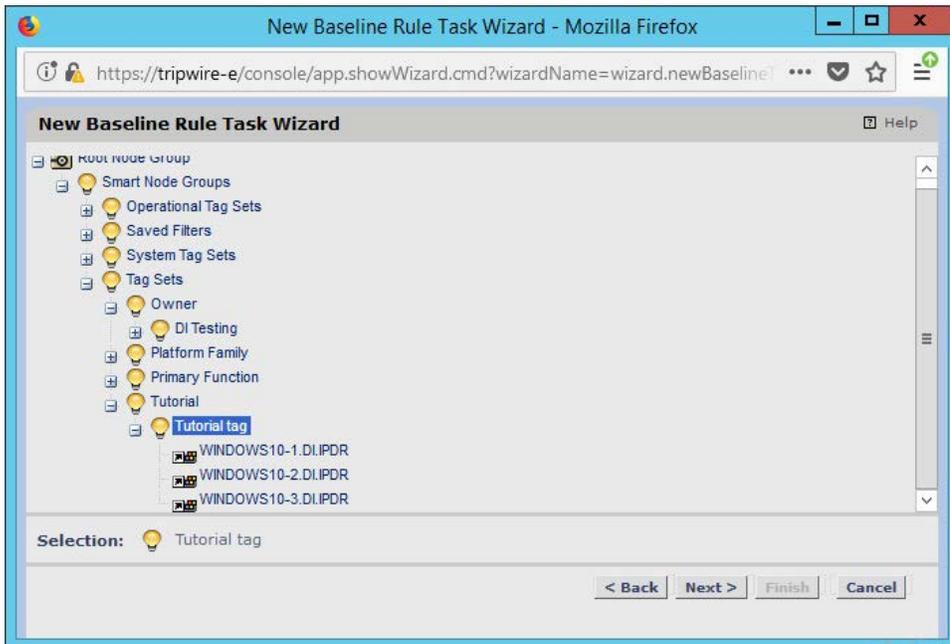
5. Click **OK**.
6. Enter a **name** and **description** for the task.



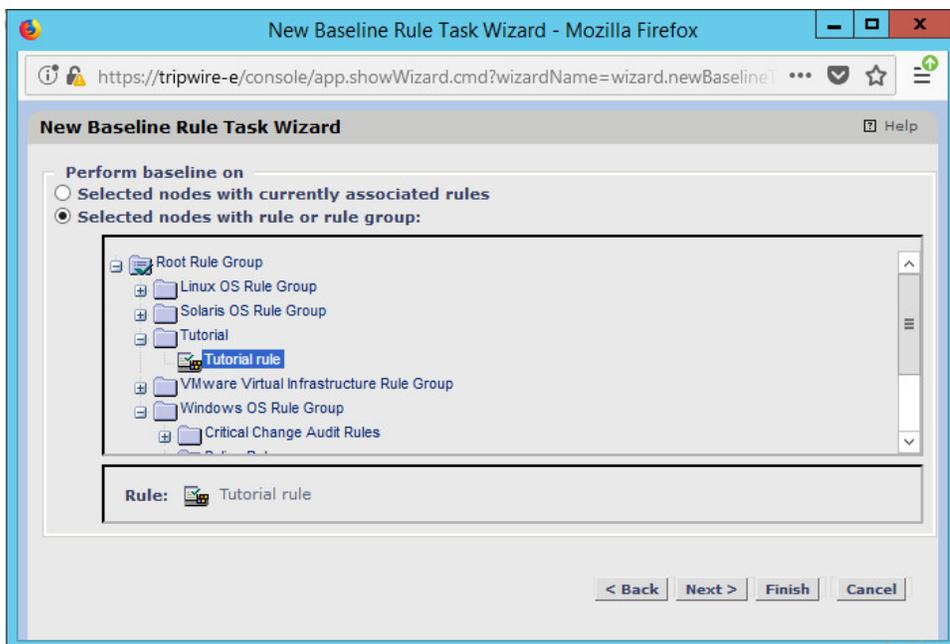
7. Click **Next**.
8. Select whether you want all baselines to be updated or to only create new baselines.



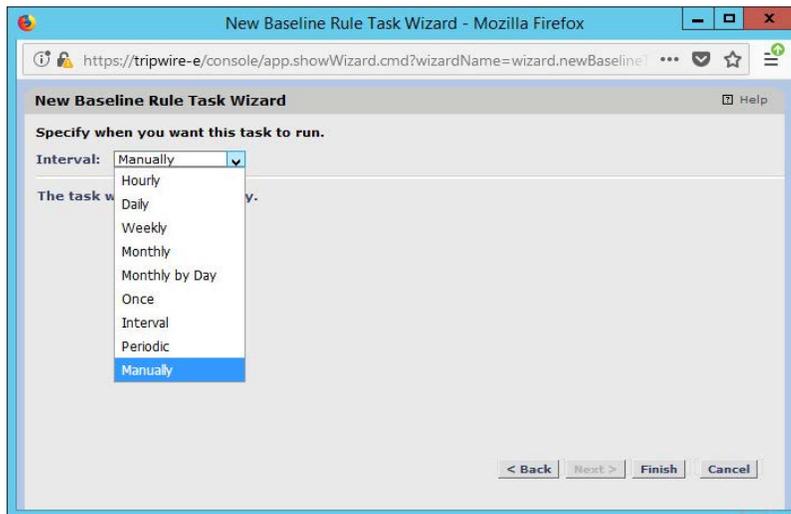
9. Click **Next**.
10. Select the systems to be included in the task. You can use tags or select by operating system (or other defaults).



11. Click **Next**.
12. Select the rule created earlier.



13. Click **Next**.
14. Set the schedule of this task according to your organization's needs.



15. Click **Finish**.

2.13 Tripwire Log Center

2.13.1 Install Tripwire Log Center Manager

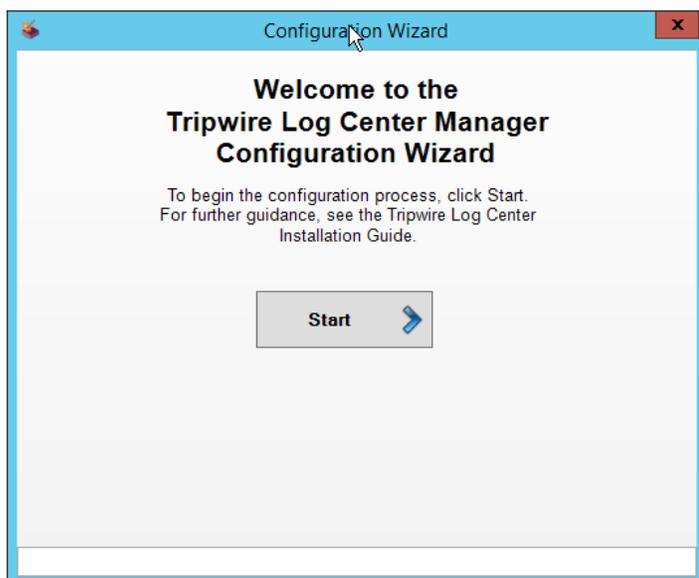
See the *Tripwire Log Center 7.3.1 Installation Guide*, which should accompany the installation media, for instructions on how to install **Tripwire Log Center**. Use the **Tripwire Log Center Manager** installer.

Notes:

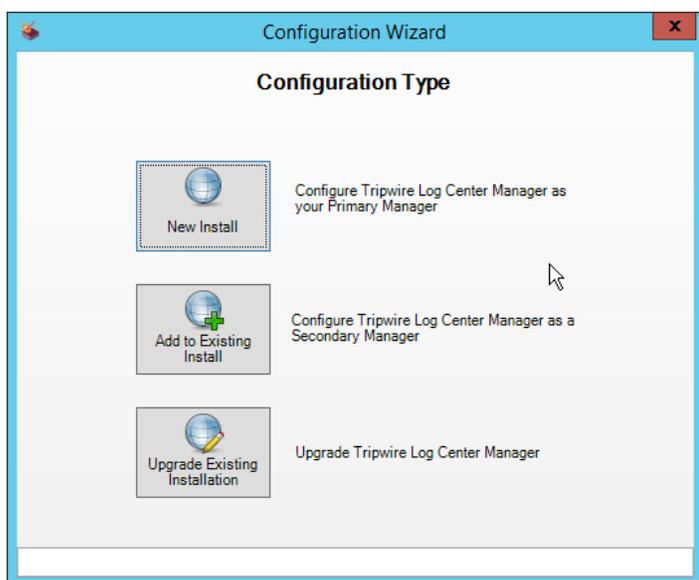
- a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise**.
- b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
- c. .NET Framework 3.5 is required for this installation—install this from the Server Manager.
- d. You may need to unblock port 9898 on your firewall for the Tripwire Enterprise agents.
- e. Do not install PostgreSQL if you wish to use a database on another system—this guide will use a local PostgreSQL database, however.
- f. When it finishes installing, there should be a configuration wizard (see below for configuration steps).

2.13.2 Configure Tripwire Log Center Manager

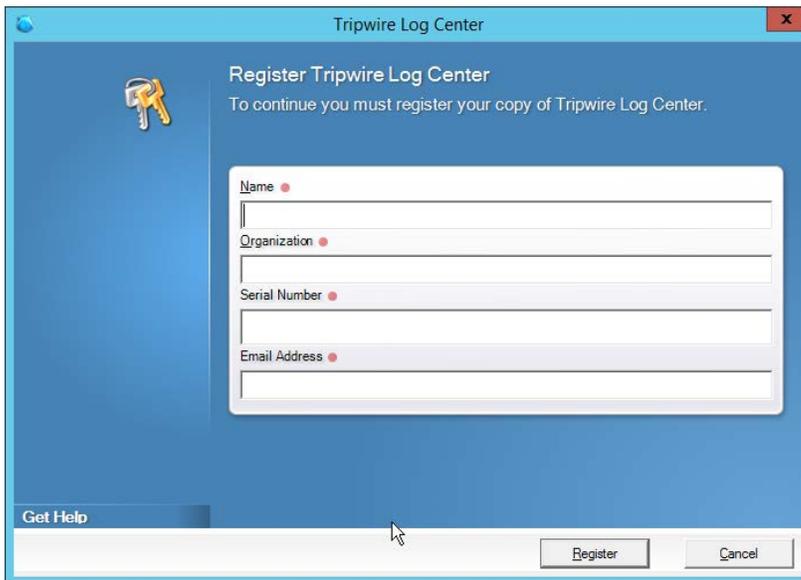
1. The configuration wizard should start after the installation is complete.



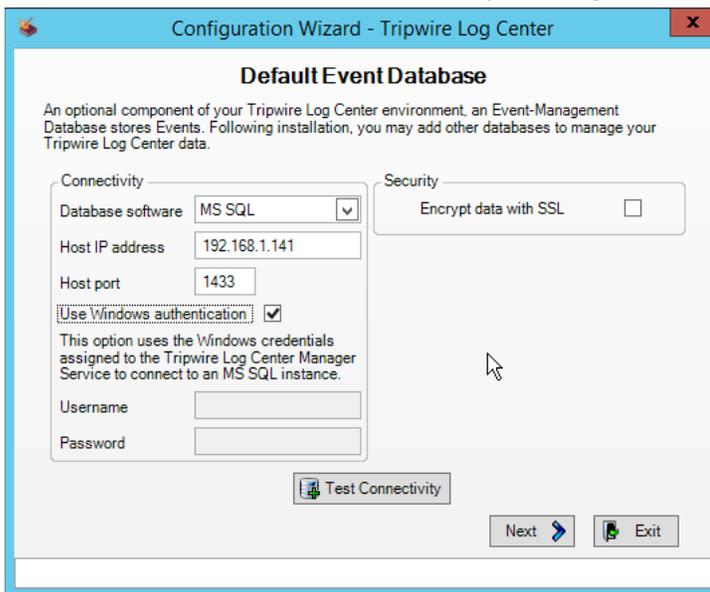
2. Click **Start**.



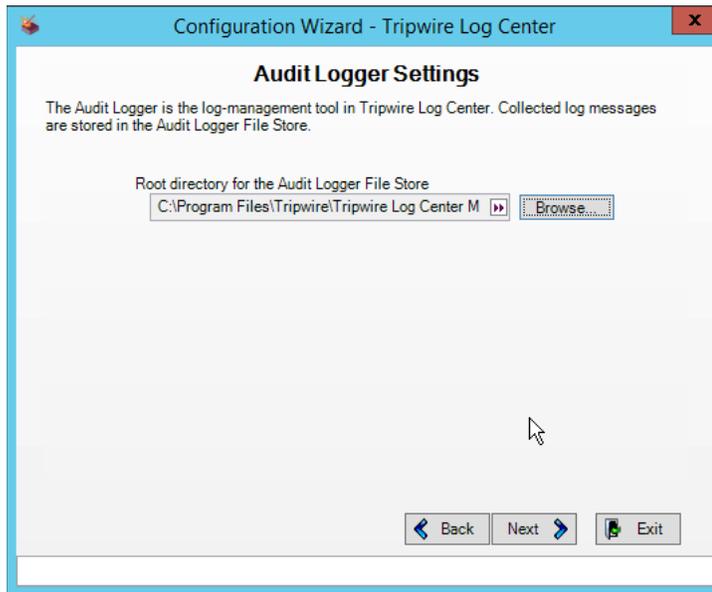
3. Click **New Install**.
4. Enter the registration details for your **Tripwire Log Center** license.



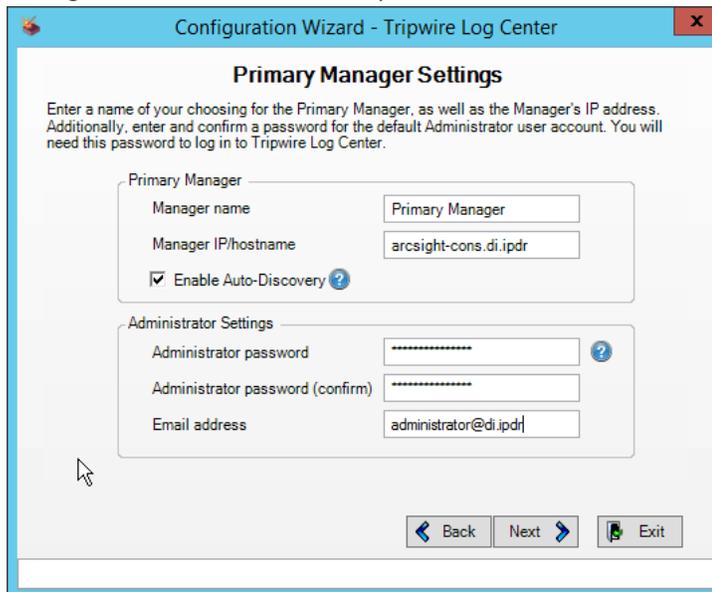
5. Click **Register**.
6. Enter details about the database that **Tripwire Log Center** should use.



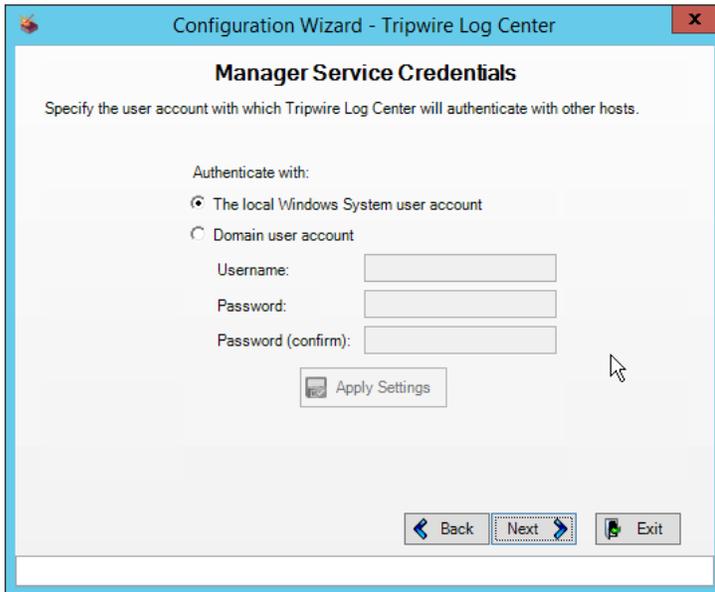
7. Click **Next**.
8. Select a directory in which to store log messages, such as C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT.



9. Click **Next**.
10. Enter a **password** and an **email**.
11. Change the IP to a hostname if preferred.

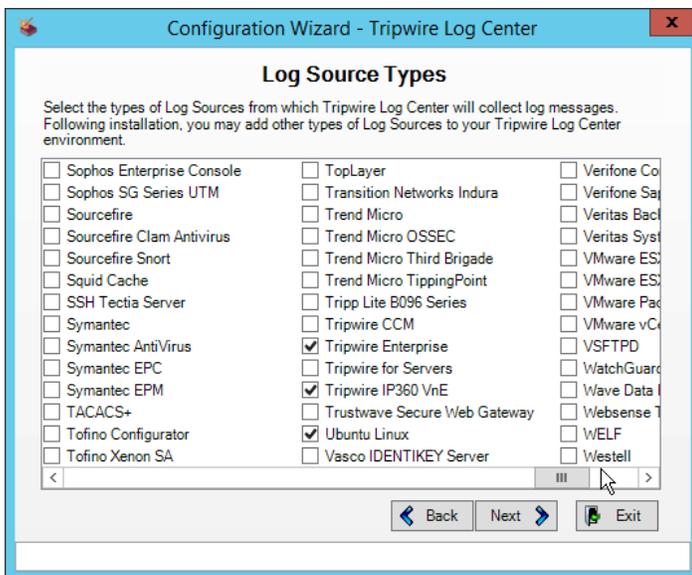


12. Click **Next**.

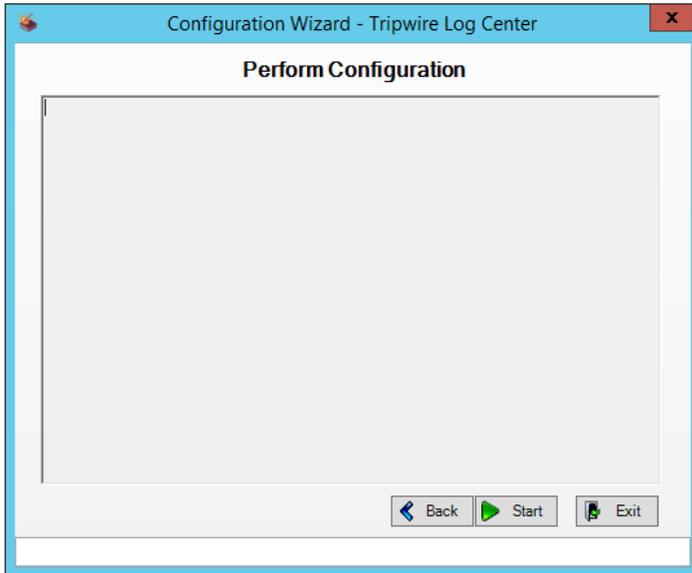


13. Click **Next**.

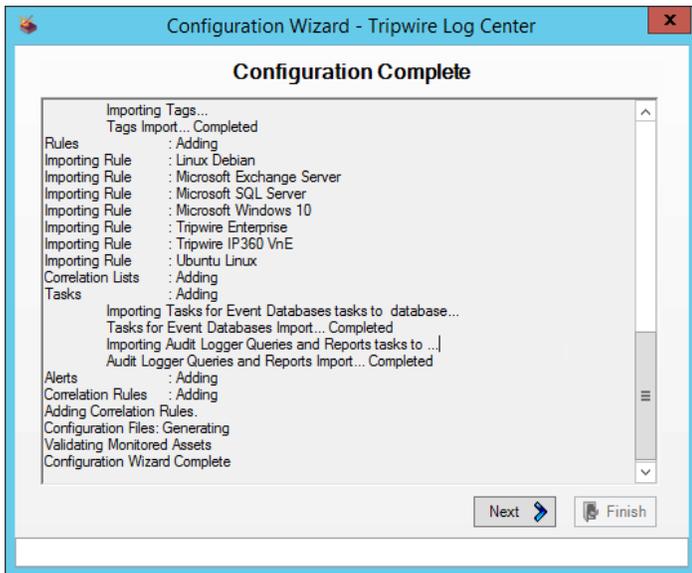
14. Select any log sources that you expect to collect with **Tripwire Log Center**. Examples: Tripwire Enterprise, Microsoft Windows 10, Tripwire IP360 VnE, Linux Debian, Ubuntu Linux, Microsoft Exchange, Microsoft SQL Server.



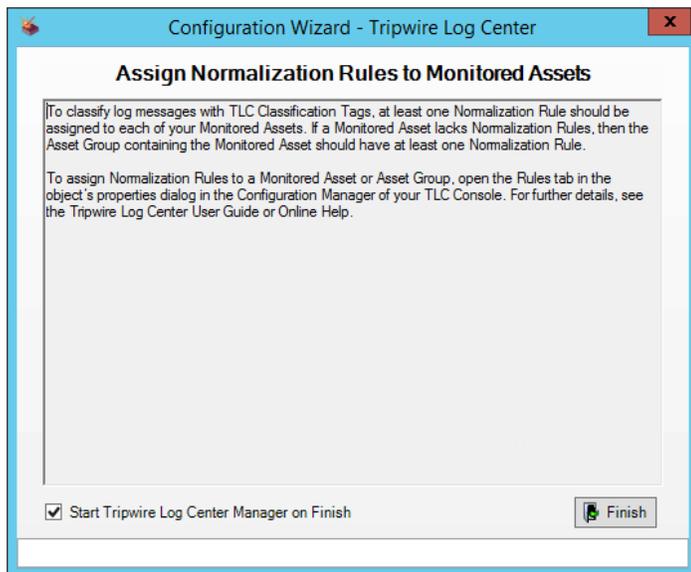
15. Click **Next**.



16. Click **Start**.



17. Click **Next**.



18. Click **Finish**.

2.13.3 Install Tripwire Log Center Console

Chapter 4 of the *Tripwire Log Center 7.3.1 Installation Guide* details installation of the **Tripwire Log Center Console**. Use the **Tripwire Log Center Console** installer.

You can install this on the same machine as the Tripwire Log Center Manager, if desired.

2.14 Cisco Web Security Appliance

This section details installation and some configurations for the Cisco Web Security Appliance (WSA). It assumes the use of the WSA virtual machine.

2.14.1 Network Configuration

1. Log in to WSA by using the default **username** and **password** (admin/ironport).
2. Use the command `sethostname` to set the hostname of the machine.
3. Use the command `dnsconfig` to set the DNS server. Enter **SETUP** when prompted, and then enter DNS information specific to your organization's needs.
4. Use the command `interfaceconfig` to set the IP of the machine. Enter **EDIT** when prompted, and then enter IP information specific to your organization's needs.
5. Use the command `passwd` to change the default password of the machine.

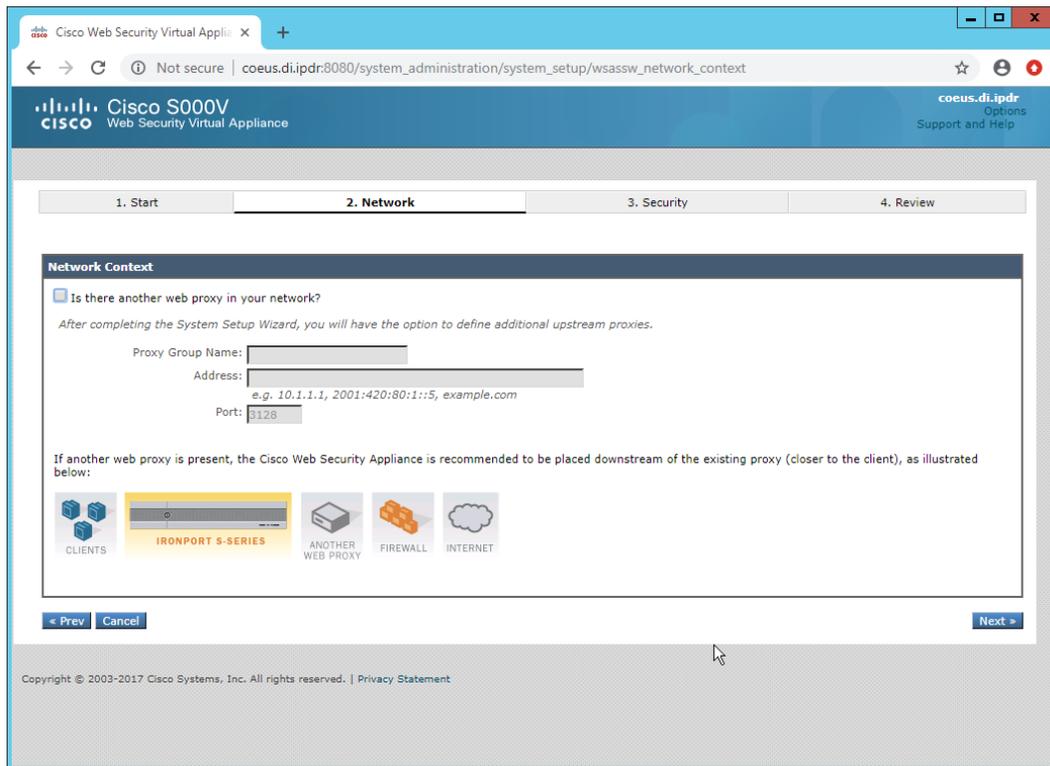
6. Use the command `commit` to commit all of these changes.
7. Use the command `reboot` to reboot the machine.
8. Use the command `loadlicense` to either paste the license file contents or select a license file uploaded via FTP. You can enable FTP in the `interfaceconfig` command.
9. You should be prompted at the console to visit a web page in the browser, usually `http://<ip_address>:8080`. The setup wizard will be here.

2.14.2 System Setup

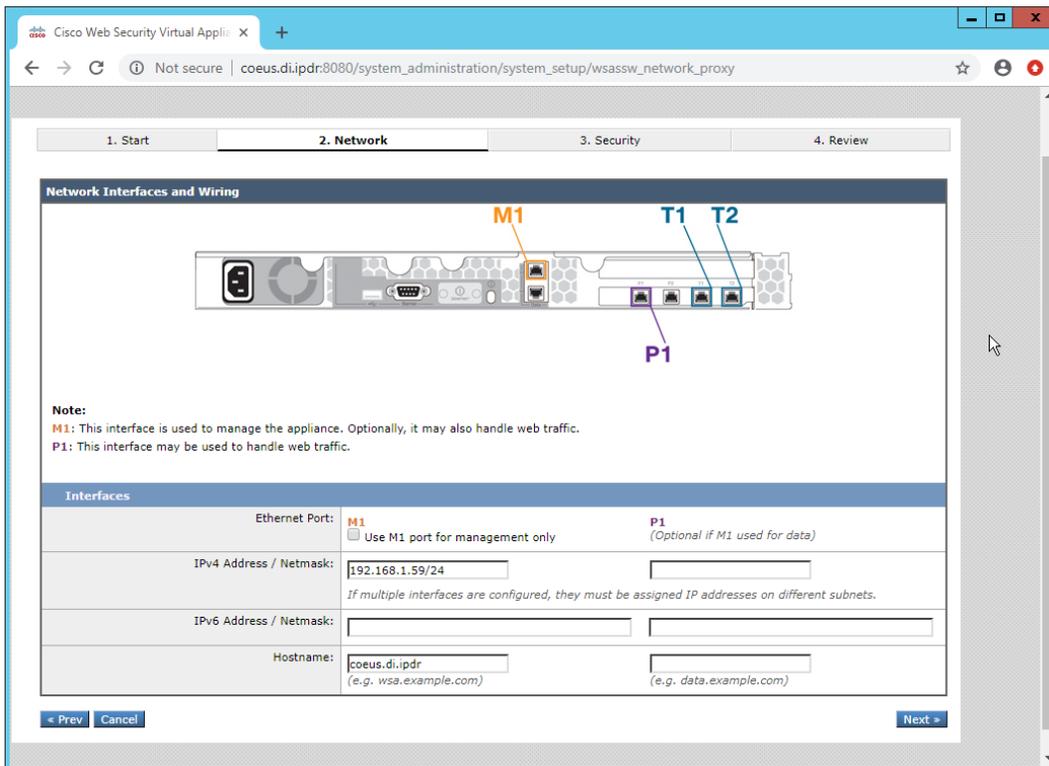
1. In the web console, click **System Administration > System Setup Wizard**.
2. Verify that the hostname matches the desired hostname.
3. Enter the desired **DNS servers**.
4. Enter a **time server** if desired.
5. Select the time zone.
6. Select **Standard** for an on-premises setup.

The screenshot shows the Cisco S000V Web Security Virtual Appliance System Setup Wizard. The wizard is at the '2. Network' step. The 'System Settings' section includes: Default System Hostname: coeus.di.ipdr; DNS Server(s): Use these DNS Servers (192.168.1.12); NTP Server: time.dmz.nccoe.nist.gov; Time Zone: Region: America, Country: United States, Time Zone / GMT Offset: Eastern Time (New_York). The 'Appliance Mode' section has 'Standard' selected. Navigation buttons: < Prev, Cancel, Next >.

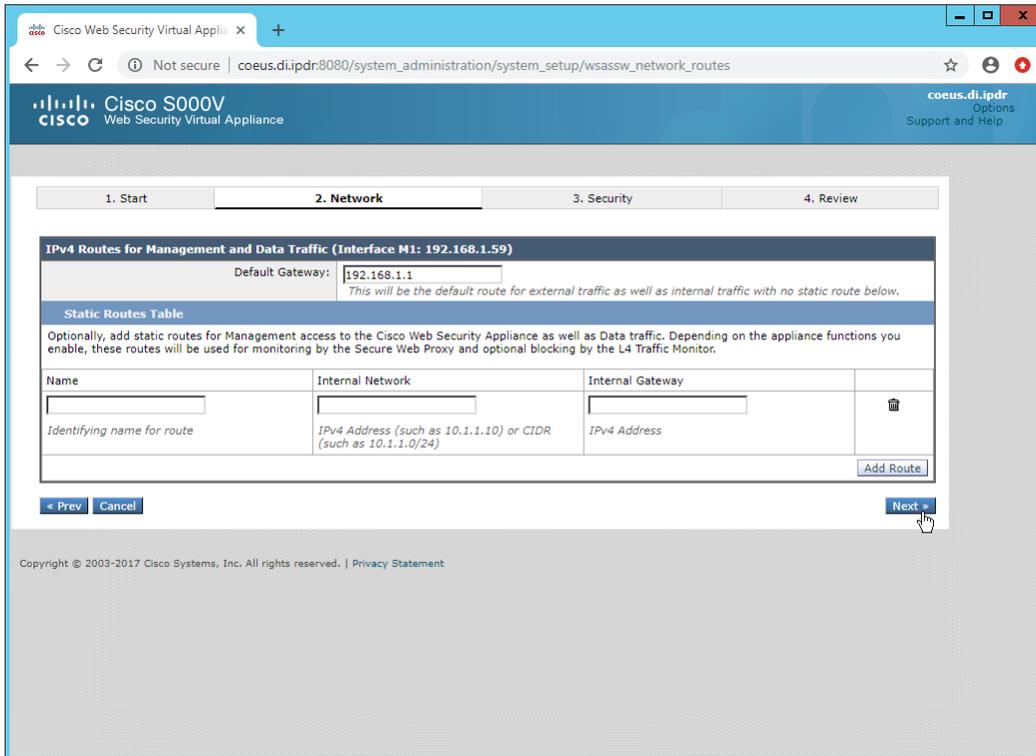
7. Click **Next**.



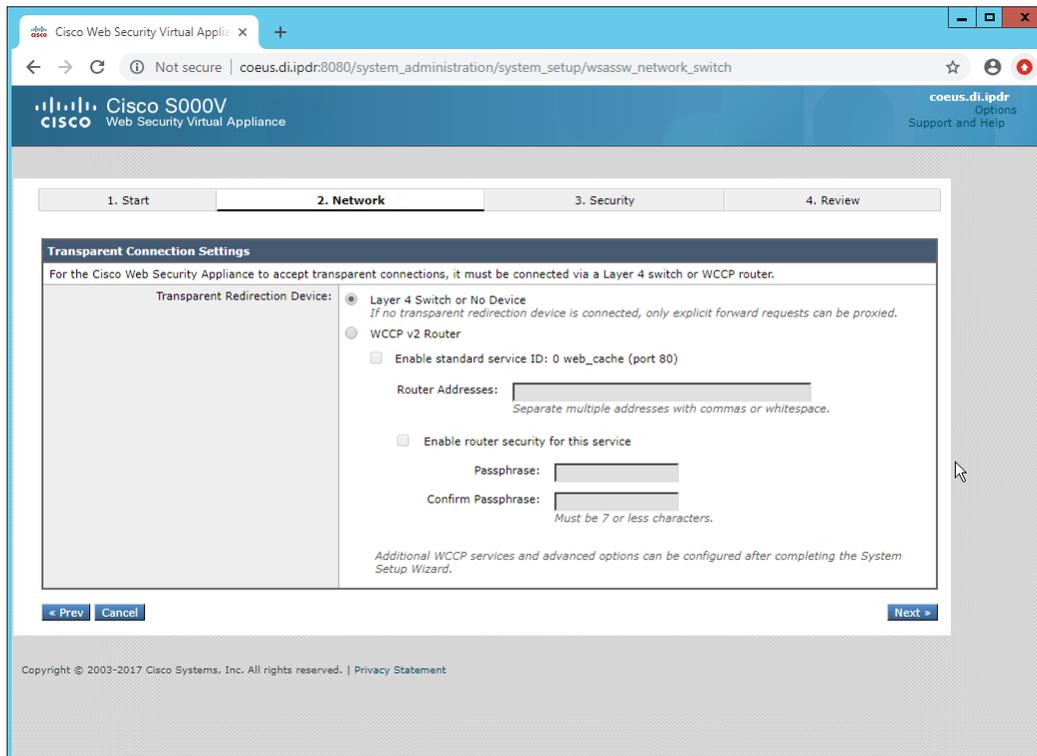
8. Click **Next**.
9. Verify that the interface is correctly configured.



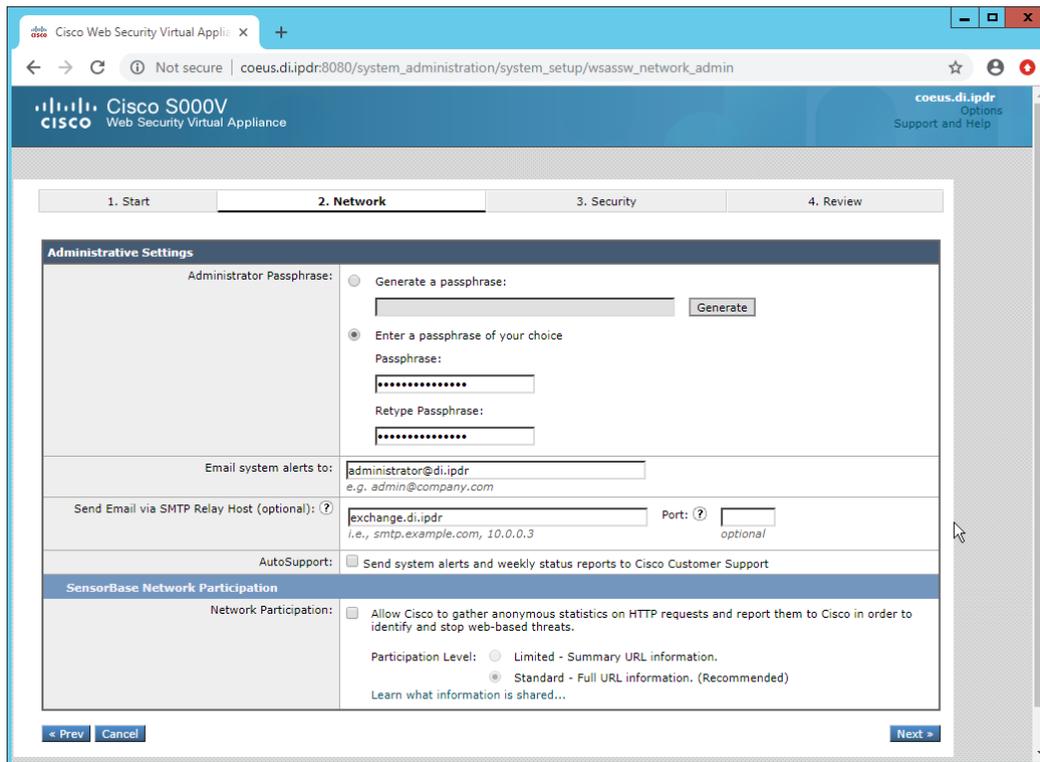
10. Click **Next**.



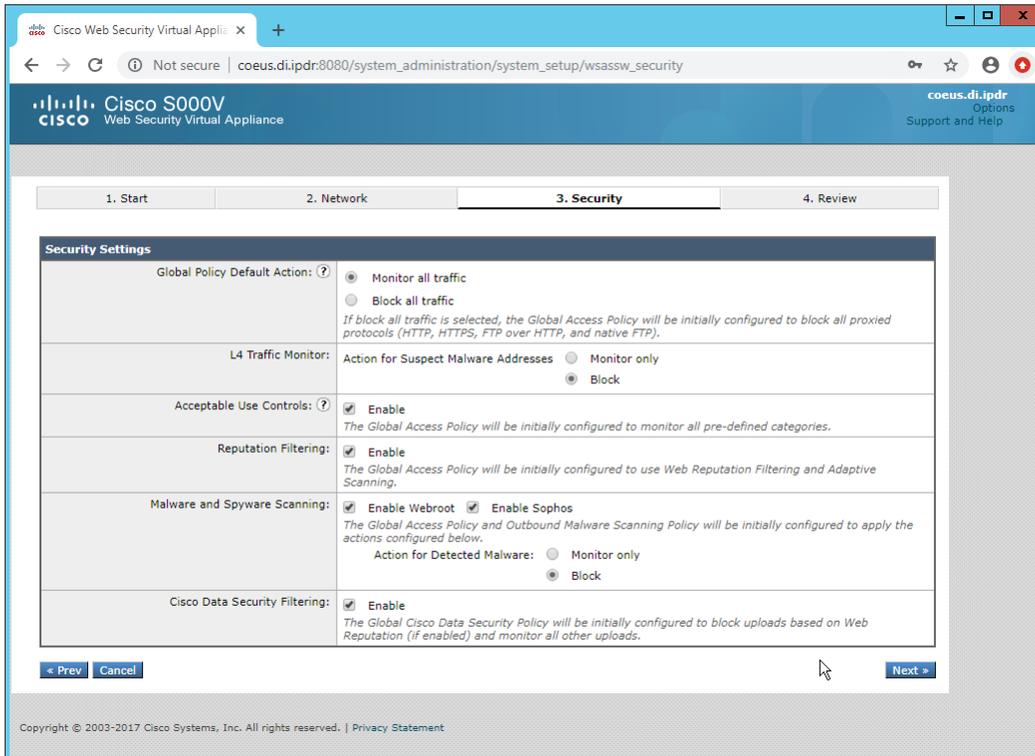
13. Click **Next**.



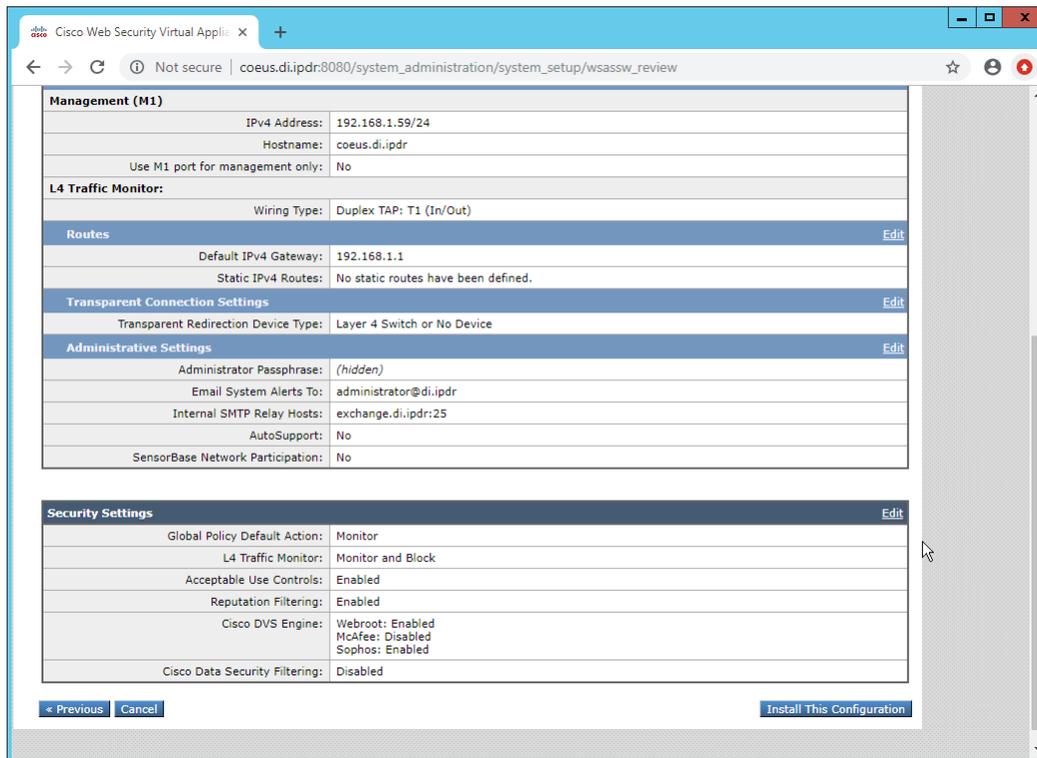
14. Click **Next**.
15. Set a **passphrase** for the administrator.
16. Enter an **email address** to which alerts should be sent.
17. Enter the **hostname** of the email server.
18. Decide whether to forward alerts and reports to Cisco Customer Support, as well as whether to share anonymous statistics based on the needs of your organization.



19. Click **Next**.
20. Select **Monitor All Traffic**.
21. Select **Block** for **Action for Suspect Malware Addresses**.
22. Select **Block** for **Action for Detected Malware**.
23. Configure the rest of the malware policy according to your organization's needs.



24. Click **Next**.



25. Click **Install This Configuration**.

2.14.3 Using WSA to Proxy Traffic

Cisco WSA is intended to act as a proxy between clients and the internet, to prevent malicious traffic and software from reaching the client systems before they can do any damage. The appliance must have a way of intercepting traffic from the clients to the internet.

To achieve this, we used a Proxy Auto Config (PAC) file on our DNS server (Windows 2012 DNS), and this section details how to set up a simple PAC file to forward all traffic to WSA. This may not be an ideal setup for every environment, particularly in environments that use an external DNS server.

2.14.3.1 Creating a PAC File

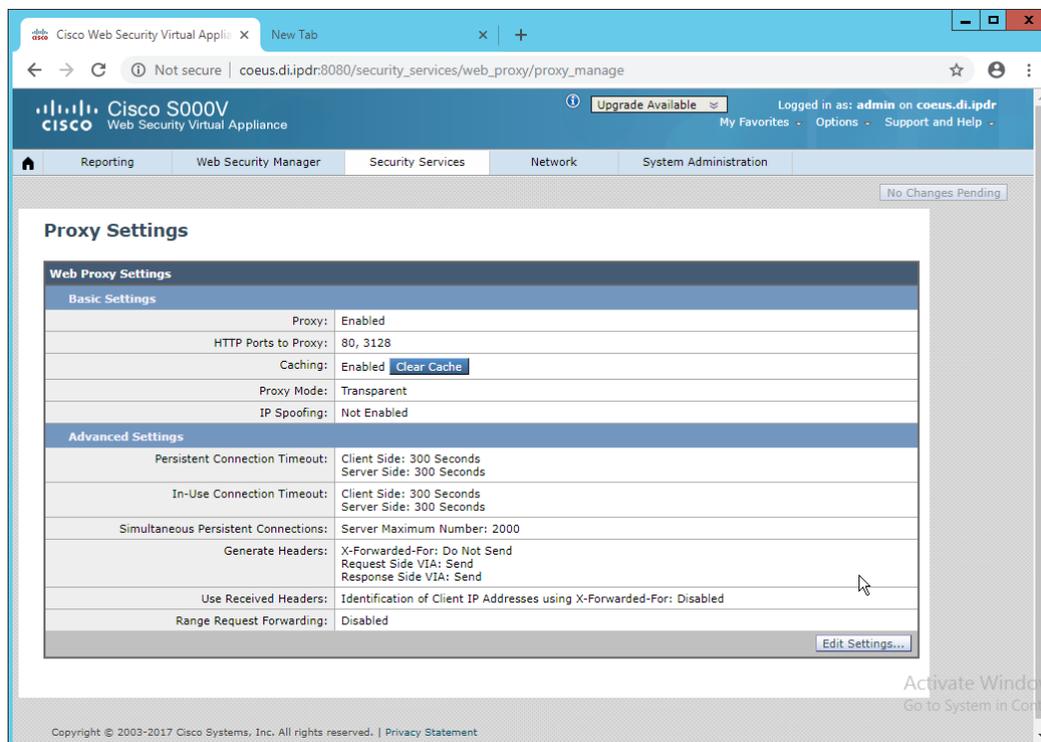
1. Create a new file named **wpad.dat** and enter the following JavaScript function:

```
function FindProxyForURL(url, host) {  
    return "PROXY coeus.di.ipdr:3128";  
}
```

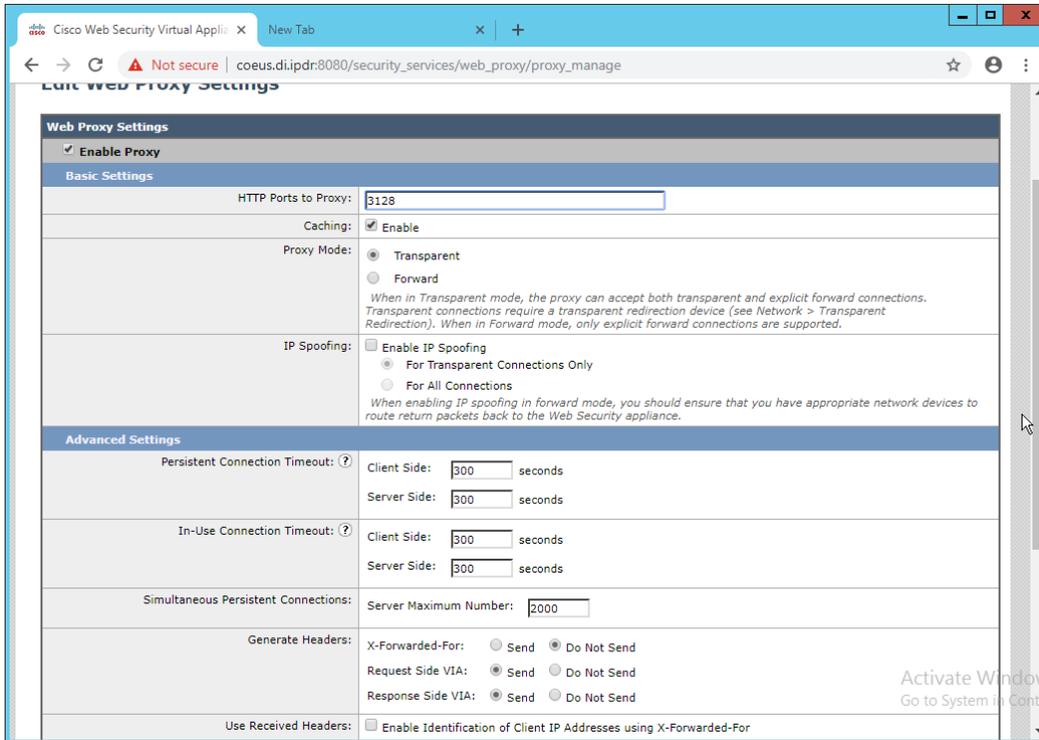
This is the most basic template for a proxy that directs all traffic to the host coeus.di.ipdr. The return value of this function can take the form "PROXY <hostname1>; PROXY <hostname2>" if you wish to have fail-over proxies, or "DIRECT" to not use any proxy. You can also add rules to allow certain types of traffic through the proxy or direct them to other proxies. For more information, see <https://findproxyforurl.com>.

For the purposes of our setup, we will simply direct all traffic to Cisco WSA, but be aware that PAC files can be more complex and designed according to the needs of the organization.

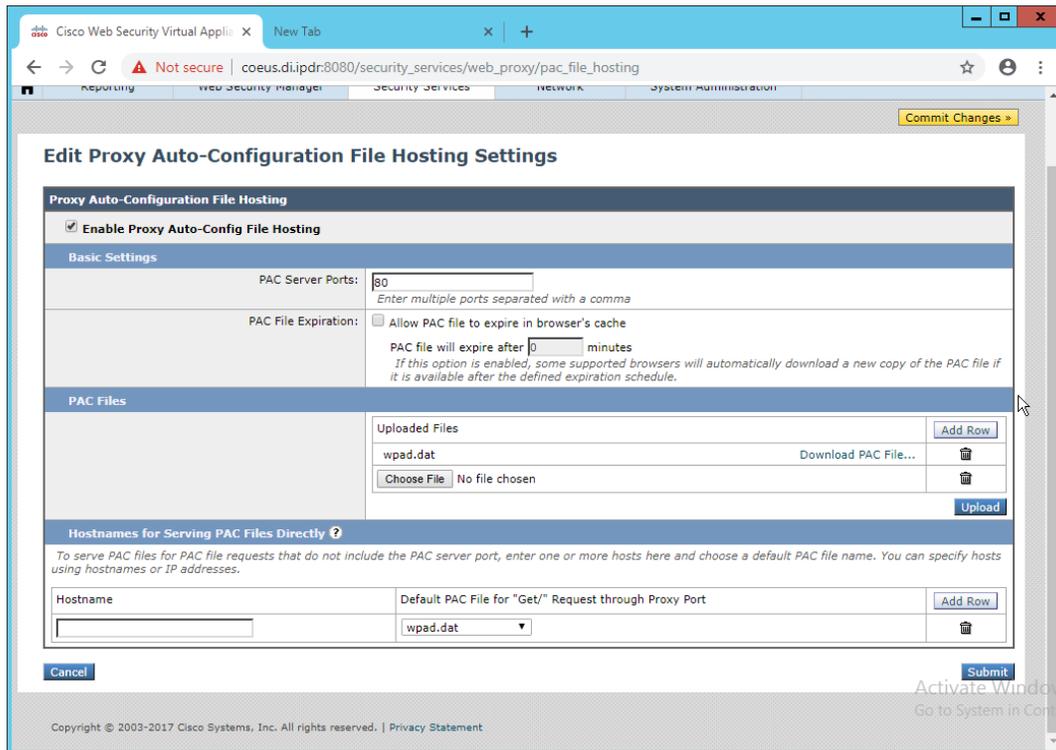
2. In the web console, navigate to **Security Services > Web Proxy**.



3. Click **Edit Settings**.
4. Remove port 80 from **HTTP Ports to Proxy** (ensure that **3128** is in this field).



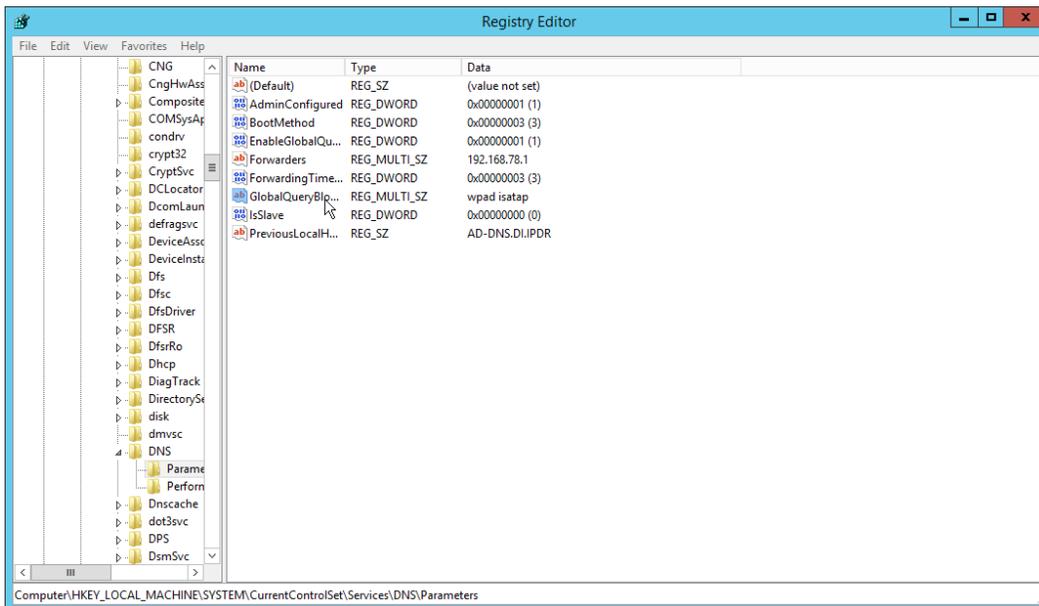
5. Click **Submit**.
6. Navigate to **Security Services > PAC File Hosting**.
7. Click **Enable and Edit Settings**.
8. Under **PAC Files**, click **Choose File**.
9. Select the **wpad.dat** file created earlier.
10. Click **Open**.
11. Click **Upload**.
12. Enter **80** for **PAC Server Ports**.



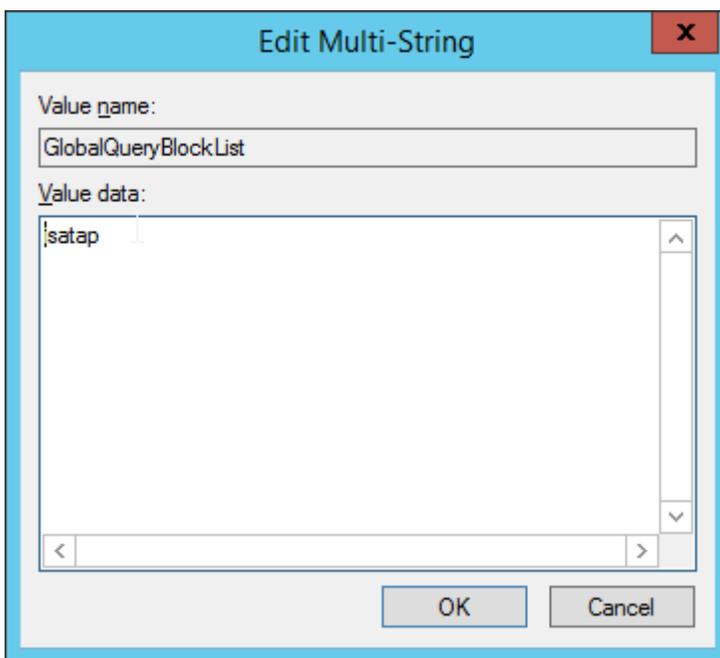
13. Click **Submit**.
14. Click **Commit Changes**.
15. Enter a comment if desired.
16. Click **Commit Changes**.

2.14.3.2 Setting Up Web Proxy Auto Discovery (WPAD)

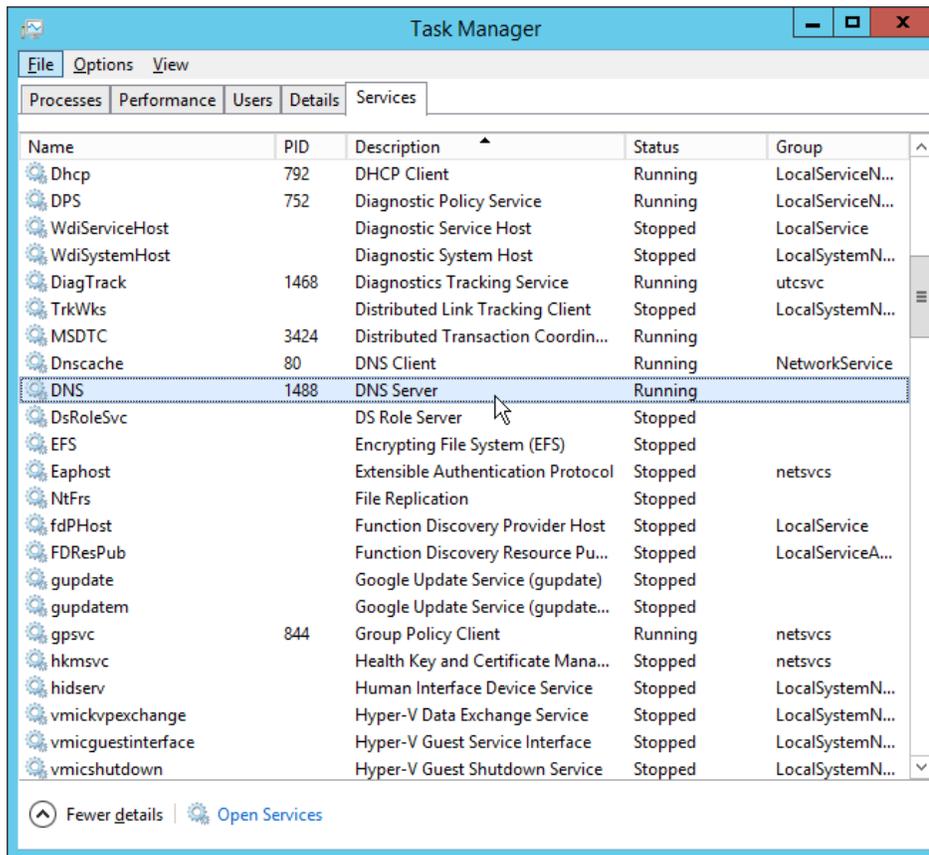
1. On the DNS server, open **regedit.exe**.
2. Navigate to **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > DNS > Parameters**.



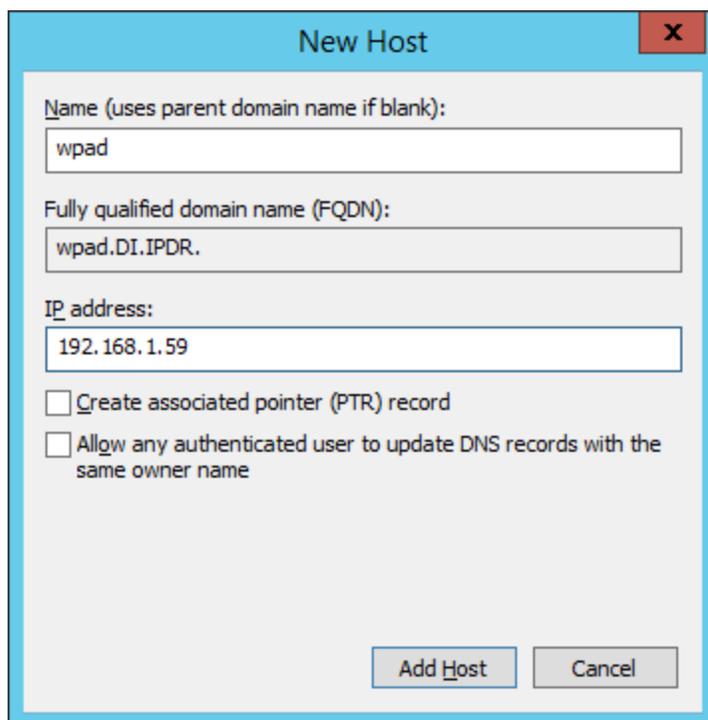
3. Double-click **GlobalQueryBlockList**.
4. Remove wpad from the list but leave isatap on the list.



5. Click **OK**.
6. Open **Task Manager**.
7. Click **Services**.



8. Restart the **DNS Server** service.
9. Open **DNS Manager**.
10. Right-click on your enterprise's domain, and click **New Host (A or AAAA)**.
11. Enter **wpad** for **Name**.
12. Enter the **IP address** of WSA.



13. Click **Add Host**.

This will set up the WPAD proxy file as the default proxy—so browsers that are using “Automatically detect settings” for their proxy setting will find this file. Be aware that this is not sufficient for a secure setup but will allow you to quickly test the proxy’s functionality.

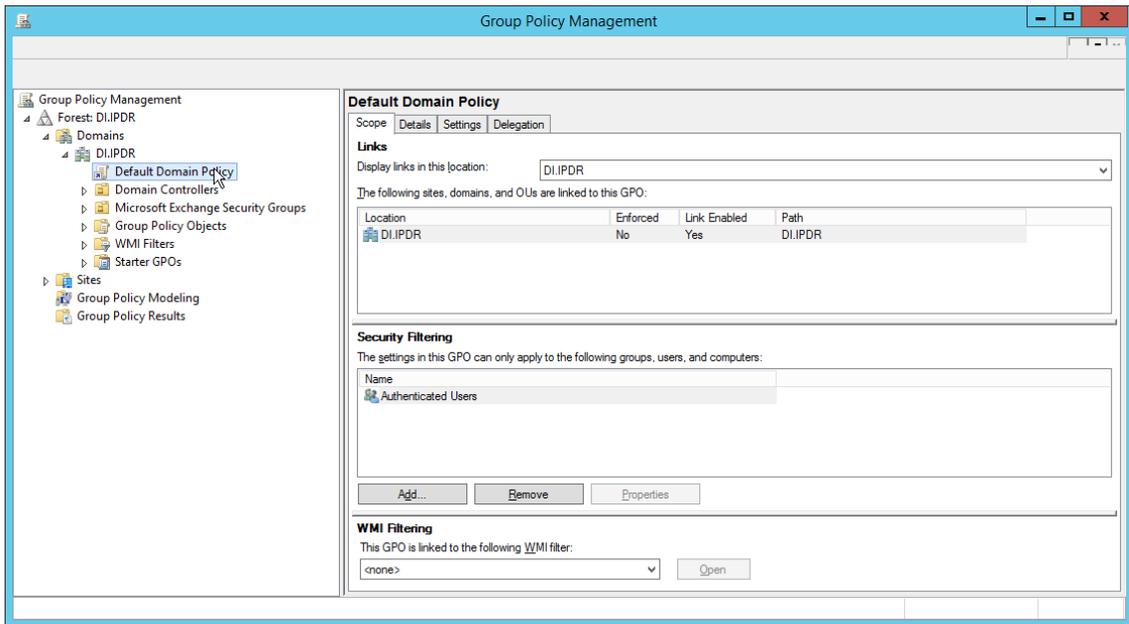
2.14.3.3 Configure Group Policy to Use Explicit Proxy

Note that, at this point, WPAD is vulnerable to an attack where the server hosting WPAD is brought down and the browser automatically attempts to find the next WPAD proxy, which may be controlled by an attacker.

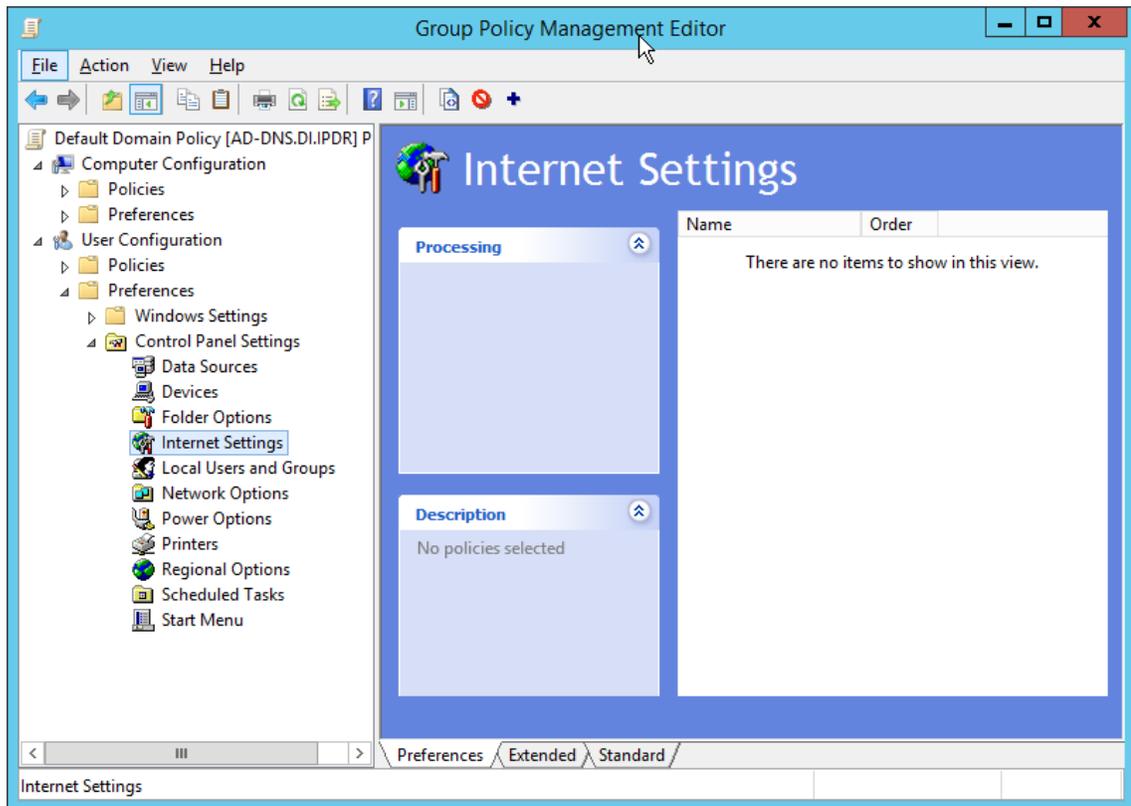
To mitigate this vulnerability, we explicitly point to this proxy file with any browsers used by clients. For Internet Explorer and Google Chrome, it is sufficient to change group policy in Active Directory to direct the change across all systems.

For Mozilla Firefox, see this link (<https://support.mozilla.org/en-US/kb/connection-settings-firefox>) for configuration, including how to set it to “Use system proxy settings.”

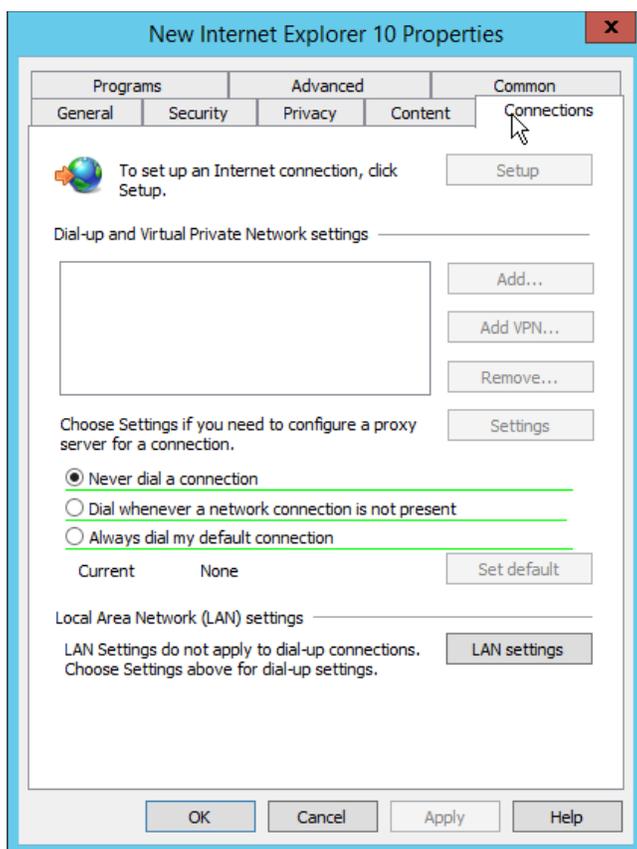
1. In **Group Policy Management**, right-click the **Default Domain Policy** and click **Edit**.



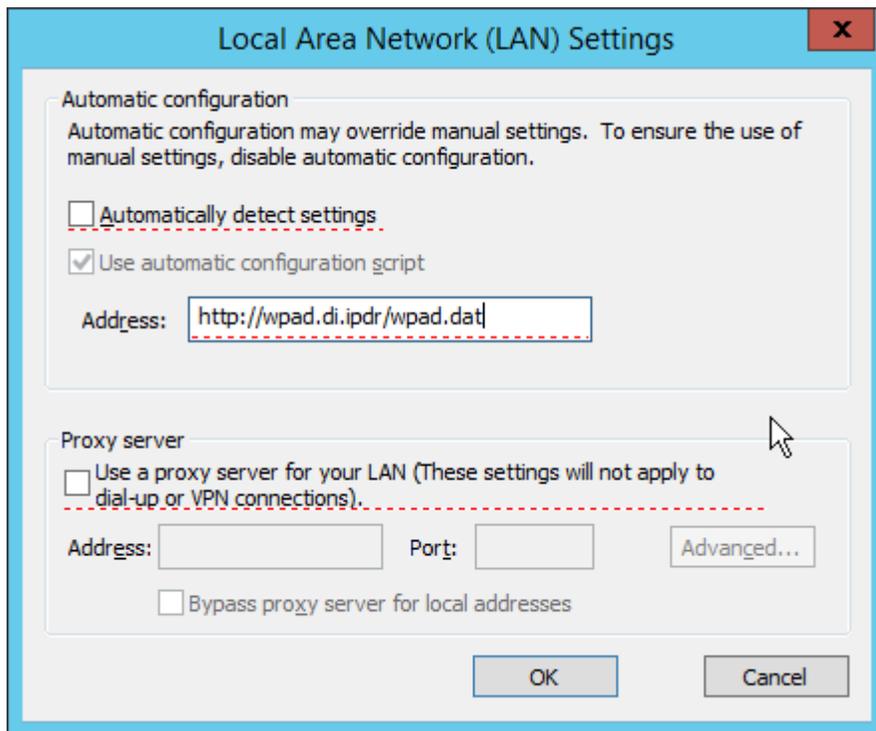
2. In **Group Policy Management Editor**, navigate to **User Configuration > Preferences > Control Panel Settings > Internet Settings**.



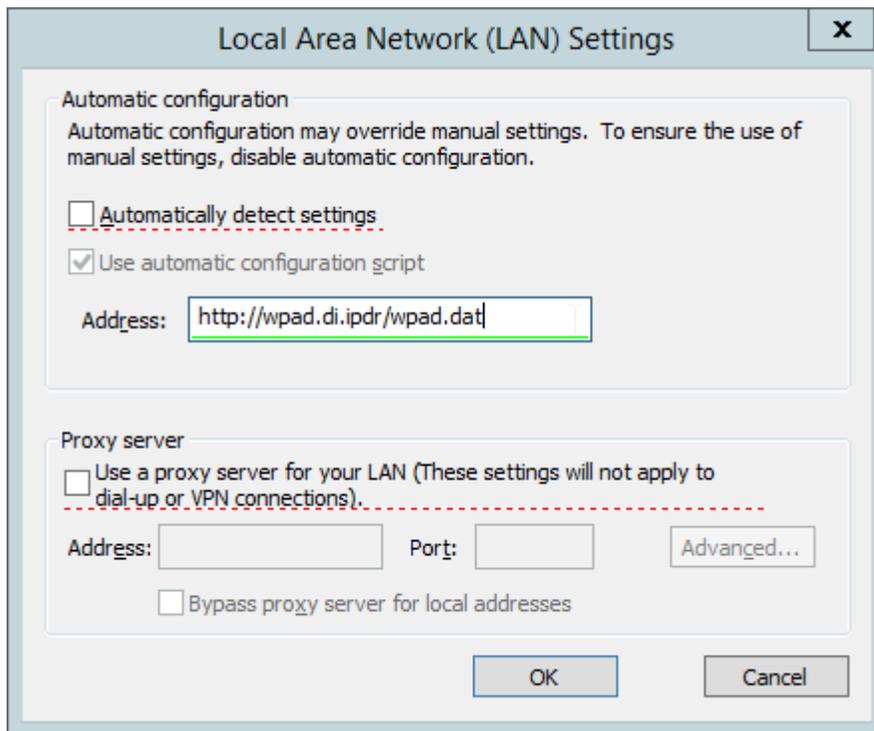
3. Right-click **Internet Settings** and select **New > Internet Explorer 10**.
4. Click the **Connections** tab.



5. Click **LAN Settings**.
6. Enter the **address** of the WPAD file for address. This will likely take the form `http://wpad.my.domain/wpad.dat` if you followed these instructions for configuring the proxy file.
7. Press the **F8** key to disable all settings in this dialogue box. (Note: This should underline everything in the box in red.)



8. Select the **Address** you just entered.

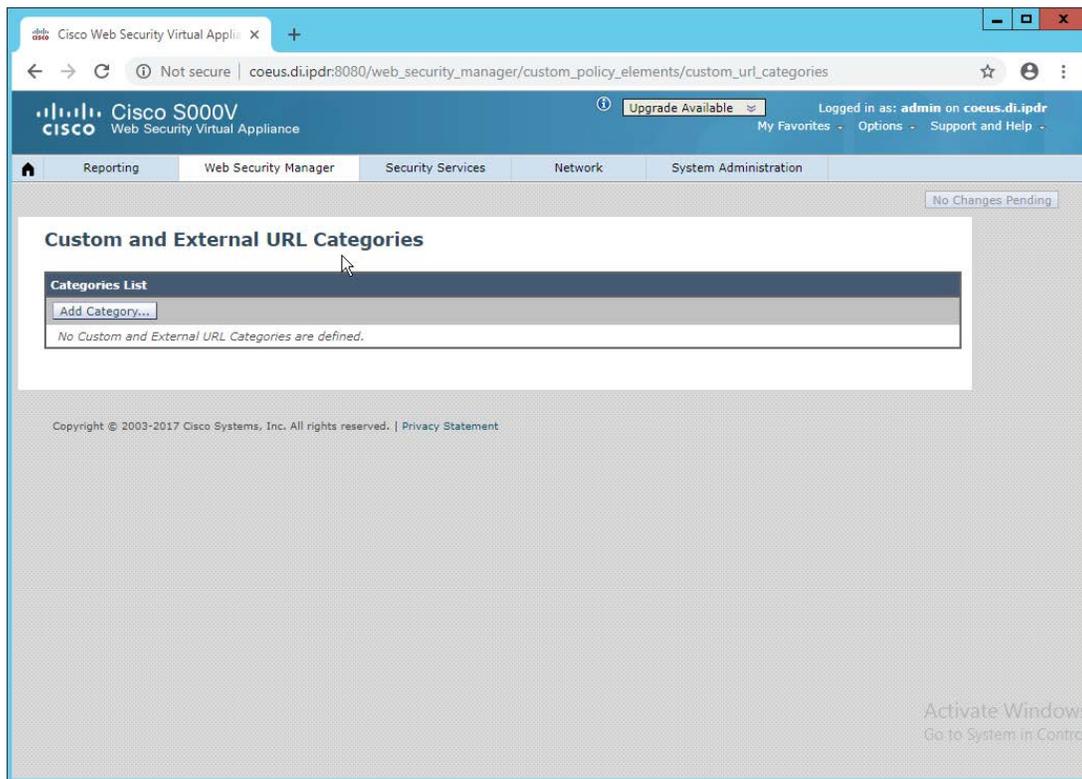


9. Press **F6** to enable this setting. (Note: The explicit WPAD address should now be underlined in green.)
10. Click **OK**.
11. Click **OK**.

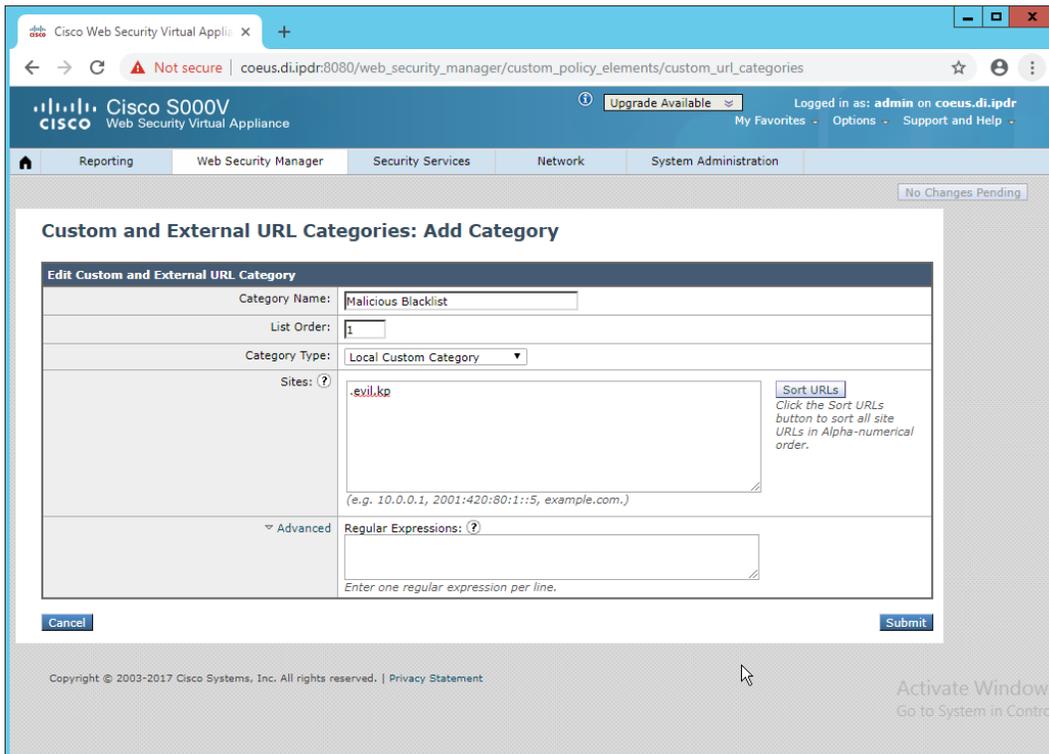
This Group Policy Object will update across all Windows systems whenever gpupdate.exe runs. An insider or technically capable user could manually disable this to avoid using the proxy, but benign clients who do not attempt to circumvent it will be protected from external (internet-based) threats by Cisco WSA. Protection from insiders and local threats on the network is provided by other products in the architecture, such as the network protection component (CryptoniteNXT).

2.14.4 Denylisting

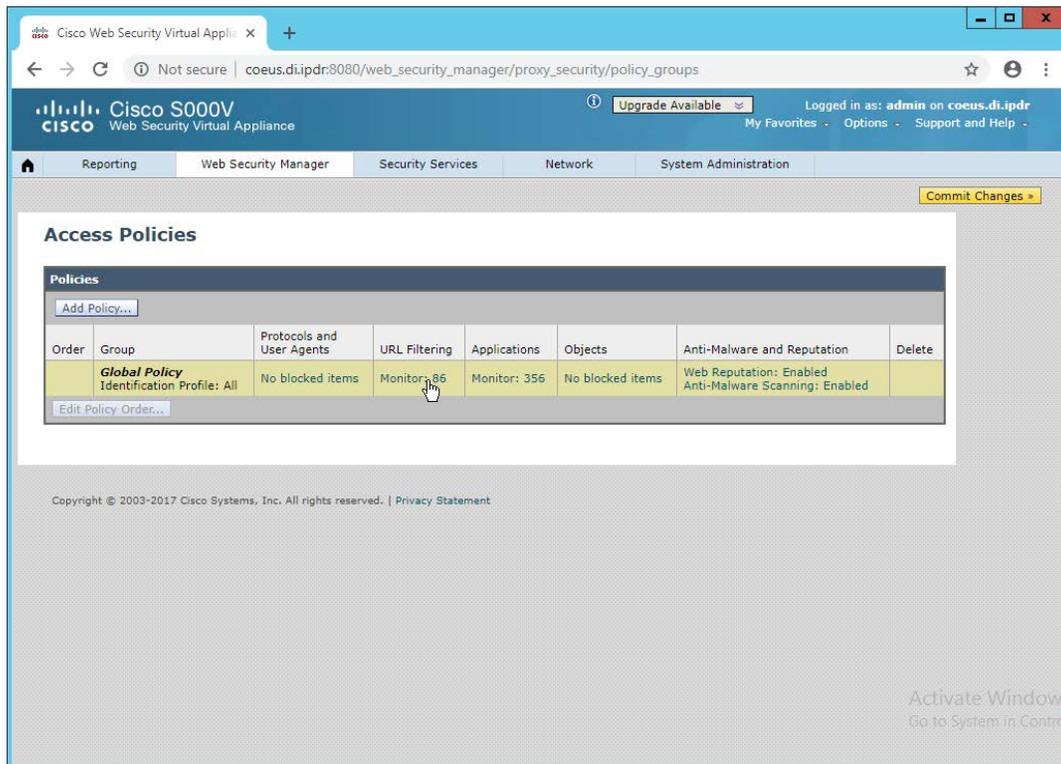
1. Navigate to **Web Security Manager > Custom and External URL Categories**.



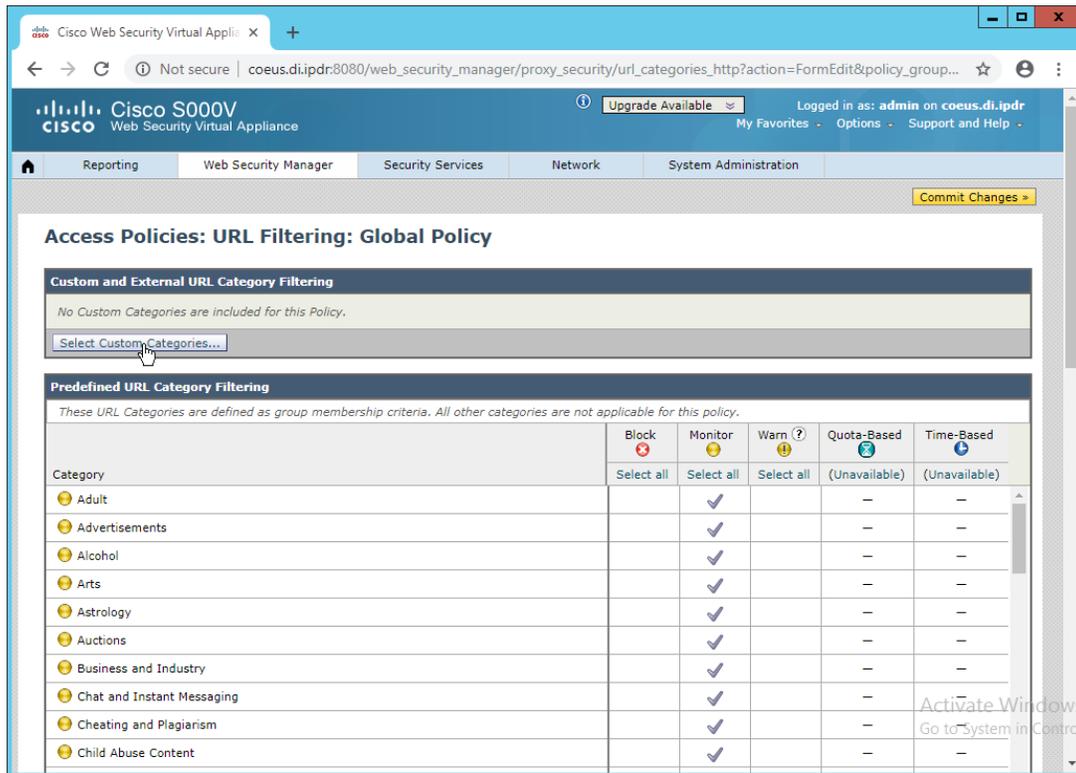
2. Click **Add Category**.
3. Enter a **name** for **Category Name**.
4. Select **Local Custom Category**. (The other option, **External Live Feed Category**, allows WSA to use a list of websites hosted somewhere else, potentially externally. For this demonstration we will simply enter websites in the **Sites** field, but note that this other option is available for convenience.)
5. For **Sites**, enter any sites to denylist. (Note: Entering **.mysite.abc** will include any subdomains of **mysite.abc**.)



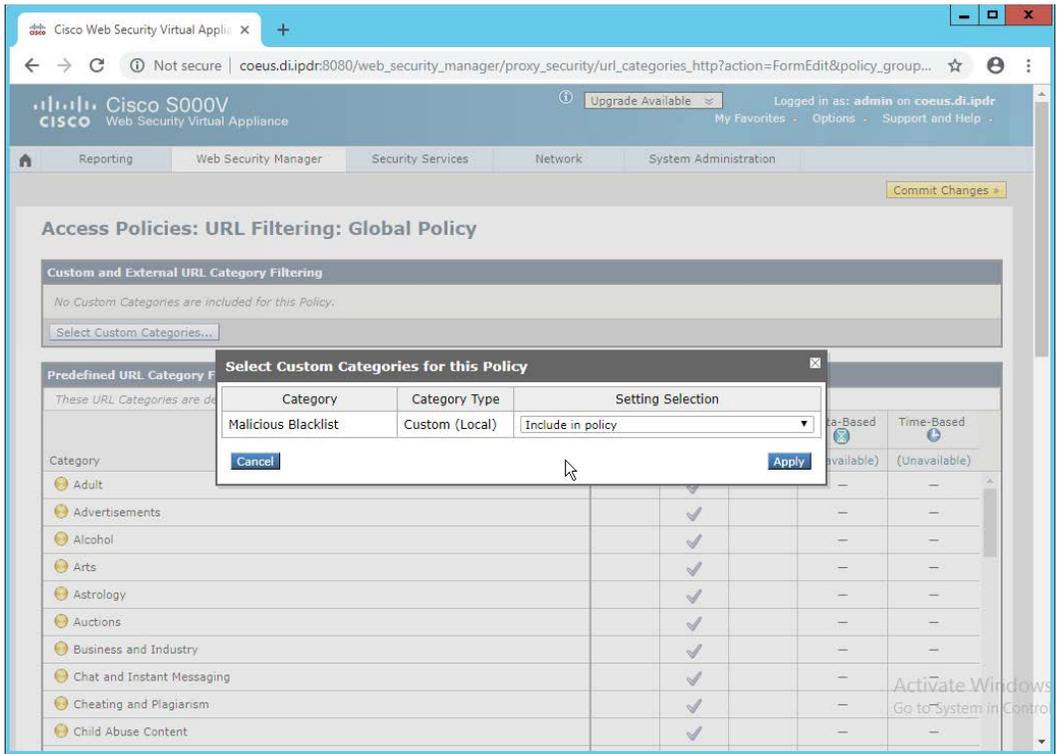
6. Click **Submit**.
7. Navigate to **Web Security Manager > Access Policies**.



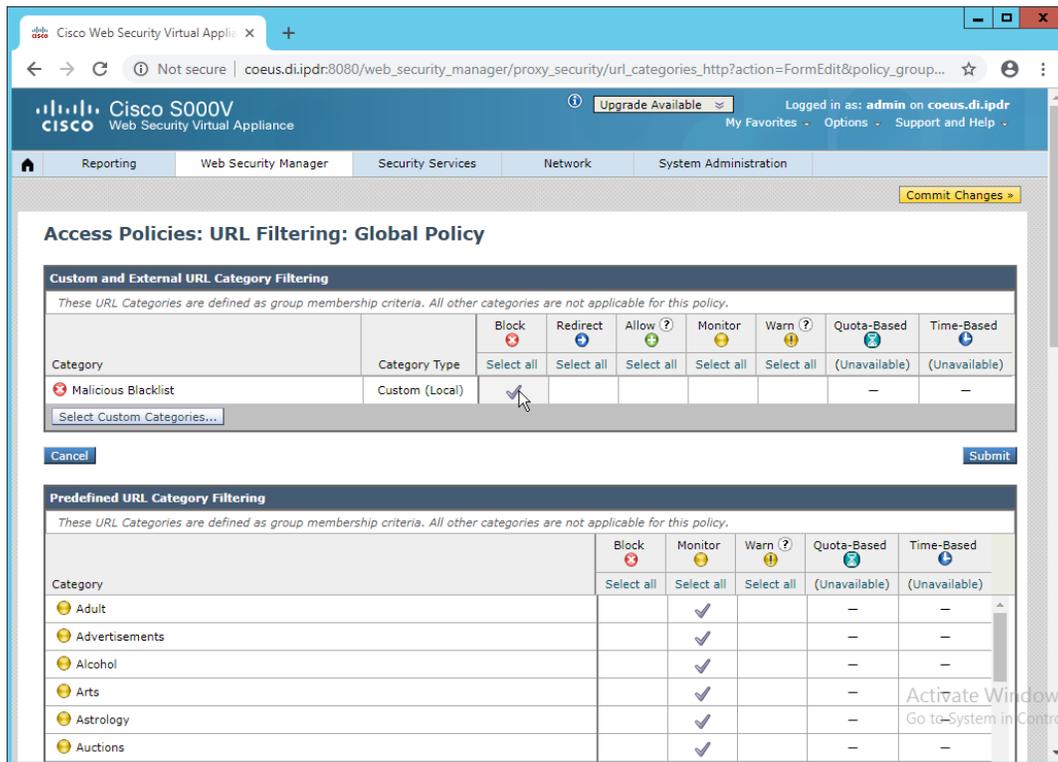
8. Click the link under **URL Filtering**.



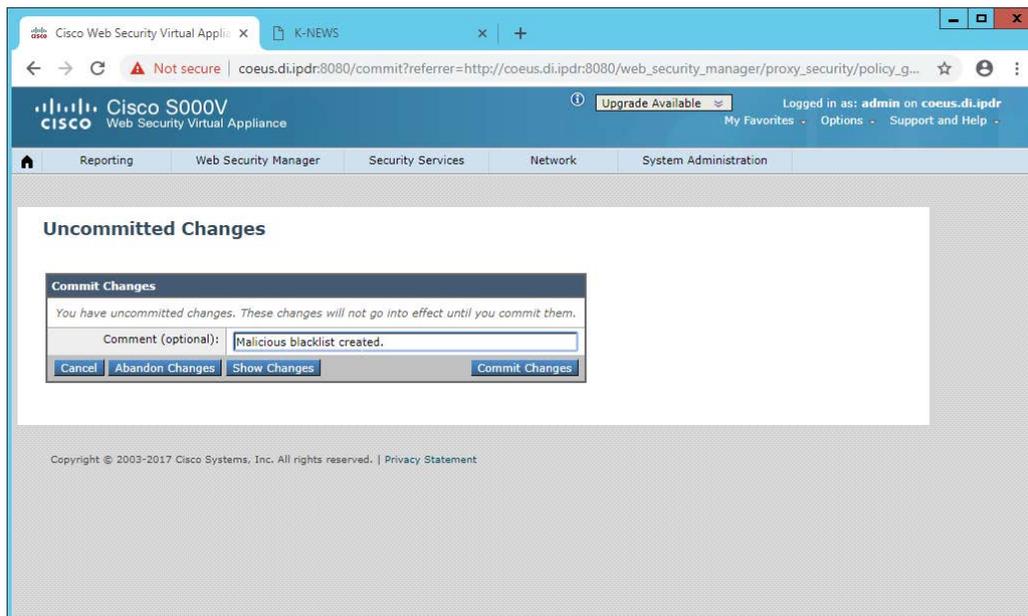
9. Click **Select Custom Categories**.
10. For the category just created, select **Include in policy** under **Setting Selection**.



11. Click **Apply**.



12. The category should now show under **Custom and External URL Category Filtering**. Put a checkmark in the **Block** box. (Selecting **Allow** lets you permit domains that are being incorrectly classified as malicious.)
13. Click **Submit**.
14. Click **Commit Changes**.
15. Enter a comment if desired.



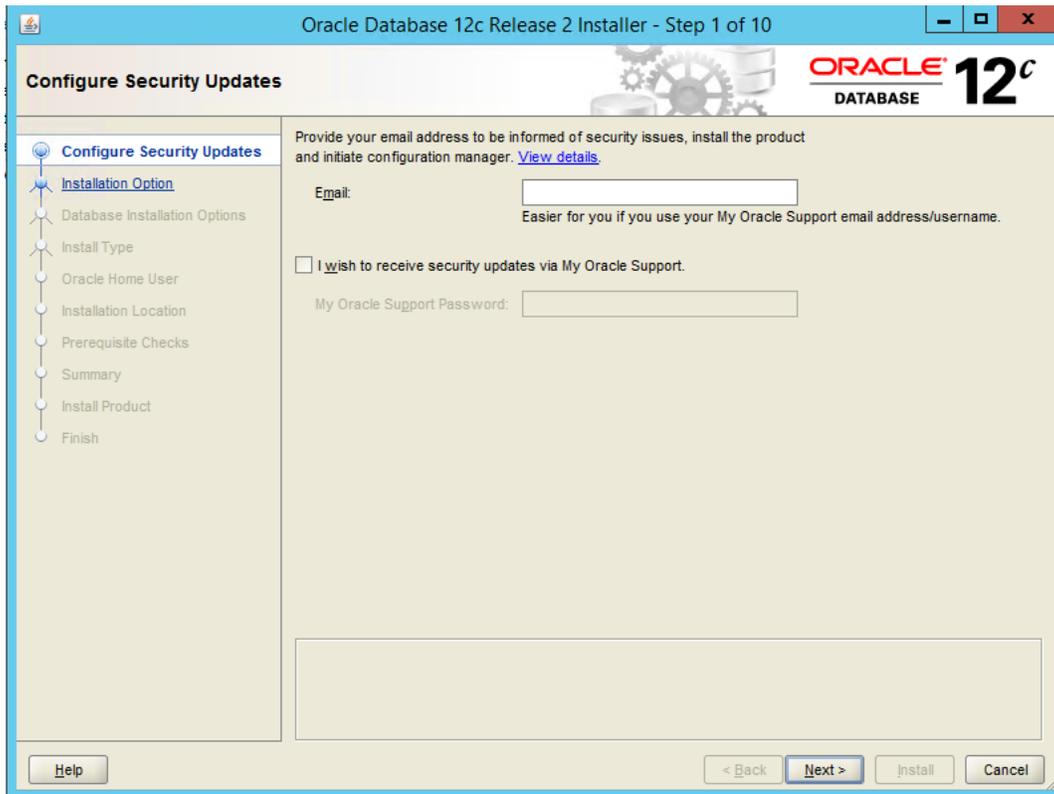
16. Click **Commit Changes**.

2.15 Symantec Data Loss Prevention

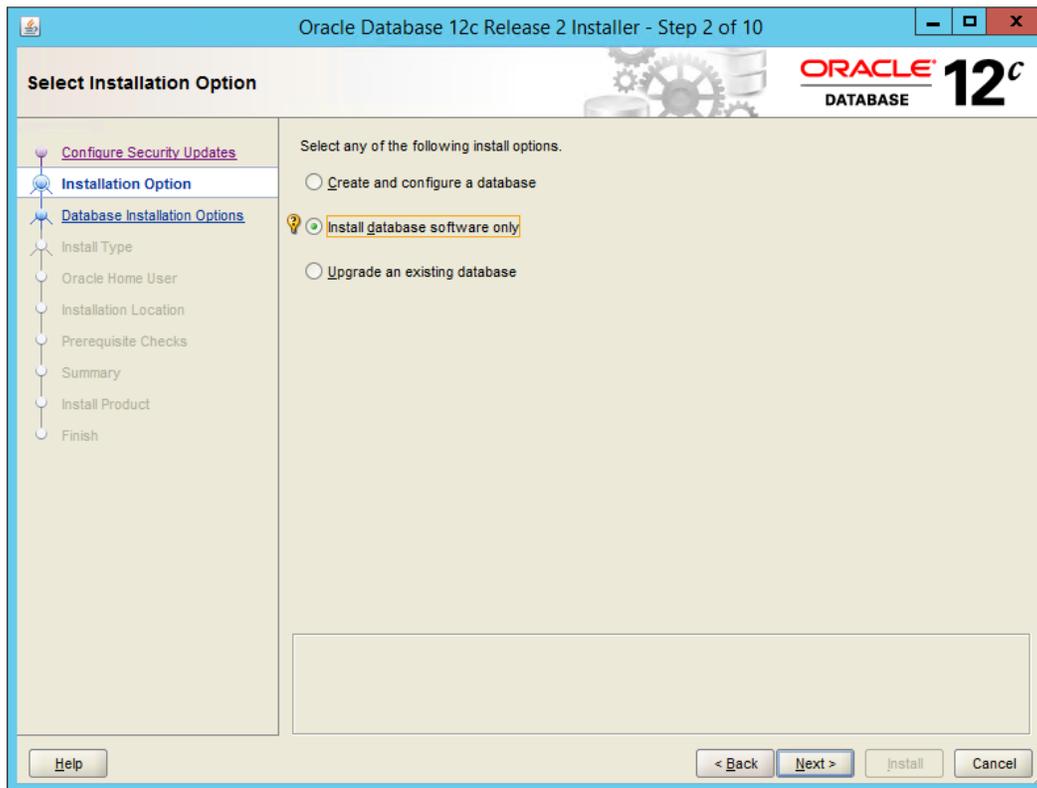
2.15.1 Install Oracle 12c Enterprise

1. Unzip the Symantec DLP installation files.
2. Download the Oracle 12c installation files from <https://www.oracle.com> if they are not included with the Symantec DLP installation files.
3. Move both sets of installation files to a temporary directory, such as **C:\temp**.
4. Copy the Symantec **12.2.0.1_64_bit_Installation_Tools** folder to **C:\temp\Oracle\tools**.
5. From a command prompt, navigate to **C:\temp\Oracle\database**, assuming the Oracle installation files were unzipped to **C:\temp\Oracle**.
6. Run the following command:

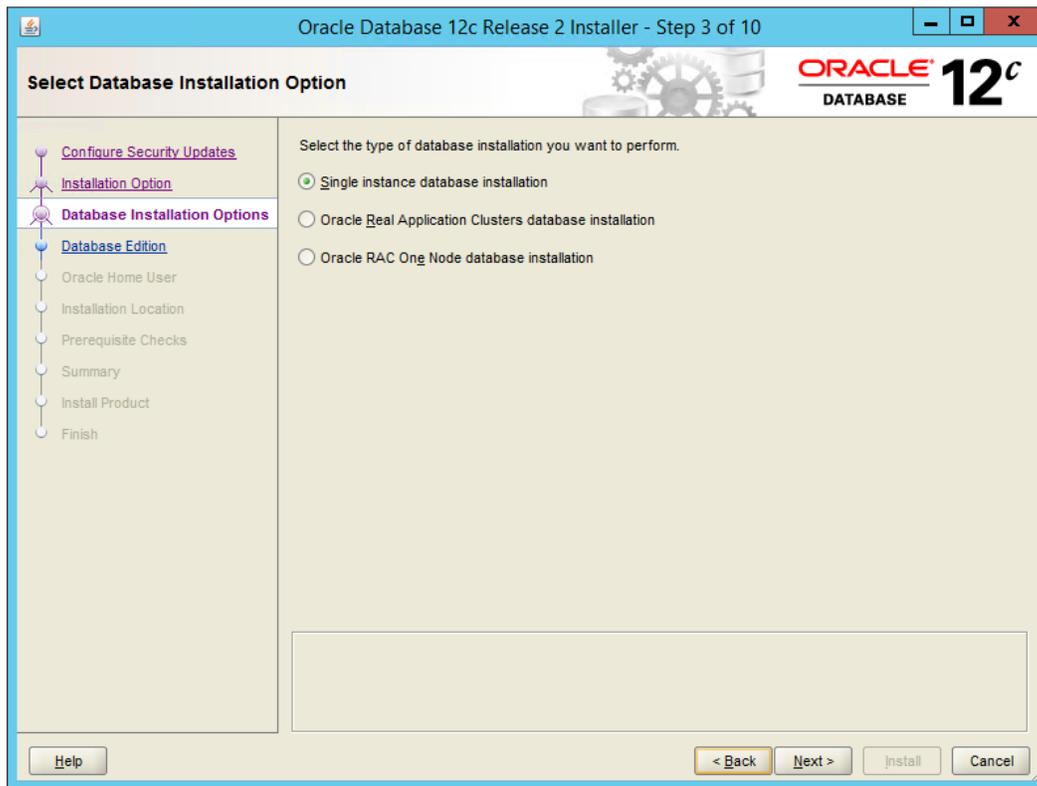

```
> C:\temp\Oracle\database\setup.exe -noconfig -responsefile
C:\temp\Oracle\tools\responsefiles\Oracle_12.2.0.1_Enterprise_Edi
tion_Installation_WIN.rsp
```
7. Once the wizard opens, you will be asked to configure security updates. If you do not possess a My Oracle Support account, leave the box unchecked and provide an **email**.



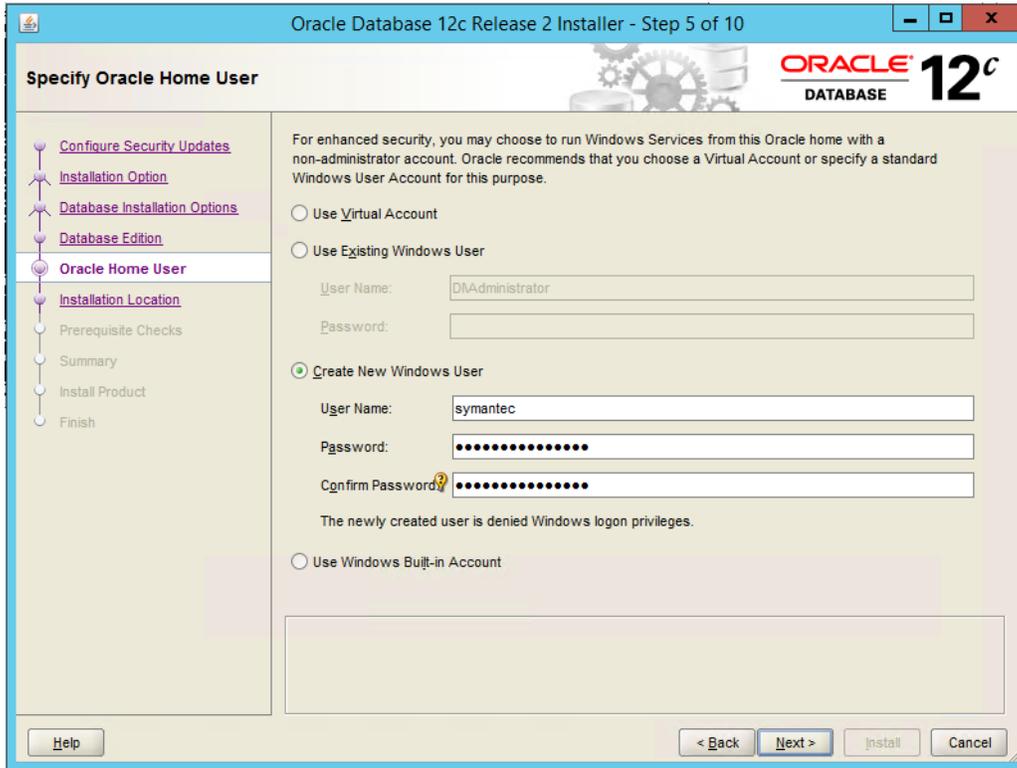
8. Click **Next**.
9. Select **Install database software only**.



10. Click **Next**.
11. Select **Single instance database installation**.

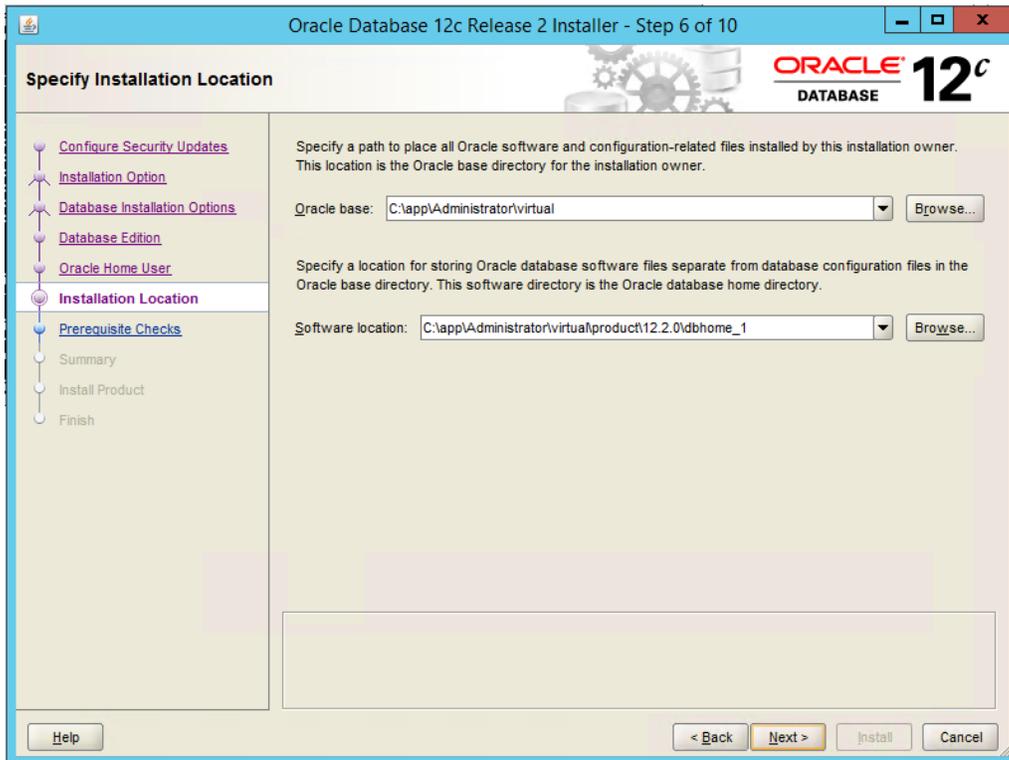


12. Click **Next**.
13. Select **Standard Edition**.
14. Click **Next**.
15. Select **Create New Windows User**.
16. Enter the **username** and **password** of a new user for Active Directory.

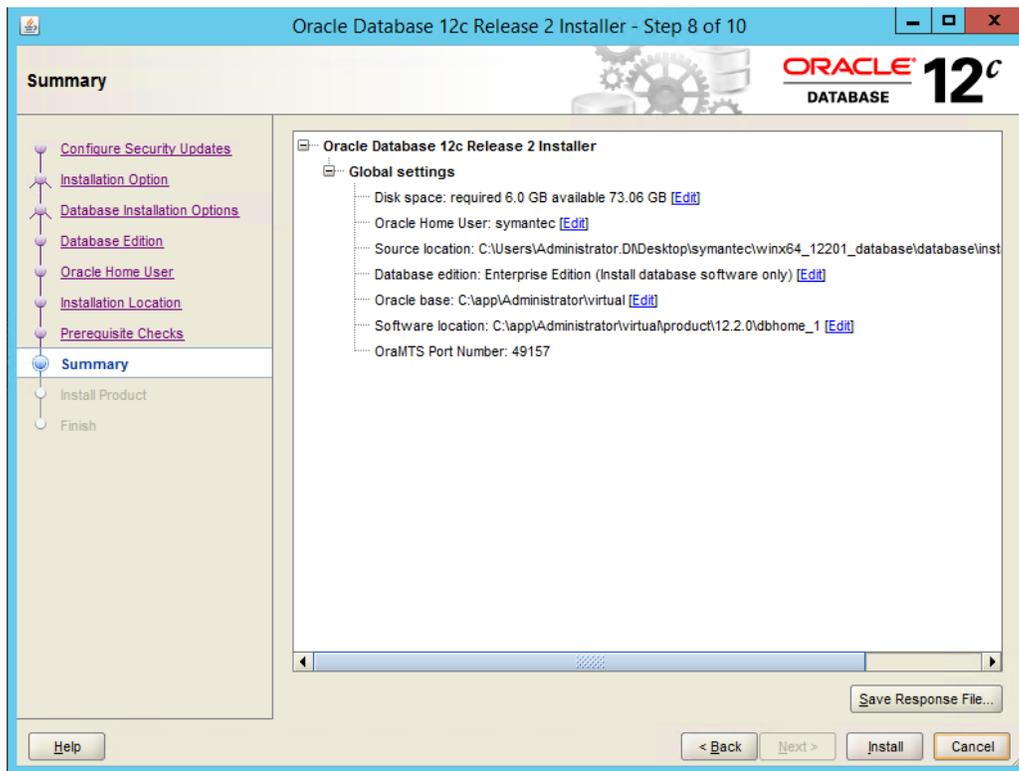


17. Click **Next**.

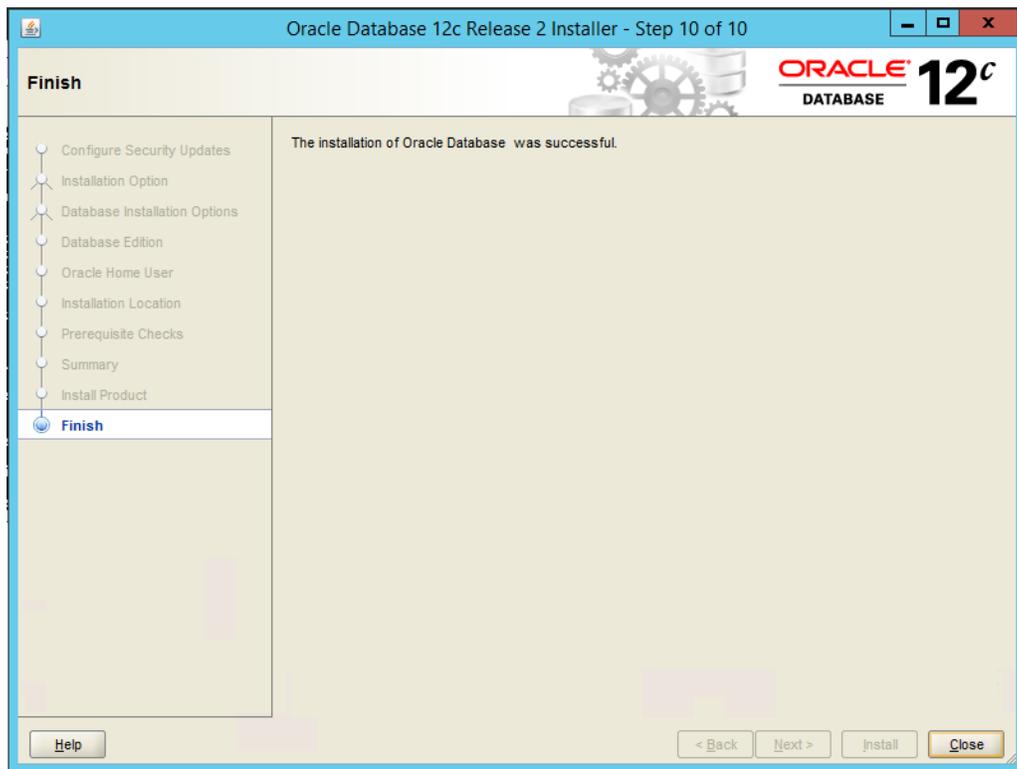
18. Select a location to install the software, if desired.



19. Click **Next**.



20. Verify the information and click **Install**. The installation may take a long time.



21. Click **Close** when the installation is complete.

2.15.2 Create an Oracle Database for Symantec DLP

1. Set the ORACLE_HOME environment variable by running the following command. Adjust the path accordingly if using a version other than 12.2.0.

```
> set
ORACLE_HOME=C:\app\Administrator\virtual\product\12.2.0\dbhome_1
```

2. Copy the Oracle database template named **Oracle_12.2.0.1_Template_for_64_bit_WIN.dbt** from the Symantec DLP zip file into **C:\app\Administrator\virtual\product\12.2.0\dbhome_1\assistants\dbca\templates.**

3. Ensure that the response file **Oracle_12.2.0.1_DBCA_WIN.rsp** is located in the folder **C:\temp\Oracle\database\tools\responsefiles.**

4. Run the following command.

```
> %ORACLE_HOME%\bin\dbca -createDatabase -progressOnly -
responseFile
```

C:\temp\Oracle\database\tools\responsefiles\Oracle_12.2.0.1_DBCA_
WIN.rsp

5. Enter a **password** for the **SYS** user. (Only the special characters **_**, **#**, or **\$** are allowed.)
6. Enter a **password** for the **SYSTEM** user. (Only the special characters **_**, **#**, or **\$** are allowed.)
7. Enter a **password** for the **Oracle Home User**.

2.15.3 Configuring the Oracle Listener

1. Ensure that the database services OracleServicePROTECT and DistributedTransactionCoordinator are running.
2. In the file `%ORACLE_HOME%\network\admin\sqlnet.ora`, change the line `SQLNET.AUTHENTICATION_SERVICES=(NTS)` to `SQLNET.AUTHENTICATION_SERVICES=(none)`.
3. Navigate to **Start > All Programs > Oracle 12.2.0 > Configuration and Migration Tools > Net Configuration Assistant** and run the program.
4. Select **Listener configuration**.



5. Click **Next**.
6. Select **Add**.



7. Click **Next**.
8. Enter a **name** for the listener.
9. Enter a **password**.

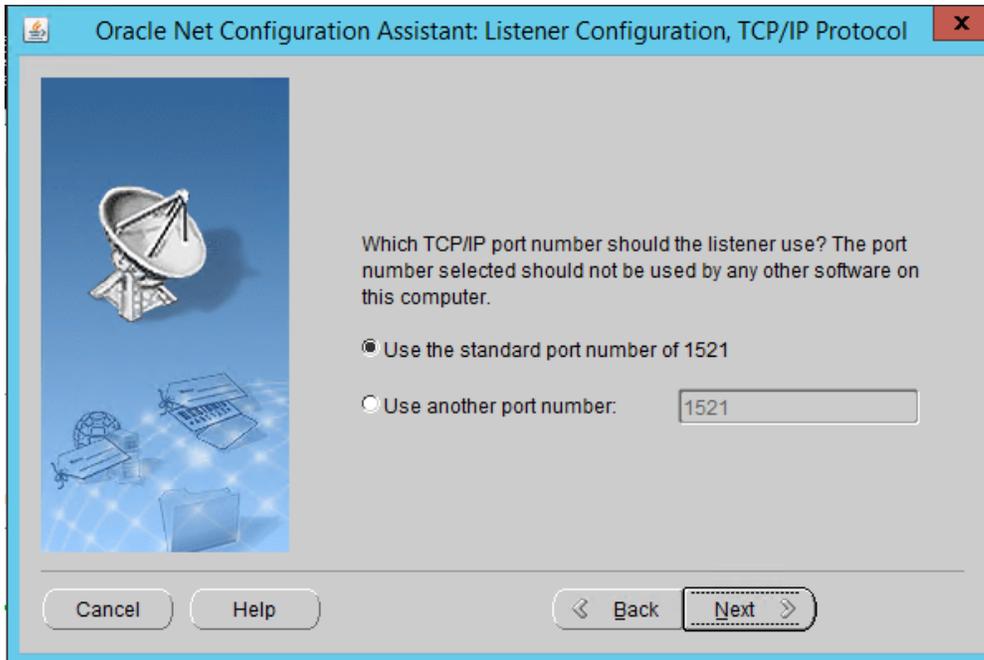


10. Click **Next**.

11. Move the **TCP** protocol to the **Selected Protocols** column.

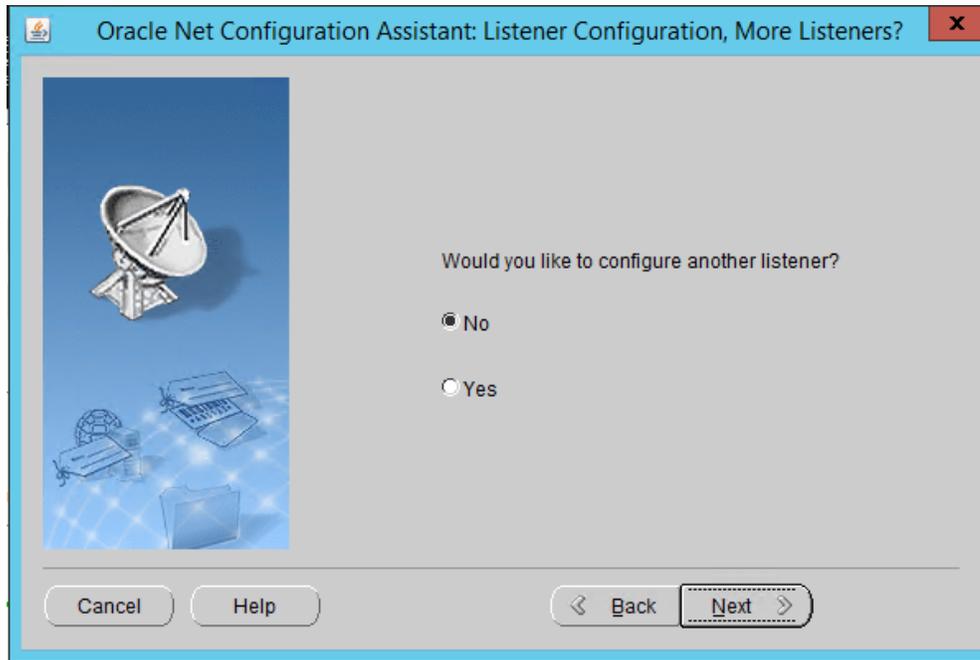


12. Click **Next**.
13. Select **Use the standard port number of 1521**.



14. Click **Next**.

15. Select **No**.

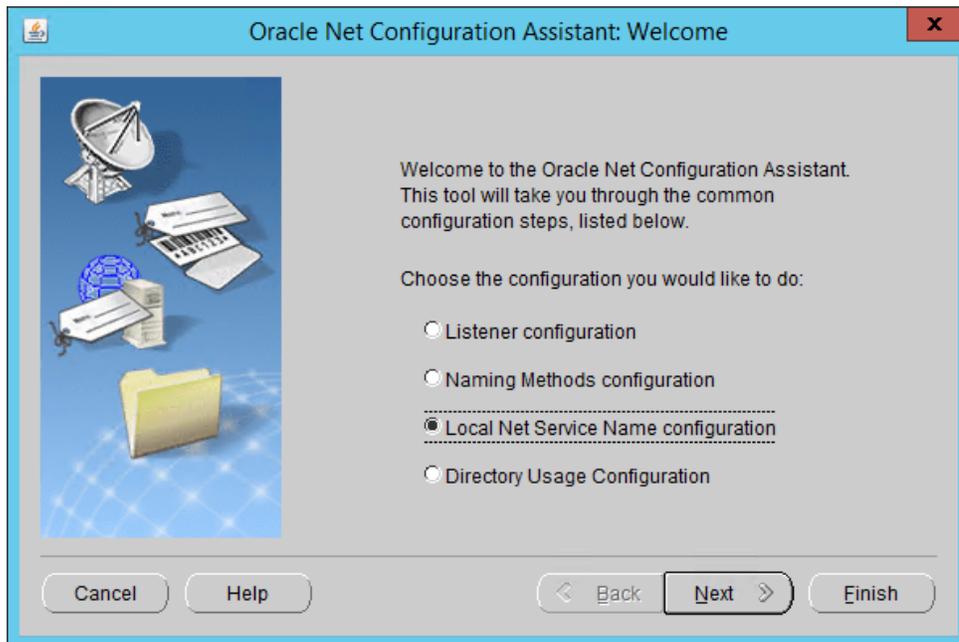


16. Click **Next**.



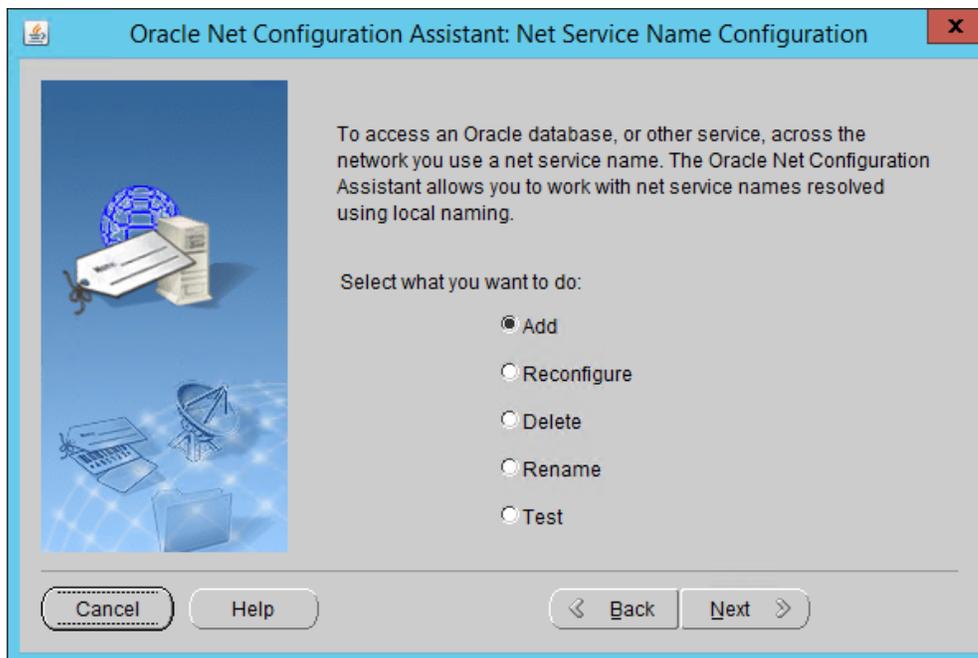
17. Click **Next**.

18. Select **Local Net Service Name configuration**.



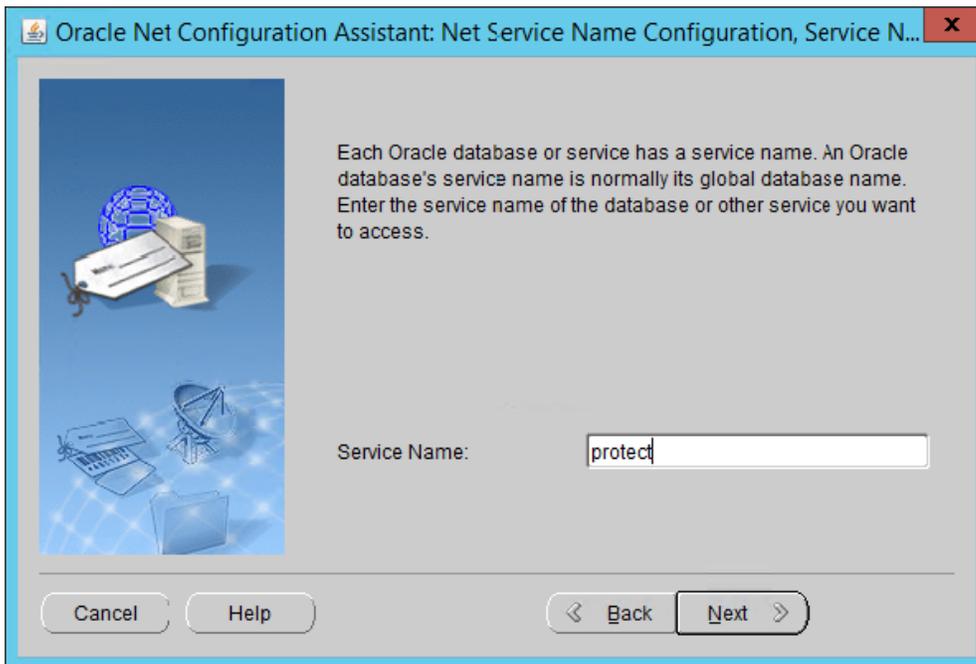
19. Click **Next**.

20. Select **Add**.



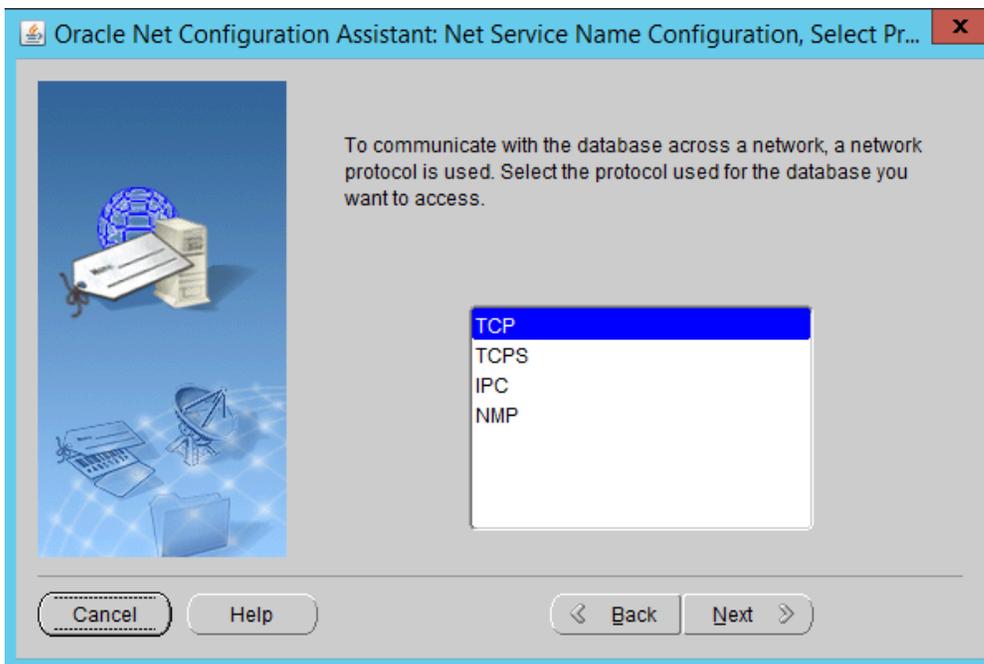
21. Click **Next**.

22. Enter the word "protect" for the **name**.



23. Click **Next**.

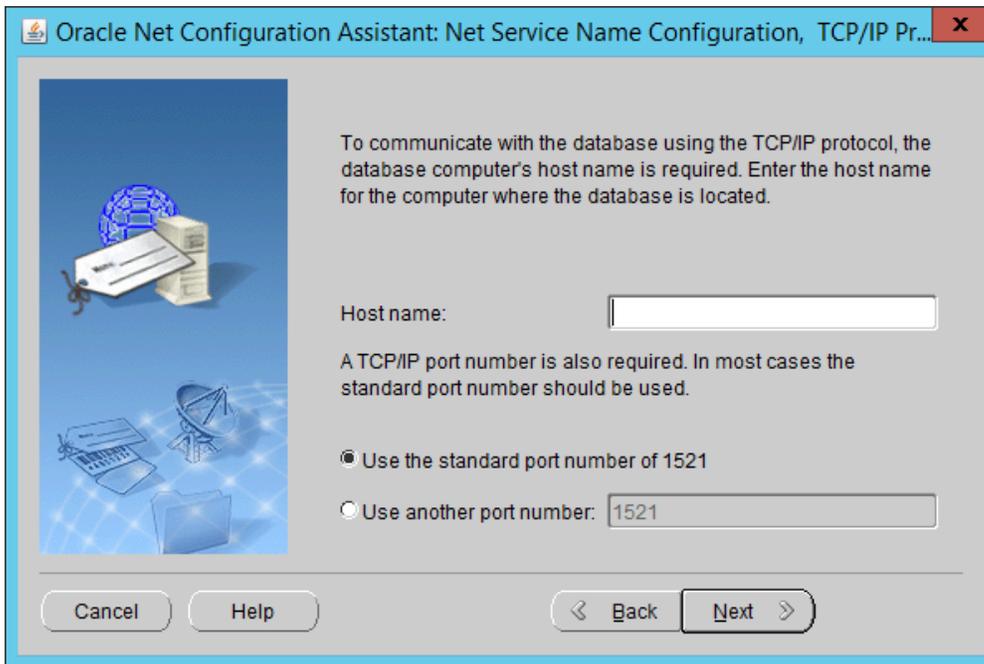
24. Select **TCP**.



25. Click **Next**.

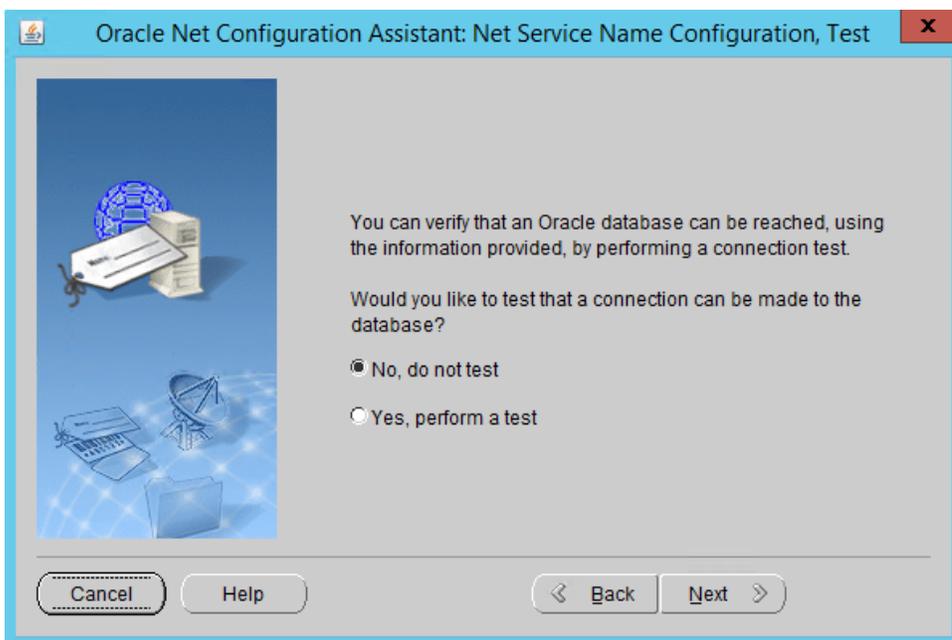
26. Enter the **IP address** of the system hosting the Oracle Database.

27. Select **Use the standard port number of 1521**.

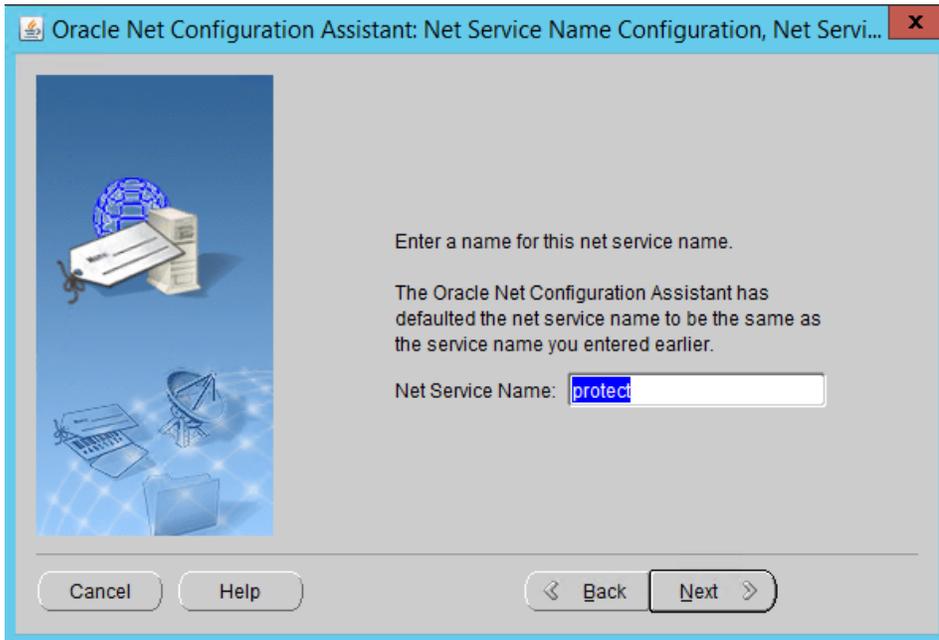


28. Click **Next**.

29. Select **No, do not test**.

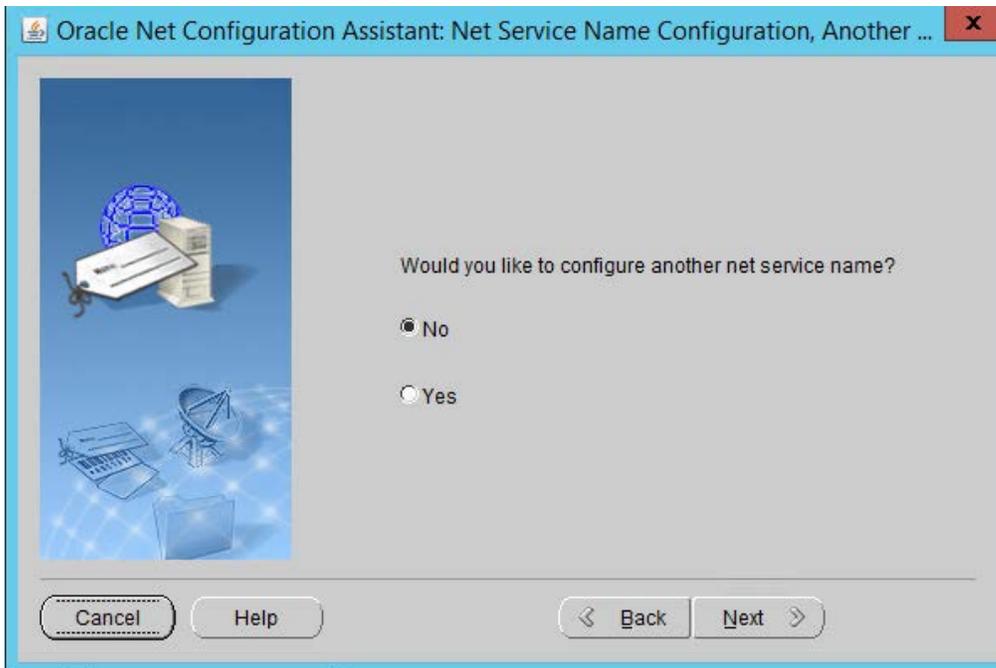


30. Click **Next**.

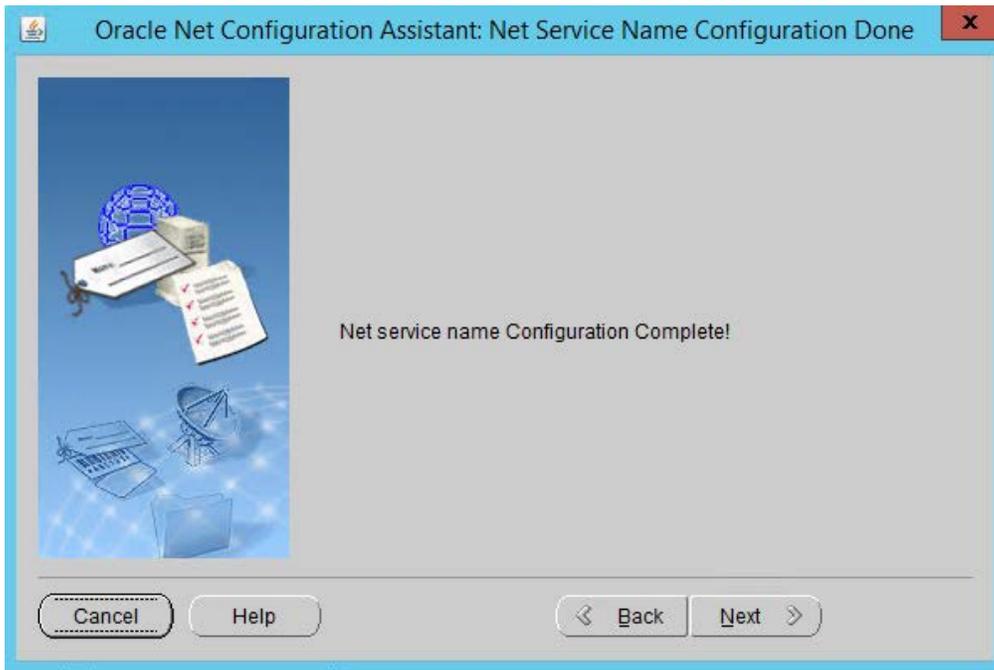


31. Click **Next**.

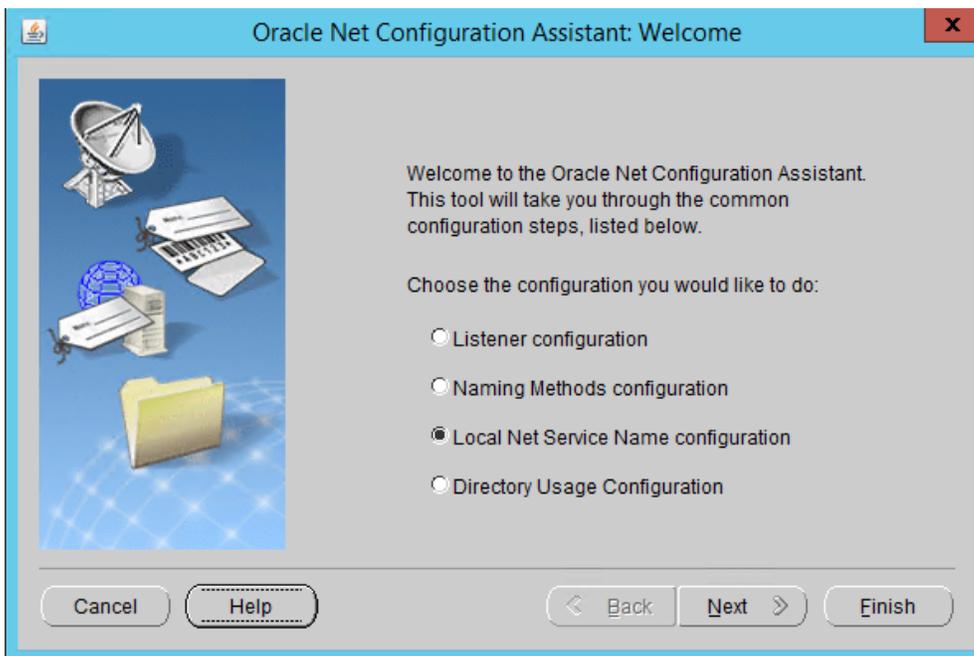
32. Select **No**.



33. Click **Next**.



34. Click **Next**.

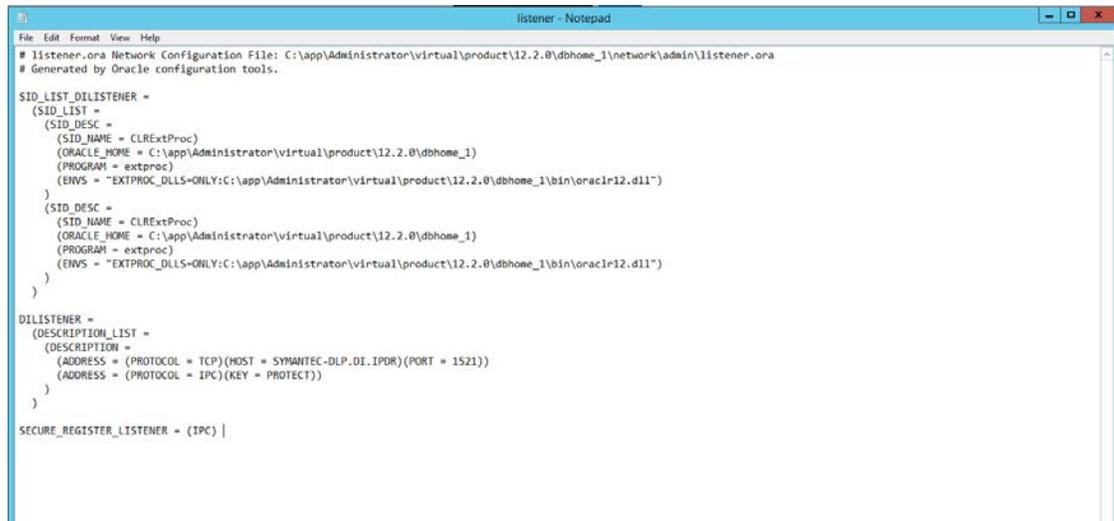


35. Click **Finish**.

36. In an administrative command prompt, run the following command to stop the listener.

```
> lsnrctl stop
```

37. Open the file **%ORACLE_HOME%\network\admin\listener.ora**.
38. Change (ADDRESS = (PROTOCOL = IPC)(KEY = <key_value>)) to (ADDRESS = (PROTOCOL = IPC)(KEY = PROTECT)).
39. Add the line **SECURE_REGISTER_LISTENER=(IPC)** to the end of the file.



```
listener - Notepad
File Edit Format View Help
# listener.ora Network Configuration File: C:\app\Administrator\virtual\product\12.2.0\dbhome_1\network\admin\listener.ora
# Generated by Oracle configuration tools.

SID_LIST_DILISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\app\Administrator\virtual\product\12.2.0\dbhome_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\app\Administrator\virtual\product\12.2.0\dbhome_1\bin\oraclr12.dll")
)
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\app\Administrator\virtual\product\12.2.0\dbhome_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\app\Administrator\virtual\product\12.2.0\dbhome_1\bin\oraclr12.dll")
)
)
DILISTENER =
(DESCRIPTION_LIST =
(ADDRESS = (PROTOCOL = TCP)(HOST = SYMANTEC-DLP.DE.IPDOR)(PORT = 1521))
(ADDRESS = (PROTOCOL = IPC)(KEY = PROTECT))
)
)
SECURE_REGISTER_LISTENER = (IPC) |
```

40. Save the file and exit the editor.
41. Ensure that OracleServicePROTECT and OracleVssWriterPROTECT services are running in Task Manager.
42. In an administrative command prompt, run the following command to start the listener. Replace dilistener with the name given to your listener.

```
> lsnrctl start dilistener
```

43. Run the following commands to connect the listener to the database using SQL Plus. Replace password with the password used for the SYS user.

```
> sqlplus /nolog
```

```
> conn sys/password as sysdba
```

44. Run the following commands in the SQL prompt. (Note: If errors occur relating to the SPFILE, try replacing ORACLE_HOME or ORACLE_base values in %ORACLE_HOME%\dbs\init.ora with the

absolute path. Then run `CREATE SPFILE FROM PFILE='%ORACLE_HOME%\dbs\init.ora'` and `CREATE PFILE FROM SPFILE='%ORACLE_HOME%\dbs\init.ora'`. Restart the database after doing this.)

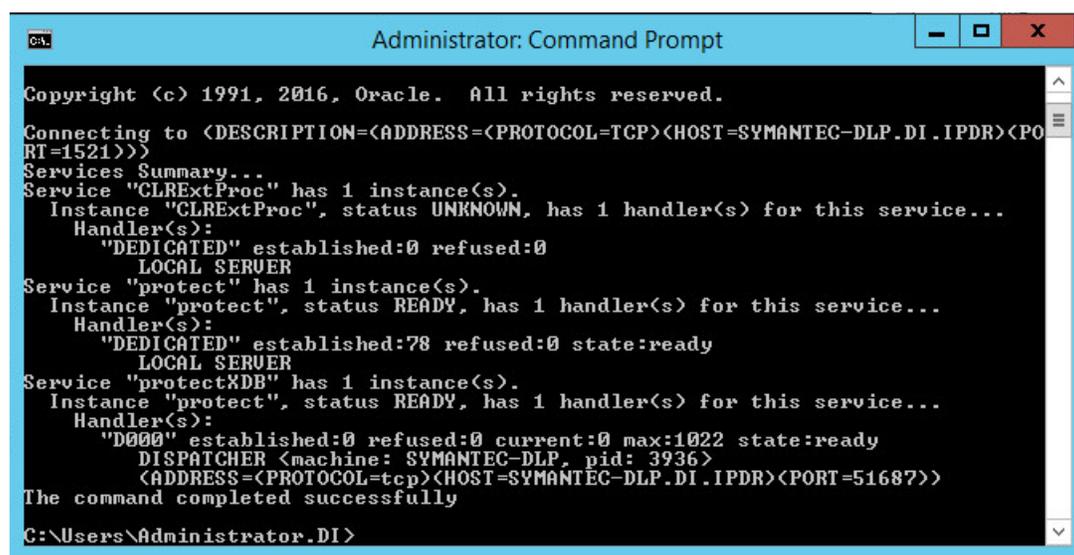
```
> ALTER SYSTEM SET local_listener = '(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=PROTECT)))' SCOPE=both;
```

```
> ALTER SYSTEM REGISTER;
```

```
> exit
```

45. Run the following command to verify the status of the listeners:

```
> lsnrctl services
```



```
Administrator: Command Prompt

Copyright (c) 1991, 2016, Oracle. All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=SYMANTEC-DLP.DI.IPDR)(PORT=1521)))
Services Summary...
Service "CLRExtProc" has 1 instance(s).
  Instance "CLRExtProc", status UNKNOWN, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:0 refused:0
      LOCAL SERVER
Service "protect" has 1 instance(s).
  Instance "protect", status READY, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:78 refused:0 state:ready
      LOCAL SERVER
Service "protectXDB" has 1 instance(s).
  Instance "protect", status READY, has 1 handler(s) for this service...
    Handler(s):
      "D000" established:0 refused:0 current:0 max:1022 state:ready
      DISPATCHER <machine: SYMANTEC-DLP, pid: 3936>
      (ADDRESS=(PROTOCOL=tcp)(HOST=SYMANTEC-DLP.DI.IPDR)(PORT=51687))
The command completed successfully

C:\Users\Administrator.DI>
```

46. Open a new administrative command window.

47. Navigate to `C:\Temp\Oracle\database\tools`.

48. Run the following command:

```
> sqlplus /nolog
```

```
> @oracle_create_user.sql
```

49. Enter the **password** for the **SYS** user.

50. For **sid**, enter "protect".

51. For a **username**, enter "protect".

52. Enter a **password** for the “protect” user. (The special characters &, \$, and # are not allowed.)
53. When this process is finished, open a new administrative command window and run the following command.

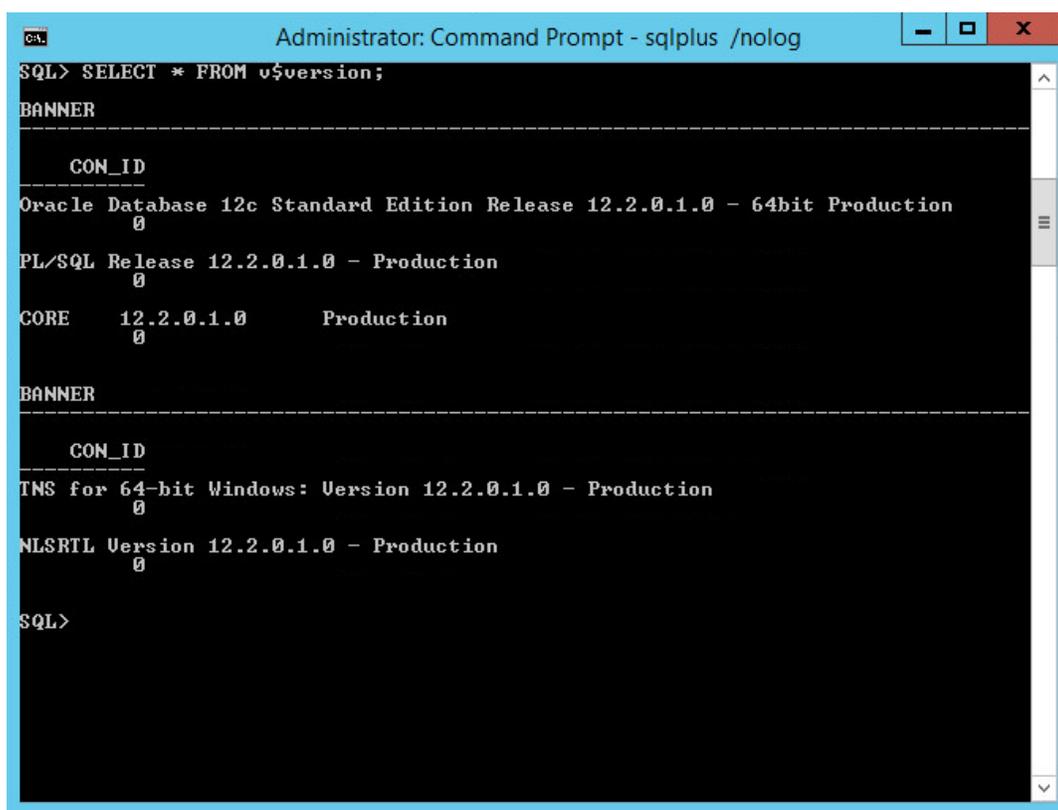
```
> sqlplus /nolog
```

54. Log in as the **SYS** user with the following command (replace “password” with the password for the **SYS** user).

```
> connect sys/password@protect as sysda
```

55. Verify the version information with the following command.

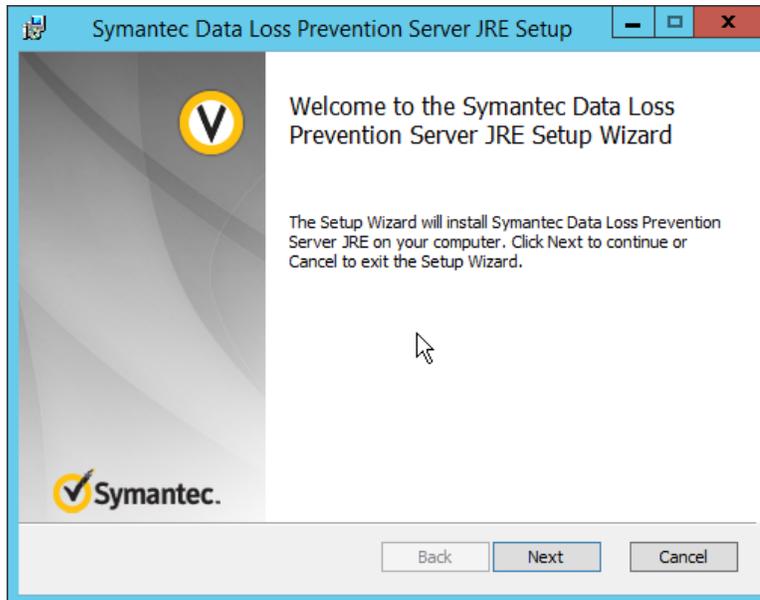
```
> SELECT * FROM v$version;
```



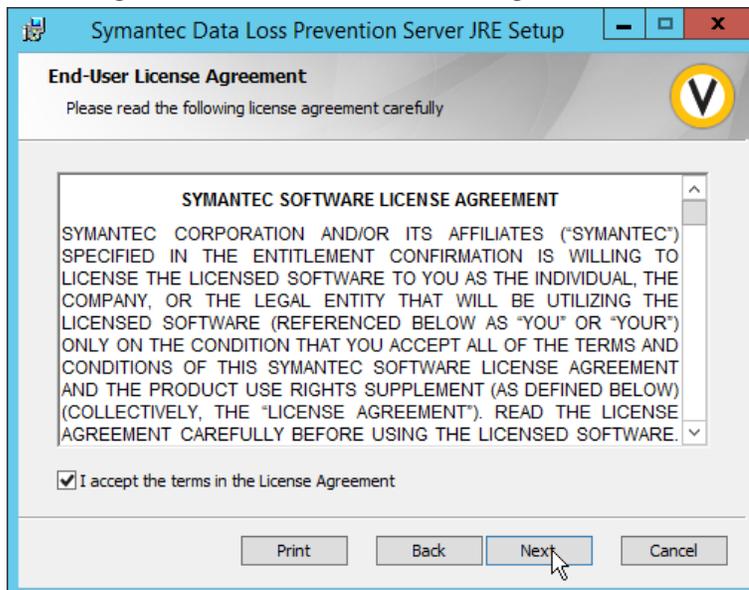
```
Administrator: Command Prompt - sqlplus /nolog
SQL> SELECT * FROM v$version;
BANNER
-----
      CON_ID
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production
      0
PL/SQL Release 12.2.0.1.0 - Production
      0
CORE      12.2.0.1.0      Production
      0
BANNER
-----
      CON_ID
TNS for 64-bit Windows: Version 12.2.0.1.0 - Production
      0
NLSRTL Version 12.2.0.1.0 - Production
      0
SQL>
```

2.15.4 Install Symantec DLP

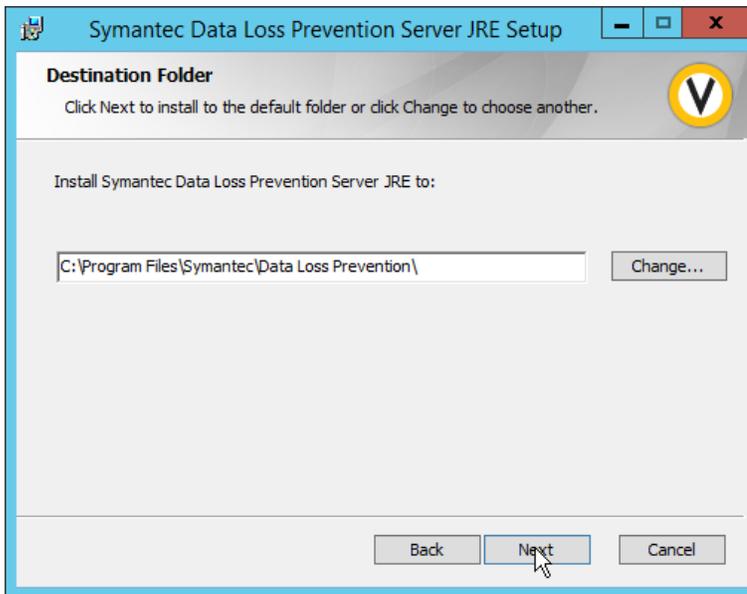
1. In the folder **DLP Installs\DLP 15.1\Symantec_DLP_15.1_Platform_Win-IN_15.1.0.25021\DLP\15.1\New_Installs\x64\Release**, located in the download folder for the DLP files, run **ServerJRE.msi**.



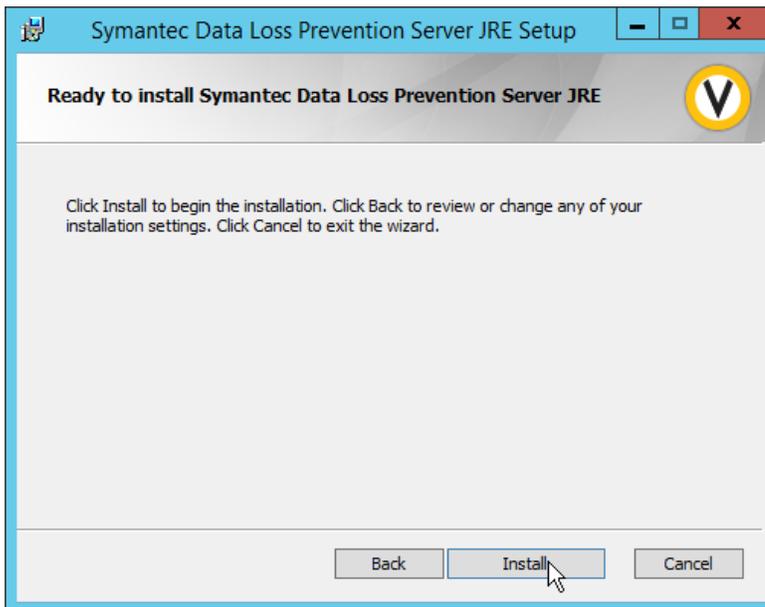
2. Click **Next**.
3. Select **I agree to the terms in the license agreement**.



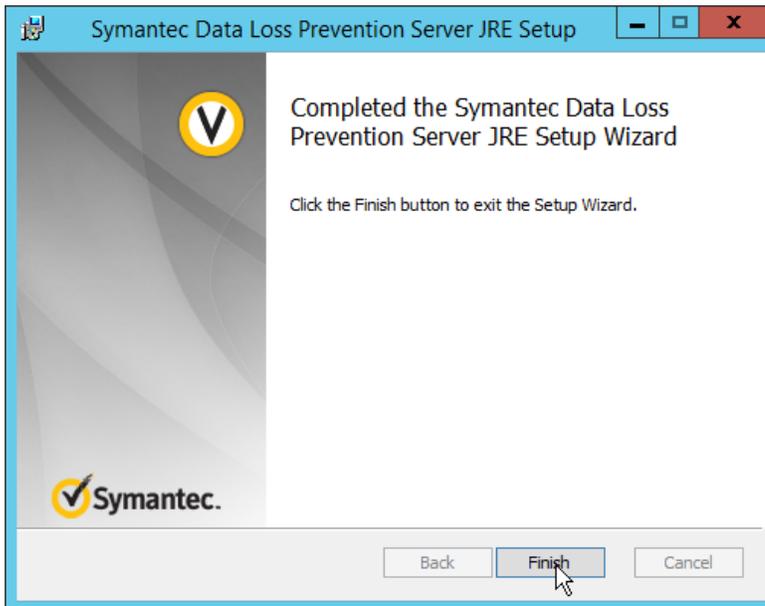
4. Click **Next**.



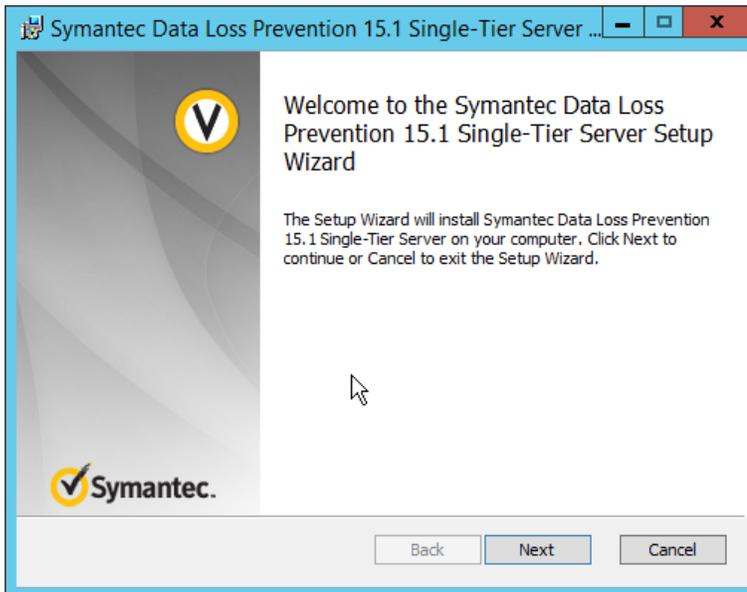
5. Click **Next**.



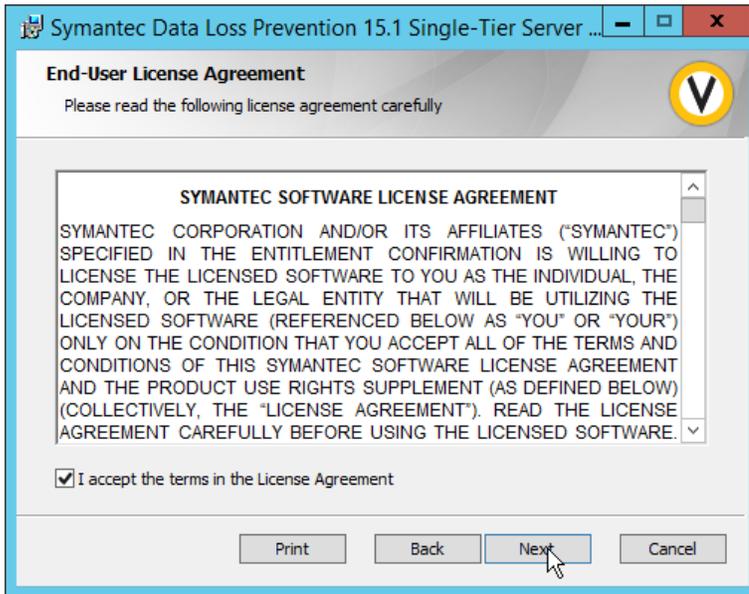
6. Click **Install**.



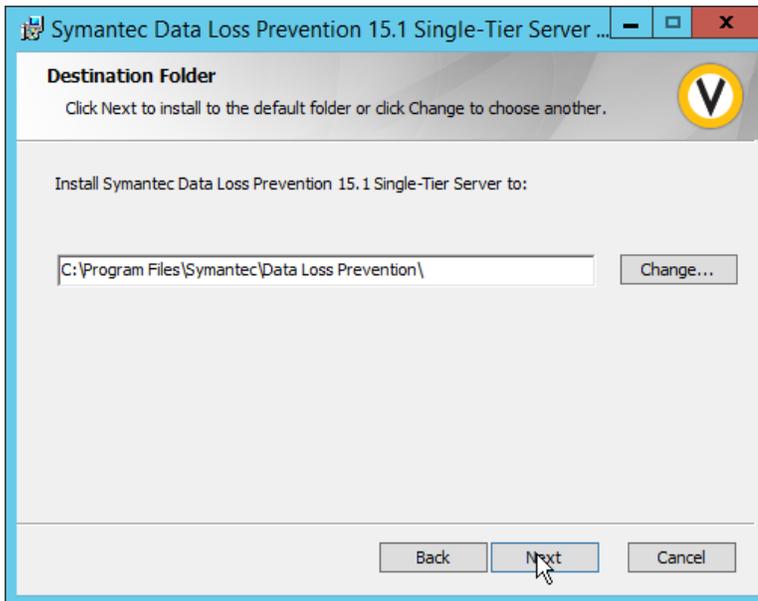
7. Click **Finish**.
8. Run **SingleTierServer.msi** (located in the same folder as **ServerJRE.msi**).



9. Click **Next**.
10. Check the box to accept the license agreement.

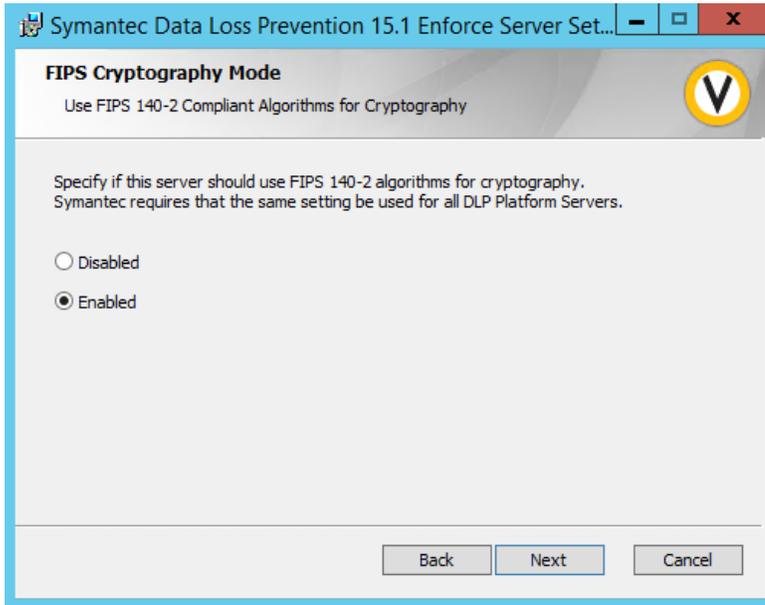


11. Click **Next**.

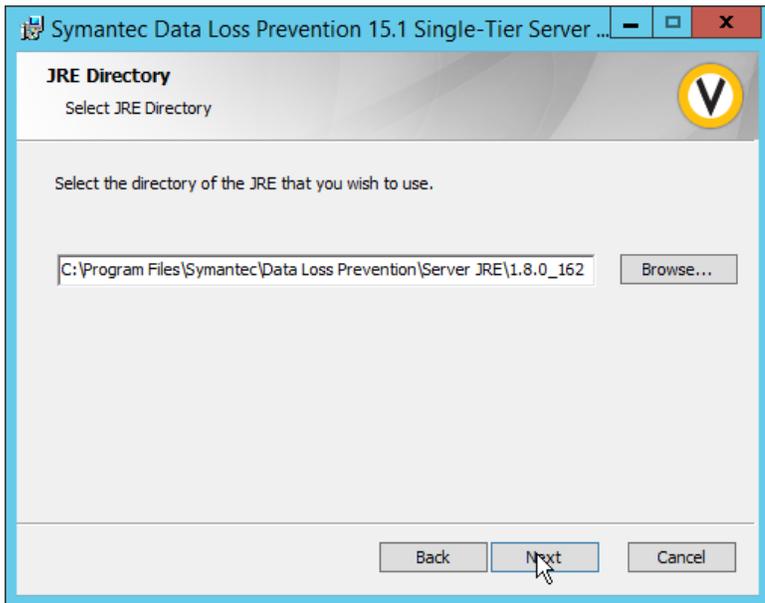


12. Click **Next**.

13. Select **Enabled** for **FIPS 140-2 Compliant Algorithms**.

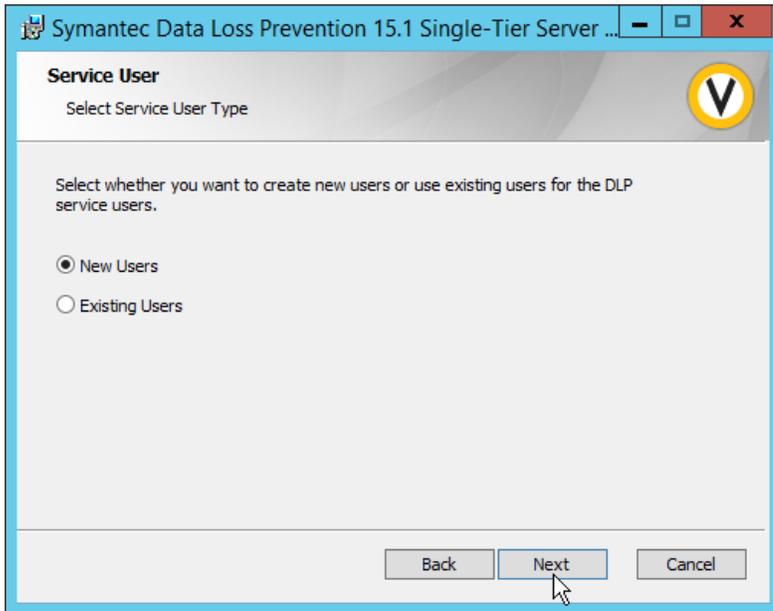


14. Click **Next**.

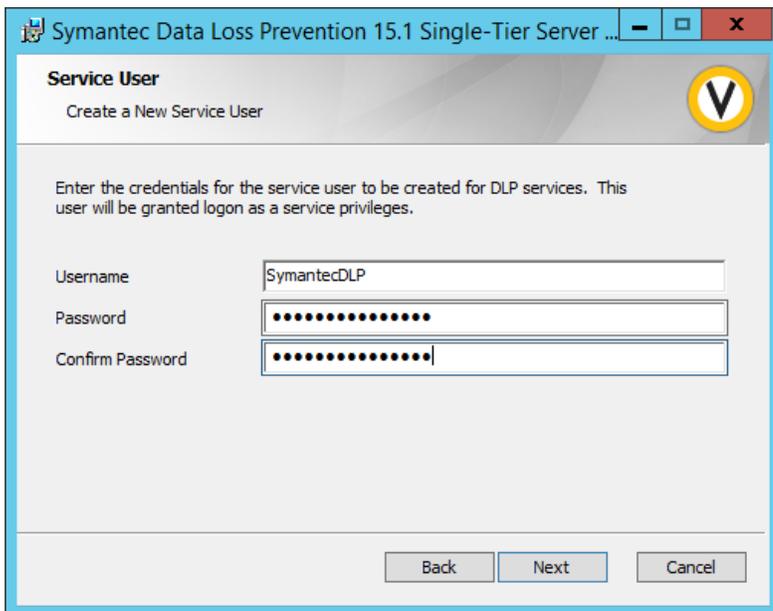


15. Click **Next**.

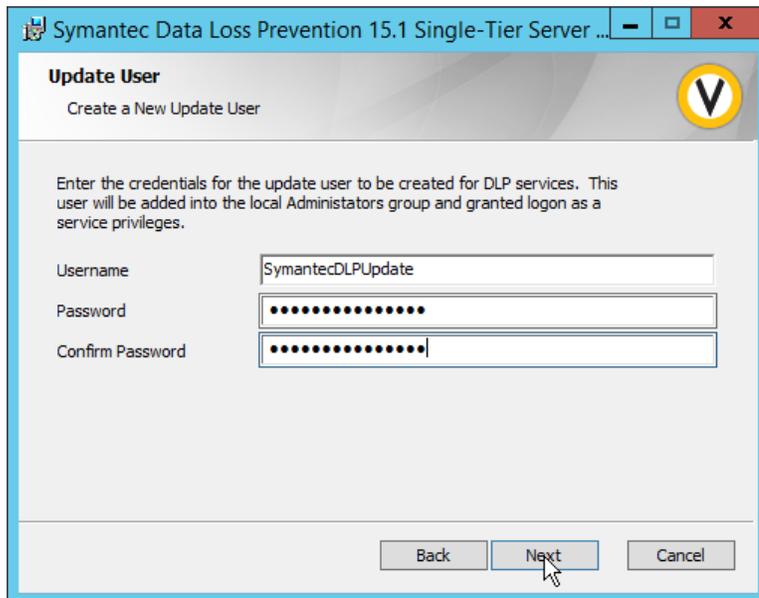
16. Click on **New Users**.



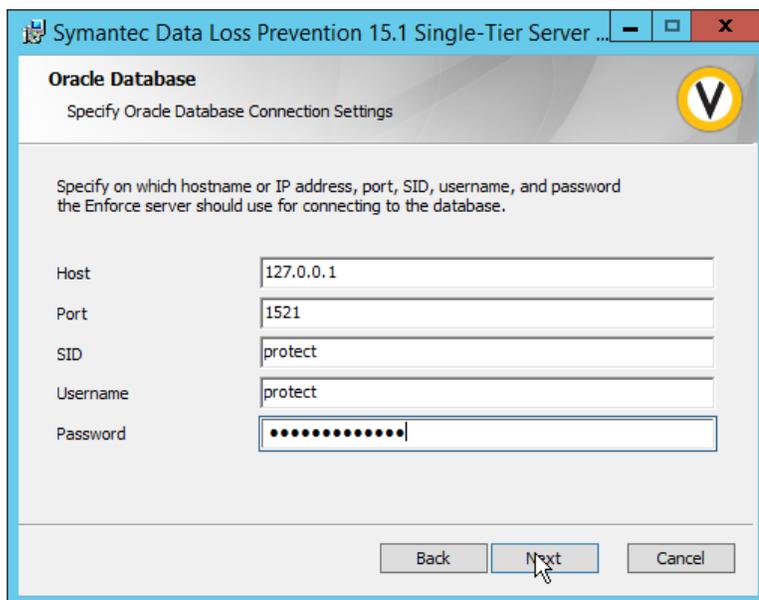
17. Click **Next**.
18. Enter a **password** and optionally a **username**.



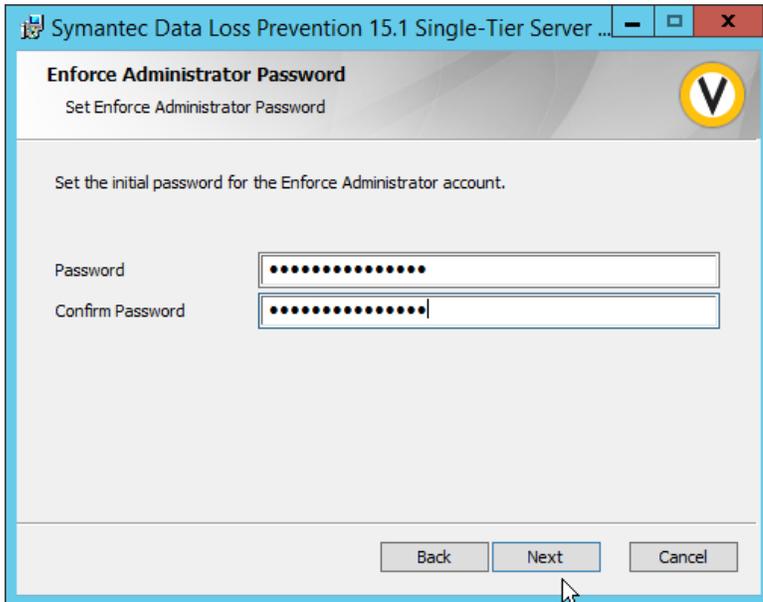
19. Click **Next**.
20. Enter a **password** and optionally a **username**.



21. Click **Next**.
22. Enter the **password** used for the “protect” user.

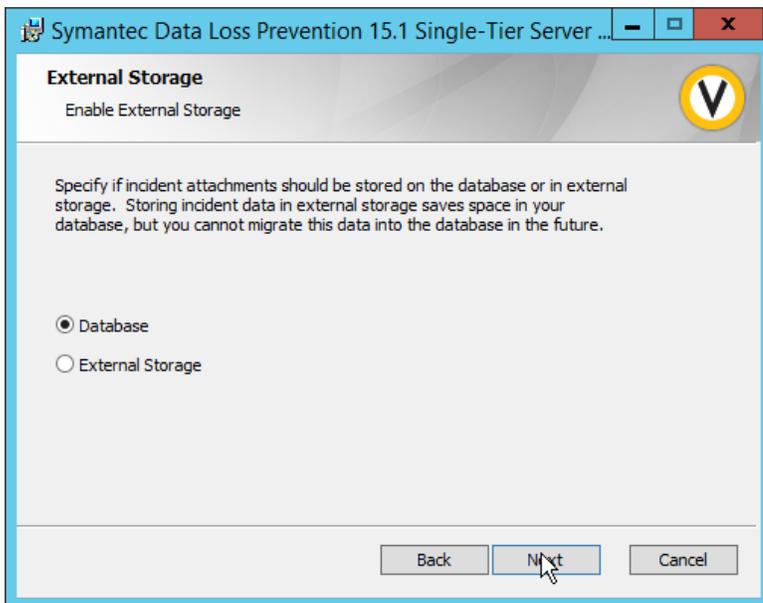


23. Click **Next**.
24. Select **Initialize Database**.
25. Click **Next**.
26. Set the initial **password** for logging into the Enforce Administrator account.



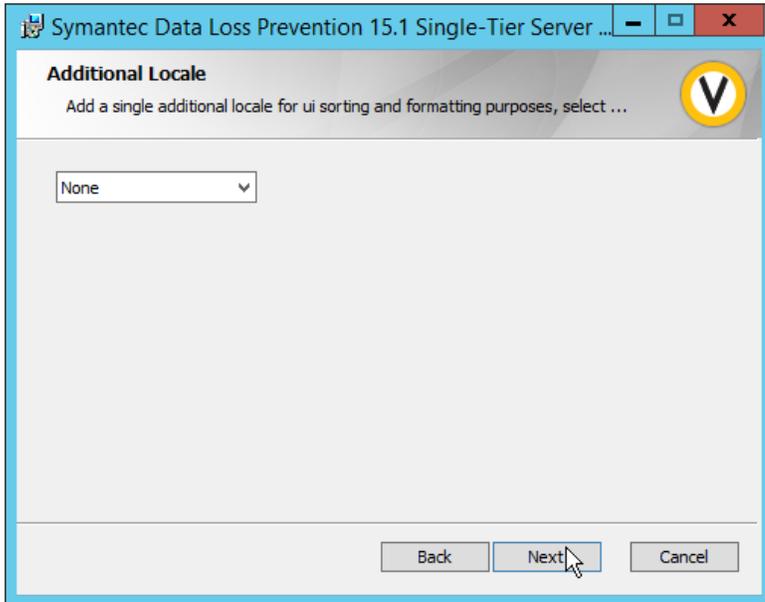
27. Click **Next**.

28. Select **Database**.

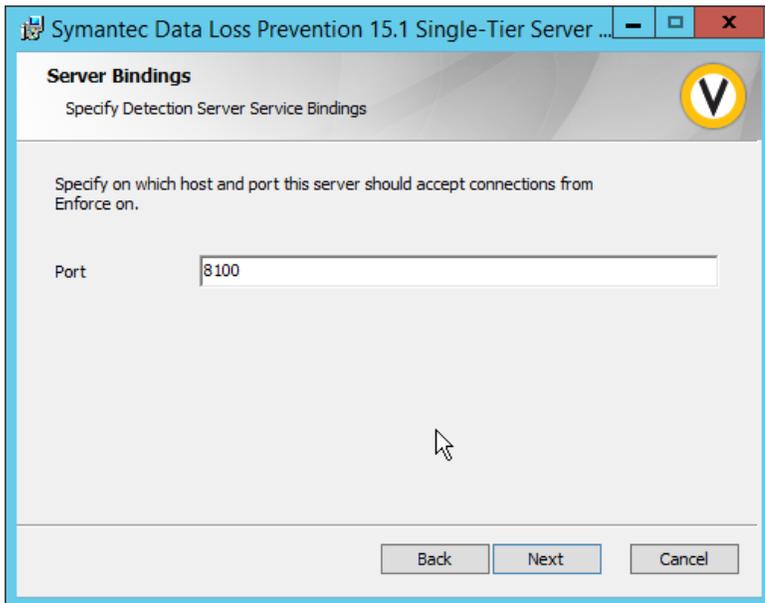


29. Click **Next**.

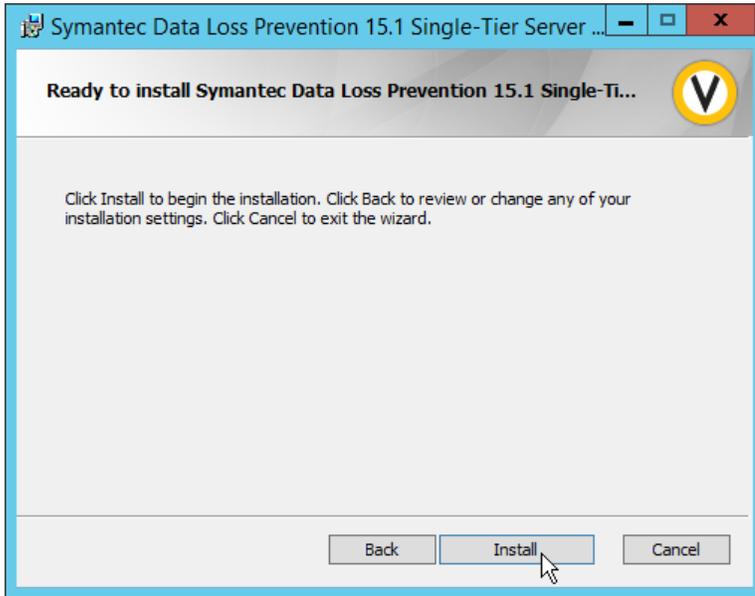
30. Select **None**.



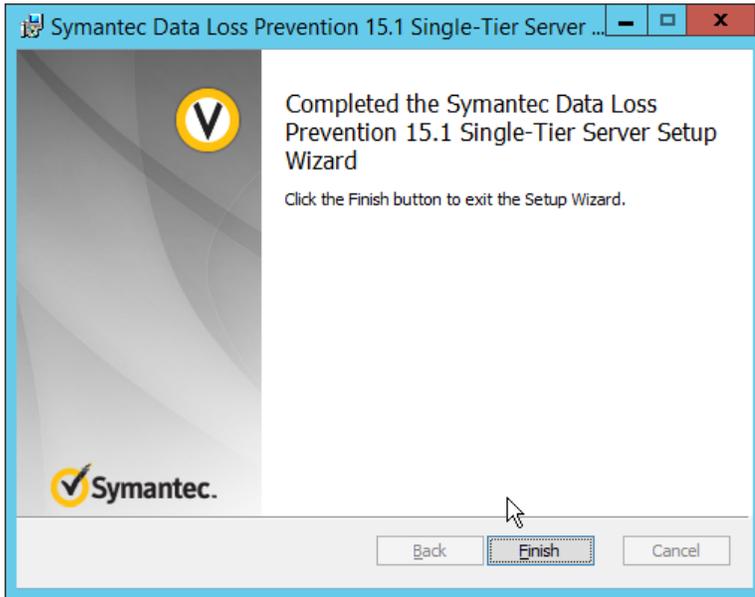
31. Click **Next**.



32. Click **Next**.



33. Click **Install**.



34. Click **Finish**.

35. Ensure that the services are running in Task Manager:

- a. SymantecDLPManager
- b. SymantecDLPIncidentPersister
- c. SymantecDLPNotifier

d. SymantecDLPDetectionServer

2.15.5 Configure Symantec DLP

1. Navigate to <https://127.0.0.1> in the browser to get to the Symantec DLP web console.
2. Navigate to **System > Settings > General** and click **Configure**.
3. In the **Edit General Settings** screen, upload your license file provided by Symantec.
4. Click **Save**.
5. In Task Manager, stop the **SymantecDLPManager** service.
6. Copy the *classpath.txt* file located in **<DLP Download Home>\DLP\15.1\Solution_Packs** and overwrite the *classpath.txt* located at **C:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\Config\SolutionPackInstaller**.
7. In an administrative command window, use the following commands to import the chosen solution pack. For example, to import the financial solution pack, use:

```
> cd "C:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\protect\bin"
```

```
> .\SolutionPackInstaller.exe import "C:\Program Files\Symantec\Data Loss Prevention\Financial_v15.1.vsp"
```

8. After this is installed, restart the **SymantecDLPManager** service.
9. Log on to the Enforce Web Console as Administrator.
10. Navigate to **System > Servers > Overview**.
11. Click **Add Server**.
12. Select the type of Detection Server to add.
13. Click **Next**.
14. Enter a **name**.
15. Enter the **hostname** of the DLP server.
16. Enter **8100** for the **port**.
17. Navigate to **System > Settings > General**.

Process Control

Advanced Process Control



18. Check the box next to **Advanced Process Control**.
19. Specify any configuration options according to the needs of your organization.
20. Click **Save**.

2.16 Cisco Identity Services Engine

This section details the installation and some configurations for the Cisco Identity Services Engine (ISE). It assumes the use of the ISE virtual machine.

2.16.1 Initial Setup

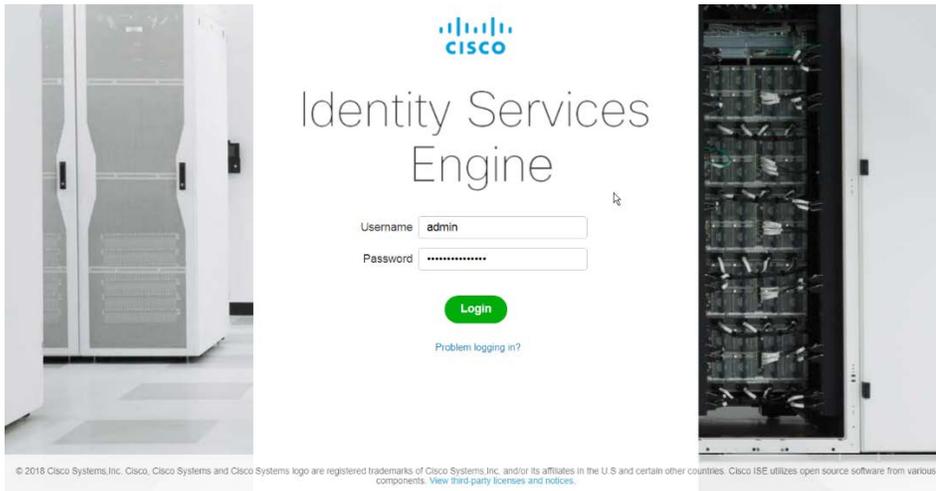
1. When prompted to log in for the first time, enter `setup`. (You can use the command `reset-config` to change these values later.)
2. Enter the desired **hostname** for the machine.
3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated with this IP address in your DNS.)
4. Enter the **netmask** for the machine.
5. Enter the **default gateway**.
6. Enter the **default DNS domain** (the name of your domain).
7. Enter the **primary nameserver** (the IP address of your DNS).
8. Enter a second nameserver if desired.
9. Enter a **Network Time Protocol (NTP) time server**.
10. Enter the **timezone**.
11. Enter **Y** for **SSH service**.
12. Enter an administrator **username** for the machine.
13. Enter a **password** twice.

2.16.2 Inventory: Configure SNMP on Routers/Network Devices

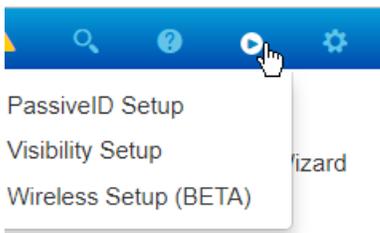
See the corresponding vendor documentation for the correct way to enable Simple Network Management Protocol (SNMP) on your network device. Ensure that the community string you choose is considered sensitive, like a password.

2.16.3 Inventory: Configure Device Detection

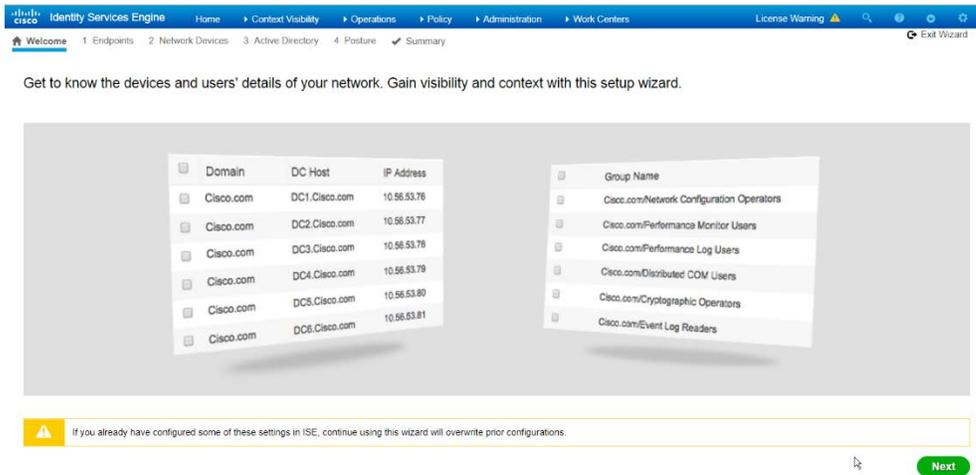
1. Log in to the web client by visiting `https://hostname/admin` but replace **hostname** with the hostname of the ISE machine.



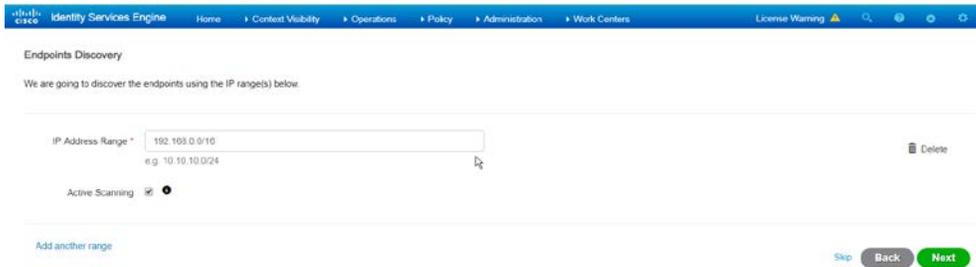
2. On the top right, use the small Play button to select **Visibility Setup**.



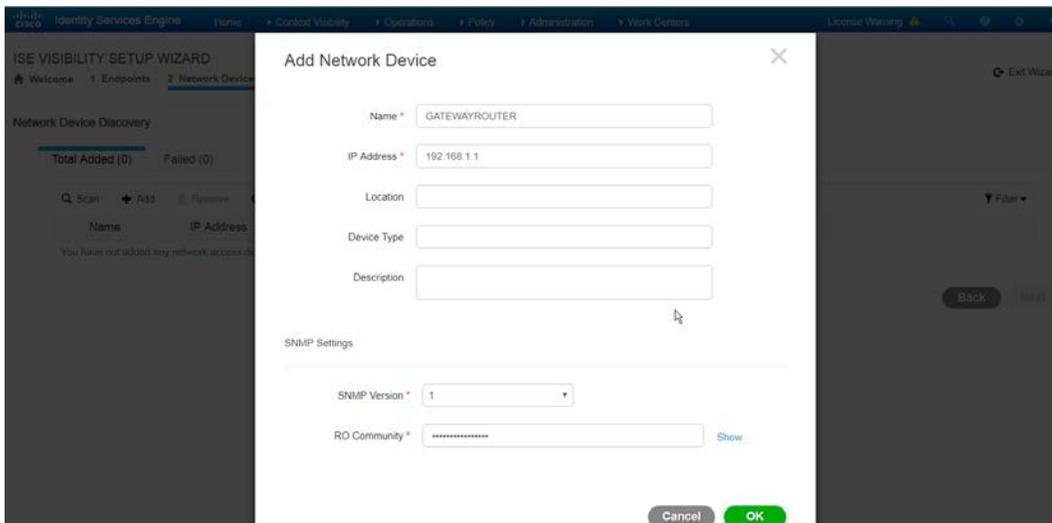
3. Click **Next**.



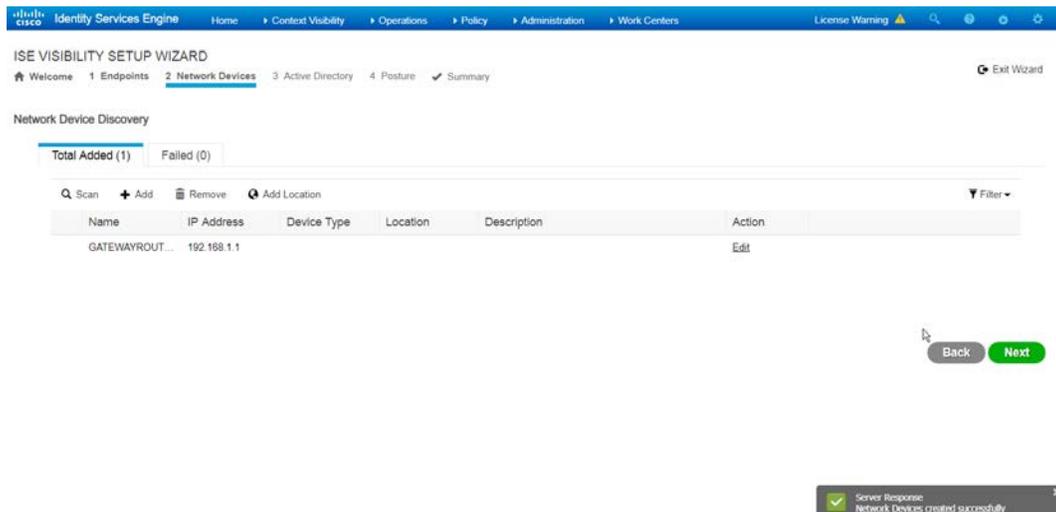
4. Enter the range of IP addresses to add to ISE's inventory.
5. Ensure that **Active Scanning** is checked.



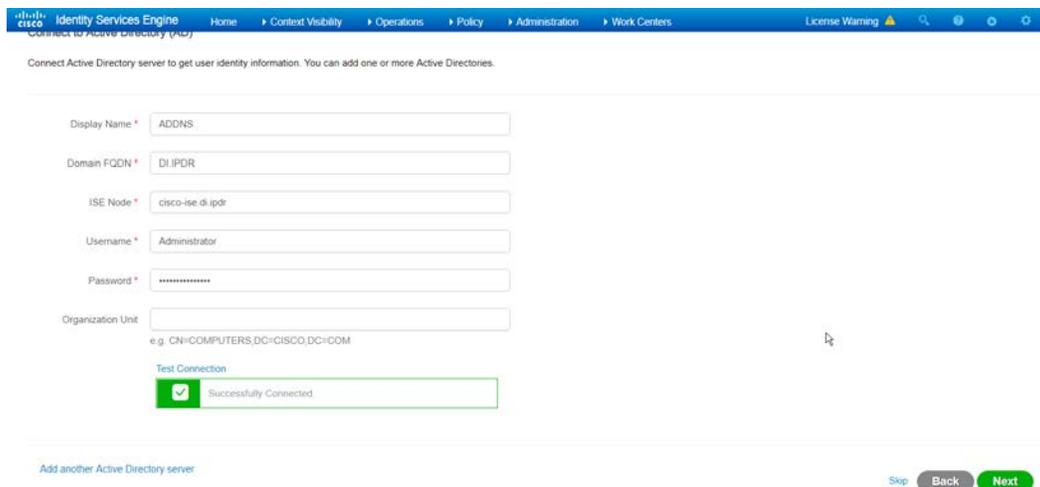
6. Click **Next**.
7. Click the **Add Device Manually** link.
8. Enter a **name**.
9. Enter the **IP address** of the network device you configured for SNMP.
10. Select **1** for **SNMP version**.
11. Enter the **community string** you created.



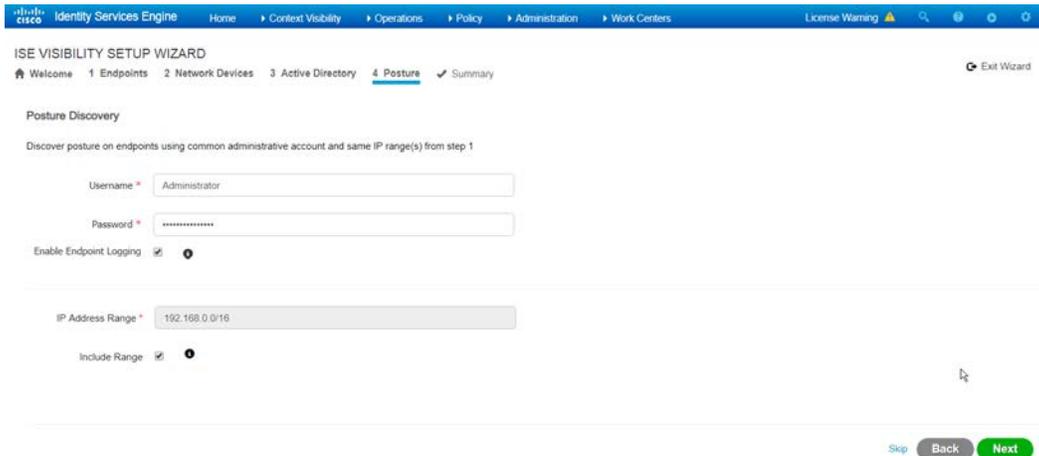
12. Click **OK**.



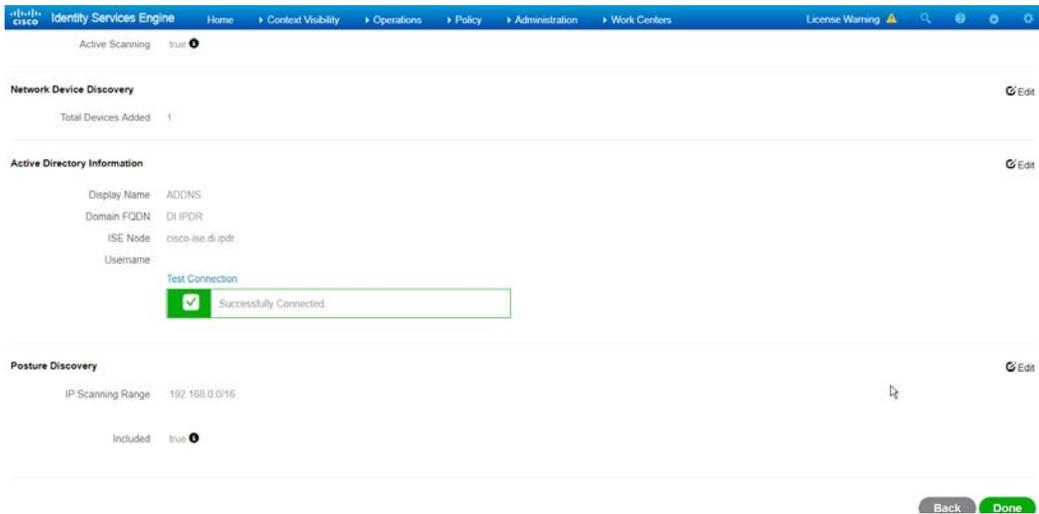
13. Click **Next**.
14. Enter a **display name**.
15. Enter the **domain name**.
16. Enter the **hostname** of Cisco ISE.
17. Enter a **username** and **password**.
18. Click **Test Connection** to ensure that this works.



19. Click **Next**.
20. Enter a **username** and **password**.
21. Check the box next to **Enable Endpoint Logging**.
22. Check the box next to **Include Range**.



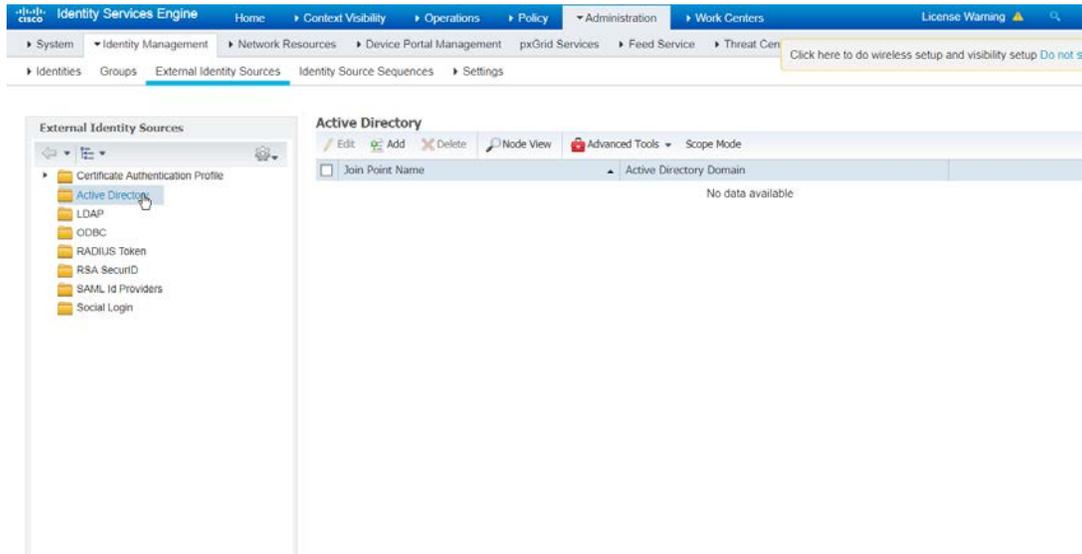
23. Click **Next**.



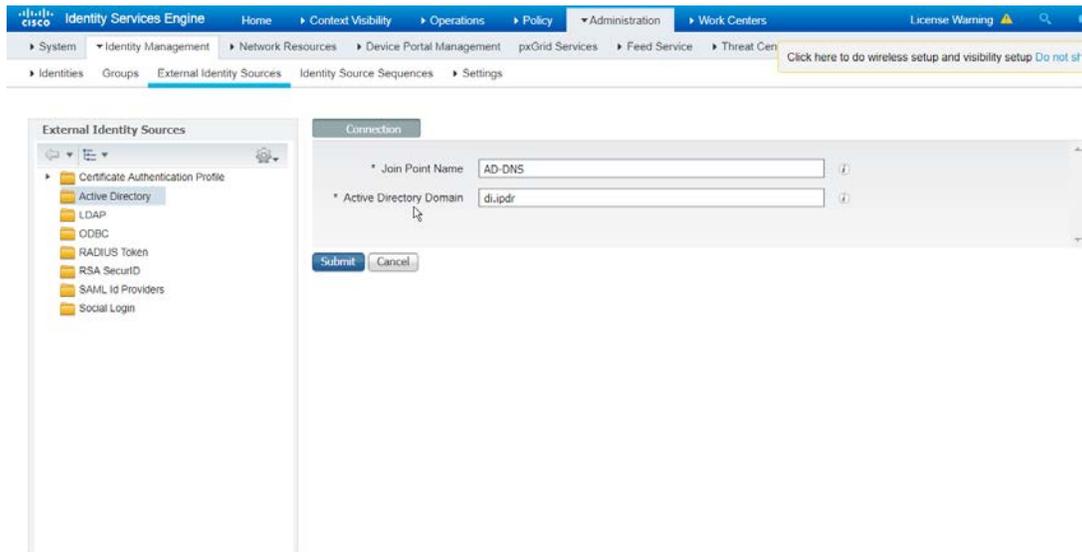
24. Verify the settings and click **Done**. (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

2.16.4 Policy Enforcement: Configure Active Directory Integration

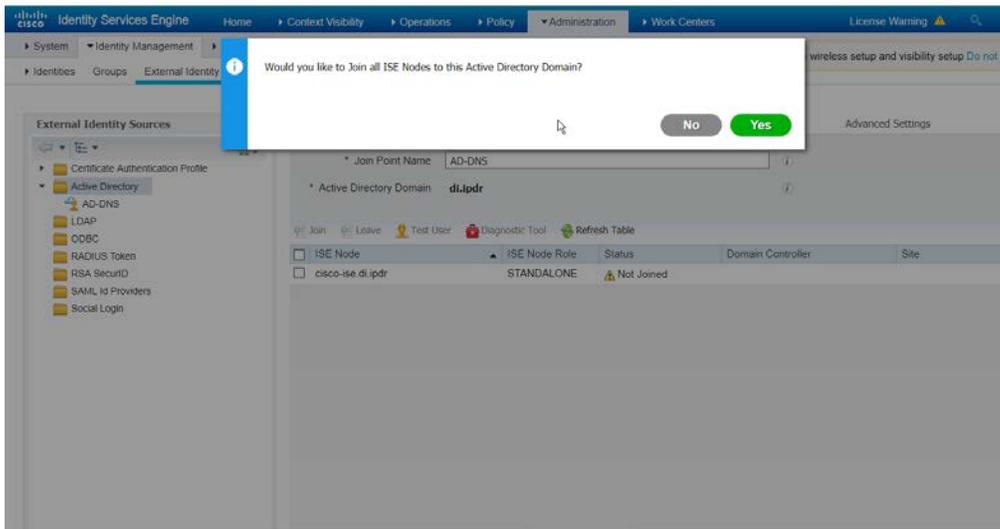
1. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.



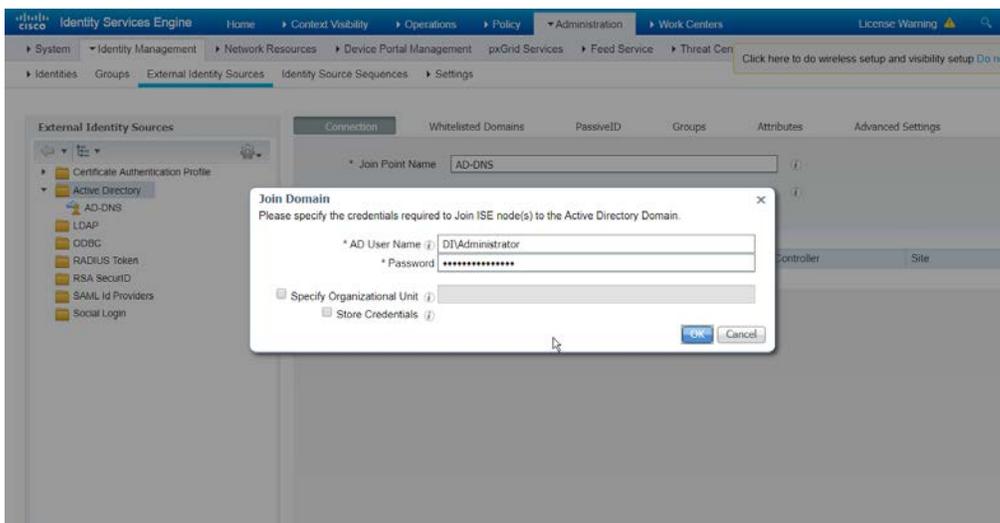
2. Click **Add**.
3. Enter a **name**.
4. Enter the **domain**.



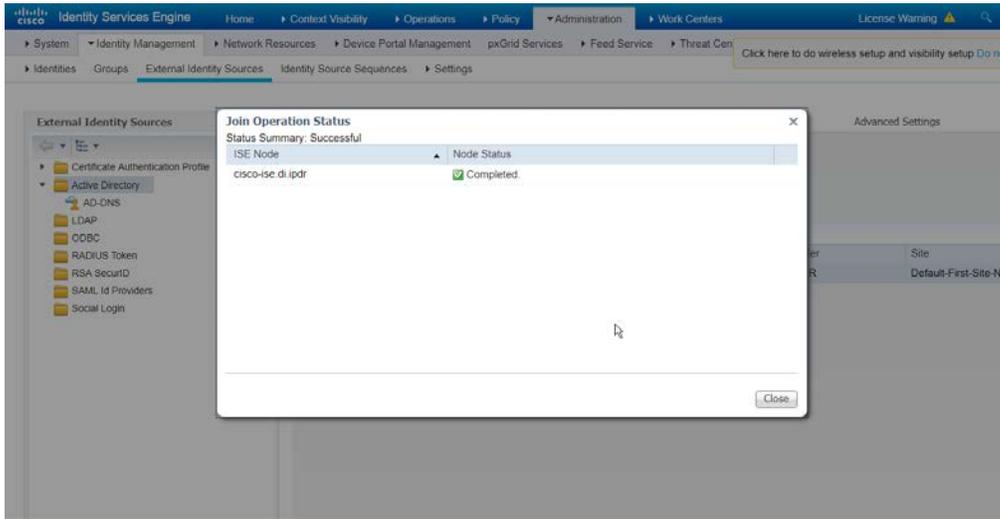
5. Click **Submit**.



6. Click **Yes**.
7. Enter a **username** and **password** to join ISE to the domain.



8. Click **OK**.

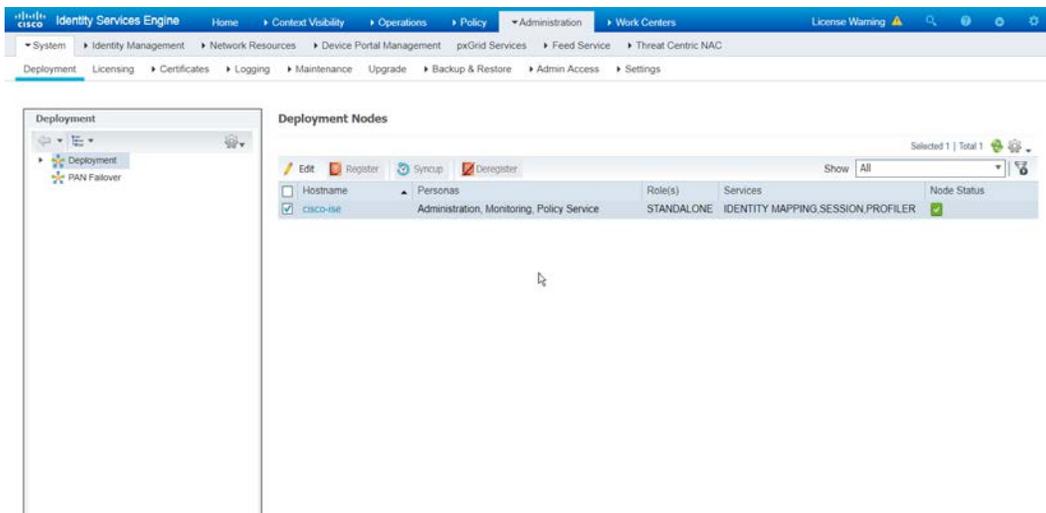


9. Click **Close** when the join is finished.

2.16.5 Policy Enforcement: Enable Passive Identity with AD

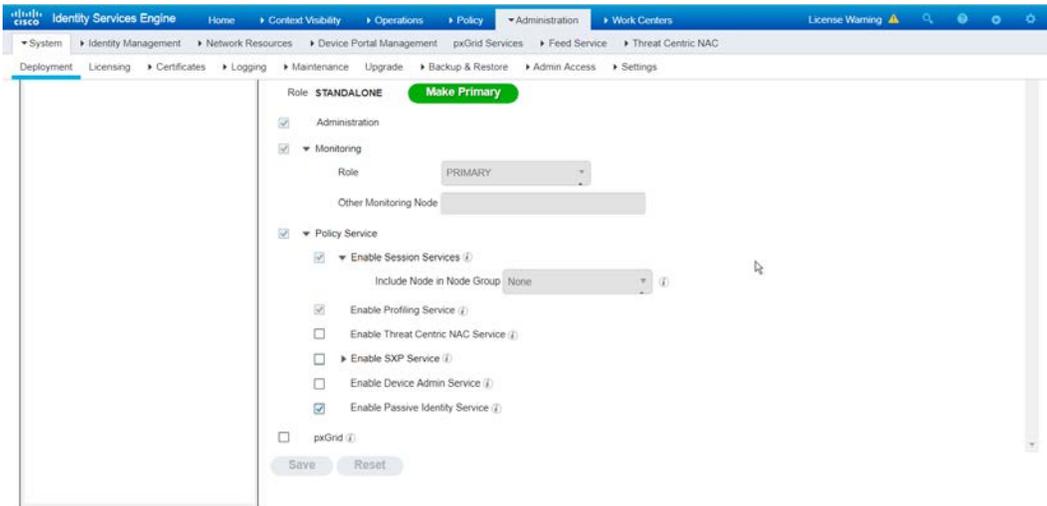
This configuration allows users to use Active Directory usernames/passwords as authentication for the portal. The web portal will allow clients to download profiling software to ensure that clients have up to date software and can be trusted on the network.

1. Navigate to **Administration > System > Deployment**.
2. Check the box next to ISE.



3. Click **Edit**.

4. Check the box next to **Enable Passive Identity Service**.

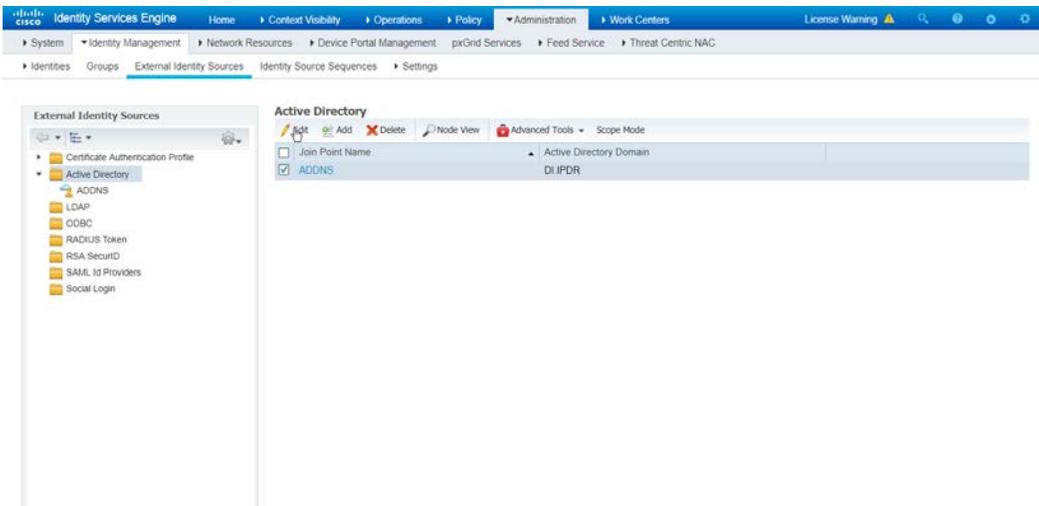


5. Click **Save**.

6. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.

7. Click the name of the Active Directory machine.

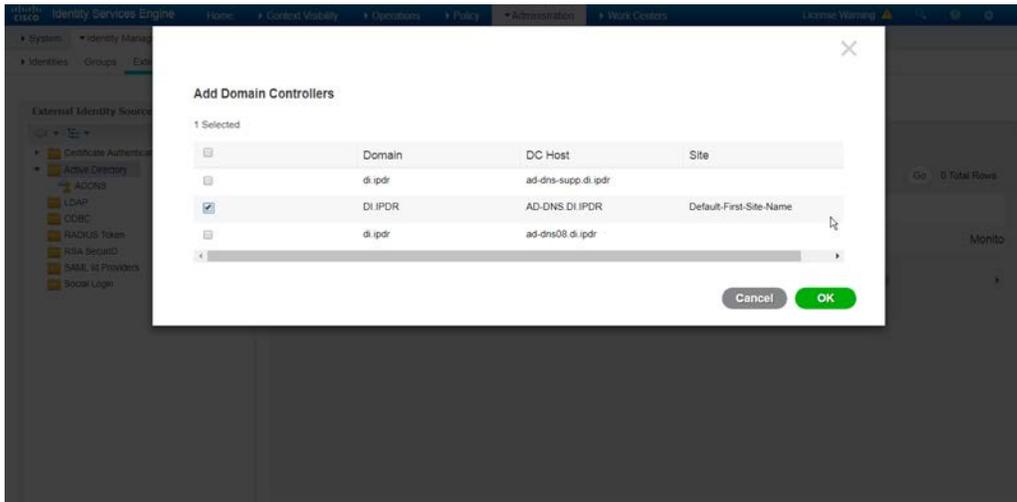
8. Check the box next to the join point you just created.



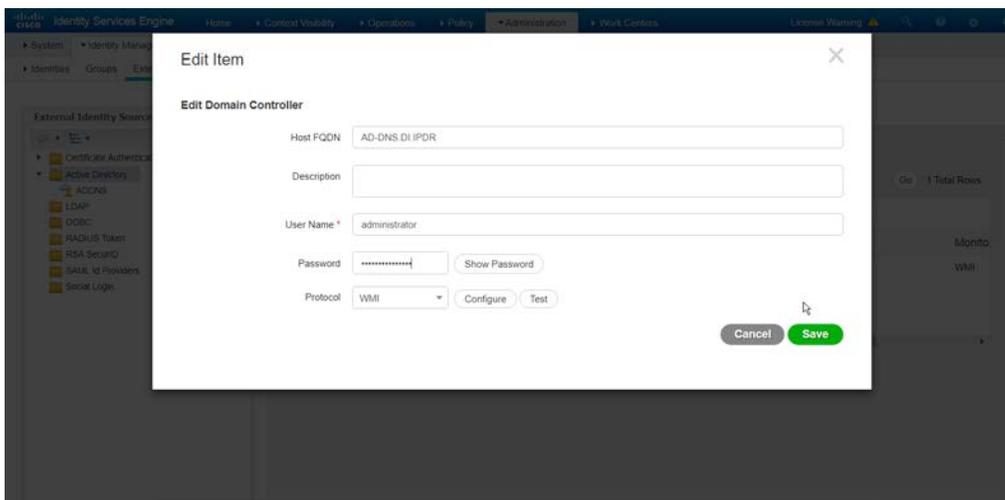
9. Click **Edit**.

10. Click the **PassiveID** tab.

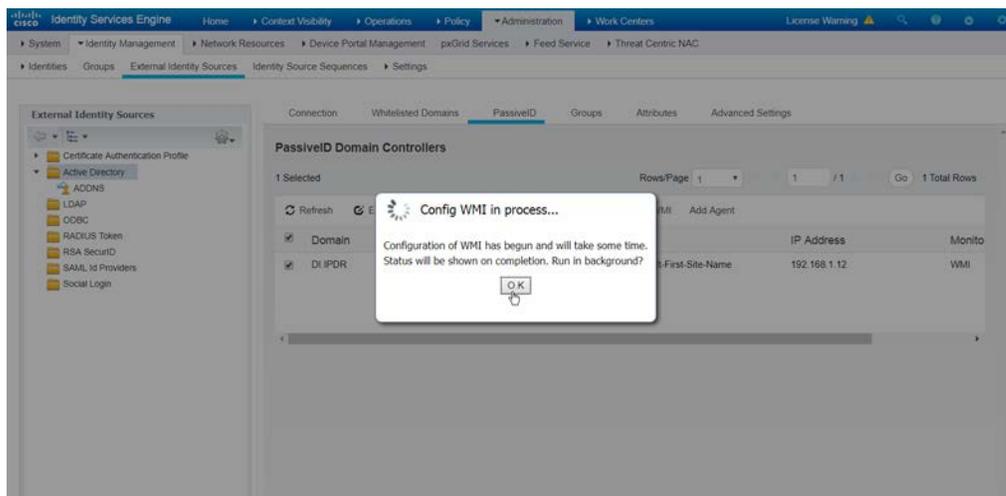
11. Click **Add DCs** if there are no domain controllers listed.



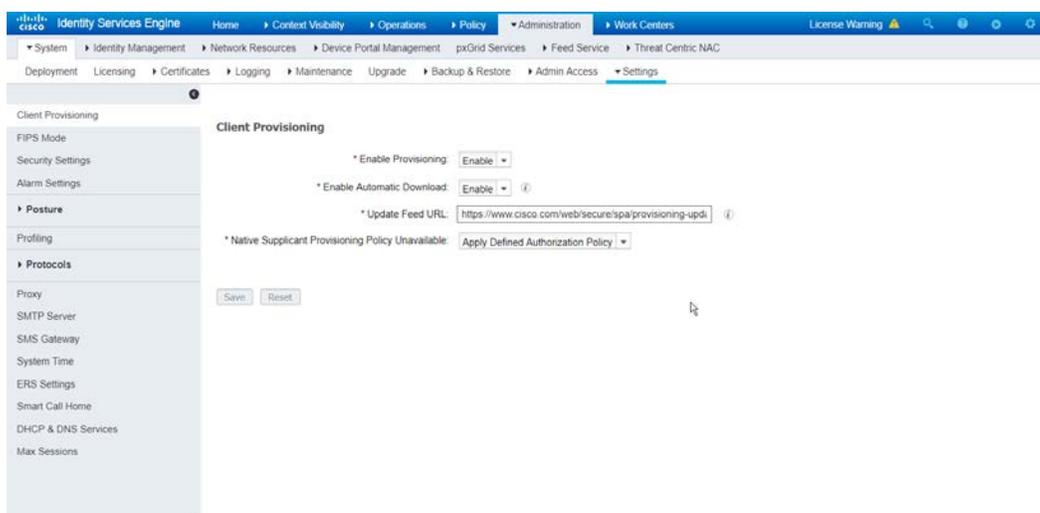
12. Select the Active Directory domain controller.
13. Click **OK**.
14. Check the box next to the selected domain controller.
15. Click **Edit**.
16. Enter credentials for an administrator account.



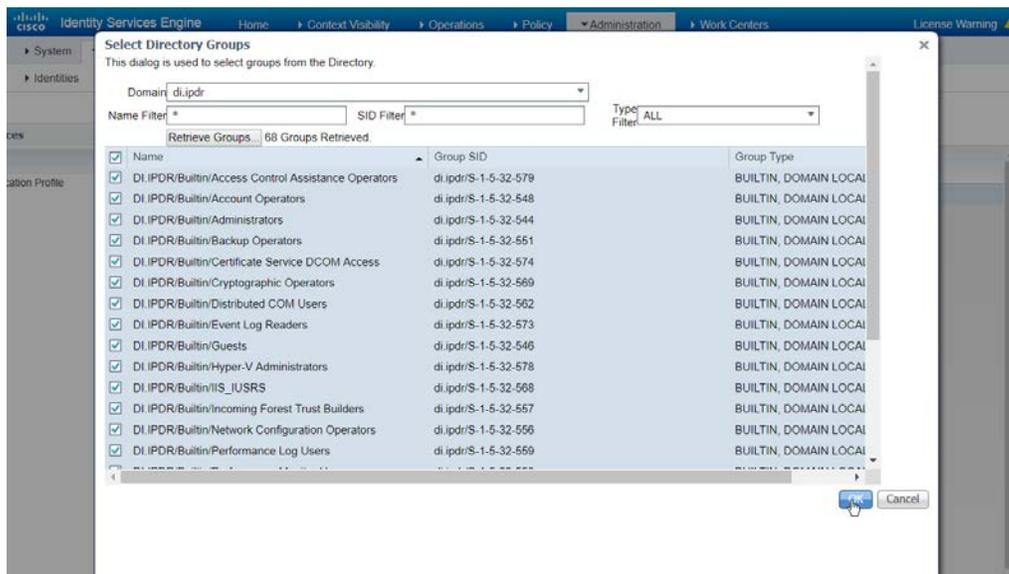
17. Click **Save**.
18. Click **Config WMI**.
19. Click **OK**.



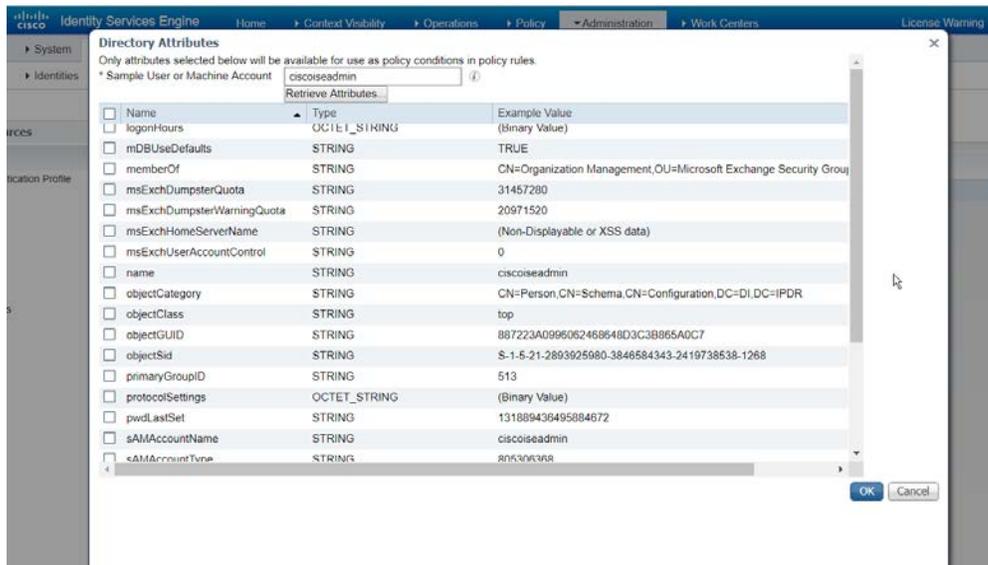
20. Click **OK** when this configuration finishes.
21. Navigate to **Administration > System > Settings > Client Provisioning**.
22. Set **Enable Automatic Download** to **Enable**.



23. Click **Save**.
24. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.
25. Click the **Groups** tab.
26. Click **Add > Select Groups from Directory**.
27. Click **Retrieve Groups**. (This should populate the window with the groups from Active Directory.)
28. Select them all.



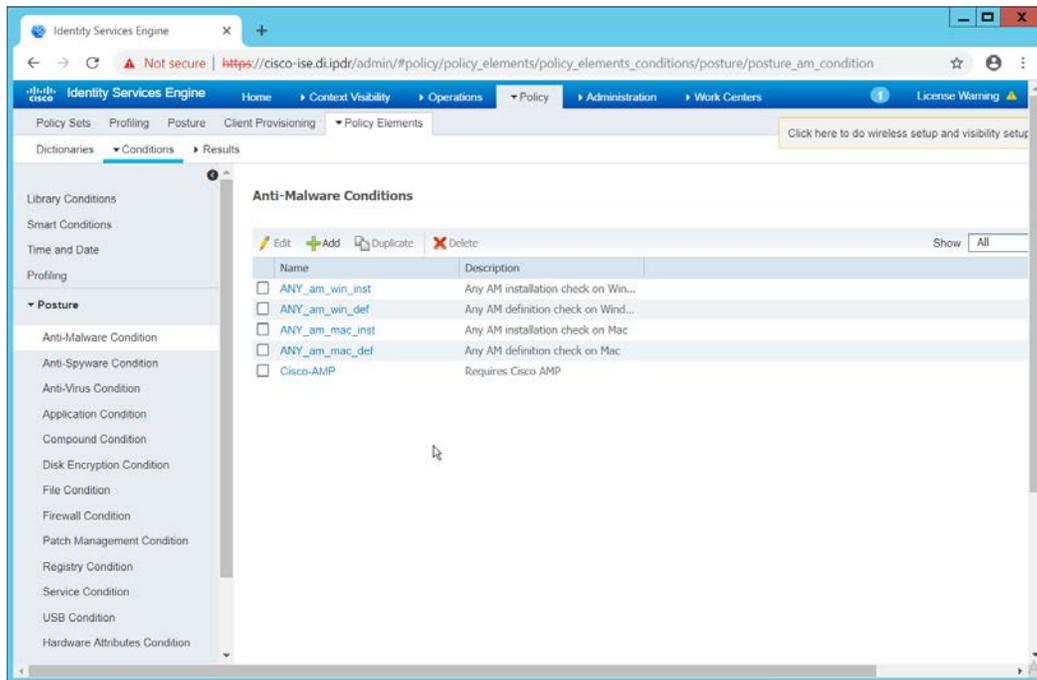
29. Click **OK**. (If you add more groups to Active Directory they can be imported in the same way in the future.)
30. Click the **Attributes** tab.
31. Click **Add > Select Attributes from Directory**.
32. Enter a **username**.
33. Click **Retrieve Attributes**. (This will populate the window with Active Directory's available attributes, so they can be used for policy in Cisco ISE.)
34. Click **OK**.
35. Select any desired attributes.



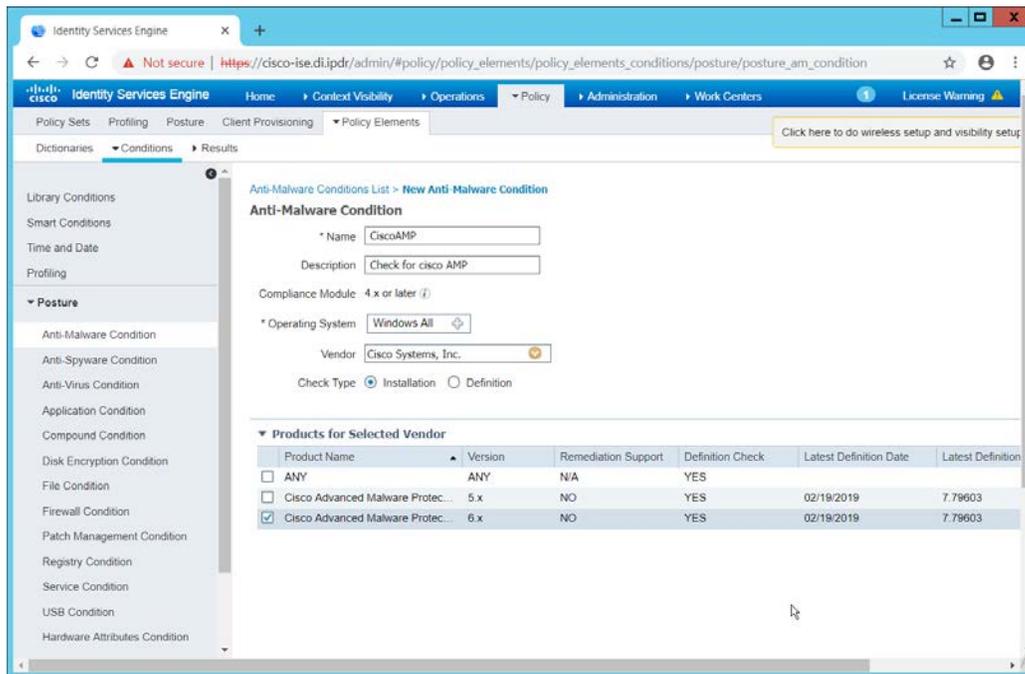
36. Click **OK**.
37. Click **Save**.

2.16.6 Policy Enforcement: Developing Policy Conditions

1. Navigate to **Policy > Policy Elements > Conditions > Posture**.
2. Expand the **Posture** section. This will reveal a list of categories for conditions. (Note: These conditions allow you to select or define requirements that endpoints should meet. In typical enterprises, these conditions can be used as requirements to gain network access—however, this strongly depends on the capabilities of your network device.)
3. As an example, we will require that Cisco AMP be installed on all Windows devices. If you are using a different anti-malware software, locate that instead. Click **Anti-Malware Condition**.



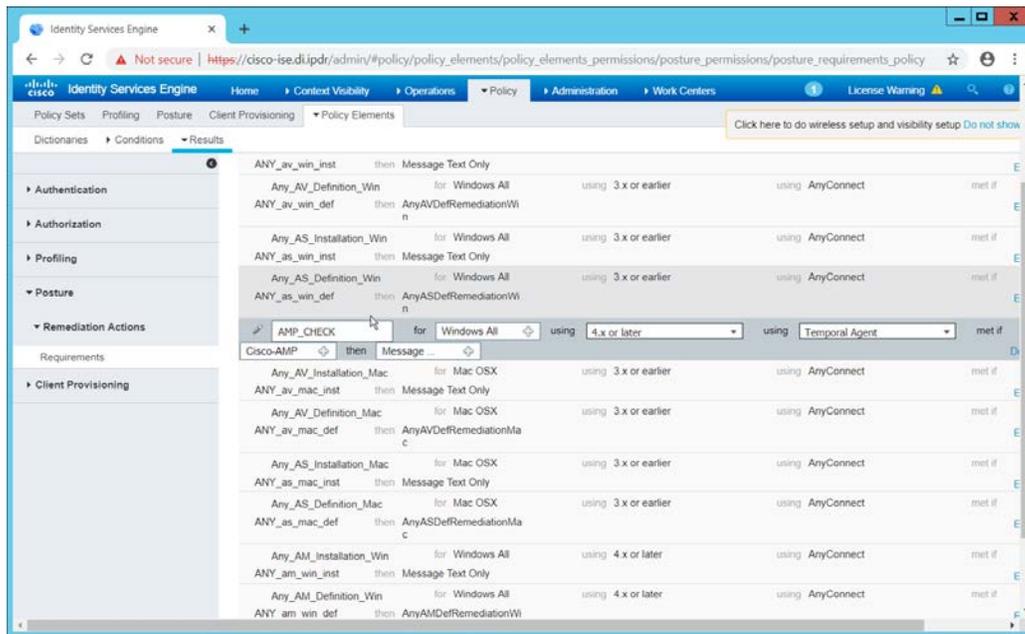
4. Click **Add**.
5. Enter a **name**.
6. Enter a **description** if desired.
7. Select **Windows All** for **Operating System**.
8. Select **Cisco Systems, Inc.** for **Vendor**.
9. Under **Products for Selected Vendor**, check the box next to **Cisco Advanced Malware Protection** with the version number you have installed.



10. Click **Submit**.

2.16.7 Policy Enforcement: Developing Policy Results

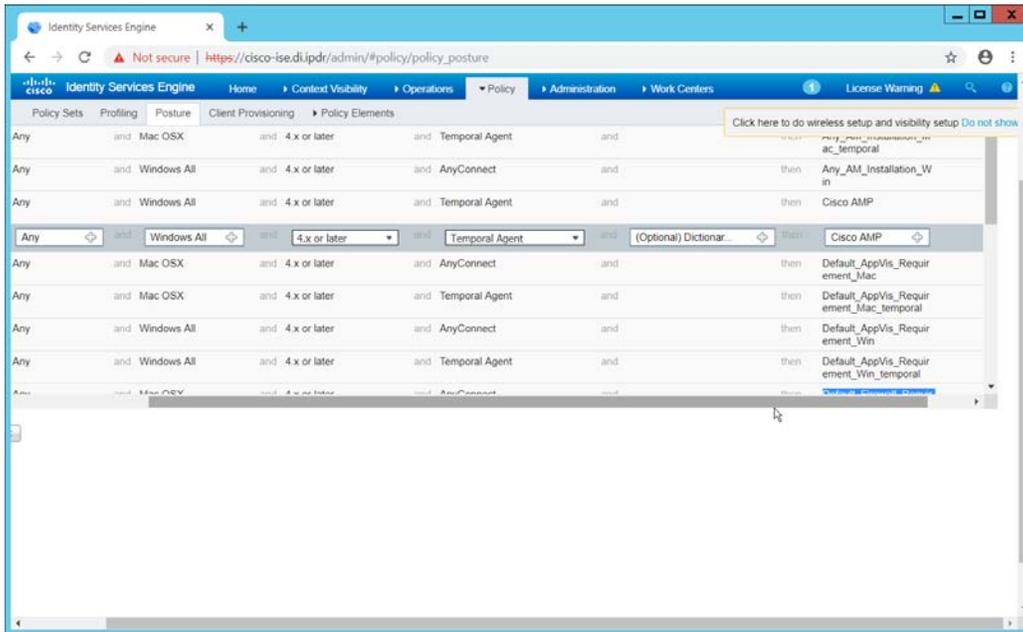
1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements**.
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement**.
3. Enter a **name**.
4. Select **Windows All** for **Operating Systems**.
5. Select **4.x or later** for **Compliance Module**.
6. Select **Temporal Agent** for **Posture**.
7. Select **User Defined Conditions > Anti-Malware Condition > Cisco AMP** (substitute Cisco AMP with the name of the condition you just created).
8. Select **Message Text Only** for the **Remediation Action**. (Other remediation actions can be defined by going to **Policy > Policy Elements > Results > Posture > Remediation Actions**, but there is not an option for Cisco AMP to be installed, so we leave the default for now.)
9. Enter a **Message** to inform the user that they must install Cisco AMP.



10. Click **Save**.

2.16.8 Policy Enforcement: Enforcing a Requirement in Policy

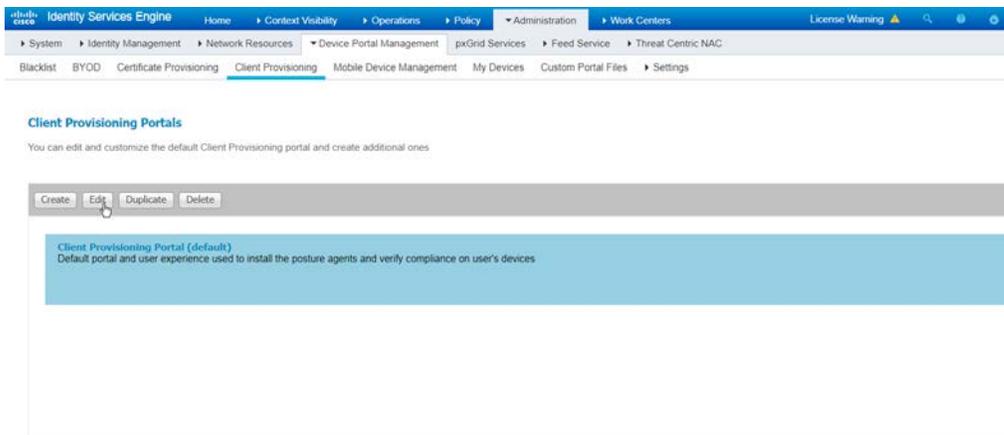
1. Navigate to **Policy > Posture**.
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Policy**.
3. Enter a **name**.
4. Select **Windows All** for **Operating Systems**.
5. Select **4.x or later** for **Compliance Module**.
6. Select **Temporal Agent** for **Posture Type**.
7. Select **Cisco AMP** (substitute Cisco AMP with the name of the requirement you just created).



8. Click **Done**.
9. Ensure that the green checkboxes next to the rules you wish to apply are the only checkboxes enabled, as anything enabled will be enforced.

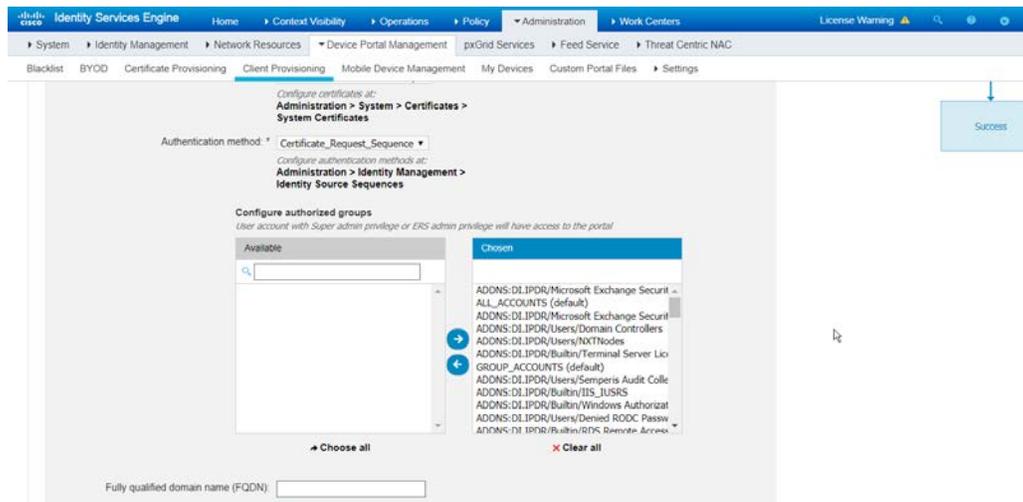
2.16.9 Policy Enforcement: Configuring a Web Portal

1. Navigate to **Administration > Device Portal Management > Client Provisioning**.
2. Select the **Client Provisioning Portal (default)**.



3. Click **Edit**.

4. Under **Portal Settings**, go to **Configure authorized groups** and select the groups that should require a Cisco ISE client.
5. Enter a domain name for **FQDN**, and add it to your DNS.



6. Click **Save**.

2.16.10 Configuring RADIUS with Your Network Device

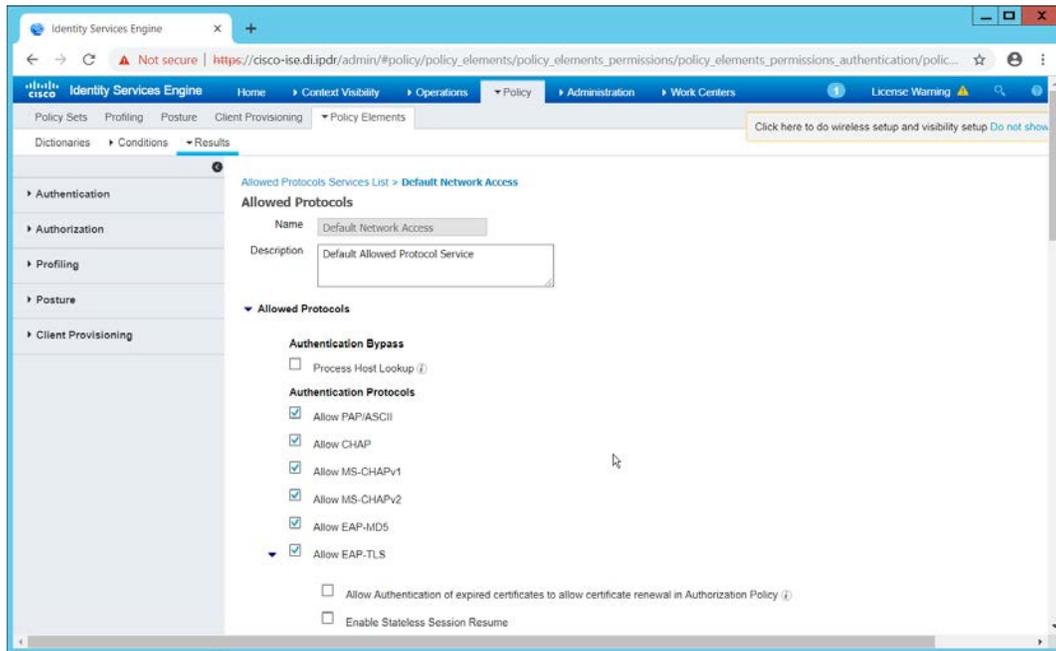
Cisco ISE requires a Remote Authentication Dial-In User Service (RADIUS) session for posture to function. Posture refers to ISE’s ability to check that a machine complies with a specified policy, which may be based on the operating system (OS) and may contain requirements such as installation of certain security applications or the presence of configuration files. Machines that are not in compliance can be kept separated from the network. The process for setting this up varies widely among machines, but the overall requirements have commonalities among systems.

- The **Network Device** (i.e., the router or switch) must support RADIUS functions, specifically **Authentication, Authorization, and Accounting**. Furthermore, it must also support **CoA**, which is **Change of Authorization**. To configure this, you must configure your network device to use Cisco ISE as a RADIUS server. What this means is that your network device will forward authentication requests to Cisco ISE, and Cisco ISE will respond with an “accept” or “reject.”
- The **Network Device** must support some form of **802.1x**. Note that this is not supported on certain routers, even if RADIUS is supported. **802.1x** is a mechanism for authenticating the end workstation to the network device, potentially over wireless or through Ethernet.
 - a. This can take various forms, such as a captive web portal, MAC address authentication, or user authentication. A captive web portal, if the device supports it, may be ideal for configuration without the correct hardware.

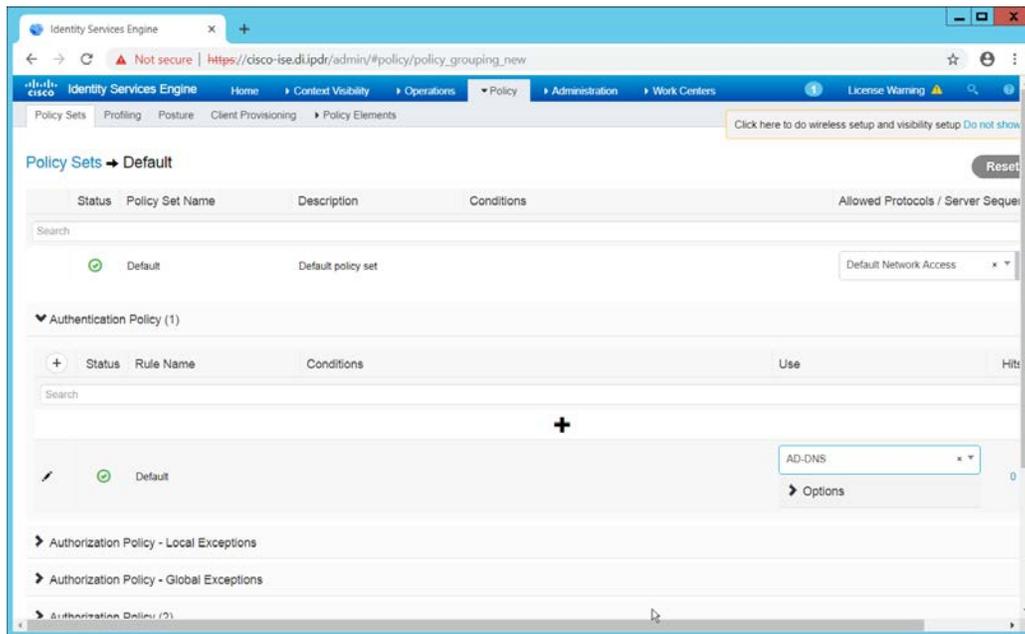
- b. There are also many switches that provide direct 802.1x username/password authentication. Note that if you choose to use this mechanism, a client is still required, and it will not be in the web browser. Windows has a built-in 802.1x client, which can be configured on network adapters under the **Authentication** tab. To enable it, you must first start the service **Wired AutoConfig**, and then the **Authentication** tab will become available for configuration.
 - c. Whatever form of 802.1x is chosen, the request for authentication must be forwarded to Cisco ISE. Cisco ISE will process the request for authentication.
- The two steps above detail the **authentication** phase. Once authenticated, the network device must redirect the user to the client provisioning portal (or to a guest portal), depending on the setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.
 - The user will then authenticate to the **Guest Portal** or **Client Provisioning Portal** (depending on your setup). The portal will prompt the user to download an executable, which will run posture.
 - The executable will *first* check for the existence of a RADIUS session in Cisco ISE for the user who downloaded the executable. It will primarily check the MAC address that visited the ISE web portal against the MAC addresses of existing sessions. *If and only if a session exists*, it will run posture based on the policy you set up. You can verify that a session exists by navigating to **Operations > RADIUS > Live Sessions**.

2.16.11 Configuring an Authentication Policy

1. Navigate to **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.
2. Select the **Default Network Access** protocol or create your own.
3. Ensure that any protocols that need to be supported for your network setup are allowed. In particular, if using 802.1x, it is likely that you should check the box next to **Allow MS-CHAPv2**.



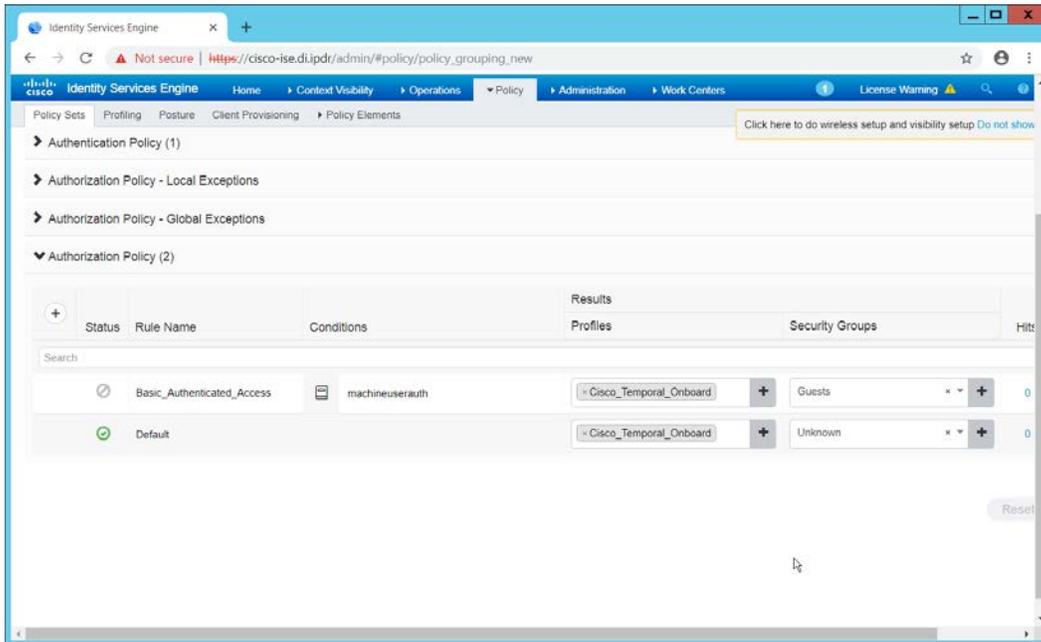
4. Click **Save**.
5. Navigate to **Policy > Policy Sets**.
6. Select the default policy.
7. Ensure that the **Allowed Protocol** selection matches the allowed protocol you just created/edited.
8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate users. For example, if you set up an Active Directory integration, it may be desirable to authenticate users from there.



9. Click **Save**.

2.16.12 Configuring an Authorization Policy

1. The Authorization Profile is likely dependent on your network device, but it is possible that the **Cisco_Temporal_Onboard** profile will work even for non-Cisco devices. You can edit the authorization policy by navigating to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
2. The temporal onboard profile will attempt to redirect the user to a client-provisioning portal. This redirection will most likely happen only automatically on compatible Cisco network devices. If another device is used, the device may need to manually redirect the user to the client-provisioning portal after authentication. (We accomplished this in pfSense for our build by using a “post-authentication redirection” feature in the Captive Portal.)
3. Once you are finished configuring the **Authorization Profile**, navigate to **Policy > Policy Sets**.
4. Select the default policy.
5. Expand the **Authorization Policy** section.
6. Note that you can configure this for as many groups and conditions as desired, potentially specifying different authorization profiles for various user groups or levels of authentication, including unauthenticated access. Under **Results > Profiles**, you can select the authorization profiles you configured.



7. Click **Save**.

2.17 Tripwire IP360

This section details installation and configuration for Tripwire IP360.

2.17.1 Installation

1. Move or copy the Tripwire IP360 Virtual Machine into your virtual environment; start Virtual Machine and observe its successful start-up.

2. Log in using default admin credentials.

```

Running airs-firstboot: [ OK ]
Starting postfix: [ OK ]
Running vnc-airs-firstboot: [ OK ]
Installing Ontology: [ 2789.687610] sched: RT throttling activated [ OK ]

Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Waiting for Tripwire Axon Access Point Gateway.....
running: PID:27875
Starting HAL daemon: [ OK ]
Starting ched: [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory
Starting dbd: [ OK ]
Starting hostd: [ OK ]
Starting objectapixx: [ OK ]
Starting reportd: [ OK ]
Starting vnc-php-fpm: [ OK ]
Starting vnc-airs: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U7.48 and libche: U4.6
Starting imageserver: [ OK ]
Starting httpd: [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cronld: [ OK ]
digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting loader: [ OK ]

Starting incronld: [ OK ]
Starting monit: Cannot translate 'vnc-934358a2' to FQDN name -- Name or service not known
Generated unique Monit id fdc3ed1c4764a7a1c25183899c9e128a and stored to '/var/monit/id'
Starting Monit 5.14 daemon with http interface at [localhost]:2812 [ OK ]

Starting ntlmups:

Tripwire Appliance
vnc-934358a2 login:

Tripwire Appliance
vnc-934358a2 login: admin
Password: _

```

3. When prompted after initial login, set a new password and record it in a safe location.

```

Installing Ontology: [ 2789.687610] sched: RT throttling activated [ OK ]

Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Waiting for Tripwire Axon Access Point Gateway.....
running: PID:27875
Starting HAL daemon: [ OK ]
Starting ched: [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory
Starting dbd: [ OK ]
Starting hostd: [ OK ]
Starting objectapixx: [ OK ]
Starting reportd: [ OK ]
Starting vnc-php-fpm: [ OK ]
Starting vnc-airs: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U7.48 and libche: U4.6
Starting imageserver: [ OK ]
Starting httpd: [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cronld: [ OK ]
digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting loader: [ OK ]

Starting incronld: [ OK ]
Starting monit: Cannot translate 'vnc-934358a2' to FQDN name -- Name or service not known
Generated unique Monit id fdc3ed1c4764a7a1c25183899c9e128a and stored to '/var/monit/id'
Starting Monit 5.14 daemon with http interface at [localhost]:2812 [ OK ]

Starting ntlmups:

Tripwire Appliance
vnc-934358a2 login:

Tripwire Appliance
vnc-934358a2 login: admin
Password:
You must change your password.
This will also change the password for ip360@tripwire.com.
New password:

```

- Use the command **system hostname update <hostname>** to update the system's hostname in accordance with your environment's naming scheme.

```
[ 1.647488] [drm] Max dedicated hypervisor surface memory is 0 kiB
[ 1.647586] [drm] Maximum display memory size is 20488 kiB
[ 1.647799] [drm] VRAM at 0xc0000000 size is 20488 kiB
[ 1.647995] [drm] TTU0 at 0xc0000000 size is 256 kiB
[ 1.648122] [drm] global init.
[ 1.648373] [TTM] Zone kernel: Available graphics memory: 8214352 kiB
[ 1.648544] [TTM] Zone dma32: Available graphics memory: 2897152 kiB
[ 1.648694] [TTM] Initializing pool allocator
[ 1.648837] [TTM] Initializing DMA pool allocator
[ 1.649381] [drm] Supports vblank timestamp caching Rev 2 (21.10.2013).
[ 1.649576] [drm] No driver support for vblank timestamp query.
[ 1.659538] [drm] Screen Target Display device initialized
[ 1.659551] [drm] width 1288
[ 1.659561] [drm] height 768
[ 1.659801] [drm] bpp 32
[ 1.651637] [drm] Fifo max 0x00040000 min 0x00001000 cap 0x000007ff
[ 1.652583] [drm] Using command buffers with DMA pool.
[ 1.652695] [drm] DX: no.
[ 1.656728] [fbcon: sgdmafb (FBD) is primary device
[ 1.659833] Console: switching to colour frame buffer device 160x48
[ 1.672613] [drm] Initialized vmagfx 2.12.0 20170221 for 0000:00:0f:0 on minor 0
[ 1.716876] random: fast init done
[ 1.728549] Floppy device(s): fdd is 1.44M
[ 1.733271] PVE 0 is a post-1991 82877.
[ 1.817166] EXT4-Fs (sda2): mounted filesystem with ordered data mode. Dpts: (null)
[ 1.822838] dracut: Mounted root filesystem /dev/sda2
[ 1.881843] dracut: Switching root
Welcome to Tripwire Appliance
Starting udev: [ 2.251929] udev: starting version 147
[ 2.353284] shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
[ 2.562832] random: crng init done
[ 3.843626] p1vx_smbus 0000:00:07:3: SMBus Host Controller not enabled!
[ 3.851658] vma_vnc1 0000:00:07:7: Found VNC PCI device at 0x1000, irq 16
[ 3.851728] vma_vnc1 0000:00:07:7: Using capabilities 0xc
[ 3.851843] Guest personality initialized and is active
[ 3.851989] VNC host device registered (name=vnc1, major=10, minor=57)
[ 3.852853] Initialized host personality.
[ 3.869249] input: PC Speaker at /devices/platform/pcspkr/input/input5
[ 3.118276] FUJITSU Extended Socket Network Device Driver - version 1.1 - Copyright (c) 2015 FUJITSU LIMITED
[ 3.195277] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 3.195365] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 3.538322] e1000 0000:02:00:0 eth0: (PCI:16MHz:32-bit) 00:50:56:12:3a:b1
[ 3.538615] e1000 0000:02:00:0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.557272] ppdev: user-space parallel port driver
Setting hostname localhost.localdomain: [ OK ]
Checking filesystems: [ OK ]
```

- Use command **network interface update <interface> <IP>/<Broadcast IP>** to update network interface information in accordance with your environment's network.

```
Stopping esentd: [ OK ]
Stopping hostd: [ FAILED ]
Stopping reportd: [ OK ]
Stopping cheserver: [ OK ]
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events [ OK ]
digest_proxy does not need to start
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory [ OK ]
Starting hostd: [ OK ]
Starting reportd: [ OK ]
Starting esentd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U2.40 and libche: U4.6 [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cronpd: [ OK ]
digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting monit: Cannot translate 'vnc-934358a2' to FQDN name -- Name or service not known
Starting Monit 5.14 daemon with http interface at [localhost]:2012 [ OK ]

Tripwire Appliance
vnc-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vnc-934358a2: system hostname update tw360.d1.ipdr
Command succeeded.
vnc-934358a2: network interface update eth0 192.168.1.144/255.255.255.0
[552868.264771] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552868.264771] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552868.275441] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vnc-934358a2: _
```

6. Use command `network route_default create <gateway>` to update the system's default gateway information in accordance with your environment's network.

```
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events [ OK ]
Digest_proxy does not need to start
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events [ OK ]
Starting cheserver? [ OK ]
Configuring PostgreSQL Memory
Starting hostd: [ OK ]
Starting reportd: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nc11b: 07.40 and libche: 04.6
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting croncd: [ OK ]
Digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting monit: Cannot translate 'vne-934358a2' to FQDN name -- Name or service not known
Starting Moinit 5.14 daemon with http interface at [localhost]:2012 [ OK ]

Tripwire Appliance
vne-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vne-934358a2> system hostname update tw360.di.ipdr
Command succeeded.
vne-934358a2> network interface update eth0 192.168.1.144/255.255.255.0
[552860.264771] e1800: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552860.264774] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552860.275411] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> network route_default create 192.168.1.1
[552116.590551] e1800: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552116.603950] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552116.608700] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2>
```

7. Use command **system nameserver create <nameserver IP>** to set up the DNS server.

```
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events          [ OK ]
Starting cheserver:                    [ OK ]
Configuring PostgreSQL Memory
Starting hosts:                        [ OK ]
Starting reports:                     [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U7.40 and libche: U4.6
Starting axon-agent-supervisor:        [ OK ]
Starting axon-data-loader:             [ OK ]
Starting axon-data-transformer:        [ OK ]
Starting axon-stream-listener:         [ OK ]
Starting cron:                         [ OK ]
Digest proxy does not need to start
Starting lifeguard:                    [ OK ]
Starting monit: Cannot translate 'vne-934358a2' to FQDN name -- Name or service not known
Starting Monit 5.14 daemon with http interface at [localhost]:2812
[ OK ]

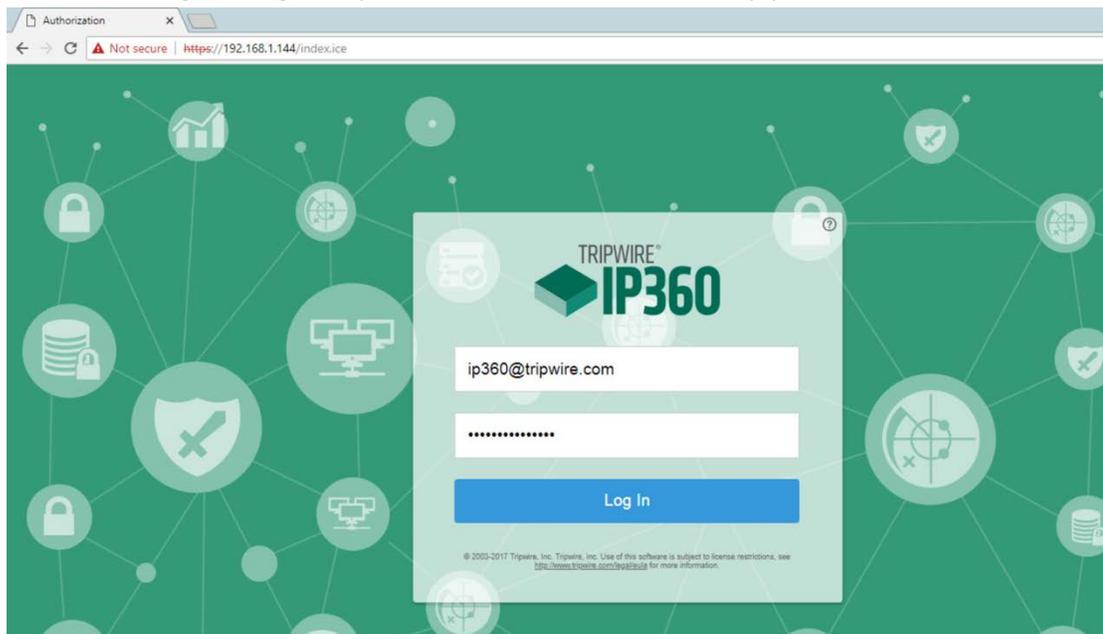
Tripwire Appliance
vne-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vne-934358a2> system hostname update tu360.di.ipdr
Command succeeded.
vne-934358a2> network interface update eth0 192.168.1.144/255.255.255.0
[552869.264771] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552869.264774] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552869.275441] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> network route default create 192.168.1.1
[552116.598551] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552116.603958] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552116.608788] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> system name server create 192.168.1.12
add nameserver.

Usage:
system nameserver create <ip>

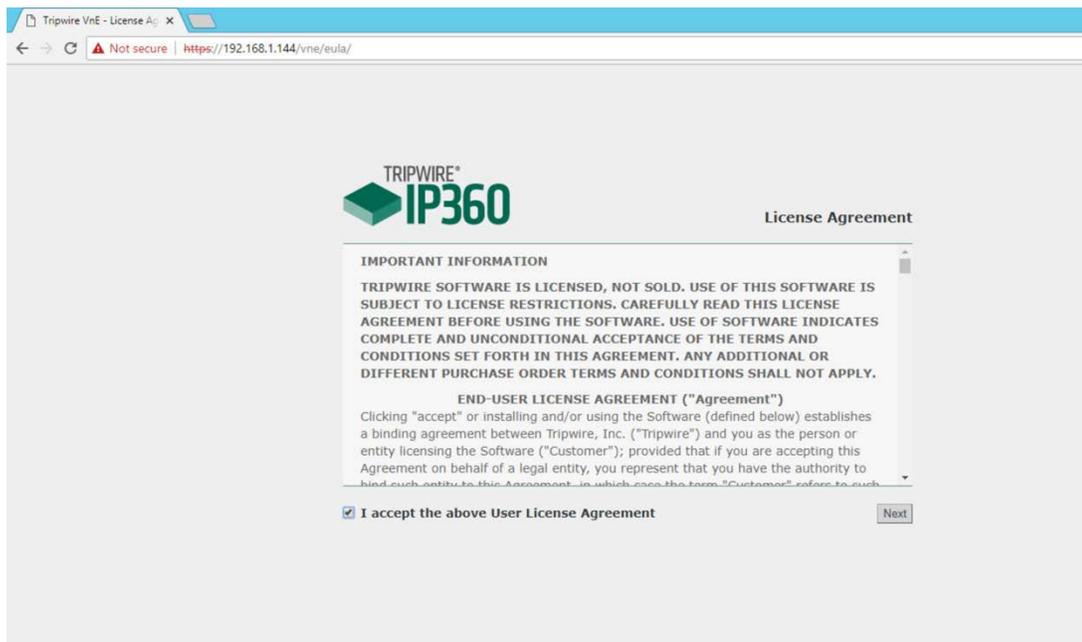
Example:
system nameserver create 192.168.1.2
tu360.di.ipdr> system nameserver create 192.168.1.12
Command succeeded.
tu360.di.ipdr> _
```

2.17.2 Web Portal

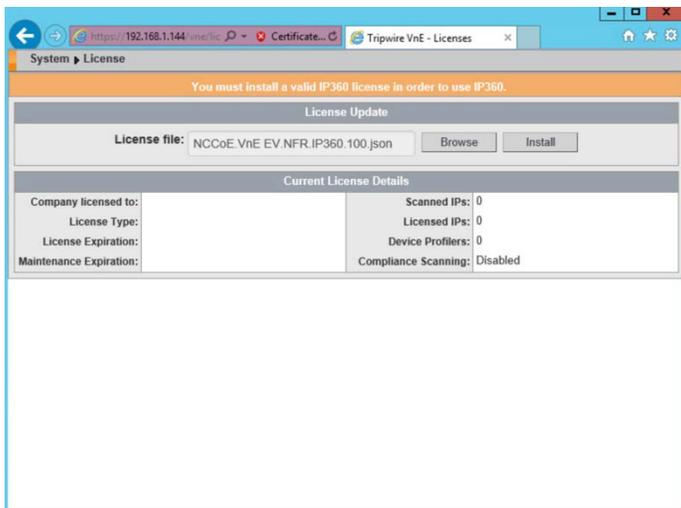
1. From a web browser that can access the newly installed machine's IP address, navigate to the IP address and log in using the updated credentials from the setup process.



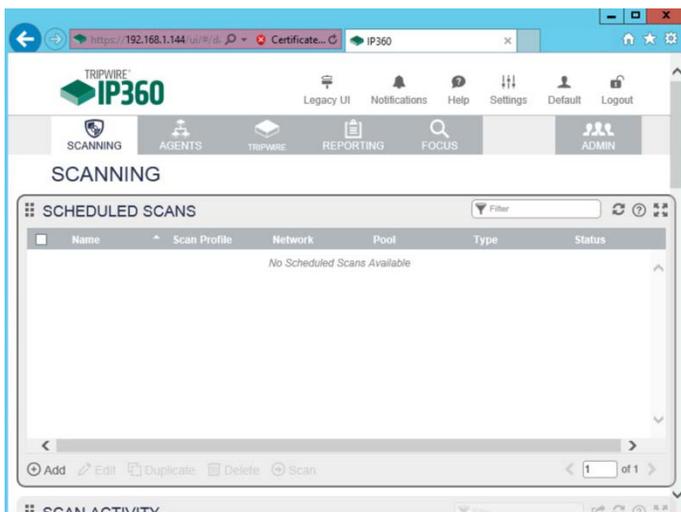
2. Check the box next to **I accept the above User License Agreement.**



3. Click **Next**.
4. Browse to location of downloaded license file.



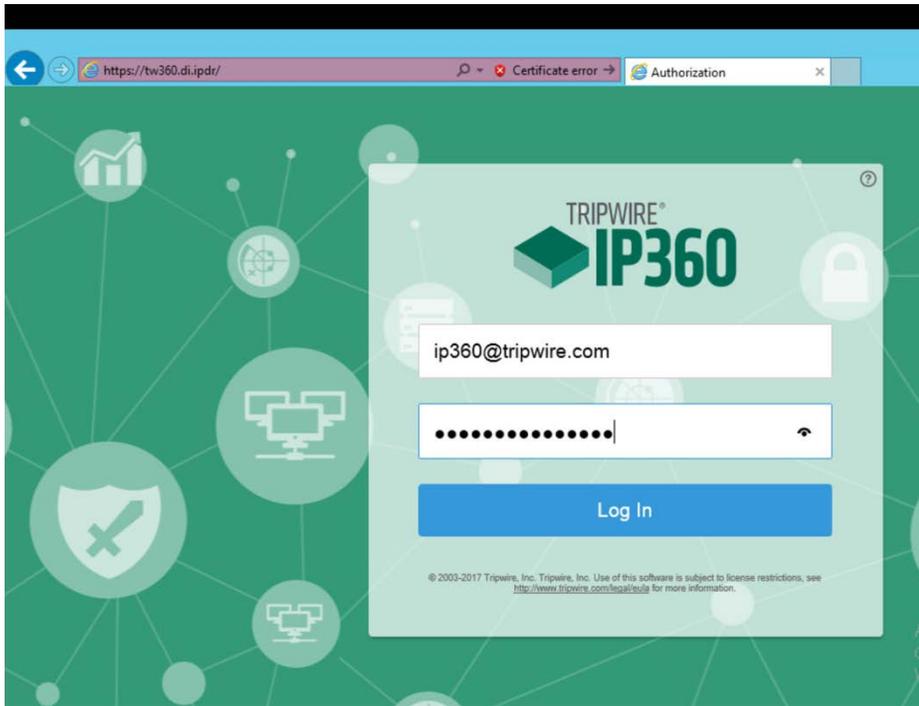
5. Click **Install**.
6. Tripwire IP360 should now be installed and running.



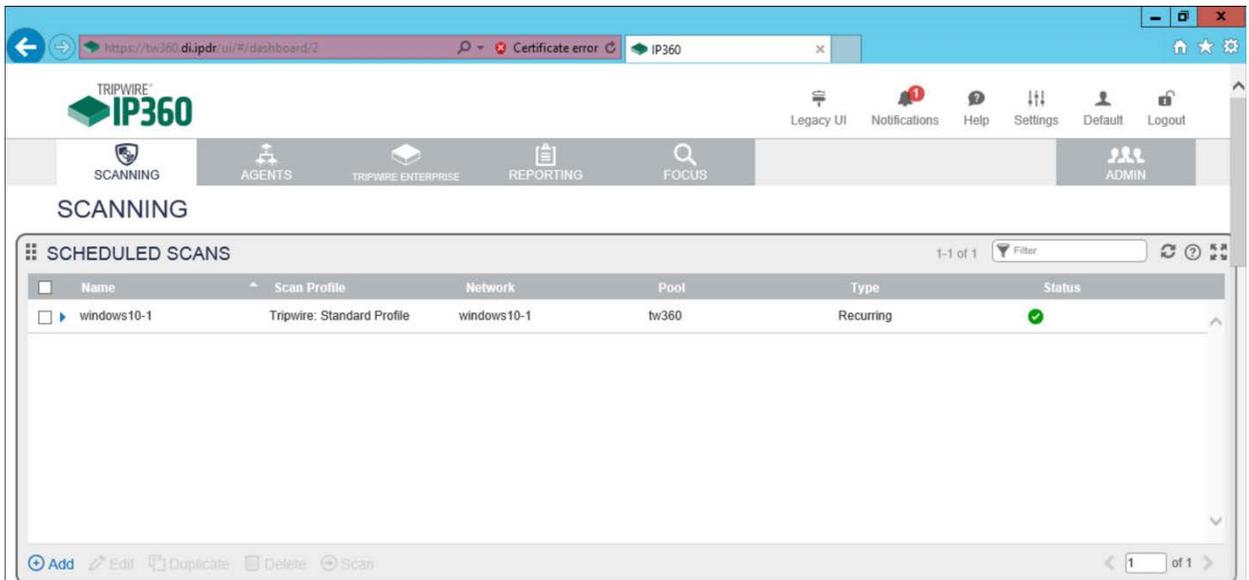
2.17.3 Scanning

This section details instructions for using Tripwire IP360 to run a scan on enterprise systems. The specific details of the scan will vary based on each enterprise’s security needs.

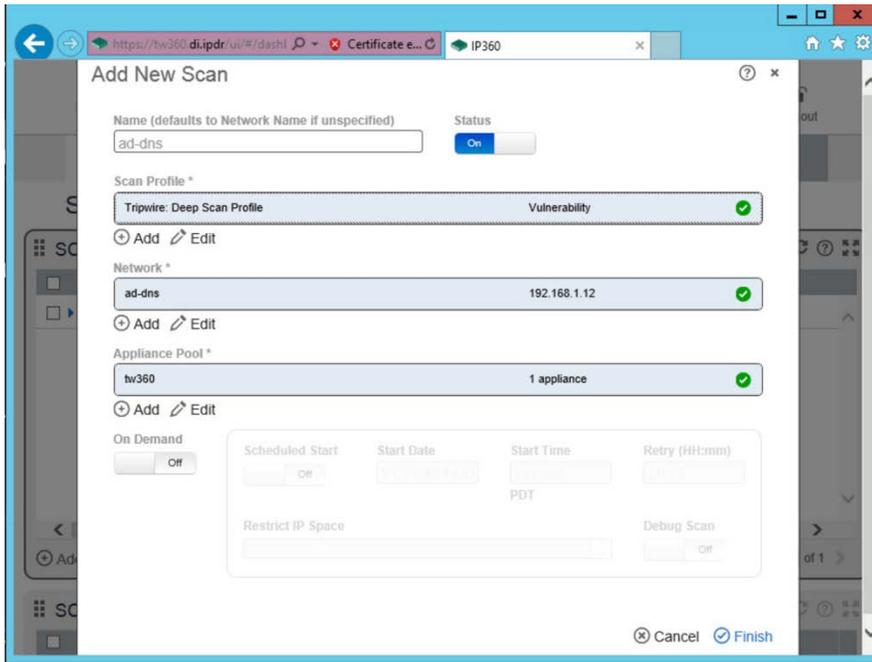
1. Navigate to the web interface and log in.



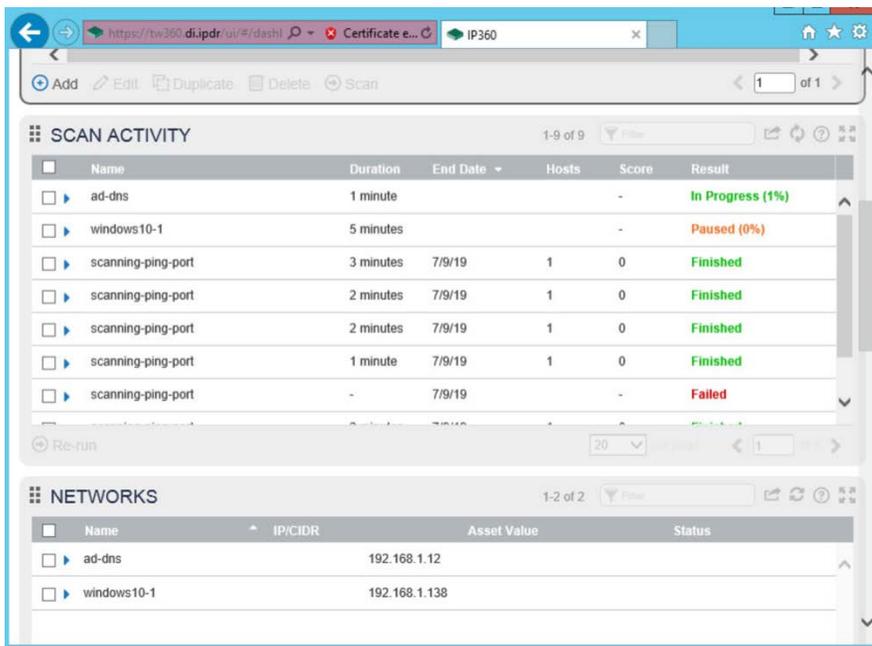
2. Navigate to the **Scanning** tab.



3. Click **Add**.
4. Complete the information regarding the new scan according to the preferences of your organization.

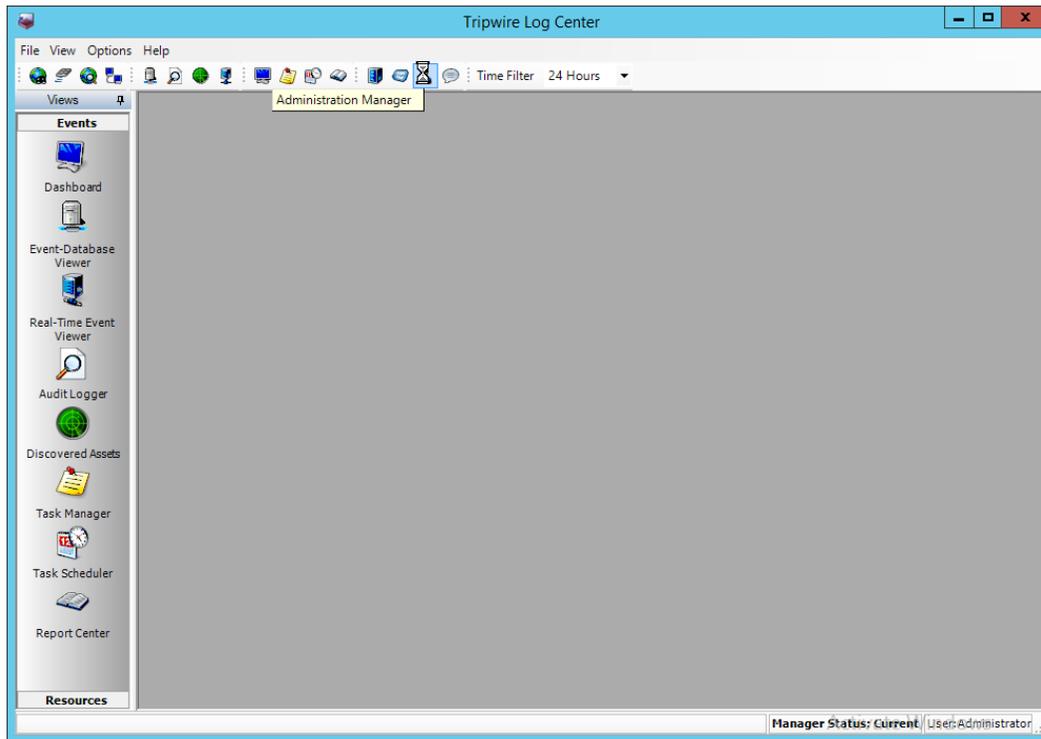


5. Observe successful scan activity.

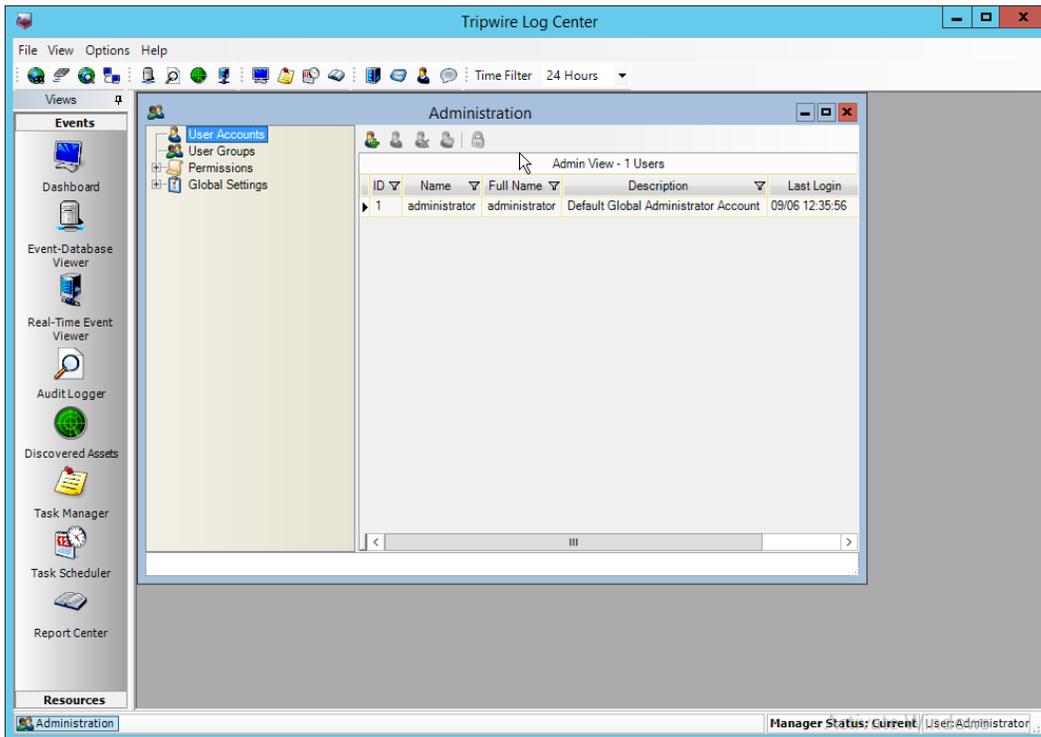


2.18 Integration: Tripwire Log Center and Tripwire Enterprise

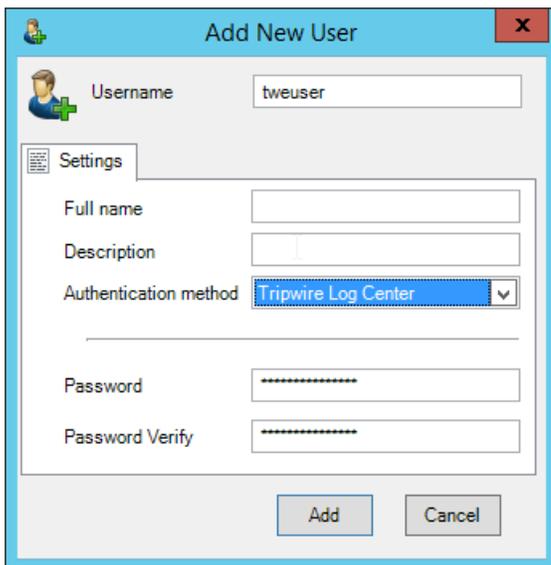
1. Create a user account in **Tripwire Log Center** by logging into **Tripwire Log Center Console**.



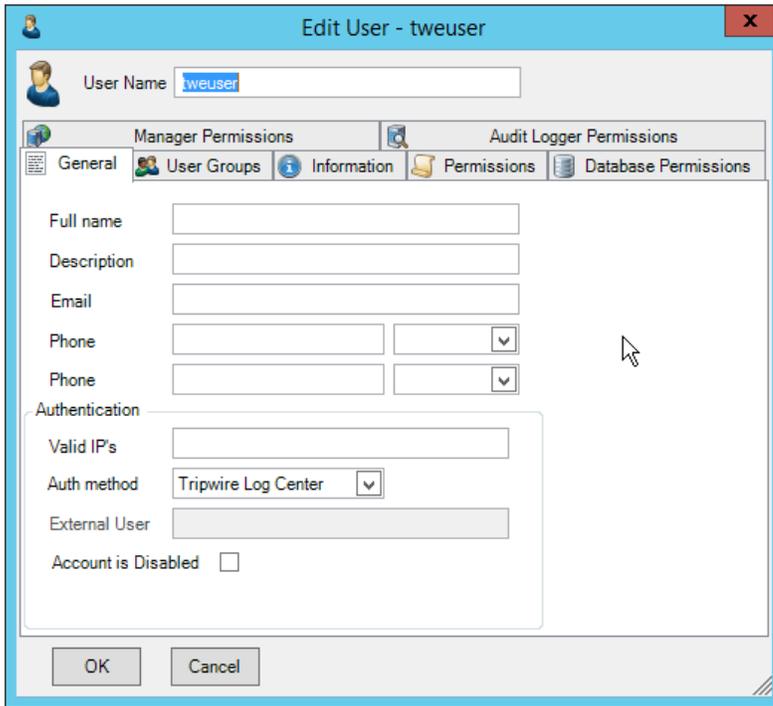
2. Click the **Administration Manager** button.
3. Click **User Accounts**.



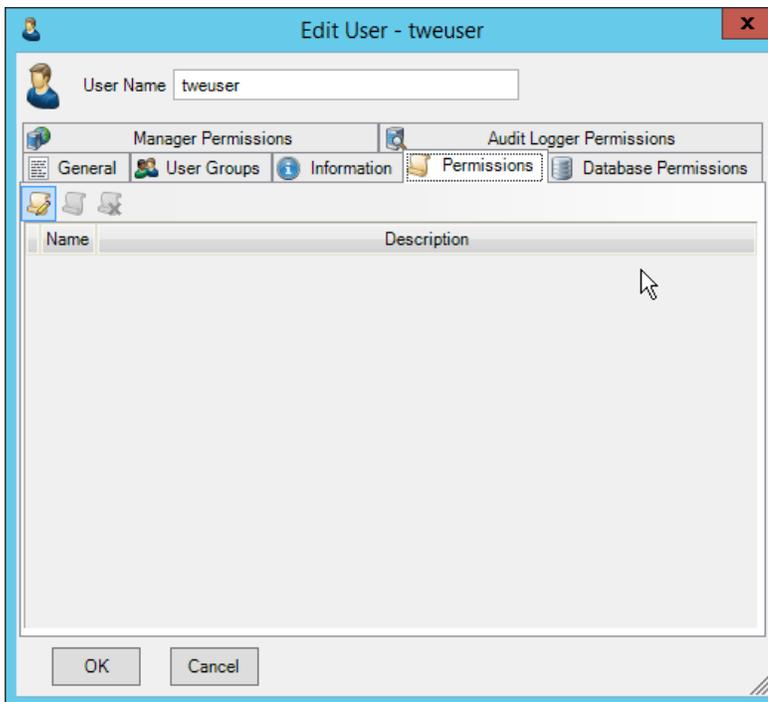
4. Click the **Add** button.
5. Enter the details of the user.



6. Click **Add**.
7. Double-click the user account.

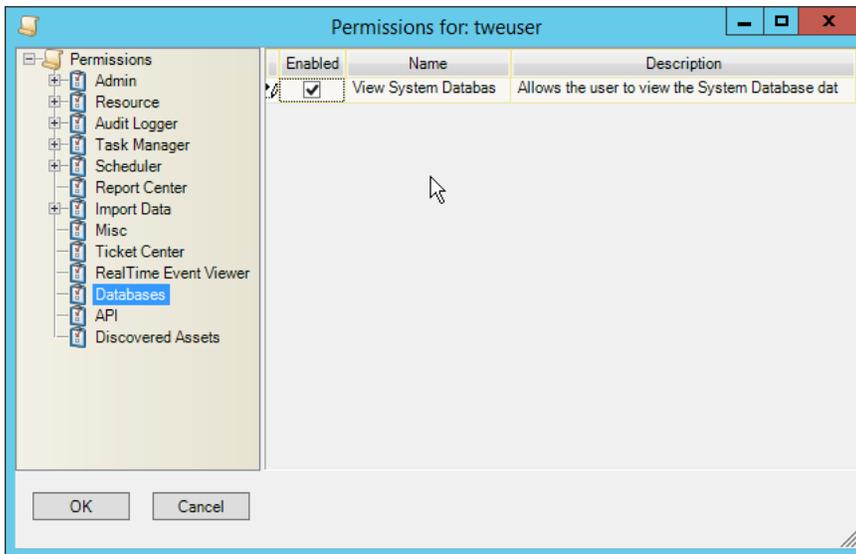


8. Click the **Permissions** tab.



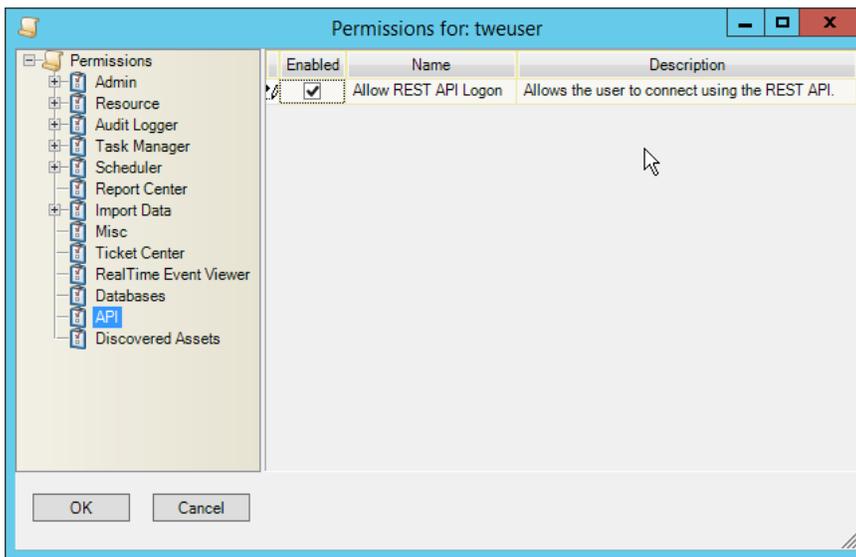
9. Click **Edit list of permissions**.

10. Select **Databases**.

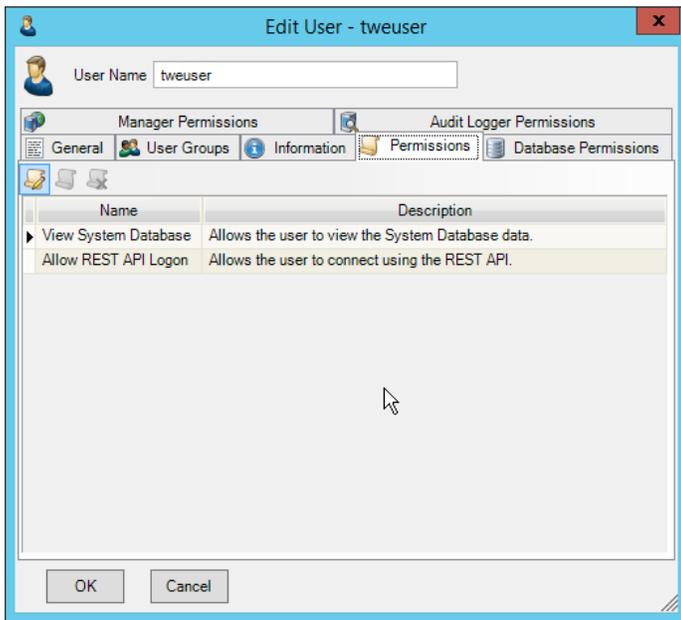


11. Check the box next to **View System Database**.

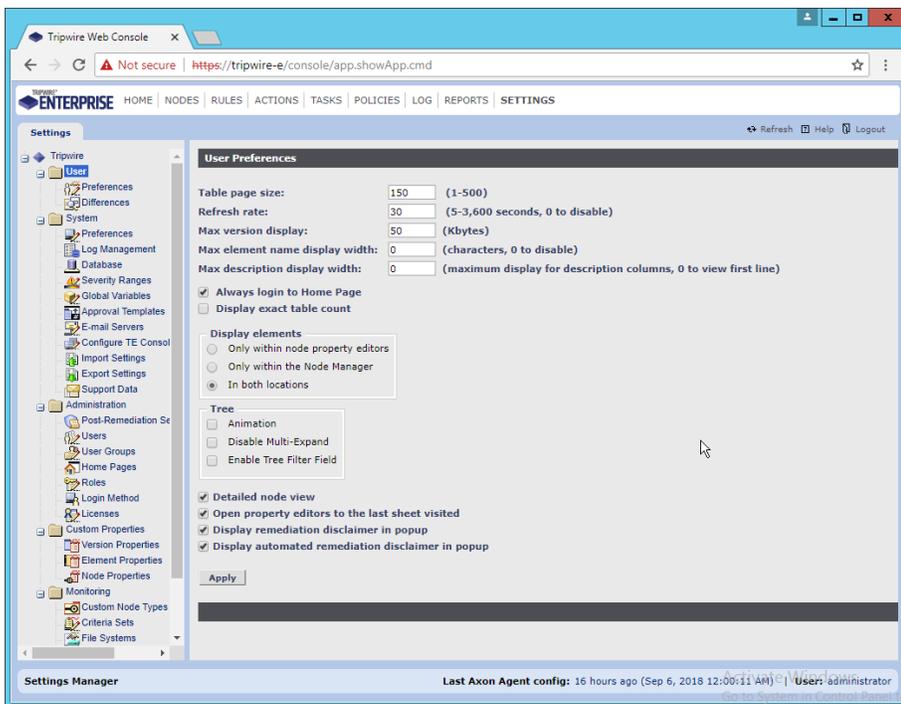
12. Select **API**.



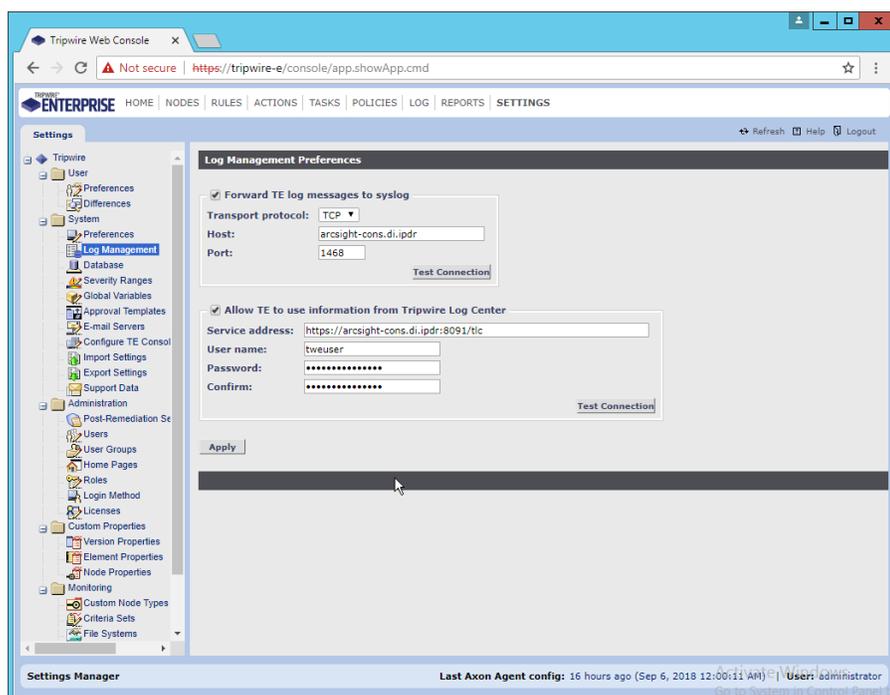
13. Check the box next to **Allow REST API Logon**.



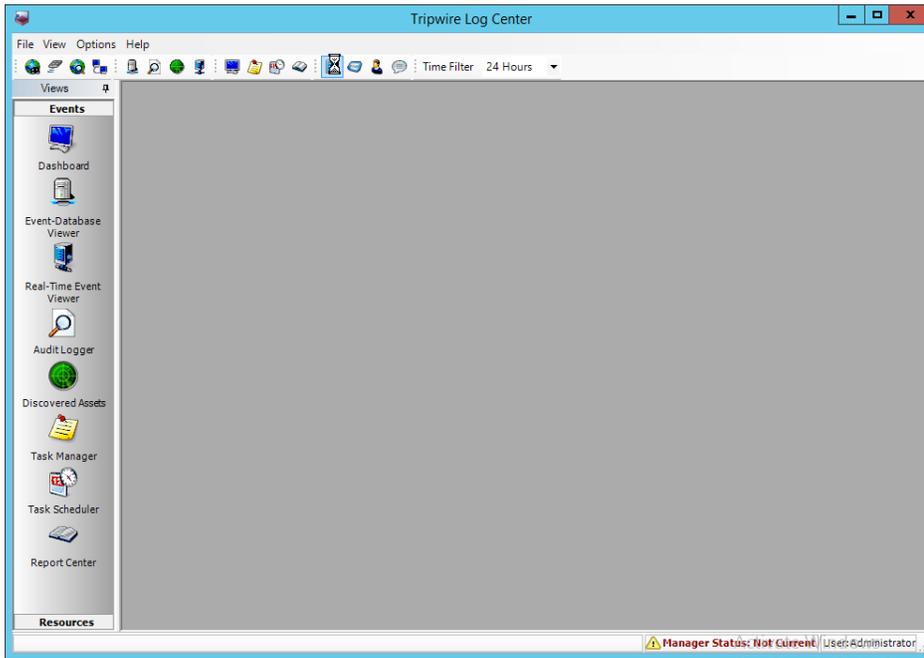
14. Click **OK**.
15. Click **OK**.
16. Log in to the **Tripwire Enterprise** web console.
17. Click **Settings**.



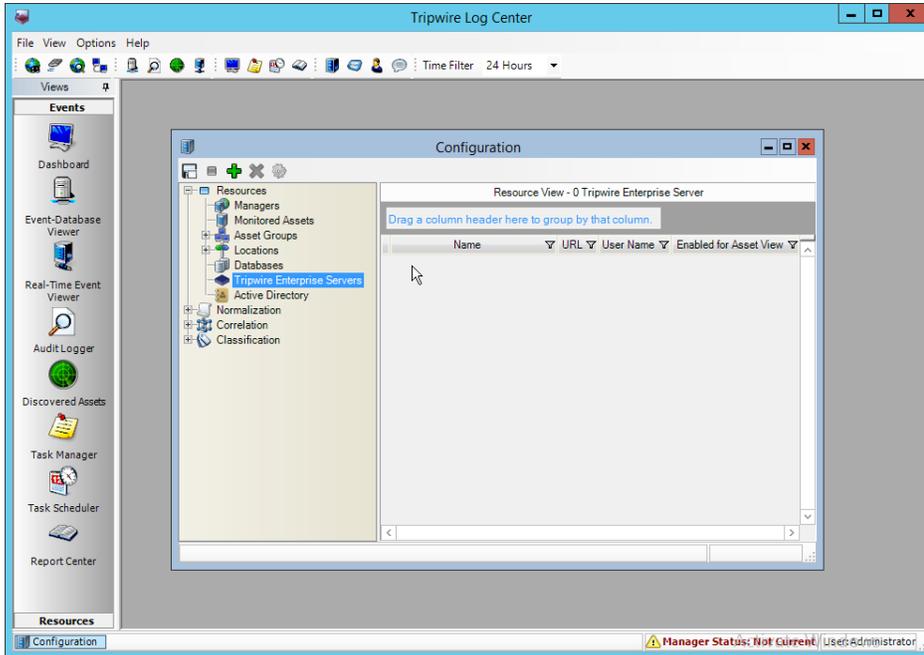
18. Go to **System > Log Management**.
19. Check the box next to **Forward TE log messages to syslog**.
20. Enter the **hostname** and **port** of the **Tripwire Log Center** server. The default port is 1468.
21. Check the box next to **Allow TE to use information from Tripwire Log Center**.
22. Enter the **service address** like this: `https://arcsight-cons.di.ipdr:8091/tlc`. Replace the **hostname** with the hostname of your **Tripwire Log Center** server.
23. Enter the account information of the account just created for **Tripwire Log Center**.
24. You can use **Test Connection** to verify that the connection is working.



25. Click **Apply** when finished.
26. Go back to the **Tripwire Log Center Console**.

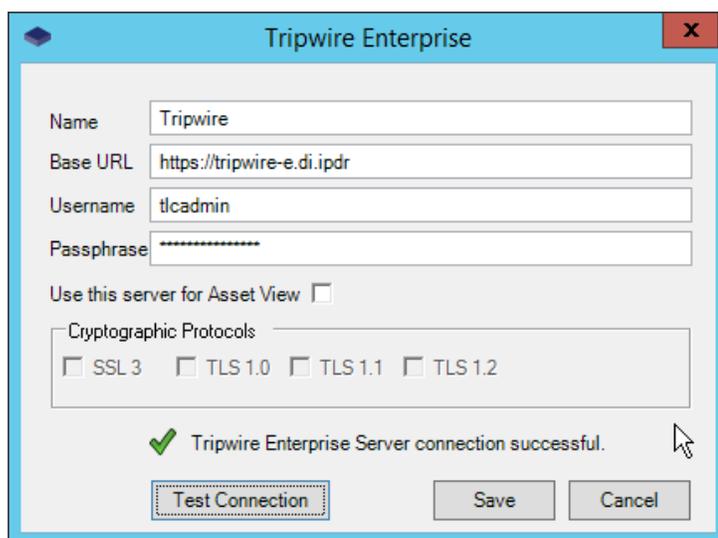


- 27. Click **Configuration Manager**.
- 28. Click **Resources > Tripwire Enterprise Servers**.



- 29. Click **Add**.
- 30. Enter a **name** for the server.

31. Enter the **URL** of the Tripwire Enterprise server.
32. Enter the **name** of a user account on the Tripwire Enterprise server. The account must have the following permissions: create, delete, link, load, update, view.



33. Click **Save**.

2.19 Integration: Tripwire Log Center and Tripwire IP360

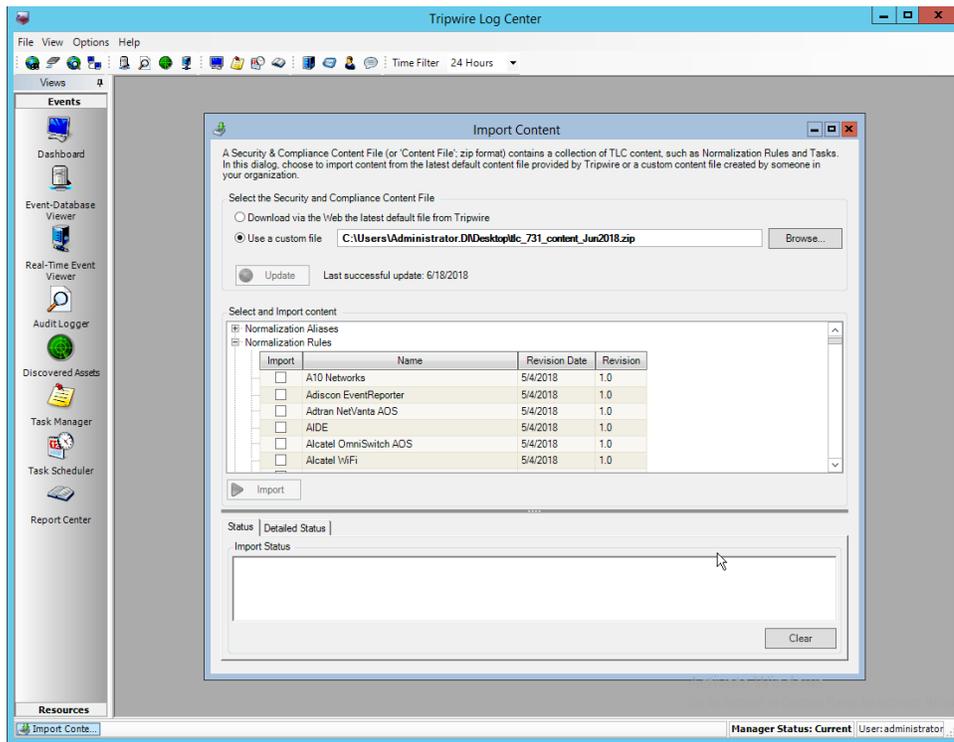
2.19.1 Configure IP360 and Log Center

1. On the **Tripwire Log Center Manager** machine, navigate to C:\Program Files\Tripwire\Tripwire Log Center Manager\Agent Services\config.
2. Copy **bridge_sample.properties** to **bridge.properties**.
3. Modify the Pre-Shared Key to use a password by changing the following line (be sure to remove the “#” sign):
`tw.cap.bridge.registrationPreSharedKey=newpasswordhere`
4. Save the file.
5. From the command line, run the following two commands:
`> net stop TripwireBridge`
`> net start TripwireBridge`
6. On the Tripwire IP360 machine, from the command line, enter the following command to specify the hostname of the Tripwire Log Center (TLC) machine:
`> tlc config bridge host update <hostname>`
7. Enter the following command using the preshared key specified earlier:

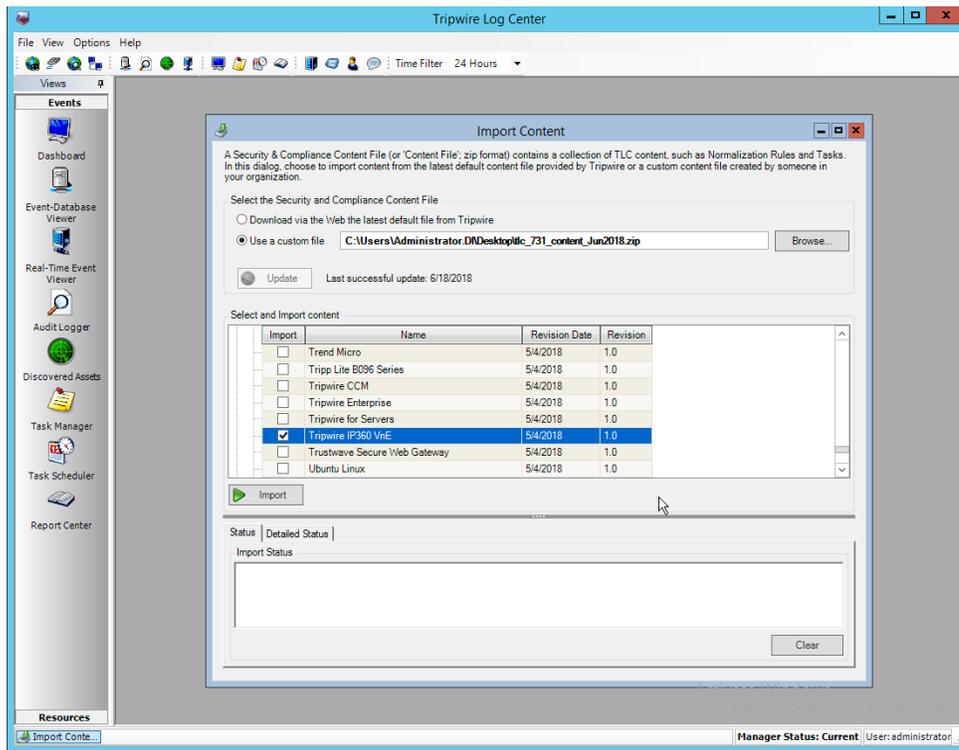
- > `tlc config bridge password update <password>`
- 8. Enter the following command to start the TLC service on the IP360 machine (this will use port 5670 on the TLC machine by default):
 - > `system service tlc enable`
- 9. Download the “Content update–June 2018” package from the **Tripwire Customer Center**.
- 10. Open the **Tripwire Log Center Console**.
- 11. Enter the **username** and **password**.



- 12. Click **Login**.
- 13. Click **Options > Import TLC Content > Content**.
- 14. Select **Use a custom file**.
- 15. Click **Browse**, and locate the zip file downloaded from the **Tripwire Customer Center**.



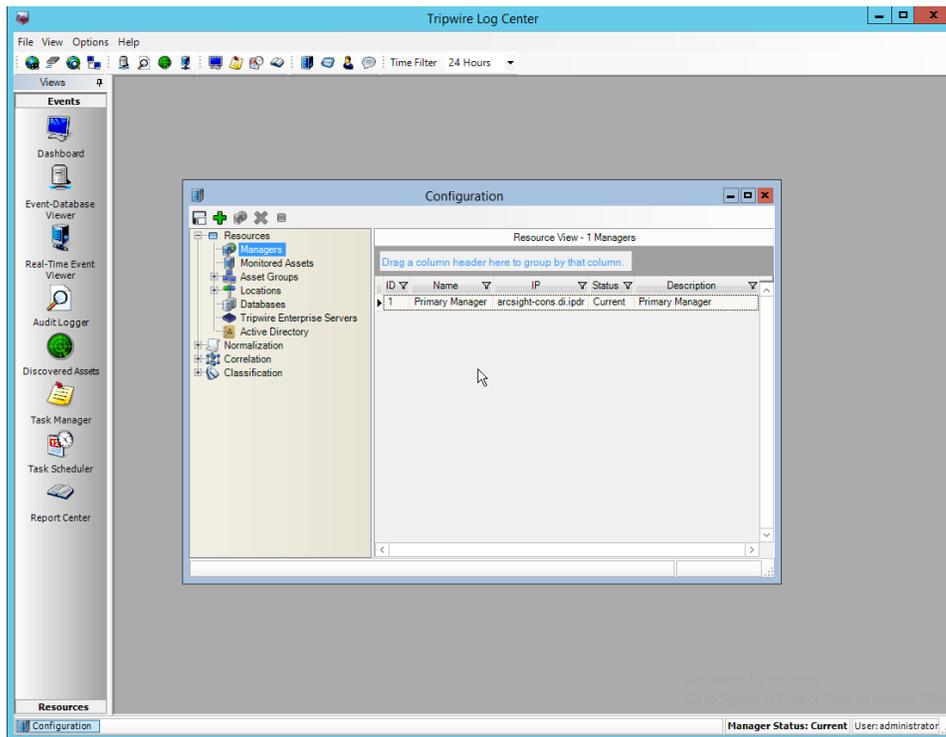
16. Expand the **Normalization Rules** section.
17. Check the box next to **Tripwire IP360 VnE**.



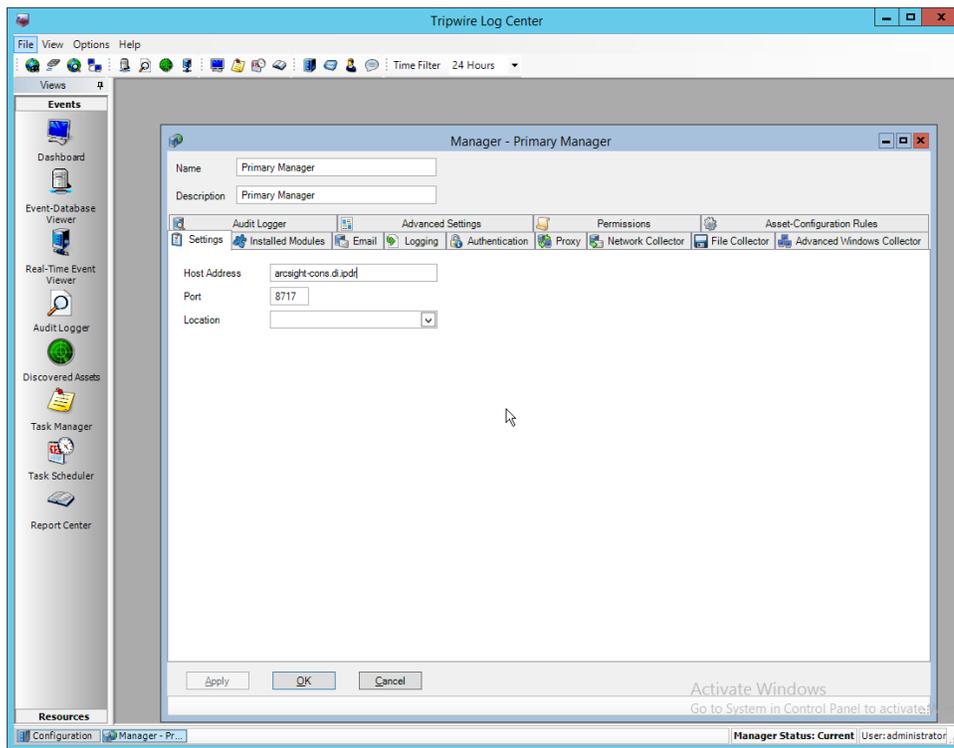
18. Click **Import**.

2.19.2 Collect Tripwire IP360 Operational Logs

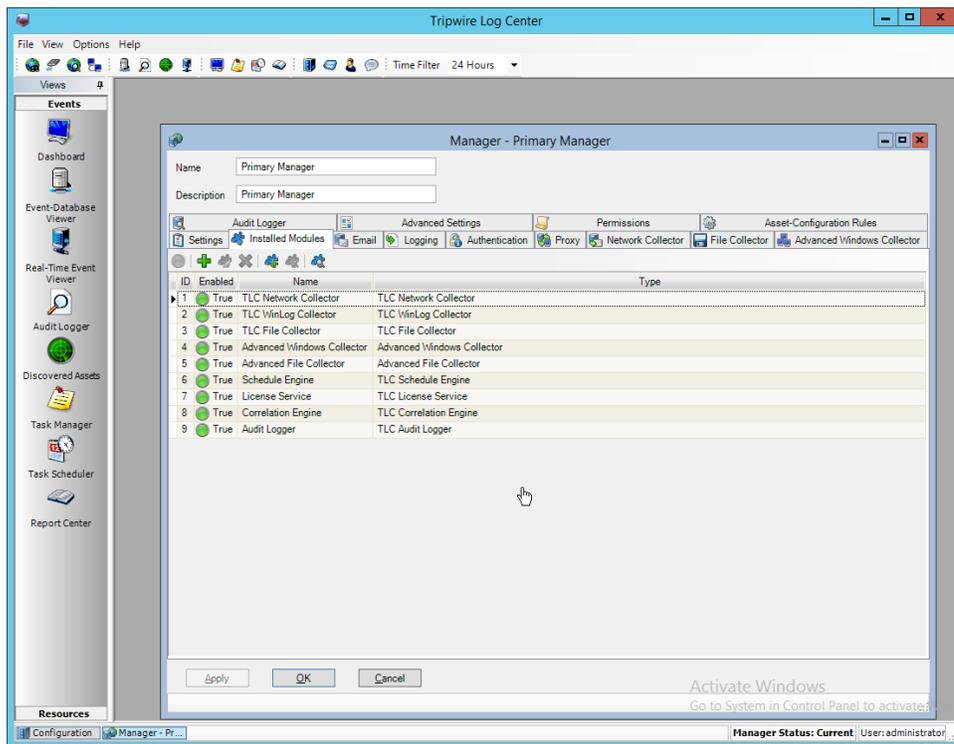
1. Click **Configuration Manager**.
2. Click **Resources > Managers**.



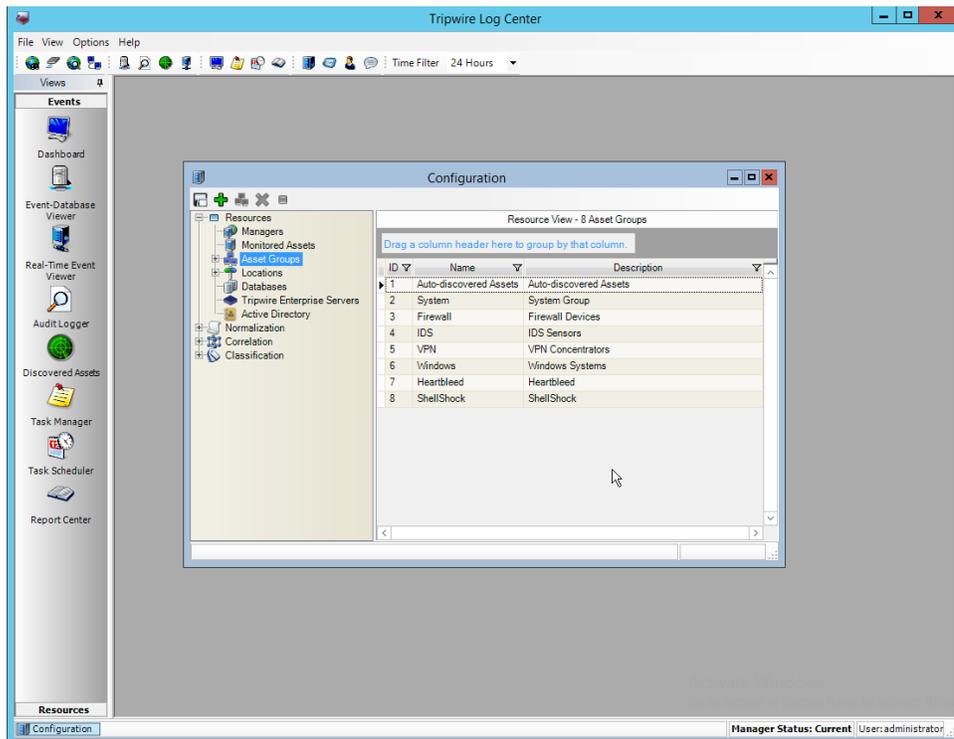
3. Double-click the **Primary Manager**.



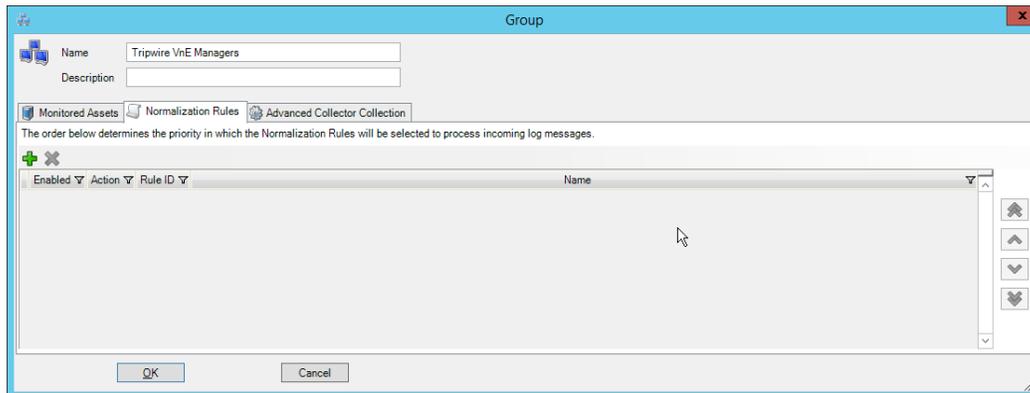
4. Click the **Installed Modules** tab.



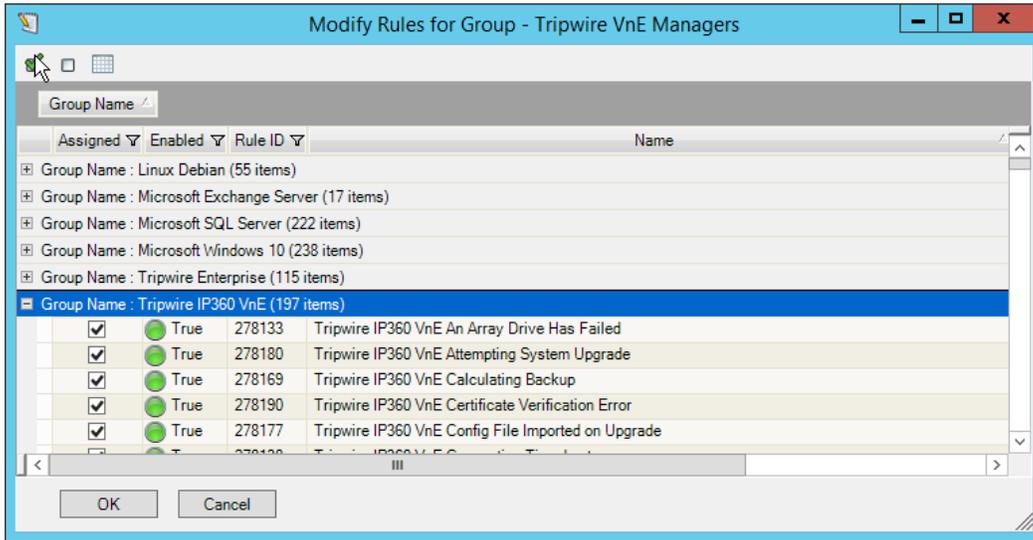
5. Ensure that there is an **Advanced File Collector**. If not, click the **Create new module** button, and specify a **name**. Set the type to **Advanced File Collector**. If there is an **Advanced File Collector**, skip this step.
6. Click **OK**.
7. Click **Resources > Asset Groups**.



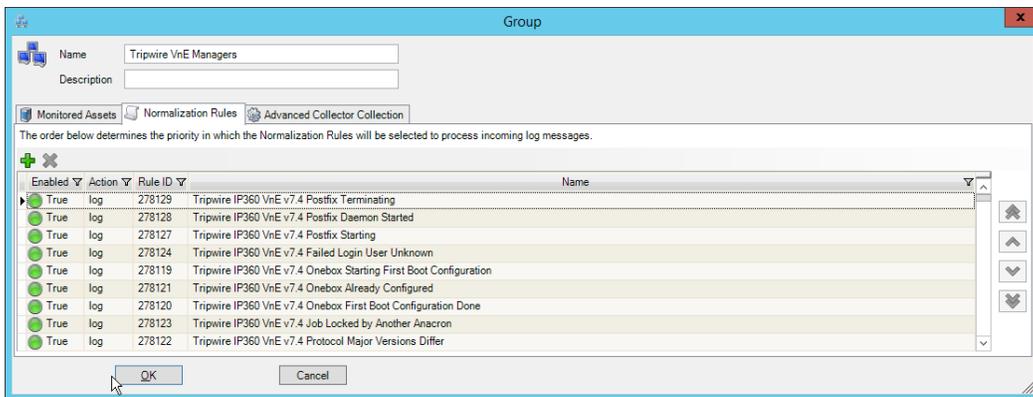
8. Click **Add**.
9. Enter **Tripwire VnE Managers** in the **Name** field.
10. Click the **Normalization Rules** tab.



11. Click **Add**.
12. Expand the **Tripwire IP360 VnE** group.
13. Click the **Check selected rows** button at the top to check the box next to everything in this section.

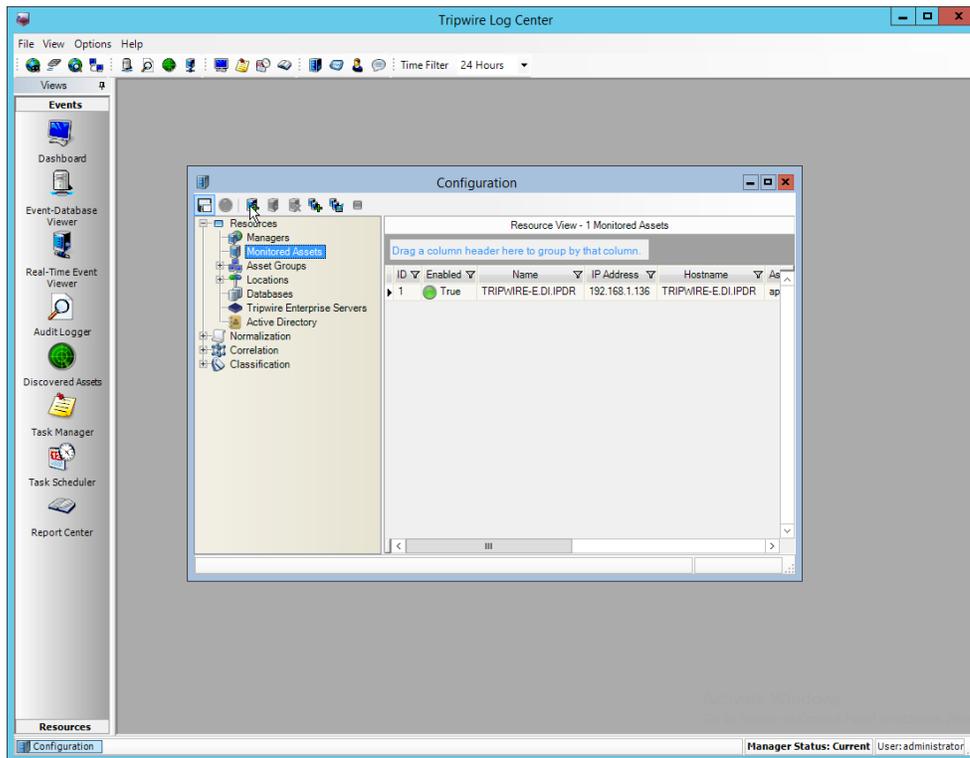


14. Click **OK**.

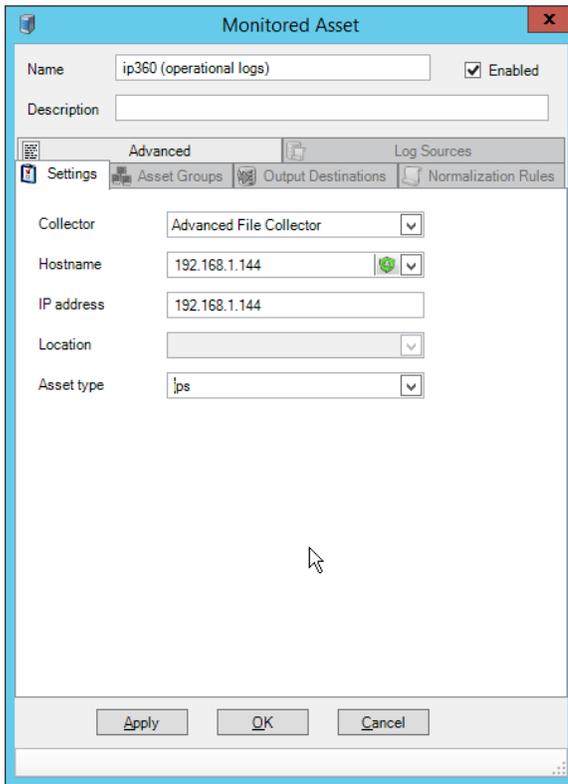


15. Click **OK**.

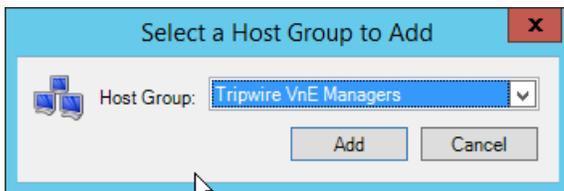
16. Click **Resources > Monitored Assets**.



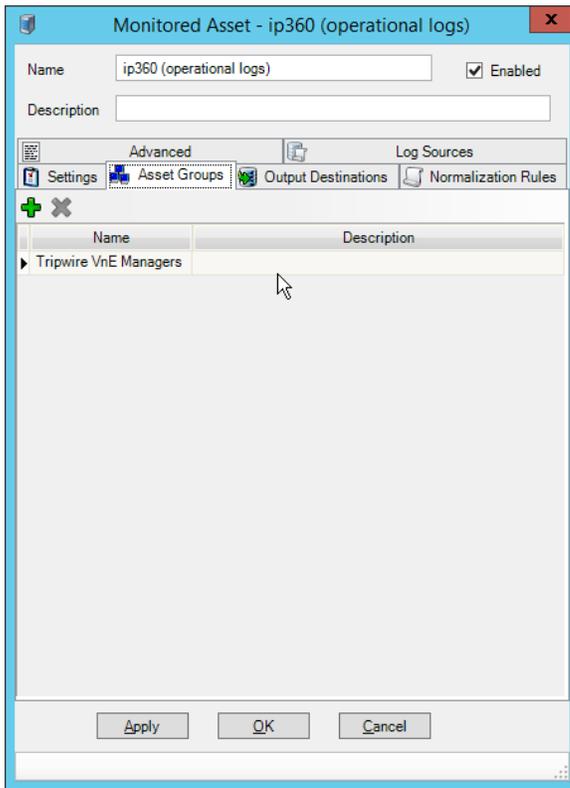
17. Click **Add Monitored Asset**.
18. Enter a **name**.
19. Select **Advanced File Collector** for **Collector**.
20. Select the IP360 server from the **Hostname** drop-down. It may appear as an IP address.
21. Enter the **IP address** of the server.
22. Select **ips** for **Asset type**.



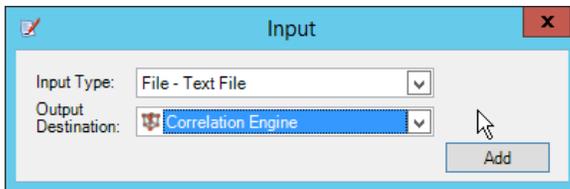
- 23. Click the **Asset Groups** tab.
- 24. Click **Add**.
- 25. Select **Tripwire VnE Managers**.



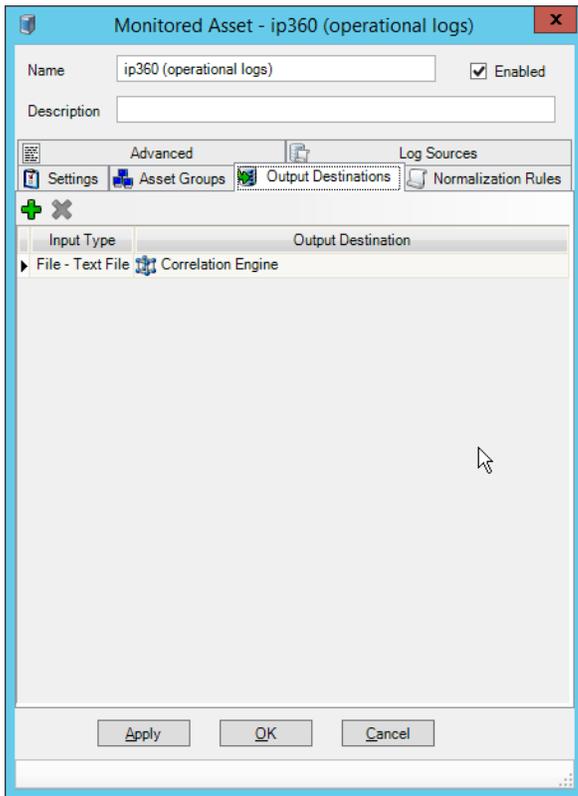
- 26. Click **Add**.



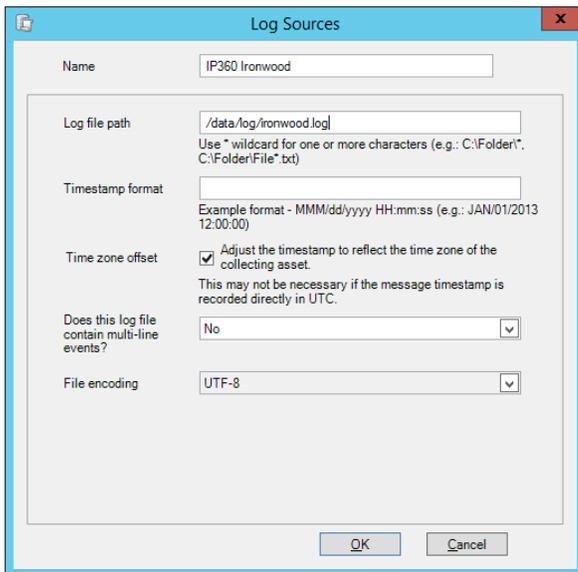
27. Click the **Output Destinations** tab.
28. Click **Add**.
29. Select **File–Text File** for **Input Type**.
30. Select **Correlation Engine** for Output Destination.



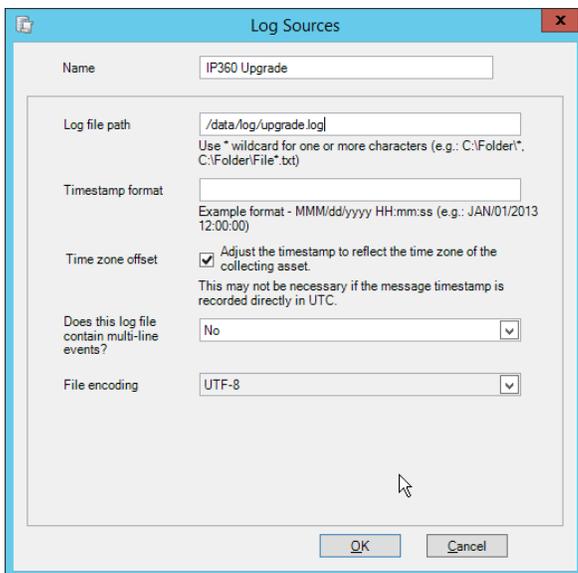
31. Click **Add**.



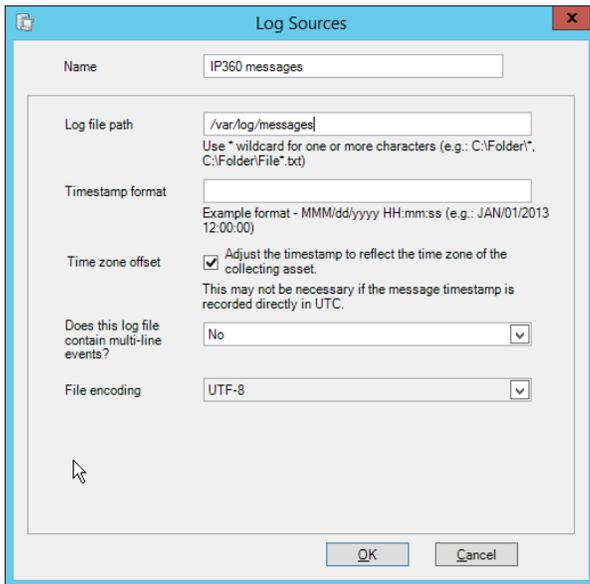
32. Click the **Log Sources** tab.
33. Click **Add**.
34. Enter a **name** for the log.
35. Enter /data/log/ironwood.log for **Log file path**.



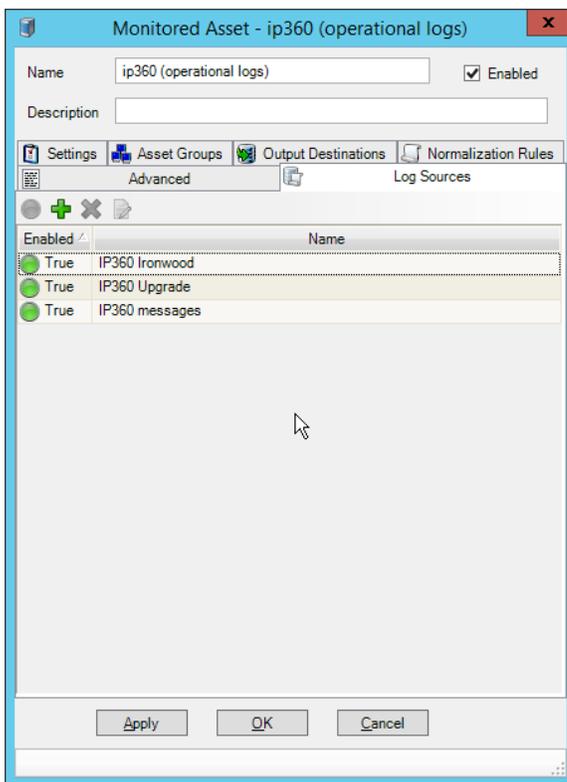
36. Click **OK**.
37. Click **Add**.
38. Enter a **name** for the log.
39. Enter /data/log/upgrade.log for **Log file path**.



40. Click **OK**.
41. Click **Add**.
42. Enter a **name** for the log.
43. Enter /var/log/messages for **Log file path**.

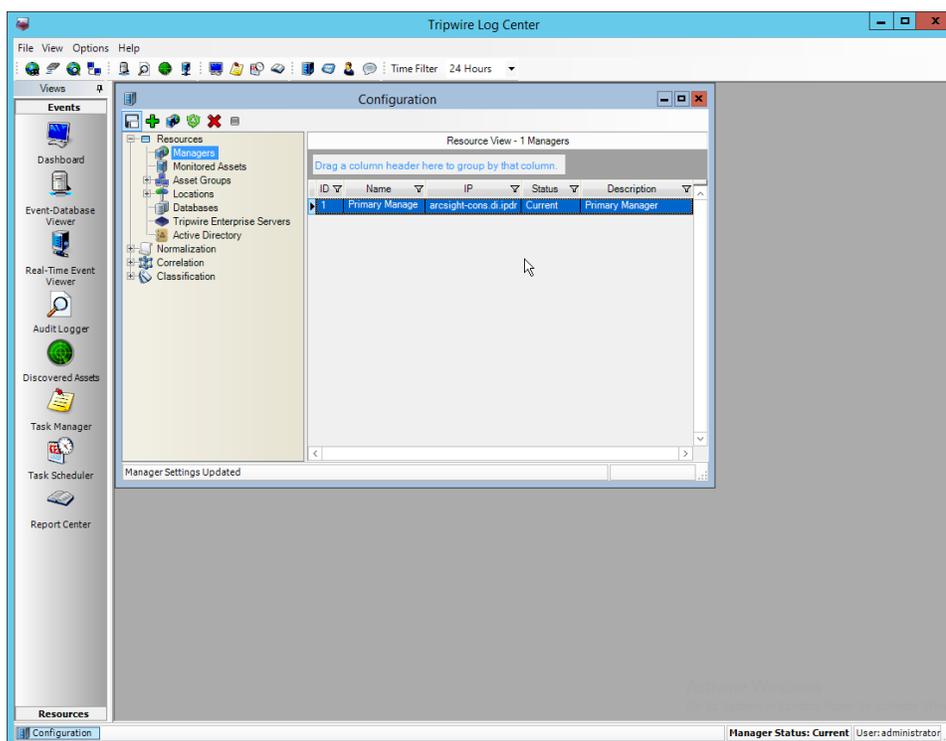


44. Click **OK**.



45. Click **OK**.

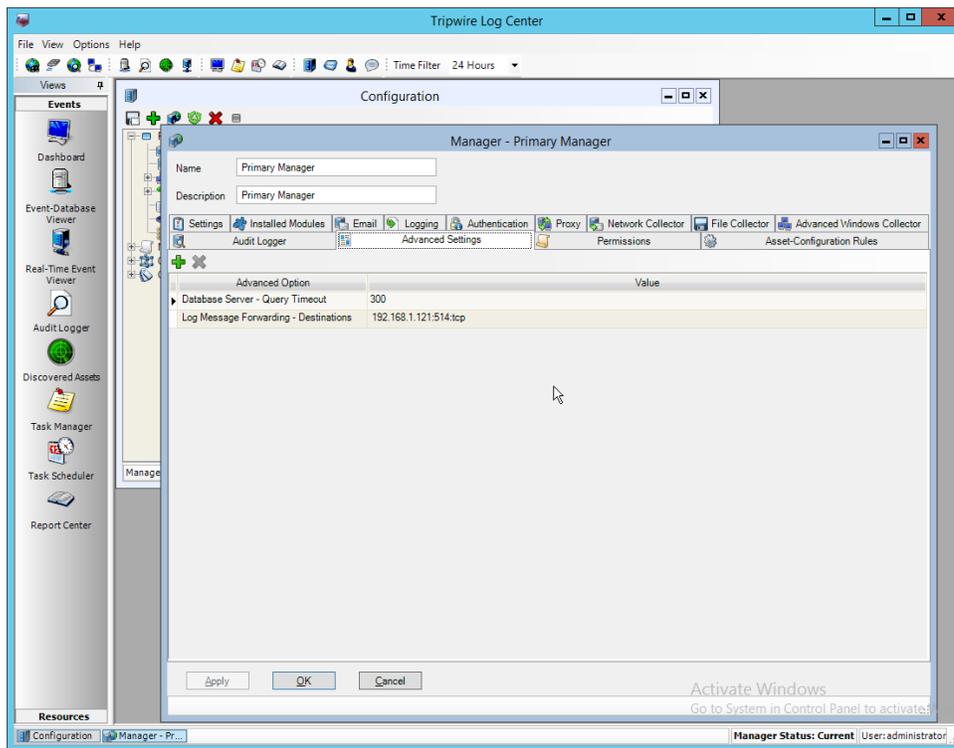
46. Click **Resources > Managers**.



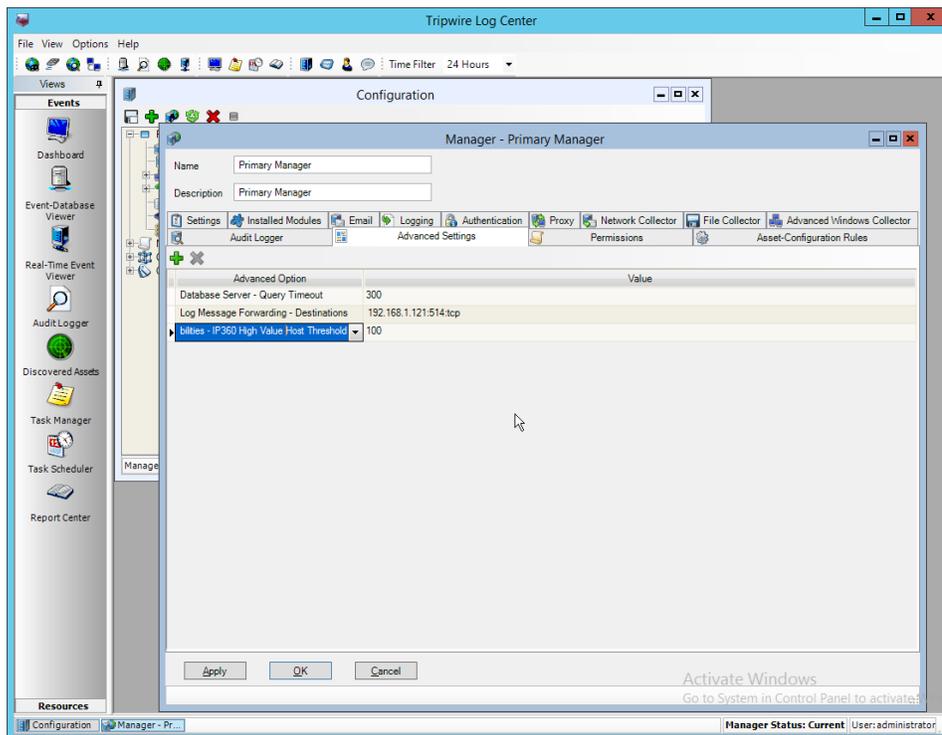
47. Select the **Primary Manager** and click **Push Updates to Manager**.

2.19.3 Configure Tripwire IP360 Scan Results Forwarding

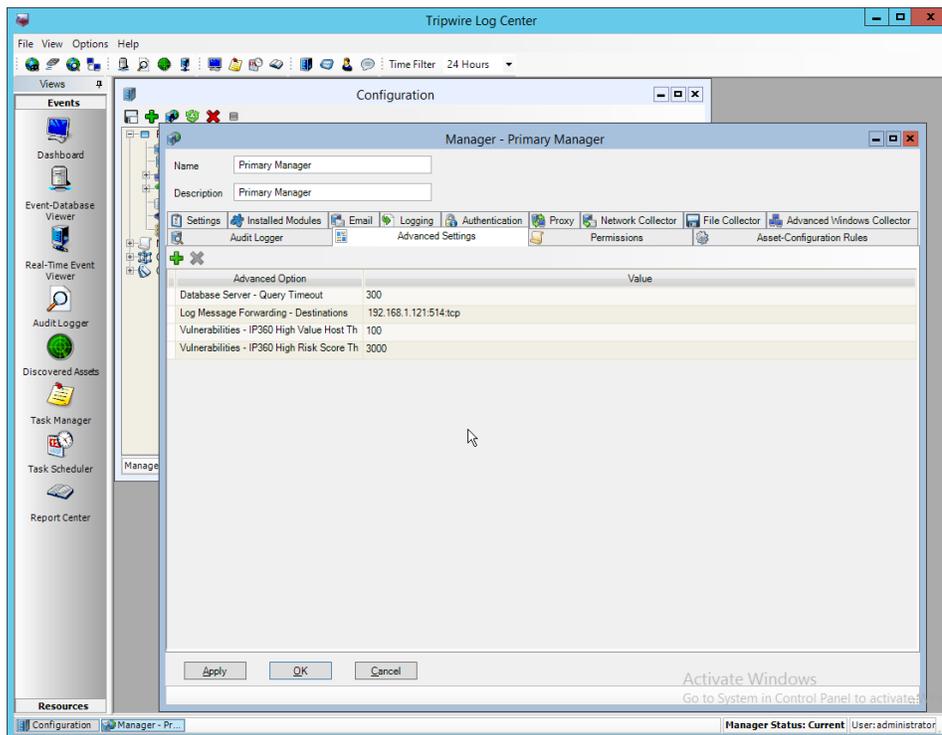
1. Click **Configuration Manager**.
2. Click **Resources > Manager**.
3. Double-click the **Primary Manager**.
4. Click the **Advanced Settings** tab.



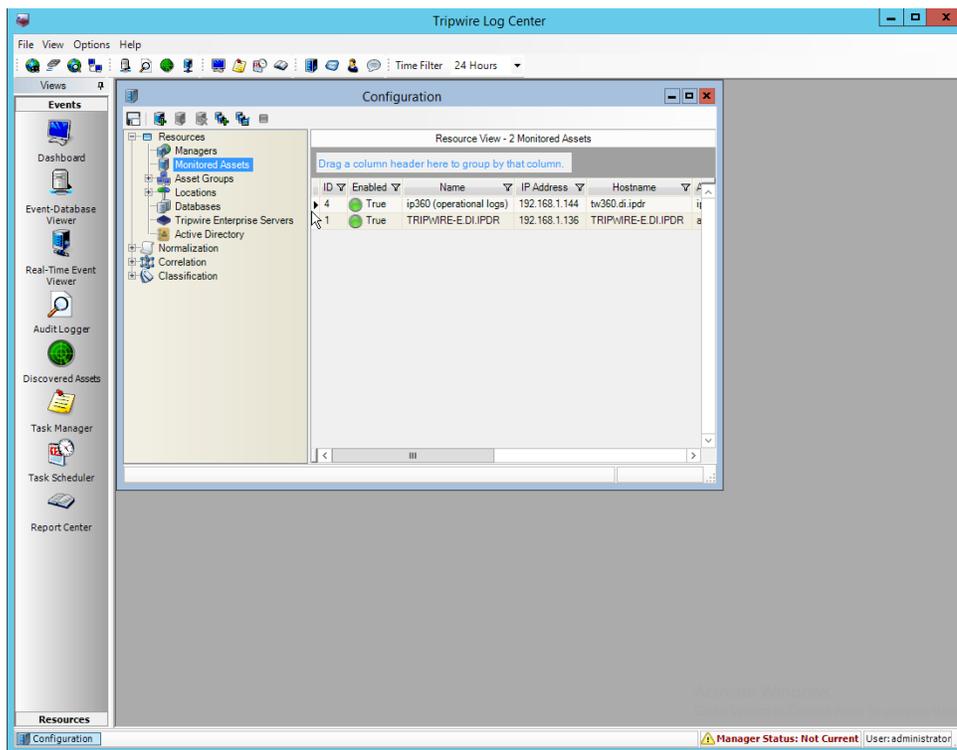
5. Click **Add**.
6. Select **Vulnerabilities–IP360 High Value Host Threshold** for the **Advanced Option**.
7. Enter a number between 0 and 999,999,999 for the **Value**. This number corresponds to the priority level of the host system being scanned. The value entered will be the minimum value for a host machine to be considered high priority. Half of this value will be the minimum value for a host machine to be considered medium priority.



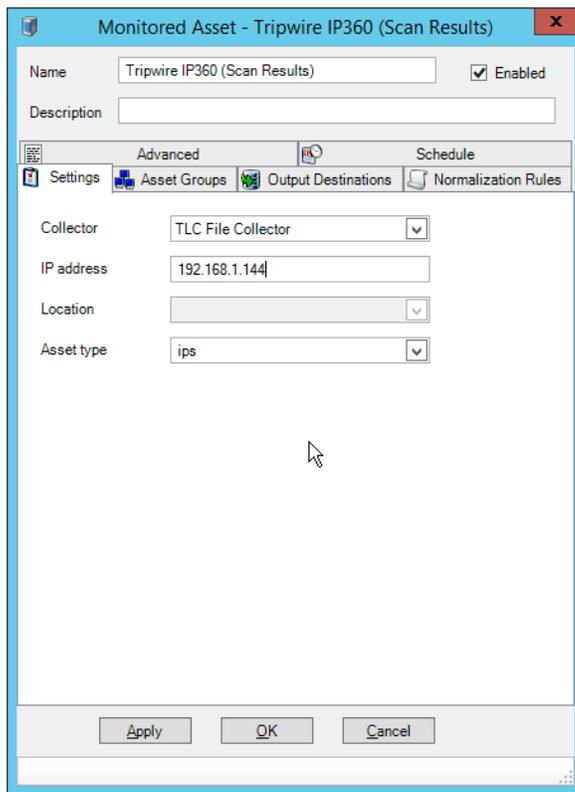
8. Click **Add**.
9. Select **Vulnerabilities—IP360 High Risk Score Threshold** for the **Advanced Option**.
10. Enter a number between 0 and 999,999,999 for the **Value**. This number corresponds to the risk level of a vulnerability event. The value entered will be the minimum value for an event to be considered high risk. Half of this value will be the minimum value for an event to be considered medium risk.



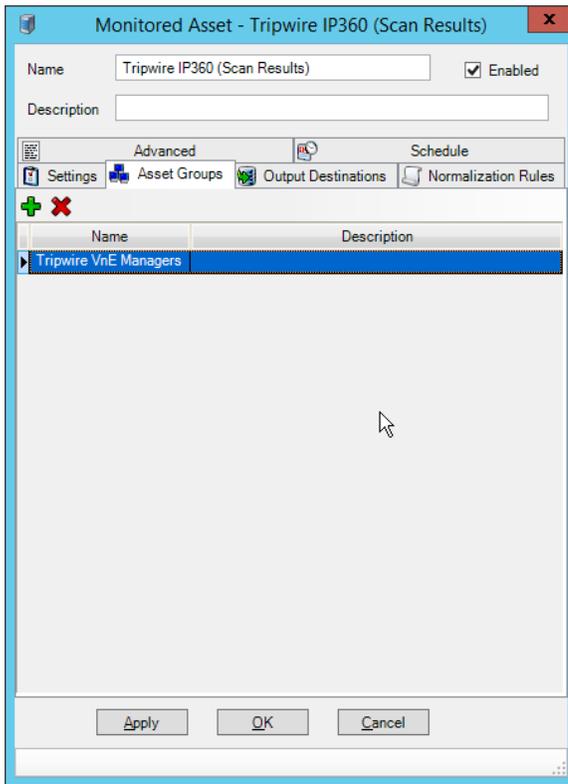
11. Click **Apply**.
12. Click **OK**.
13. Click **Resources > Monitored Assets**.



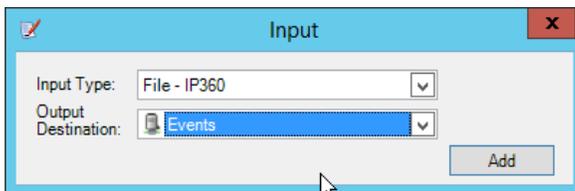
14. Click **Add Asset**.
15. Select **TLC File Collector** for **Collector**.
16. Enter the **IP address** of the **IP360** machine.
17. Select **ips** for **Asset type**.



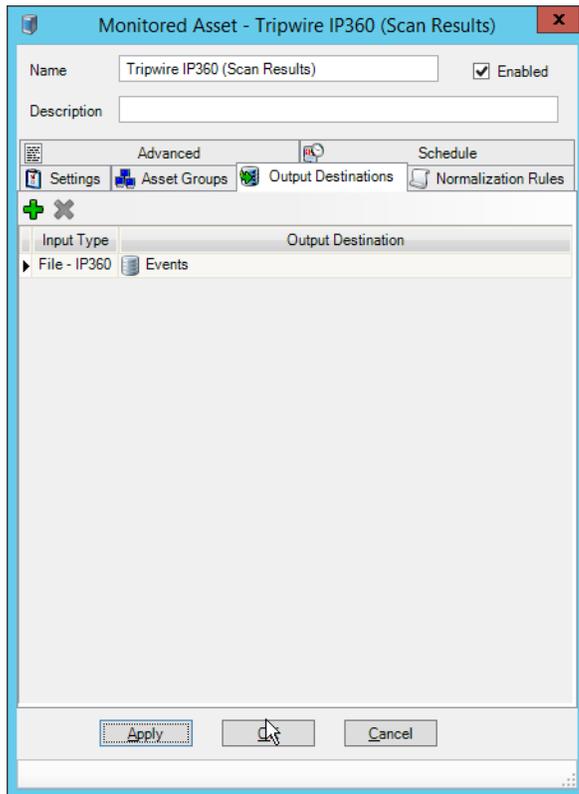
18. Click the **Asset Groups** tab.
19. Click **Add**.
20. Select **Tripwire VnE Managers** for **Host Group**.
21. Click **Add**.



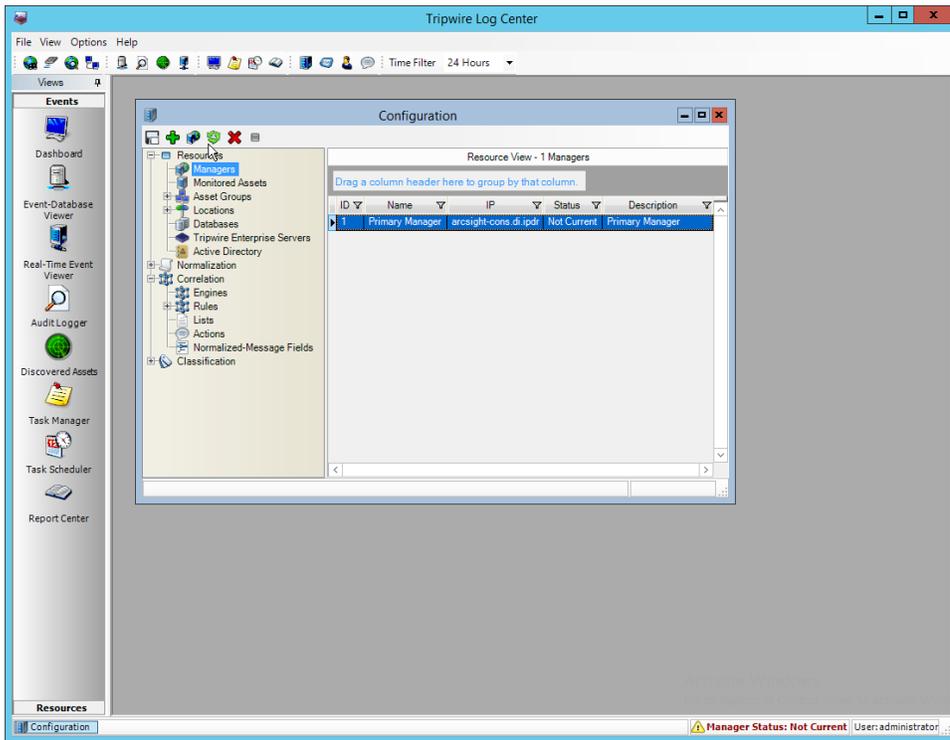
22. Click the **Output Destinations** tab.
23. Select **File–IP360** for **Input Type**.
24. Select **Events** for **Output Destination**.



25. Click **Add**.

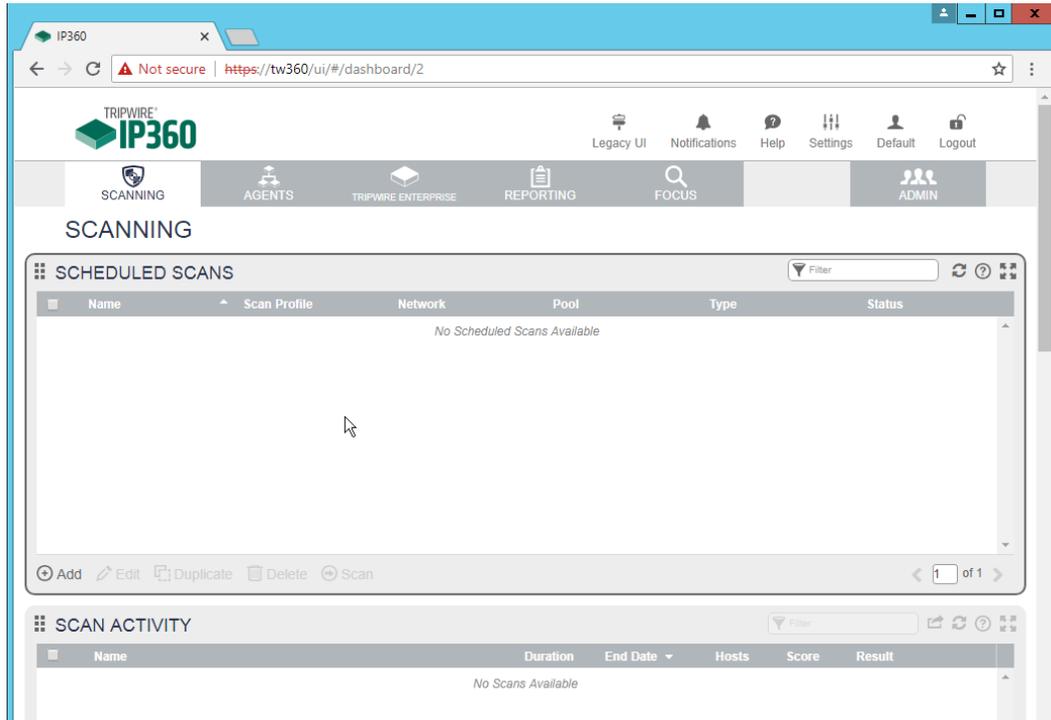


26. Click **OK**.
27. Click **Resources > Managers**.
28. Select the **Primary Manager**.

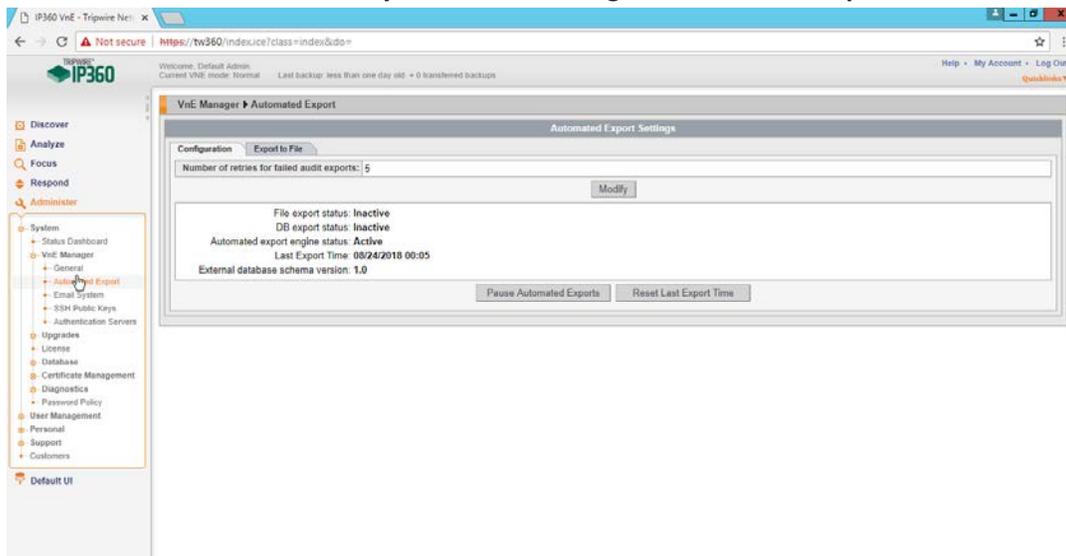


29. Click **Push Update to Manager**.

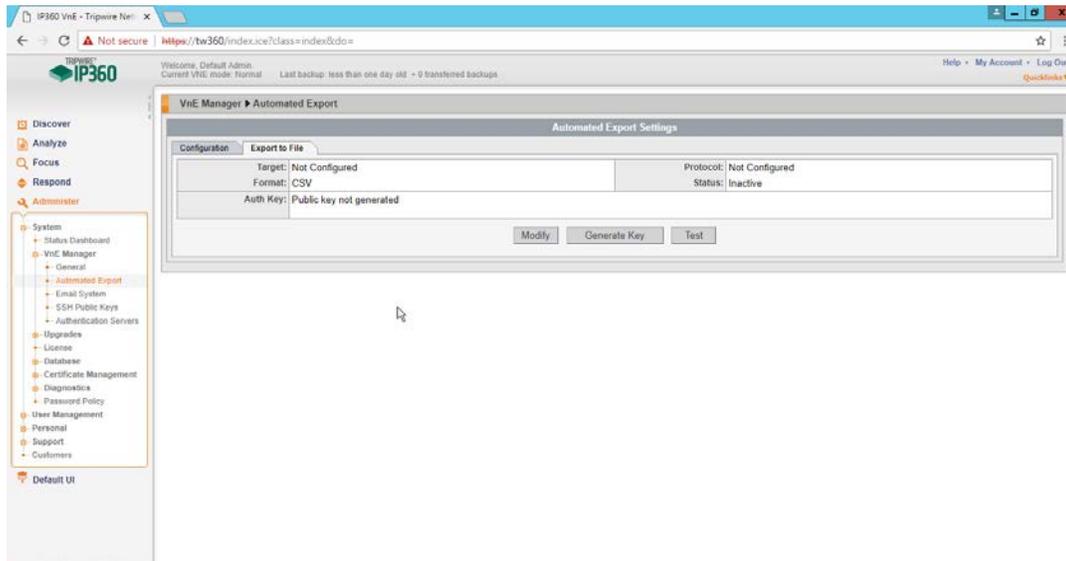
30. Log in to the **Tripwire IP360 Web Console**.



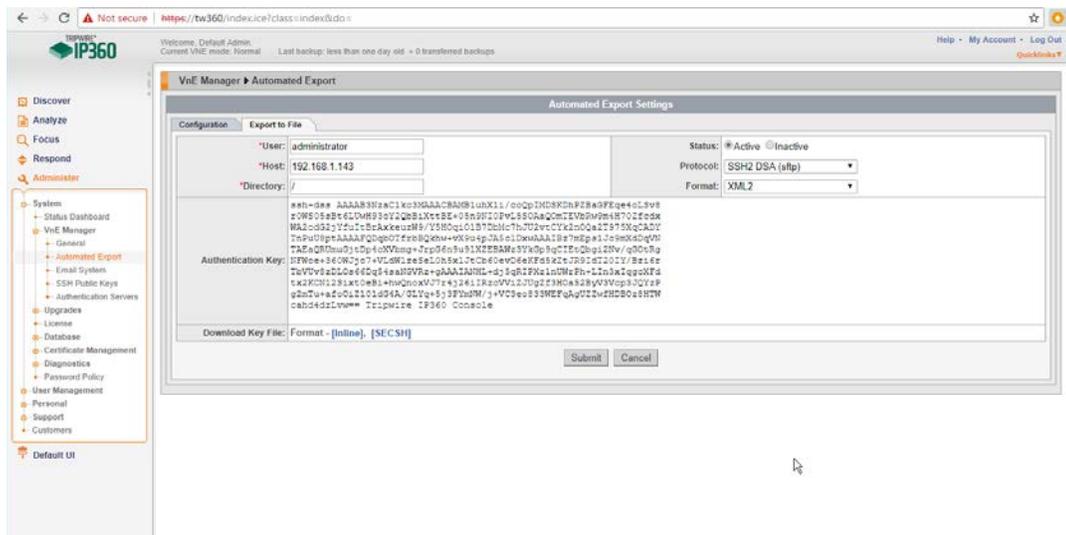
31. Click **Legacy UI** at the top.
32. On the left, click **Administer > System > VnE Manager > Automated Export**.



33. Click the **Export to File** tab.



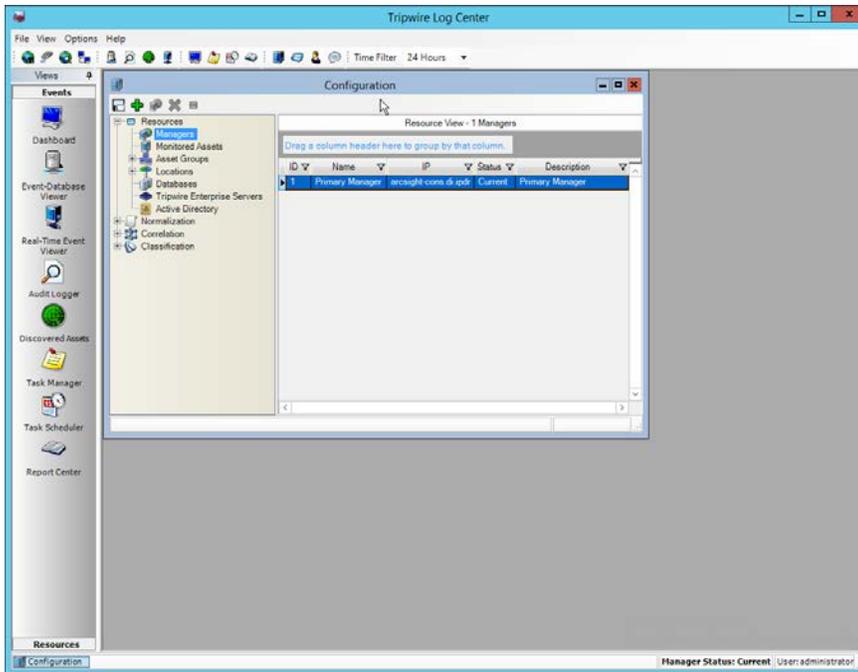
34. Click **Modify**.
35. Enter the **username** of a TLC user account for **User**.
36. Enter the **IP address** of the TLC Manager for **Host**.
37. Enter **"/"** for the **directory**.
38. Select **Active**.
39. Select **SSH2 DSA (sftp)** for **Protocol**.
40. Select **XML2** for **Format**.



41. Click **Submit**.
42. Download the generated key by clicking **[Inline]**.

43. In **TLC Console**, click **Configuration Manager**.

44. Click **Resources > Managers**.



45. Double-click the **Primary Manager**.

46. Click the **File Collector** tab.

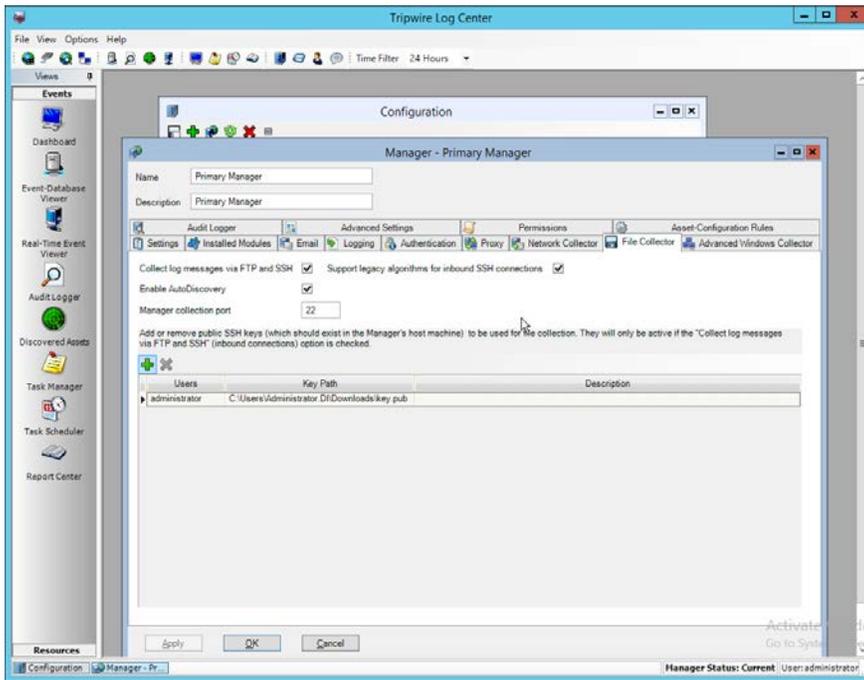
47. Ensure that the **Collect log messages via FTP and SSH** option is enabled.

48. Enter **22** for the **port**. (Note: The *IP360 Integration Guide* says to use a different port, but the IP360 system appears to be unable to use a port other than 22.)

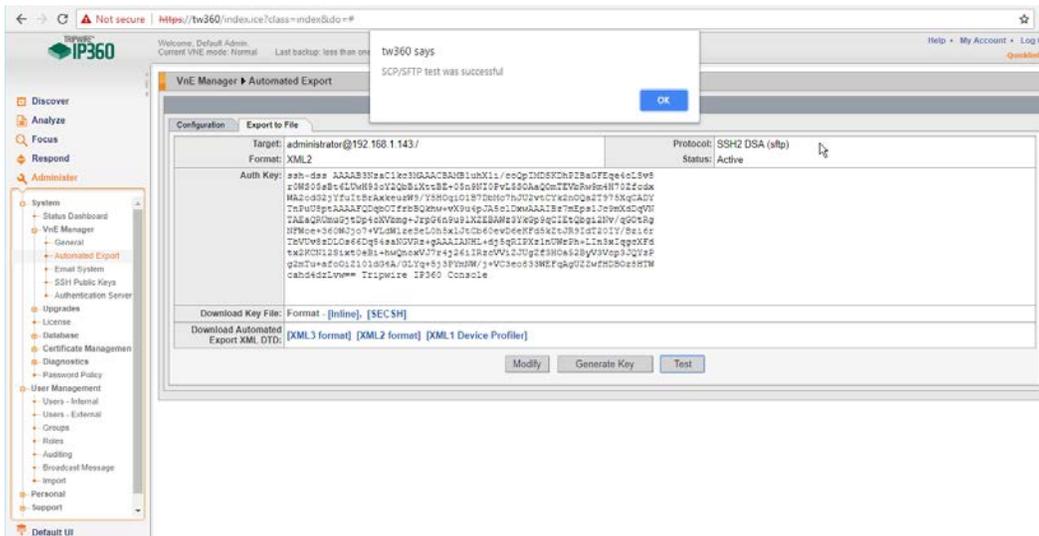
49. Click **Add**.

50. Under **Users**, select the user for whom the key was generated.

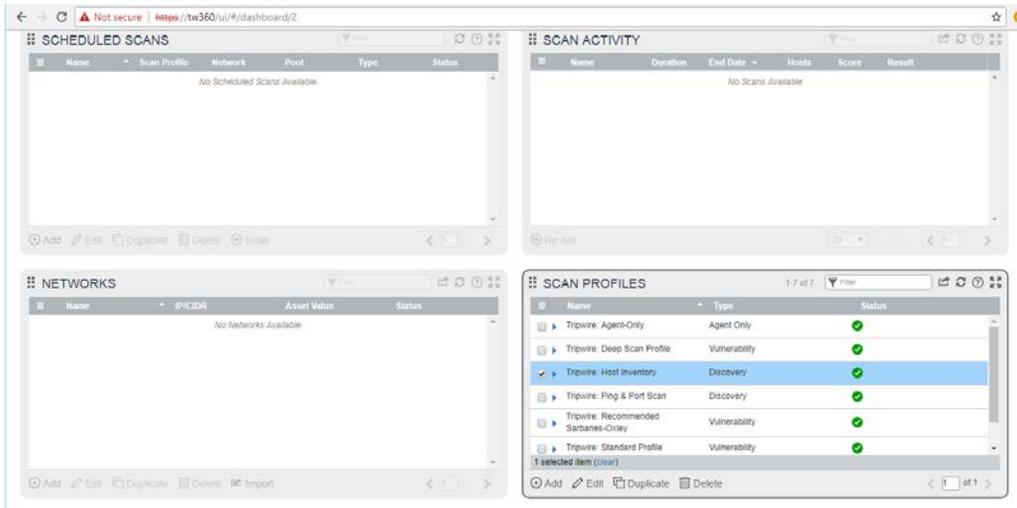
51. Under **Key Path**, enter the path to the downloaded key.



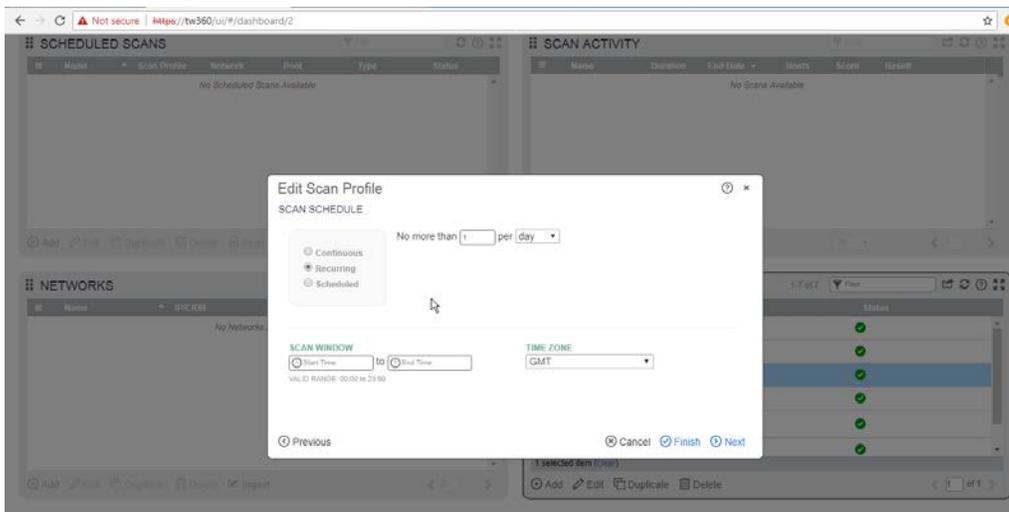
52. Click **OK**.
53. Select the **Primary Manager**.
54. Click **Push Updates to Manager**.
55. On the **IP360** web console, click **Test** to ensure that the connection is successful.



56. Any recurring scans will now forward the scan results to **Tripwire Log Center**. To ensure that a scan is recurring, select a scan in **Scan Profiles** on the main dashboard of the **IP360** web console.



- 57. Click **Edit**.
- 58. Click **Next** until the **Scan Schedule** page.
- 59. Select **Recurring**, and set a schedule for the scan according to the needs of the organization.



- 60. Click **Finish**.

2.20 Integration: Tripwire Enterprise and Backups

This section details how to back up **Tripwire Enterprise** configuration data.

To back up **Tripwire Enterprise** integrity information, refer to the database vendor’s documentation for backing up data.

2.20.1 Export Configuration from Tripwire Enterprise

1. On the Tripwire Enterprise server, navigate to C:\Program Files\Tripwire\TE\Server\bin.
2. Run the following command to stop **Tripwire Services**.
> `twservices stop`
3. Run the following command to export the configuration files to a backup (replace config.bak with the desired name of the backup).
> `tetool backup config.bak`
4. Run the following command to restart **Tripwire Services**.
> `twservices start`

2.20.2 Back Up the Tripwire Enterprise Configuration

The configuration backup will be stored in the file specified in step 3 of the previous section. To back this up to the enterprise backup server through a **Duplicati** client, see the documentation in [Section 2.8.4](#) for how to set up a **Duplicati** instance on the **Tripwire Enterprise** server, and then simply select the configuration file.

2.21 Integration: Cisco ISE and CryptoniteNXT

This section details an integration between **Cisco ISE** and **CryptoniteNXT**, allowing ISE to dictate the Cryptonite registration process based on the posture of the client machine. Please see the *CryptoniteNXT Generic RADIUS Integration Guide* for more details about the integration.

2.21.1 Requirements for Integrating Cisco ISE and CryptoniteNXT

As described in the ISE installation section, ISE requires RADIUS to be configured to perform posture. As such, this guide assumes the use of some sort of switch to provide RADIUS functionality.

CryptoniteNXT requires the switch to use L2 technologies for the RADIUS server, which means a captive portal will not work for this scenario. The feasibility of this depends on your networking setup.

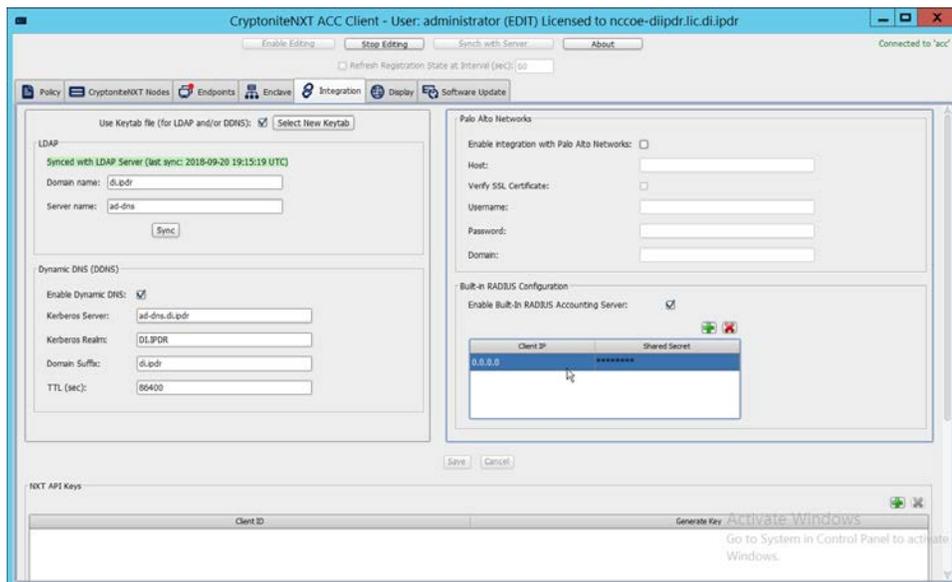
This integration requires the following:

1. The switch is bridged to CryptoniteNXT.
2. Cryptonite is configured to accept RADIUS packets from the switch (detailed below).
3. Clients on the switch's Local Area Network (LAN) authenticate to the switch via 802.1x (see your switch's documentation).

4. The switch is configured to accept CoA packets from ISE (see ISE installation).
5. The switch sends RADIUS accounting and authentication packets to Cisco ISE (see ISE installation).
6. ISE sends an authentication response to the switch and then later uses CoA to modify the authorization based on posture (see ISE installation).
7. If the authorization is successful, the switch tells the client and forwards the accounting packets to the CryptoniteNXT ACC node (see your switch's documentation).

2.21.2 Configuring CryptoniteNXT for RADIUS

1. Open the CryptoniteNXT GUI and log in.
2. Navigate to the **CryptoniteNXT Nodes** tab.
3. Click **Enable Editing**.
4. Select the **Endpoint** node, which will have your switch attached to it.
5. Under **Endpoint Node-Specific Configuration**, select **Strict Access** for **Access Control**.
6. Select **After Delay** for the next field.
7. Enter -1 for **Captive Portal delay**.
8. Enter 5 for the **Registration delay**.
9. Select the **Gateway** node.
10. Click **Save**.
11. Navigate to the Integration tab.
12. Under **Built-In RADIUS Configuration**, check the box next to Enable Built-In RADIUS Accounting Server.



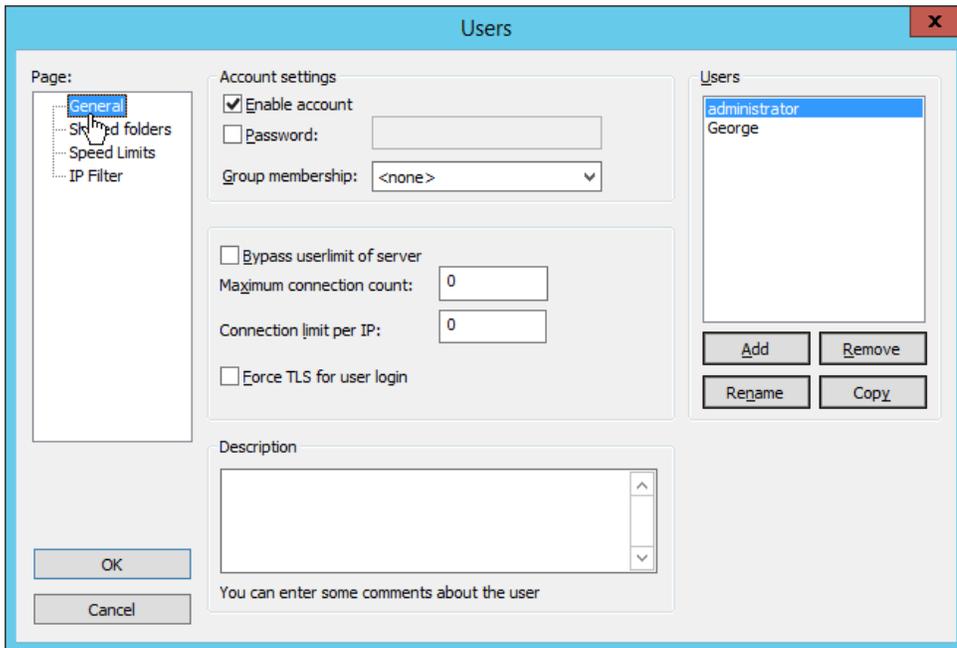
13. Click the **plus button** to add the IP of the switch as well as a shared secret. You can use 0.0.0.0/0 as the IP to accept RADIUS Accounting packets from all IPs, however this is not recommended in production.

2.22 Integration: Backups and GreenTec

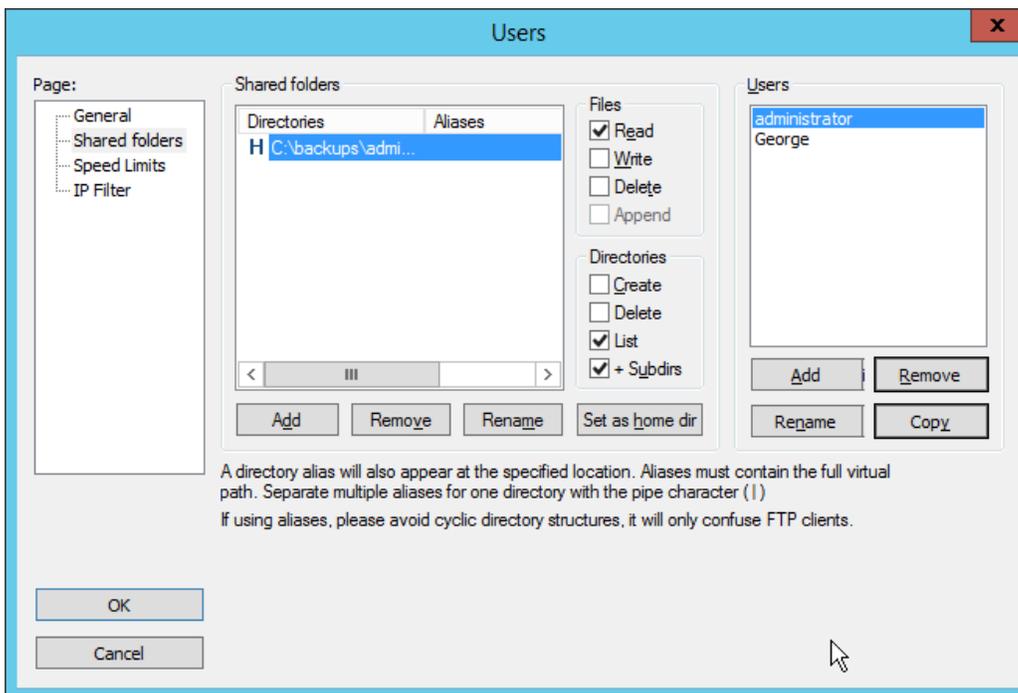
This section details integration between the backup capability and **GreenTec WORMdisks**. Because **GreenTec WORMdisks** provide write protection for files on the disk, they are an ideal place to store important backups. There are a couple options for this integration, but before these backups can be replicated onto secure storage, it is important to be able to identify the location of backups to be replicated.

2.22.1 Locate Backups with FileZilla and Duplicati

1. To locate backups in **FileZilla**, open the **FileZilla Server** console.
2. Click **Edit > Users**.

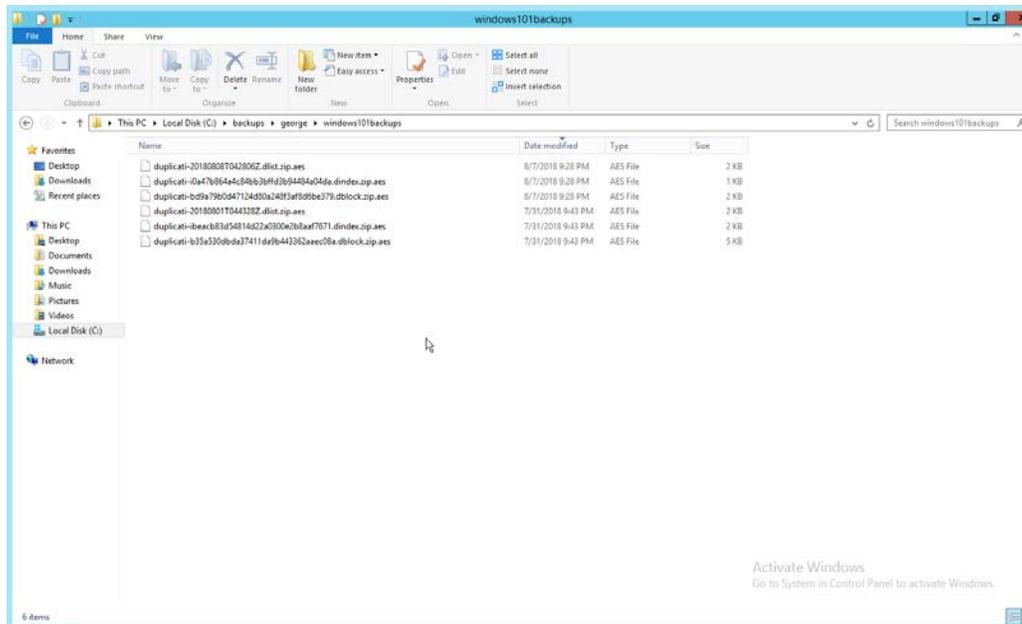


3. Click **Shared folders** in the left pane.



4. Under **Directories** is a list of directories in which the selected user can store backups. The one marked **H** is the default home directory.

- The path to the backups from the home directory is specified in the **Path on server** field in **Duplicati** (see [Section 2.8.6](#)).



- Each backup should have three associated files. An easy way to determine what files belong together is to check the **Date Modified** field. These files are encrypted.

2.22.2 Back Up to a GreenTec Disk

The first, most flexible option involves backing up the backup server to a separate server with **GreenTec WORMdisks**. Simply set up a **FileZilla** server on the **GreenTec** storage server and a **Duplicati** client on the backup server (see [Section 2.8](#) for these installation processes). When choosing where to store files on FileZilla, indicate a folder on the **GreenTec WORMdisk**. Sectors of the disk can be locked using the mechanism in [Section 2.6.4](#), providing firmware-level write security for any backups in the locked sectors.

There are some considerations when doing this. First, if this is done on a schedule and permanent locks are used, space will be consumed quickly and the **WORMdisks** will need replacements as the space cannot be reused. The trade-off between space and backup frequency must be considered—a lower backup frequency inevitably means more data loss in the event of a restoration, while higher backup frequency increases the cost of maintaining secure storage.

Alternatively, secure storage can be used for specific types of backups, such as “golden disks”—which would contain backups of the basic level of functionality required for the enterprise without necessarily

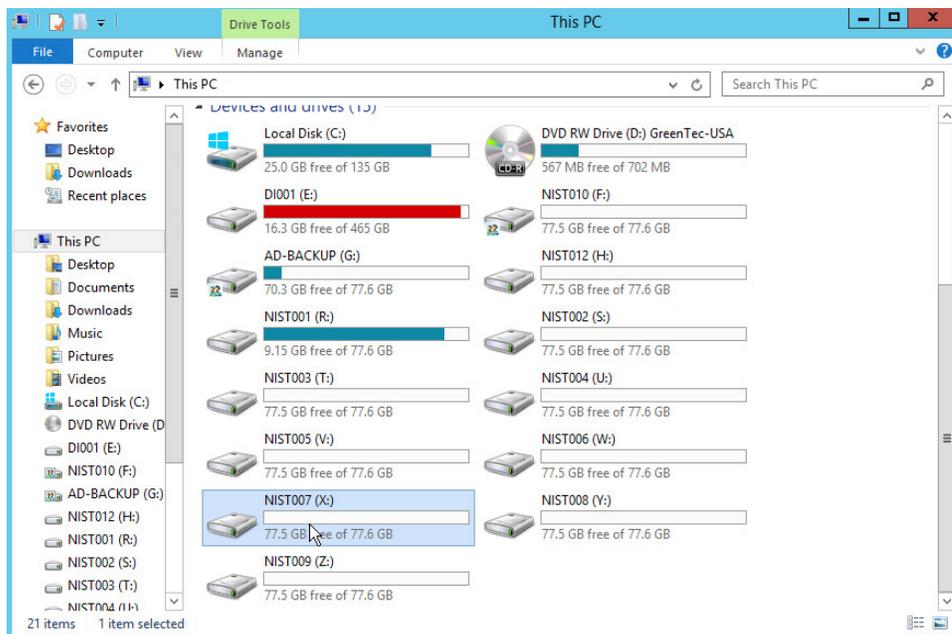
utilizing a backup schedule. This would afford protection for some basic functionality but would forfeit the secure storage capability for day-to-day data.

In addition to the options above, there are other ways to minimize wasted space on a GreenTec disk. Temporary Locks, or TLocks, can be employed after the data is backed up to a GreenTec disk to protect data integrity while making less space unavailable for future use. After the drive is full, a permanent lock should still be executed. Wasted space can also be minimized with the use of dynamic partitions, or with the Force-Field Write-Once File System, which can also reduce the overhead administration of the GreenTec disk.

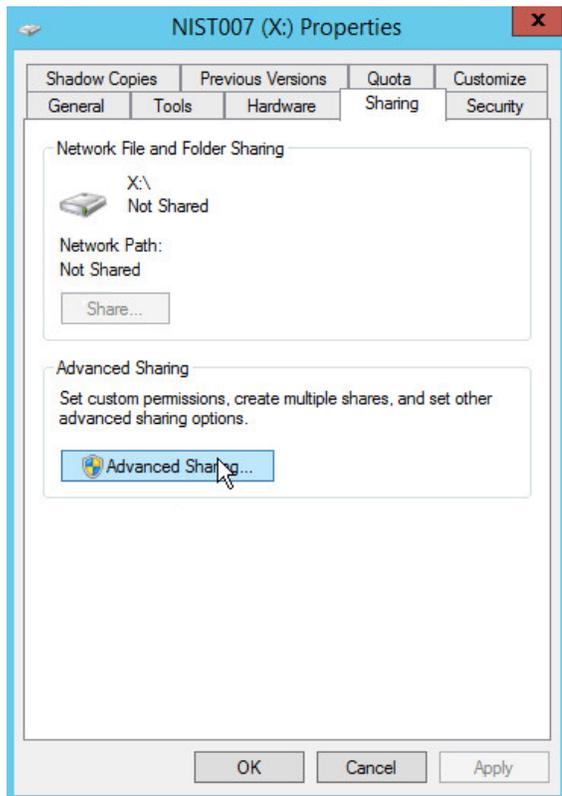
2.22.3 Configure Network-Accessible GreenTec Disk

Another option for GreenTec disks is to make them network accessible. This allows them to be used specifically in situations where secure storage protection is desired, and it makes them options for backup locations even on servers to which they are not necessarily physically connected.

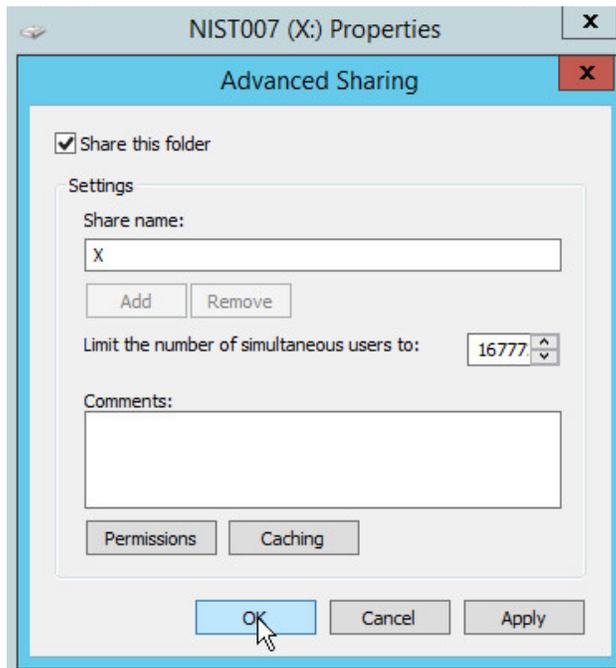
1. To configure a GreenTec disk to be network accessible, right-click the disk on the GreenTec server.



2. Click **Share With > Advanced Sharing**.



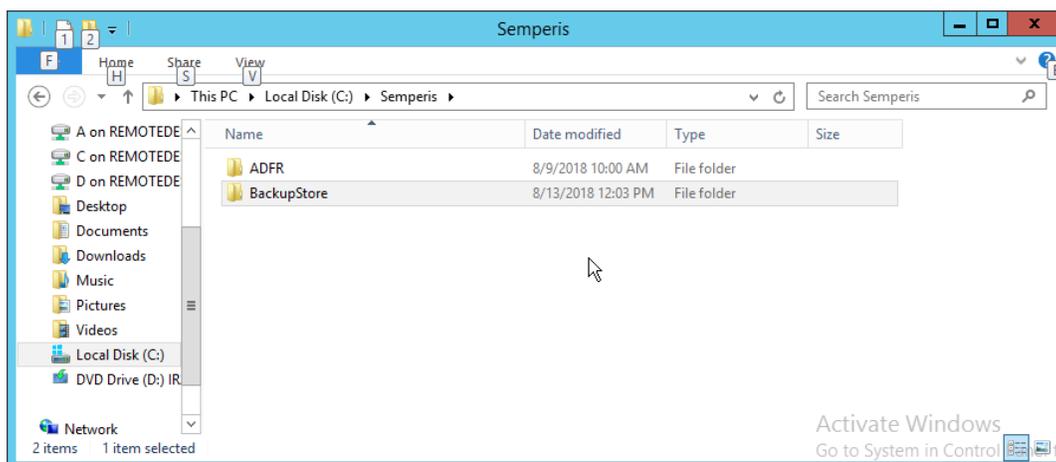
3. Click **Advanced Sharing**.
4. Check the box next to **Share this folder**.
5. Enter a name for the drive if desired.



6. Click **OK**.
7. Click **Close**.
8. The drive should now be accessible at **//SERVER-NAME/X**.

2.22.4 Secure Storage for Semperis ADFR

1. On the Semperis ADFR server, the default backup location is C:\Semperis.
2. In this folder there is metadata for the backups (C:\Semperis\ADFR) as well as the backups themselves (C:\Semperis\BackupStore).



It is important to consider the limitations of the backup software when considering whether to replicate backups to secure storage. Ideally, the replication of backups ensures that they can be used on a separate server when the original server is affected by an incident. The replication of backups in this case can offer some write protection for these specific backup files, but if the entire server is lost, it is not guaranteed that the backups will be usable on a new instance of ADFR. This risk can be mitigated by exporting the configuration of the ADFR server for the purpose of building a failover ADFR server.

Though these backups can be replicated to WORMdisks, this is currently not supported by Semperis ADFR. Instead, Semperis ADFR offers a different type of “secure storage” by not joining to the domain, allowing the machine to be taken offline and brought online only during creation/application of a backup.

2.23 Integration: Micro Focus ArcSight and FileZilla

In this section an integration between ArcSight and FileZilla is detailed so that logs from FileZilla are forwarded to ArcSight by using an ArcSight syslog file connector.

2.23.1 Enable Logs in FileZilla

1. On the server with **FileZilla** installed, open **FileZilla Server**.

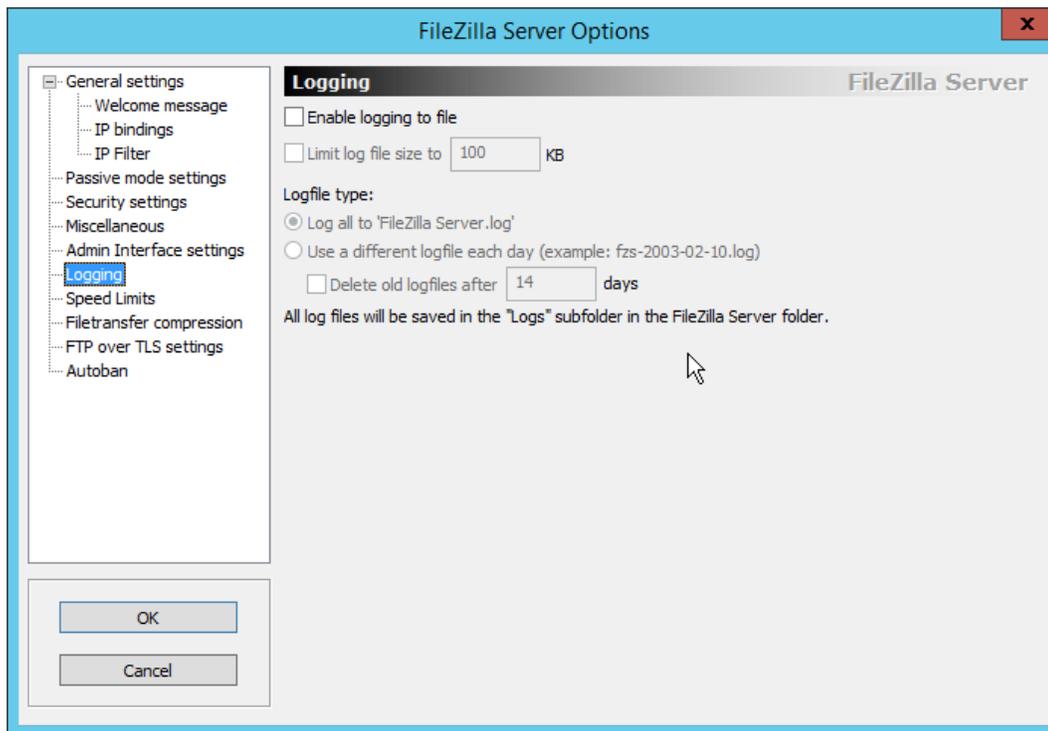
The screenshot shows the FileZilla Server (127.0.0.1) interface. The main window displays a terminal window with the following logs:

```
(not logged in) (192.168.1.138)> 220 FileZilla Server 0.9.60 beta
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> 220 Please visit https://filezilla-project.org/
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> AUTH TLS
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> 234 Using authentication type TLS
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> TLS connection established
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> USER george
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> 331 Password required for george
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> PASS *****
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 230 Logged on
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PBSZ 0
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 200 PBSZ=0
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PROT P
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 200 Protection level set to P
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> OPTS utf8 on
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 202 UTF8 mode is always enabled. No need to send this command.
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PWD
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 257 "/" is current directory.
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> TYPE I
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 200 Type set to I
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PASV
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 227 Entering Passive Mode (192.168.1.121,199,178)
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> RETR windows10backups/duplicati-bd9a73b0d47124d80a248f3af8d6e379.dblock.zip.aes
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 150 Opening data channel for file download from server of "/windows10backups/duplicati-bd9a73b0d47124d80a248f3af8d6e379.dblock.zip.aes"
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> TLS connection for data connection established
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 226 Successfully transferred "/windows10backups/duplicati-bd9a73b0d47124d80a248f3af8d6e379.dblock.zip.aes"
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> QUIT
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 221 Goodbye
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> disconnected.
Retrieving settings, please wait...
Done retrieving settings
```

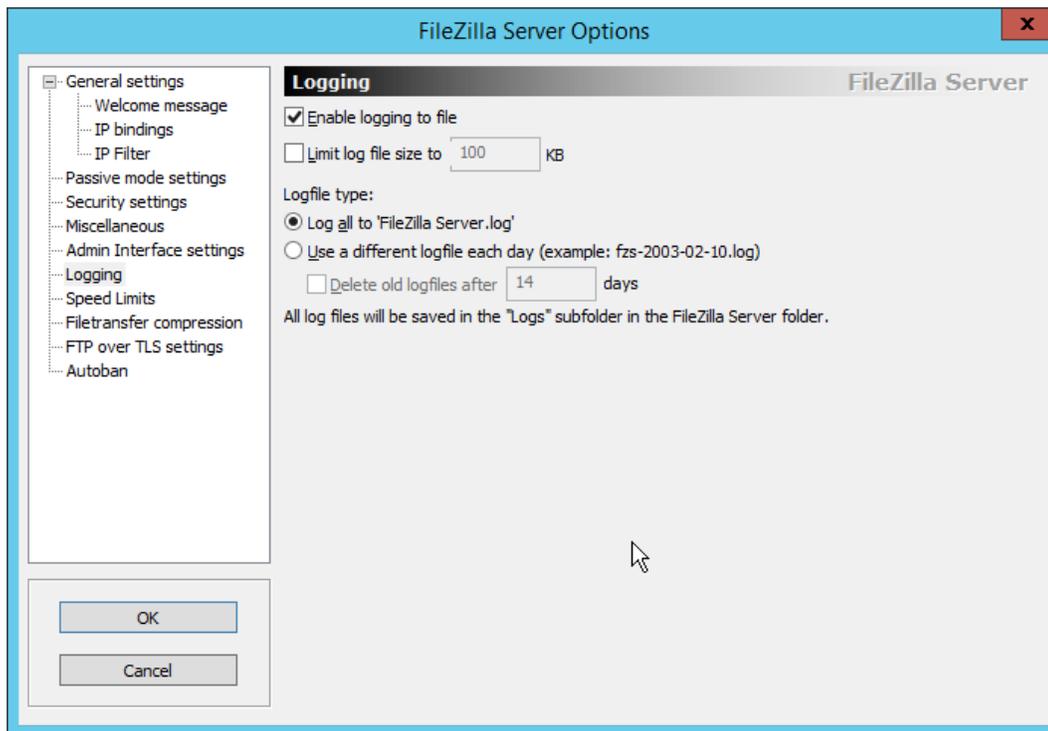
Below the terminal window, there is a table with columns: ID, Account, IP, Transfer, Progress, Speed. The table is currently empty.

At the bottom of the window, it shows: 7,712 bytes received 0 B/s 39,760 bytes sent 0 B/s

2. Click **Edit > Settings**.
3. Click **Logging**.



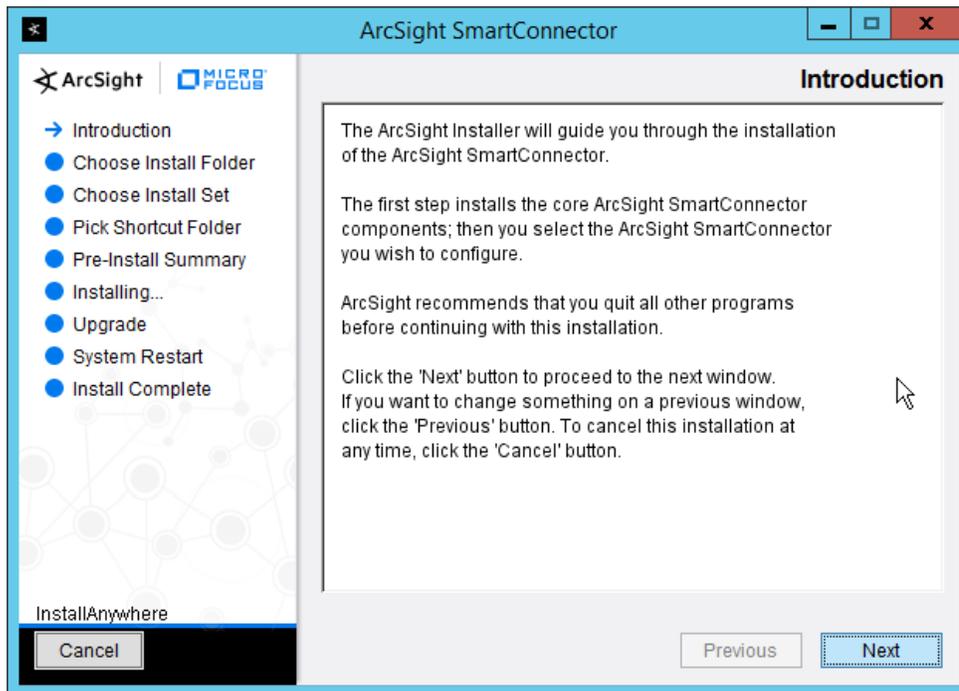
4. Check the box next to **Enable logging to file**.



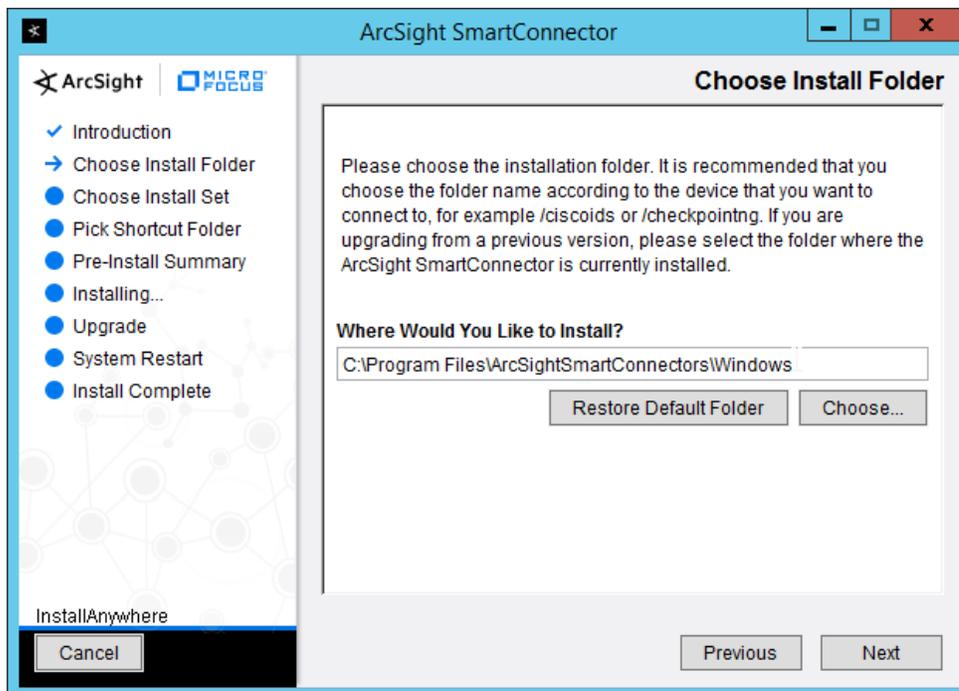
5. Click **OK**.

2.23.2 Install Micro Focus ArcSight

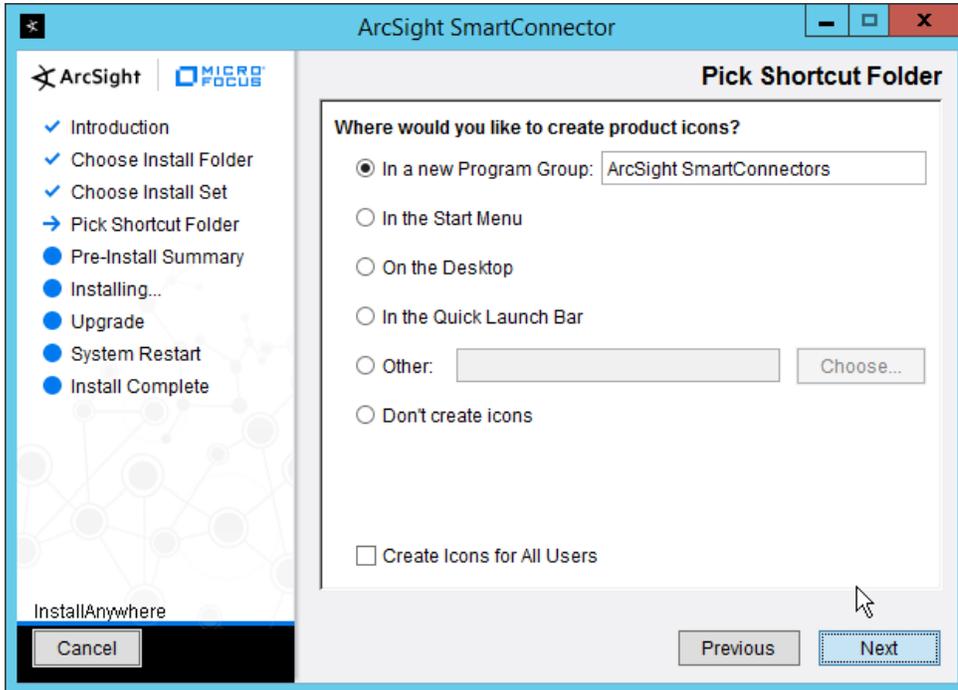
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



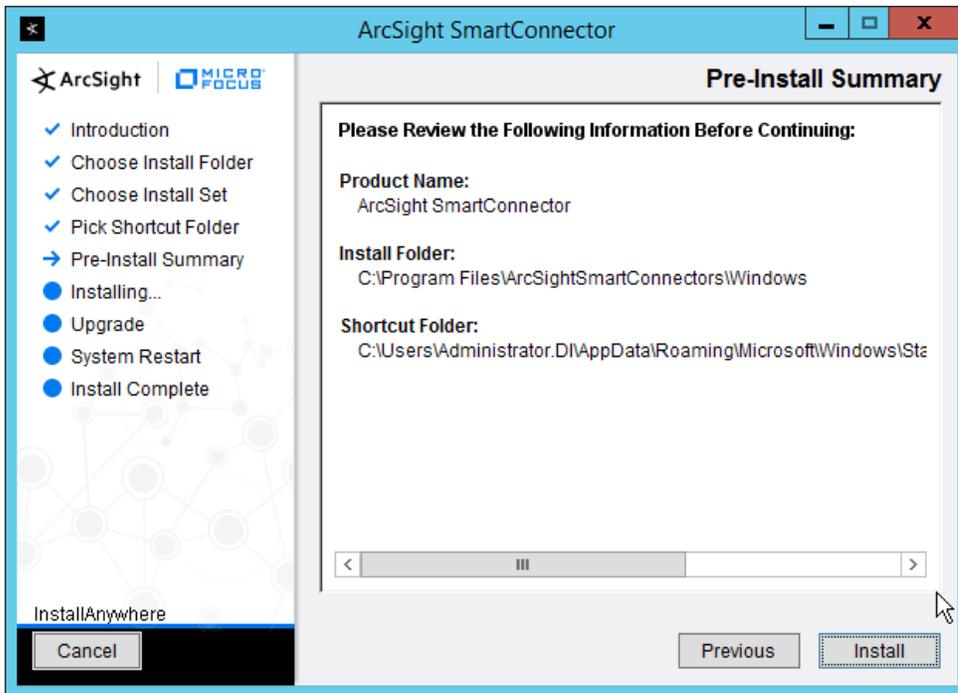
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



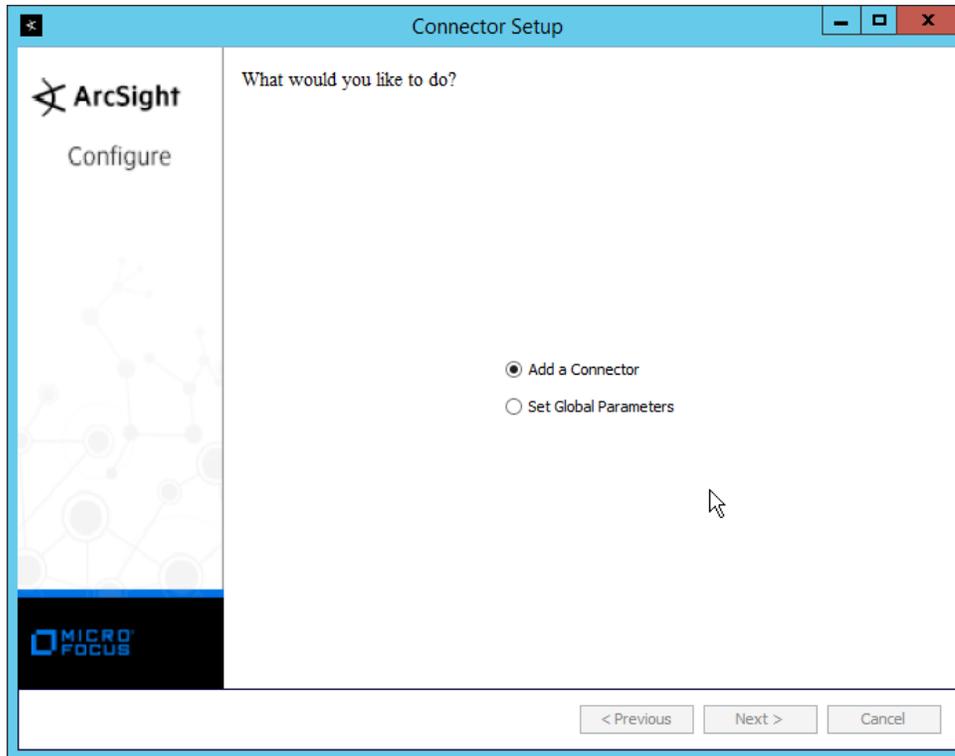
4. Click **Next**.



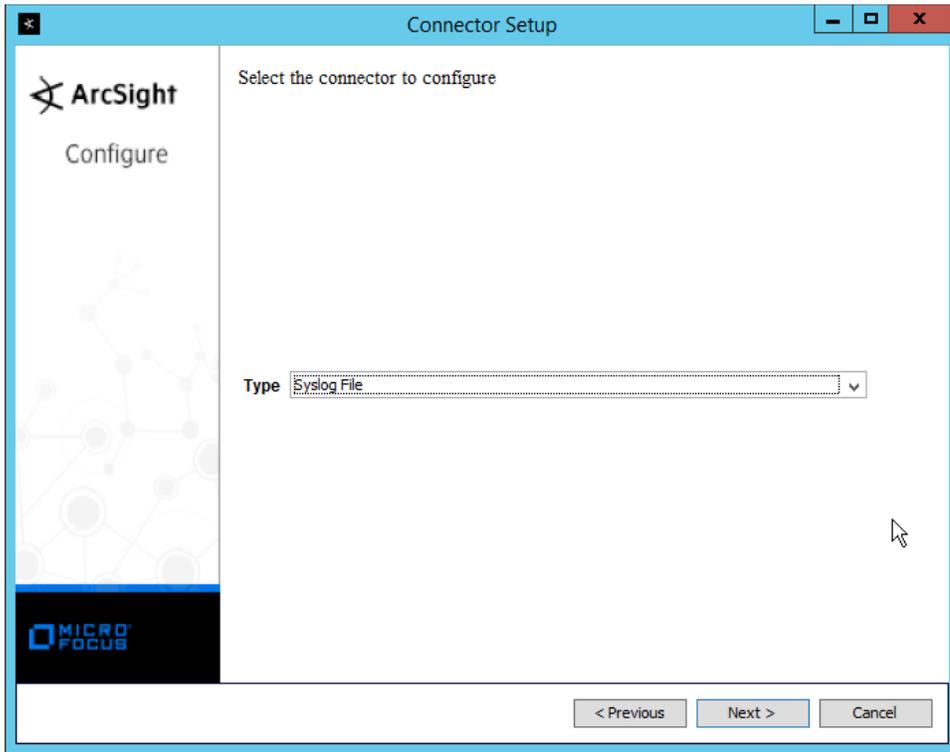
5. Click **Next**.



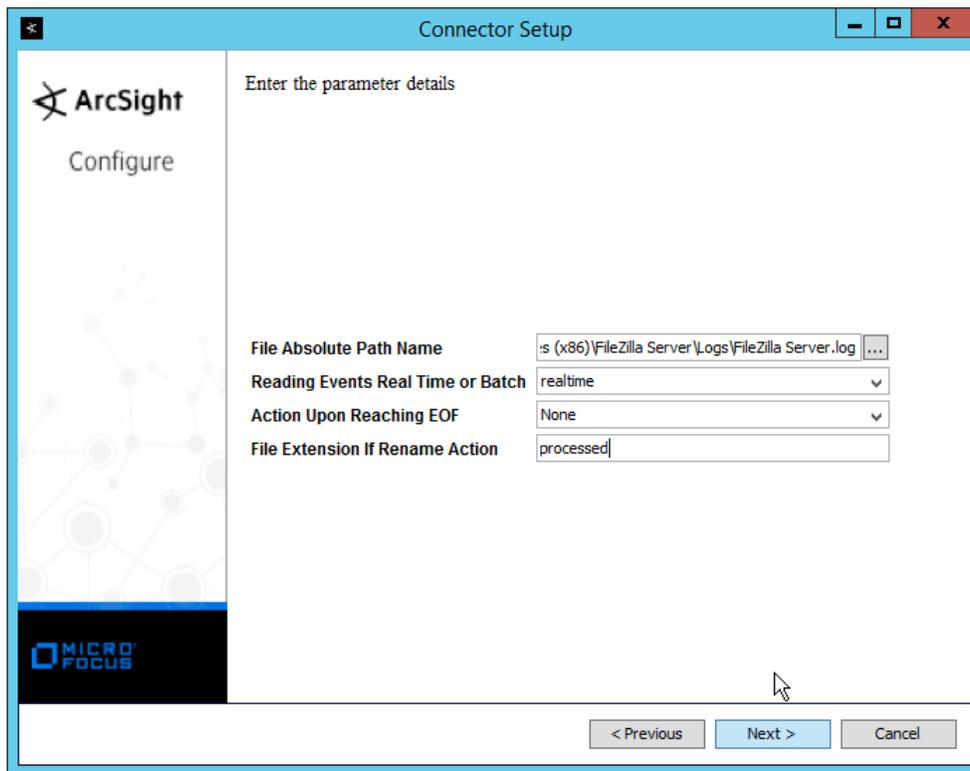
6. Click **Install**.
7. Select **Add a Connector**.



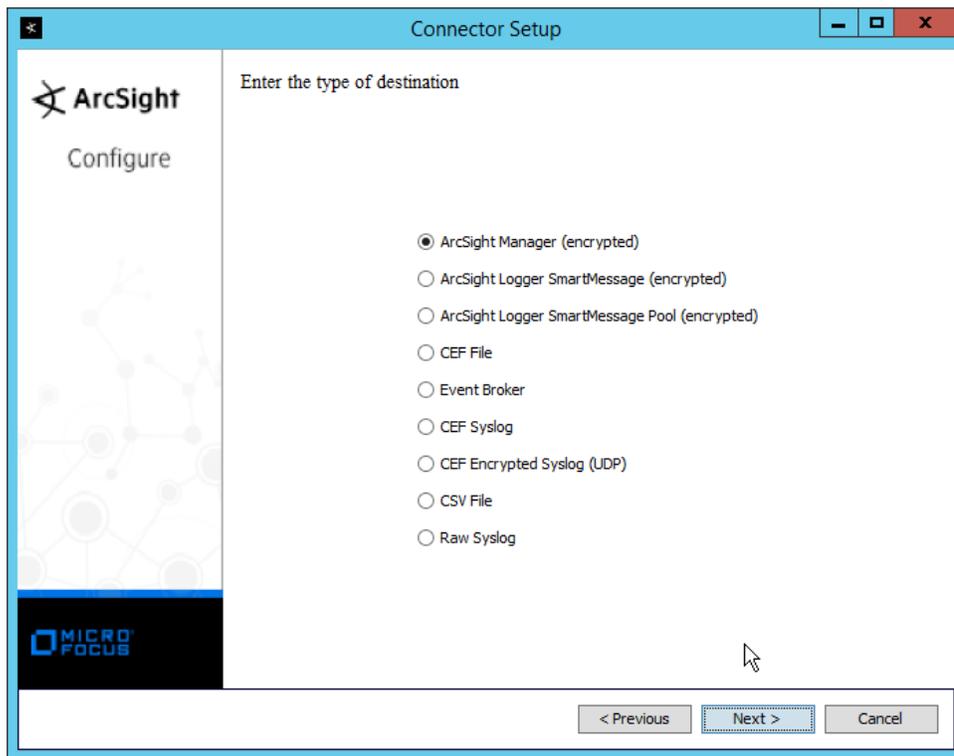
8. Click **Next**.
9. Select **Syslog File**.



10. Click **Next**.
11. Enter C:\Program Files (x86)\FileZilla Server\Logs\FileZilla Server.log for **File Absolute Path Name**.

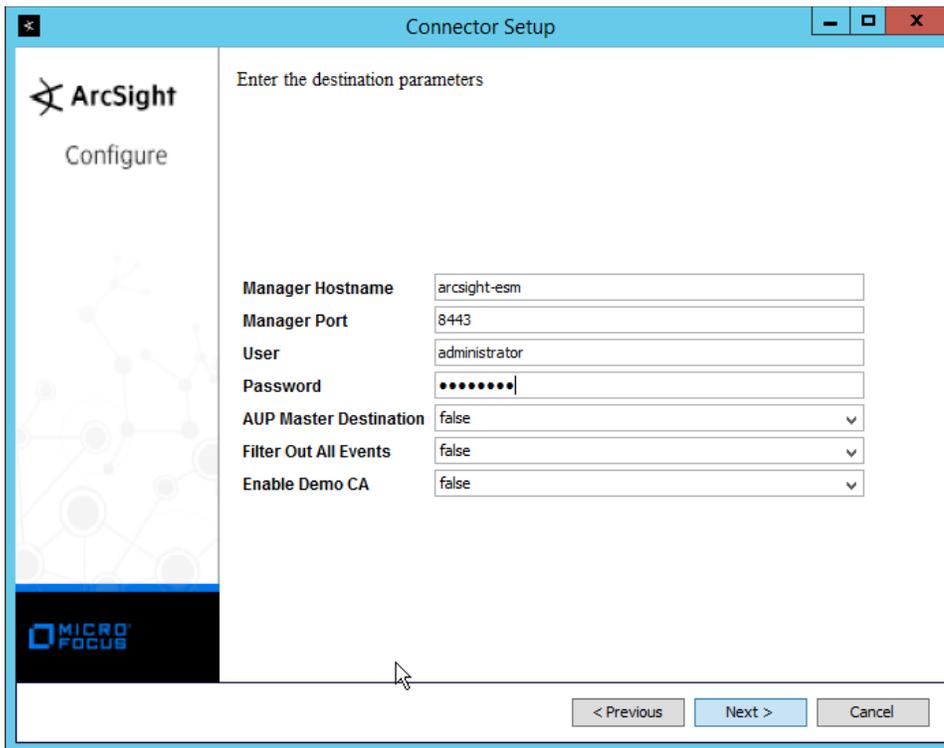


12. Click **Next**.
13. Select **ArcSight Manager (encrypted)**.

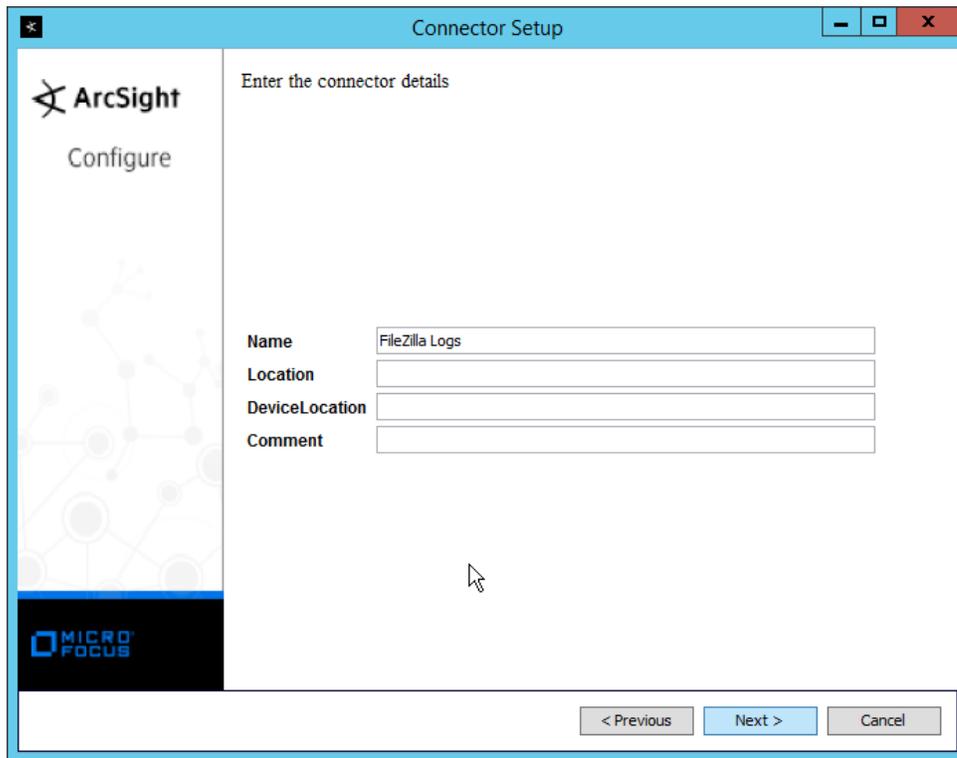


14. Click **Next**.

15. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.

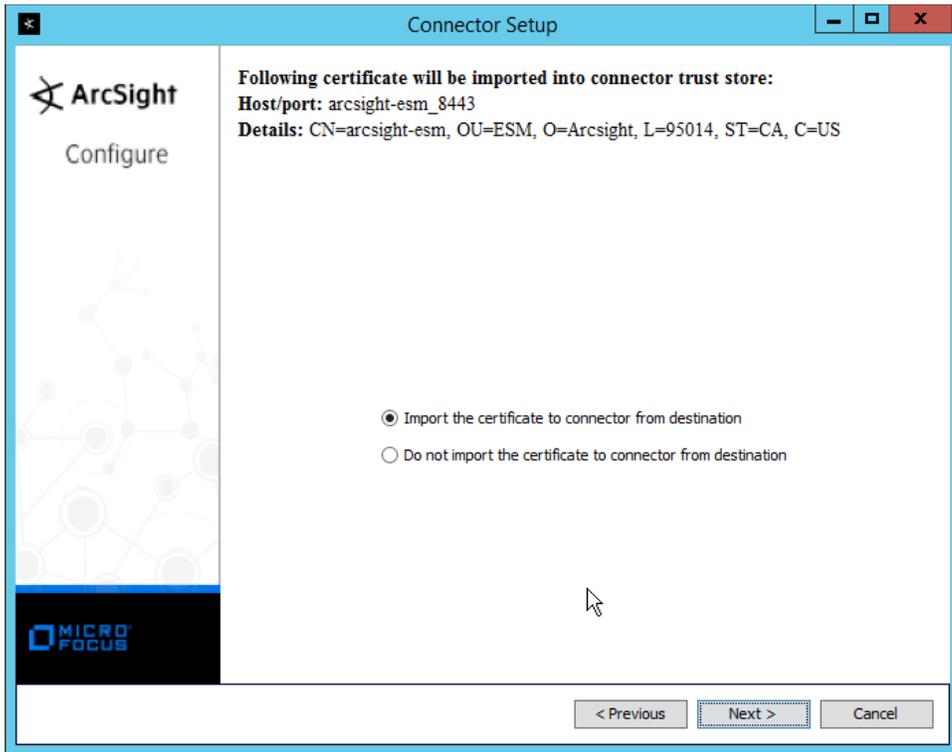


16. Click **Next**.
17. Enter identifying details about the system (only **Name** is required).

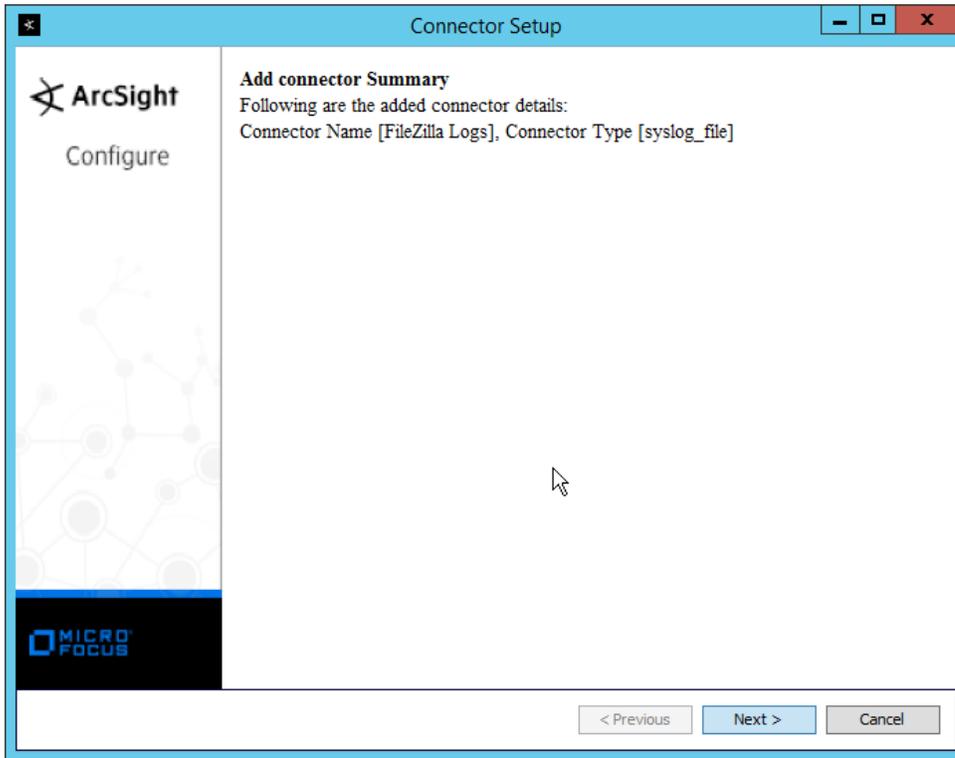


18. Click **Next**.

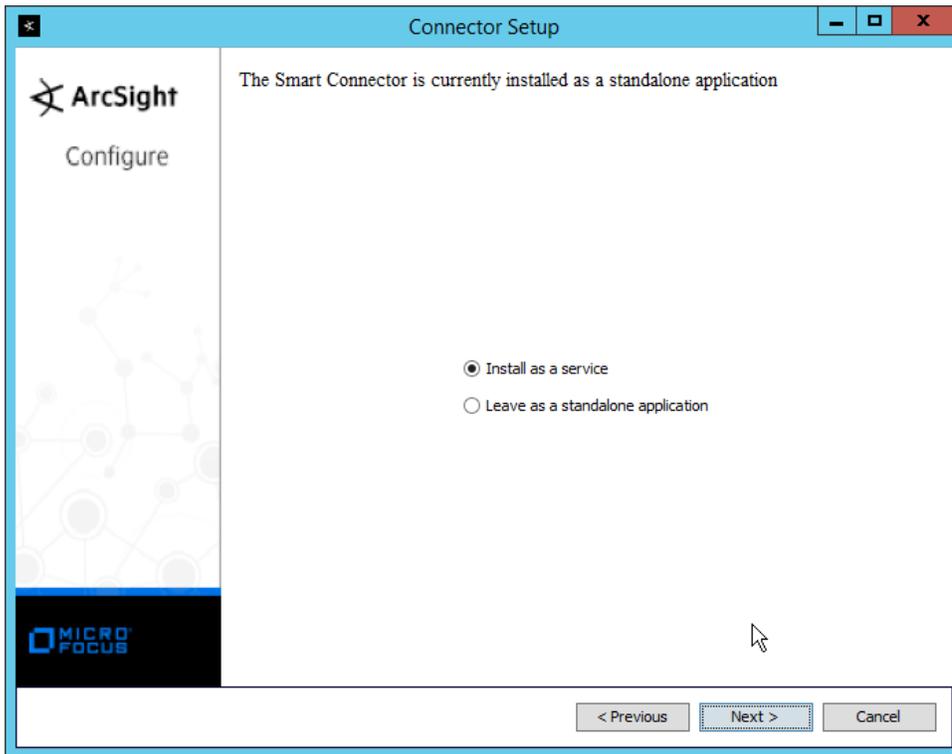
19. Select **Import the certificate to connector from destination**.



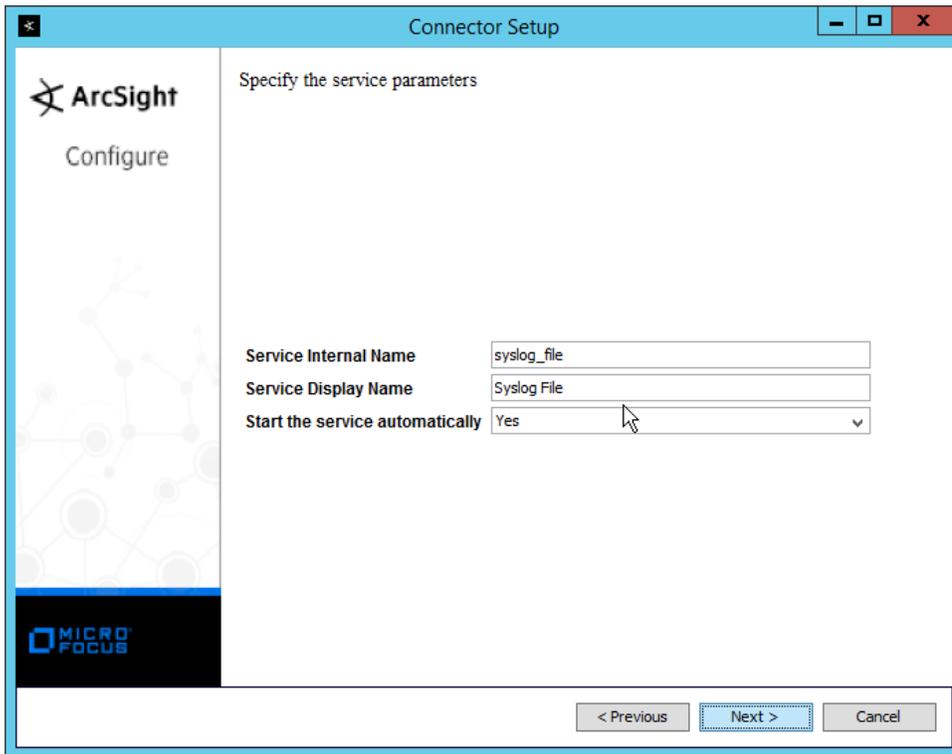
20. Click **Next**.



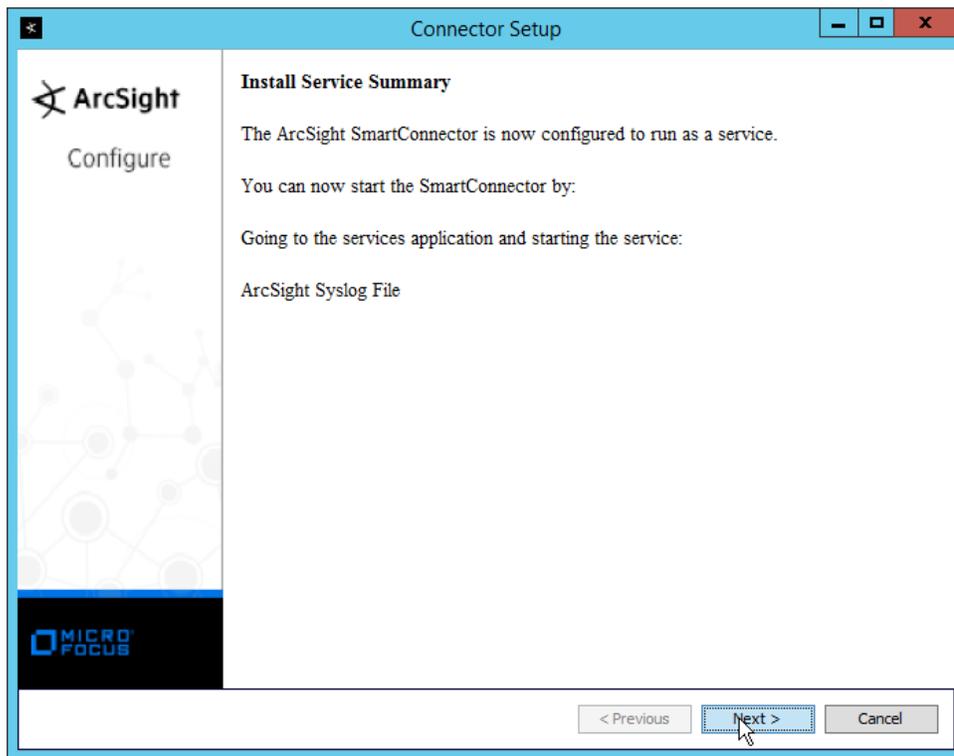
21. Click **Next**.
22. Select **Install as a service**.



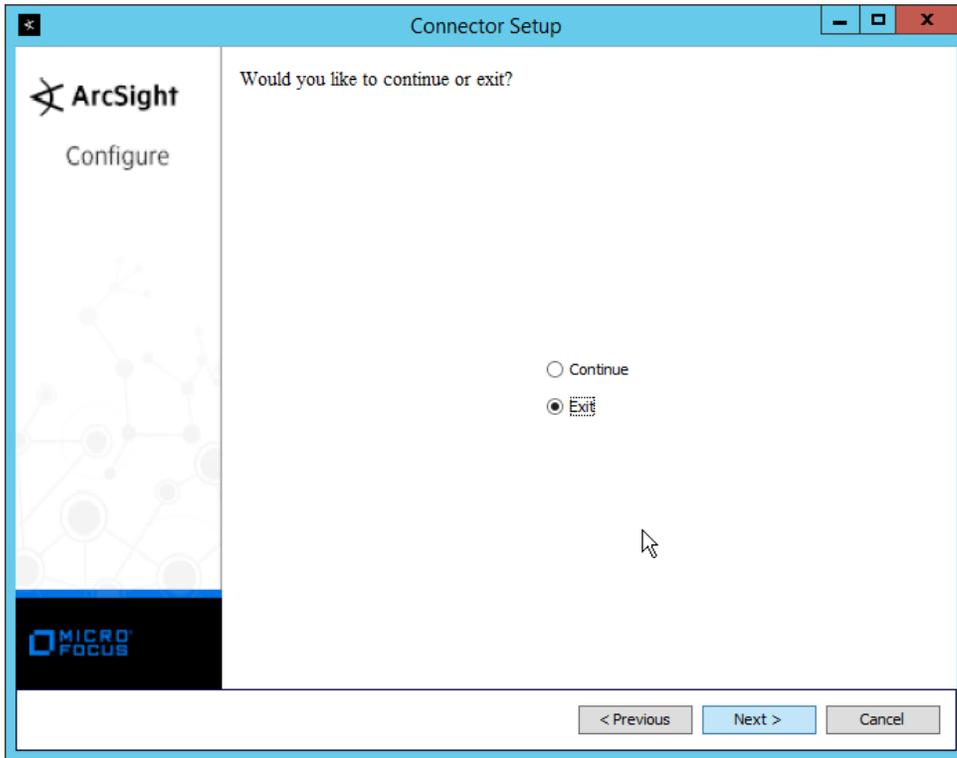
23. Click **Next**.



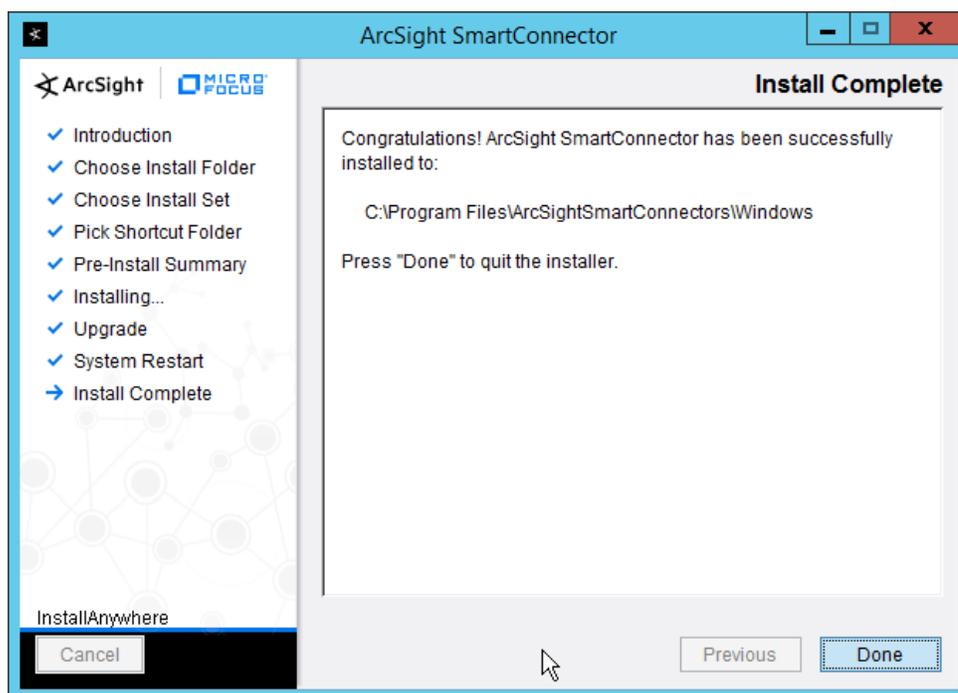
24. Click **Next**.



25. Click **Next**.
26. Select **Exit**.



27. Click **Next**.



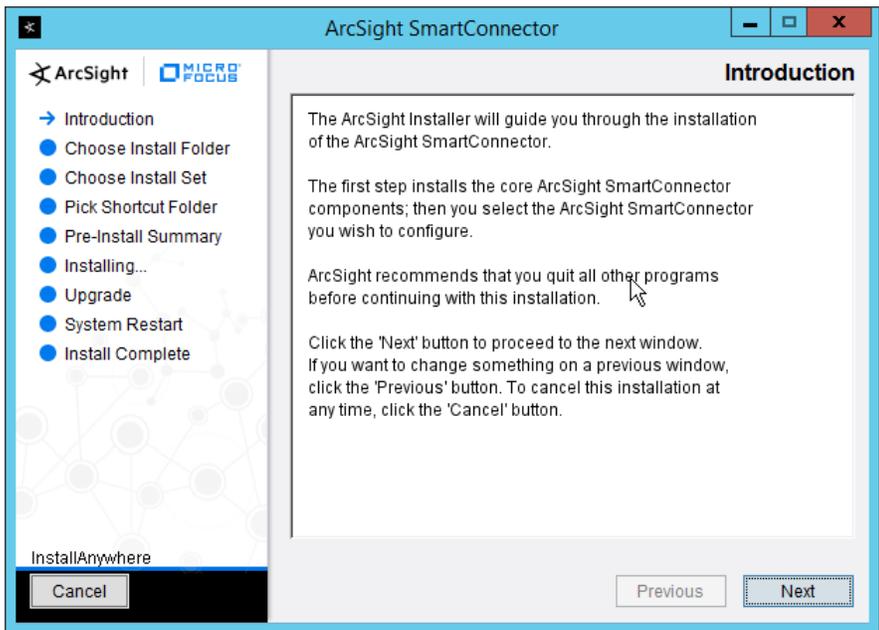
28. Click **Done**.

2.24 Integration: Micro Focus ArcSight and Tripwire

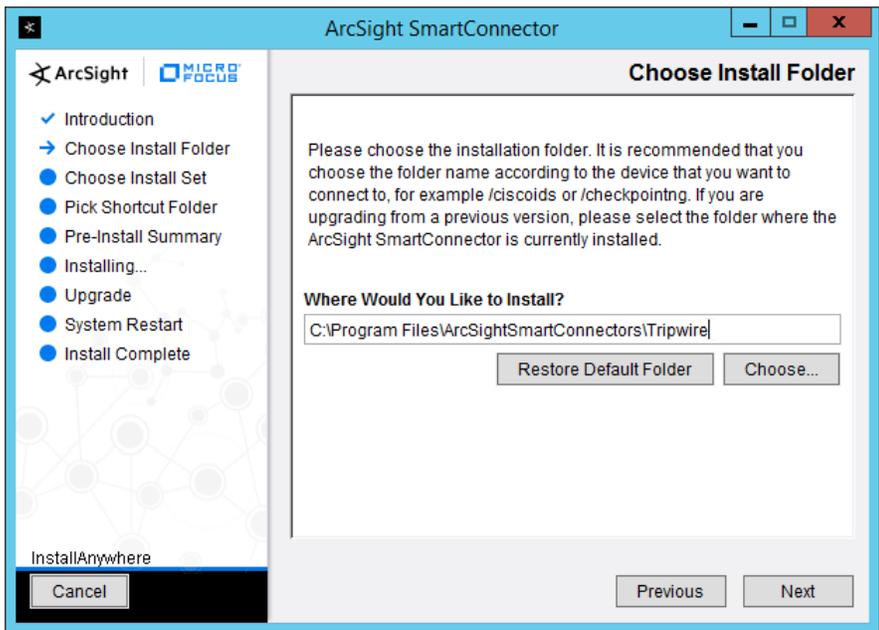
This section details forwarding logs from **Tripwire Log Center** to **Micro Focus ArcSight**. This will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight**, assuming those logs are being collected by **Tripwire Log Center**.

2.24.1 Install Micro Focus ArcSight

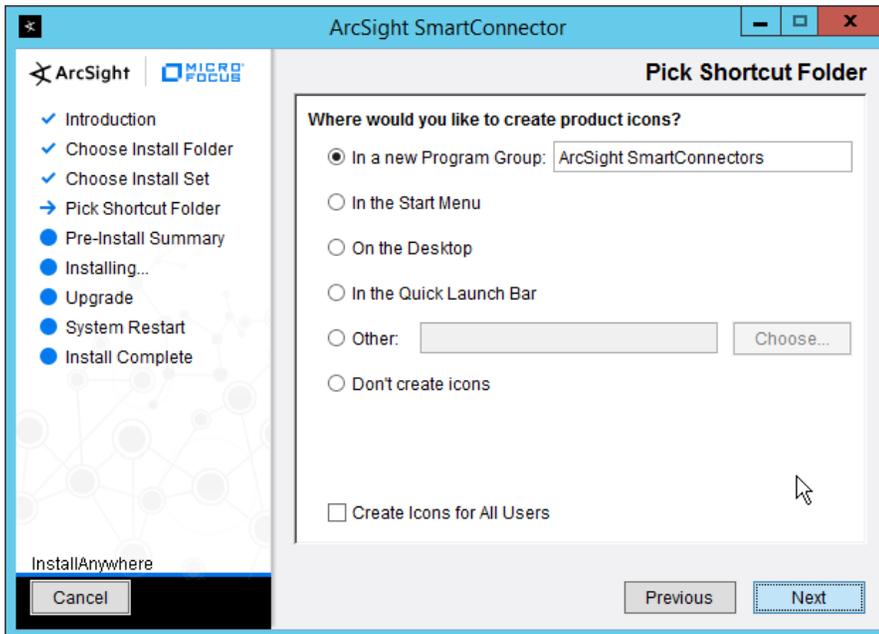
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running Tripwire Log Center.



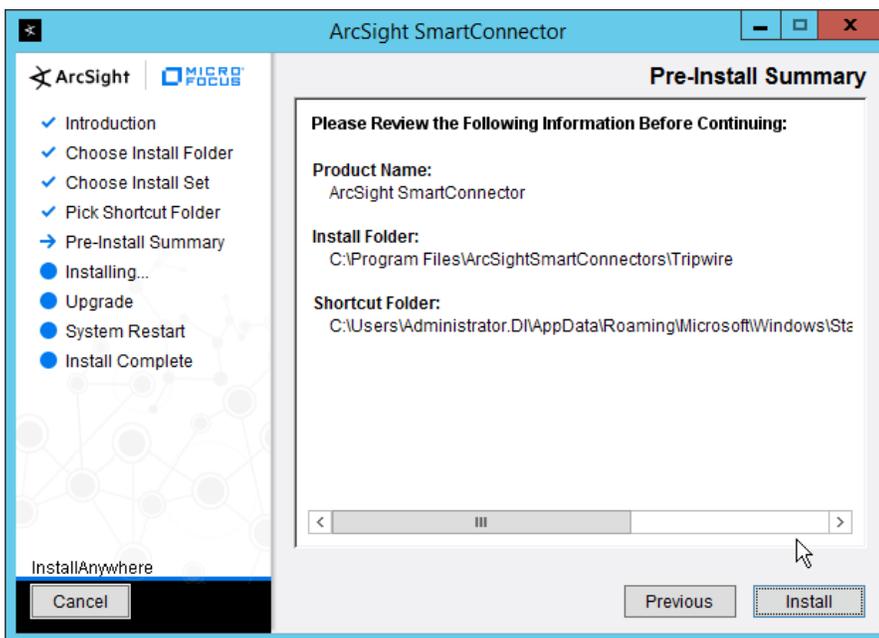
2. Click **Next**.



3. Enter C:\Program Files\ArcSightSmartConnectors\Tripwire.

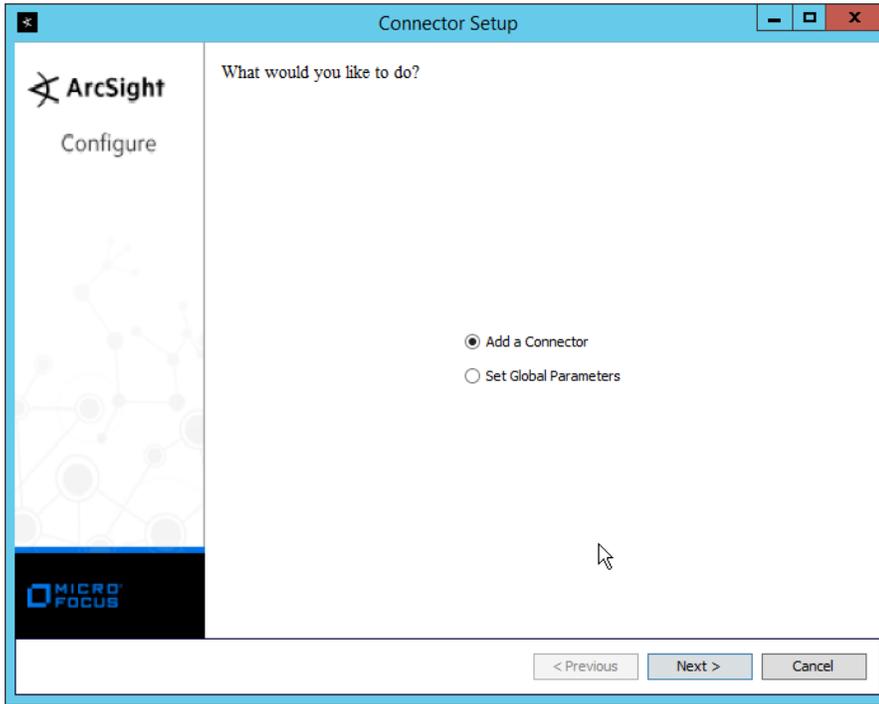


4. Click **Next**.

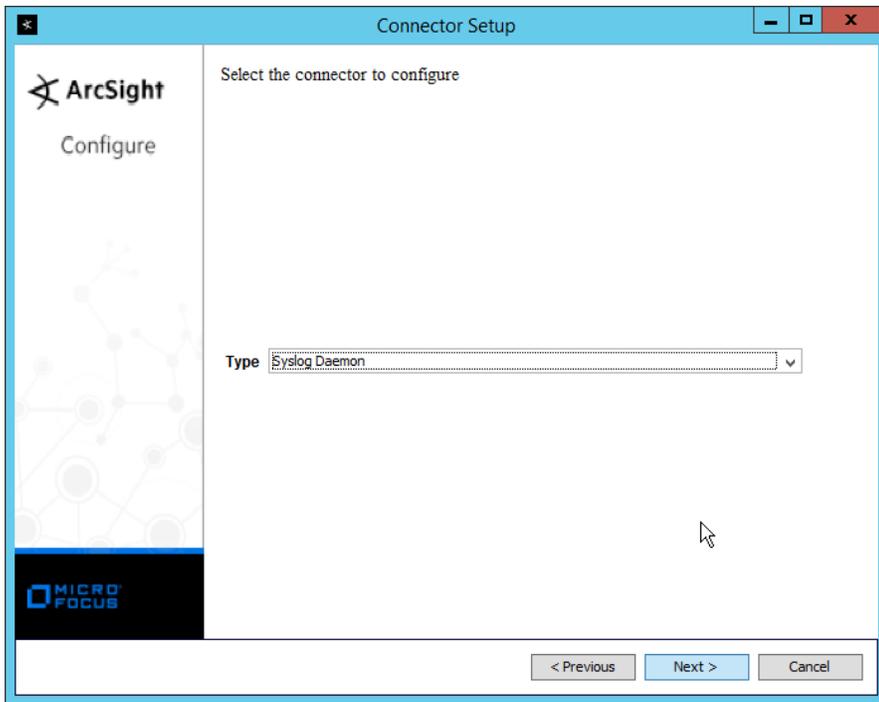


5. Click **Install**.

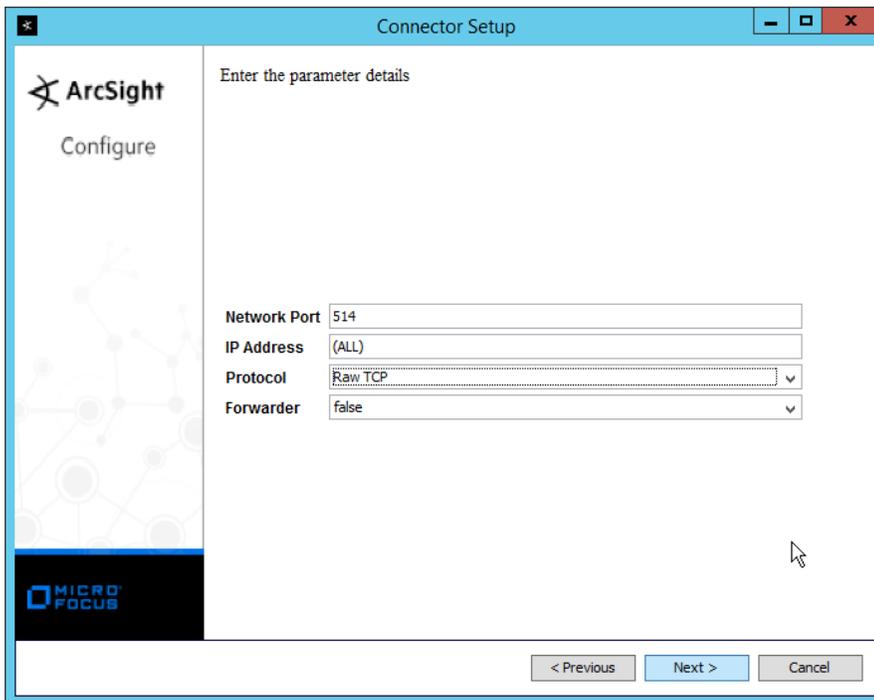
6. Select **Add a Connector**.



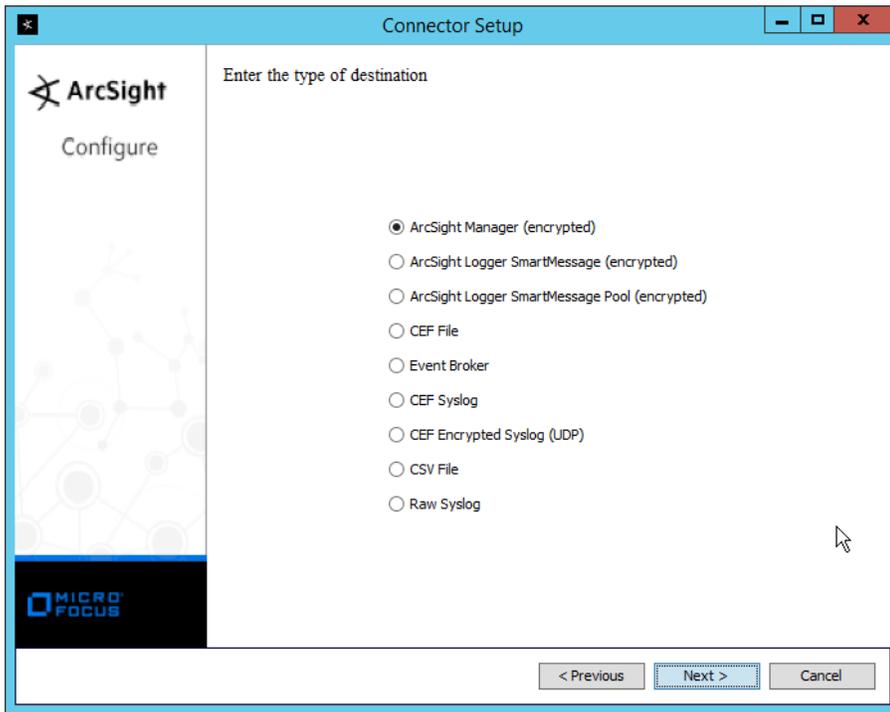
7. Click **Next**.
8. Select **Syslog Daemon**.



9. Click **Next**.
10. Enter a port for the daemon to run on.
11. Select **Raw TCP** for **Protocol**.

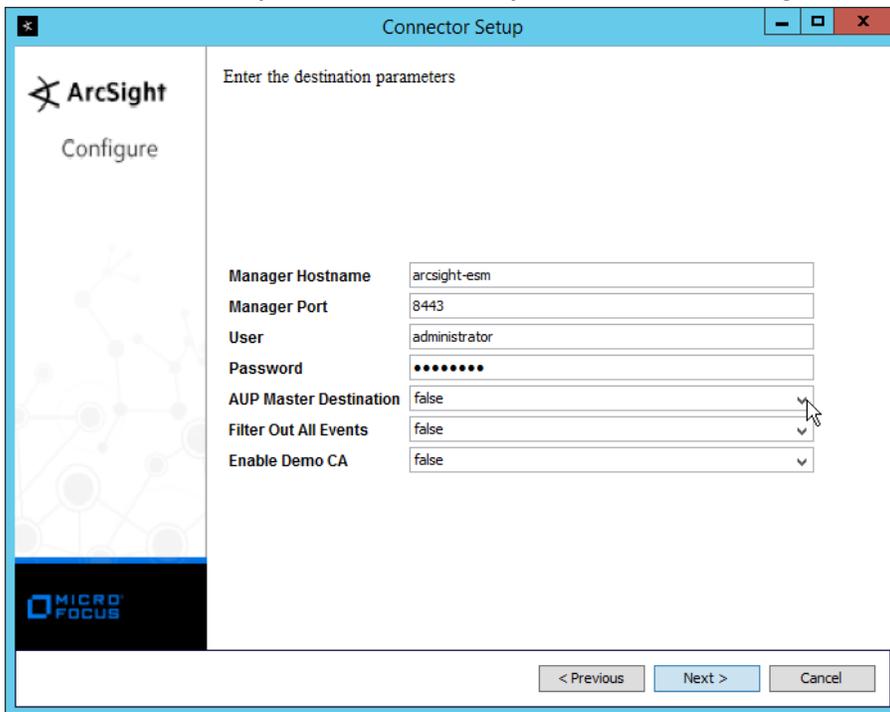


12. Click **Next**.
13. Select **ArcSight Manager (encrypted)**.



14. Click **Next**.

15. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.



16. Click **Next**.

17. Enter identifying details about the system (only **Name** is required).

Connector Setup

ArcSight
Configure

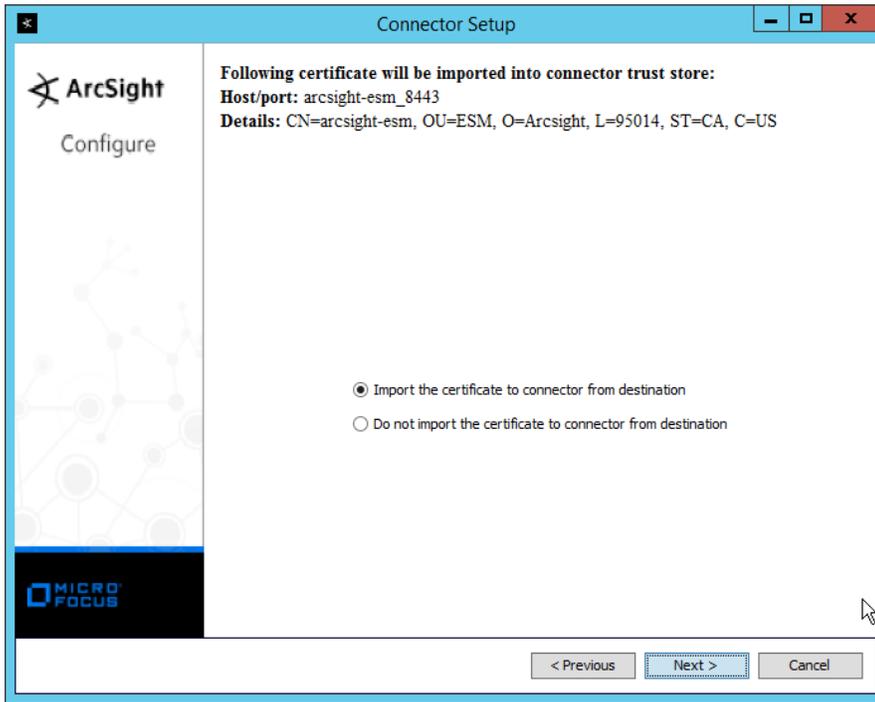
Enter the connector details

Name: Tripwire Log Center
Location:
DeviceLocation:
Comment:

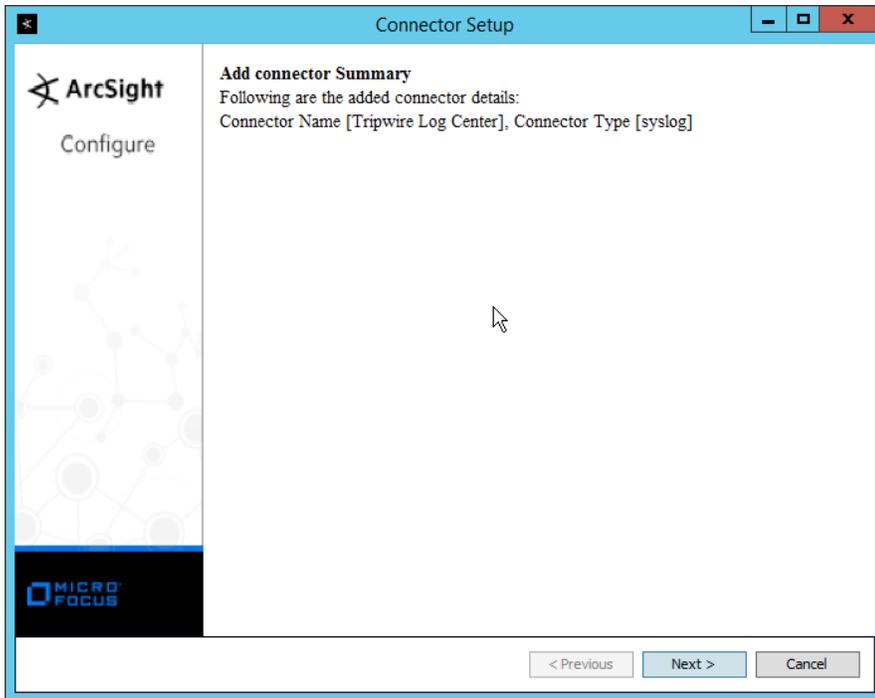
< Previous Next > Cancel

18. Click **Next**.

19. Select **Import the certificate to connector from destination**.

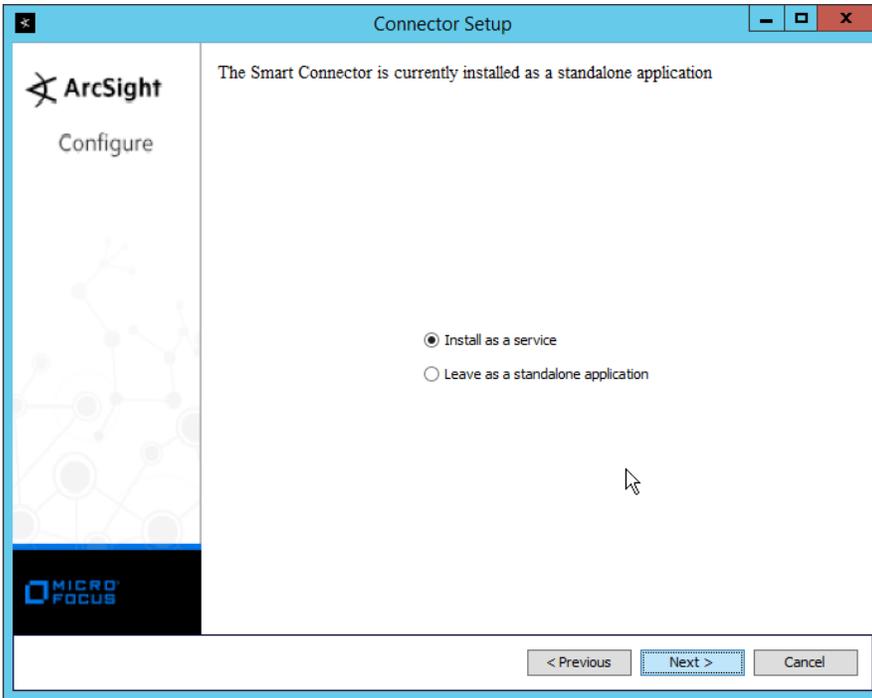


20. Click **Next**.

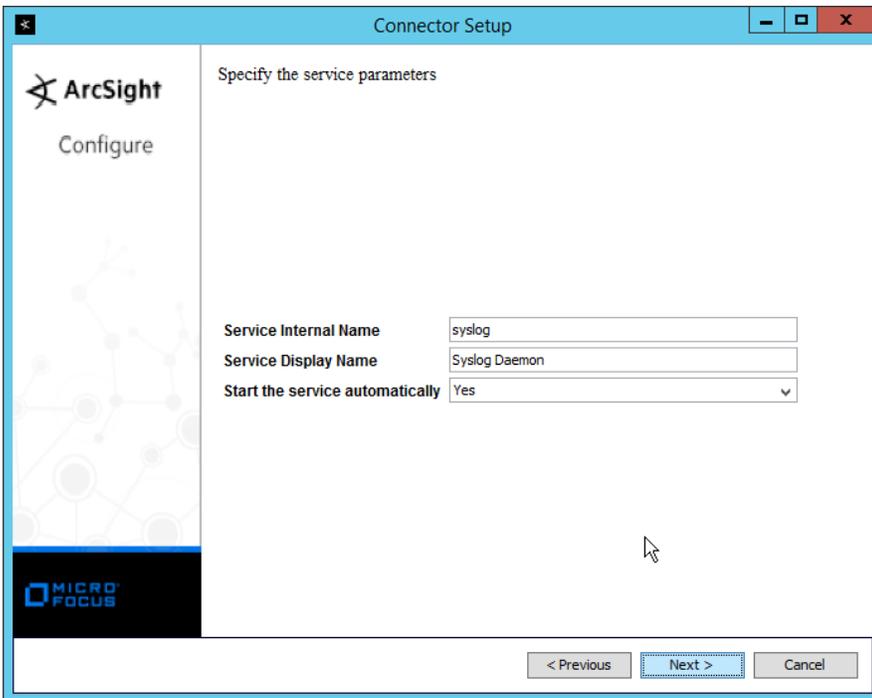


21. Click **Next**.

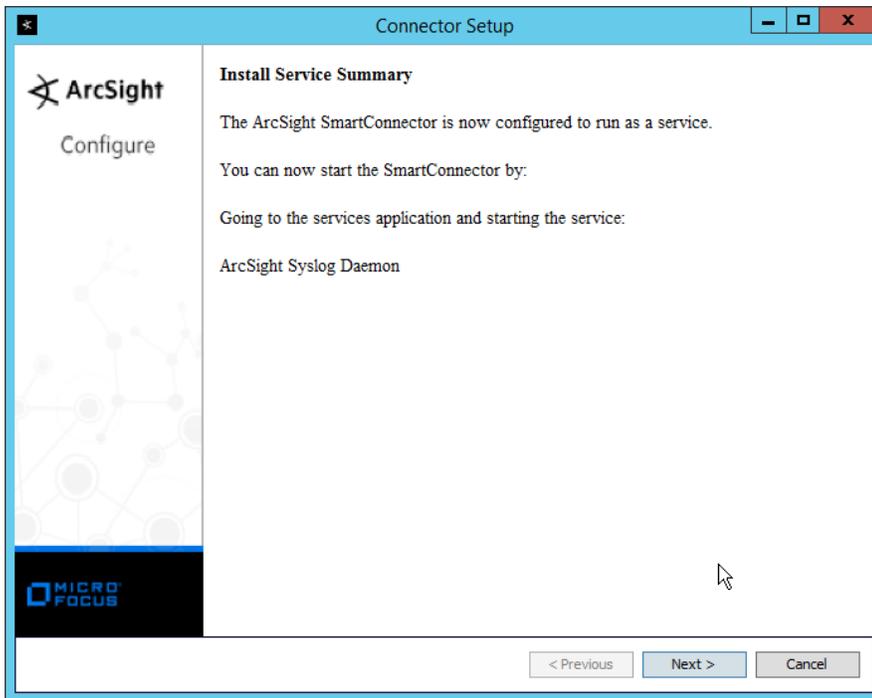
22. Select **Install as a service**.



23. Click **Next**.

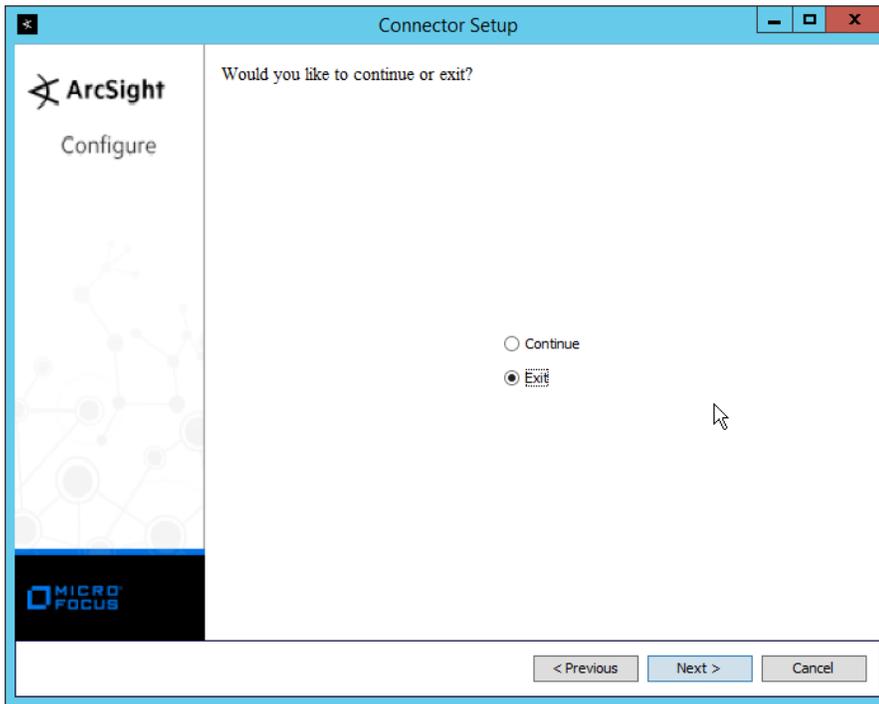


24. Click **Next**.

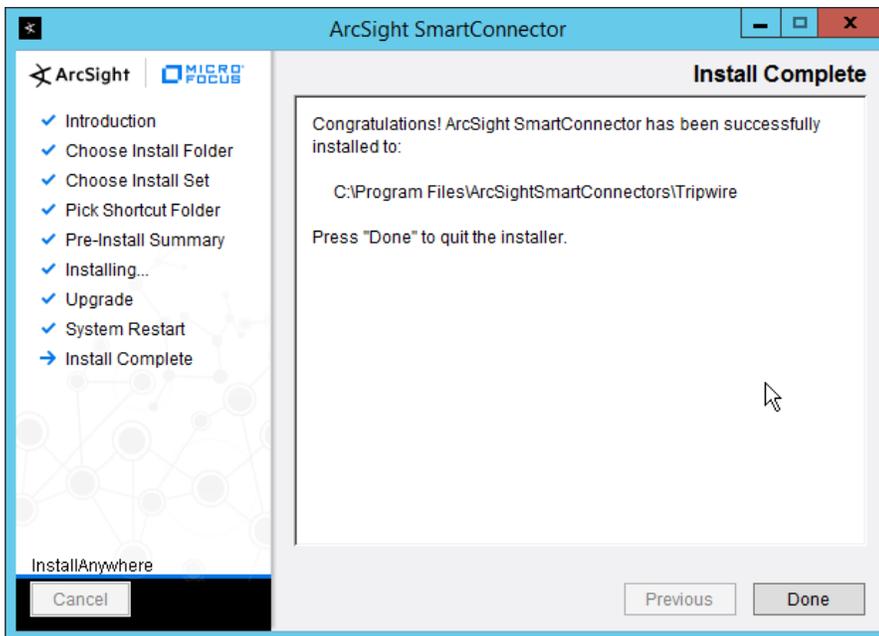


25. Click **Next**.

26. Select **Exit**.



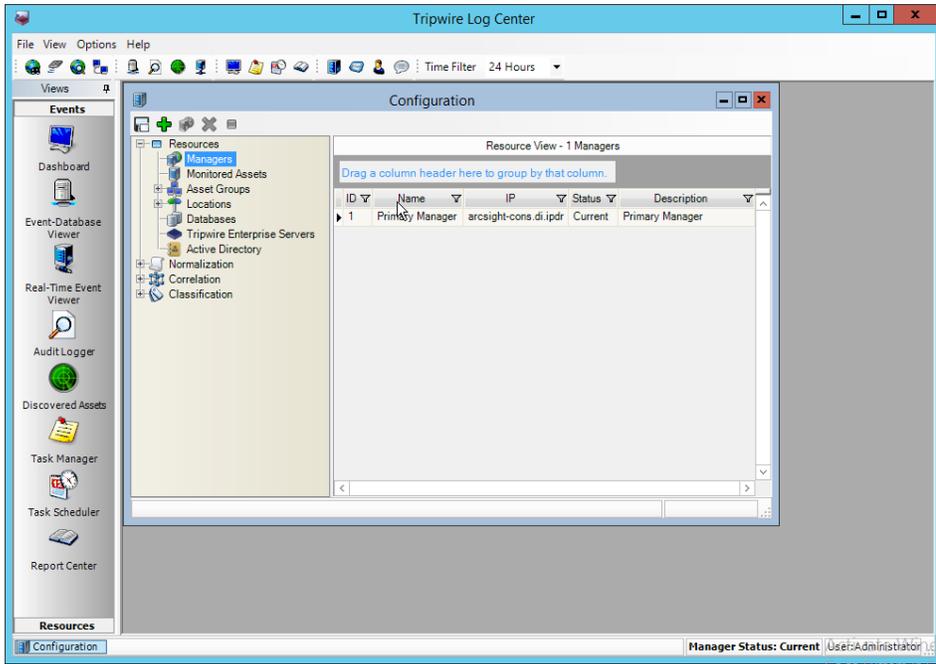
27. Click **Next**.



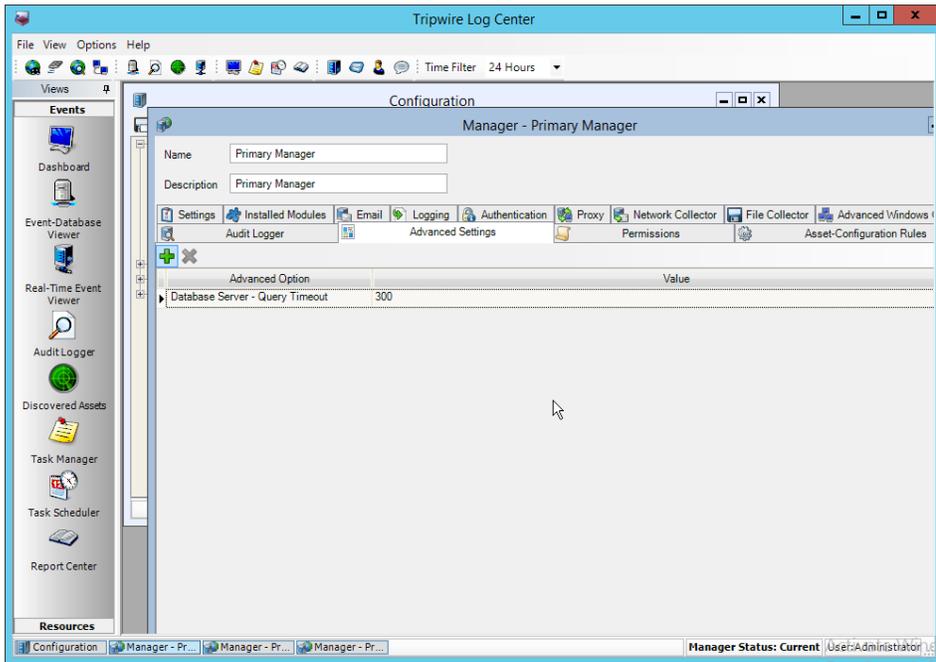
28. Click **Done**.

29. Open the **Tripwire Log Center Console**.

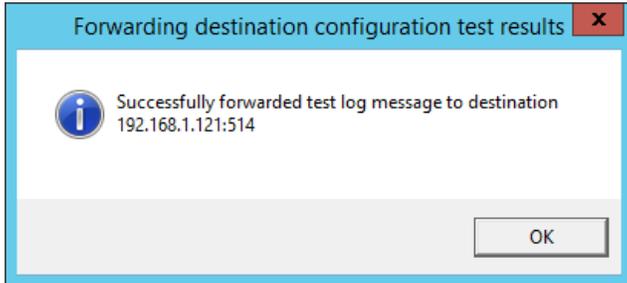
30. Go to the **Configuration Manager**.



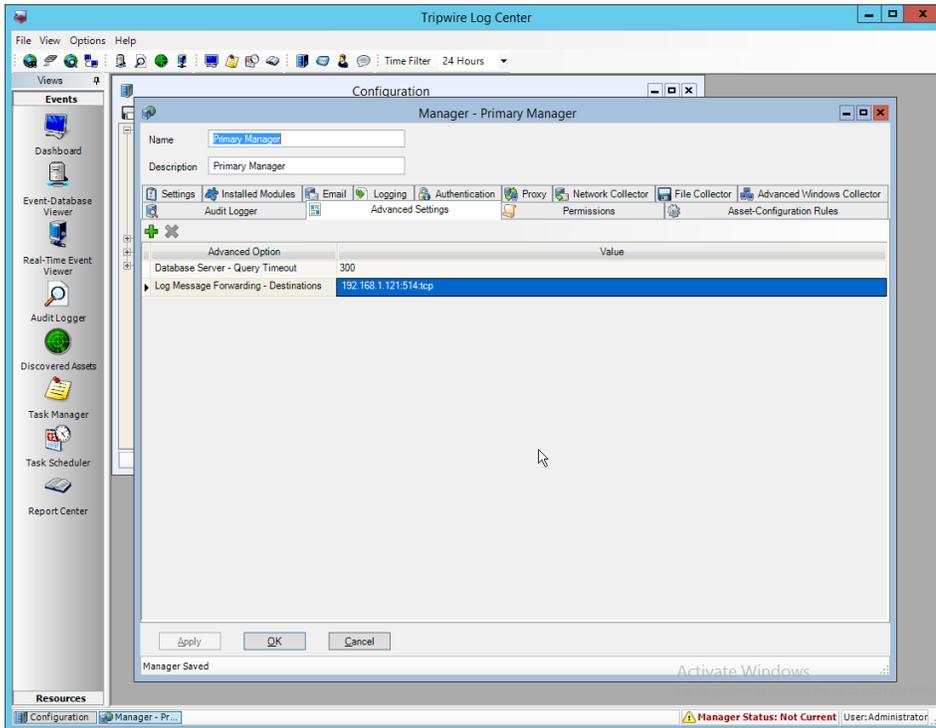
- 31. Select **Resources > Managers**.
- 32. Double-click the **Primary Manager**.
- 33. Click the **Advanced Settings** tab.



34. Click the **Add** button.
35. In the **Advanced Option** box select **Log Message Forwarding–Destinations**.
36. In the Value box next to it, type **<ip_address>:<port>:tcp** with the **IP address** and **port** of the syslog daemon just created.



37. Click **OK**.



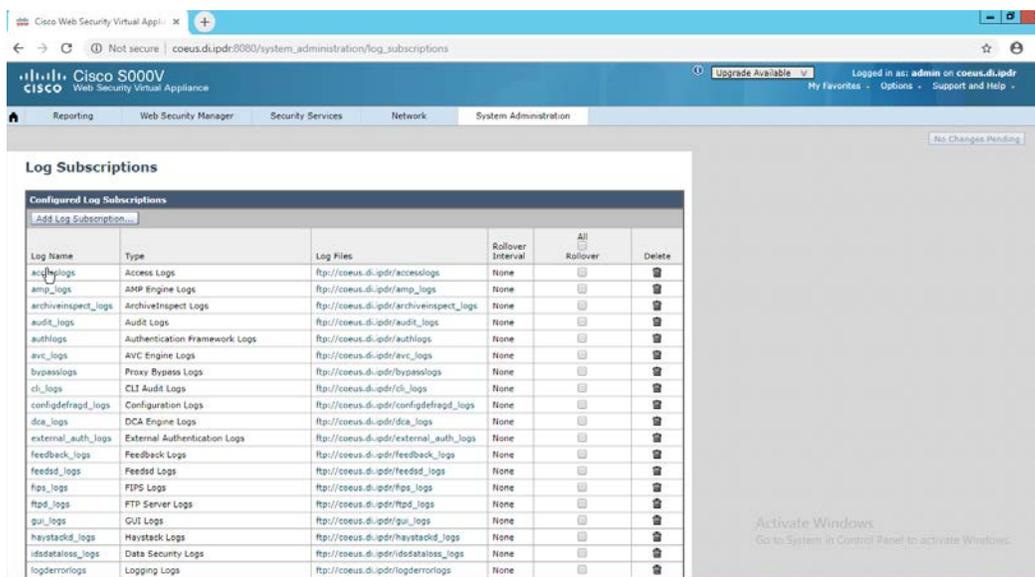
38. Click **OK**.
39. Restart the **Tripwire Log Center Manager**.

2.25 Integration: Micro Focus ArcSight and Cisco WSA

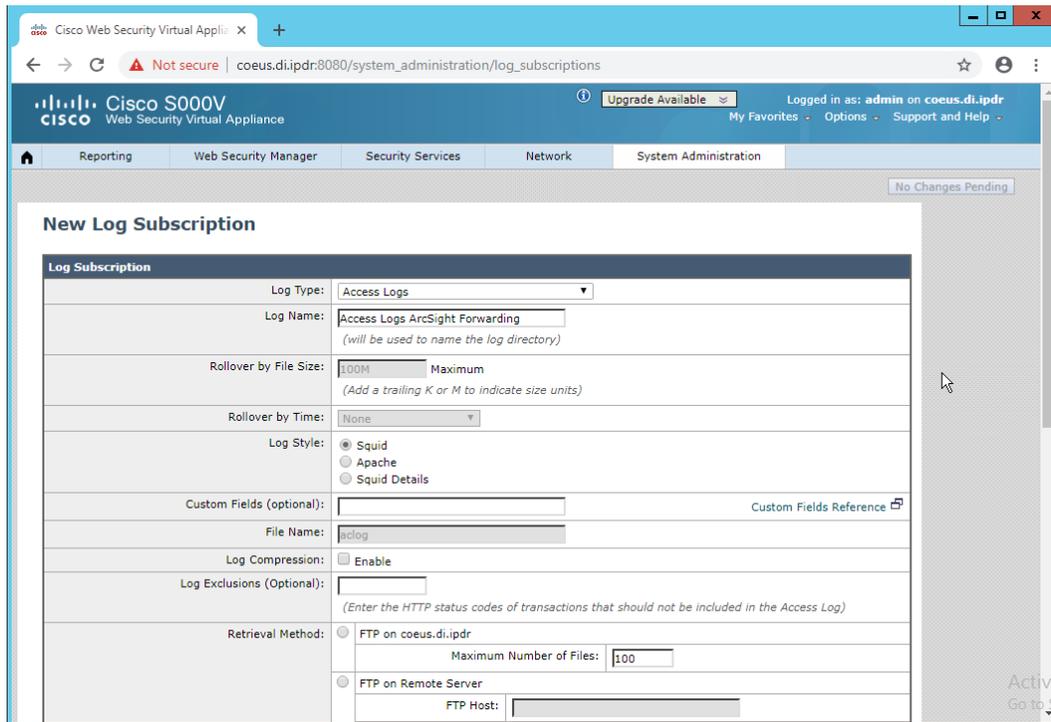
This integration briefly details how to send logs to an ArcSight syslog collector from Cisco WSA. Please see [Section 2.24](#) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one— simply forward logs to the address of that server.

2.25.1 Configure Cisco WSA to Forward Logs

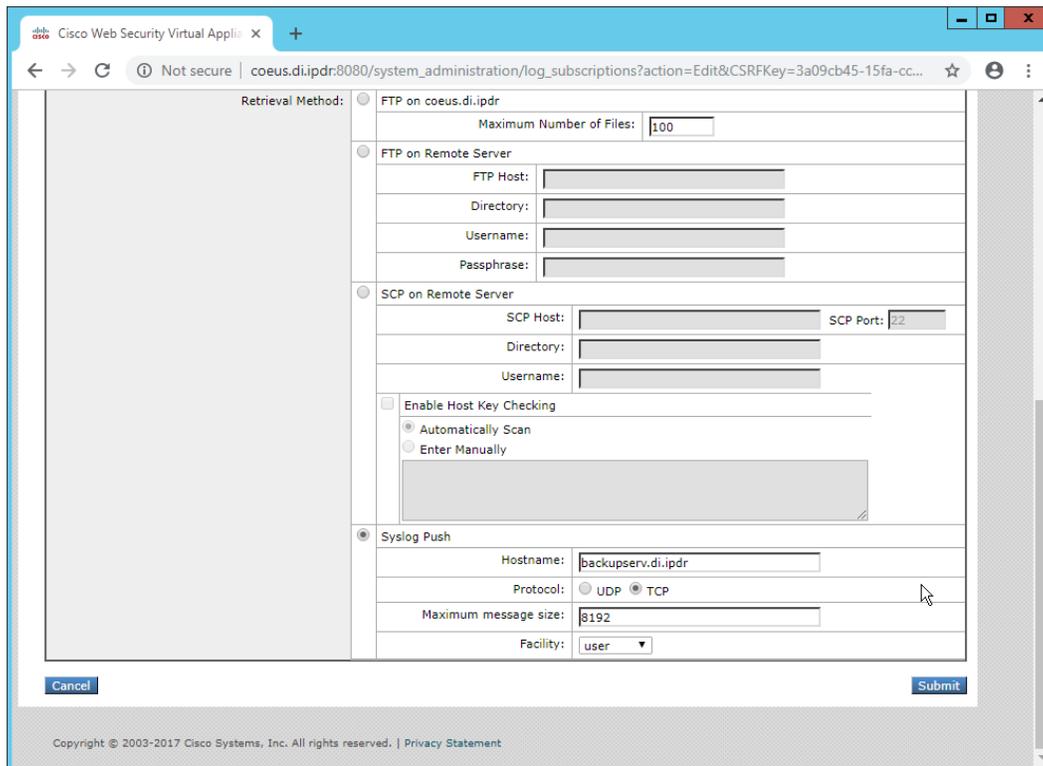
1. In the Cisco WSA web client, navigate to **System Administration > Log Subscriptions**.



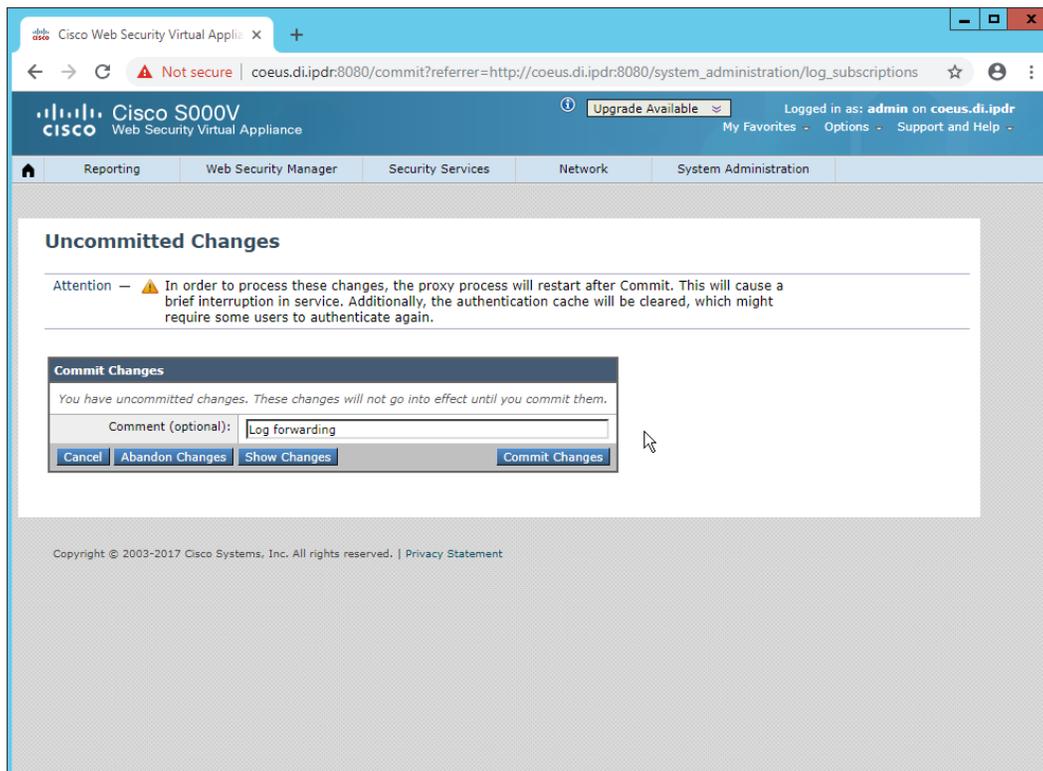
2. Click **Add Log Subscription**.
3. Select **Access Logs** for **Log Type**. (These are the logs of client web requests that have gone through the proxy.)
4. Enter a **name** for **Log Name**.



5. Select **Syslog Push**.
6. Enter the **hostname** of the ArcSight syslog collector server.
7. Select **TCP**. (Ensure that your syslog collector server is configured to use TCP.)
8. Enter **8192** or a custom message-size limit.



9. Click **Submit**.
10. Click **Commit Changes**.
11. Enter a **comment** if desired.



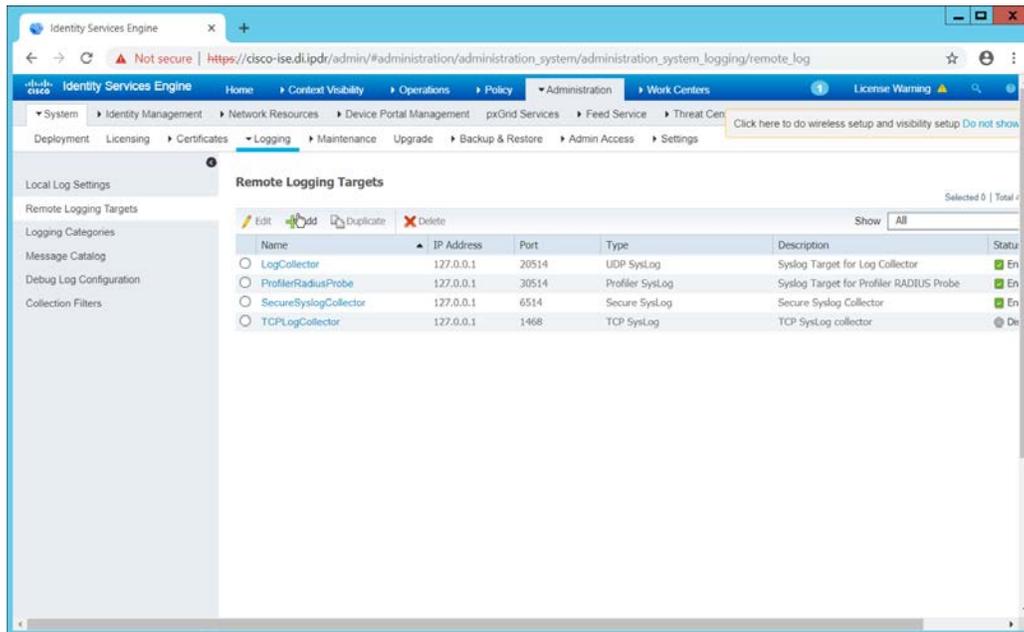
12. Click **Commit Changes**. The server will restart, so the web page connection will be temporarily lost.

2.26 Integration: Micro Focus ArcSight and Cisco ISE

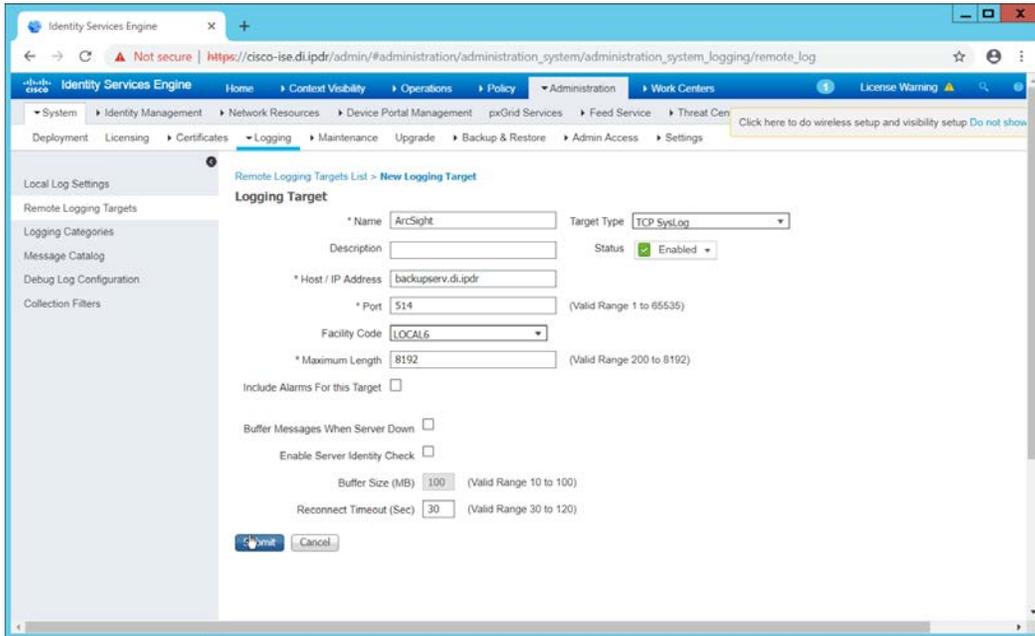
This integration briefly details how to send logs to an ArcSight syslog collector from Cisco ISE. Please see [Section 2.24](#) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one—simply forward logs to the address of that server.

2.26.1 Configure Cisco ISE to Forward Logs

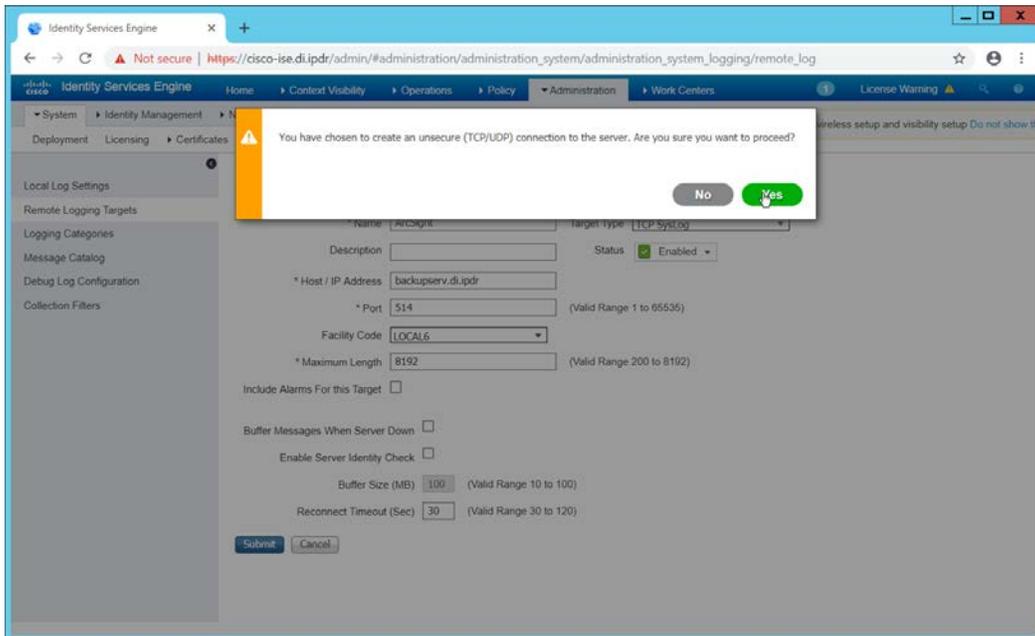
1. In the Cisco ISE web client, navigate to **Administration > System > Logging > Remote Logging Targets**.



2. Click **Add**.
3. Enter a **Name**.
4. Enter the **hostname** of the ArcSight syslog collector server for **Host/IP Address**.
5. Select **TCP SysLog** for Target Type. (Ensure that your syslog collector server is configured to use TCP.)
6. Enter **514** or the port used on the syslog server.
7. Enter **8192** or a custom message-size limit for **Maximum Length**.
8. Ensure that **Status** is set to **Enabled**.



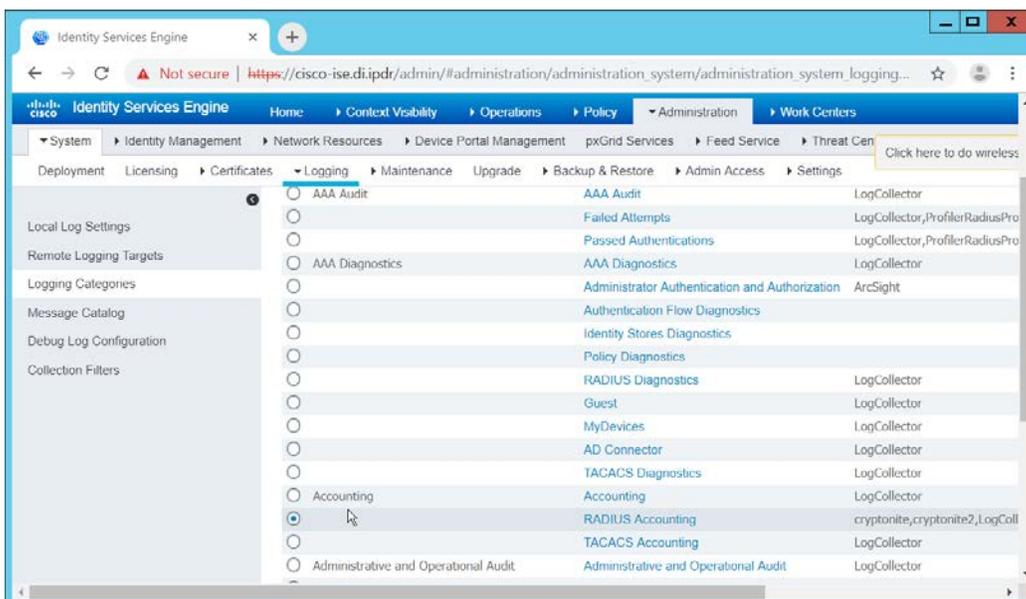
9. Click **Submit**.



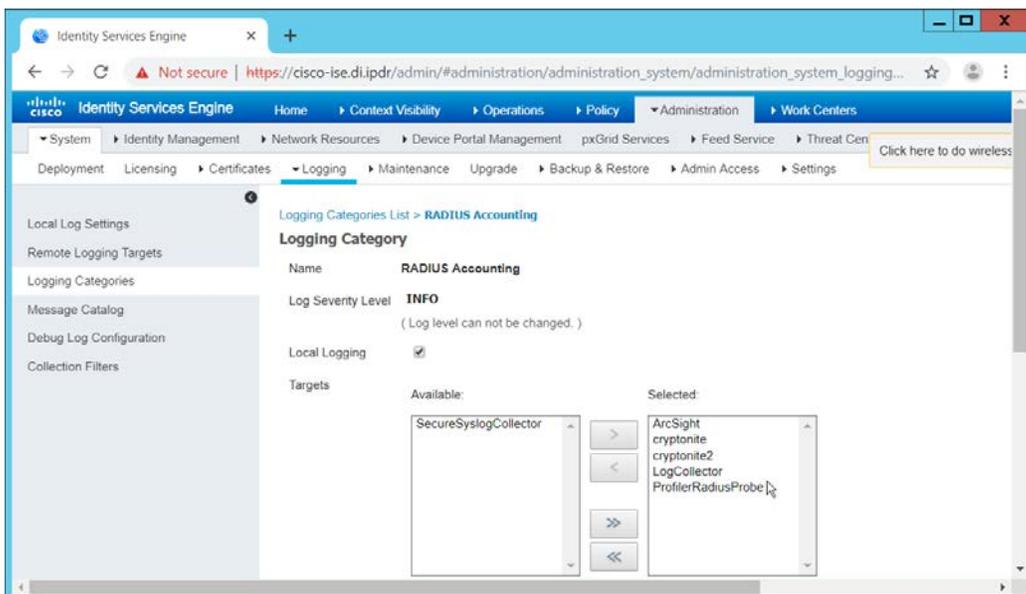
10. Click **Yes**.

2.26.2 Select Logs for Forwarding

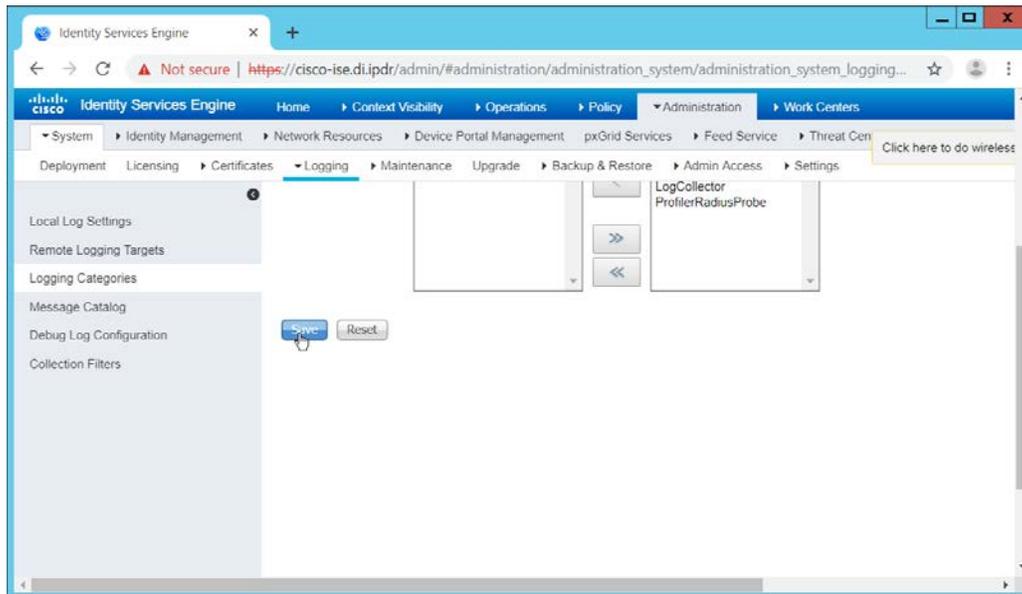
1. Navigate to **System > Logging > Logging Categories**.



2. Select a log file to forward to ArcSight.
3. Click **Edit**.



4. Move the ArcSight logging target you just created to the **Selected** box.



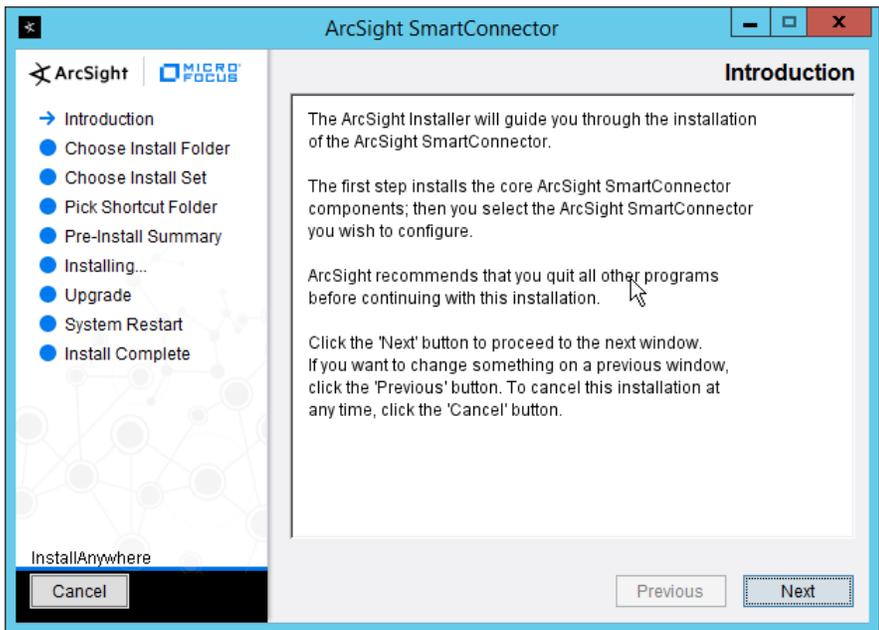
5. Click **Save**.
6. Repeat steps 1–5 for any log files you wish to forward to ArcSight.

2.27 Integration: Micro Focus ArcSight and Symantec DLP

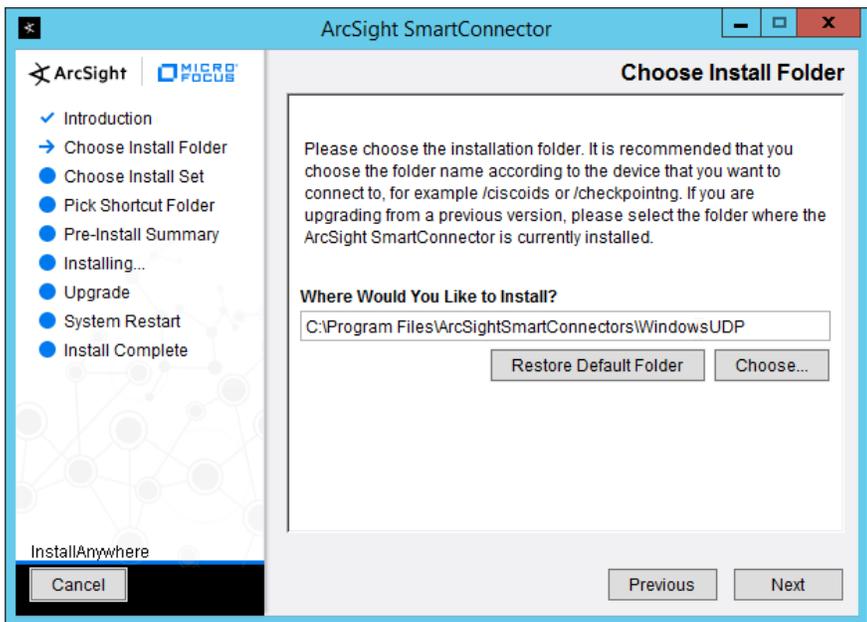
This integration briefly details how to send logs to an ArcSight syslog collector from Symantec DLP. If a server is already configured, you do not need to install a new one—simply forward logs to the address of that server. It is important to note that DLP requires a UDP server, so a TCP syslog server will not work.

2.27.1 Install Micro Focus ArcSight

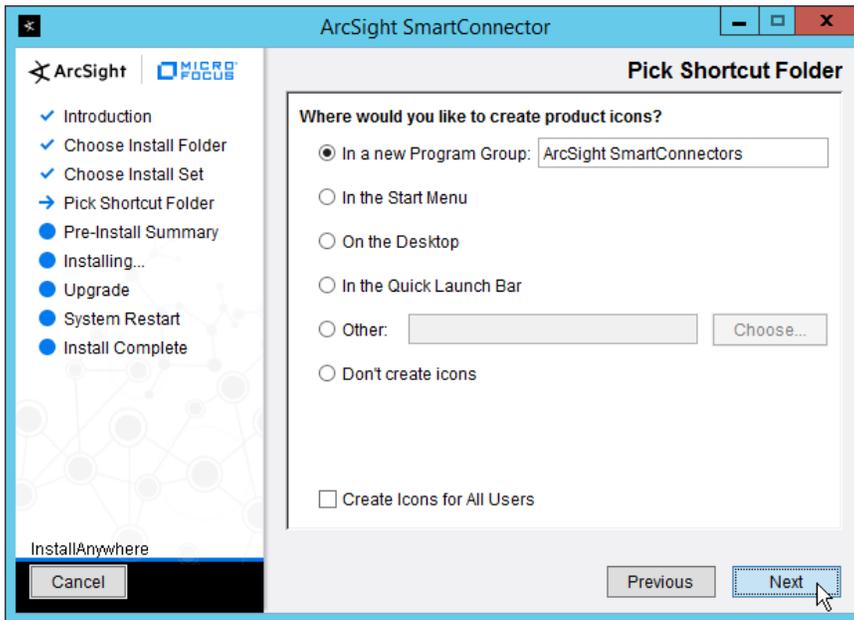
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running Cisco Stealthwatch.



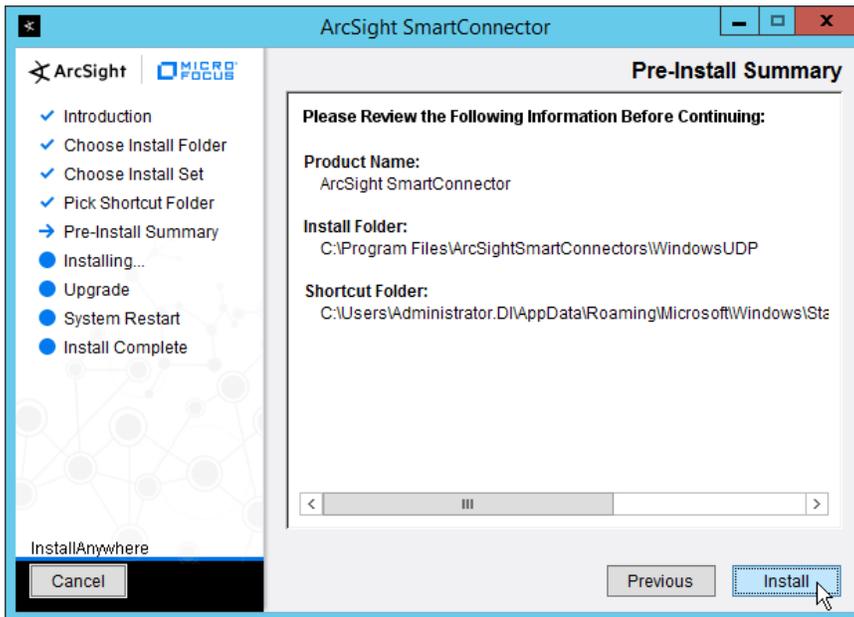
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\WindowsUDP.



4. Click **Next**.

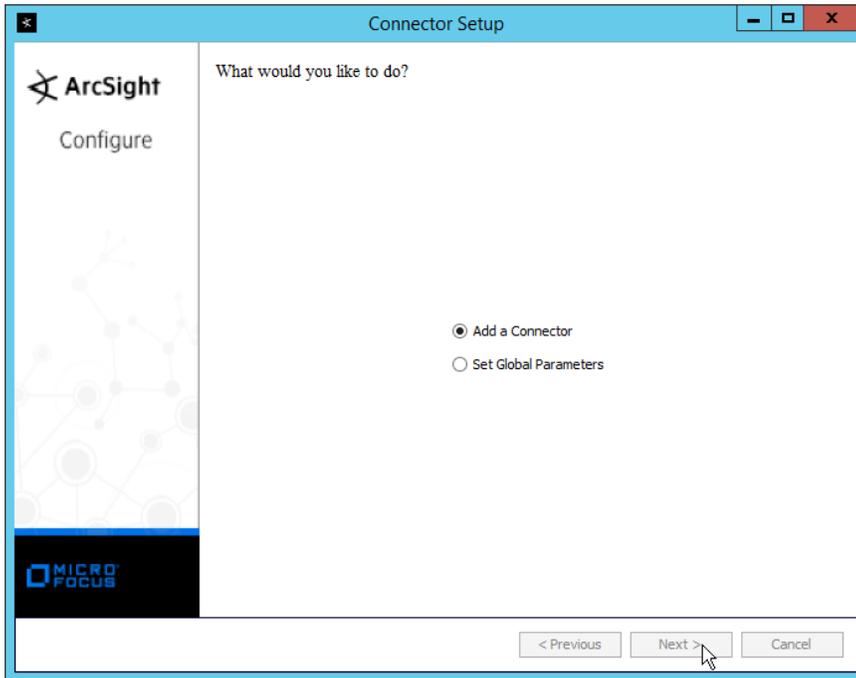


5. Click **Next**.

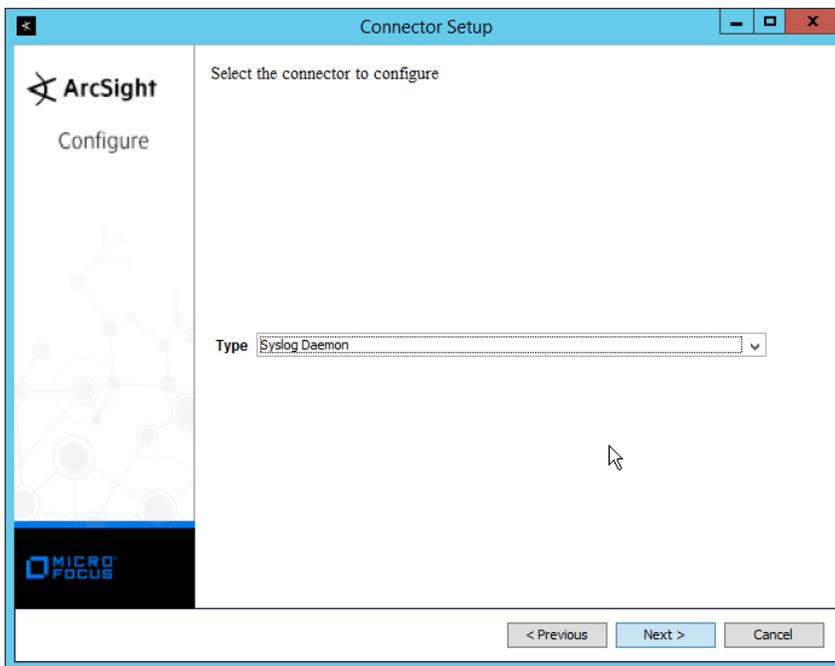


6. Click **Install**.

7. Select **Add a Connector**.



8. Click **Next**.
9. Select **Syslog Daemon**.



10. Click **Next**.

11. Enter an unused port on which the daemon can run. (Ensure that this port is allowed through the firewall.)
12. Select **UDP** for Protocol.

Connector Setup

ArcSight
Configure

Enter the parameter details

Network Port: 6514

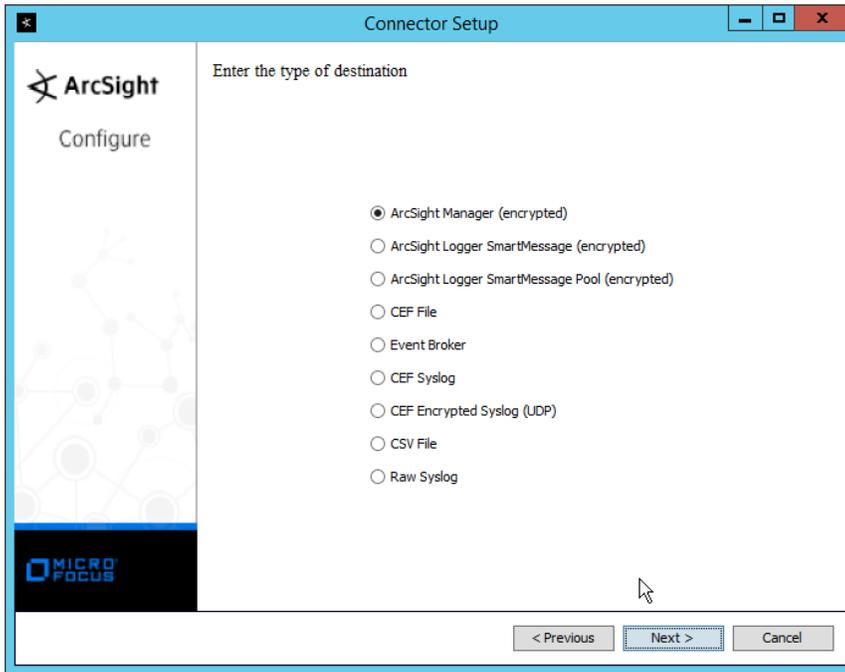
IP Address: (ALL)

Protocol: UDP

Forwarder: False

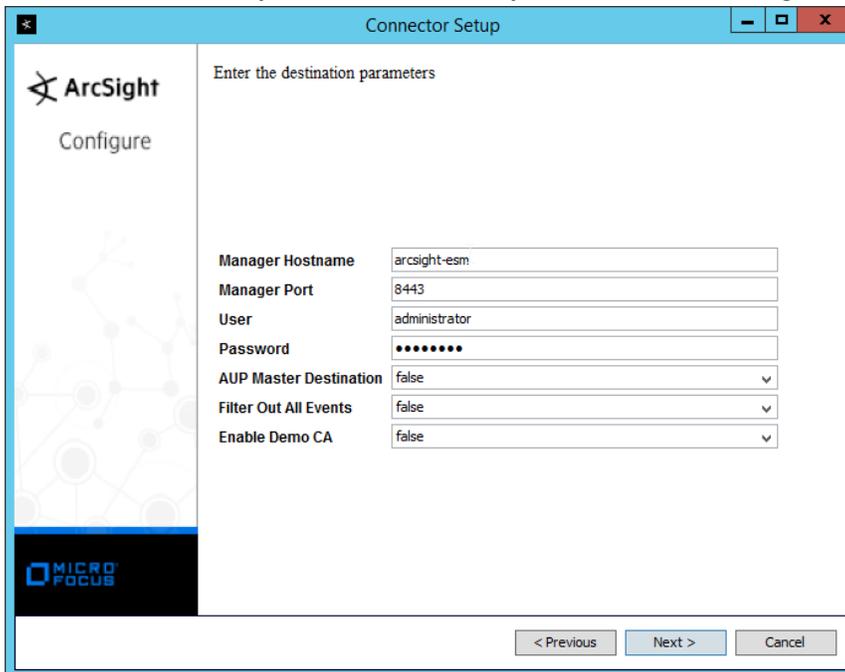
< Previous Next > Cancel

13. Click **Next**.
14. Select **ArcSight Manager (encrypted)**.



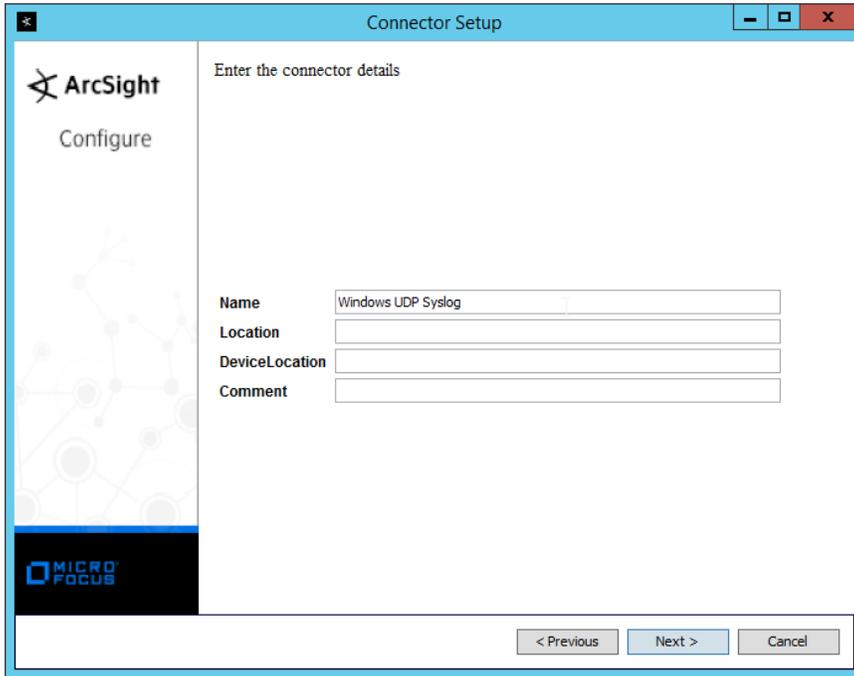
15. Click **Next**.

16. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.



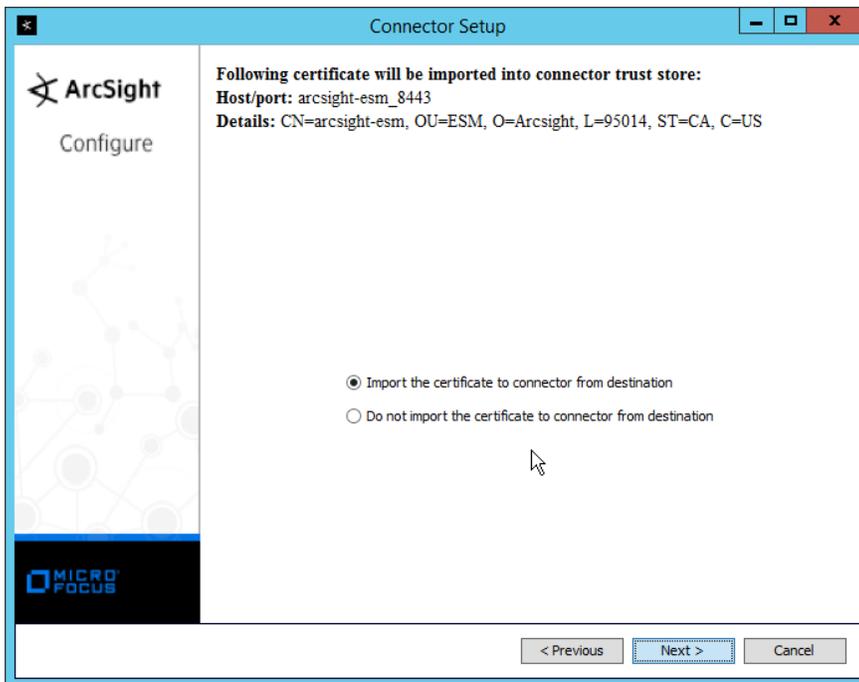
17. Click **Next**.

18. Enter identifying details about the system (only **Name** is required).

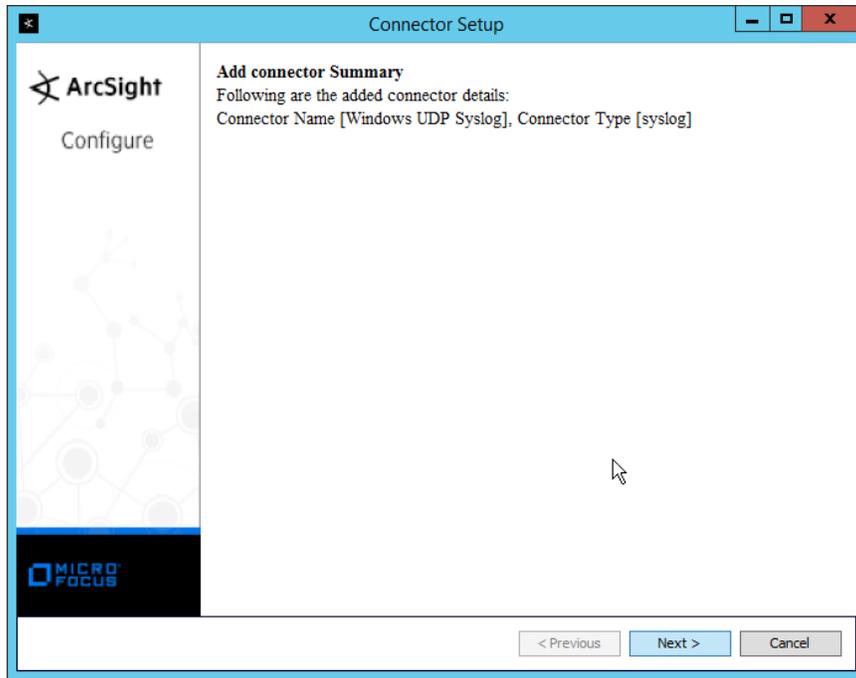


19. Click **Next**.

20. Select **Import the certificate to connector from destination**.

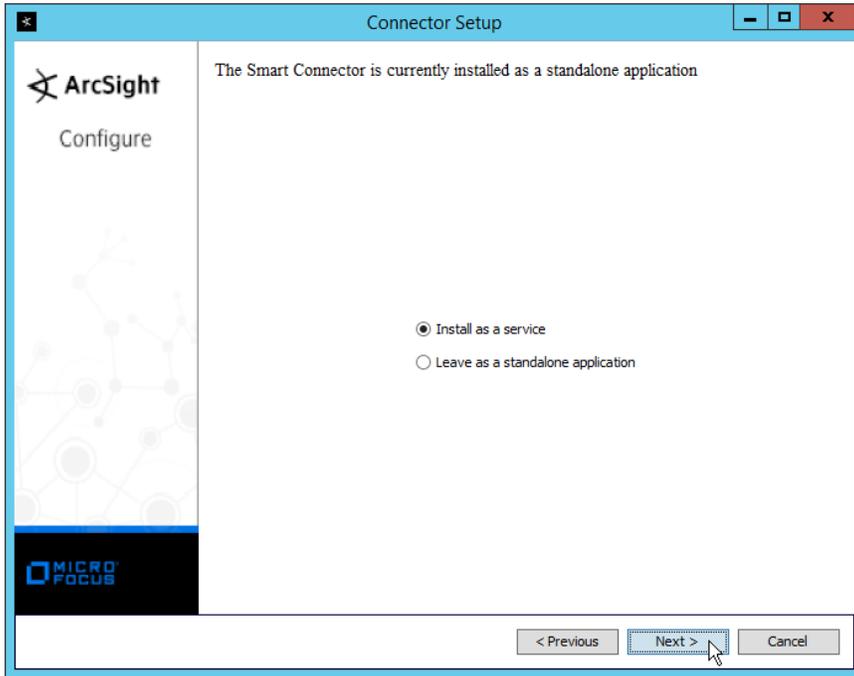


21. Click **Next**.

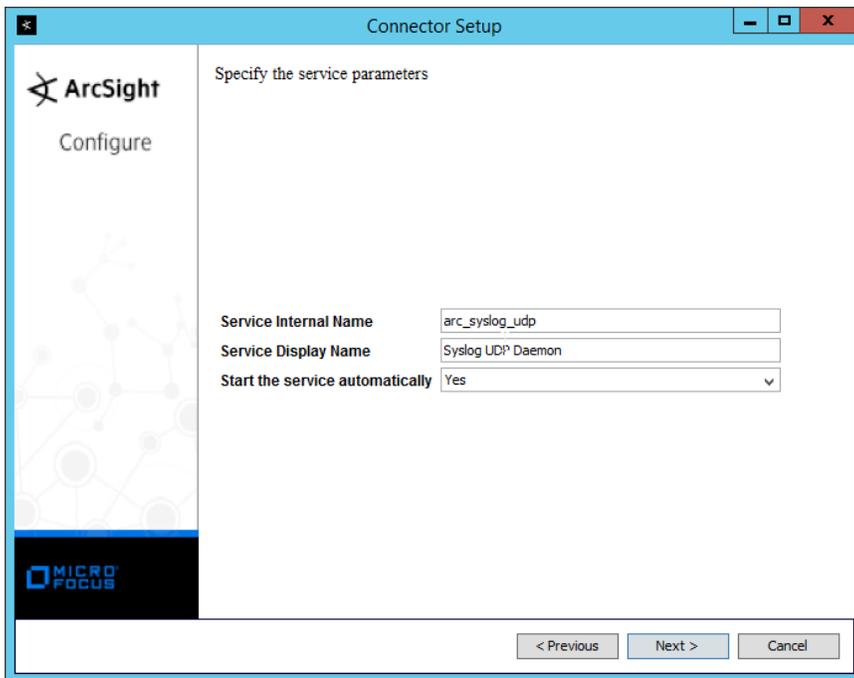


22. Click **Next**.

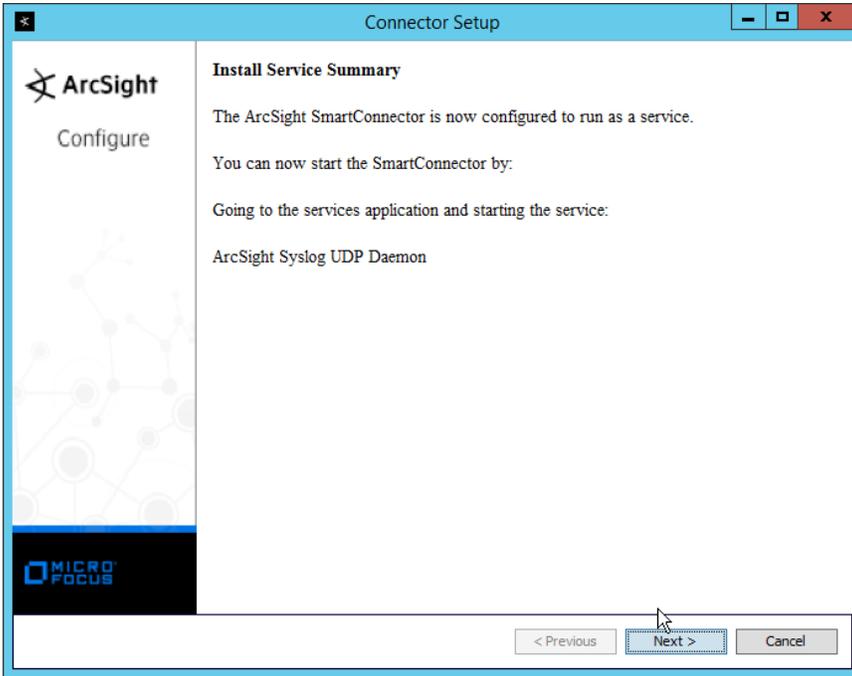
23. Select **Install as a service**.



24. Click **Next**.
25. Enter a **service name** and **display name**.

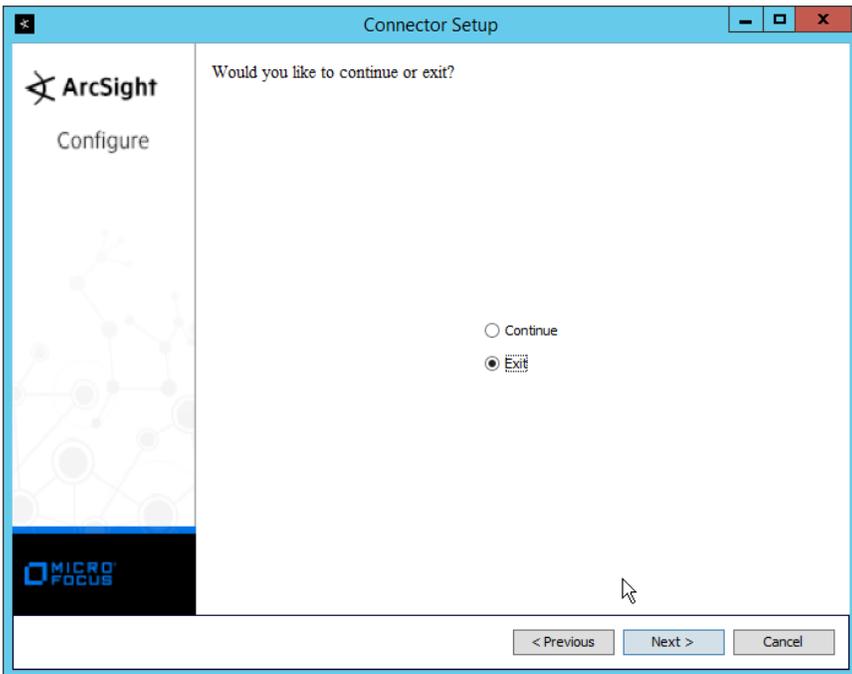


26. Click **Next**.

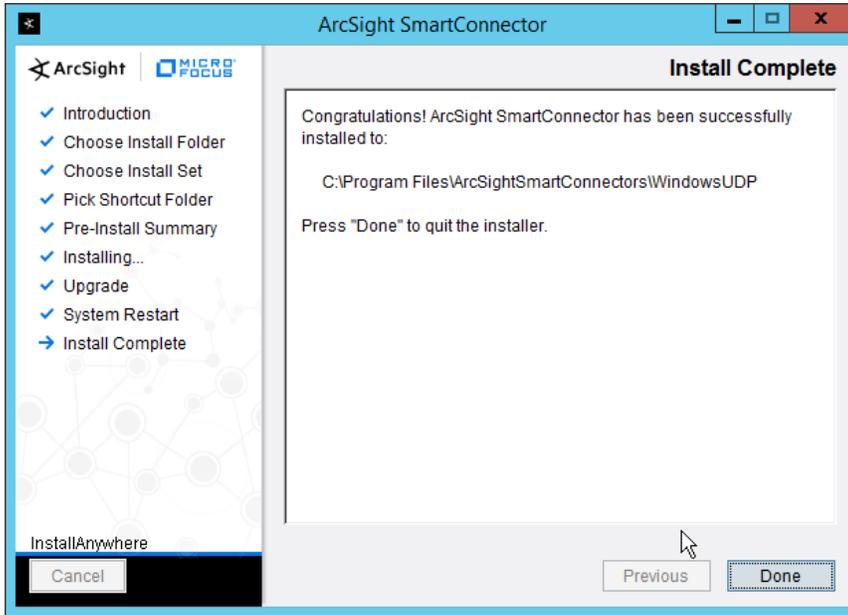


27. Click **Next**.

28. Select **Exit**.



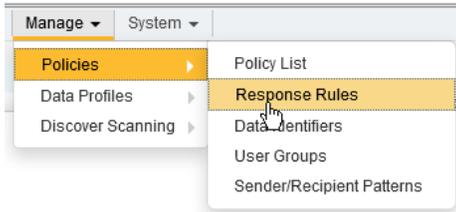
29. Click **Next**.



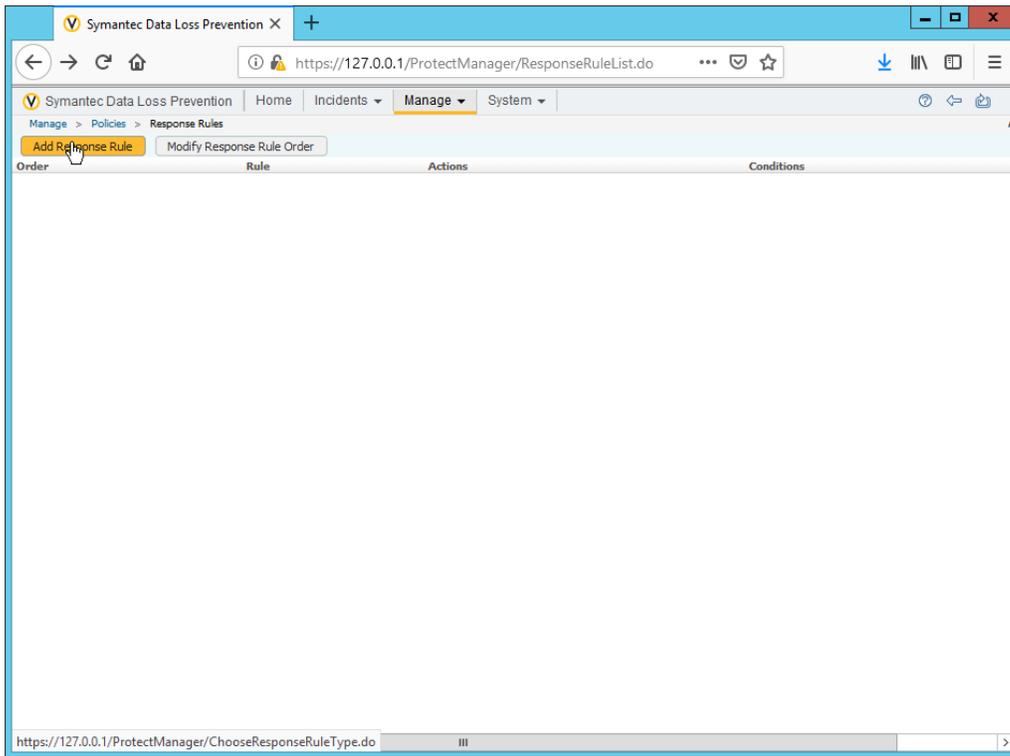
30. Click **Done**.

2.27.2 Configure Symantec DLP to Forward Logs

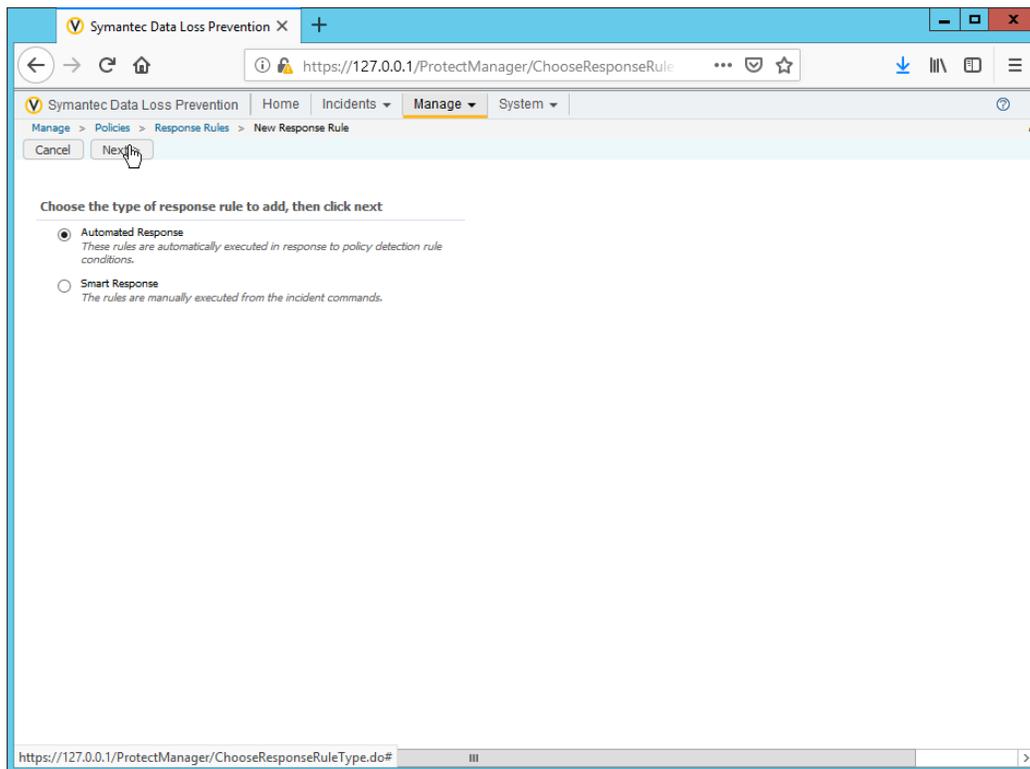
1. Log in to the Symantec DLP web console.



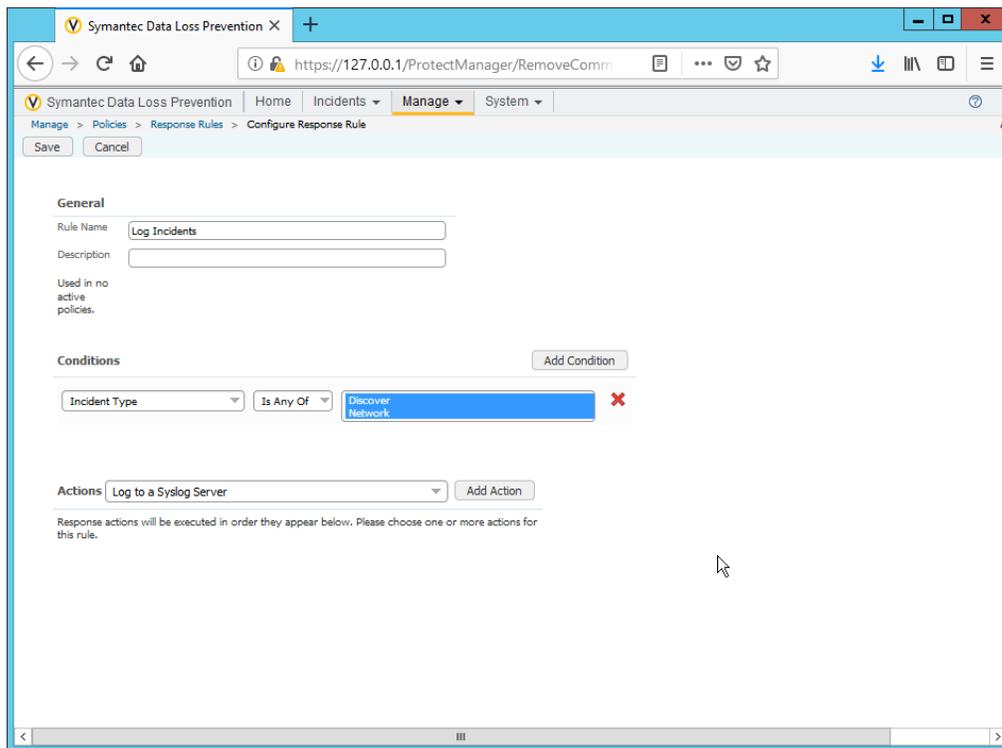
2. Navigate to **Manage > Policies > Response Rules**.



3. Click **Add Response Rule**.

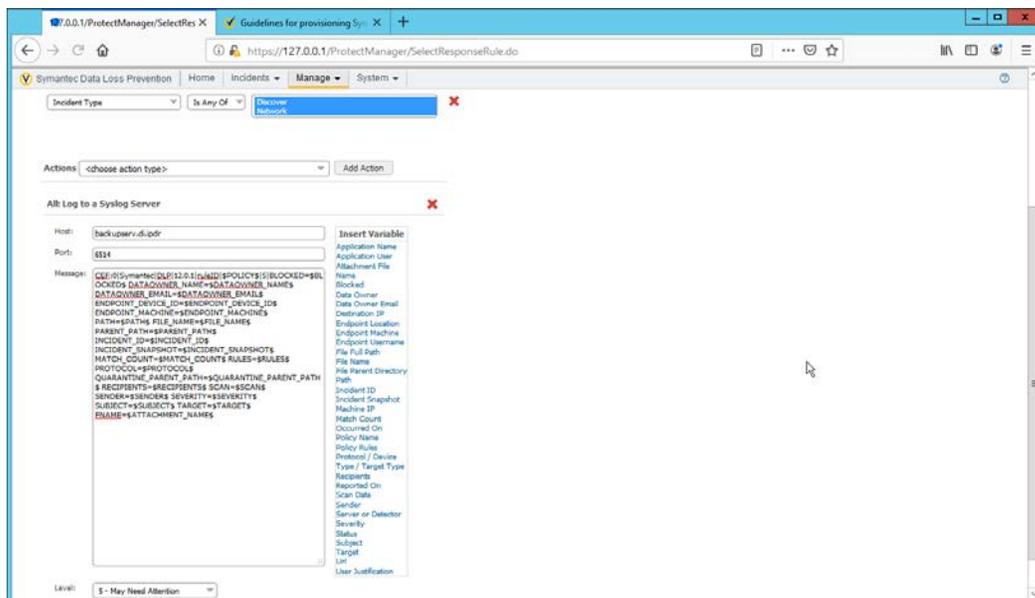


4. Click **Next**.
5. Enter a **name** for the rule.
6. Set any conditions for sending syslog messages. If you do not add conditions, all incidents will be forwarded.
7. Select **Log to a Syslog Server** for **Actions**.



8. Click **Add Action**.
9. Enter the **IP address** of the ArcSight syslog server.
10. Enter the **port** of the ArcSight syslog UDP server.
11. Select variables and format a log message to include all the information desired to be sent to the ArcSight server. Below is a sample format for the syslog message, which can potentially be parsed according to the needs of your organization.

```
CEF:0|Symantec|DLP|12.0.1|ruleID|$POLICY$|5|BLOCKED=$BLOCKED$
DATAOWNER_NAME=$DATAOWNER_NAME$ DATAOWNER_EMAIL=$DATAOWNER_EMAIL$
ENDPOINT_DEVICE_ID=$ENDPOINT_DEVICE_ID$
ENDPOINT_MACHINE=$ENDPOINT_MACHINE$ PATH=$PATH$
FILE_NAME=$FILE_NAME$ PARENT_PATH=$PARENT_PATH$
INCIDENT_ID=$INCIDENT_ID$ INCIDENT_SNAPSHOT=$INCIDENT_SNAPSHOT$
MATCH_COUNT=$MATCH_COUNT$ RULES=$RULES$ PROTOCOL=$PROTOCOL$
QUARANTINE_PARENT_PATH=$QUARANTINE_PARENT_PATH$
RECIPIENTS=$RECIPIENTS$ SCAN=$SCAN$ SENDER=$SENDER$
SEVERITY=$SEVERITY$ SUBJECT=$SUBJECT$ TARGET=$TARGET$
FNAME=$ATTACHMENT_NAME$
```



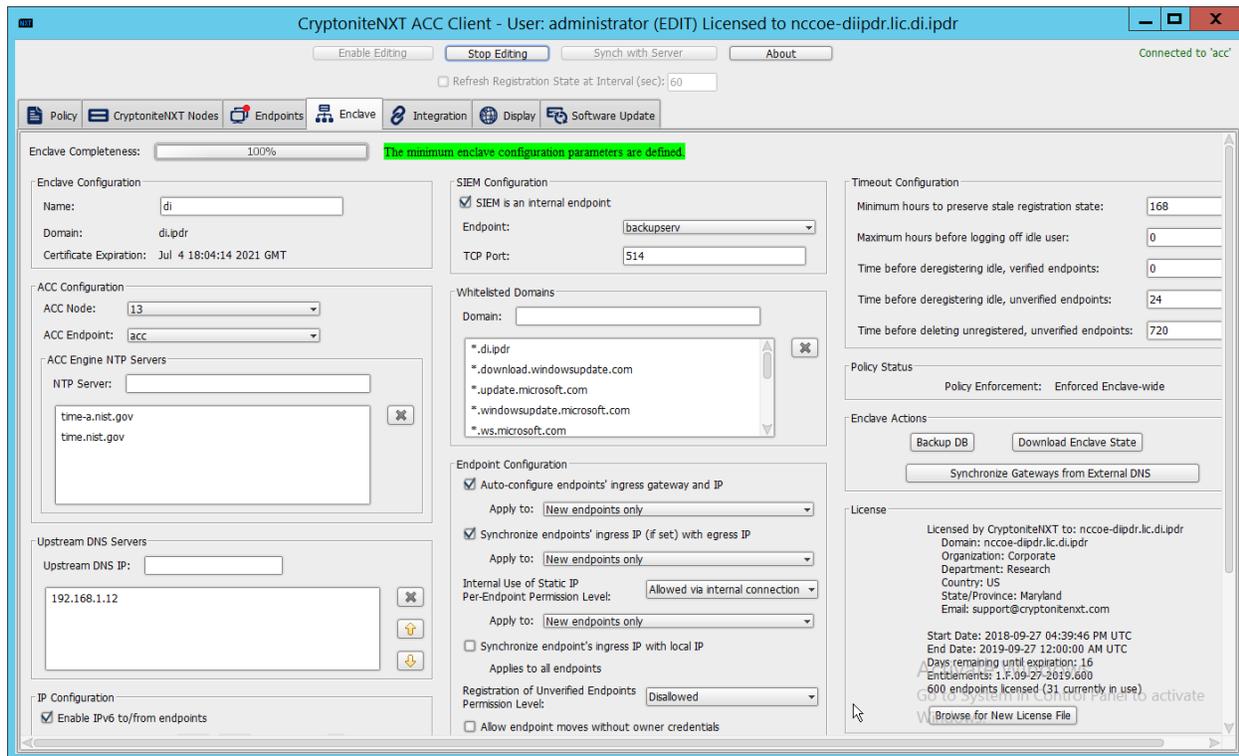
12. Click **Save**.

2.28 Integration: Micro Focus ArcSight and CryptoniteNXT

This integration briefly details how to send logs to an ArcSight syslog collector from CryptoniteNXT. Please see [Section 2.24](#) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one— simply forward logs to the address of that server. Ensure that you are using a TCP syslog collector. This section assumes that the collector is already under CryptoniteNXT’s network protection.

2.28.1 Configure CryptoniteNXT to Forward Logs to ArcSight

1. Navigate to the **Enclave** tab in the **CryptoniteNXT ACC GUI**.
2. Under **SIEM Configuration**, check the box next to **SIEM is an internal endpoint**.
3. Select the endpoint running the TCP syslog collector.
4. Enter the port used.



5. Click **Save**.

2.29 Integration: Micro Focus ArcSight and Semperis DSP

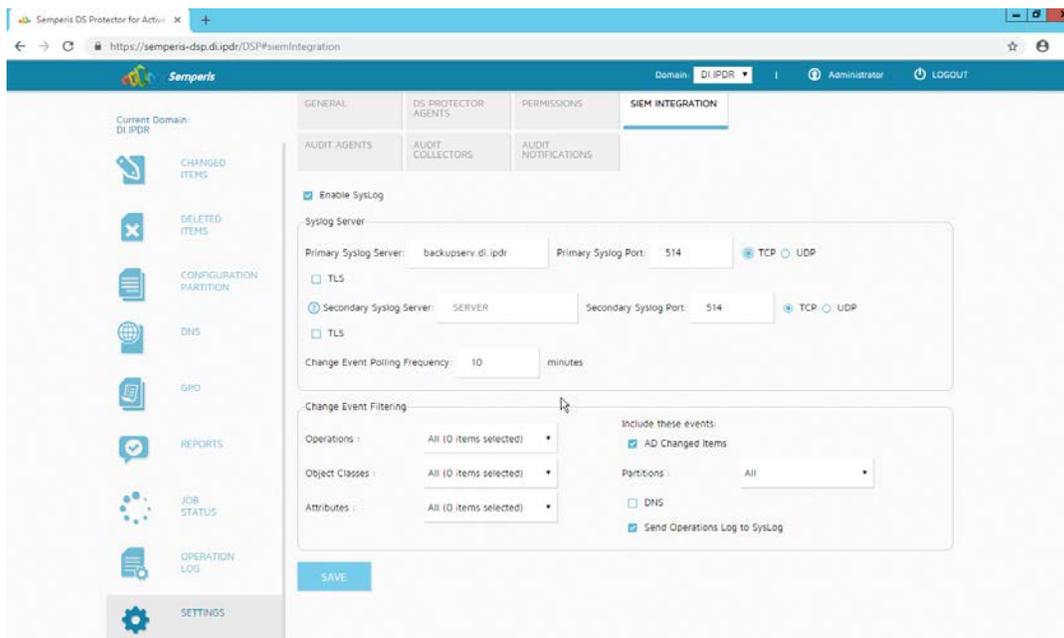
This integration briefly details how to send logs to an ArcSight syslog collector from Semperis DSP. Please see [Section 2.24](#) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one—simply forward logs to the address of that server.

Note: This integration requires Semperis DSP version 2.6.

2.29.1 Configure Semperis DSP to Forward Logs

1. In Semperis DSP, navigate to **Settings > SIEM Integration**.
2. Check the box next to **Enable SysLog**.
3. Under **Syslog Server**, enter the **hostname** for the ArcSight syslog collector, as well as the **port**.
4. Select **TCP**.
5. Enter a value for **Change Event Polling Frequency** based on the needs of your organization— this is how often it will poll for new logs to forward.

6. Under **Change Event Filtering**, select **AD Changed Items**, and **Send Operation Log to SysLog**. Ensure that **All** is selected for **Partitions**.
7. You can also select any specific **operations**, **classes**, and **attributes** to be forwarded or simply leave as **All**.



8. Click **Save**.



9. Click **Close**.

2.30 Integrations: CryptoniteNXT

For the architecture, it is necessary to create the following source groups. If your organization's desired architecture is different from the one described in this document, it is necessary to adapt the following instructions to avoid loss of network or security function. This section will describe the creation of source groups and destination groups used in this enterprise.

Create the following destination groups and source groups and apply them to the correct endpoints to allow these products and integrations to communicate under CryptoniteNXT.

2.30.1 Active Directory and DNS

This guide assumes the use of Active Directory and DNS on the same Windows 2012 server. The following ports may vary for other products.

Destination Group Name	Source Group Name	Protocol	Port Range
ad-dns	ad-dns-clients	TCP	389
ad-dns	ad-dns-clients	UDP	389
ad-dns	ad-dns-clients	UDP	53
ad-dns	ad-dns-clients	TCP	88
ad-dns	ad-dns-clients	UDP	88
ad-dns	ad-dns-clients	TCP	25
ad-dns	ad-dns-clients	TCP	42
ad-dns	ad-dns-clients	TCP	137
ad-dns	ad-dns-clients	TCP	139
ad-dns	ad-dns-clients	TCP	53
ad-dns	ad-dns-clients	TCP	636
ad-dns	ad-dns-clients	TCP	3268:3269
ad-dns	ad-dns-clients	TCP	445
ad-dns	ad-dns-clients	UDP	445
ad-dns	ad-dns-clients	TCP	9389
ad-dns	ad-dns-clients	TCP	5722
ad-dns	ad-dns-clients	TCP	464
ad-dns	ad-dns-clients	UDP	464
ad-dns	ad-dns-clients	UDP	123
ad-dns	ad-dns-clients	UDP	137:138
ad-dns	ad-dns-clients	UDP	67
ad-dns	ad-dns-clients	UDP	2535

Destination Group Name	Source Group Name	Protocol	Port Range
ad-dns	ad-dns-clients	UDP	49152:65535
ad-dns	ad-dns-clients	TCP	49152:65535

Endpoint	Source Groups	Destination Groups
(all endpoints that need access to AD/DNS)	ad-dns-clients	
AD/DNS server		ad-dns

2.30.2 Microsoft Exchange

This guide assumes the use of Microsoft Exchange. The following ports may vary for other products.

Destination Group Name	Source Group Name	Protocol	Port Range
exchange	exchange-clients	TCP	443
exchange	exchange-clients	TCP	80
exchange	exchange-clients	TCP	25
exchange	exchange-clients	TCP	379
exchange	exchange-clients	TCP	3268:3269
exchange	exchange-clients	TCP	636
exchange	exchange-clients	TCP	143
exchange	exchange-clients	TCP	993
exchange	exchange-clients	TCP	110
exchange	exchange-clients	TCP	995
exchange	exchange-clients	TCP	119
exchange	exchange-clients	TCP	563
exchange	exchange-clients	TCP	465
exchange	exchange-clients	TCP	443691
exchange	exchange-clients	TCP	102
exchange	exchange-clients	TCP	135

Destination Group Name	Source Group Name	Protocol	Port Range
exchange	exchange-clients	TCP	389:390
exchange	exchange-clients	TCP	53
exchange	exchange-clients	UDP	53
exchange	exchange-clients	TCP	2525
exchange	exchange-clients	TCP	475

Endpoint	Source Groups	Destination Groups
MS Exchange	exchange-clients	exchange
(all email clients)	exchange-clients	
AD/DNS server	exchange-clients	

2.30.3 FileZilla

The default port for FileZilla is 21.

1. To determine the ports being used for your instance, open the FileZilla console.
2. Navigate to **Edit > Settings > General Settings > Listen on these ports**, and allow any ports listed here.
3. If your server listens in passive mode, navigate to **Edit > Settings > Passive mode settings > Use custom port range**, and allow any ports listed here.

Destination Group Name	Source Group Name	Protocol	Port Range
FileZilla	BackupClients	TCP	21 (default—see instructions)
FileZilla	BackupClients	TCP	51120-511230 (passive mode—see instructions)

Endpoint	Source Groups	Destination Groups
(any endpoints that need to perform backups)	BackupClients	
FileZilla server		FileZilla

2.30.4 GreenTec

If GreenTec is configured to use a FileZilla server, refer to the above section. If GreenTec is configured to use Windows Network Share, see below for ports required.

Destination Group Name	Source Group Name	Protocol	Port Range
NetworkShare	GreenTecClients	TCP	80
NetworkShare	GreenTecClients	TCP	135-139
NetworkShare	GreenTecClients	TCP	445

Endpoint	Source Groups	Destination Groups
(any endpoints that need access to GreenTec disks)	GreenTecClients	
GreenTec server		NetworkShare

2.30.5 Tripwire Enterprise

In Tripwire, the Axon Bridge is used for Tripwire Enterprise to contact endpoints. Therefore, the port 5670 must be allowed on endpoints to allow TE to initiate communications. Furthermore, TE requires MSSQL to function, so it must be granted access to that as well.

Destination Group Name	Source Group Name	Protocol	Port Range
TripwireEnterprise	TEClients	TCP	443
TripwireEnterprise	TEClients	TCP	8080
TripwireEnterprise	TEClients	TCP	9898
TripwireEnterprise	TEClients	TCP	1169
TEAxon	TripwireE	TCP	5670
MSSQL	MSSQLClients	TCP	1433

Endpoint	Source Groups	Destination Groups
(any endpoints that need to be monitored by Tripwire Enterprise)	TEClients	TEAxon
Tripwire Enterprise server	TripwireE, MSSQLClients	TripwireEnterprise
MSSQL server		MSSQL

2.30.6 ArcSight ESM

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSight	ArcSightConnectors	TCP	8443

Endpoint	Source Groups	Destination Groups
(any endpoints with an ArcSight Connector installed)	ArcSightConnectors	
ArcSight ESM server		ArcSight

2.30.7 Cisco ISE

Please see the *CryptoniteNXT Generic RADIUS Integration Guide* for instructions on how ISE should be integrated with CryptoniteNXT.

To access the web console for ISE, allow port 443 for any machines that should be able to access the ISE administrative console.

To access the portal for ISE, allow port 8443 (default) for any machines that will need to access the portal. You can find this value by looking at your portal configuration in ISE.

Furthermore, if RADIUS is configured for the posture integration, you will need to add any ports used in RADIUS for both ISE and the internal switch. The default for these is 1812 (Authentication), 1813 (Accounting), and 1700 (CoA). RADIUS can be TCP or UDP, so you can restrict this to your organization's configuration.

Destination Group Name	Source Group Name	Protocol	Port Range
ISE	ISEConsole	TCP	443
ISE	ISEClients	TCP	8443
radius	ISESwitch, ISEServer	TCP	1812
radius	ISESwitch, ISEServer	UDP	1812
radius	ISESwitch, ISEServer	TCP	1813
radius	ISESwitch, ISEServer	UDP	1813
radius	ISESwitch, ISEServer	TCP	1700
radius	ISESwitch, ISEServer	UDP	1700

Endpoint	Source Groups	Destination Groups
(any endpoints that need to do posture under ISE)	ISEClients	
(any endpoints that need to access the ISE web console)	ISEConsole	
ISE server	ISEServer	ISE, radius
(internal switches or RADIUS servers used for ISE Posture)	ISESwitch, ISEClients	radius
Cryptonite ACC Node		radius

2.30.8 Semperis DSP

Semperis DSP recommends allowing full network access during the initial database sync. After that, the following ports should be left open for communication.

Destination Group Name	Source Group Name	Protocol	Port Range
dsp	dsp-admin	TCP	443
dsp	dsp-agents	TCP	8903
dsp	dsp-agents	TCP	135
dsp	dsp-agents	TCP	445

Destination Group Name	Source Group Name	Protocol	Port Range
dsp	dsp-agents	TCP	1024:1034
ad-dsp	dsp-client	TCP	8772
ad-dsp	dsp-client	TCP	8750
ad-dsp	dsp-client	ICMP	0:255

Endpoint	Source Groups	Destination Groups
(any endpoints that need admin access to DSP)	dsp-admin	
Semperis DSP	ad-dns-clients, dsp-client, exchange-clients	dsp
Active Directory server	dsp-agents	ad-dsp

2.30.9 Symantec DLP

This largely depends on how distributed the setup of DLP is. See here for a list of ports required by Symantec DLP: <https://support.symantec.com/us/en/article.tech220846.html>.

For this build, we used a single server that contained the database, so only the agents and administrative clients needed to be allowed to communicate through Cryptonite.

Destination Group Name	Source Group Name	Protocol	Port Range
dlp	dlp-admin	TCP	443
dlp	dlp-clients	TCP	10443

2.30.10 Cisco WSA

WSA uses a proprietary command line, which means it does not have a way of authenticating to the CryptoniteNXT portal. For devices such as this, there are two options.

1. The device can be left outside CryptoniteNXT.
2. The device can be placed under CryptoniteNXT on a CryptoniteNXT Endpoint Node with the portal disabled.

To prevent MAC spoofing, by default Cryptonite pins MAC addresses to the port + VLAN (Virtual LAN) to which a device is connected, so a malicious device connecting to the end-point node with the same MAC as an already connected IP360 would still be required to authenticate. Physical security for the end-point node can further mitigate concerns about MAC spoofing.

If you can find a way to authenticate WSA to CryptoniteNXT or decide to use the disabled portal option with strong physical security, we provide the ports below for integration.

To access the web console for WSA, allow port 8080 for any machines that should be able to access the ISE administrative console.

To access the proxy, allow port 80 and port 3128 for any machines that will need to go through the proxy, which will likely be most clients in the enterprise. Port 80 is for the *wpad.dat* file, and port 3128 is for the proxy itself.

Destination Group Name	Source Group Name	Protocol	Port Range
wsa	wsa-clients	TCP	80
wsa	wsa-clients	TCP	3128
wsa	wsa-admin	TCP	8080

Endpoint	Source Groups	Destination Groups
(any endpoints that need to use the proxy to connect to the internet)	wsa-clients	
(any endpoints that need to access the WSA web console)	wsa-admin	
Cisco WSA		wsa

2.30.11 Tripwire IP360

IP360 uses a proprietary command line, which means it does not have a way of authenticating to the CryptoniteNXT portal. For devices such as this, there are two options.

1. The device can be left outside CryptoniteNXT.
2. The device can be placed under CryptoniteNXT on a CryptoniteNXT Endpoint Node with the portal disabled.

To prevent MAC spoofing, by default Cryptonite pins MAC addresses to the port+VLAN to which a device is connected, so a malicious device connecting to the end-point node with the same MAC as an already connected IP360 would still be required to authenticate. Physical security for the end-point node can further mitigate concerns about MAC spoofing.

If you can find a way to authenticate IP360 to CryptoniteNXT or decide to use the disabled portal option with strong physical security, we provide the ports below for integration.

To access the web console for IP360, allow port 443 for any machines that should be able to access the IP360 administrative console.

IP360 should have access to all ports of the client machines it needs to scan. Another option is to simply add IP360 to all the source groups present in your enterprise, and it will give an overview of the vulnerabilities of clients on ports that CryptoniteNXT is not actively protecting. Alternatively, you can disable policy enforcement temporarily on the CryptoniteNXT Endpoint Node to which IP360 is connected, but you should do this only during scans.

Destination Group Name	Source Group Name	Protocol	Port Range
ip360	ip360admin	TCP	443
scantarget	ip360scanner	TCP	1:65535
scantarget	ip360scanner	UDP	1:65535
scantarget	ip360scsanner	ICMP	0:255

Endpoint	Source Groups	Destination Groups
(any endpoints need to access the IP360 web console)	ip360admin	
(any endpoints to be fully scanned by IP360)		scantarget
IP360	ip360scanner	ip360

2.30.11.1 Tripwire Log Center, Tripwire IP360, Tripwire Enterprise, and ArcSight ESM

The guide details an integration among Tripwire IP360, Tripwire Enterprise, Tripwire Log Center, and ArcSight ESM. This section describes the ports needed to allow the integrations through Cryptonite.

First, traffic must be allowed from Tripwire Log Center to the MSSQL server. To do this, ensure that Tripwire Log Center can access 1433 on the MSSQL server. (Note: Tripwire Enterprise also has access to this port, as described above in the Tripwire Enterprise section.)

Then traffic from Tripwire Enterprise to Tripwire Log Center should be allowed on ports 8091 and 1468.

Traffic from IP360 to Tripwire Log Center should be allowed on port 22 for the SFTP (Secure FTP) transfer. Also, traffic from Tripwire Log Center to 5670 on Tripwire IP360 should be allowed. If you chose to leave IP360 out of the Cryptonite NXT enclave, Tripwire Log Center will need to be able to reach it externally.

Traffic from Tripwire Log Center to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514). As a last note, the server running the ArcSight syslog connector requires an IP and not a hostname for its integration with Tripwire Log Center—you must set a static IP for the connector server in Cryptonite and enter this IP in the appropriate place in Tripwire Log Center’s configuration.

Destination Group Name	Source Group Name	Protocol	Port Range
MSSQL	MSSQLClients	TCP	1443
TLC	TLCClients	TCP	8091
TLC	TLCClients	TCP	1468
TLC	TLCClients	TCP	22
ArcSightTCPSysConn	TCPSysClients	TCP	514
ip360	ip360admin	TCP	5670

Endpoint	Source Groups	Destination Groups
Tripwire Log Center	TCPSysClients, MSSQLClients, ip360admin	TLC
Tripwire Enterprise	TLCClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn
MSSQL		MSSQL
IP360	TLCClients	ip360

2.30.12 FileZilla and ArcSight

The guide details an integration between FileZilla and ArcSight ESM to forward logs from FileZilla to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Because this integration involves the use of an ArcSight Connector directly on the FileZilla server, only one port is needed. The FileZilla server should be able to directly communicate with 8443 on the ArcSight ESM server.

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSight	ArcSightConnectors	TCP	8443

Endpoint	Source Groups	Destination Groups
FileZilla	ArcSightConnectors	
ArcSight ESM		ArcSight

2.30.13 Cisco ISE and ArcSight

The guide details an integration between Cisco ISE and ArcSight ESM to forward logs from ISE to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Cisco ISE to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

Endpoint	Source Groups	Destination Groups
Cisco ISE	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

2.30.14 Cisco WSA and ArcSight

The guide details an integration between Cisco WSA and ArcSight ESM to forward logs from WSA to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Cisco WSA to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

Endpoint	Source Groups	Destination Groups
Cisco WSA	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

2.30.15 Semperis DSP and ArcSight

The guide details an integration between Semperis DSP and ArcSight ESM to forward logs from DSP to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Semperis DSP to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

Endpoint	Source Groups	Destination Groups
Semperis DSP	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

2.30.16 Symantec DLP and ArcSight

The guide details an integration between Symantec DLP and ArcSight ESM to forward logs from DLP to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Symantec DLP to the machine containing the ArcSight UDP syslog container should be allowed on the port configured (in the guide, we use UDP and port 6514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	UDP	6514

Endpoint	Source Groups	Destination Groups
Symantec DLP	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

Appendix A List of Acronyms

ACC	Administration Control Center
AD	Active Directory
ADFR	Active Directory Forest Recovery
CoA	Change of Authorization
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSP	Directory Services Protector
ESM	Enterprise Security Manager
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over TLS
GUI	Graphical User Interface
IIS	Internet Information Services
ISE	Identity Services Engine
IT	Information Technology
JCE	Java Cryptography Extension
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MSSQL	Microsoft SQL
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
PAC	Proxy Auto Config
RADIUS	Remote Authentication Dial-In User Service
SDK	Software Developer Kit
SFTP	Secure FTP
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TE	Tripwire Enterprise
TLC	Tripwire Log Center
VLAN	Virtual LAN
WDV	WORM Disk Volume
WORM	Write Once Read Many
WPAD	Web Proxy Auto Discovery

WSA Web Security Appliance