

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

December 2020

FINAL

This publication is available free of charge from
<https://doi.org/10.6028/NIST.SP.1800-26>.

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, 442 pages, (December 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Ransomware, destructive malware, insider threats, and even honest 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

Name	Organization
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	1
1.1	Practice Guide Structure	1
1.2	Build Overview	2
1.3	Typographical Conventions.....	3
2	Product Installation Guides	3
2.1	Active Directory and Domain Name System Server.....	3
2.1.1	Install Features.....	3
2.1.2	Create a Certificate Authority.....	17
2.1.3	Configure Account to Add Computers to Domain.....	30
2.1.4	Add Machines to the Domain	36
2.1.5	Configure Active Directory to Audit Account Activity	41
2.1.6	Configure Reverse Lookup Zones	43
2.2	Microsoft Exchange Server.....	48
2.2.1	Install Microsoft Exchange.....	49
2.3	Windows Server Hyper-V Role	59
2.3.1	Production Installation	59
2.4	MS SQL Server	65
2.4.1	Install and Configure MS SQL.....	65
2.4.2	Open Port on Firewall.....	73
2.4.3	Add a New Login to the Database	78
2.5	Microsoft IIS Server	80
2.5.1	Install IIS.....	80
2.5.2	IIS Configuration	87
2.6	Semperis Directory Services Protector	91
2.6.1	Configure Active Directory for Semperis DSP	91
2.6.2	Install Semperis DSP	103
2.6.3	Roll Back Changes with Semperis DSP	116
2.6.4	Configure Reporting with Semperis DSP	117

2.6.5	Configure Email Alerts with Semperis DSP	118
2.7	Glasswall FileTrust™ for Email	120
2.7.1	Install Prerequisites	120
2.7.1.1	Install the IIS web server.....	120
2.7.1.2	Install Microsoft SQL 2014 Enterprise	122
2.7.1.3	Install Microsoft Visual C++ 2015	122
2.7.2	Install the Glasswall FileTrust Server Component	124
2.7.2.1	Install Glasswall Hub	124
2.7.2.2	Install Glasswall Integration Service	128
2.7.2.3	Install Glasswall Administrator Console	131
2.7.2.4	Add the Server's Certificate	133
2.7.2.5	Install the Smtip Analysis Agent	147
2.7.2.6	Distribute the Glasswall License File.....	149
2.7.3	Configure Glasswall FileTrust.....	151
2.7.3.1	Create a New Administrator Account.....	152
2.7.3.2	Configure Notifications and Policies.....	157
2.7.3.3	Configure Inbound SMTP Policy	158
2.7.3.4	Create a Receiver Group.....	159
2.7.3.5	Create a ThreatCensor Policy Set	161
2.7.3.6	Create a Processing Rule	162
2.7.4	Configure Intelligence Sharing.....	163
2.8	Micro Focus ArcSight Enterprise Security Manager	165
2.8.1	Install the ArcSight Console	165
2.8.2	Install Individual ArcSight Windows Connectors	179
2.8.3	Install Individual ArcSight Ubuntu Connectors.....	197
2.8.4	Install a Connector Server for ESM on Windows 2012 R2.....	210
2.8.5	Install Pre-Configured Filters for ArcSight	221
2.8.5.1	Install Activate Base	221
2.8.5.2	Install Packages.....	223
2.8.6	Apply Filters to a Channel.....	224

2.8.7	Configure Email Alerts in ArcSight	225
2.8.7.1	Configure a New Destination.....	225
2.8.7.2	Configure a New Rule	226
2.9	Tripwire Enterprise	229
2.9.1	Install Tripwire Enterprise.....	230
2.9.2	Install the Axon Bridge.....	242
2.9.3	Install the Axon Agent (Windows)	242
2.9.4	Install the Axon Agent (Linux).....	243
2.9.5	Configure Tripwire Enterprise.....	244
2.9.5.1	Terminology	244
2.9.5.2	Tags.....	245
2.9.5.3	Rules.....	247
2.9.5.4	Tasks	251
2.10	Tripwire Log Center.....	254
2.10.1	Install Tripwire Log Center Manager	254
2.10.2	Configure Tripwire Log Center Manager	255
2.10.3	Install Tripwire Log Center Console	260
2.11	Cisco Identity Services Engine.....	261
2.11.1	Initial Setup	261
2.11.2	Inventory: Configure SNMP on Routers/Network Devices.....	261
2.11.3	Inventory: Configure Device Detection	261
2.11.4	Policy Enforcement: Configure Active Directory Integration	265
2.11.5	Policy Enforcement: Enable Passive Identity with AD	268
2.11.6	Policy Enforcement: Developing Policy Conditions	273
2.11.7	Policy Enforcement: Developing Policy Results.....	274
2.11.8	Policy Enforcement: Enforcing a Requirement in Policy	275
2.11.9	Policy Enforcement: Configuring a Web Portal	276
2.11.10	Configuring RADIUS with your Network Device	277
2.11.11	Configuring an Authentication Policy	278
2.11.12	Configuring an Authorization Policy	280
2.12	Cisco Advanced Malware Protection	281

2.12.1	Dashboard Configuration.....	281
2.12.2	Installing the Connector on a Windows Server	281
2.12.3	Installing the Connector on a Windows 10 Machine.....	283
2.12.4	Scanning using AMP.....	284
2.12.5	Configure AMP Policy	285
2.13	Cisco Stealthwatch.....	287
2.13.1	Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor	287
2.13.2	Change Default Stealthwatch Console Passwords	292
2.13.3	Configure the Stealthwatch Management Console Web Interface	296
2.13.4	Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces	299
2.14	Symantec Analytics	302
2.14.1	Initial Setup.....	302
2.14.2	Capturing Data.....	308
2.15	Symantec Information Centric Analytics	309
2.15.1	Installing MS SQL 2017	309
2.15.2	Install Windows Services	317
2.15.3	Installing Symantec ICA.....	325
2.15.4	Configuring Symantec ICA for Analysis.....	332
2.15.4.1	Installing Integration Packs.....	332
2.15.4.2	Create a View.....	333
2.15.4.3	Open an Existing View	334
2.15.4.4	Viewing Detailed Analyzer Data	336
2.16	Integration: Cisco Identity Services Engine and Cisco Stealthwatch	336
2.16.1	Configuring Certificates for pxGrid	336
2.16.2	Configuring Stealthwatch to Quarantine through ISE	348
2.17	Integration: Tripwire Log Center and Tripwire Enterprise.....	353
2.18	Integration: Symantec ICA and ArcSight ESM.....	360
2.18.1	Export the CSV File from ArcSight Console.....	360
2.18.2	Import the CSV File to Symantec ICA.....	362

2.18.3	Create a Mapping between ArcSight events and Symantec ICA	366
2.18.4	View ArcSight Events in the Analyzer	371
2.19	Integration: Micro Focus ArcSight and Tripwire	372
2.19.1	Install Micro Focus ArcSight.....	372
2.20	Integration: Micro Focus ArcSight and Cisco AMP	384
2.20.1	Create API Credentials for ArcSight to access AMP	384
2.20.2	Install Micro Focus ArcSight.....	385
2.20.3	Create a Parser for Cisco AMP REST events.....	393
2.21	Integration: Micro Focus ArcSight and Cisco ISE	394
2.21.1	Configure Cisco ISE to Forward Logs.....	395
2.21.2	Select Logs for Forwarding	396
2.22	Integration: Micro Focus ArcSight and Semperis DSP	398
2.22.1	Configure Semperis DSP to Forward Logs	398
2.23	Integration: Micro Focus ArcSight and Symantec Analytics	399
2.23.1	Configure Symantec Analytics to Forward Logs	399
2.23.2	Install Symantec Analytics Package for ArcSight	401
2.24	Integration: Micro Focus ArcSight and Glasswall FileTrust.....	409
2.24.1	Install Micro Focus ArcSight.....	409
2.25	Integration: Micro Focus ArcSight and Cisco Stealthwatch.....	424
2.25.1	Install Micro Focus ArcSight.....	424
2.25.2	Configure Cisco Stealthwatch	433
Appendix A List of Acronyms.....		441

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

2 Product Installation Guides

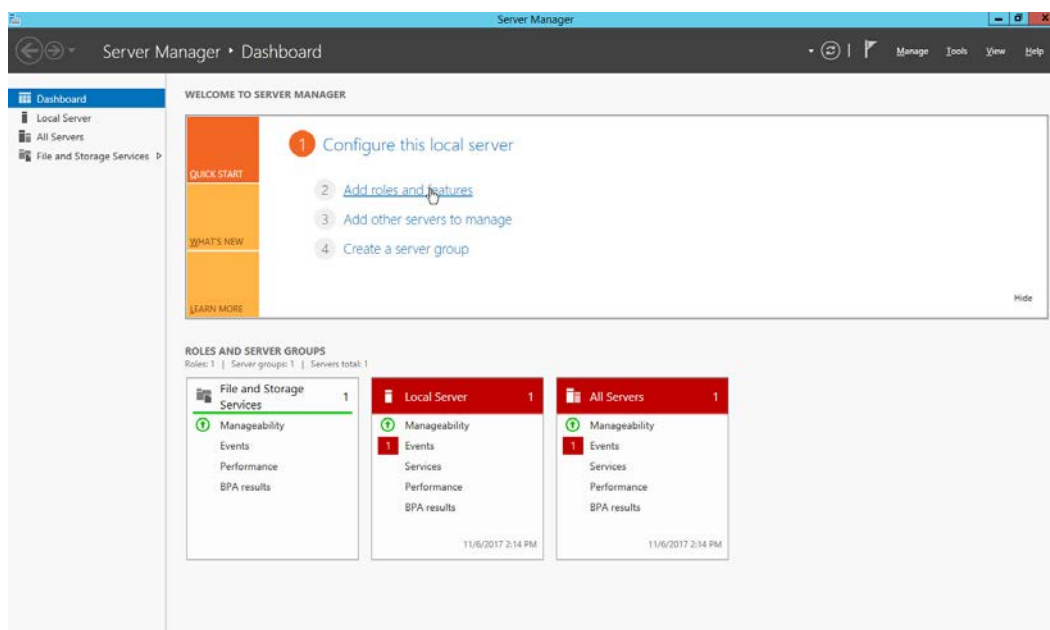
This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

2.1 Active Directory and Domain Name System Server

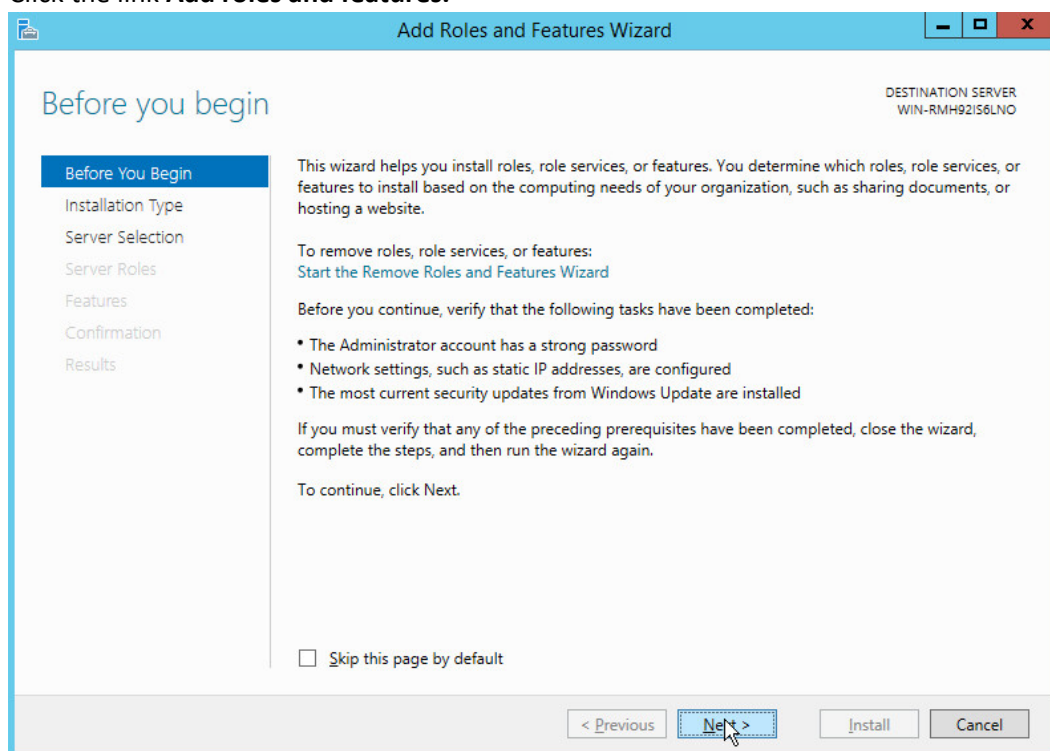
As part of our enterprise emulation, we included an Active Directory server that doubles as a Domain Name System (DNS) server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

2.1.1 Install Features

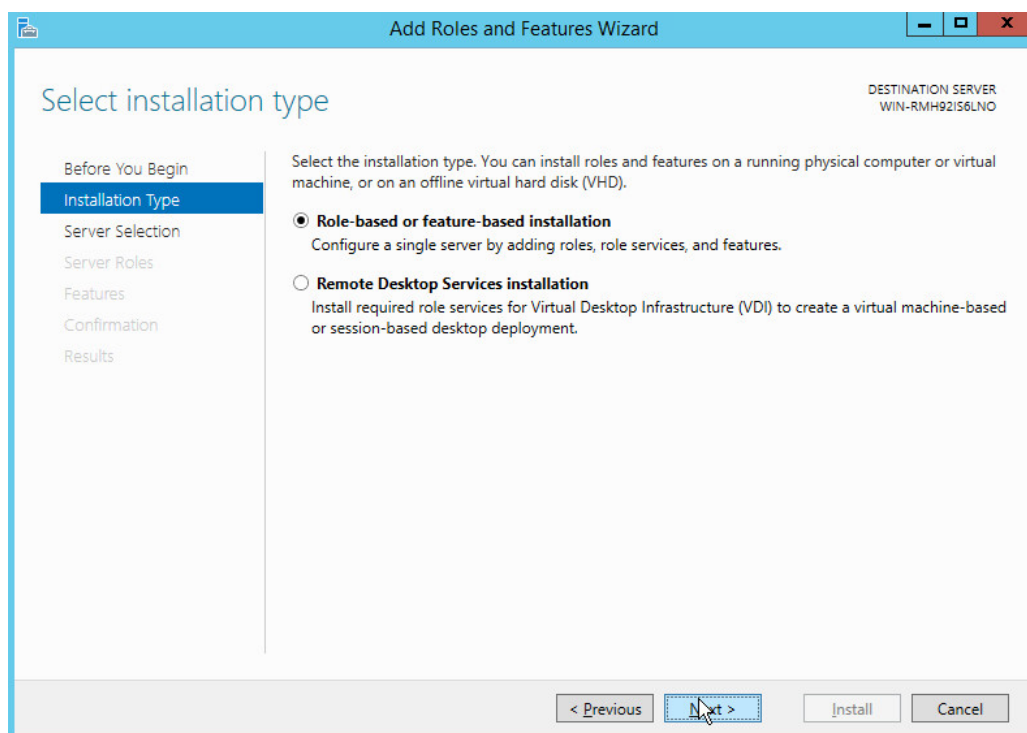
1. Open **Server Manager**.



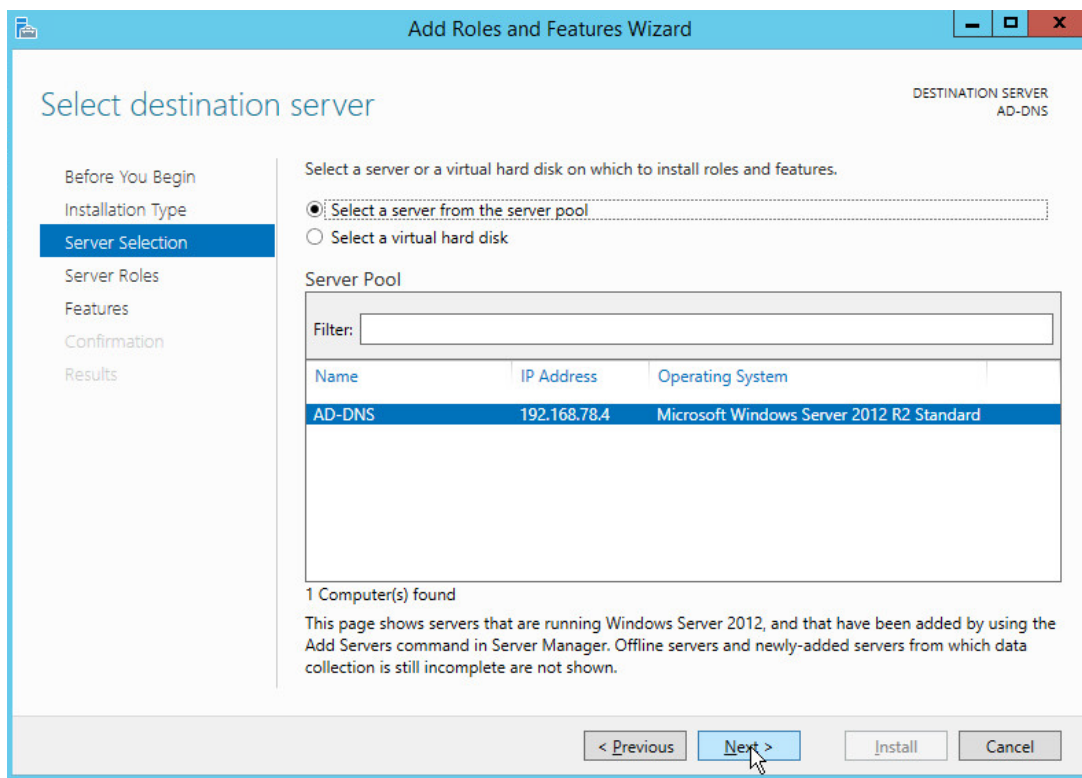
2. Click the link **Add roles and features**.



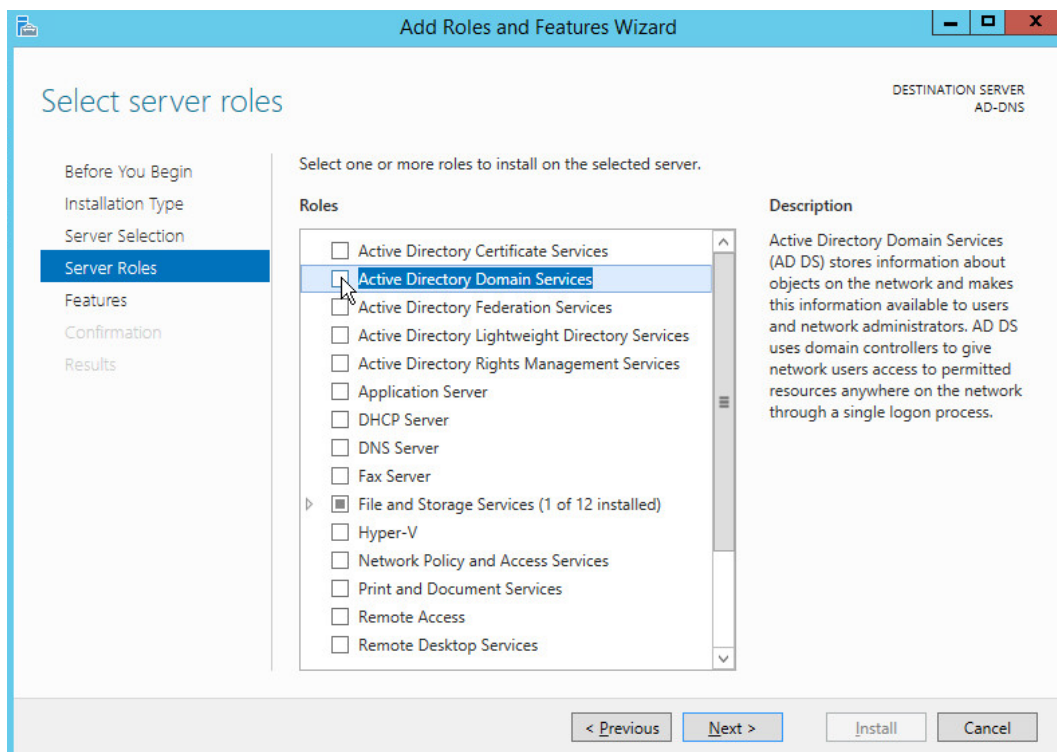
3. Click **Next**.
4. Select **Role-based or feature-based installation**.



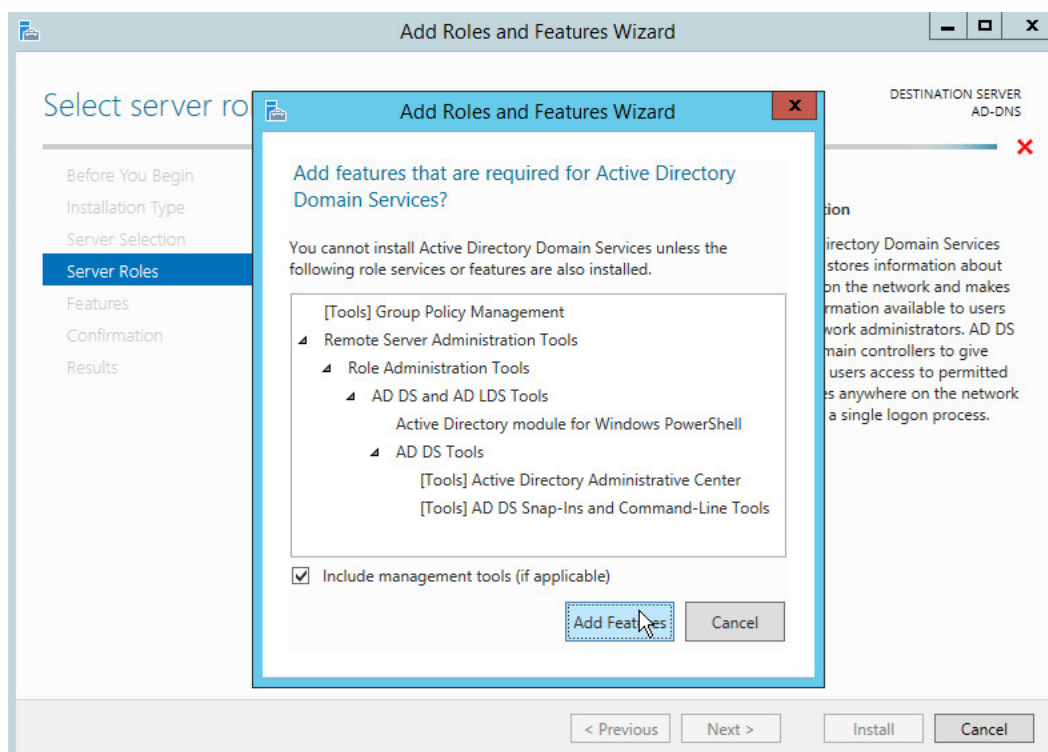
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Select the intended active directory server.



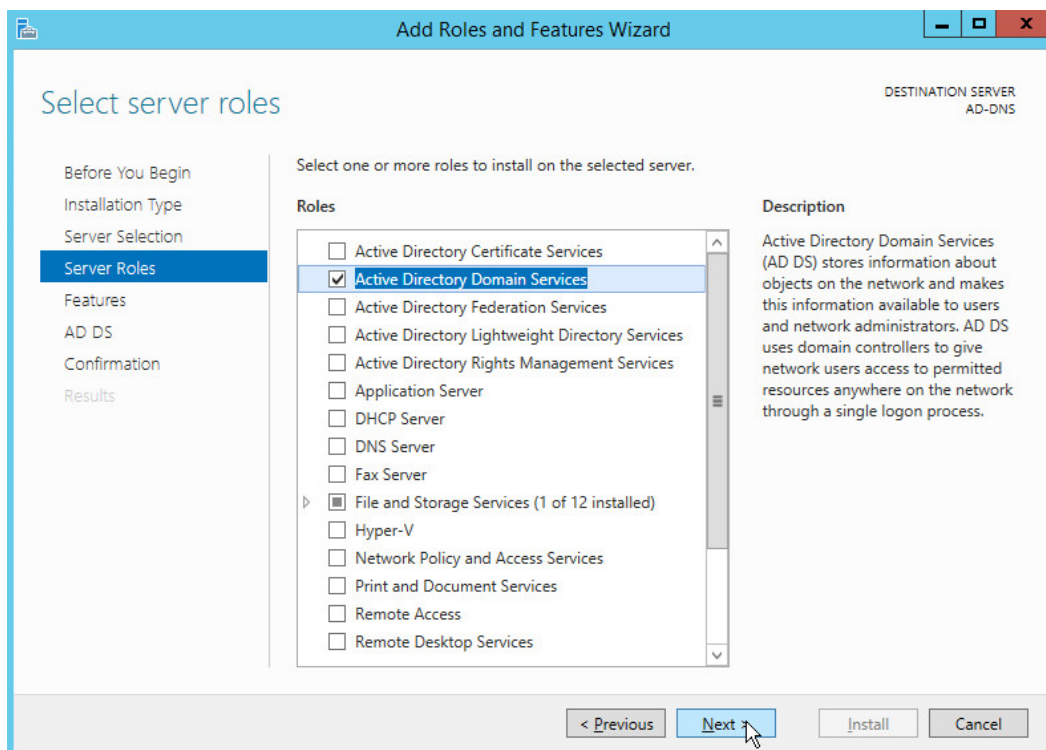
8. Click **Next**.



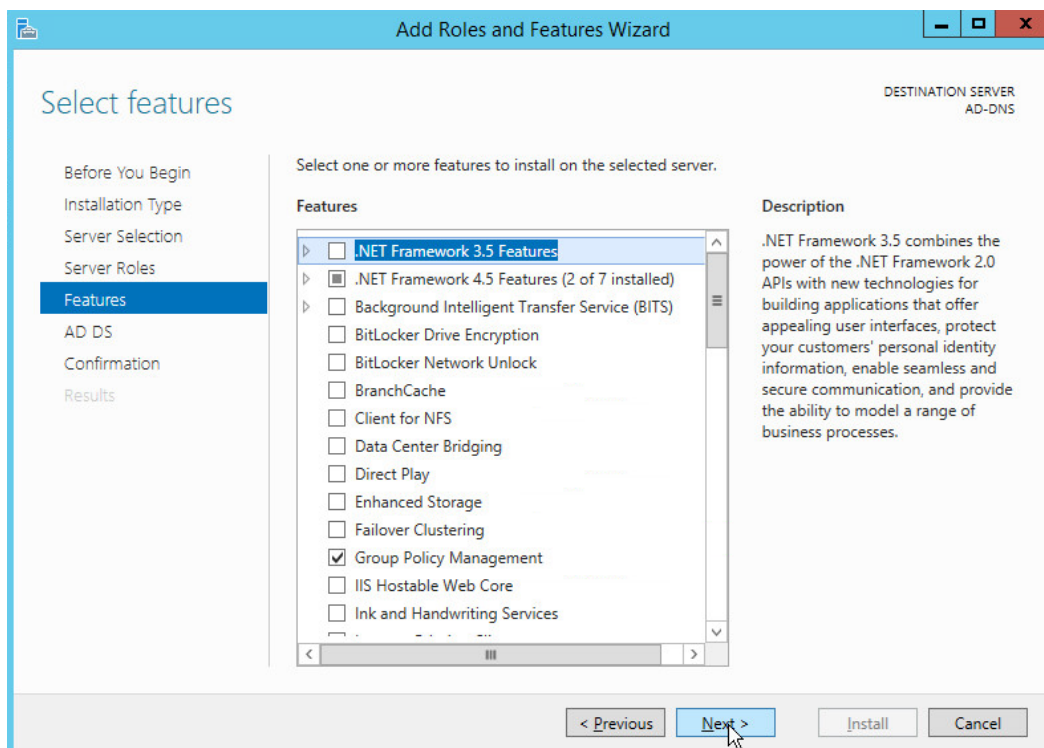
9. Check the box next to **Active Directory Domain Services**.



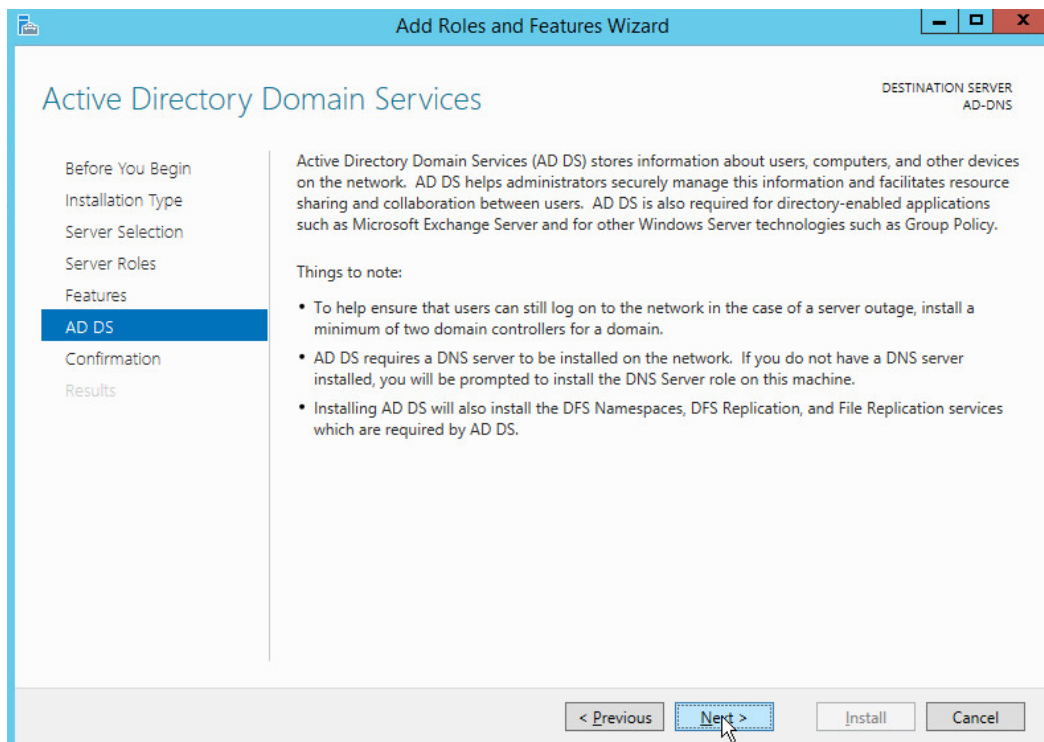
10. Click **Add Features**.



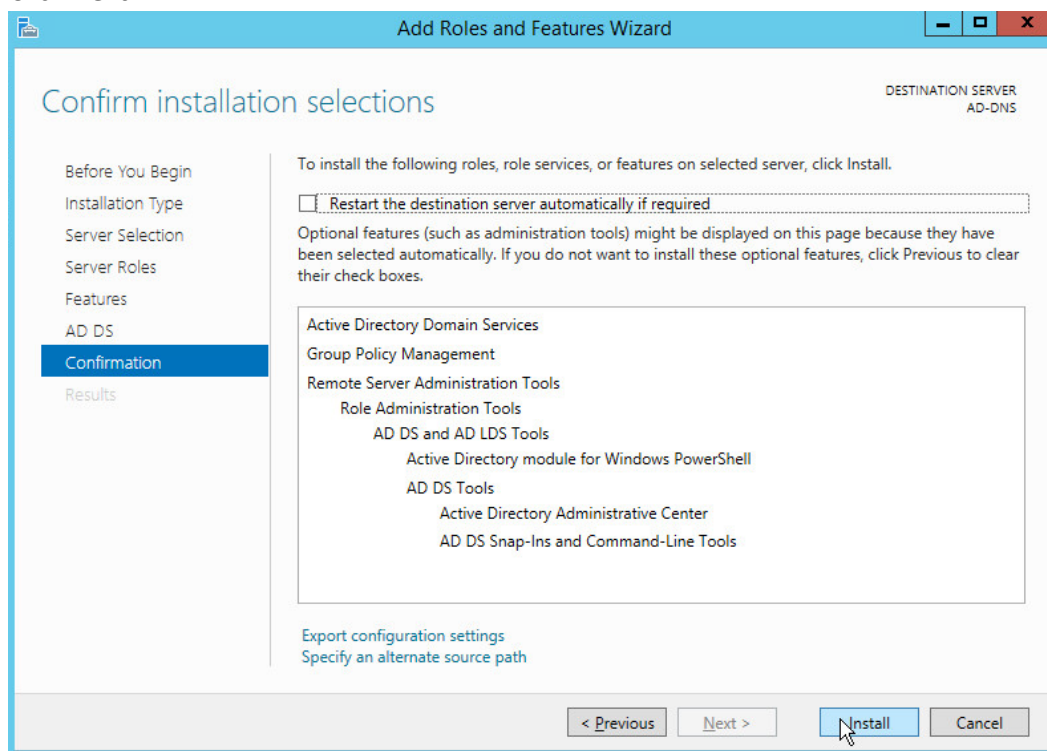
11. Click **Next**.



12. Click **Next**.

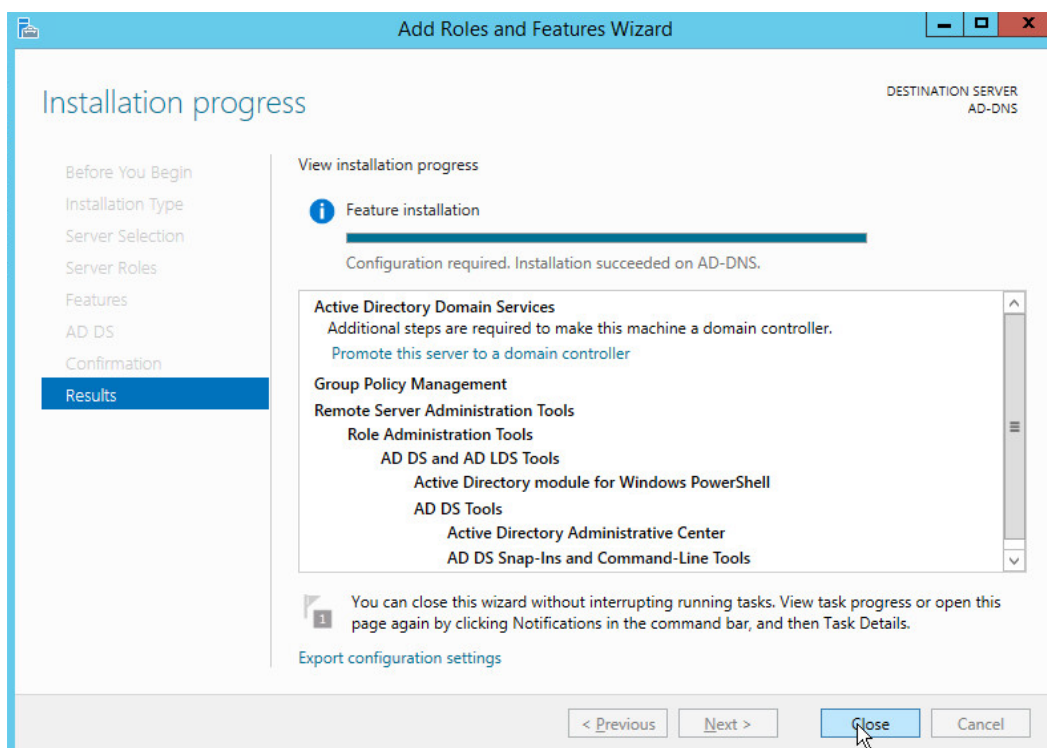


13. Click **Next**.

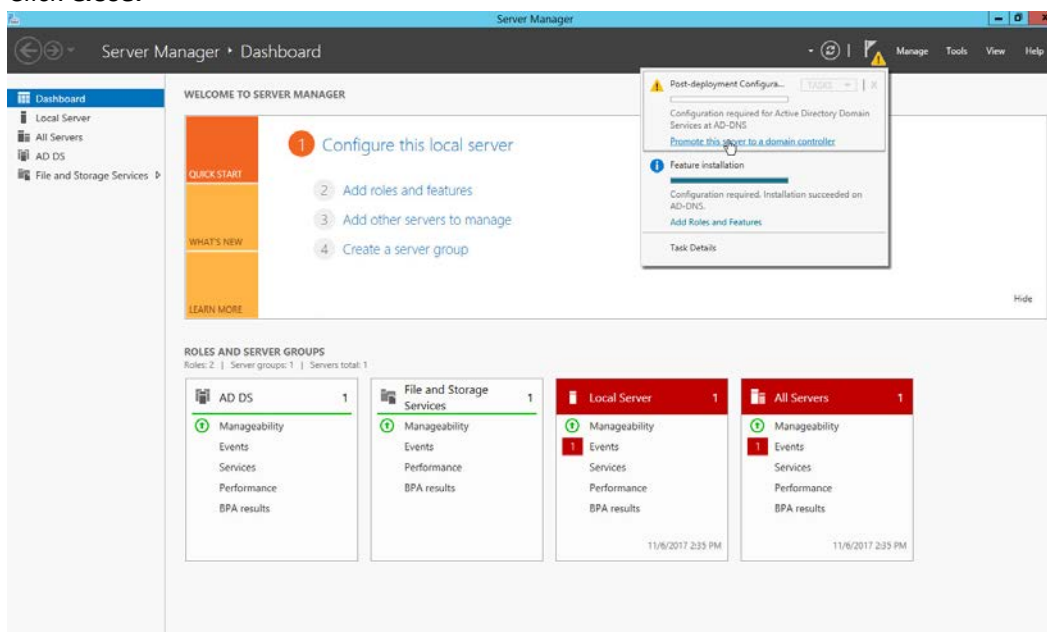


14. Click **Install**.

15. Wait for the installation to complete.



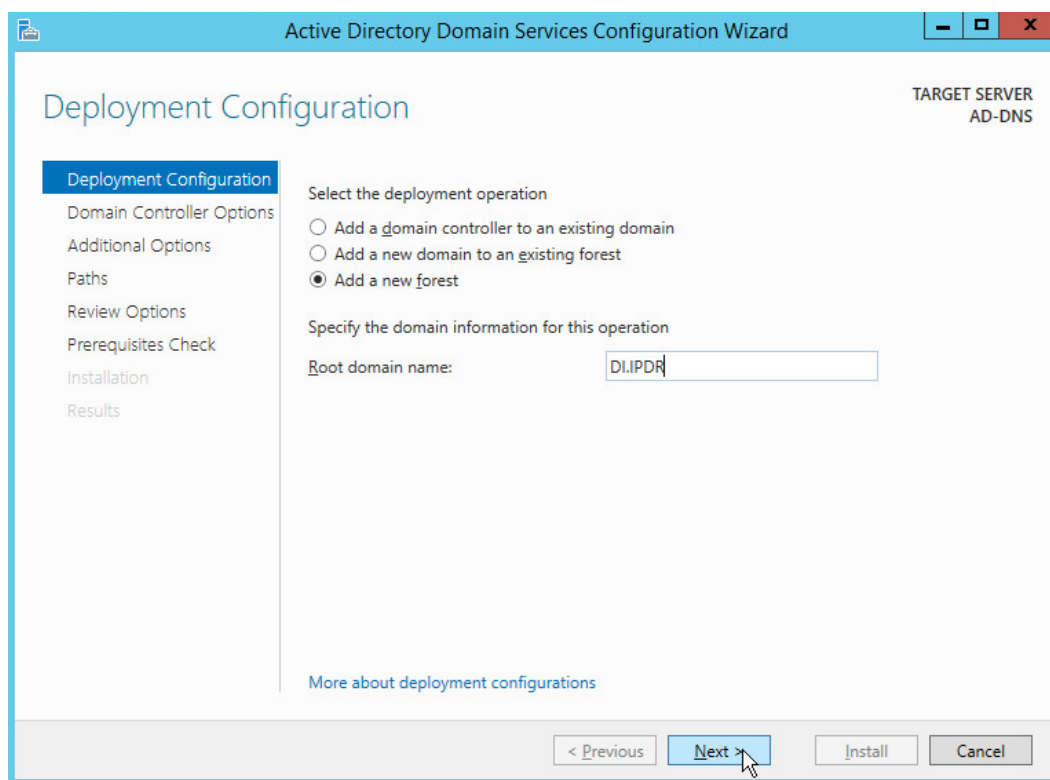
16. Click **Close**.



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

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

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



20. Click **Next**.
21. Select **Windows Server 2012 R2** for **Forest functional level** and **Domain functional level**.
22. Check the box next to **Domain Name System (DNS) server**.
23. Enter a password.

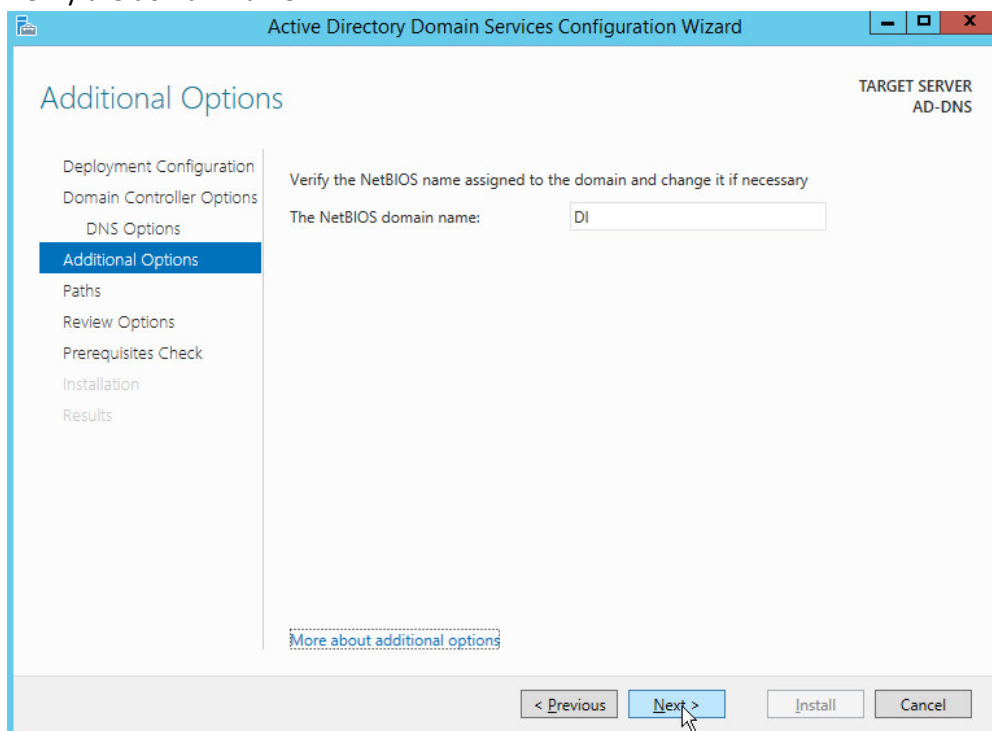
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes standard Windows window controls. The main window has a blue header with the title 'Active Directory Domain Services Configuration Wizard'. Below the header, the window is titled 'Domain Controller Options'. On the right side, it says 'TARGET SERVER AD-DNS'. On the left, there is a navigation pane with the following items: 'Deployment Configuration', 'Domain Controller Options' (which is highlighted with a blue background), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select functional level of the new forest and root domain'. It contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2012 R2'. Below these, there is a section titled 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Further down, there is a section titled 'Type the Directory Services Restore Mode (DSRM) password' with two password fields labeled 'Password:' and 'Confirm password:'. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (which is highlighted with a blue background and has a mouse cursor over it), 'Install', and 'Cancel'. A link 'More about domain controller options' is located at the bottom left of the main content area.

24. Click **Next**.

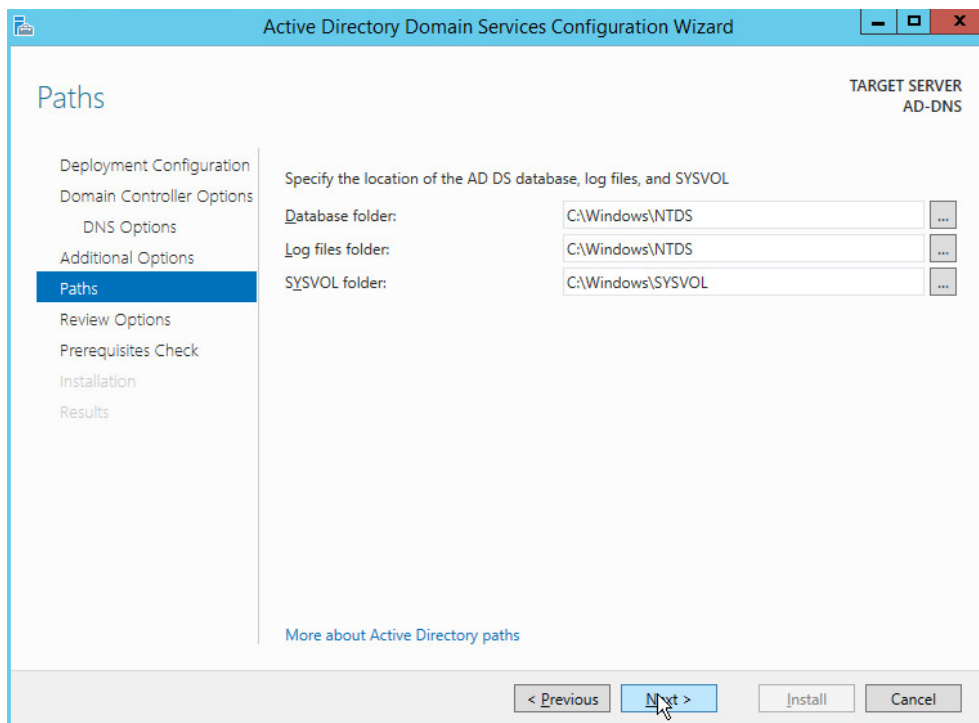
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, now on the 'DNS Options' screen. The title bar and header are the same as the previous screenshot. The navigation pane on the left now has 'DNS Options' highlighted with a blue background. The main content area is titled 'Specify DNS delegation options' and contains a single checkbox labeled 'Create DNS delegation', which is currently unchecked. At the bottom of the window, the 'Next >' button is highlighted with a blue background and has a mouse cursor over it. A link 'More about DNS delegation' is located at the bottom left of the main content area.

25. Click **Next**.

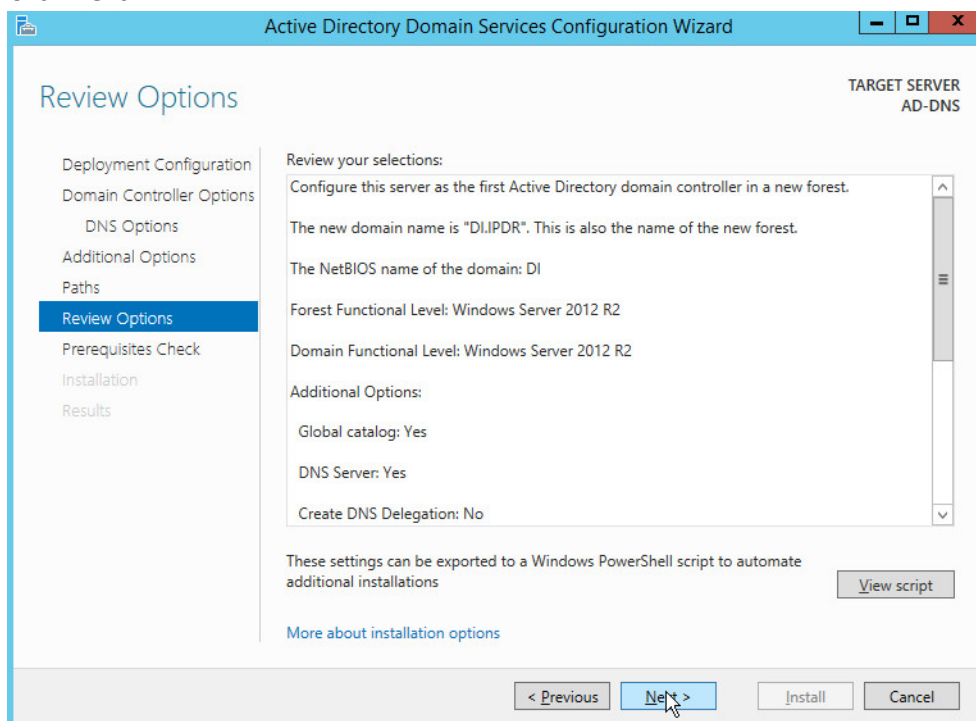
26. Verify the domain name.



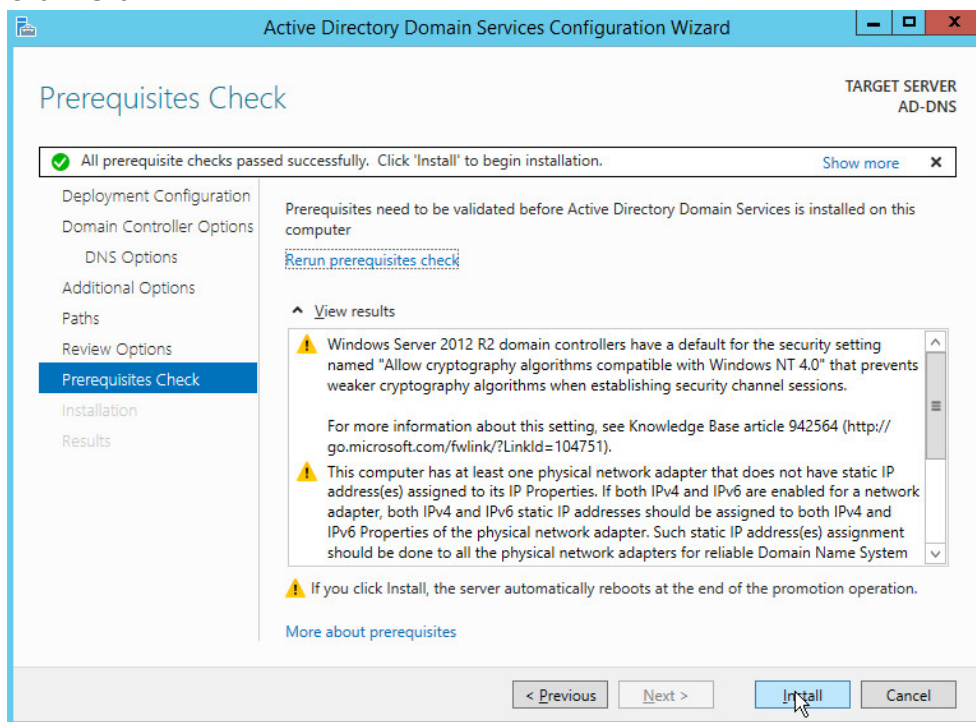
27. Click Next.



28. Click **Next**.



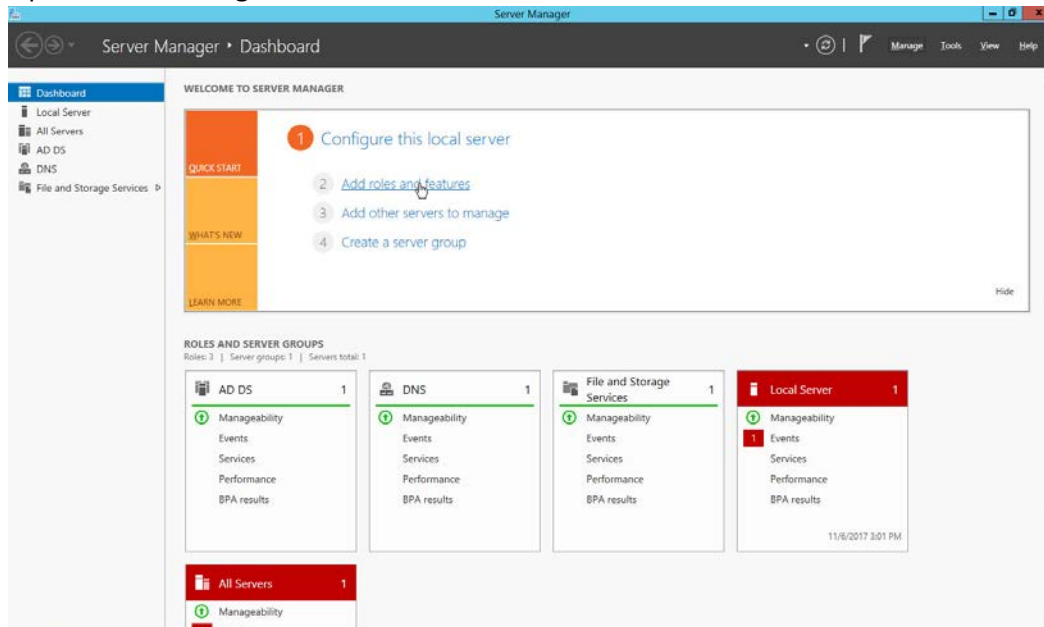
29. Click **Next**.



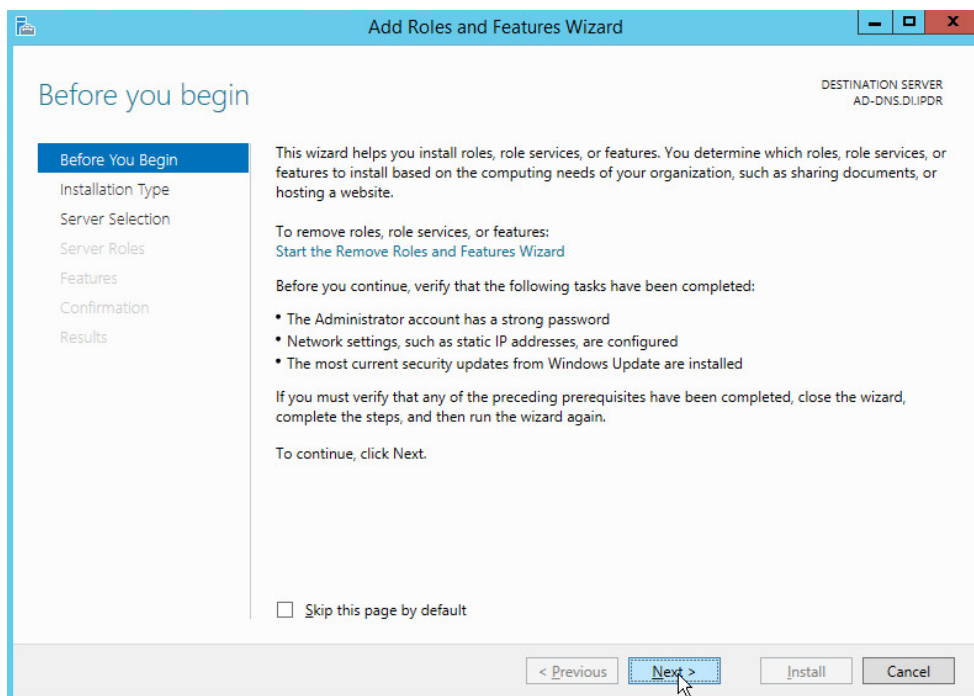
30. Click **Install**.
31. Wait for the installation to complete.
32. The server automatically reboots.

2.1.2 Create a Certificate Authority

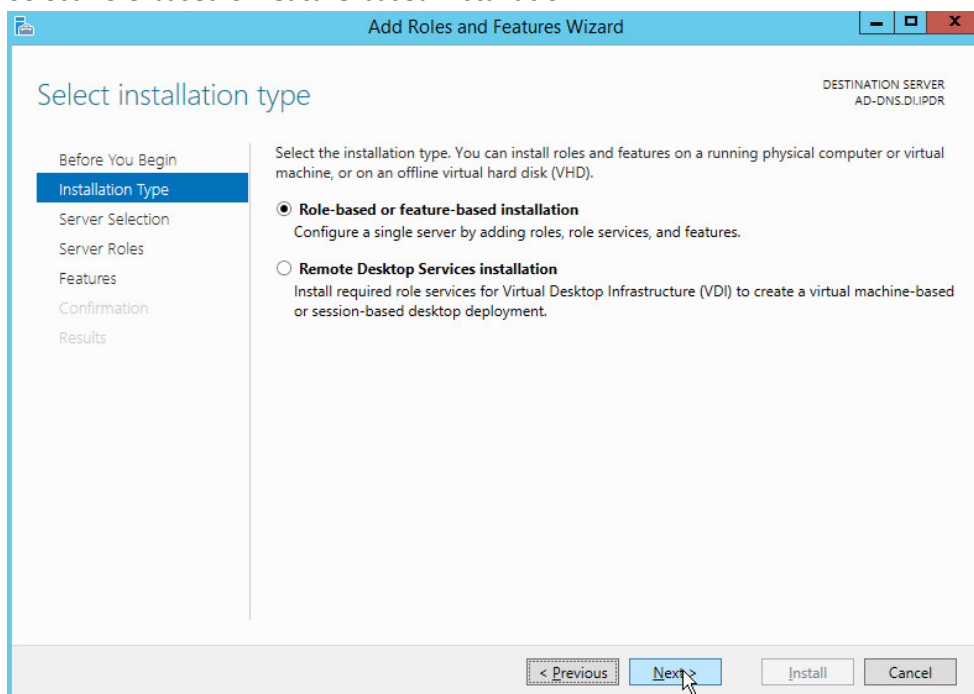
1. Open **Server Manager**.



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

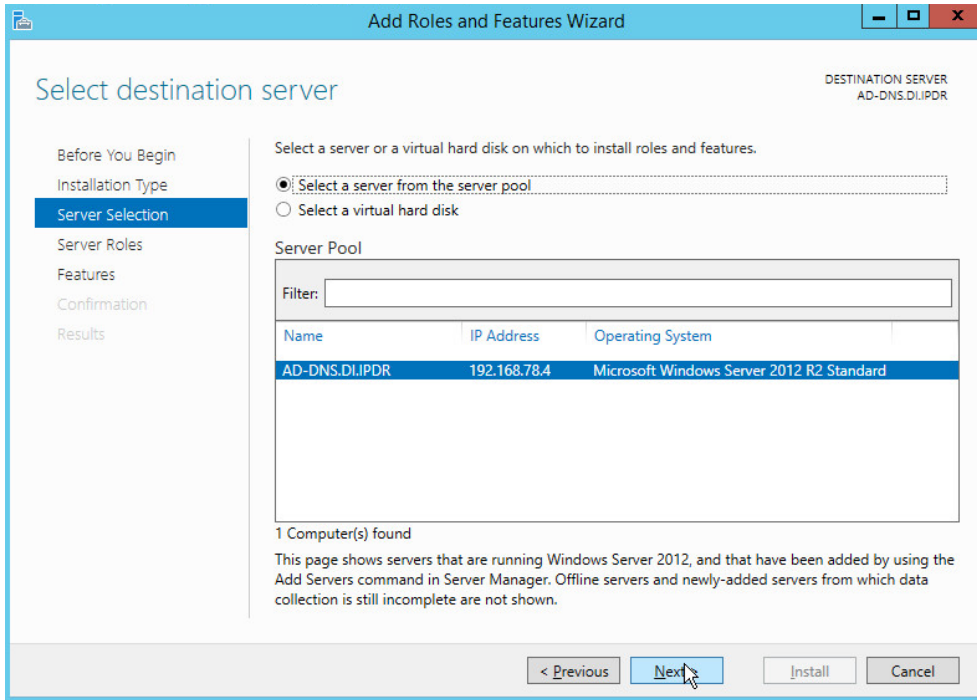


3. Click **Next**.
4. Select **Role-based or feature-based installation**.

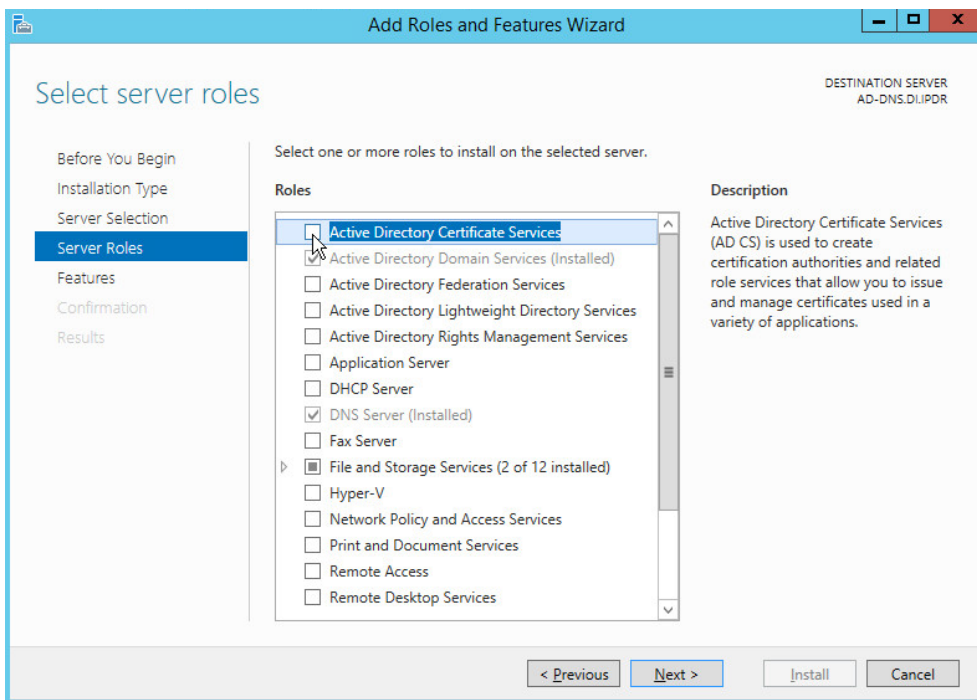


5. Click **Next**.

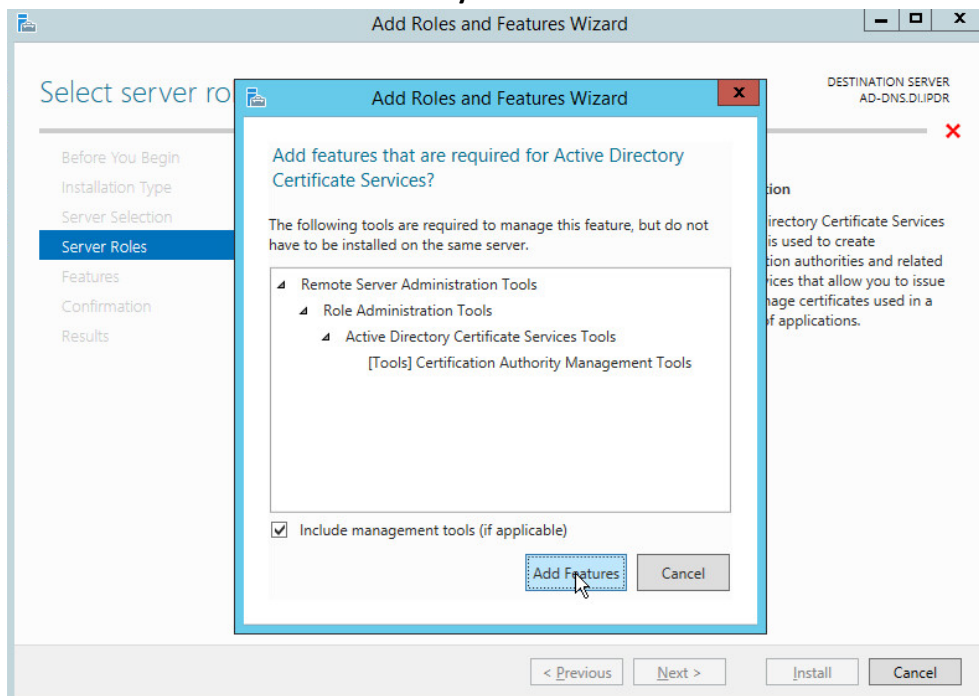
6. Select **Select a server from the server pool**.
7. Select the intended Active Directory server.



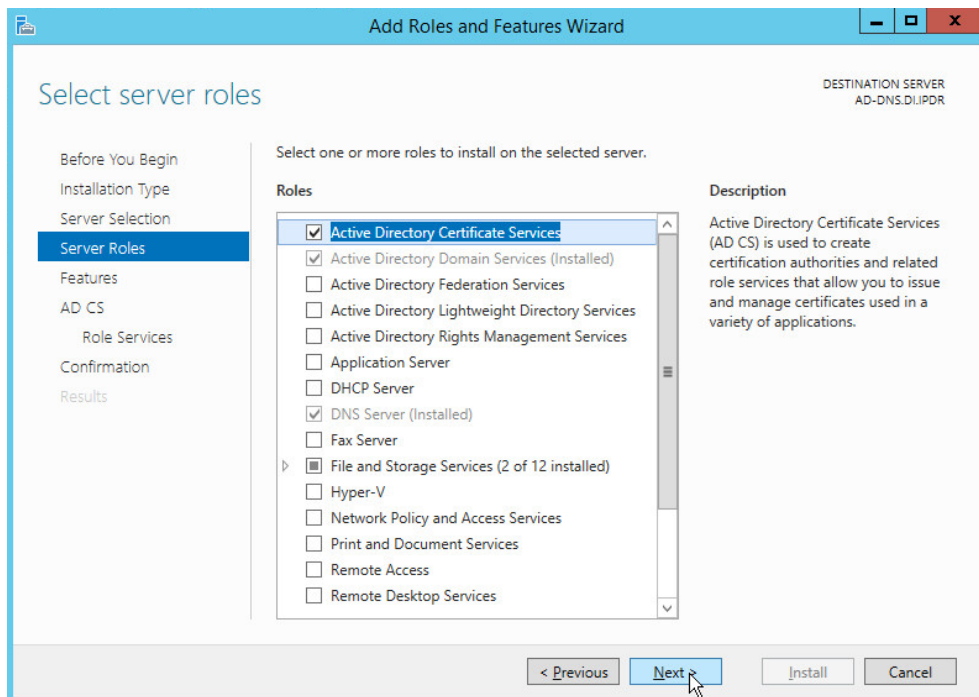
8. Click **Next**.



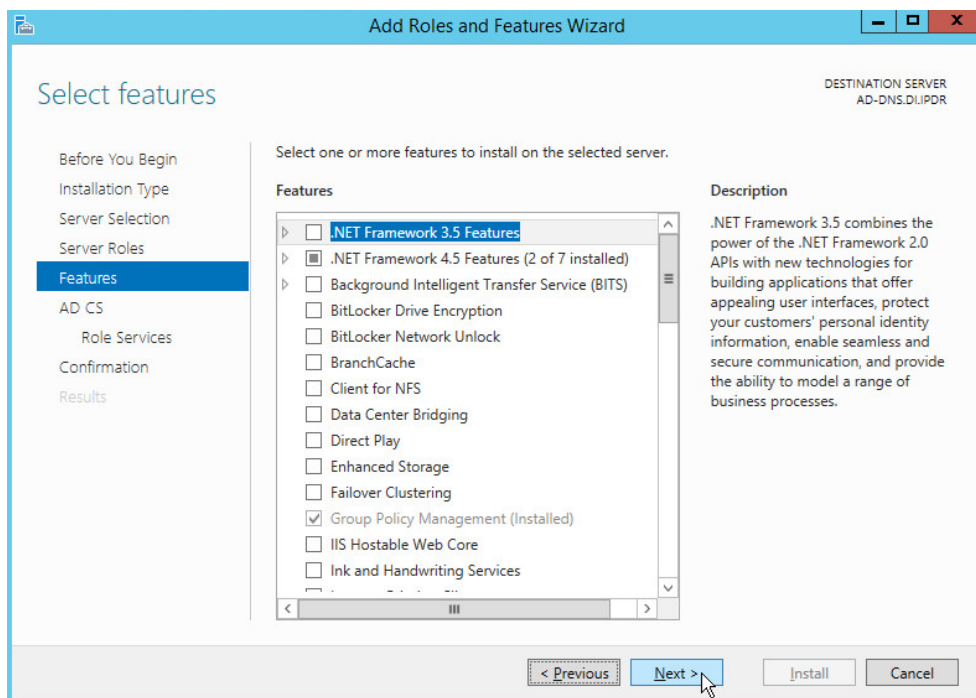
9. Check the box next to **Active Directory Certificate Services**.



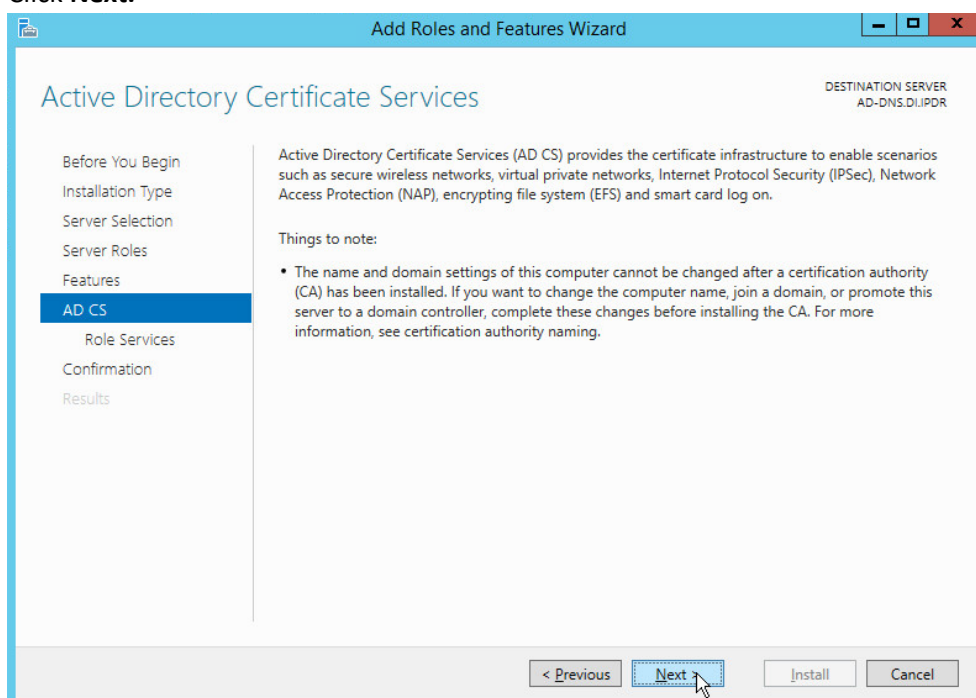
10. Click **Add Features**.



11. Click **Next**.

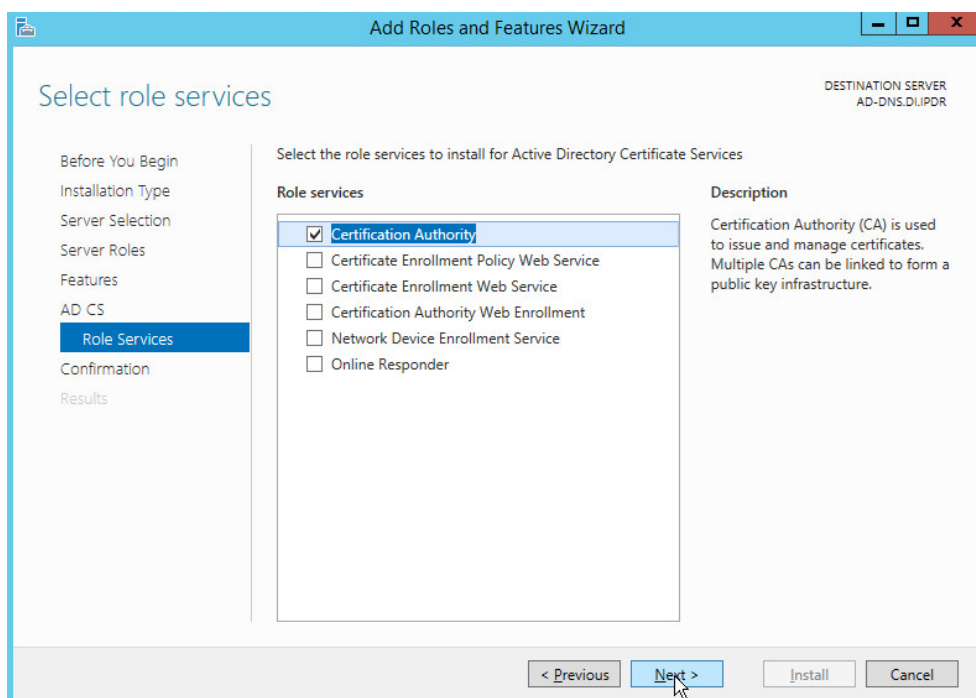


12. Click **Next**.

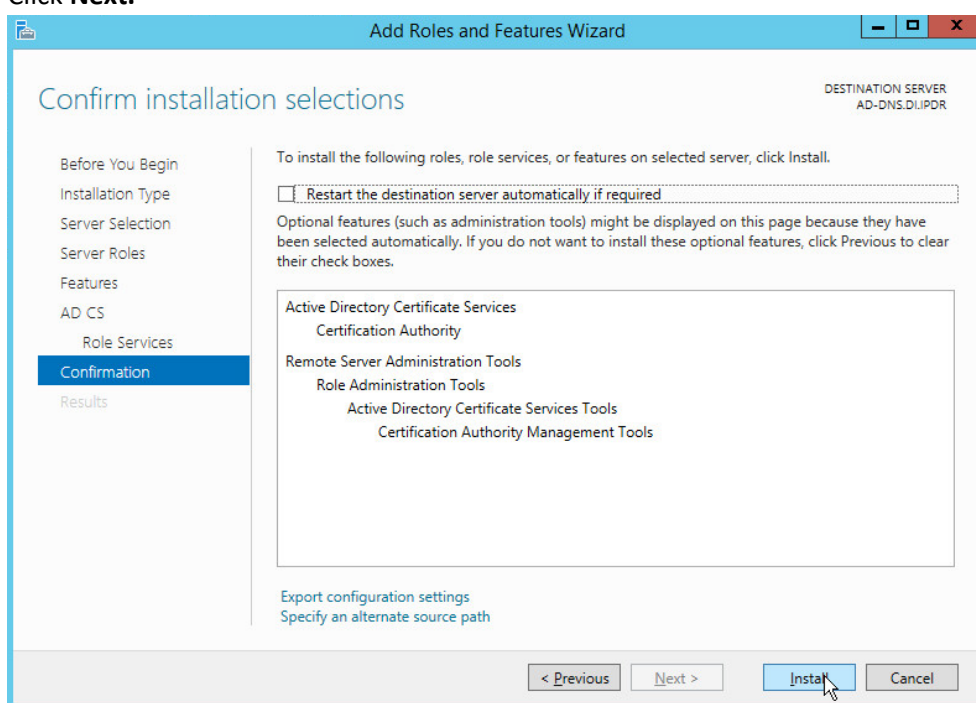


13. Click **Next**.

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

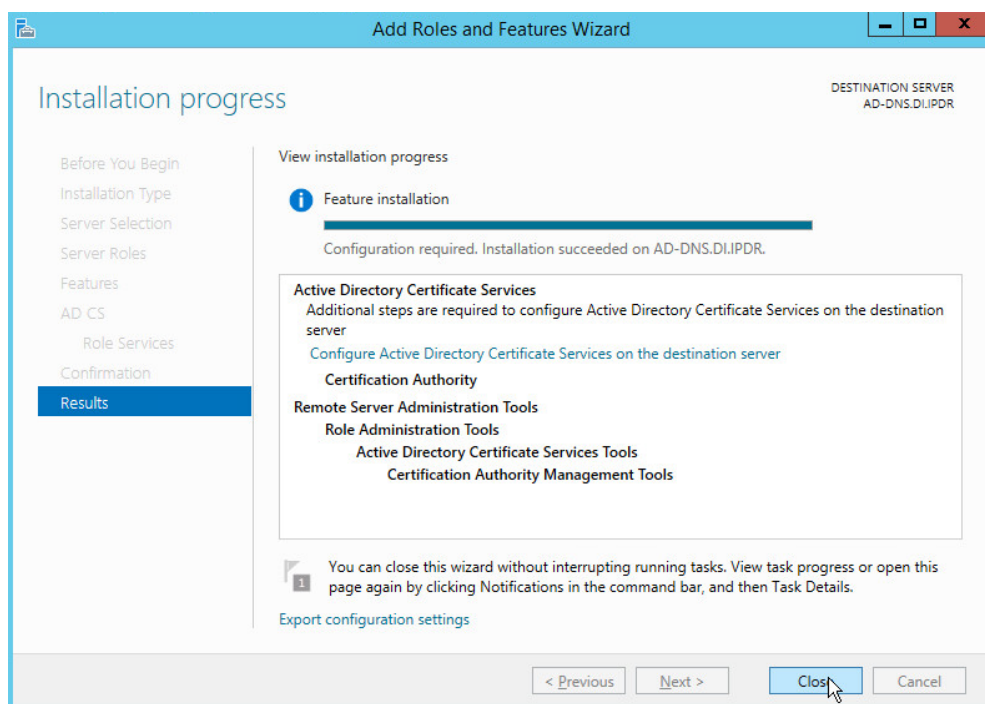


15. Click **Next**.

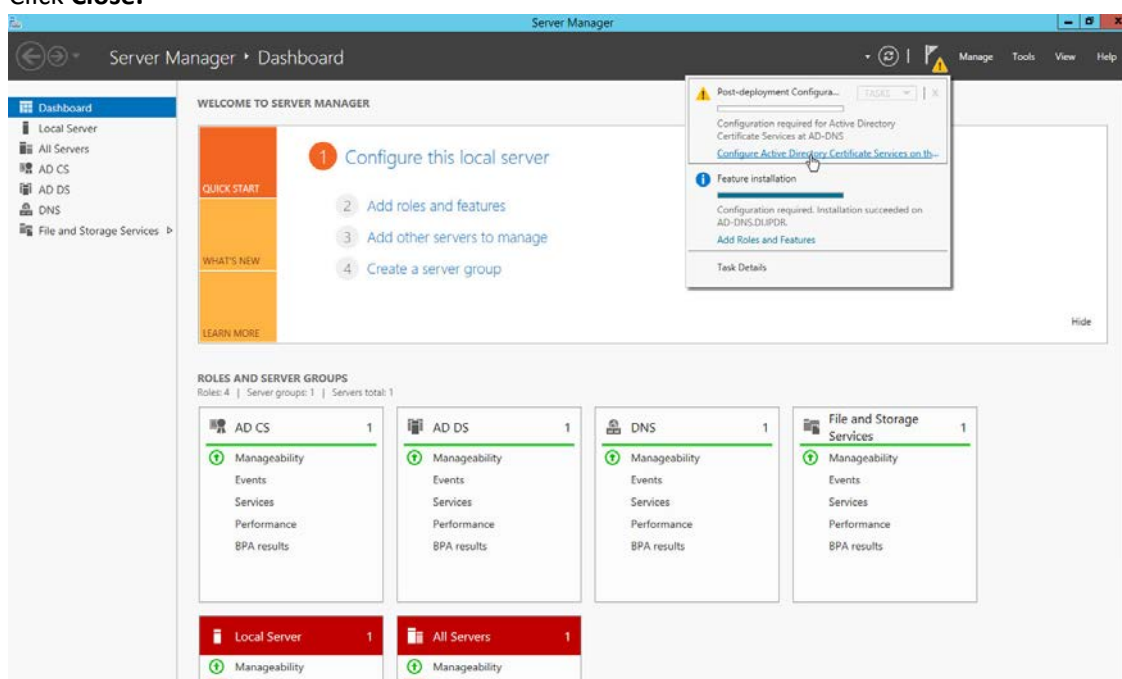


16. Click **Install**.

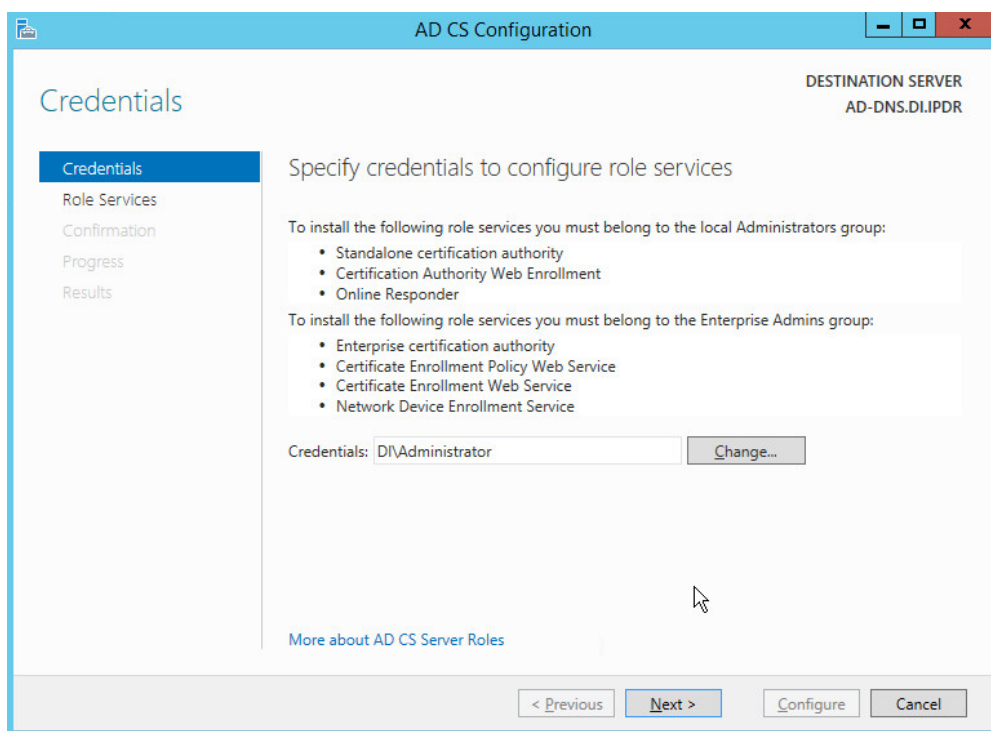
17. Wait for the installation to complete.



18. Click **Close**.

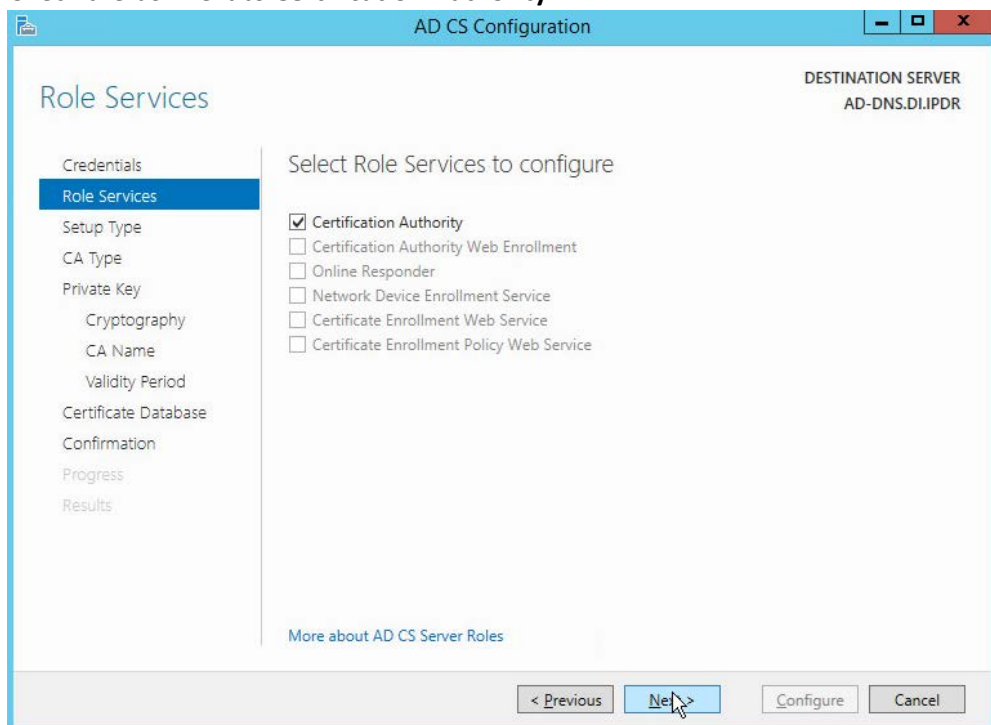


19. Click **Configure Active Directory Certificate Services on the destination server**.



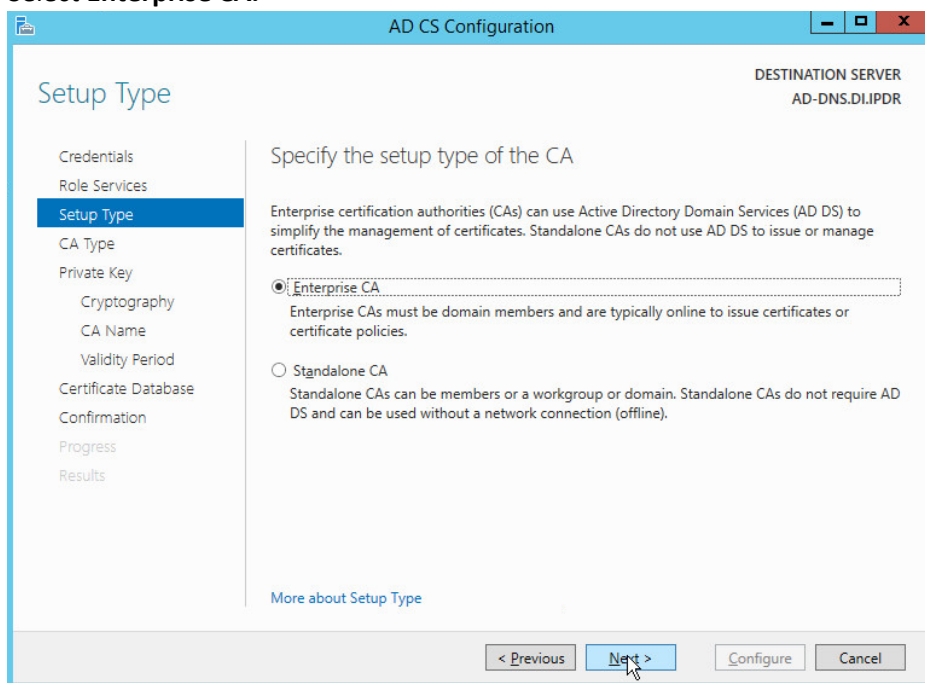
20. Click **Next**.

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



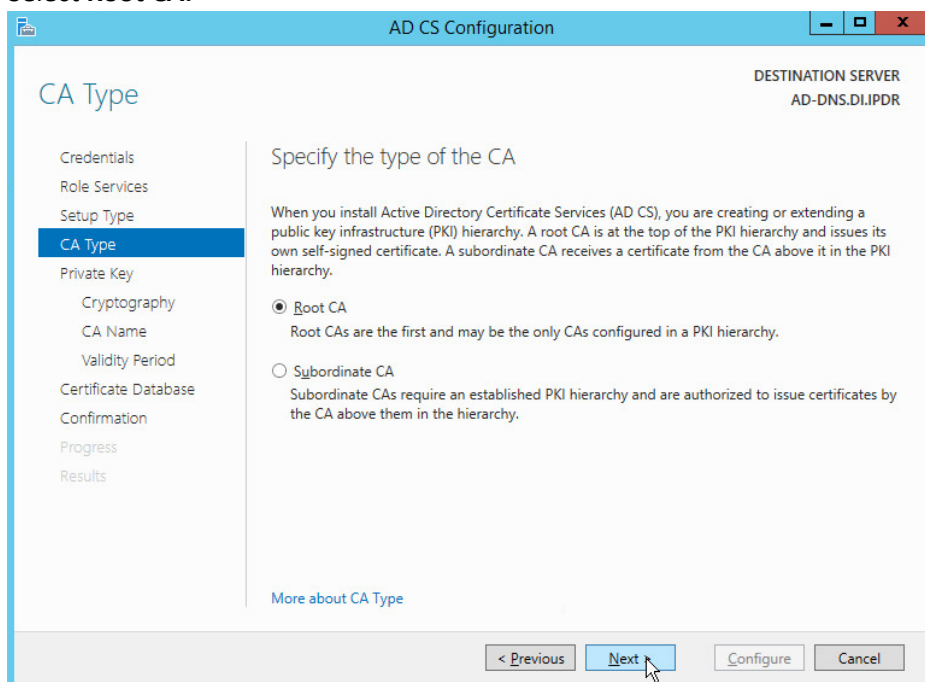
22. Click **Next**.

23. Select **Enterprise CA**.



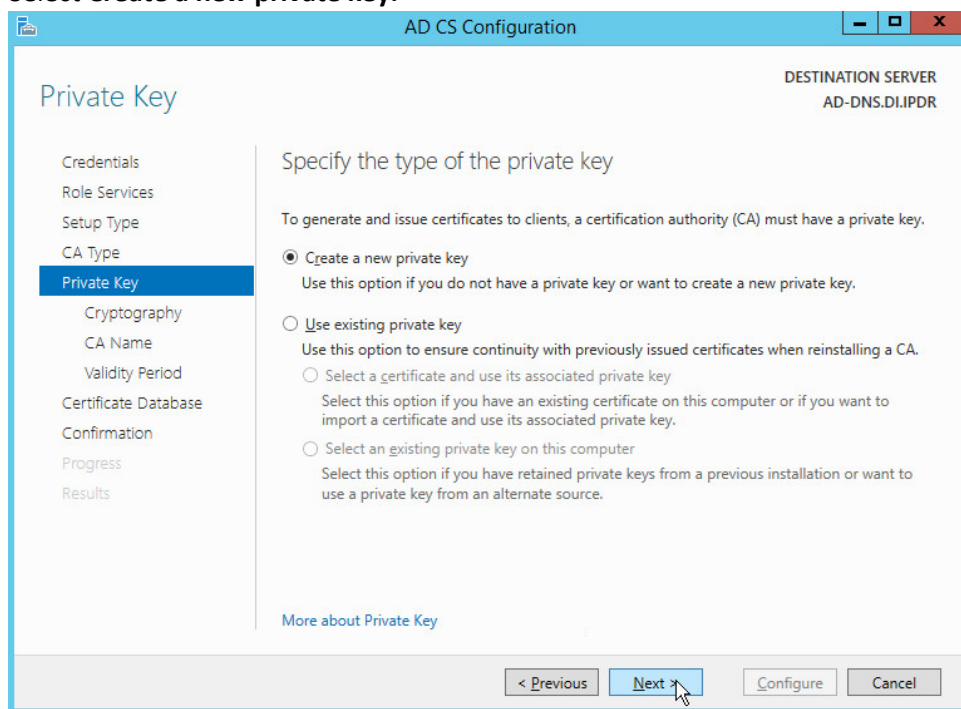
24. Click **Next**.

25. Select **Root CA**.



26. Click **Next**.

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

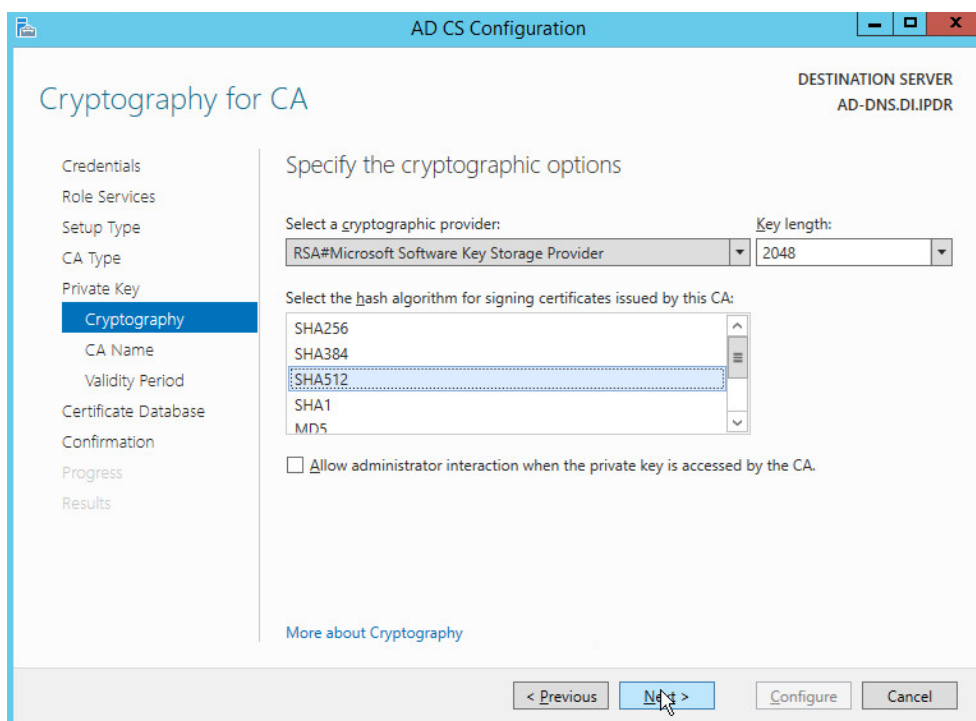


28. Click **Next**.

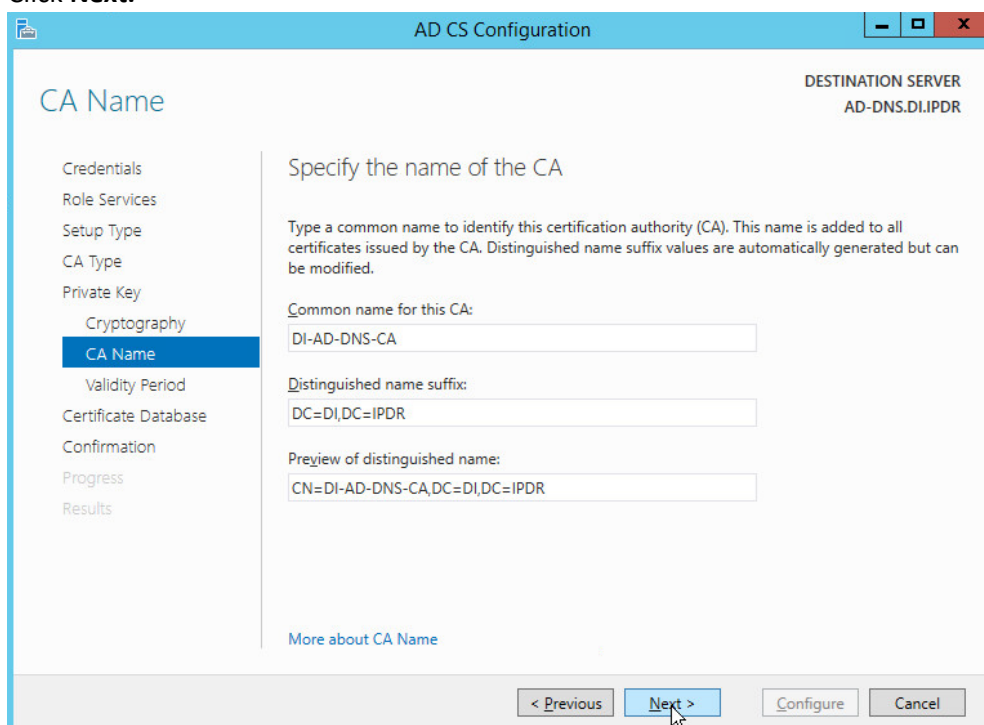
29. Select **RSA#Microsoft Software Key Storage Provider**.

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

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

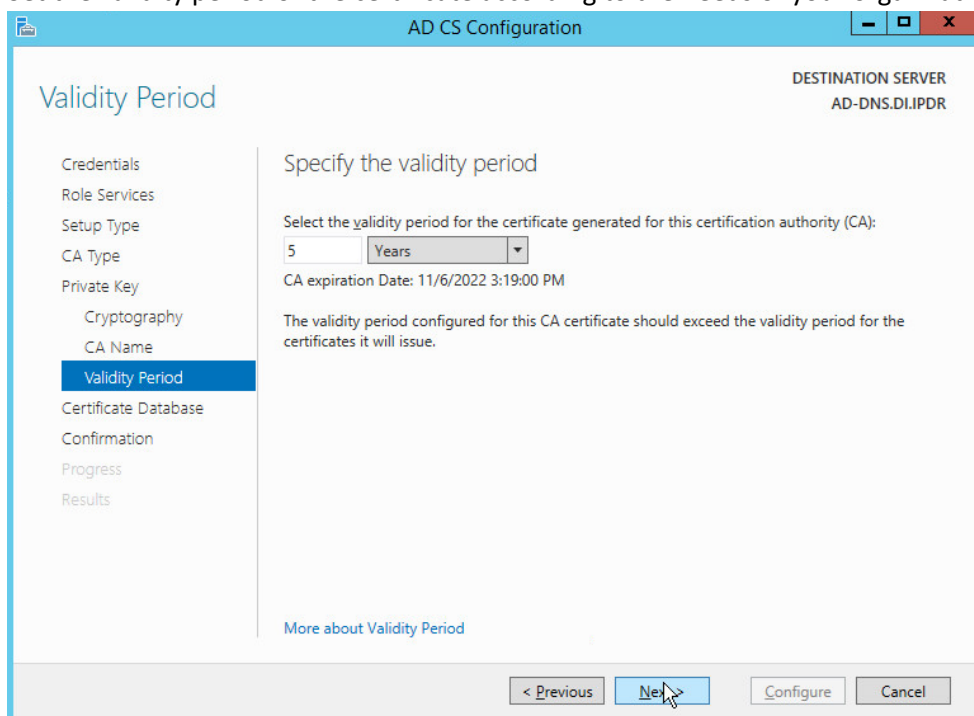


32. Click **Next**.



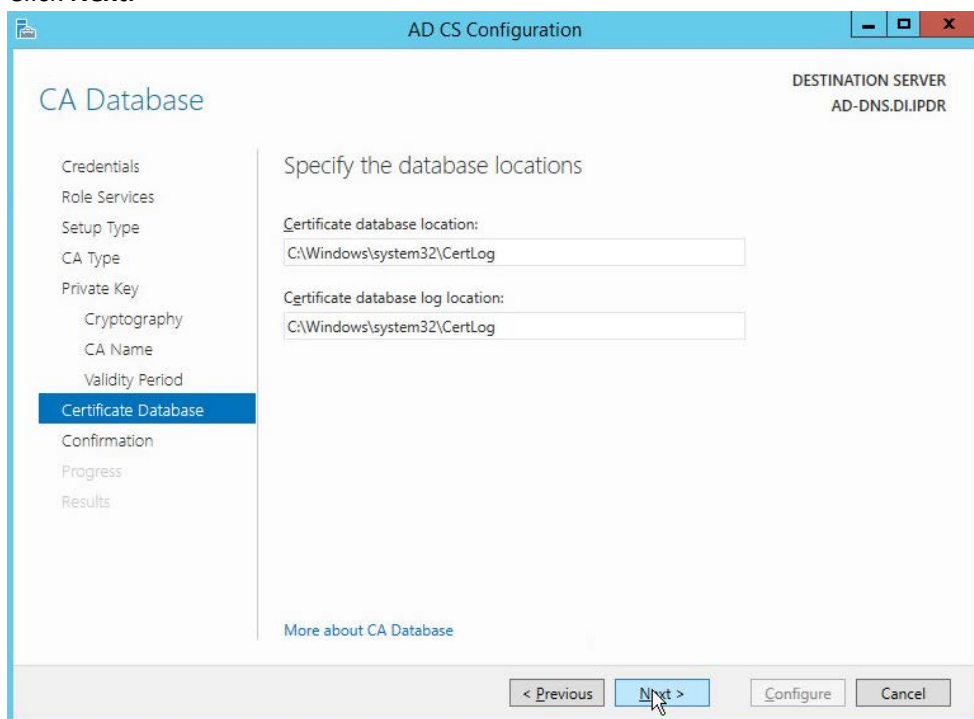
33. Click **Next**.

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



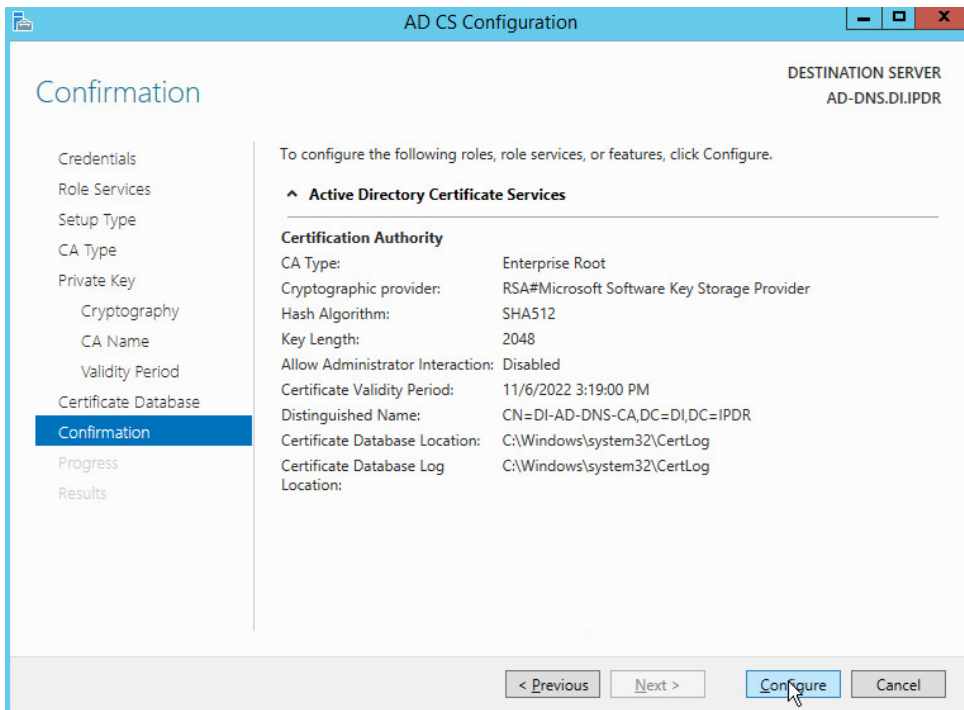
The screenshot shows the 'AD CS Configuration' window with the 'Validity Period' step selected in the left-hand navigation pane. The main area is titled 'Specify the validity period'. It includes a section 'Select the validity period for the certificate generated for this certification authority (CA):' with a text box containing '5' and a dropdown menu set to 'Years'. Below this, it shows 'CA expiration Date: 11/6/2022 3:19:00 PM'. A note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

35. Click **Next**.

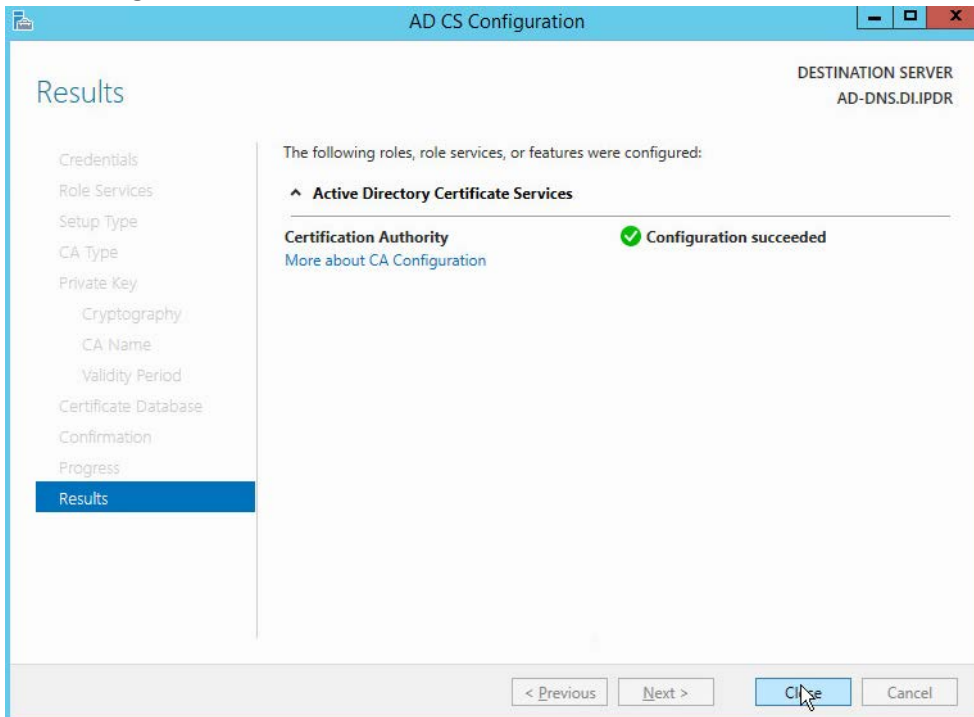


The screenshot shows the 'AD CS Configuration' window with the 'CA Database' step selected in the left-hand navigation pane. The main area is titled 'Specify the database locations'. It includes two text boxes: 'Certificate database location:' with the value 'C:\Windows\system32\CertLog' and 'Certificate database log location:' with the value 'C:\Windows\system32\CertLog'. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

36. Click **Next**.



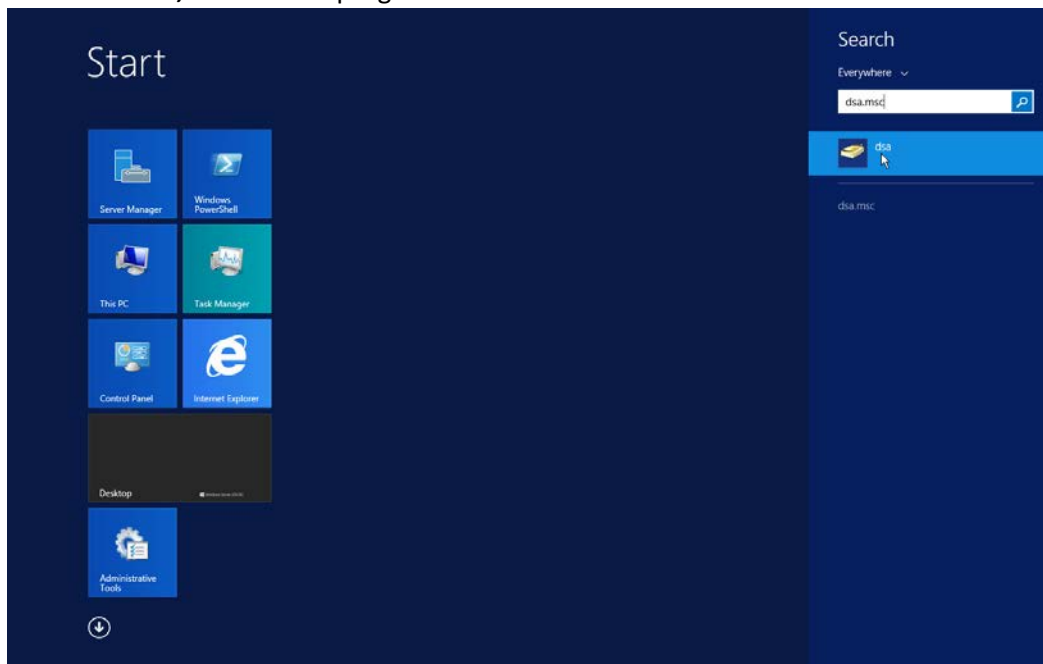
37. Click **Configure**.



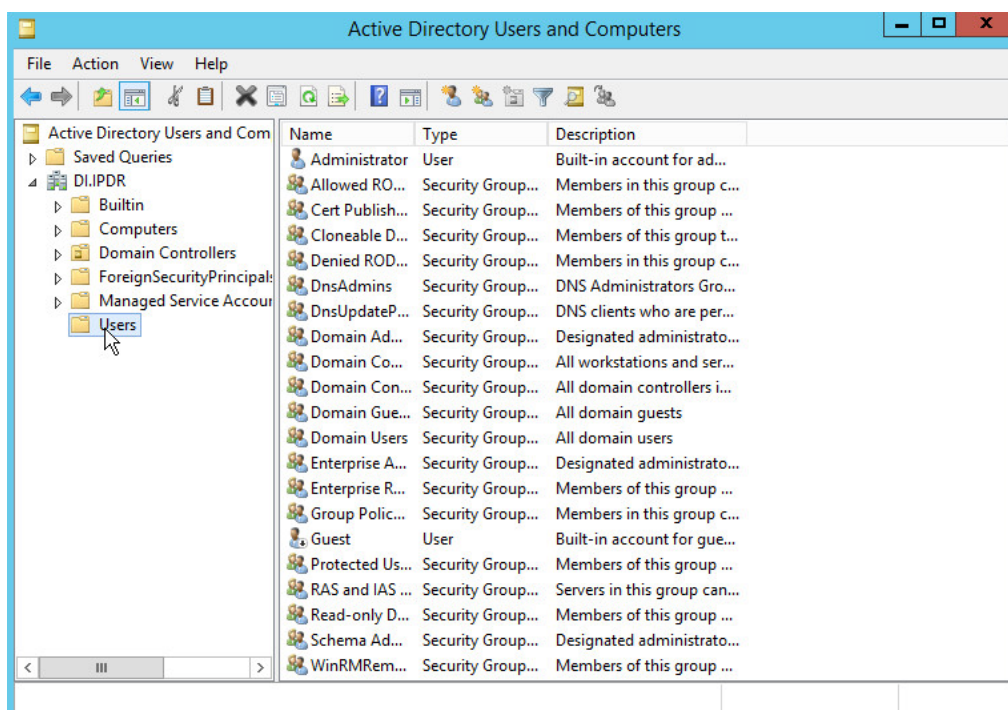
38. Click **Close**.

2.1.3 Configure Account to Add Computers to Domain

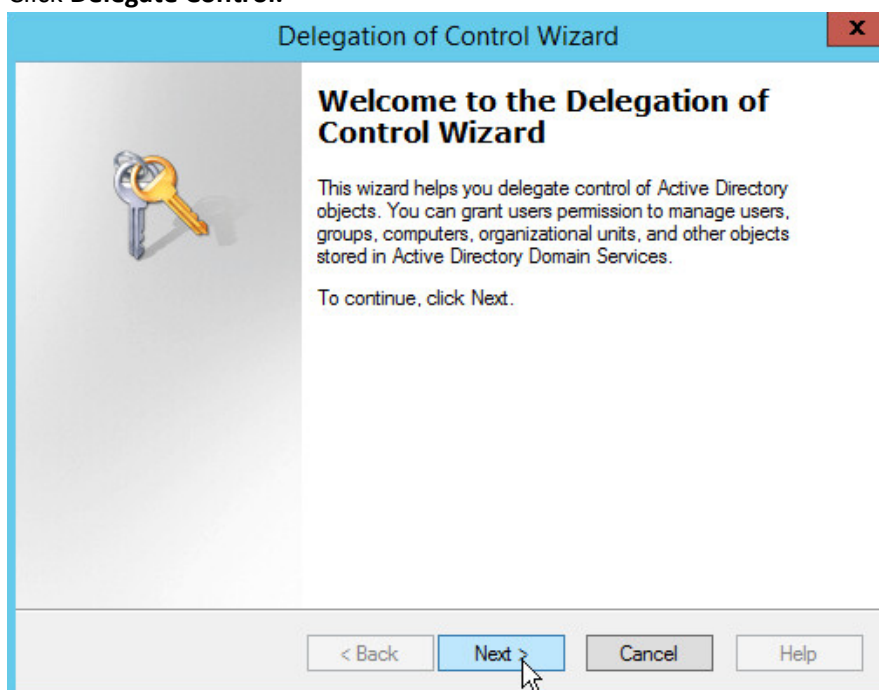
1. Open the **Start** menu.
2. Enter **dca.msc**, and run the program.



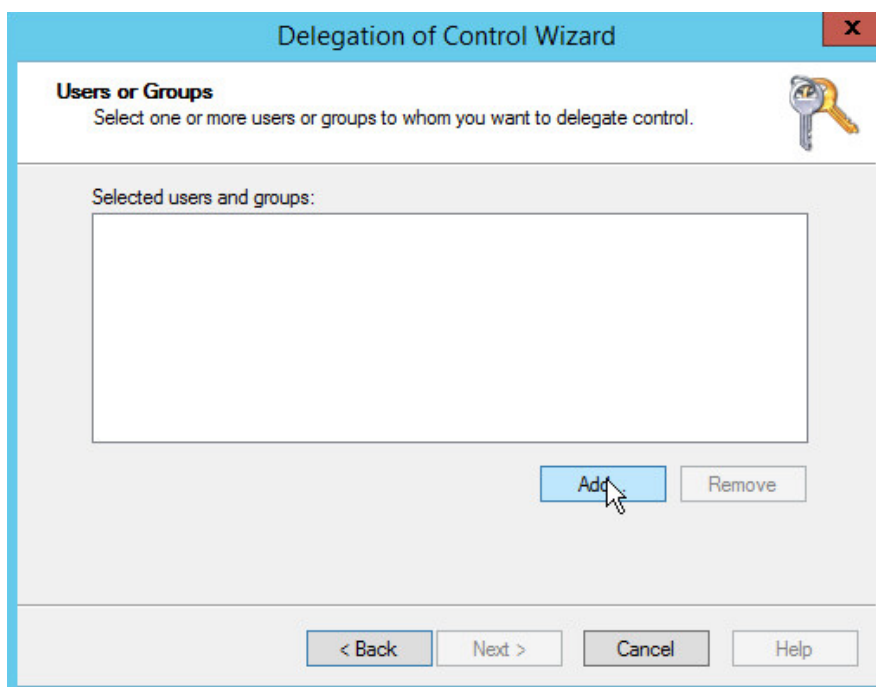
3. Right-click on **Users** in the left panel.



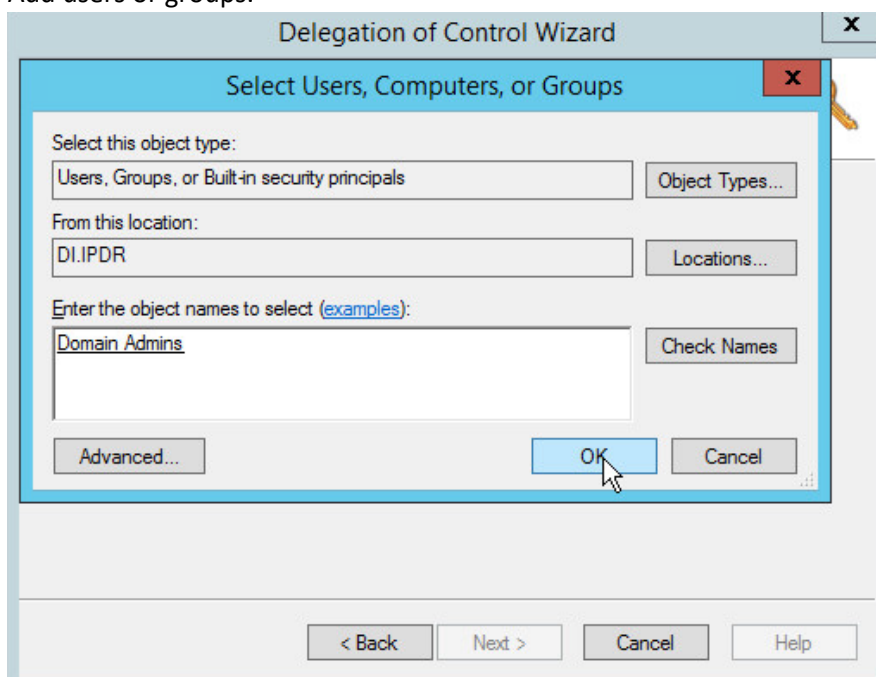
4. Click **Delegate Control**.



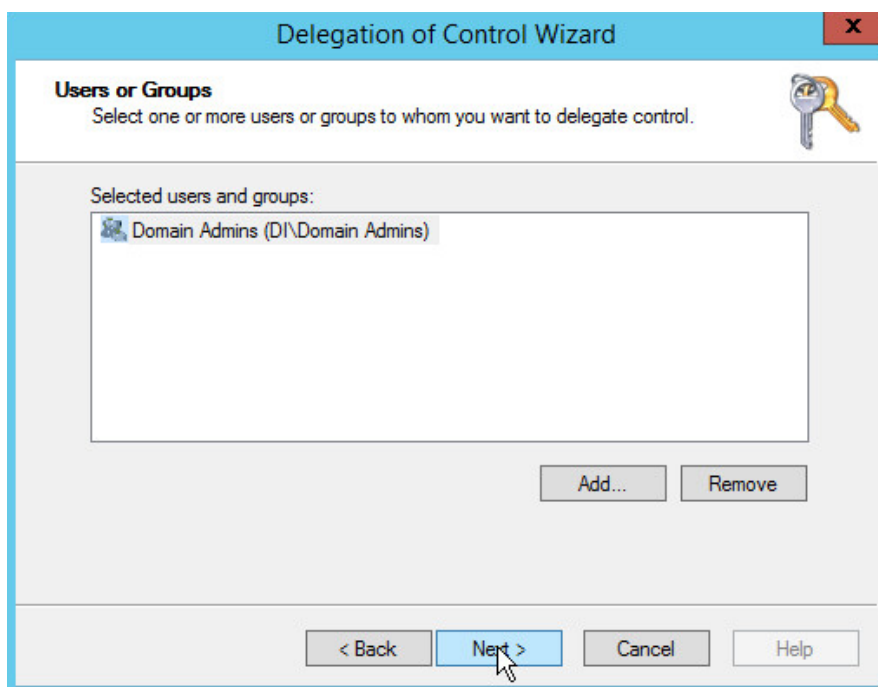
5. Click **Next**.



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

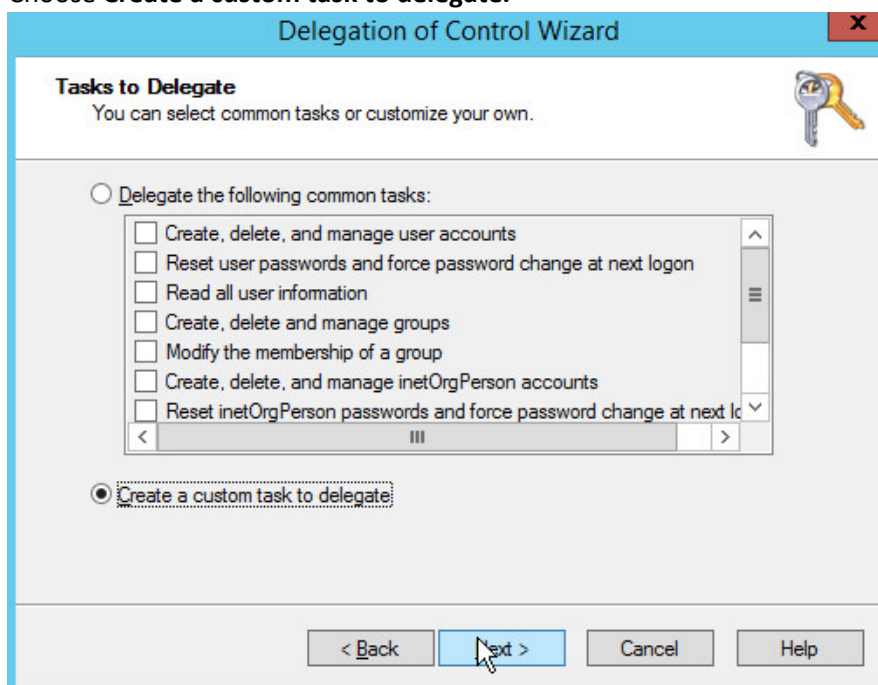


8. Click **OK**.



9. Click **Next**.

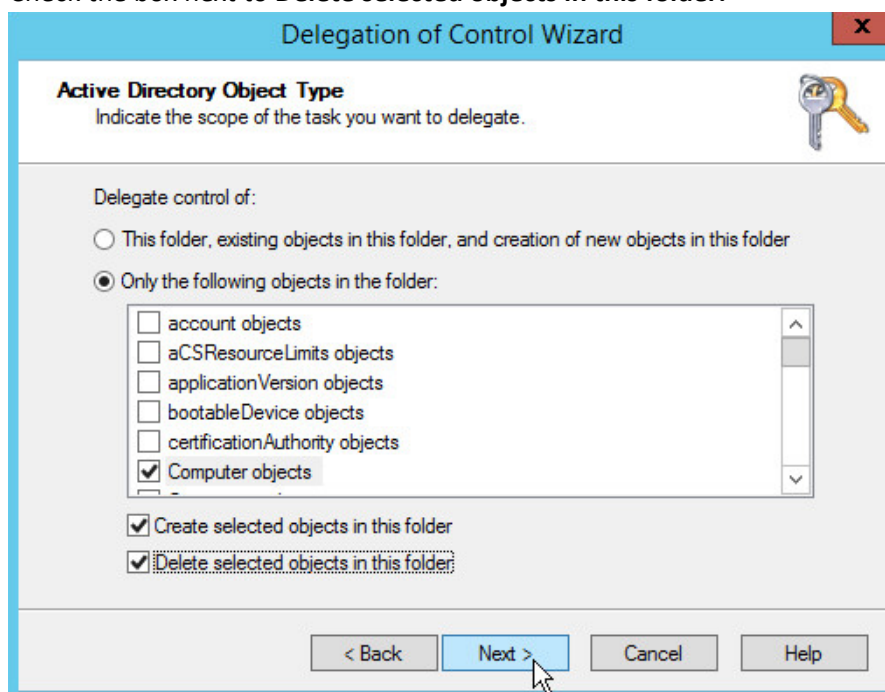
10. Choose **Create a custom task to delegate**.



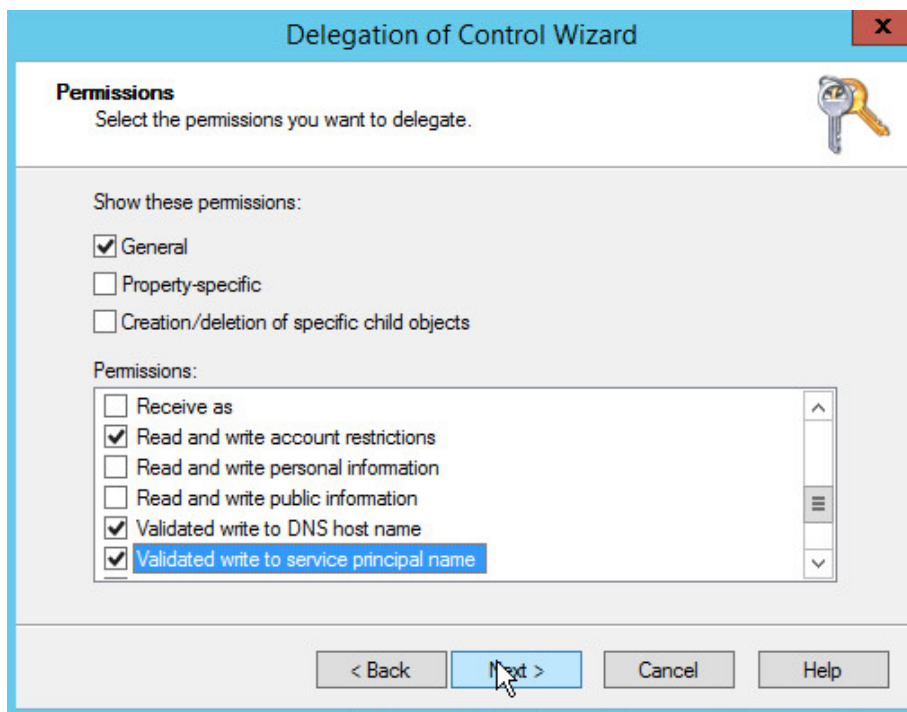
11. Click **Next**.

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**.



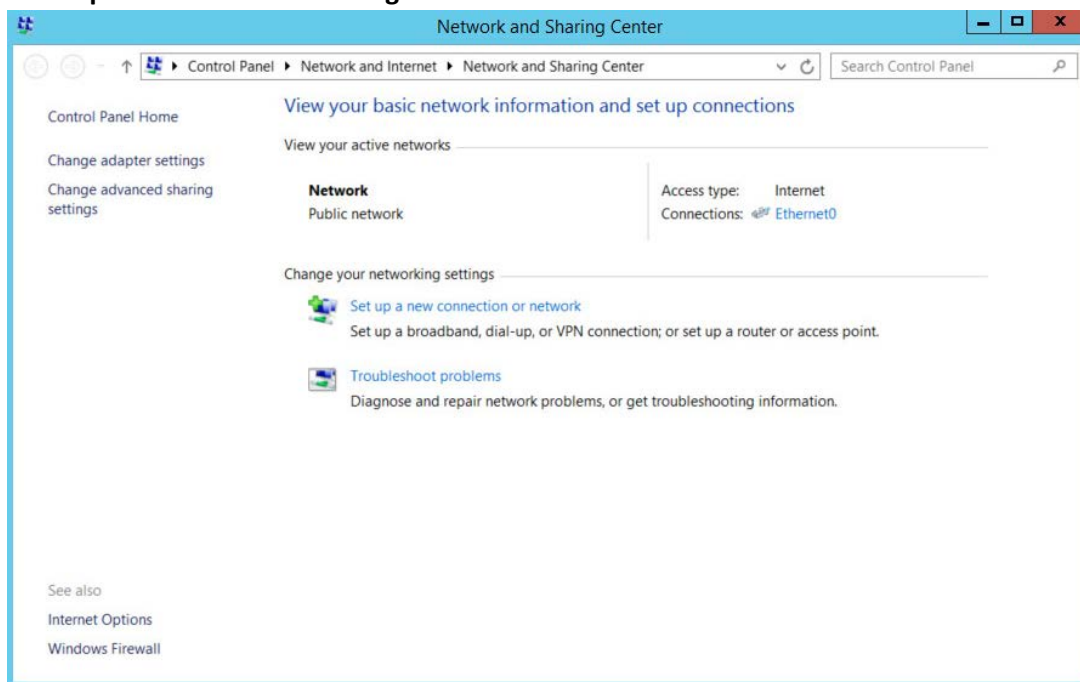
18. Click **Next**.



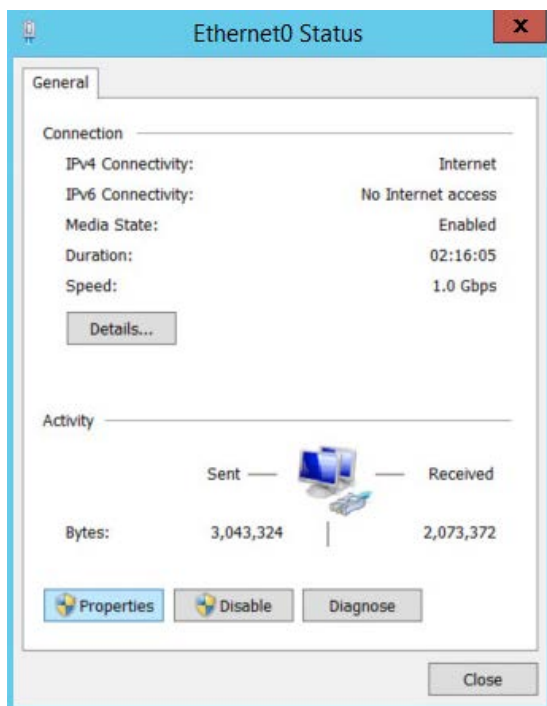
19. Click **Finish**.

2.1.4 Add Machines to the Domain

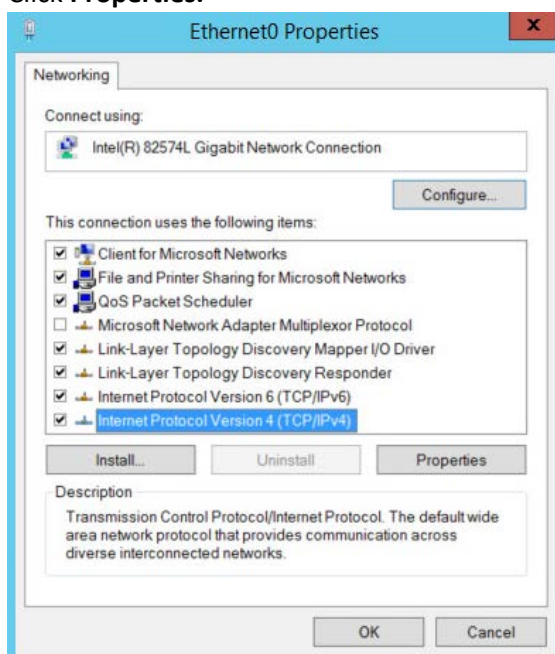
1. Right-click the network icon in the task bar, on a computer that you wish to add to the domain.
2. Click **Open Network and Sharing Center**.



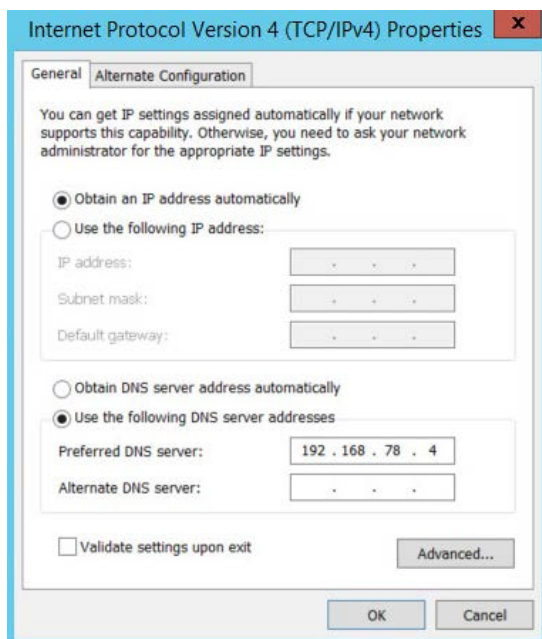
3. Click the name of the internet adapter.



4. Click **Properties**.

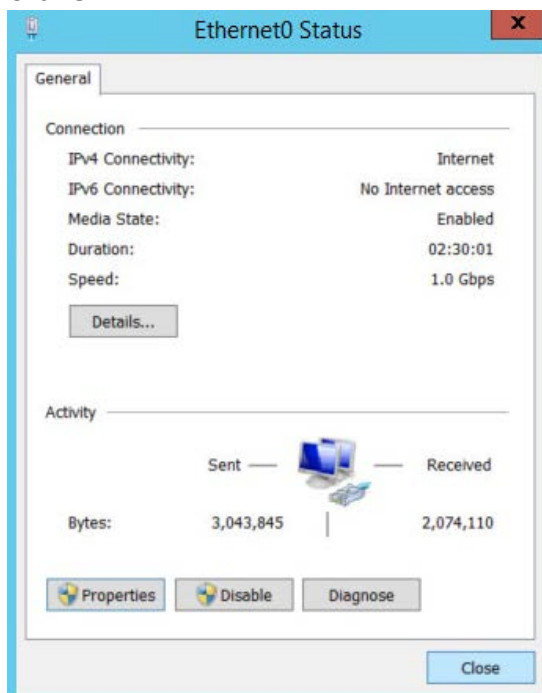


5. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
6. Select **Use the following DNS server addresses**.
7. Enter the **IP address** of the DNS server.



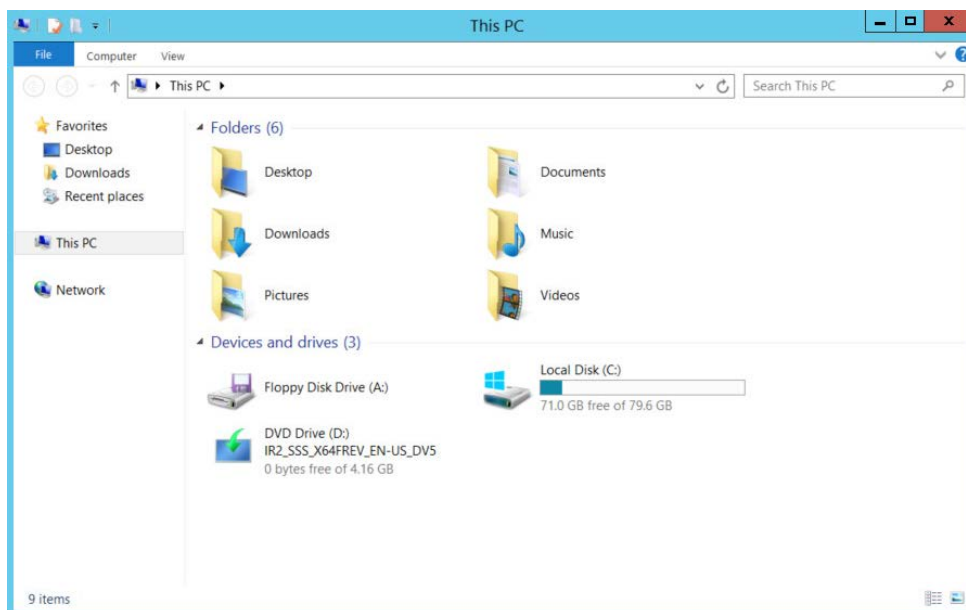
8. Click **OK**.

9. Click **OK**.

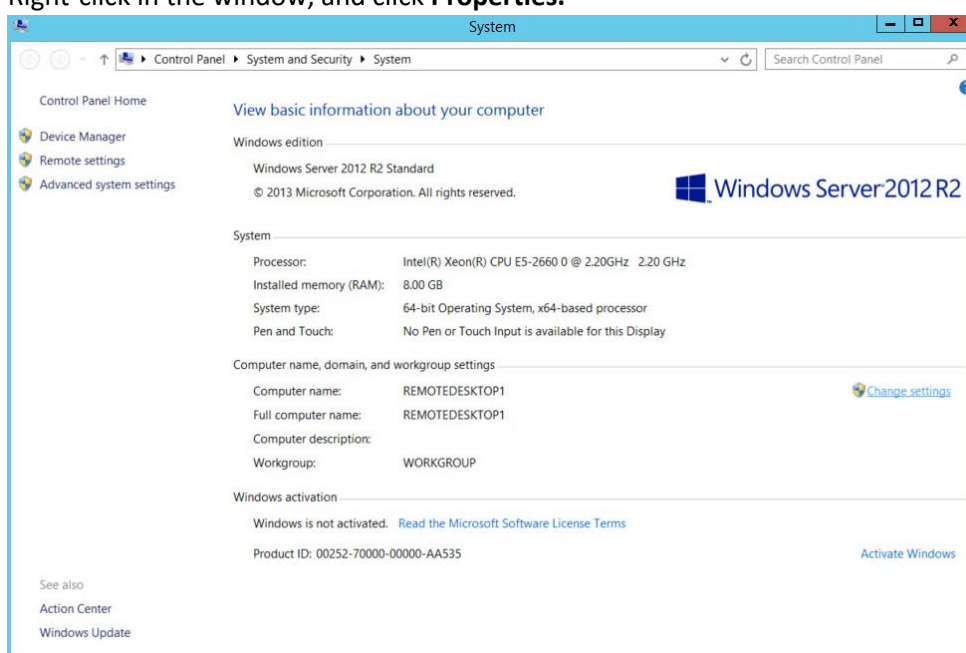


10. Click **Close**.

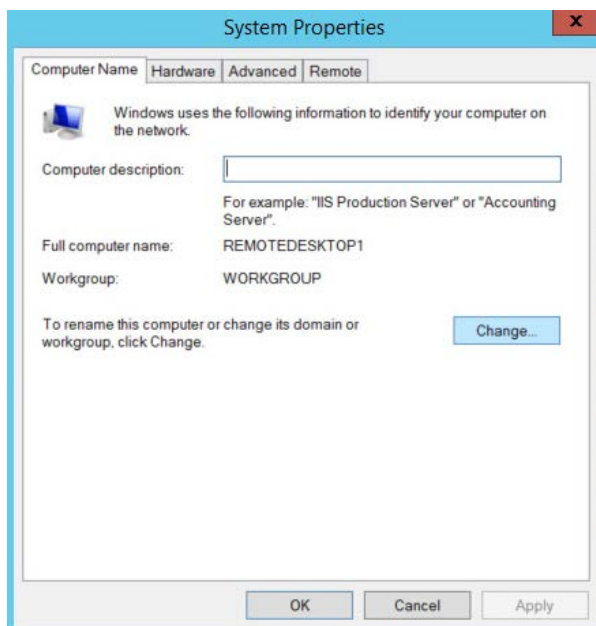
11. Navigate to **This PC**.



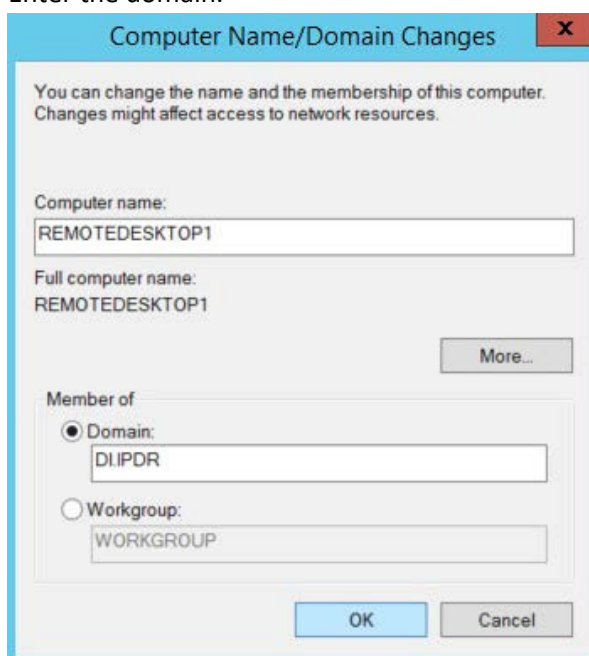
12. Right-click in the window, and click **Properties**.



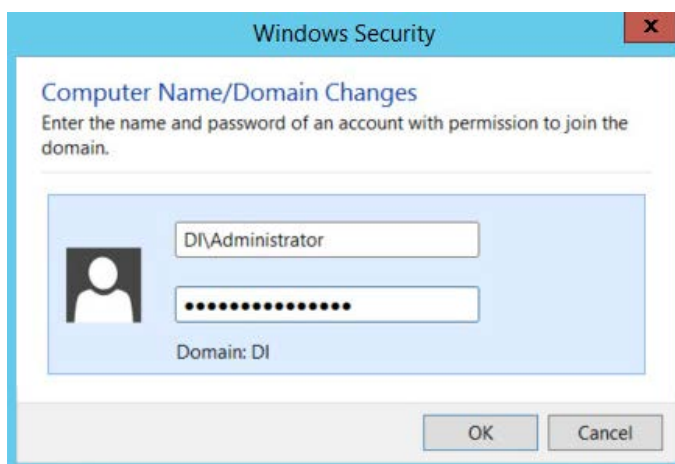
13. Click **Change Settings**.



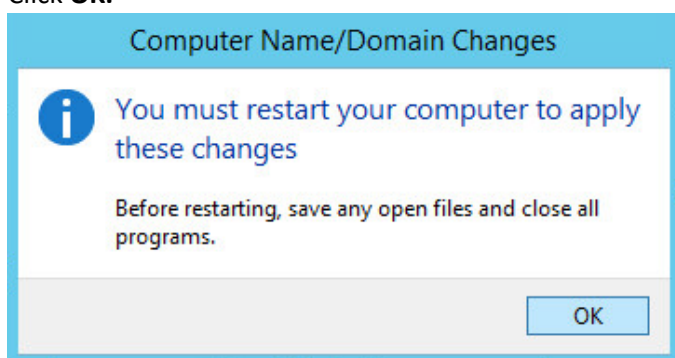
14. Click **Change**.
15. Select **Domain**.
16. Enter the domain.



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



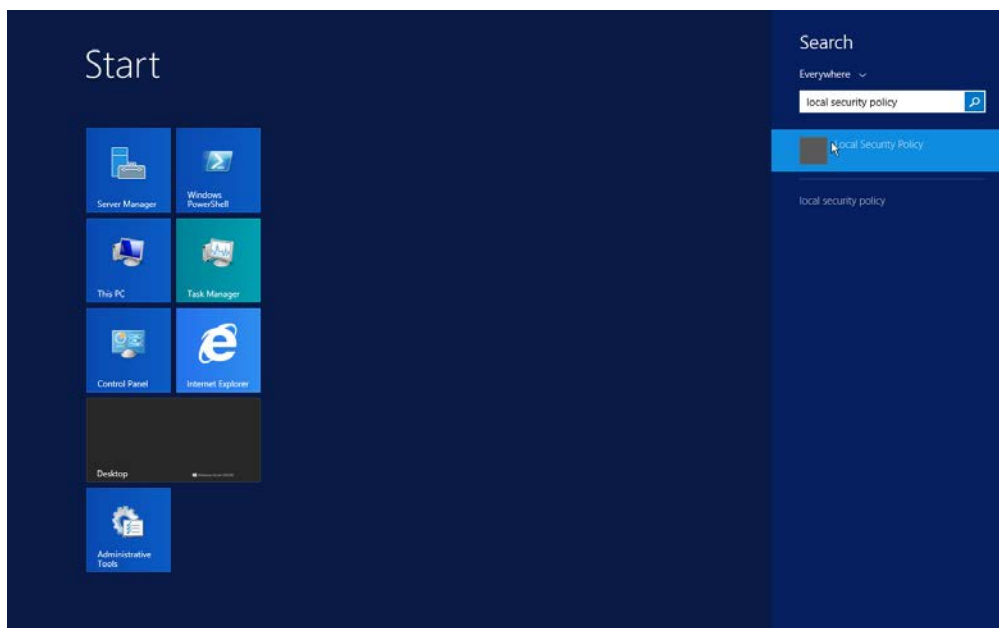
19. Click **OK**.



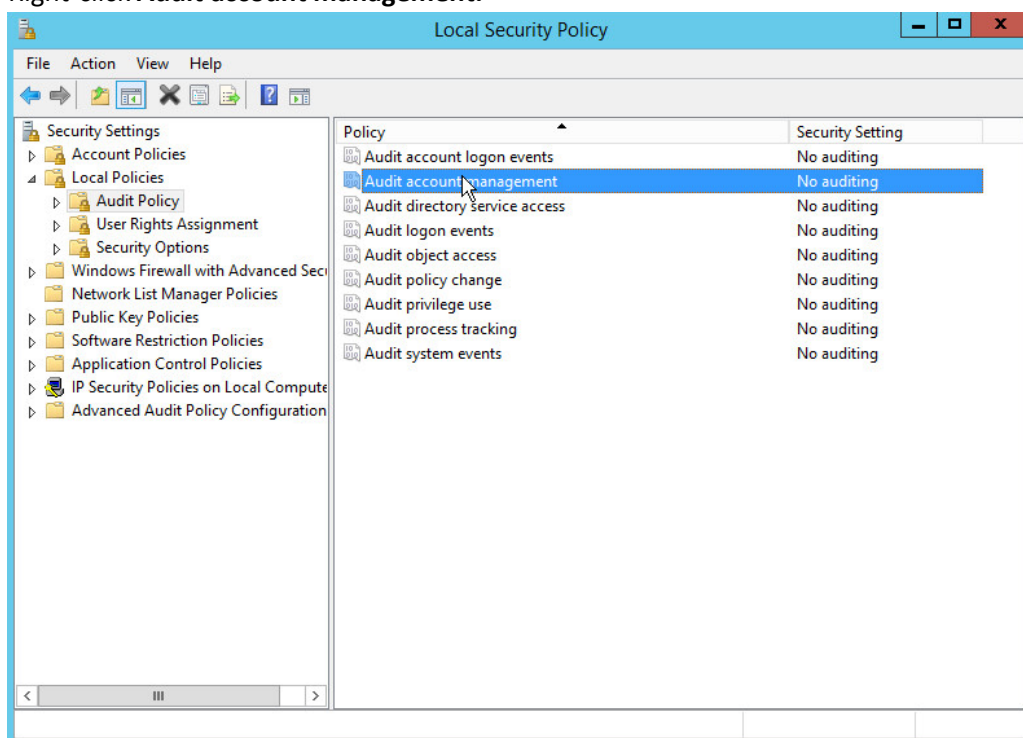
20. Click **OK** when prompted to restart the computer.

2.1.5 Configure Active Directory to Audit Account Activity

1. Open the **Start** Menu.

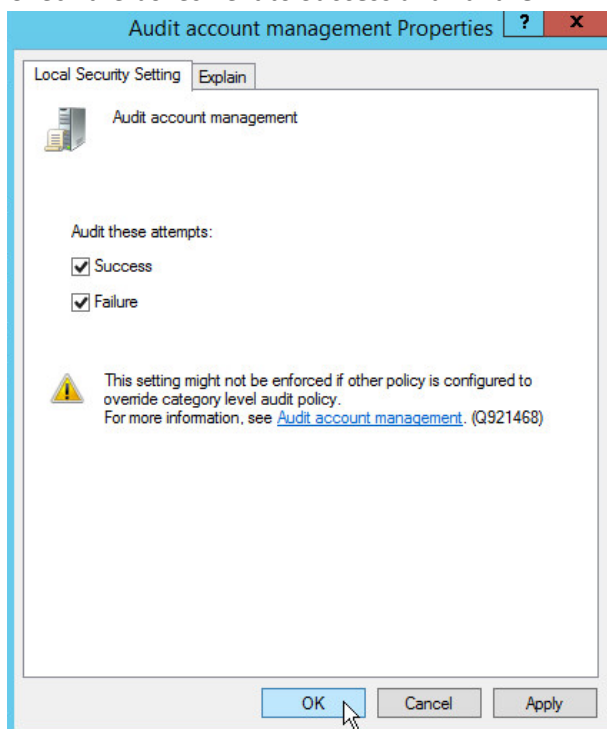


2. Enter Local Security Policy in the search bar, and open the program.
3. Navigate to **Local Policies > Audit Policy**.
4. Right-click **Audit account management**.



5. Click **Properties**.

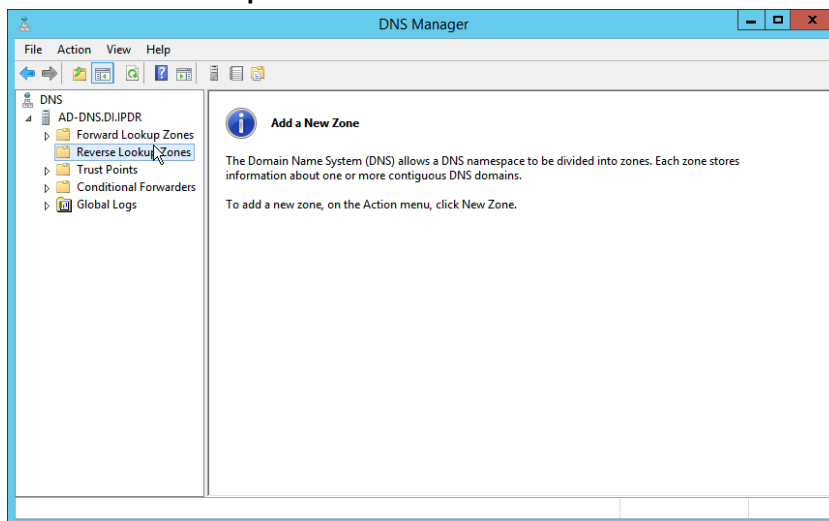
6. Check the boxes next to **Success** and **Failure**.



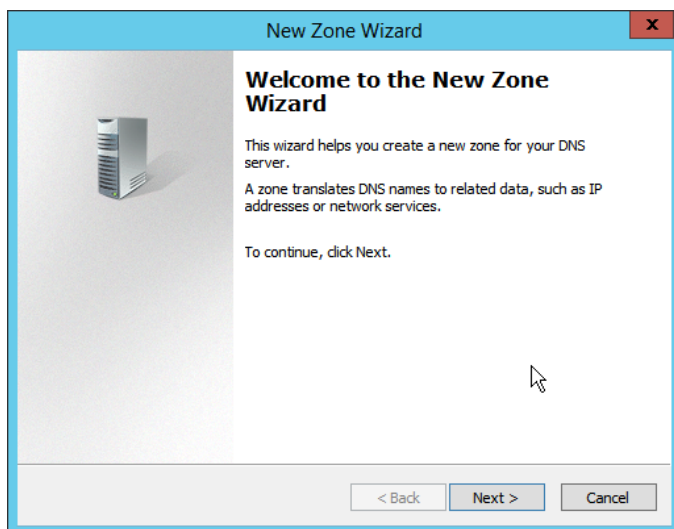
7. Click **OK**.

2.1.6 Configure Reverse Lookup Zones

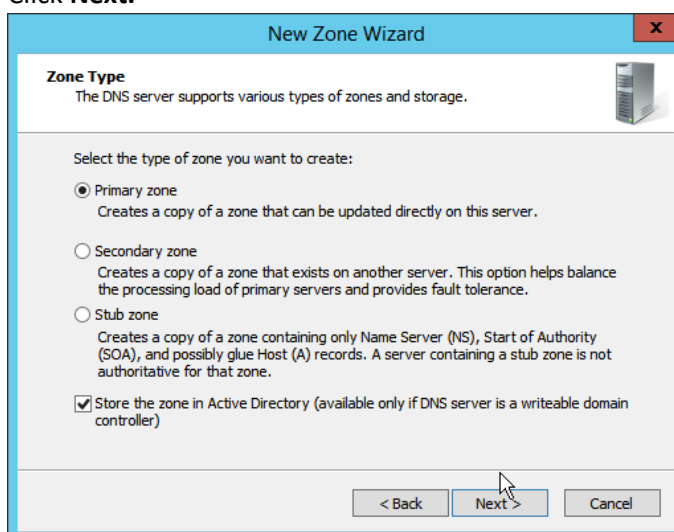
1. Open **DNS Manager** by right-clicking the DNS server in **Server Manager**.
2. Click **Reverse Lookup Zones**.



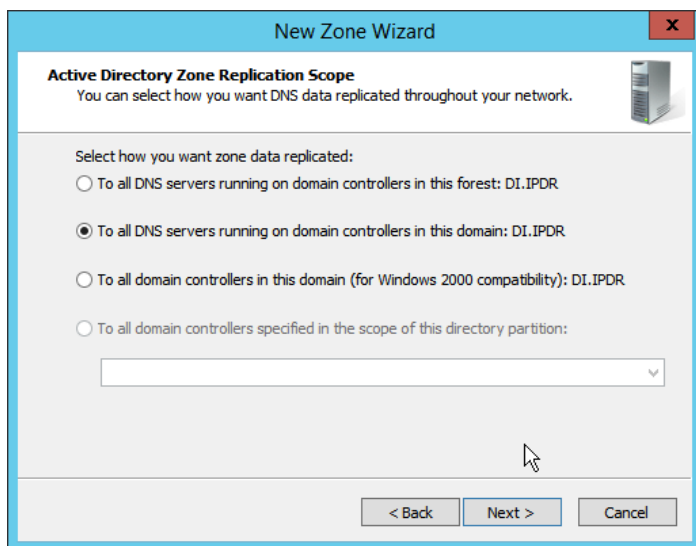
3. Click **Action > New Zone**.



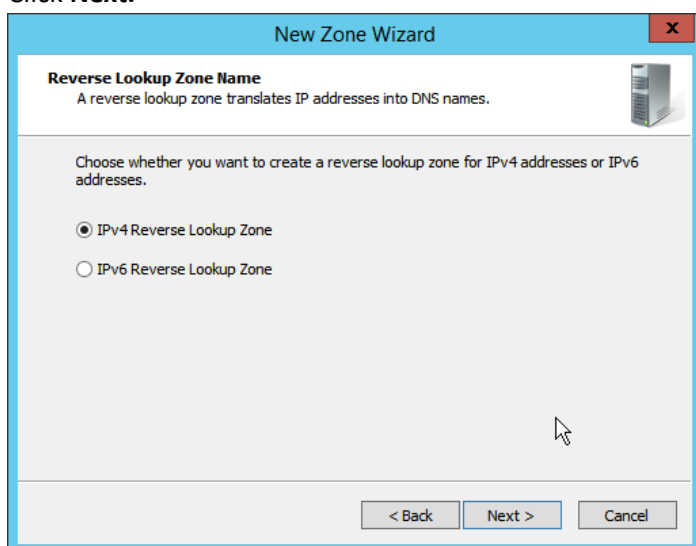
4. Click **Next**.



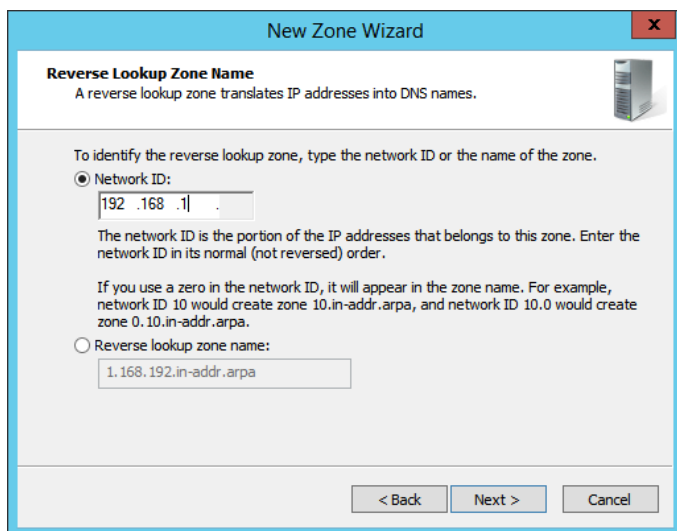
5. Click **Next**.



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).



New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:

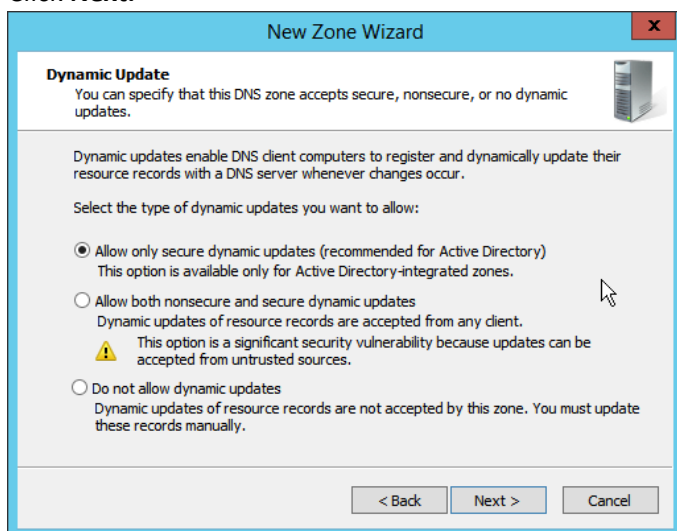
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:

< Back Next > Cancel

9. Click **Next**.



New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

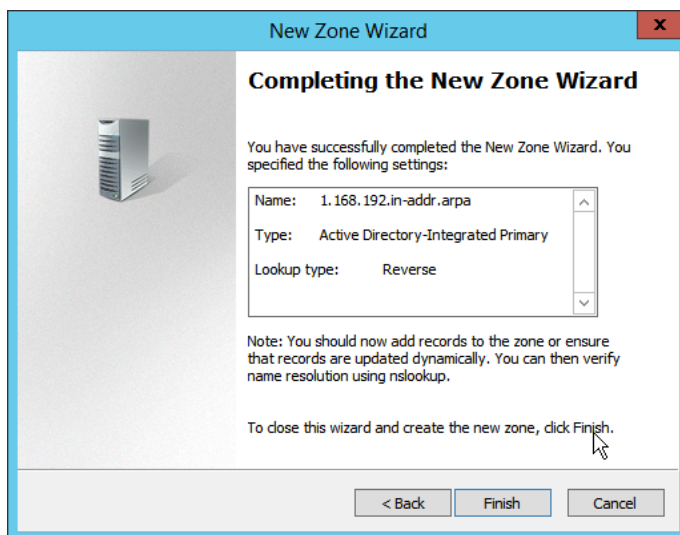
☒ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

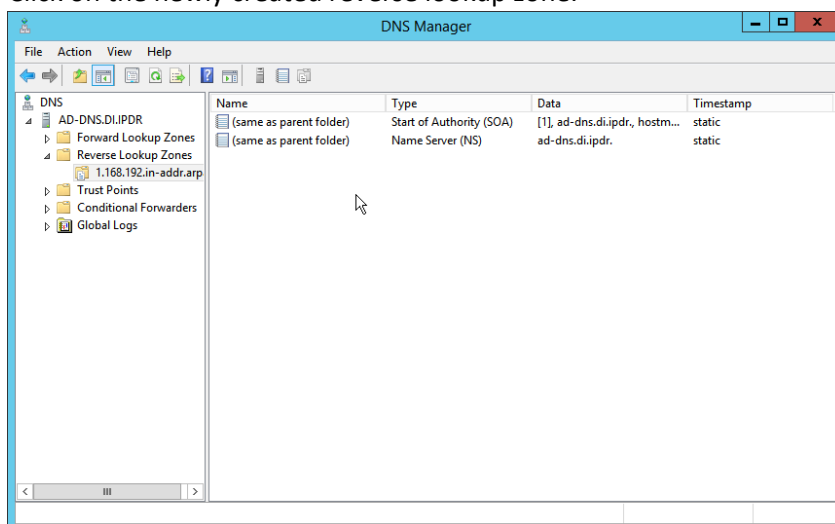
☐ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

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.

New Resource Record

Pointer (PTR)

Host IP Address:
192.168.1.12

Fully qualified domain name (FQDN):
12.1.168.192.in-addr.arpa

Host name:
ad-dns.di.ipdr Browse...

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel

16. Click **OK**.

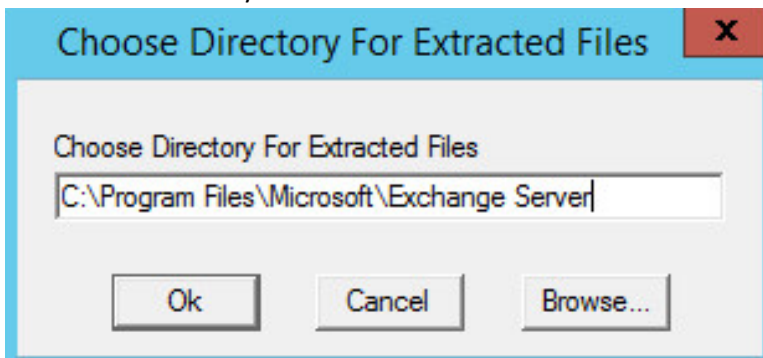
Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1] ad-dns.di.ipdr, hostm...	static
(same as parent folder)	Name Server (NS)	ad-dns.di.ipdr.	static
192.168.1.12	Pointer (PTR)	ad-dns.di.ipdr	

2.2 Microsoft Exchange Server

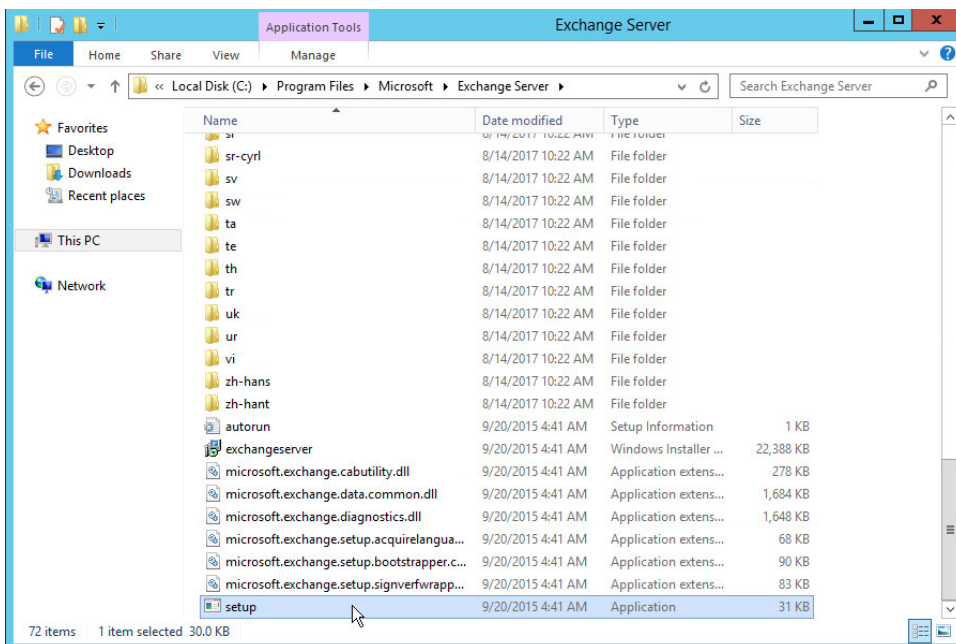
As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

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.

Check for Updates?

You can have Setup download Exchange Server 2016 updates from the Internet before you install Exchange. If updates are available, they'll be downloaded and used by Setup. By downloading updates now, you'll have the latest security and product updates. If you don't want to check for updates right now, or if you don't have access to the Internet, skip this step. If you skip this step, be sure to download and install any available updates after you've completed Setup.

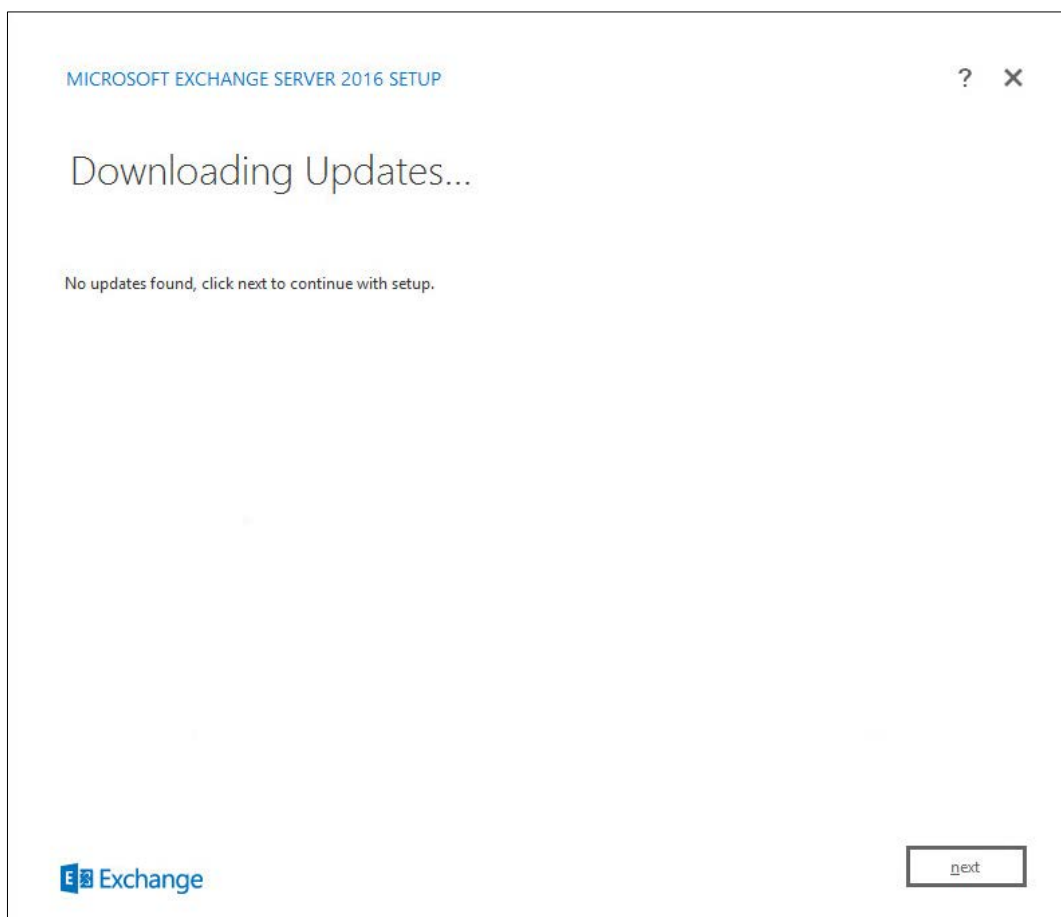
Select one of the following options:

- ☒ Connect to the Internet and check for updates
- ☐ Don't check for updates right now



next

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



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

Introduction

Welcome to Microsoft Exchange Server 2016!

Exchange Server is designed to help you increase user productivity, keep your data safe, and provide you with the control you need. You can tailor your solution to your unique needs with flexible deployment options, including hybrid deployments that enable you to take advantage of both on-premises and online solutions. You can use compliance management features to protect against the loss of sensitive information and help with internal and regulatory compliance efforts. And, of course, your users will be able to access their email, calendar, and voice mail on virtually any device and from any location. This wizard will guide you through the installation of Exchange Server 2016.

Plan your Exchange Server 2016 deployment:

[Read about Exchange Server 2016](#)

[Read about supported languages](#)

[Use the Exchange Server Deployment Assistant](#)



next

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

License Agreement

Please read and accept the Exchange Server 2016 license agreement.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT EXCHANGE SERVER 2016 STANDARD, ENTERPRISE, TRIAL AND HYBRID

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

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

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

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or the Microsoft Store for more information about Microsoft's refund policy. See [https://aka.ms/MSRPRefundPolicy](#).

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

[next](#)

12. Click **Next**.

13. Click **Use Recommended Settings**.

Recommended Settings

☒ Use recommended settings

Exchange server will automatically check online for solutions when encountering errors and provide usage feedback to Microsoft to help improve future Exchange features.

☐ Don't use recommended settings

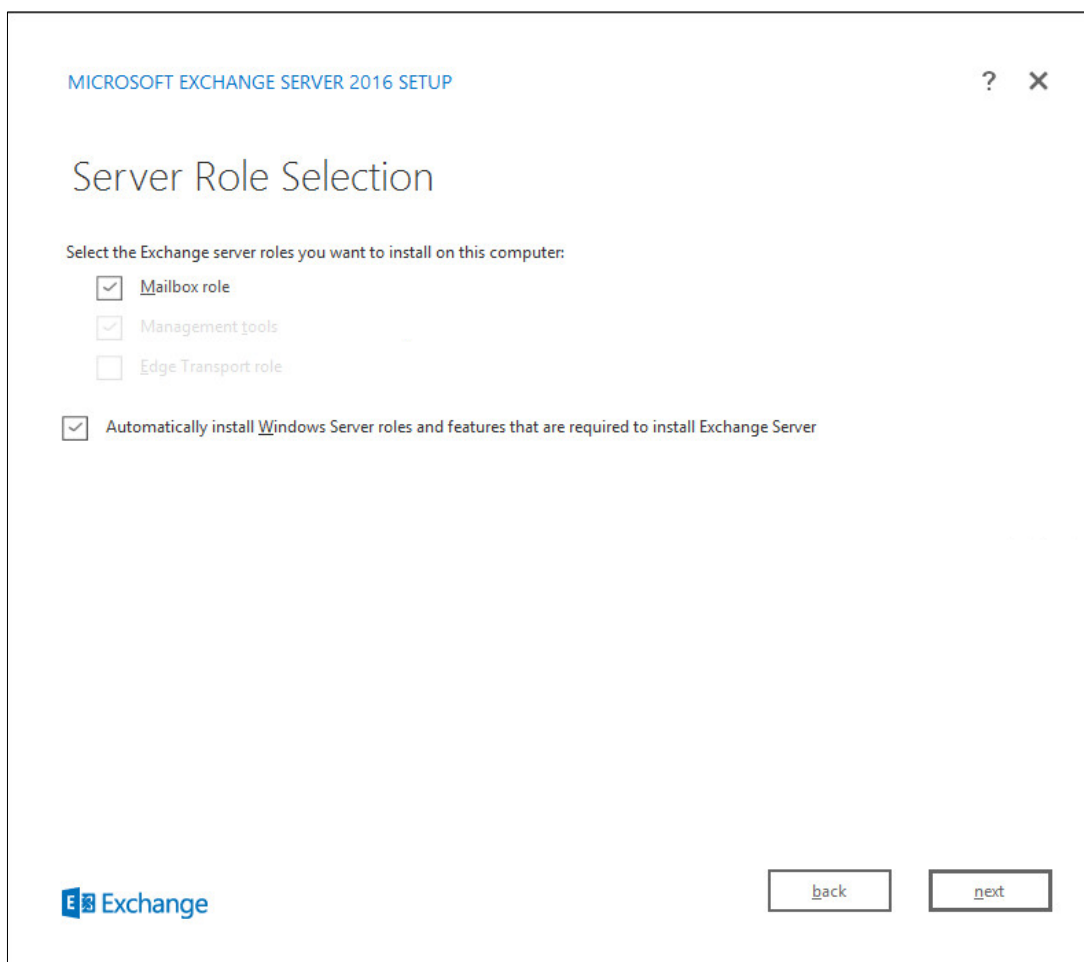
Manually configure these settings after installation is complete (see help for more information).

[Read more about providing usage feedback to Microsoft](#)

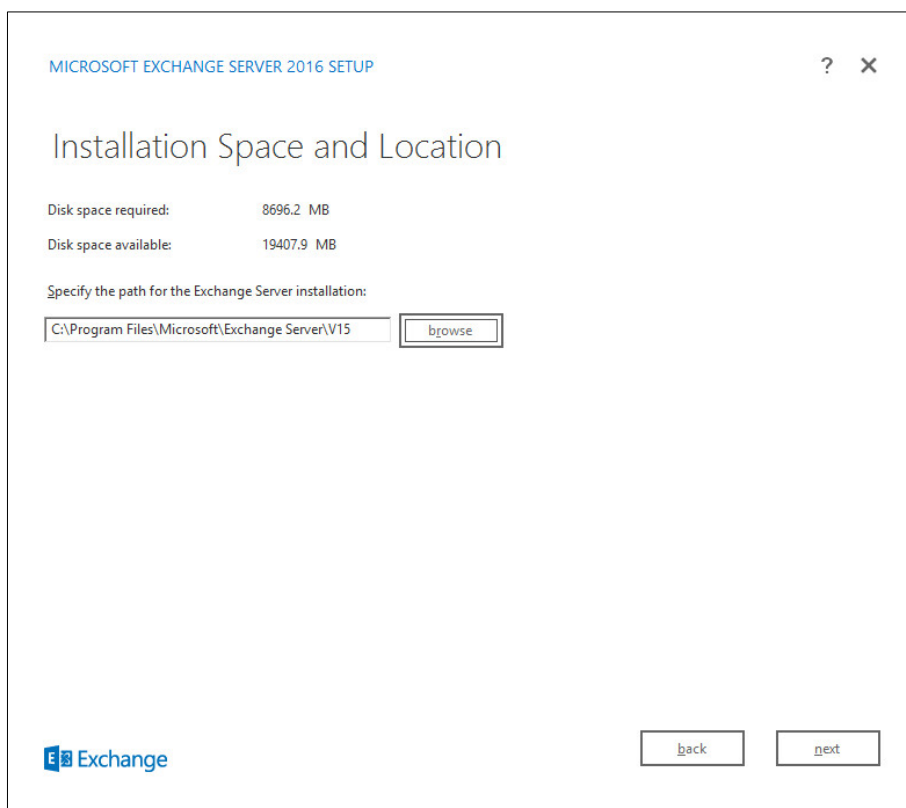
[Read more about checking for error solutions online](#)

[back](#)[next](#)

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.

Exchange Organization

Specify the name for this Exchange organization:

☐ Apply Active Directory split permissions security model to the Exchange organization

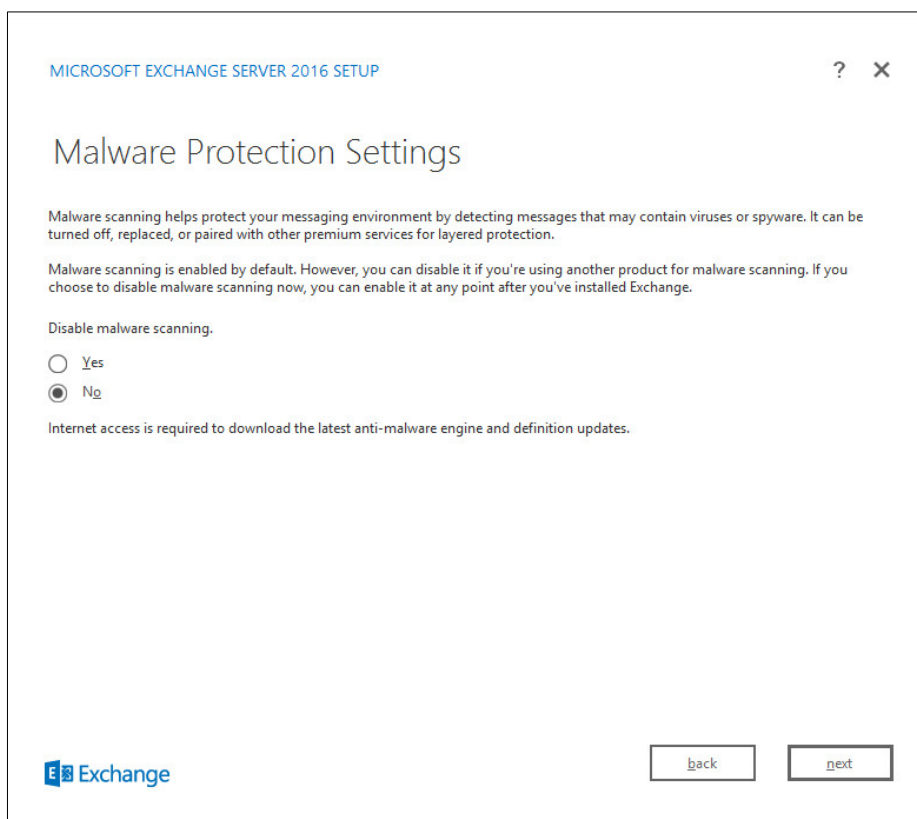
The Active Directory split permissions security model is typically used by large organizations that completely separate the responsibility for the management of Exchange and Active Directory among different groups of people. Applying this security model removes the ability for Exchange servers and administrators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

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

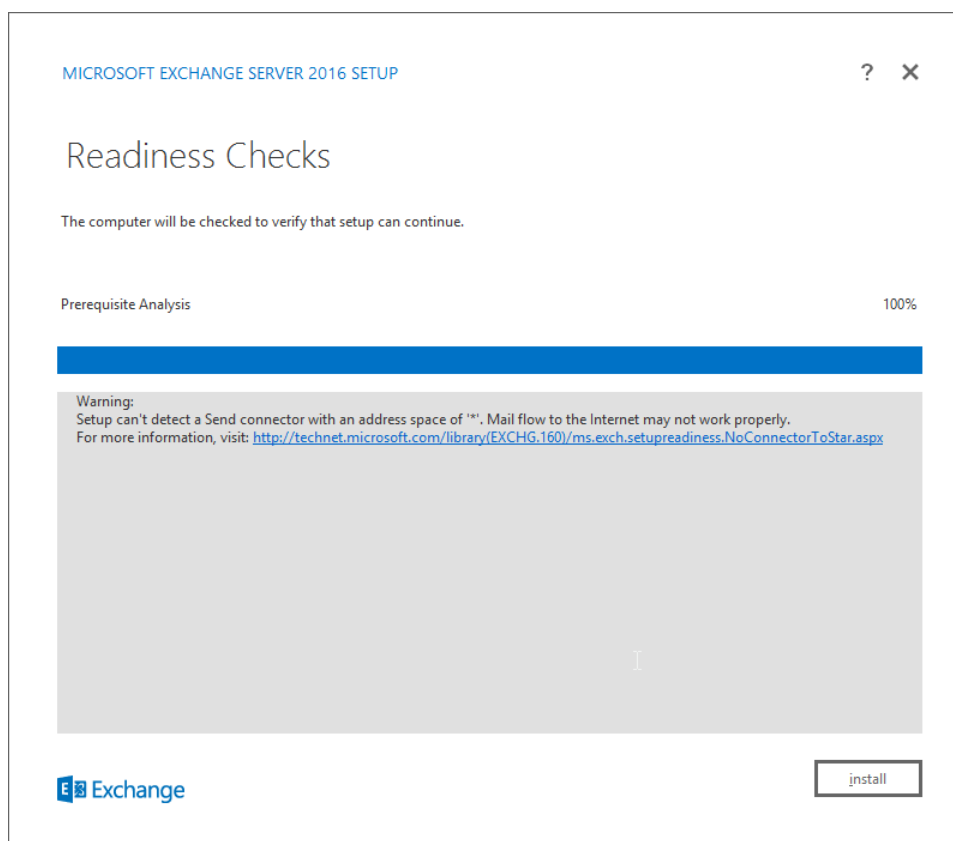
[back](#)[next](#)

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**.

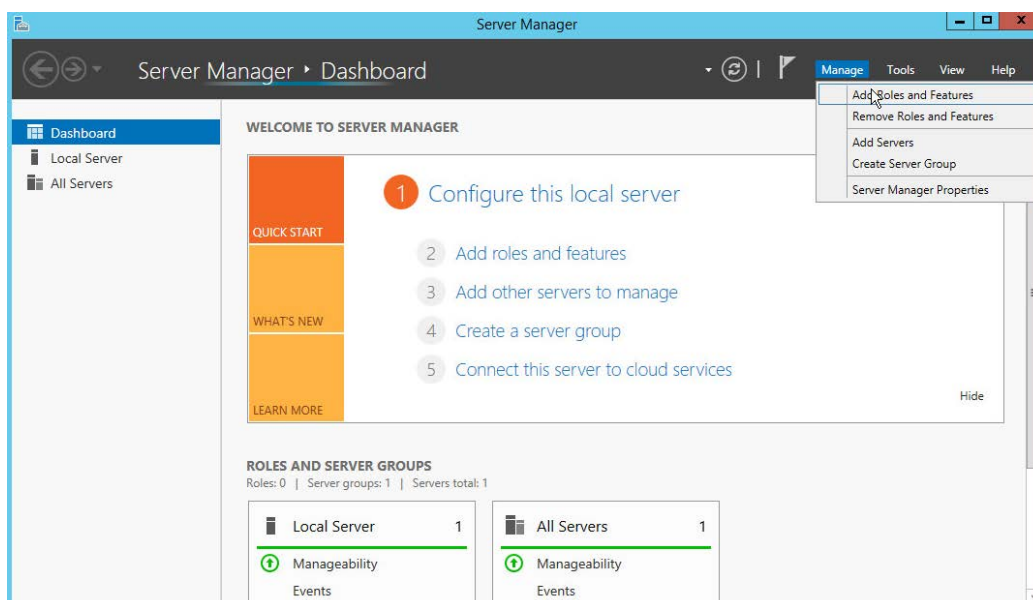
2.3 Windows Server Hyper-V Role

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.

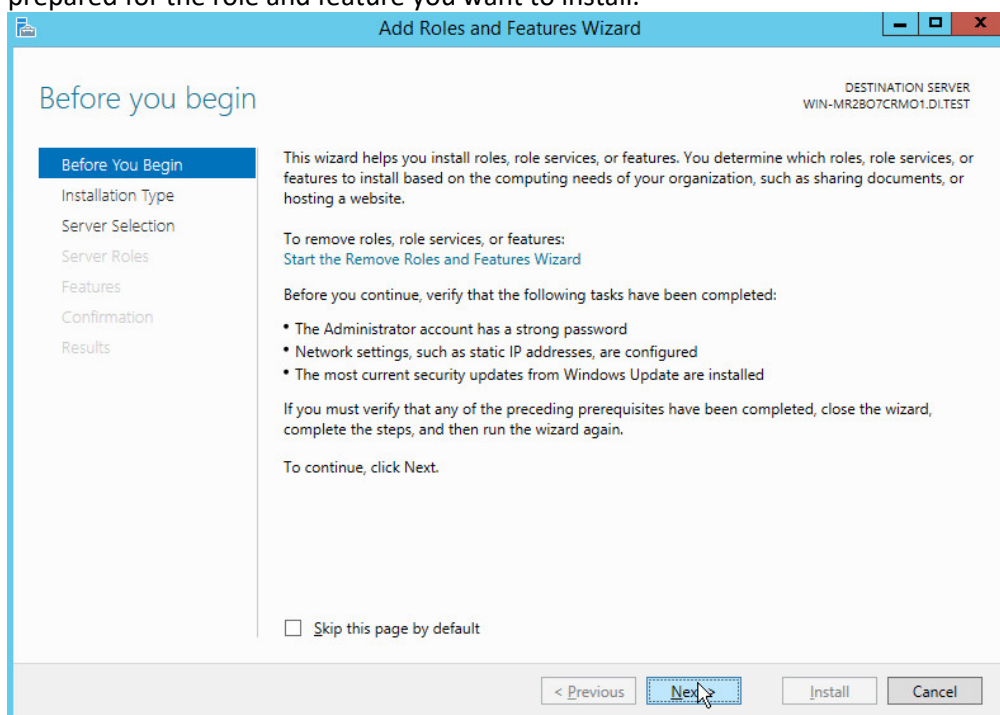
The instructions for enabling the Windows Server Hyper-V Role are retrieved from [https://technet.microsoft.com/en-us/library/hh846766\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx) and are replicated below for preservation and ease of use.

2.3.1 Production Installation

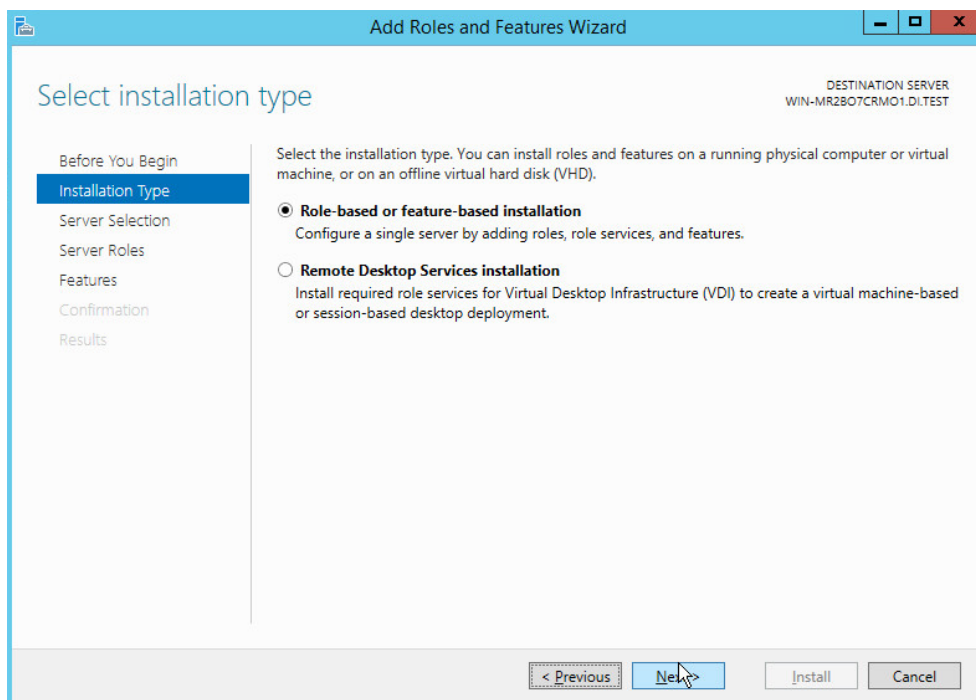
1. In **Server Manager**, on the **Manage** menu, click **Add Roles and Features**.



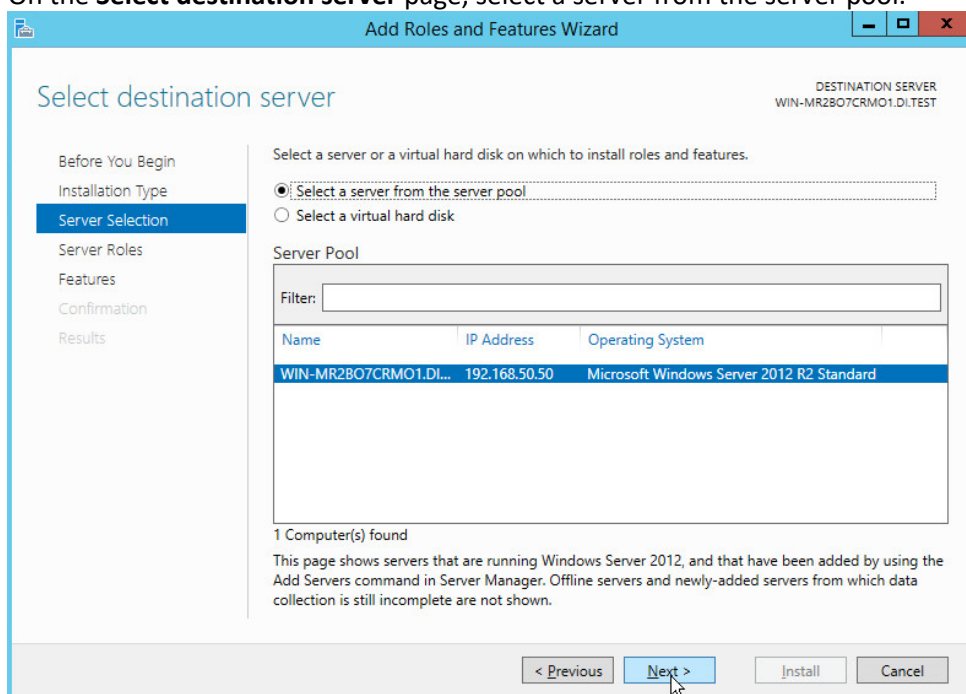
2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.



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

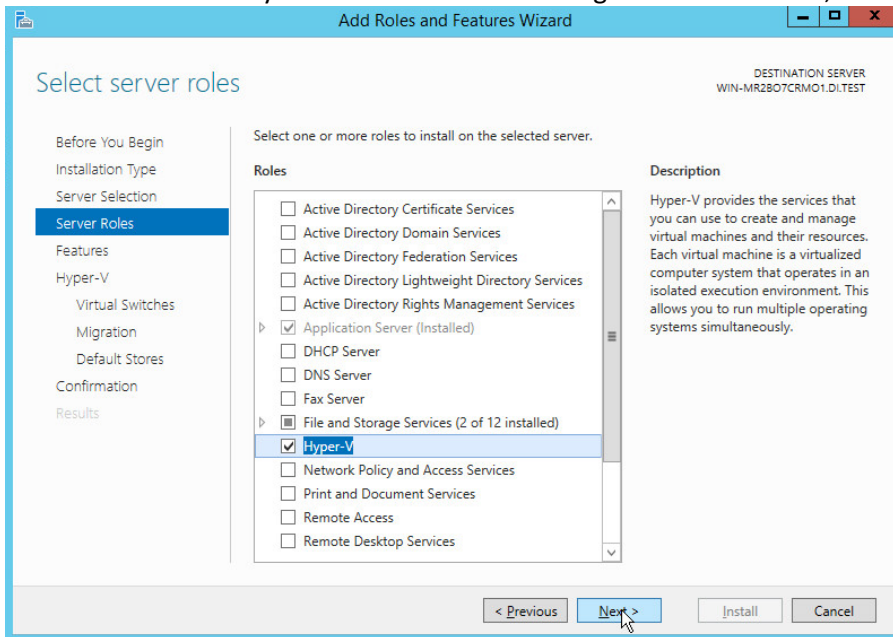


5. Click **Next**.
6. On the **Select destination server** page, select a server from the server pool.

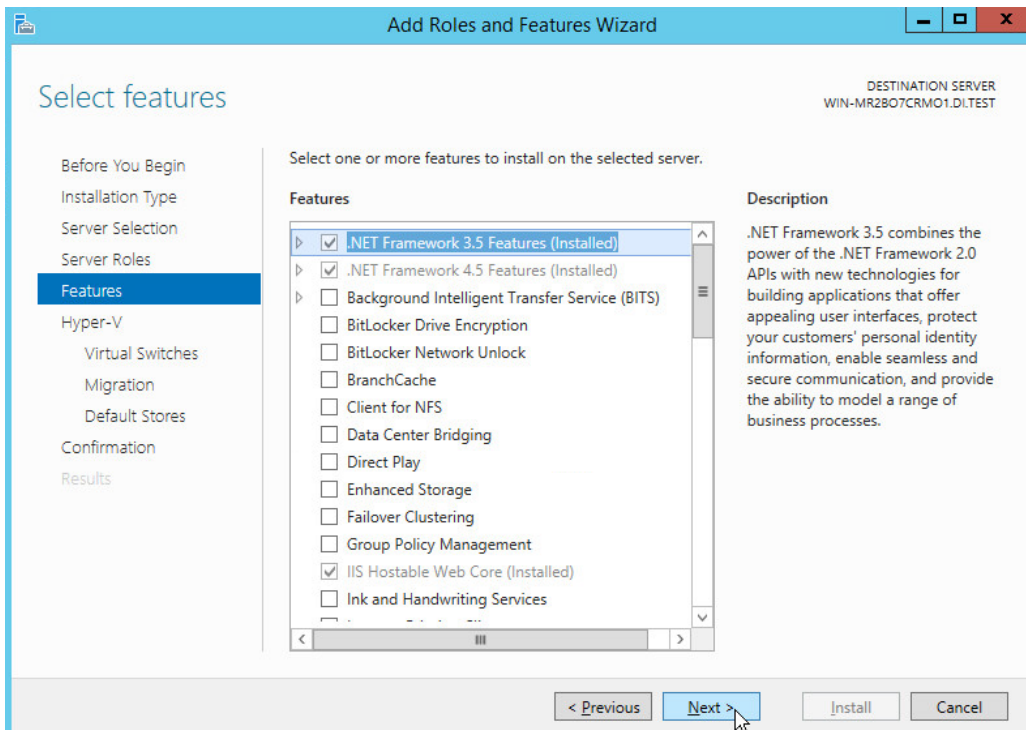


7. Click **Next**.
8. On the **Select server roles** page, select **Hyper-V**.

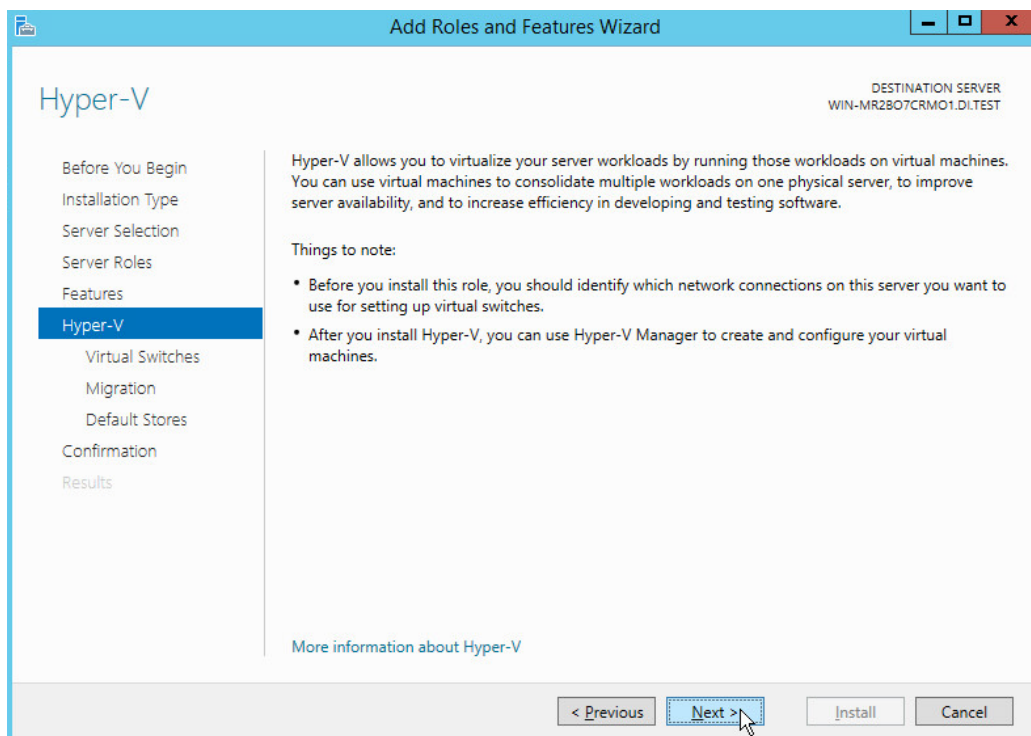
9. To add the tools that you use to create and manage virtual machines, click **Add Features**.



10. Click **Next**.

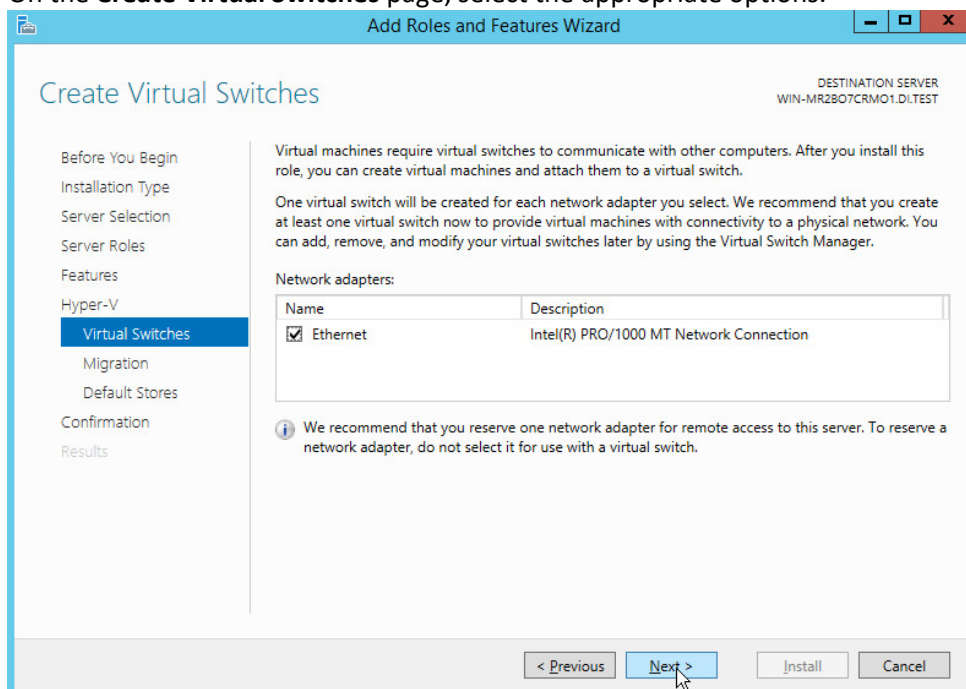


11. Click **Next**.



12. Click **Next**.

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



14. Click **Next**.

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

The screenshot shows the 'Virtual Machine Migration' page within the 'Add Roles and Features Wizard'. The left-hand navigation pane lists the following steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Hyper-V', 'Virtual Switches', 'Migration' (which is highlighted in blue), 'Default Stores', 'Confirmation', and 'Results'. The main content area is titled 'Virtual Machine Migration' and includes the text: 'Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migrations. If you want to dedicate specific networks for live migration, use Hyper-V settings after you install the role.' Below this text is a checkbox labeled 'Allow this server to send and receive live migrations of virtual machines', which is currently unchecked. Underneath the checkbox is a section titled 'Authentication protocol' with the instruction: 'Select the protocol you want to use to authenticate live migrations.' There are two radio button options: 'Use Credential Security Support Provider (CredSSP)' (which is selected) and 'Use Kerberos'. The 'CredSSP' option has a sub-note: 'This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.' The 'Kerberos' option has a sub-note: 'This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.' At the bottom of the main content area, there is a yellow warning icon and a message: 'If this server will be part of a cluster, do not enable migration now. Instead, you will configure the server for live migration, including specifying networks, when you create the cluster.' The bottom of the wizard window contains four buttons: '< Previous', 'Next >' (which is highlighted with a mouse cursor), 'Install', and 'Cancel'. The top right corner of the window indicates the 'DESTINATION SERVER' as 'WIN-MR2B07CRMO1.D1.TEST'.

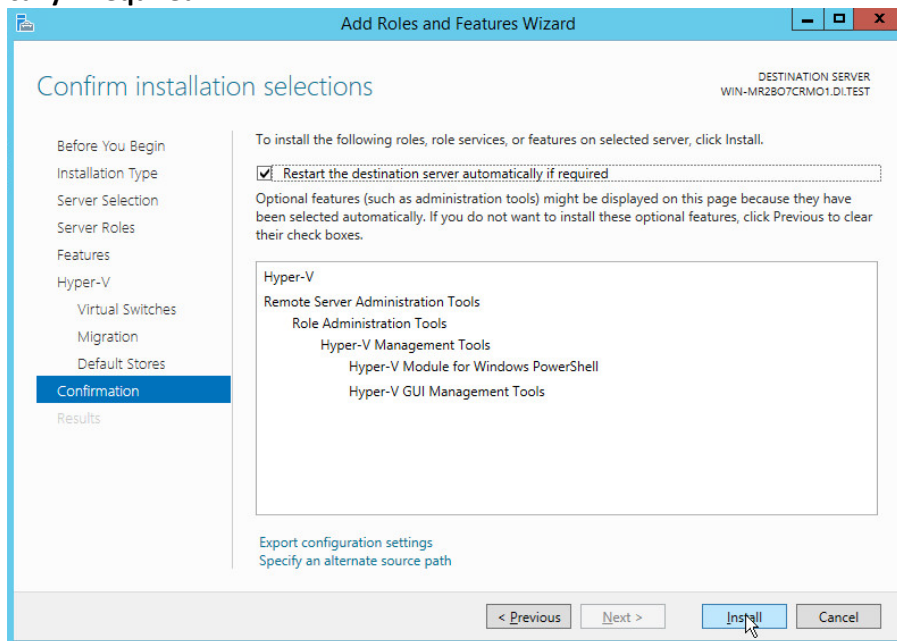
16. Click **Next**.

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

The screenshot shows the 'Default Stores' page within the 'Add Roles and Features Wizard'. The left-hand navigation pane is identical to the previous screenshot, with 'Default Stores' now highlighted in blue. The main content area is titled 'Default Stores' and includes the text: 'Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.' Below this text are two sections. The first section is 'Default location for virtual hard disk files:' followed by a text box containing 'C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks' and a 'Browse...' button. The second section is 'Default location for virtual machine configuration files:' followed by a text box containing 'C:\ProgramData\Microsoft\Windows\Hyper-V' and a 'Browse...' button. The bottom of the wizard window contains the same four buttons as the previous screenshot: '< Previous', 'Next >' (highlighted with a mouse cursor), 'Install', and 'Cancel'. The top right corner of the window indicates the 'DESTINATION SERVER' as 'WIN-MR2B07CRMO1.D1.TEST'.

18. Click **Next**.

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



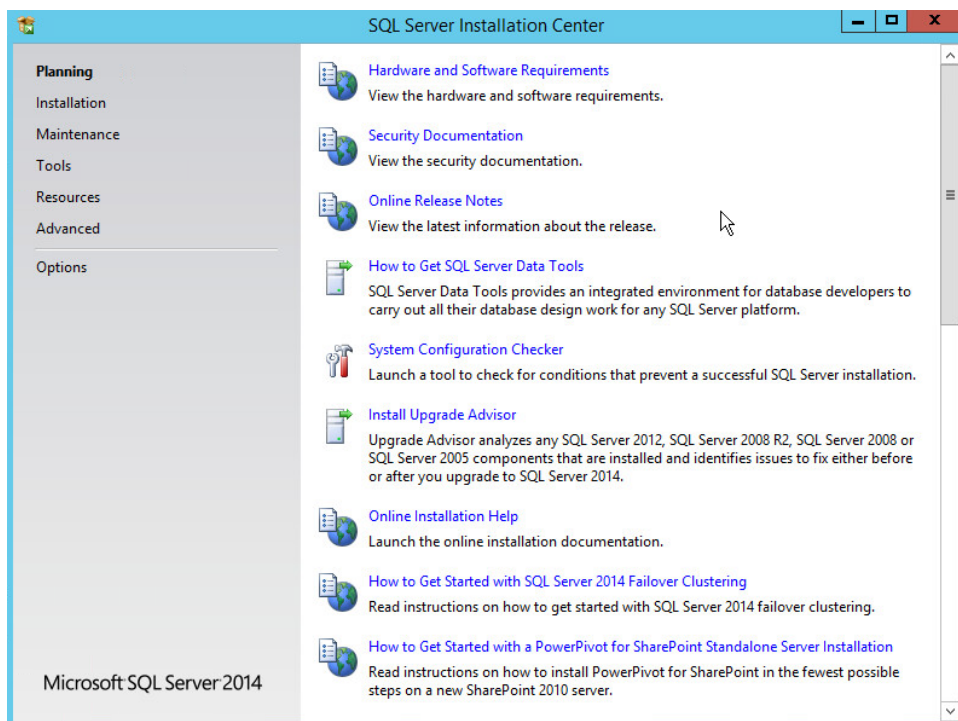
20. Click **Install**.
21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

2.4 MS SQL Server

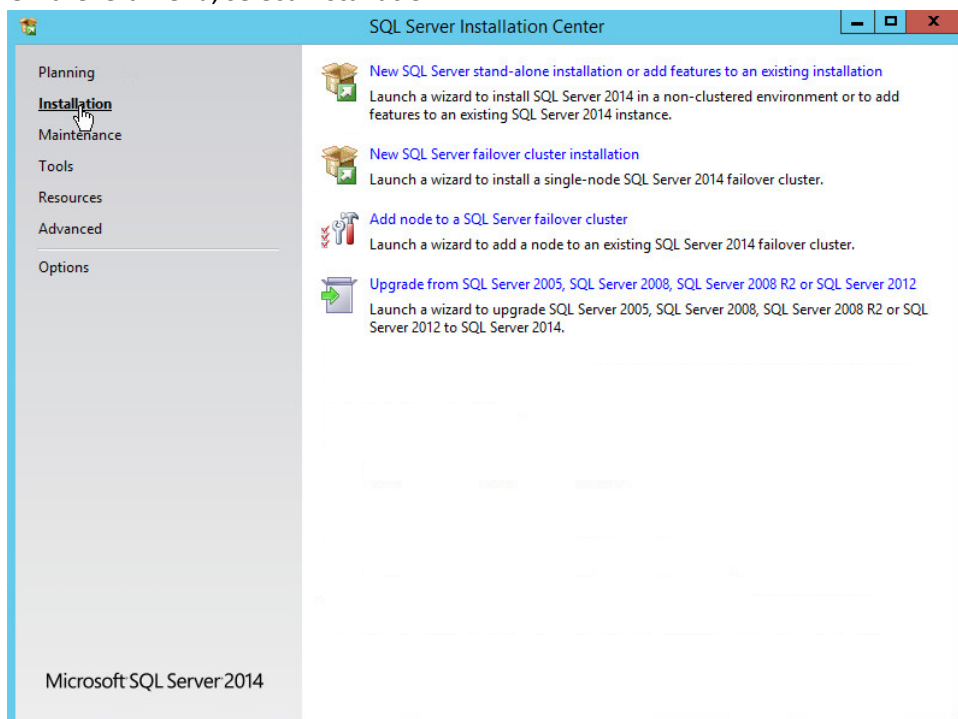
As part of both our enterprise emulation and data integrity solution, we include a Microsoft Structured Query Language (SQL) Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

2.4.1 Install and Configure MS SQL

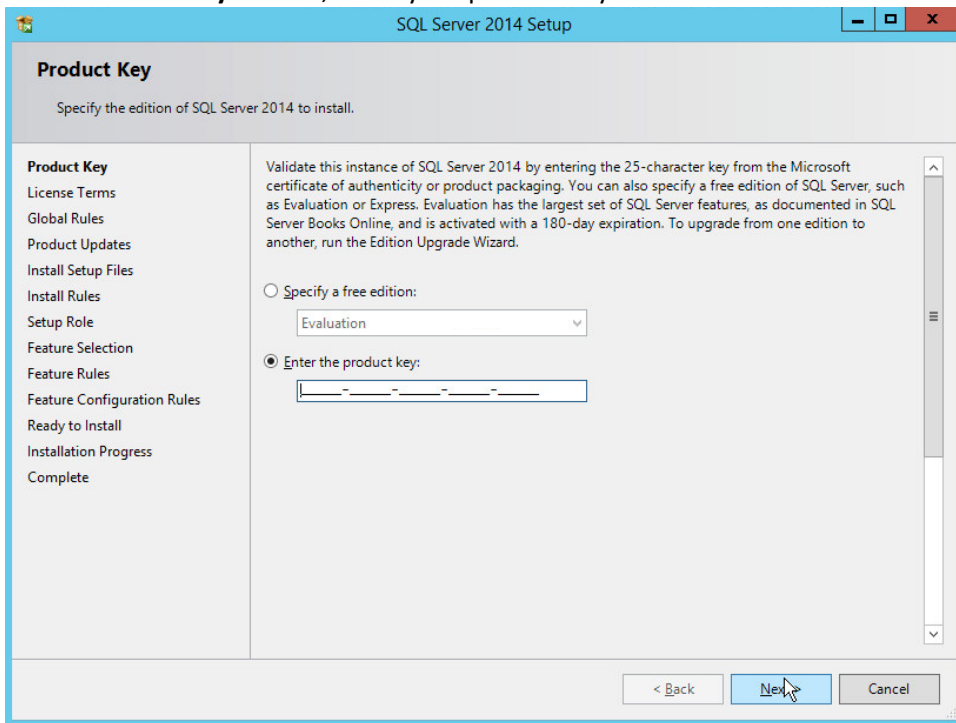
1. Acquire **SQL Server 2014 Installation Media**.
2. Locate the installation media in the machine and click on **SQL2014_x64_ENU** to launch **SQL Server Installation Center**.



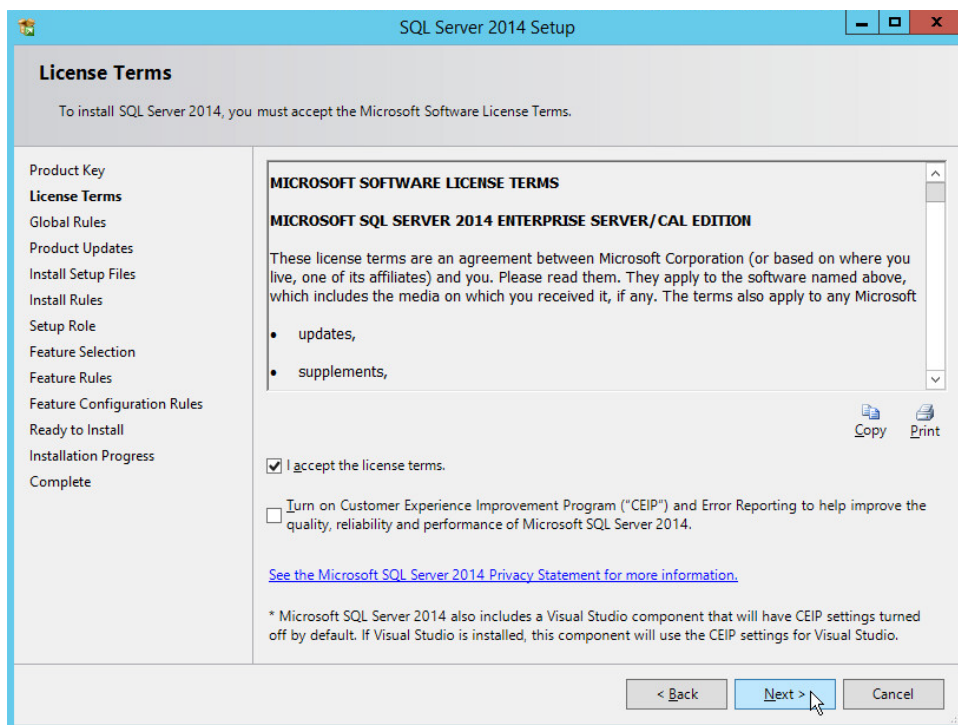
3. On the left menu, select **Installation**.



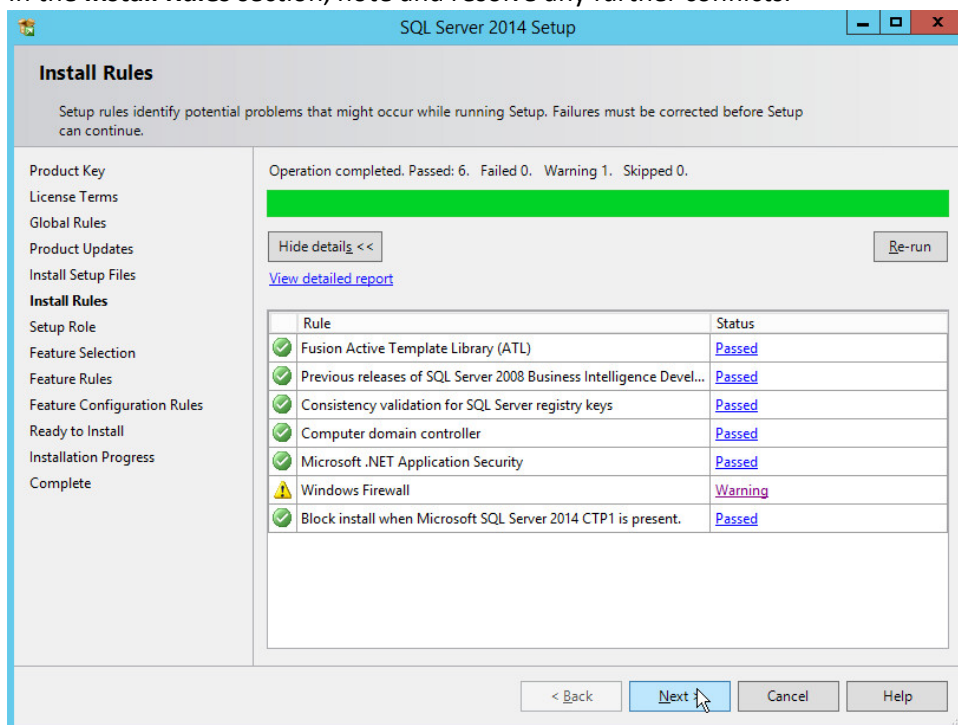
4. Select **New SQL Server stand-alone installation or add features to an existing installation**. This will launch the SQL Server 2014 setup.
5. In the **Product Key** section, enter your product key.



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

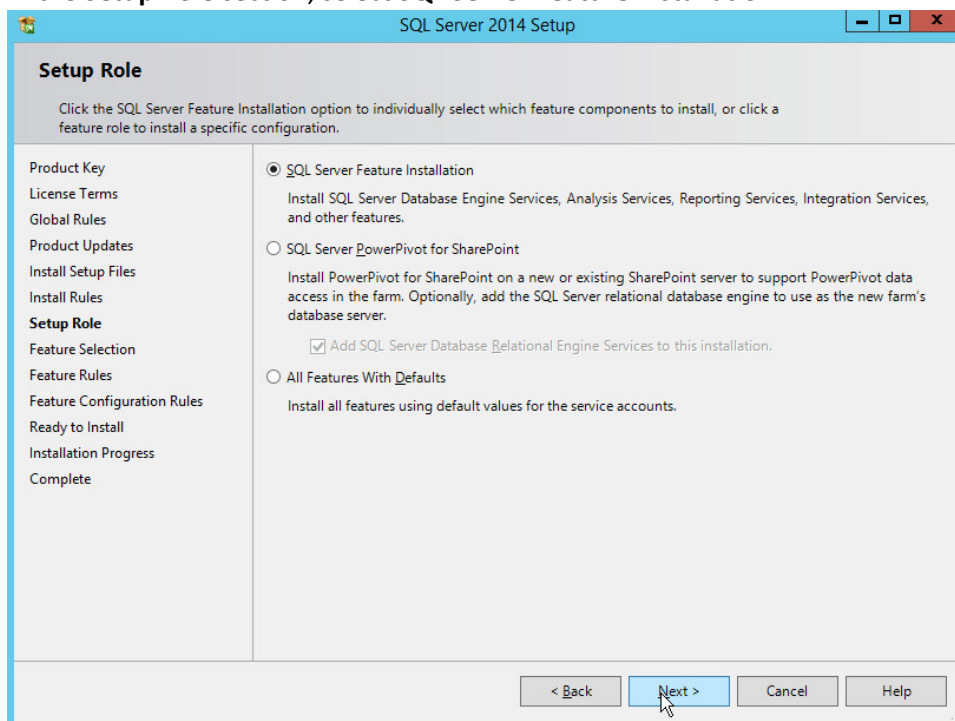


8. Click **Next**.
9. In the **Install Rules** section, note and resolve any further conflicts.



10. Click **Next**.

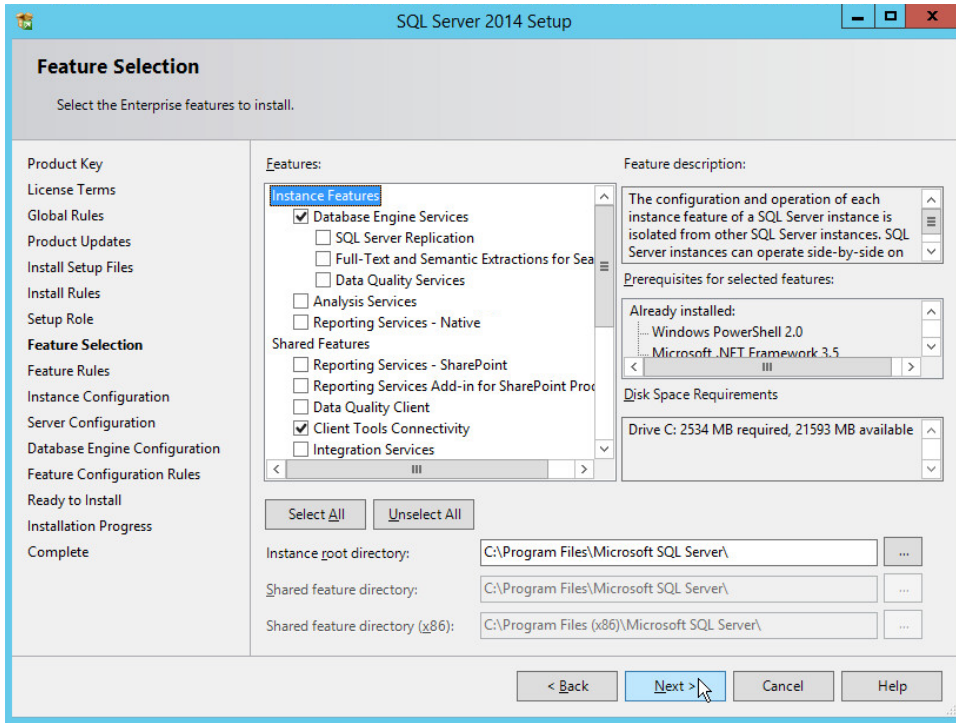
11. In the **Setup Role** section, select **SQL Server Feature Installation**.



12. Click **Next**.

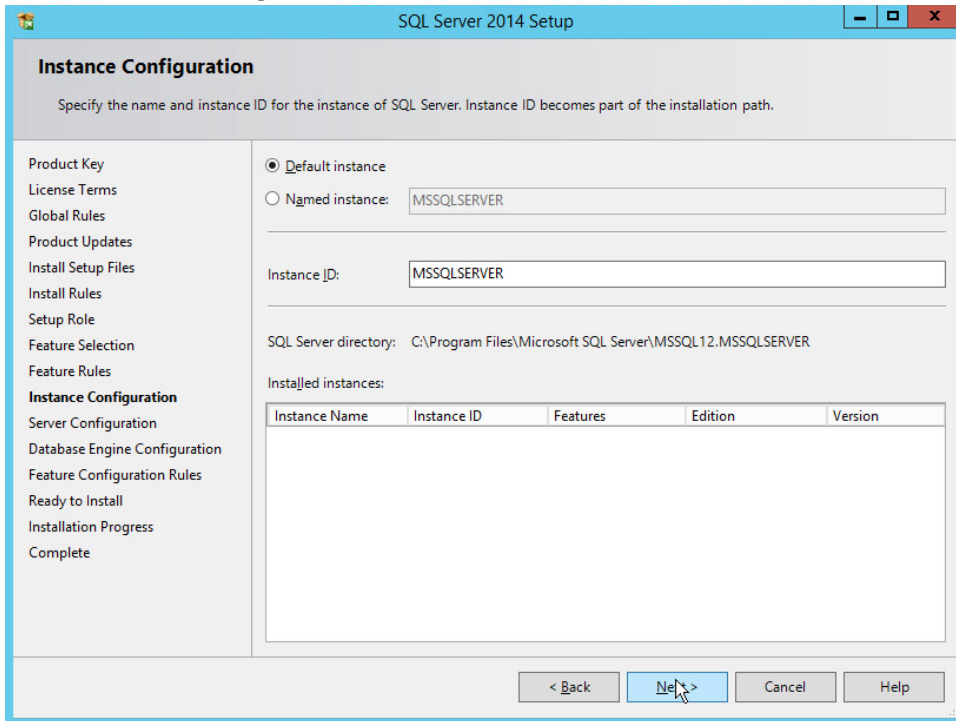
13. In the **Feature Selection** section, select the following:

- 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**

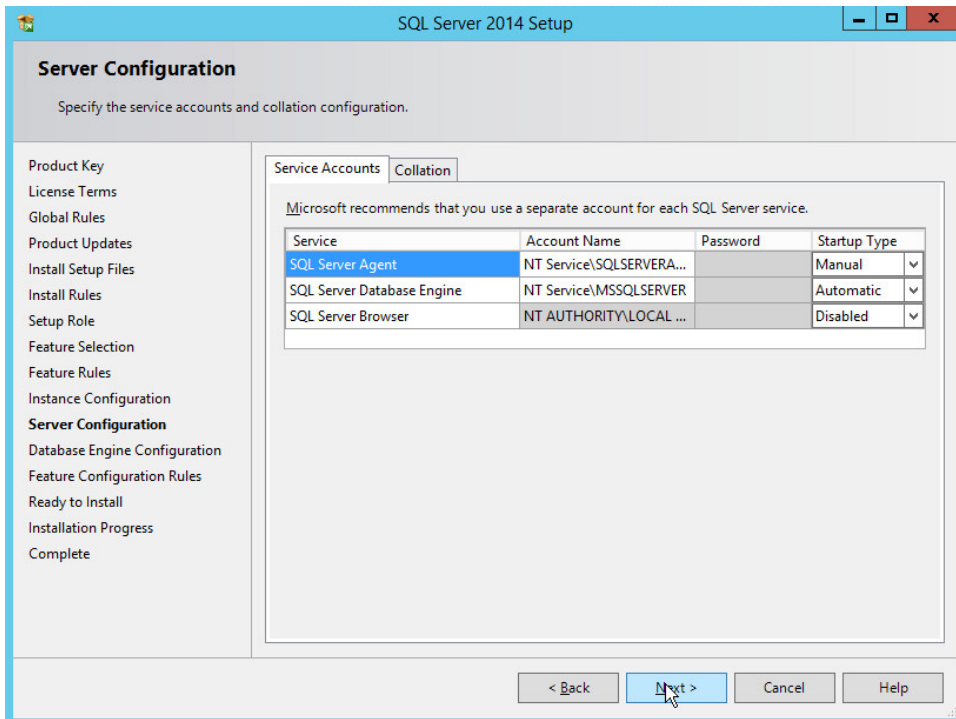


14. Click **Next**.

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



16. Click **Next**.

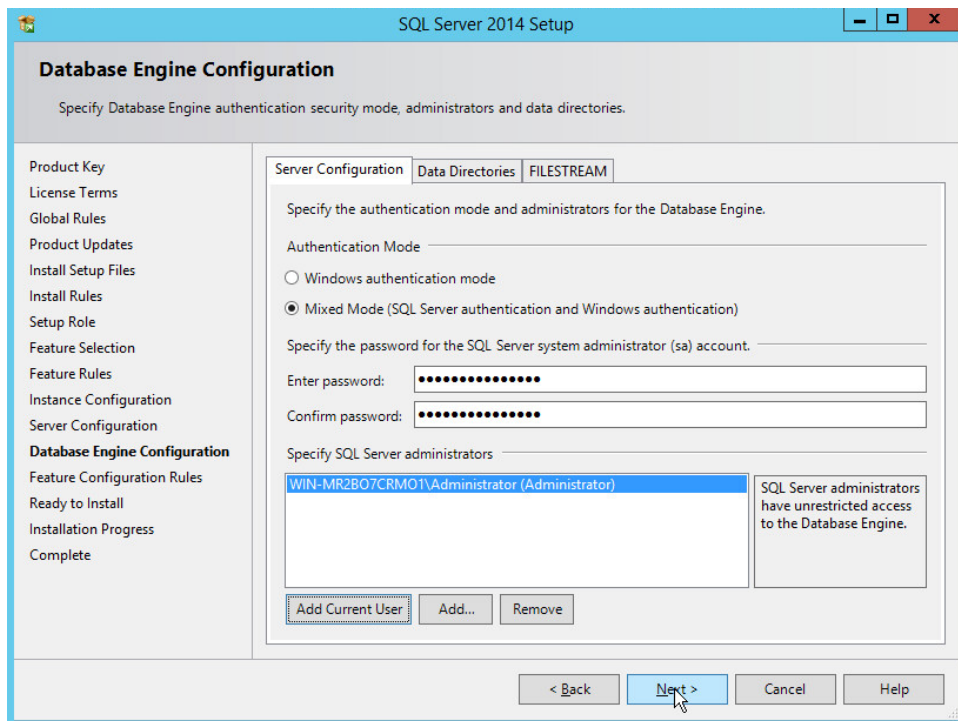


17. In the **Server Configuration** section, click **Next**.

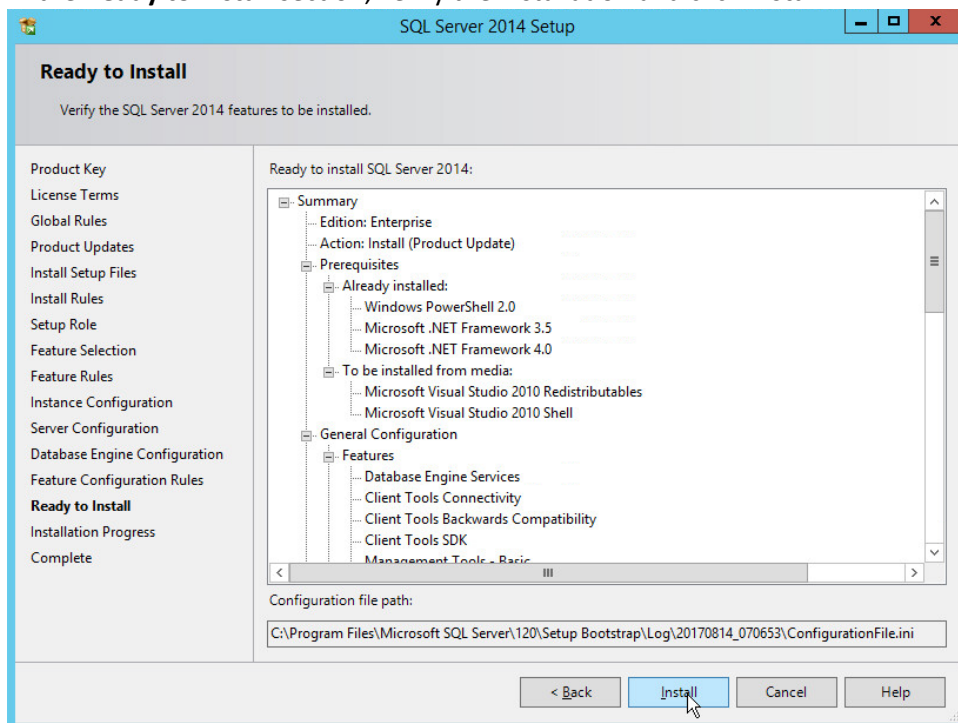
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.

19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User**.

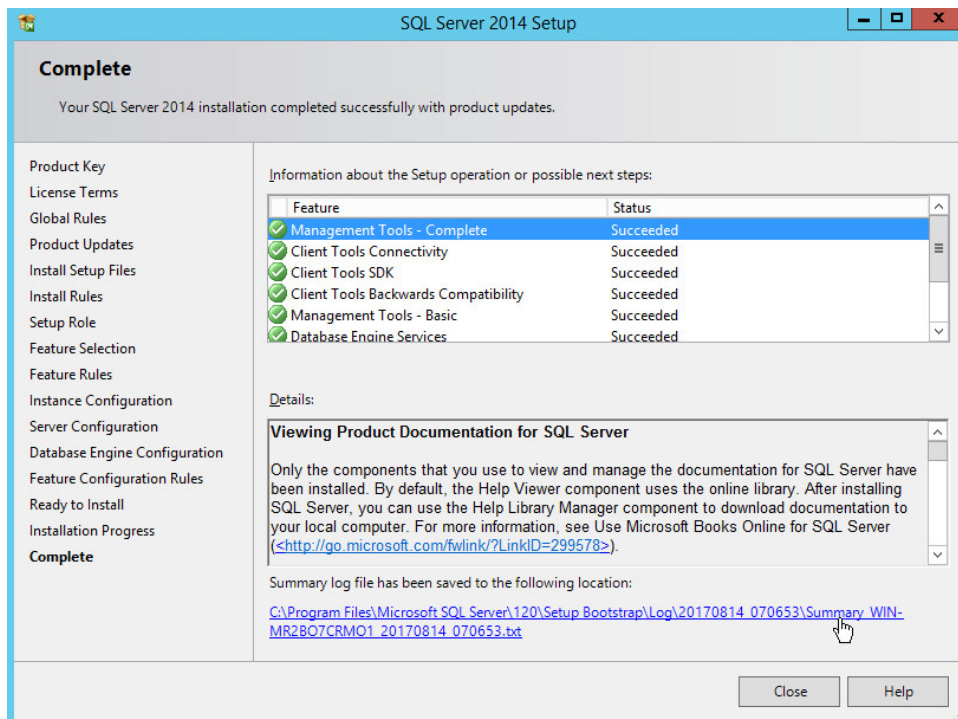
- For Domain accounts, type in **\$DOMAINNAME\USERNAME** into **Enter the object names to select** textbox.
- Click **OK**.
- For local computer accounts, click on **locations** and select the computer's name.
- Click **OK**.
- Type the username into the **Enter the object names to select** textbox.
- Once you are finished adding users, click **Next**.



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



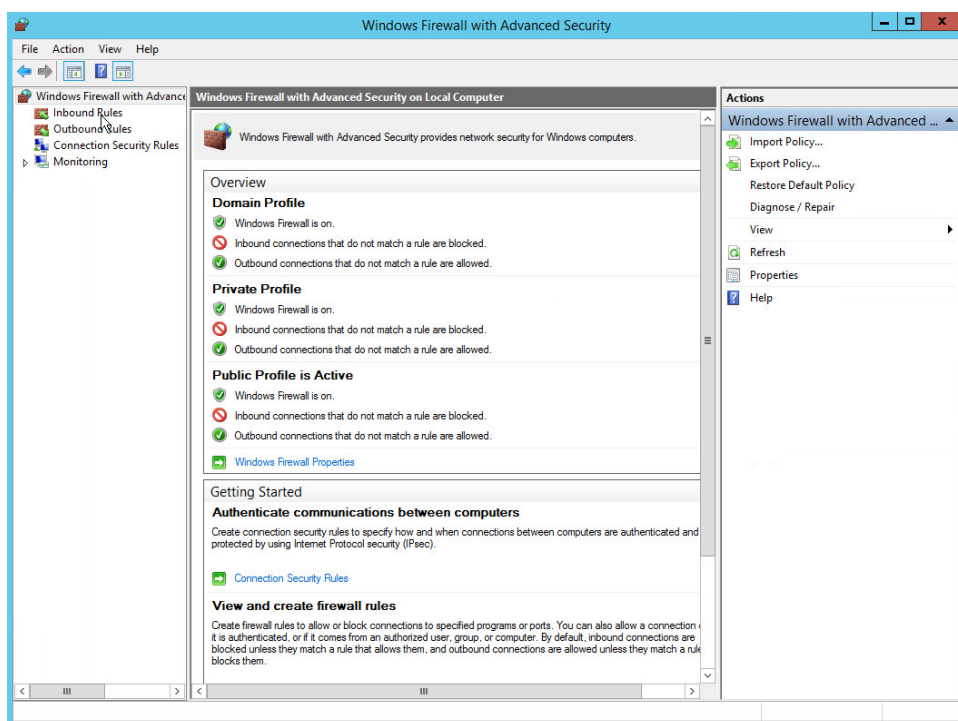
21. Wait for the install to finish.



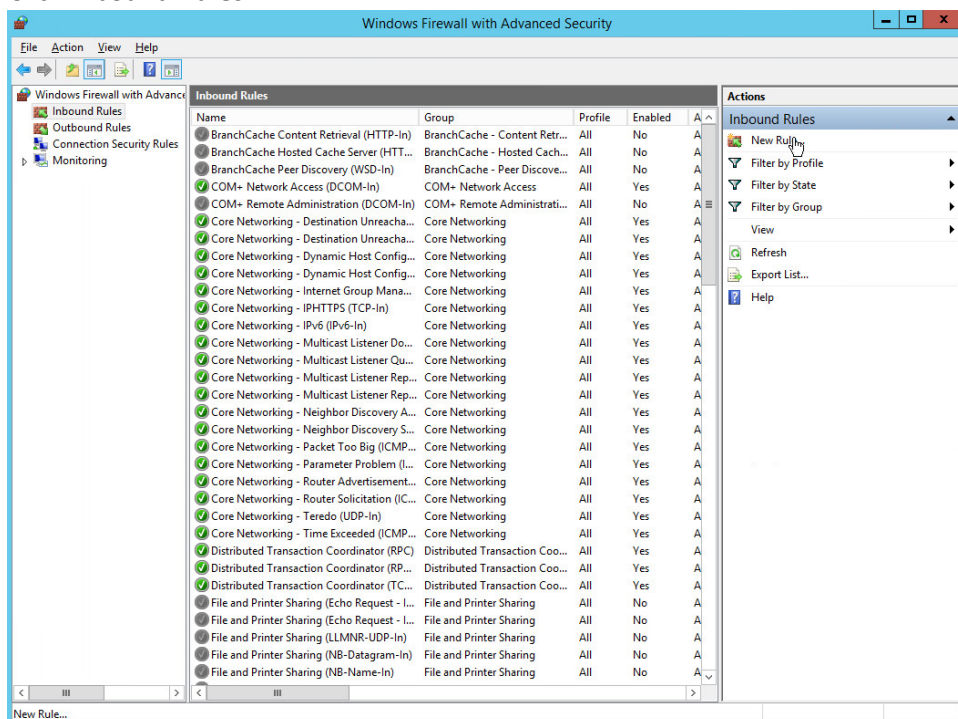
22. Click **Close**.

2.4.2 Open Port on Firewall

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



2. Click Inbound Rules.



3. Click New Rule.

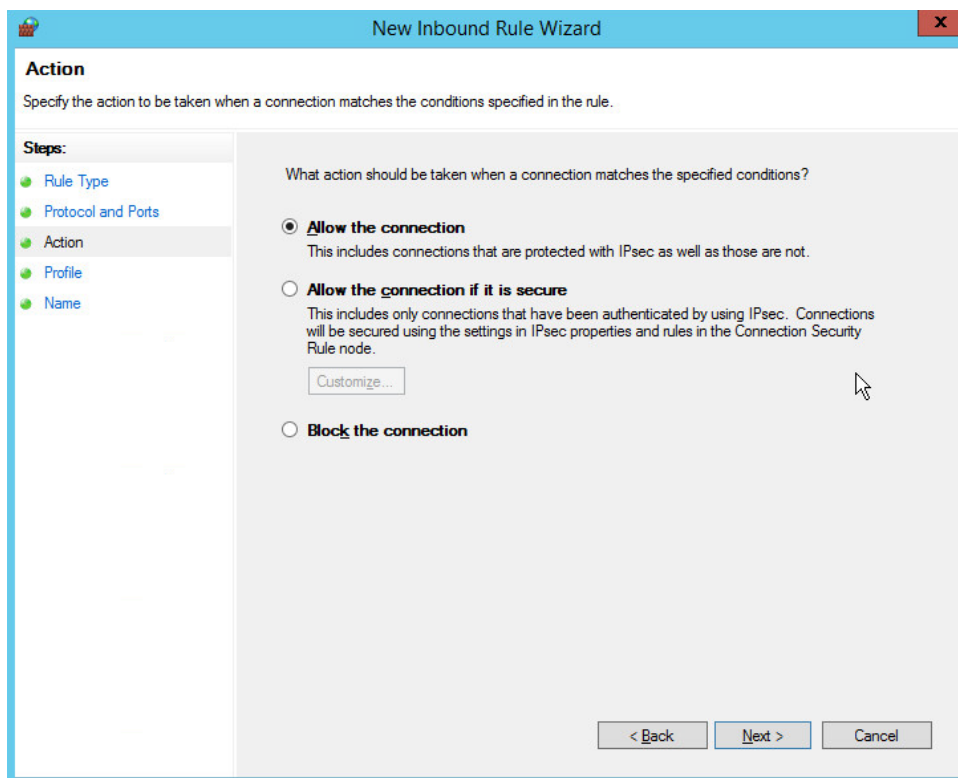
4. Select **Port**.
5. Click **Next**.
6. Select **TCP** and **Specific local ports**.
7. Type **1433** into the text field.

The screenshot shows the 'New Inbound Rule Wizard' window with the 'Protocol and Ports' step selected in the 'Steps' pane on the left. The main area contains the following options:

- Does this rule apply to TCP or UDP?**
 - ☒ **TCP**
 - ☐ **UDP**
- Does this rule apply to all local ports or specific local ports?**
 - ☐ **All local ports**
 - ☒ **Specific local ports:**
Example: 80, 443, 5000-5010

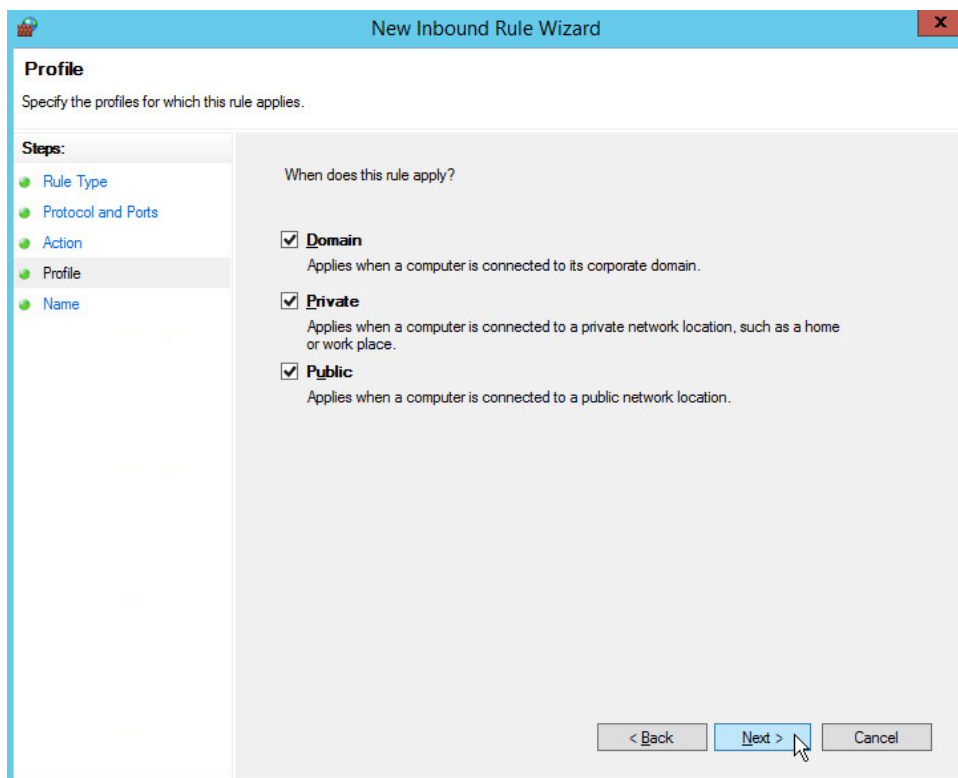
At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

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

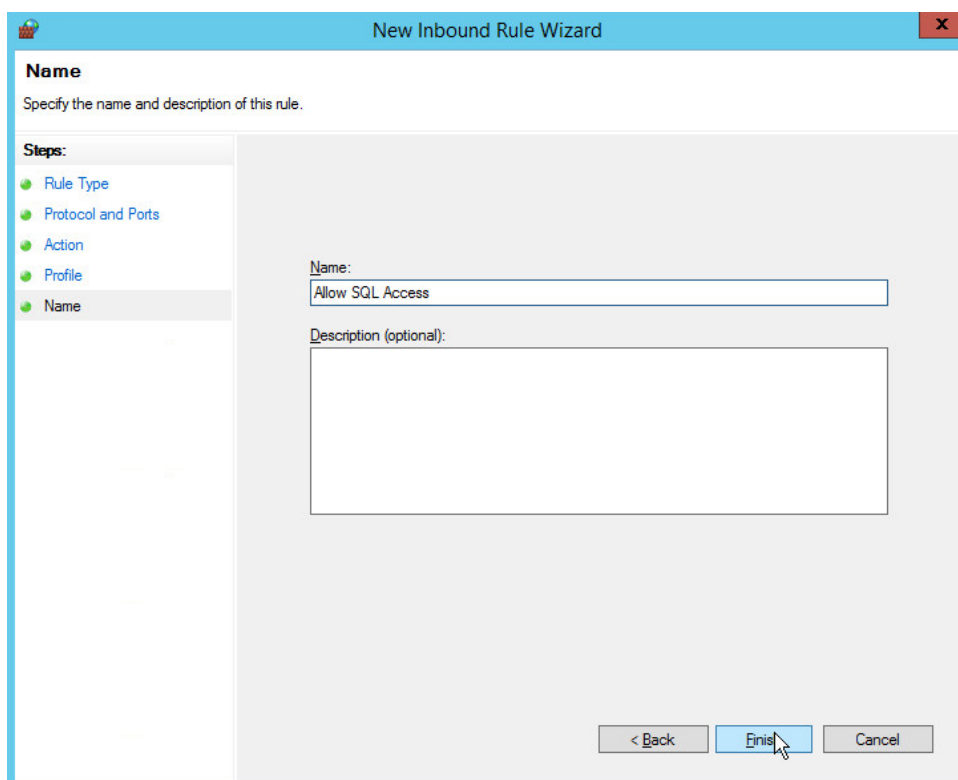


10. Click **Next**.

11. Select all applicable locations.



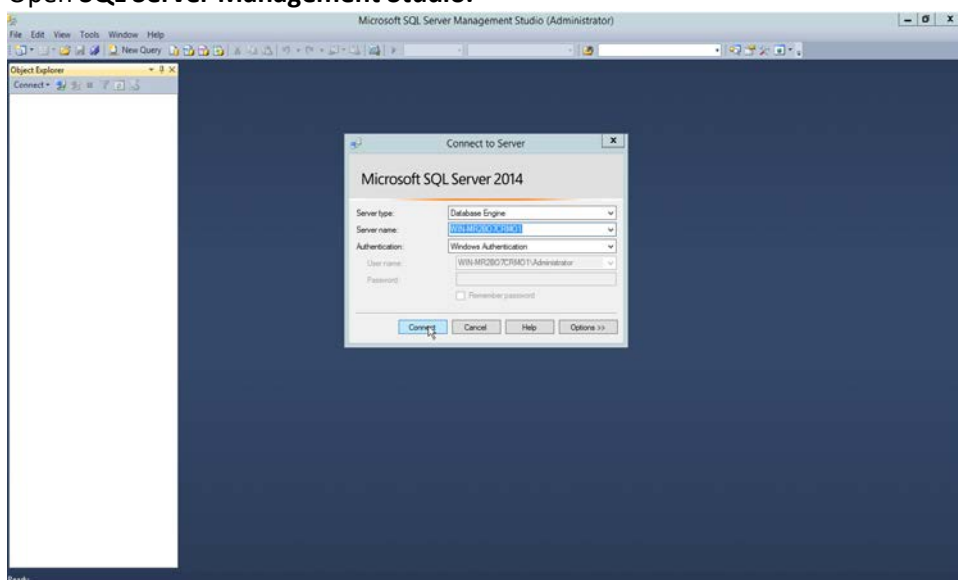
12. Click **Next**.
13. Name the rule **Allow SQL Access**.



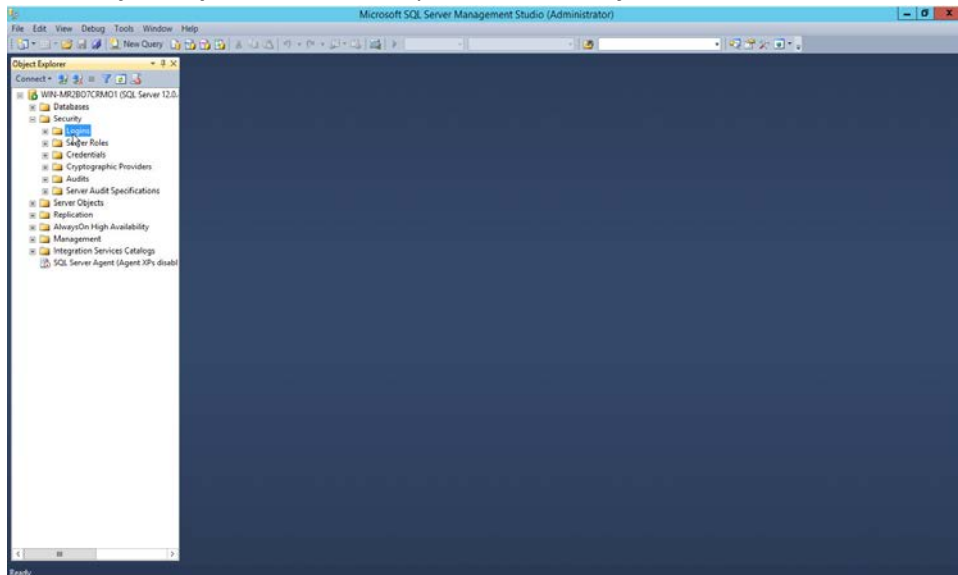
14. Click **Finish**.

2.4.3 Add a New Login to the Database

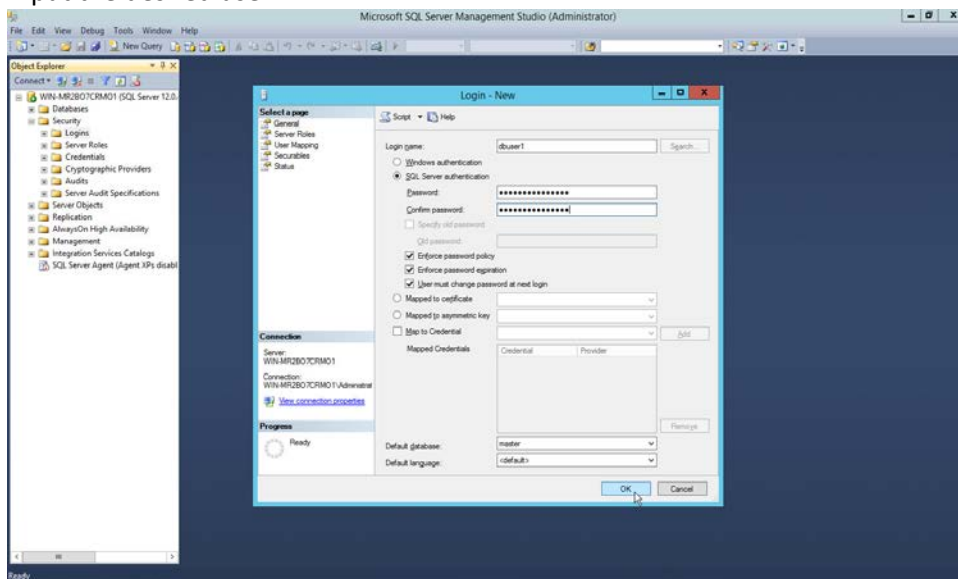
1. Open **SQL Server Management Studio**.



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



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



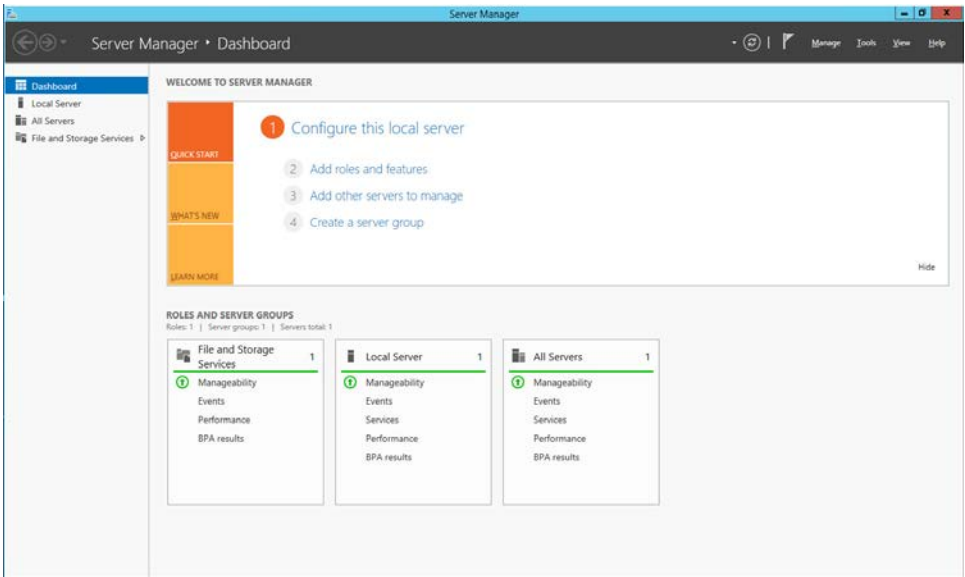
6. Click **OK**.

2.5 Microsoft IIS Server

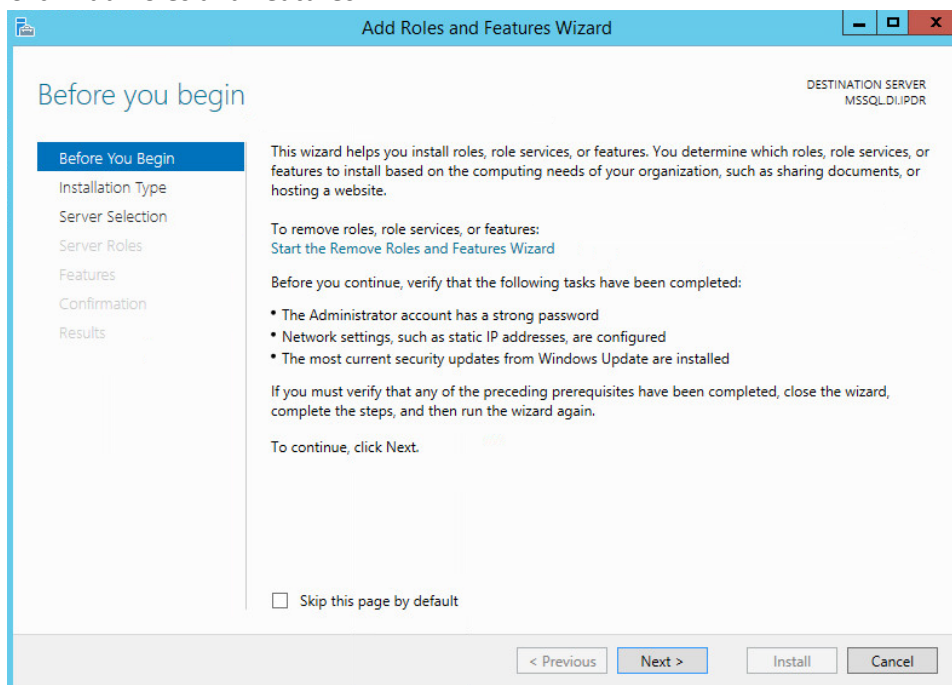
As part of our enterprise emulation, we include a Microsoft Internet Information Services (IIS) server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine. This was conducted on the same machine as [Section 2.4](#).

2.5.1 Install IIS

1. Open **Server Manager**.

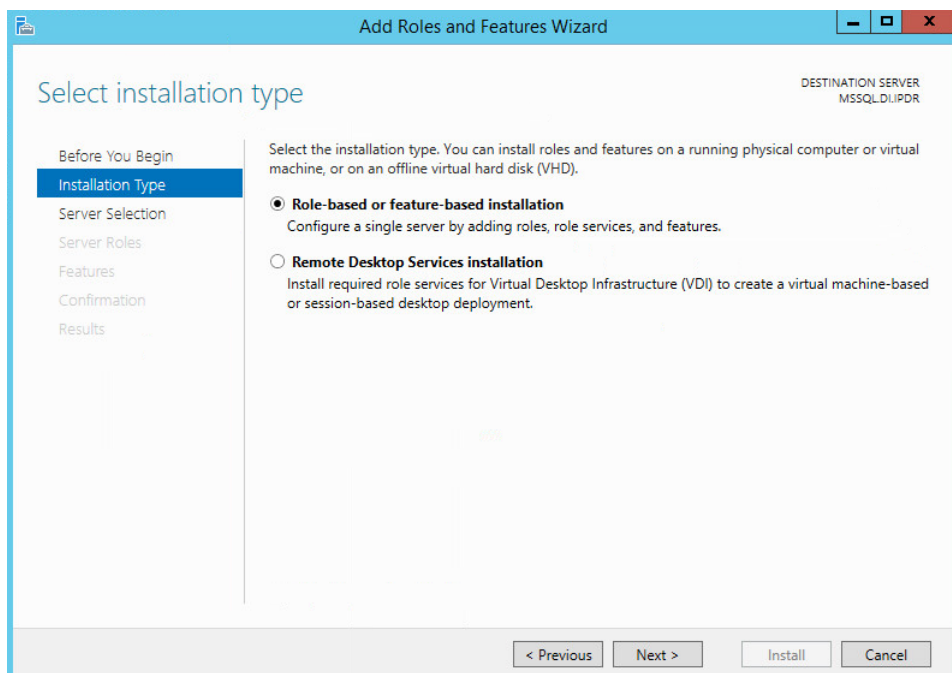


2. Click **Add Roles and Features**.



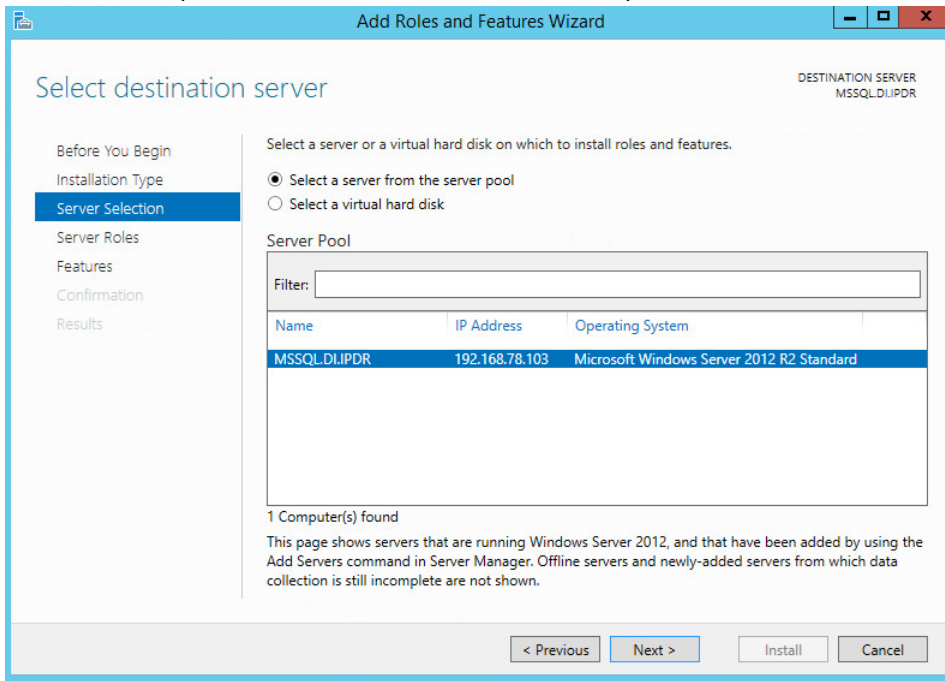
3. Click **Next**.

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

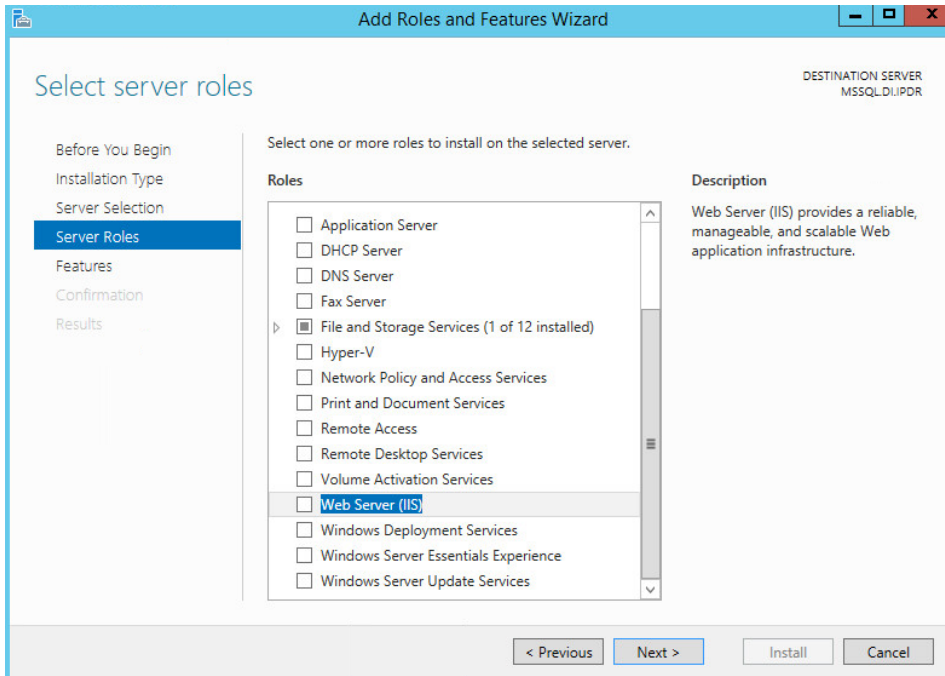


5. Click **Next**.

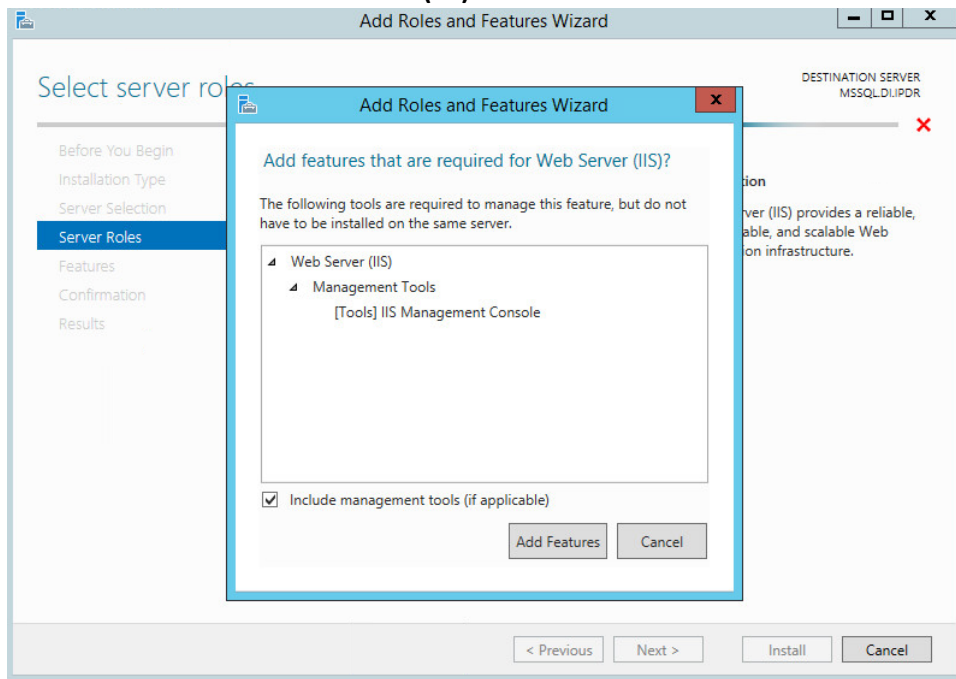
6. Select **MSSQL** (or the correct Windows Server name) from the list.



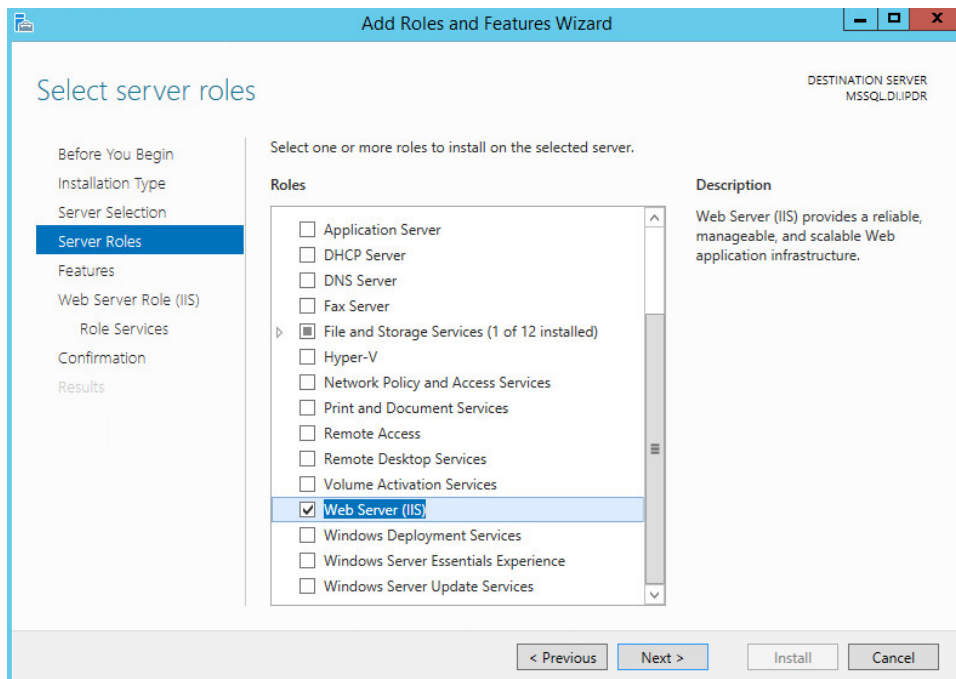
7. Click **Next**.



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

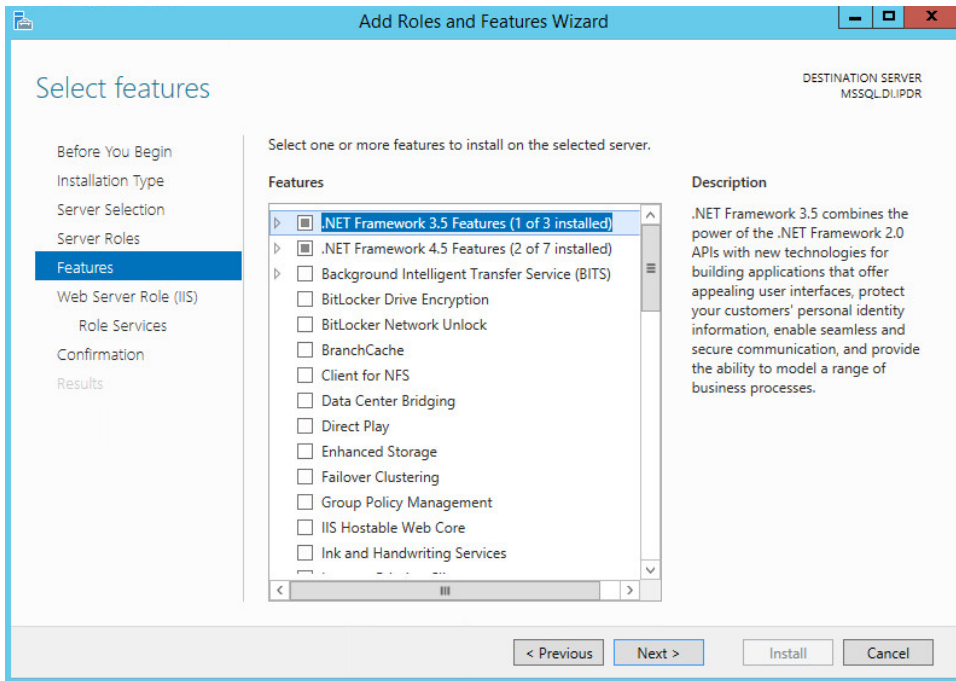


9. Click **Add Features**.

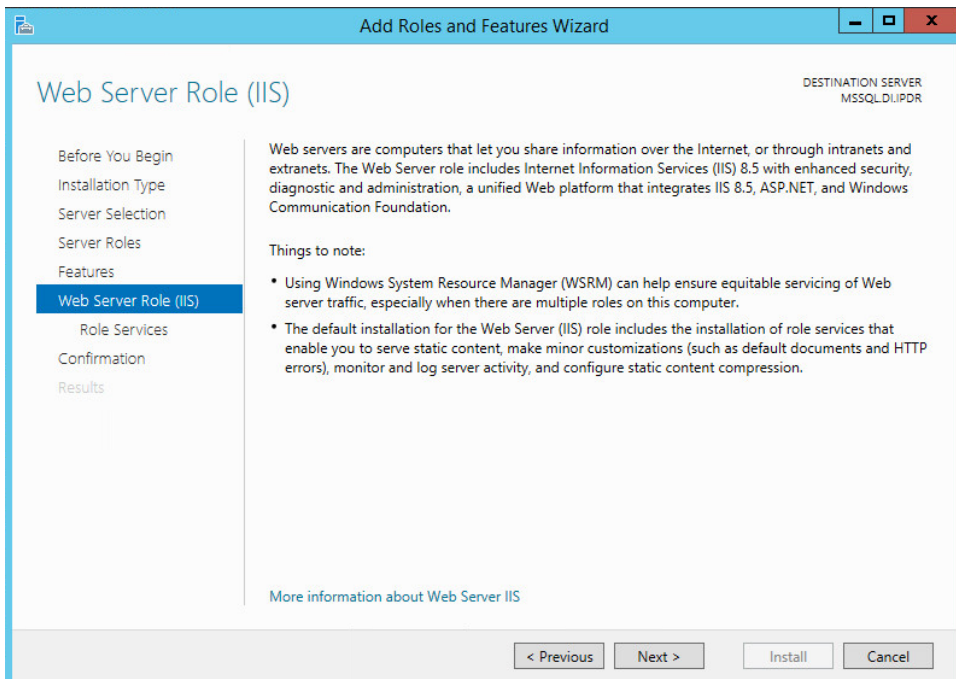


10. Click **Next**.

11. Ensure that all desired features are selected.

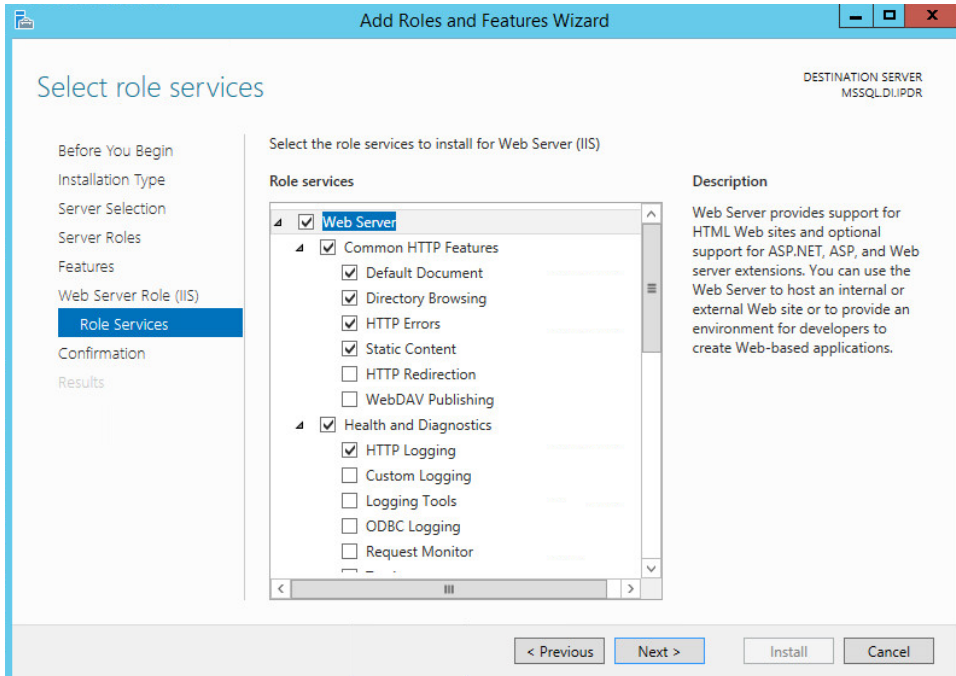


12. Click **Next**.

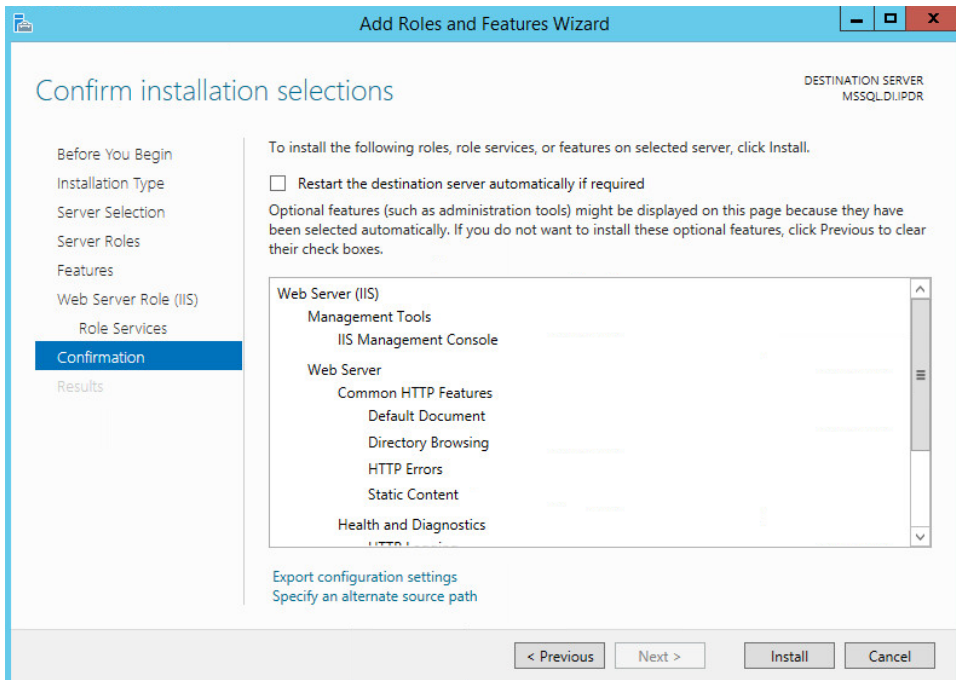


13. Click **Next**.

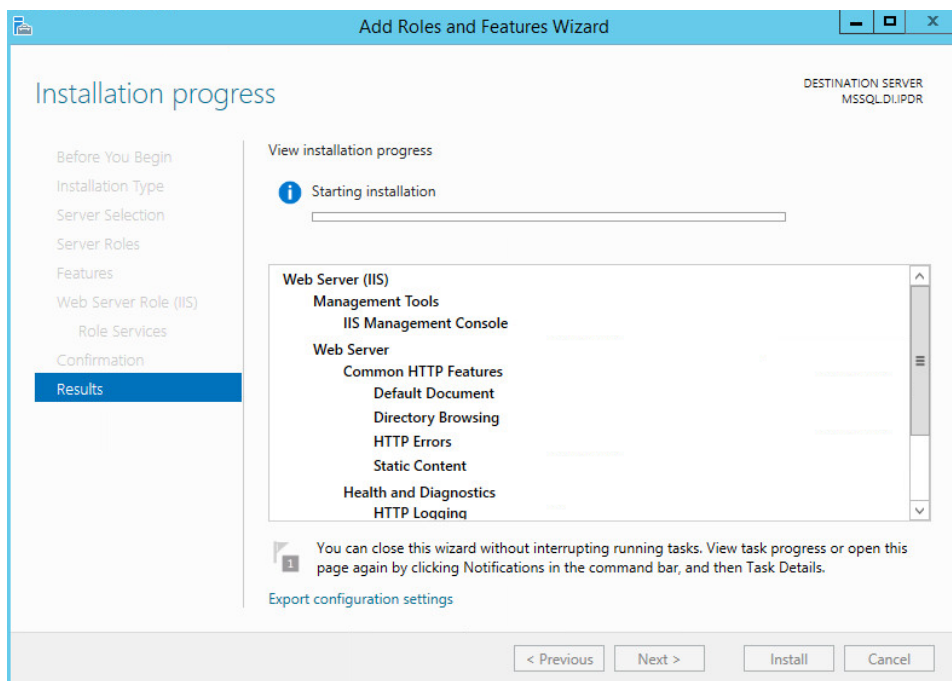
14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging**, and any other desired Role services are selected.



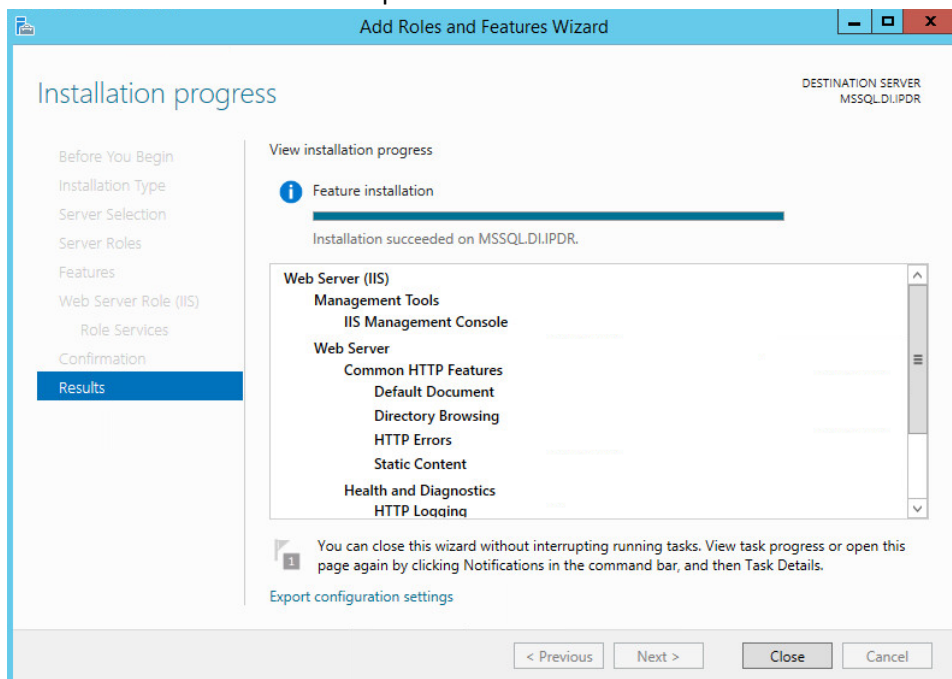
15. Click **Next**.



16. Click **Install**.



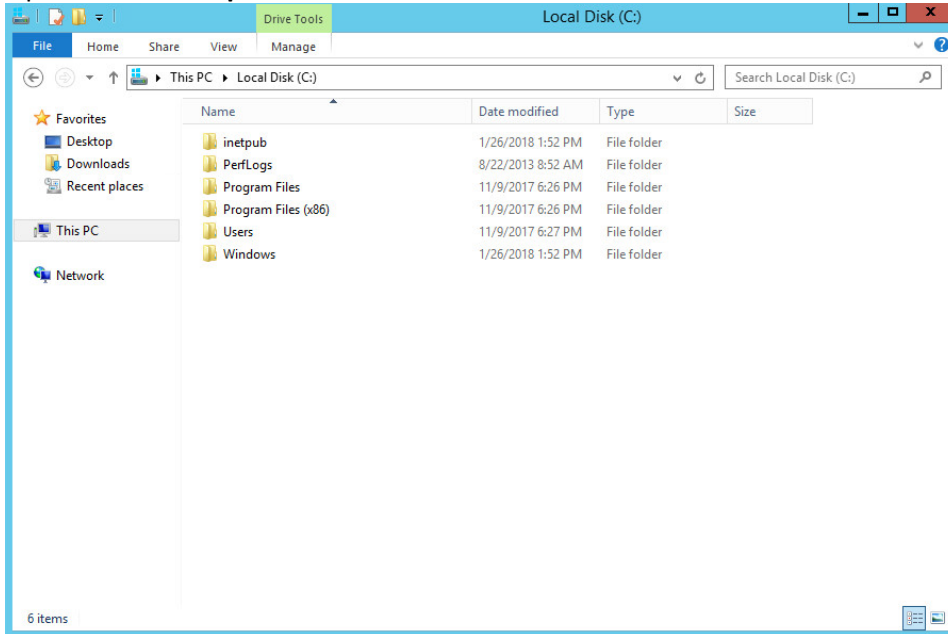
17. Wait for the installation to complete.



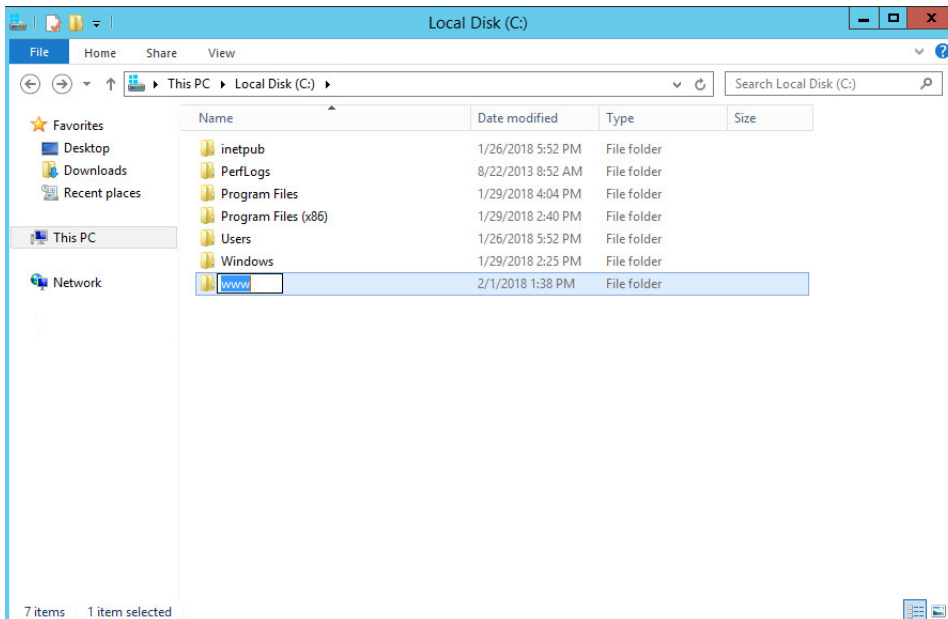
18. Click **Close**.

2.5.2 IIS Configuration

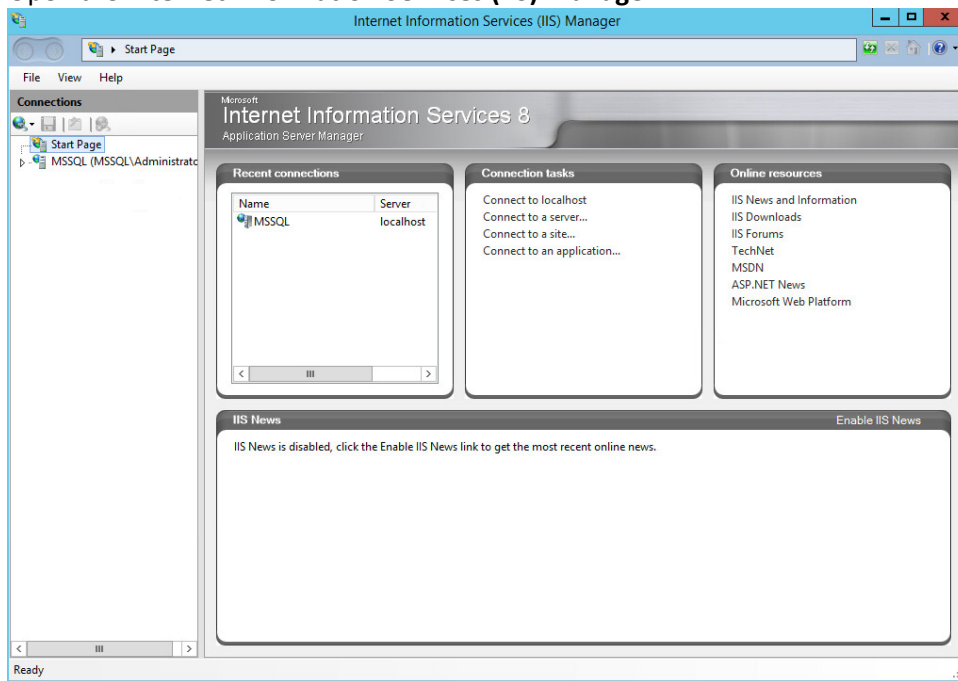
1. Open **Windows Explorer** and click **This PC**.



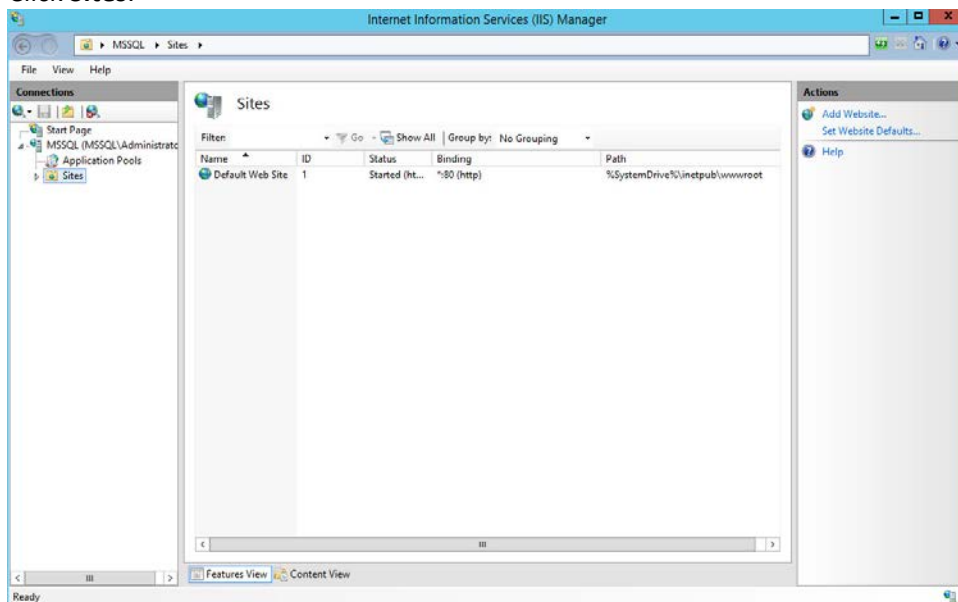
2. Right-click, and select **Create Folder**.
3. Name the folder **www**.



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



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



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

Add Website

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

8. Enter the desired site name.

Add Website

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

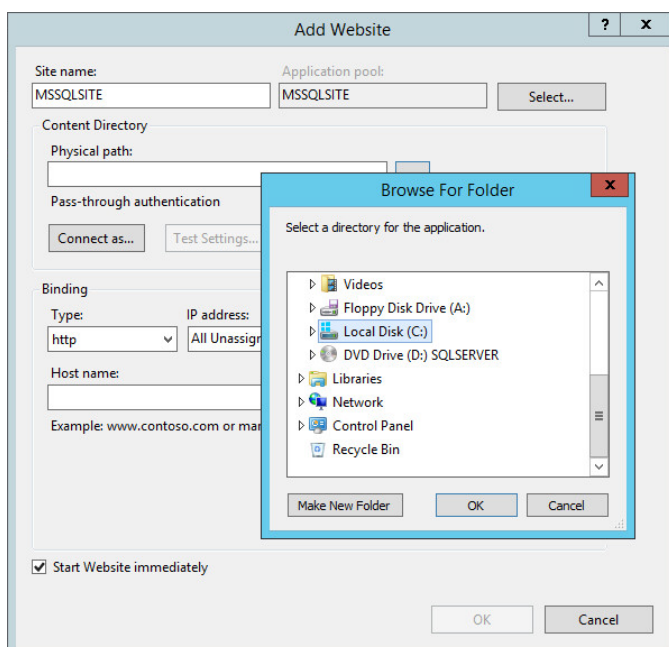
Type: IP address: Port:

Host name:

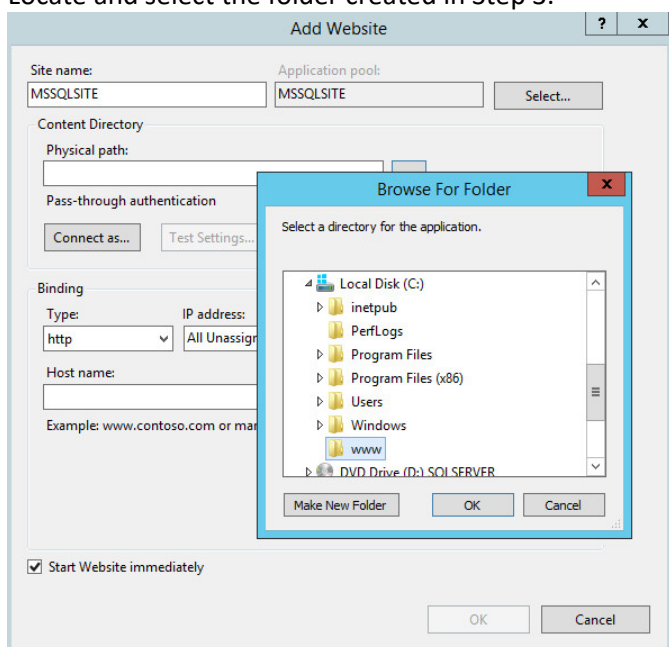
Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

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.

The screenshot shows the 'Add Website' dialog box. The 'Site name' field contains 'MSSQLSITE'. The 'Application pool' dropdown is set to 'MSSQLSITE'. The 'Physical path' field contains 'C:\www'. The 'Binding' section has 'Type' set to 'http', 'IP address' set to '192.168.81.107', and 'Port' set to '80'. The 'Host name' field contains 'MSSQL.di.ipdr'. The 'Start Website immediately' checkbox is checked. The 'OK' button is highlighted.

15. Click **OK**.

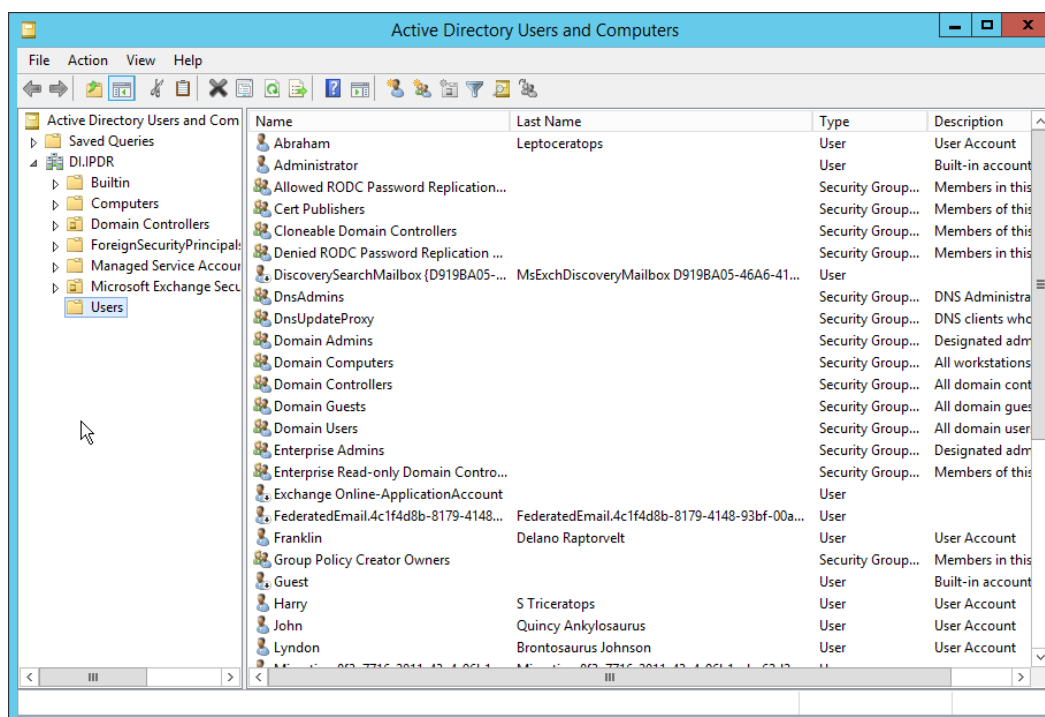
2.6 Semperis Directory Services Protector

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, 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**.



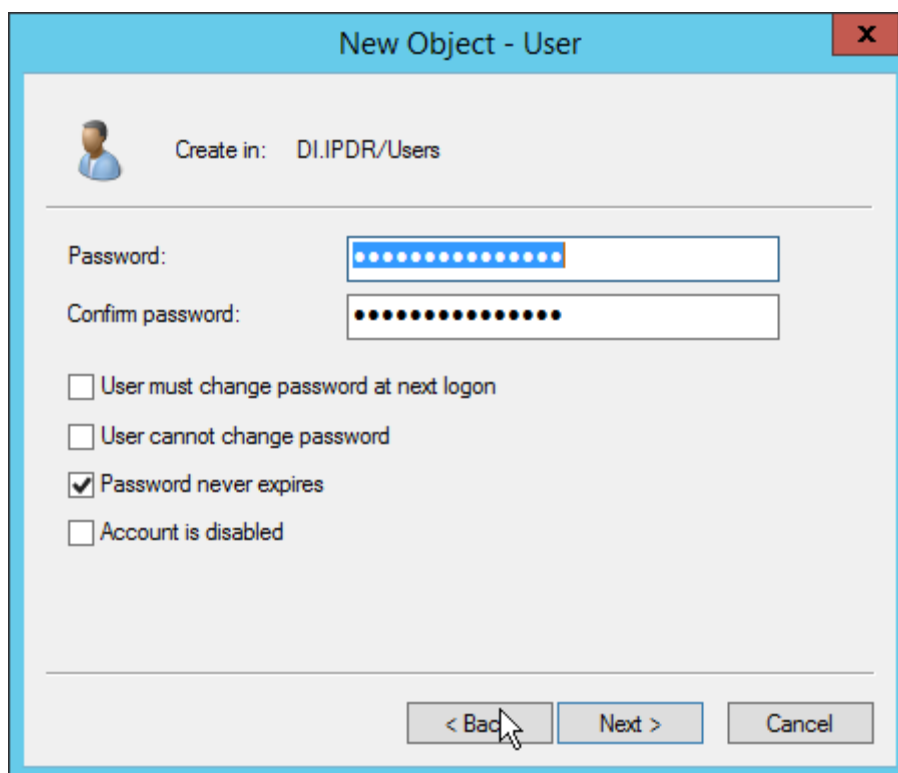
2. Right-click **Users** in the left pane, and select **New > User**.
3. Enter the information for a new user for the DSP service.

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'DI.IPDR/Users'. The fields are filled with the following information:

Field	Value
First name	DSP
Last name	Service
Full name	DSP Service
User logon name	dspservice
User logon name (pre-Windows 2000)	DI\dspservice

The 'Initials' field is empty. The 'User logon name' dropdown is set to '@DI.IPDR'. The 'Next >' button is highlighted by the mouse cursor.

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: [password field]

Confirm password: [password field]

☐ User must change password at next logon

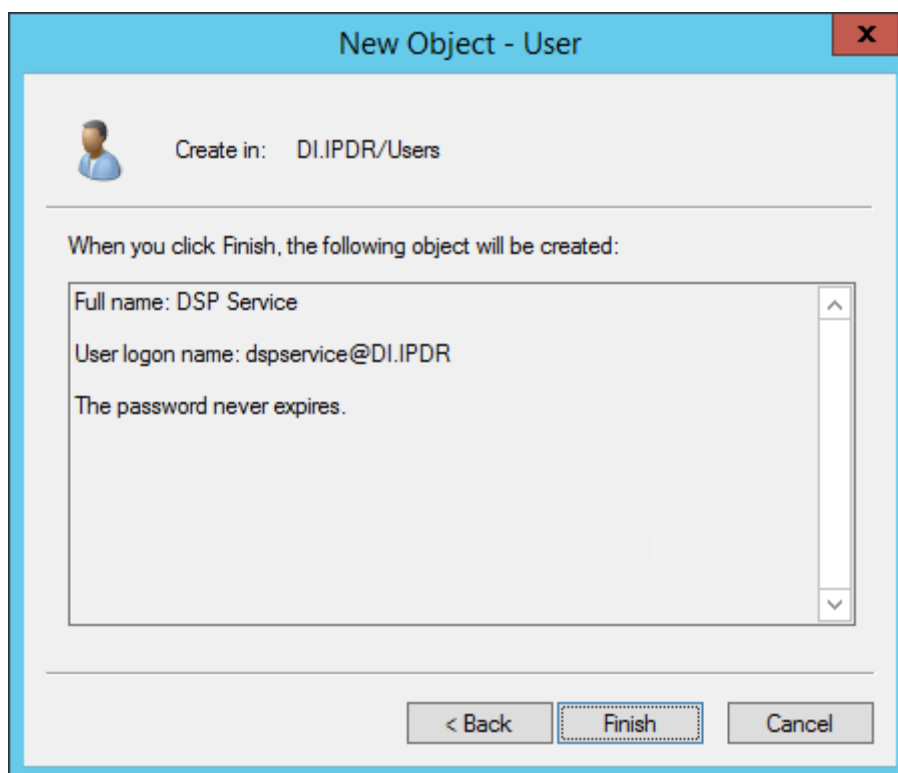
☐ User cannot change password

☒ Password never expires

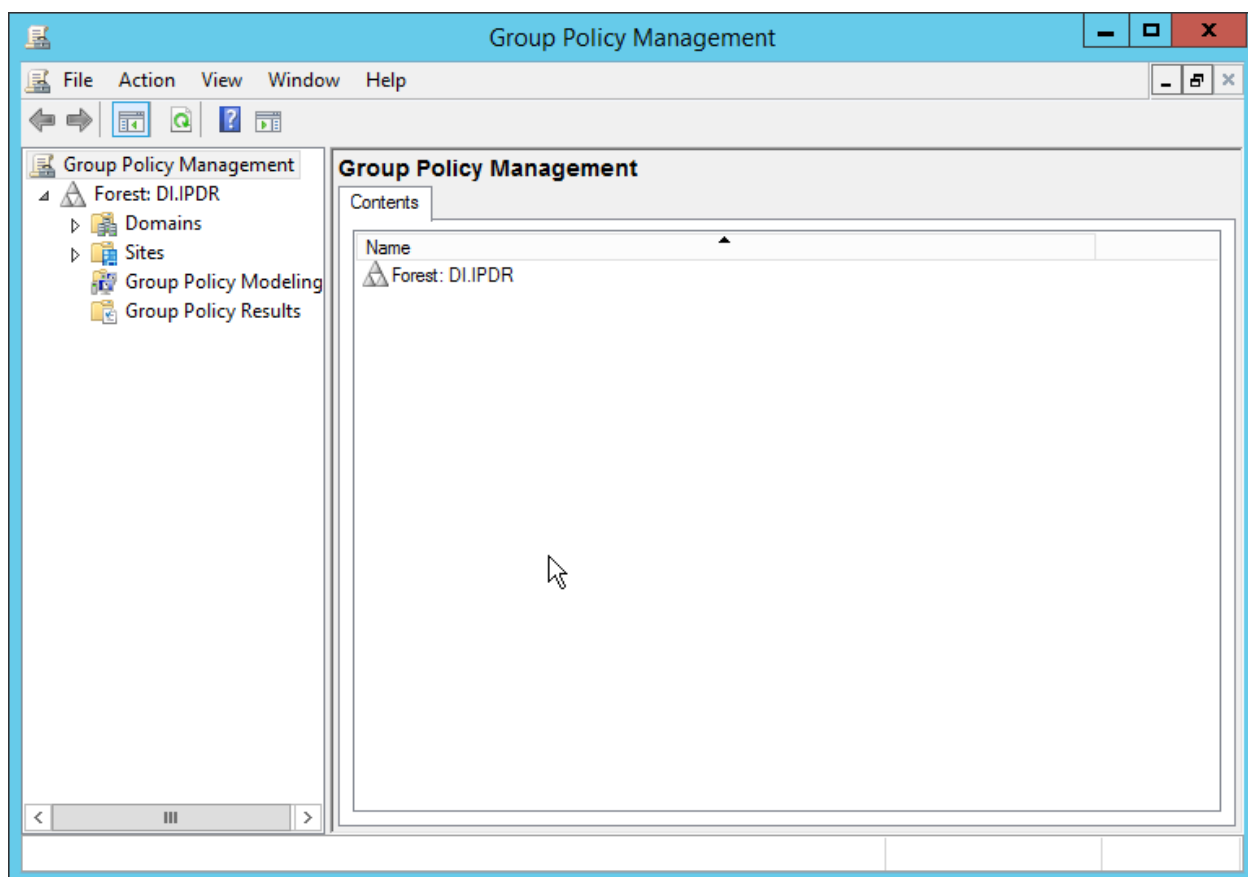
☐ Account is disabled

< Back Next > Cancel

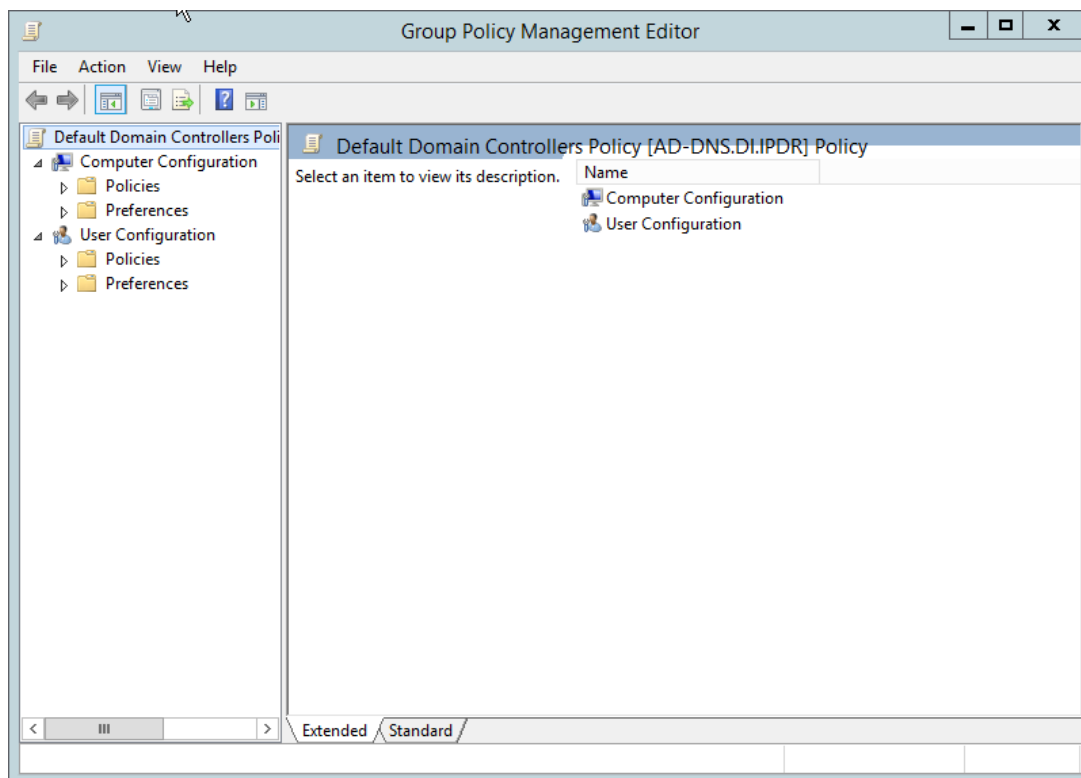
7. Click **Next**.



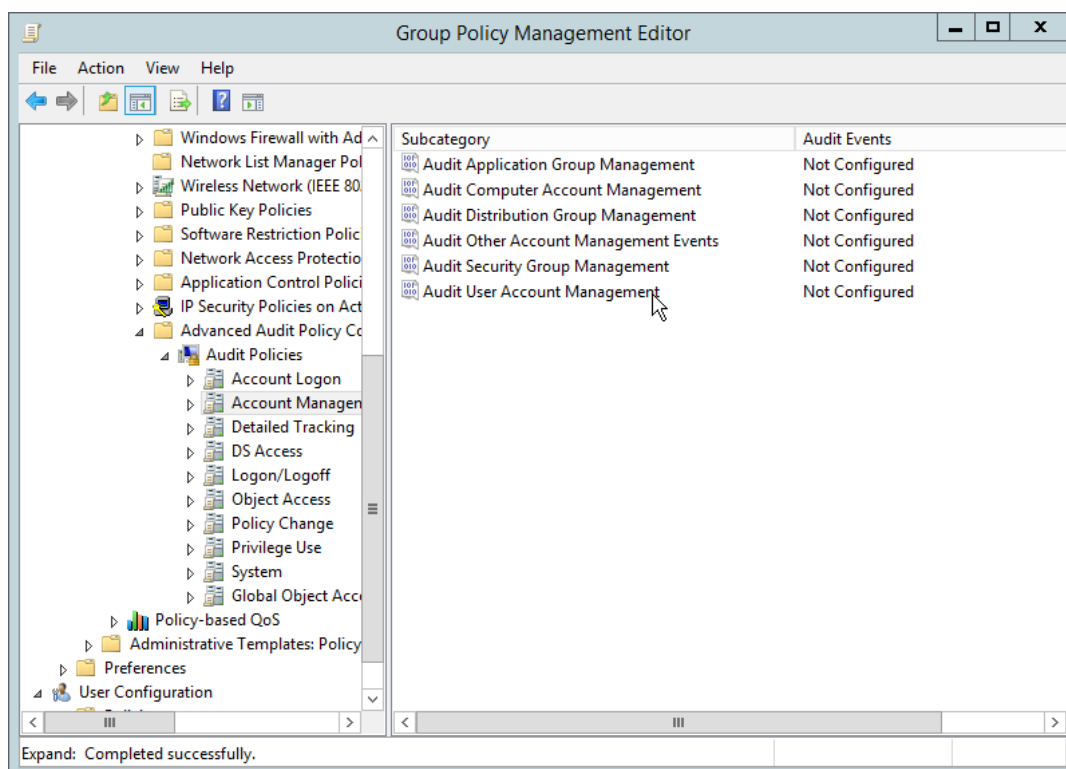
8. Click **Finish**.
9. Open **Group Policy Management**.



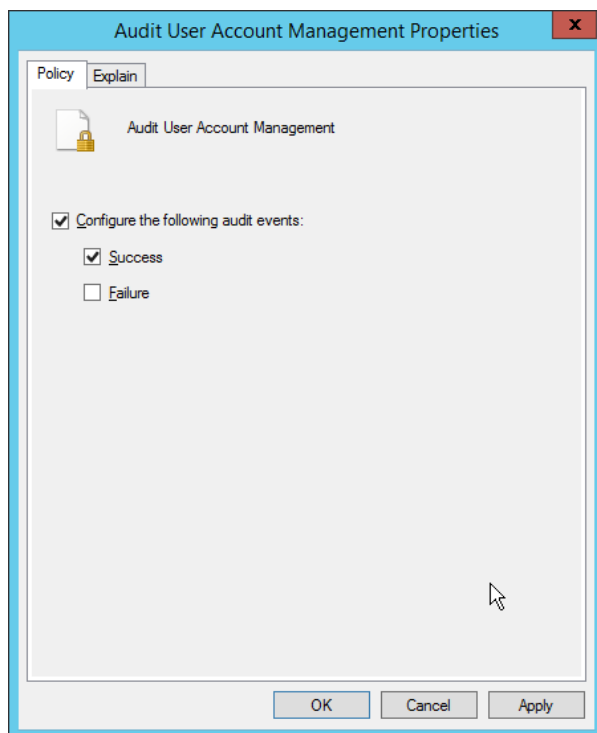
10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy**, and click **Edit**.



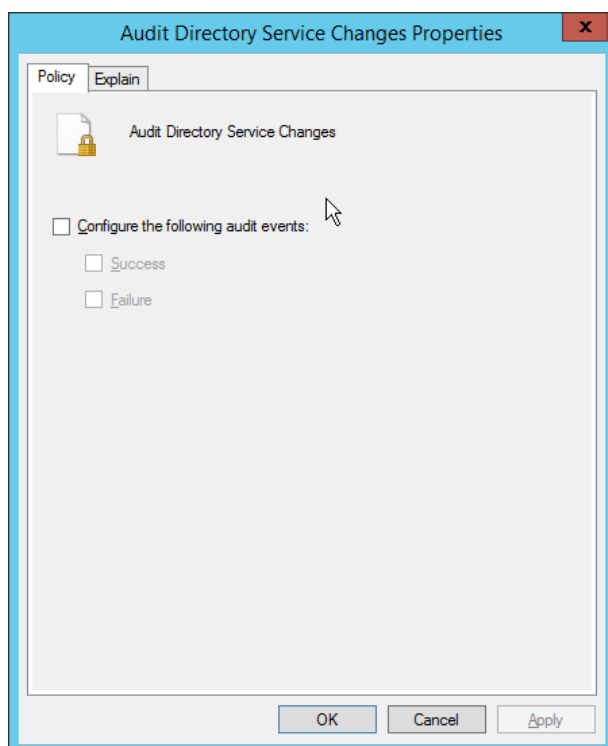
11. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management**.



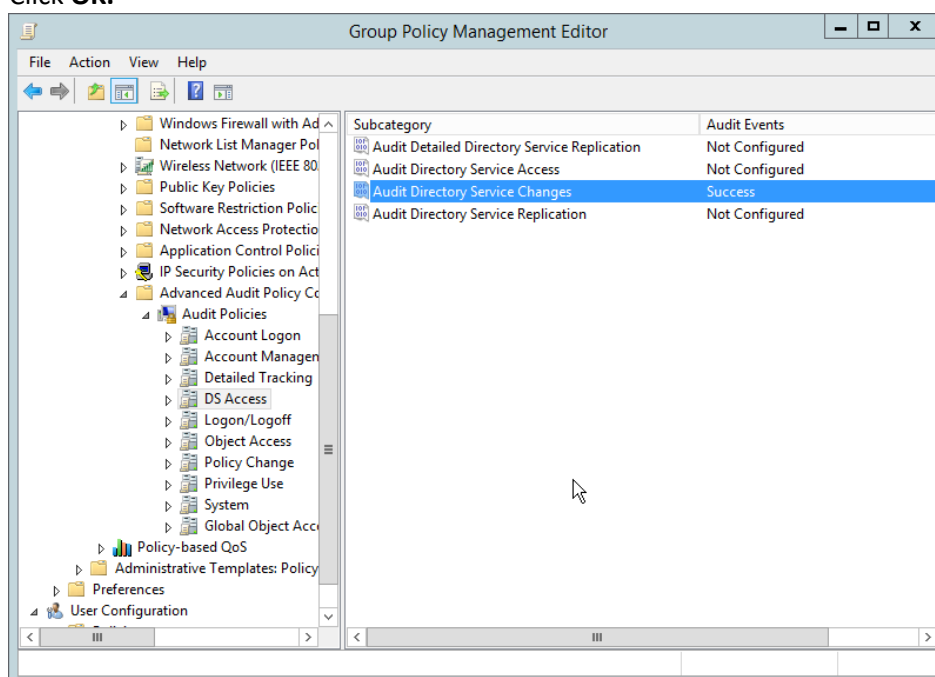
12. Edit the **Audit User Account Management** field by double-clicking it.
13. Check the box next to **Configure the following audit events**.
14. Check the box next to **Success**.



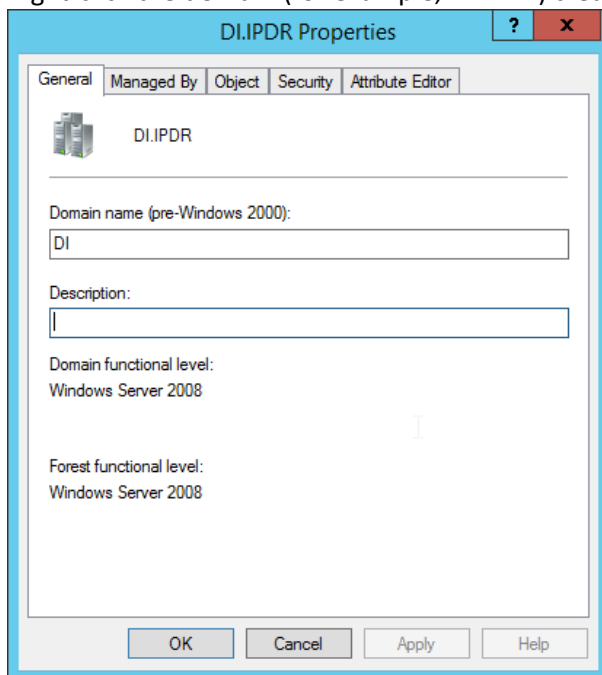
15. Click **OK**.
16. Go to **Audit Policies > DS Access**.
17. Double-click **Audit Directory Services Changes**.



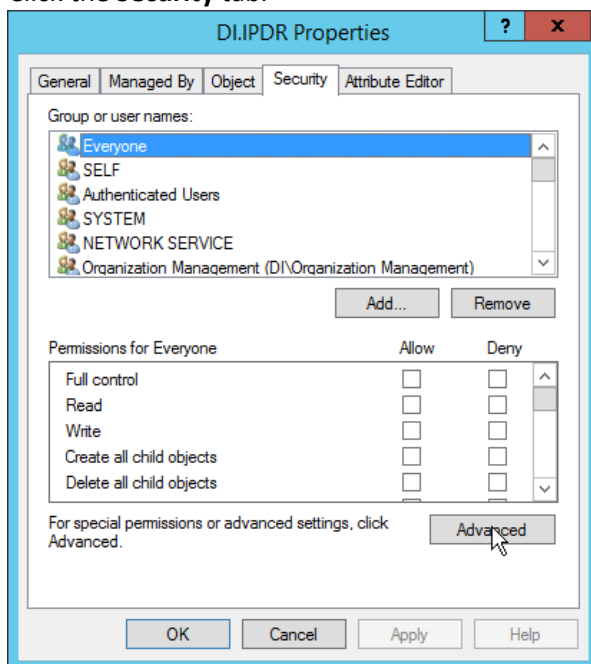
18. Check the box next to **Configure the following audit events**.
19. Check the box next to **Success**.
20. Click **OK**.



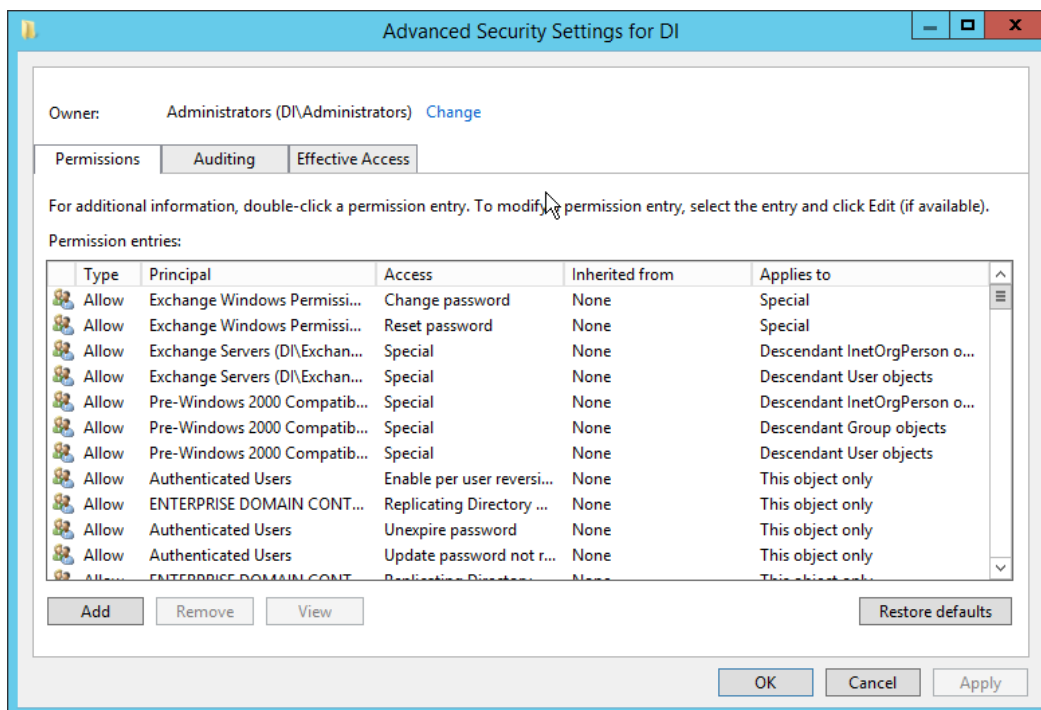
21. Open **Active Directory Users and Computers**.
22. Ensure **View > Advanced Features** is enabled.
23. Right-click the **domain** (for example, DI.IPDR) created earlier, and click **Properties**.



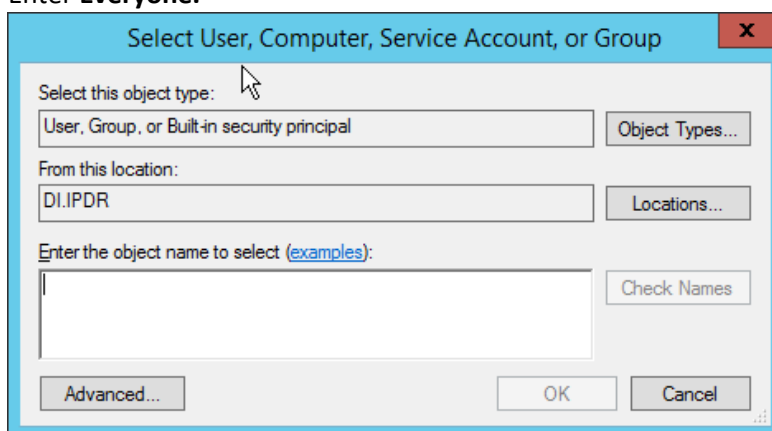
24. Click the **Security** tab.



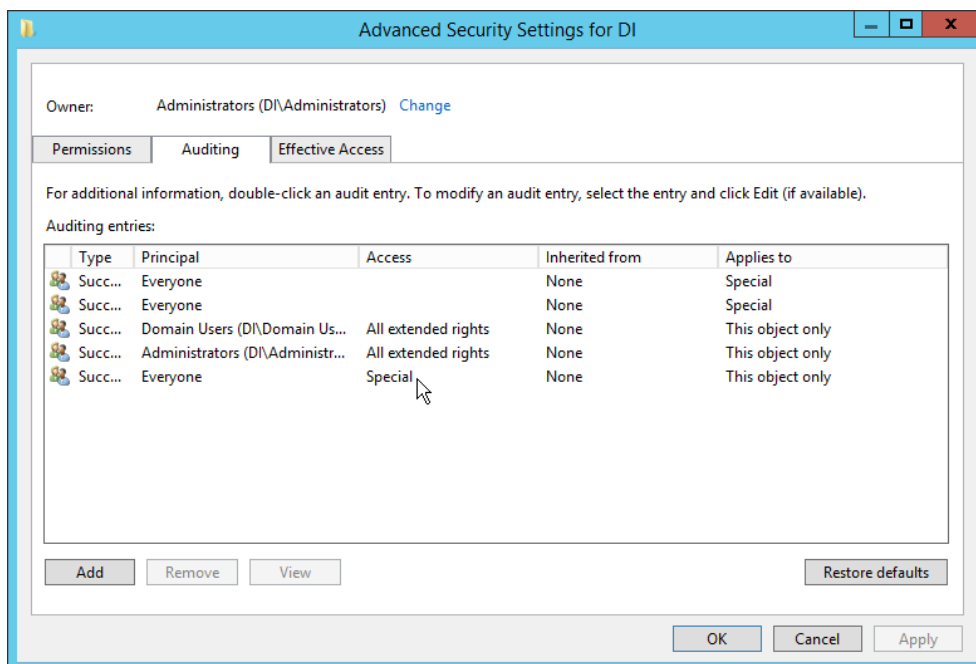
25. Click **Advanced**.



26. Click the **Auditing** tab.
27. Click **Add**.
28. Enter **Everyone**.

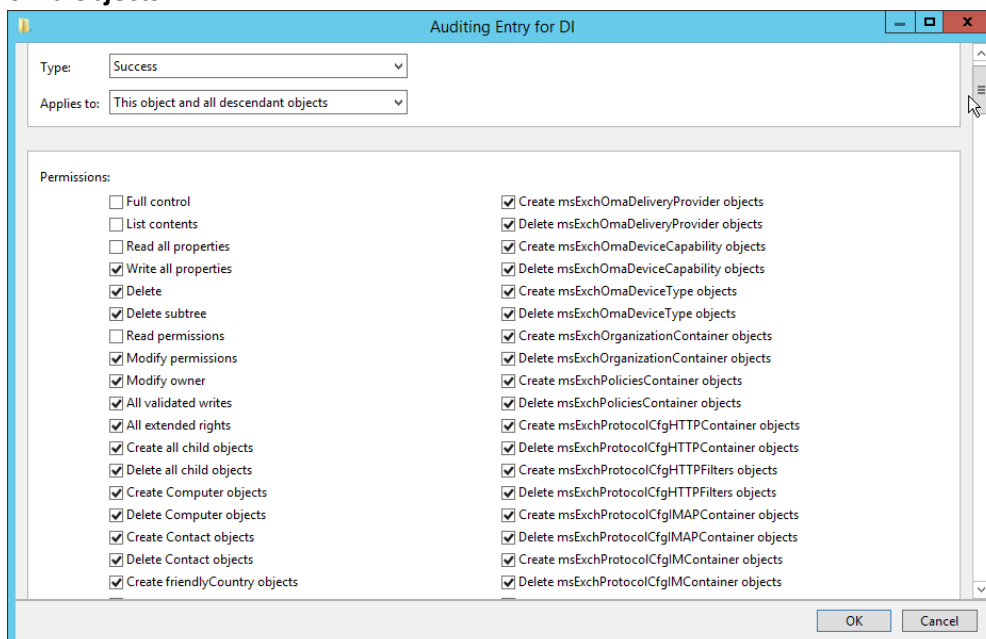


29. Click **OK**.

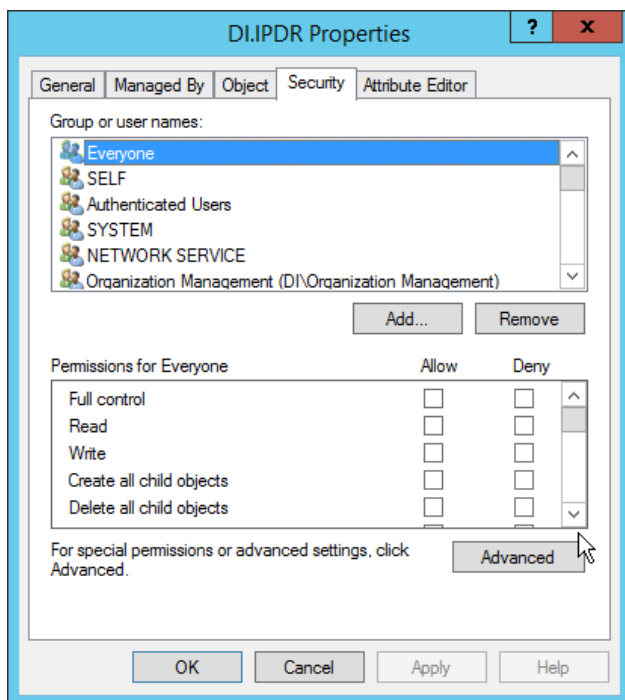


30. Double-click **Everyone**.

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



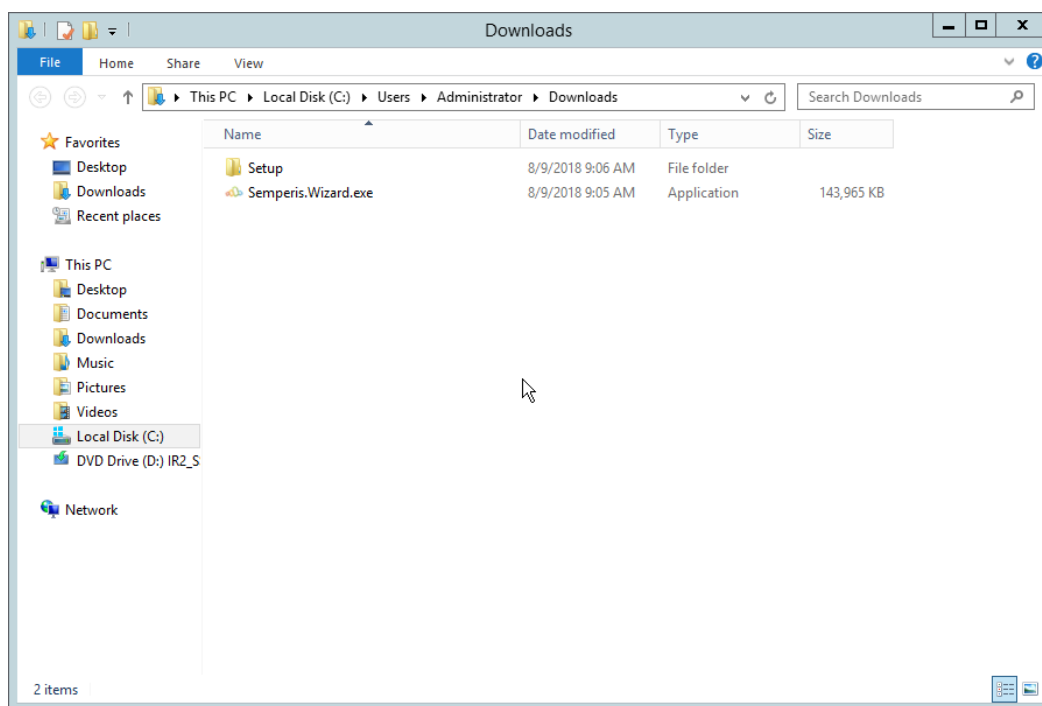
32. Click **OK**.



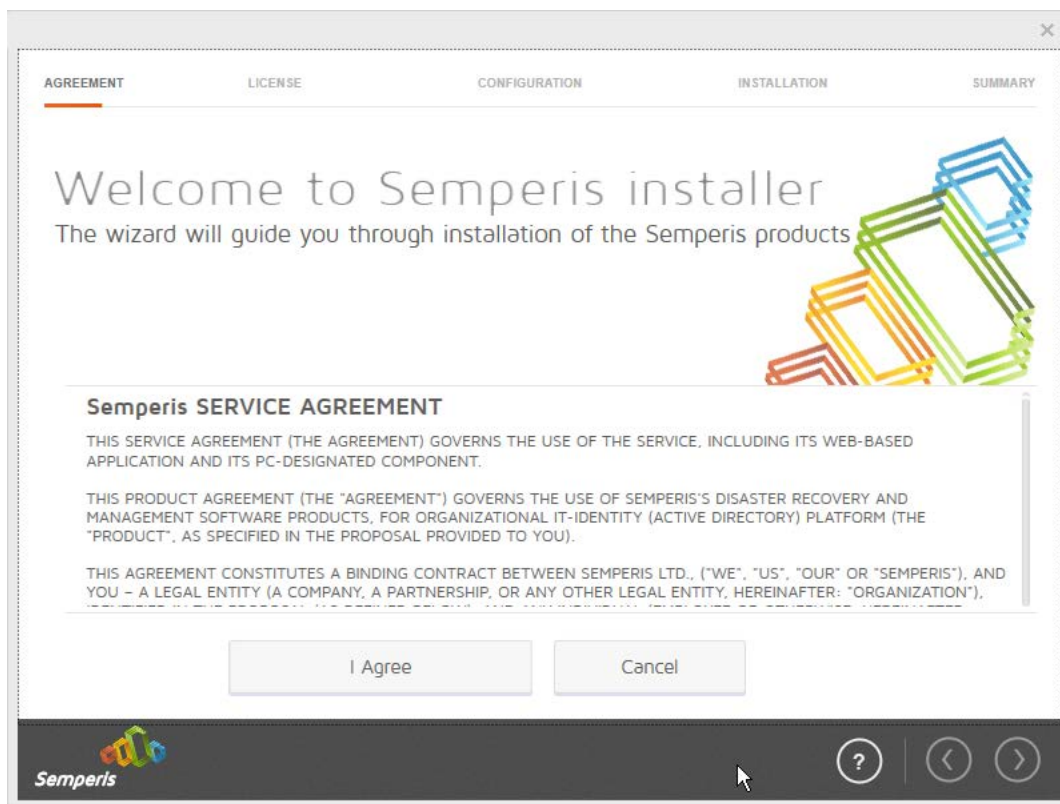
33. Click **OK**.

2.6.2 Install Semperis DSP

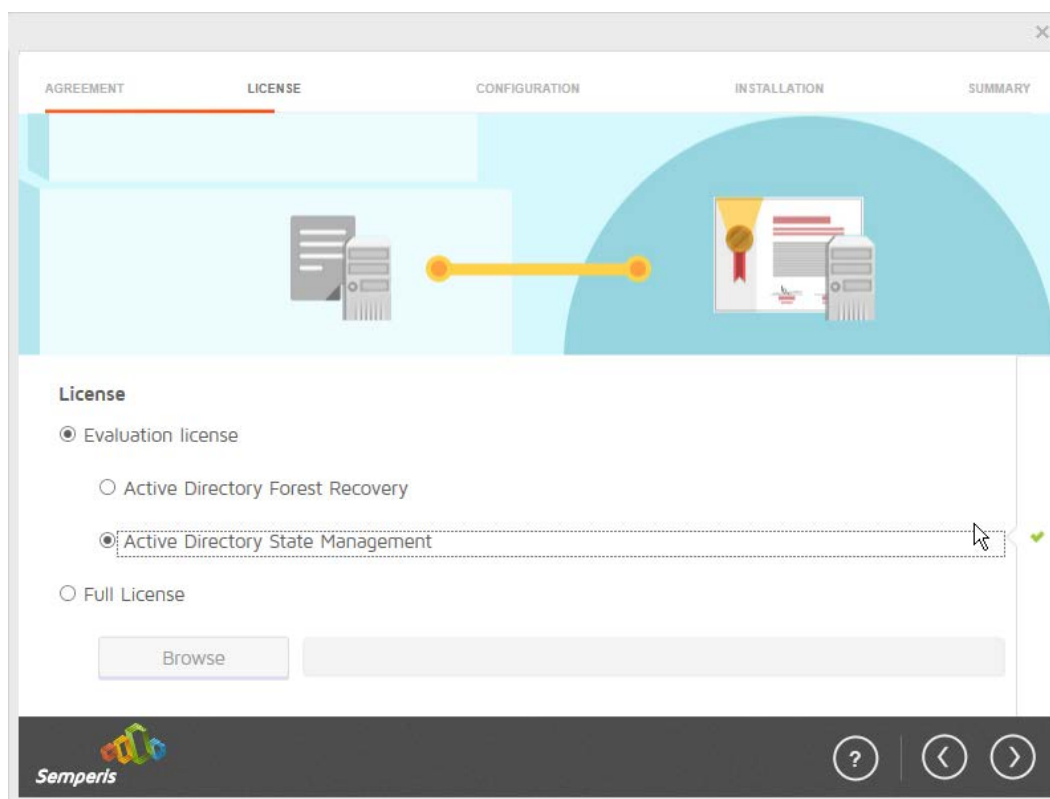
1. If you are using a local SQL Express Advanced server, place the **SQLXPADV_x64_ENU.exe** installer in a directory called *Setup*, and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it). If a SQL Express Advanced server is not being used, no **Setup** folder is required.



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

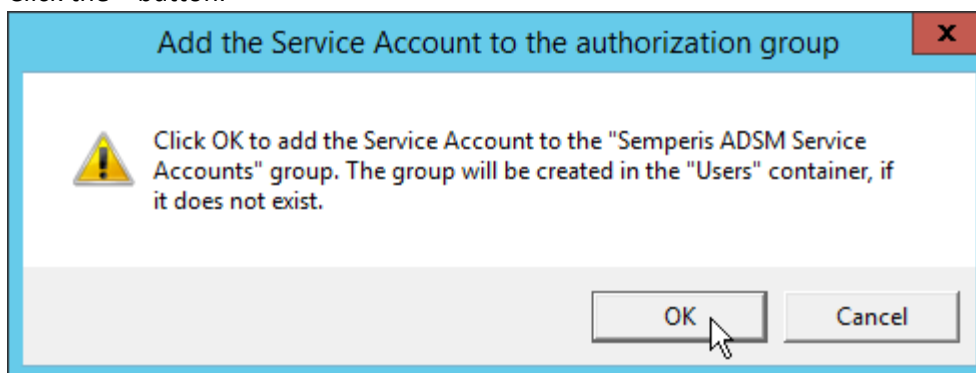


3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory State Management**.

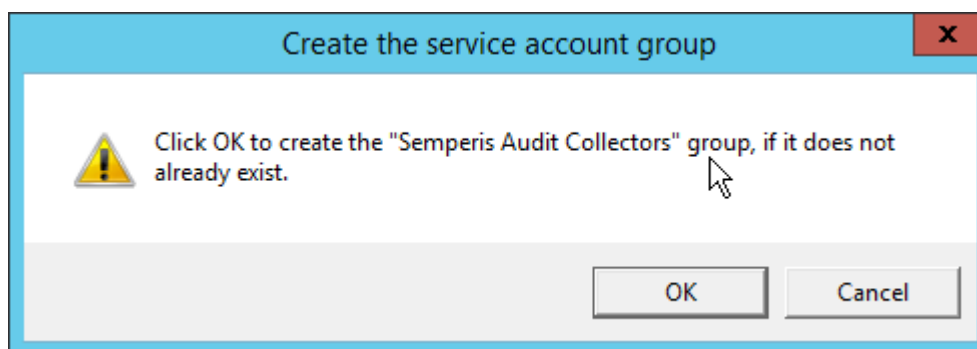


6. Click the > button.
7. Enter the **username** and **password** of the account created earlier.

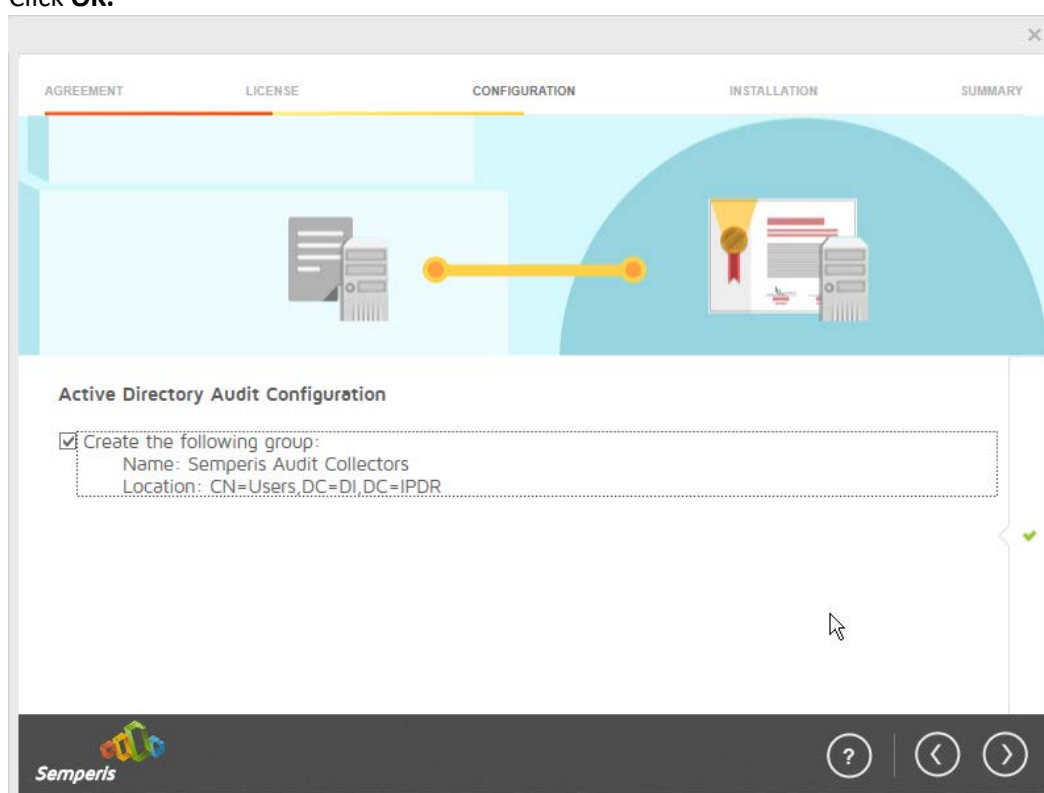
8. Click the > button.



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

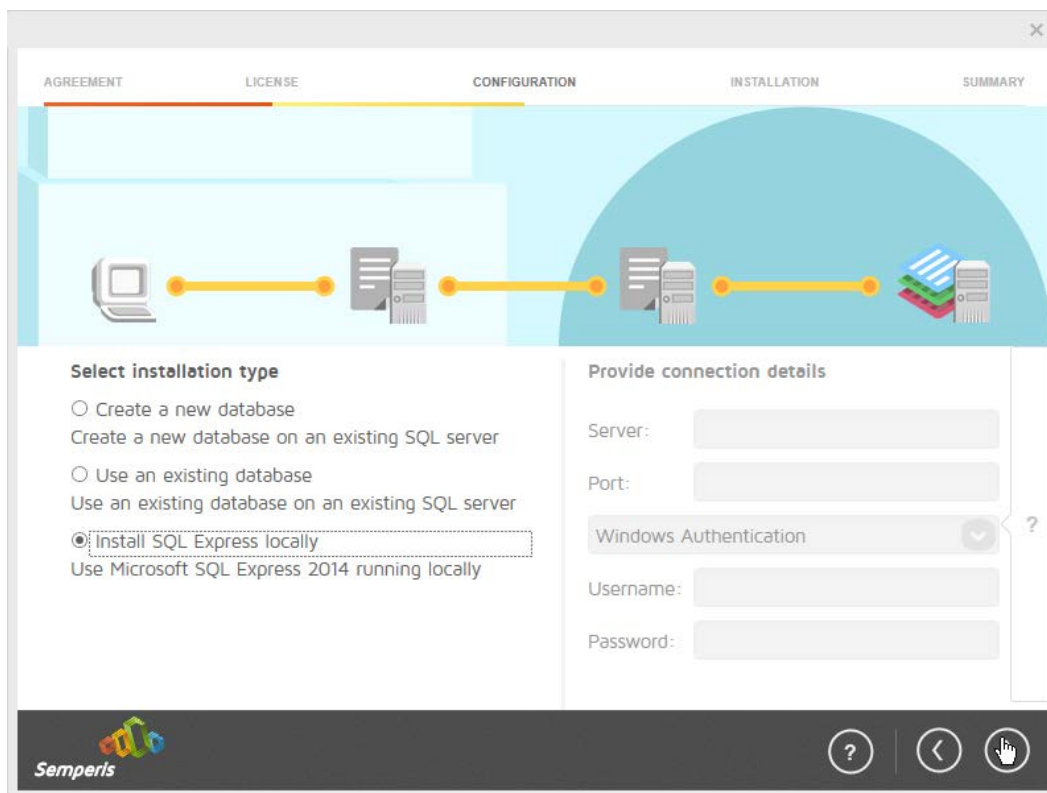


11. Click **OK**.

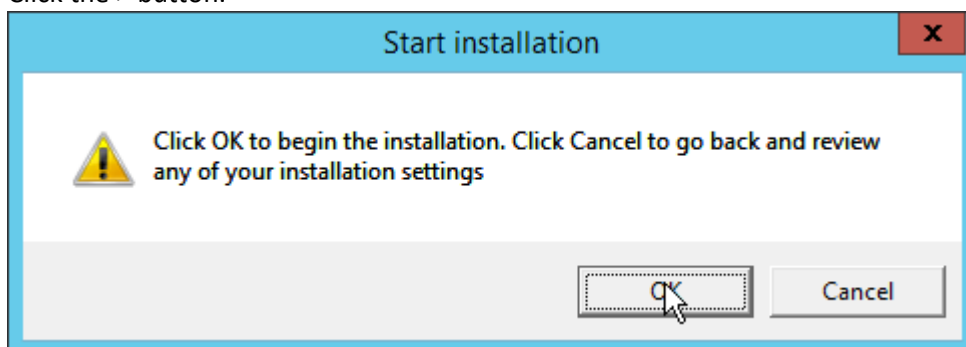


12. Click the **>** button.

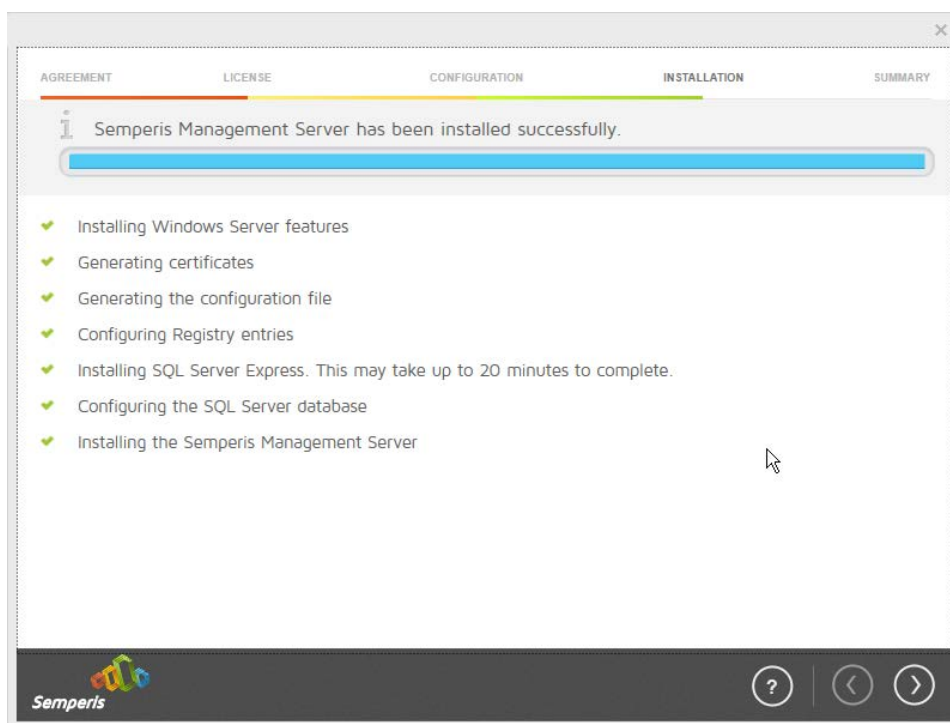
13. Select the appropriate database option, and enter any required information.



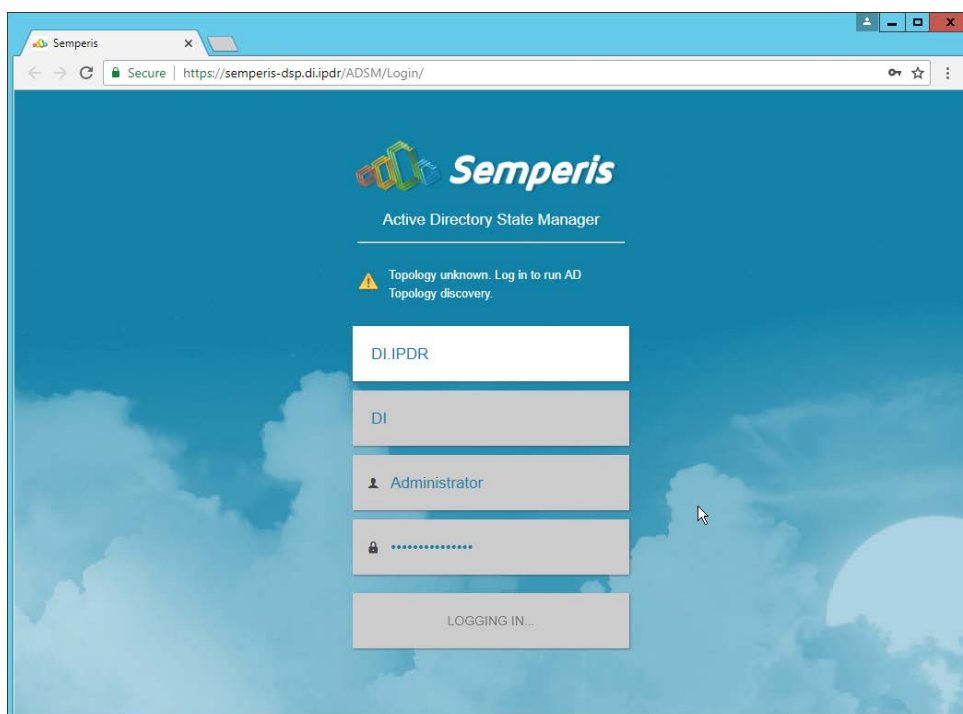
14. Click the > button.



15. Click **OK**.

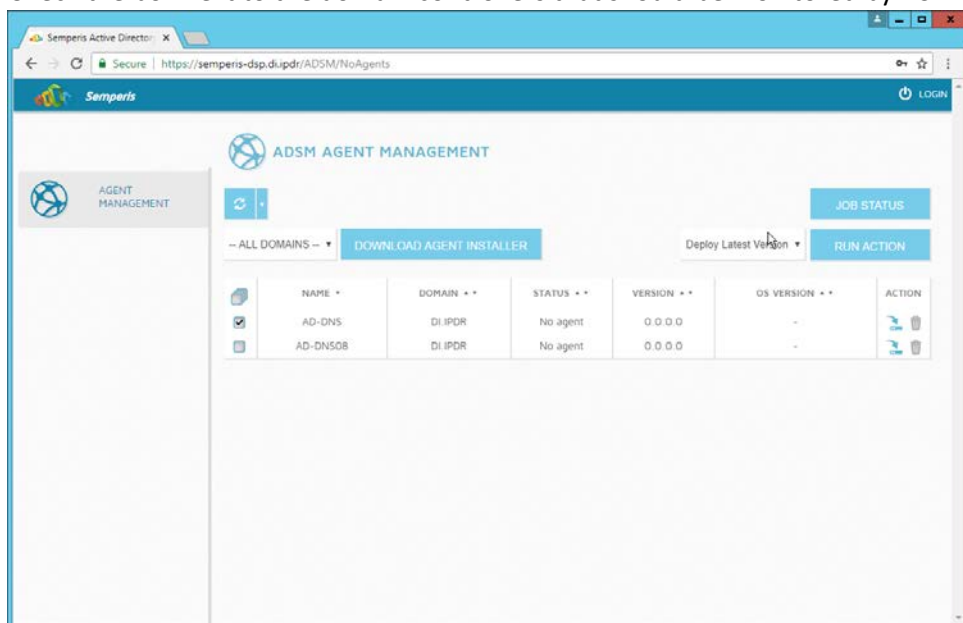


16. Click the > button after the installation completes.
17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector**.
18. On the login page, enter the full domain as well as the NetBIOS name.
19. Enter the **username** and **password** of an administrator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



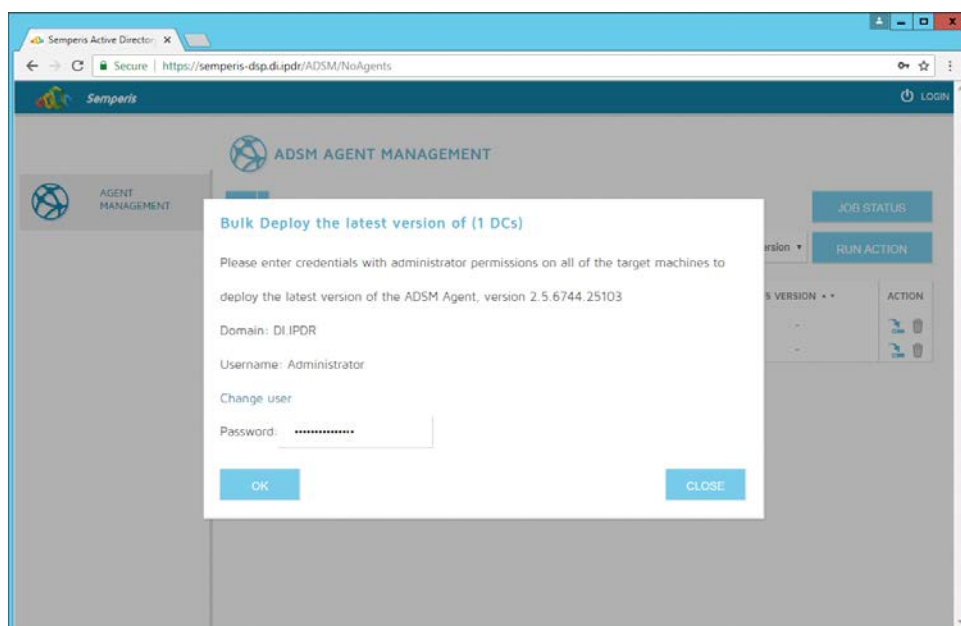
20. Click **Login**.

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

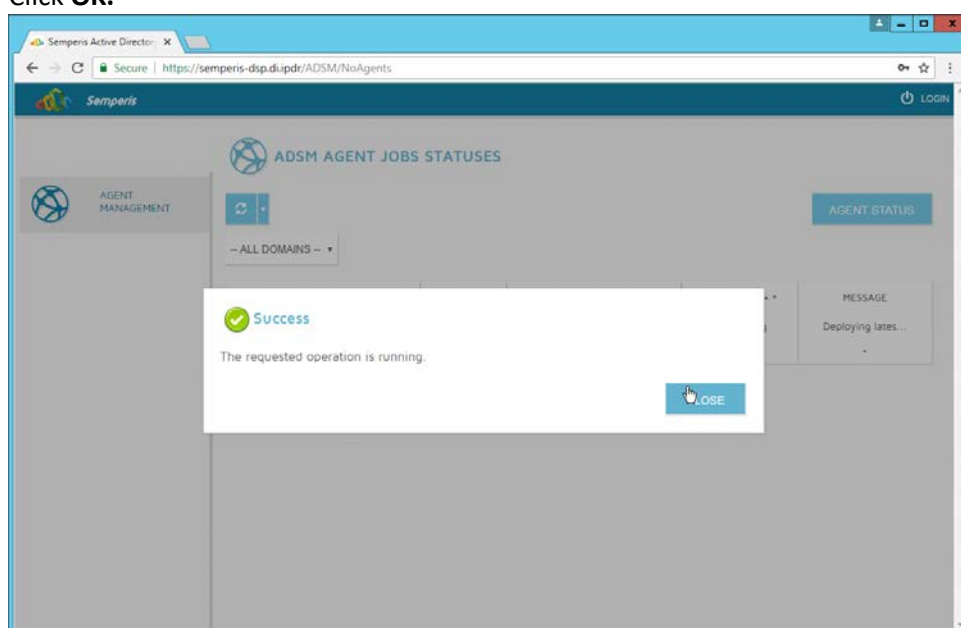


22. Click **Run Action**.

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

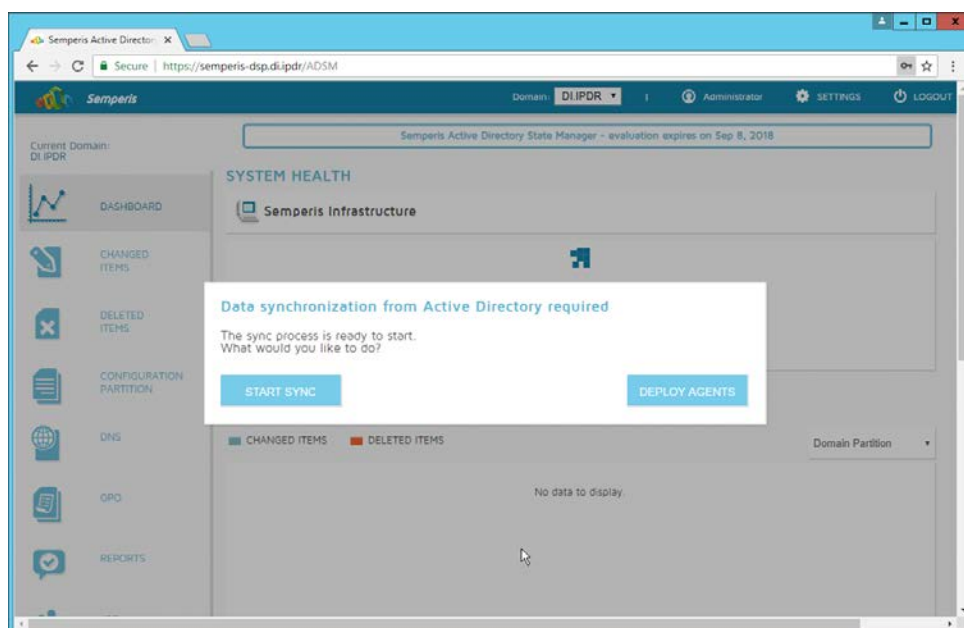


24. Click **OK**.



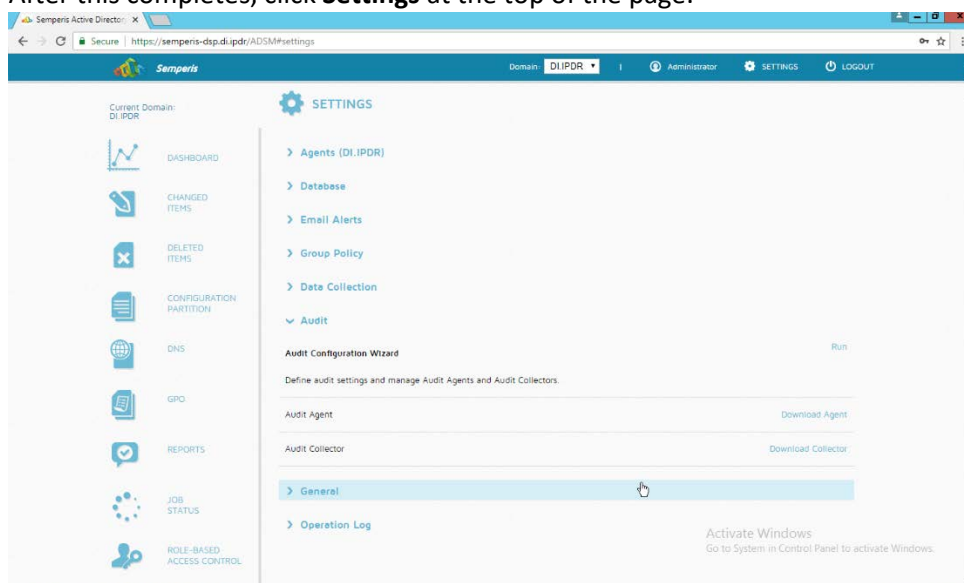
25. Click **Close**.

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



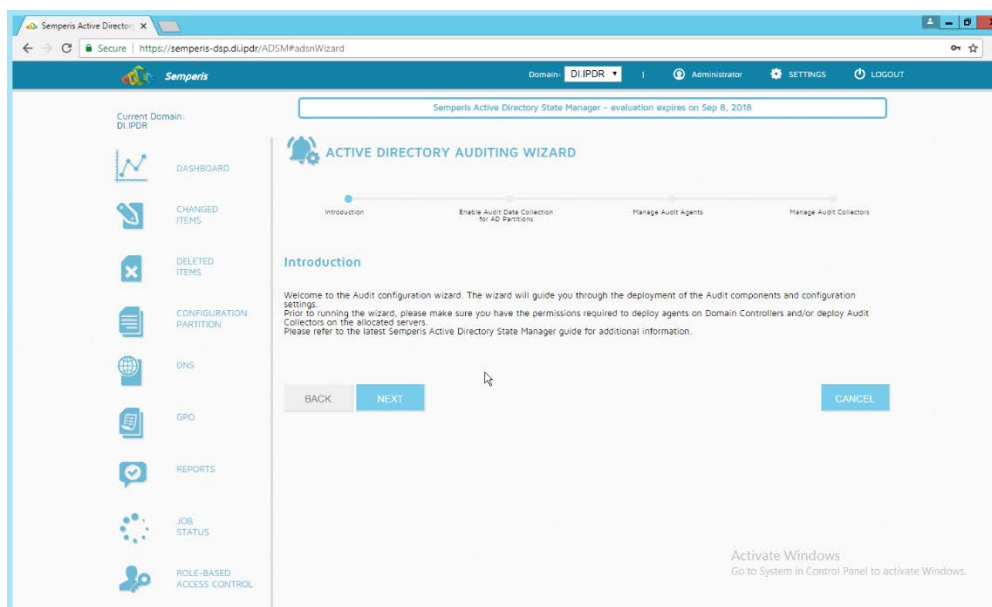
27. Click **Start Sync**.

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

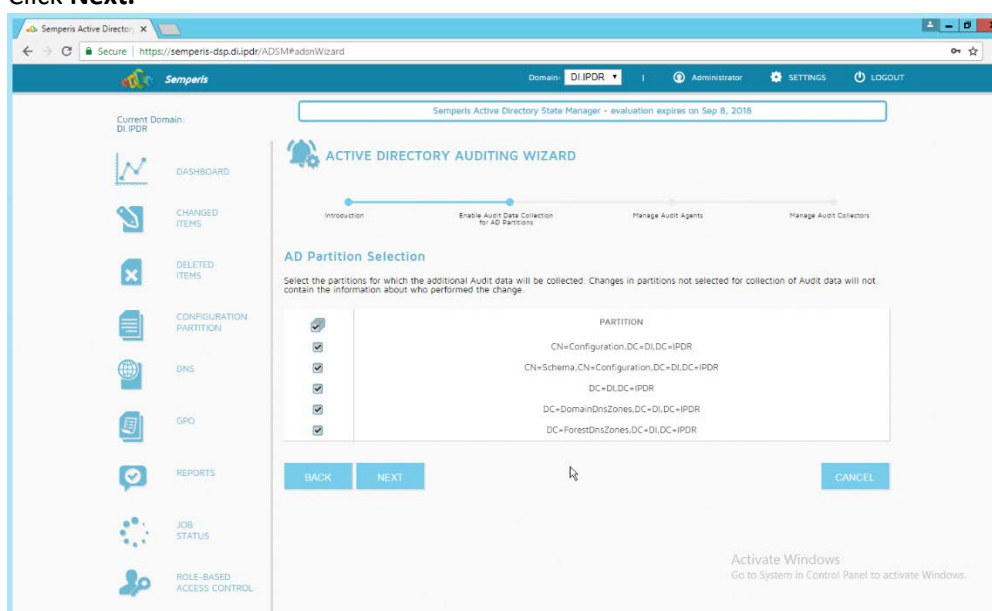


29. Click **Audit**.

30. Click **Run**.

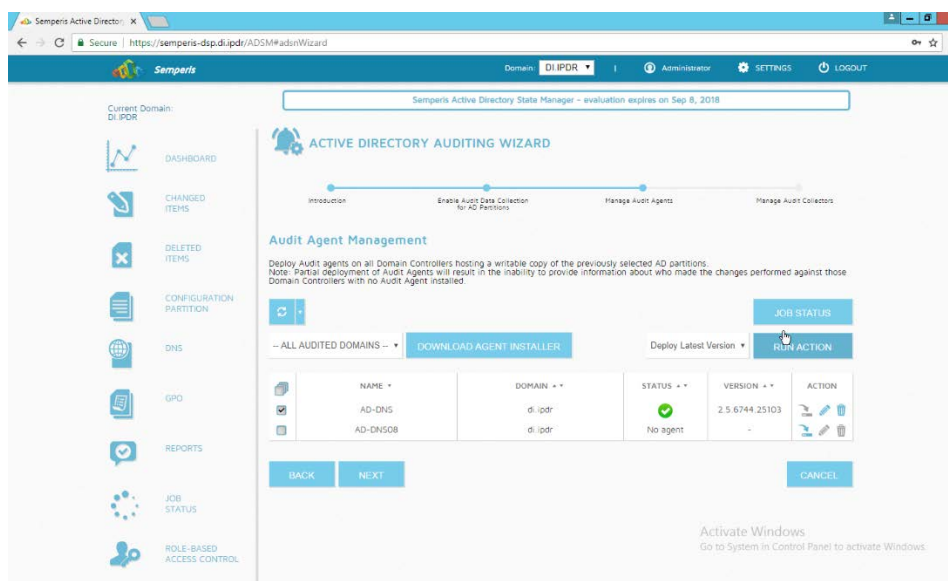


31. Click **Next**.



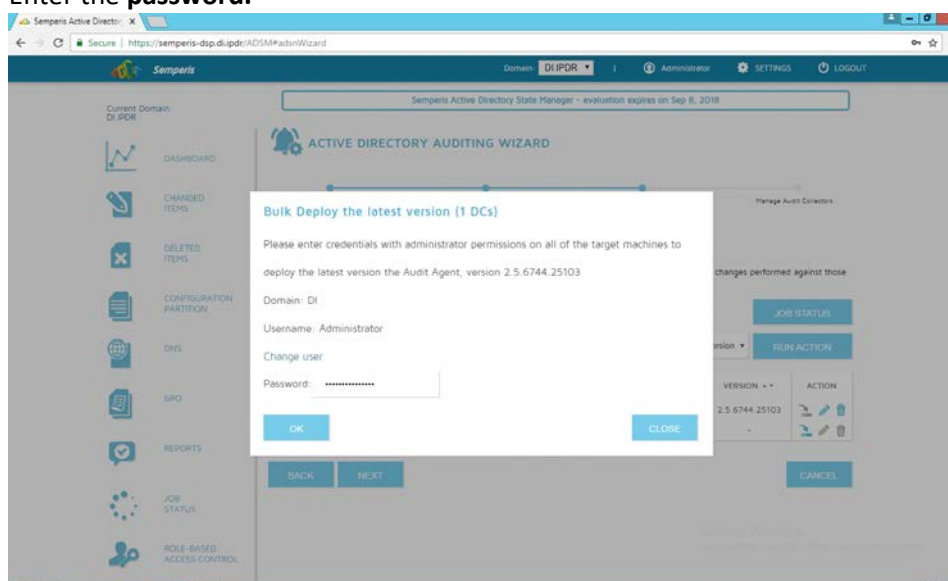
32. Click **Next**.

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



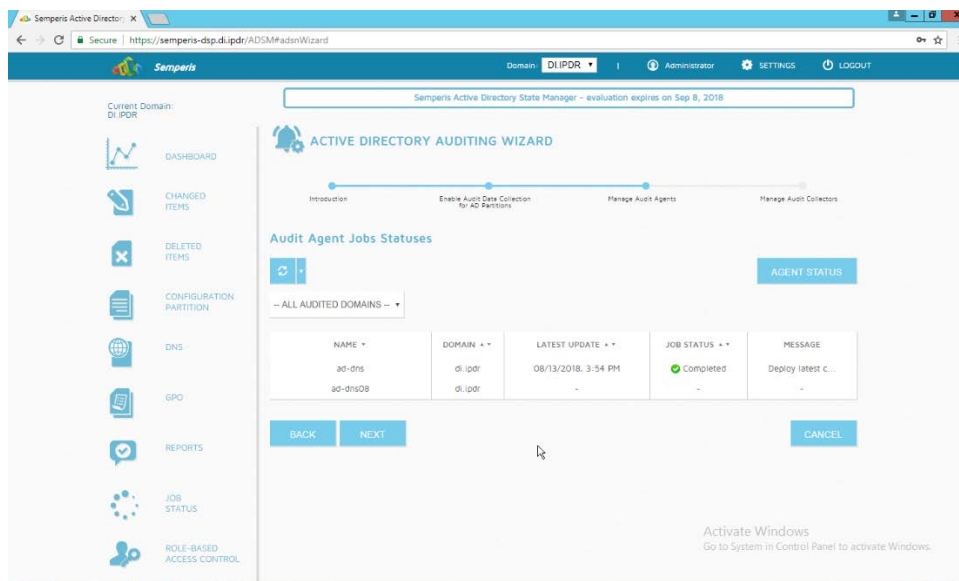
34. Click **Run Action**.

35. Enter the **password**.

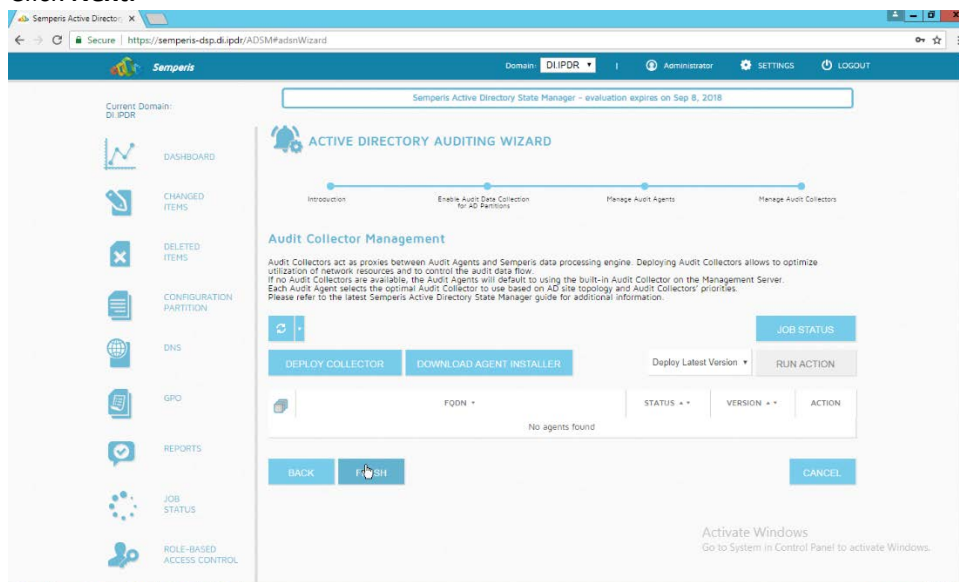


36. Click **OK**.

37. Wait for the deployment to finish.



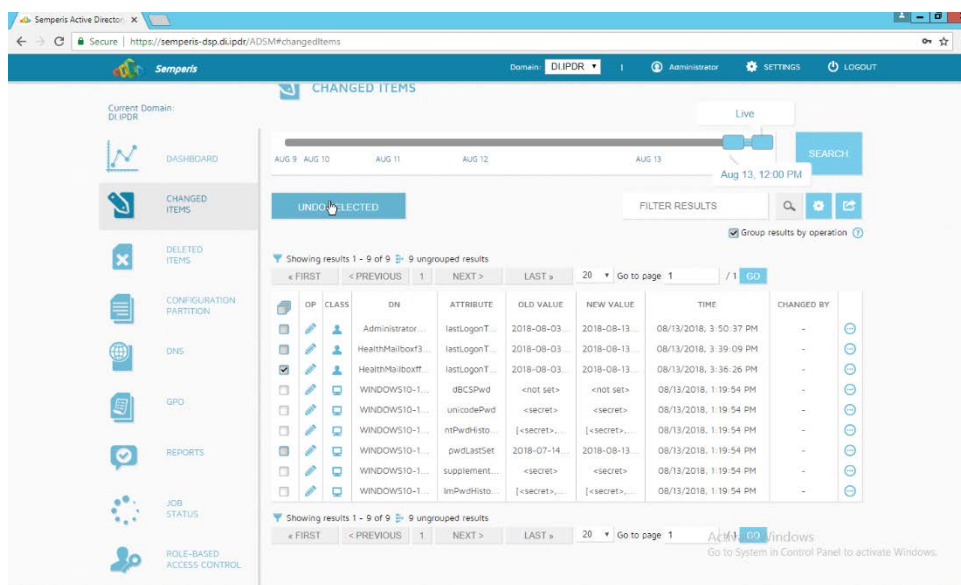
38. Click **Next**.



39. Click **Finish**.

2.6.3 Roll Back Changes with Semperis DSP

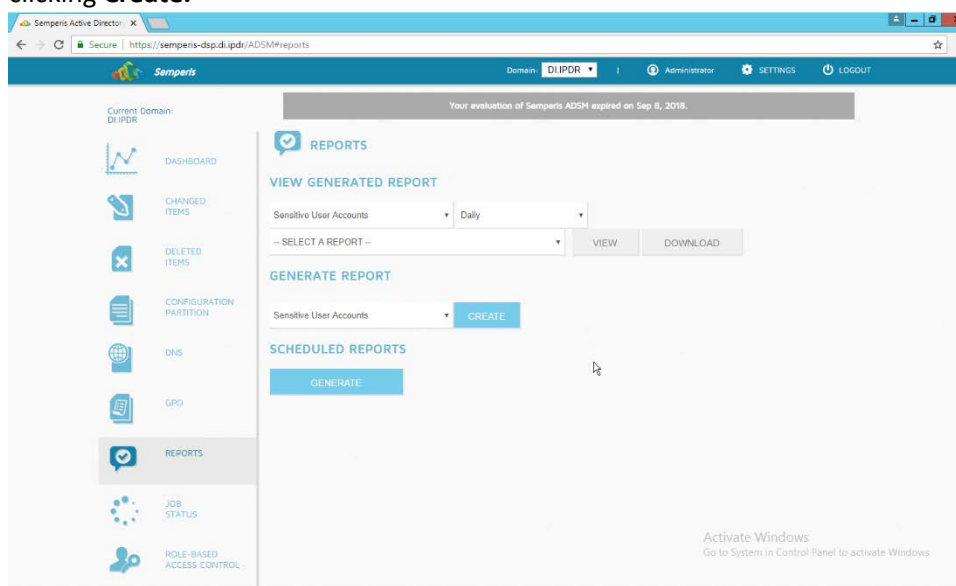
1. Go to **Changed Items** on the left navigation bar.
2. Check the box next to any undesired Active Directory changes.
3. Click the ... button to view more details about the change.



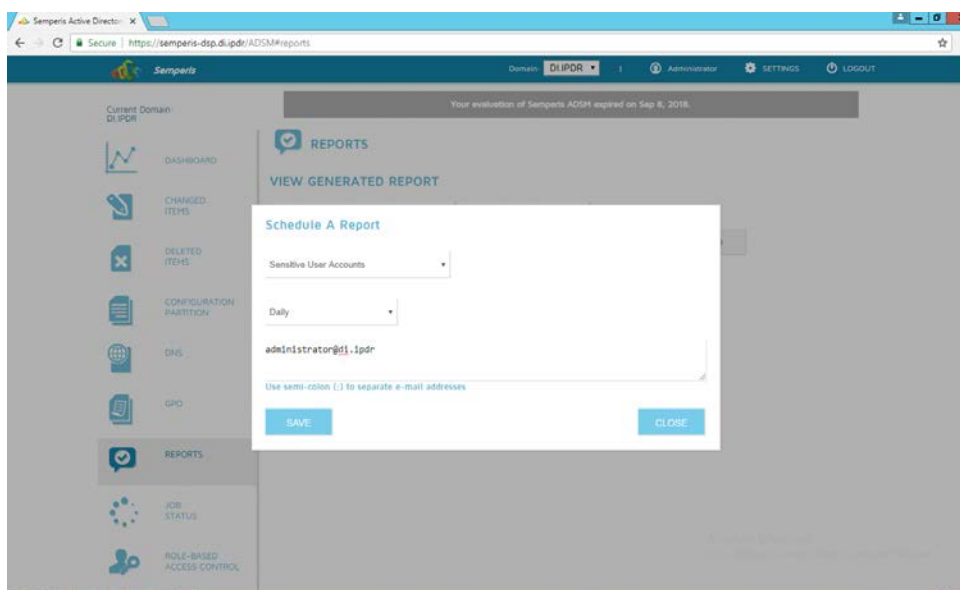
4. Click **Undo Selected** to roll back these changes.

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**.



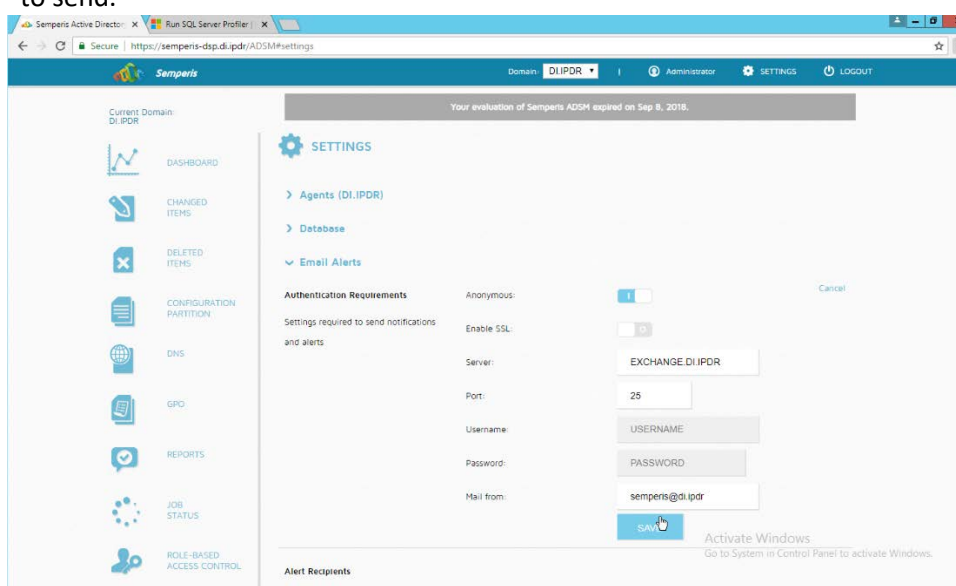
3. Under **Scheduled Reports**, click **Generate** to automatically email specific reports.
4. Select a report type and a schedule.
5. Enter the email addresses of anyone who should receive this report.



6. Click **Save**.

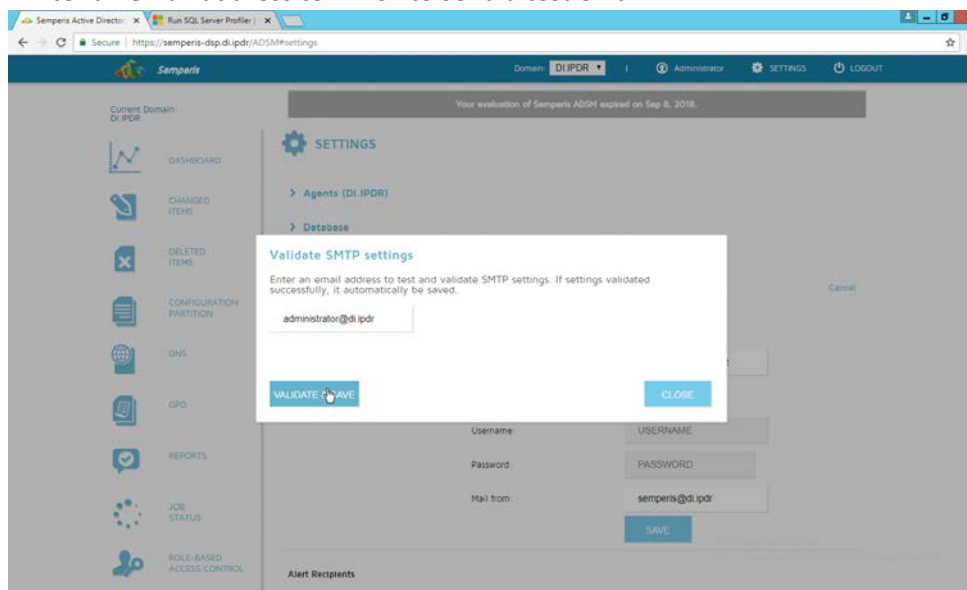
2.6.5 Configure Email Alerts with Semperis DSP

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.

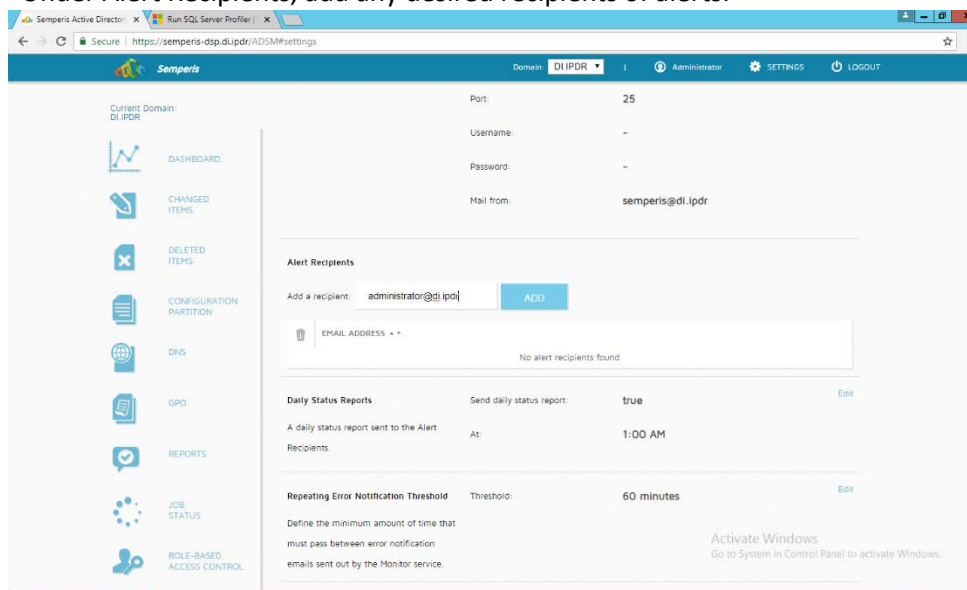


5. Click **Save**.

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.

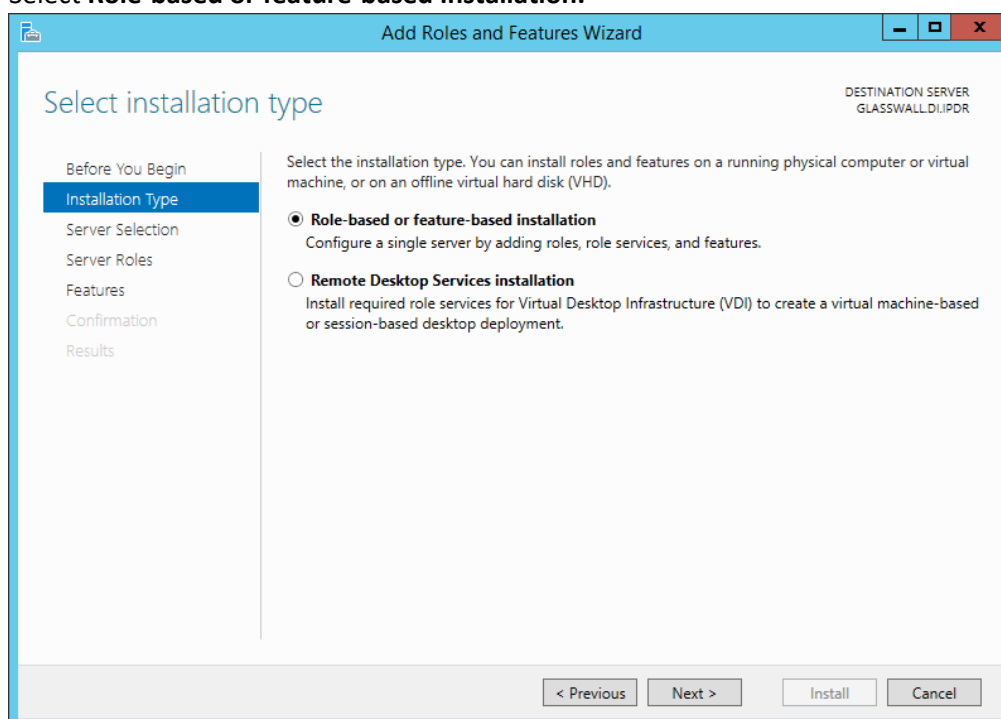
2.7 Glasswall FileTrust™ for Email

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.

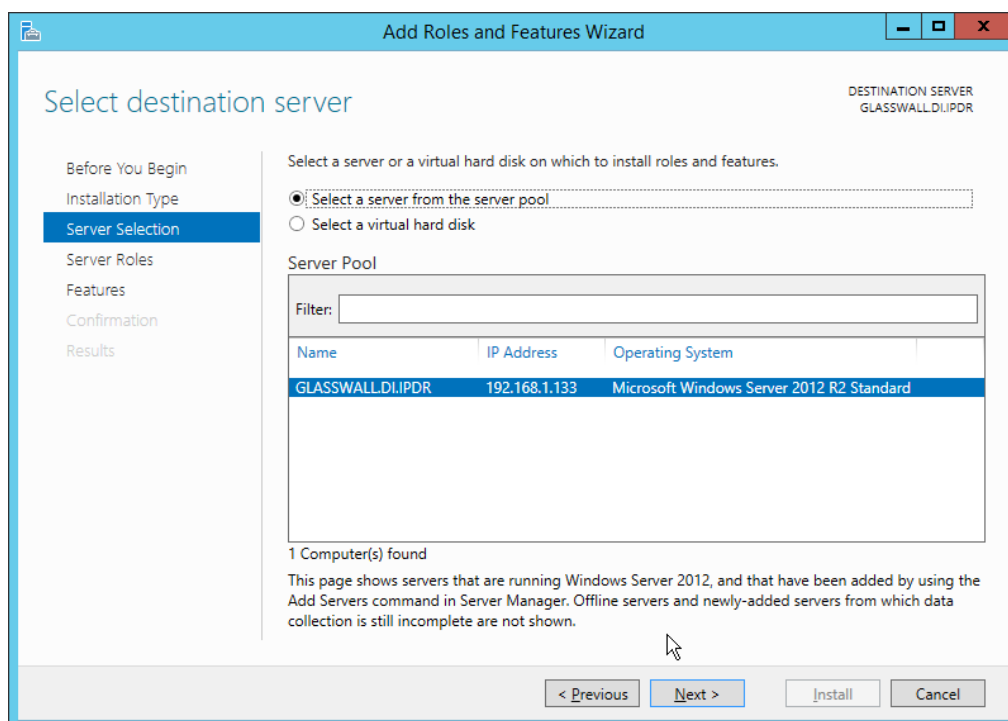
2.7.1 Install Prerequisites

2.7.1.1 *Install the IIS web server*

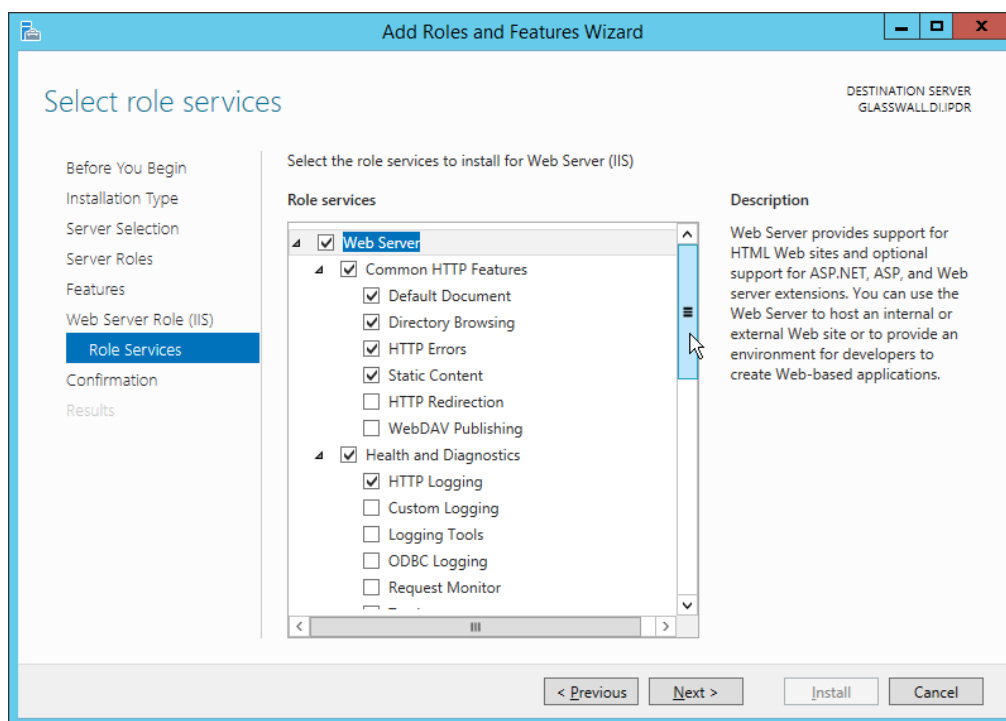
1. In **Server Manager**, click **Add Roles and Features**.
2. Click **Next**.
3. Select **Role-based or feature-based installation**.



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**.



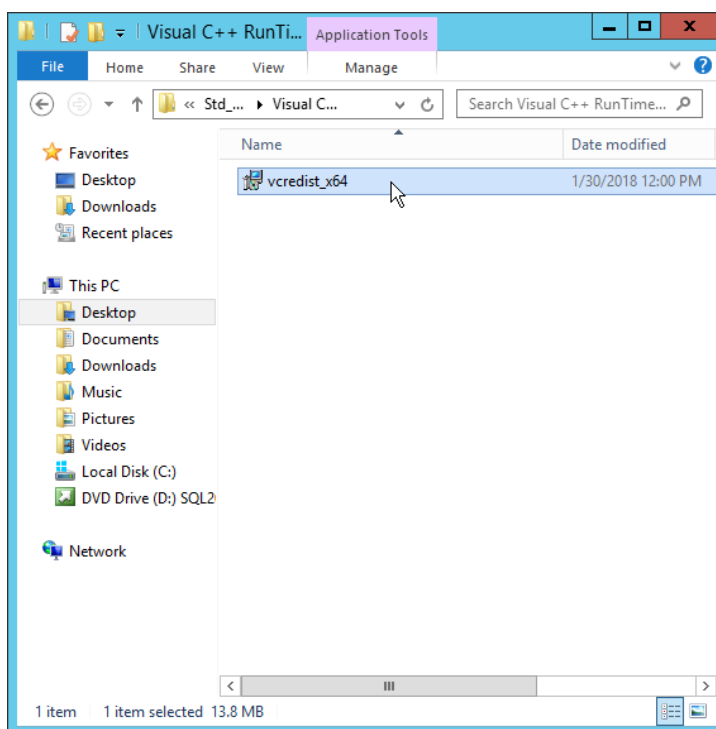
12. Click **Next**.
13. Check the box next to **Restart the destination server automatically if required**.
14. Click **Install**.

2.7.1.2 *Install Microsoft SQL 2014 Enterprise*

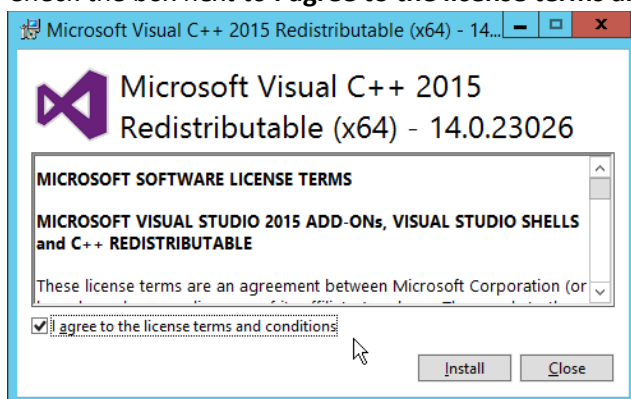
Please see [Section 2.4](#) for an installation guide for MS SQL 2014; for simplicity it should be installed on the same server as Glasswall FileTrust. Ensure that Mixed Mode authentication is selected when installing.

2.7.1.3 *Install Microsoft Visual C++ 2015*

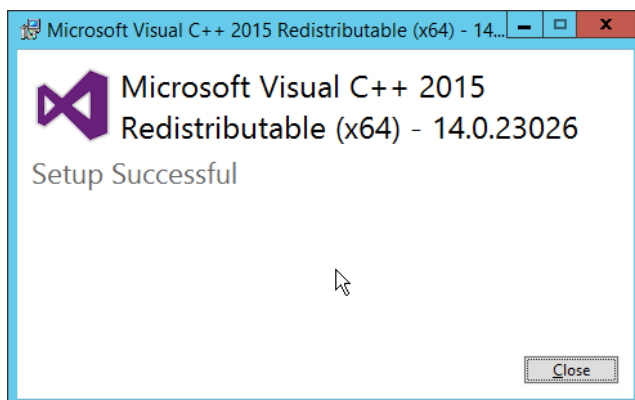
1. Run the **vcredist_x64** installer.



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



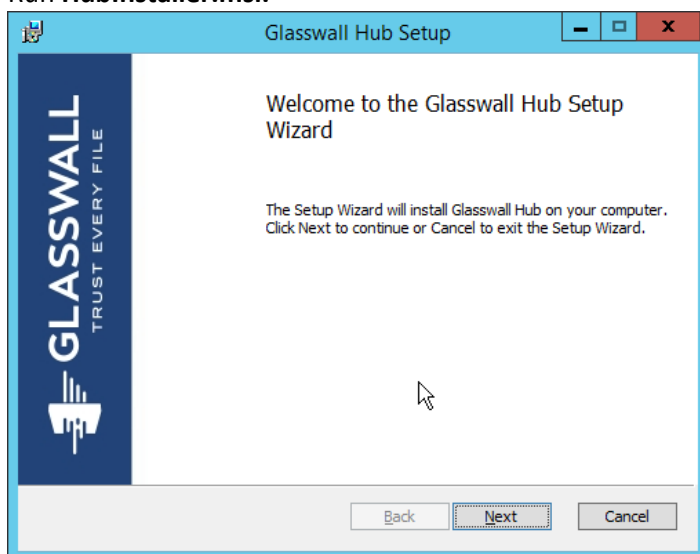
3. Click **Install**.
4. After the installation is complete, click **Close**.



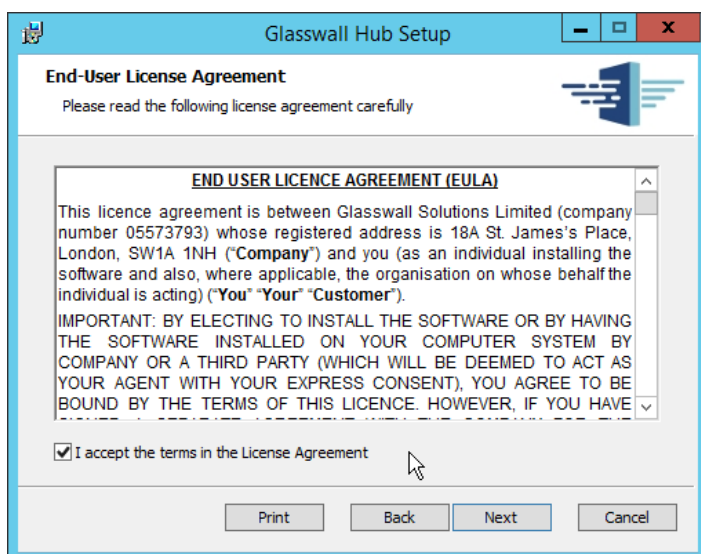
2.7.2 Install the Glasswall FileTrust Server Component

2.7.2.1 *Install Glasswall Hub*

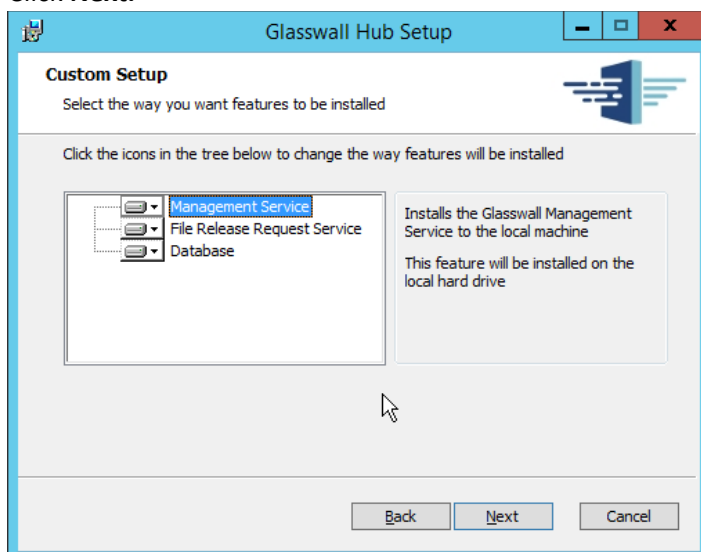
1. Run **HubInstaller.msi**.



2. Click **Next**.



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



5. Click **Next**.
6. 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).

Glasswall Hub Setup

Database Configuration

Specify the Glasswall Database Configuration

Database Server: localhost

Database Name: HubDatabase

Database Login: GWDBUser

Database Password: [Masked]

Back Next Cancel

9. Click **Next**.

10. Select **Windows Authentication**.

Glasswall Hub Setup

Database Installation Settings

Specify the Installation Setting for the Glasswall Database

Database Administrator Credentials

Configure the credentials that will be used to create the database (all fields required)

Authentication Method: Windows Authentication

User name: [Empty]

Password: [Empty]

Database Installation Log File

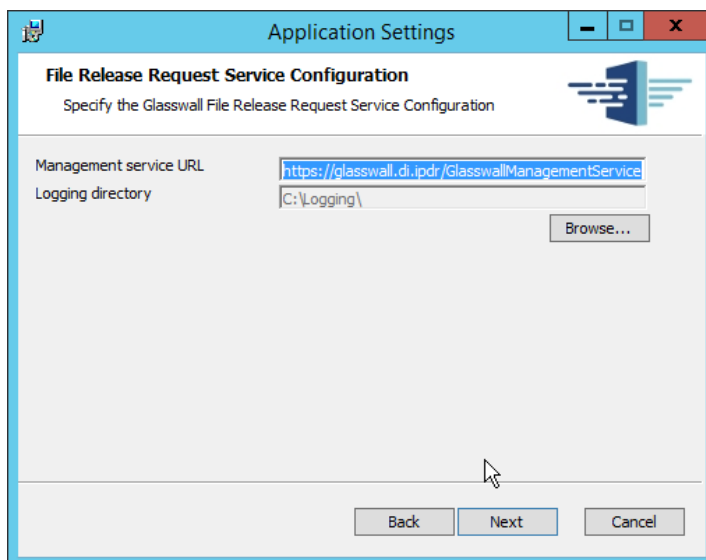
Location of the database installation log file

Installation Log File: C:\Logging\gw-Database-Install.log

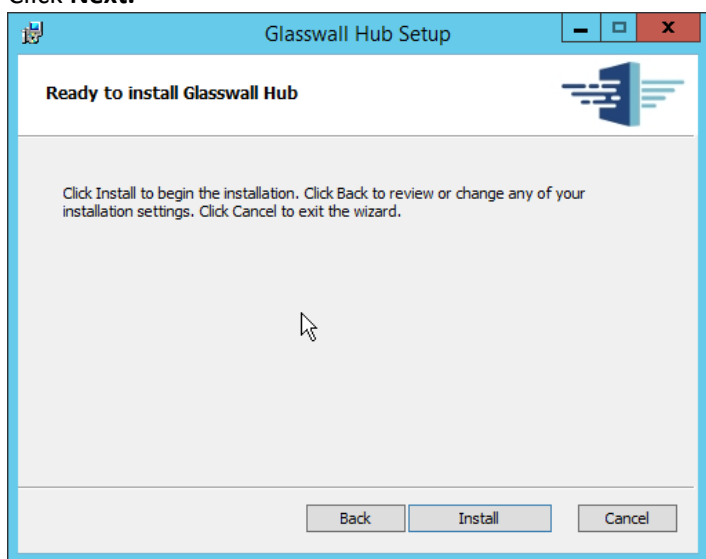
Back Next Cancel

11. Click **Next**.

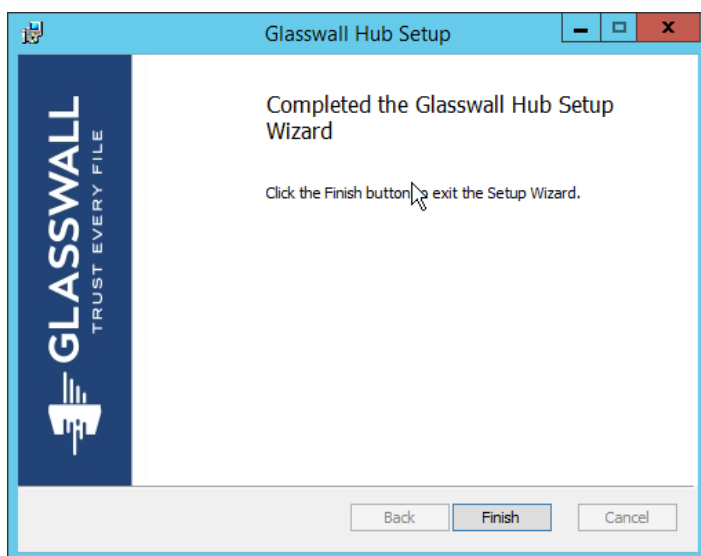
12. Replace the domain of the **management service URL** with the address of the current machine, such as **glasswall.di.ipdr**.



13. Click **Next**.



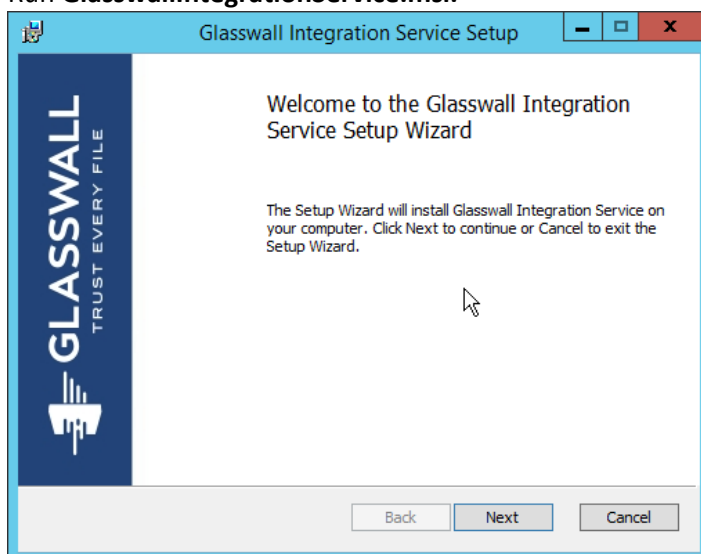
14. Click **Install**.



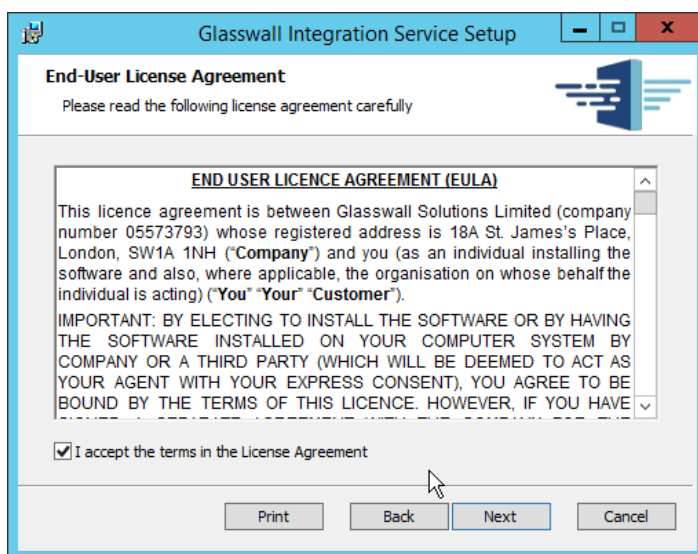
15. Click **Finish**.

2.7.2.2 *Install Glasswall Integration Service*

1. Run **GlasswallIntegrationService.msi**.



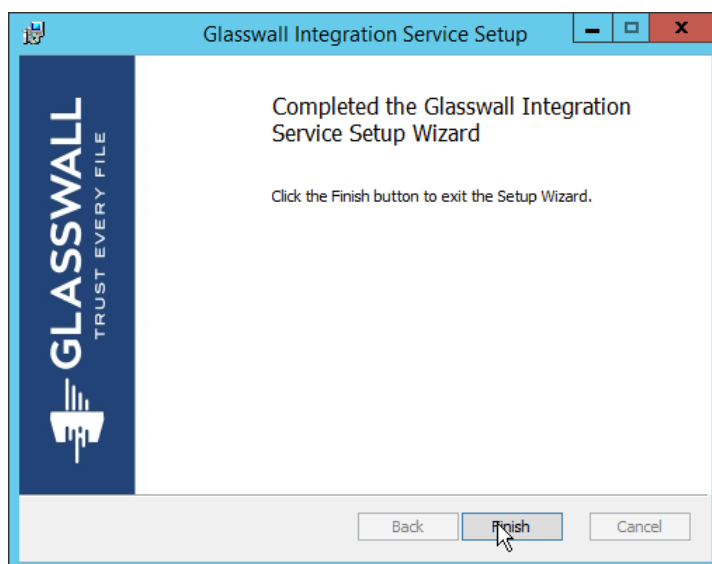
2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



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 Smtip Mail From**.
8. Enter the **address** for the mail server for **Notifications Smtip Host**.
9. Enter a **port** (**25** is used here) for **Notifications Smtip Port**.

10. Click **Next**.

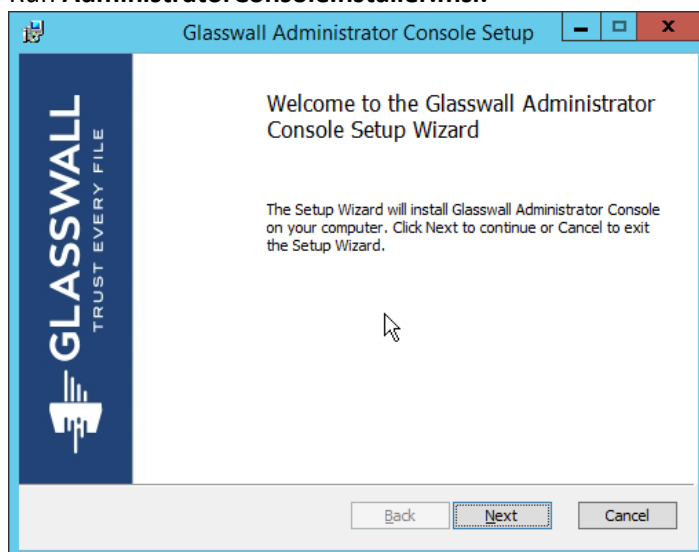
11. Click **Install**.



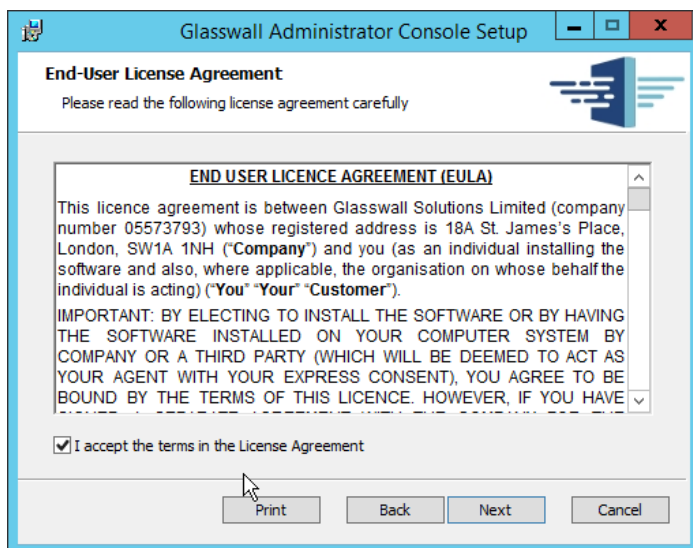
12. Click **Finish**.

2.7.2.3 *Install Glasswall Administrator Console*

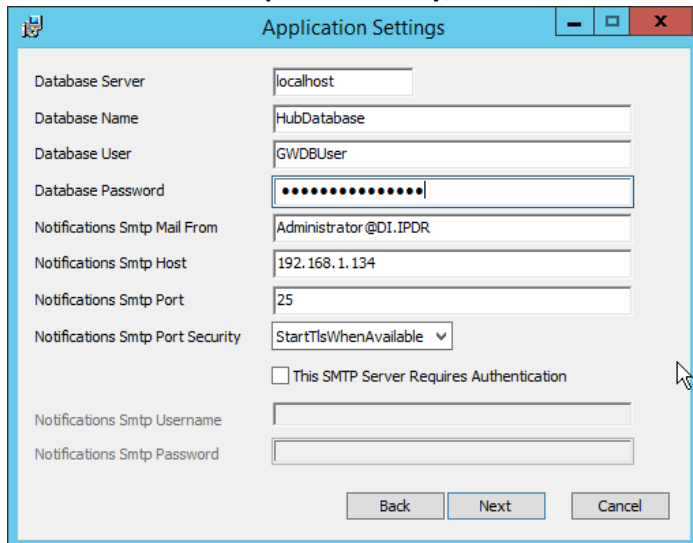
1. Run **AdministratorConsoleInstaller.msi**.



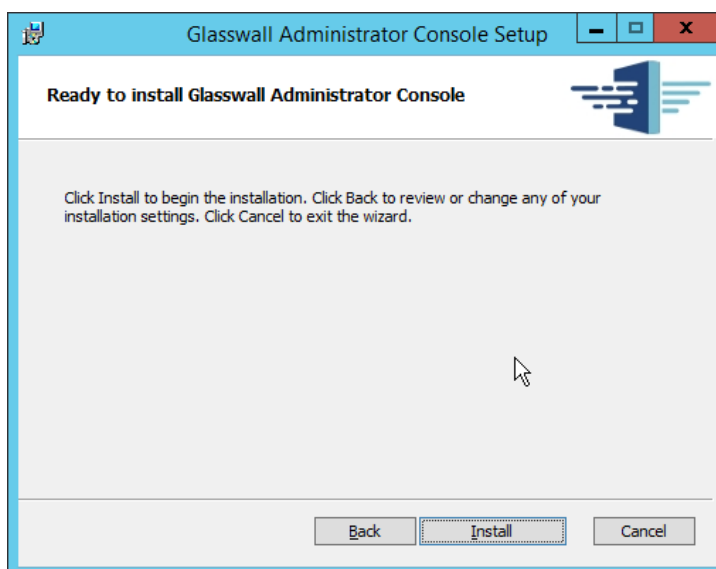
2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



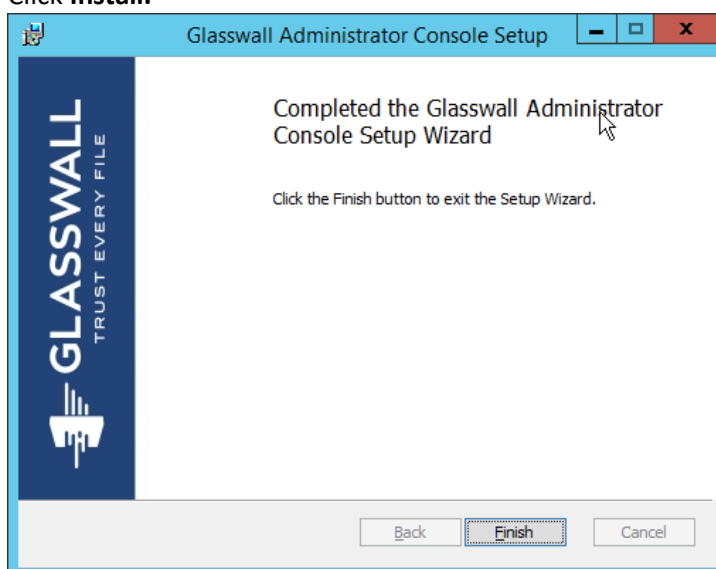
4. Click **Next**.
5. For **Database Server**, **Database Name**, **Database User**, and **Database Password**, enter the information entered in the **Glasswall Hub Installer**.
6. For **Notifications Smtip Mail From**, **Notifications Smtip Host**, **Notifications Smtip Port**, enter the information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



8. Click **Next**.



9. Click **Install**.

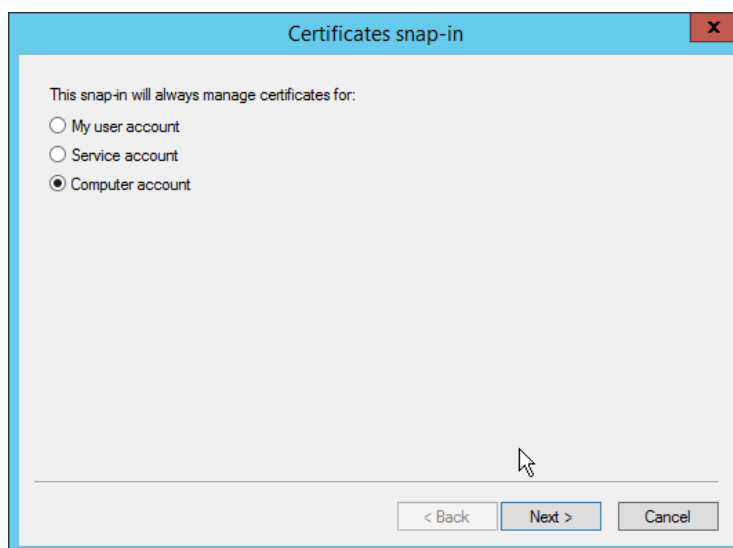


10. Click **Finish**.

2.7.2.4 *Add the Server's Certificate*

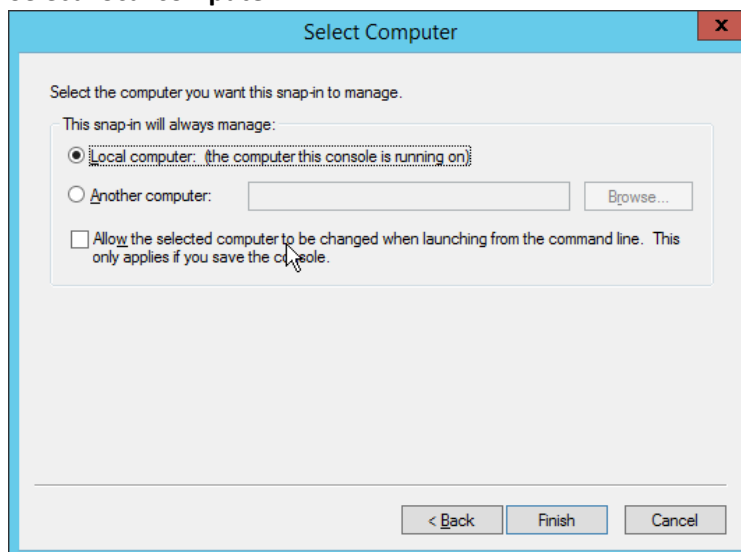
1. For the purposes of this build, a self-signed certificate is used, but this is dependent on the needs of the organization. Ensure that the certificate used is issued to the domain, such as ***.di.ipdr**.
2. Open **mmc**.
3. Click **File > Add/Remove Snap-In....**
4. Select **Certificates** from the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

5. Select **Computer Account**.

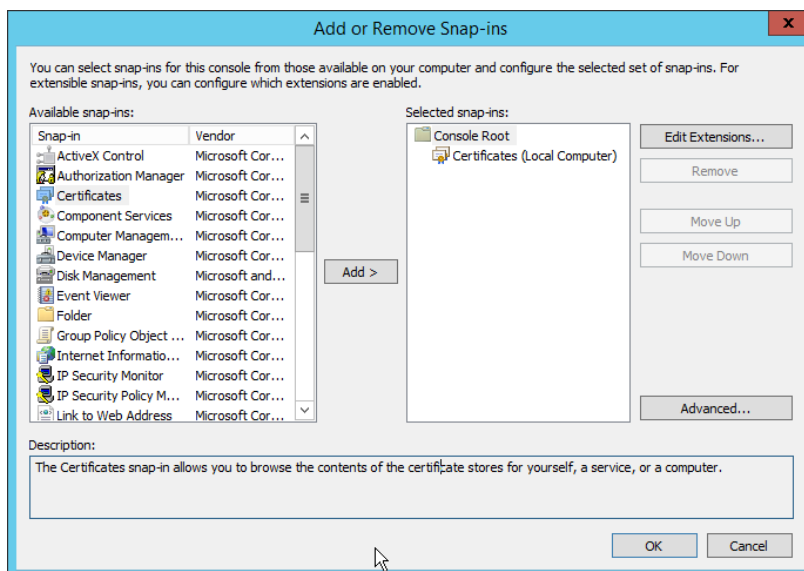


6. Click **Next**.

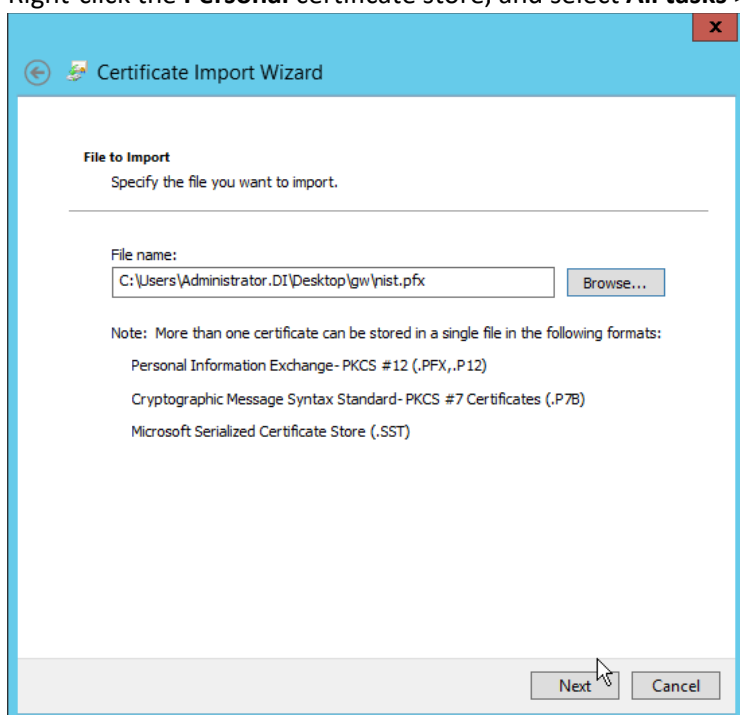
7. Select **Local computer**.



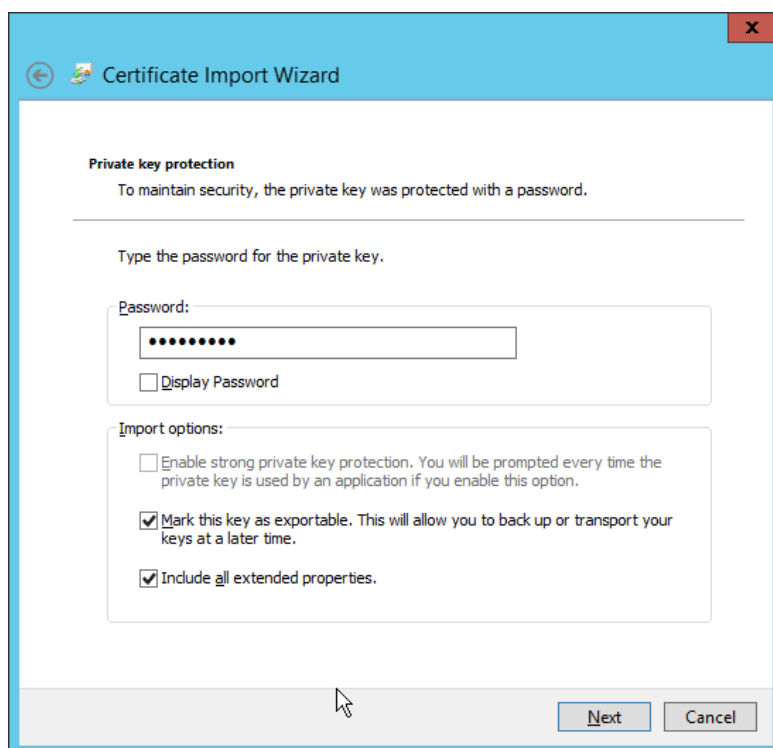
8. Click **Finish**.



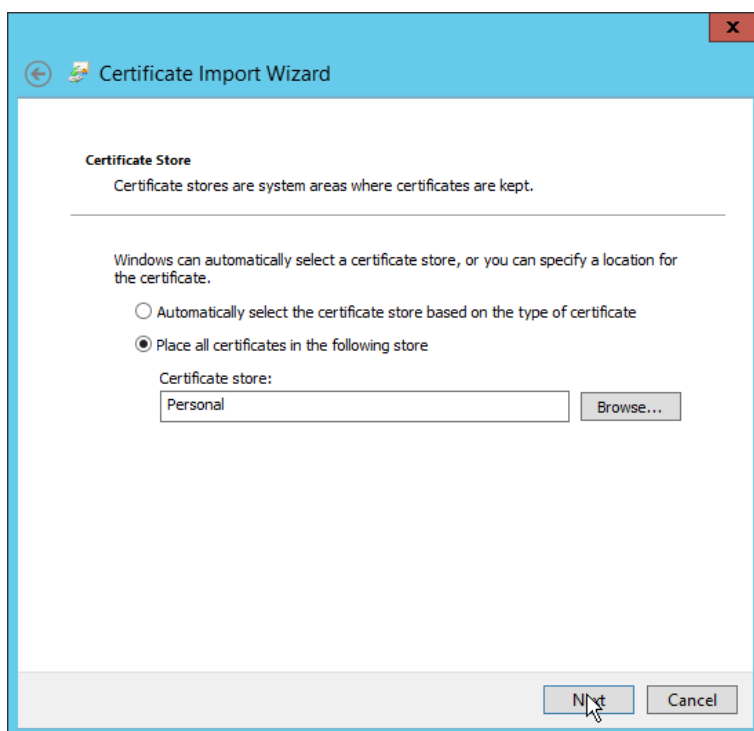
9. Click **OK**.
10. Right-click the **Personal** certificate store, and select **All tasks > Import....**



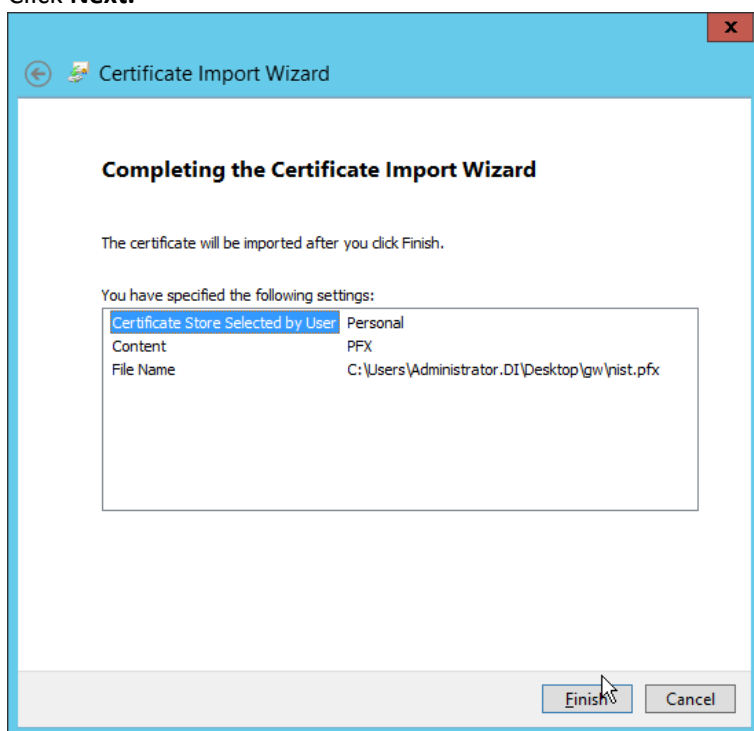
11. Enter the **file name** of the certificate.
12. Click **Next**.
13. Enter the **password** for the certificate.
14. Check the box next to **Mark this key as exportable**.



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

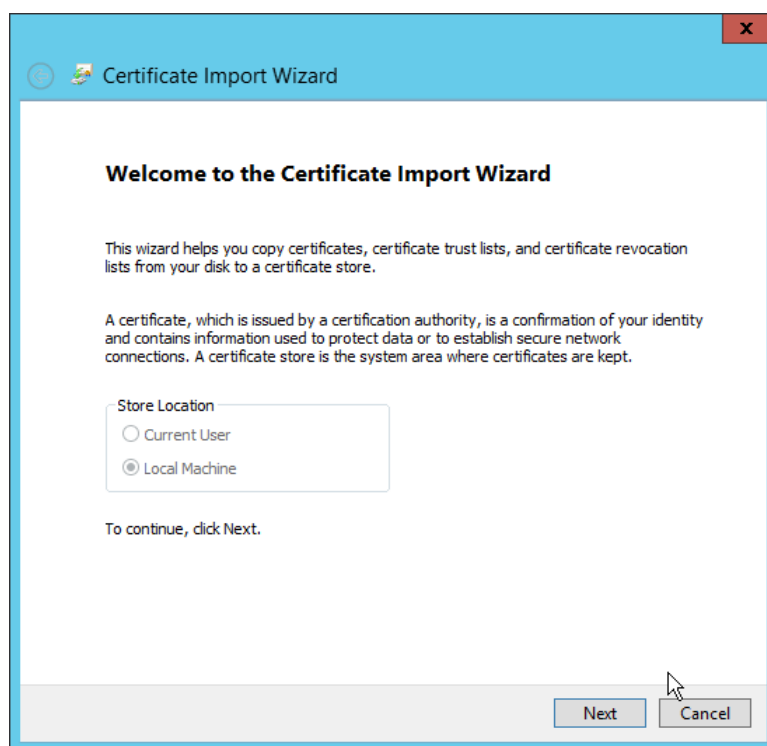


17. Click **Next**.



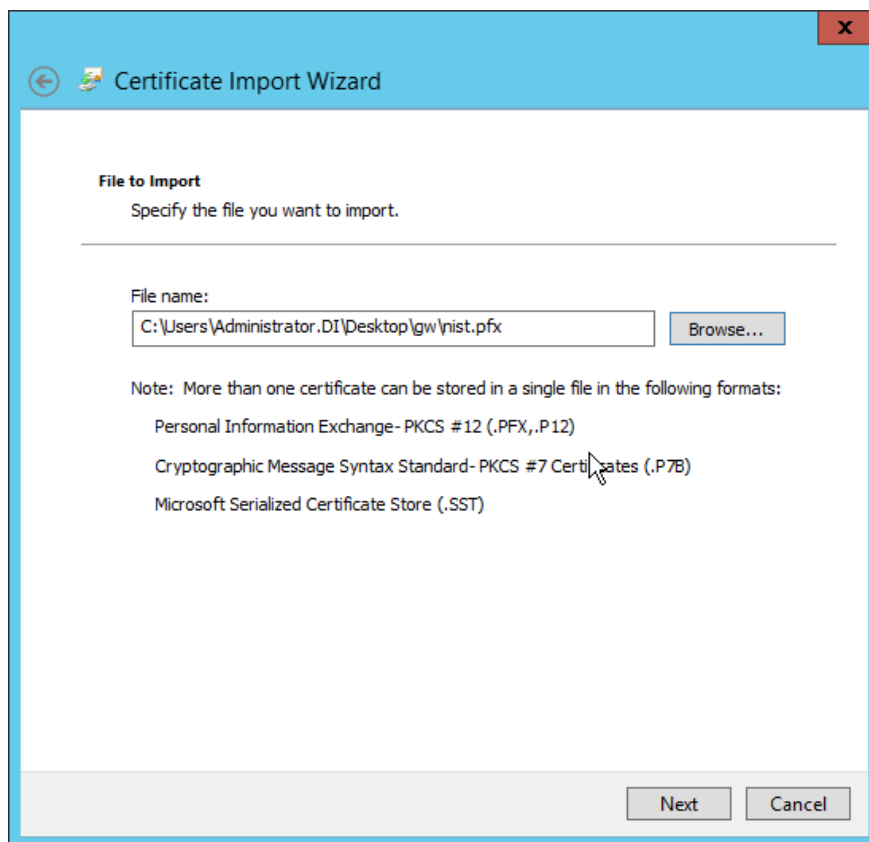
18. Click **Finish**.

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

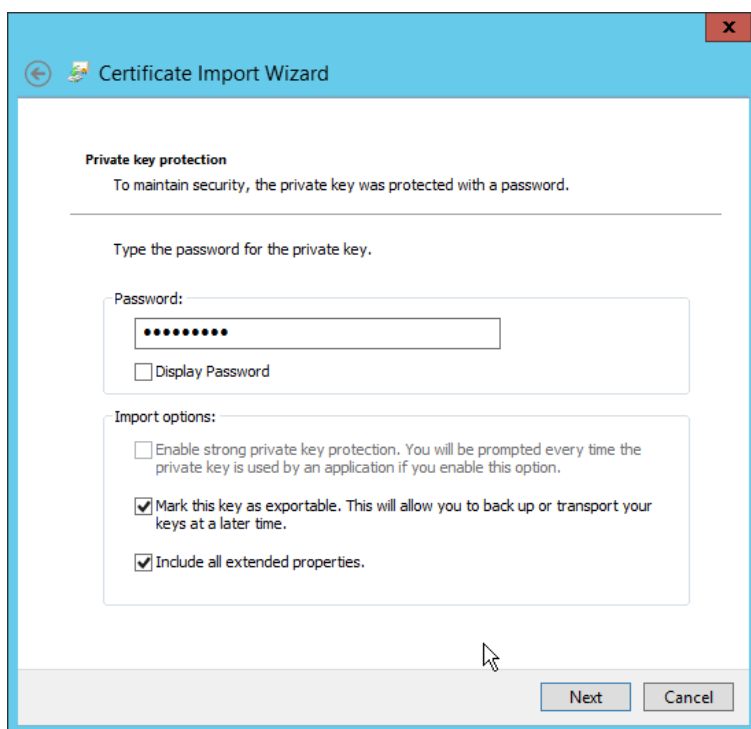


20. Click **Next**.

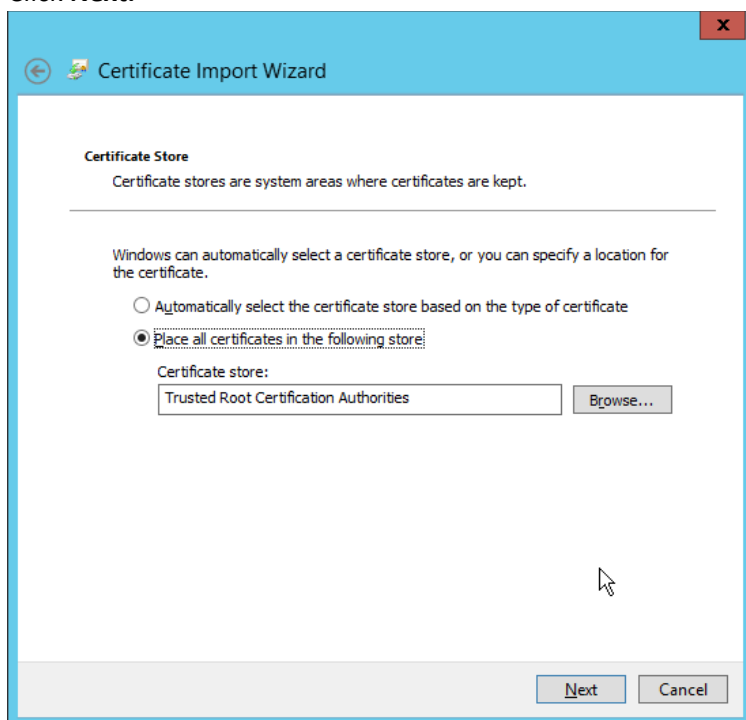
21. Select the same certificate.



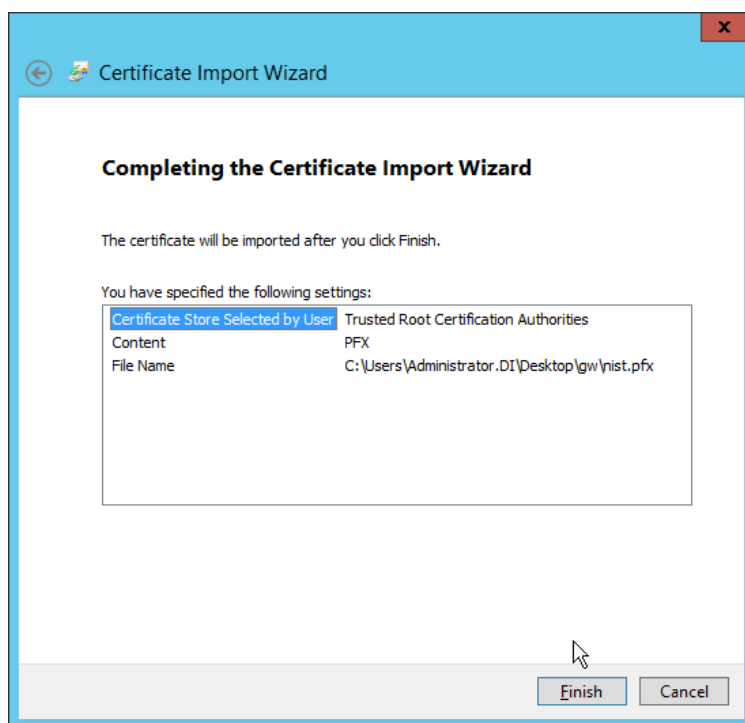
22. Click **Next**.
23. Enter the certificate's **password**.
24. Check the box next to **Mark this key as exportable**.



25. Click **Next**.

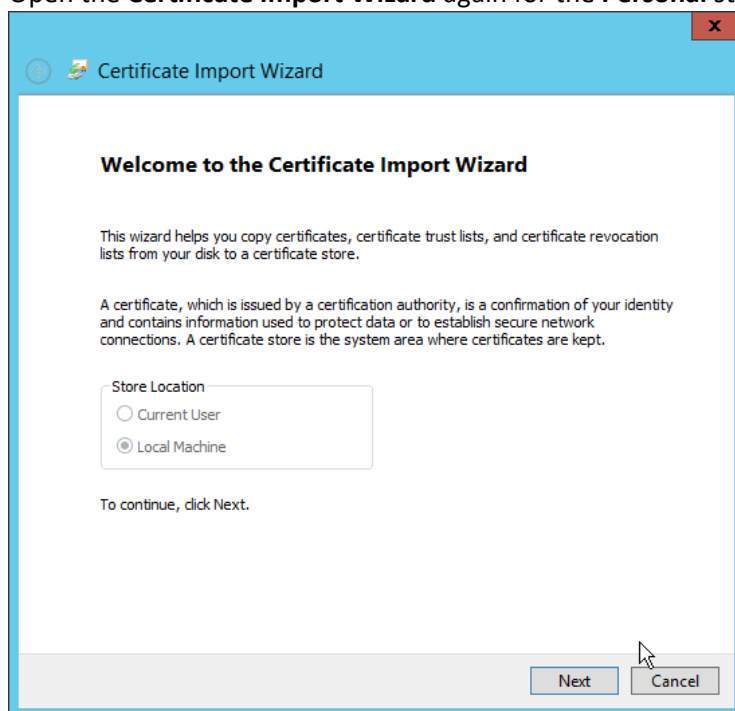


26. Click **Next**.



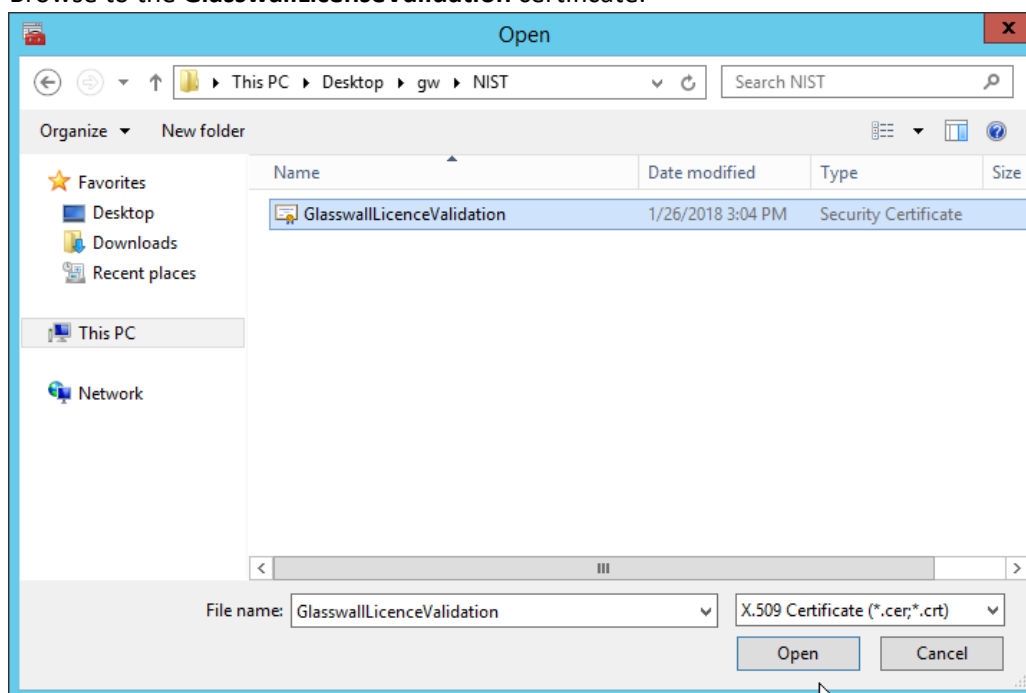
27. Click **Finish**.

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

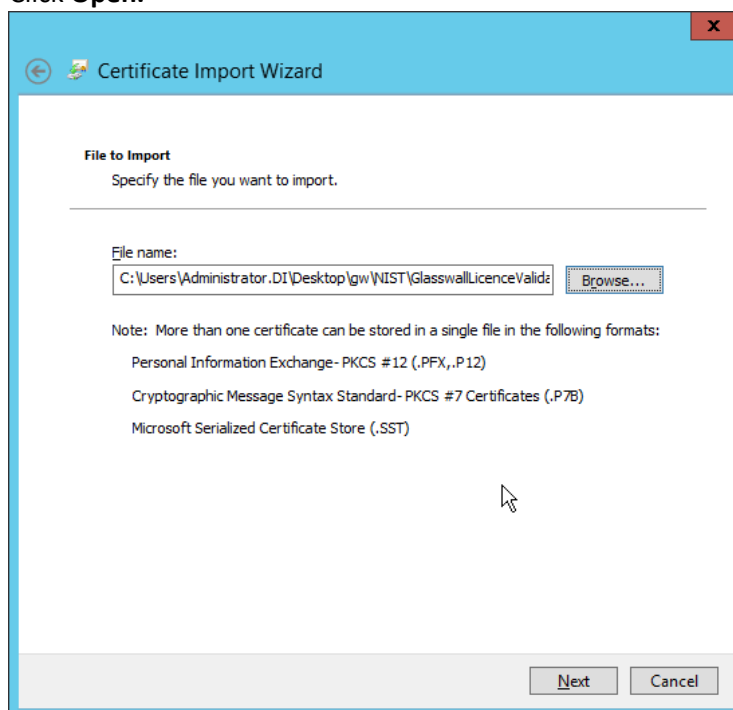


29. Click **Next**.

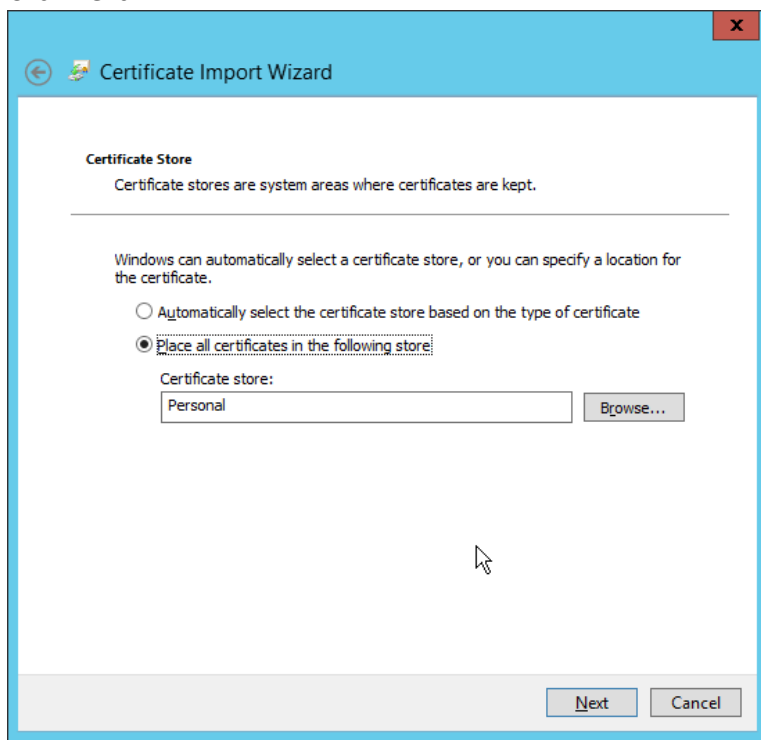
30. Browse to the **GlasswallLicenceValidation** certificate.



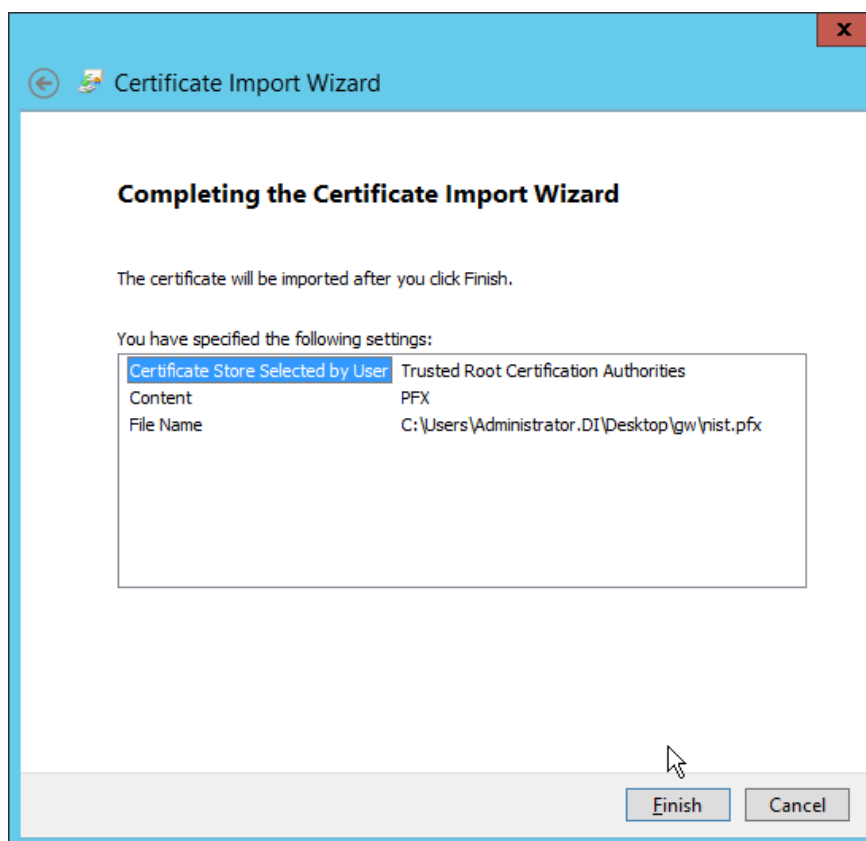
31. Click **Open**.



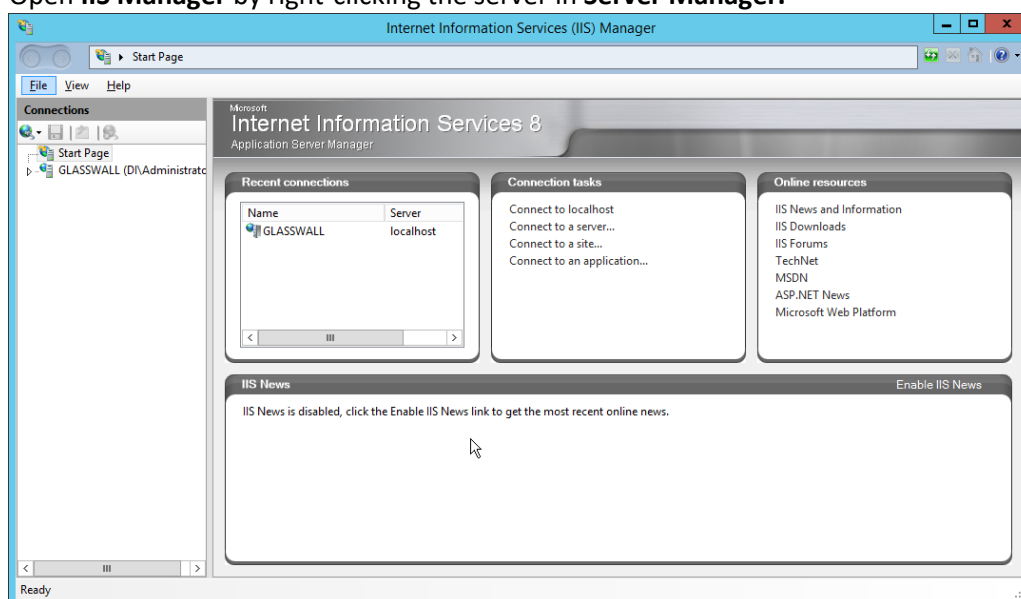
32. Click **Next**.



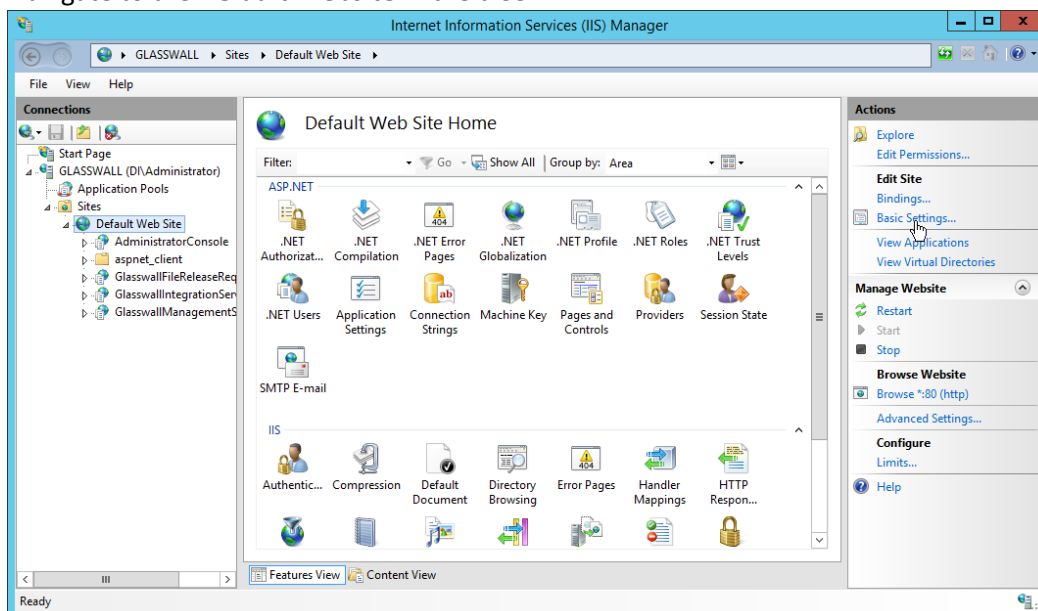
33. Click **Next**.



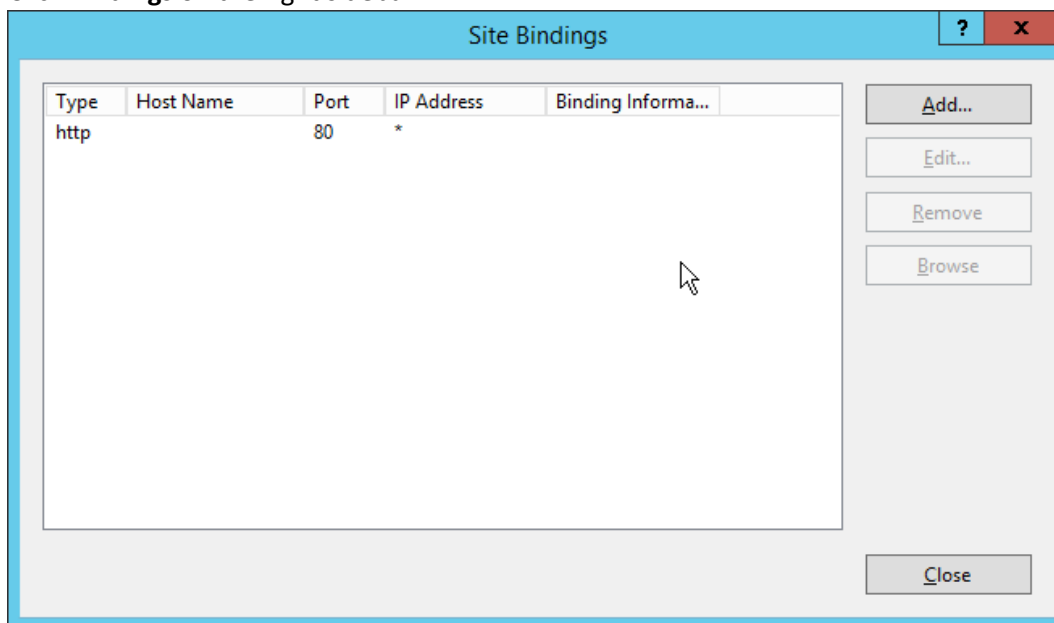
34. Click **Finish**.
35. Open **IIS Manager** by right-clicking the server in **Server Manager**.



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



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

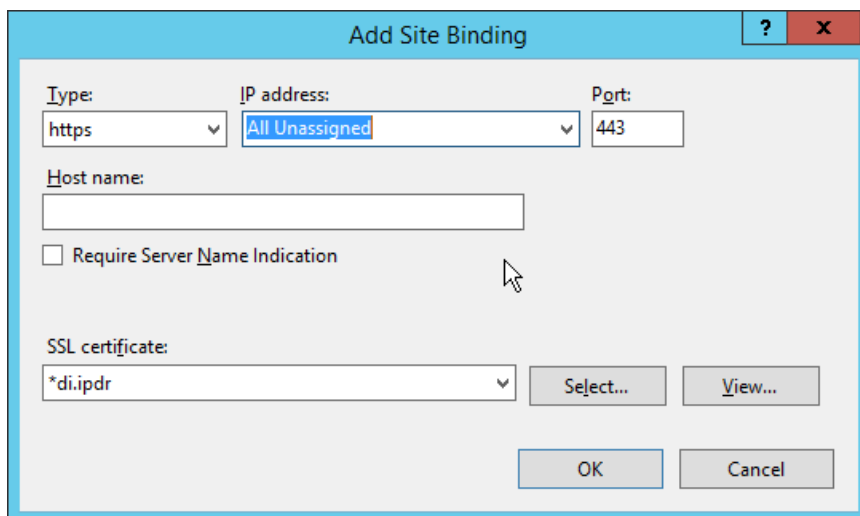


38. Click **Add**.

39. Select **https** for the **Type**.

40. Select **All Unassigned** for **IP address**.

41. Select the **domain certificate** for **SSL certificate**.

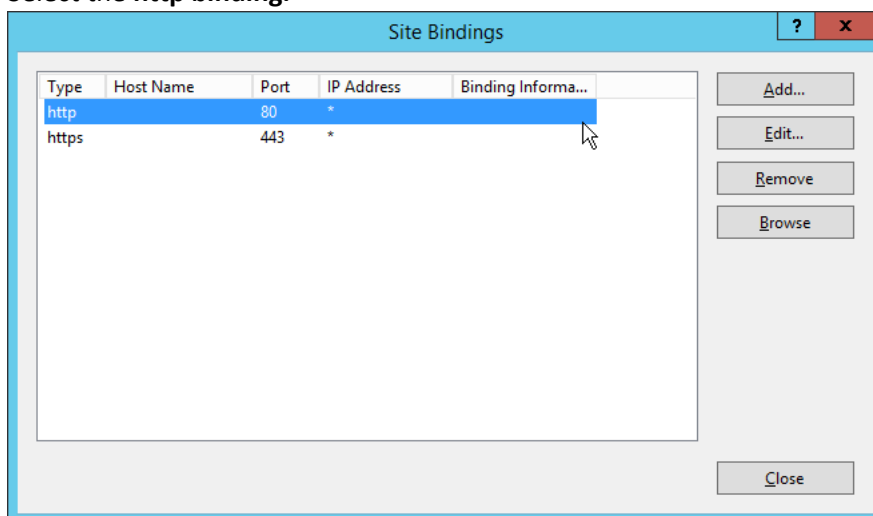


The "Add Site Binding" dialog box is shown. It has a title bar with a question mark and a close button. The main area contains the following fields and controls:

- Type:** A dropdown menu set to "https".
- IP address:** A dropdown menu set to "All Unassigned".
- Port:** A text box containing "443".
- Host name:** An empty text box.
- Require Server Name Indication:** An unchecked checkbox.
- SSL certificate:** A dropdown menu set to "*di.ipdr".
- Select...:** A button next to the SSL certificate dropdown.
- View...:** A button next to the SSL certificate dropdown.
- OK:** A button at the bottom right.
- Cancel:** A button at the bottom right.

42. Click **OK**.

43. Select the **http** binding.

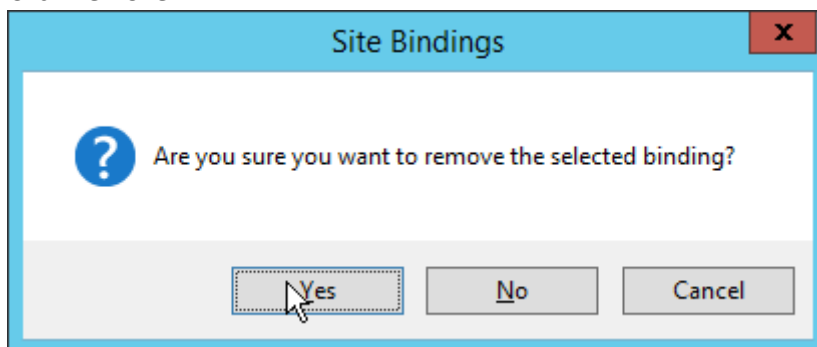


The "Site Bindings" dialog box is shown. It has a title bar with a question mark and a close button. The main area contains a table with the following data:

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

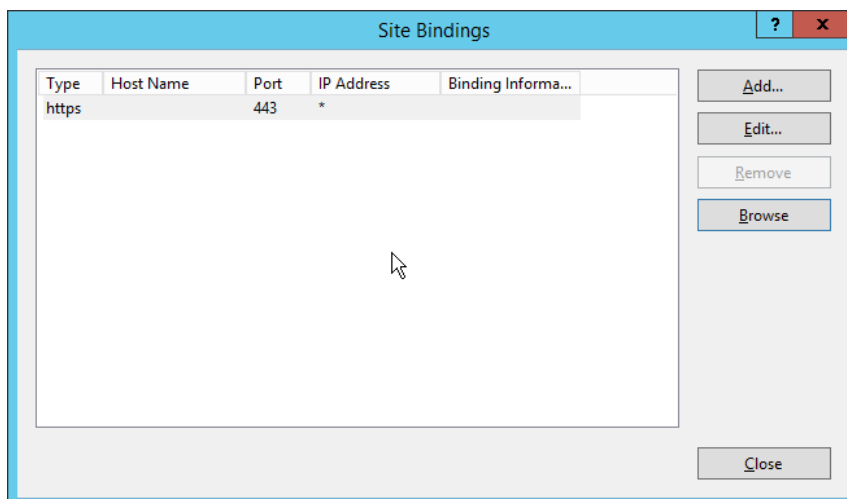
On the right side of the dialog, there are four buttons: "Add...", "Edit...", "Remove", and "Browse". At the bottom right, there is a "Close" button. The "http" row in the table is selected.

44. Click **Remove**.



The "Site Bindings" dialog box is shown, displaying a confirmation message. The message is: "Are you sure you want to remove the selected binding?". Below the message are three buttons: "Yes", "No", and "Cancel". The "Yes" button is highlighted with a mouse cursor.

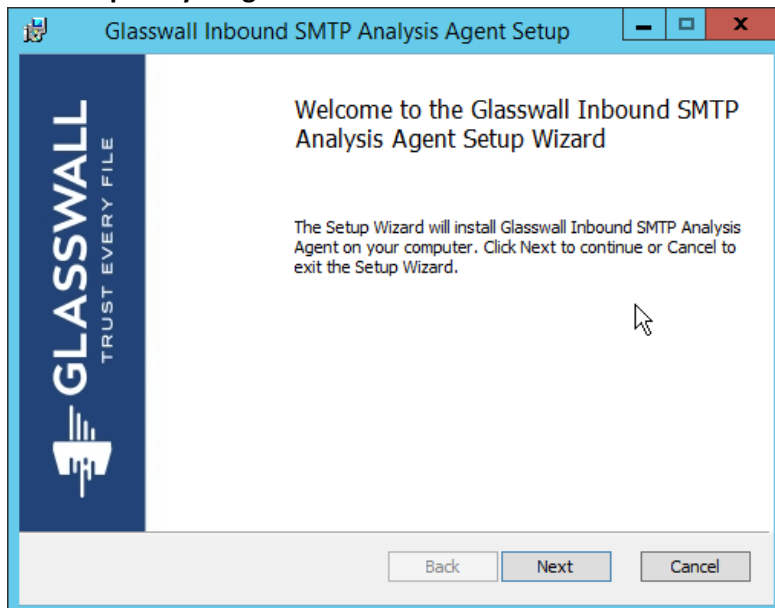
45. Click **Yes**.



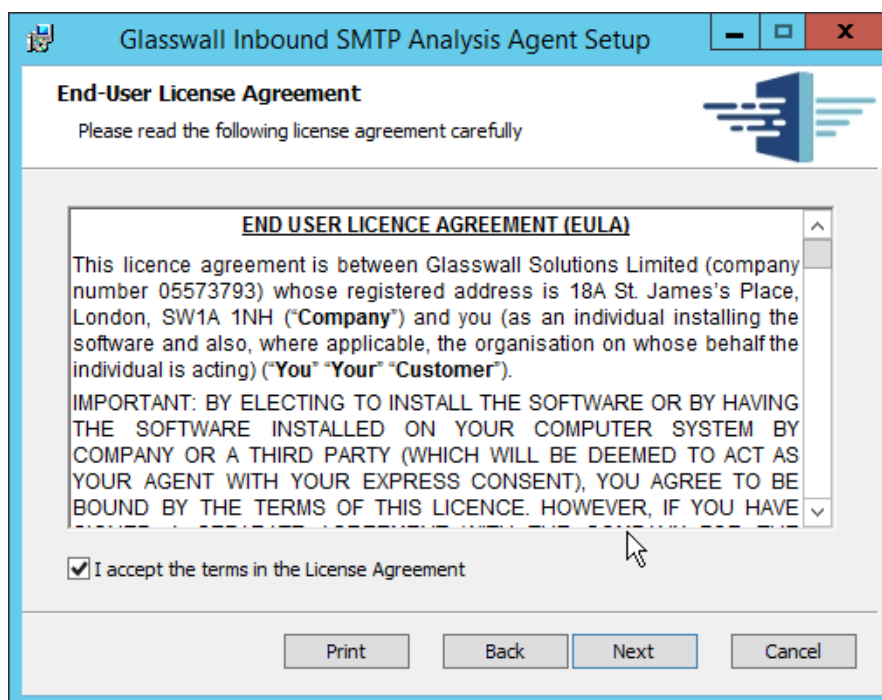
46. Click **Close**.
47. Restart the IIS server. The Glasswall FileTrust console should now be accessible through a browser. (For example, <https://glasswall.di.ipdr/AdministratorConsole>). Ensure that there are no certificate errors.

2.7.2.5 *Install the Smtplib Analysis Agent*

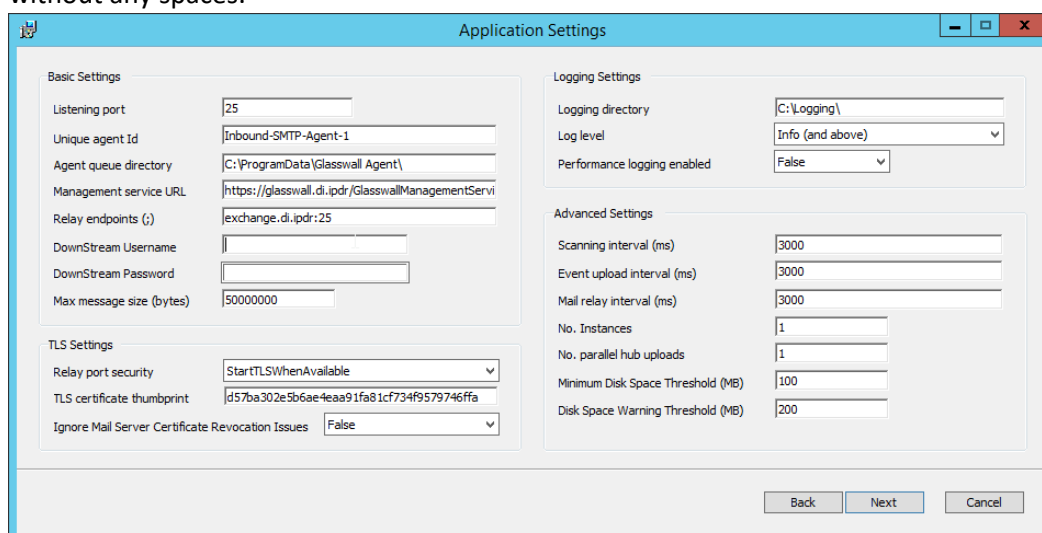
1. Run **SmtplibAnalysisAgentInstaller.msi**.



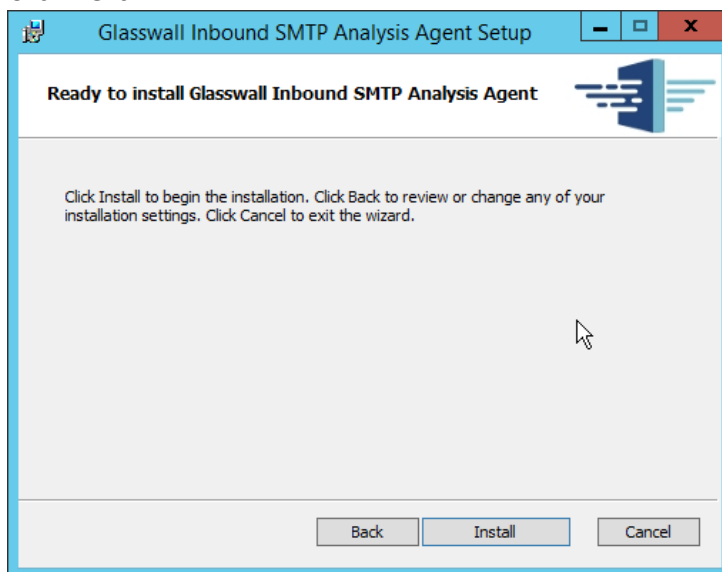
2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



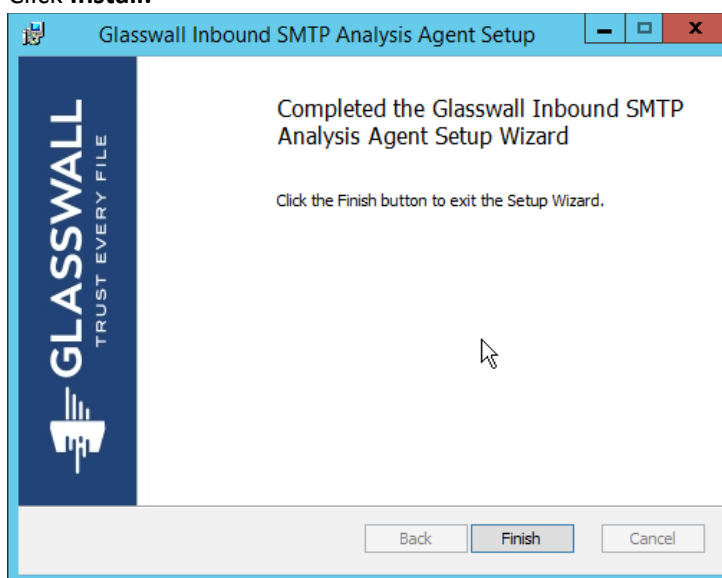
4. Click **Next**.
5. For **Listening port**, enter **25**.
6. For **Management service URL**, correct the domain to be the web domain of the IIS server (for example, glasswall.di.ipdr).
7. For the **Relay endpoints**, enter the address of the Exchange server, followed by the port (for example, exchange.di.ipdr:25).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



9. Click **Next**.



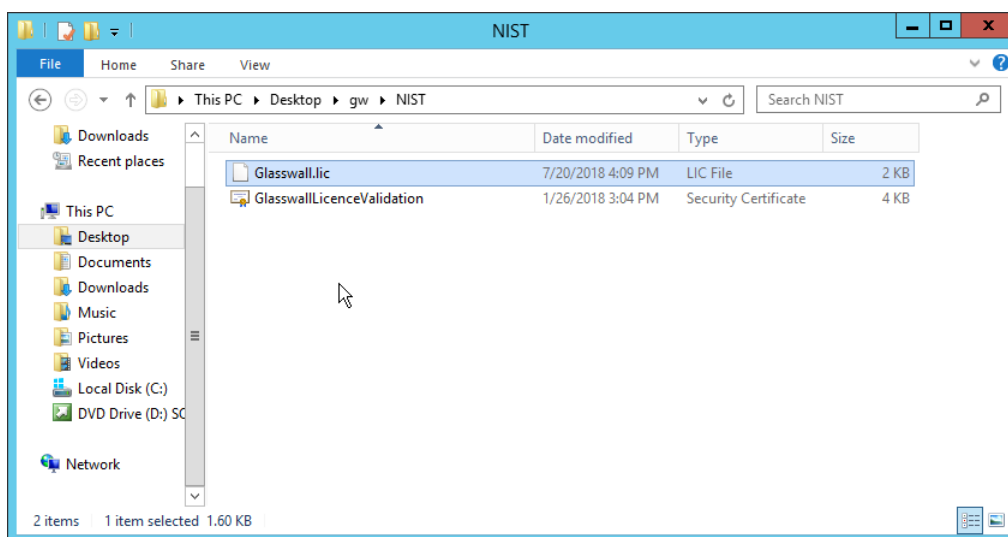
10. Click **Install**.



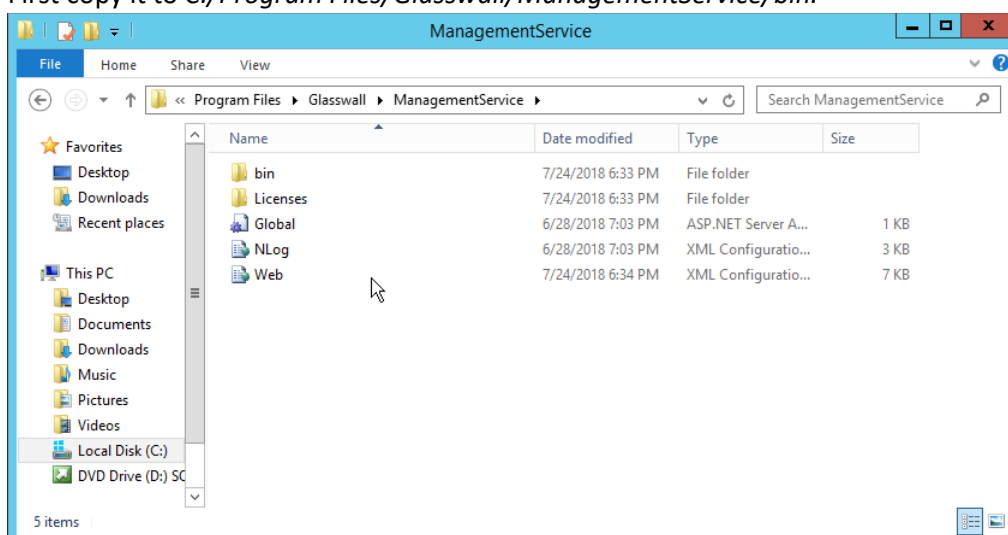
11. Click **Finish**.

2.7.2.6 *Distribute the Glasswall License File*

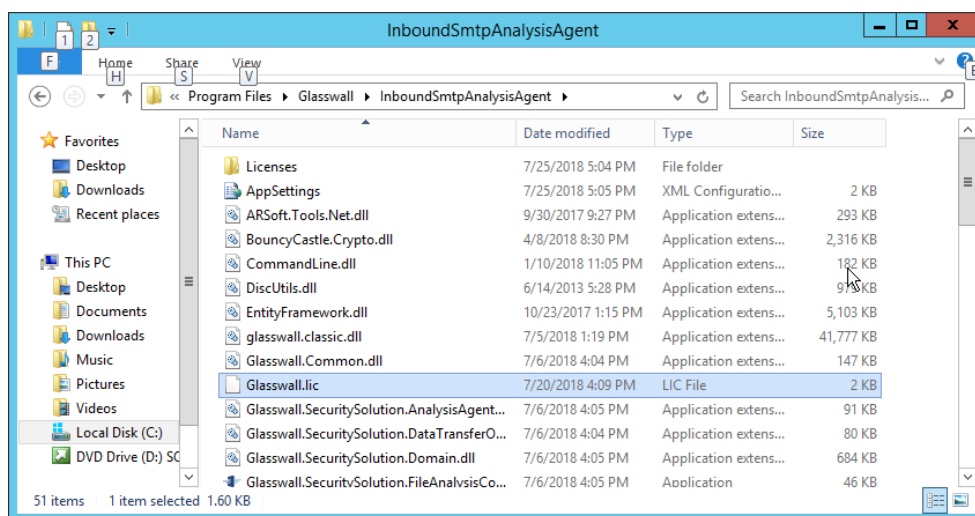
1. Copy the **Glasswall License** file to the following locations, assuming **Glasswall** was installed to *C:/Program Files/Glasswall*.



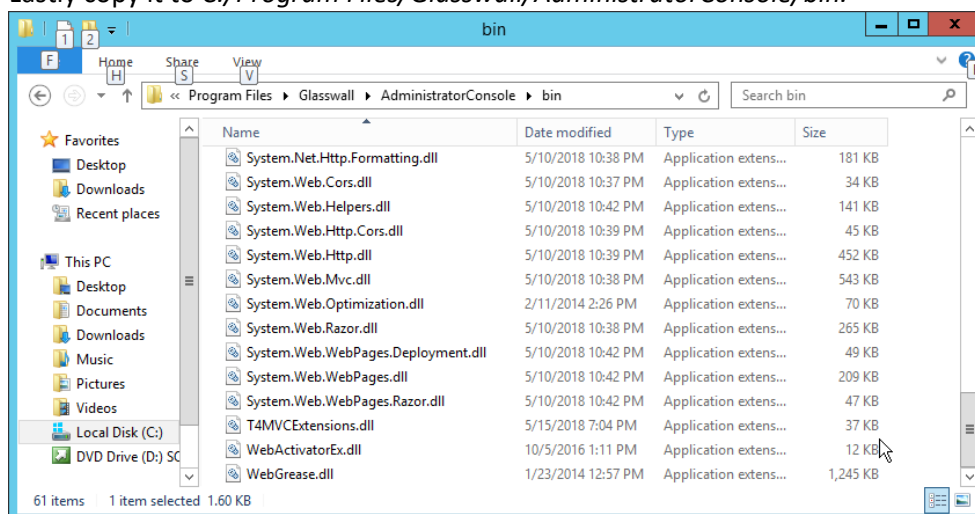
2. First copy it to *C:/Program Files/Glasswall/ManagementService/bin*.



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



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



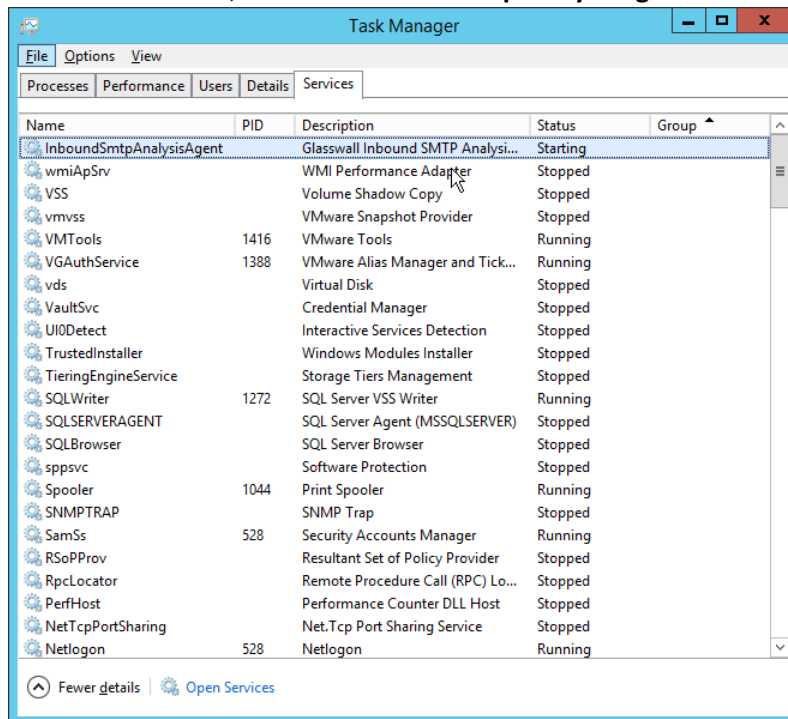
2.7.3 Configure Glasswall FileTrust

Please see <https://docs.glasswallsolutions.com/cloud/Content/Configuring/Office365-Integration.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.

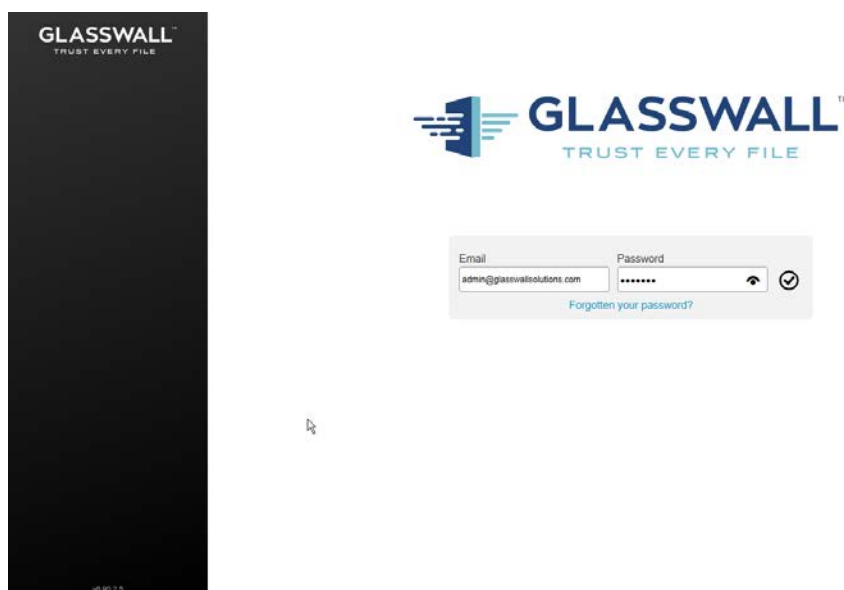
Instead, to achieve the goal of routing email through Glasswall, we redirect local mail exchange (MX) records to Glasswall FileTrust. We implemented it this way because of limitations of the lab environment, but organizations should consult with the vendor for the best solution to route email through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

2.7.3.1 Create a New Administrator Account

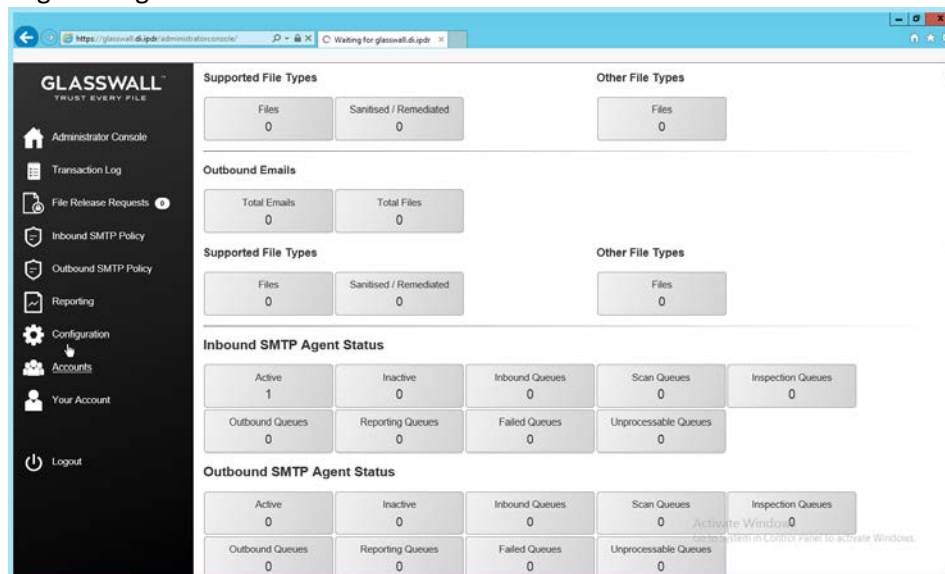
1. Open **Task Manager**.
2. In the **Services** tab, start the **InboundSntpAnalysisAgent** service.



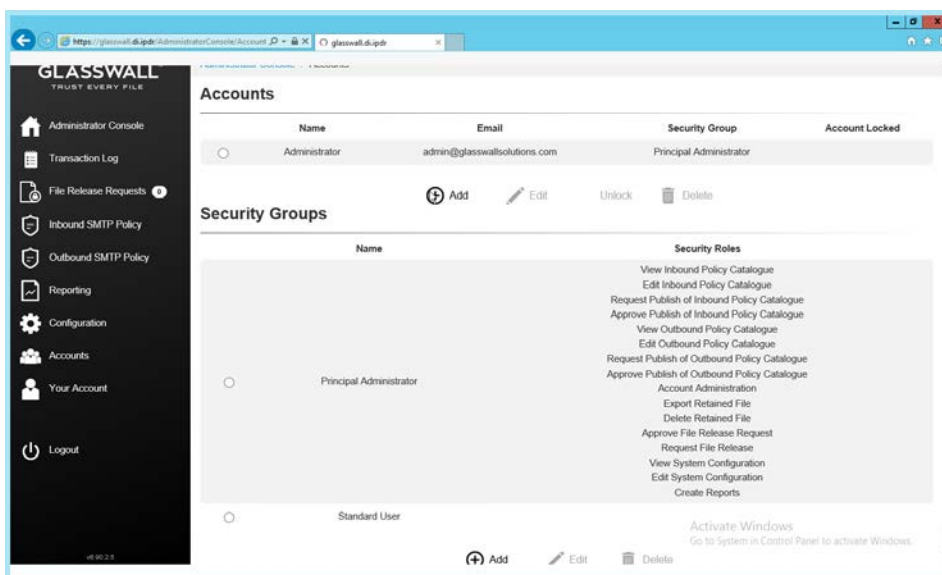
3. Close **Task Manager**.
4. Open a browser and navigate to the **Glasswall Administration Console** (for example, <http://glasswall.di.ipdr/AdministratorConsole>).
5. If this is the first time logging in, the default account will be **admin@glasswallsolutions.com**, and the password is **Welcome1?**.



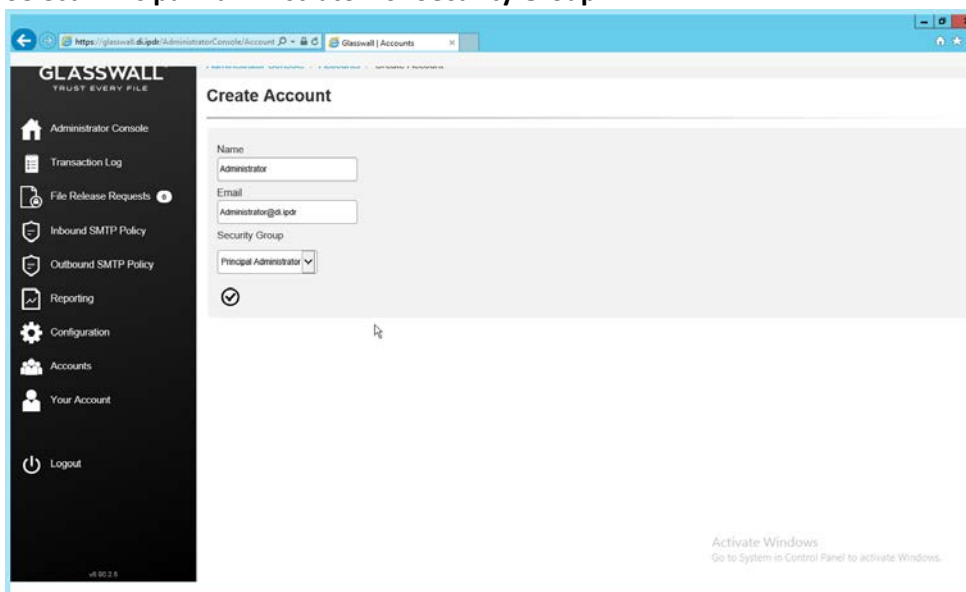
6. Log in using these credentials.



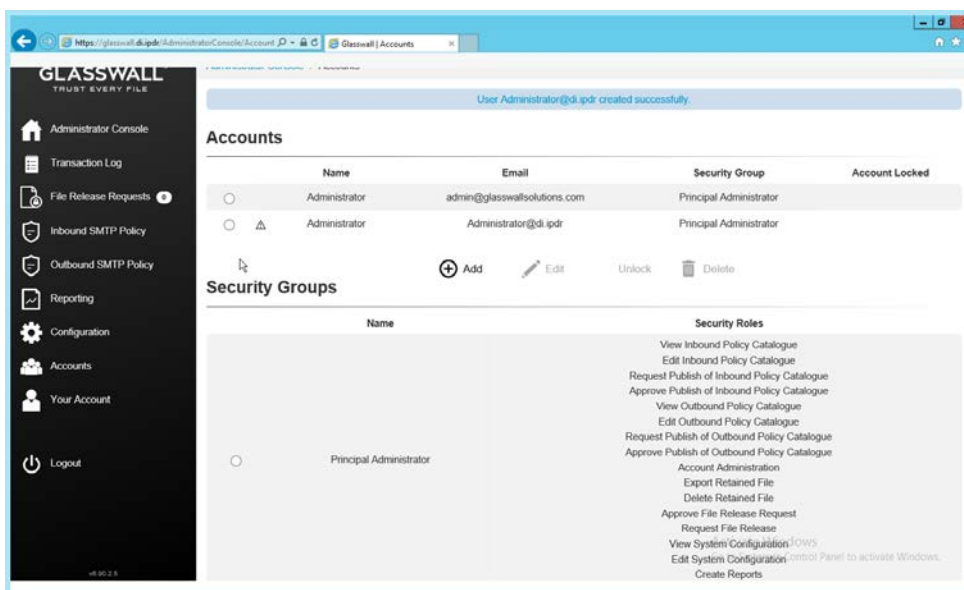
7. On the left sidebar, click **Accounts**.



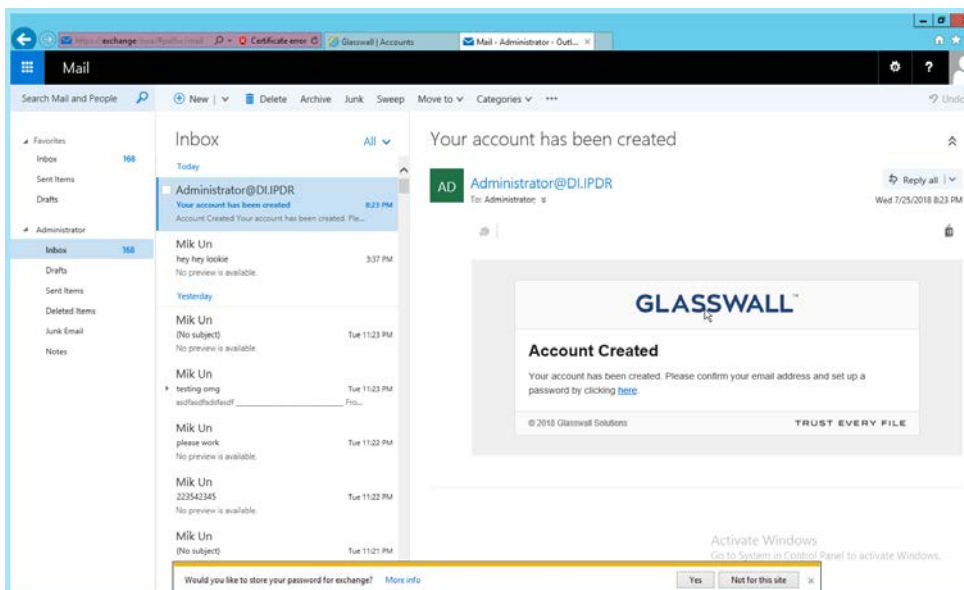
8. Under **Accounts**, click **Add**.
9. Enter the **name** and **email address** of an administrator account from the email server.
10. Select **Principal Administrator** for **Security Group**.



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



12. The new administrator account should be created.



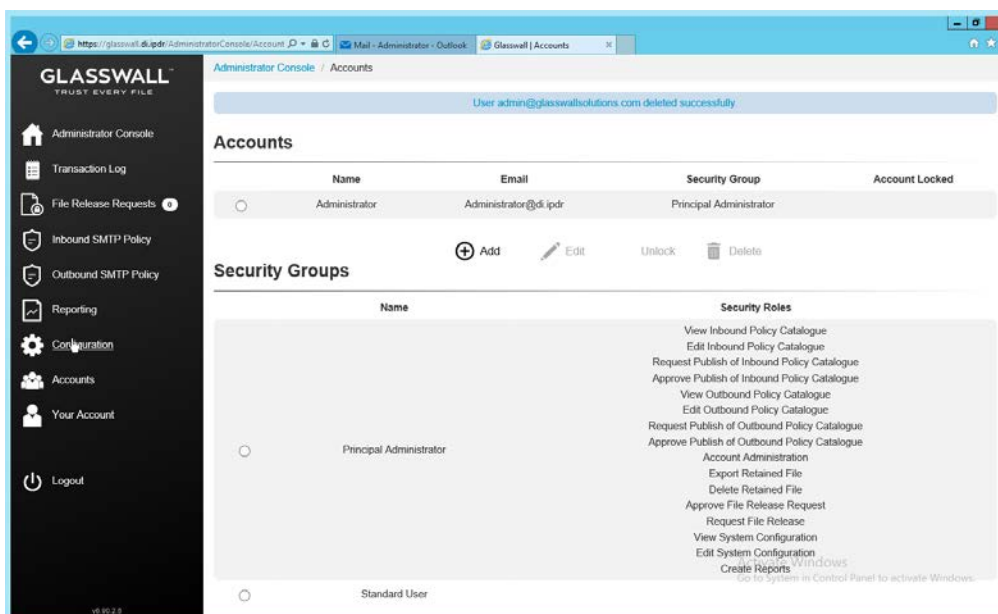
13. Check the email inbox of the specified email address for a confirmation email, and click the link in the email.

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.

Name	Email	Security Group	Account Locked
<input checked="" type="radio"/> Administrator	admin@glasswallsolutions.com	Principal Administrator	
<input type="radio"/> Administrator	Administrator@di.ipdr	Principal Administrator	

Name	Security Roles
<input type="radio"/> Principal Administrator	View Inbound Policy Catalogue Edit Inbound Policy Catalogue Request Publish of Inbound Policy Catalogue Approve Publish of Inbound Policy Catalogue View Outbound Policy Catalogue Edit Outbound Policy Catalogue Request Publish of Outbound Policy Catalogue Approve Publish of Outbound Policy Catalogue Account Administration Export Retained File Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration Create Reports
<input type="radio"/> Standard User	

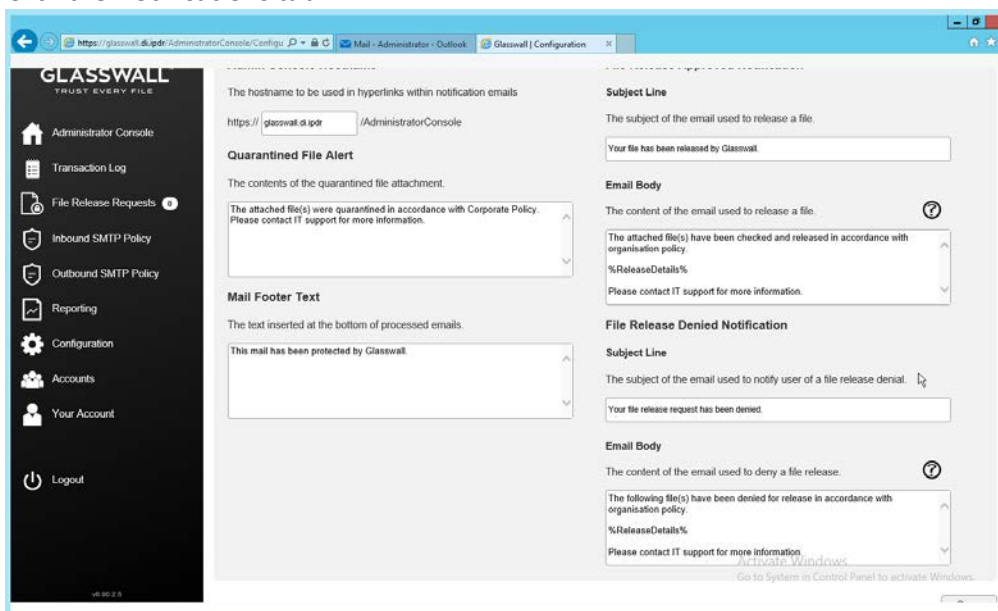
17. Click **Delete**.



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

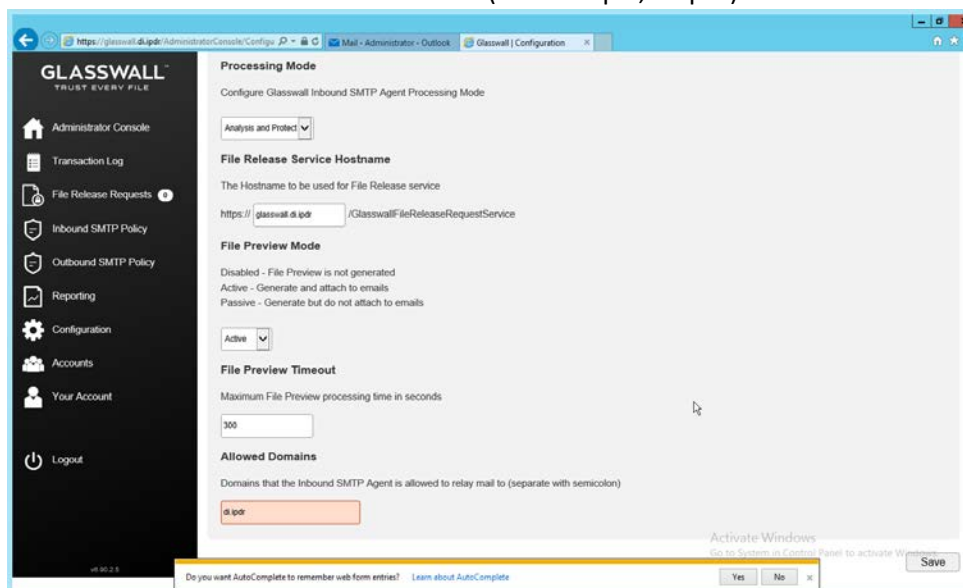
2.7.3.2 *Configure Notifications and Policies*

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**.

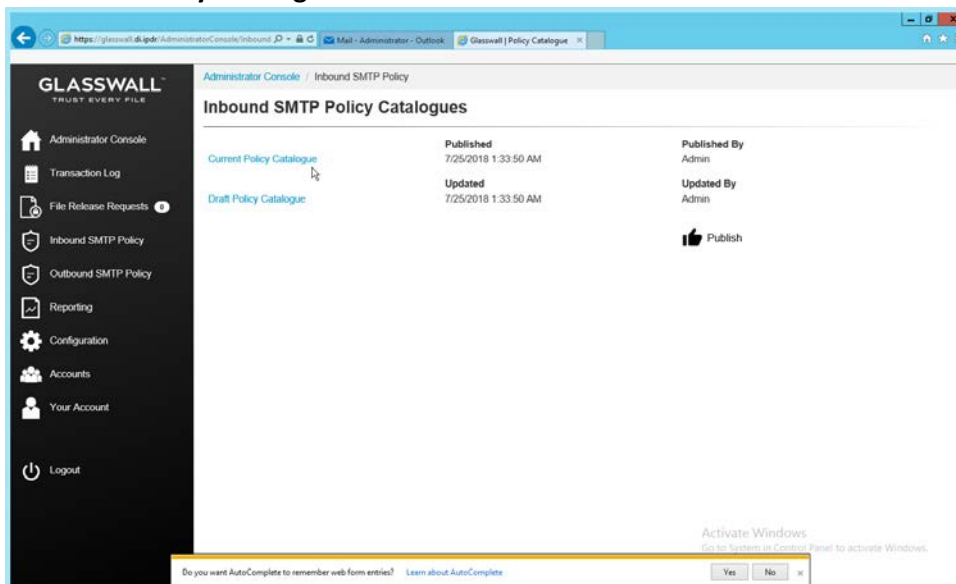
2.7.3.3 Configure Inbound SMTP Policy

This section discusses Simple Mail Transfer Protocol (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.

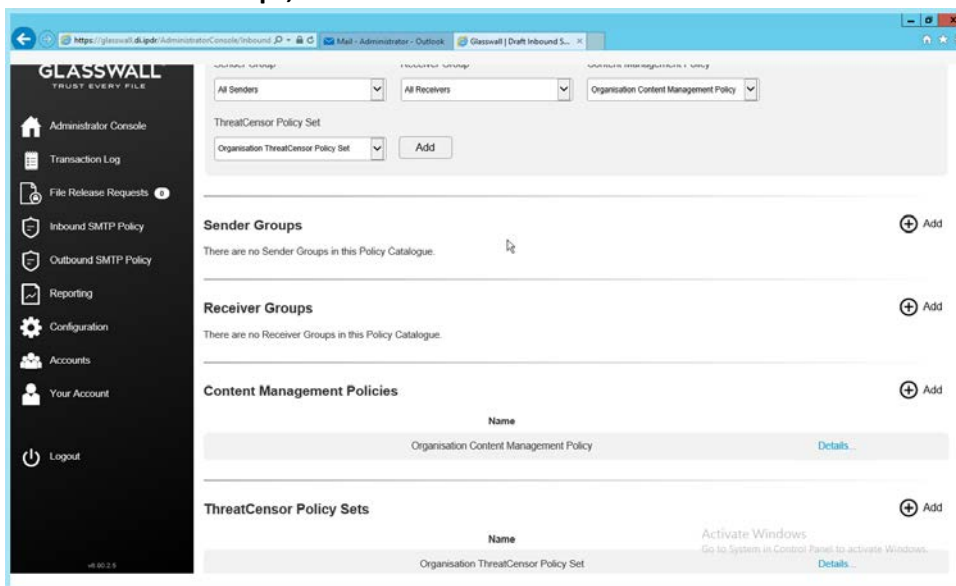
Policy in Glasswall FileTrust consists of **Sender Groups**, **Receiver Groups**, **Content Management Policies**, and **ThreatCensor Policy Sets**. **Receiver groups** allow for the specification of users who receive email. **Sender groups** allow for the specification of emails received from specific 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**.



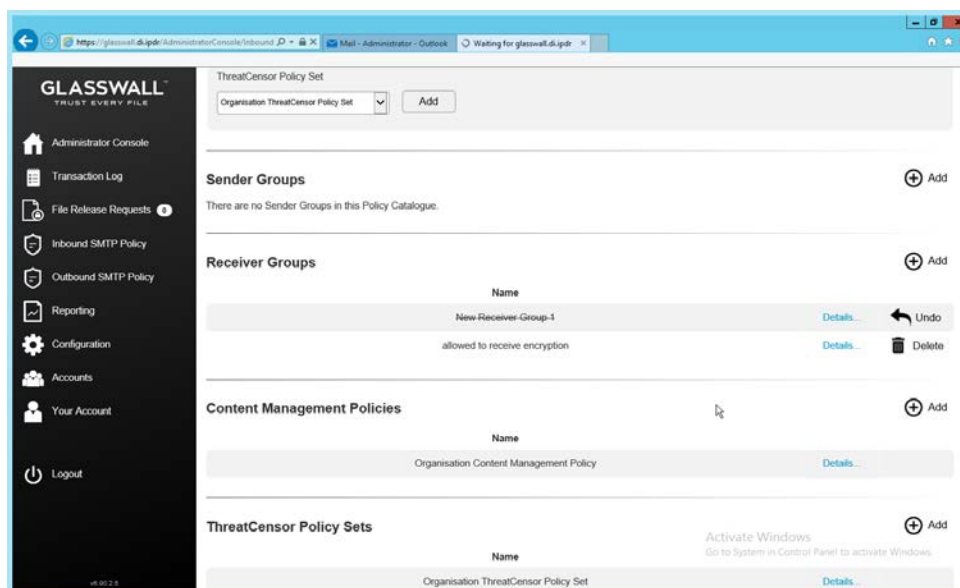
4. Under **User Defined Mailboxes**, click **Edit**.

The screenshot shows the 'New Receiver Group 2' configuration page in the Glasswall Administrator Console. The left sidebar contains navigation links: Administrator Console, Transaction Log, File Release Requests, Inbound SMTP Policy, Outbound SMTP Policy, Reporting, Configuration, Accounts, Your Account, and Logout. The main content area has a breadcrumb trail: Administrator Console / Inbound SMTP Policy / Policy Catalogue / Receiver Group Details. Below this is the title 'New Receiver Group 2' with an 'Edit' link. The 'LDAP Synchronisation Settings' section includes fields for Server (myserver/DN-instance.DC-company.DC-COM), User Name (username), Password (password), Query ((& (department=department name) (co=country code)), and Mailbox Attribute Name (mail). The 'User Defined Mailboxes' section states 'There are currently no user-defined mailboxes for this receiver group' and includes an 'Edit' link. An 'Activate Windows' watermark is visible at the bottom right.

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

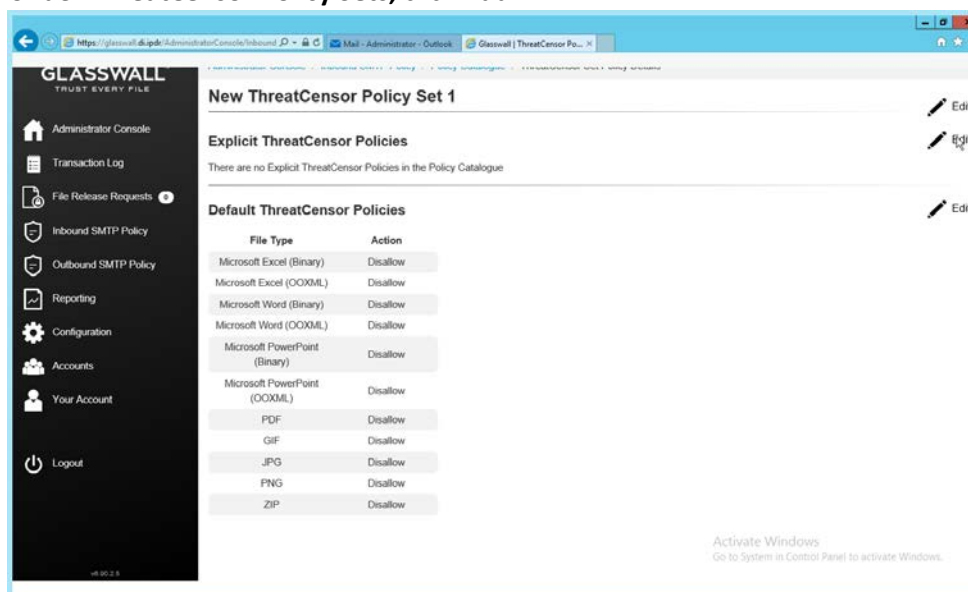
The screenshot shows the 'New Receiver Group 2 Mailboxes' configuration page in the Glasswall Administrator Console. The left sidebar is identical to the previous screenshot. The main content area has a breadcrumb trail: Administrator Console / Inbound SMTP Policy / Policy Catalogue / Receiver Group Details. Below this is the title 'New Receiver Group 2 Mailboxes' with an 'Edit' link. The 'Add User-Defined Mailbox' section includes an 'E-Mail Address' input field and an 'Add' button. The 'User Defined Mailboxes' section states 'There are currently no user-defined mailboxes for this receiver group'. An 'Activate Windows' watermark is visible at the bottom right.

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

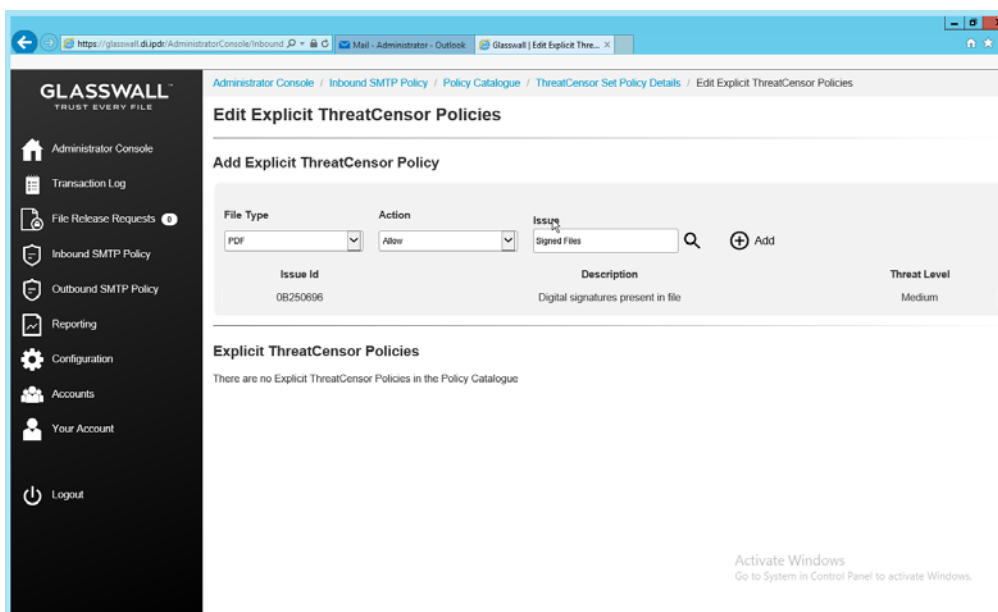


2.7.3.5 Create a ThreatCensor Policy Set

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



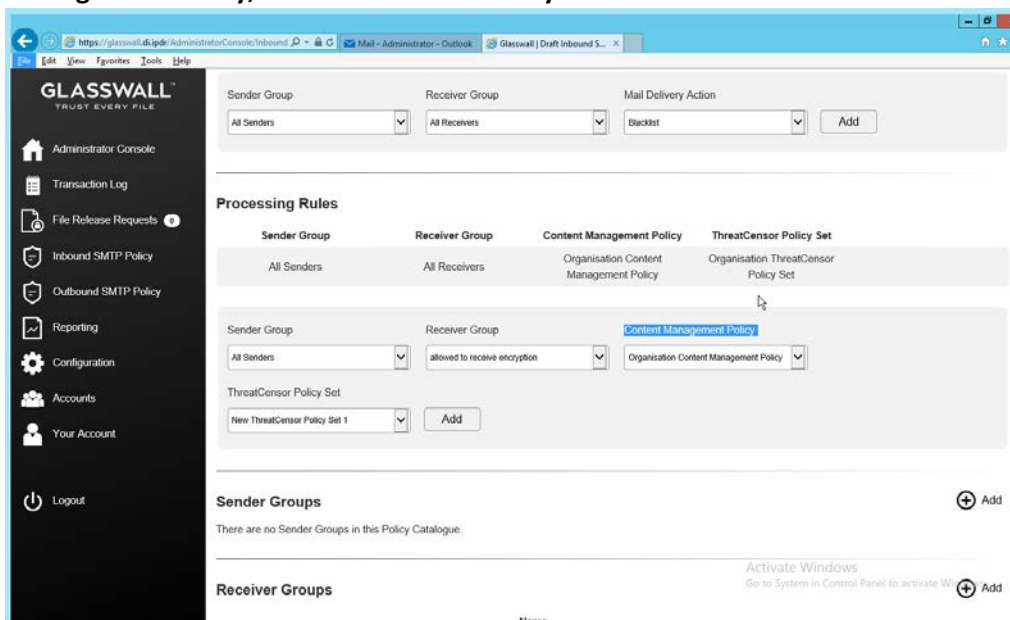
2. Under **Explicit ThreatCensor Policies**, click **Edit**.



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

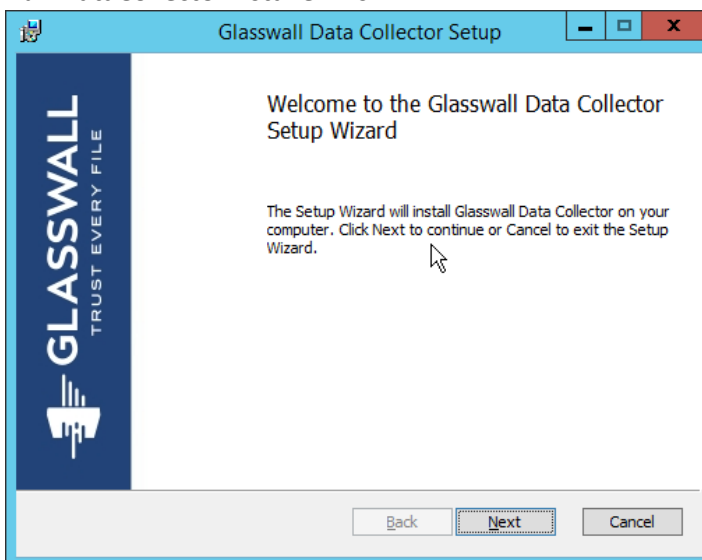
1. Under Processing Rules, select the appropriate **Sender Group**, **Receiver Group**, **Content Management Policy**, and **ThreatCensor Policy Set**.



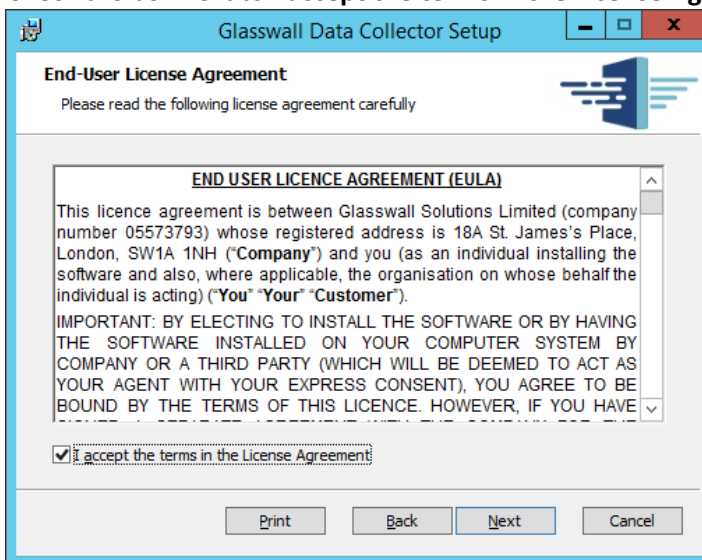
2. Click **Add**.
3. This allows for granular policy for email inspection, quarantine, and reconstruction.

2.7.4 Configure Intelligence Sharing

1. Run **DataCollectorInstaller.msi**.

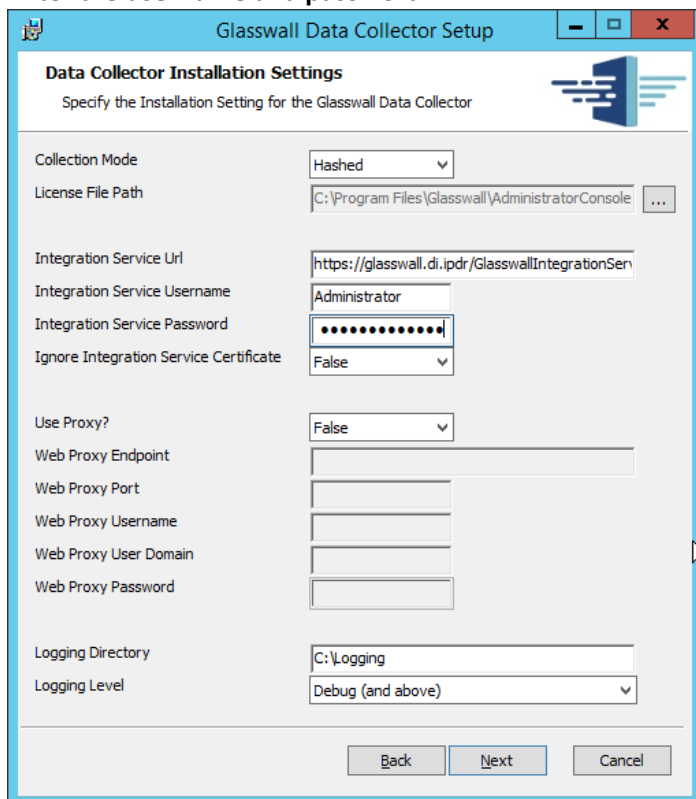


2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



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**.



Glasswall Data Collector Setup

Data Collector Installation Settings
Specify the Installation Setting for the Glasswall Data Collector

Collection Mode: Hashed

License File Path: C:\Program Files\Glasswall\AdministratorConsole ...

Integration Service Url: https://glasswall.di.ipdr/GlasswallIntegrationSer

Integration Service Username: Administrator

Integration Service Password: [Masked]

Ignore Integration Service Certificate: False

Use Proxy?: False

Web Proxy Endpoint: [Empty]

Web Proxy Port: [Empty]

Web Proxy Username: [Empty]

Web Proxy User Domain: [Empty]

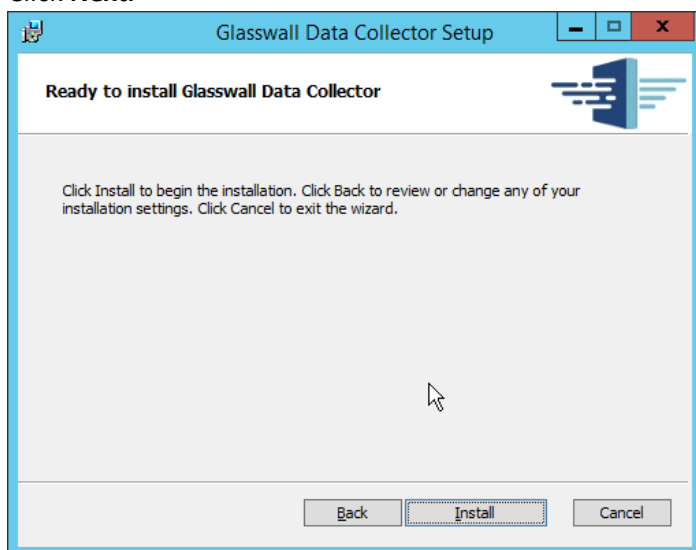
Web Proxy Password: [Empty]

Logging Directory: C:\Logging

Logging Level: Debug (and above)

Buttons: Back, Next, Cancel

8. Click **Next**.



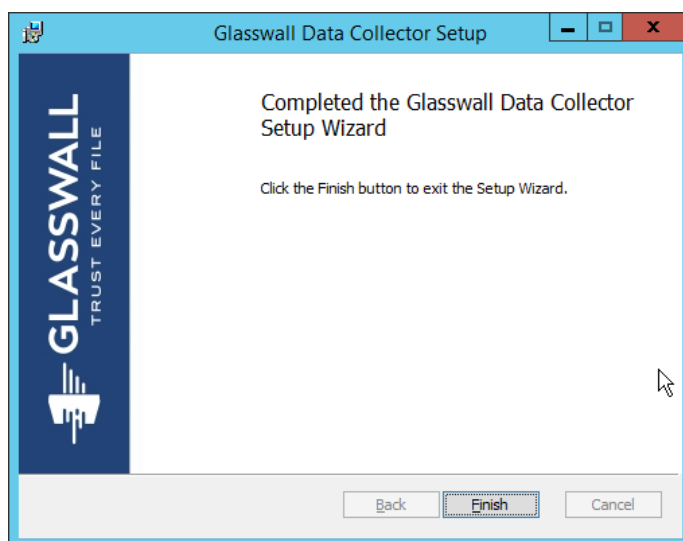
Glasswall Data Collector Setup

Ready to install Glasswall Data Collector

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Buttons: Back, Install, Cancel

9. Click **Install**.



10. Click **Finish**.

2.8 Micro Focus ArcSight Enterprise Security Manager

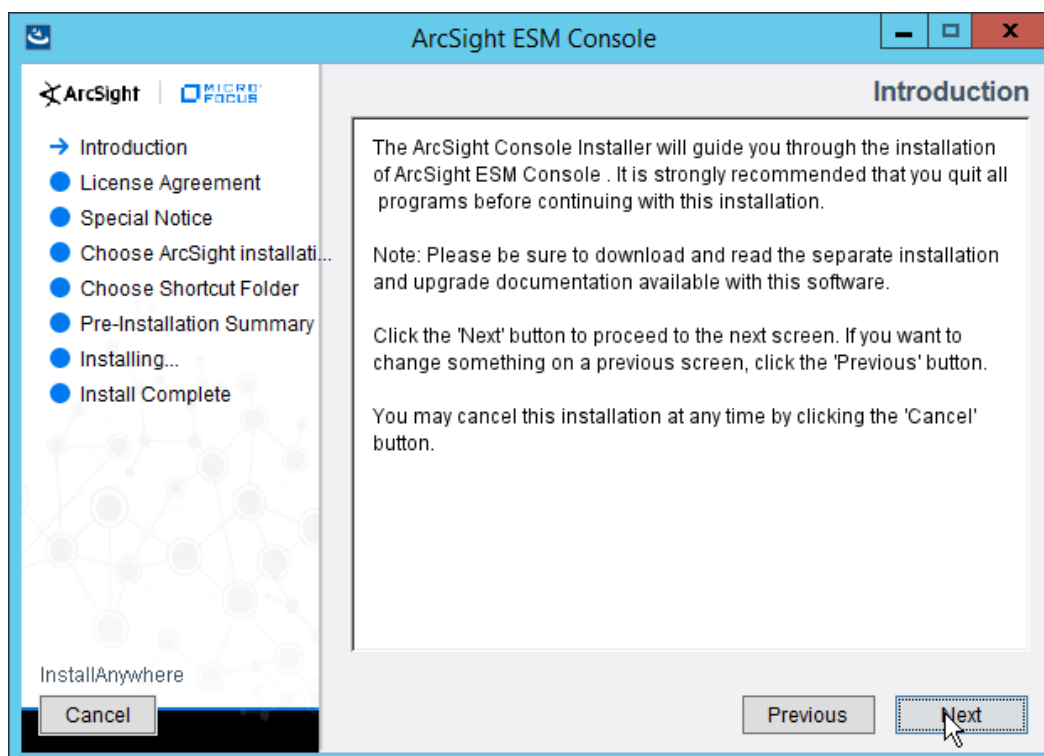
Micro Focus ArcSight Enterprise Security Manager (ESM) is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

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.

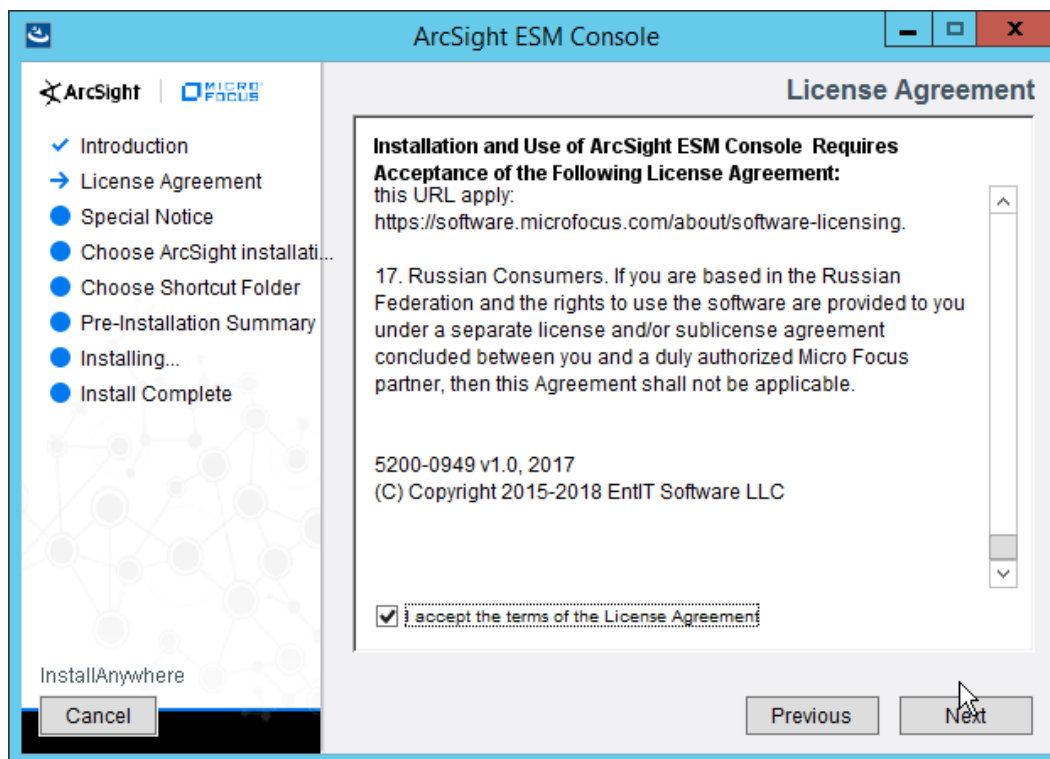
Installation instructions are included for both Windows and UNIX machines, as well as for collecting from multiple machines. Furthermore, integrations with other products in the build are included in later sections.

2.8.1 Install the ArcSight Console

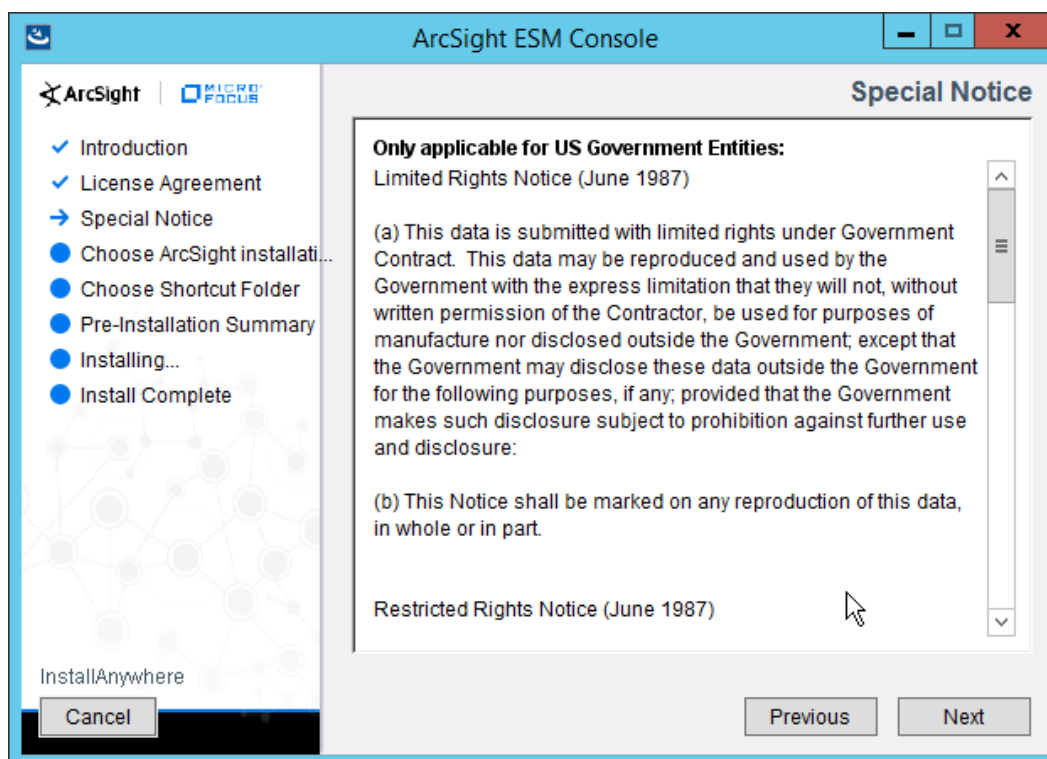
1. Run **ArcSight-7.0.0.2436.1-Console-Win.exe**.



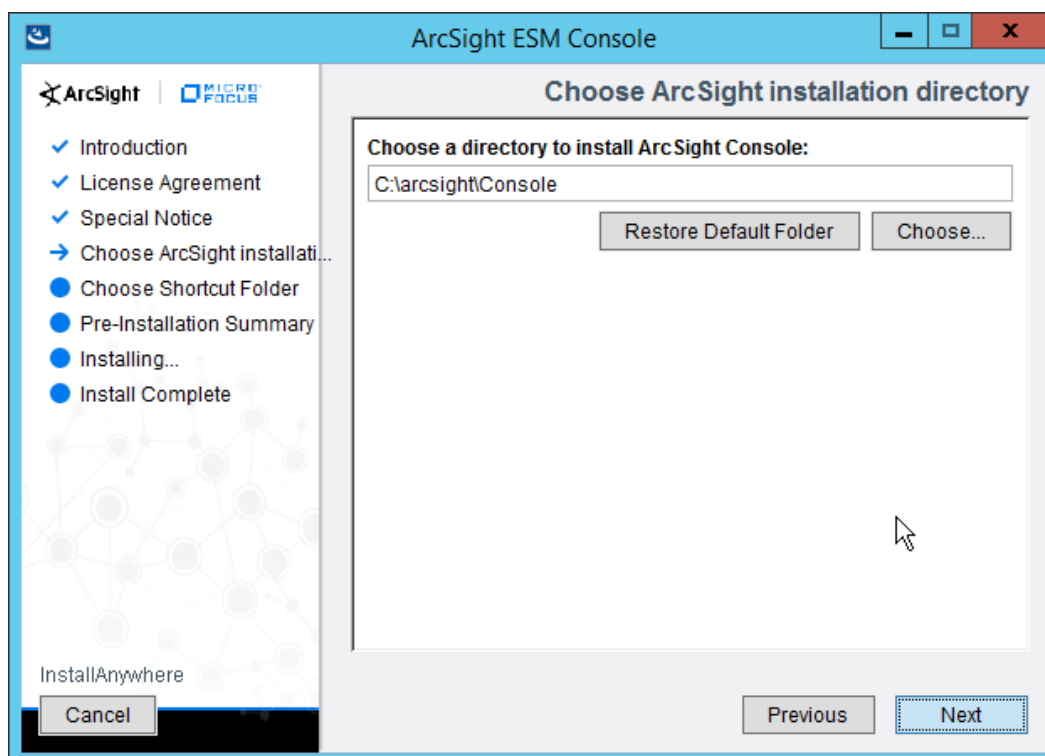
2. Click **Next**.
3. Check the box next to **I accept the License Agreement**.



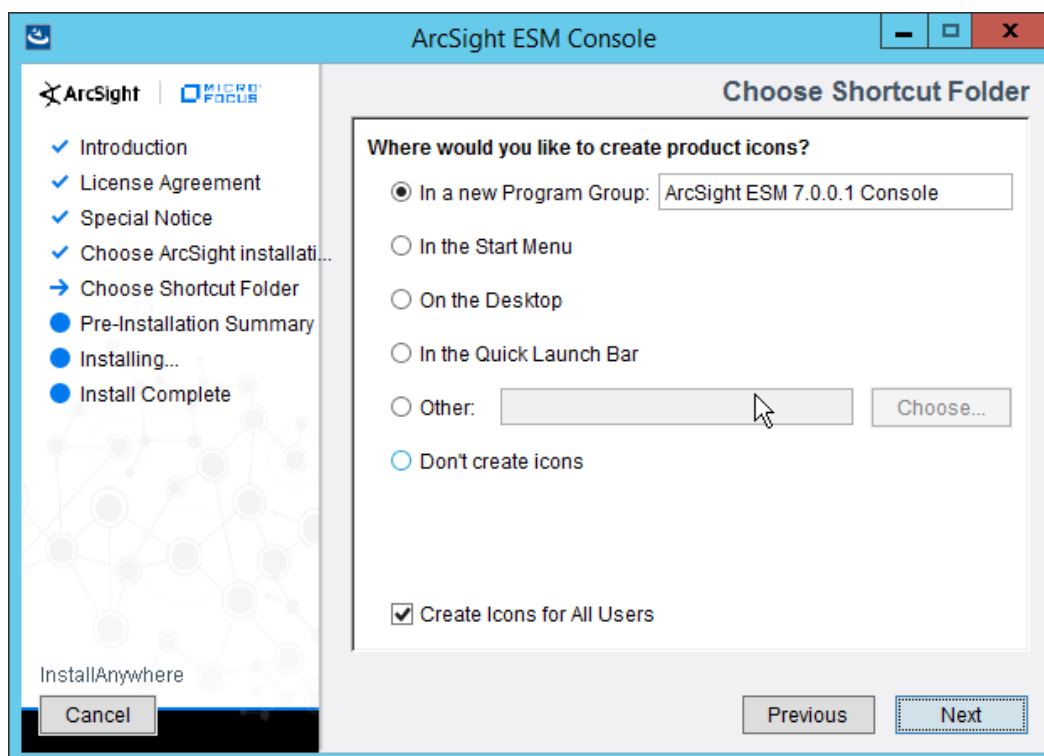
4. Click **Next**.



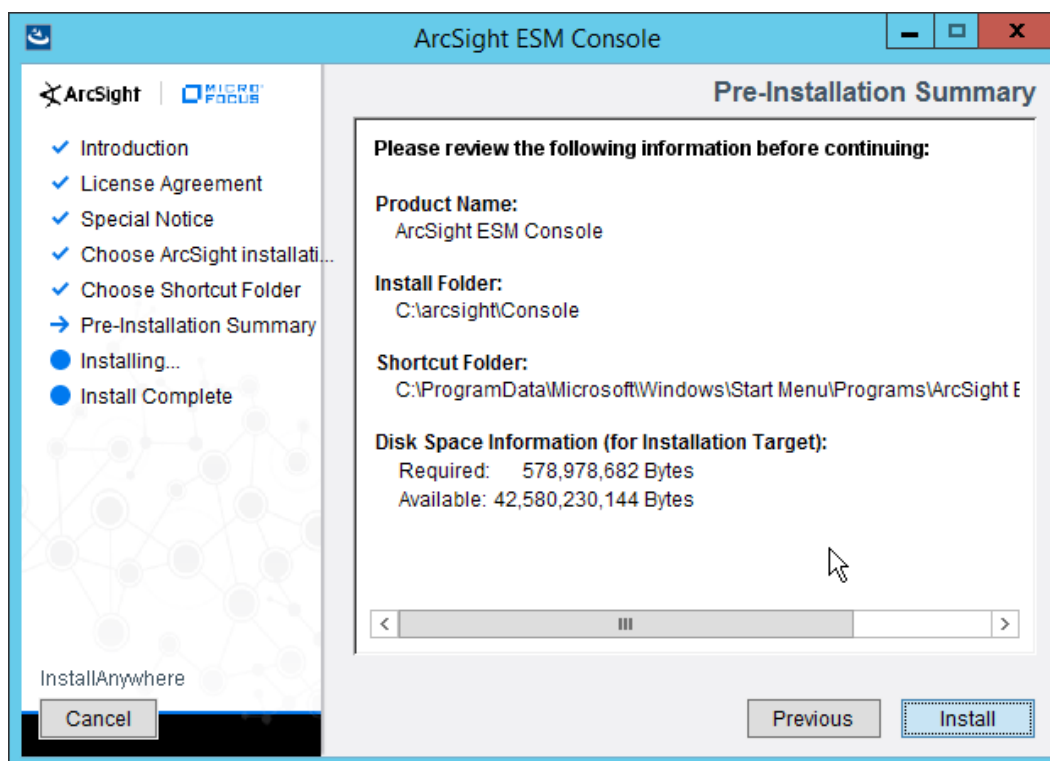
5. Click **Next**.



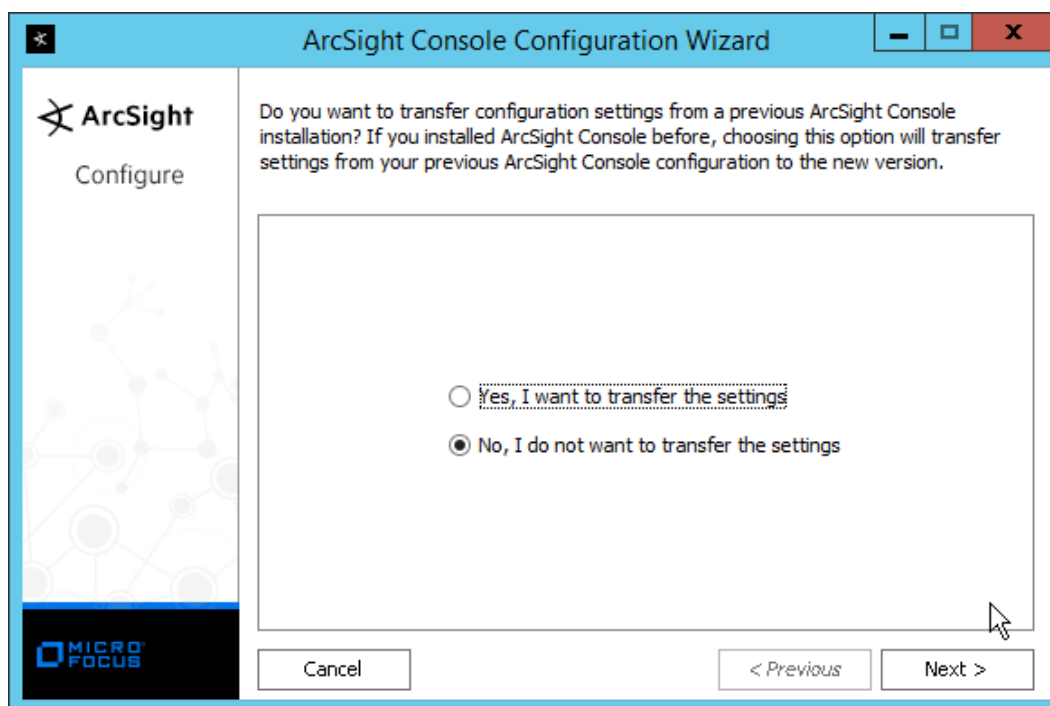
6. Click **Next**.



7. Click **Next**.

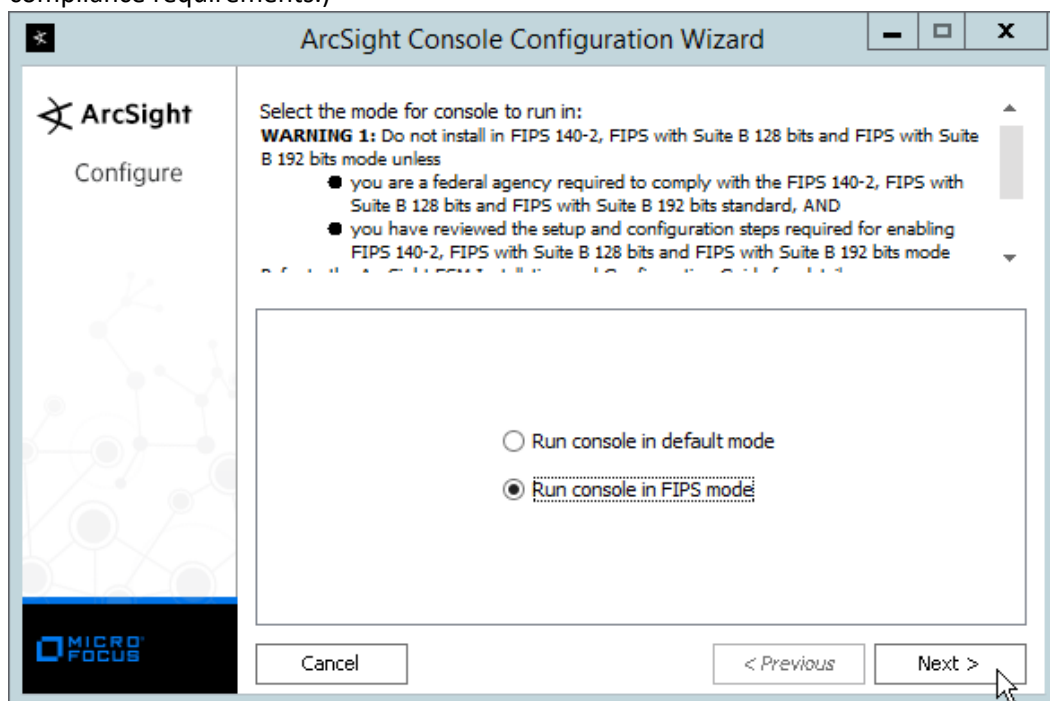


8. Click **Install**.
9. Select **No, I do not want to transfer the settings**.

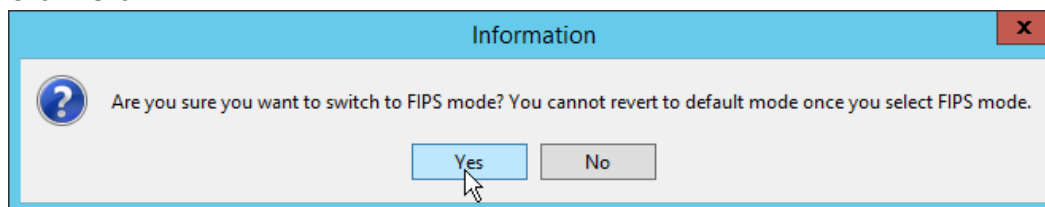


10. Click **Next**.

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

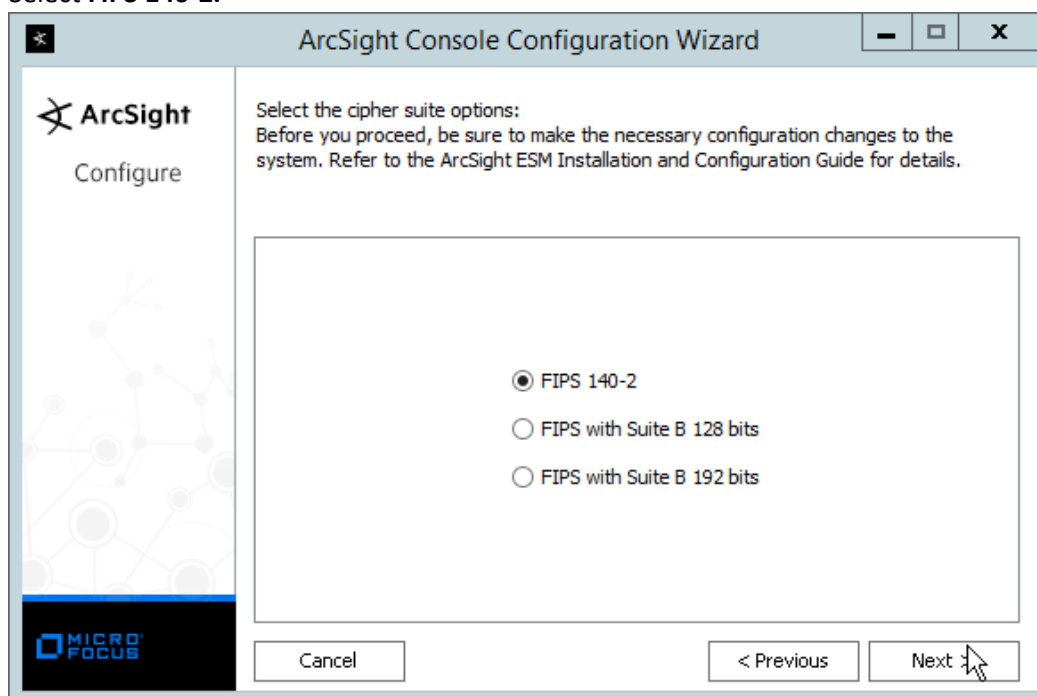


12. Click **Next**.



13. Click **Yes**.

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



15. Click **Next**.

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

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

ArcSight Console Configuration Wizard

ArcSight
Configure

Please complete the following ArcSight Manager information.

NOTE: Only IPv4 is available as a Preferred IP Protocol.

Manager Host Name: arcsight-esm

Manager Port: 8443

Buttons: Cancel, < Previous, Next >

18. Click **Next**.

19. Select **Use direct connection**.

ArcSight Console Configuration Wizard

ArcSight
Configure

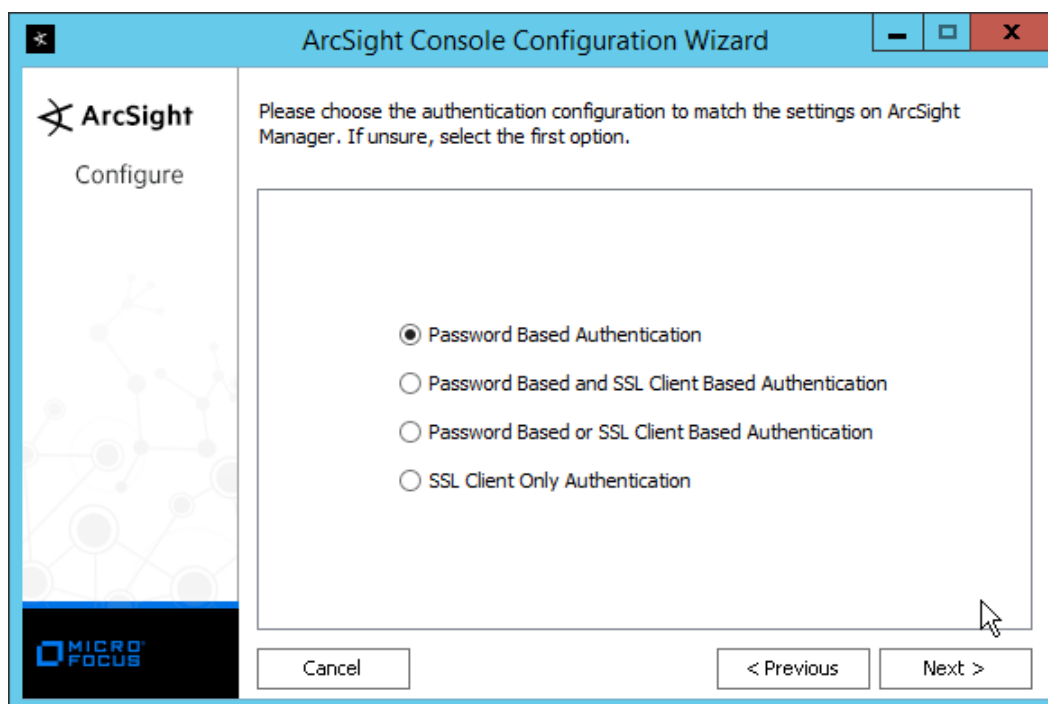
ArcSight Console can connect to ArcSight Manager using a HTTP proxy server. Please choose whether you would like to configure ArcSight Console for a proxy connection.

☒ Use direct connection.

☐ Use proxy server.

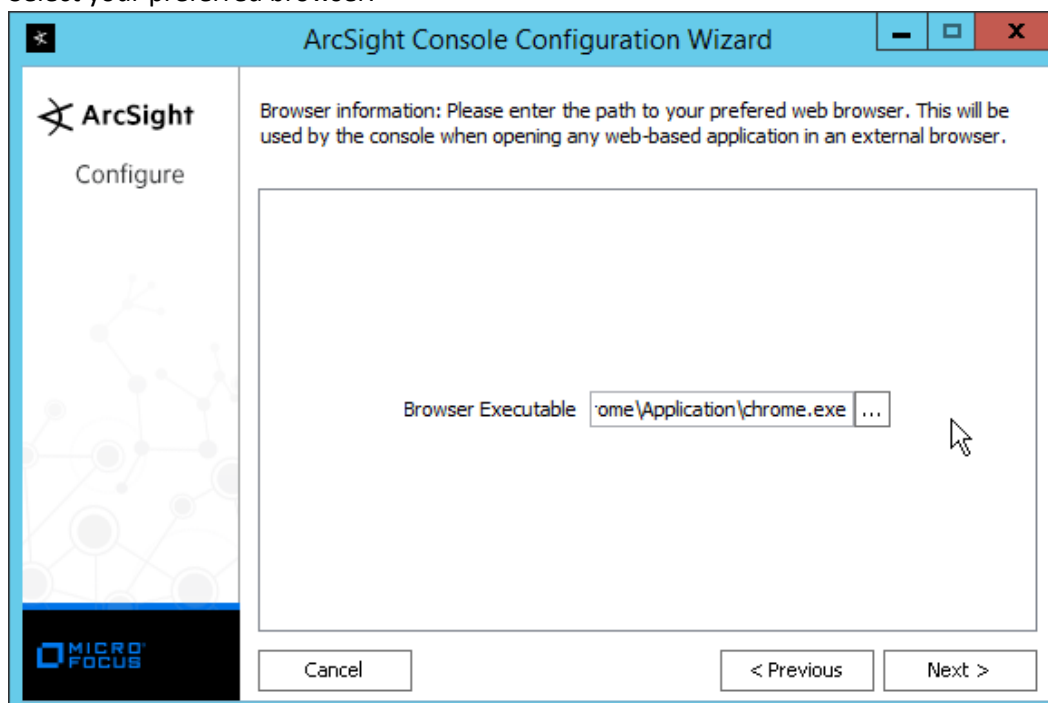
Buttons: Cancel, < Previous, Next >

20. Click **Next**.

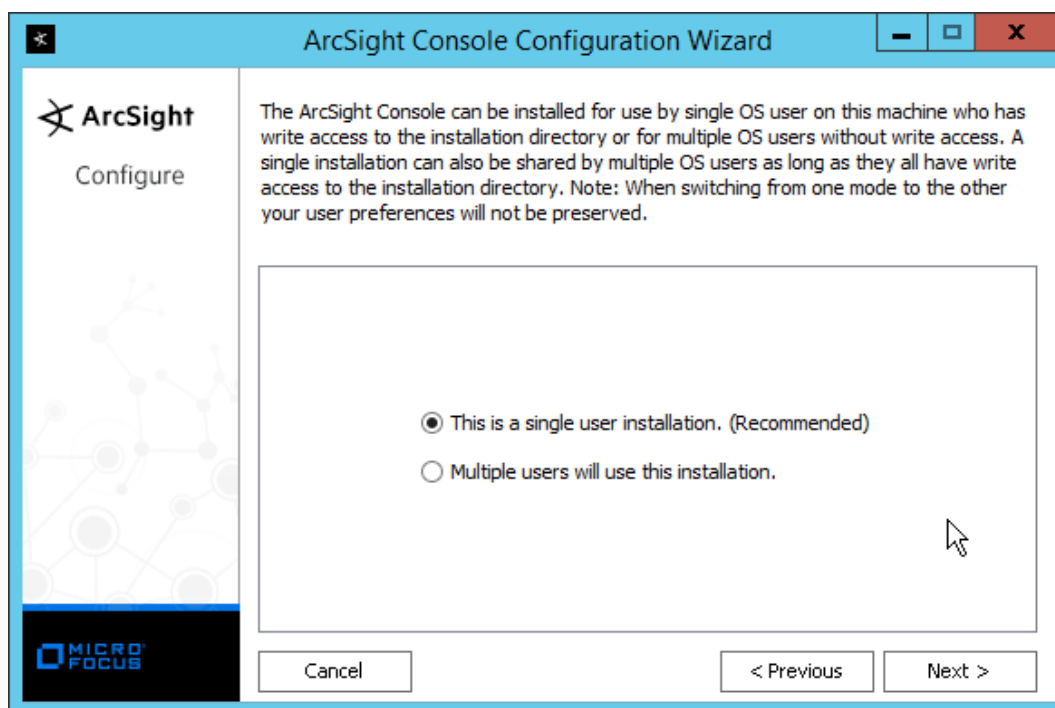


21. Click **Next**.

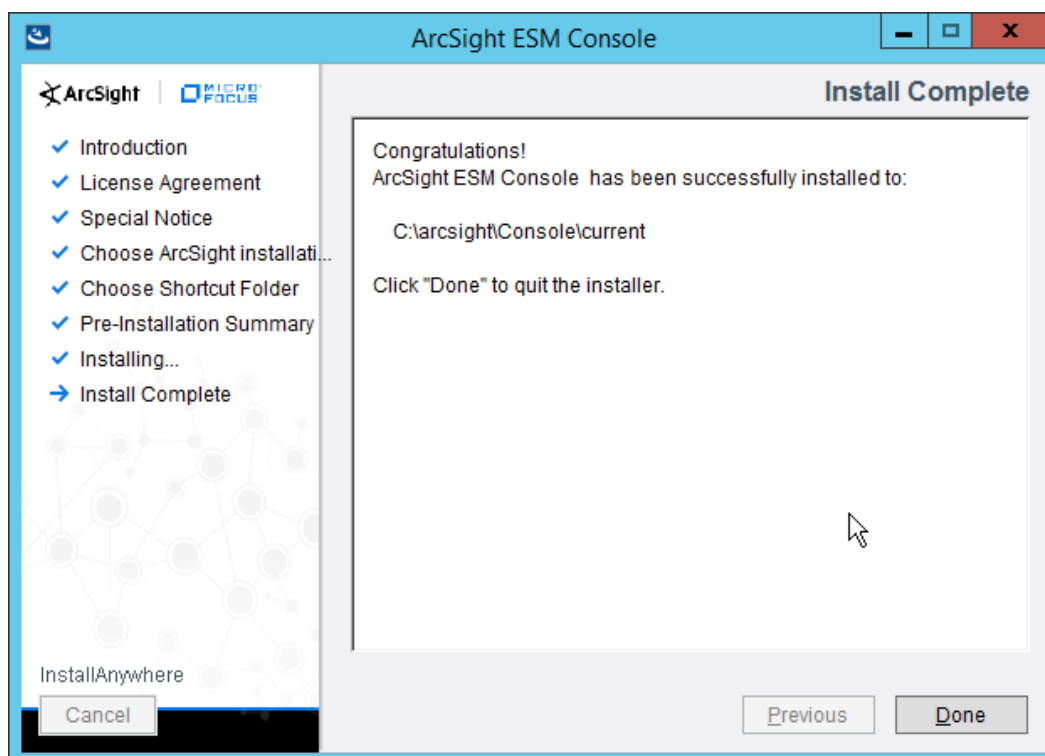
22. Select your preferred browser.



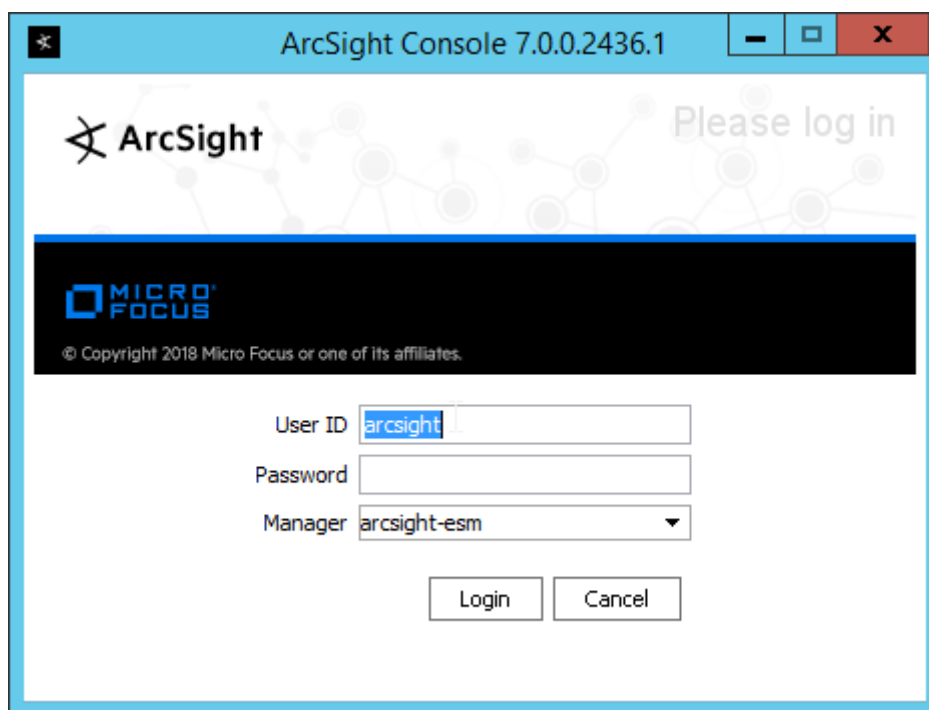
23. Click **Next**.



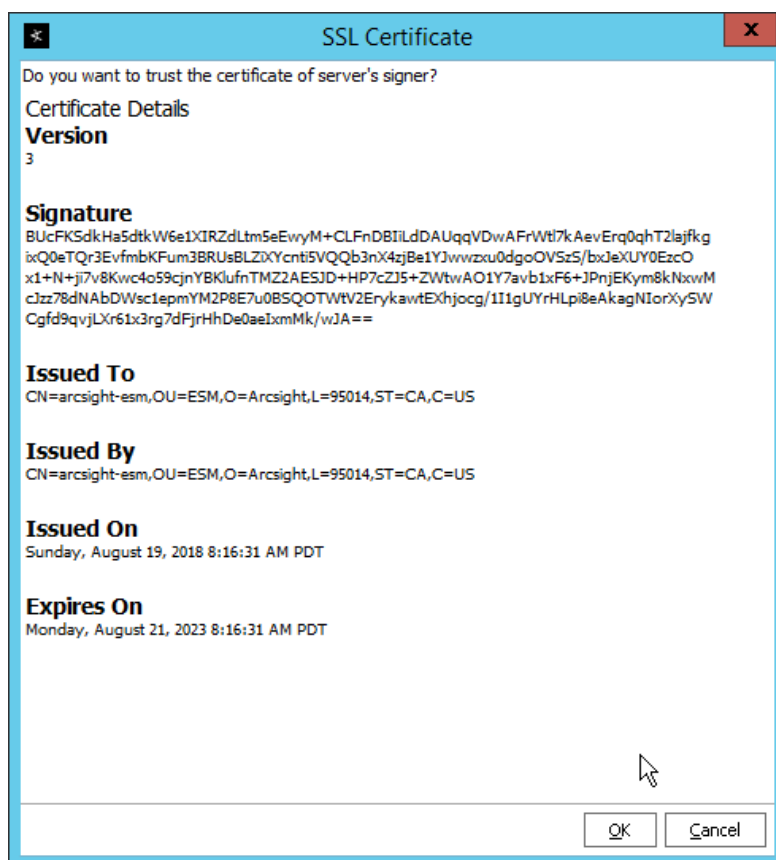
24. Click **Next**.
25. Click **Finish**.



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



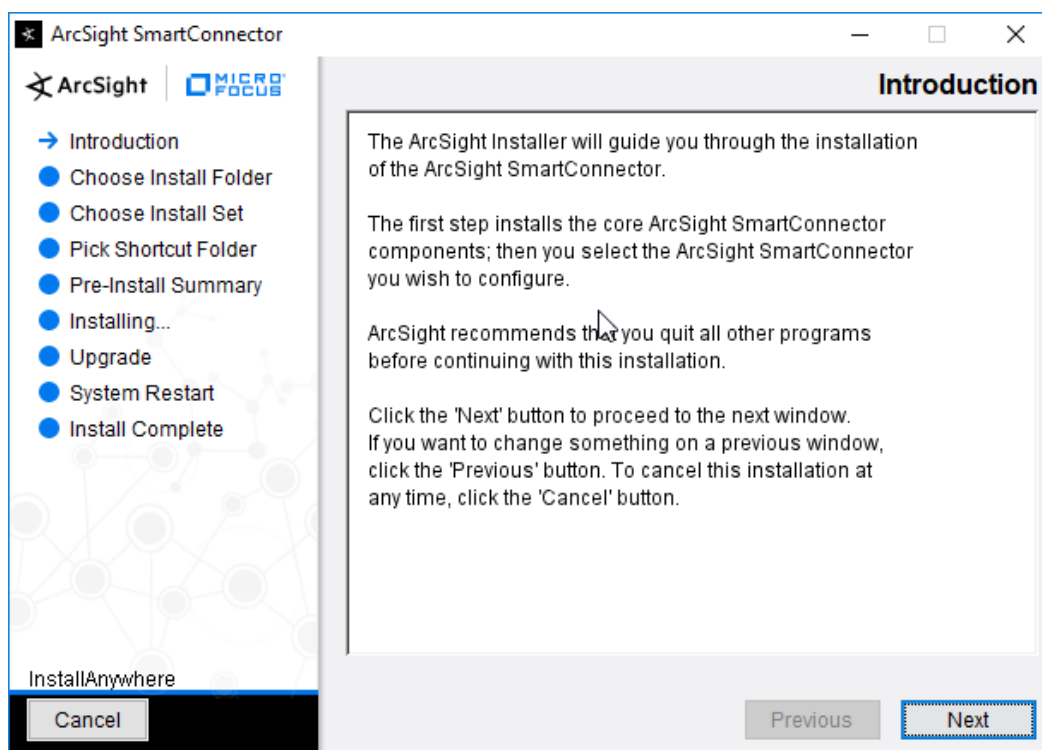
29. Click **Login**. (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)



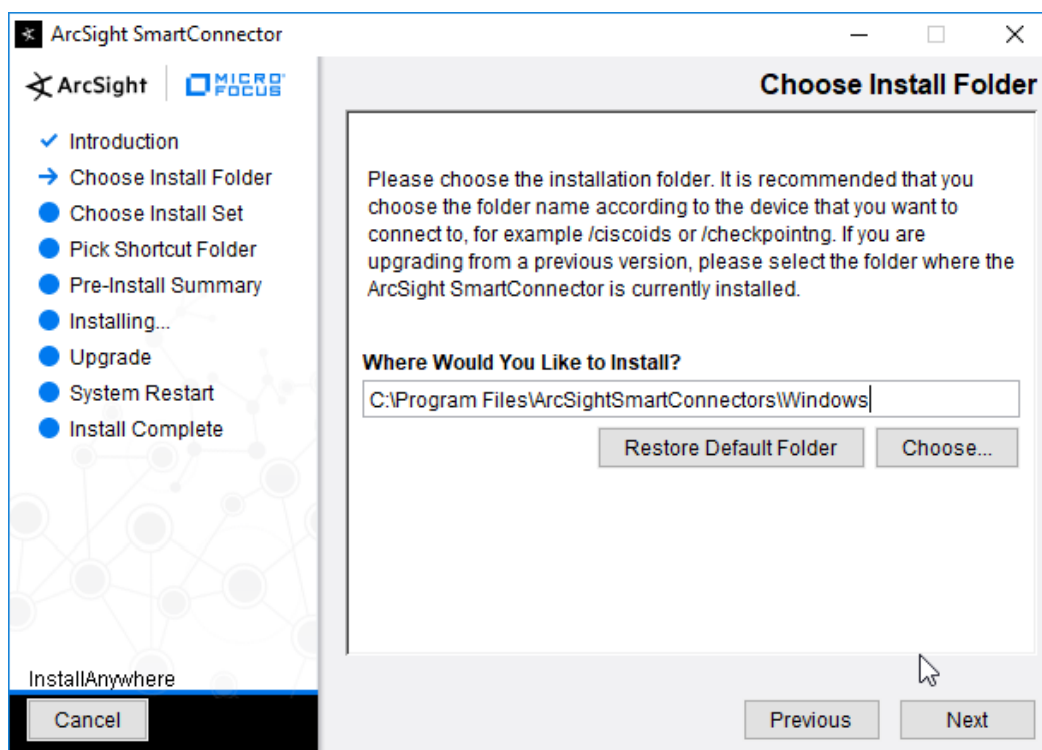
30. Click **OK**.

2.8.2 Install Individual ArcSight Windows Connectors

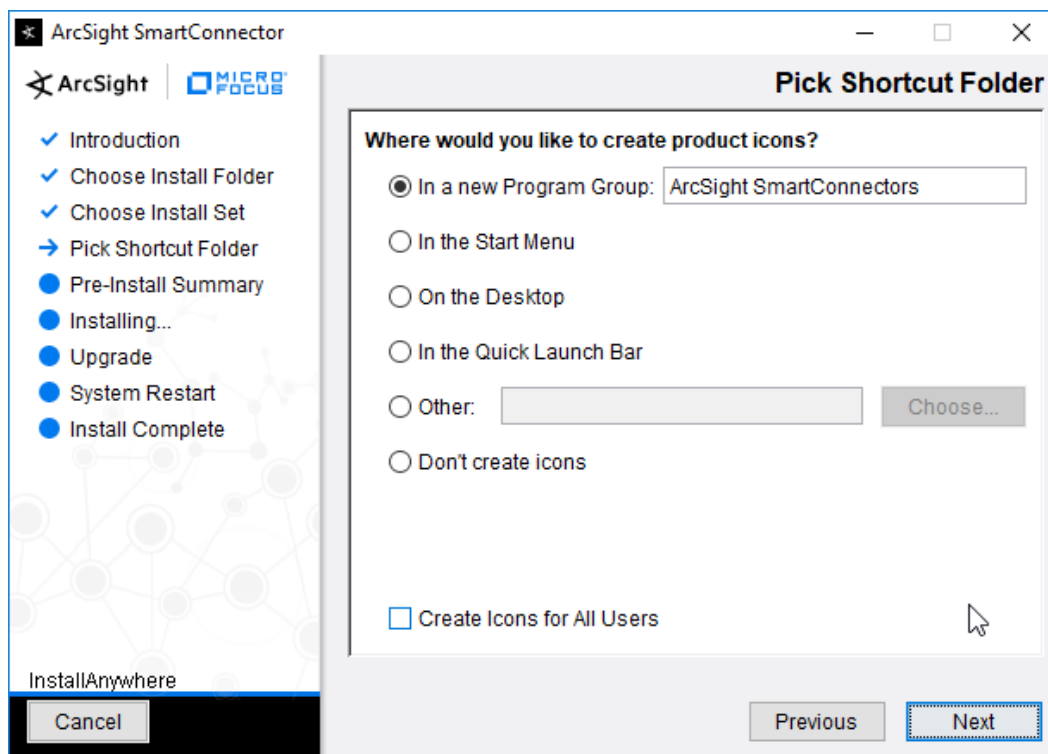
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



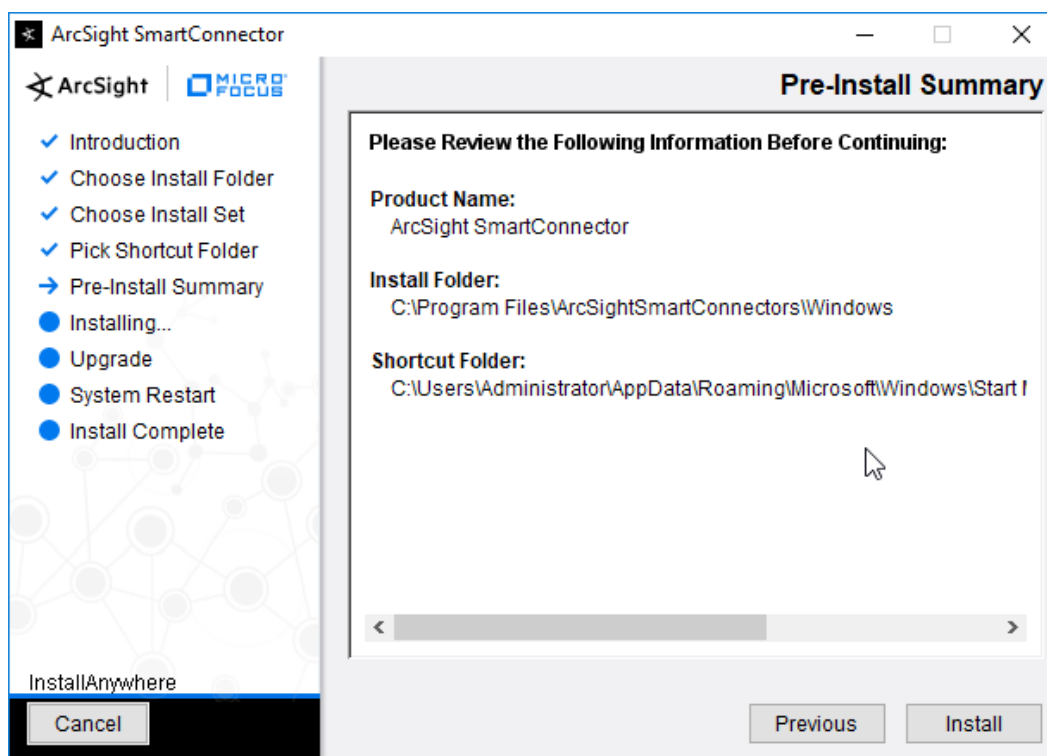
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



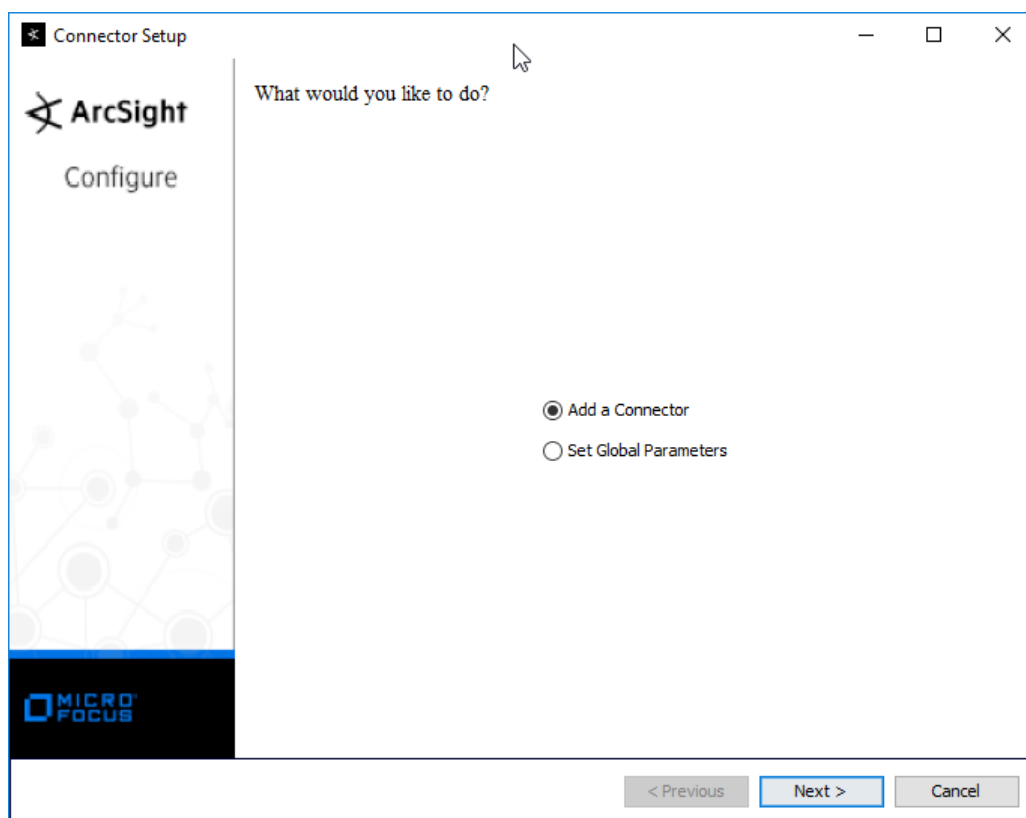
4. Click **Next**.



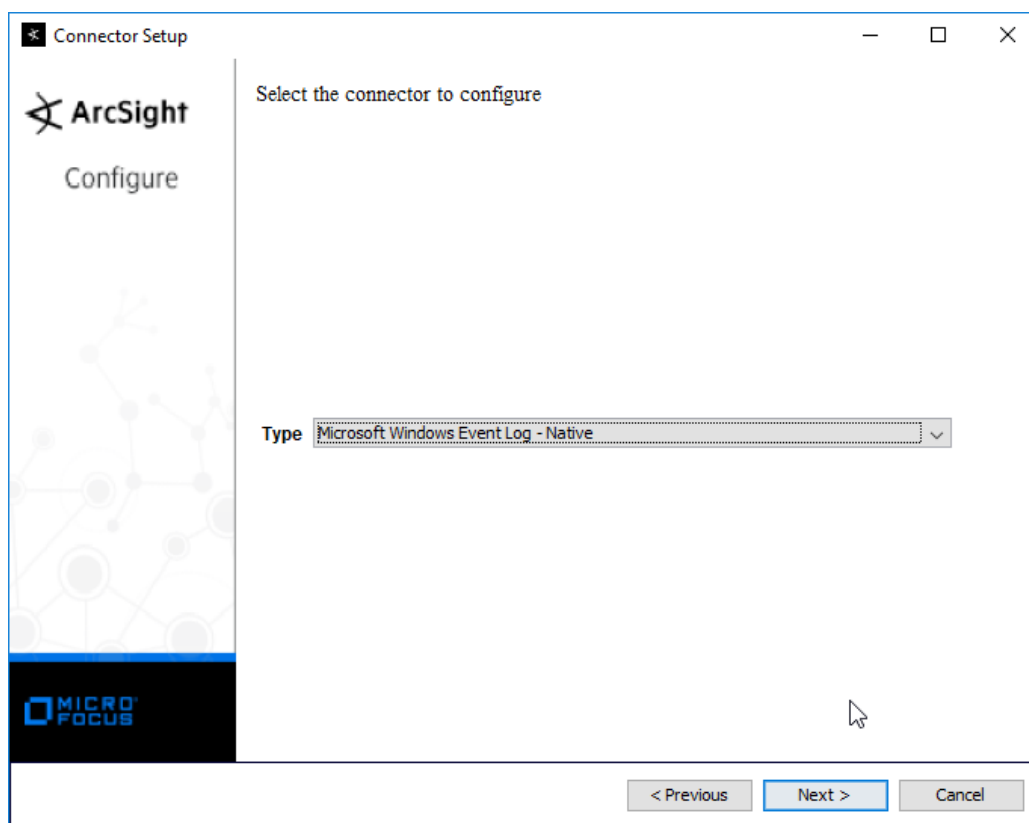
5. Click **Next**.



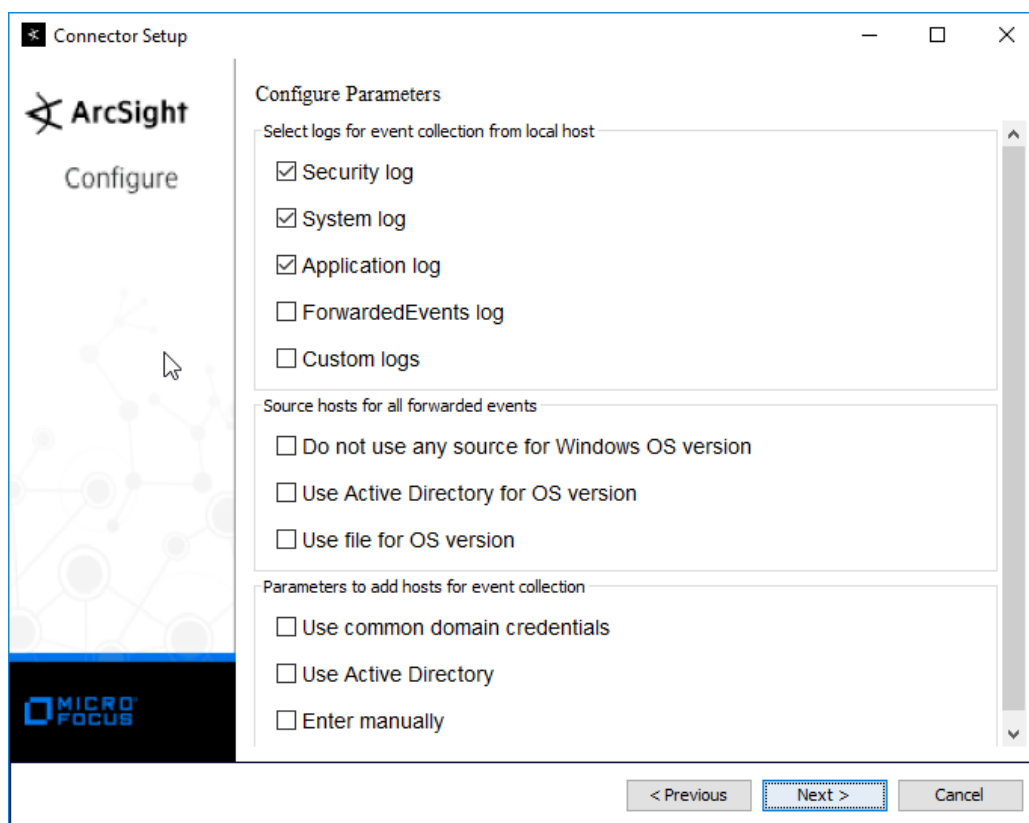
6. Click **Install**.
7. Select **Add a Connector**.



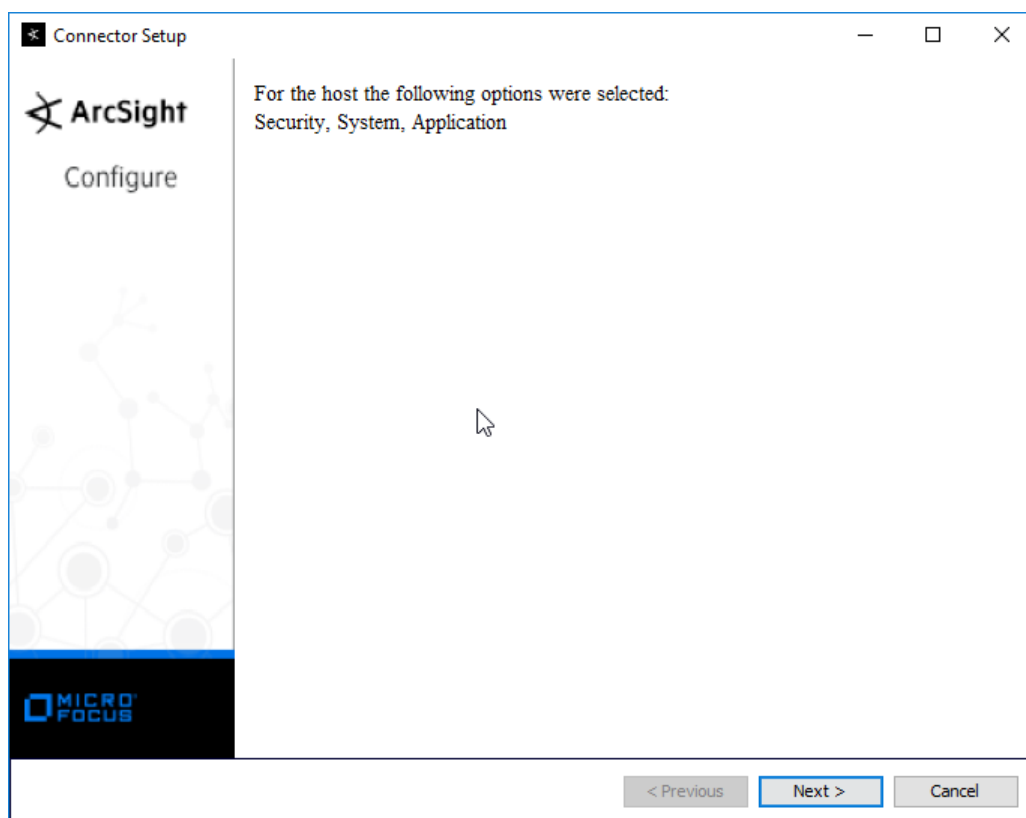
8. Click **Next**.
9. Select **Microsoft Windows Event Log – Native**.



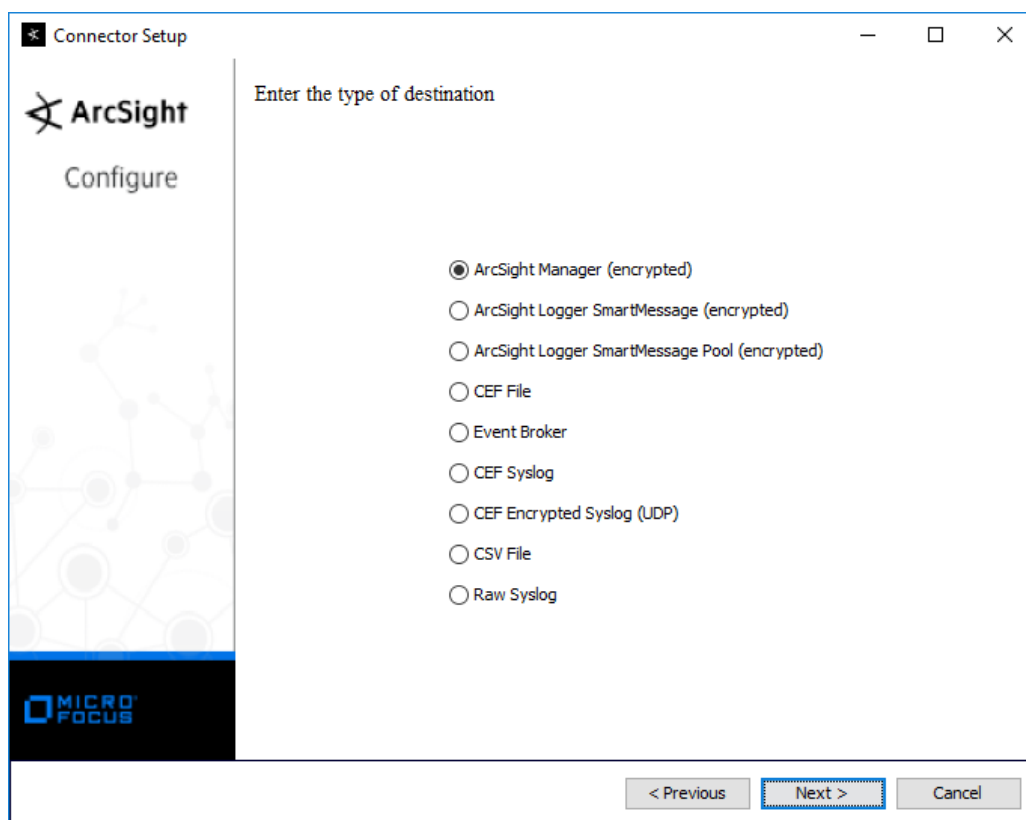
10. Click **Next**.



11. Click **Next**.



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



14. Click **Next**.

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

Connector Setup

ArcSight
Configure

Enter the destination parameters

Manager Hostname: arcsight-esm

Manager Port: 8443

User: administrator

Password: ••••••••

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: false

< Previous Next > Cancel

16. Click **Next**.

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

Connector Setup

ArcSight
Configure

Enter the connector details

Name: Windows10-1

Location:

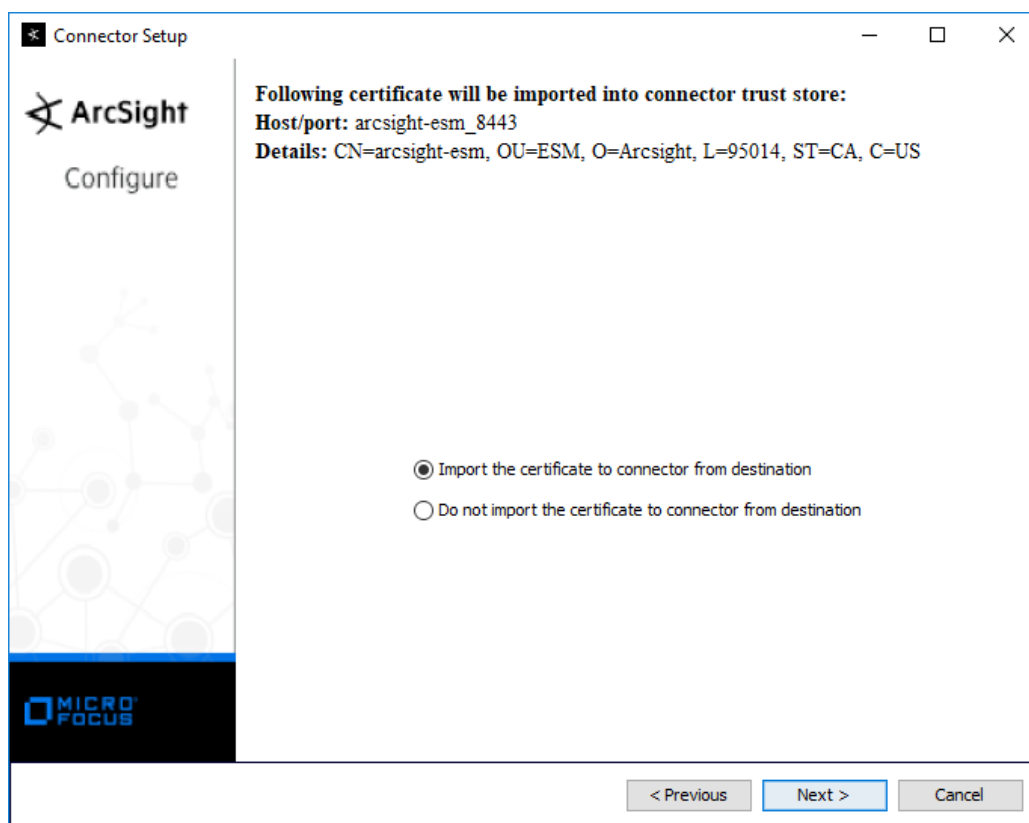
DeviceLocation:

Comment: Windows10-1 Client

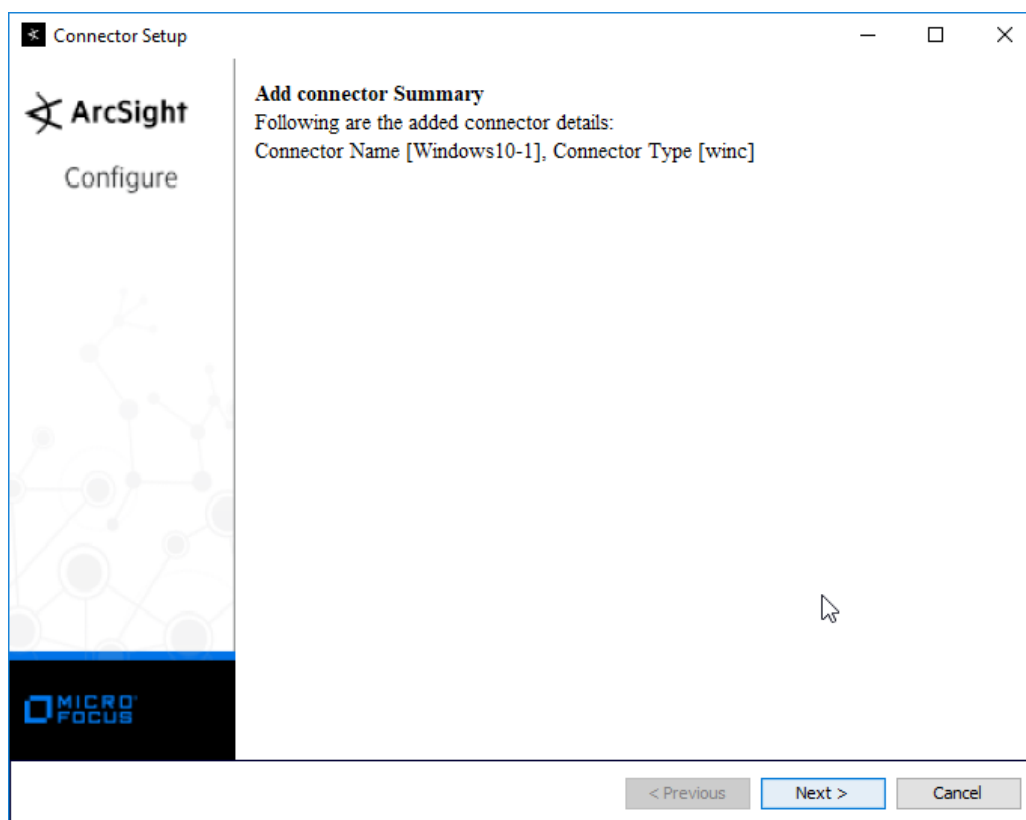
< Previous Next > Cancel

18. Click **Next**.

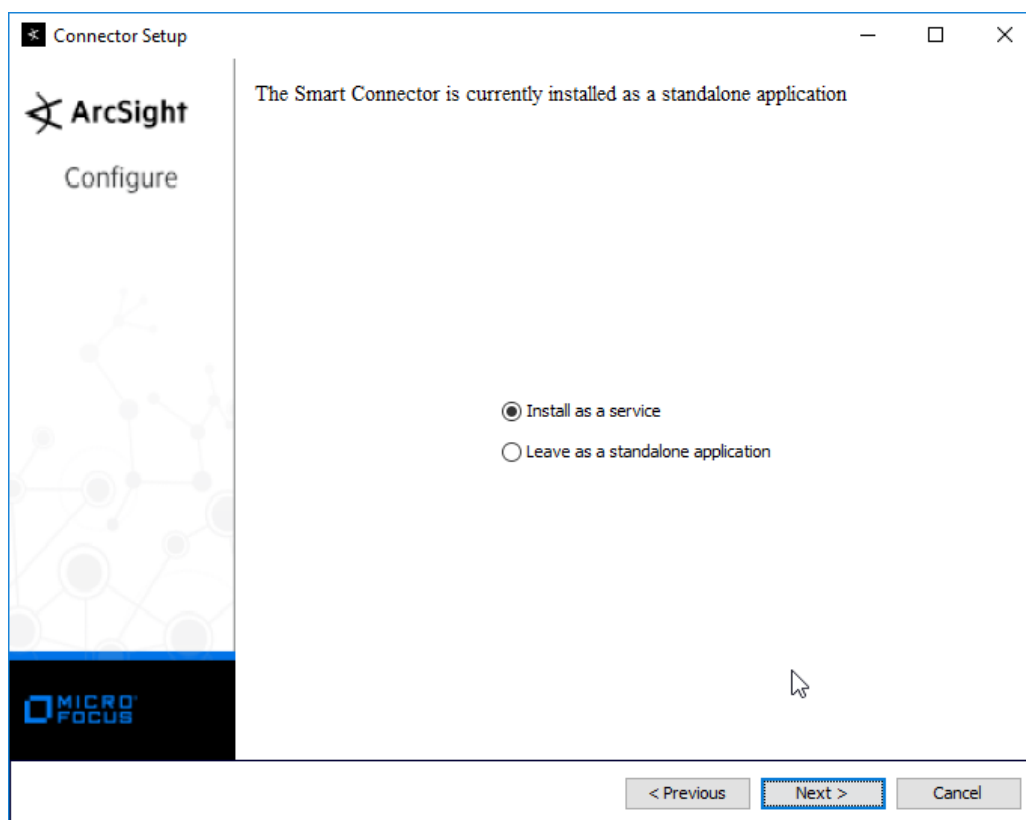
19. Select **Import the certificate to connector from destination**.



20. Click **Next**.



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



23. Click **Next**.

Connector Setup

ArcSight
Configure

Specify the service parameters

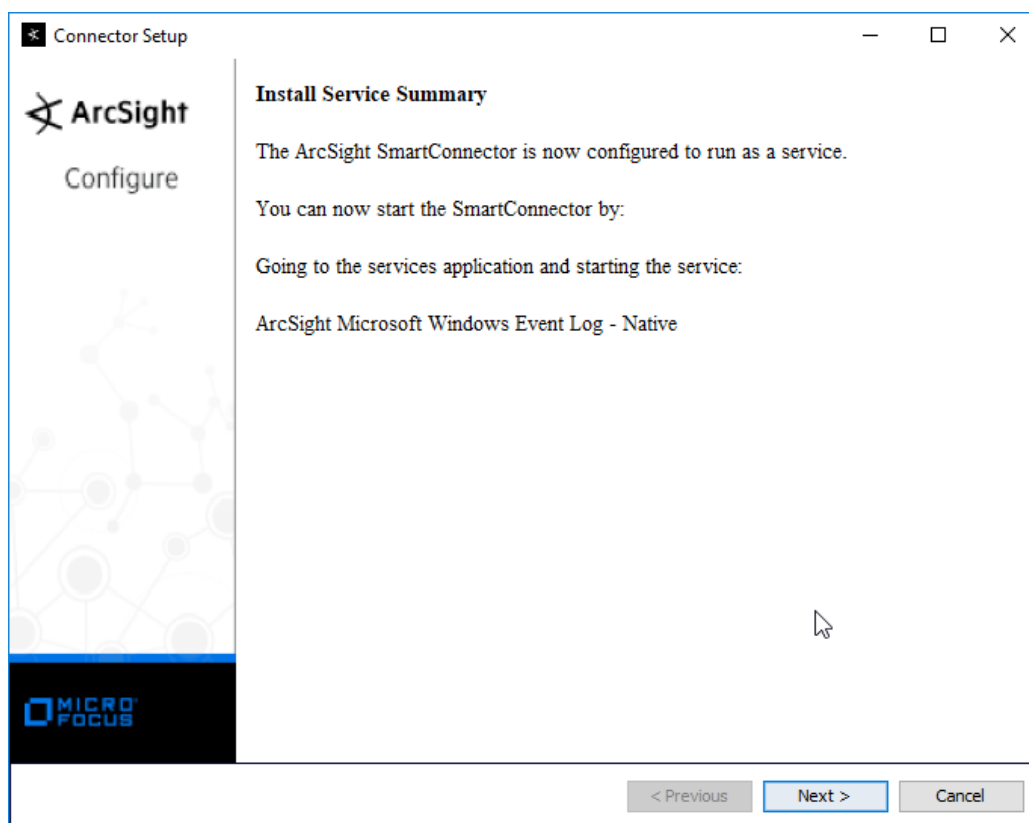
Service Internal Name: winc

Service Display Name: Microsoft Windows Event Log - Native

Start the service automatically: Yes

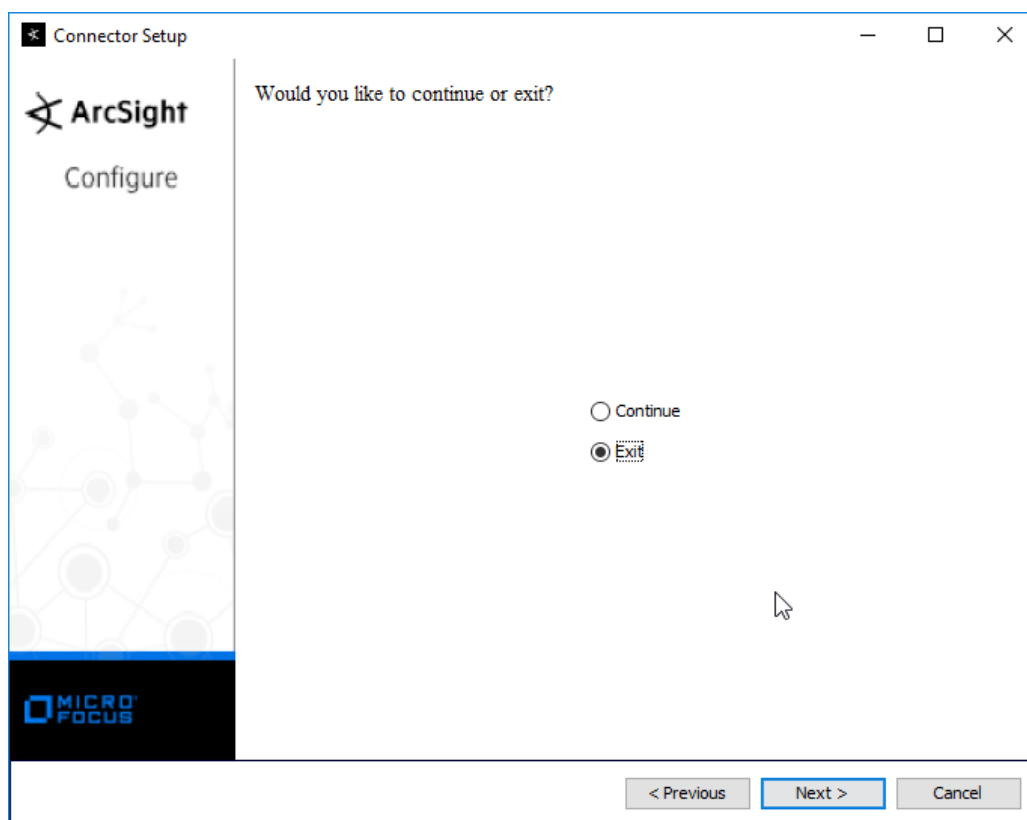
< Previous Next > Cancel

24. Click **Next**.

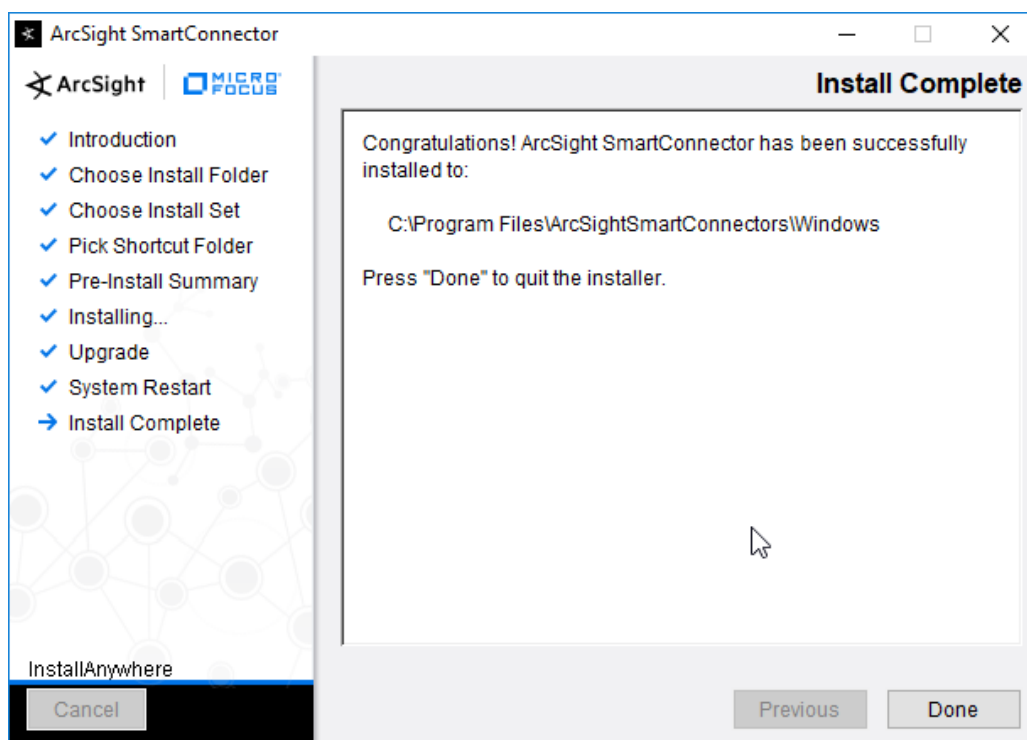


25. Click **Next**.

26. Select **Exit**.



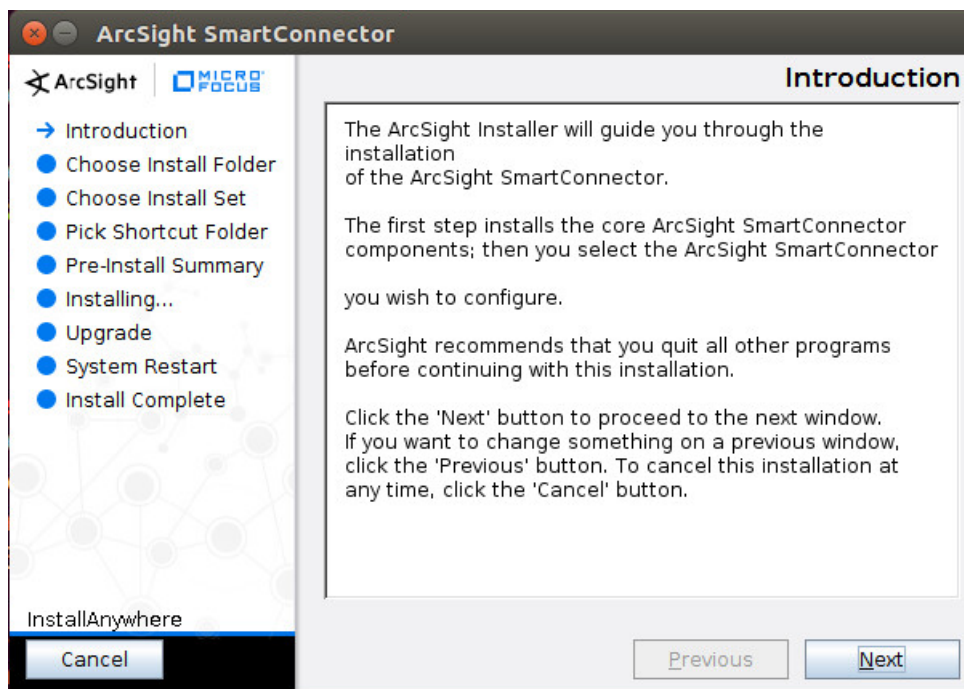
27. Click **Next**.



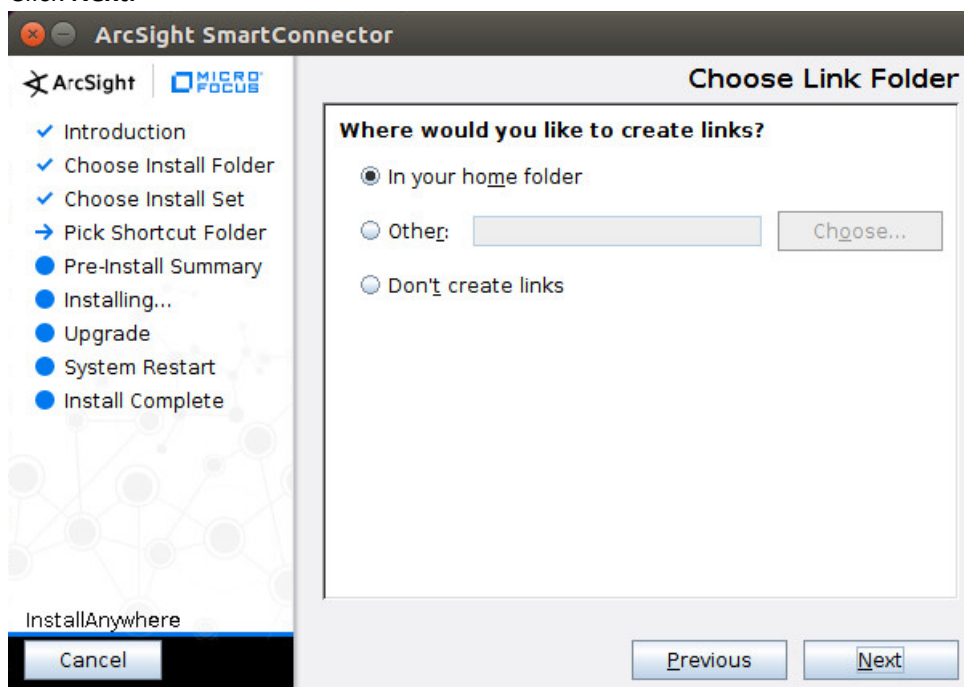
28. Click **Done**.

2.8.3 Install Individual ArcSight Ubuntu Connectors

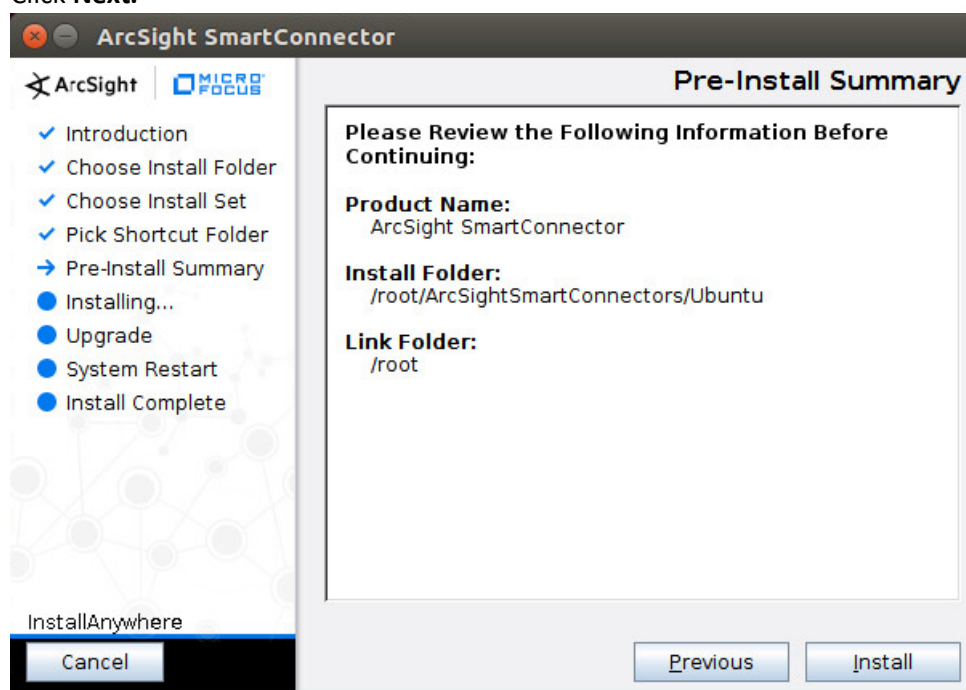
1. From the command line, run:
> `sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin`
2. Enter the **password** if prompted.



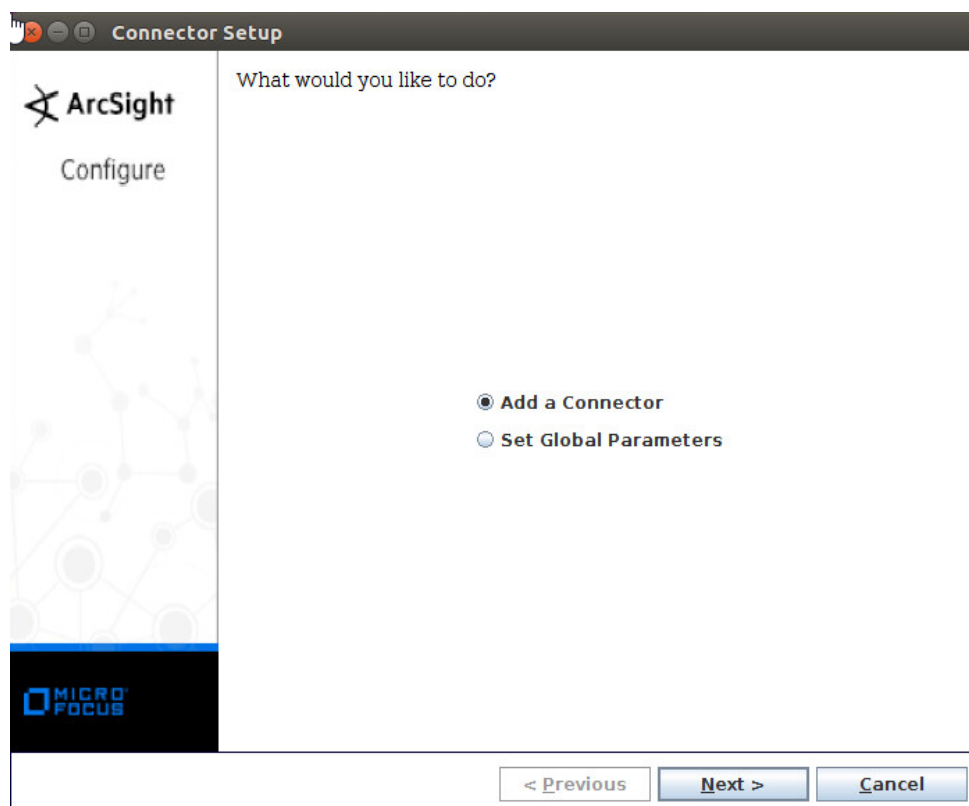
3. Click **Next**.
4. Enter `/root/ArcSightSmartConnectors/Ubuntu`.
5. Click **Next**.



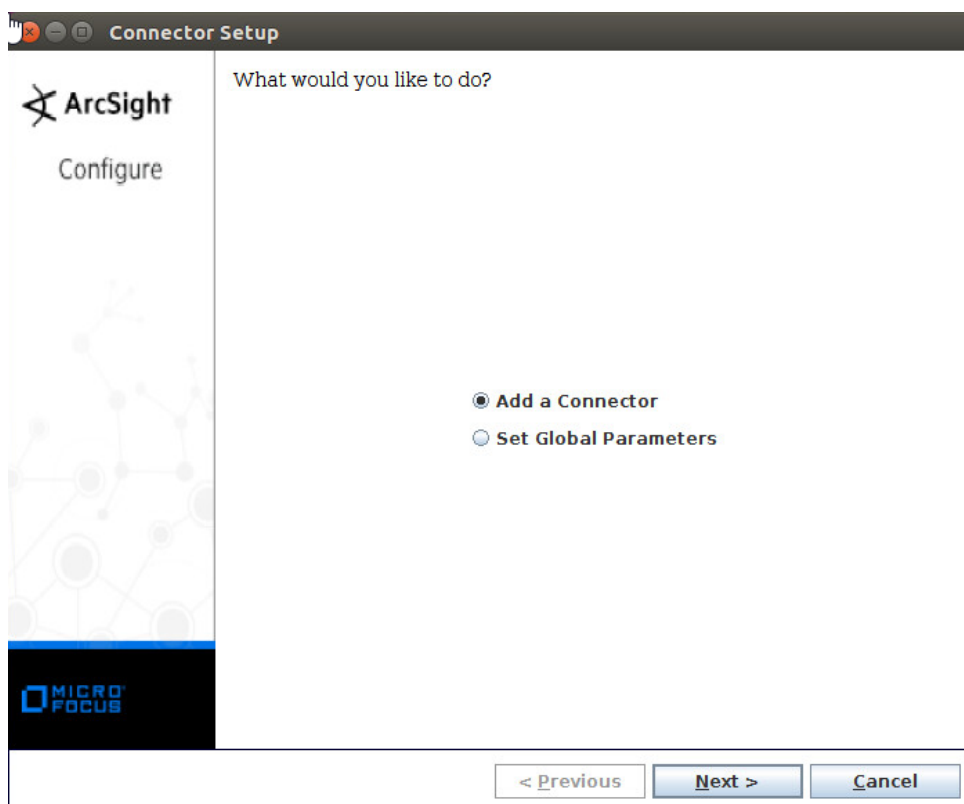
6. Click **Next**.



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



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



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

Connector Setup

ArcSight
Configure

Enter the parameter details

File Absolute Path Name ...

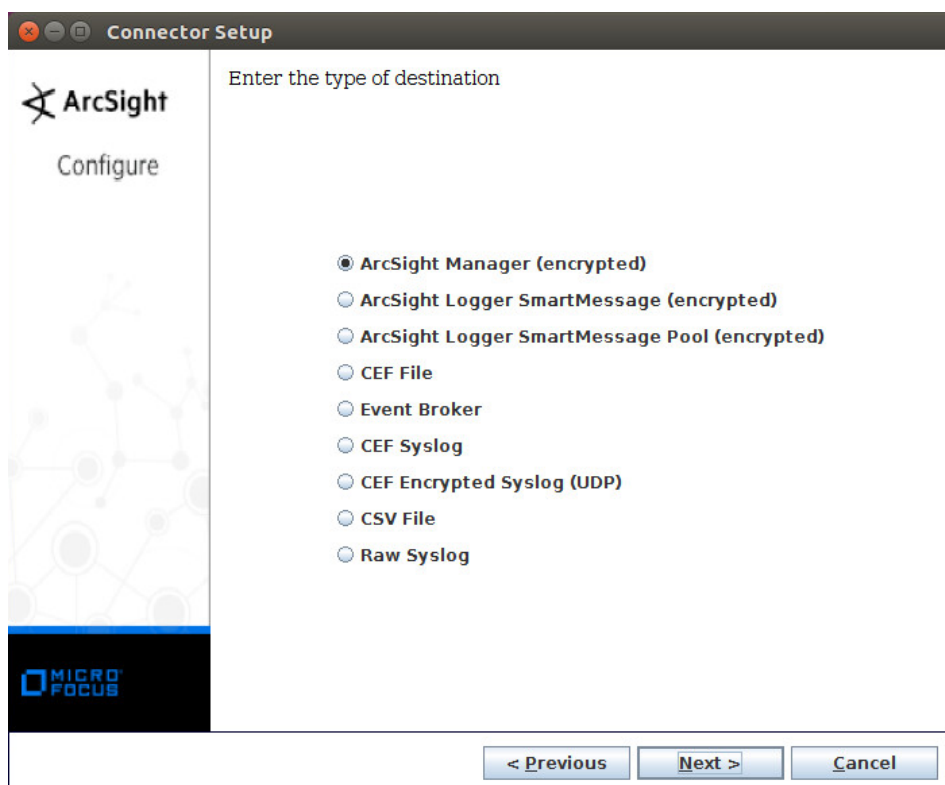
Reading Events Real Time or Batch **realtime** ▼

Action Upon Reaching EOF **None** ▼

File Extension If Rename Action

< Previous Next > Cancel

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



15. Click **Next**.

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

Connector Setup

ArcSight
Configure

Enter the destination parameters

Manager Hostname: arcsight-esm

Manager Port: 8443

User: administrator

Password:

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: false

< Previous Next > Cancel

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

Connector Setup

ArcSight
Configure

Enter the connector details

Name

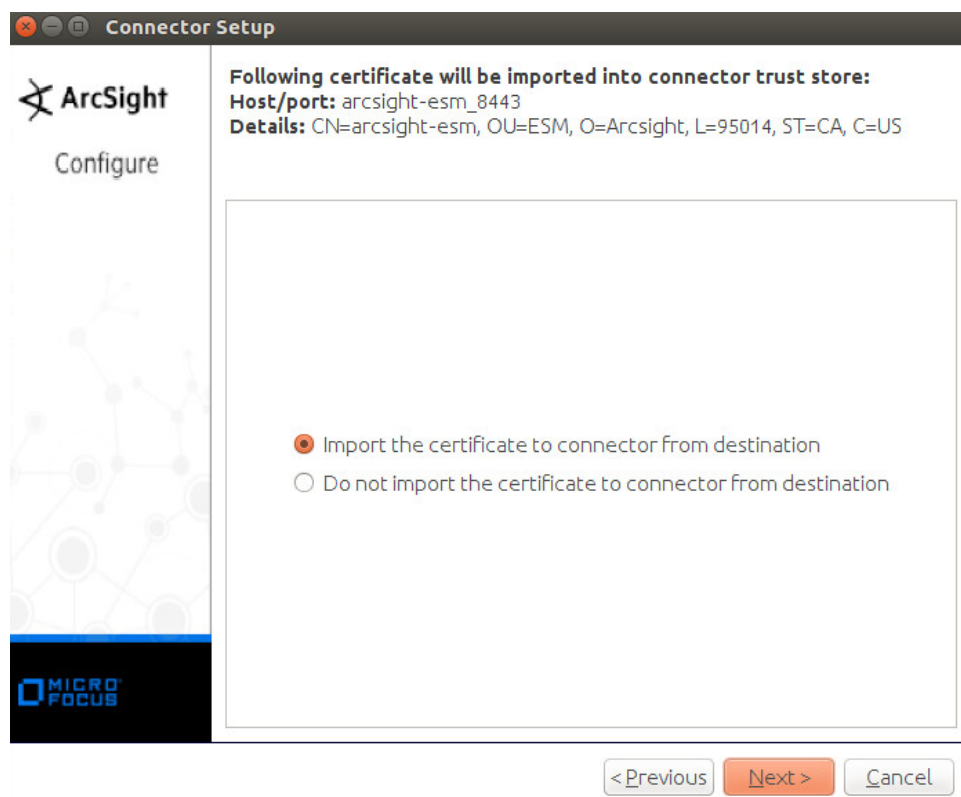
Location

DeviceLocation

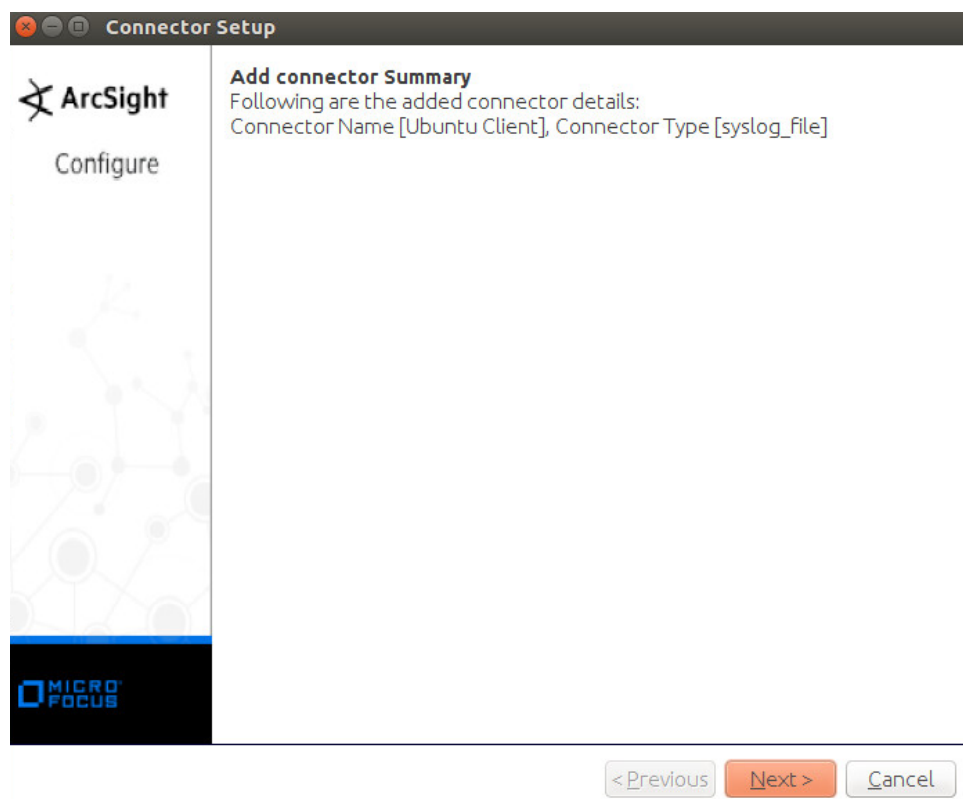
Comment

< Previous Next > Cancel

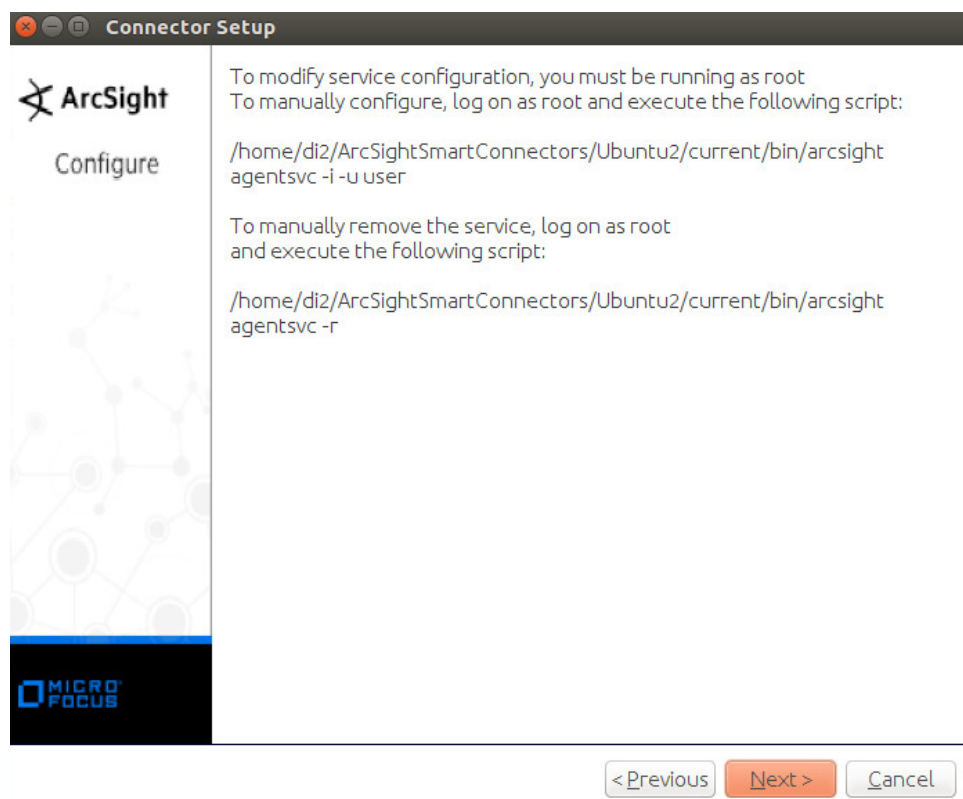
19. Click **Next**.
20. Select **Import the certificate to connector from destination**.



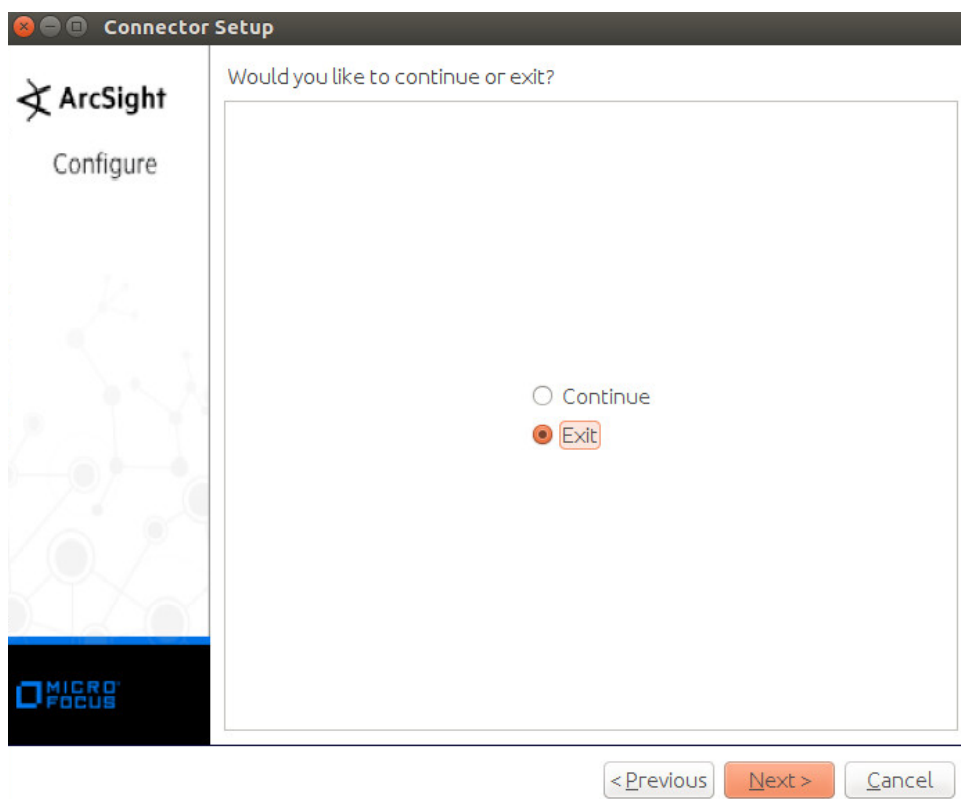
21. Click **Next**.



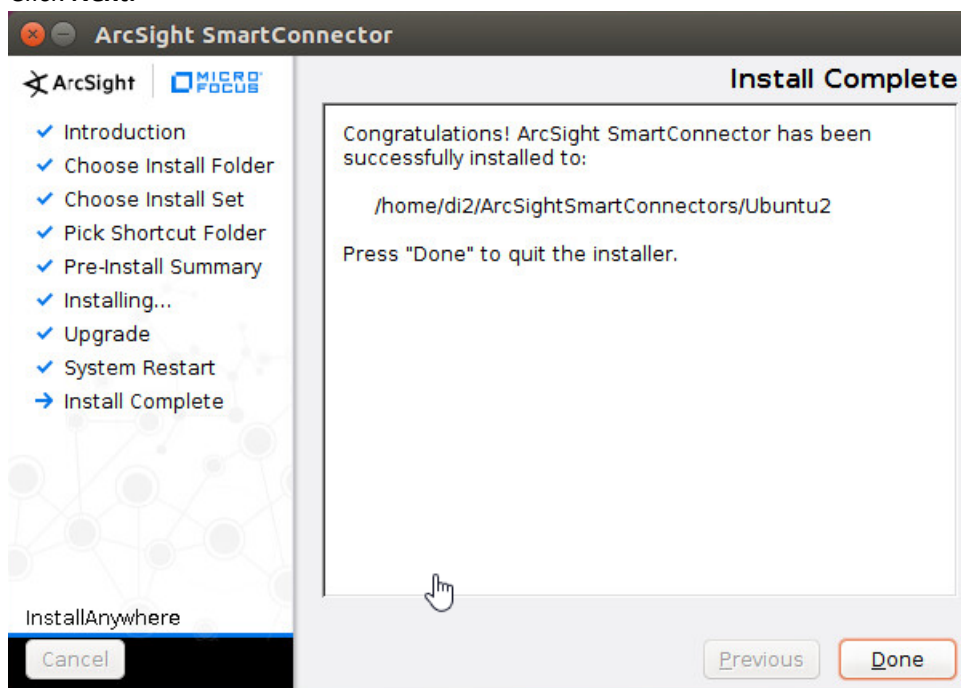
22. Click **Next**.



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



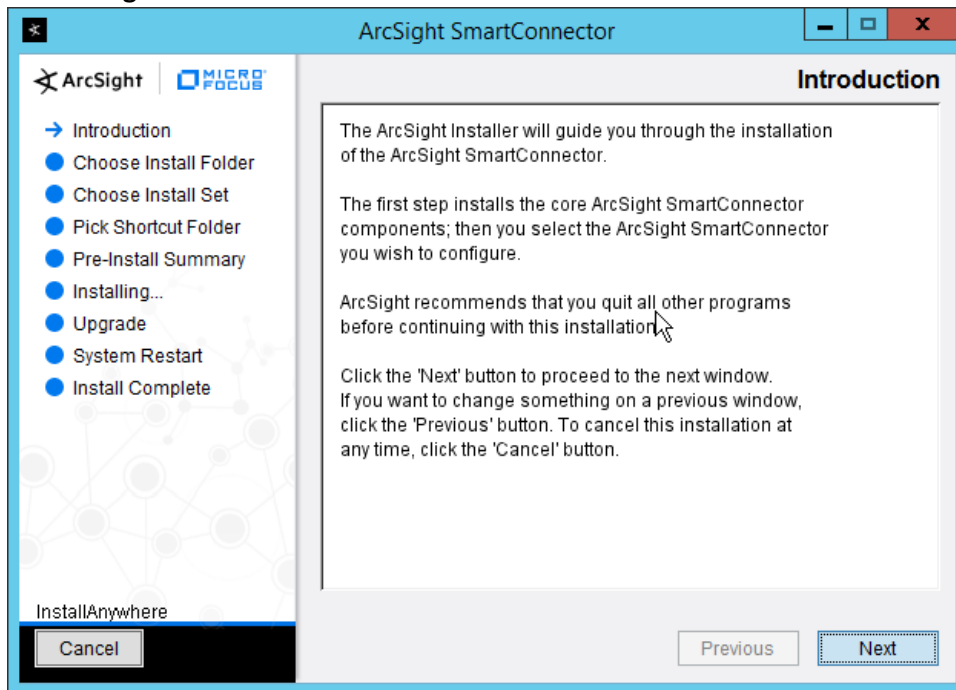
25. Click **Next**.



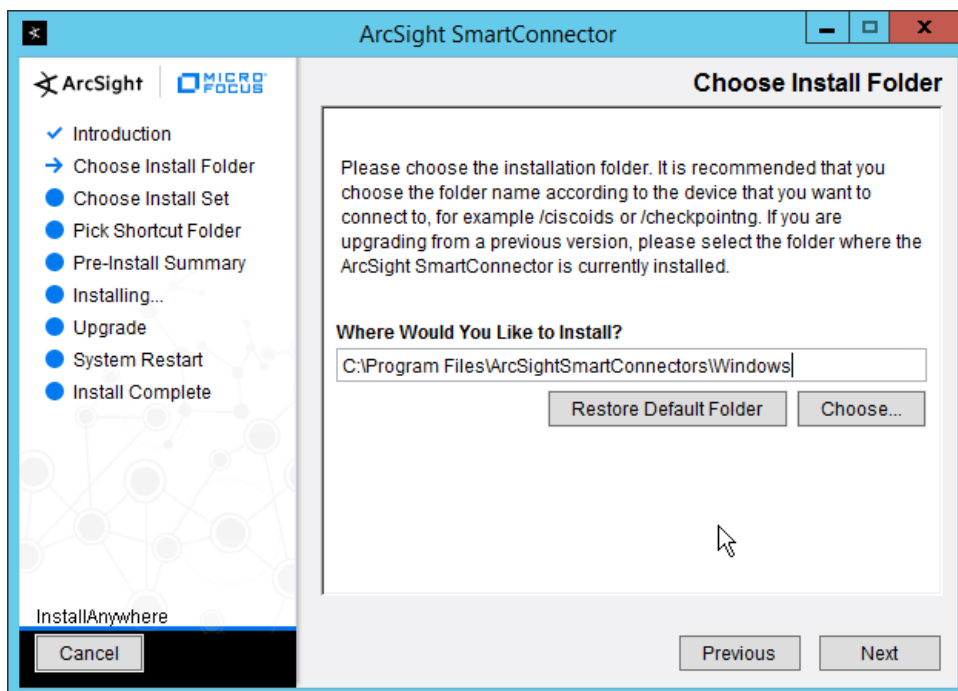
26. Click **Done**.

2.8.4 Install a Connector Server for ESM on Windows 2012 R2

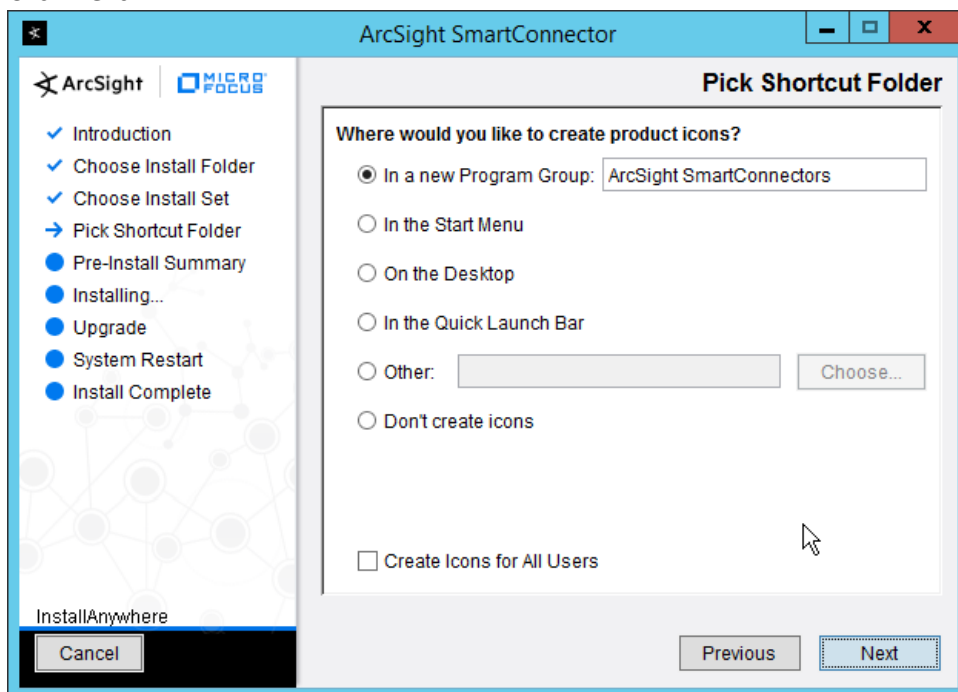
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



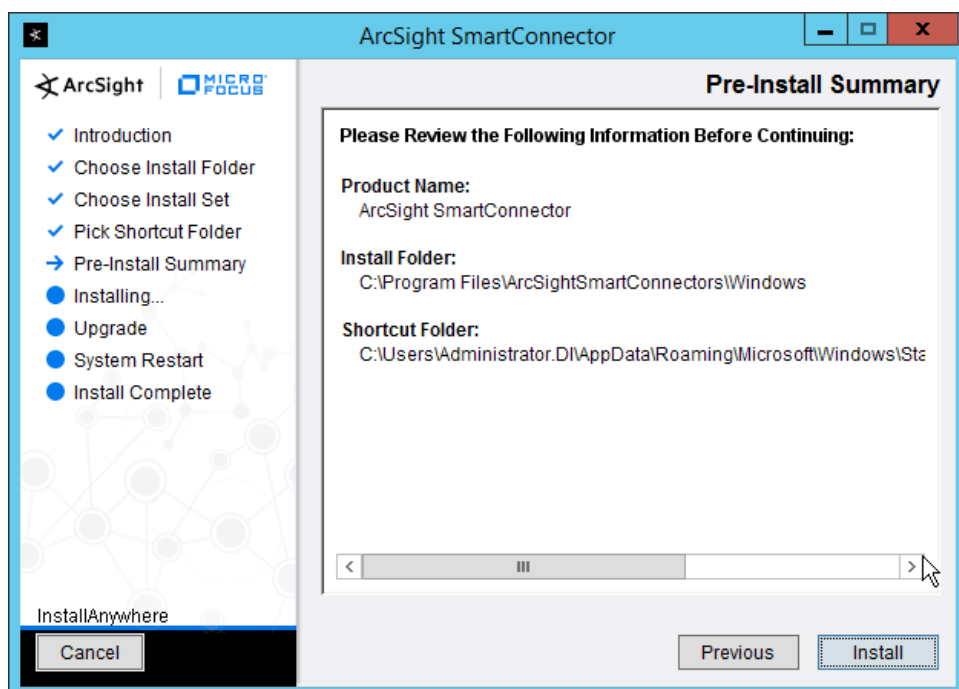
2. Click **Next**.
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows*.



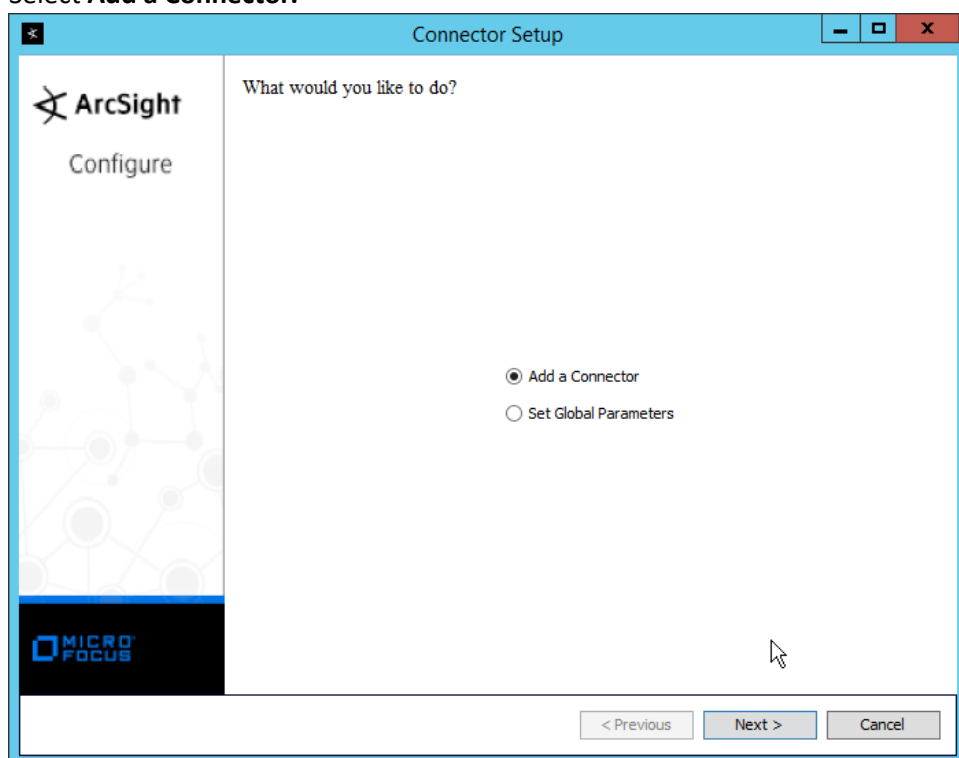
4. Click **Next**.



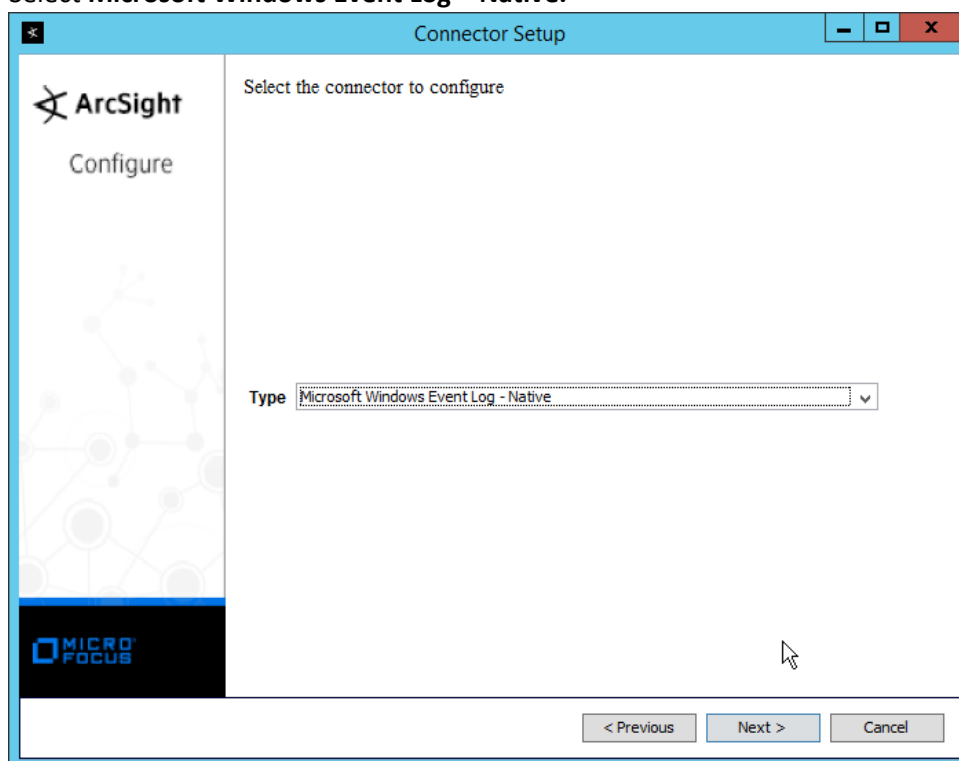
5. Click **Next**.



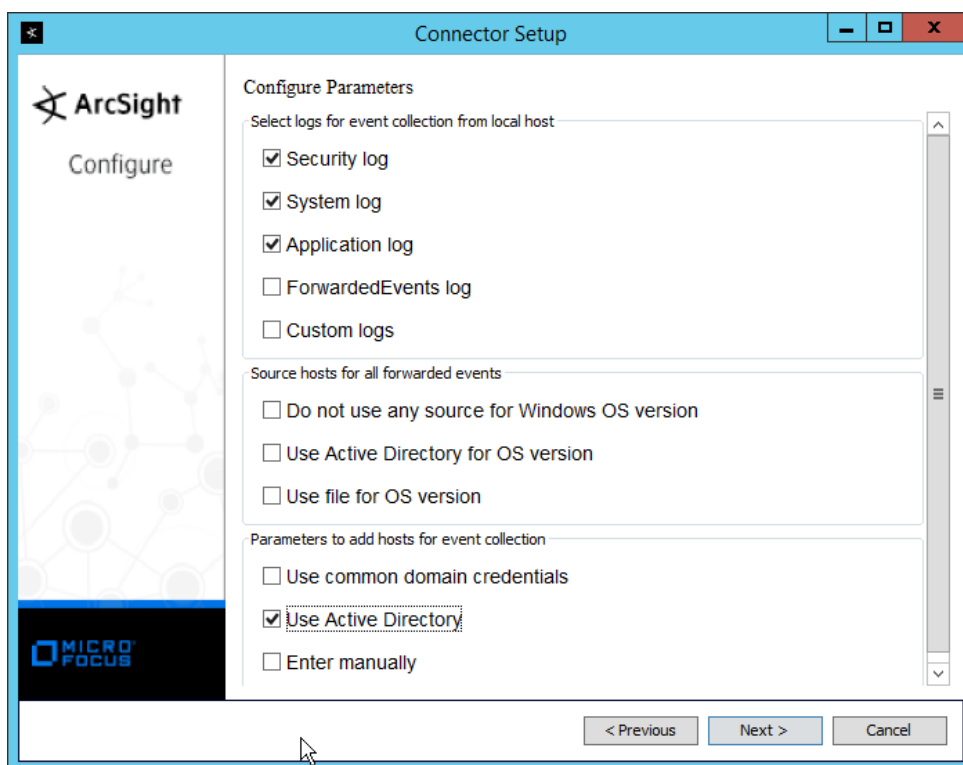
6. Click **Install**.
7. Select **Add a Connector**.



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**.

Connector Setup

Enter the parameter details

Domain Name: DI

Domain User Name: arcsight_admin

Domain User Password:

Active Directory Domain: DI.IPDR

Active Directory User Name: arcsight_admin

Active Directory User Password:

Active Directory Server: ad-dns.di.ipdr

Active Directory Filter: (&(cn=*)(operatingsystem=*)(whencreated=*))

Active Directory Protocol: non_ssl

Use Active Directory host results for: Replace Hosts

< Previous **Next >** Cancel

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**.

Connector Setup

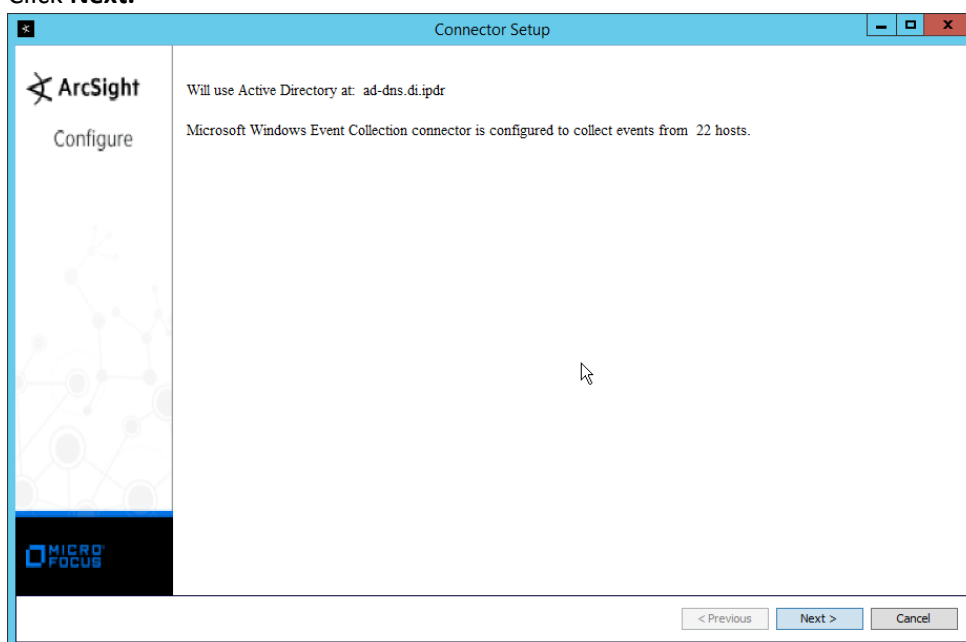
Enter the device details

	Host Name	Do...	Use...	Pas...	Win...	Is...	Sec...	Sys...	Appl...	For...	Cus...	Filter	Locale	Enc...
<input checked="" type="checkbox"/>	EXCHANGE-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	REMOTEDESKTOP3-DI...			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	WINDOWS10-1-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	WINDOWS10-2-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	HYPERV-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	MSSQL-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	WINDOWS10-3-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	UC-TEST-SERVER-DI.IP...			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	DESKTOP-7REQ7X0-DI...			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	TRIPWIRE-E-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	WIN-0LIQ7SM6HS2-DI...			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	WIN-K812P6E60K8-DI.I...			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	WIN-3H4L73215VT-DI.I...			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	AD-DNS08-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	BACKUP-STORAGE-DI.I...			Wind...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	BACKUPSERV-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	GLASSWALL-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8
<input checked="" type="checkbox"/>	SEMPERIS-DSP-DI.IPDR			Wind...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		*	en_US	UTF-8

Add Import Export

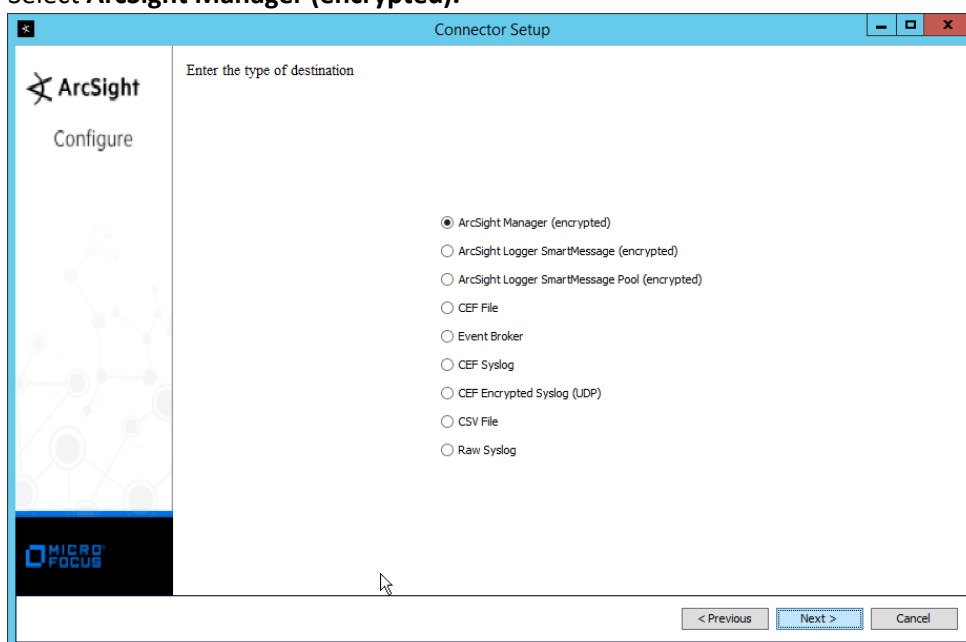
< Previous **Next >** Cancel

17. Click **Next**.



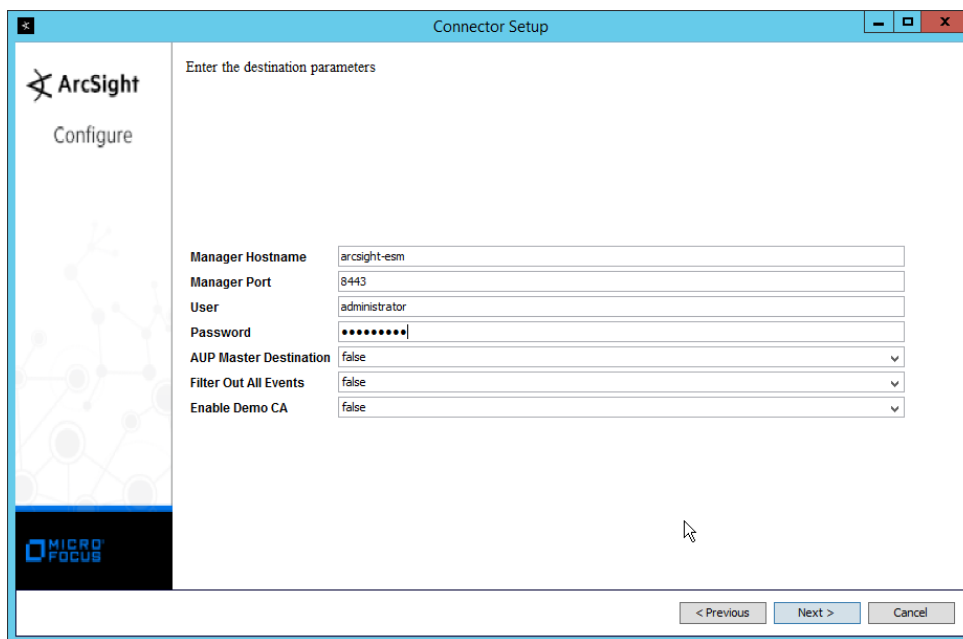
18. Click **Next**.

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



20. Click **Next**.

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



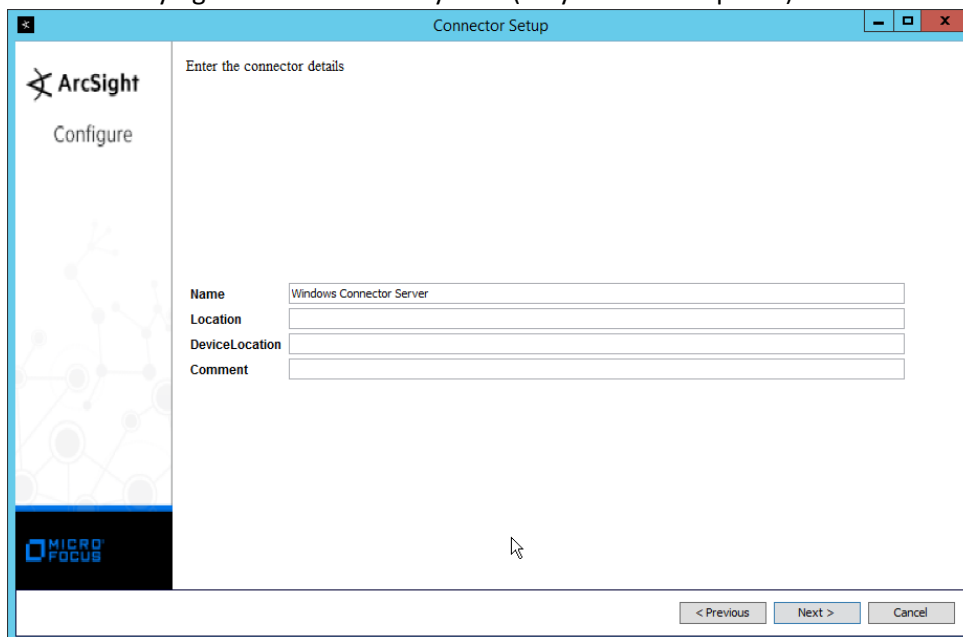
The screenshot shows the 'Connector Setup' window with the 'Enter the destination parameters' step. The left sidebar contains the ArcSight logo and a 'Configure' button. The main area has a form with the following fields:

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

At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

22. Click **Next**.

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



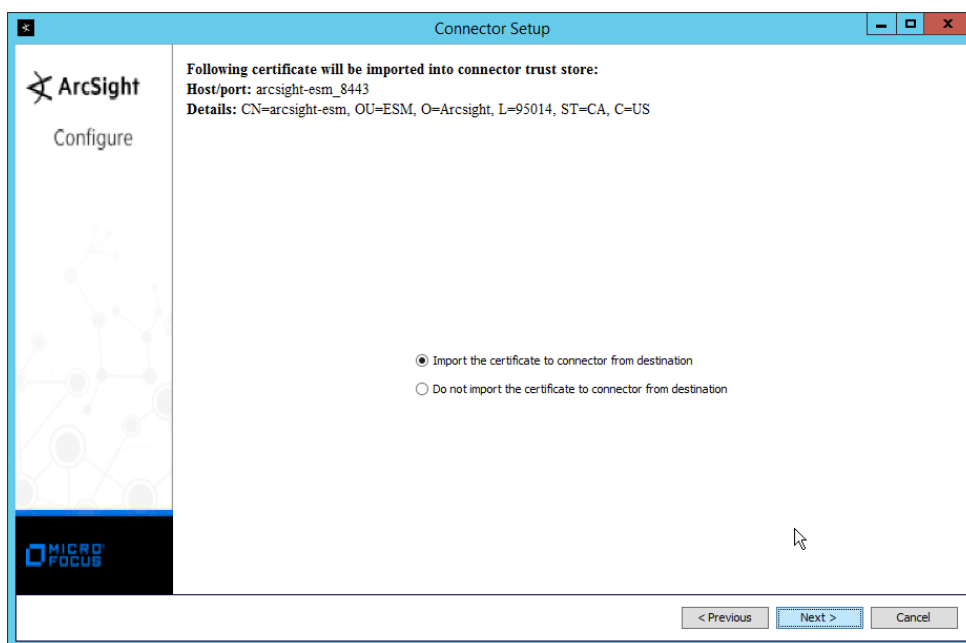
The screenshot shows the 'Connector Setup' window with the 'Enter the connector details' step. The left sidebar is the same as the previous screenshot. The main area has a form with the following fields:

Name	Windows Connector Server
Location	
DeviceLocation	
Comment	

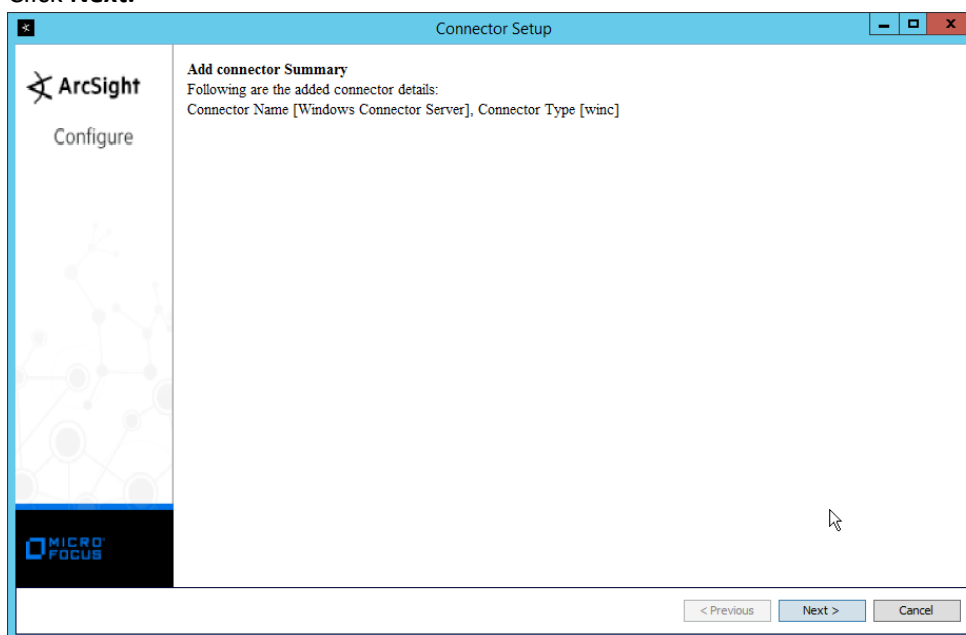
At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

24. Click **Next**.

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

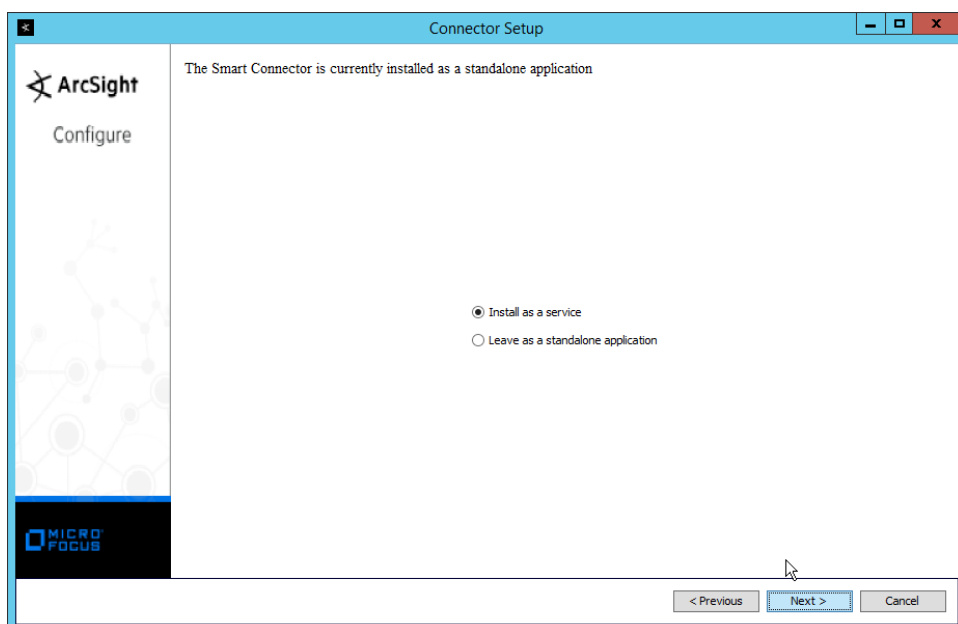


26. Click **Next**.

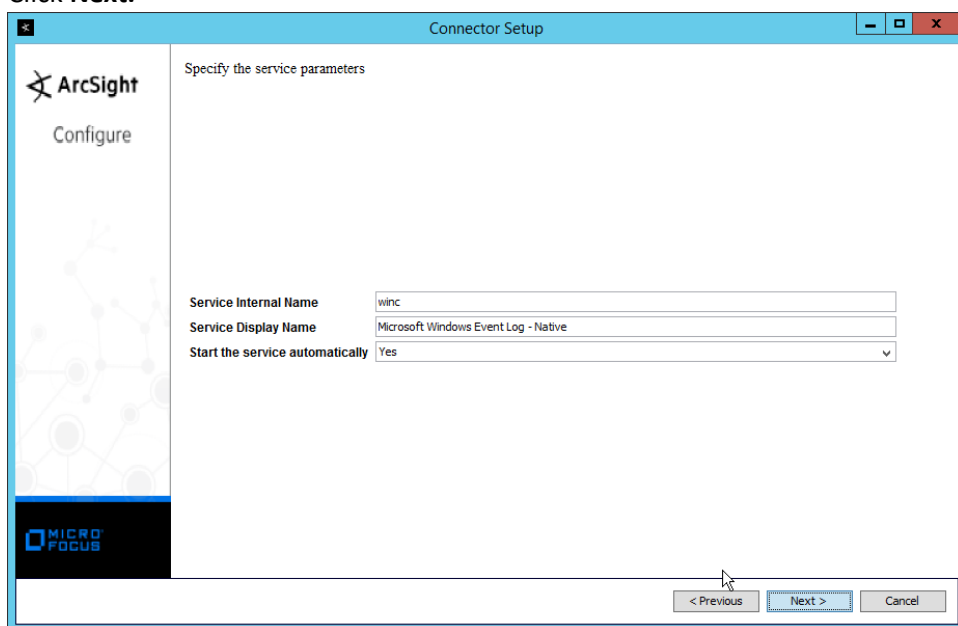


27. Click **Next**.

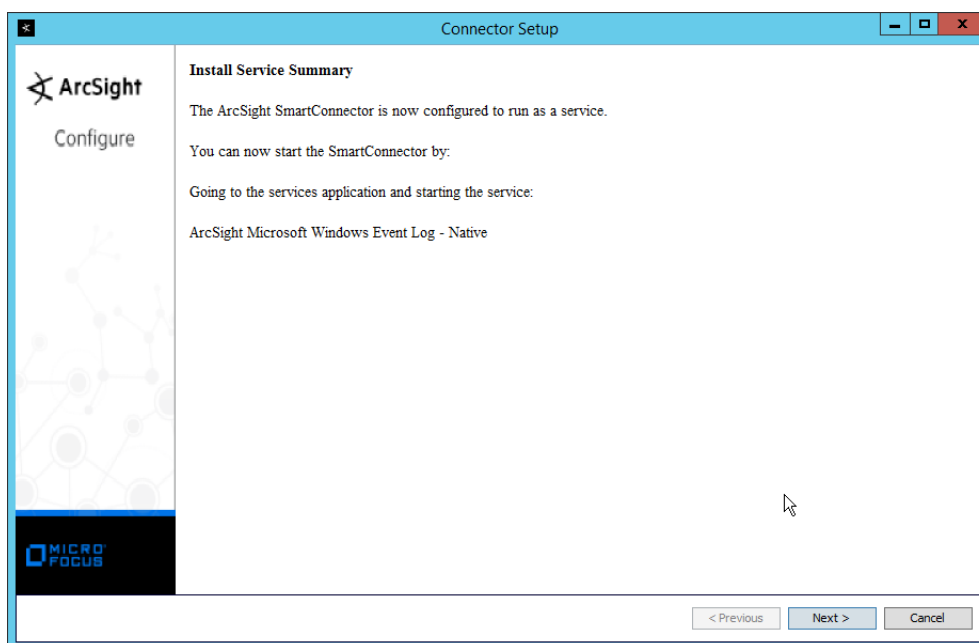
28. Select **Install as a service**.



29. Click **Next**.

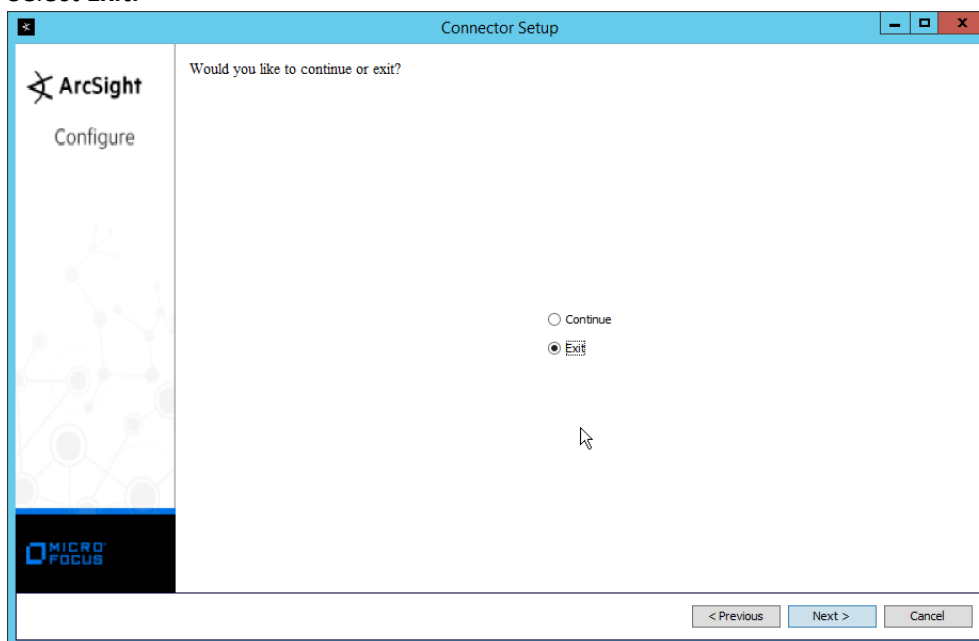


30. Click **Next**.

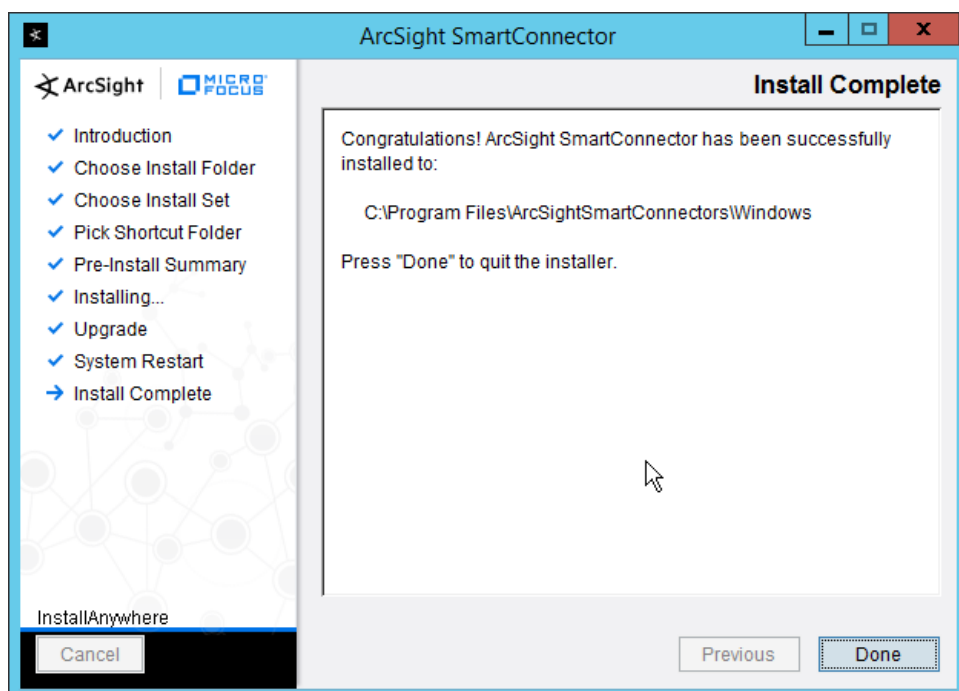


31. Click **Next**.

32. Select **Exit**.



33. Click **Next**.

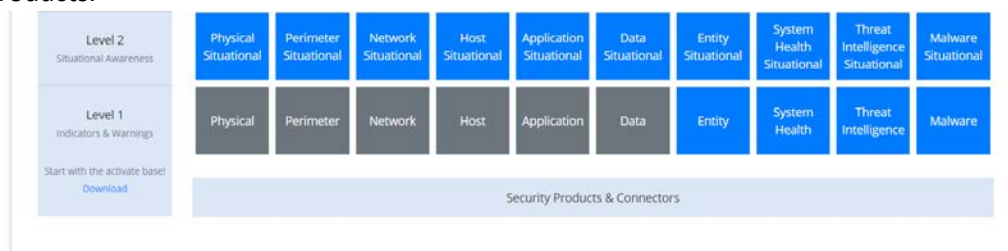


34. Click **Done**.
35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.

2.8.5 Install Pre-Configured Filters for ArcSight

2.8.5.1 *Install Activate Base*

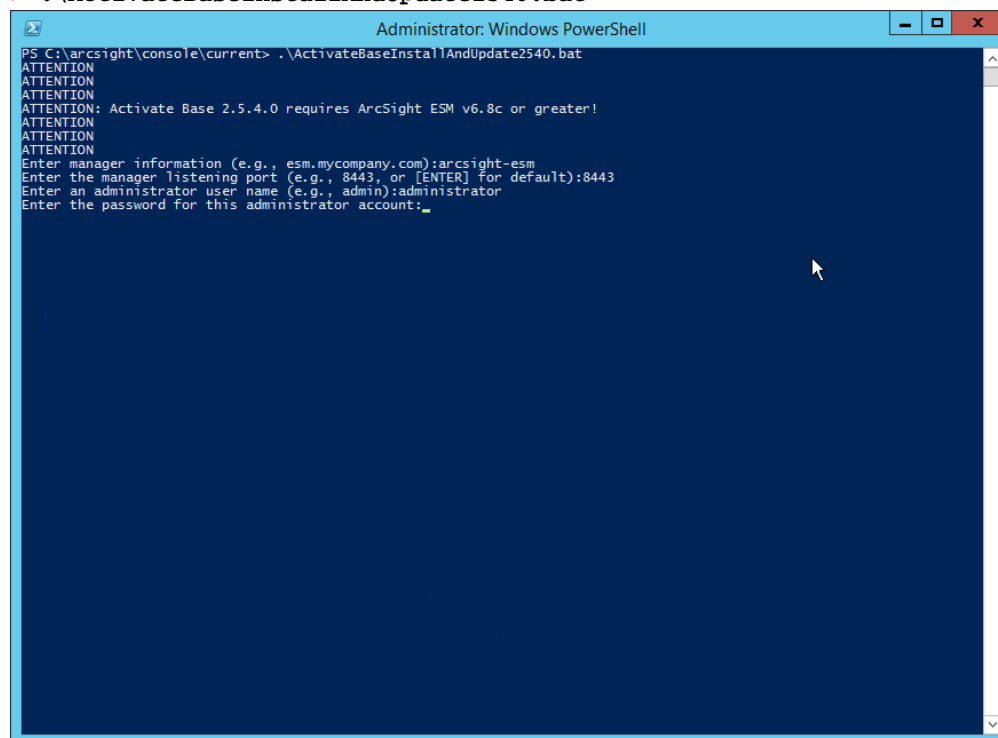
1. Go to the ArcSight Content Brain web app (<https://arcsightcontentbrain.com/app/>) and log in. This page allows you to keep track of packages to be installed—which packages should be installed is dependent on the needs of the organization, but the “activate base” is required for all products.



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:

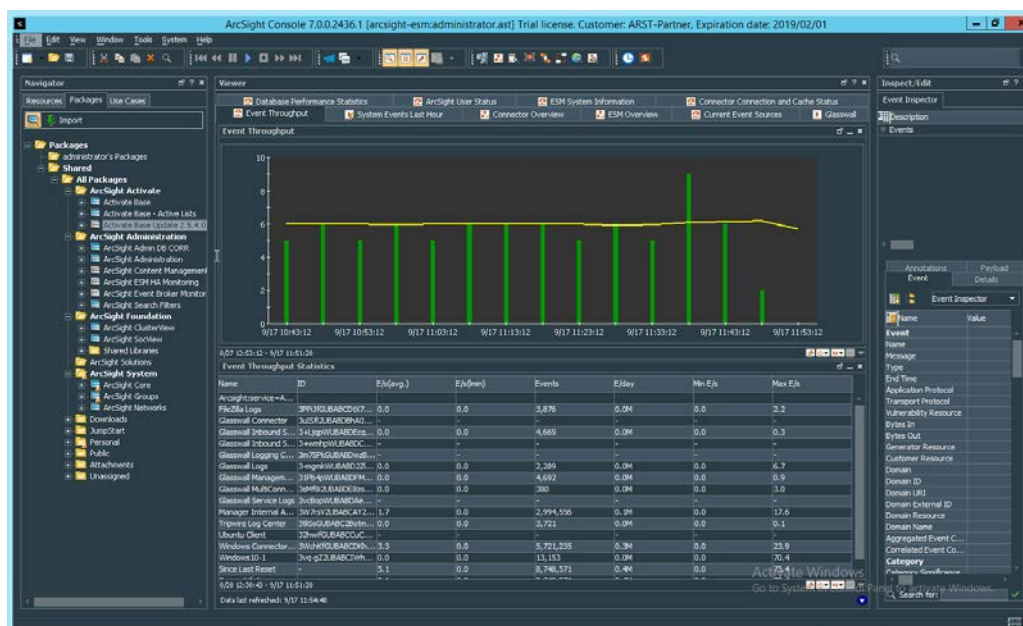
```
> .\ActivateBaseInstallAndUpdate2540.bat
```



```

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

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

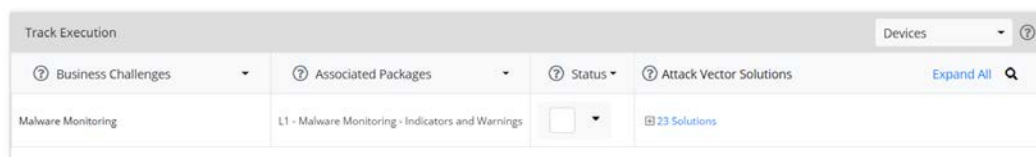


- Under **Packages > Shared > All Packages > ArcSight Activate**, right-click **Activate Base Update 2.5.4.0**, and select **Delete Package**.

2.8.5.2 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.

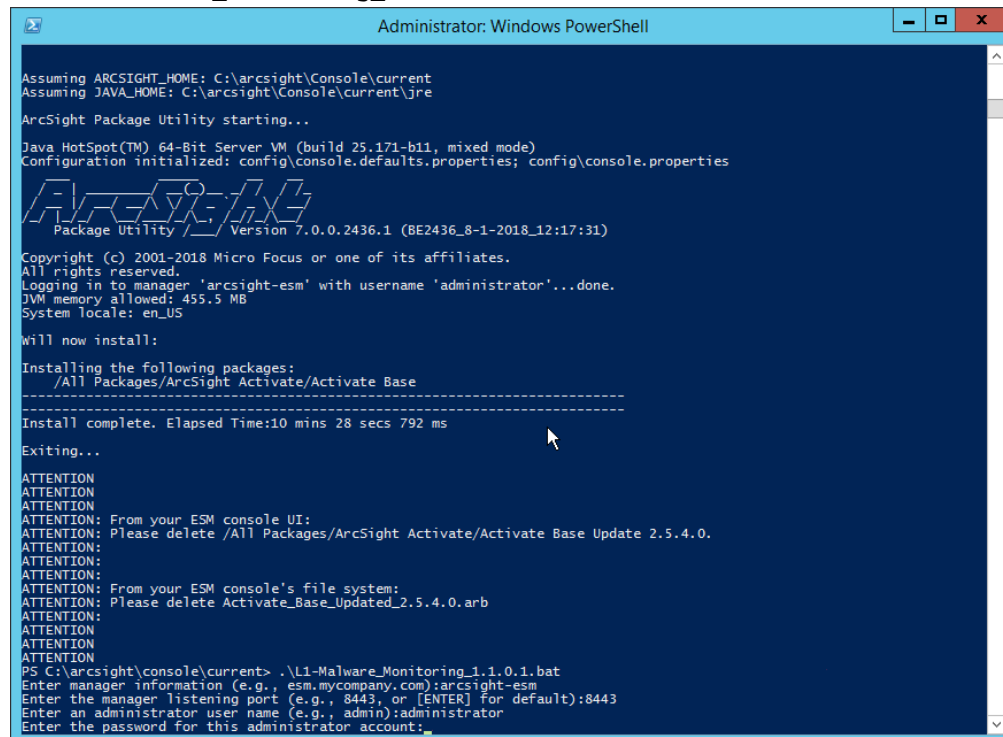
- Navigate to the **ArcSight Content Brain** web app.
- Select the **Level 1** box labeled **Malware**.



- In the **Track Execution** section, under **Associated Packages**, you can see the list of packages used to address the challenge of “Malware Monitoring.” In this case, there is just one package, “L1 – Malware Monitoring – Indicators and Warnings.” Click the link to be taken to a download page for the package, and download it. (Note: This package should be installed on the Arcsight Console, not on the ESM.)

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

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



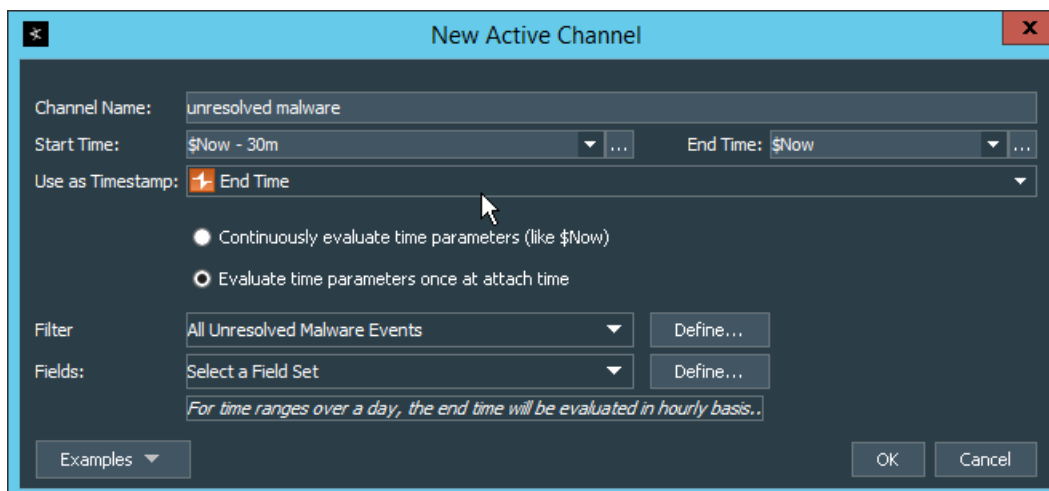
```
Administrator: Windows PowerShell

Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
ArcSight Package Utility starting...
Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)
Configuration initialized: config\console.defaults.properties; config\console.properties
ArcSight Package Utility Version 7.0.0.2436.1 (8E2436_8-1-2018_12:17:31)
Copyright (c) 2001-2018 Micro Focus or one of its affiliates.
All rights reserved.
Logging in to manager 'arcsight-esm' with username 'administrator'...done.
JVM memory allowed: 455.5 MB
System locale: en_US
will now install:
Installing the following packages:
/All Packages/ArcSight Activate/Activate Base
-----
Install complete. Elapsed Time:10 mins 28 secs 792 ms
Exiting...
ATTENTION
ATTENTION
ATTENTION
ATTENTION: From your ESM console UI:
ATTENTION: Please delete /All Packages/ArcSight Activate/Activate Base Update 2.5.4.0.
ATTENTION:
ATTENTION:
ATTENTION: From your ESM console's file system:
ATTENTION: Please delete Activate_Base_Updated_2.5.4.0.arb
ATTENTION:
ATTENTION:
ATTENTION:
PS C:\arcsight\console\current> .\L1-Malware_Monitoring_1.1.0.1.bat
Enter manager information (e.g., esm.mycompany.com):arcsight-esm
Enter the manager listening port (e.g., 8443, or [ENTER] for default):8443
Enter an administrator user name (e.g., admin):administrator
Enter the password for this administrator account:
```

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

2.8.6 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.

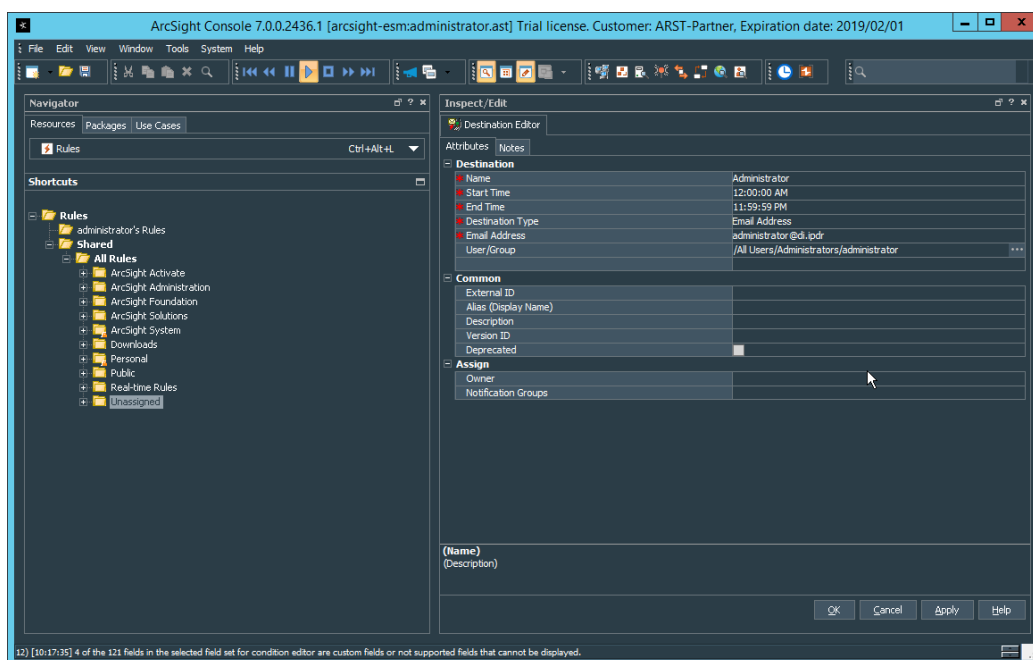


5. Click **OK**. All events that match the filter can be displayed in the newly created channel. Filters from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate > Solutions**.

2.8.7 Configure Email Alerts in ArcSight

2.8.7.1 Configure a New Destination

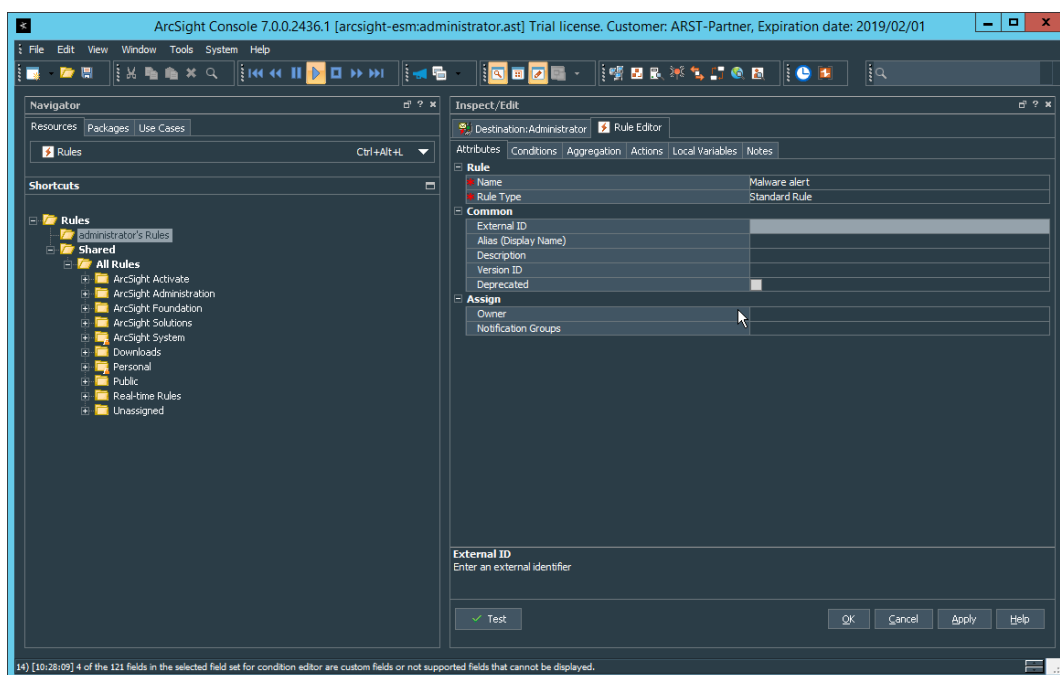
1. In **ArcSight Console**, click **File > New > Destination**.
2. Enter a name for the **Destination**.
3. For **Destination Type**, select **Email Address**.
4. For **Email Address**, enter the email that should be associated with this destination.



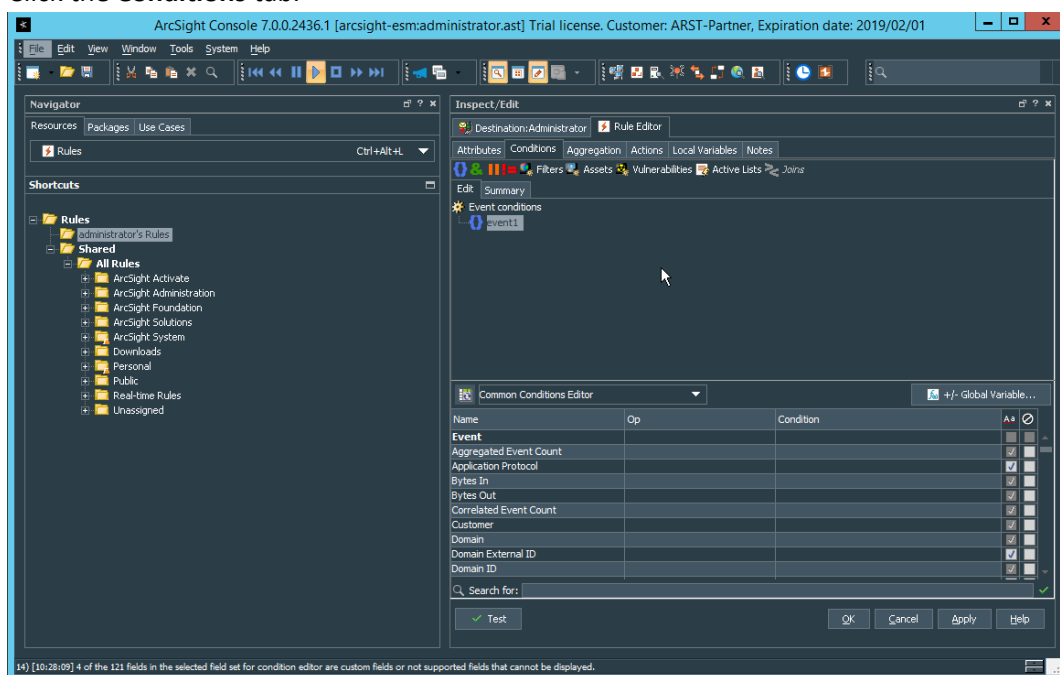
5. Click **OK**.
6. Select a place to save the new **Destination**.
7. Click **OK**.

2.8.7.2 *Configure a New Rule*

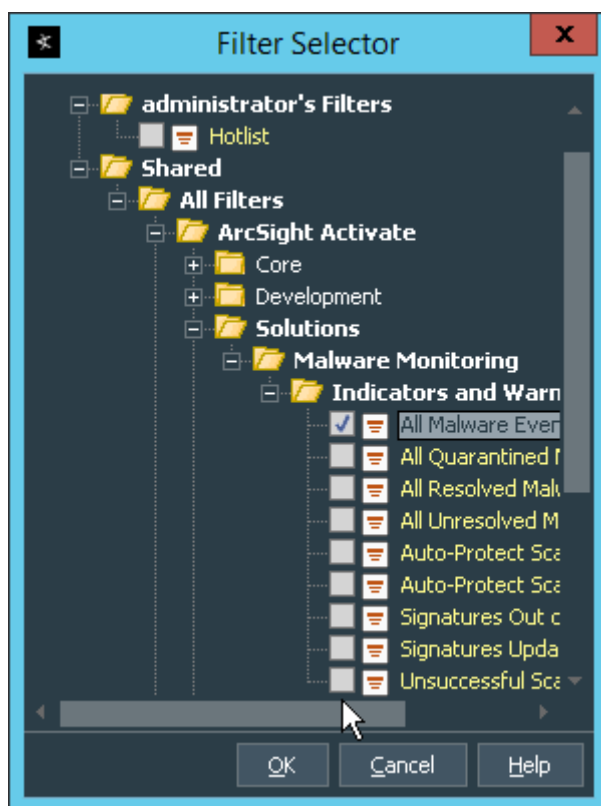
1. Click **File > New > Rule > Standard Rule**.
2. Enter a name for the rule.



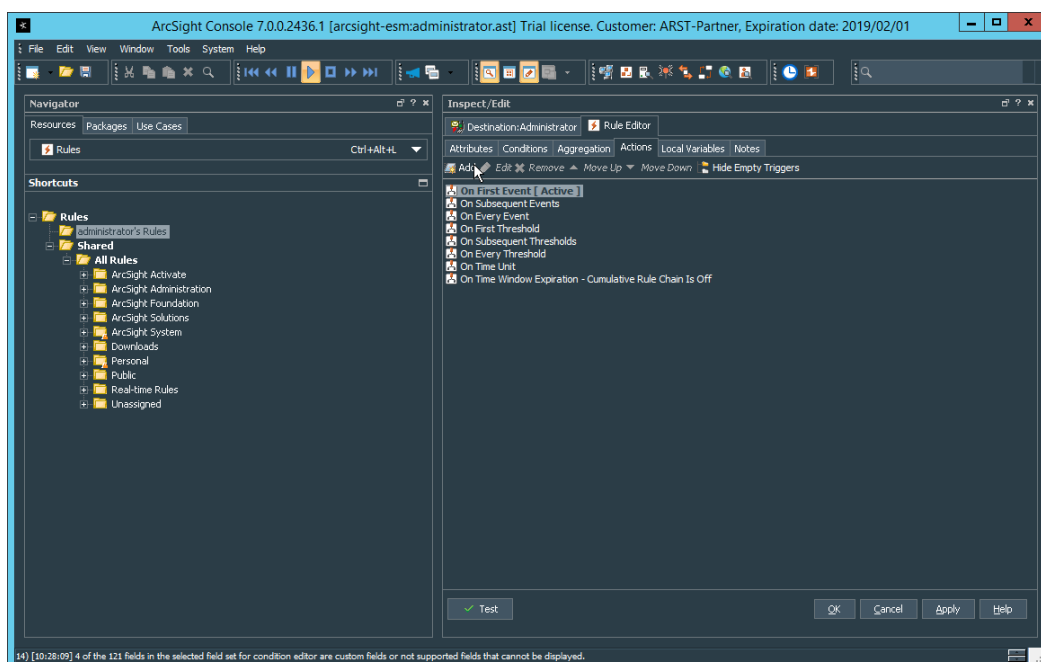
3. Click the **Conditions** tab.



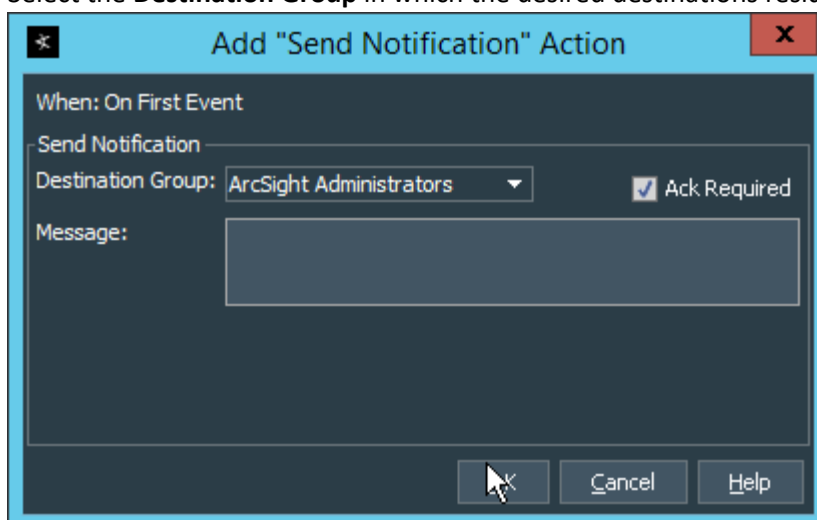
4. Either create a custom condition for the rule or click the **Filters** button to select a pre-configured Filter. (Ensure you check the box next to desired filters if you choose to select a pre-configured filter.)



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**.

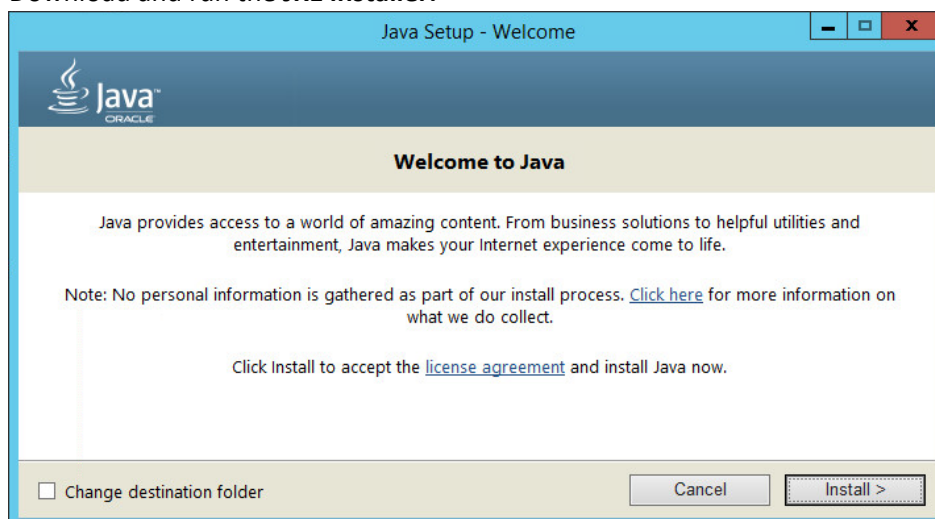
2.9 Tripwire Enterprise

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

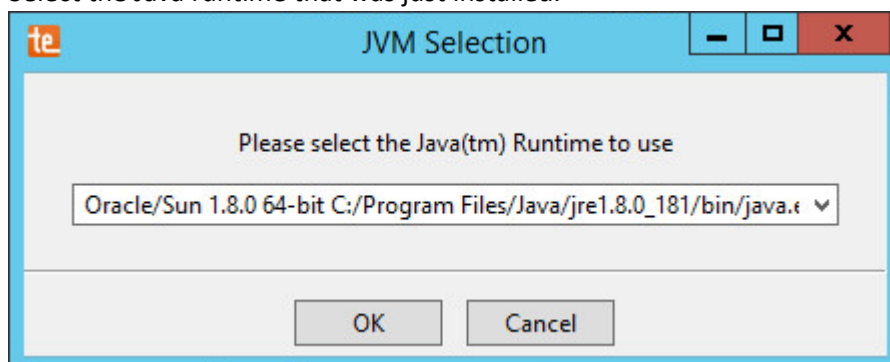
1. Ensure that you have a current version of Oracle Java. You must install both the Java Runtime Environment (JRE) and the Java Cryptography Extension (JCE).
2. Download and run the **JRE installer**.



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

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

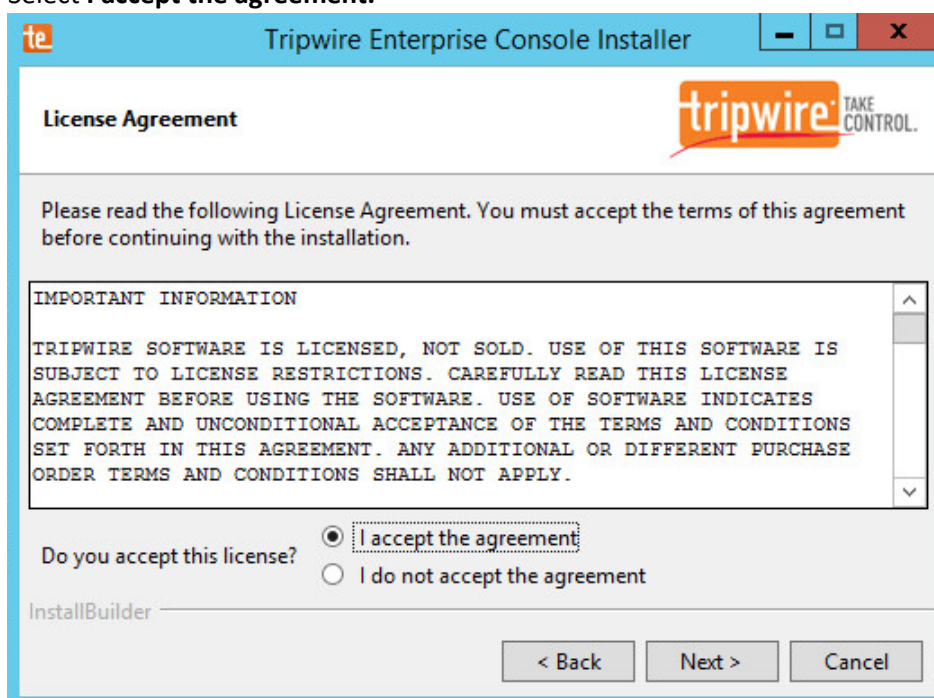
5. Copy the **local_policy.jar** and **US_export_policy.jar** files to **/lib/security/Unlimited/** and **/lib/security/Limited** in the Java installation directory.
6. Run **install-server-windows-amd64**.
7. Select the Java runtime that was just installed.



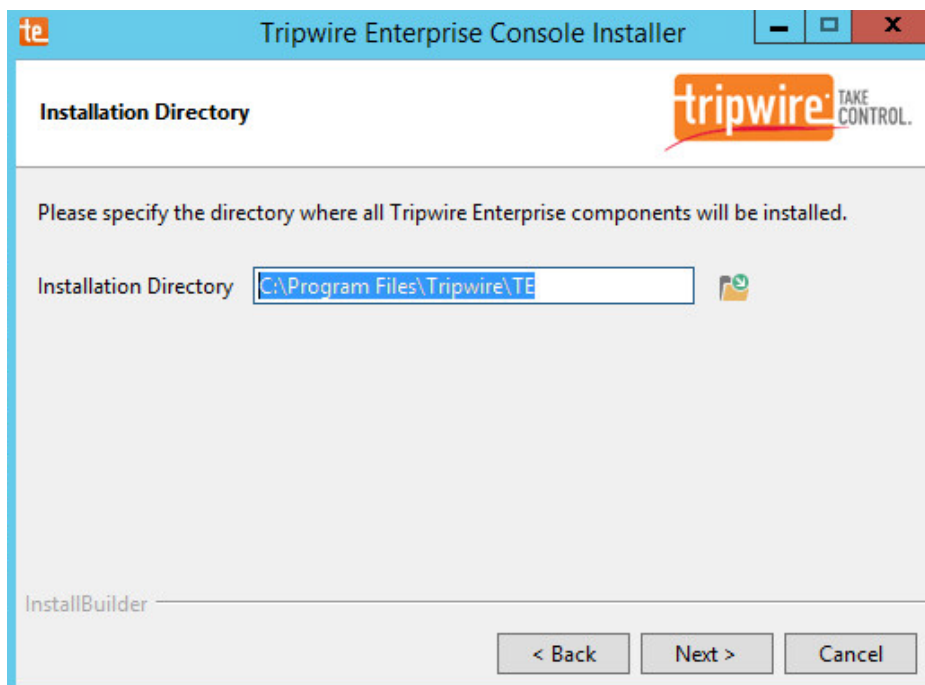
8. Click **OK**.



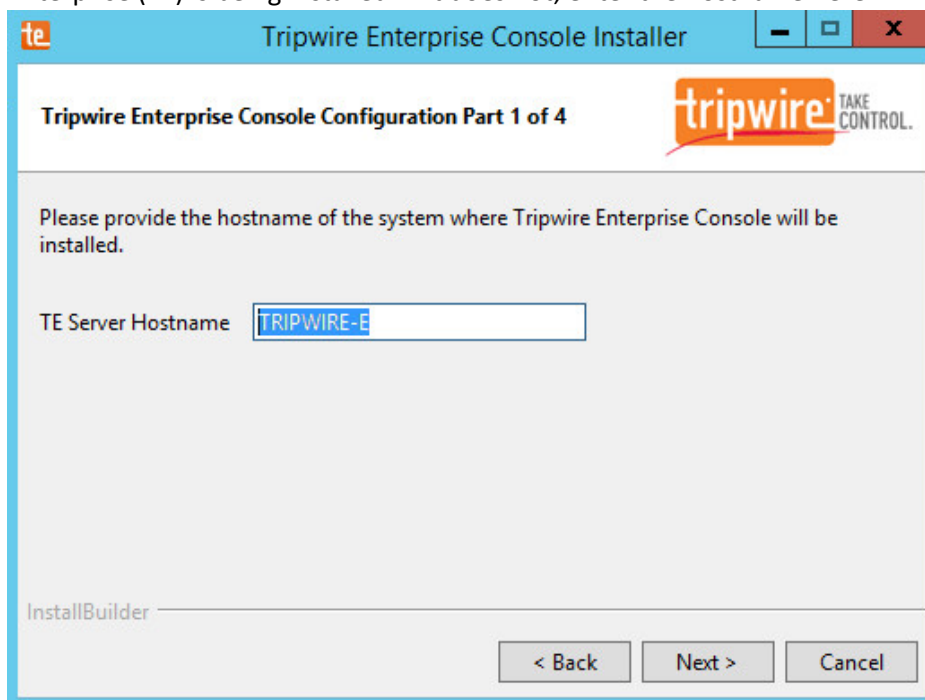
9. Click **Next**.
10. Select **I accept the agreement**.



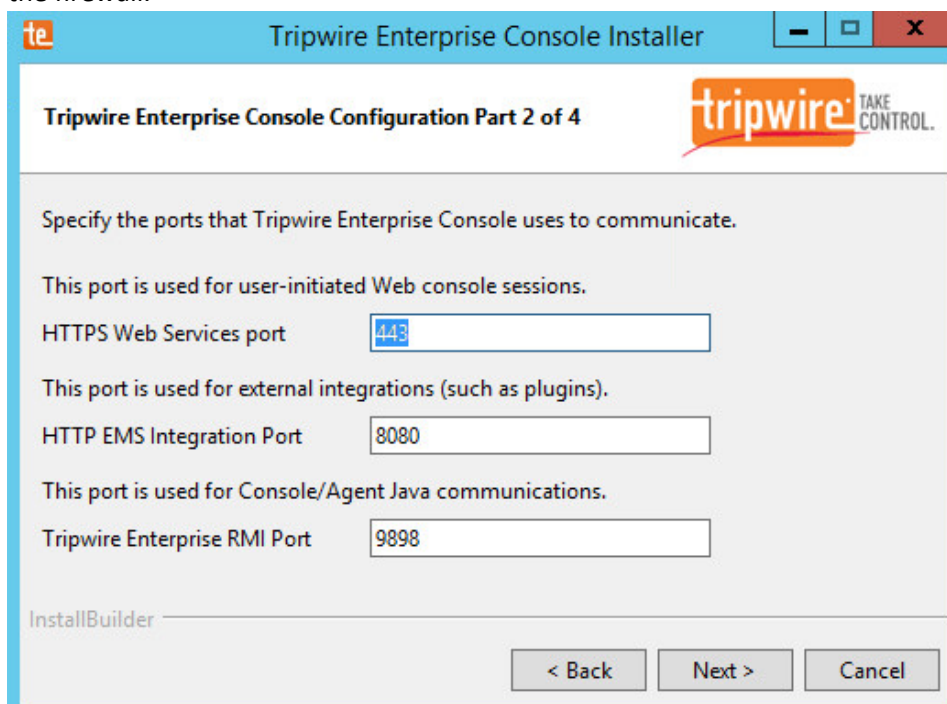
11. Click **Next**.



12. Click **Next**.
13. The installer should automatically detect the hostname of the system on which Tripwire Enterprise (TE) 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 Remote Method Invocation (RMI) port is used for inbound communication from Tripwire agents to the server, so ensure that it is allowed through the firewall.



The screenshot shows a window titled "Tripwire Enterprise Console Installer". Inside, the header says "Tripwire Enterprise Console Configuration Part 2 of 4" with the Tripwire logo and the tagline "TAKE CONTROL.". The main text says "Specify the ports that Tripwire Enterprise Console uses to communicate." Below this, there are three sections:

- "This port is used for user-initiated Web console sessions." followed by "HTTPS Web Services port" and a text box containing "443".
- "This port is used for external integrations (such as plugins)." followed by "HTTP EMS Integration Port" and a text box containing "8080".
- "This port is used for Console/Agent Java communications." followed by "Tripwire Enterprise RMI Port" and a text box containing "9898".

At the bottom left, it says "InstallBuilder". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

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

Tripwire Enterprise Console Configuration Part 3 of 4

The services passphrase is used to secure Tripwire Enterprise communications.

This password must be between 19 and 64 characters, and cannot contain single-quote ('), double-quote ("), less-than (<), greater-than (>), or backslash (\) characters, most other characters are allowed. See the Installation and Maintenance Guide for more details.

Services Passphrase

Confirm Passphrase

InstallBuilder

< Back Next > Cancel

18. Click **Next**.

Tripwire Enterprise Console Configuration Part 4 of 4

Please review the installation settings for Tripwire Enterprise Console.

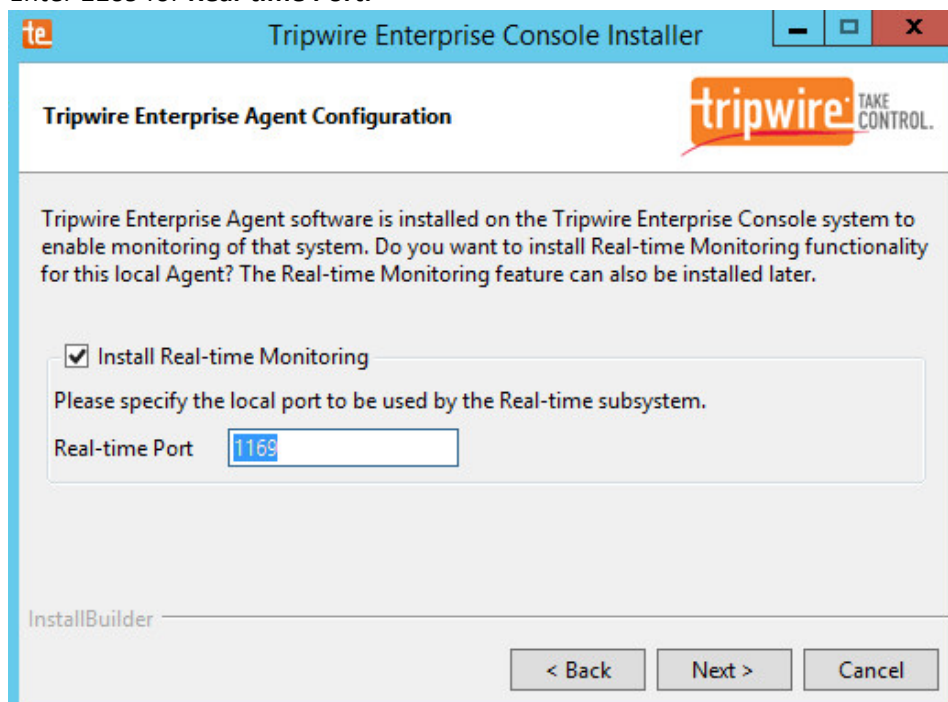
The following settings are configured for Tripwire Enterprise Console:

Installation Directory: C:\Program Files\Tripwire\TE
 Available Disk Space: 184716 MB
 Hostname: TRIPWIRE-E
 IP Address(Listening): 0.0.0.0
 HTTPS Web Services Port: 443
 HTTP EMS Integration Port: 8080
 TE Services (RMI) Port: 9898
 TEConsoleInstaller: Java Version detected: 1.8.0_181 64

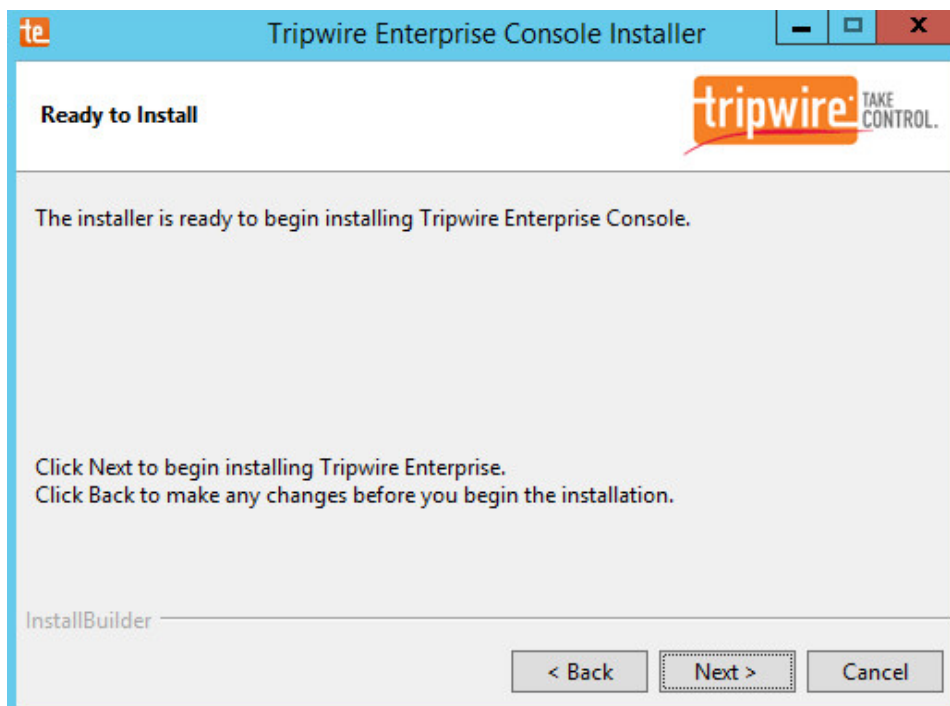
InstallBuilder

< Back Next > Cancel

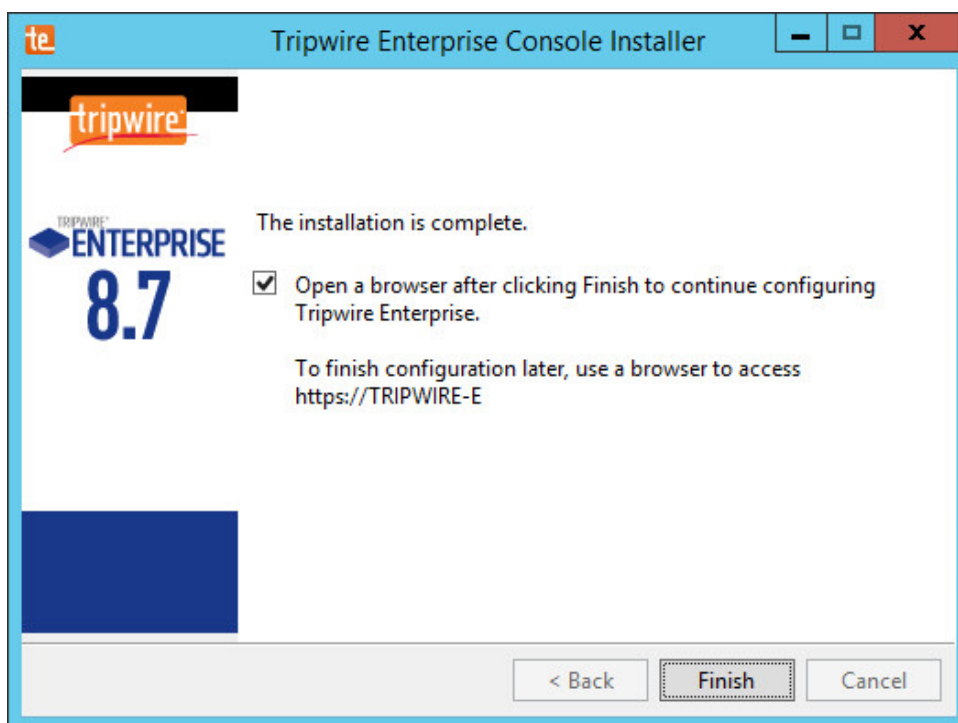
19. Click **Next**.
20. Check the box next to **Install Real-time Monitoring**.
21. Enter **1169** for **Real-time Port**.



22. Click **Next**.

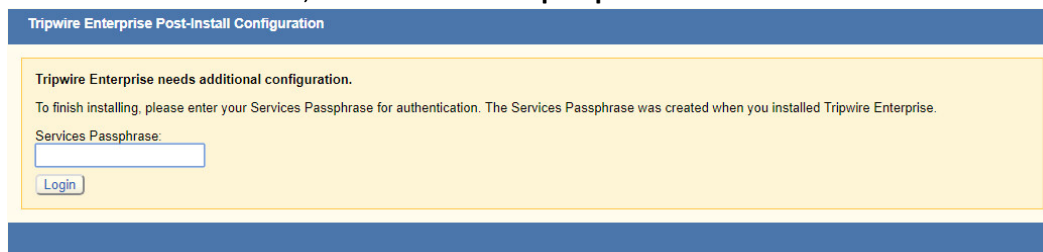


23. Click **Next**.
24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise**.

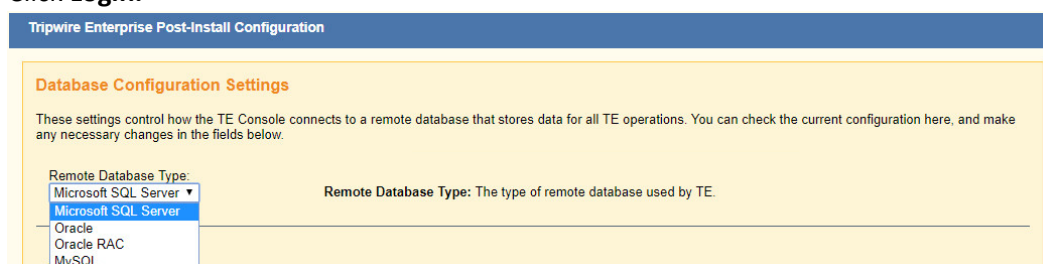


25. Click **Finish**.

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 TE.
34. Select the appropriate setting for **SSL** according to your organization's needs.

Authentication Type:

Authentication Type: Specifies whether the database login should authenticate using a Windows account (typically of the format domain\user), or an SQL Server account (an account defined only in SQL Server). With the Windows authentication type, NTLMv2 should be used, as it is cryptographically superior to the first version of NTLM. However, as NTLMv2 is configured in the operating system, not in the database or application, TE can be used with NTLM to ensure compatibility.

Login Name:

Login Name: The login name that TE will use to authenticate with the database.

Password:

Password: The password that TE will use to authenticate with the database.

Database Host:

Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.

Port (default 1433):

Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.

Database Name:

Database Name: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.

Instance Name (Optional):

Instance Name (Optional): The location/name of the database instance on the server. Ask your DBA if a non-default instance should be used for TE.

SSL:

SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.

- Request - SSL will be used if available.
- Require - SSL will always be used, and an error will occur if SSL is not available for the database.
- Authenticate - SSL will always be used, and an error will occur if SSL is not available for the database. In addition, the certificate chain of the database server's public key will be authenticated using TE's trust store. If the certificate chain does not originate from a trusted source, an error will occur.
- Off - SSL will never be used. This setting is not recommended.

[Test Database Login](#) ✓

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

[Test Database Login](#) ✓

Test Results:

[Save Configuration and Restart Console](#) [Logout](#)

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

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

Tripwire Enterprise Post-Install Configuration

Configuration Steps Needed:

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

Create Administrator Password

Passwords must:

- Be between 8 and 128 characters in length
- Contain at least 1 numeric character
- Contain at least 1 uppercase character
- Contain at least 1 non-alphanumeric character

Supported characters: ~!@#\$%^&*()-_+=+{}|\\;:~'"<>./?

Password:

Confirm Password:

Confirm and Continue

Support Information

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

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

Generate Support Bundle

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

Logout

38. Click **Confirm and Continue**.

Tripwire Enterprise Fast Track

Welcome to Tripwire Enterprise Fast Track!



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

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

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

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

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

Configure Tripwire Enterprise

Cancel

39. Click **Configure Tripwire Enterprise**.

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

Choose File No file chosen

40. Click **Choose File**, and select the TE license file, which should be a .cert file.

41. Check the box next to **Change Auditing and Policy Management**.

Step 2: Configure Change Auditing and/or Policy Management

Monitoring Solutions ☒ Change Auditing
☒ Policy Management

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

42. Select any available policies desired.

Step 3: Specify the platforms to monitor

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

Operating System
<input checked="" type="checkbox"/> Microsoft Windows Server 2008 R2
<input checked="" type="checkbox"/> Microsoft Windows Server 2012 R2
<input checked="" type="checkbox"/> Oracle Solaris 10
<input checked="" type="checkbox"/> Oracle Solaris 11
<input checked="" type="checkbox"/> Red Hat Enterprise Linux 6
<input checked="" type="checkbox"/> Red Hat Enterprise Linux 7
Virtual Infrastructure
<input checked="" type="checkbox"/> VMware ESXi 5.5 Server

Selected Platforms:

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

43. Select all the operating systems that you wish to monitor with TE.

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

Change Audit Scheduling

Checks

How frequently would you like to run checks on your assets?

Daily

Run the checks at 1:00 AM

Reports

How frequently would you like to run reports on your assets?

Daily

Run the reports at 4:00 AM

Policy Scheduling

Checks

How frequently would you like to run checks on your assets?

Weekly on Sundays

Run the checks at 1:00 AM

Reports

How frequently would you like to run reports on your assets?

Weekly on Sundays

Run the reports at 4:00 AM

☐ Enable Checks and Reports (Optional)

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

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

Step 5: Configure an email server for sending reports and alerts

☐ Set up the email server now
☒ Set up the email server at another time

Before Tripwire Enterprise can deliver alerts or reports, an email server must be created. You can set up the server now, or you can wait and do it later using the Tripwire Enterprise Console.

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

Step 6: Create an administrator account for Tripwire Enterprise Console access

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

User Name:
 ✓

Password:
 ✓

Confirm Password:
 ✓

Email Address:

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

47. Click **Preview Configuration**.

Policy Rules - VMware ESX/ESX Server

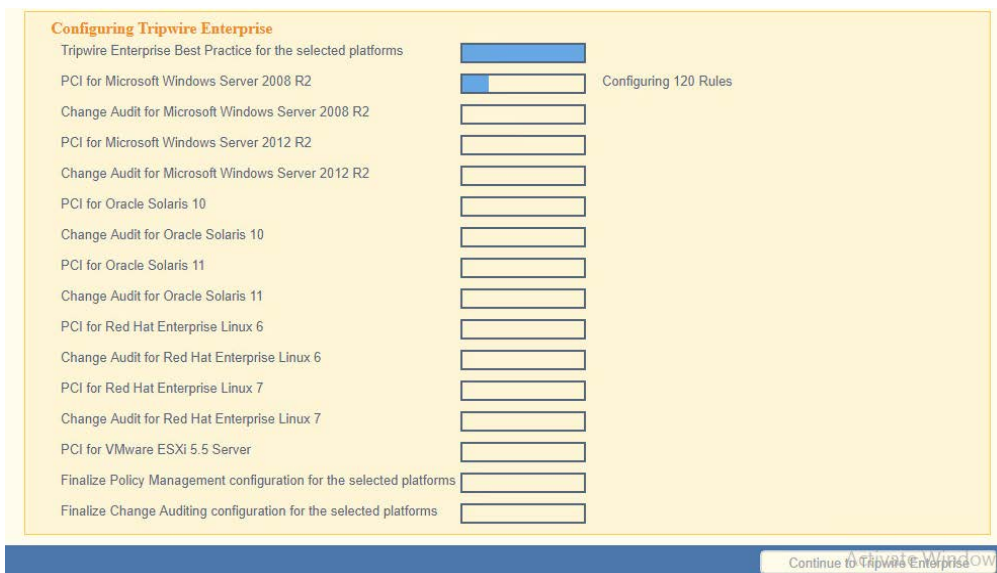
These tasks will be applied to your configuration

- Critical Change Audit Check - RHEL 6
- Critical Change Audit Check - RHEL 7
- Critical Change Audit Check - Solaris 10
- Critical Change Audit Check - Solaris 11
- Critical Change Audit Check - Windows
- Policy Check - RHEL 6
- Policy Check - RHEL 7
- Policy Check - Solaris 10
- Policy Check - Solaris 11
- Policy Check - VMware ESX
- Policy Check - Windows
- Report Task - Daily File System Changes by Node
- Report Task - Daily File System Changes by Rule
- Report Task - Test Result Summary - Red Hat - PCI v3.1
- Report Task - Test Result Summary - Solaris - PCI v3.1
- Report Task - Test Result Summary - VMware ESX - PCI v3.1
- Report Task - Test Result Summary - Windows - PCI v3.1
- Report Task - Test Results by Node - Red Hat - PCI v3.1
- Report Task - Test Results by Node - Solaris - PCI v3.1
- Report Task - Test Results by Node - VMware ESX - PCI v3.1
- Report Task - Test Results by Node - Windows - PCI v3.1
- Report Task - Top 5 Nodes with Daily Changes
- Report Task - Waivers - Red Hat - PCI v3.1
- Report Task - Waivers - Solaris - PCI v3.1
- Report Task - Waivers - VMware ESX - PCI v3.1
- Report Task - Waivers - Windows - PCI v3.1

These home pages will be applied to your configuration

- Change Audit
- Customer Center Home Page
- PCI Overview - Red Hat
- PCI Overview - Solaris
- PCI Overview - VMware ESX
- PCI Overview - Windows
- Tripwire Enterprise Administrator

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
```

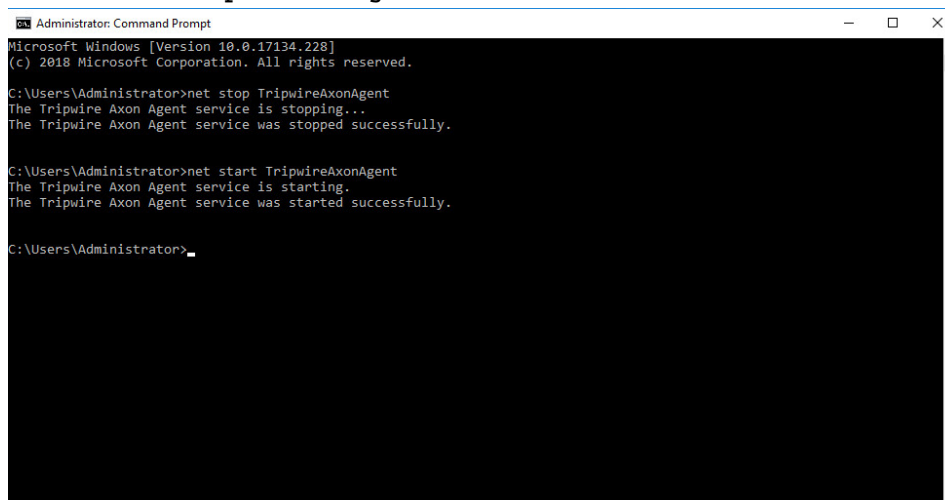
2.9.3 Install the Axon Agent (Windows)

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
```



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

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

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

C:\Users\Administrator>
```

2.9.4 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:
Red Hat Enterprise Linux (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.

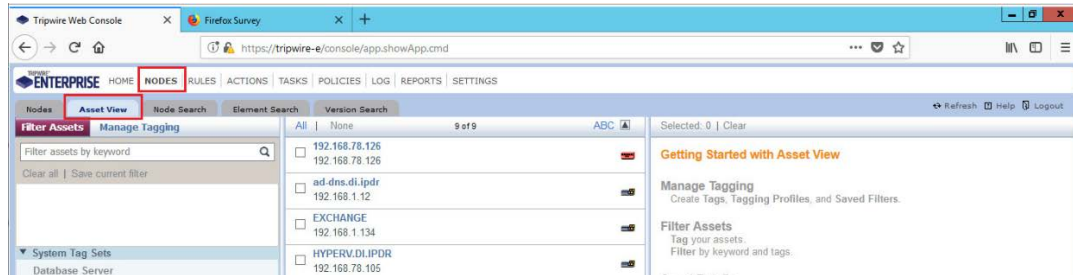
Baseline: The act of creating an element that reflects the current state of a monitored object (also called the **current baseline**. When a node's baseline is promoted, TE saves the former baseline as a **historic baseline**.

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.

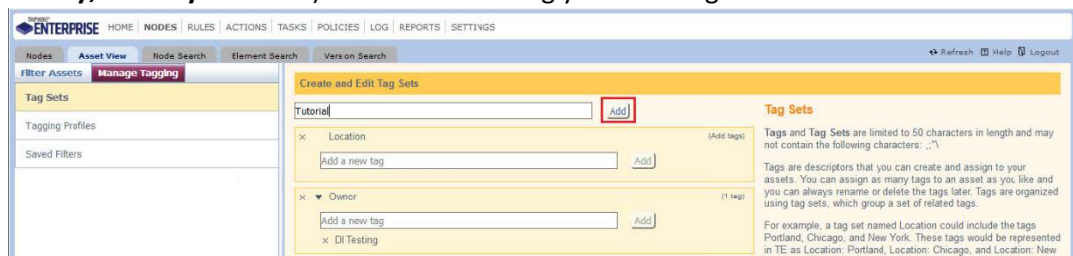
2.9.5.2 Tags

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.

Create and Edit Tag Sets

add a new tag set

× Location (Add tags)

Add a new tag Add

× ▼ Owner (1 tag)

Add a new tag Add

× DI Testing

× ▼ Platform Family (4 tags)

Add a new tag Add

× Red Hat

× Solaris

× VMware ESX

× Windows

× ▼ Primary Function (1 tag)

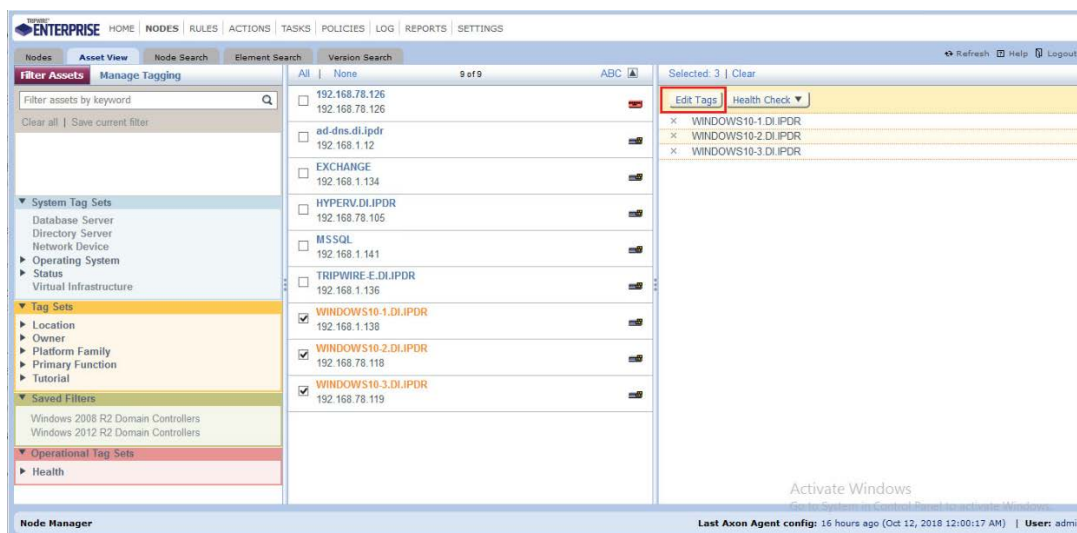
Add a new tag Add

× Domain Controller

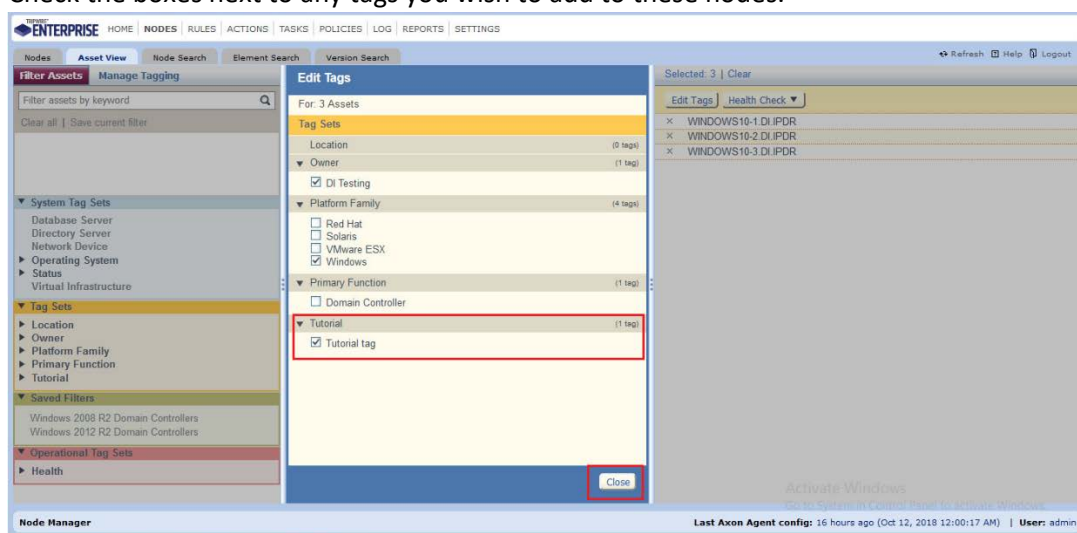
× Tutorial (Add tags)

Tutorial tag Add

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**.

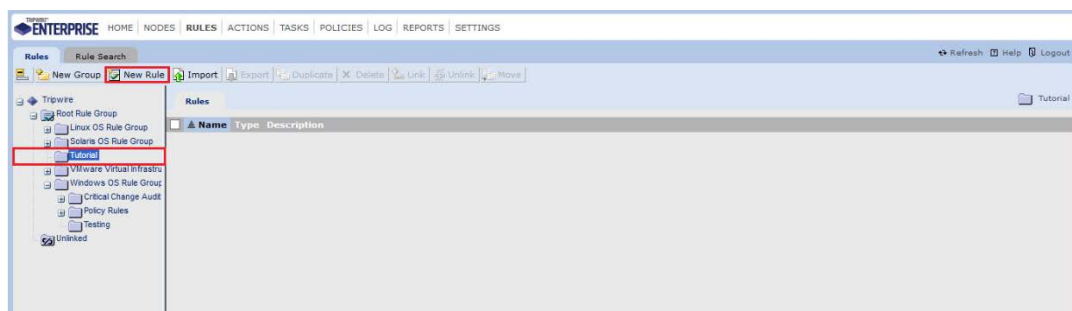
2.9.5.3 Rules

This section will describe how to create a rule.

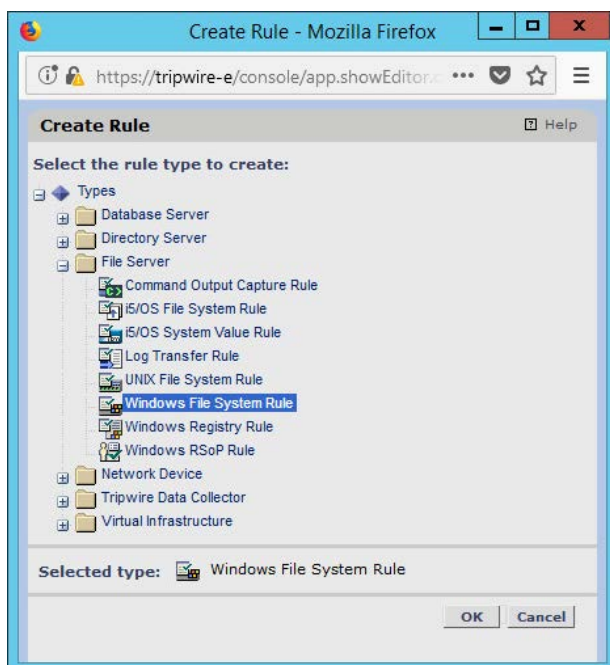
1. Click **Rules**.



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.

New Windows File System Rule Wizard - Mozilla Firefox

https://tripwire-e/console/app.showWizard.cmd?wizardName=si.web.specifierRuleV

New Windows File System Rule Wizard

Enter a name and description for the rule.

Name: tutorial rule

Description: a rule specifically for tutorial documentation

☒ Enable Tracking Identifier

< Back Next > Finish Cancel

7. Click **Next**.

New Windows File System Rule Wizard - Mozilla Firefox

https://tripwire-e/console/app.showWizard.cmd?wizardName=si.web.specifierRuleV

New Windows File System Rule Wizard

New Start Point New Stop Point Browse Delete

Path	Type	Default Severity	Criteria Set	Recurse Level	Archive Content

< Back Next > Finish Cancel

8. Click **New Start Point**.

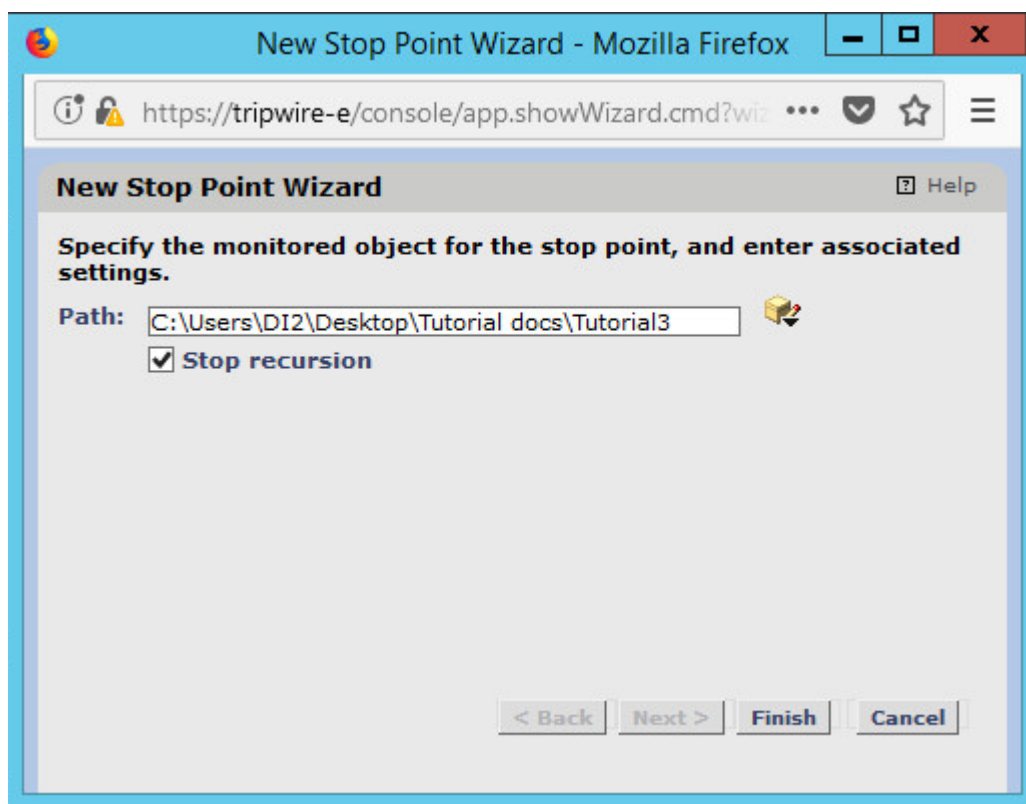
9. For **Path**, enter a directory that represents the scope of the scan. It can be limited to the documents folder or be wide enough to encompass all the files on a system. Note that the latter will take much longer to scan.

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**.

Name	Description
<input checked="" type="radio"/> Windows - Content and Permissions	
<input type="radio"/> Windows - Content Only	
<input type="radio"/> Windows - Permissions Only	

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.

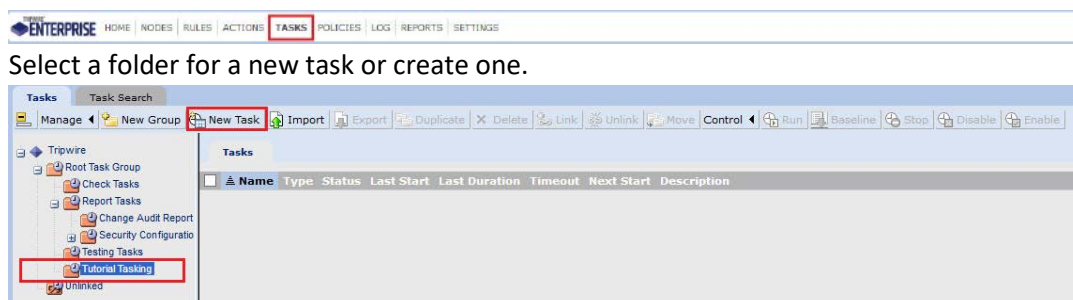


16. Click **Finish**.
17. Click **Next**.
18. Click **Next**.
19. Click **Finish**.

2.9.5.4 Tasks

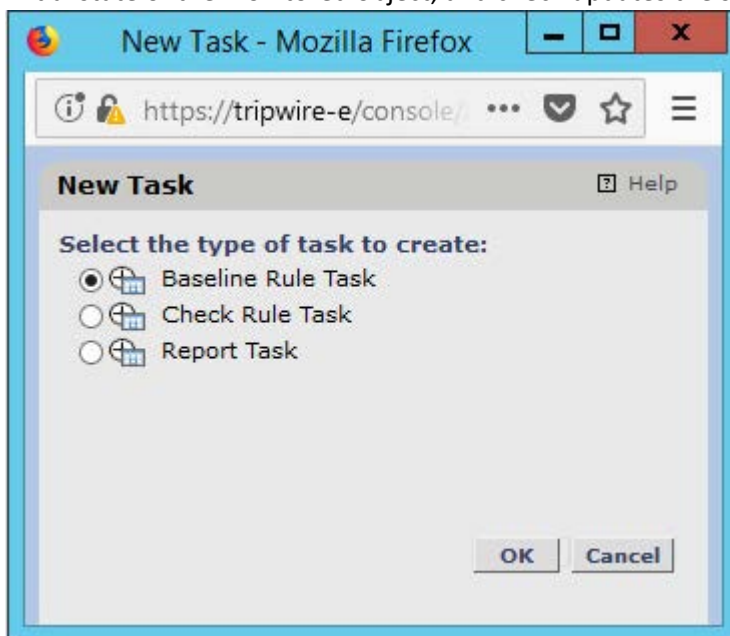
This section will describe how to create a task.

1. Click **Tasks**.
2. Select a folder for a new task or create one.

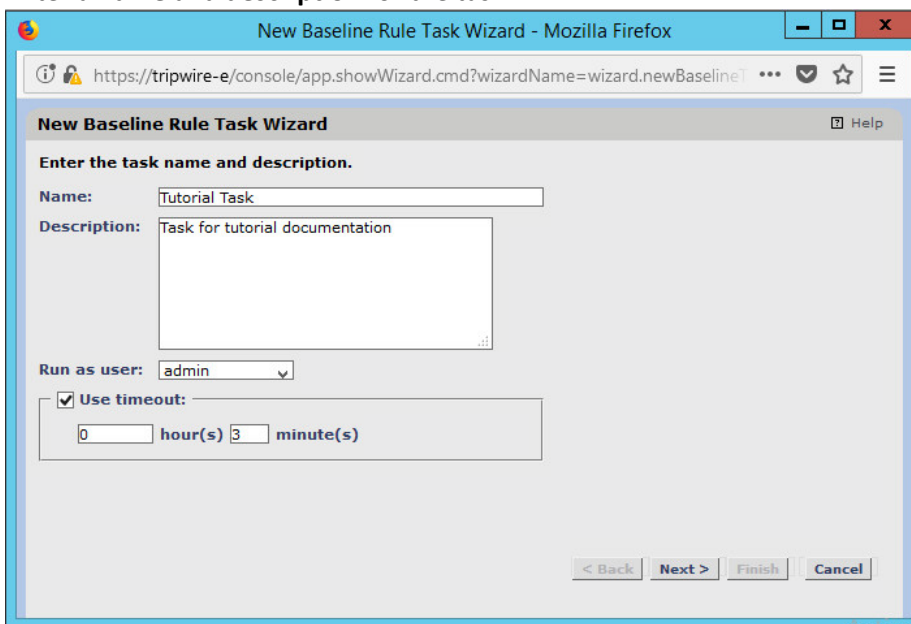


3. Click **New Task**.

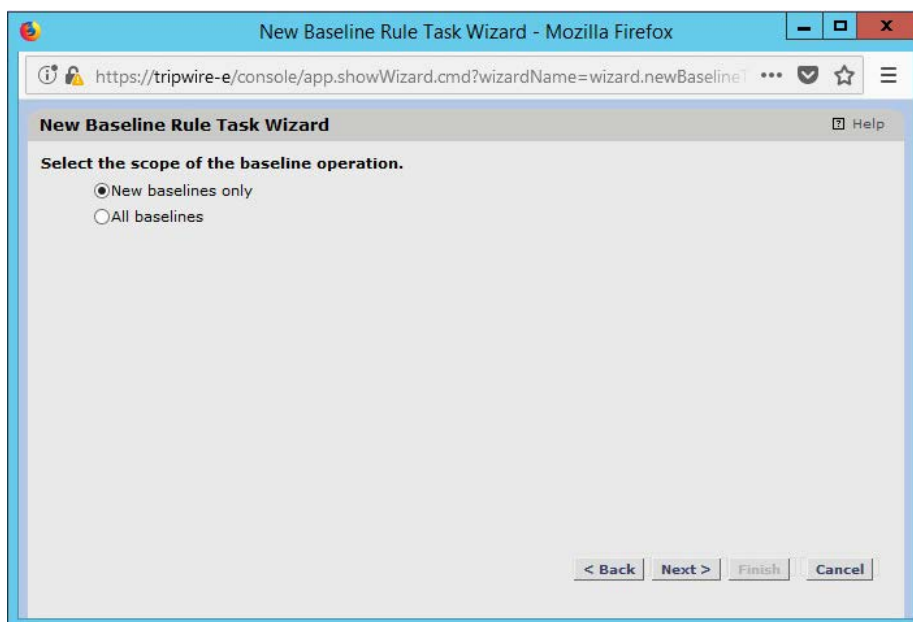
4. Select **Baseline Rule Task** or **Check Rule Task** (Note: Both are needed: baseline creates the initial state of the monitored object, and check updates the state and reports any changes).



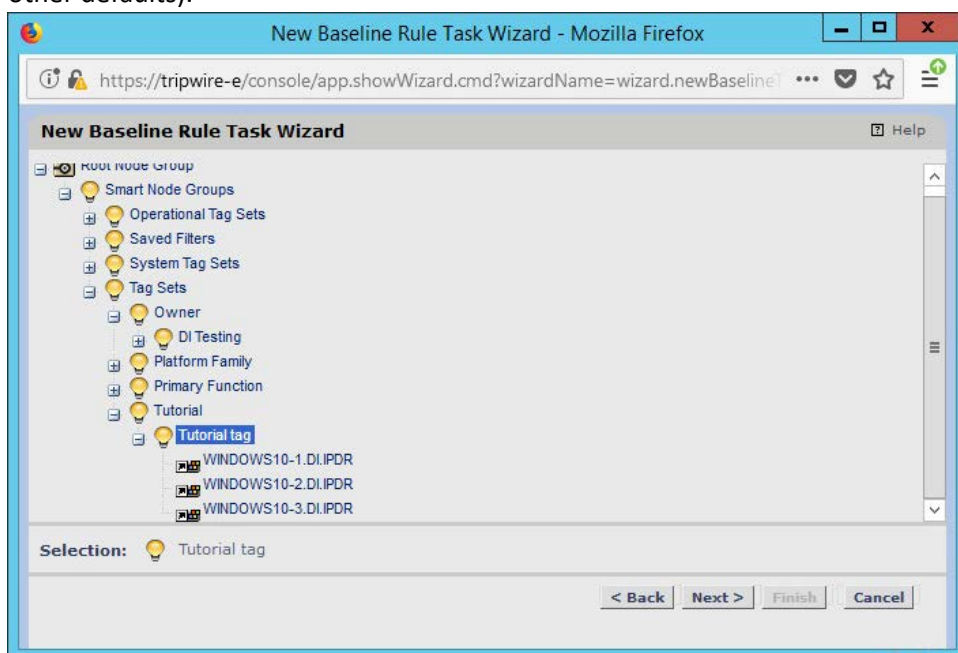
5. Click **OK**.
6. Enter a **name** and **description** for the task.



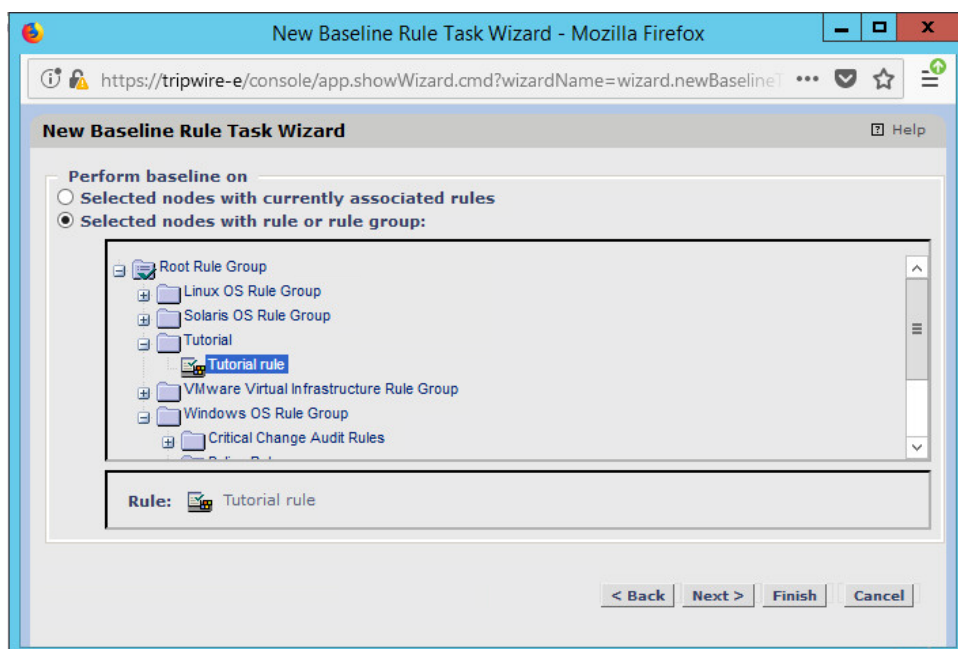
7. Click **Next**.
8. Select whether you want all baselines to be updated or to only create new baselines.



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).

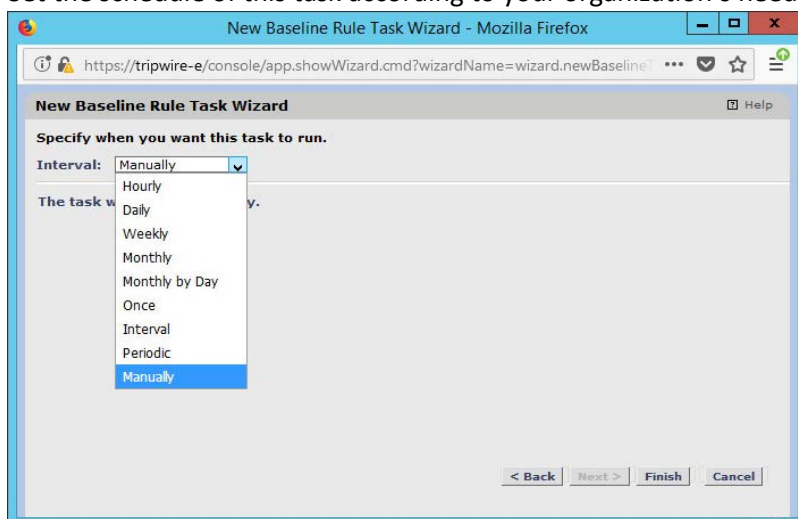


11. Click **Next**.
12. Select the rule created earlier.



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

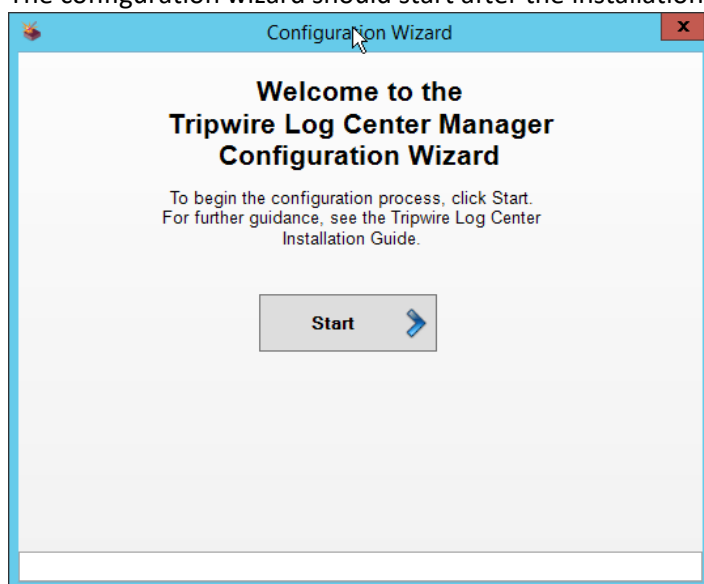
See the *Tripwire Log Center 7.3.1 Installation Guide* that should accompany the installation media for instructions on how to install **Tripwire Log Center**. Use the **Tripwire Log Center Manager** installer.

Notes:

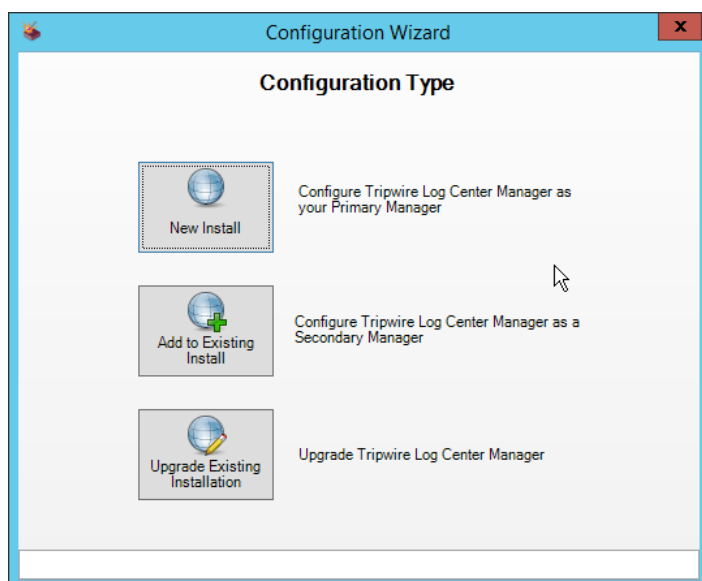
- a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise**.
- b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
- c. .NET Framework 3.5 is required for this 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

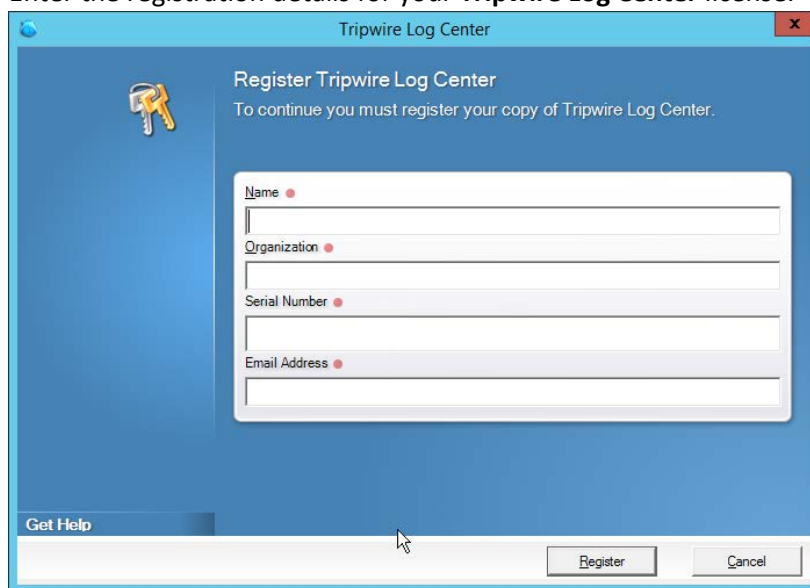
1. The configuration wizard should start after the installation is complete.



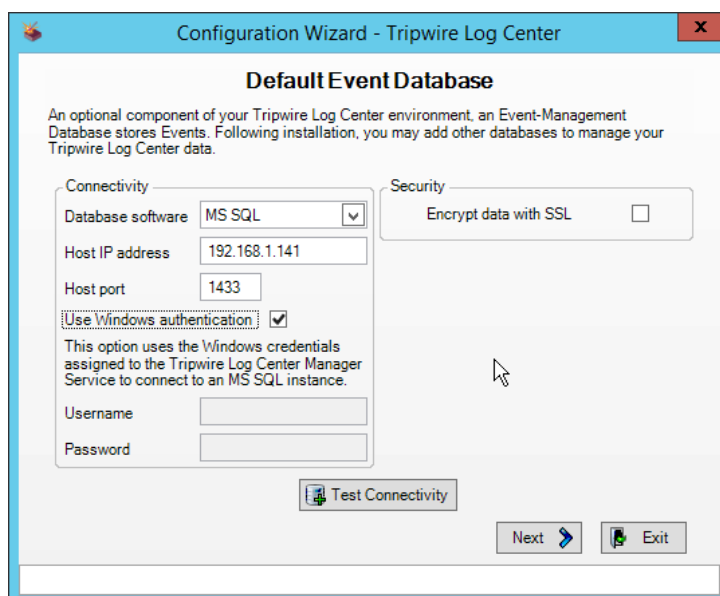
2. Click **Start**.



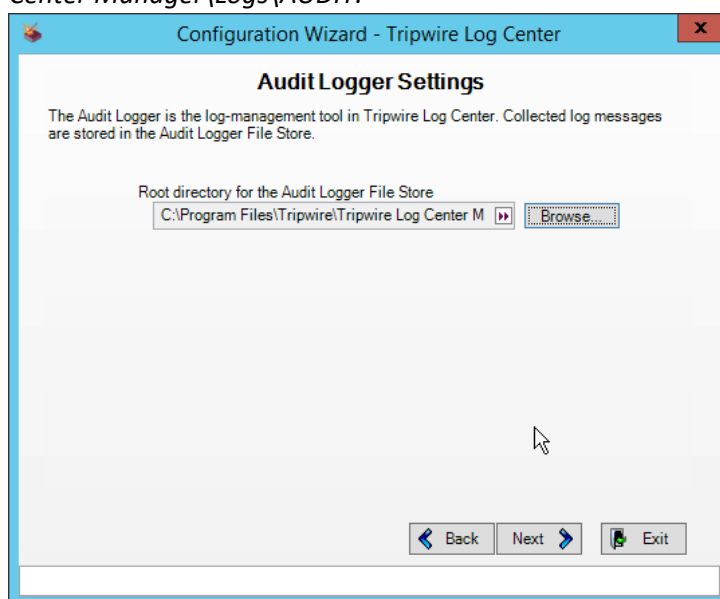
3. Click **New Install**.
4. Enter the registration details for your **Tripwire Log Center** license.



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*.

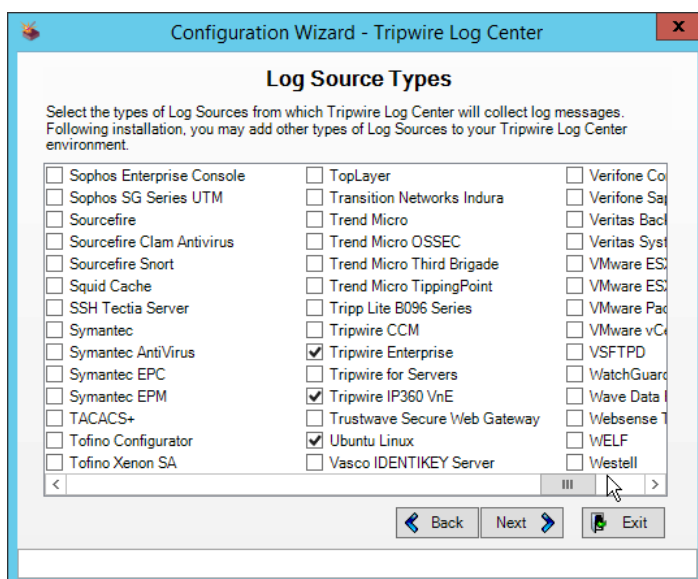


9. Click **Next**.
10. Enter a **password** and an **email**.
11. Change the IP to a hostname, if preferred.

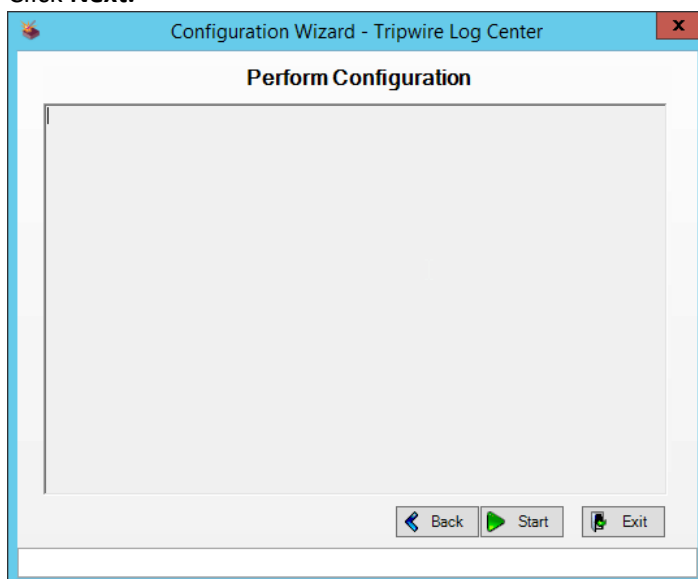
12. Click **Next**.

13. Click **Next**.

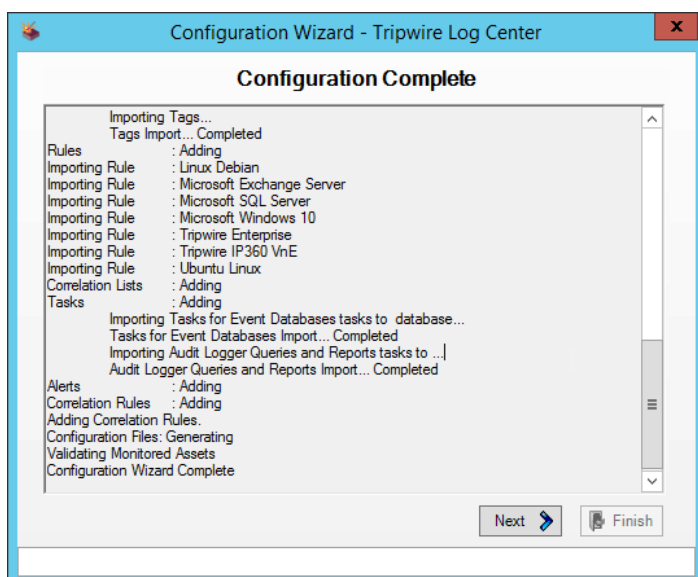
14. Select any log sources that you expect to collect with **Tripwire Log Center**. Examples: **Tripwire Enterprise, Microsoft Windows 10, Tripwire IP360 VnE, Linux Debian, Ubuntu Linux, Microsoft Exchange, Microsoft SQL Server**.



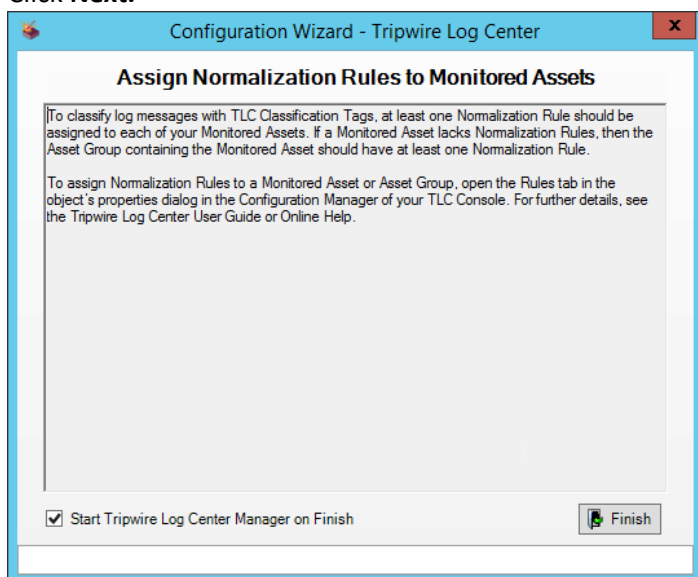
15. Click **Next**.



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

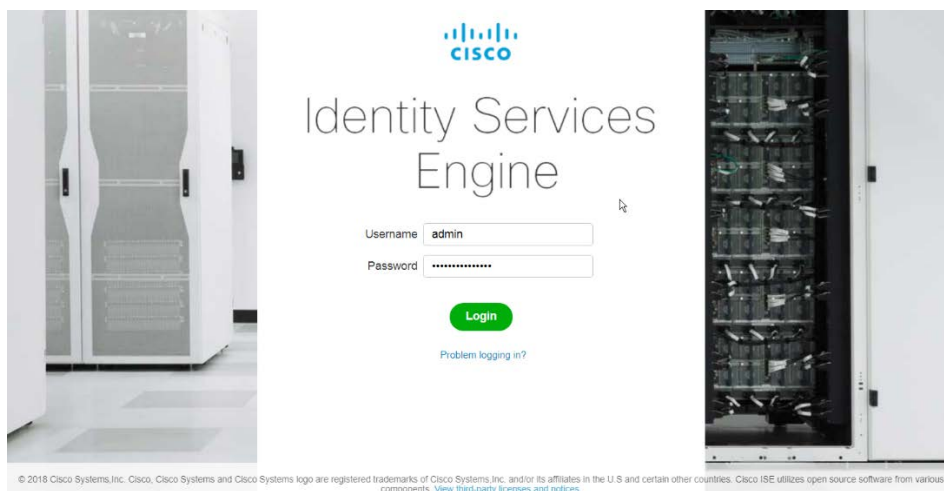
1. When prompted to log in for the first time, enter **setup**. (You can use the command **reset-config** to change these values later.)
2. Enter the desired **hostname** for the machine.
3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated with this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

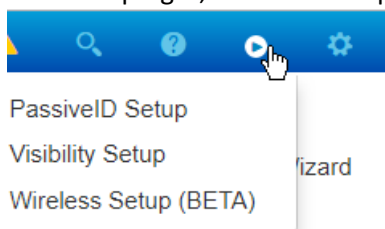
See the corresponding vendor documentation for the correct way to enable SNMP on your network device. Ensure that the community string you choose is considered sensitive, like a password.

2.11.3 Inventory: Configure Device Detection

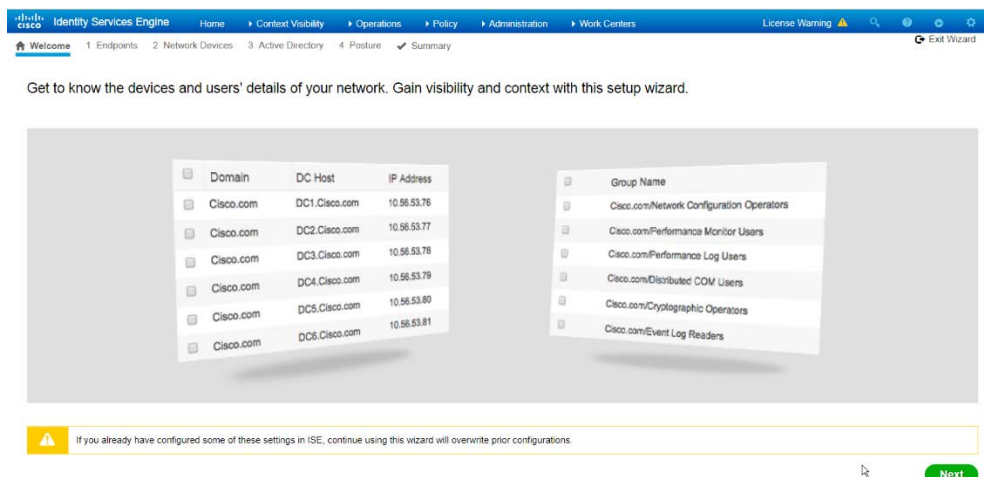
1. Log in to the web client by visiting <https://hostname/admin>, but replace **hostname** with the hostname of the ISE machine.



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



3. Click **Next**.



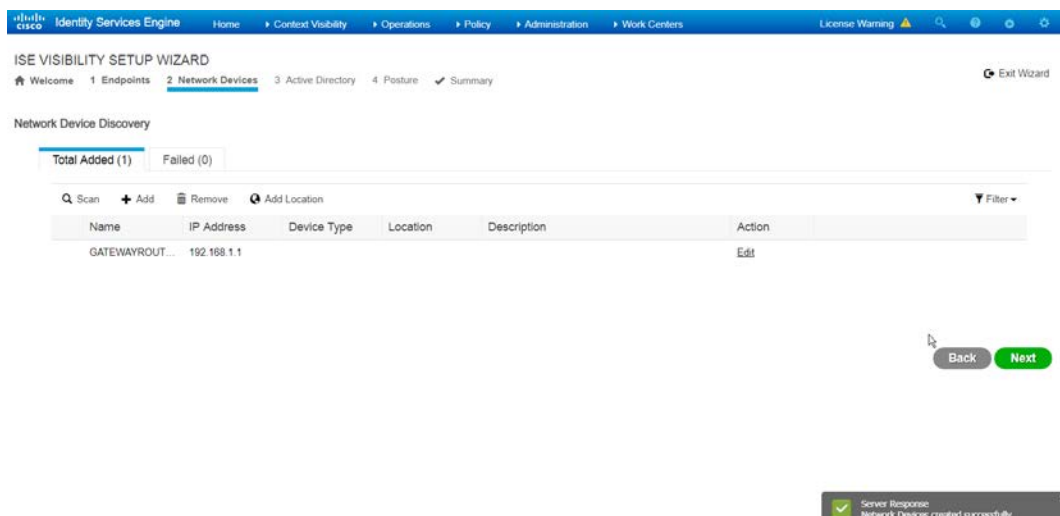
4. Enter the range of IP addresses to add to ISE's inventory.
5. Ensure that **Active Scanning** is checked.

The screenshot shows the 'Endpoints Discovery' screen in the Identity Services Engine (ISE) interface. The breadcrumb navigation at the top includes: Home > Context Visibility > Operations > Policy > Administration > Work Centers. A 'License Warning' icon is visible in the top right. The main heading is 'Endpoints Discovery'. Below it, a message states: 'We are going to discover the endpoints using the IP range(s) below.' There is a text input field for 'IP Address Range' containing '192.168.0.0/16' and a 'Delete' button to its right. Below the input field, a hint text says 'e.g. 10.10.10.0/24'. There is a checkbox for 'Active Scanning' which is currently checked. At the bottom, there is a link 'Add another range' and three buttons: 'Skip', 'Back', and 'Next'.

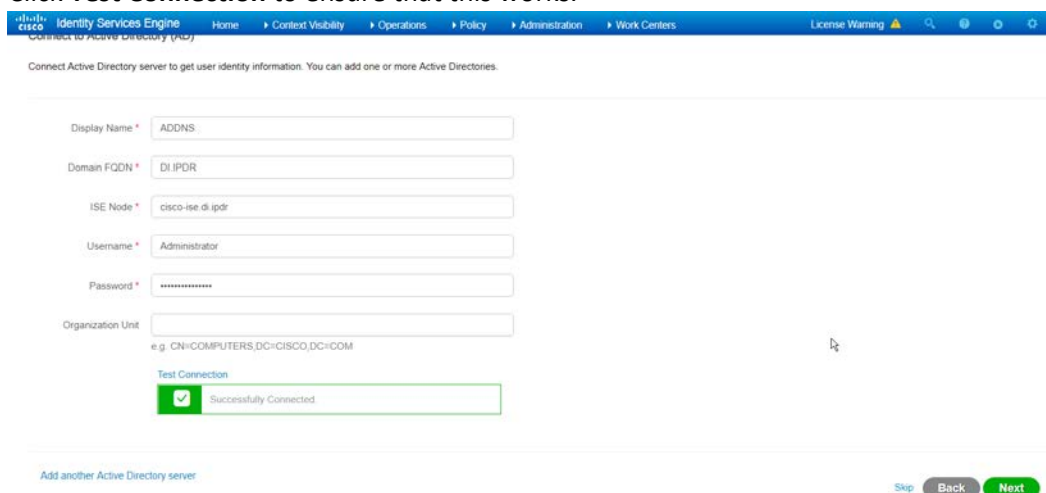
6. Click **Next**.
7. Click the **Add Device Manually** link.
8. Enter a **name**.
9. Enter the **IP address** of the network device you configured for SNMP.
10. Select **1** for **SNMP version**.
11. Enter the **community string** you created.

The screenshot shows the 'Add Network Device' dialog box in the ISE interface. The background shows the 'ISE VISIBILITY SETUP WIZARD' with steps: Welcome, 1. Endpoints, 2. Network Device. The dialog has a close button (X) in the top right. It contains several input fields: 'Name' (containing 'GATEWAYROUTER'), 'IP Address' (containing '192.168.1.1'), 'Location', 'Device Type', and 'Description'. Below these is the 'SNMP Settings' section, which includes a dropdown for 'SNMP Version' (set to '1') and a text field for 'RO Community' (containing a series of asterisks). There is a 'Show' button next to the 'RO Community' field. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

12. Click **OK**.



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



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

ISE VISIBILITY SETUP WIZARD

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Welcome 1 Endpoints 2 Network Devices 3 Active Directory 4 **Posture** ✓ Summary

Posture Discovery

Discover posture on endpoints using common administrative account and same IP range(s) from step 1

Username * Administrator

Password *

Enable Endpoint Logging ☒

IP Address Range * 192.168.0.0/16

Include Range ☒

Skip Back Next

23. Click **Next**.

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

Active Scanning true

Network Device Discovery

Total Devices Added 1

Active Directory Information

Display Name ADDNS

Domain FQDN DI IPDR

ISE Node cisco-ise di.ipdr

Username

Test Connection

Successfully Connected

Posture Discovery

IP Scanning Range 192.168.0.0/16

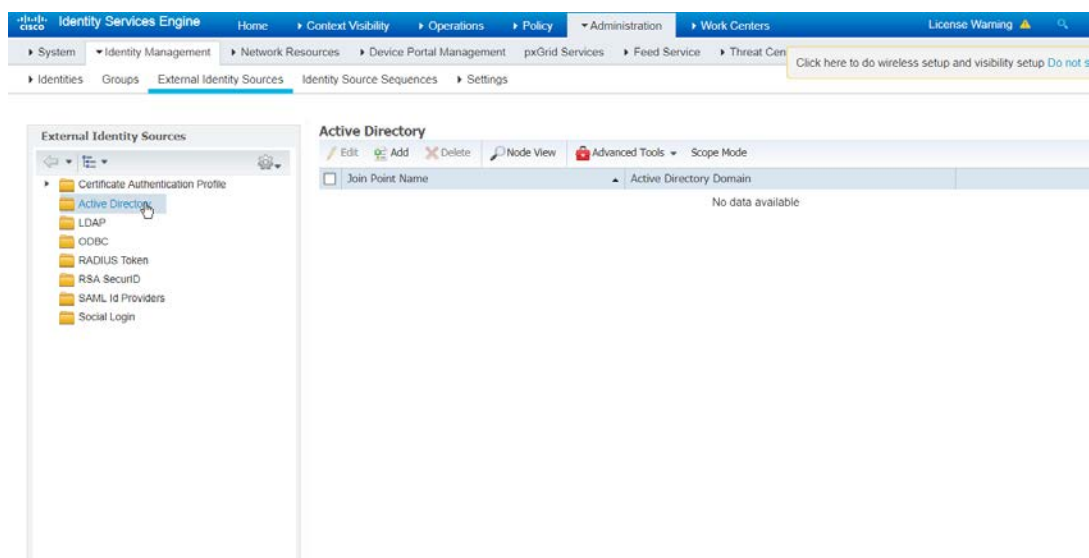
Included true

Back Done

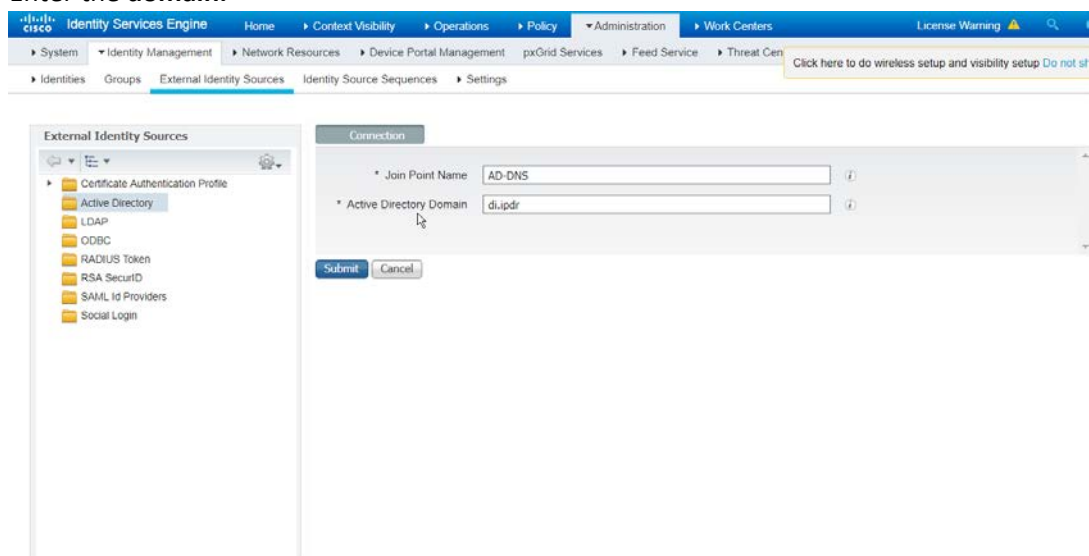
24. Verify the settings, and click **Done**. (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

2.11.4 Policy Enforcement: Configure Active Directory Integration

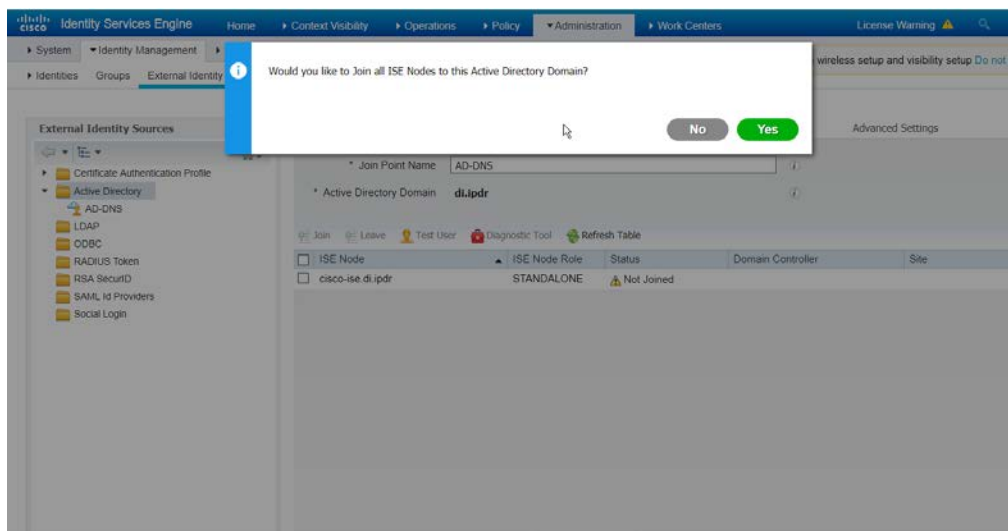
1. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory*.



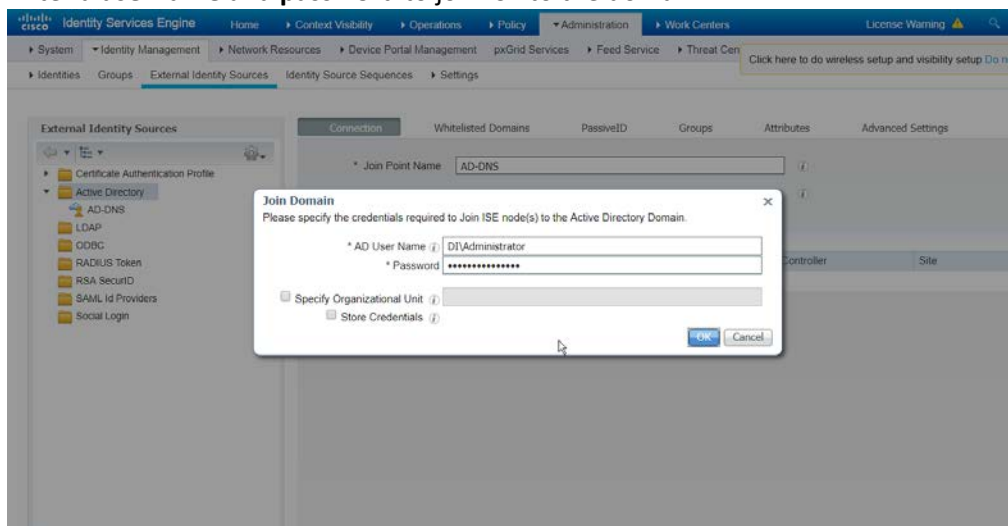
2. Click **Add**.
3. Enter a **name**.
4. Enter the **domain**.



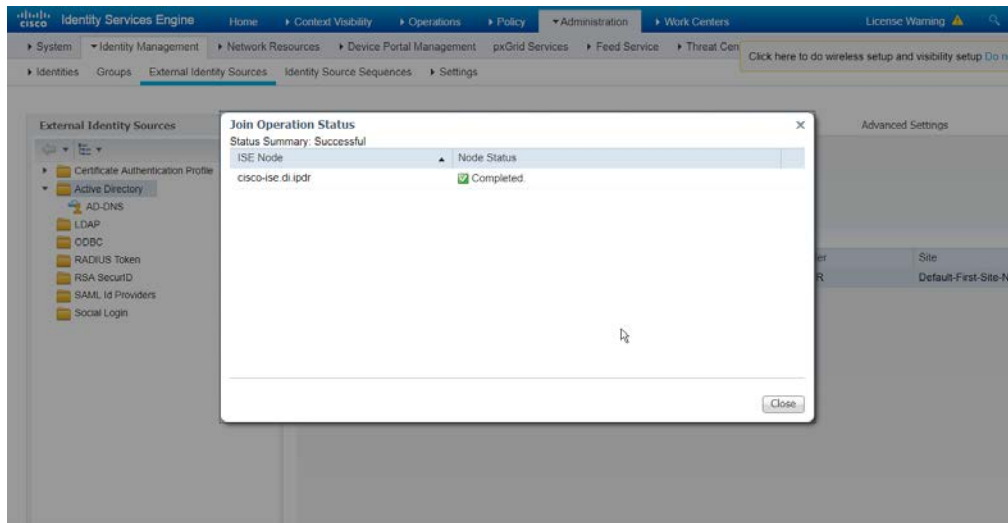
5. Click **Submit**.



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



8. Click **OK**.

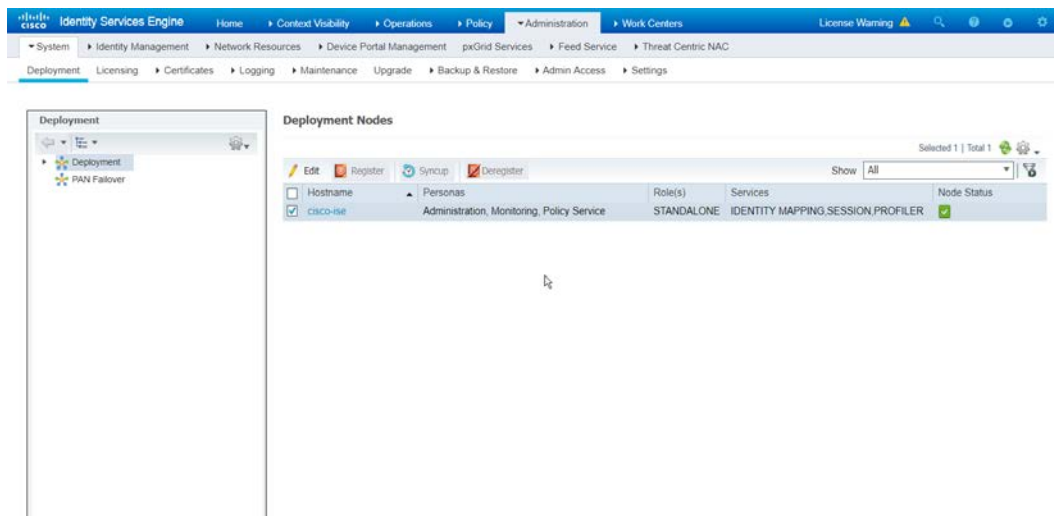


9. Click **Close** when the join is finished.

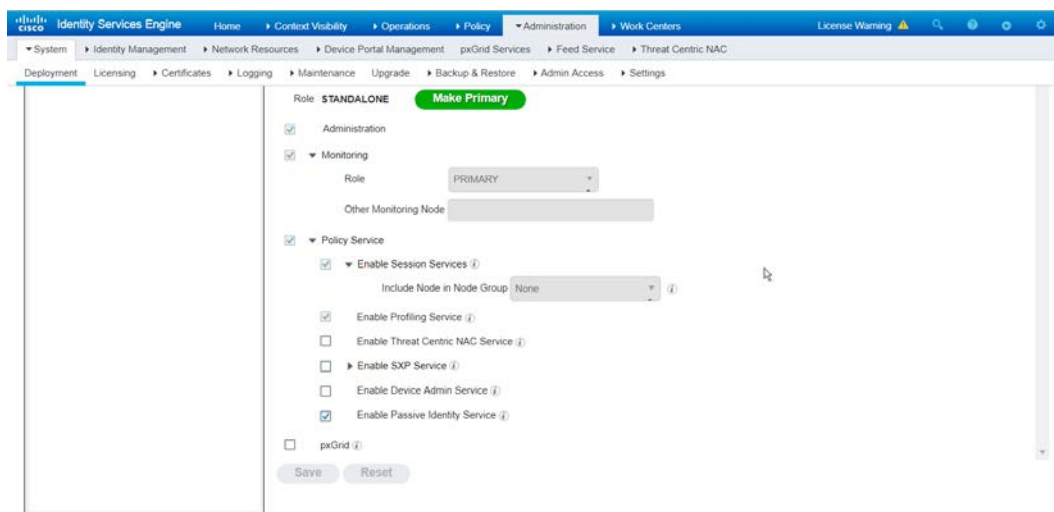
2.11.5 Policy Enforcement: Enable Passive Identity with AD

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.

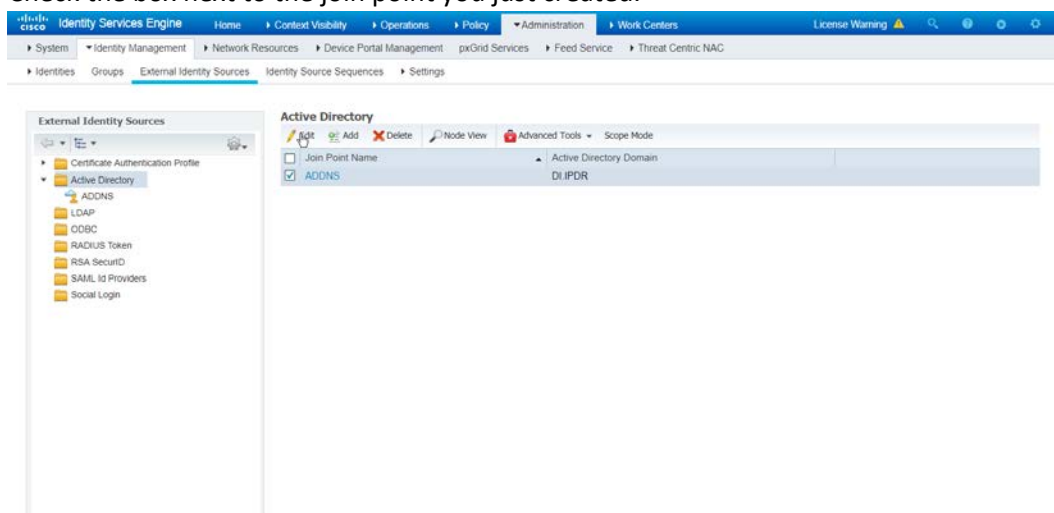
1. Navigate to **Administration > System > Deployment**.
2. Check the box next to **ISE**.



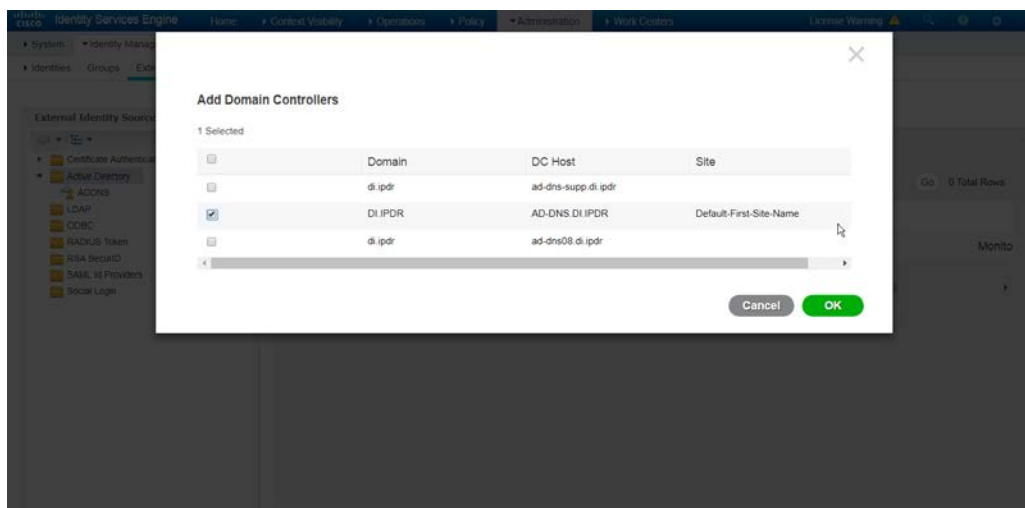
3. Click **Edit**.
4. Check the box next to **Enable Passive Identity Service**.



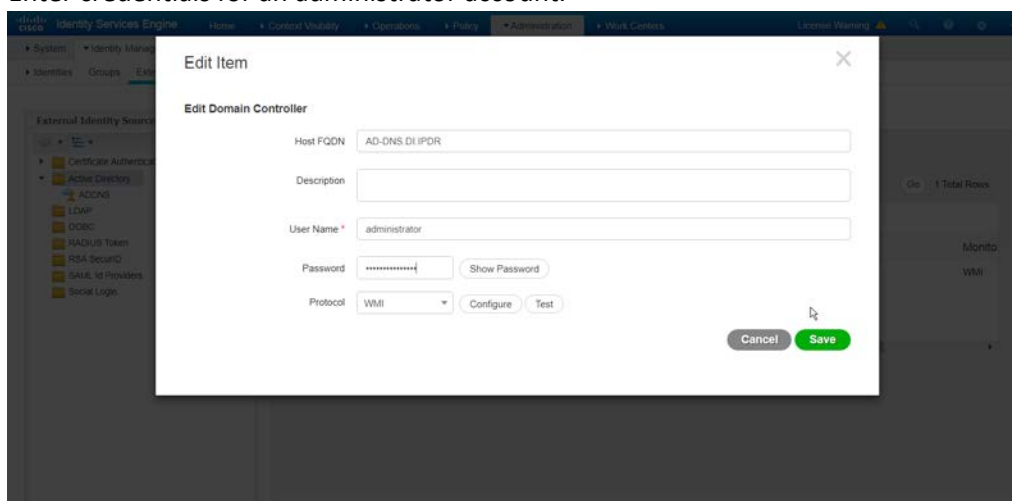
5. Click **Save**.
6. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory*.
7. Click the name of the Active Directory machine.
8. Check the box next to the join point you just created.



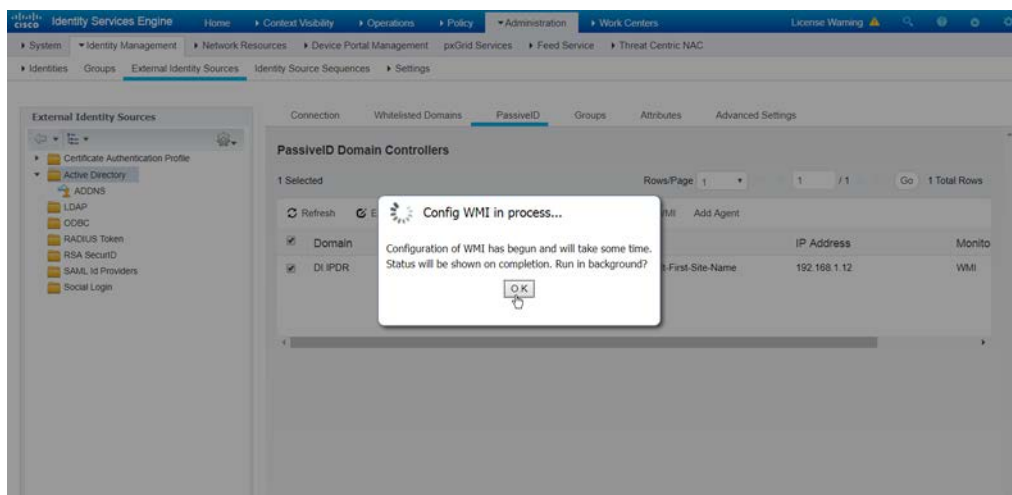
9. Click **Edit**.
10. Click the **PassiveID** tab.
11. Click **Add DCs** if there are no domain controllers listed.



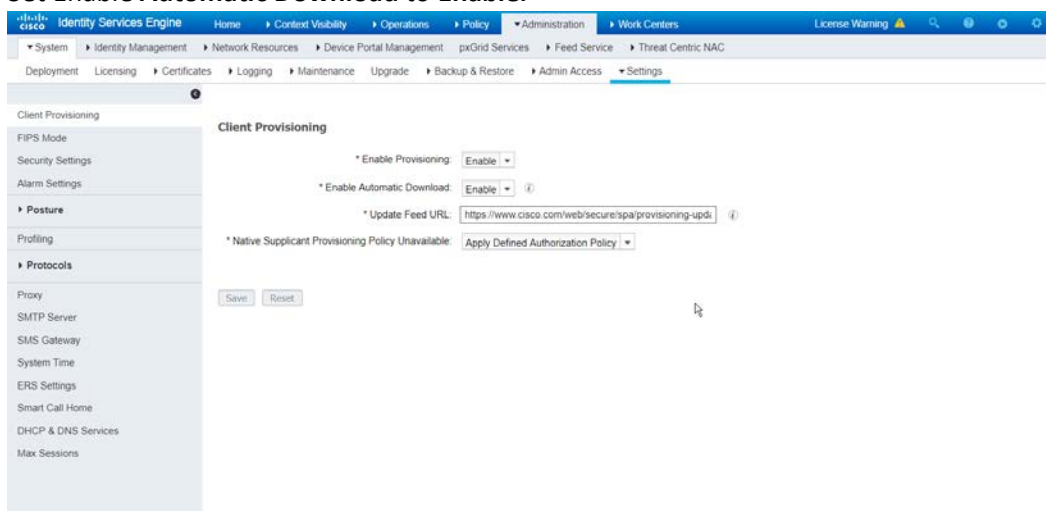
12. Select the Active Directory domain controller.
13. Click **OK**.
14. Check the box next to the selected domain controller.
15. Click **Edit**.
16. Enter credentials for an administrator account.



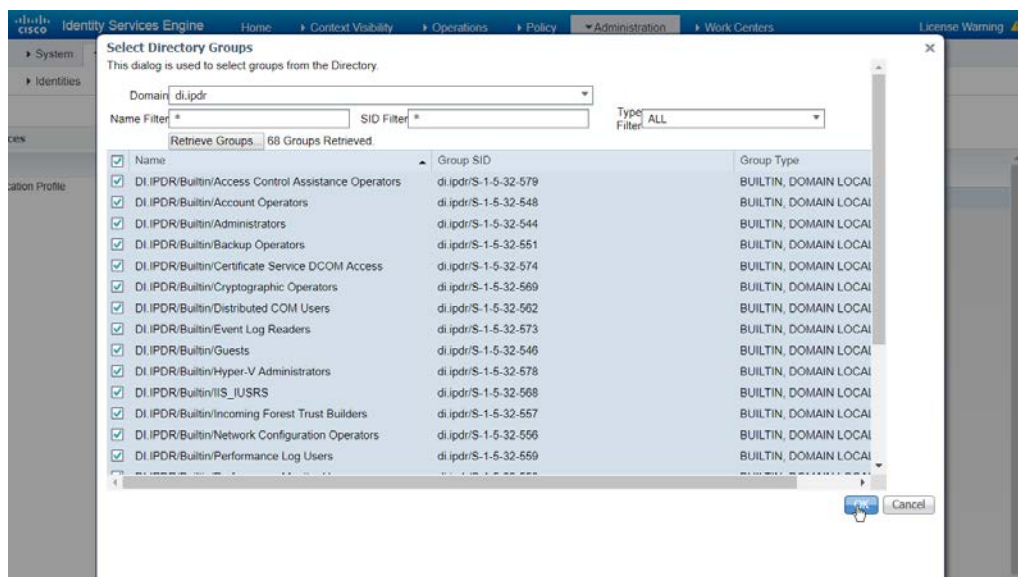
17. Click **Save**.
18. Click **Config WMI**.
19. Click **OK**.



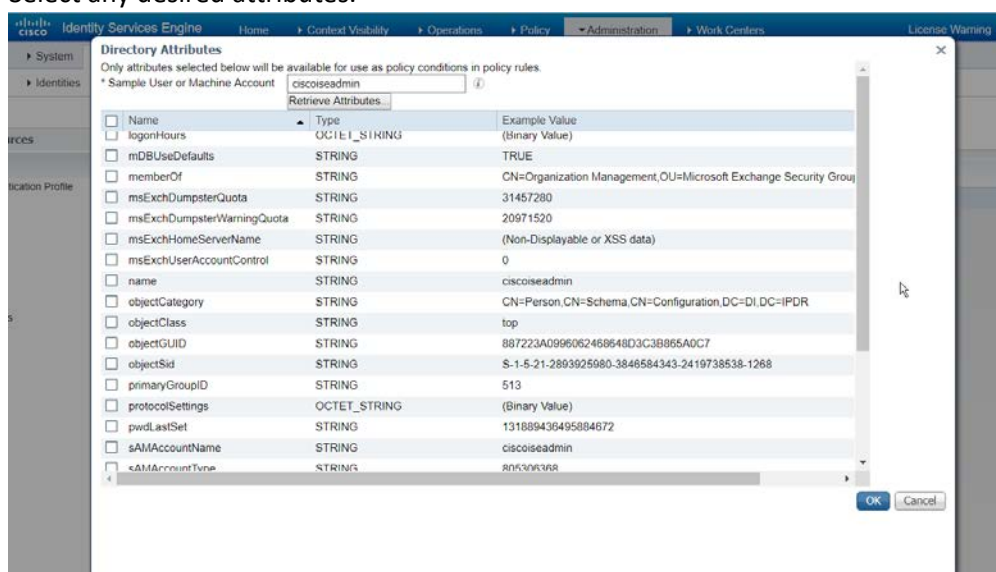
20. Click **OK** when this configuration finishes.
21. Navigate to *Administration > System > Settings > Client Provisioning*.
22. Set **Enable Automatic Download** to **Enable**.



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.

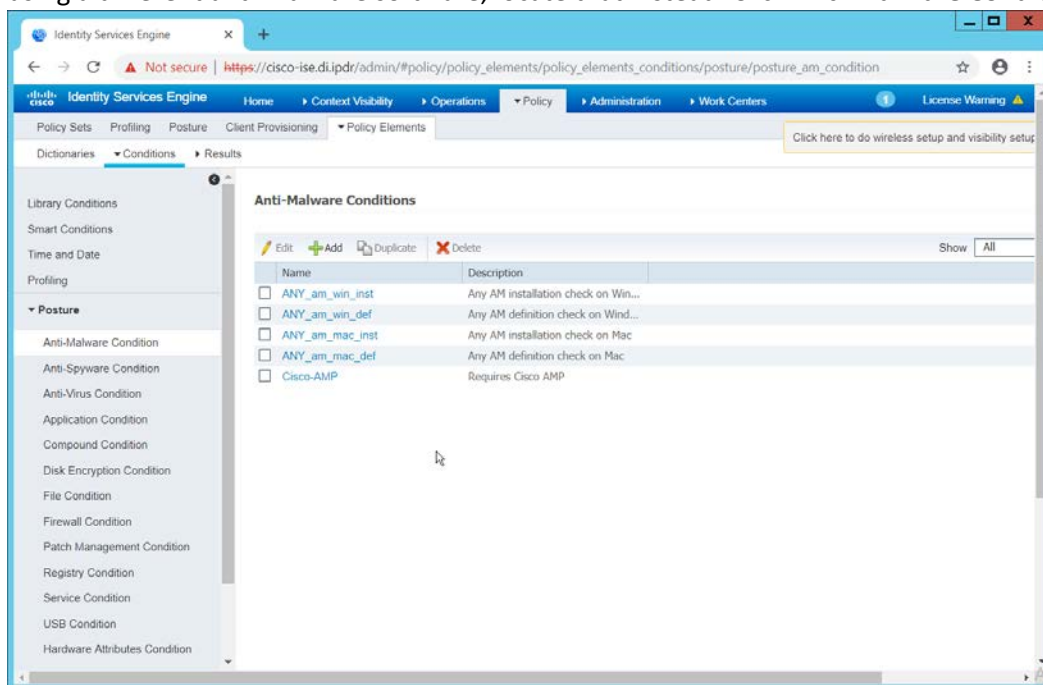


36. Click **OK**.

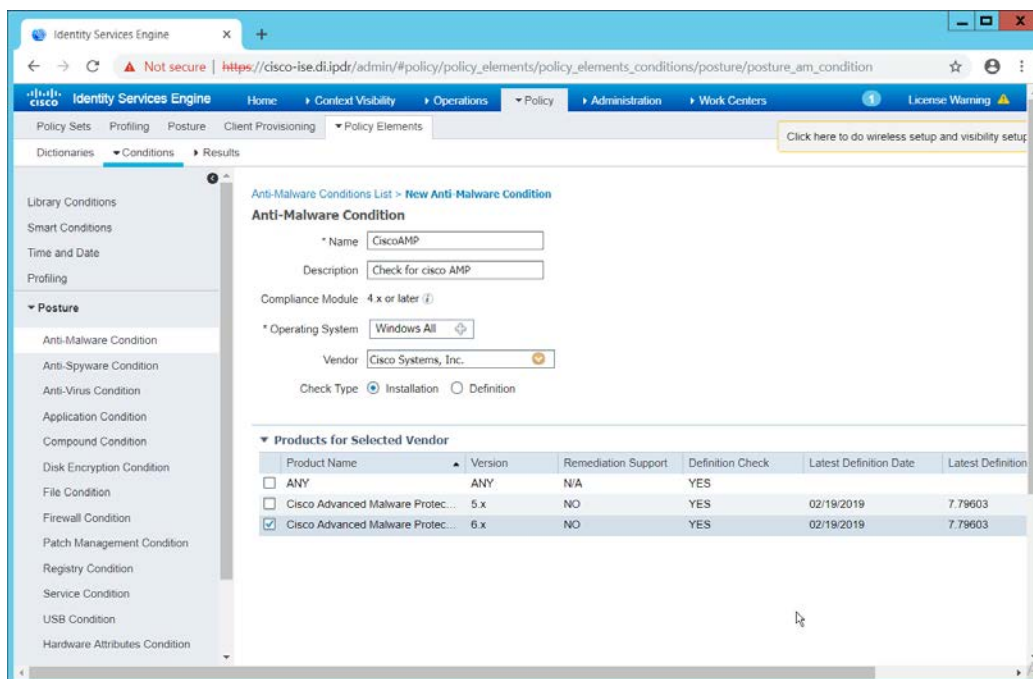
37. Click **Save**.

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**.



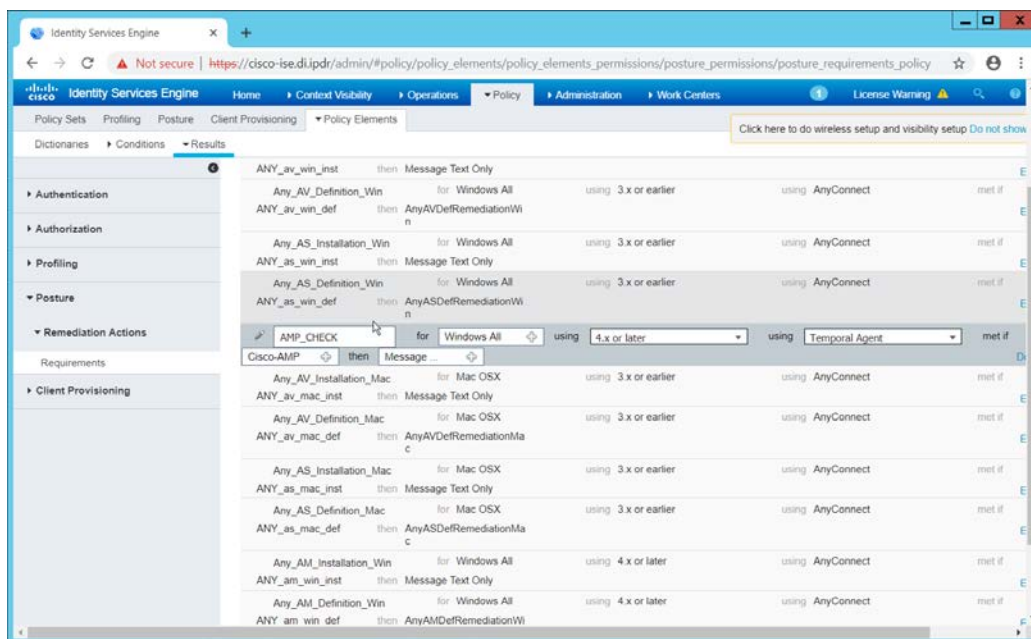
4. Click **Add**.
5. Enter a **name**.
6. Enter a **description** if desired.
7. Select **Windows All** for **Operating System**.
8. Select **Cisco Systems, Inc.** for **Vendor**.
9. Under **Products for Selected Vendor**, check the box next to **Cisco Advanced Malware Protection**, with the version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



10. Click **Submit**.

2.11.7 Policy Enforcement: Developing Policy Results

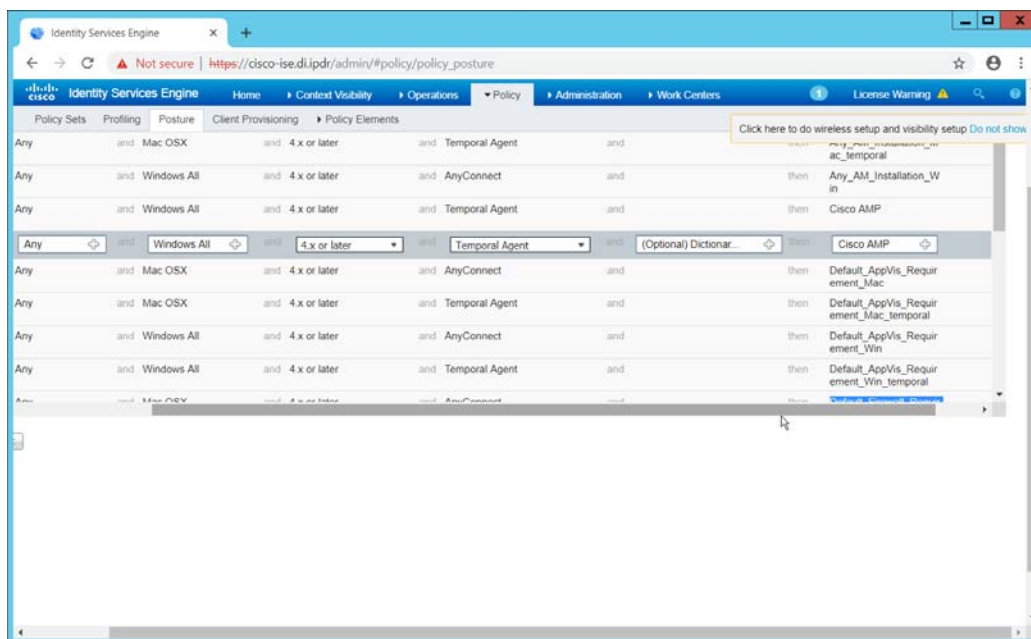
1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements**.
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement**.
3. Enter a **name**.
4. Select **Windows All** for **Operating Systems**.
5. Select **4.x or later** for **Compliance Module**.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

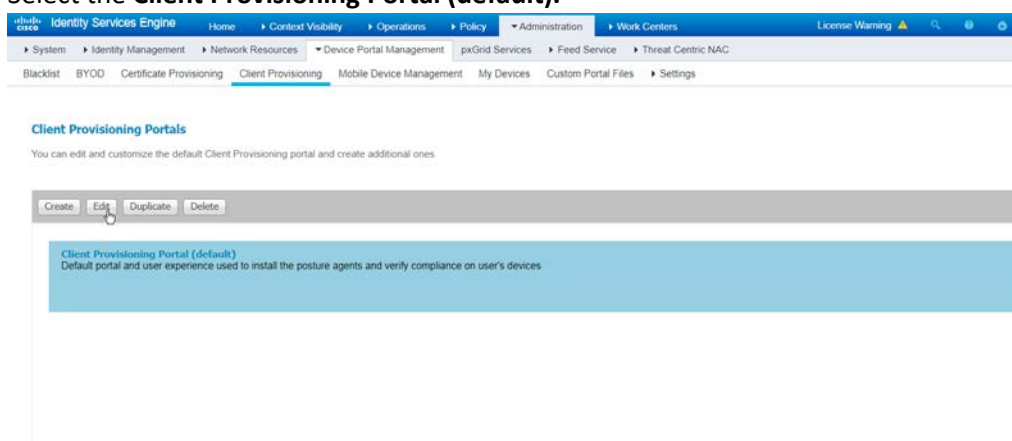
1. Navigate to **Policy > Posture**.
2. Click one of the black arrows next to the **Edit** link and select **Insert New Policy**.
3. Enter a **name**.
4. Select **Windows All** for **Operating Systems**.
5. Select **4.x or later** for **Compliance Module**.
6. Select **Temporal Agent** for **Posture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

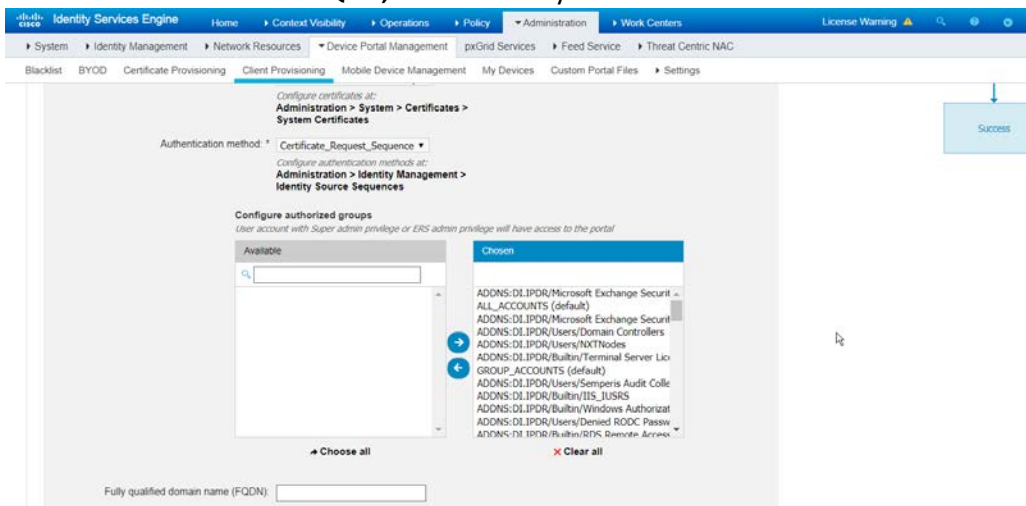
2.11.9 Policy Enforcement: Configuring a Web Portal

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

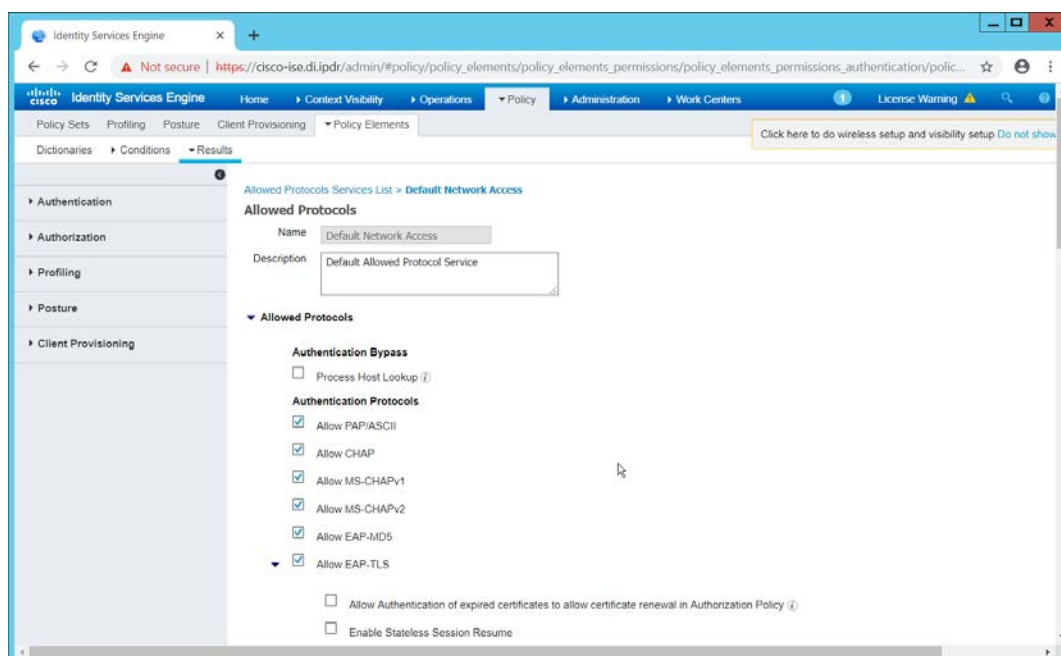
Cisco ISE requires a Remote Authentication Dial-In User Service (RADIUS) session for posture to function. Posture refers to ISE's ability to check that a machine complies with a specified policy, which may be based on the OS and may contain requirements such as the installation of certain security applications 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, Media Access Control (MAC) address authentication, or user authentication. A captive web portal, if the device supports it, may be ideal for configuration without the correct hardware.

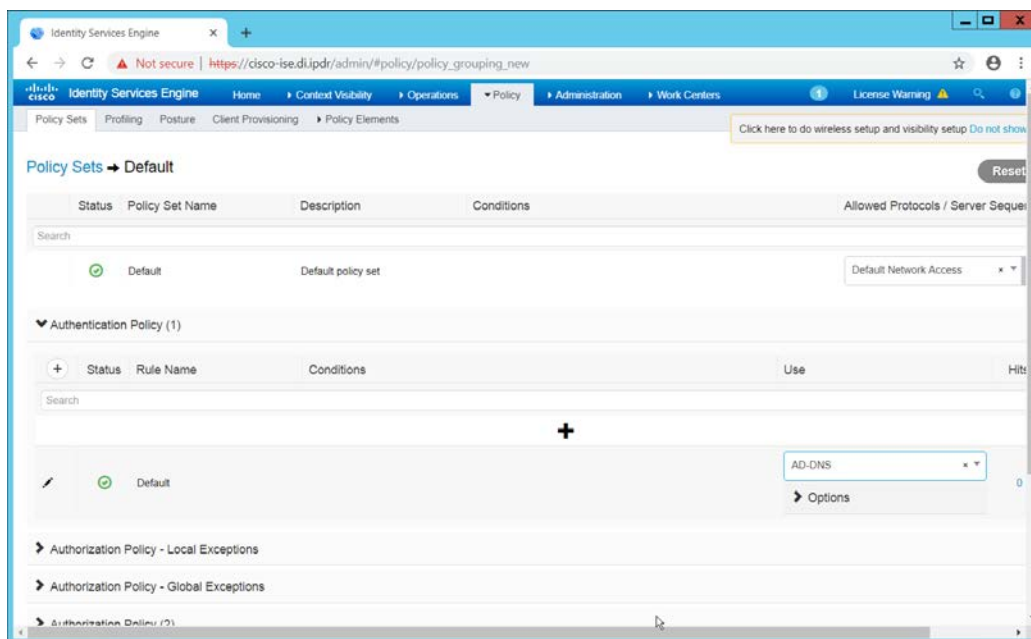
- b. There are also many switches that provide direct 802.1x username/password authentication. Note that if you choose to use this mechanism, a client is still required, and it will not be in the web browser. Windows has a built-in **802.1x** client that can be configured on Network adapters under the **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**.



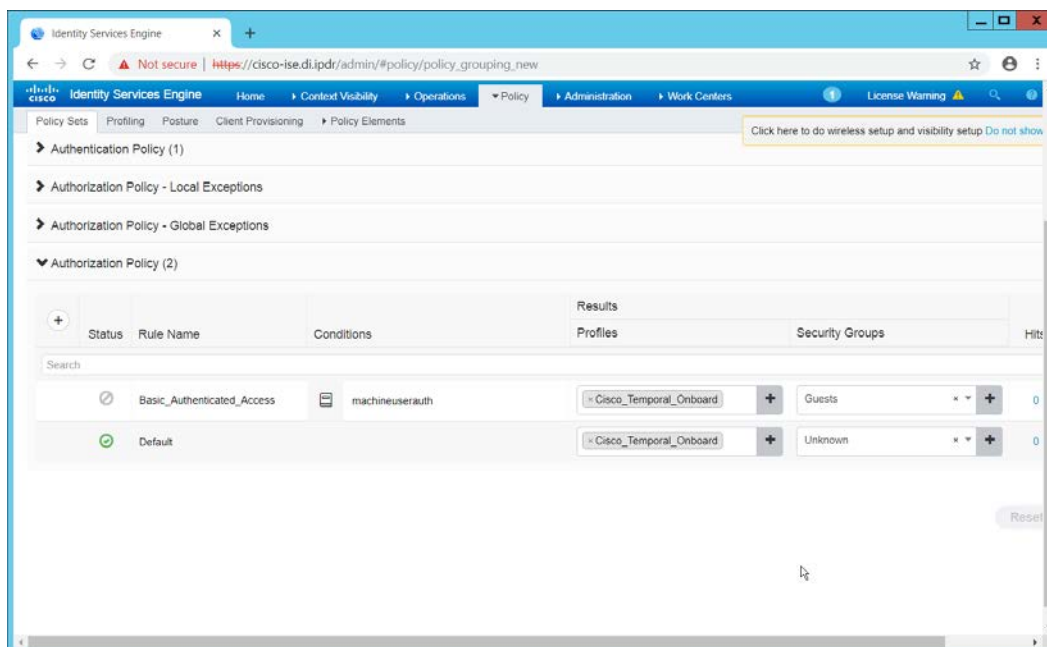
4. Click **Save**.
5. Navigate to **Policy > Policy Sets**.
6. Select the default policy.
7. Ensure that the **Allowed Protocol** selection matches the allowed protocol you just created/edited.
8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate users. 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>.

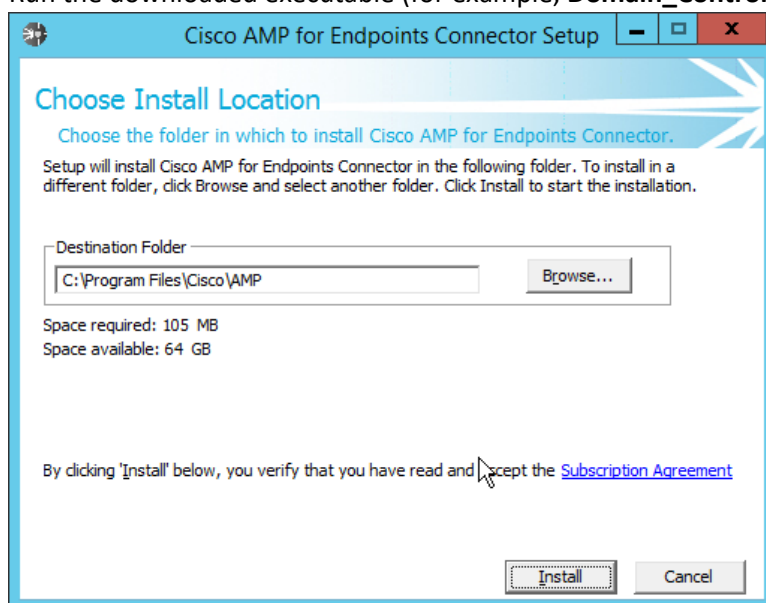
2.12.1 Dashboard Configuration

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.

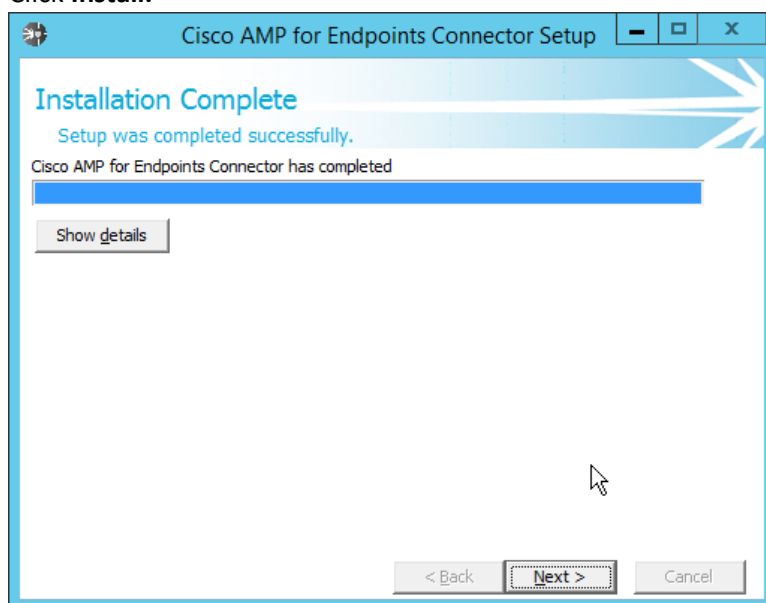
2.12.2 Installing the Connector on a Windows Server

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**.

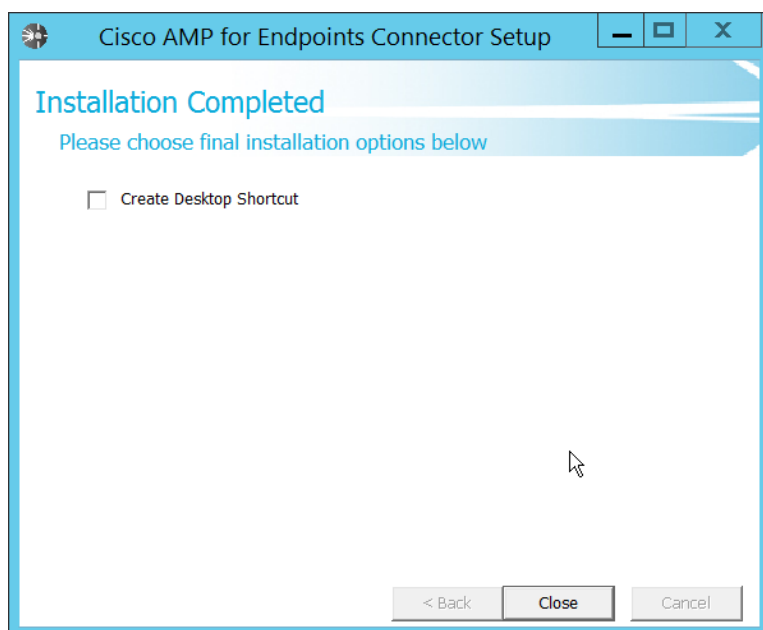
3. Find the correct OS version of the installer, and click **Download**.
4. Run the downloaded executable (for example, **Domain_Controller_FireAMPSetup.exe**).



5. Click **Install**.



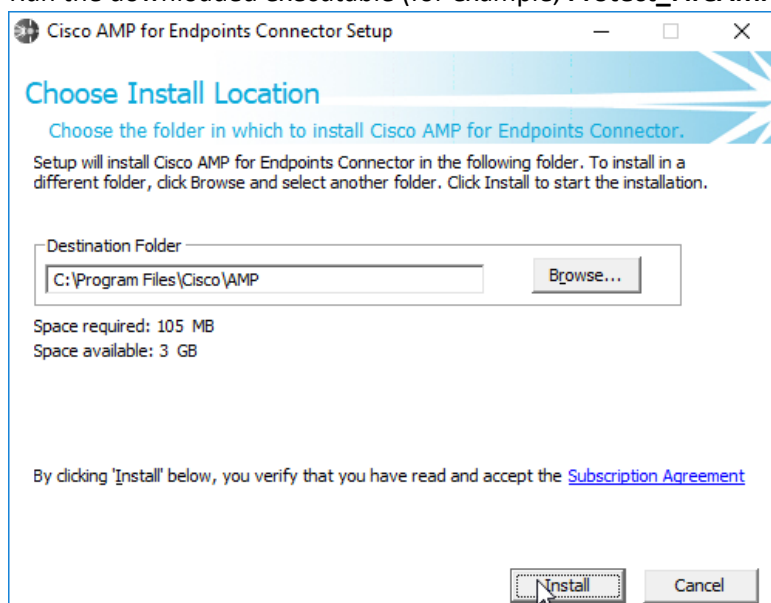
6. Click **Next**.



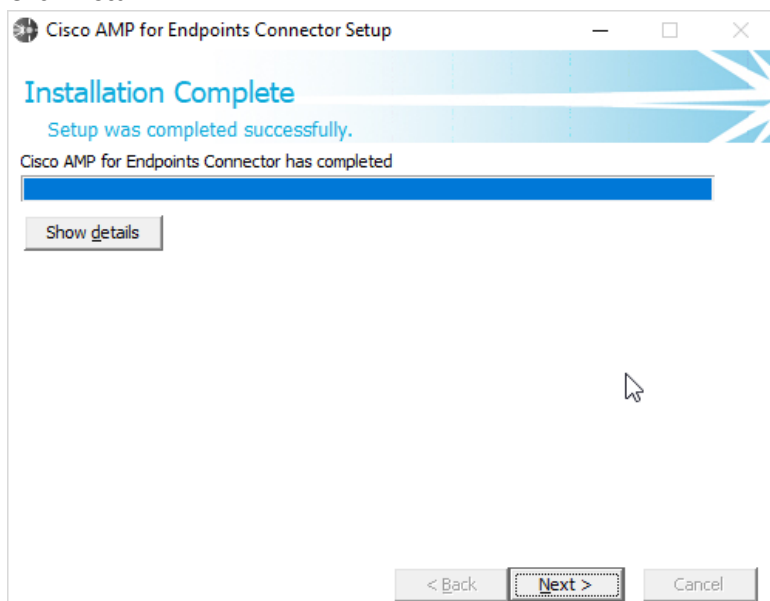
7. Click **Close**.

2.12.3 Installing the Connector on a Windows 10 Machine

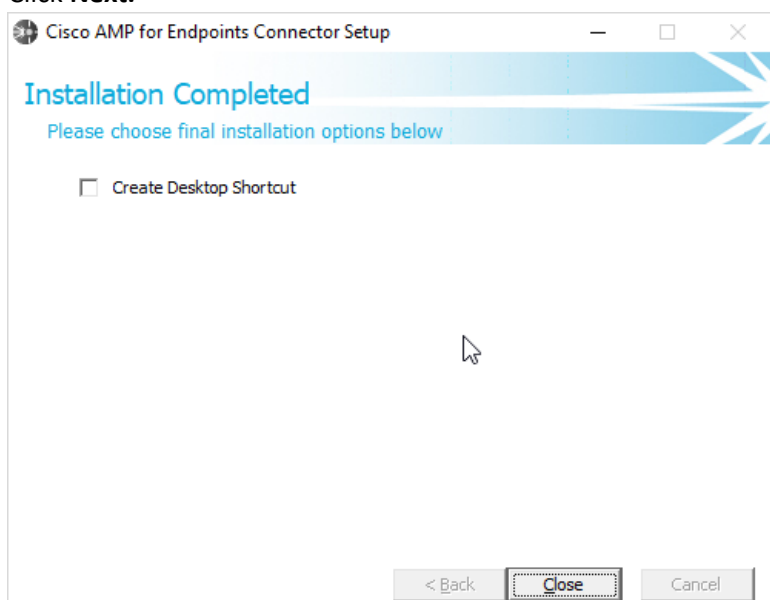
1. On the Cisco AMP dashboard, navigate to **Management > Download Connector**.
2. Select the AMP group in which to put the machine. For this installation we chose **Protect**.
3. Find the correct OS version of the installer, and click **Download**.
4. Run the downloaded executable (for example, **Protect_FireAMPSetup.exe**).



5. Click **Install**.



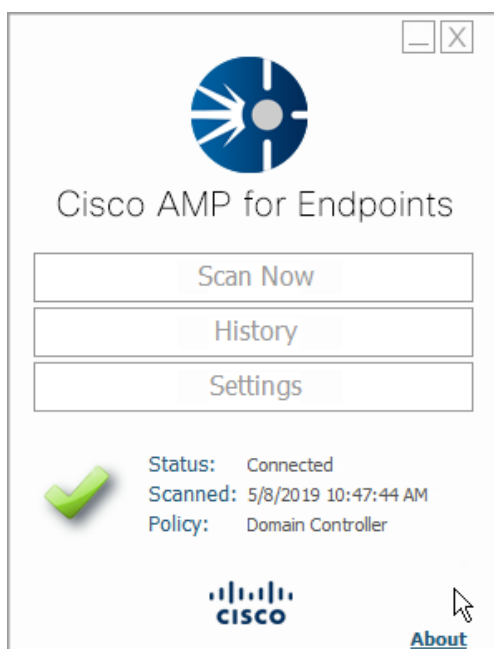
6. Click **Next**.



7. Click **Close**.

2.12.4 Scanning using AMP

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.)

Policies

[View All Changes](#)

The screenshot shows the McAfee Endpoint Protection Policies management interface. The 'Domain Controller' policy is selected and expanded, showing configuration details for Modes and Engines, Exclusions, Proxy, Groups, Outbreak Control, and Application Control. The 'Groups' tab shows the 'Domain Controller' group with 2 devices.

Modes and Engines		Exclusions	Proxy	Groups
Files	Audit	Altiris by Symantec	Not Configured	Domain Controller
Network	Disabled	AVAST		
Malicious Activity Protection	Disabled	Avira		
System Process Protection	Protect	Diebold Warsaw		

Outbreak Control		Application Control	Network
Custom Detections - Simple	Custom Detections - Advanced	Execution Blacklist	Blocked
File Blacklist	Not Configured	File Whitelist	Allowed

View Changes Modified: 2019-05-20 14:56:48 UTC Serial Number: 54 Download XML Duplicate Edit Delete

1 - 8 of 8 total records 25 / page 1 of 1

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.

Name: Domain Controller

Description: This is a lightweight policy for use on Active Directory Domain Controllers.

Modes and Engines

Exclusions
20 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Conviction Modes

These settings control how AMP for Endpoints responds to suspicious files and network activity.

Files

Quarantine Audit

Network

Block Audit Disabled

Malicious Activity Protection

Quarantine Block Audit Disabled

System Process Protection

Protect Audit Disabled

Detection Engines

☒ TETRA ⓘ

☒ Exploit Prevention ⓘ

Recommended Settings

Workstation

Files: Quarantine

Network: Block

Malicious Activity Protection: Quarantine

System Process Protection: Protect

Server

Files: Quarantine

Network: Disabled

Malicious Activity Protection: Disabled

System Process Protection: Disabled

Cancel Save

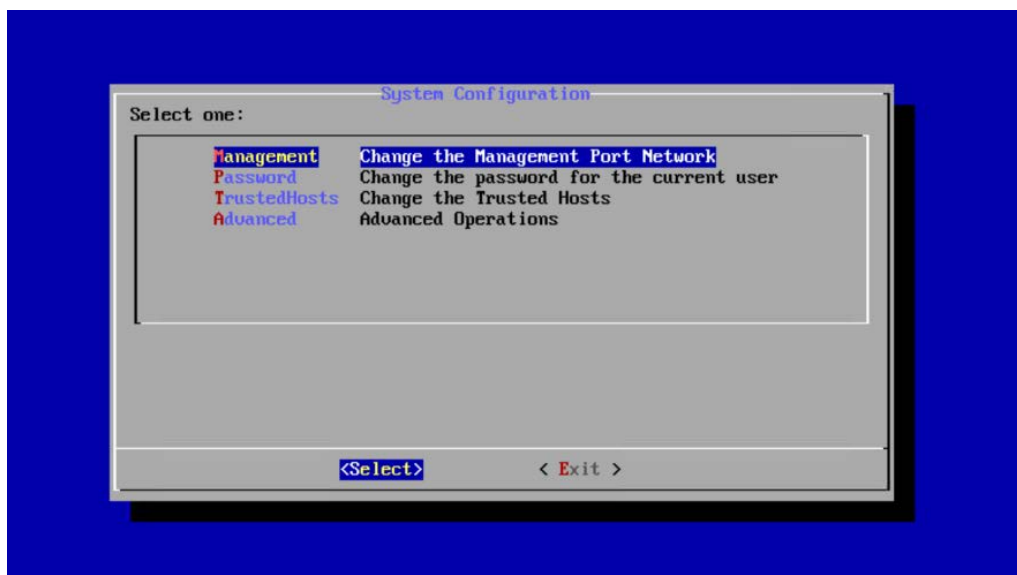
6. Click **Save**.

2.13 Cisco Stealthwatch

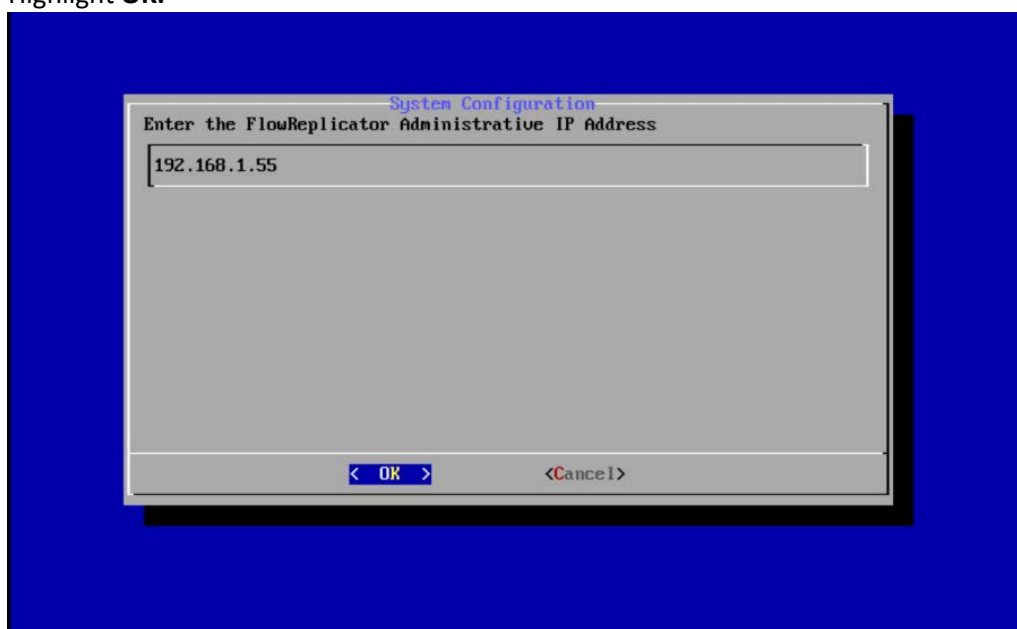
This section will describe the setup and configuration of Cisco Stealthwatch, a network monitoring solution. This guide assumes the use of the Stealthwatch virtual machines.

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

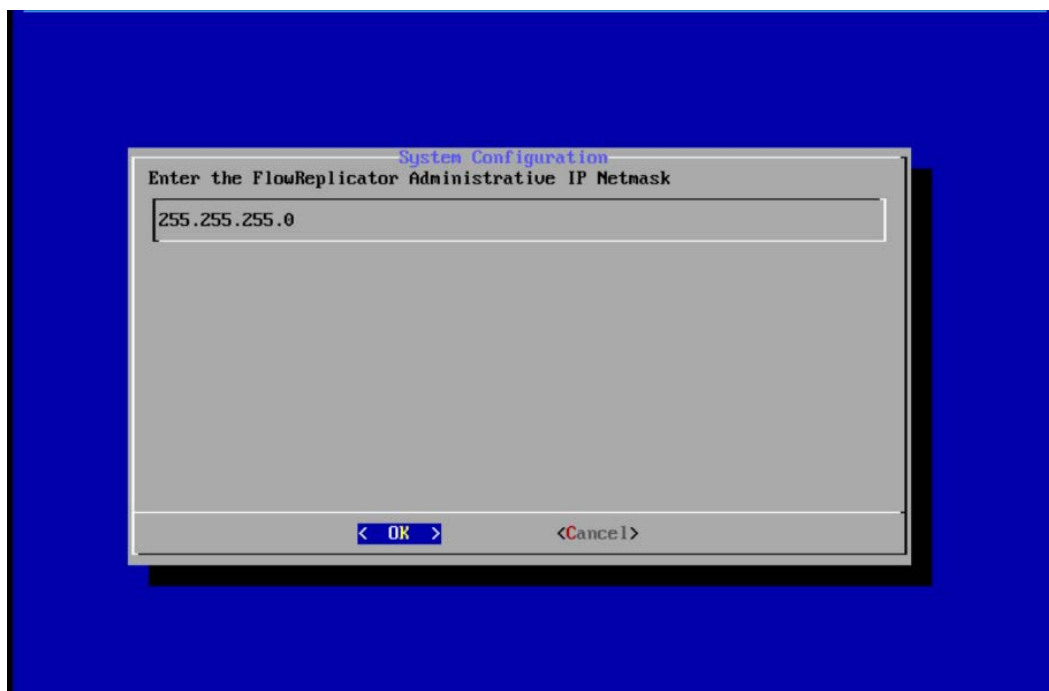
1. Log in to the console of **Stealthwatch Flow UDP Director**.
2. Navigate the menu to highlight **Management** and **Select**.



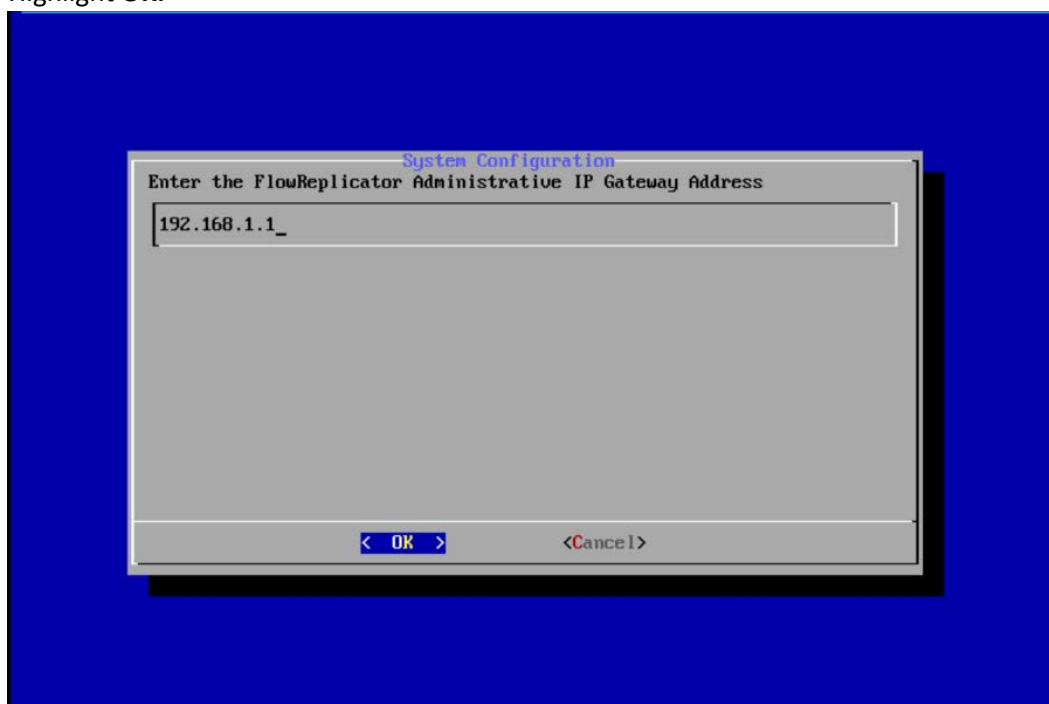
3. Press **Enter**.
4. Enter an **IP Address** for this machine.
5. Highlight **OK**.



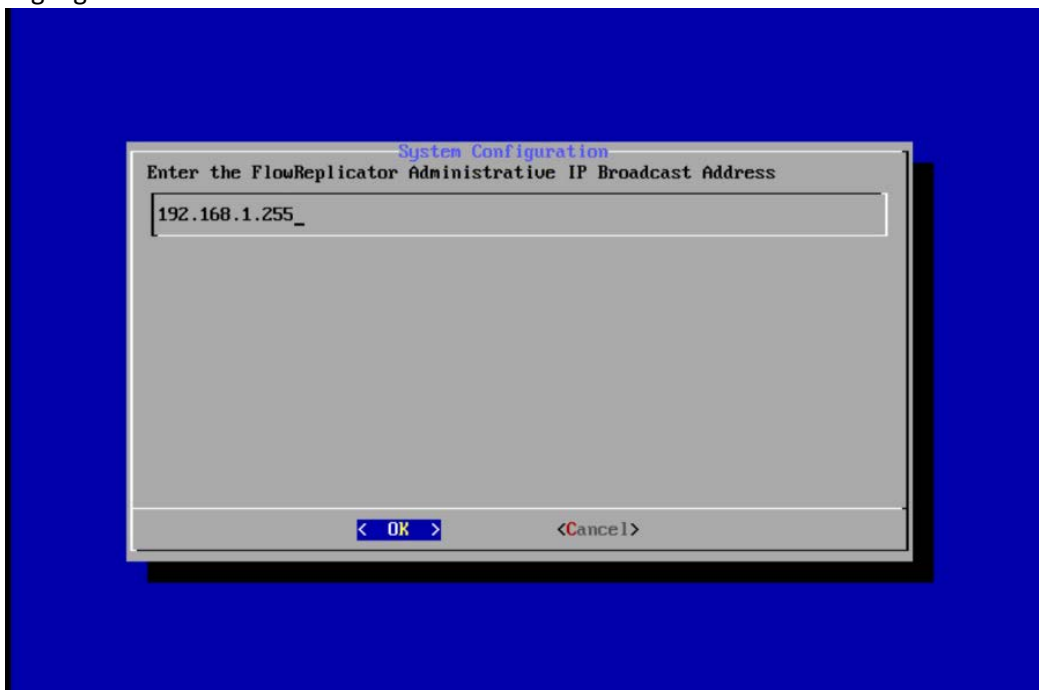
6. Press **Enter**.
7. Enter a **network mask** for the IP Address.
8. Highlight **OK**.



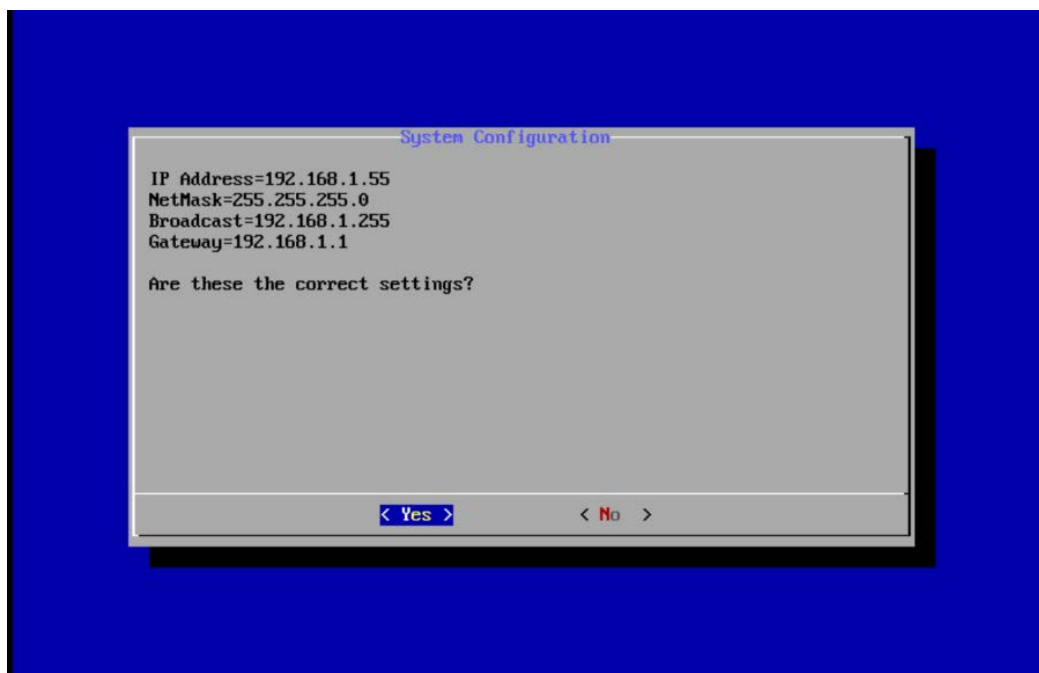
9. Press **Enter**.
10. Enter the network **gateway**.
11. Highlight **OK**.



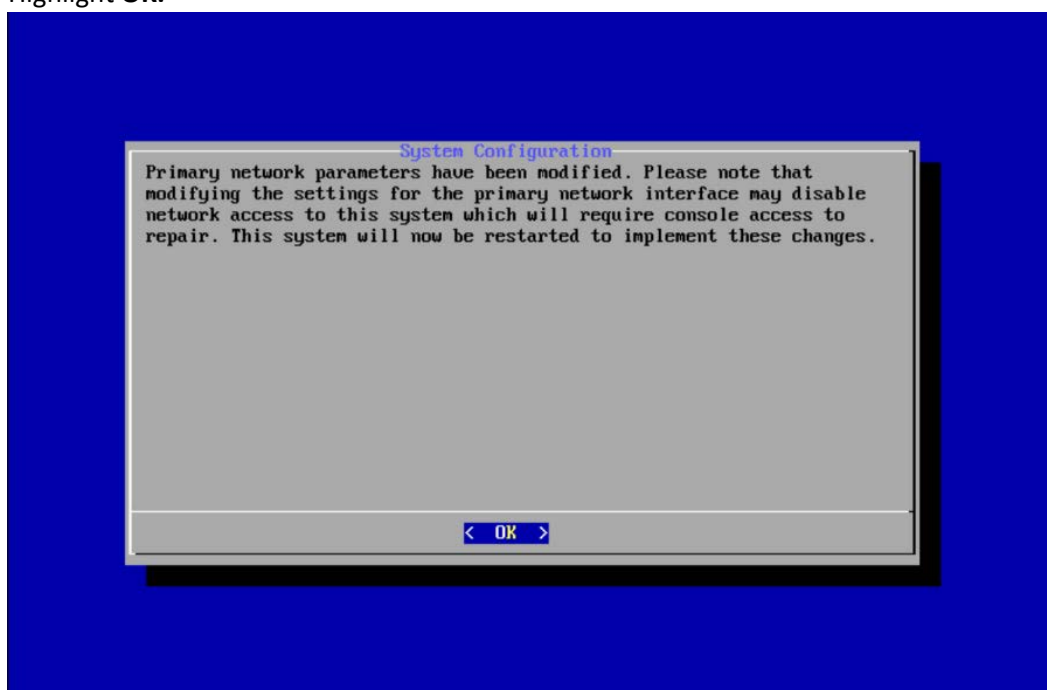
12. Press **Enter**.
13. Enter the network **broadcast address**.
14. Highlight **OK**.



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



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

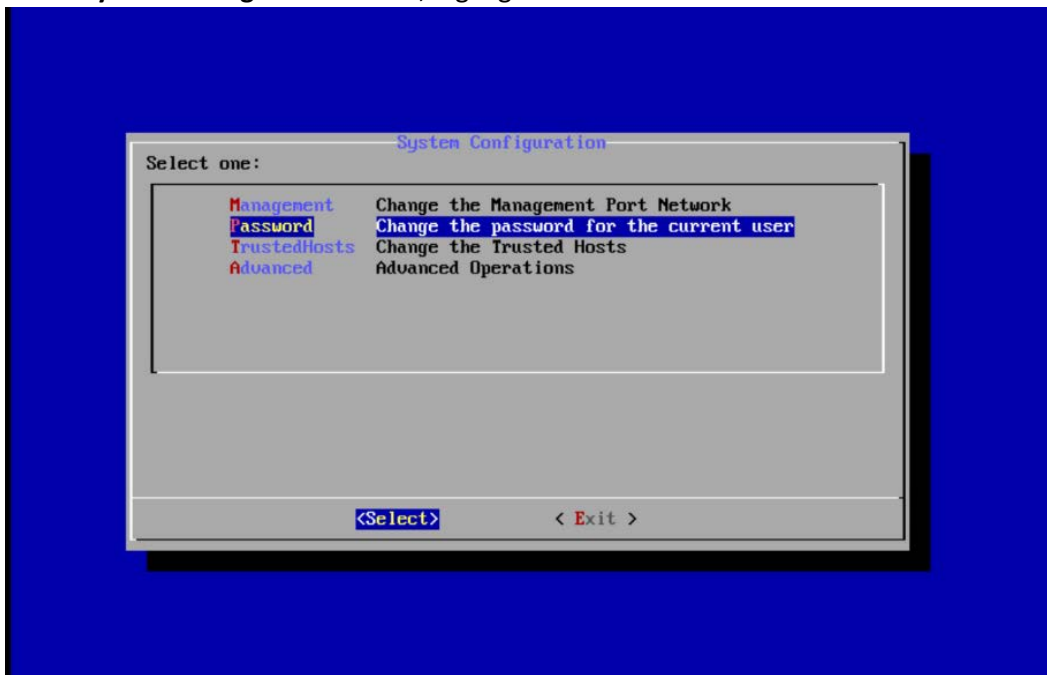


19. Press **Enter**.

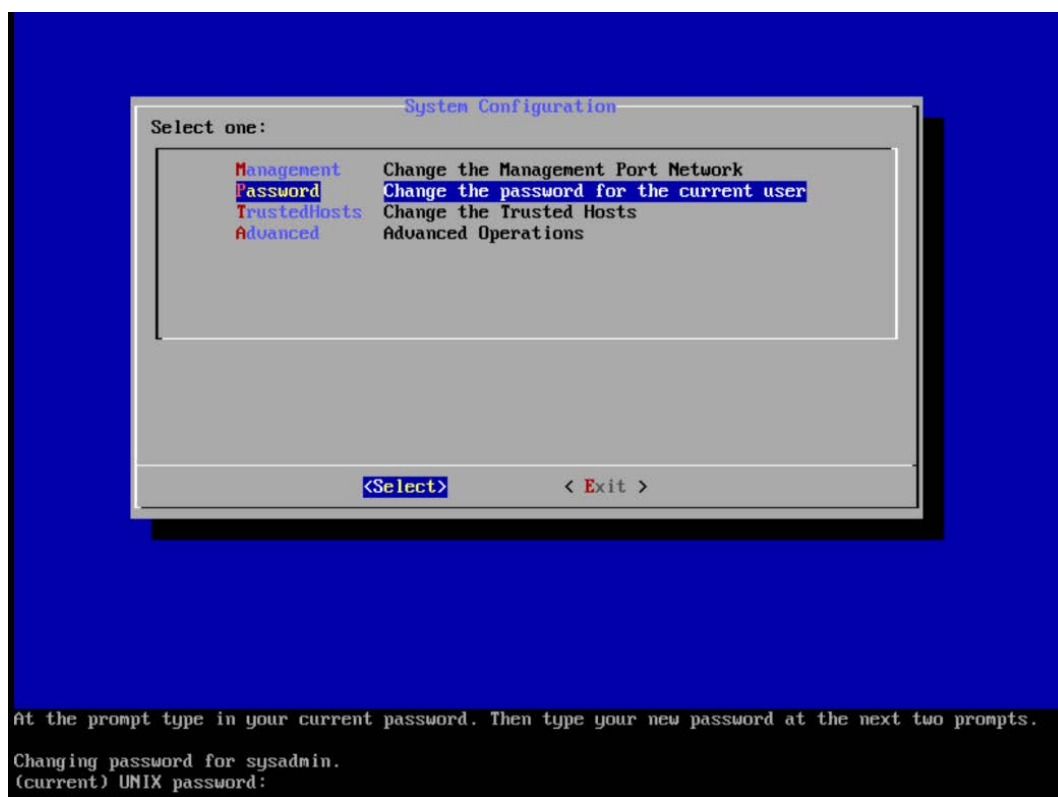
20. Repeat steps 1-19 for each of the **Stealthwatch Management Console**, **Stealthwatch UDP Director**, **Stealthwatch Flow Sensor**, and **Stealthwatch Flow Collector**.

2.13.2 Change Default Stealthwatch Console Passwords

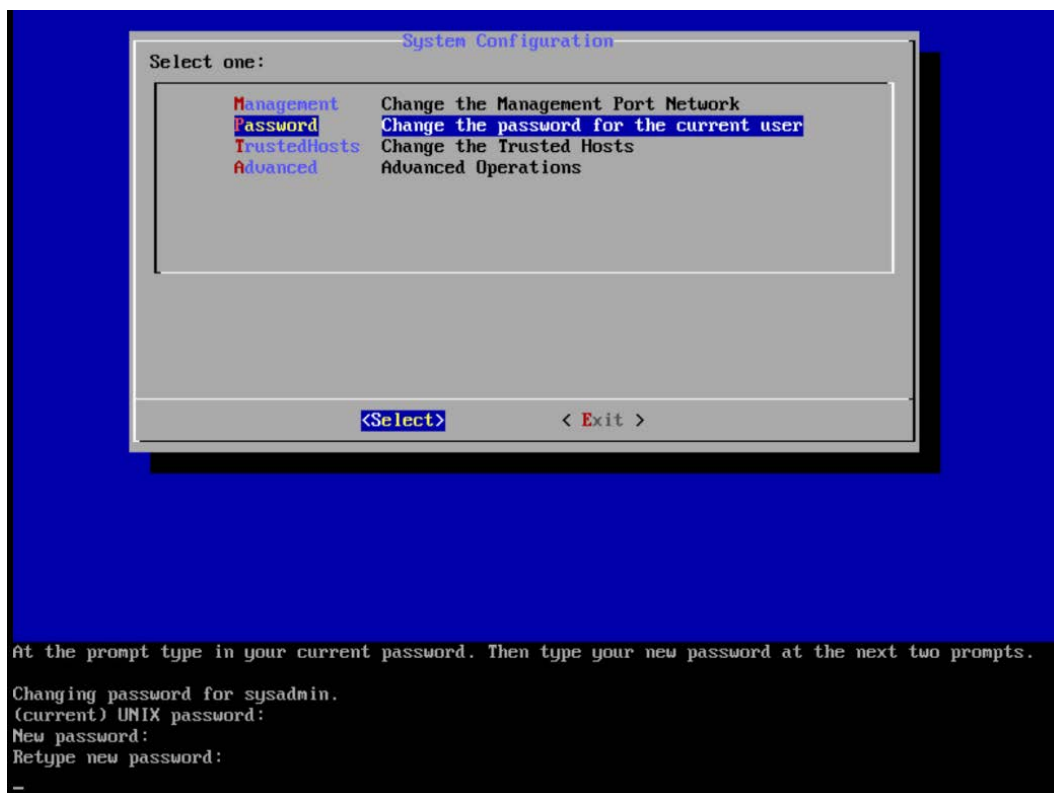
1. In the **System Configuration** menu, highlight **Password** and **Select**.



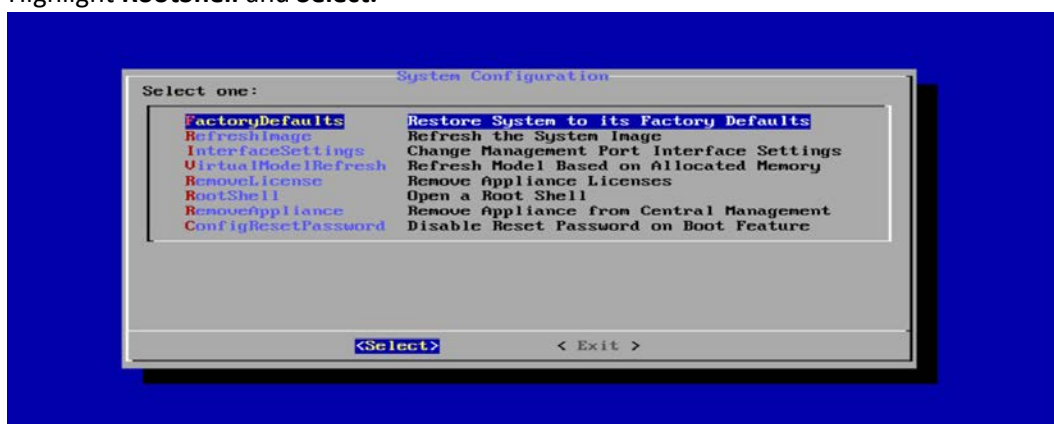
2. Press **Enter**.
3. Enter the original password.



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.

Type the root password at the prompt to open a root shell.

```
Password:  
snc-01:~#
```

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

Type the root password at the prompt to open a root shell.

```
Password:  
snc-01:~# passwd root  
New password:  
Retype new password:  
passwd: password updated successfully  
snc-01:~#
```


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**.

The screenshot shows the 'StealthWatch Management Console VE' Appliance Setup interface. The top left displays system information: 'Serial Number: SMCVE-VMware-4232d9d8e1b32e14-e810b21f42a1f570', 'Version: 7.0.0', and 'Build: 2018.12.12.1645-0'. The top right features the 'STEALTH WATCH' logo. A vertical sidebar on the left lists the setup steps: Step 1 (Change Default Passwords, highlighted in orange), Step 2 (Management Network Interface), Step 3 (Host Name and Domains), Step 4 (DNS Settings), Step 5 (NTP Settings), and a Review section. The main area is titled 'Change Default Passwords'. It includes a 'Password Format (Case Sensitive)' section with requirements: 'Must be between 8 and 30 characters' and 'Must be different from the previous password by at least 4 characters'. A green note states: 'Note: You must change the password for all the users before continuing.' Below this, a dropdown menu shows 'ADMIN' selected. Three password fields are present: 'Current Password' (containing 'current.admin.password'), 'New Password' (containing 'new.admin.password'), and 'Confirm New Password' (containing 'confirm.new.admin.password'). Each field has a 'Required' label to its right. A 'Next' button with a right-pointing arrow is located at the bottom right of the form.

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

StealthWatch Management Console VE
Appliance Setup
Serial Number: SMCVE-VMware-4232d8dbe1b32e14-e810b21f42a1f570
Version: 7.0.0
Build: 2018.12.12.1645-0

Step 2: Management Network Interface

Enable communication between this appliance and the network. Default network settings for this appliance appear below. Before changing any of these settings, confer with your network administrator.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Interface Name: eth0 Interface MAC Address: 00:50:56:b2:64:52

IPv4	IPv6
IP Address: 192.168.1.52	
Subnet Mask: 255.255.255.0	
Default Gateway: 192.168.1.1	
Broadcast Address: 192.168.1.255	

Next →

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**.

StealthWatch Management Console VE
Appliance Setup
Serial Number: SMCVE-VMware-4232d8dbe1b32e14-e810b21f42a1f570
Version: 7.0.0
Build: 2018.12.12.1645-0

Step 3: Host Name and Domains

Enter identifying information for this appliance and the network domain where it is installed.

Warning! If you change your IP address, host name, or network domain name, the appliance identity certificate is replaced automatically. If you have a custom certificate, save the certificate and private key before you change these fields so you don't lose data.

Host Name: smc-01

Network Domain: di.ipdr

Identify your organization's domain and the IP addresses that Stealthwatch will be monitoring.

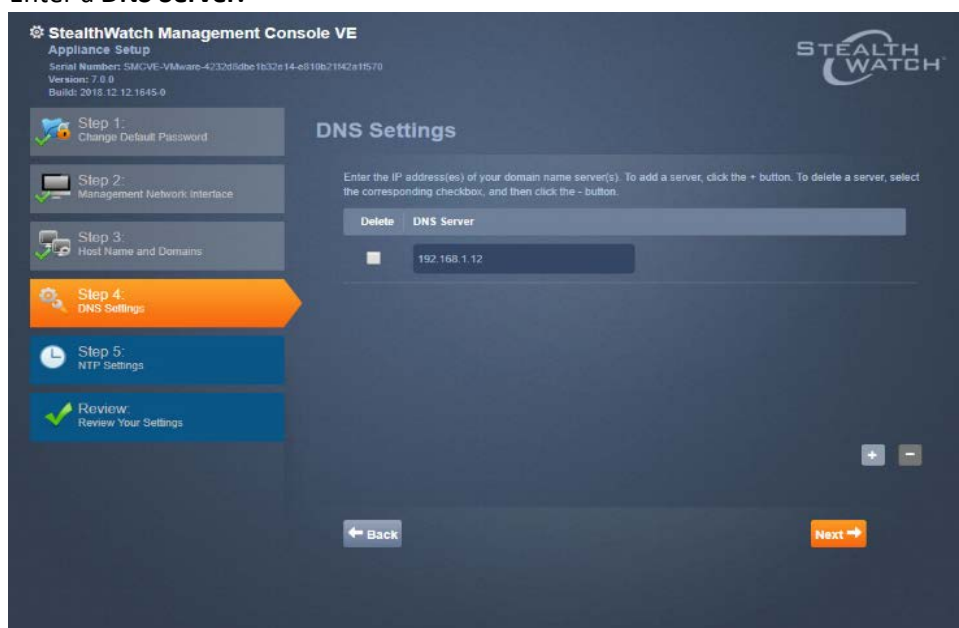
Stealthwatch Domain: di.ipdr

IP Address Ranges:

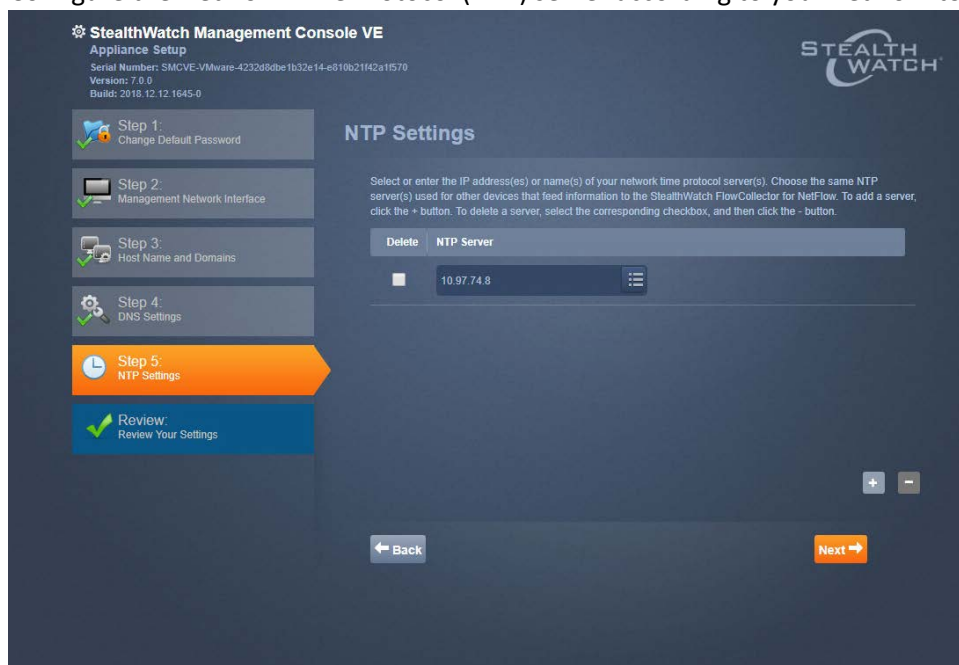
10.0.0.0/8
192.168.0.0/16
172.16.0.0/12
fc00::/7

Back **Next** →

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



10. Click **Next**.
11. Configure the Network Time Protocol (NTP) server according to your network topology.



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



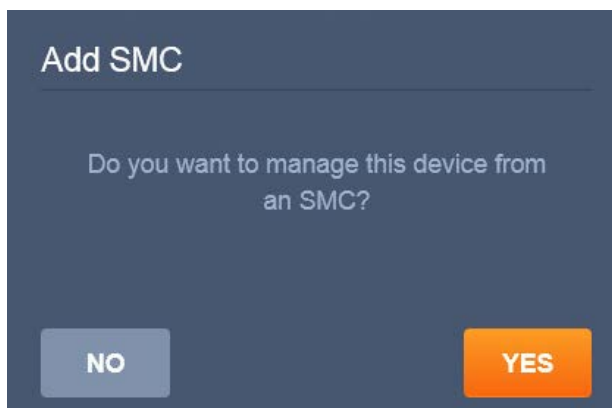
14. Click **Apply**.



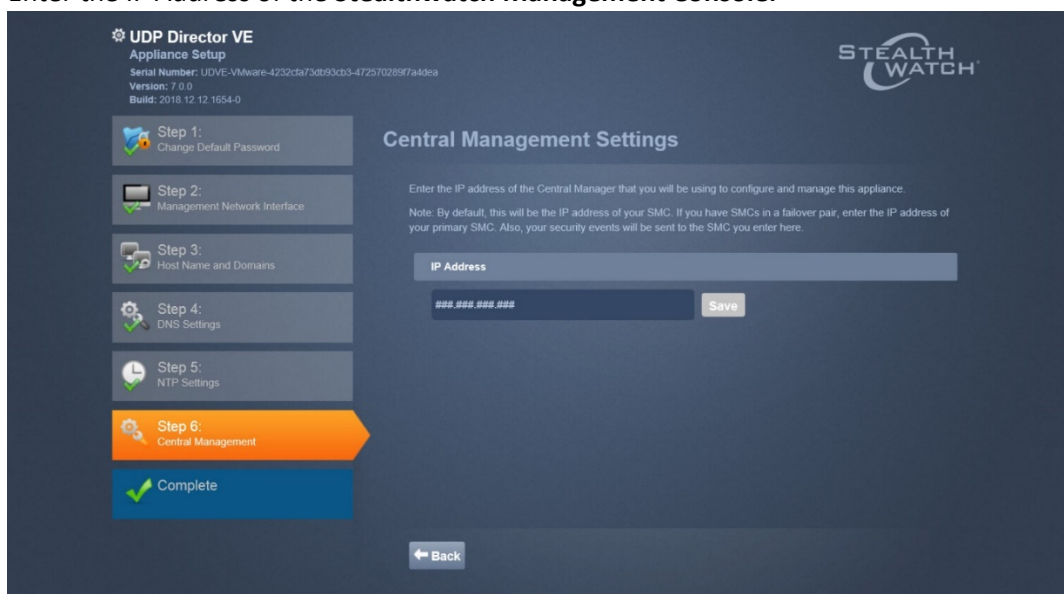
15. After the restart, click **Next**.

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

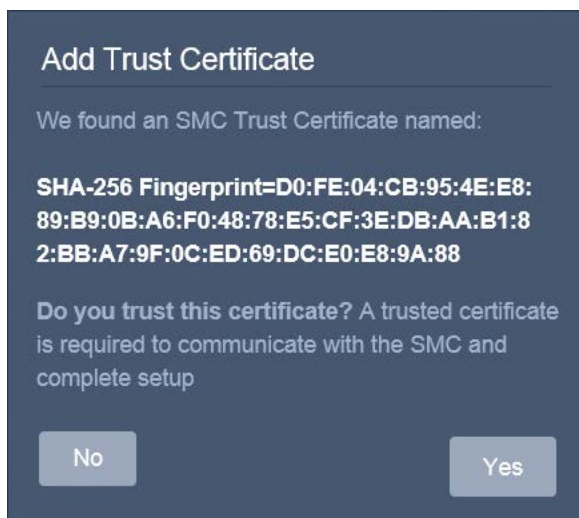
1. Repeat steps 1-12 from *Configure the Stealthwatch Management Console Web Interface*.



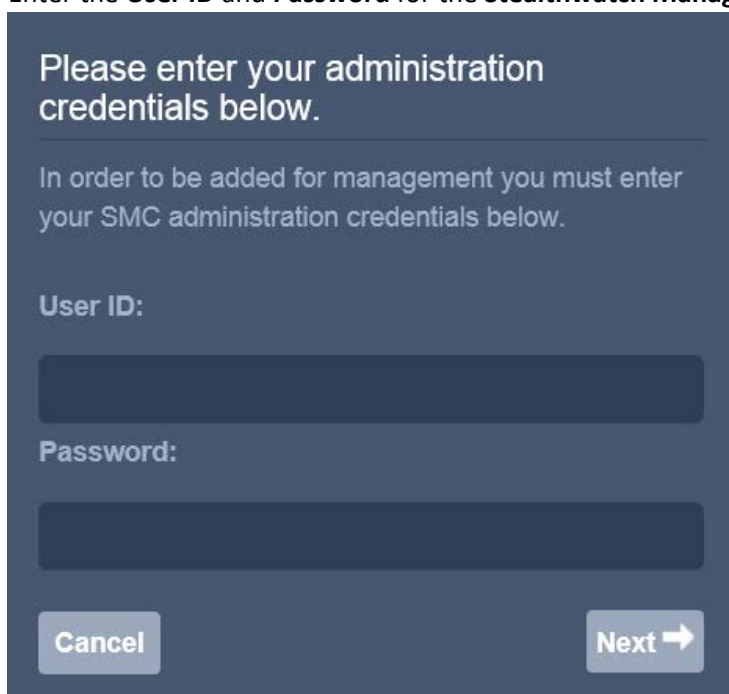
2. When prompted to manage this device from an SMC, click **Yes**.
3. Enter the IP Address of the **Stealthwatch Management Console**.



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
```

```
COM2 - PuTTY
ether 00:e0:ed:7a:82:1d txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe00000-fbe1ffff

eth2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 00:e0:ed:7a:82:1c txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe20000-fbe3ffff

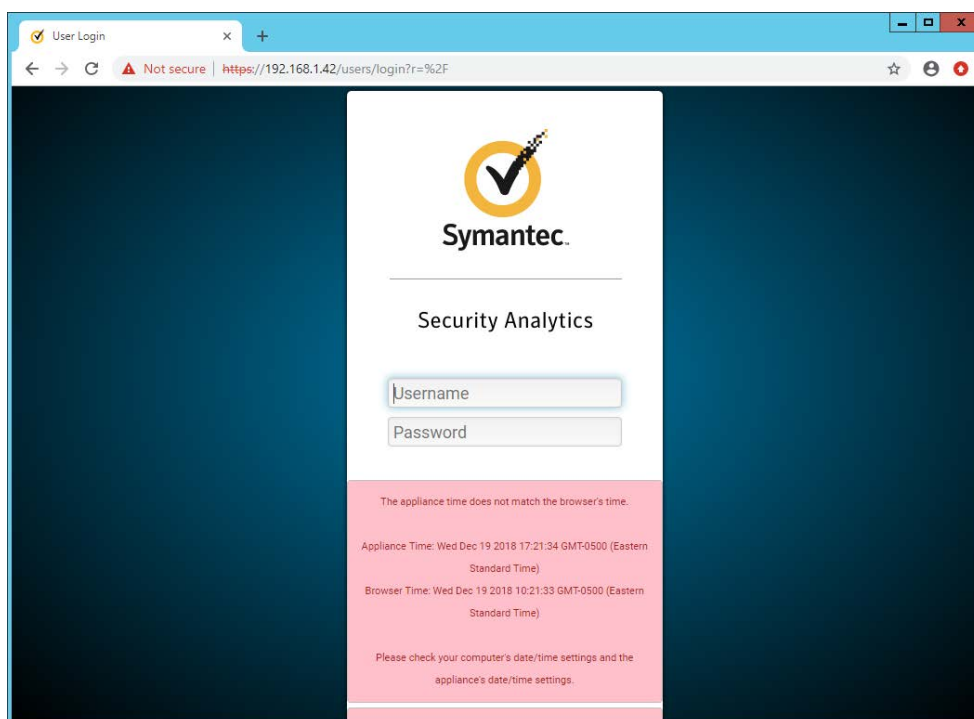
eth3: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 00:e0:ed:7a:82:1b txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe40000-fbe5ffff

eth4: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 00:e0:ed:7a:82:1a txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe60000-fbe7ffff

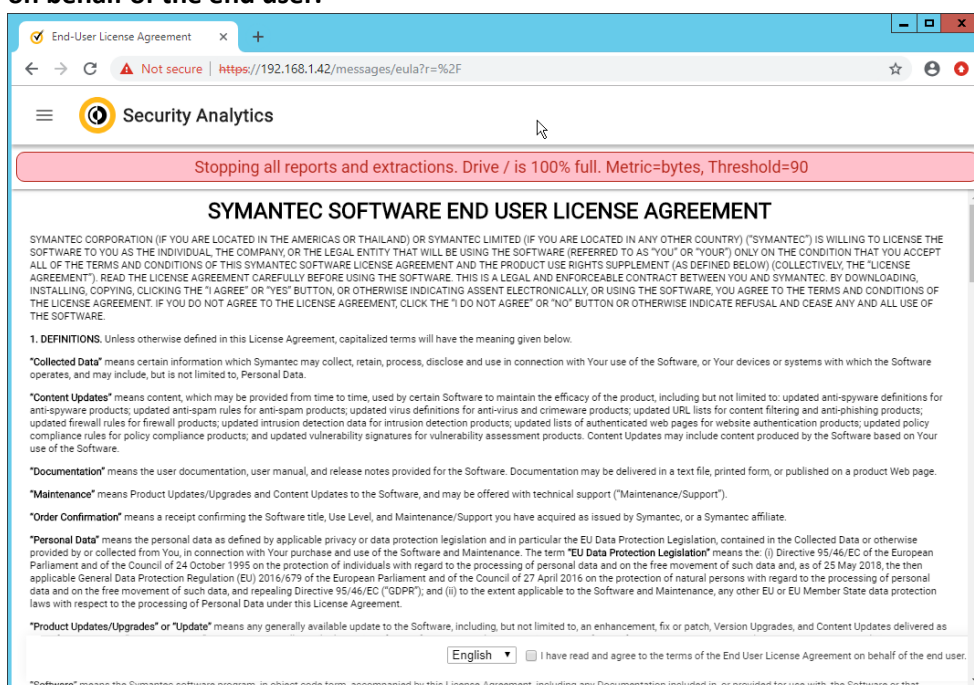
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
RX packets 1165 bytes 428654 (418.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1165 bytes 428654 (418.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@DS2B7A ~]# cfg_bond_interface.py -i eth0 192.168.1.42/255.255.255.0 -g 192.168.1.1
[root@DS2B7A ~]# sudo cfg_bond_interface.py -i eth0 -n 192.168.1.42/255.255.255.0 -g 192.168.1.1
```

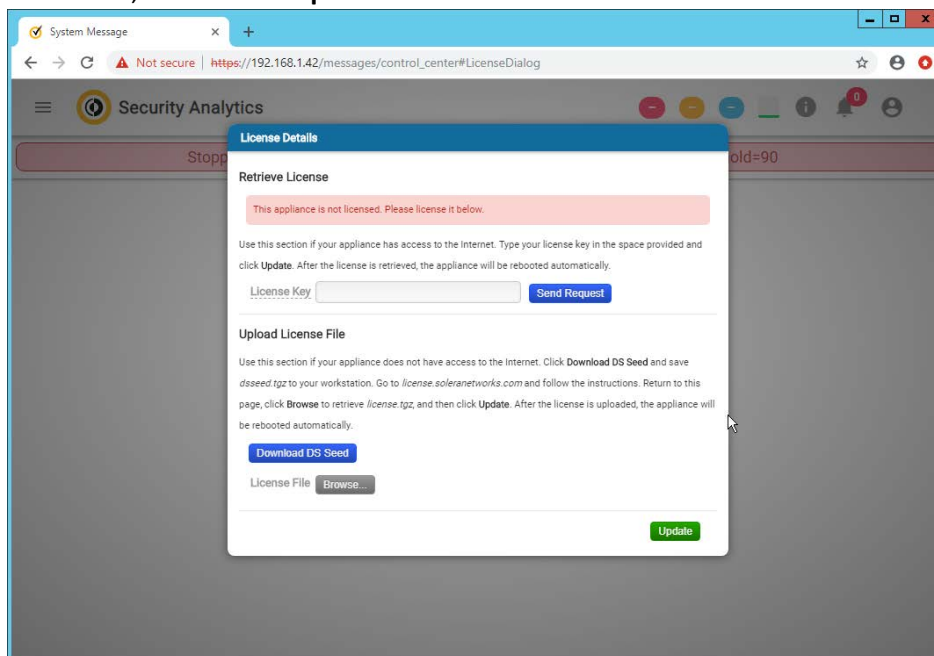
3. Navigate to the IP you assigned in a browser.



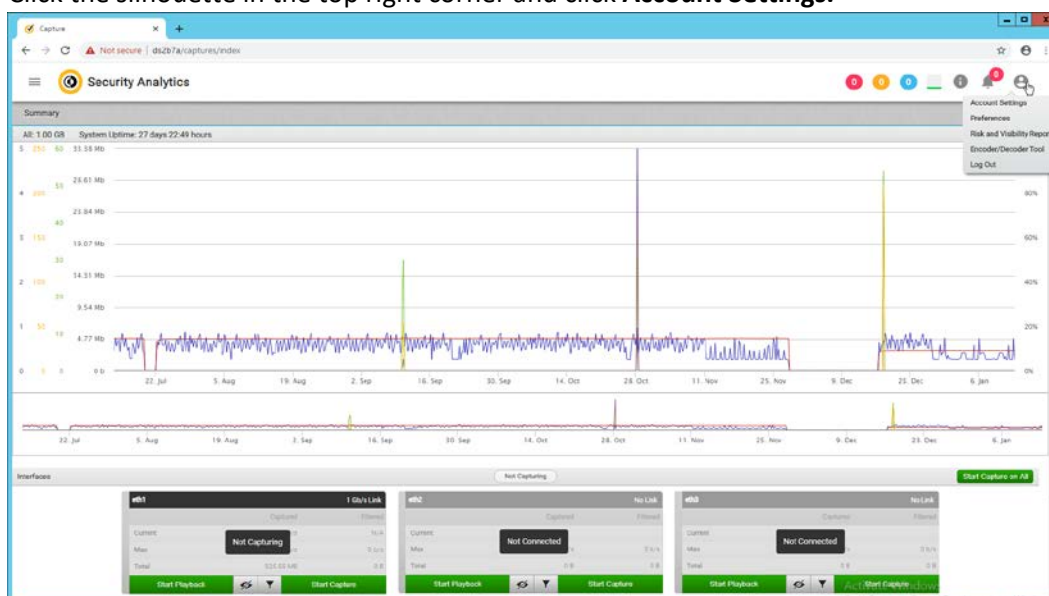
4. Enter the username and password to log in. The default is **(Admin/Solera)**.
5. Check the box next to **I have read and agreed to the terms of the End User License Agreement on behalf of the end user.**



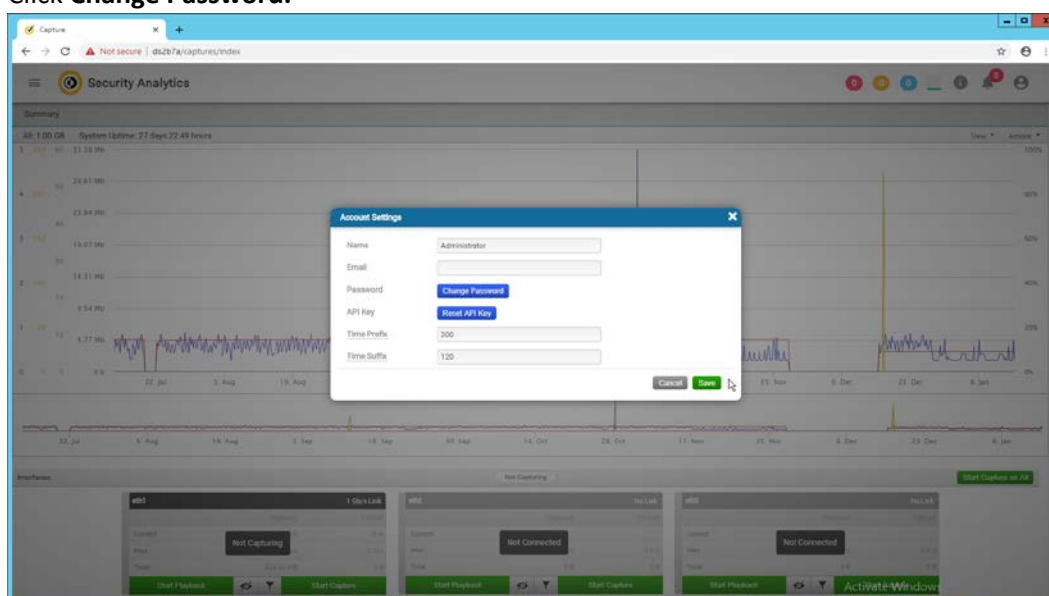
6. Click **Next**.
7. Enter the license key.
8. If you do not have internet connectivity, follow the instructions under **Upload License File**. Otherwise, click **Send Request**.



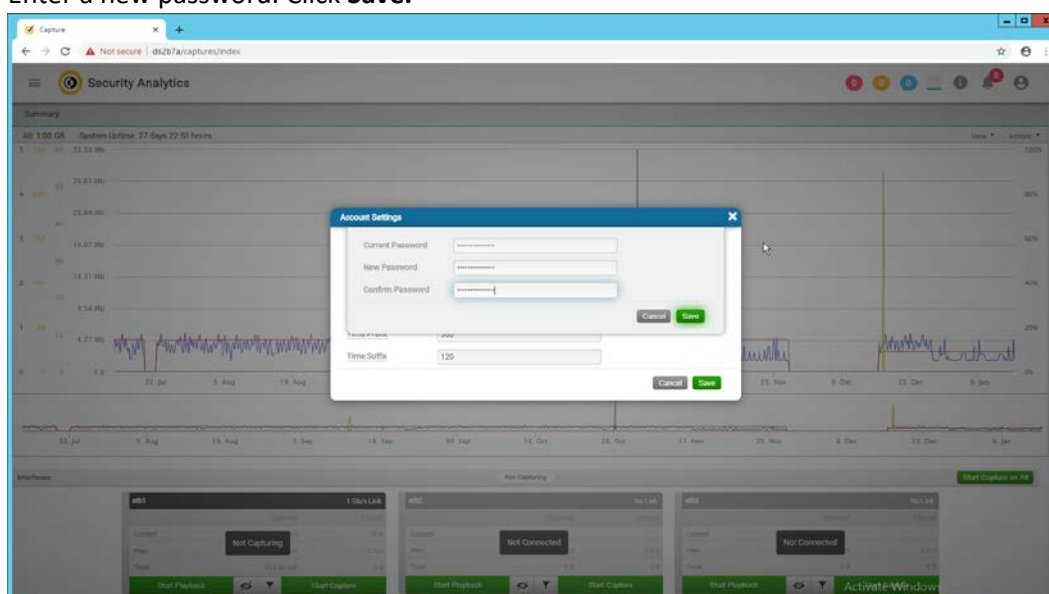
9. Click **Update**. The device will reboot.
10. Log in to the web page again.
11. Click the silhouette in the top right corner and click **Account Settings**.



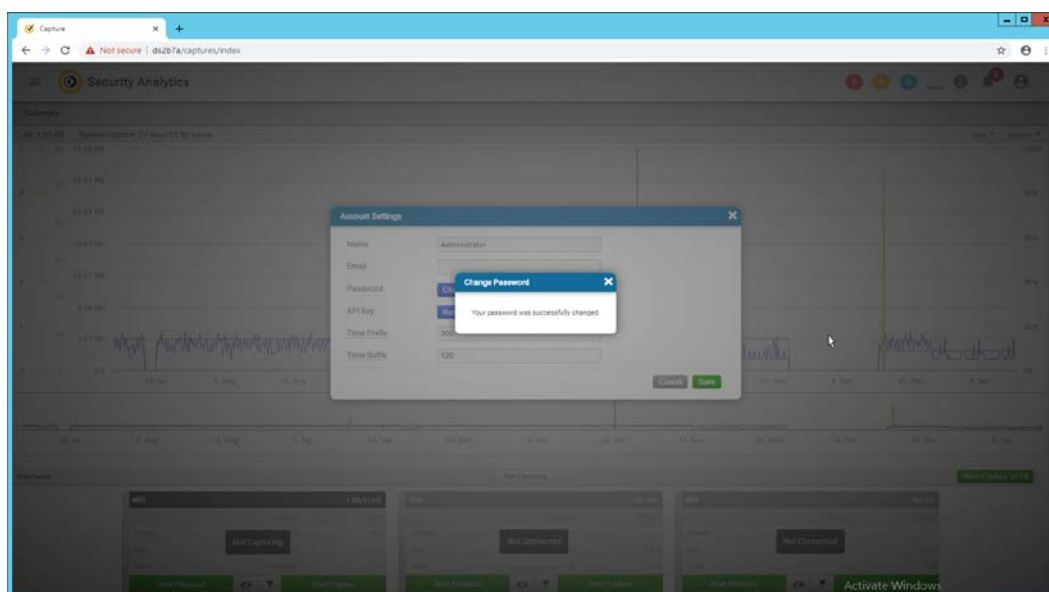
12. Click **Change Password**.



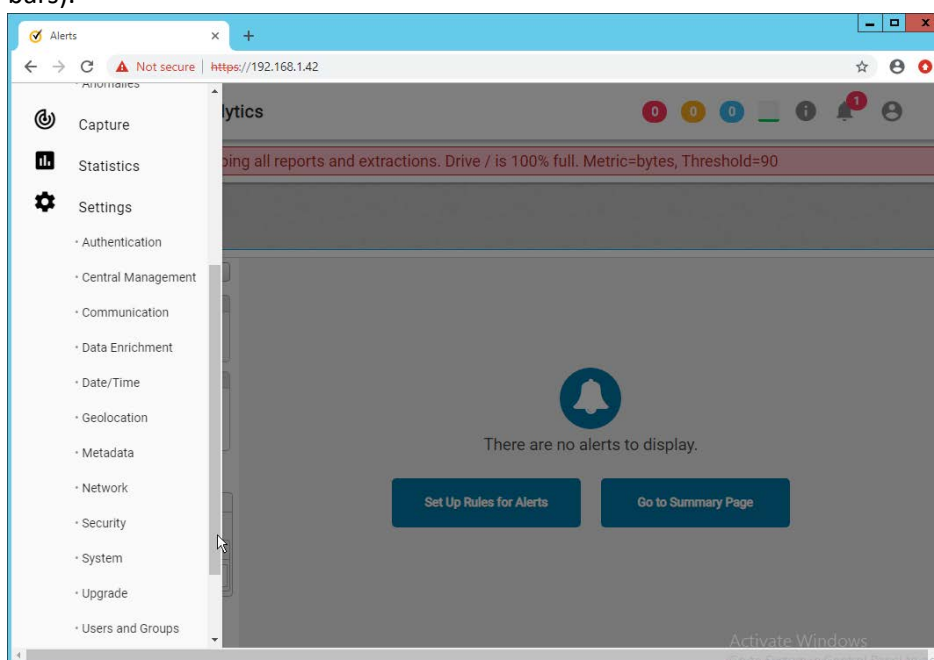
13. Enter a new password. Click **Save**.



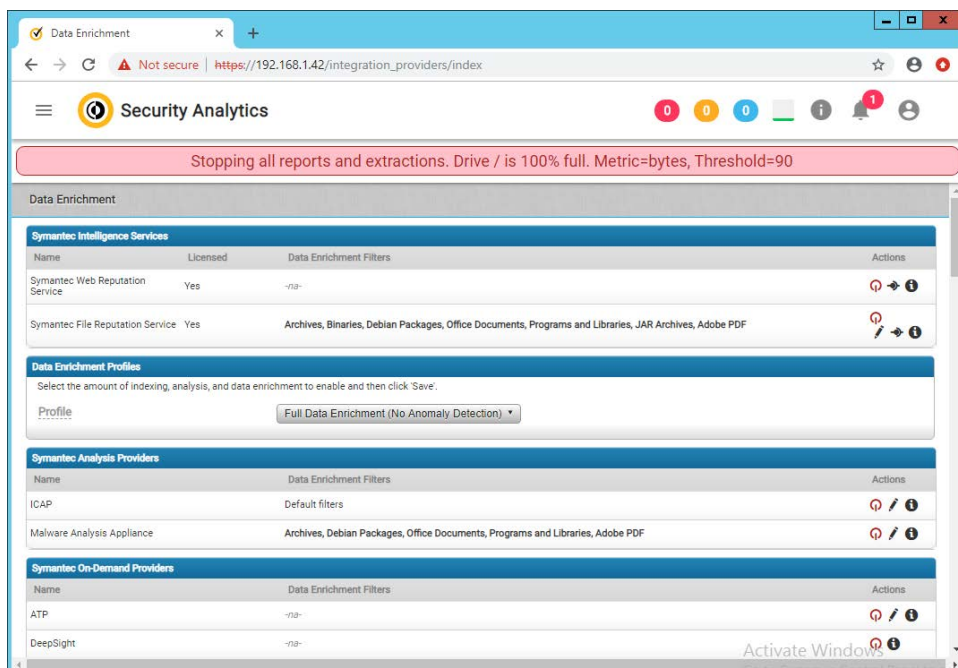
14. The screen should reflect that the password has been changed. Close out of both windows and return to the main web console.



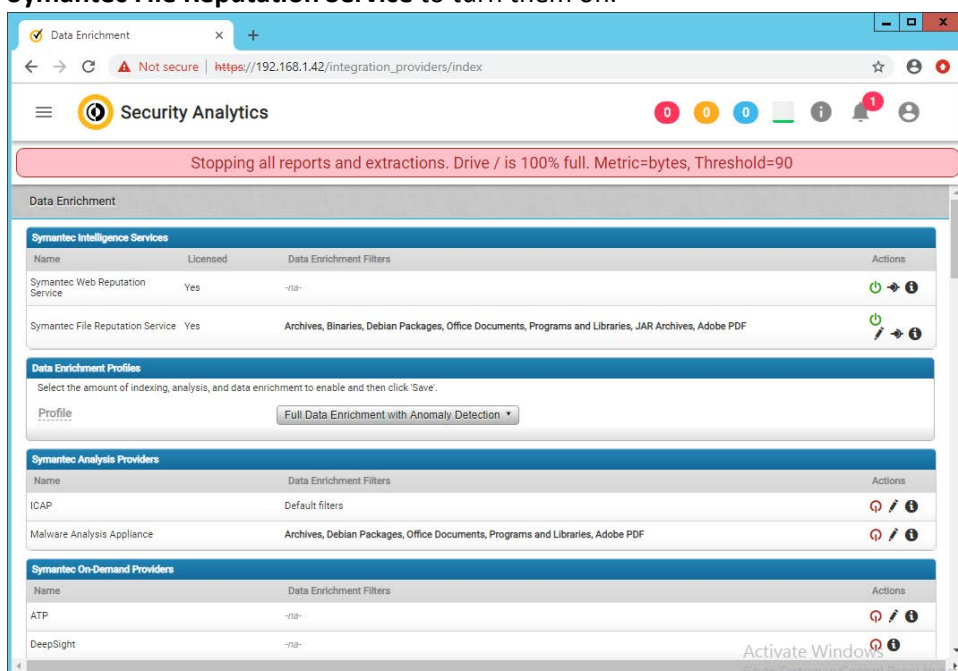
15. In the top left corner of the web console, click the menu button. (It shows as three horizontal bars).



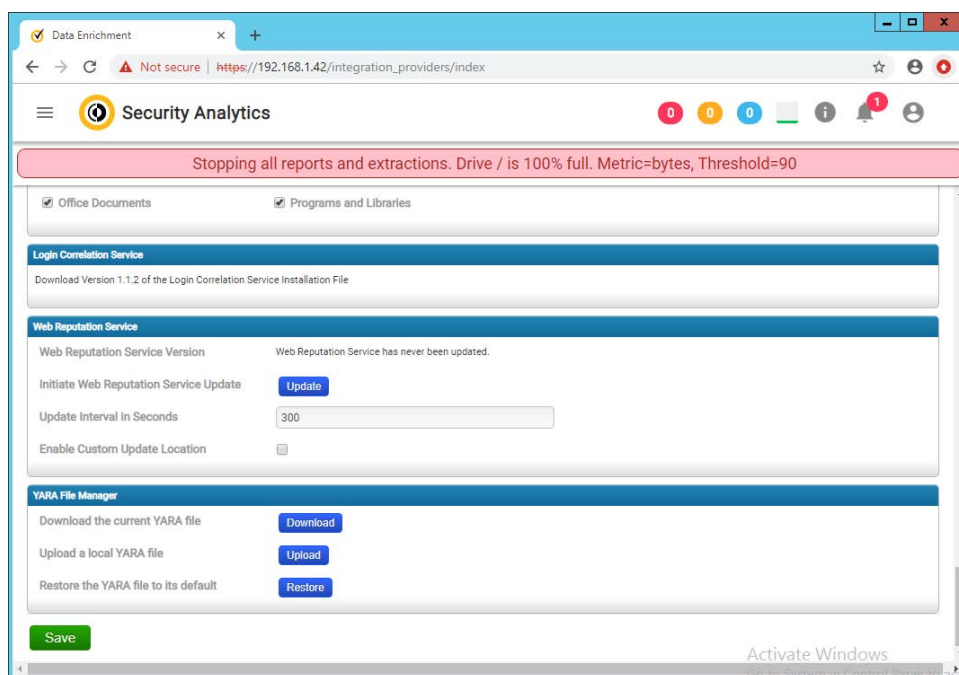
16. Navigate to **Settings > Data Enrichment**.



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



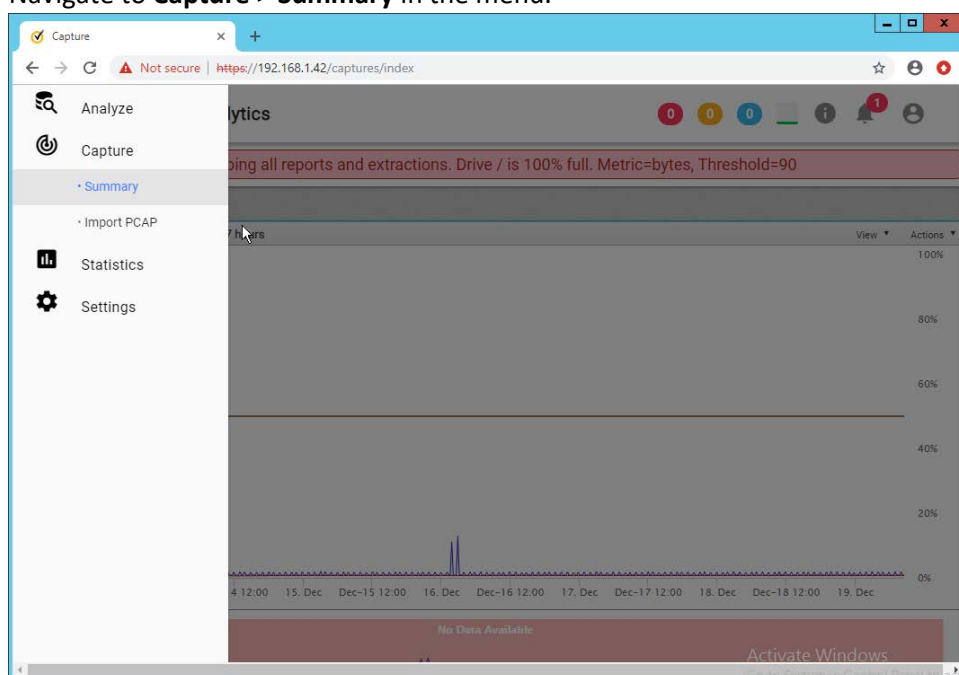
18. Select **Full Data Enrichment (with Anomaly Protection)** for the profile under **Data Enrichment Profiles**.



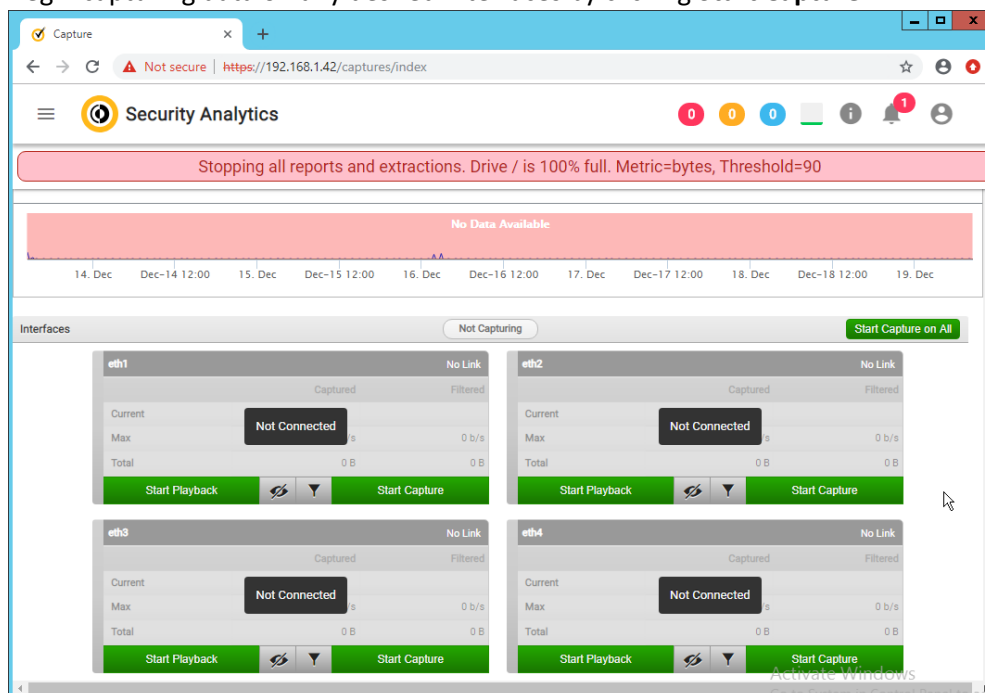
19. Click **Save**.

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**.

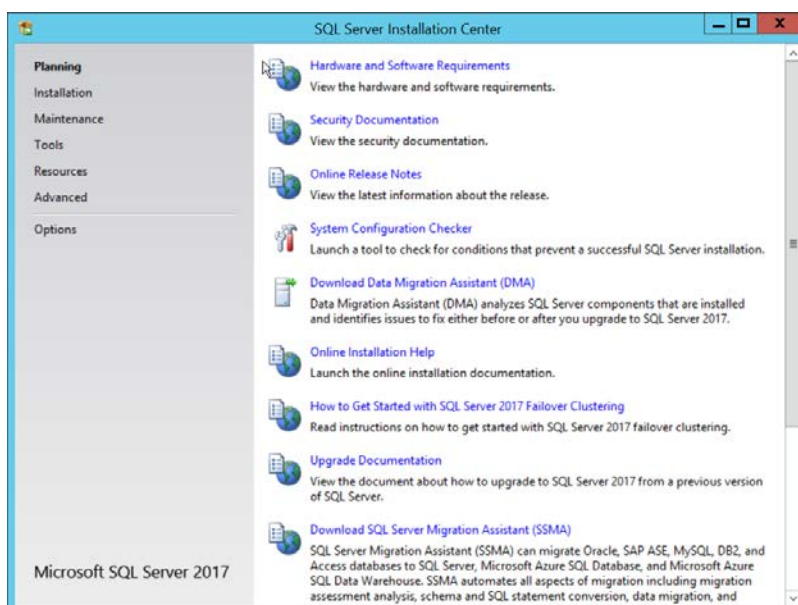


2.15 Symantec Information Centric Analytics

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

2.15.1 Installing MS SQL 2017

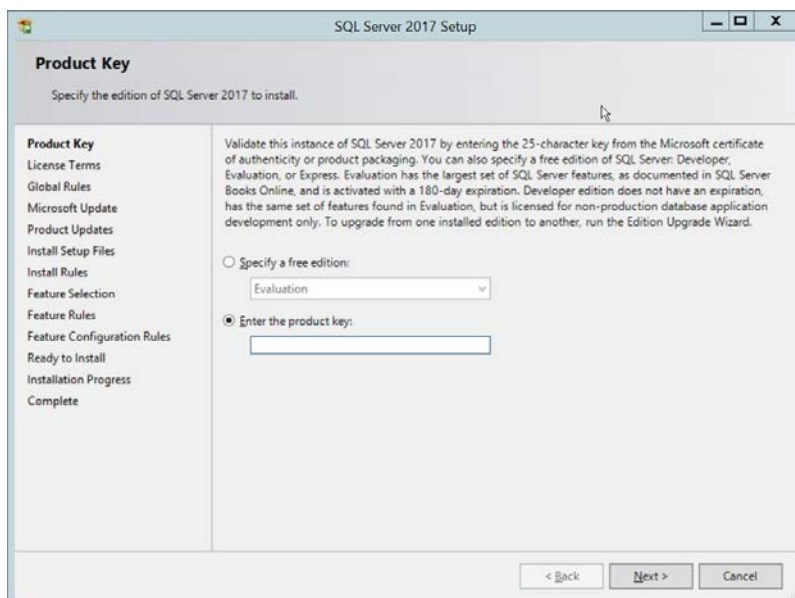
1. Launch the SQL Setup Wizard.



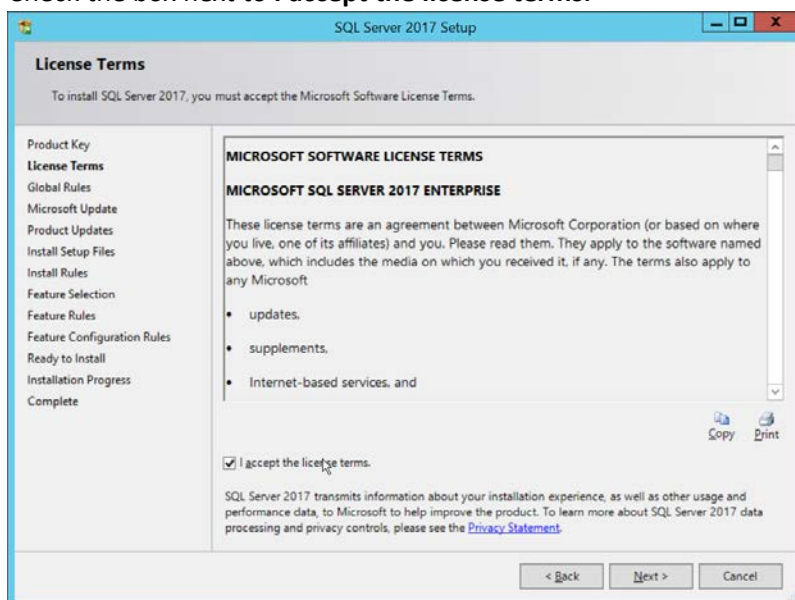
2. Click **Installation**.



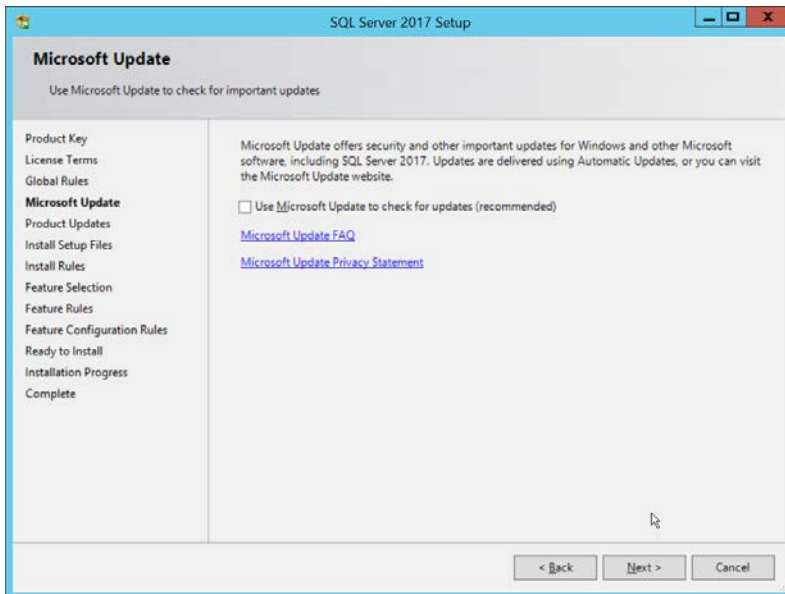
3. Click **New SQL Server stand-alone installation or add features to an existing installation**.
4. Enter a **product key**.



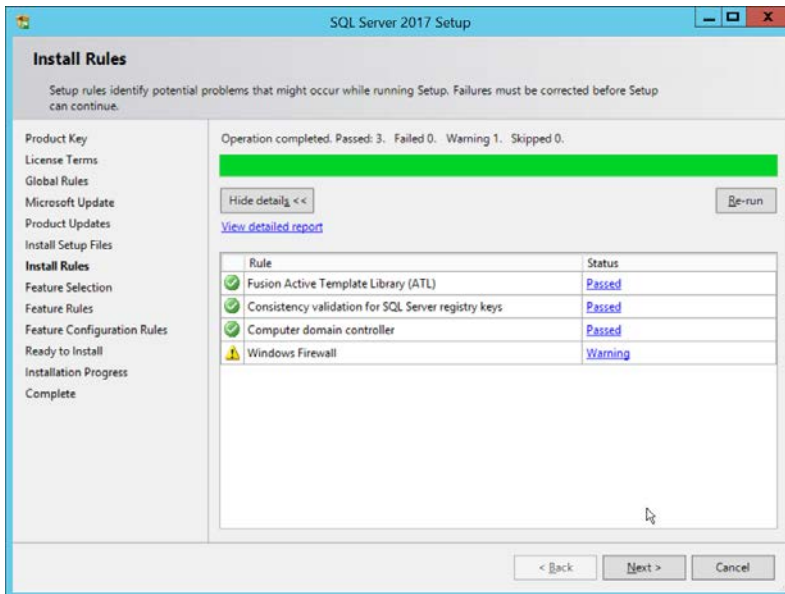
5. Click **Next**.
6. Check the box next to **I accept the license terms**.



7. Click **Next**.

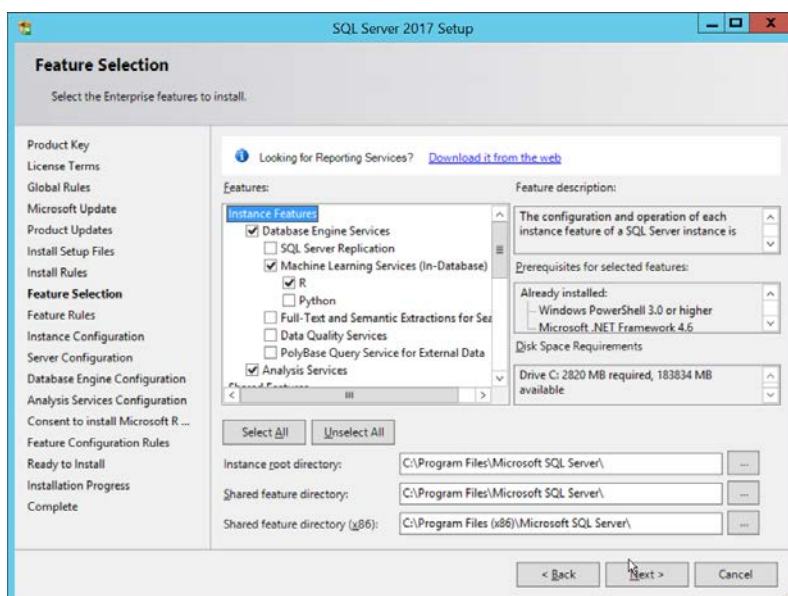


8. Click **Next**.

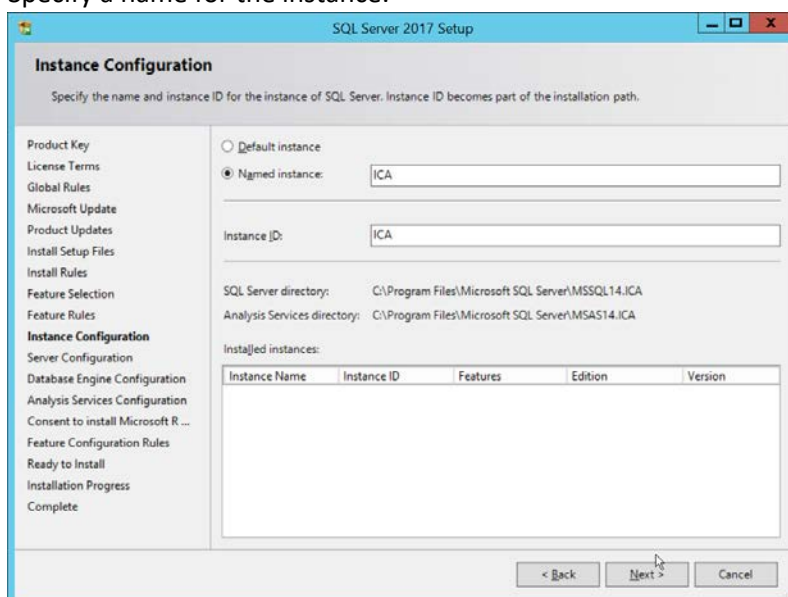


9. Click **Next**.

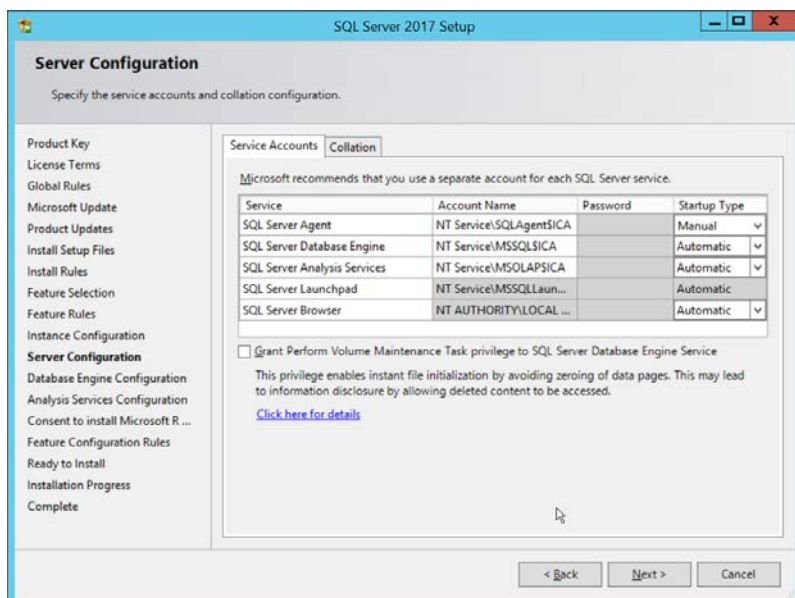
10. Ensure that box next to **R** and the box next to **Analysis Services** is checked.



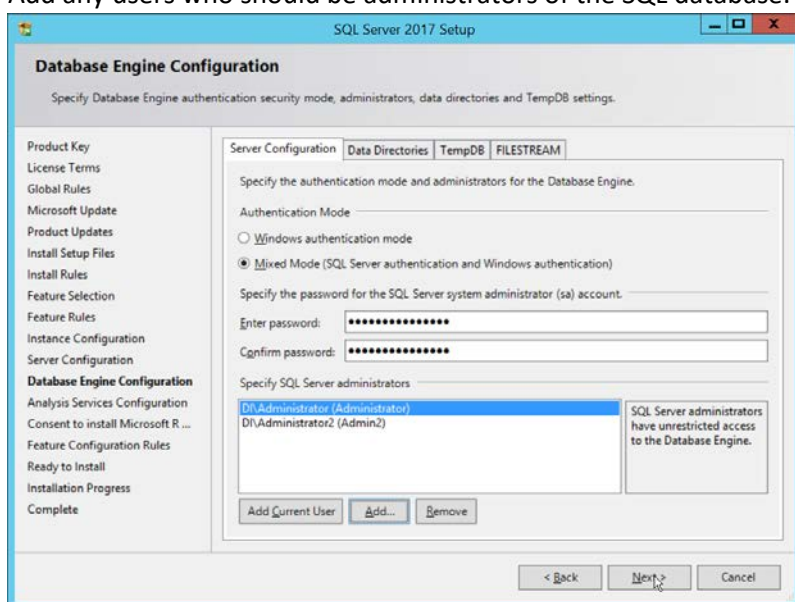
11. Click **Next**.
12. Select **Named instance**.
13. Specify a name for the instance.



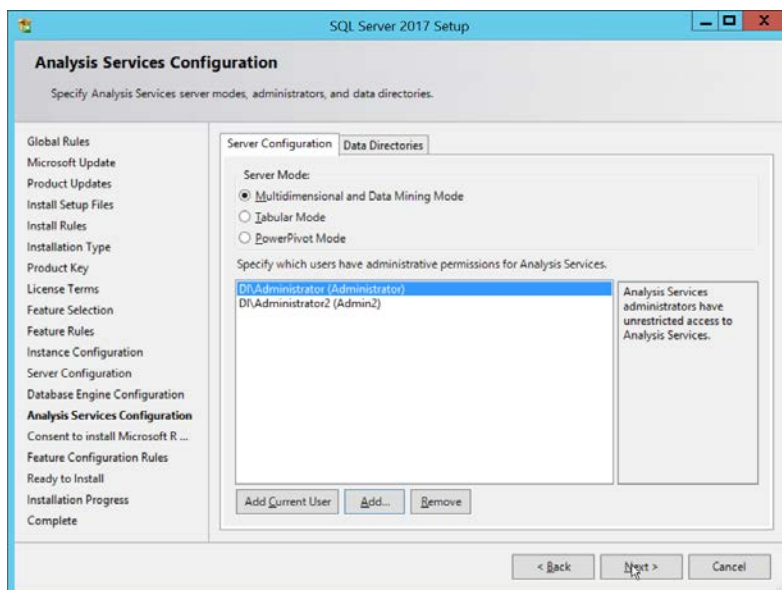
14. Click **Next**.



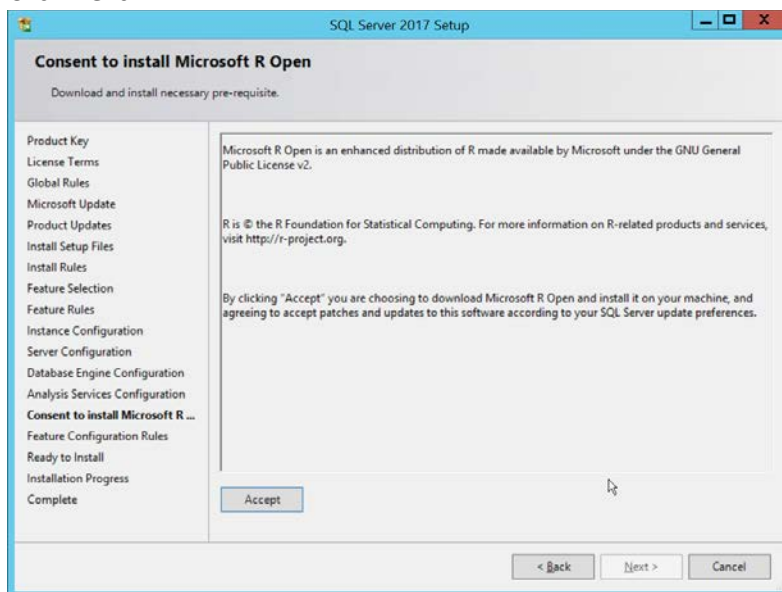
15. Click **Next**.
16. Select **Mixed Mode (SQL Server authentication and Windows authentication)**.
17. Enter a **password**.
18. Add any users who should be administrators of the SQL database.



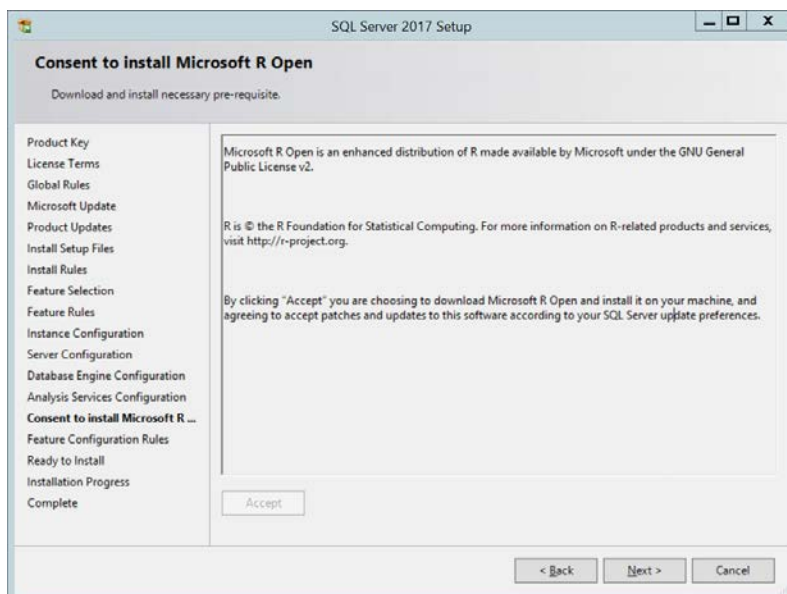
19. Click **Next**.
20. Select **Multidimensional and Data Mining Mode**.
21. Add any users who should be administrators of the Analysis Services.



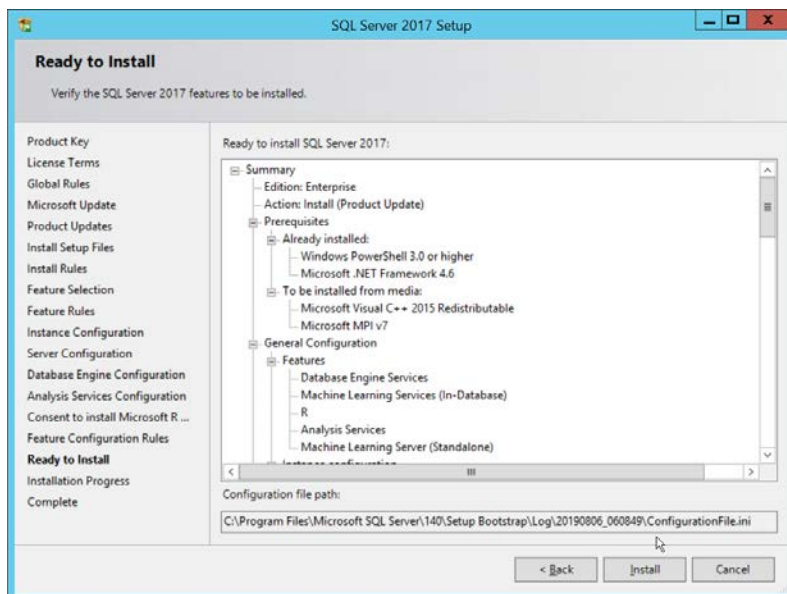
22. Click **Next**.



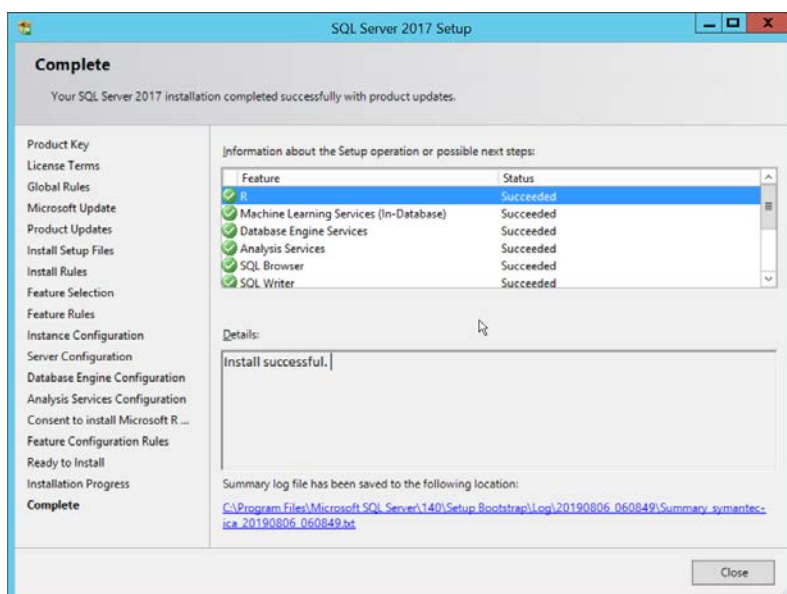
23. Click **Accept**.



24. Click **Next**.



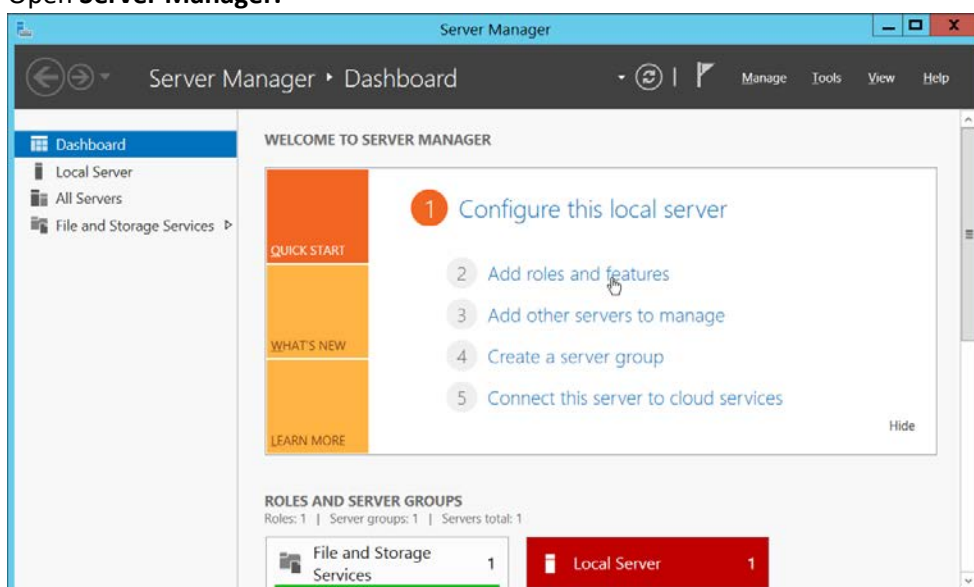
25. Click **Install**.



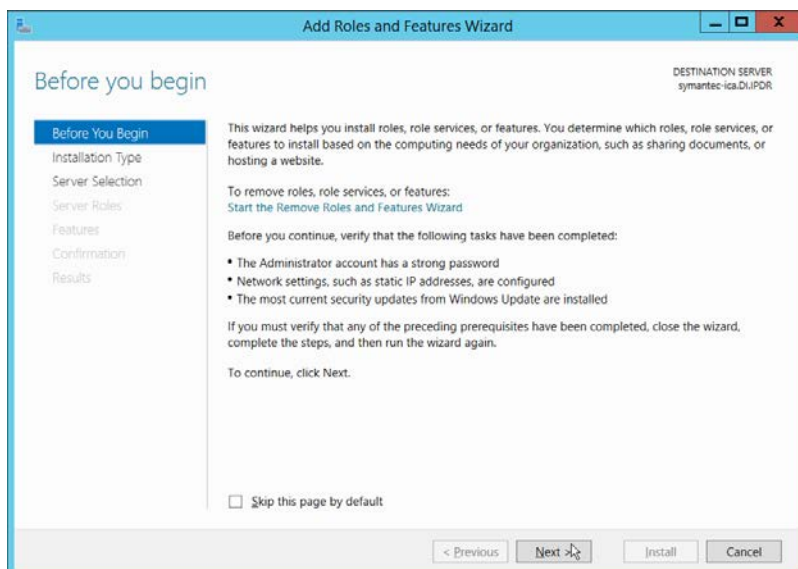
26. Click **Close**.

2.15.2 Install Windows Services

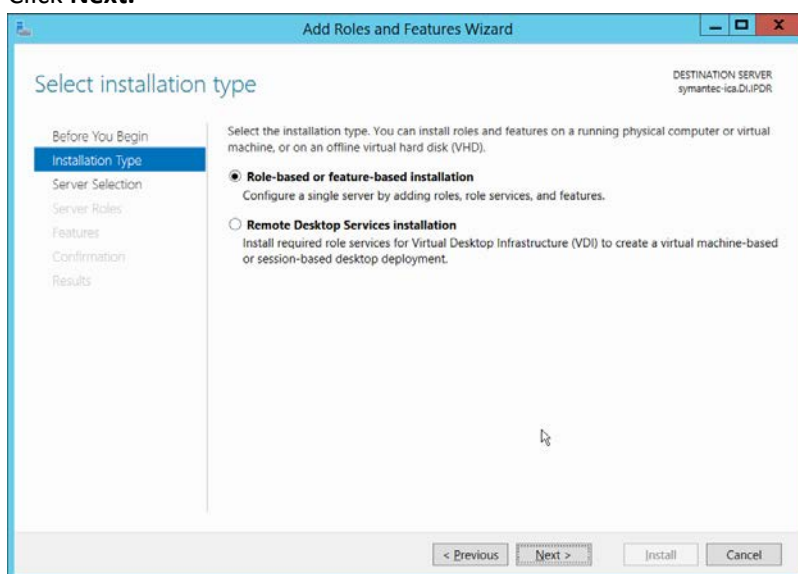
1. Open **Server Manager**.



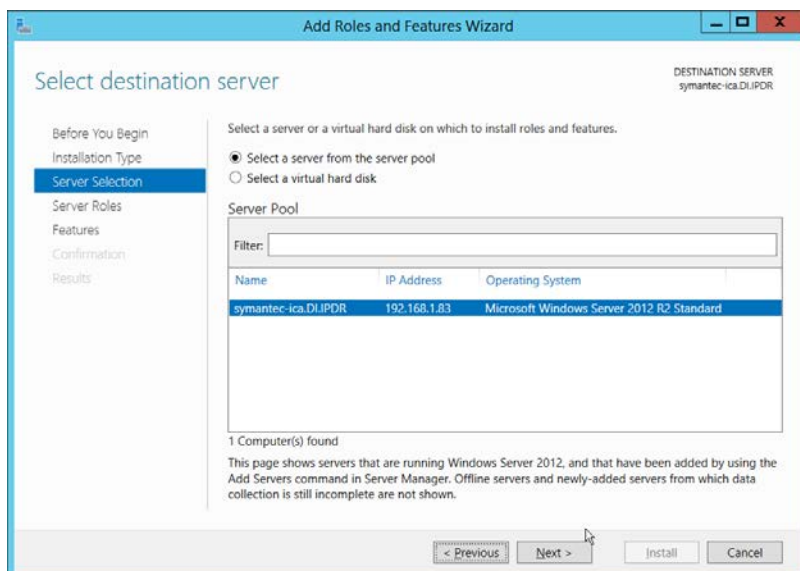
2. Click **Add Roles and Features**.



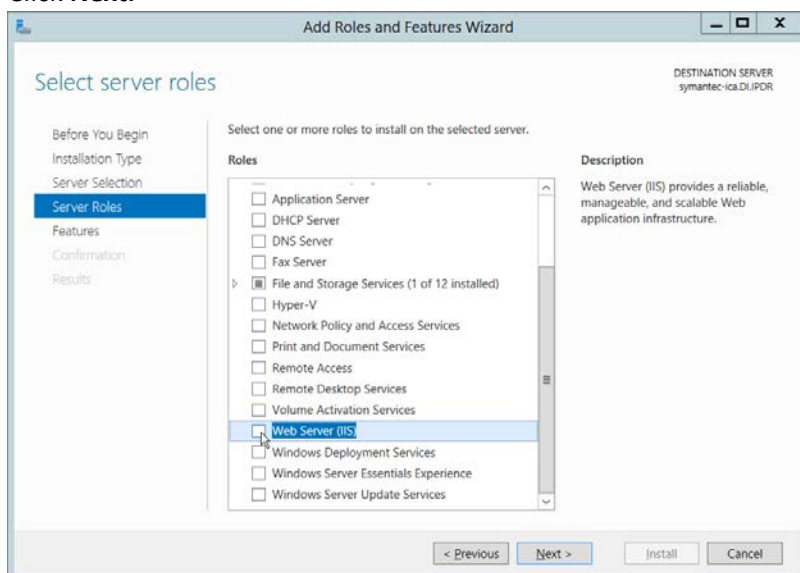
3. Click **Next**.



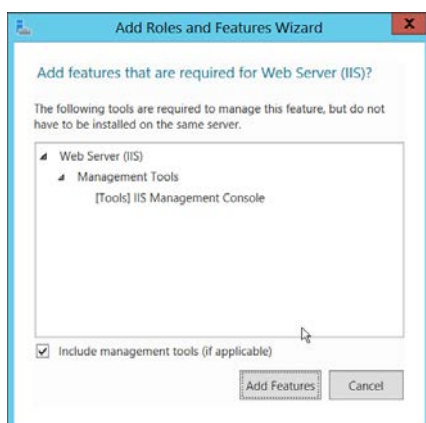
4. Click **Next**.



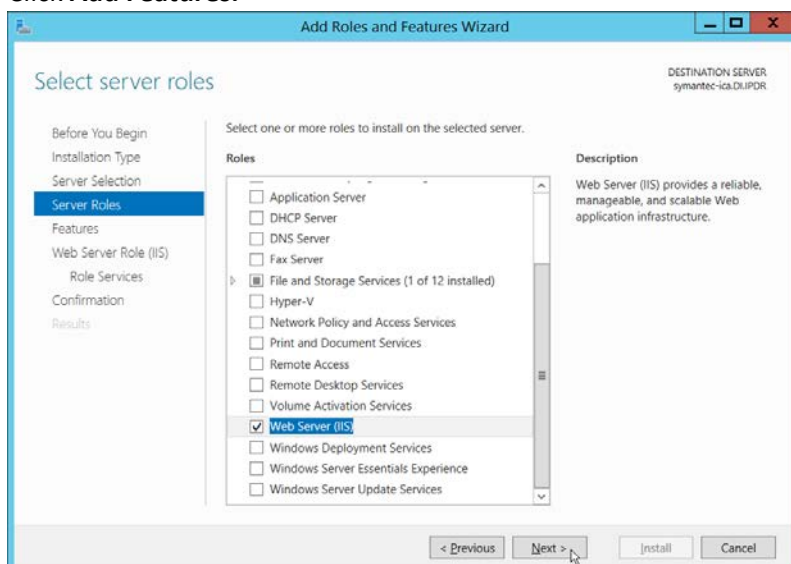
5. Click **Next**.



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



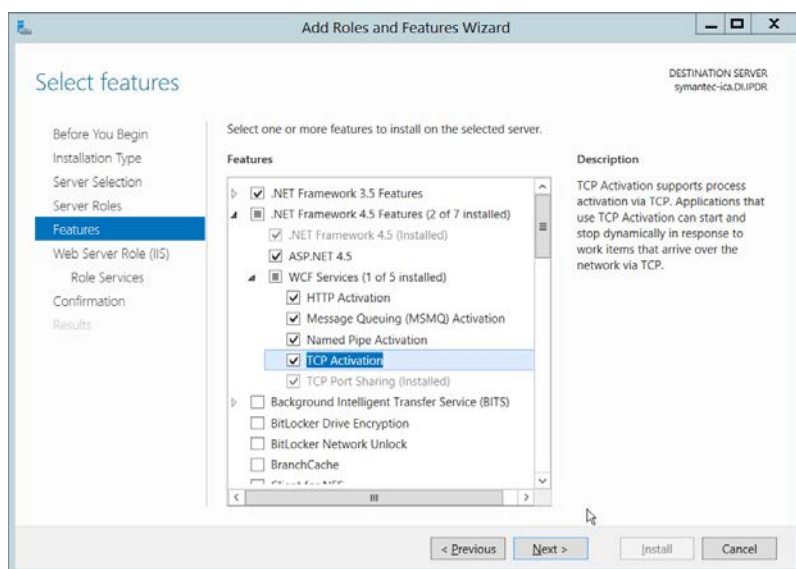
7. Click **Add Features**.



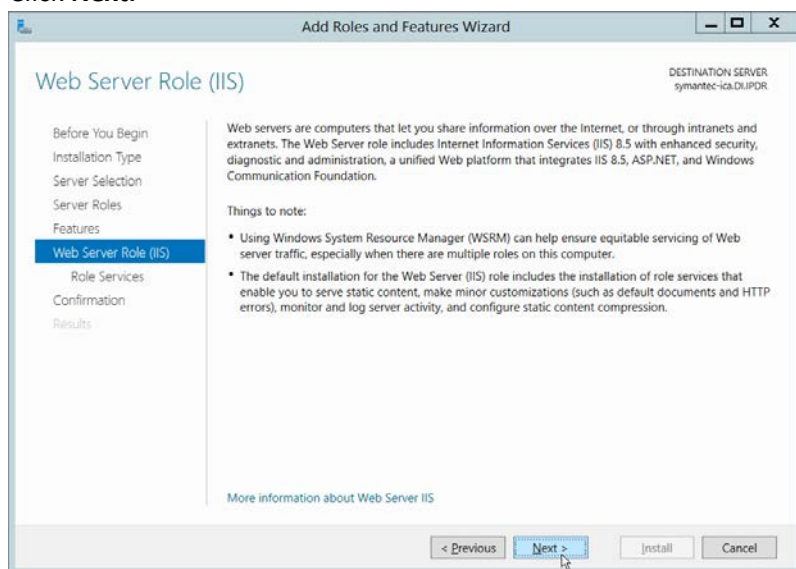
8. Click **Next**.

9. Select all services under **.NET Framework 3.5 Features**.

10. Select all services under **.NET Framework 4.5 Features**.



11. Click **Next**.

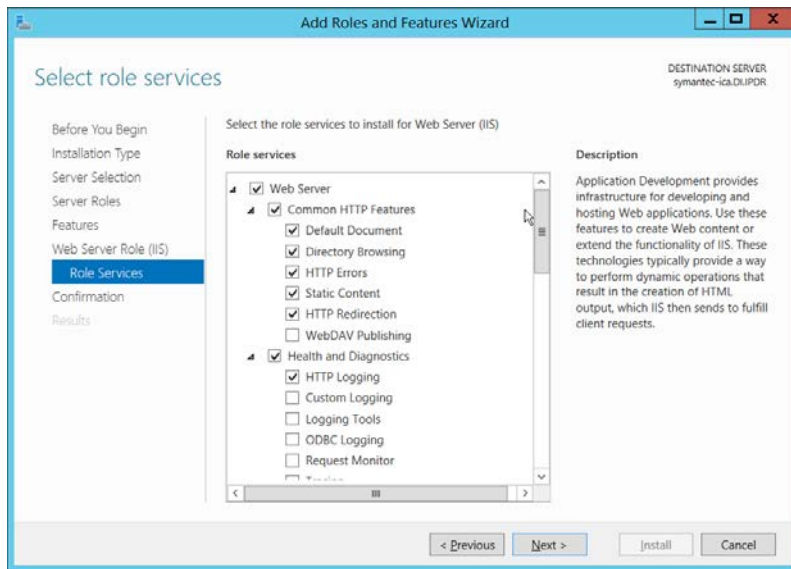


12. Click **Next**.

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**

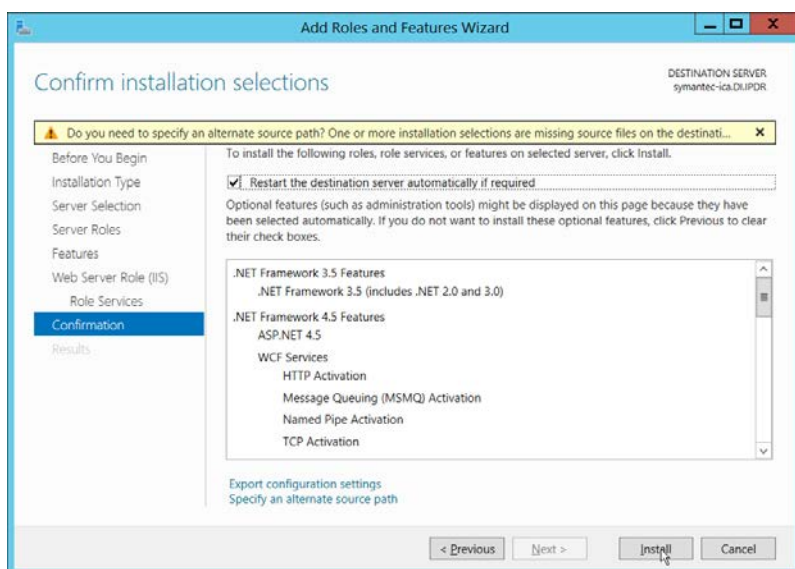
- i. **Static Content Compression**
- d. **Security**
 - i. **Windows Authentication**
- e. **Application Development**
 - i. **.NET Extensibility 4.5**
 - ii. **ASP.NET 4.5**
 - iii. **ISAPI Extensions**
 - iv. **ISAPI Filters**



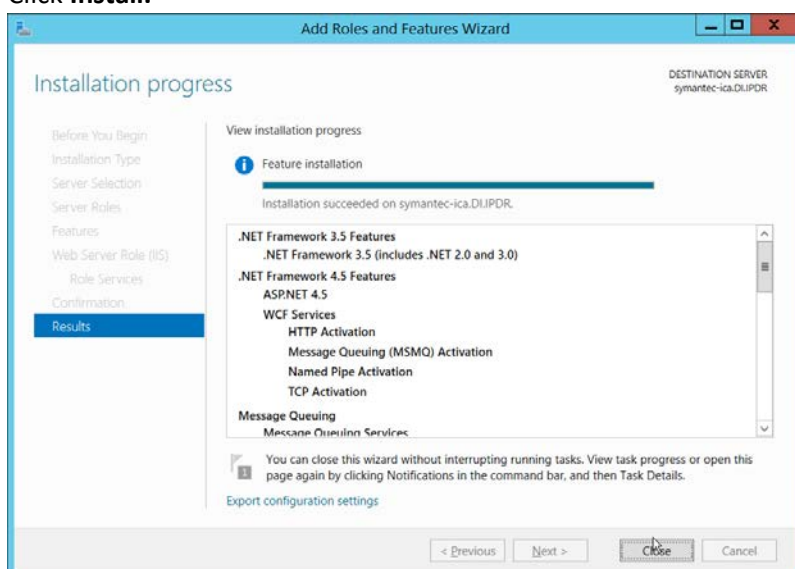
14. Click **Next**.

15. If necessary, specify a path to **/Sources/SxS**, which is found in the Windows Installation Media.

16. Check the box next to **Restart the destination server automatically if required**.

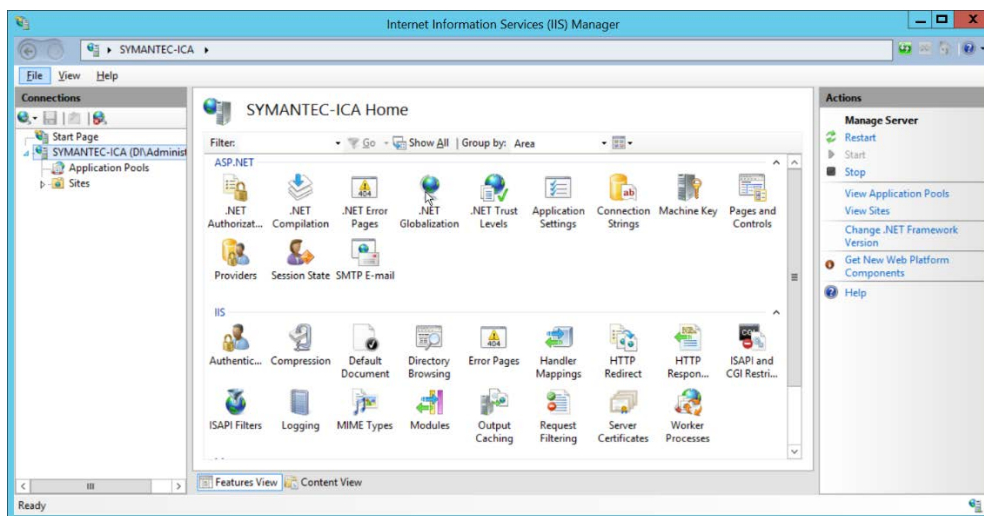


17. Click **Install**.

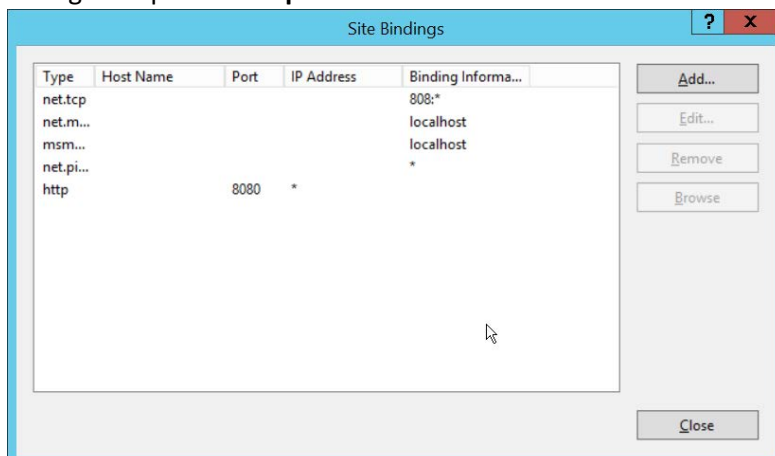


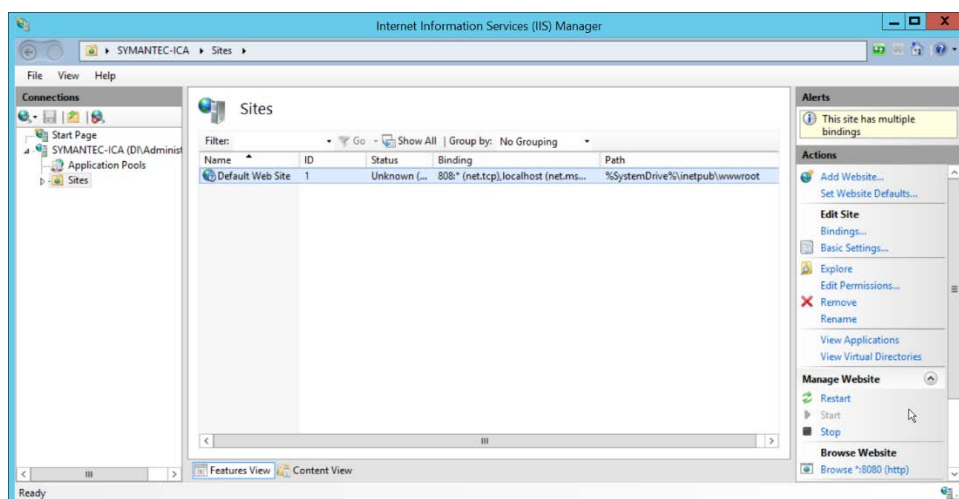
18. Click **Close** when the installation finishes.

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**.

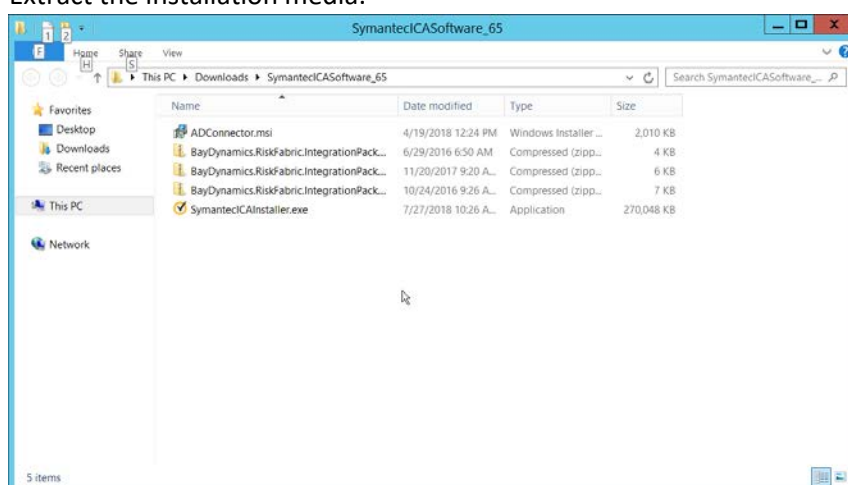




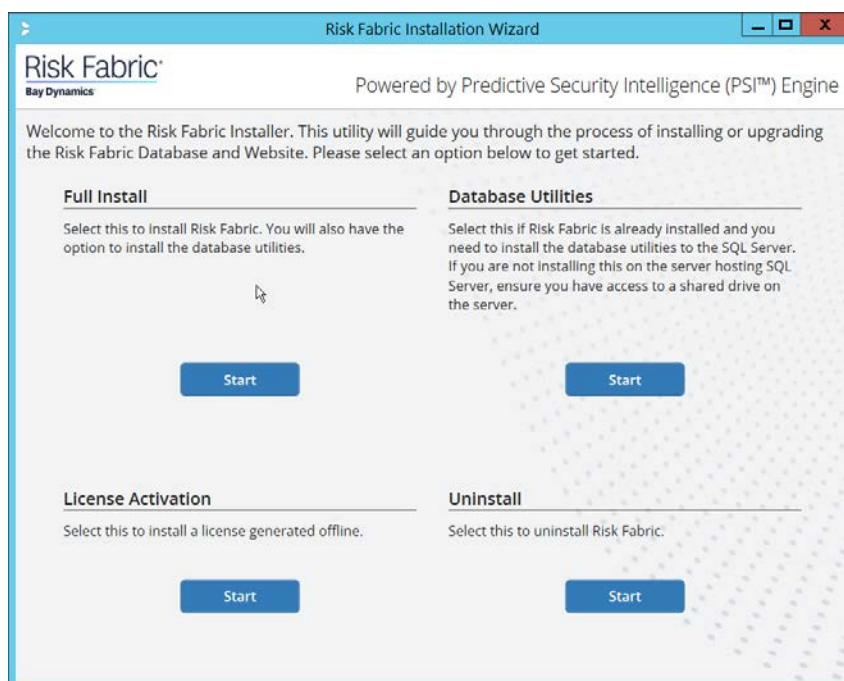
24. Click **Restart** under **Manage Website**.

2.15.3 Installing Symantec ICA

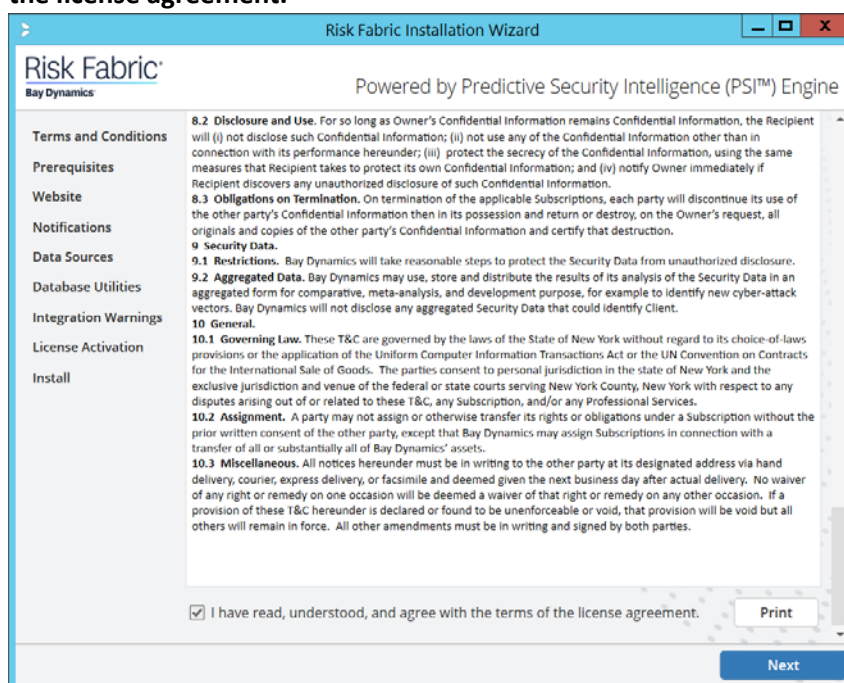
1. In Task Manager, verify that the **SQL Server Agent** service is running.
2. Copy the installation media **SymantecICASoftware_65.zip** onto the server.
3. Extract the installation media.



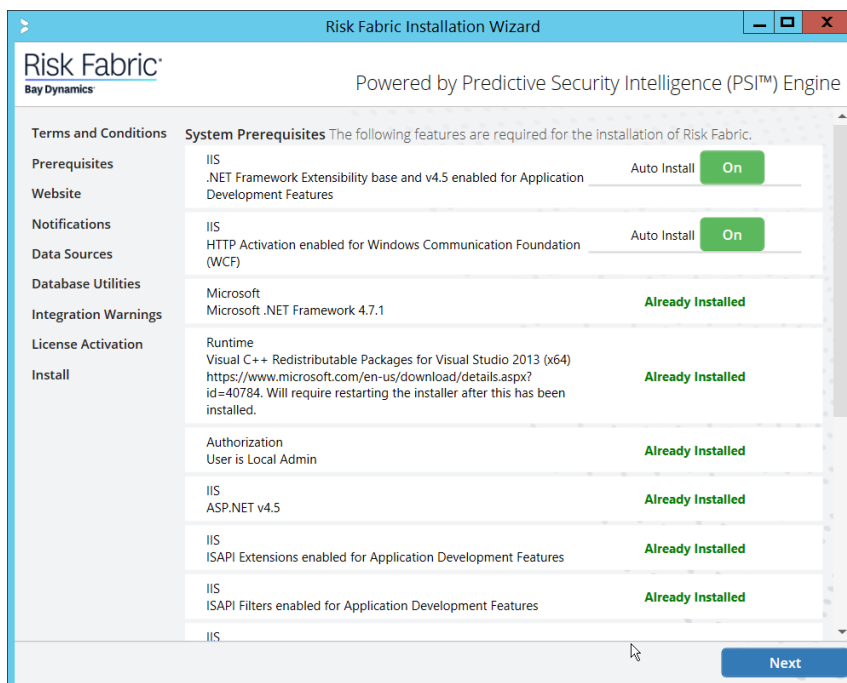
4. Run **SymantecICAInstaller.exe**.



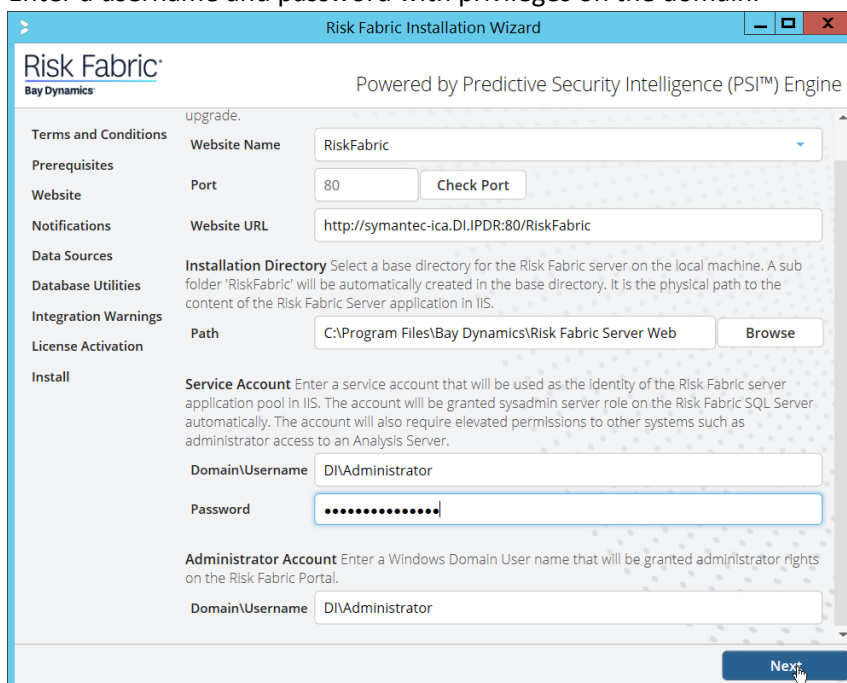
5. Under **Full Install**, click **Start**.
6. Scroll down and check the box next to **I have read, understood, and agree with the terms of the license agreement**.



7. Click **Next**.



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

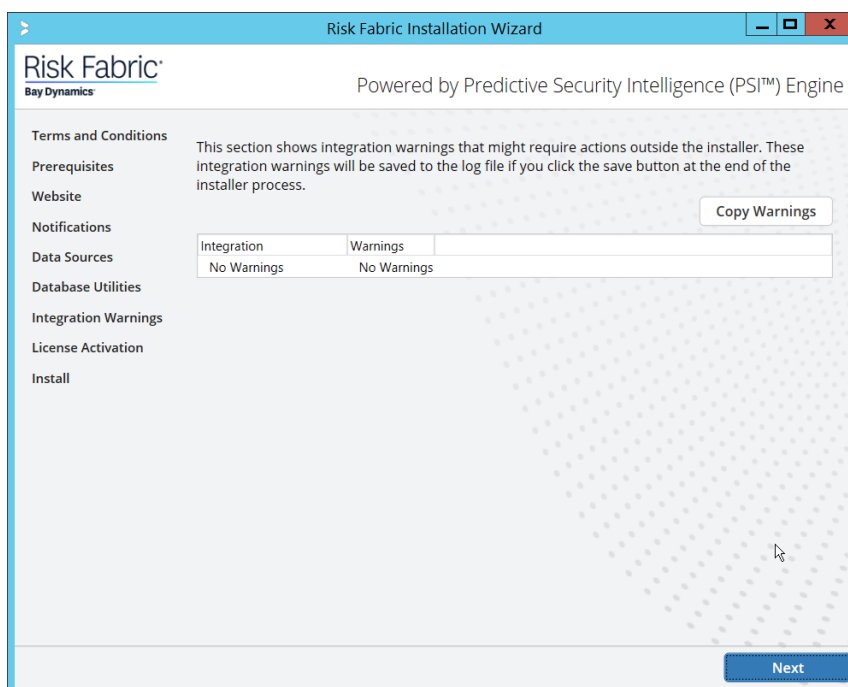


10. Click **Next**.
11. Configure any alert settings desired; these can be changed later.

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.

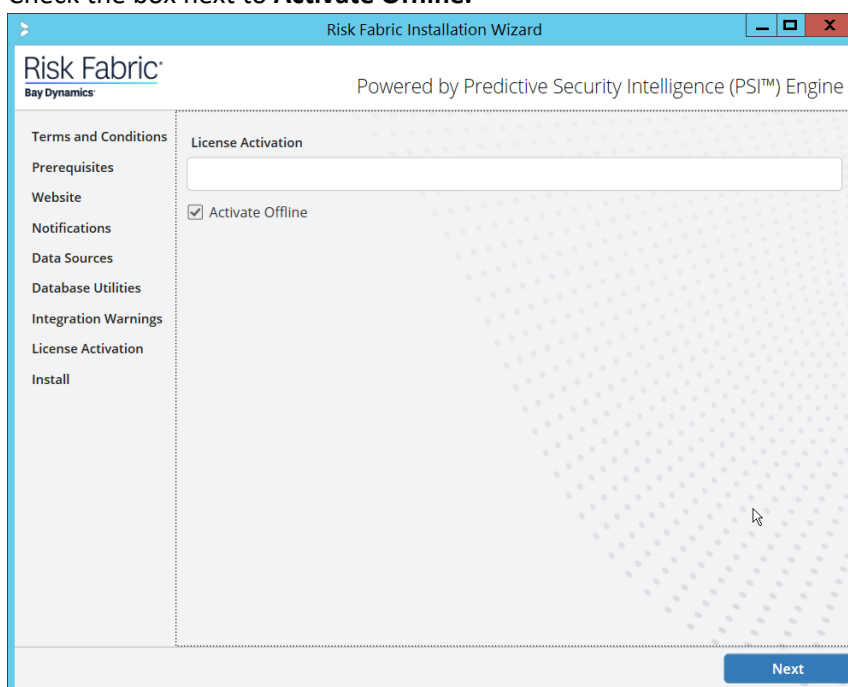
17. Click **Next**.

18. Click **Next**.

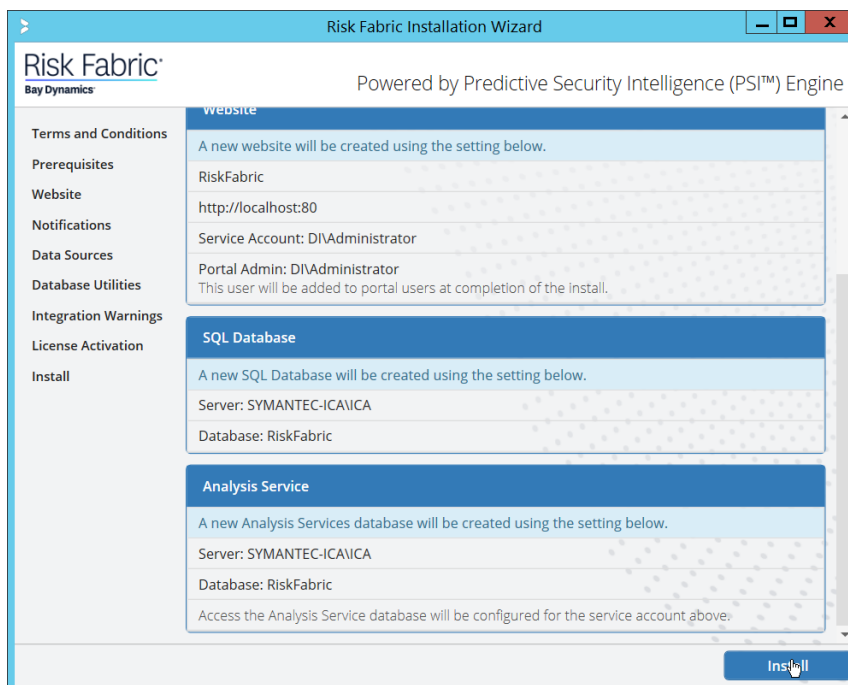


19. Click **Next**.

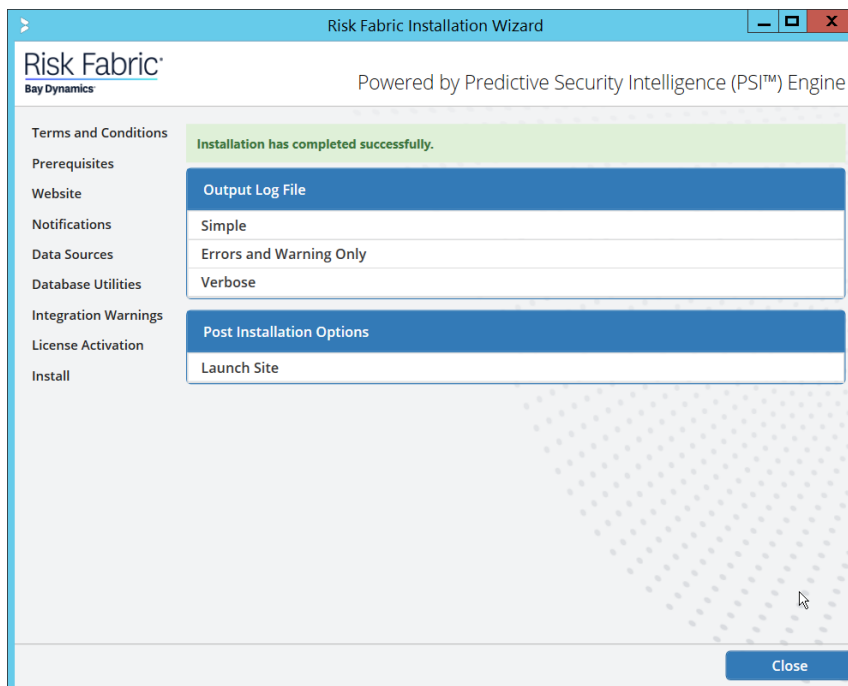
20. Check the box next to **Activate Offline**.



21. Click **Next**.



22. Click **Install**.



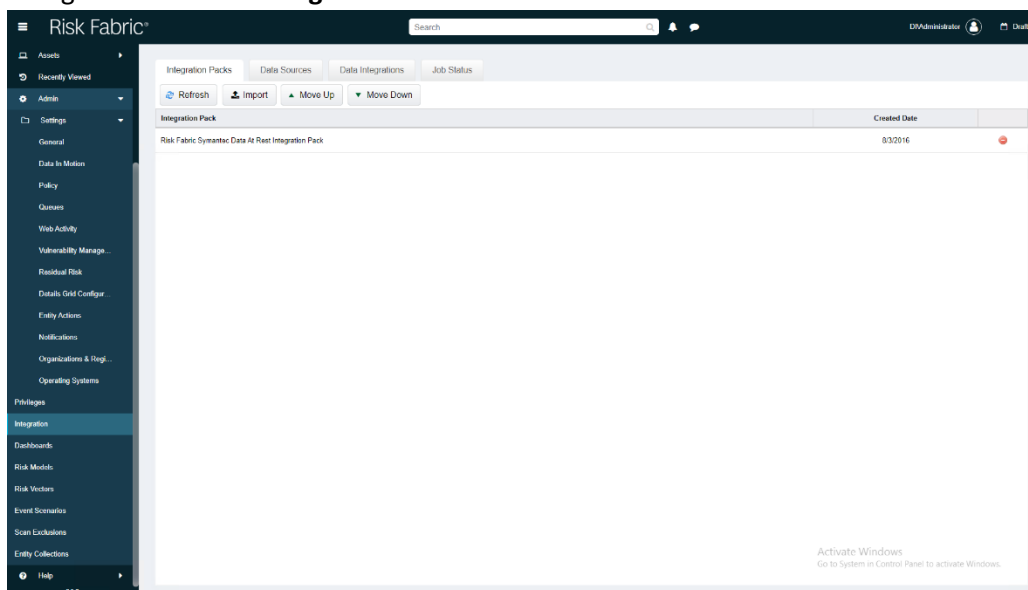
23. Click **Close**.

2.15.4 Configuring Symantec ICA for Analysis

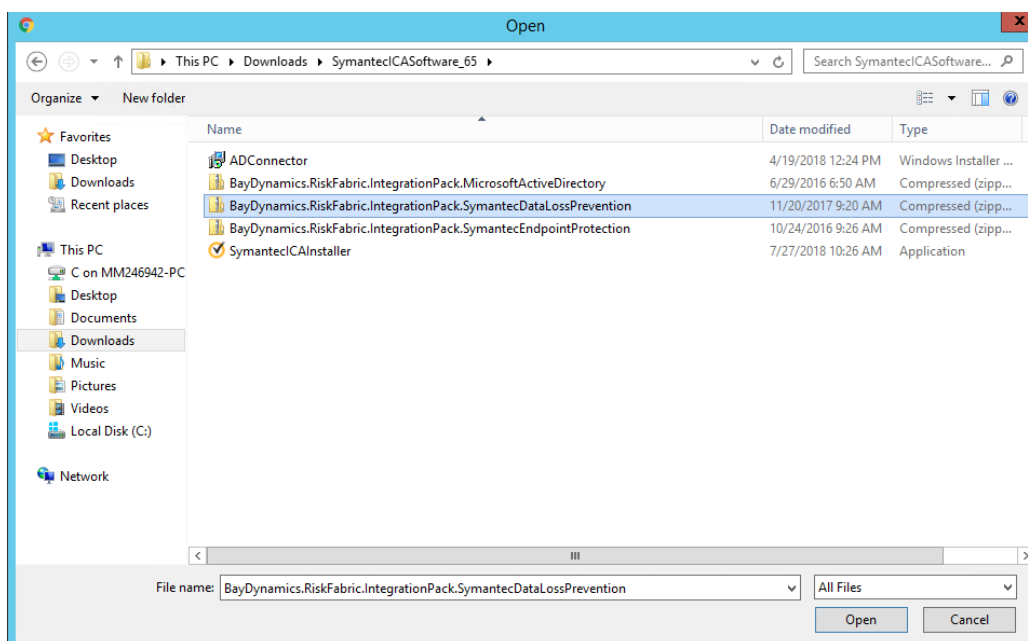
This section will contain instructions for navigating some aspects of the ICA admin console and dashboards, though this largely depends on the specific data your organization has identified and is trying to analyze.

2.15.4.1 *Installing Integration Packs*

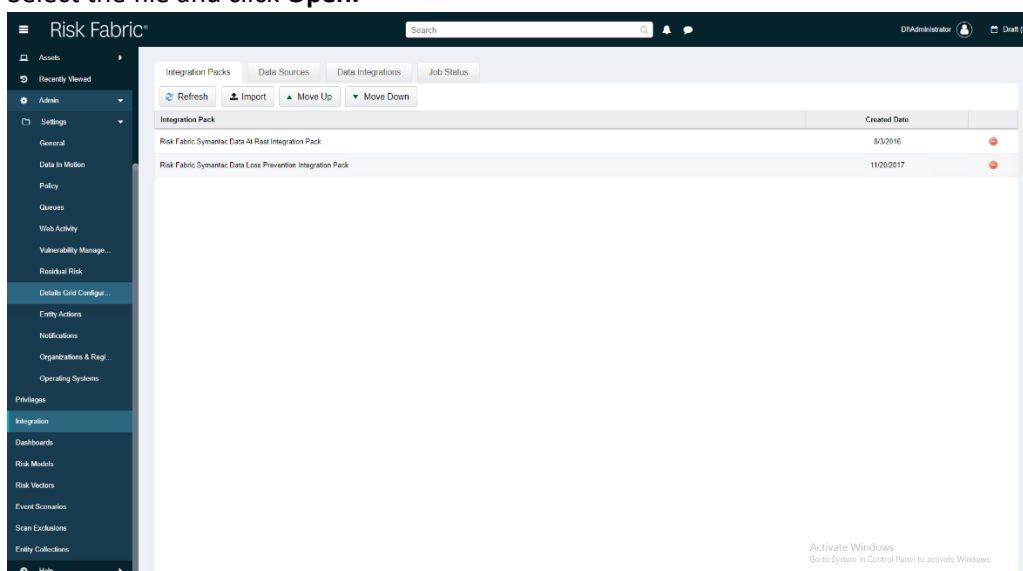
1. Download the relevant integration packs to someone on the local system. These are typically provided by Symantec, in a zip file. The zip file should be titled in the format of *BayDynamics.RiskFabric.IntegrationPack.<productName>*.
2. Log in to the Risk Fabric web interface.
3. Navigate to **Admin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



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

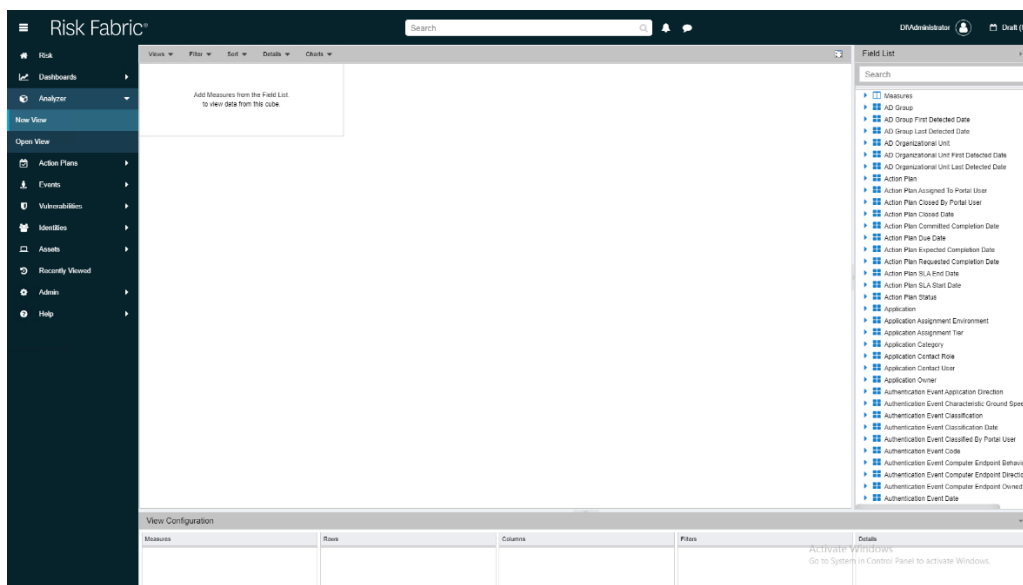


6. Select the file and click **Open**.



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.

Save View

Create new View

Overwrite existing View

View Name:

Testing

Type:

Analyzer View

Existing View Name:

☒ This view is accessible by all Users (Public)

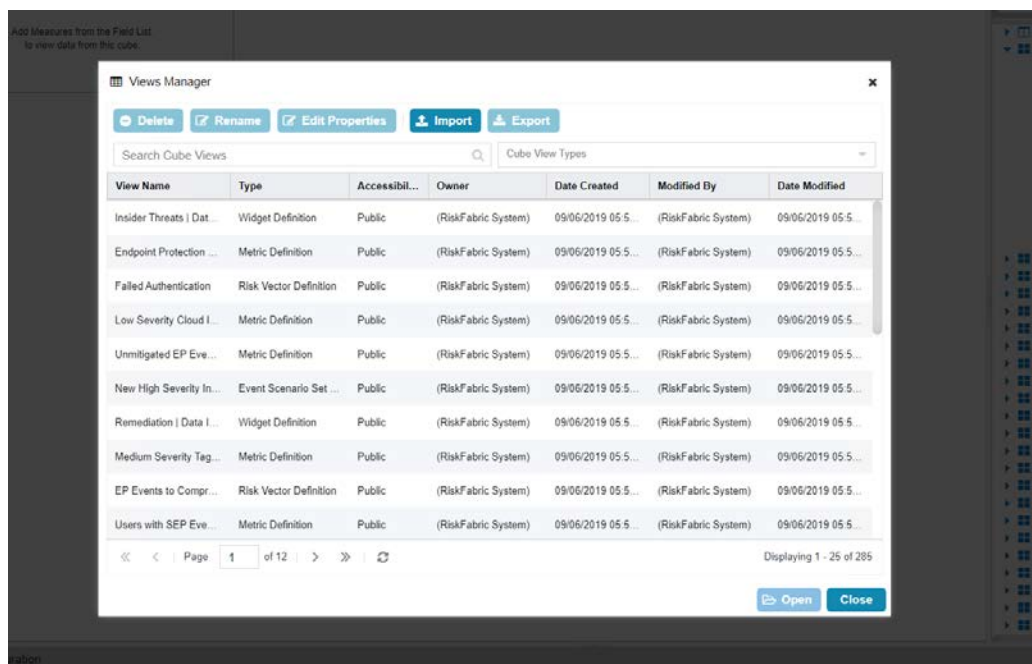
Save

Cancel

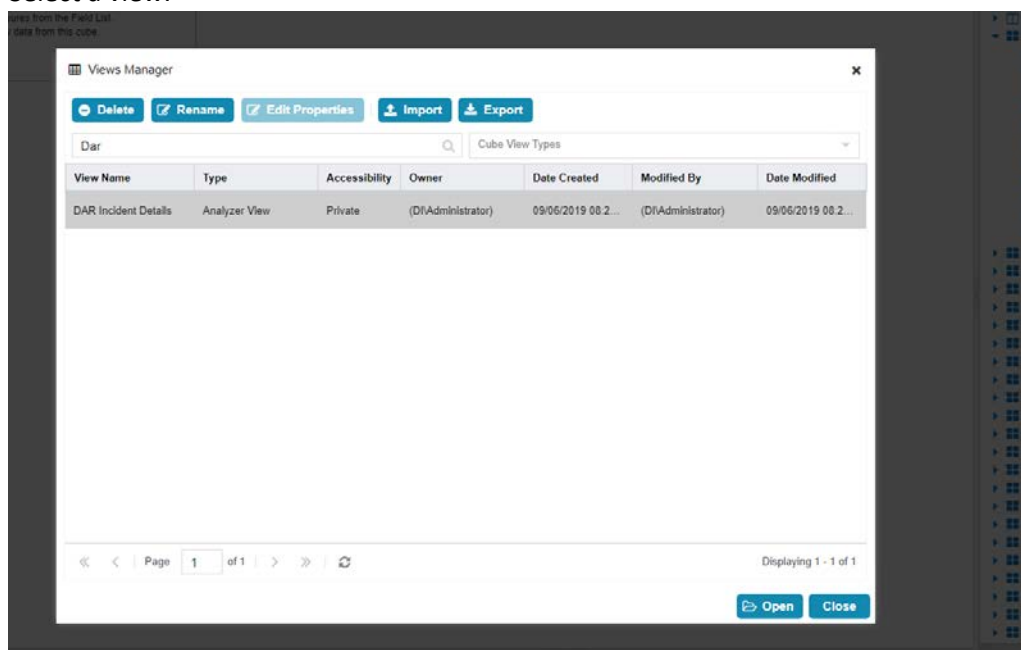
8. Click **Save**.

2.15.4.3 Open an Existing View

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



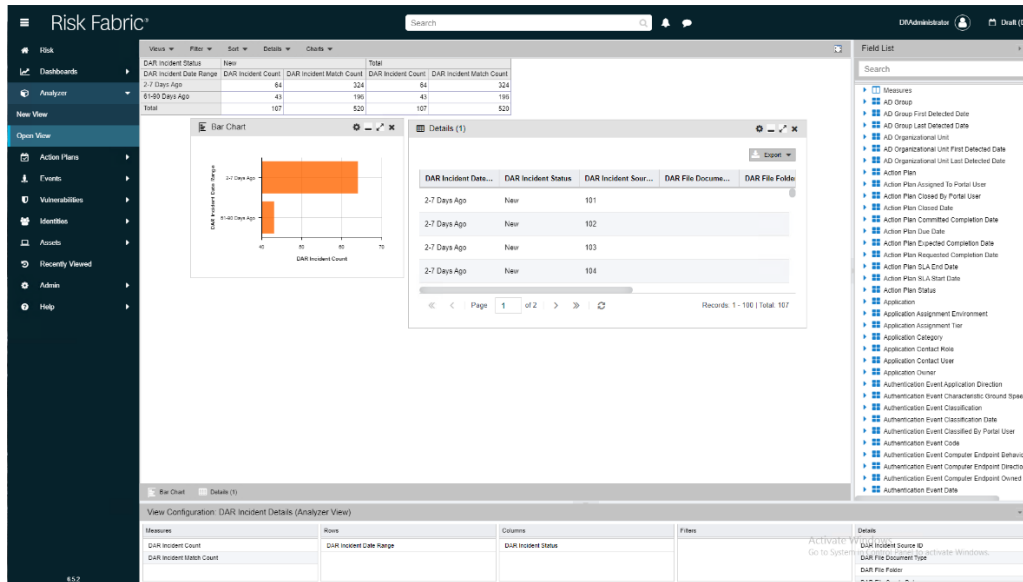
2. Begin to search for the view you want by typing a search term into **Search Cube Views**. (Note: if you created a view, it will also be present in this list).
3. Click the **Search** icon.
4. Select a view.



5. Click **Open**.

2.15.4.4 Viewing Detailed Analyzer Data

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



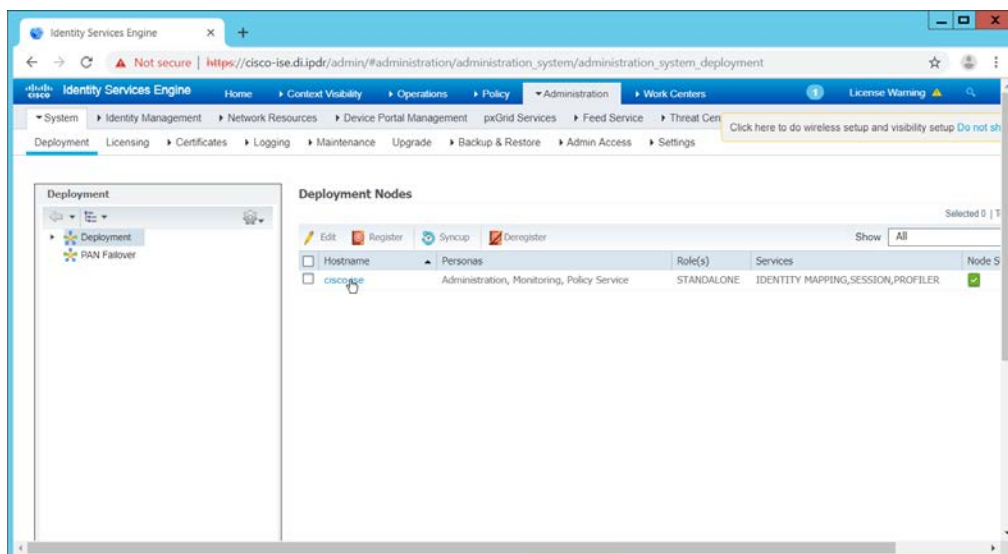
2. Charts can be added or removed using the **Charts** dropdown menu near the top of the analyzer.
3. Any data in the **Field List** on the right side can be added to or removed from the view and will be automatically incorporated into its relevant rows or columns.
4. The entire view format can be exported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

2.16 Integration: Cisco Identity Services Engine and Cisco Stealthwatch

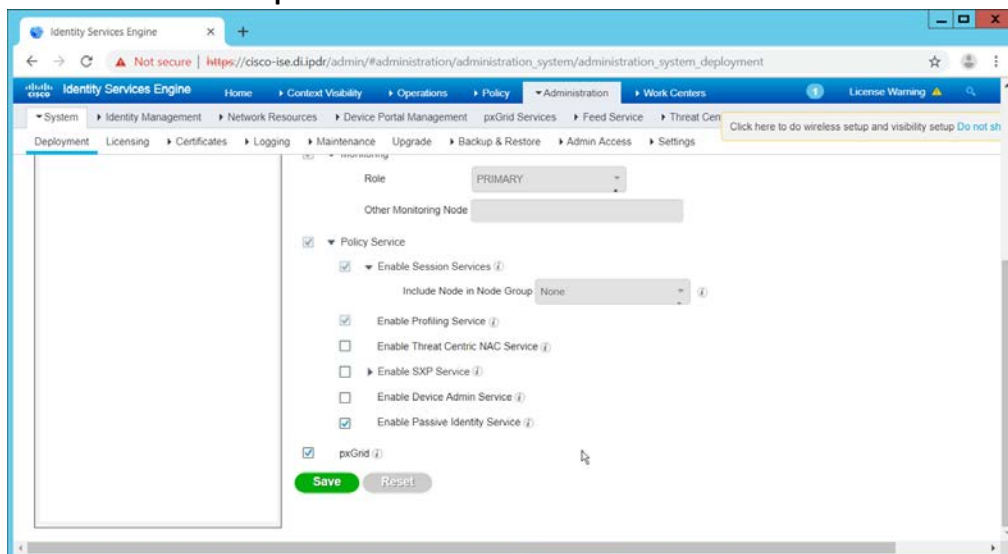
This section will detail an integration between Cisco Identity Services Engine (ISE) and Cisco Stealthwatch, allowing Stealthwatch to apply certain policies to hosts in ISE. Stealthwatch acts as a network monitoring solution and can be integrated with ISE to enable mitigation capabilities in response 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

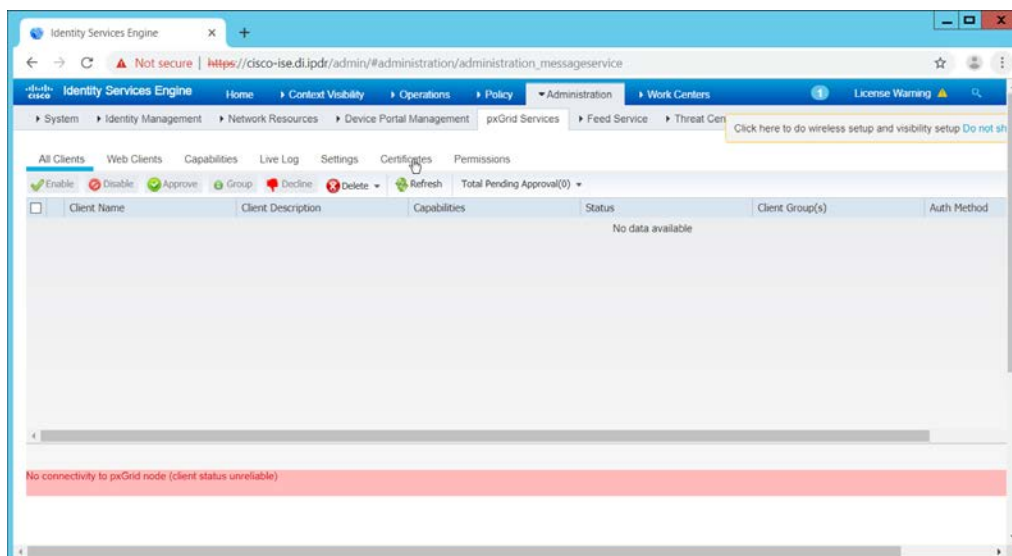
1. Log in to the Cisco ISE web console in a browser.
2. Navigate to **Administration > System > Deployment**.



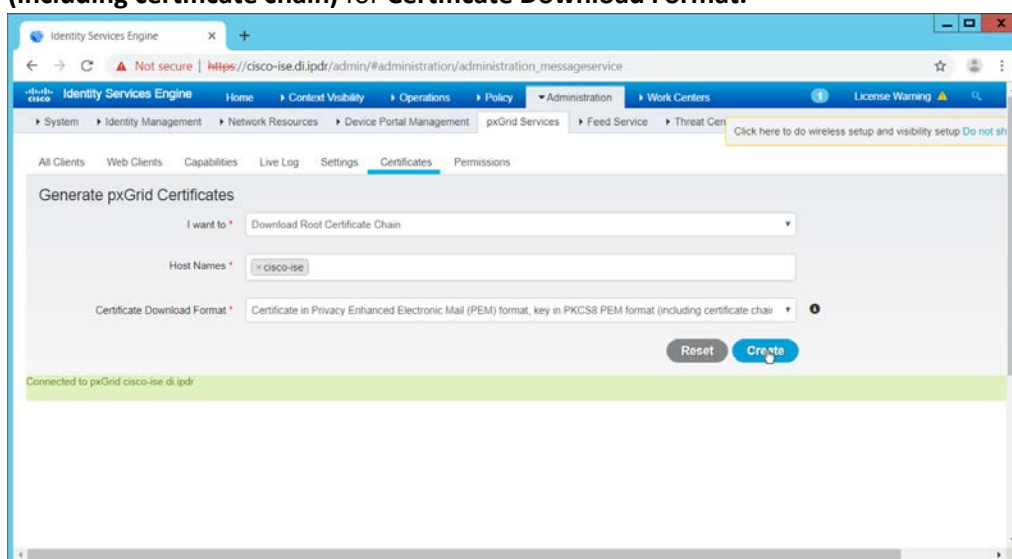
3. Click the hostname of the Cisco ISE machine.
4. Check the box next to **pxGrid**.



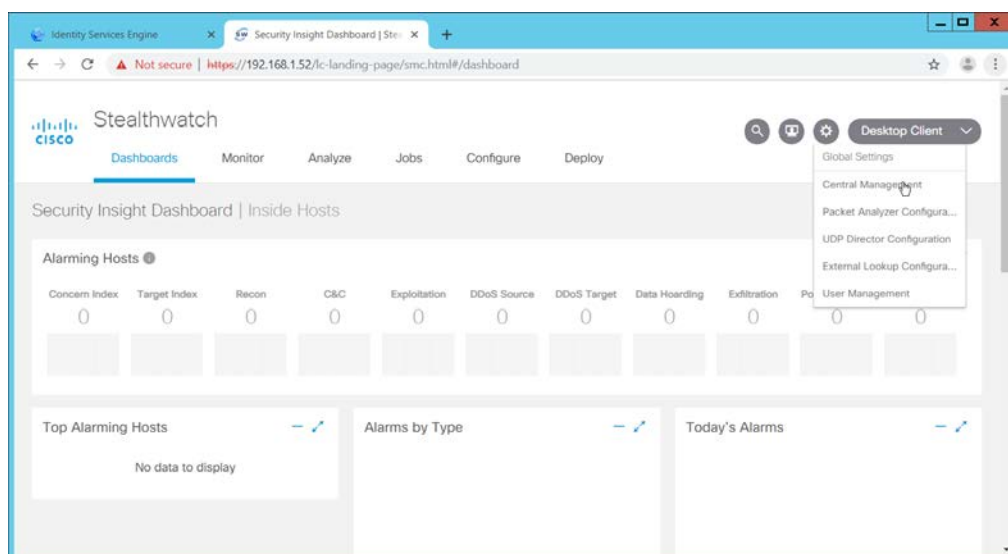
5. Click **Save**.
6. Navigate to **Administration > pxGrid Services**.



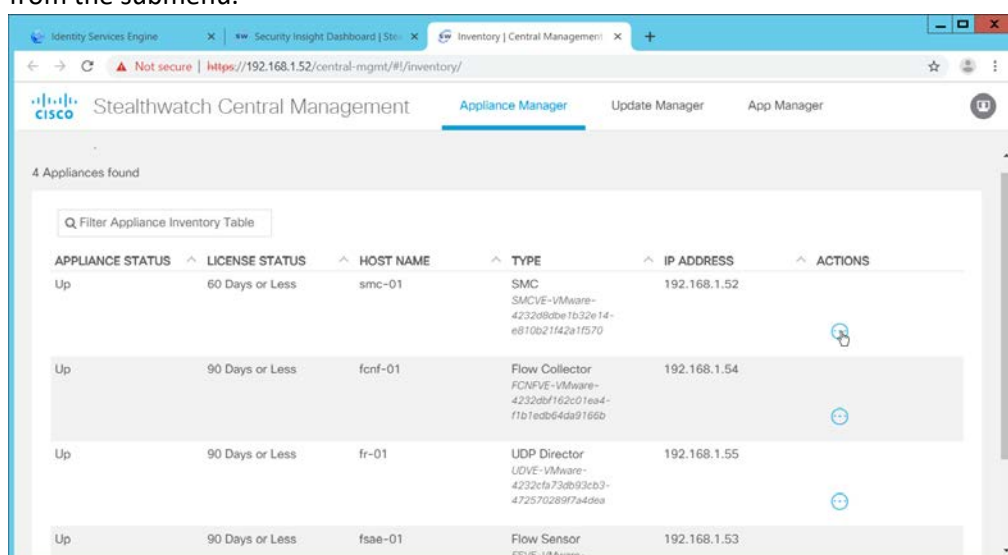
7. Click **Certificates**.
8. Select **Download Root Certificate Chain** for **I want to**.
9. Select the hostname of the Cisco ISE server for **Host Names**.
10. Select **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)** for **Certificate Download Format**.



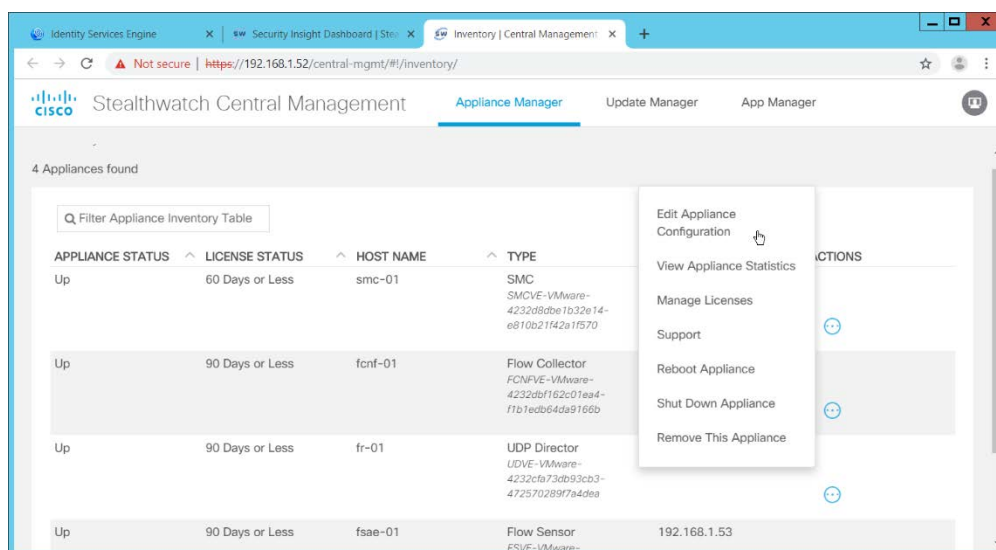
11. Click **Create**. This will download a zip file containing the certificate.
12. Extract the zip file—it may contain several files—the one we are interested in is the Root CA.
13. Log in to the **Stealthwatch Management Console** through the browser.



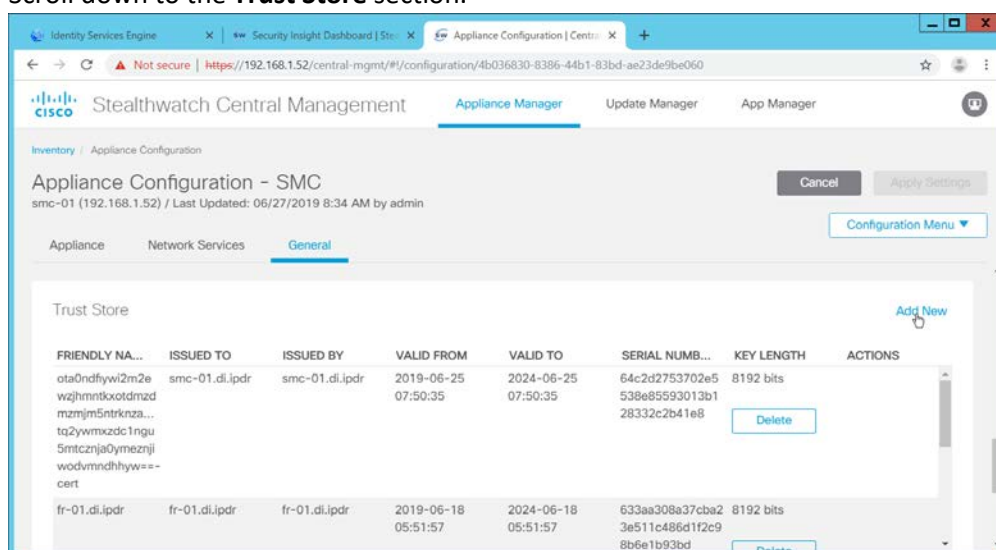
14. In the top right corner of the console, hover over the **gear icon** and select **Central Management** from the submenu.



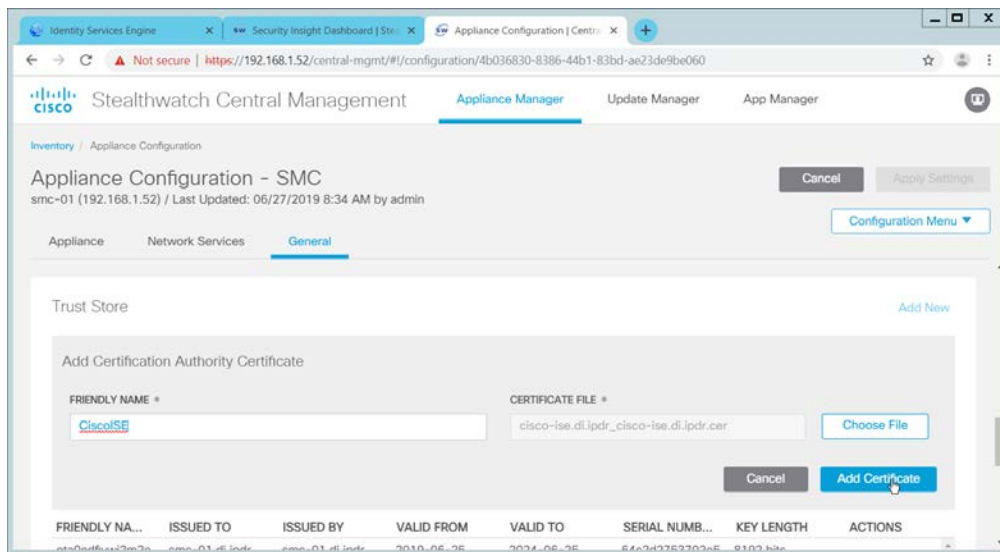
15. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.



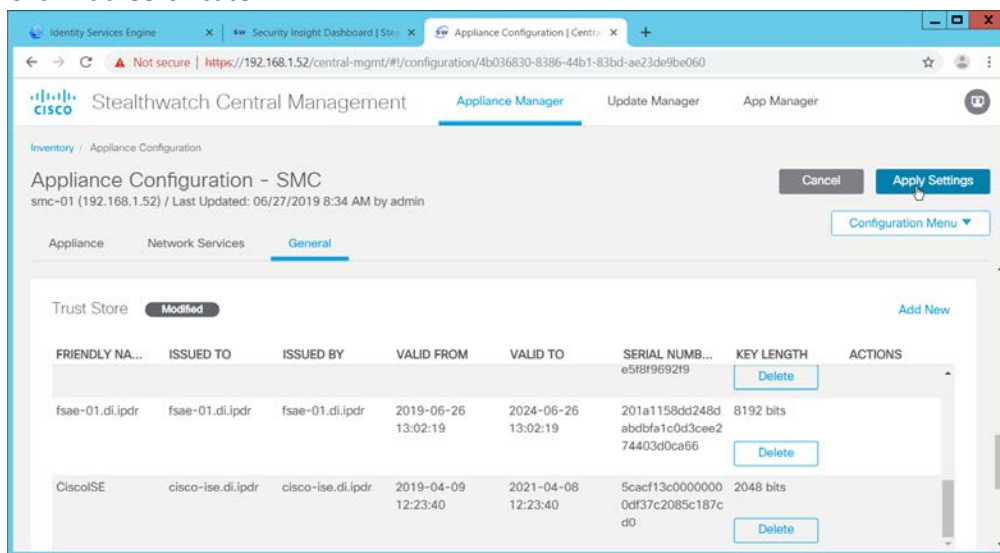
16. This will open a submenu. Select **Edit Appliance Configurations**.
17. Click the **General** tab.
18. Scroll down to the **Trust Store** section.



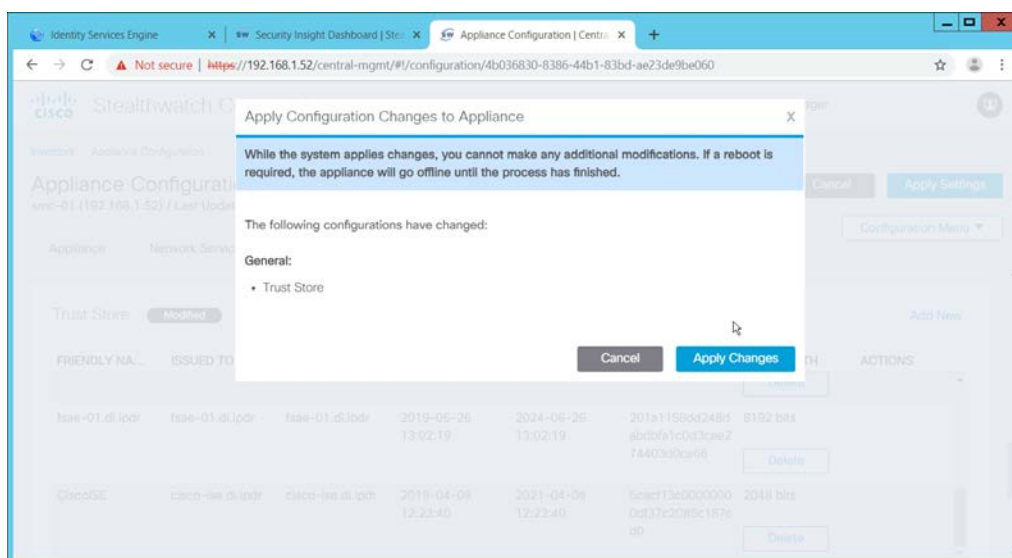
19. Click **Add New**.
20. Enter a **name**.
21. Click **Choose File**.
22. Select the Cisco ISE Root certificate from the files downloaded earlier.



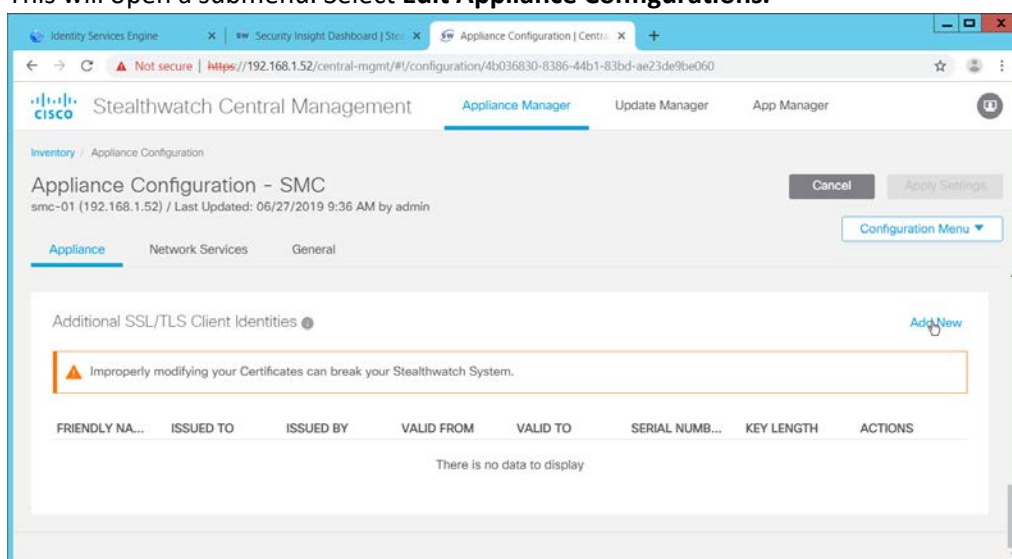
23. Click **Add Certificate**.



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.

The screenshot shows the 'Appliance Configuration - SMC' page in the Cisco Stealthwatch Central Management console. The 'Appliance' tab is selected, and the 'Generate a CSR' section is active. The form contains the following fields:

- RSA KEY LENGTH ***: Radio buttons for 2048 bits (selected), 4096 bits, and 8192 bits.
- COMMON NAME**: Text field with value 'sw-smc.di.ipdr'.
- ORGANIZATION**: Text field with value 'DI'.
- ORGANIZATIONAL UNIT**: Text field with value 'IPDR'.
- LOCALITY OR CITY**: Text field with value 'Rockville'.
- STATE OR PROVINCE**: Text field with value 'MD'.
- COUNTRY CODE**: Text field with value 'US'.
- EMAIL ADDRESS**: Text field with value 'administrator@di.ipdr'.

Buttons at the bottom include 'Cancel' and 'Generate CSR'.

32. Click **Generate CSR**.

The screenshot shows the 'Add SSL/TLS Client Identity' section of the 'Appliance Configuration - SMC' page. The form contains the following fields:

- FRIENDLY NAME ***: Text field.
- CERTIFICATE FILE ***: Text field with a 'Choose File' button next to it.

Buttons include 'Download CSR' (highlighted with a mouse cursor), 'Cancel', and 'Add Client Identity'. Below the form is a warning message: 'Your certificates are critical for your system's security. Improperly modifying your certificates can break your Stealthwatch system. Follow the instructions in [Stealthwatch Help](#) to update the Additional SSL/TLS Client Identities.'

At the bottom, there is a table header with columns: FRIENDLY N..., ISSUED TO, ISSUED BY, VALID FROM, VALID TO, SERIAL NUM..., KEY LENGTH, and ACTIONS. Below the header, it says 'There is no data to display'.

33. When this finishes, click **Download CSR**.

34. Open the Certificate Signing Request (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.

Identity Services Engine | Cisco ISE Configuration | Stealthwatch Central Management | Appliance Configuration | SMC

Appliance Configuration - SMC
sw-smc (192.168.1.150) / Last Updated: 08/08/2019 7:34 AM by admin

Appliance | Network Services | General

Add SSL/TLS Client Identity

FRIENDLY NAME *
SMC_PKCS12

CERTIFICATE FILE *
sw-smc.dl.ipdr_192.168.1.150.p12

BUNDLE PASSWORD *

CONFIRM PASSWORD *

Download CSR | Choose File | Add Client Identity

⚠ Your certificates are critical for your system's security. Improperly modifying your certificates can break your Stealthwatch system. Follow the instructions in [Stealthwatch Help](#) to update the Additional SSL/TLS Client Identities.

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
---------------	-----------	-----------	------------	----------	---------------	------------	---------

49. Click **Add Client Identity**.

Identity Services Engine | Security Insight Dashboard | Stealthwatch Central Management | Appliance Configuration | SMC

Appliance Configuration - SMC
sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:55 AM by admin

Appliance | Network Services | General

Additional SSL/TLS Client Identities | Modified | Add New

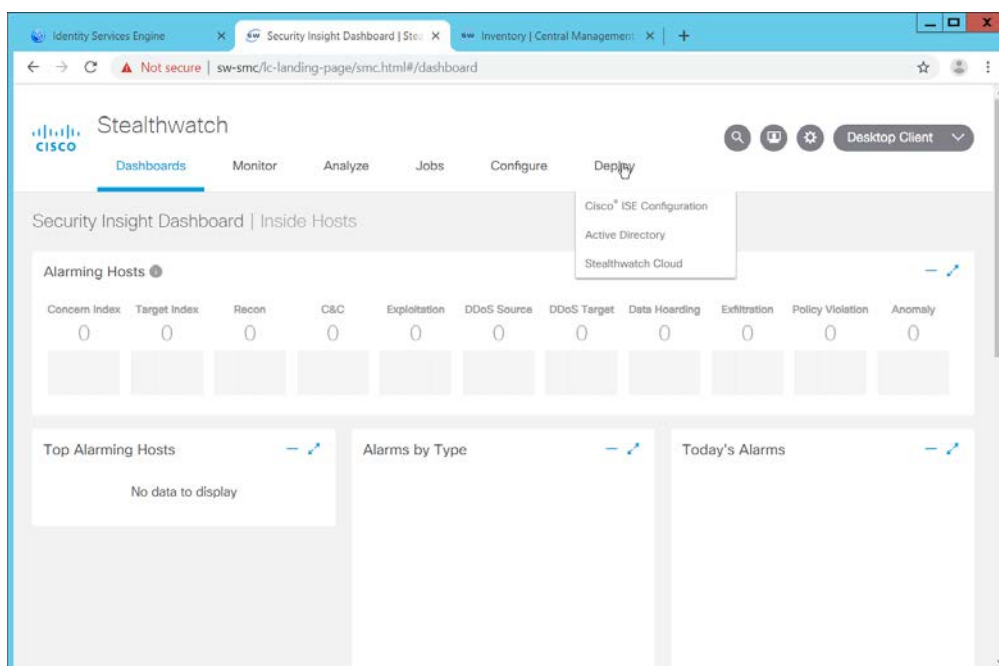
⚠ Improperly modifying your Certificates can break your Stealthwatch System.

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
SMC_PKCS12	DI	Certificate Services Endpoint Sub CA - cisco-ise	2019-08-07 07:02:34	2021-08-07 07:02:34	55e8a9bc7748406f9d07c429641e5b05	2048 bits	Delete

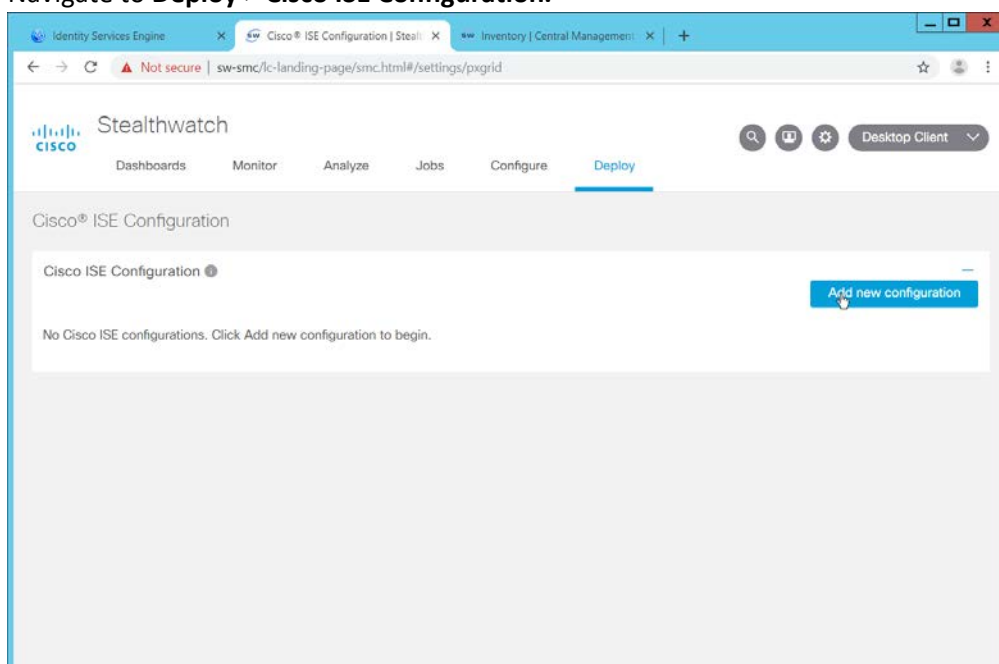
Revert | Apply Settings

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.

Cisco ISE Configuration Setup

CLUSTER NAME: cisco-ise

CERTIFICATE: SMC_PKCS12

PRIMARY PXGRID NODE: 192.168.1.61

SECONDARY PXGRID NODE: ex. 10.10.10.10

USER NAME: SMC

Integration options

- ☒ Adaptive Network Control
- ☒ Static SGT Classifications
- ☒ User sessions

Cancel Save

58. Click **Save**.

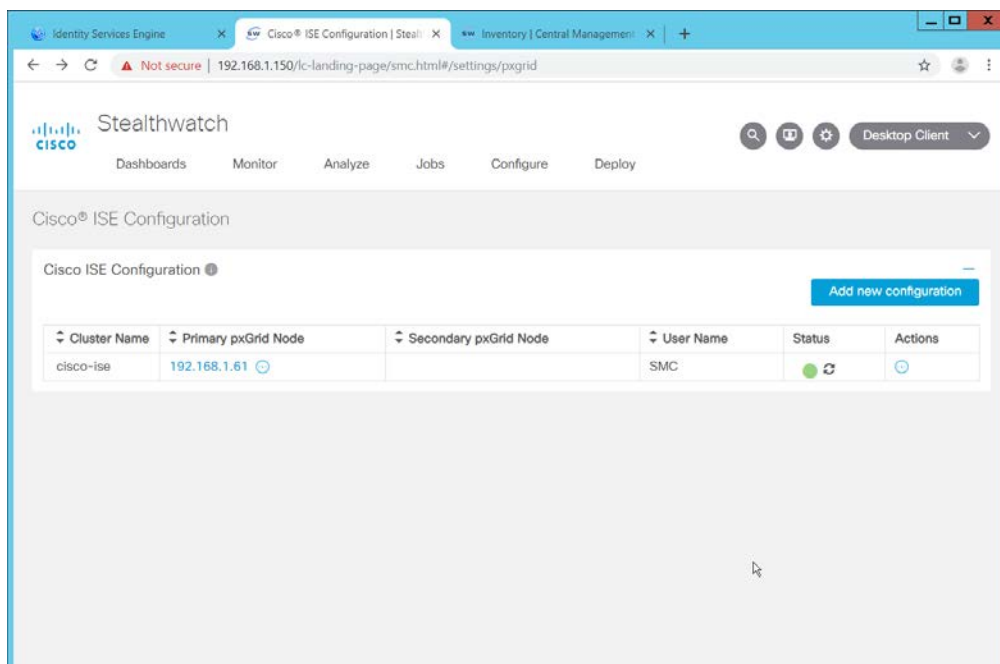
59. On the Cisco ISE web portal, navigate to **Administration > pxGrid Services > All Clients**.

Administration > pxGrid Services > All Clients

Client Name	Capabilities	Status	Client Group(s)	Auth
ise-fanout-cisco-ise	Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Cert
ise-admin-cisco-ise	Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Cert
ise-pubsub-cisco-ise	Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Cert
ise-bridge-cisco-ise	Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Cert
ise-mnt-cisco-ise	Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Cert
<input checked="" type="checkbox"/> smc	Capabilities(0 Pub, 0 Sub)	Pending		

Connected to pxGrid cisco-ise di ipdr

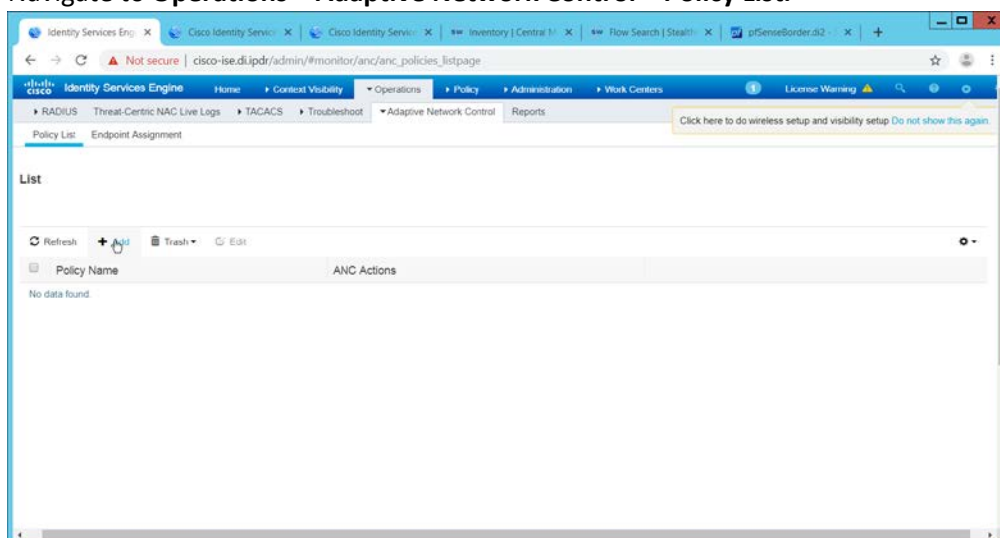
60. If the SMC client you just created says **Pending**, check the box next to it and click **Approve**.



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.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Policy List Endpoint Assignment

Click here to do wireless setup and visibility setup Do not show this again.

List > New

Input fields marked with an asterisk (*) are required.

name: QUARANTINE

Action *:

- QUARANTINE
- SHUT_DOWN
- PORT_BOUNCE

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

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Policy List Endpoint Assignment

Click here to do wireless setup and visibility setup Do not show this again.

List > New

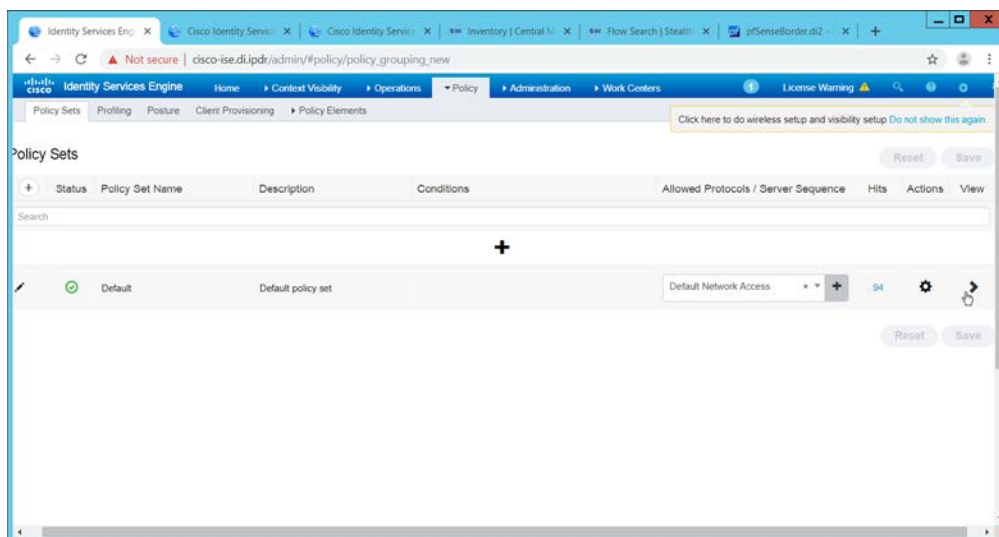
Input fields marked with an asterisk (*) are required.

name: ANC_QUARANTINE

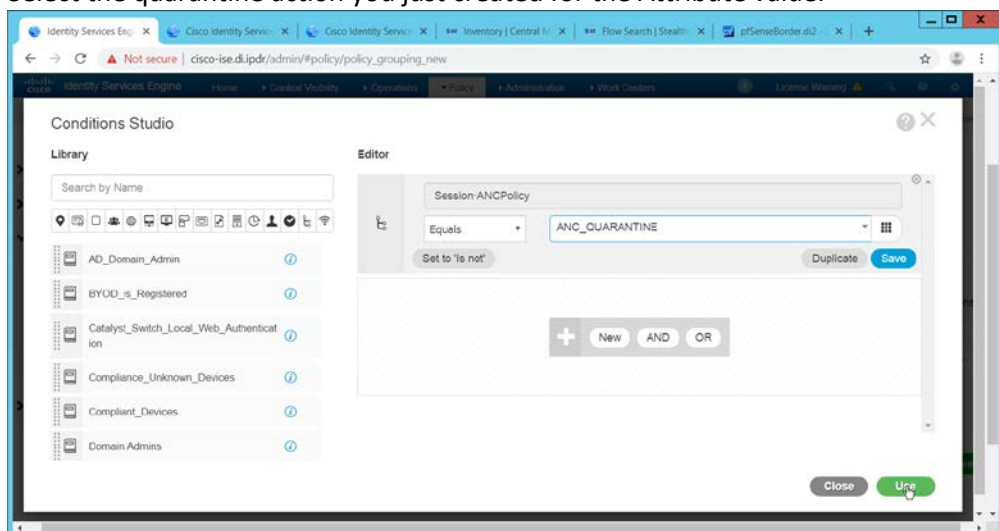
Action *: QUARANTINE

Cancel Submit

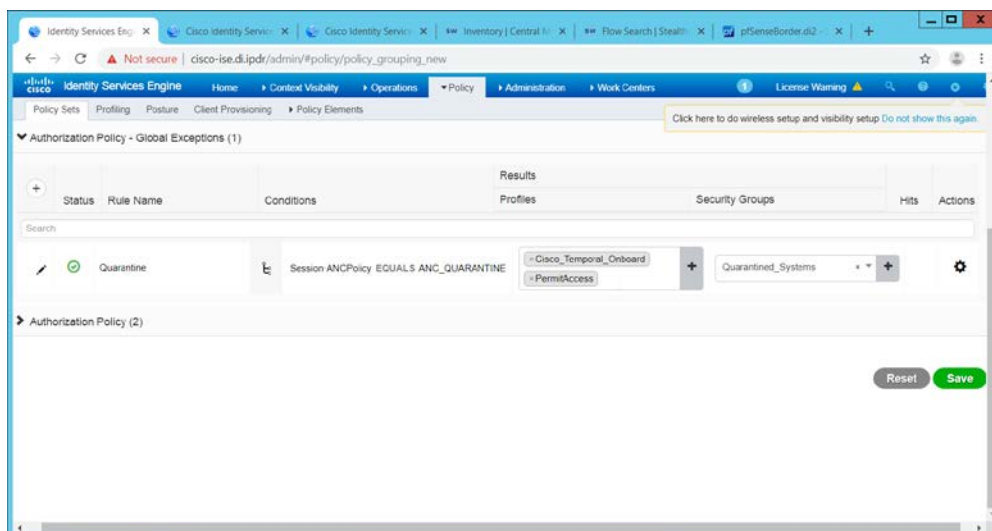
5. Click **Submit**.
6. Navigate to **Policy > Policy Sets**.



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.

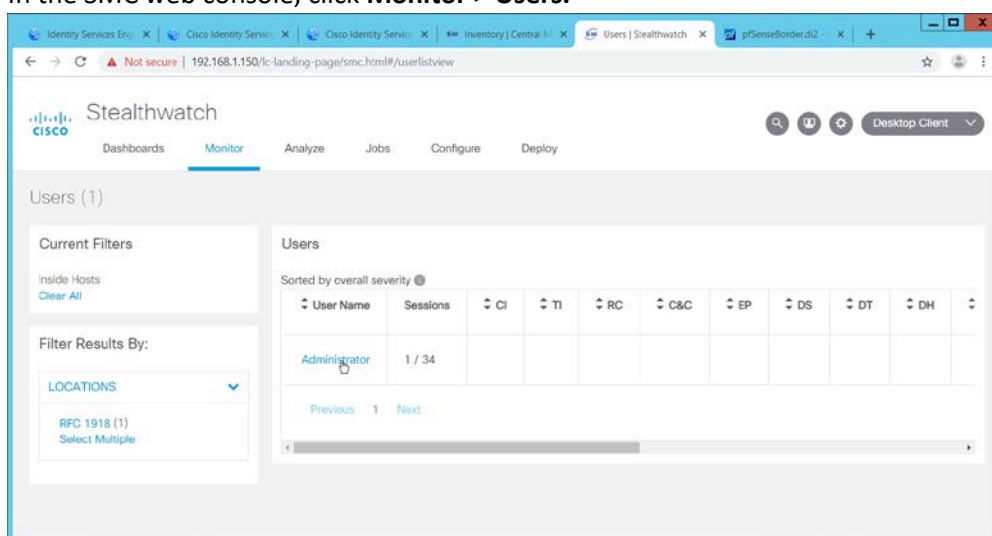


13. Click **Use**.
14. Select the **Deny Access** profile; the profile selected here will be applied to the machine when the machine is added to the quarantine group.
15. Select **Quarantined_Systems** for **Security Groups**.

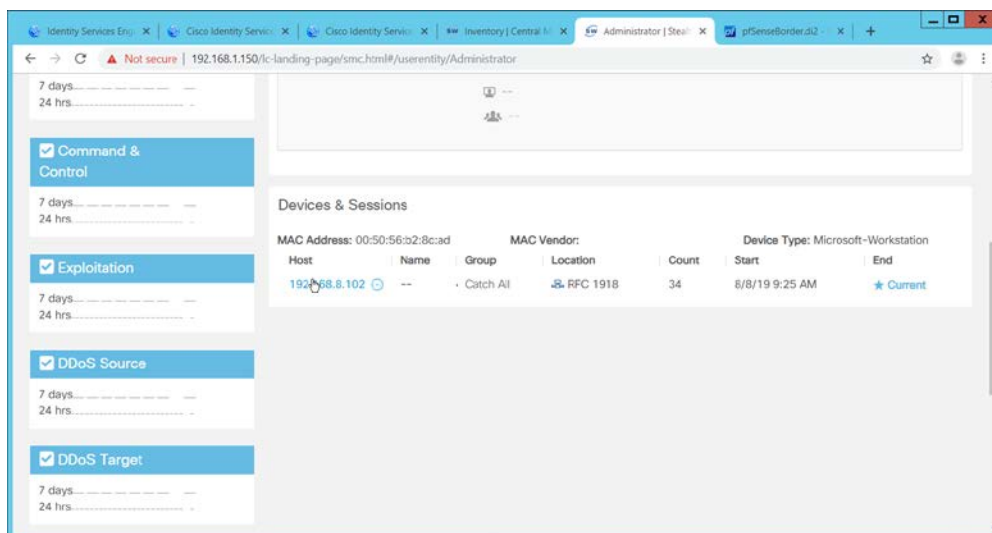


16. Click **Save**.

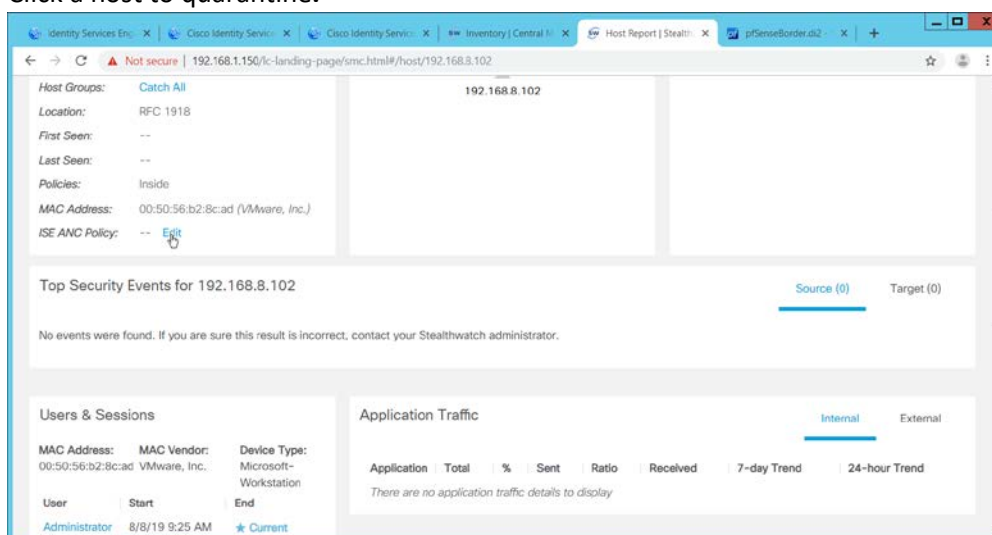
17. In the SMC web console, click **Monitor > Users**.



18. Select a user to quarantine.

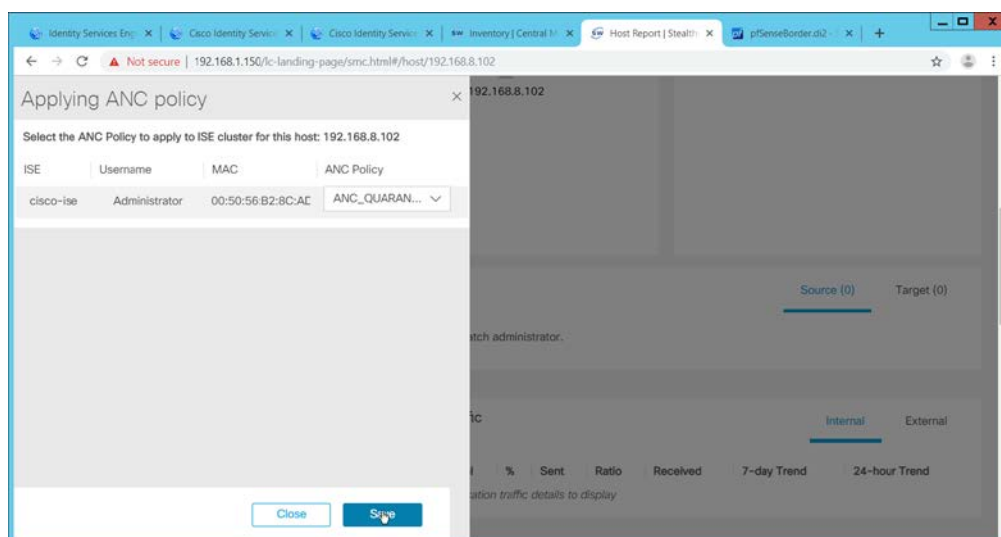


19. Click a host to quarantine.



20. Click **Edit** next to **ISE ANC Policy**.

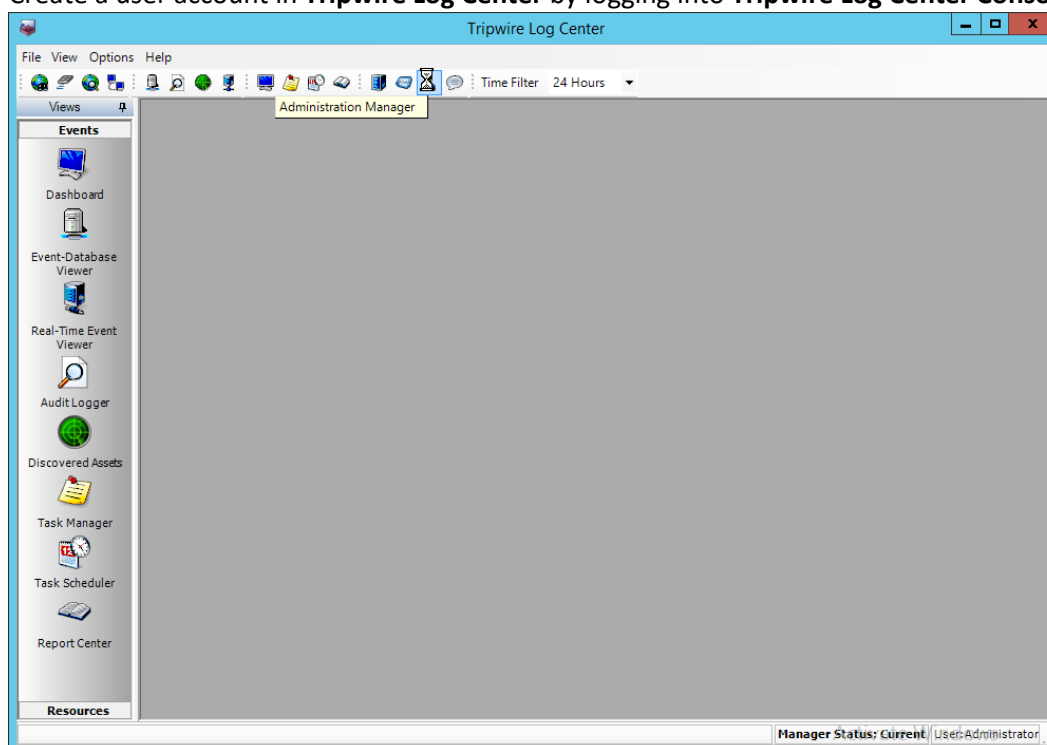
21. From the drop down, select the quarantine action you created earlier.



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

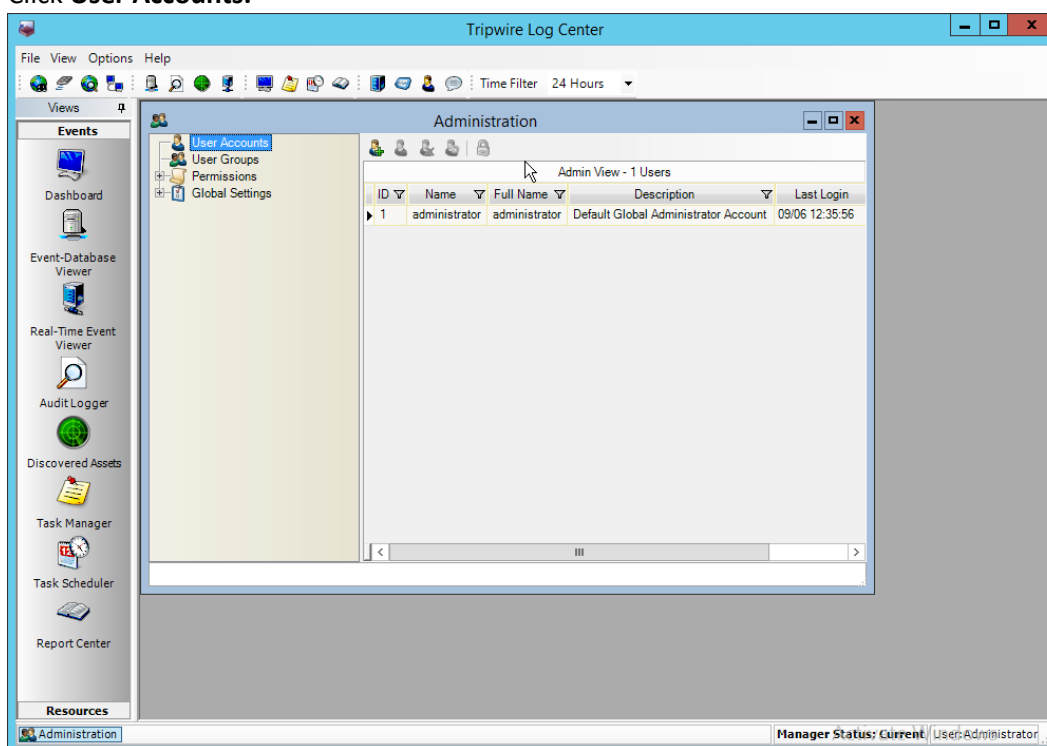
2.17 Integration: Tripwire Log Center and Tripwire Enterprise

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.

The 'Add New User' dialog box is shown. It contains the following fields and controls:

- Username:** A text field containing 'tweuser'.
- Settings:** A tabbed section with the following fields:
 - Full name:** An empty text field.
 - Description:** An empty text field.
 - Authentication method:** A dropdown menu with 'Tripwire Log Center' selected.
 - Password:** A text field with masked characters (dots).
 - Password Verify:** A text field with masked characters (dots).
- Buttons:** 'Add' and 'Cancel' buttons at the bottom.

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

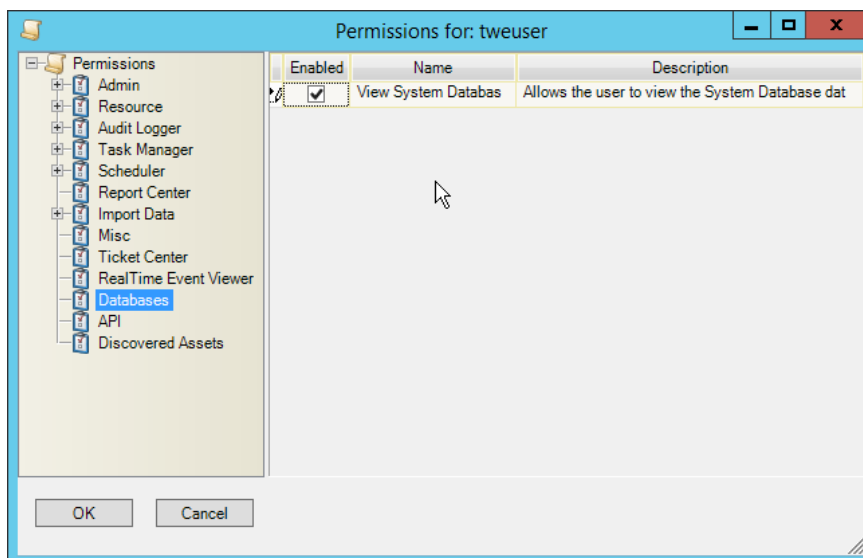
The screenshot shows the 'Edit User - tweuser' dialog box with the 'General' tab selected. The 'User Name' field contains 'tweuser'. Below the tabs, there are input fields for 'Full name', 'Description', 'Email', and two 'Phone' fields, each with a dropdown arrow. The 'Authentication' section includes a 'Valid IPs' field, an 'Auth method' dropdown set to 'Tripwire Log Center', an 'External User' field, and an 'Account is Disabled' checkbox. At the bottom are 'OK' and 'Cancel' buttons.

8. Click the **Permissions** tab.

The screenshot shows the 'Edit User - tweuser' dialog box with the 'Permissions' tab selected. The 'User Name' field still contains 'tweuser'. The 'Permissions' tab displays a table with two columns: 'Name' and 'Description'. The table is currently empty. At the bottom are 'OK' and 'Cancel' buttons.

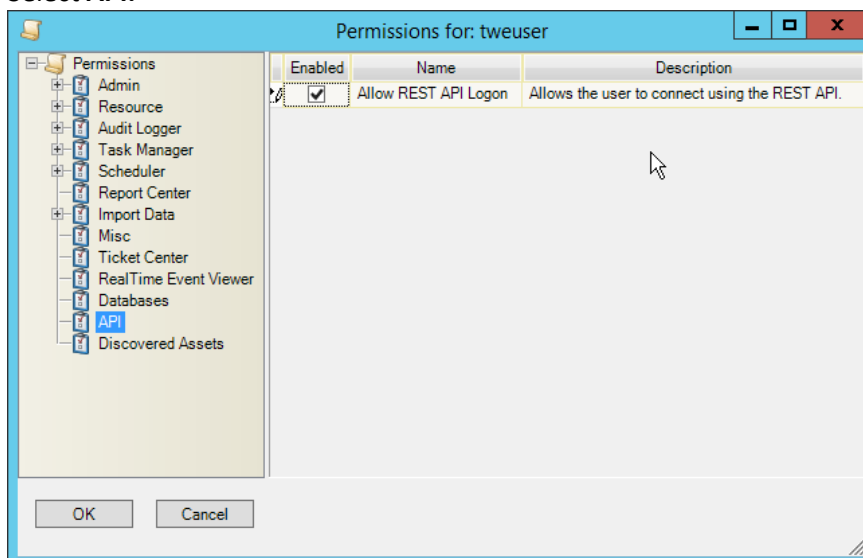
9. Click **Edit list of permissions**.

10. Select **Databases**.

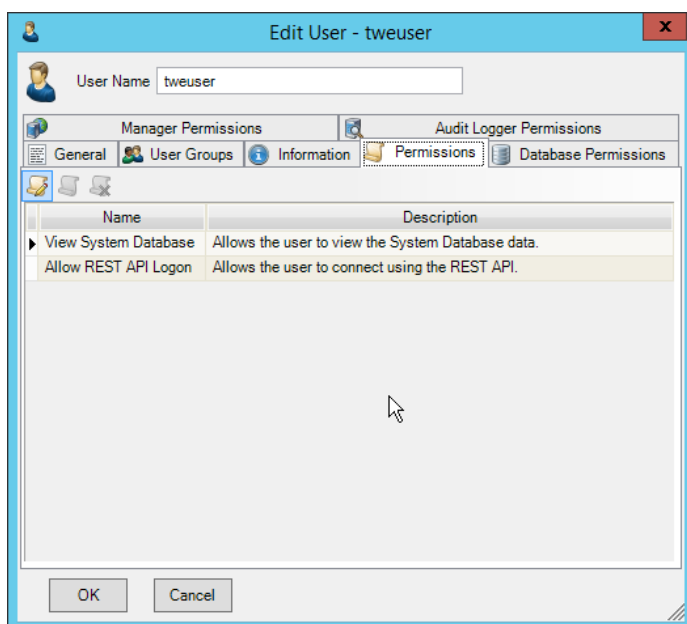


11. Check the box next to **View System Database**.

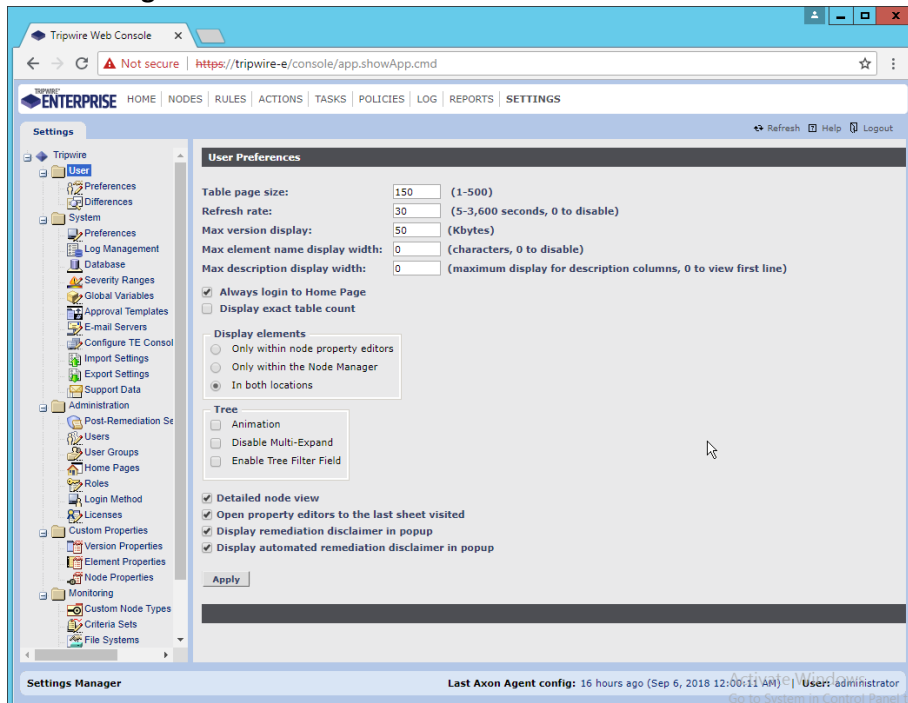
12. Select **API**.



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

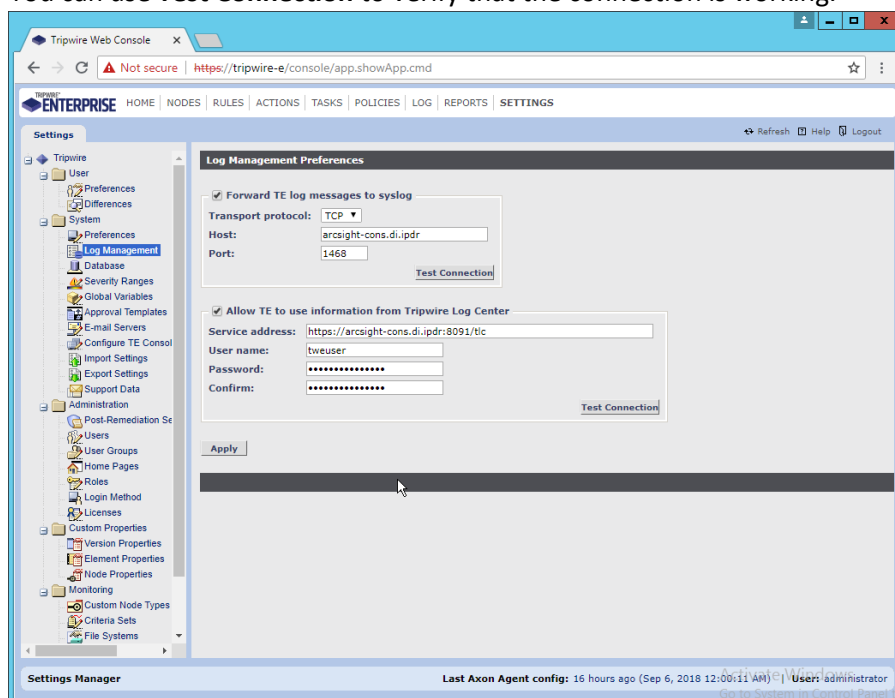


14. Click **OK**.
15. Click **OK**.
16. Log in to the **Tripwire Enterprise** web console.
17. Click **Settings**.

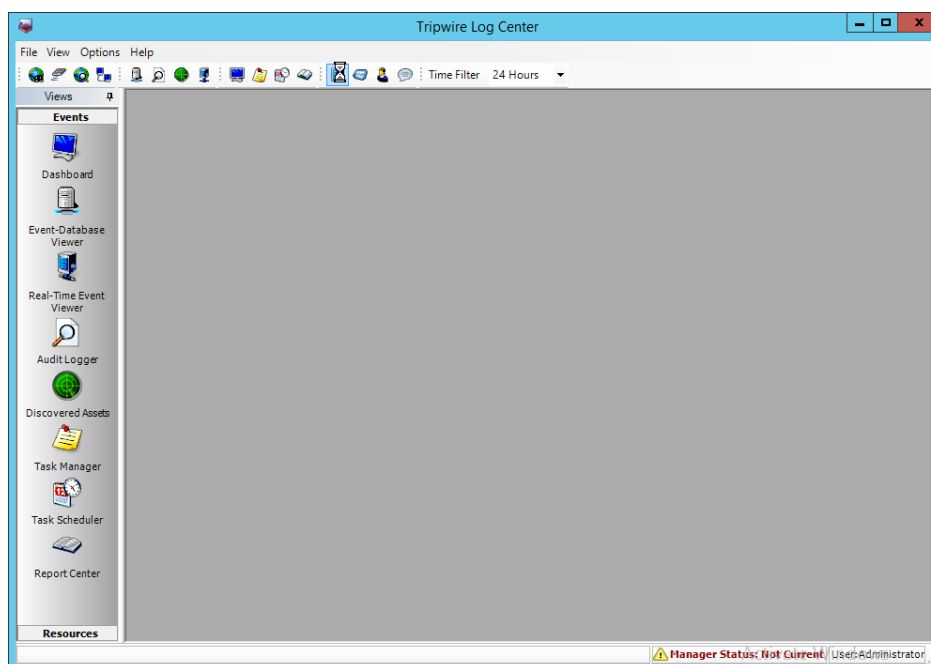


18. Go to **System > Log Management**.

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.

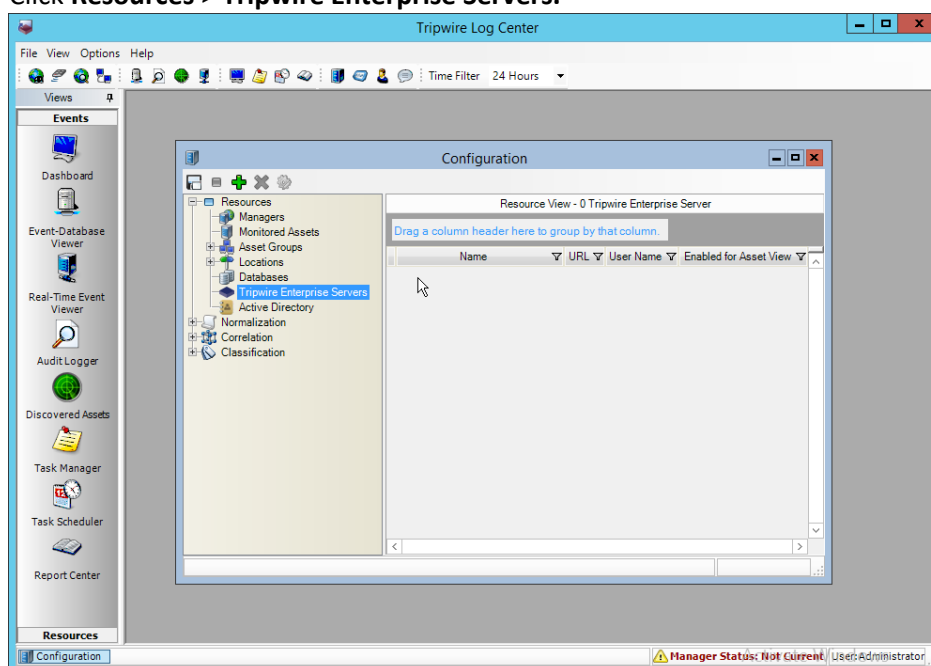


25. Click **Apply** when finished.
26. Go back to the **Tripwire Log Center Console**.



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**.

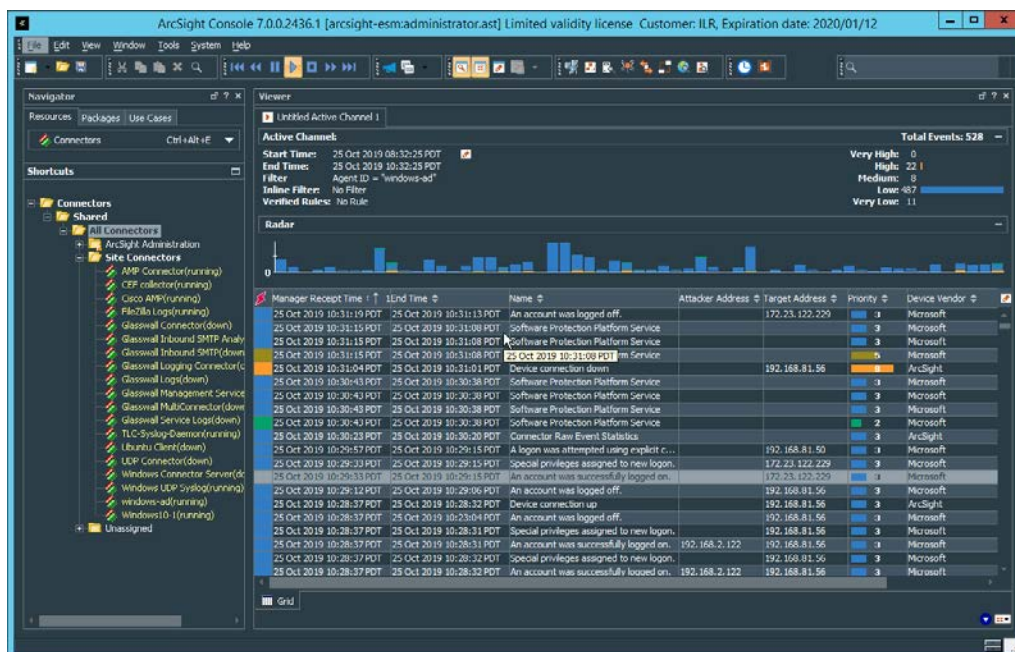
2.18 Integration: Symantec ICA and ArcSight ESM

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 Application Programming Interface (API) for other applications. Because of this, the standard integration between ICA and ESM was unavailable. However, it is still possible to import Comma-Separated Values (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:

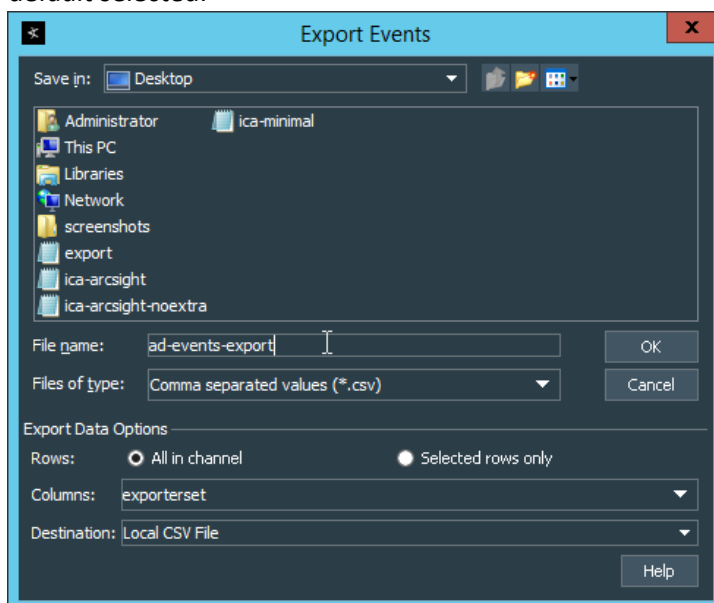
- On the version of Symantec ICA we are using, it is required to replace empty fields in the CSV with NULL. This may be unnecessary in future updates.
- The CSV file should be in a location accessible to the ICA server. You can replace this file with a new CSV file on a daily basis, and Symantec ICA 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.

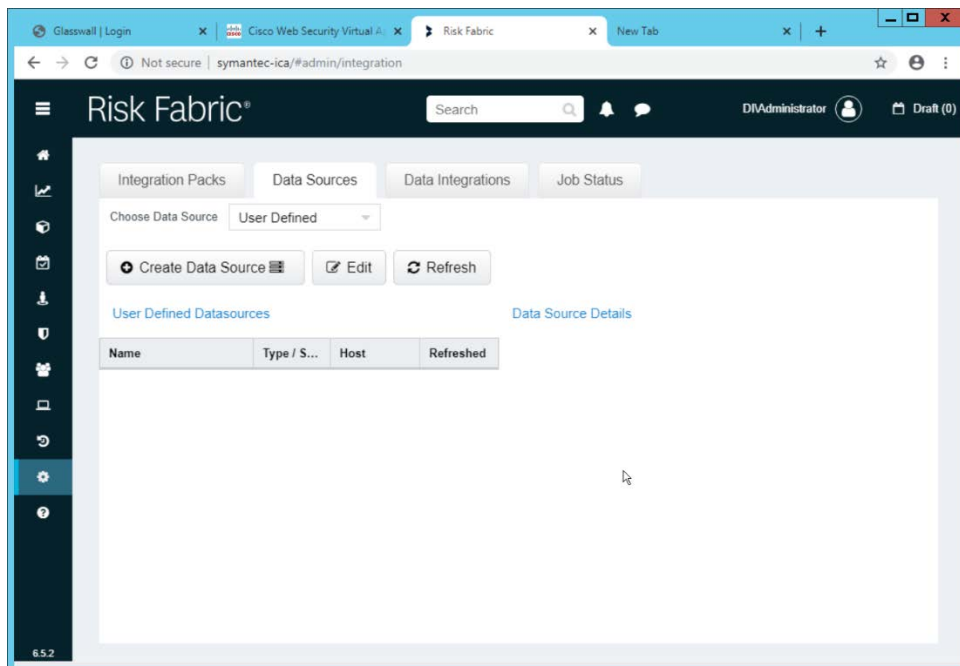


7. Click **OK**.

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).

Risk Fabric

Integration Packs | Data Sources | Data Integrations | Job Status

Choose Data Source: User Defined

Create Data Source

Data Source Type: File System I/W

Data Source Label: ArcSight Import

Server Name: symantec-ica.di.ipdr

Authentication Mode: Windows / Active Directory

Download Directory: C:\Temp\processed

Source Folder: C:\Temp\unprocessed

Save Cancel

11. Click **Save**.

Risk Fabric

Integration Packs | Data Sources | Data Integrations | Job Status

Choose Data Source: User Defined

Create Data Source Edit Refresh

User Defined Datasources

Name	Type / S...	Host	Refreshed
ArcSight Import	File Syst...	symantec-ica...	

Edit Data Source Create Query

Data Source Details

Data Source Label: ArcSight Import

Server Name: symantec-ica.di.ipdr

Authentication Mode: Windows

Username: *****

Password: *****

Download Directory: C:\Temp\processed

12. Right-click the newly created data source and select **Create Query**.

13. Enter a **Query Name** and **Query Description**.

Risk Fabric

Integration Packs | Data Sources | Data Integrations | Job Status

Choose Data Source: User Defined

ArcSight CSV Import

Query Details | Watermarking / Scheduling

Query Name: ArcSight CSV Import

Query Description: Importing AD events from ArcSight exported CSV

Table Name: Leave blank for auto-creation

Days to Retain: 0

Minutes Before Restarting Hanging Jobs:

Delimiter: Leave blank to use system default delimiter

Custom Options:

Timeout (sec): 30

Save Cancel Test Query

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.

Risk Fabric

Integration Packs | Data Sources | Data Integrations | Job Status

Choose Data Source: User Defined

ArcSight CSV Import

Query Details | Watermarking / Scheduling

Minutes Before Restarting Hanging Jobs:

Delimiter: Leave blank to use system default delimiter

Custom Options:

Select which files to import into the table:

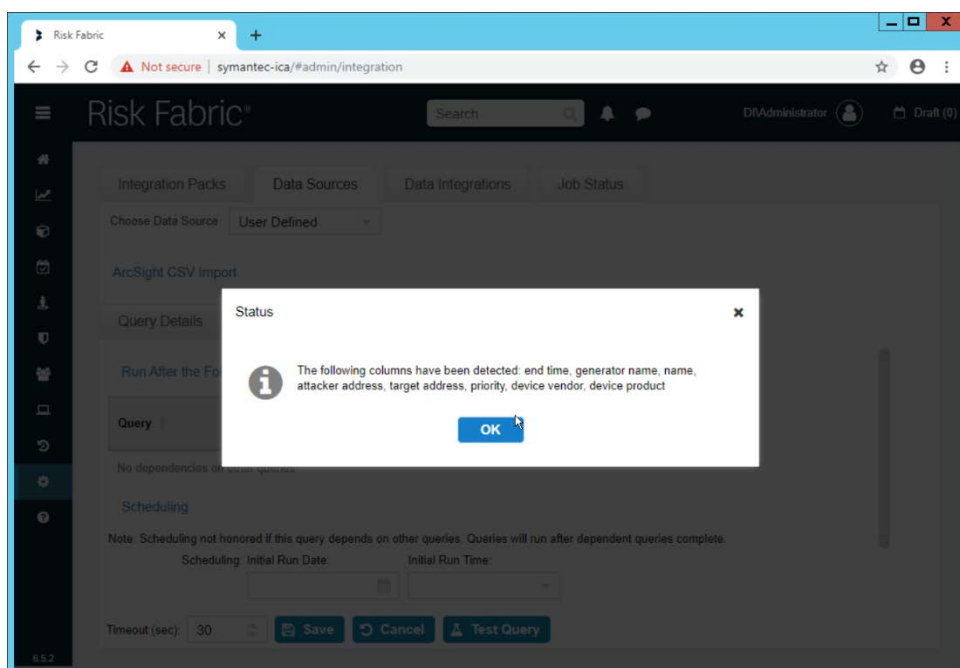
<input checked="" type="checkbox"/> Path	Modified Date
<input checked="" type="checkbox"/> C:\Temp\unprocessed\export_withnulls.csv	10/28/2019 8:27 AM

Note: The destination table will be completely replaced with the latest spreadsheet data

Timeout (sec): 30

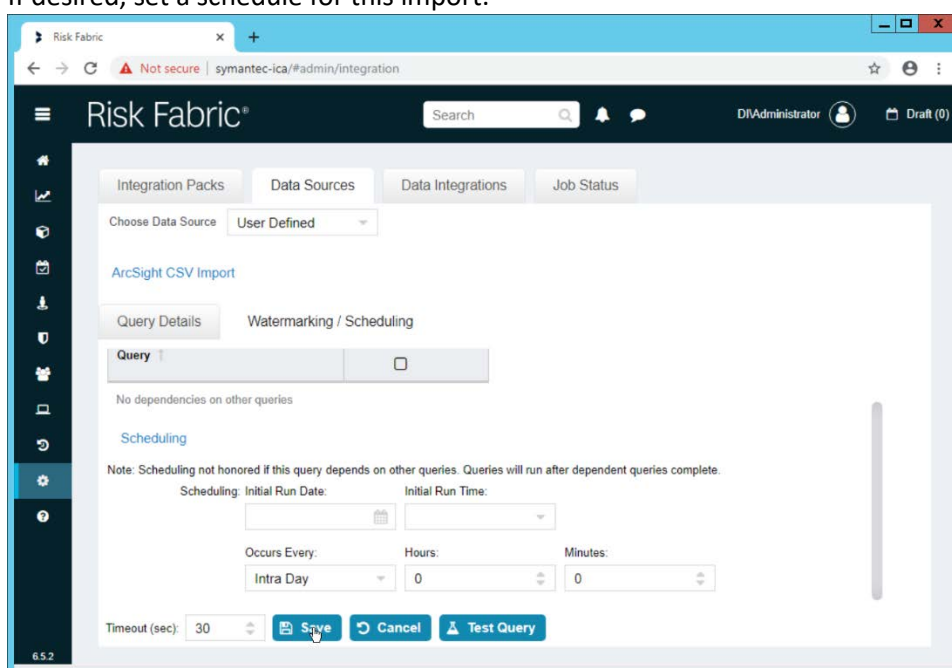
Save Cancel Test Query

16. Click **Save**.

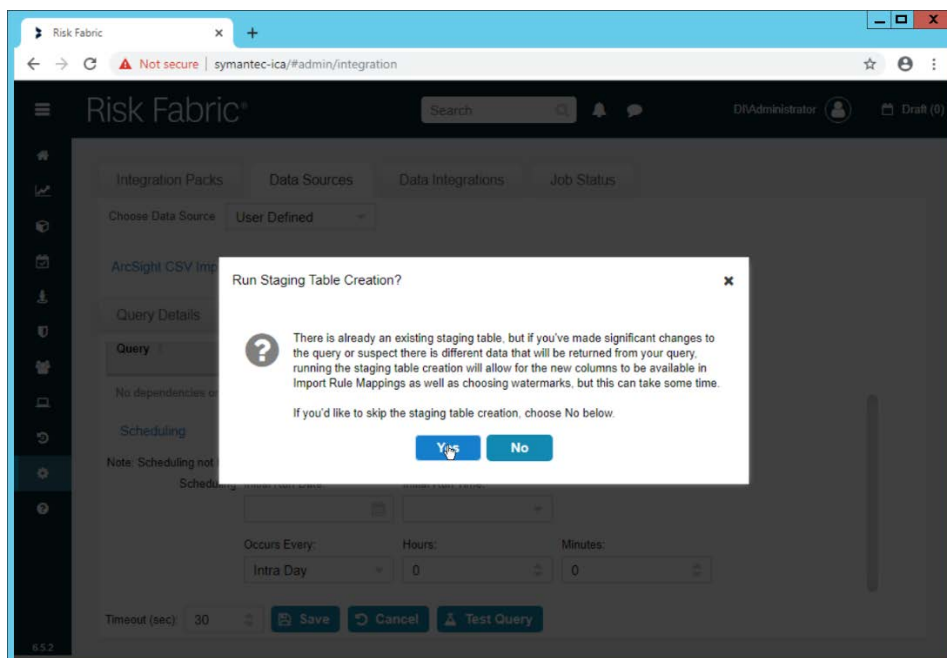


17. Click **OK**.

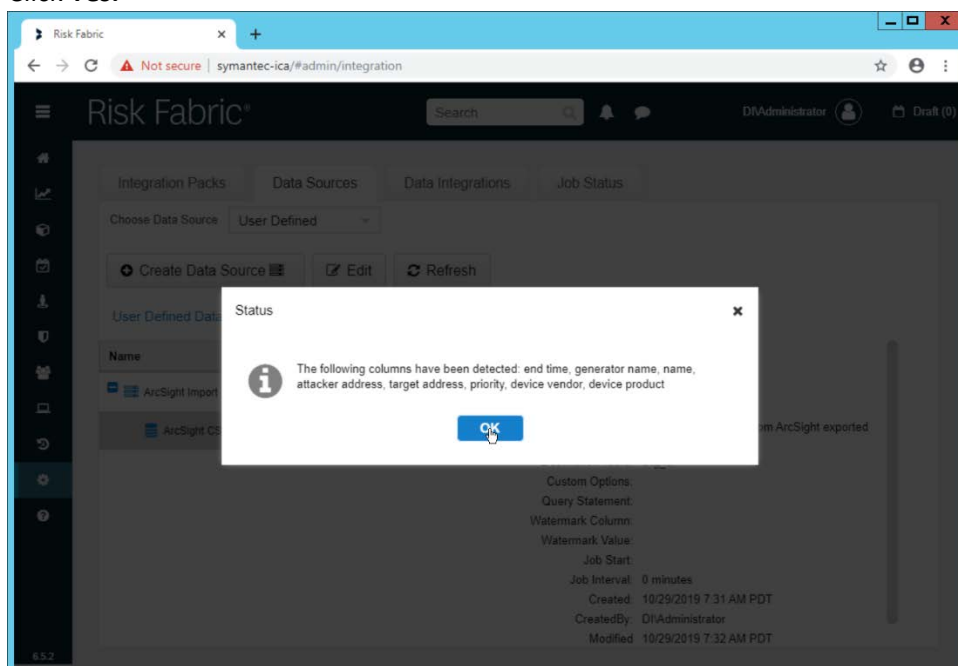
18. If desired, set a schedule for this import.



19. Click **Save**.



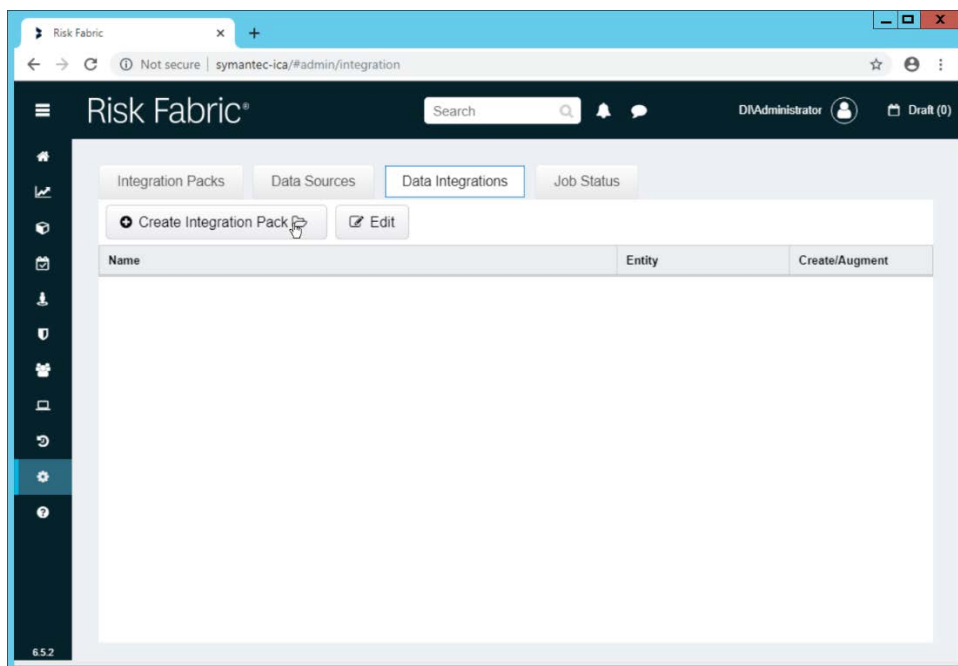
20. Click **Yes**.



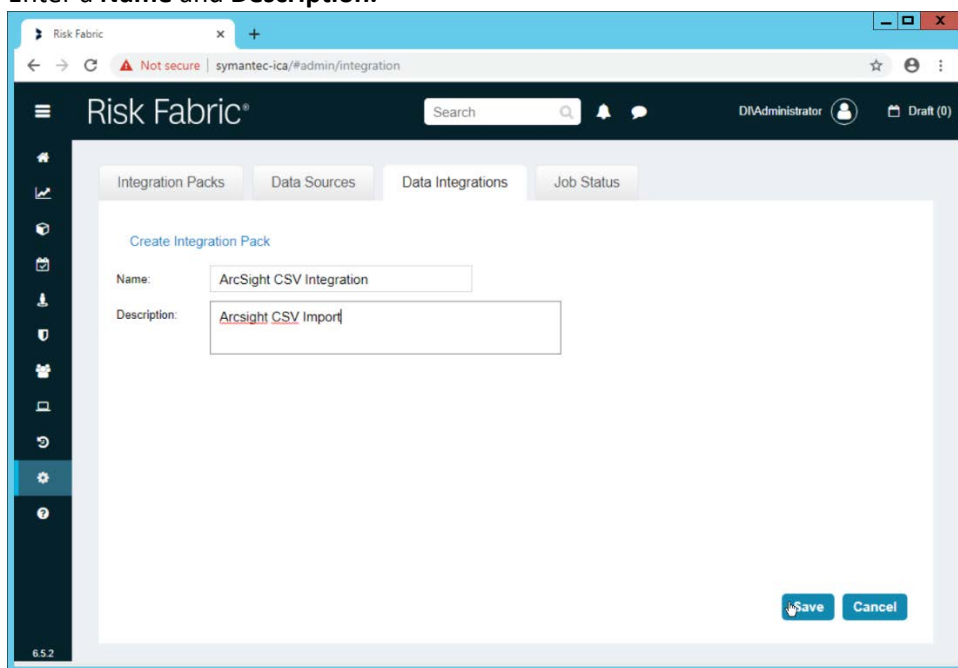
21. Click **OK**.

2.18.3 Create a Mapping between ArcSight events and Symantec ICA

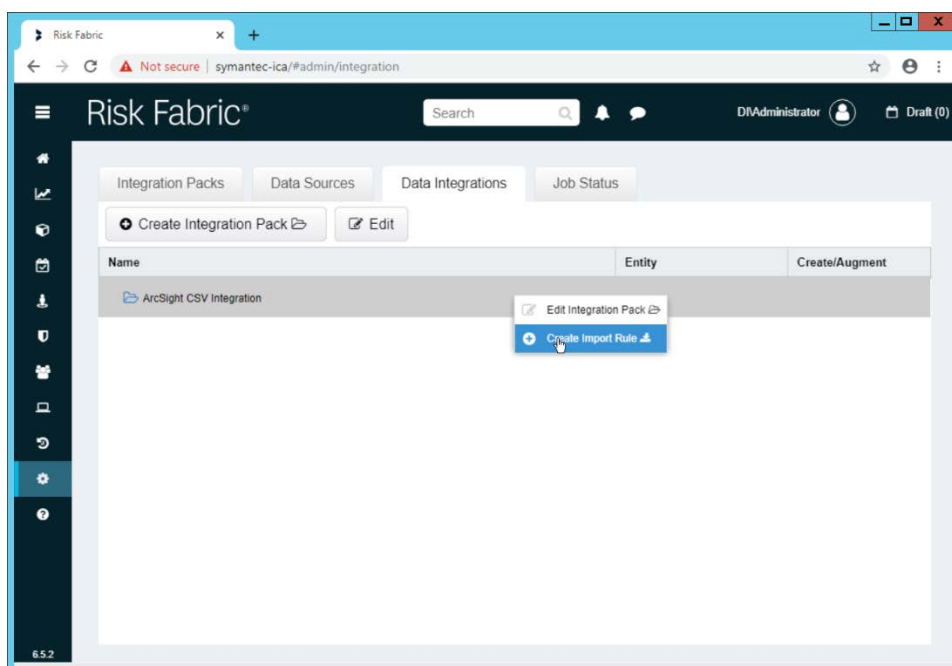
1. Navigate to the **Data Integrations** tab.



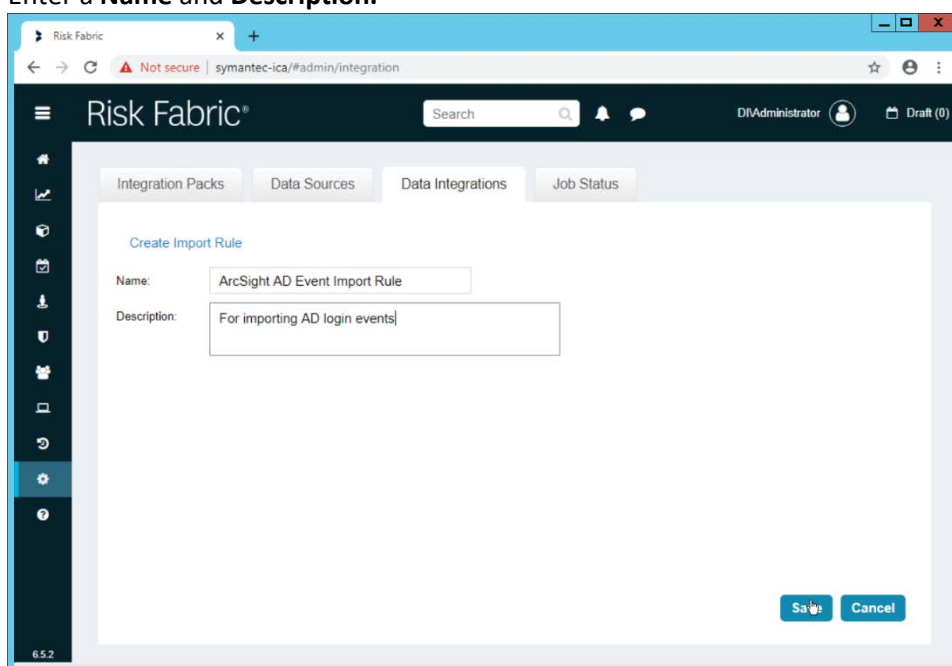
2. Click **Create Integration Pack**.
3. Enter a **Name** and **Description**.



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).

The screenshot shows the Risk Fabric web interface. The browser address bar indicates the URL is symantec-ica/#admin/integration. The interface has a dark blue header with the 'Risk Fabric' logo, a search bar, and user information 'DIAdministrator'. Below the header, there are tabs for 'Integration Packs', 'Data Sources', 'Data Integrations', and 'Job Status'. The 'Data Integrations' tab is active, showing a form titled 'Edit Import Rule Mapping: ArcSight AD Event Import Rule Mapping'. The form contains the following fields:

- Mapping Name: ArcSight AD Event Import Rule Mapping
- Description: AD events
- Data Source: ArcSight Import
- Query: ArcSight CSV Import
- Risk Fabric Processing Watermark: 528
- Run Intra-Day: No
- Run Order: 0
- Entity Type: EP Events
- Update Pre-Process Table: Yes
- Create Entities: Yes

At the bottom of the form are 'Save' and 'Cancel' buttons. The version number '6.5.2' is visible in the bottom left corner of the interface.

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.

Required Fields

Entity Column	Type	Value	Default Value
EventDate datetime	Source Column	End Time	
SourceEventID nvarchar(50)	Formula	Convert unique &	

Optional Fields

Search:

Entity Column	Type	Value	Default Value
---------------	------	-------	---------------

Save Cancel

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.

Create Import Rule Mapping

EventObjectTypeName
nvarchar(254)

Source Column

Create and Associate Event Activity Type

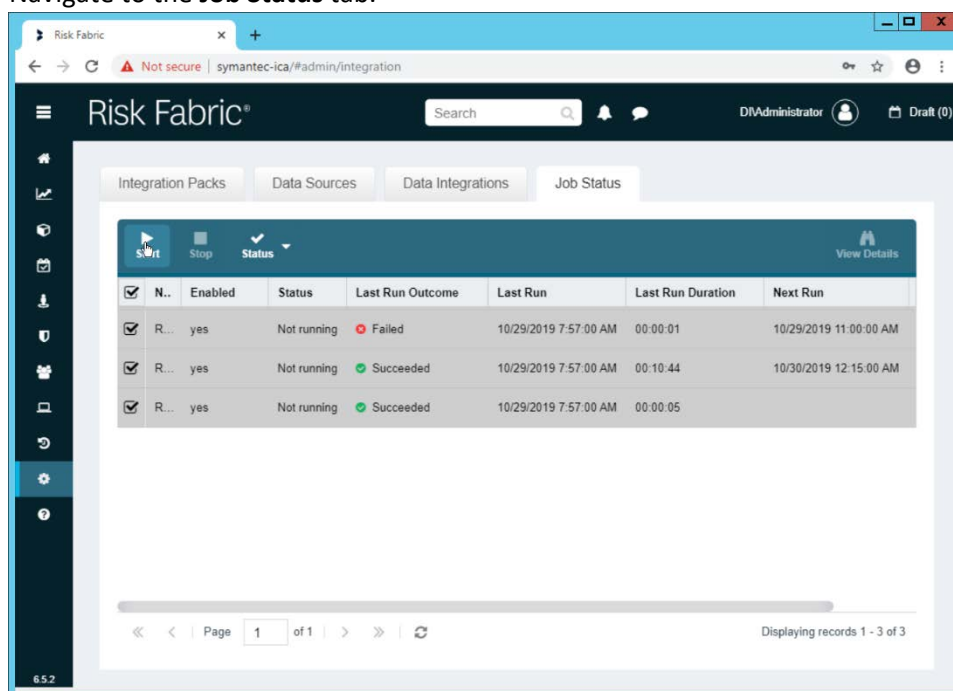
Entity Column	Type	Value	Default Value
EventActivityTypeName nvarchar(254)	Source Column		

Create and Associate Event Rule

Entity Column	Type	Value	Default Value
EventRuleName nvarchar(1000)	Source Column		

Save Cancel

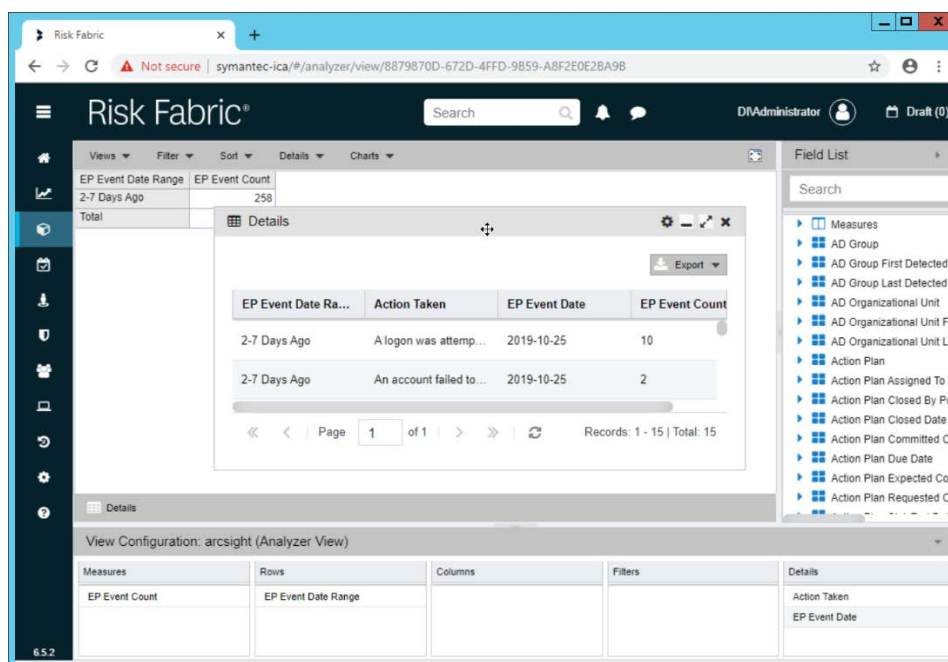
18. Click **Save** when finished.
19. Navigate to the **Job Status** tab.



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**.



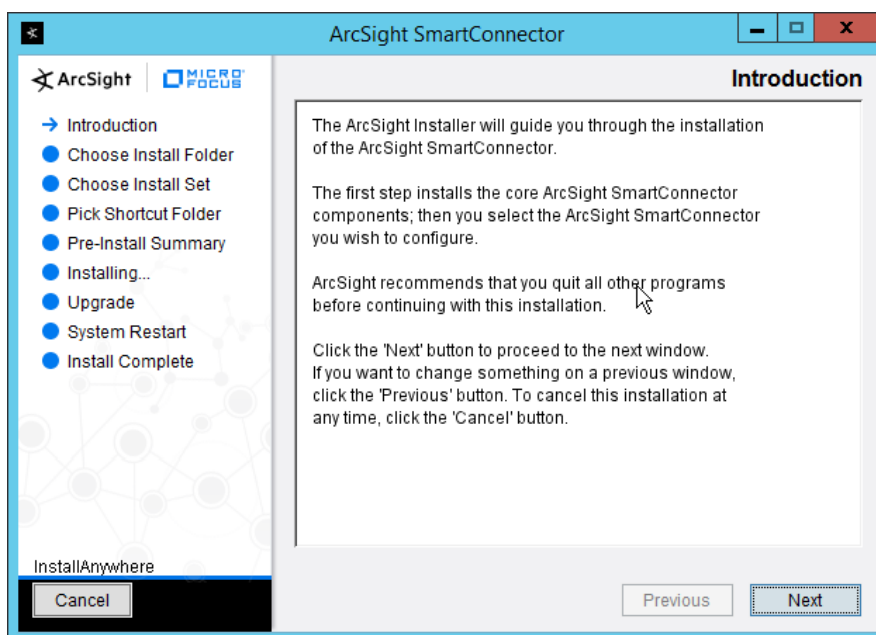
2. Drag mapped columns (from the import rule mapping you created) from the list on the right to view them in the analyzer.

2.19 Integration: Micro Focus ArcSight and Tripwire

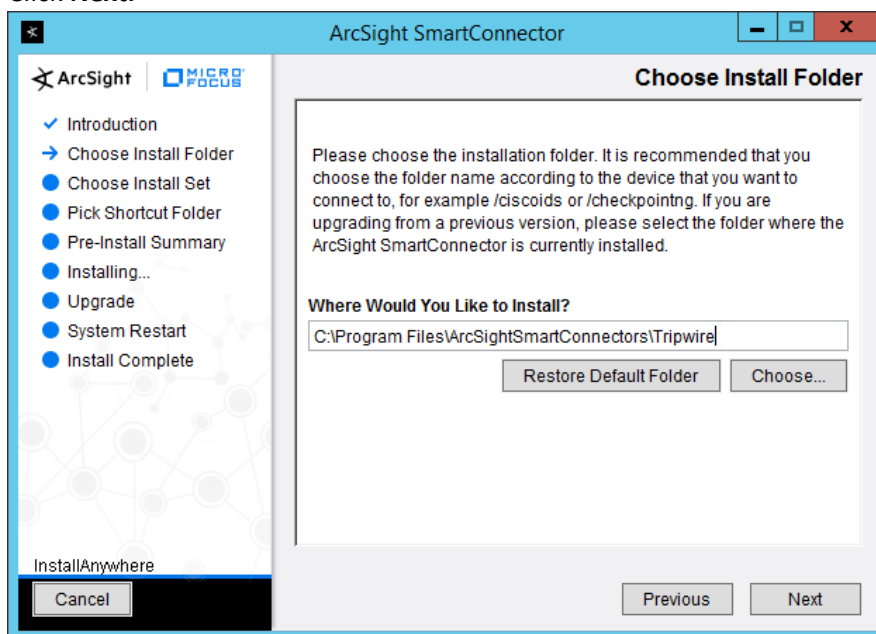
This section will detail the forwarding of logs from **Tripwire Log Center** to **Micro Focus ArcSight**. This will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight**, assuming those logs are being collected by **Tripwire Log Center**.

2.19.1 Install Micro Focus ArcSight

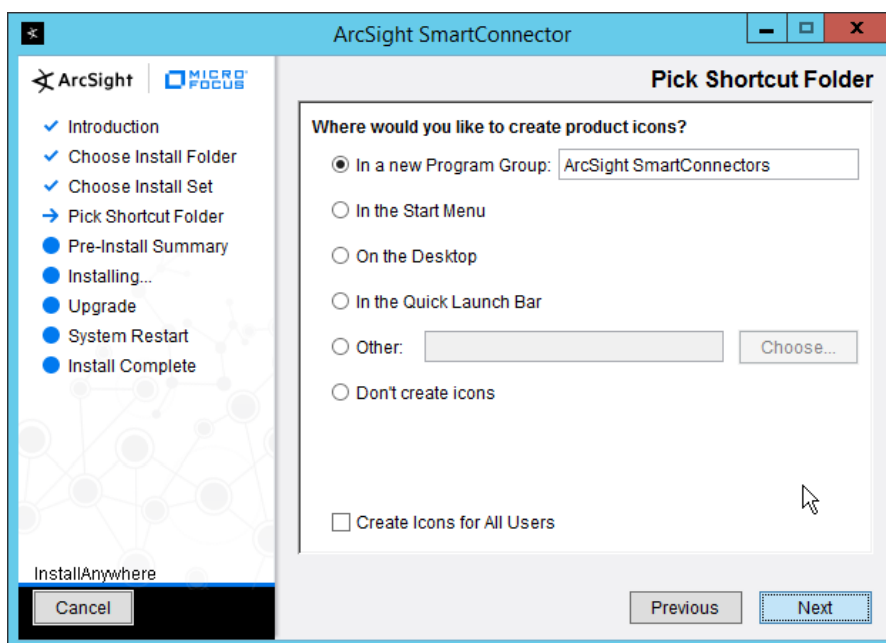
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Tripwire Log Center**.



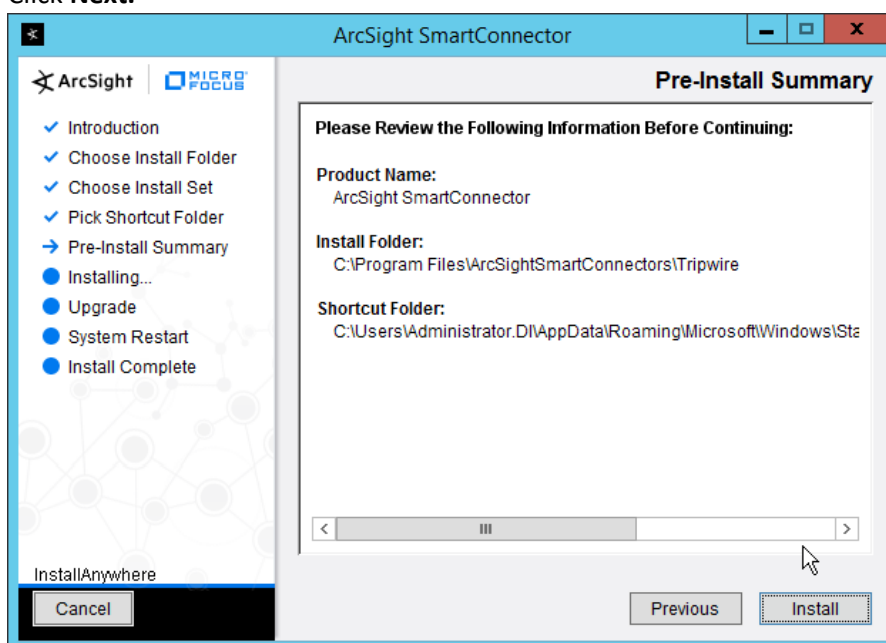
2. Click **Next**.



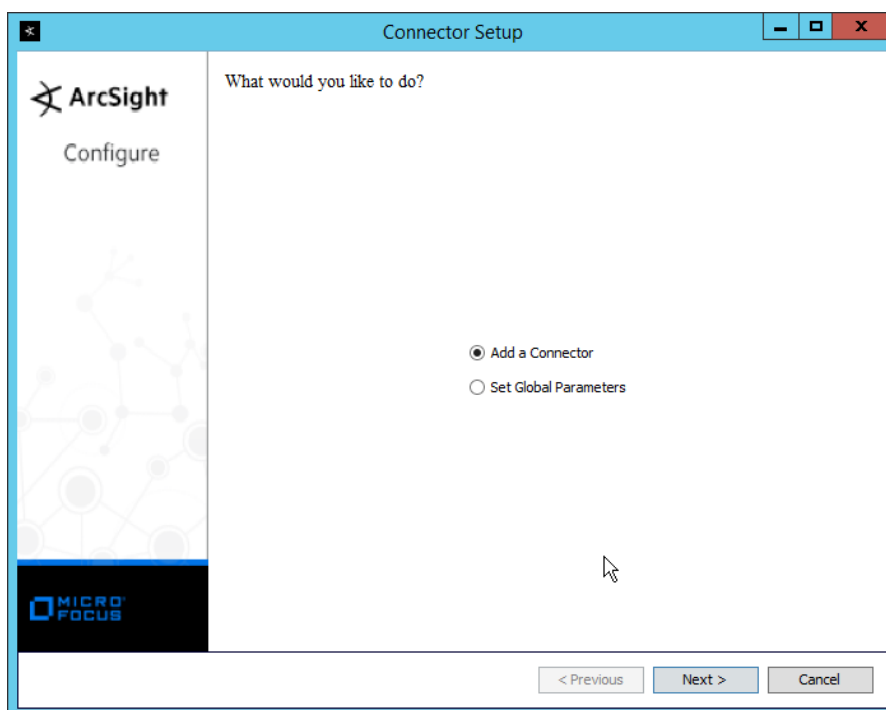
3. Enter *C:\Program Files\ArcSightSmartConnectors\Tripwire*.



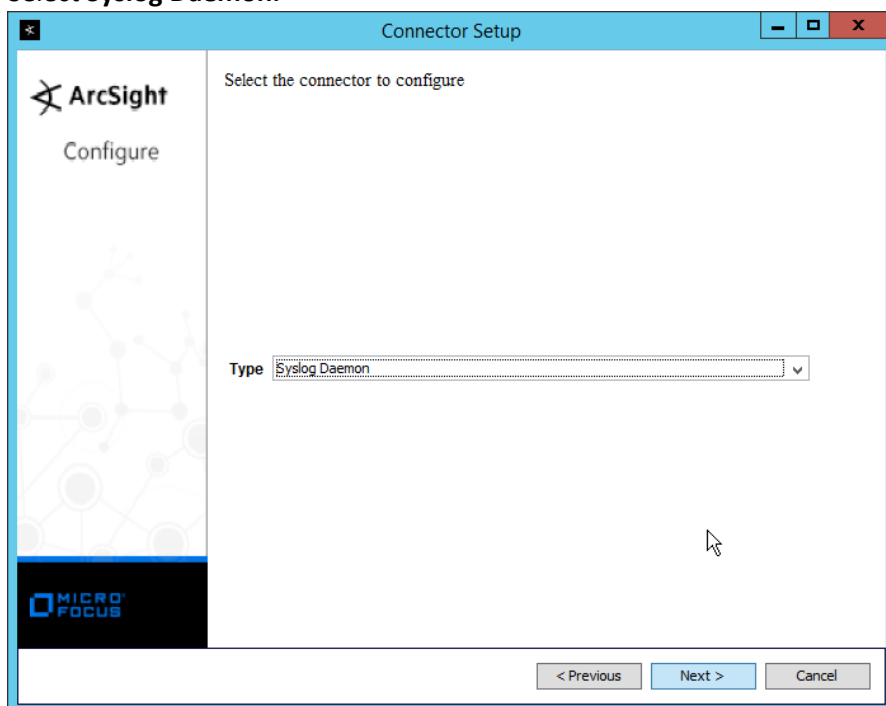
4. Click **Next**.



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



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



9. Click **Next**.

10. Enter a port for the daemon to run on.

11. Select **Raw TCP** for **Protocol**.

Connector Setup

ArcSight
Configure

Enter the parameter details

Network Port: 514

IP Address: (ALL)

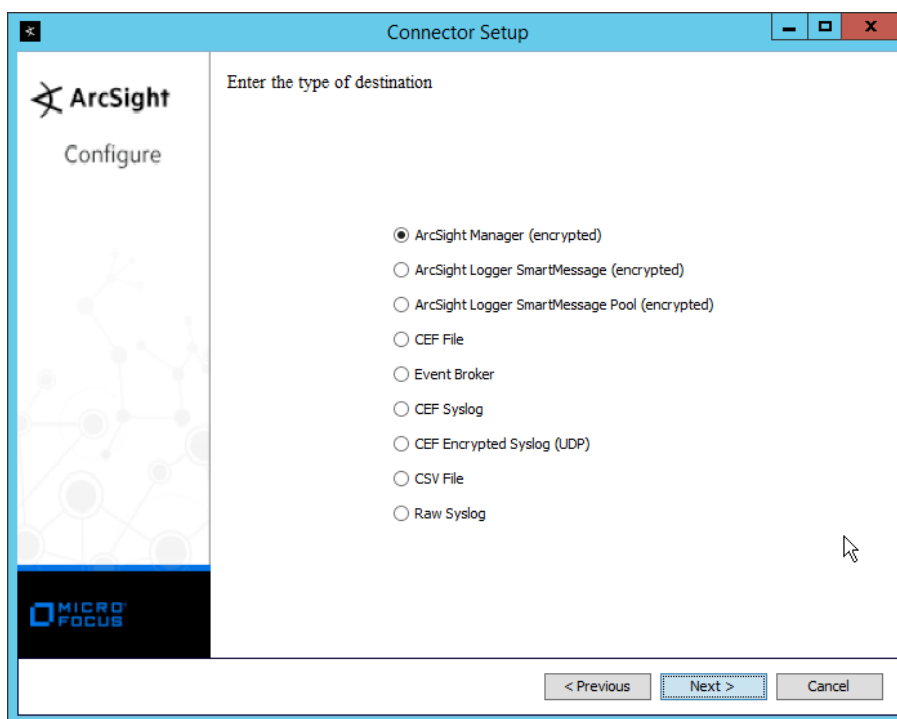
Protocol: Raw TCP

Forwarder: false

< Previous Next > Cancel

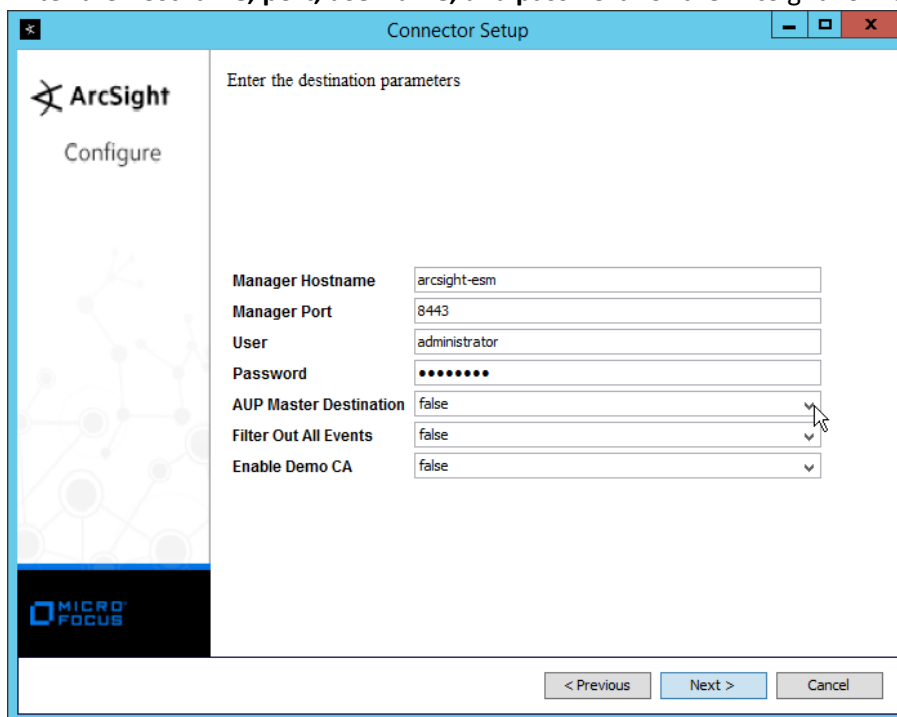
12. Click **Next**.

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



14. Click **Next**.

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



16. Click **Next**.

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

Connector Setup

ArcSight
Configure

Enter the connector details

Name: Tripwire Log Center

Location:

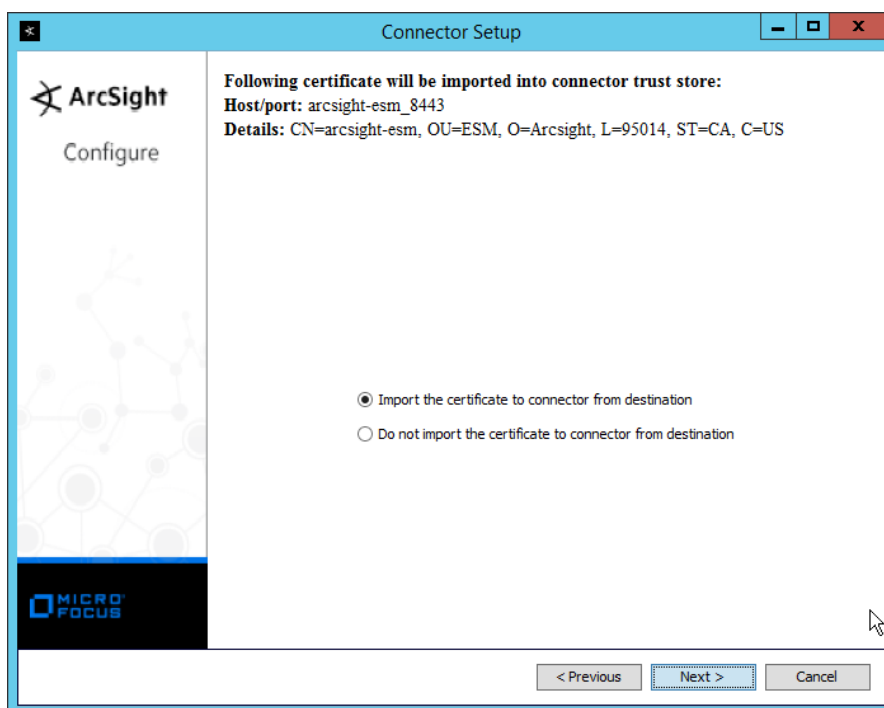
DeviceLocation:

Comment:

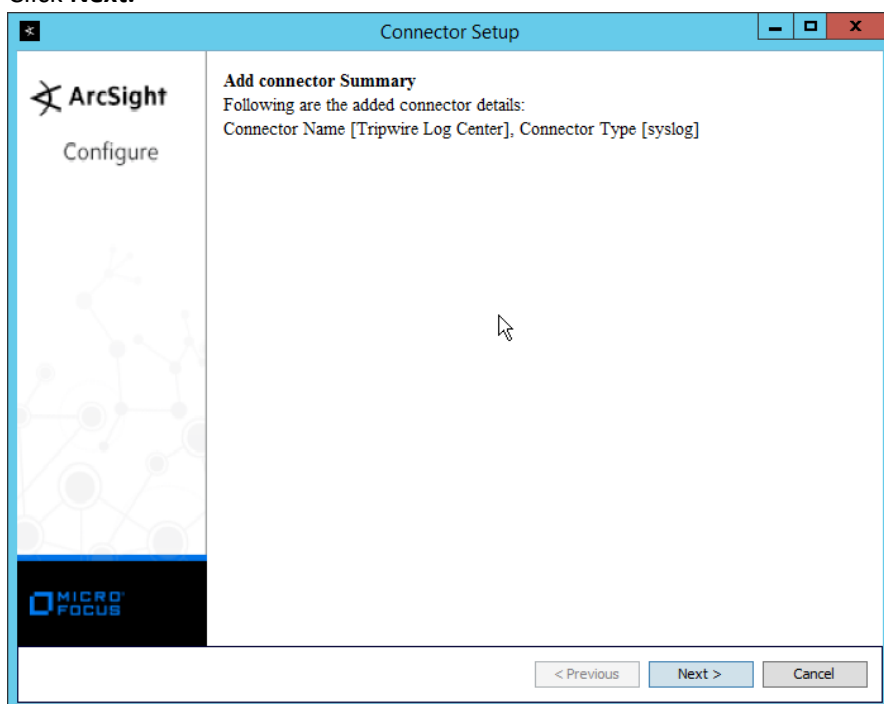
< Previous Next > Cancel

18. Click **Next**.

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

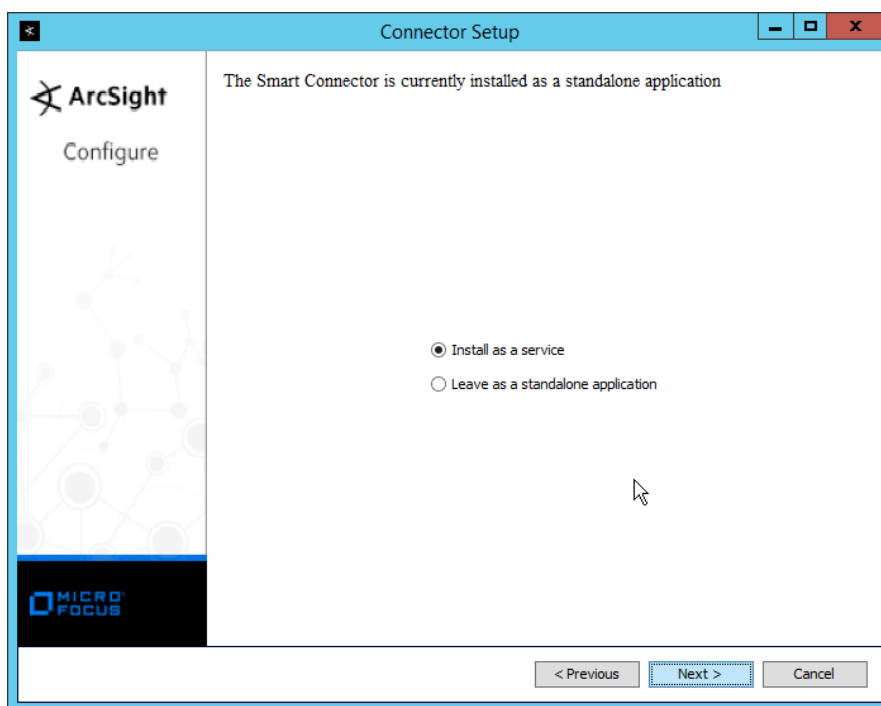


20. Click **Next**.

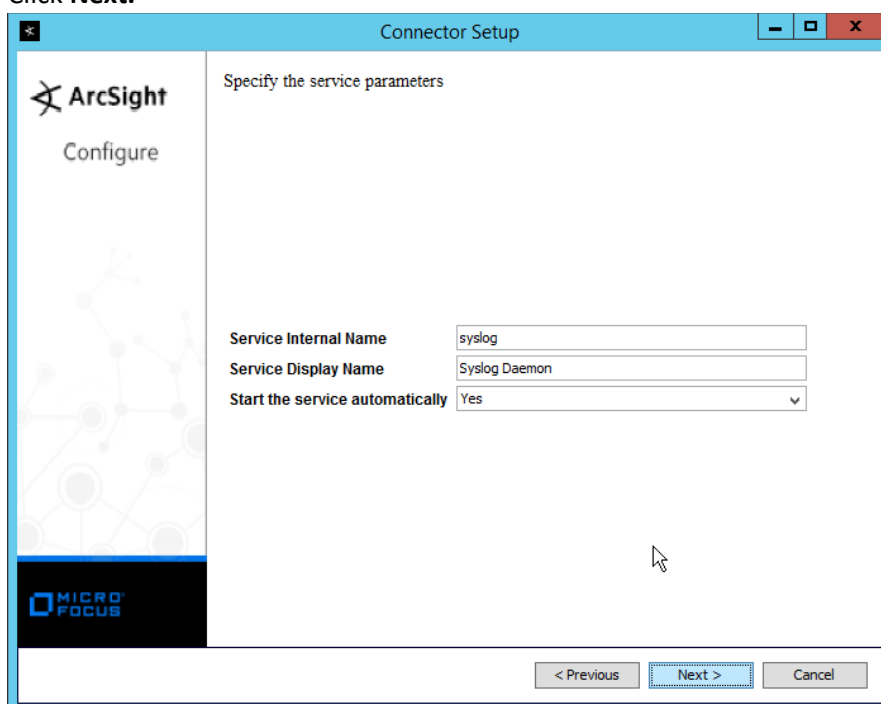


21. Click **Next**.

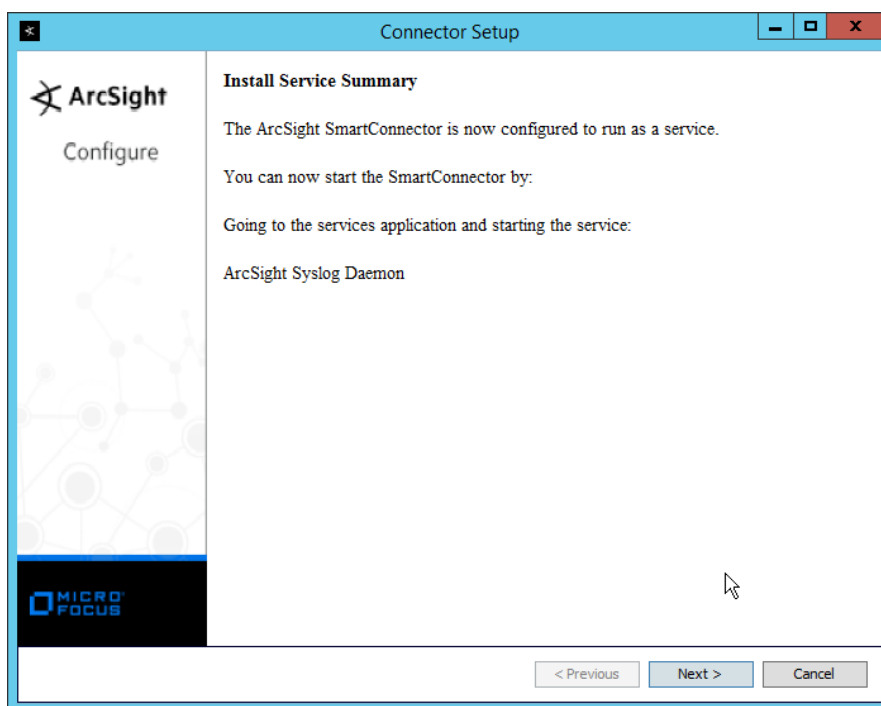
22. Select **Install as a service**.



23. Click **Next**.

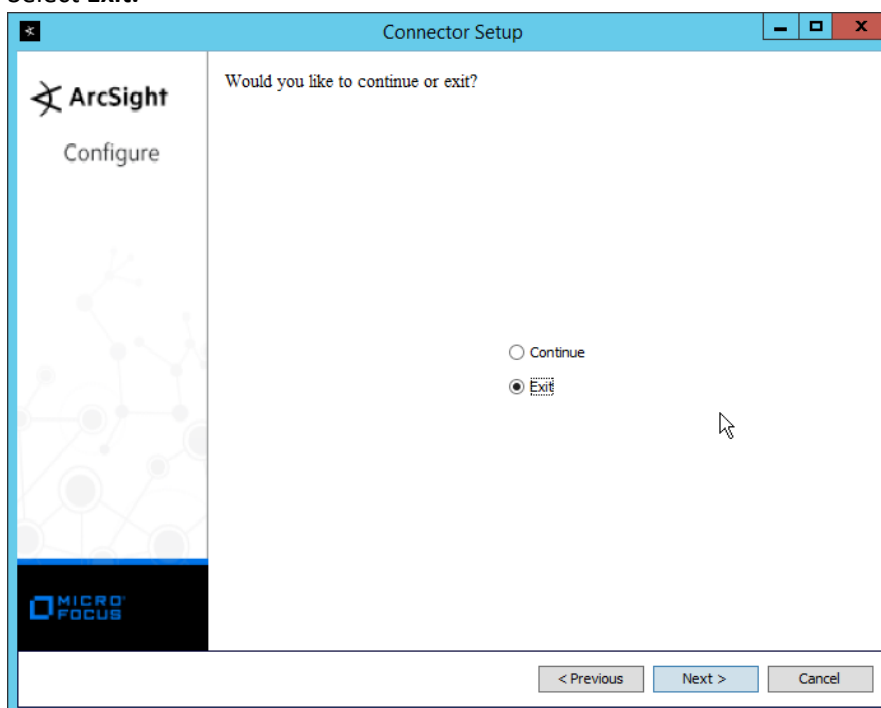


24. Click **Next**.

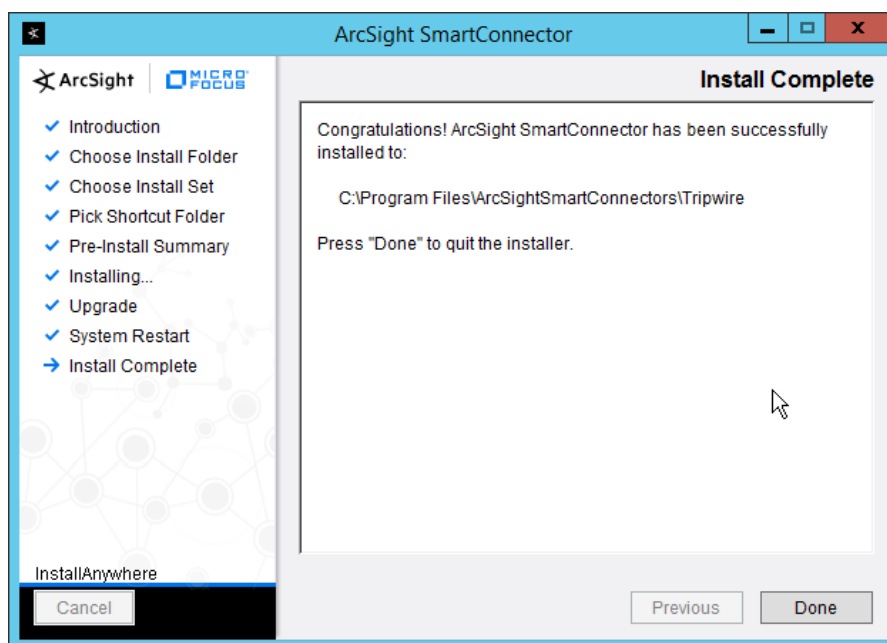


25. Click **Next**.

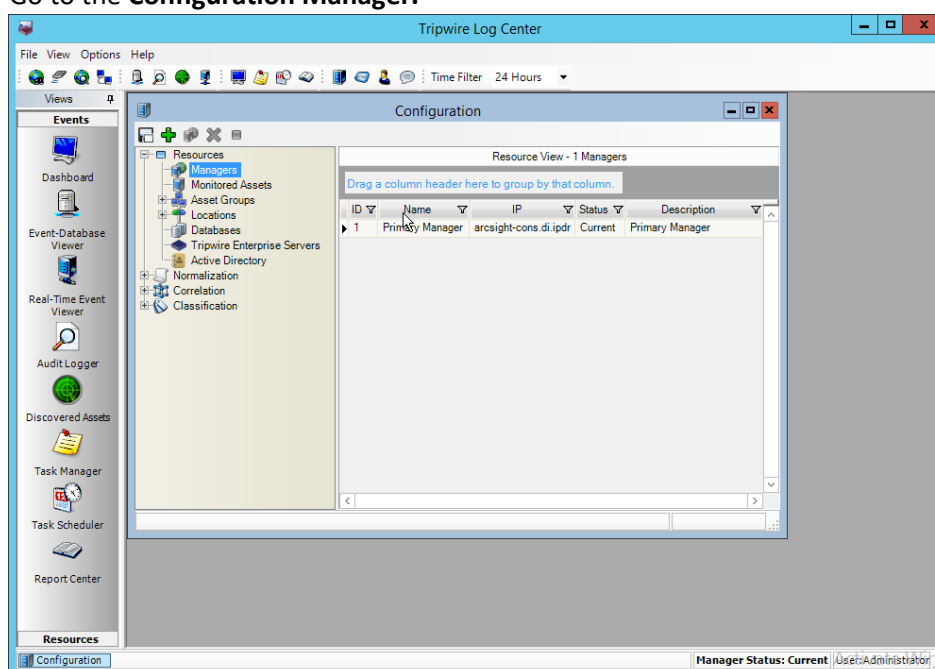
26. Select **Exit**.



27. Click **Next**.

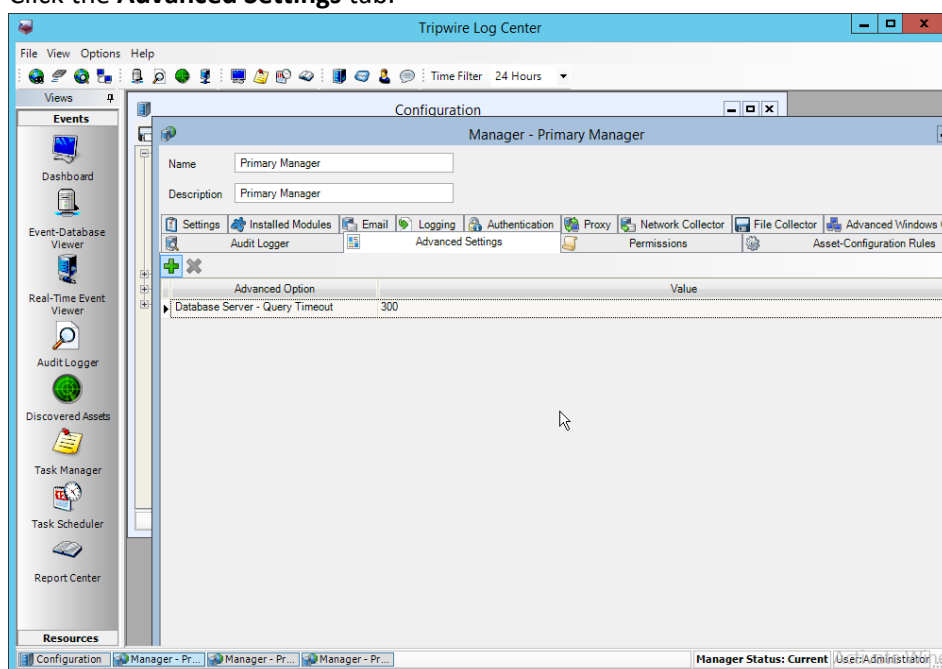


28. Click **Done**.
29. Open the **Tripwire Log Center Console**.
30. Go to the **Configuration Manager**.



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

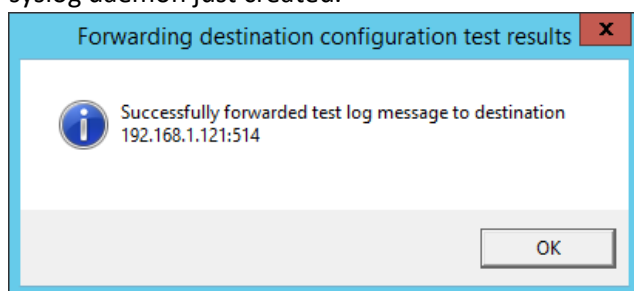
33. Click the **Advanced Settings** tab.



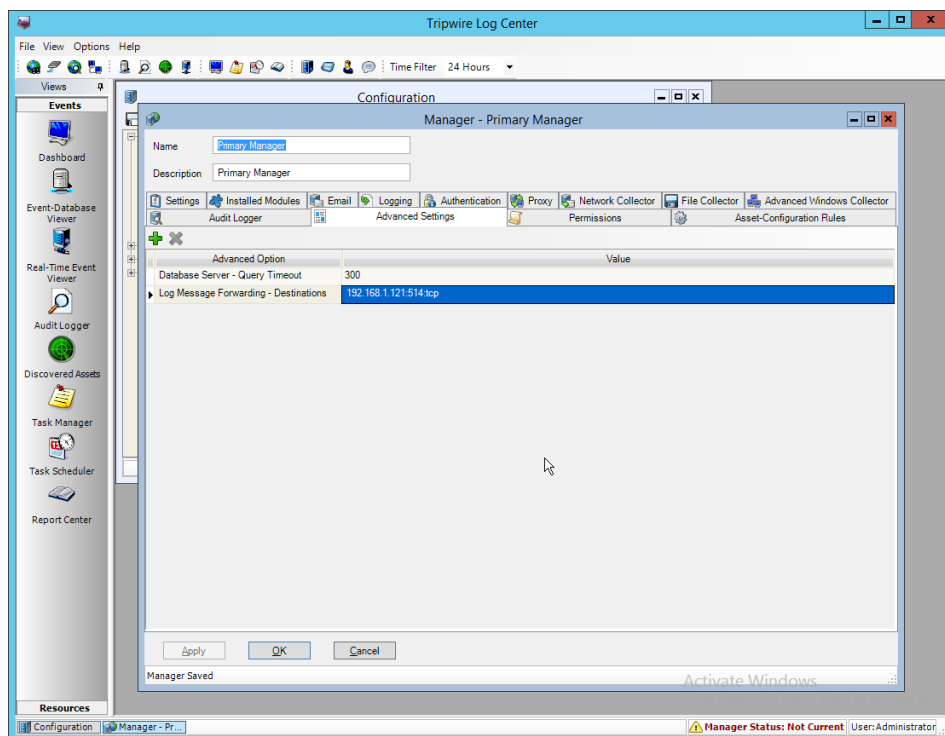
34. Click the **Add** button.

35. In the **Advanced Option** box select **Log Message Forwarding – Destinations**.

36. In the **Value** box next to it, type `<ip_address>:<port>:tcp` with the IP address and port of the syslog daemon just created.



37. Click **OK**.



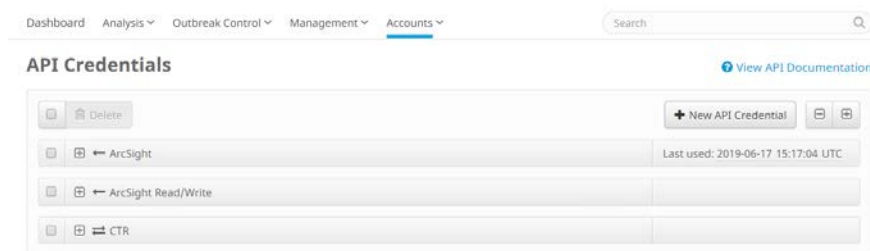
38. Click **OK**.
39. Restart the **Tripwire Log Center Manager**.

2.20 Integration: Micro Focus ArcSight and Cisco AMP

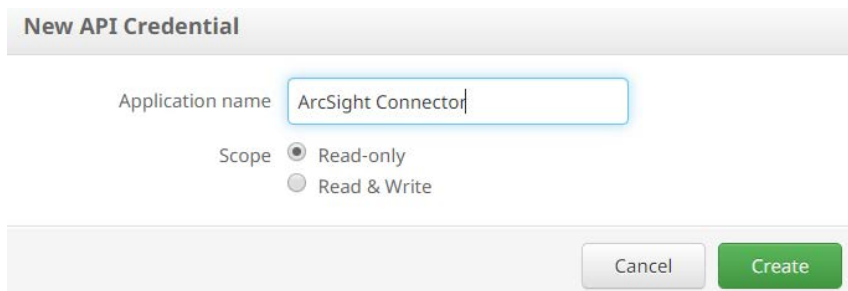
This section will detail the collection of logs from **Cisco AMP's** REST APIs using **Micro Focus ArcSight**.

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**.



New API Credential

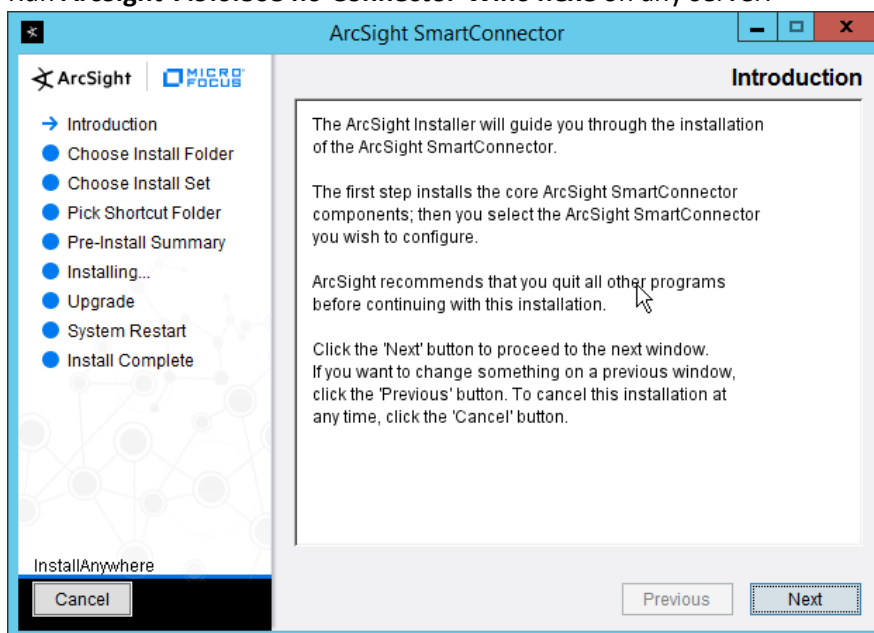
Application name:

Scope: ☒ Read-only ☐ Read & Write

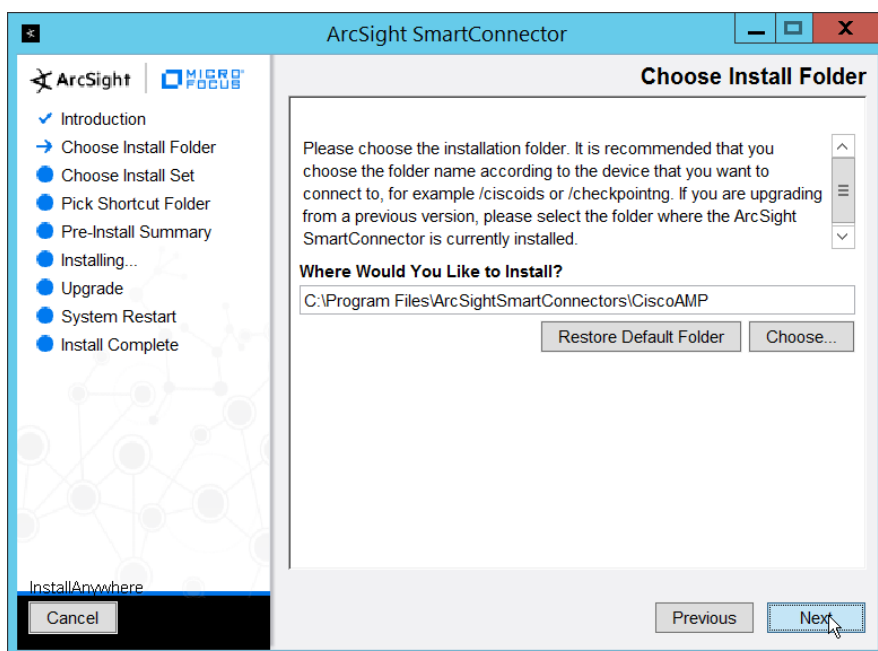
5. Click **Create**.
6. This will direct you to a page with an **ID** and **API Key**. Keep track of these, as you will need them in the setup for the ArcSight Connector, and Cisco AMP may not let you view them again.

2.20.2 Install Micro Focus ArcSight

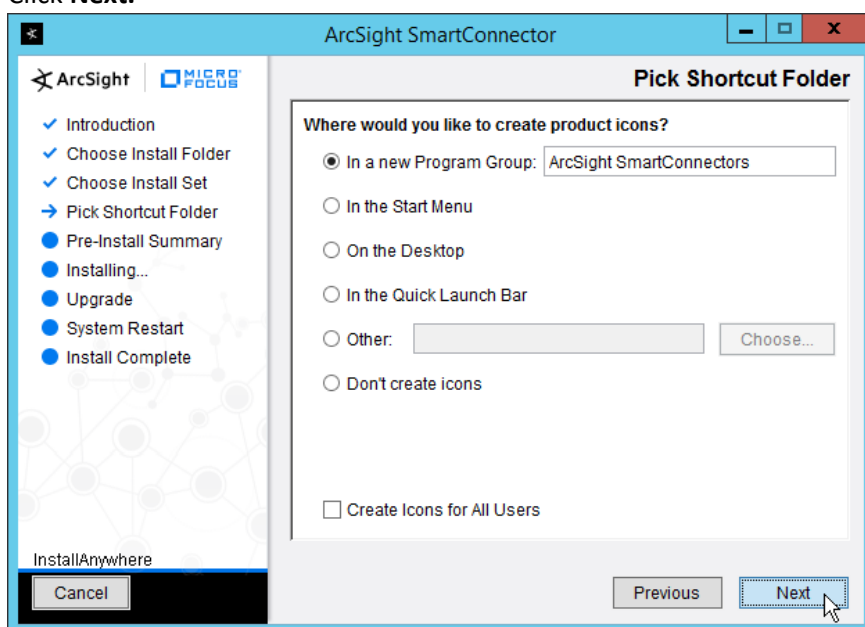
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server.



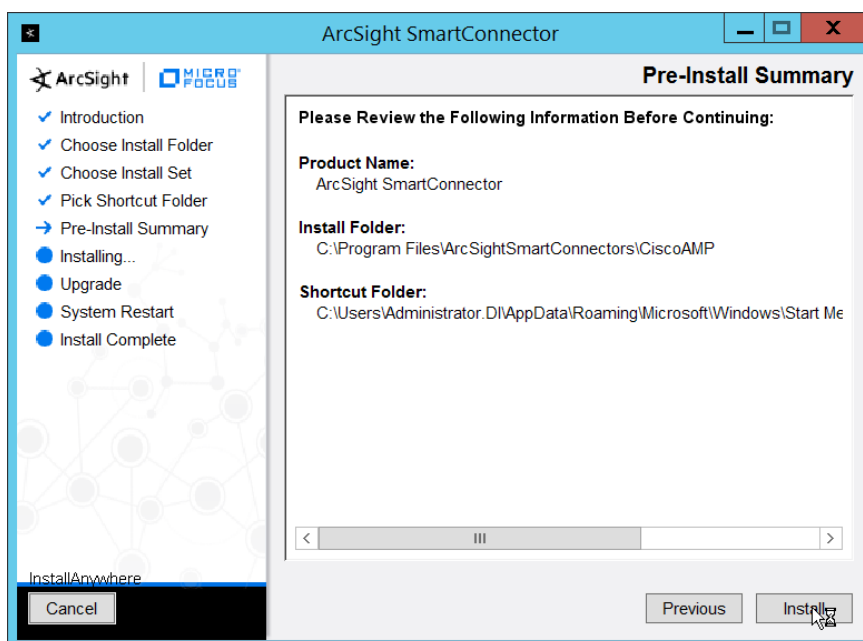
2. Click **Next**.
3. Enter **C:\Program Files\ArcSightSmartConnectors\CiscoAMP**.



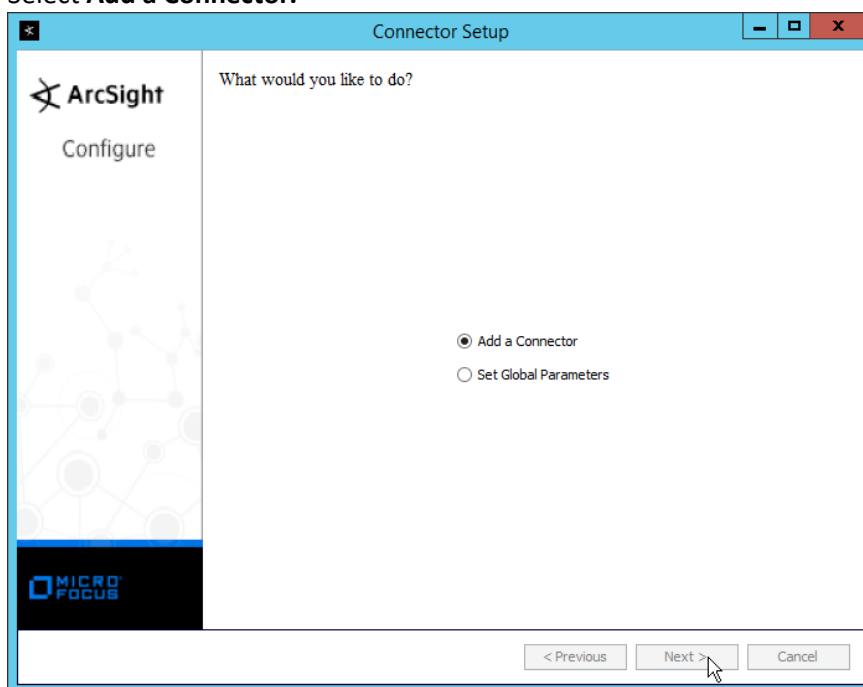
4. Click **Next**.



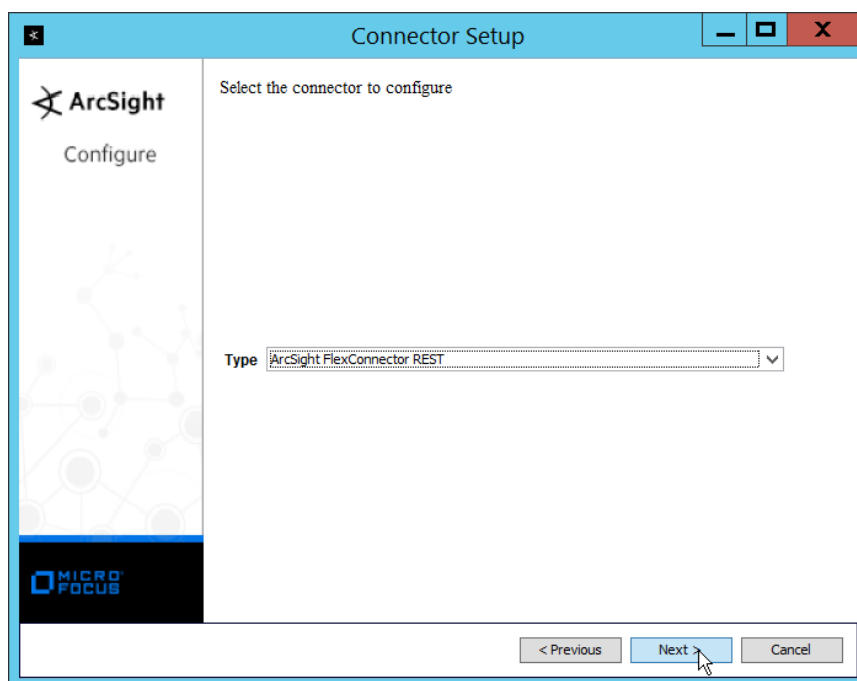
5. Click **Next**.



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](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](#).

The screenshot shows the 'Connector Setup' window with the title bar. On the left is the ArcSight logo and a 'Configure' button. The main area is titled 'Enter the parameter details'. It contains the following fields:

- Proxy Host: [Empty text box]
- Proxy Port: [Empty text box]
- Proxy User Name: [Empty text box]
- Proxy Password: [Empty text box]
- Configuration File: [Cisco_AMP]
- Events URL: [https://api.amp.cisco.com/v1/events?start_date=\$START]
- Authentication Type: [Basic (dropdown menu)]
- User Name: [Redacted with black box]
- Password: [Redacted with black box]
- OAuth2 Client Properties File: [Empty text box with a small icon]
- Refresh Token: [Empty text box]

At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

14. Click **Next**.

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

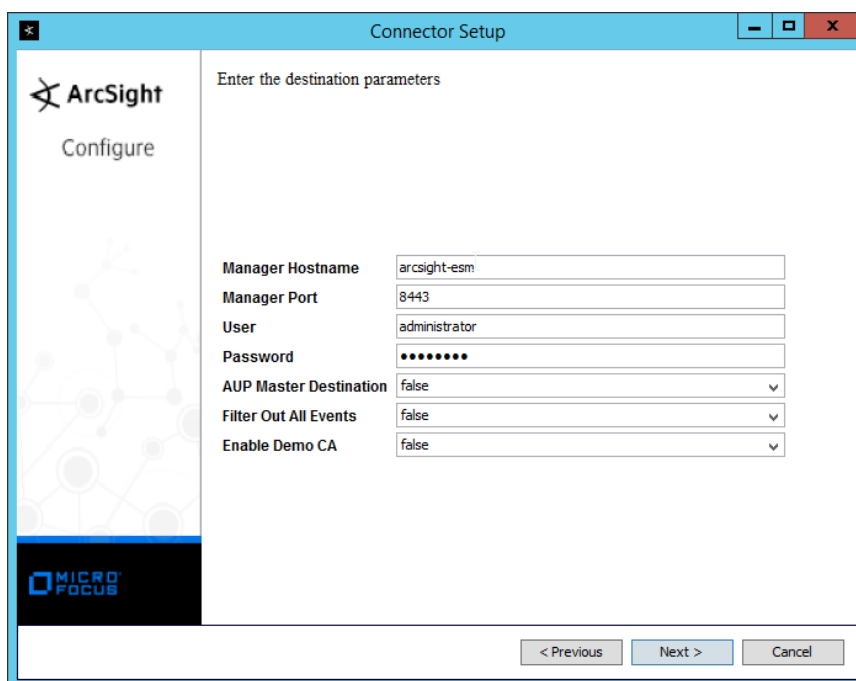
The screenshot shows the 'Connector Setup' window with the title bar. On the left is the ArcSight logo and a 'Configure' button. The main area is titled 'Enter the type of destination'. It contains a list of radio button options:

- ☒ ArcSight Manager (encrypted)
- ☐ ArcSight Logger SmartMessage (encrypted)
- ☐ ArcSight Logger SmartMessage Pool (encrypted)
- ☐ CEF File
- ☐ Event Broker
- ☐ CEF Syslog
- ☐ CEF Encrypted Syslog (UDP)
- ☐ CSV File
- ☐ Raw Syslog

At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

16. Click **Next**.

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



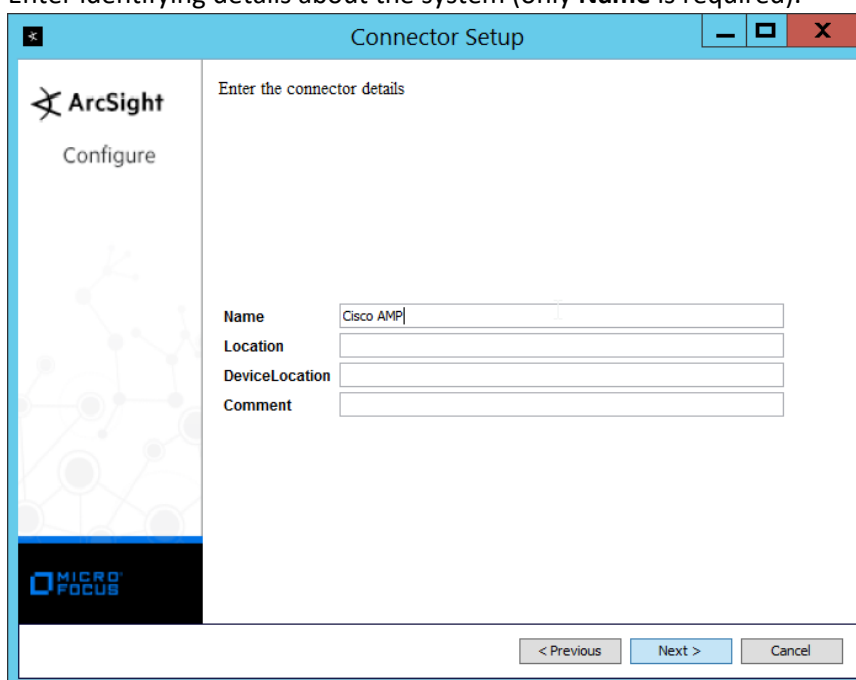
The screenshot shows the 'Connector Setup' window with the 'Enter the destination parameters' step. The left sidebar contains the ArcSight logo and a 'Configure' button. The main area has a form with the following fields:

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

At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

18. Click **Next**.

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



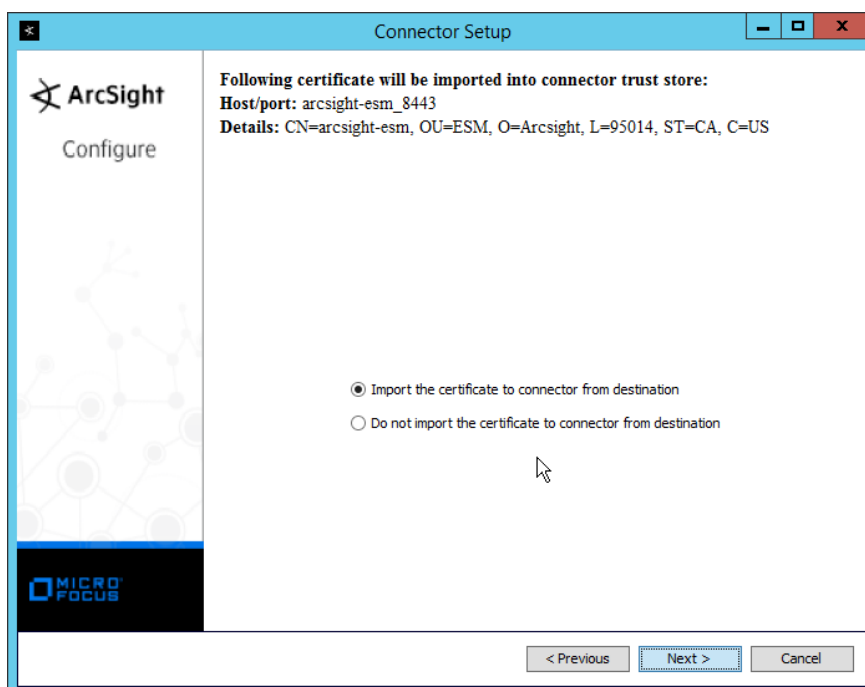
The screenshot shows the 'Connector Setup' window with the 'Enter the connector details' step. The left sidebar contains the ArcSight logo and a 'Configure' button. The main area has a form with the following fields:

Name	Cisco AMP
Location	
DeviceLocation	
Comment	

At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

20. Click **Next**.

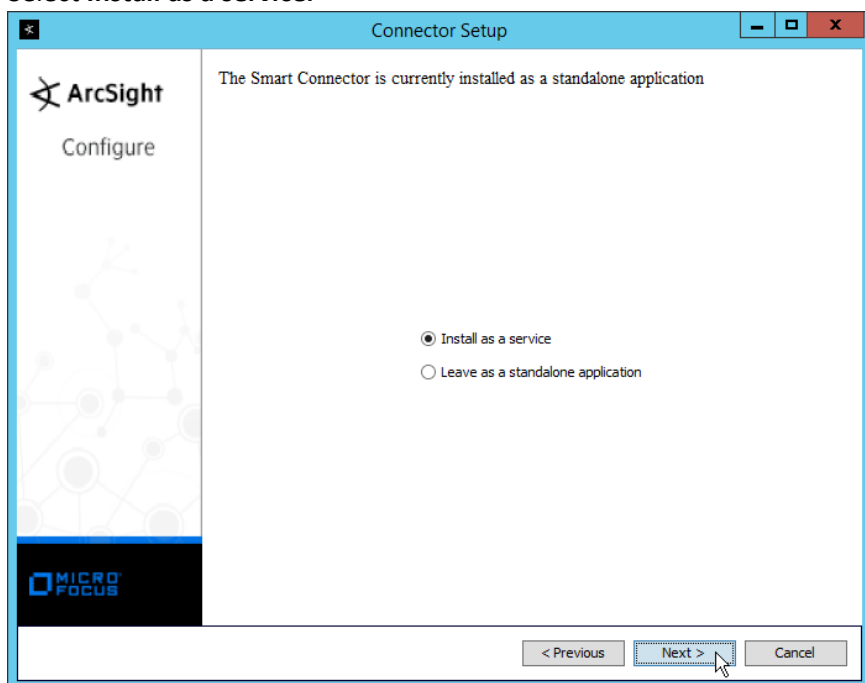
21. Select **Import the certificate to connector from destination**.



22. Click **Next**.

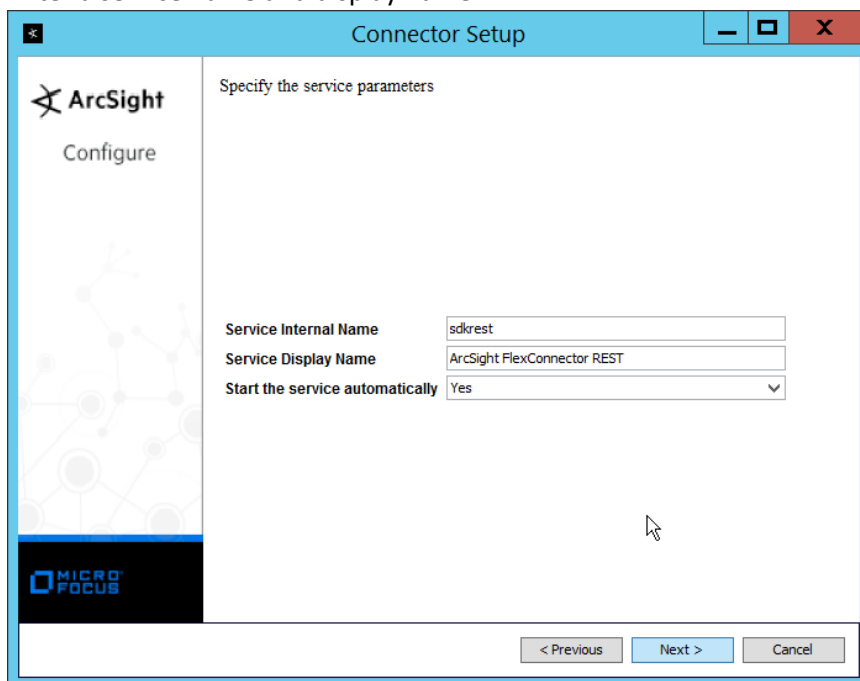
23. Click **Next**.

24. Select **Install as a service**.



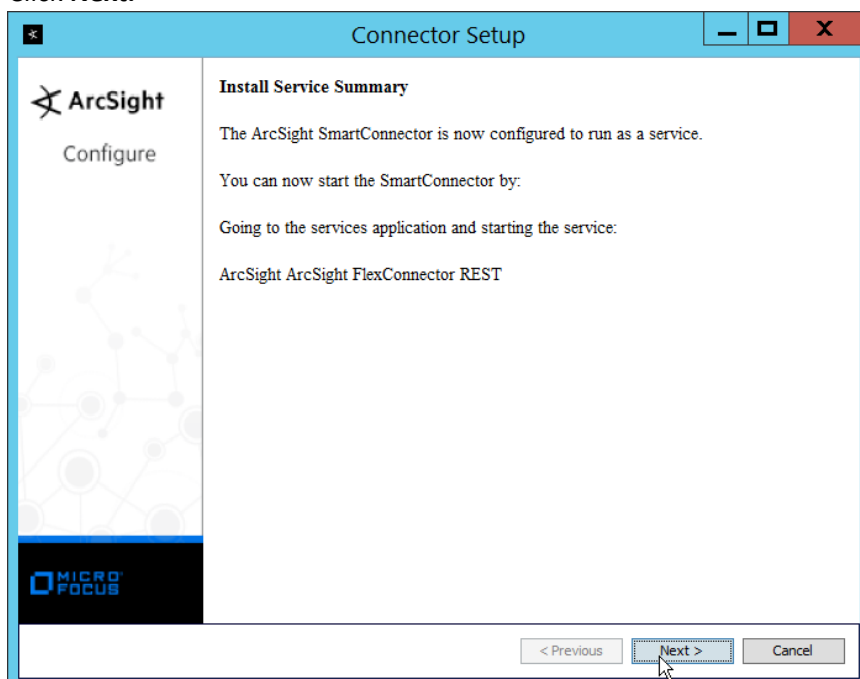
25. Click **Next**.

26. Enter a service name and display name.



The screenshot shows the 'Connector Setup' window with the 'Specify the service parameters' section. The left sidebar contains the ArcSight logo and a 'Configure' button. The main area has three input fields: 'Service Internal Name' with the value 'sdkrest', 'Service Display Name' with the value 'ArcSight FlexConnector REST', and 'Start the service automatically' with a dropdown menu set to 'Yes'. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

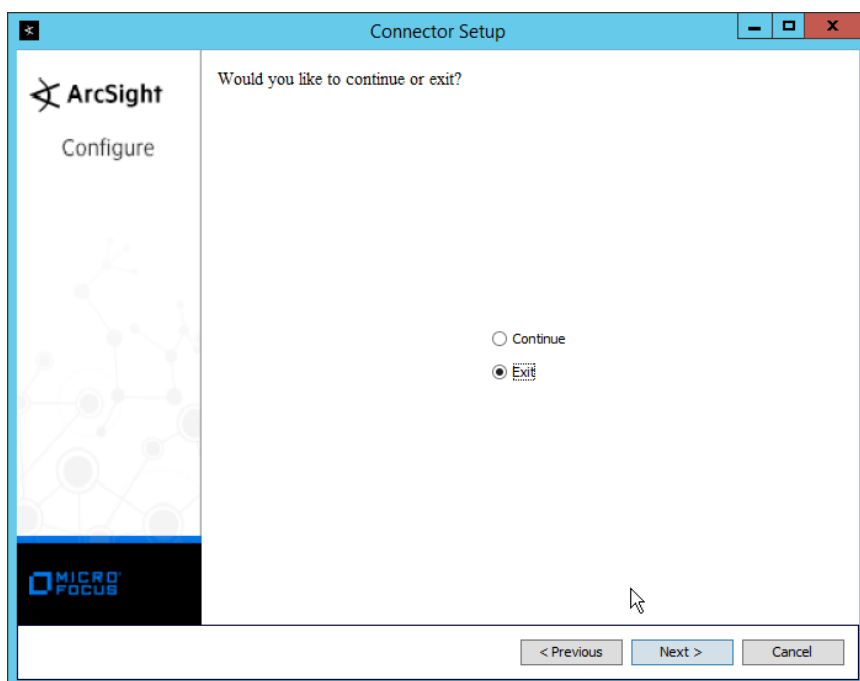
27. Click **Next**.



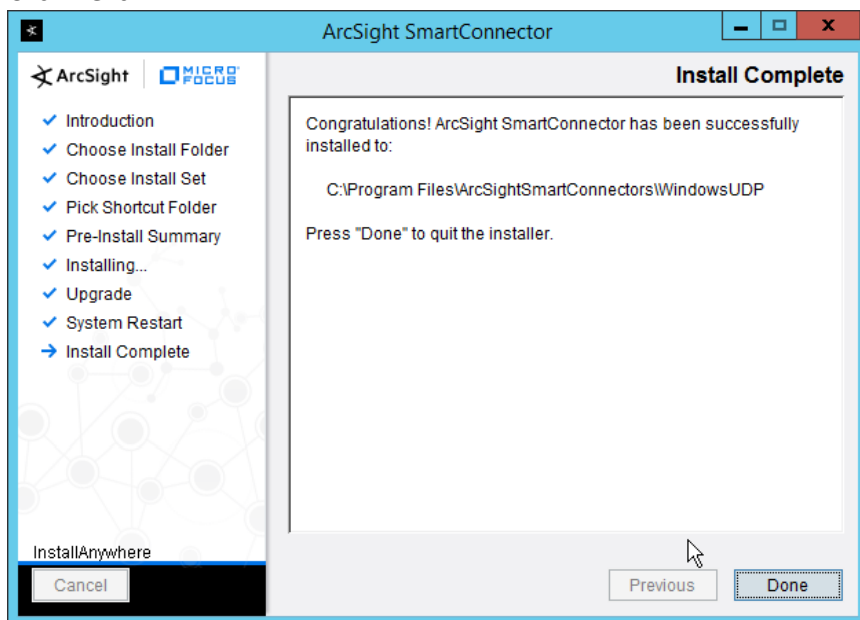
The screenshot shows the 'Connector Setup' window with the 'Install Service Summary' section. The left sidebar is the same as in the previous step. The main area contains the following text: 'The ArcSight SmartConnector is now configured to run as a service.', 'You can now start the SmartConnector by:', 'Going to the services application and starting the service:', and 'ArcSight ArcSight FlexConnector REST'. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

28. Click **Next**.

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.

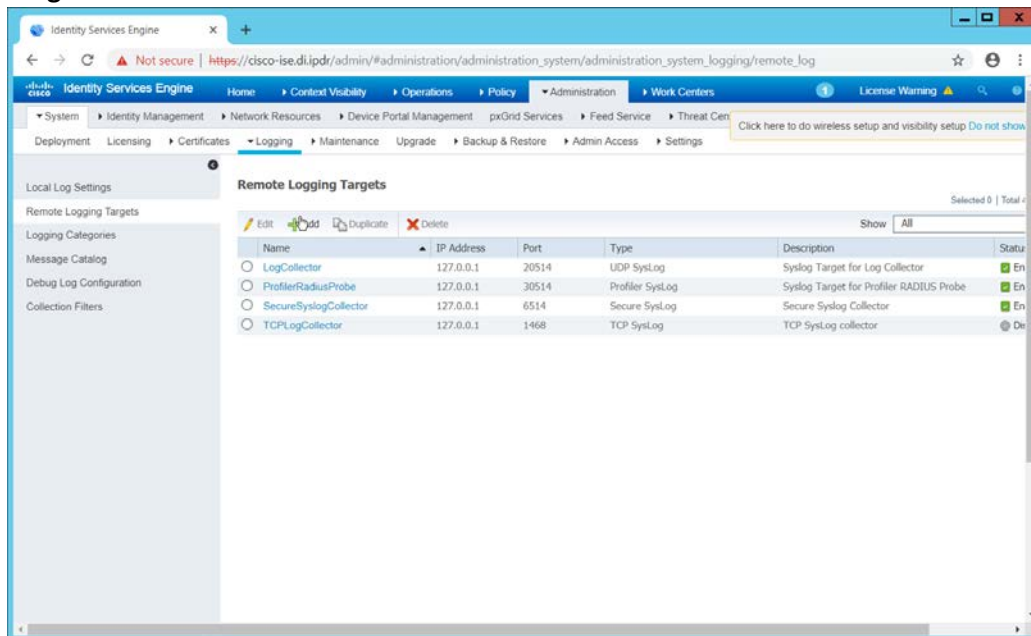
2.21 Integration: Micro Focus ArcSight and Cisco ISE

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—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**.

Identity Services Engine

Not secure | https://cisco-ise.dupdr/admin/#administration/administration_system/administration_system_logging/remote_log

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Center

Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Local Log Settings

Remote Logging Targets

Logging Categories

Message Catalog

Debug Log Configuration

Collection Filters

Remote Logging Targets List > New Logging Target

Logging Target

* Name: ArcSight Target Type: TCP SysLog

Description: Status: Enabled

* Host / IP Address: backupserv.dupdr

* Port: 514 (Valid Range 1 to 65535)

Facility Code: LOCAL6

* Maximum Length: 8192 (Valid Range 200 to 8192)

Include Alarms For this Target: ☐

Buffer Messages When Server Down: ☐

Enable Server Identity Check: ☐

Buffer Size (MB): 100 (Valid Range 10 to 100)

Reconnect Timeout (Sec): 30 (Valid Range 30 to 120)

Submit Cancel

9. Click **Submit**.

Identity Services Engine

Not secure | https://cisco-ise.dupdr/admin/#administration/administration_system/administration_system_logging/remote_log

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Center

Deployment > Licensing > Certificates > Logging > Maintenance > Upgrade > Backup & Restore > Admin Access > Settings

Local Log Settings

Remote Logging Targets

Logging Categories

Message Catalog

Debug Log Configuration

Collection Filters

Remote Logging Targets List > New Logging Target

Logging Target

* Name: ArcSight Target Type: TCP SysLog

Description: Status: Enabled

* Host / IP Address: backupserv.dupdr

* Port: 514 (Valid Range 1 to 65535)

Facility Code: LOCAL6

* Maximum Length: 8192 (Valid Range 200 to 8192)

Include Alarms For this Target: ☐

Buffer Messages When Server Down: ☐

Enable Server Identity Check: ☐

Buffer Size (MB): 100 (Valid Range 10 to 100)

Reconnect Timeout (Sec): 30 (Valid Range 30 to 120)

Submit Cancel

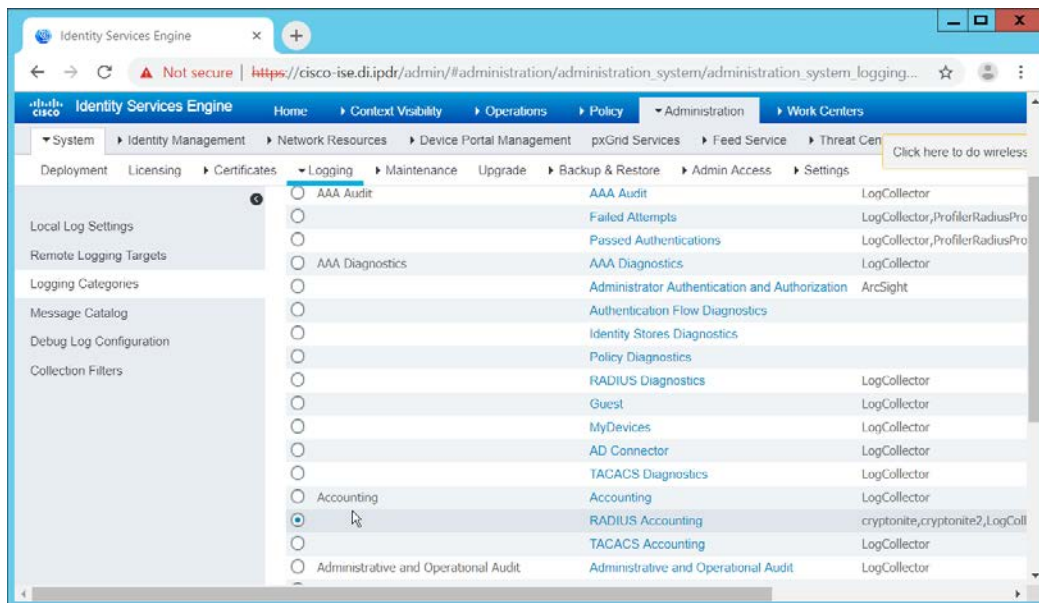
You have chosen to create an insecure (TCP/UDP) connection to the server. Are you sure you want to proceed?

No Yes

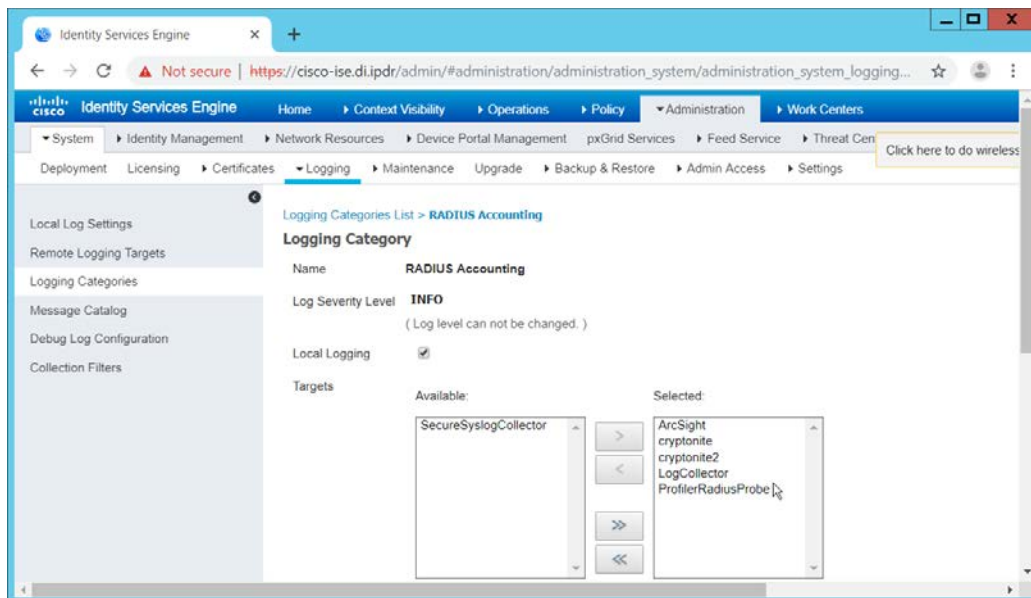
10. Click **Yes**.

2.21.2 Select Logs for Forwarding

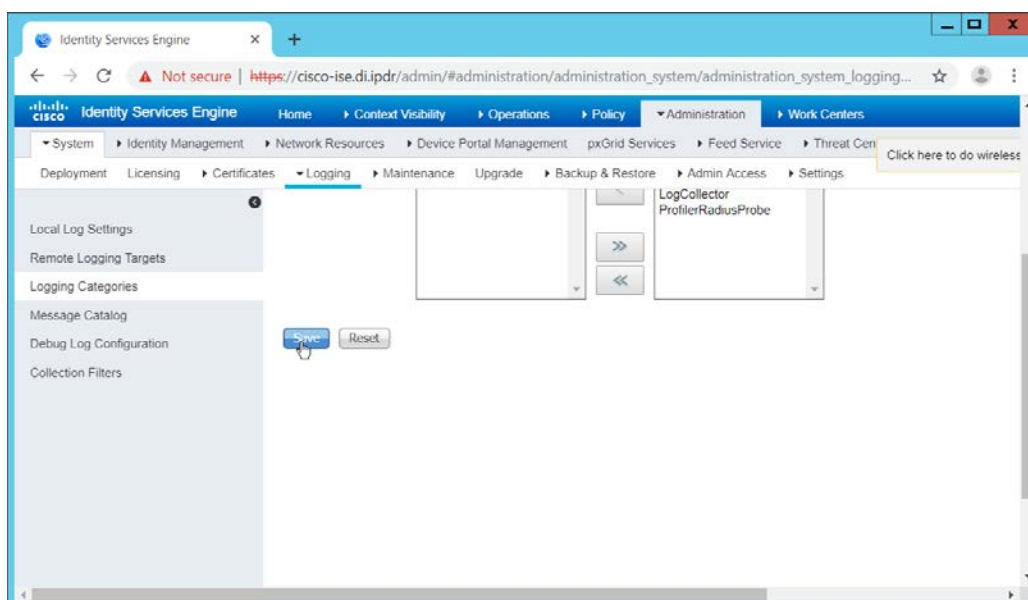
1. Navigate to **System > Logging > Logging Categories**.



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—use the address of that server to which to forward logs.

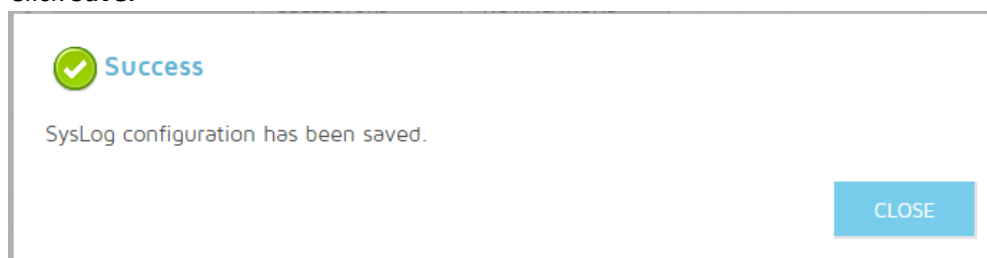
Note: This integration requires Semperis DSP version 2.6.

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 leave it as **All**.

The screenshot shows the Semperis DS Protector for Active Directory web interface. The browser address bar displays <https://semperis-dsp.dipdr/DSP#siemIntegration>. The interface has a top navigation bar with 'Domain: DI:IPDR', 'Administrator', and 'LOGOUT'. A left sidebar contains various icons and labels: 'Current Domain: DI:IPDR', 'CHANGED ITEMS', 'DELETED ITEMS', 'CONFIGURATION PARTITION', 'DNS', 'GPO', 'REPORTS', 'JOB STATUS', 'OPERATION LOG', and 'SETTINGS'. The main content area is titled 'SIEM INTEGRATION' and includes tabs for 'GENERAL', 'DS PROTECTOR AGENTS', 'PERMISSIONS', 'AUDIT AGENTS', 'AUDIT COLLECTORS', and 'AUDIT NOTIFICATIONS'. The 'Enable SysLog' checkbox is checked. The 'Syslog Server' section contains fields for 'Primary Syslog Server' (backupserv.dipdr), 'Primary Syslog Port' (514), and radio buttons for 'TCP' (selected) and 'UDP'. There is also a 'Secondary Syslog Server' field (SERVER) and 'Secondary Syslog Port' (514) with similar radio buttons. A 'Change Event Polling Frequency' is set to 10 minutes. The 'Change Event Filtering' section has dropdowns for 'Operations' (All (0 items selected)), 'Object Classes' (All (0 items selected)), and 'Attributes' (All (0 items selected)). To the right, 'Include these events' has a checked 'AD Changed Items' checkbox, a 'Partitions' dropdown (All), an unchecked 'DNS' checkbox, and a checked 'Send Operations Log to SysLog' checkbox. A 'SAVE' button is at the bottom left of the configuration area.

8. Click **Save**.



9. Click **Close**.

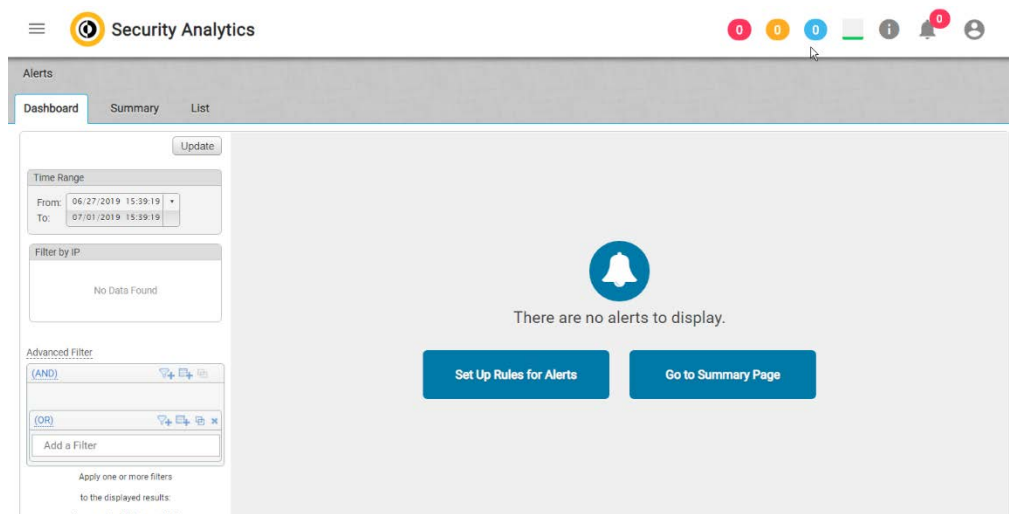
2.23 Integration: Micro Focus ArcSight and Symantec Analytics

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; use the address of that server to which to forward logs.

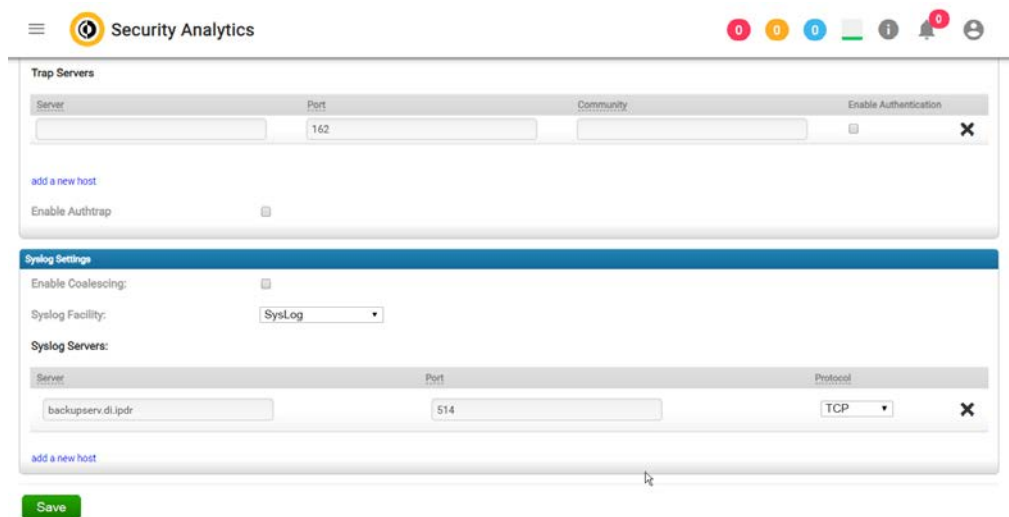
The second part of this section will detail a further integration for ArcSight that allows ArcSight to better analyze network packets received from Symantec Analytics.

2.23.1 Configure Symantec Analytics to Forward Logs

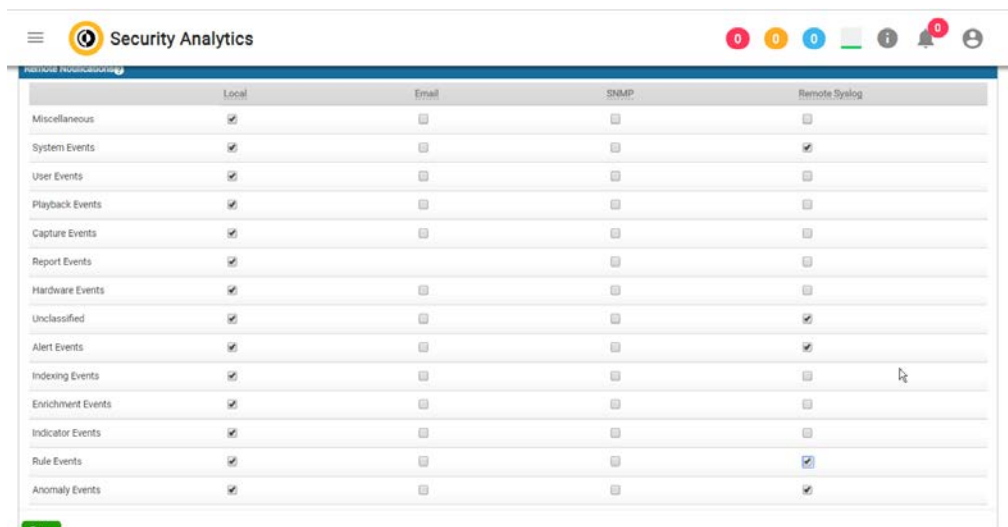
1. Log in to the Symantec Analytics web console.



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.



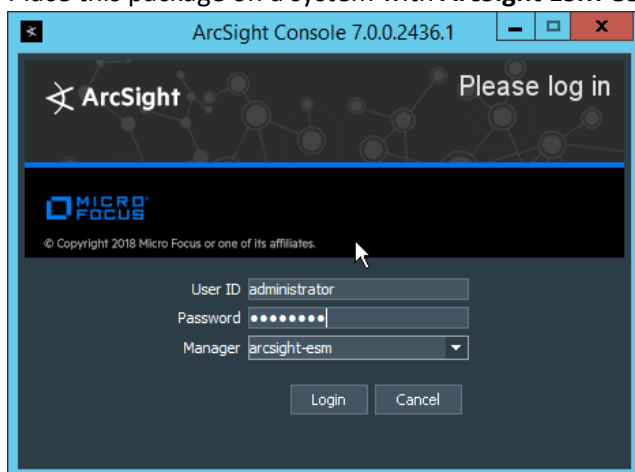
9. Click **Save**.
10. Click the **Advanced** tab.
11. Select the box under **Remote Syslog** column for any events that you wish to forward to ArcSight, for example, **System Events**, **Unclassified Events**, **Alert Events**, **Rule Events**, **Anomaly Events**.



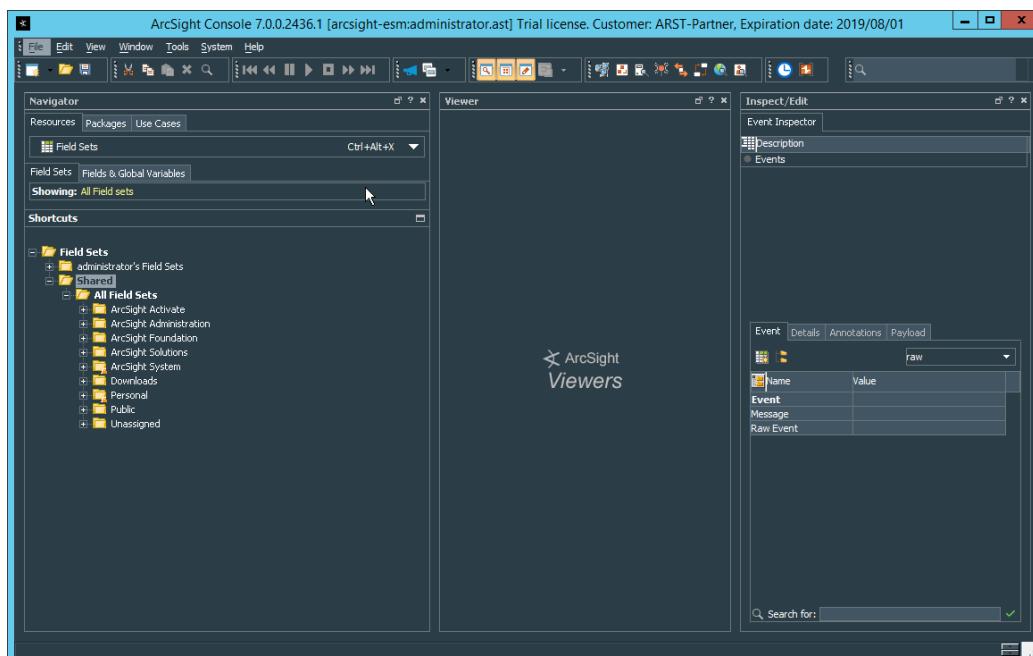
12. Click **Save**.

2.23.2 Install Symantec Analytics Package for ArcSight

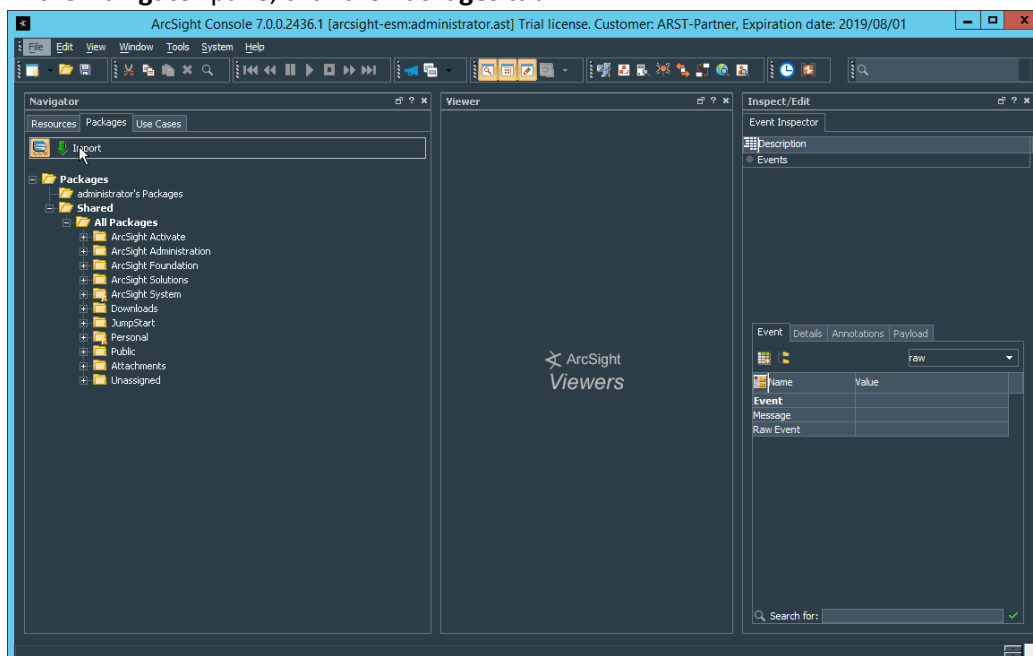
1. Navigate to the ArcSight marketplace. Look for the “Blue Coat Security Analytics” package for ArcSight. It may be available here: <https://marketplace.microfocus.com/arc-sight/content/blue-coat-security-analytics-platform> but not please contact your ArcSight representative to get the package. The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



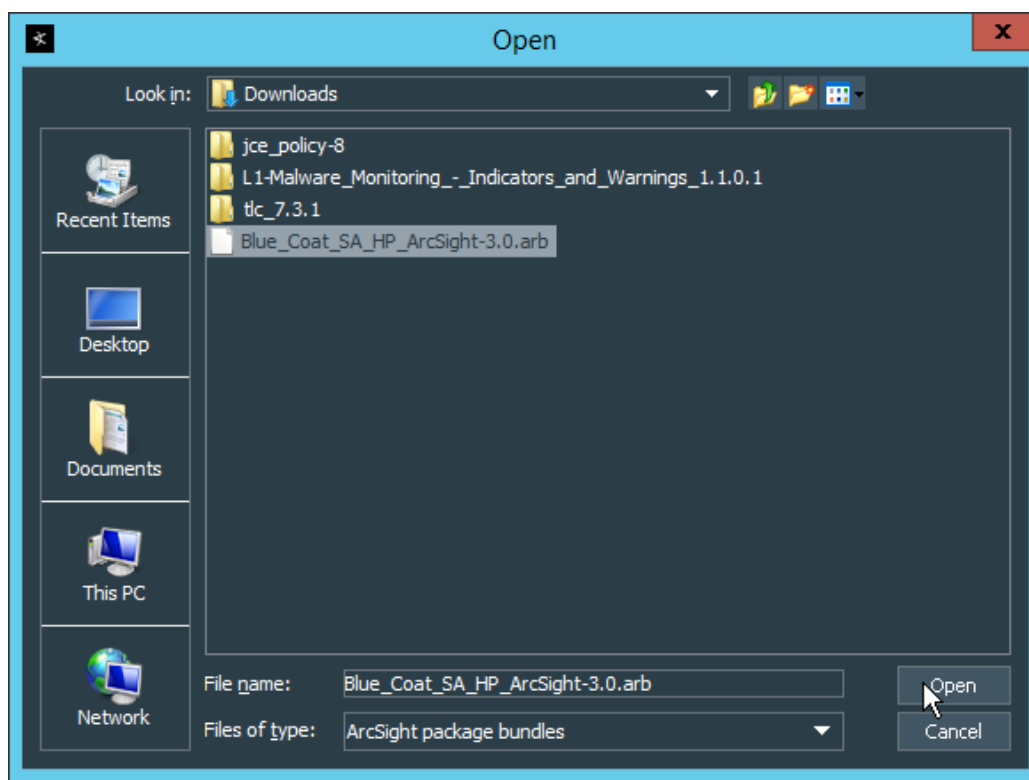
3. Log in to the **ArcSight ESM Console** with a user that has the privileges to install packages.



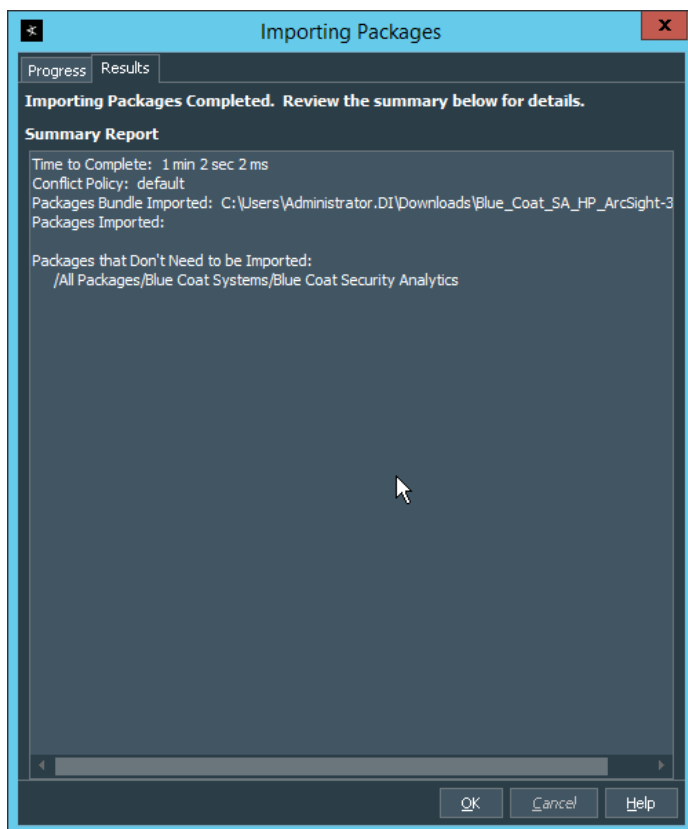
4. In the **Navigator** pane, click the **Packages** tab.



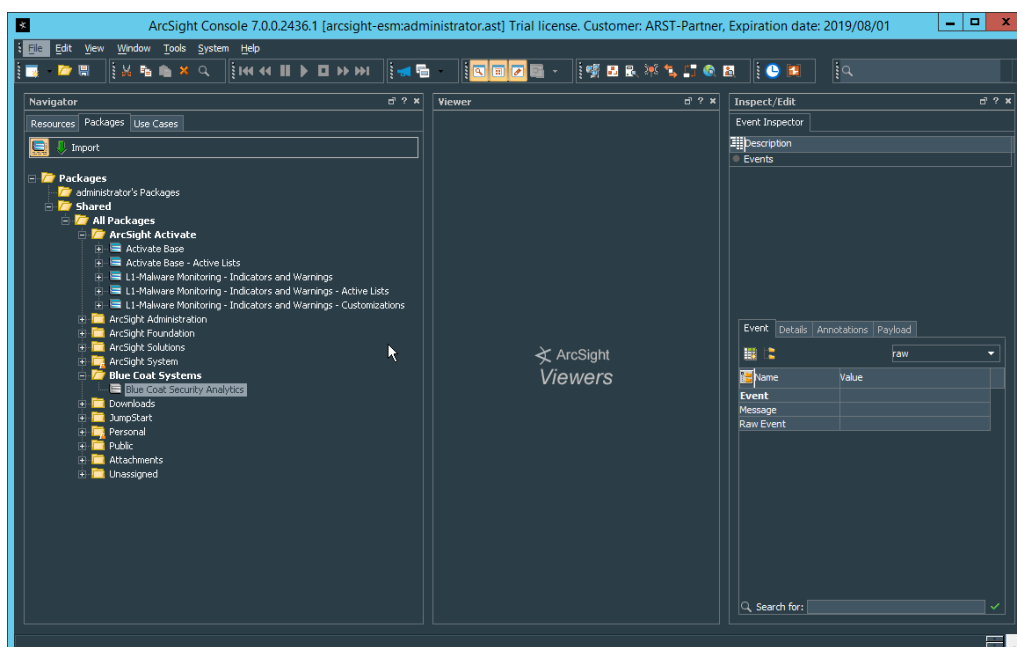
5. Click **Import**.
6. In the window that it opens, find and select the package you downloaded.



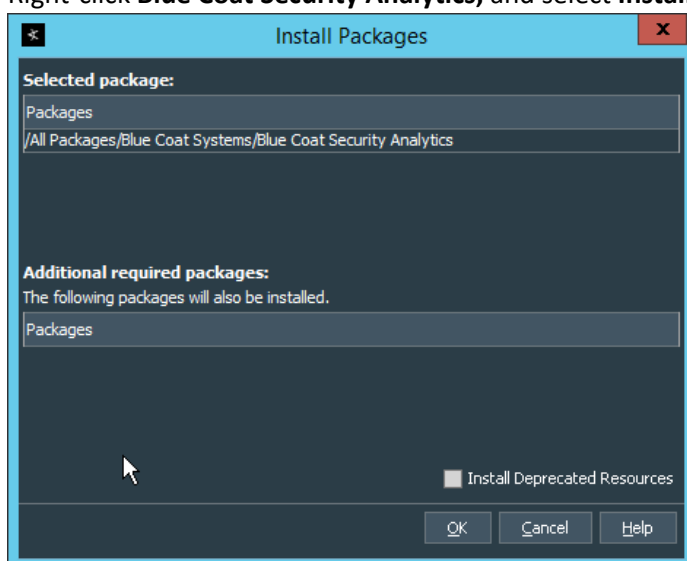
7. Click **Open**.



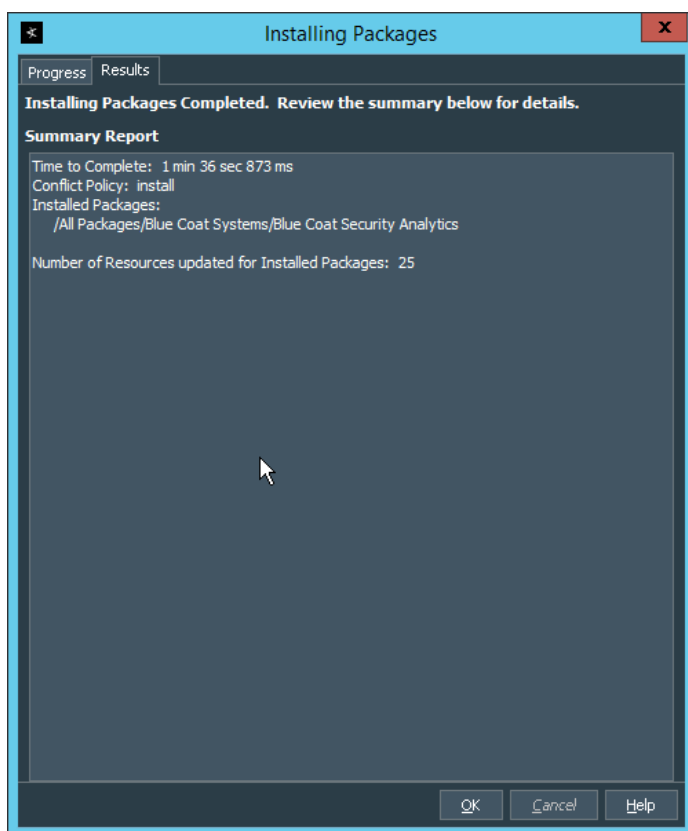
8. Click **OK** when the import finishes.
9. Under the **Packages** tab in the **Navigator** pane, navigate to **Packages > Shared > All Packages > Blue Coat Systems > Blue Coat Security Analytics**.



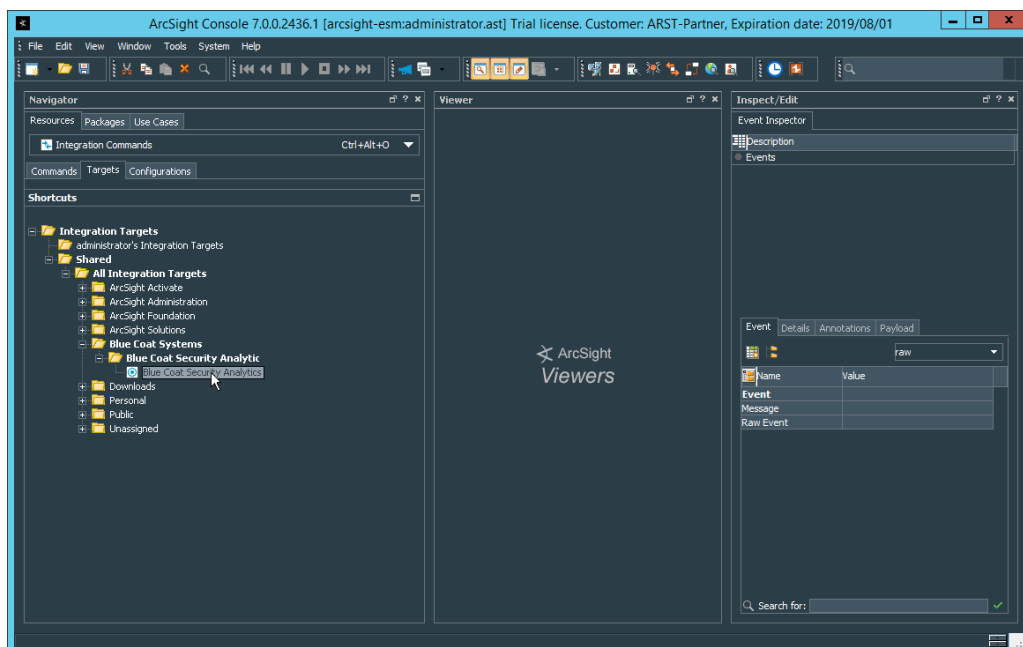
10. Right-click **Blue Coat Security Analytics**, and select **Install Package**.



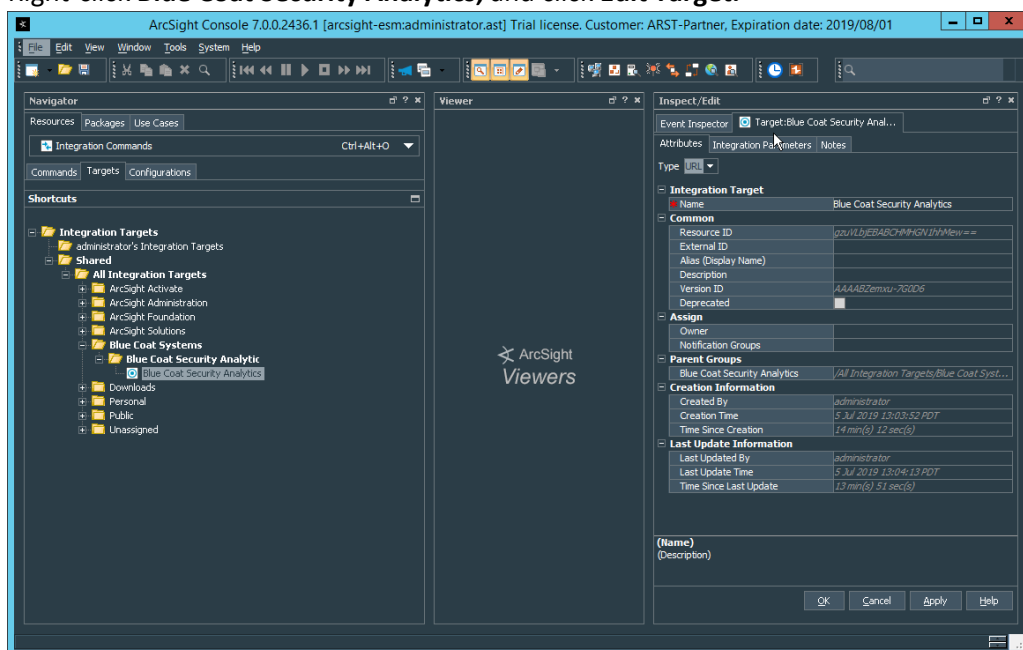
11. Click **OK**.



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**.

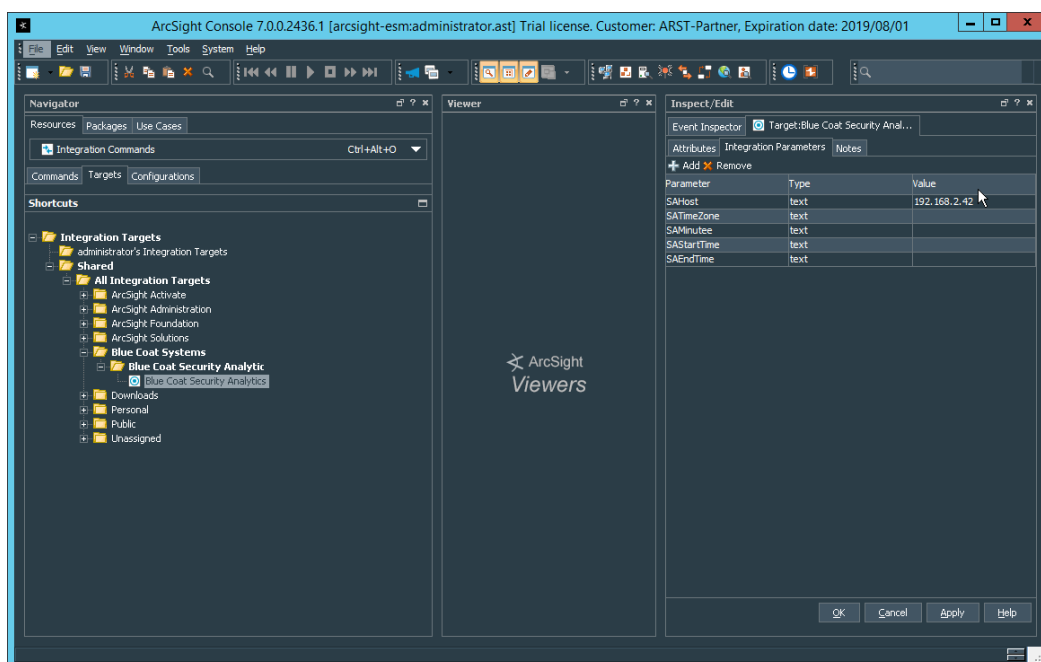


16. Right-click **Blue Coat Security Analytics**, and click **Edit Target**.



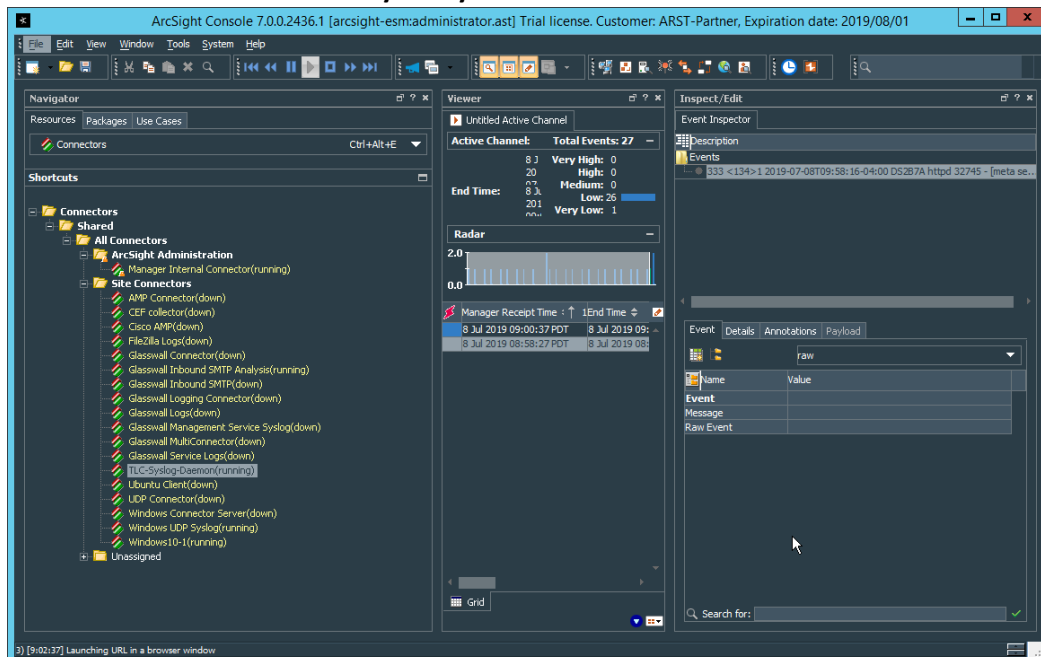
17. Click the **Integration Parameters** tab.

18. Replace the **SAHost** value with the IP address of Symantec Analytics.

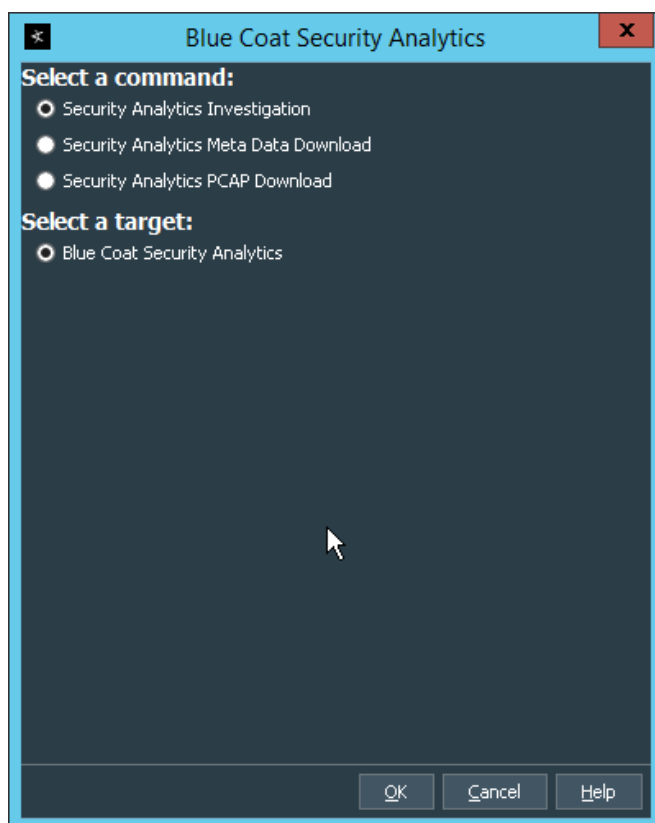


19. Click **OK**.

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**.



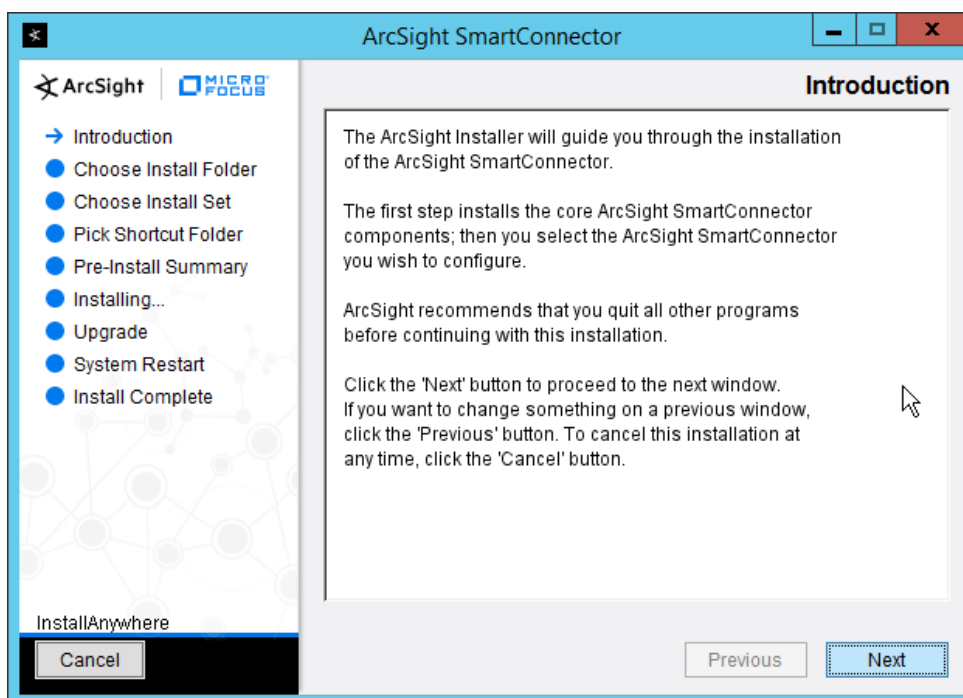
22. Click **OK**. This will open Security Analytics in the browser and perform a packet search based on the event parameters.

2.24 Integration: Micro Focus ArcSight and Glasswall FileTrust

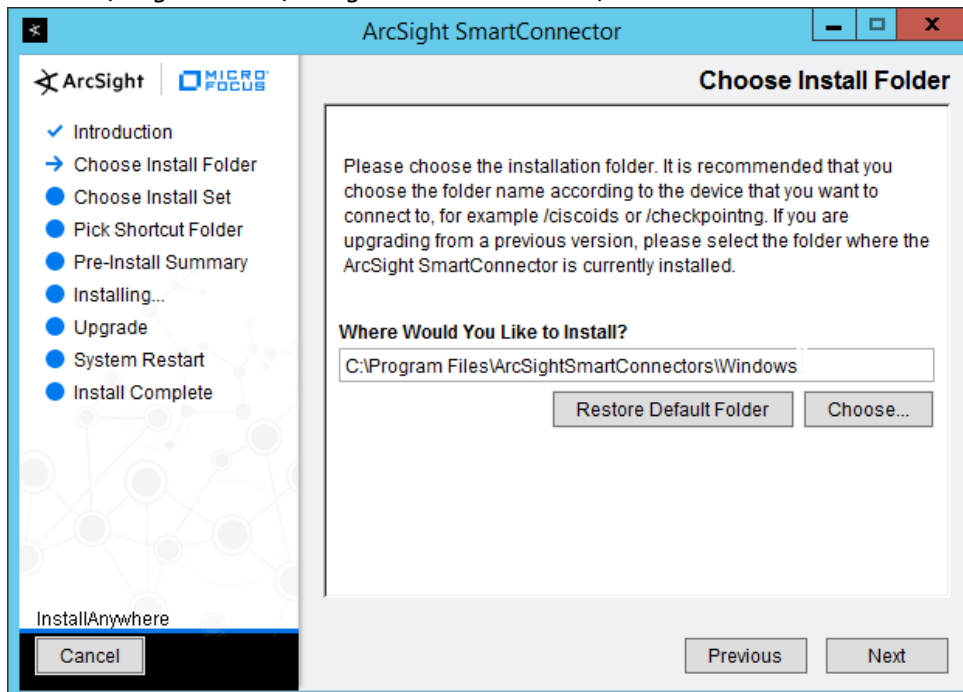
Glasswall FileTrust for Email stores its logs in *C:\Logging*, on the server running the **Glasswall** services.

2.24.1 Install Micro Focus ArcSight

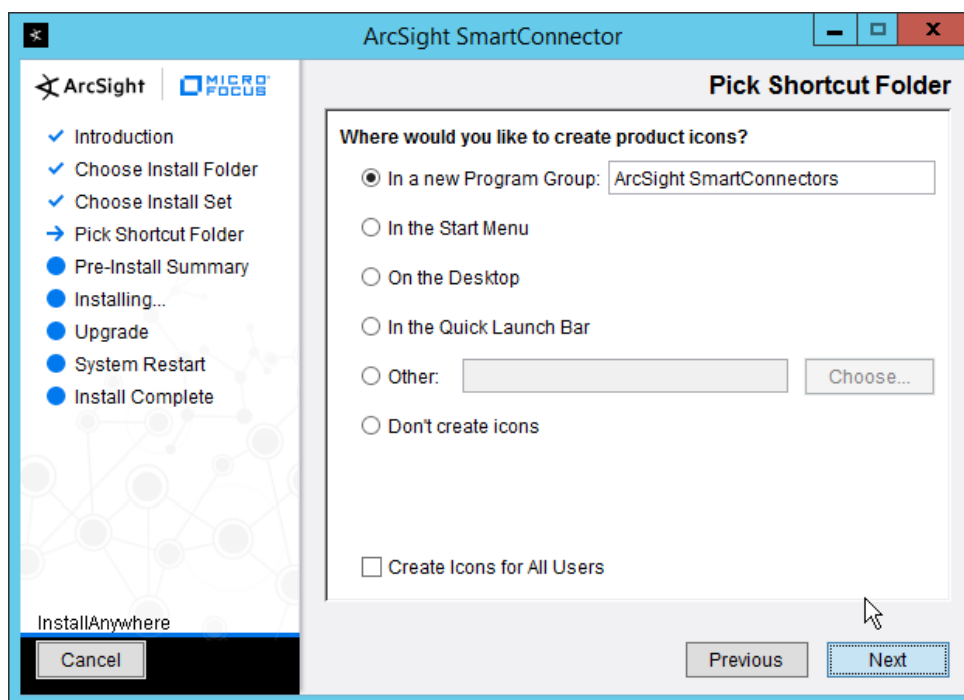
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on the same server as **Glasswall FileTrust**.



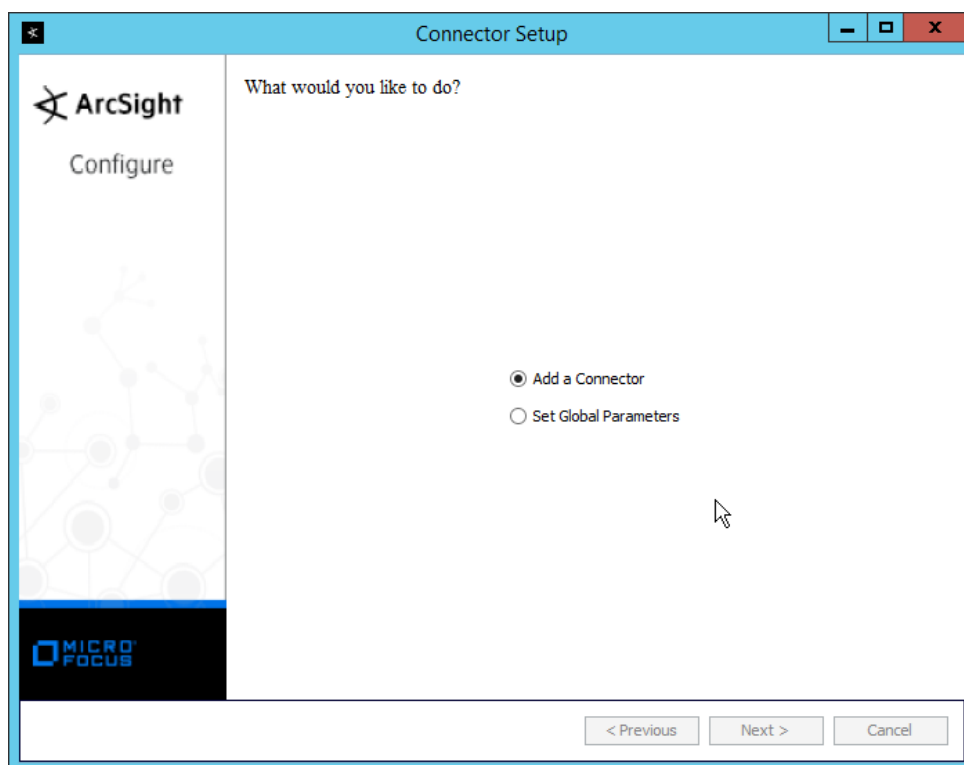
2. Click **Next**.
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows*.



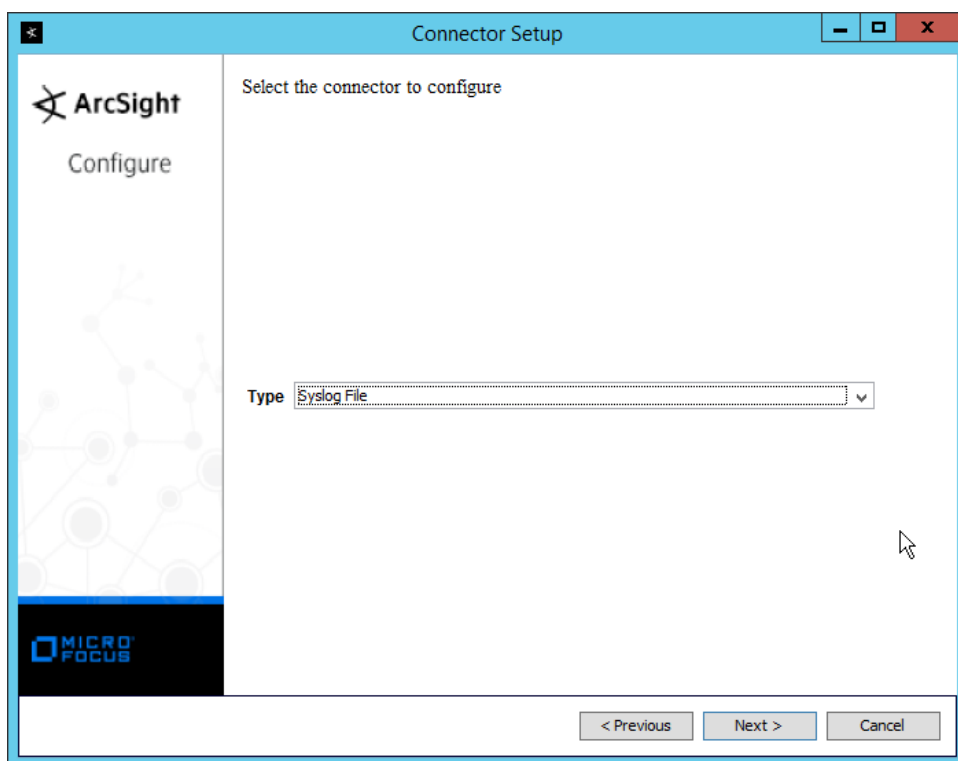
4. Click **Next**.



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**.

Connector Setup

ArcSight
Configure

Enter the parameter details

File Absolute Path Name: ig\gw-inbound-smtp-analysis-agent.current.log

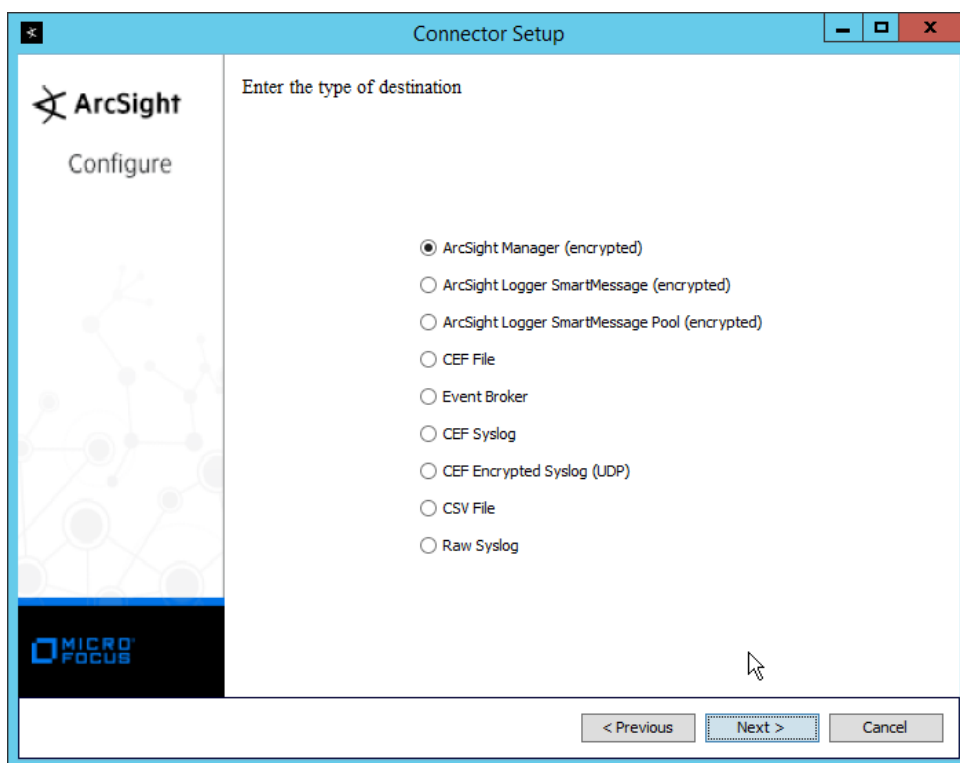
Reading Events Real Time or Batch: realtime

Action Upon Reaching EOF: None

File Extension If Rename Action: processed

< Previous Next > Cancel

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



14. Click **Next**.

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

Connector Setup

ArcSight
Configure

Enter the destination parameters

Manager Hostname: arcsight-esm

Manager Port: 8443

User: administrator

Password: ••••••••

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: false

< Previous Next > Cancel

16. Click **Next**.

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

Connector Setup

ArcSight
Configure

Enter the connector details

Name: Glasswall Inbound SMTP Analysis

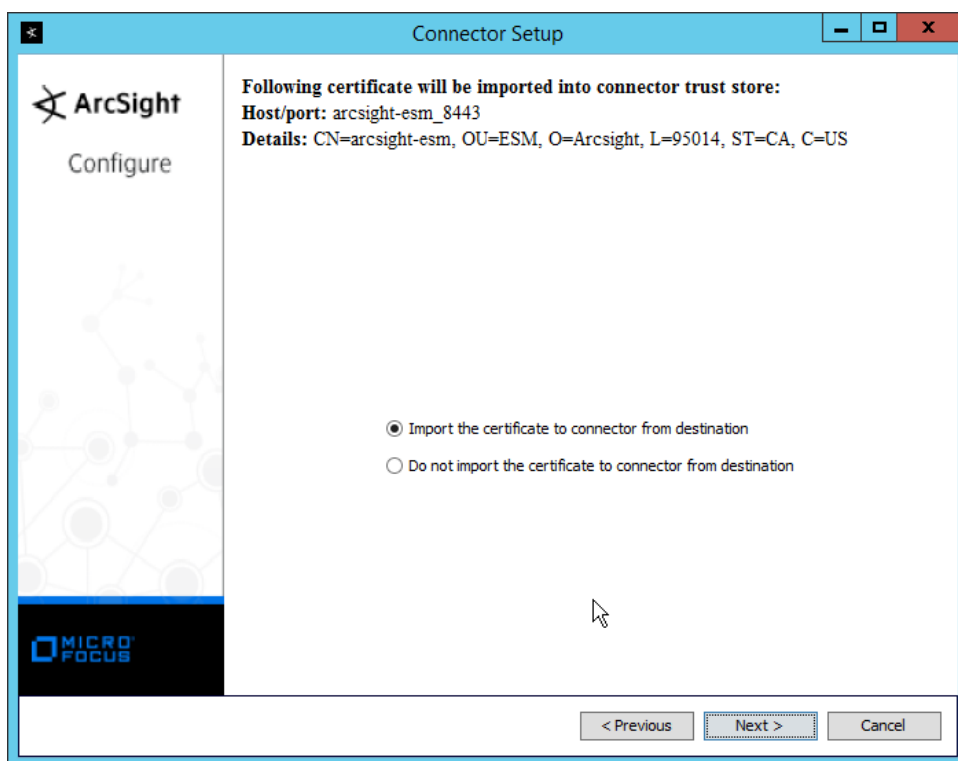
Location:

DeviceLocation:

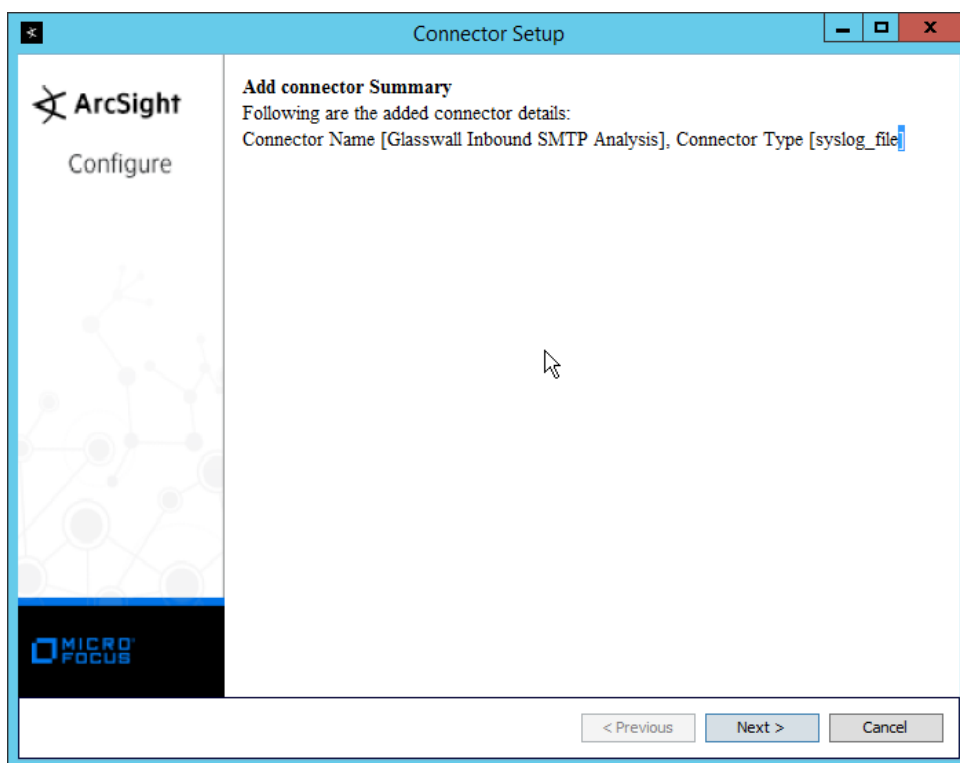
Comment:

< Previous Next > Cancel

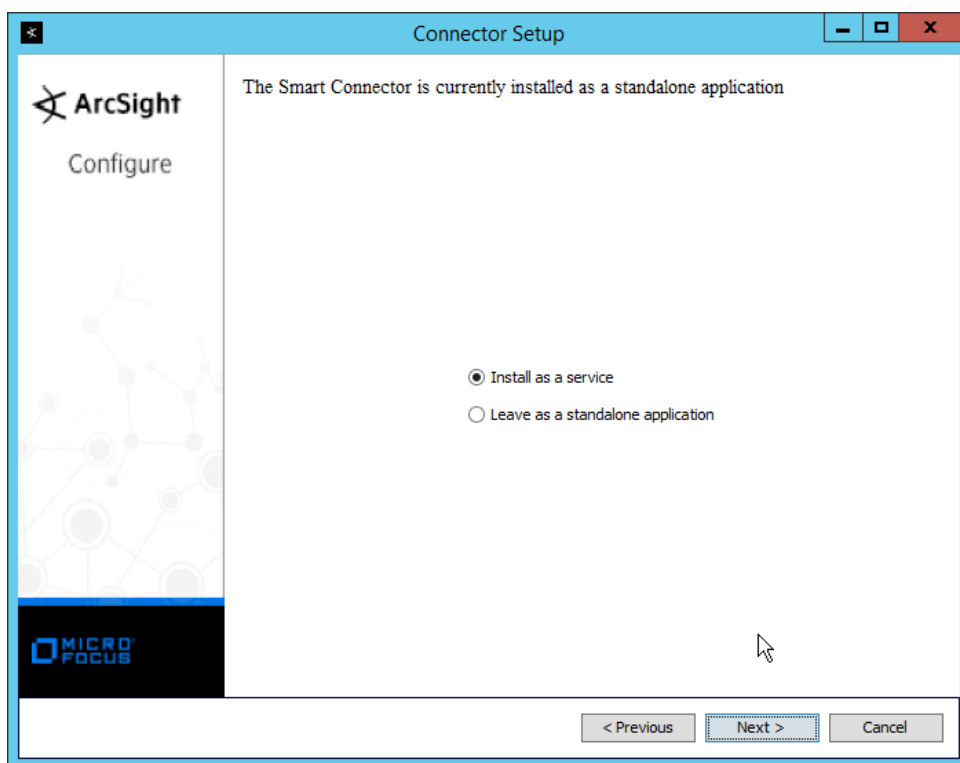
18. Click **Next**.
19. Select **Import the certificate to connector from destination**.



20. Click **Next**.



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



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

Connector Setup

ArcSight
Configure

Specify the service parameters

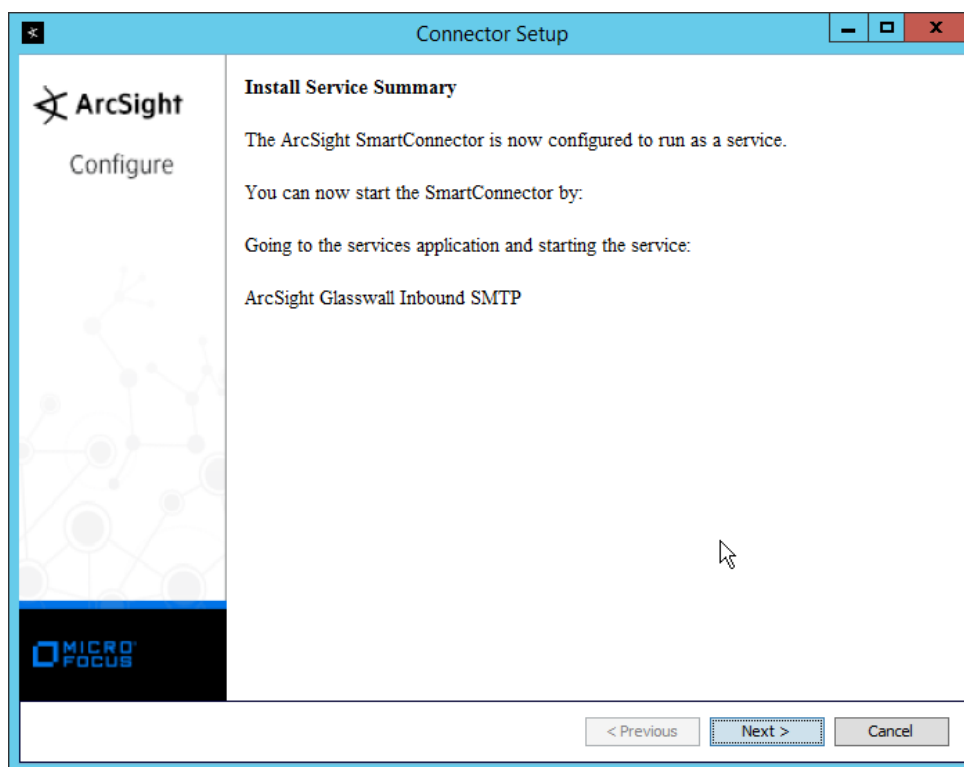
Service Internal Name: glasswall_inbound_smtp

Service Display Name: GlasswallInbound SMTP

Start the service automatically: Yes

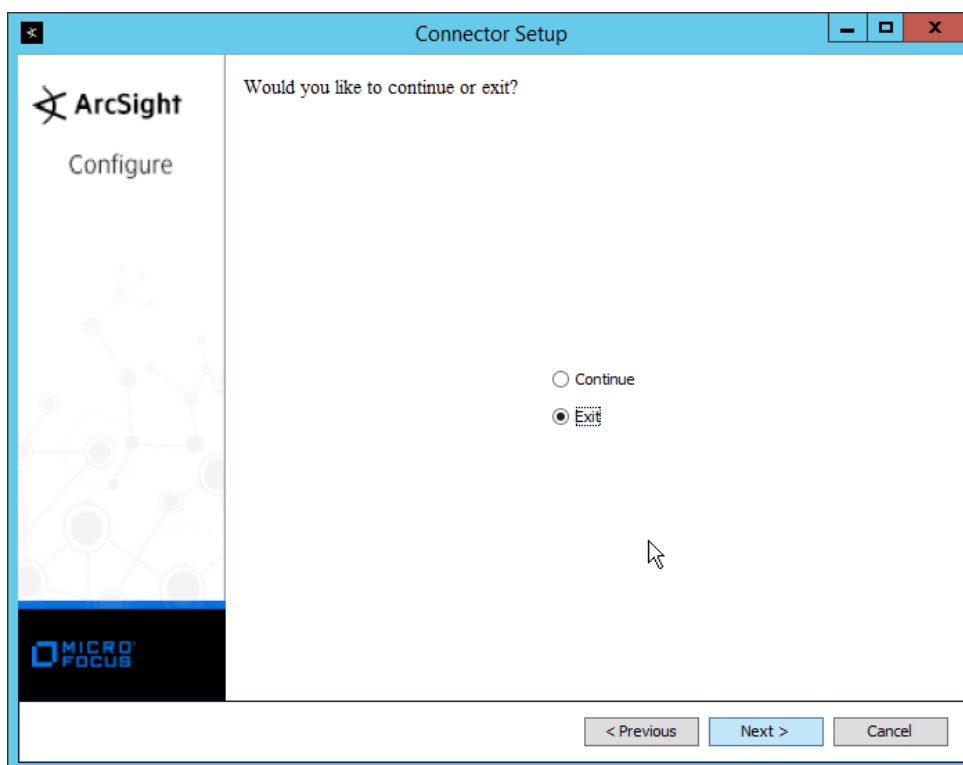
< Previous Next > Cancel

25. Click **Next**.

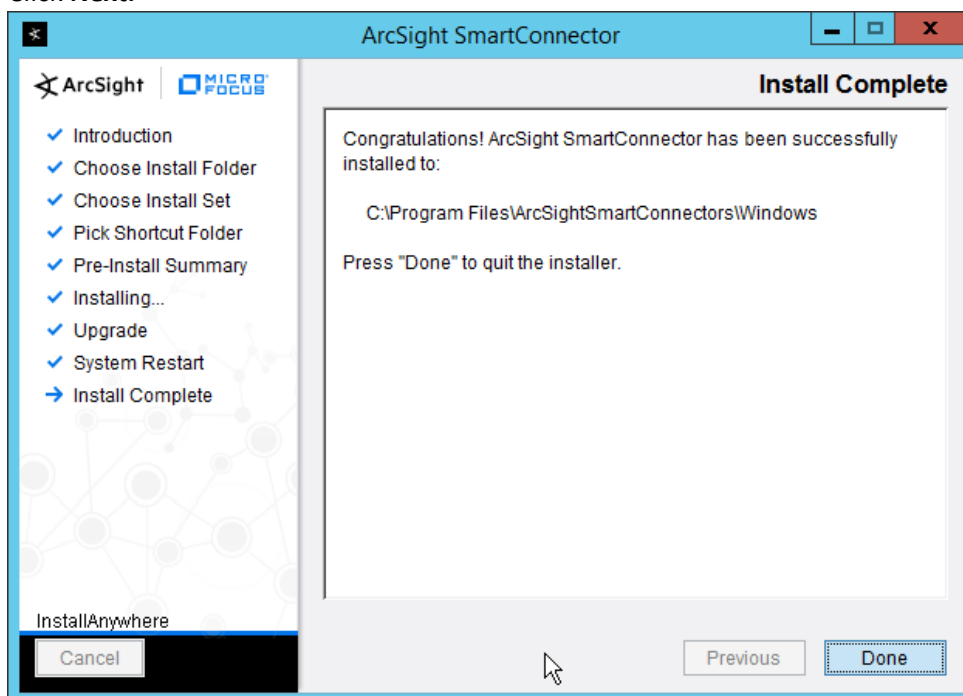


26. Click **Next**.

27. Select **Exit**.



28. Click **Next**.



29. Click **Done**.

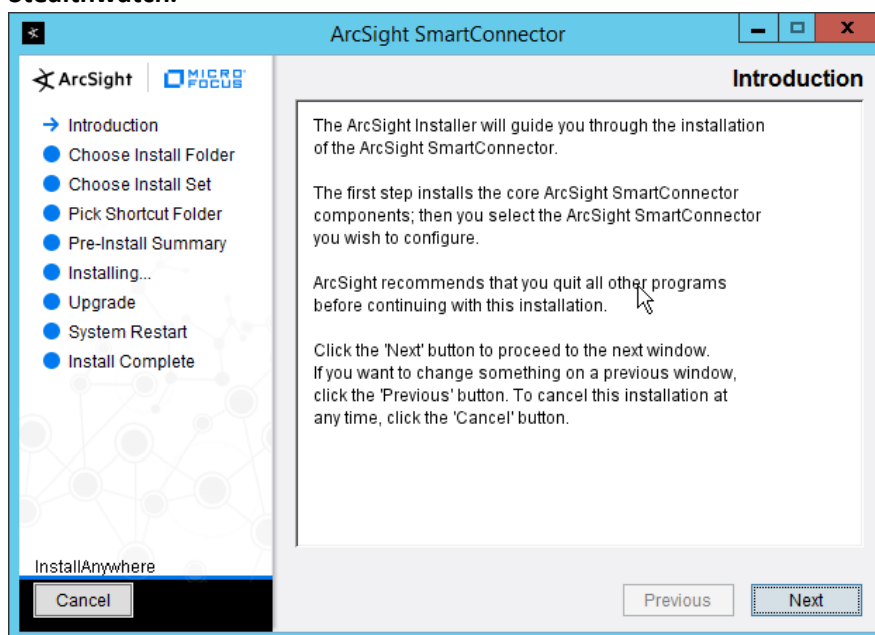
30. Repeat steps 1 to 29 for the other three “current” log files in *C:\Logging*, with the following caveats:
 - a. Replace *C:\Program Files\ArcSightSmartConnectors\Windows* with a different folder name for each connector.
 - b. Replace *C:\Logging\gw-inbound-smtp-analysis-agent.current.log* with the 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

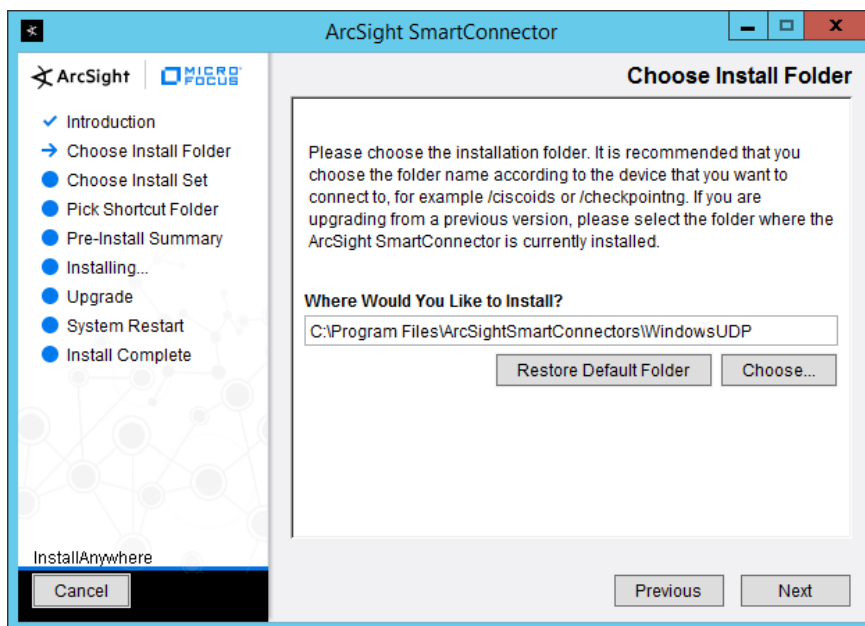
This section will detail the forwarding of logs from **Cisco Stealthwatch** to **Micro Focus ArcSight**.

2.25.1 Install Micro Focus ArcSight

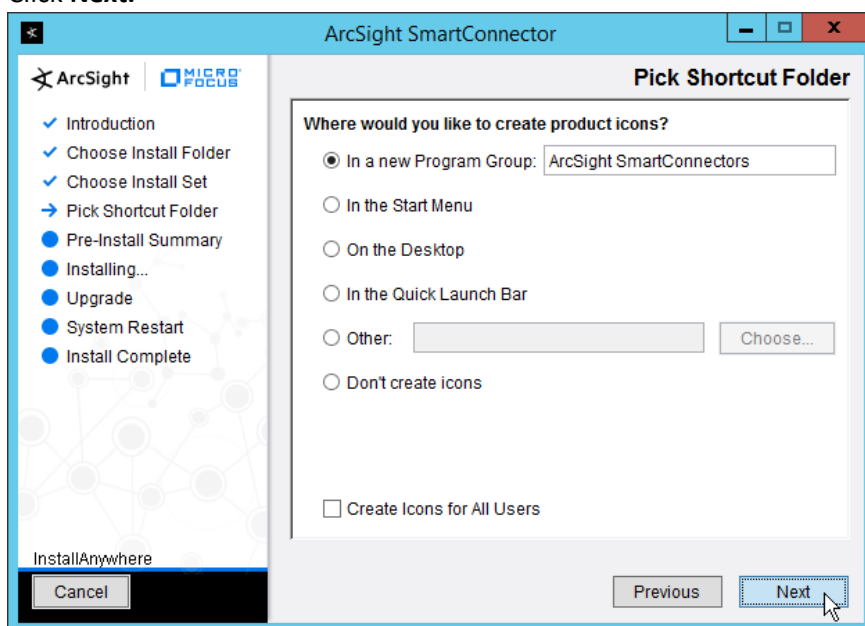
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Cisco Stealthwatch**.



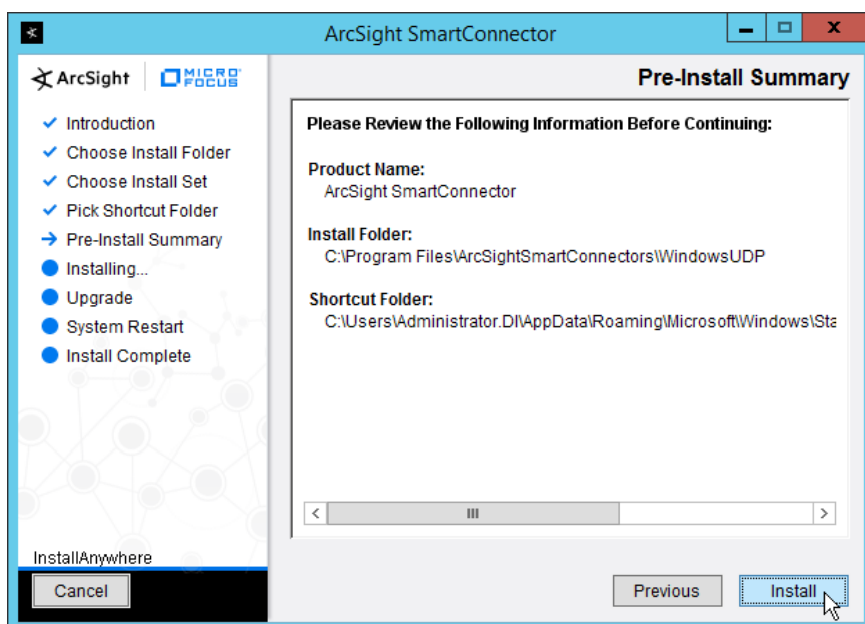
2. Click **Next**.
3. Enter *C:\Program Files\ArcSightSmartConnectors\WindowsUDP*.



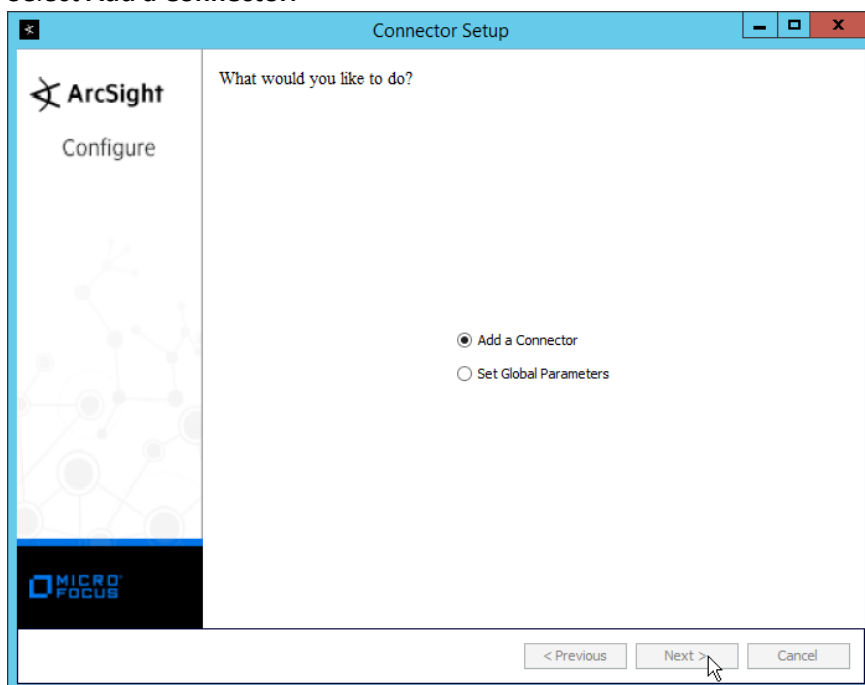
4. Click **Next**.



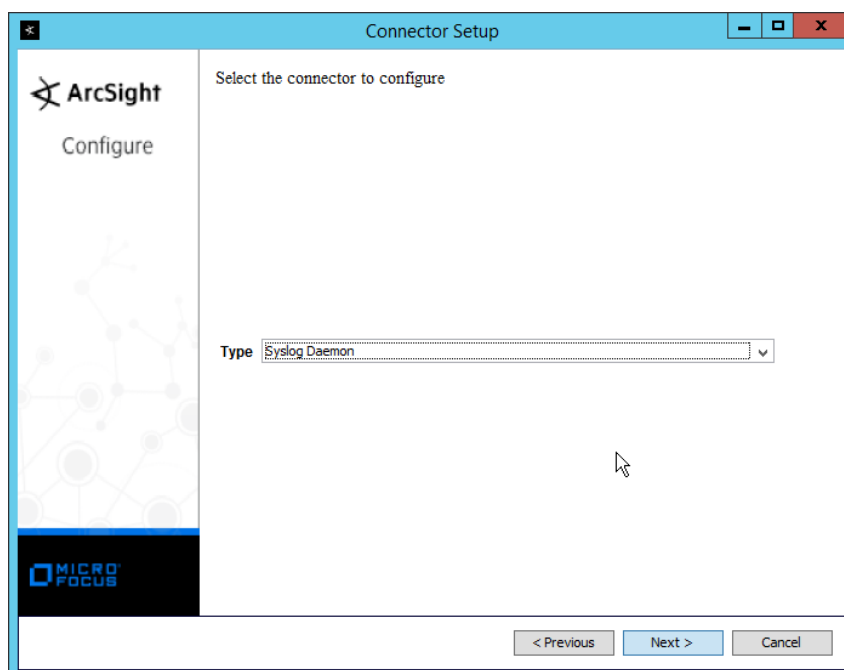
5. Click **Next**.



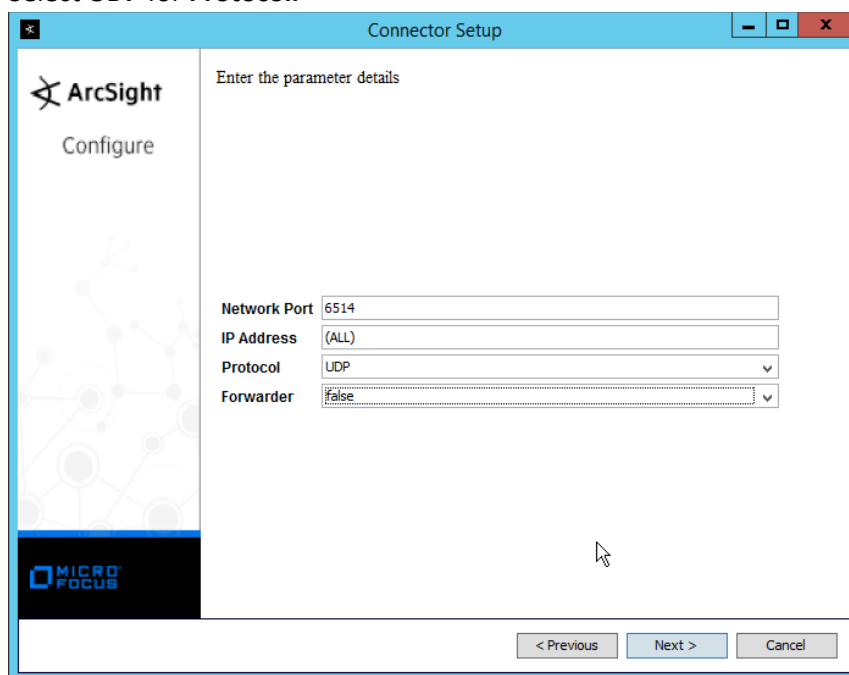
6. Click **Install**.
7. Select **Add a Connector**.



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)**.

Connector Setup

Enter the type of destination

☒ ArcSight Manager (encrypted)

☐ ArcSight Logger SmartMessage (encrypted)

☐ ArcSight Logger SmartMessage Pool (encrypted)

☐ CEF File

☐ Event Broker

☐ CEF Syslog

☐ CEF Encrypted Syslog (UDP)

☐ CSV File

☐ Raw Syslog

< Previous Next > Cancel

15. Click **Next**.

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

Connector Setup

Enter the destination parameters

Manager Hostname: arcsight-esm

Manager Port: 8443

User: administrator

Password: ••••••••

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: false

< Previous Next > Cancel

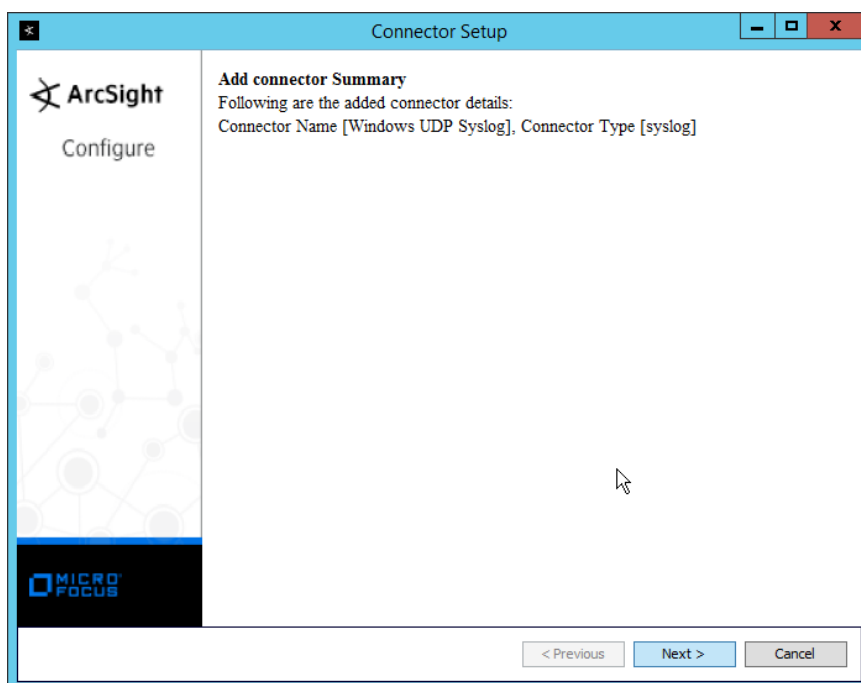
17. Click **Next**.

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

19. Click **Next**.

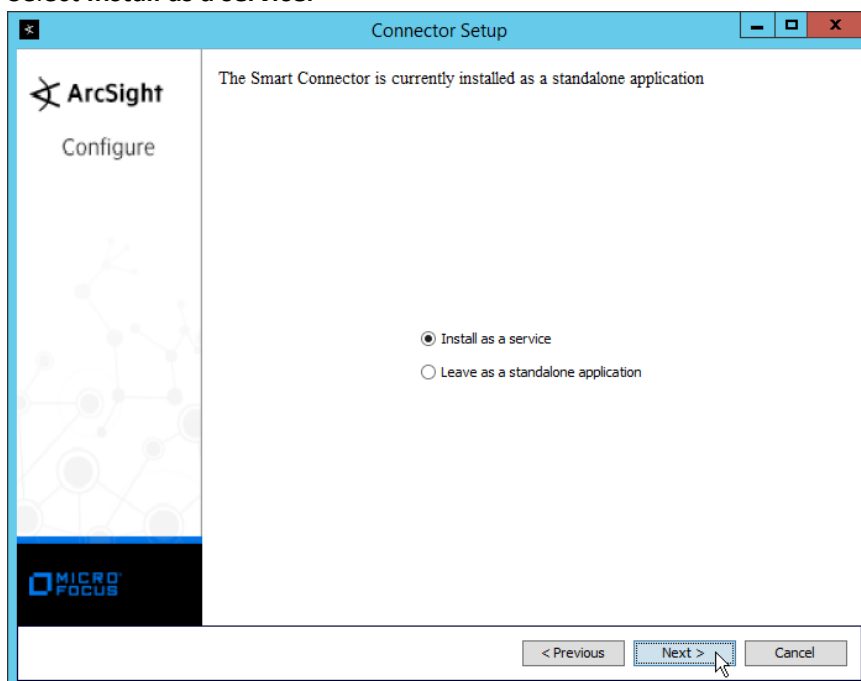
20. Select **Import the certificate to connector from destination**.

21. Click **Next**.



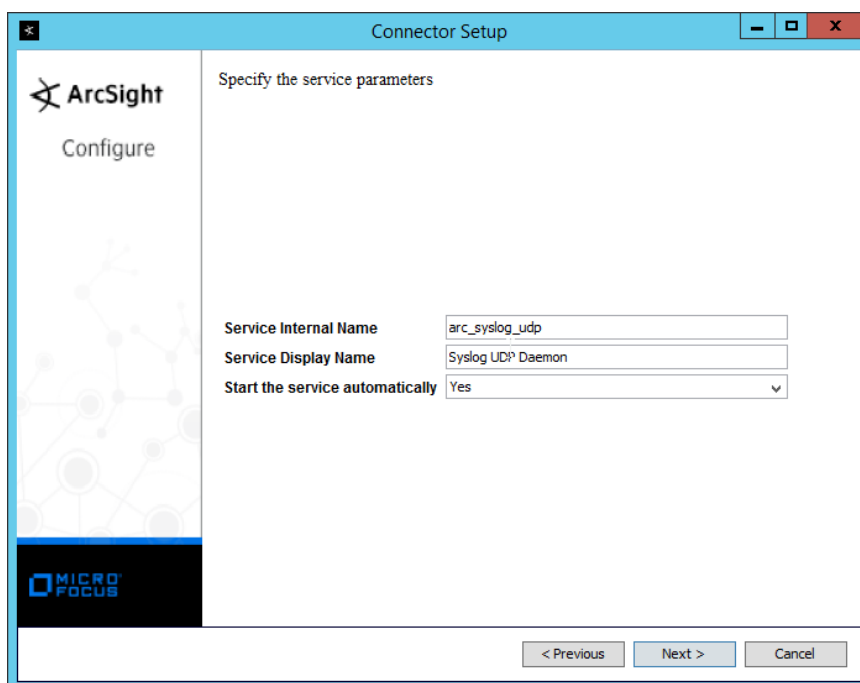
22. Click **Next**.

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



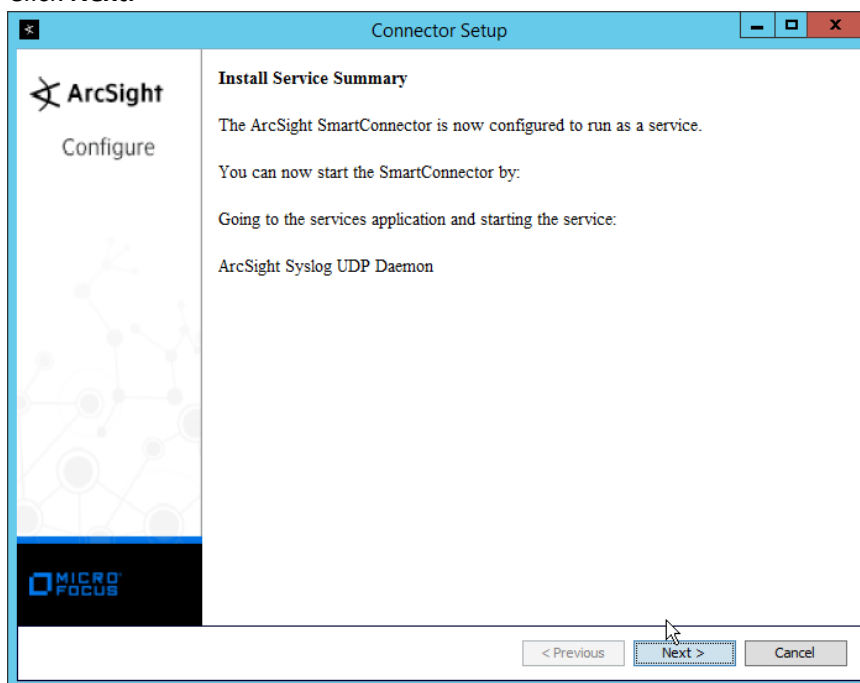
24. Click **Next**.

25. Enter a service name and display name.



The screenshot shows the 'Connector Setup' window with the 'Specify the service parameters' section. The left sidebar contains the ArcSight logo and 'Configure' text. The main area has three input fields: 'Service Internal Name' with the value 'arc_syslog_udp', 'Service Display Name' with the value 'Syslog UDP Daemon', and 'Start the service automatically' with a dropdown menu set to 'Yes'. At the bottom are buttons for '< Previous', 'Next >', and 'Cancel'.

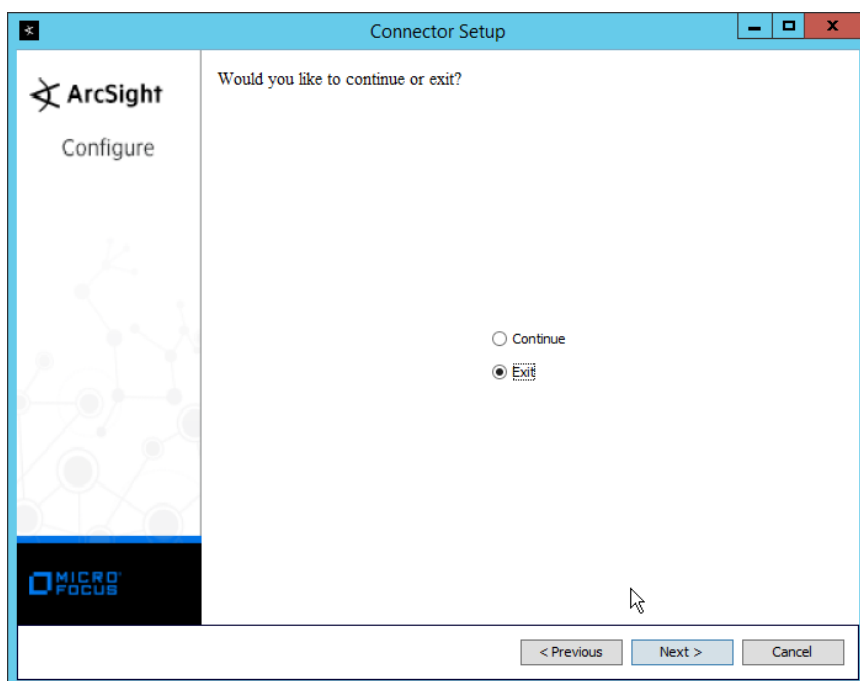
26. Click **Next**.



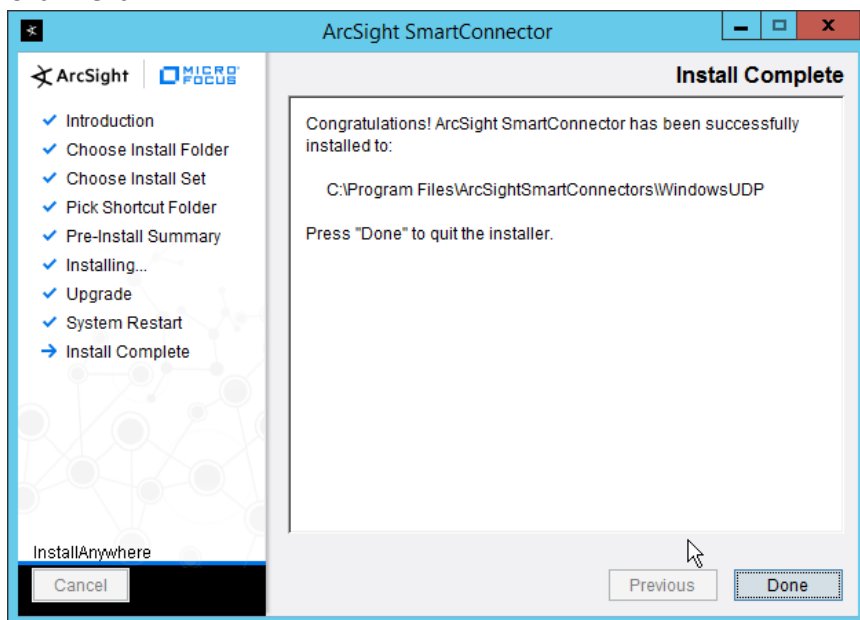
The screenshot shows the 'Connector Setup' window with the 'Install Service Summary' section. The left sidebar is the same as the previous step. The main area contains the following text: 'Install Service Summary', 'The ArcSight SmartConnector is now configured to run as a service.', 'You can now start the SmartConnector by:', 'Going to the services application and starting the service:', and 'ArcSight Syslog UDP Daemon'. At the bottom are buttons for '< Previous', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

27. Click **Next**.

28. Select **Exit**.



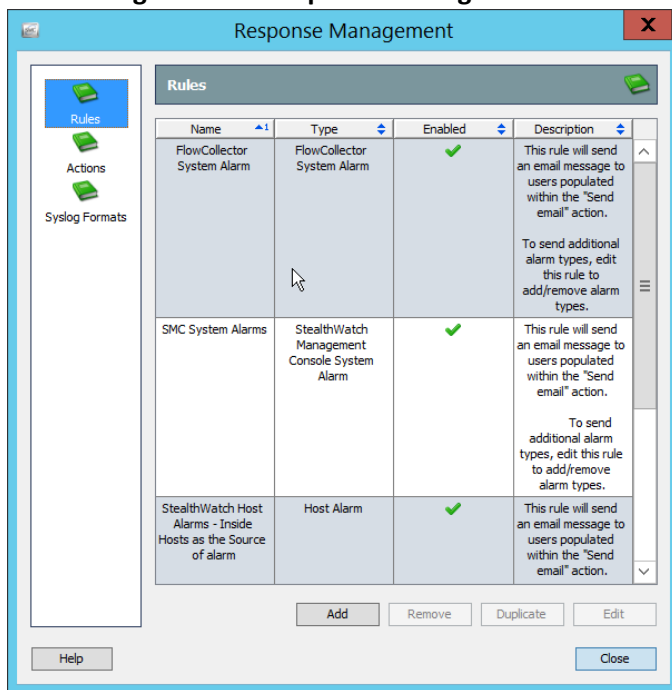
29. Click **Next**.



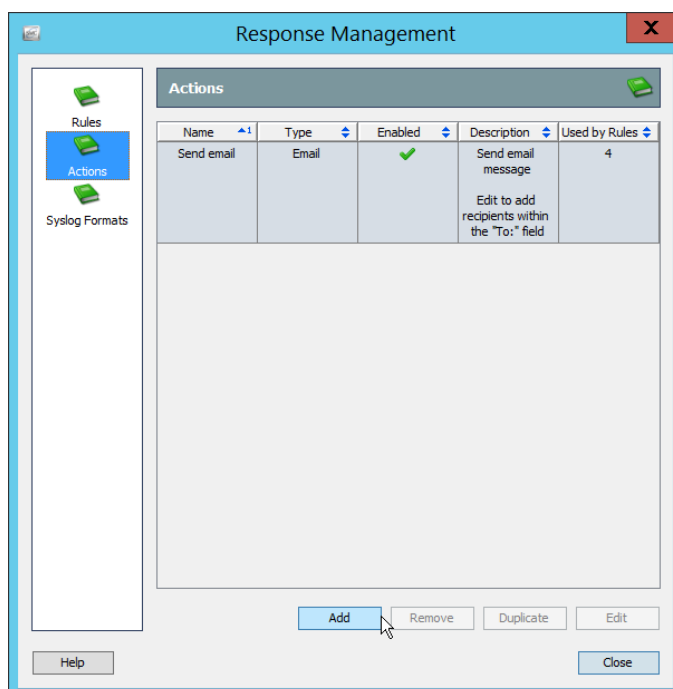
30. Click **Done**.

2.25.2 Configure Cisco Stealthwatch

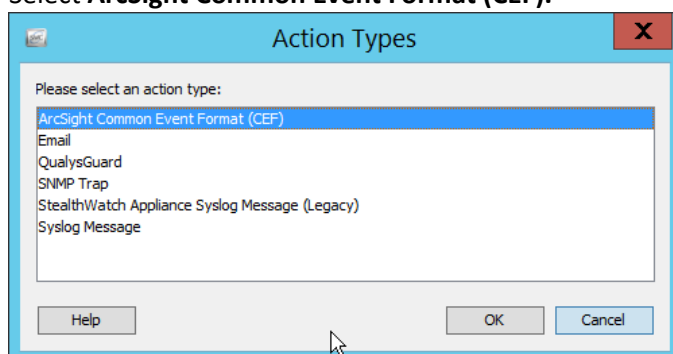
1. Log in to the **Cisco Stealthwatch Management Console** desktop interface. (This can be downloaded from the web interface and run using **javaws.exe**. You may need to add the site to your Java exceptions in **Control Panel > Java**.)
2. Click **Configuration > Response Management**.



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 User Datagram Protocol (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.

Add ArcSight Common Event Format (CEF) Action

Action

Name:

Description:

Enabled: ☒

Destination

IP Address:

Port:

Test

Help OK Cancel

12. Click **OK**.

13. Verify that the action was created properly.

Response Management

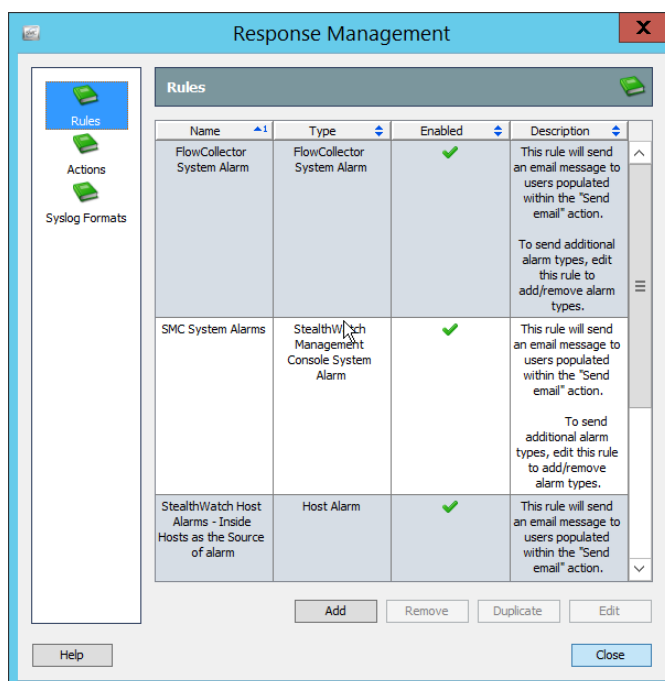
Actions

Name	Type	Enabled	Description	Used by Rules
ArcSight CEF	ArcSight Common Event Format (CEF)	✓	Send to ArcSight.	
Send email	Email	✓	Send email message Edit to add recipients within the "To:" field	4

Add Remove Duplicate Edit

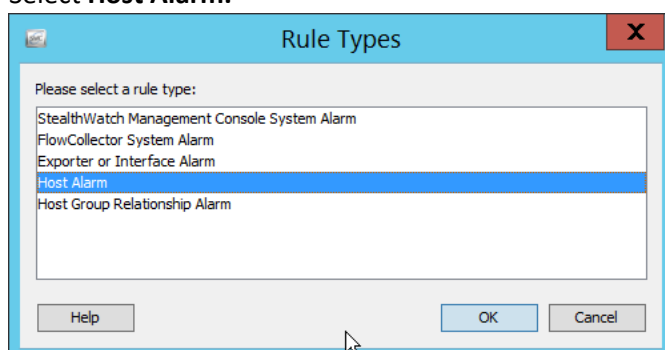
Help Close

14. Click **Rules**.



15. Click **Add**.

16. Select **Host Alarm**.



17. Click **OK**.

18. Enter a **name**.

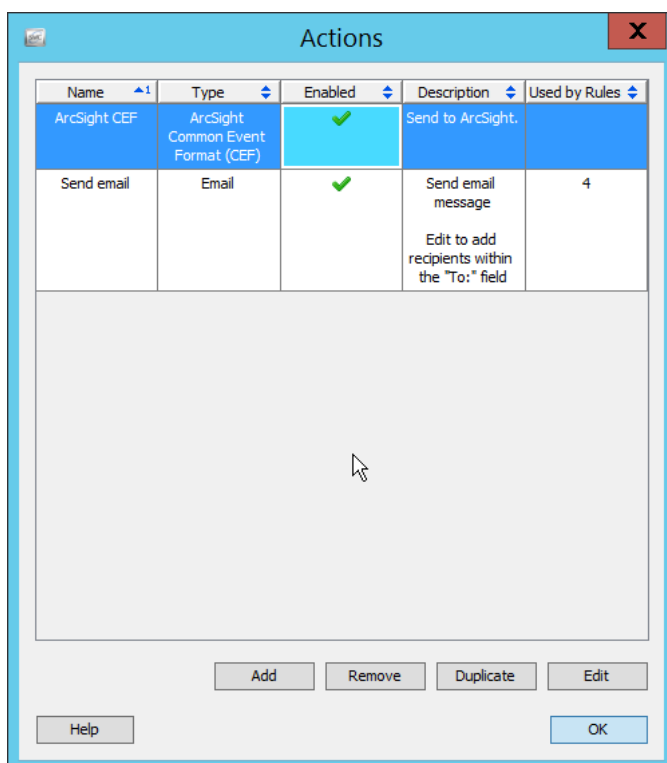
19. Enter a **description**.

The 'Add Host Alarm Rule' dialog box is shown with the 'Rule' tab selected. The 'Name' field contains 'Host Alarm to ArcSight'. The 'Description' field contains 'This rule sends host alarms to ArcSight.'. The 'Enabled' checkbox is checked. The trigger condition is 'This rule is triggered if The Domain that originated this alarm is di-smc and All of the following are true'. The 'OK' button is highlighted.

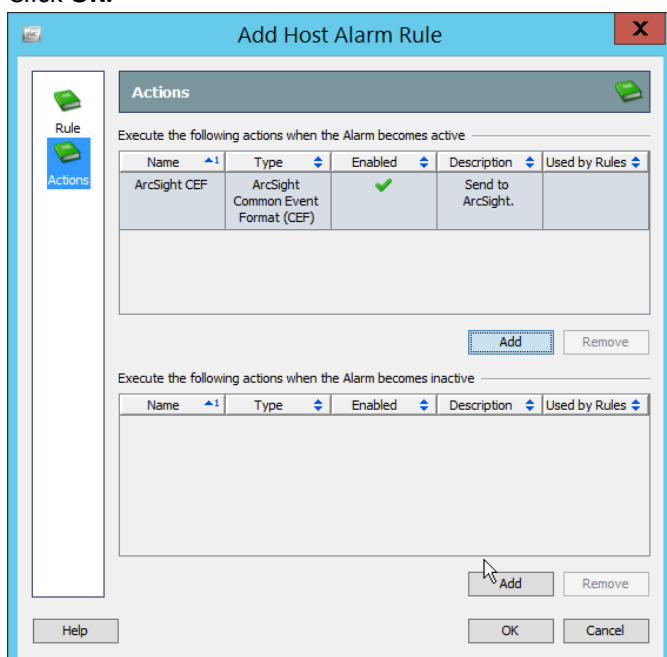
20. Click **Actions**.

The 'Add Host Alarm Rule' dialog box is shown with the 'Actions' tab selected. The 'Execute the following actions when the Alarm becomes active' section is visible. The 'Add' button is highlighted with a mouse cursor. The 'OK' button is highlighted.

21. Click the **Add** button for the top section; this adds an action when the alarm becomes active.
22. Select the ArcSight CEF rule you just created.

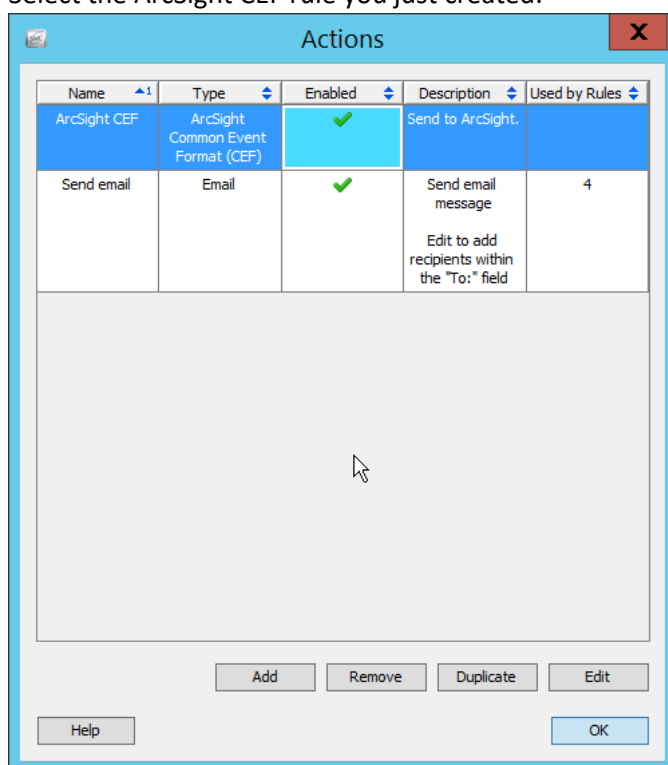


23. Click **OK**.

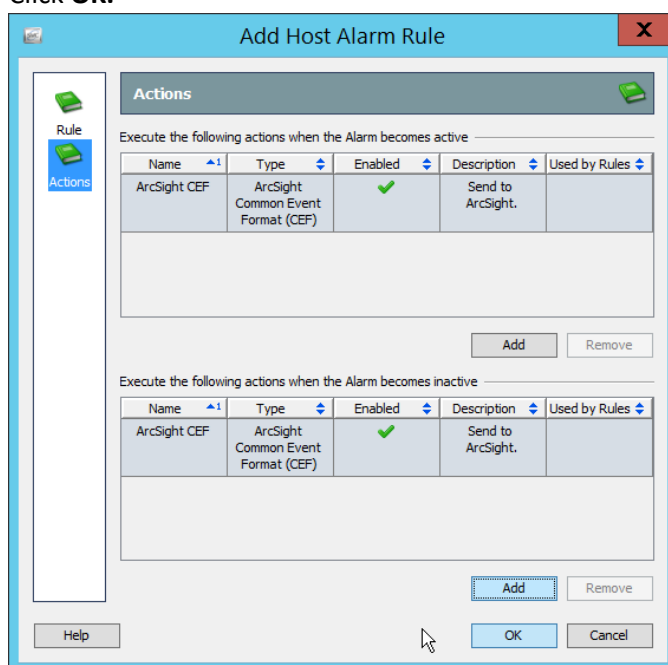


24. Click the **Add** button for the bottom section; this adds an action when the alarm becomes inactive.

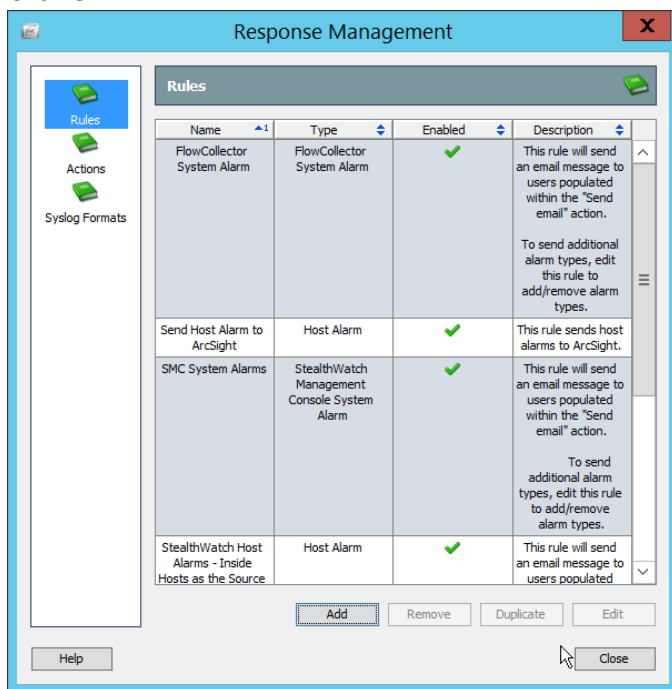
25. Select the ArcSight CEF rule you just created.



26. Click **OK**.



27. Click **OK**.



28. Click **Close**.

Appendix A List of Acronyms

AD	Active Directory
AMP	Advanced Malware Protection
API	Application Programming Interface
CEF	Common Event Format
CSR	Certificate Signing Request
CSV	Comma-Separated Values
DNS	Domain Name System
DSP	Directory Services Protector
ESM	Enterprise Security Manager
ICA	Information Centric Analytics
IIS	Internet Information Services
ISAPI	Internet Server Application Programming Interface
ISE	Identity Services Engine
IT	Information Technology
JCE	Java Cryptography Extension
JRE	Java Runtime Environment
MAC	Media Access Control
MMC	Microsoft Management Console
MSSQL	Microsoft Structured Query Language
MX	Mail Exchange

NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PEM	Privacy Enhanced Mail
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RMI	Remote Method Invocation
SAN	Subject Alternative Name
SDK	Software Development Kit
SMC	Stealthwatch Management Console
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
TE	Tripwire Enterprise
UDP	User Datagram Protocol