NIST SPECIAL PUBLICATION 1800-26C

Data Integrity

Detecting and Responding to 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

January 2020

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond.

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 1800-26C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-26C, 440 pages, (January 2020), CODEN: NSPUE2

FEEDBACK

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

Comments on this publication may be submitted to: ds-nccoe@nist.gov.

Public comment period: January 27, 2020 through February 25, 2020

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, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST 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 more easily with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Ransomware, destructive malware, insider threats, and even honest mistakes present an ongoing threat to organizations that manage data in various forms. Database records and structure, system files, configurations, user files, application code, and customer data are all potential targets of data corruption and destruction.

A quick, accurate, and thorough detection and response to a loss of data integrity can save an organization time, money, and headaches. While human knowledge and expertise is an essential component of these tasks, the right tools and preparation are essential to minimizing downtime and

losses due to data integrity events. 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. This project details methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network. It also identifies tools and strategies to aid in a security team's response to such an event.

KEYWORDS

attack vector; data integrity; malicious actor; malware; malware detection; malware response; 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
Matthew Shabat	Glasswall Government Solutions
Justin Rowland	Glasswall Government Solutions
Greg Rhein	Glasswall Government Solutions
Steve Roberts	Micro Focus
Timothy McBride	NIST
Christopher Lowde	Semperis

Thomas Leduc	Semperis
Darren Mar-Elia	Semperis
Kirk Lashbrook	Semperis
Mickey Bresman	Semperis
Humphrey Christian	Symantec Corporation
Jon Christmas	Symantec Corporation
Kenneth Durbin	Symantec Corporation
Matthew Giblin	Symantec Corporation
Jim Wachhaus	Tripwire
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
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 Information Centric Analytics v6.5.2 Symantec Security Analytics v8.0.1
Cisco Systems	Cisco Identity Services Engine v2.4, Cisco Advanced Malware Protection v5.4, Cisco Stealthwatch v7.0.0
Glasswall Government Solutions	Glasswall FileTrust ATP for Email v6.90.2.5
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Semperis	Semperis Directory Services Protector v2.7

Contents

1 Introduction

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

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

1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the data integrity detection and response solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-26a: *Executive Summary*
- NIST SP 1800-26b: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-26c: *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 1800-26a)*, which describes the:

- challenges enterprises face in detecting and responding to 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 1800-26b,* which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Risk, provides a description of the risk analysis we performed.
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-26a,* 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 the How-To portion of the guide, *NIST SP 1800-26c*, to replicate all or parts of the build created in our lab. The How-To 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 detection and response solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Volume B, Section 3.5, 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 NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively detect and respond to a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also explored the issues of analysis and reporting to support incident response. 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 non-comprehensive) 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.

1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

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

2 Product Installation Guides

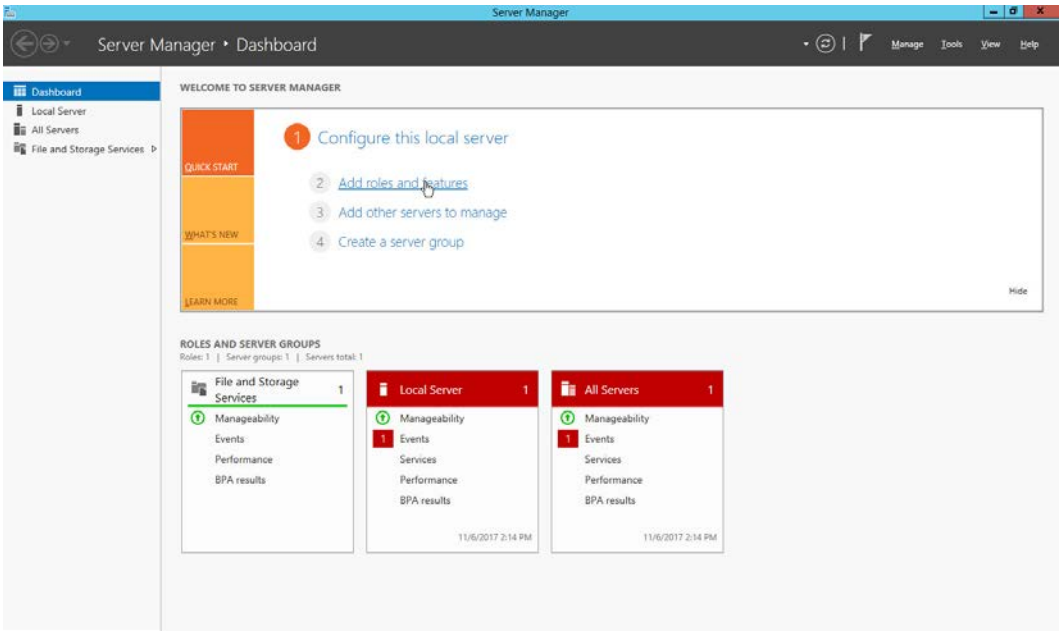
This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

2.1 Active Directory and Domain Name System Server

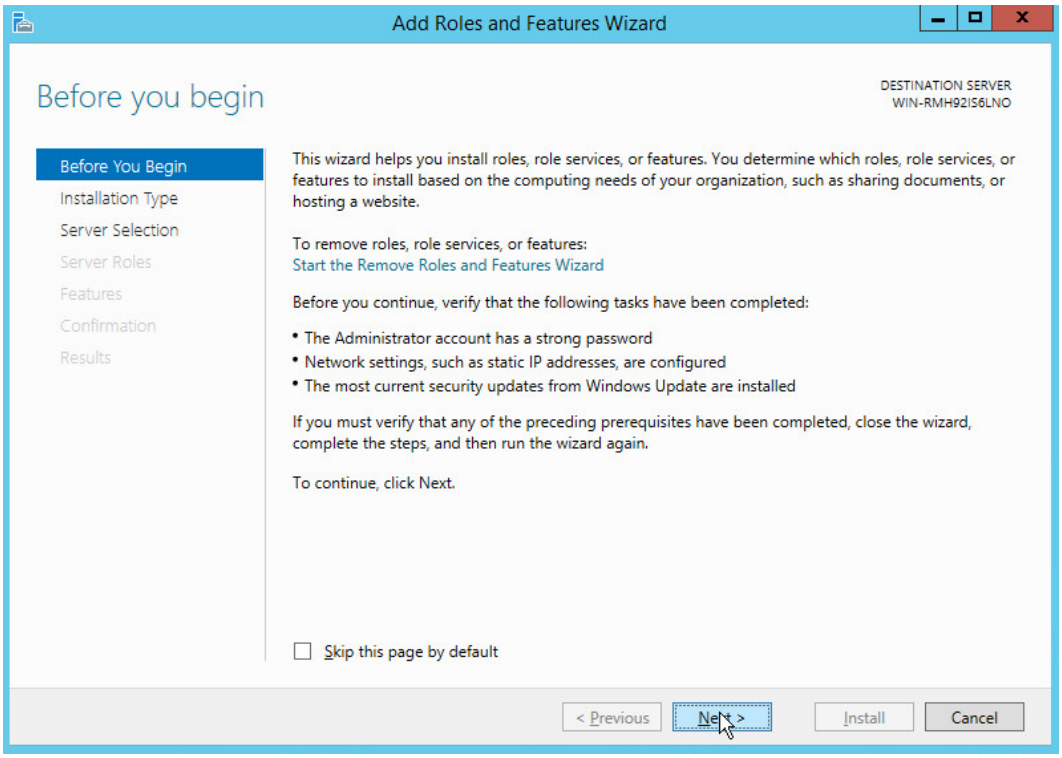
As part of our enterprise emulation, we included an Active Directory server that doubles as a Domain Name System (DNS) server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

2.1.1 Install Features

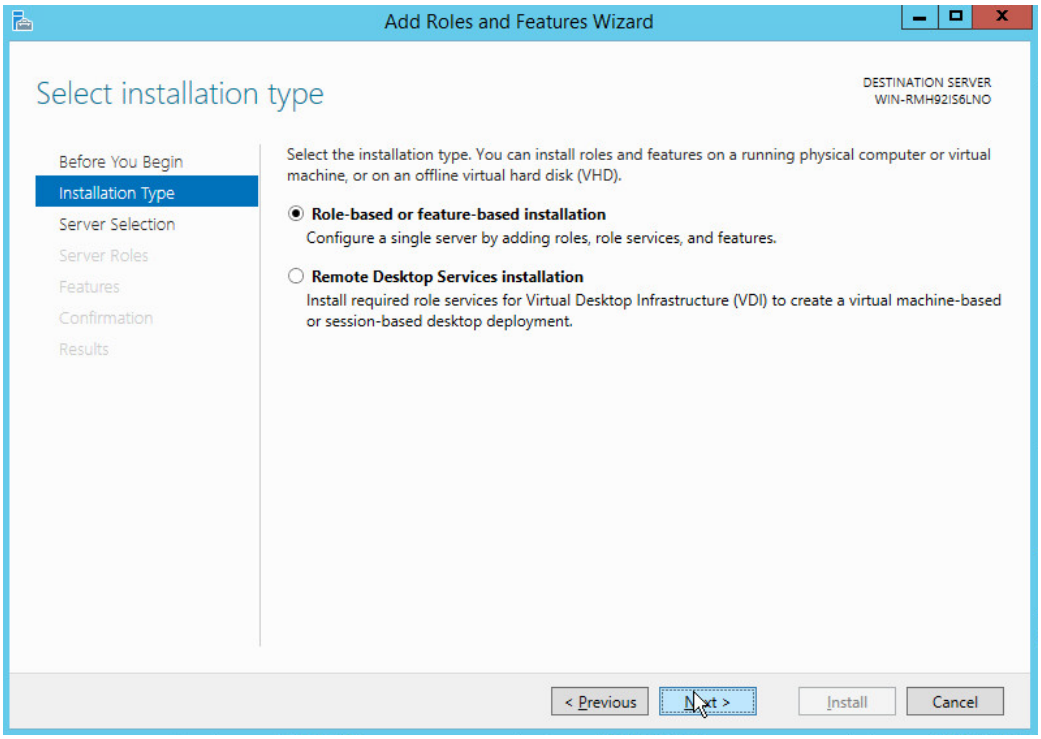
1. Open **Server Manager.**



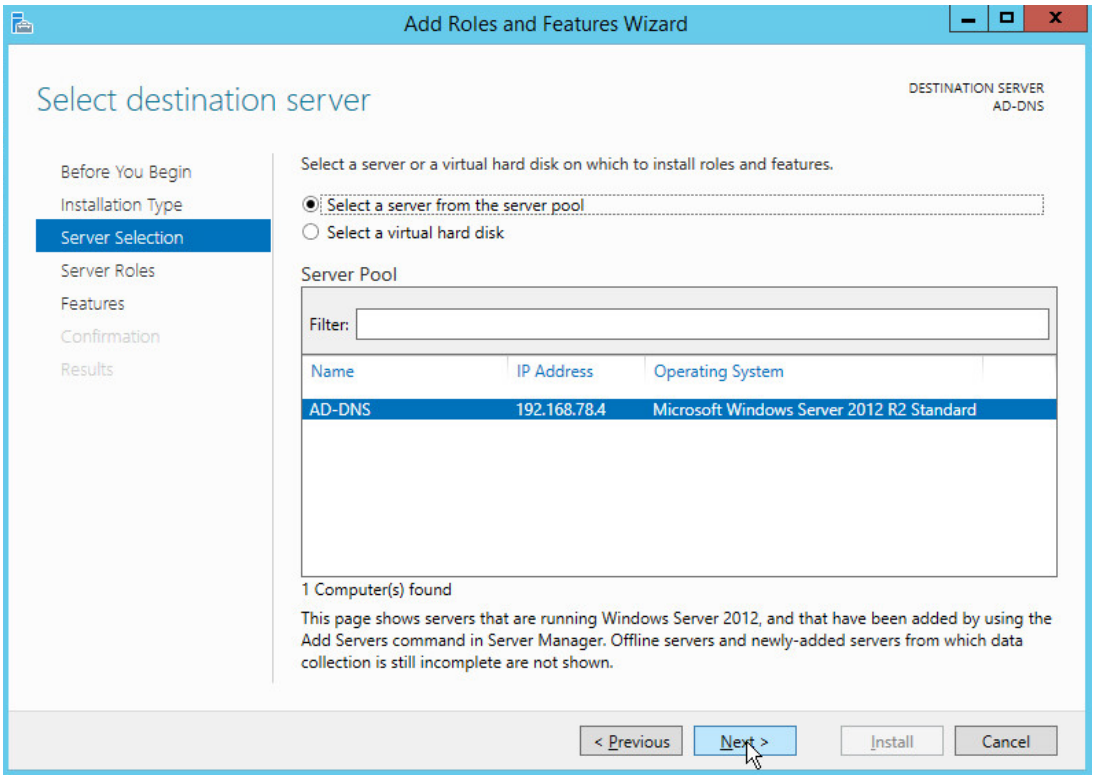
2. Click the link **Add roles and features.**



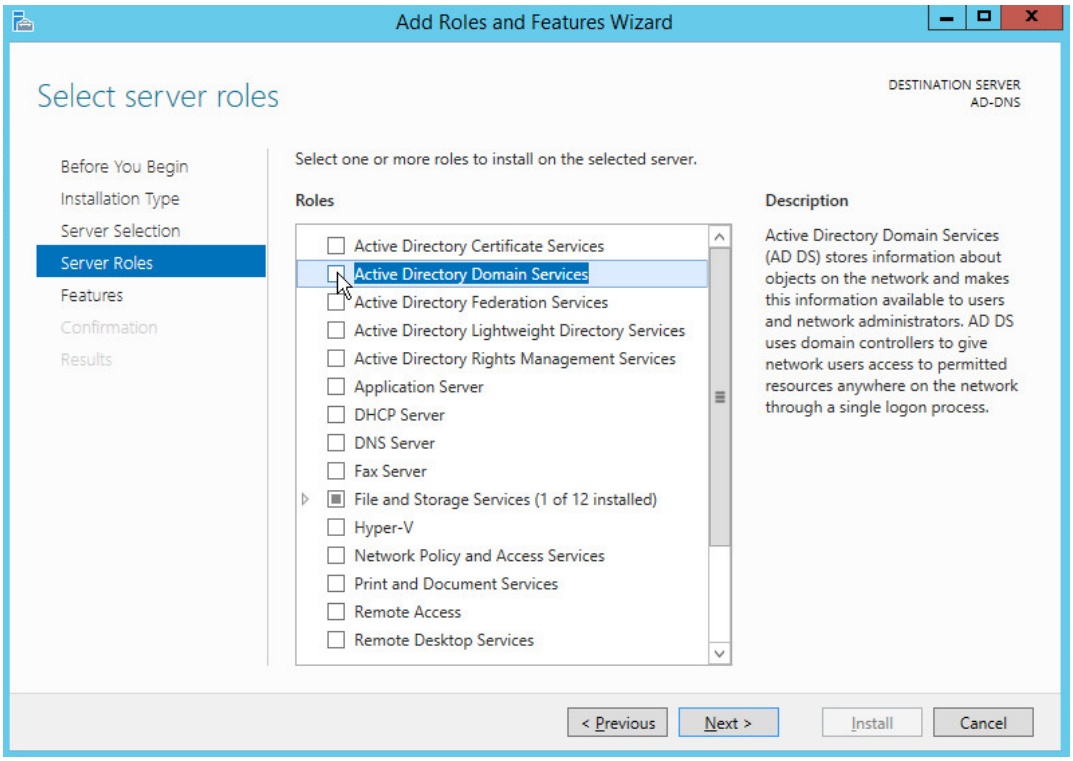
3. Click **Next.**
4. Select **Role-based or feature-based installation.**



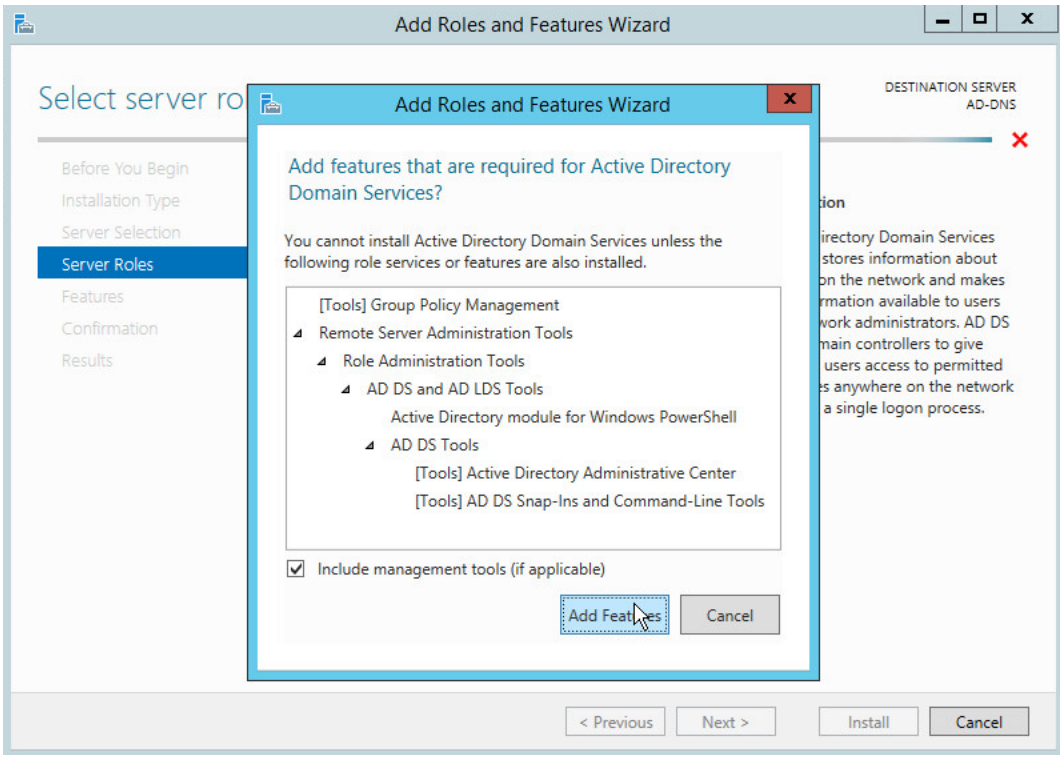
5. Click **Next.**
6. Select **Select a server from the server pool.**
7. Select the intended active directory server.


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
AD-DNS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
AD-DNS
192.168.78.4
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

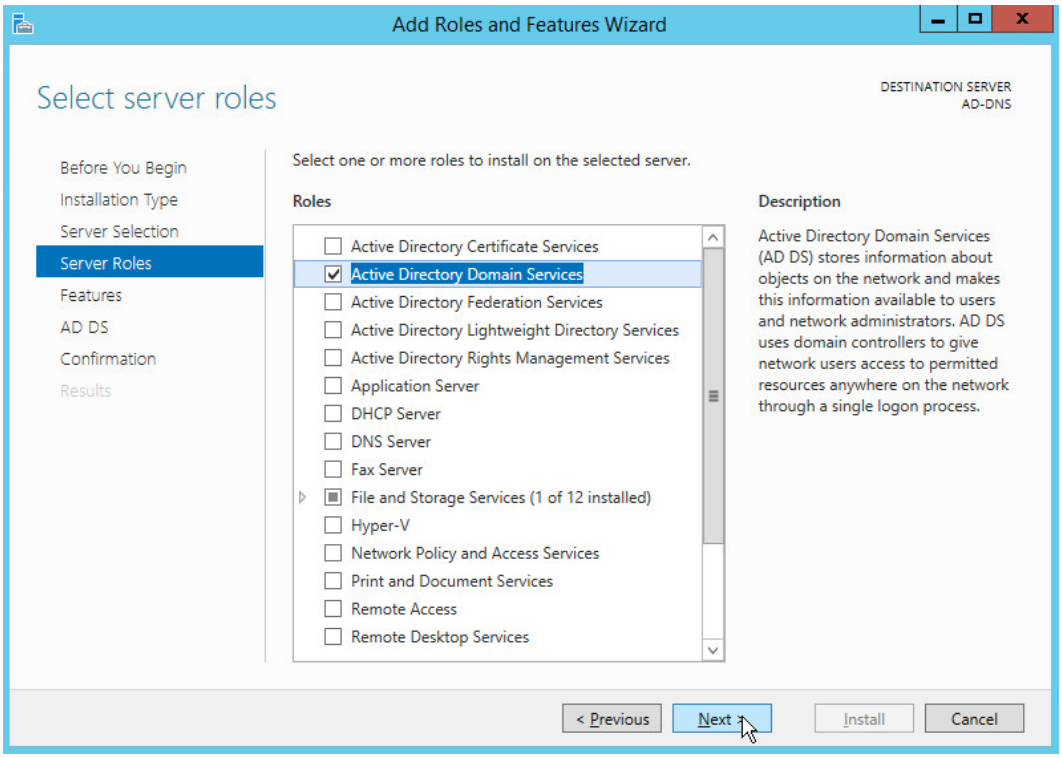
8. Click **Next.**



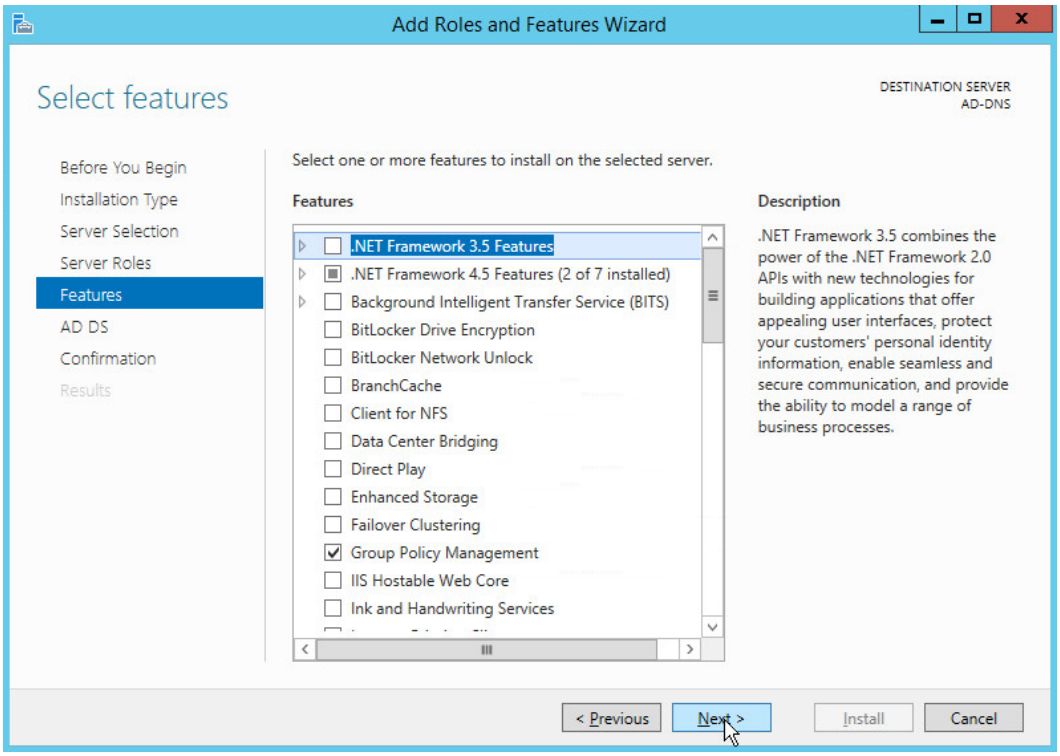
9. Check the box next to **Active Directory Domain Services.**



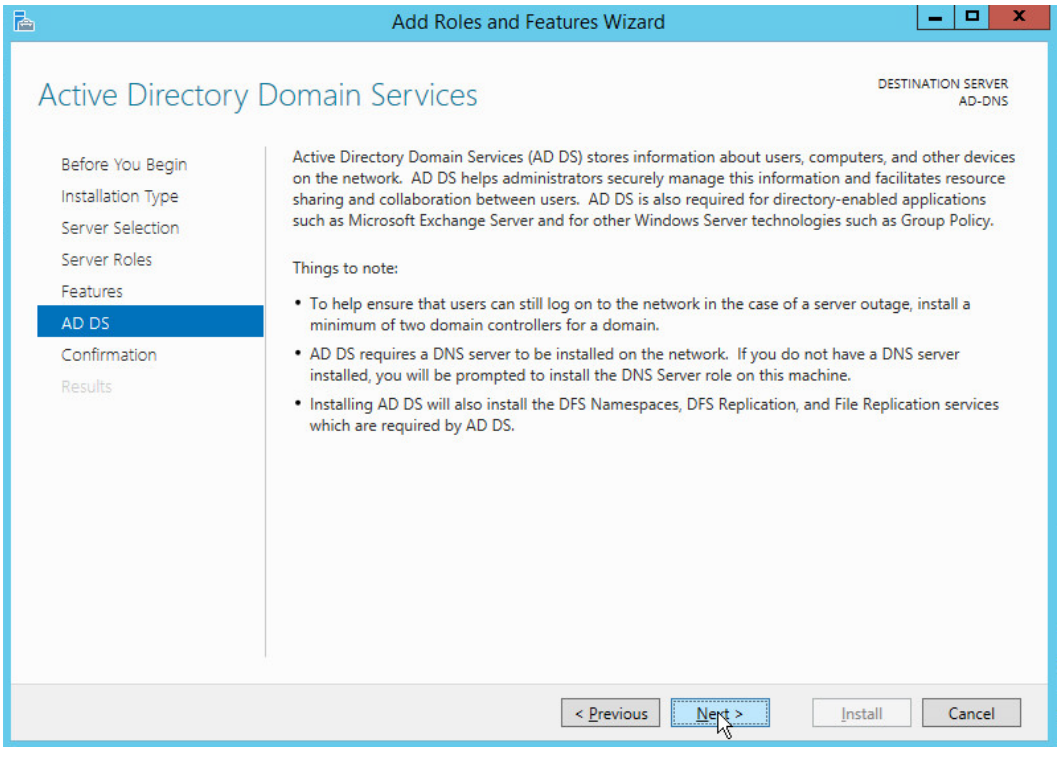
296
297 10. Click **Add Features.**



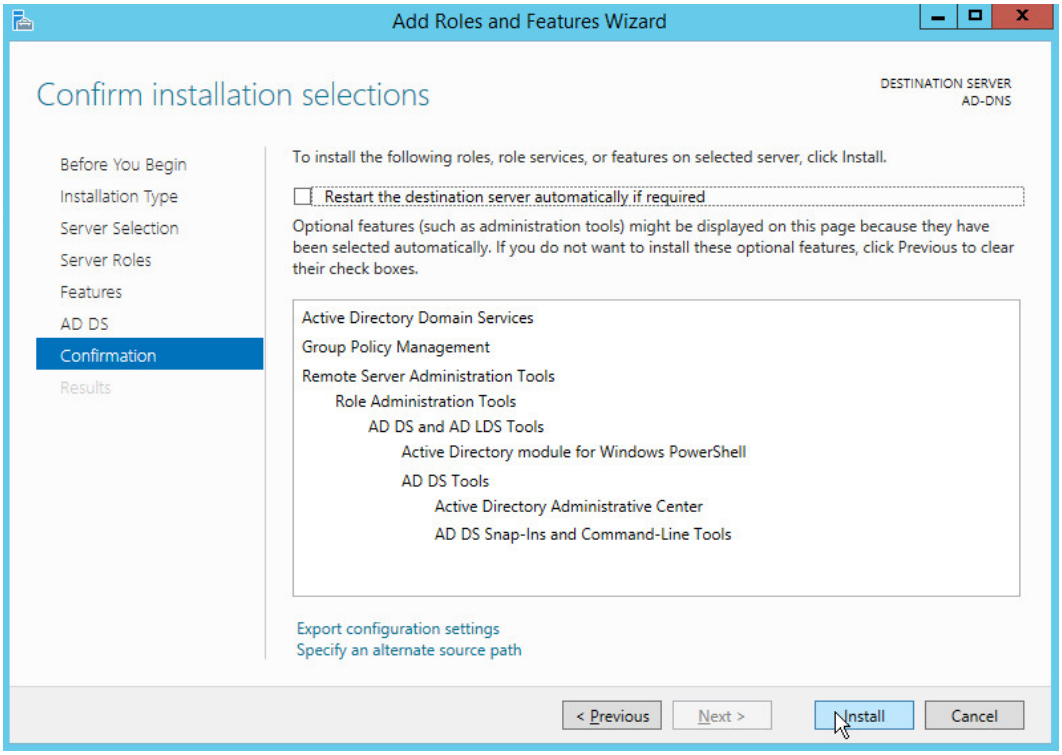
11. Click **Next.**



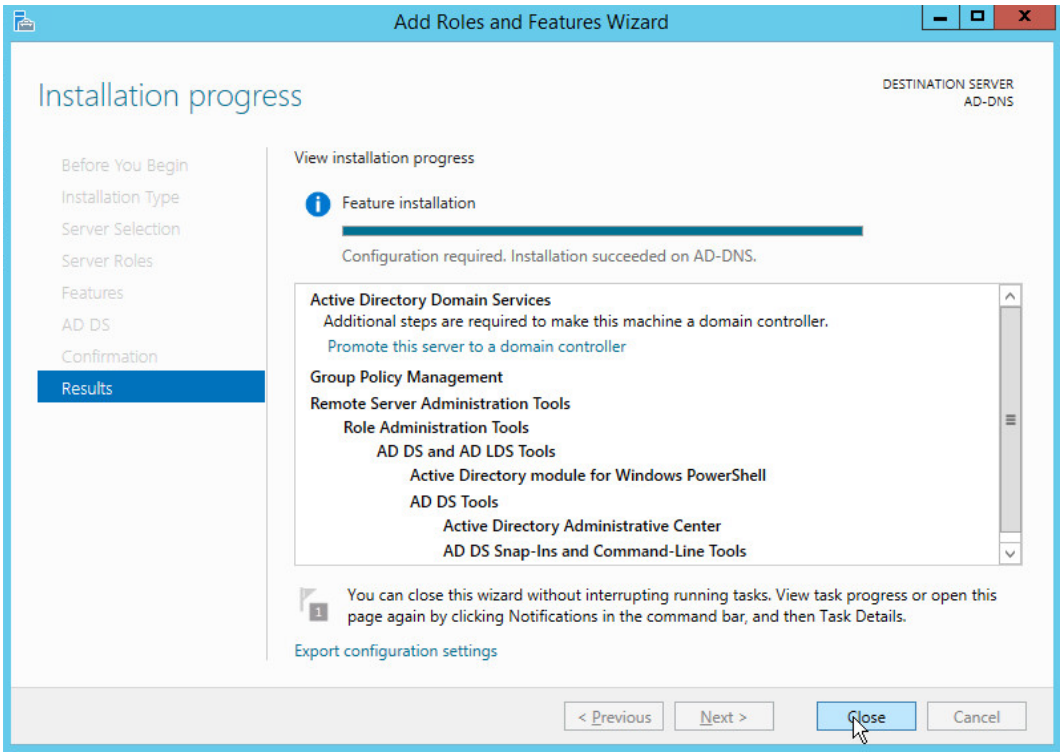
12. Click **Next.**



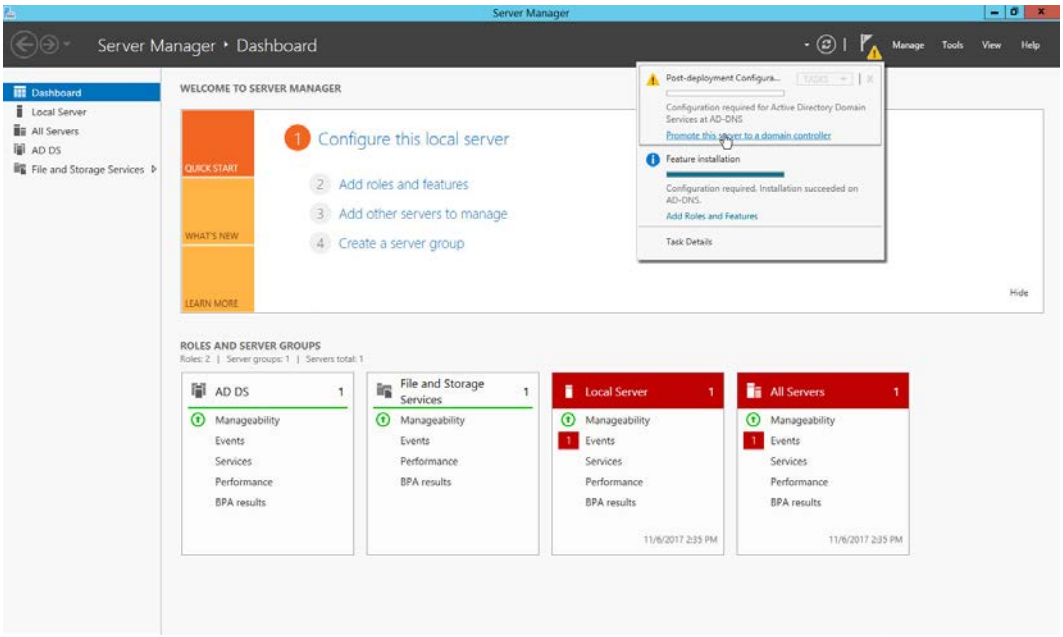
13. Click **Next.**



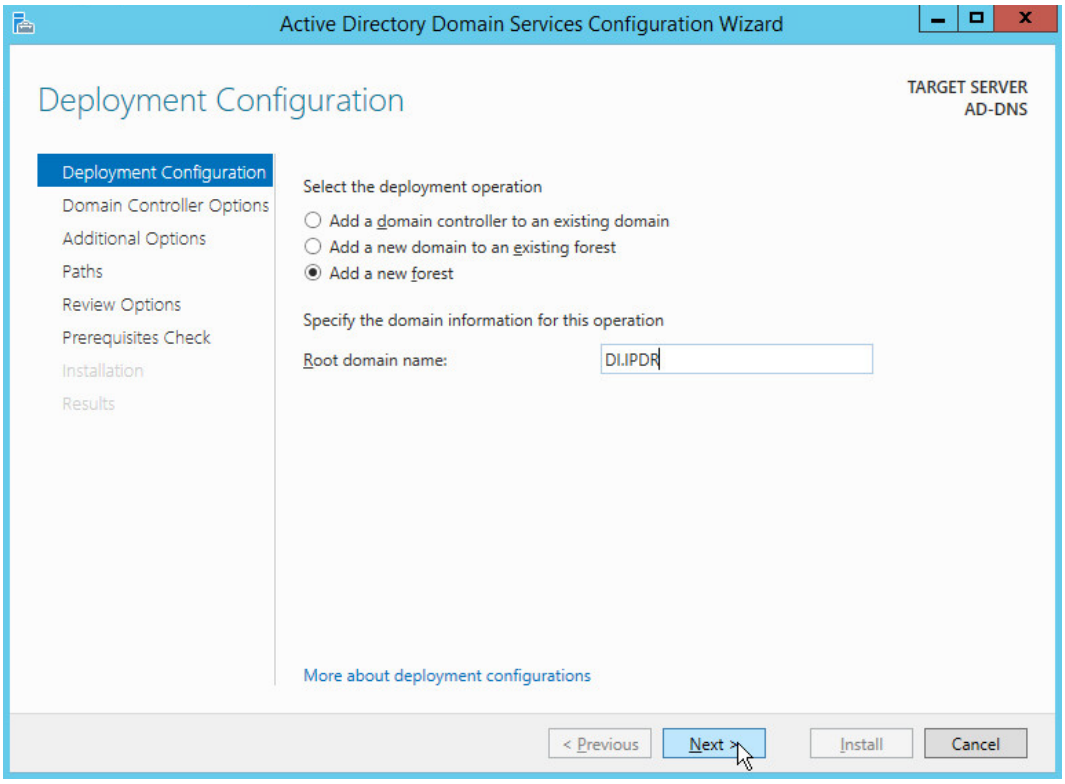
14. Click **Install.**
15. Wait for the installation to complete.



16. Click **Close.**



17. Click **Promote this server to a domain controller.**
18. Select **Add a new forest.**
19. Enter a **Root domain name.**



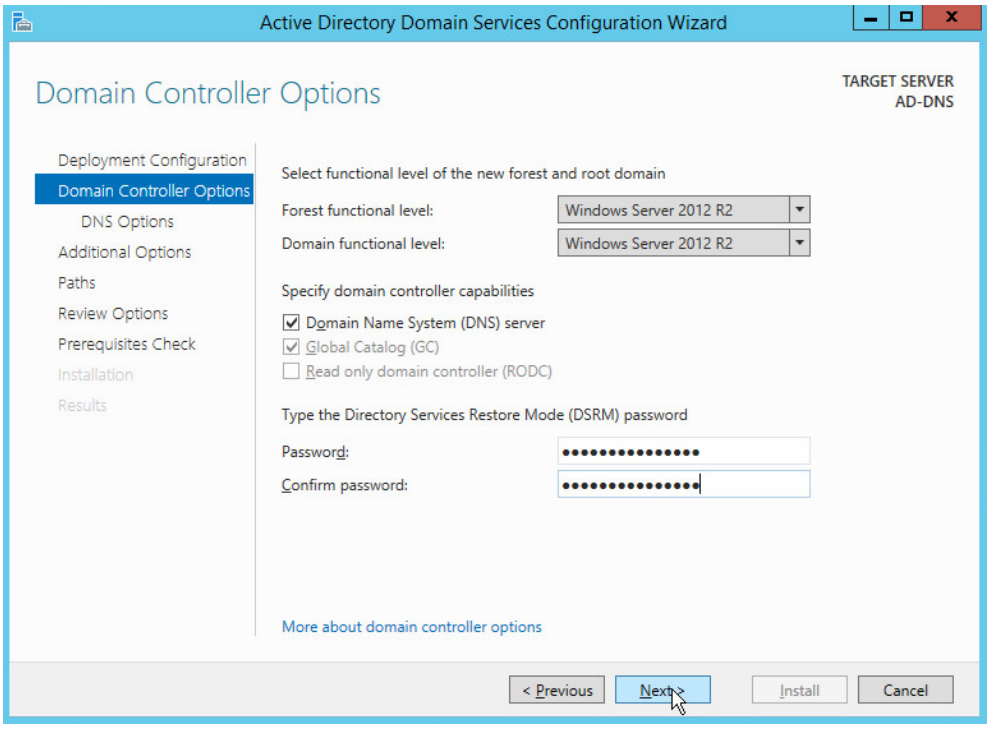
313

314 20. Click **Next.**

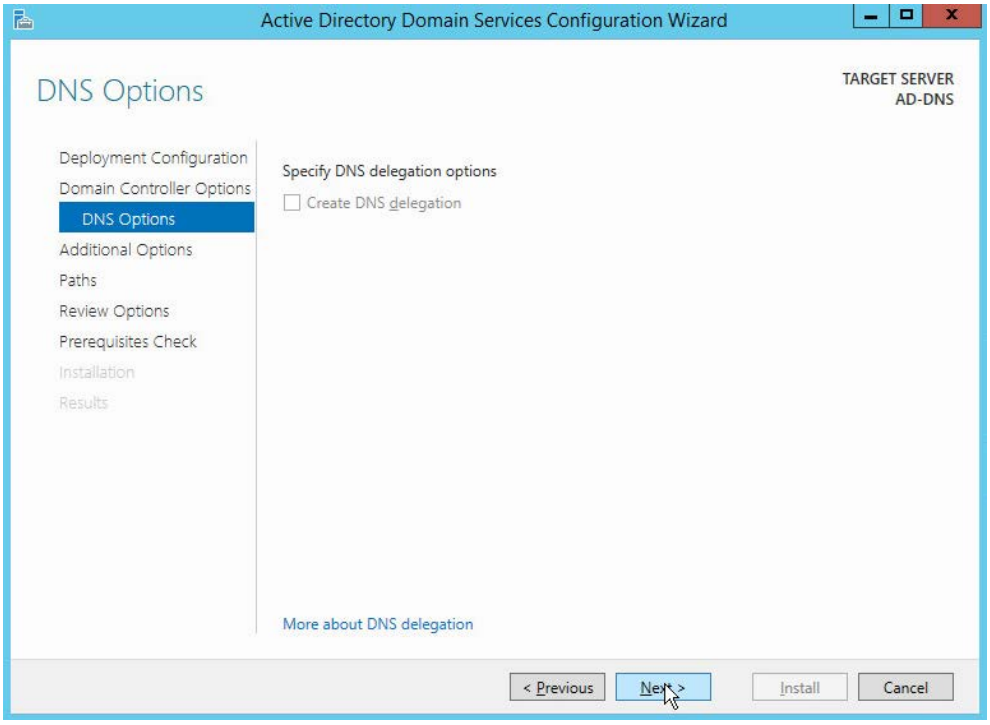
315 21. Select **Windows Server 2012 R2** for **Forest functional level** and **Domain functional level.**

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

317 23. Enter a password.

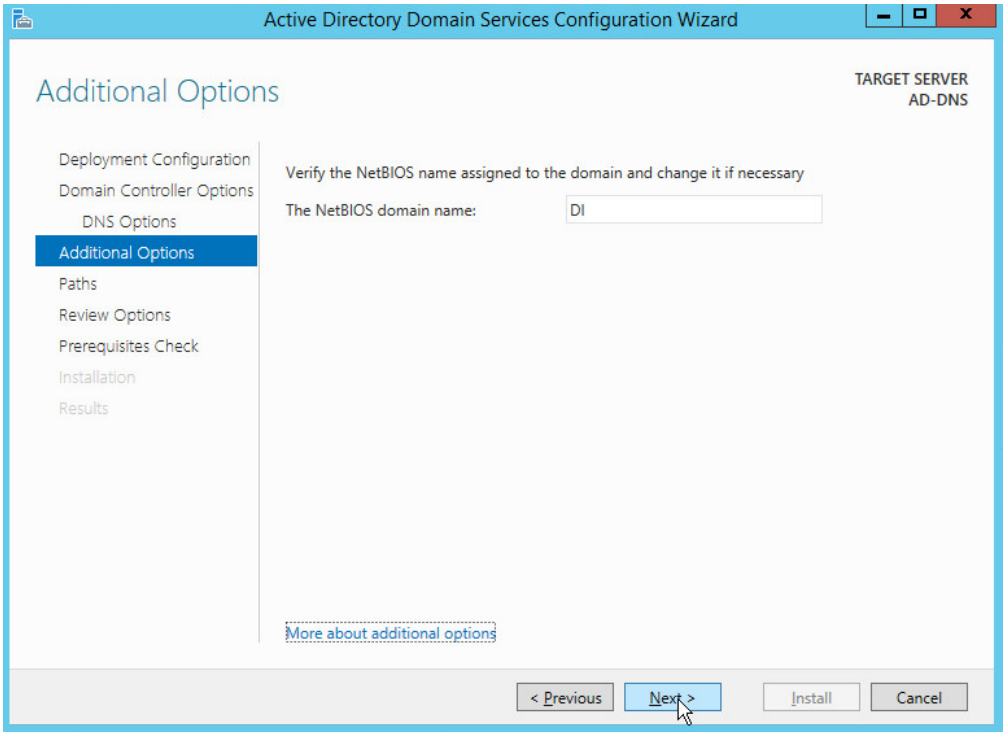


318
319 24. Click **Next.**

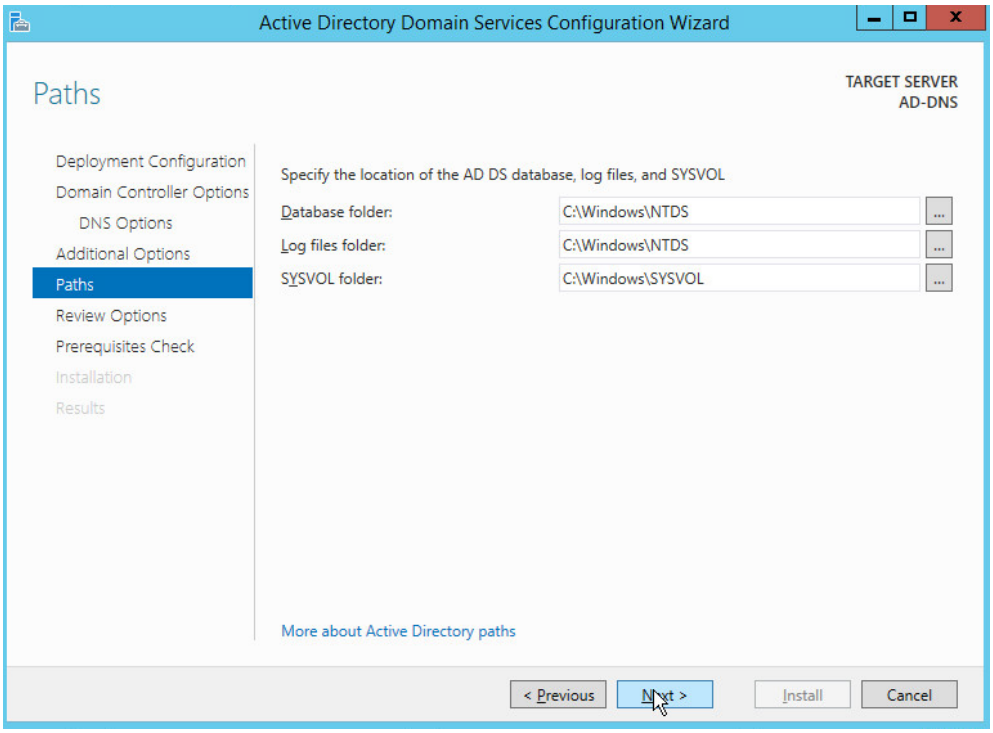


320
321 25. Click **Next.**

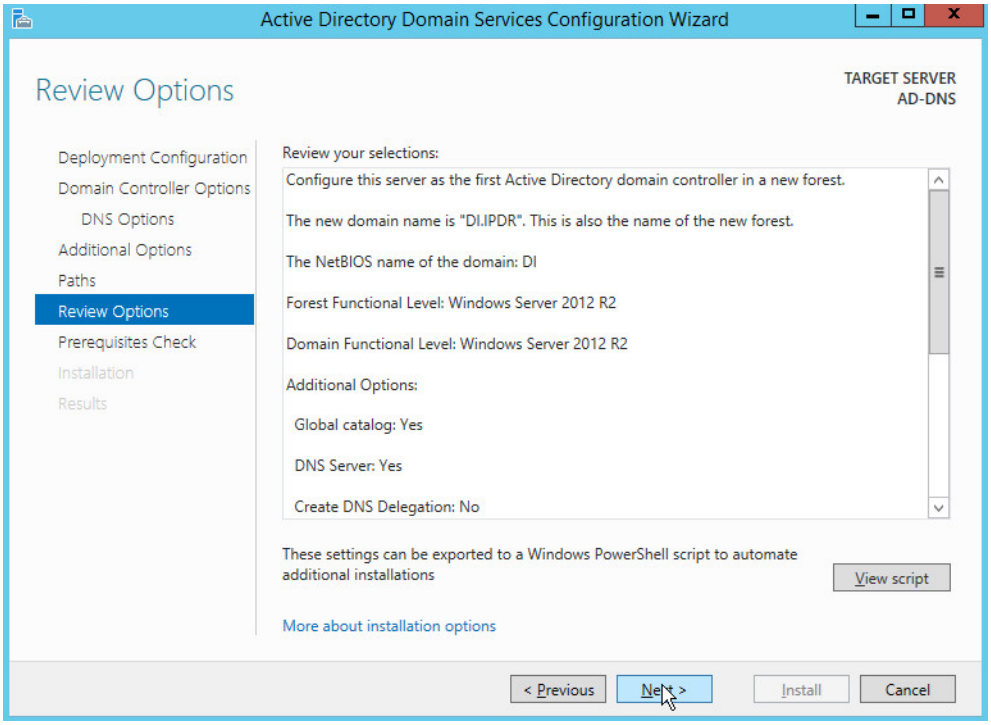
26. Verify the domain name.



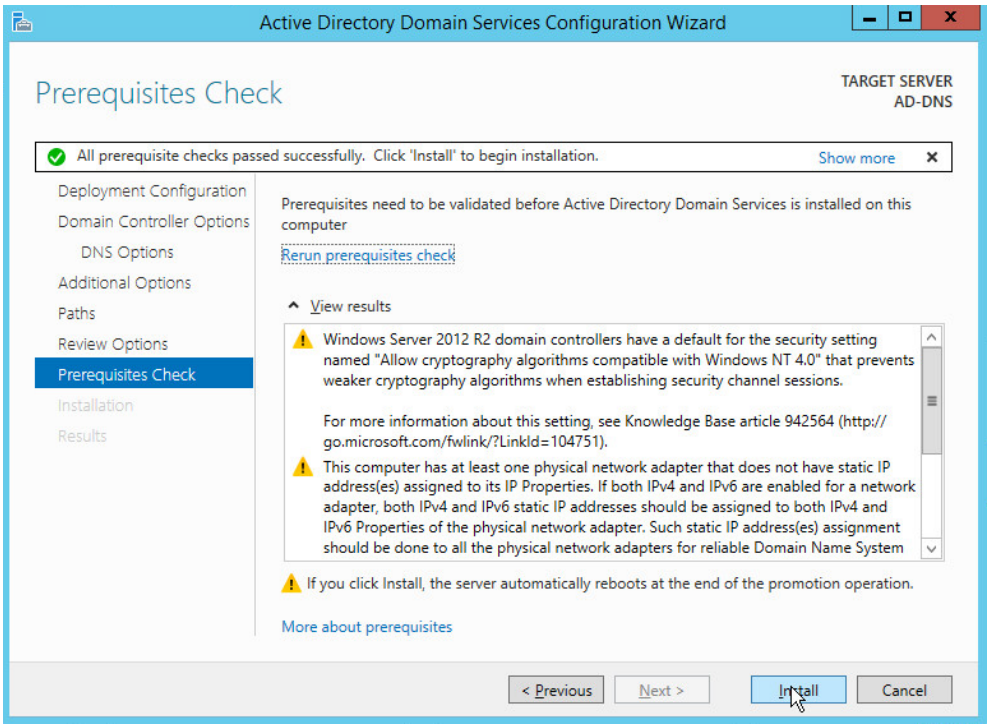
27. Click **Next.**



28. Click **Next.**



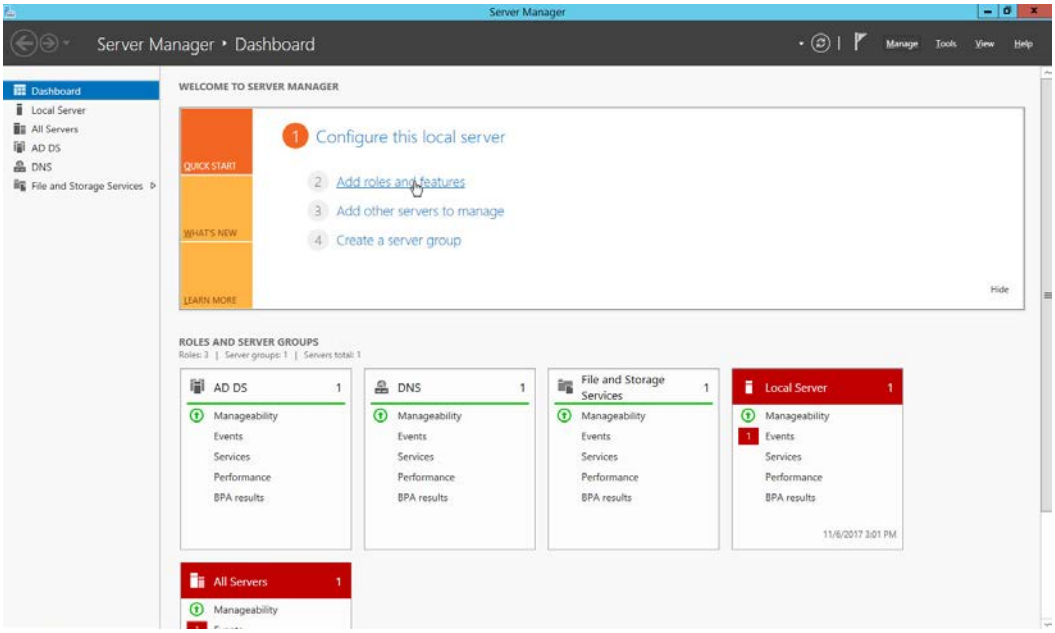
29. Click **Next.**



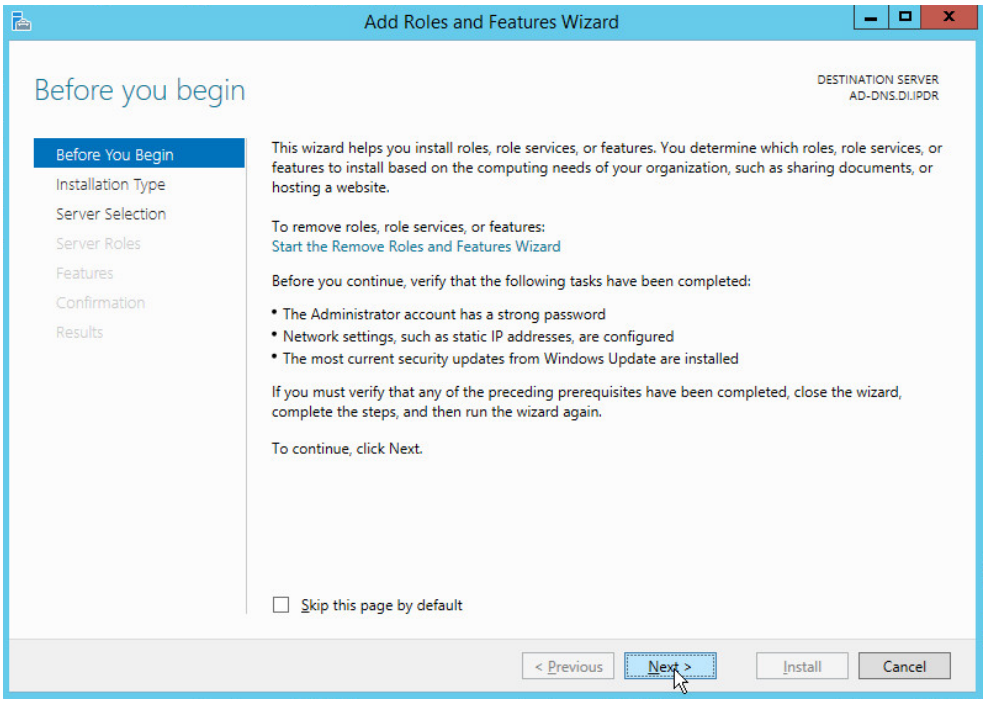
30. Click **Install.**
31. Wait for the installation to complete.
32. The server automatically reboots.

2.1.2 Create a Certificate Authority

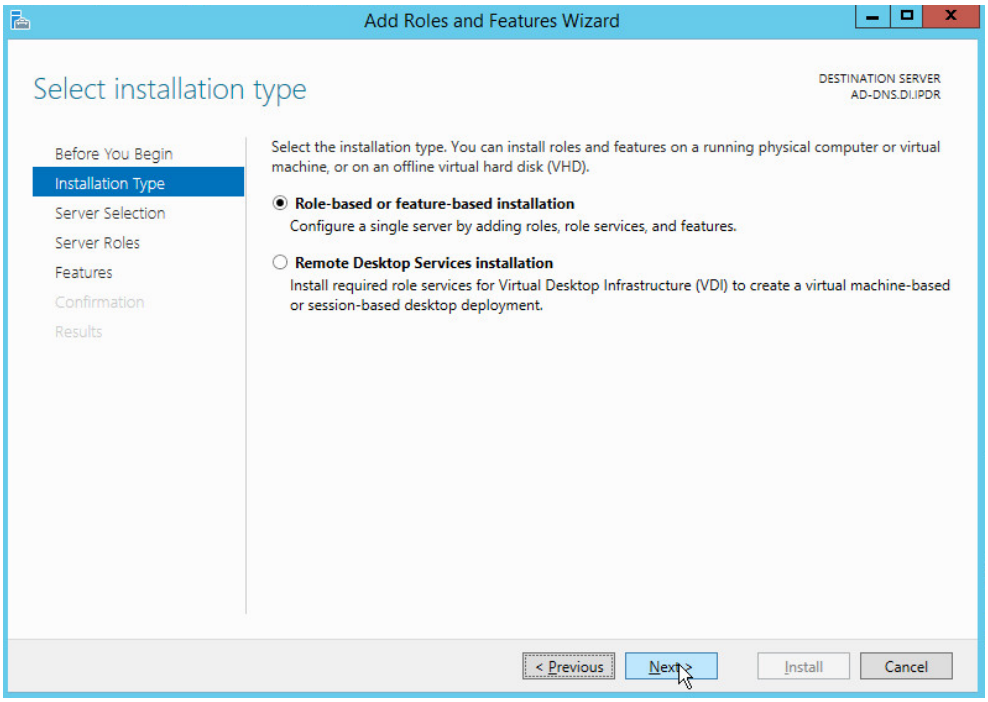
1. Open **Server Manager.**



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

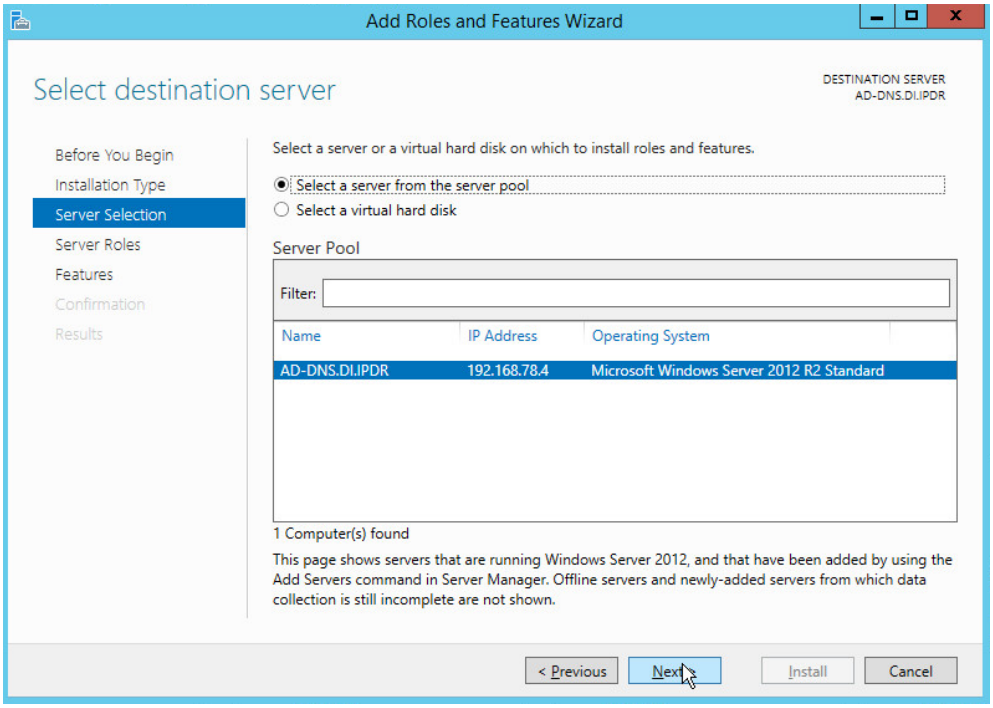


3. Click **Next.**
4. Select **Role-based or feature-based installation.**

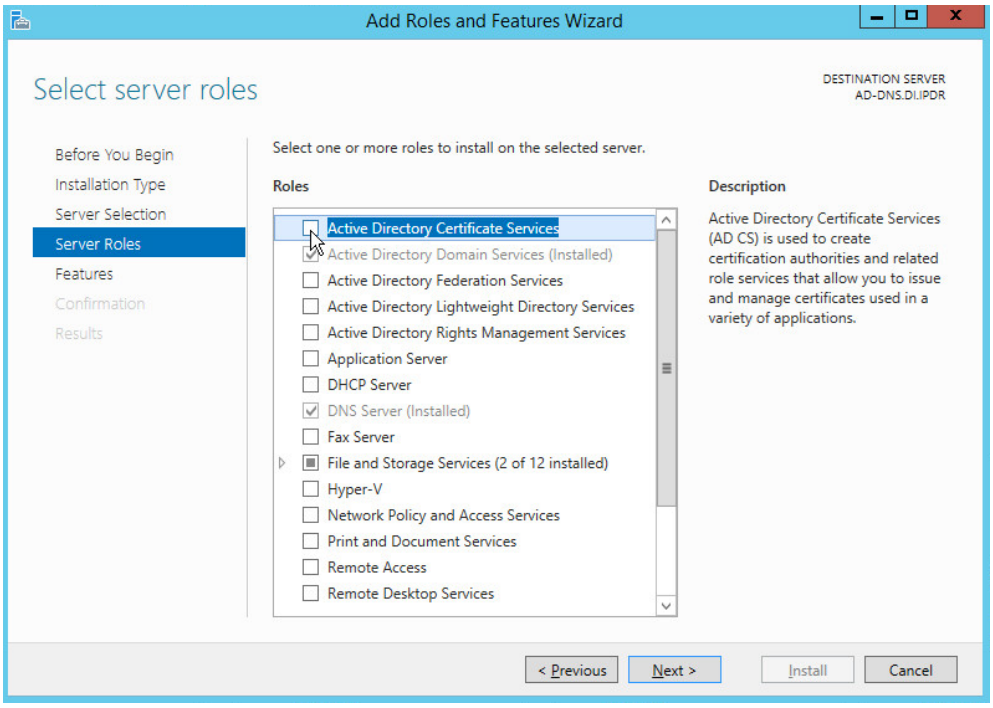


5. Click **Next.**

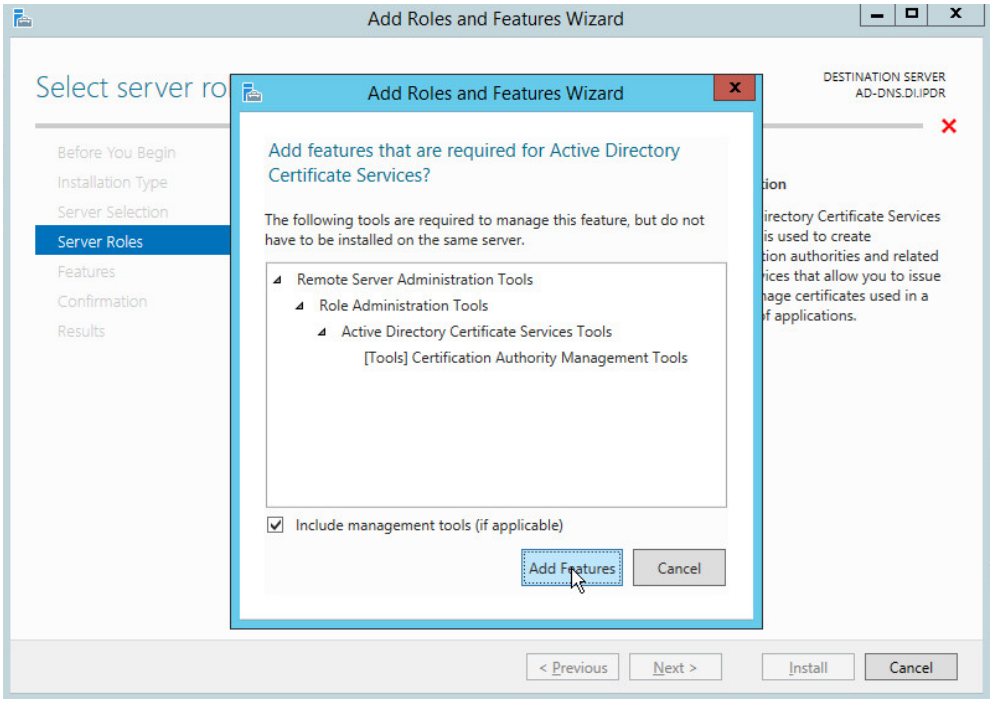
6. Select **Select a server from the server pool.**
7. Select the intended Active Directory server.



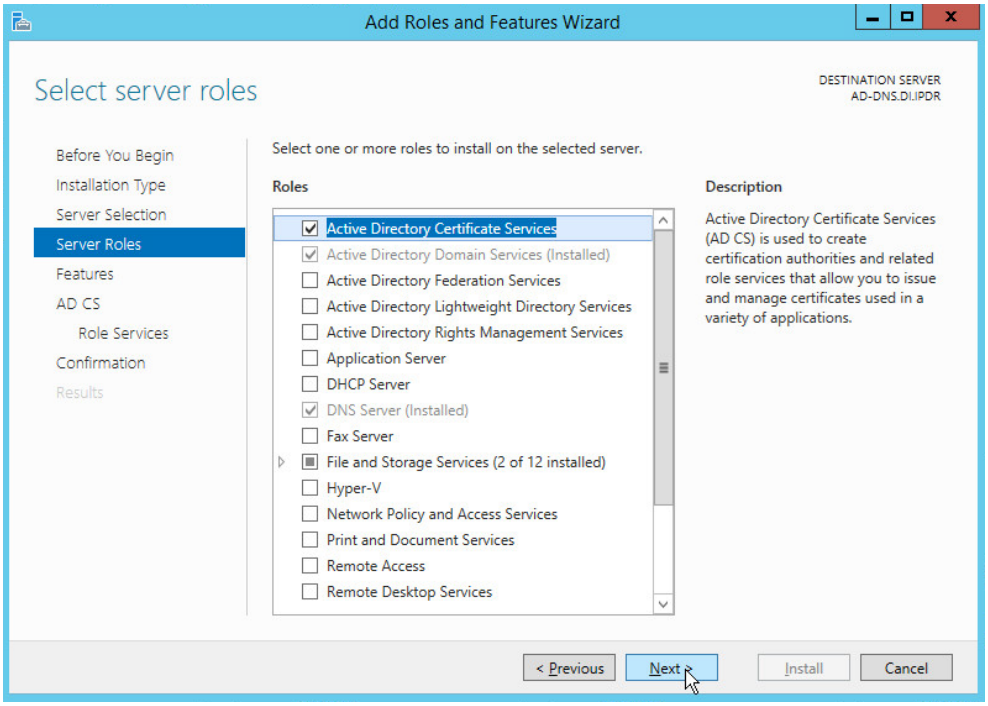
8. Click **Next.**



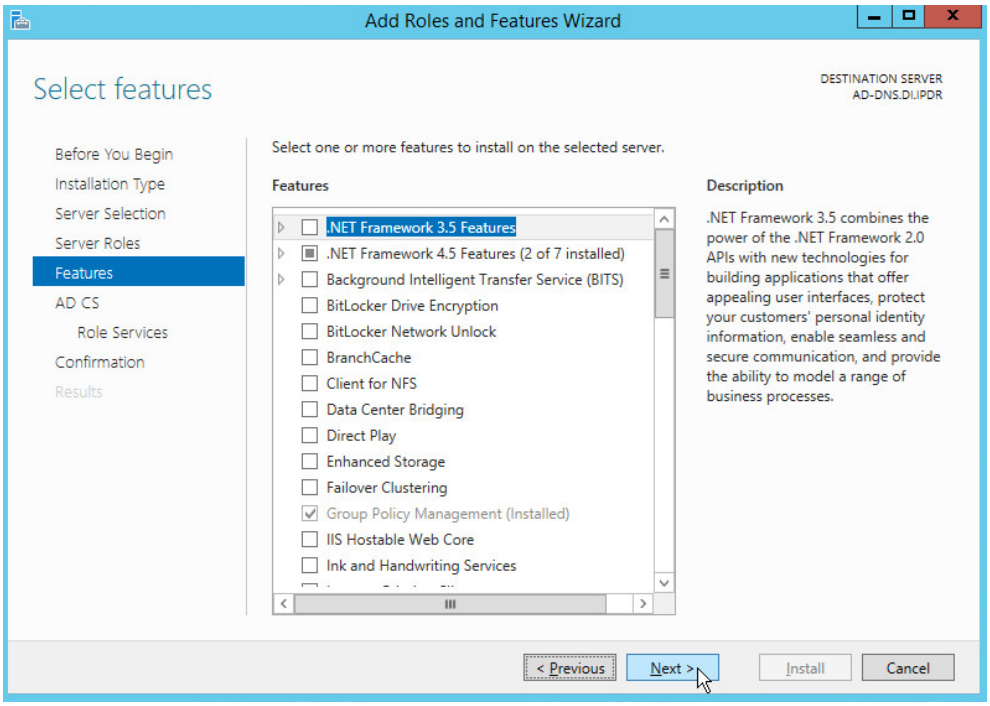
9. Check the box next to **Active Directory Certificate Services.**



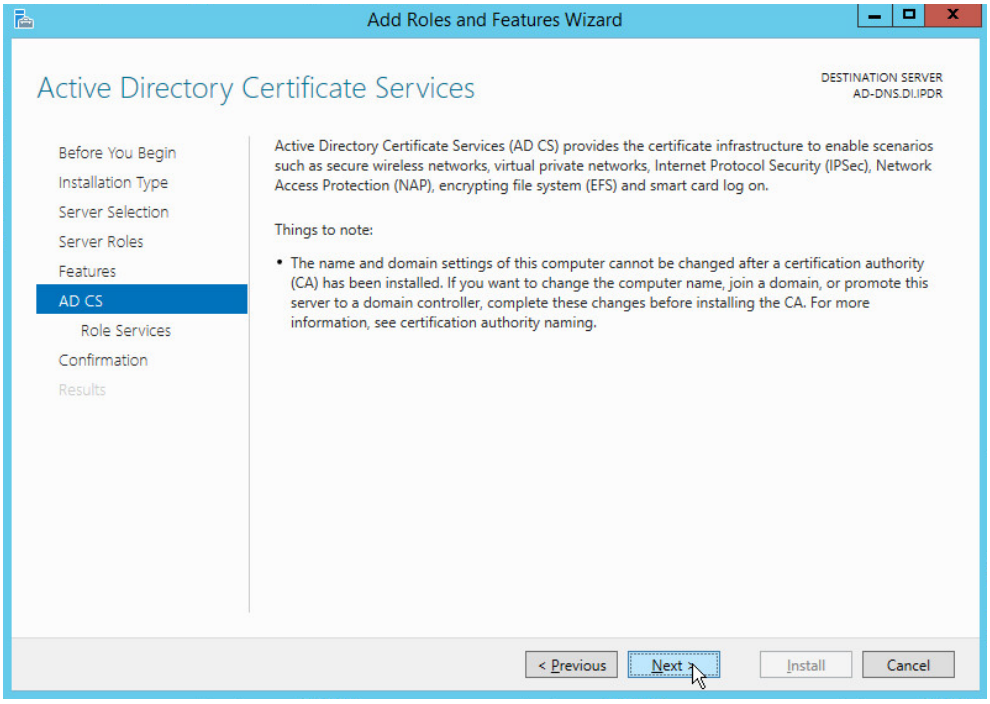
10. Click **Add Features.**



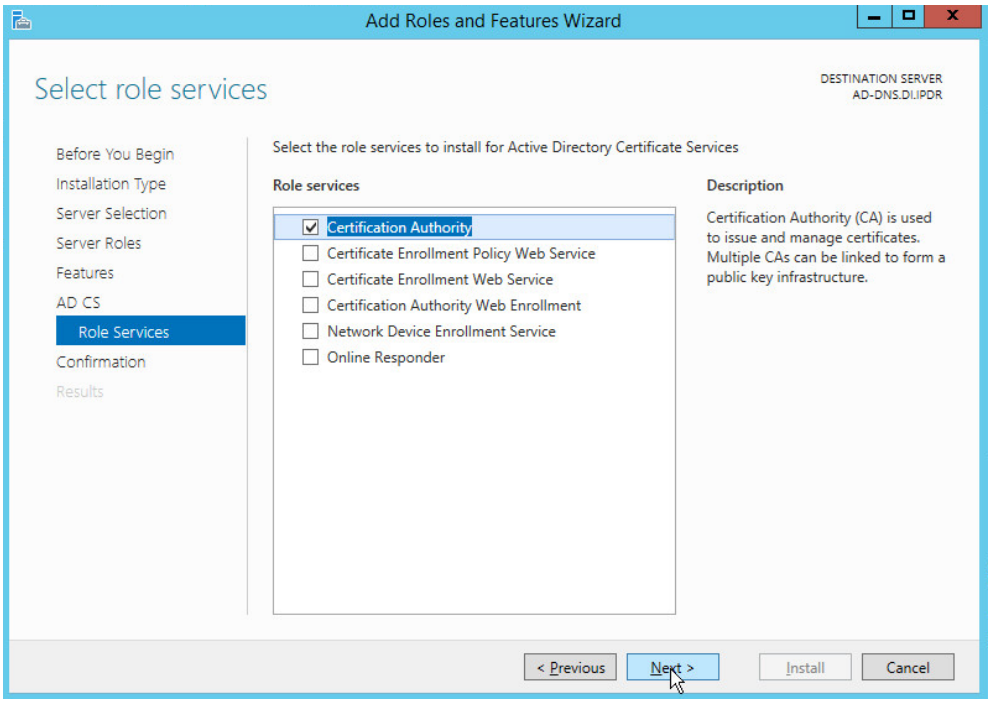
11. Click **Next.**



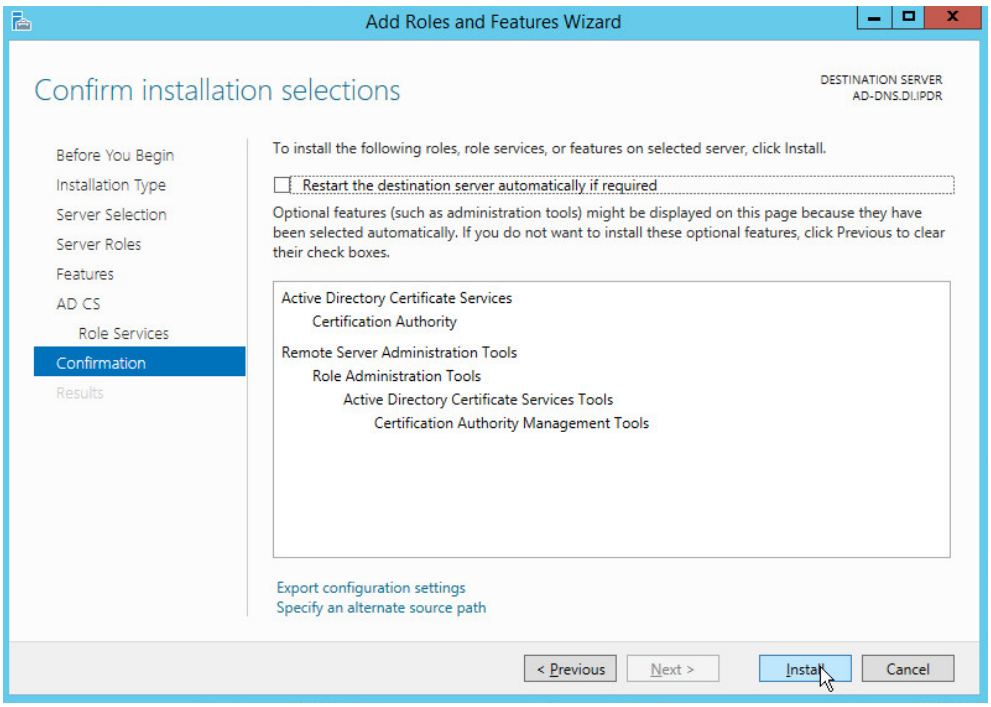
12. Click **Next.**



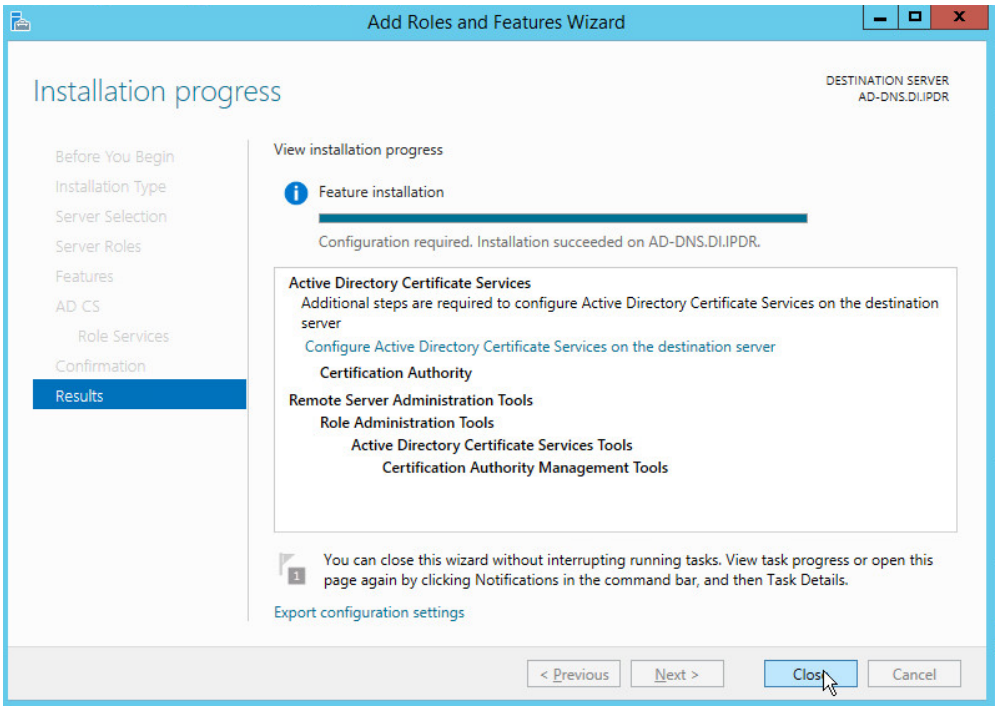
13. Click **Next.**
14. Check the box next to **Certification Authority.**



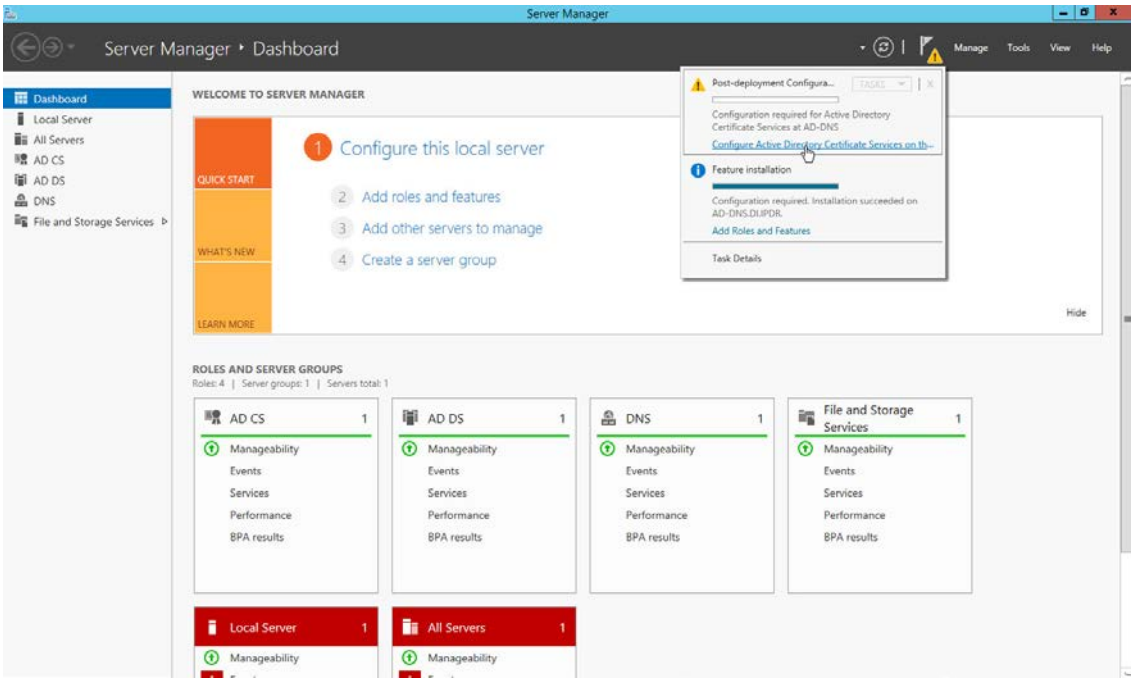
15. Click **Next.**



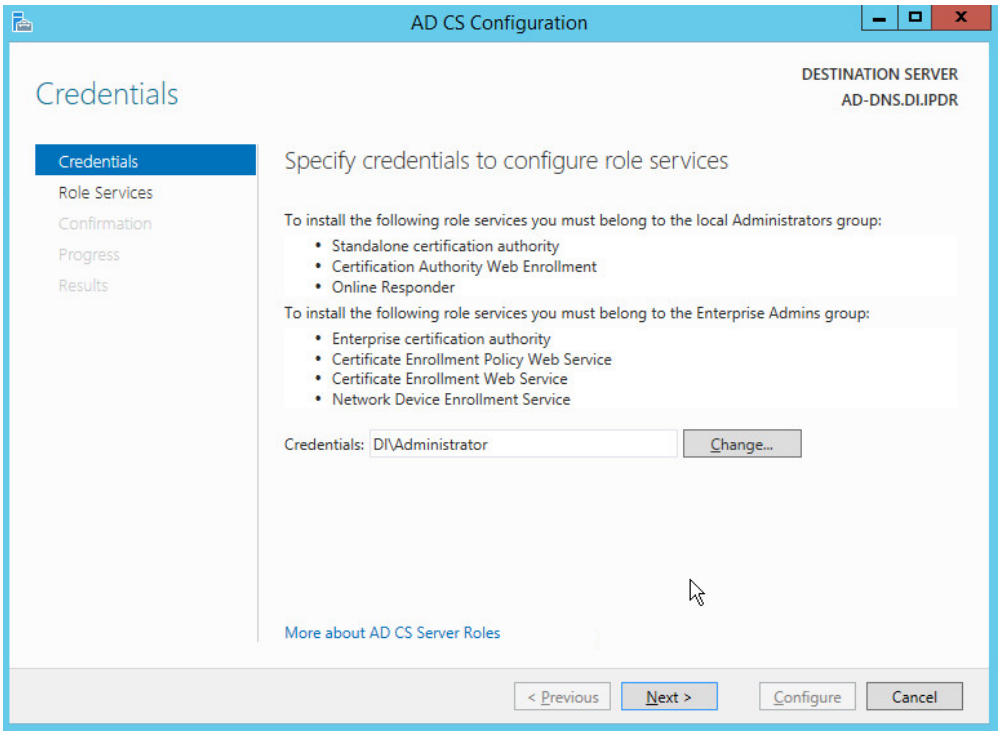
16. Click **Install.**
17. Wait for the installation to complete.



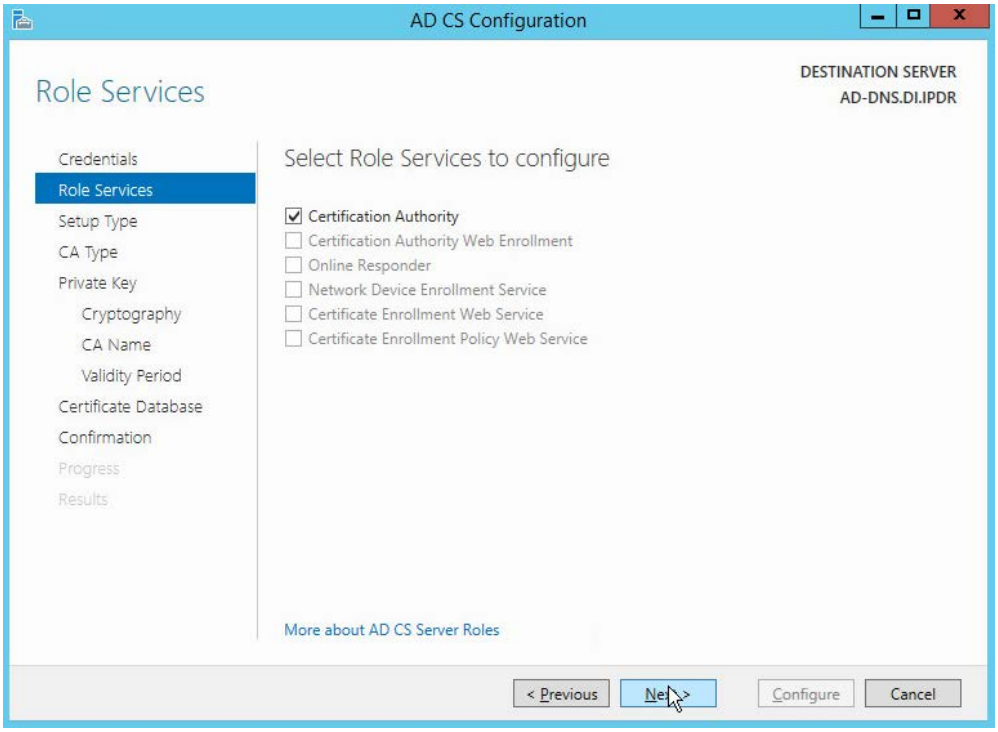
18. Click **Close.**



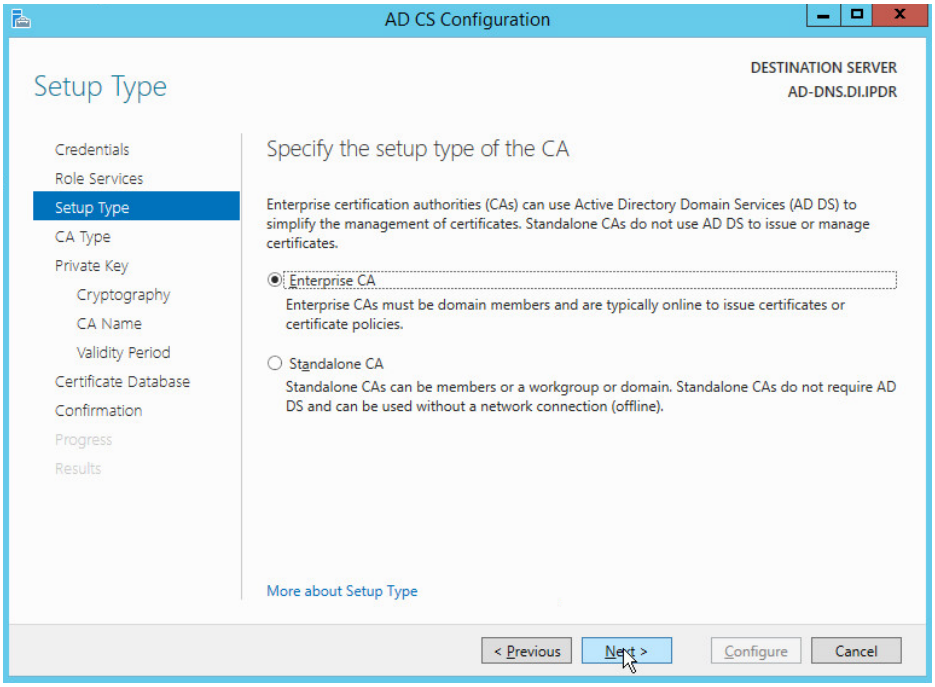
19. Click **Configure Active Directory Certificate Serves on the destination server.**



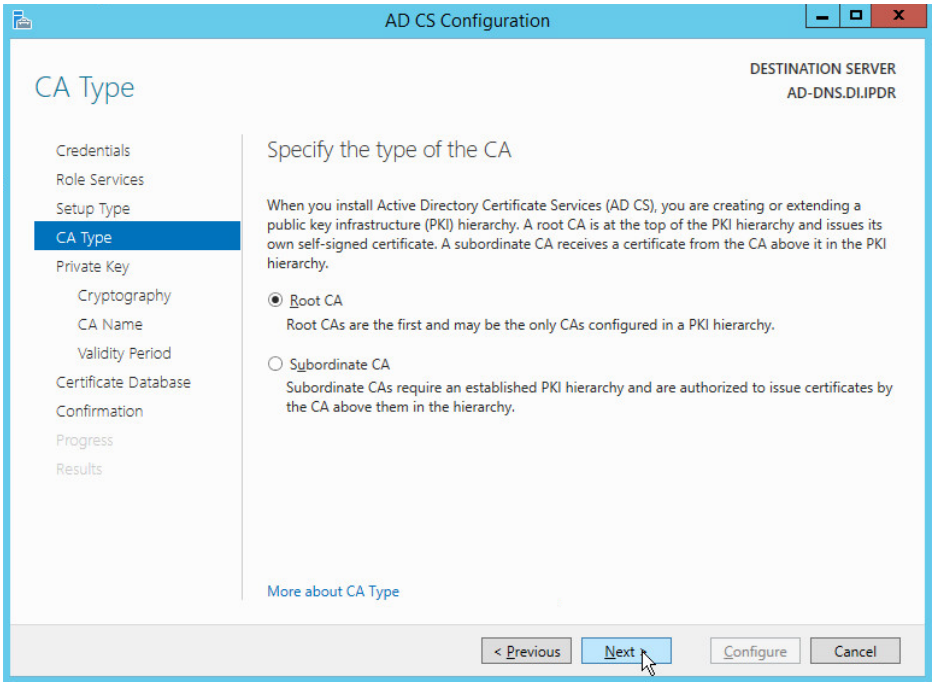
20. Click **Next.**
21. Check the box next to **Certification Authority.**



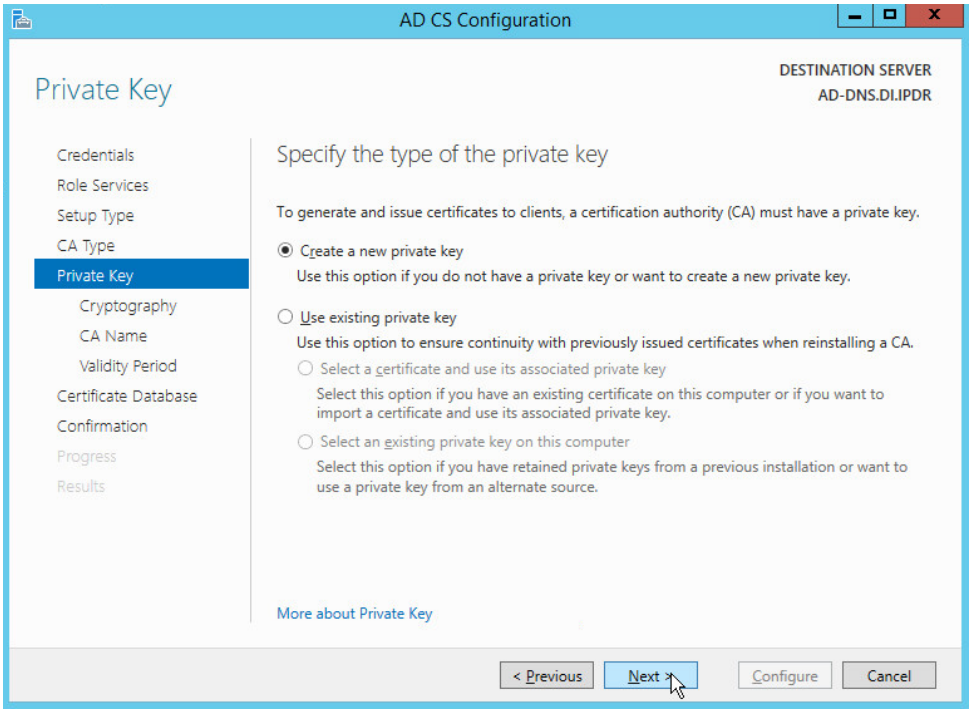
22. Click **Next.**
23. Select **Enterprise CA.**



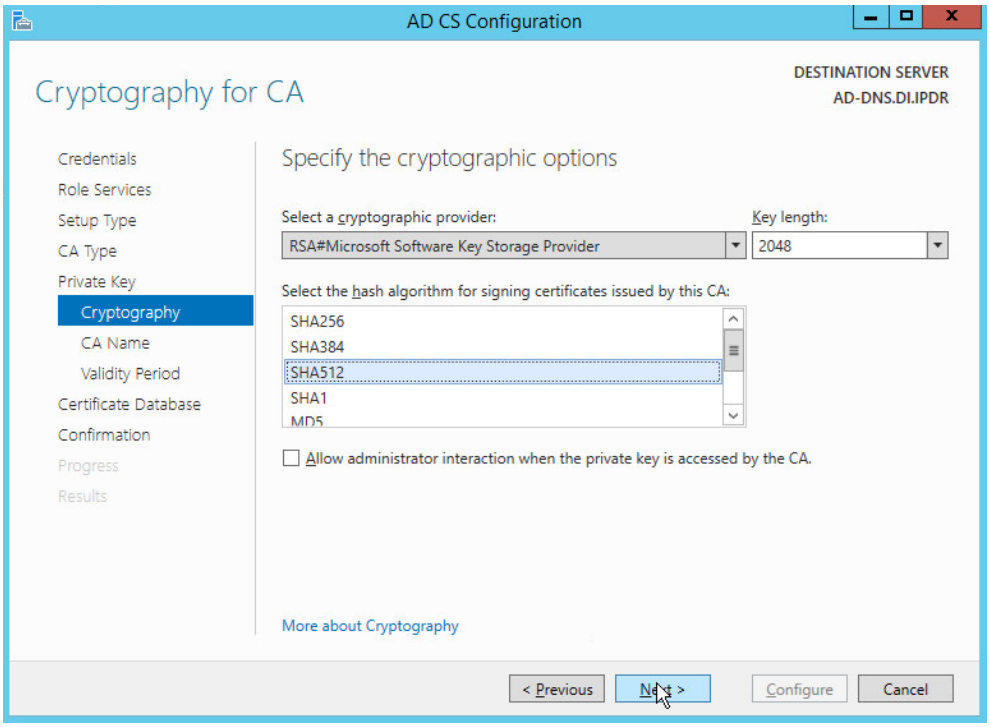
24. Click **Next.**
25. Select **Root CA.**



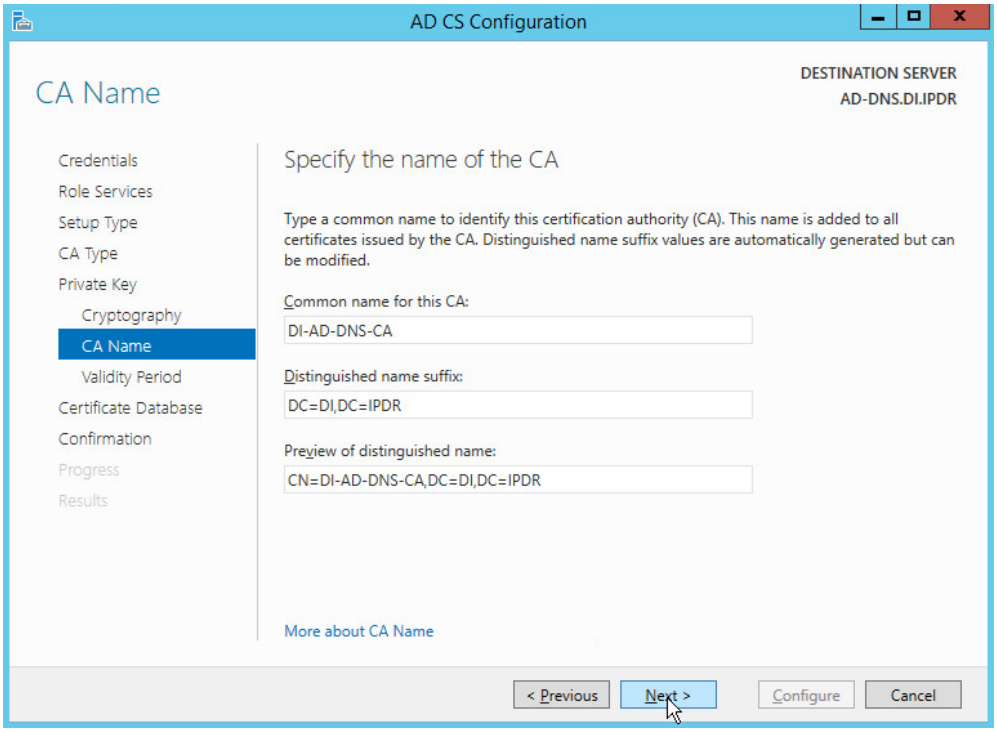
26. Click **Next.**
27. Select **Create a new private key.**



28. Click **Next.**
29. Select **RSA#Microsoft Software Key Storage Provider.**
30. Set the **Key length** to **2048.**
31. Select **SHA512** from the list**.**

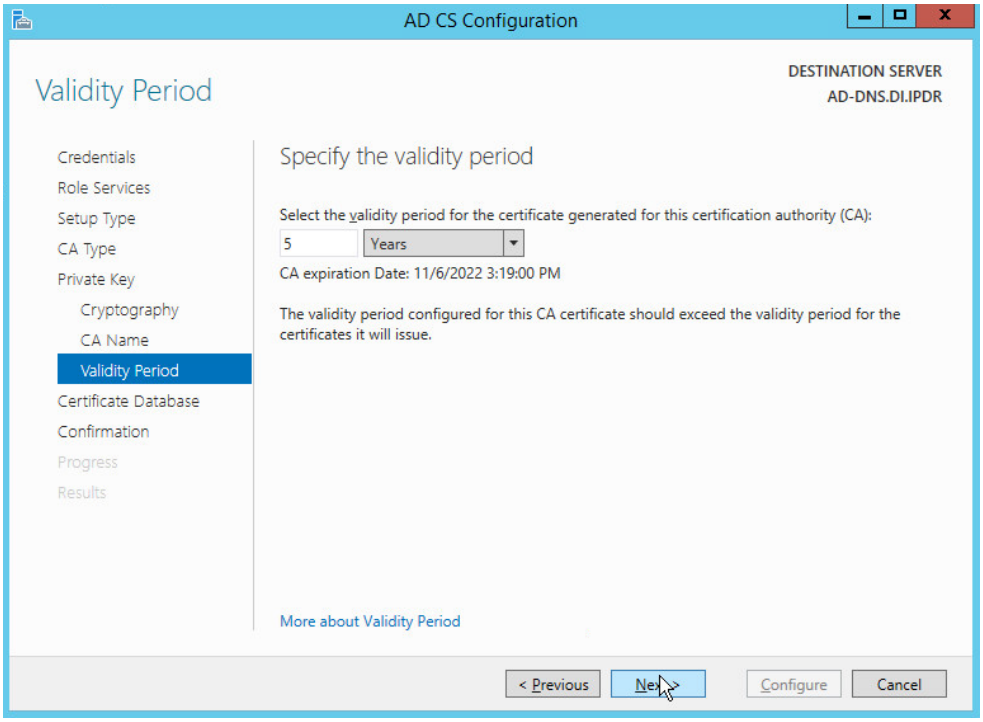


383
384 32. Click **Next.**

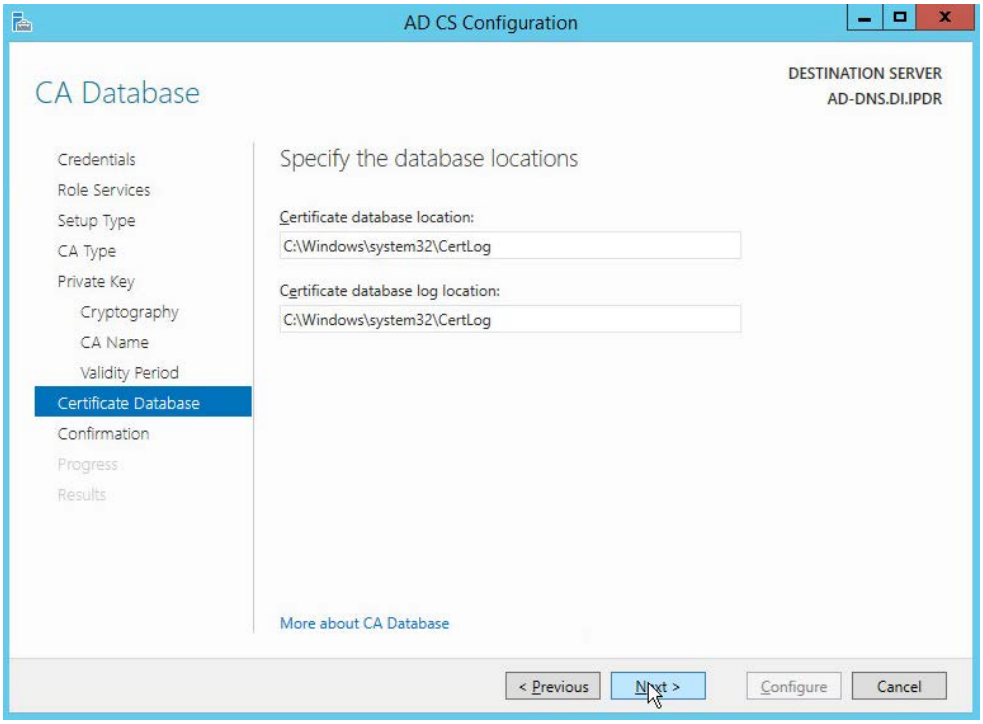


385
386 33. Click **Next.**

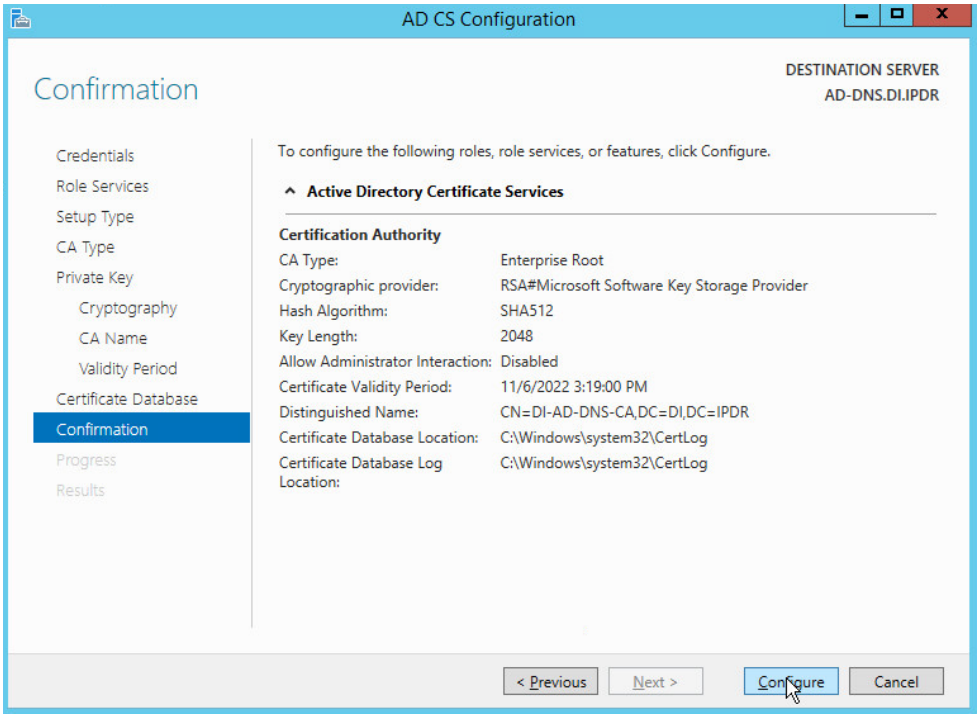
34. Set the validity period of the certificate according to the needs of your organization.



35. Click **Next.**

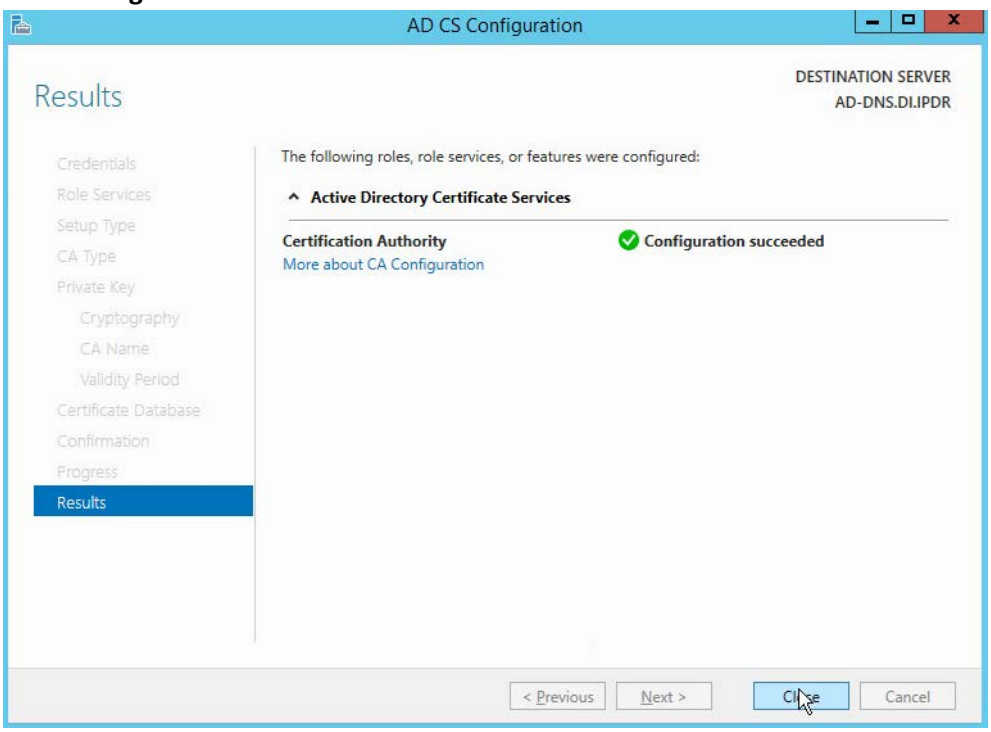


391 36. Click **Next.**



392

393 37. Click **Configure.**

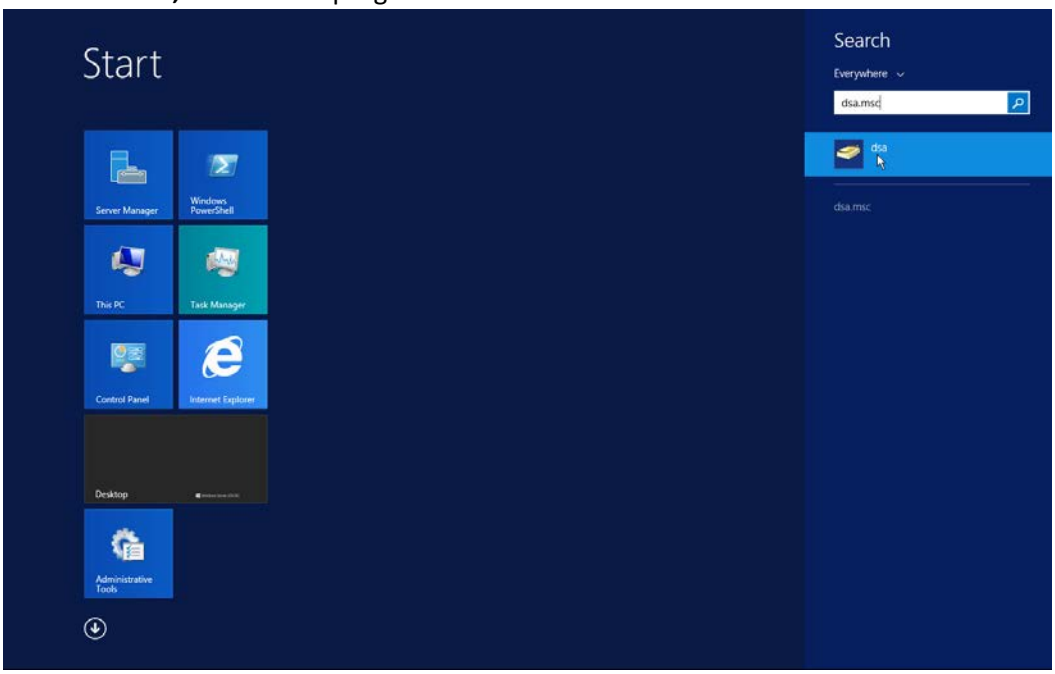


394

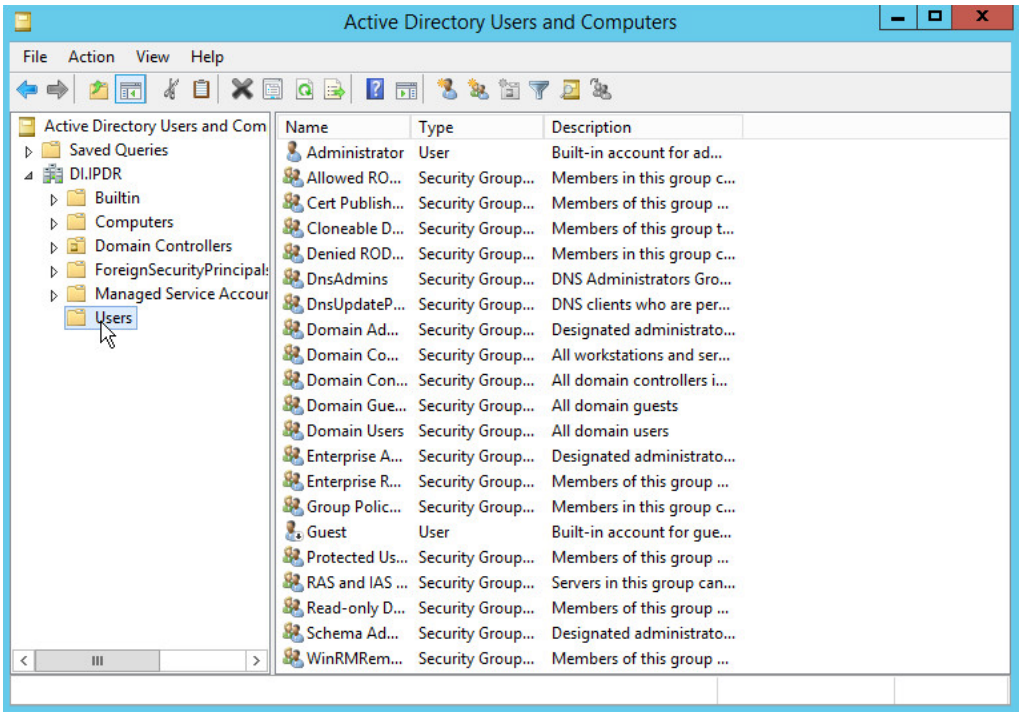
38. Click **Close.**

2.1.3 Configure Account to Add Computers to Domain

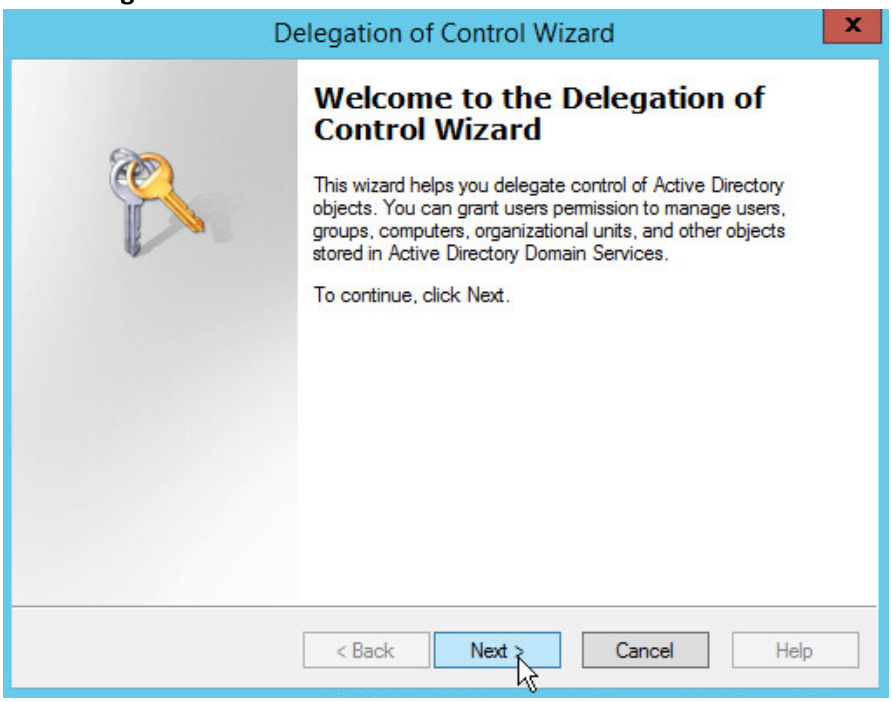
1. Open the **Start** menu.
2. Enter **dsa.msc,** and run the program.



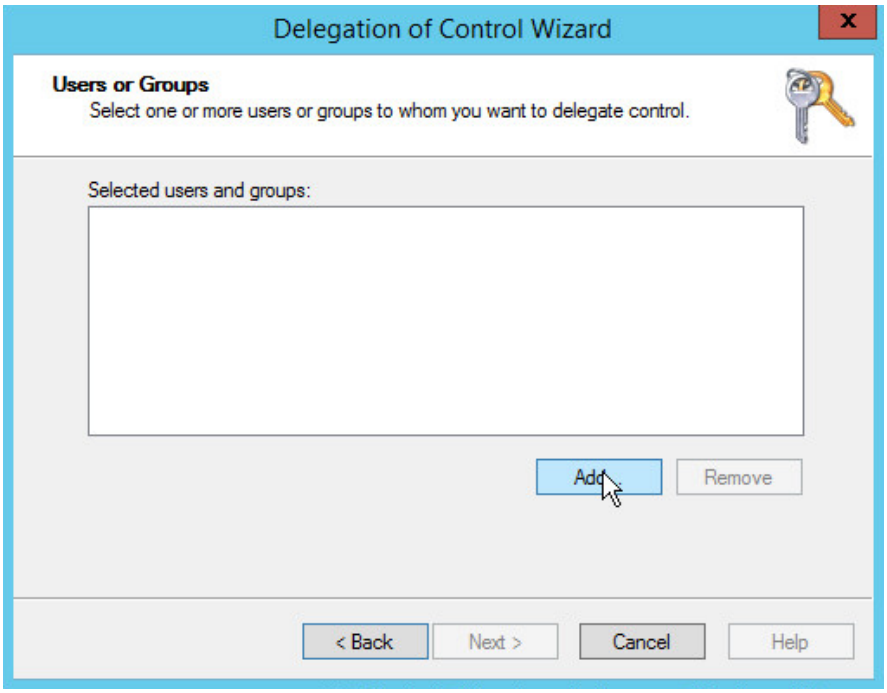
3. Right-click on **Users** in the left panel.



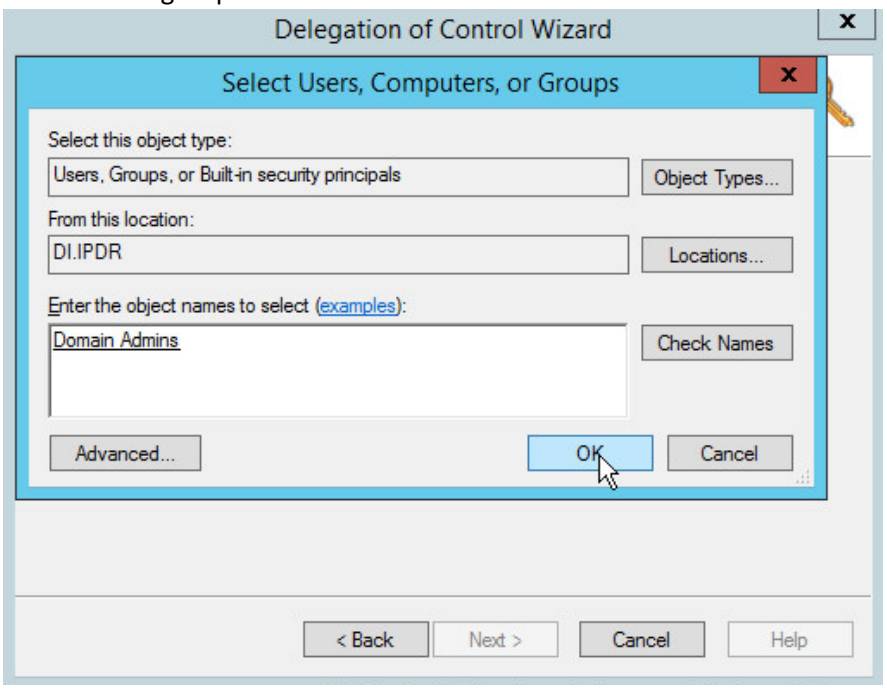
4. Click **Delegate Control.**



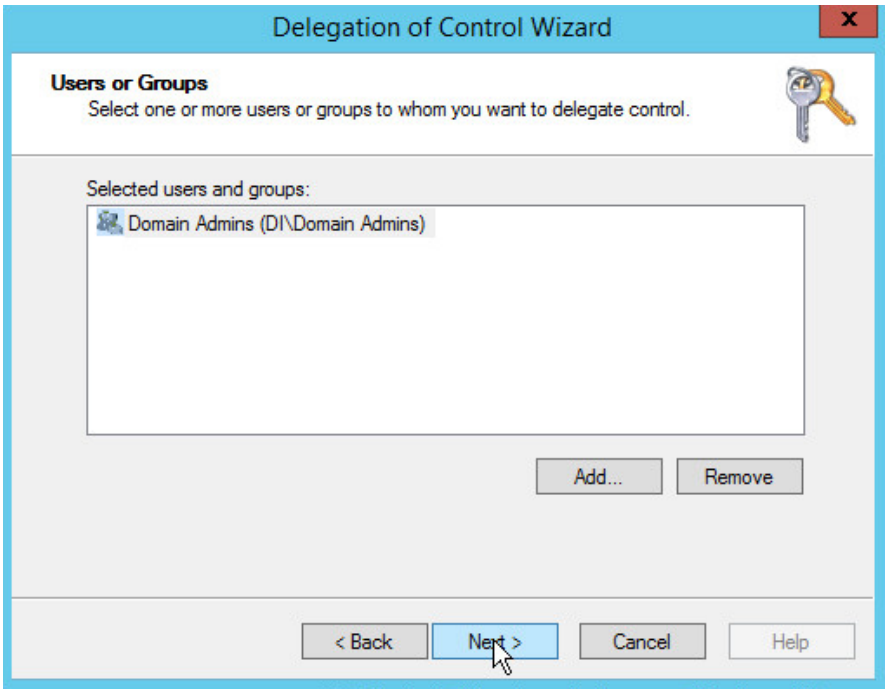
5. Click **Next.**



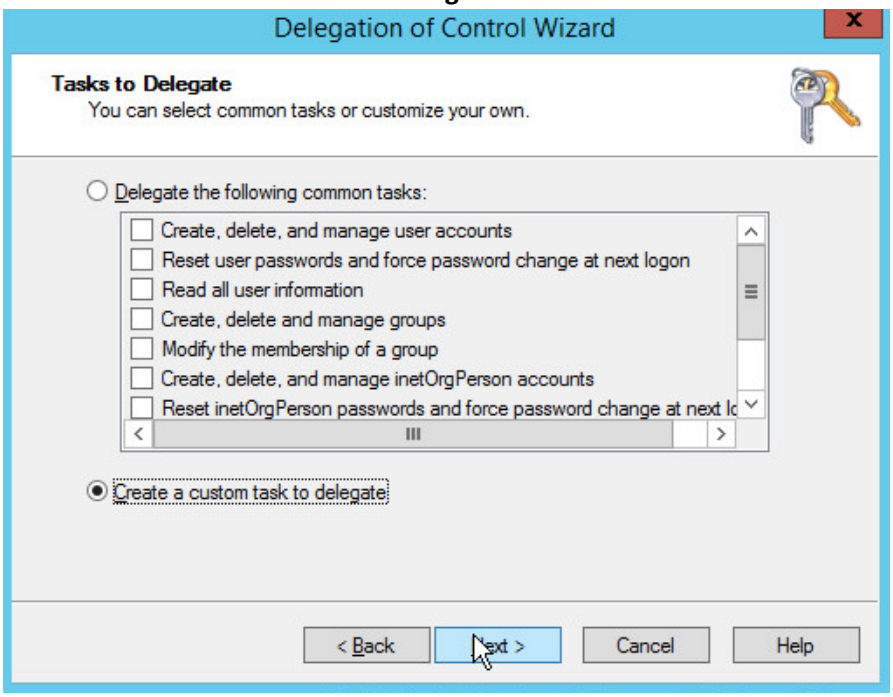
6. Click **Add** to select users or groups.
7. Add users or groups.



8. Click **OK.**

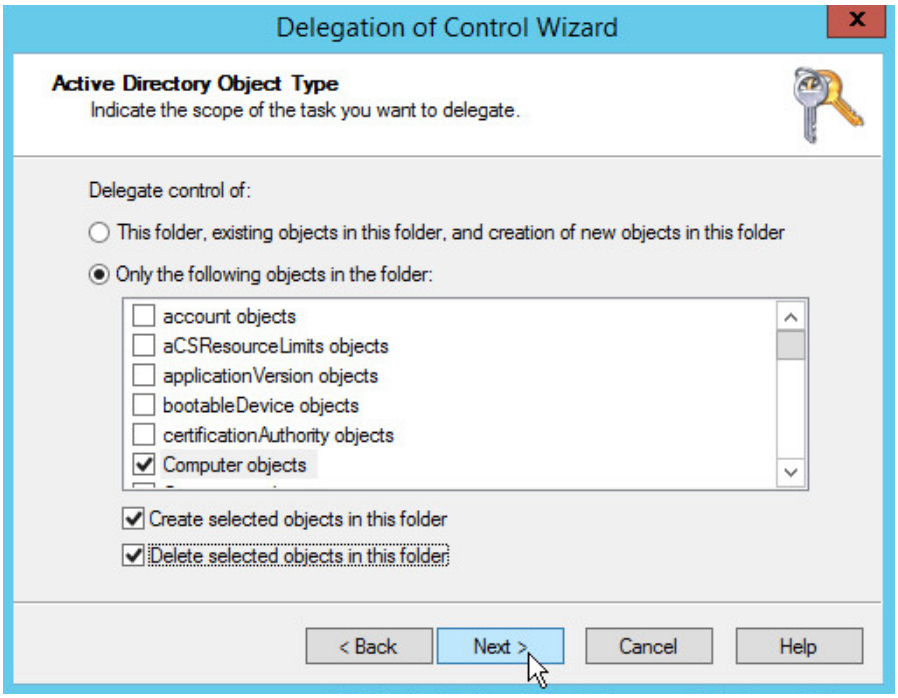


9. Click **Next.**
10. Choose **Create a custom task to delegate.**

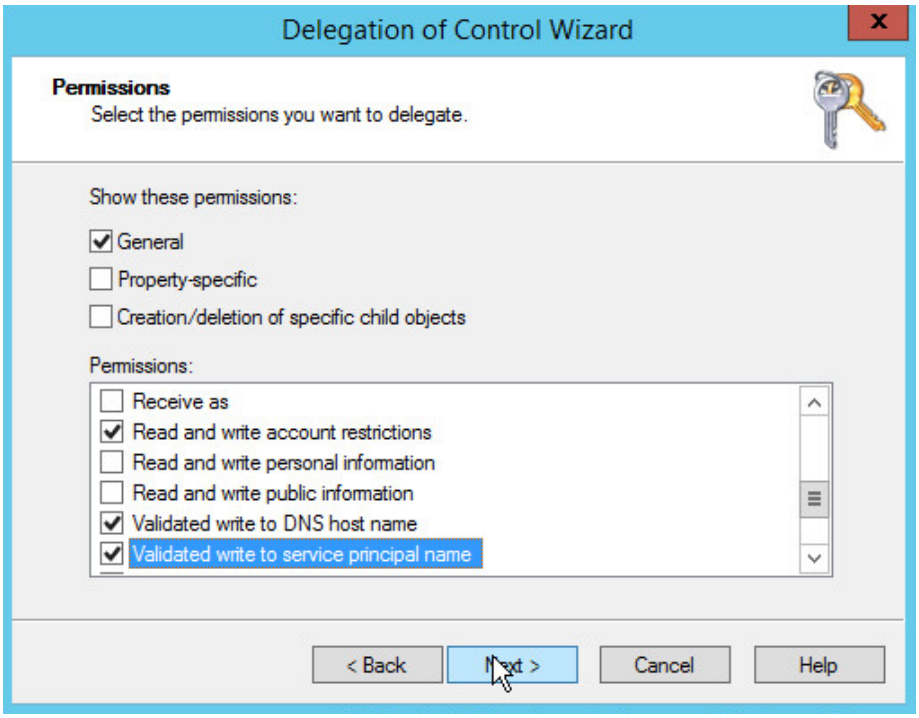


11. Click **Next.**
12. Choose **Only the following objects in the folder.**

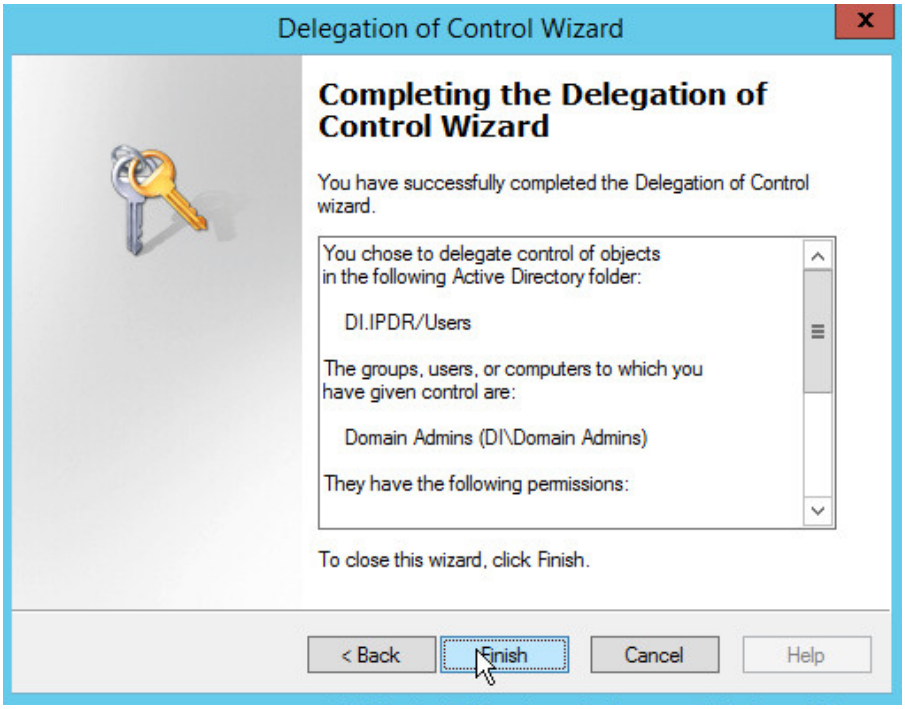
13. Check the box next to **Computer objects.**
14. Check the box next to **Create selected objects in this folder.**
15. Check the box next to **Delete selected objects in this folder.**



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.**



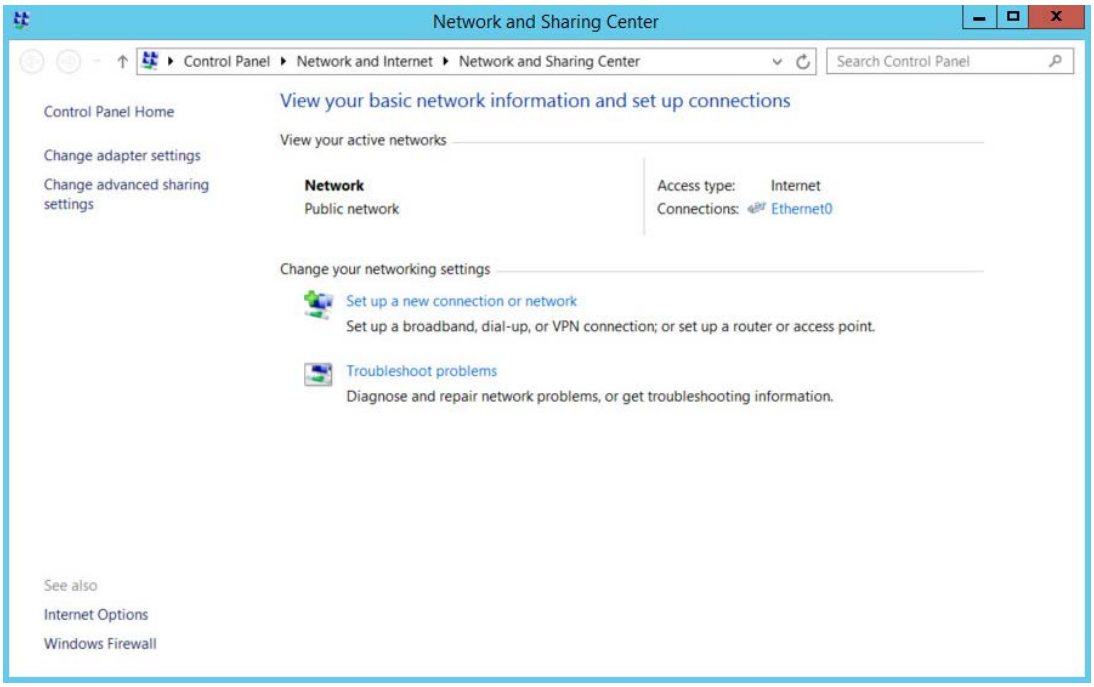
18. Click **Next.**



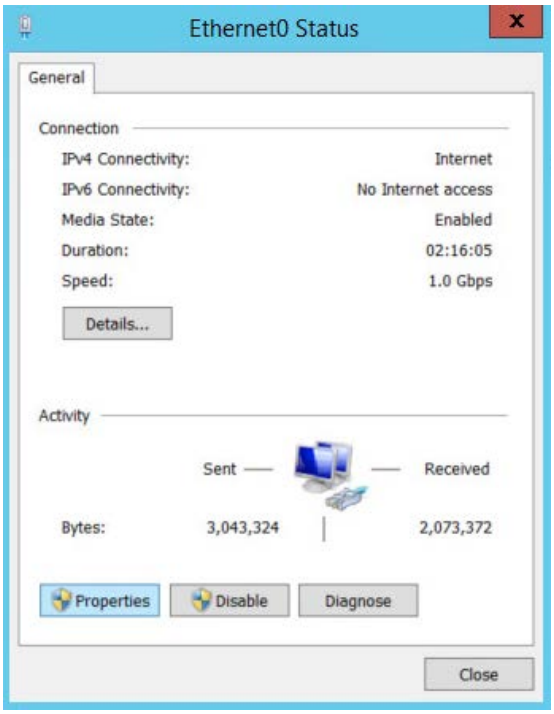
19. Click **Finish.**

2.1.4 Add Machines to the Domain

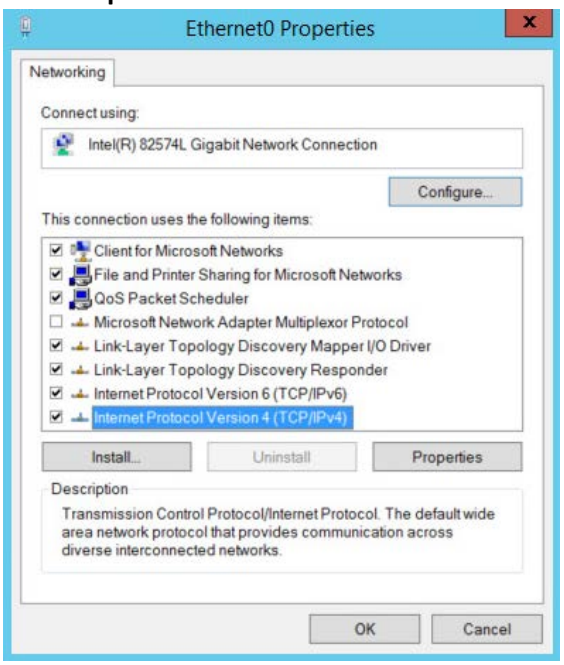
1. Right-click the network icon in the task bar, on a computer that you wish to add to the domain.
2. Click **Open Network and Sharing Center.**



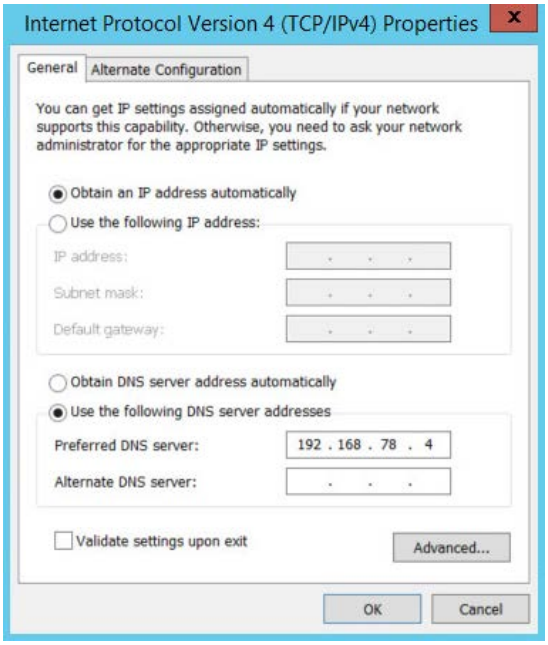
3. Click the name of the internet adapter.



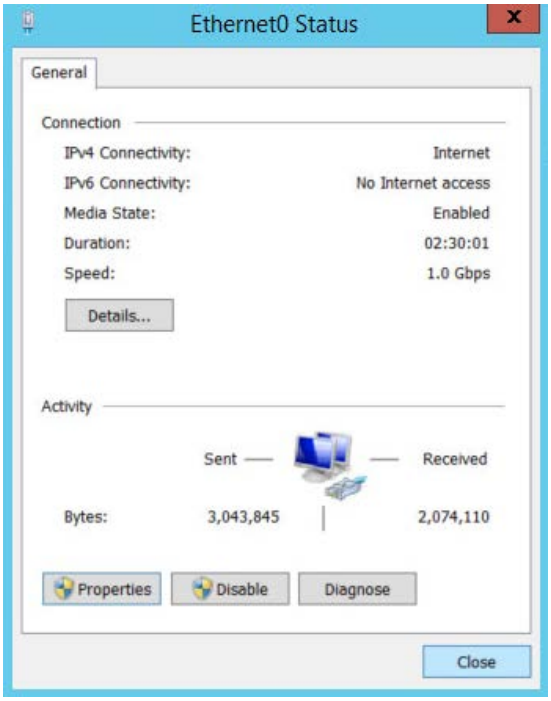
4. Click **Properties.**



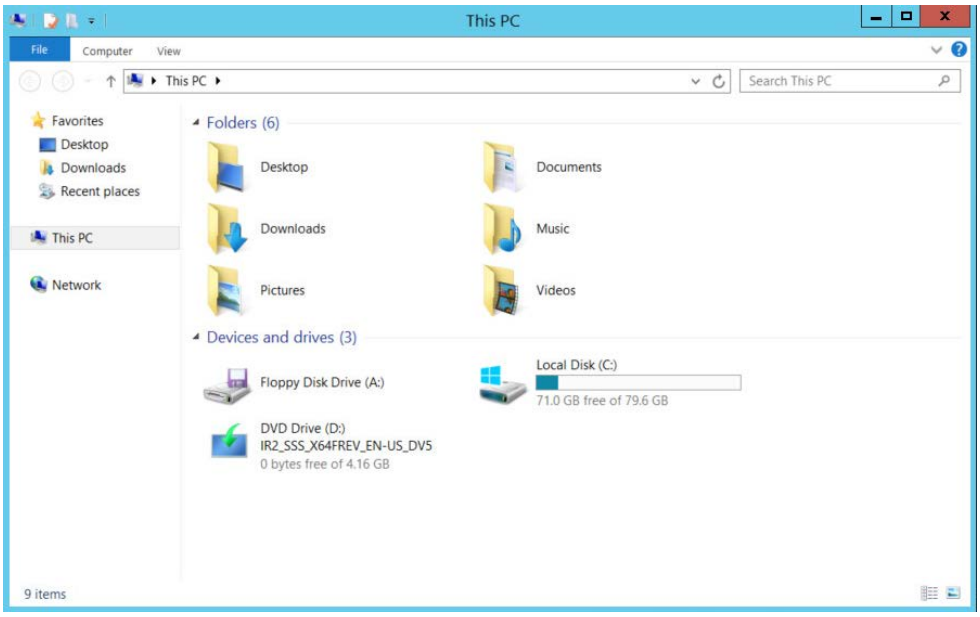
5. Double-click **Internet Protocol Version 4 (TCP/IPv4).**
6. Select **Use the following DNS server addresses.**
7. Enter the **IP address** of the DNS server.



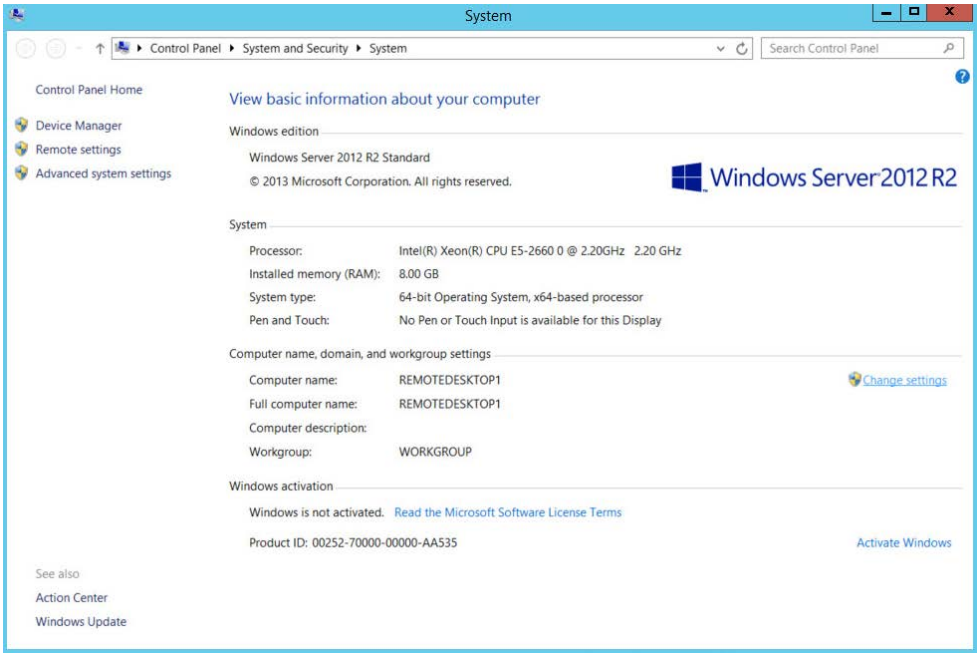
8. Click **OK.**
9. Click **OK.**



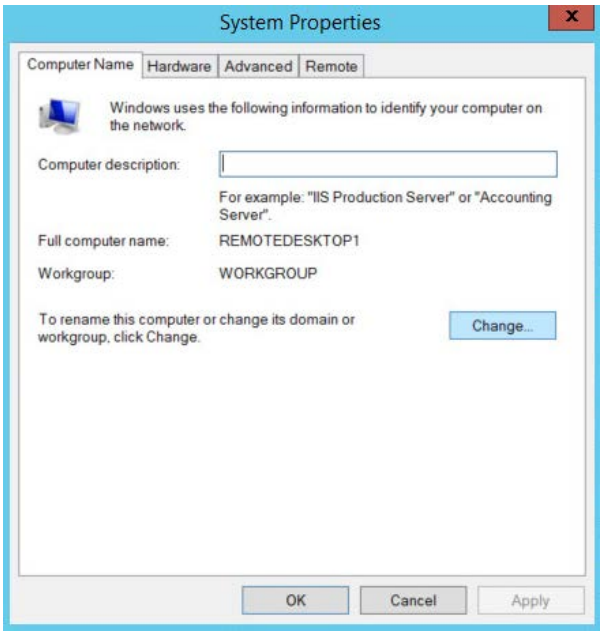
10. Click **Close.**
11. Navigate to **This PC.**



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

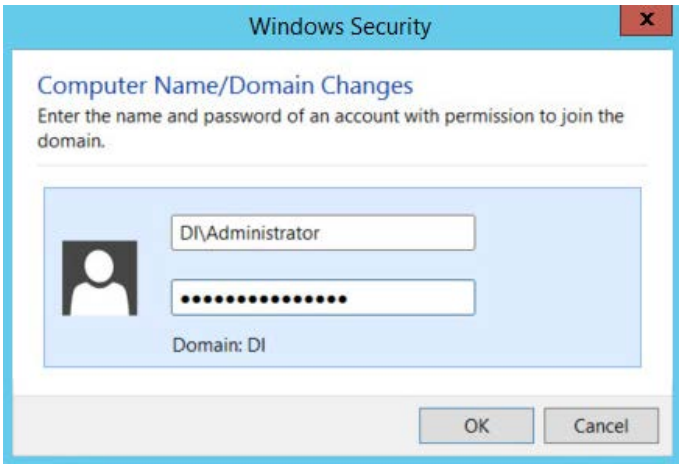


13. Click **Change Settings.**

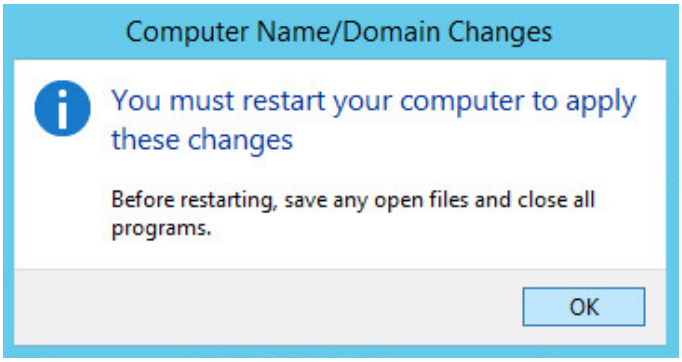


14. Click **Change.**
15. Select **Domain.**
16. Enter the domain.

17. Click **OK.**
18. Enter the name and password of an account with privileges to add computers to the domain.



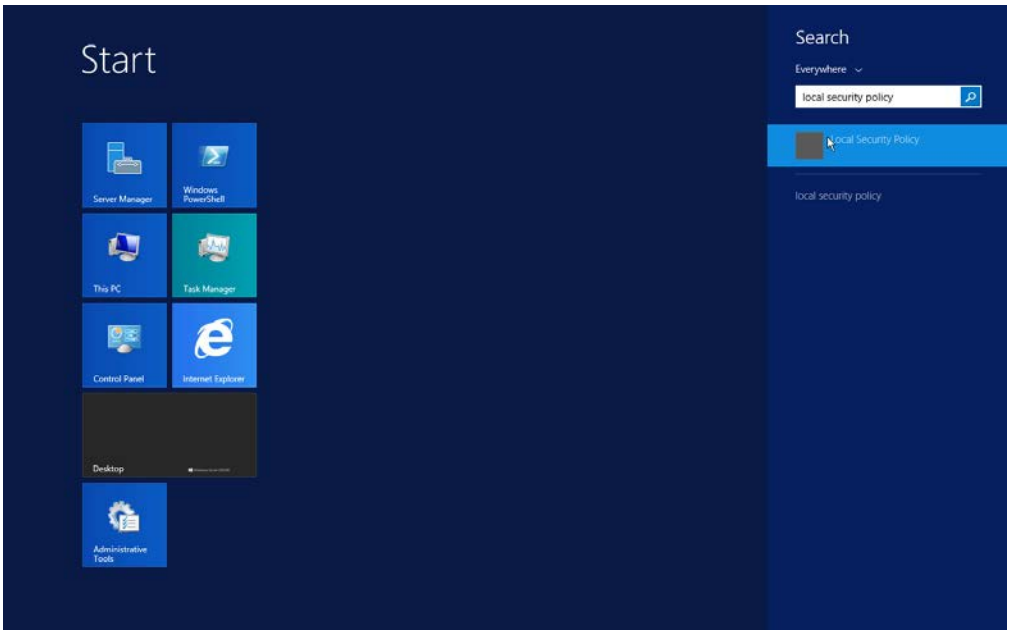
19. Click **OK.**



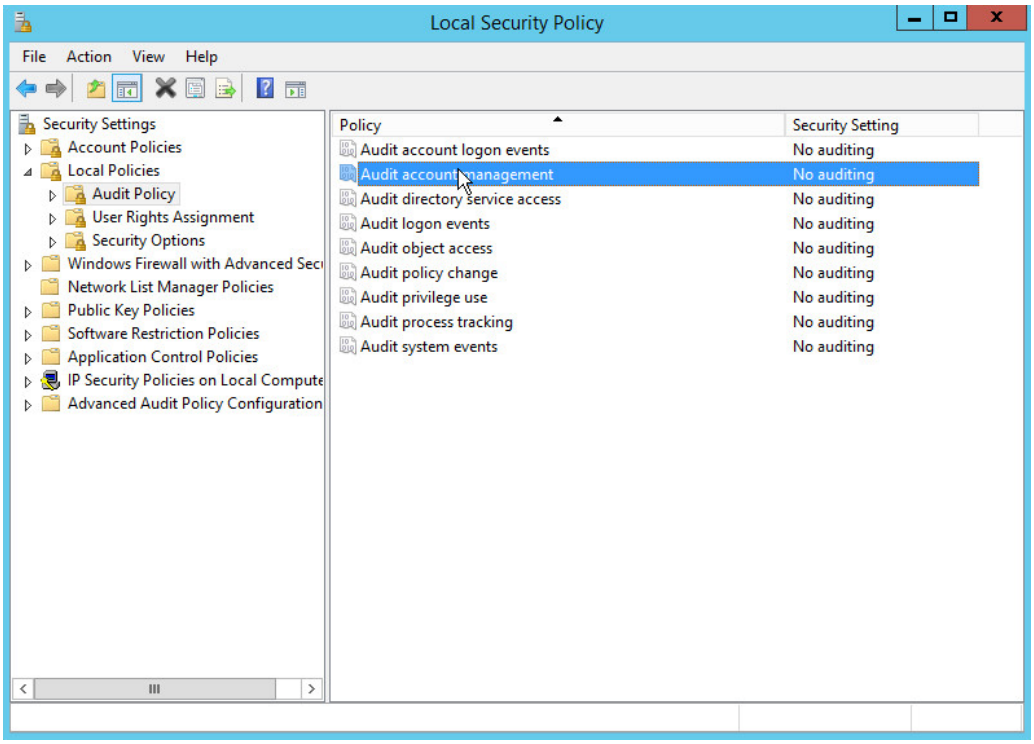
20. Click **OK** when prompted to restart the computer**.**

2.1.5 Configure Active Directory to Audit Account Activity

1. Open the **Start** Menu.

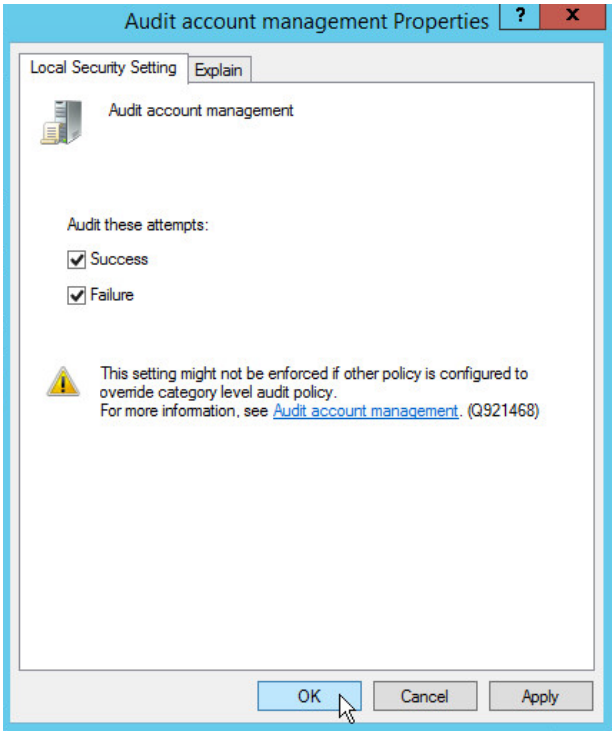


2. Enter Local Security Policy in the search bar, and open the program.
3. Navigate to **Local Policies > Audit Policy.**
4. Right-click **Audit account management.**



5. Click **Properties.**

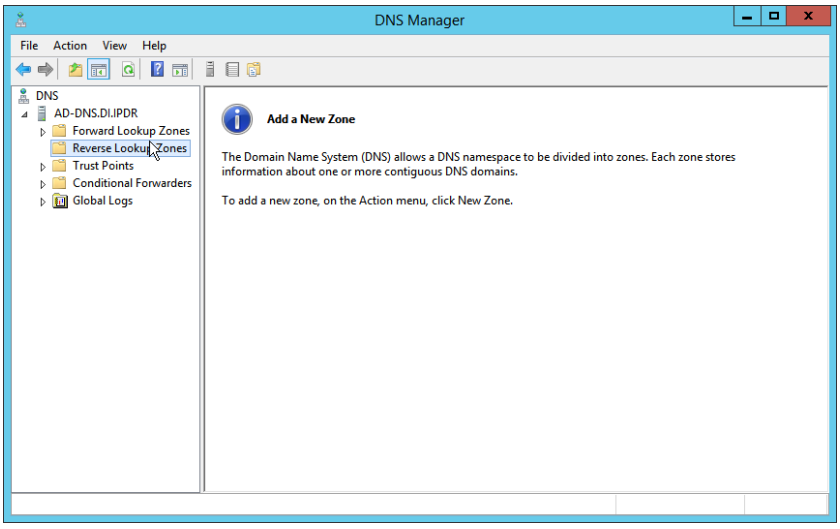
6. Check the boxes next to **Success** and **Failure.**



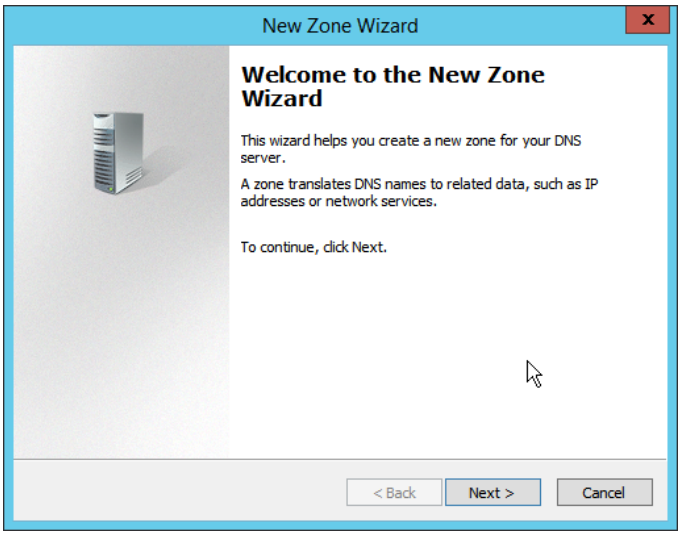
7. Click **OK.**

2.1.6 Configure Reverse Lookup Zones

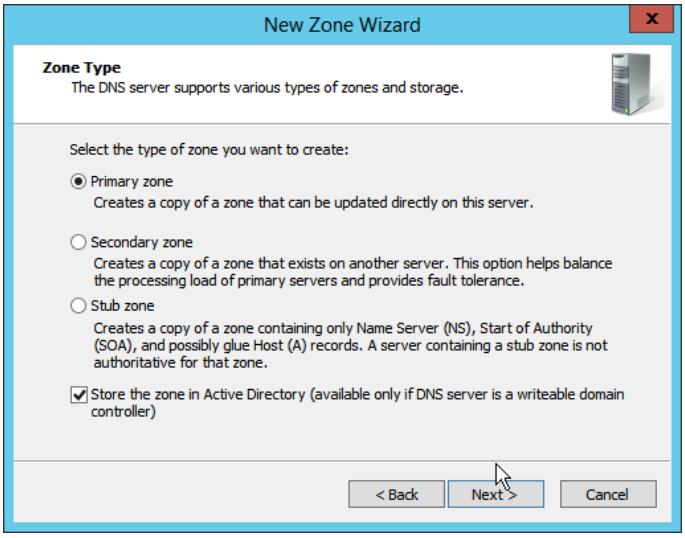
1. Open **DNS Manager** by right-clicking the DNS server in **Server Manager.**
2. Click **Reverse Lookup Zones.**



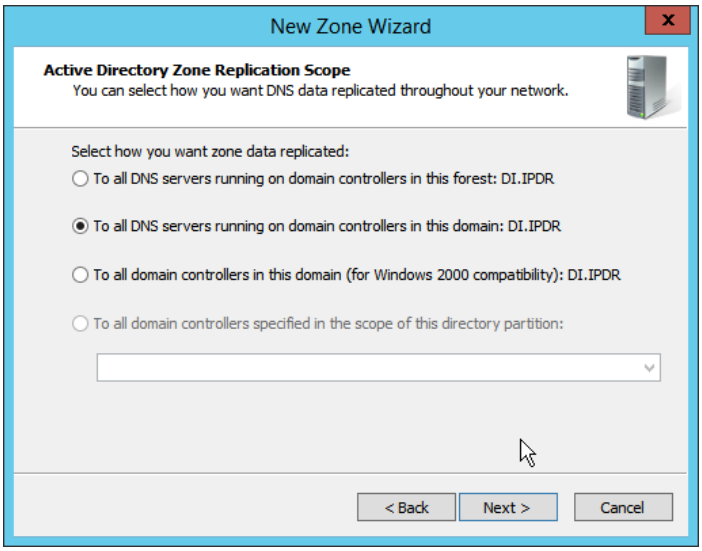
3. Click **Action > New Zone.**



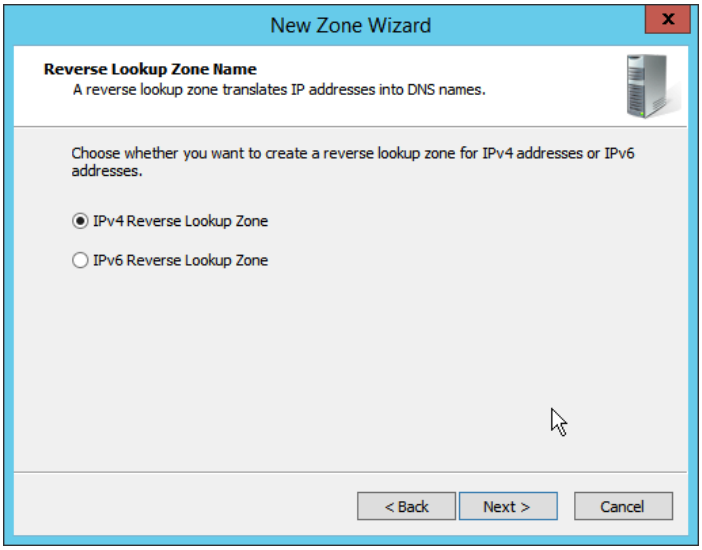
4. Click **Next.**



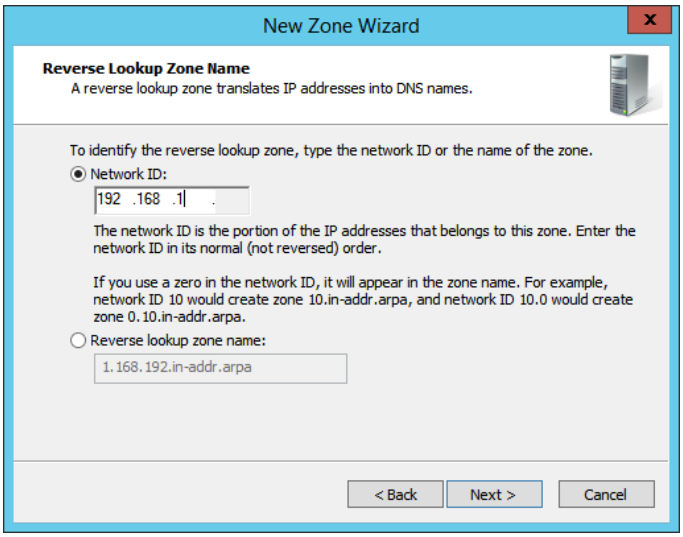
5. Click **Next.**



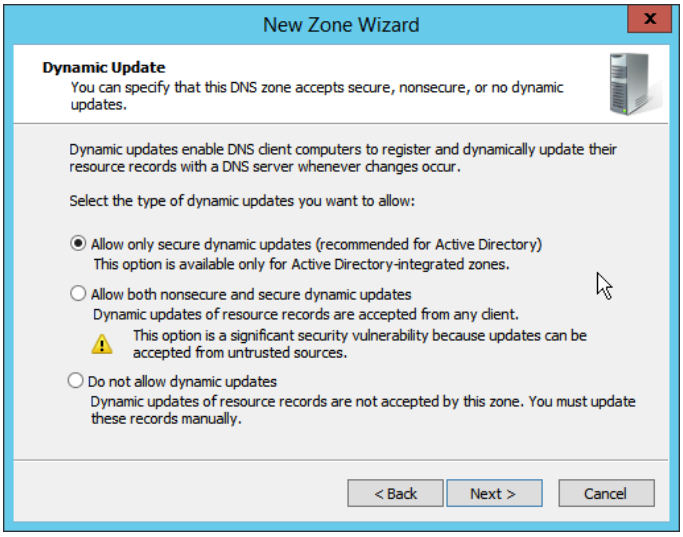
6. Click **Next.**



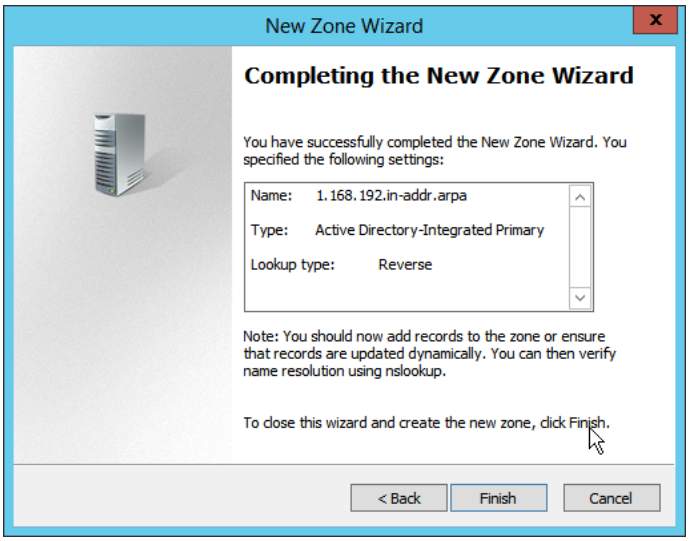
7. Click **Next.**
8. Enter the first three parts of the IP address of the AD/DNS server (for example, 192.168.1).



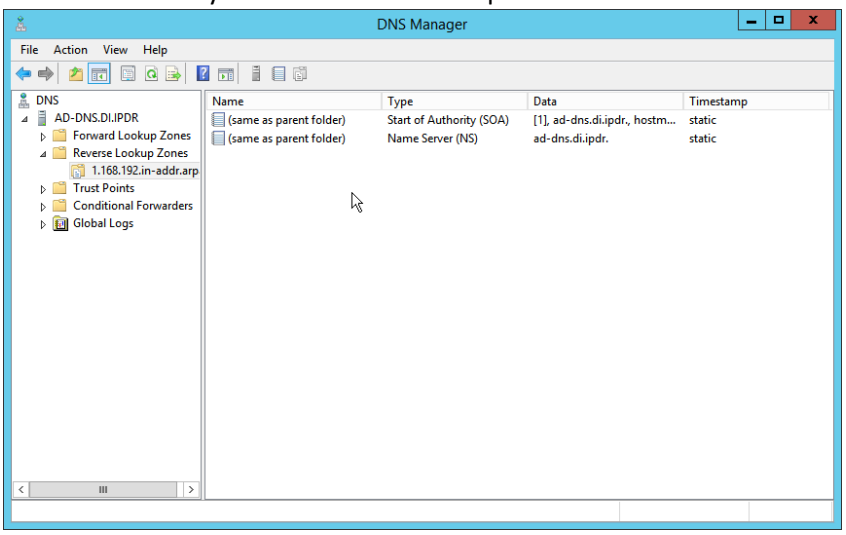
9. Click **Next.**



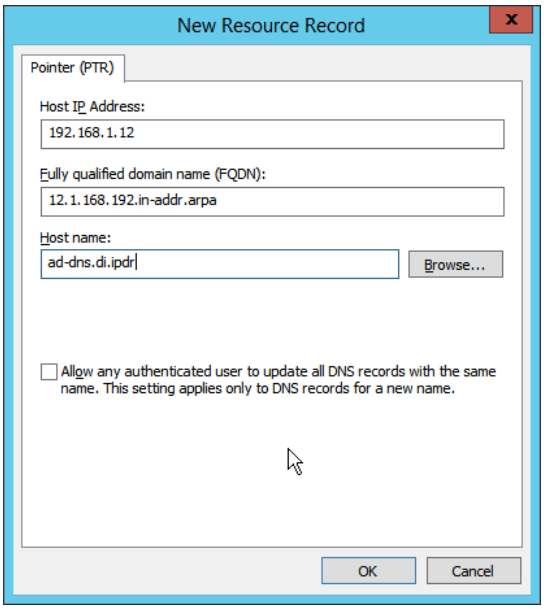
10. Click **Next.**



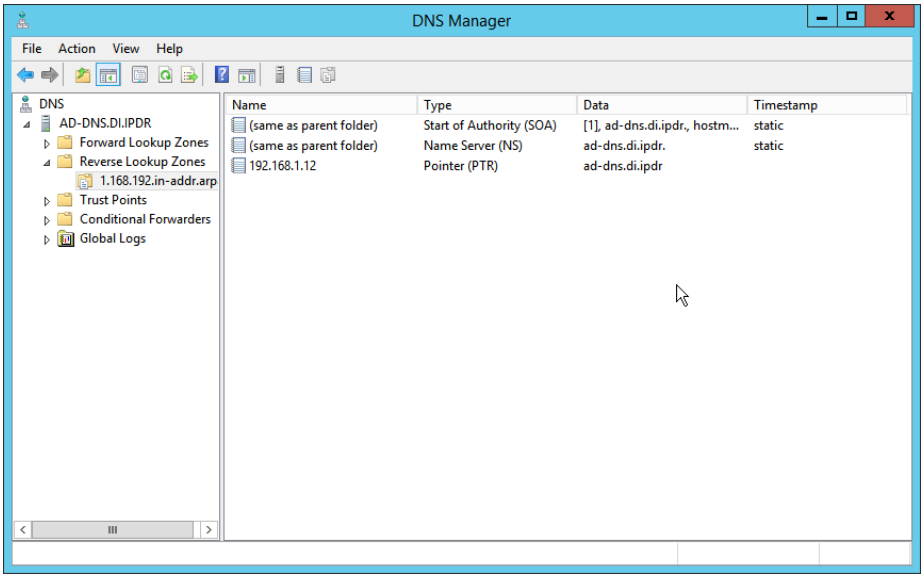
11. Click **Finish.**
12. Click on the newly created reverse lookup zone.



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.**

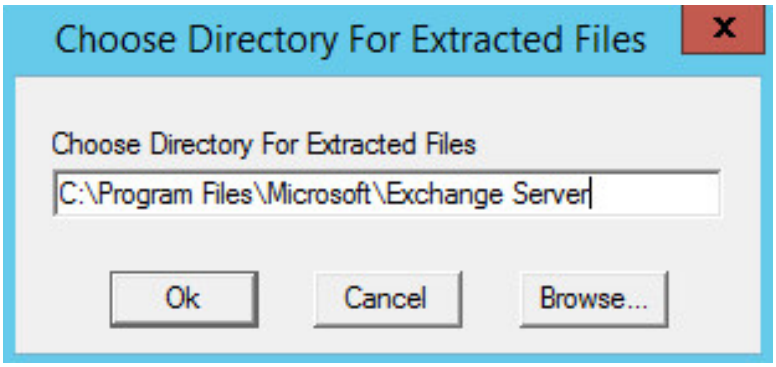


2.2 Microsoft Exchange Server

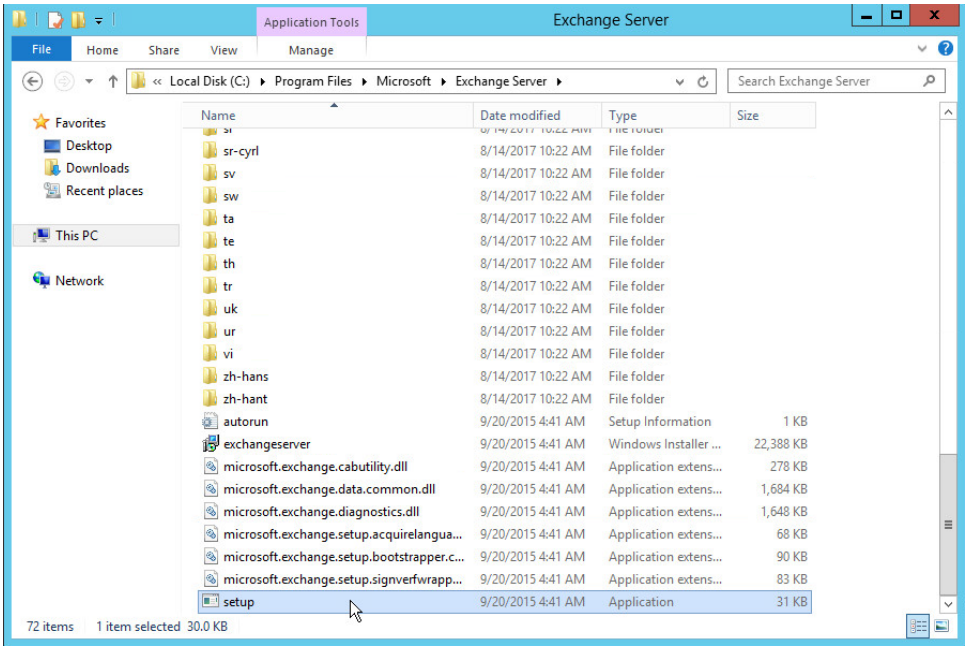
As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

2.2.1 Install Microsoft Exchange

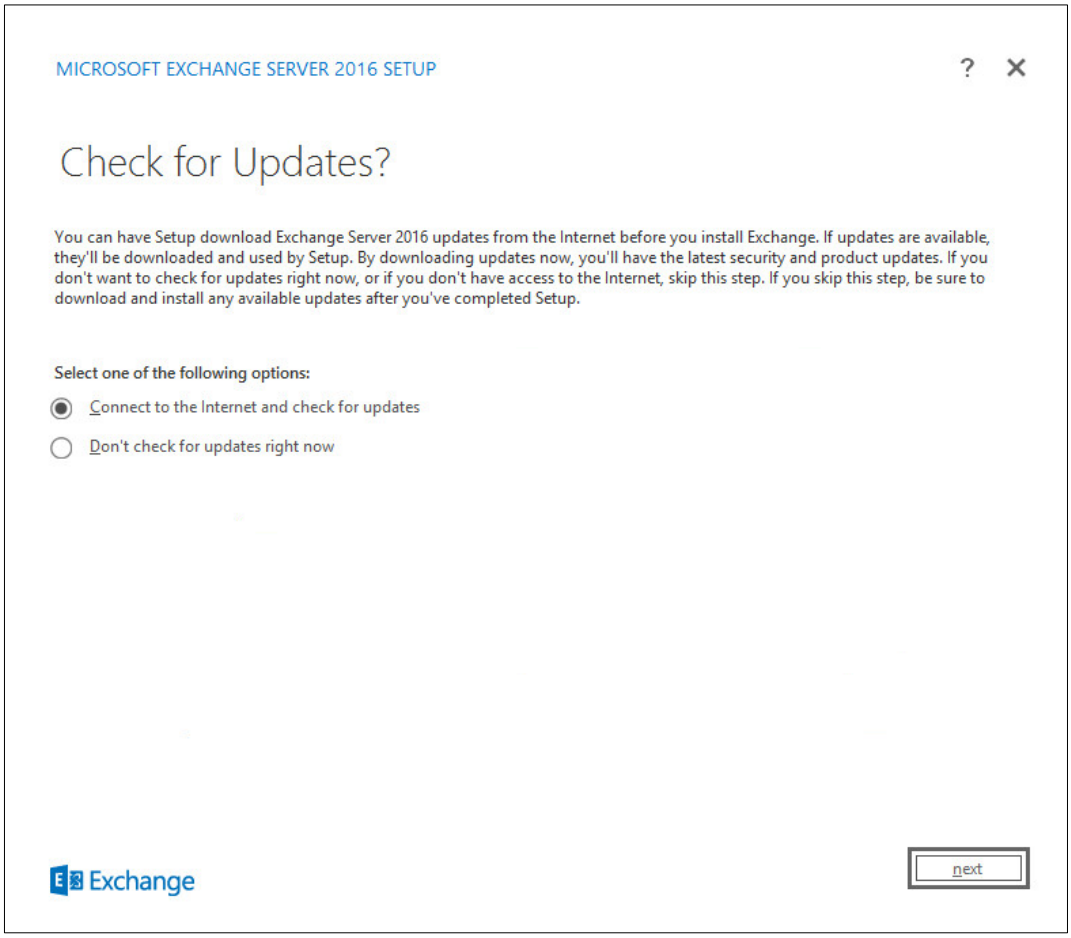
1. Run **Exchange2016-x64.exe.**
2. Choose the directory for the extracted files.



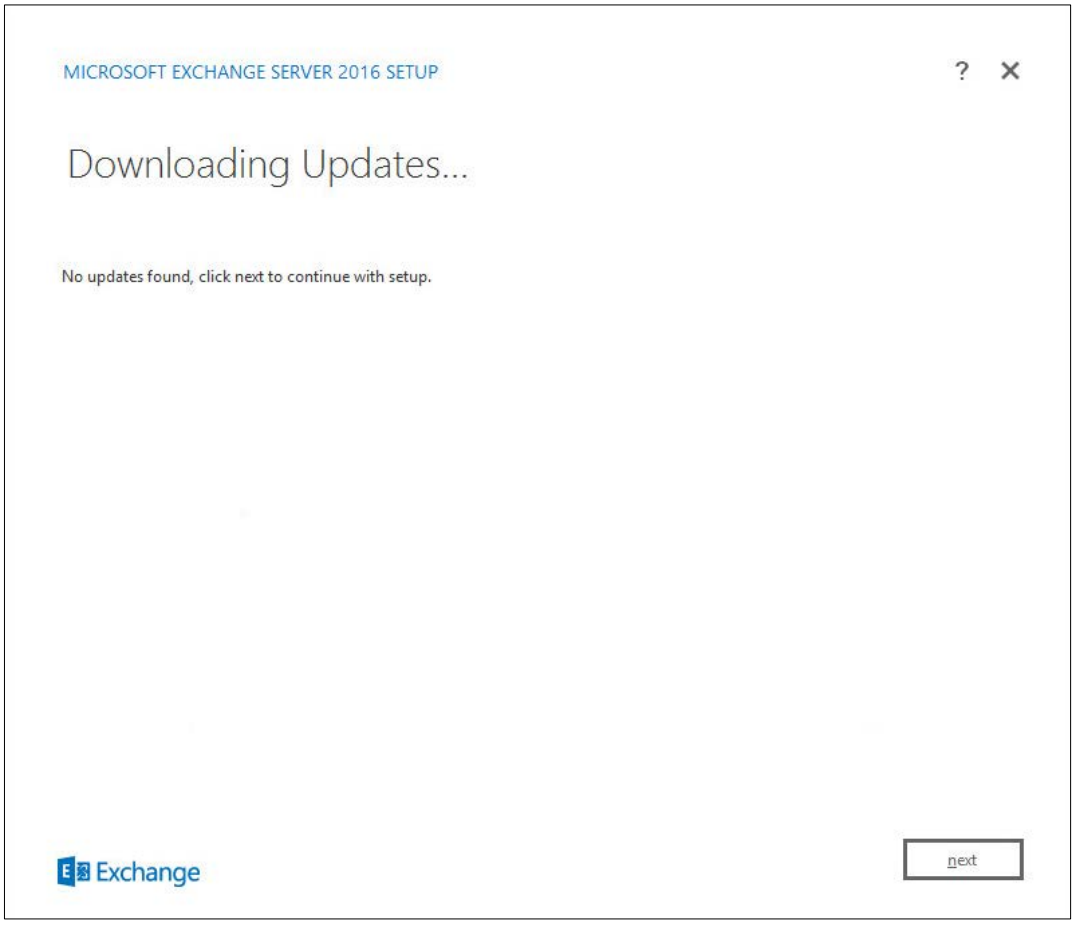
3. Click **OK.**



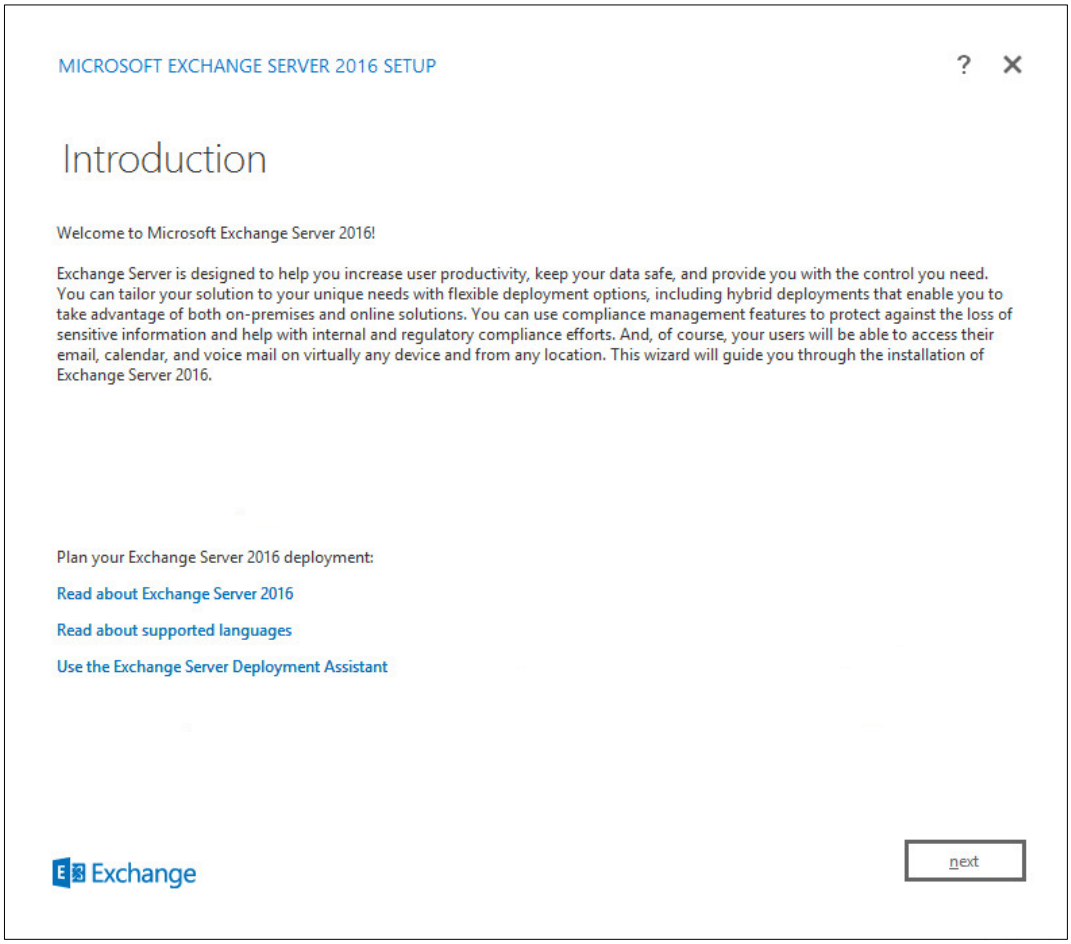
4. Enter the directory and run **setup.exe.**
5. Select **Connect to the Internet and check for updates.**



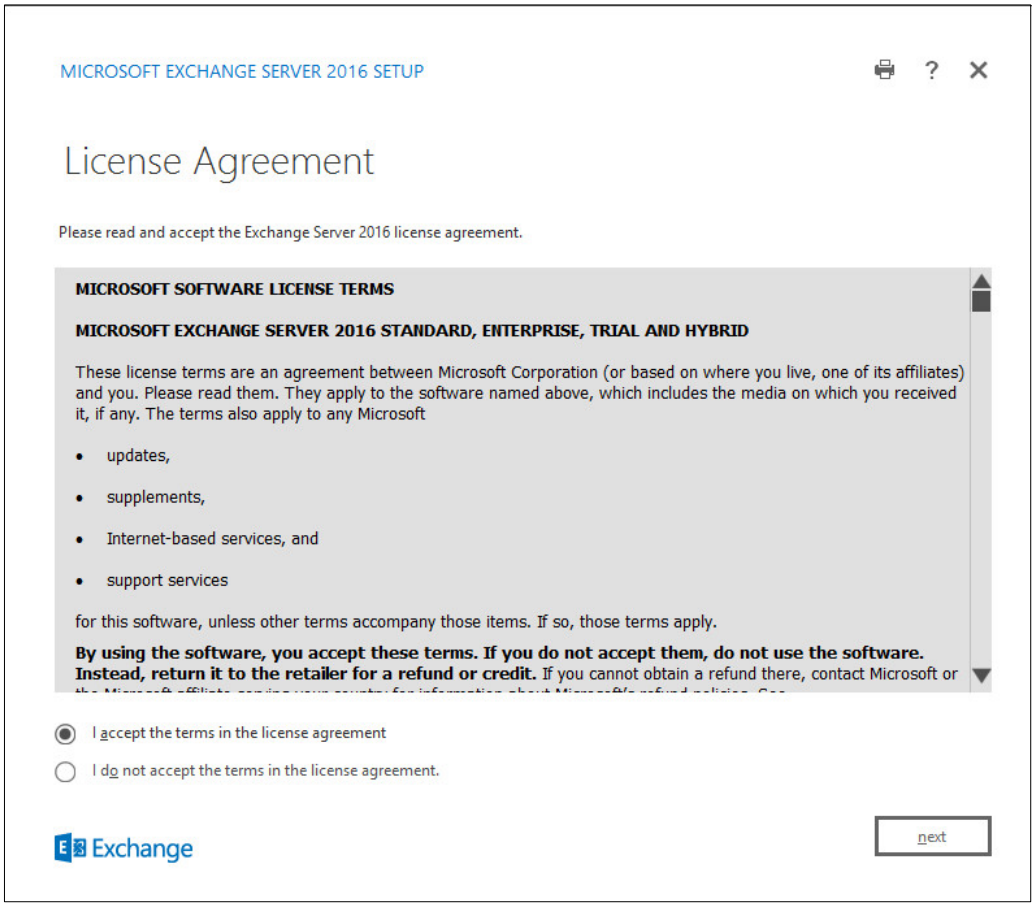
6. Click **Next.**
7. Wait for the check to finish.



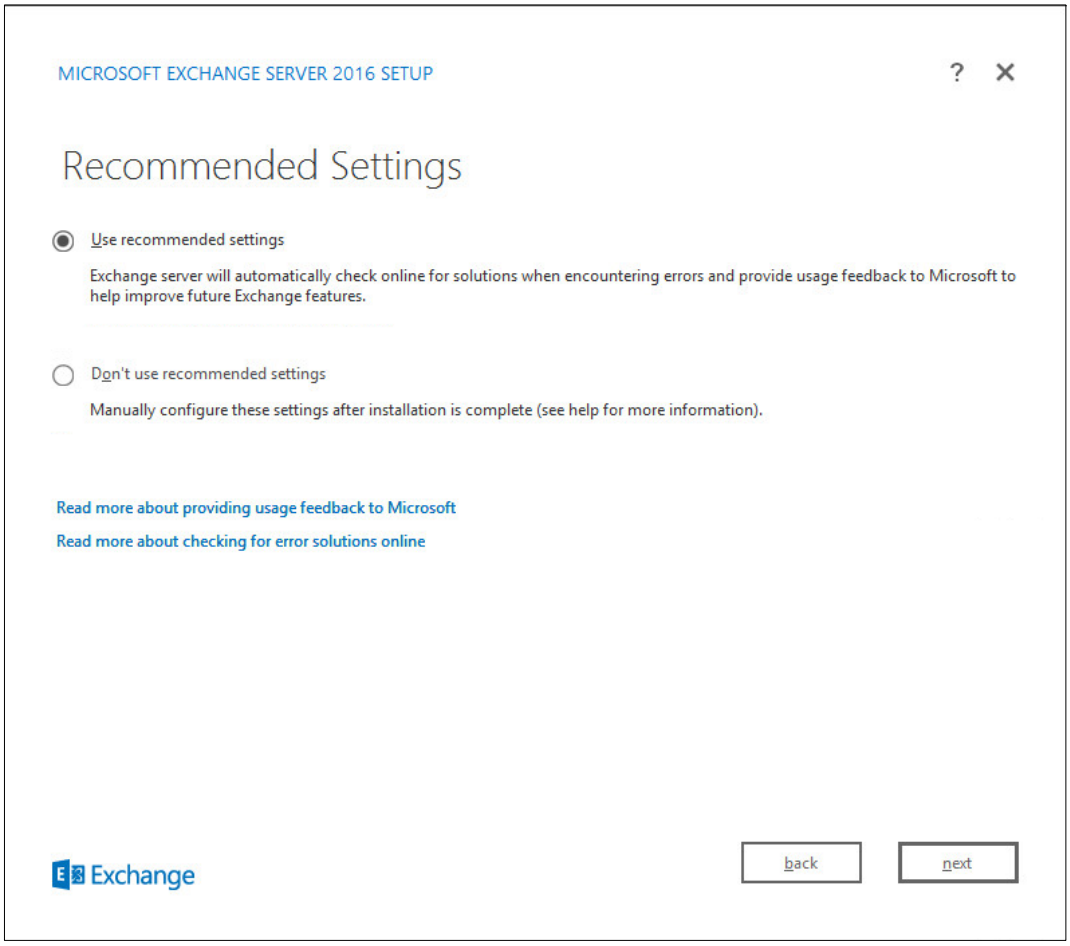
8. Click **Next.**
9. Wait for the copying to finish.



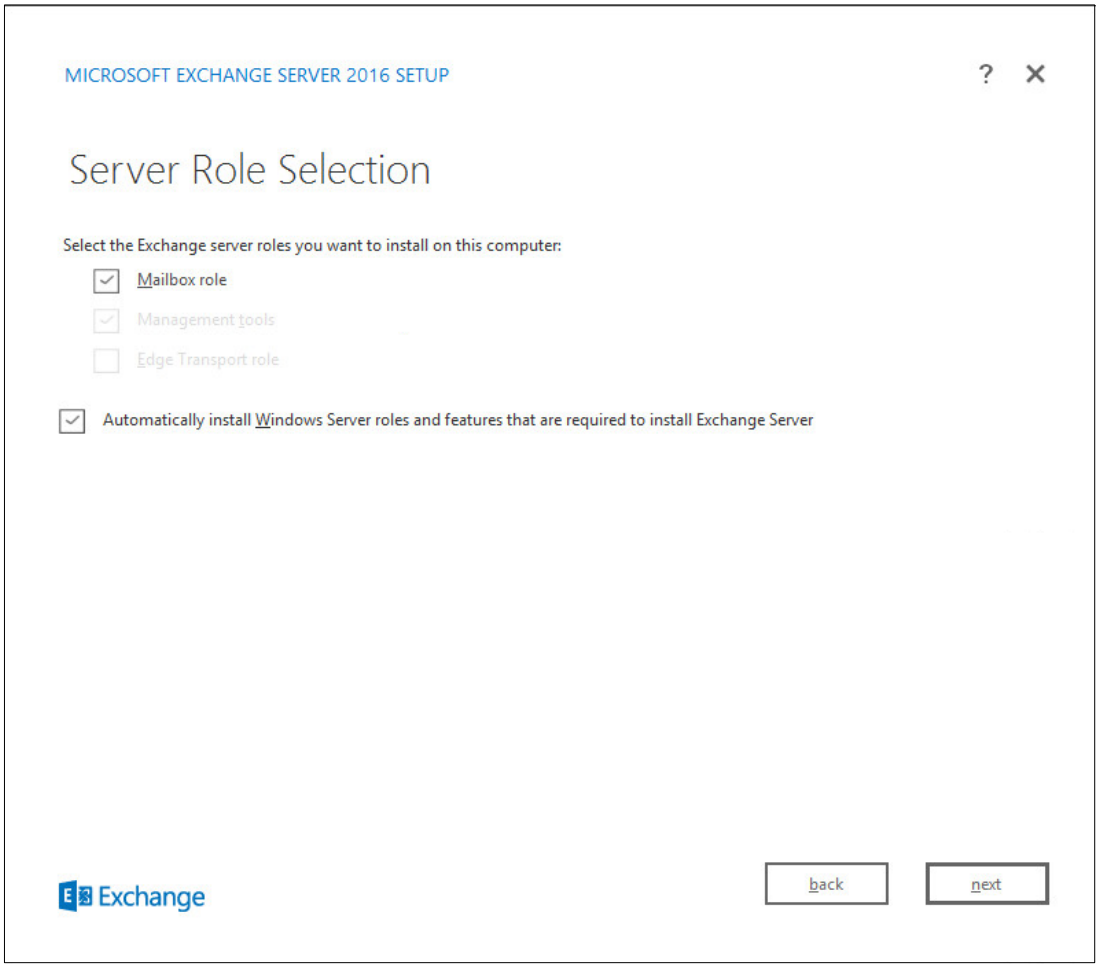
10. Click **Next.**
11. Click **I accept the terms in the license agreement.**



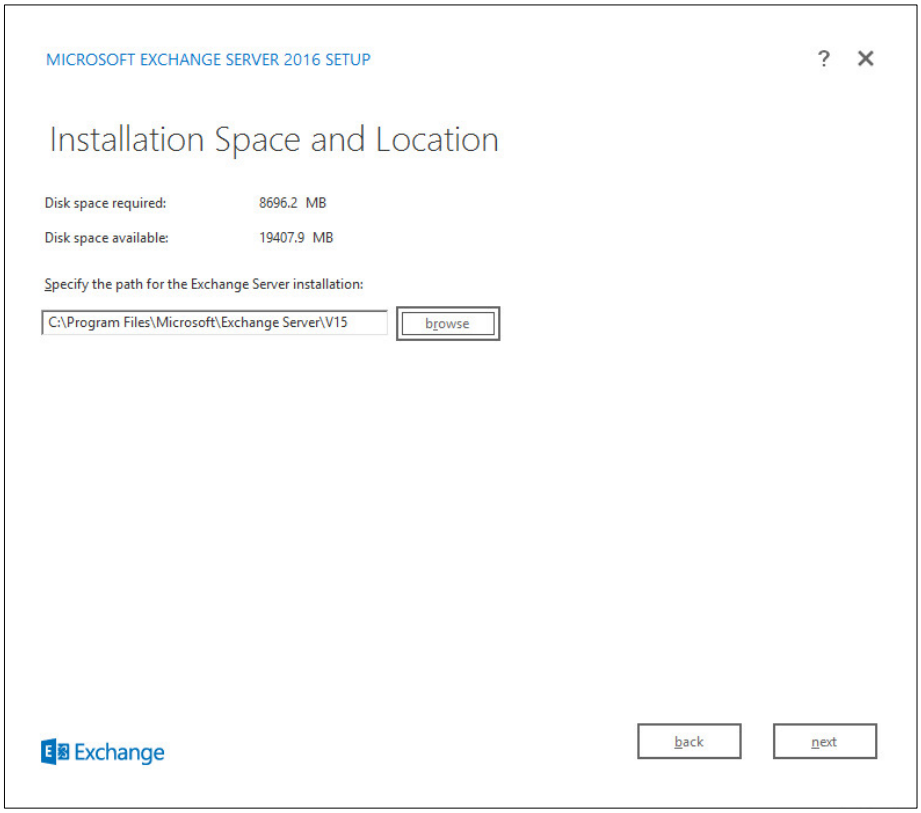
12. Click **Next.**
13. Click **Use Recommended Settings.**



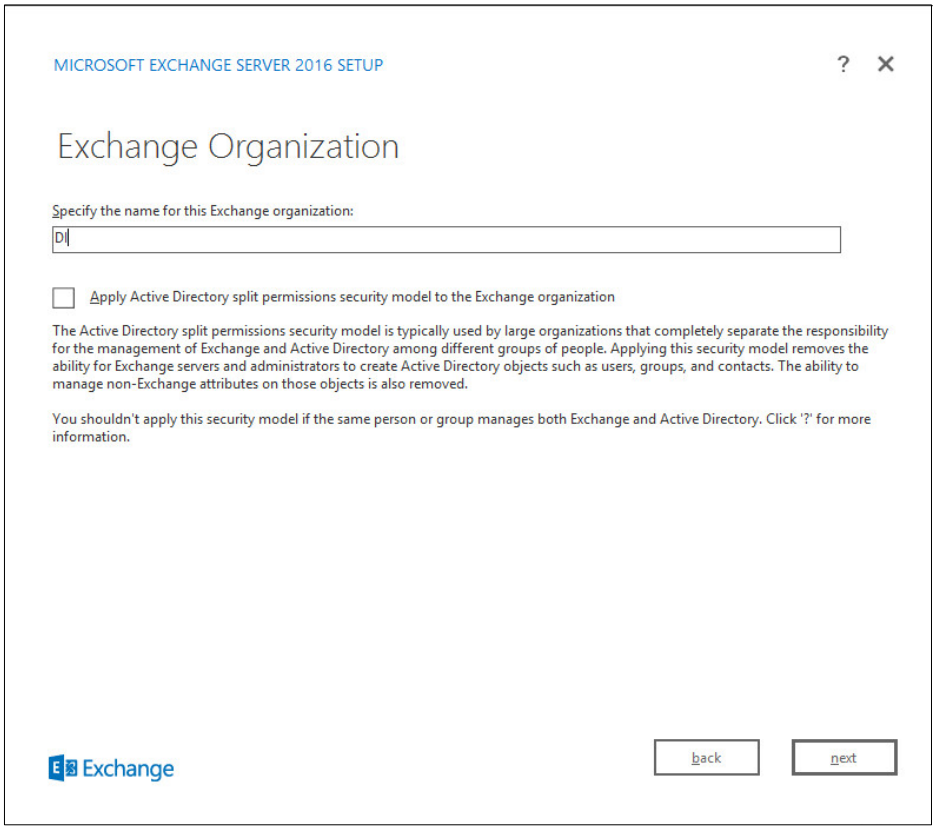
14. Click **Next.**
15. Check **Mailbox role.**
16. Check **Automatically install Windows Server roles and features that are required to install Exchange Server.**



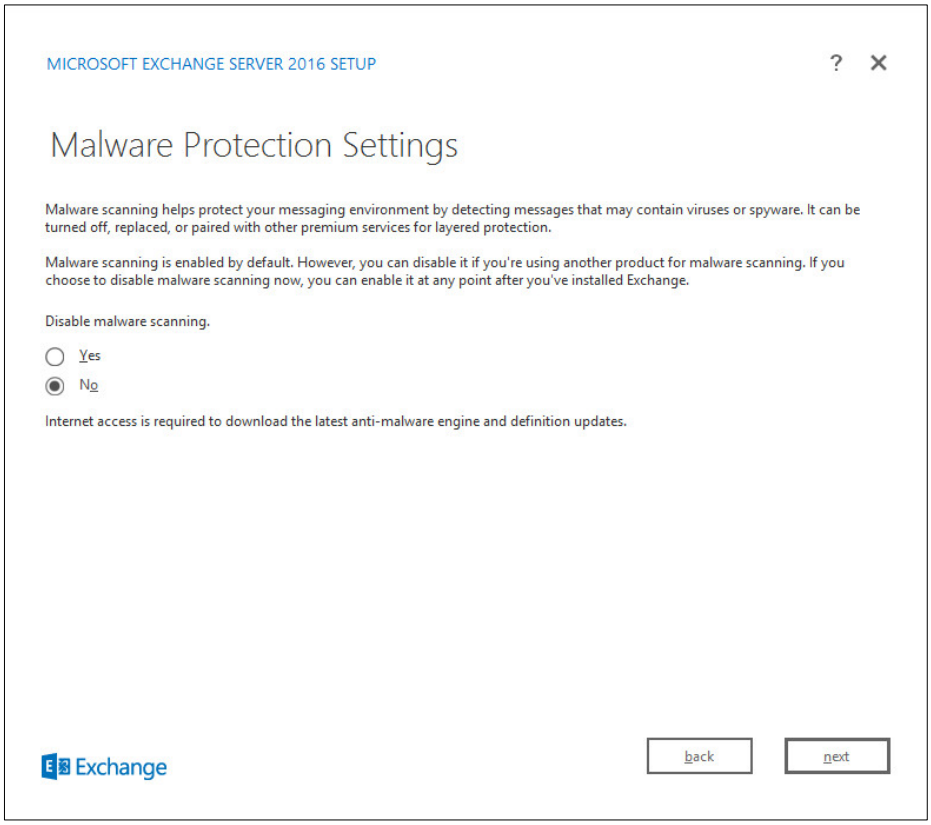
17. Click **Next.**
18. Specify the installation path for MS Exchange.



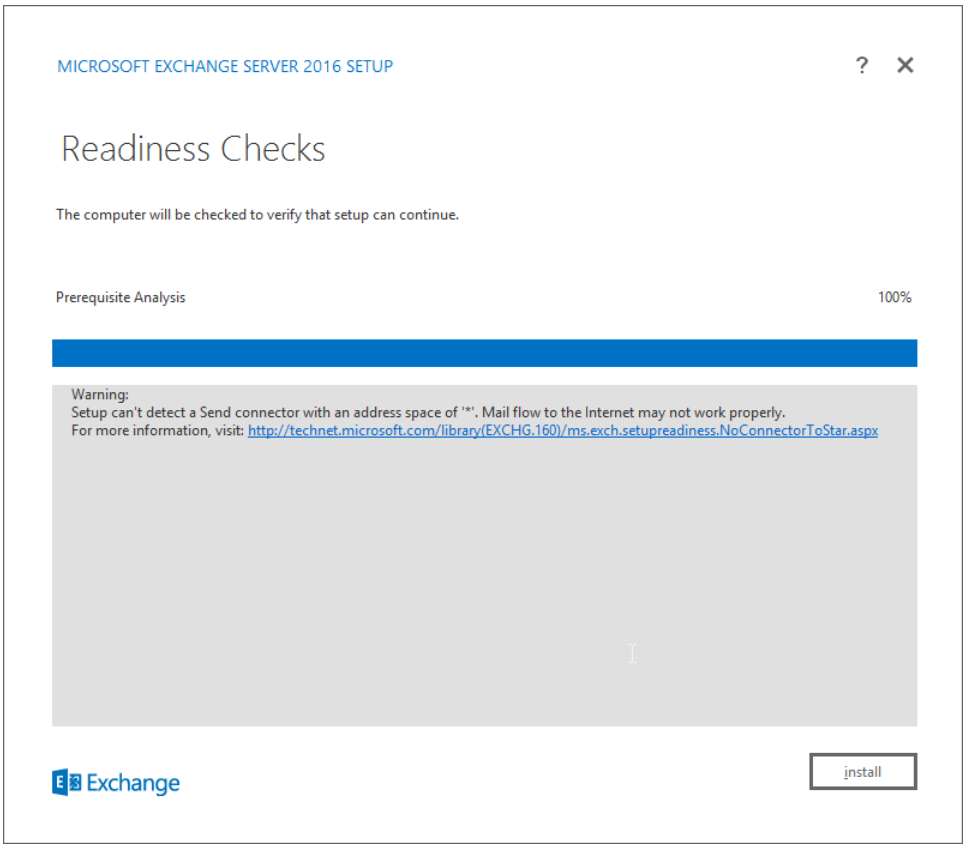
19. Click **Next.**
20. Specify the name for the Exchange organization, for example, DI.
21. Decide whether to apply split permissions, based on the needs of the enterprise.



22. Click **Next.**
23. Select **No.**



24. Click **Next.**
25. Install any **prerequisites** listed.
26. If necessary, restart the server and re-run **setup.exe,** completing steps 3-22 again.



27. Click **Install.**

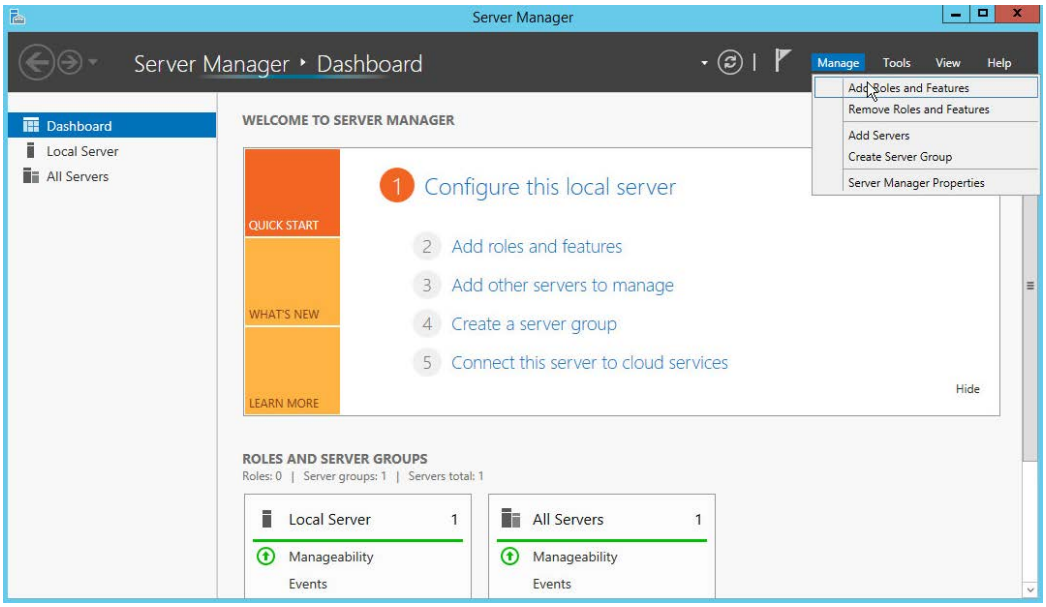
2.3 Windows Server Hyper-V Role

As part of our simulated enterprise, we include a Windows Hyper-V server. This section covers the instructions for installing Windows Server Hyper-V 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 and are replicated below for preservation and ease of use.

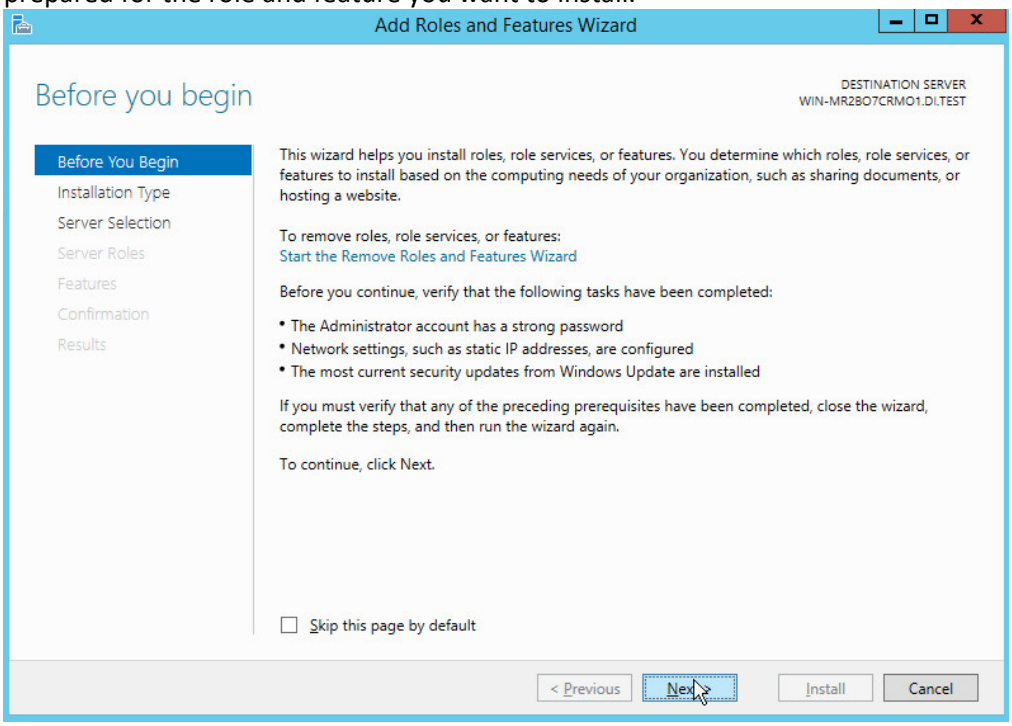
2.3.1 Production Installation

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



551

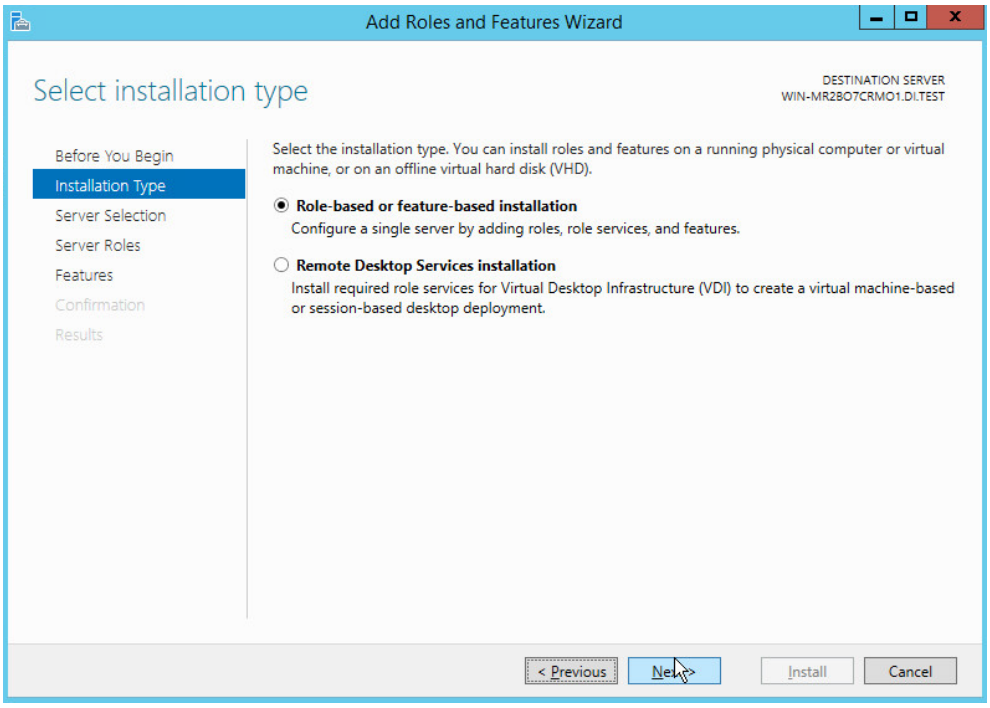
552 2. On the **Before you begin** page, verify that your destination server and network environment are
553 prepared for the role and feature you want to install.



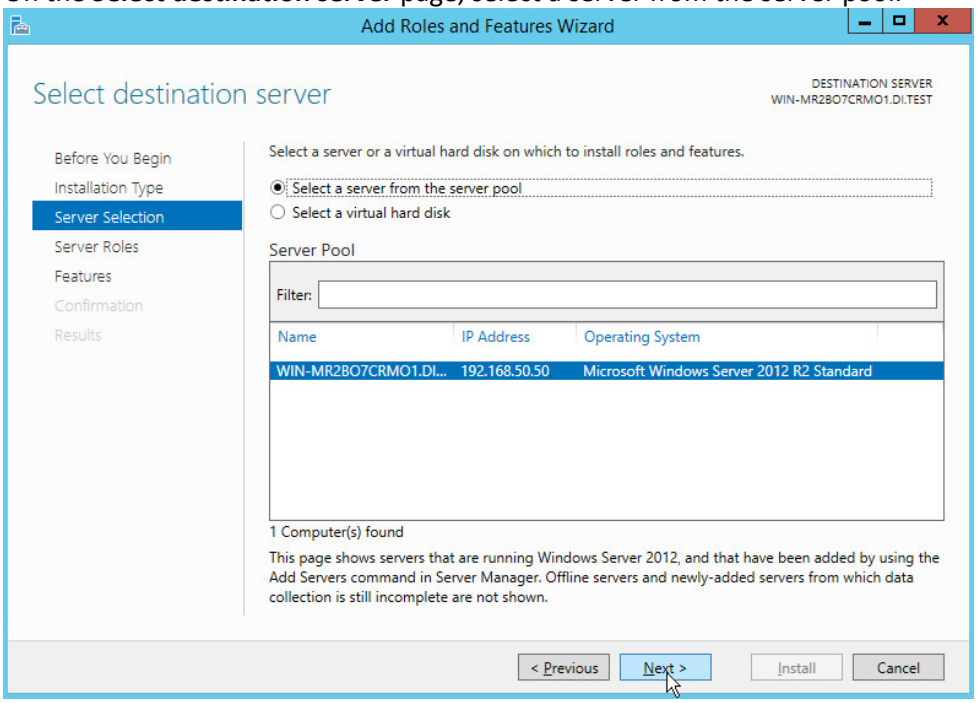
554

555 3. Click **Next.**

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

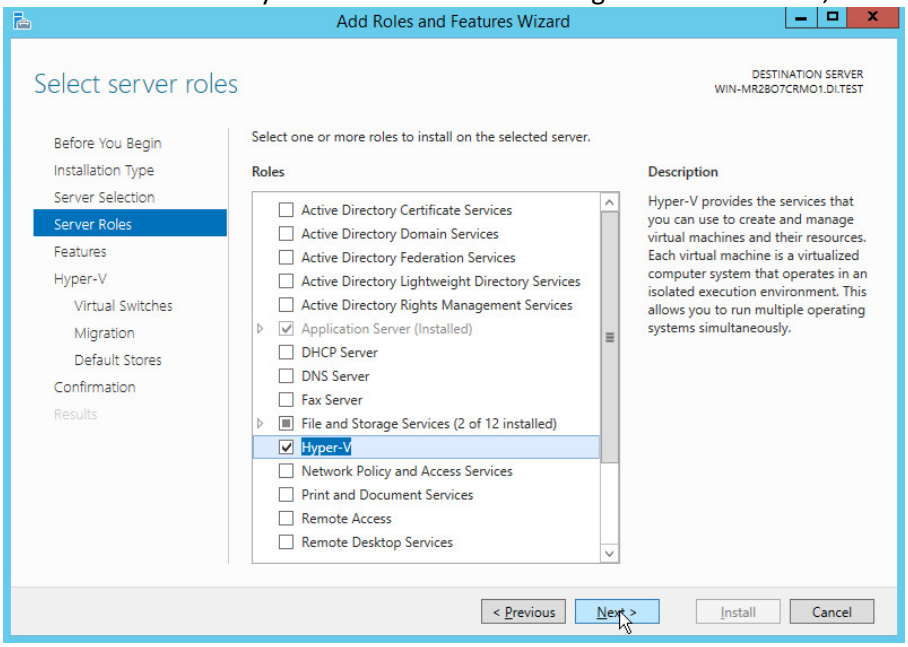


5. Click **Next.**
6. On the **Select destination server** page, select a server from the server pool.



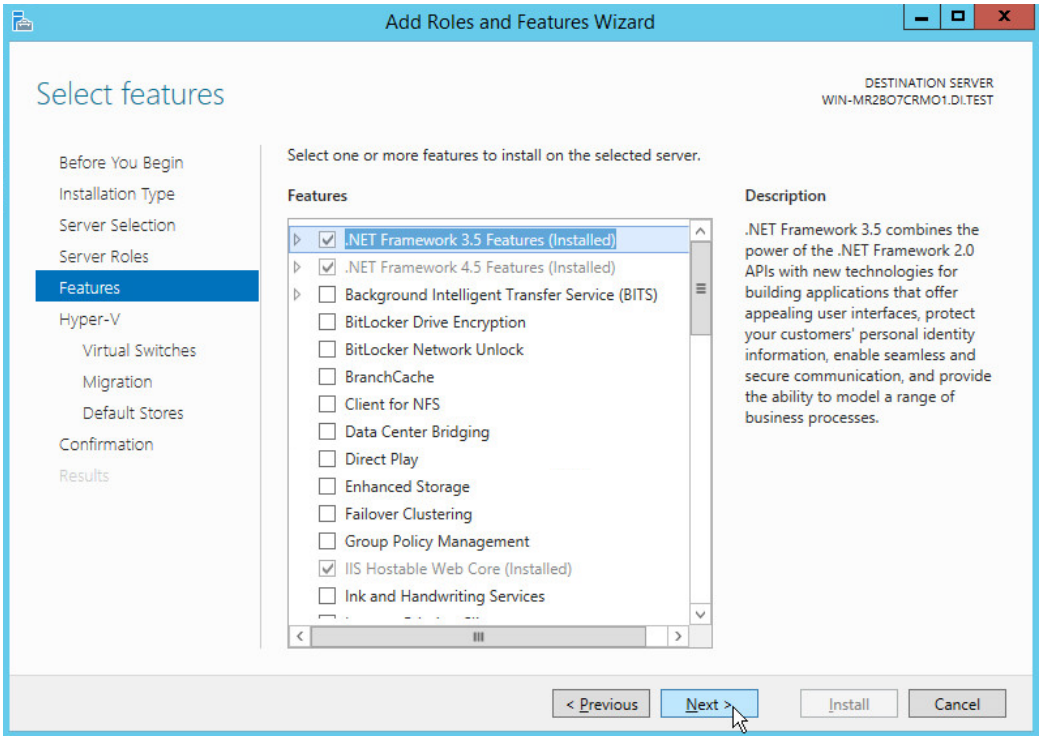
7. Click **Next.**
8. On the **Select server roles** page, select **Hyper-V.**

563 9. To add the tools that you use to create and manage virtual machines, click **Add Features.**



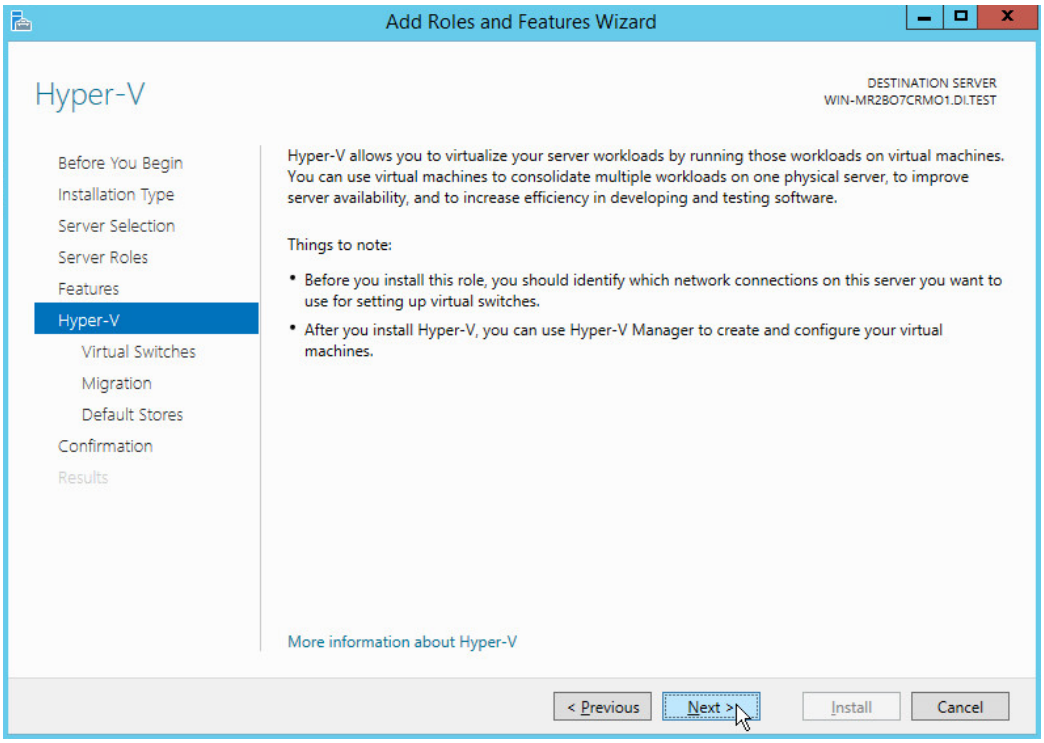
564

565 10. Click **Next.**

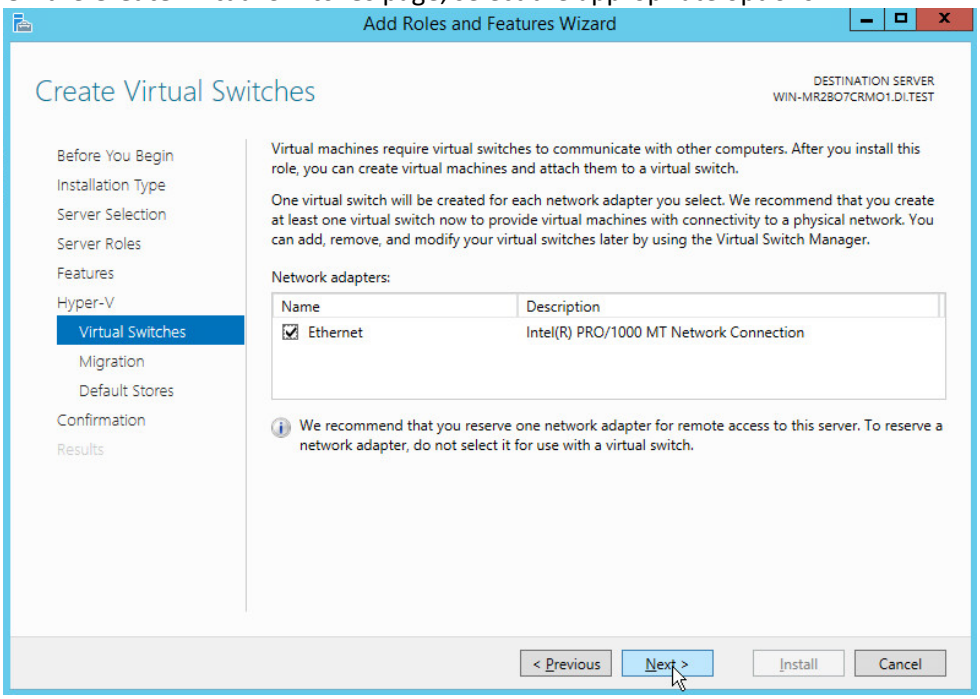


566

567 11. Click **Next.**

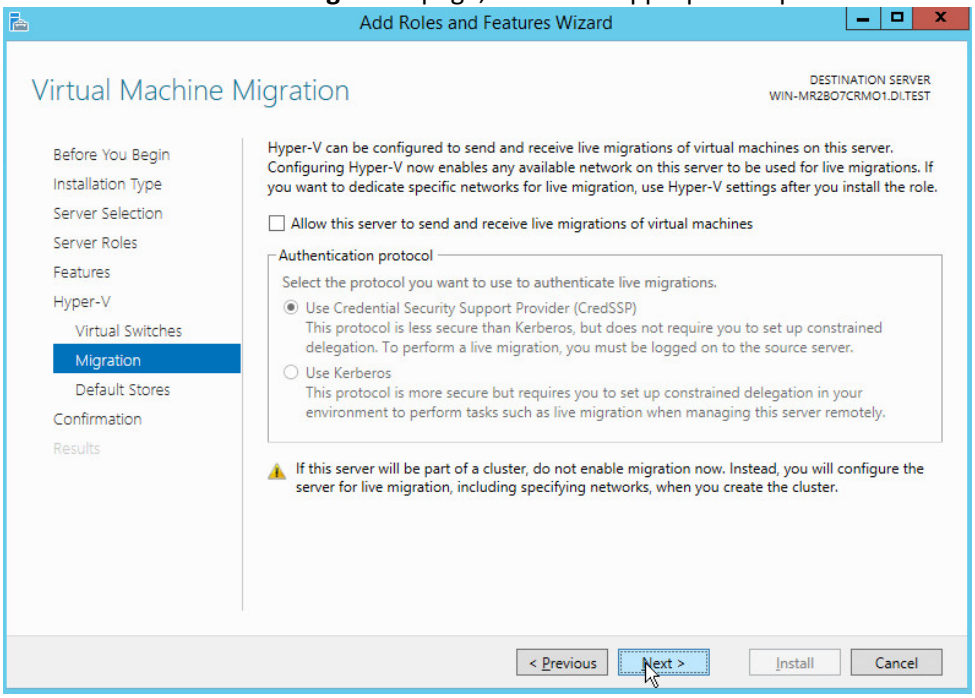


12. Click **Next.**
13. On the **Create Virtual Switches** page, select the appropriate options.



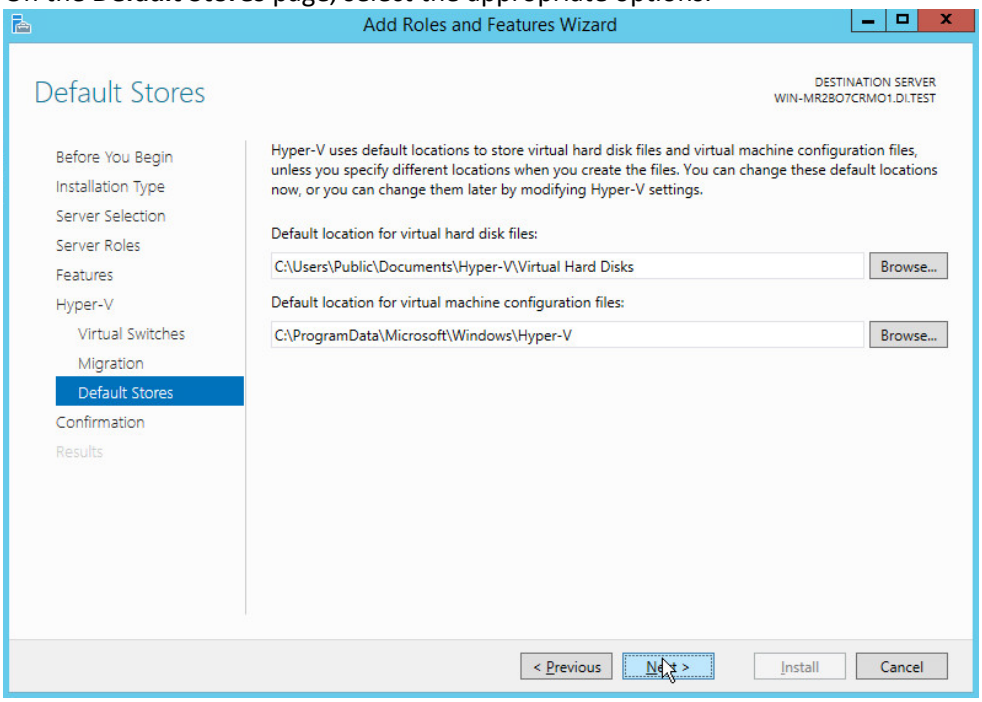
14. Click **Next.**

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



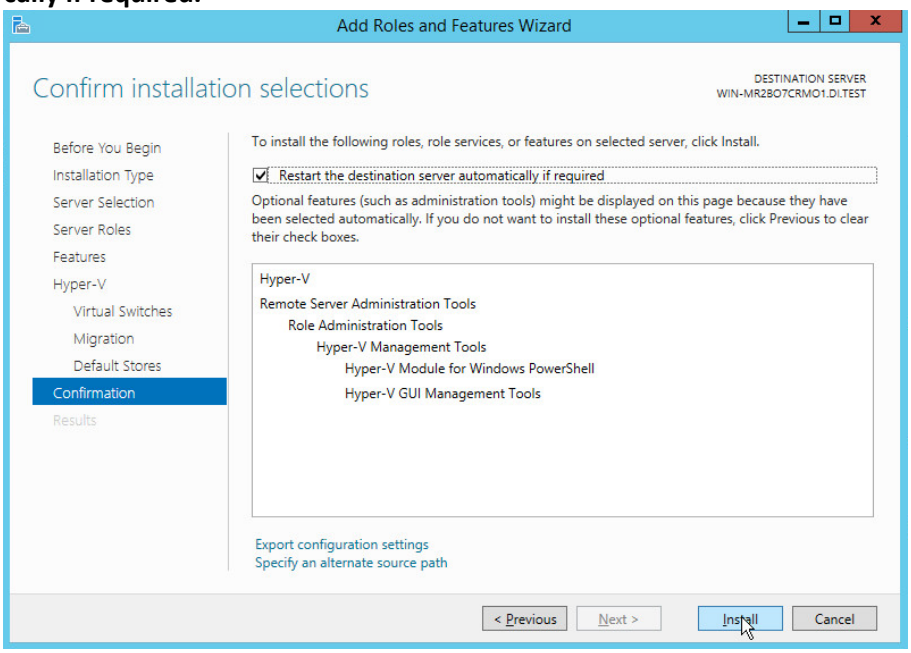
16. Click **Next.**

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.**



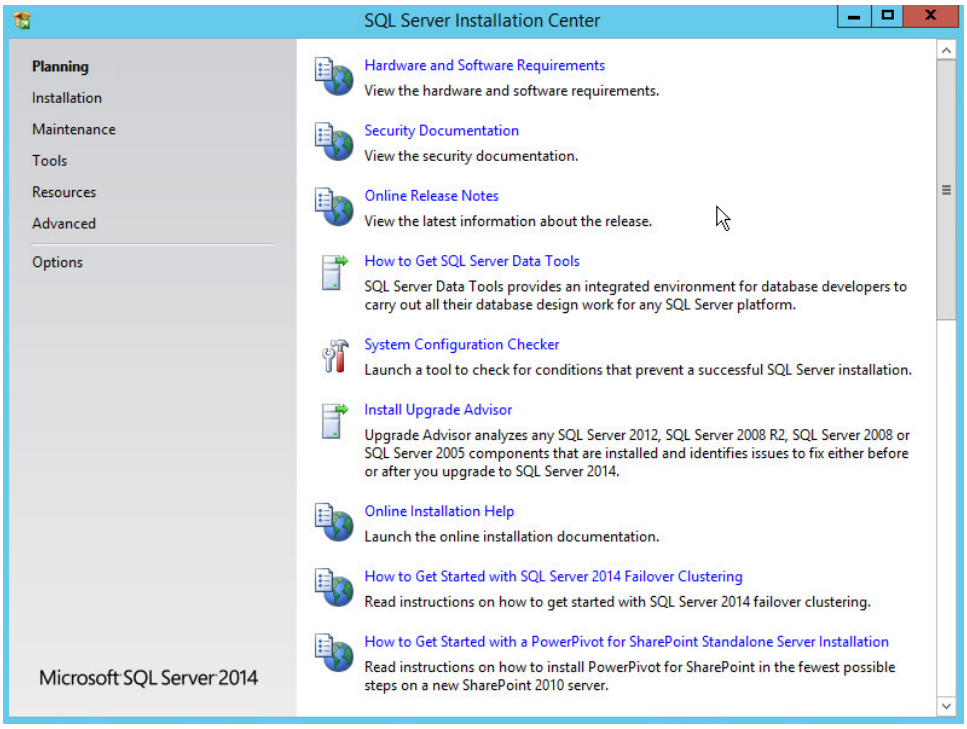
20. Click **Install.**
21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

2.4 MS SQL Server

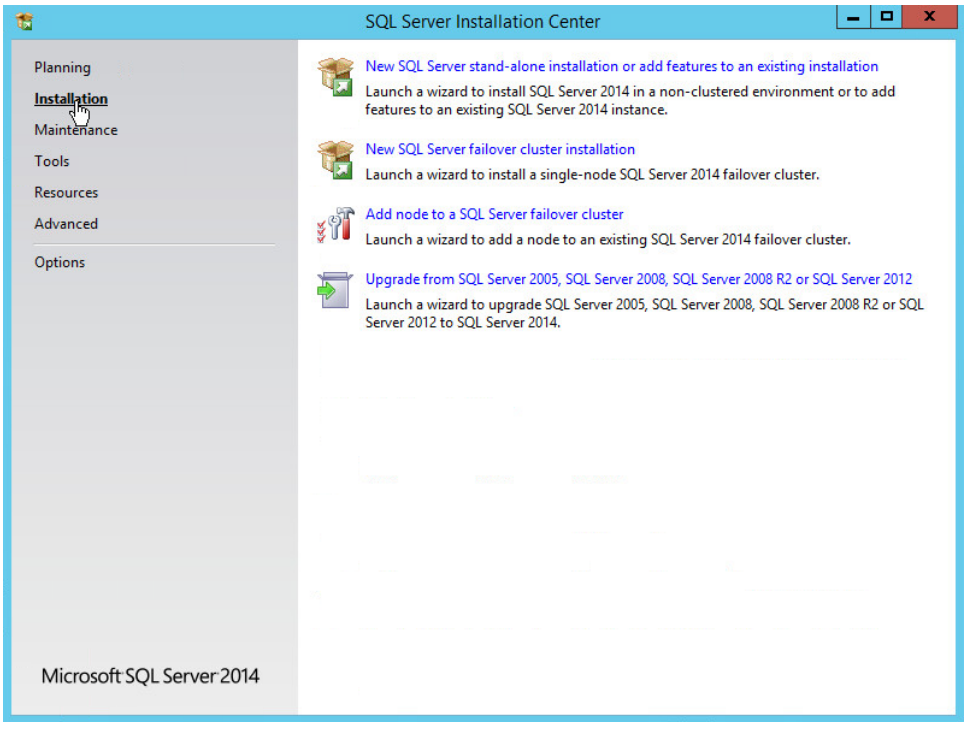
As part of both our enterprise emulation and data integrity solution, we include a Microsoft SQL Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

2.4.1 Install and Configure MS SQL

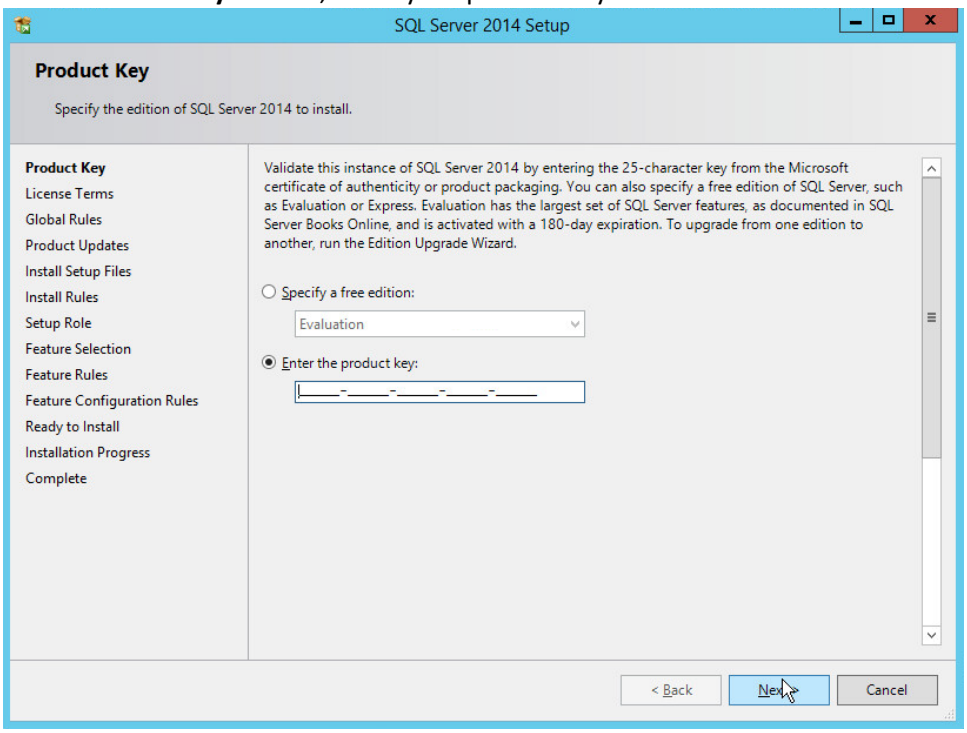
1. Acquire **SQL Server 2014 Installation Media.**
2. Locate the installation media in the machine and click on **SQL2014_x64_ENU** to launch **SQL Server Installation Center.**



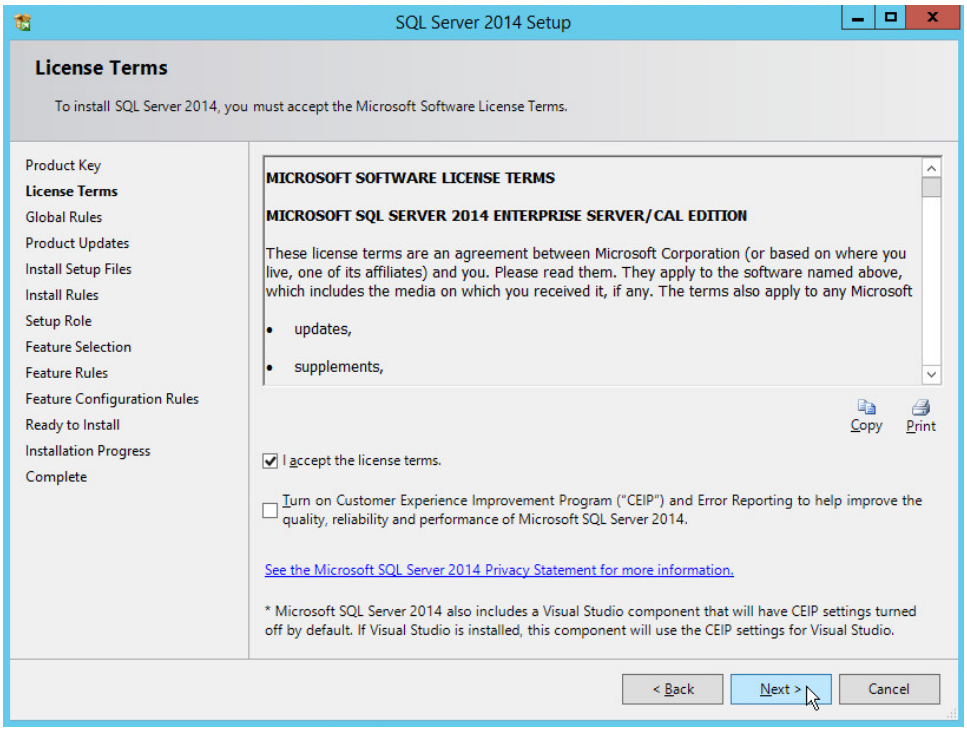
3. On the left menu, select **Installation.**



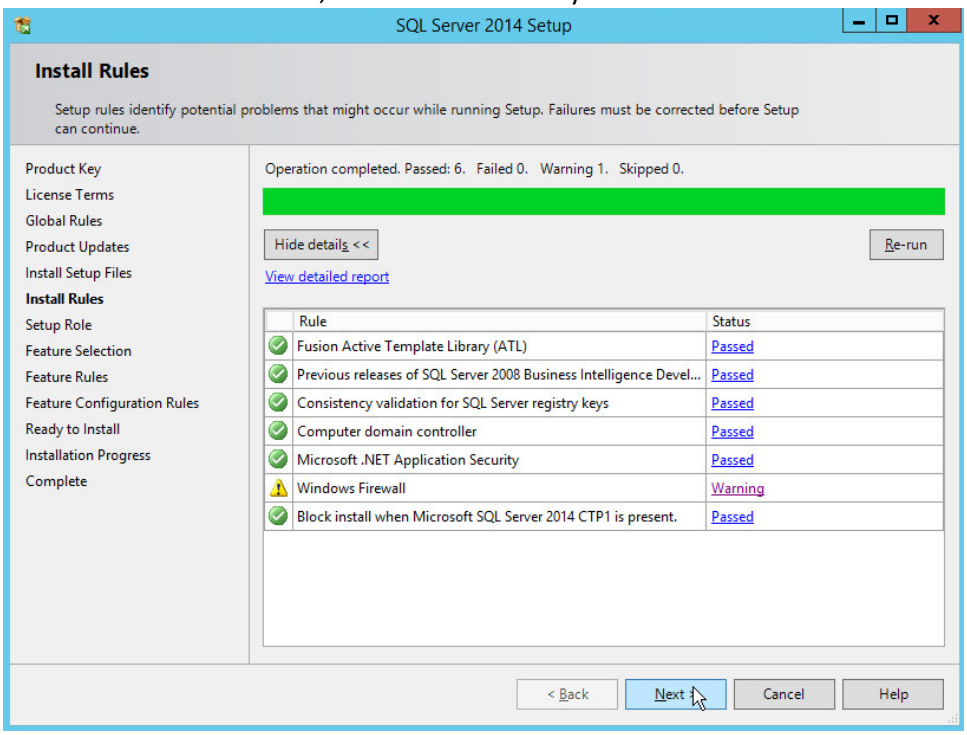
4. Select **New SQL Server stand-alone installation or add features to an existing installation.** This will launch the SQL Server 2014 setup.
5. In the **Product Key** section, enter your product key.



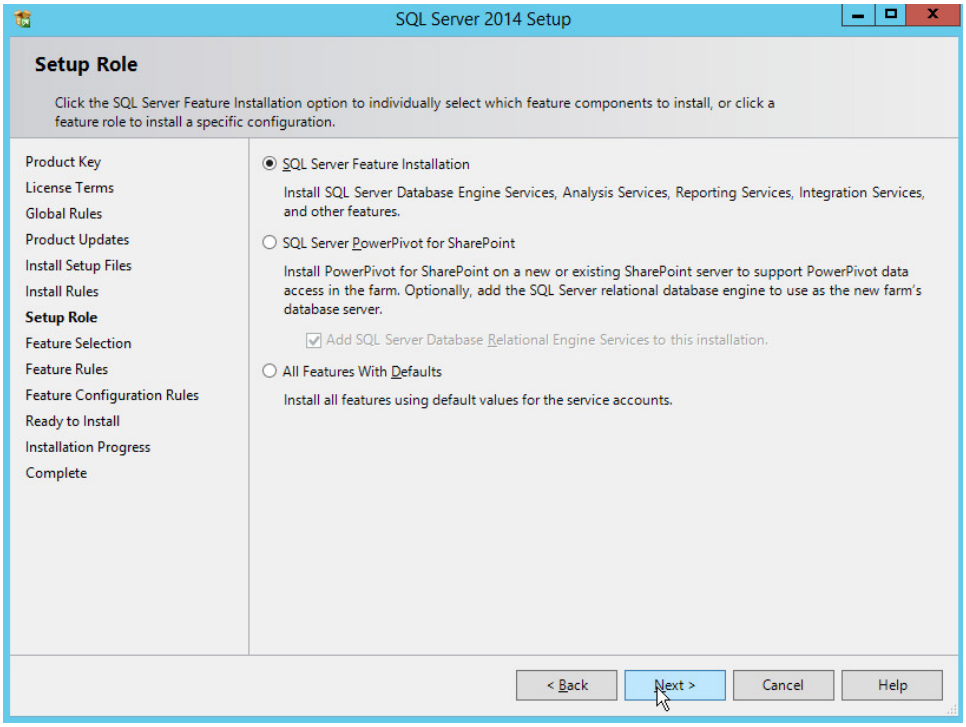
6. Click **Next.**
7. In the **License Terms** section, read and click **I accept the license terms.**



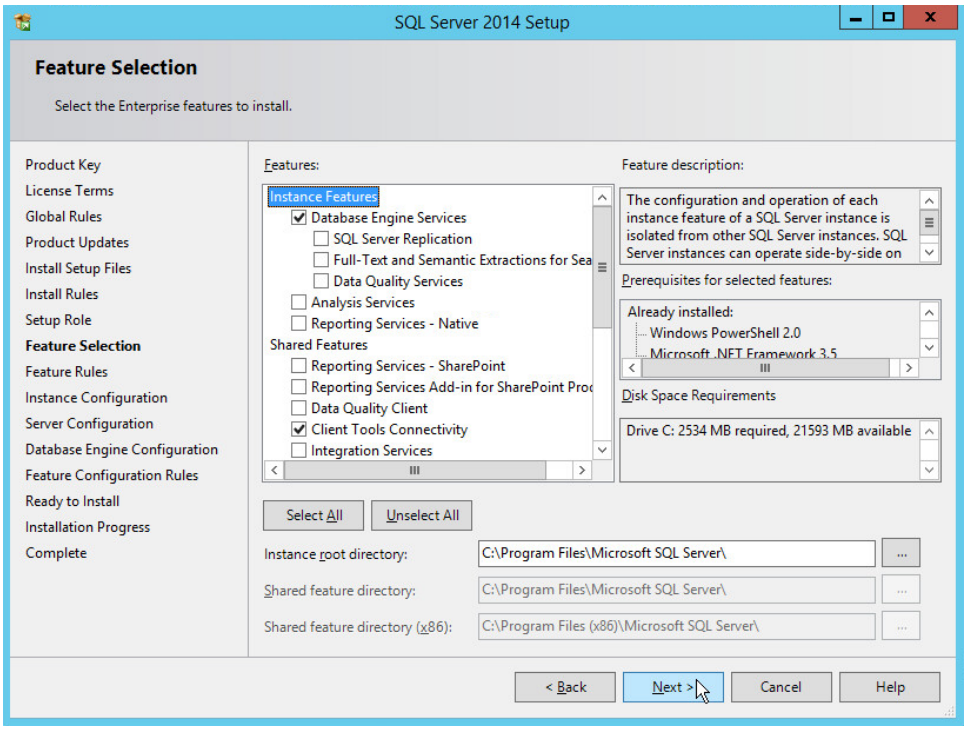
8. Click **Next.**
9. In the **Install Rules** section, note and resolve any further conflicts.



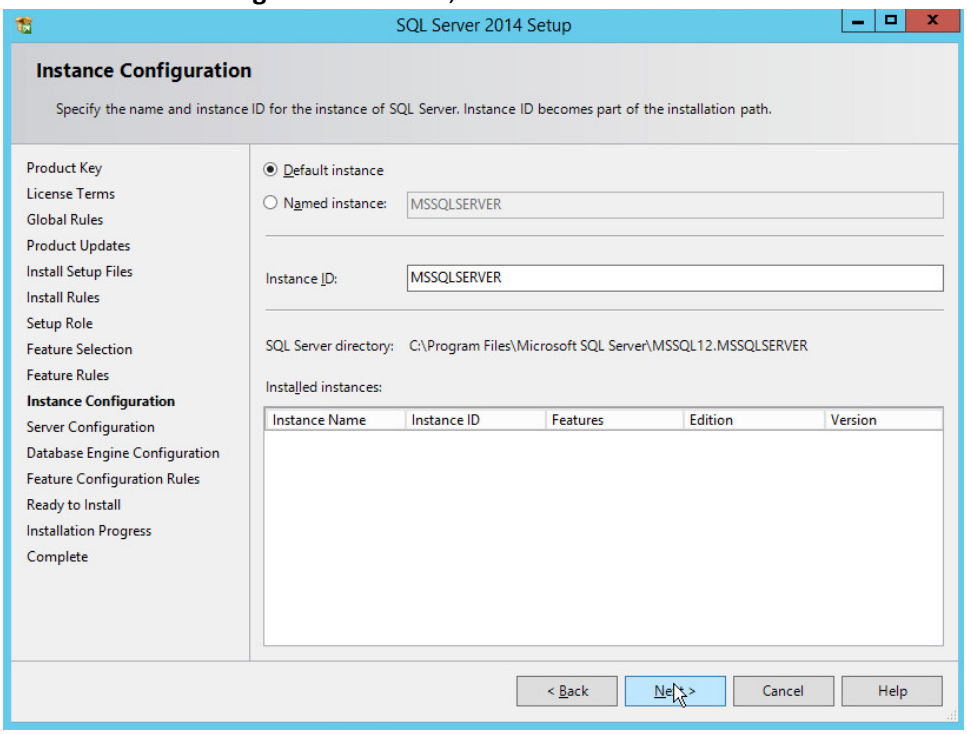
10. Click **Next.**
11. In the **Setup Role** section, select **SQL Server Feature Installation.**



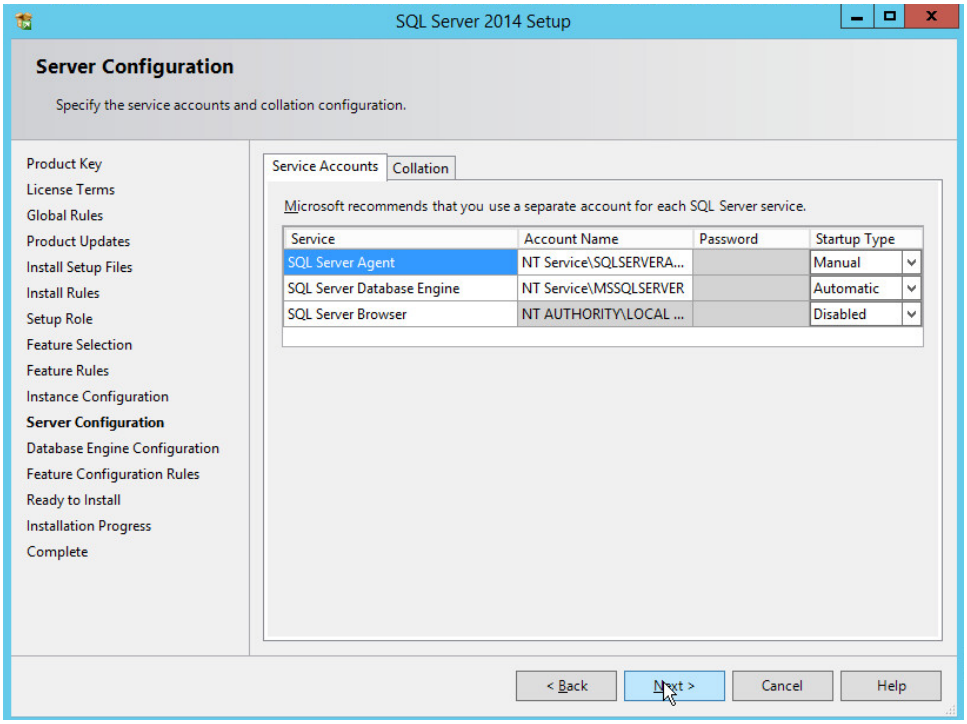
12. Click **Next.**
13. In the **Feature Selection** section, select the following:
    a. **Database Engine Services**
    b. **Client Tools Connectivity**
    c. **Client Tools Backwards Compatibility**
    d. **Client Tools SDK**
    e. **Management Tools – Basic**
    f. **Management Tools – Complete**
    g. **SQL Client Connectivity SDK**
    h. **Any other desired features**



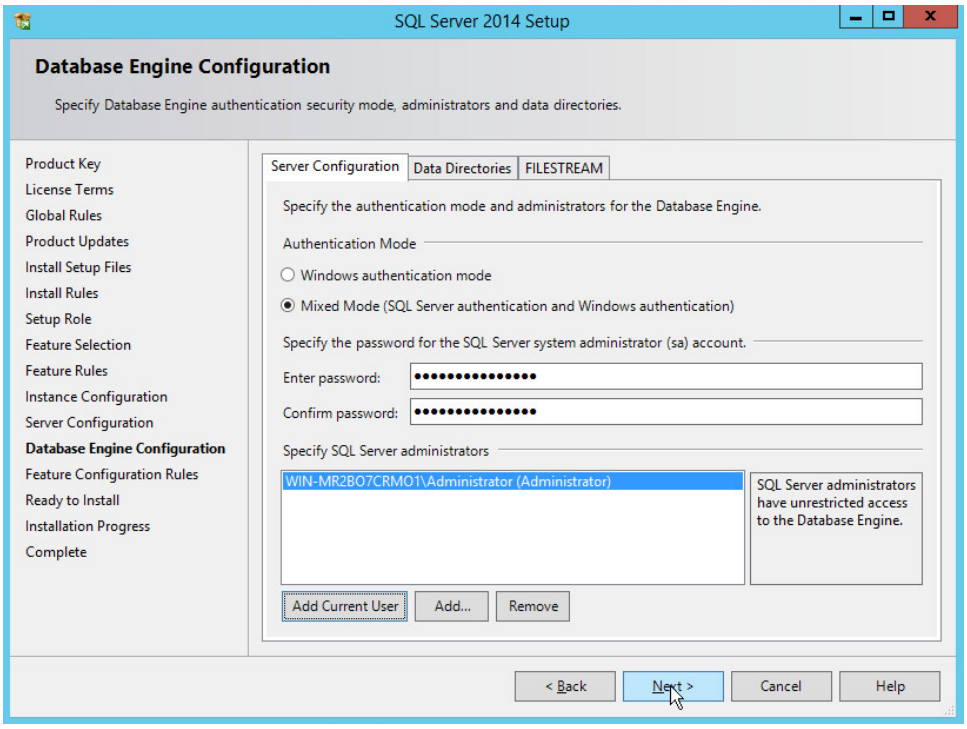
14. Click **Next.**
15. In the **Instance Configuration** section, select **Default instance.**



16. Click **Next.**

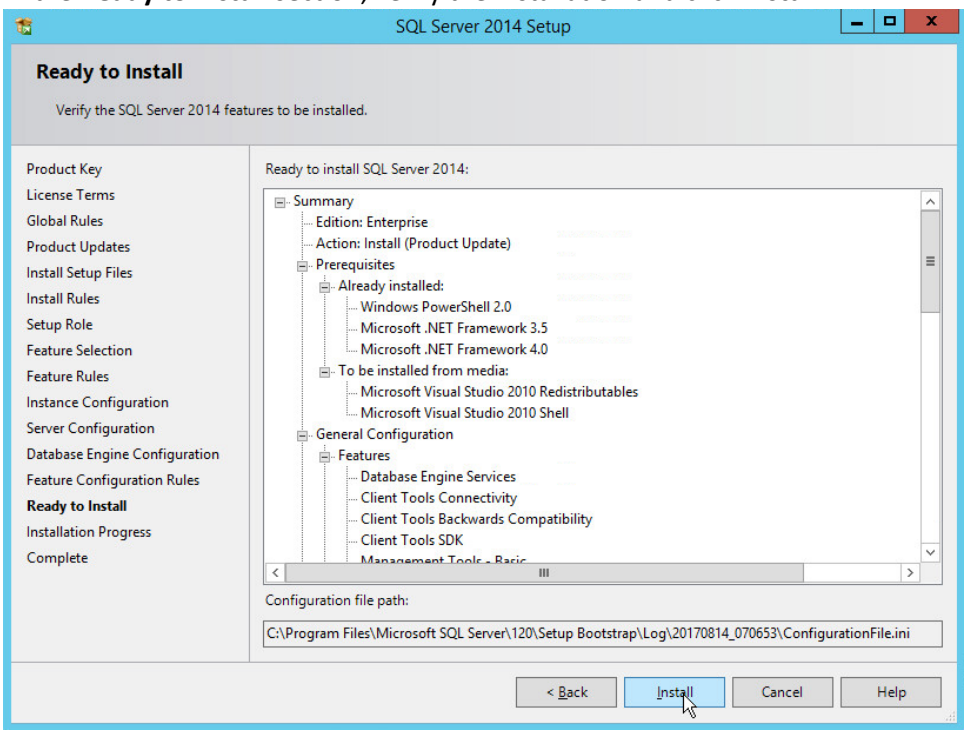


17. In the **Server Configuration** section, click **Next.**
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.
19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User.**
    a. For Domain accounts, simply type in **$DOMAINNAME\$USERNAME** into **Enter the object names to select** textbox.
    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** textbox.
    f. Once you are finished adding users, click **Next.**



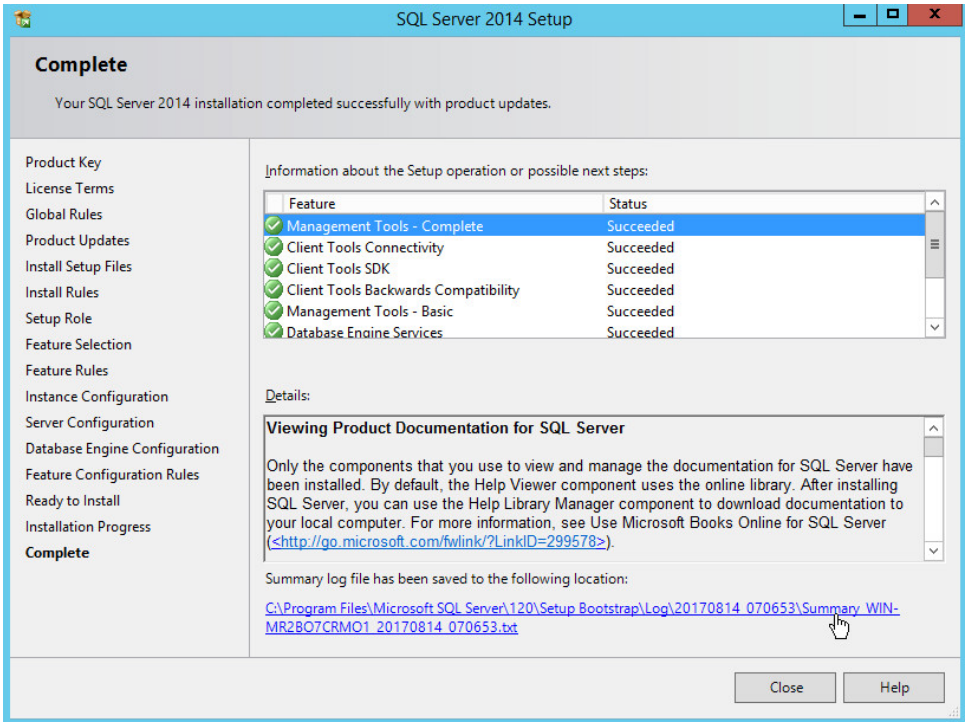
637

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



639

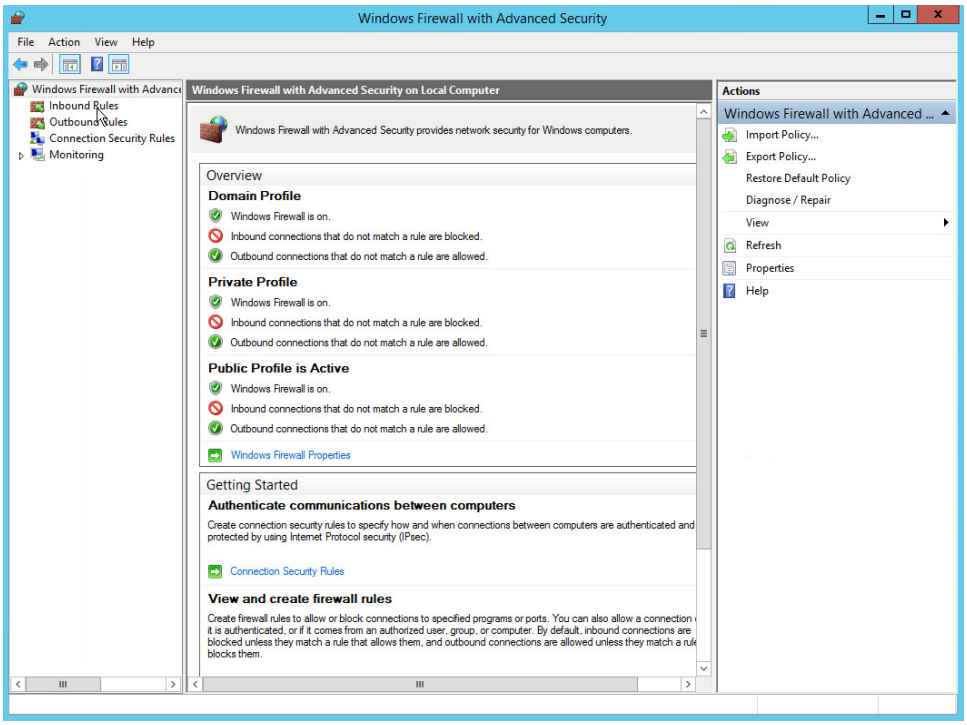
21. Wait for the install to finish.



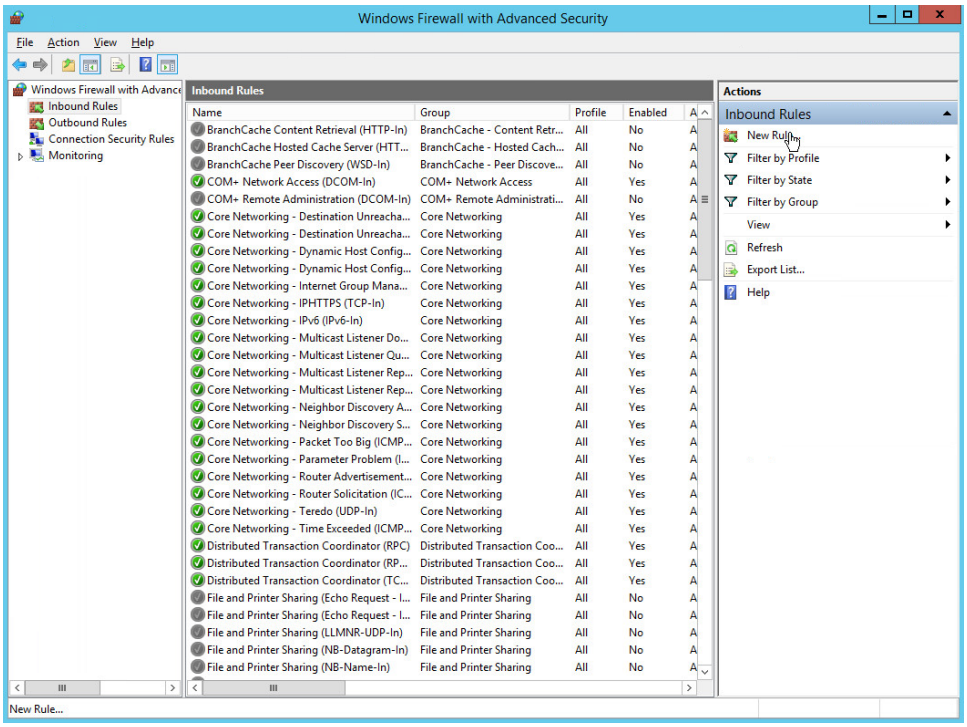
22. Click **Close.**

2.4.2 Open Port on Firewall

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

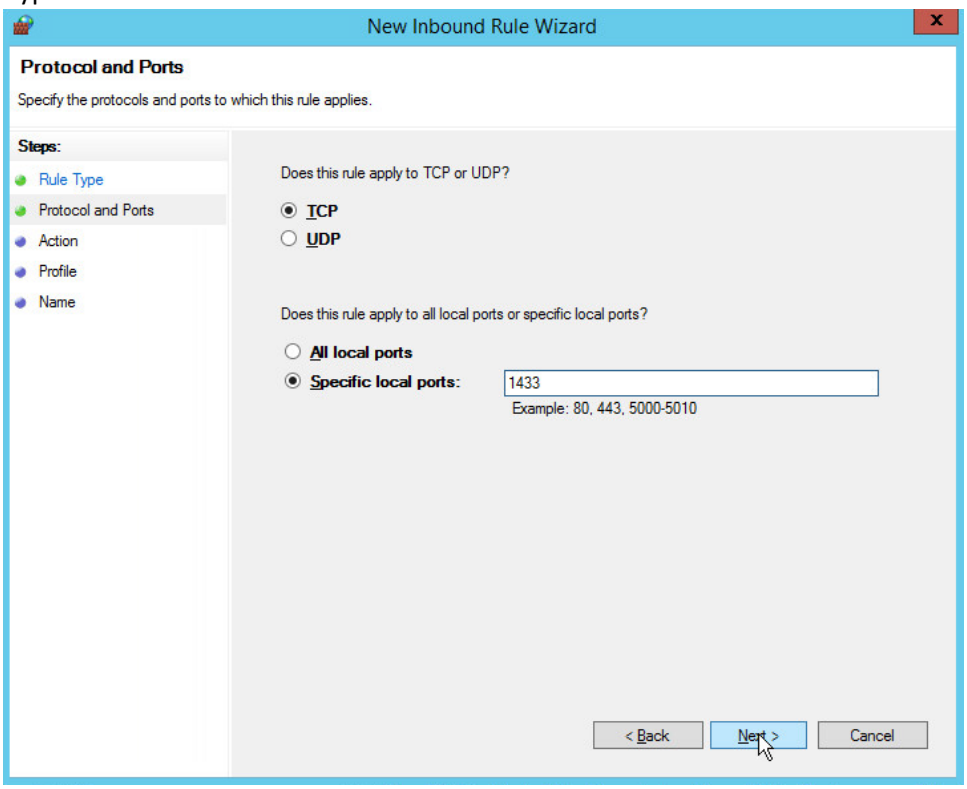


2. Click **Inbound Rules.**

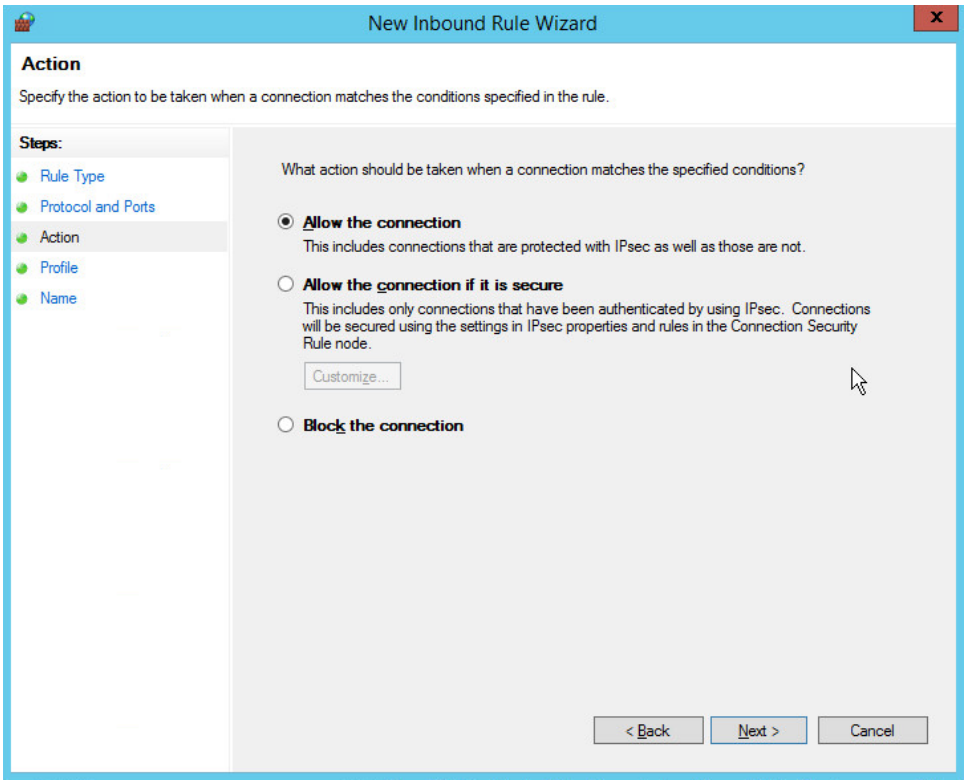


3. Click **New Rule.**

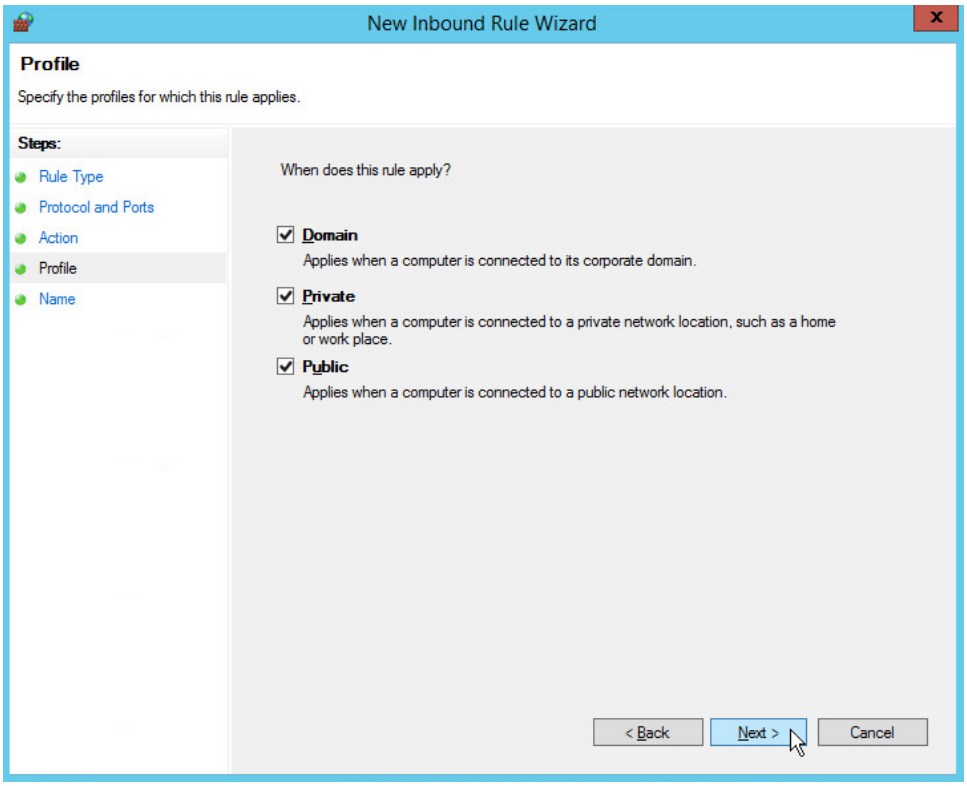
4. Select **Port.**
5. Click **Next.**
6. Select **TCP** and **Specific local ports.**
7. Type **1433** into the text field.



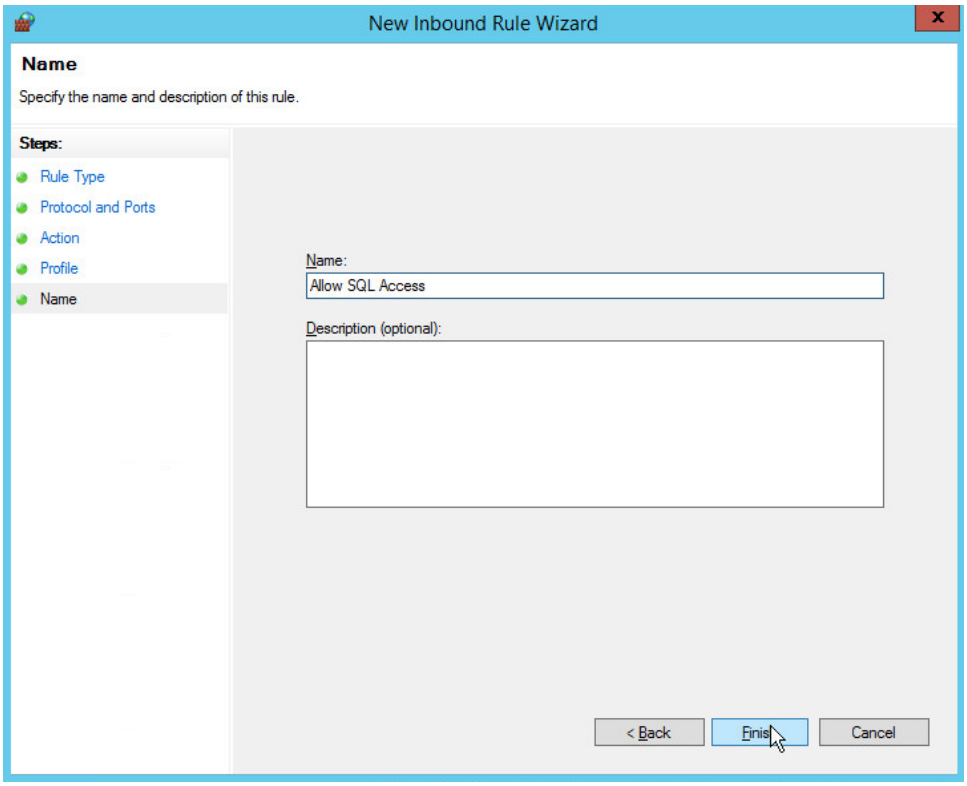
8. Click **Next.**
9. Select **Allow the connection.**



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



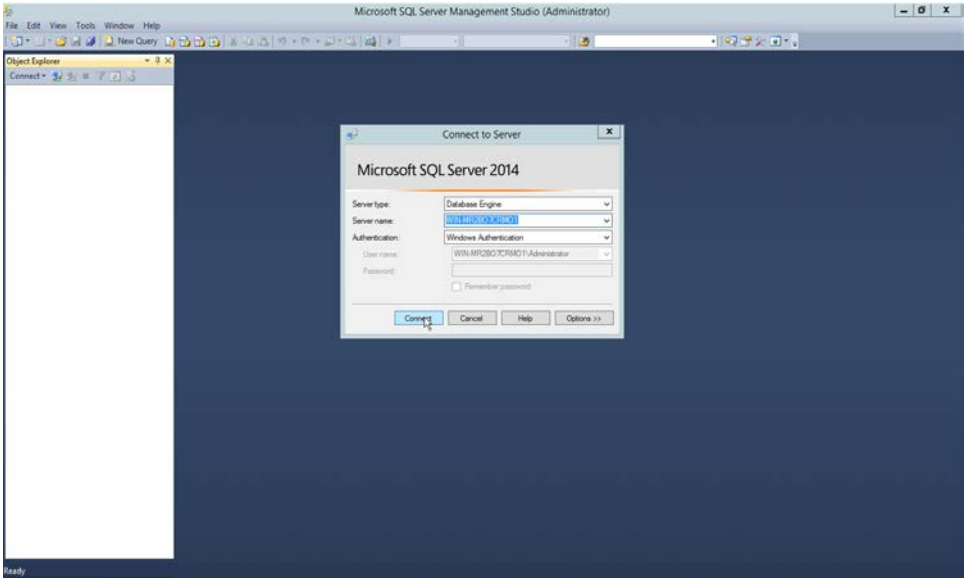
12. Click **Next.**
13. Name the rule **Allow SQL Access.**



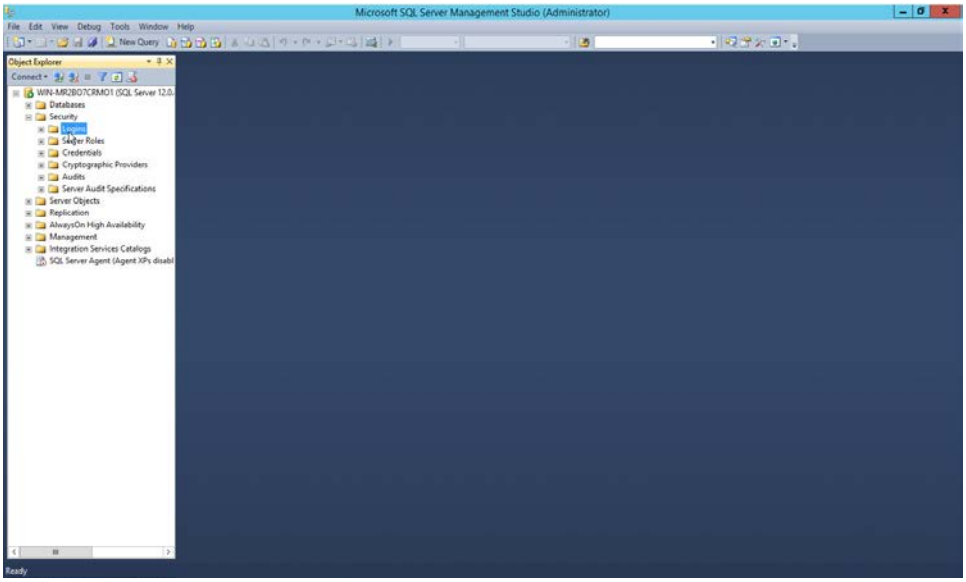
14. Click **Finish.**

2.4.3 Add a New Login to the Database

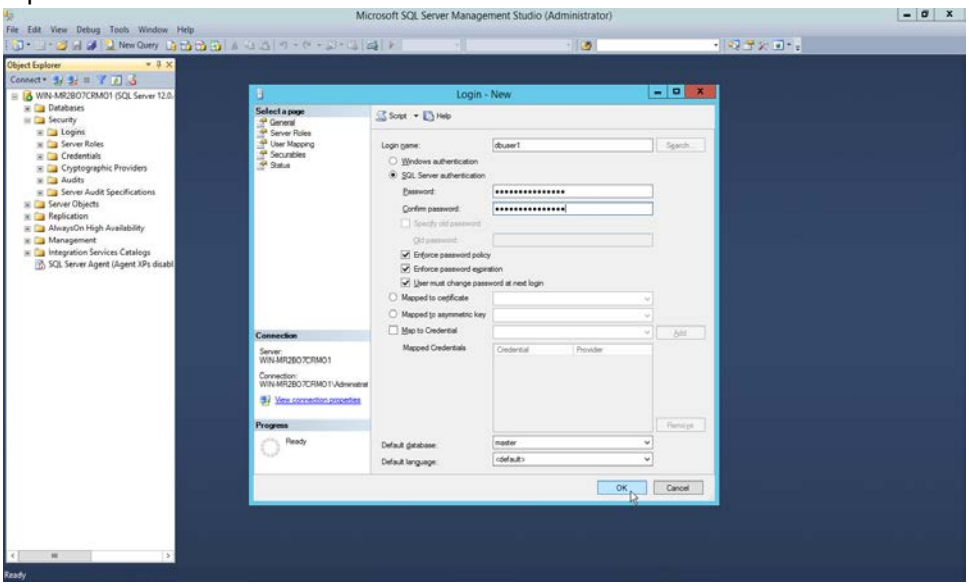
1. Open **SQL Server Management Studio.**



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



669
670 4. Right-click on the **Logins** folder and click **New Login….**
671 5. Input the desired user.



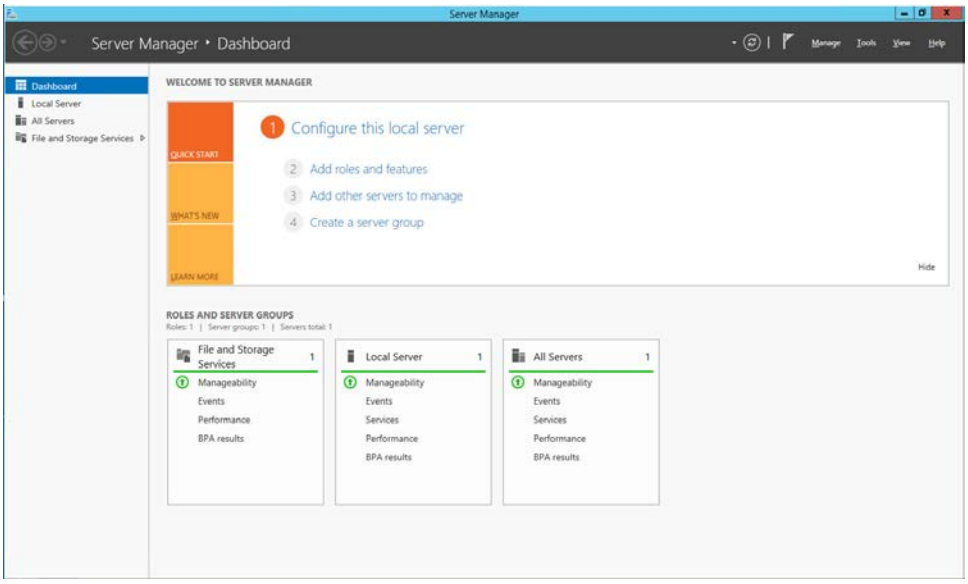
672
673 6. Click **OK.**

2.5 Microsoft IIS Server

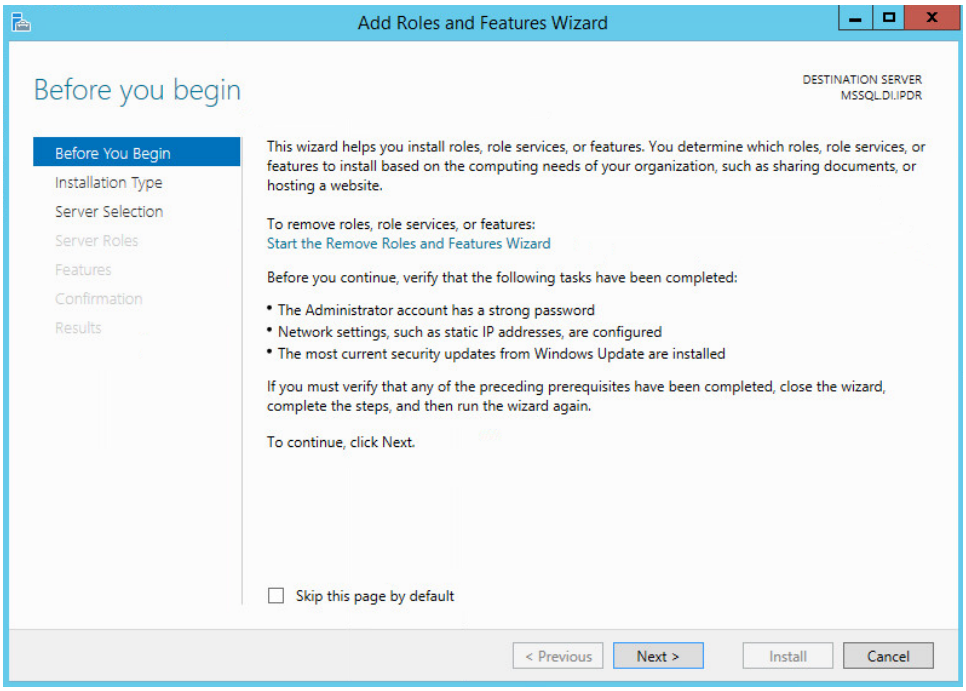
As part of our enterprise emulation, we include a Microsoft IIS server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine. This was conducted on the same machine as section 2.4.

2.5.1 Install IIS

1. Open **Server Manager.**

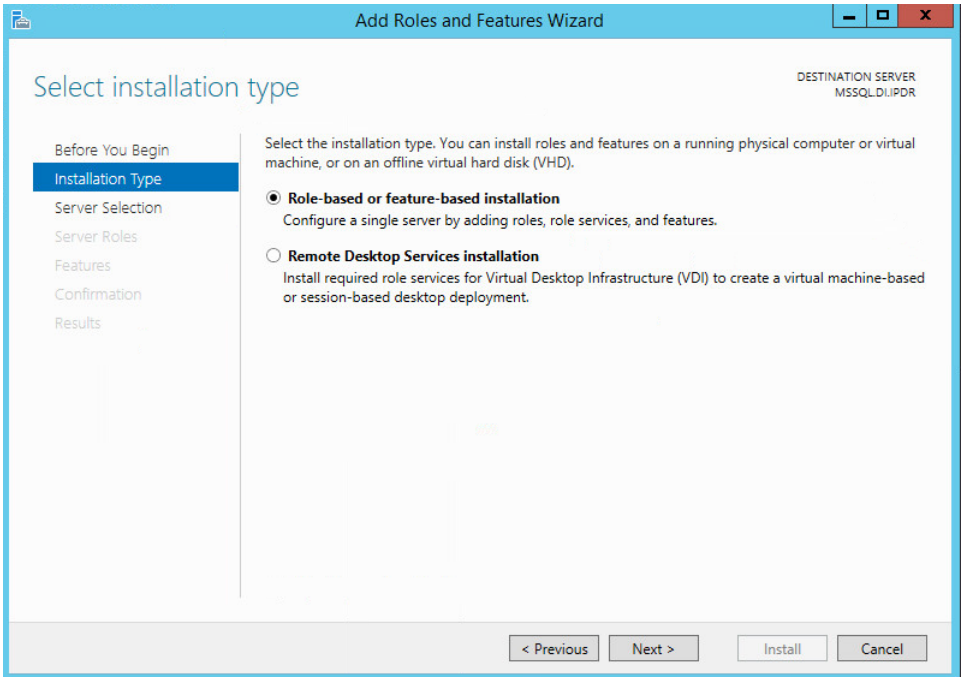


2. Click **Add Roles and Features.**



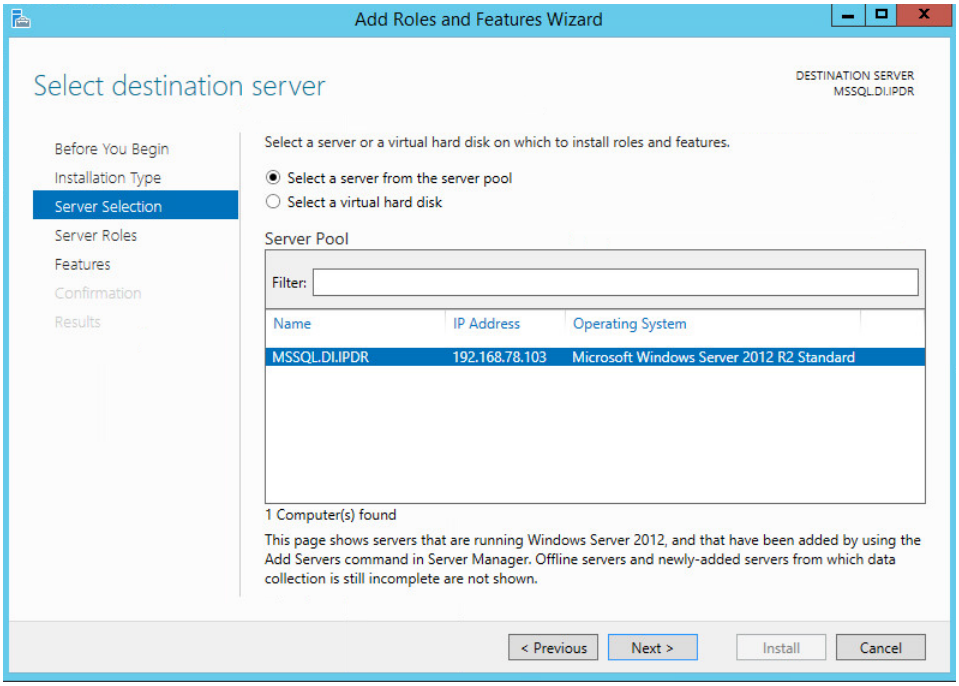
3. Click **Next.**

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



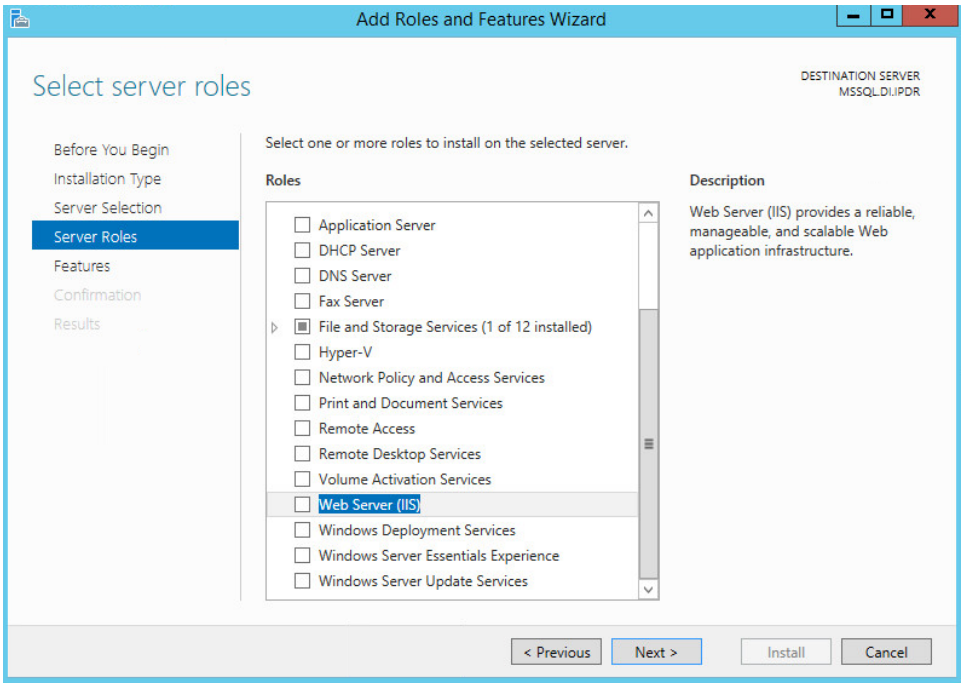
5. Click **Next.**

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



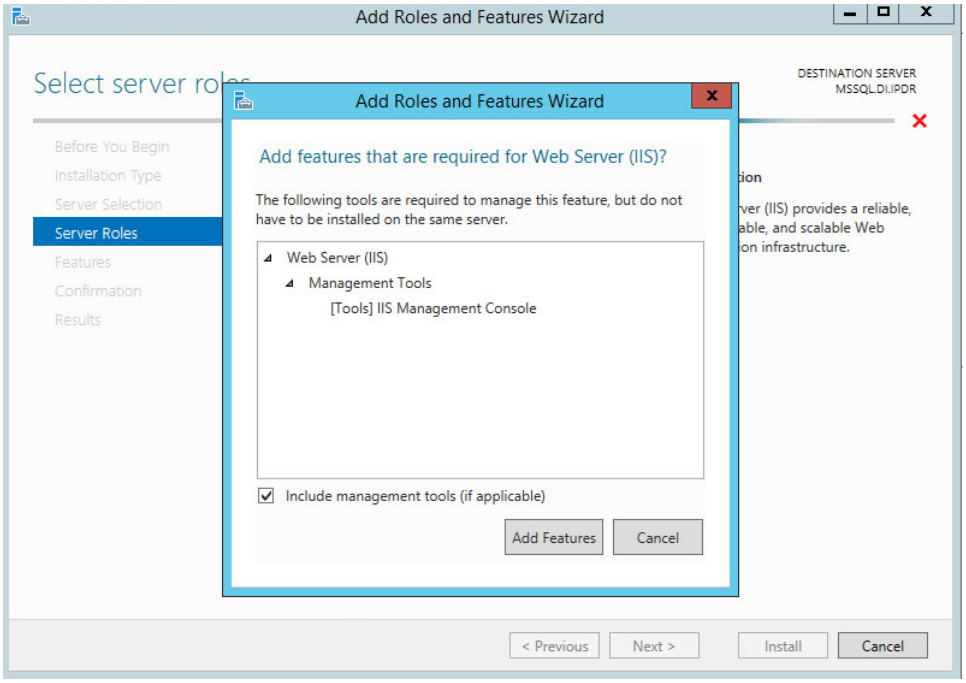
688

689 7. Click **Next.**

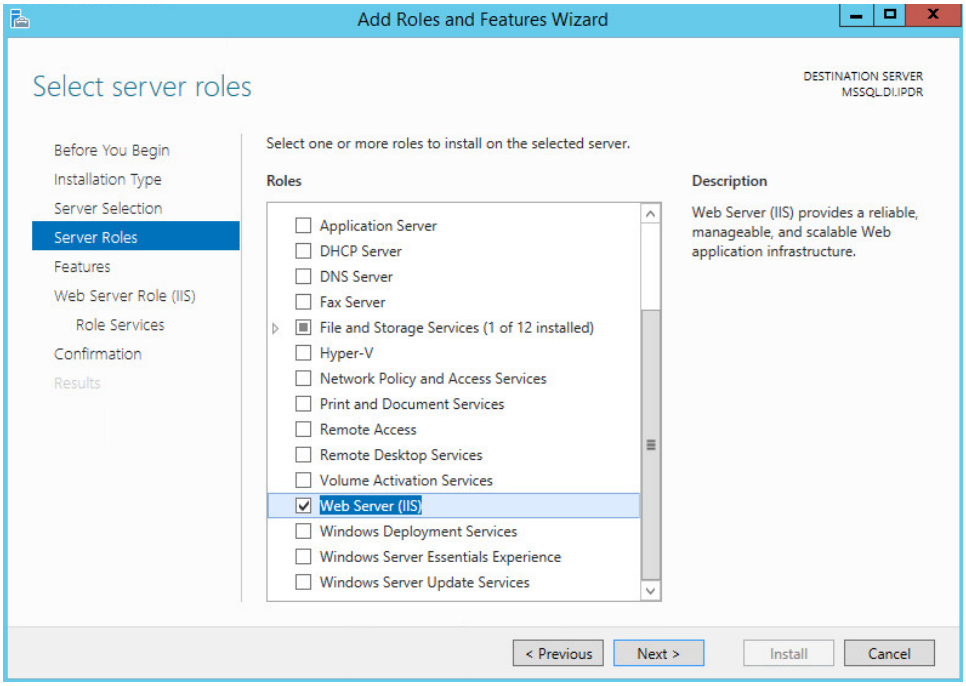


690

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

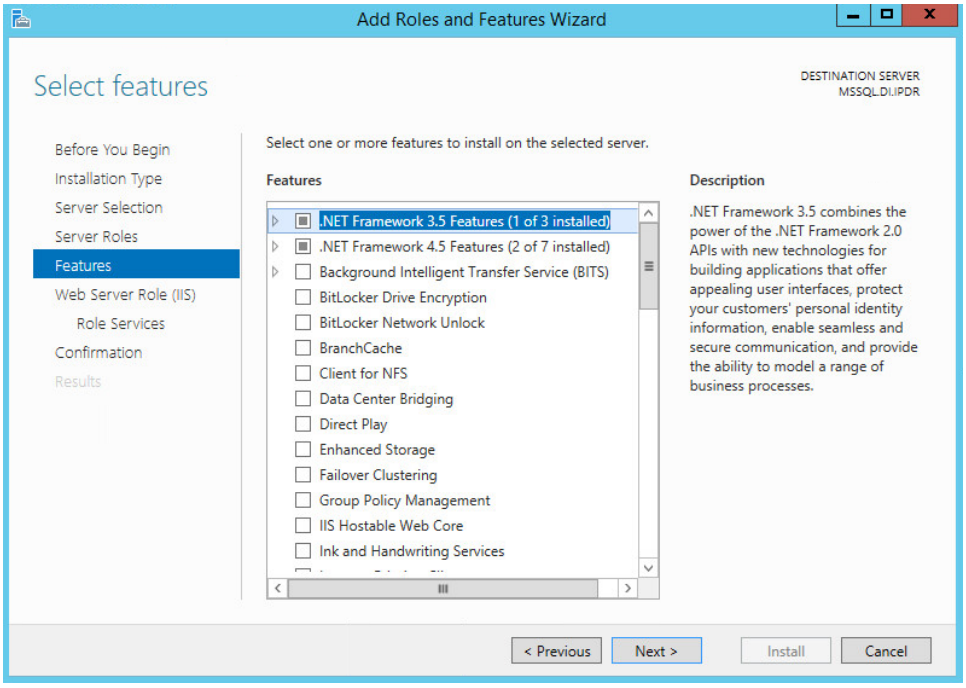


9. Click **Add Features.**

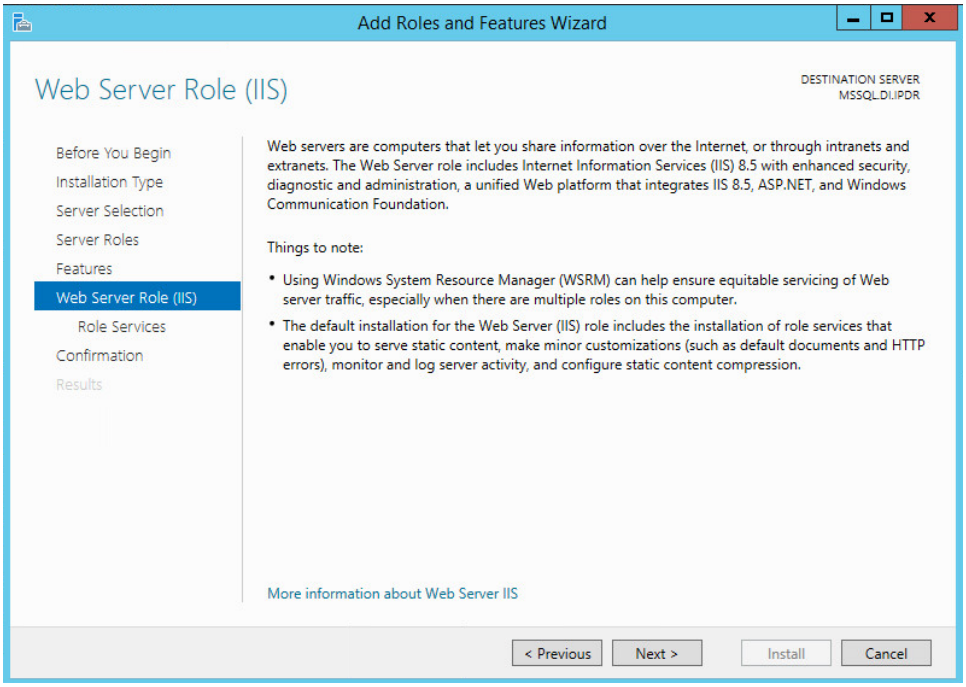


10. Click **Next.**

11. Ensure that all desired features are selected.

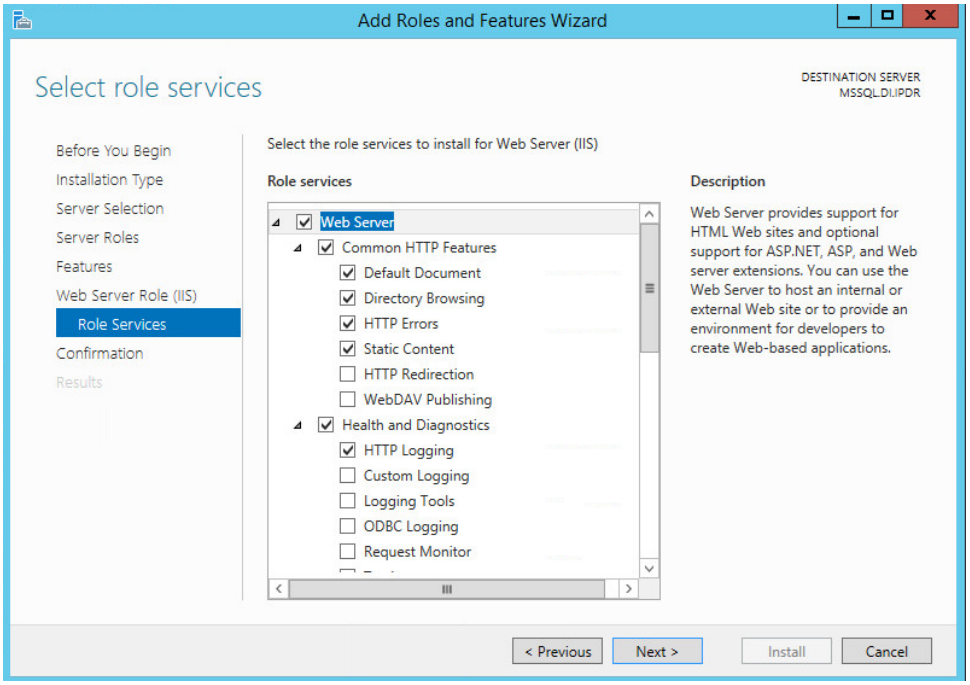


12. Click **Next.**

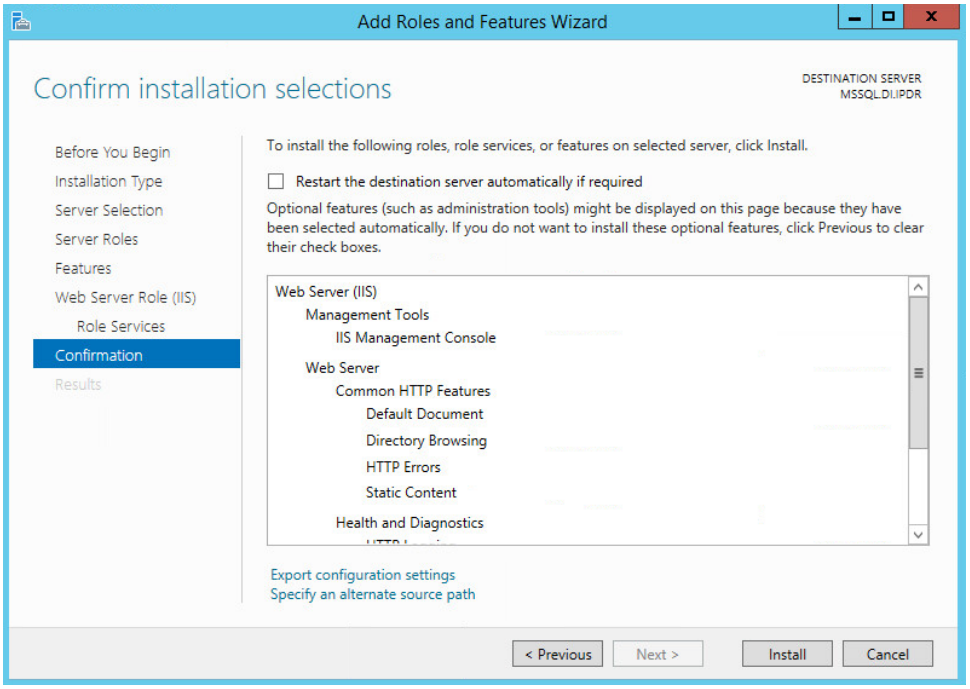


13. Click **Next.**

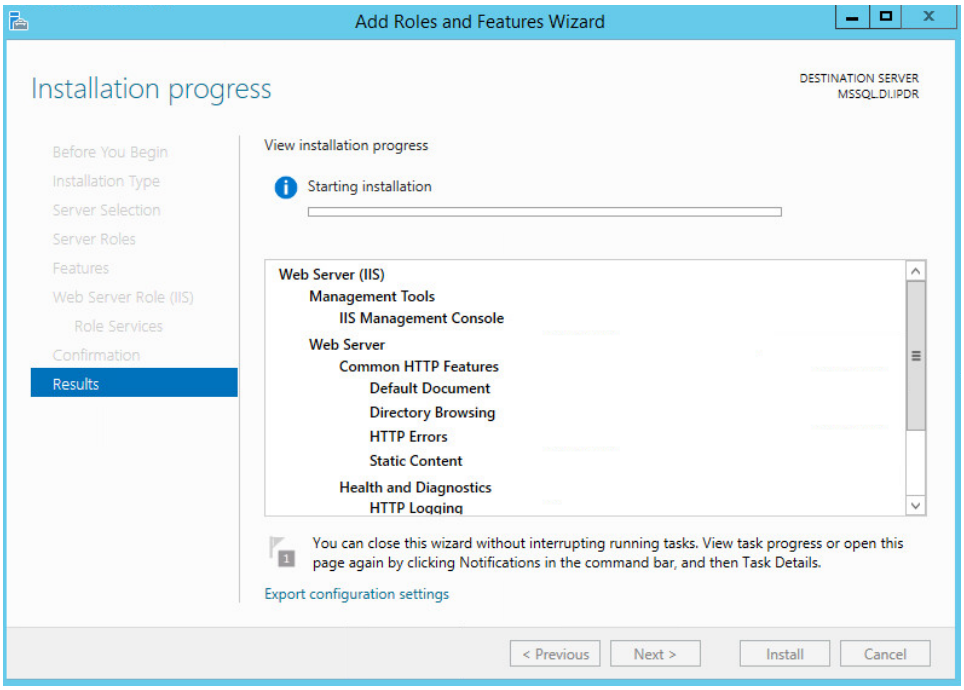
14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging,** and any other desired Role services are selected.



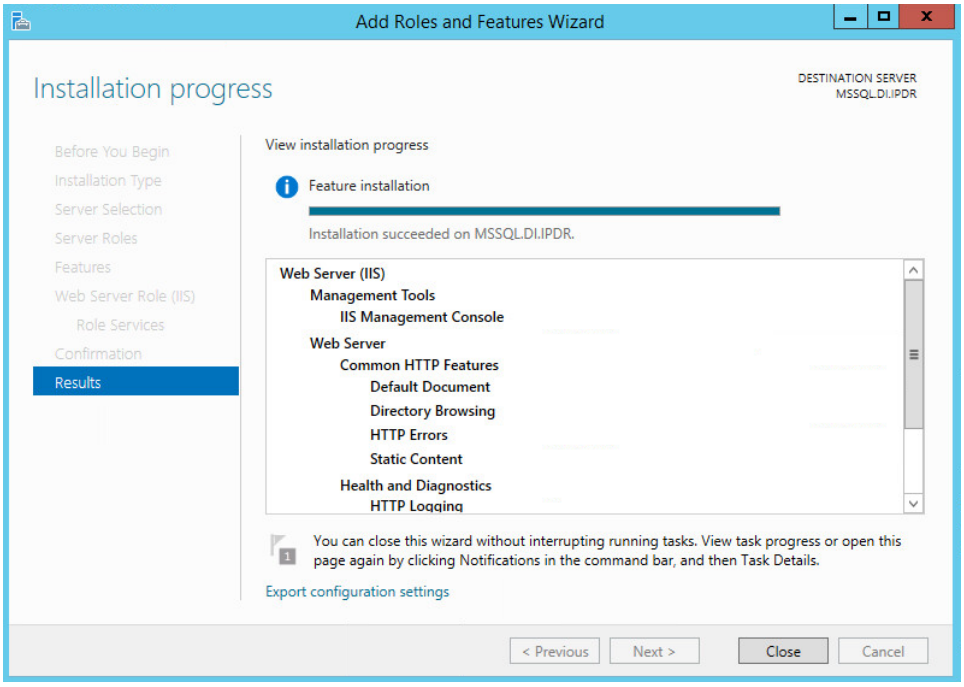
15. Click **Next.**



16. Click **Install.**



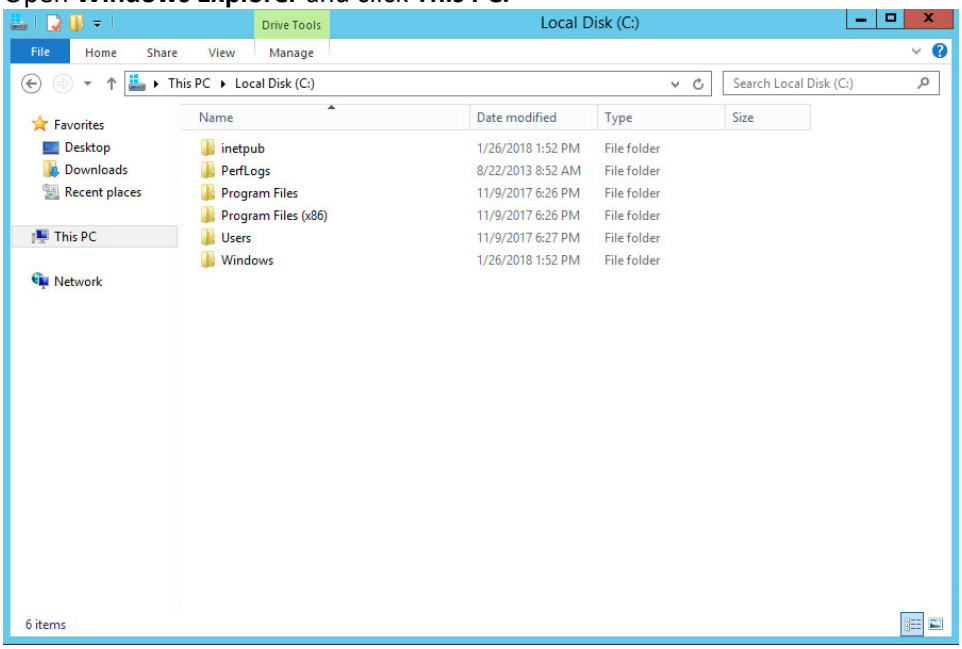
707
708 17. Wait for the installation to complete.



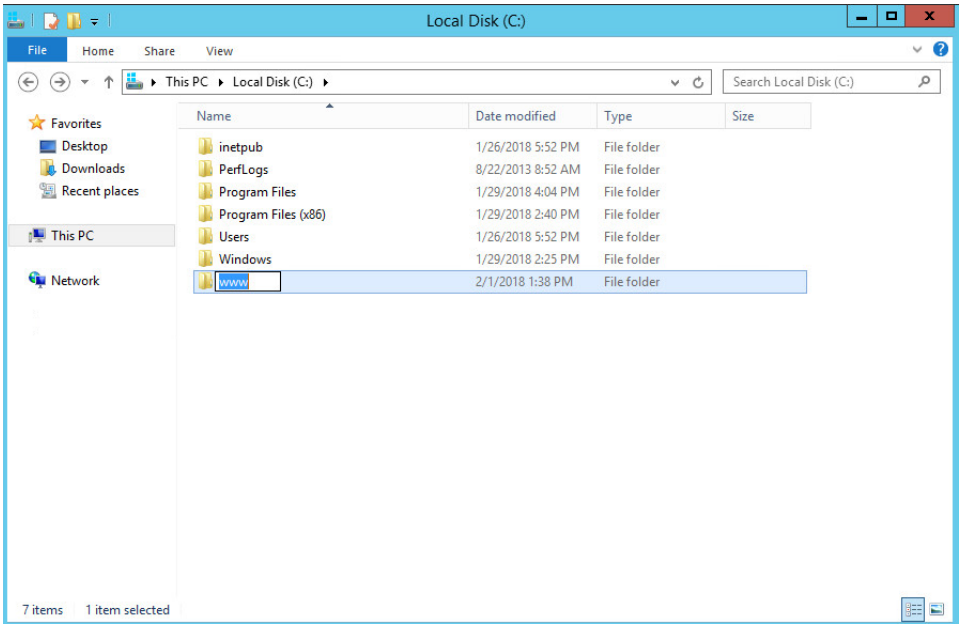
709
710 18. Click **Close.**

2.5.2 IIS Configuration

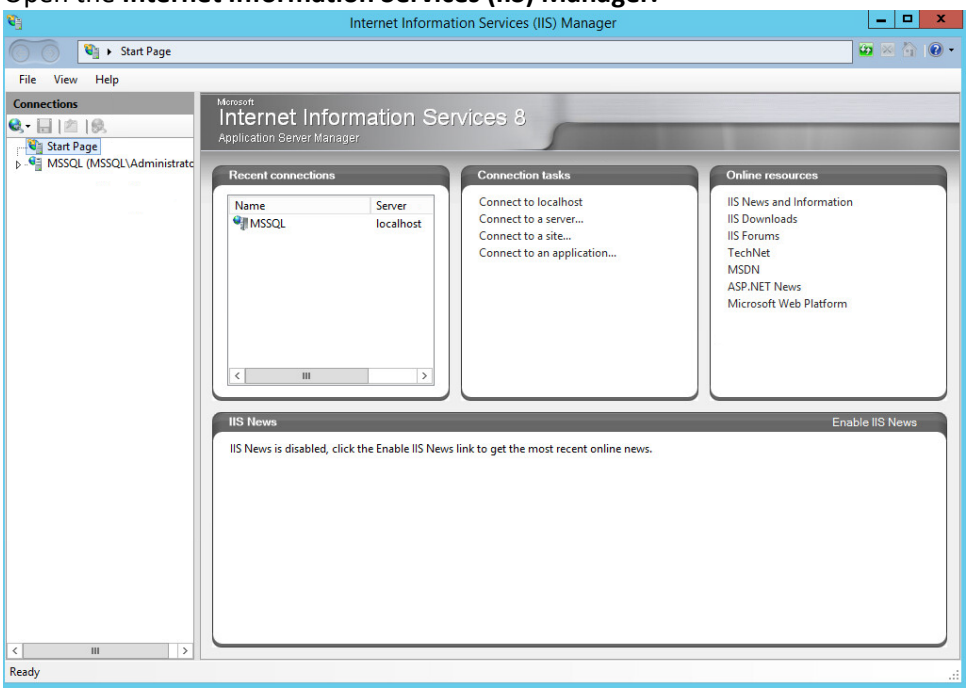
1. Open **Windows Explorer** and click **This PC.**



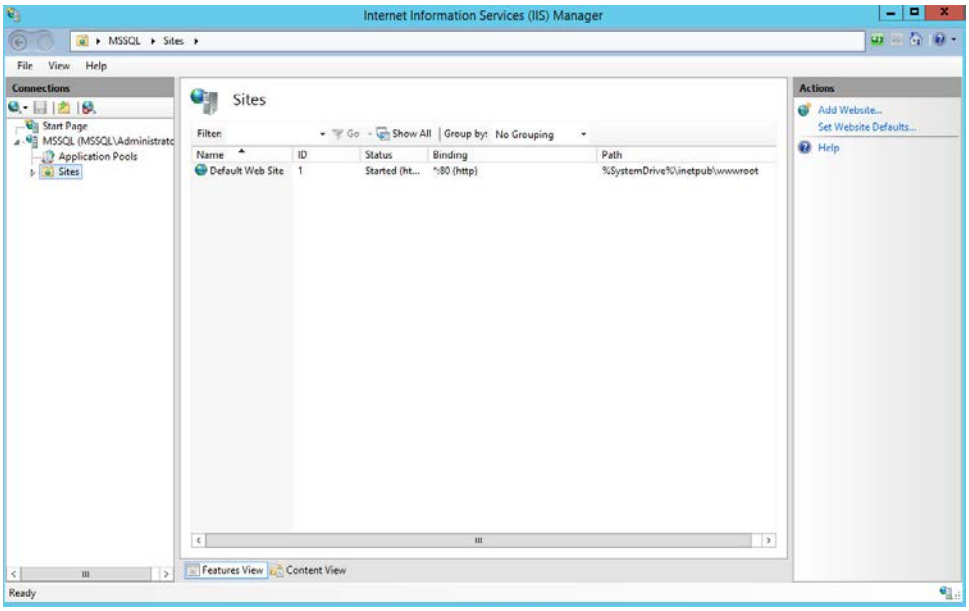
2. Right-click, and select **Create Folder.**
3. Name the folder **www.**



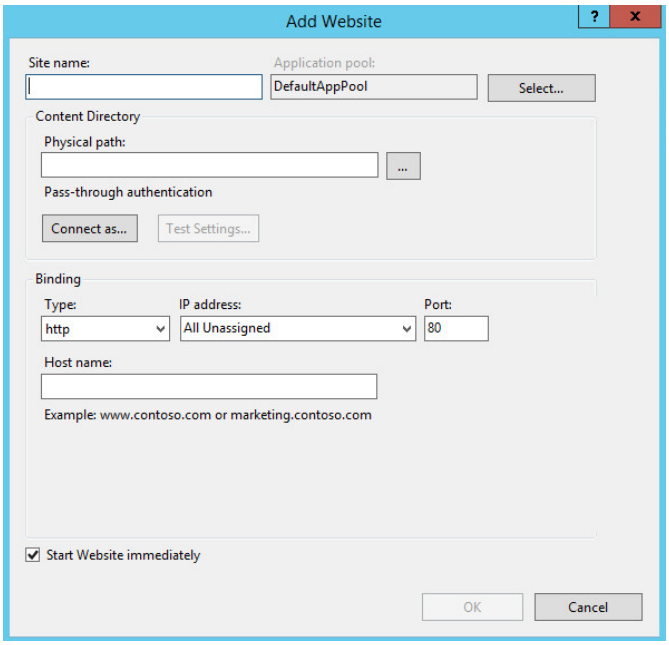
4. Open the **Internet Information Services (IIS) Manager.**



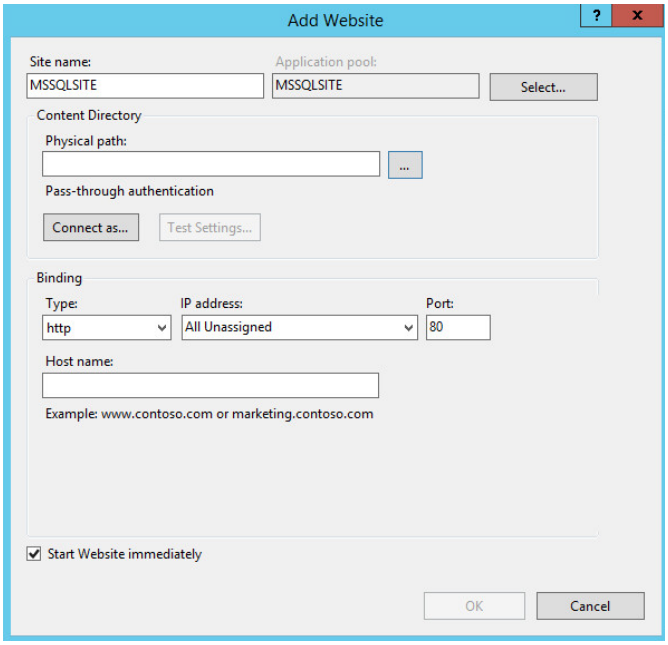
5. Click the arrow next to **MSSQL** (or the chosen name of the server).
6. Click **Sites**.



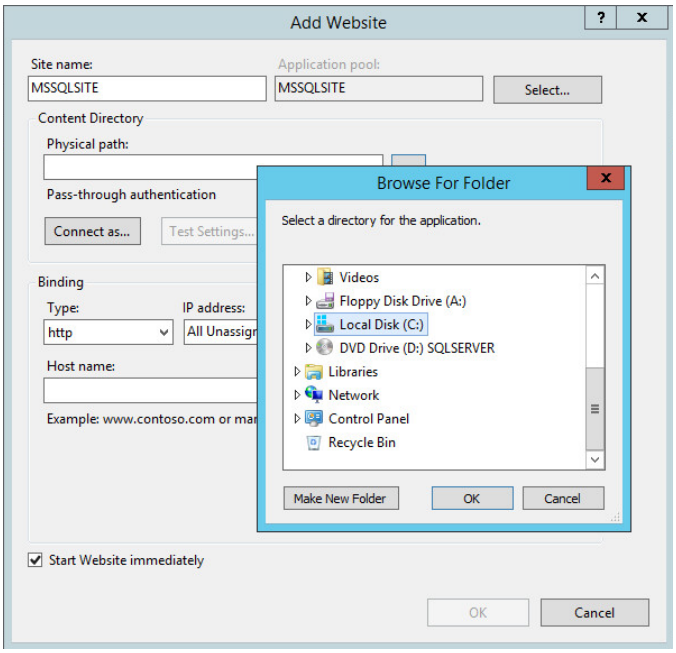
7. Click **Add Website….**



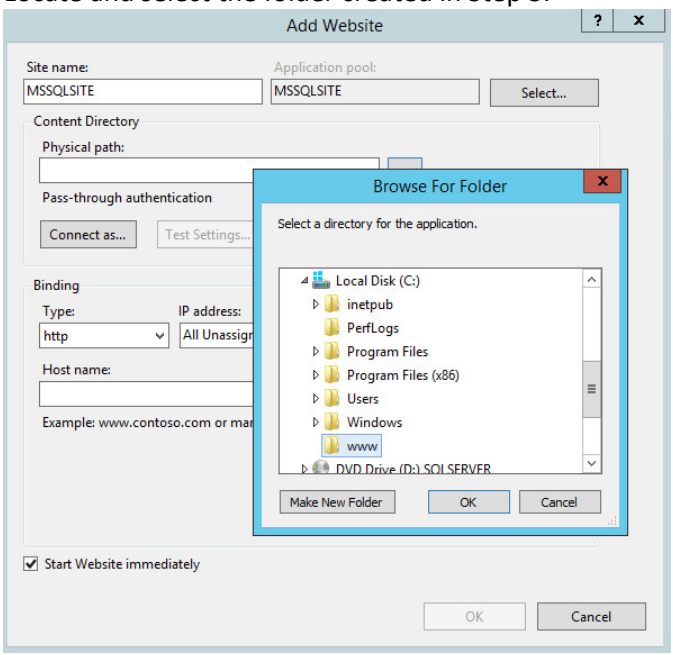
8. Enter the desired site name.



9. Click **…** under **Physical path:.**

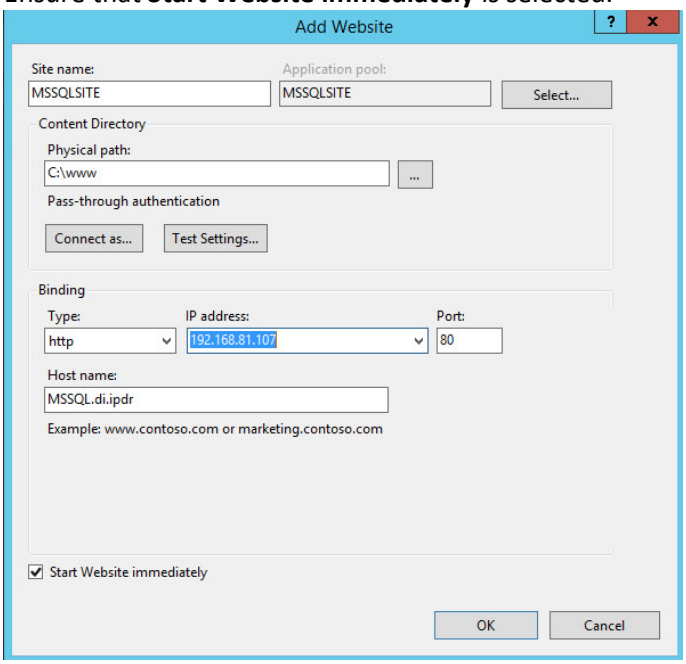


10. Locate and select the folder created in Step 3.



11. Click **OK.**
12. Set **Type** to **http** and **Port** to **80.**
13. Ensure 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.



15. Click **OK.**

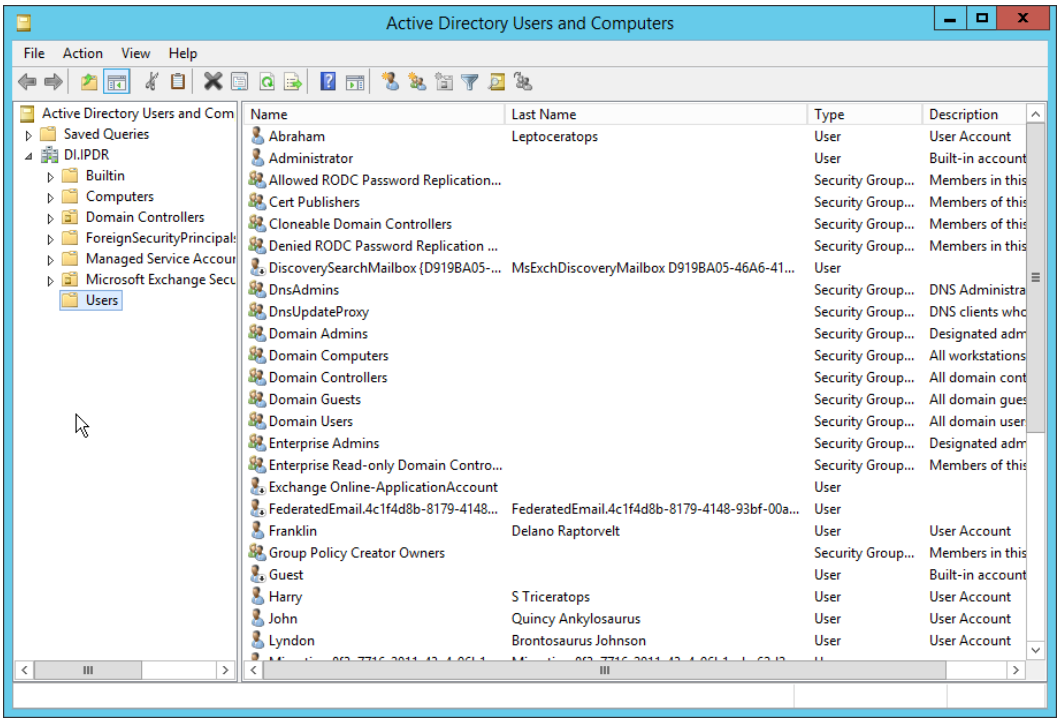
2.6 Semperis Directory Services Protector

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:

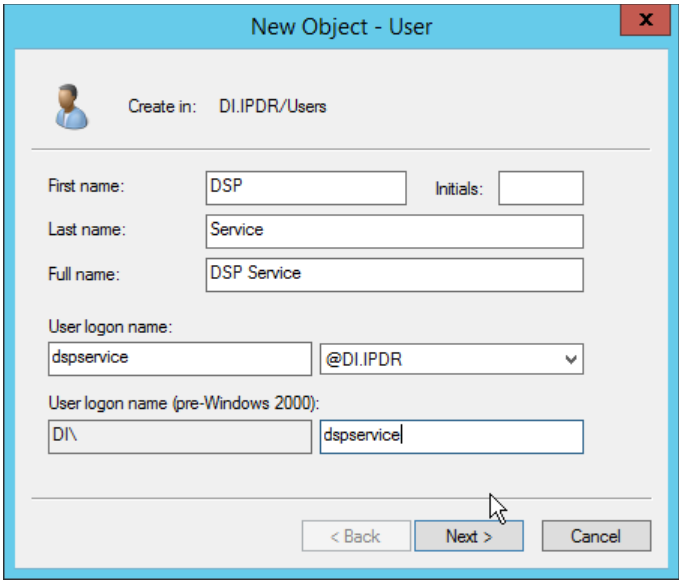
- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- Joined to the Active Directory Domain it is protecting
- Either the installer for SQL Express Advanced or connection information and credentials for a full version of Microsoft SQL (MSSQL)

2.6.1 Configure Active Directory for Semperis DSP

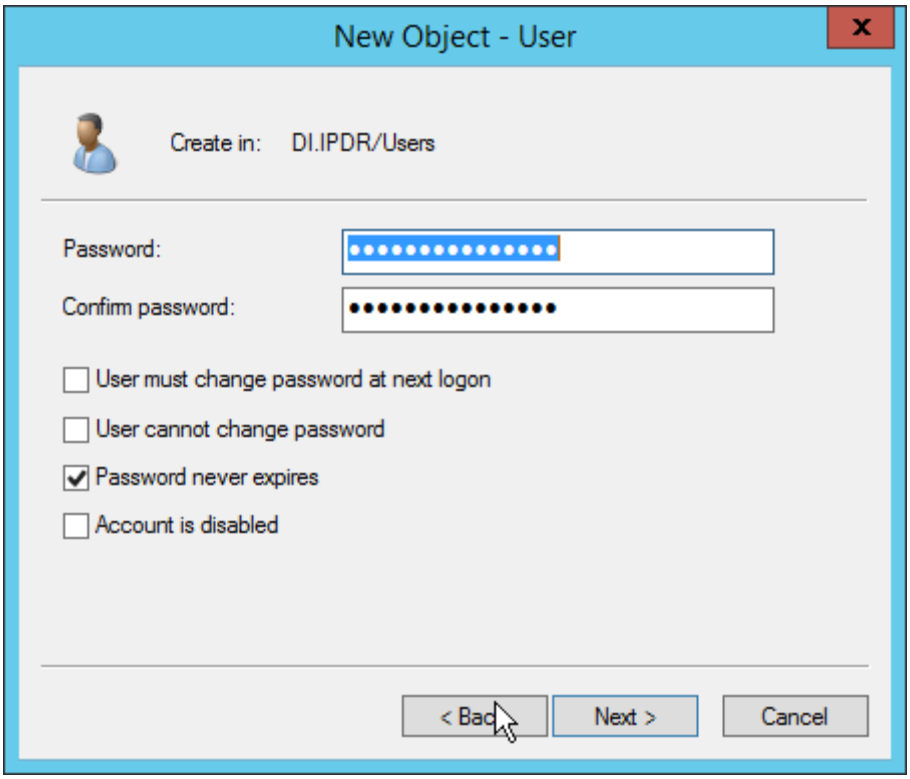
1. Open **Active Directory Users and Computers.**



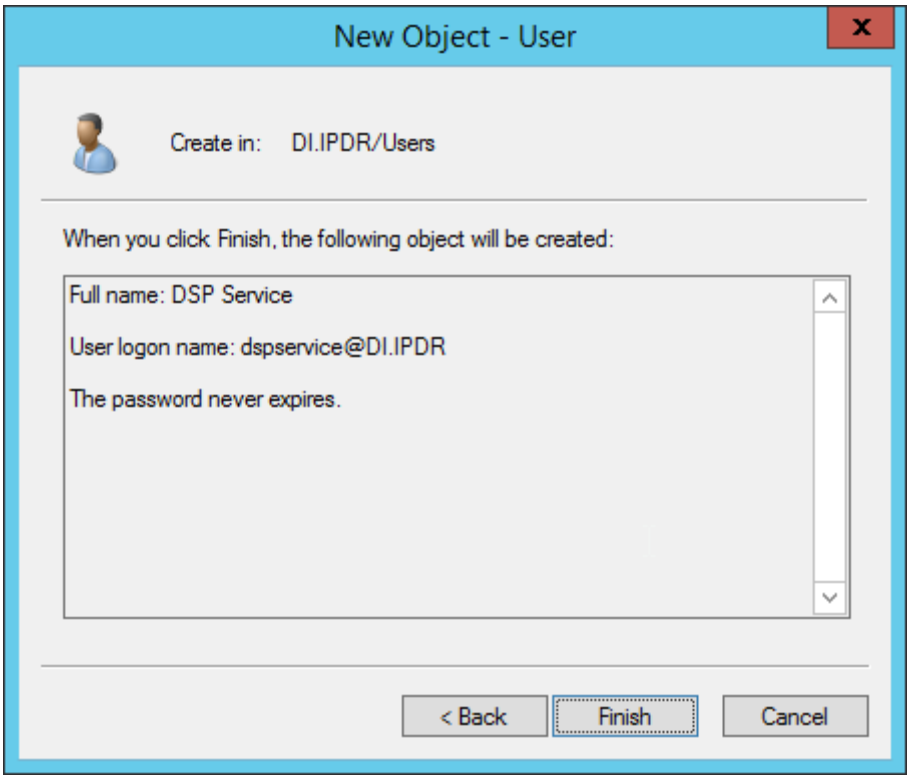
2. Right-click **Users** in the left pane, and select **New > User.**
3. Enter the information for a new user for the DSP service.



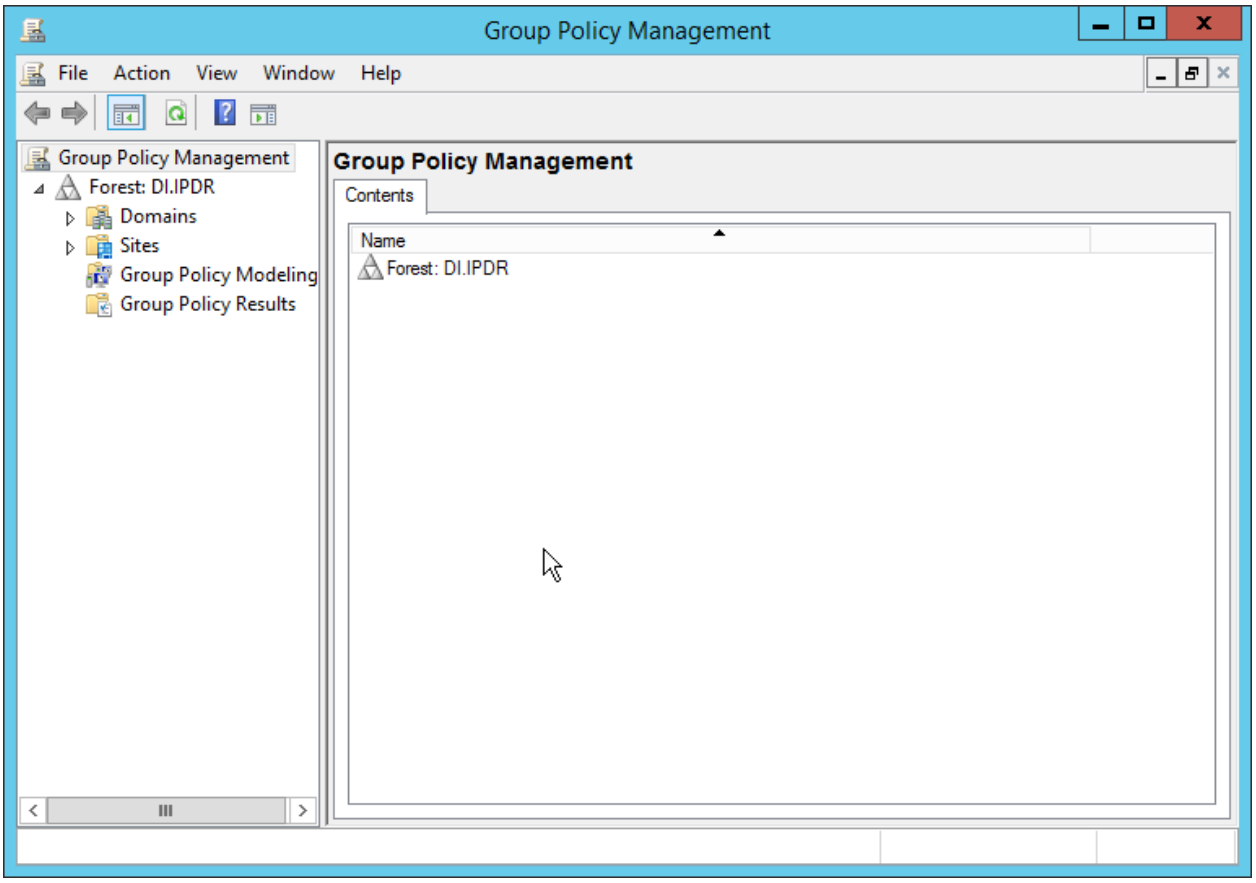
4. Click **Next.**
5. Enter a **password** twice for this user.
6. Set the password policy.


New Object - User
Create in: DI.IPDR/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel

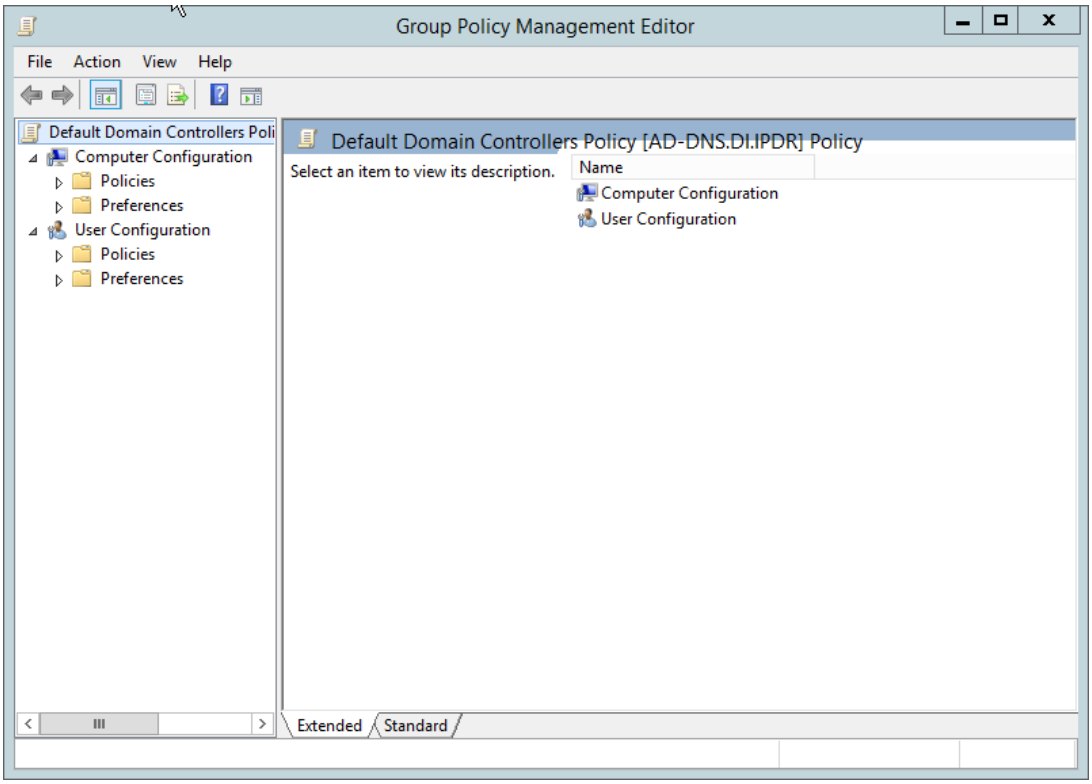
7. Click **Next.**



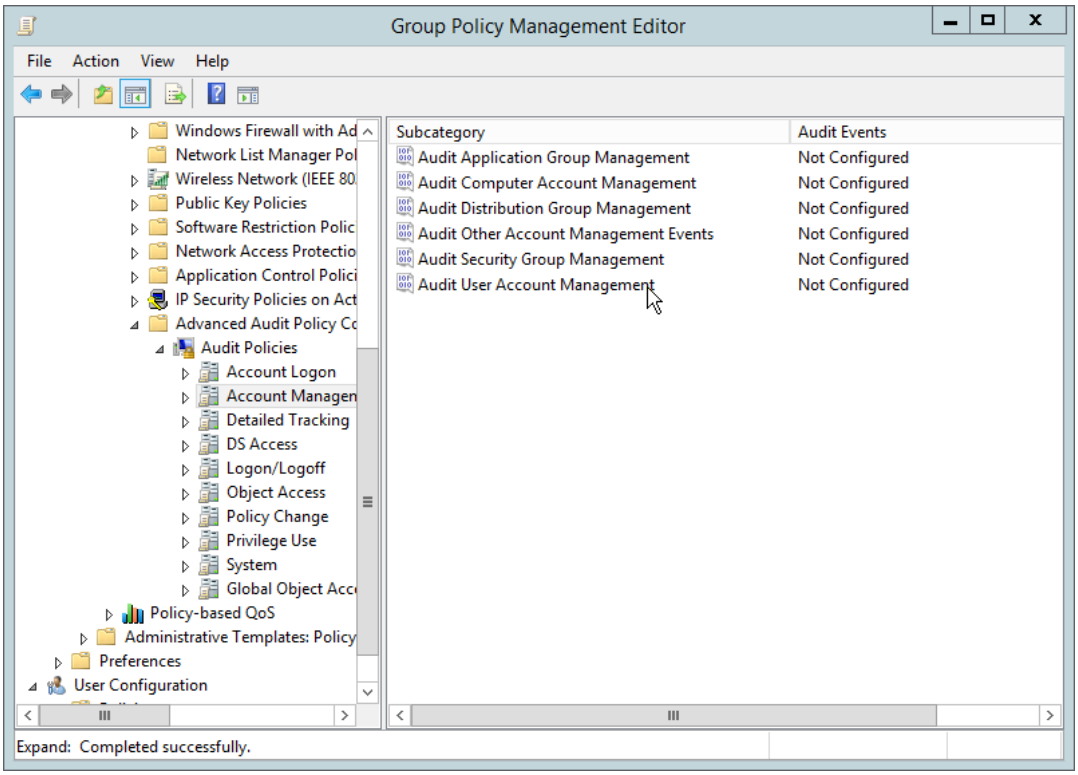
8. Click **Finish.**
9. Open **Group Policy Management.**



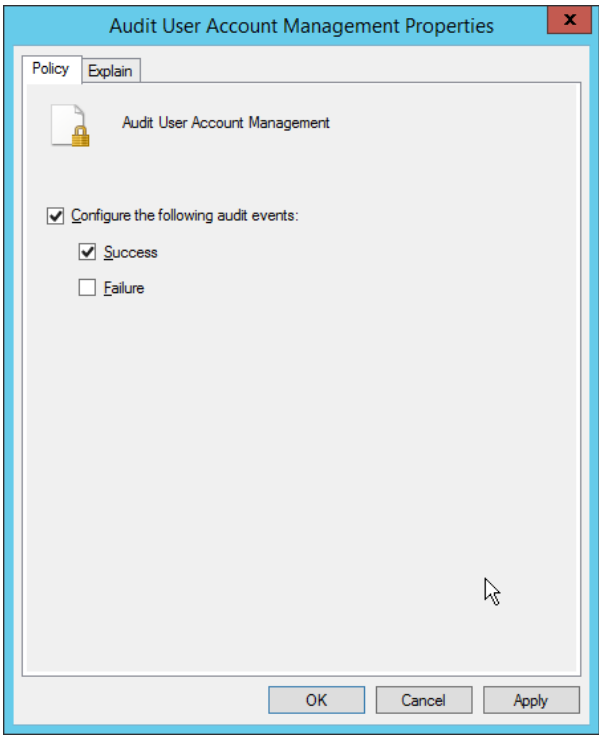
10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy,** and click **Edit.**



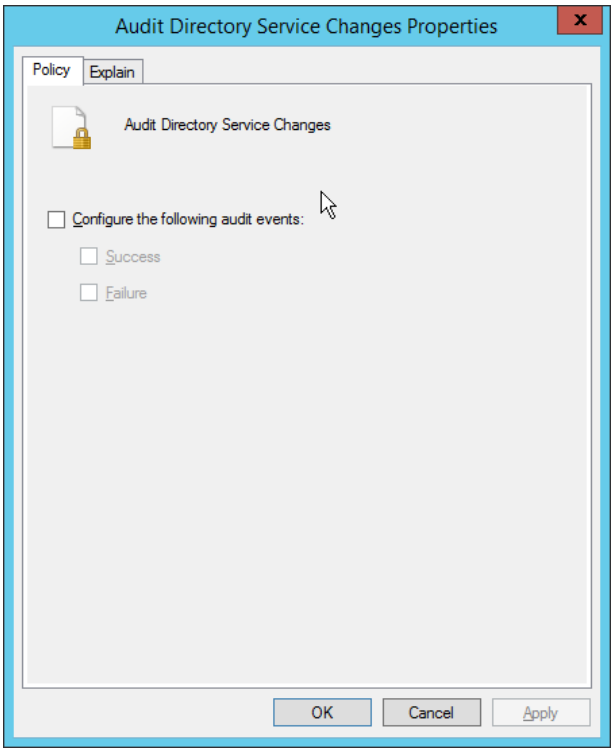
11. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management.**



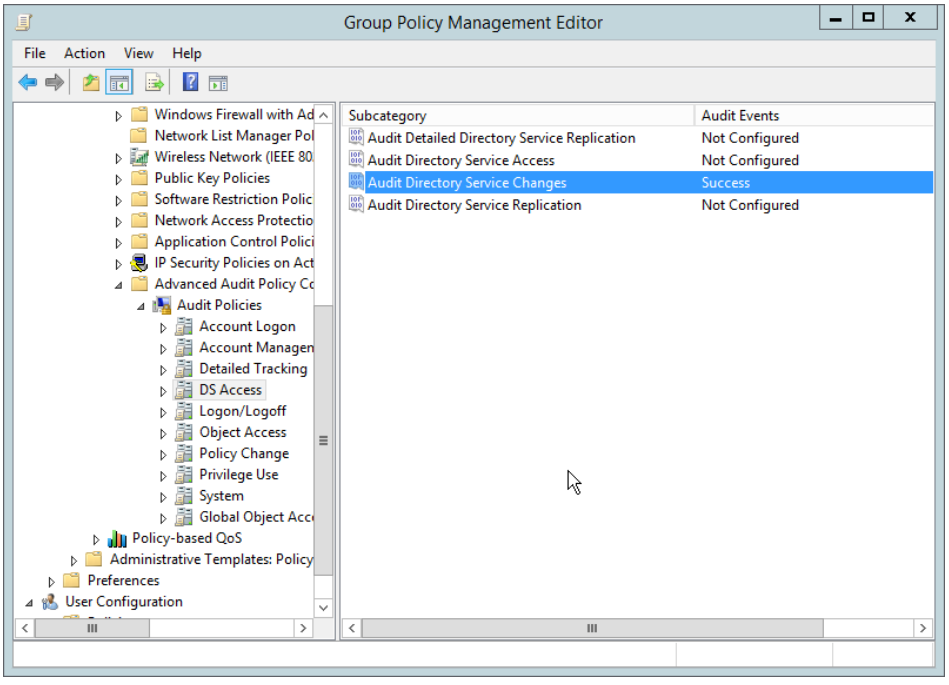
12. Edit the **Audit User Account Management** field by double-clicking it.
13. Check the box next to **Configure the following audit events.**
14. Check the box next to **Success.**



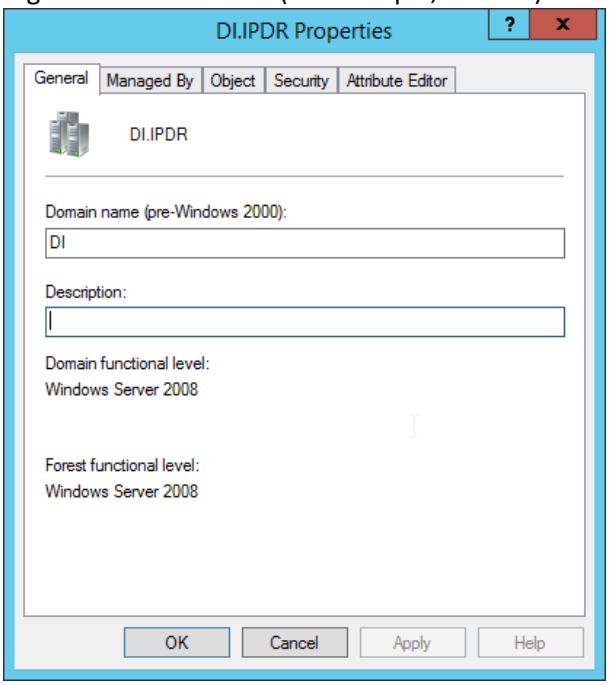
15. Click **OK.**
16. Go to **Audit Policies > DS Access.**
17. Double-click **Audit Directory Services Changes.**



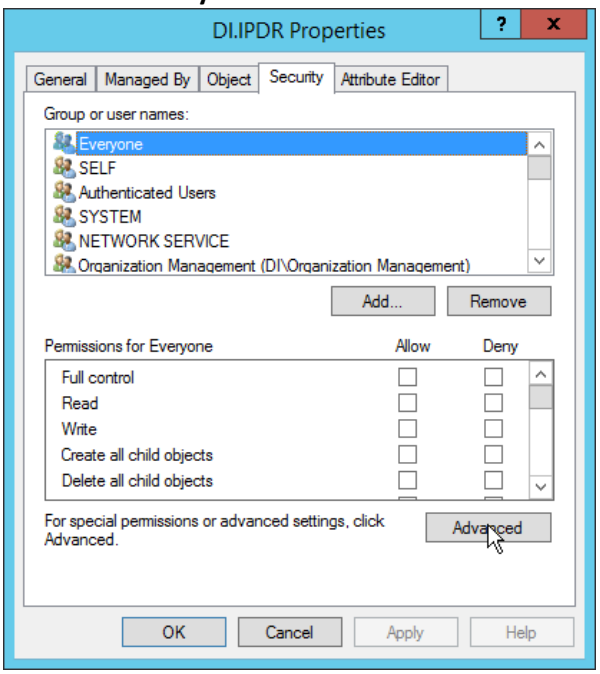
18. Check the box next to **Configure the following audit events.**
19. Check the box next to **Success.**
20. Click **OK.**



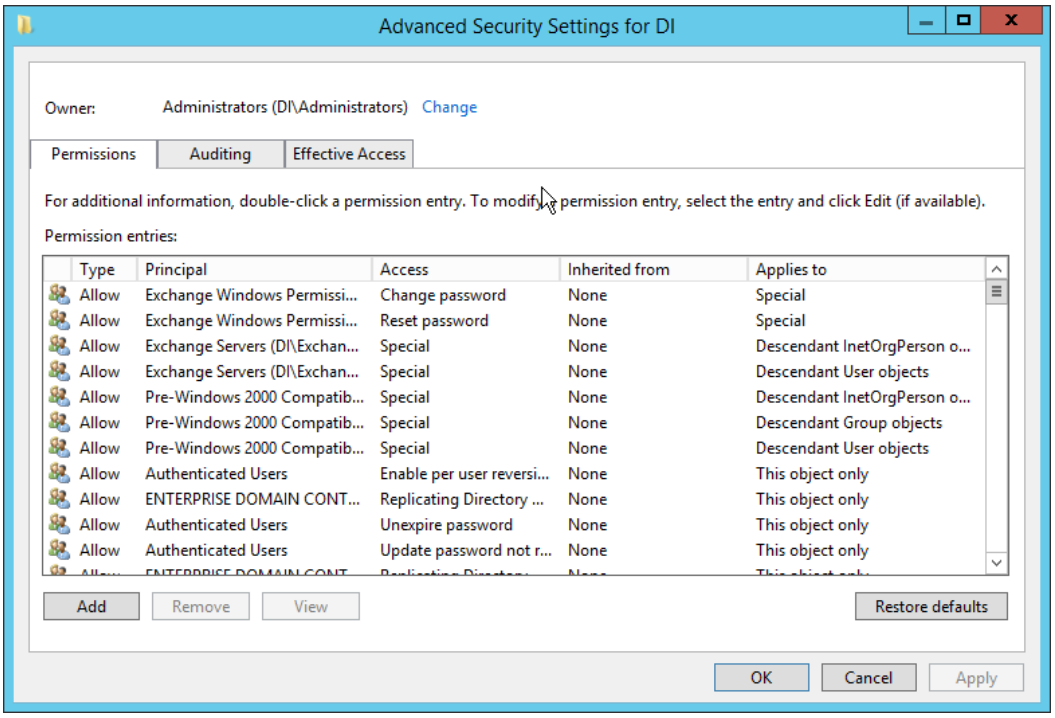
21. Open **Active Directory Users and Computers.**
22. Ensure **View > Advanced Features** is enabled.
23. Right-click the **domain** (for example, DI.IPDR) created earlier, and click **Properties.**



24. Click the **Security** tab.



25. Click **Advanced.**

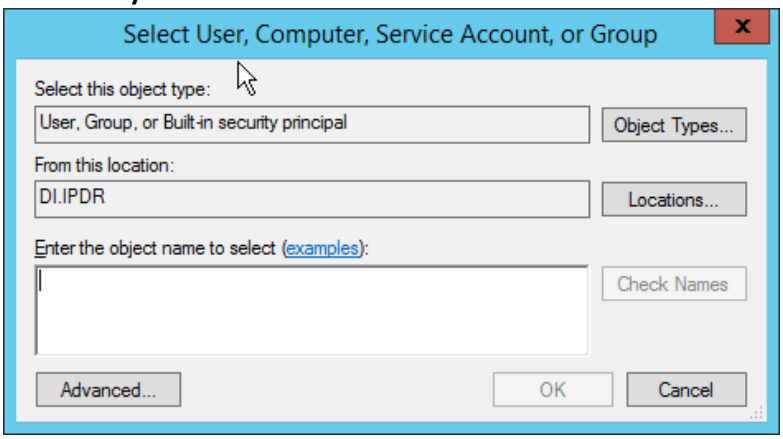


788

789 26. Click the **Auditing** tab.

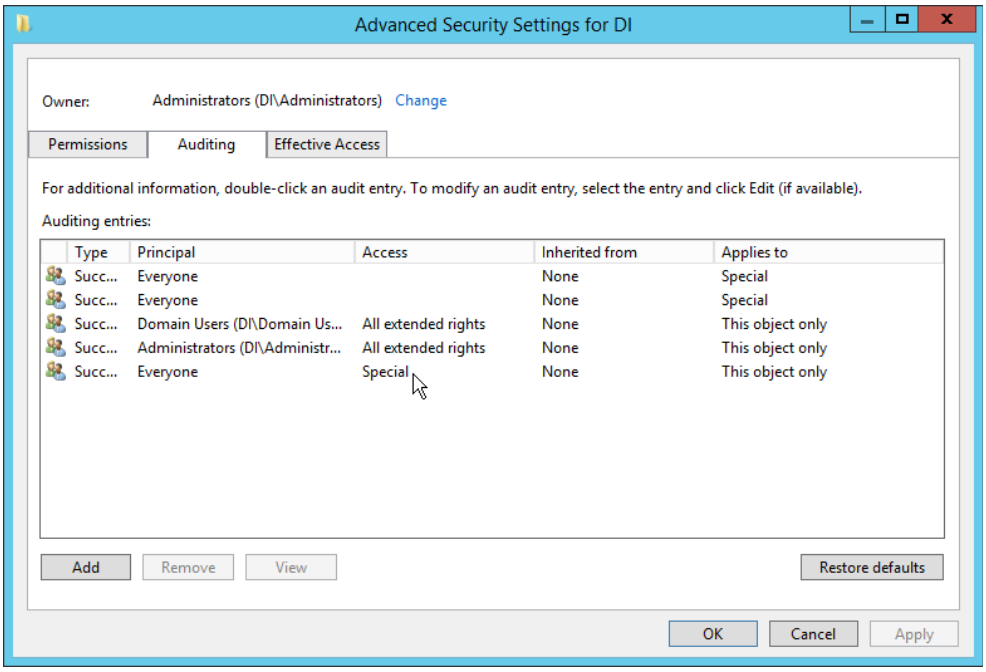
790 27. Click **Add.**

791 28. Enter **Everyone.**

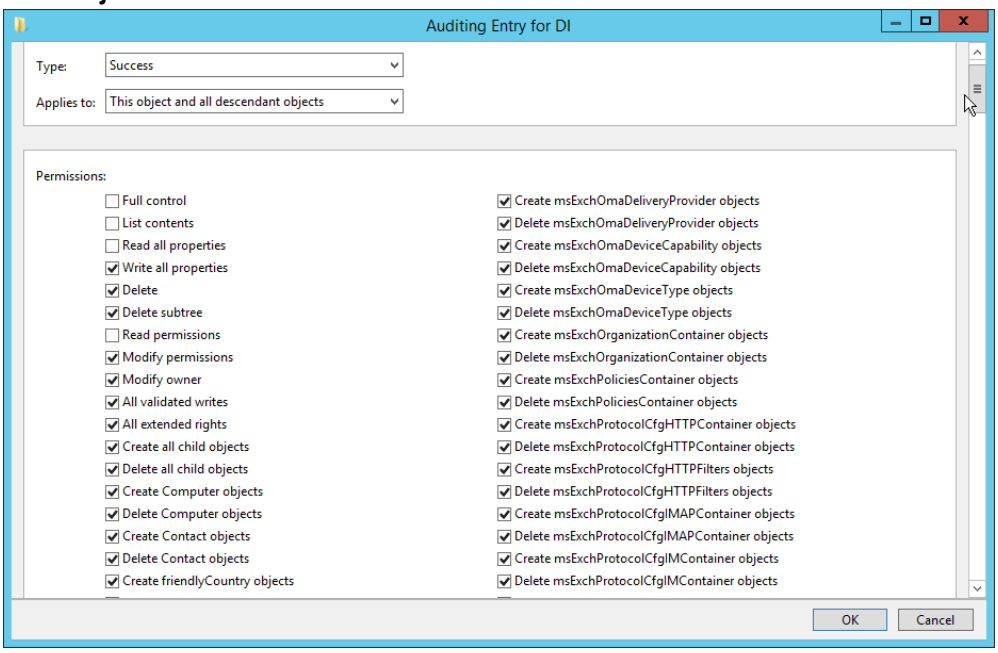


792

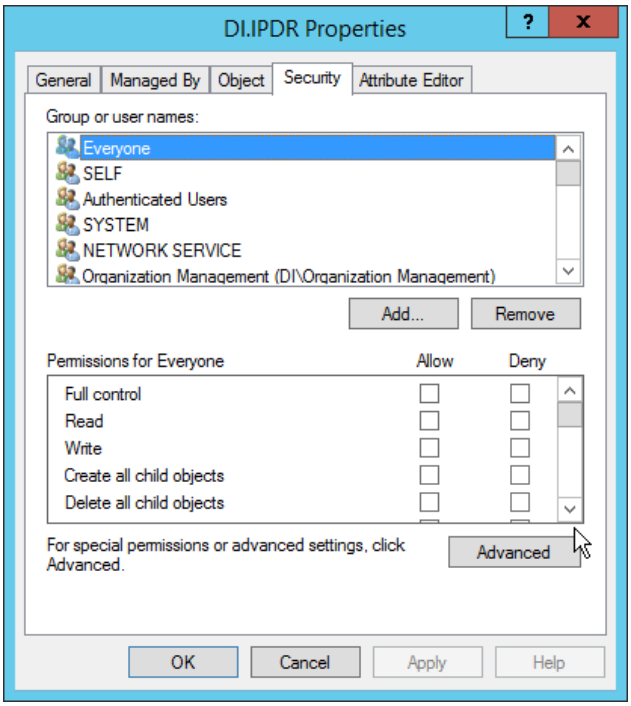
793 29. Click **OK.**



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.**



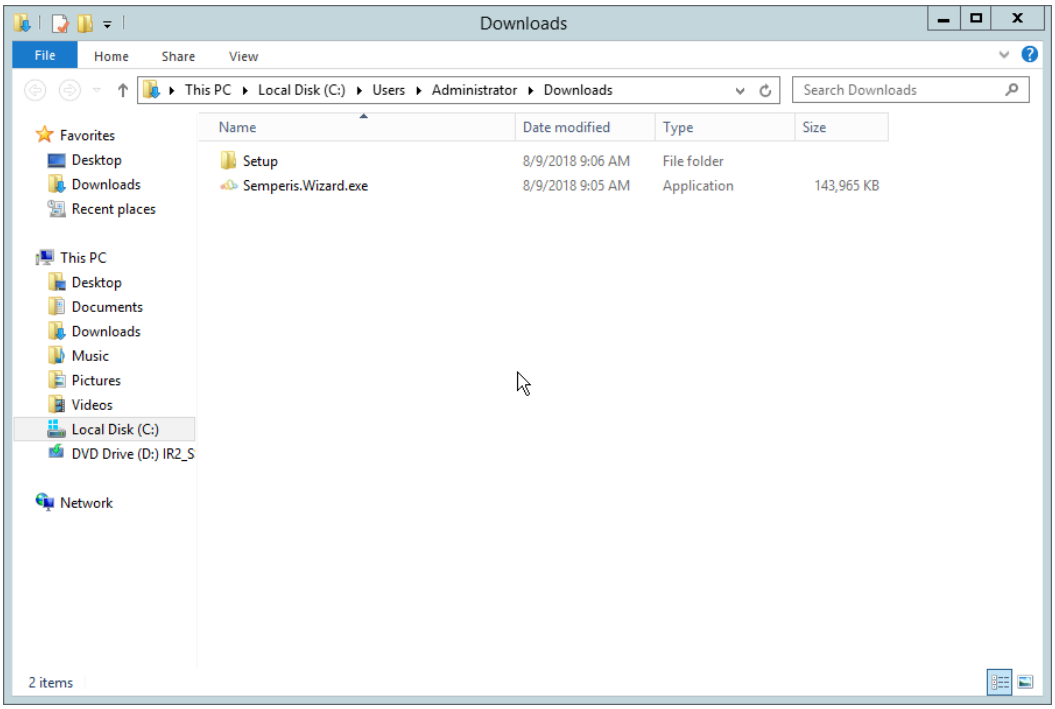
32. Click **OK.**



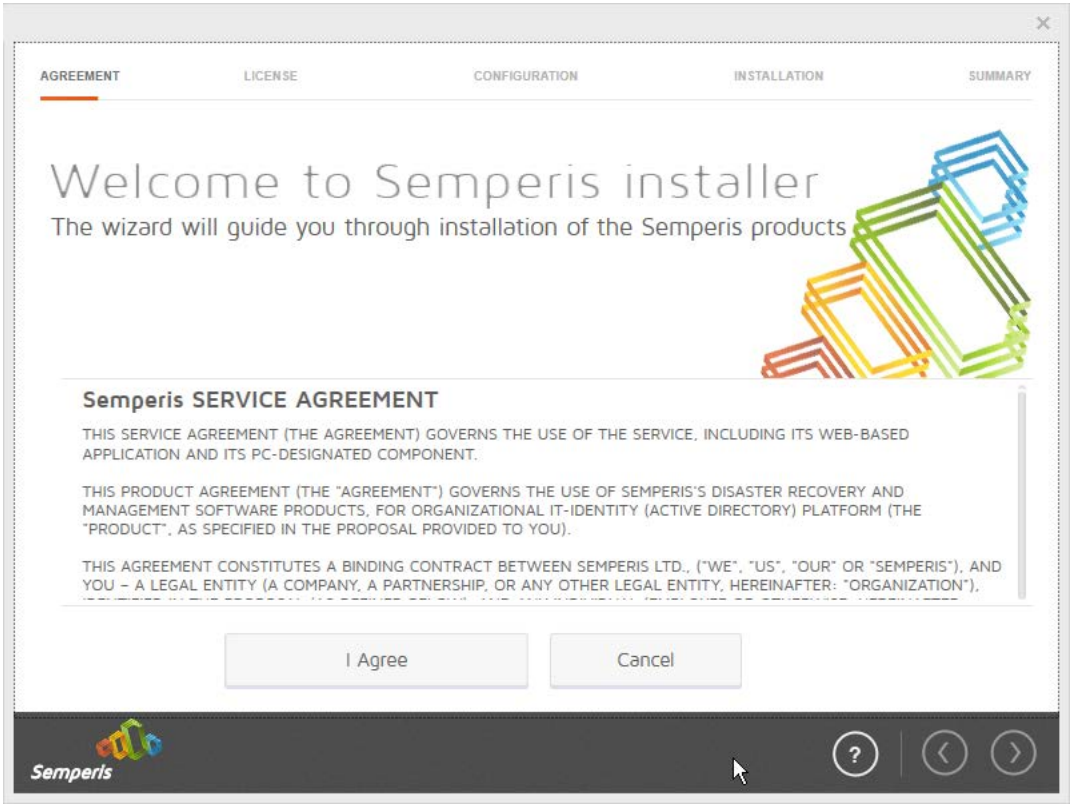
33. Click **OK.**

2.6.2 Install Semperis DSP

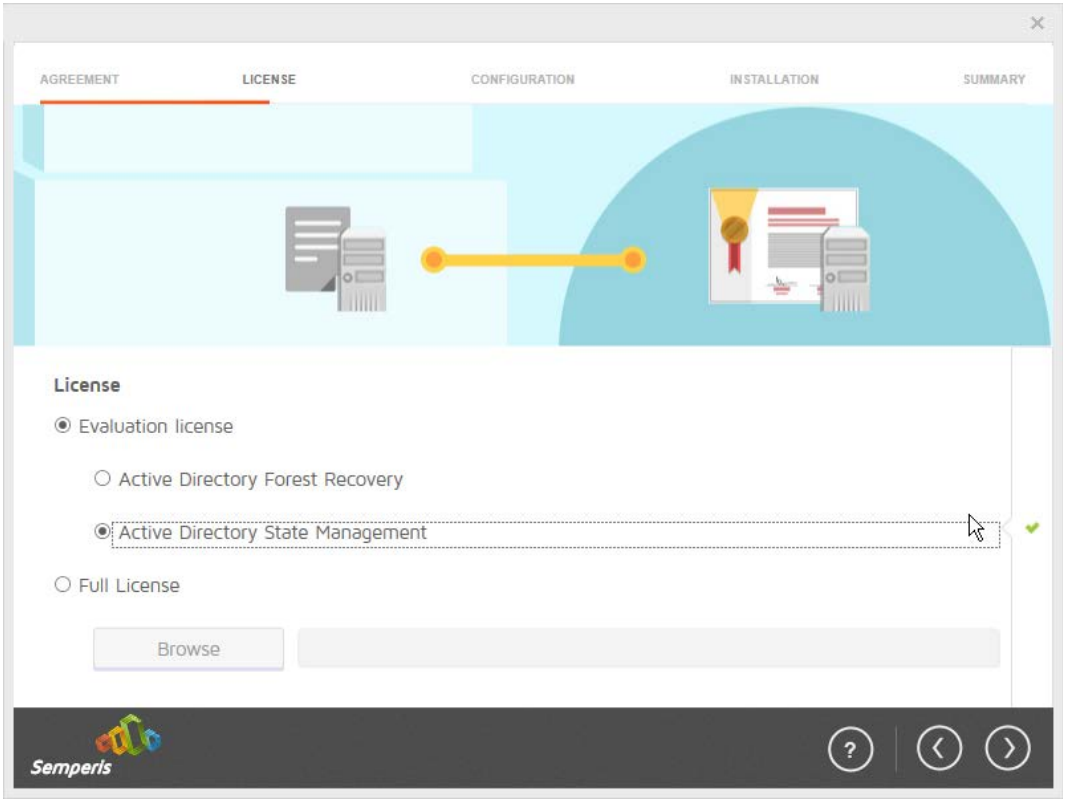
1. If you are using a local SQL Express Advanced server, place the **SQLEXPRADV_x64_ENU.exe** installer in a directory called *Setup,* and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it). If a SQL Express Advanced server is not being used, no **Setup** folder is required.



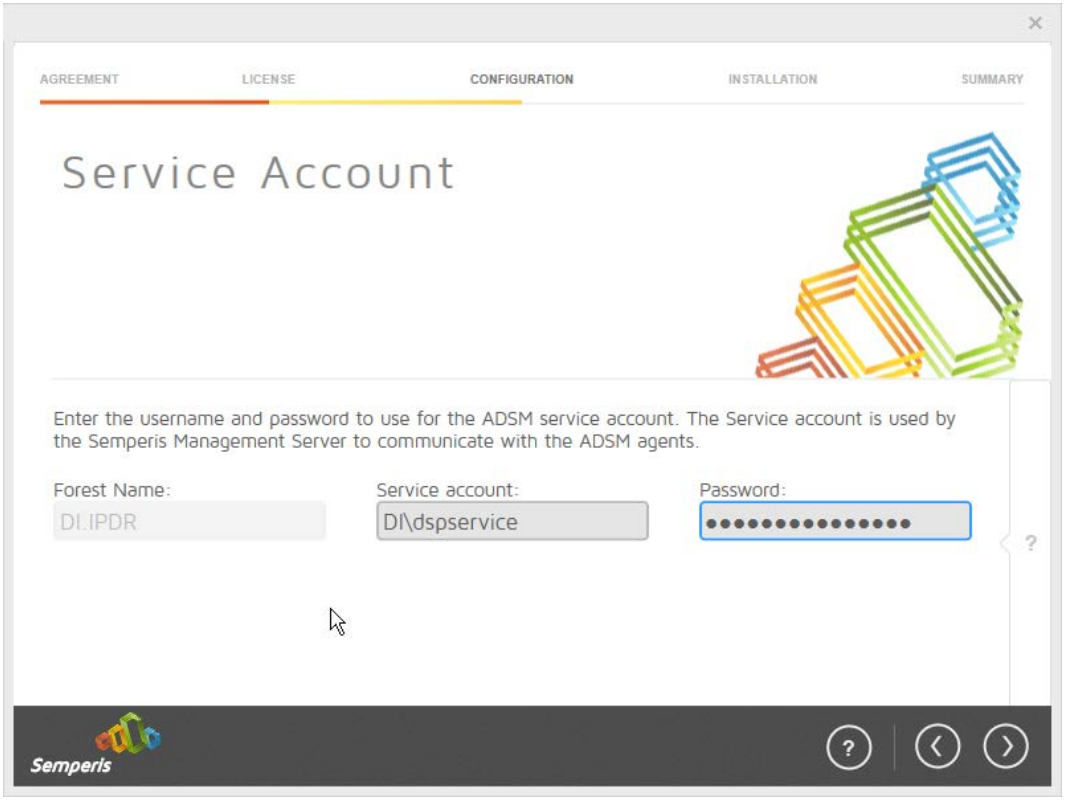
808
809 2. If prompted to restart the computer, do so.



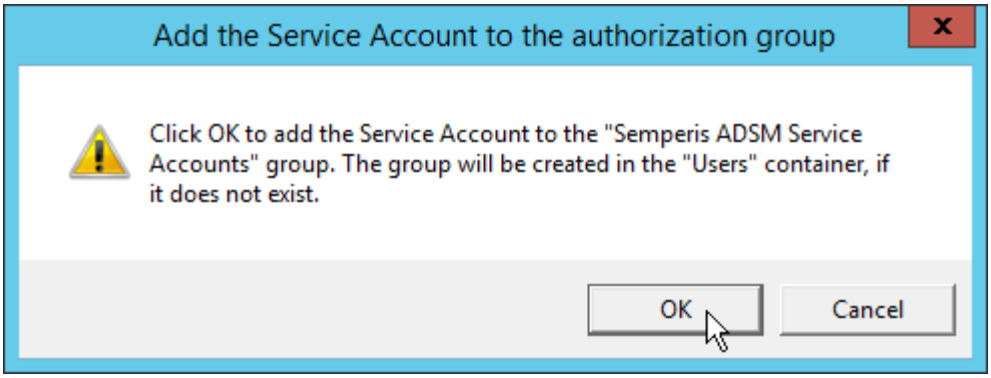
3. Click **I Agree.**
4. Select **Evaluation License.**
5. Select **Active Directory State Management.**



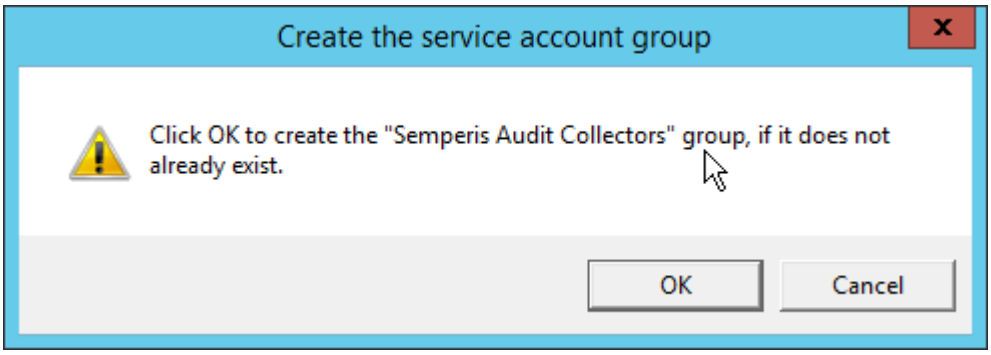
6. Click the **>** button.
7. Enter the **username** and **password** of the account created earlier.



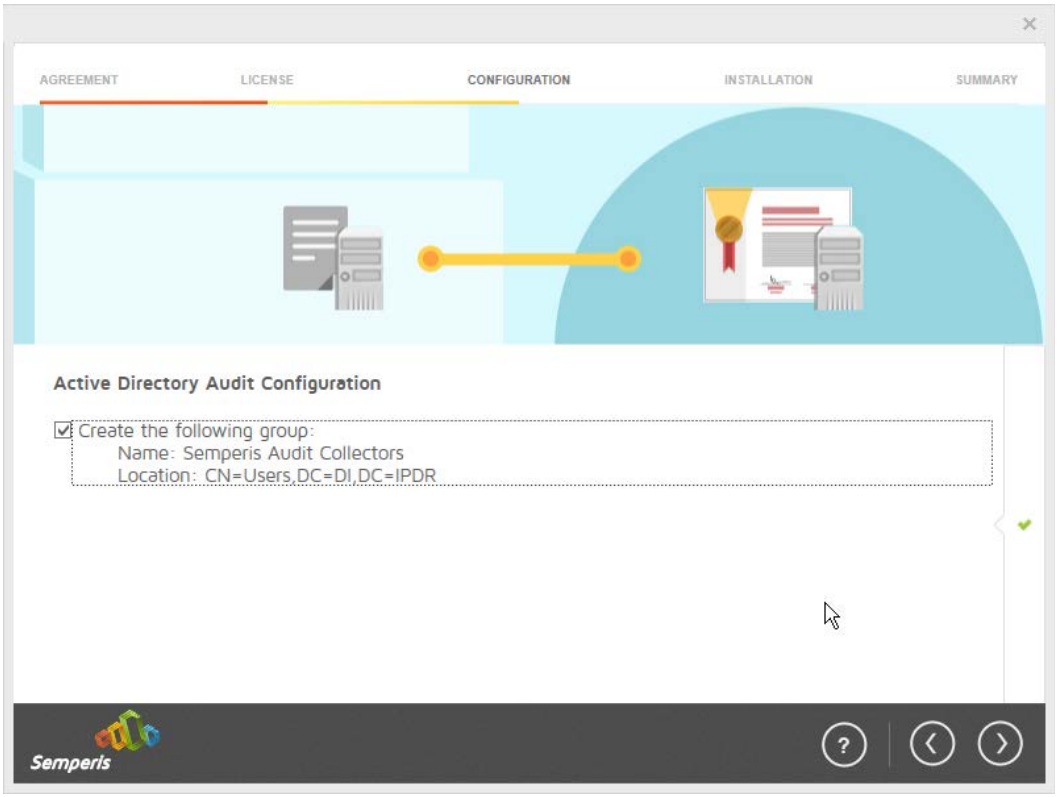
8. Click the **>** button.



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

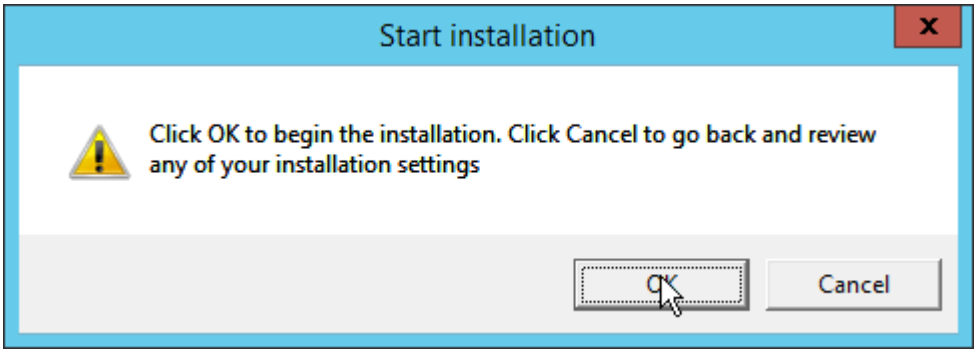


11. Click **OK.**

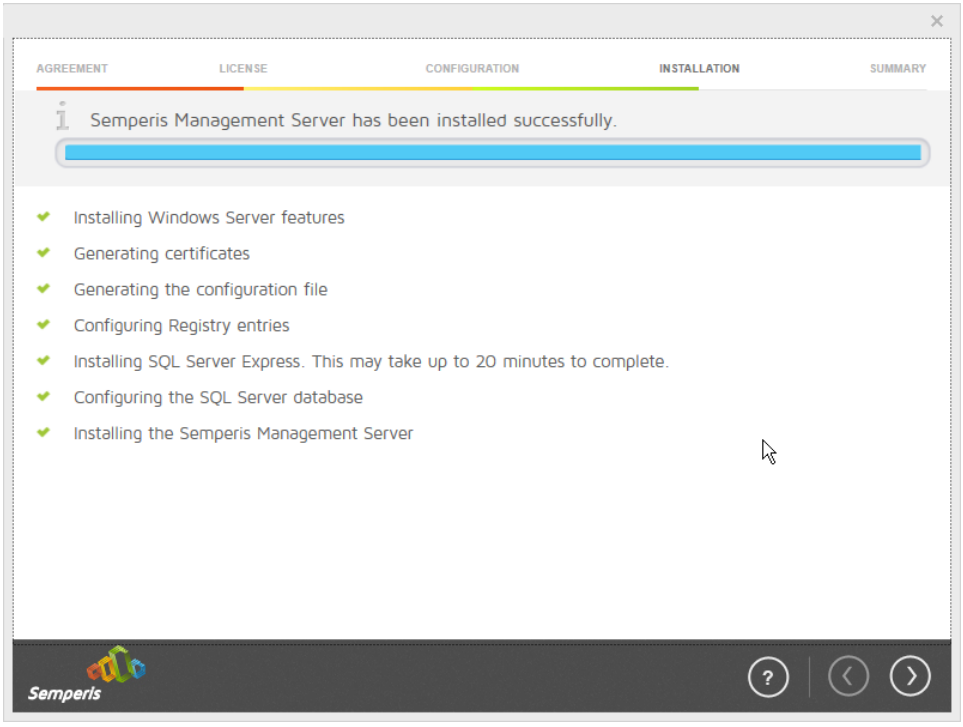


12. Click the **>** button.
13. Select the appropriate database option, and enter any required information.

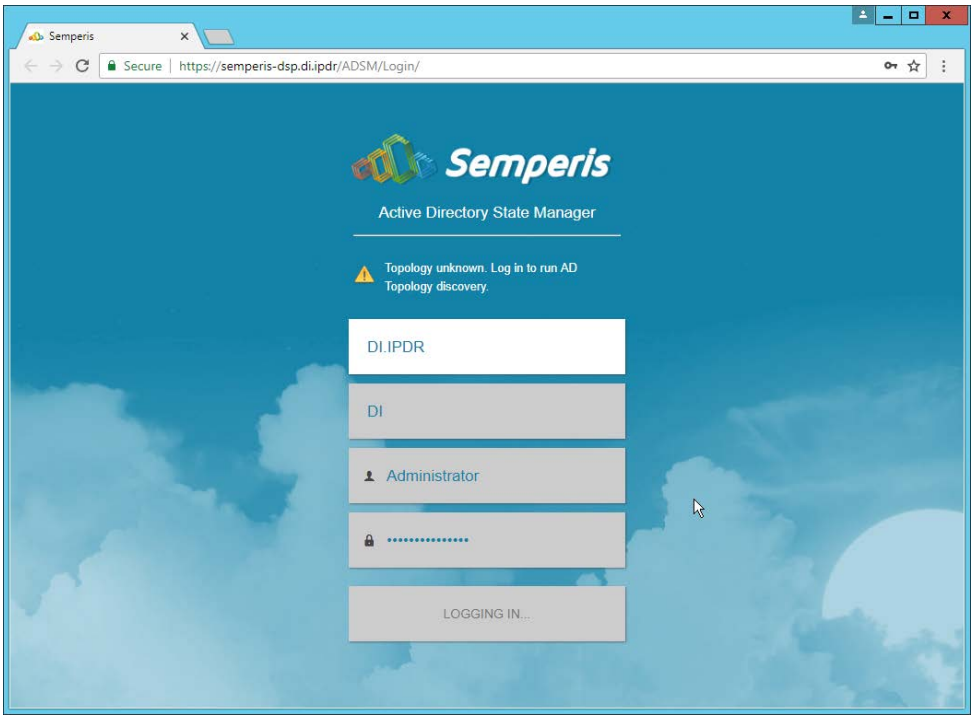
14. Click the **>** button.



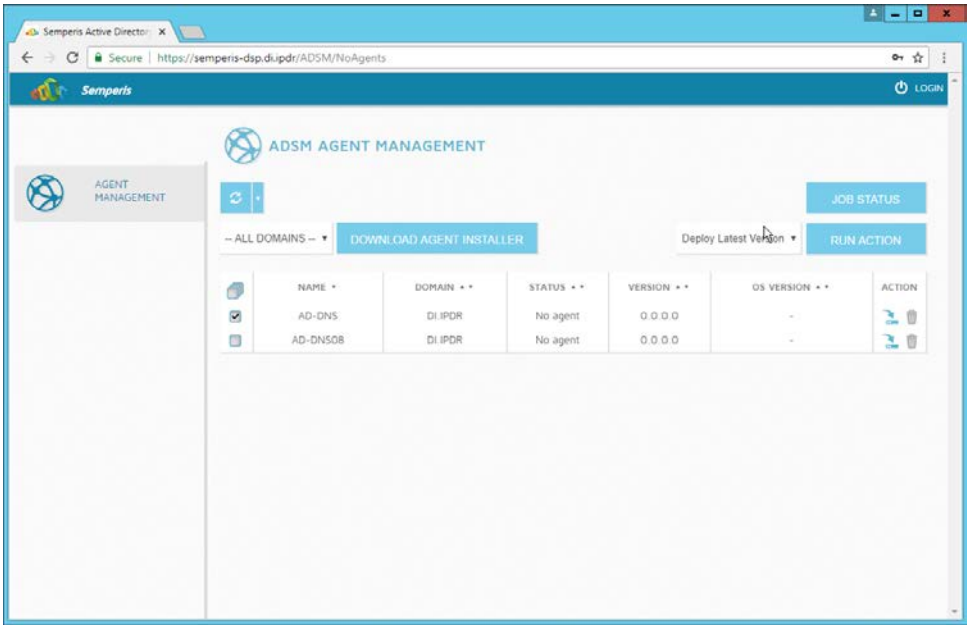
15. Click **OK.**



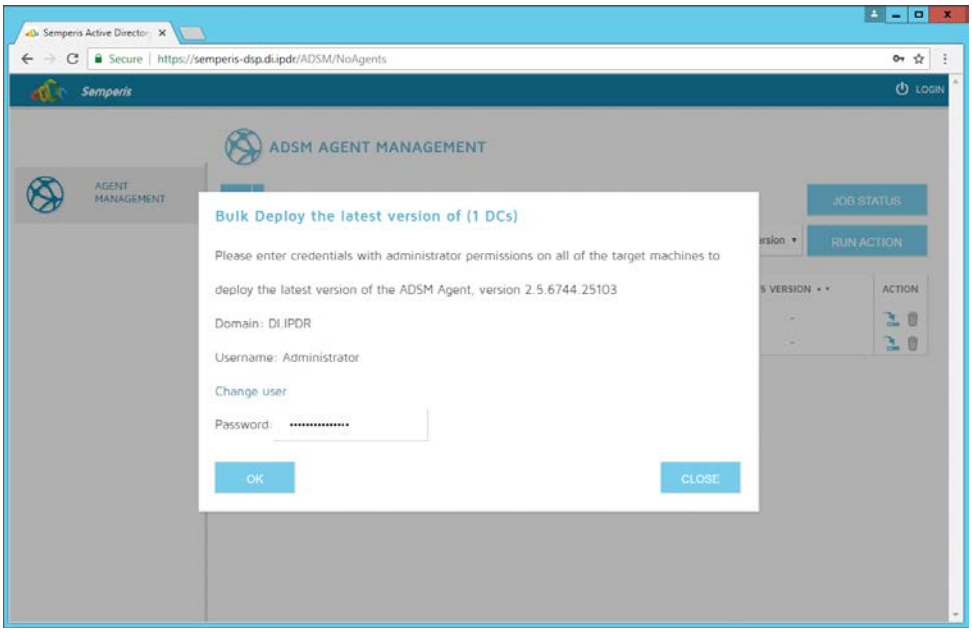
16. Click the **>** button after the installation completes.
17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector.**
18. On the login page, enter the full domain as well as the NetBIOS name.
19. Enter the **username** and **password** of an administrator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



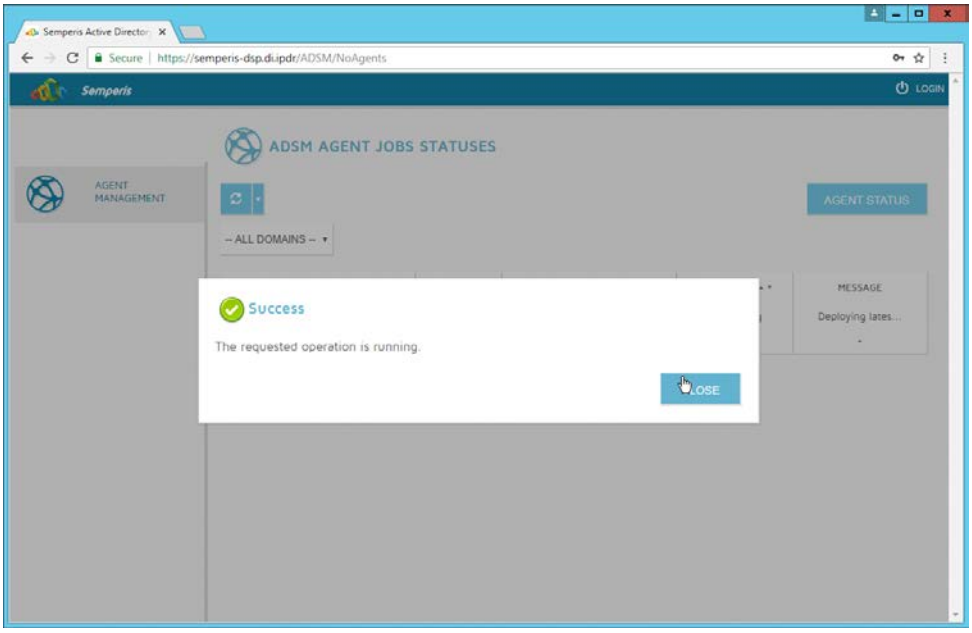
20. Click **Login.**
21. Check the box next to the domain controllers that should be monitored by DSP.



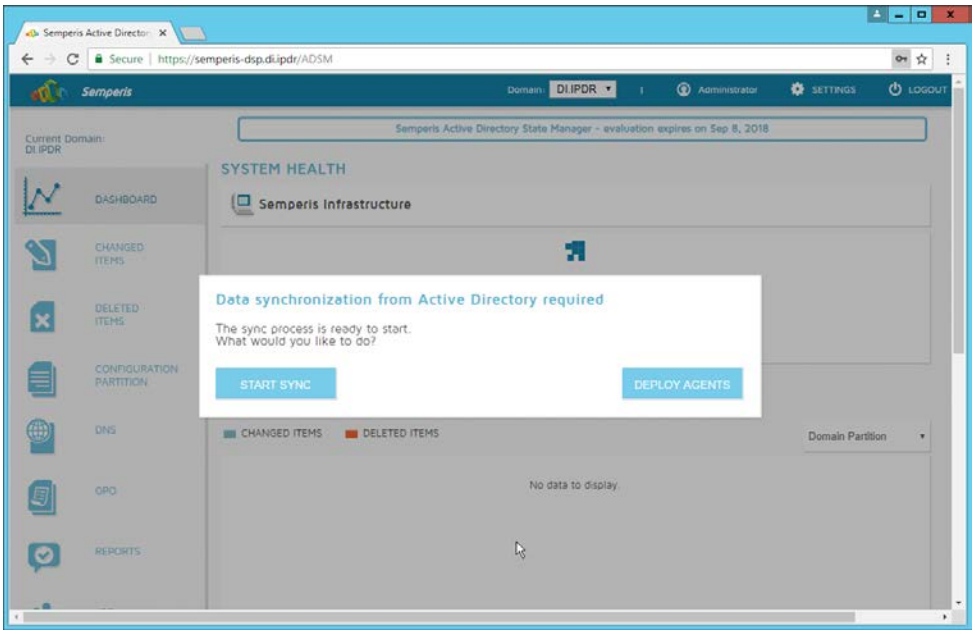
22. Click **Run Action.**
23. Enter the **password** for the account.



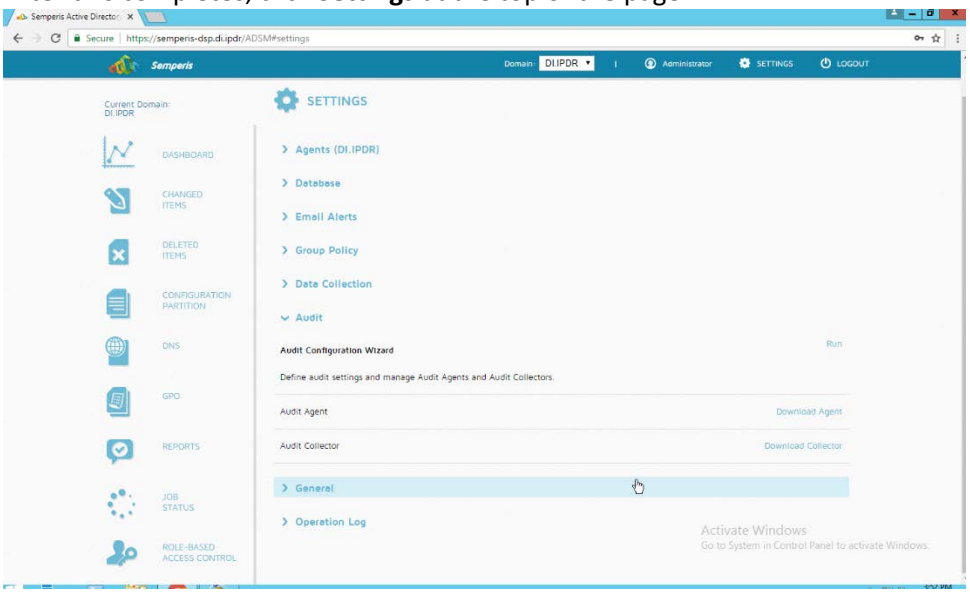
843
844 24. Click **OK.**



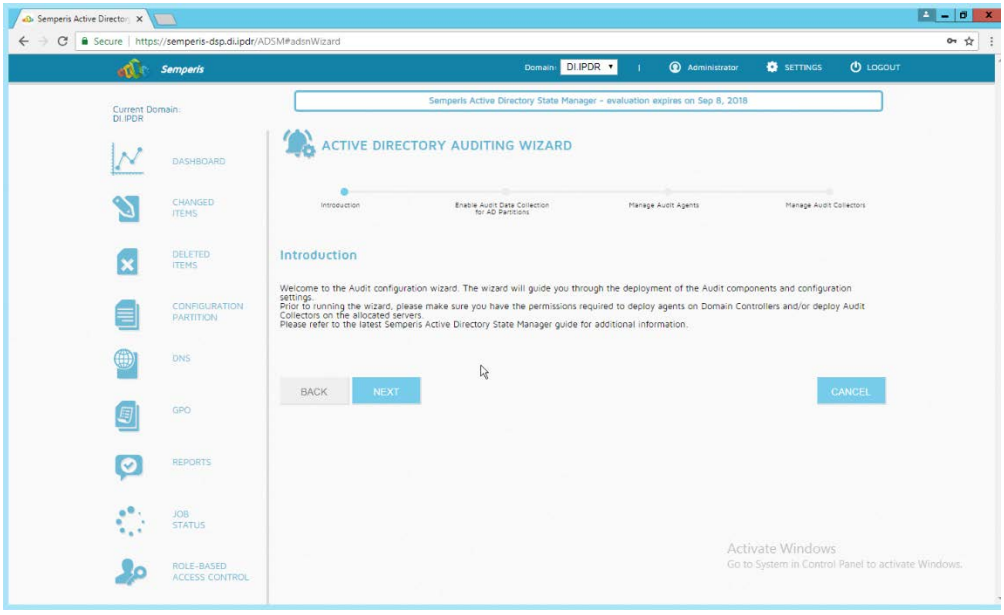
845
846 25. Click **Close.**
847 26. After the agent finishes deploying, click **Login** at the top of the page, and log in.



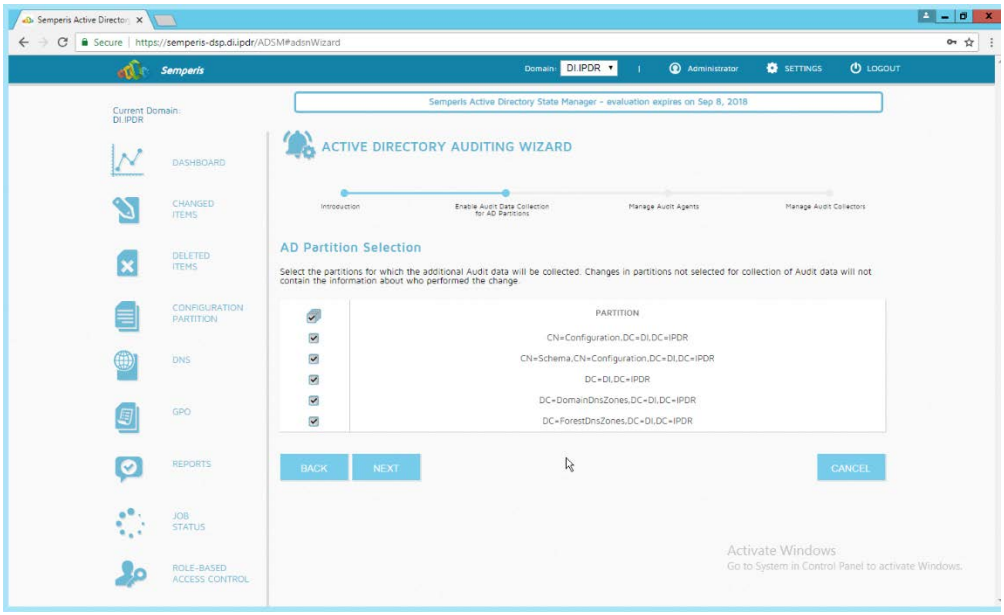
27. Click **Start Sync.**
28. After this completes, click **Settings** at the top of the page.



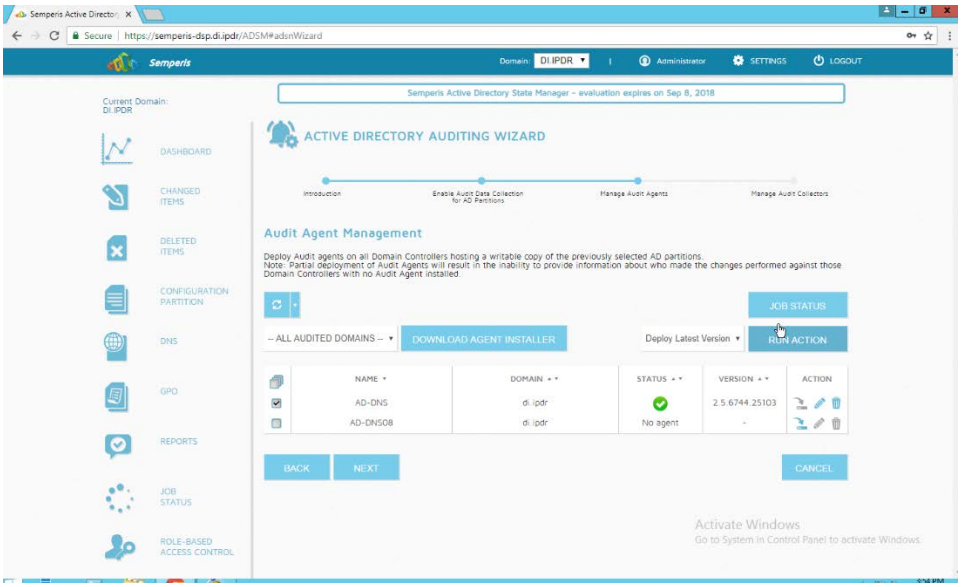
29. Click **Audit.**
30. Click **Run.**



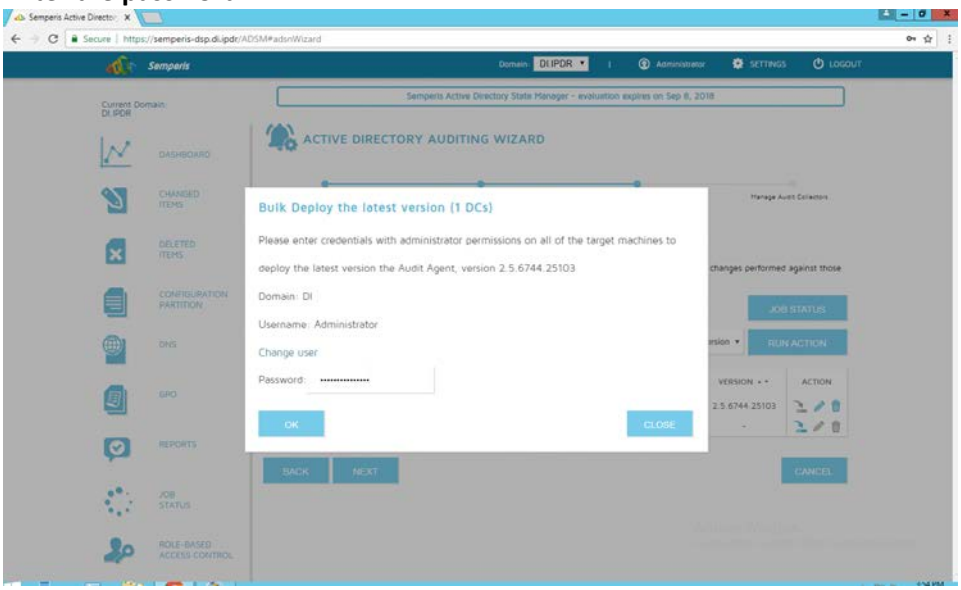
854
855 31. Click **Next.**



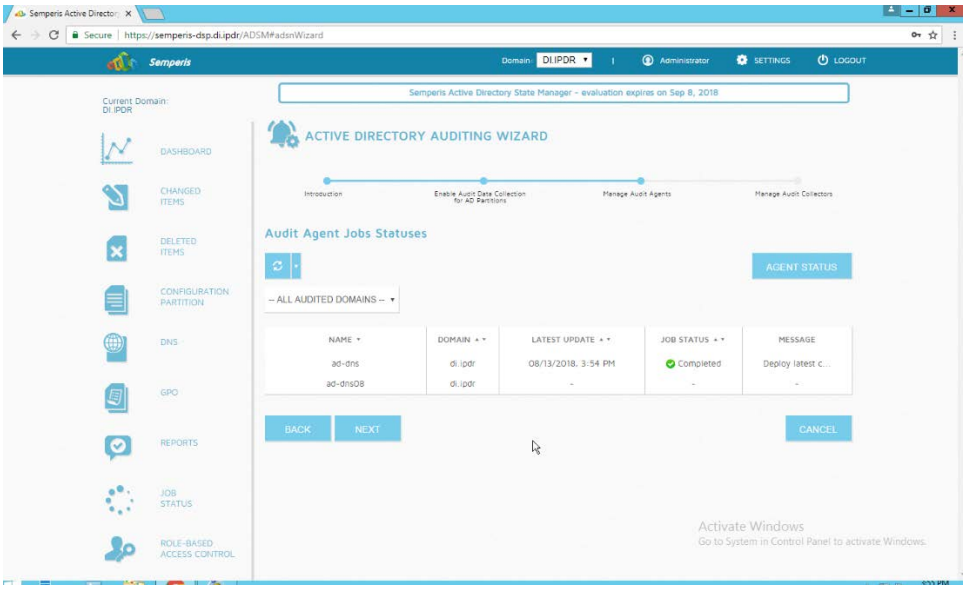
856
857 32. Click **Next.**
858 33. Check the boxes next to any Domain Controllers that should be monitored.



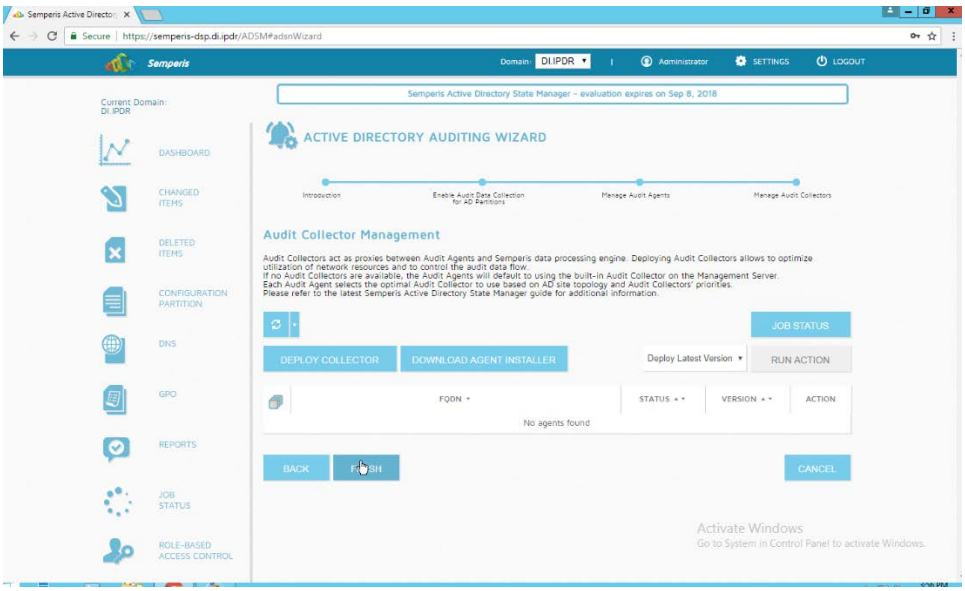
34. Click **Run Action.**
35. Enter the **password.**



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



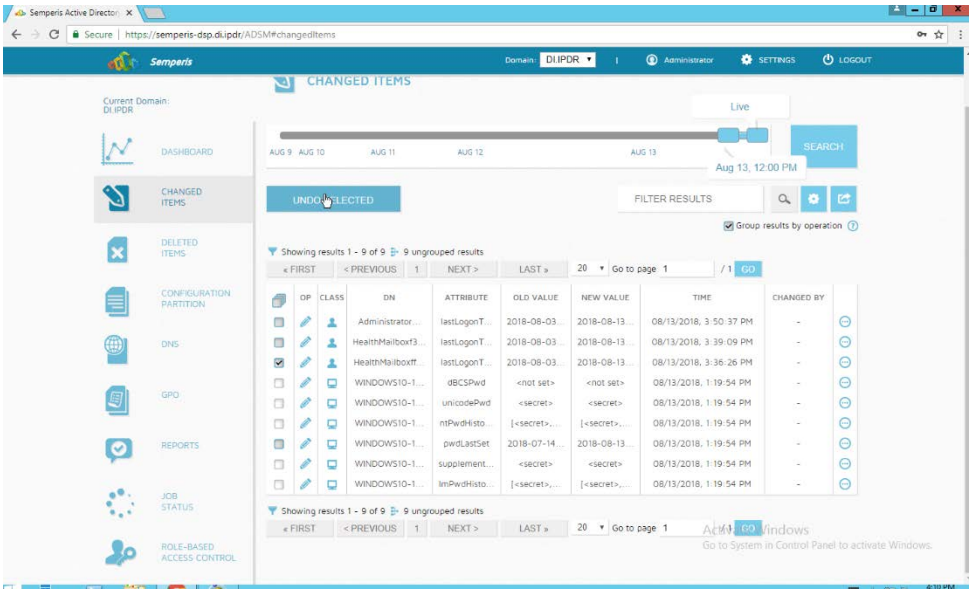
38. Click **Next.**



39. Click **Finish.**

2.6.3 Roll Back Changes with Semperis DSP

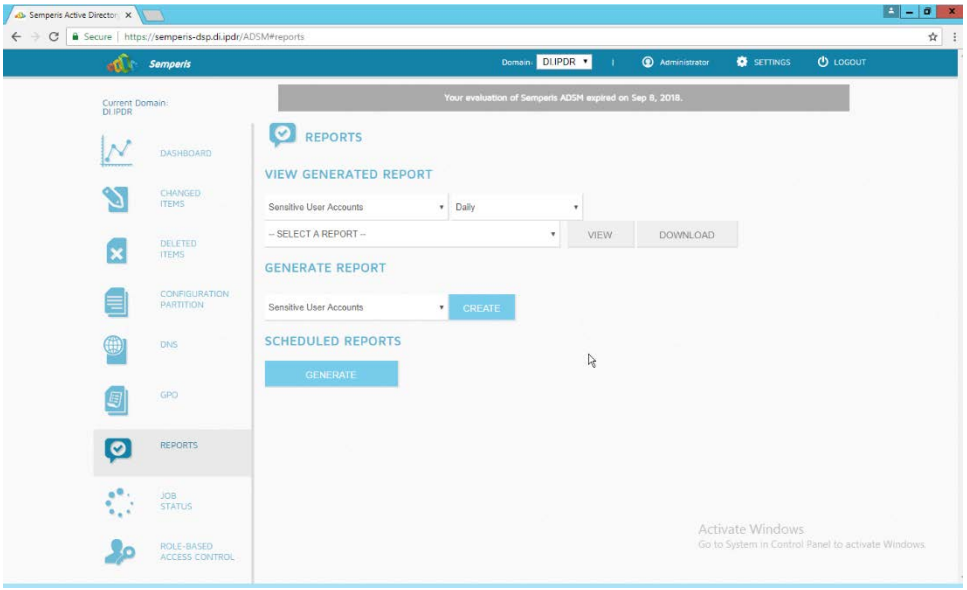
1. Go to **Changed Items** on the left navigation bar.
2. Check the box next to any undesired Active Directory changes.
3. Click the **…** button to view more details about the change.



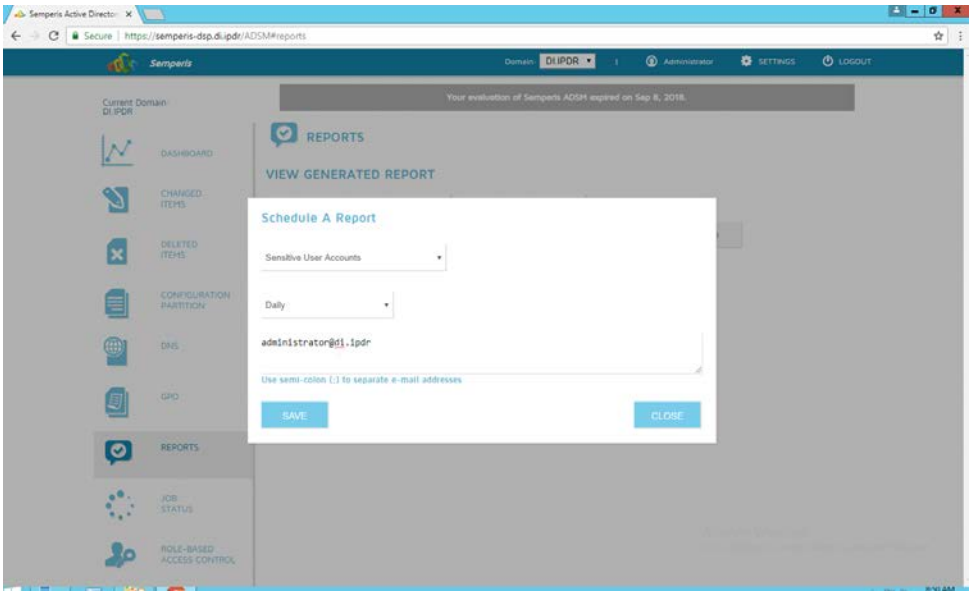
4. Click **Undo Selected** to roll back these changes.

2.6.4 Configure Reporting with Semperis DSP

1. Click **Reports** on the left sidebar in the **Semperis DSP** web console.
2. Under **Generate Report,** reports can be viewed instantly, by selecting a type of report and clicking **Create.**



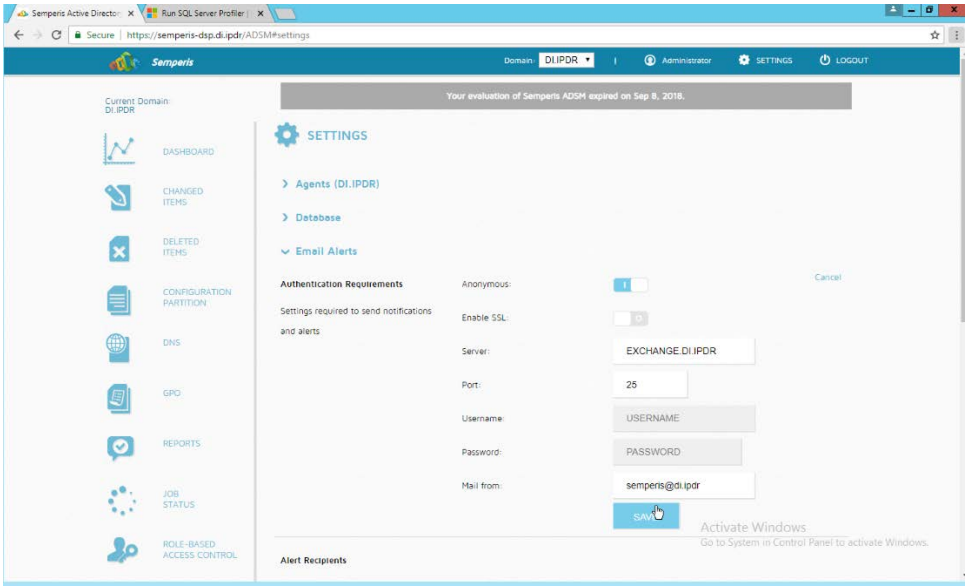
3. Under **Scheduled Reports,** click **Generate** to automatically email specific reports.
4. Select a report type and a schedule.
5. Enter the email addresses of anyone who should receive this report.



6. Click **Save.**

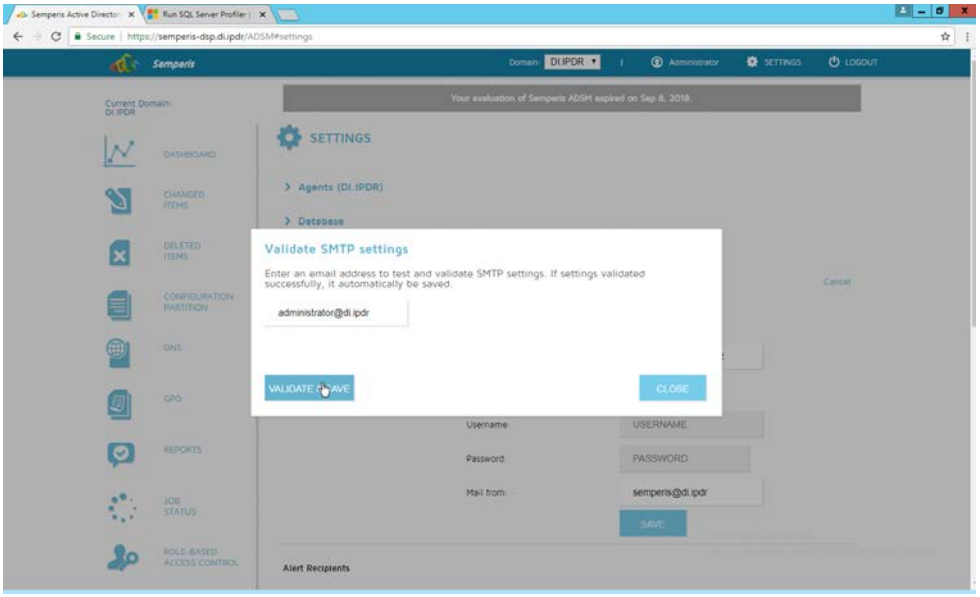
2.6.5 Configure Email Alerts with Semperis DSP

1. Click **Settings** on the **Semperis DSP** web console.
2. Expand the **Email Alerts** section.
3. Click **Edit.**
4. Enter the information of the organization's email server as well as an email address from which to send.

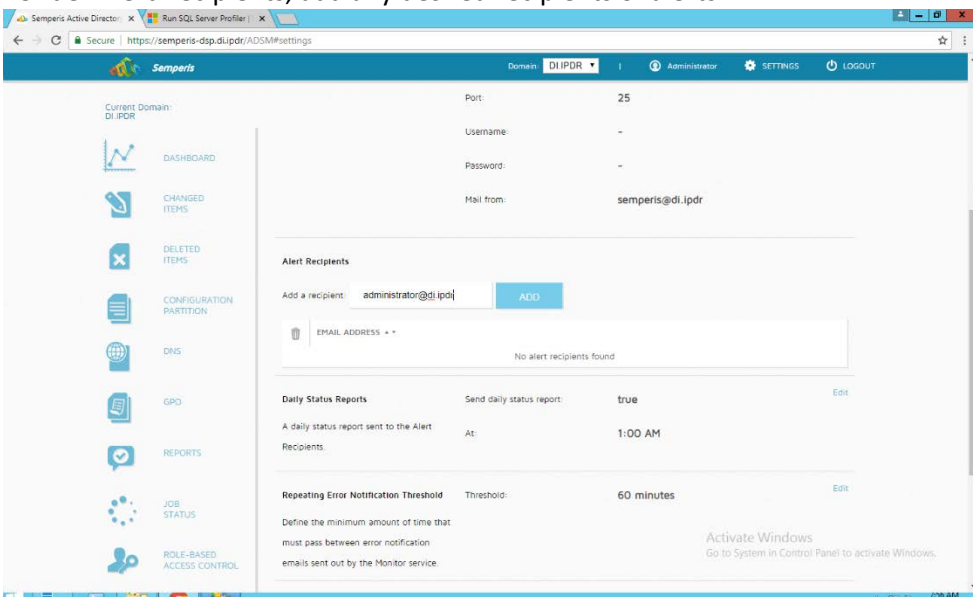


5. Click **Save.**

6. Enter an email address to which to send a test email.



7. Click **Validate & Save.**
8. Under Alert Recipients, add any desired recipients of alerts.



9. Click **Add.**
10. Configure any schedule settings according to your organization's needs.

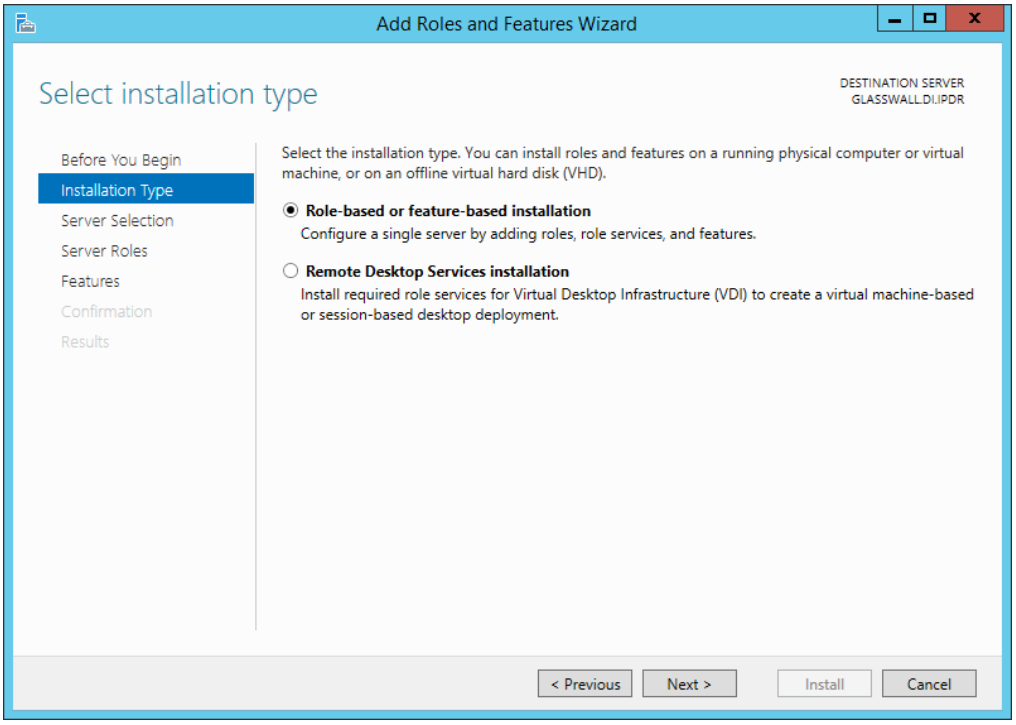
2.7 Glasswall FileTrust™ for Email

The following sections will detail the installation of **Glasswall FileTrust™ for Email**, an email security product, on a new Windows 2012 R2 machine. For the purposes of this guide, we use Microsoft Exchange as the email service provider.

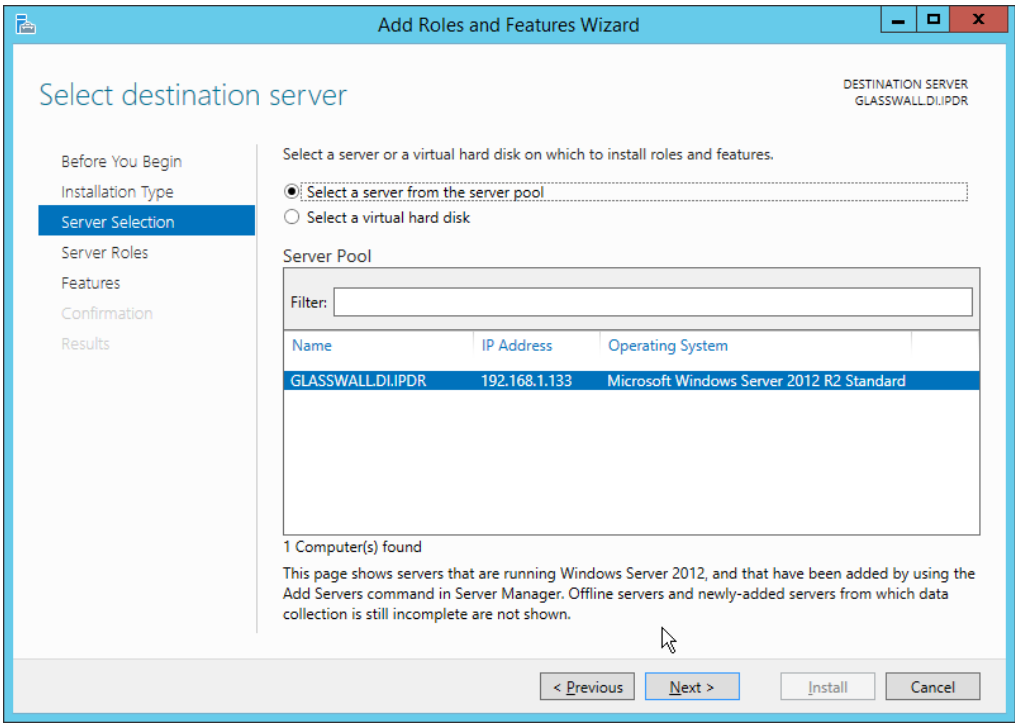
2.7.1 Install Prerequisites

2.7.1.1 *Install the IIS web server*

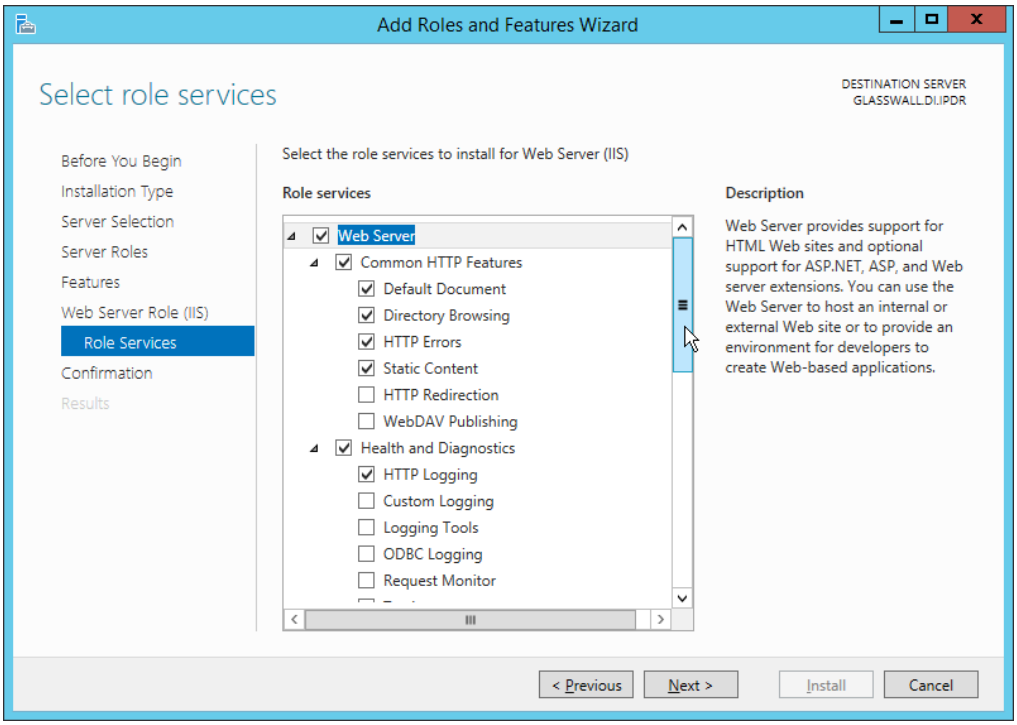
1. In **Server Manager,** click **Add Roles and Features.**
2. Click **Next.**
3. Select **Role-based or feature-based installation.**



4. Click **Next.**
5. Select the current server.



6. Click **Next.**
7. Select **Web Server (IIS).**
8. Click **Next.**
9. Select **.NET Framework 4.5 Features.**
10. Click **Next.**
11. Select the following Role Services: **Web Server, Common HTTP Features, Default Document, Directory Browsing, HTTP Errors, Static Content, Health and Diagnostics, HTTP Logging, Performance, Static Content Compression, Security, Request Filtering, Client Certificate Mapping Authentication, Application Development, .NET Extensibility 4.5, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters, Management Tools, and IIS Management Console.**



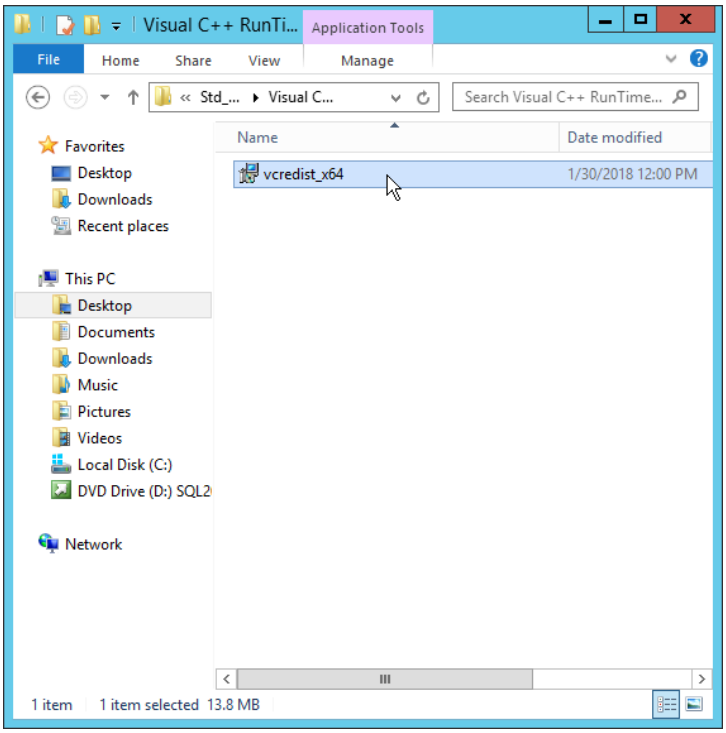
12. Click **Next.**
13. Check the box next to **Restart the destination server automatically if required.**
14. Click **Install.**

2.7.1.2 *Install Microsoft SQL 2014 Enterprise*

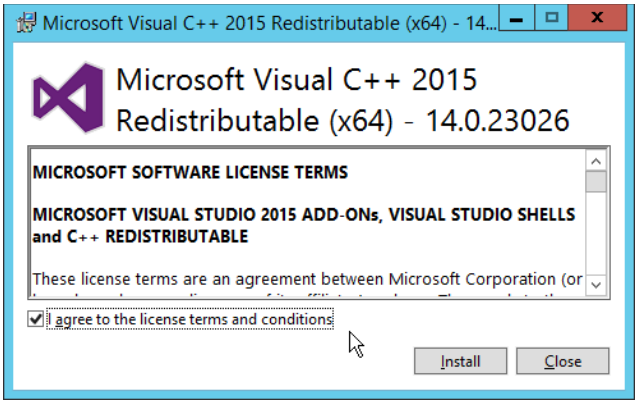
Please see Section 2.4 for an installation guide for MS SQL 2014; for simplicity it should be installed on the same server as Glasswall FileTrust. Ensure that Mixed Mode authentication is selected when installing.

2.7.1.3 *Install Microsoft Visual C++ 2015*

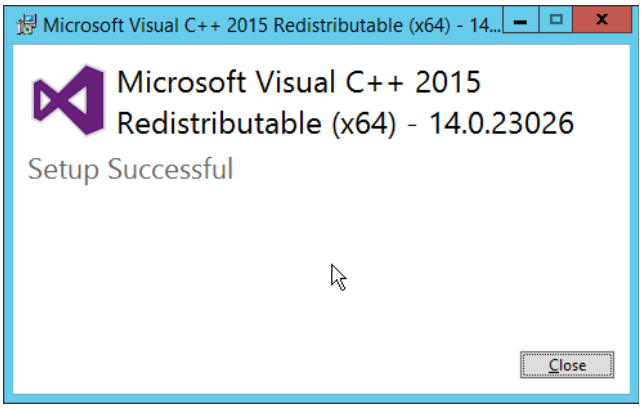
1. Run the **vcredist_x64** installer.



2. Check the box next to **I agree to the license terms and conditions.**



3. Click **Install.**
4. After the installation is complete, click **Close.**

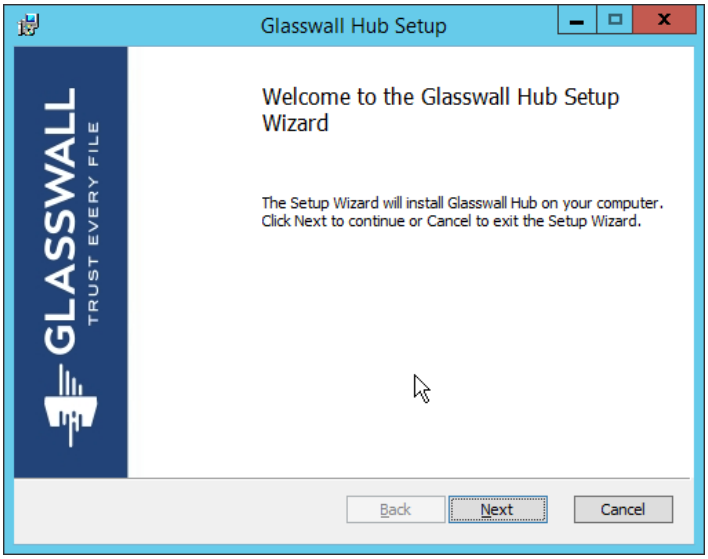


938

939 ## 2.7.2 Install the Glasswall FileTrust Server Component

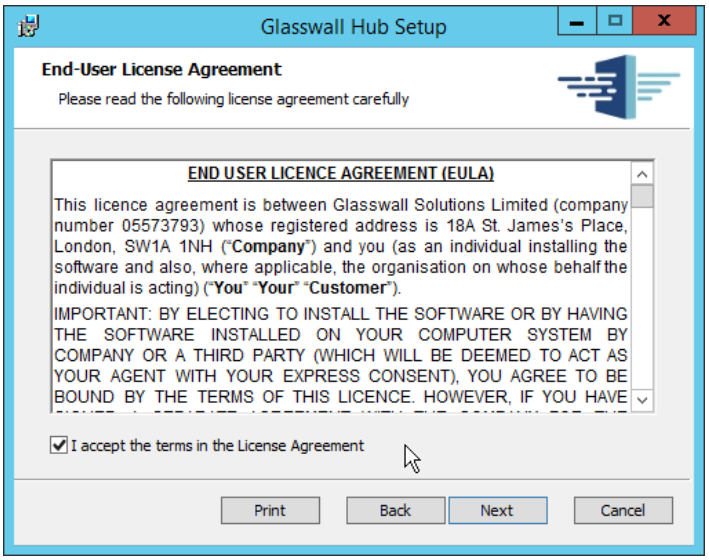
940 ### 2.7.2.1 *Install Glasswall Hub*

941 1. Run **HubInstaller.msi.**

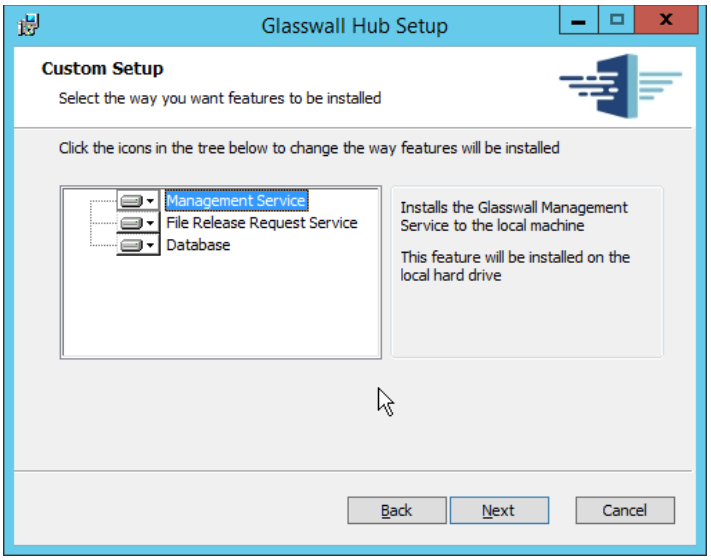


942

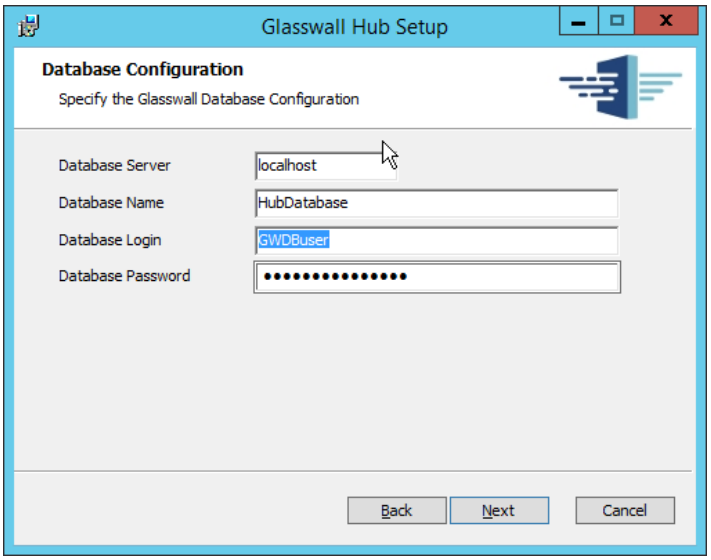
943 2. Click **Next.**



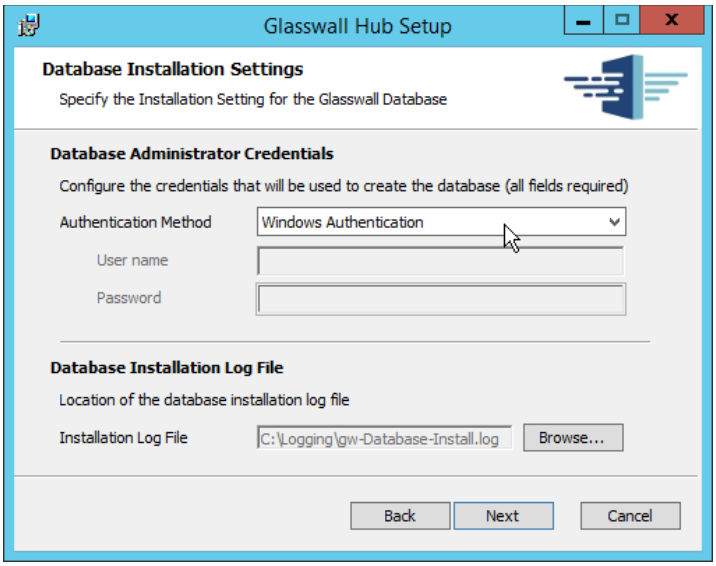
3. Check the box next to **I accept the terms in the License Agreement.**
4. Click **Next.**



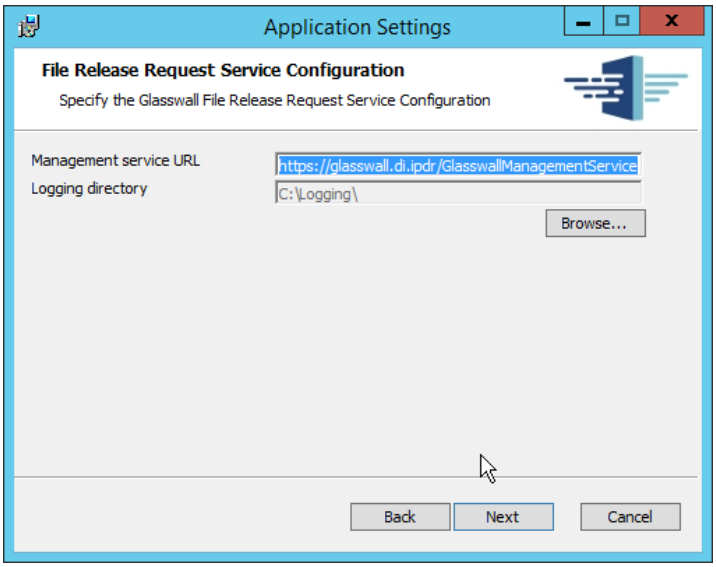
5. Click **Next.**
6. Enter **localhost** for the **Database Server**.
7. Enter **HubDatabase** for the **Database Name.**
8. Enter a **username** and **password** (and take note of these for later).



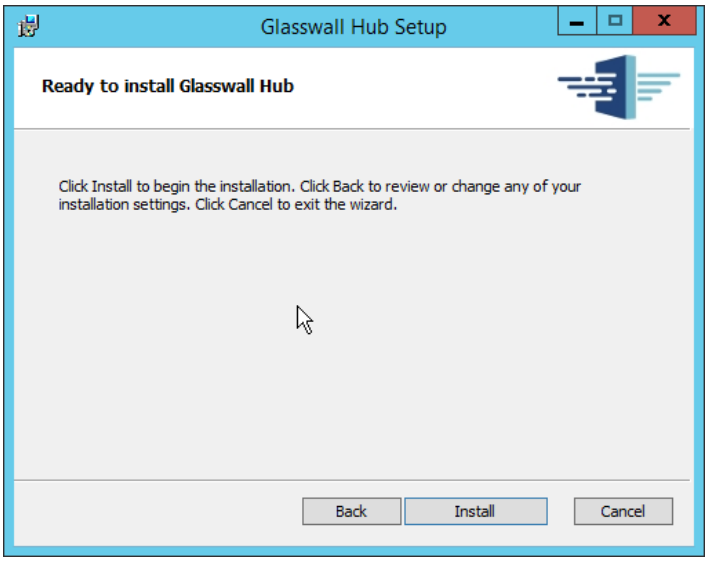
9. Click **Next.**
10. Select **Windows Authentication.**



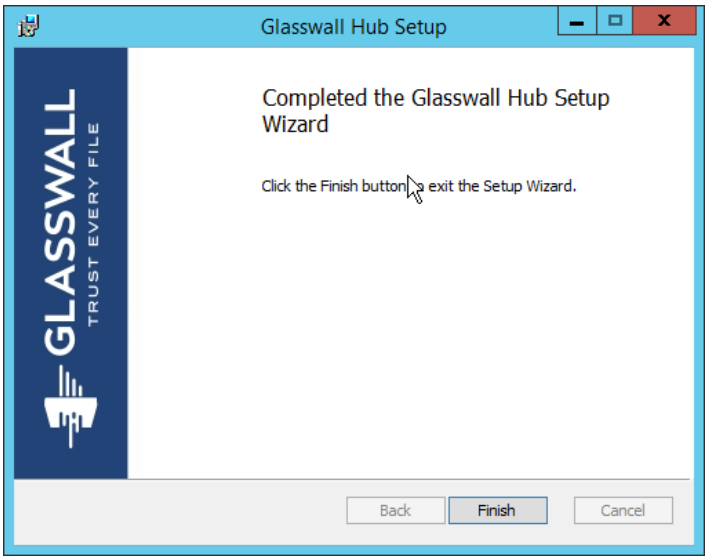
11. Click **Next.**
12. Replace the domain of the **management service URL** with the address of the current machine, such as **glasswall.di.ipdr.**



13. Click **Next.**



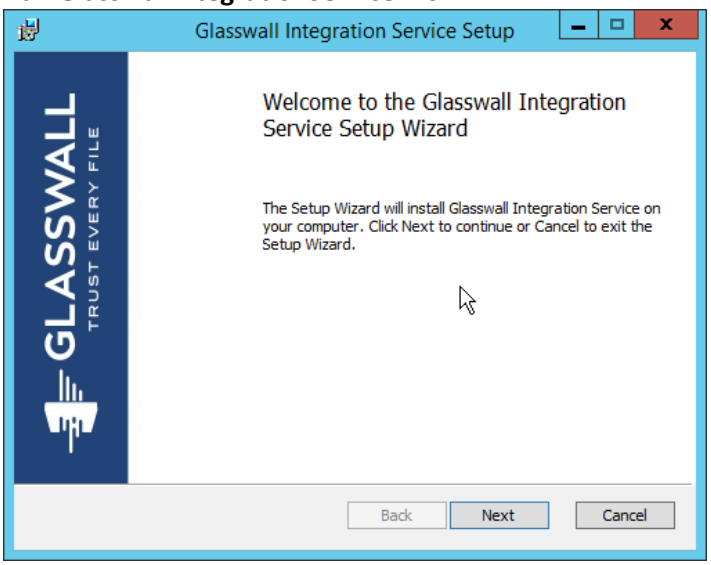
14. Click **Install.**



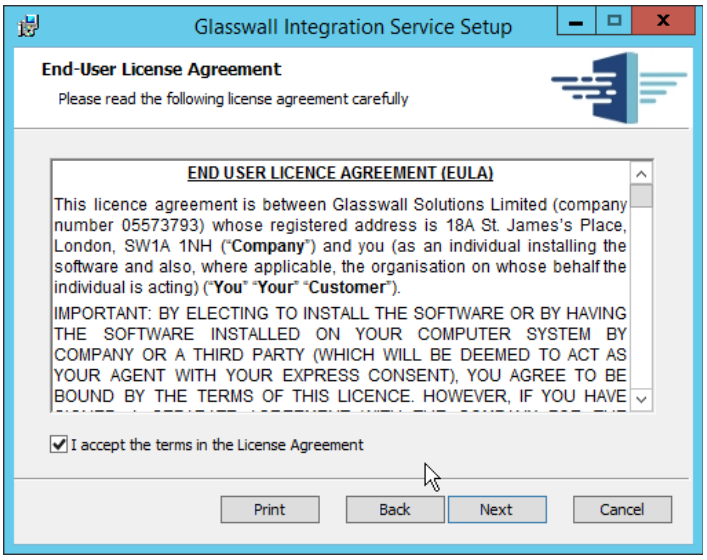
15. Click **Finish.**

2.7.2.2 *Install Glasswall Integration Service*

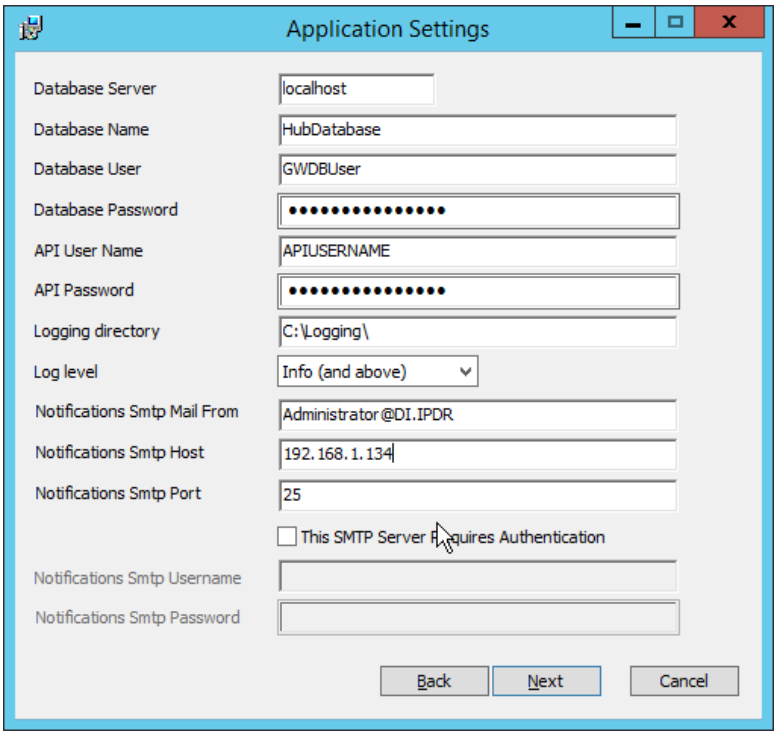
1. Run **GlasswallIntegrationService.msi.**



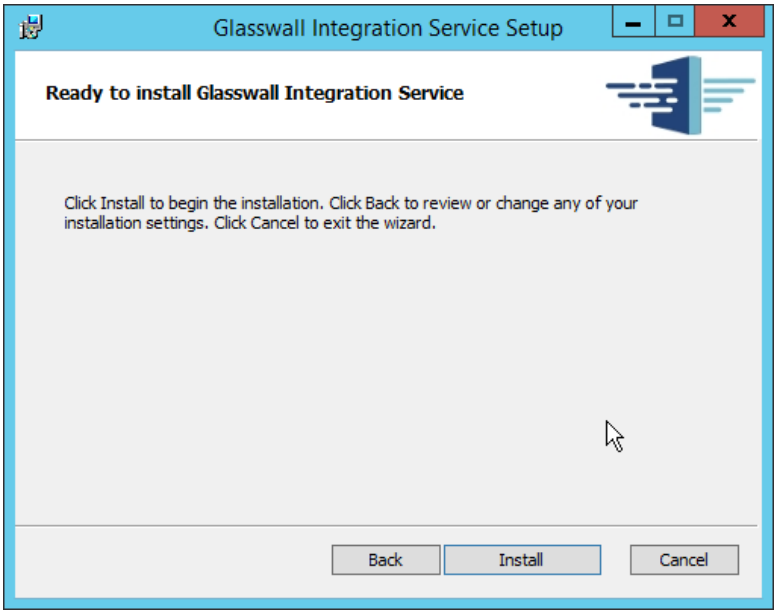
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**



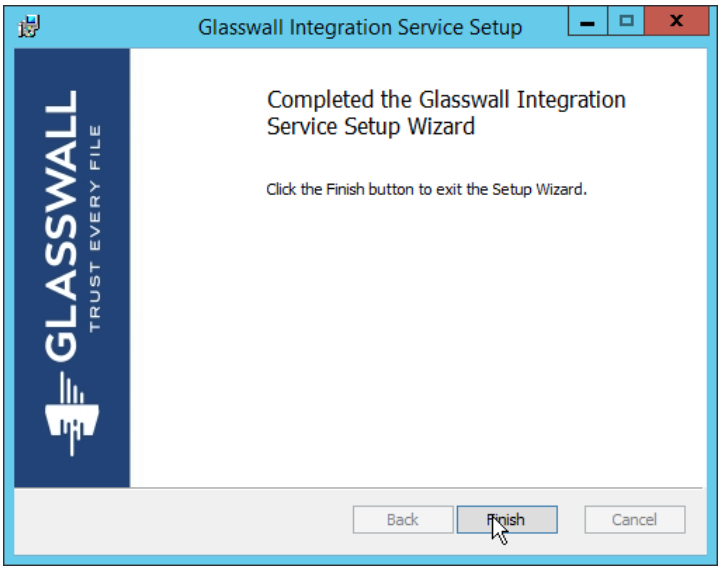
4. Click **Next.**
5. For **Database Server, Database Name, Database User,** and **Database Password,** enter the information entered in the **Glasswall Hub Installer.**
6. Create a **username** and **password** for **API User Name** and **API Password.**
7. Enter an email address to be used for notifications in **Notifications Smtp Mail From.**
8. Enter the **address** for the mail server for **Notifications Smtp Host.**
9. Enter a **port** (**25** is used here) for **Notifications Smtp Port.**



978
979 10. Click **Next.**



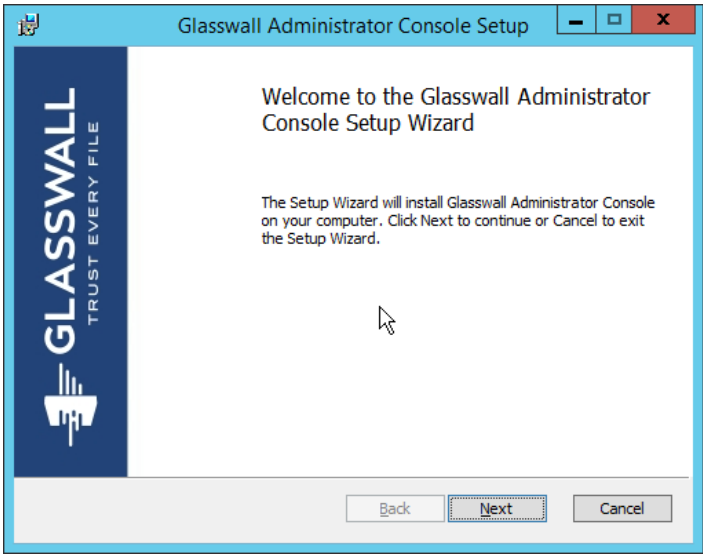
980
981 11. Click **Install.**



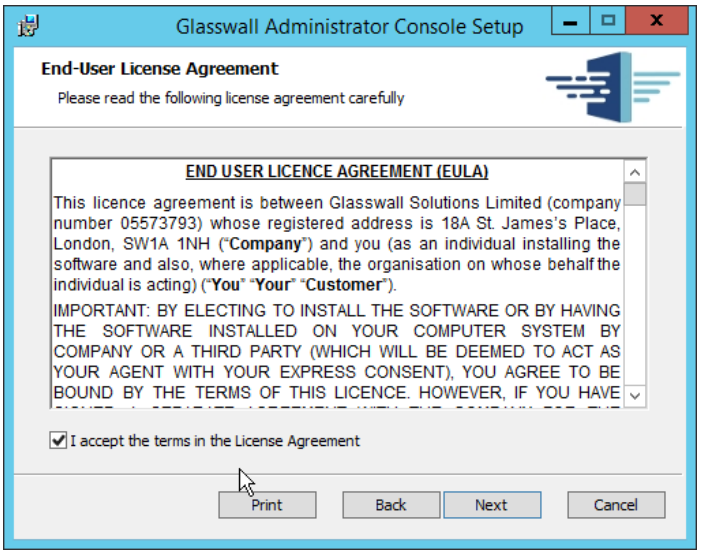
12. Click **Finish.**

2.7.2.3 *Install Glasswall Administrator Console*

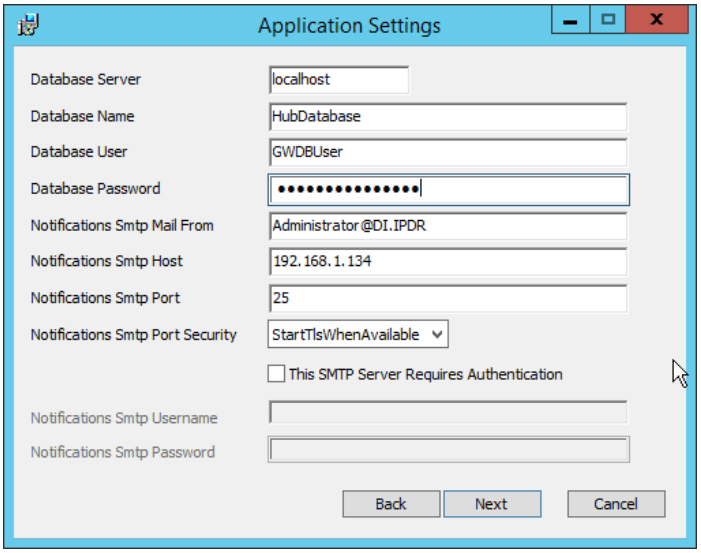
1. Run **AdministratorConsoleInstaller.msi.**



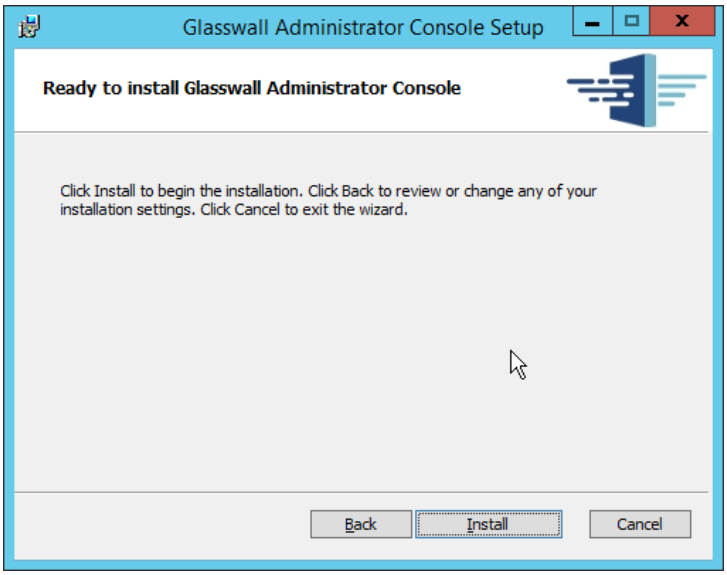
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**



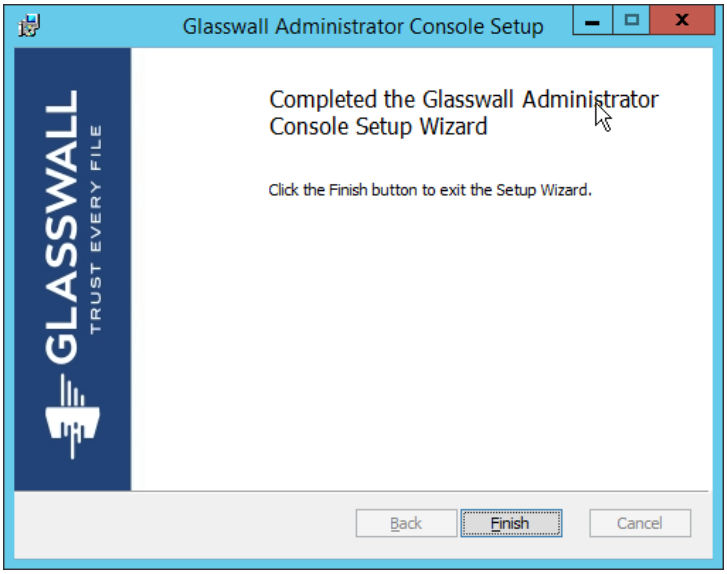
4. Click **Next.**
5. For **Database Server, Database Name, Database User,** and **Database Password,** enter the information entered in the **Glasswall Hub Installer.**
6. For **Notifications Smtp Mail From, Notifications Smtp Host, Notifications Smtp Port,** enter the information entered in the **Glasswall Integration Service Installer.**
7. For **Notifications Smtp Port Security**, select **StartTlsWhenAvailable.**



8. Click **Next.**



9. Click **Install.**

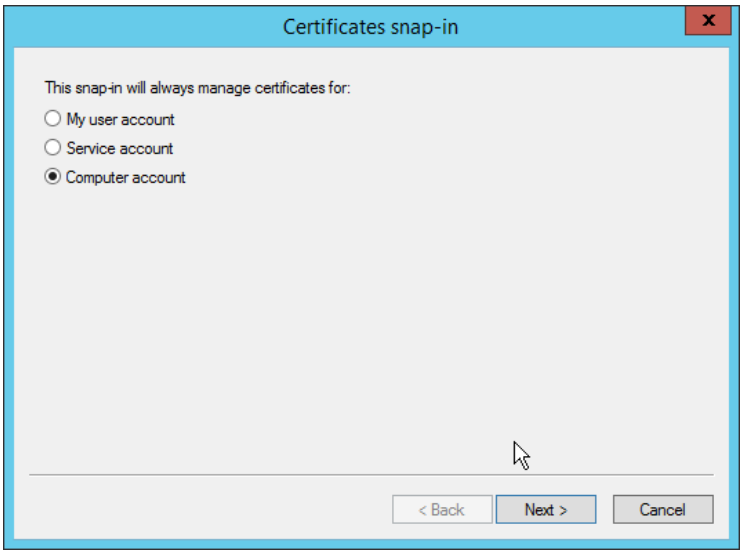


10. Click **Finish.**

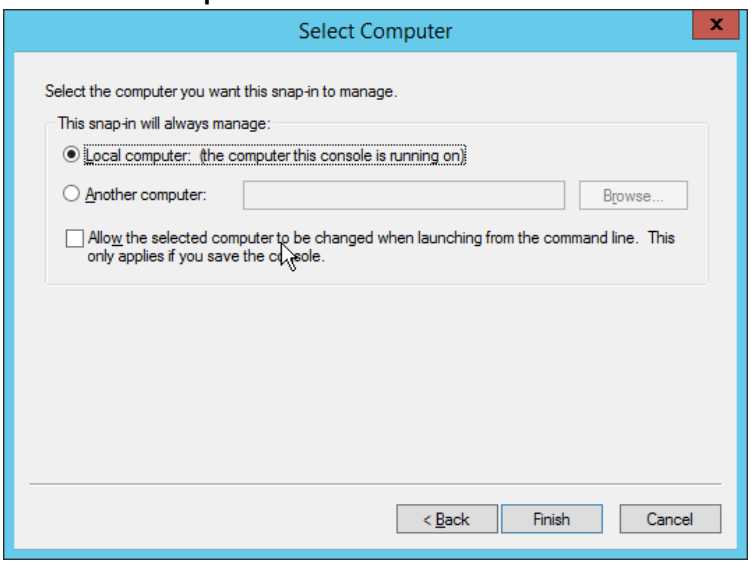
2.7.2.4 *Add the Server's Certificate*

1. For the purposes of this build, a self-signed certificate is used, but this is dependent on the needs of the organization. Ensure that the certificate used is issued to the domain, such as ***.di.ipdr.**
2. Open **mmc.**
3. Click **File > Add/Remove Snap-In….**
4. Select **Certificates** from the left pane, and click **Add.**

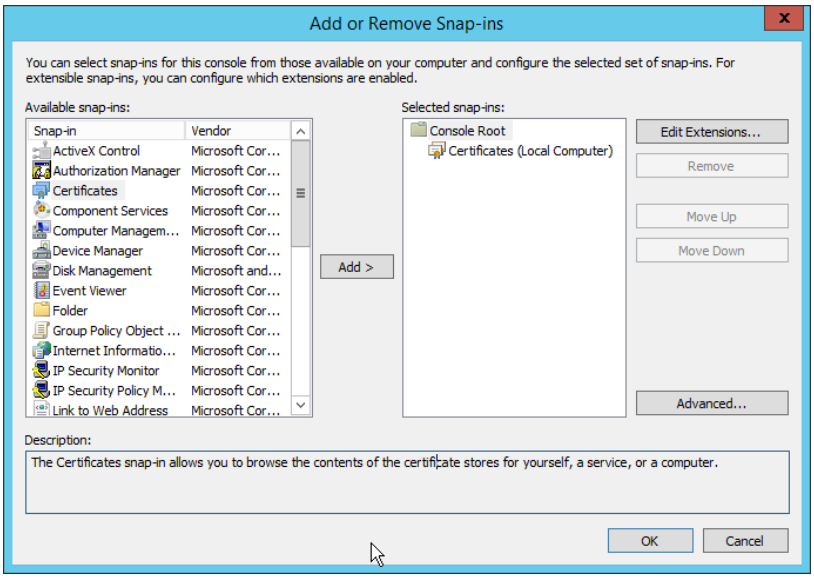
5. Select **Computer Account.**



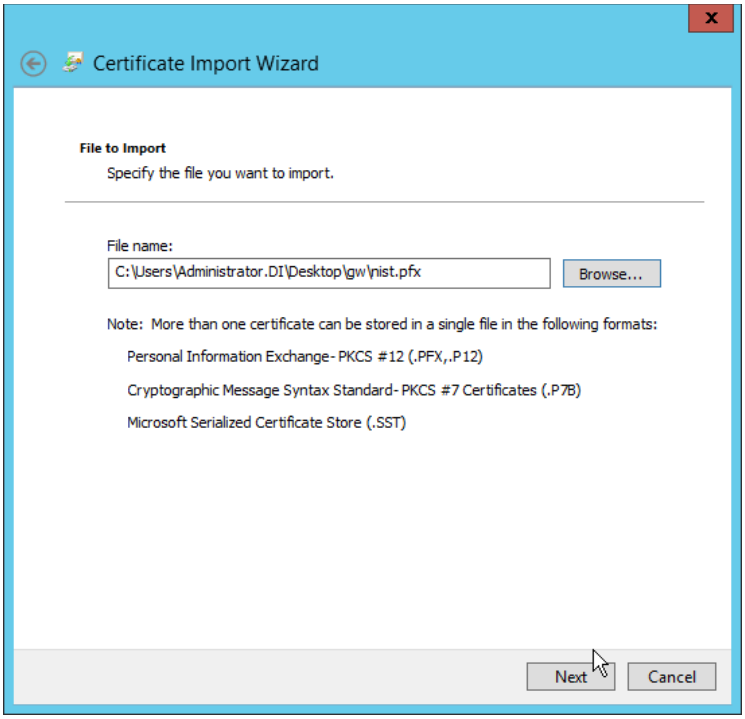
6. Click **Next.**
7. Select **Local computer.**



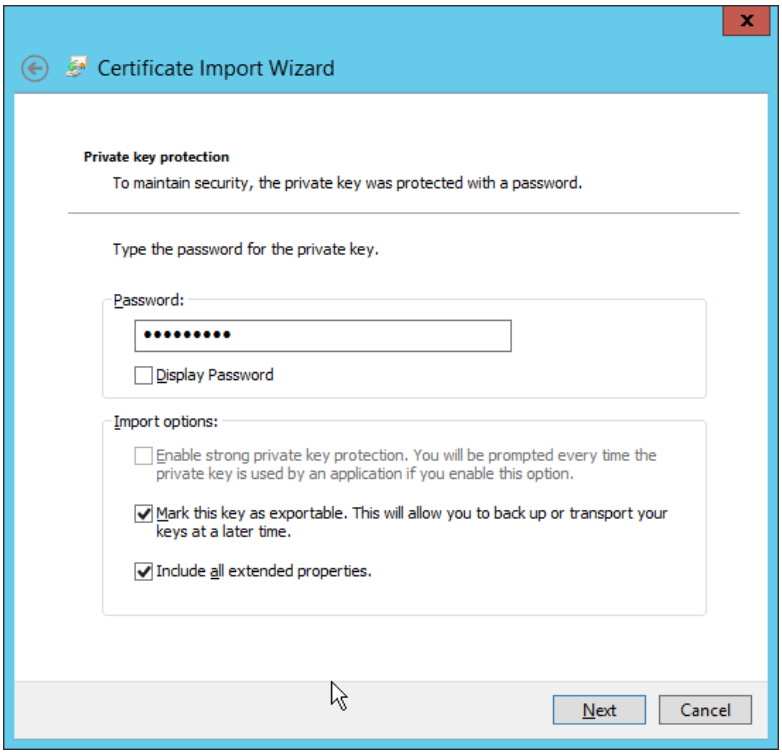
8. Click **Finish.**



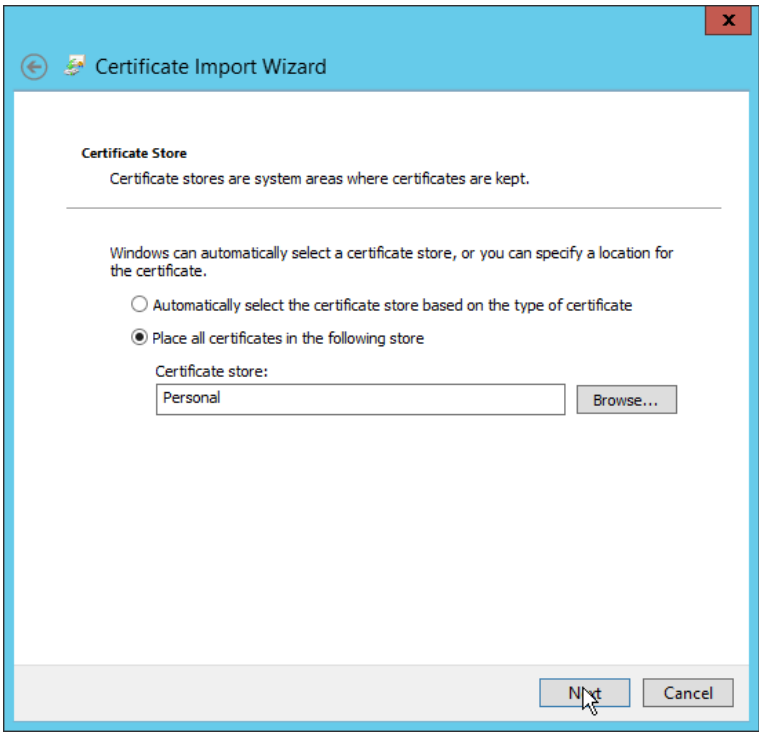
9. Click **OK.**
10. Right-click the **Personal** certificate store, and select **All tasks > Import….**



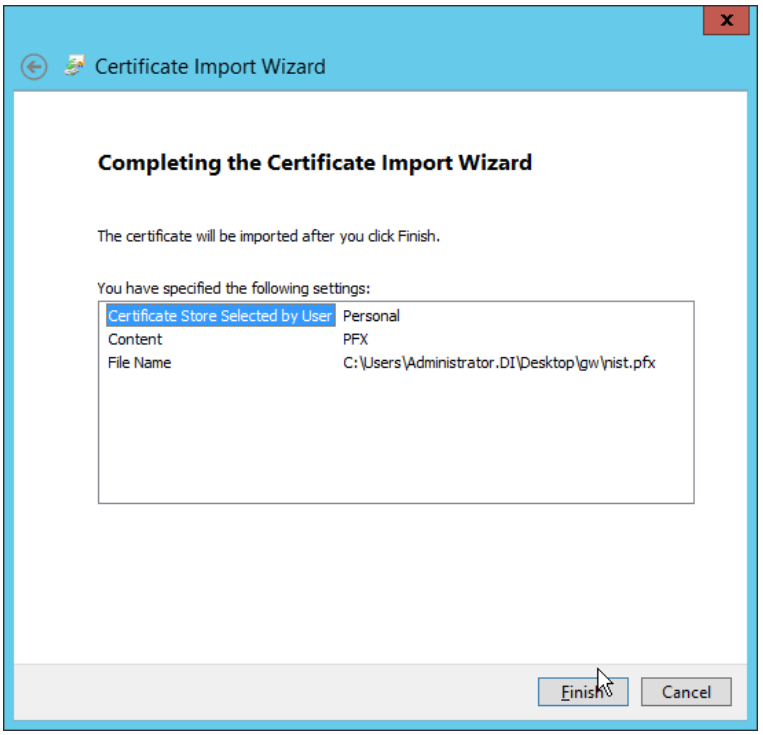
11. Enter the **file name** of the certificate**.**
12. Click **Next.**
13. Enter the **password** for the certificate**.**
14. Check the box next to **Mark this key as exportable.**



15. Click **Next.**
16. Ensure that the **Certificate store** says **Personal.**

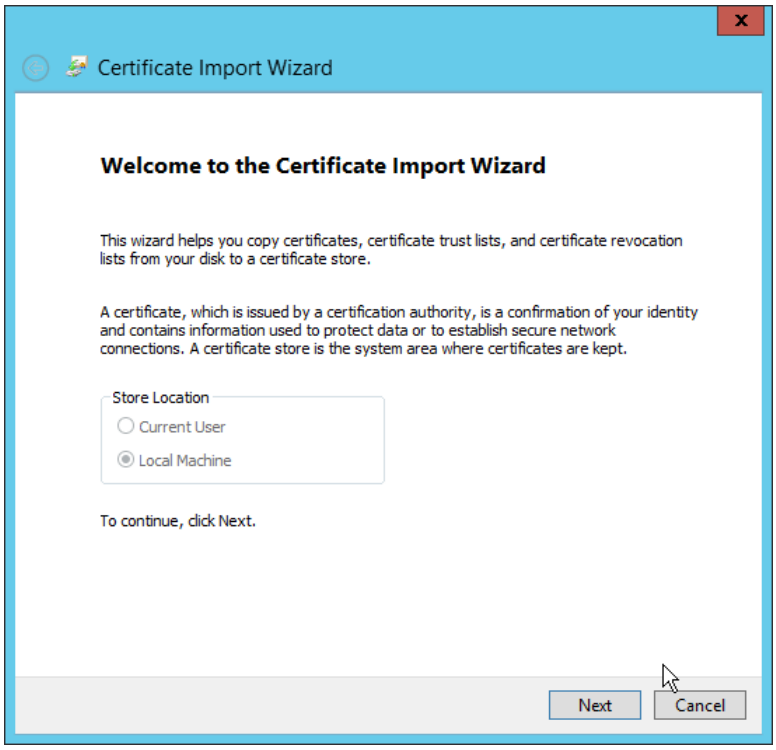


17. Click **Next.**

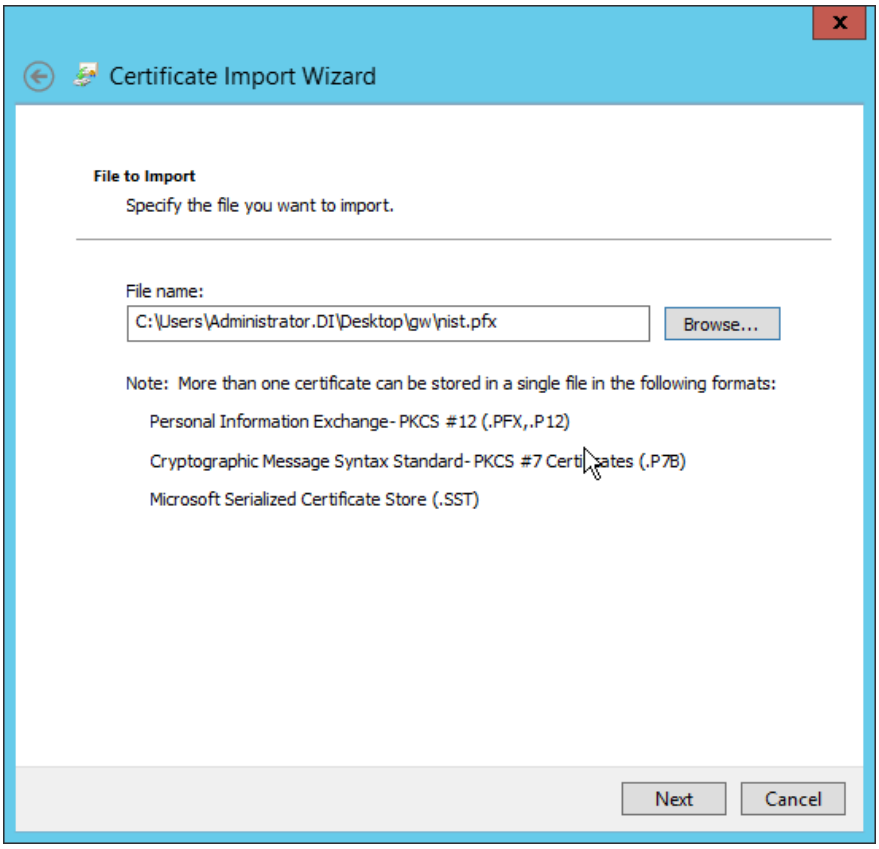


18. Click **Finish.**

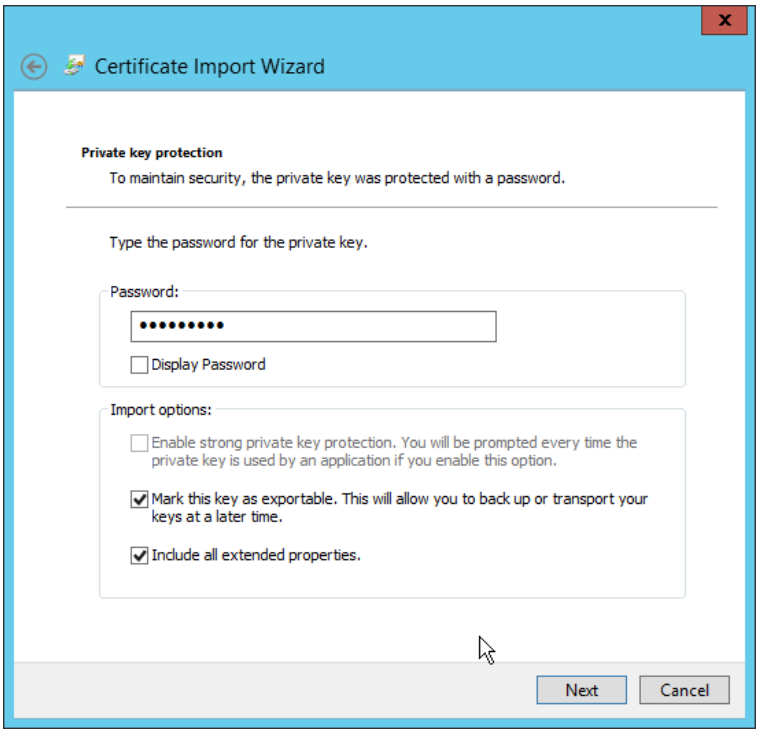
19. Re-open the certificate import wizard but this time for **Trusted Root Certification Authorities.**



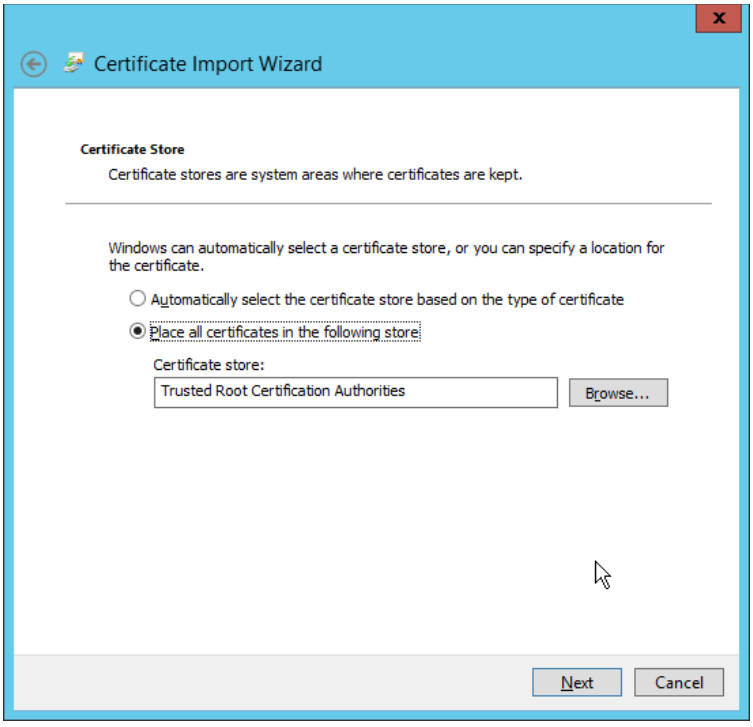
20. Click **Next.**
21. Select the same certificate.



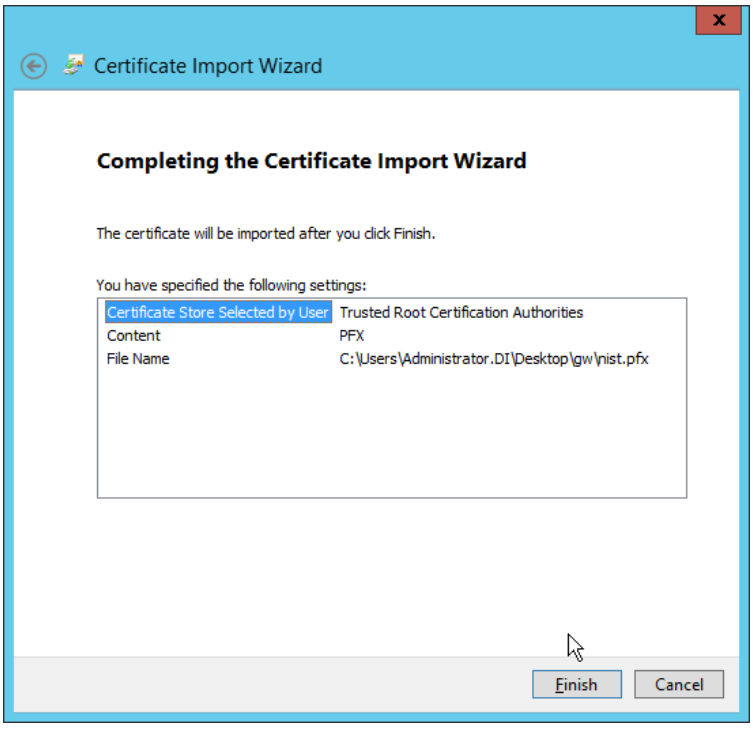
22. Click **Next.**
23. Enter the certificate's **password.**
24. Check the box next to **Mark this key as exportable.**



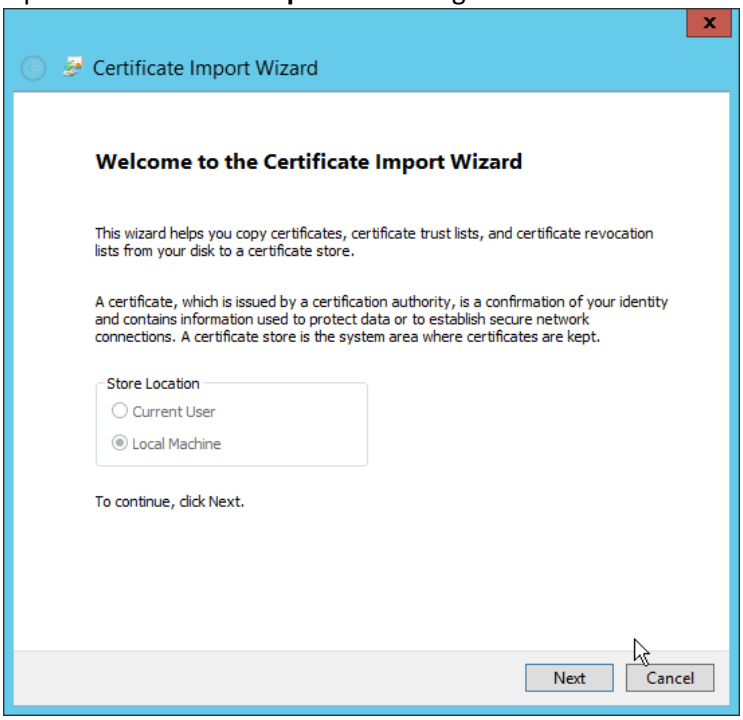
25. Click **Next.**



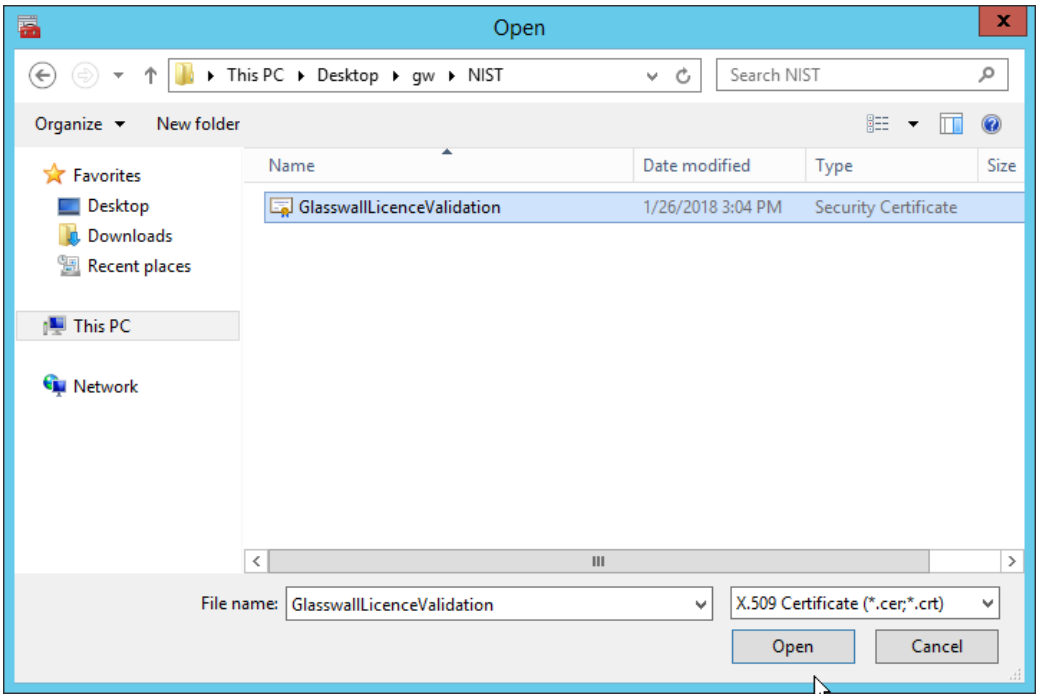
26. Click **Next.**



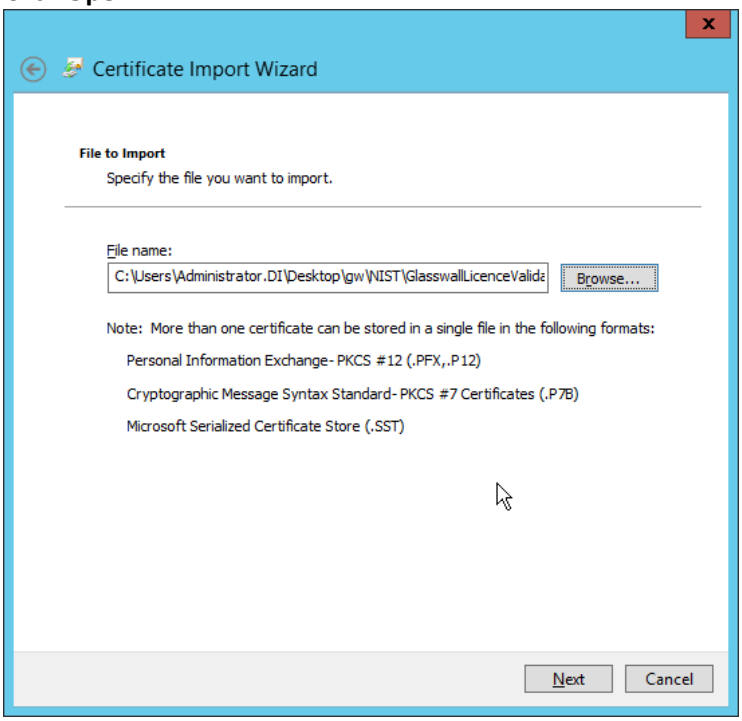
27. Click **Finish.**
28. Open the **Certificate Import Wizard** again for the **Personal** store**.**



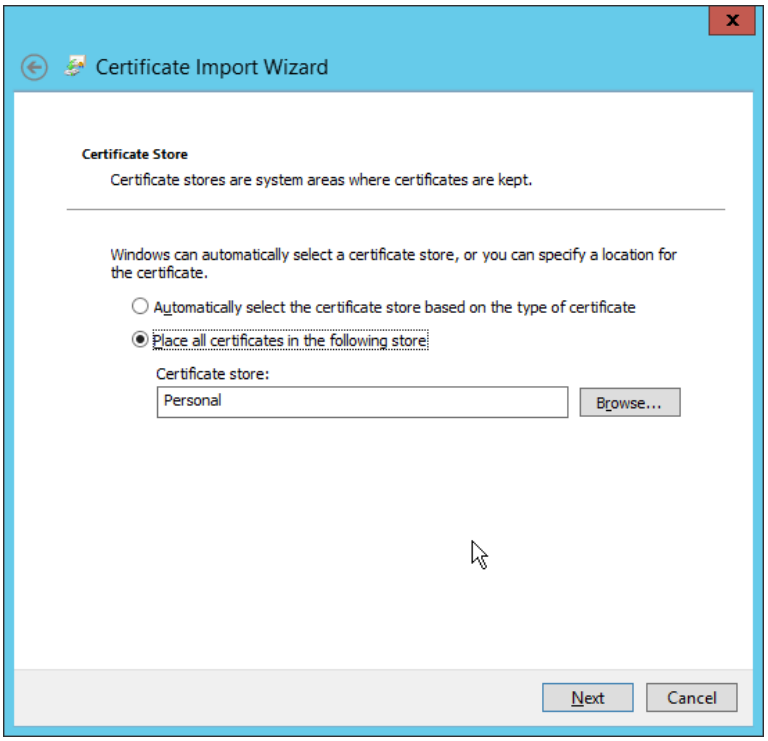
29. Click **Next.**
30. Browse to the **GlasswallLicenseValidation** certificate.



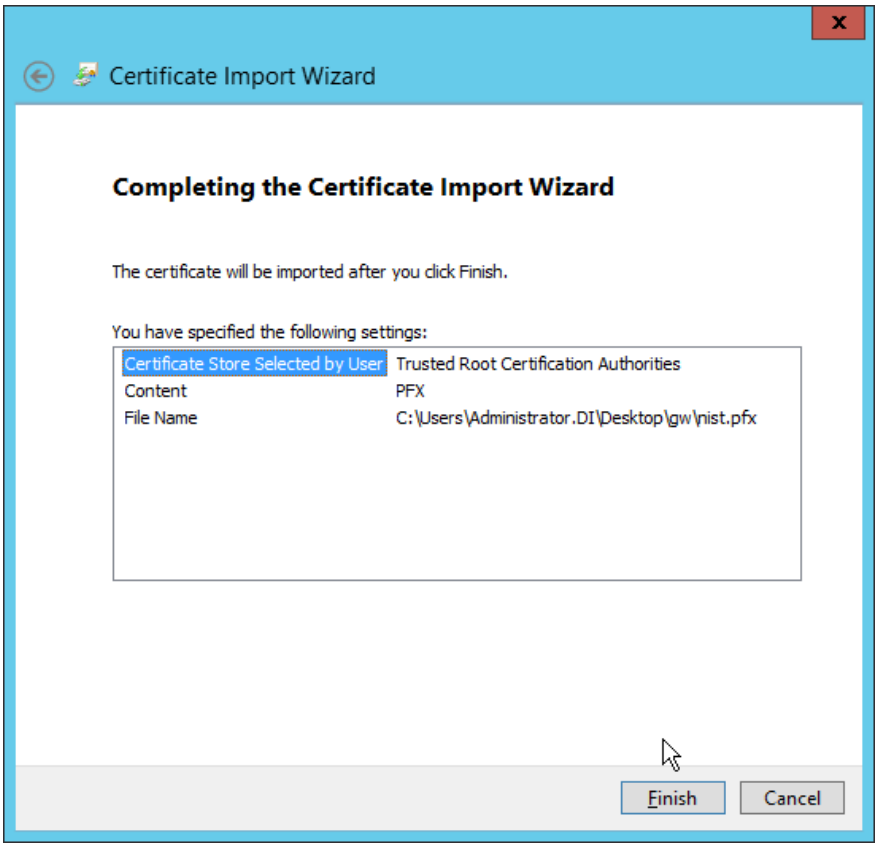
31. Click **Open.**



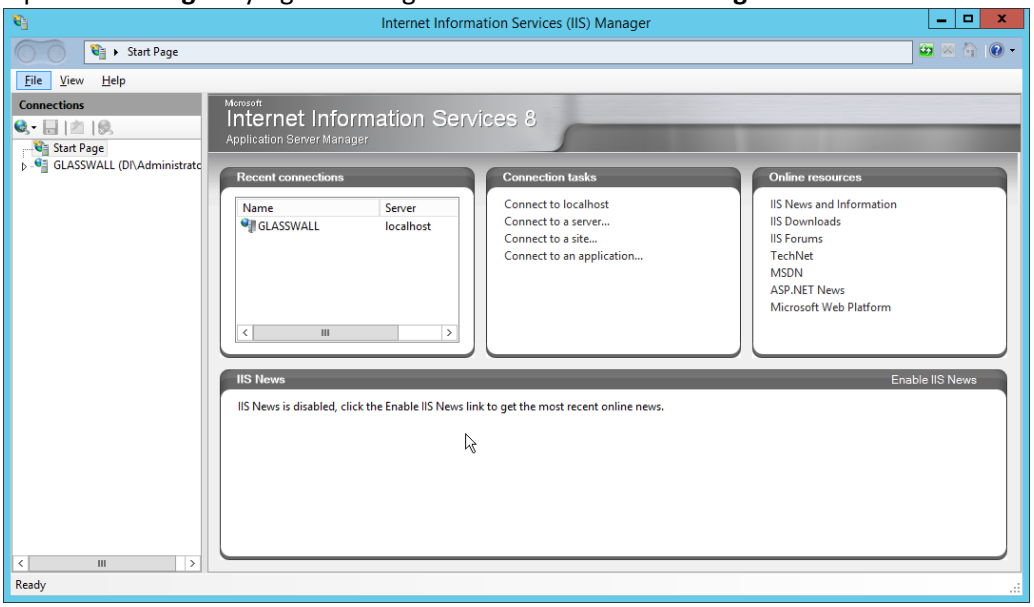
32. Click **Next.**



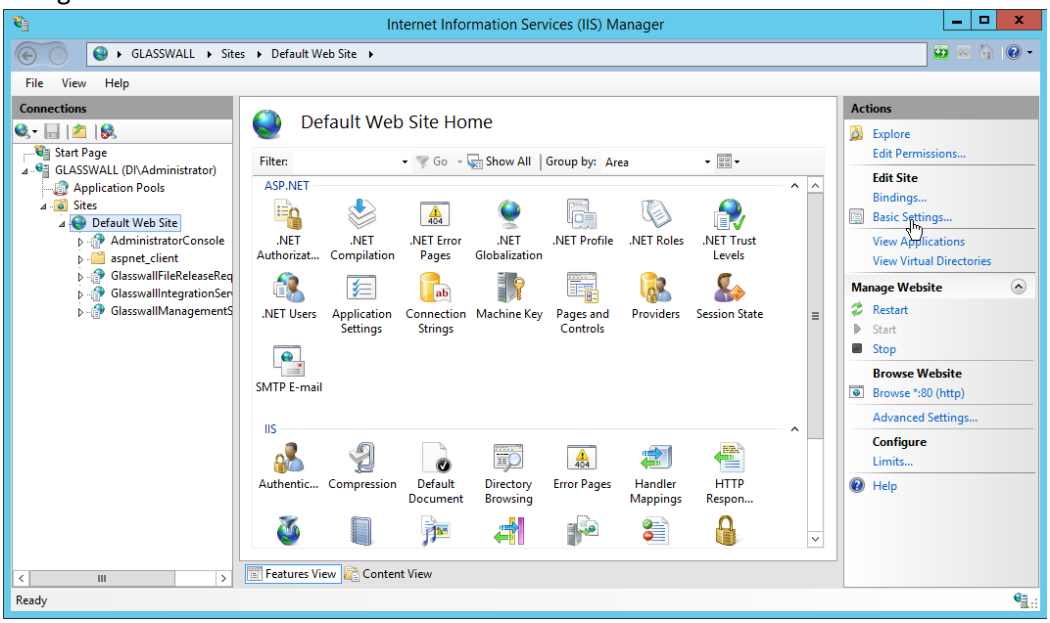
33. Click **Next.**



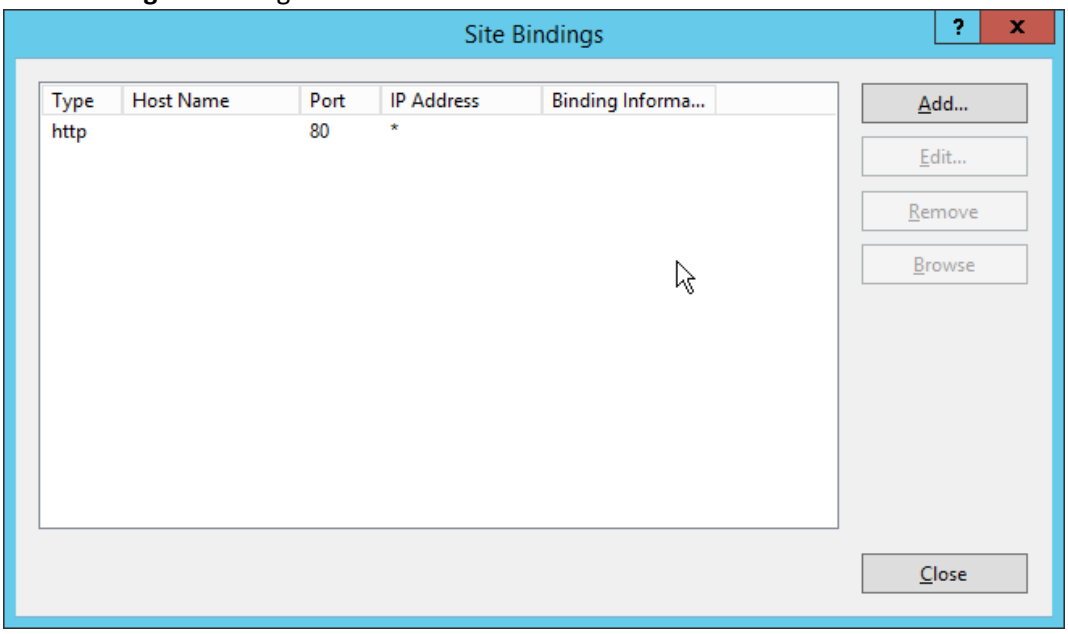
34. Click **Finish.**
35. Open **IIS Manager** by right-clicking the server in **Server Manager.**



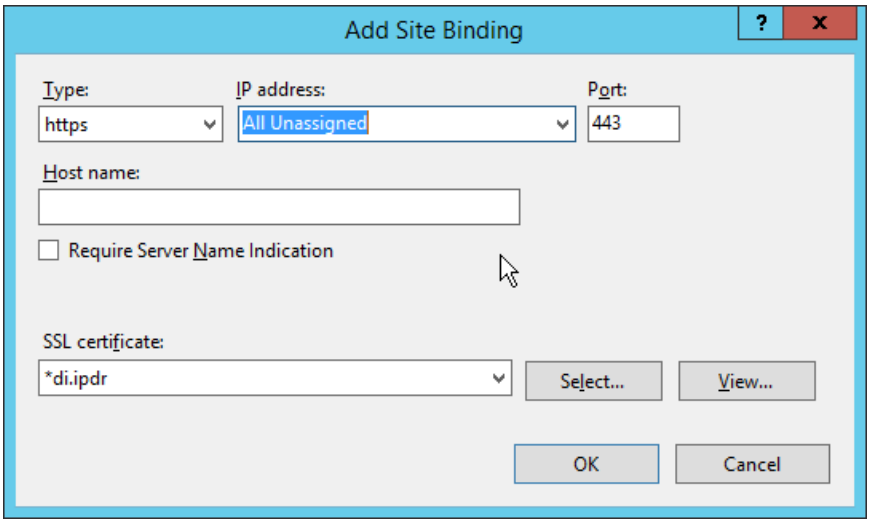
36. Navigate to the **Default Website** in the tree.



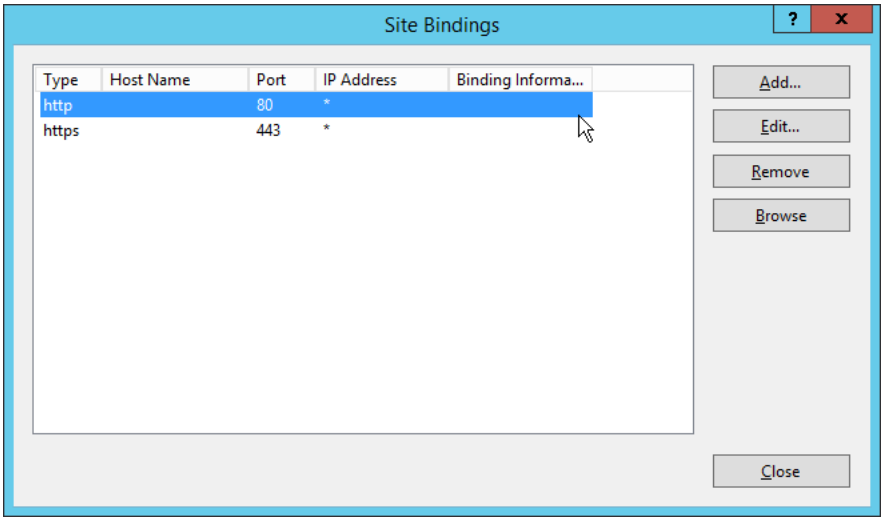
37. Click **Bindings** on the right sidebar.



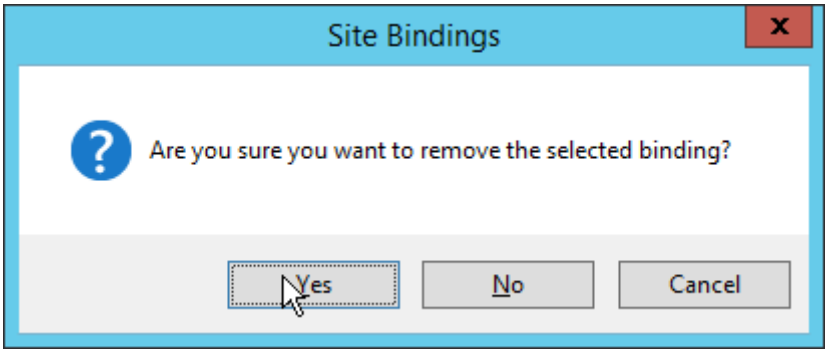
38. Click **Add.**
39. Select **https** for the **Type.**
40. Select **All Unassigned** for **IP address.**
41. Select the **domain certificate** for **SSL certificate.**



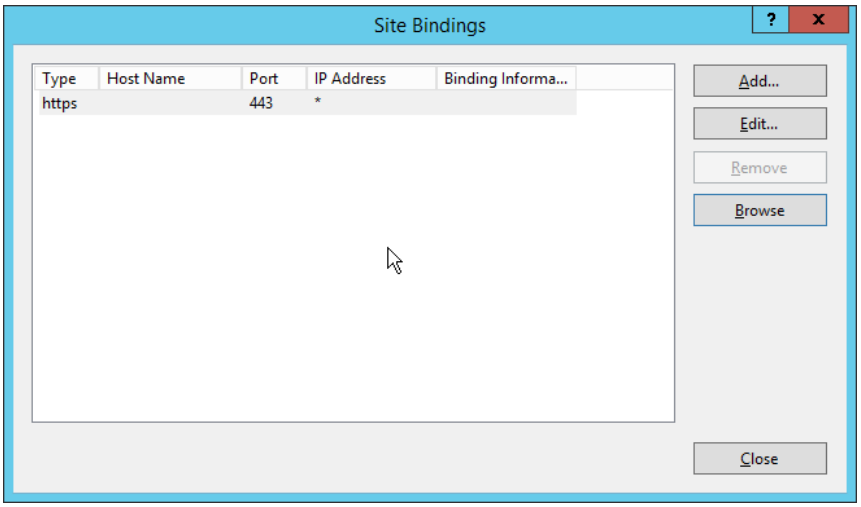
42. Click **OK.**
43. Select the **http binding.**



44. Click **Remove.**



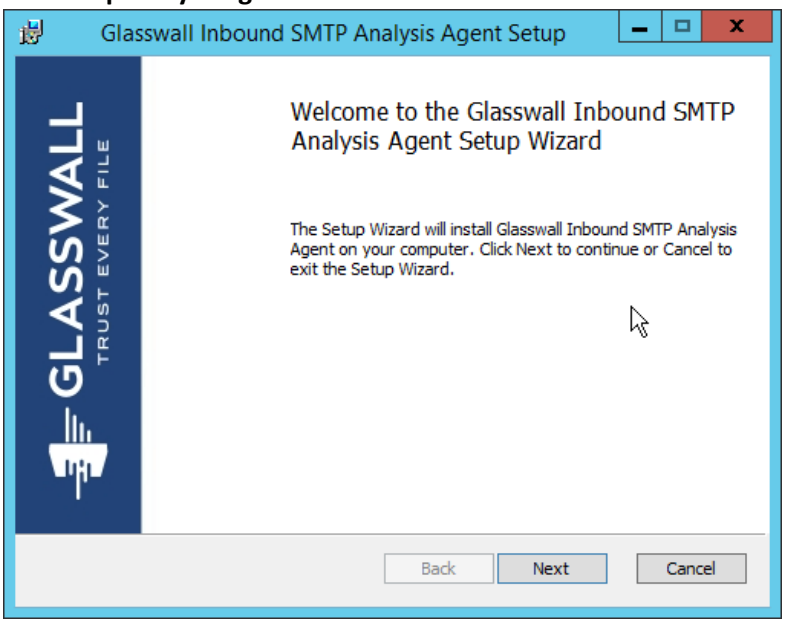
45. Click **Yes.**



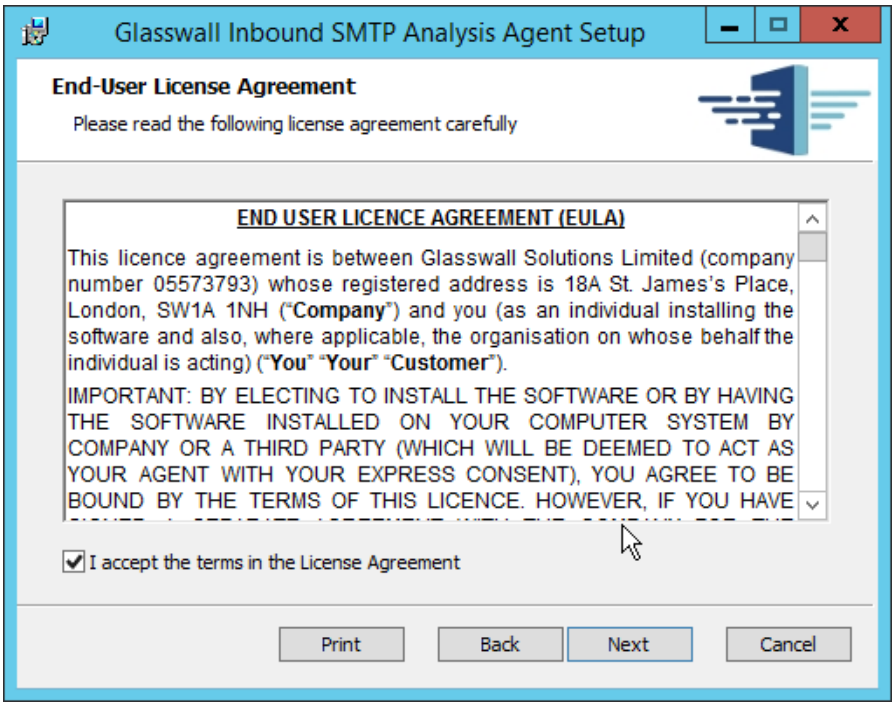
46. Click **Close.**
47. Restart the IIS server. The Glasswall FileTrust console should now be accessible through a browser. (For example, https://glasswall.di.ipdr/AdministratorConsole). Ensure that there are no certificate errors.

2.7.2.5 *Install the Smtp Analysis Agent*

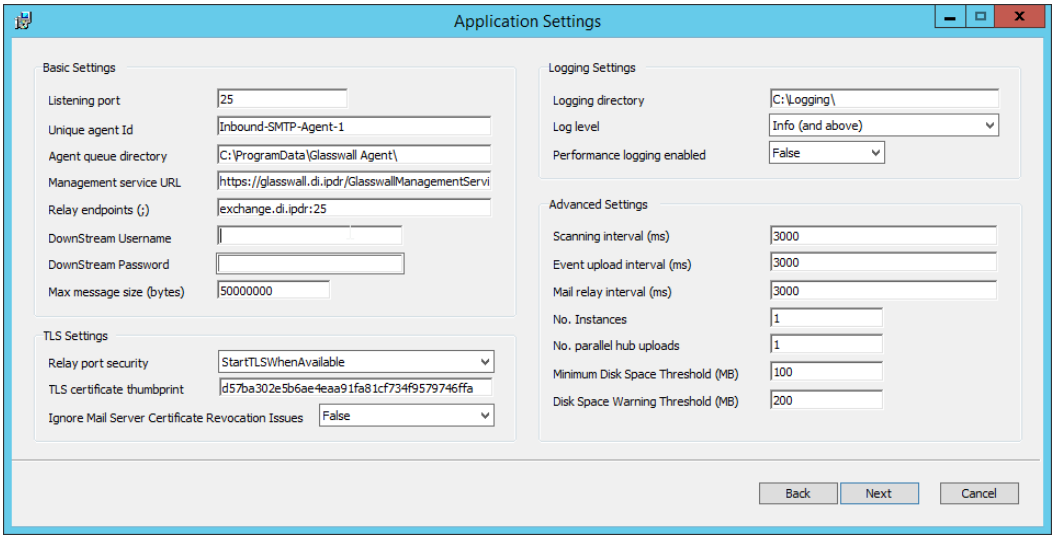
1. Run **SmtpAnalysisAgentInstaller.msi.**



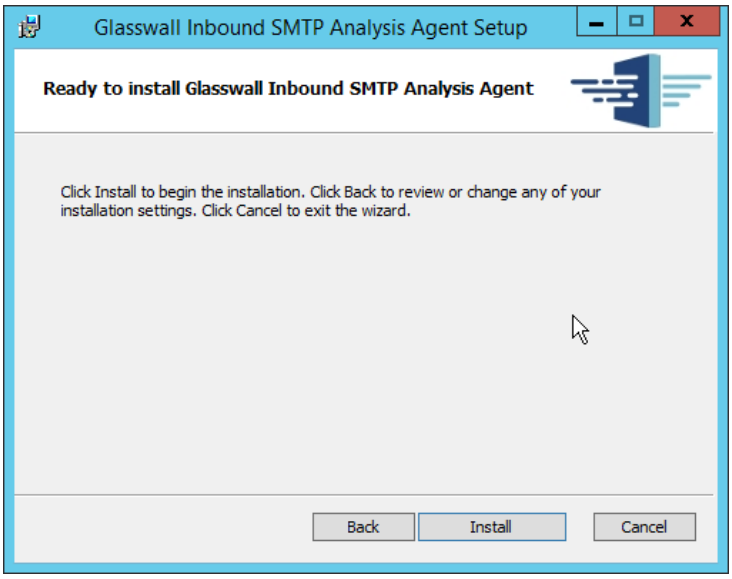
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**



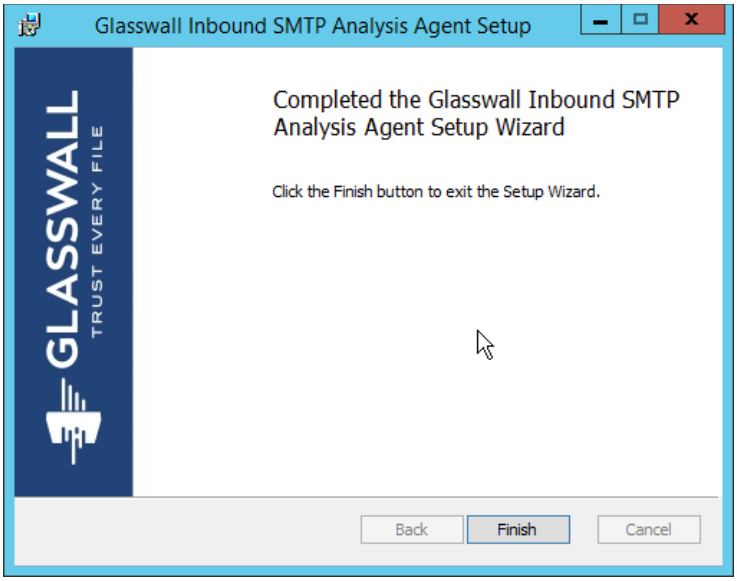
4. Click **Next.**
5. For **Listening** port, enter **25.**
6. For **Management service URL,** correct the domain to be the web domain of the IIS server (for example, glasswall.di.ipdr).
7. For the **Relay endpoints,** enter the address of the Exchange server, followed by the port (for example, exchange.di.ipdr:25).
8. For the **TLS certificate thumbprint,** enter the value from the **thumbprint** field on the certificate, without any spaces.



9. Click **Next.**



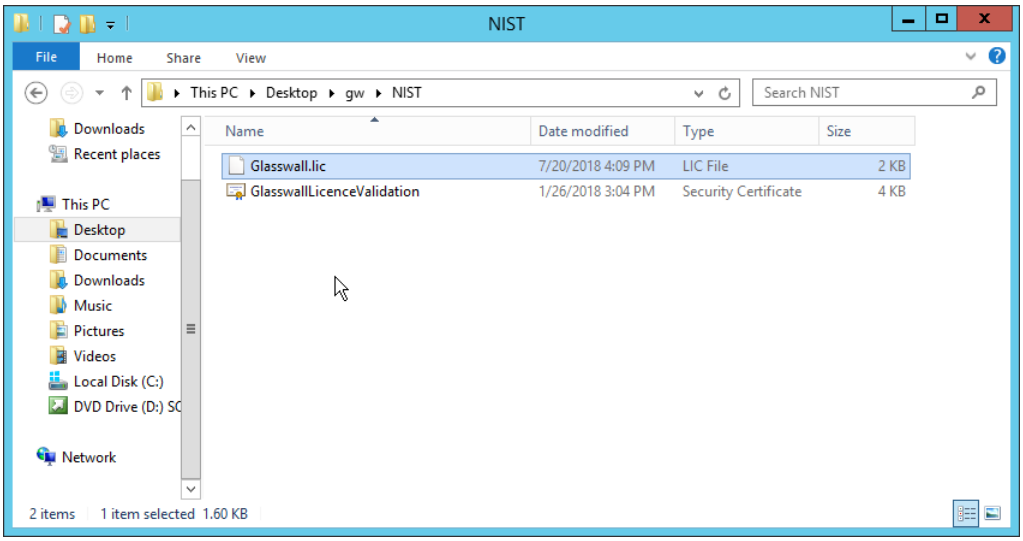
10. Click **Install.**



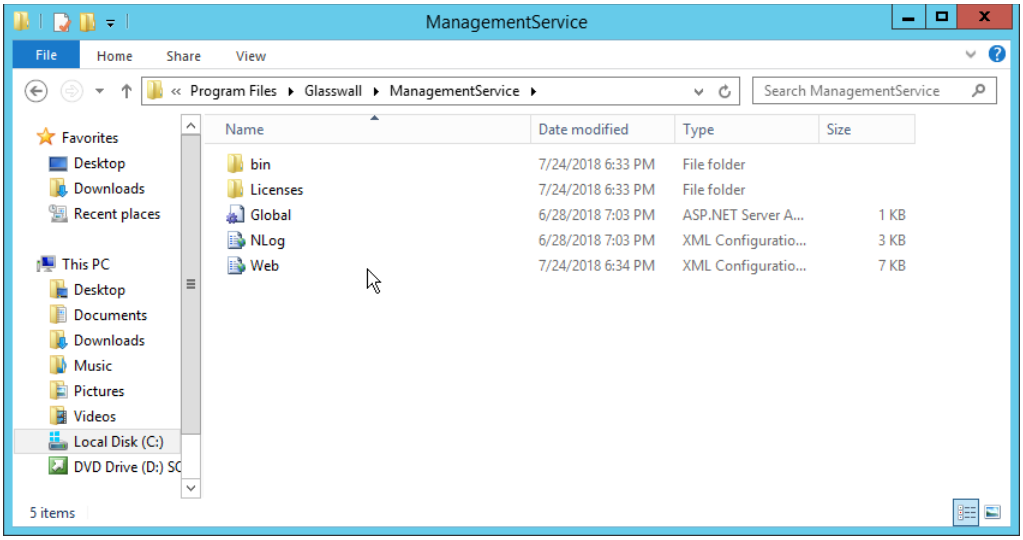
11. Click **Finish.**

2.7.2.6 *Distribute the Glasswall License File*

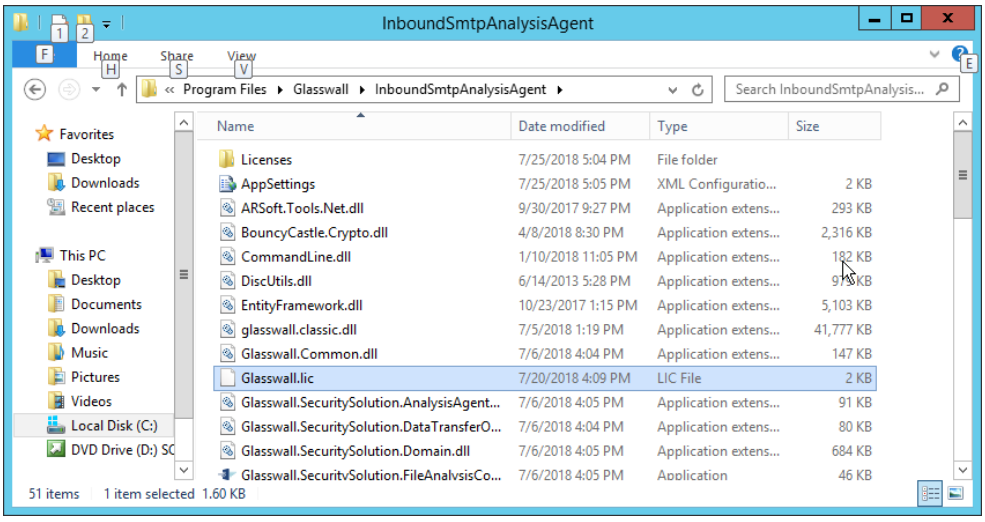
1. Copy the **Glasswall License** file to the following locations, assuming **Glasswall** was installed to *C:/Program Files/Glasswall.*



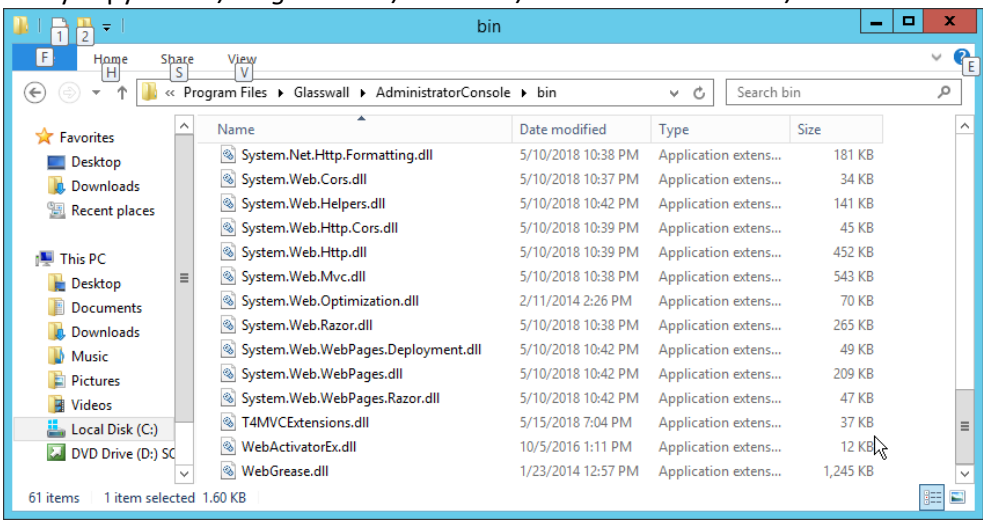
2. First copy it to *C:/Program Files/Glasswall/ManagementService/bin.*



3. Then copy it to *C:/Program Files/Glasswall/InboundSmtpAnalysisAgent.*



4. Lastly copy it to *C:/Program Files/Glasswall/AdministratorConsole/bin.*



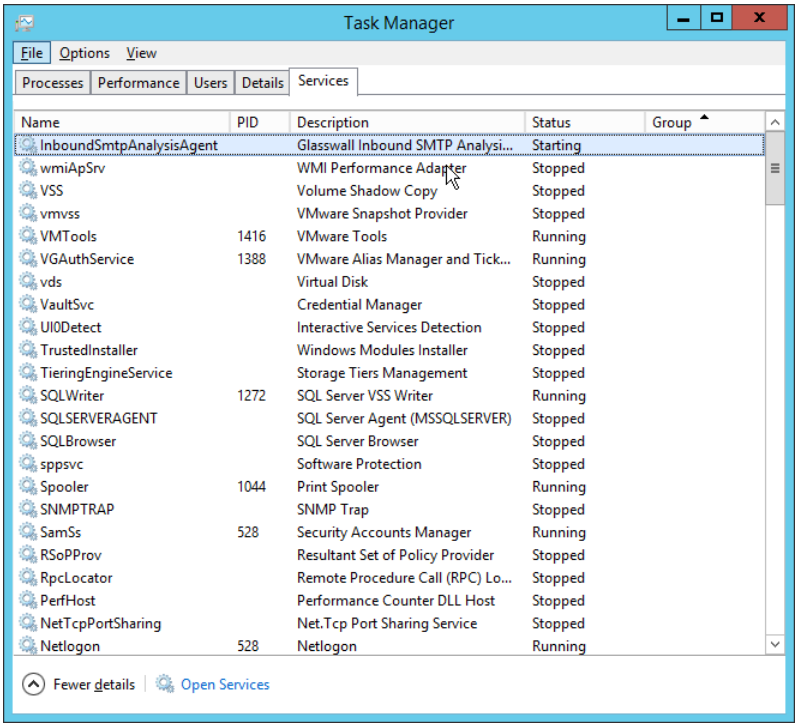
2.7.3 Configure Glasswall FileTrust

Please see https://docs.glasswallsolutions.com/#Configuring/Office%20365%20Integration.htm for an example configuration that routes email with attachments from Office365 to Glasswall FileTrust. Glasswall then forwards email back to Office365, after processing. Note that this linked configuration does not work with on-premise Exchange setups.

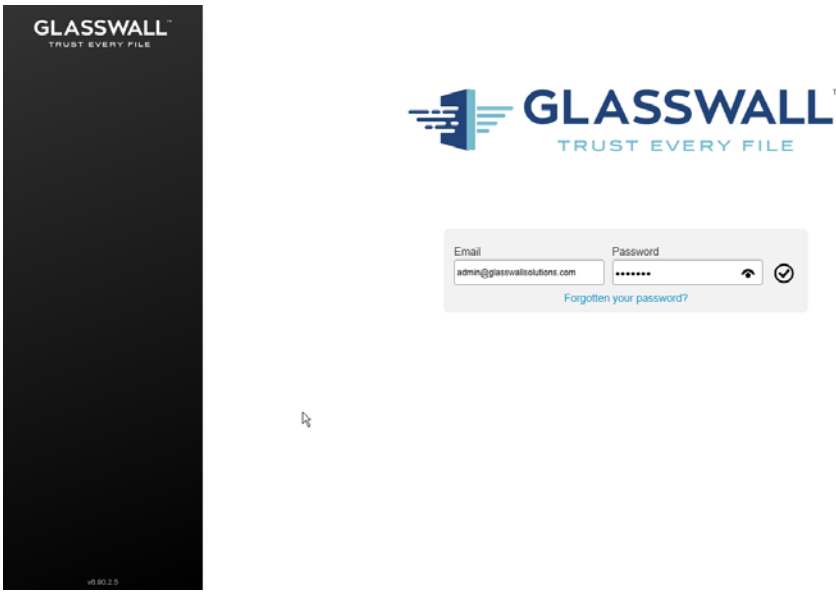
Instead, to achieve the goal of routing email through Glasswall, we redirect local MX records to Glasswall FileTrust. We implemented it this way because of limitations of the lab environment, but organizations should consult with the vendor for the best solution to route email through the email sanitization component, as other options may be available depending on the enterprise.

2.7.3.1 *Create a New Administrator Account*

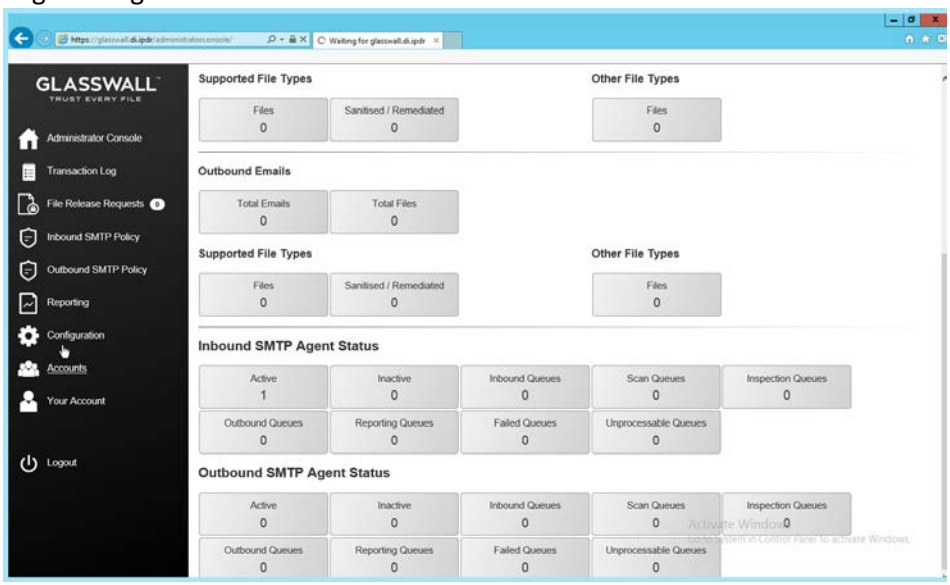
1. Open **Task Manager.**
2. In the **Services** tab, start the **InboundSmtpAnalysisAgent** service.



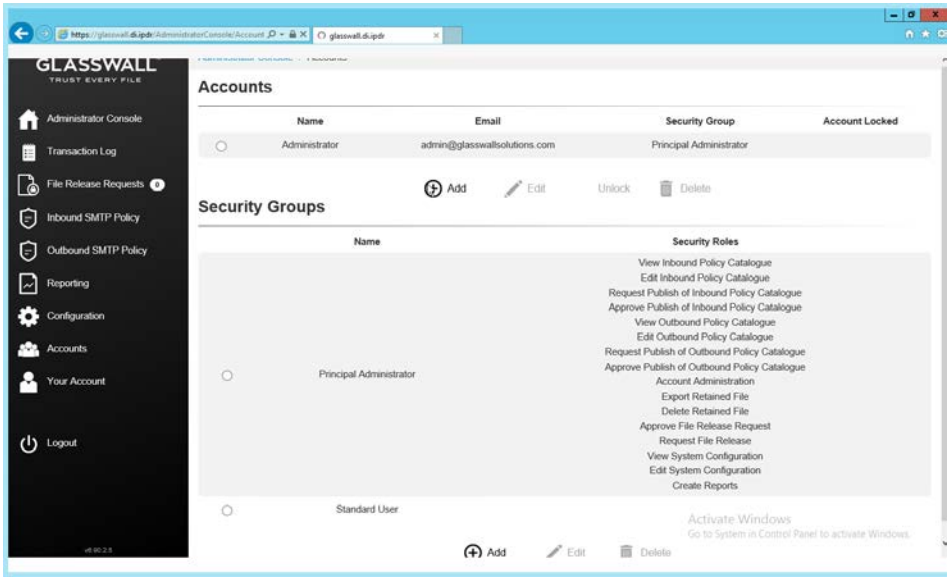
3. Close **Task Manager.**
4. Open a browser and navigate to the **Glasswall Administration Console** (for example, http://glasswall.di.ipdr/AdministratorConsole).
5. If this is the first time logging in, the default account will be **admin@glasswallsolutions.com,** and the password is **Welcome1?** .



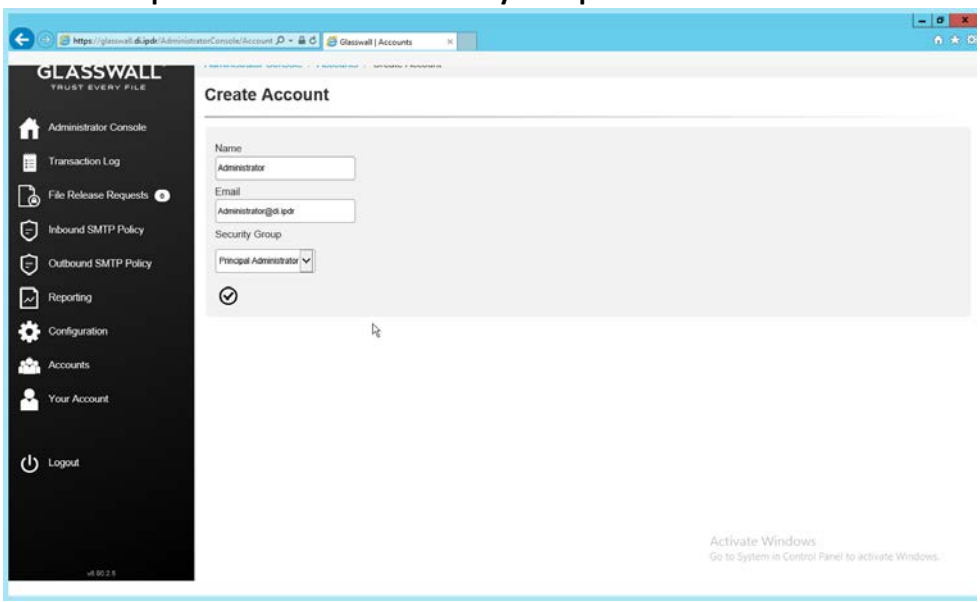
6. Log in using these credentials.



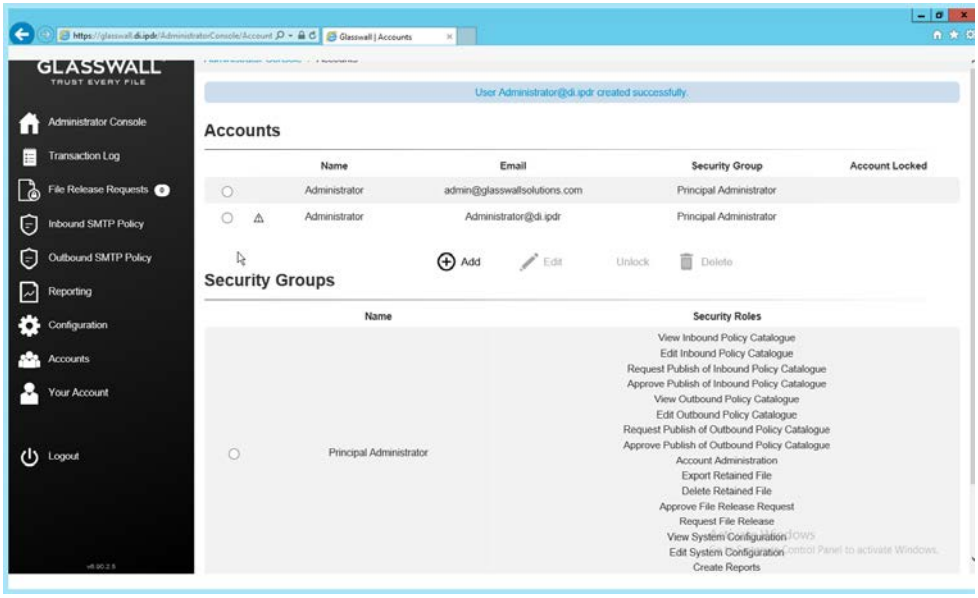
7. On the left sidebar, click **Accounts.**



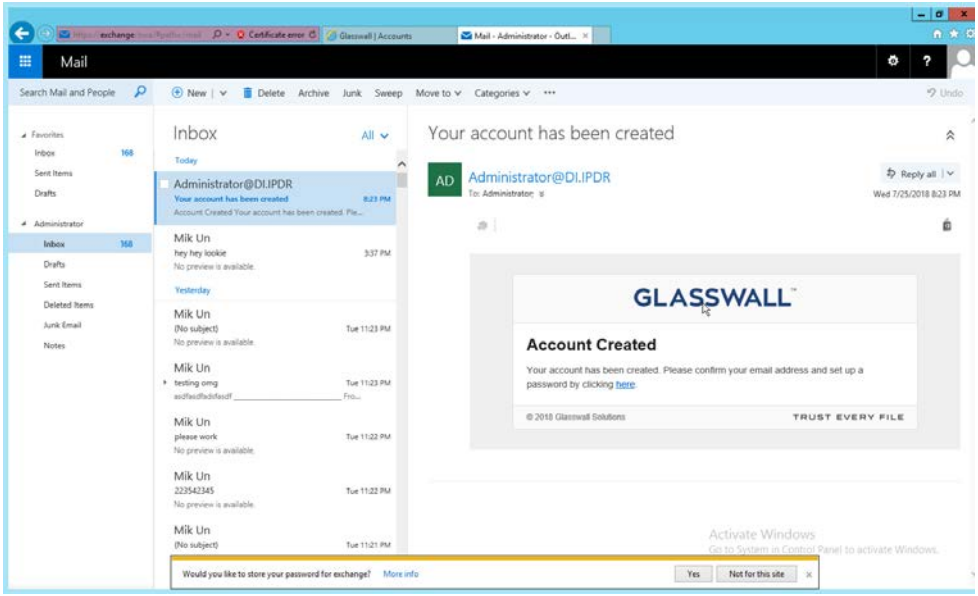
8. Under **Accounts**, click **Add.**
9. Enter the **name** and **email address** of an administrator account from the email server.
10. Select **Principal Administrator** for **Security Group.**



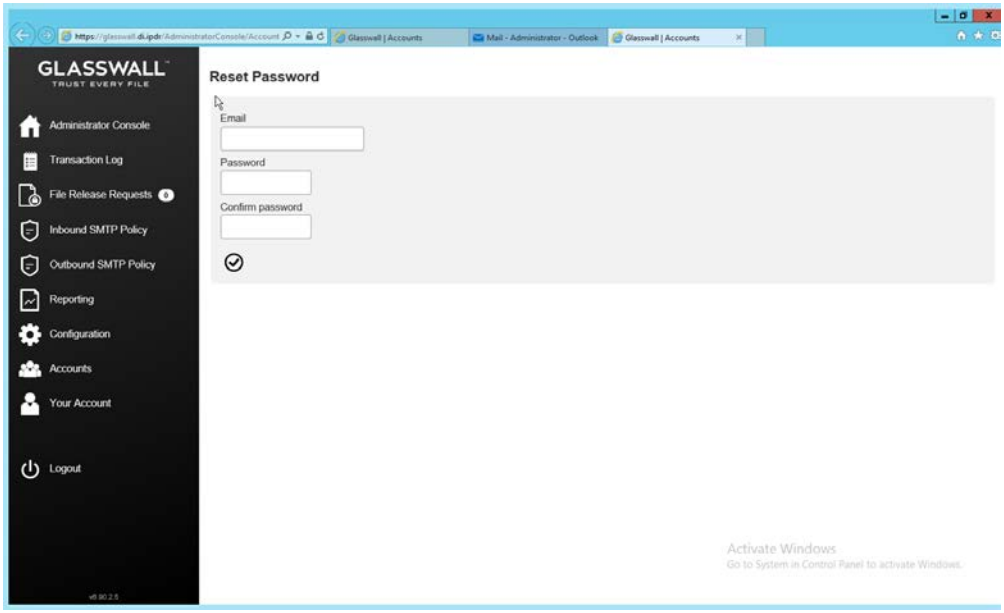
11. Click the **checkmark** button when finished.



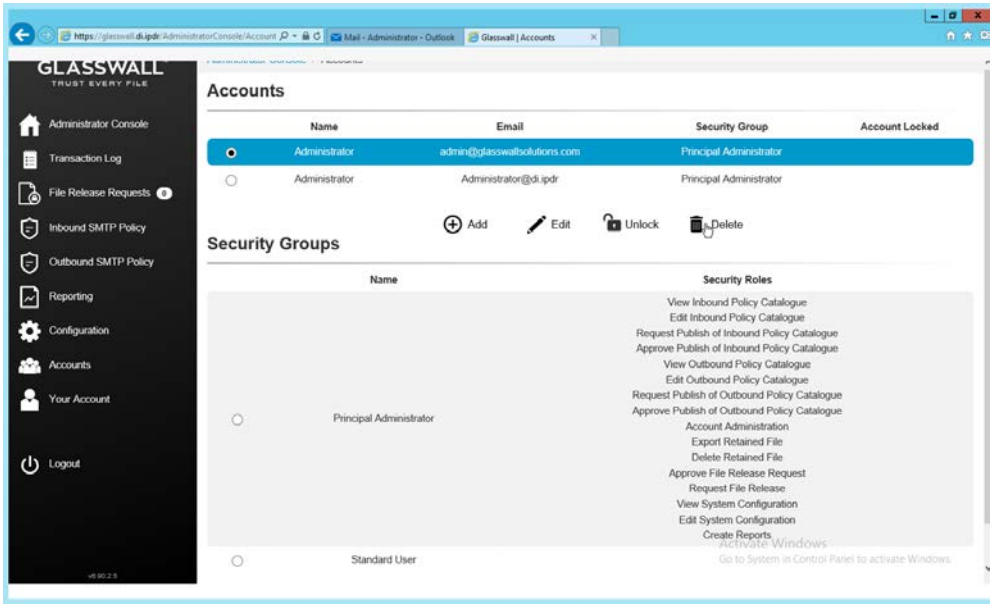
12. The new administrator account should be created.



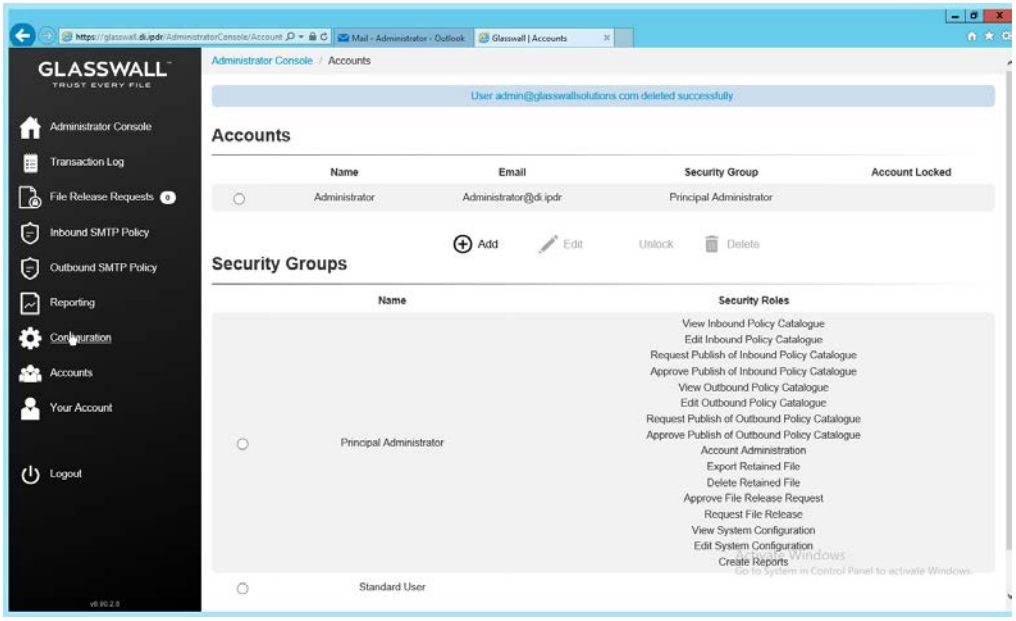
13. Check the email inbox of the specified email address for a confirmation email, and click the link in the email.



14. Enter the email address as well as a password for this account.
15. Log in as this user, and then go to **Accounts.**
16. Select the old (default) Administrator account.



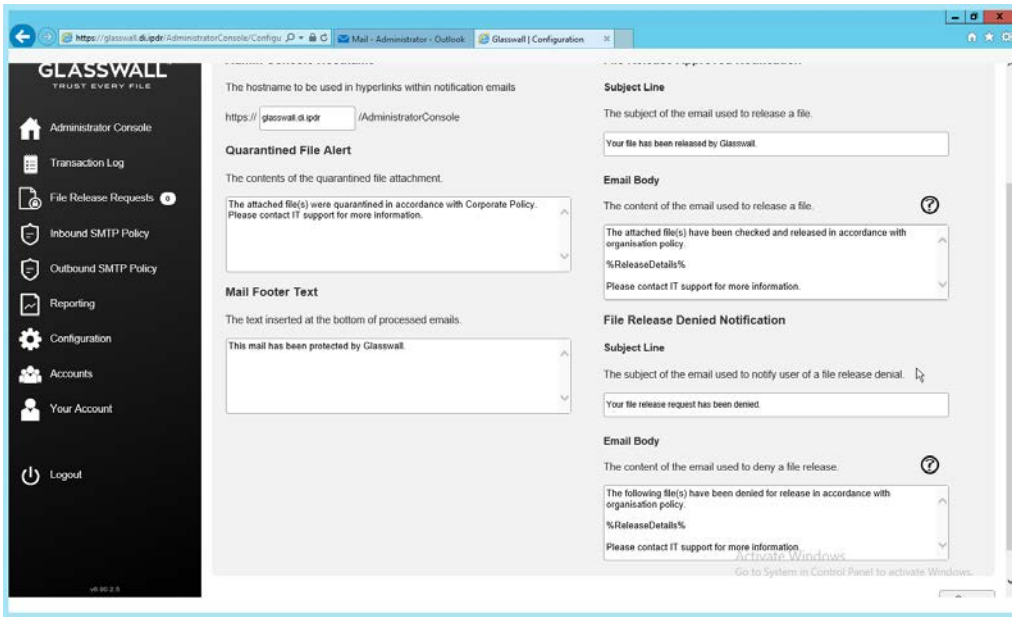
17. Click **Delete.**



18. This should remove the old administrator account (note: failure to remove this can result in a significant vulnerability for this server).

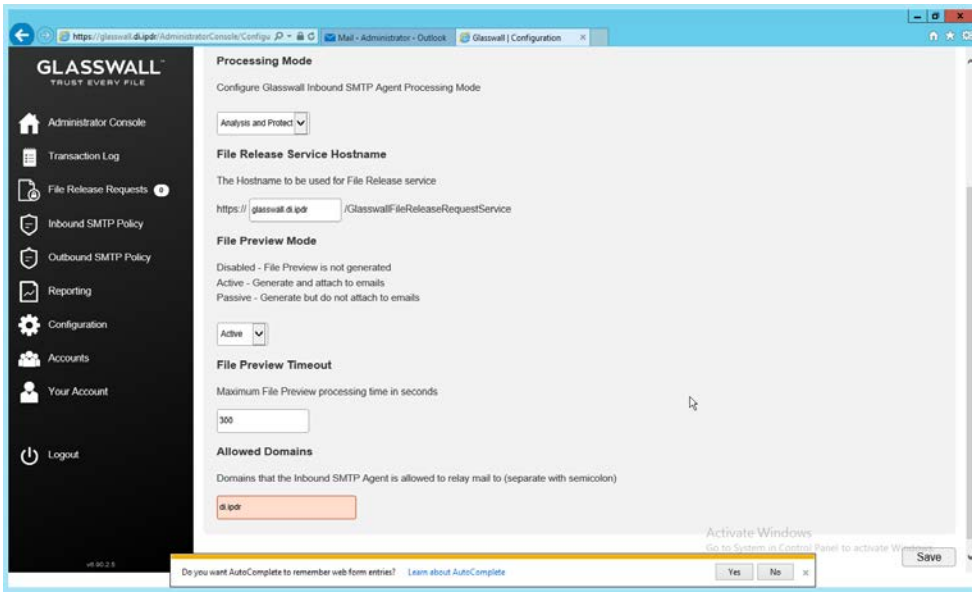
2.7.3.2 *Configure Notifications and Policies*

1. Click **Configuration** on the left sidebar.
2. Click the **Notifications** tab.



3. On this page, enter the web domain in the first input box (for example, glasswall.di.ipdr).

4. The various input boxes on this page allow you to specify the messages sent when files are quarantined, released, or prevented from being released.
5. Click the **Inbound Agents** tab.
6. Select **Analysis and Protect** for **Processing Mode.** (This analyzes and quarantines/reconstructs files based on policy.)
7. Select **Active** for **File Preview Mode.** (This provides clients with a preview of their received files if they were quarantined, so they can determine whether they should request the file be released.)
8. Enter the **domain** for **Allowed Domains** (for example, di.ipdr).



9. Click **Save.**

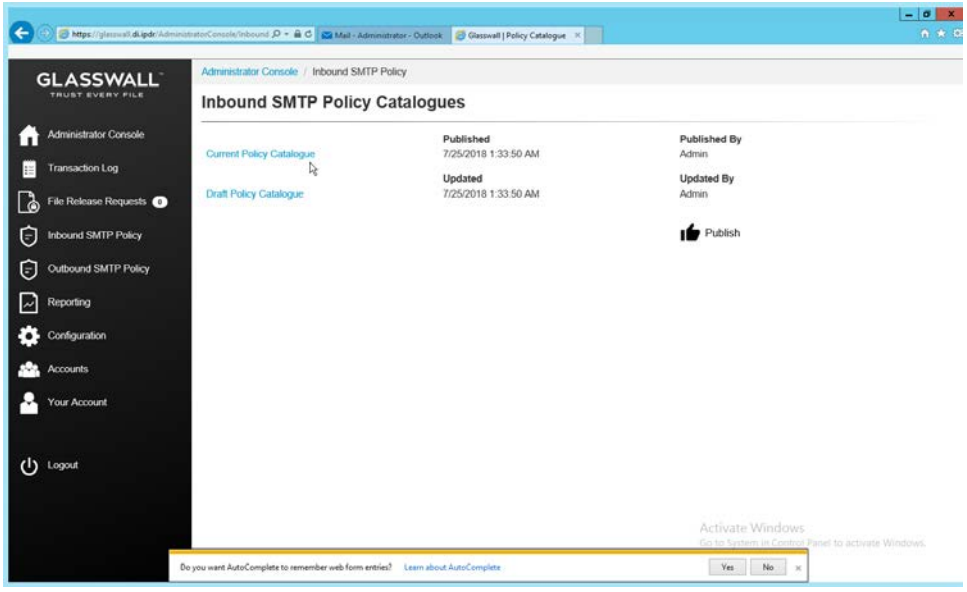
2.7.3.3 *Configure Inbound SMTP Policy*

This section discusses SMTP policy under Glasswall FileTrust. There are several layers of granularity for configuring Email policy. Because policy is dependent on the organization's needs, we will not prescribe a policy but will showcase how a policy is formed.

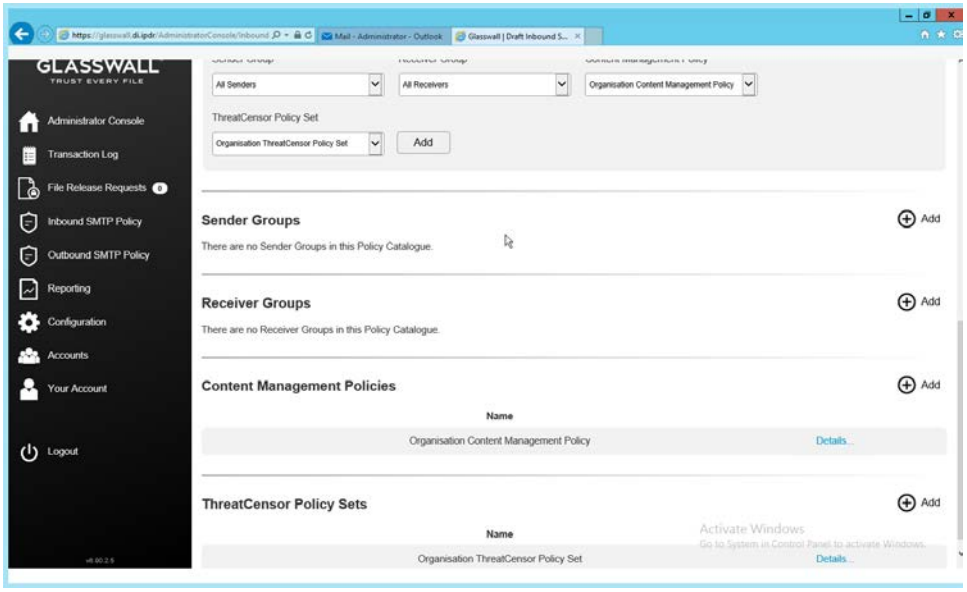
Policy in Glasswall FileTrust consists of **Sender Groups, Receiver Groups, Content Management Policies,** and **ThreatCensor Policy Sets. Receiver groups** allow for the specification of users who receive email. **Sender groups** allow for the specification of emails received from specific senders. **Content Management Policies** refer to the default policy on various filetypes. Lastly, **ThreatCensor Policy Sets** allow for the specification of policy on specific error codes; through this it is possible to place policies on encrypted email, for example, depending on the organization's needs.

2.7.3.4 *Create a Receiver Group*

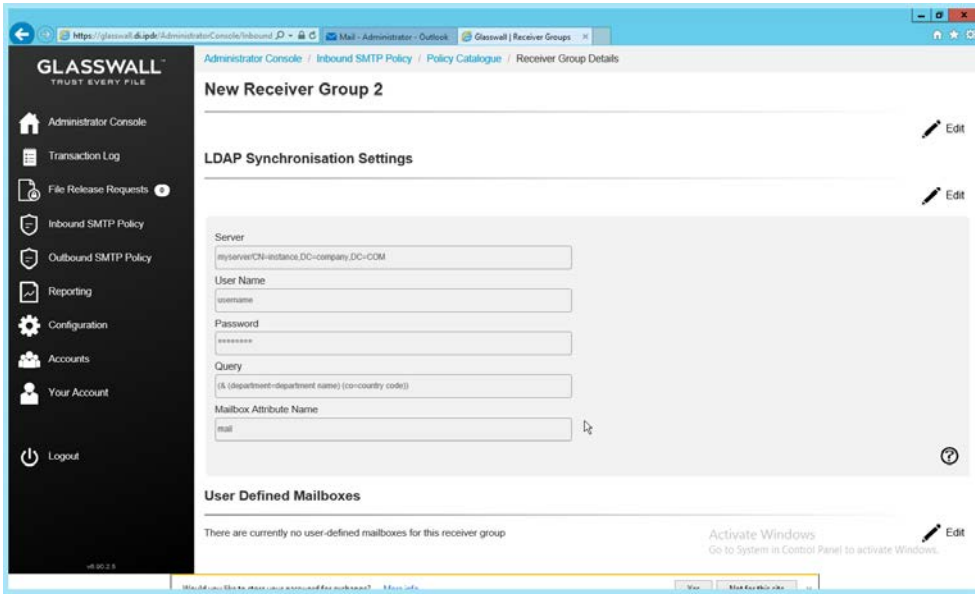
1. On the left sidebar, click **Inbound SMTP Policy.**
2. Click **Draft Policy Catalogue.**



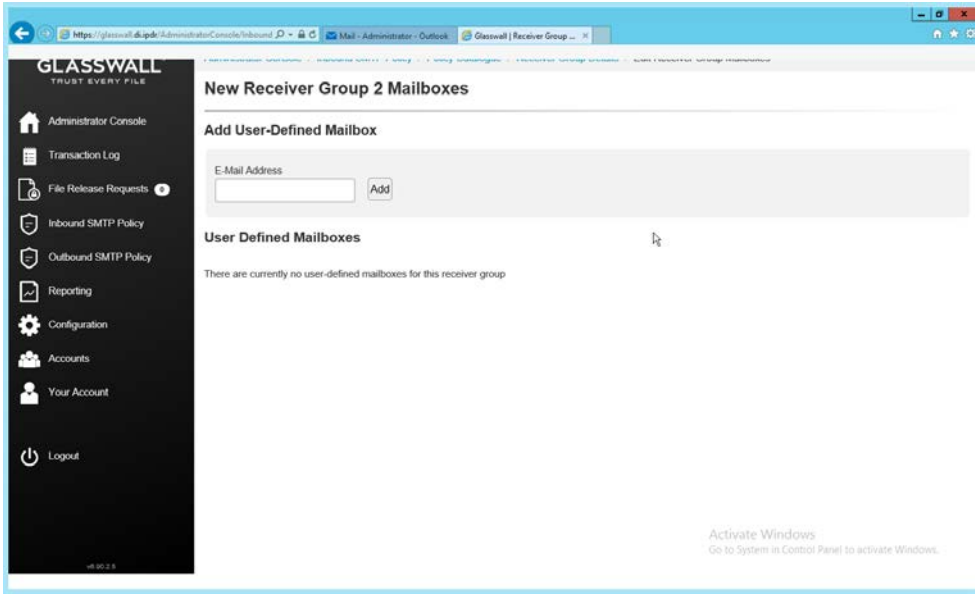
3. Under **Receiver Groups,** click **Add.**



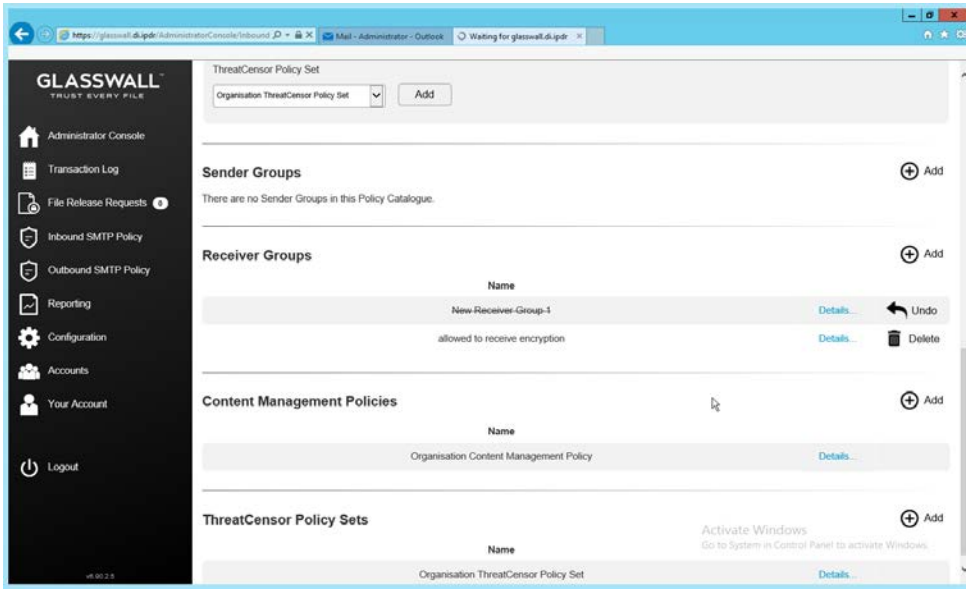
4. Under **User Defined Mailboxes,** click **Edit.**



5. Enter the email address(es) of users who should be in this receiver group.



6. Click **Add.**
7. When finished, return to the **Policy Catalogue** page.

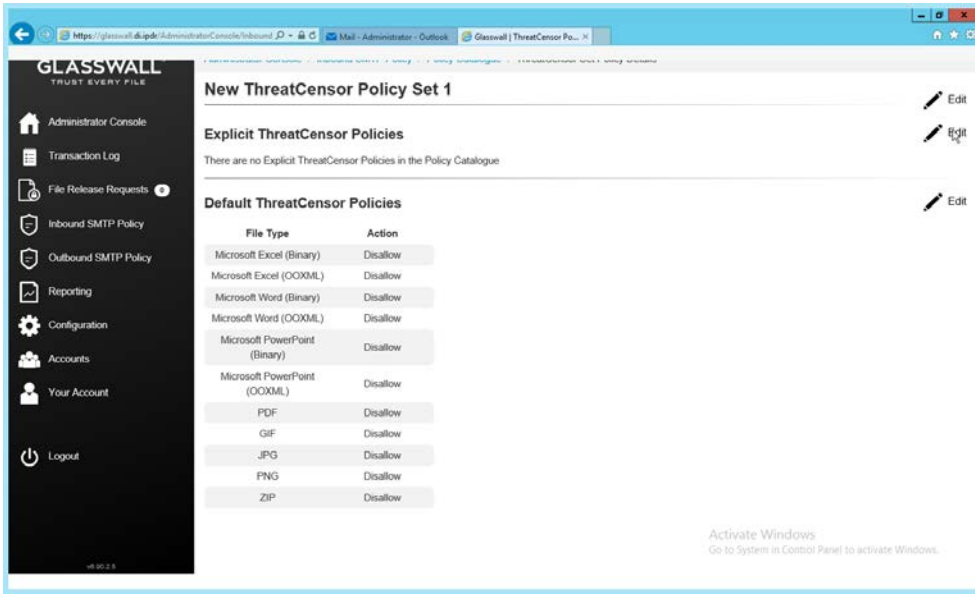


1189

2.7.3.5 *Create a ThreatCensor Policy Set*

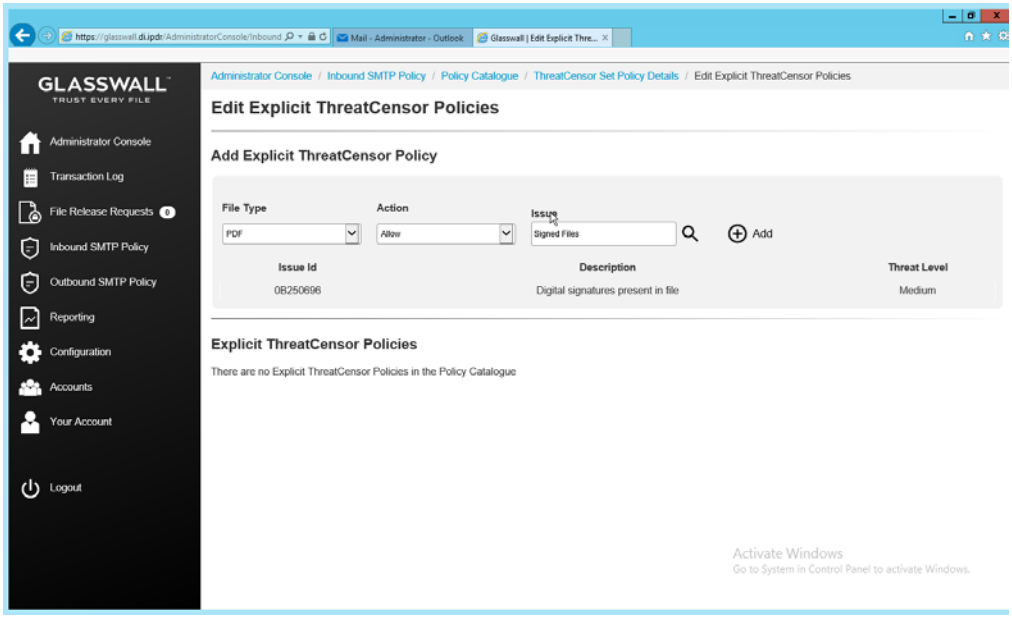
1190

1191 **1.** Under **ThreatCensor Policy Sets,** click **Add.**



1192

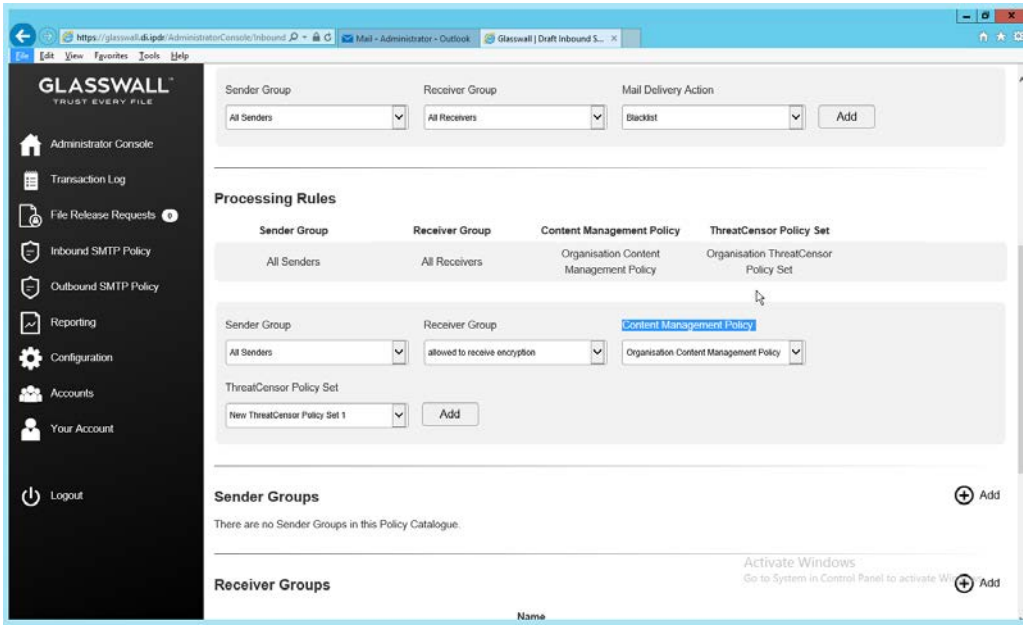
1193 **2.** Under **Explicit ThreatCensor Policies,** click **Edit.**



3. Select the **File Type** and **Action** for the rule.
4. Under **Issue,** click the magnifying glass to search for an error code.
5. Return to the **Policy Catalogue** page when finished.

2.7.3.6 *Create a Processing Rule*

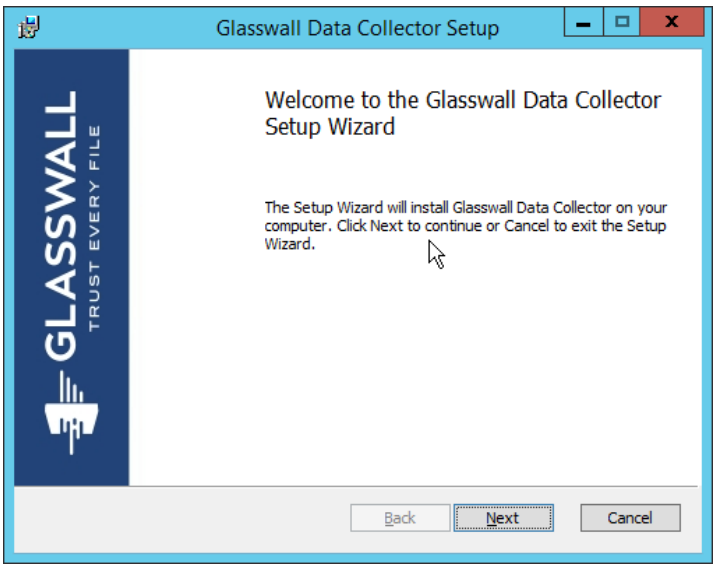
1. Under Processing Rules, select the appropriate **Sender Group, Receiver Group, Content Management Policy,** and **ThreatCensor Policy Set.**



2. Click **Add.**
3. This allows for granular policy for email inspection, quarantine, and reconstruction.

2.7.4 Configure Intelligence Sharing

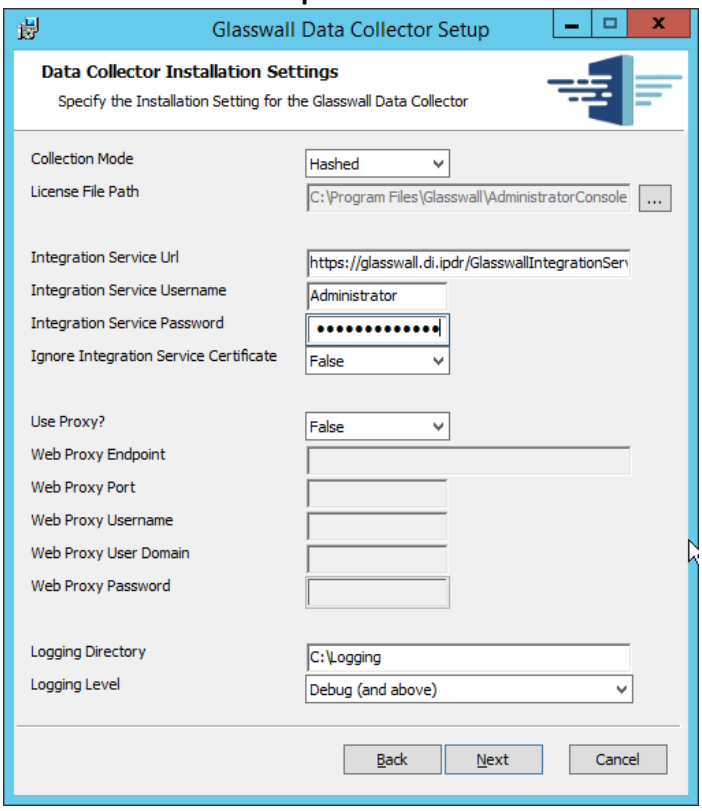
1. Run **DataCollectorInstaller.msi.**



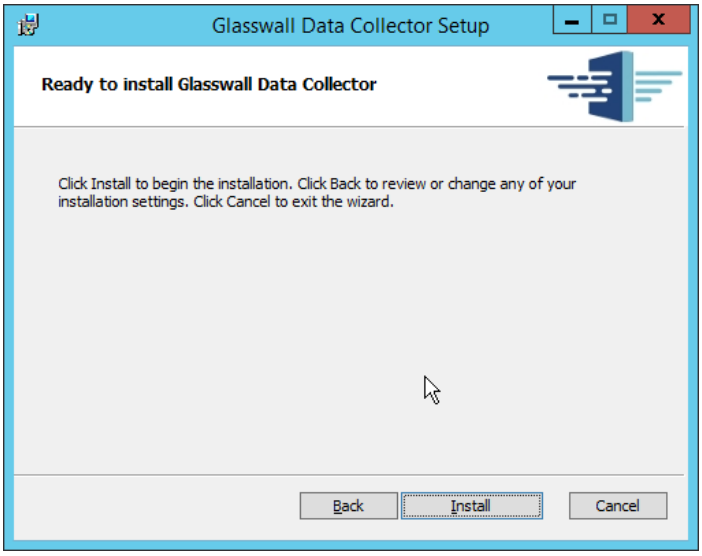
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**

4. Click **Next.**
5. Select **Hashed** for **Collection Mode** (especially if your data is sensitive; this will prevent the release of any identifying information).

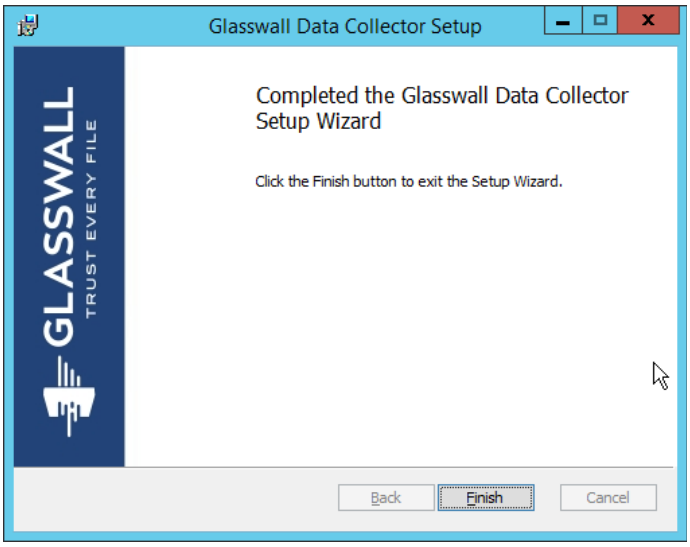
6. For **Integration Service Url** replace **localhost** with the name of the computer running the **Integration Service.**
7. Enter the **username** and **password.**



8. Click **Next.**



9. Click **Install.**



10. Click **Finish.**

2.8 Micro Focus ArcSight Enterprise Security Manager

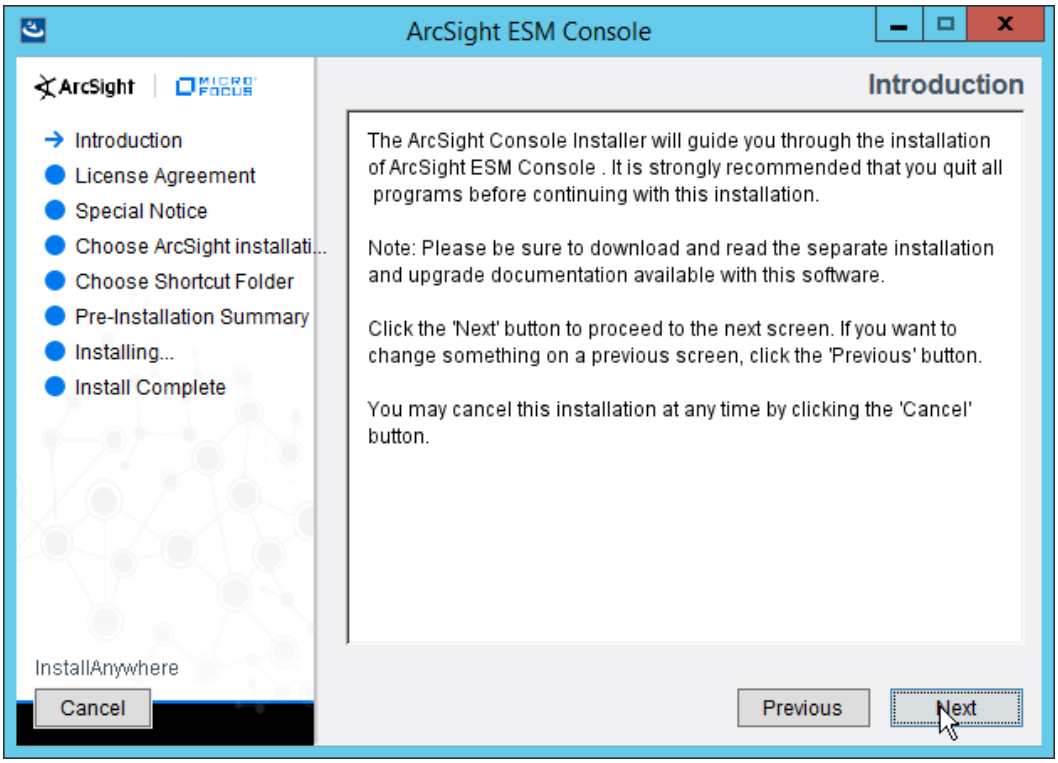
Micro Focus ArcSight Enterprise Security Manager (ESM) is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

This installation guide assumes a pre-configured CentOS 7 machine with 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.

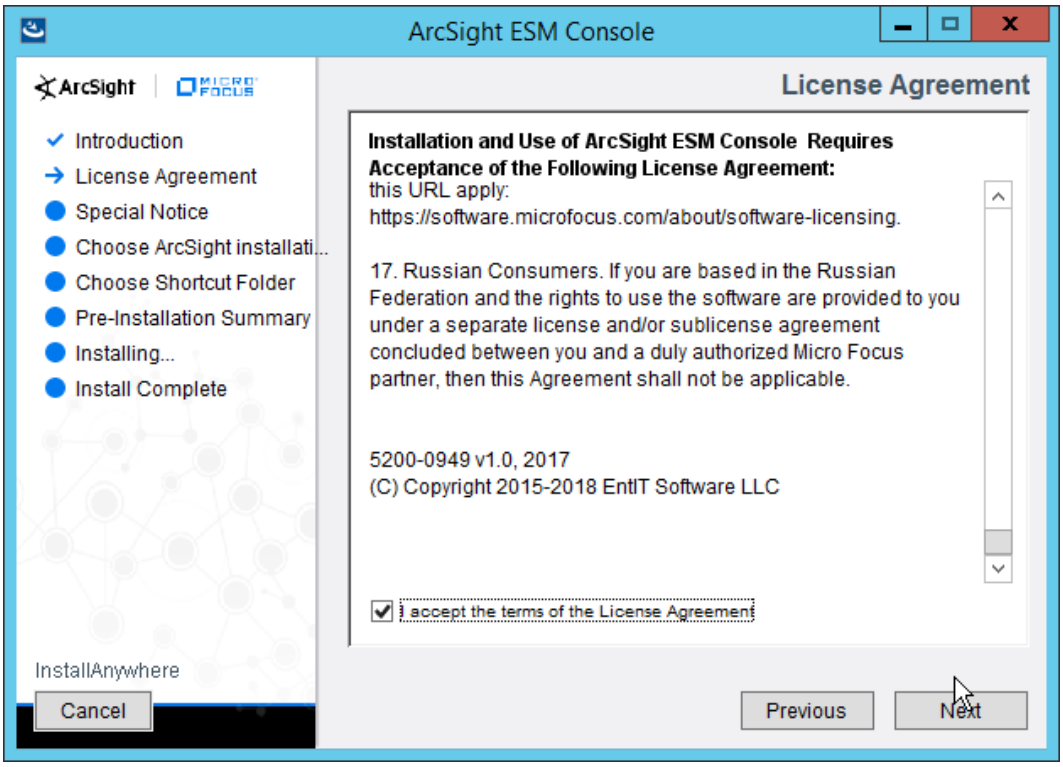
Installation instructions are included for both Windows and UNIX machines, as well as for collecting from multiple machines. Furthermore, integrations with other products in the build are included in later sections.

2.8.1 Install the ArcSight Console

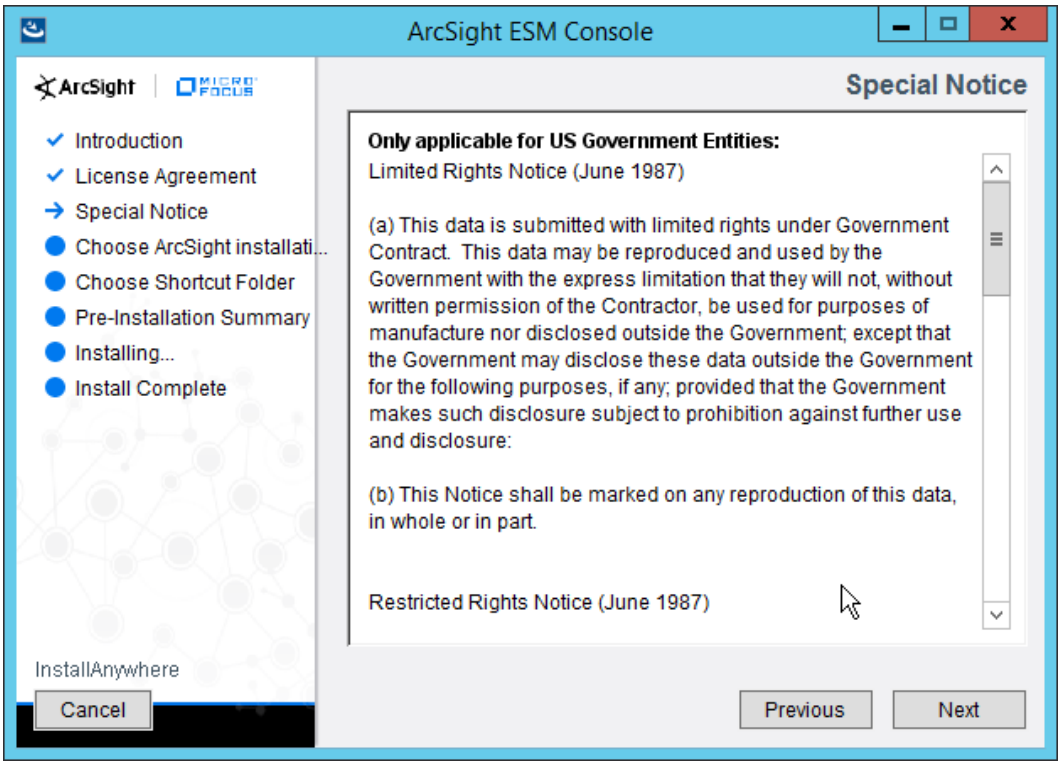
1. Run **ArcSight-7.0.0.2436.1-Console-Win.exe.**



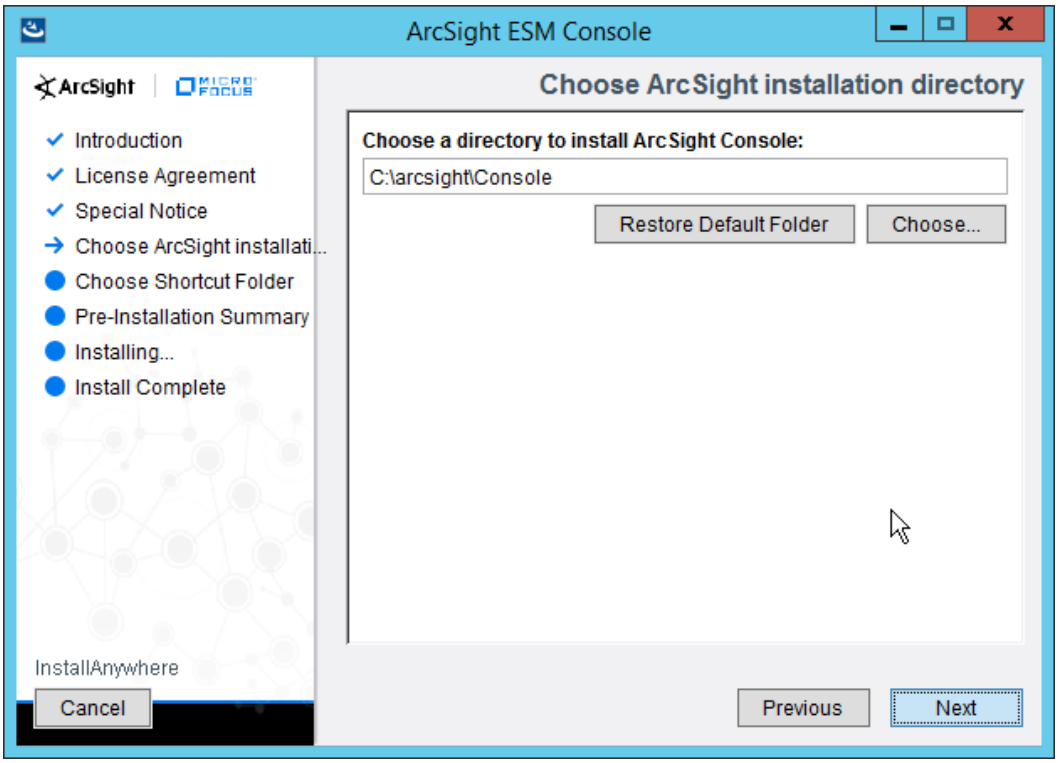
2. Click **Next.**
3. Check the box next to **I accept the License Agreement.**


ArcSight ESM Console
ArcSight
Introduction
License Agreement
Special Notice
Choose ArcSight installati...
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere
Cancel
License Agreement
Installation and Use of ArcSight ESM Console Requires Acceptance of the Following License Agreement:
this URL apply:
https://software.microfocus.com/about/software-licensing.
17. Russian Consumers. If you are based in the Russian Federation and the rights to use the software are provided to you under a separate license and/or sublicense agreement concluded between you and a duly authorized Micro Focus partner, then this Agreement shall not be applicable.
5200-0949 v1.0, 2017
(C) Copyright 2015-2018 EntIT Software LLC
I accept the terms of the License Agreement
Previous
Next

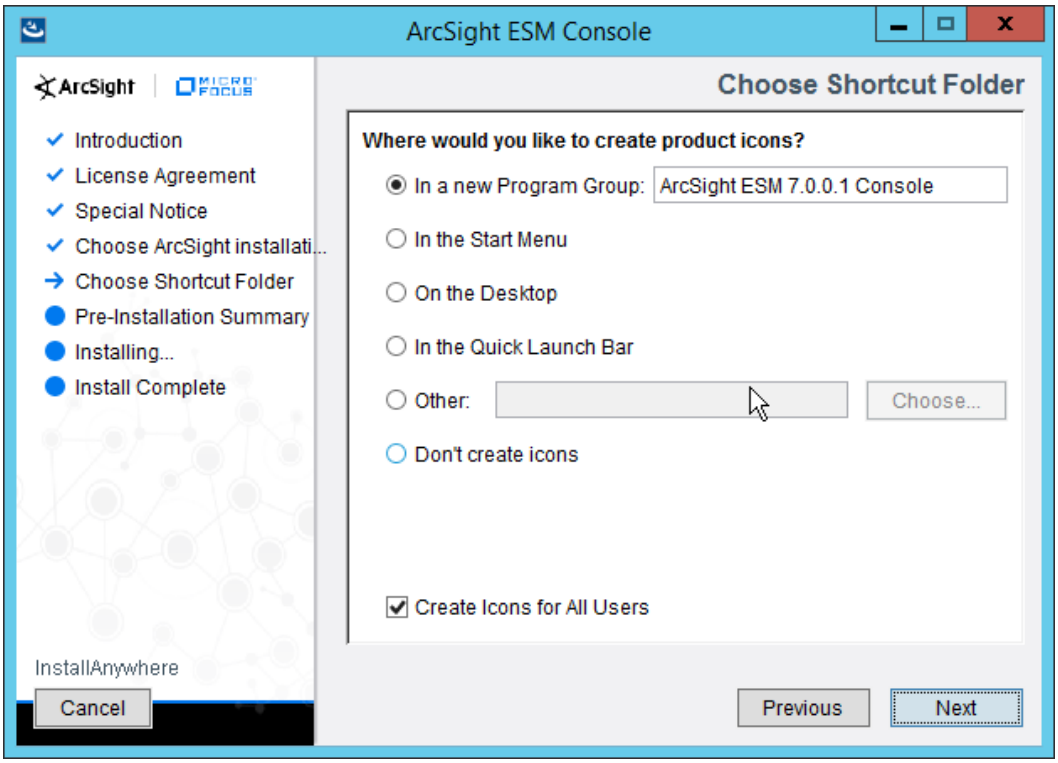
4. Click **Next.**


ArcSight ESM Console
ArcSight
Introduction
License Agreement
Special Notice
Choose ArcSight installati...
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere
Cancel
Special Notice
Only applicable for US Government Entities:
Limited Rights Notice (June 1987)
(a) This data is submitted with limited rights under Government Contract. This data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure:
(b) This Notice shall be marked on any reproduction of this data, in whole or in part.
Restricted Rights Notice (June 1987)
Previous
Next

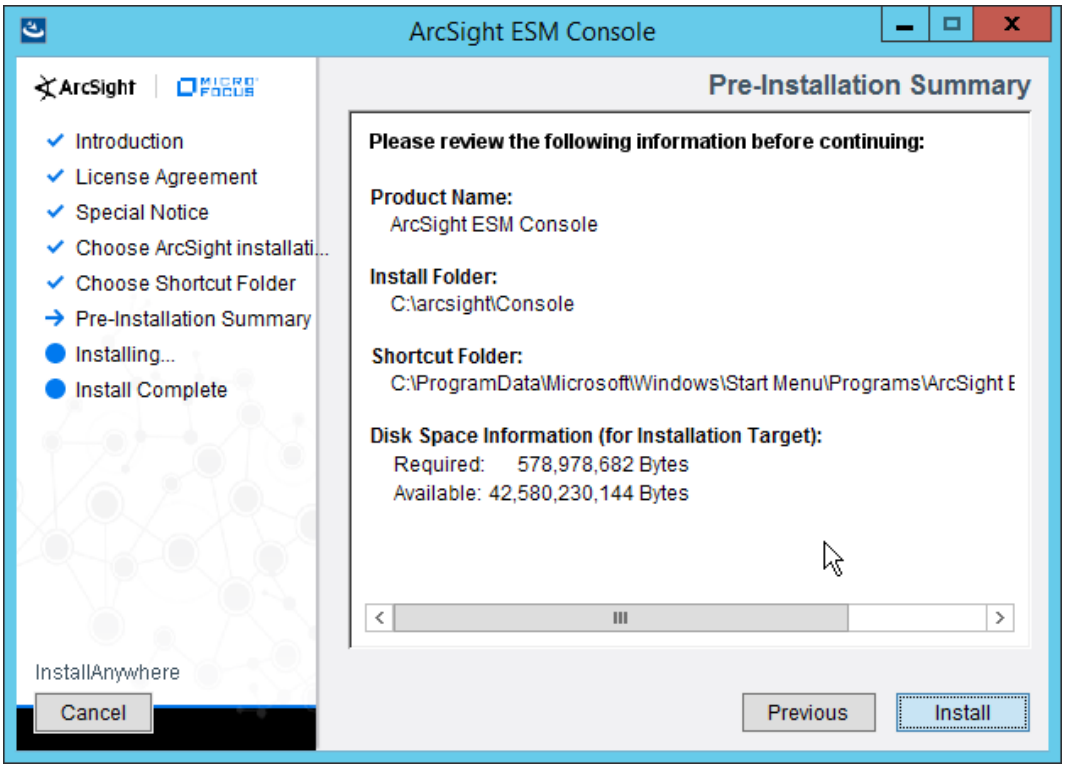
5. Click **Next.**


ArcSight ESM Console
ArcSight
MICRO FOCUS
Introduction
License Agreement
Special Notice
Choose ArcSight installati...
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere
Cancel
Choose ArcSight installation directory
Choose a directory to install ArcSight Console:
C:\arcsight\Console
Restore Default Folder
Choose...
Previous
Next

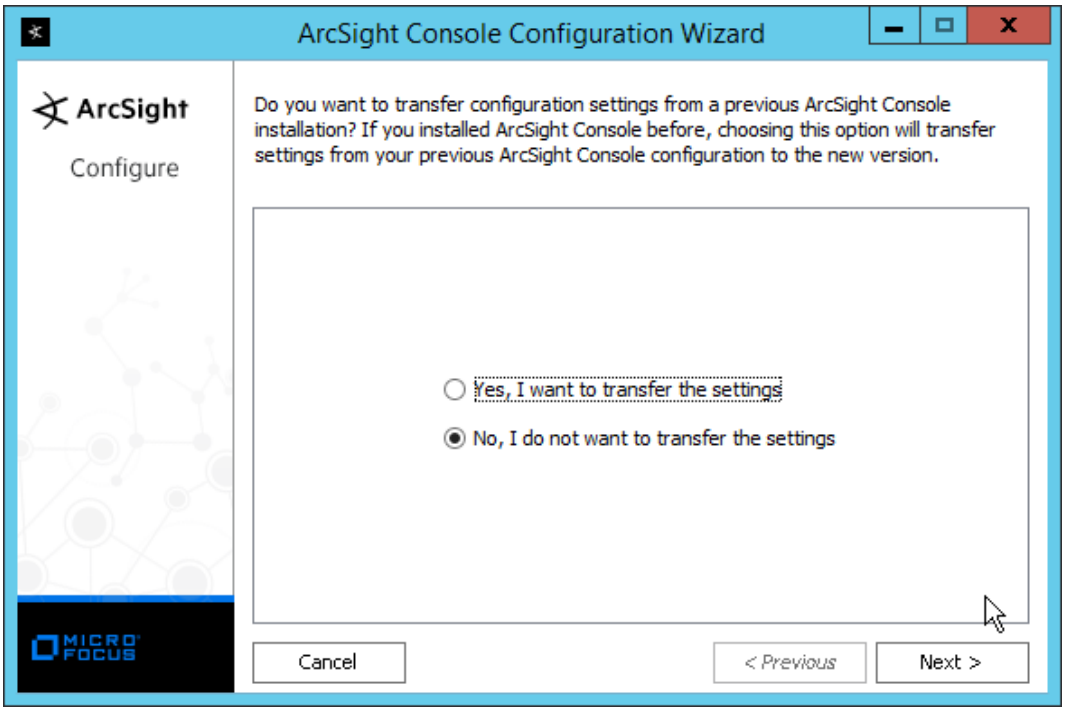
6. Click **Next.**


ArcSight ESM Console
ArcSight
Introduction
License Agreement
Special Notice
Choose ArcSight installati...
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere
Cancel
Choose Shortcut Folder
Where would you like to create product icons?
In a new Program Group:
ArcSight ESM 7.0.0.1 Console
In the Start Menu
On the Desktop
In the Quick Launch Bar
Other:
Choose...
Don't create icons
Create Icons for All Users
Previous
Next

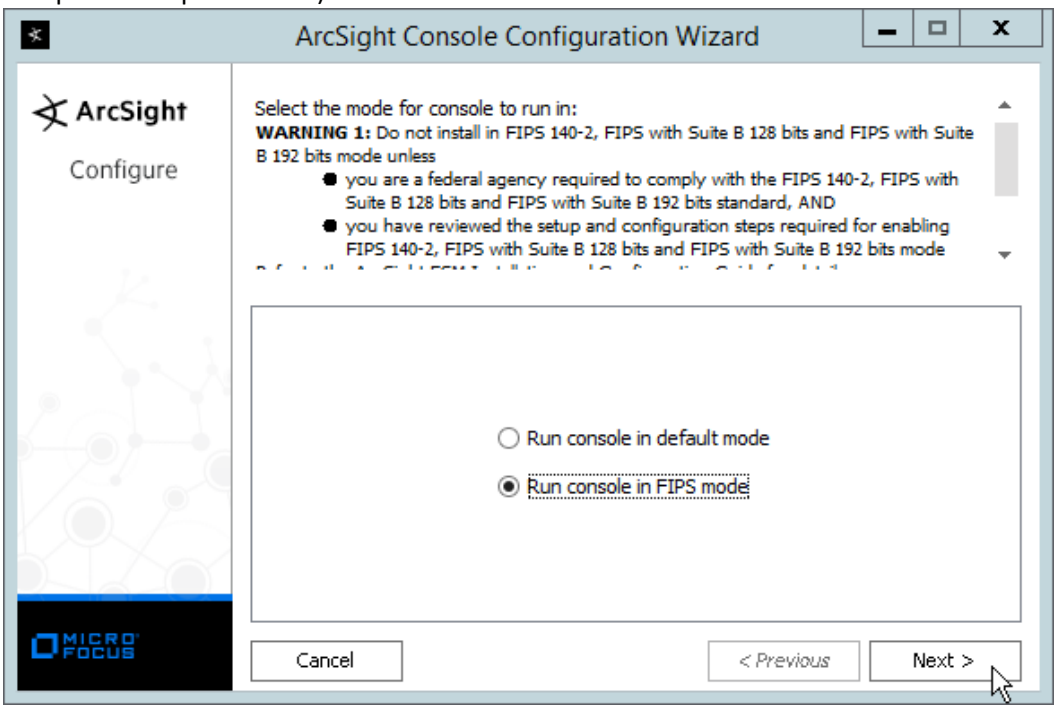
7. Click **Next.**



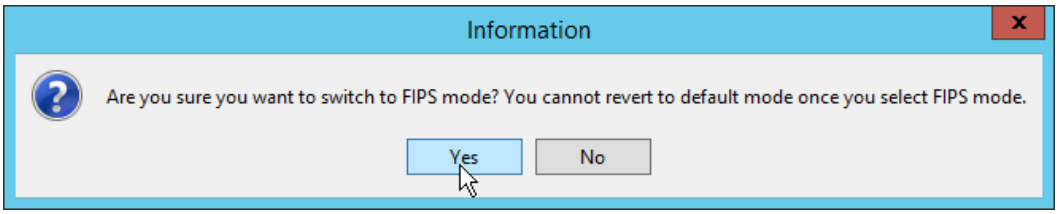
8. Click **Install.**
9. Select **No, I do not want to transfer the settings.**



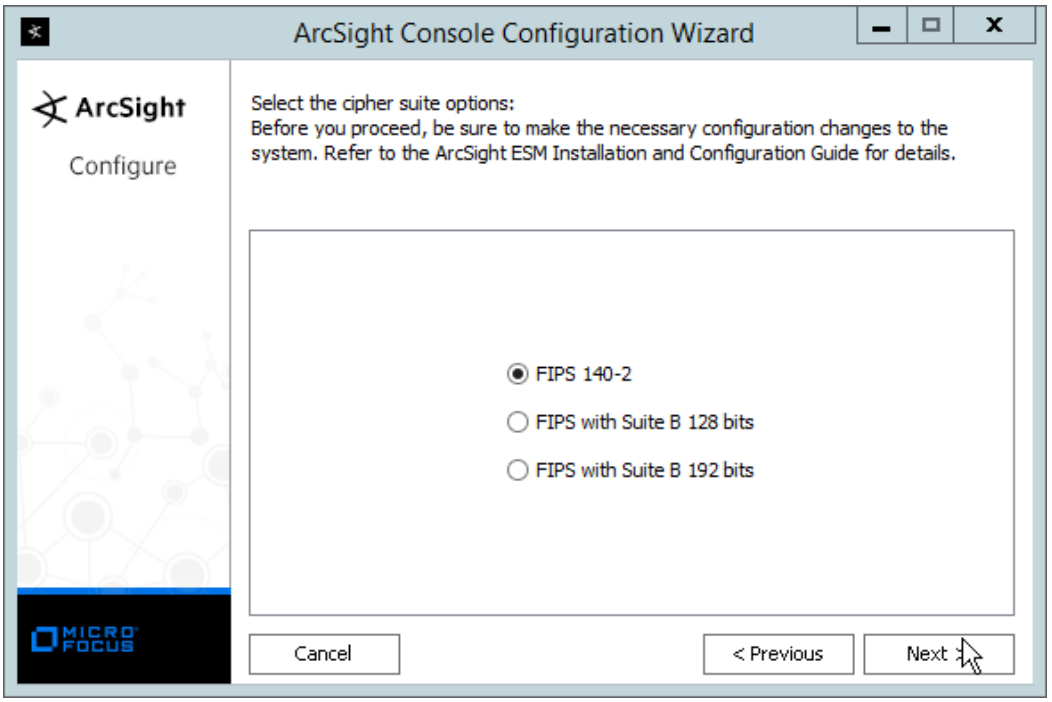
10. Click **Next.**
11. Select **Run console in default mode.** (This can be changed later according to your organization's compliance requirements.)



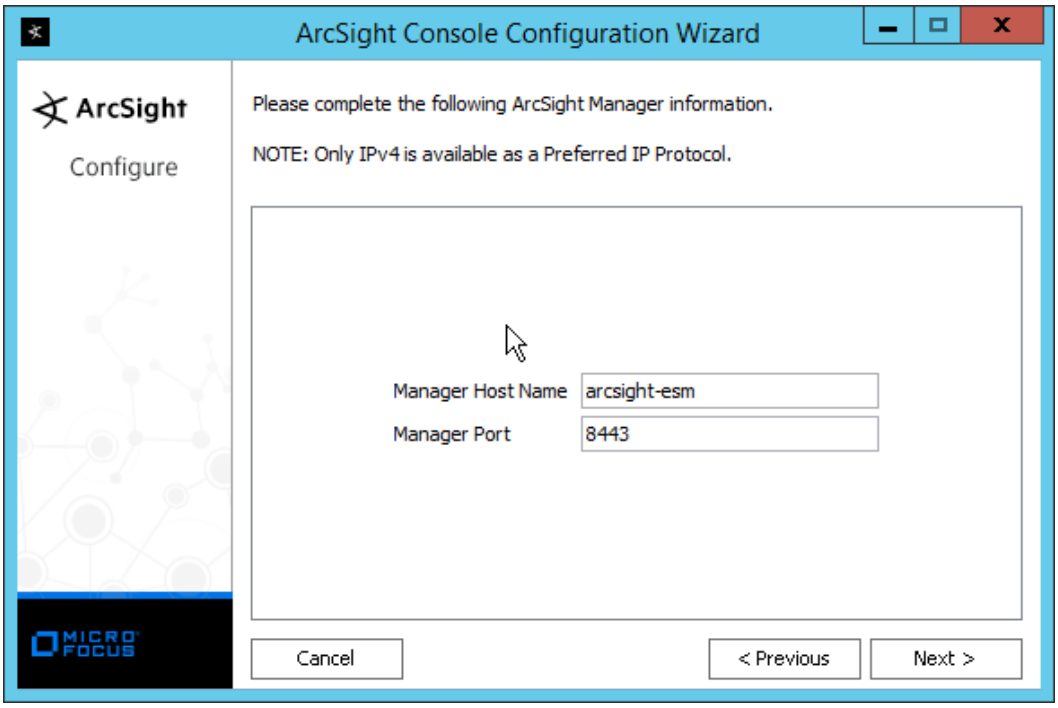
12. Click **Next.**



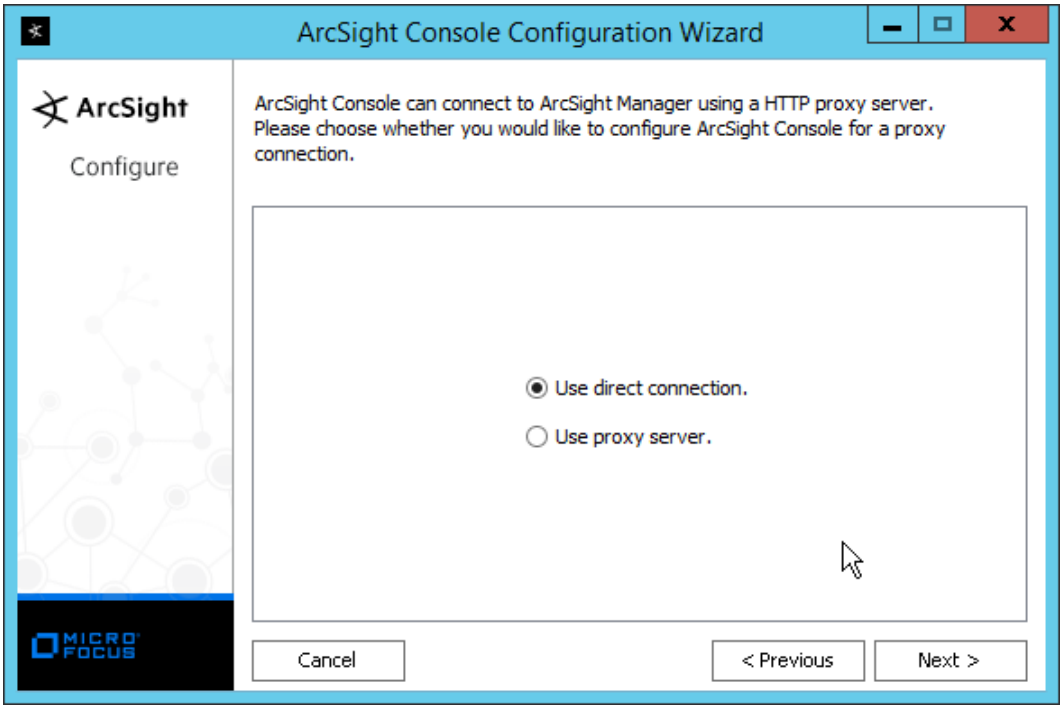
13. Click **Yes.**
14. Select **FIPS 140-2.**



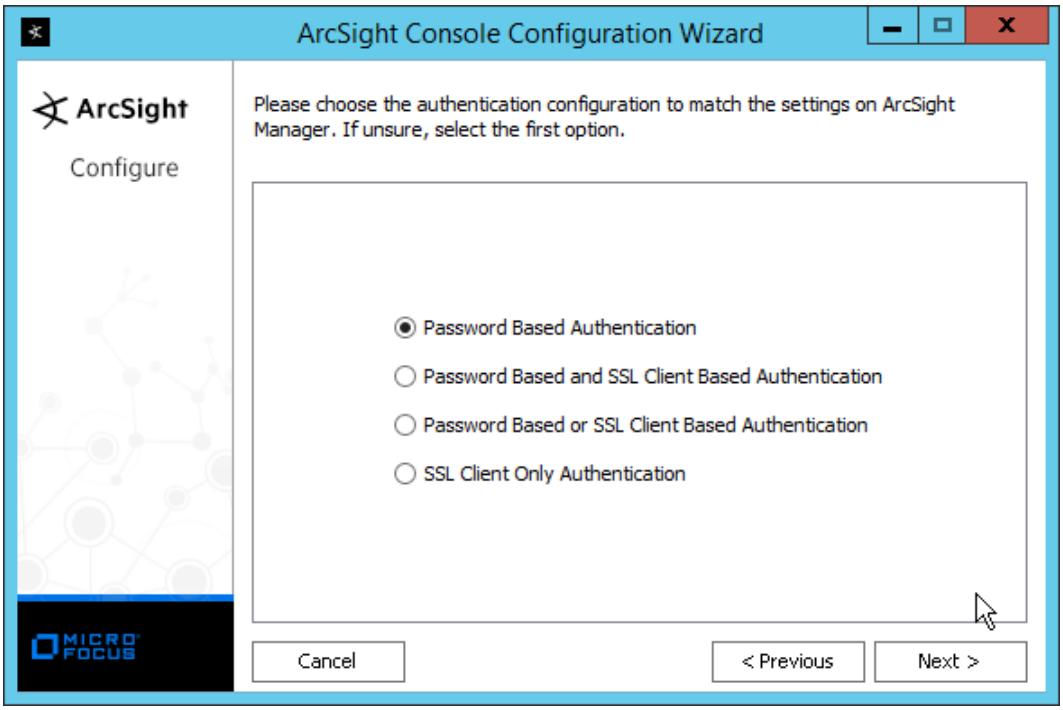
15. Click **Next.**
16. Enter the **hostname** of the ESM server for **Manager Host Name.**
17. Enter the **port** that ESM is running on for **Manager Port** (default: **8443**).



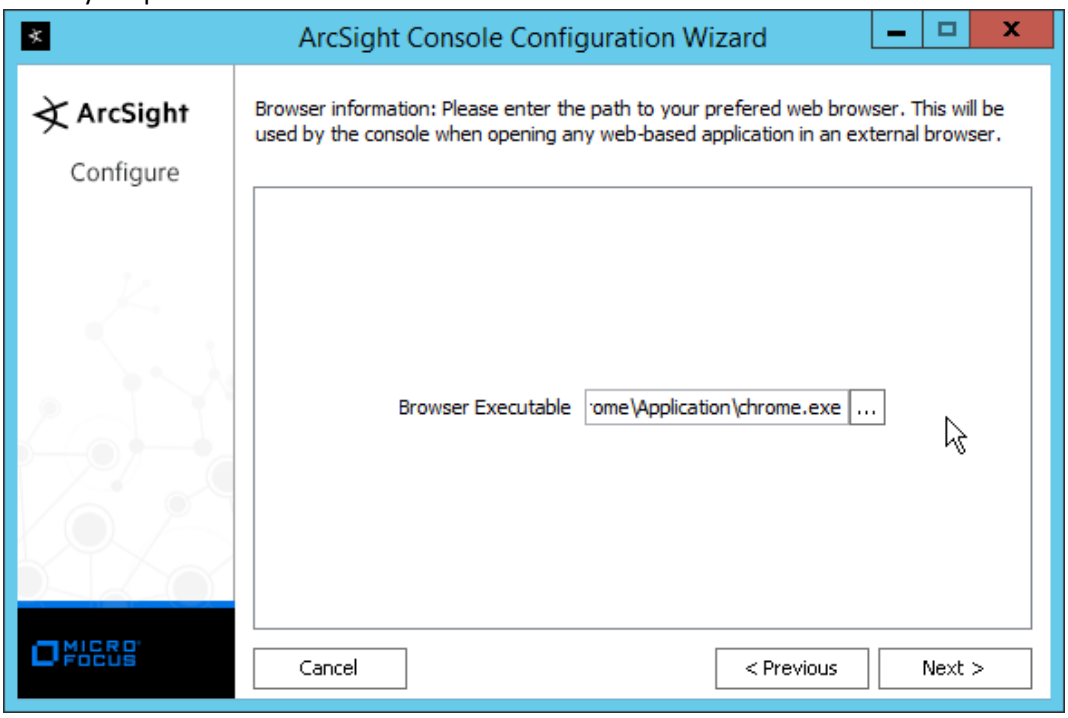
18. Click **Next.**
19. Select **Use direct connection.**



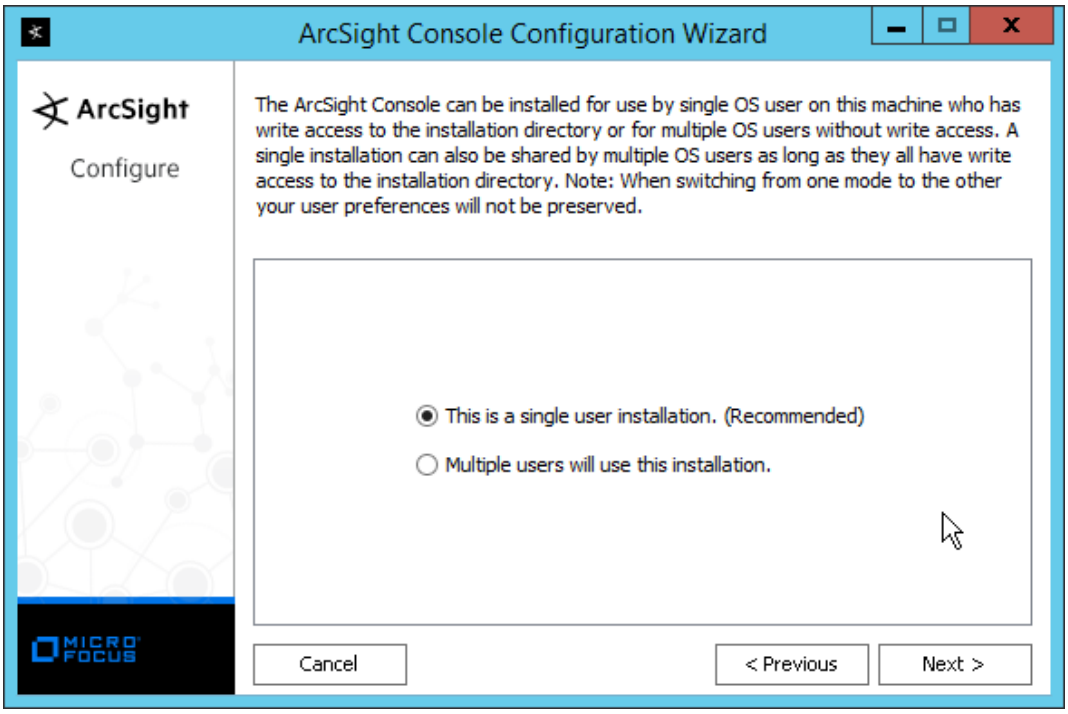
20. Click **Next.**



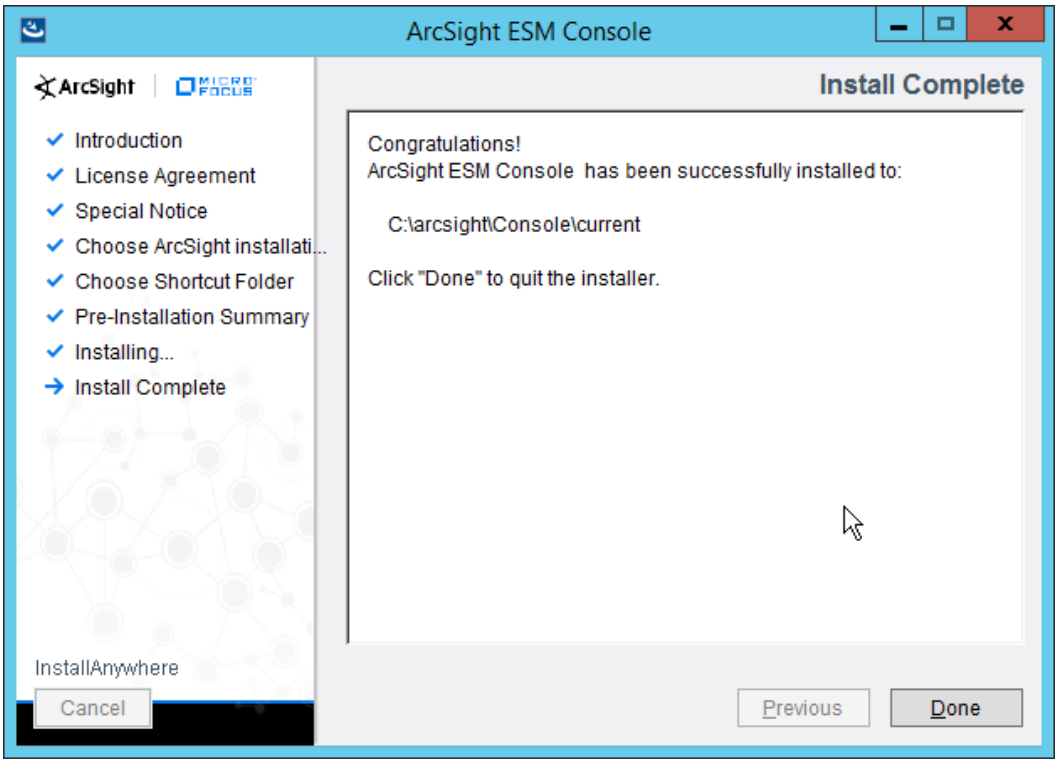
21. Click **Next.**
22. Select your preferred browser.



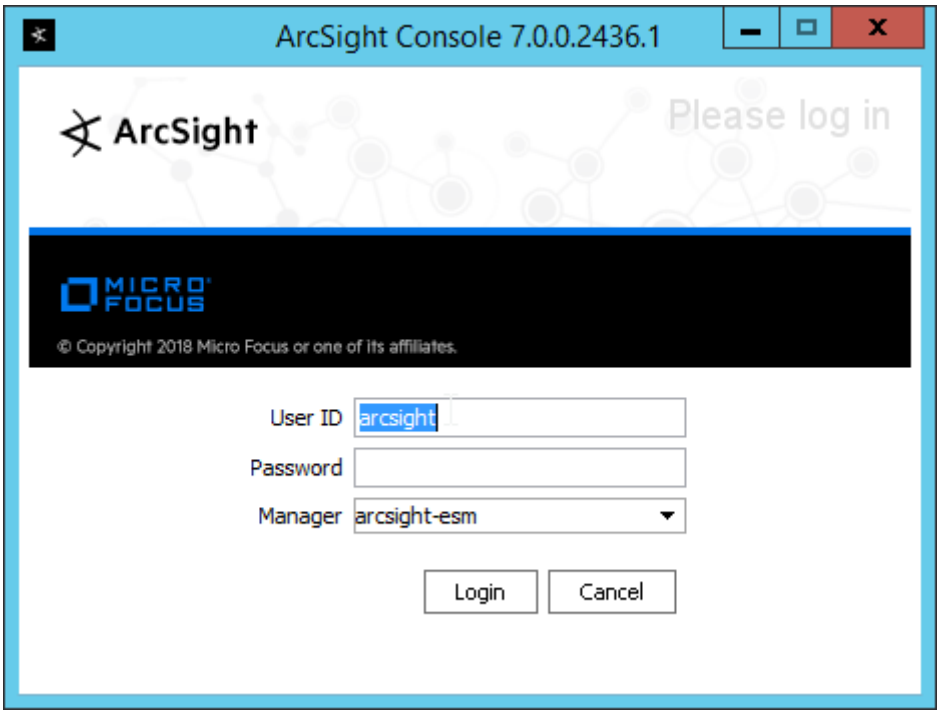
23. Click **Next.**



24. Click **Next.**
25. Click **Finish.**



26. Click **Done.**
27. Run **ArcSight Console** from the start menu.
28. Enter the **username** and **password.**

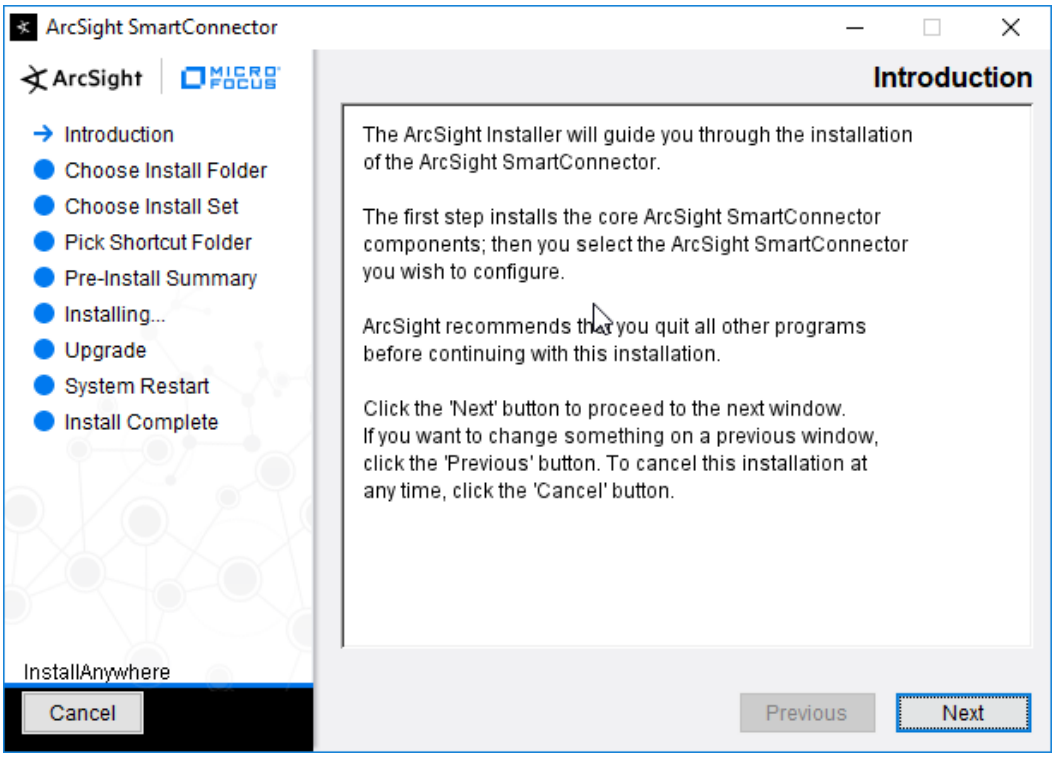


29. Click **Login.** (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)

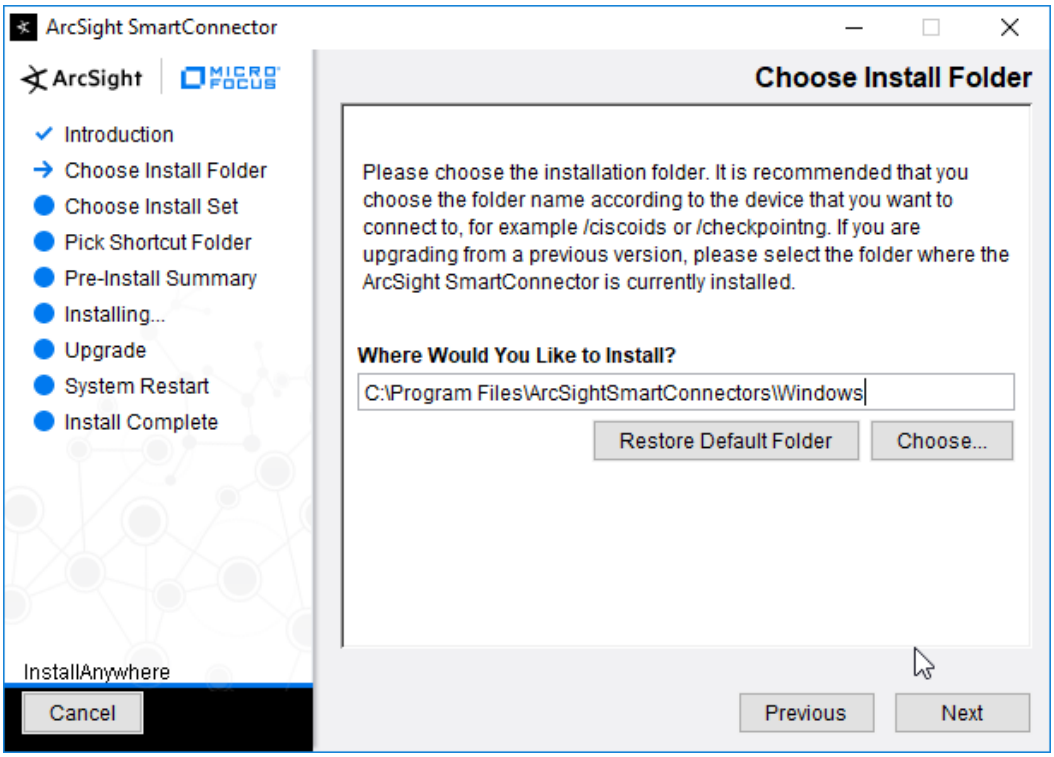
30. Click **OK.**

2.8.2 Install Individual ArcSight Windows Connectors

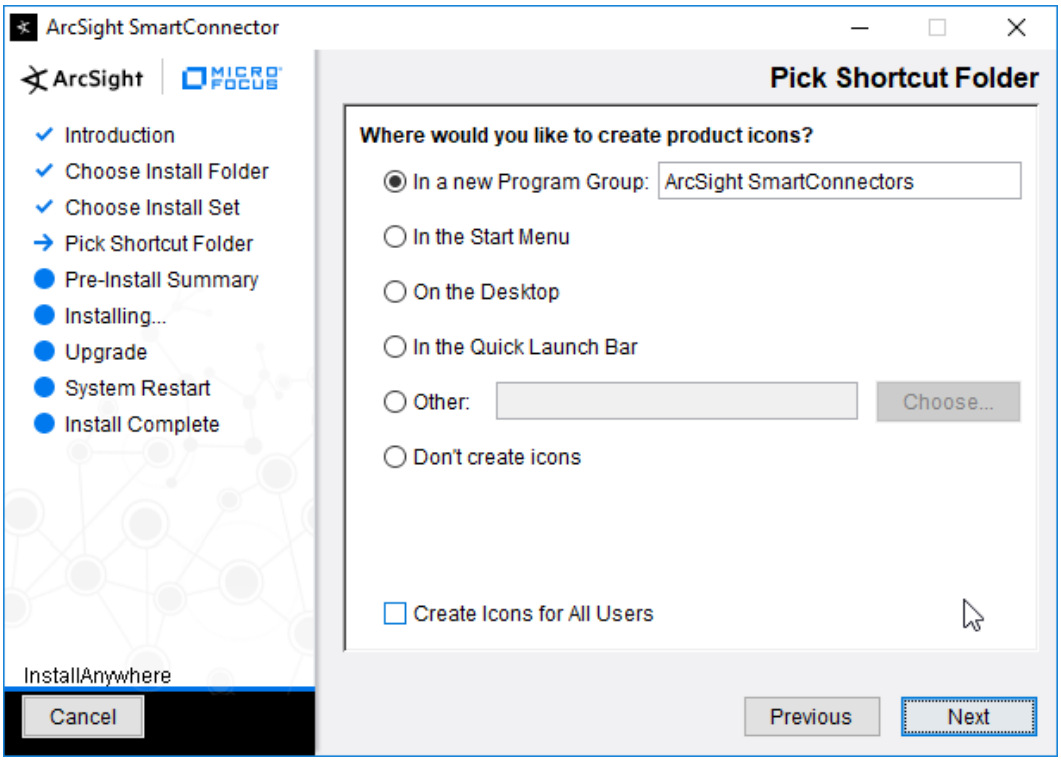
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe.**



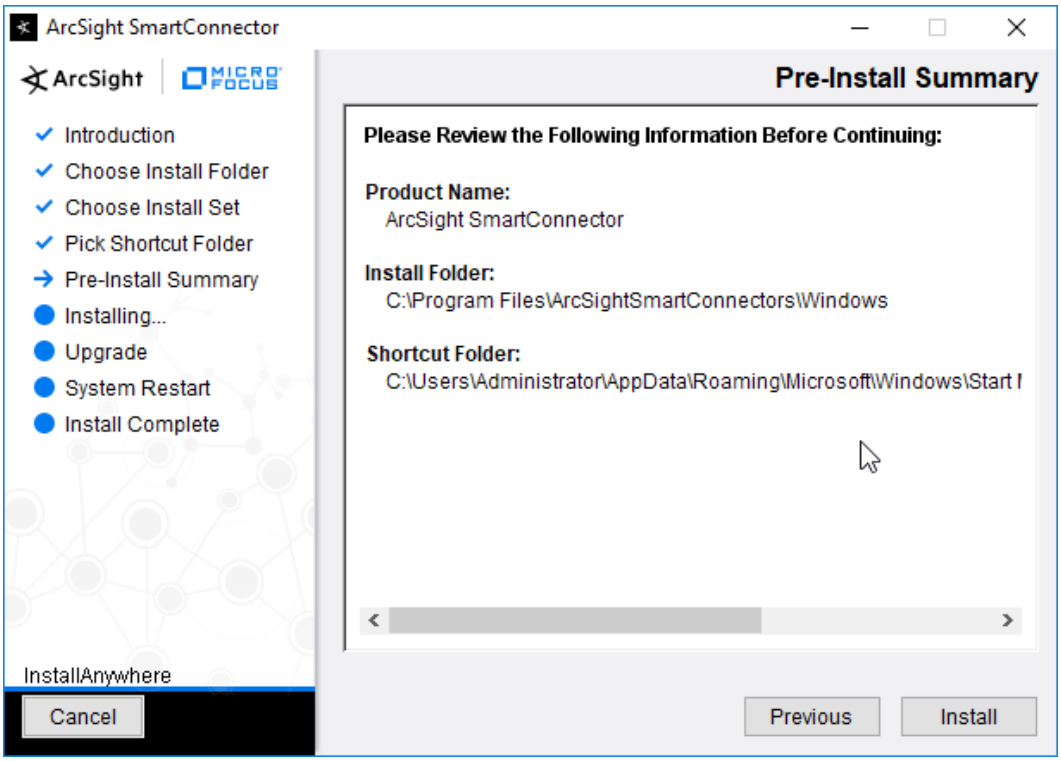
2. Click **Next.**
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.


ArcSight SmartConnector
ArcSight
MICRO FOCUS
Introduction
Choose Install Folder
Choose Install Set
Pick Shortcut Folder
Pre-Install Summary
Installing...
Upgrade
System Restart
Install Complete
InstallAnywhere
Cancel
Choose Install Folder
Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.
Where Would You Like to Install?
C:\Program Files\ArcSightSmartConnectors\Windows
Restore Default Folder
Choose...
Previous
Next

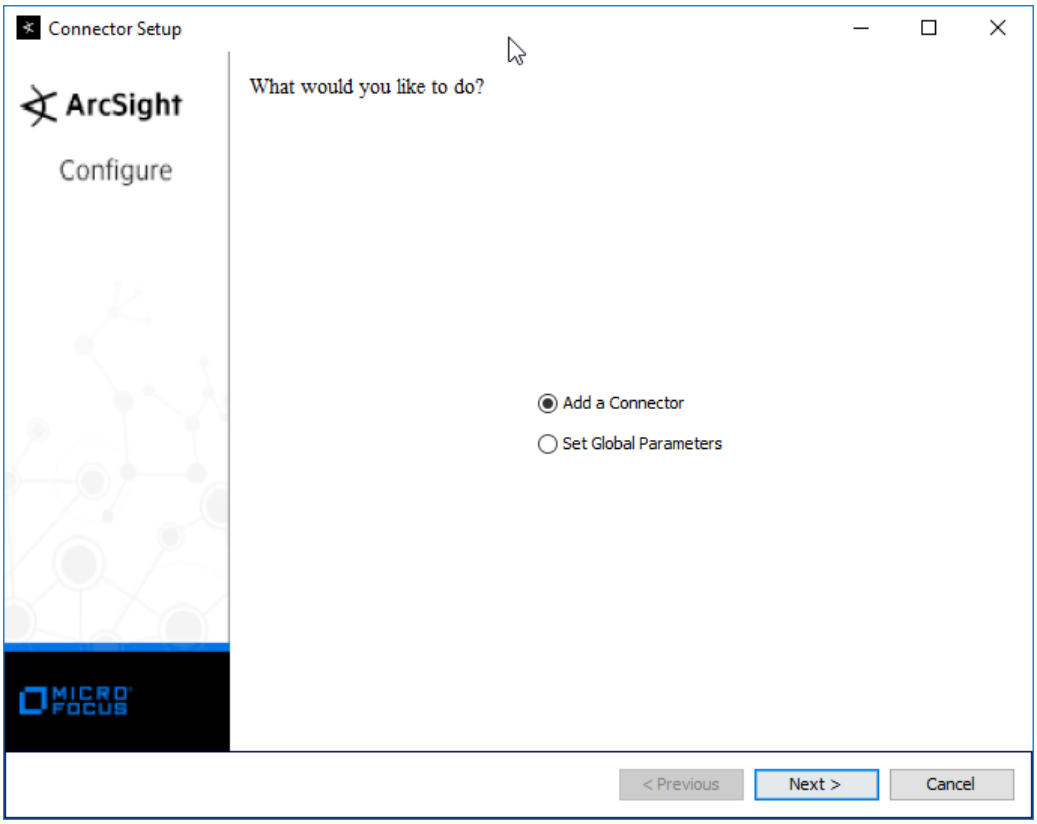
4. Click **Next.**


ArcSight SmartConnector
ArcSight
MICRO FOCUS
Introduction
Choose Install Folder
Choose Install Set
Pick Shortcut Folder
Pre-Install Summary
Installing...
Upgrade
System Restart
Install Complete
InstallAnywhere
Cancel
Pick Shortcut Folder
Where would you like to create product icons?
In a new Program Group: ArcSight SmartConnectors
In the Start Menu
On the Desktop
In the Quick Launch Bar
Other:
Choose...
Don't create icons
Create Icons for All Users
Previous
Next

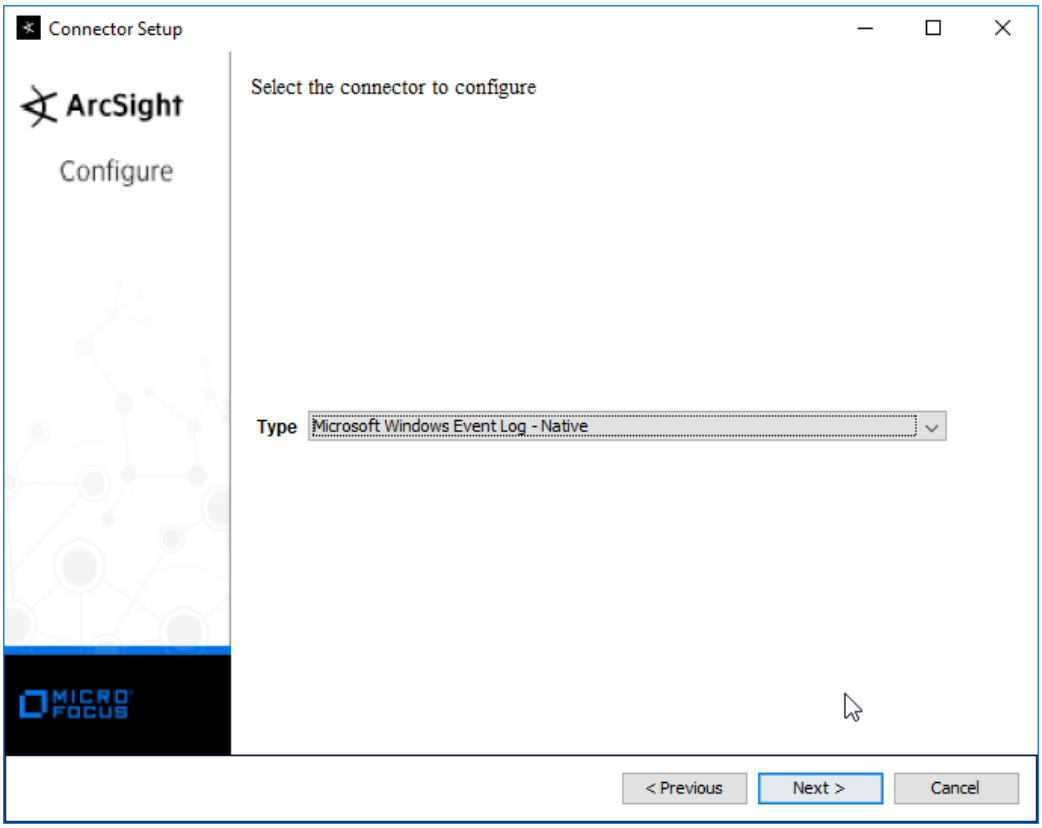
5. Click **Next.**



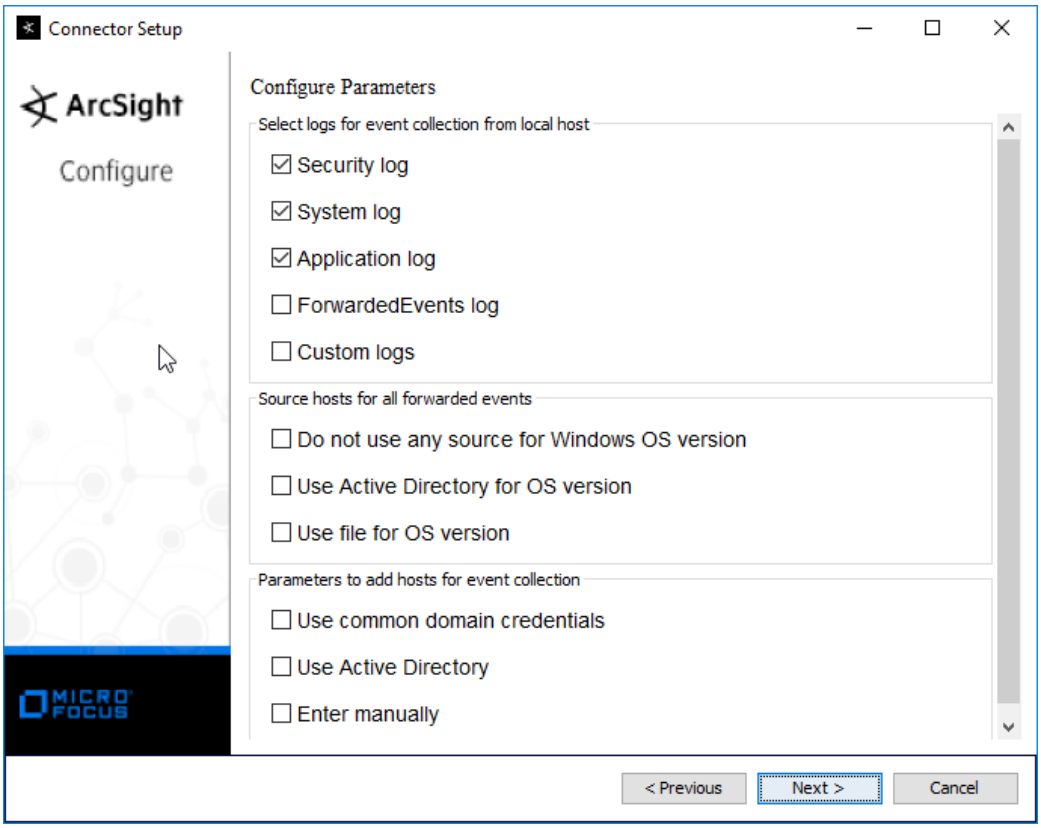
6. Click **Install.**
7. Select **Add a Connector.**



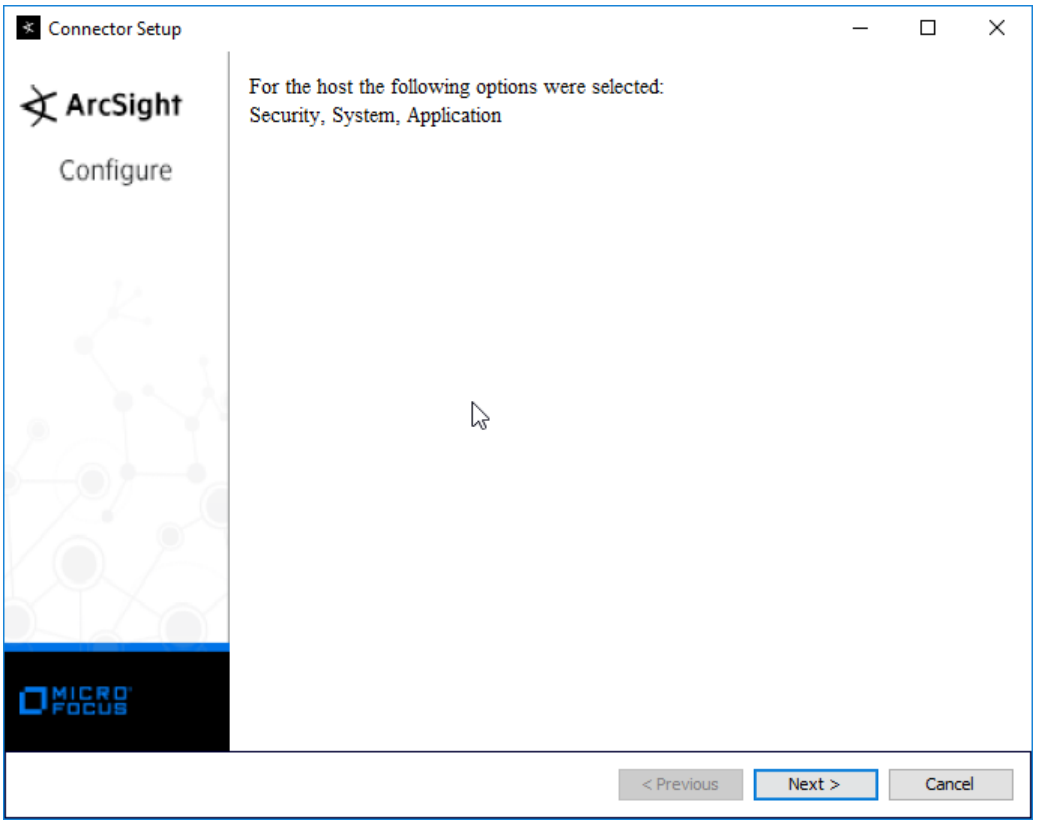
8. Click **Next.**
9. Select **Microsoft Windows Event Log – Native.**



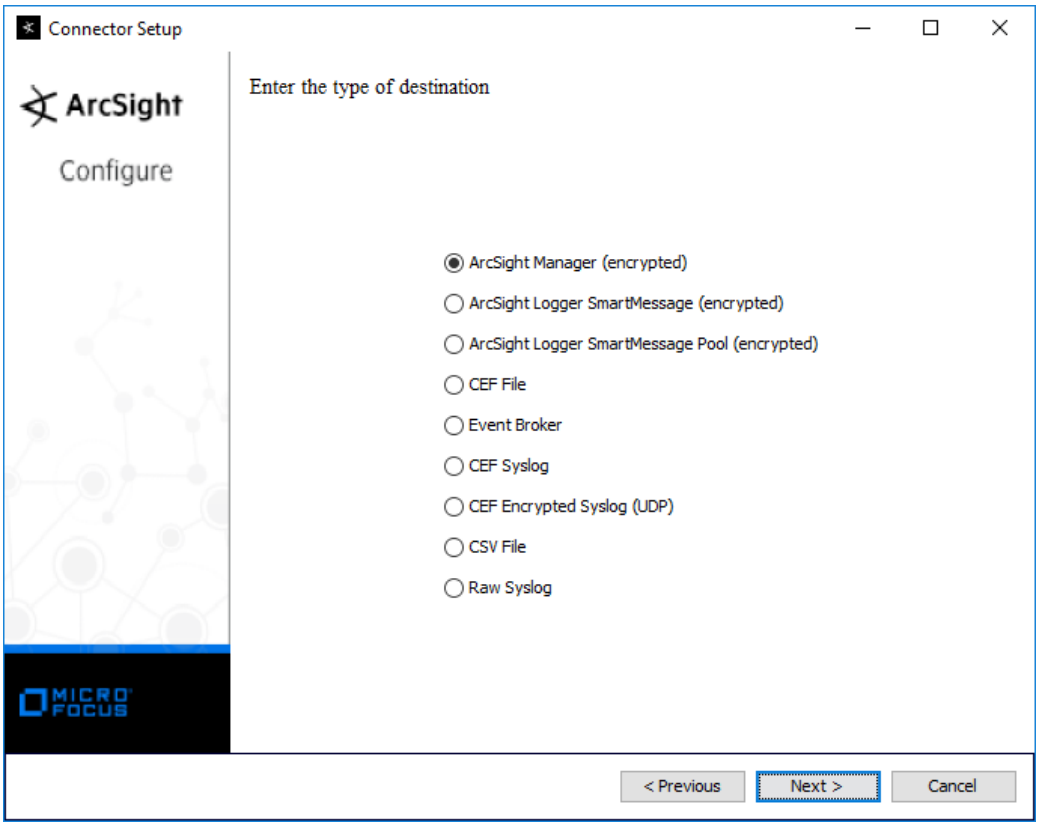
10. Click **Next.**



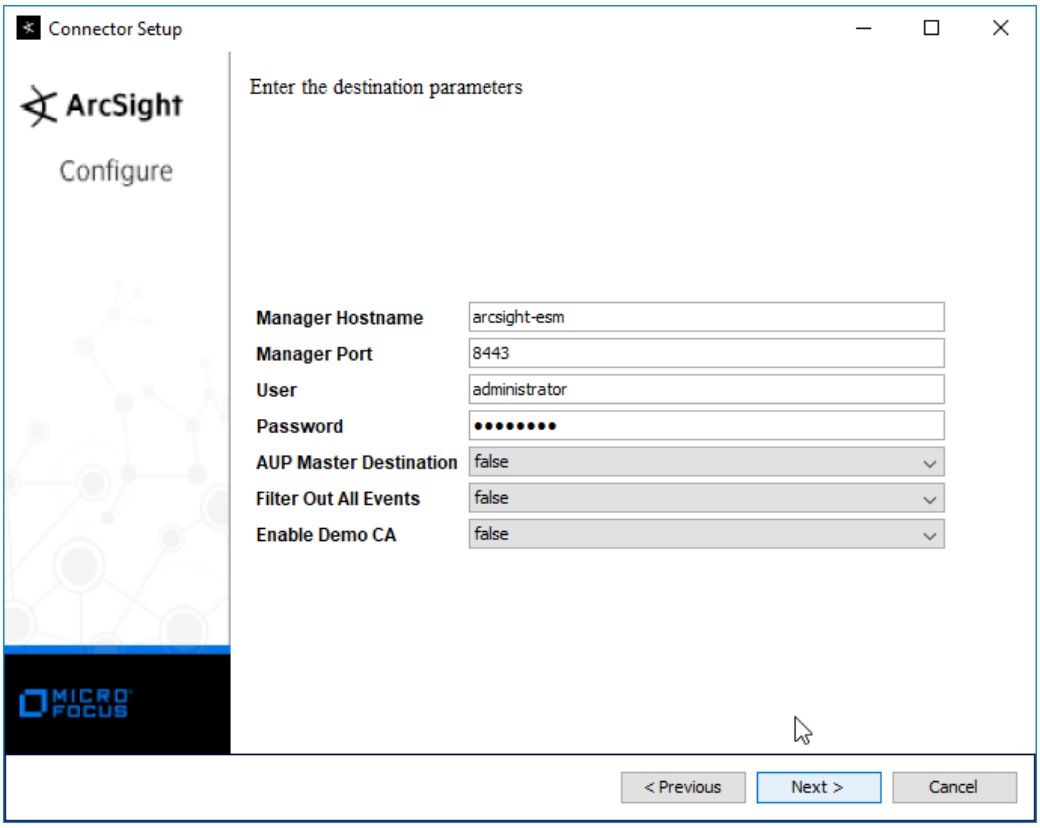
11. Click **Next.**



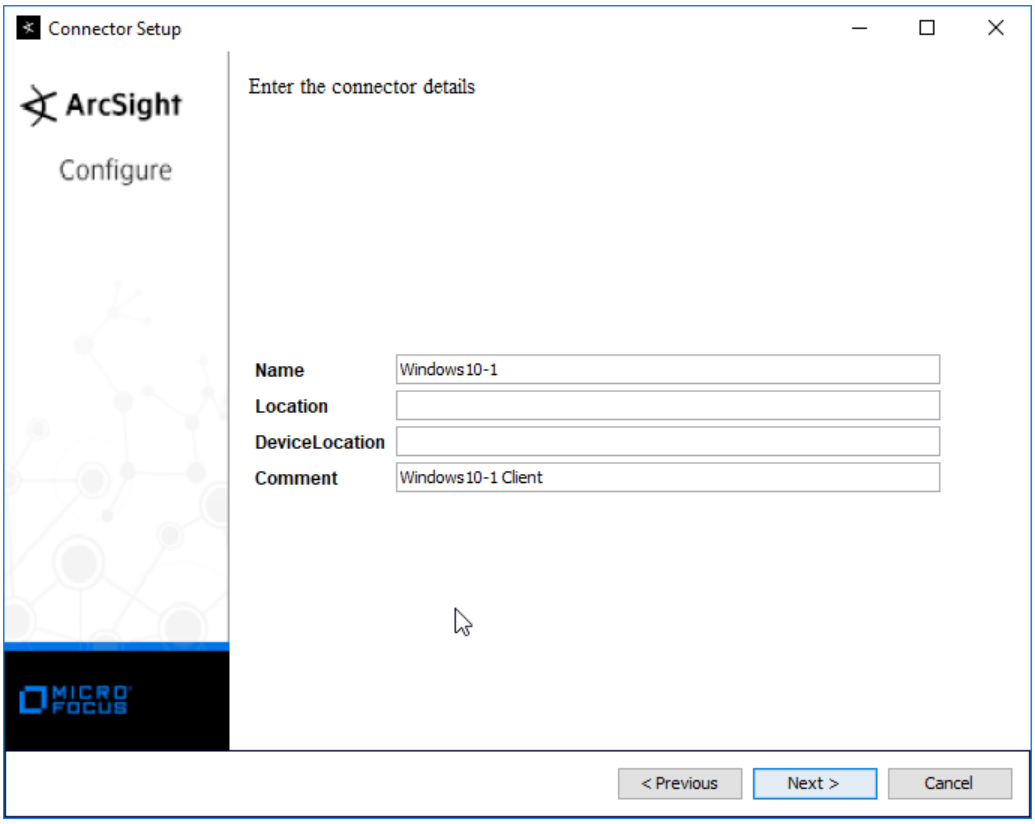
12. Click **Next.**
13. Select **ArcSight Manager (encrypted).**



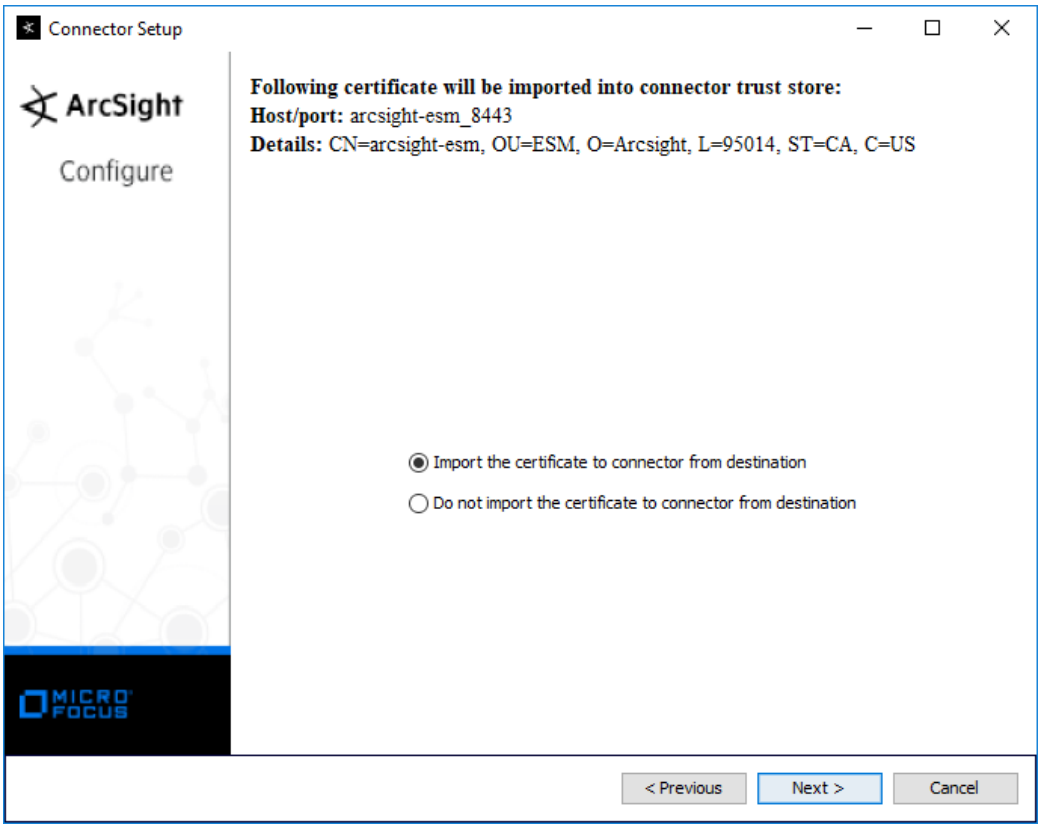
14. Click **Next.**
15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



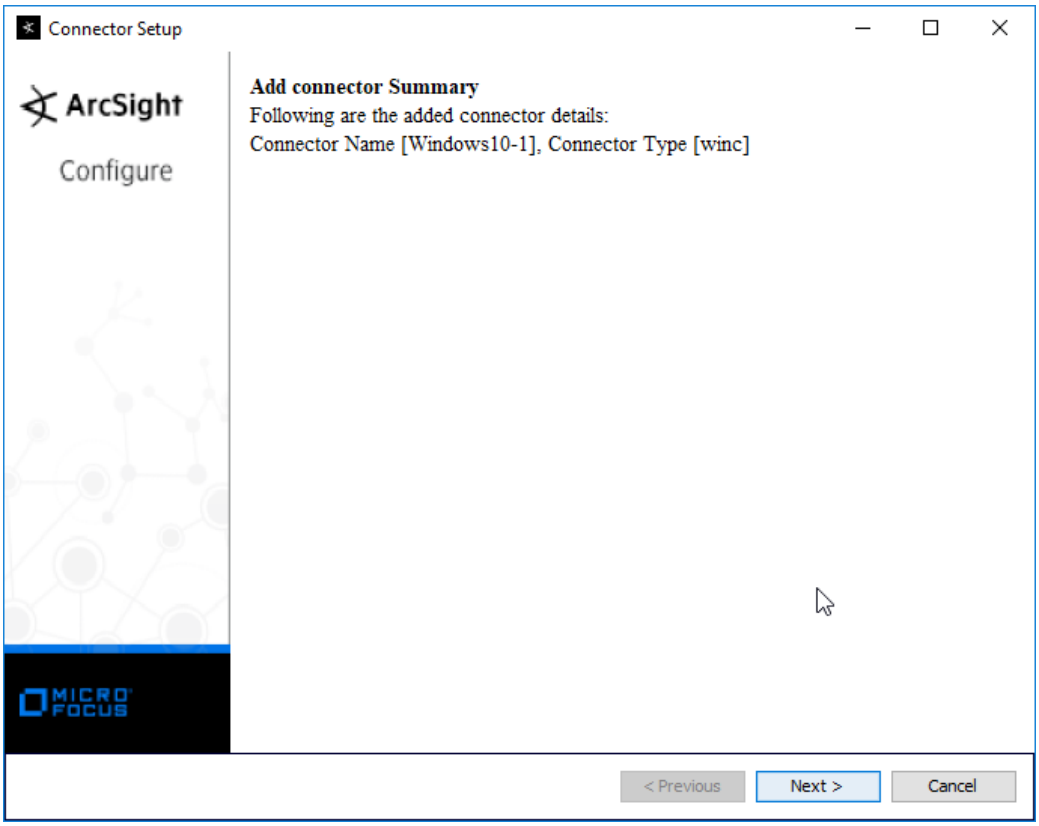
16. Click **Next.**
17. Enter identifying details about the system (only **Name** is required).



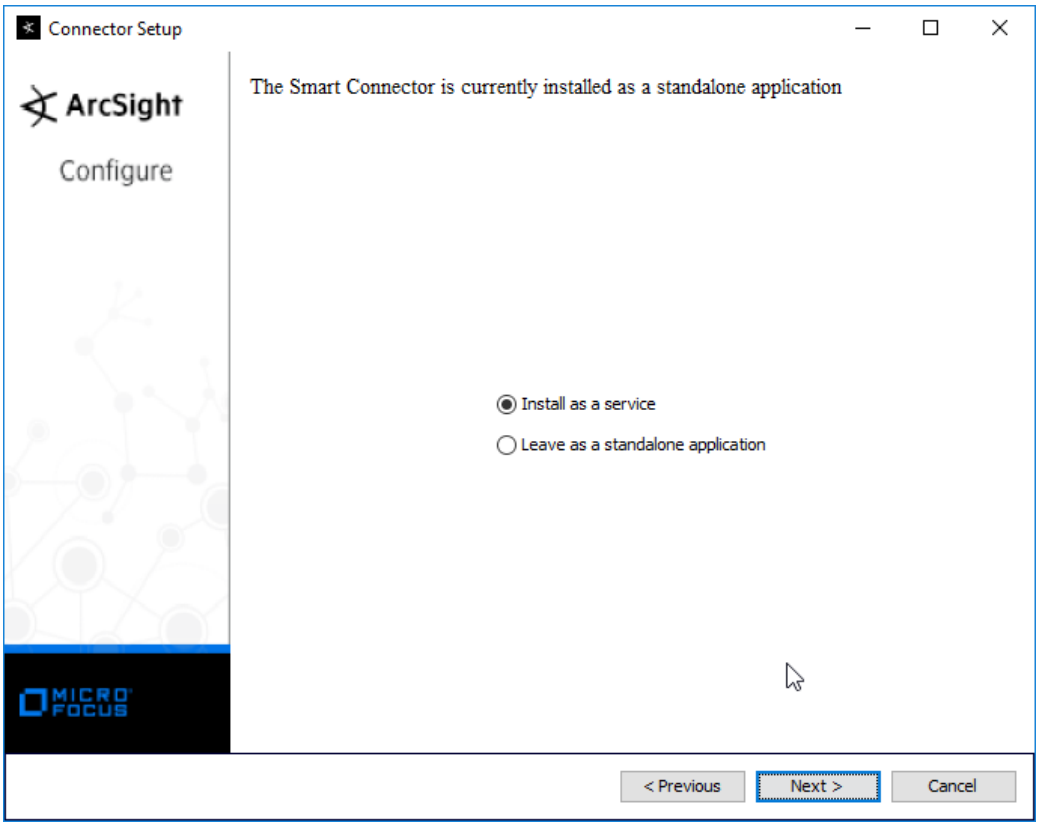
18. Click **Next.**
19. Select **Import the certificate to connector from destination.**



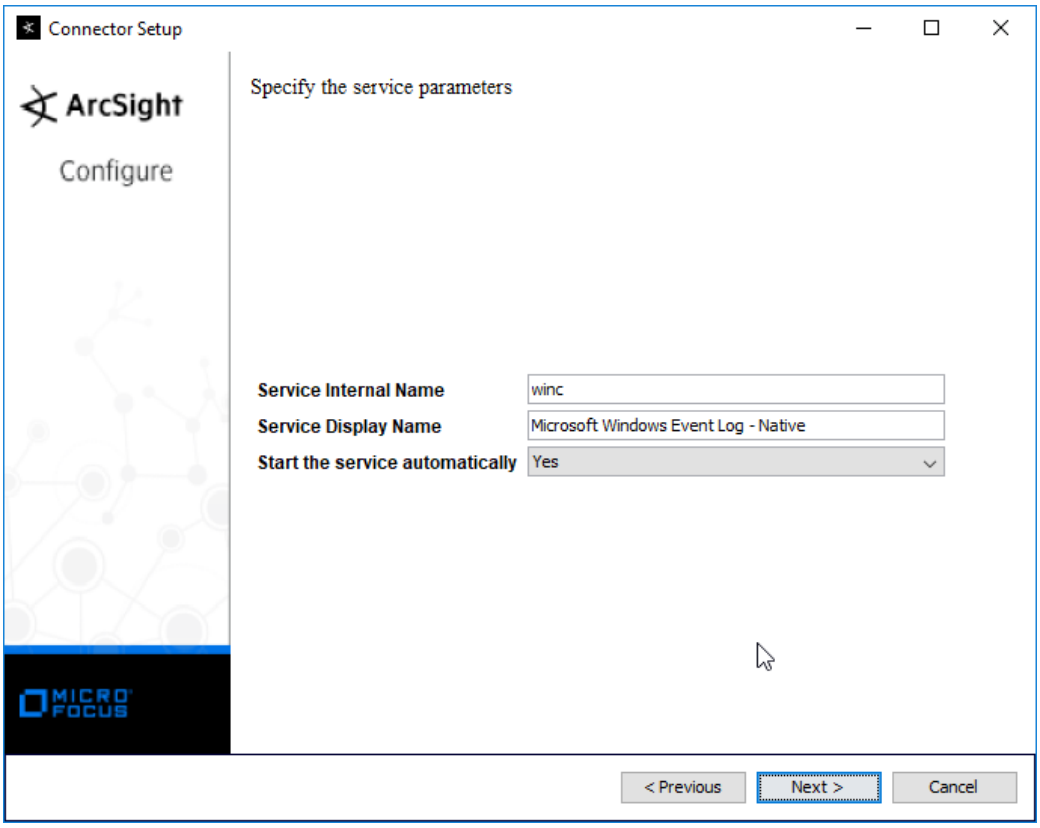
20. Click **Next.**



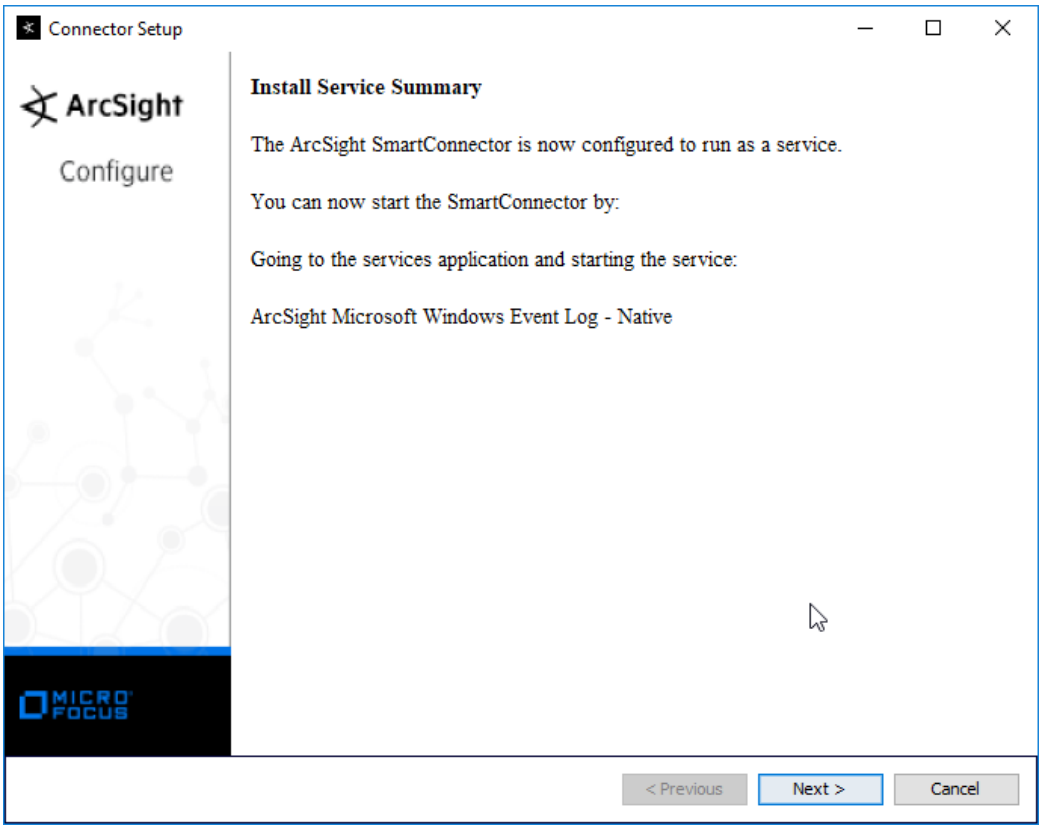
21. Click **Next.**
22. Select **Install as a service.**



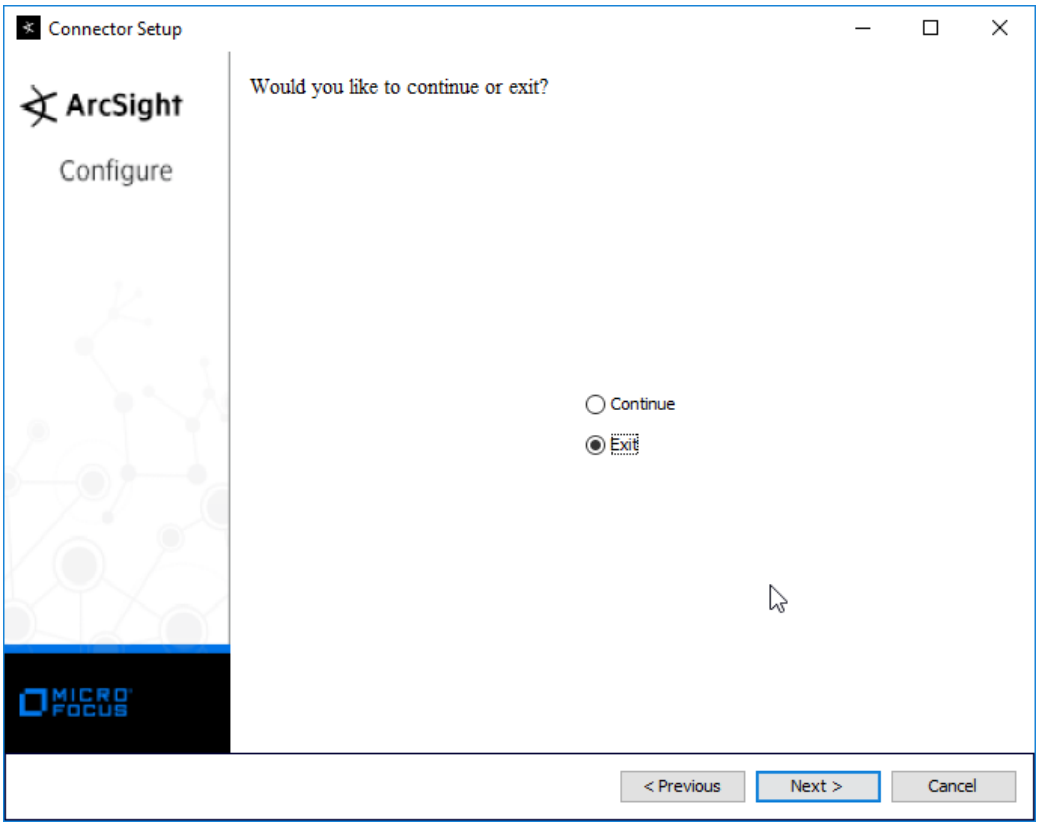
23. Click **Next.**



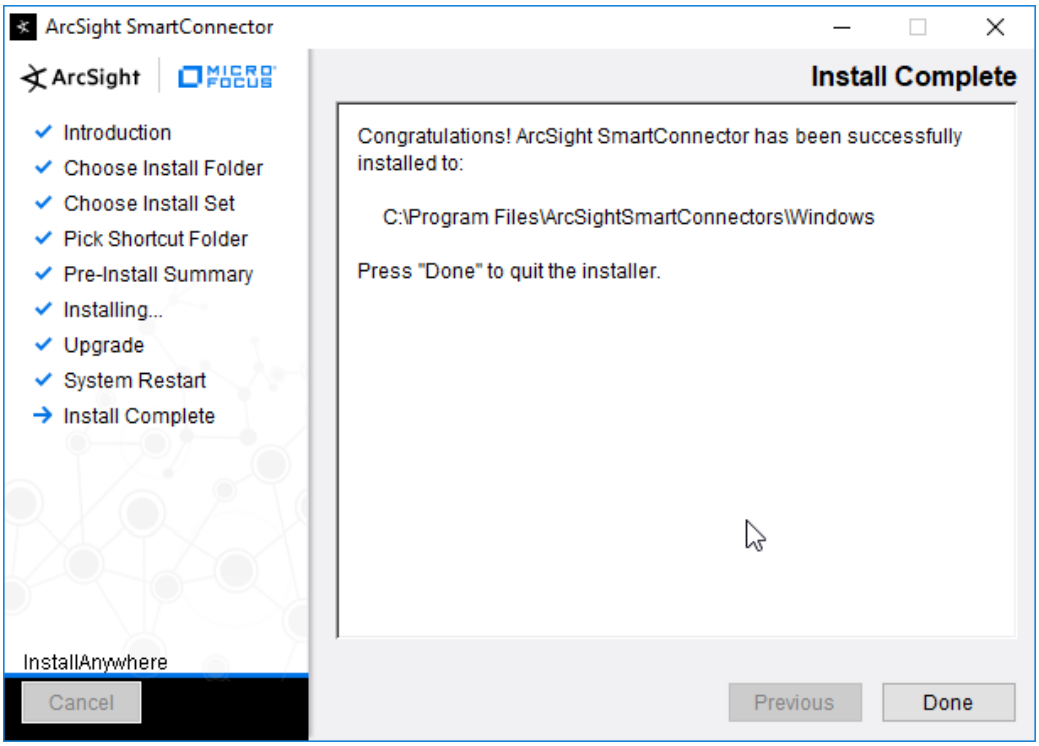
24. Click **Next.**



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



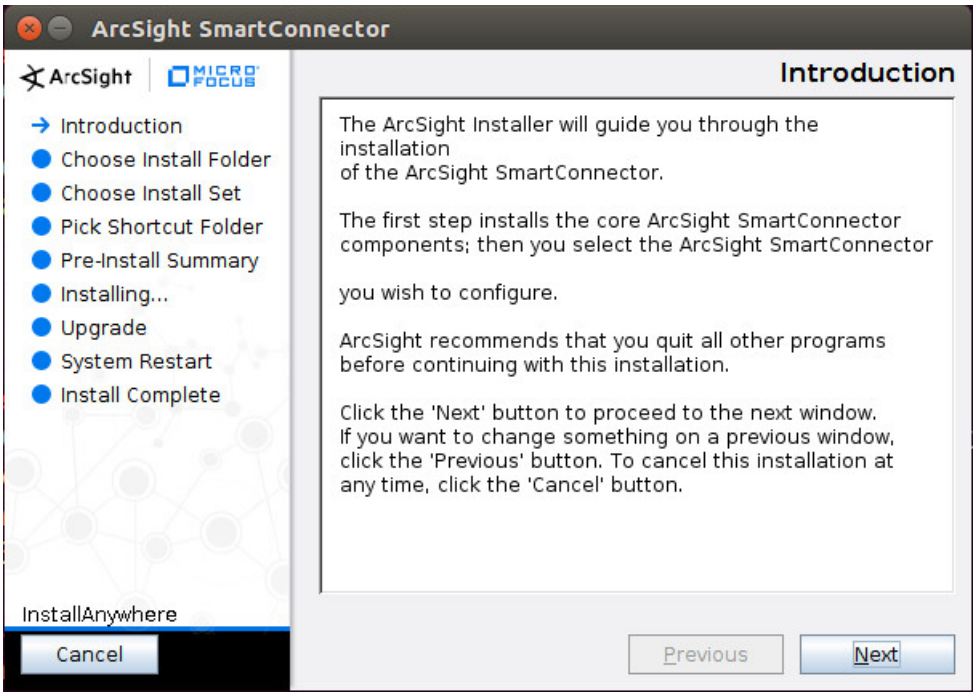
27. Click **Next.**



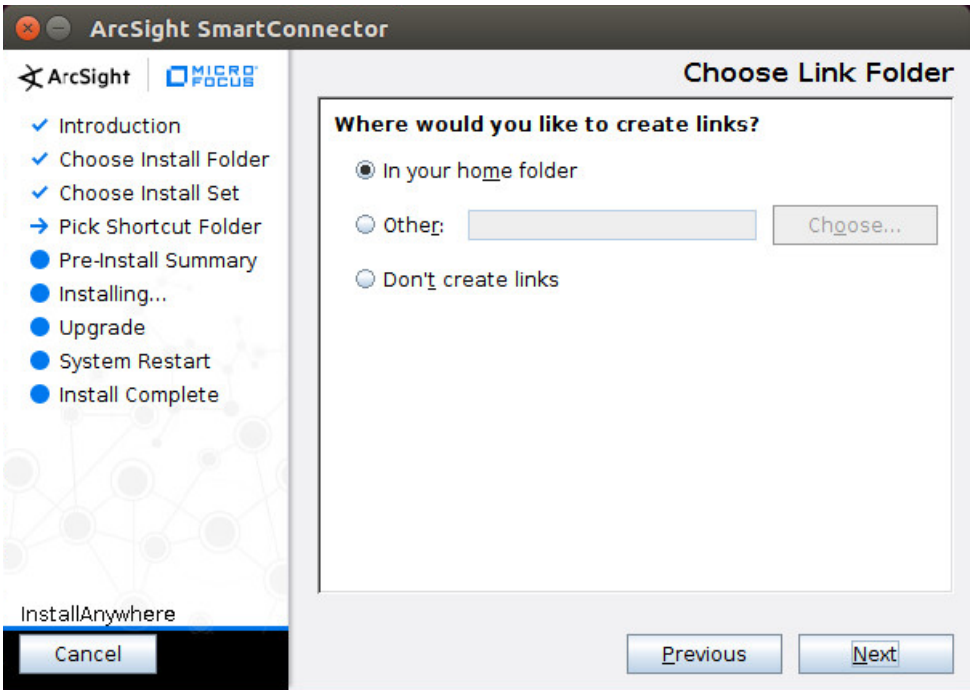
28. Click **Done.**

2.8.3 Install Individual ArcSight Ubuntu Connectors

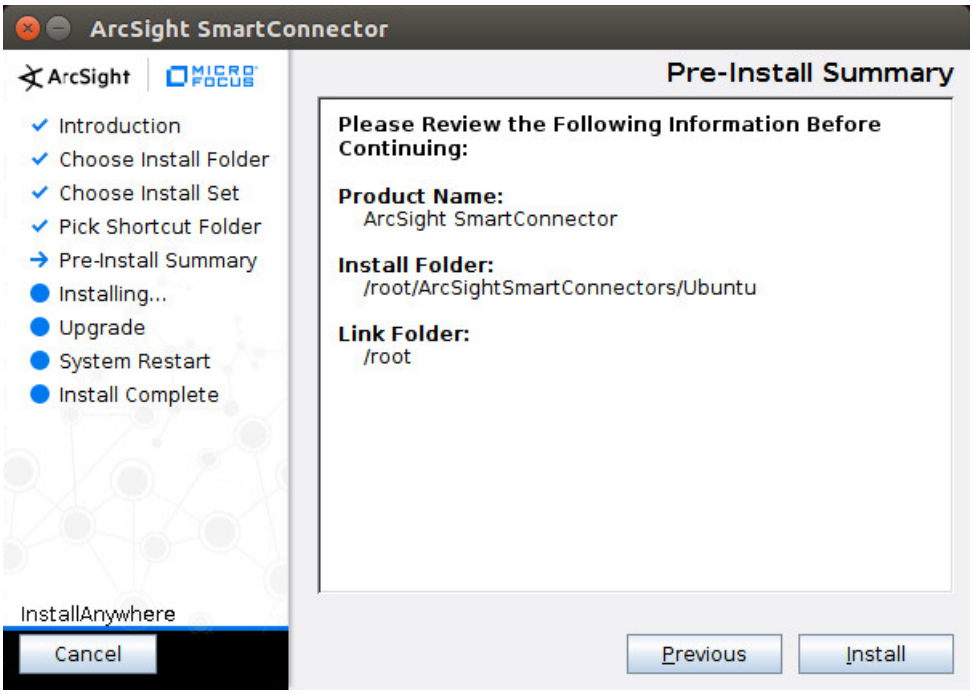
1. From the command line, run:
   ```
   > sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin
   ```
2. Enter the **password** if prompted.



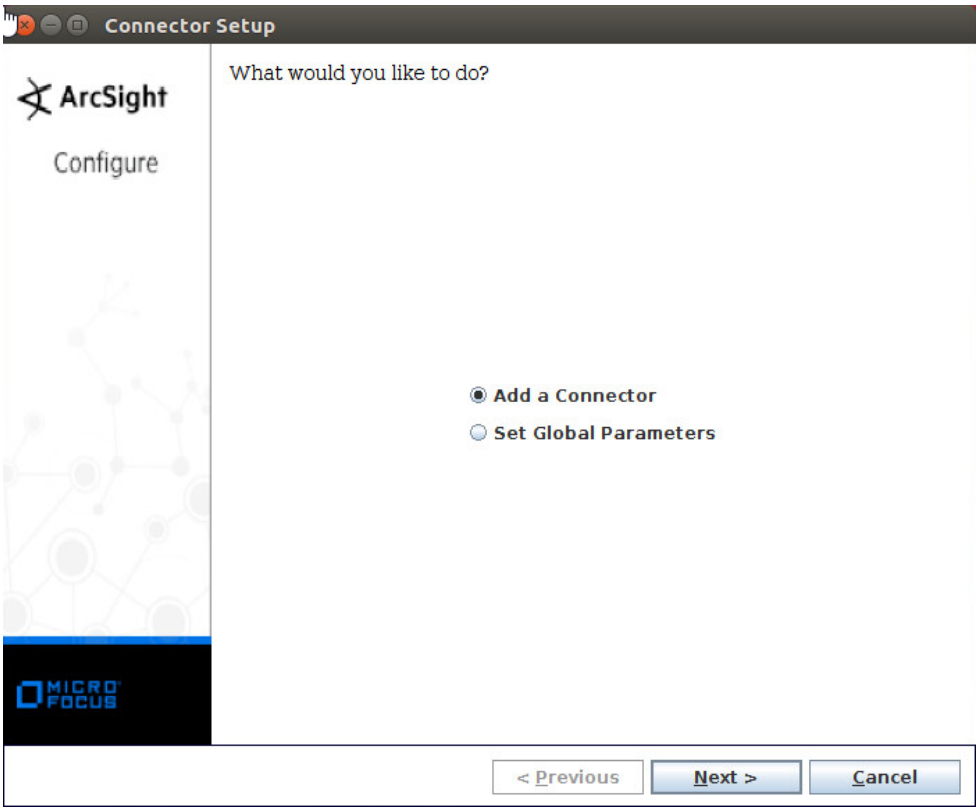
3. Click **Next.**
4. Enter */root/ArcSightSmartConnectors/Ubuntu.*
5. Click **Next.**



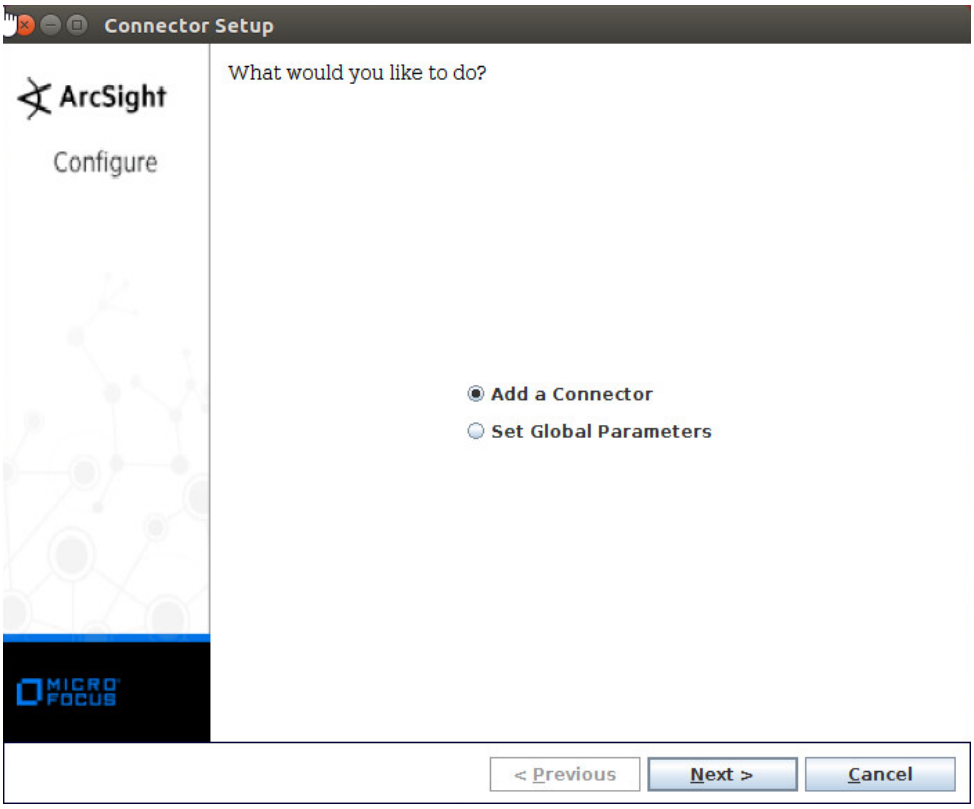
1340 6. Click **Next.**



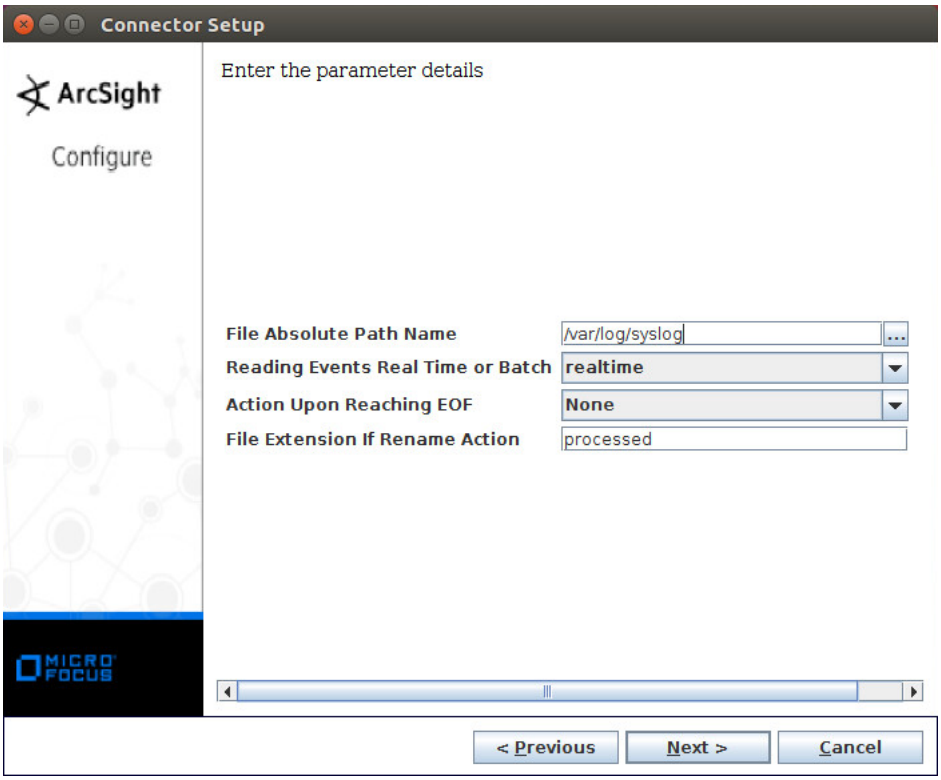
1341
1342 7. Click **Install.**
1343 8. Select **Add a Connector.**



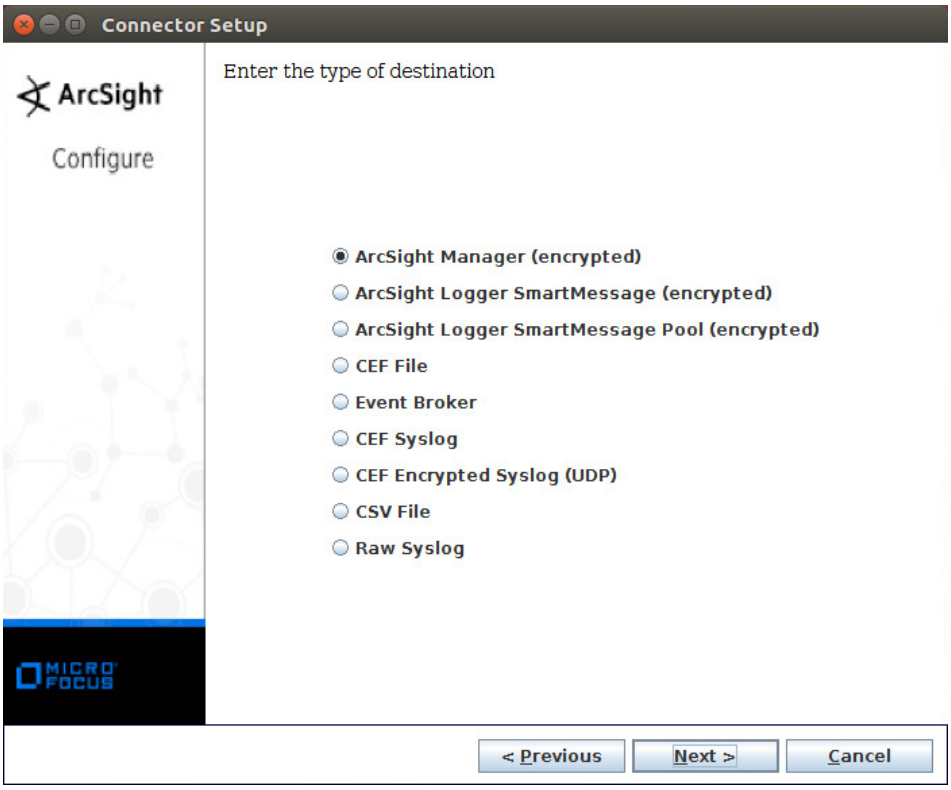
9. Click **Next.**
10. Select **Syslog File.**



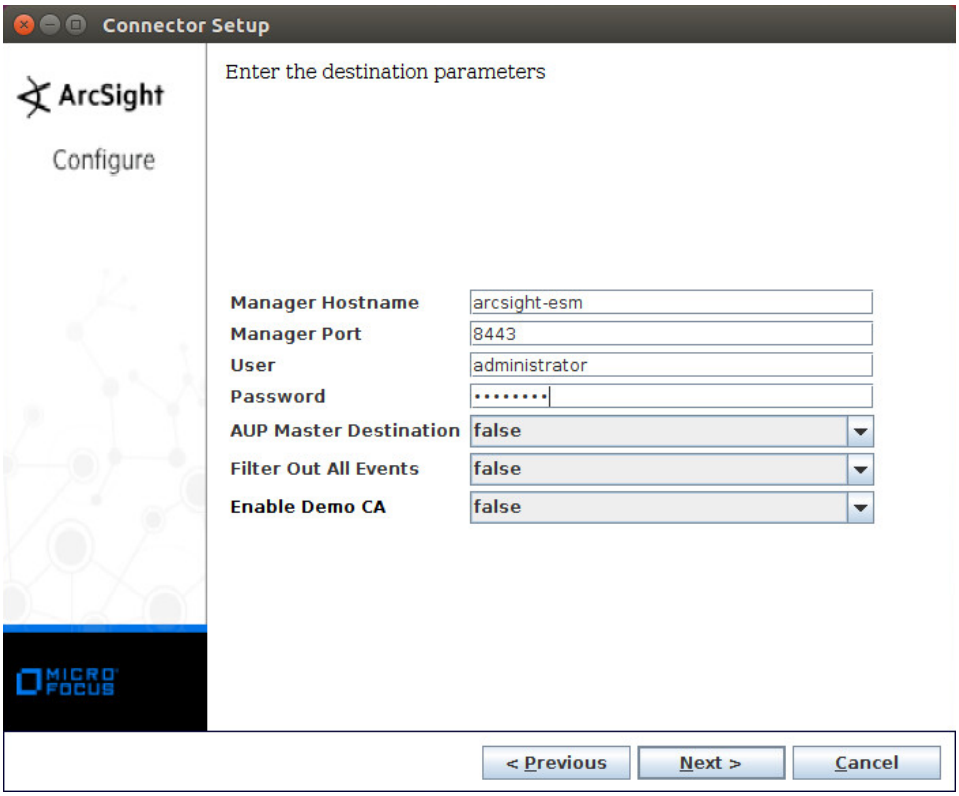
11. Click **Next.**
12. Enter */var/log/syslog* for the File Absolute Path Name.



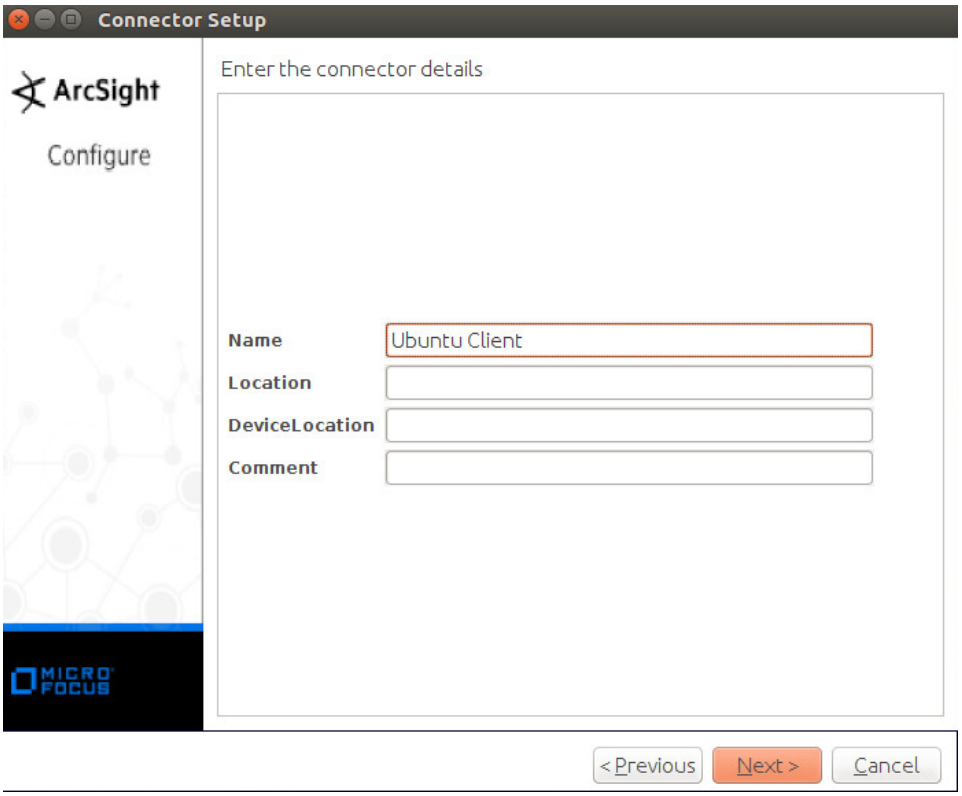
13. Click **Next.**
14. Select **ArcSight Manager** (encrypted).



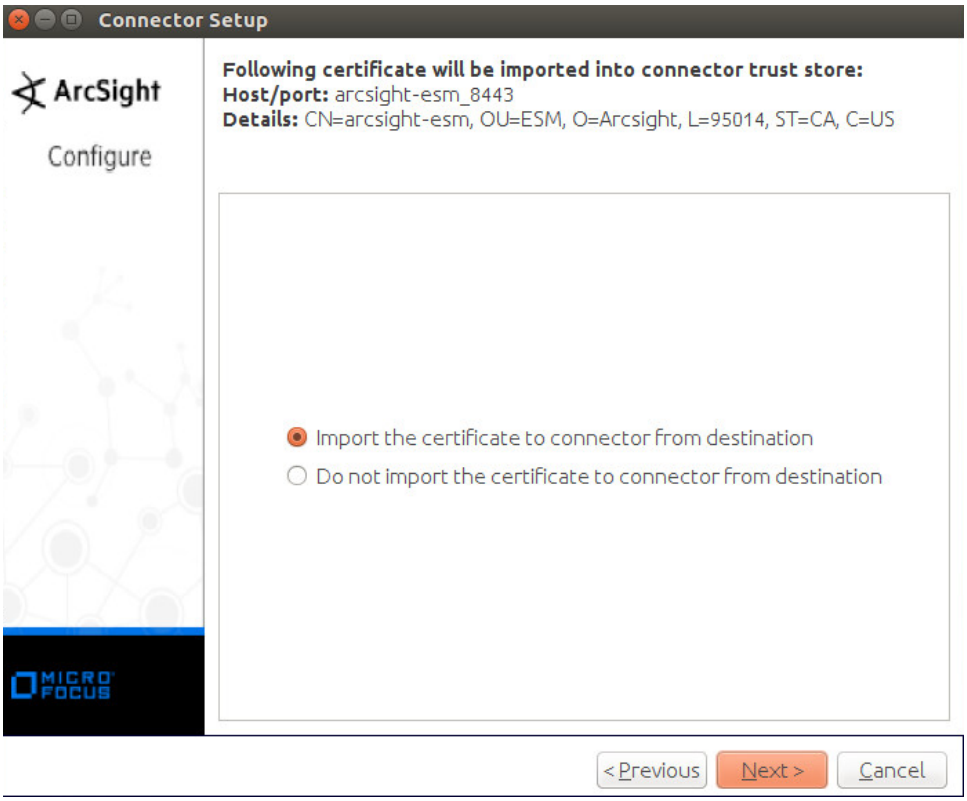
15. Click **Next.**
16. Enter the **hostname, port, username,** and **password** for ArcSight ESM.



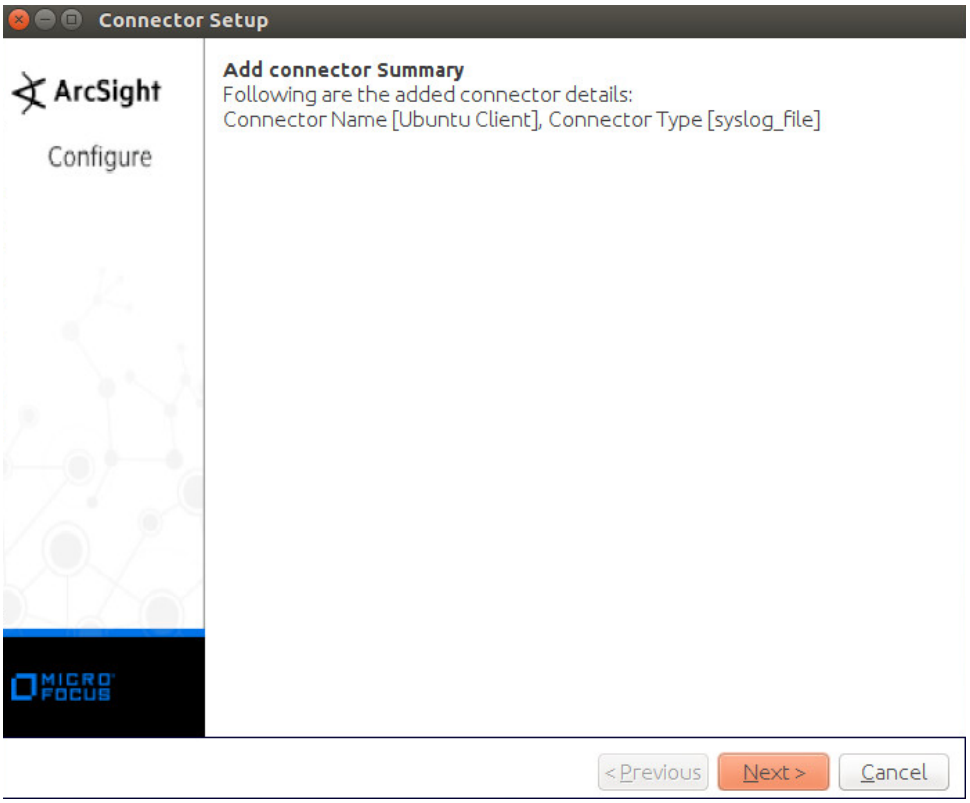
17. Click **Next.**
18. Enter identifying details about the system (only **Name** is required).



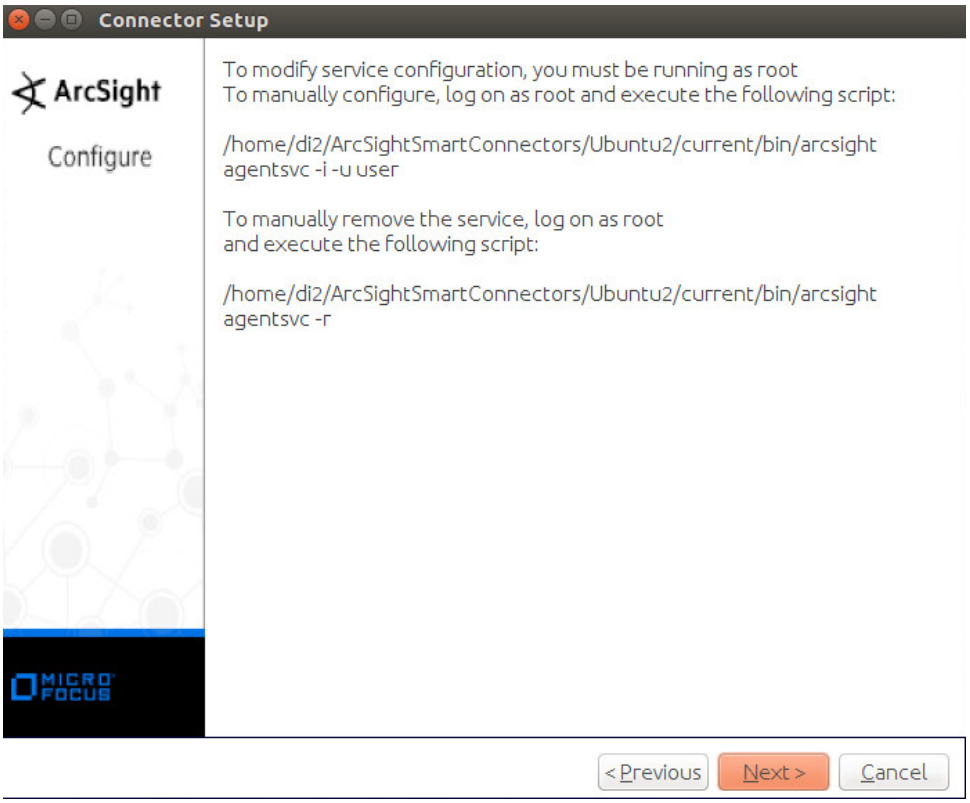
19. Click **Next.**
20. Select **Import the certificate to connector from destination.**



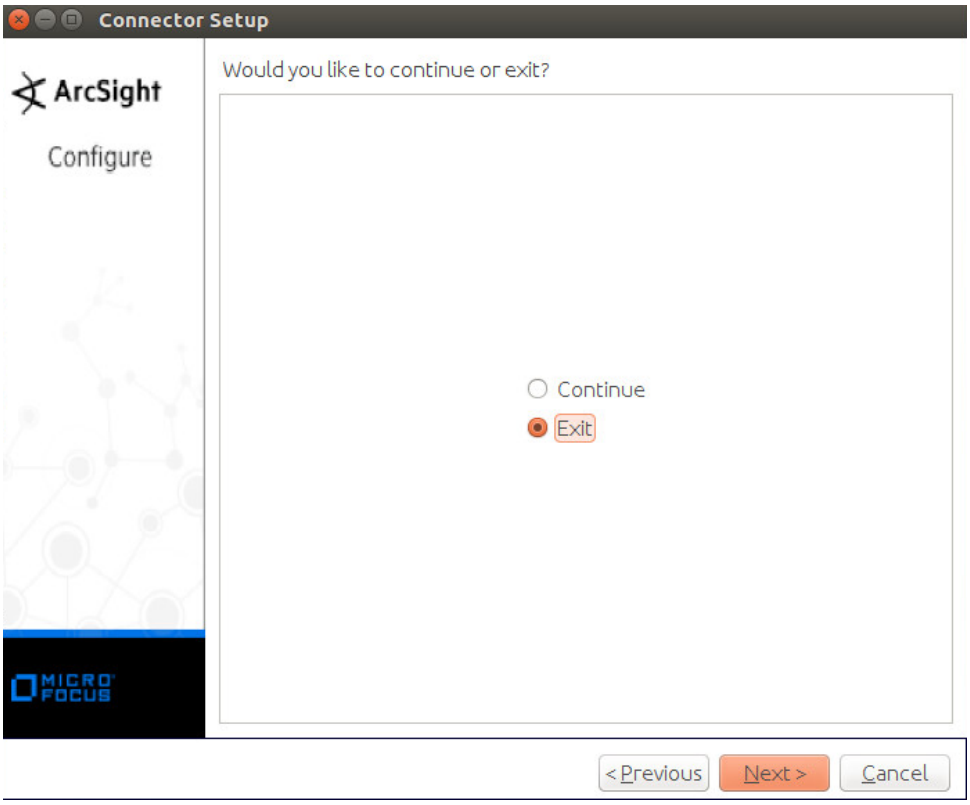
21. Click **Next.**



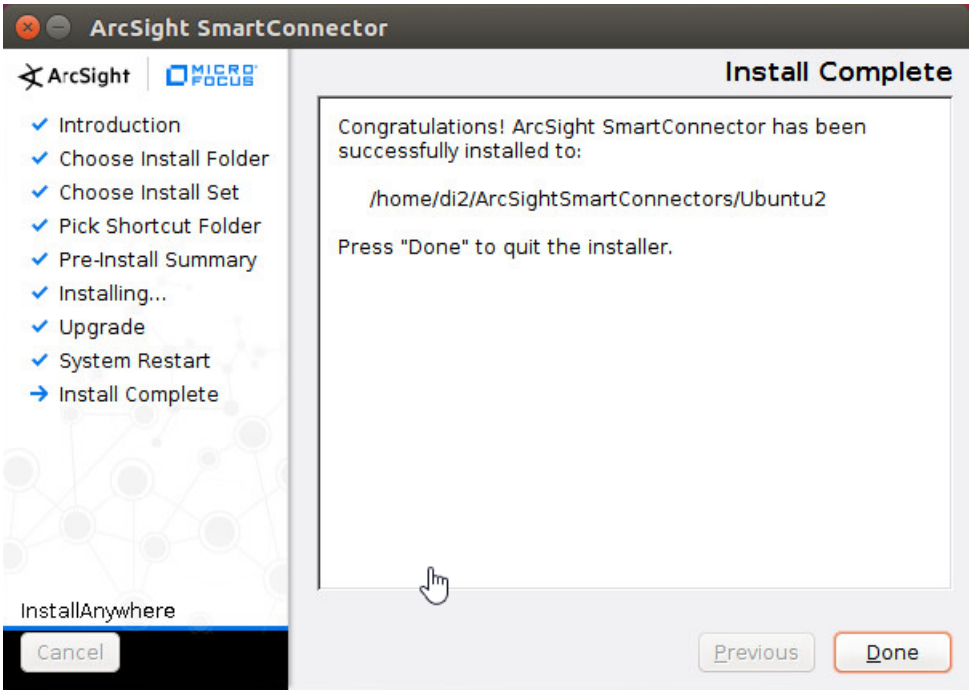
22. Click **Next.**



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



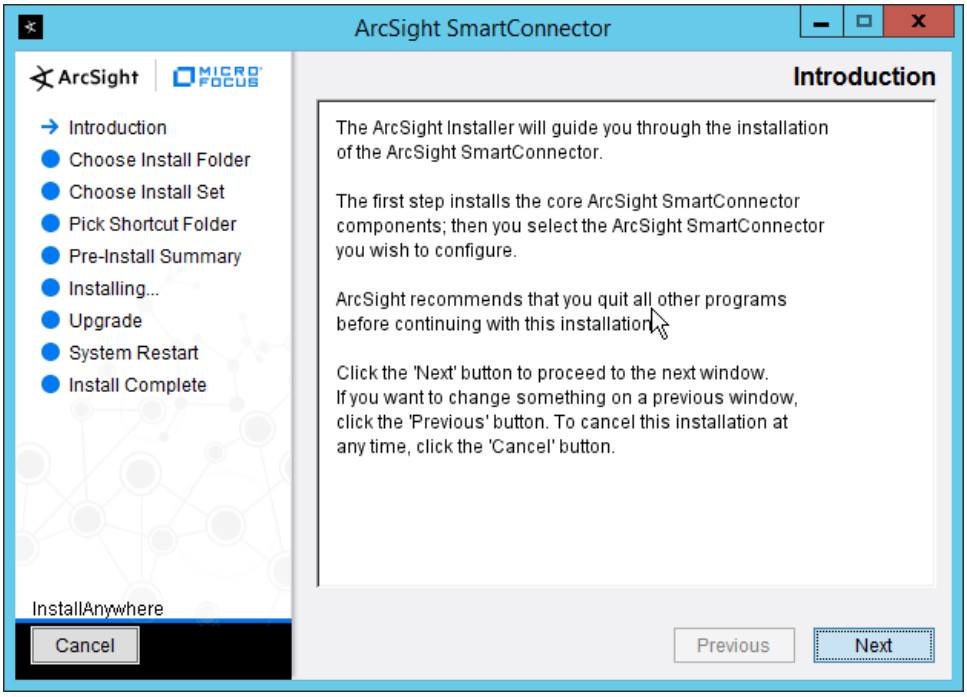
25. Click **Next.**



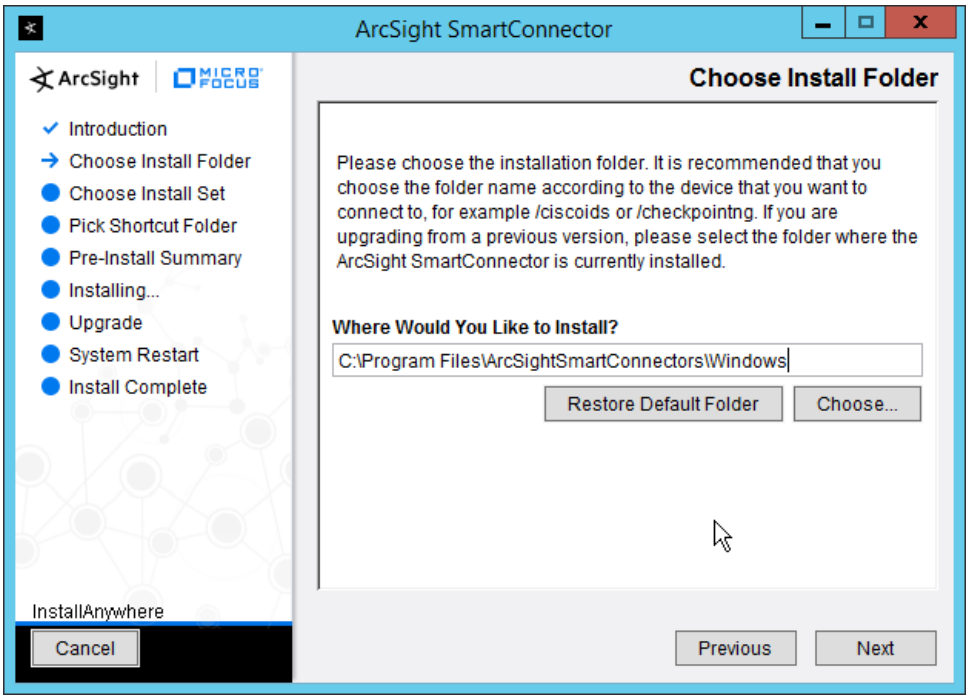
26. Click **Done.**

2.8.4 Install a Connector Server for ESM on Windows 2012 R2

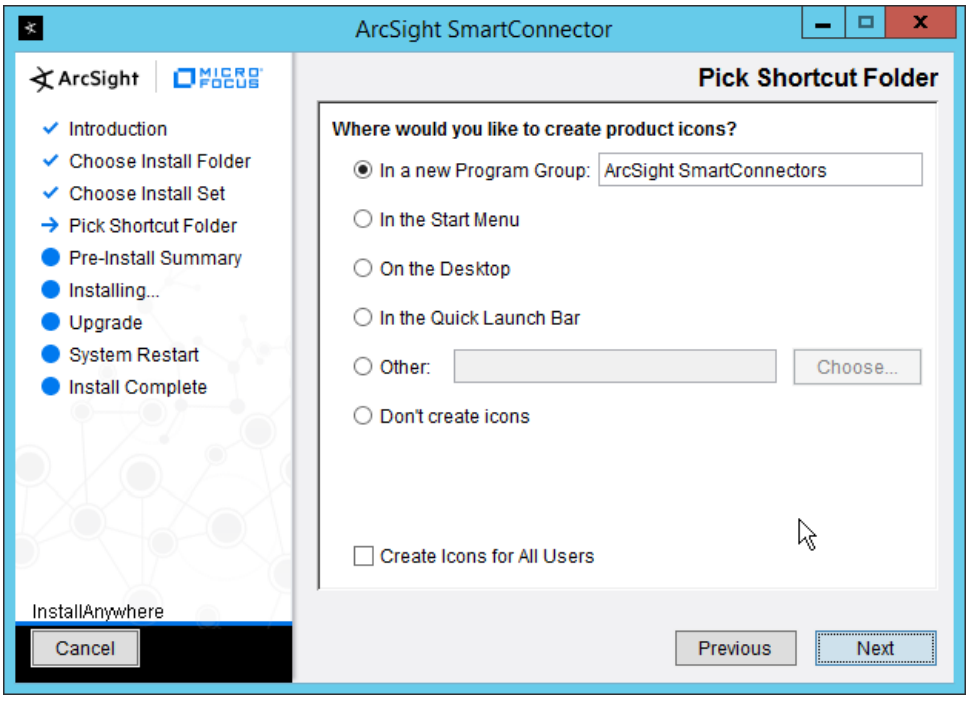
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe.**



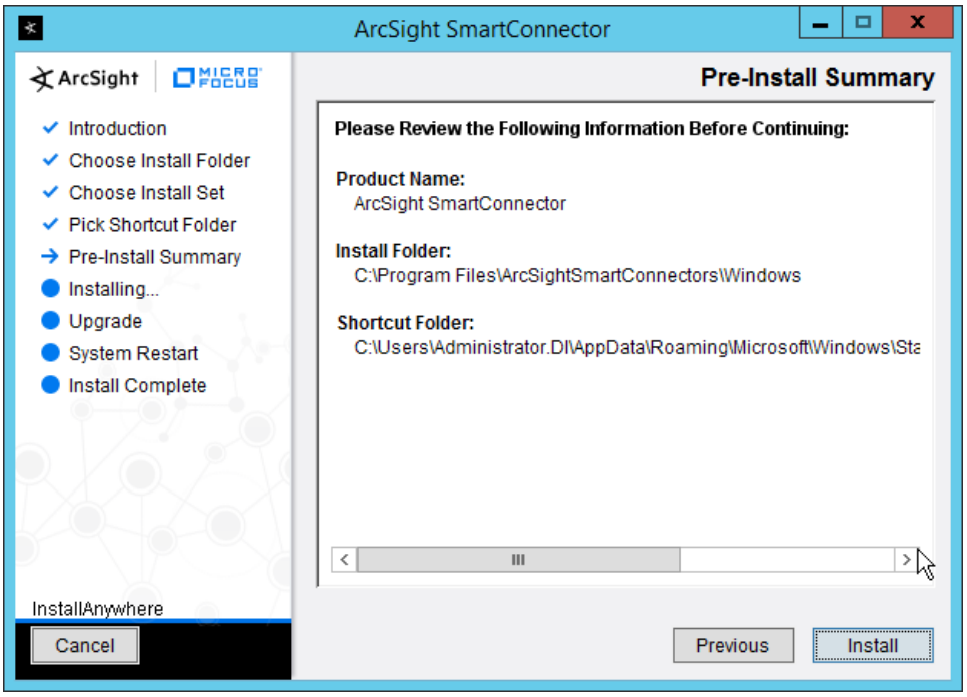
2. Click **Next.**
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows.*



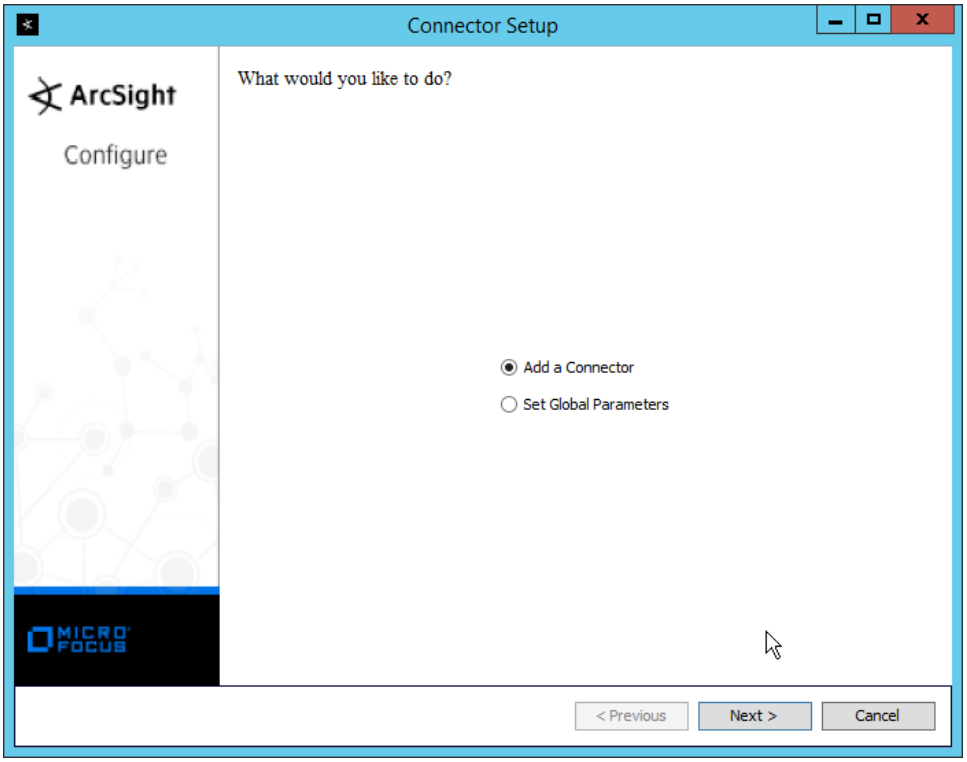
4. Click **Next.**



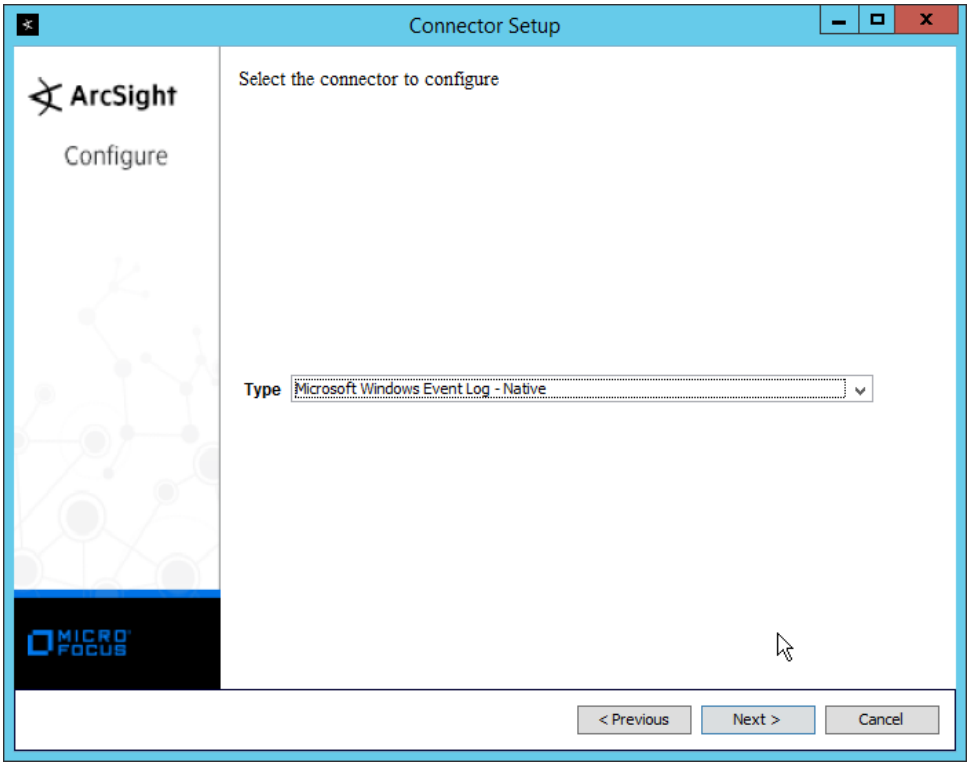
5. Click **Next.**



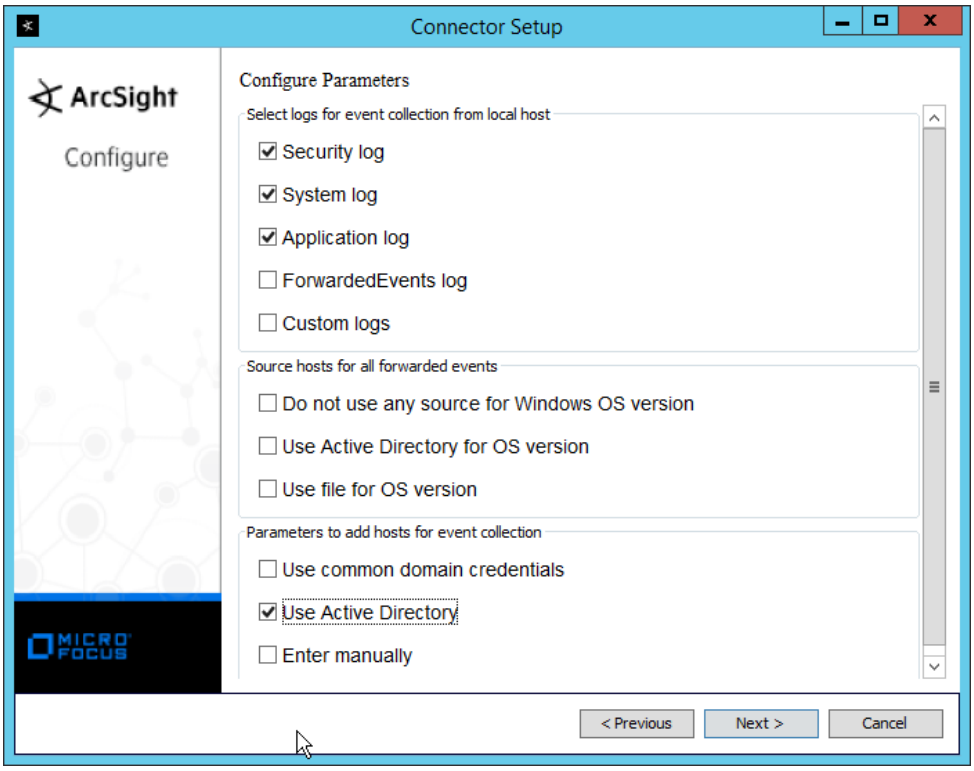
6. Click **Install.**
7. Select **Add a Connector.**



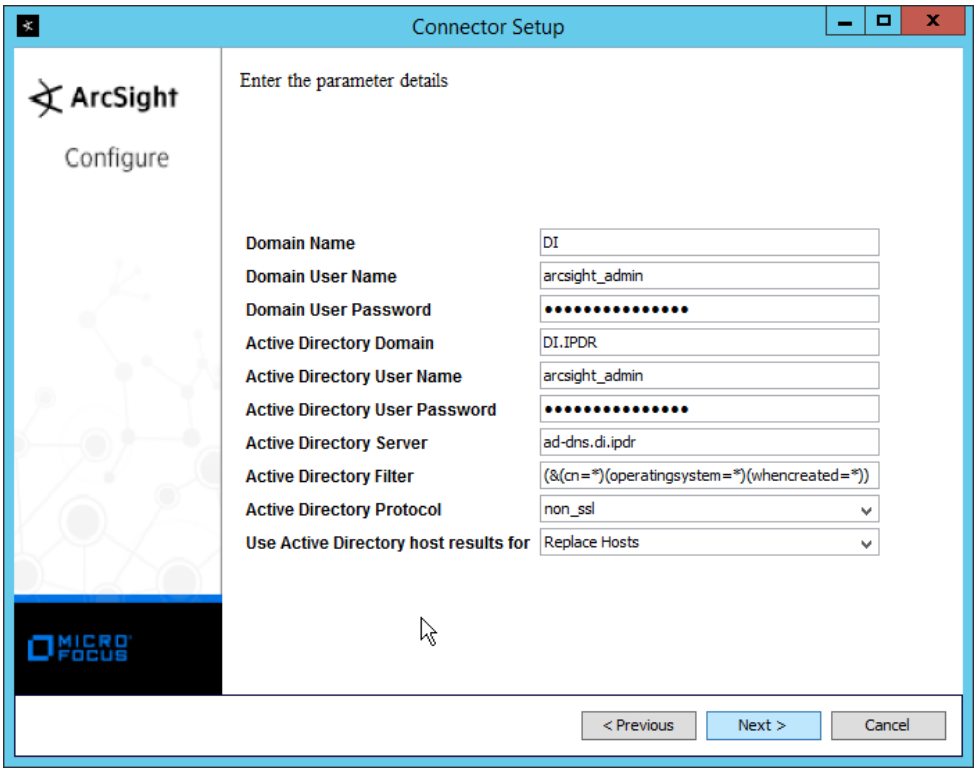
8. Click **Next.**
9. Select **Microsoft Windows Event Log – Native.**



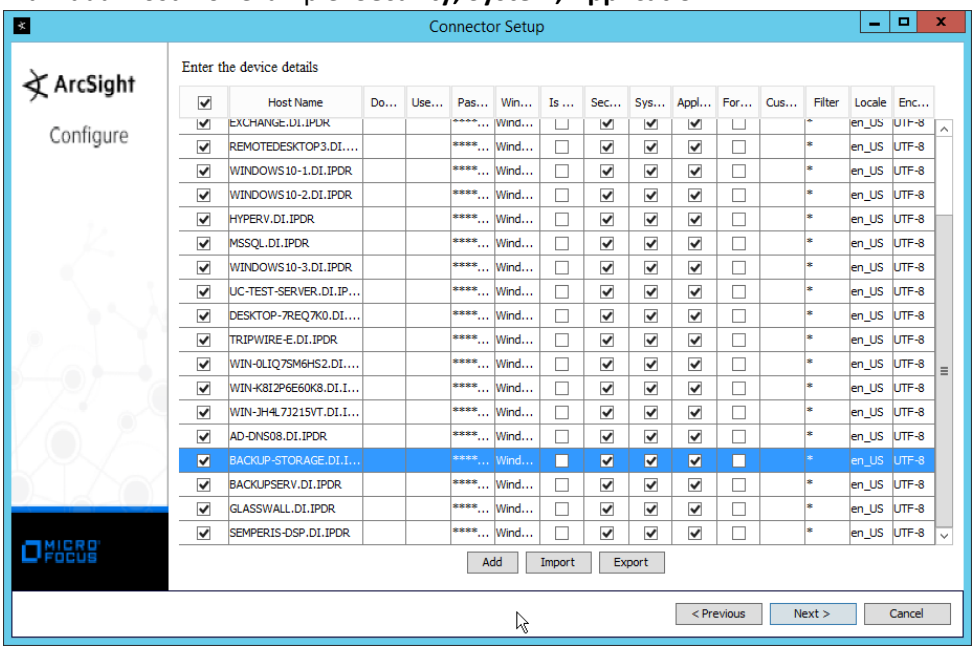
10. Click **Next.**
11. Check the box next to **Use Active Directory.**



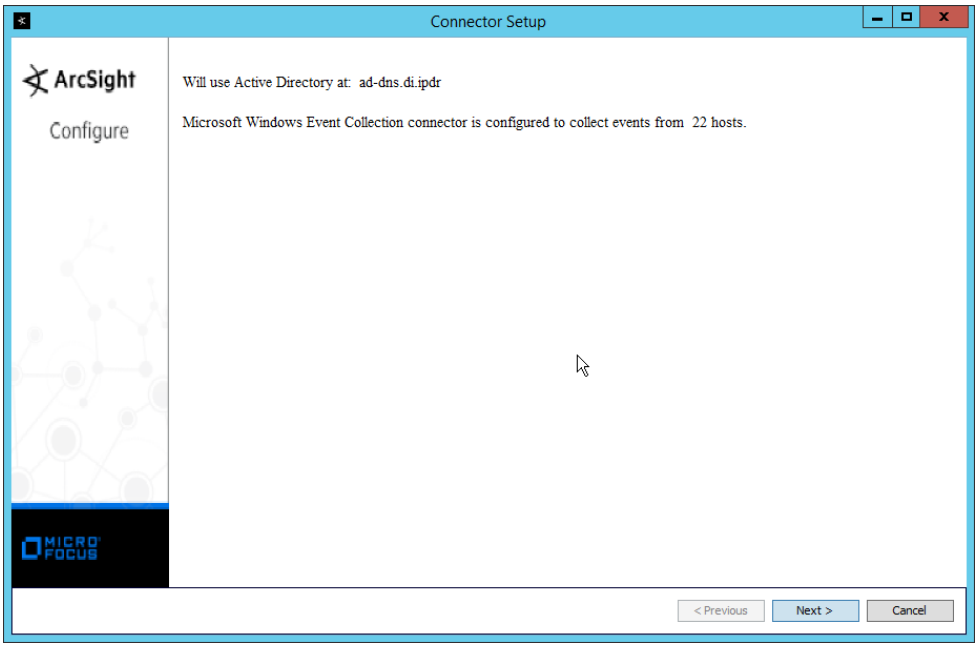
12. Click **Next.**
13. Enter information about your Active Directory server (it is recommended to create a new administrator account for ArcSight to use).
14. Set **Use Active Directory host results for** to **Replace Hosts**.



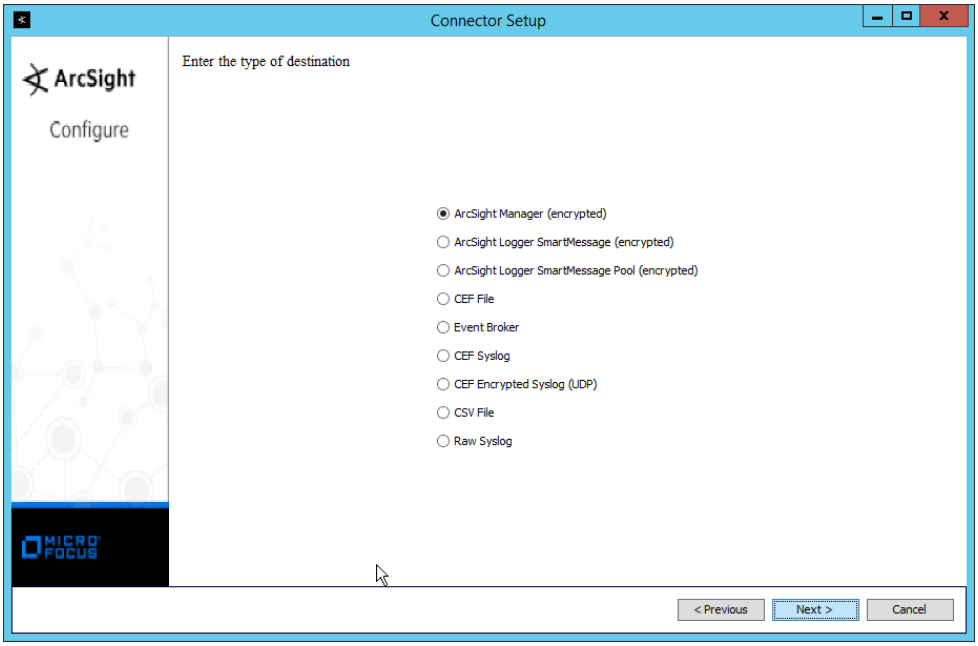
15. Click **Next.**
16. Check the boxes under any event types that should be forwarded to this connector, for each individual host. For example: **Security, System, Application.**



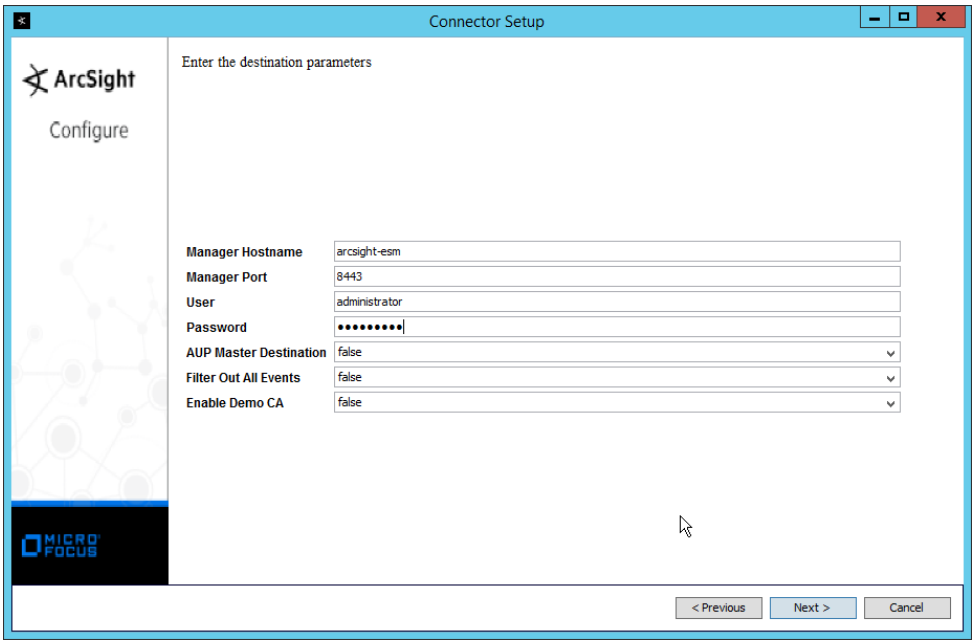
17. Click **Next.**



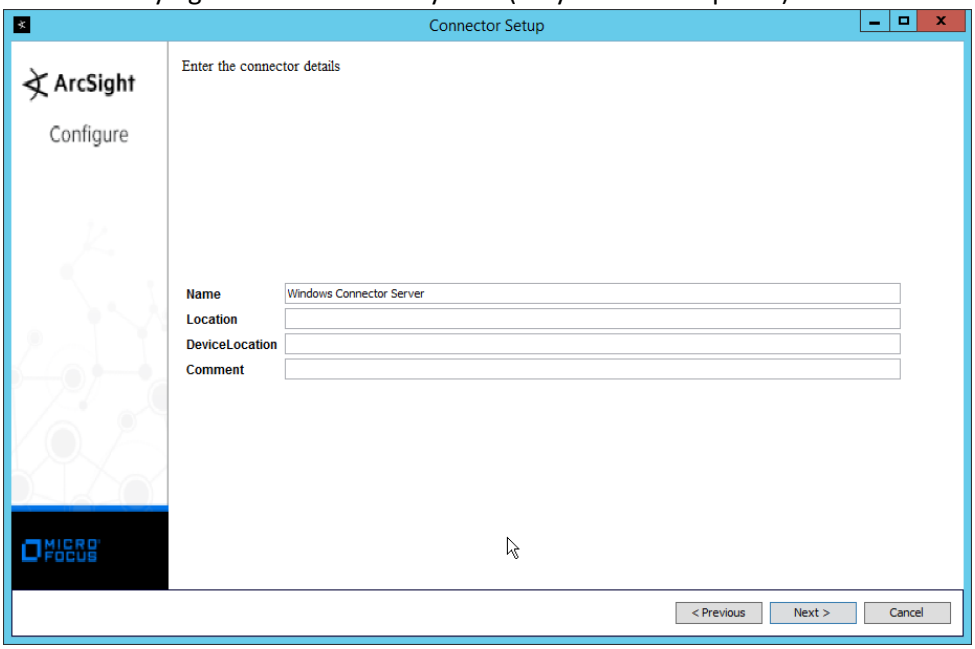
18. Click **Next.**
19. Select **ArcSight Manager (encrypted).**



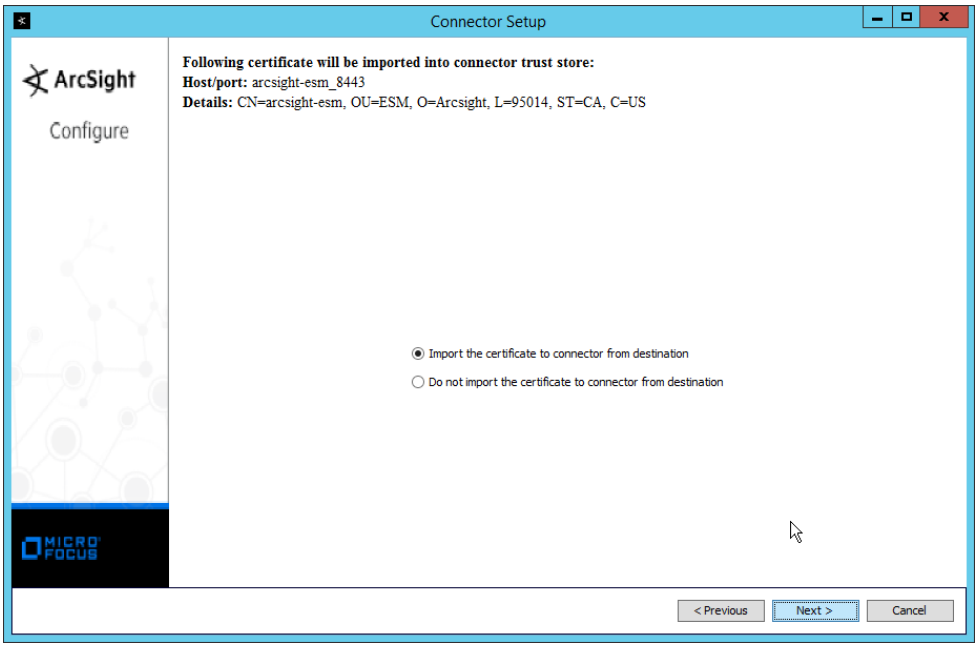
20. Click **Next.**
21. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



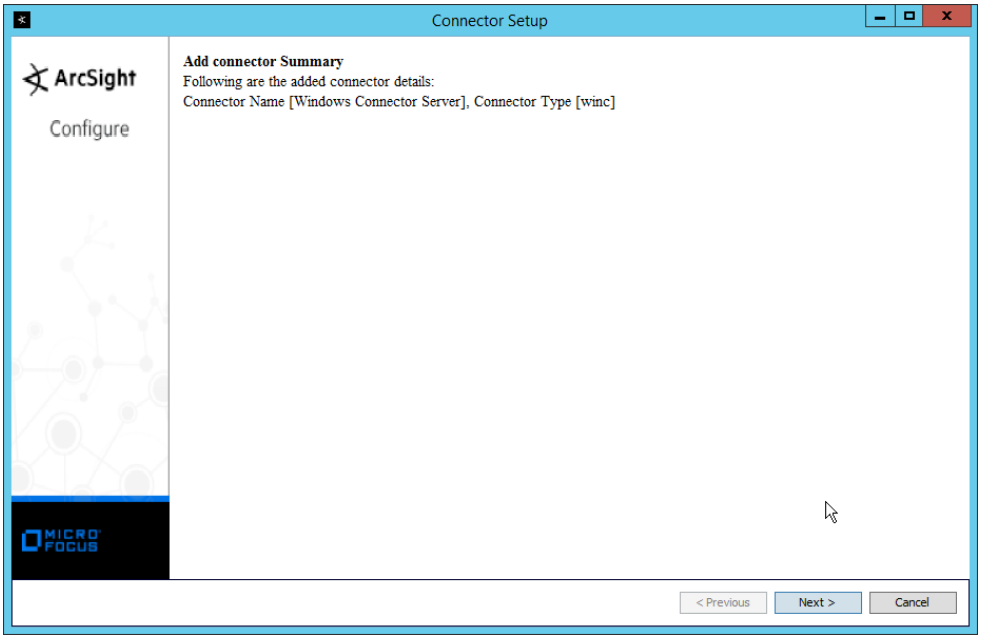
22. Click **Next.**
23. Enter identifying details about the system (only **Name** is required).



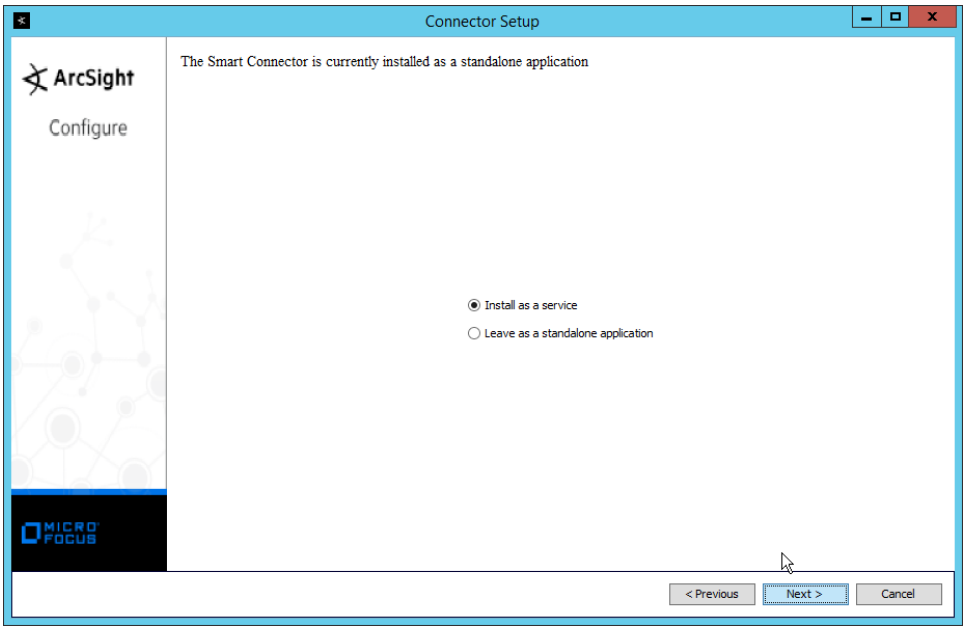
24. Click **Next.**
25. Select **Import the certificate to connector from destination.**



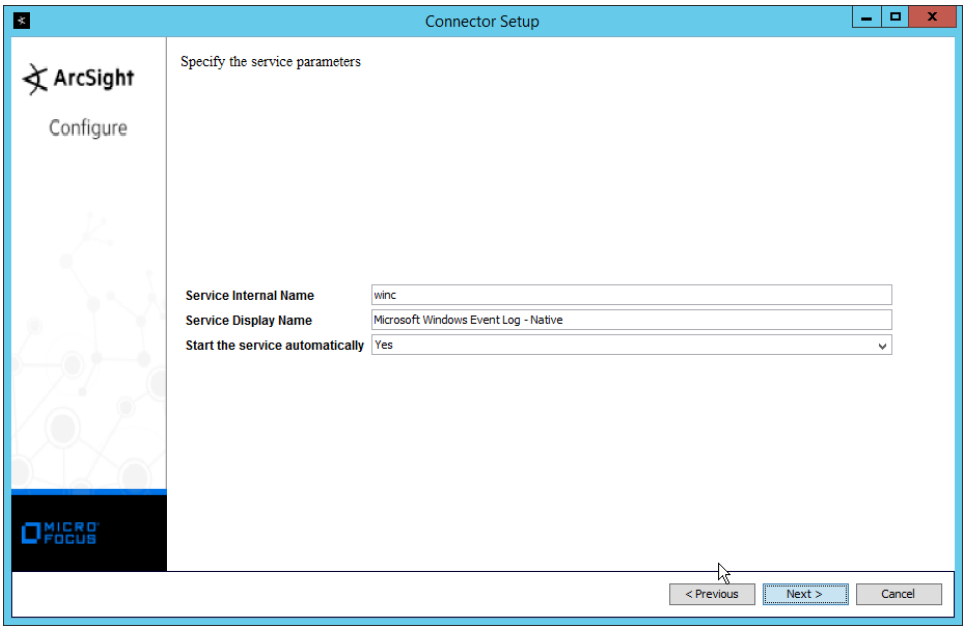
1414
1415 26. Click **Next.**



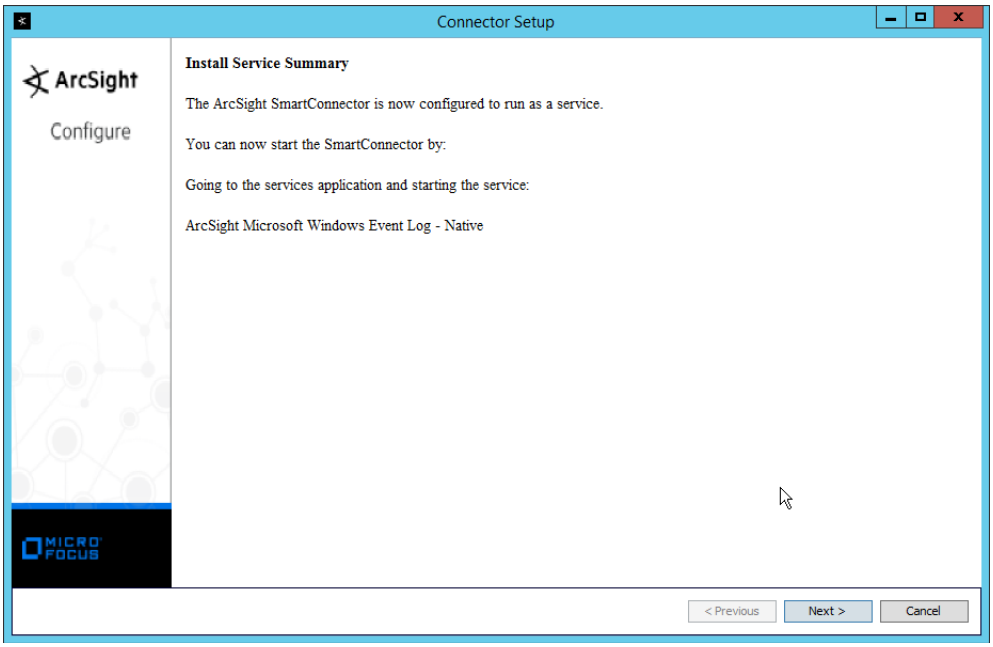
1416
1417 27. Click **Next.**
1418 28. Select **Install as a service.**



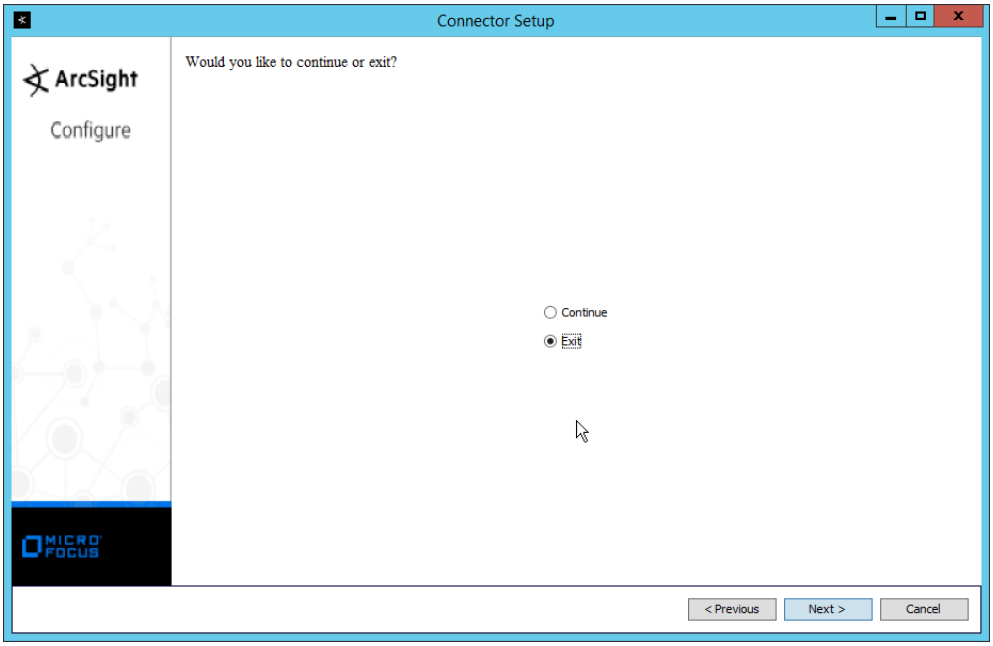
29. Click **Next.**



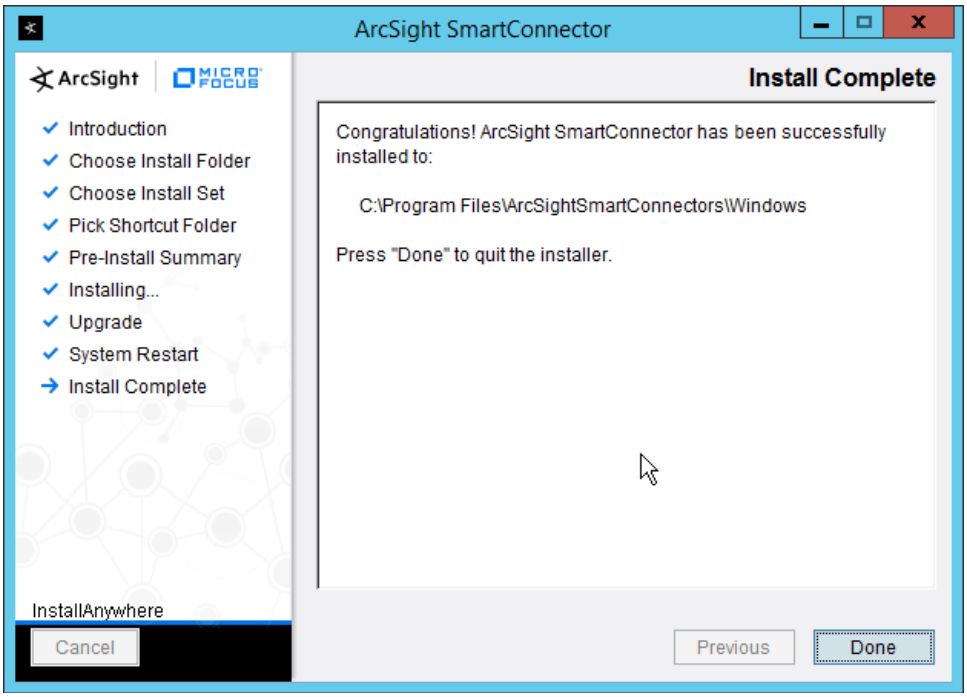
30. Click **Next.**



1423
1424 31. Click **Next.**
1425 32. Select **Exit.**



1426
1427 33. Click **Next.**

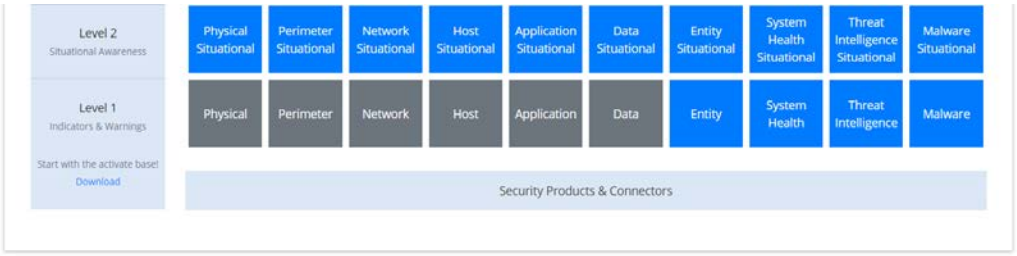


34. Click **Done.**
35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.

2.8.5 Install Pre-Configured Filters for ArcSight

2.8.5.1 *Install Activate Base*

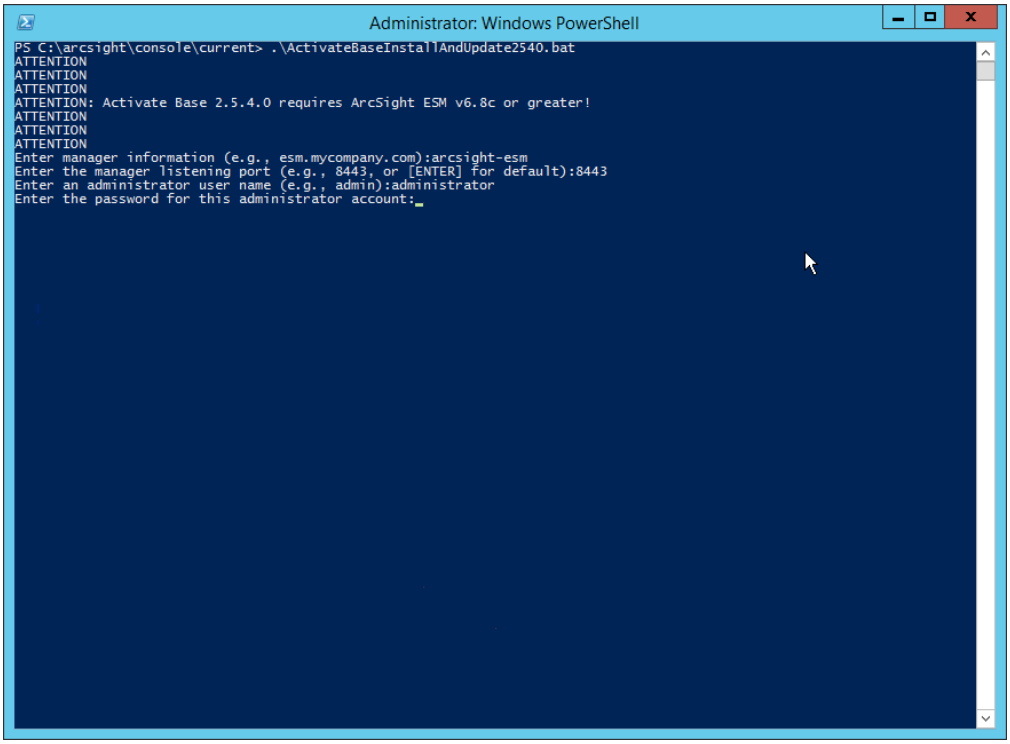
1. Go to the ArcSight Content Brain web app (https://arcsightcontentbrain.com/app/) and log in. This page allows you to keep track of packages to be installed—which packages should be installed is dependent on the needs of the organization, but the "activate base" is required for all products.



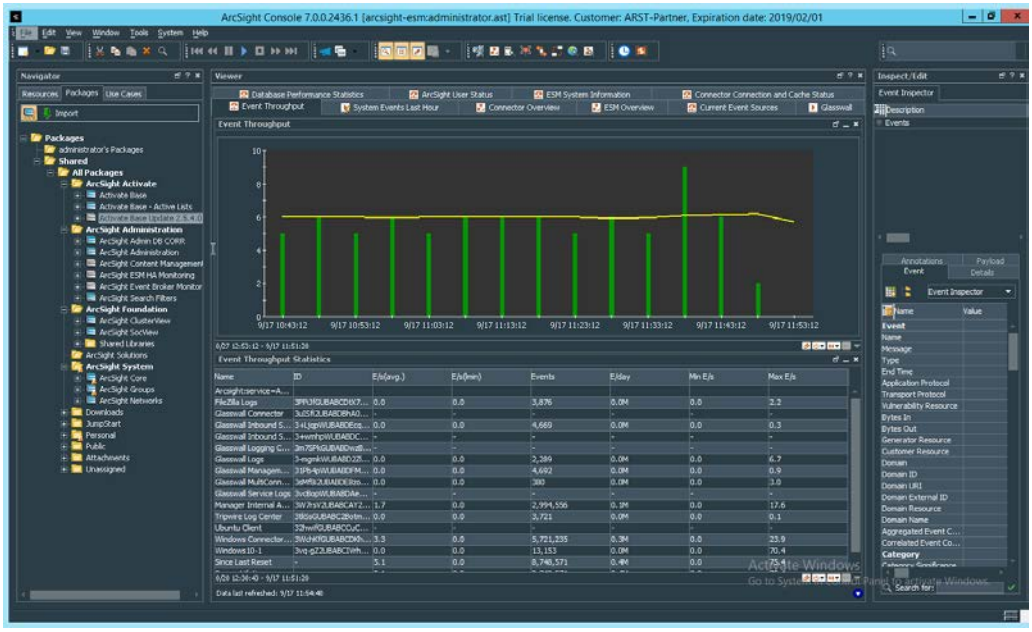
2. Click the **Download** link for the activate base. (Note: This package should be installed on the Arcsight Console, not on the ESM.)
3. Copy the contents of the zip file to *ARCSIGHT_HOME*. The default for this is *C:\arcsight\Console\current*, assuming a Windows Server.

4. In PowerShell, navigate to the *ARCSIGHT_HOME* directory *(C:\arcsight\Console\current),* and run:

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



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.**

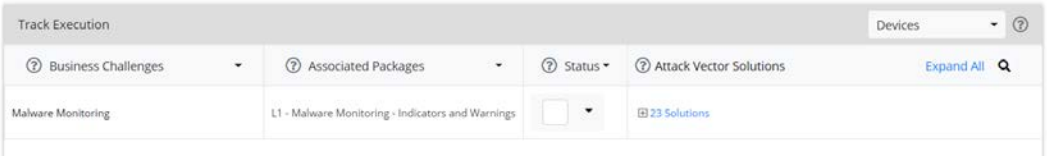


8. Under **Packages > Shared > All Packages > ArcSight Activate,** right-click **Activate Base Update 2.5.4.0,** and select **Delete Package.**

2.8.5.2 *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.

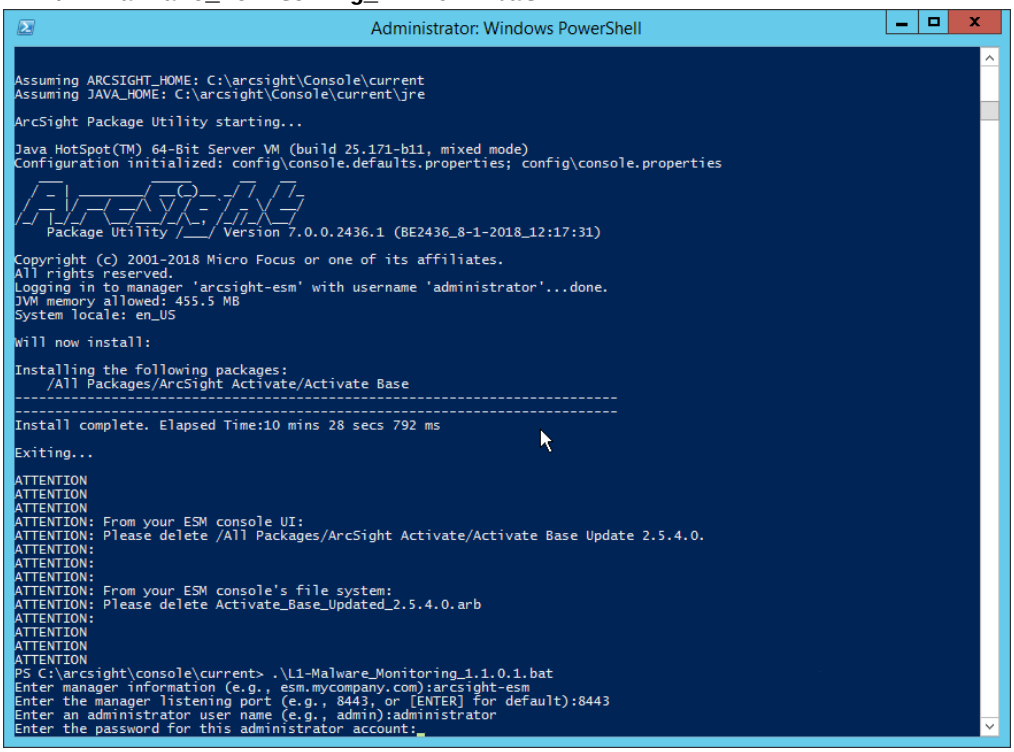
1. Navigate to the **ArcSight Content Brain** web app.
2. Select the **Level 1** box labeled **Malware.**



3. 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:

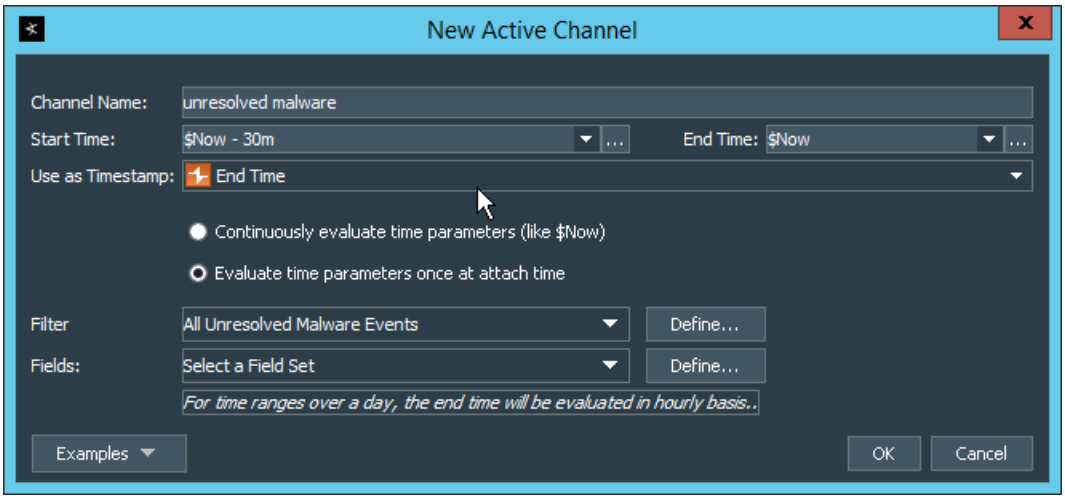
```
> .\L1-Malware_Monitoring_1.1.0.1.bat
```



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

2.8.6 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.

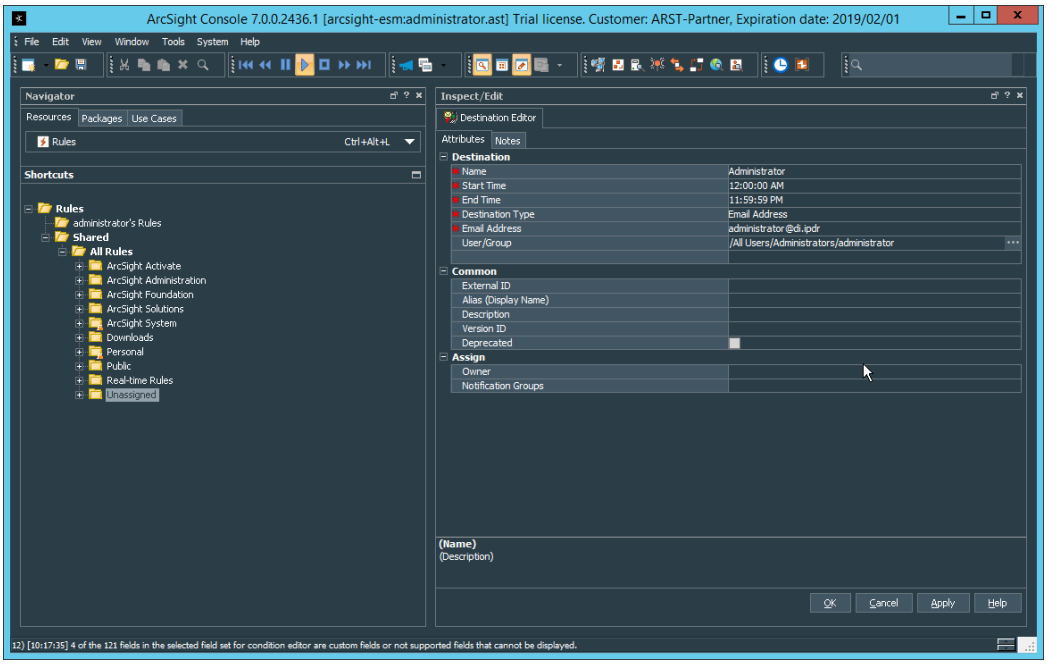


5. Click **OK.** All events that match the filter can be displayed in the newly created channel. Filters from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate > Solutions.**

2.8.7 Configure Email Alerts in ArcSight

2.8.7.1 *Configure a New Destination*

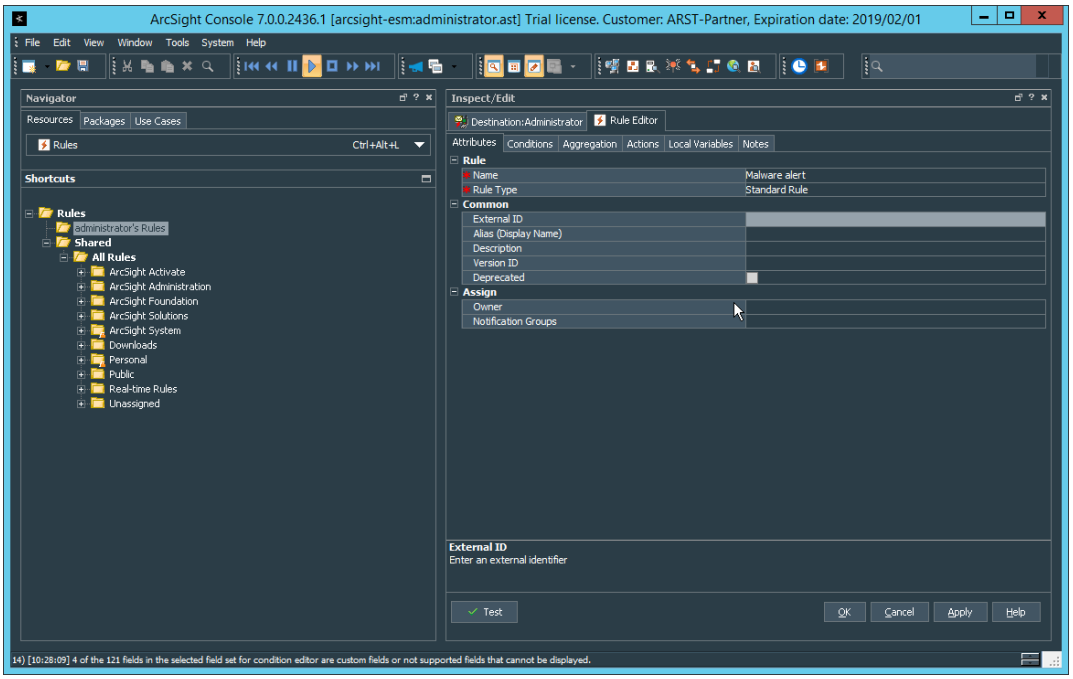
1. In **ArcSight Console,** click **File > New > Destination.**
2. Enter a name for the **Destination.**
3. For **Destination Type,** select **Email Address.**
4. For **Email Address,** enter the email that should be associated with this destination.



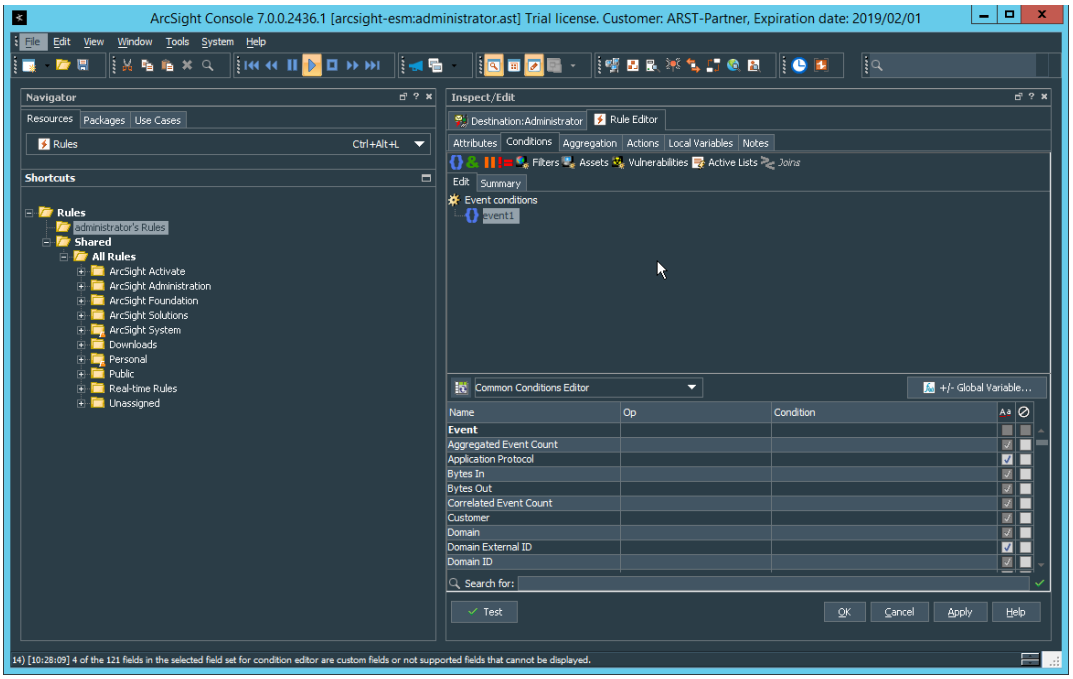
5. Click **OK.**
6. Select a place to save the new **Destination.**
7. Click **OK.**

2.8.7.2 *Configure a New Rule*

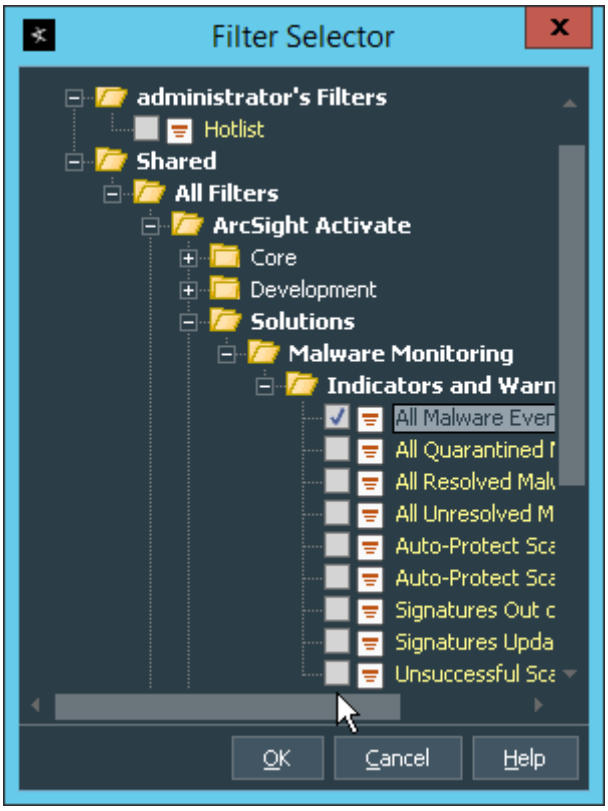
1. Click **File > New > Rule > Standard Rule.**
2. Enter a name for the rule.



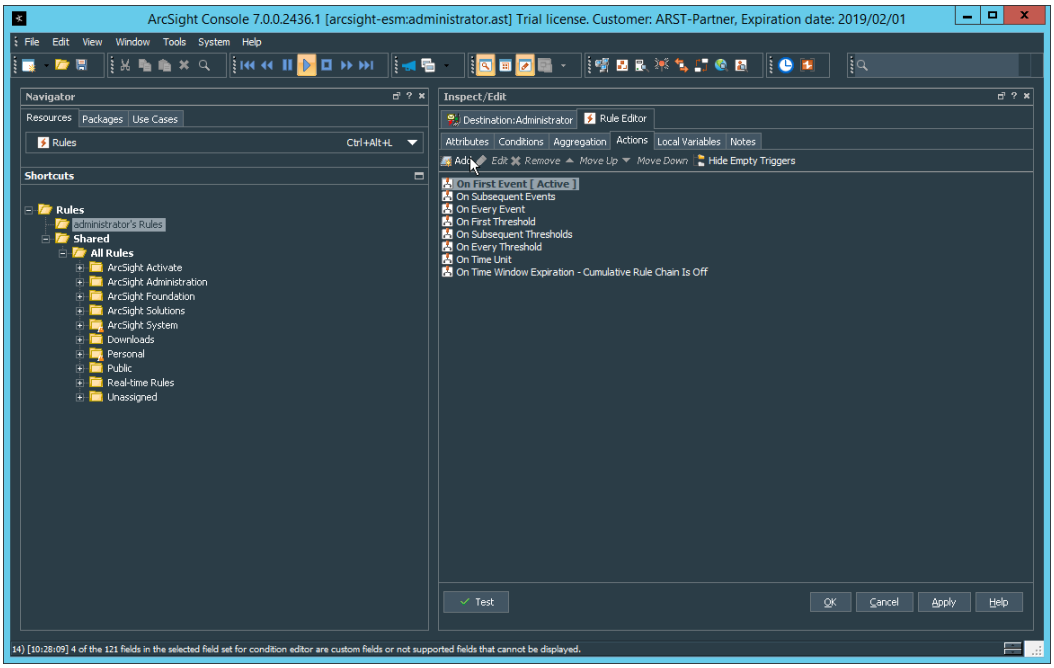
3. Click the **Conditions** tab.



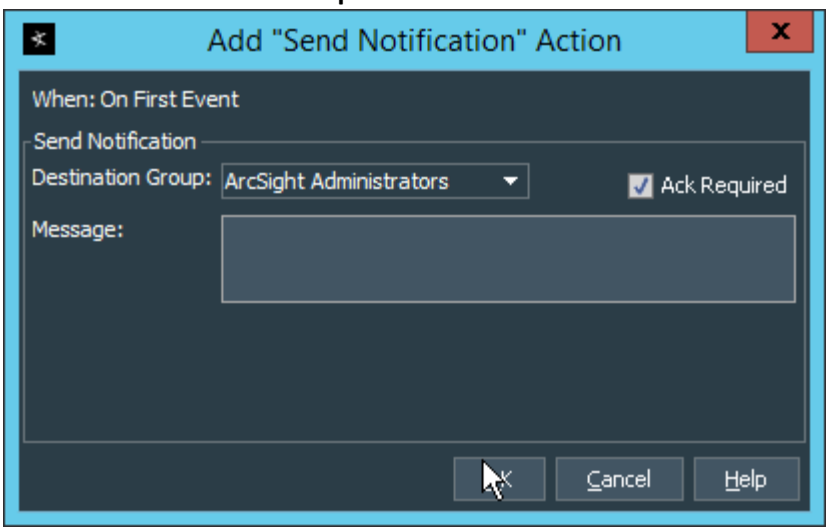
4. Either create a custom condition for the rule or click the **Filters** button to select a pre-configured Filter. (Ensure you check the box next to desired filters if you choose to select a pre-configured filter.)



5. If you selected a filter, click **OK.**
6. Click the **Actions** tab.



7. Select the trigger for the notification, and click **Add > Send Notification.**
8. Select the **Destination Group** in which the desired destinations reside.



9. Click **OK.**

2.9 Tripwire Enterprise

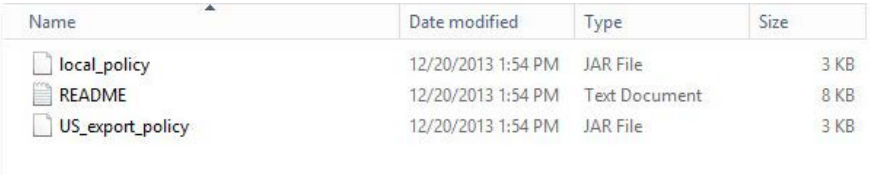
Notes:

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.*

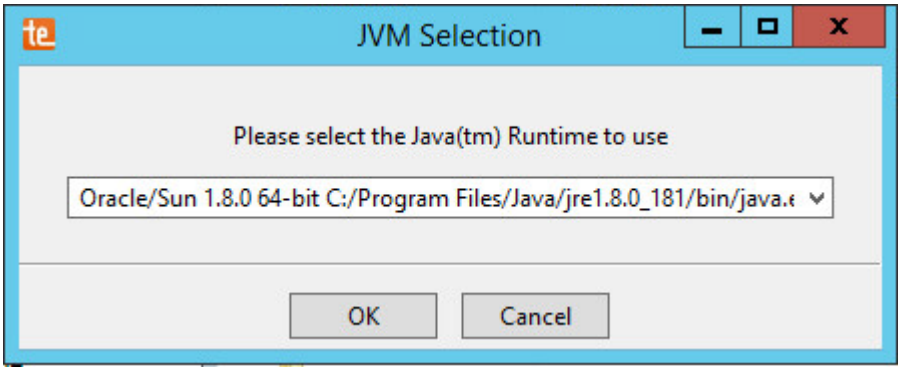
2.9.1 Install Tripwire Enterprise

1. Ensure that you have a current 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.**

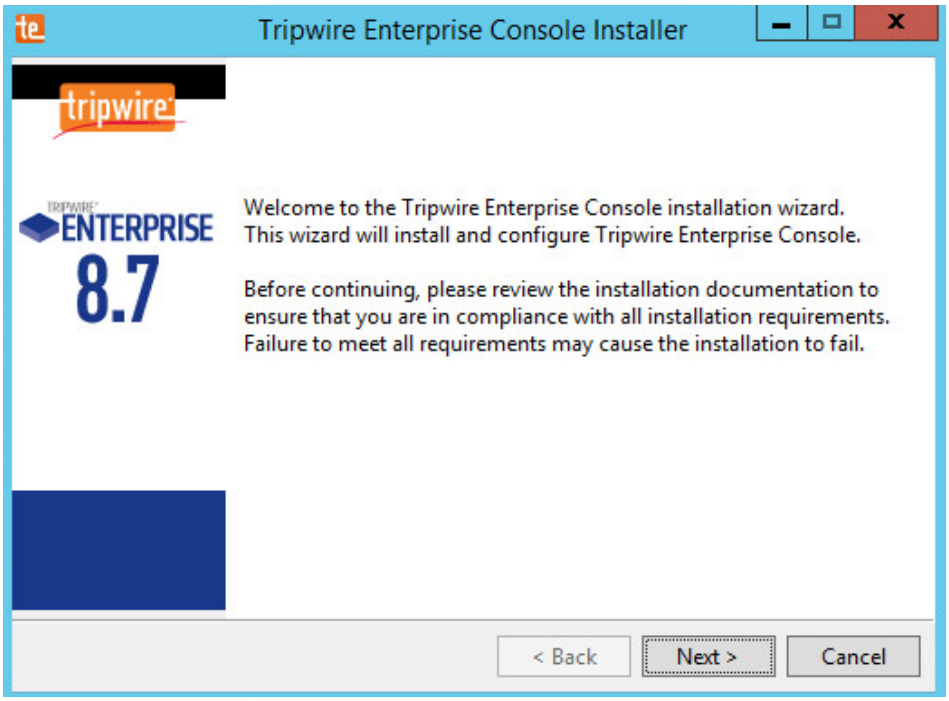
3. Click **Install.**
4. Download the JCE, and extract the files.



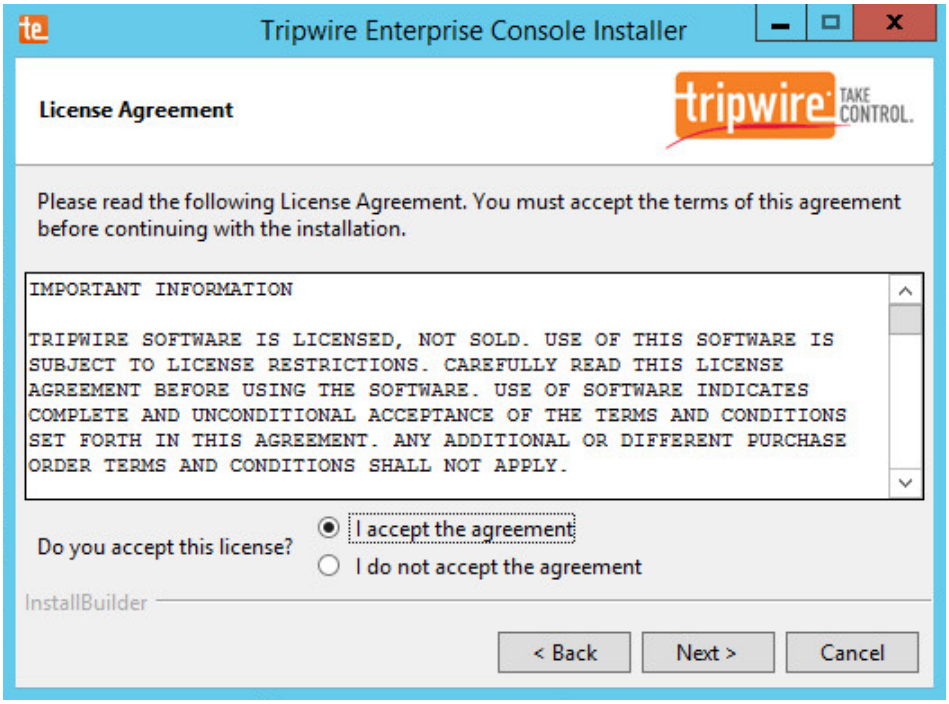
5. Copy the **local_policy.jar** and **US_export_policy.jar** files to */lib/security/Unlimited/* and */lib/security/Limited* in the Java installation directory.
6. Run **install-server-windows-amd64.**
7. Select the Java runtime that was just installed.



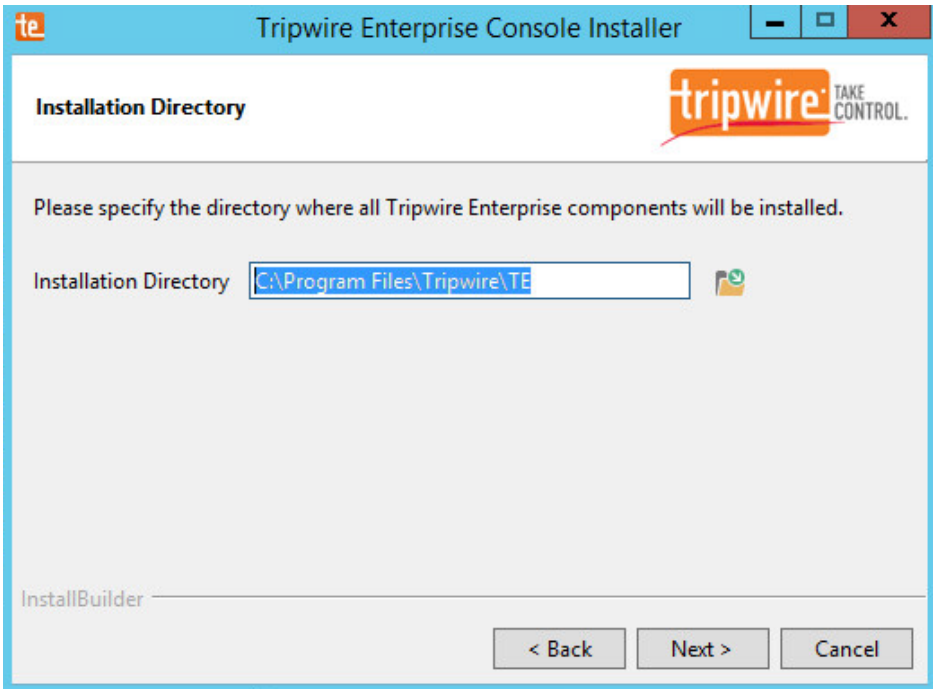
8. Click **OK.**



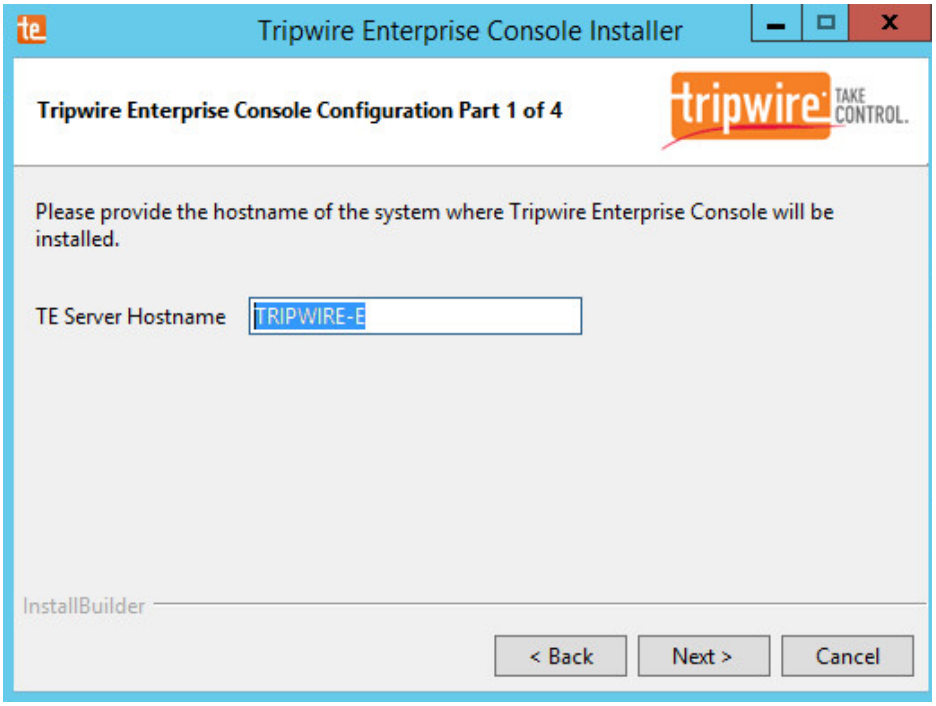
9. Click **Next.**
10. Select **I accept the agreement.**



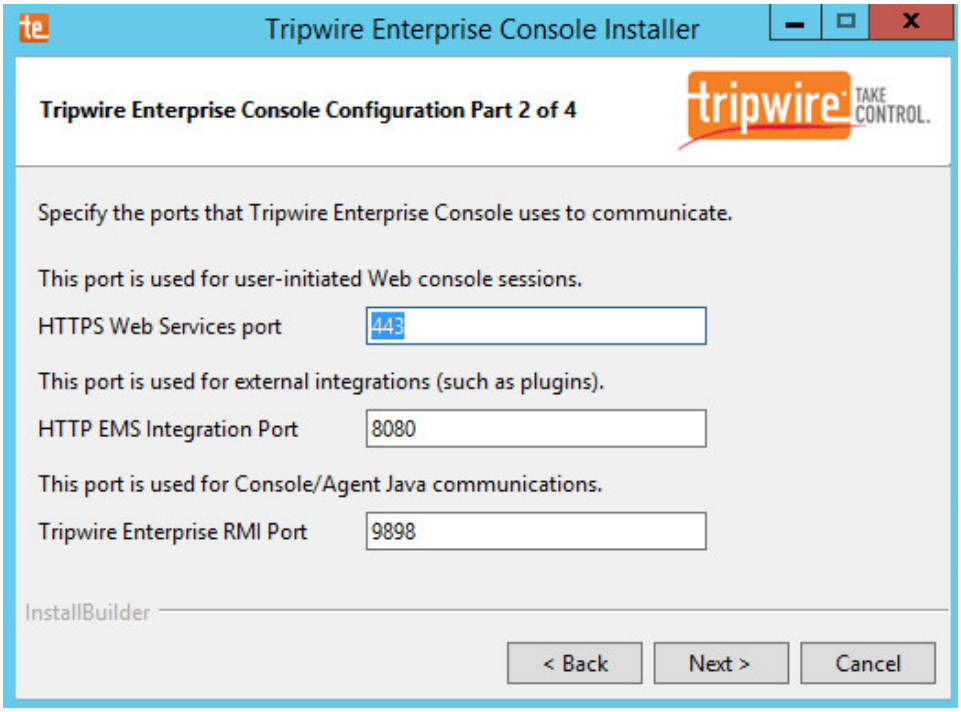
11. Click **Next.**



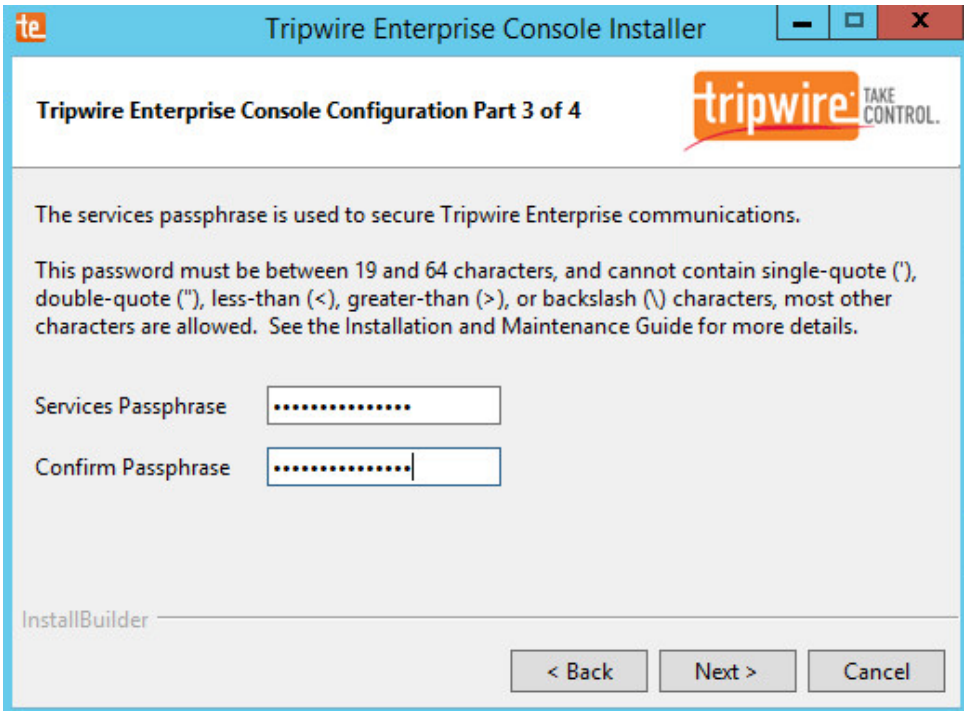
12. Click **Next.**
13. The installer should automatically detect the hostname of the system on which Tripwire Enterprise is being installed. If it does not, enter the hostname here.



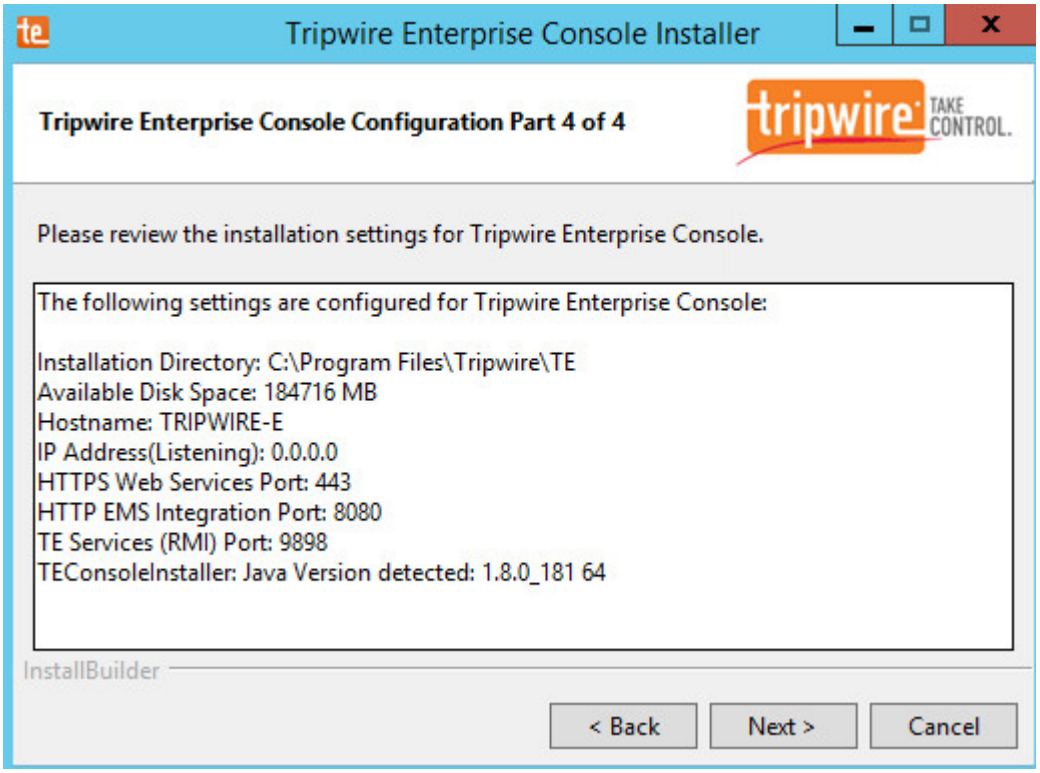
14. Click **Next.**
15. Enter the port numbers to use for each of the **HTTPS Web Services port, HTTP EMS Integration Port,** and **Tripwire Enterprise RMI port.** The RMI port is used for inbound communication from Tripwire agents to the server, so ensure that it is allowed through the firewall.



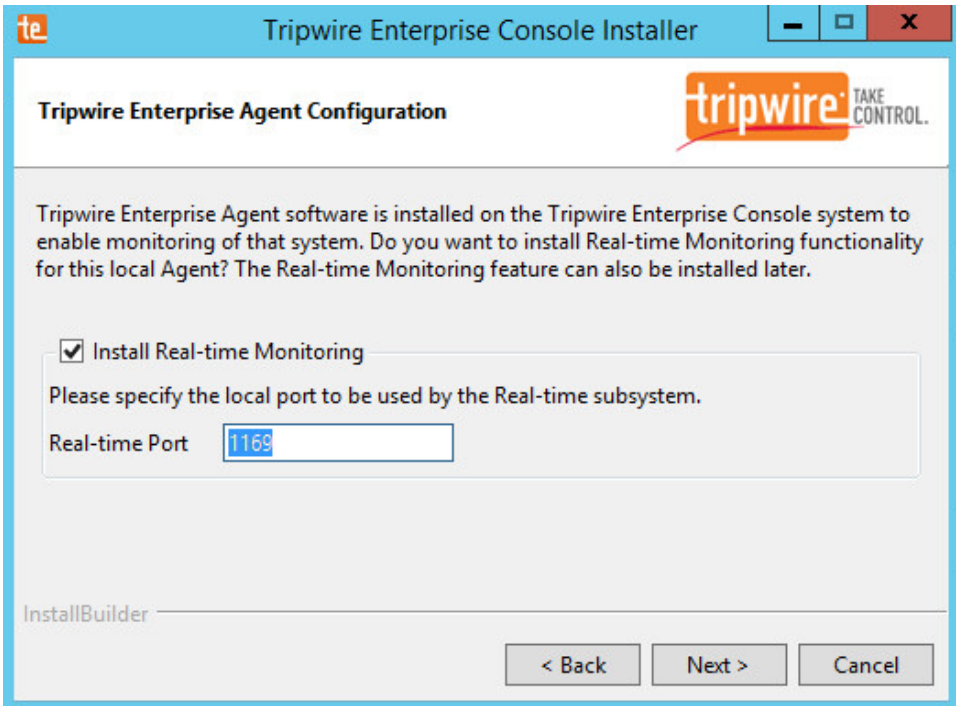
16. Click **Next.**
17. Enter a passphrase to use.



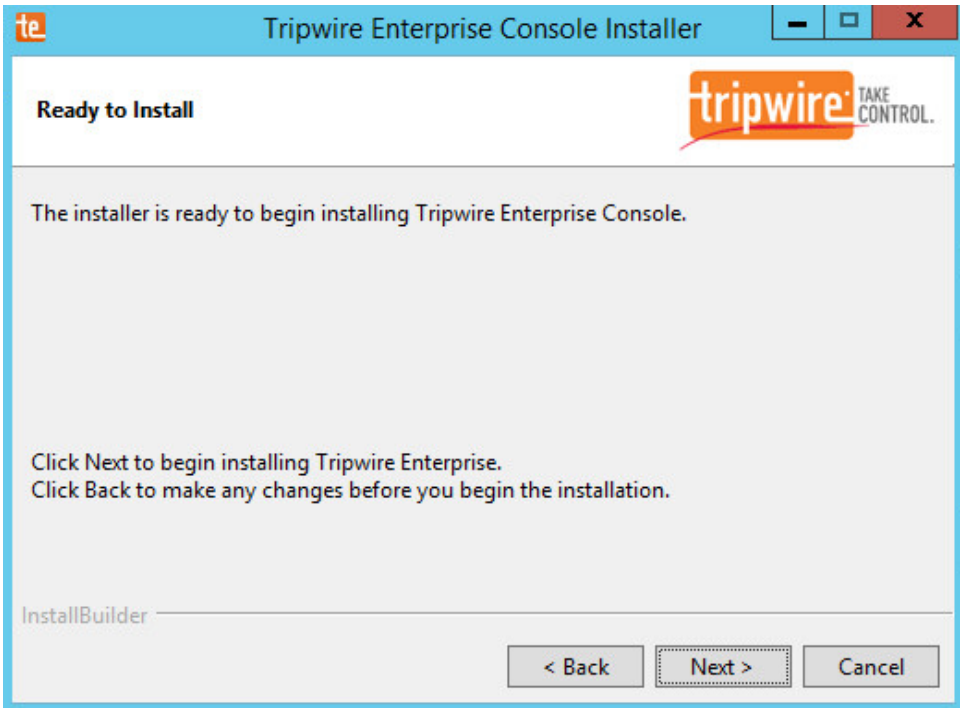
18. Click **Next.**



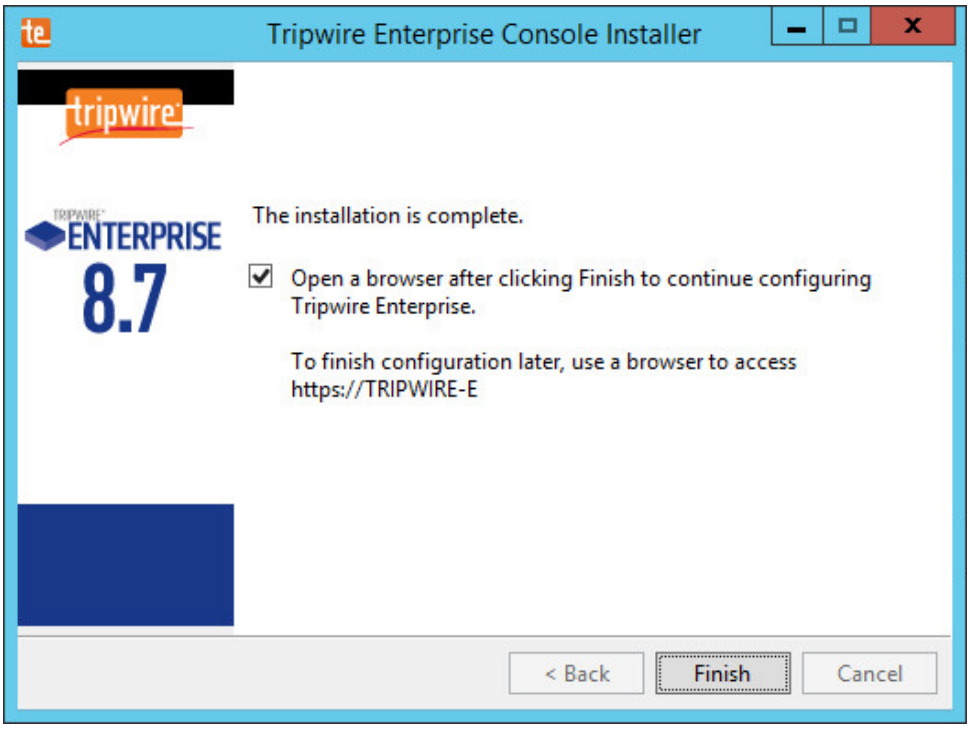
19. Click **Next.**
20. Check the box next to **Install Real-time Monitoring.**
21. Enter **1169** for **Real-time Port.**



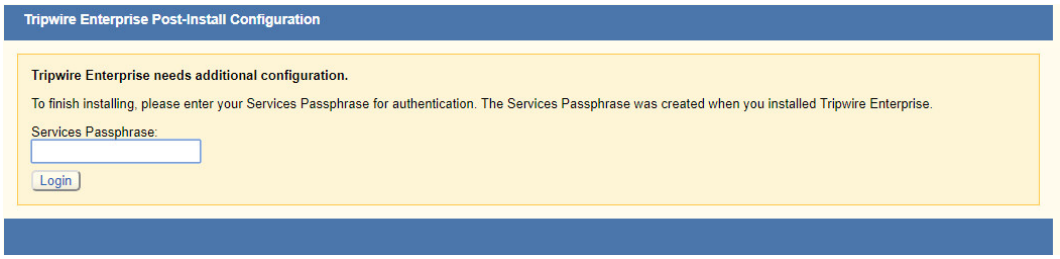
22. Click **Next.**



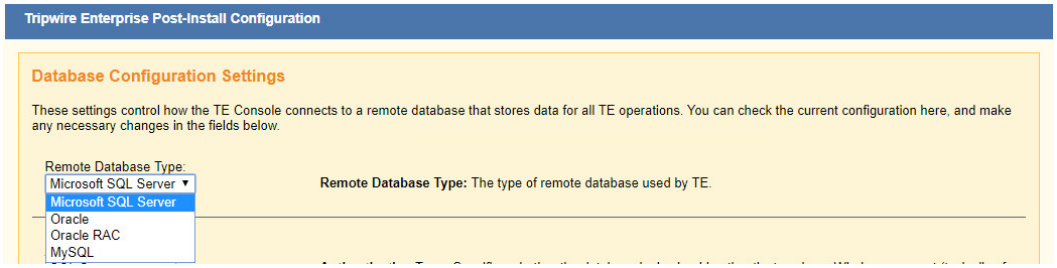
23. Click **Next.**
24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise.**



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

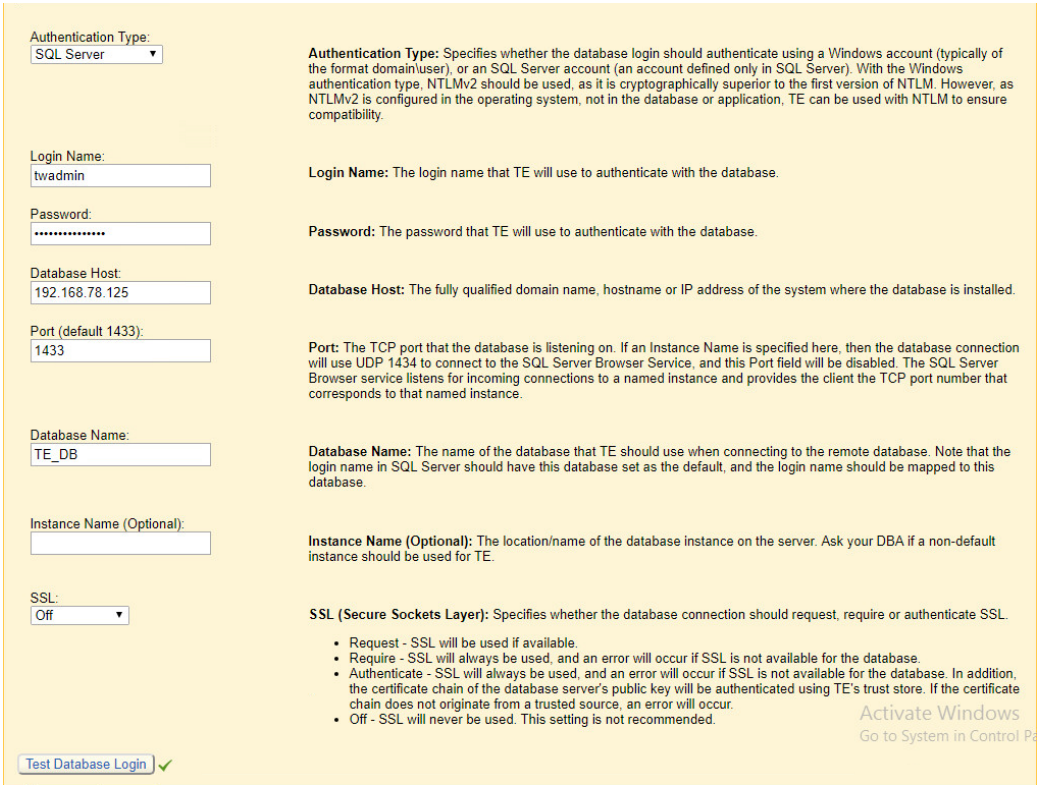


27. Click **Login.**

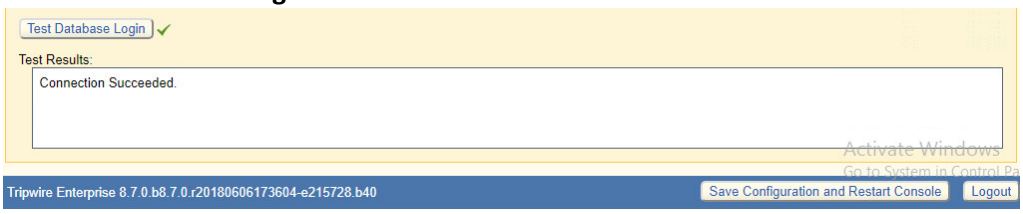


28. Select **Microsoft SQL Server** for **Remote Database Type.**
29. Select **SQL Server** for **Authentication Type.**
30. Enter login details for the account created during the MSSQL setup.
31. Enter the **hostname** or **IP** of the database server.

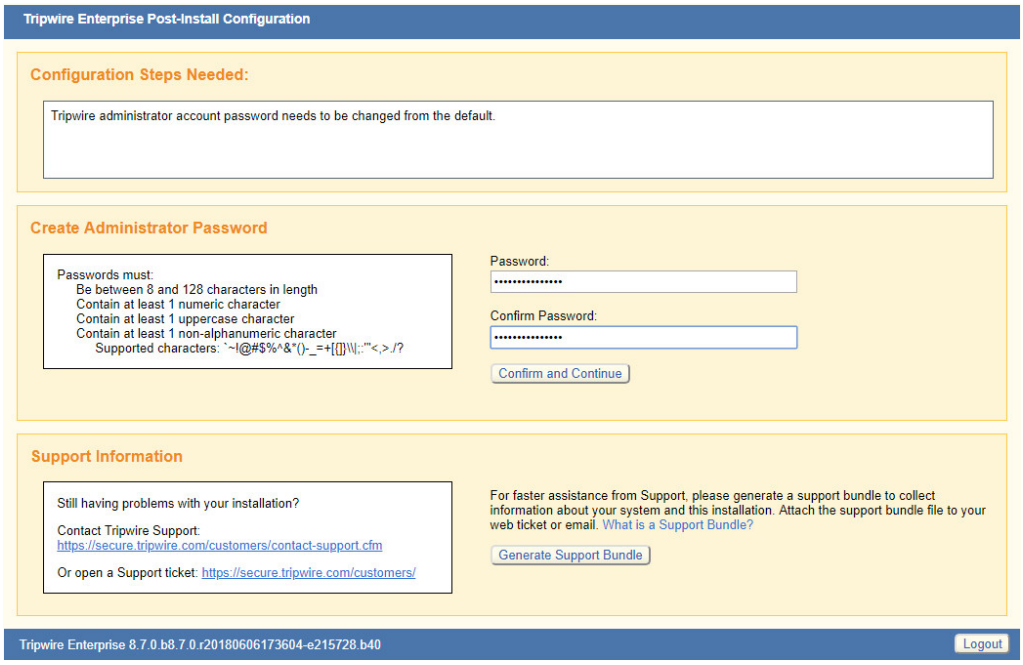
32. Enter the **port** on which the database is operating.
33. Enter the **name** of the database to be used for Tripwire Enterprise.
34. Select the appropriate setting for **SSL** according to your organization's needs.



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



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

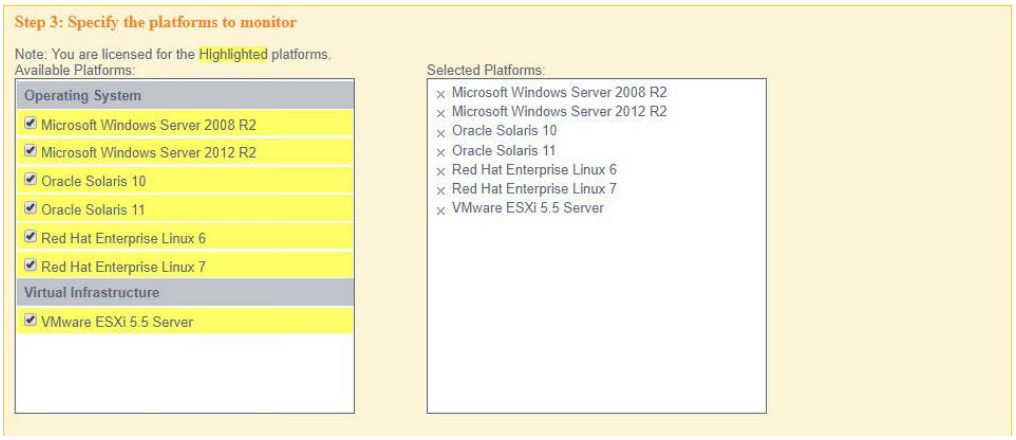


38. Click **Confirm and Continue.**

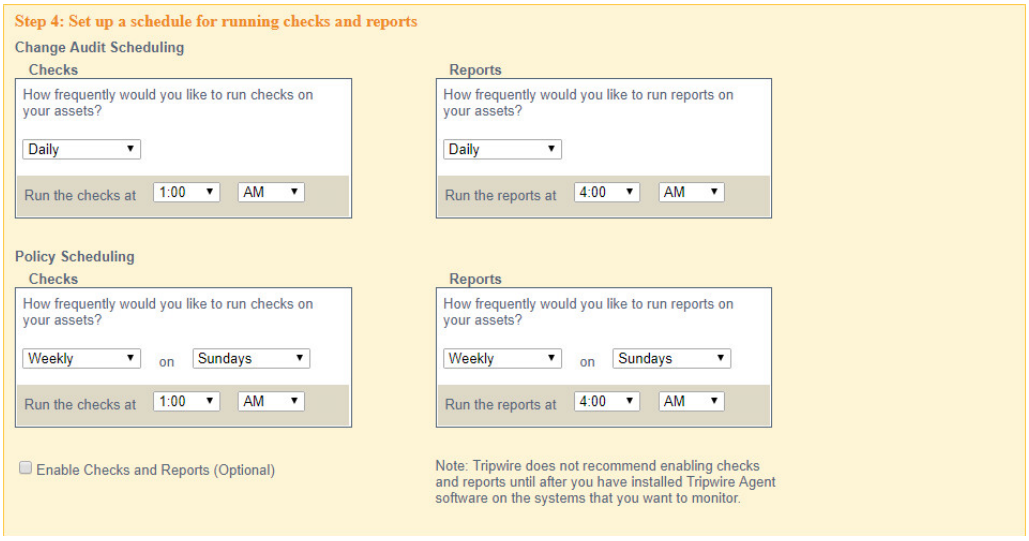
39. Click **Configure Tripwire Enterprise.**

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

42. Select any available policies desired.

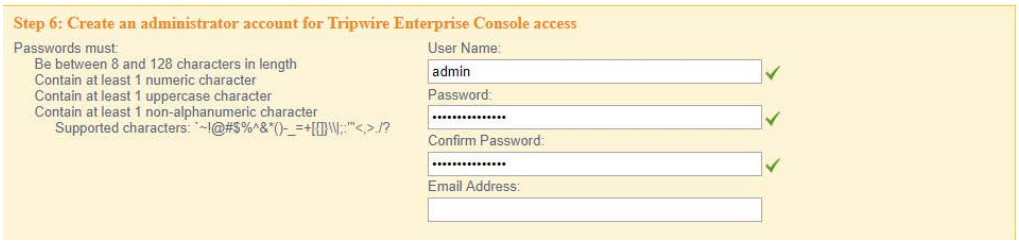


43. Select all the operating systems that you wish to monitor with Tripwire Enterprise (TE).



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.

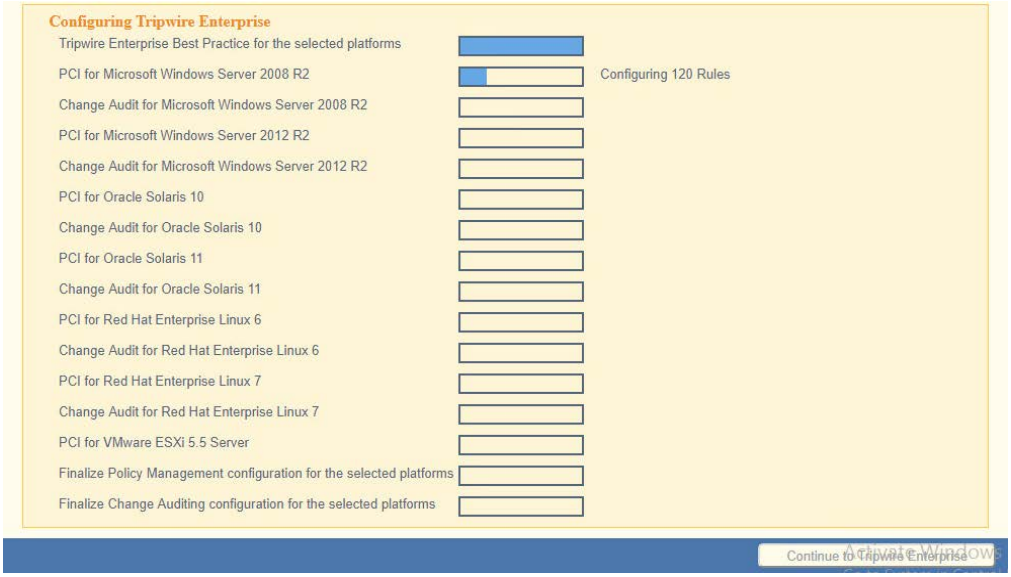
45. Select **Set up the email server at another time.**



46. Enter a username and password for a new administrator account for TE Console.

47. Click **Preview Configuration.**

48. Click **Apply Configuration.**



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

2.9.2 Install the Axon Bridge

1. Ensure that TCP traffic on port 5670 is allowed through the firewall.
2. Navigate to the TE 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 if the connection fails later.
4. Restart the TE console by running the following command from an administrator command prompt, where *<te_root>* is the TE installation directory:

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

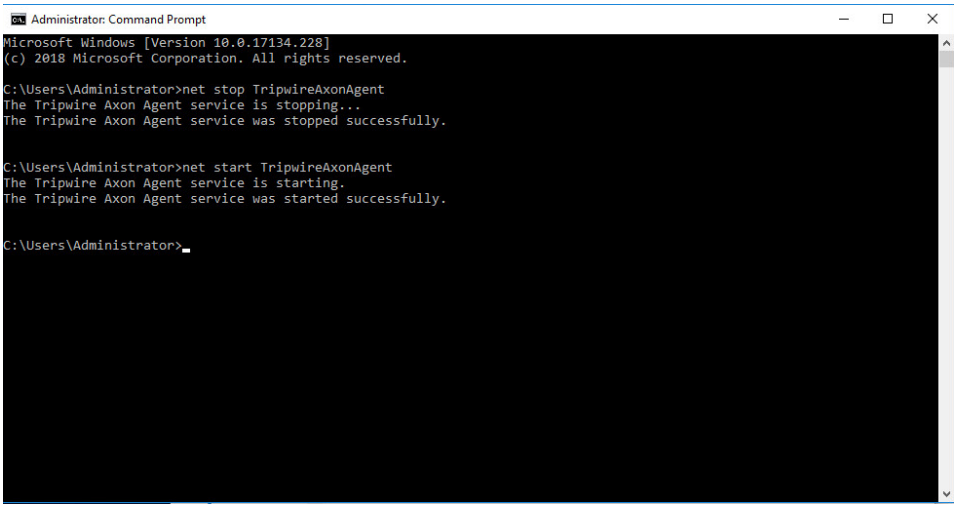
2.9.3 Install the Axon Agent (Windows)

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 pre-shared 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`



2.9.4 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 pre-shared 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
```

2.9.5 Configure Tripwire Enterprise

2.9.5.1 *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.

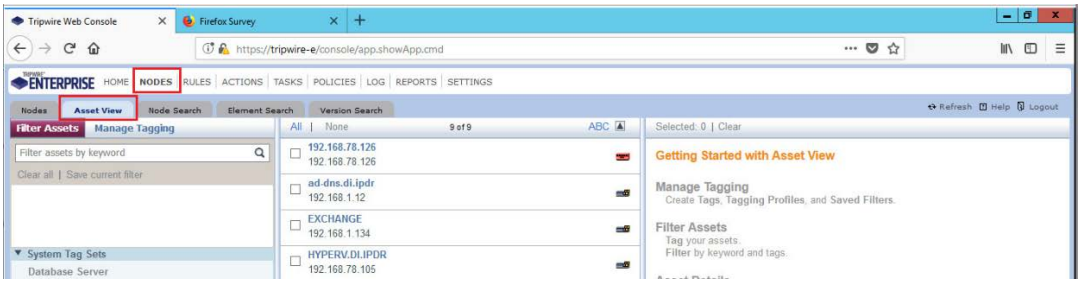
Baseline: The act of creating an element that reflects the current state of a monitored object (also called the **current baseline.** When a node's baseline is promoted, TE saves the former baseline as a **historic baseline.**

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.

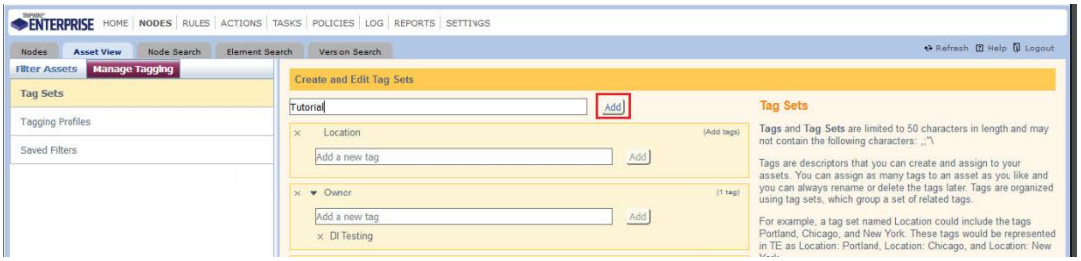
2.9.5.2 *Tags*

In TE, 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 will describe how to create and assign tags.

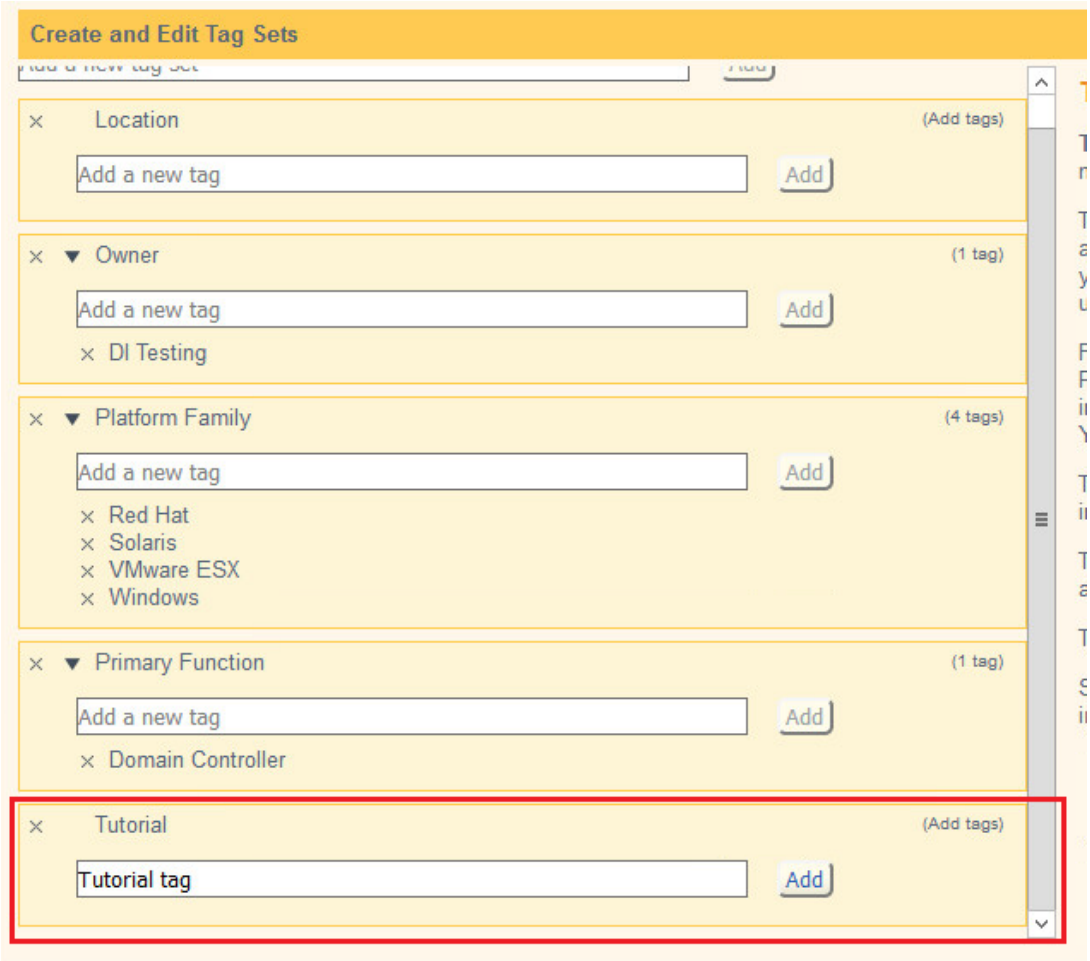
1. Navigate to the TE Console in your browser.
2. Click **Asset View.**



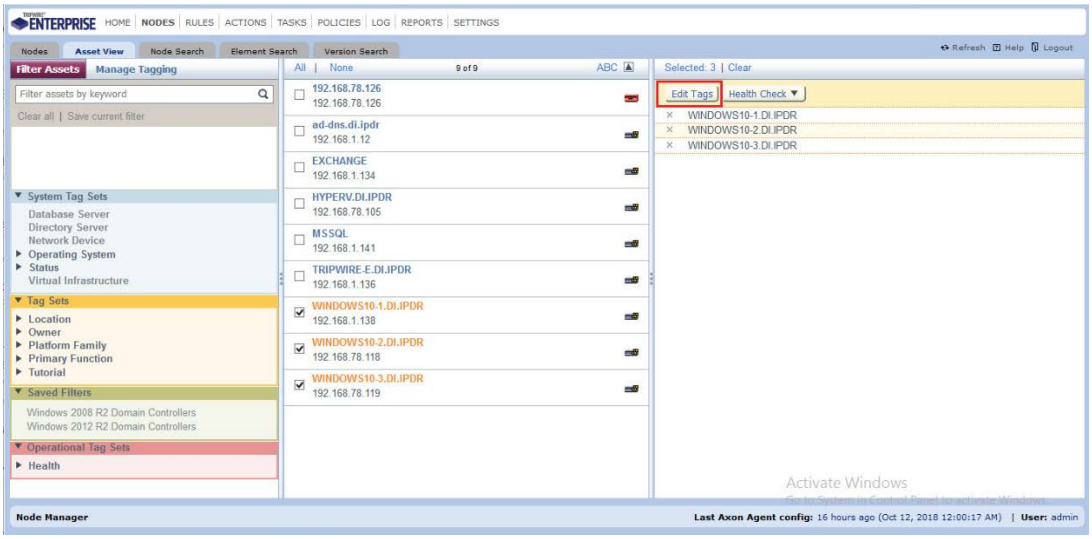
3. Click the **Manage Tagging** tab.
4. Enter the name of a tag set or use one of the four existing ones (**Location, Owner, Platform Family, Primary Function**). Click **Add** if adding your own tag set.



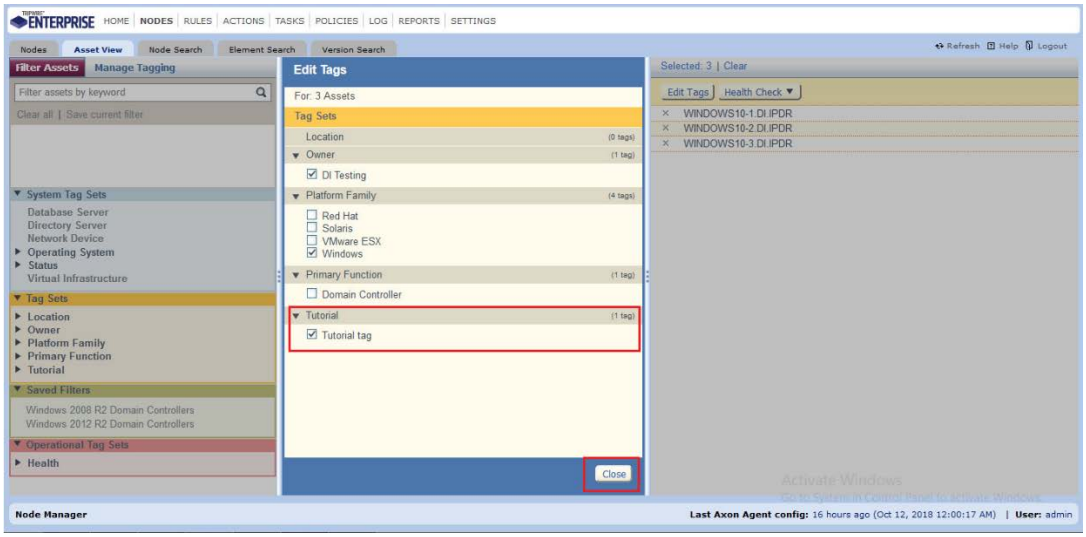
5. Under the tag set you wish to add a tag to, enter the name of the tag.



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.



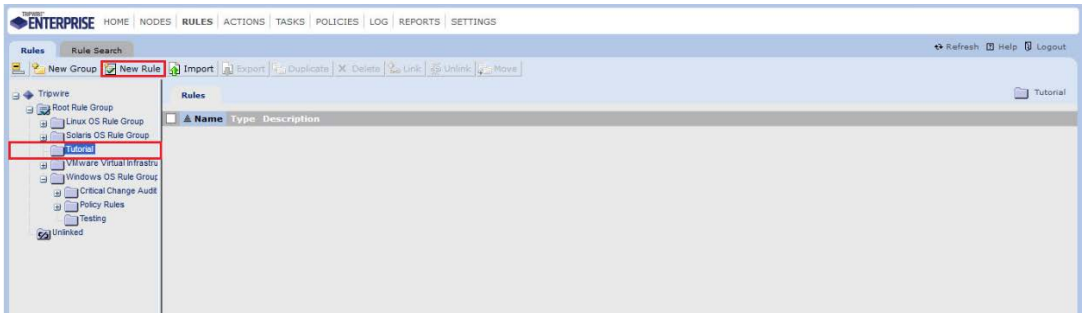
11. Click **Close.**

2.9.5.3 *Rules*

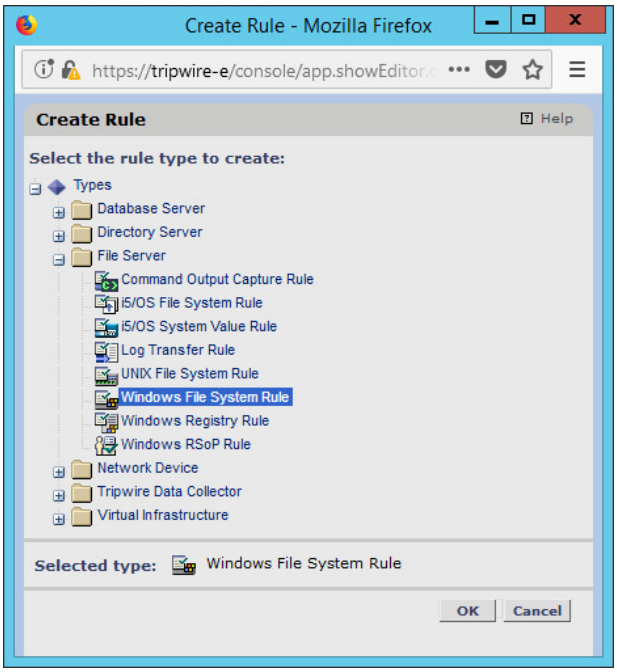
This section will describe how to create a rule.

1. Click **Rules.**

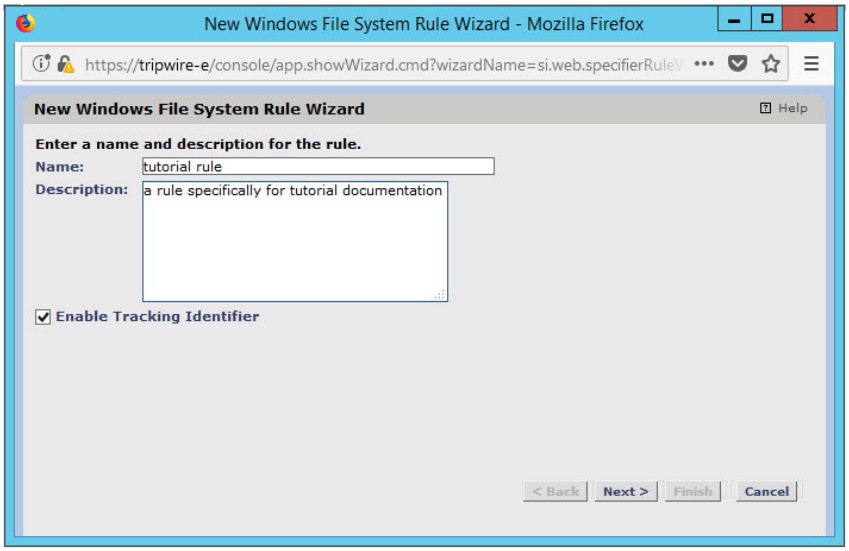
2. Select or create a rule group in which to put the new rule.



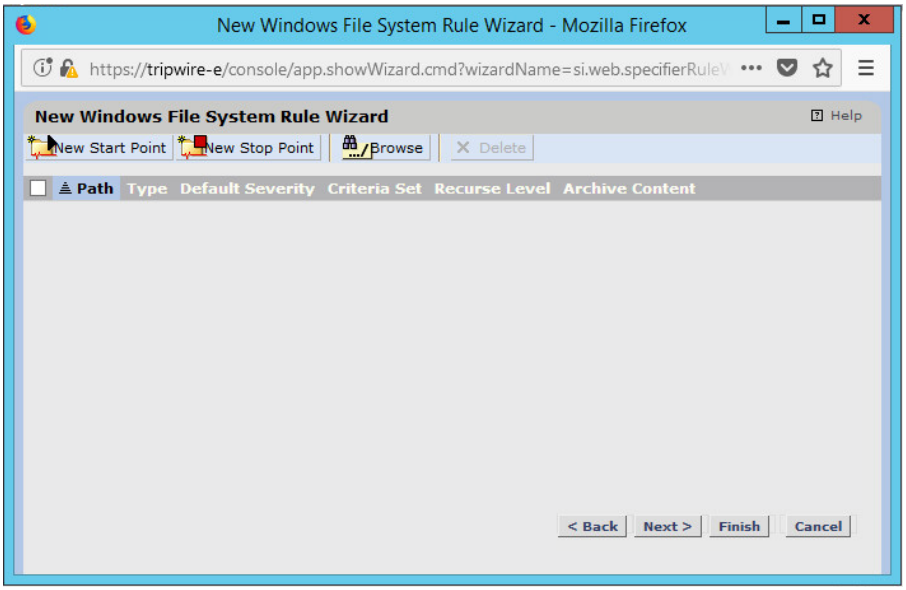
3. Click **New Rule.**
4. Select the type of rule. For monitoring Windows filesystems, we choose **Windows File System Rule.**



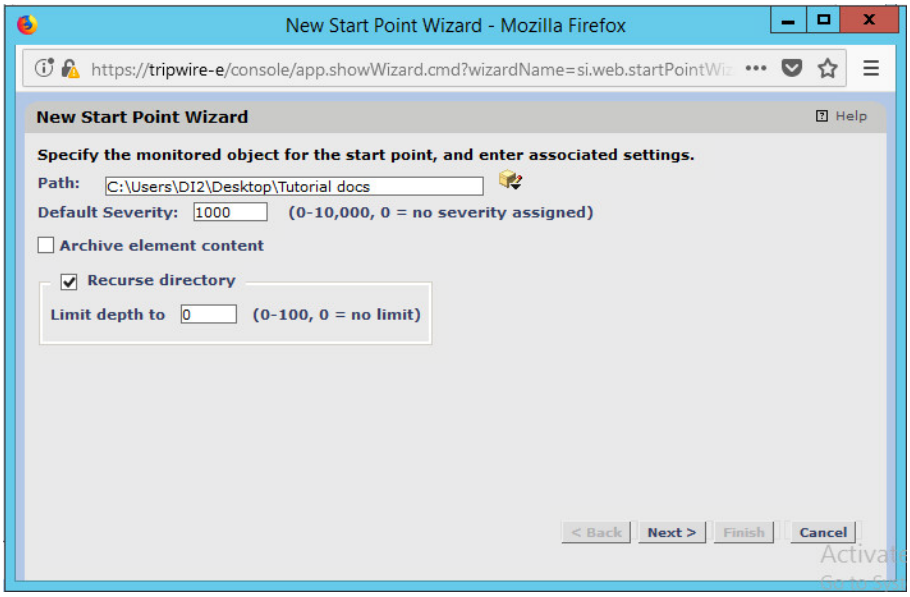
5. Click **OK.**
6. Enter a **name** and **description** for the rule.



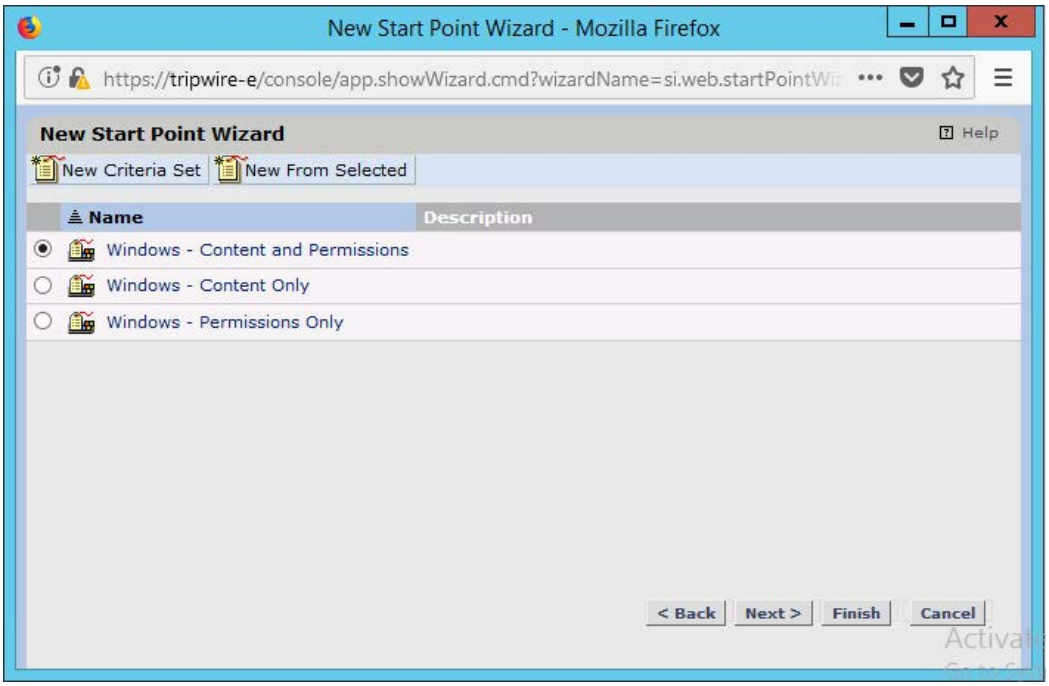
7. Click **Next.**



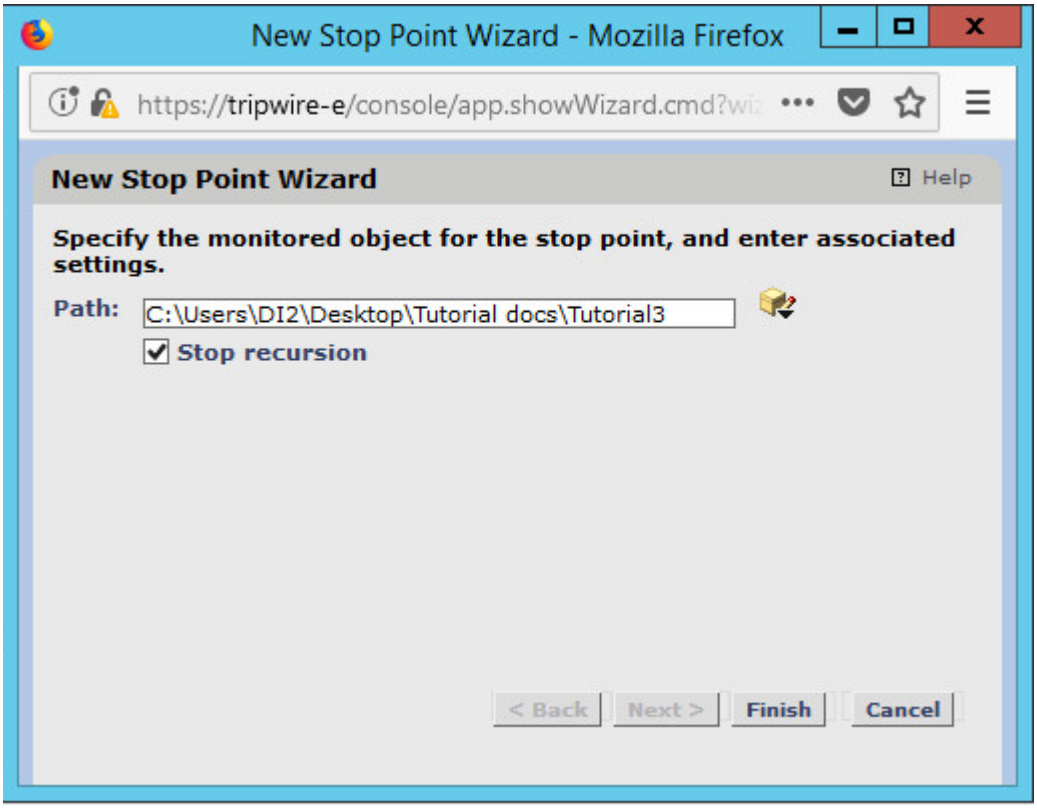
8. Click **New Start Point.**
9. For **Path**, enter a directory that represents the scope of the scan. It can be limited to the documents folder or be wide enough to encompass all the files on a system. Note that the latter will take much longer to scan.
10. Check the box next to **Recurse directory** 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.



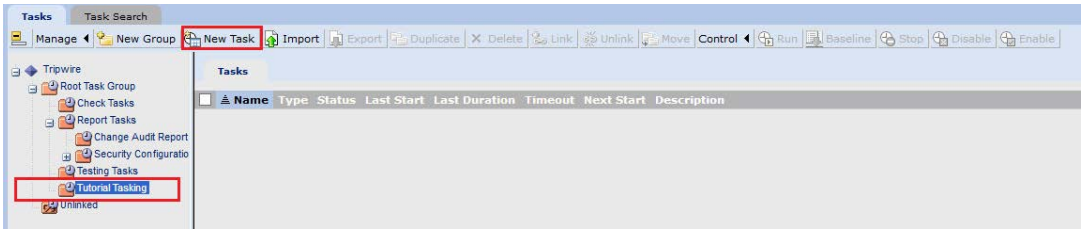
16. Click **Finish.**
17. Click **Next.**
18. Click **Next.**
19. Click **Finish.**

2.9.5.4 *Tasks*

This section will describe how to create a task.

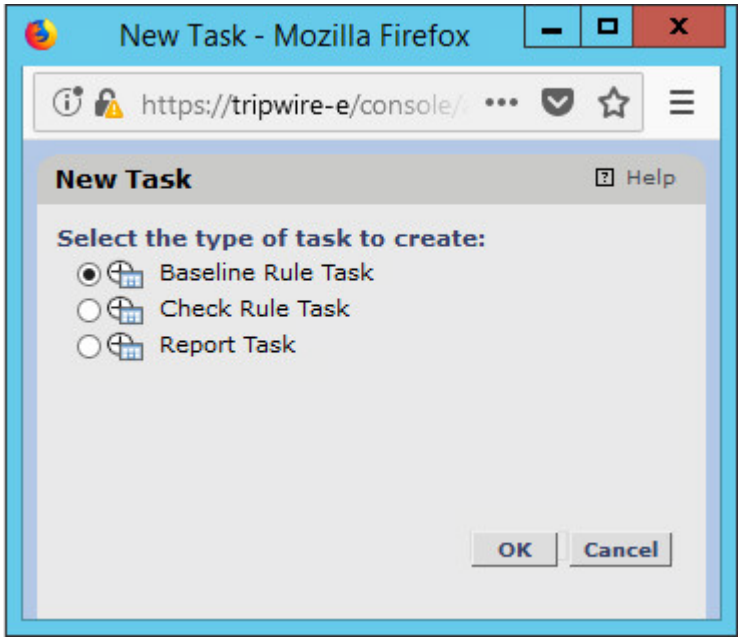
1. Click **Tasks.**

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

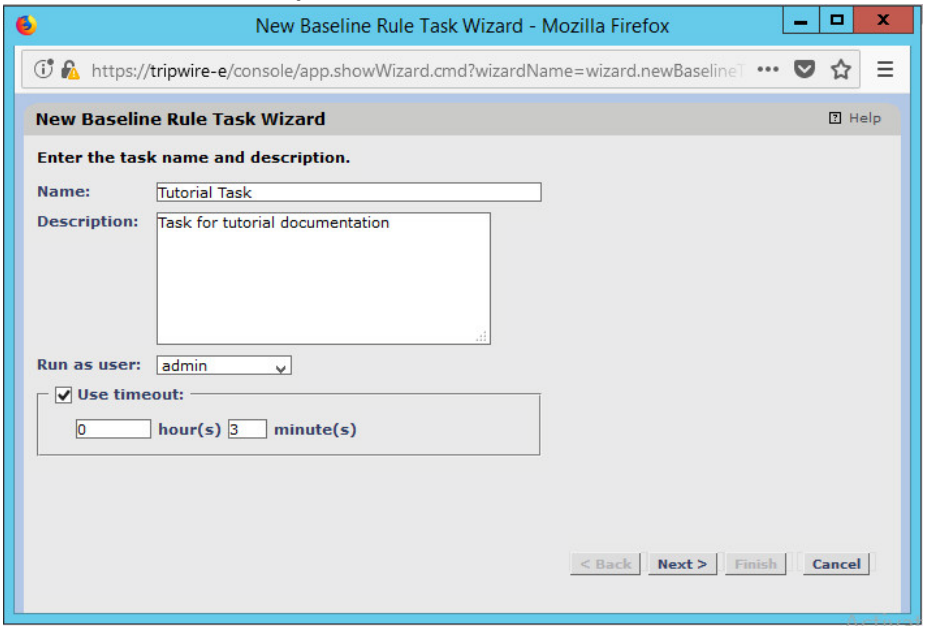


3. Click **New Task.**

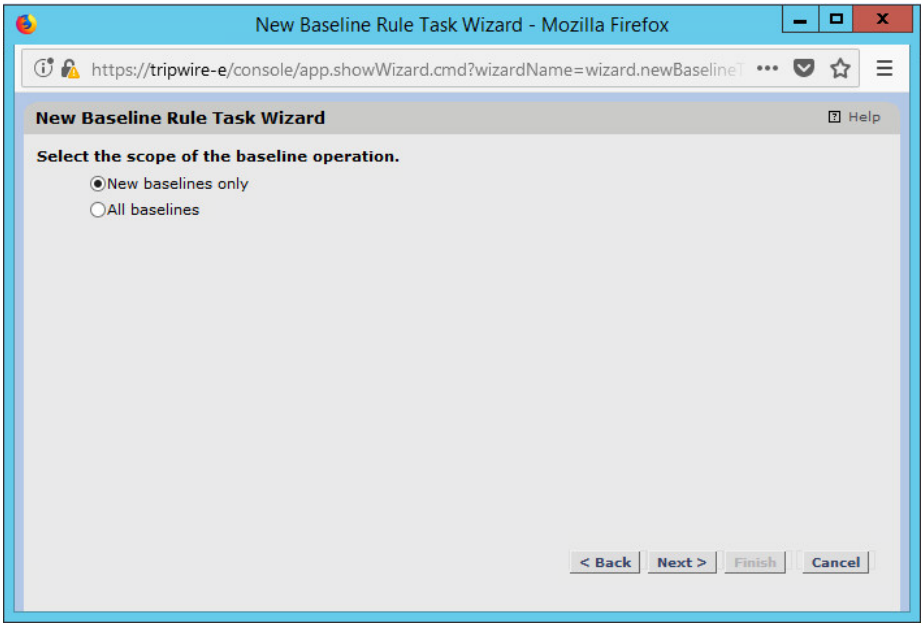
4. Select **Baseline Rule Task** or **Check Rule Task** (Note: Both are needed: baseline creates the initial state of the monitored object, and check updates the state and reports any changes).



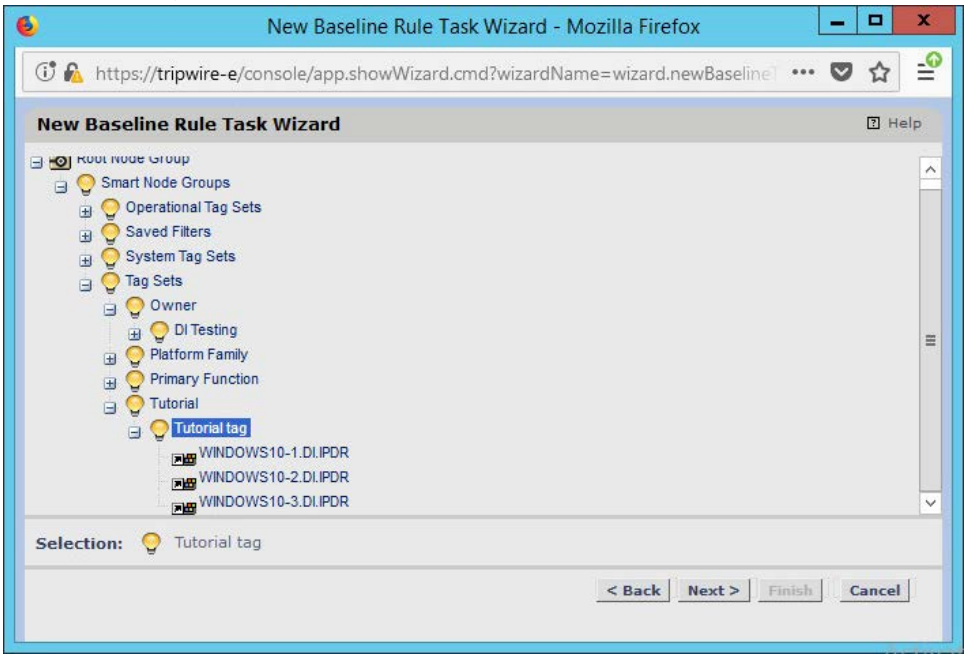
5. Click **OK.**
6. Enter a **name** and **description** for the task.



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

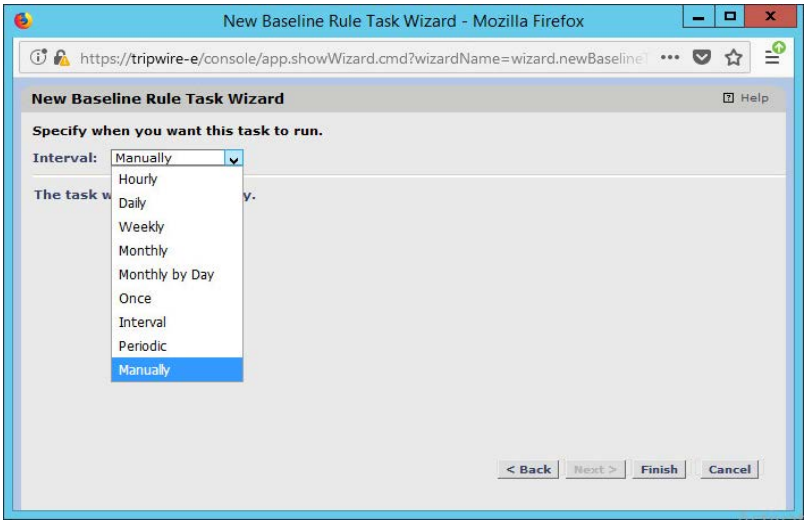


9. Click **Next.**
10. Select the systems to be included in the task. You can use tags or select by operating system (or other defaults).



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.**

2.10 Tripwire Log Center

2.10.1 Install Tripwire Log Center Manager

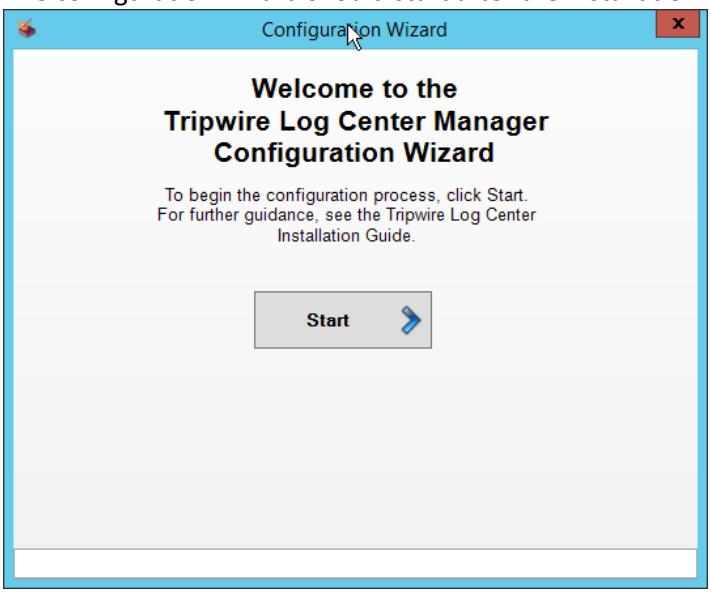
See the *Tripwire Log Center 7.3.1 Installation Guide* that should accompany the installation media for instructions on how to install **Tripwire Log Center.** Use the **Tripwire Log Center Manager** installer.

Notes:

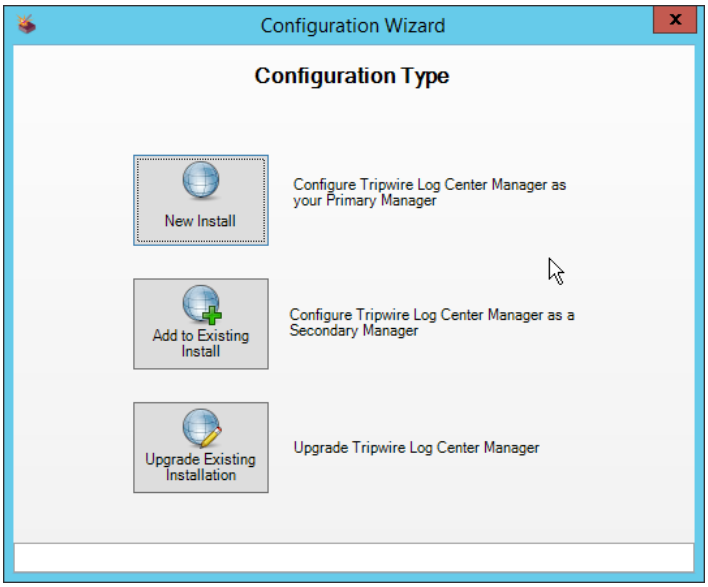
a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise.**
b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
c. .NET Framework 3.5 is required for this installation; install this from the Server Manager.
d. You may need to unblock port **9898** on your firewall for the TE 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).

2.10.2 Configure Tripwire Log Center Manager

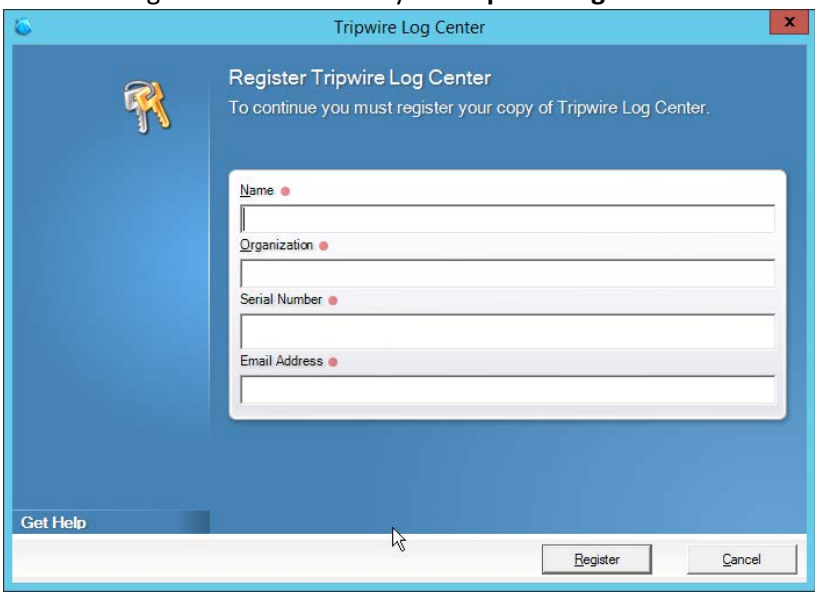
1. The configuration wizard should start after the installation is complete.



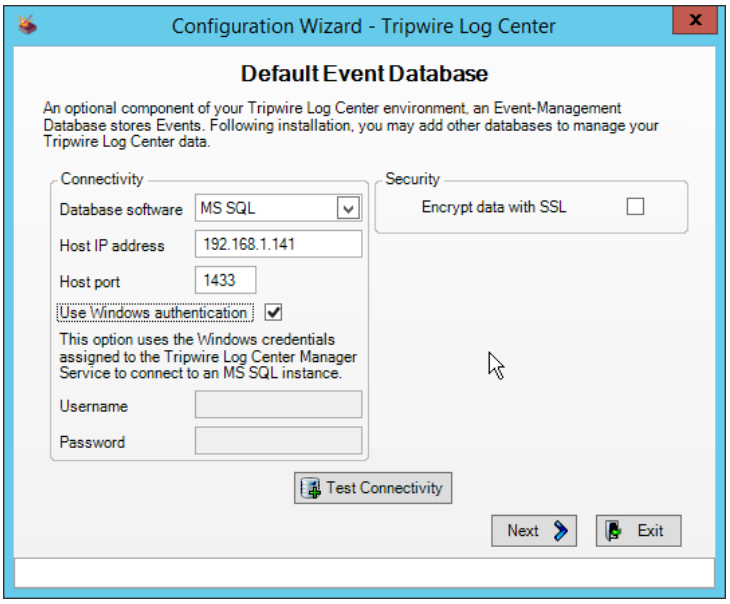
2. Click **Start.**



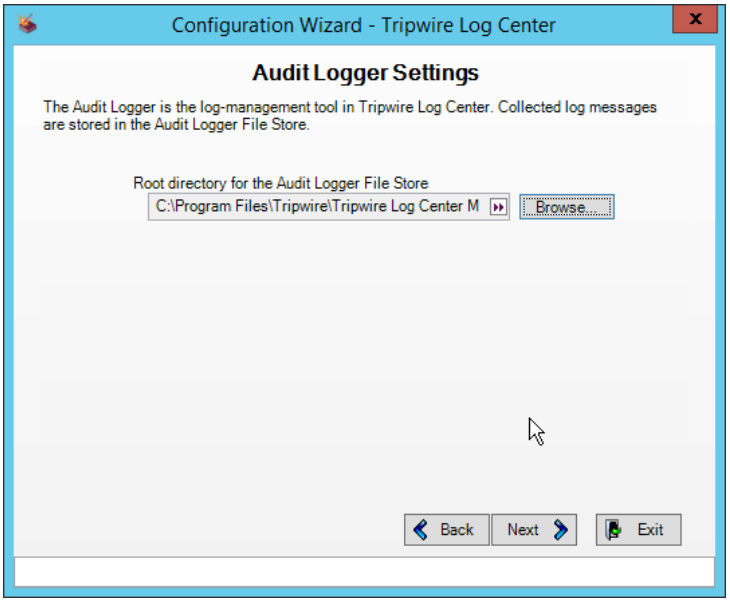
3. Click **New Install.**
4. Enter the registration details for your **Tripwire Log Center** license.



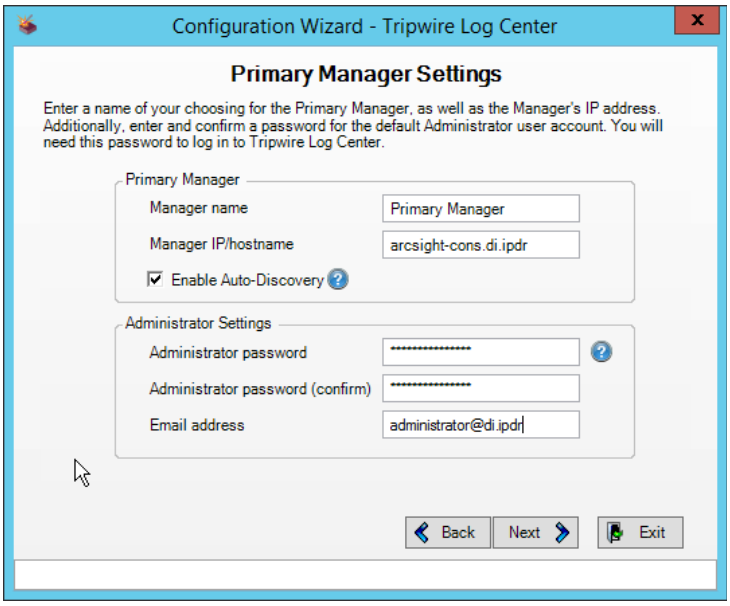
5. Click **Register.**
6. Enter details about the database that **Tripwire Log Center** should use.



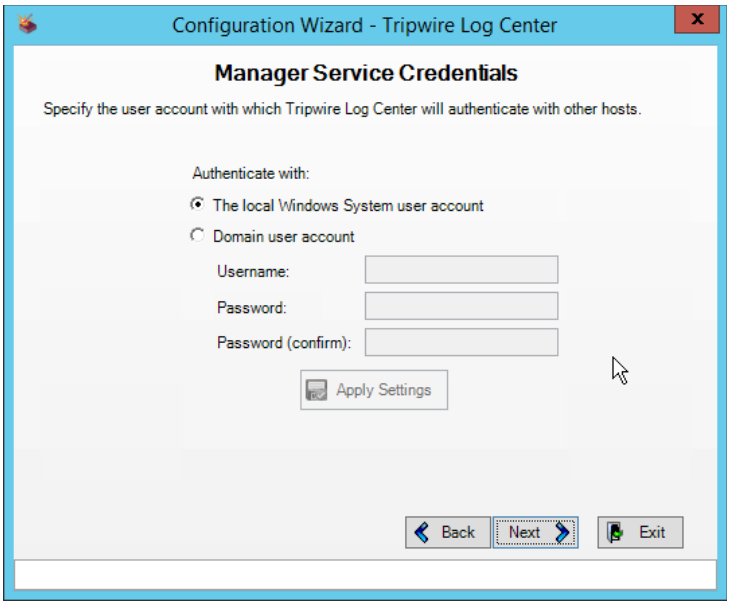
7. Click **Next.**
8. Select a directory to store log messages in, such as *C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT.*



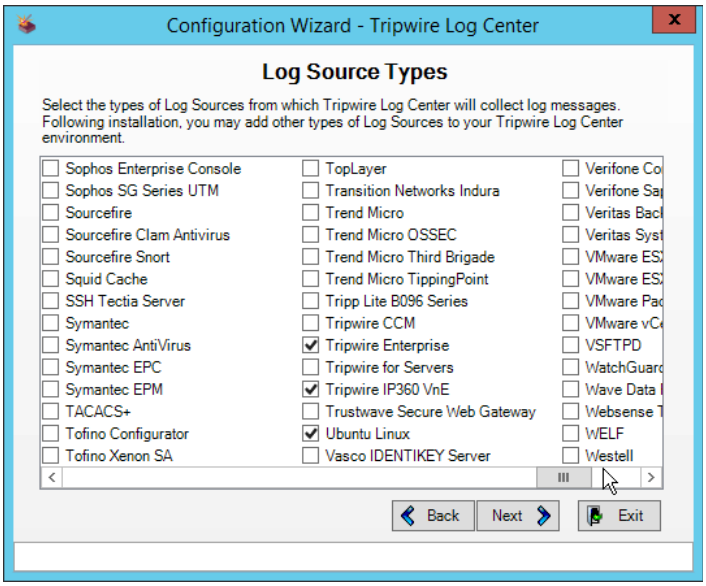
9. Click **Next.**
10. Enter a **password** and an **email**.
11. Change the IP to a hostname, if preferred.



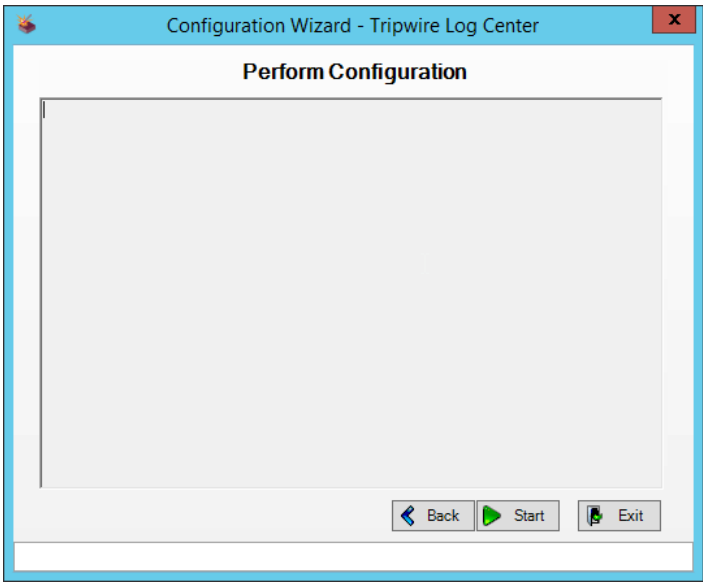
12. Click **Next.**



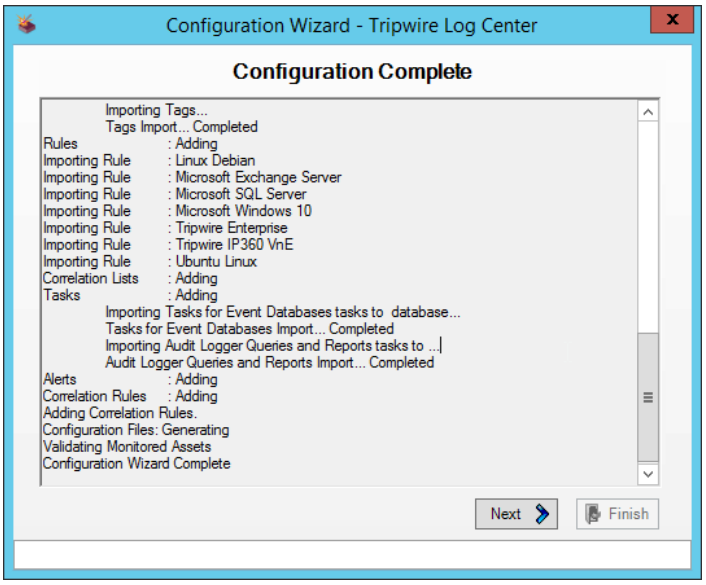
13. Click **Next.**
14. Select any log sources that you expect to collect with **Tripwire Log Center.** Examples: **Tripwire Enterprise, Microsoft Windows 10, Tripwire IP360 VnE, Linux Debian, Ubuntu Linux, Microsoft Exchange, Microsoft SQL Server.**



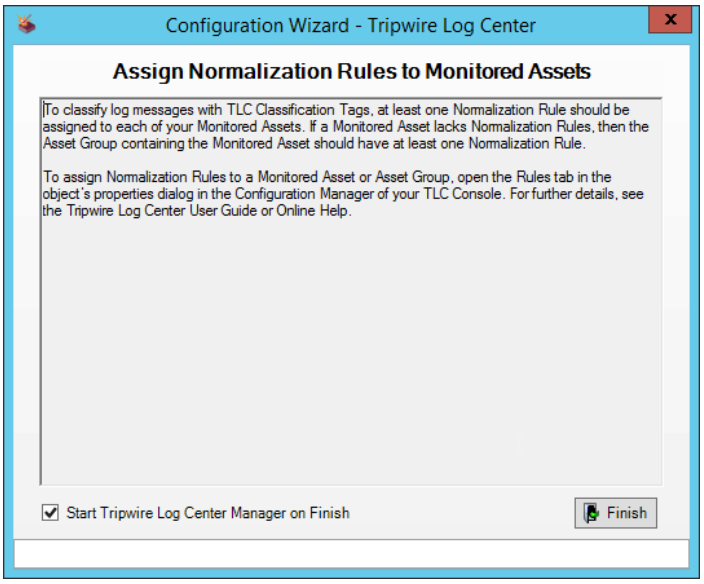
1787
1788 15. Click **Next.**



1789
1790 16. Click **Start.**



17. Click **Next.**



18. Click **Finish.**

2.10.3 Install Tripwire Log Center Console

Chapter 4 of the *Tripwire Log Center 7.3.1 Installation Guide* details the 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.

2.11 Cisco Identity Services Engine

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

2.11.1 Initial Setup

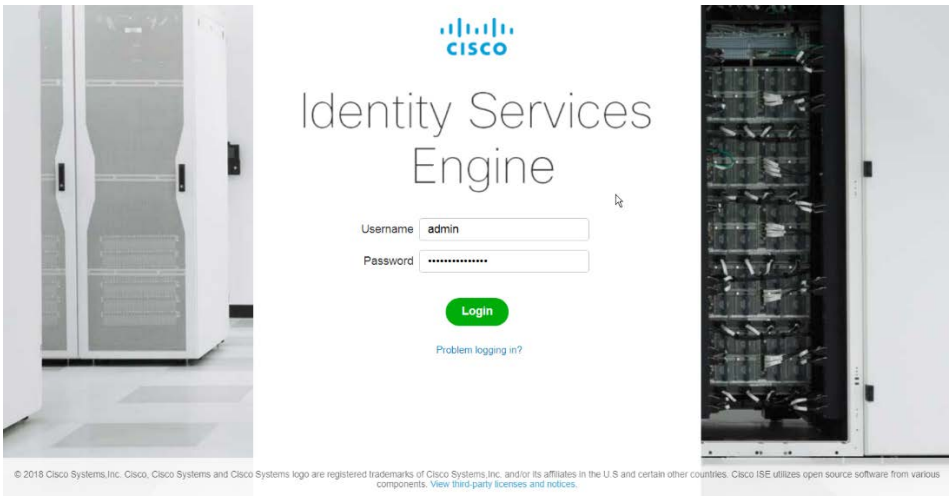
1. When prompted to log in for the first time, enter **`setup`**. (You can use the command **`reset-config`** to change these values later.)
2. Enter the desired **hostname** for the machine.
3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated with this 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 an **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.

2.11.2 Inventory: Configure SNMP on Routers/Network Devices

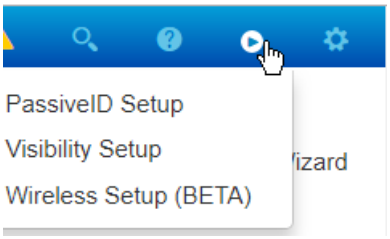
See the corresponding vendor documentation for the correct way to enable SNMP on your network device. Ensure that the community string you choose is considered sensitive, like a password.

2.11.3 Inventory: Configure Device Detection

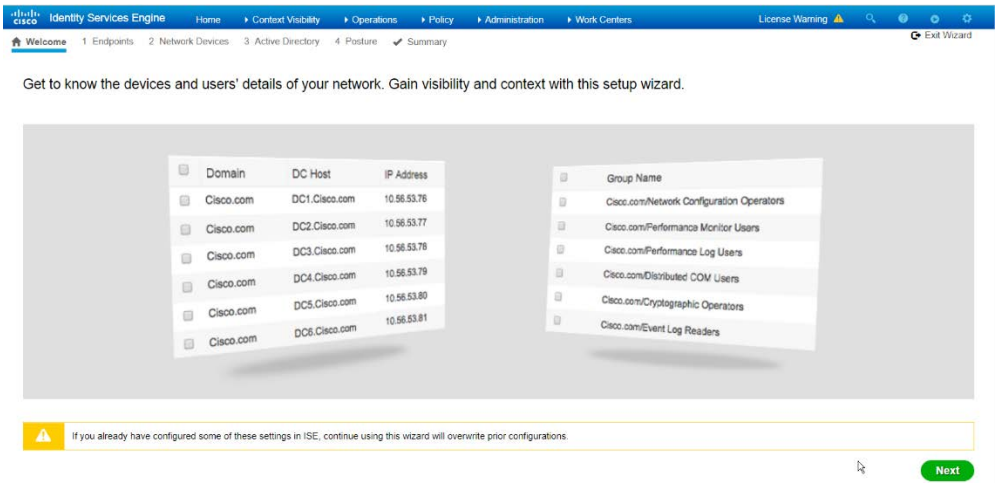
1. Log in to the web client by visiting https://hostname/admin, but replace **hostname** with the hostname of the ISE machine.



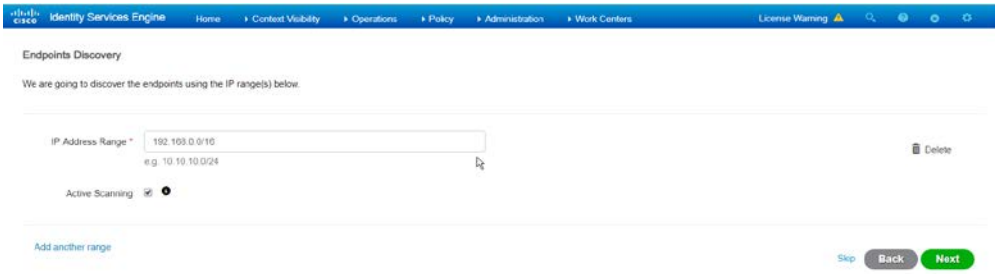
2. On the top right, use the small play button to select **Visibility Setup.**



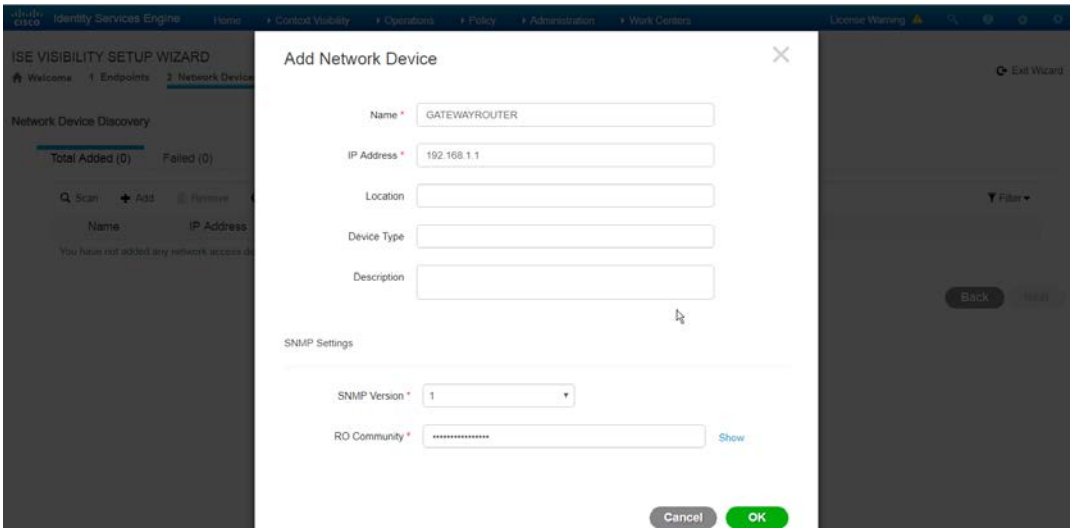
3. Click **Next.**



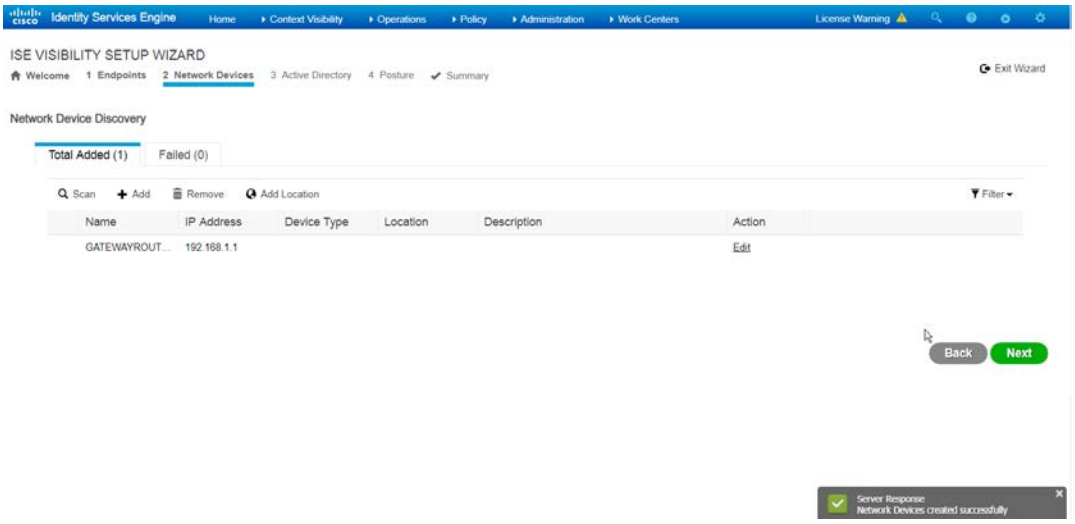
4. Enter the range of IP addresses to add to ISE's inventory.
5. Ensure that **Active Scanning** is checked.



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.**



1840

1841 13. Click **Next.**

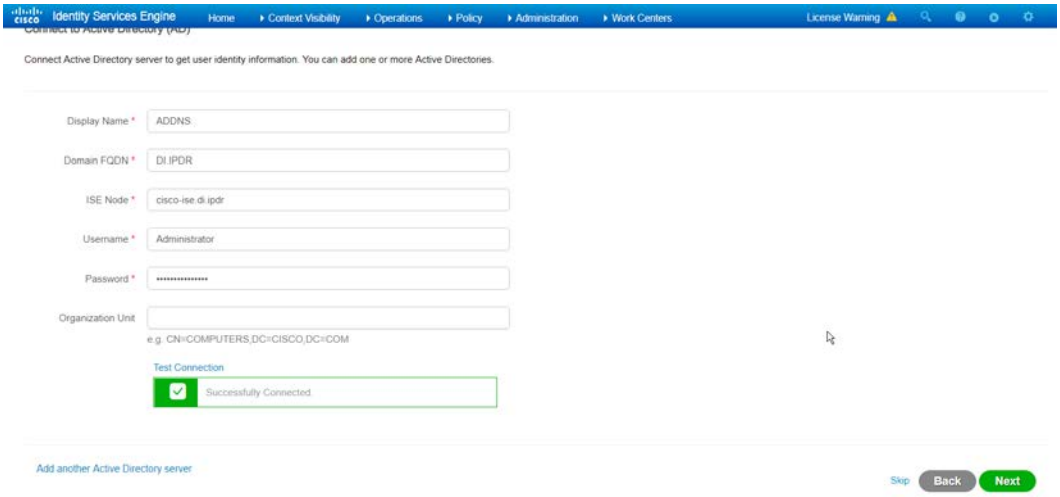
1842 14. Enter a **display name.**

1843 15. Enter the **domain name.**

1844 16. Enter the **hostname** of **Cisco ISE.**

1845 17. Enter a **username** and **password.**

1846 18. Click **Test Connection** to ensure that this works.



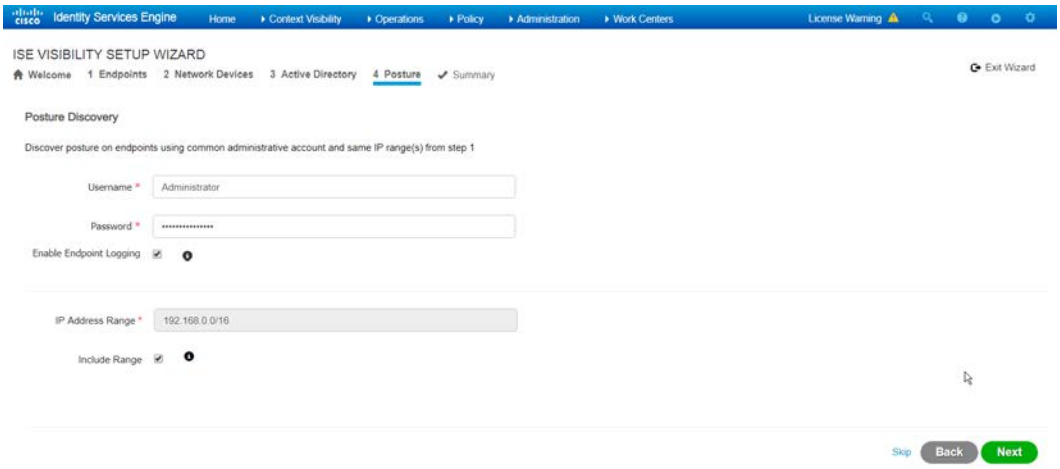
1847

1848 19. Click **Next.**

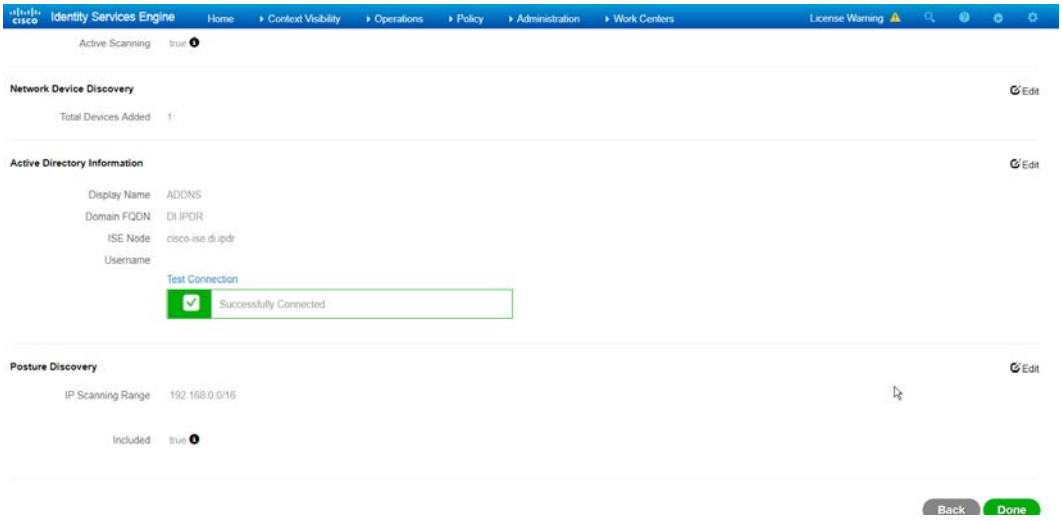
1849 20. Enter a **username** and **password.**

1850 21. Check the box next to **Enable Endpoint Logging.**

1851 22. Check the box next to **Include Range.**



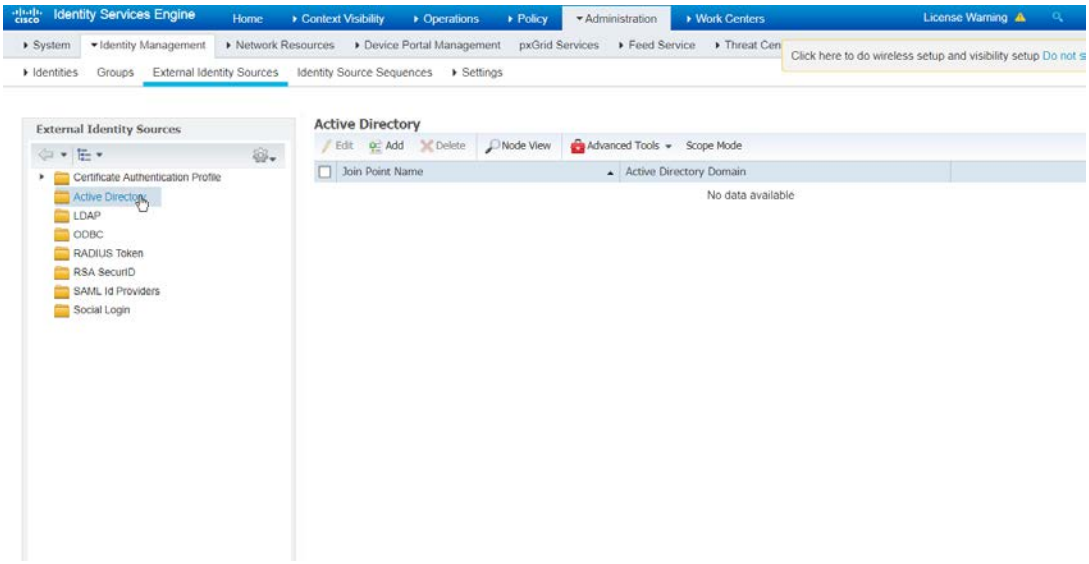
23. Click **Next.**



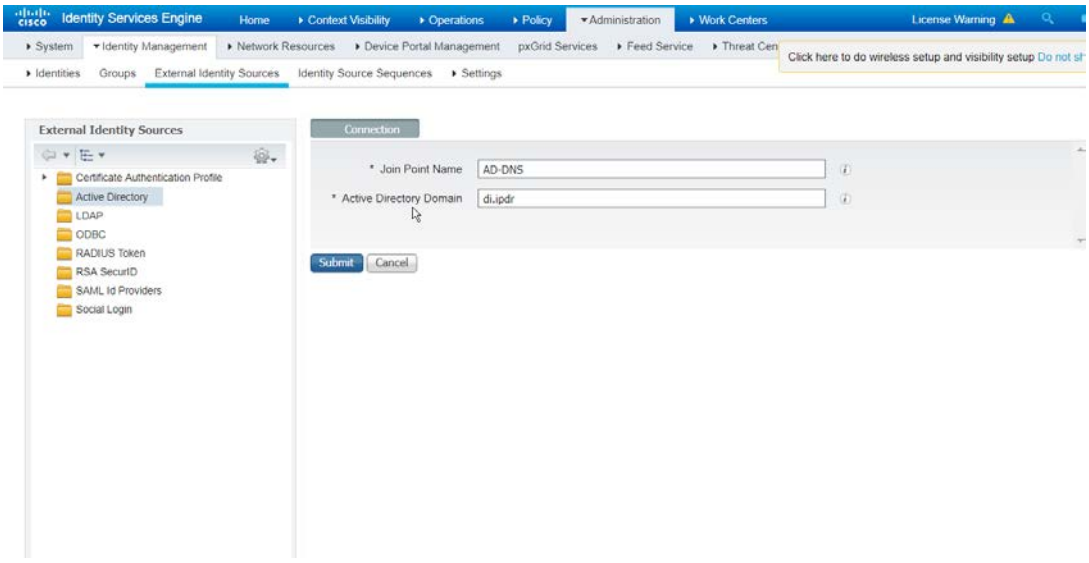
24. Verify the settings, and click **Done.** (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

2.11.4 Policy Enforcement: Configure Active Directory Integration

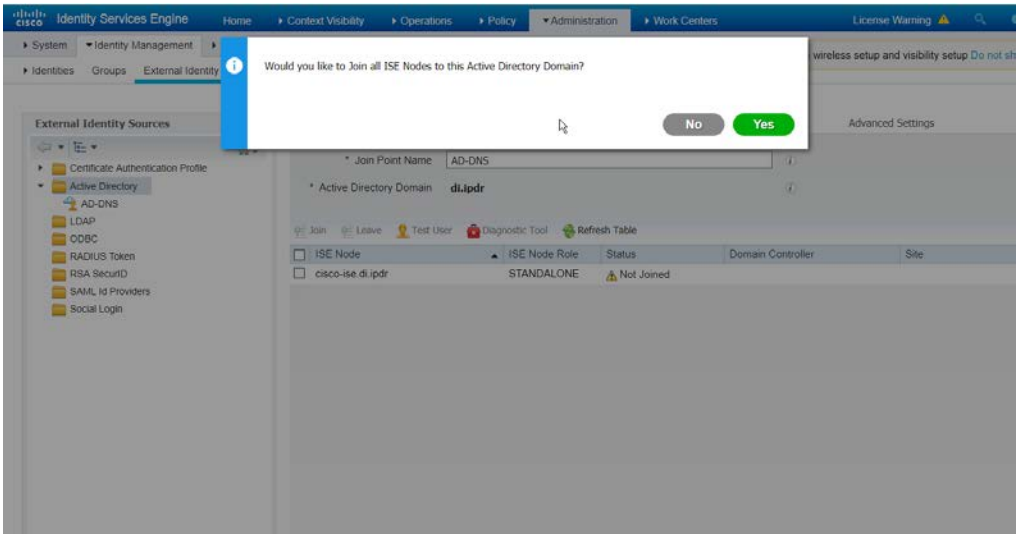
1. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory.*



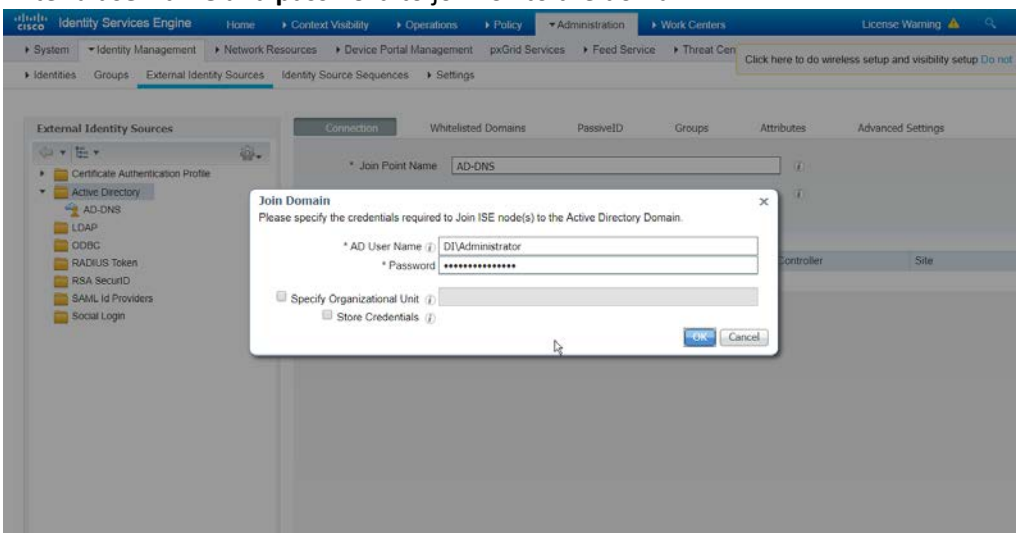
1860
1861 2. Click **Add.**
1862 3. Enter a **name.**
1863 4. Enter the **domain.**



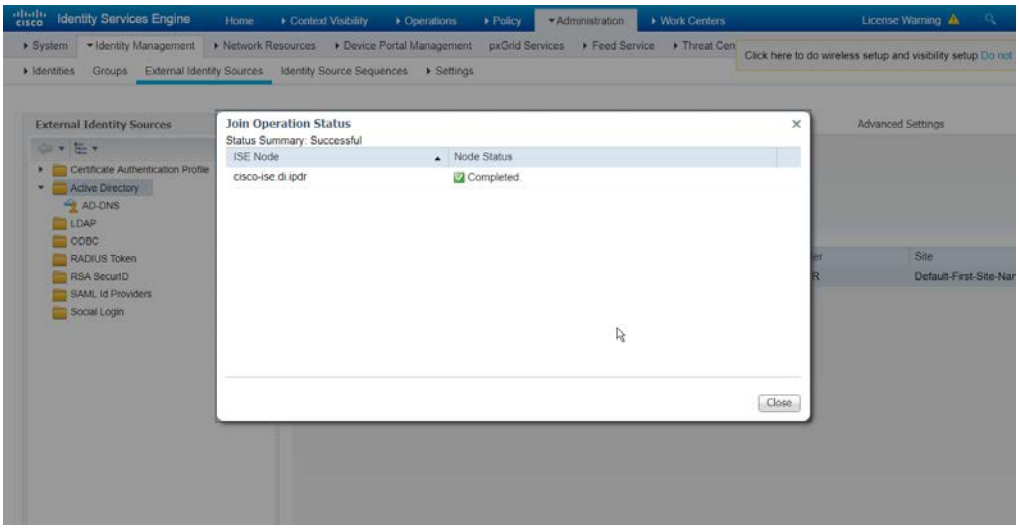
1864
1865 5. Click **Submit.**



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



8. Click **OK.**

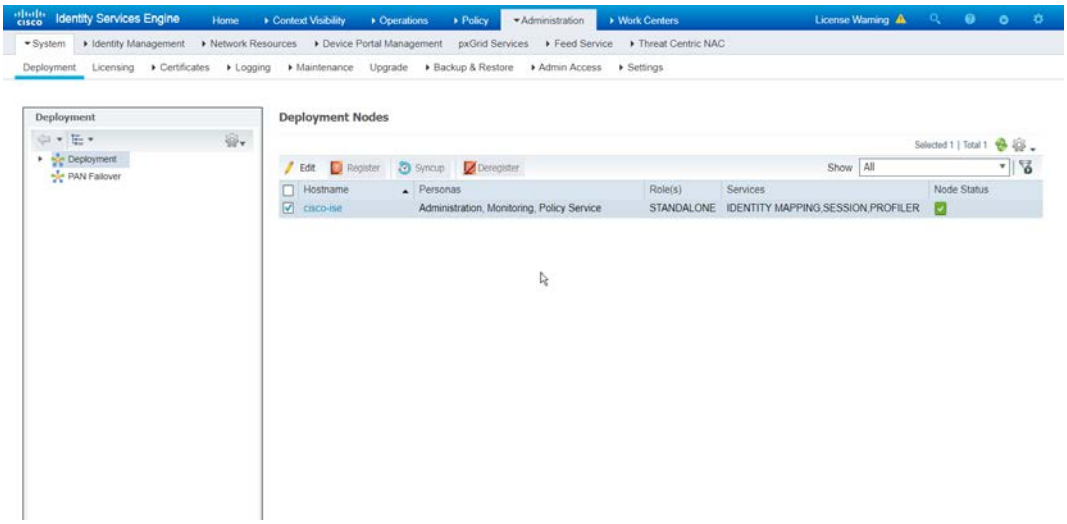


9. Click **Close** when the join is finished.

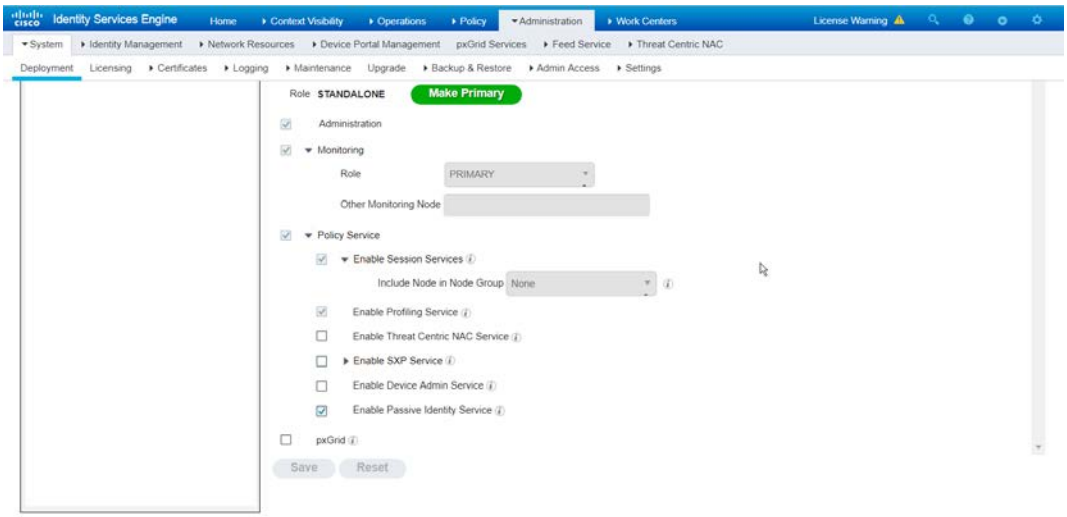
2.11.5 Policy Enforcement: Enable Passive Identity with AD

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.

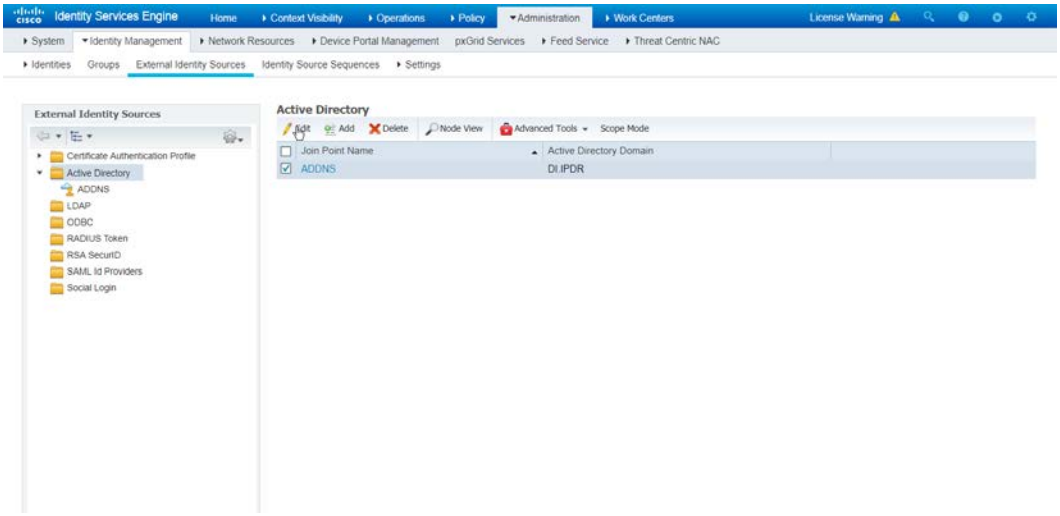
1. Navigate to **Administration > System > Deployment.**
2. Check the box next to **ISE.**



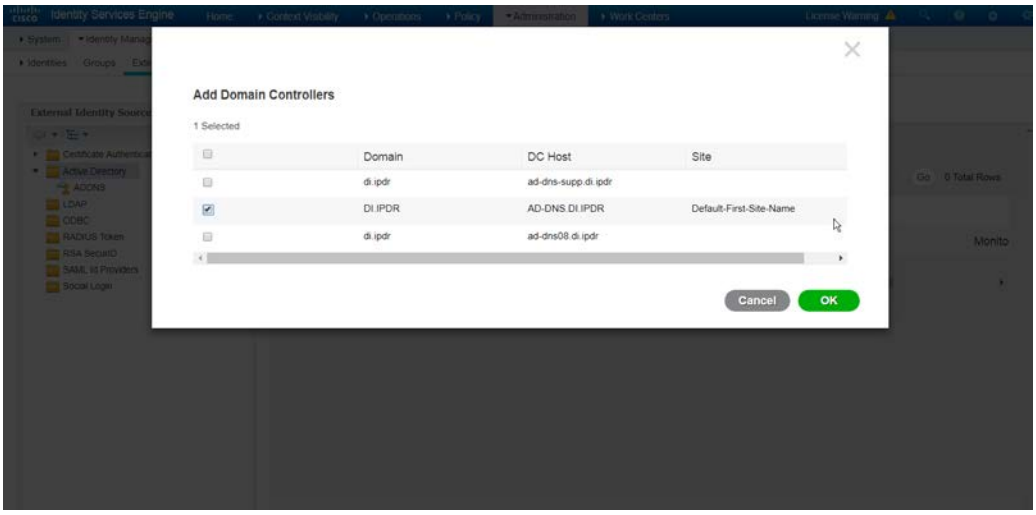
3. Click **Edit.**
4. Check the box next to **Enable Passive Identity Service.**



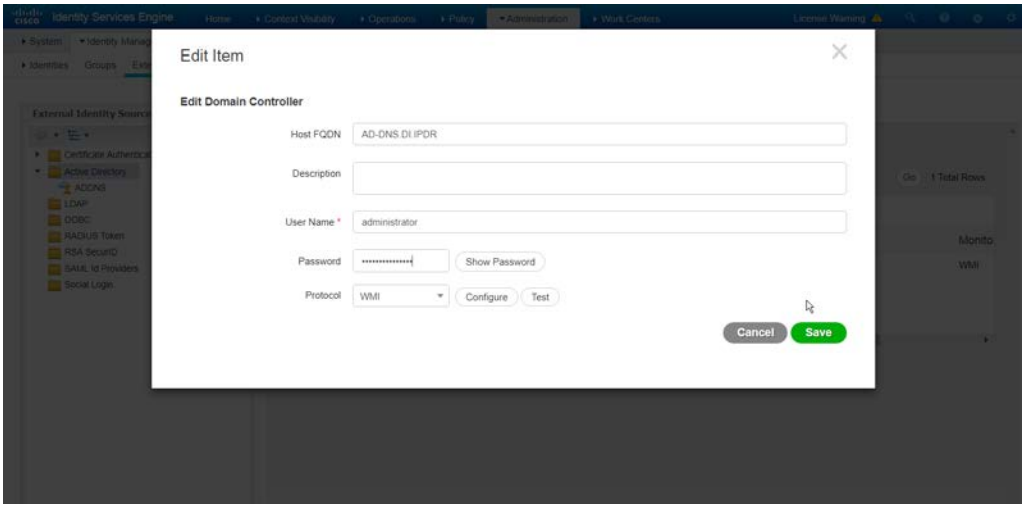
5. Click **Save.**
6. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory.*
7. Click the name of the Active Directory machine.
8. Check the box next to the join point you just created.



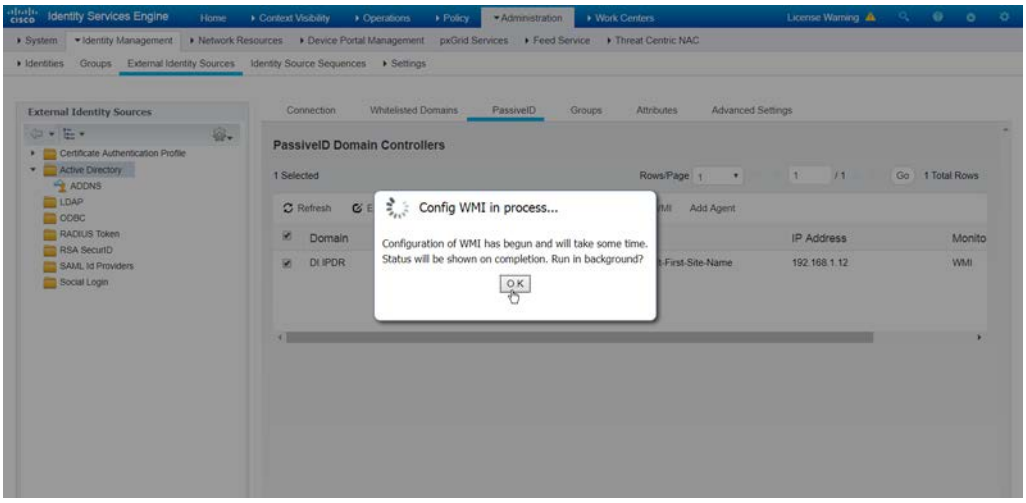
9. Click **Edit.**
10. Click the **PassiveID** tab.
11. Click **Add DCs** if there are no domain controllers listed.



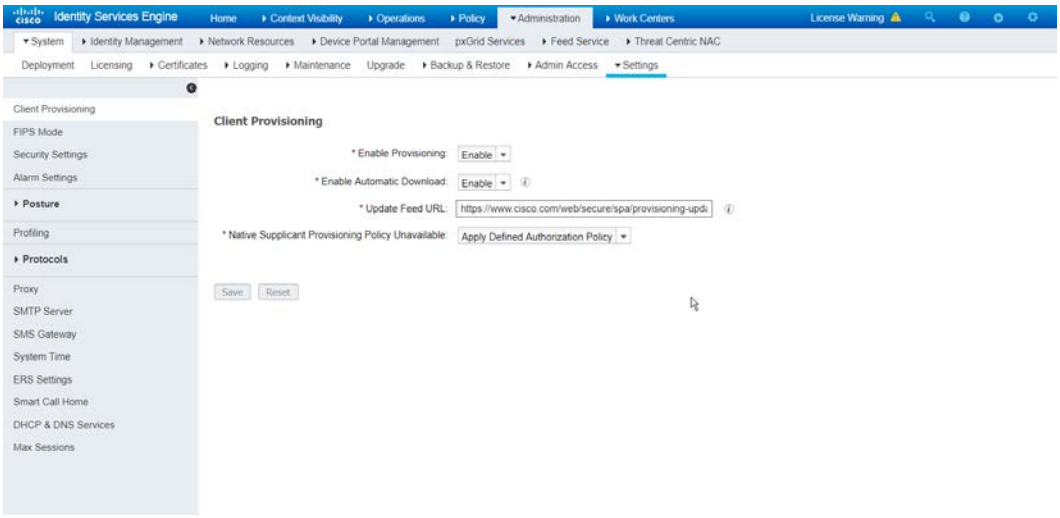
12. Select the Active Directory domain controller.
13. Click **OK.**
14. Check the box next to the selected domain controller.
15. Click **Edit.**
16. Enter credentials for an administrator account.



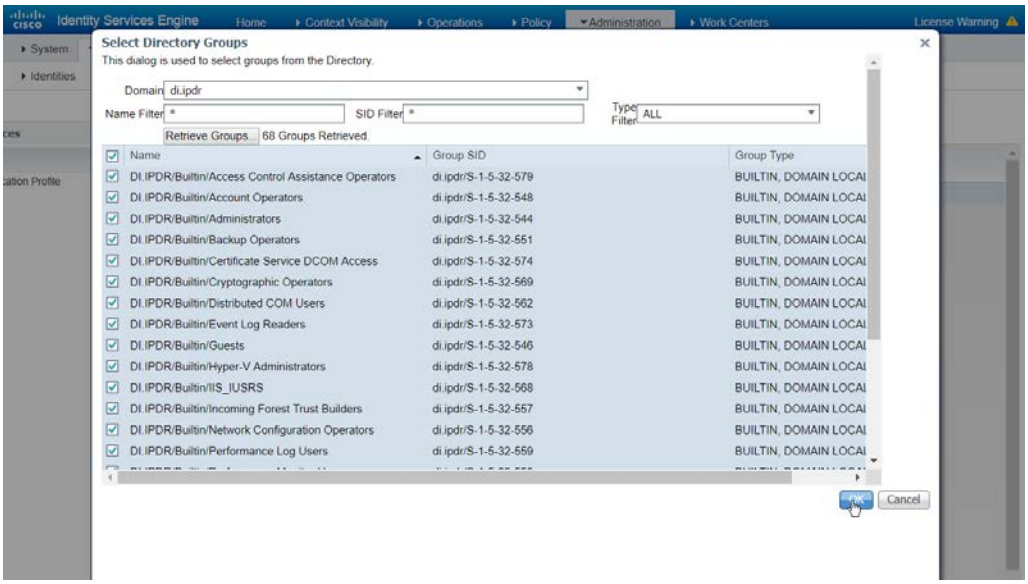
17. Click **Save.**
18. Click **Config WMI.**
19. Click **OK.**



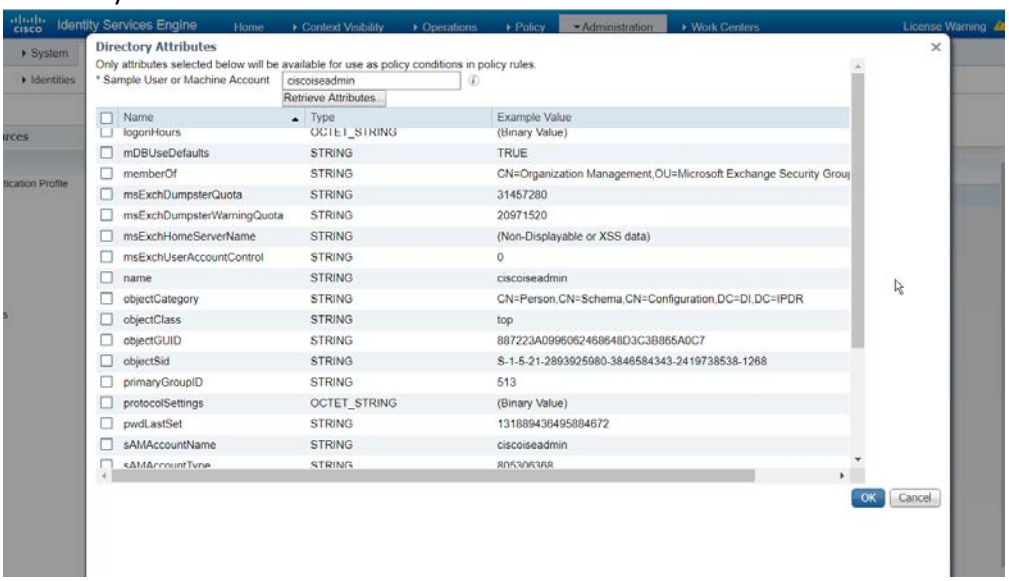
20. Click **OK** when this configuration finishes.
21. Navigate to *Administration > System > Settings > Client Provisioning.*
22. Set Enable **Automatic Download** to **Enable.**



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.

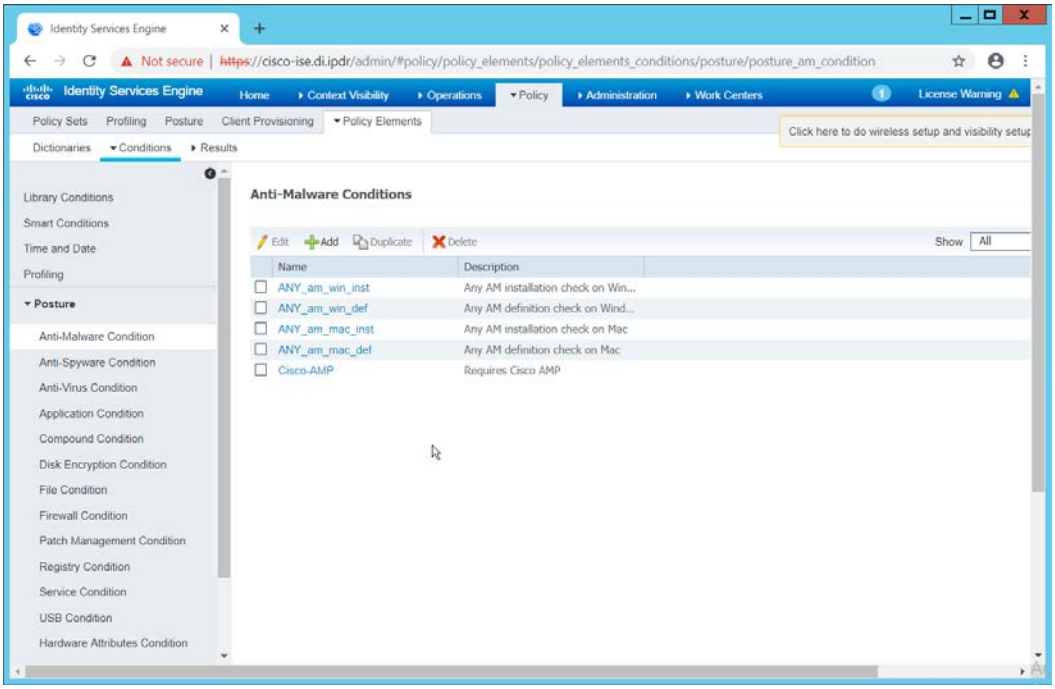


36. Click **OK.**

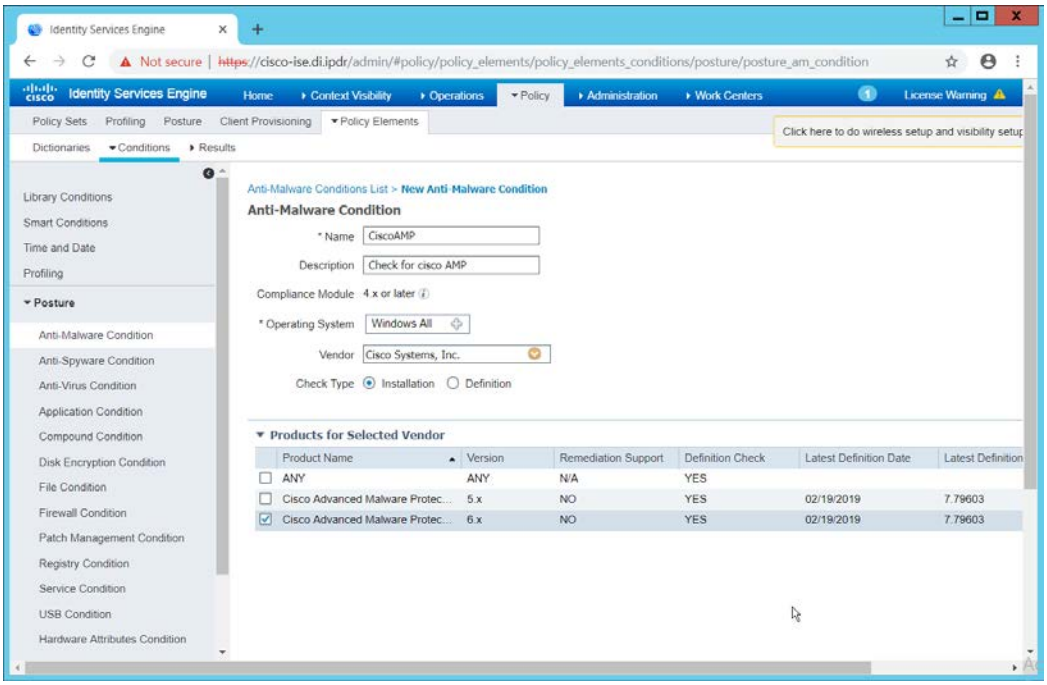
37. Click **Save.**

2.11.6 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. Furthermore, the 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.**



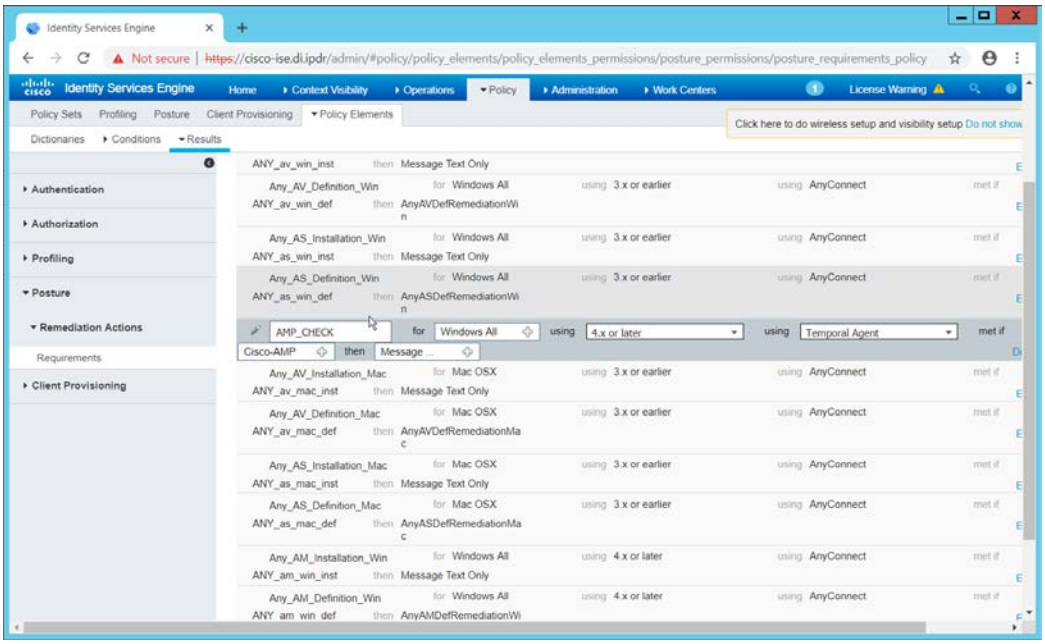
4. Click **Add.**
5. Enter a **name.**
6. Enter a **description** if desired.
7. Select **Windows All** for **Operating System.**
8. Select **Cisco Systems, Inc.** for **Vendor.**
9. Under **Products for Selected Vendor,** check the box next to **Cisco Advanced Malware Protection,** with the version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



10. Click **Submit.**

2.11.7 Policy Enforcement: Developing Policy Results

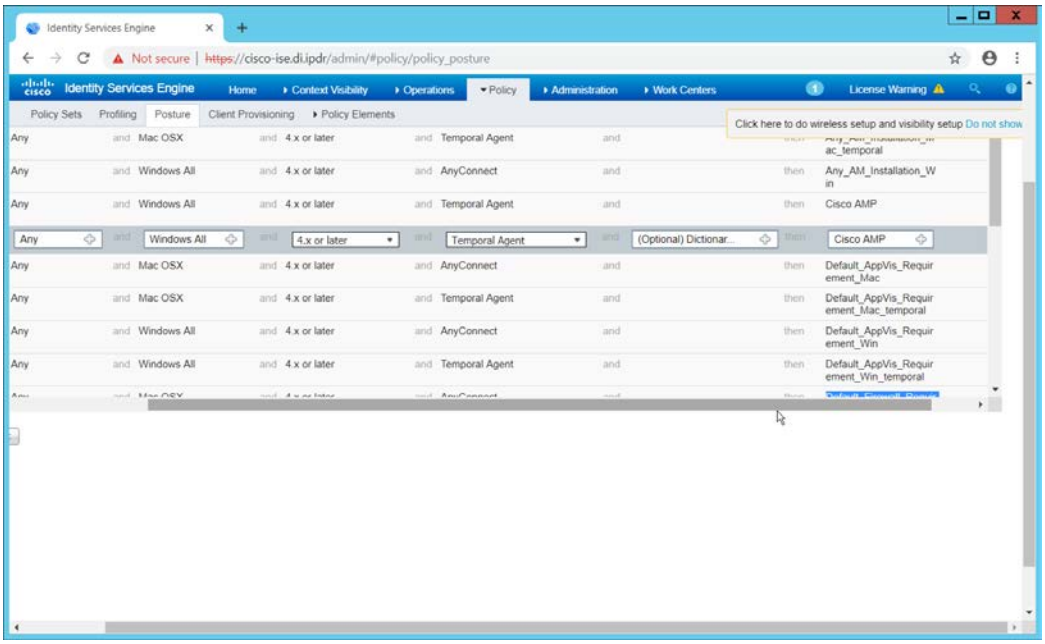
1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements.**
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement.**
3. Enter a **name.**
4. Select **Windows All** for **Operating Systems.**
5. Select **4.x or later** for **Compliance Module.**
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 no option for Cisco AMP to be installed, so we leave the default for now.)
9. Enter a **Message** to show to the user to inform them that they must install Cisco AMP.



10. Click **Save.**

2.11.8 Policy Enforcement: Enforcing a Requirement in Policy

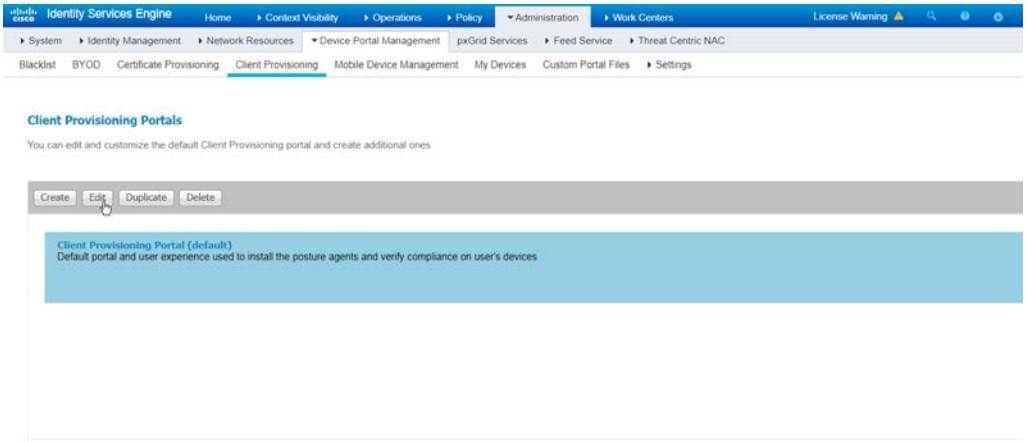
1. Navigate to **Policy > Posture.**
2. Click one of the black arrows next to the **Edit** link and select **Insert New Policy.**
3. Enter a **name.**
4. Select **Windows All** for **Operating Systems.**
5. Select **4.x or later** for **Compliance Module.**
6. Select **Temporal Agent** for **Posture 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.

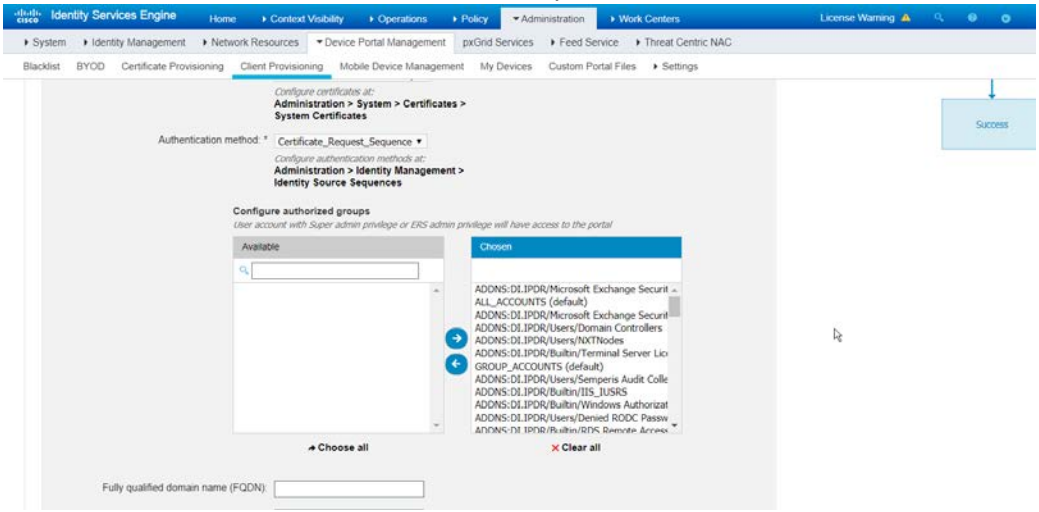
2.11.9 Policy Enforcement: Configuring a Web Portal

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.**

2.11.10 Configuring RADIUS with your Network Device

Cisco ISE requires a 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 OS and may contain requirements such as the 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 between machines, but the overall requirements have commonalities between systems.

1. 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.**
    a. 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."
2. 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,

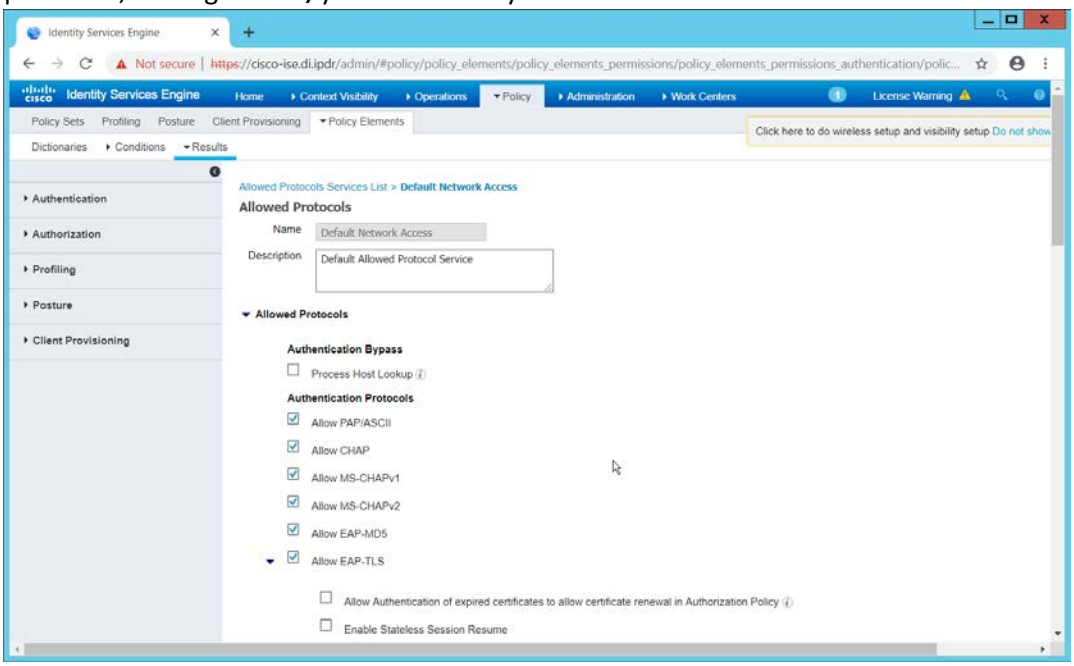
and it will not be in the web browser. Windows has a built-in **802.1x** client that can be configured on Network adapters under the **Authentication** tab. To enable it, you must first start the service **Wired AutoConfig,** and then the **Authentication** tab will become available for configuration.

c. Whichever form of **802.1x** is chosen, the request for authentication must be forwarded to Cisco ISE. Cisco ISE will process the request for authentication.

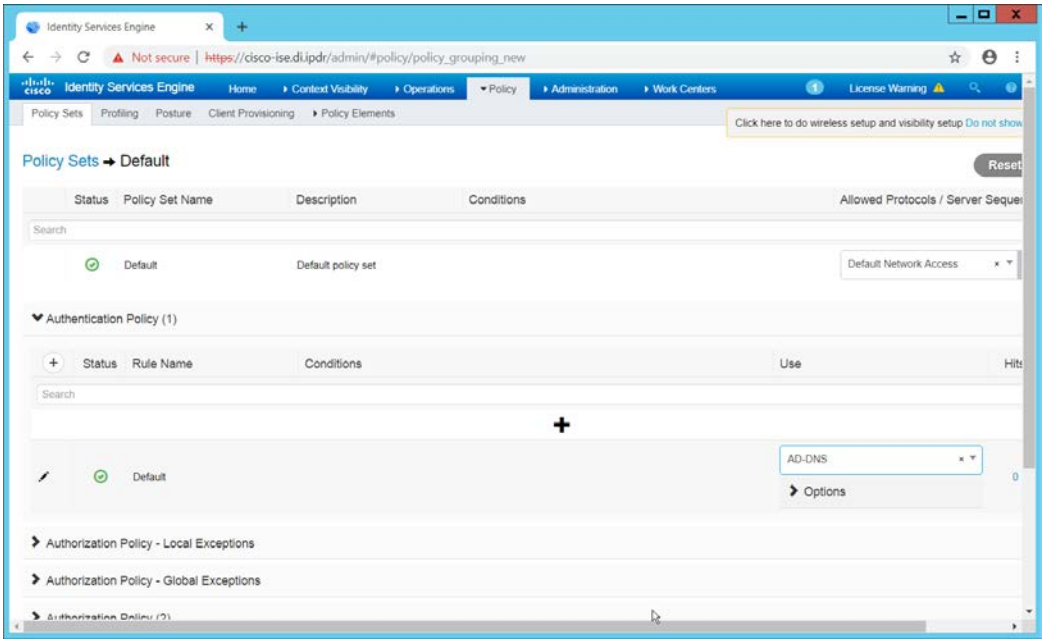
3. The two steps above detail the **authentication** phase. Once authenticated, the network device must redirect the user to the client provisioning portal (or to a guest portal), depending on the setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.
4. The user will 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.
5. 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.**

2.11.11 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 any protocols that need to be supported for your network setup are allowed. In particular, if using **802.1x,** you should likely 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.

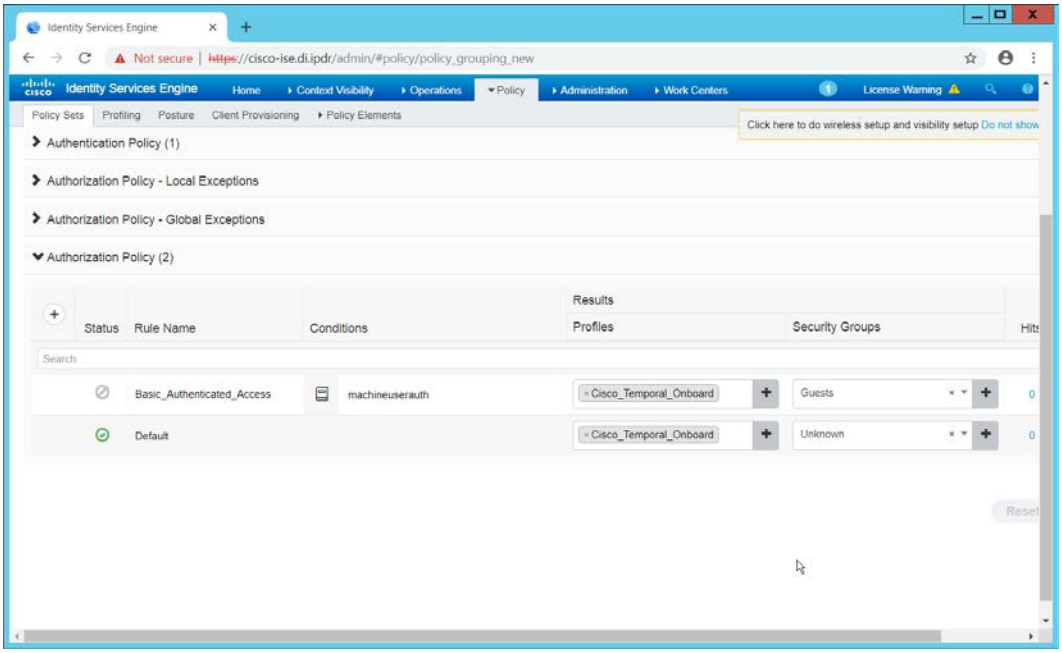


9. Click **Save.**

2.11.12 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 only happen 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 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.**

2.12 Cisco Advanced Malware Protection

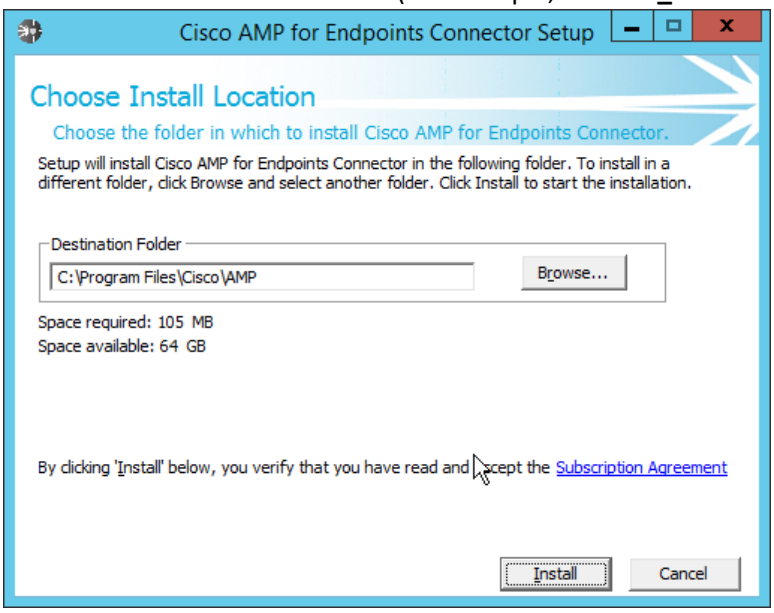
This section assumes the use of the Cisco Advanced Malware Protection (AMP) Console, a cloud-based server that connects to clients on individual machines. There is some configuration to be done on this cloud-based server, which may impact the installation. Cisco provides best practices guides online for AMP configuration. Here is a link to one such guide: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/213681-best-practices-for-amp-for-endpoint-excl.html.

2.12.1 Dashboard Configuration

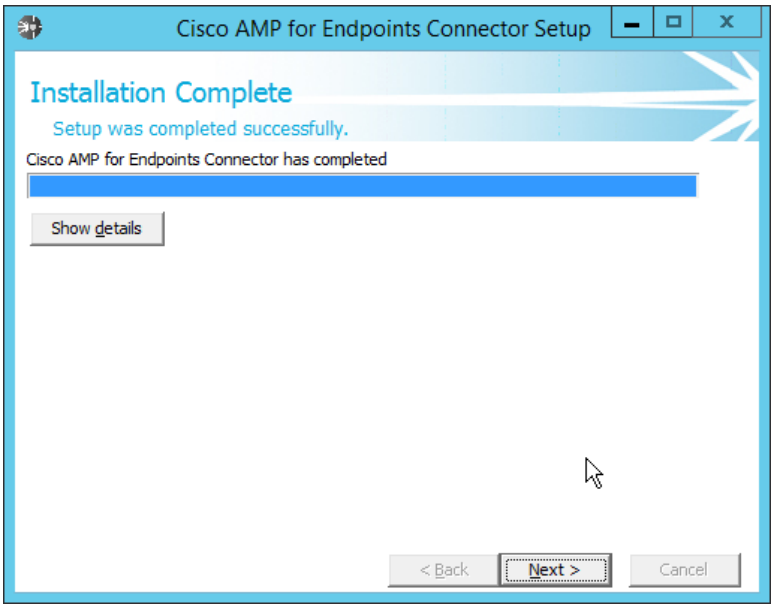
1. From the Cisco AMP dashboard, located at https://console.amp.cisco.com/dashboard, click **Set Up Windows Connector.**
2. The configuration of this will be different for each enterprise, so consult your Cisco representative for the proper way to set this up. For the purposes of this build, we accepted the default values.

2.12.2 Installing the Connector on a Windows Server

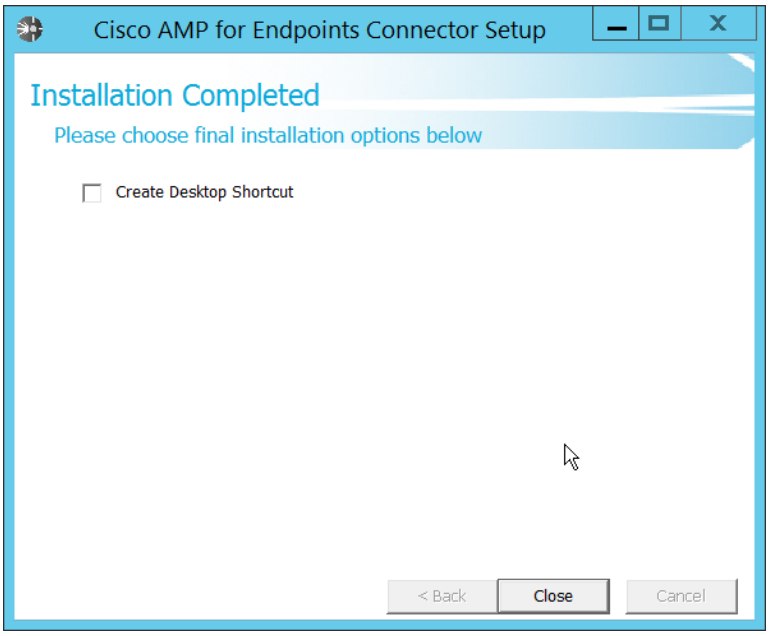
1. On the Cisco AMP dashboard, navigate to **Management > Download Connector.**
2. Select the AMP group in which to put the machine. For example, when installing on an Active Directory machine, we chose **Domain Controller.**
3. Find the correct OS version of the installer, and click **Download.**
4. Run the downloaded executable (for example, **Domain_Controller_FireAMPSetup.exe).**



5. Click **Install.**



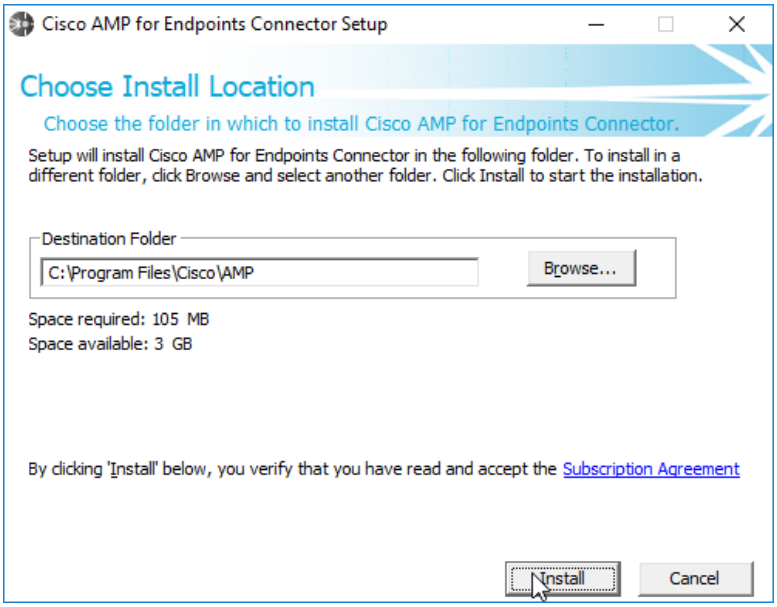
6. Click **Next.**



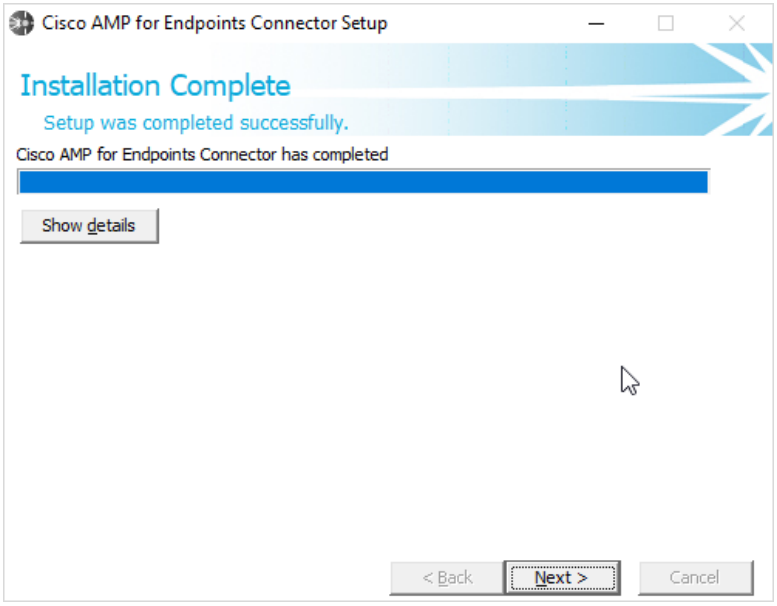
7. Click **Close.**

2.12.3 Installing the Connector on a Windows 10 Machine

1. On the Cisco AMP dashboard, navigate to **Management > Download Connector.**
2. Select the AMP group in which to put the machine. For this installation we chose **Protect.**
3. Find the correct OS version of the installer, and click **Download.**
4. Run the downloaded executable (for example, **Protect_FireAMPSetup.exe**).

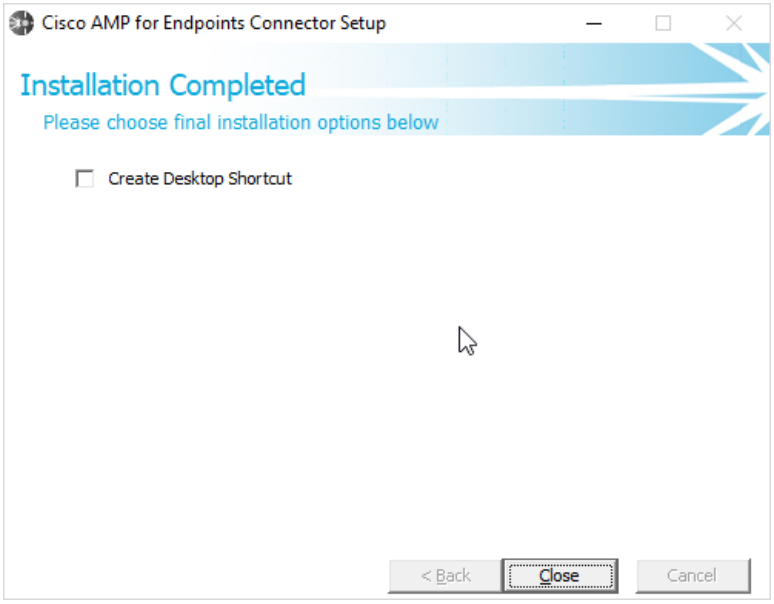


2085 5. Click **Install.**



2086

2087 6. Click **Next.**

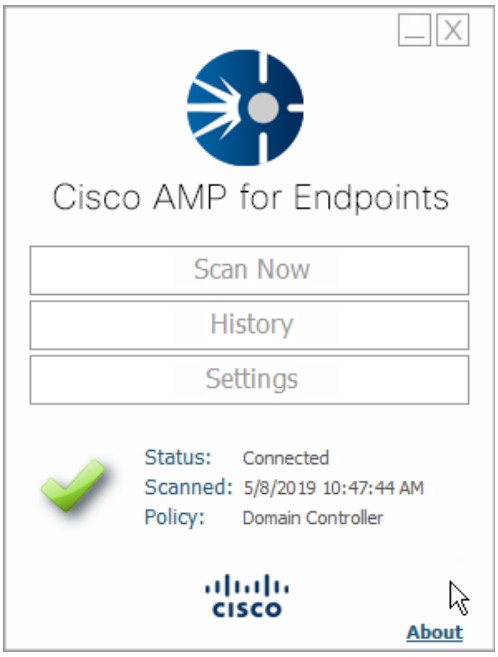


2088

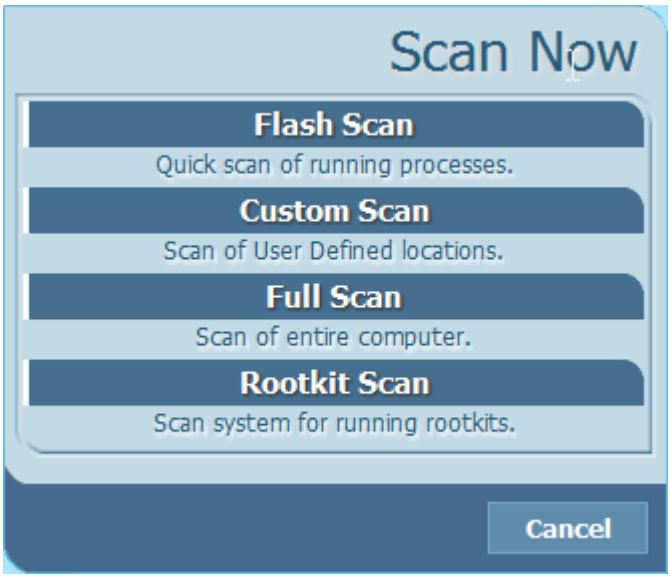
2089 7. Click **Close.**

2090 2.12.4 Scanning using AMP

2091 1. If the AMP software does not run automatically, open it from the **start** menu.



2. Click **Scan Now.**

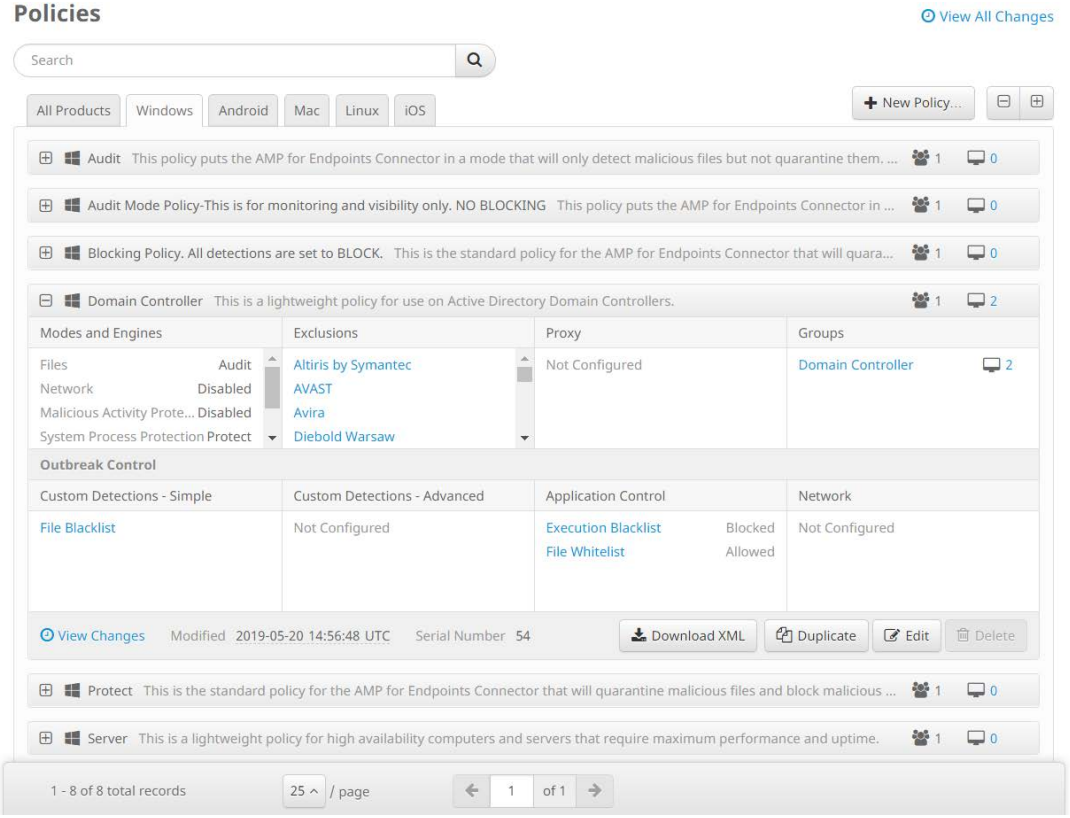


3. Click **Full Scan.**
4. A scan should begin.

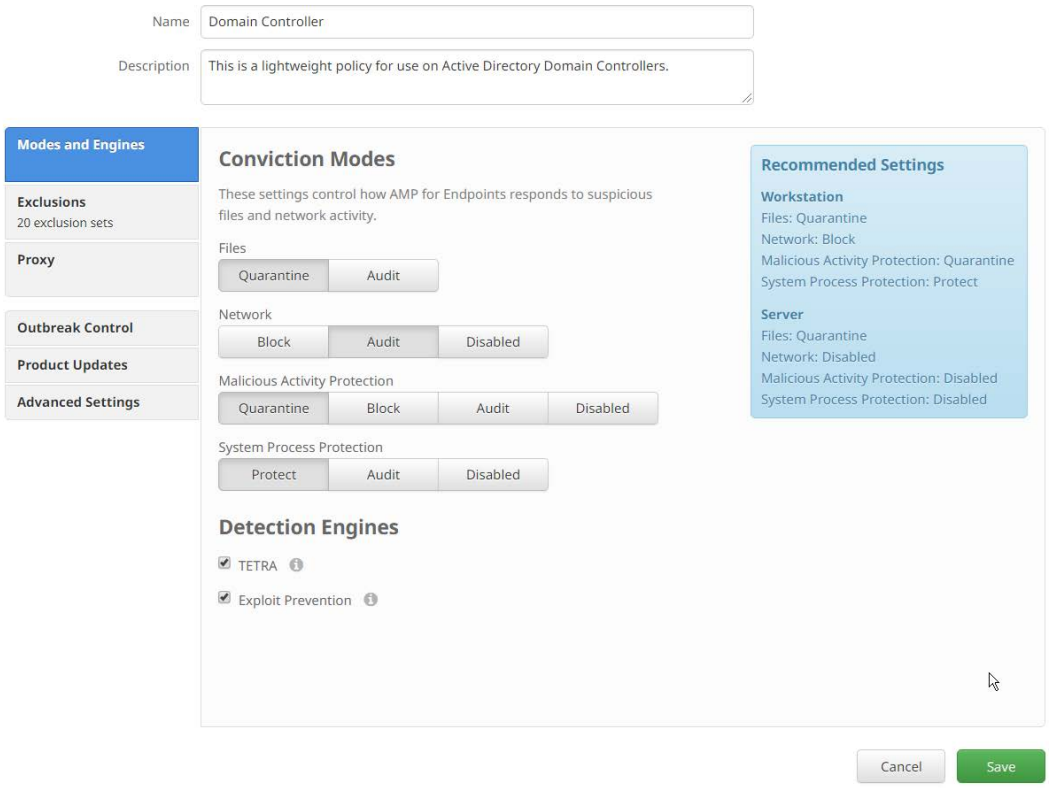
2.12.5 Configure AMP Policy

1. On the web console, navigate to **Management > Policies.**

2. Select a policy to edit; for this example, we choose **Domain Controllers.** (To edit which policies map to which groups, select **Management > Groups,** and click **Edit** on the group for which you wish to select a policy. You can select a policy for each Operating System (OS) in that group.)



3. Click **Edit.**
4. In the **Modes and Engines** tab, "Conviction Modes" refers to the *response* taken to various detected suspicious activity or files.
    - **Audit** is a detection/logging approach that does not take any action other than logging the activity.
    - **Quarantine** involves the move of the offending file to its own folder, where it is monitored and deleted after a certain amount of time. Quarantining can also be applied to processes, in which the process is monitored and prevented from affecting system operations.
    - **Block** involves the deletion of the file or the stopping of the process or network traffic.
5. "Detection Engines" refer to the actual detection of the suspicious activity.
    - **TETRA** is intended to be an anti-malware engine and recommends that it not be used when other antimalware software is in use.
    - **Exploit Prevention** refers to an engine that defends endpoints against memory injection attacks.



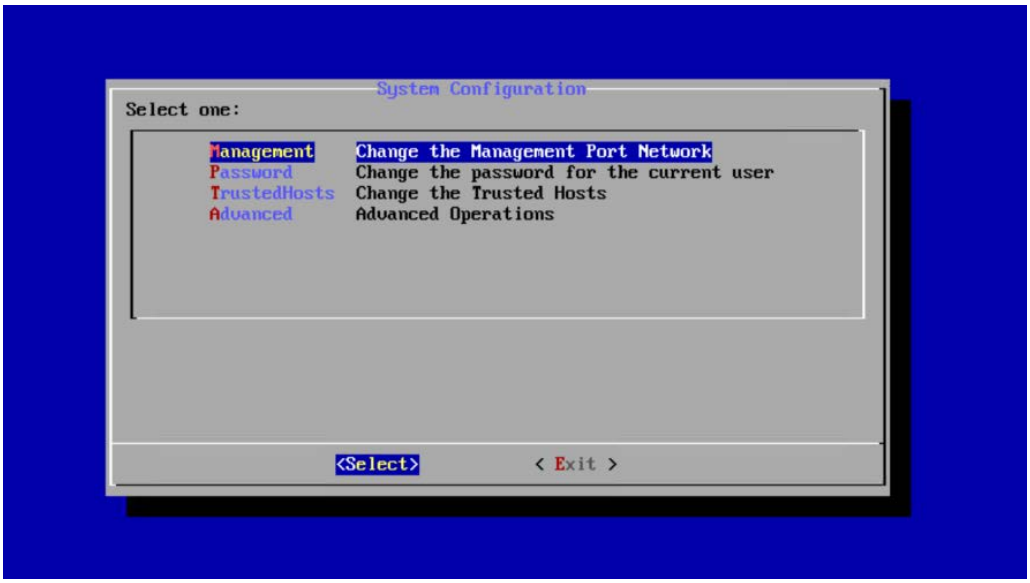
6. Click **Save.**

2.13 Cisco Stealthwatch

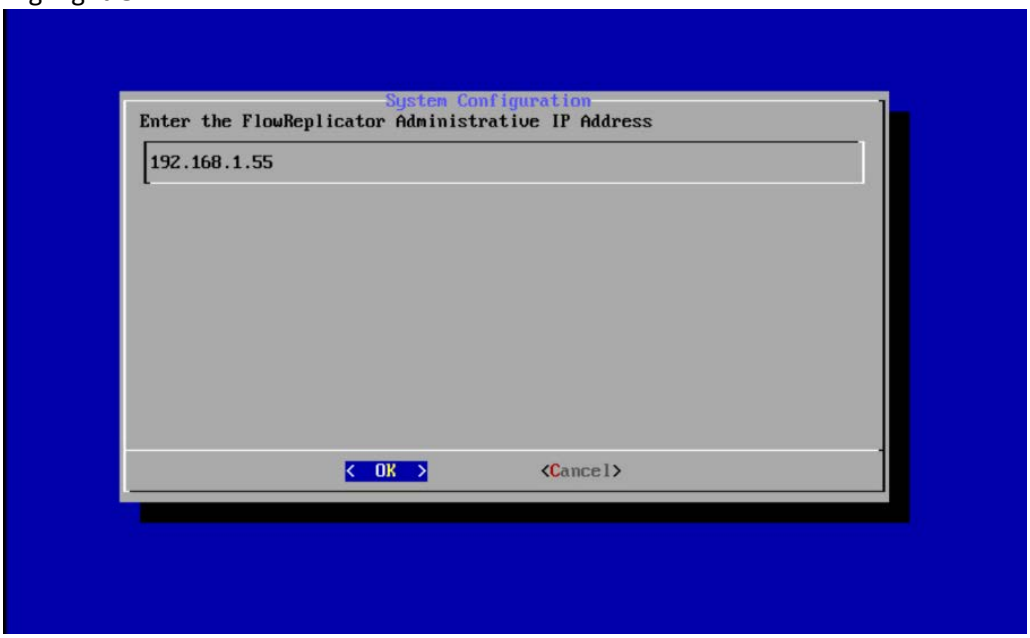
This section will describe the setup and configuration of Cisco Stealthwatch, a network monitoring solution. This guide assumes the use of the Stealthwatch virtual machines.

2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor

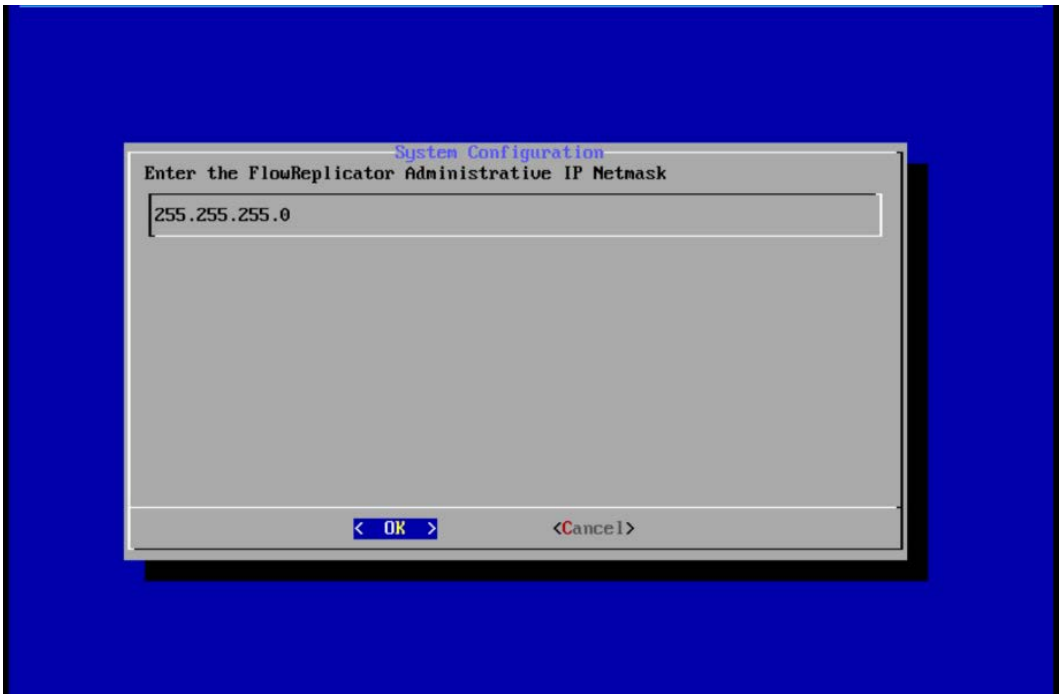
1. Log in to the console of **Stealthwatch Flow UDP Director.**
2. Navigate the menu to highlight **Management** and **Select.**



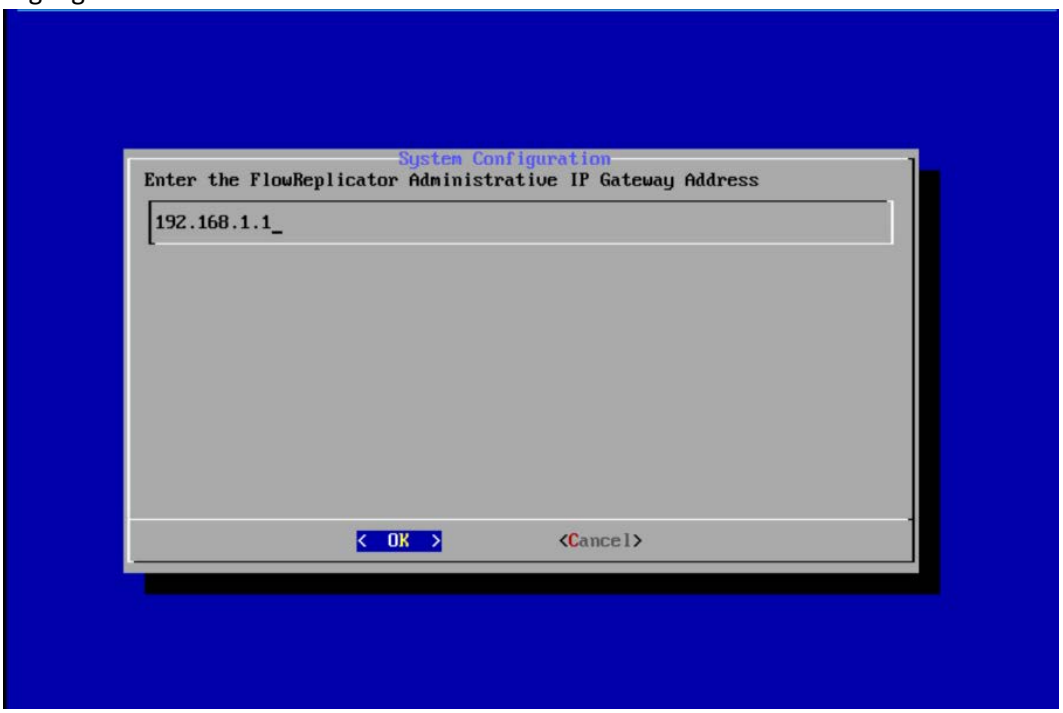
3. Press **Enter.**
4. Enter an **IP Address** for this machine.
5. Highlight **OK.**



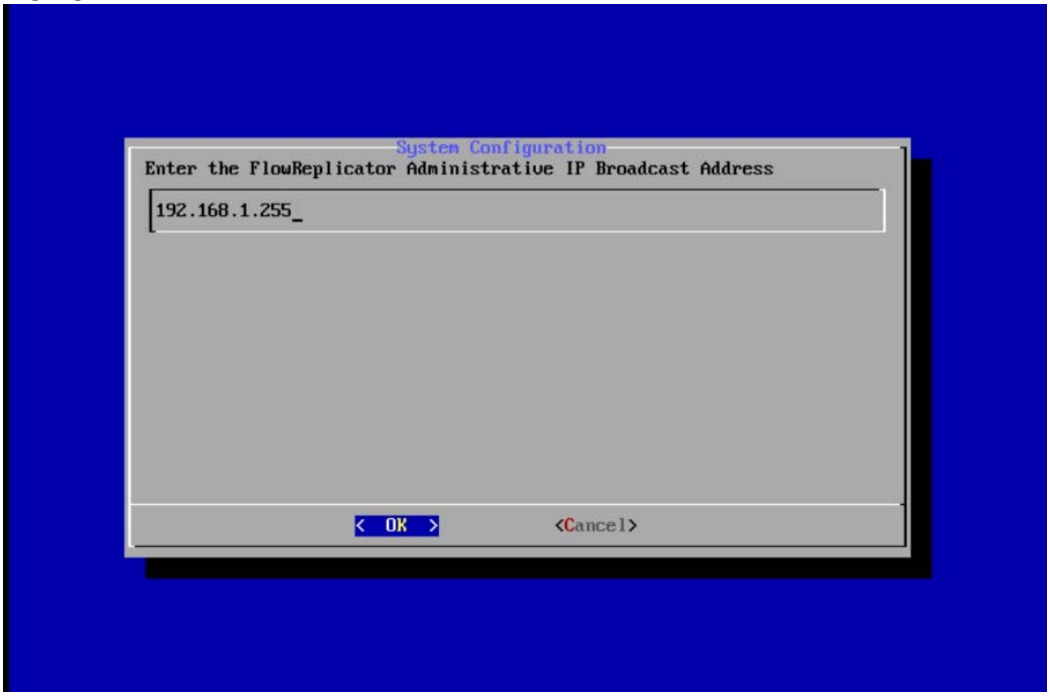
6. Press **Enter.**
7. Enter a **network mask** for the IP Address.
8. Highlight **OK.**



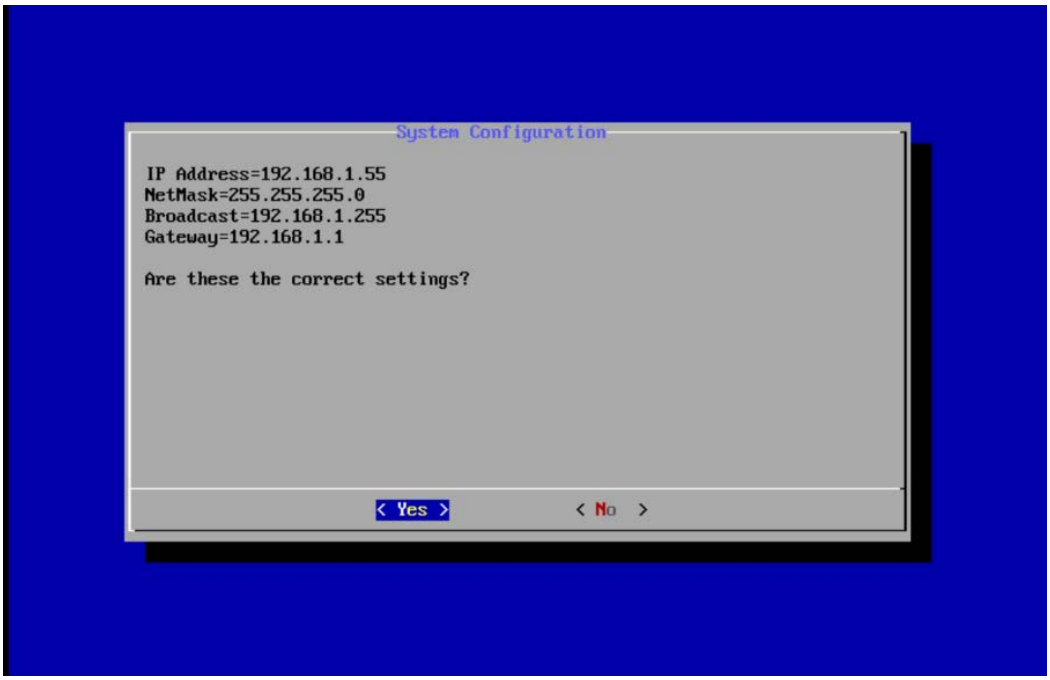
9. Press **Enter.**
10. Enter the network **gateway.**
11. Highlight **OK.**



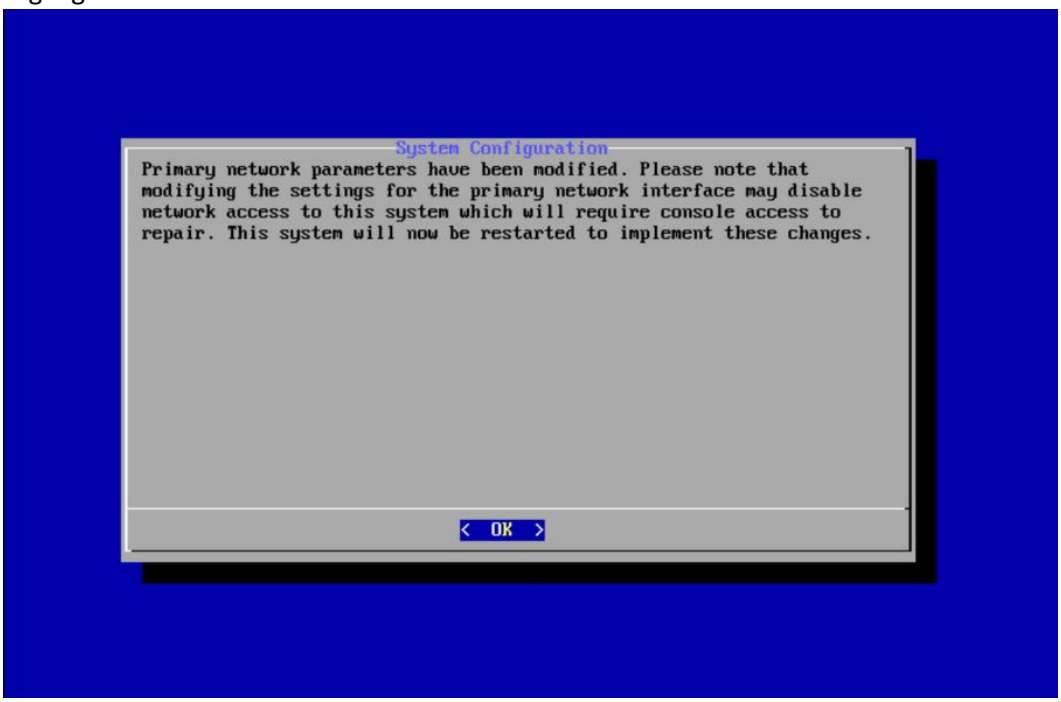
12. Press **Enter.**
13. Enter the network **broadcast address.**
14. Highlight **OK.**



15. Press **Enter.**
16. Highlight **Yes.**



17. Press **Enter.**
18. Highlight **OK.**

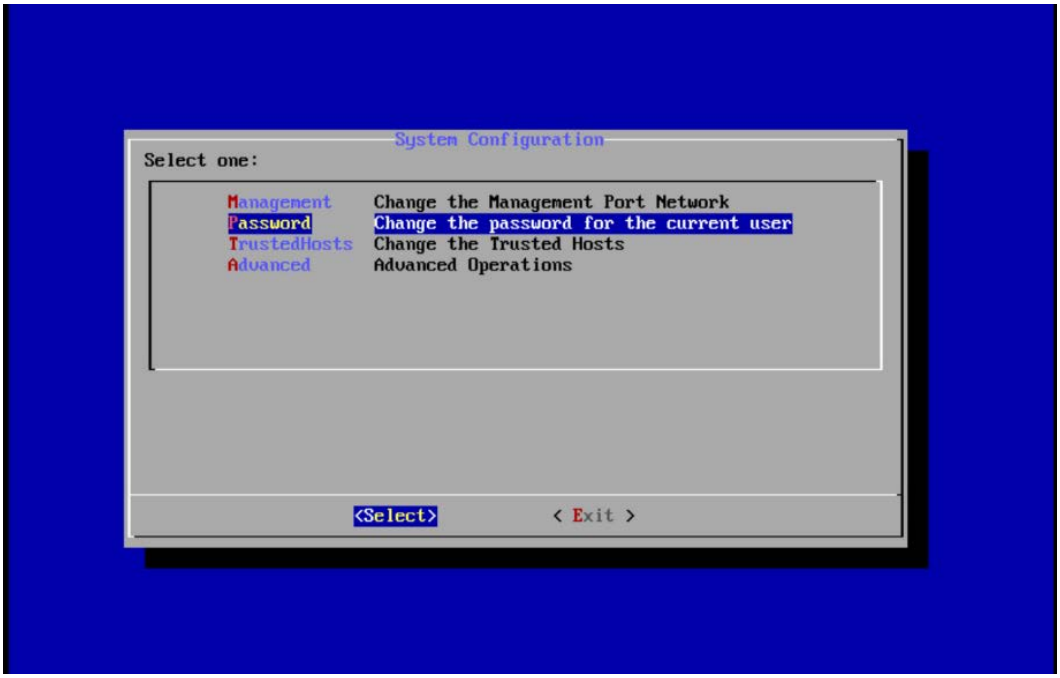


19. Press **Enter.**

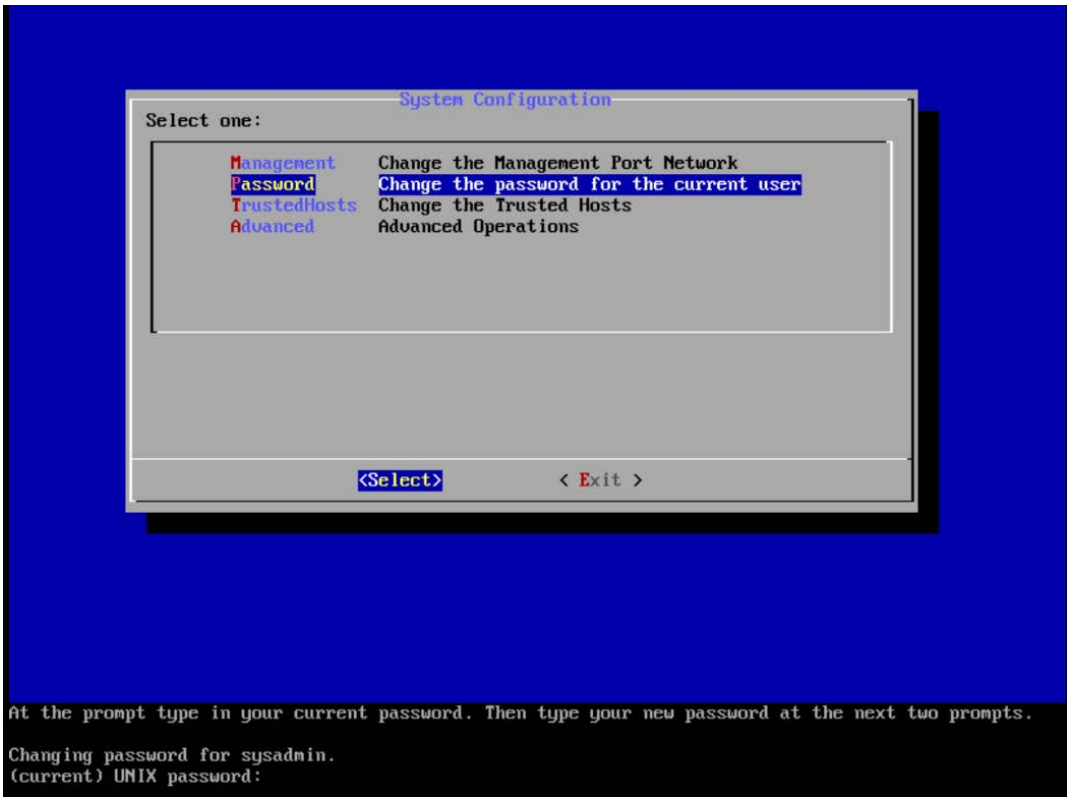
20. Repeat steps 1-19 for each of the **Stealthwatch Management Console, Stealthwatch UDP Director, Stealthwatch Flow Sensor,** and **Stealthwatch Flow Collector.**

2.13.2 Change Default Stealthwatch Console Passwords

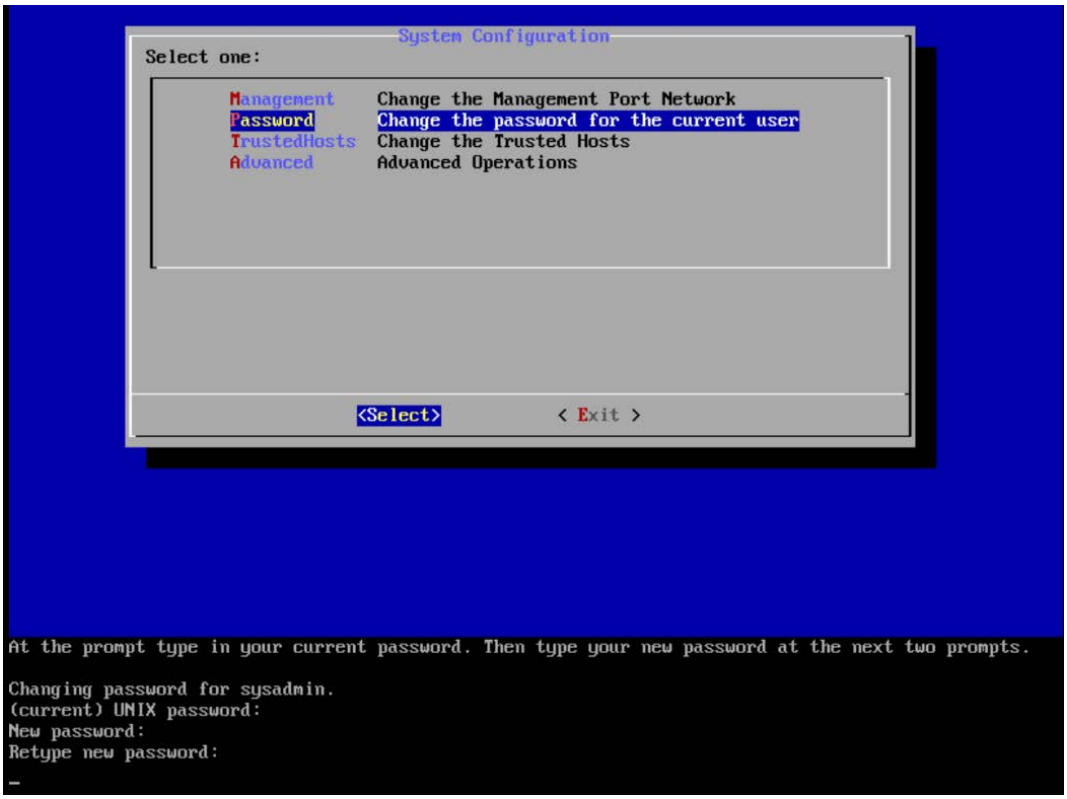
1. In the **System Configuration** menu, highlight **Password** and **Select.**



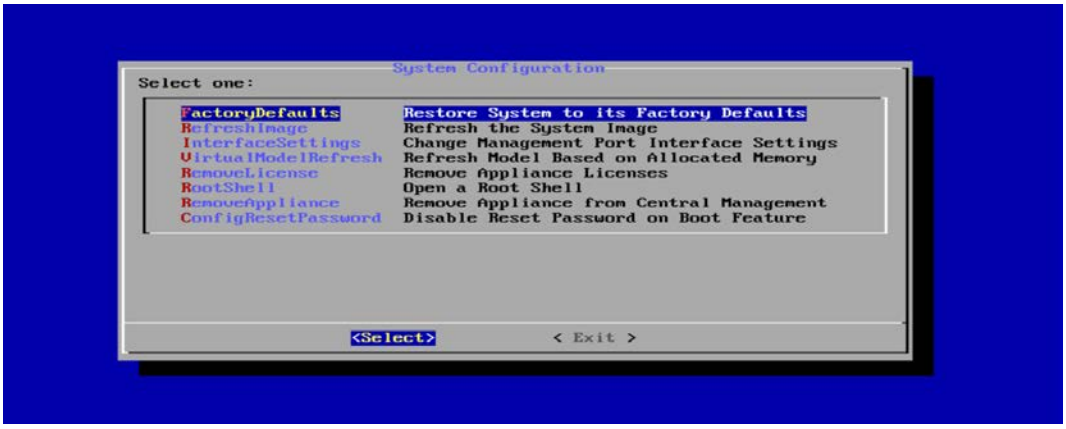
2. Press **Enter.**
3. Enter the original password.



4. Press **Enter.**
5. Enter the new password, and confirm it.

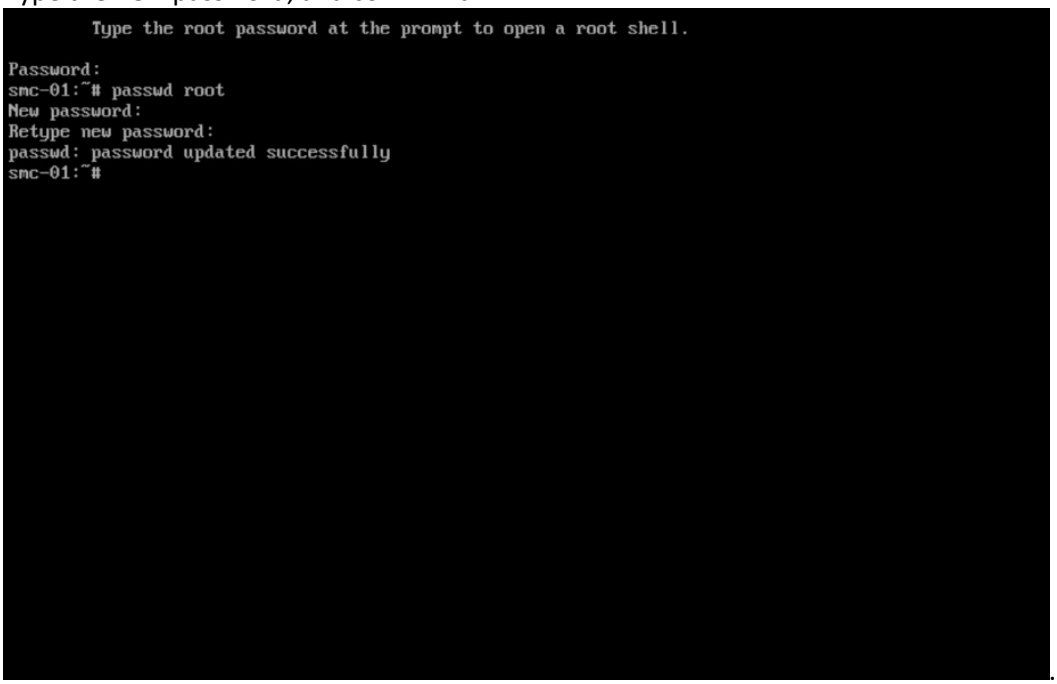


6. Press **Enter.**
7. In the **System Configuration** menu, highlight **Advanced** and **Select.**
8. Press **Enter.**
9. Highlight **RootShell** and **Select.**



10. Press **Enter.**
11. Log in using the original root shell password.

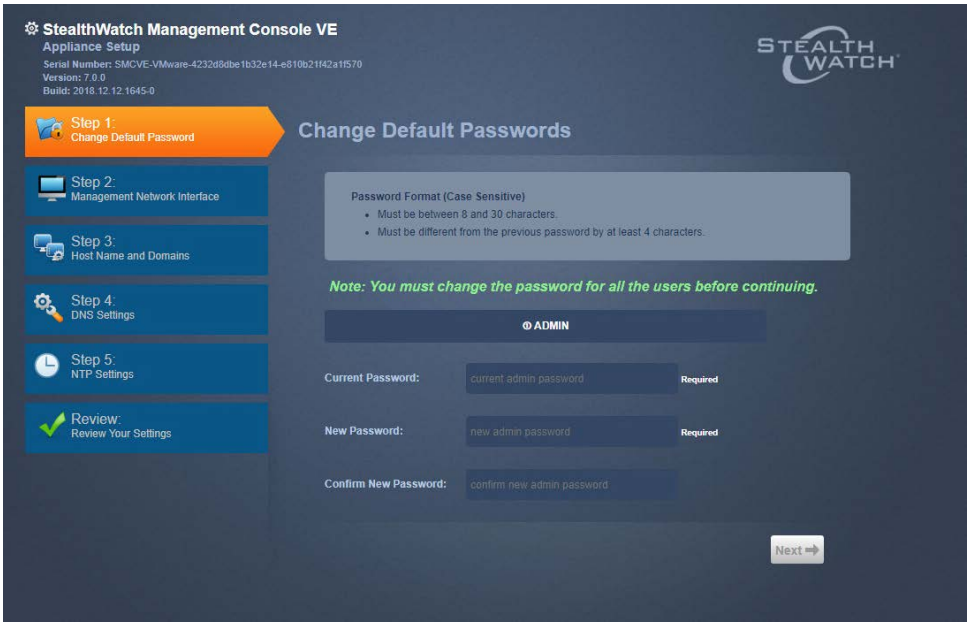
12. Enter the command **root.**
13. Type the new password, and confirm it.



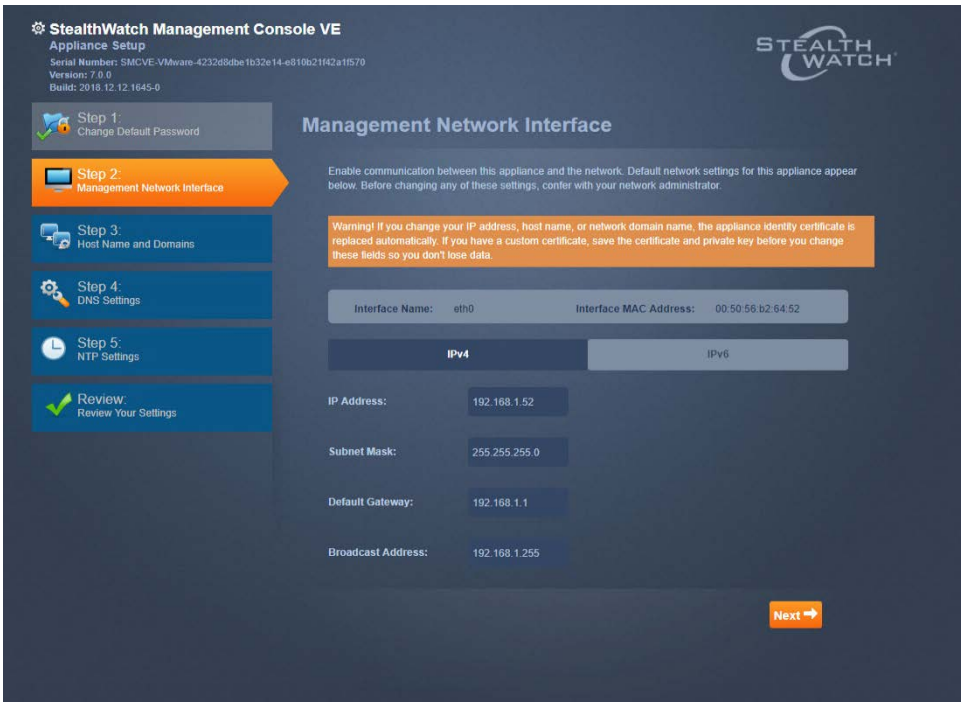
14. Press **Enter.**
15. Repeat steps 1-14 for each console.

2.13.3 Configure the Stealthwatch Management Console Web Interface

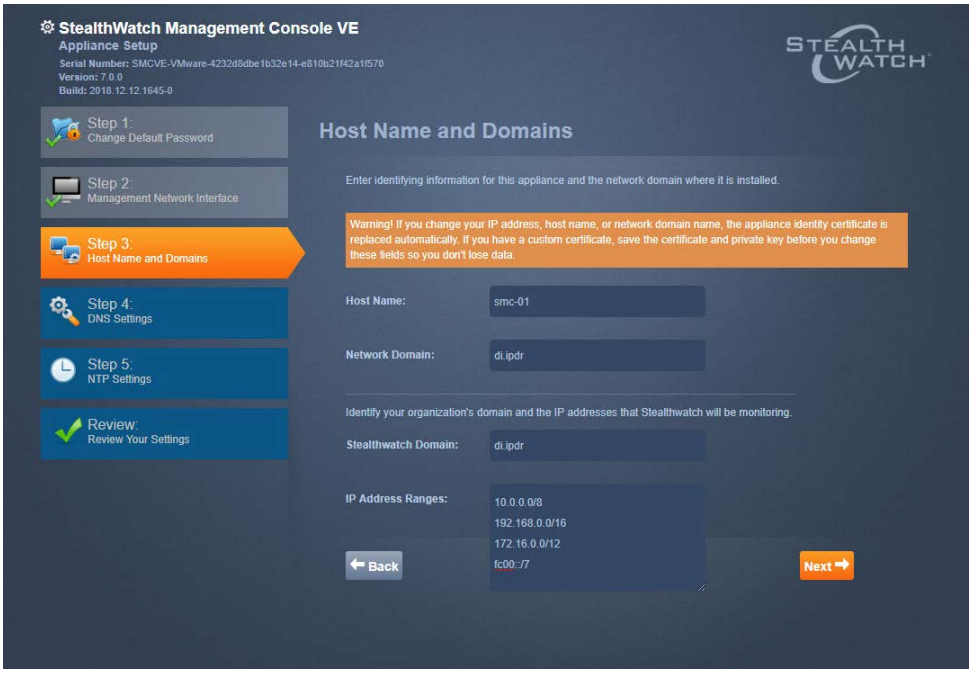
1. Change the default password by filling in the fields for **Current Password, New Password,** and **Confirm New Password.**



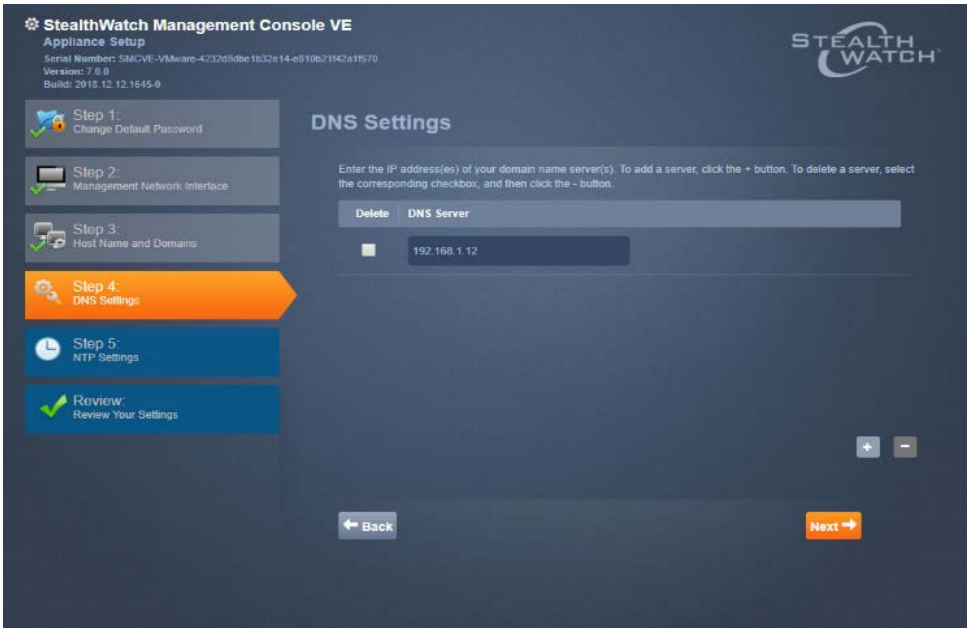
2. Click **Next.**
3. Fill in the fields for **IP Address, Subnet Mask, Default Gateway** and **Broadcast Address** according to your network topology.



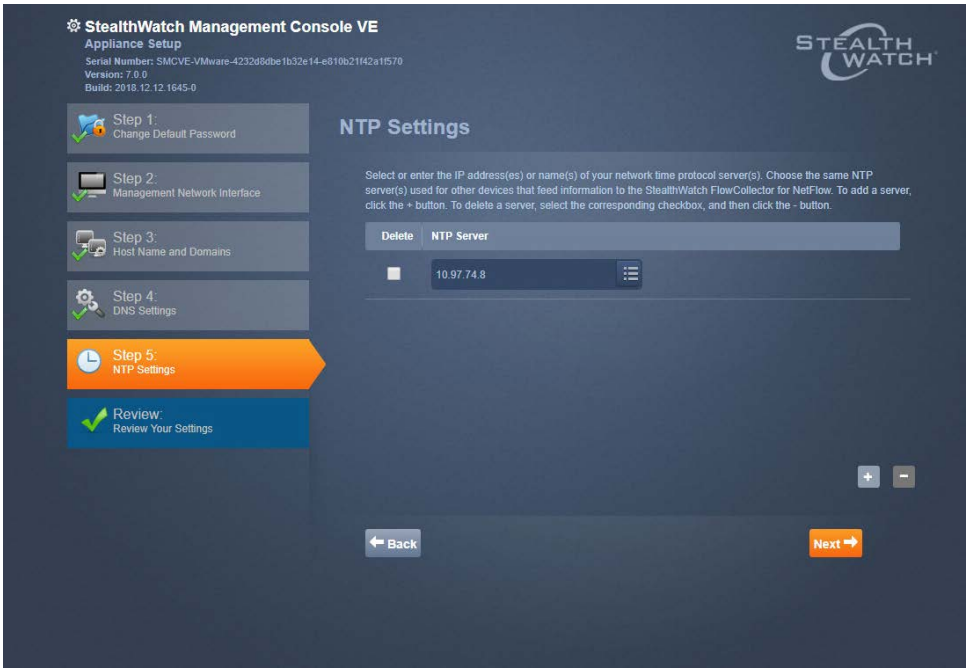
4. Click **Next.**
5. Enter a **host name.**
6. Enter the network domain that Stealthwatch is in for **Network Domain.**
7. Enter the network domain that Stealthwatch will be monitoring for **Stealthwatch Domain.**



8. Click **Next.**
9. Enter a **DNS Server.**

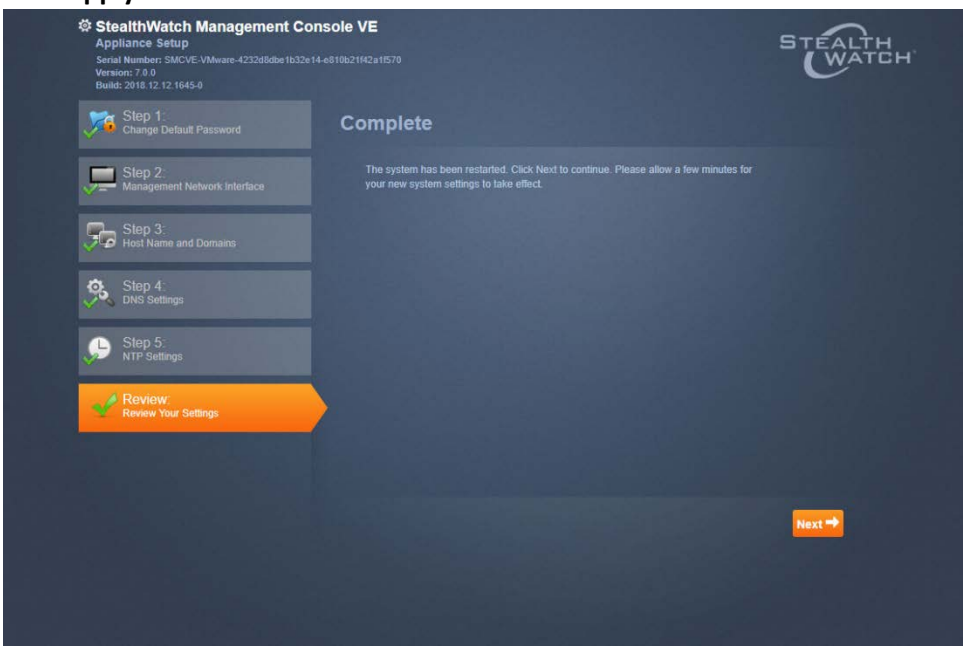


10. Click **Next.**
11. Configure the NTP server according to your network topology.



12. Click **Next.**
13. Select **Restart.**

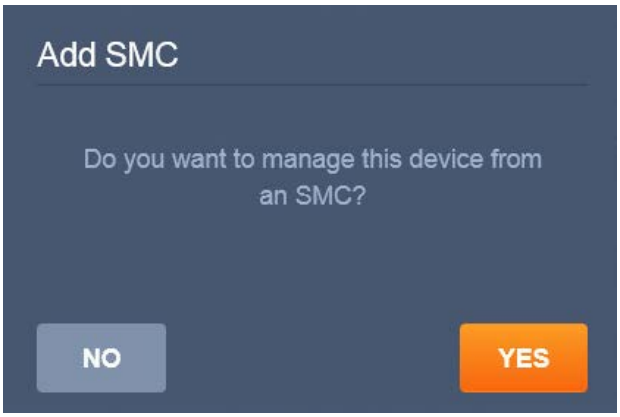
14. Click **Apply.**



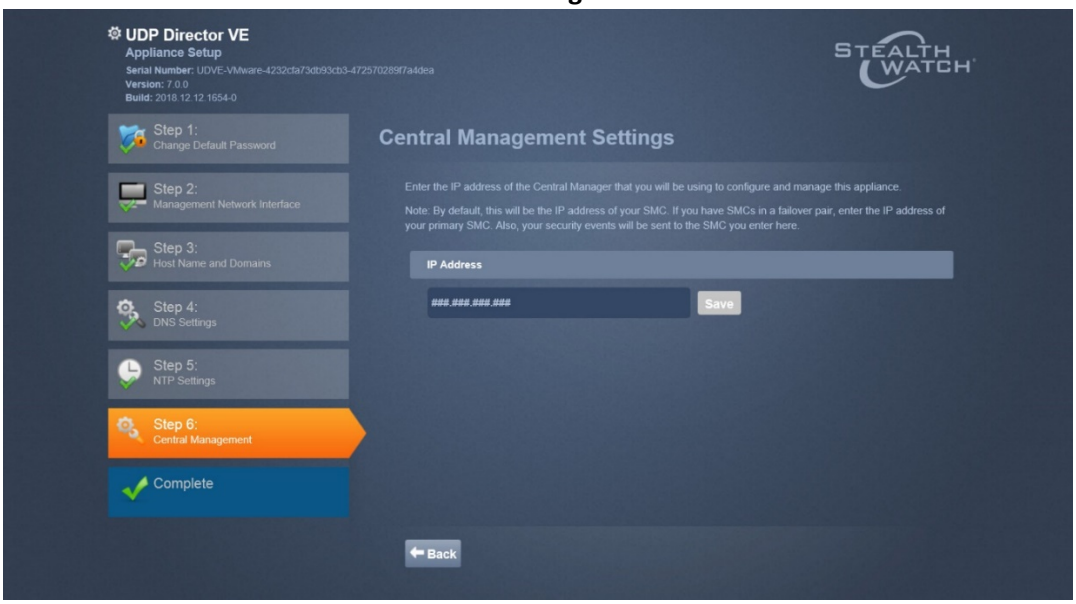
15. After the restart, click **Next.**

2.13.4 Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces

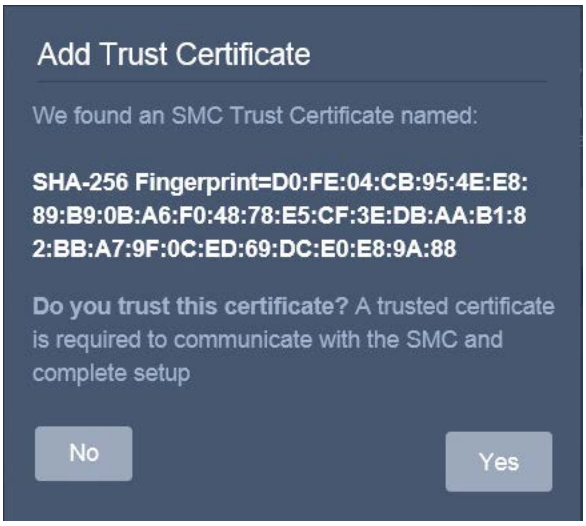
1. Repeat steps 1-12 from *Configure the Stealthwatch Management Console Web Interface.*



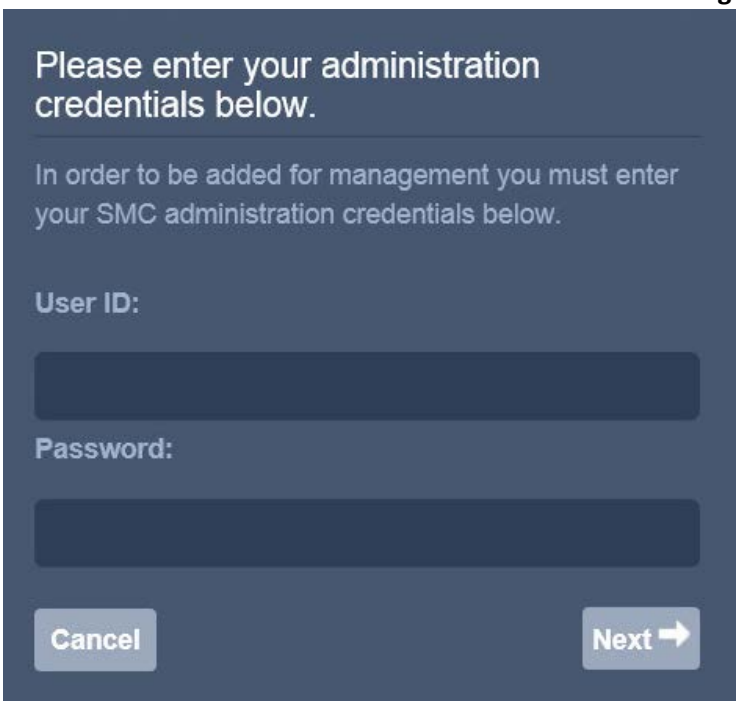
2. When prompted to manage this device from an SMC, click **Yes.**
3. Enter the IP Address of the **Stealthwatch Management Console.**



4. Click **Save.**
5. Verify the certificate.



6. Click **Yes.**
7. Enter the **User ID** and **Password** for the **Stealthwatch Management Console.**



8. Click **Next.**
9. Repeat steps 1-8 for the Flow Collector *first* and *then* for the Flow Sensor. The Flow Sensor cannot be added to the Management Console until after the Flow Collector is successfully added.

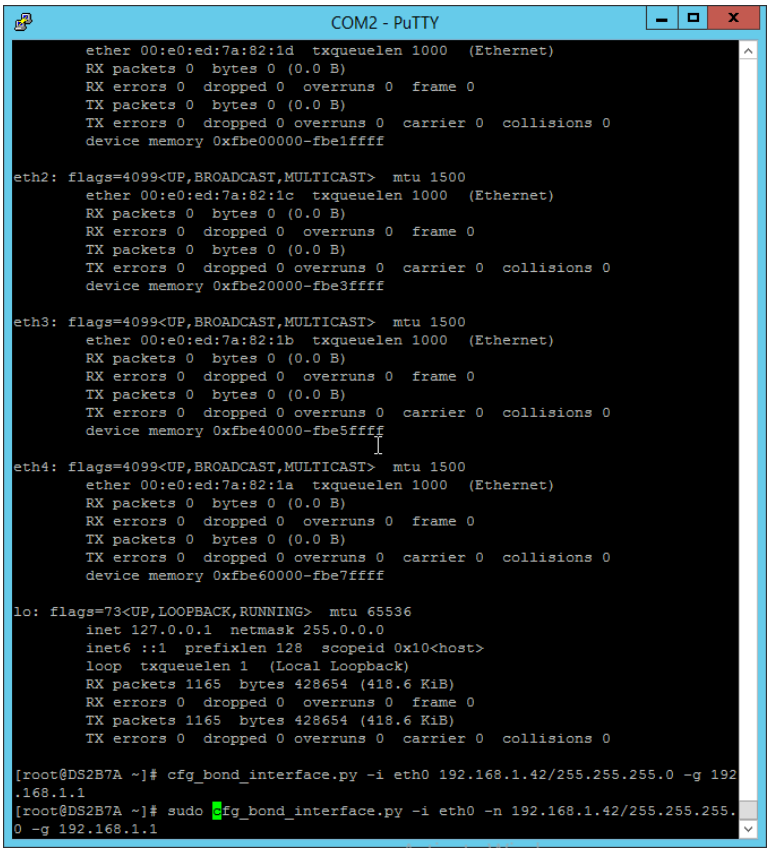
2.14 Symantec Analytics

This section details the installation and configuration of Symantec Analytics, a network analysis tool. This guide assumes that Symantec Analytics is connected via serial to a terminal.

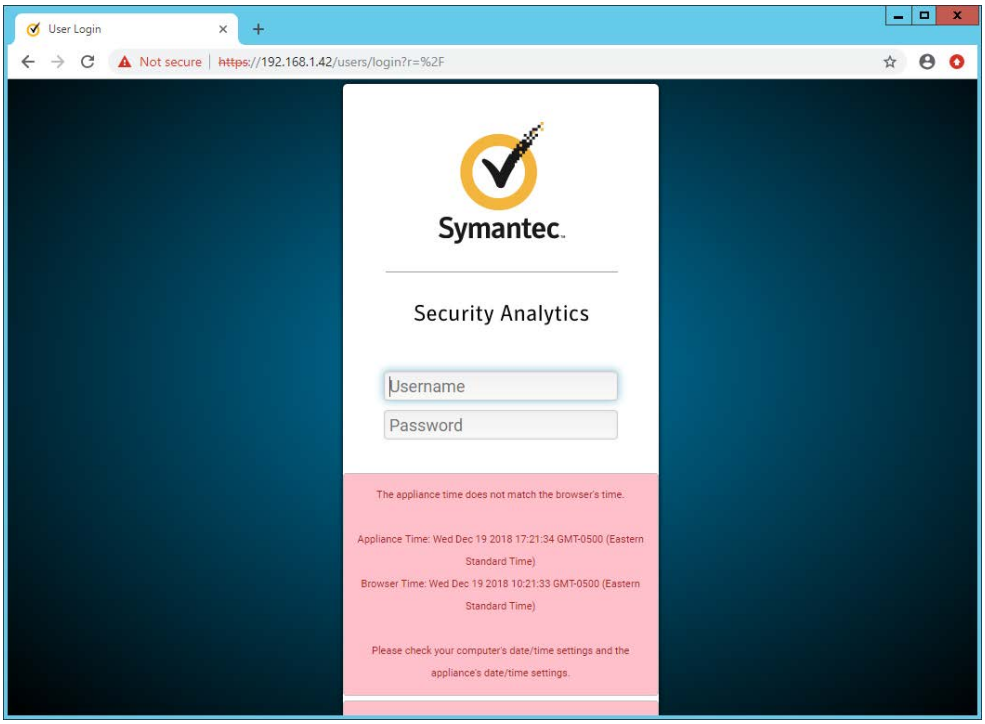
2.14.1 Initial Setup

1. Log in to the Symantec Analytics command line.
2. Enter the following command to configure the IP for the interface:

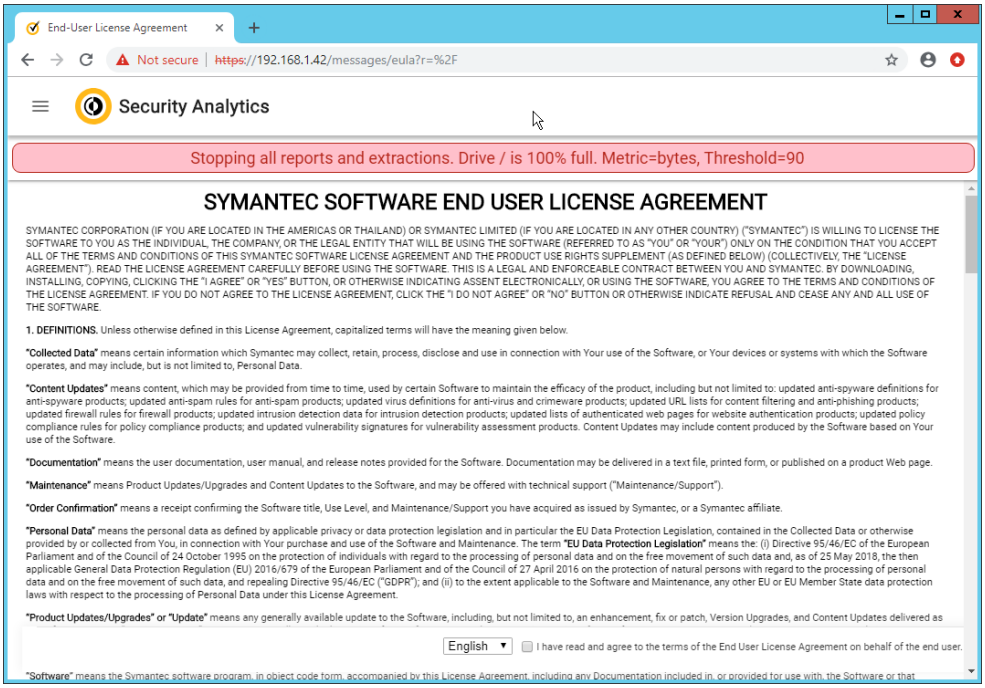
```
sudo cfg_bond_interface.py -i eth0 -n 192.168.1.42/255.255.255.0 -g 192.168.1.1
```



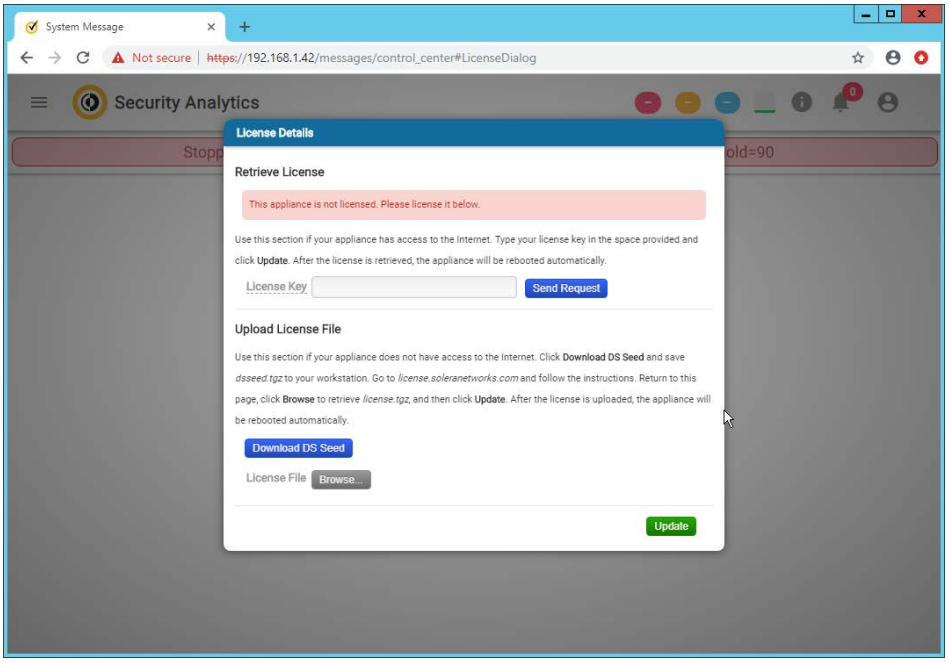
3. Navigate to the IP you assigned in a browser.



4. Enter the username and password to log in. The default is **(Admin/Solera).**
5. Check the box next to **I have read and agreed to the terms of the End User License Agreement on behalf of the end user.**

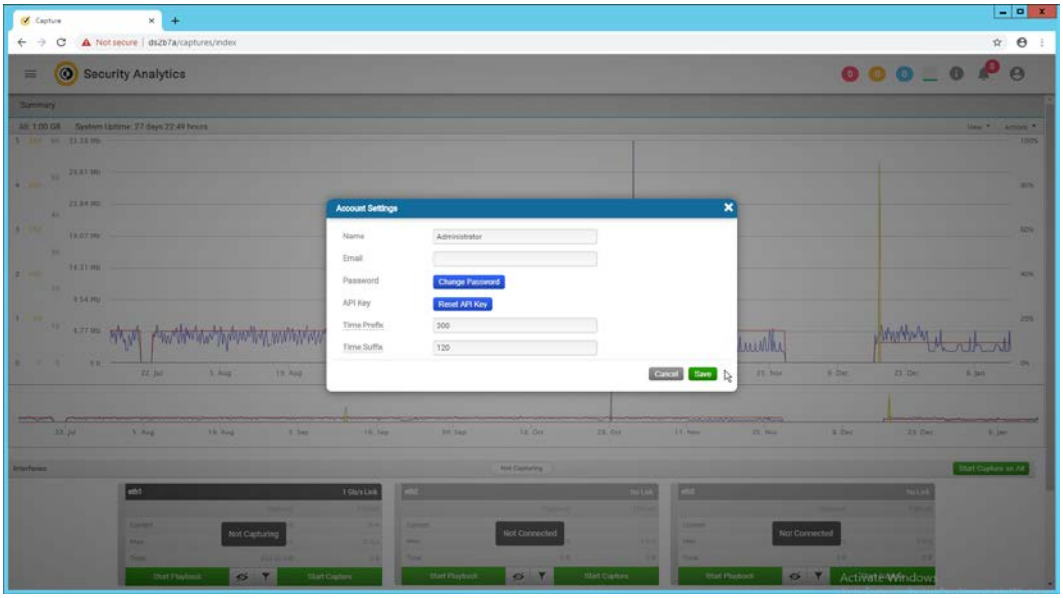


6. Click **Next.**
7. Enter the license key.
8. If you do not have internet connectivity, follow the instructions under **Upload License File.** Otherwise, click **Send Request.**

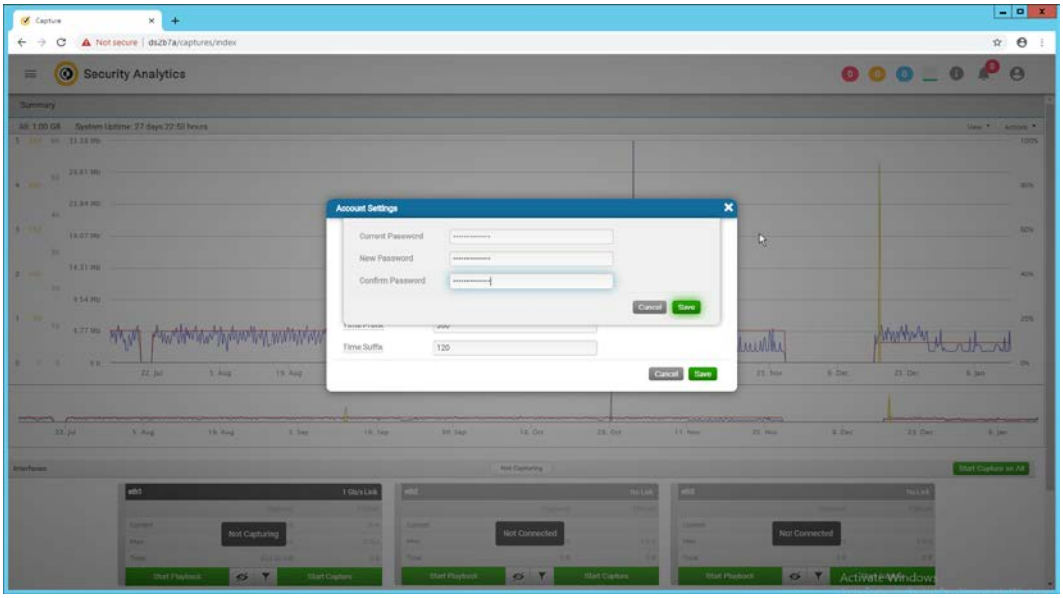


9. Click **Update.** The device will reboot.
10. Log in to the web page again.
11. Click the silhouette in the top right corner and click **Account Settings.**

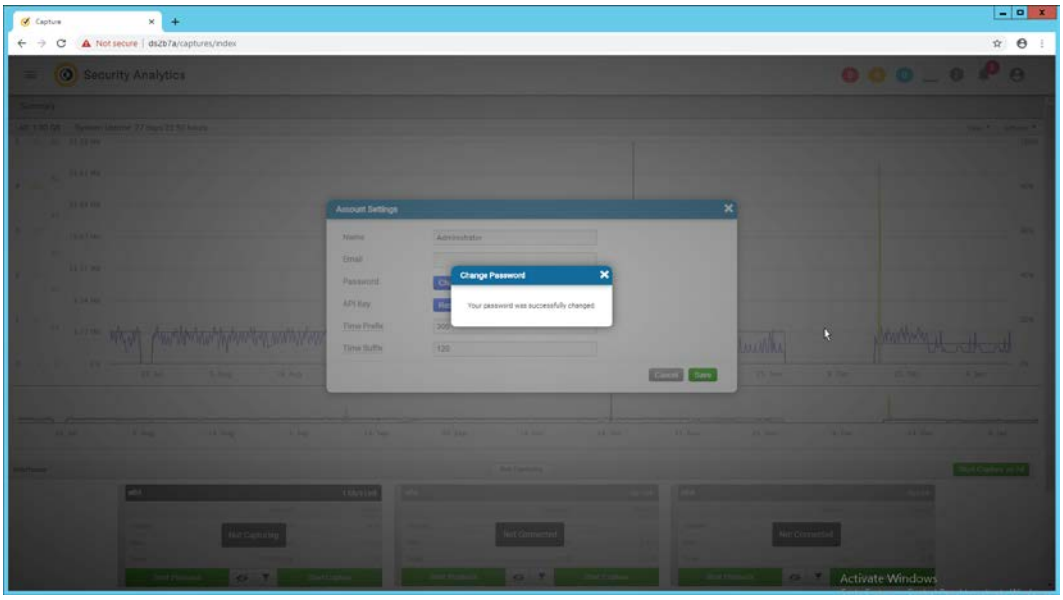
12. Click **Change Password.**



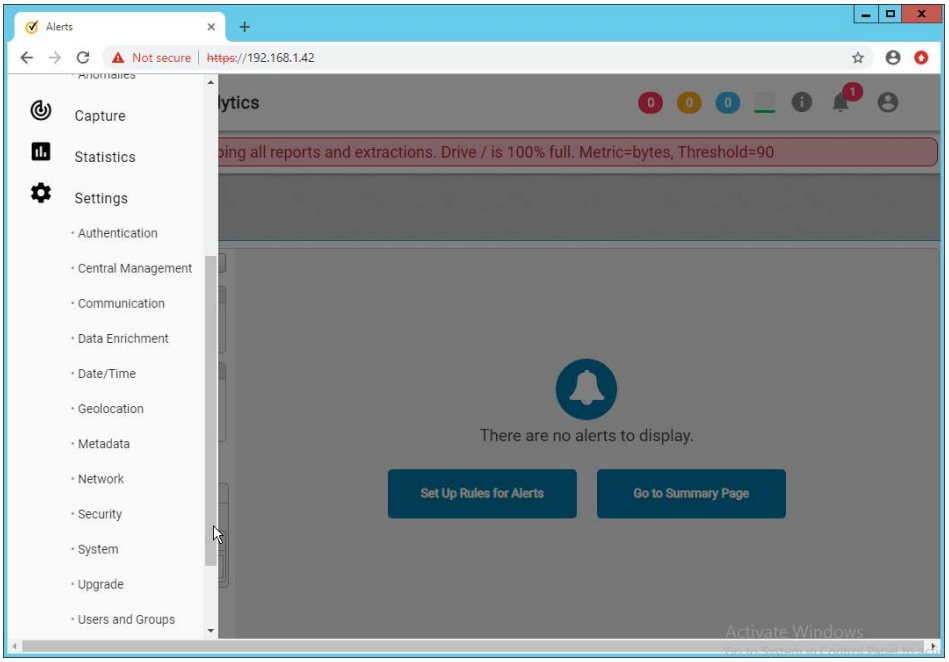
13. Enter a new password. Click **Save.**



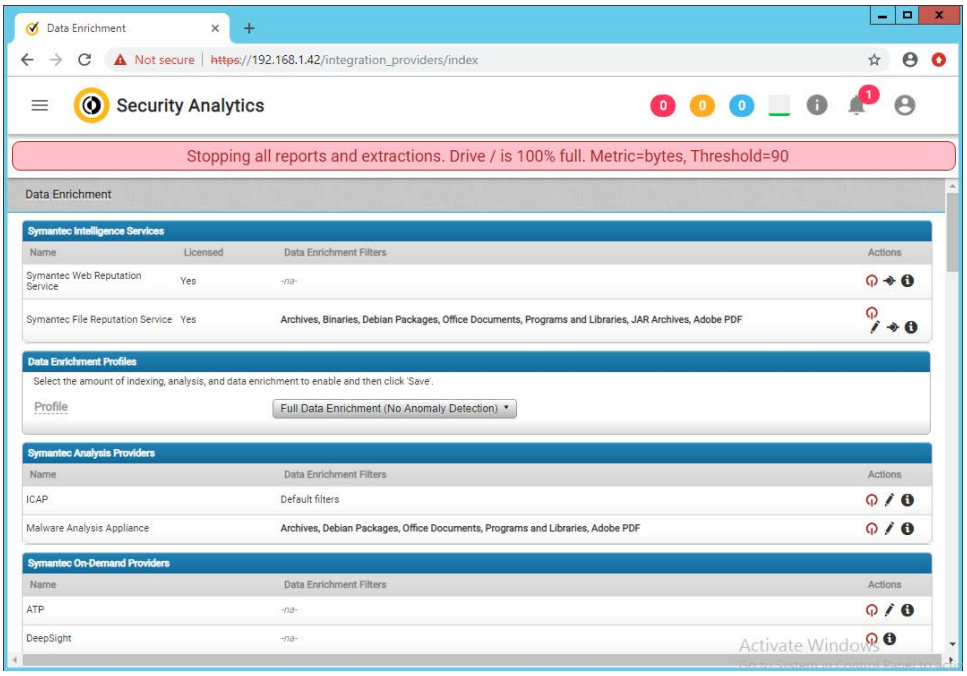
14. The screen should reflect that the password has been changed. Close out of both windows and return to the main web console.



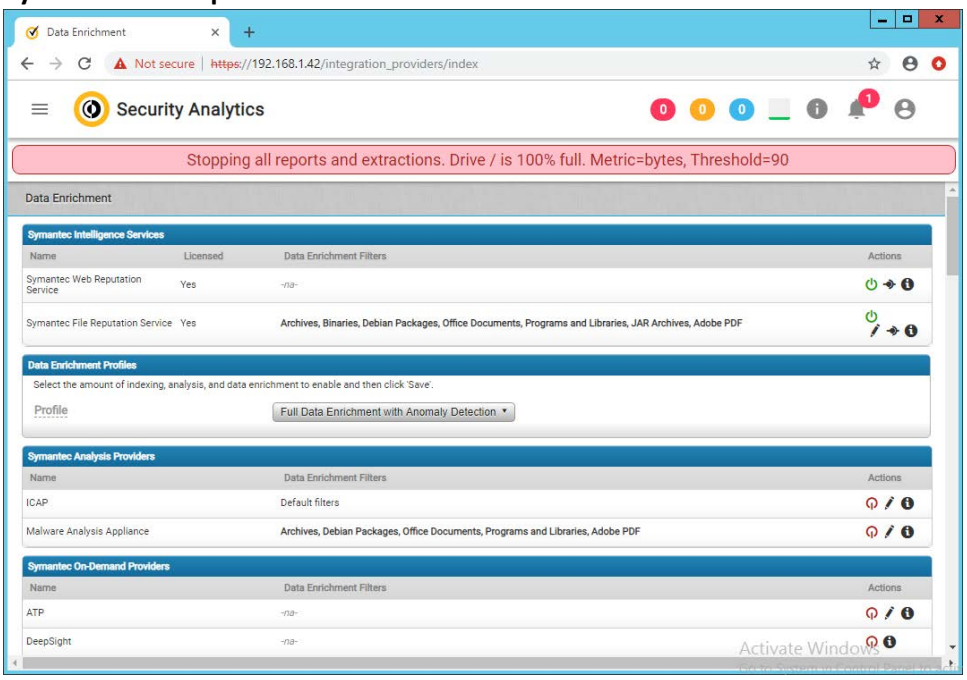
15. In the top left corner of the web console, click the menu button. (It shows as three horizontal bars).



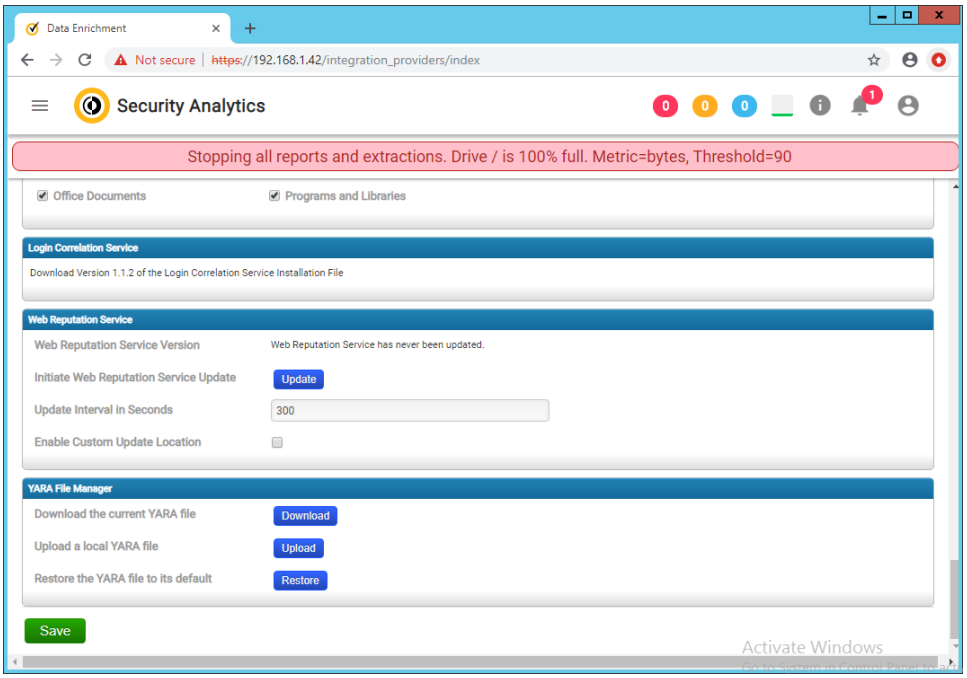
16. Navigate to **Settings > Data Enrichment.**



17. Click the red upside-down power symbols next to **Symantec Web Reputation Service** and **Symantec File Reputation Service** to turn them on.



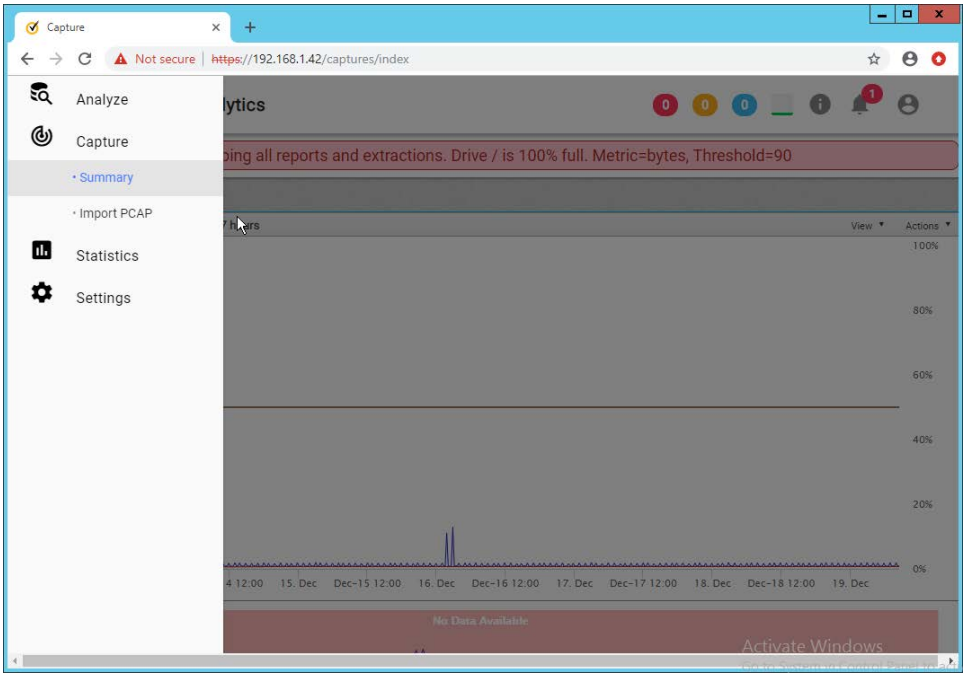
18. Select **Full Data Enrichment (with Anomaly Protection)** for the profile under **Data Enrichment Profiles.**



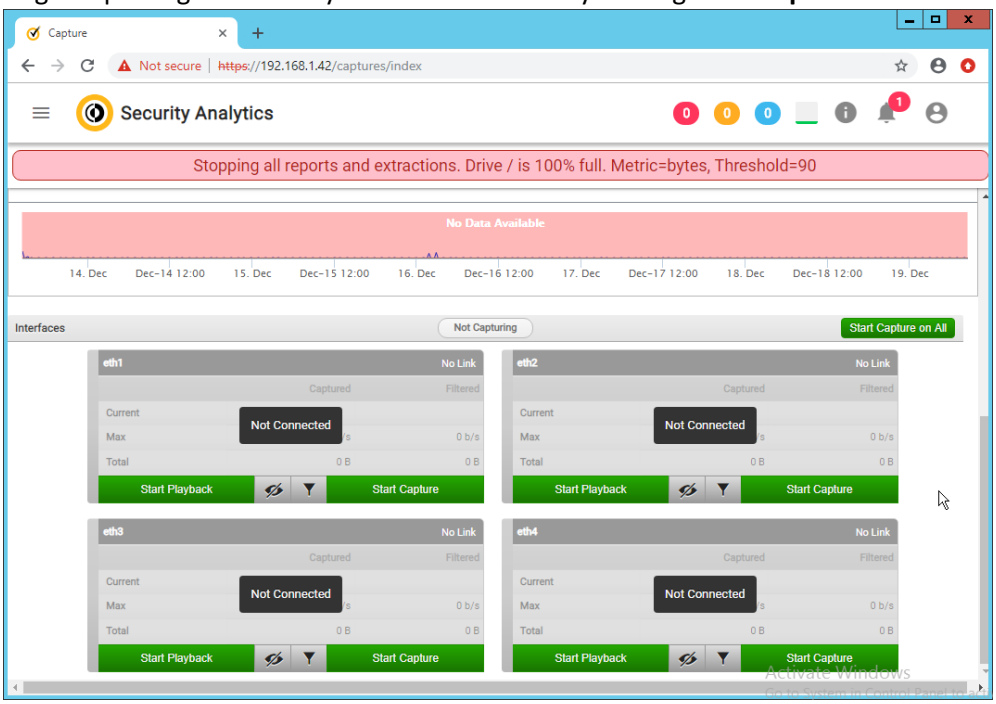
19. Click **Save.**

2.14.2 Capturing Data

1. Navigate to **Capture > Summary** in the menu.



2. Begin capturing data on any desired interfaces by clicking **Start Capture.**

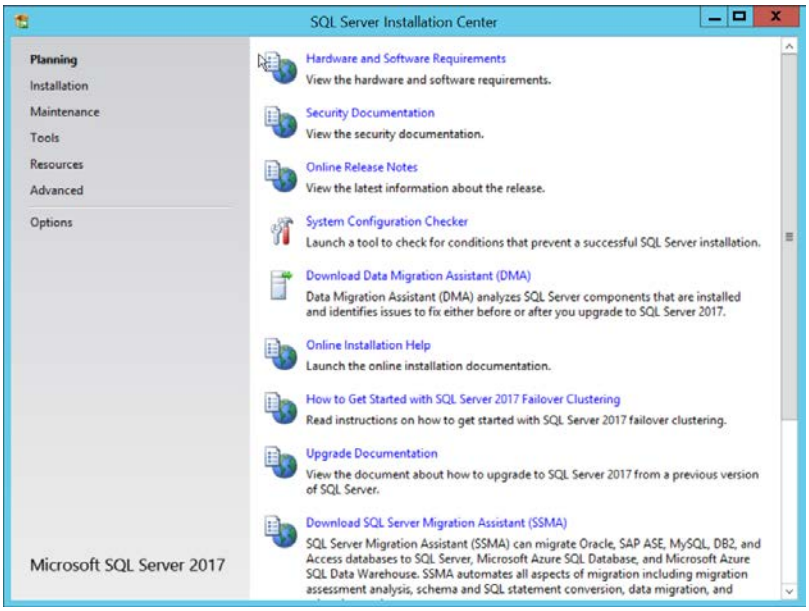


2.15 Symantec Information Centric Analytics

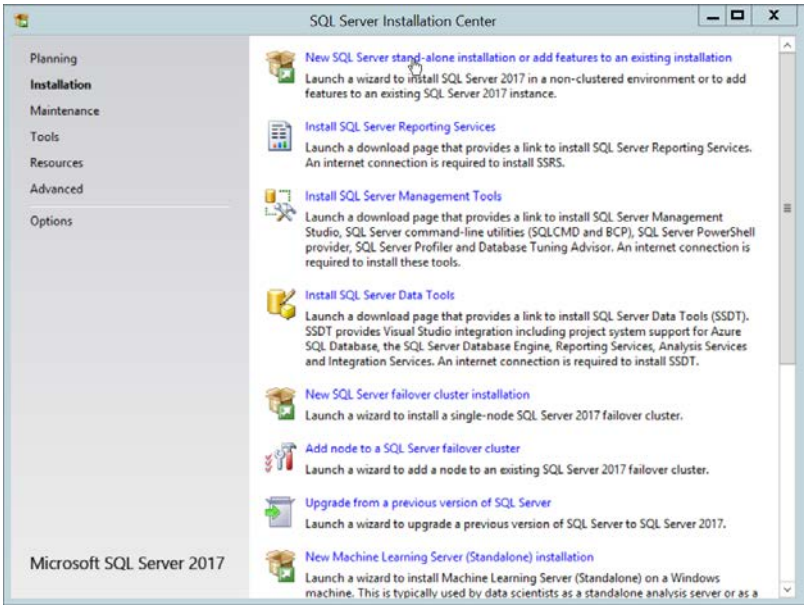
This section describes the installation and configuration of Symantec Information Centric Analytics (ICA).

2.15.1 Installing MS SQL 2017

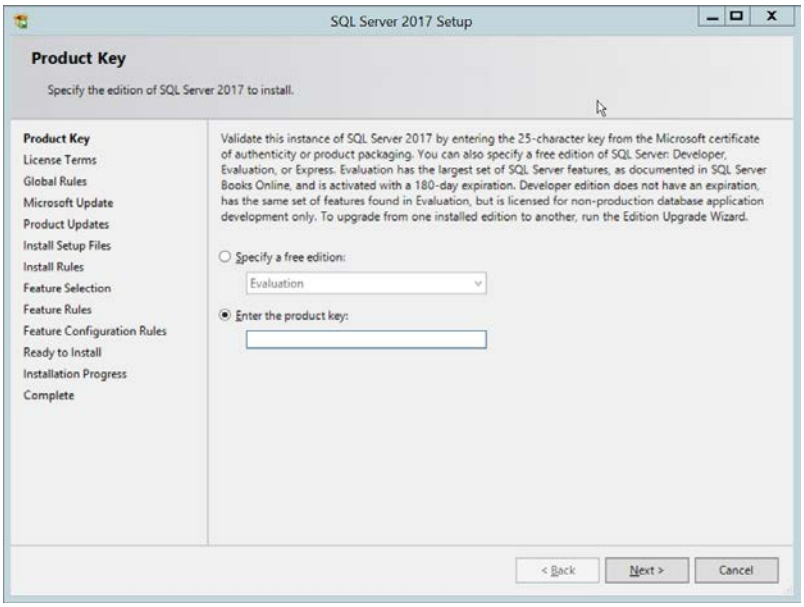
1. Launch the SQL Setup Wizard.



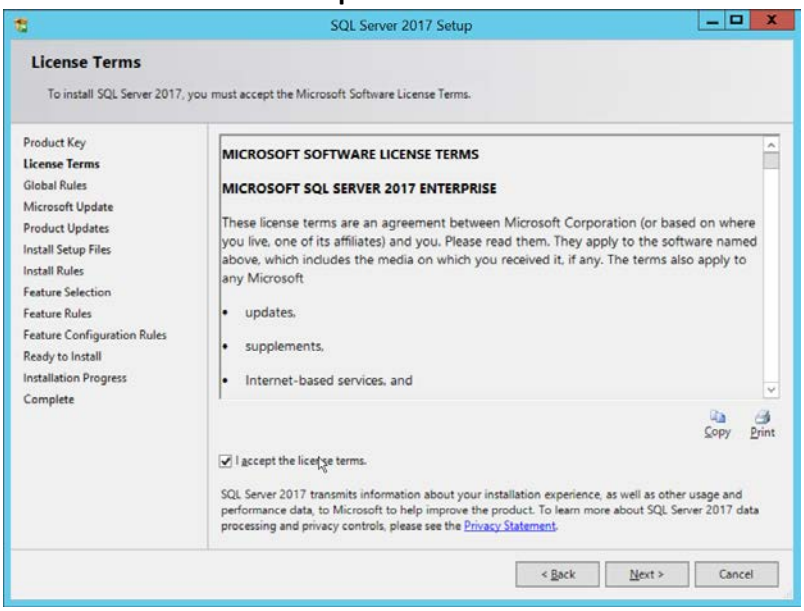
2. Click **Installation.**



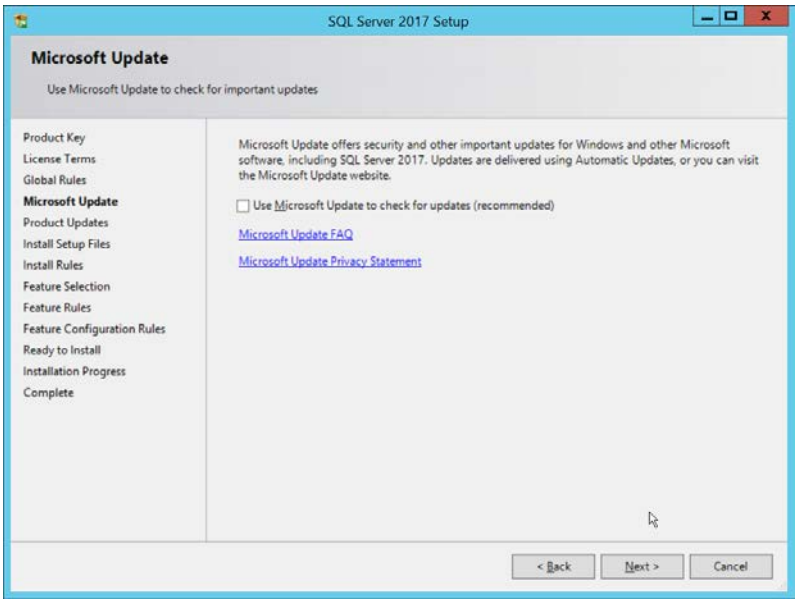
3. Click **New SQL Server stand-alone installation or add features to an existing installation.**
4. Enter a **product key.**



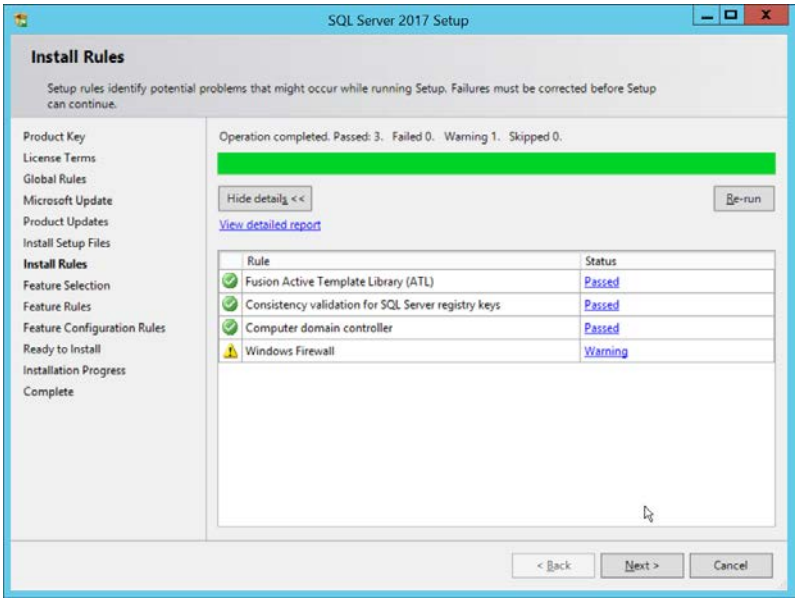
5. Click **Next.**
6. Check the box next to **I accept the license terms.**



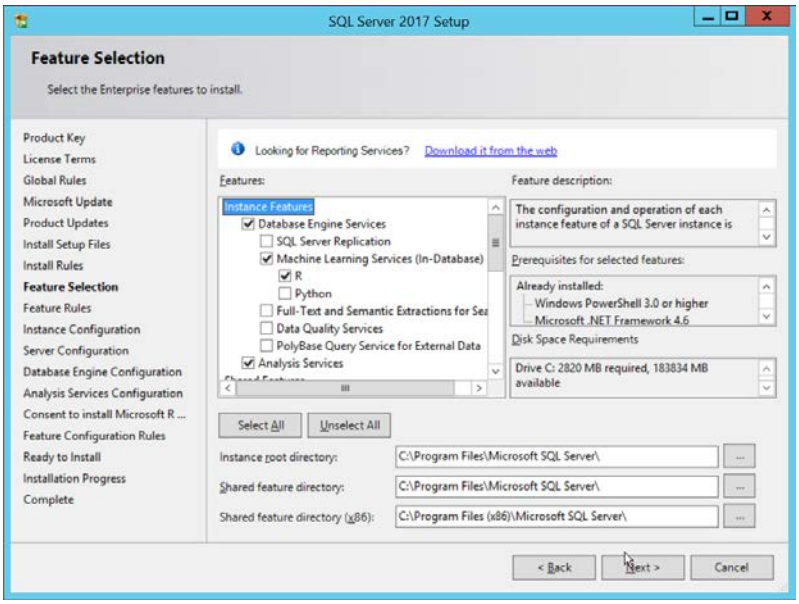
7. Click **Next.**



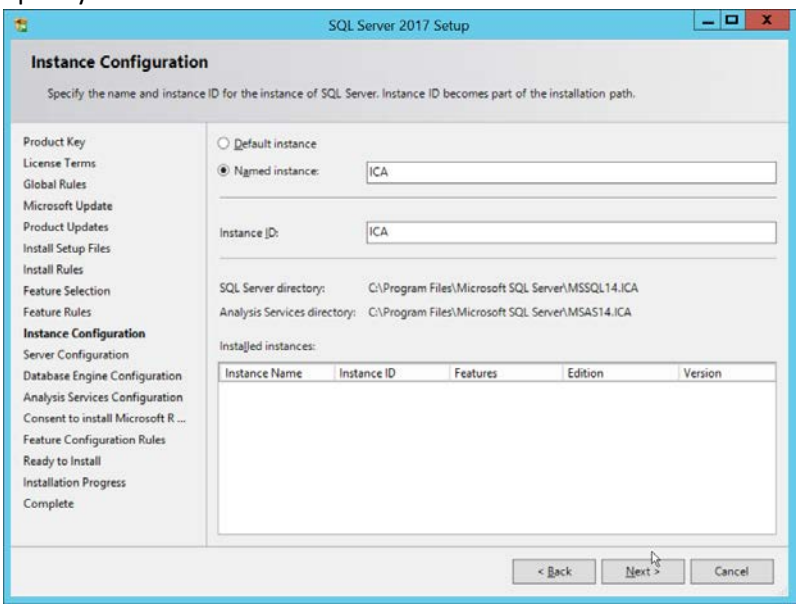
8. Click **Next.**



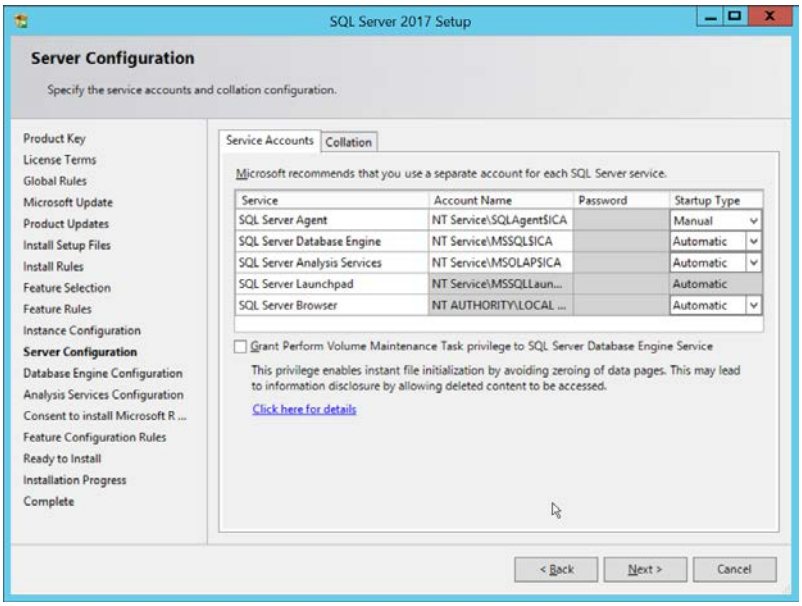
9. Click **Next.**
10. Ensure that box next to **R** and the box next to **Analysis Services** is checked.



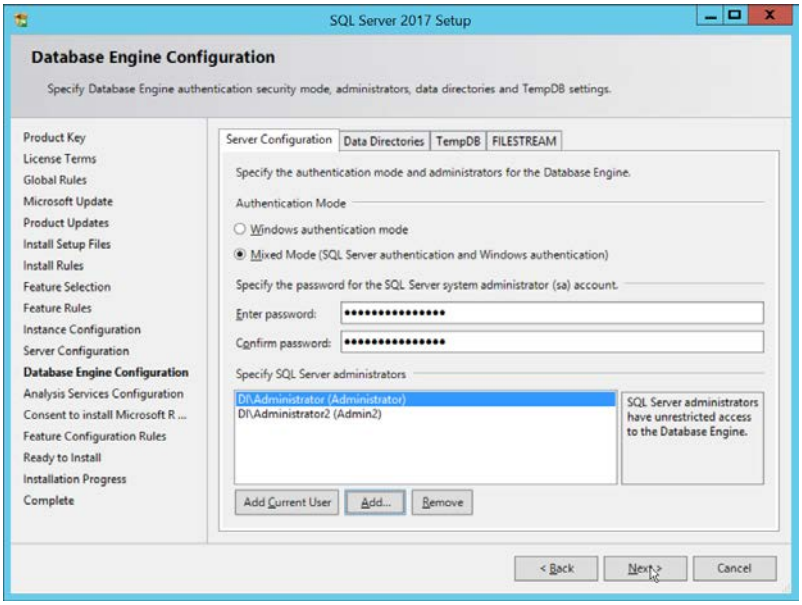
11. Click **Next.**
12. Select **Named instance.**
13. Specify a name for the instance.



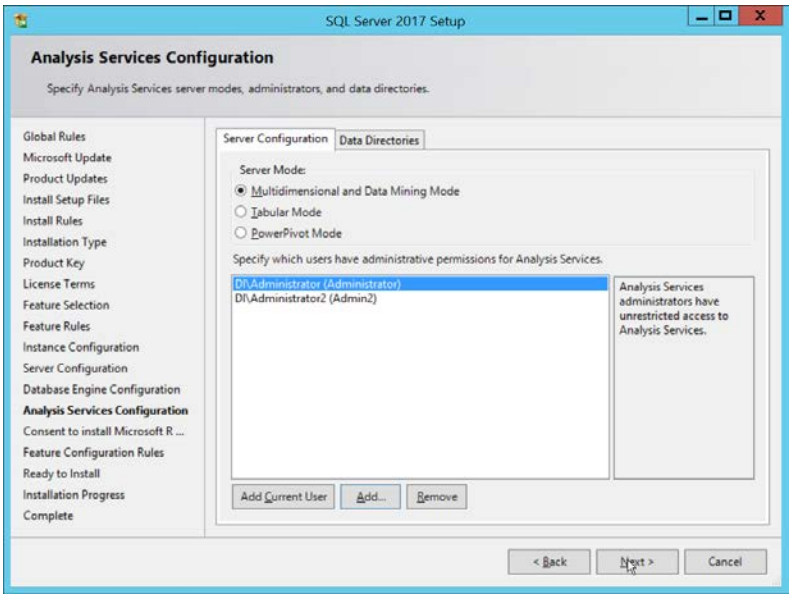
14. Click **Next.**



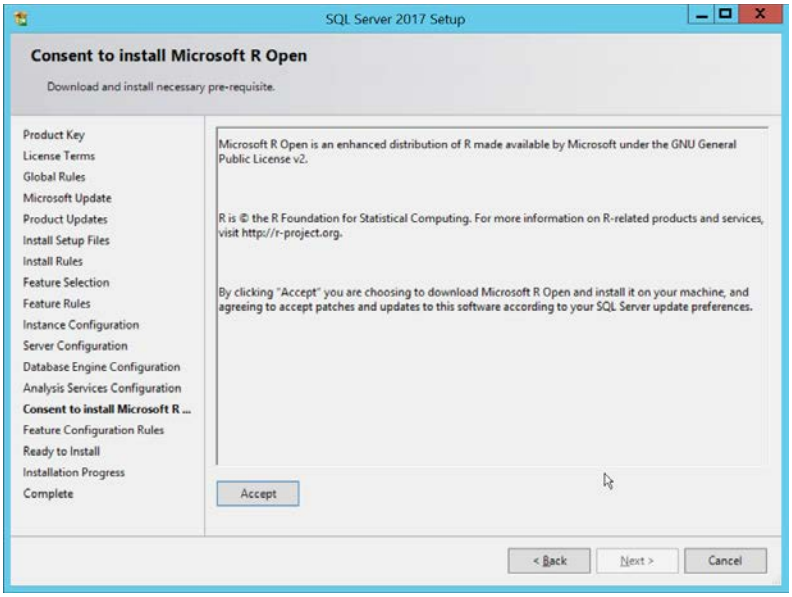
15. Click **Next.**
16. Select **Mixed Mode (SQL Server authentication and Windows authentication).**
17. Enter a **password.**
18. Add any users who should be administrators of the SQL database.



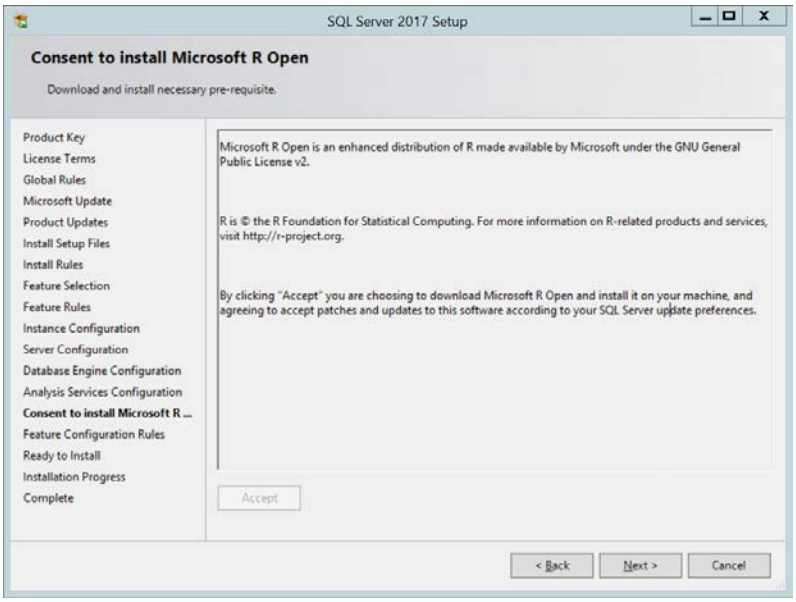
19. Click **Next.**
20. Select **Multidimensional and Data Mining Mode.**
21. Add any users who should be administrators of the Analysis Services.



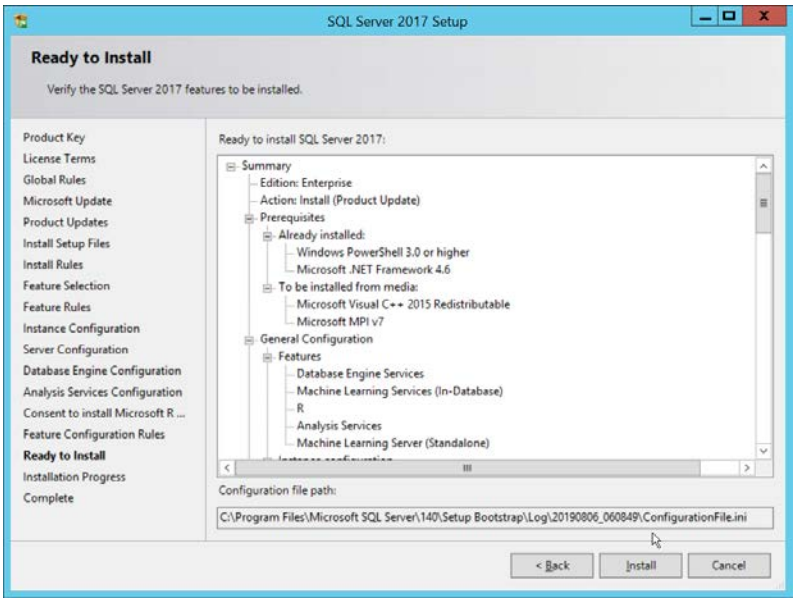
22. Click **Next.**



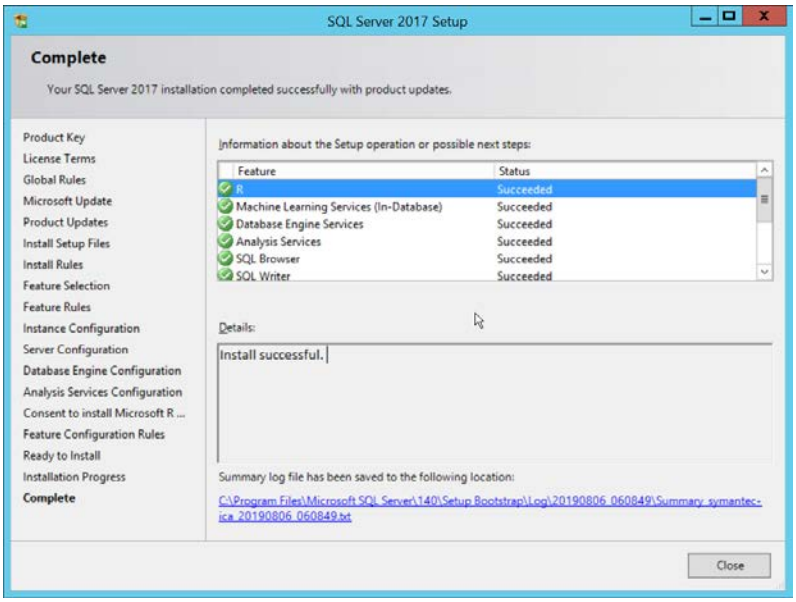
23. Click **Accept.**



24. Click **Next.**



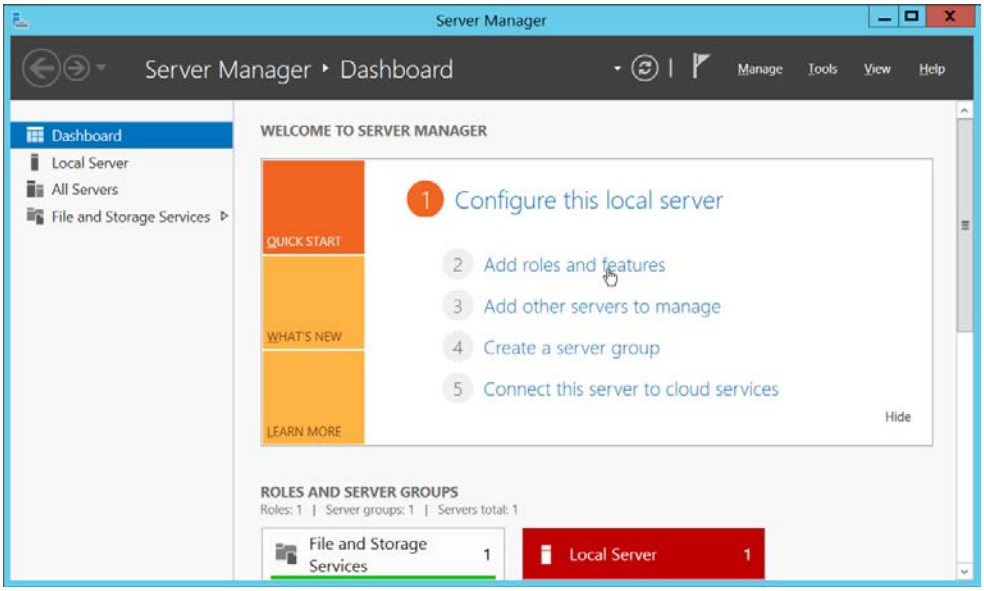
25. Click **Install.**



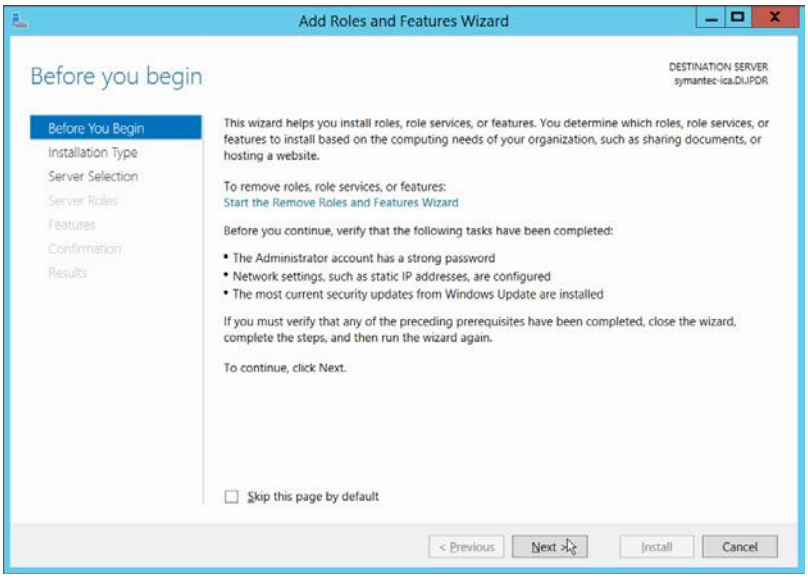
26. Click **Close.**

2.15.2 Install Windows Services

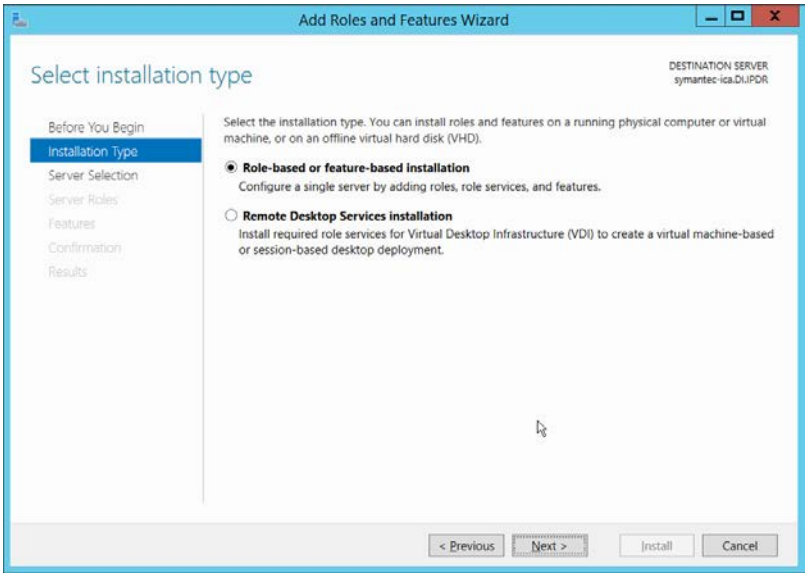
1. Open **Server Manager.**



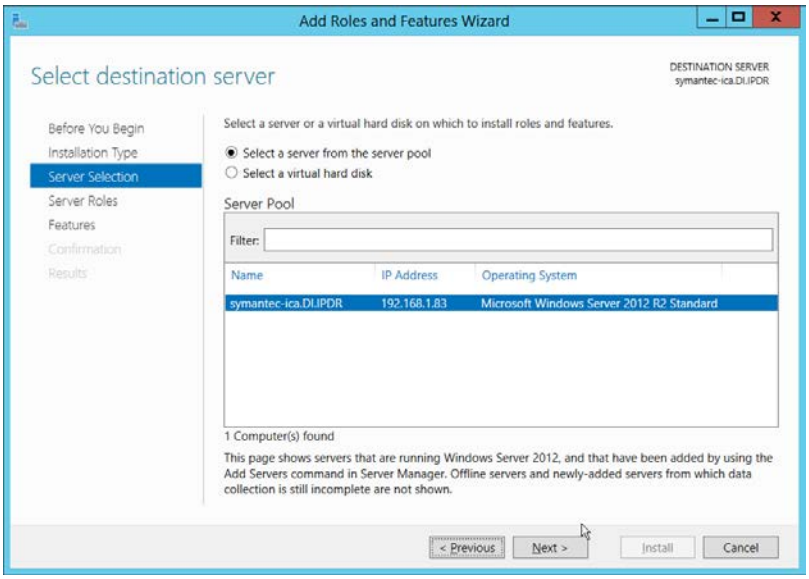
2. Click **Add Roles and Features.**



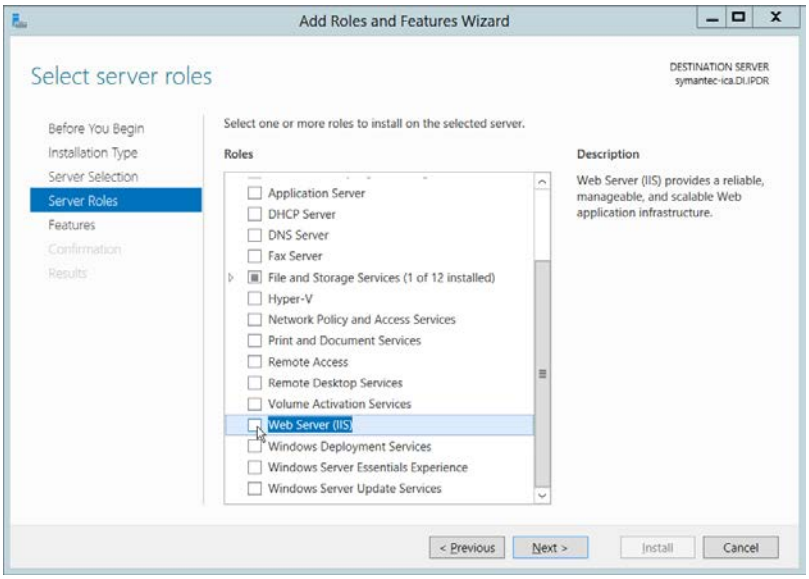
3. Click **Next.**



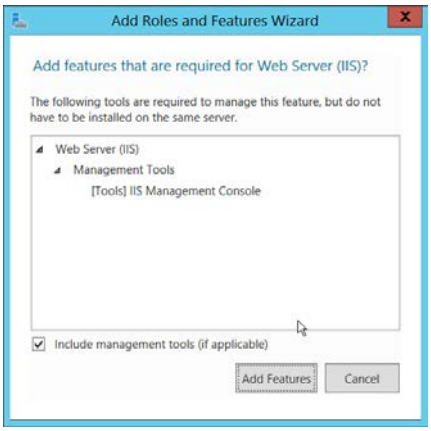
4. Click **Next.**



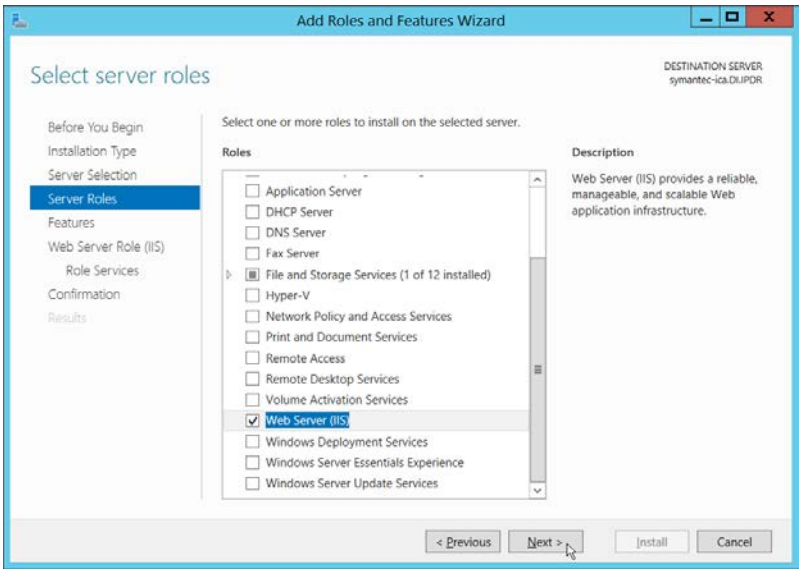
2319
2320 5. Click **Next.**



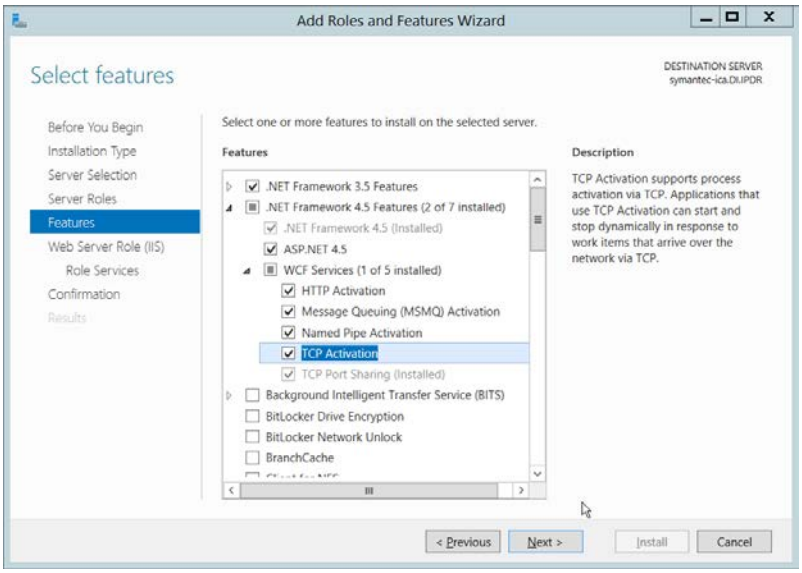
2321
2322 6. Select **Web Server (IIS).**



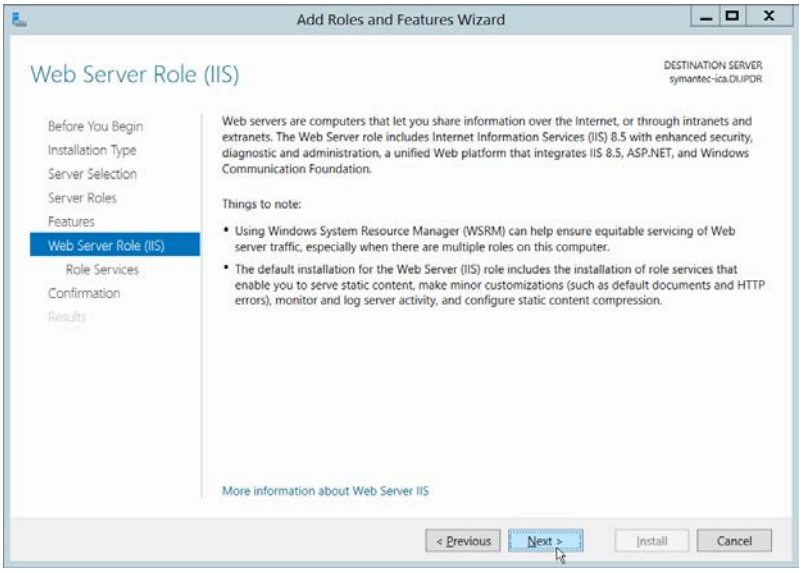
7. Click **Add Features.**



8. Click **Next.**
9. Select all services under **.NET Framework 3.5 Features.**
10. Select all services under **.NET Framework 4.5 Features.**

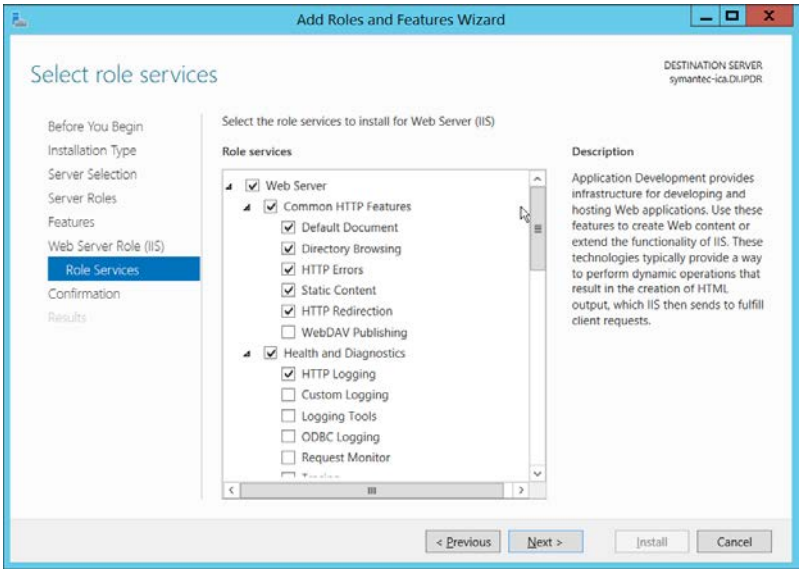


11. Click **Next.**

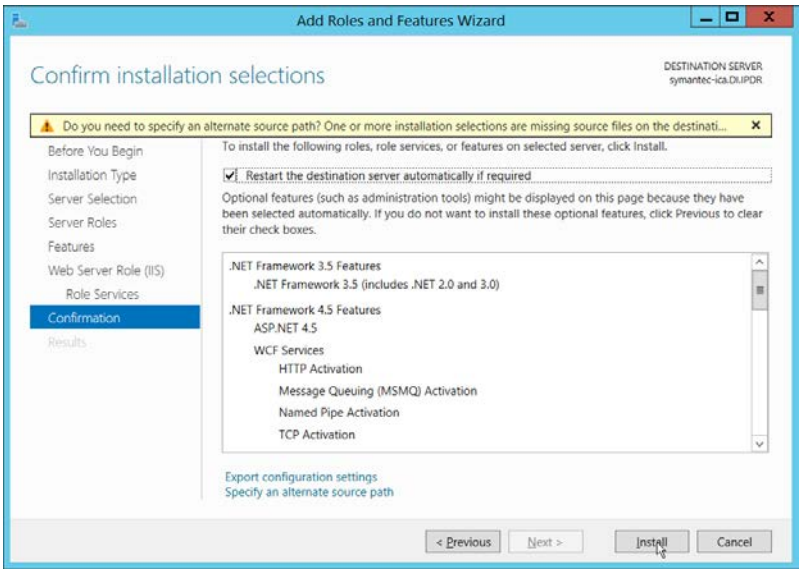


12. Click **Next.**
13. Ensure that the following **Role Services** are selected:
    a. **Common HTTP Features**
        i. **Default Document**
        ii. **Directory Browsing**
        iii. **HTTP Redirection**
    b. **Health and Diagnostics**
        i. **HTTP Logging**
    c. **Performance**

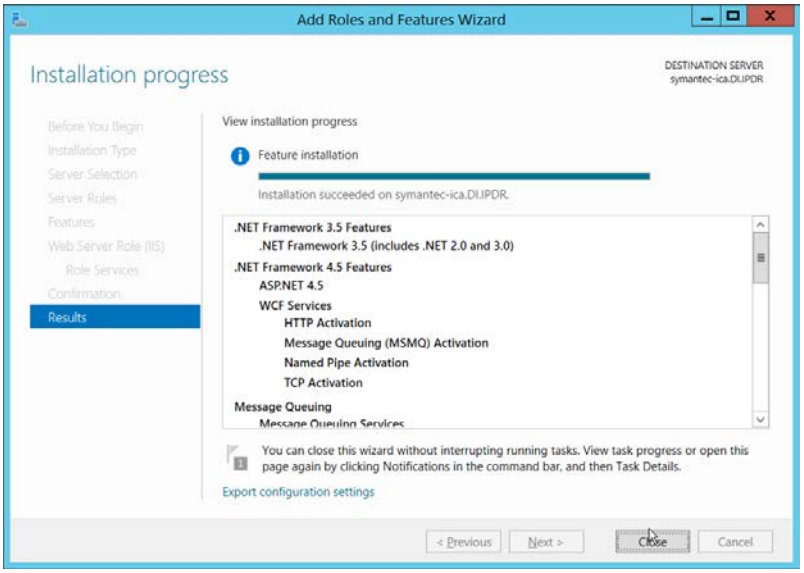
2341 **i. Static Content Compression**
2342 **d. Security**
2343 **i. Windows Authentication**
2344 **e. Application Development**
2345 **i. .NET Extensibility 4.5**
2346 **ii. ASP.NET 4.5**
2347 **iii. ISAPI Extensions**
2348 **iv. ISAPI Filters**



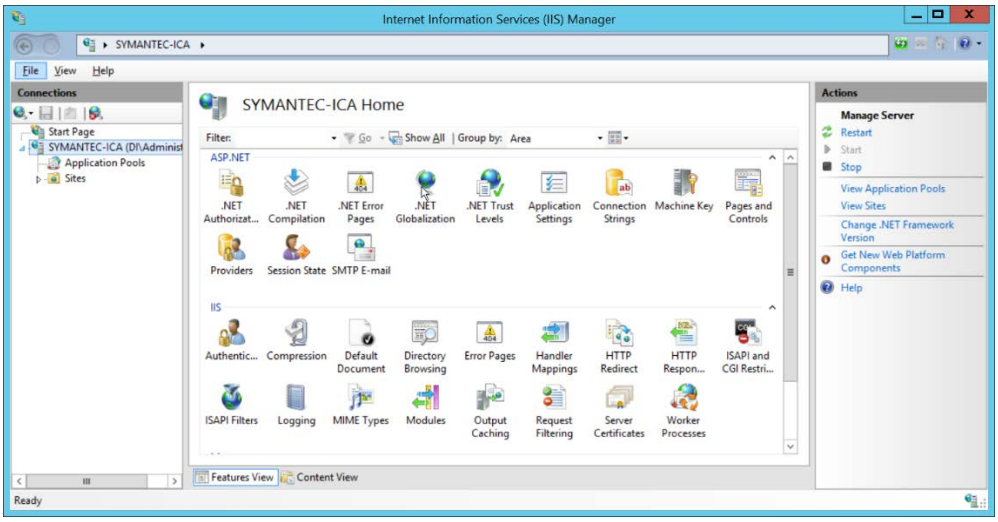
2349
2350 14. Click **Next.**
2351 15. If necessary, specify a path to **/Sources/SxS,** which is found in the Windows Installation Media.
2352 16. Check the box next to **Restart the destination server automatically if required.**



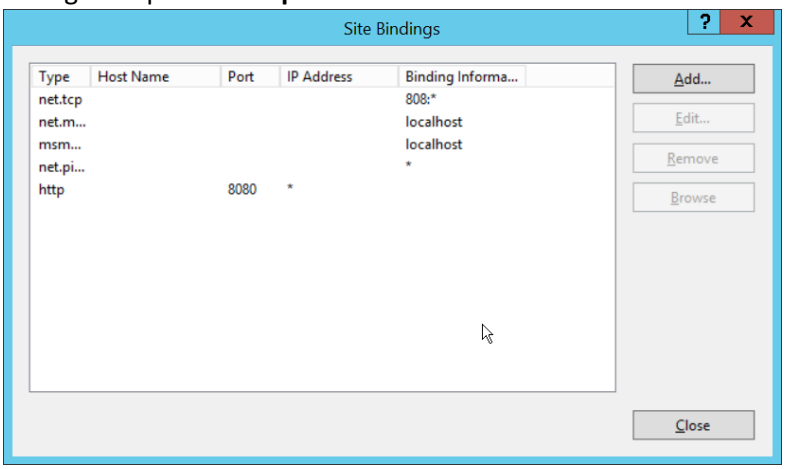
17. Click **Install.**



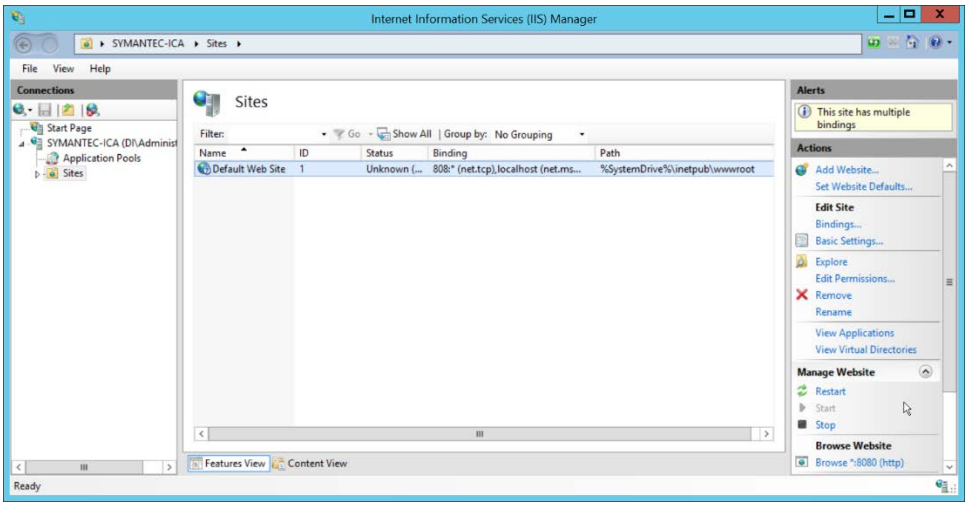
18. Click **Close** when the installation finishes.
19. Open **Internet Information Services Manager.**



20. Navigate to **SERVER-NAME > Sites.**
21. Right-click the **Default Web Site,** and select **Bindings.**
22. Change the port for **http** to **8080.**



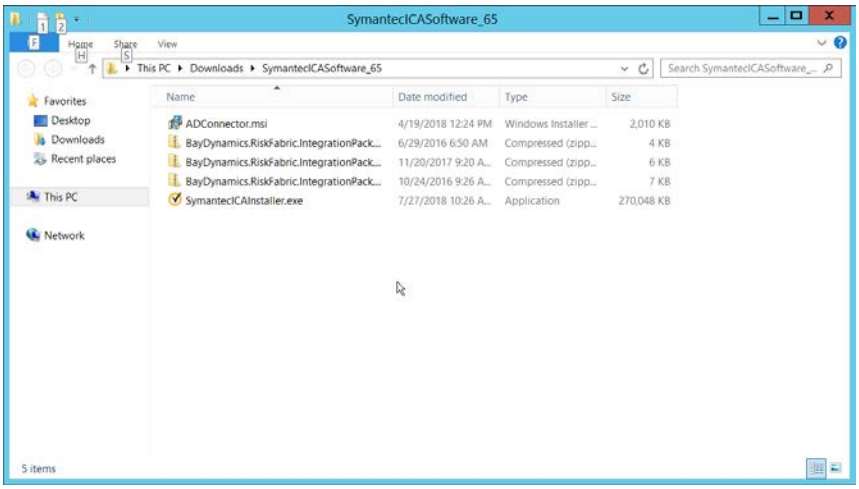
23. Click **Close.**



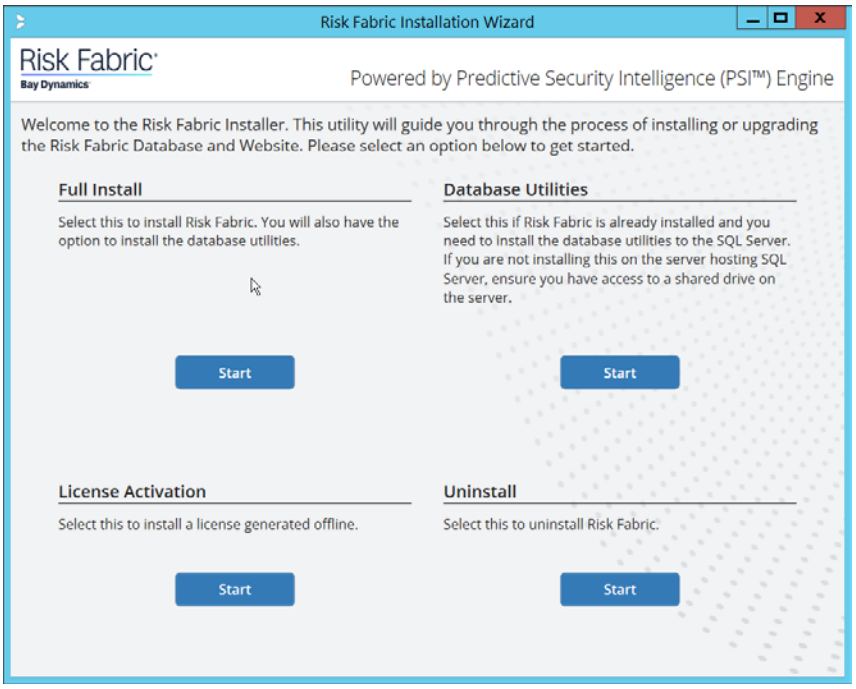
24. Click **Restart** under **Manage Website.**

2.15.3 Installing Symantec ICA

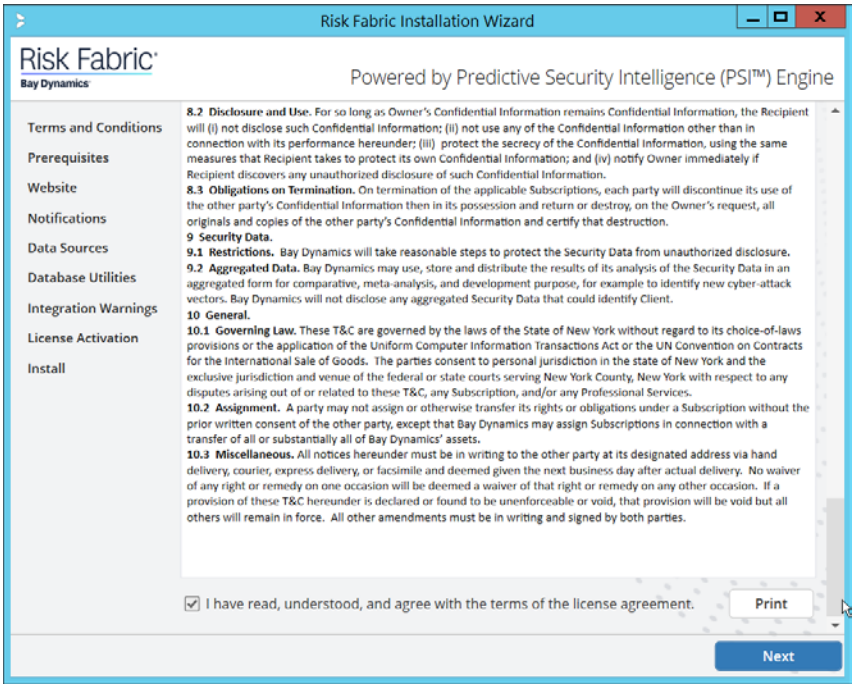
1. In Task Manager, verify that the **SQL Server Agent** service is running.
2. Copy the installation media **SymantecICASoftware_65.zip** onto the server.
3. Extract the installation media.



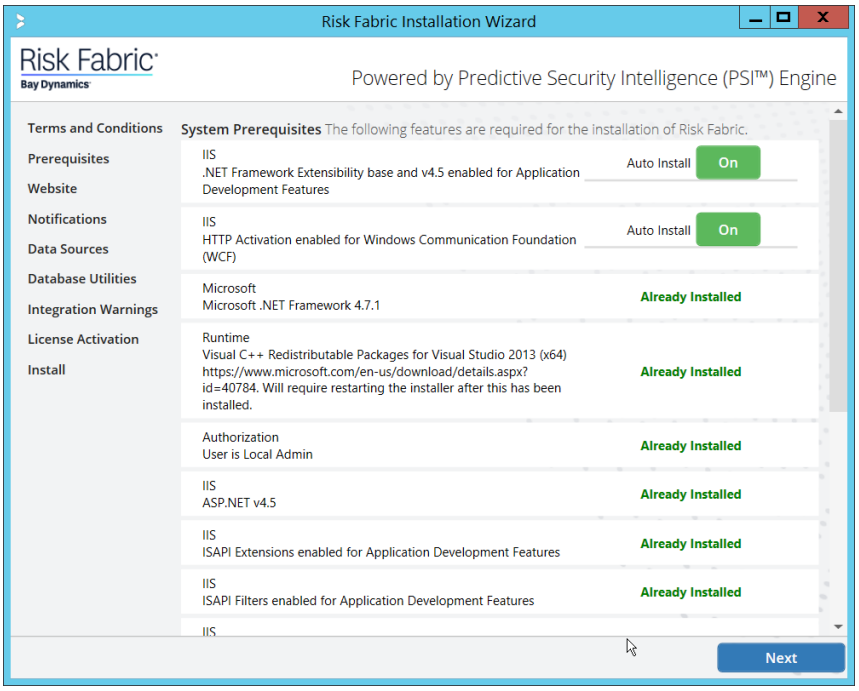
4. Run **SymantecICAInstaller.exe.**



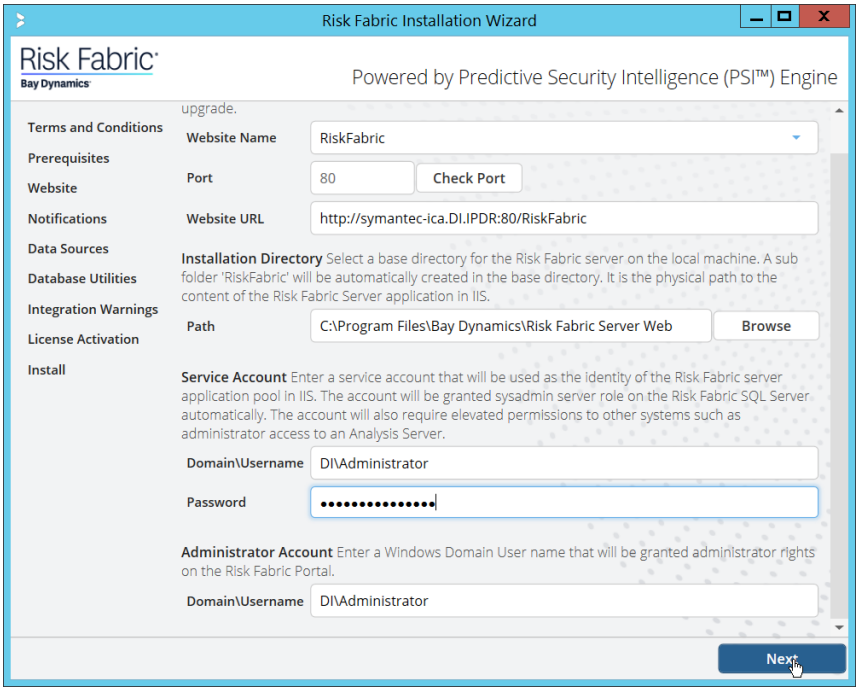
5. Under **Full Install,** click **Start.**
6. Scroll down and check the box next to **I have read, understood, and agree with the terms of the license agreement.**



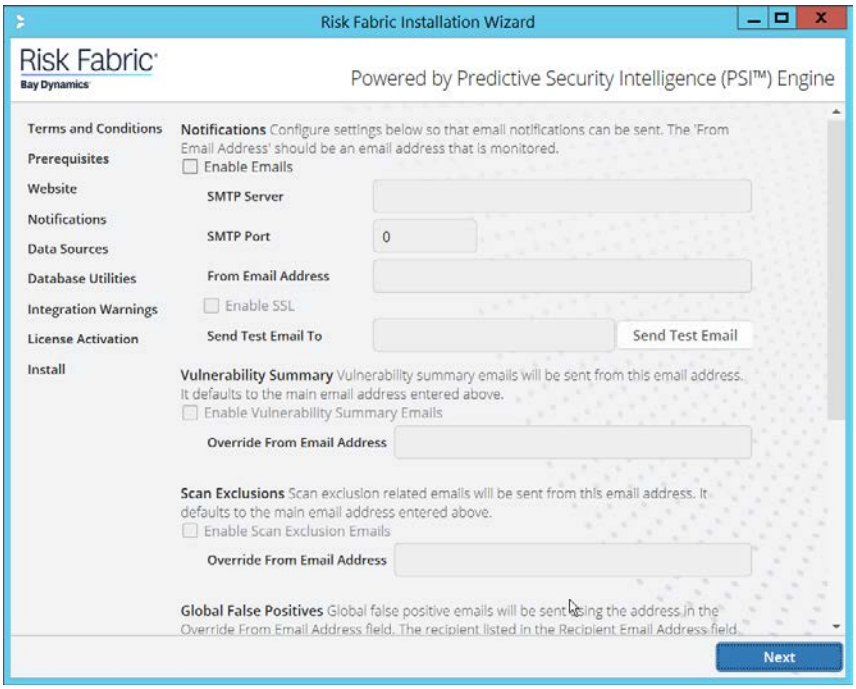
7. Click **Next.**



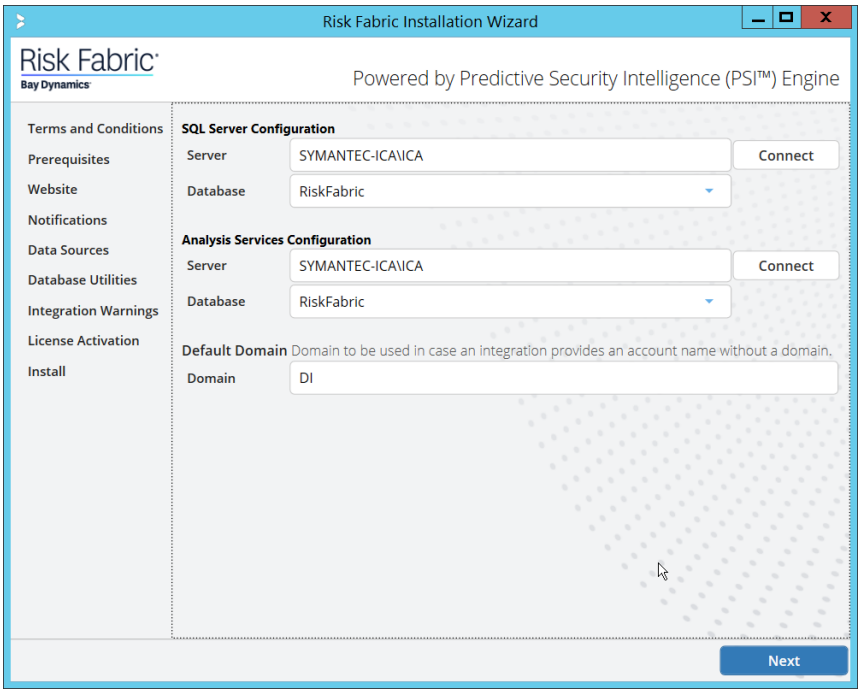
8. Click **Next.**
9. Enter a username and password with privileges on the domain.



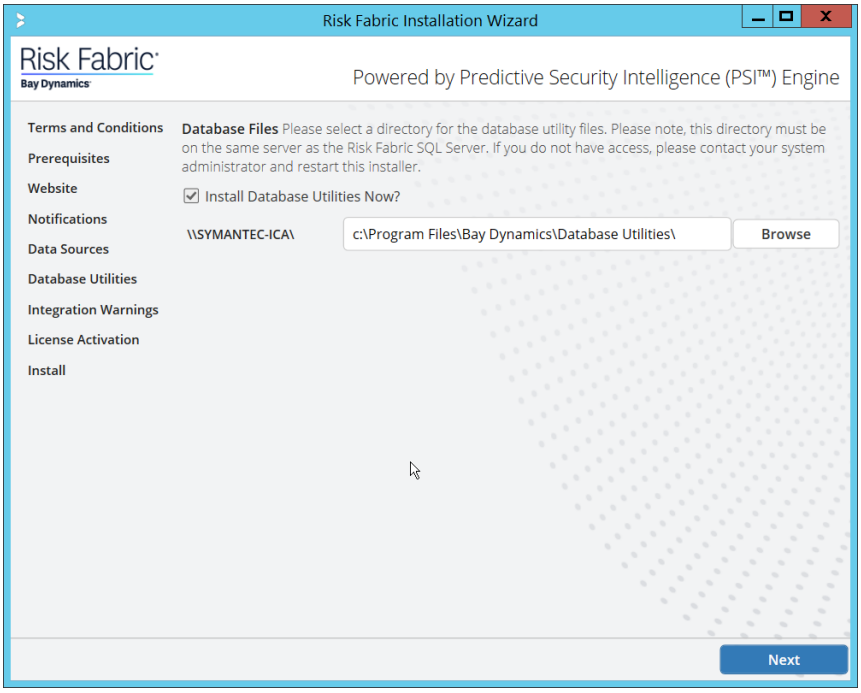
10. Click **Next.**
11. Configure any alert settings desired; these can be changed later.



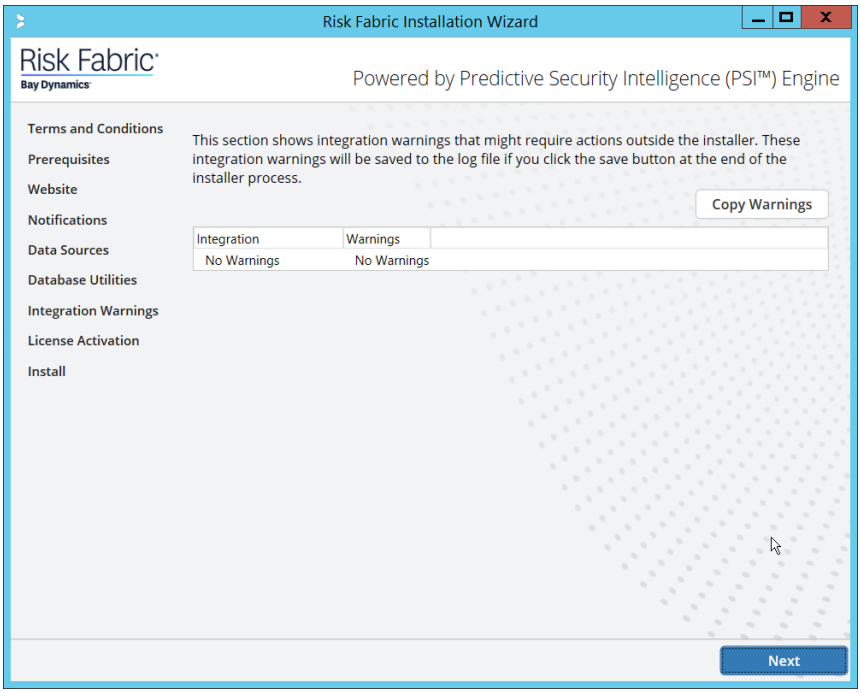
12. Click **Next.**
13. Enter the name of the SQL Server you created in the format **<SERVER-DOMAIN-NAME>\<SQL-SERVER-NAME>.**
14. Click **Connect,** and verify that there are no connection issues.
15. Enter the name of the SQL Analysis Services server you created in the format **<SERVER-DOMAIN-NAME>\<SQL-SERVER-NAME>.** (It may be the same as the SQL Server).
16. Click **Connect,** and verify that there are no connection issues.



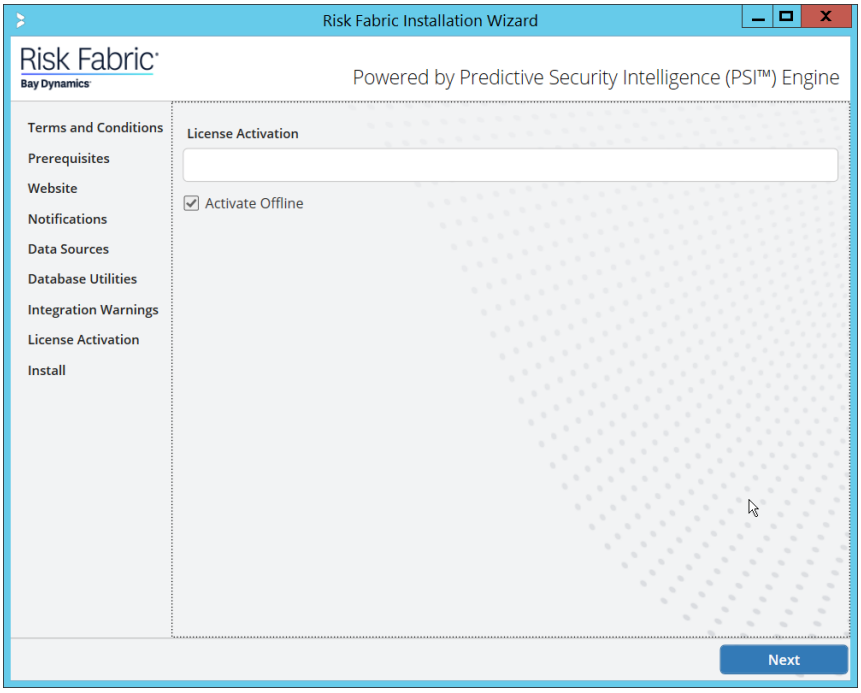
17. Click **Next.**



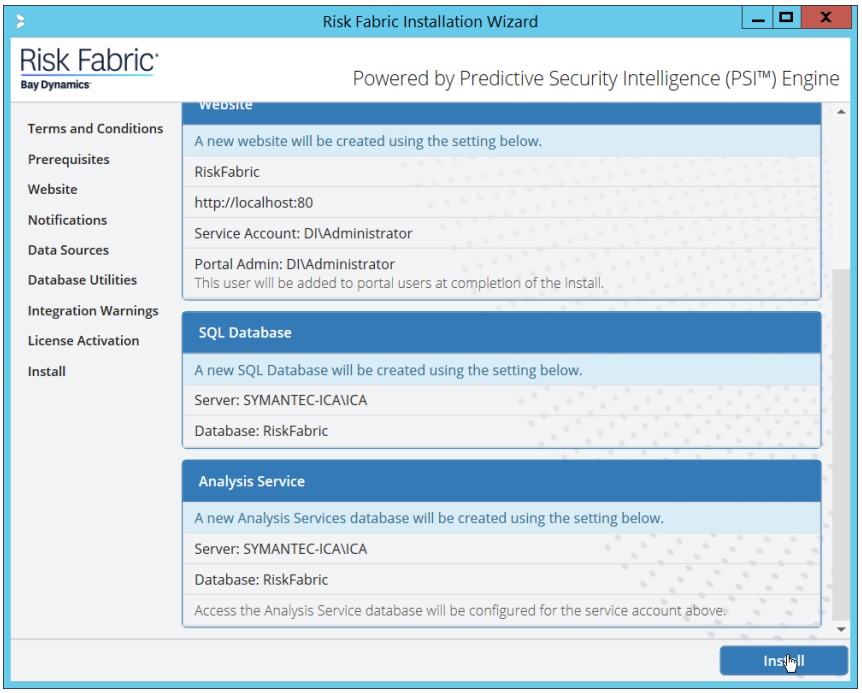
18. Click **Next.**



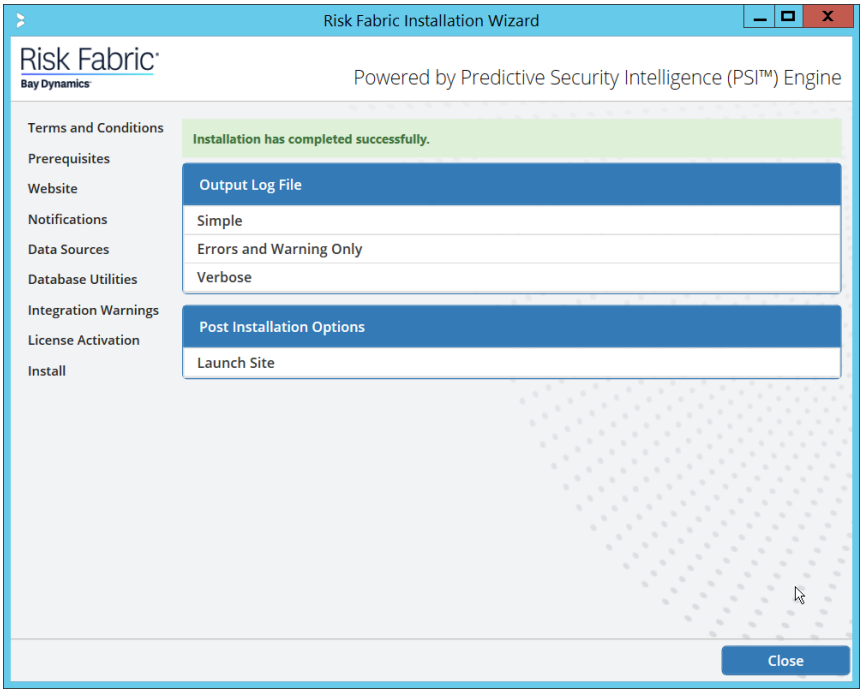
19. Click **Next.**
20. Check the box next to **Activate Offline.**



21. Click **Next.**



22. Click **Install.**



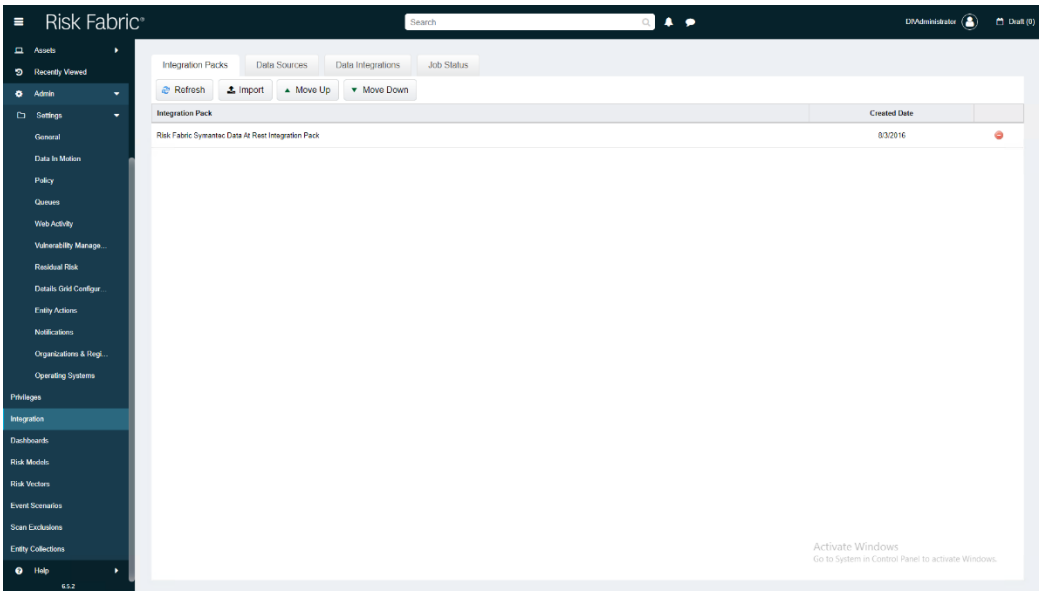
23. Click **Close.**

2.15.4 Configuring Symantec ICA for Analysis

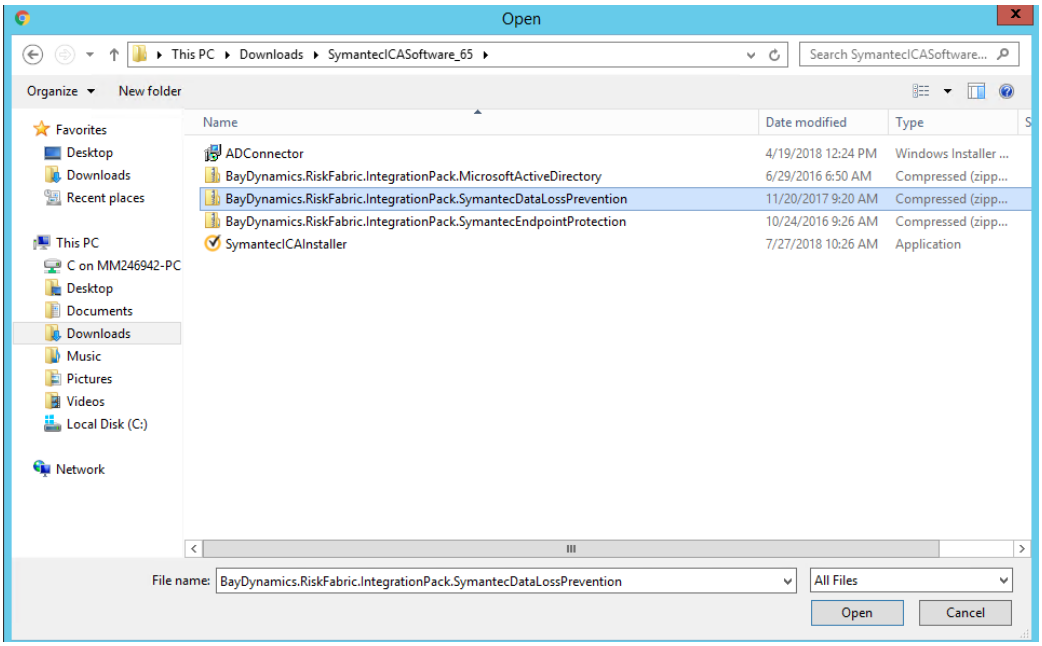
This section will contain instructions for navigating some aspects of the ICA admin console and dashboards, though this largely depends on the specific data your organization has identified and is trying to analyze.

2.15.4.1 *Installing Integration Packs*

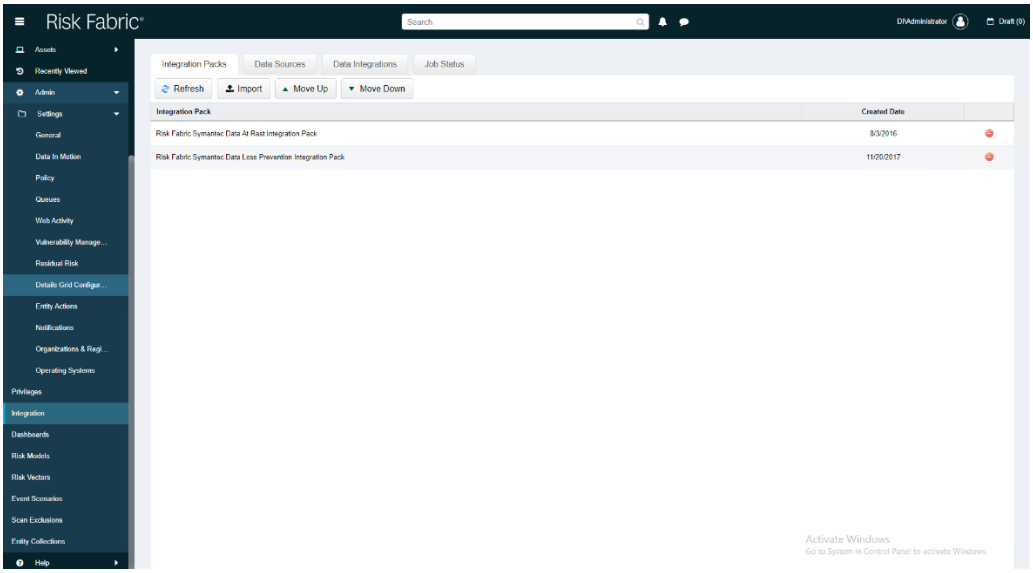
1. Download the relevant integration packs to someone on the local system. These are typically provided by Symantec, in a zip file. The zip file should be titled in the format of *BayDynamics.RiskFabric.IntegrationPack.<productName>.*
2. Log in to the Risk Fabric web interface.
3. Navigate to **Admin > Integration.**



4. Click **Import.**
5. Find the zip file for the integration pack that you downloaded earlier.

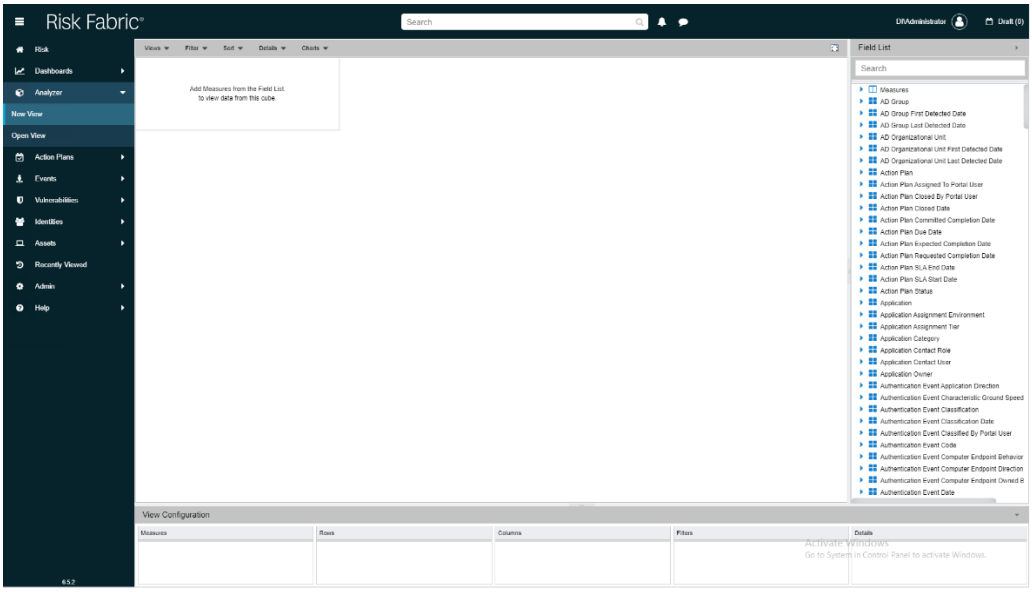


6. Select the file and click **Open.**

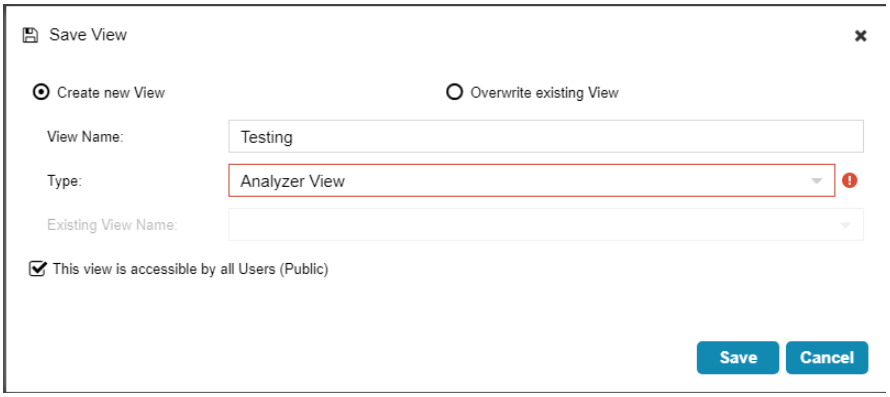


2.15.4.2 *Create a View*

1. Navigate to **Analyzer > New View.**



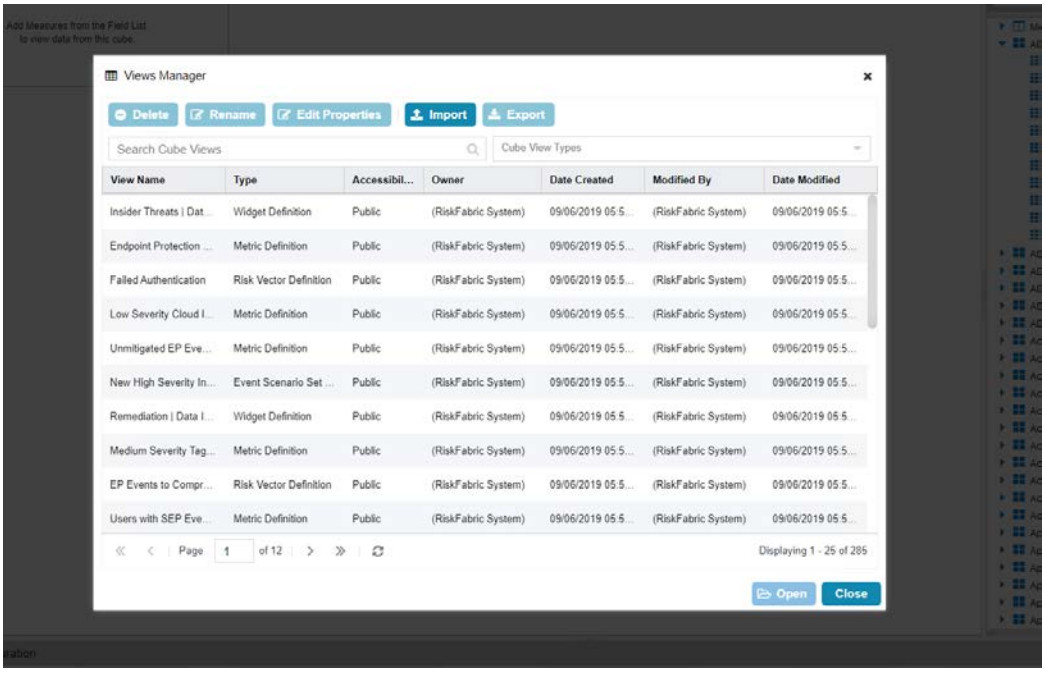
2. In the field list on the right, manually select or search for the data fields desired.
3. The fields can be added either by dragging the field onto the screen or by right-clicking on the field and selecting where it should be added. Ultimately, which views to select depends on the needs and preferences of your organization.
4. When finished, click **Save.**
5. Enter a name for the **View Name.**
6. Select the type of View for **Type.**
7. Check the box next to **This view is accessible by all Users (Public)** only if you wish for this view to be visible by anyone logged in.



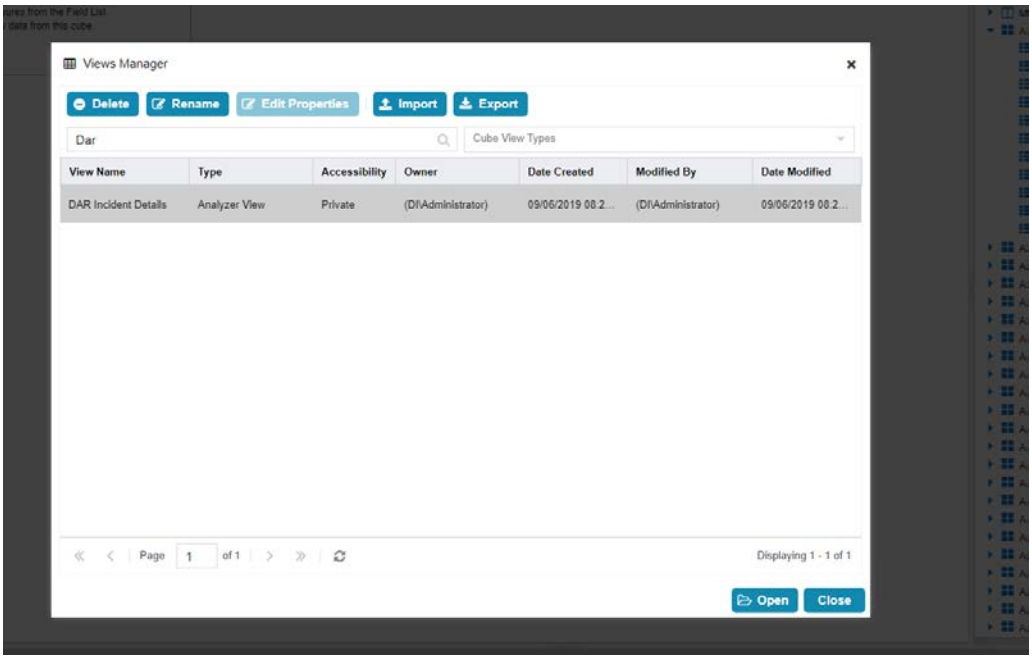
8. Click **Save.**

2.15.4.3 *Open an Existing View*

1. Navigate to **Analyzer > Open View.**



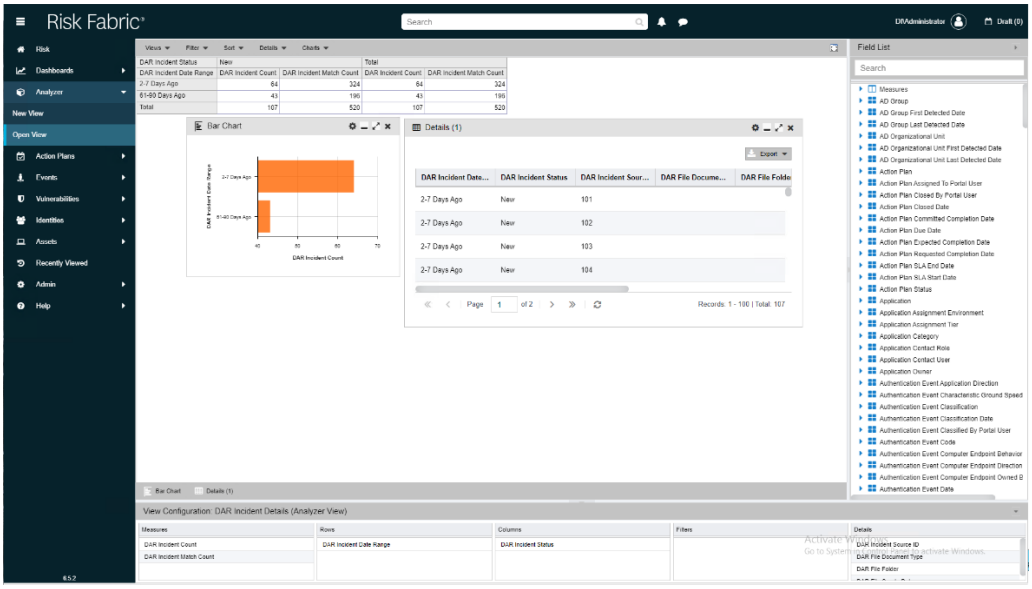
2. Begin to search for the view you want by typing a search term into **Search Cube Views.** (Note: if you created a view, it will also be present in this list).
3. Click the **Search** icon.
4. Select a view.



5. Click **Open.**

2.15.4.4 *Viewing Detailed Analyzer Data*

1. The desired field data can be exported to either a *.csv* or *.excel* format, by clicking on the **Export** button in the details tab.



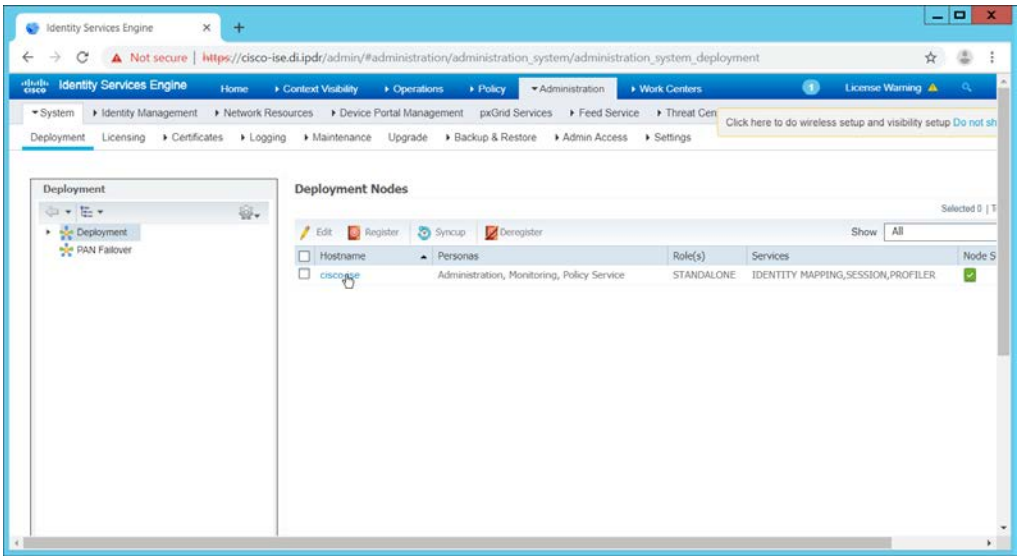
2. Charts can be added or removed using the **Charts** dropdown menu near the top of the analyzer.
3. Any data in the **Field List** on the right side can be added to or removed from the view and will be automatically incorporated into its relevant rows or columns.
4. The entire view format can be exported as a *.json* file from the **Open View** option.

2.16 Integration: Cisco Identity Services Engine and Cisco Stealthwatch

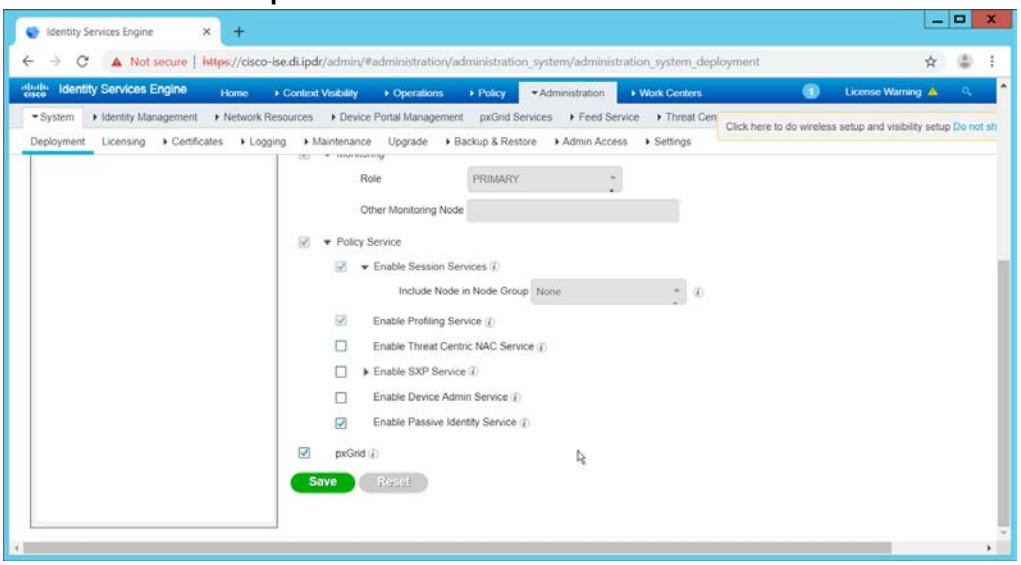
This section will detail an integration between Cisco Identity Services Engine (ISE) and Cisco Stealthwatch, allowing Stealthwatch to apply certain policies to hosts in ISE. Stealthwatch acts as a network monitoring solution and can be integrated with ISE to enable mitigation capabilities in response to events. Please see *Deploying Cisco Stealthwatch 7.0 with Cisco ISE 2.4 using pxGrid* for details and other potential uses of the integration.

2.16.1 Configuring Certificates for pxGrid

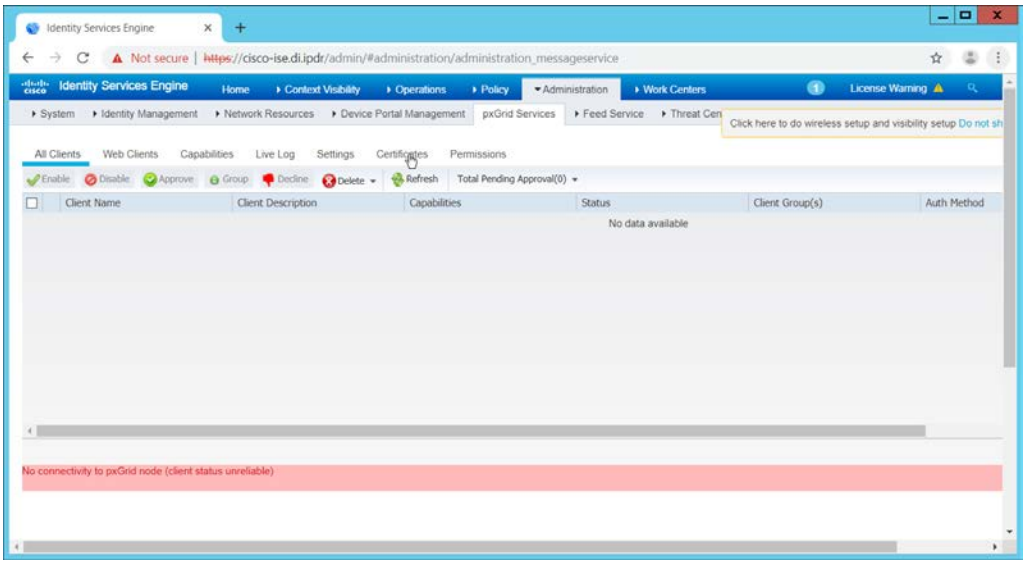
1. Log in to the Cisco ISE web console in a browser.
2. Navigate to **Administration > System > Deployment.**



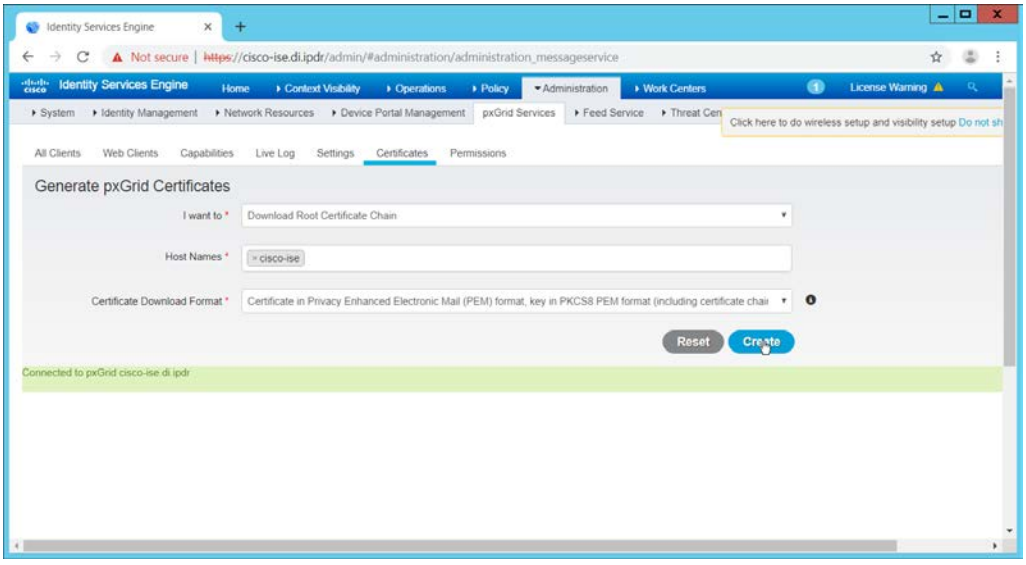
3. Click the hostname of the Cisco ISE machine.
4. Check the box next to **pxGrid.**



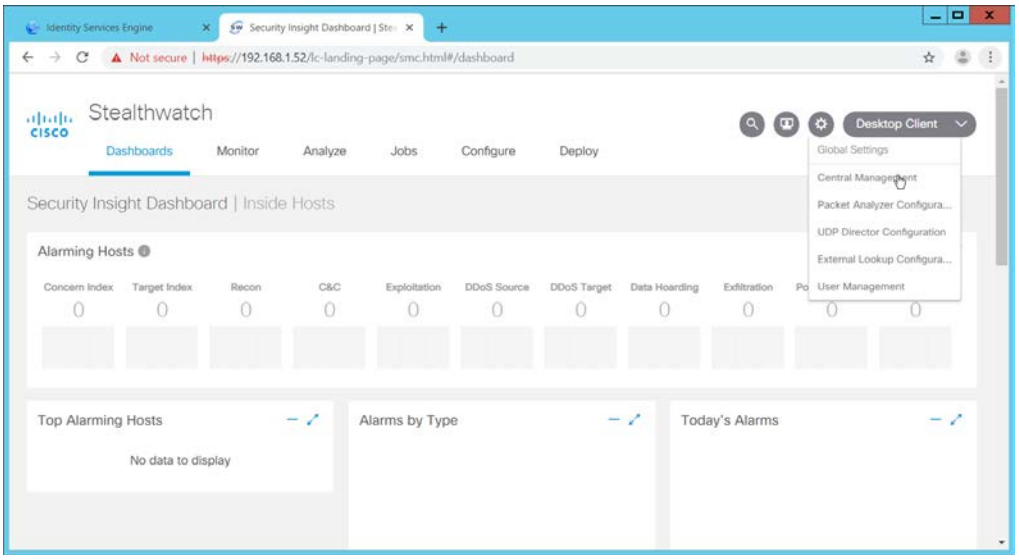
5. Click **Save.**
6. Navigate to **Administration > pxGrid Services.**



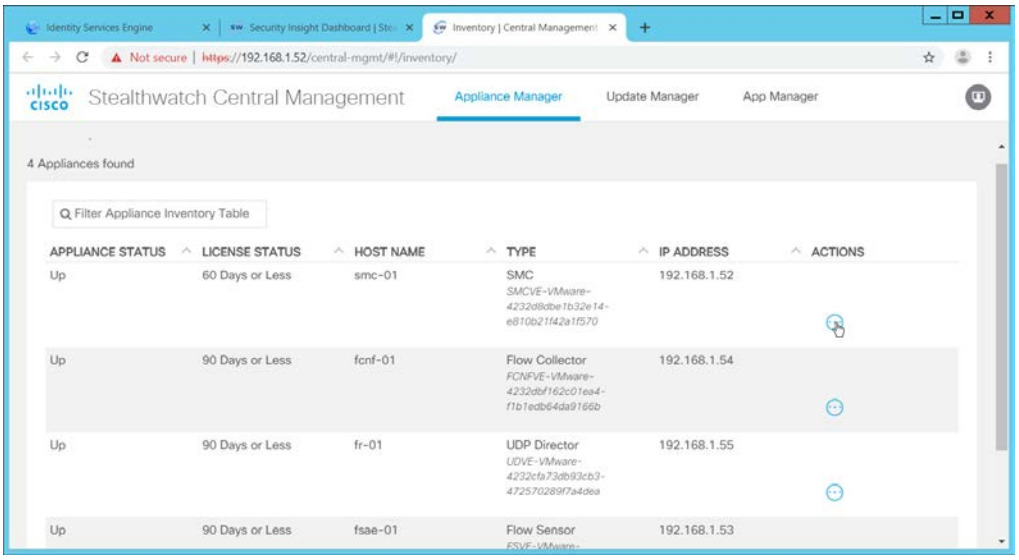
7. Click **Certificates.**
8. Select **Download Root Certificate Chain** for **I want to.**
9. Select the hostname of the Cisco ISE server for **Host Names.**
10. Select **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PLCS8 PEM format (including certificate chain)** for **Certificate Download Format.**



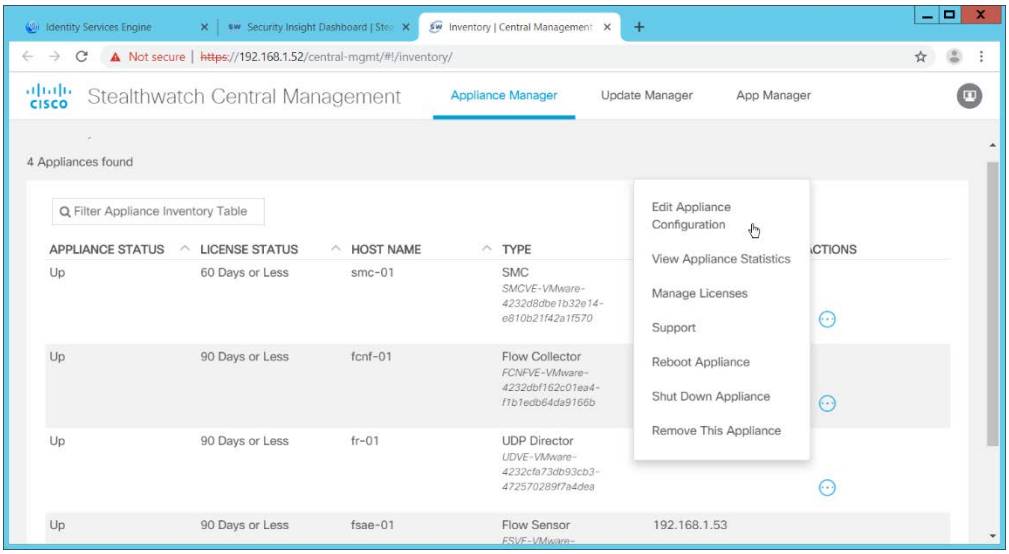
11. Click **Create.** This will download a zip file containing the certificate.
12. Extract the zip file—it may contain several files—the one we are interested in is the Root CA.
13. Log in to the **Stealthwatch Management Console** through the browser.



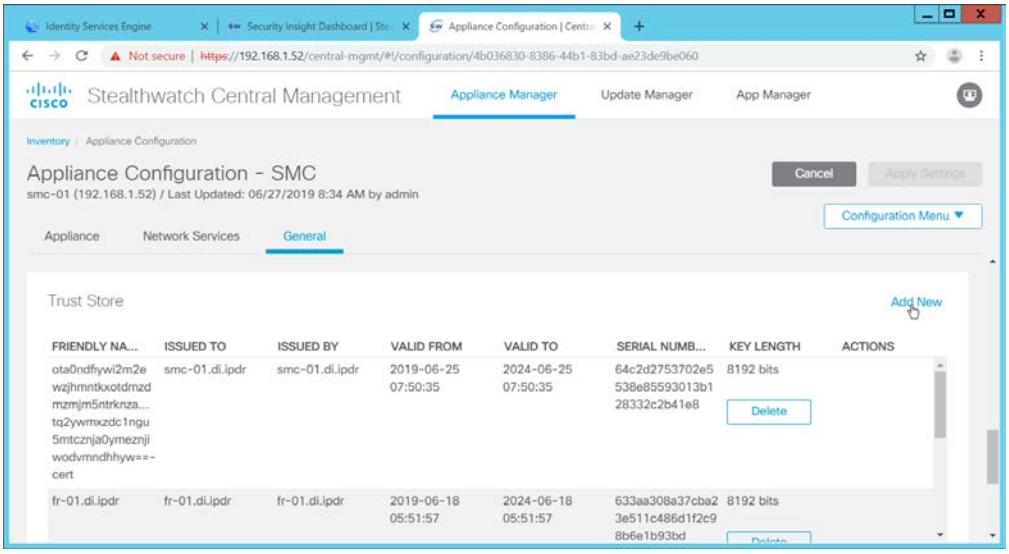
2477
2478 14. In the top right corner of the console, hover over the **gear icon** and select **Central Management**
2479 from the submenu.



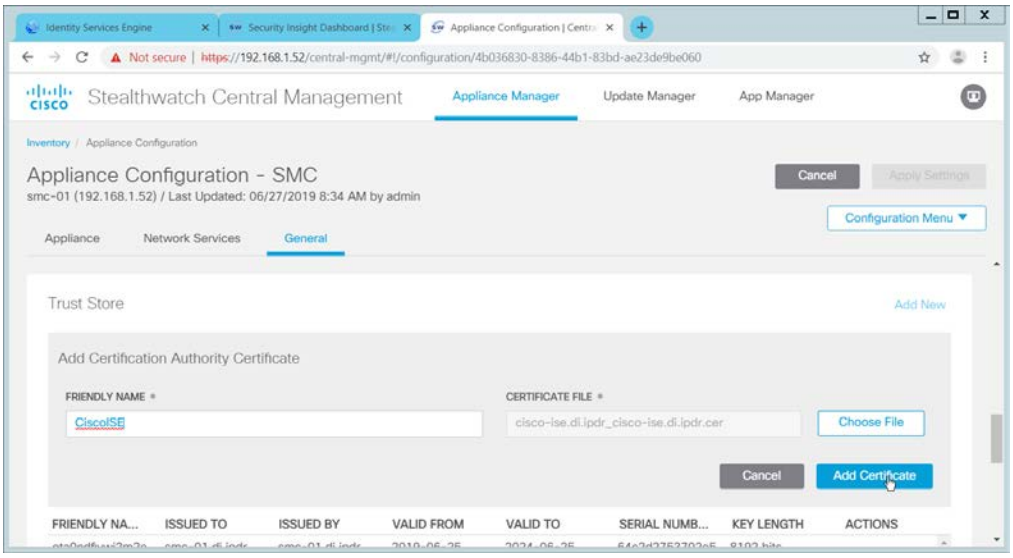
2480
2481 15. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC).
2482 Click the **ellipses button** in the **Actions** column.



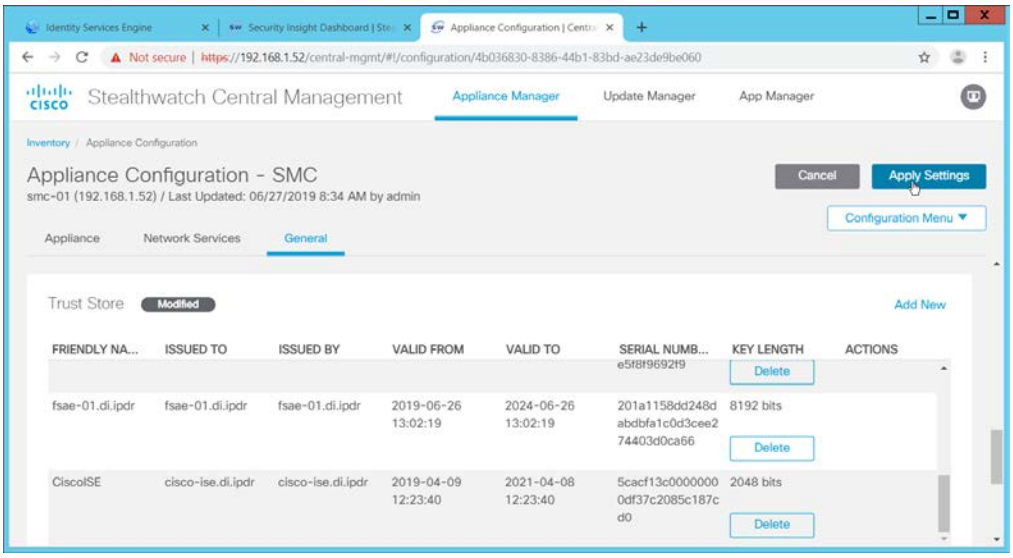
16. This will open a submenu. Select **Edit Appliance Configurations.**
17. Click the **General** tab.
18. Scroll down to the **Trust Store** section.



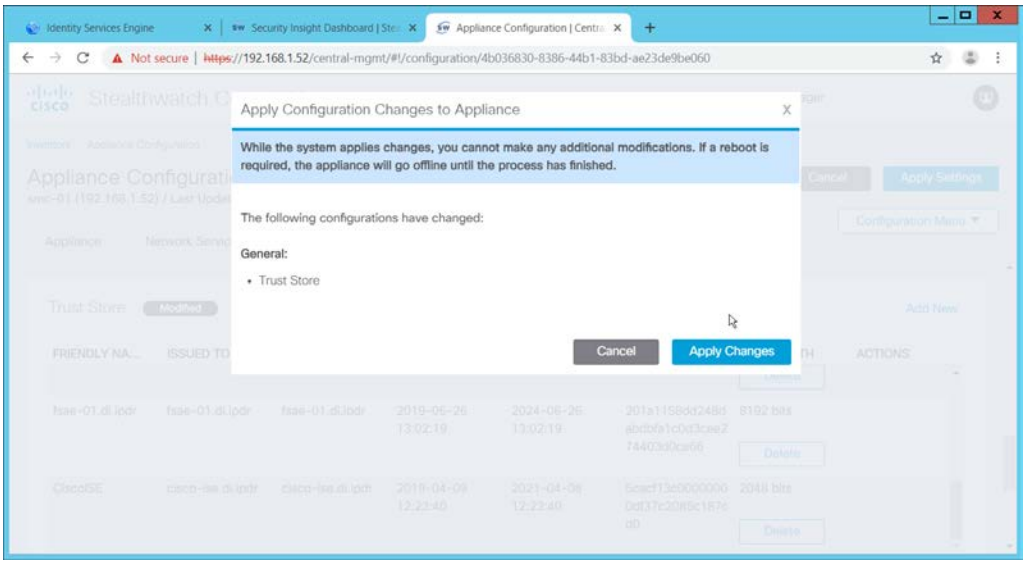
19. Click **Add New.**
20. Enter a **name.**
21. Click **Choose File.**
22. Select the Cisco ISE Root certificate from the files downloaded earlier.



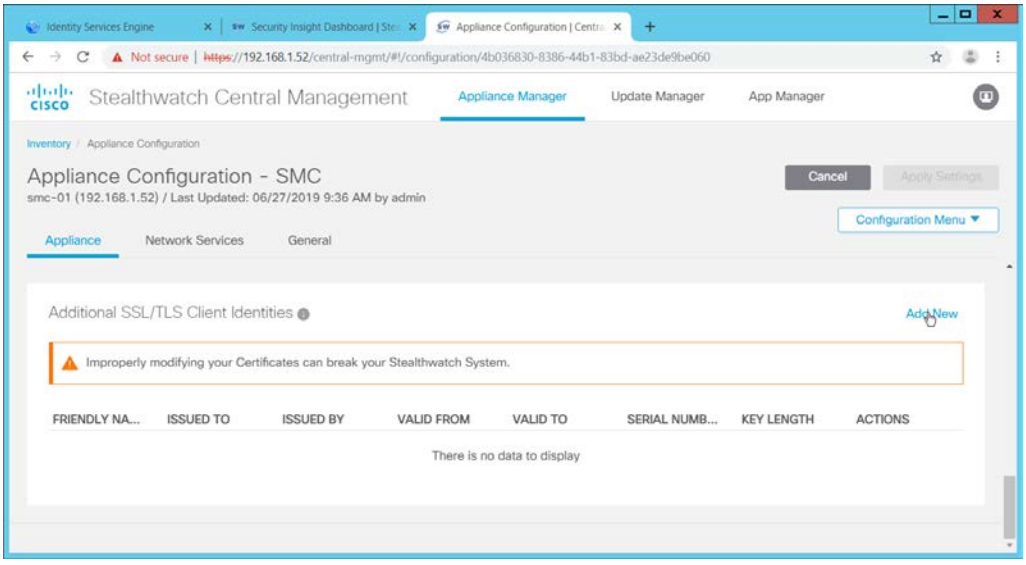
23. Click **Add Certificate.**



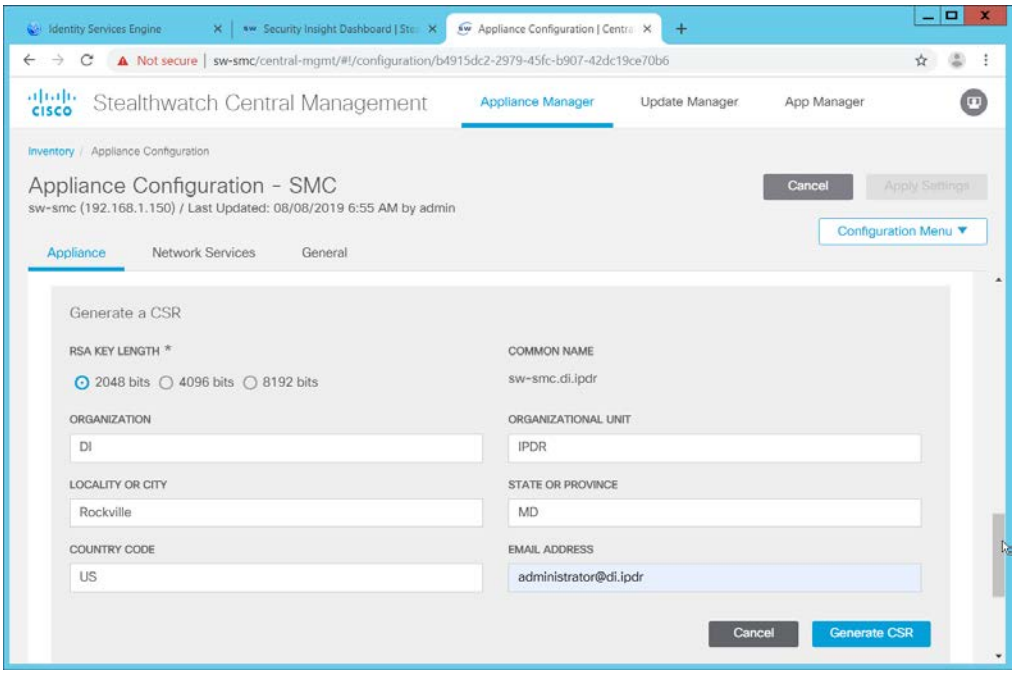
24. Click **Apply Settings.**



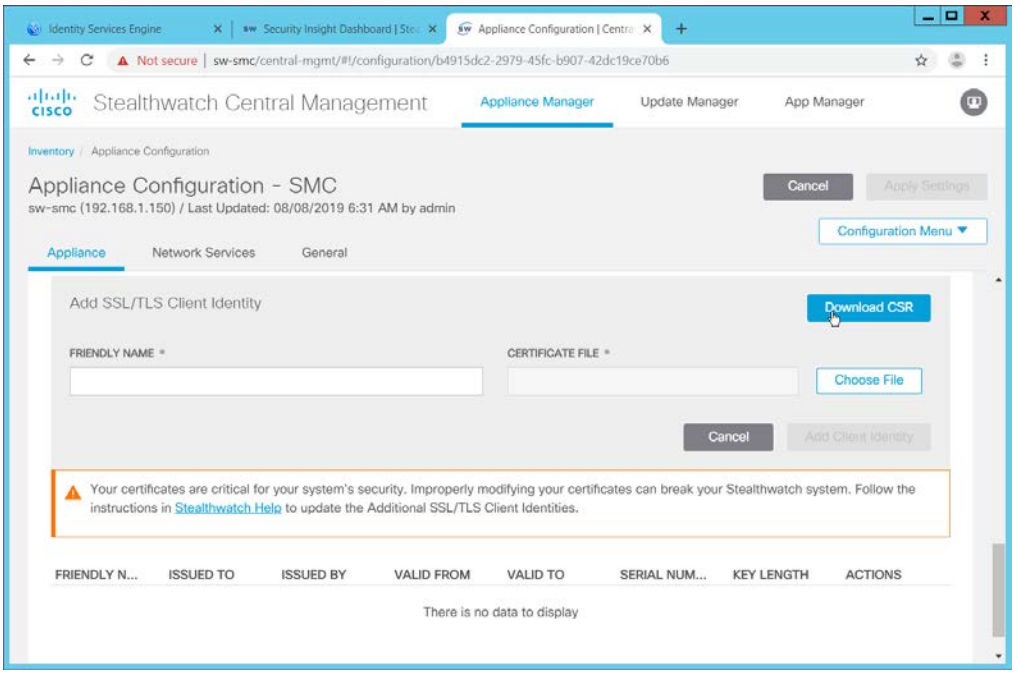
25. Click **Apply Changes** if prompted to confirm the changes.
26. When that finishes, navigate back to the **Appliance Configurations** section.
27. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.
28. This will open a submenu. Select **Edit Appliance Configurations.**



29. Click **Add New** under **Additional SSL/TLS Client Identities.**
30. Select **2048** for **RSA Key Length.**
31. Enter your organization's information.

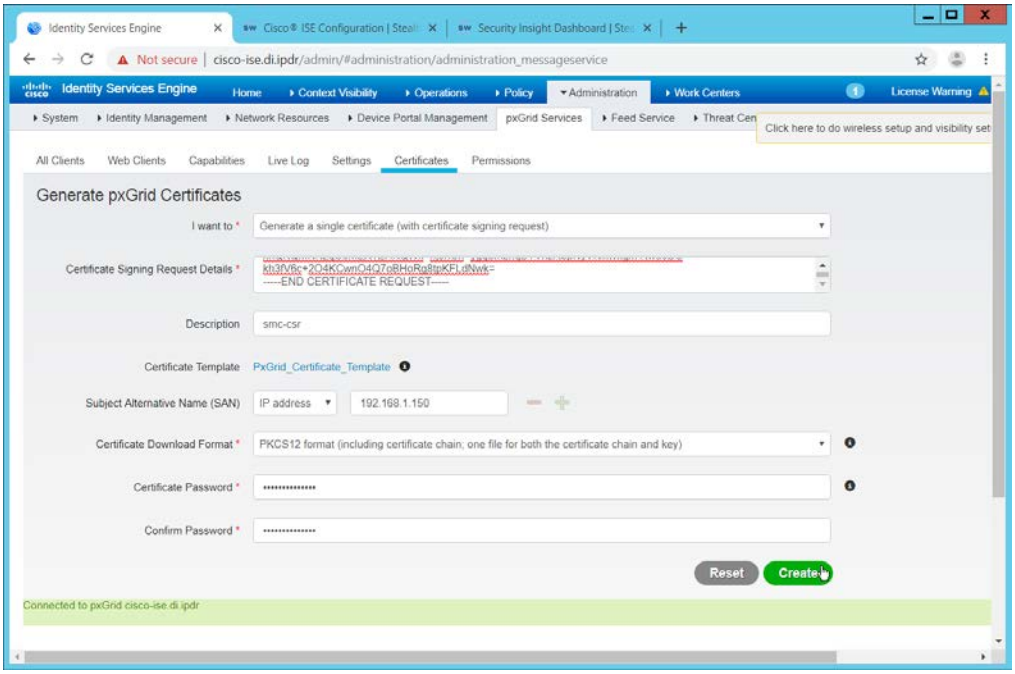


32. Click **Generate CSR.**

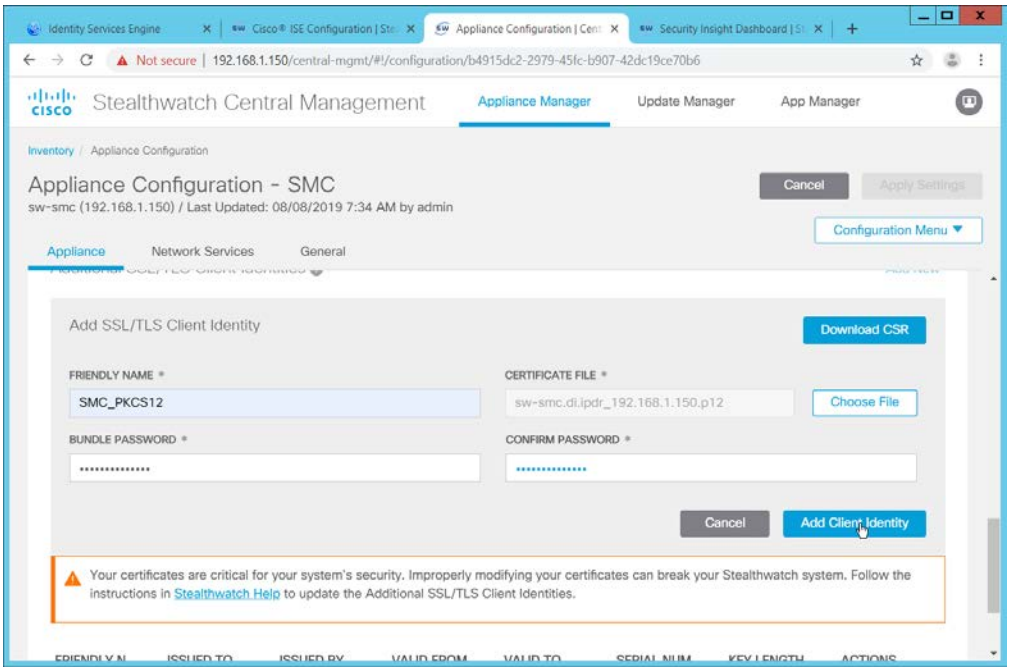


33. When this finishes, click **Download CSR.**
34. Open the CSR in a text file, and copy all the contents.
35. On the ISE web console, navigate to **Administration > pxGrid Services > Certificates > Generate pxGrid Certificates.**

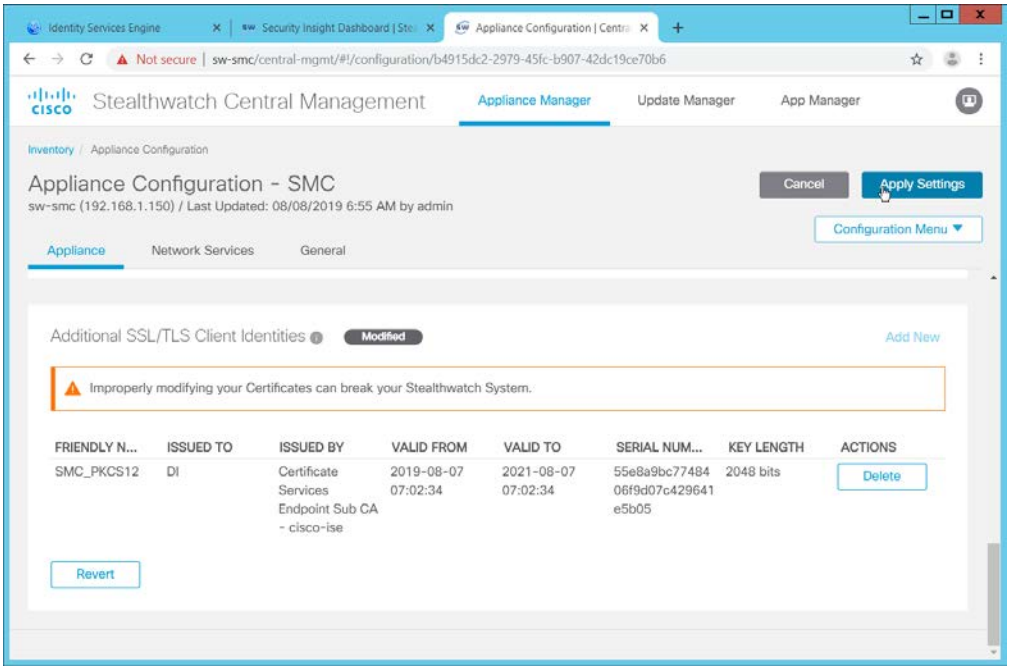
36. Select **Generate a single certificate (with certificate signing request)** for **I want to.**
37. Paste the copied text into the **Certificate Signing Request Details.**
38. Enter a description such as **SMC** for the **Description.**
39. Select **IP Address** for **Subject Alternative Name (SAN).**
40. Enter the **IP Address** of the Stealthwatch Management Console.
41. Select **PKCS12 format (including certificate chain; one file for both the certificate chain and key)** for **Certificate Download Format.**
42. Enter a password, and confirm the password.



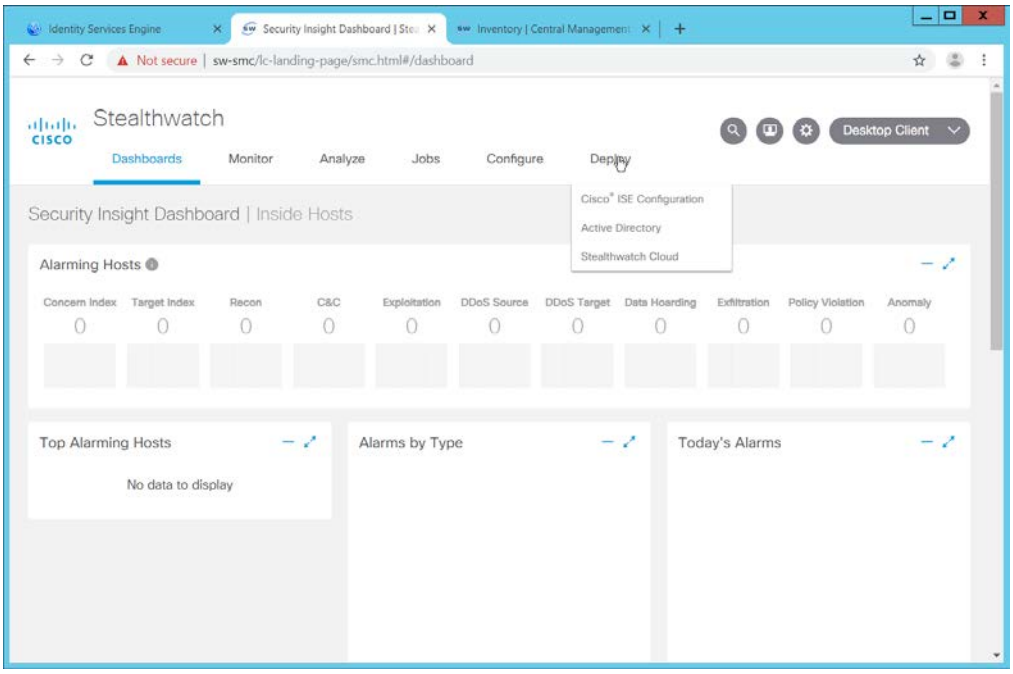
43. Click **Create.**
44. This will download a zip file. Unzip the file.
45. On the Stealthwatch Management Console (SMC) web console, under **Additional SSL/TLS Client Identities** (where you downloaded the CSR), click **Choose File.**
46. Upload the certificate file from the zip file that has the hostname of the SMC in it; the file extension should be *.p12.*
47. Enter a name for **Friendly Name.**
48. Enter the password used in ISE when generating the certificate.



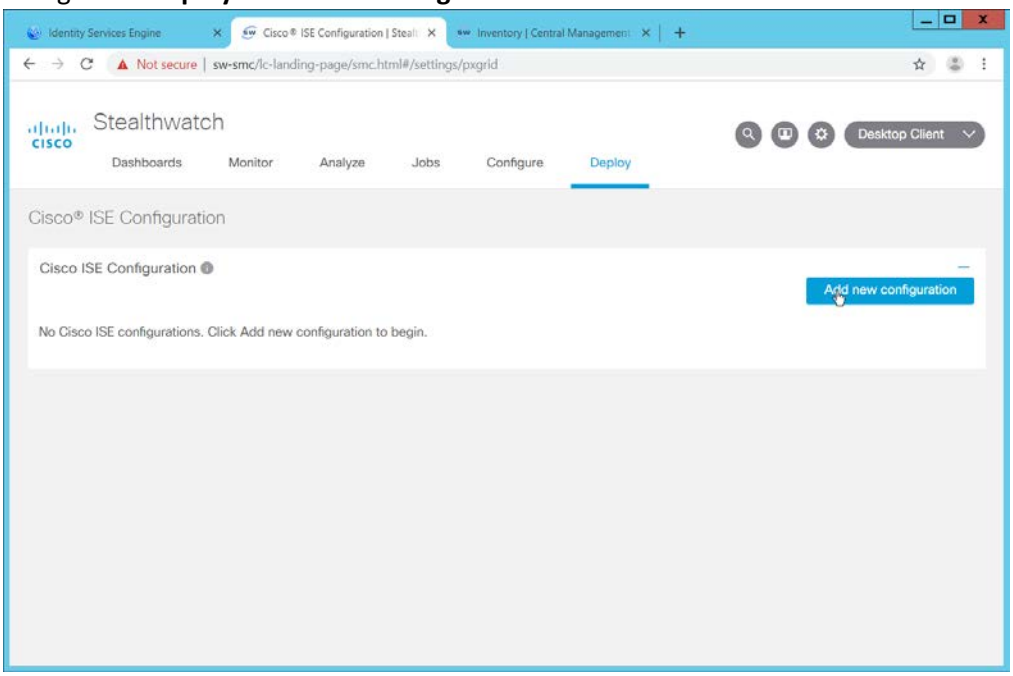
49. Click **Add Client Identity.**



50. Click **Apply Settings.**
51. Navigate back to the SMC web console home screen.

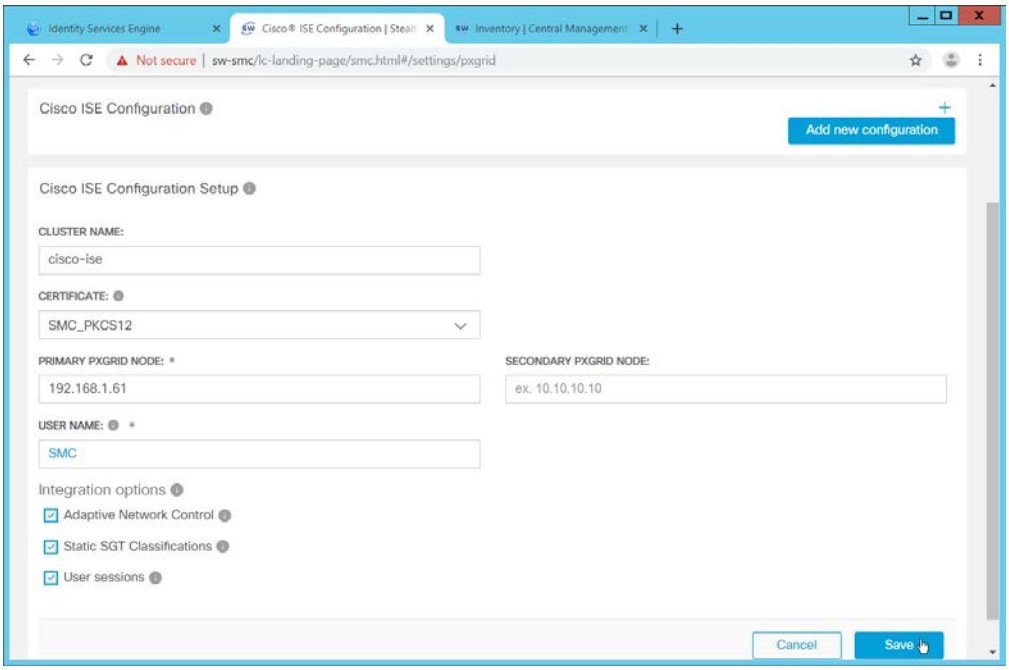


52. Navigate to **Deploy > Cisco ISE Configuration.**



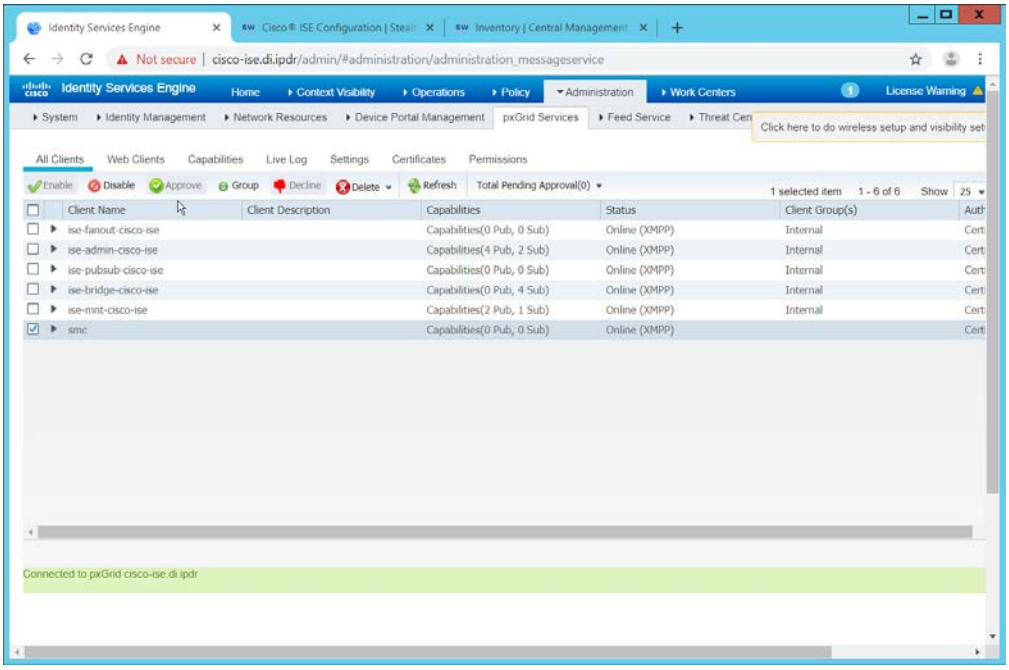
53. Click **Add New Configuration.**
54. Enter a Cisco ISE cluster name.
55. Select the certificate you just uploaded for **Certificate.**
56. Enter the **IP Address** of Cisco ISE for **Primary pxGrid Node.**

57. Enter a **username** for the SMC to use.

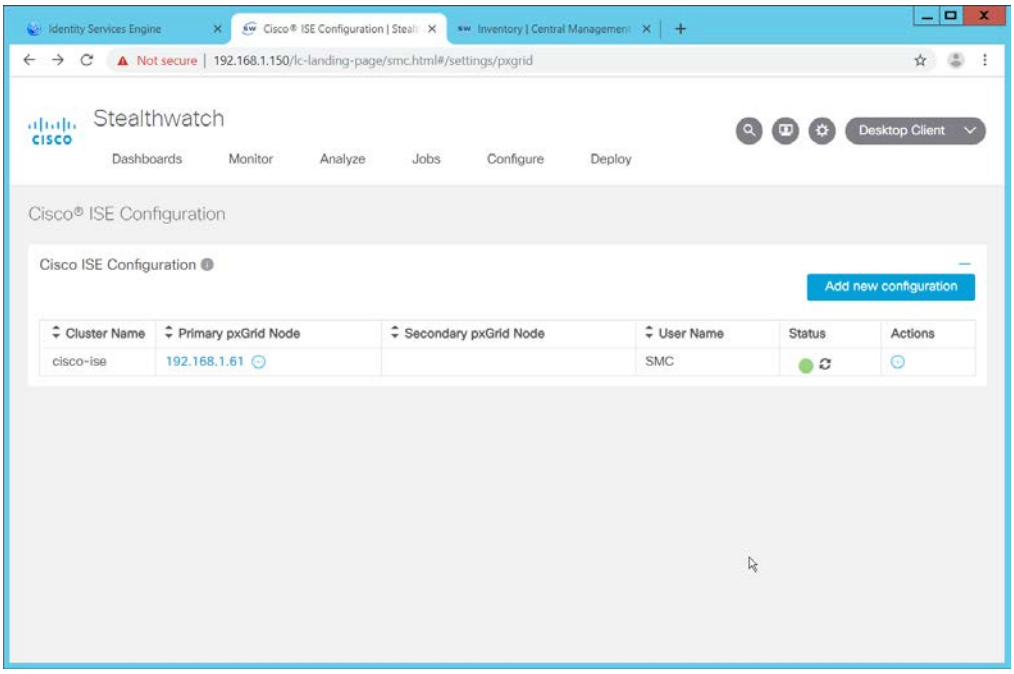


58. Click **Save.**

59. On the Cisco ISE web portal, navigate to **Administration > pxGrid Services > All Clients.**



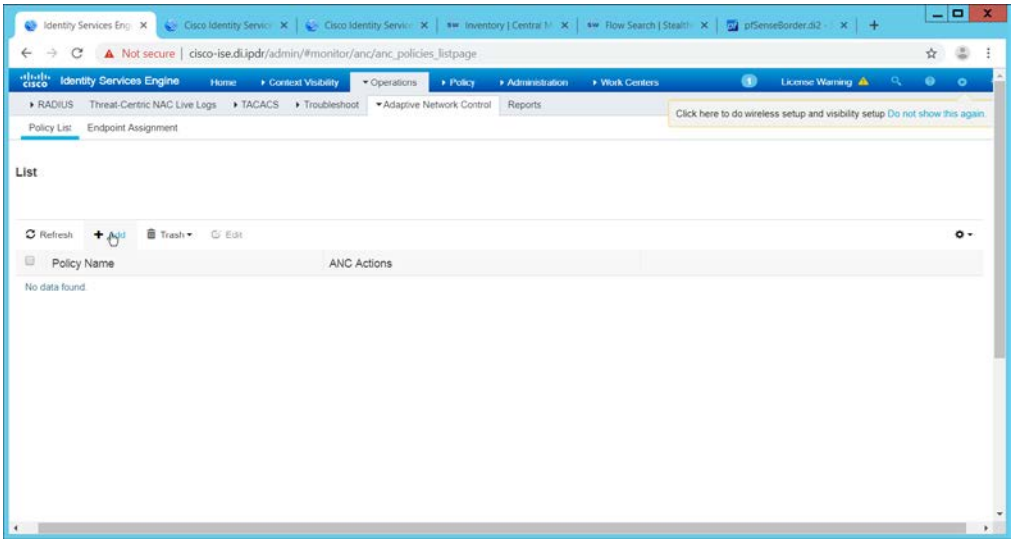
60. If the SMC client you just created says **Pending,** check the box next to it and click **Approve.**



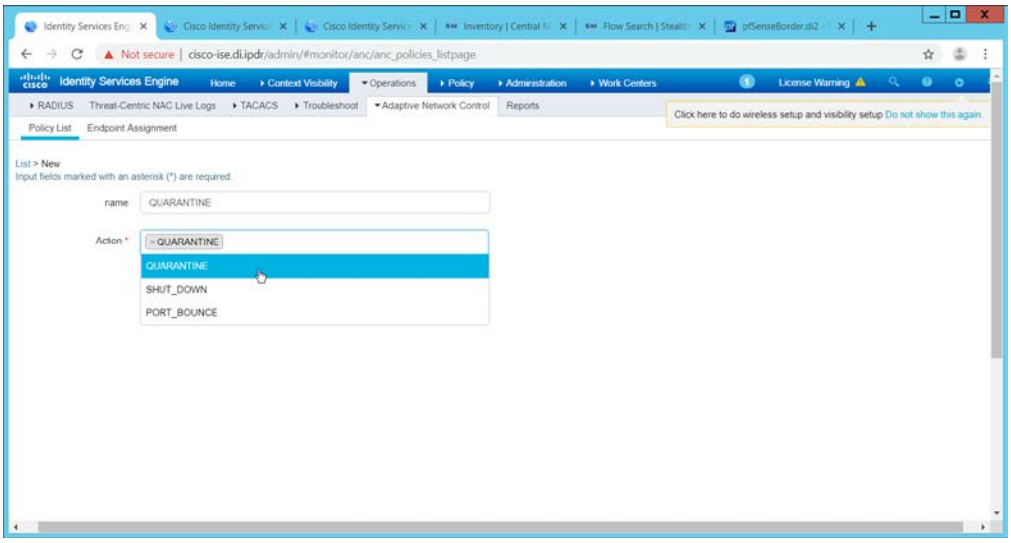
61. The SMC Cisco ISE Configuration page will have a green status icon if it can successfully authenticate to ISE.

2.16.2 Configuring Stealthwatch to Quarantine through ISE

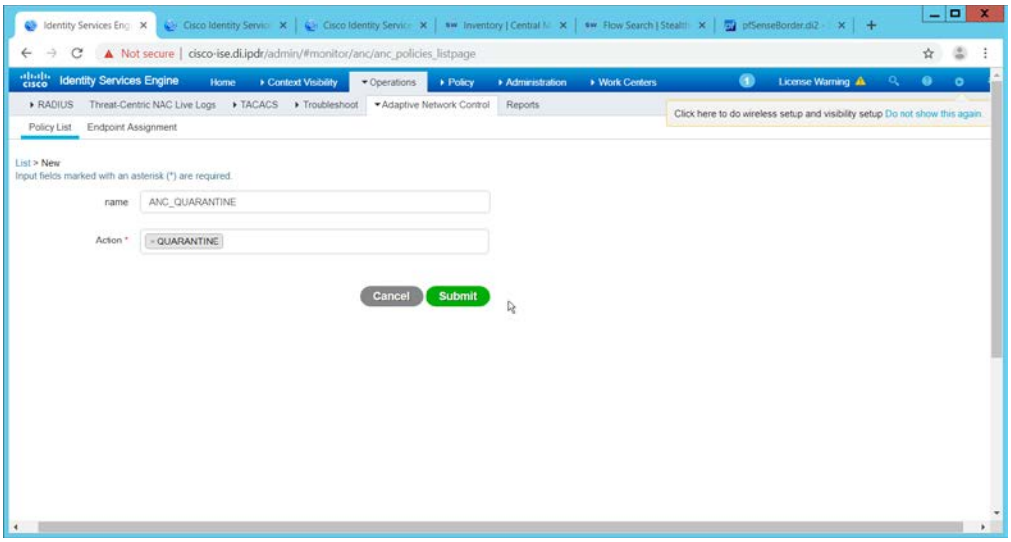
1. Navigate to **Operations > Adaptive Network Control > Policy List.**



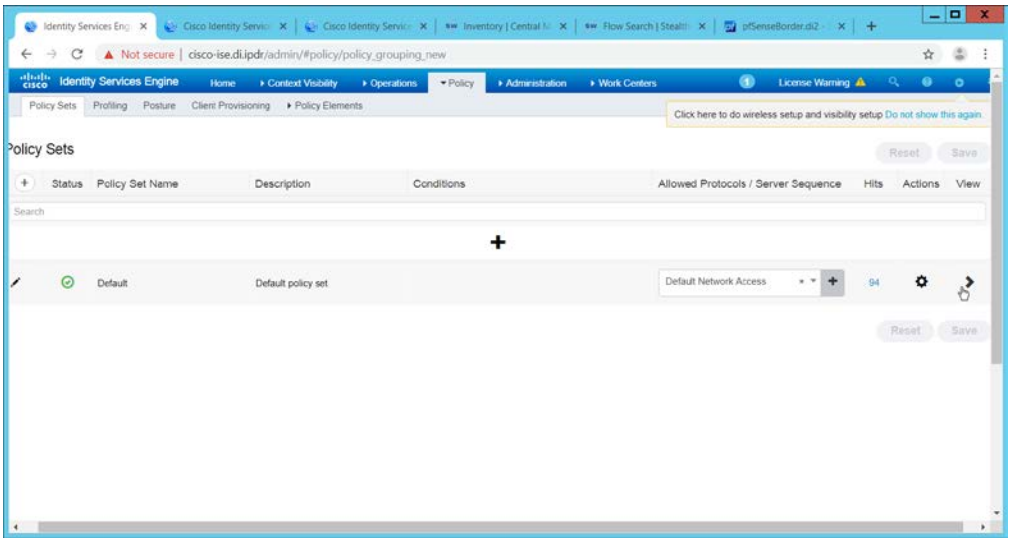
2. Click **Add.**
3. Enter a name for a quarantine action.



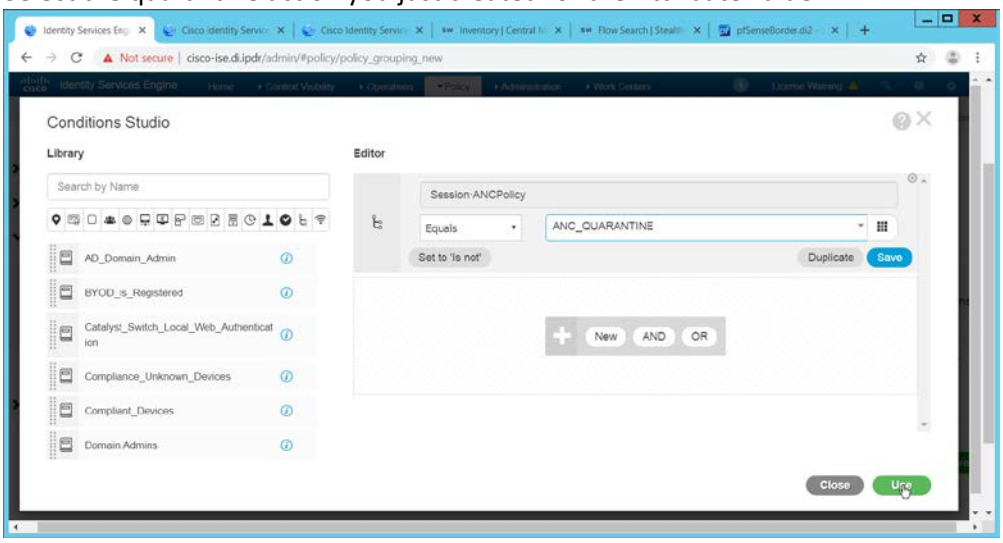
4. Select **QUARANTINE** for the **Action.**



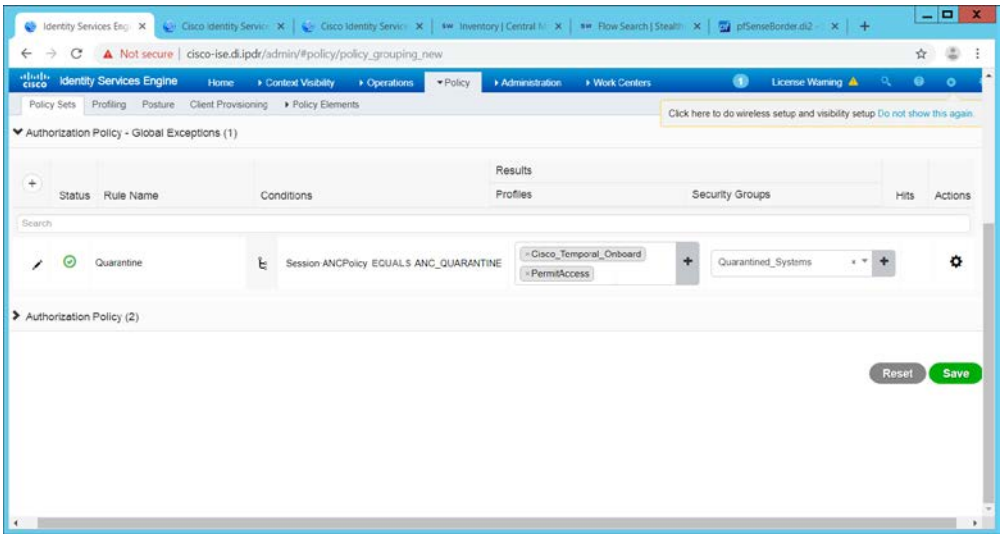
5. Click **Submit.**
6. Navigate to **Policy > Policy Sets.**



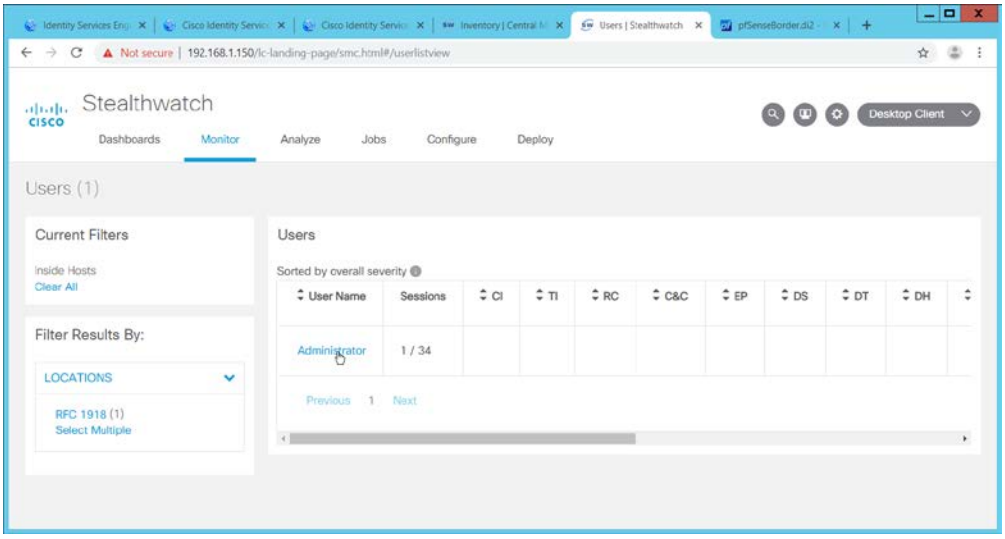
7. Click the **>** arrow next to the default policy set.
8. Expand the **Authorization Policy - Global Exceptions** section.
9. Click the **+** plus sign to add a new policy.
10. Click the **+** plus sign under **Conditions.**
11. Select the field **Session – ANCPolicy.**
12. Select the quarantine action you just created for the Attribute value.



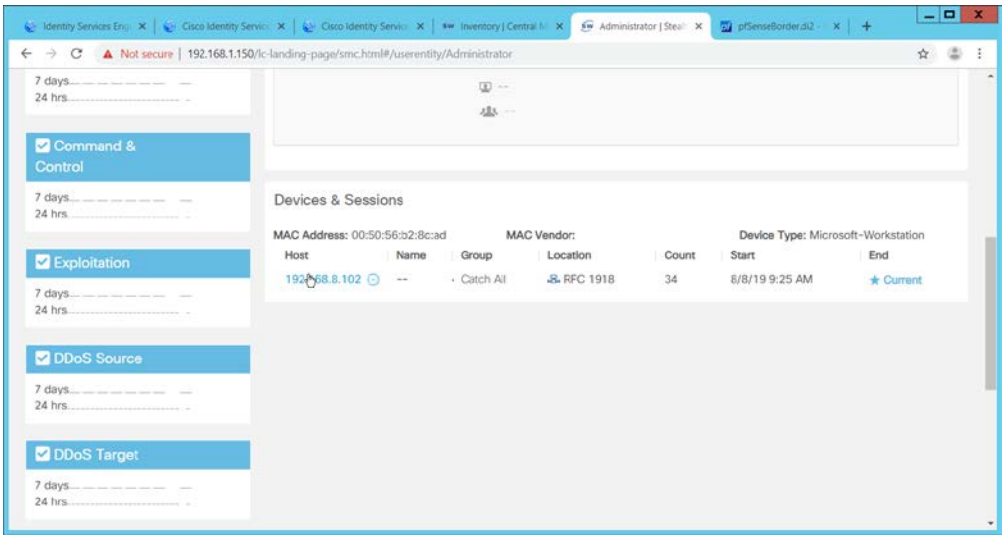
13. Click **Use.**
14. Select the **Deny Access** profile; the profile selected here will be applied to the machine when the machine is added to the quarantine group.
15. Select **Quarantined_Systems** for **Security Groups.**



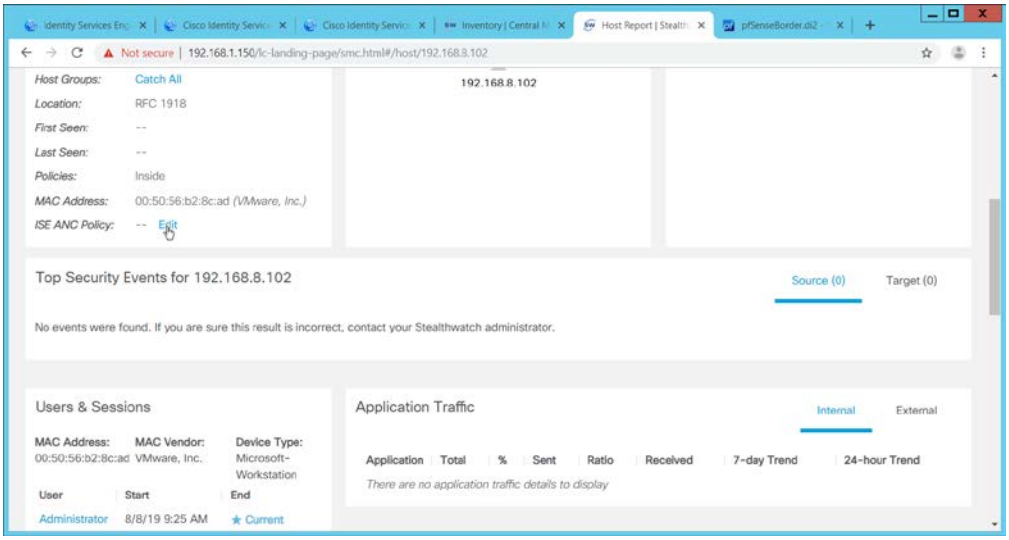
16. Click **Save.**
17. In the SMC web console, click **Monitor > Users.**



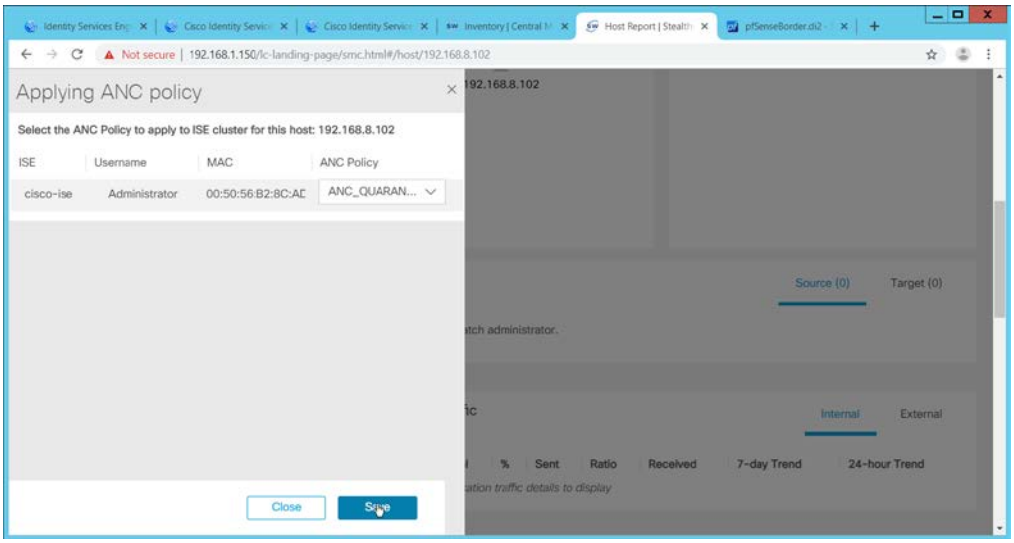
18. Select a user to quarantine.



19. Click a host to quarantine**.**



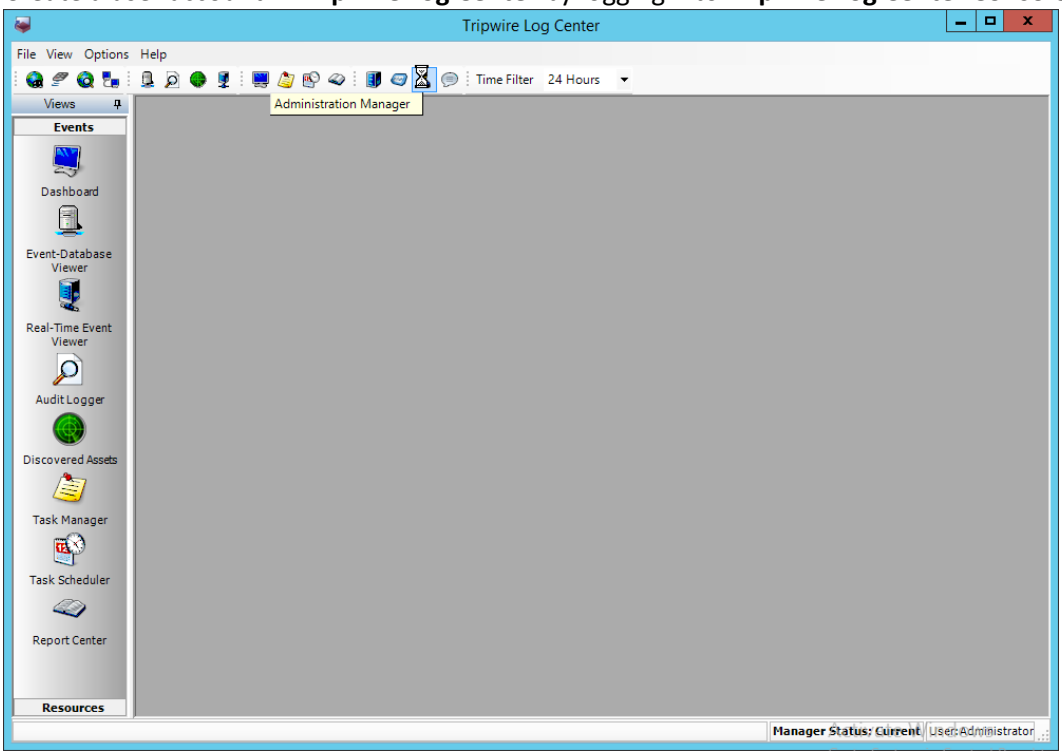
20. Click **Edit** next to **ISE ANC Policy.**
21. From the drop down, select the quarantine action you created earlier.



22. Click **Save.**
23. This will apply the quarantine action to the machine.

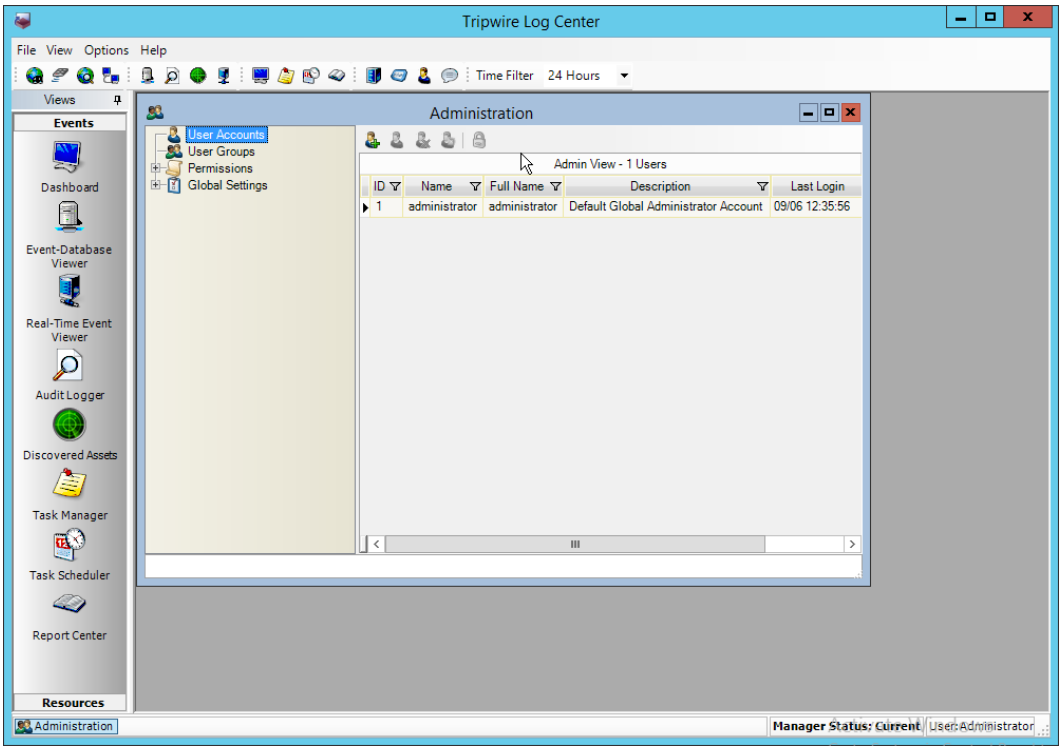
2.17 Integration: Tripwire Log Center and Tripwire Enterprise

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

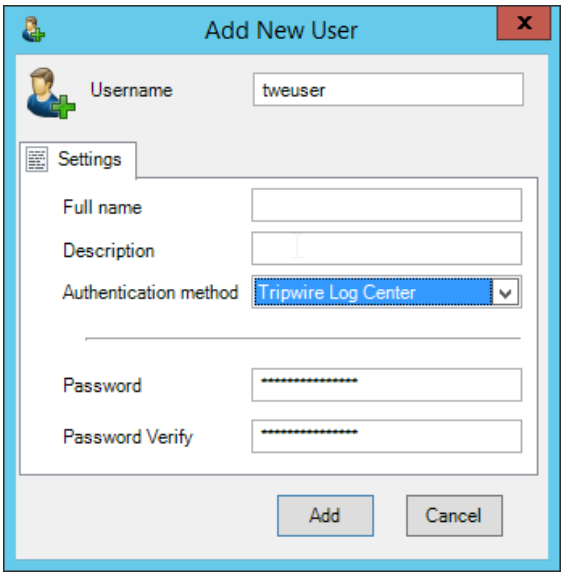


2. Click the **Administration Manager** button.

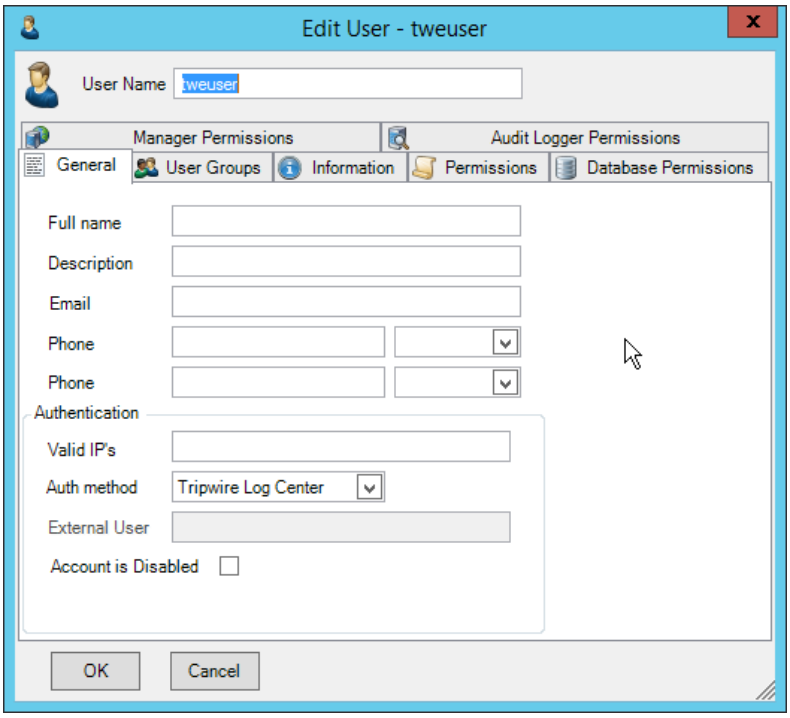
3. Click **User Accounts.**



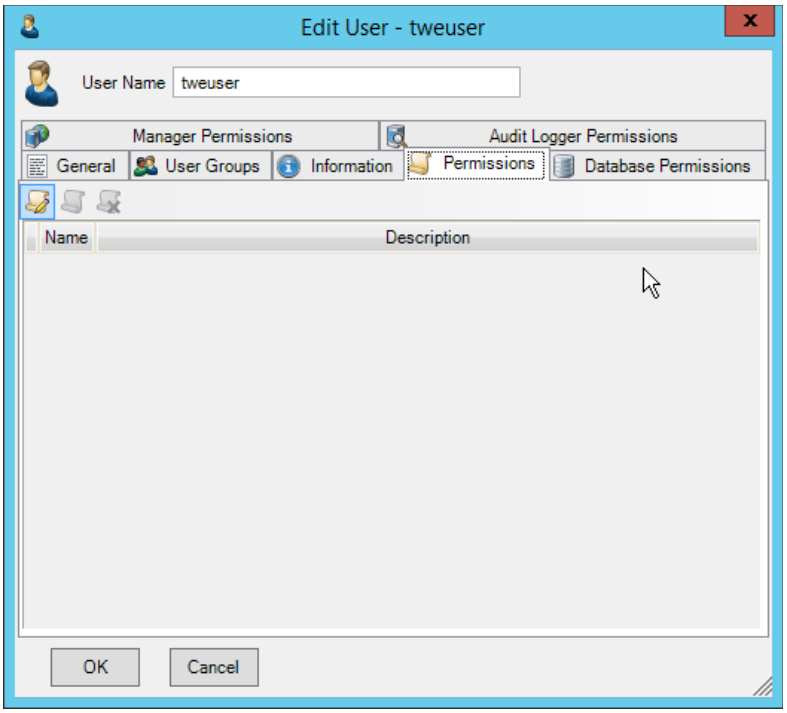
4. Click the **Add** button.
5. Enter the details of the user.



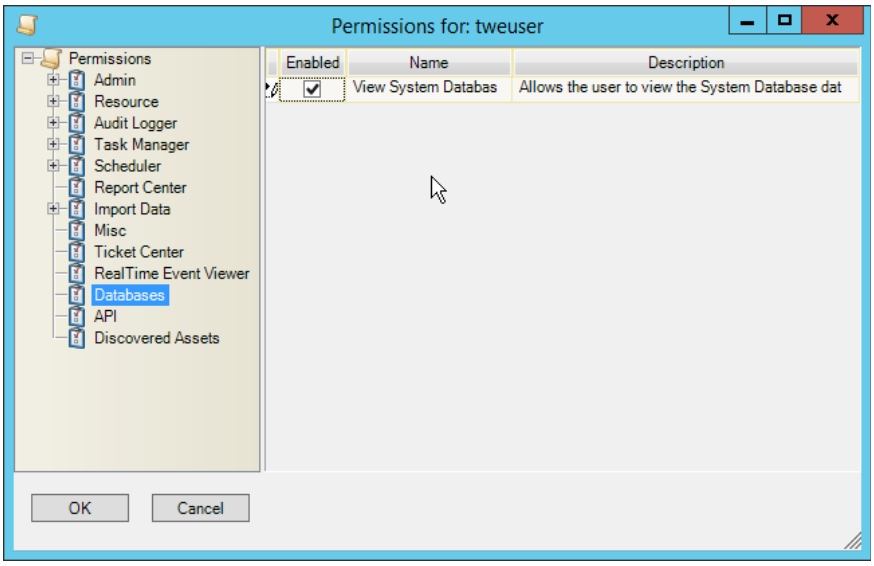
6. Click **Add.**
7. Double-click the user account.



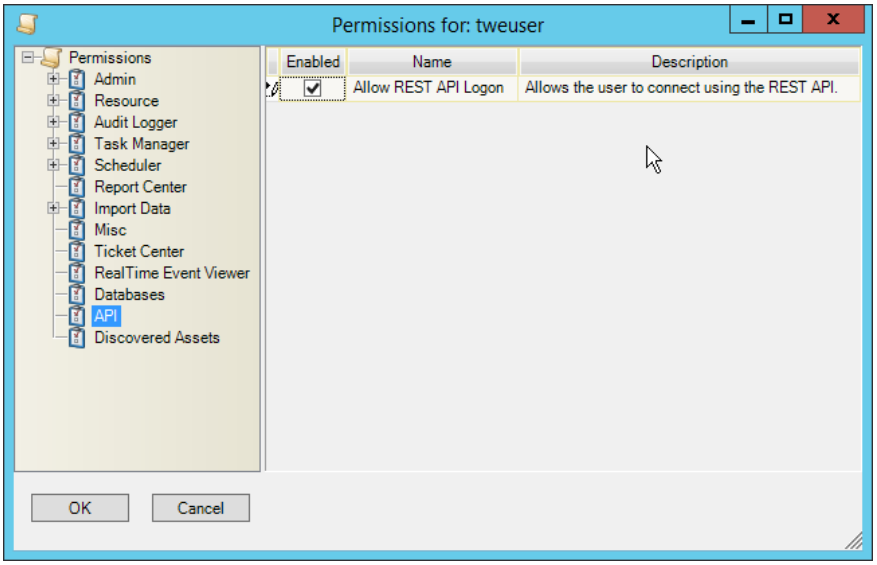
8. Click the **Permissions** tab.



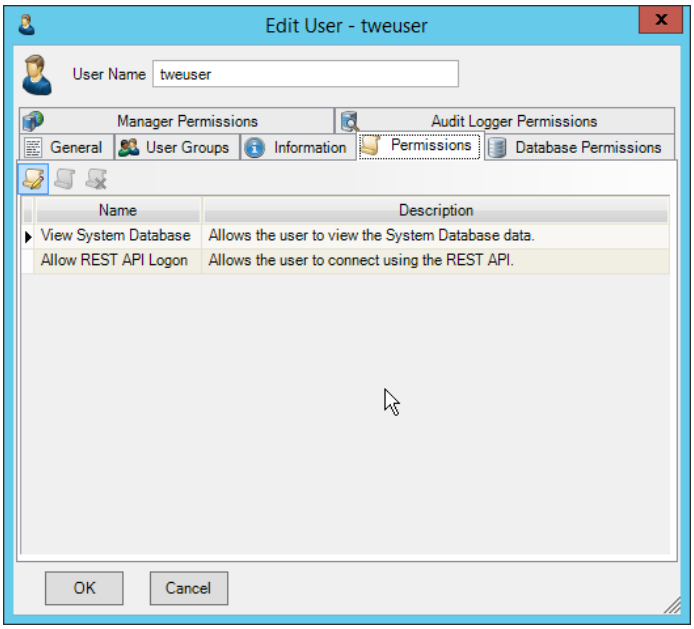
9. Click **Edit list of permissions.**
10. Select **Databases.**



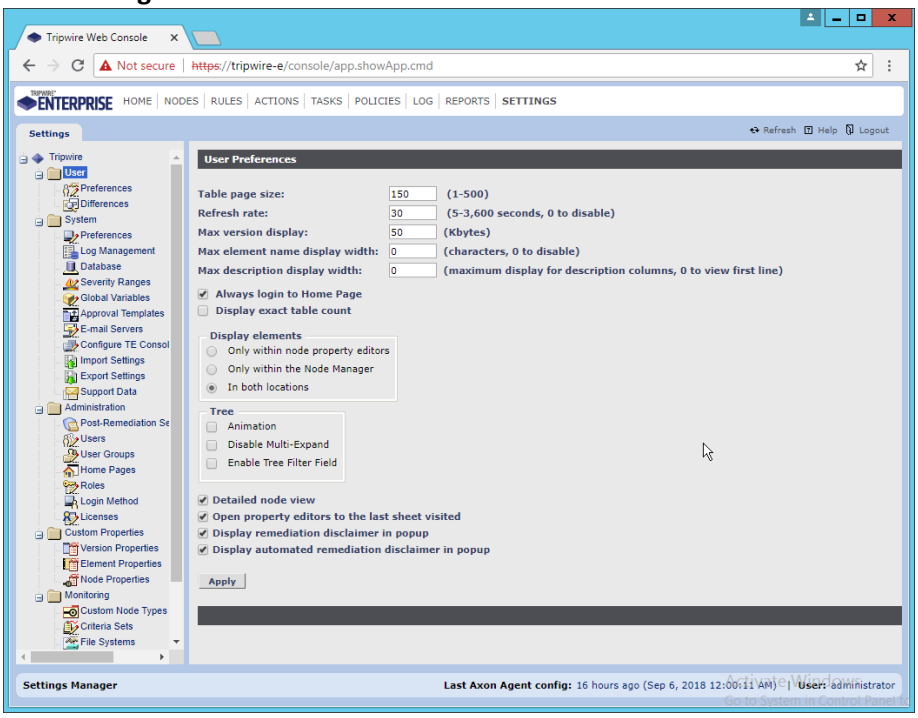
11. Check the box next to **View System Database.**
12. Select **API.**



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

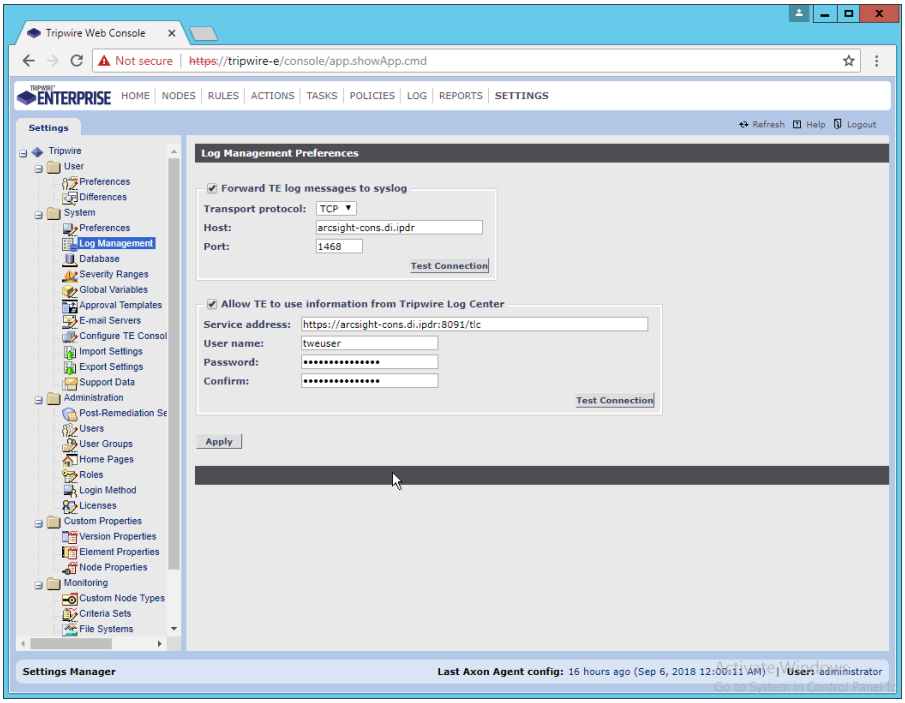


14. Click **OK.**
15. Click **OK.**
16. Log in to the **Tripwire Enterprise** web console.
17. Click **Settings.**

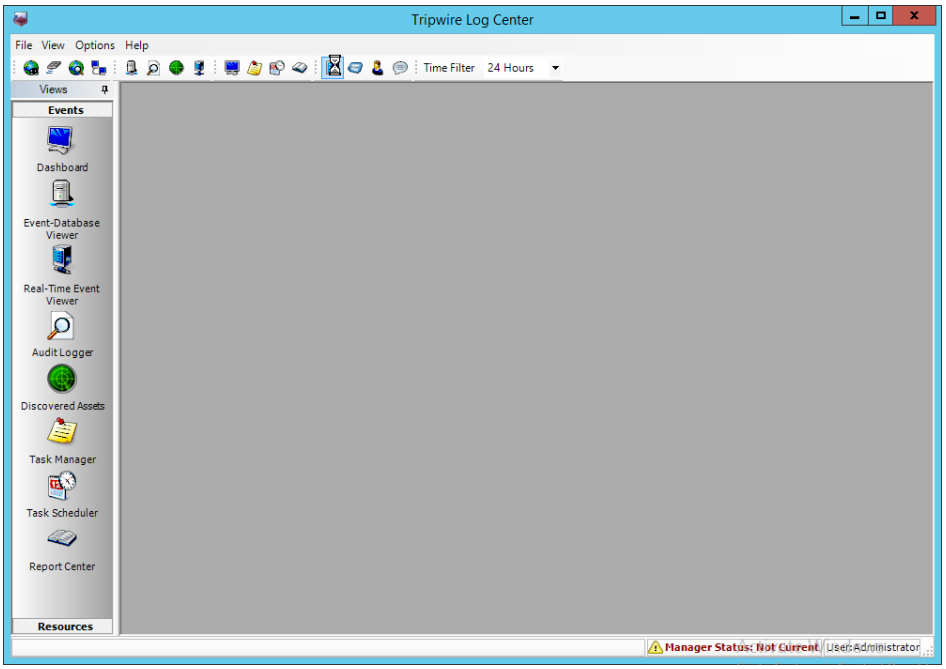


18. Go to **System** > **Log Management.**

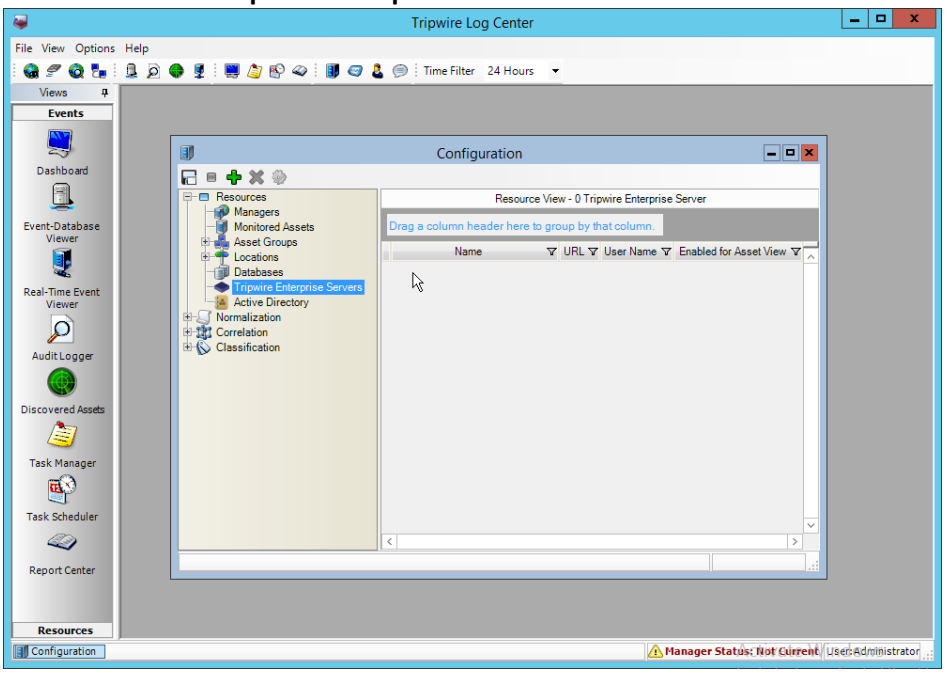
19. Check the box next to **Forward TE log messages to syslog.**
20. Enter the **hostname** and **port** of the **Tripwire Log Center** server. The default port is **1468.**
21. Check the box next to **Allow TE to use information from Tripwire Log Center.**
22. Enter the **service address** like this: https://arcsight-cons.di.ipdr:8091/tlc, replacing 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.**

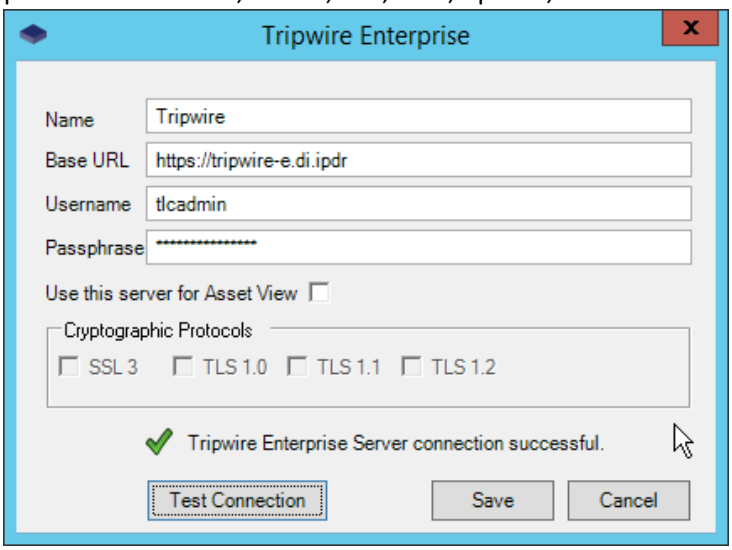


27. Click **Configuration Manager.**
28. Click **Resources** > **Tripwire Enterprise Servers.**



29. Click **Add.**
30. Enter a **name** for the server.
31. Enter the **URL** of the TE server.

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



33. Click **Save.**

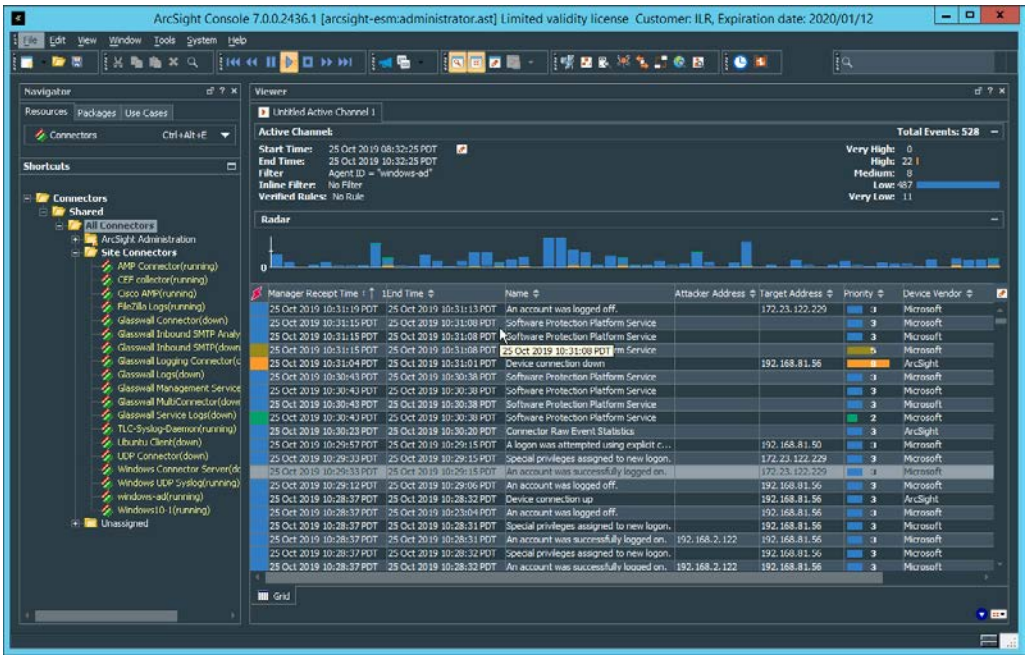
2.18 Integration: Symantec ICA and ArcSight ESM

This section describes the integration of Symantec ICA and ArcSight ESM, to import data from ArcSight into ICA for analysis. For the purposes of this build, we did not use ArcSight Logger, a tool which provides a web API for other applications. Because of this, the standard integration between ICA and ESM was unavailable. However, it is still possible to import CSV files exported from ArcSight into ICA, and we will detail the process below. There are a few things to note when doing this import:

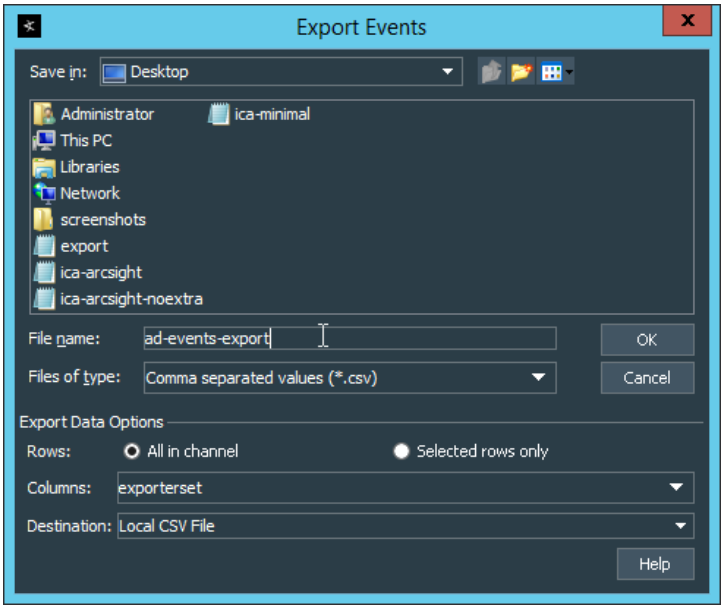
- On the version of Symantec ICA we are using, it is required to replace empty fields in the CSV with NULL. This may be unnecessary in future updates.
- The CSV file should be in a location accessible to the ICA server. You can replace this file with a new CSV file on a daily basis, and Symantec ICA has the capability to import the new data.
- The following integration details how to do it for a subset of fields on Active Directory logging events, but the process can be expanded for your organization's needs.

2.18.1 Export the CSV File from ArcSight Console

1. In ArcSight Console, find a connector which you wish to import events from. Right-click it, and select **Create Channel with Filter.**
2. In the channel, apply any filters desired.



3. When finished, right-click any of the events in the channel, and select **Export > Events in Channel….**
4. Enter a name for the CSV file for **File name:.**
5. Select **All in Channel** for **Rows:.**
6. For **Columns:** either select a custom field-set to determine the output columns or leave the default selected.

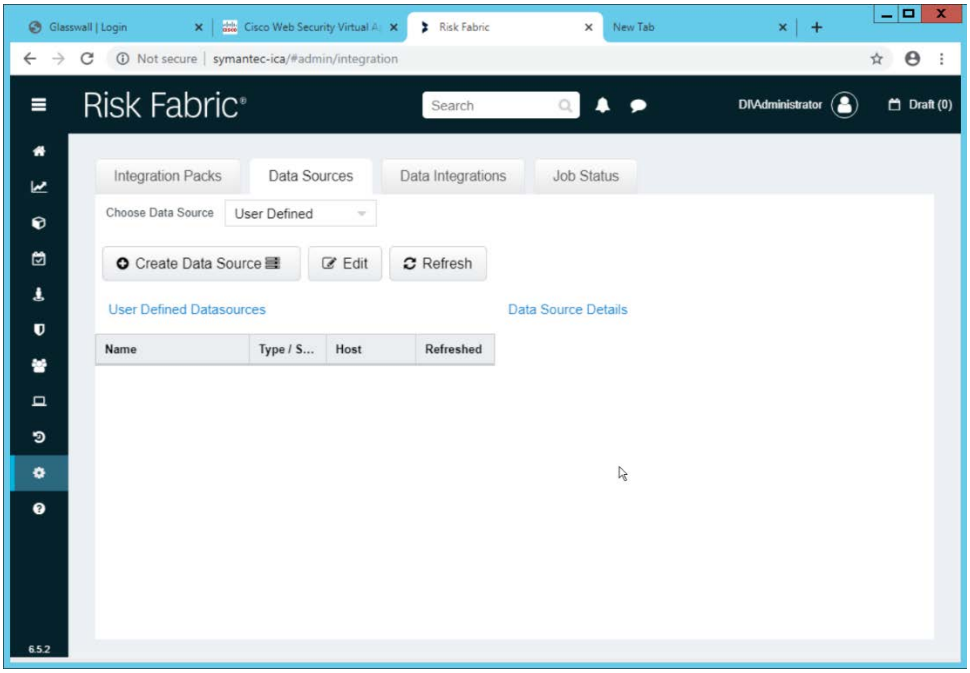


7. Click **OK.**

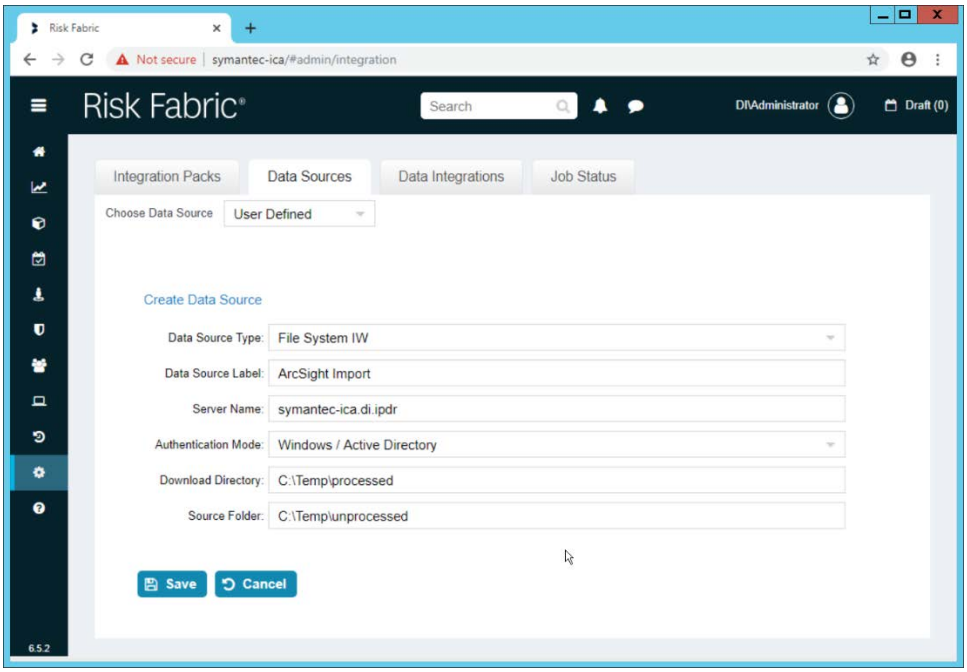
8. Move the file to the desired location for ICA to collect. (Ensure that if required for your version of Symantec ICA, all empty fields are replaced with "NULL") For the purposes of this demonstration, we moved it to *C:\Temp\unprocessed* on the Symantec ICA server.

2.18.2 Import the CSV File to Symantec ICA

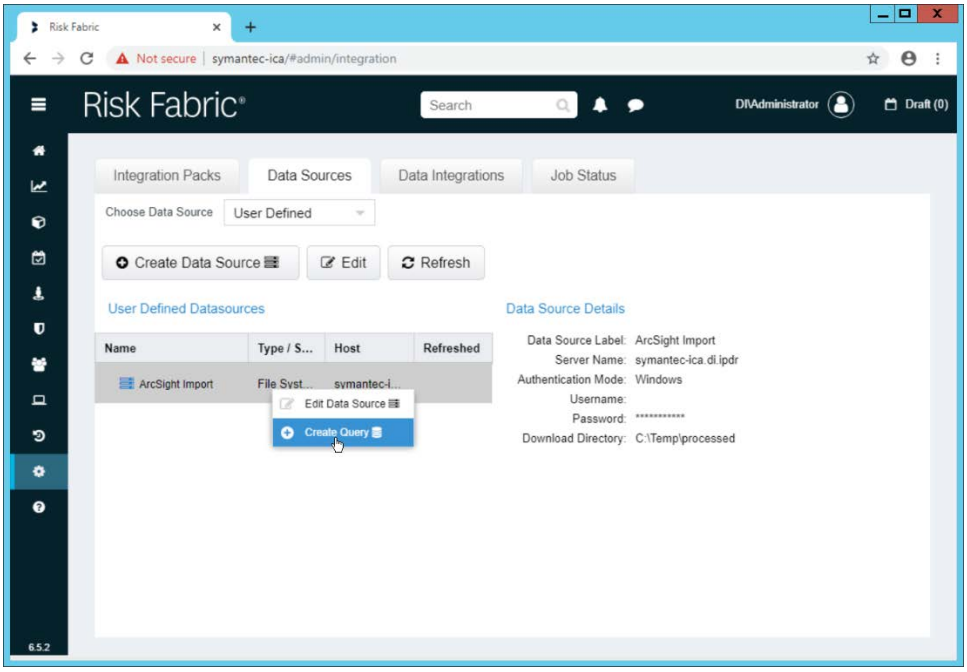
1. On the Symantec ICA web console, navigate to **Gear Icon > Integration.**
2. Click the **Data Sources** tab.



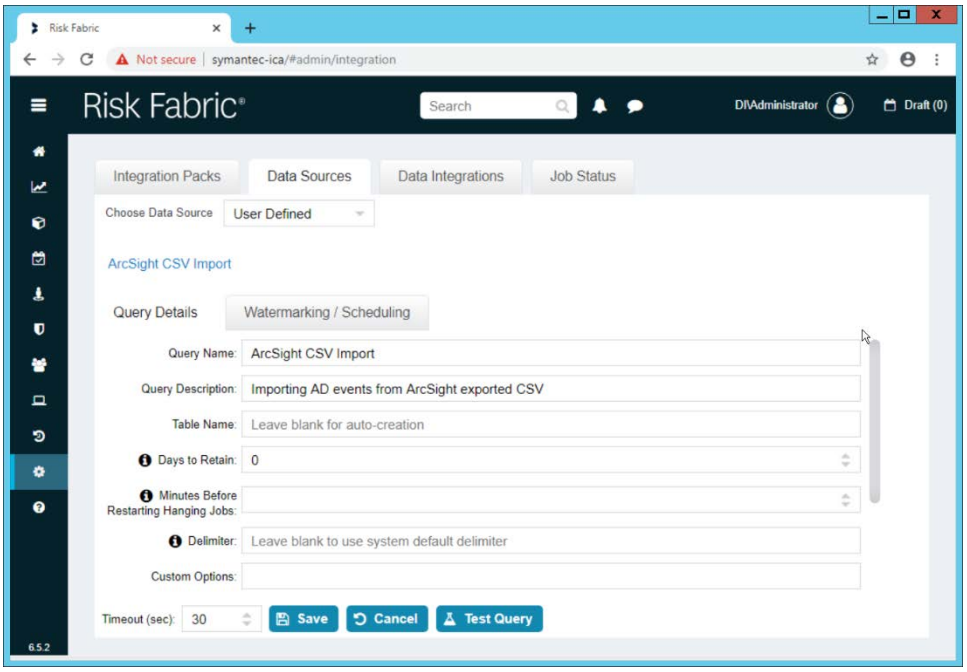
3. Select **User Defined** for **Choose Data Source.**
4. Click **Create Data Source.**
5. Select **File System IW** for the **Data Source Type.**
6. Enter a name for the data source for **Data Source Label.**
7. Enter the hostname of the Symantec ICA server for **Server Name.**
8. Select **Windows/Active Directory** for the **Authentication Mode.**
9. Enter the location for the downloaded CSV file for **Download Directory** (relative to the Symantec ICA server).
10. Enter the location for the CSV file to be downloaded from for **Source Folder** (relative to the Symantec ICA server).



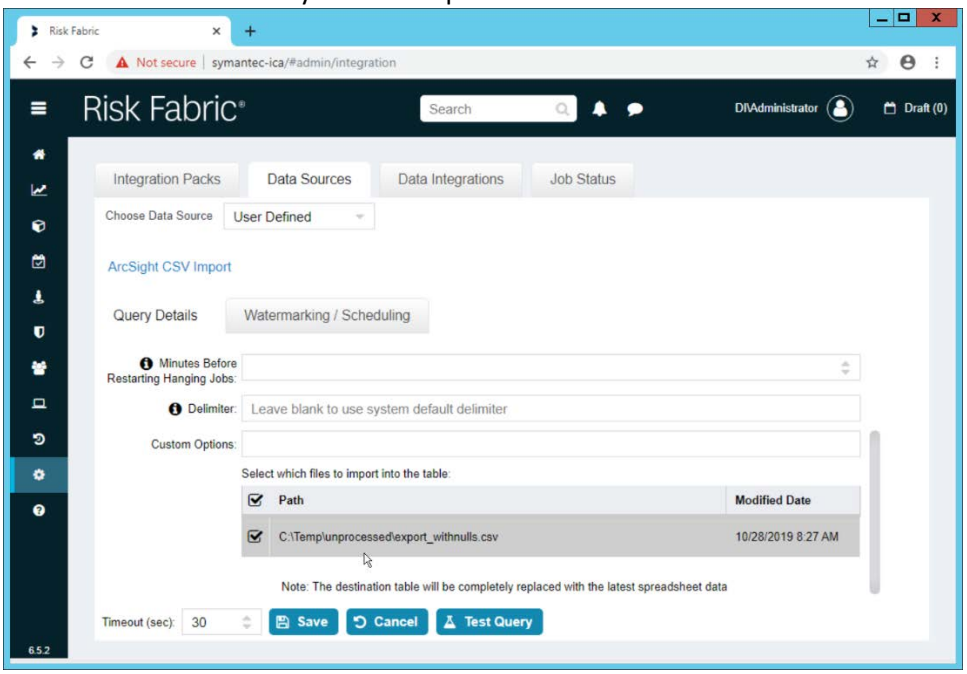
11. Click **Save.**



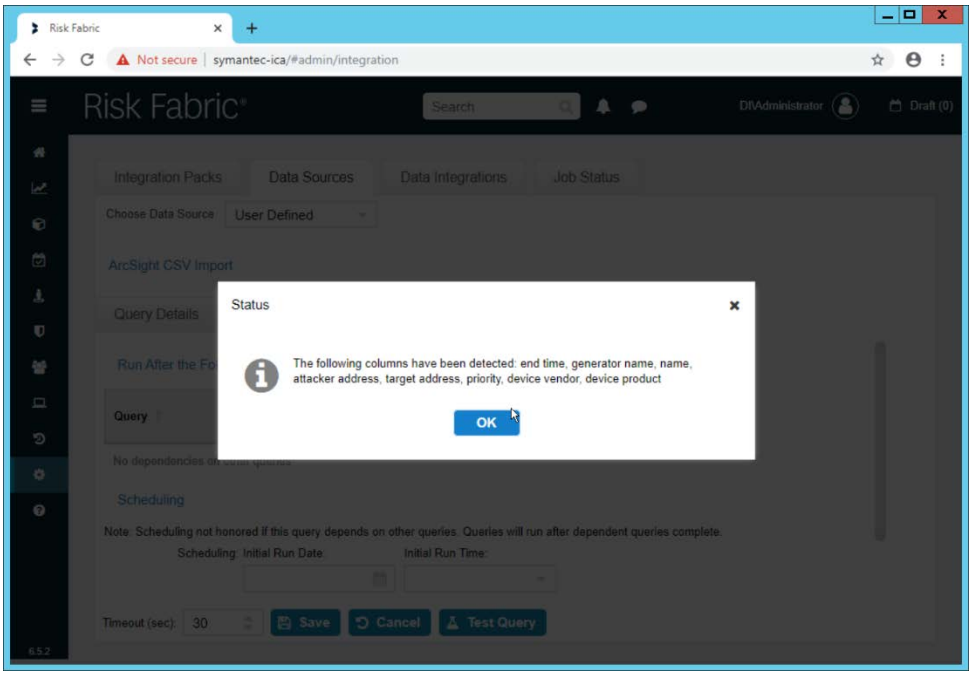
12. Right-click the newly created data source and select **Create Query.**
13. Enter a **Query Name** and **Query Description.**



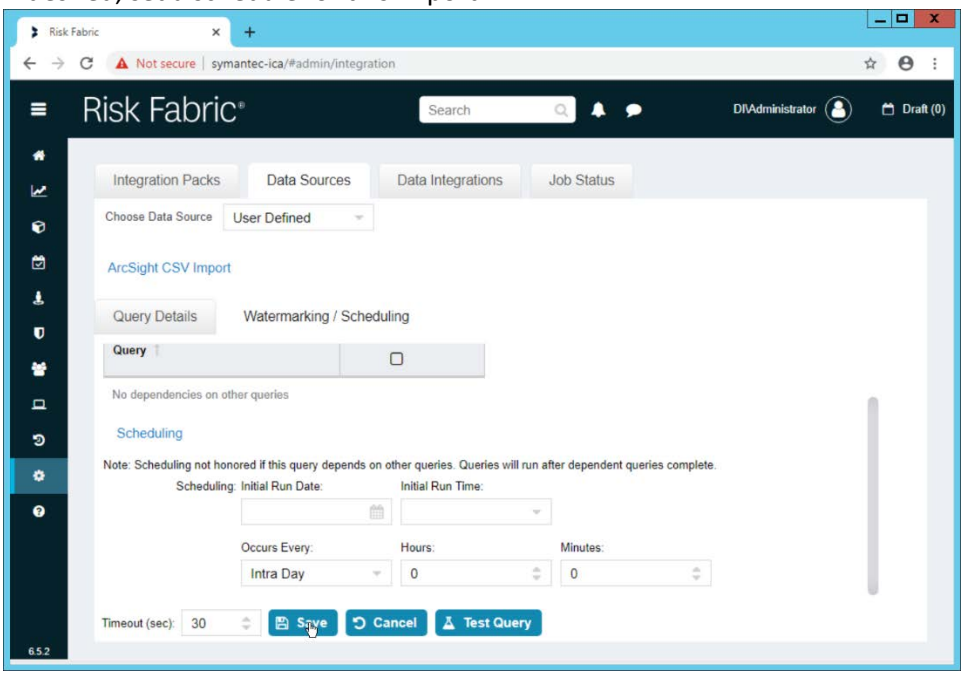
14. If you specified the **Source Folder** correctly, you will see the CSV file listed.
15. Check the box next to any CSVs to import.



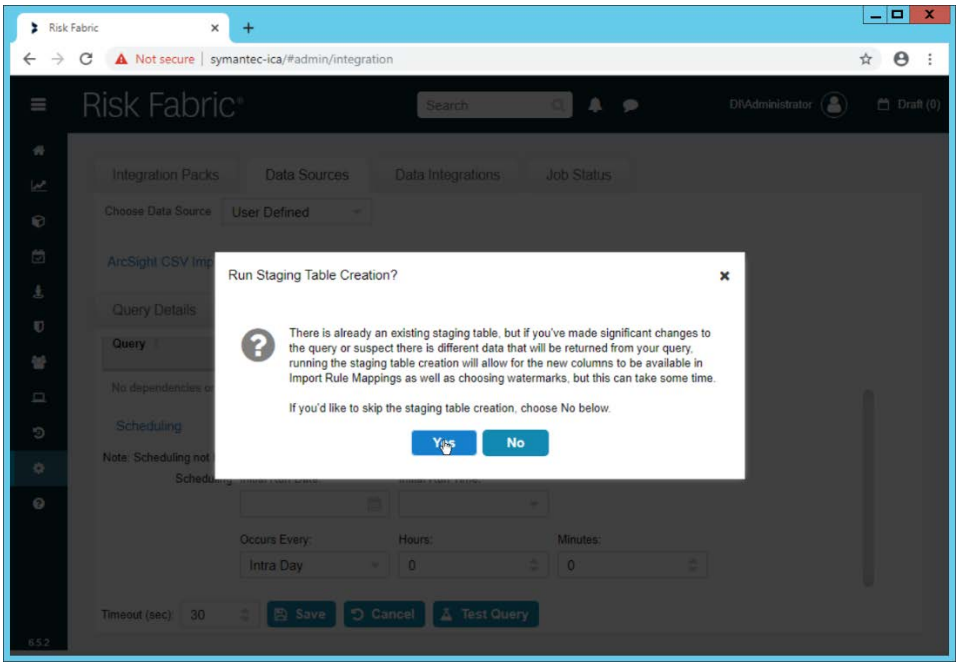
16. Click **Save.**



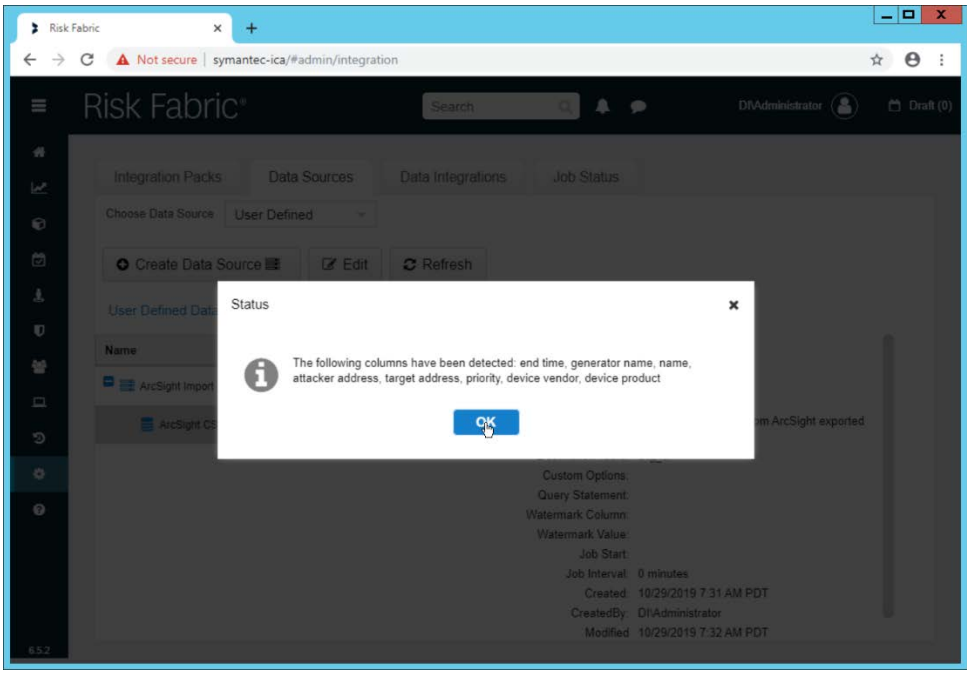
17. Click **OK.**
18. If desired, set a schedule for this import.



19. Click **Save.**



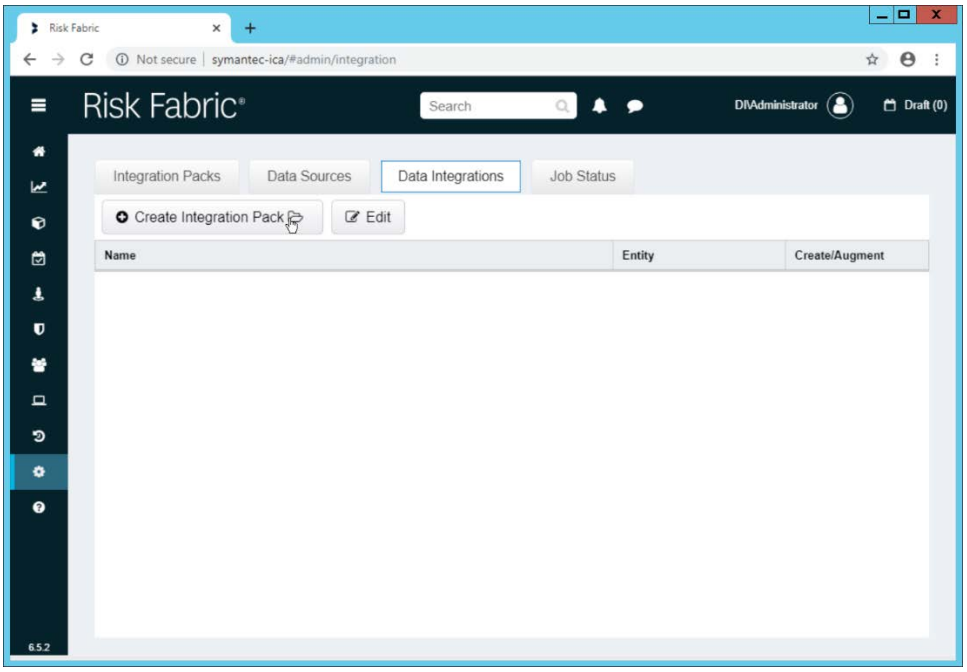
20. Click **Yes.**



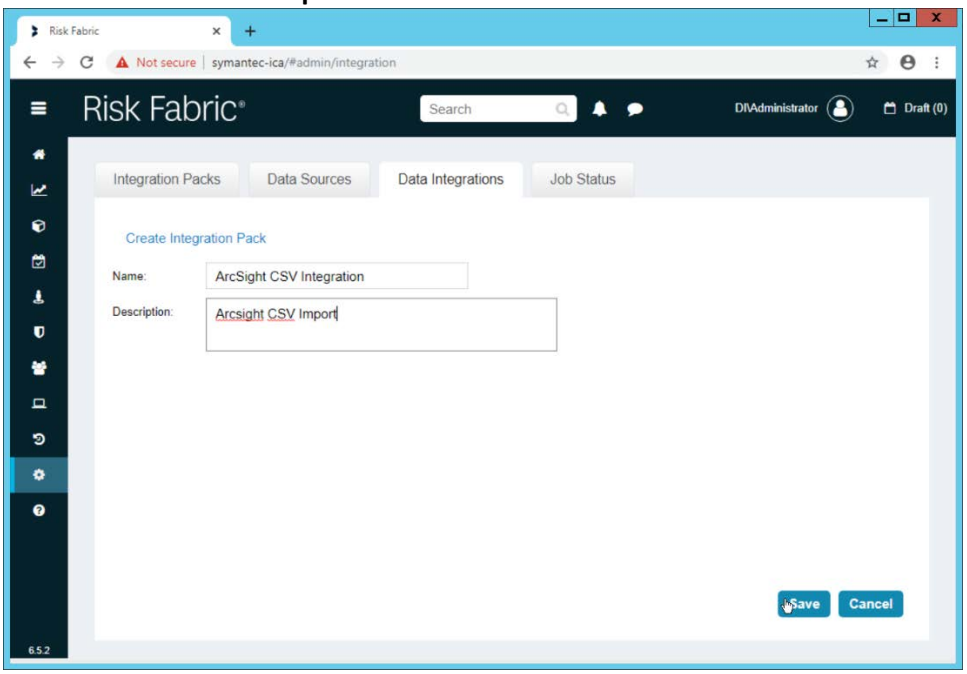
21. Click **OK.**

2.18.3 Create a Mapping between ArcSight events and Symantec ICA

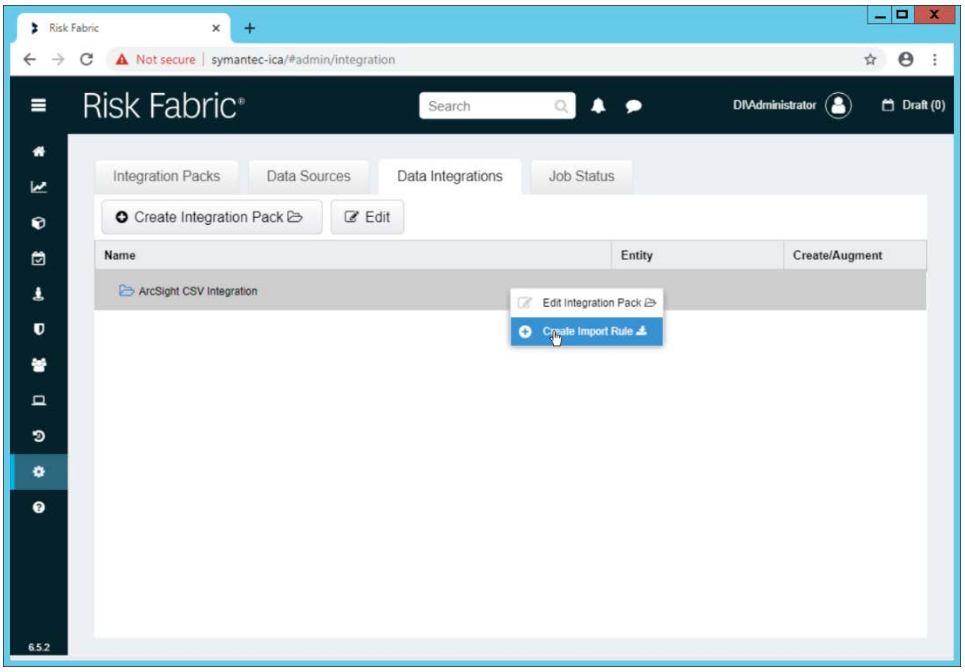
1. Navigate to the **Data Integrations** tab.



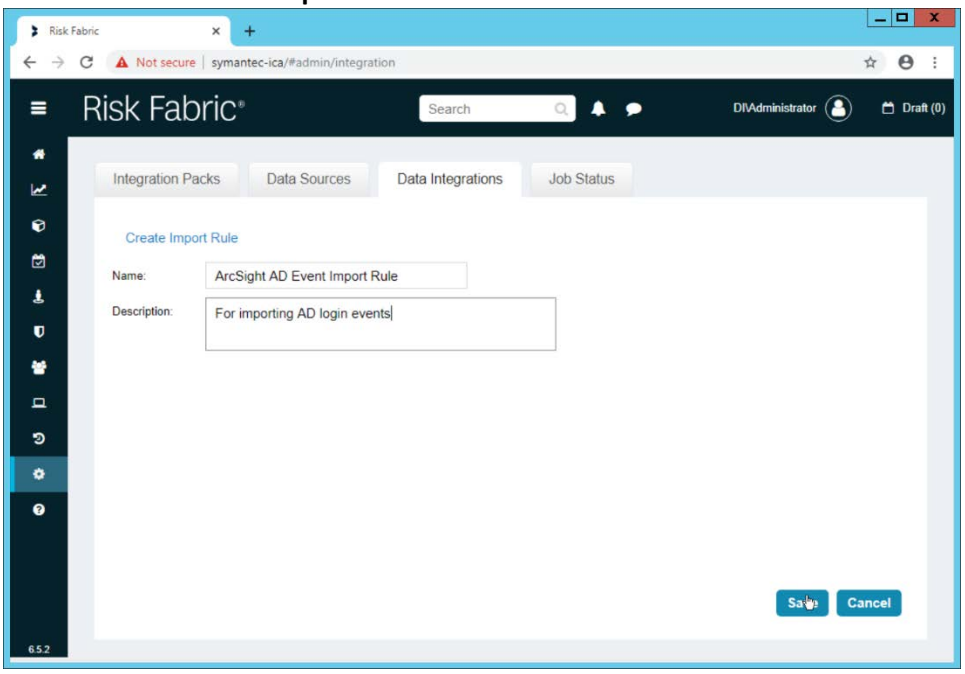
2. Click **Create Integration Pack.**
3. Enter a **Name** and **Description.**



4. Click **Save.**

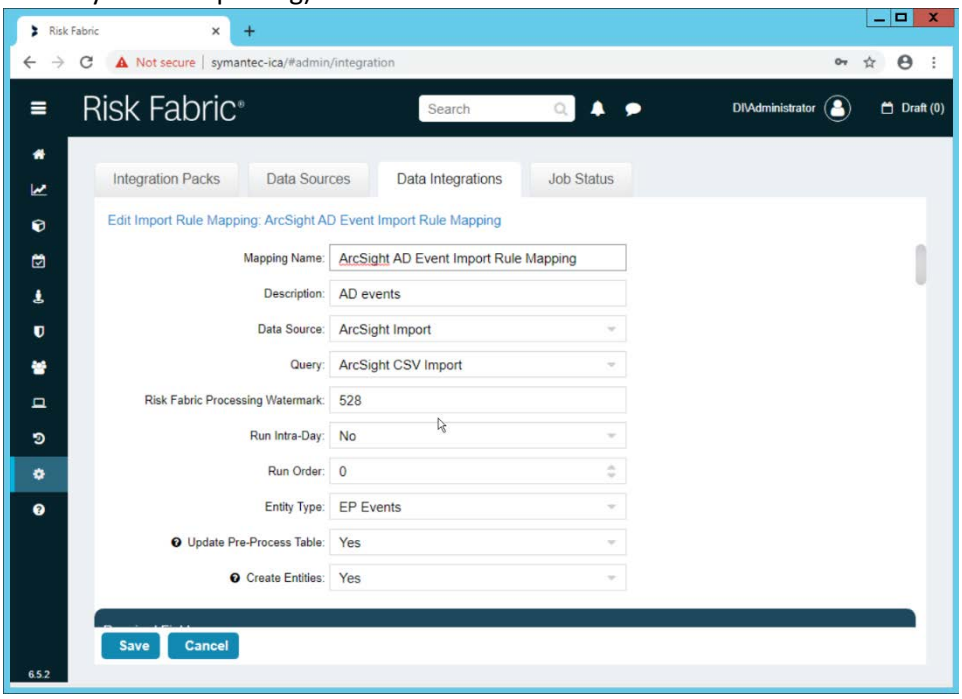


5. Right-click the newly created Integration Pack, and select **Create Import Rule.**
6. Enter a **Name** and **Description.**

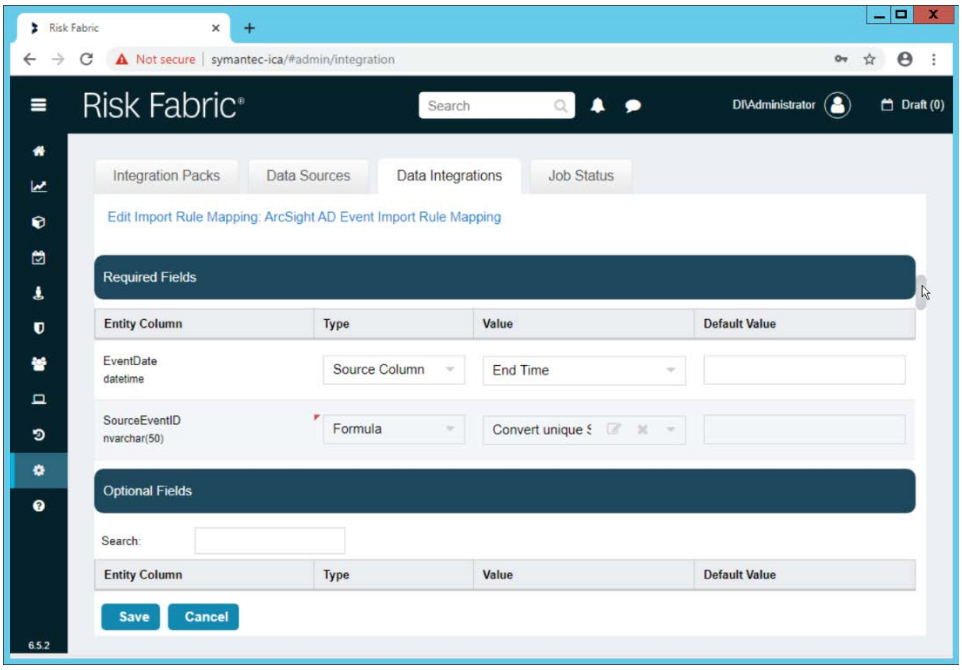


7. Click **Save.**
8. Right-click the newly created **Import Rule** and select **Create Import Rule Mapping.**
9. Enter a **Name** for the mapping.

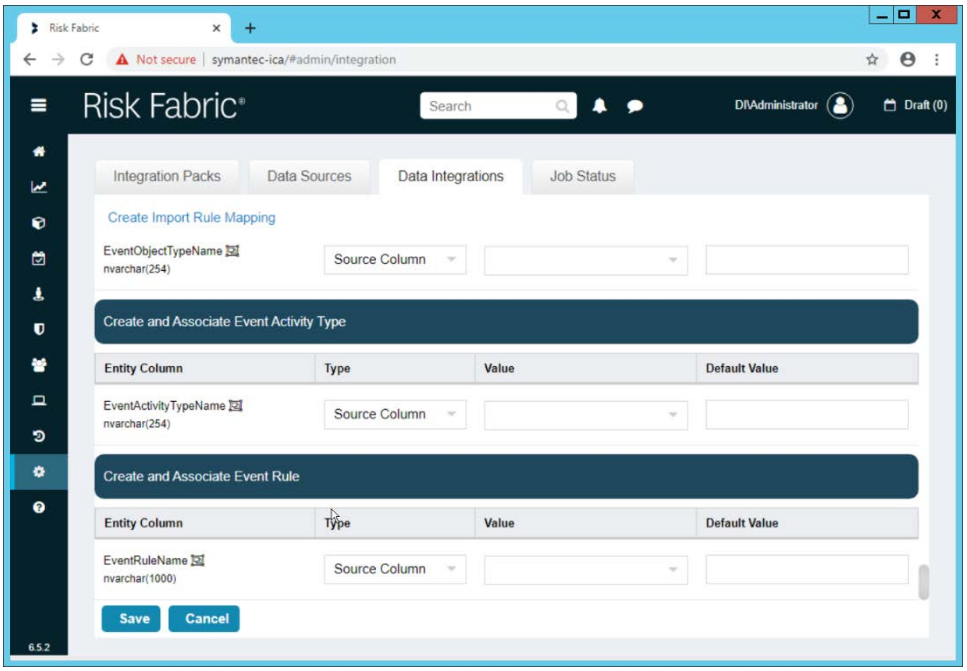
10. Enter a **Description.**
11. Select the **Data Source** created earlier.
12. Select the **Query** created earlier.
13. Select **EP Events** for the **Entity Type** (or explore other Entity Types that may better match the events you are importing).



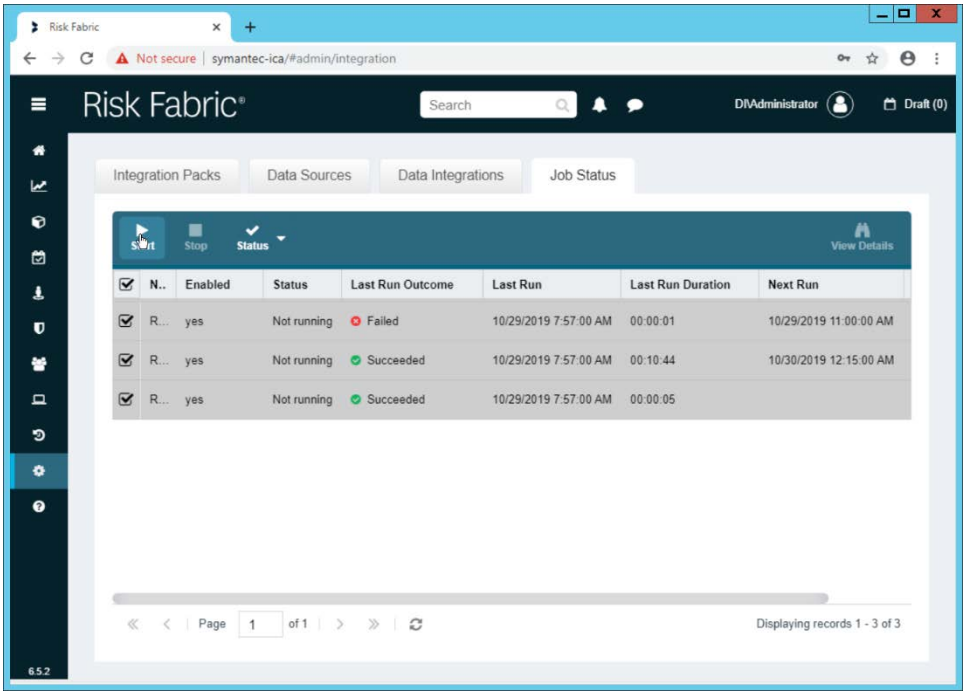
14. Below, the **Entity Column** refers to the target field in ICA to which a field is being mapped. Map event fields from the CSV to fields in the Entity Column.
15. For example, **EventDate** in ICA corresponds directly to the **End Time** in ArcSight, so we select that value directly as a **Source Column** for the mapping.



16. **Formulas** can be used to transform columns in the CSV to something more specific in ICA. Because we did not export an event ID to our CSV file, we use a formula to create a hash of the **End Time** and use that as the ID.
17. All **Required Fields** must be mapped, and you will likely also want to map some optional fields to make useful data.



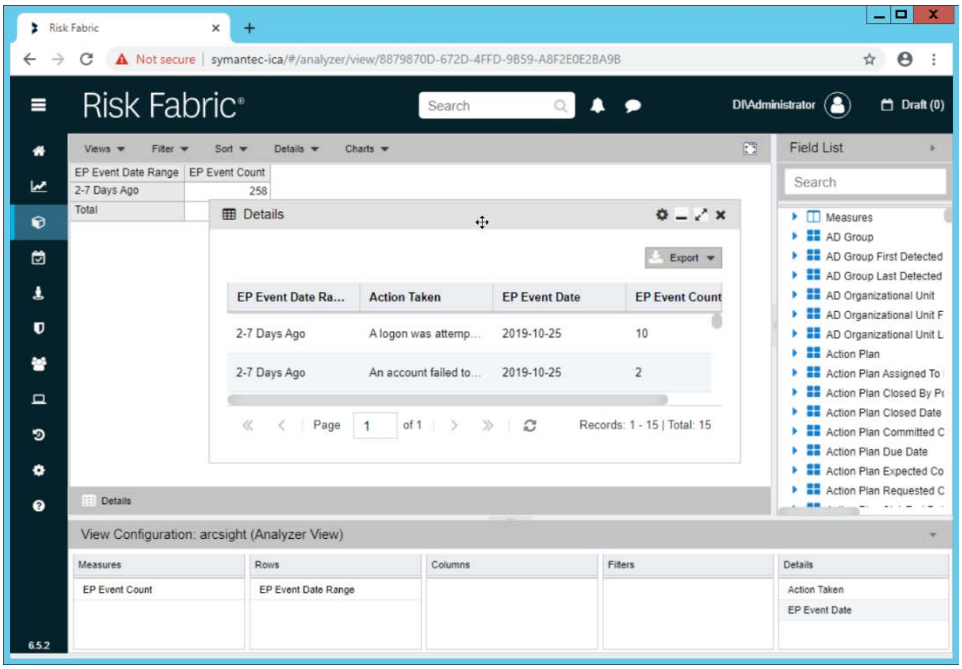
18. Click **Save** when finished.
19. Navigate to the **Job Status** tab.



20. Select all the jobs and click **Start.** This is to force a refresh of the ICA processing, allowing the data from the CSV to be imported immediately.

2.18.4 View ArcSight Events in the Analyzer

1. Once the processing jobs are finished, navigate to the **Analyzer.**



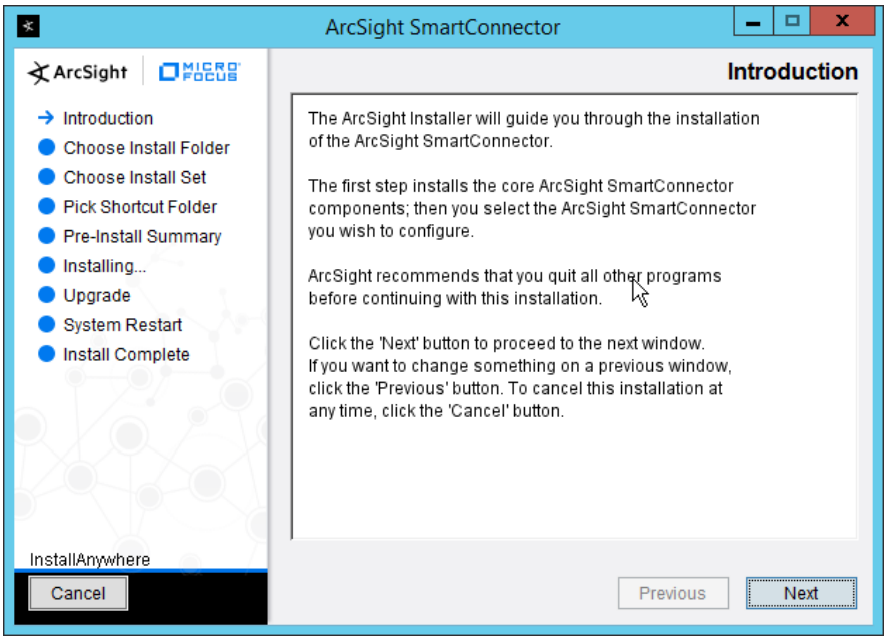
2. Drag mapped columns (from the import rule mapping you created) from the list on the right to view them in the analyzer.

2.19 Integration: Micro Focus ArcSight and Tripwire

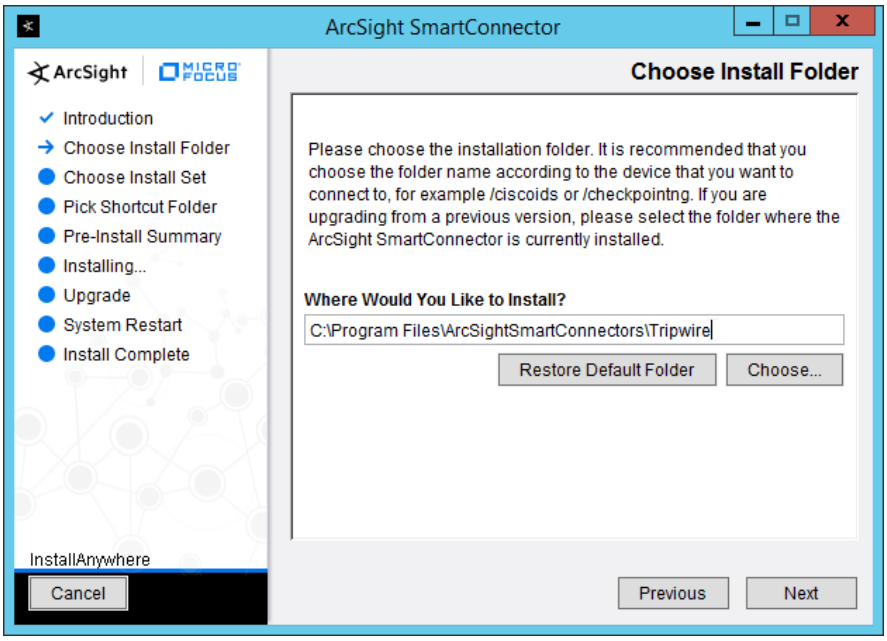
This section will detail the forwarding of logs from **Tripwire Log Center** to **Micro Focus ArcSight.** This will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight,** assuming those logs are being collected by **Tripwire Log Center.**

2.19.1 Install Micro Focus ArcSight

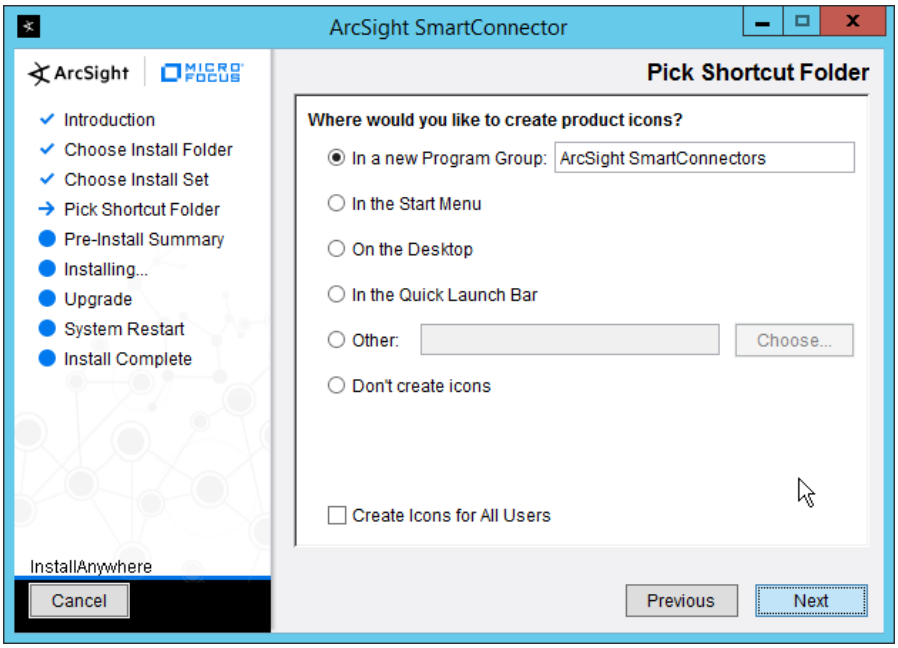
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Tripwire Log Center.**



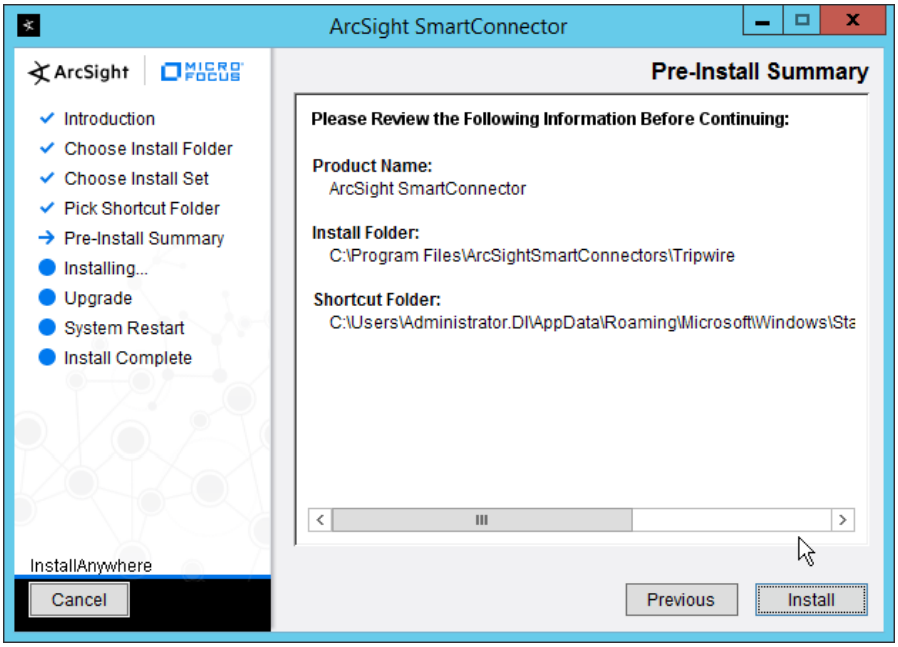
2744
2745 2. Click **Next.**



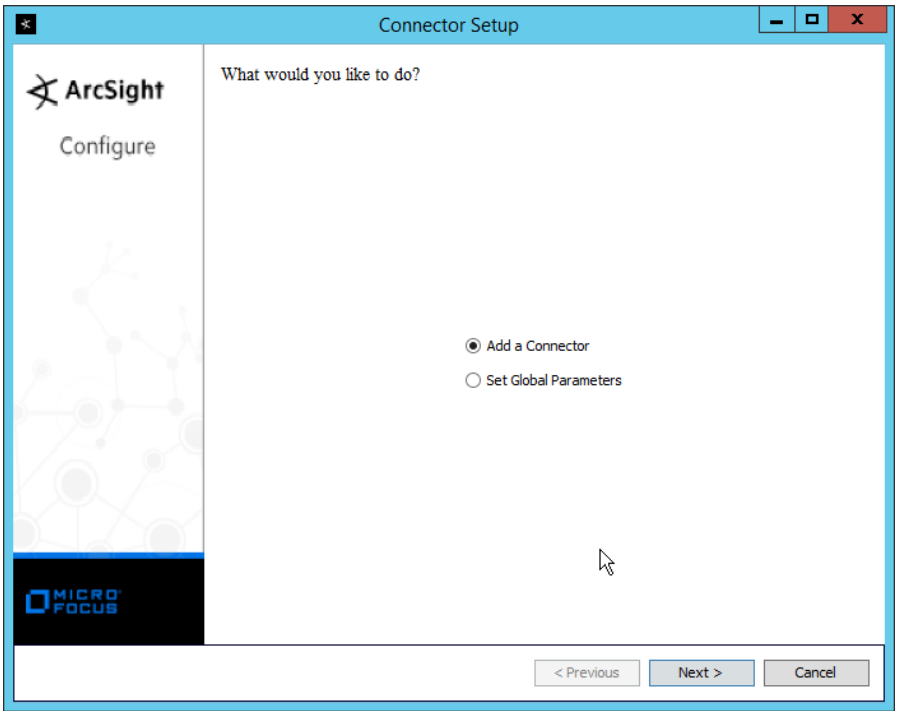
2746
2747 3. Enter *C:\Program Files\ArcSightSmartConnectors\Tripwire.*



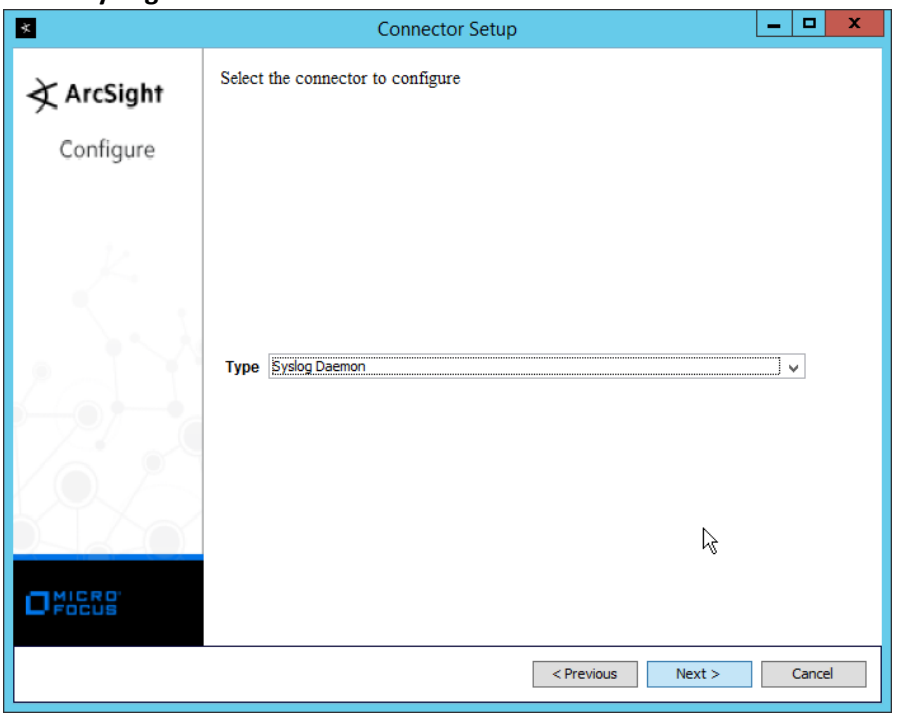
4. Click **Next.**



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

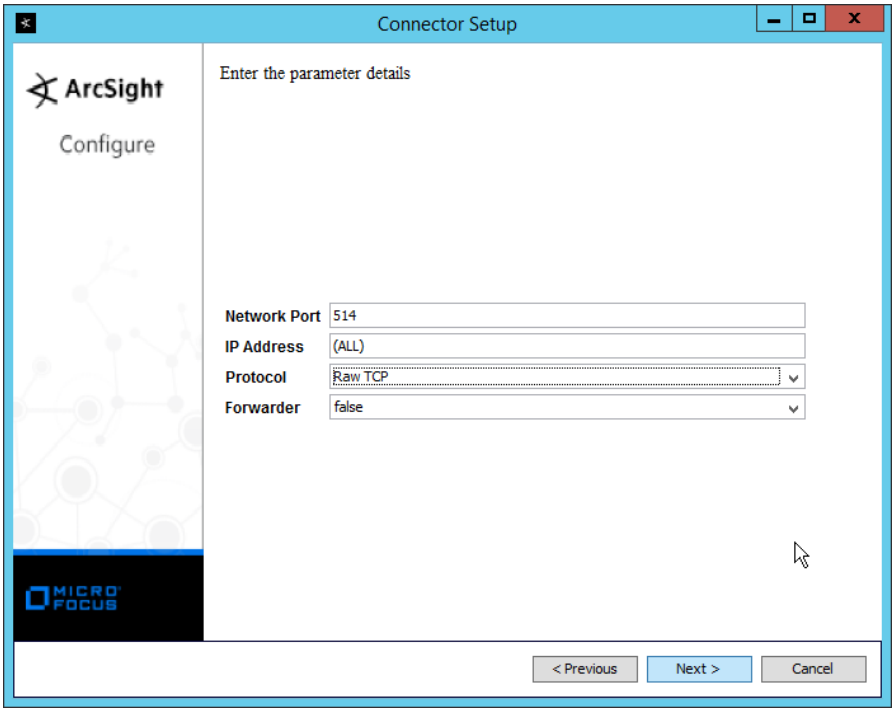


7. Click **Next.**
8. Select **Syslog Daemon.**

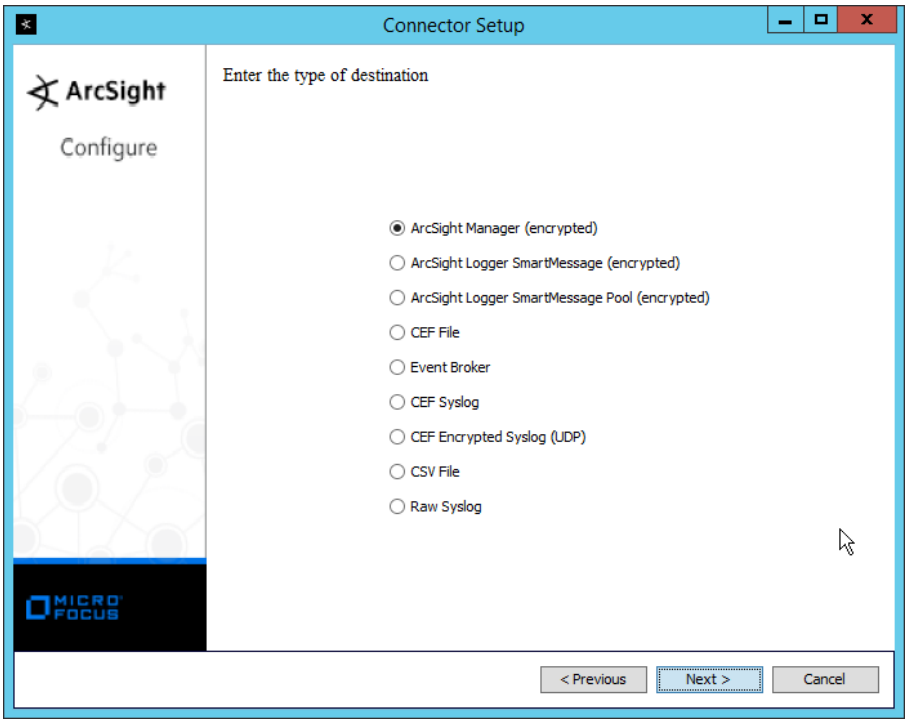


9. Click **Next.**

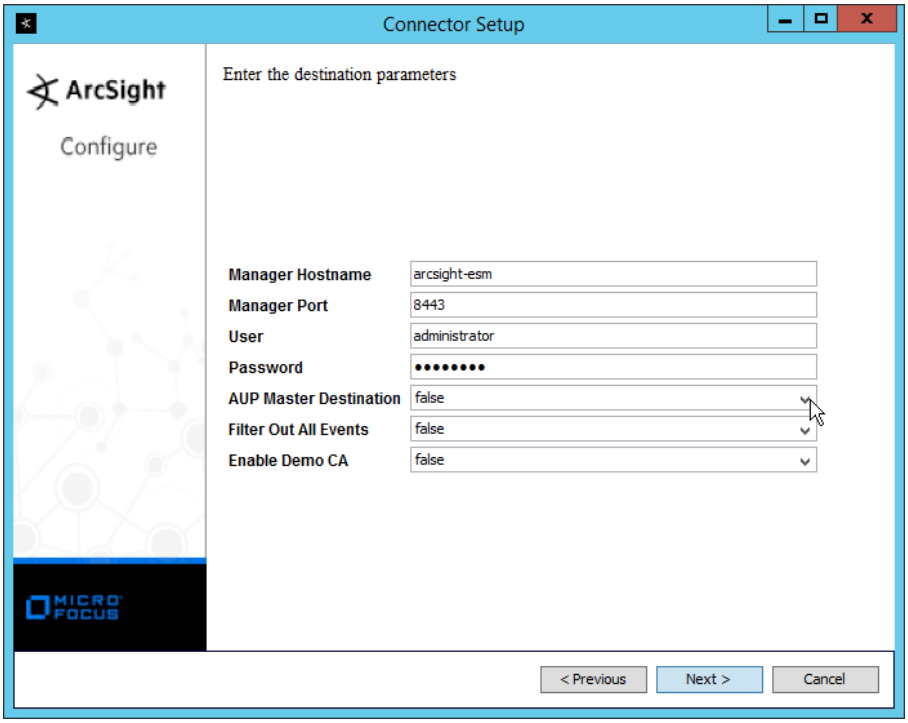
10. Enter a port for the daemon to run on.
11. Select **Raw TCP** for **Protocol.**



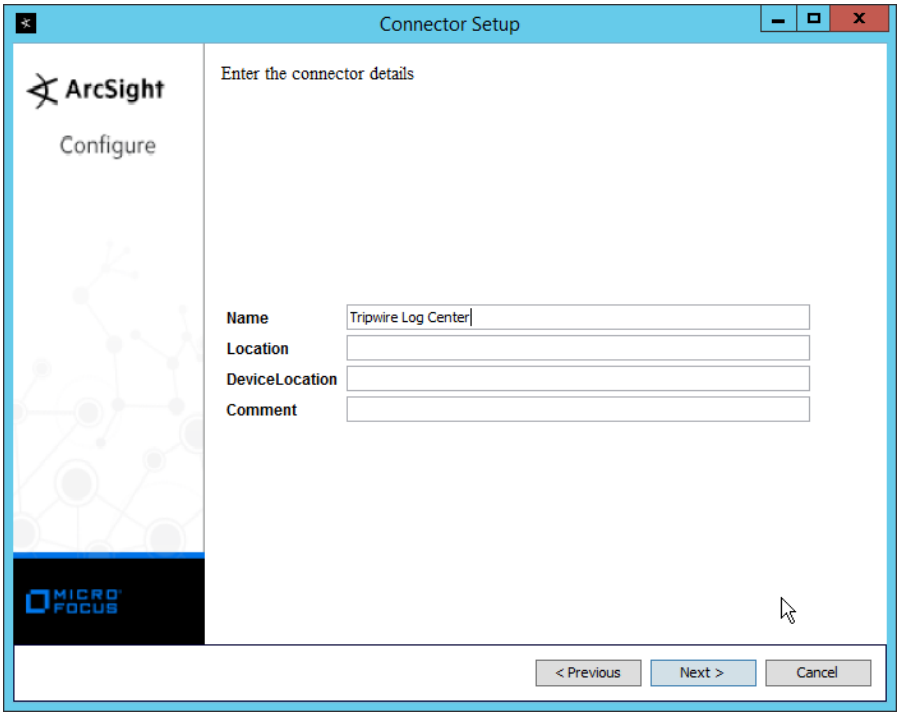
12. Click **Next.**
13. Select **ArcSight Manager (encrypted).**



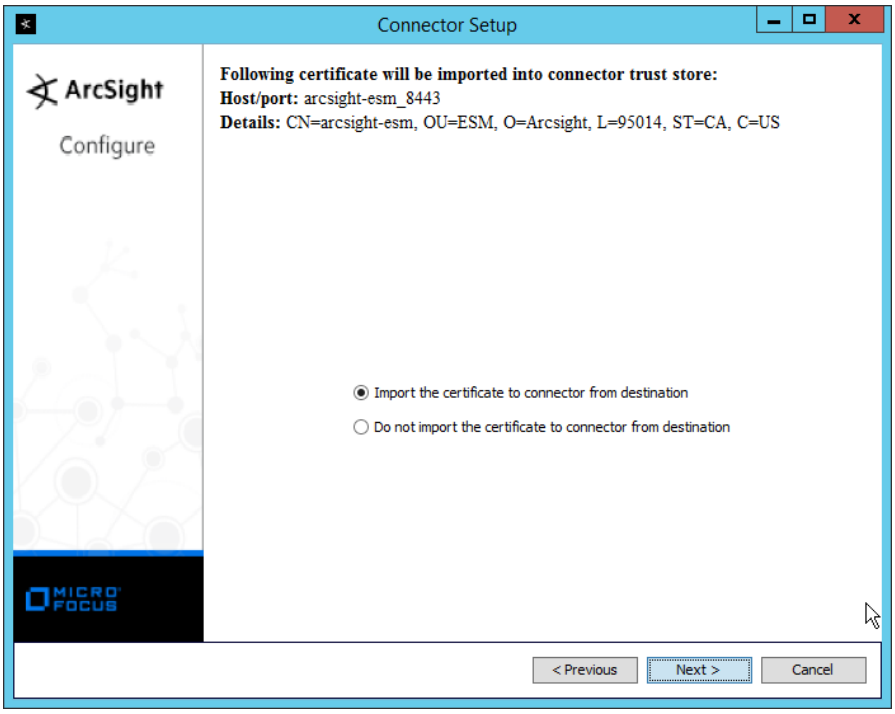
14. Click **Next.**
15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



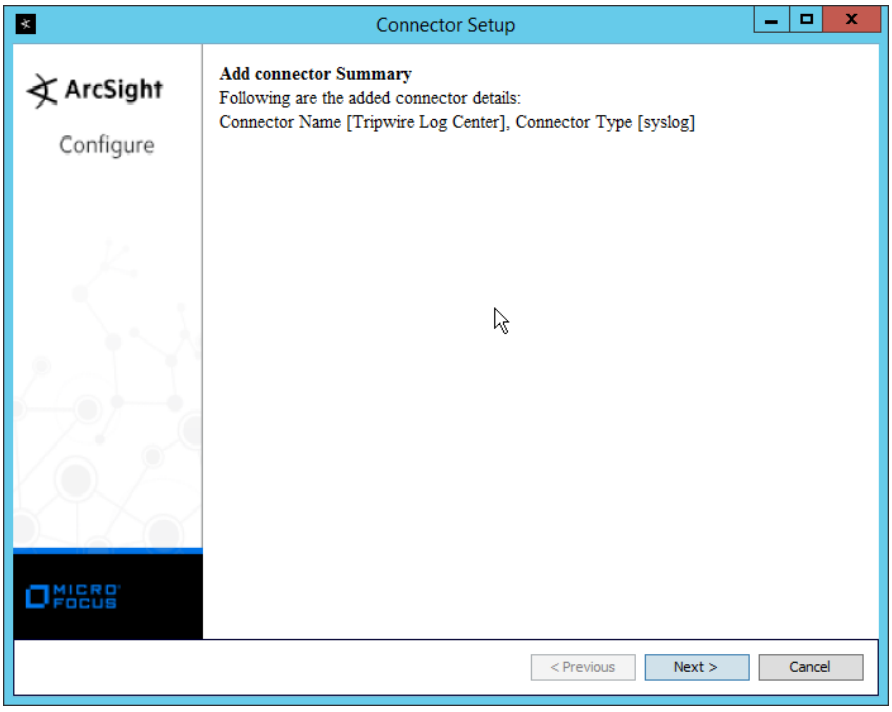
16. Click **Next.**
17. Enter identifying details about the system (only **Name** is required).



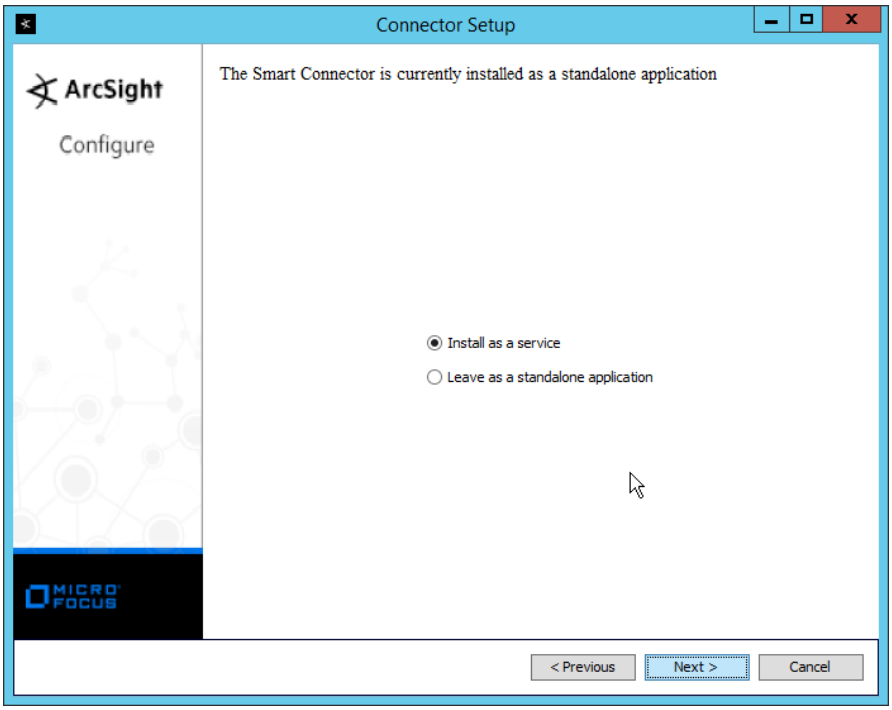
18. Click **Next.**
19. Select **Import the certificate to connector from destination.**



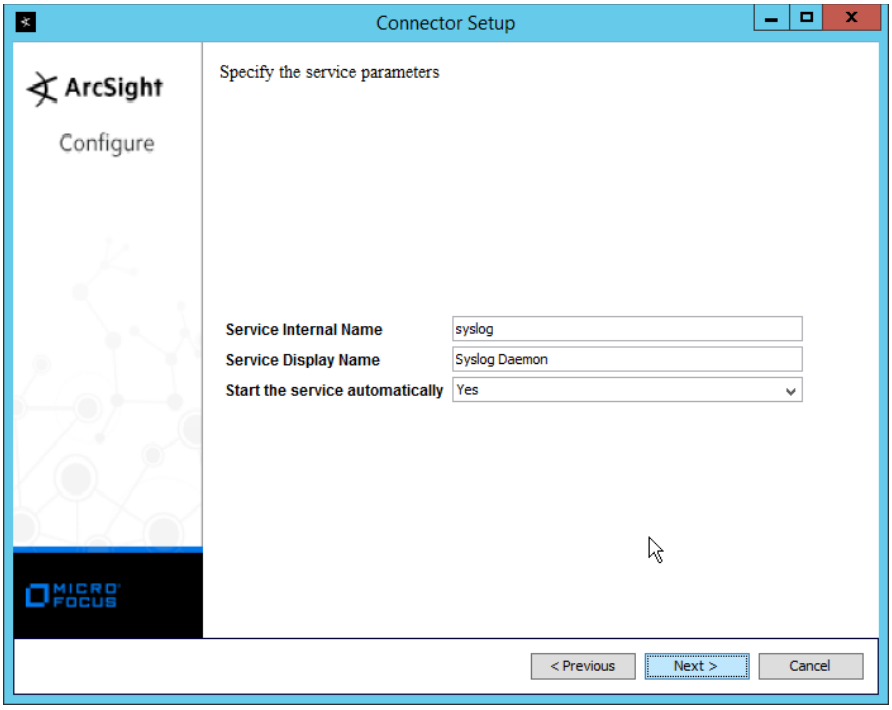
20. Click **Next.**



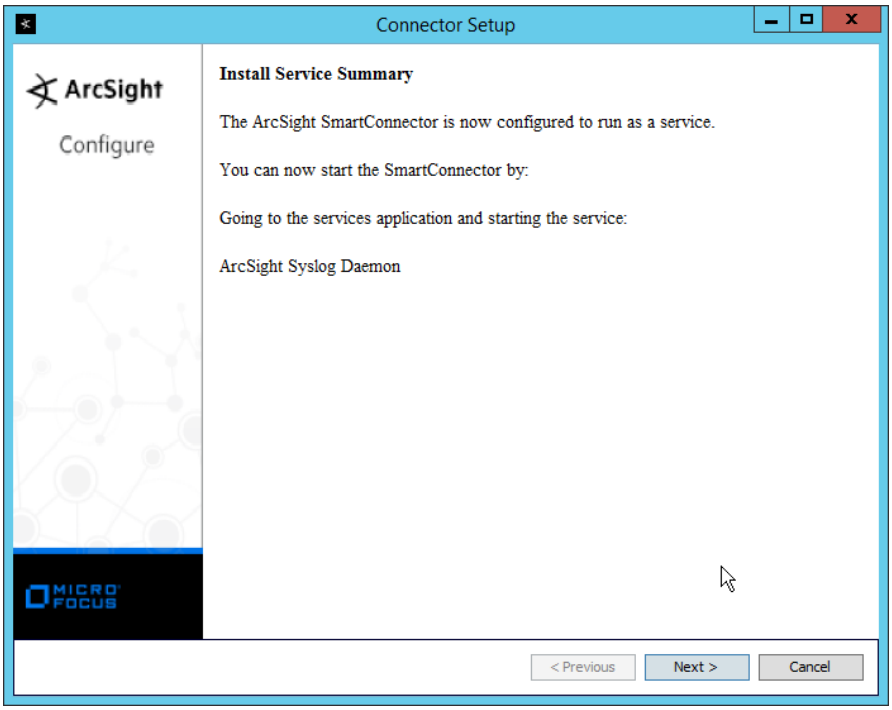
21. Click **Next.**
22. Select **Install as a service.**



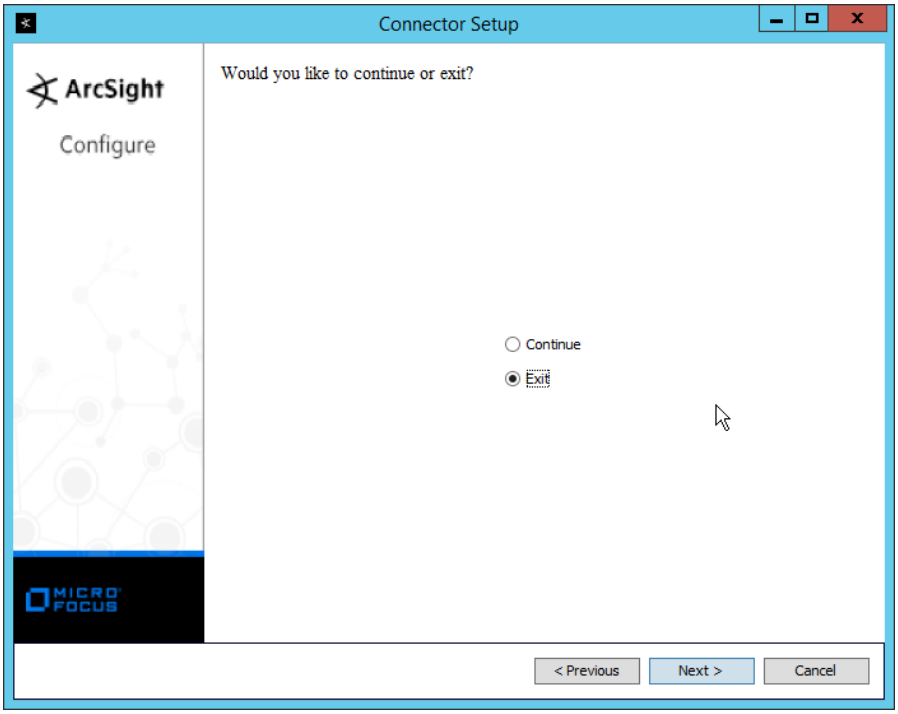
23. Click **Next.**



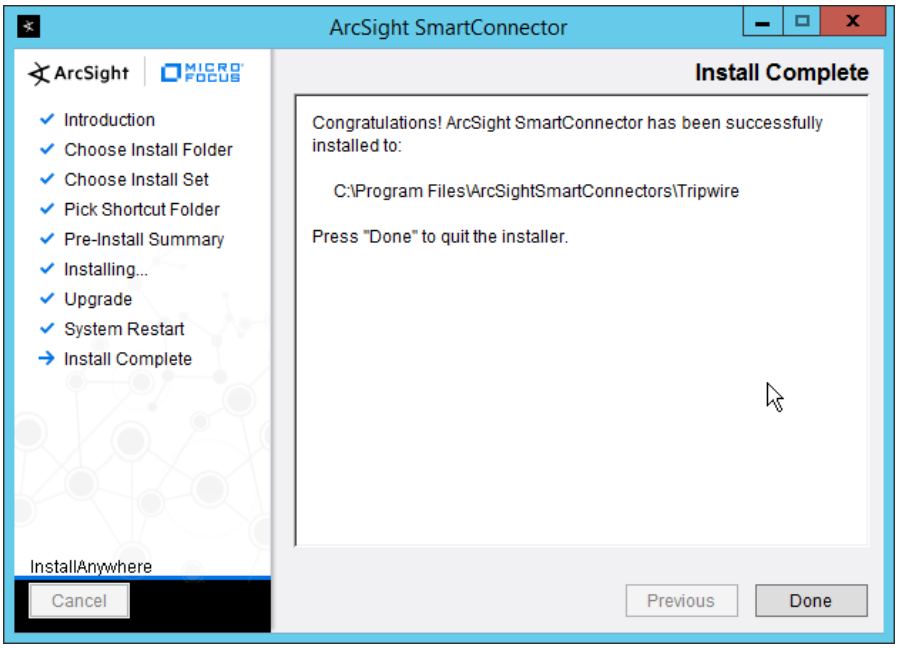
24. Click **Next.**



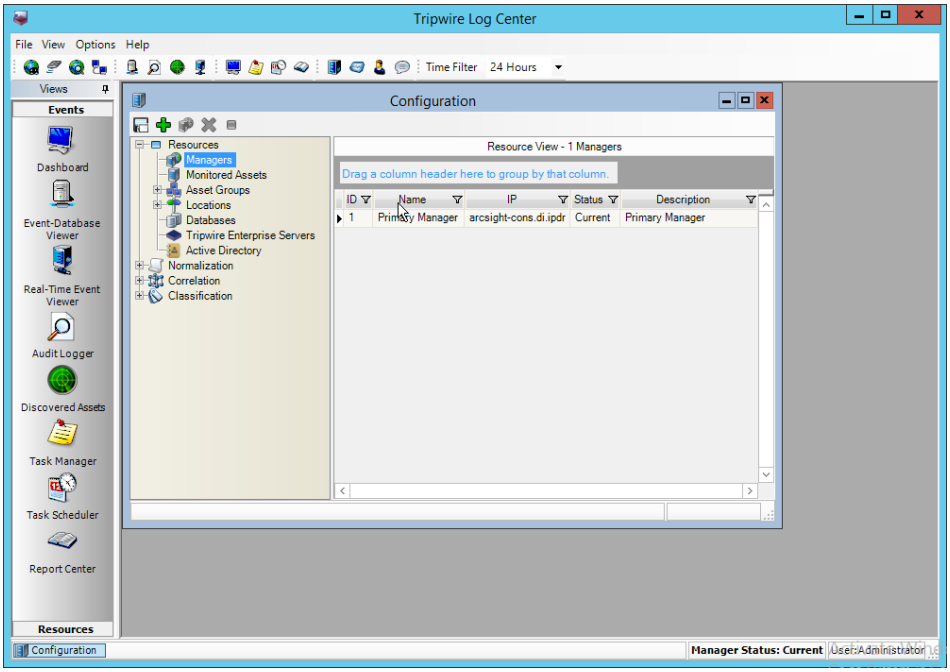
25. Click **Next.**
26. Select **Exit.**



27. Click **Next.**

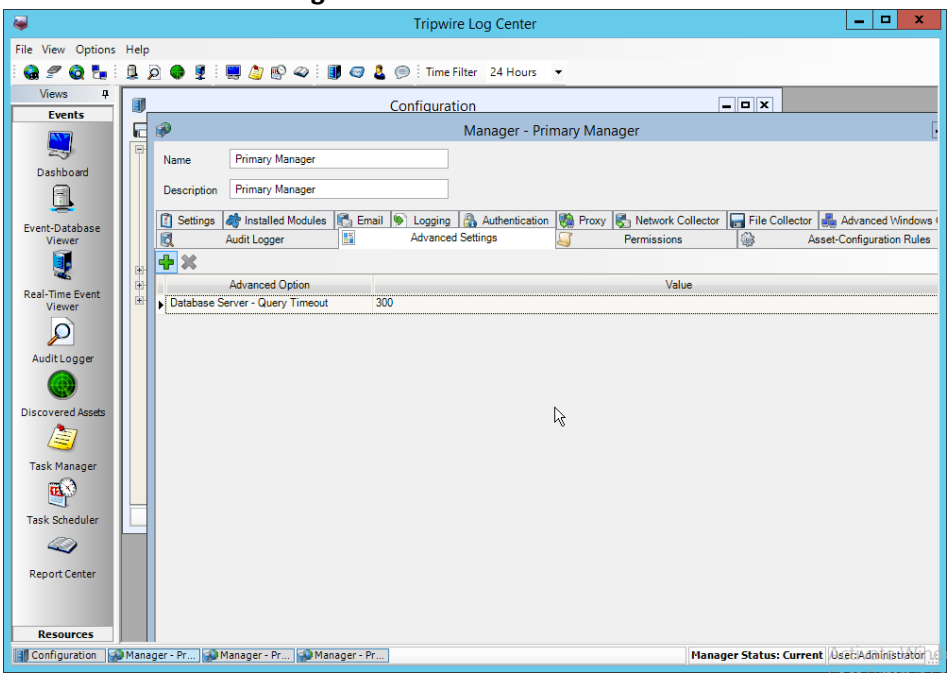


28. Click **Done.**
29. Open the **Tripwire Log Center Console.**
30. Go to the **Configuration Manager.**

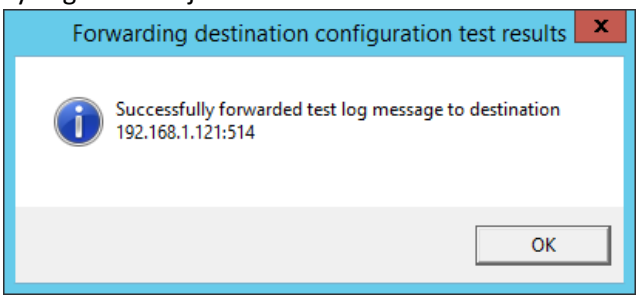


31. Select **Resources** > **Managers.**
32. Double-click the **Primary Manager.**

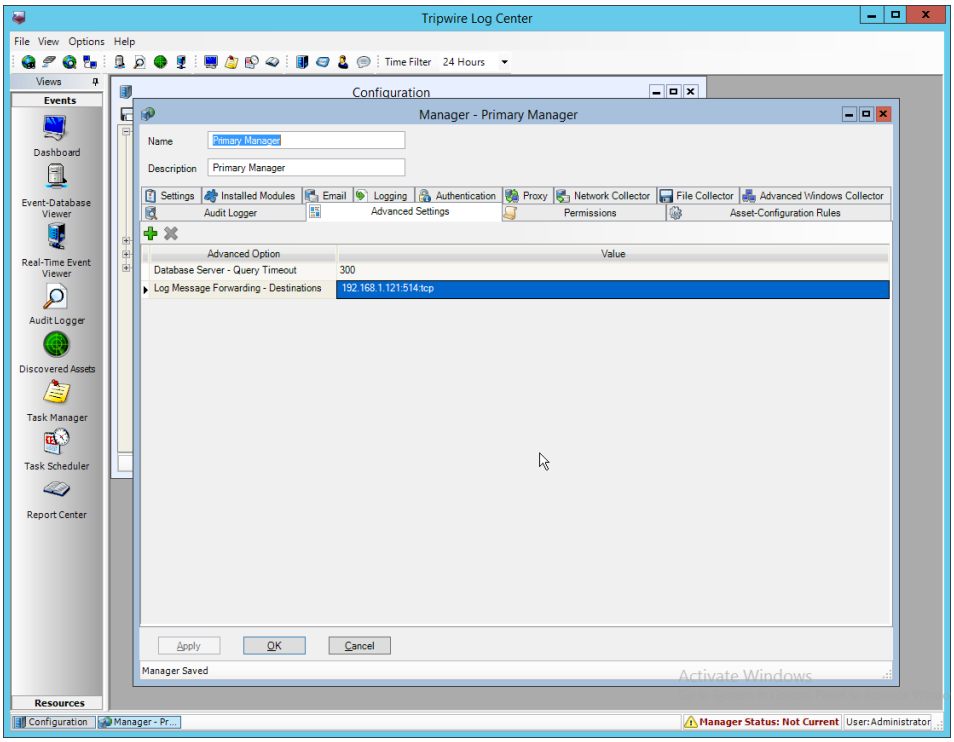
33. Click the **Advanced Settings** tab.



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**.



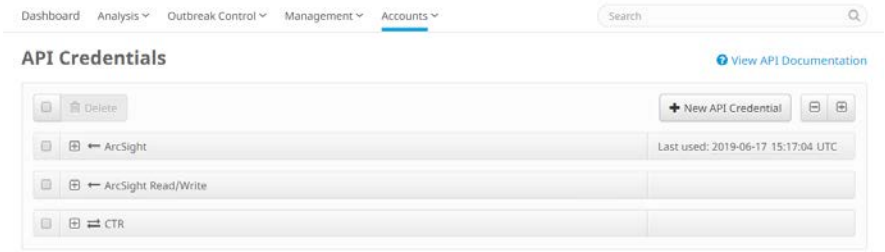
38. Click **OK.**
39. Restart the **Tripwire Log Center Manager.**

2.20 Integration: Micro Focus ArcSight and Cisco AMP

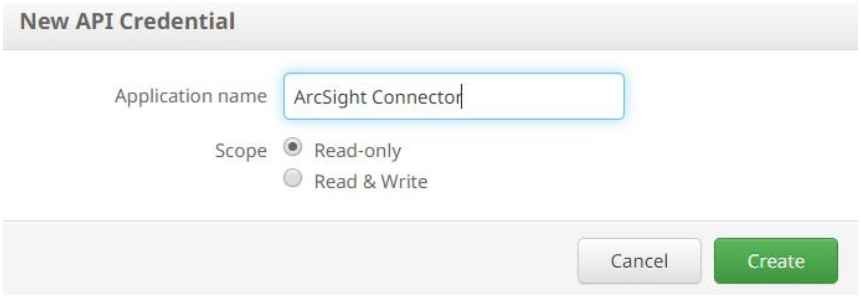
This section will detail the collection of logs from **Cisco AMP's** REST APIs using **Micro Focus ArcSight.**

2.20.1 Create API Credentials for ArcSight to access AMP

1. On the Cisco AMP web console, log in and navigate to **Accounts > API Credentials.**



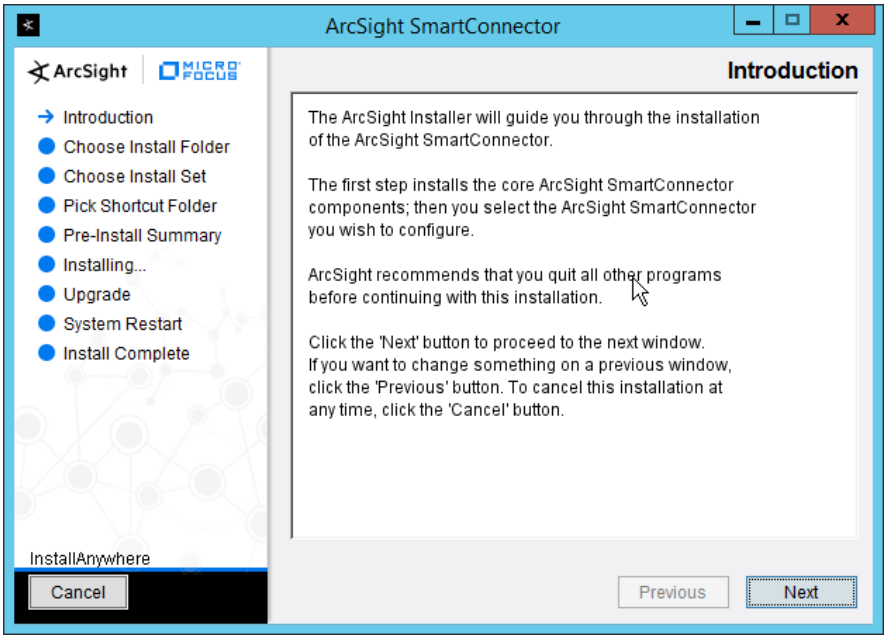
2. Click **New API Credential.**
3. Enter a name for the credential.
4. Select **Read-only.**



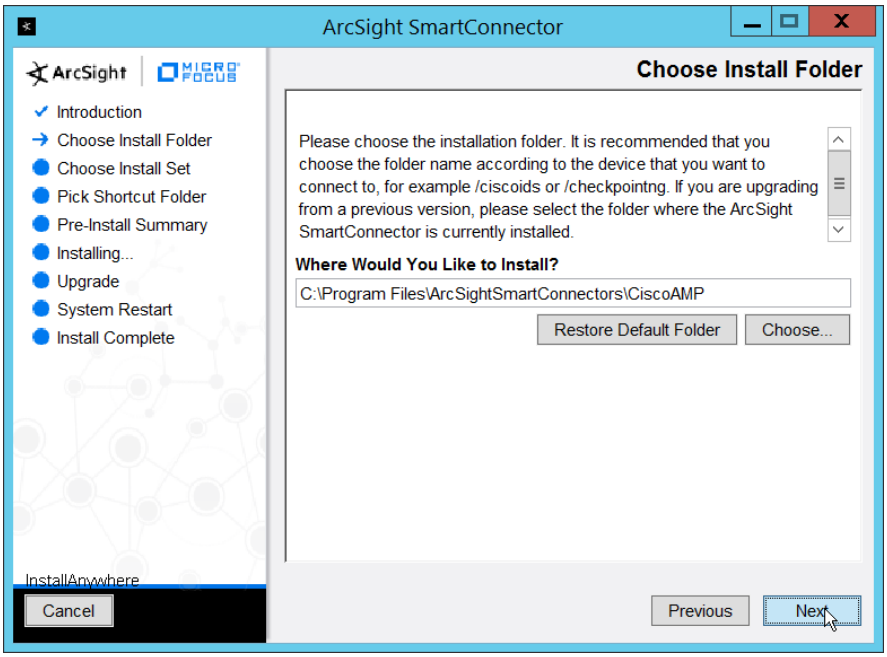
5. Click **Create.**
6. This will direct you to a page with an **ID** and **API Key.** Keep track of these, as you will need them in the setup for the ArcSight Connector, and Cisco AMP may not let you view them again.

2.20.2 Install Micro Focus ArcSight

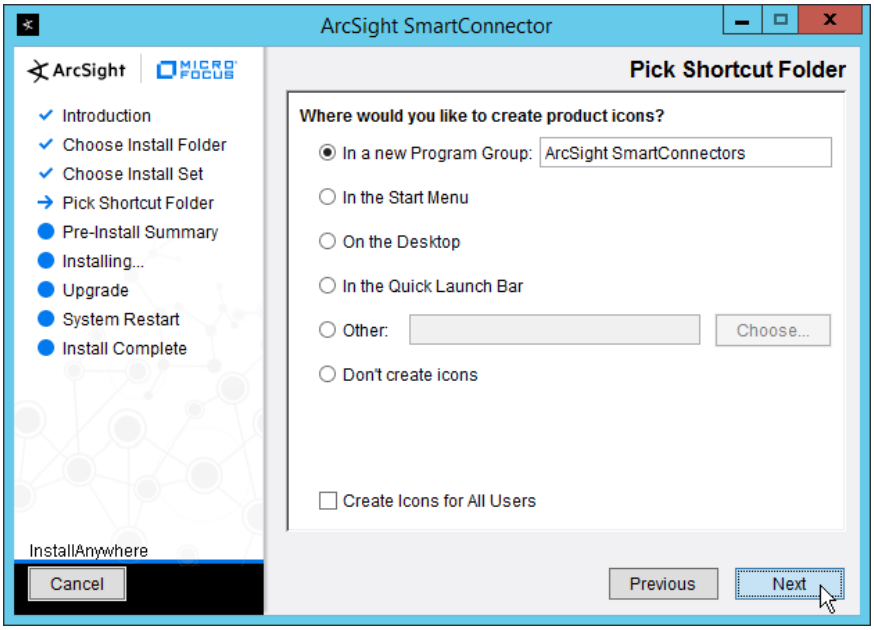
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server.



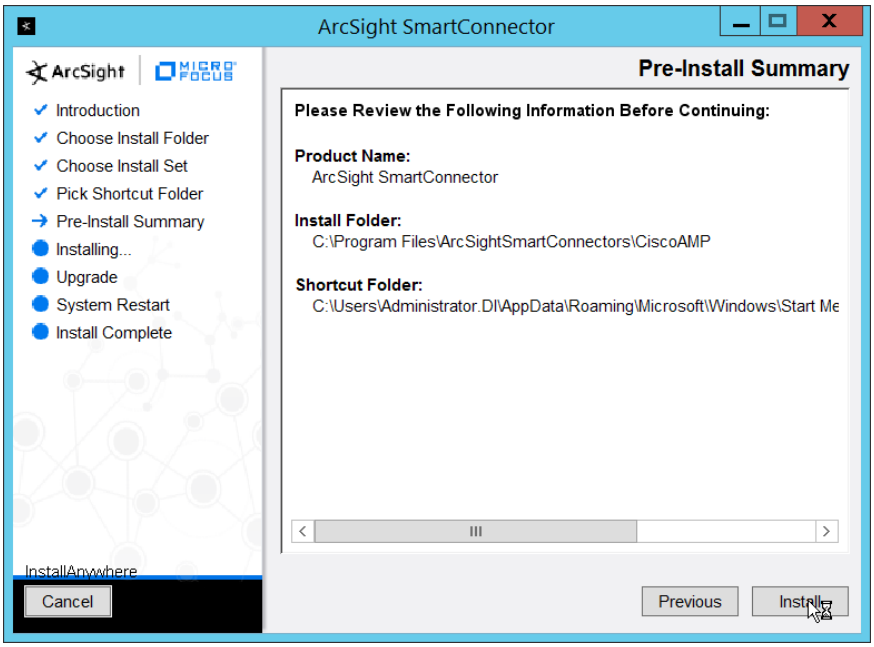
2. Click **Next.**
3. Enter *C:\Program Files\ArcSightSmartConnectors\CiscoAMP.*



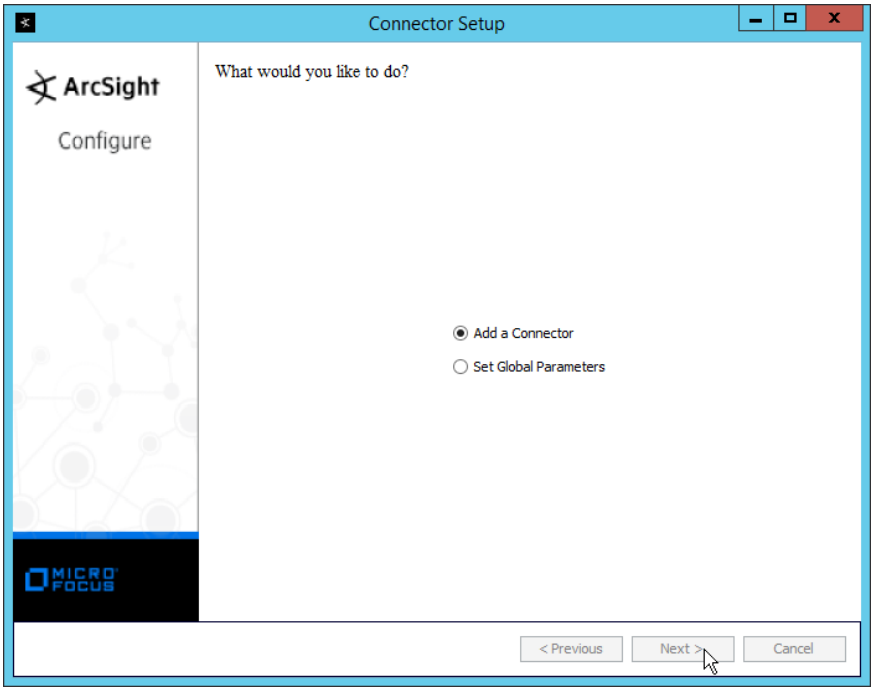
2821
2822 4. Click **Next.**



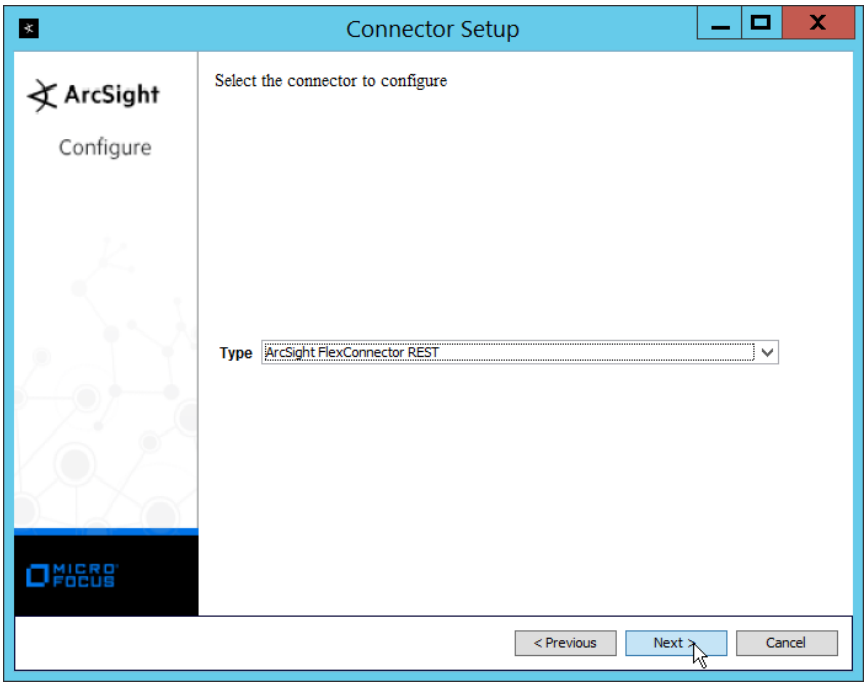
2823
2824 5. Click **Next.**



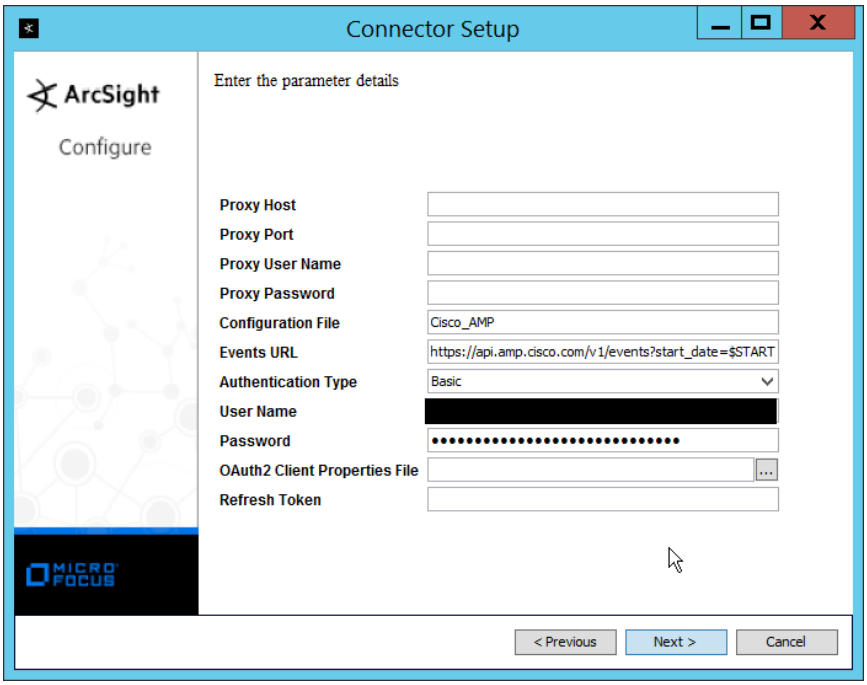
6. Click **Install.**
7. Select **Add a Connector.**



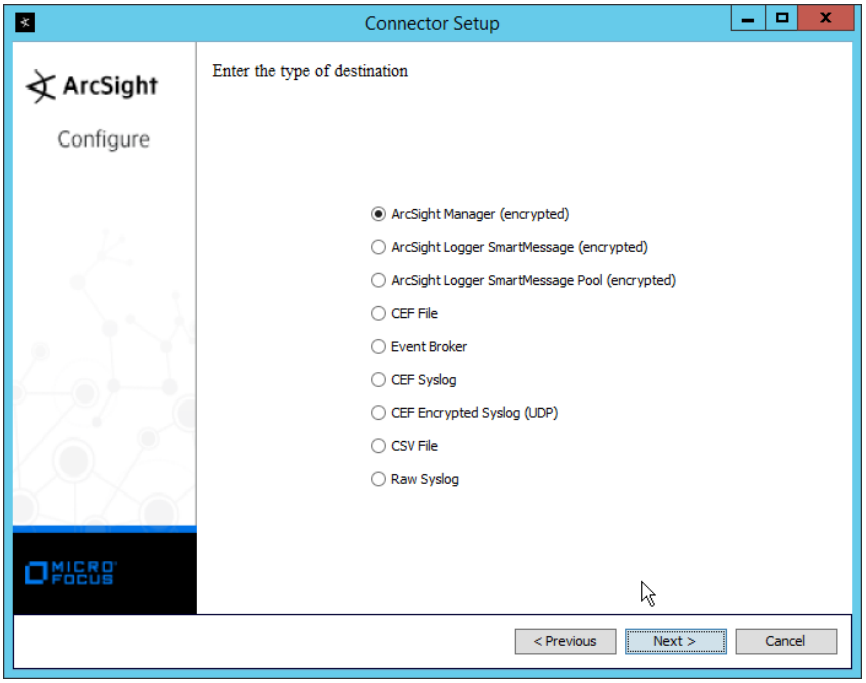
8. Click **Next.**
9. Select **ArcSight FlexConnector REST.**



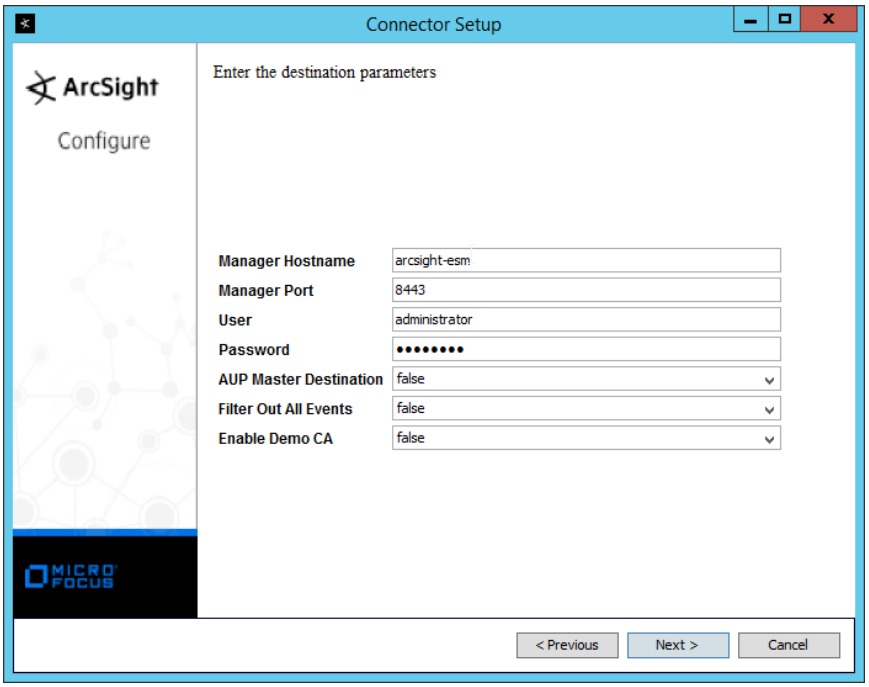
10. Click **Next.**
11. Enter *Cisco_AMP* for the **Configuration File.**
12. Enter https://api.amp.cisco.com/v1/events?start_date=$START_AT_TIME for the **Events URL.** (Note: You can see the Cisco AMP REST API documentation for more information on how to formulate this URL for things other than events.)
13. Enter the username and password from the credential generated on Cisco AMP in Section 2.20.1.



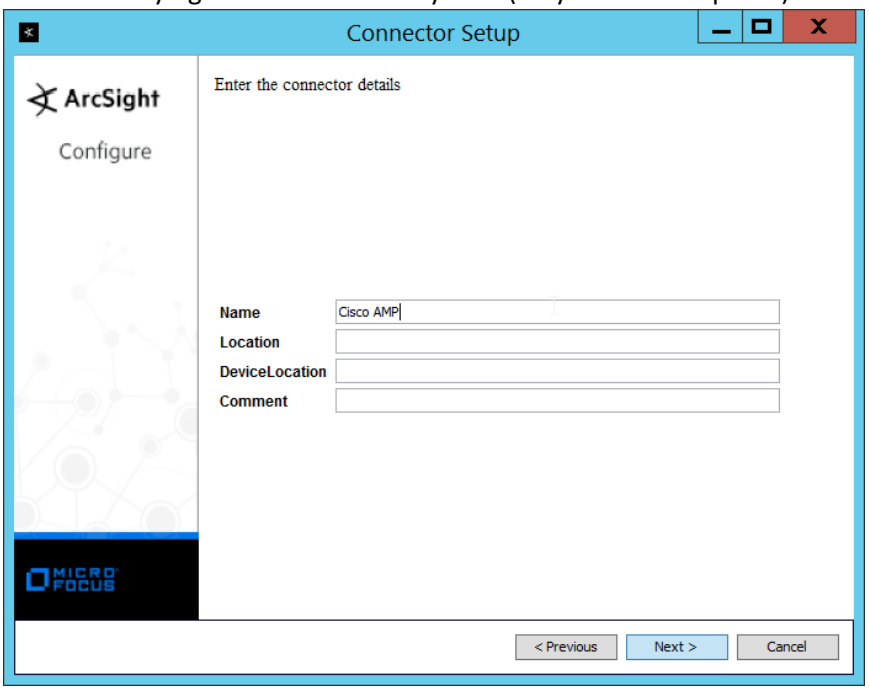
14. Click **Next.**
15. Select **ArcSight Manager (encrypted).**



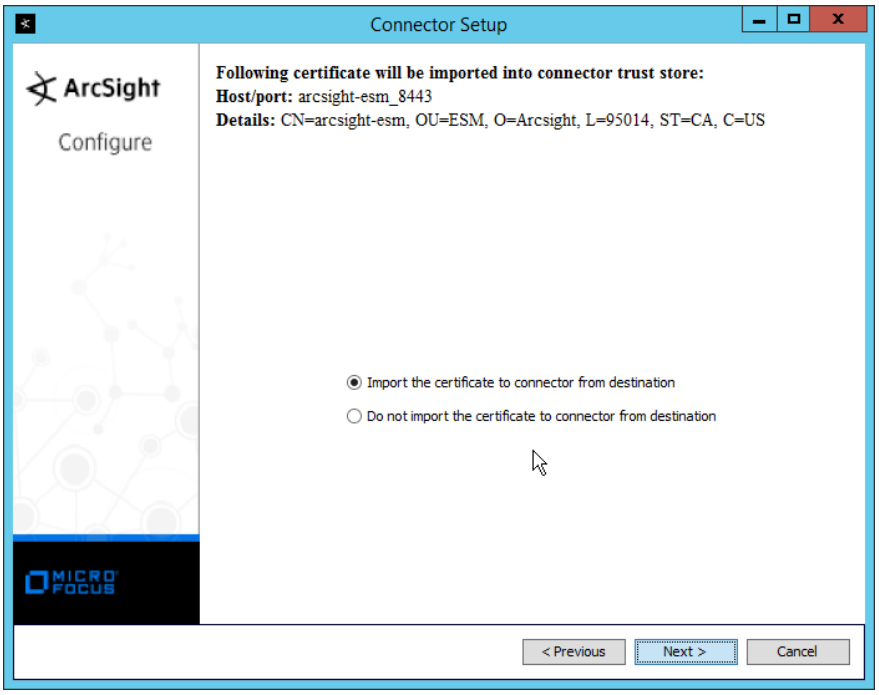
16. Click **Next.**
17. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



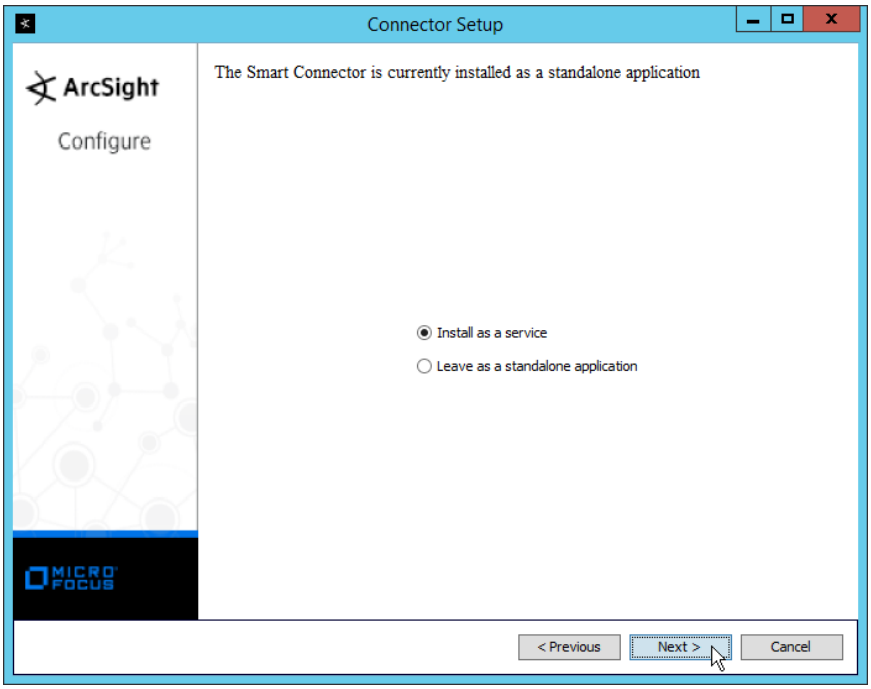
18. Click **Next.**
19. Enter identifying details about the system (only **Name** is required).



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

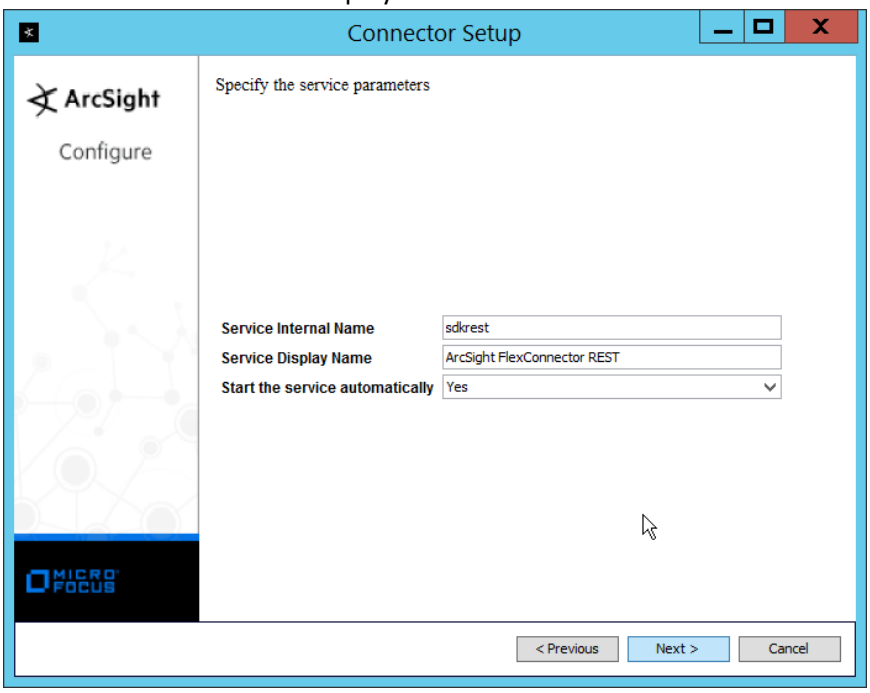


22. Click **Next.**
23. Click **Next.**
24. Select **Install as a service.**

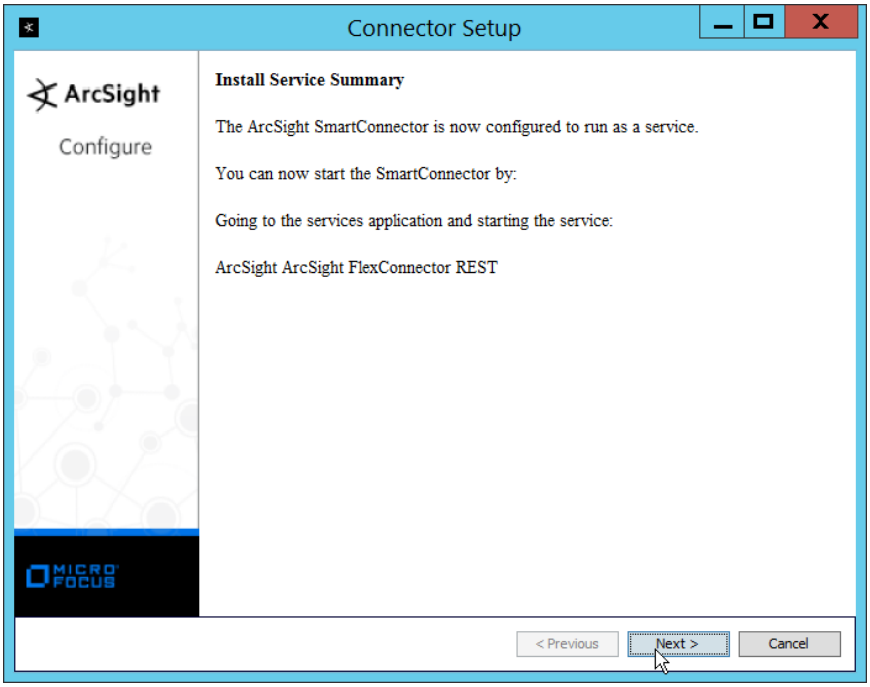


25. Click **Next.**

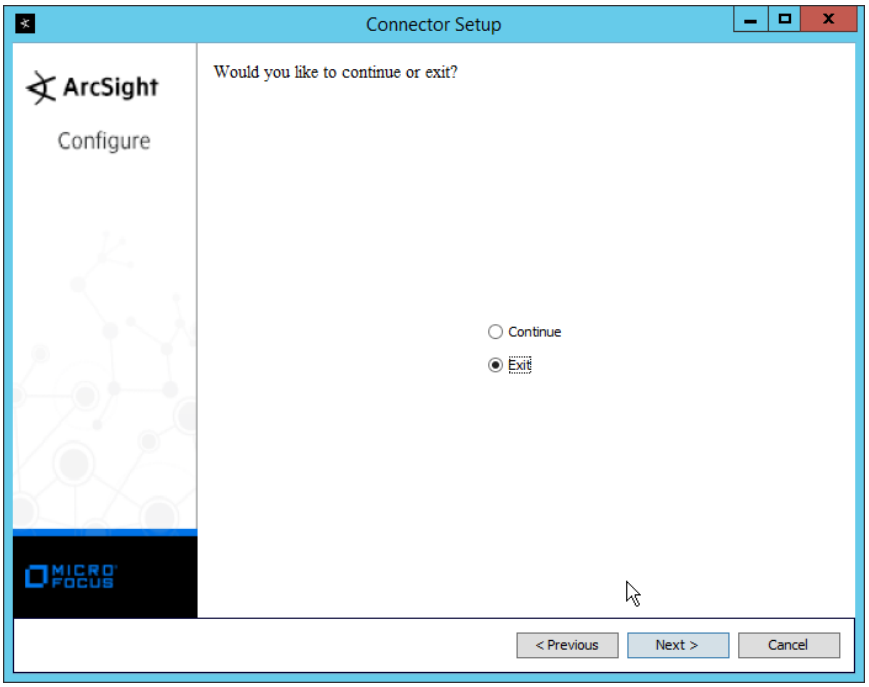
2857 26. Enter a service name and display name.



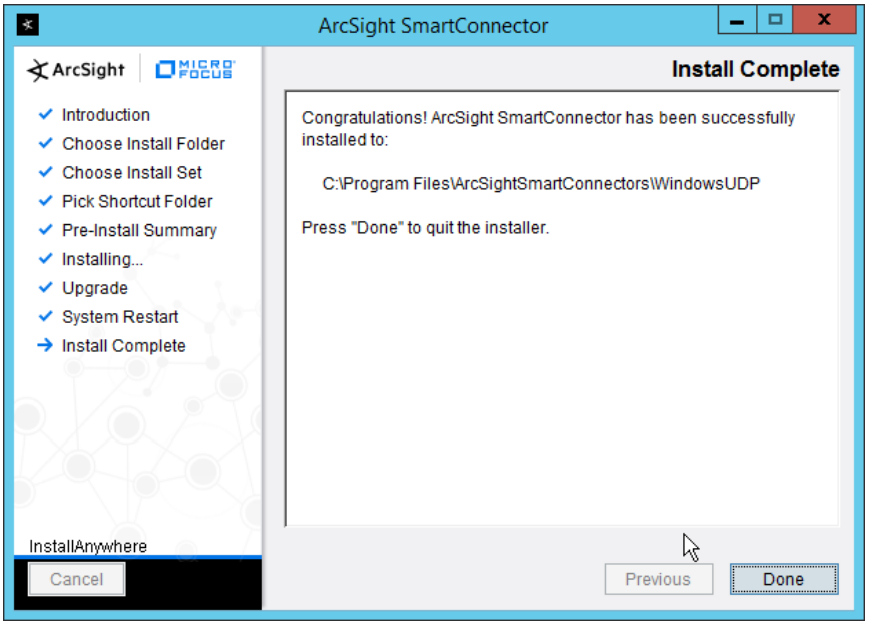
2858
2859 27. Click **Next.**



2860
2861 28. Click **Next.**
2862 29. Select **Exit.**



30. Click **Next.**



31. Click **Done.**

2.20.3 Create a Parser for Cisco AMP REST events

1. Ensure that the ArcSight connector service is not running.

2. Create a text file located at *<ARCSIGHT_HOME>/current/user/agent/flexagent/Cisco_AMP.jsonparser.properties.* (Note: Replace *Cisco_AMP* with the name used for "Configuration File" during setup.)
3. Use the following text to parse some basic information such as the IP, the type of event, and links to Cisco AMP's more detailed descriptions of the event.

```
trigger.node.location=/data
token.count=6

token[0].name=id
token[0].type=String
token[0].location=id

token[1].name=timestamp
token[1].type=String
token[1].location=date

token[2].name=event_type
token[2].type=String
token[2].location=event_type

token[3].name=hostname
token[3].type=String
token[3].location=computer/hostname

token[4].name=external_ip
token[4].type=IPAddress
token[4].location=computer/external_ip

token[5].name=links
token[5].type=String
token[5].location=links

event.deviceReceiptTime=__createOptionalTimeStampFromString(timestamp,"y
yyy-MM-dd'T'HH:mm:ssX")
event.destinationAddress=external_ip
event.destinationHostName=hostname
event.name=event_type
event.message=links
event.deviceCustomString1=id
event.deviceCustomString1Label=__stringConstant("AMP Event ID")
```

4. This parser will allow for details of Cisco AMP events to be shown in ArcSight. Custom parsers are a functionality of ArcSight. For more information on the creation of custom parsers, please see the *ArcSight FlexConnector Developer's Guide* as well as the *FlexConnector REST Developer's Guide*. You can start the service for these changes to take effect.

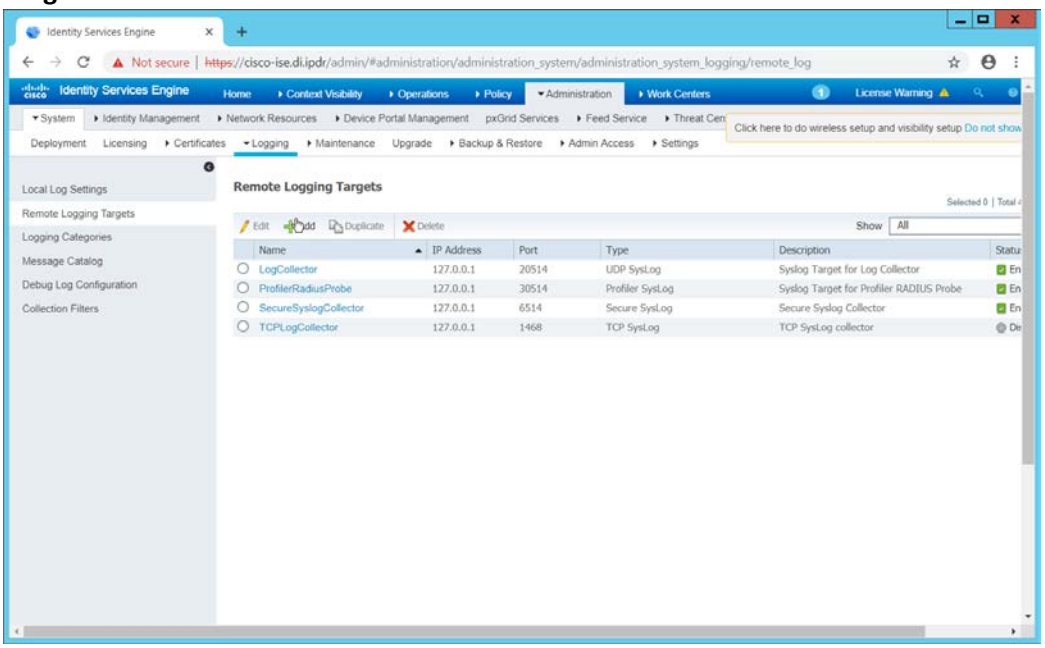
2.21 Integration: Micro Focus ArcSight and Cisco ISE

This integration will briefly detail how to send logs to an ArcSight syslog collector from Cisco ISE. Please see Section 2.18 (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog

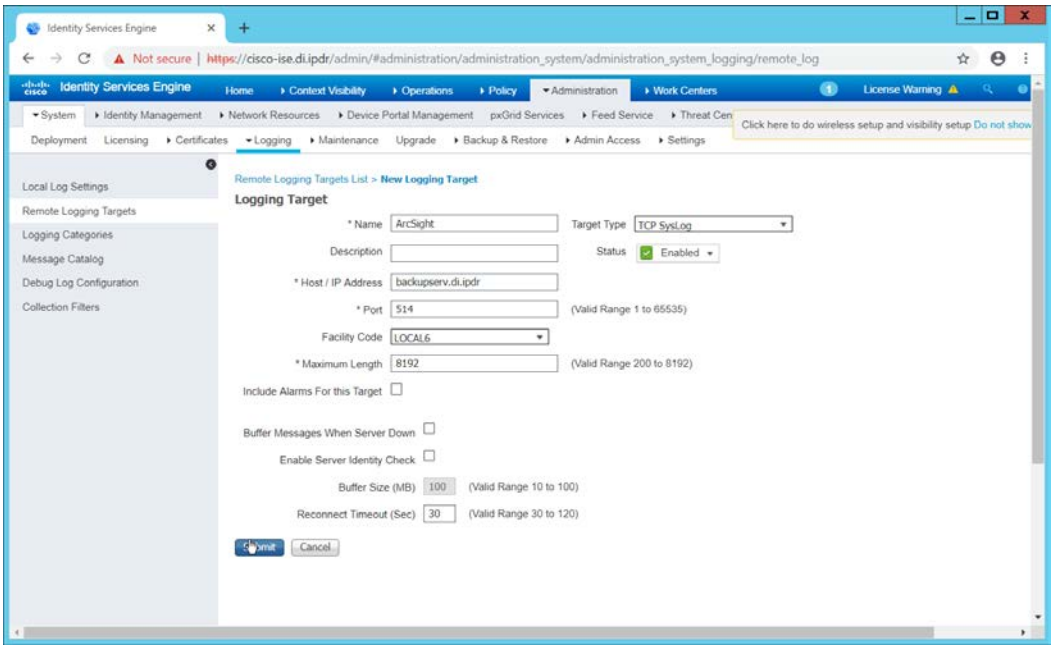
collector. If a server is already configured, you do not need to install a new one—simply use the address of that server to which to forward logs.

2.21.1 Configure Cisco ISE to Forward Logs

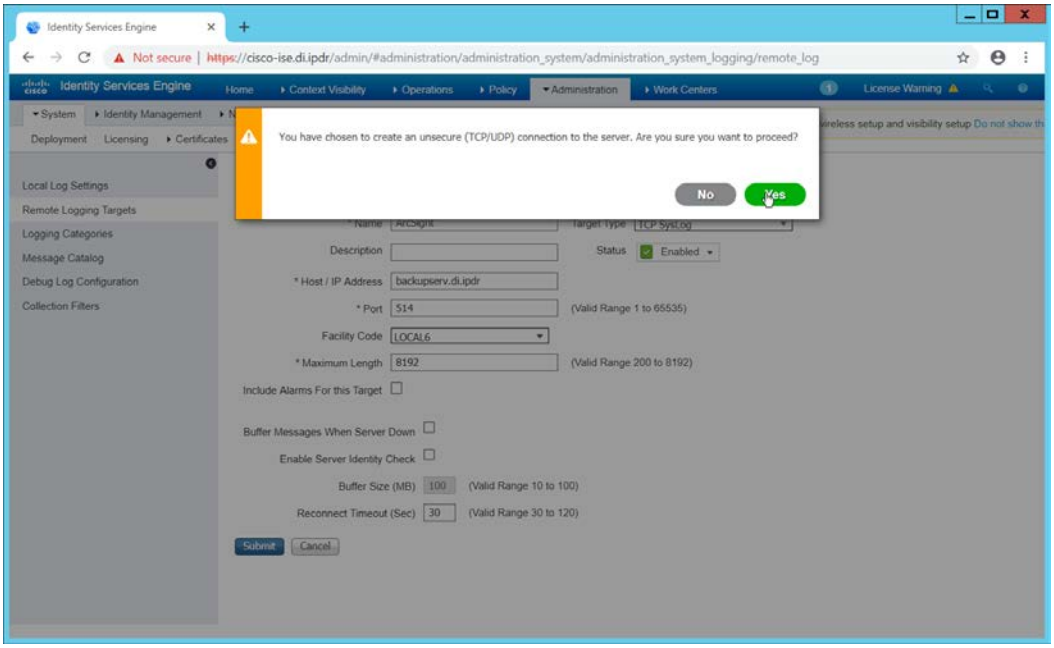
1. In the Cisco ISE web client, navigate to **Administration > System > Logging > Remote Logging Targets.**



2. Click **Add.**
3. Enter a name for **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.**



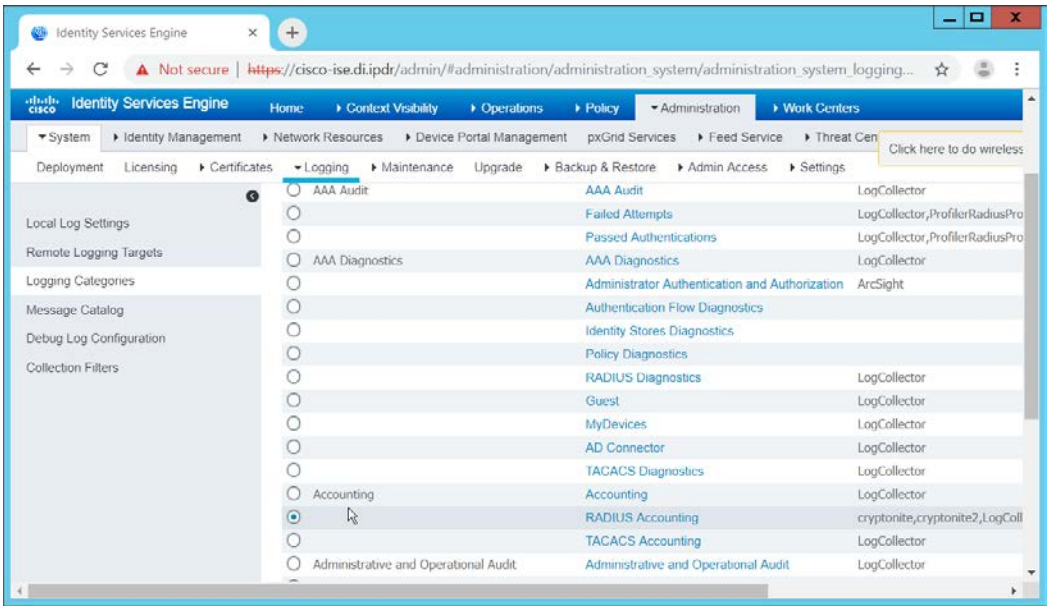
9. Click **Submit.**



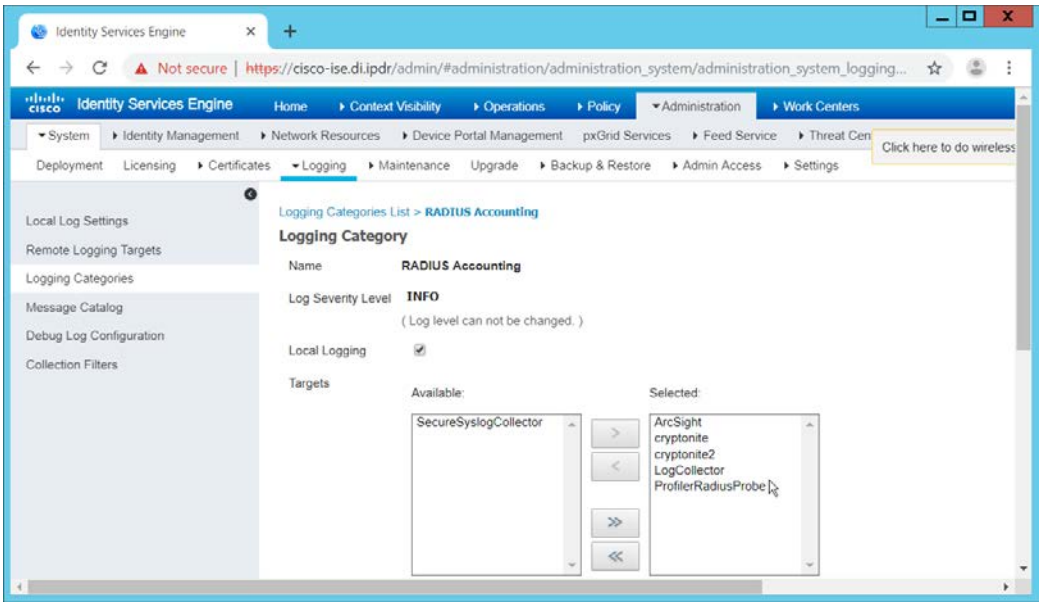
10. Click **Yes.**

2.21.2 Select Logs for Forwarding

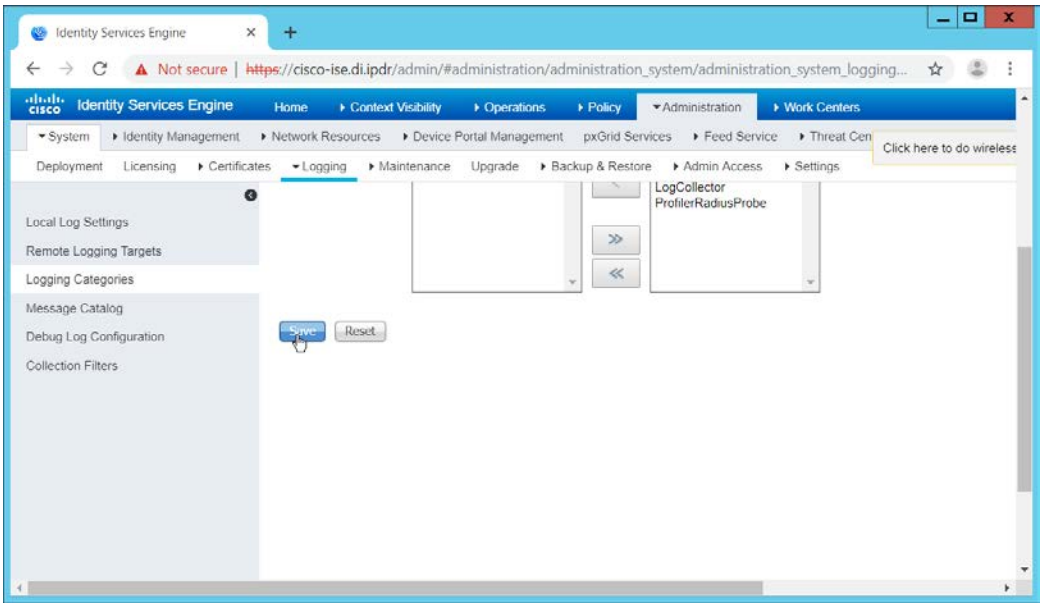
1. Navigate to **System > Logging > Logging Categories.**



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.

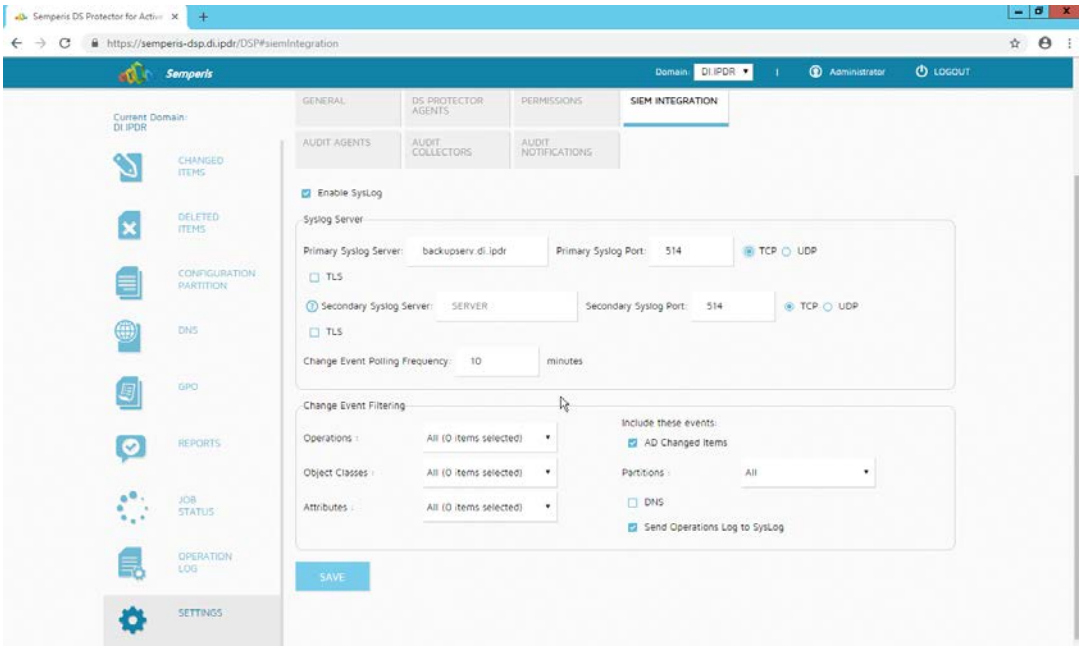
2.22 Integration: Micro Focus ArcSight and Semperis DSP

This integration will briefly detail how to send logs to an ArcSight syslog collector from Semperis DSP. Please see Section 2.18 (under integrating Tripwire & ArcSight) 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 use the address of that server to which to forward logs.

Note: This integration requires Semperis DSP version 2.6.

2.22.1 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 it as **All.**



8. Click **Save.**

9. Click **Close.**

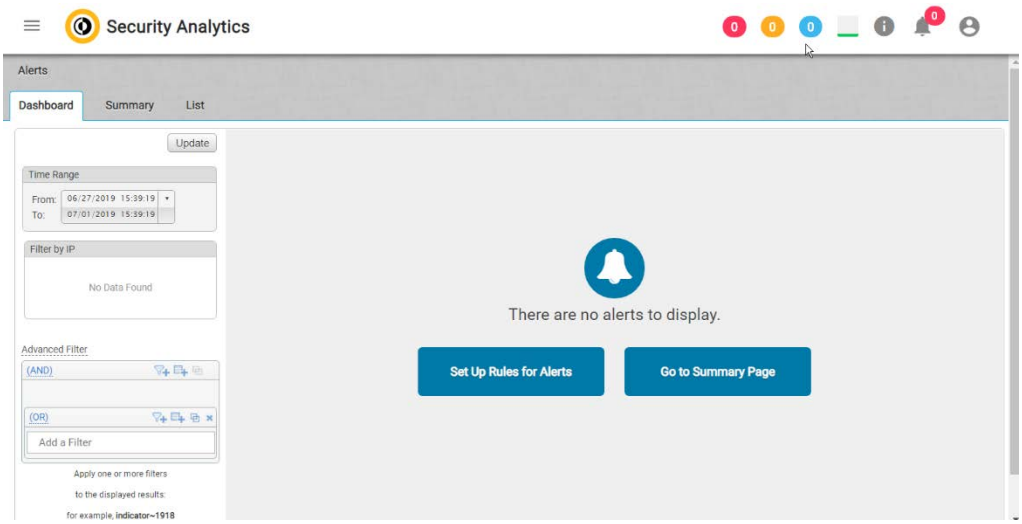
2.23 Integration: Micro Focus ArcSight and Symantec Analytics

This section will first detail the forwarding of logs from **Symantec Analytics** to **Micro Focus ArcSight**. Please see section **2.18** (under integrating Tripwire & ArcSight) 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 use the address of that server to which to forward logs.

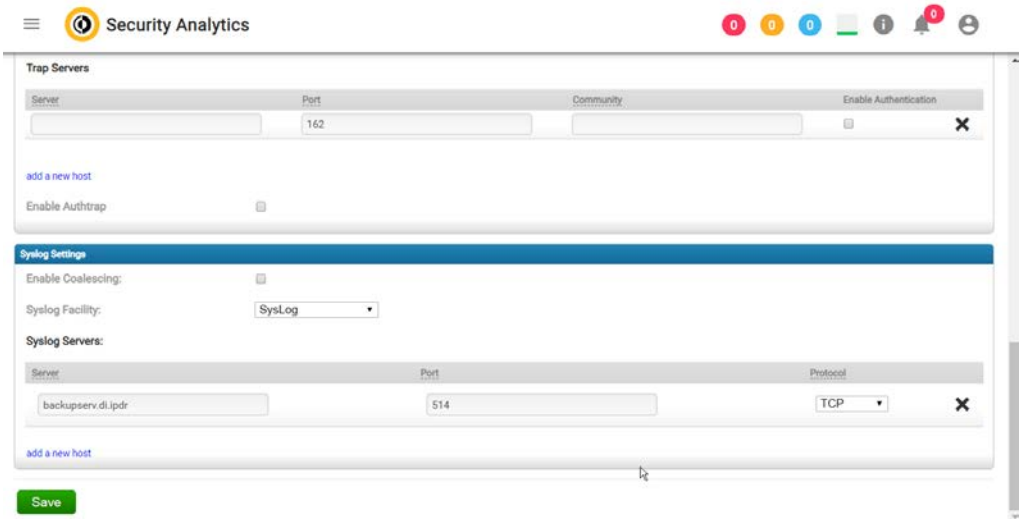
The second part of this section will detail a further integration for ArcSight that allows ArcSight to better analyze network packets received from Symantec Analytics.

2.23.1 Configure Symantec Analytics to Forward Logs

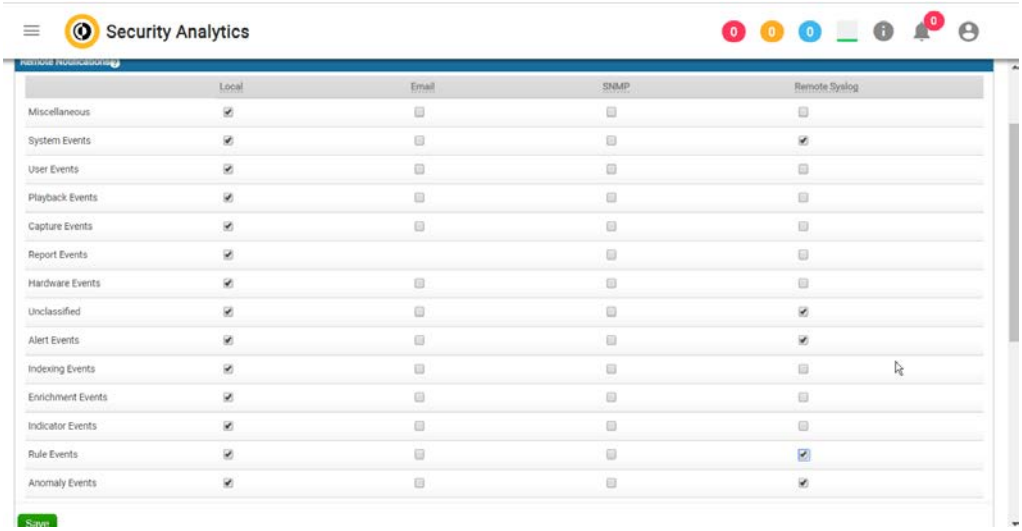
1. Log in to the Symantec Analytics web console.



2. Click the **menu** icon in the top left.
3. Navigate to **Settings** > **Communication.**
4. Scroll down to the **Syslog Settings** section.
5. Select **SysLog** for **Syslog Facility.**
6. Enter the hostname or IP of the ArcSight syslog collector server under **Server.**
7. Enter **514** for the port.
8. Select **TCP** for the protocol.



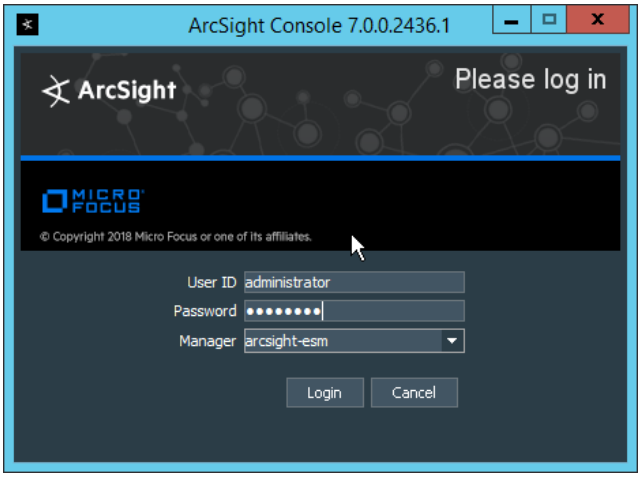
9. Click **Save.**
10. Click the **Advanced** tab.
11. Select the box under **Remote Syslog** column for any events that you wish to forward to ArcSight, for example, **System Events**, **Unclassified Events**, **Alert Events**, **Rule Events**, **Anomaly Events.**



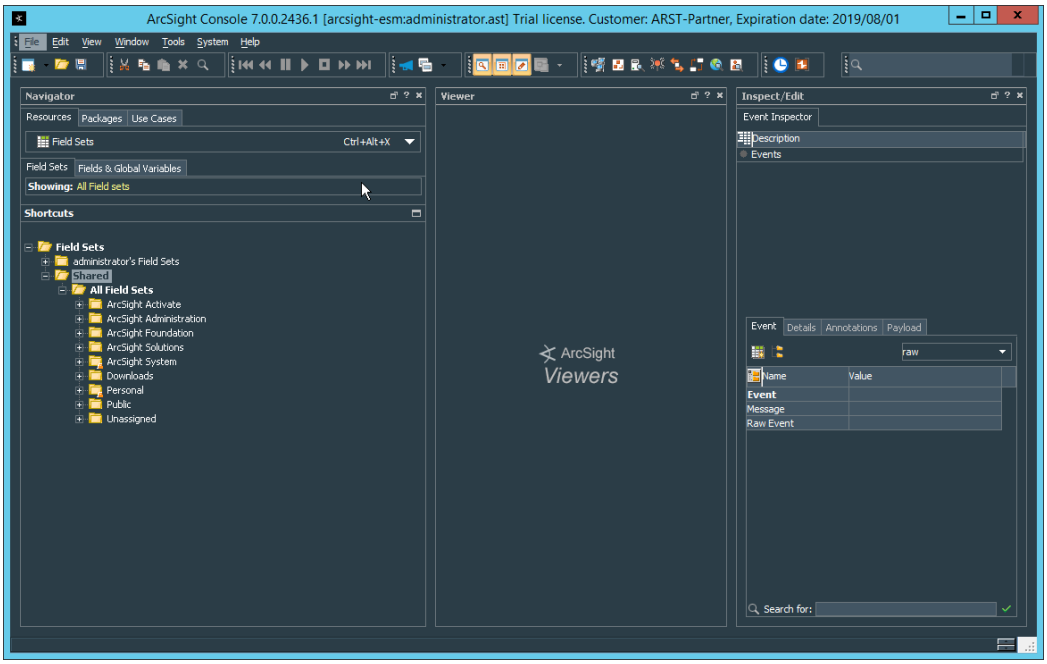
12. Click **Save.**

2.23.2 Install Symantec Analytics Package for ArcSight

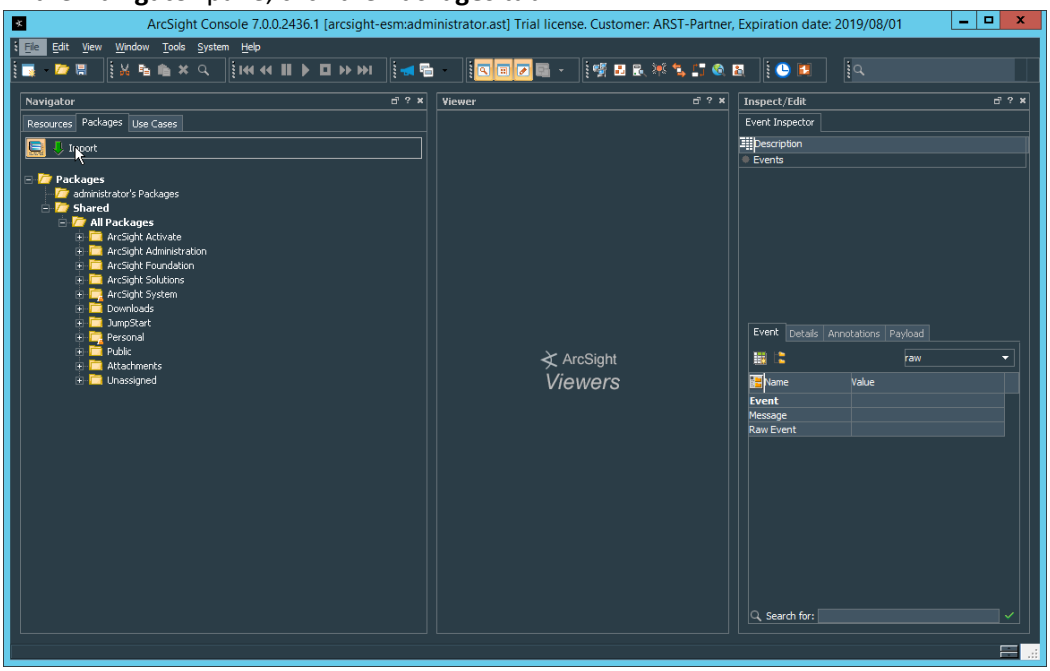
1. Navigate to the ArcSight marketplace. Look for the "Blue Coat Security Analytics" package for ArcSight. It may be available here: https://marketplace.microfocus.com/arcsight/content/blue-coat-security-analytics-platform but not please contact your ArcSight representative to get the package. The package should be called **Blue_Coat_SA_HP_ArcSight-3.0.arb.**
2. Place this package on a system with **ArcSight ESM Console** installed.



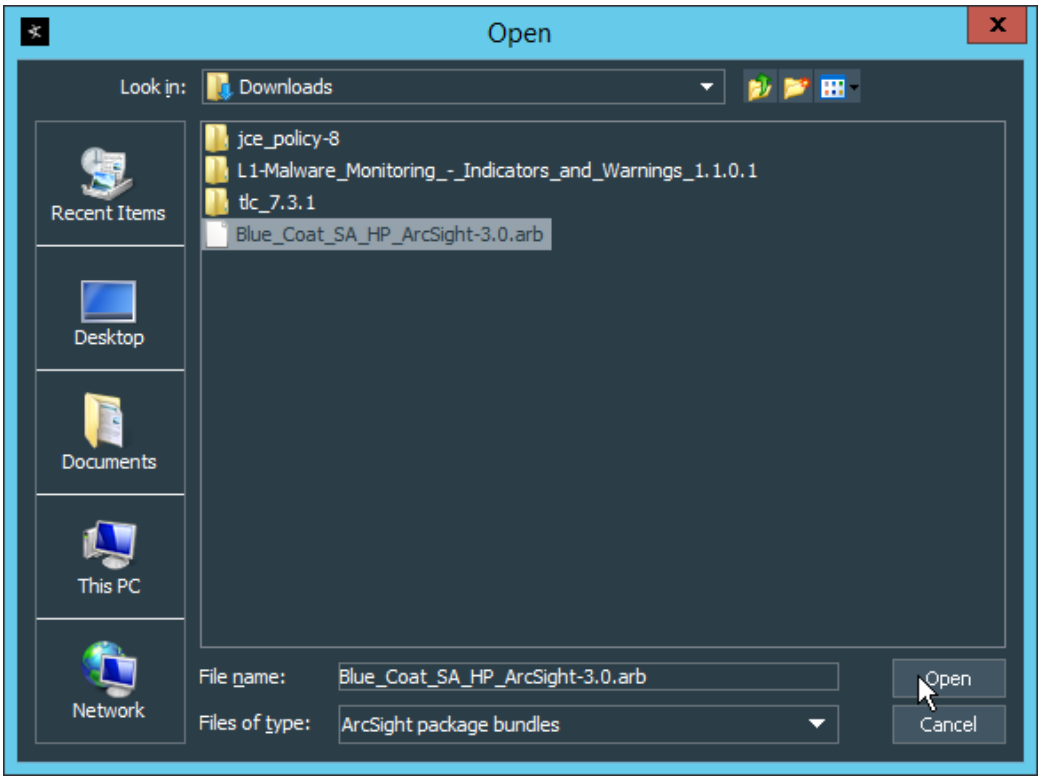
3. Log in to the **ArcSight ESM Console** with a user that has the privileges to install packages.



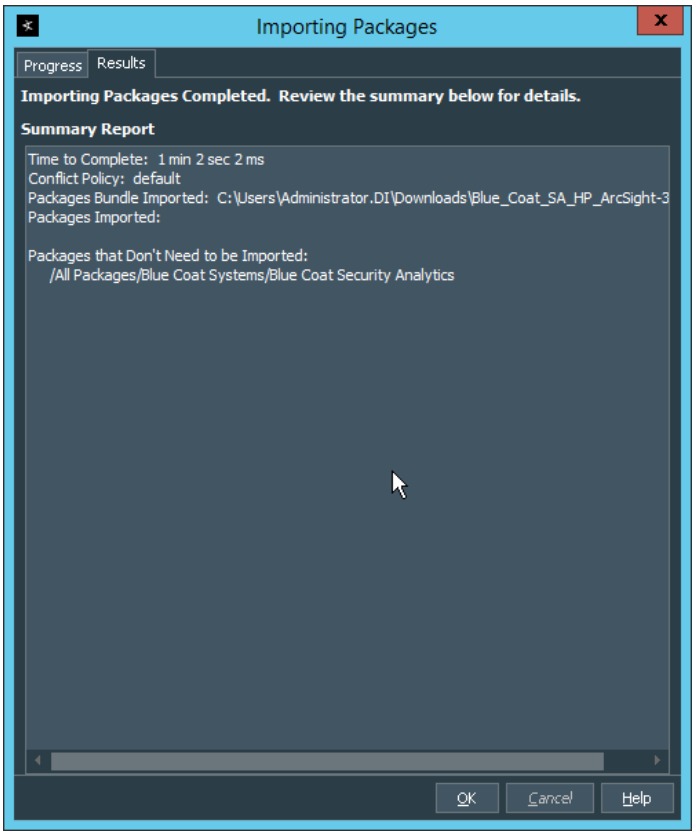
4. In the **Navigator** pane, click the **Packages** tab.



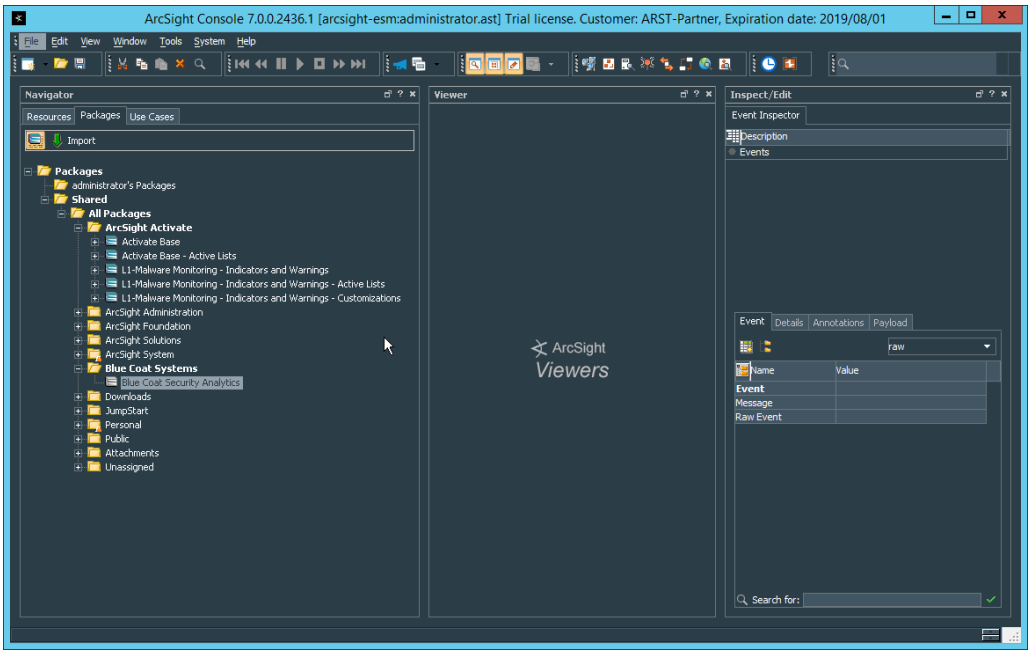
5. Click **Import.**
6. In the window that it opens, find and select the package you downloaded.


Open
Look in:
Downloads
jce_policy-8
L1-Malware_Monitoring_-_Indicators_and_Warnings_1.1.0.1
tlc_7.3.1
Blue_Coat_SA_HP_ArcSight-3.0.arb
Recent Items
Desktop
Documents
This PC
Network
File name:
Blue_Coat_SA_HP_ArcSight-3.0.arb
Files of type:
ArcSight package bundles
Open
Cancel

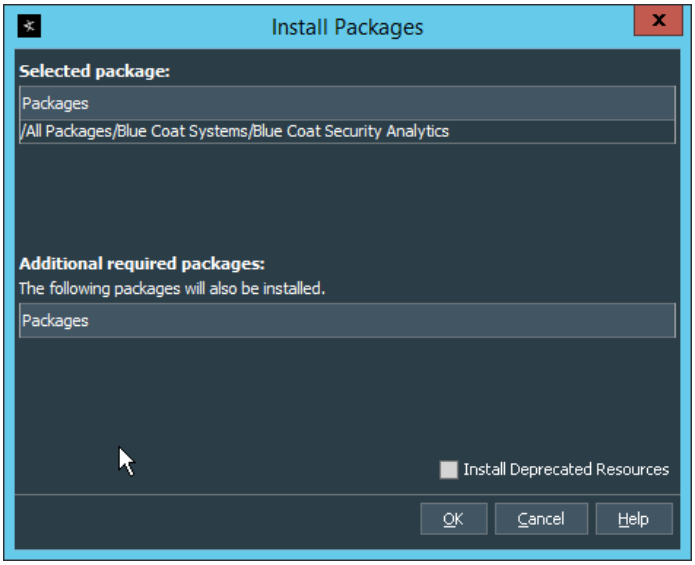
7. Click **Open.**



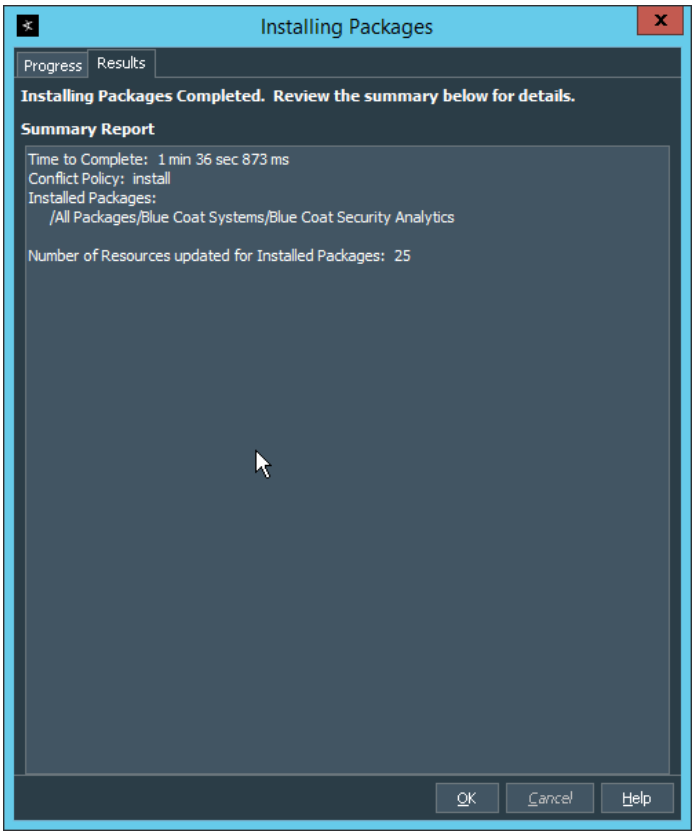
8. Click **OK** when the import finishes.
9. Under the **Packages** tab in the **Navigator** pane, navigate to **Packages > Shared > All Packages > Blue Coat Systems > Blue Coat Security Analytics.**



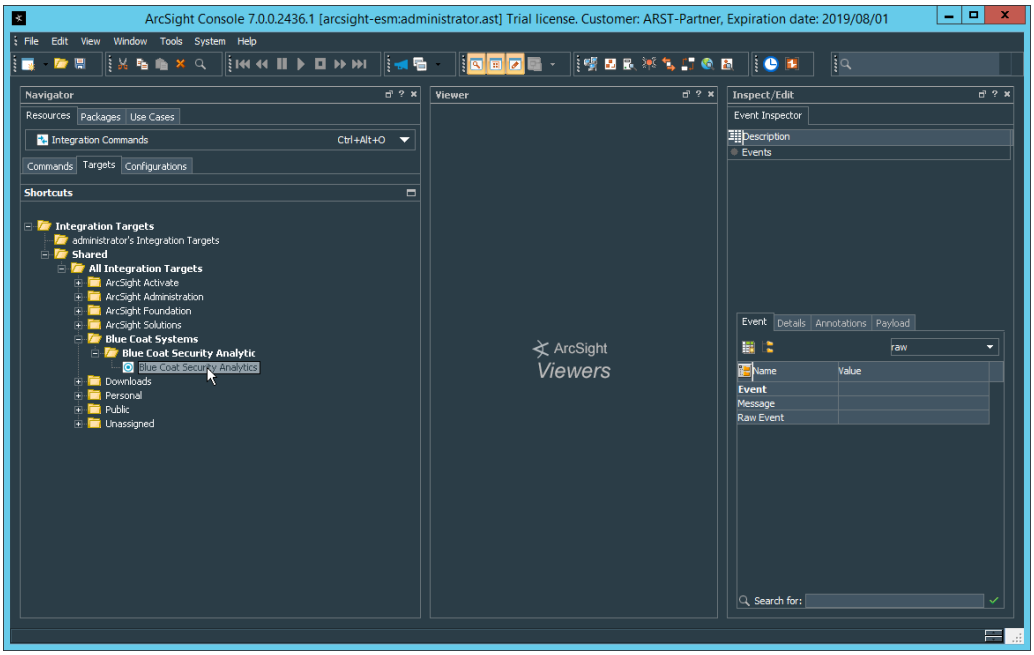
10. Right-click **Blue Coat Security Analytics,** and select **Install Package.**



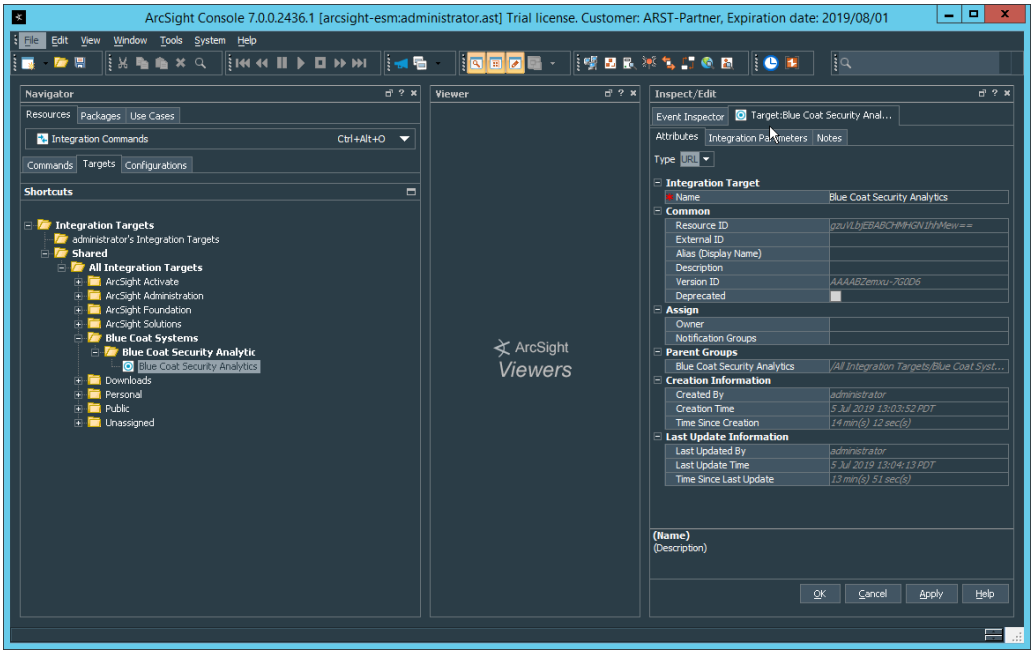
11. Click **OK.**



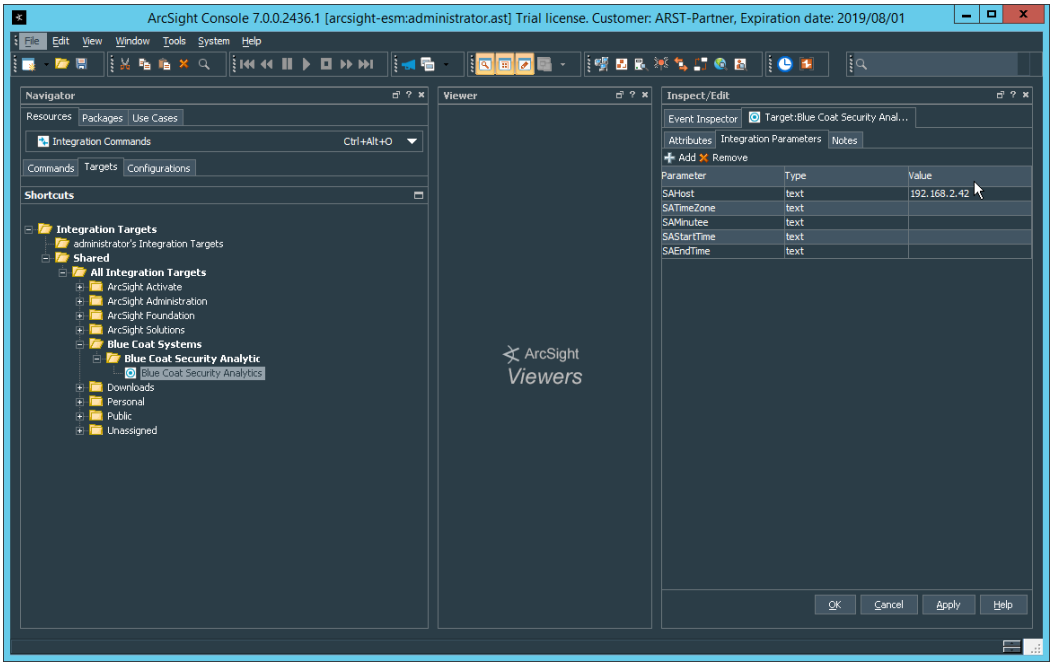
12. Click **OK.**
13. When this completes, you can verify that the installation was successful by the existence of a **Blue Coat Systems** folder when you navigate to **Resources > Integration Commands > Commands > Shared > All Integration Commands.**
14. In the **Resources** tab of the **Navigation** pane, under **Integration Commands,** select the **Targets** tab.
15. Navigate to **Integration Targets > Shared > All Integration Targets > Blue Coat Systems > Blue Coat Security Analytic > Blue Coat Security Analytics.**



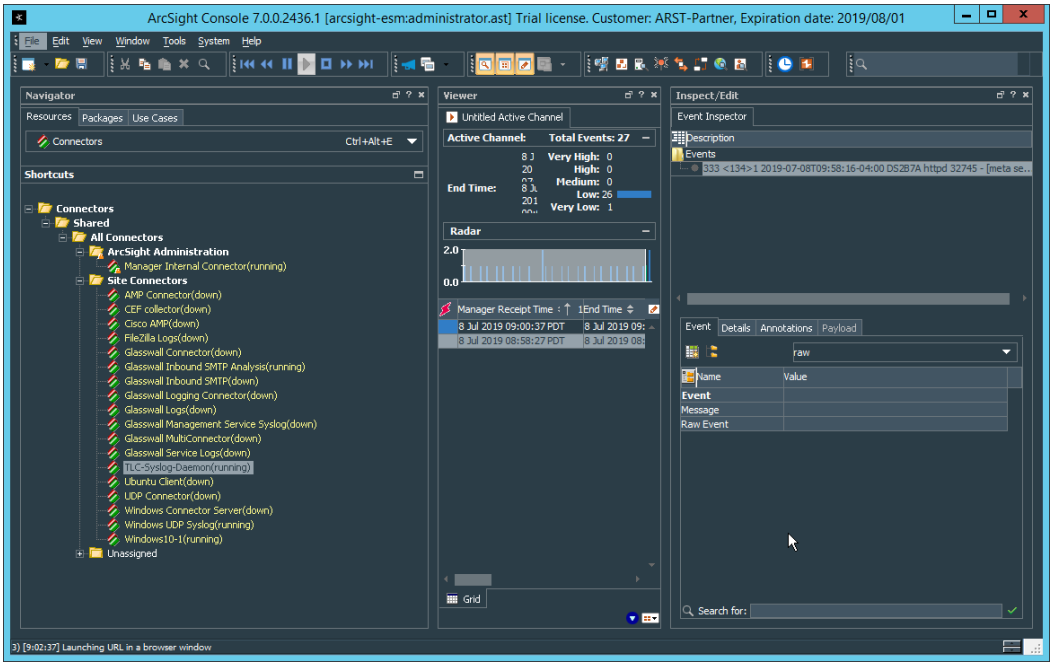
16. Right-click **Blue Coat Security Analytics,** and click **Edit Target.**



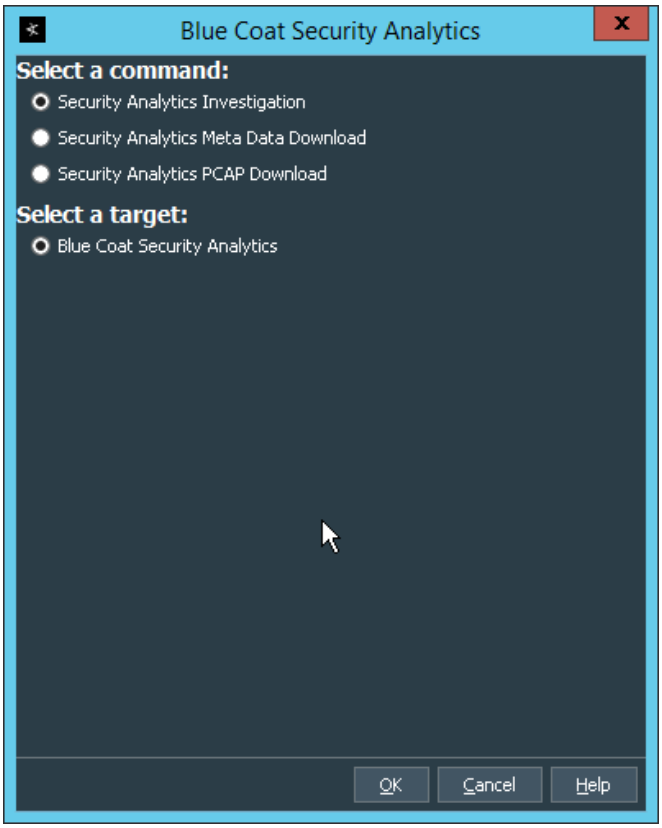
17. Click the **Integration Parameters** tab.
18. Replace the **SAHost** value with the IP address of Symantec Analytics.



19. Click **OK.**
20. To verify the functionality, right-click an event in any channel, and select **Integration Commands > Blue Coat Security Analytics.**



21. Select **Security Analytics Investigation.**



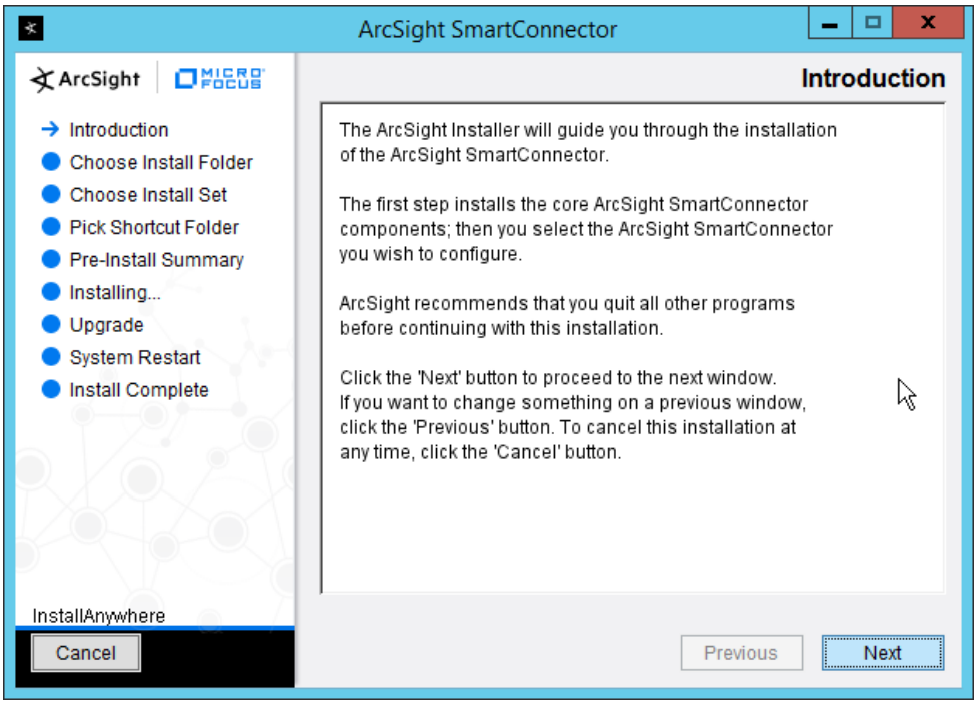
22. Click **OK.** This will open Security Analytics in the browser and perform a packet search based on the event parameters.

2.24 Integration: Micro Focus ArcSight and Glasswall FileTrust

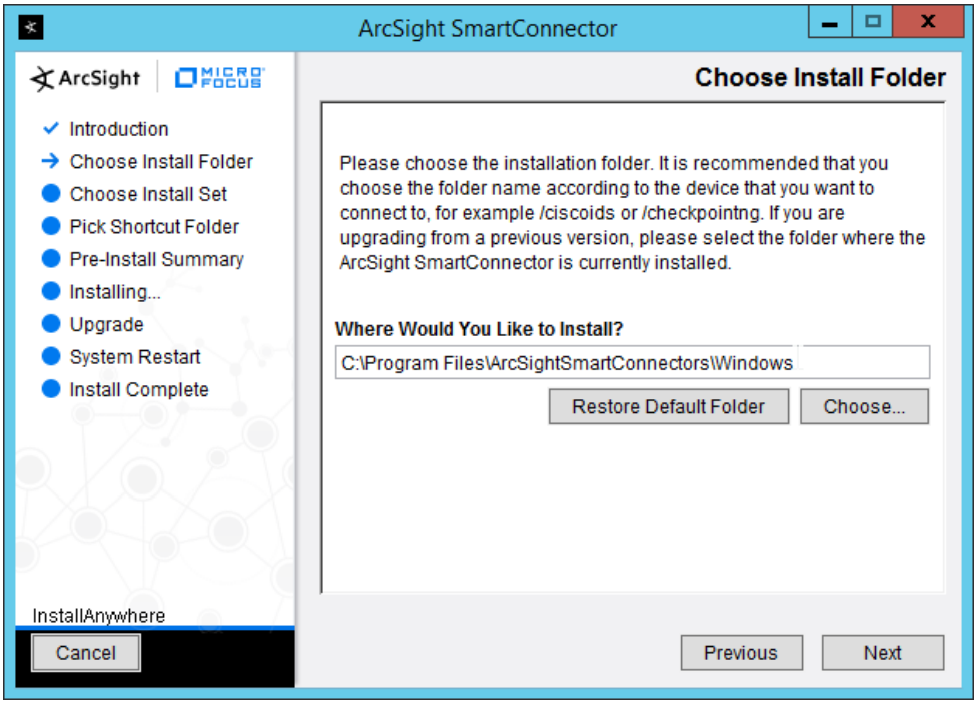
Glasswall FileTrust for Email stores its logs in *C:\Logging*, on the server running the **Glasswall** services.

2.24.1 Install Micro Focus ArcSight

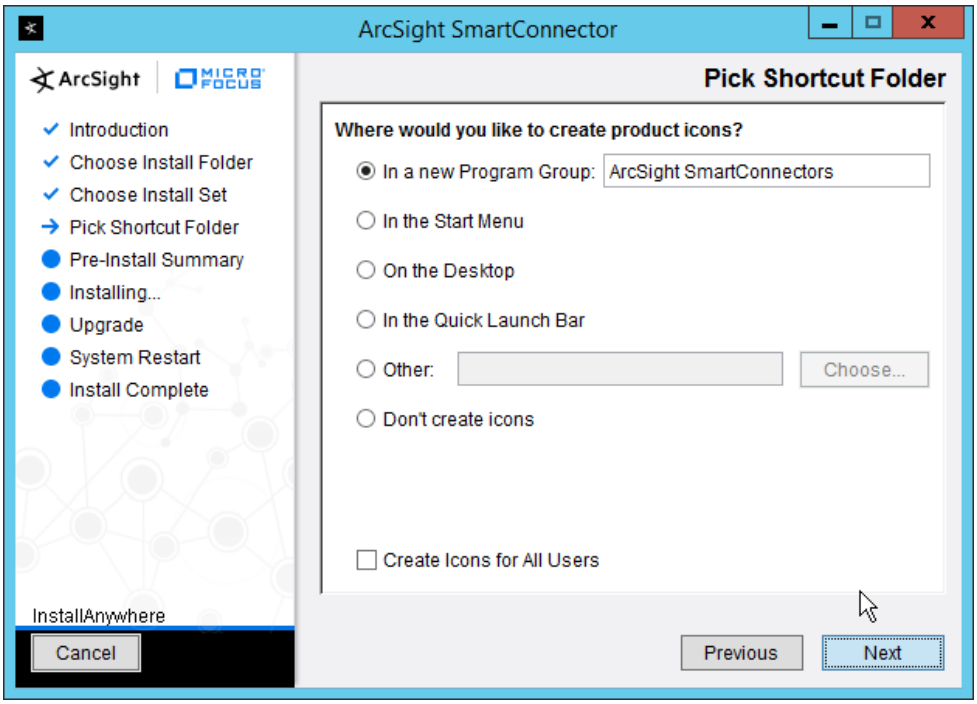
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on the same server as **Glasswall FileTrust.**



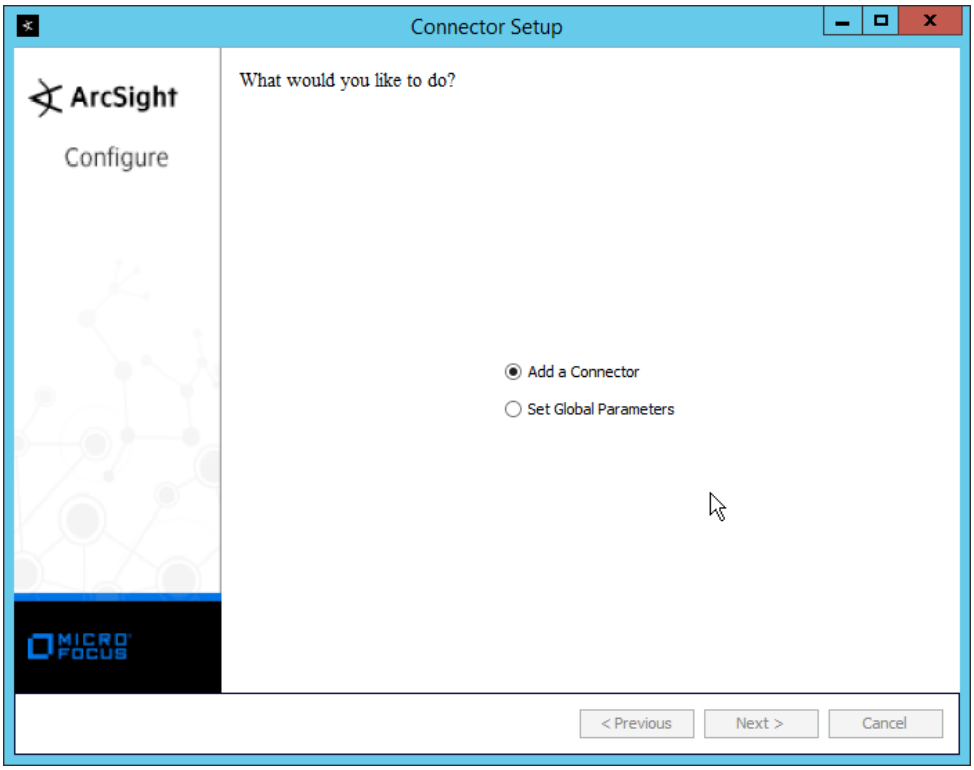
2. Click **Next.**
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows.*



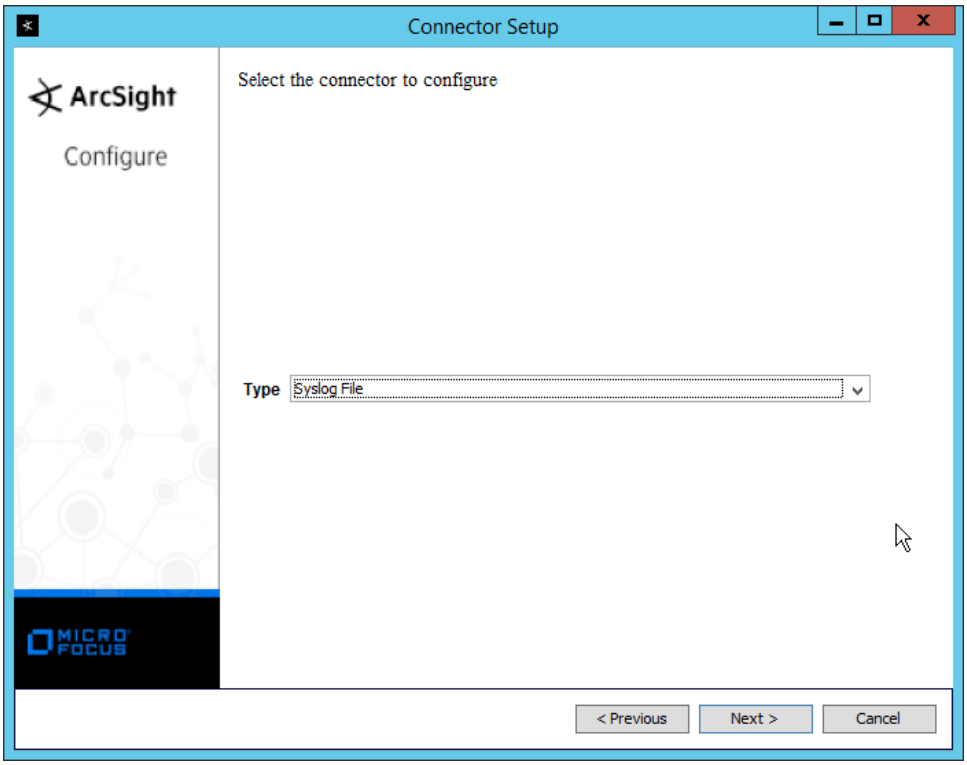
4. Click **Next.**



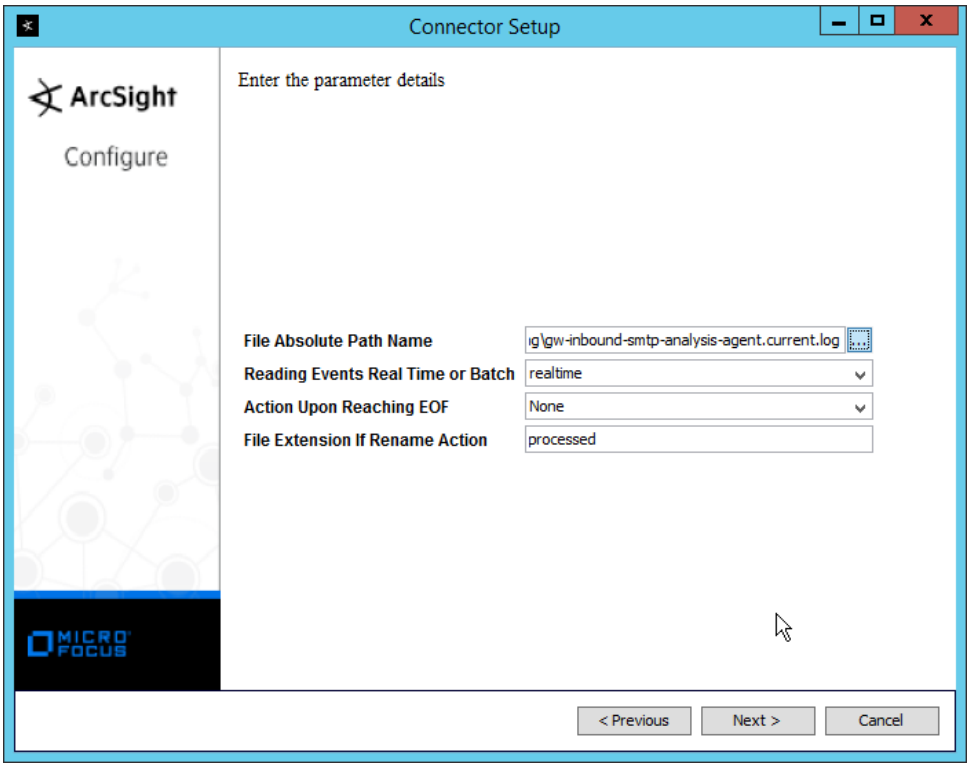
5. Click **Next.**
6. Click **Install.**
7. Select **Add a Connector.**



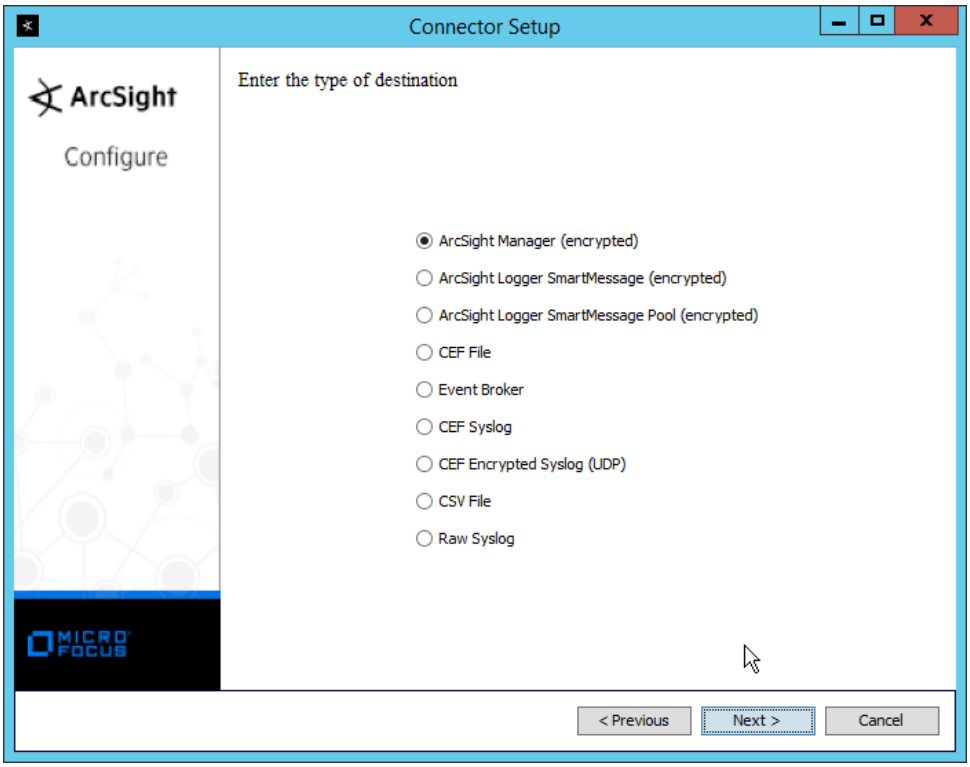
8. Click **Next.**
9. Select **Syslog File.**



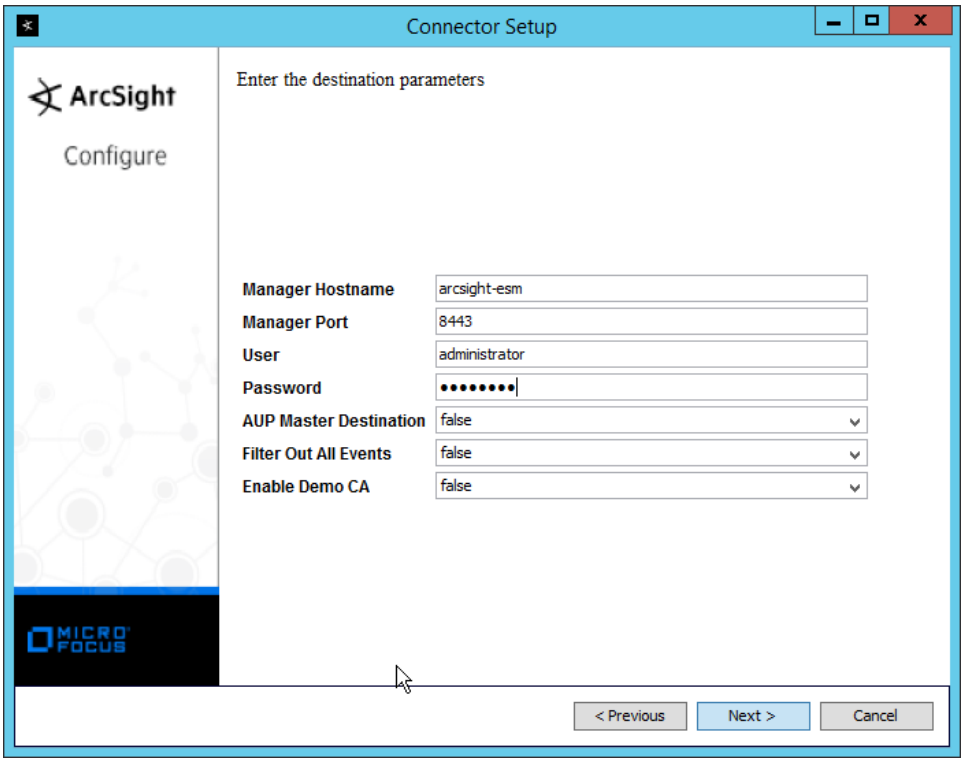
10. Click **Next.**
11. Enter *C:\Logging\gw-inbound-smtp-analysis-agent.current.log* for **File Absolute Path Name.**



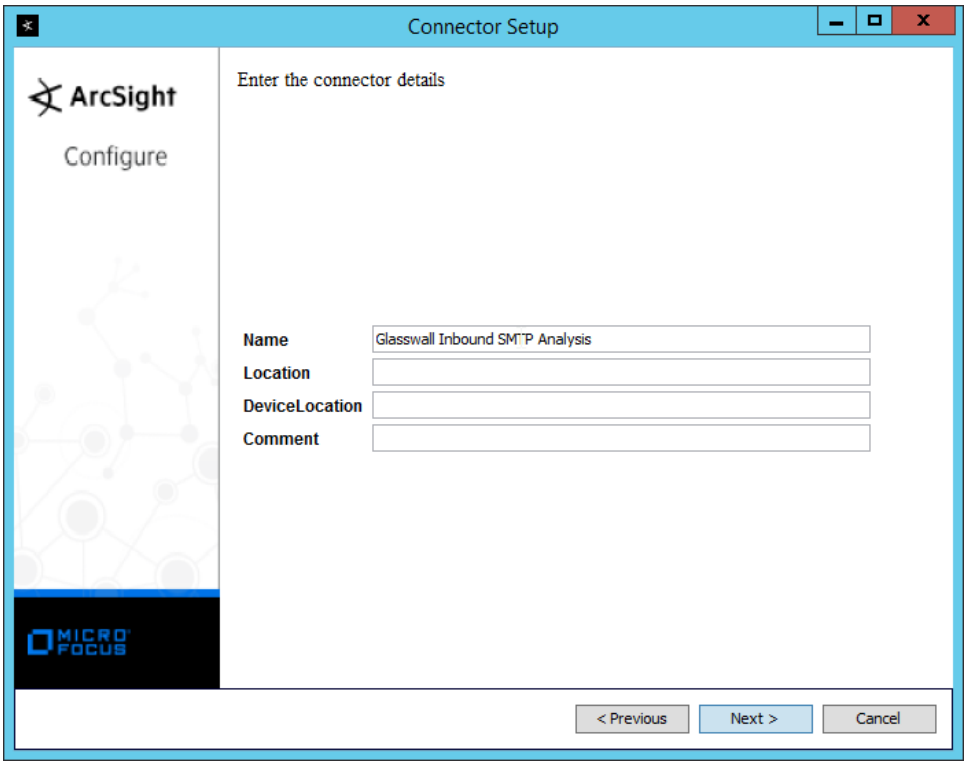
12. Click **Next.**
13. Select **ArcSight Manager (encrypted).**



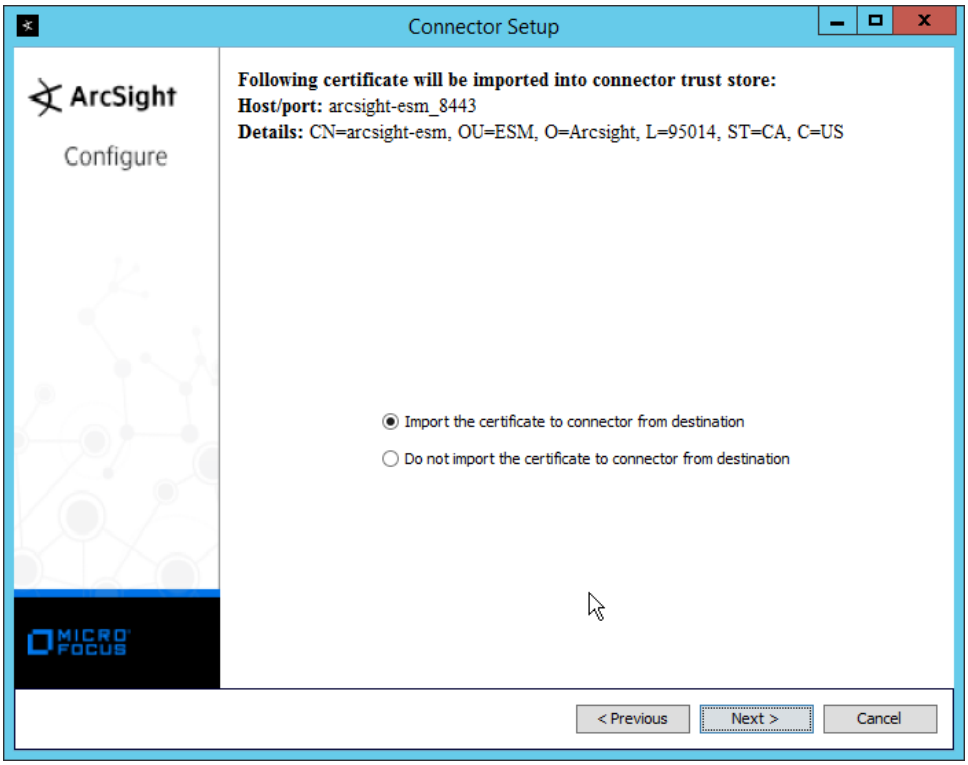
14. Click **Next.**
15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



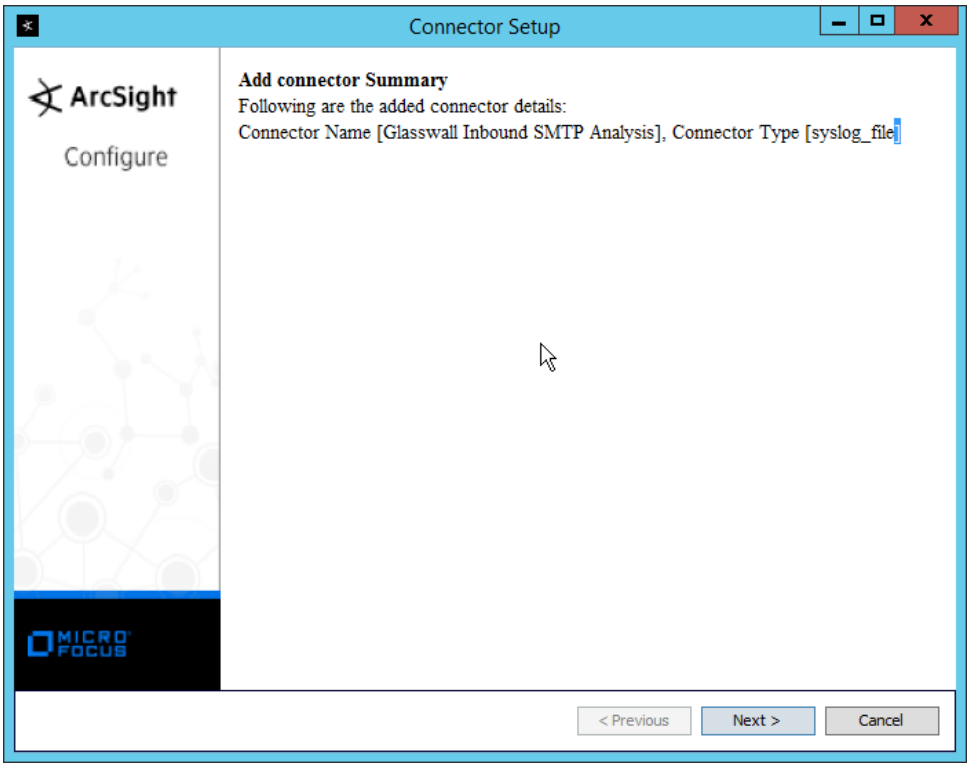
16. Click **Next.**
17. Enter identifying details about the system (only **Name** is required).



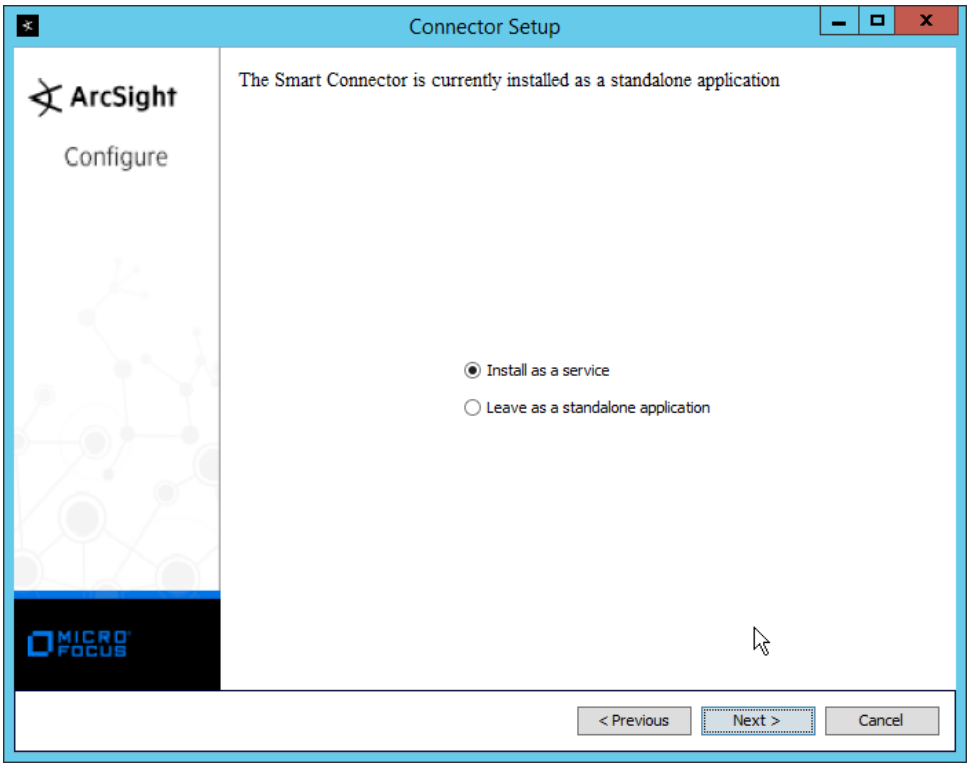
18. Click **Next.**
19. Select **Import the certificate to connector from destination.**



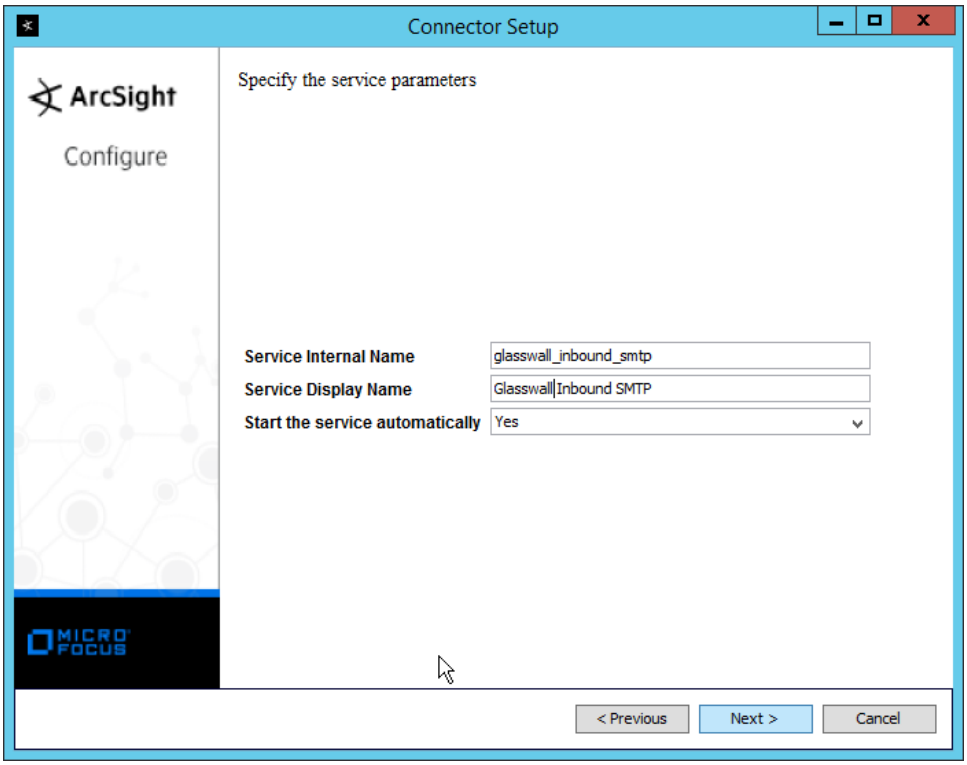
20. Click **Next.**



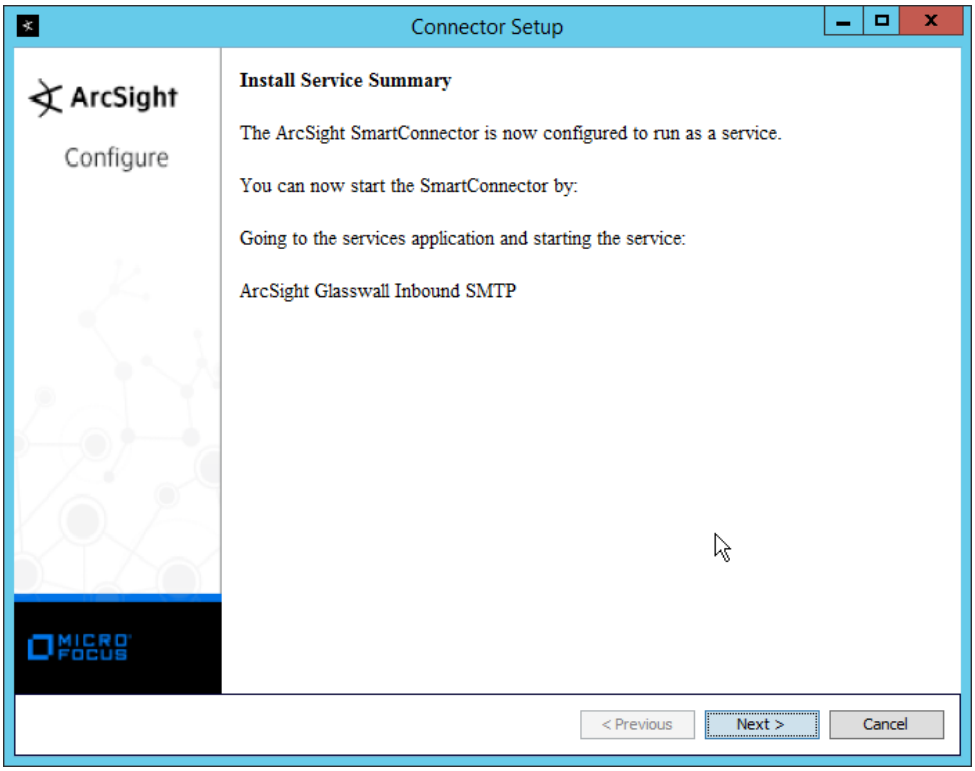
21. Click **Next.**
22. Select **Install as a service.**



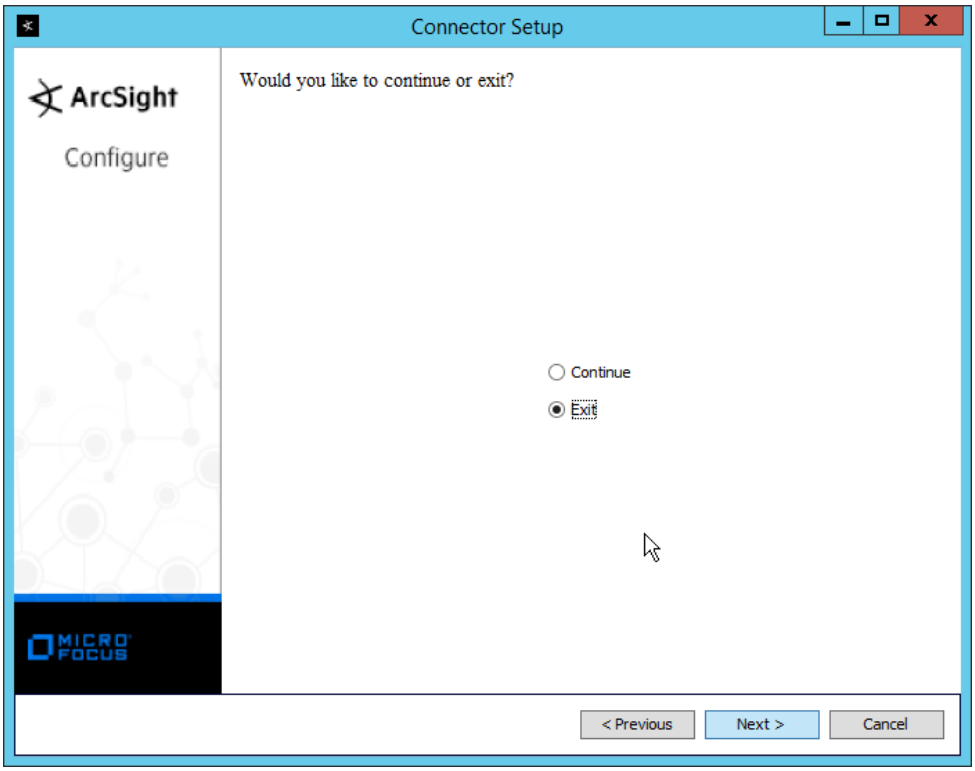
23. Click **Next.**
24. Change the service parameters to more appropriate names, because multiple connectors need to be installed on this server.



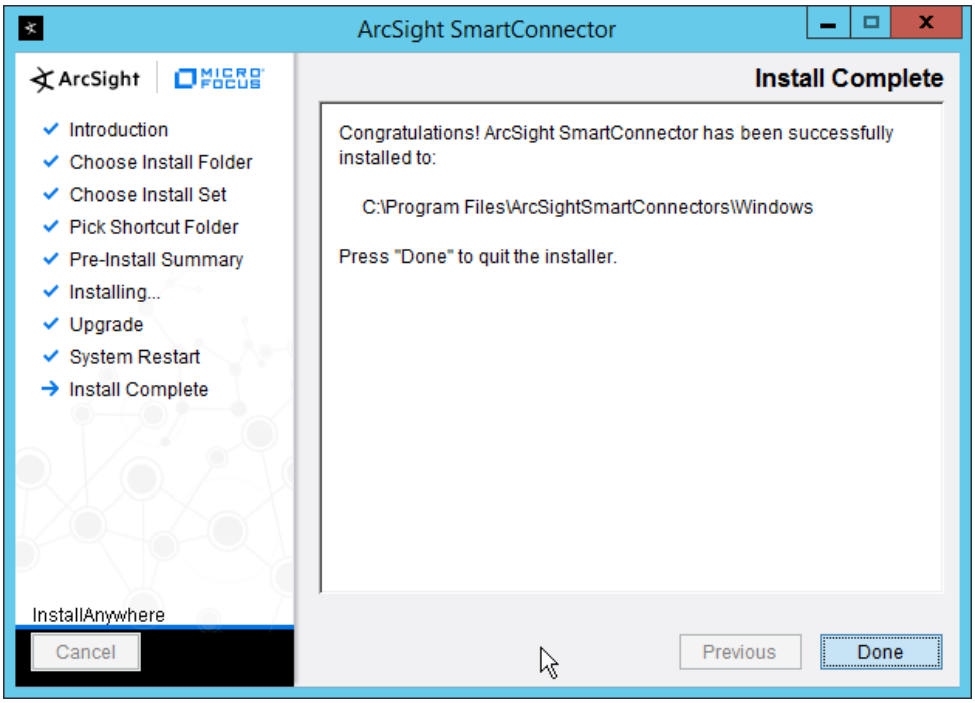
25. Click **Next.**



26. Click **Next.**
27. Select **Exit.**



28. Click **Next.**



29. Click **Done.**

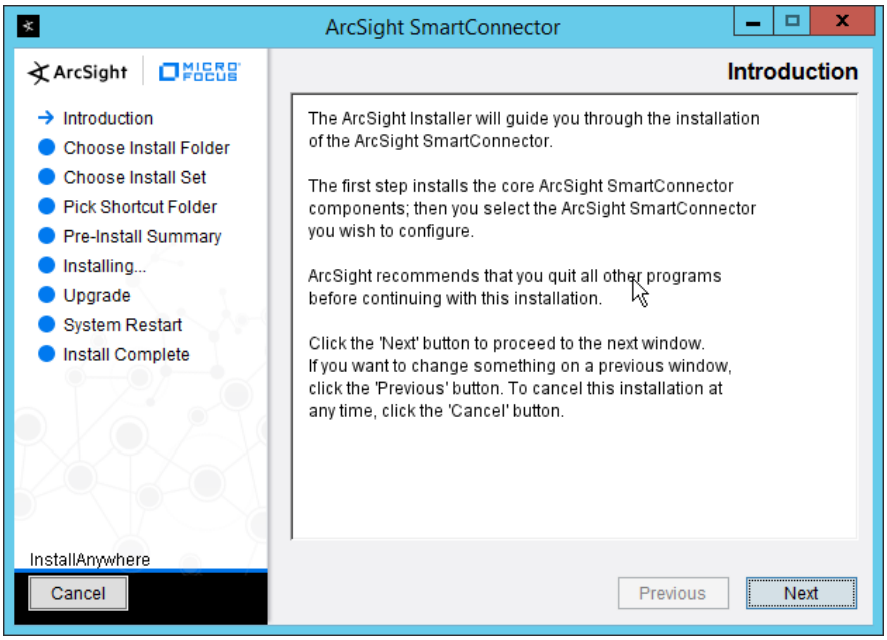
30. Repeat steps 1-29 for the other three "current" log files in *C:\Logging,* with the following caveats:
    a. Replace *C:\Program Files\ArcSightSmartConnectors\Windows* with a different folder name for each connector.
    b. Replace *C:\Logging\gw-inbound-smtp-analysis-agent.current.log* with the appropriate log file.
        i. C:\Logging\gw-management-service.current.log
        ii. C:\Logging\gw-file-analysis-process-InboundSMTPAgent-0.current.log
        iii. C:\Logging\gw-administration-console.current.log
    c. Replace the **Name** of the connector in its identifying details.
    d. Replace the **service parameters** with different names so that the services do not conflict.

2.25 Integration: Micro Focus ArcSight and Cisco Stealthwatch

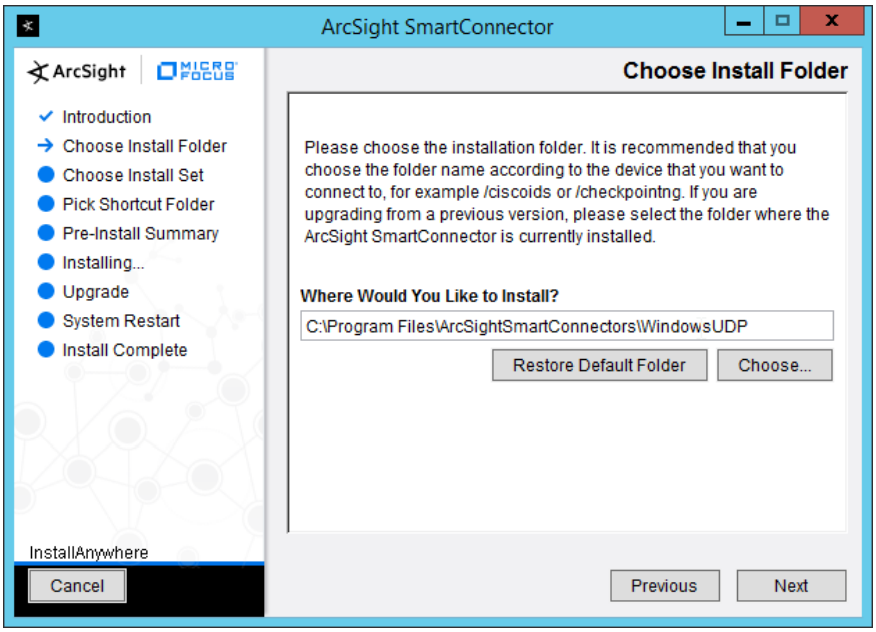
This section will detail the forwarding of logs from **Cisco Stealthwatch** to **Micro Focus ArcSight.**

2.25.1 Install Micro Focus ArcSight

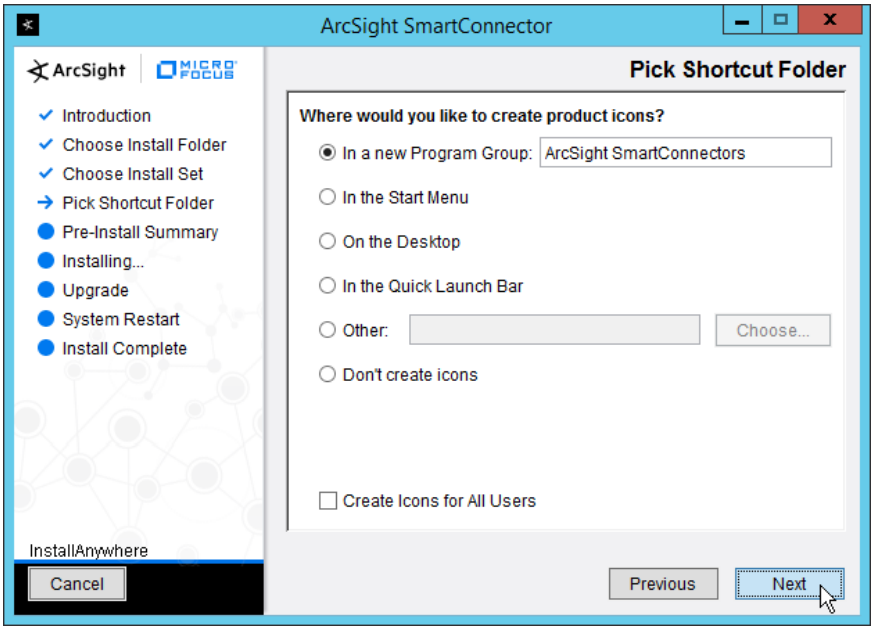
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Cisco Stealthwatch.**



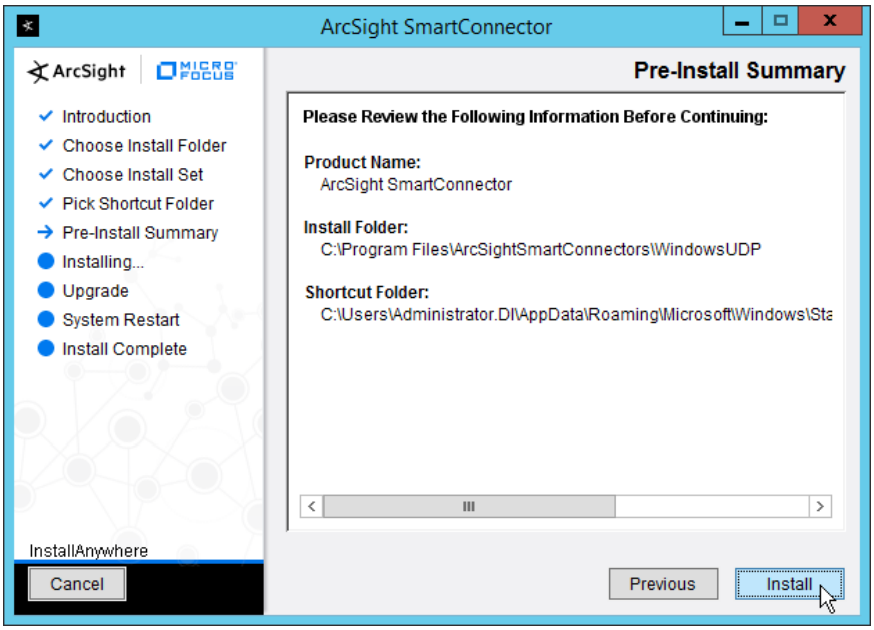
2. Click **Next.**
3. Enter C*:\Program Files\ArcSightSmartConnectors\WindowsUDP.*



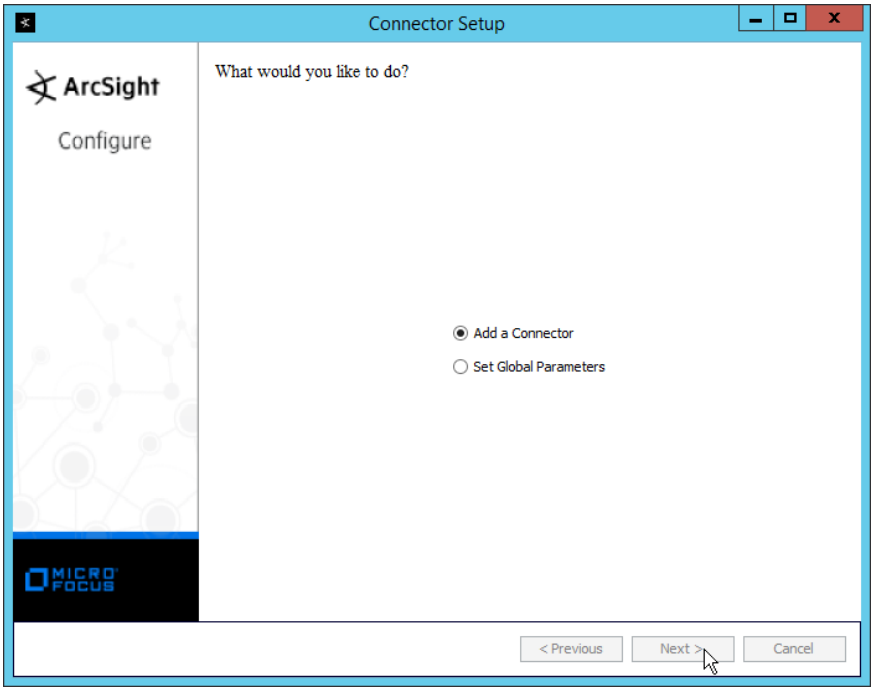
4. Click **Next.**



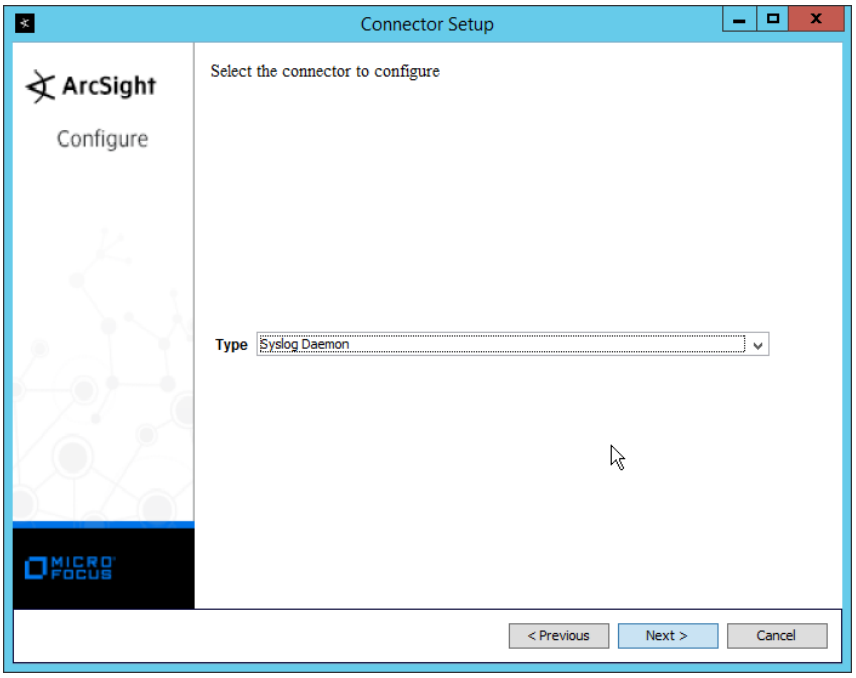
5. Click **Next.**



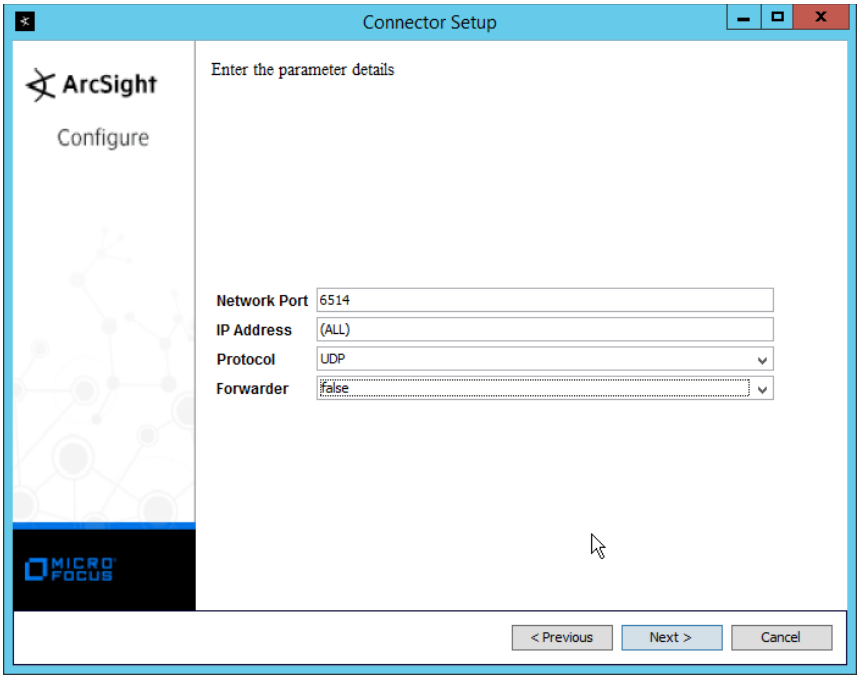
6. Click **Install.**
7. Select **Add a Connector.**



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

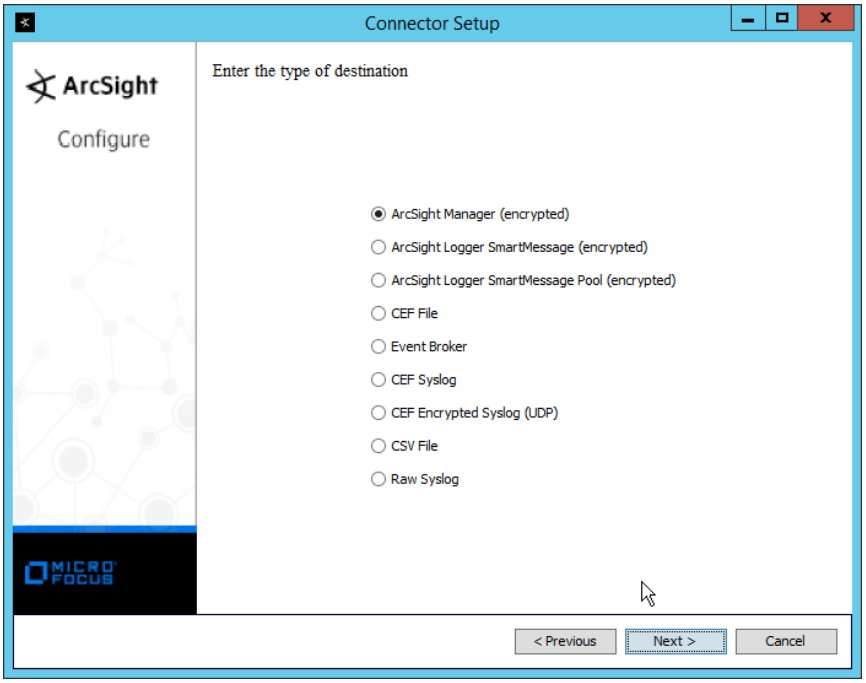


10. Click **Next.**
11. Enter an unused port for the daemon to run on. (Ensure that this port is allowed through the firewall.)
12. Select **UDP** for **Protocol.**



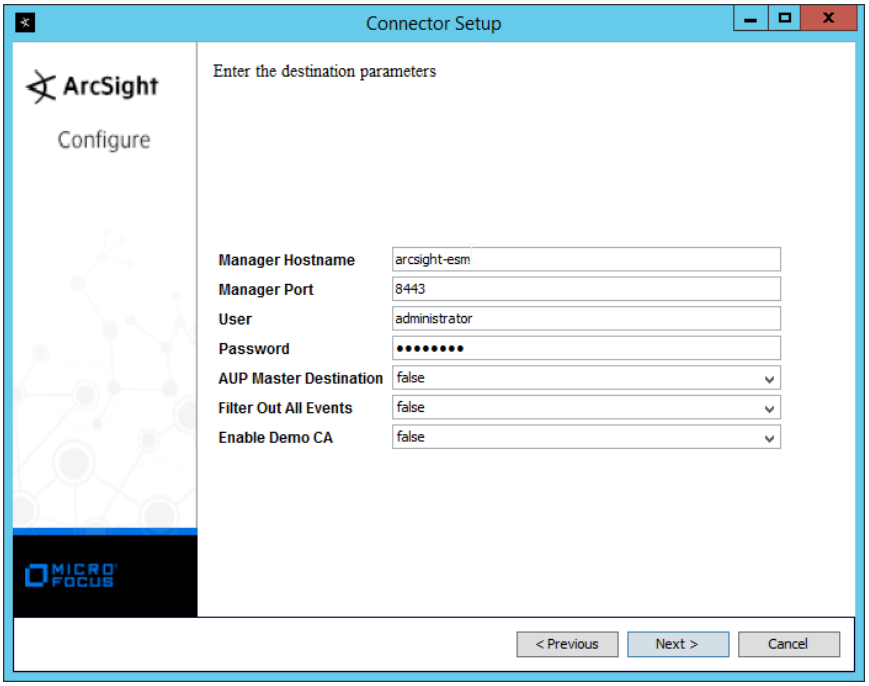
13. Click **Next.**

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



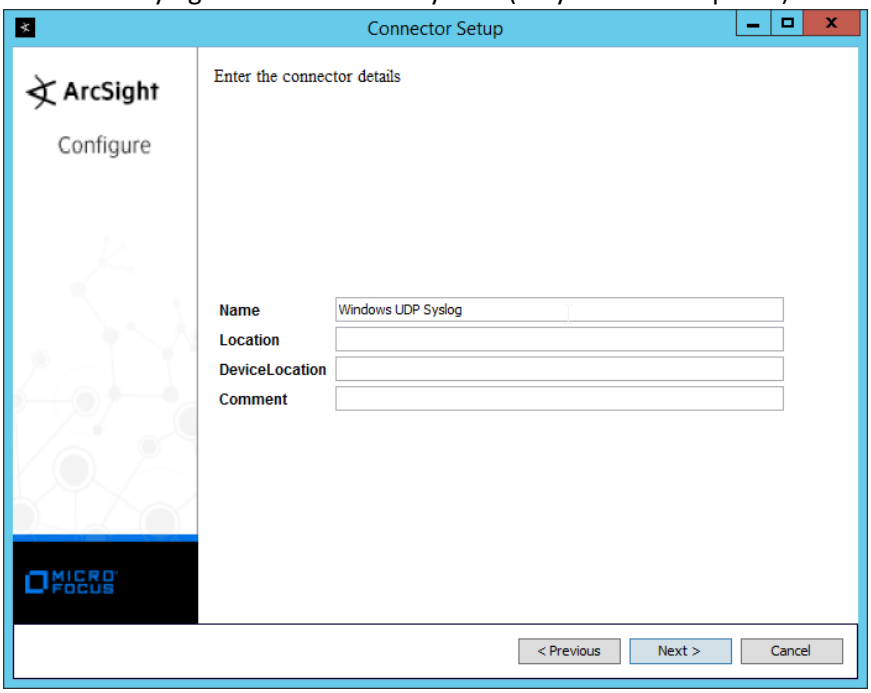
15. Click **Next.**

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



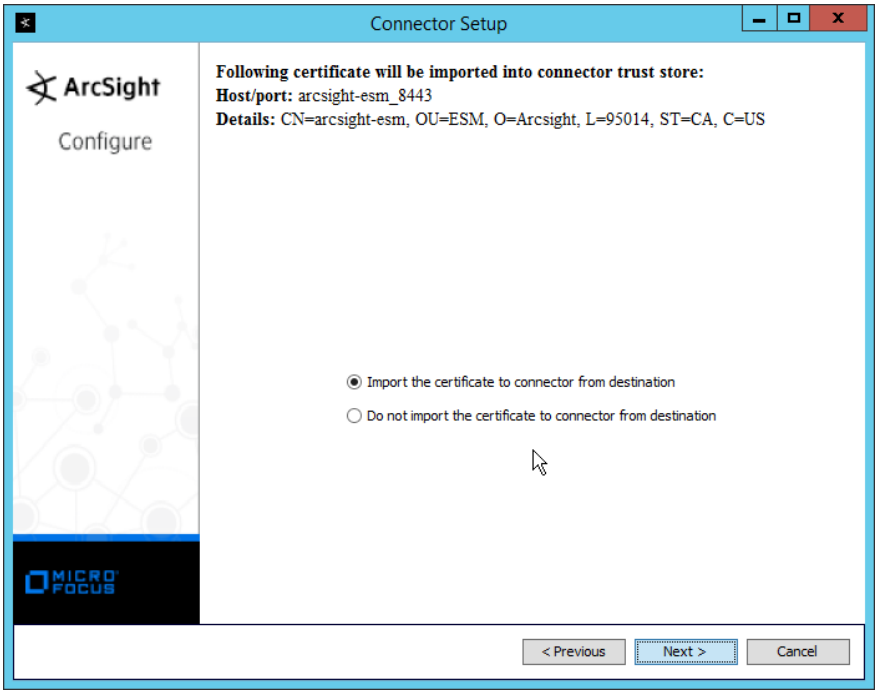
17. Click **Next.**

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

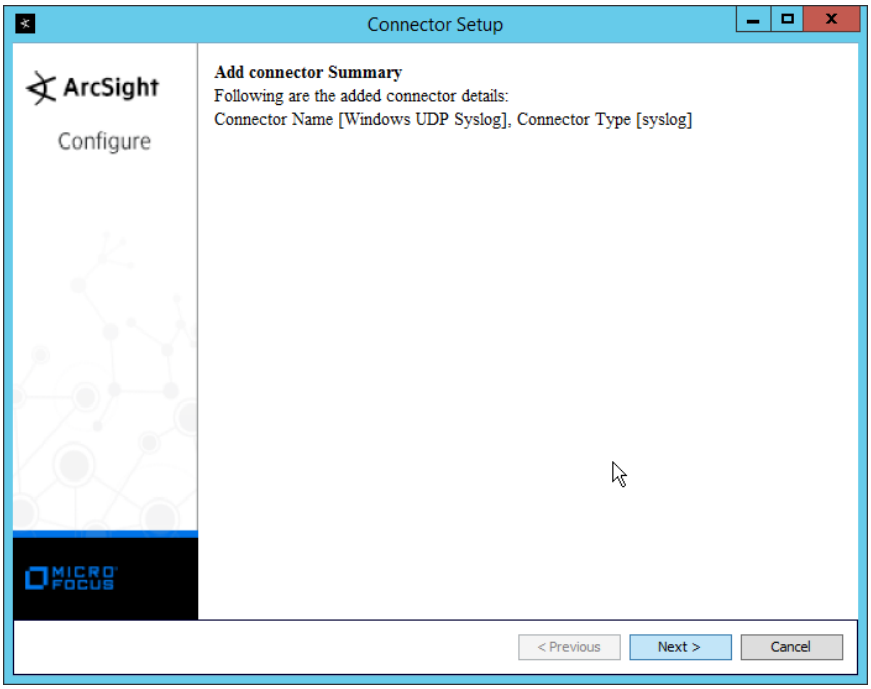


19. Click **Next.**

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

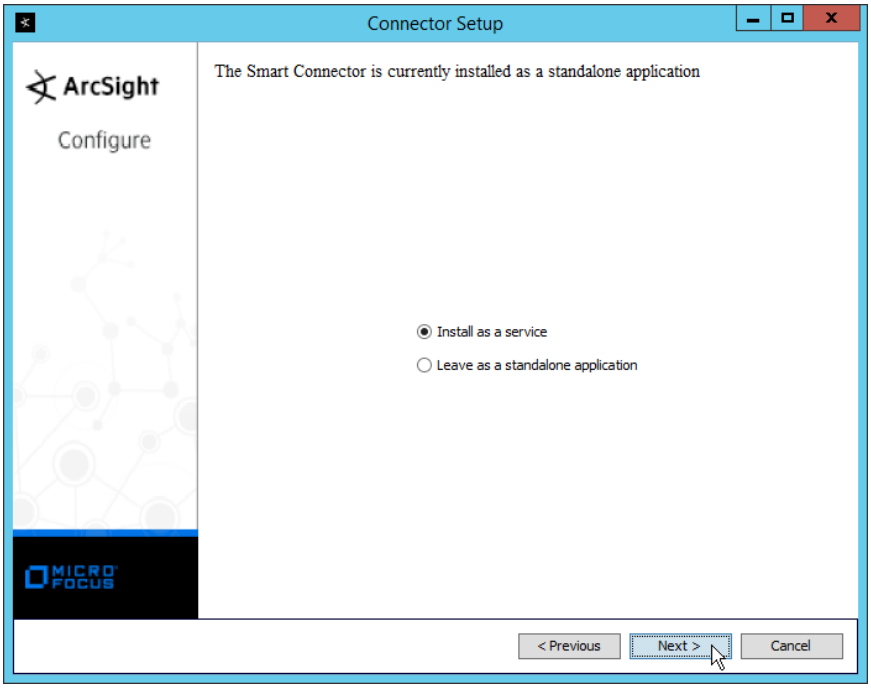


21. Click **Next.**



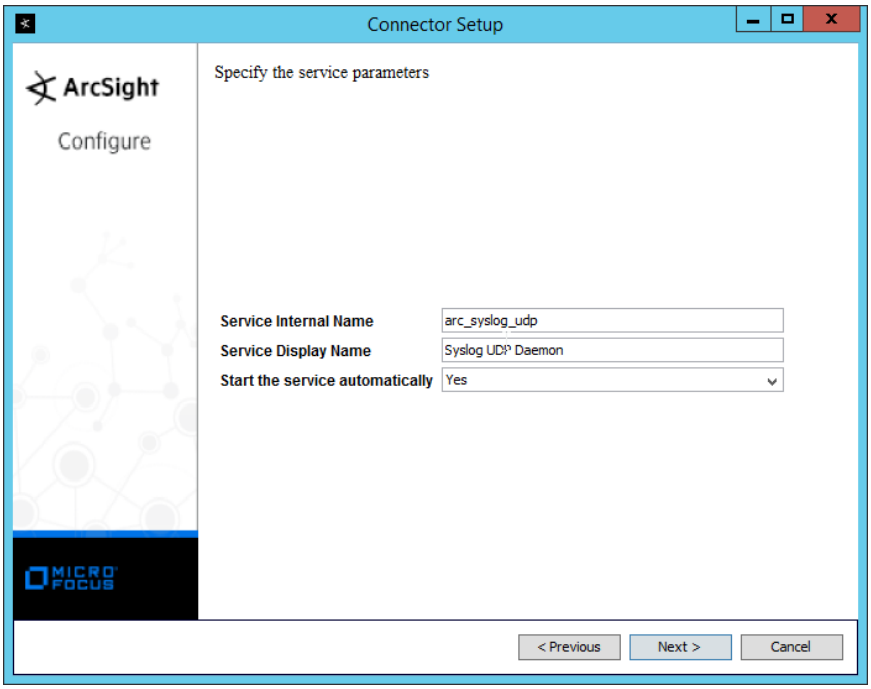
3135 22. Click **Next.**

3136 23. Select **Install as a service.**

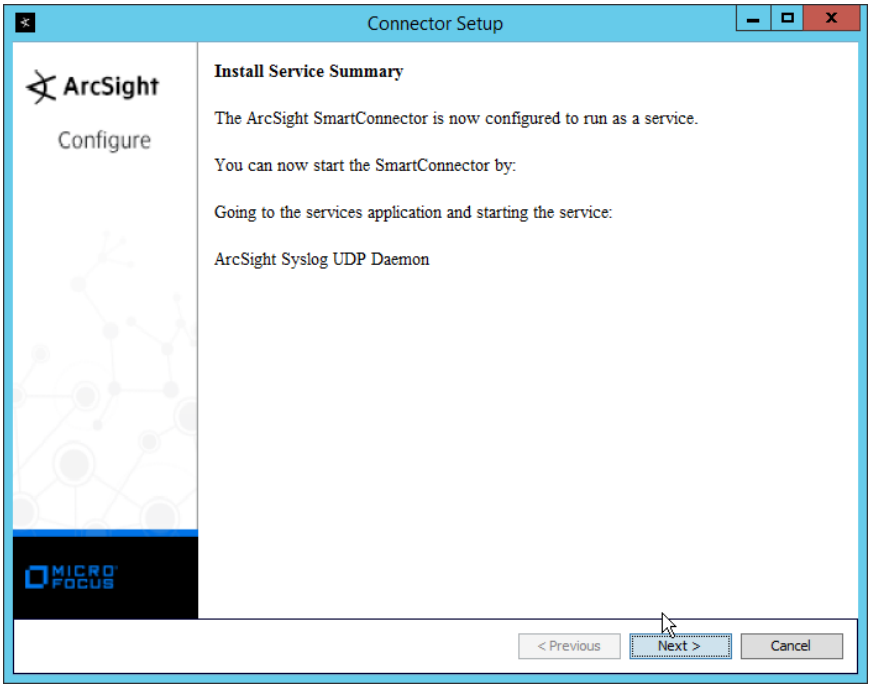


3137 24. Click **Next.**

3138 25. Enter a service name and display name.

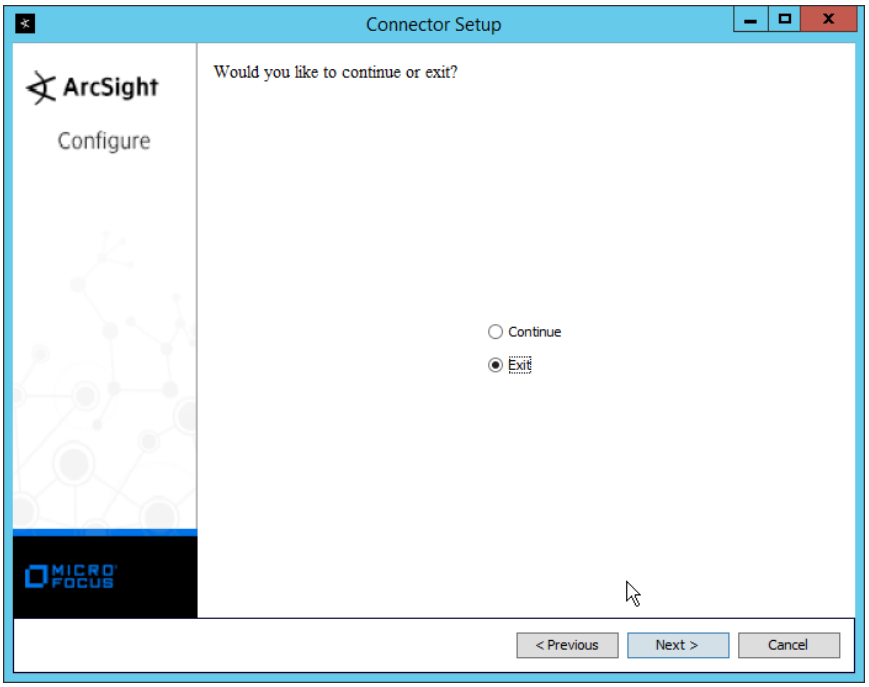


3139 26. Click **Next.**

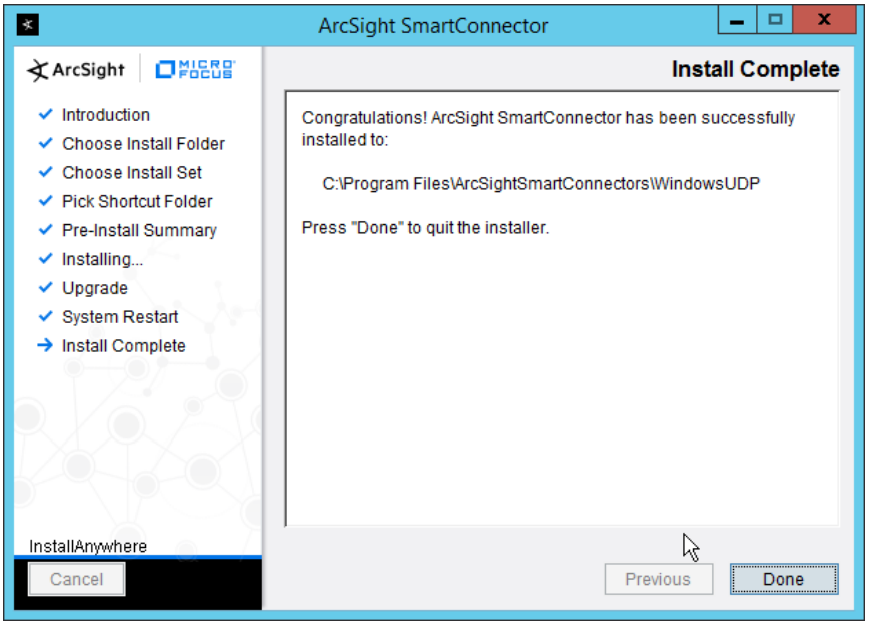


3140 27. Click **Next.**

3141 28. Select **Exit.**



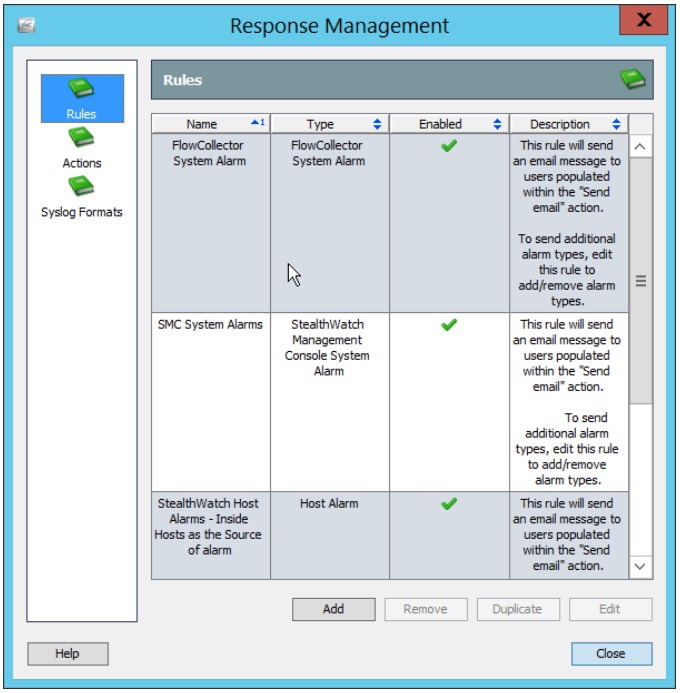
3142 29. Click **Next.**



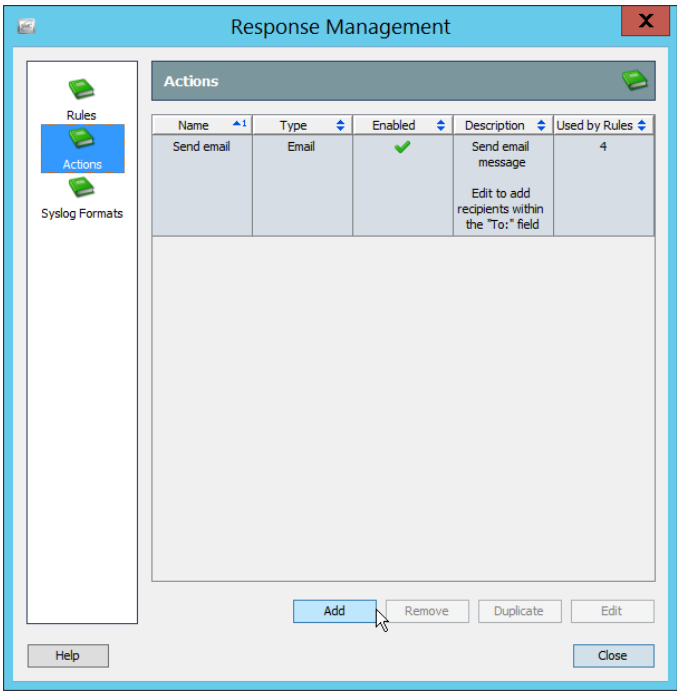
3143 30. Click **Done.**

2.25.2 Configure Cisco Stealthwatch

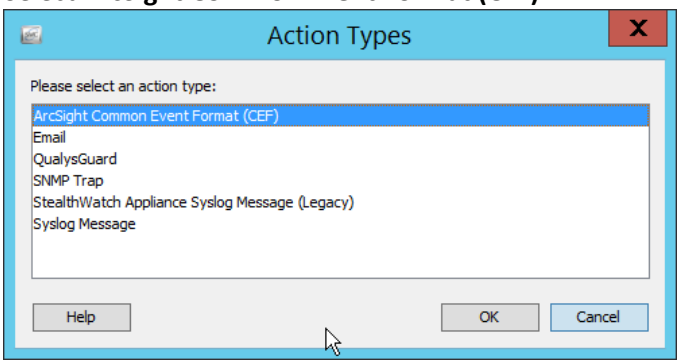
1. Log in to the **Cisco Stealthwatch Management Console** desktop interface. (This can be downloaded from the web interface and run using **javaws.exe.** You may need to add the site to your Java exceptions in **Control Panel > Java.**)
2. Click **Configuration > Response Management.**



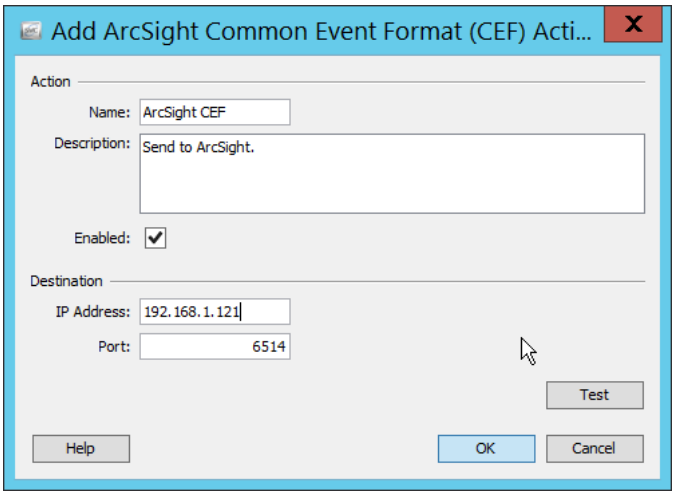
3. Click **Actions.**



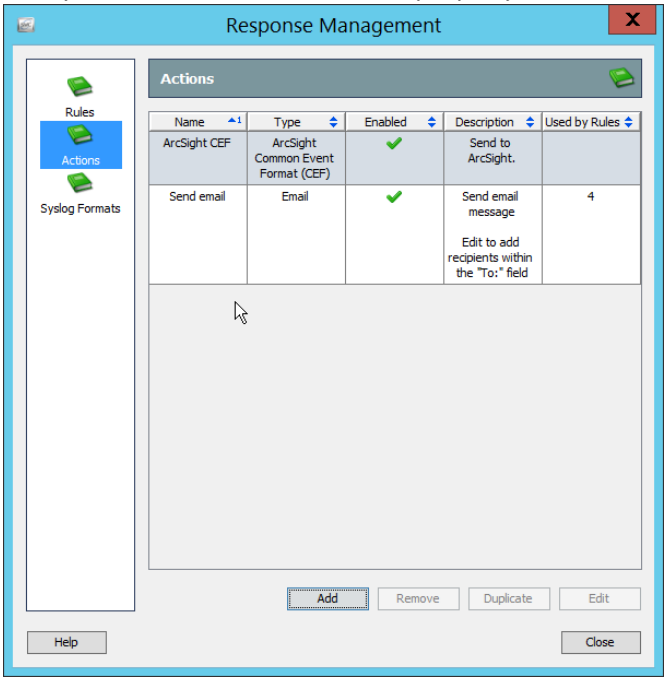
4. Click **Add.**
5. Select **ArcSight Common Event Format (CEF).**



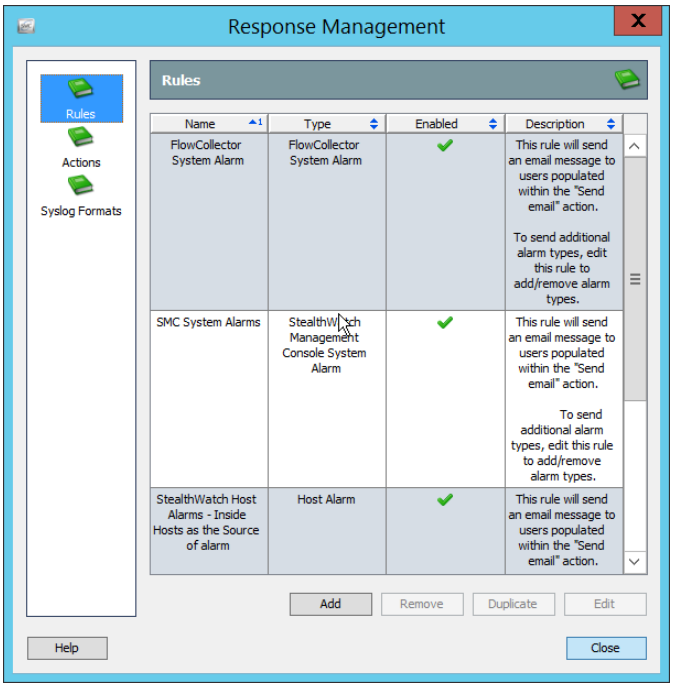
6. Click **OK.**
7. Enter a **name** for the **Action.**
8. Enter a **description.**
9. Enter the **IP address** of the server with the UDP ArcSight Connector that you just created.
10. Enter the **port** used in the UDP ArcSight Connector that you just created.
11. (Optional) Click **Test** to send a test message to ArcSight, and verify that ArcSight receives the message.



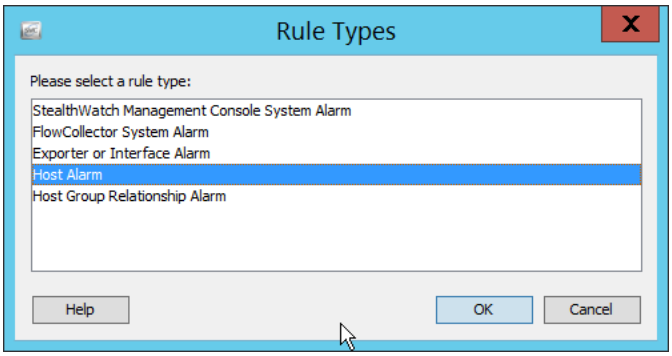
12. Click **OK.**
13. Verify that the action was created properly.



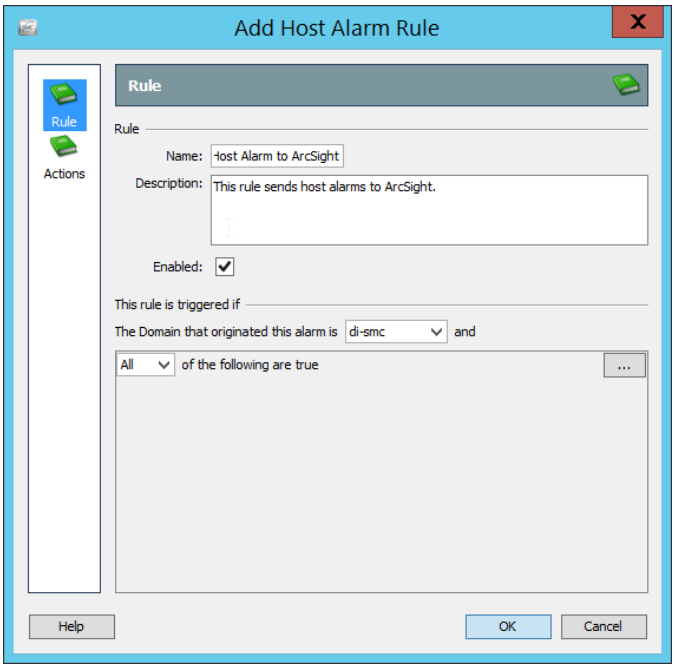
14. Click **Rules.**



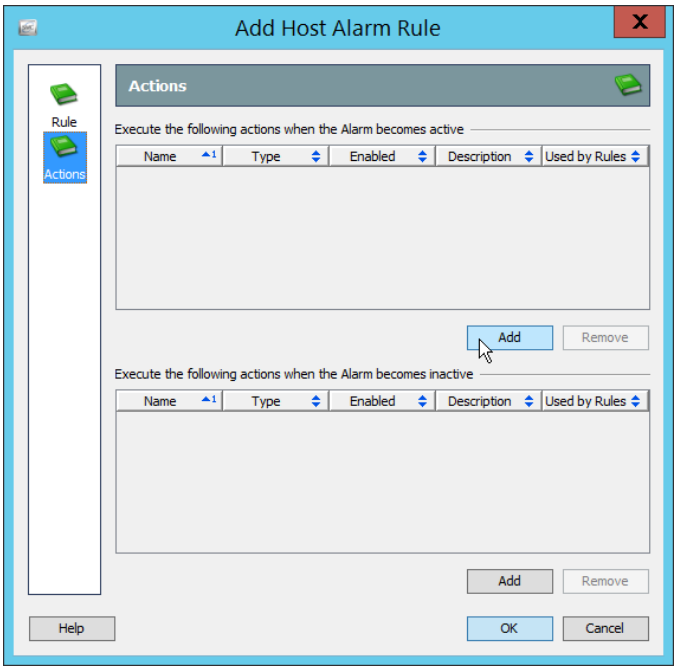
15. Click **Add.**
16. Select **Host Alarm.**



17. Click **OK.**
18. Enter a **name.**
19. Enter a **description.**

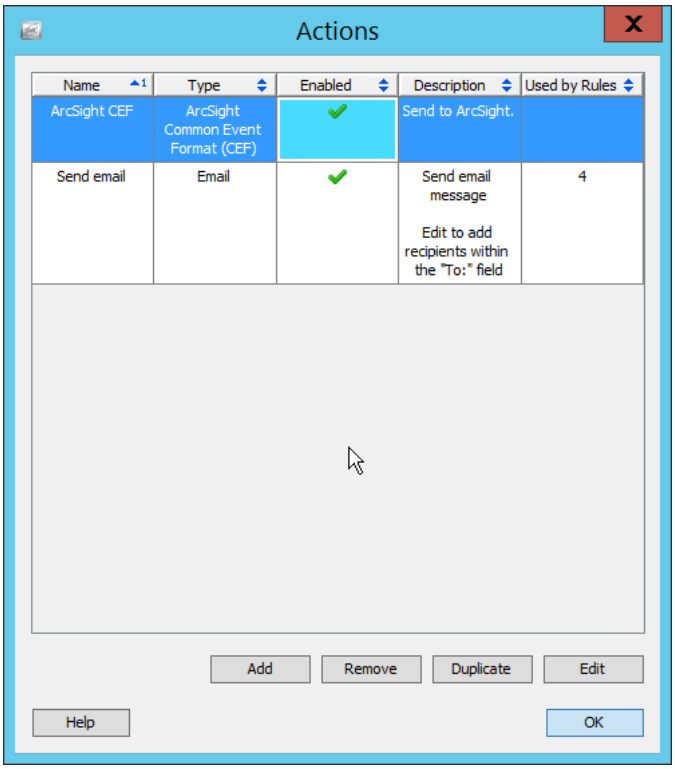


3167 20. Click **Actions.**

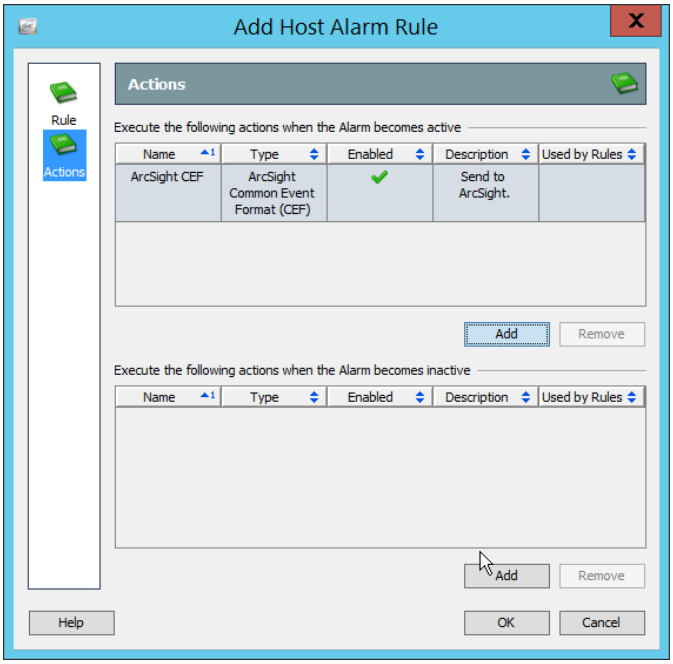


3168 21. Click the **Add** button for the top section; this adds an action when the alarm becomes active.

3169 22. Select the ArcSight CEF rule you just created.

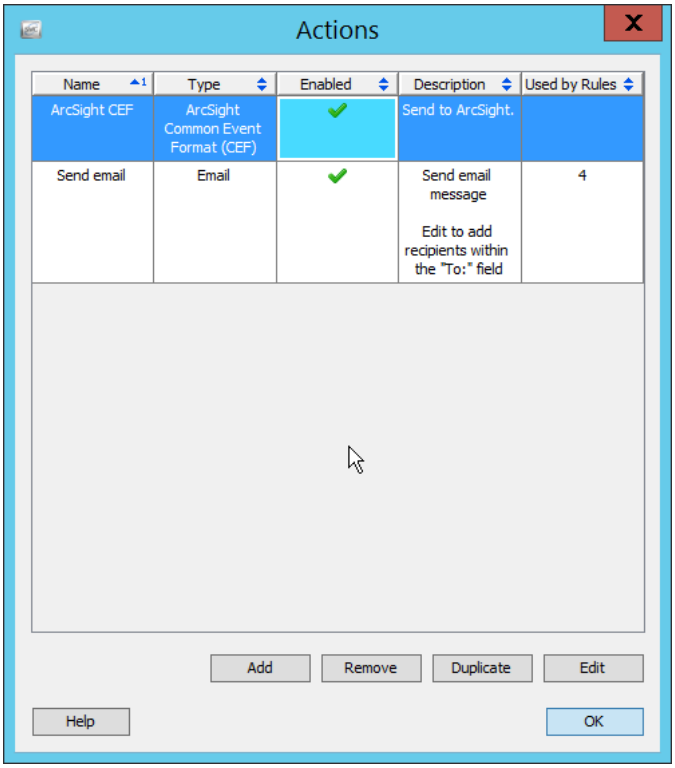


3170 23. Click **OK.**

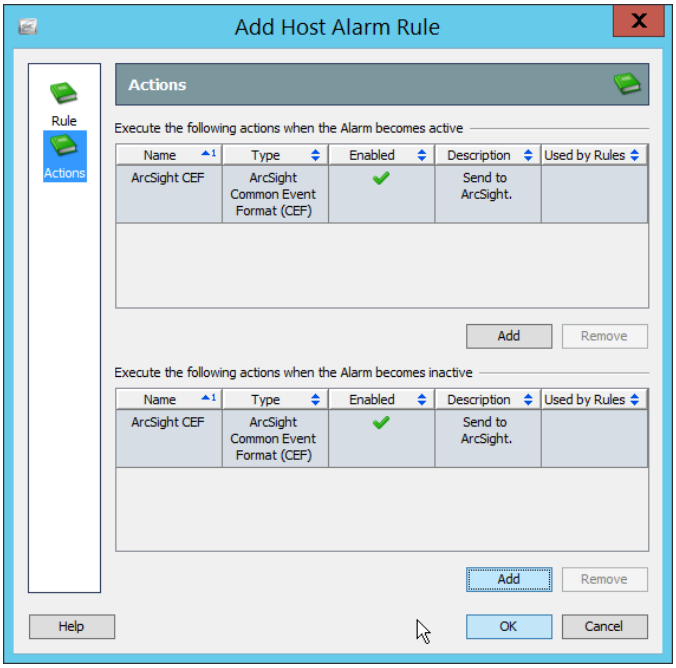


3171 24. Click the **Add** button for the bottom section; this adds an action when the alarm becomes
3172 inactive.

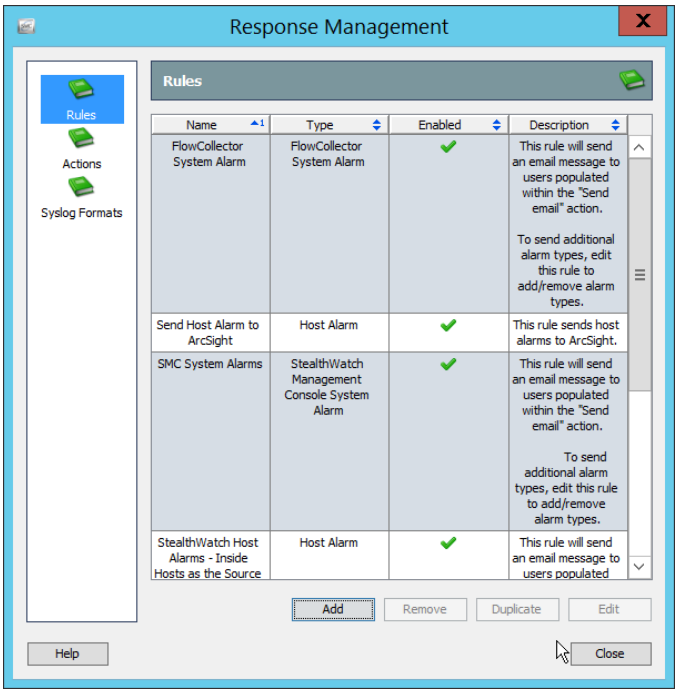
3173 25. Select the ArcSight CEF rule you just created.



3174 26. Click **OK.**



27. Click **OK.**



28. Click **Close.**

Appendix A List of Acronyms

AD	Active Directory
AMP	Advanced Malware Protection
CEF	Common Event Format
DNS	Domain Name System
DSP	Directory Services Protector
ESM	Enterprise Security Manager
ICA	Information Centric Analytics
IIS	Internet Information Services
ISE	Identity Services Engine
IT	Information Technology
JCE	Java Cryptography Extension
JRE	Java Runtime Environment
MSSQL	Microsoft SQL
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
PEM	Privacy Enhanced Mail
SAN	Subject Alternative Name
SMC	Stealthwatch Management Console