

# Data Integrity:

## Identifying and Protecting Assets Against Ransomware and Other Destructive Events

---

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra  
Michael Ekstrom  
Lauren Lusty  
Julian Sexton  
John Sweetnam

FINAL

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

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



NIST SPECIAL PUBLICATION 1800-25

# Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B);  
and How-To Guides (C)*

Jennifer Cawthra  
*National Cybersecurity Center of Excellence*  
NIST

Michael Ekstrom  
Lauren Lusty  
Julian Sexton  
John Sweetnam  
*The MITRE Corporation*  
McLean, Virginia

FINAL

December 2020



U.S. Department of Commerce  
*Wilbur Ross, Secretary*

National Institute of Standards and Technology  
*Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology*



## NIST SPECIAL PUBLICATION 1800-25A

---

# Data Integrity:

## Identifying and Protecting Assets Against Ransomware and Other Destructive Events

---

### Volume A: Executive Summary

**Jennifer Cawthra**

National Cybersecurity Center of Excellence  
NIST

**Michael Ekstrom**

**Lauren Lusty**

**Julian Sexton**

**John Sweetnam**

**Anne Townsend**

The MITRE Corporation  
McLean, Virginia

December 2020

FINAL

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

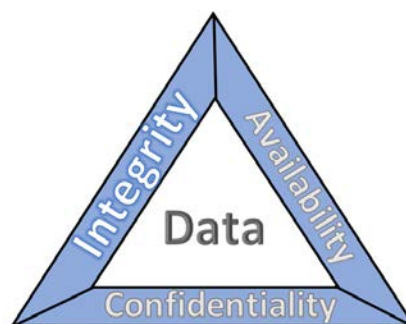
This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect>.



# Executive Summary

The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability, as follows:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- Availability – ensuring timely and reliable access to and use of information



This series of practice guides focuses on data integrity: the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

(Note: These definitions are from National Institute of Standards and Technology ([NIST Special Publication \(SP\) 800-12 Rev 1, An Introduction to Information Security](#).)

- Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set the stage for why organizations need to properly identify and protect against events that impact data integrity. Businesses must be confident that data is protected and safe.
- Attacks against an organization's data can compromise emails, employee records, financial records, and customer information—impacting business operations, revenue, and reputation.
- Examples of data integrity attacks include unauthorized insertion, deletion, or modification of data to corporate information such as emails, employee records, financial records, and customer data.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore methods to effectively identify and protect against data integrity attacks in various information technology (IT) enterprise environments to prevent impacts to business operations.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions before a detected data integrity cybersecurity event.



## CHALLENGE

Some organizations have experienced systemic attacks that force operations to cease. One variant of a data integrity attack—ransomware—encrypts data, rendering it unusable. This type of impact to data affects business operations and often leads them to shut down. Other variants of data integrity attacks can steer organizations to make decisions that can impact the bottom line or execute ill-fated decisions.

For example, adversarial actors could create backdoor accounts in company login systems, change payroll information to their benefit, or expose the company with unsafe software updates for their own benefit.

## SOLUTION

NIST published version 1.1 of the Cybersecurity Framework in April 2018 to help organizations better manage and reduce cybersecurity risk to critical infrastructure and other sectors. The framework core contains five functions, listed below.

- **Identify** – develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- **Protect** – develop and implement appropriate safeguards to ensure delivery of critical services
- **Detect** – develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- **Respond** – develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- **Recover** – develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident



For more information, see the [Framework for Improving Critical Infrastructure Cybersecurity](https://doi.org/10.6028/NIST.SP.1800-25).

Applying the Cybersecurity Framework to data integrity, this practice guide informs organizations of how to identify and protect assets against a data integrity attack, and in turn understand how to manage data integrity risks and implement the appropriate safeguards.

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to identify and protect assets against detected data integrity cybersecurity events. The solution isolates the opportunities that would allow for the cybersecurity events to occur and implements strategies to remediate the opportunities. Also, the solution applies additional protections from cybersecurity events to IT infrastructure.

In developing this solution, the NCCoE sought existing technologies that provided the following capabilities:

- **inventory**
- **policy enforcement**
- **logging**
- **backups**
- **vulnerability management**

- **secure storage**
- **integrity monitoring**

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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 solution.

## BENEFITS

This practice guide can help your organization:

- develop a strategy for identifying and protecting assets against a data integrity cybersecurity event
- facilitate comprehensive protection from adverse events to maintain operations and ensure the integrity of data critical to supporting business operations and revenue-generating activities
- manage enterprise risk (consistent with foundations of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*)

## SHARE YOUR FEEDBACK

You can view or download the guide at <https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect>. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at [ds-nccoe@nist.gov](mailto:ds-nccoe@nist.gov).

---

## TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.



CRYPTONITE NXT™



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.

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 challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

#### LEARN MORE

Visit <https://www.nccoe.nist.gov>  
[nccoe@nist.gov](mailto:nccoe@nist.gov)  
301-975-0200

## NIST SPECIAL PUBLICATION 1800-25B

---

# Data Integrity:

## Identifying and Protecting Assets Against Ransomware and Other Destructive Events

---

### Volume B:

#### Approach, Architecture, and Security Characteristics

#### Jennifer Cawthra

National Cybersecurity Center of Excellence  
NIST

#### Michael Ekstrom

#### Lauren Lusty

#### Julian Sexton

#### John Sweetnam

The MITRE Corporation  
McLean, Virginia

December 2020

FINAL

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

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



## DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-25B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-25B, 50 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](mailto: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](mailto:nccoe@nist.gov)

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

## ABSTRACT

Ransomware, destructive malware, insider threats, and even honest user mistakes present ongoing threats to organizations. Organizations' data, such as database records, system files, configurations, user files, applications, and customer data, are all potential targets of data corruption, modification, and destruction. Formulating a defense against these threats requires two things: a thorough knowledge of the assets within the enterprise, and the protection of these assets against the threat of data corruption and destruction. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, has built an example solution to address these data integrity challenges.



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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

Name	Organization
Kyle Black	Bay Dynamics
Sunjeet Randhawa	Broadcom Inc.
Peter Romness	Cisco Systems
Matthew Hyatt	Cisco Systems
Hans Ismirnioglou	Cryptonite
Sapna George	Cryptonite
Justin Yackoski	Cryptonite
Steve Petruzzo	GreenTec USA
Steve Roberts	Micro Focus
Timothy McBride	NIST

Name	Organization
Christopher Lowde	Semperis
Thomas Leduc	Semperis
Darren Mar-Elia	Semperis
Kirk Lashbrook	Semperis
Mickey Bresman	Semperis
Jim Wachhaus	Tripwire
Humphrey Christian	Symantec Corporation
Jon Christmas	Symantec Corporation
Kenneth Durbin	Symantec Corporation
Matthew Giblin	Symantec Corporation
Nancy Correll	The MITRE Corporation
Chelsea Deane	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Milissa McGinnis	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Denise Schiavone	The MITRE Corporation

Name	Organization
Anne Townsend	The MITRE Corporation

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Data Loss Prevention v15.1
Cisco Systems	Cisco ISE v2.4, Cisco Web Security Appliance v10.1
GreenTec USA	GreenTec WORMdisk v151228
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7, Tripwire IP360 v9.0.1
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Cryptonite	CryptoniteNXT v2.9.1
Semperis	Semperis Active Directory Forest Recovery v2.5, Semperis Directory Services Protector v2.7

# Contents

<b>1</b>	<b>Summary.....</b>	<b>1</b>
1.1	Challenge.....	2
1.2	Solution.....	2
1.3	Benefits.....	3
<b>2</b>	<b>How to Use This Guide .....</b>	<b>4</b>
2.1	Typographic Conventions.....	5
<b>3</b>	<b>Approach .....</b>	<b>6</b>
3.1	Audience.....	6
3.2	Scope .....	6
3.3	Assumptions .....	7
3.4	Risk Assessment .....	7
3.4.1	Risk.....	8
3.4.2	Security Control Map .....	9
3.5	Technologies.....	14
<b>4</b>	<b>Architecture .....</b>	<b>17</b>
4.1	Architecture Description .....	17
4.1.1	High-Level Architecture .....	17
4.1.2	Architecture Components.....	18
<b>5</b>	<b>Security Characteristic Analysis.....</b>	<b>22</b>
5.1	Assumptions and Limitations .....	22
5.2	Build Testing .....	22
5.3	Scenarios and Findings .....	22
5.3.1	Ransomware via Web Vector and Self-Propagation.....	23
5.3.2	Destructive Malware via USB Vector .....	24
5.3.3	Accidental VM Deletion via Maintenance Script .....	24
5.3.4	Backdoor Creation via Email Vector .....	25
5.3.5	Database Modification via Malicious Insider .....	26

5.3.6	File Modification via Malicious Insider .....	27
5.3.7	Backdoor Creation via Compromised Update Server .....	28
5.3.8	New Employee .....	28
<b>6</b>	<b>Future Build Considerations .....</b>	<b>29</b>
<b>Appendix A</b>	<b>List of Acronyms .....</b>	<b>30</b>
<b>Appendix B</b>	<b>Glossary .....</b>	<b>31</b>
<b>Appendix C</b>	<b>References .....</b>	<b>35</b>
<b>Appendix D</b>	<b>Functional Evaluation .....</b>	<b>37</b>
D.1	Data Integrity Functional Test Plan .....	37
D.2	Data Integrity Use Case Requirements .....	38
D.3	Test Case: Data Integrity IP-1 .....	42
D.4	Test Case: Data Integrity IP-2 .....	43
D.5	Test Case: Data Integrity IP-3 .....	44
D.6	Test Case: Data Integrity IP-4 .....	45
D.7	Test Case: Data Integrity IP-5 .....	46
D.8	Test Case: Data Integrity IP-6 .....	47
D.9	Test Case: Data Integrity IP-7 .....	48
D.10	Test Case: Data Integrity IP-8 .....	49

## List of Figures

<b>Figure 4-1</b>	<b>DI Identify and Protect High-Level Architecture .....</b>	<b>17</b>
-------------------	--	-----------

## List of Tables

<b>Table 3-1</b>	<b>DI Reference Design Cybersecurity Framework Core Components Map .....</b>	<b>10</b>
<b>Table 3-2</b>	<b>Products and Technologies .....</b>	<b>15</b>
<b>Table 6-1</b>	<b>Test Case Fields .....</b>	<b>37</b>
<b>Table 6-2</b>	<b>Capability Requirements .....</b>	<b>38</b>

Table 6-3 Test Case ID: Data Integrity IP-1.....	42
Table 6-4 Test Case ID: Data Integrity IP-2.....	43
Table 6-5 Test Case ID: Data Integrity IP-3.....	44
Table 6-6 Test Case ID: Data Integrity IP-4.....	45
Table 6-7 Test Case ID: Data Integrity IP-5.....	46
Table 6-8 Test Case ID: Data Integrity IP-6.....	47
Table 6-9 Test Case ID: Data Integrity IP-7.....	48
Table 6-10 Test Case ID: Data Integrity IP-8.....	49

# 1 Summary

Businesses face a near-constant threat of destructive malware, ransomware, malicious insider activities, and even honest mistakes that can alter or destroy critical data. These types of adverse events ultimately impact data integrity (DI). It is imperative for organizations to be able to identify assets that may be impacted by a DI attack and to protect their enterprise against such attacks.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore methods to identify and protect assets from a data corruption event in various information technology (IT) enterprise environments. The example solution outlined in this guide describes the solution built in the NCCoE lab. It encourages identification of vulnerabilities and assets that may be present in the enterprise, as well as several protections that can significantly mitigate the effects of DI attacks before they occur.

The goals of this NIST Cybersecurity Practice Guide are to help organizations confidently:

- identify systems, users, data, applications, and entities on the network
- identify vulnerabilities in enterprise components and clients
- baseline the integrity and activity of enterprise systems, in preparation for an attack
- create backups of enterprise data in advance of an attack
- protect these backups and other potentially important data against alteration
- manage enterprise health by assessing machine posture

For ease of use, a short description of the different sections of this volume follows.

- **Section 1:** Summary presents the challenge addressed by the NCCoE project, with an in-depth look at our approach, the architecture, and the security characteristics we used; the solution demonstrated to address the challenge; benefits of the solution; and technology partners that participated in building, demonstrating, and documenting the solution. The Summary also explains how to provide feedback on this guide.
- **Section 2:** How to Use This Guide explains how readers—business decision makers, program managers, and IT professionals (e.g., systems administrators)—might use each volume of the guide.
- **Section 3:** Approach offers a detailed treatment of the scope of the project and describes the assumptions on which the security platform development was based, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.
- **Section 4:** Architecture describes the usage scenarios supported by project security platforms, including Cybersecurity Framework [1] functions supported by each component contributed by our collaborators.

- [Section 5](#): Security Characteristics Analysis provides details about the tools and techniques we used to perform risk assessments.
- [Section 6](#): Future Build Considerations is a brief treatment of other Data Security implementations NIST considers consistent with Framework Core Functions: Identify, Protect, Detect and Respond, and Recovery.

## 1.1 Challenge

Thorough collection of quantitative and qualitative data is important to organizations of all types and sizes. It can impact all aspects of a business, including decision-making, transactions, research, performance, and profitability. When these data collections sustain a DI attack caused by unauthorized insertion, deletion, or modification of information, the attack can affect emails, employee records, financial records, and customer data, rendering them unusable or unreliable. Some organizations have experienced systemic attacks that caused a temporary cessation of operations. One variant of a DI attack—ransomware—encrypts data and holds it hostage while the attacker demands payment for the decryption keys.

Before DI events occur, organizations should identify their assets and vulnerabilities and have defenses and preparations in place to preemptively mitigate the events. This reduces the workload of actions to take during and after an attack occurs, as well as the enterprise's data loss and number of successful attacks.

## 1.2 Solution

The NCCoE implemented a solution that incorporates appropriate actions before the start of a DI event. The solution comprises systems working together to identify and protect assets against a data corruption event in standard enterprise components. These components include mail servers, databases, end user machines, virtual infrastructure, and file share servers. Essential to protection of assets is understanding of what those assets are and what vulnerabilities they have.

The NCCoE sought existing technologies that provided the following capabilities:

- **inventory**
- **policy enforcement**
- **logging**
- **backups**
- **vulnerability management**
- **secure storage**
- **integrity monitoring**



In developing our solution, we used standards and guidance from the following sources, which can also provide your organization with relevant standards and best practices:

- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (commonly known as the NIST Cybersecurity Framework) [\[1\]](#)
- NIST Interagency or Internal Report (NISTIR) 8050: *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy* [\[2\]](#)
- NIST Special Publication (SP) 800-30 Rev. 1: *Guide for Conducting Risk Assessments* [\[3\]](#)
- NIST SP 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [\[4\]](#)
- NIST SP 800-39: *Managing Information Security Risk* [\[5\]](#)
- NIST SP 800-40 Rev. 3: *Guide to Enterprise Patch Management Technologies* [\[6\]](#)
- NIST SP 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and Organizations* [\[7\]](#)
- Federal Information Processing Standard 140-3: *Security Requirements for Cryptographic Modules* [\[8\]](#)
- NIST SP 800-86: *Guide to Integrating Forensic Techniques into Incident Response* [\[9\]](#)
- NIST SP 800-92: *Guide to Computer Security Log Management* [\[10\]](#)
- NIST SP 800-100: *Information Security Handbook: A Guide for Managers* [\[11\]](#)
- NIST SP 800-34 Rev. 1: *Contingency Planning Guide for Federal Information Systems* [\[12\]](#)
- Office of Management and Budget, Circular Number A-130: *Managing Information as a Strategic Resource* [\[13\]](#)
- NIST SP 800-61 Rev. 2: *Computer Security Incident Handling Guide* [\[14\]](#)
- NIST SP 800-83 Rev. 1: *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [\[15\]](#)
- NIST SP 800-150: *Guide to Cyber Threat Information Sharing* [\[16\]](#)
- NIST SP 800-184: *Guide for Cybersecurity Event Recovery* [\[17\]](#)

## 1.3 Benefits

The NCCoE's practice guide can help your organization:

- develop a plan for identifying assets and vulnerabilities and protecting these assets from a cybersecurity event
- facilitate detection, response, and recovery from a DI event by collecting information about the enterprise before an attack occurs

- maintain integrity and availability of data critical to supporting business operations and revenue-generating activities
- manage enterprise risk (consistent with the foundations of the NIST Cybersecurity Framework)

## 2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the DI identify-and-protect solution. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-25A: *Executive Summary*
- NIST SP 1800-25B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-25C: *How-To Guides* – instructions for building the example solution

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

**Business decision makers, including chief security and technology officers**, will be interested in the *Executive Summary*, NIST SP 1800-25A, which describes the following topics:

- challenges that enterprises face in identifying assets and protecting them from DI 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 this part of the guide, NIST SP 1800-25B, 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 1800-25A, with your leadership team members to help them understand the importance of adopting a standards-based solution to identify and protect assets from DI attacks.

**IT professionals** who want to implement such an approach will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-25C, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create 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 DI identify-and-protect solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. [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](mailto:ds-nccoe@nist.gov).

Acronyms used in figures can be found in the Acronyms appendix.

## 2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b><code>service sshd start</code></b>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a> .

## 3 Approach

Based on key points expressed in NISTIR 8050, *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy* (2015), the NCCoE is pursuing a series of DI projects to map the Core Functions of the NIST Cybersecurity Framework. This project is centered on the Core Functions of Identify and Protect, which consist of identifying assets and protecting them from DI attacks. For instance, the first step in building a strategy requires an organization to inventory its assets. This involves identifying systems, applications, data sources, users, and other relevant entities that may be targets or facilitators of DI attacks. Once this exercise is complete, an organization can then create a customized strategy to protect the identified assets against the possibility of data corruption, modification, and destruction. NCCoE engineers working with a community of interest (COI) defined the requirements for this DI project.

Members of the COI, which include participating vendors referenced in this document, contributed to development of the architecture and reference design, providing technologies that meet the project requirements and assisting in installation and configuration of those technologies. The practice guide highlights the approach used to develop the NCCoE reference solution. Elements include risk assessment and analysis, logical design, build development, test and evaluation, and security control mapping. This guide aims to provide practical guidance to any organization interested in implementing a solution for identifying and protecting assets against a cybersecurity event.

### 3.1 Audience

This guide is intended for individuals responsible for implementing security solutions in organizations' IT support activities. Current IT systems, particularly in the private sector, often lack the ability to comprehensively identify enterprise assets that need protection from integrity attacks, as well as the protections themselves. The platforms demonstrated by this project, and the implementation information provided in these practice guides, permit integration of products to implement a data identification and protection system. The technical components will appeal to system administrators, IT managers, IT security managers, and others directly involved in the secure and safe operation of business IT networks.

### 3.2 Scope

The guide provides practical, real-world guidance on developing and implementing a DI solution consistent with the principles in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 [1], specifically the Core Functions of Identify and Protect. The Identify Function emphasizes the development and implementation of the appropriate activities to discover and manage an organization's assets, services, and the threats to these assets and services. The Protect Function emphasizes development and implementation of activities that protect these assets and services from

cybersecurity events. Examples of outcomes within these Functions include asset inventory, logging, backups, vulnerability management, policy enforcement, and file/system integrity management.

### 3.3 Assumptions

This project is guided by the following assumptions:

- The solution was developed in a lab environment. The environment is based on a generic organization's IT enterprise—it uses services found commonly across typical enterprises, such as a database, a domain controller, a mail/web server, etc. It does not reflect the complexity of a production environment, for example, building across numerous physical locations, accommodating for extreme working conditions, or configuring systems to meet specific network/user needs. These demands can all increase the level of complexity needed to implement a DI solution.
- An organization has access to the skills and resources required to implement an asset identification and protection system.
- An organization is seeking to preemptively mitigate the damage a DI event would cause.

### 3.4 Risk Assessment

[NIST SP 800-30 Revision 1, \*Guide for Conducting Risk Assessments\*](#) states that risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.”

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of [NIST SP 800-37 Revision 2, \*Risk Management Framework for Information Systems and Organizations\*](#)—material available to the public. The [Risk Management Framework \(RMF\)](#) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

We performed two types of risk assessments:

- Initial analysis of the risk factors discussed with financial, retail, and hospitality institutions: this analysis led to creation of the DI project and desired security posture. See NISTIR 8050, *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy*, for additional participant information.

- Analysis of how to secure the components within the solution and minimize any vulnerabilities they might introduce: see [Section 5](#), Security Characteristic Analysis.

### 3.4.1 Risk

Using the guidance in NIST's series of publications concerning risk, we worked with financial institutions and the Financial Sector Information Sharing and Analysis Center to identify the most compelling risk factors encountered by this business group. We participated in conferences and met with members of the financial sector to define the main security risks to business operations. From these discussions came identification of an area of concern—DI. We produced the practice guide *Data Integrity: Recovering from Ransomware and Other Destructive Events*, which primarily focused on the recovery aspect of DI. From responses to the recovery project, we also identified a need for guidance in identifying and protecting assets from DI attacks.

When considering risk from the perspective of identifying and protecting assets prior to a cybersecurity event, we must consider not only the impact of an event on an organization's assets but also the threats to those assets and the potential vulnerabilities these threats could exploit.

When discussing threats to an organization's assets from the perspective of DI, we consider the following factors:

- malware
- insider threats
- accidents caused by human error
- compromise of trusted systems

Types of vulnerabilities we consider in relation to these threats are:

- zero-day vulnerabilities
- vulnerabilities due to outdated or unpatched systems
- custom software vulnerabilities/errors
- social engineering and user-driven events
- poor access control

Finally, we consider the potential impact on an organization from a DI event:

- systems incapacitated
- modification/deletion of organization's assets
- negative impact on the organization's reputation

Analyses of the threats, vulnerabilities, and potential impact to an organization give us an understanding of the risk to an organization with respect to DI. NIST SP 800-39, *Managing Information Security Risk*, focuses on the business aspect of risk, namely at the enterprise level. This understanding is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. The following summary lists the strategic risk areas we identified and their mitigations:

- Impact on system function: ensuring the availability of accurate data or sustaining an acceptable level of DI reduces the risk of systems' availability being compromised.
- Cost of implementation: implementing asset identification and protection from DI events once and using it across all systems may reduce system continuity costs.
- Compliance with existing industry standards contributes to the industry requirement to maintain a continuity of operations plan.
- Maintenance of reputation and public image helps reduce level and likelihood of impact as well as facilitates the information required for impact reduction.
- Increased focus on DI includes not just loss of confidentiality but also harm from unauthorized alteration of data (per NISTIR 8050).

We subsequently translated the risk factors identified to security Functions and Subcategories within the NIST Cybersecurity Framework. In [Table 3-1](#), we mapped the categories to NIST SP 800-53 Rev. 4 controls.

### 3.4.2 Security Control Map

As explained in [Section 3.4.1](#), we identified the Cybersecurity Framework Functions and Subcategories that we wanted the reference design to support, through a risk analysis process. This was a critical first step in designing the reference design and example implementation to mitigate the risk factors. [Table 3-1](#) lists the addressed Cybersecurity Framework Functions and Subcategories and maps them to relevant NIST standards, industry standards, and controls and best practices. The references provide solution validation points in that they list specific security capabilities that a solution addressing the Cybersecurity Framework Subcategories would be expected to exhibit. Organizations can use [Table 3-1](#) to identify the Cybersecurity Framework Subcategories and NIST SP 800-53 Rev. 4 controls they are interested in addressing.

When cross-referencing Functions of the Cybersecurity Framework with product capabilities used in this practice guide, it is important to consider:

- This practice guide, though primarily focused on Identify/Protect Functions also uses DE.CM-8 and RS.MI-3, Detect and Respond Subcategories respectively. This is primarily because these two Subcategories deal with vulnerability discovery and mitigation, which are techniques used to prevent future damage and are not as useful for preventing attacks previously exploited a given vulnerability. Often, it is unlikely that an organization will be able to resolve a newly

discovered vulnerability during an attack; for attacks where patches are available, it can be dangerous to allow updates on a compromised system.

- Not all the guidance of Cybersecurity Framework Subcategories can be implemented using technology. Any organization executing a DI solution would need to adopt processes and organizational policies that support the reference design. For example, some of the Subcategories within the Cybersecurity Framework Function known as Identify are processes and policies that should be developed prior to implementing recommendations.

**Table 3-1 DI Reference Design Cybersecurity Framework Core Components Map**

Cybersecurity Framework v1.1				Standards and Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.	CM-8, PM-5	A.8.1.1, A.8.1.2	OM-STS-001
		ID.AM-2: Software platforms and applications within the organization are inventoried.	CM-8, PM-5	A.8.1.1, A.8.1.2, A.12.5.1	OM-STS-001
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	A.12.6.1, A.18.2.3	PR-VAM-001
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	SI-5, PM-15, PM-16	A.6.1.4	CO-OPL-002
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	RA-2, RA-3, PM-16	A.12.6.1	SP-SYS-001



Cybersecurity Framework v1.1				Standards and Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
PROTECT (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	SP-DEV-001, OV-PMA-003
		PR.AC-3: Remote access is managed.	AC-1, AC-17, AC-19, AC-20, SC-15	A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1	SP-SYS-001, OM-ADM-001
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	OM-STS-001
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	AC-4, AC-10, SC-7	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	OM-NET-001
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected.	MP-8, SC-12, SC-28	A.8.2.3	OM-DTA-002
		PR.DS-2: Data-in-transit is protected.	SC-8, SC-11, SC-12	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	OM-DTA-002, PR-CDA-001

Cybersecurity Framework v1.1				Standards and Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	SC-16, SI-7	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	OM-DTA-001
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	SP-ARC-001
		PR.IP-3: Configuration change control processes are in place.	CM-3, CM-4, SA-10	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	SP-DEV-001, OM-ANA-001
		PR.IP-4: Backups of information are conducted, maintained, and tested.	CP-4, CP-6, CP-9	A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3	SP-SYS-001
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	PR-CIR-001
		PR.IP-10: Response and recovery plans are tested.	CP-4, IR-3, PM-14	A.17.1.3	SP-SYS-001

Cybersecurity Framework v1.1				Standards and Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
		PR.IP-12: A vulnerability management plan is developed and implemented.	RA-3, RA-5, SI-2	A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3	SP-RSK-002
	Maintenance (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	MA-2, MA-3, MA-5, MA-6	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6	OM-ADM-001
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	MA-4	A.11.2.4, A.15.1.1, A.15.2.1	SP-TRD-001
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	AU Family	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	OV-LGA-002
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	AC-3, CM-7	A.9.1.2	PR-CDA-001, OM-ANA-001

Cybersecurity Framework v1.1				Standards and Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
		PR.PT-4: Communications and control networks are protected.	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	A.13.1.1, A.13.2.1, A.14.1.3	SP-ARC-002
<b>DETECT (DE)</b>	Security Continuous Monitoring (DE.CM)	DE.CM-8: Vulnerability scans are performed.	RA-5	A.12.6.1	SP-TRD-001
<b>RE-SPOND (RS)</b>	Mitigation (RS.MI)	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	CA-7, RA-3, RA-5	A.12.6.1	PR-CIR-001

### 3.5 Technologies

[Table 3-2](#) lists all the technologies used in this project and provides a mapping among the generic application term, the specific product used, and the security control(s) the product provides. Refer to [Table 3-1](#) for an explanation of the NIST Cybersecurity Framework Subcategory codes.

Please note that PR.AC-4 is not included in this table. Access controls are detailed more thoroughly in other NCCoE practice guides [\[18\]](#), [\[19\]](#). For the purposes of this practice guide, we assume a minimal Active Directory setup with an administrator and several users.

**Table 3-2 Products and Technologies**

Component	Product	Function	Cybersecurity Framework Subcategories
Inventory	Cisco ISE v2.4	<ul style="list-style-type: none"> <li>• Identification and status information for users</li> <li>• Identification and status information for devices</li> <li>• Identification and status information for software</li> <li>• Identification and status information for data assets</li> </ul>	ID.AM-1, ID.AM-2, PR.AC-1, PR.PT-2
	Symantec Data Loss Prevention (DLP) v15.1		
Vulnerability Management	Tripwire IP360 v9.0.1	<ul style="list-style-type: none"> <li>• Identification for vulnerabilities on various systems in the enterprise</li> <li>• An interface for managing/prioritizing vulnerabilities, based on organizational needs</li> </ul>	ID.RA-1, ID.RA-5, PR.IP-12, DE.CM-8, RS.MI-3
Policy Enforcement	Cisco ISE v2.4	<ul style="list-style-type: none"> <li>• Enforce machine posture across an enterprise</li> <li>• Quarantine machines that do not comply with organizational policy</li> </ul>	ID.RA-1, PR.AC-3, PR.MA-1, PR.MA-2, RS.MI-3
Integrity Monitoring	Tripwire Enterprise v8.7	<ul style="list-style-type: none"> <li>• Baselines integrity activity for data</li> <li>• Baselines integrity activity for Active Directory</li> <li>• Provides file hashes and integrity baselines for files and software, regardless of file type</li> </ul>	PR.DS-6, PR.IP-3, PR.PT-1
	Semperis Directory Services Protector (DSP) v2.7		
Logging	Micro Focus ArcSight Enterprise Security Manager (ESM) v7.0 Patch 2	<ul style="list-style-type: none"> <li>• Provides auditing and logging capabilities configurable to corporate policy</li> <li>• Provides logs of baseline network operations</li> </ul>	PR.IP-1, PR.IP-3, PR.PT-1

Component	Product	Function	Cybersecurity Framework Subcategories
	Tripwire Log Center v7.3.1	<ul style="list-style-type: none"> <li>Provides logs of database activity and database backup operations</li> <li>Provides logs of integrity changes</li> <li>Provides logs of some user activity of monitored systems</li> </ul>	
Backups	Semperis Active Directory Forest Recovery (ADFR) v2.5	<ul style="list-style-type: none"> <li>Backs up Active Directory information</li> <li>Backs up systems</li> <li>Backs up configurations</li> <li>Backs up organizational data</li> </ul>	PR.DS-1, PR.IP-3, PR.IP-4, PR.IP-9, PR.IP-10
	FileZilla v0.9.60.2 OPEN SOURCE		
	Duplicati v2.0.3.3 OPEN SOURCE		
Secure Storage	GreenTec WORMdisk v151228	<ul style="list-style-type: none"> <li>Provides immutable storage</li> <li>Provides configurable prevention of backup modification</li> </ul>	PR.DS-1, PR.IP-4
Network Protection	CryptoniteNXT v2.9.1	<ul style="list-style-type: none"> <li>Prevents unapproved network communication</li> <li>Prevents malicious reconnaissance</li> <li>Quarantines unauthorized machines on the network</li> </ul>	ID.AM-1, PR.AC-1, PR.AC-3, PR.AC-5, PR.DS-2, PR.PT-4
Denylisting	Cisco Web Security Appliance v10.1	<ul style="list-style-type: none"> <li>Provides capability to denylist websites</li> <li>Provides capability to denylist communication with malicious or disallowed IP addresses</li> </ul>	PR.AC-3, PR.AC-5, PR.DS-2, PR.PT-4

## 4 Architecture

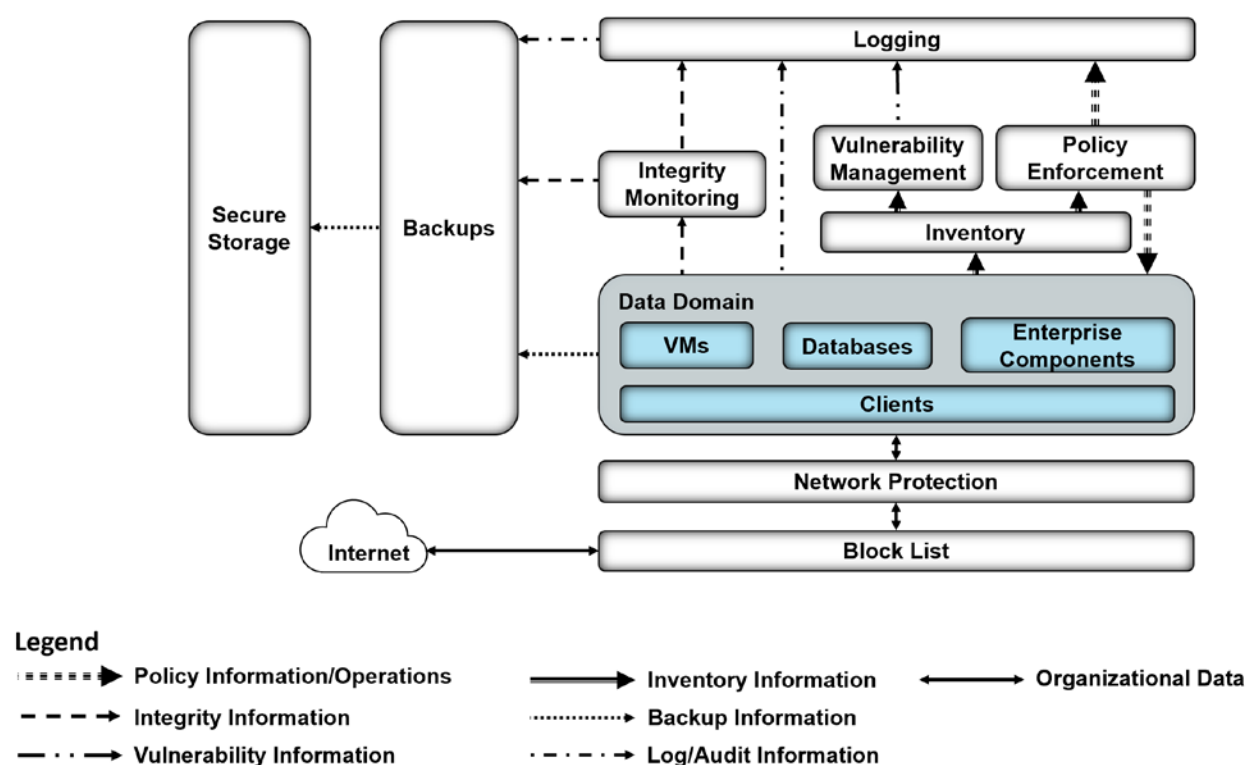
This section presents the high-level architecture used for implementation of a DI solution that identifies and protects assets from ransomware and other destructive events.

### 4.1 Architecture Description

#### 4.1.1 High-Level Architecture

The DI solution is designed to address the security Functions and Subcategories described in Table 3-1 and is composed of the capabilities illustrated in Figure 4-1.

Figure 4-1 DI Identify and Protect High-Level Architecture



- **Inventory** allows discovering and keeping track of devices connected to the enterprise.
- **Vulnerability management** provides a mechanism for analyzing various system and network components, for a better understanding of resolved and unresolved vulnerabilities in the enterprise.
- **Policy enforcement** uses feedback from logs and vulnerability management to target machines with unresolved vulnerabilities and maintain overall enterprise health.

- **Integrity monitoring** establishes baselines of file/system integrity.
- **Logging** records and stores all the log files produced by the components within the enterprise.
- **Backups** allow components within the enterprise to produce backups.
- **Secure storage** allows data storage with additional data protection measures, such as Write Once Read Many (WORM) technologies. Data encryption can also be used, but this will not inherently protect data against corruption.
- **Network protection** can defend an enterprise network against both intrusion and lateral movement of malicious actors and programs.
- **Denylisting** can filter allowed programs or network communications. Often, this may be provided in the form of a firewall or even an allowlist, but products exist that allow finer-grained control over these filters.

These capabilities work together to provide the functions of Identify and Protect for the reference architecture. The inventory capability allows accurate and complete discovery and status reporting of all network assets. The inventory capability feeds into vulnerability management, which analyzes the assets and network for vulnerabilities. Vulnerability management feeds its information into the logging capability, which aggregates and collects logs from various sources for use as a baseline of normal system operations. Policy enforcement uses information from logging and vulnerability management, to repair vulnerabilities found in the enterprise and maintain the system with up-to-date patches. Integrity monitoring records normal file/system integrity information to be used as a baseline in the event of an attack and forwards this information to the logging capability as part of the organization's baseline. Backups create periodic backups of organizational data to be used in a cybersecurity event. Secure storage allows storing files—such as backups, gold images, logs, or configuration files—in a format that cannot be corrupted, because files cannot be altered or changed while in storage.

## 4.1.2 Architecture Components

### 4.1.2.1 Inventory

The inventory capability allows discovering and visualizing the enterprise's network as well as the present network devices. This component also informs the other components in the enterprise, providing information such as what systems to monitor, back up, and scan for vulnerabilities. This component provides the basic knowledge of what assets there are to protect.

For the inventory capability, we use a combination of two products: Cisco ISE and Symantec DLP. Cisco ISE provides inventory capabilities for machines, devices, and users on its network and can use that information in tandem with other capabilities. Symantec DLP provides data asset inventory, allowing organizations to identify potentially sensitive data.



#### *4.1.2.2 Vulnerability Management*

The vulnerability management capability allows scanning and managing vulnerabilities across the enterprise. It provides a priority system for these vulnerabilities, as well as logs on existing vulnerabilities and potentially resolved vulnerabilities. The information produced by this capability informs the policy enforcement capability, which aims to fix the discovered vulnerabilities or quarantine the machine until they are fixed.

For the vulnerability management capability, we use Tripwire IP360. Tripwire IP360 is a vulnerability scanner and management tool, which can scan a variety of hosts for known vulnerabilities and report on the results. Furthermore, the tool can manage and assign risk levels to these vulnerabilities, allowing security teams to effectively manage vulnerabilities throughout the enterprise.

#### *4.1.2.3 Policy Enforcement*

Through various mechanisms, the policy enforcement capability maintains the health of the enterprise. Policy enforcement acts on log information provided by the inventory and vulnerability management capabilities, often with the help of a security team, to ensure the health and compliance of enterprise systems. This can include mechanisms such as pushing software updates, resolving vulnerabilities, or quarantining noncompliant machines, but the capabilities of policy enforcement tools vary from product to product.

For policy enforcement, we use Cisco ISE. Cisco ISE can identify machines on its network and perform a posture check on these machines. This can entail checking that certain services are enabled, that anti-malware is installed, or that certain files are present. Using this information, Cisco ISE can then disable network access to noncompliant machines.

#### *4.1.2.4 Integrity Monitoring*

Integrity monitoring provides the ability to test, understand, and measure attacks that occur on files and components within the enterprise. When considering DI from the perspective of protecting assets prior to an attack, it is important to establish an integrity baseline for files and systems across the enterprise, to be used in comparison with daily operations. The value of integrity monitoring becomes clear both during and after an attack. Alerts can be set to notify the security team to act when abnormal changes are detected to a file or system, such as changes made at abnormal times or by users who typically do not make changes to these assets. Furthermore, the information produced by integrity monitoring systems can be used to inform a recovery process; they provide information about what changes happened, when changes began to take place, as well as what programs were involved in the changes.

For integrity monitoring, we use a combination of two tools: Tripwire Enterprise and Semperis Directory Services Protector. Tripwire Enterprise is a file integrity monitoring tool that establishes a baseline for integrity activity within the enterprise. This baseline is used in the event of an attack, to detect and alert on changes within the enterprise as well as aid recovery should it be necessary. Semperis Directory

Services Protector also provides integrity monitoring, but for Active Directory it allows granular rollbacks of Active Directory changes and provides a baseline for any attacks on the enterprise account configuration.

#### *4.1.2.5 Logging*

Logging from each enterprise component serves several functions in an architecture that aims to identify and protect assets. Logs are produced through integrity monitoring, which aids in establishing a baseline for the enterprise's daily activity. Logs are also produced through vulnerability scanning and asset inventory, which inform policy enforcement: maintaining up-to-date systems requires information about what systems exist in the enterprise and their status.

For logging, we use a combination of two tools: Micro Focus ArcSight and Tripwire Log Center (TLC). While TLC's purpose in this build is primarily to collect, transform, and forward logs from Tripwire IP360 and Tripwire Enterprise to ArcSight, ArcSight performs a wider function. ArcSight collects logs from various sources in the enterprise, such as vulnerability management, backups, network protection, denylisting, inventory, integrity monitoring, as well as Windows event logs and Ubuntu syslogs. This widespread collection aims to provide a baseline for activity throughout the enterprise. ArcSight can analyze and alert, which can be used in the event of an attack, but it requires thorough log collection from all components of the enterprise.

#### *4.1.2.6 Backups*

The backups capability backs up both the organization's data and data from other components, such as logs and integrity information. These backups are most often used as part of the Recover Function as part of the restoration process. Backups must be taken prior to an event to be useful, though; the restoration process requires backups from before the event to adequately restore a system.

The configuration of this capability needs to align with the tempo of the enterprise. For example, if an enterprise performs thousands of transactions per hour per day, then a backup solution that performs a backup only once a day would not adequately provide for the enterprise. This type of configuration would allow a potentially large data loss. If backups occur every morning and a loss of DI happened at the end of the day, then a full day's worth of transactions would be lost. The decision for the correct configuration of backups is determined by an organization's risk tolerance.

For the backups capability, we use a combination of two open-source tools: FileZilla and Duplicati. FileZilla is a user-based File Transfer Protocol (FTP) server with the option to force FTP over Transport Layer Security (TLS). It allows control over where individual users/groups store files, and its primary purpose in this build is as a receptacle for backups produced by Duplicati. Duplicati is a client-based backup system configured on individual hosts to back up to a provided FTP server. It packages and encrypts backups before sending them to the FTP server, potentially on a schedule.

We also use Semperis ADFR to provide more fine-grained backups for Active Directory. As Active Directory is often critical to enterprise operations, Semperis ADFR is designed to work off-site in the event of a disaster.

#### *4.1.2.7 Secure Storage*

Secure storage stores the most critical files for an enterprise. These include backup data, configuration files, logs, golden images, and other files critical to both system operation and the organization's mission. Additional measures need to be applied to provide increased security to these files so they are not subject to attacks or corruption.

For secure storage, we use GreenTec's WORMdisk, a transparent hard disk that can prevent any data deletion and modification at a firmware level. WORMdisks provide a user-friendly graphical user interface and a command line interface for automating locking and disk rotation. In this architecture they are used primarily to store backups to prevent any damage to the backups, but they can be used at the discretion of the organization to store other critical files.

#### *4.1.2.8 Network Protection*

Network protection defends the network against threats that require network movement. This should preemptively protect against lateral movement, in which malware or a malicious actor attempts to spread across machines in the network. Furthermore, it should also protect against external threats attempting to gain access to the network.

For network protection, we use CryptoniteNXT. CryptoniteNXT provides zero-trust moving-target defense for the network it protects. This means that all enterprise communication goes through the CryptoniteNXT device, which provides granular access control for allowed types of communication. This allows defense against lateral propagation. Furthermore, as internet protocol (IP) addresses are dynamic and managed by CryptoniteNXT, reconnaissance is significantly more difficult for attackers on and outside the network.

#### *4.1.2.9 Denylisting*

Denylisting enables control of allowed communications and applications within an enterprise. This may include restricting installed software on enterprise machines to a predefined list or specifically disallowing software. Furthermore, it should restrict network communication with websites, servers, or external actors as well as restrict based on protocol or port usage. Some of these capabilities are covered by firewalls, but further control can allow more complex policies based on the organization's needs.

For the denylisting capability we use Cisco Web Security Appliance (WSA). Cisco WSA enables enterprises to denylist web traffic through a proxy. This allows for prevention of malware downloads from known malicious websites as identified by site reputation updates from Cisco Talos threat

intelligence. These websites can also be identified through the implementation of a Detect and Respond build and can also be provided by an integration with other information sharing services.

## 5 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating a DI identify-and-protect solution. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

### 5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

### 5.2 Build Testing

The purpose of the security characteristic analysis is to understand the extent to which the building block meets its objective of identifying enterprise assets and vulnerabilities. Furthermore, the project aims to protect these assets prior to the start of an attack. In addition, it seeks to understand the security benefits and drawbacks of the reference design. To accomplish this, we created a set of use cases—each an individual attack on DI with different aspects to test various parts of the build.

When doing this, we aim not to test individual components for their capabilities but rather for the ability of the architecture to deal with these use cases. Furthermore, as this architecture is focused on defending against attacks before they happen, the resolutions to these use cases are primarily preventative rather than responsive.

### 5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

Below is a list of the scenarios created to test various aspects of this architecture. More detailed resolutions and mappings of these scenarios' requirements to the Cybersecurity Framework can be found in [Appendix D](#).

### 5.3.1 Ransomware via Web Vector and Self-Propagation

#### 5.3.1.1 Scenario

The following scenario was simulated to test the architecture's defense against ransomware.

A user mistakenly downloads ransomware from an external web server. When the user executes this malicious software, it generates a cryptographic key, which is sent back to the external web server. The malware then utilizes a privilege escalation exploit to propagate across the network. The malicious software encrypts files on the machines it propagated to, and it demands payment in exchange for decrypting these files.

#### 5.3.1.2 Resolution

This build provides a significant defense in depth against this use case to prevent the majority of its functions from taking place.

The **denylisting** capability is used to prevent the user from reaching the malicious site that hosts the ransomware, preventing the download before it happens.

The **vulnerability management** capability is used to detect the vulnerability exploited by the ransomware to propagate, allowing resolution before the attack occurs.

The **network protection** capability is used to prevent the ransomware's propagation by disallowing network traffic between computers on the network, through a traffic allowlist policy.

The **inventory** capability is used to identify the enterprise's assets for backup and monitoring.

The **backups** capability is used to take backups of potential ransomware targets before the attack hits, nullifying the effects of potential attacks on files.

The **integrity monitoring** capability, in tandem with the **logging** capability, is used to take a baseline of the file system, so that an attack on the file system is detected and the scope can be identified.

#### 5.3.1.3 Other Considerations

Malware comes in many forms and from many places, and as a result, requires a defense in depth against it. For example, though preventing a piece of malware from getting on enterprise systems may be possible through denylisting a website, it is often impossible to have full knowledge of all malicious websites before an attack happens. Because of this, other tools are necessary to prevent the effects of malware at every step of its potential execution, and preparation is necessary to mitigate effects.

It is important to improve upon these capabilities over time by learning from attacks on the enterprise and from attacks on other enterprises. Both information-sharing technologies and after-the-fact analysis of attacks can inform capabilities to prevent future attacks.

## 5.3.2 Destructive Malware via USB Vector

### 5.3.2.1 Scenario

The following scenario was simulated to test the architecture's defense against destructive malware.

A user finds an unmarked Universal Serial Bus (USB) device and inserts it into their system. The USB device contains malicious software that may run automatically or with user interaction. The malicious software modifies and deletes the user's files, removing text from text files and entirely deleting any media files it finds. The software does not offer a recovery mechanism as ransomware might, aiming only to corrupt files.

### 5.3.2.2 Resolution

This build provides two main layers of defense against this scenario: backups and Integrity baselining.

The **integrity monitoring** capability provides a baseline for file system activity as a point of comparison post-modification/deletion.

The **logging** capability provides a baseline for events across the enterprise, including typical USB and file modification activity.

The **backups** capability provides the ability to take backups of the file system, allowing restoration of files after the incident is resolved.

### 5.3.2.3 Other Considerations

A use case involving USBs is often best prevented through organizational training. In some cases, just the action of inserting the USB is enough to destroy an entire system on a physical level. Furthermore, not all malicious USBs will be file systems with auto-run malware on them—they can come disguised as keyboards or use lower-level attacks. Because of this, it is important for organizations to educate members on the dangers of unknown USB insertion, while also preparing if the attack occurs anyway.

## 5.3.3 Accidental VM Deletion via Maintenance Script

### 5.3.3.1 Scenario

The following scenario was simulated to test the architecture's defense against DI events that occur on virtual machines (VMs).

A routine maintenance script on the system causes an error. During a move operation in the Hyper-V system, the script deletes an important VM. A maintenance script with an error of this type could be a side effect of a normal system function or an error made by a member of the organization. The build is expected to mitigate the damage caused to VMs in such an incident.

#### *5.3.3.2 Resolution*

This build provides two main layers of defense against this scenario: backups and Integrity baselining.

The **integrity monitoring** capability provides a baseline for virtual machine activity, as a point of comparison post-deletion.

The **logging** capability provides a baseline for events across the enterprise, including typical Hyper-V activity.

The **backups** capability enables backups of entire VMs. In the event of a deletion, these backups can be used to restore the VMs.

#### *5.3.3.3 Other Considerations*

The backups capability can also be installed on individual VMs, given proper networking, to back up the contents of VMs if desired. This will likely depend on the needs of the organization.

### 5.3.4 Backdoor Creation via Email Vector

#### *5.3.4.1 Scenario*

The following scenario was simulated to test the architecture's defense against malicious email attachments.

A user unknowingly opens a malicious attachment they received in an email. When opened, the attachment quietly fetches files from an external web server. It then creates several unapproved backdoor accounts on the authentication server. The build is expected to mitigate the impacts of such an incident.

#### *5.3.4.2 Resolution*

The build provides several layers of defense against this use case. The **integrity monitoring** capability provides a baseline for Active Directory as a point of comparison against a compromised system. Furthermore, it also provides a baseline of the file system, to aid in identifying the malicious file during and after the attack has happened.

The **logging** capability provides a baseline for activity across the enterprise, including the name of the account used to create the backdoors.

Lastly, the **denylisting** capability is used to prevent web requests to the malicious web server. This capability is informed by capabilities in the Respond Category of the Cybersecurity Framework.

#### *5.3.4.3 Other Considerations*

Note that for this scenario, prevention of the downloads before an attack happens requires organizations to know what web servers are “known bad.” Organizations can acquire this knowledge in two ways: through threat-sharing services and through self-information as part of the Respond Category of the Cybersecurity Framework. The former refers to services that collect the names of malicious domains and share them with customers. The latter refers to the addition of known-bad websites to the denylist after they are detected as malicious through the organization’s own logs and analytics during or after an event. This build allows protecting against attacks given this knowledge, but the knowledge must be gained in some way first.

Another defense that can partially prevent this use case is by denylisting the sender of the phishing email or sorting it into spam. However, as this is typically a function of the email provider and not a separate security solution, it is out of scope for this build.

### **5.3.5 Database Modification via Malicious Insider**

#### *5.3.5.1 Scenario*

The following scenario was simulated to test the architecture’s defense against unwanted database modification.

A malicious insider has access to an enterprise database through a web page. The insider leverages a vulnerability in the web page to delete a large portion of the database. Though this scenario deals with a web vulnerability, other vulnerabilities could be used to modify the database undesirably. The build is expected to mitigate a user’s potential impact on the database.

#### *5.3.5.2 Resolution*

This build provides two main layers of defense against this scenario: backups and Integrity baselining.

The **integrity monitoring** capability provides a baseline for database activity as a point of comparison post-deletion.

The **logging** capability provides a baseline for events across the enterprise, including typical database activity.

The **backups** capability enables backups of the entire database. In the event of a deletion, these backups can be used to restore the database.



### 5.3.5.3 Other Considerations

Creating backups of the entire database may, in some cases, be undesirable, particularly for enterprises that heavily use the database. For these cases, we recommend built-in database backups. Microsoft Structured Query Language databases have built-in backups that can be more granular than a full database backup.

For many applications, though, a periodic backup of the entire database is sufficient and potentially can be used in tandem with built-in database backups.

## 5.3.6 File Modification via Malicious Insider

### 5.3.6.1 Scenario

The following scenario was simulated to test the architecture's defense against malicious file and backup modification.

A malicious insider is assumed to have stolen administrator-level credentials through nontechnical means. The insider, using these credentials, uses remote Windows PowerShell sessions to uniformly modify employee stock information across several machines, to the insider's benefit. This attack will also target the enterprise's backups system, to modify all records of the previous stock information. The aspects of the build described above are expected to mitigate the ability of the user to target and modify enterprise data and backups. The method of securing administrator credentials will be considered out of scope for this solution.

### 5.3.6.2 Resolution

The build provides several layers of defense against this use case. Because this use case specifically targets the backups, the solution includes mechanisms for protecting and monitoring the backups.

The **inventory** capability is used to identify potentially sensitive information across the enterprise.

The **integrity monitoring** capability is used to baseline file activity, both for backups and for organizational files.

This information is forwarded to the **logging** capability for analysis.

The **backups** capability is used to take encrypted backups of the file system, preventing targeted attacks against information in the backups.

The **secure storage** capability is used to prevent write-access to the backups once taken, allowing a guarantee of modification/deletion protection for backups stored on the disk.

### 5.3.6.3 Other Considerations

A significant trade-off between memory and frequency of backups occurs when implementing a secure storage solution for backups. As WORM space may be limited by the number of disks purchased or by a cloud service's limitations, it is important for organizations to consider the cost of storing all backups in secure storage, especially for organizations that frequently take backups to reduce the loss of data.

## 5.3.7 Backdoor Creation via Compromised Update Server

### 5.3.7.1 Scenario

The following scenario was simulated to test the architecture's defense against compromised update servers.

An update server that services an enterprise machine is compromised and provides an update to the enterprise machine that contains a backdoor. The update contains a vulnerable version of vsftpd, allowing a malicious actor root access into the machine updated by the compromised server. The build is expected to mitigate the impact of a compromised update server.

### 5.3.7.2 Resolution

The build provides several layers of defense against this use case. The **integrity monitoring** capability is used to baseline the integrity of both files and programs, as an intrusion via compromised update server can potentially affect both. This aids in early detection and recovery.

The **backups** capability is used to back up the file system, to preemptively mitigate the damage done by the intrusion.

The **denylisting** capability is used to denylist the compromised update server, to prevent use of the update server by other machines.

### 5.3.7.3 Other Considerations

To prevent updates through denylisting, organizations should either use their denylisting capability as a transparent proxy or ensure that the update mechanism uses the proxy; the process for configuring this will differ between update mechanisms. The denylisting and network protection capabilities are especially important in the event of a breach, as these two can help prevent the spread of the intrusion.

## 5.3.8 New Employee

### 5.3.8.1 Scenario

The following scenario was simulated to test the architecture's identification capabilities with respect to machines and vulnerabilities.

A new employee joins the organization and connects their machine to the network. The machine, however, is not up-to-date on its patches and poses a security risk to the organization. The build is expected to be able to identify the machine and its noncompliance with organizational maintenance policy.

#### *5.3.8.2 Resolution*

The build provides several layers of defense against this use case. The **inventory** capability provides logs and information about newly connected machines, including operating system, MAC address, IP address, and date of login. It also generates logs for the **logging** capability to collect and use for comparison against a baseline in the event of an incident.

The **policy enforcement** capability provides the ability to grant or deny network access based on the machine's posture—essentially, this verifies existence of security software and machine update status before the machine is ever allowed to use the network.

Lastly, the **Vulnerability Management** capability detects and keeps track of vulnerabilities on the newly discovered machine, allowing better understanding of the machine's vulnerabilities before and after it is allowed onto the network.

#### *5.3.8.3 Other Considerations*

Though this use case primarily targets desktops, similar considerations should be taken for enterprises that aim to include employee-owned mobile devices. These devices should be inventoried and scanned for relevant security posture, before being allowed to join the network.

## **6 Future Build Considerations**

The NCCoE is creating an overarching guide to combining the architectures of the various DI projects: Identify and Protect, Detect and Respond, and Recover. These architectures have some commonalities, such as integrity monitoring, as well as some potential integrations and cycles that could not be expressed in just one of the practice guides. The different functions of the Cybersecurity Framework are intended to prepare and inform one another, and the overarching guide addresses those issues.

The NCCoE is also considering additional data security projects that map to the Cybersecurity Framework Core Functions of Identify, Protect, Detect, Respond, and Recover. These projects will focus on data confidentiality—the defense of enterprise systems from attacks that would compromise the secrecy of data.

## Appendix A List of Acronyms

<b>COI</b>	community of interest
<b>DI</b>	data integrity
<b>DSP</b>	Directory Services Protector
<b>ESM</b>	Enterprise Security Manager
<b>IT</b>	Information Technology
<b>ISO/IEC</b>	International Organization for Standardization/International Electrotechnical Commission
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>NIST IR</b>	NIST Interagency Report
<b>RMF</b>	Risk Management Framework
<b>SP</b>	Special Publication
<b>TLC</b>	Tripwire Log Center
<b>TLS</b>	Transport Layer Security
<b>USB</b>	Universal Serial Bus
<b>VM</b>	Virtual Machine
<b>vsftpd</b>	Very Secure File Transfer Protocol Daemon
<b>WORM</b>	Write Once Read Many
<b>WSA</b>	Web Security Appliance

## Appendix B Glossary

<b>Access Control</b>	<p>The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances)</p> <p>SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009</p>
<b>Architecture</b>	<p>A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).</p> <p>SOURCE: FIPS 201-2</p>
<b>Audit</b>	<p>Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures</p> <p>SOURCE: CNSSI 4009-2015</p>
<b>Backdoor</b>	<p>An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.</p> <p>SOURCE: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2</p>
<b>Backup</b>	<p>A copy of files and programs made to facilitate recovery if necessary</p> <p>SOURCE: NIST SP 800-34 Rev. 1</p>
<b>Compromise</b>	<p>Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred</p> <p>SOURCE: NIST SP 800-32</p>

<b>Continuous Monitoring</b>	Maintaining ongoing awareness to support organizational risk decisions  SOURCE: NIST SP 800-137
<b>Cybersecurity</b>	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation  SOURCE: CNSSI 4009-2015 (NSPD-54/HSPD-23)
<b>Data</b>	A subset of information in an electronic format that allows it to be retrieved or transmitted  SOURCE: CNSSI-4009
<b>Data Integrity</b>	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner  SOURCE: CNSSI-4009
<b>Information Security</b>	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability  SOURCE: FIPS 199 (44 U.S.C., Sec. 3542)
<b>Information Security Risk</b>	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems  SOURCE: CNSSI 4009-2015 (NIST SP 800-30 Rev. 1)
<b>Information System</b>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information  SOURCE: FIPS 200 (44 U.S.C., Sec. 3502)
<b>Insider</b>	An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization

SOURCE: NIST SP 800-82 Rev. 2 (RFC 4949)

**Kerberos** An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across a public network.

SOURCE: NIST SP 800-47

**Log** A record of the events occurring within an organization's systems and networks

SOURCE: NIST SP 800-92

**Malware** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system

SOURCE: NIST SP 800-111

**Privacy** Assurance that the confidentiality of, and access to, certain information about an entity is protected

SOURCE: NIST SP 800-130

**Risk** The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring

SOURCE: FIPS 200

**Risk Assessment** The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis

SOURCE: NIST SP 800-63-2

**Risk Management Framework** The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

SOURCE: NIST SP 800-82 Rev. 2 (NIST SP 800-37)

<b>Security Control</b>	<p>A protection measure for a system</p> <p>SOURCE: NIST SP 800-123</p>
<b>Virtual Machine</b>	<p>Software that allows a single host to run one or more guest operating systems</p> <p>SOURCE: NIST SP 800-115</p>
<b>Vulnerability</b>	<p>Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source</p> <p>SOURCE: FIPS 200 (Adapted adapted from CNSSI 4009)</p>



## Appendix C References

- [1] Sedgewick, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, Gaithersburg, Maryland, Apr. 2018, 55 pp. Available: <https://www.nist.gov/cyberframework/framework>.
- [2] L. Kauffman, N. Lesser and B. Abe, *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy*, NISTIR 8050, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2015, 155pp. Available: <https://nccoe.nist.gov/sites/default/files/library/nistir-8050-draft.pdf>.
- [3] G. Stoneburner, *et al.*, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP), 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95 pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-30r1>.
- [4] R. Ross, *et al.*, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST Special Publication (SP) 800-37, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010, 101pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-37r1>.
- [5] R. Ross *et al.*, *Managing Information Security Risk*, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 87pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-39>.
- [6] M. Souppaya *et al.*, *Guide to Enterprise Patch Management Technologies*, NIST Special Publication (SP) 800-40 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 25pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-40r3>.
- [7] R. Ross *et al.*, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013, 461pp. Available: <https://doi.org/10.6028/NIST.SP.800-53r4>.
- [8] U.S. Department of Commerce. Security Requirements for Cryptographic Modules, Federal Information Processing Standards (FIPS) Publication 140-3, Mar. 2019, 65pp. Available: <https://csrc.nist.gov/publications/detail/fips/140/3/final>.
- [9] K. Kent *et al.*, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication (SP) 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2006, 121pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-86>.

- [10] K. Kent and M. Souppaya, *Guide to Computer Security Log Management*, NIST Special Publication (SP) 800-92, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2006, 72pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-92>.
- [11] P. Bowen *et al.*, *Information Security Handbook: A Guide for Managers*, NIST Special Publication (SP) 800-100, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2006, 178pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-100>.
- [12] M. Swanson *et al.*, *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication (SP) 800-34 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2010, 148pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-34r1>.
- [13] Office of Management and Budget (OMB), *Management of Federal Information Resources*, OMB Circular No. A-130, November 2000. Available: <https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>.
- [14] P. Cichonski *et al.*, *Computer Security Incident Handling Guide*, NIST Special Publication (SP) 800-61 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 79pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-61r2>.
- [15] M. Souppaya and K. Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication (SP) 800-83 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 46pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-83r1>.
- [16] C. Johnson *et al.*, *Guide to Cyber Threat Information Sharing*, NIST Special Publication (SP) 800-150, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2016, 42pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-150>.
- [17] M. Bartock *et al.*, *Guide for Cybersecurity Event Recovery*, NIST Special Publication (SP) 800-184, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2016, 52pp. <http://dx.doi.org/10.6028/NIST.SP.800-184>.
- [18] J. Banoczi *et al.*, *Access Rights Management*, NIST Special Publication (SP) 1800-9, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2017. Available: <https://www.nccoe.nist.gov/projects/use-cases/access-rights-management>.
- [19] B. Fisher *et al.*, *Attribute Based Access Control*, NIST Special Publication (SP) 1800-3, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2017. Available: <https://www.nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>.

## Appendix D Functional Evaluation

A functional evaluation of the data integrity (DI) example implementation, as constructed in our laboratory, was conducted to verify that it meets its objective of identifying assets and vulnerabilities within the enterprise. Furthermore, the project aims to protect these assets prior to an attack. The evaluation verified that the example implementation could perform the following functions:

- discover assets on the network
- discover and mitigate vulnerabilities in assets on the network
- protect data from modification prior to an attack
- provide a baseline for daily activity and asset integrity

Section D.1 describes the format and components of the functional test cases. Each functional test case is designed to assess the capability of the example implementation to perform the functions listed above and detailed in Section D.1.

### D.1 Data Integrity Functional Test Plan

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics it was intended to support. The Cybersecurity Framework Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are cited in reference to that Subcategory. The cited sections provide validation points that the example solution is expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

This plan includes the test cases necessary to conduct the functional evaluation of the DI example implementation, which is currently deployed in a lab at the National Cybersecurity Center of Excellence. The implementation tested is described in [Section 4](#).

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 6-1 describes each field in the test case.

**Table 6-1 Test Case Fields**

Test Case Field	Description
Parent Requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.

Test Case Field	Description
Description	Describes the objective of the test case
Associated Cybersecurity Framework Subcategories	Lists the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4 controls addressed by the test case
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected results	The expected results for each variation in the test procedure
Actual results	The observed results
Overall result	The overall result of the test as pass/fail. In some test cases, determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

## D.2 Data Integrity Use Case Requirements

Table 6-2 identifies the DI functional requirements addressed in the test plan and associated test cases.

**Table 6-2 Capability Requirements**

Capability Requirement (CR) ID	Parent Requirement	Sub requirement 1	Test Case
CR 1	The DI example implementation shall identify and protect assets against malware that encrypts files and displays notice demanding payment.		
CR 1.a		Vulnerability in Active Directory server is identified.	Data Integrity IP-1
CR 1.b		User is blocked from visiting malicious site.	Data Integrity IP-1

Capability Requirement (CR) ID	Parent Requirement	Sub requirement 1	Test Case
CR 1.c		Downloads from site are blocked.	Data Integrity IP-1
CR 1.d		Vulnerability is patched.	Data Integrity IP-1
CR 1.e		Ransomware cannot send information to home server.	Data Integrity IP-1
CR 1.f		Backups are taken.	Data Integrity IP-1
CR 1.g		File integrity information is baselined.	Data Integrity IP-1
CR 2	The DI example implementation shall identify and protect assets against malware inserted via Universal Serial Bus (USB) that modifies and deletes user data.		Data Integrity IP-2
CR 2.a		Backups are taken.	Data Integrity IP-2
CR 2.b		File integrity information is baselined.	Data Integrity IP-2
CR 3	The DI example shall identify and protect virtual machines against deletion.		Data Integrity IP-3
CR 3.a		Backups of virtual machines are taken.	Data Integrity IP-3
CR 4	The DI example implementation shall identify and protect assets against malware received via phishing email.		Data Integrity IP-4

Capability Requirement (CR) ID	Parent Requirement	Sub requirement 1	Test Case
CR 4.a		Downloads from the spreadsheet are blocked.	Data Integrity IP-4
CR 4.b		Backups of configurations are taken.	Data Integrity IP-4
CR 4.c		Configuration integrity information is baselined.	Data Integrity IP-4
CR 5	The DI example implementation shall identify and protect the database against changes made through a web server vulnerability in custom code.		Data Integrity IP-5
CR 5.a		Vulnerability is identified.	Data Integrity IP-5
CR 5.b		Vulnerability is resolved.	Data Integrity IP-5
CR 5.c		Backups of database are taken.	Data Integrity IP-5
CR 5.d		Database integrity information is baselined.	Data Integrity IP-5
CR 6	The DI example implementation shall identify and protect assets against targeted modification by malicious insiders with elevated privileges.		Data Integrity IP-6
CR 6.a		Backups are taken.	Data Integrity IP-6
CR 6.b		File integrity information is baselined.	Data Integrity IP-6

Capability Requirement (CR) ID	Parent Requirement	Sub requirement 1	Test Case
CR 6.c		Backups are encrypted.	Data Integrity IP-6
CR 6.d		Backups are stored securely.	Data Integrity IP-6
CR 7	The DI example implementation shall identify and protect assets against an intrusion via compromised update server.		Data Integrity IP-7
CR 7.a		Downloads from site are temporarily blocked.	Data Integrity IP-7
CR 7.b		Backups are taken.	Data Integrity IP-7
CR 7.c		Program integrity information is baselined.	Data Integrity IP-7
CR 7.d		File integrity information is baselined.	Data Integrity IP-7
CR 8	The DI example implementation shall identify new and unmaintained assets on the network.		Data Integrity IP-8
CR 8.a		Machines that are new to the network are identified.	Data Integrity IP-8
CR 8.b		Machines that are not up-to-date are identified.	Data Integrity IP-8

## D.3 Test Case: Data Integrity IP-1

Table 6-3 Test Case ID: Data Integrity IP-1

Parent requirement	(CR 1) The DI example implementation shall identify and protect assets against malware that encrypts files and displays notice demanding payment.
Testable requirement	(CR 1.a) Vulnerability identification, (CR 1.b, 1.c, 1.e) Denylisting, (CR 1.d) Maintenance, (CR 1.f) Backups, (CR 1.g) Integrity Baselineing
Description	Show that the DI solution can identify and resolve vulnerabilities and protect against ransomware.
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.RA-1, ID.RA-2, ID.RA-6, DE.CM-8, PR.IP-12, RS.MI-3, PR.IP-4, PR.DS-1, PR.DS-6, PR.PT-1, PR.MA-2
Preconditions	User navigates to a malicious website and clicks on an ad for a virus cleaner. The virus cleaner is actually ransomware, which propagates across the domain and encrypts user files.
Procedure	<p>The <b>denylisting</b> capability is used to prevent access to and downloads from known malicious sites.</p> <p>The <b>inventory</b> capability is used to identify organizational assets and devices.</p> <p>The <b>network protection</b> capability is used to prevent the propagation of ransomware across the enterprise.</p> <p>The <b>vulnerability management</b> capability is used to identify vulnerabilities that allow malware to propagate.</p> <p>The <b>integrity monitoring</b> and <b>logging</b> collect integrity information and baseline the file system.</p> <p>The <b>backups</b> capability is used to take backups of the file system.</p>
Expected Results (pass)	<p>The vulnerability that allows the ransomware to propagate is identified (CR 1.a).</p> <p>The user cannot access the site when it is blocked (CR 1.b).</p>



	<p>The user cannot download the ransomware from the site when it is blocked (CR 1.c).</p> <p>The build can identify (and possibly execute) a fix for the vulnerability. When the fix is made, the ransomware is unable to propagate (CR 1.d).</p> <p>The ransomware is unable to communicate with its home server when the site is blocked (CR 1.e).</p> <p>The build can take backups of file systems (CR 1.f).</p> <p>The build can take and log integrity baselines of file systems (CR 1.g).</p>
Actual Results	<p><b>Cisco WSA (denylisting)</b> stops the user from accessing the site when it is blocked.</p> <p><b>Cisco ISE (inventory)</b> is used to identify devices on the network.</p> <p><b>Symantec DLP (inventory)</b> is used to identify organizational data assets on monitored machines.</p> <p><b>CryptoniteNXT (network protection)</b> prevents propagation of ransomware through an allowlist of approved communications in the enterprise.</p> <p><b>Tripwire IP360 (vulnerability management)</b> detects vulnerabilities in Active Directory that allow ransomware to propagate.</p> <p><b>Tripwire Enterprise (integrity monitoring)</b> and <b>ArcSight ESM (logging)</b> baseline critical data assets across the enterprise.</p> <p><b>Duplicati</b> and <b>FileZilla (backups)</b> create backups of organizational data as a contingency, should ransomware be able to affect any systems.</p>
Overall Result	Pass. All requirements for this use case are met.

## D.4 Test Case: Data Integrity IP-2

Table 6-4 Test Case ID: Data Integrity IP-2

Parent requirement	(CR 2) The DI example implementation shall identify and protect assets against malware inserted via USB that modifies and deletes user data.
--------------------	--

Testable requirement	(CR 2.a) Backups, (CR 2.b) Integrity Baselineing
Description	Show that the DI solution can preemptively protect against destructive malware.
Associated Cybersecurity Framework Subcategories	PR.IP-4, PR.DS-1, PR.DS-6, PR.PT-1
Preconditions	A user inserts an unidentified USB drive into their computer. They click on a file on the drive, which immediately destroys any files on their machine.
Procedure	<p><b>Backups</b> schedules and creates backups of the user's documents.</p> <p>The <b>integrity monitoring</b> capability is used to take integrity baselines of the file system.</p> <p><b>Logging</b> collects logs and baselines system activity.</p>
Expected Results (pass)	<p>The build can take backups of file systems (CR 2.a).</p> <p>The build can take and log integrity baselines of file systems (CR 2.b).</p>
Actual Results	<p><b>Duplicati</b> and <b>FileZilla (backups)</b> are used to take and store backups of the user's documents.</p> <p><b>Tripwire Enterprise (integrity monitoring)</b> is used to take an integrity baseline of the user's file system prior to the malicious USB drive being inserted into the computer.</p> <p><b>ArcSight ESM (logging)</b> takes a baseline of system activity prior to the USB drive being inserted into the computer.</p>
Overall Result	Pass. All requirements for this use case are met.

## D.5 Test Case: Data Integrity IP-3

Table 6-5 Test Case ID: Data Integrity IP-3

Parent requirement	(CR 3) The DI example implementation shall identify and protect virtual machines against deletion.
Testable requirement	(CR 3.a) Backups
Description	Show that the DI solution can preemptively protect against data integrity events that involve virtual machines (VMs).

Associated Cybersecurity Framework Subcategories	PR.IP-4, PR.DS-1
Preconditions	A routine maintenance script contains an error that accidentally deletes a VM.
Procedure	The <b>backups</b> capability is used to schedule and create backups of a VM.
Expected Results (pass)	The build can take backups of VMs (CR 3.a).
Actual Results	<b>Duplicati</b> and <b>FileZilla (backups)</b> take and store backups of VMs.
Overall Result	Pass. All requirements for this use case are met.

## D.6 Test Case: Data Integrity IP-4

Table 6-6 Test Case ID: Data Integrity IP-4

Parent requirement	(CR 4) The DI example implementation shall identify and protect against malware received via phishing email.
Testable requirement	(CR 4.a, CR 4.b) Denylisting, (CR 4.c) Backups, (CR 4.d) Integrity Baselineing
Description	Show that the DI solution can identify phishing emails and protect against configuration changes made by malicious attachments.
Associated Cybersecurity Framework Subcategories	ID.AM-2, ID.AM-3, ID. RA-1, ID.RA-2, ID.RA-5, DE.CM-8, PR.IP-4, PR.DS-1, PR.PT-1
Preconditions	The user receives a phishing email with a malicious attached spreadsheet. The spreadsheet is downloaded and opened, causing account changes in Active Directory.
Procedure	<p>The <b>integrity monitoring</b> capability is used to baseline Active Directory activity.</p> <p>This information is forwarded to the <b>logging</b> capability, along with other available Active Directory information.</p> <p>The <b>backups</b> capability is used to take backups of the Active Directory configuration.</p>

	The malicious web server is added to the <b>denylisting</b> capability to prevent downloads.
Expected Results (pass)	<p>The spreadsheet cannot download files (CR 4.a).</p> <p>The build can take backups of configurations (CR 4.c).</p> <p>The build can take and log integrity baselines of configurations (CR 4.d).</p>
Actual Results	<p><b>Semperis DSP (integrity monitoring)</b> successfully baselines Active Directory activity.</p> <p><b>ArcSight ESM (logging)</b> successfully logs activity from Active Directory, including log-ons and changes.</p> <p>When the external web server is added to the denylist, <b>Cisco WSA (denylisting)</b> prevents the Excel sheet from downloading malicious files.</p> <p><b>Semperis ADFR (backups)</b> is used to successfully take backups of the Active Directory configuration.</p>
Overall Result	Pass. All requirements for this use case are met.

## D.7 Test Case: Data Integrity IP-5

Table 6-7 Test Case ID: Data Integrity IP-5

Parent requirement	(CR 5) The DI example implementation shall identify and protect the database against changes made through a web server vulnerability in custom code.
Testable requirement	(CR 5.c) Backups, (CR 5.d) Integrity Baselineing
Description	Show that the DI solution can protect the database against a vulnerability in the custom code of a web server.
Associated Cybersecurity Framework Subcategories	PR.IP-4, PR.DS-1, PR.PT-1, PR.DS-6
Preconditions	A vulnerability in the source code of an intranet webpage is discovered by a malicious insider. The insider exploits this vulnerability to delete significant portions of the database.
Procedure	The <b>backups</b> capability is used to take backups of the database.

	The <b>integrity monitoring</b> and <b>logging</b> capabilities take baselines of the database, for comparison post-modification.
Expected Results (pass)	The build can take backups of the database (CR 5.c).  The build can take and log integrity baselines of the database (CR 5.d).
Actual Results	<b>Duplicati</b> and <b>FileZilla (backups)</b> successfully backs up the database. <b>Tripwire Enterprise (integrity monitoring)</b> successfully detects changes in the database. <b>ArcSight ESM (logging)</b> successfully logs changes to the database.
Overall Result	Pass. All requirements for this use case are met.

## D.8 Test Case: Data Integrity IP-6

Table 6-8 Test Case ID: Data Integrity IP-6

Parent requirement	(CR 6) The DI example implementation shall identify and protect assets against targeted modification by malicious insiders with elevated privileges.
Testable requirement	(CR 6.a) Backups, (CR 6.b) Integrity Baselineing, (CR 6.c) Encrypted Backups, (CR 6.d) Secure Storage
Description	Show that the DI solution can protect assets and backups against targeted modification by malicious insiders.
Associated Cybersecurity Framework Subcategories	PR.IP-4, PR.DS-1, PR.PT-1, PR.DS-6
Preconditions	A malicious insider attempts to modify targeted information in both the enterprise systems and the backup systems, using elevated credentials obtained extraneously.
Procedure	The <b>inventory</b> capability is used to identify data assets.  The <b>backups</b> capability provides encrypted backups.  <b>Secure storage</b> prevents modification or deletion of backups.  <b>Integrity monitoring</b> and <b>logging</b> collect integrity information and baseline the file system.

Expected Results (pass)	<p>The build can take backups of the file system (CR 6.a).</p> <p>The build can take and log integrity baselines of the file system (CR 6.b).</p> <p>Backups are encrypted (CR 6.c).</p> <p>Backups are stored securely and cannot be modified or deleted (CR 6.d).</p>
Actual Results	<p><b>Symantec DLP (inventory)</b> identifies critical data assets across the enterprise.</p> <p><b>Duplicati</b> and <b>FileZilla (backups)</b> provide encrypted backups of the file system.</p> <p><b>GreenTec WORMdisks (secure storage)</b> provide write-protection for backups, preventing them from being modified or deleted.</p> <p><b>Tripwire Enterprise (integrity monitoring)</b> and <b>ArcSight ESM (logging)</b> baseline critical data assets across the enterprise.</p>
Overall Result	Pass. All requirements of this use case are met.

## D.9 Test Case: Data Integrity IP-7

Table 6-9 Test Case ID: Data Integrity IP-7

Parent requirement	(CR 7) The DI example implementation shall identify and protect assets against an intrusion via compromised update server.
Testable requirement	(CR 7.a) Denylisting, (CR 7.b) Backups, (CR 7.c, 7.d) Integrity Baselining
Description	Show that the DI solution can protect against compromised update server as well as intrusion made possible by vulnerable programs.
Associated Cybersecurity Framework Subcategories	ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8, PR.IP-12, RS.MI-3, PR.IP-4, PR.DS-1, PR.PT-1, PR.DS-6, PR.MA-2
Preconditions	An external update server has been compromised, and a user workstation attempts to update from this server.
Procedure	<p><b>Integrity monitoring</b> capability is used to take baselines of the integrity of both the programs and the file systems.</p> <p>The <b>backups</b> capability is used to back up the file system.</p>

	The <b>denylisting</b> capability is used to prevent communication between the update server and the machine.
Expected Results (pass)	<p>Machines cannot update from this site while it is denylisted (CR 7.a).</p> <p>The build can take backups of file systems (CR 7.b).</p> <p>The build can take integrity baselines of programs (CR 7.c).</p> <p>The build can take integrity baselines of file systems (CR 7.d).</p>
Actual Results	<p><b>Tripwire Enterprise (integrity monitoring)</b> successfully takes an integrity baseline of both programs and files.</p> <p><b>Duplicati and FileZilla (backups)</b> successfully takes backups of the file system.</p> <p><b>Cisco WSA (denylisting)</b> successfully prevents communication between the update server and workstations.</p>
Overall Result	Pass. All requirements for this use case are met.

## D.10 Test Case: Data Integrity IP-8

Table 6-10 Test Case ID: Data Integrity IP-8

Parent requirement	(CR 8) The DI example implementation shall identify new and unmaintained assets on the network.
Testable requirement	(CR 8.a) Asset Identification, (CR 8.b) Vulnerability Identification
Description	Show that the DI solution can identify machines new to the network, as well as unpatched machines.
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.RA-1, ID.RA-2, ID.RA-5, DE.CM-8
Preconditions	A new machine with several critical patches missing is connected to the network for the first time.
Procedure	The <b>inventory</b> capability is used to identify various aspects about the machine.

	<p>The <b>policy enforcement</b> identifies the existence of security solutions on the machine and grants/denies access to the network, based on their presence.</p> <p>The <b>vulnerability management</b> capability is used to scan for vulnerabilities on the new machine.</p>
Expected Results (pass)	<p>New machine is identified on the network (CR 8.a).</p> <p>New machine is identified as unmaintained, and required fixes are identified (CR 8.b).</p>
Actual Results	<p><b>Cisco ISE (inventory)</b> successfully logs information about new connections, including the user, date, device, and network information.</p> <p><b>Cisco ISE (policy enforcement)</b> successfully prevents the new machine without 50 security software from connecting to the network.</p> <p><b>Tripwire IP360 (vulnerability management)</b> successfully identifies vulnerabilities on the new machine.</p>
Overall Result	Pass. All requirements for this use case are met.



## NIST SPECIAL PUBLICATION 1800-25C

---

# Data Integrity:

## Identifying and Protecting Assets Against Ransomware and Other Destructive Events

---

### Volume C: How-To Guides

#### Jennifer Cawthra

National Cybersecurity Center of Excellence  
NIST

#### Michael Ekstrom

#### Lauren Lusty

#### Julian Sexton

#### John Sweetnam

The MITRE Corporation  
McLean, Virginia

December 2020

FINAL

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

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



## DISCLAIMER

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

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

## FEEDBACK

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

## ABSTRACT

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

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

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

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

Name	Organization
Denise Schiavone	The MITRE Corporation
Anne Townsend	The MITRE Corporation

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Data Loss Prevention v15.1
Cisco Systems	Cisco ISE v2.4, Cisco Web Security Appliance v10.1
GreenTec USA	GreenTec WORMdisk v151228
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7, Tripwire IP360 v9.0.1
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Cryptonite	CryptoniteNXT v2.9.1
Semperis	Semperis Active Directory Forest Recovery v2.5, Semperis Directory Services Protector v2.7

# Contents

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

2.6.2	Obtain Status Information About GreenTec WORMdisks .....	103
2.6.3	Map GreenTec WORMdisks to Drive Letters .....	104
2.6.4	Activate Write Protection in GreenTec WORMdisks .....	105
<b>2.7</b>	<b>CryptoniteNXT .....</b>	<b>109</b>
2.7.1	Configure Cryptonite NXT .....	109
2.7.1.1	Verify a New Device .....	109
2.7.1.2	Create a New User .....	112
2.7.1.3	Create a New Policy .....	115
2.7.2	Integrate CryptoniteNXT with Active Directory .....	122
2.7.2.1	Generate a Keytab File .....	122
2.7.2.2	Import Keytab File to ACC .....	129
<b>2.8</b>	<b>Backups .....</b>	<b>136</b>
2.8.1	FileZilla FTPS Server Setup .....	136
2.8.2	FileZilla Configuration .....	139
2.8.3	Add a User to FileZilla .....	144
2.8.4	Duplicati Client Installation (Windows) .....	146
2.8.5	Duplicati Client Installation (Ubuntu) .....	149
2.8.6	Configure Duplicati .....	150
<b>2.9</b>	<b>Semperis Active Directory Forest Recovery .....</b>	<b>155</b>
2.9.1	Install Semperis ADFR .....	155
2.9.2	Create a Backup Schedule for the Domain Controller .....	164
2.9.3	Recover the Active Directory Forest from a Backup .....	167
<b>2.10</b>	<b>Semperis Directory Services Protector .....</b>	<b>170</b>
2.10.1	Configure Active Directory for Semperis DSP .....	170
2.10.2	Install Semperis DSP .....	183
<b>2.11</b>	<b>Micro Focus ArcSight Enterprise Security Manager .....</b>	<b>195</b>
2.11.1	Install the ArcSight Console .....	196
2.11.2	Install Individual ArcSight Windows Connectors .....	209



2.11.3	Install Individual ArcSight Ubuntu Connectors .....	227
2.11.4	Install a Connector Server for ESM on Windows 2012 R2 .....	240
2.11.5	Install Preconfigured Filters for ArcSight .....	253
2.11.5.1	Install Activate Base.....	253
2.11.5.2	Install Packages.....	255
2.11.6	Apply Filters to a Channel .....	256
<b>2.12</b>	<b>Tripwire Enterprise .....</b>	<b>257</b>
2.12.1	Install Tripwire Enterprise.....	257
2.12.2	Install the Axon Bridge .....	270
2.12.3	Install the Axon Agent (Windows) .....	270
2.12.4	Install the Axon Agent (Linux) .....	271
2.12.5	Configure Tripwire Enterprise.....	272
2.12.5.1	Terminology .....	272
2.12.5.2	Tags .....	273
2.12.5.3	Rules .....	275
2.12.5.4	Tasks .....	279
<b>2.13</b>	<b>Tripwire Log Center .....</b>	<b>283</b>
2.13.1	Install Tripwire Log Center Manager .....	283
2.13.2	Configure Tripwire Log Center Manager .....	283
2.13.3	Install Tripwire Log Center Console .....	289
<b>2.14</b>	<b>Cisco Web Security Appliance .....</b>	<b>289</b>
2.14.1	Network Configuration .....	289
2.14.2	System Setup .....	290
2.14.3	Using WSA to Proxy Traffic .....	298

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

2.19	Integration: Tripwire Log Center and Tripwire IP360 .....	384
2.19.1	Configure IP360 and Log Center .....	384
2.19.2	Collect Tripwire IP360 Operational Logs.....	387
2.19.3	Configure Tripwire IP360 Scan Results Forwarding .....	399
2.20	Integration: Tripwire Enterprise and Backups .....	412
2.20.1	Export Configuration from Tripwire Enterprise .....	413
2.20.2	Back Up the Tripwire Enterprise Configuration .....	413
2.21	Integration: Cisco ISE and CryptoniteNXT .....	413
2.21.1	Requirements for Integrating Cisco ISE and CryptoniteNXT .....	413
2.21.2	Configuring CryptoniteNXT for RADIUS .....	414
2.22	Integration: Backups and GreenTec .....	415
2.22.1	Locate Backups with FileZilla and Duplicati .....	415
2.22.2	Back Up to a GreenTec Disk .....	417
2.22.3	Configure Network-Accessible GreenTec Disk.....	418
2.22.4	Secure Storage for Semperis ADFR .....	420
2.23	Integration: Micro Focus ArcSight and FileZilla.....	421
2.23.1	Enable Logs in FileZilla .....	421
2.23.2	Install Micro Focus ArcSight.....	423
2.24	Integration: Micro Focus ArcSight and Tripwire .....	438
2.24.1	Install Micro Focus ArcSight.....	438
2.25	Integration: Micro Focus ArcSight and Cisco WSA.....	451
2.25.1	Configure Cisco WSA to Forward Logs.....	451
2.26	Integration: Micro Focus ArcSight and Cisco ISE.....	454
2.26.1	Configure Cisco ISE to Forward Logs.....	454
2.26.2	Select Logs for Forwarding.....	457
2.27	Integration: Micro Focus ArcSight and Symantec DLP .....	458
2.27.1	Install Micro Focus ArcSight.....	458
2.27.2	Configure Symantec DLP to Forward Logs.....	468
2.28	Integration: Micro Focus ArcSight and CryptoniteNXT .....	472

2.28.1	Configure CryptoniteNXT to Forward Logs to ArcSight .....	472
2.29	Integration: Micro Focus ArcSight and Semperis DSP .....	473
2.29.1	Configure Semperis DSP to Forward Logs.....	473
2.30	Integrations: CryptoniteNXT.....	474
2.30.1	Active Directory and DNS.....	475
2.30.2	Microsoft Exchange .....	476
2.30.3	FileZilla .....	477
2.30.4	GreenTec.....	478
2.30.5	Tripwire Enterprise .....	478
2.30.6	ArcSight ESM .....	479
2.30.7	Cisco ISE .....	479
2.30.8	Semperis DSP .....	480
2.30.9	Symantec DLP .....	481
2.30.10	Cisco WSA .....	481
2.30.11	Tripwire IP360 .....	482
2.30.11.1	Tripwire Log Center, Tripwire IP360, Tripwire Enterprise, and ArcSight ESM .....	483
2.30.12	FileZilla and ArcSight .....	485
2.30.13	Cisco ISE and ArcSight .....	485
2.30.14	Cisco WSA and ArcSight .....	486
2.30.15	Semperis DSP and ArcSight.....	486
2.30.16	Symantec DLP and ArcSight .....	487

## Appendix A List of Acronyms ..... 488

# 1 Introduction

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

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

## 1.1 How to Use this Guide

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

This guide contains three volumes:

- NIST SP 1800-25A: *Executive Summary*
- NIST SP 1800-25B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-25C: *How-To Guides* – instructions for building the example solution (**you are here**)

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

**Business decision makers, including chief security and technology officers**, will be interested in the *Executive Summary* (NIST SP 1800-25A), which describes the following topics:

- challenges that enterprises face in identifying assets and protecting them from data integrity events
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-25B, which describes what we did and why. The following sections will be of particular interest:

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

You might share the *Executive Summary*, NIST SP 1800-25A, with your leadership team members to help them understand the importance of adopting standards-based data integrity solutions.

**IT professionals** who want to implement an approach like this will find the whole practice guide useful. You can use this How-To portion of the guide, NIST SP 1800-25C, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a data integrity identify-and-protect solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.5 of Volume B, *Technologies*, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

## 1.2 Build Overview

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

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

## Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and pathnames; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on-screen computer output, sample code examples, and status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b><code>service sshd start</code></b>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at <a href="https://nccoe.nist.gov">https://nccoe.nist.gov</a> .

## 2 Product Installation Guides

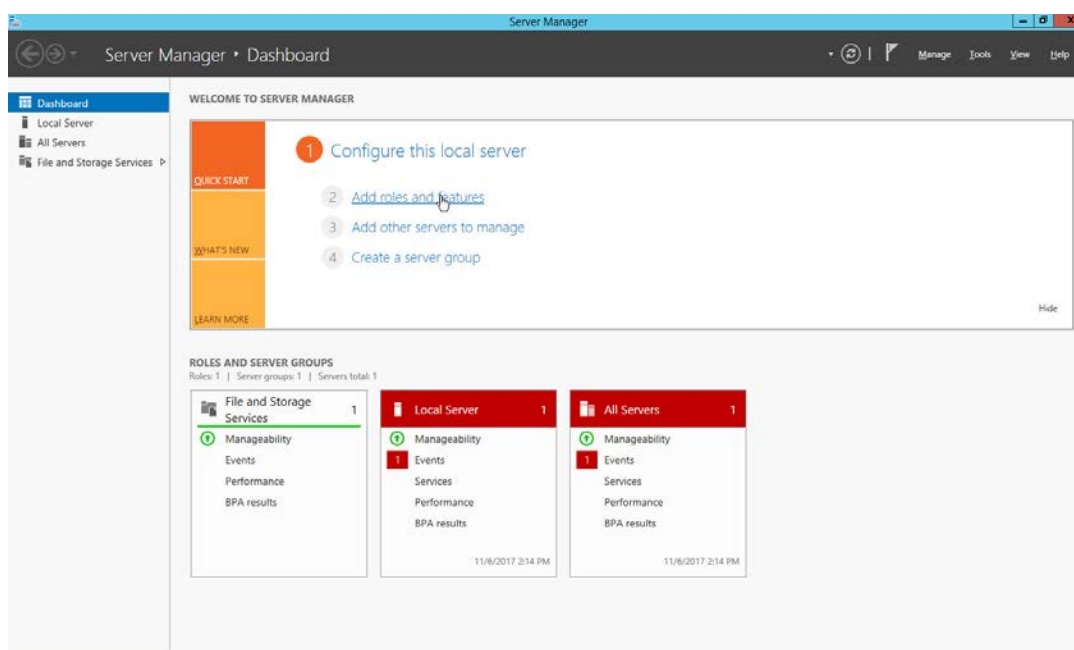
This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

### 2.1 Active Directory and Domain Name System (DNS Server)

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

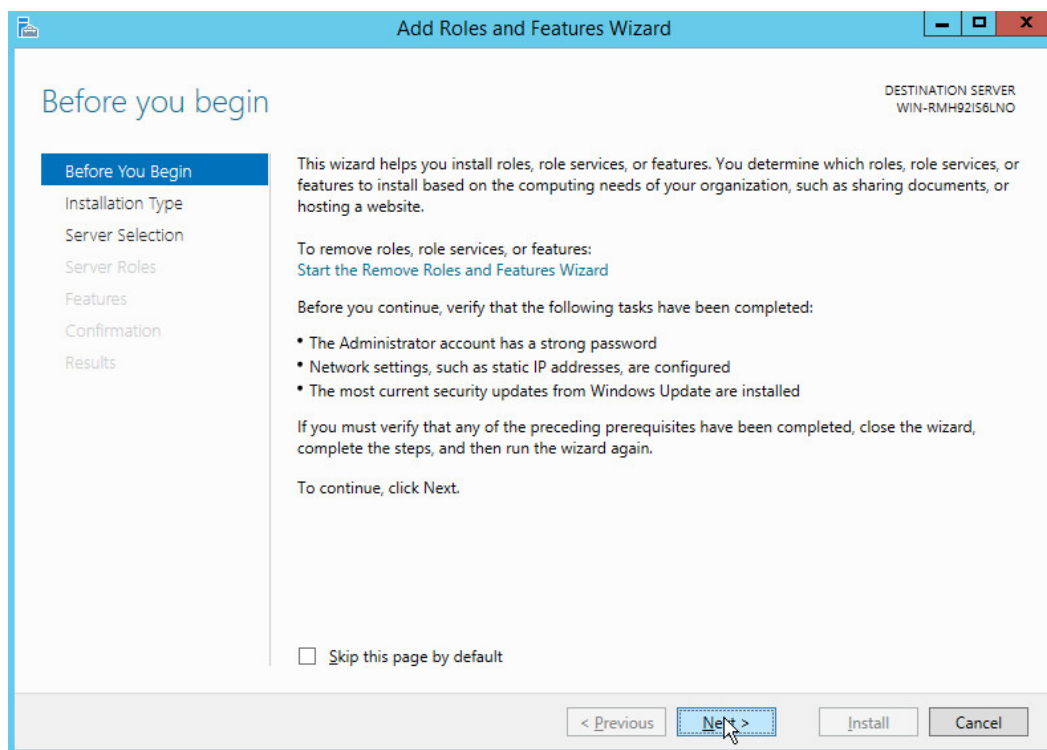
#### 2.1.1 Installing Features

1. Open **Server Manager**.

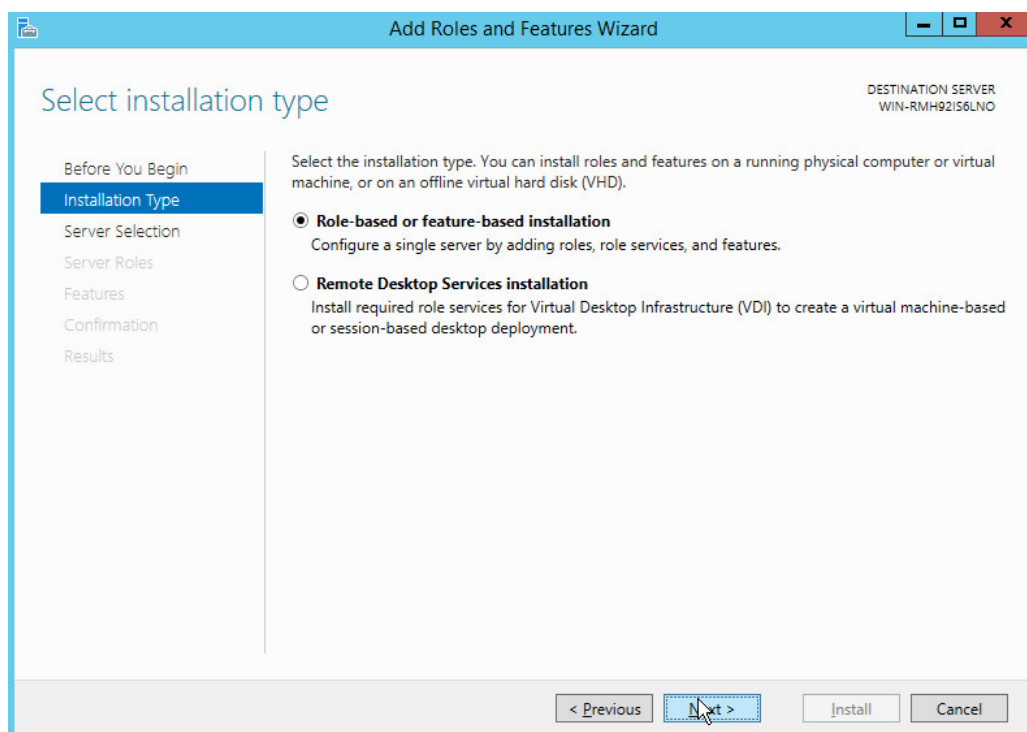


2. Click the link **Add roles and features**.

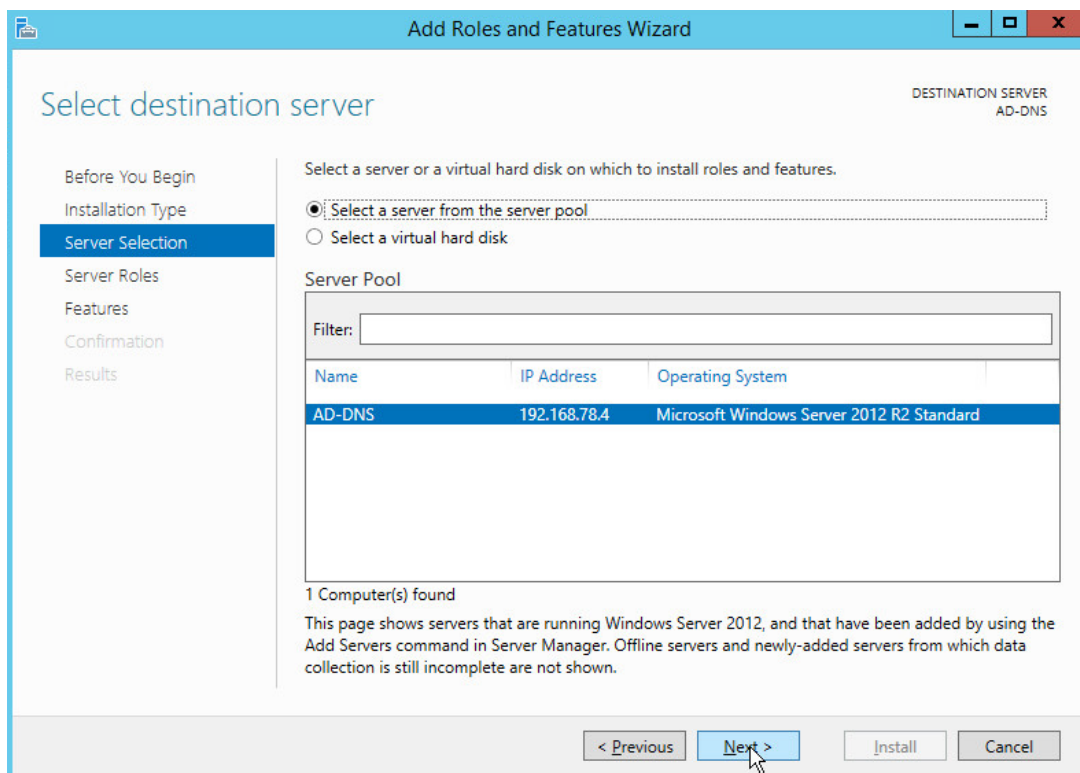




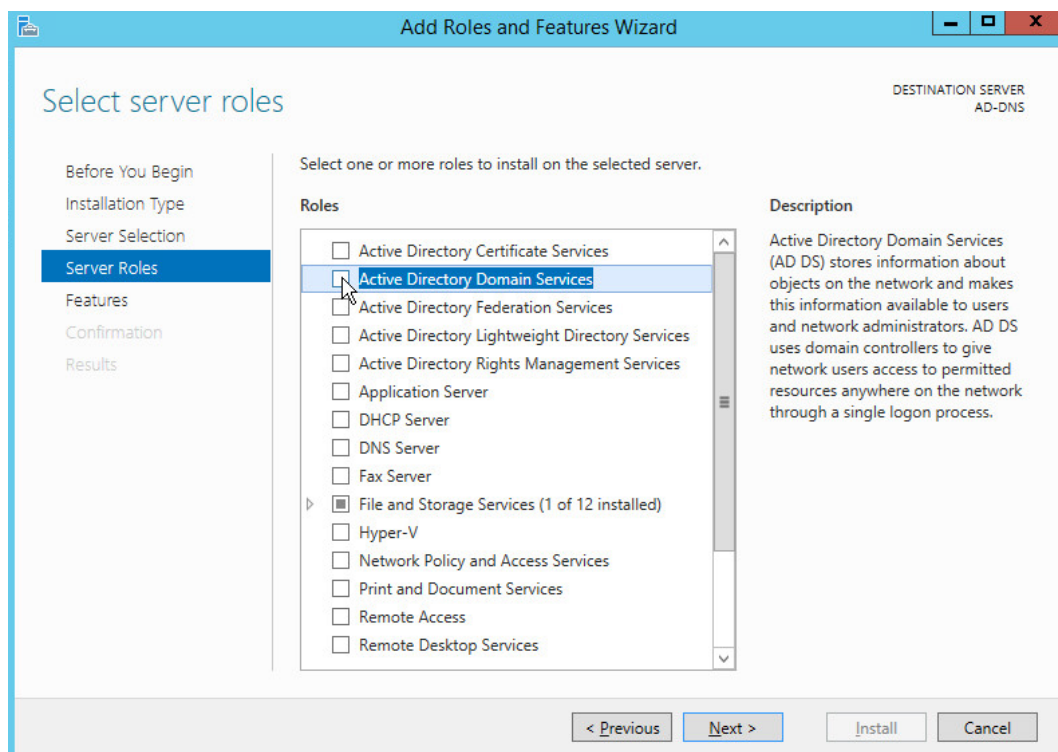
3. Click **Next**.
4. Select **Role-based or feature-based installation**.



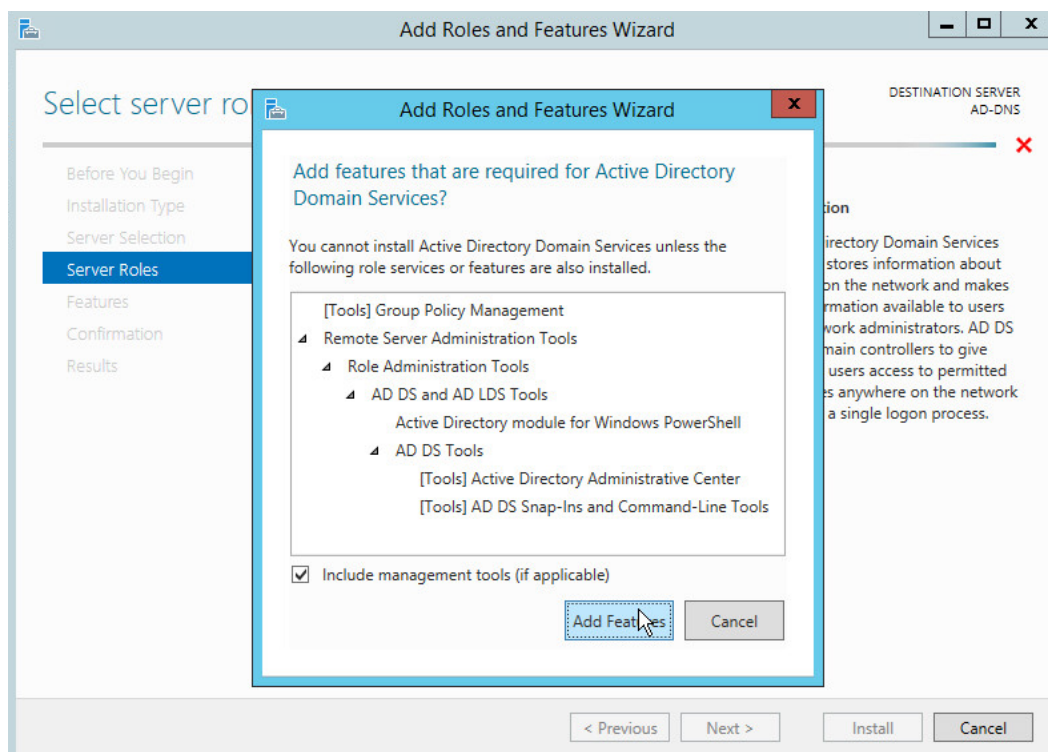
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Select the intended Active Directory server.



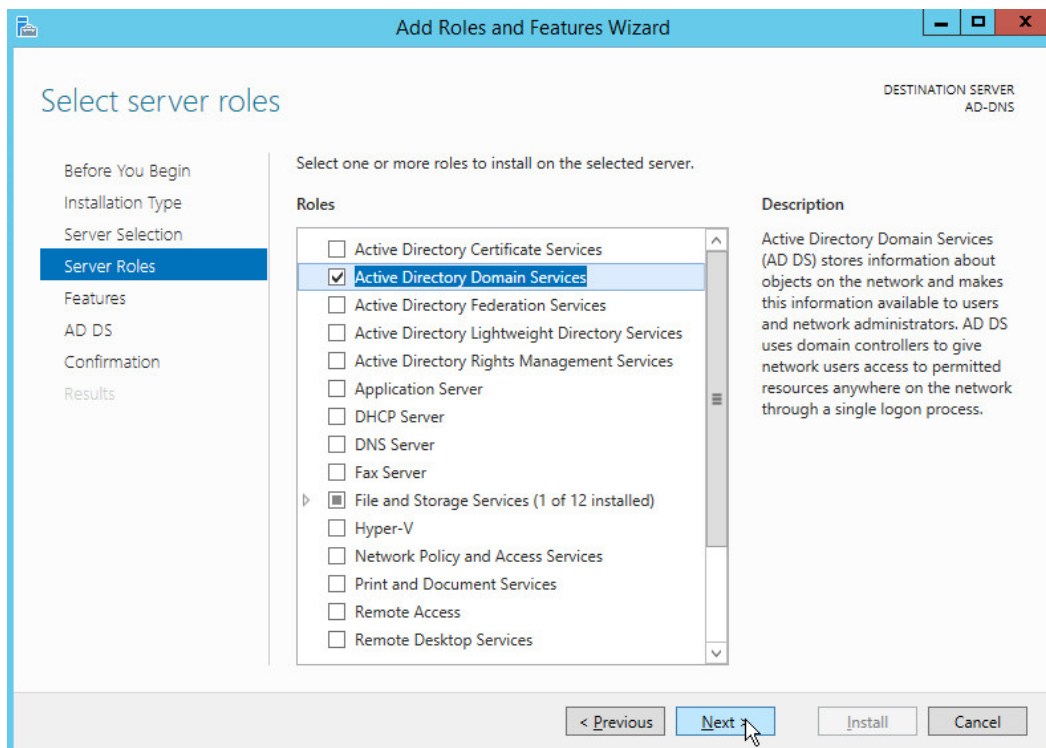
8. Click **Next**.



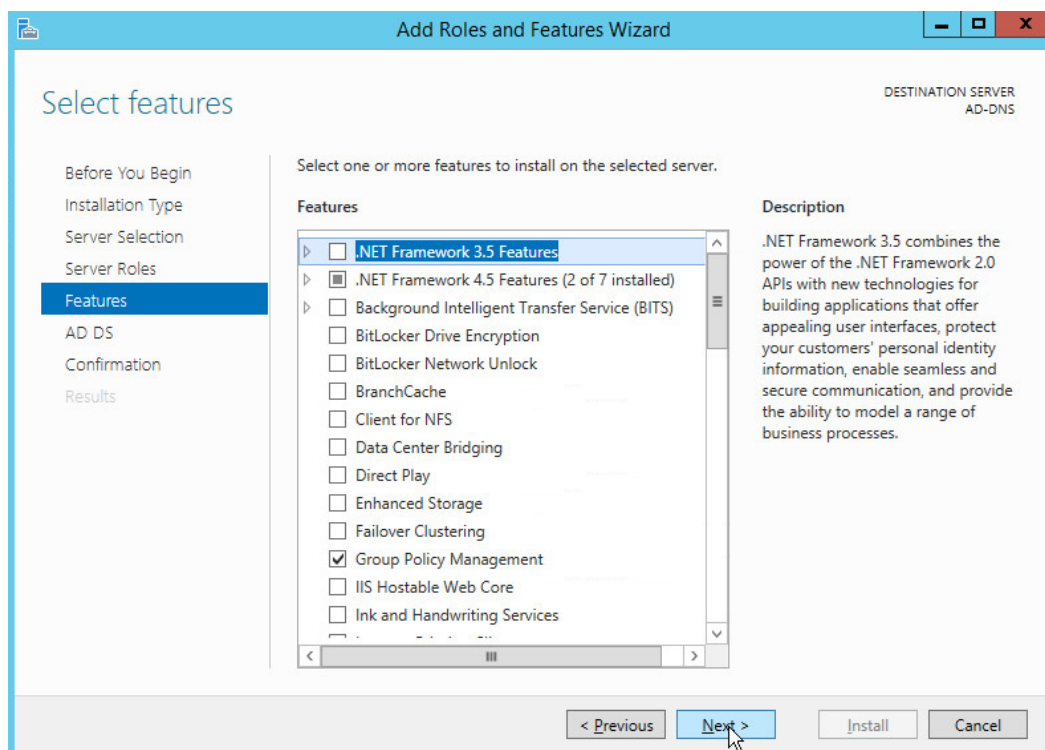
9. Check the box next to **Active Directory Domain Services**.



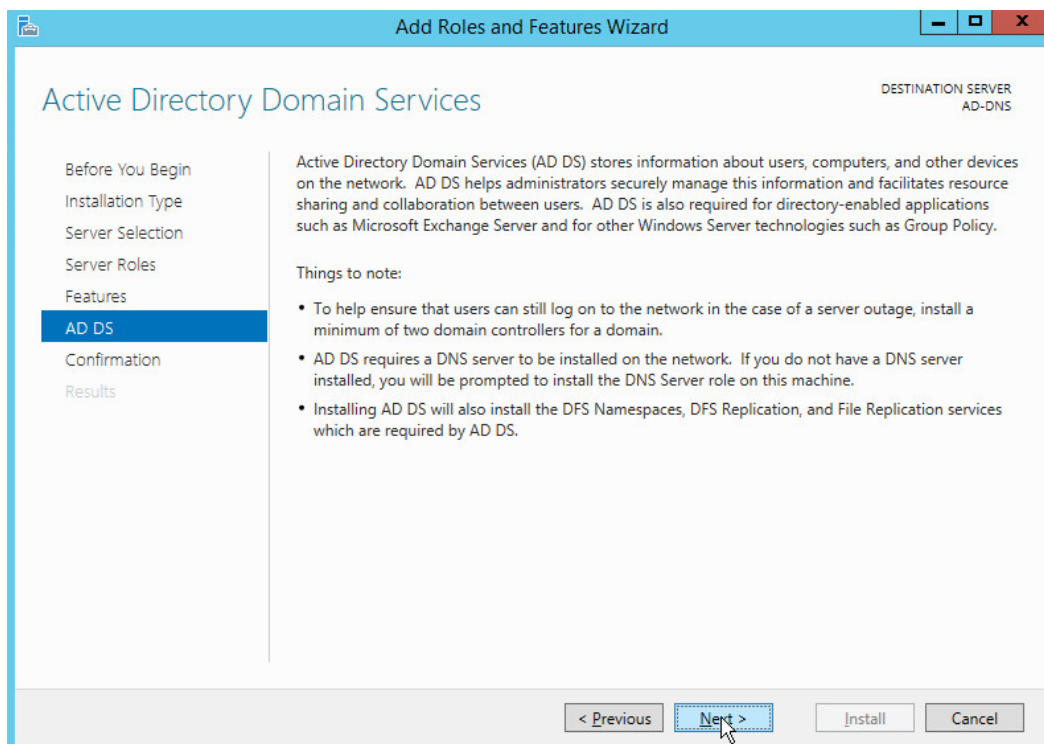
10. Click **Add Features**.



11. Click **Next**.

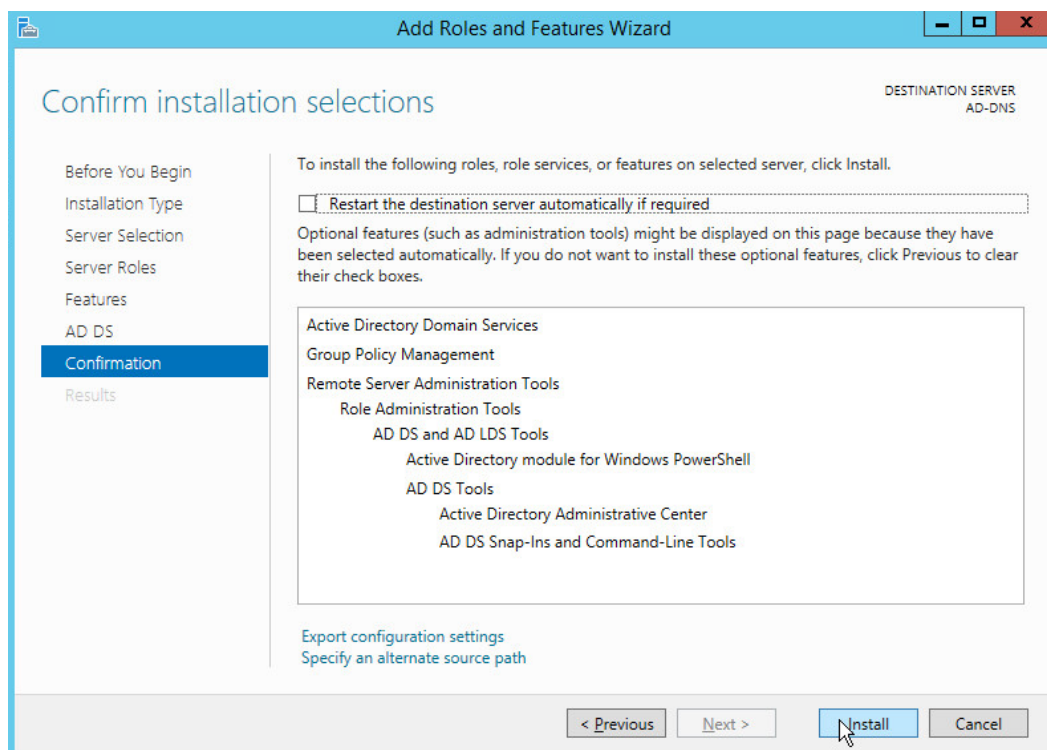


12. Click **Next**.



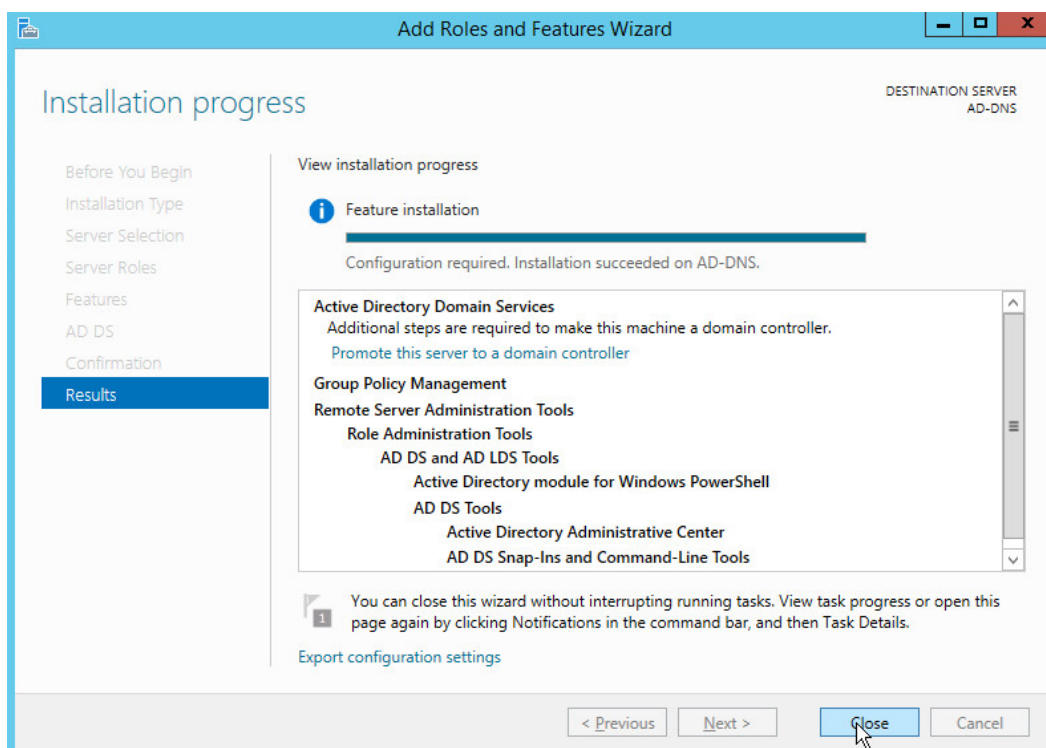
13. Click **Next**.



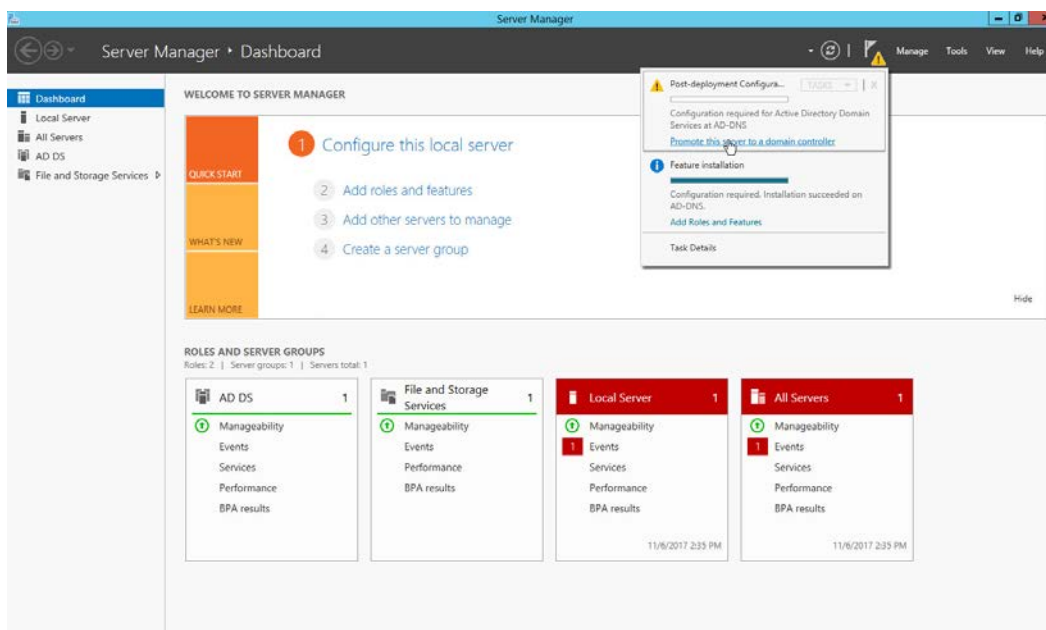


14. Click **Install**.

15. Wait for the installation to complete.



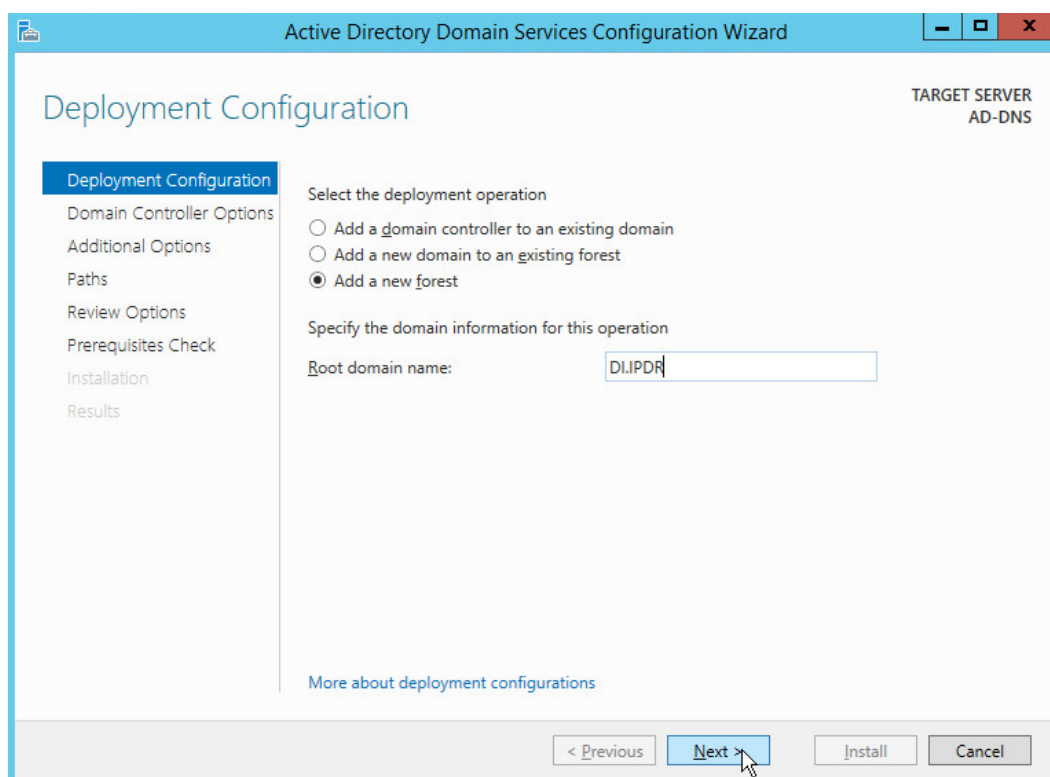
16. Click **Close**.



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

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

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



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 'Deployment Configuration'. On the left is a navigation pane with the following items: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio button options: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below these options is a section titled 'Specify the domain information for this operation' with a label 'Root domain name:' and a text input field containing 'DIJIPDR'. At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a mouse cursor), 'Install', and 'Cancel'. A link 'More about deployment configurations' is located at the bottom left of the main content area. In the top right corner, the text 'TARGET SERVER AD-DNS' is displayed.

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**.

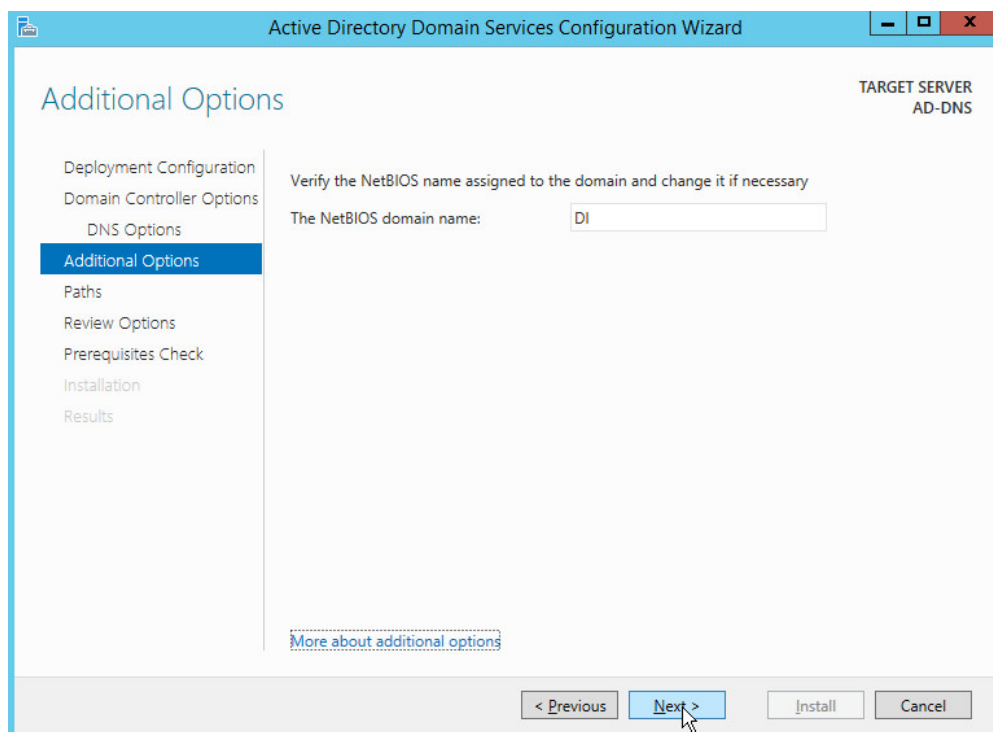
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Domain Controller Options'. On the right, it says 'TARGET SERVER AD-DNS'. A left-hand navigation pane lists the following steps: Deployment Configuration, Domain Controller Options (highlighted), 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 is the section '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 is the section 'Type the Directory Services Restore Mode (DSRM) password' with two password fields labeled 'Password:' and 'Confirm password:', both containing masked characters. At the bottom right of the main area is a link: 'More about domain controller options'. The bottom of the window features four buttons: '< Previous', 'Next >' (with a mouse cursor hovering over it), 'Install', and 'Cancel'.

24. Click **Next**.

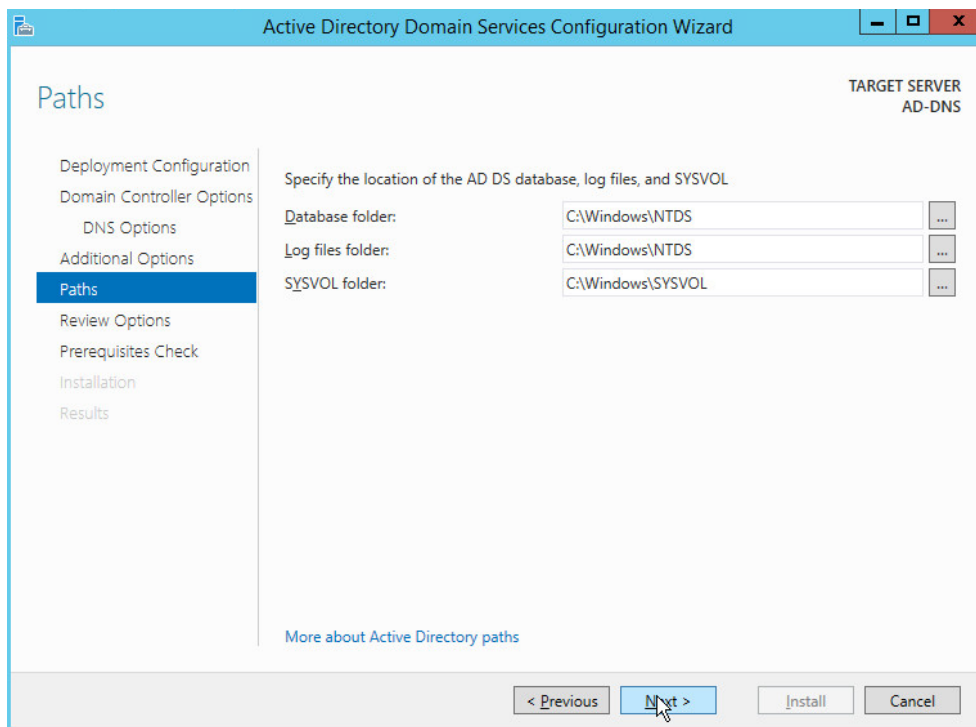
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'DNS Options' step. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'DNS Options'. On the right, it says 'TARGET SERVER AD-DNS'. The left-hand navigation pane lists the following steps: Deployment Configuration, Domain Controller Options, DNS Options (highlighted), Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. 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 right of the main area is a link: 'More about DNS delegation'. The bottom of the window features four buttons: '< Previous', 'Next >' (with a mouse cursor hovering over it), 'Install', and 'Cancel'.

25. Click **Next**.

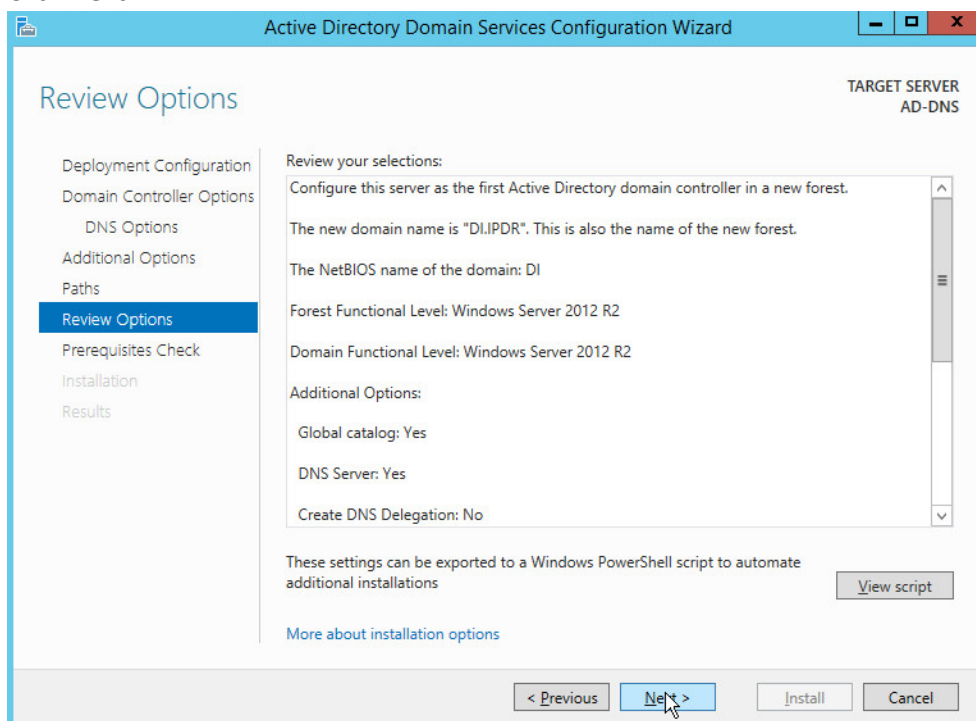
26. Verify the domain name.



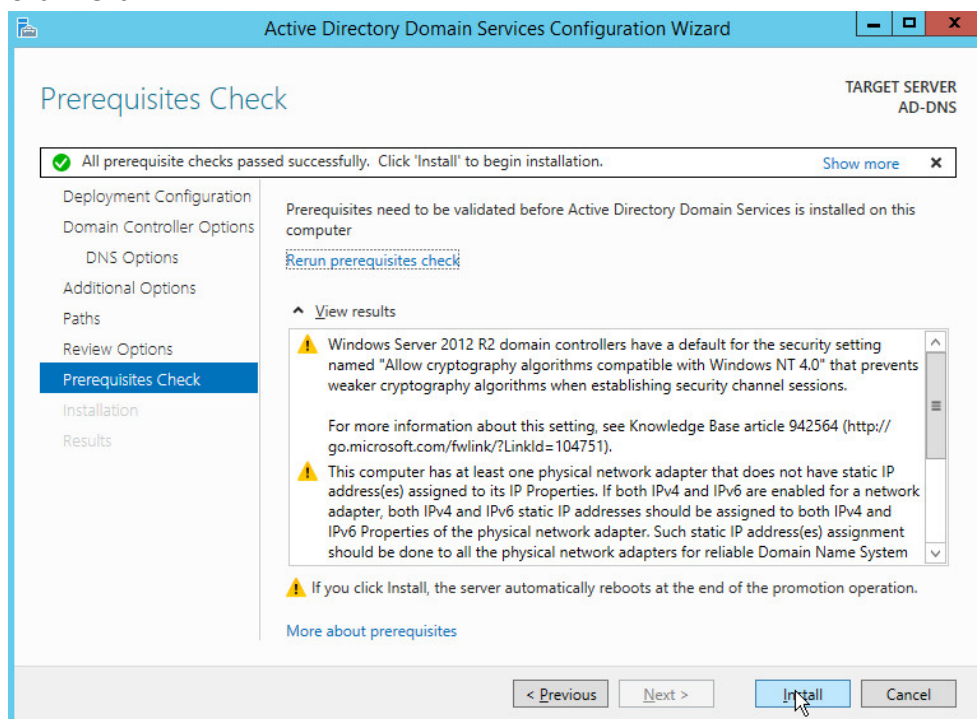
27. Click **Next**.



28. Click **Next**.



29. Click **Next**.



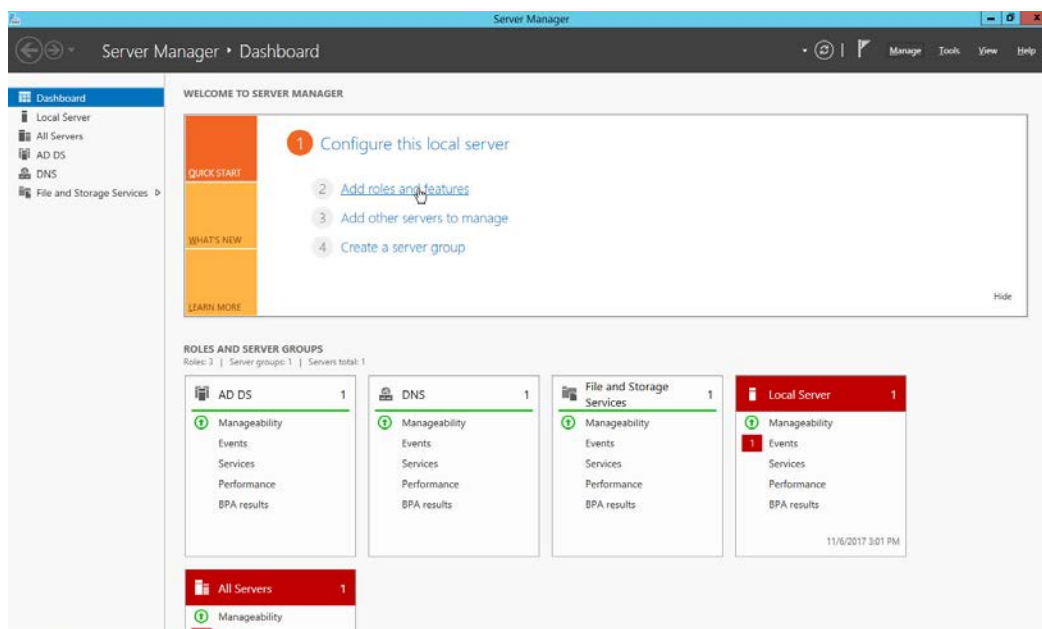
30. Click **Install**.

31. Wait for the installation to complete.

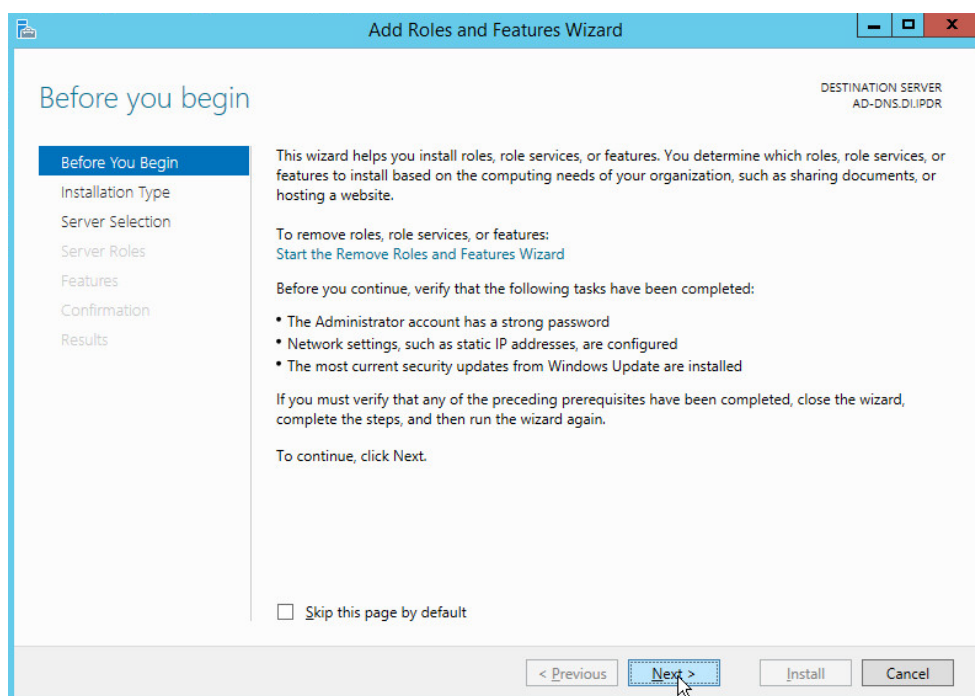
32. The server automatically reboots.

## 2.1.2 Creating a Certificate Authority

1. Open **Server Manager**.

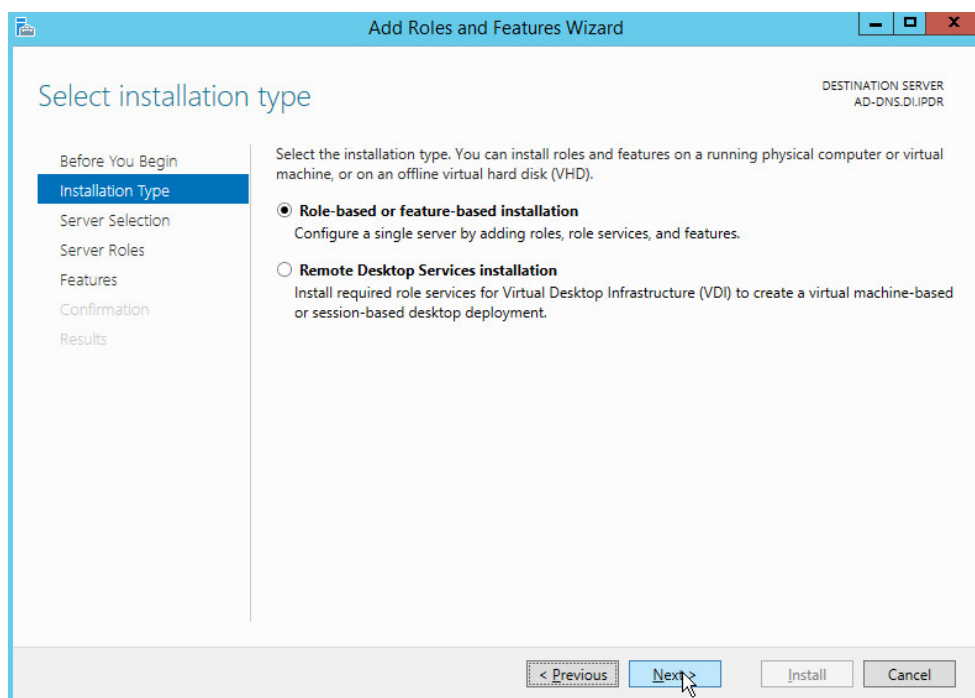


2. Click **Add roles and features**.

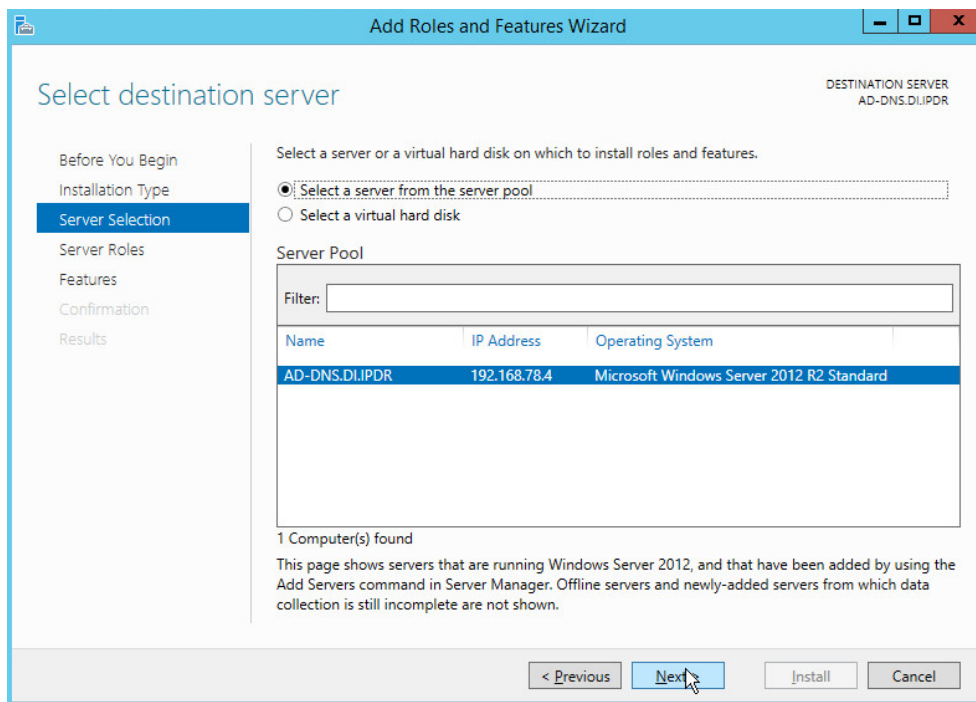


3. Click **Next**.
4. Select **Role-based or feature-based installation**.

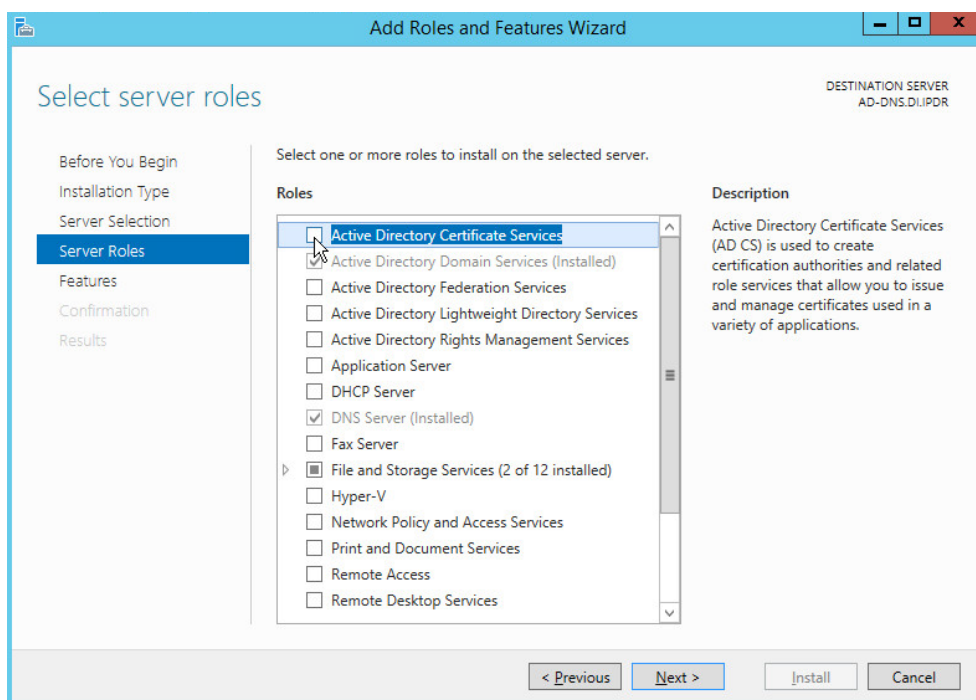




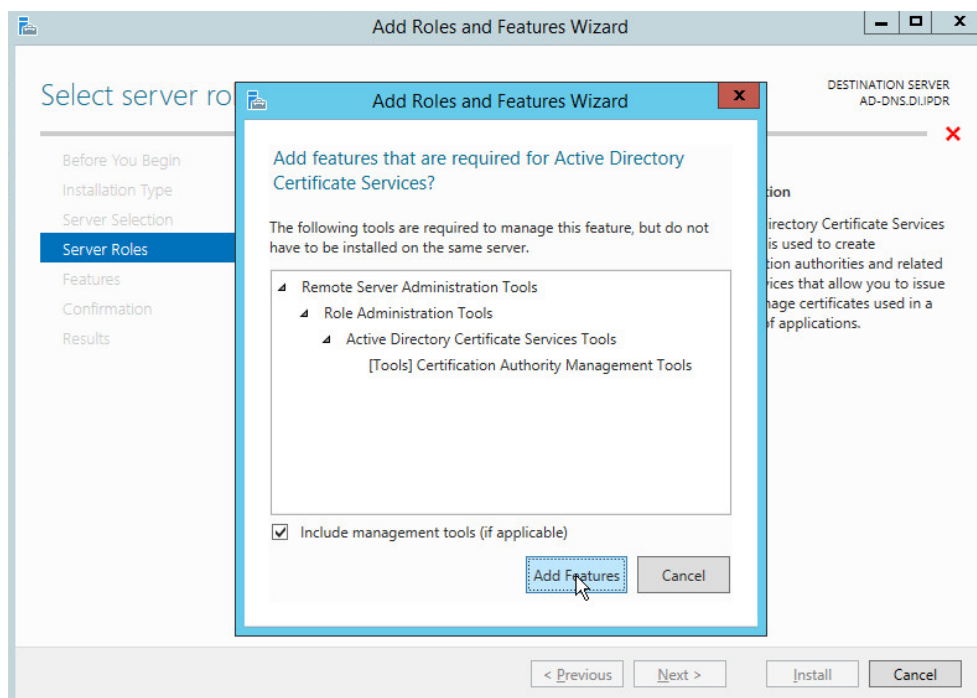
5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Select the intended Active Directory server.



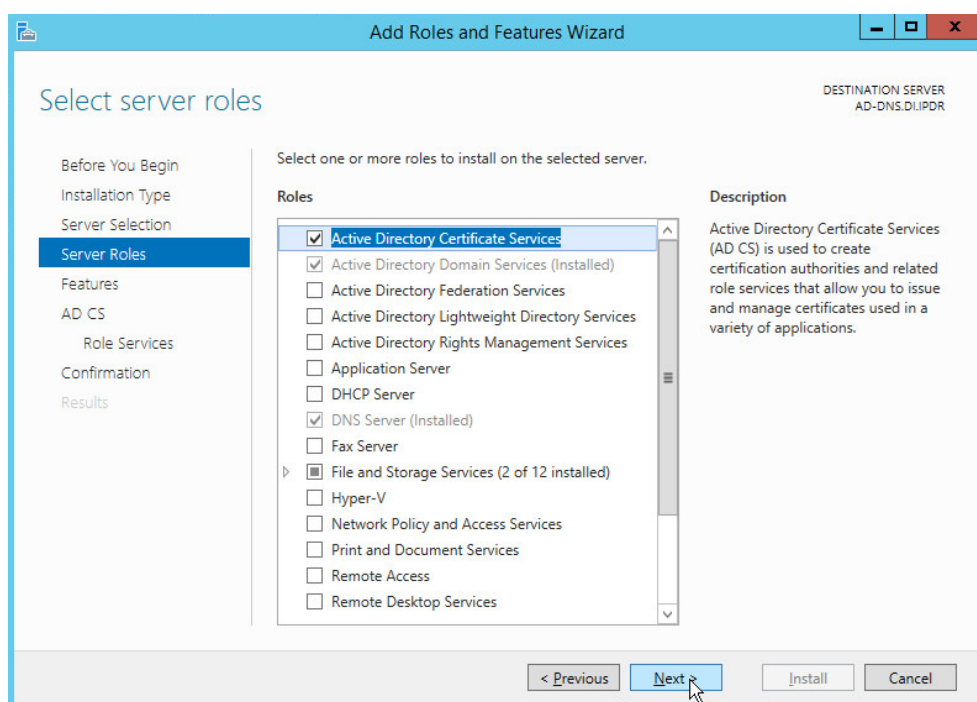
8. Click **Next**.



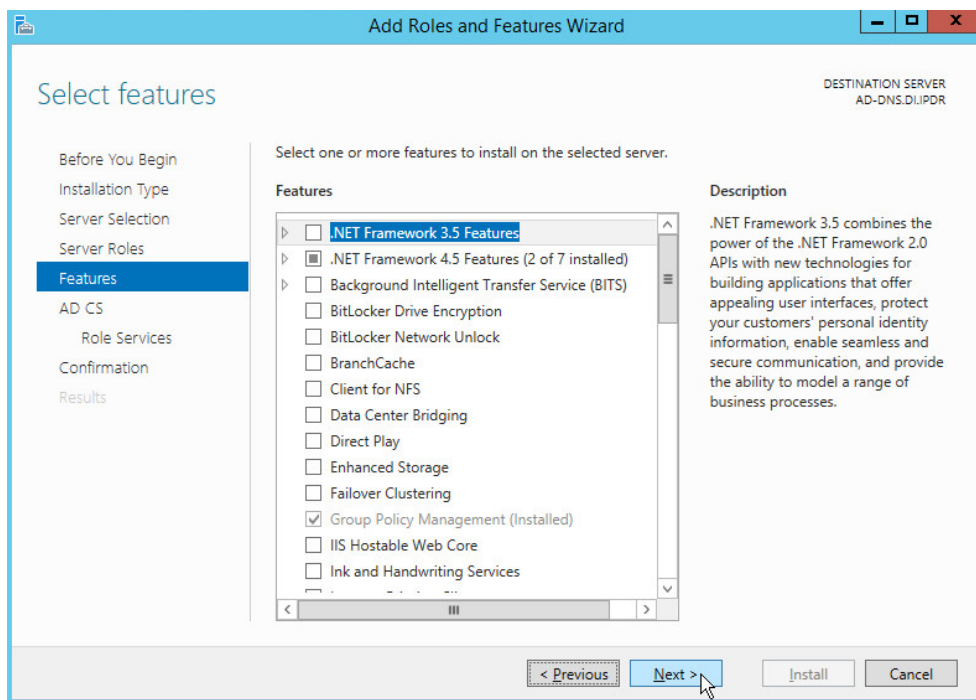
9. Check the box next to **Active Directory Certificate Services**.



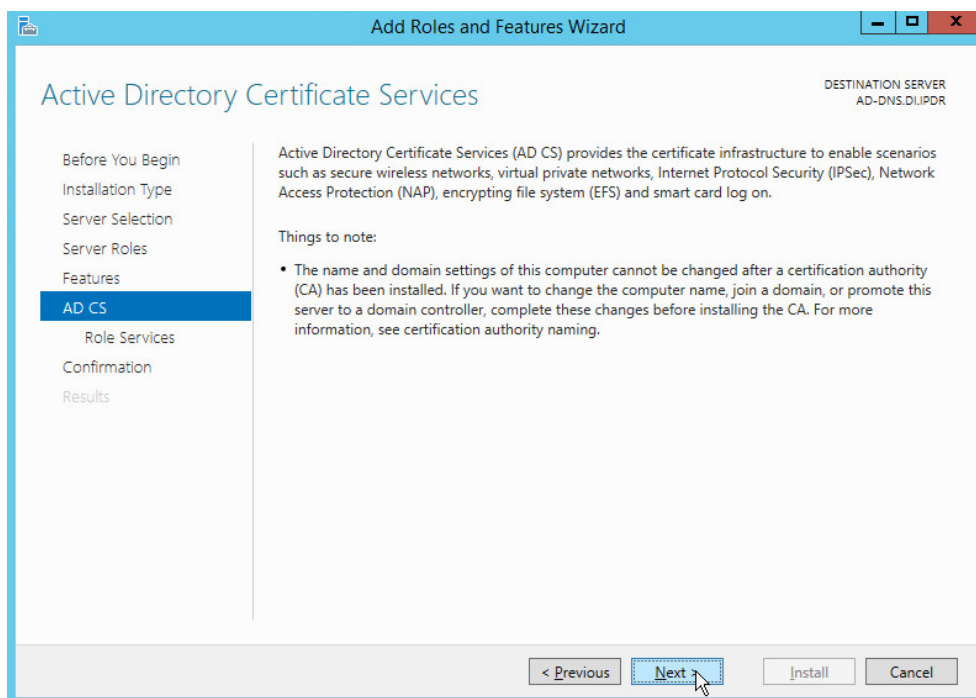
10. Click **Add Features**.



11. Click **Next**.

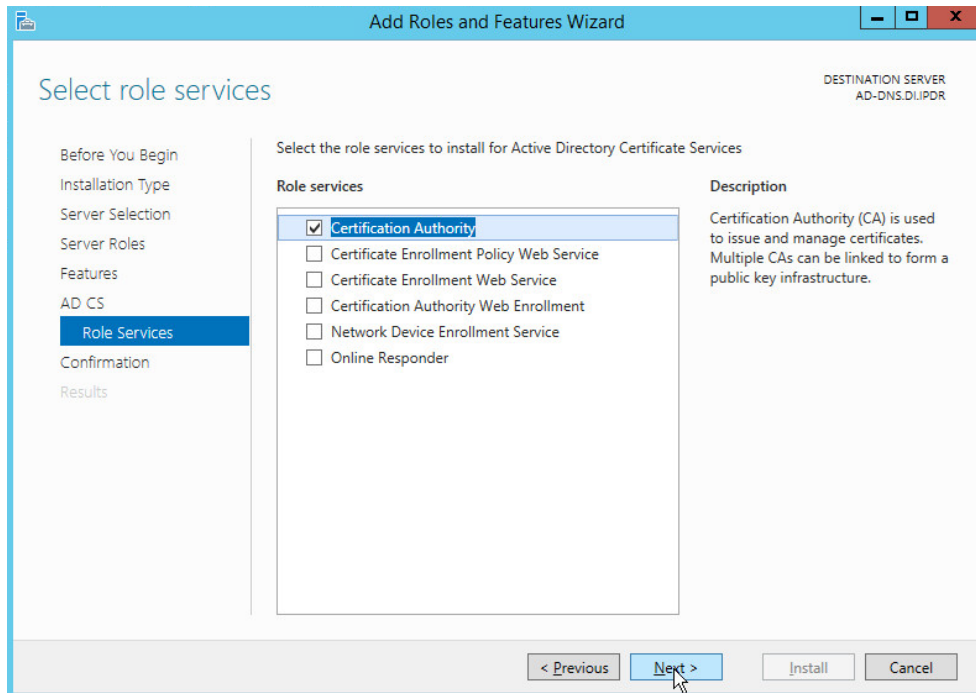


12. Click **Next**.

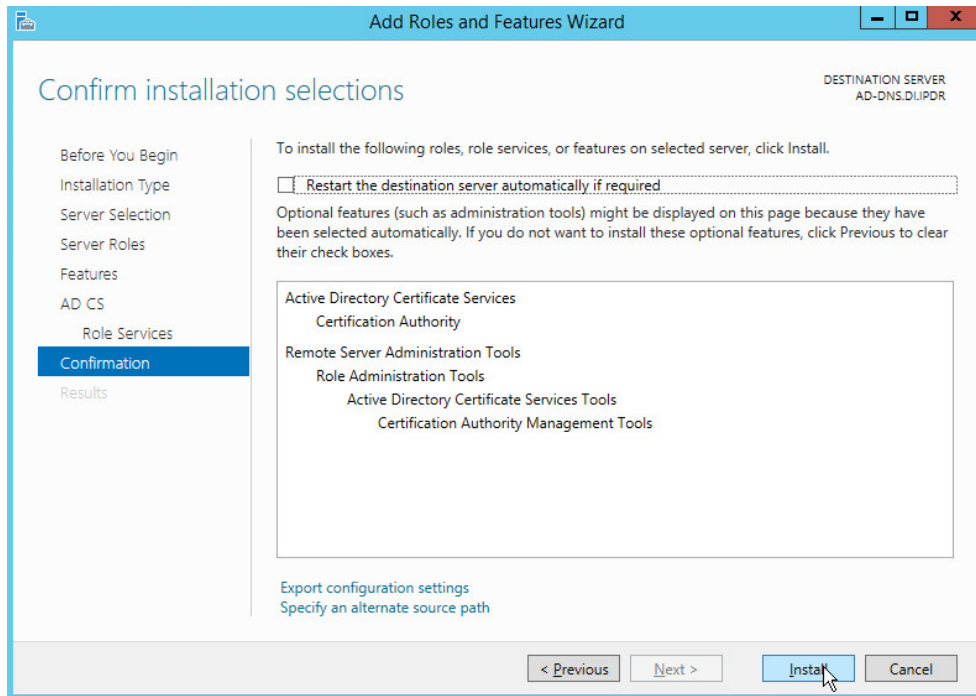


13. Click **Next**.

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

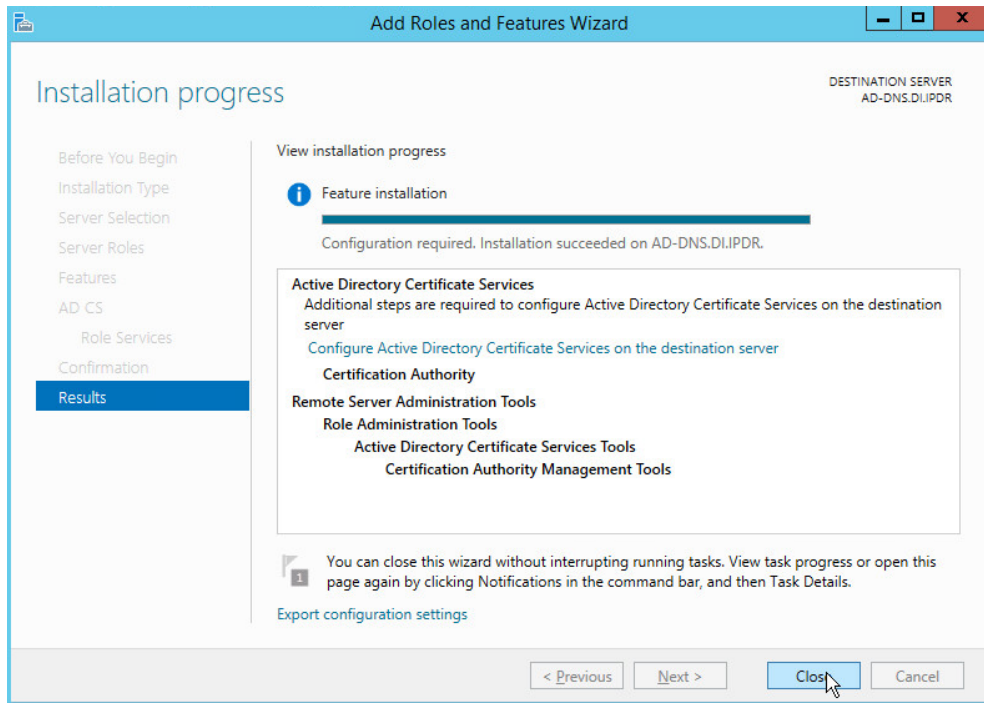


15. Click **Next**.

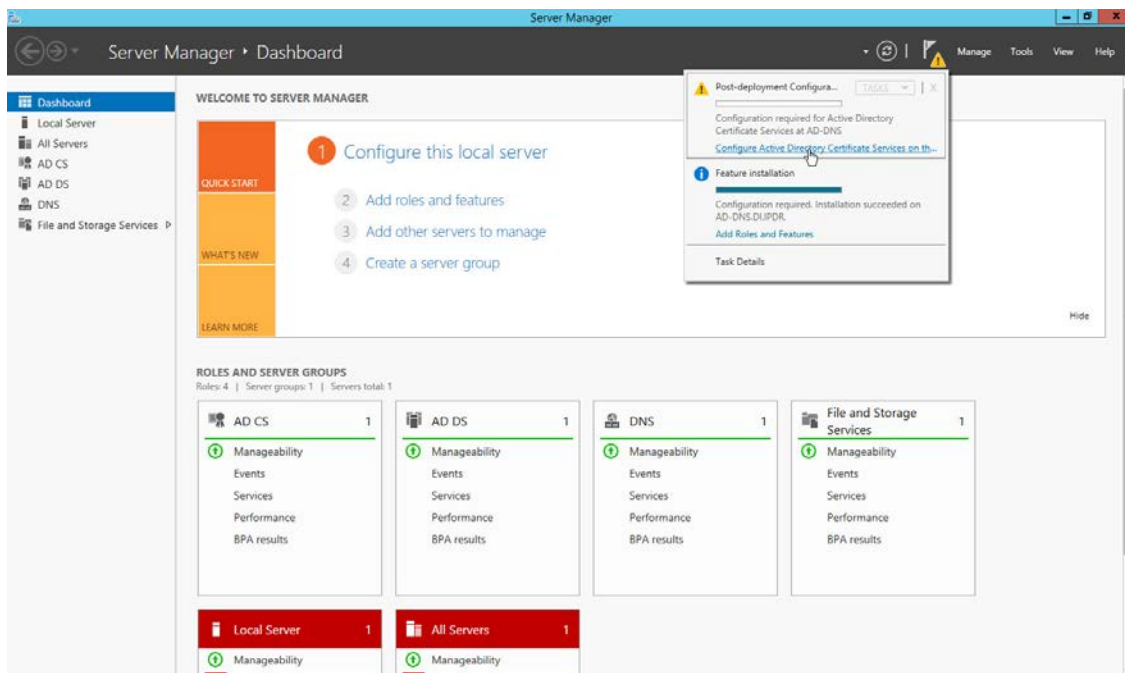


16. Click **Install**.

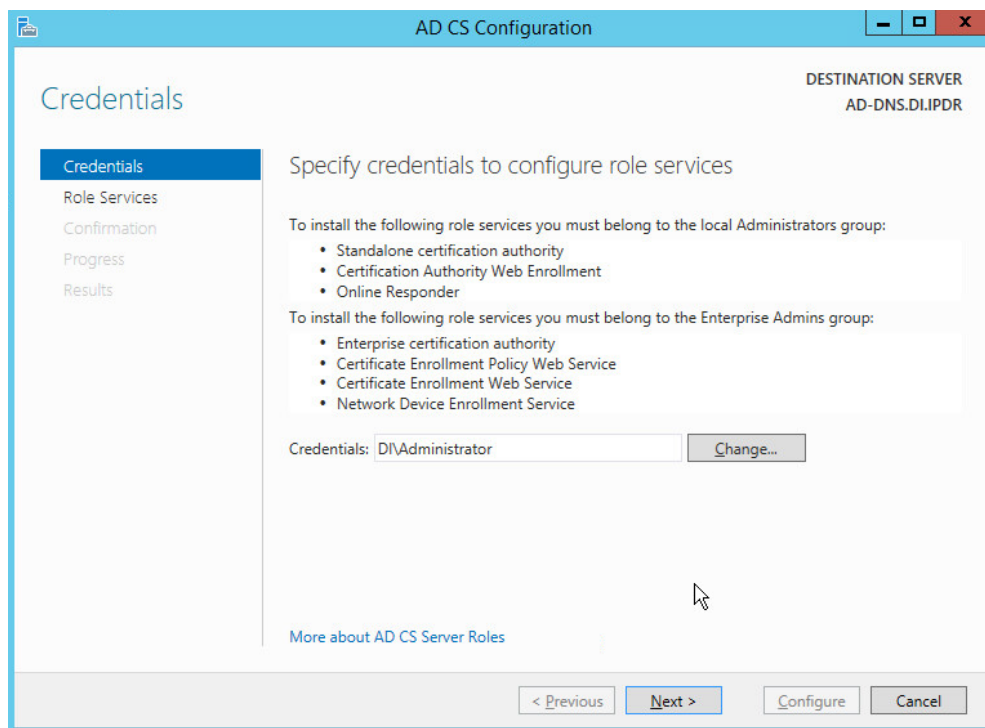
17. Wait for the installation to complete.



18. Click **Close**.



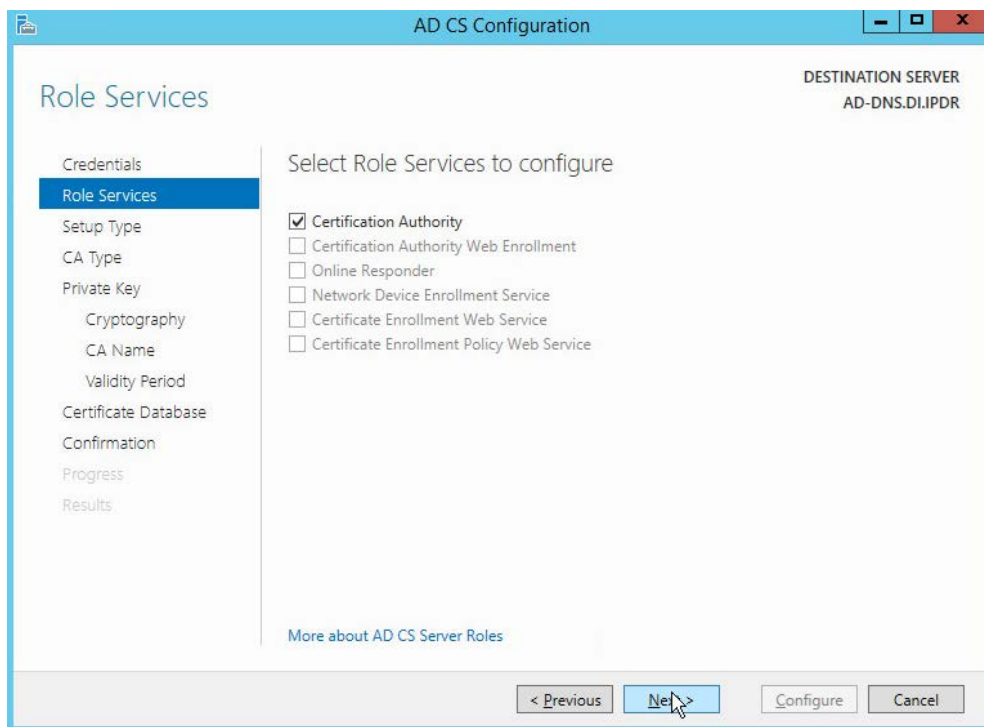
19. Click **Configure Active Directory Certificate Services on the destination server**.



20. Click **Next**.

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

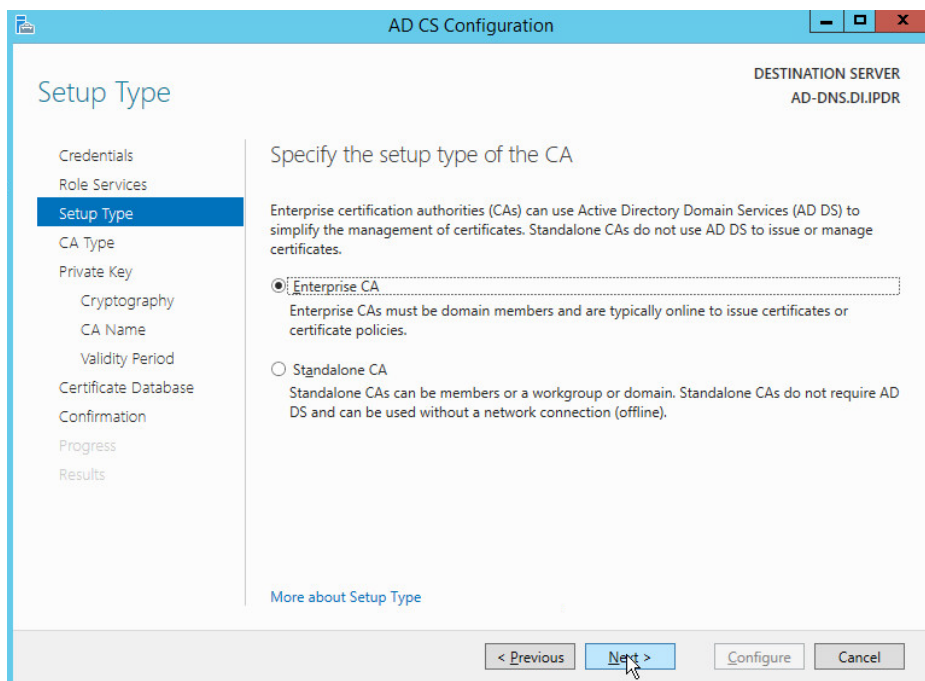




22. Click **Next**.

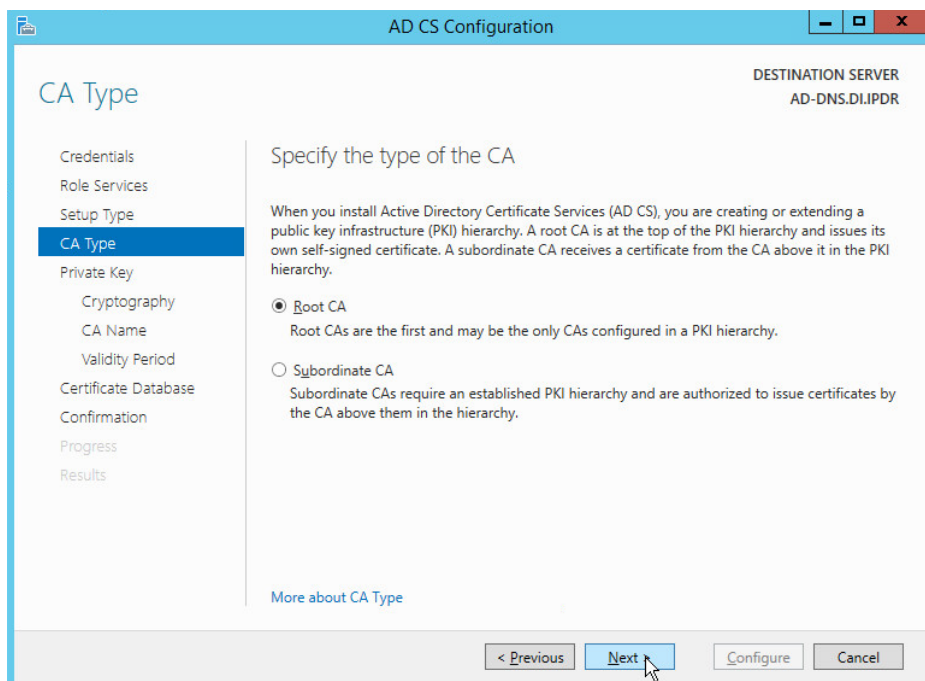
23. Select **Enterprise CA**.





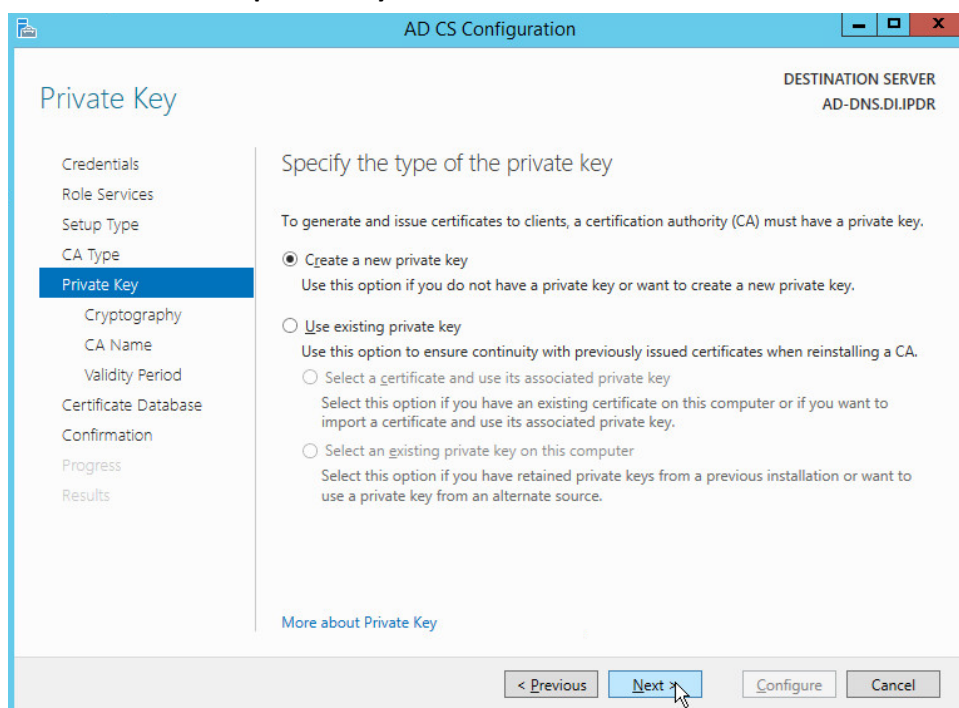
24. Click **Next**.

25. Select **Root CA**.



26. Click **Next**.

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

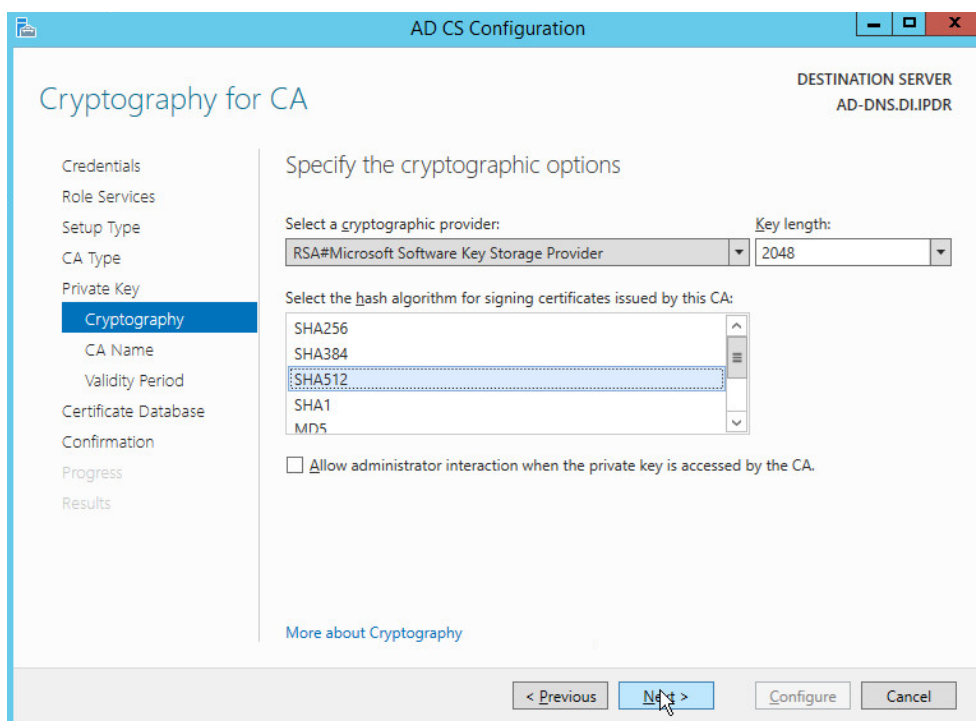


28. Click **Next**.

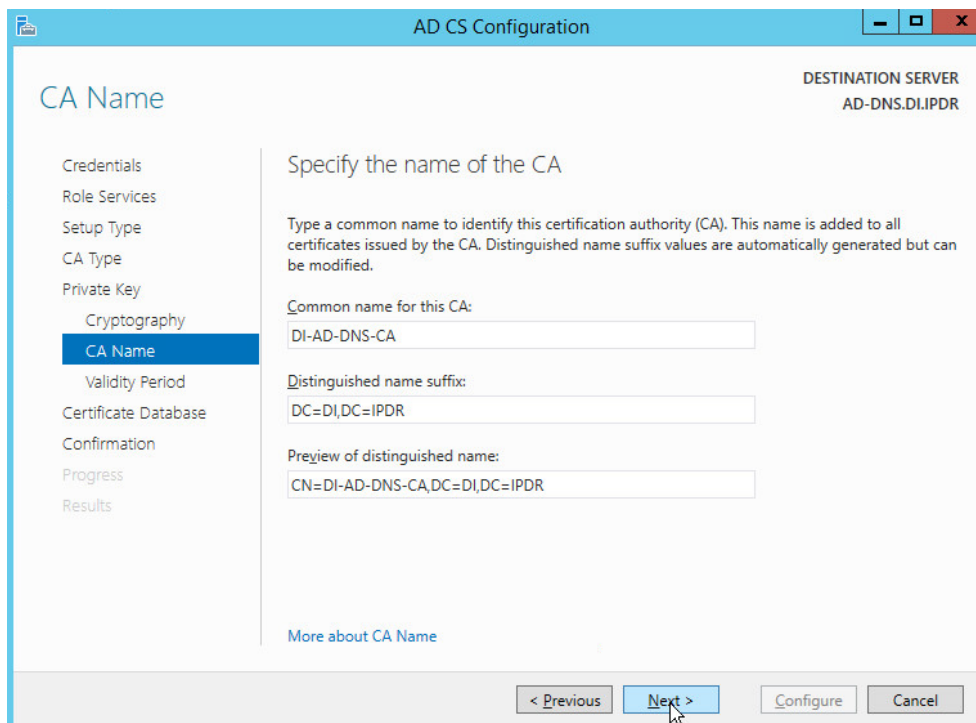
29. Select **RSA#Microsoft Software Key Storage Provider**.

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

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



32. Click **Next**.



33. Click **Next**.

34. Set the time to 5 years.

35. Click **Next**.

AD CS Configuration

DESTINATION SERVER  
AD-DNS.DI.IPDR

### CA Database

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
**Certificate Database**  
Confirmation  
Progress  
Results

Specify the database locations

Certificate database location:  
C:\Windows\system32\CertLog

Certificate database log location:  
C:\Windows\system32\CertLog

[More about CA Database](#)

< Previous   **Next >**   Configure   Cancel

36. Click **Next**.

AD CS Configuration

DESTINATION SERVER  
AD-DNS.DI.IPDR

### Confirmation

Credentials  
Role Services  
Setup Type  
CA Type  
Private Key  
Cryptography  
CA Name  
Validity Period  
Certificate Database  
**Confirmation**  
Progress  
Results

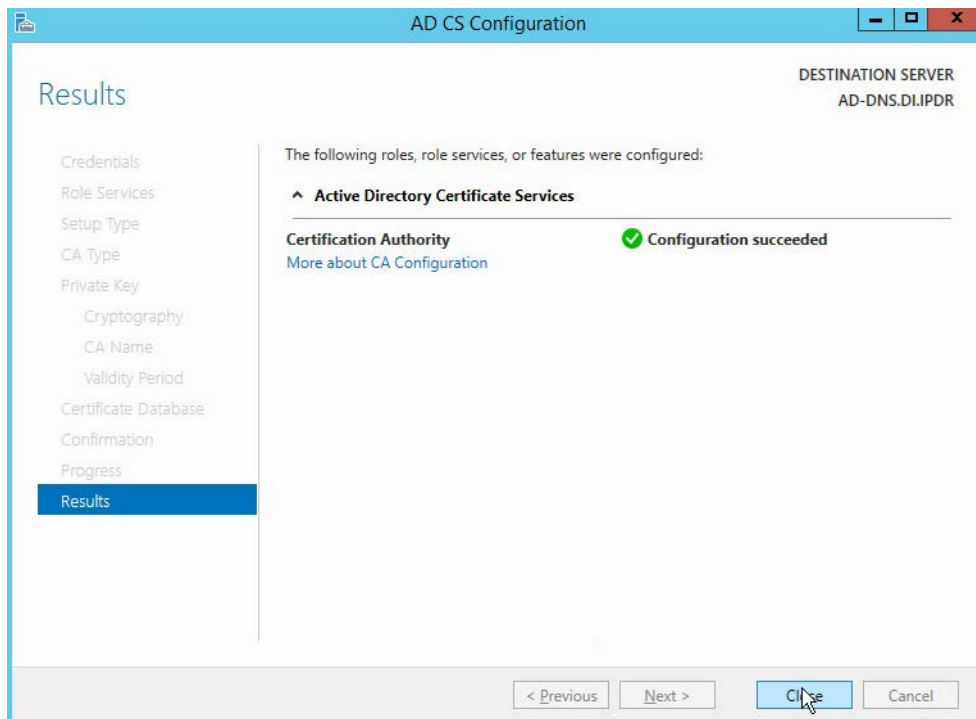
To configure the following roles, role services, or features, click Configure.

^ **Active Directory Certificate Services**

Certification Authority	
CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA512
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	11/6/2022 3:19:00 PM
Distinguished Name:	CN=DI-AD-DNS-CA,DC=DI,DC=IPDR
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

< Previous   Next >   **Configure**   Cancel

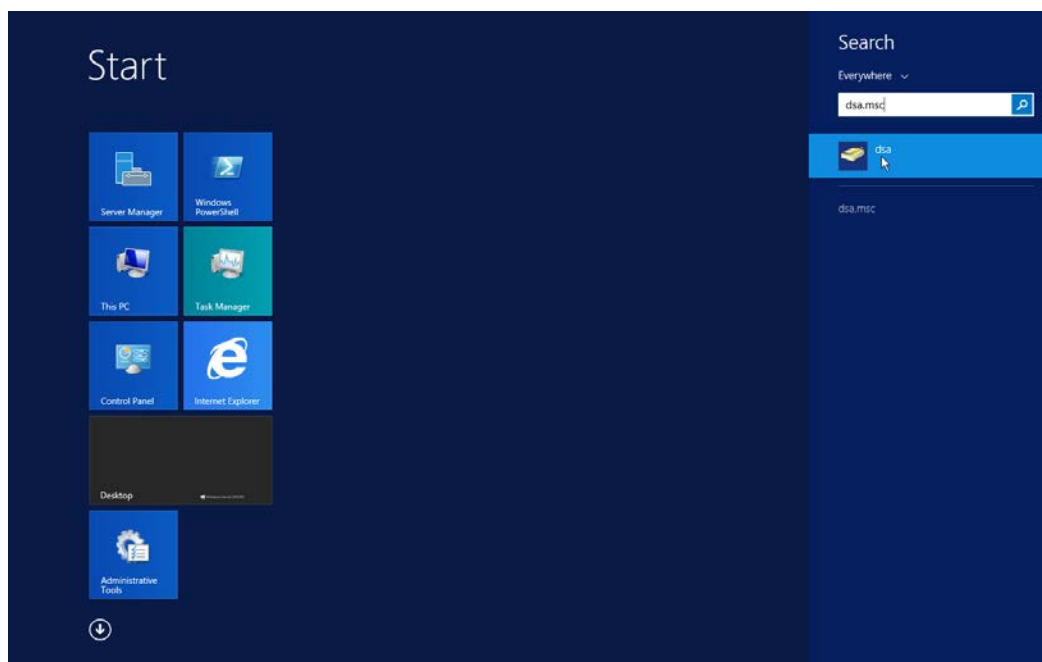
37. Click **Configure**.



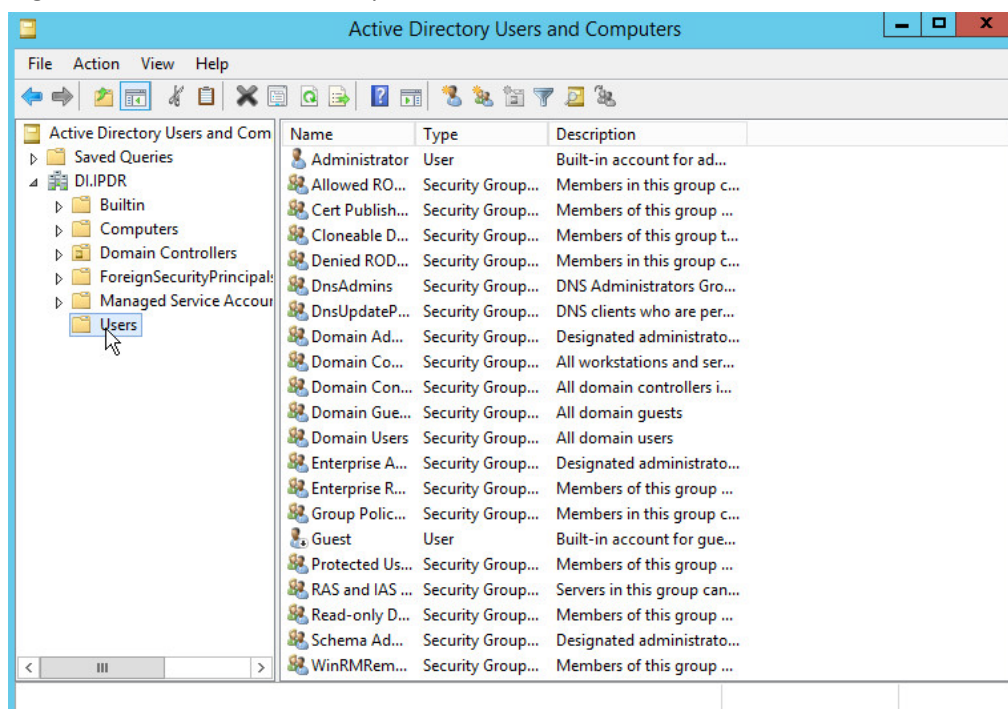
38. Click **Close**.

### 2.1.3 Configure Account to Add Computers to Domain

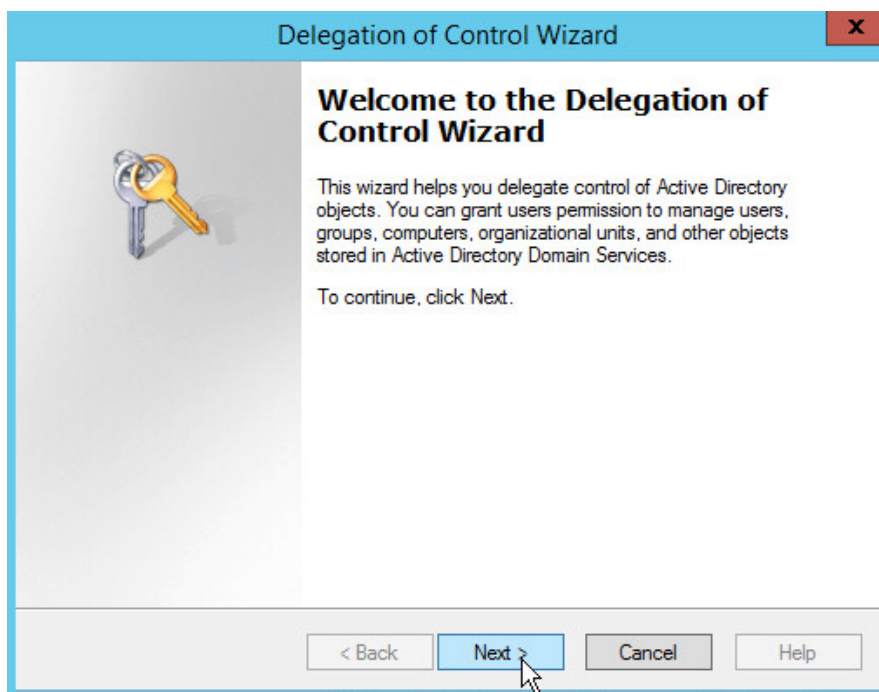
1. Open the Start menu.
2. Enter **dsa.msc** and run the program.



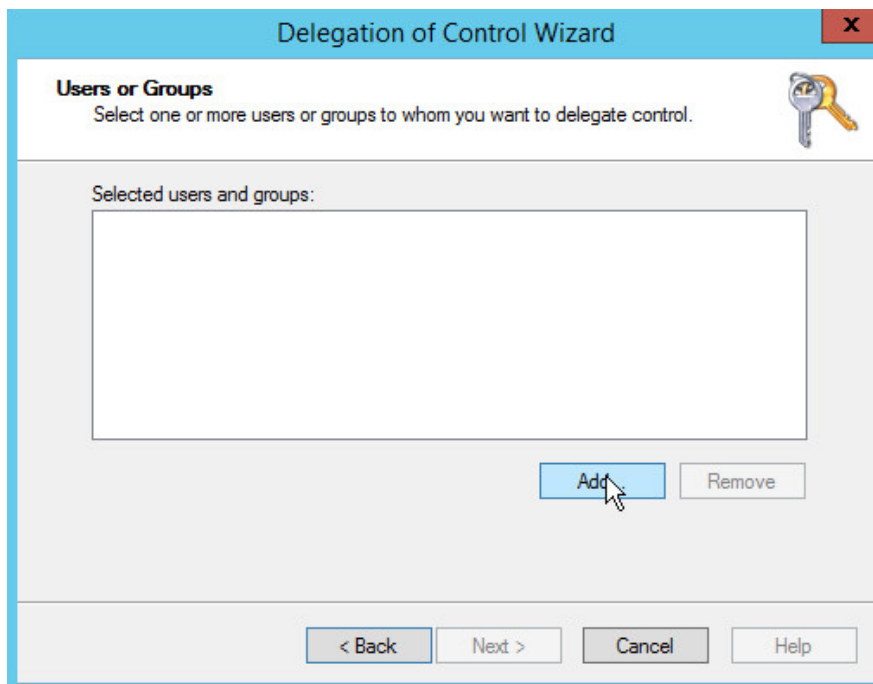
3. Right-click on **Users** in the left panel.



4. Click **Delegate Control**.



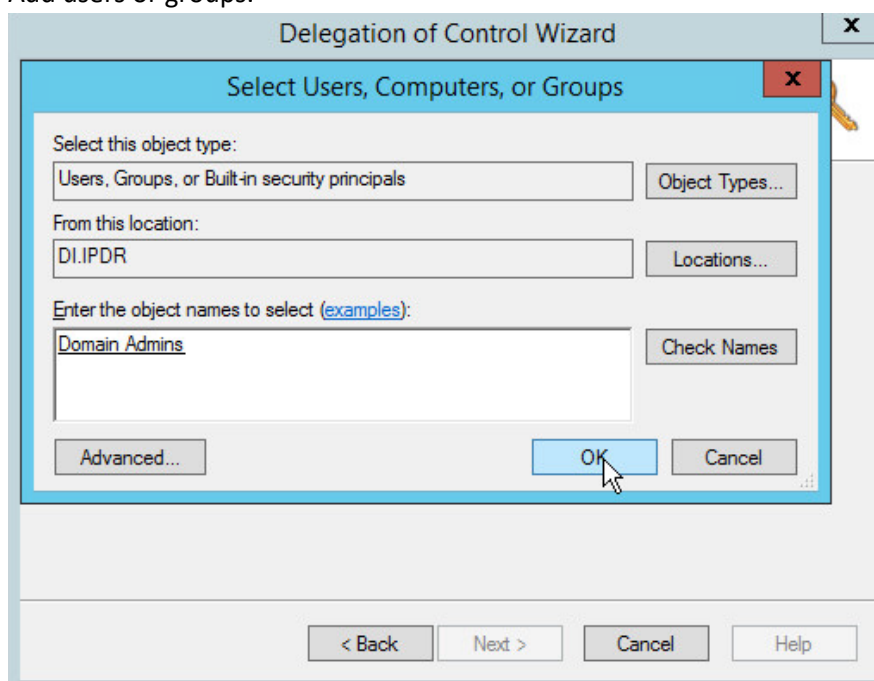
5. Click **Next**.



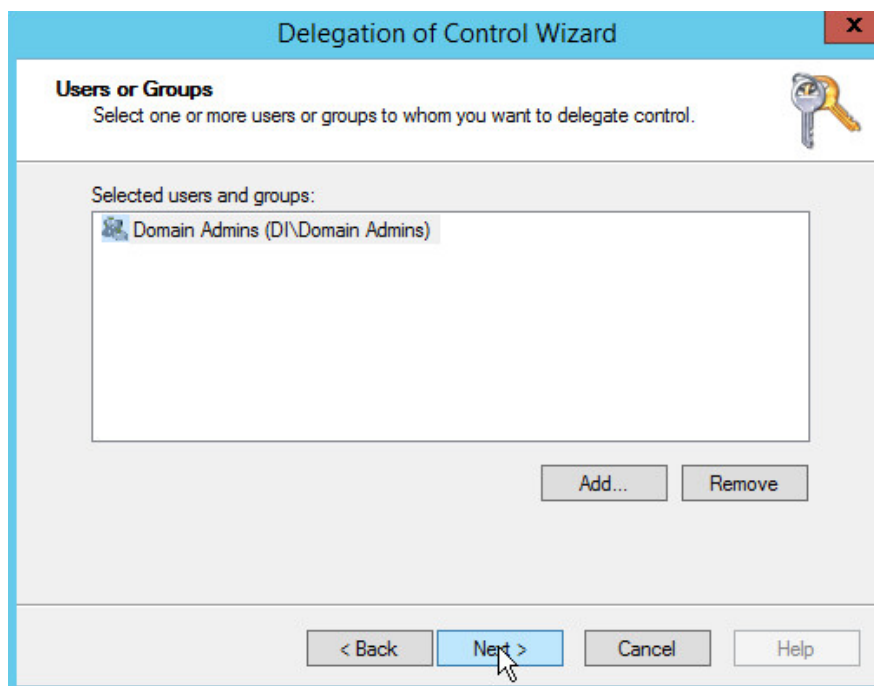
6. Click **Add** to select users or groups.



7. Add users or groups.

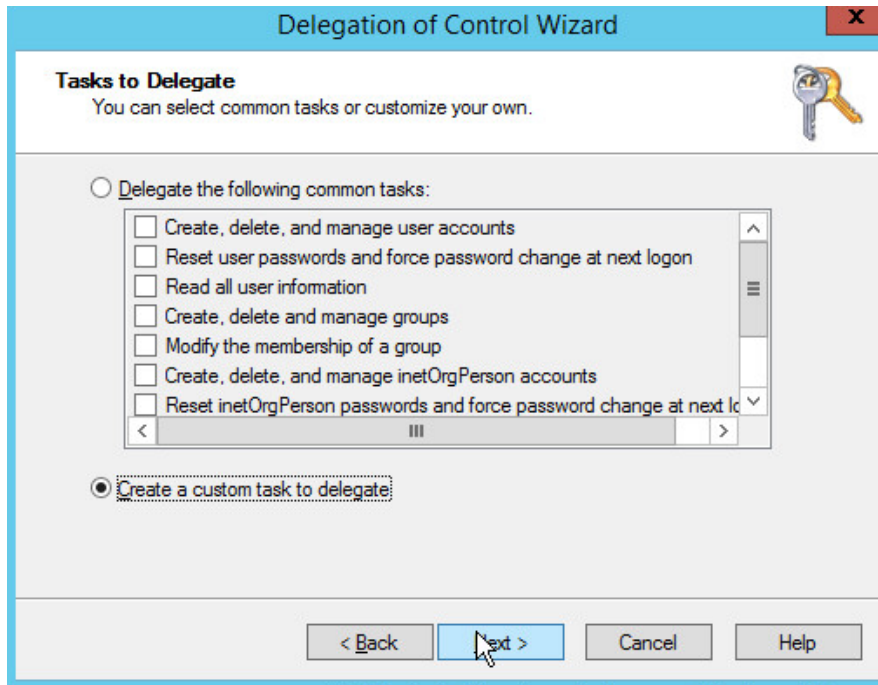


8. Click **OK**.



9. Click **Next**.

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



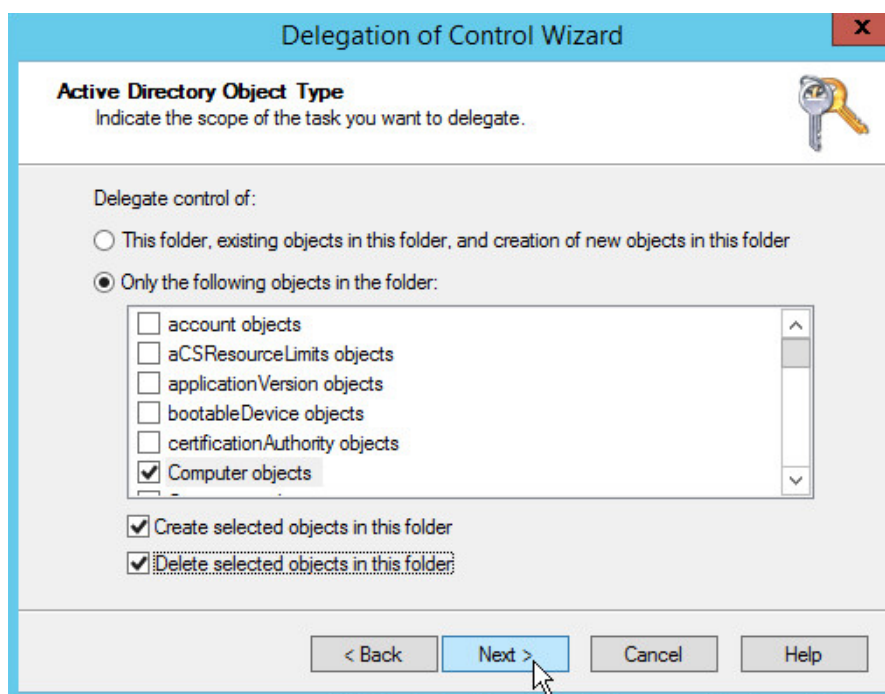
11. Click **Next**.

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

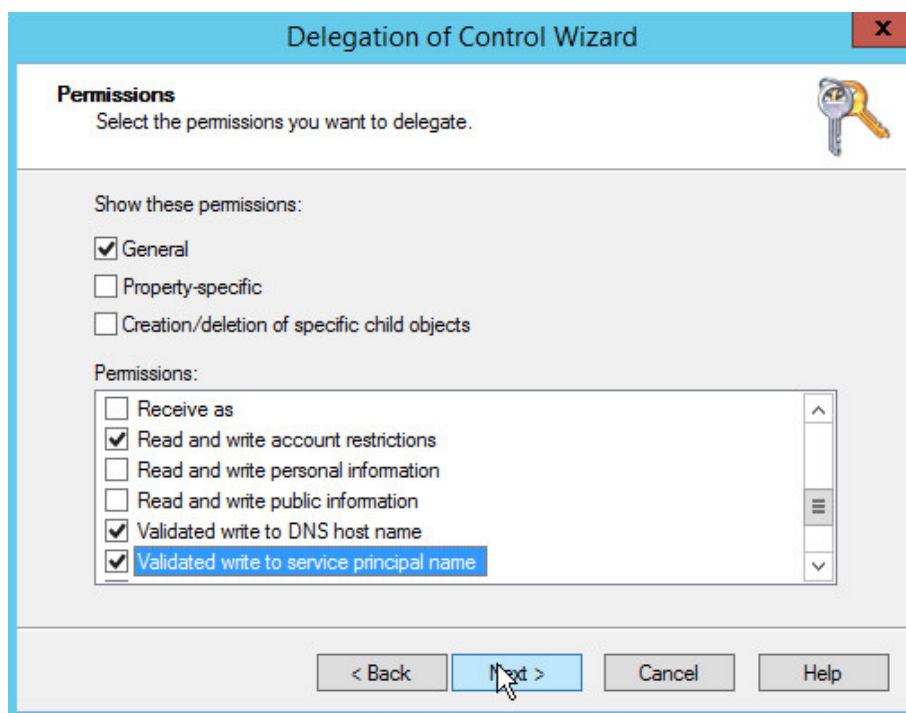
13. Check the box next to **Computer objects**.

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

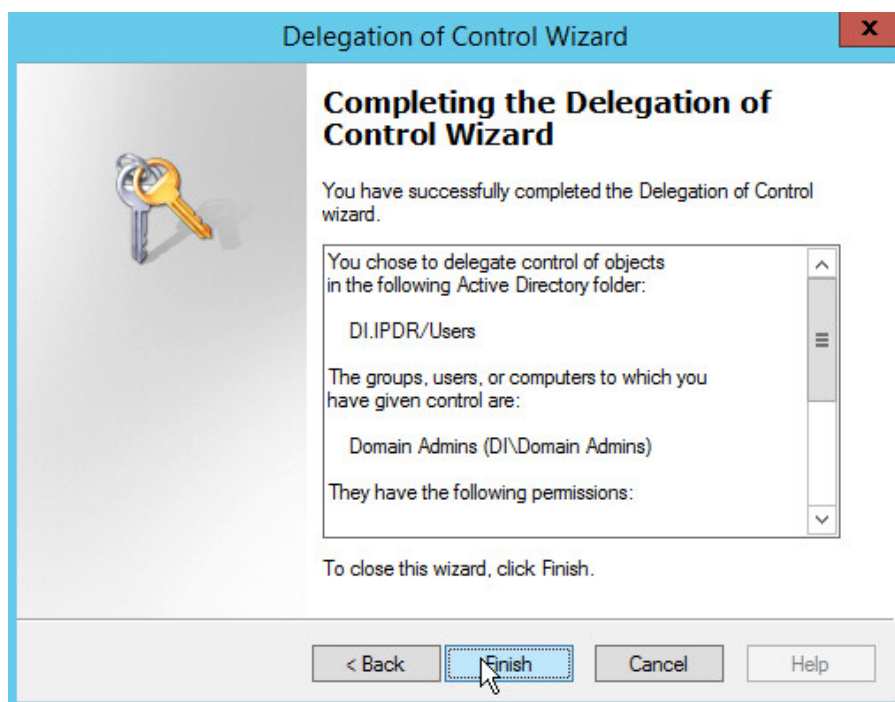
15. Check the box next to **Delete selected objects in this folder**.



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



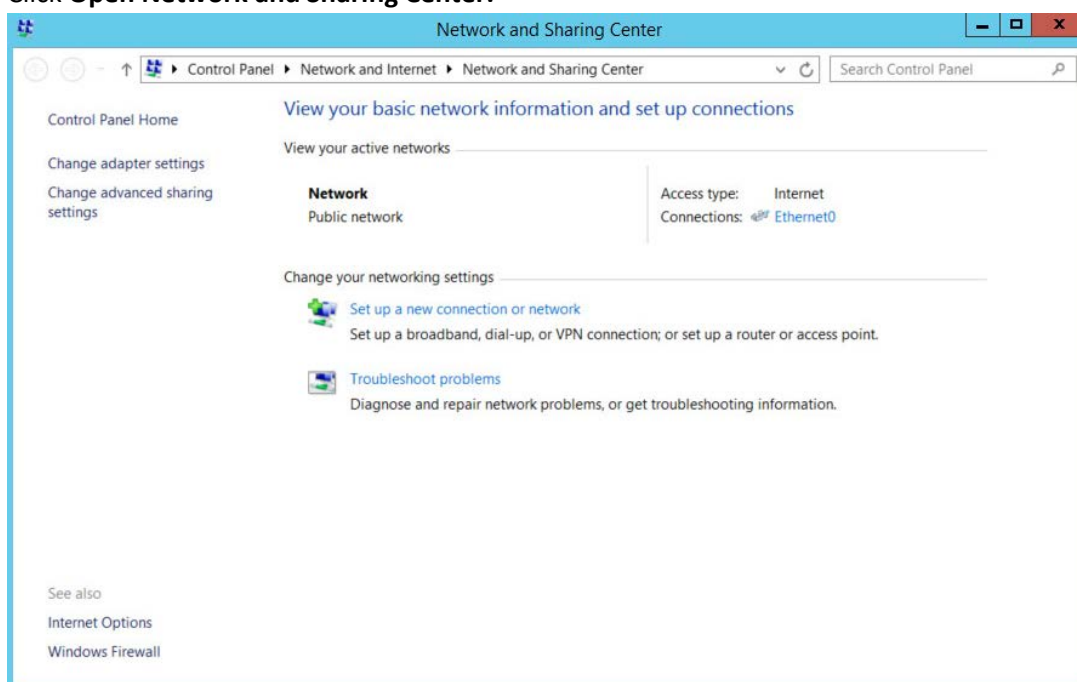
18. Click **Next**.



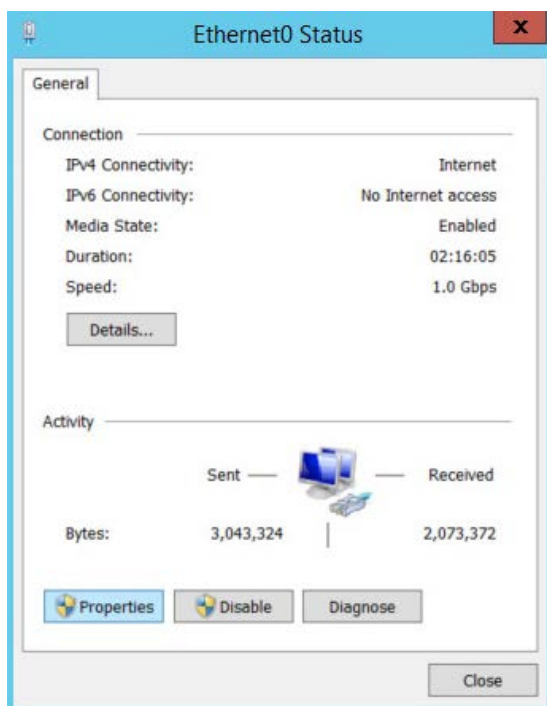
19. Click **Finish**.

## 2.1.4 Adding Machines to the Domain

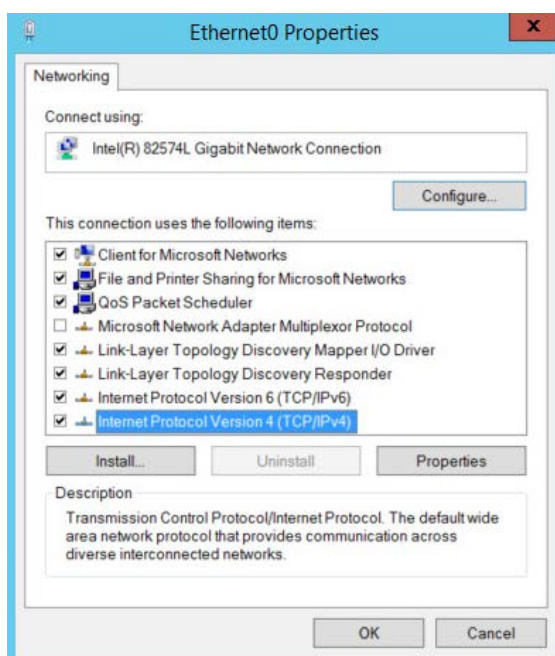
1. Right-click the network icon in the task bar on a computer that you wish to add to the domain.
2. Click **Open Network and Sharing Center**.



3. Click the name of the internet adapter.

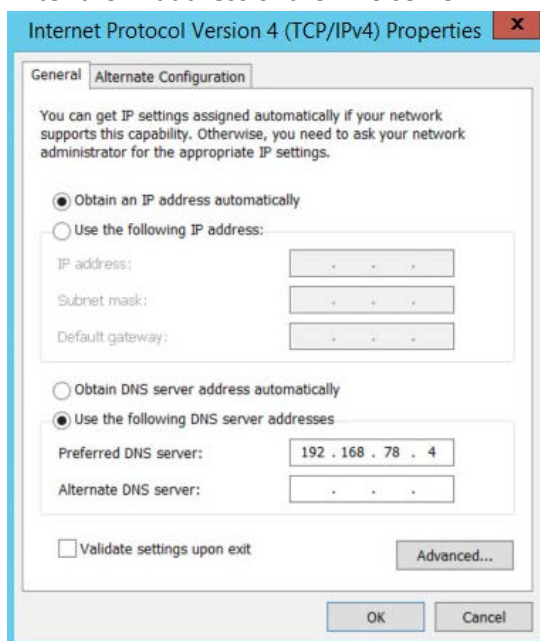


4. Click **Properties**.

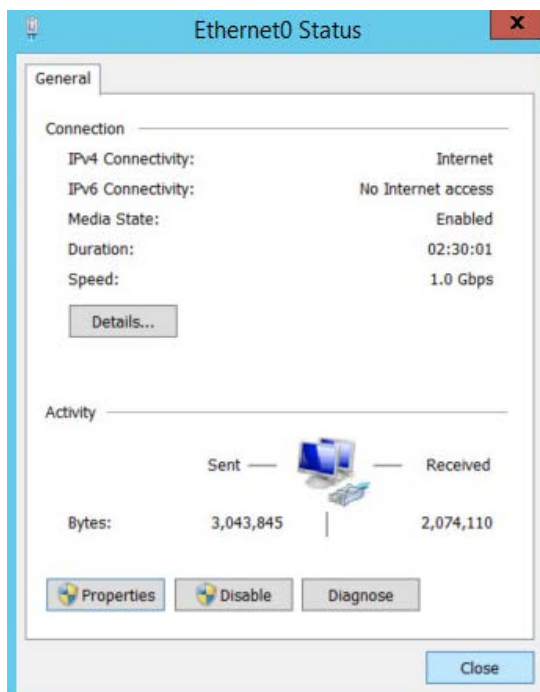


5. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
6. Select **Use the following DNS server addresses**.

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

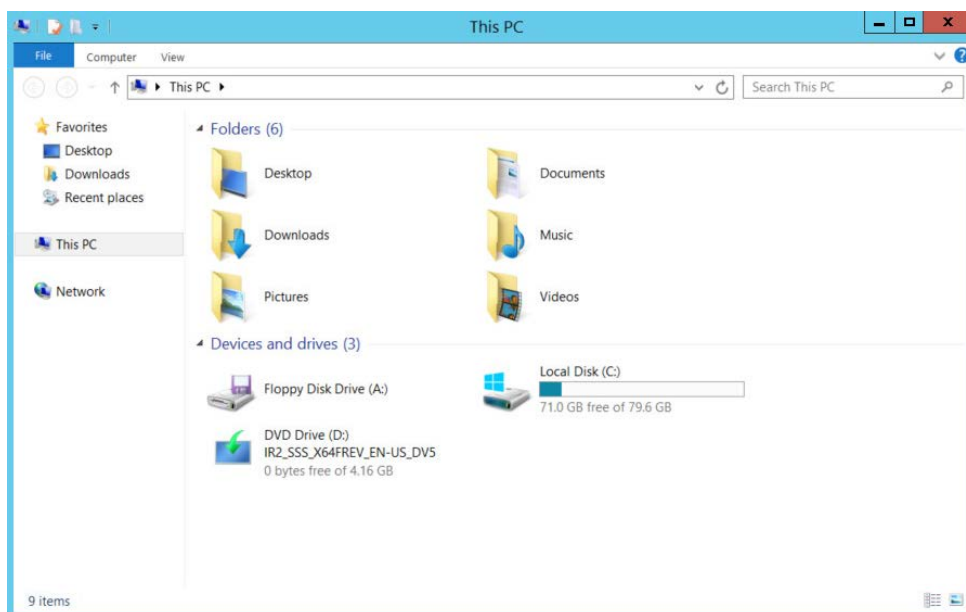


8. Click **OK**.
9. Click **OK**.

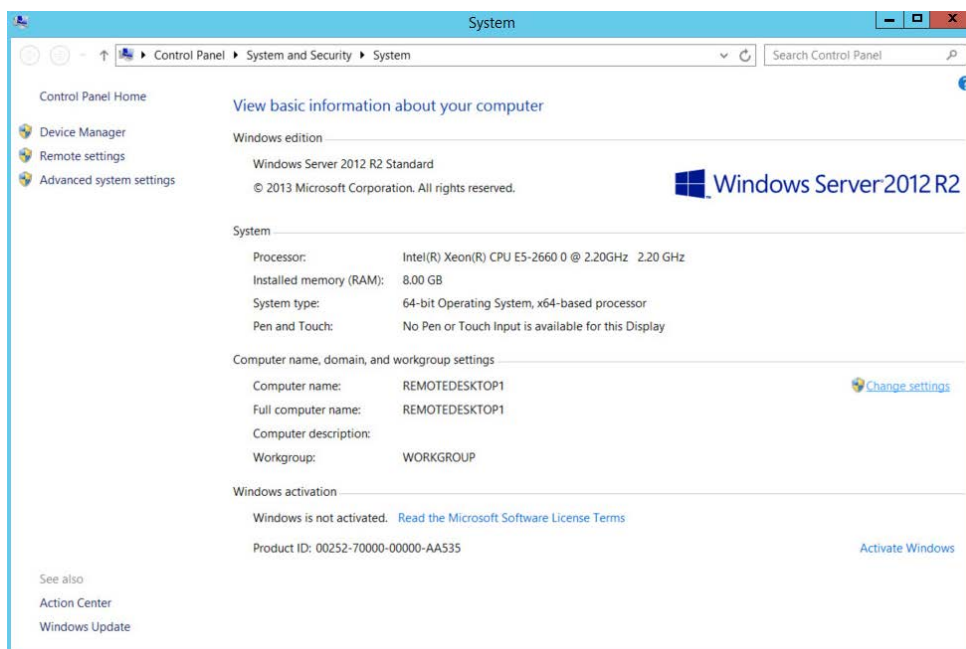


10. Click **Close**.

## 11. Navigate to **This PC**.

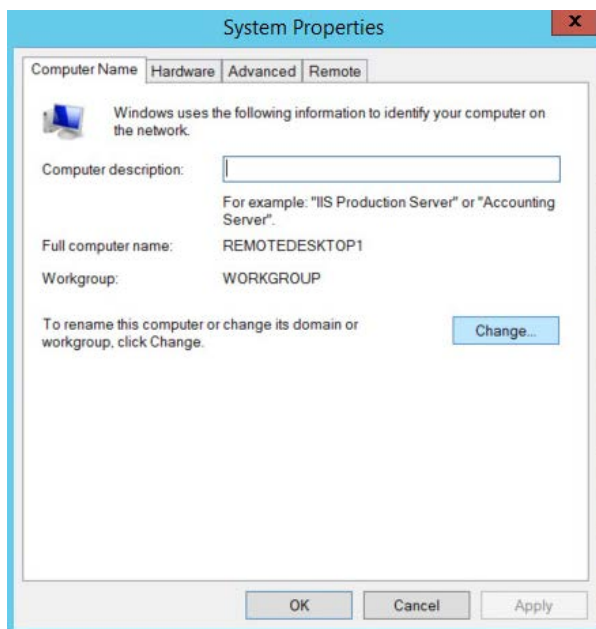


## 12. Right-click in the window and click **Properties**.

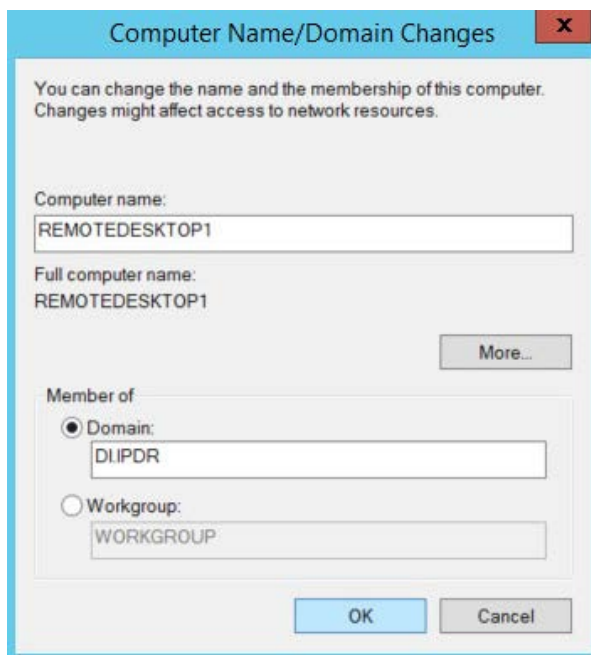


## 13. Click **Change Settings**.



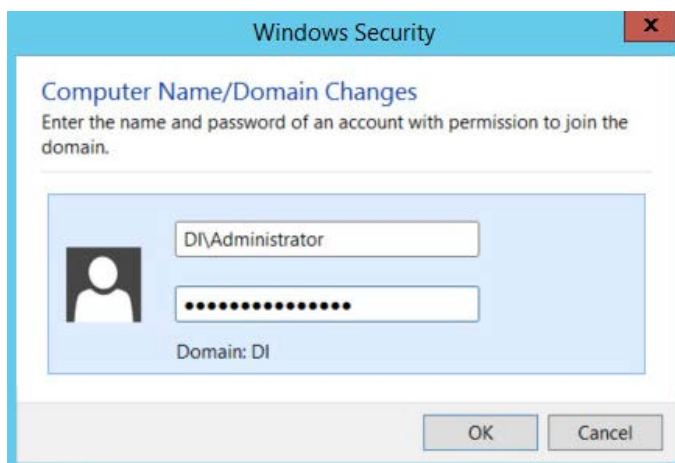


14. Click **Change**.
15. Select **Domain**.
16. Enter the domain.

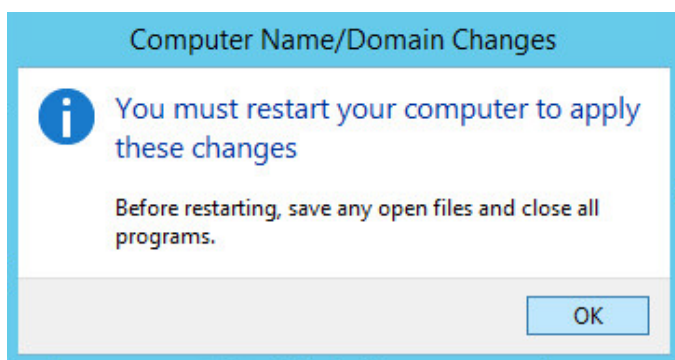


17. Click **OK**.

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



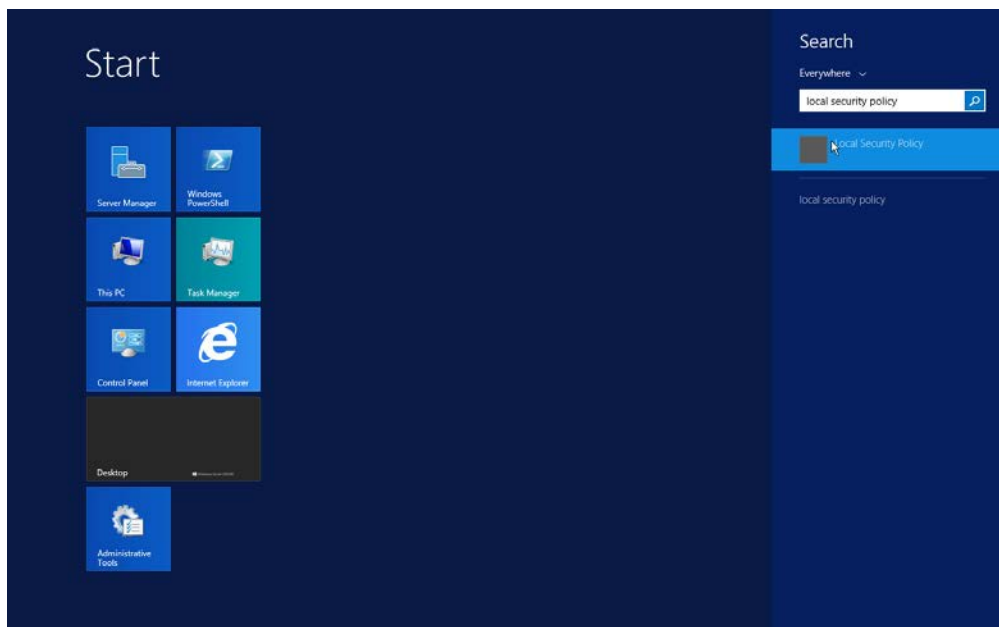
19. Click **OK**.



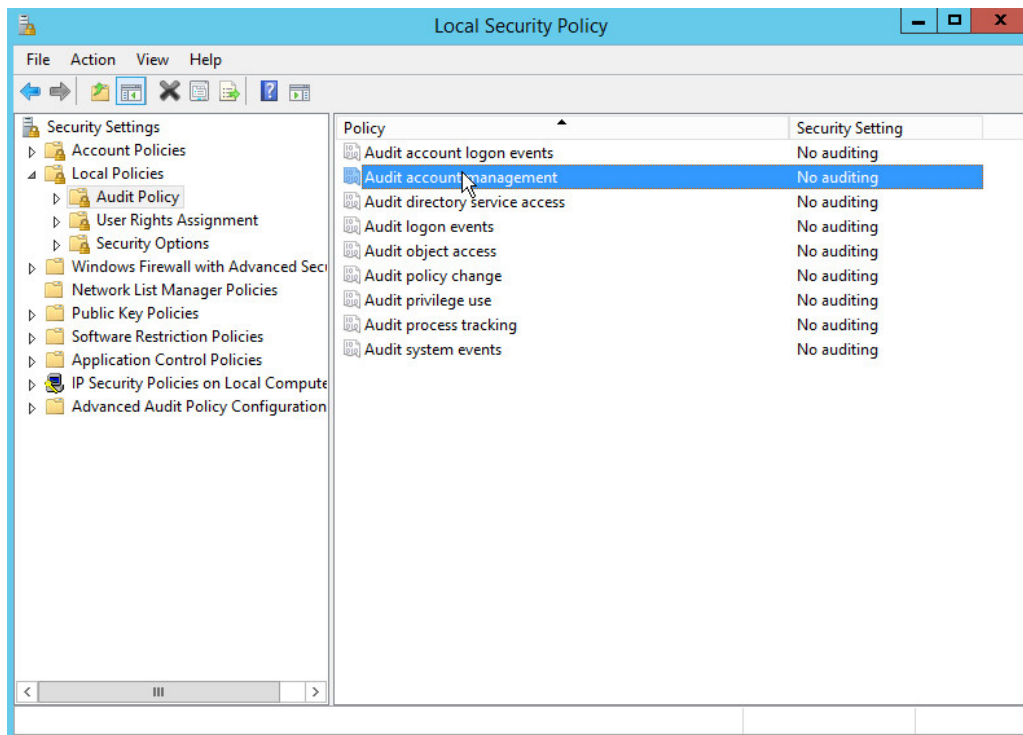
20. Click **OK** when prompted to restart the computer.

## 2.1.5 Configure Active Directory to Audit Account Activity

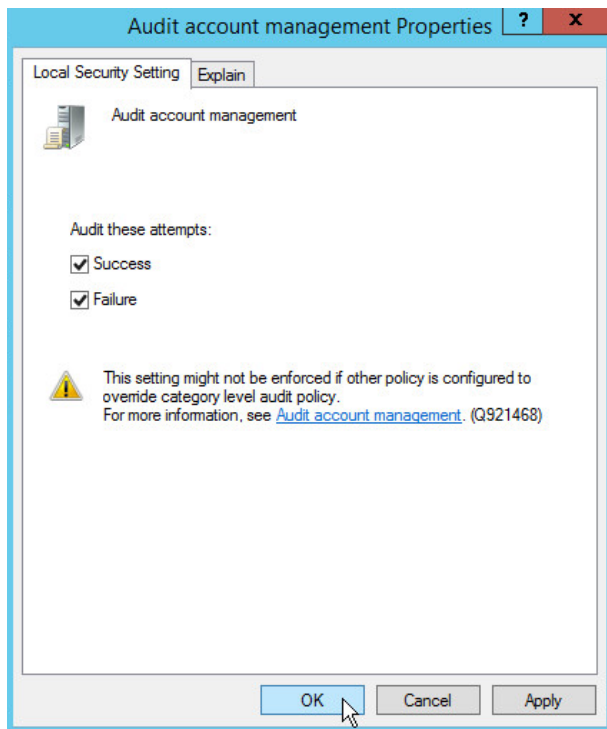
1. Open the Start menu.



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



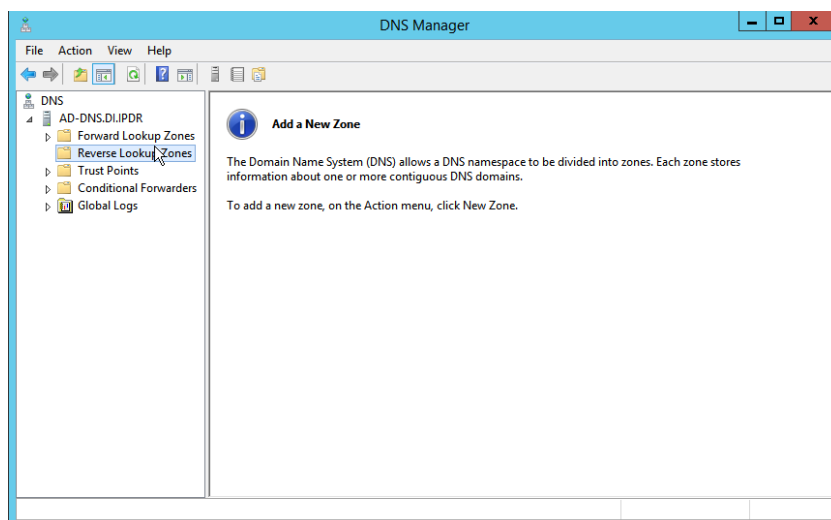
5. Click **Properties**.
6. Check the boxes next to **Success** and **Failure**.



7. Click **OK**.

### 2.1.6 Configure Reverse Lookup Zones

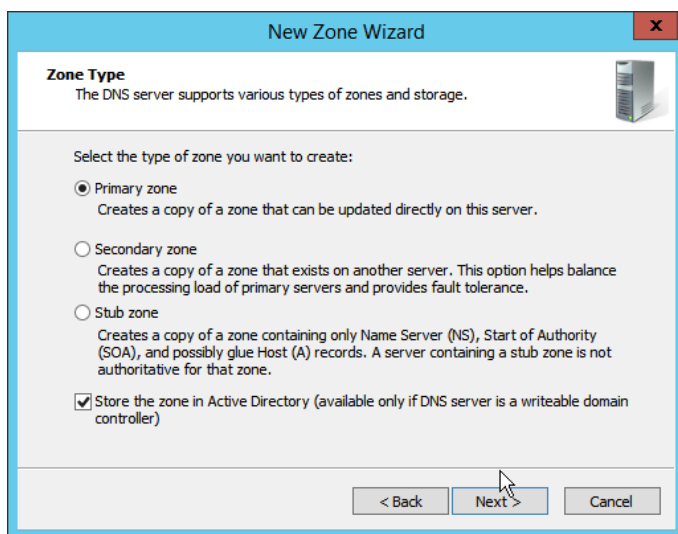
1. Open **DNS Manager** by right-clicking the DNS server in **Server Manager**.
2. Click **Reverse Lookup Zones**.



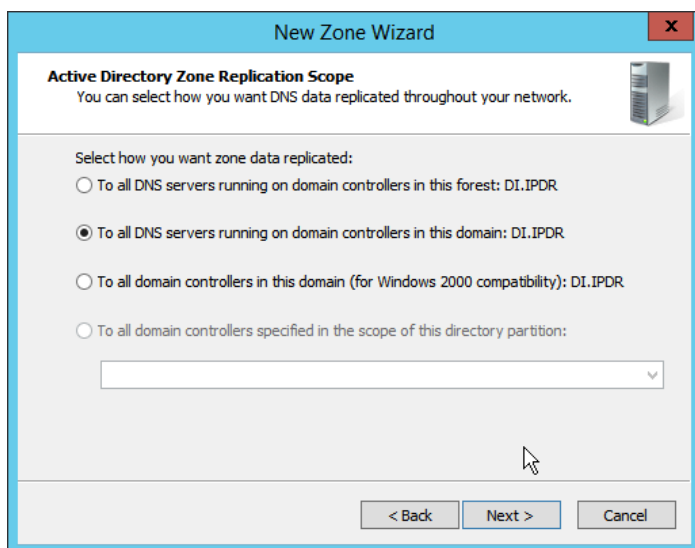
3. Click **Action > New Zone**.



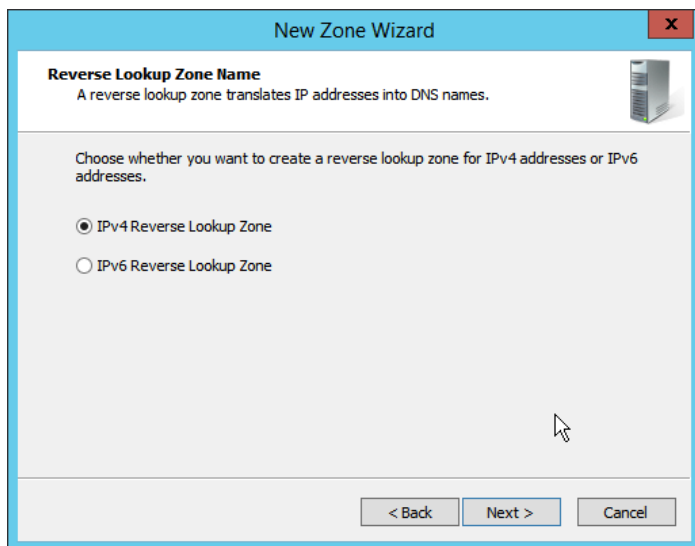
4. Click **Next**.



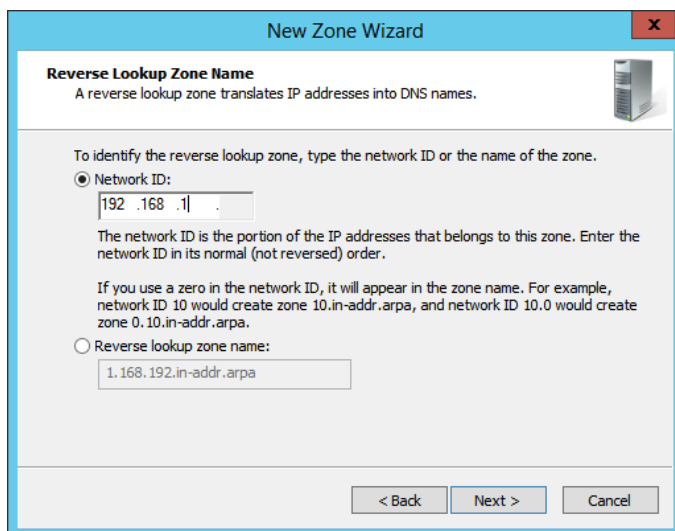
5. Click **Next**.



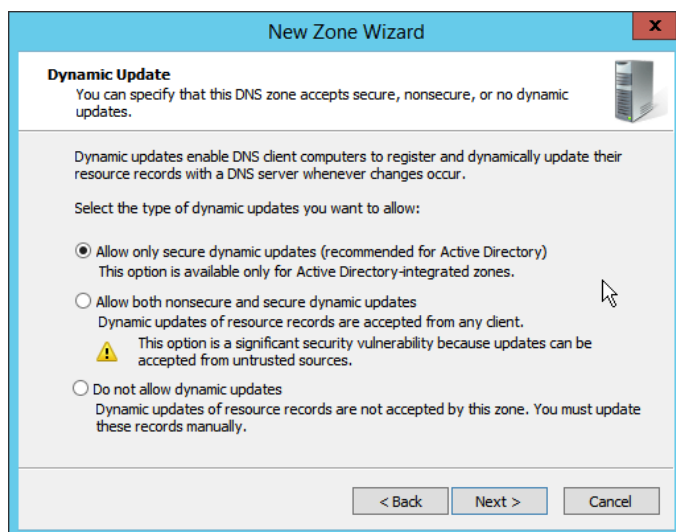
6. Click **Next**.



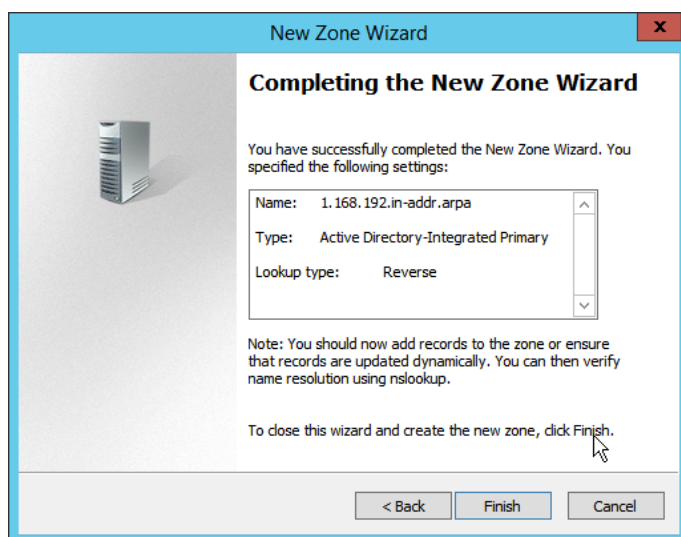
7. Click **Next**.
8. Enter the first three parts of the IP address of the Active Directory (AD)/DNS server (for example, 192.168.1).



9. Click **Next**.



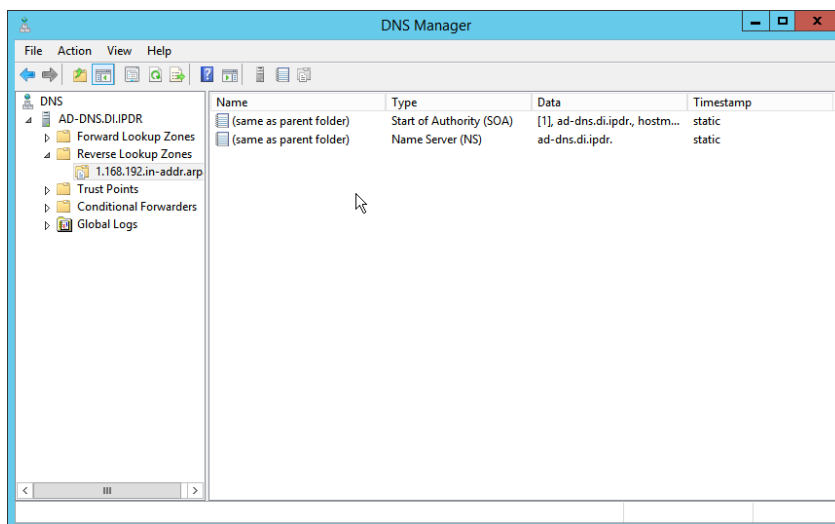
10. Click **Next**.



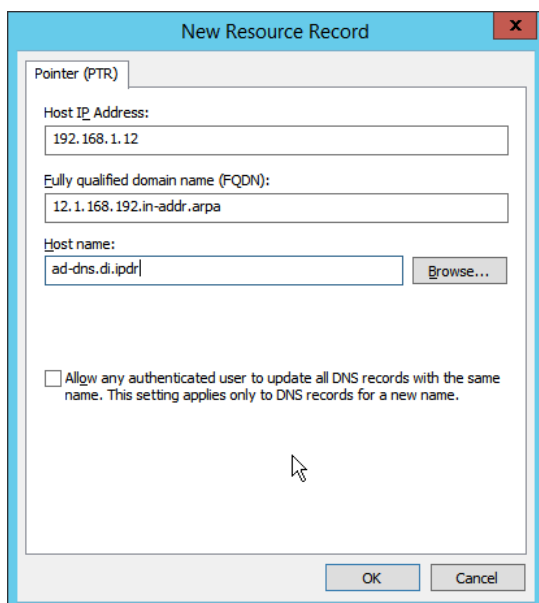
11. Click **Finish**.

12. Click on the newly created reverse lookup zone.

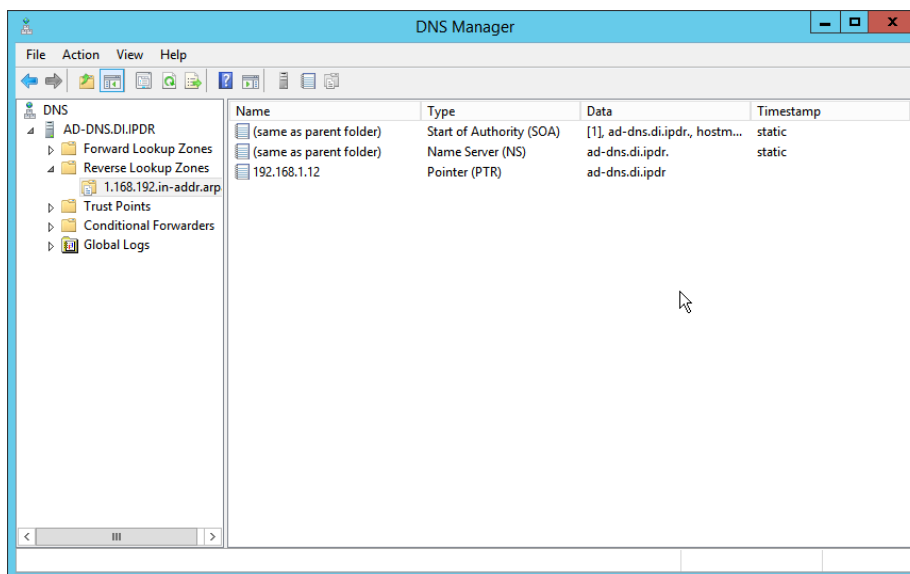




13. Right-click in the window and select **New Pointer (PTR)....**
14. Enter the **IP address** of the AD/DNS server.
15. Enter the **hostname** of the AD/DNS server.



16. Click **OK**.

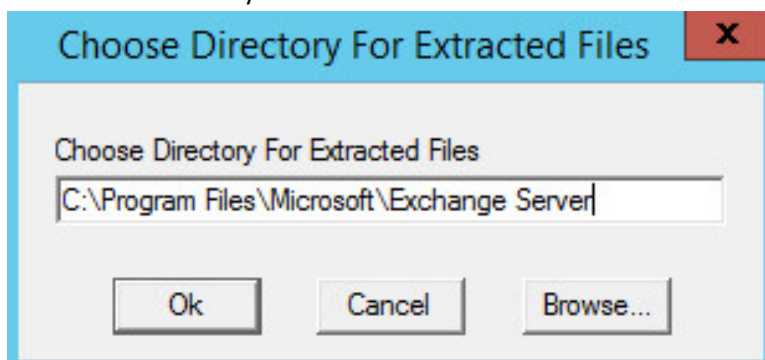


## 2.2 Microsoft Exchange Server

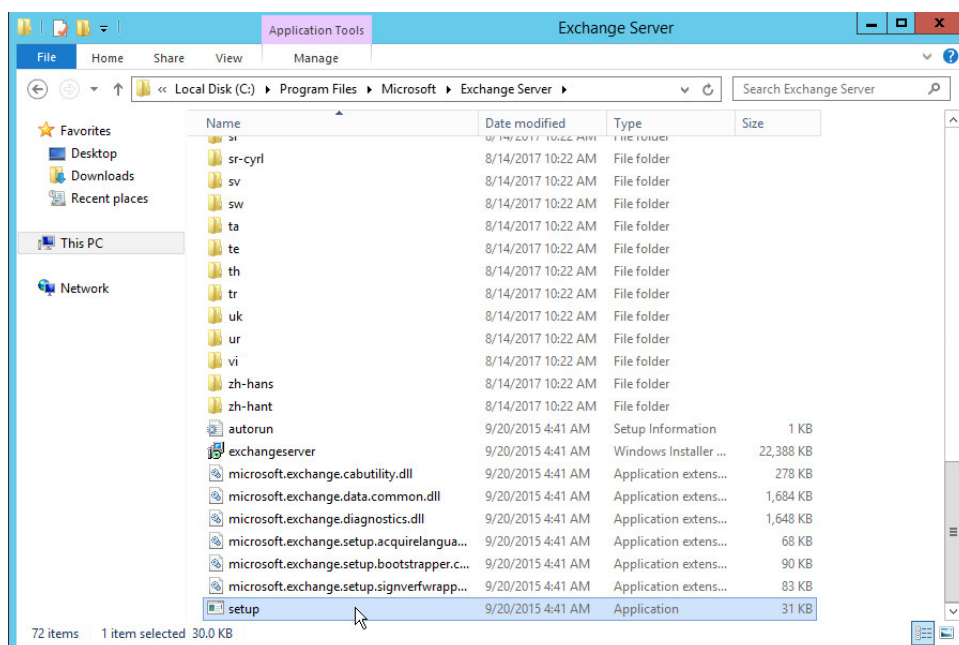
As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

### 2.2.1 Install Microsoft Exchange

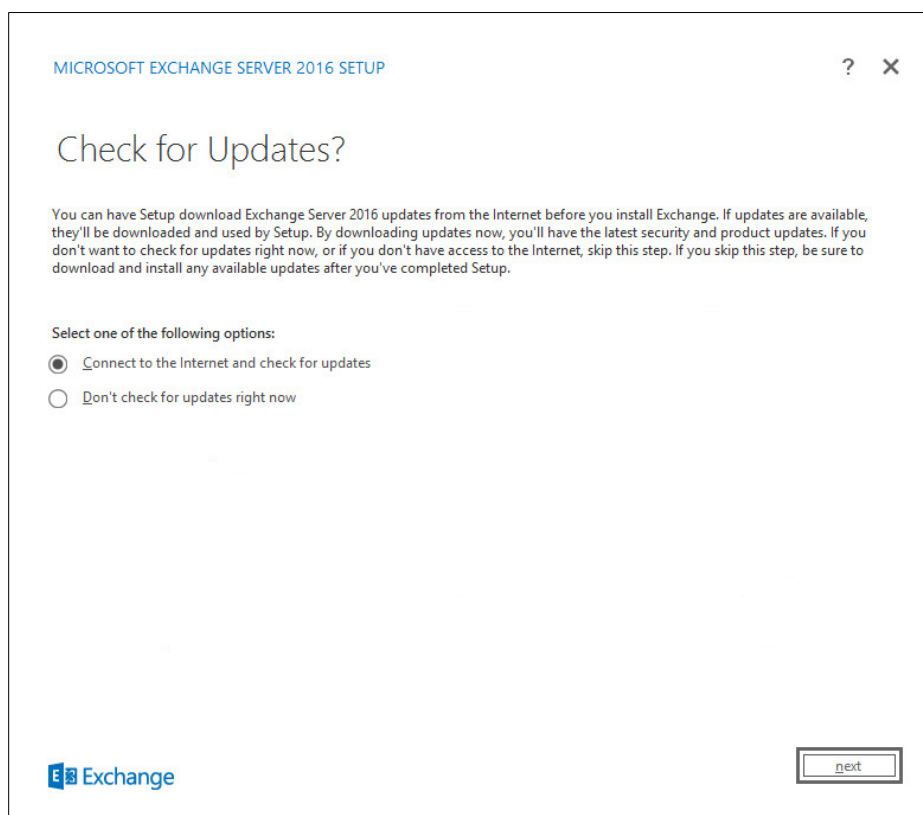
1. Run **Exchange2016-x64.exe**.
2. Choose the directory for the extracted files.



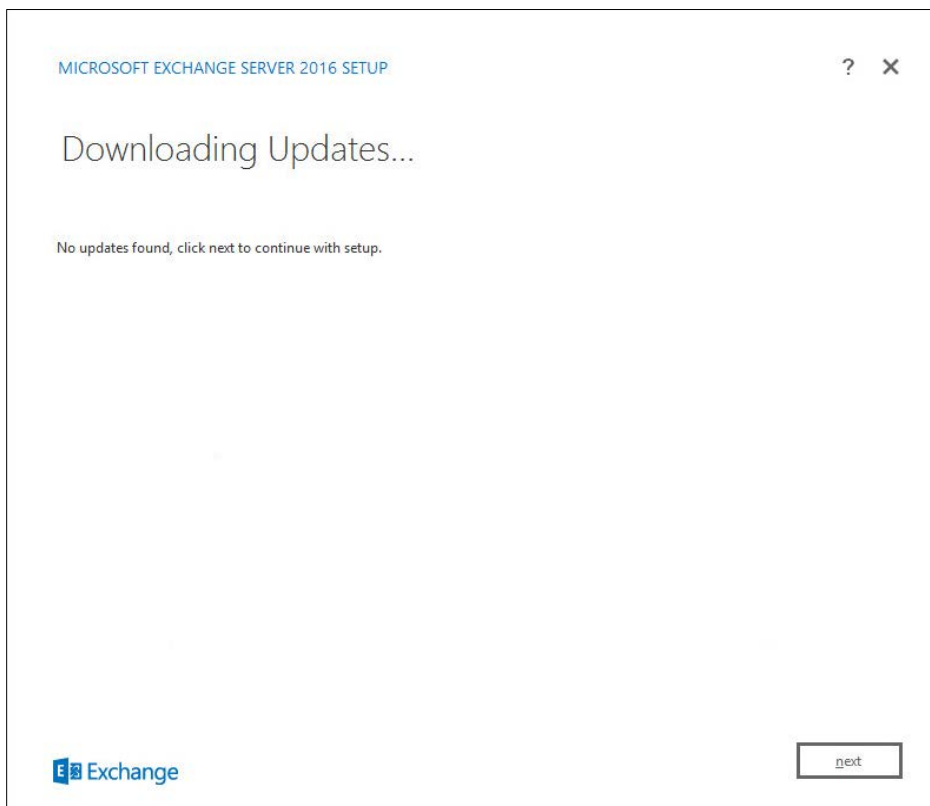
3. Click **OK**.



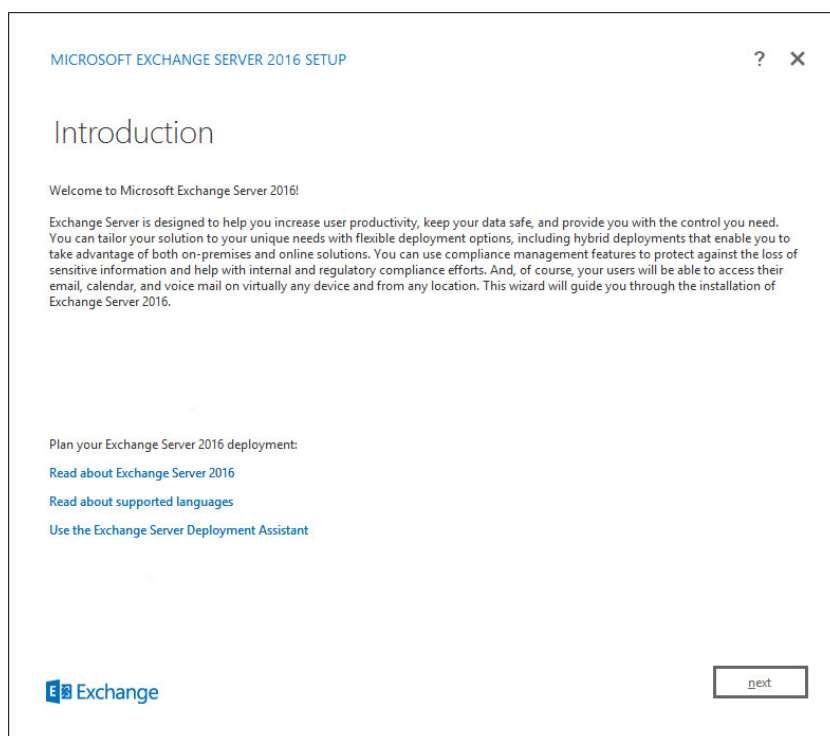
4. Enter the directory and run **setup.exe**.
5. Select **Connect to the Internet and check for updates**.



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



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



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

## License Agreement

Please read and accept the Exchange Server 2016 license agreement.

### MICROSOFT SOFTWARE LICENSE TERMS

#### MICROSOFT EXCHANGE SERVER 2016 STANDARD, ENTERPRISE, TRIAL AND HYBRID

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

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

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

**By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit.** If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate or its agent nearest you for information about Microsoft refund policies. For

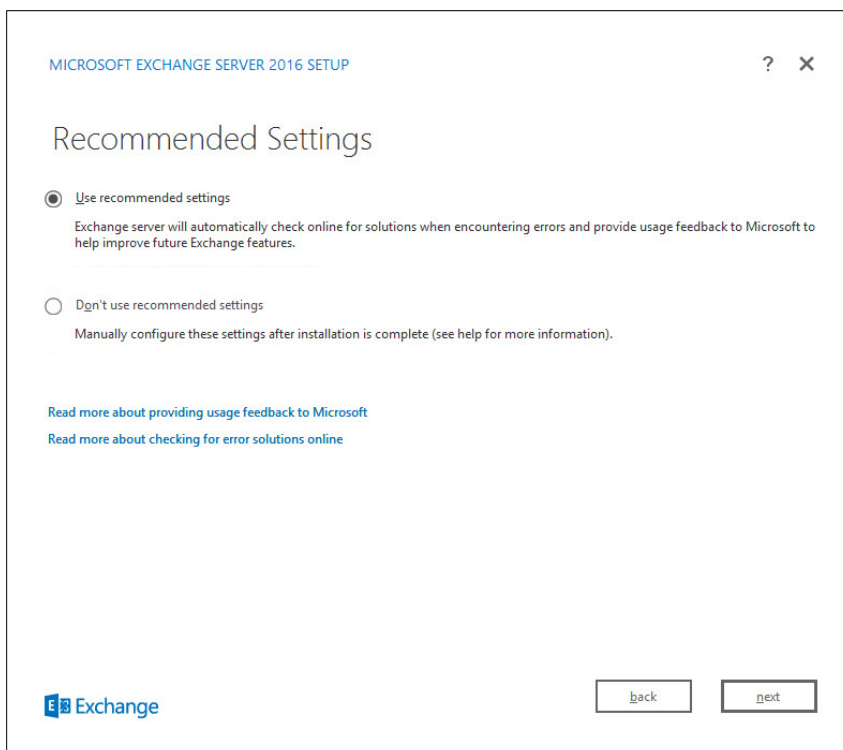
- ☒ I accept the terms in the license agreement
- ☐ I do not accept the terms in the license agreement.



next

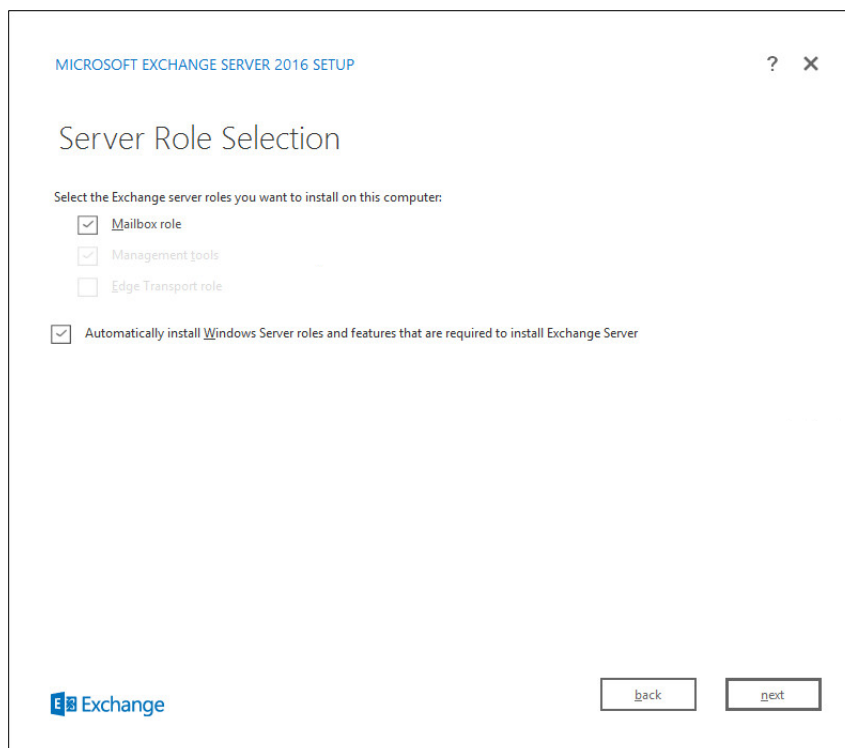
12. Click **Next**.

13. Click **Use Recommended Settings**.



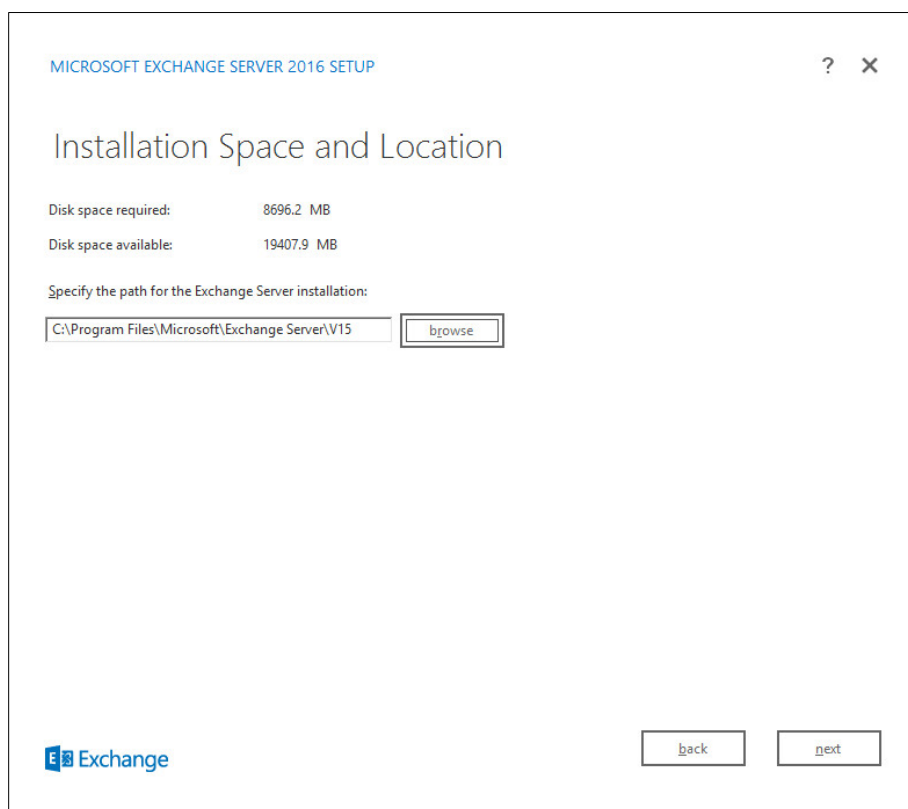
14. Click **Next**.
15. Check **Mailbox role**.
16. Check **Automatically install Windows Server roles and features that are required to install Exchange Server**.





17. Click **Next**.

18. Specify the installation path for MS Exchange.



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

## Exchange Organization

Specify the name for this Exchange organization:

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

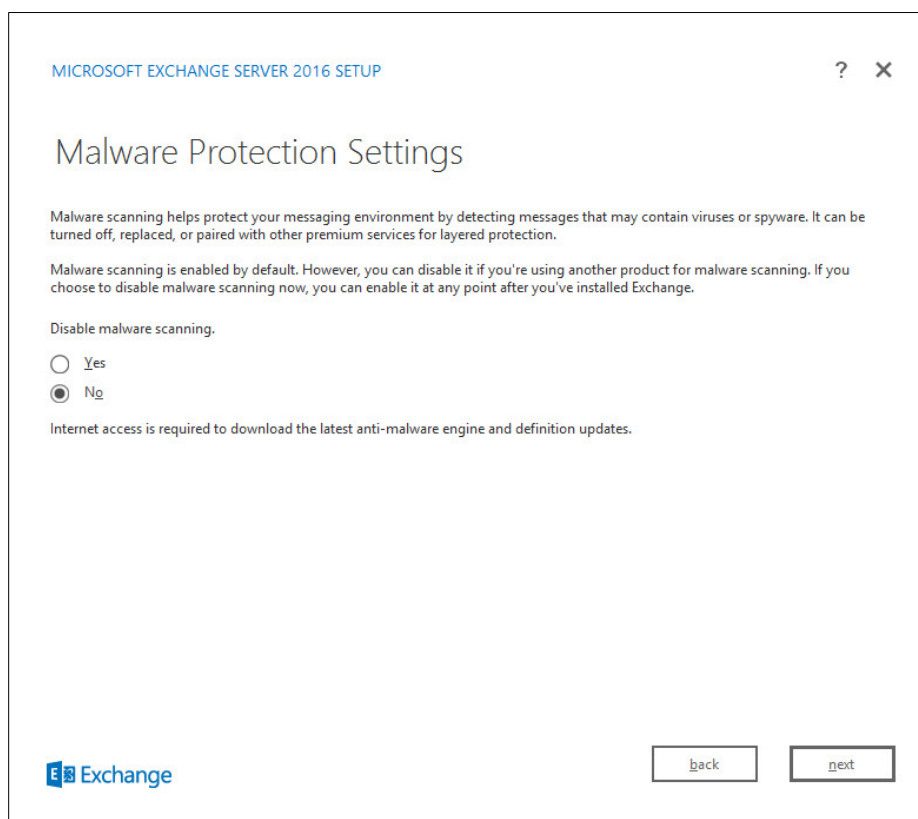
The Active Directory split permissions security model is typically used by large organizations that completely separate the responsibility for the management of Exchange and Active Directory among different groups of people. Applying this security model removes the ability for Exchange servers and administrators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

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

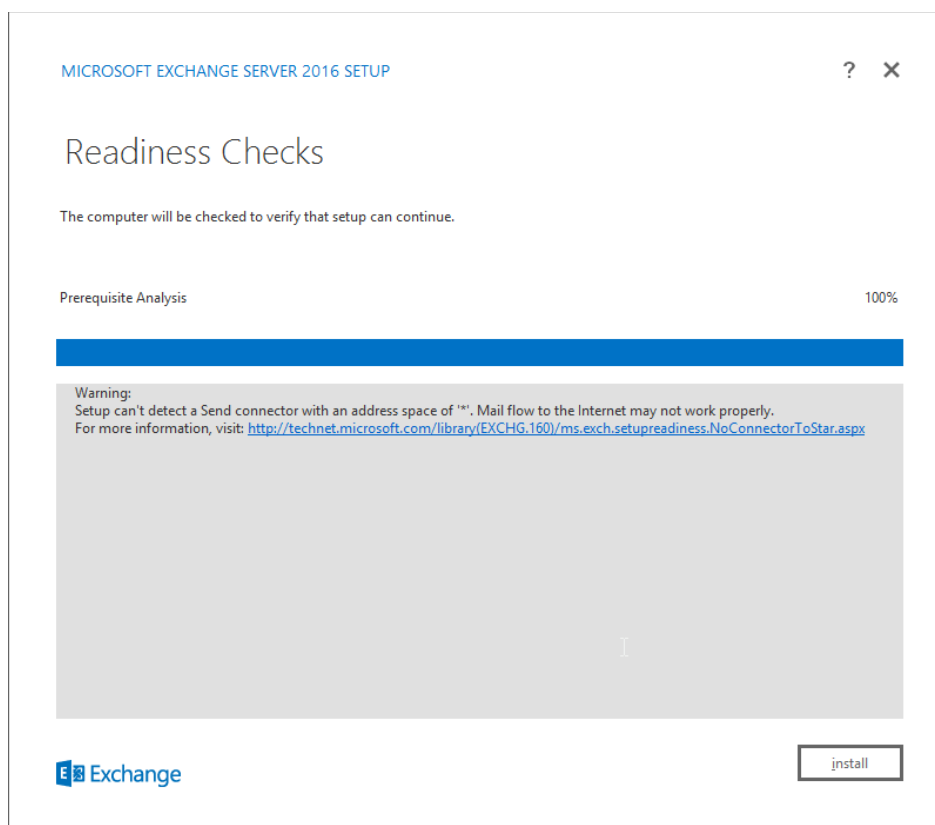
[back](#)[next](#)

22. Click **Next**.

23. Select **No**.



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



27. Click **Install**.

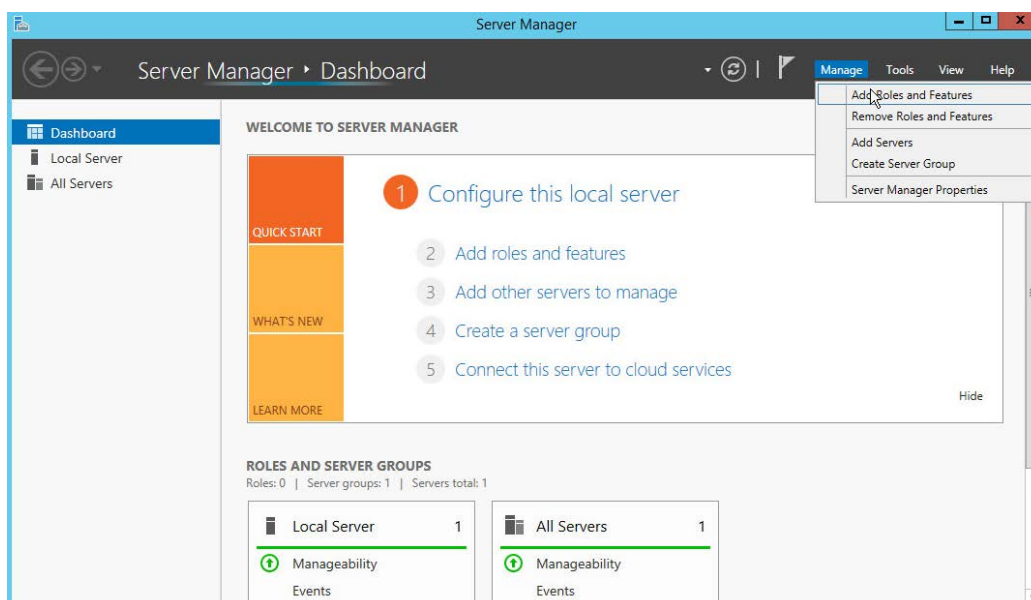
## 2.3 Windows Server Hyper-V Role

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

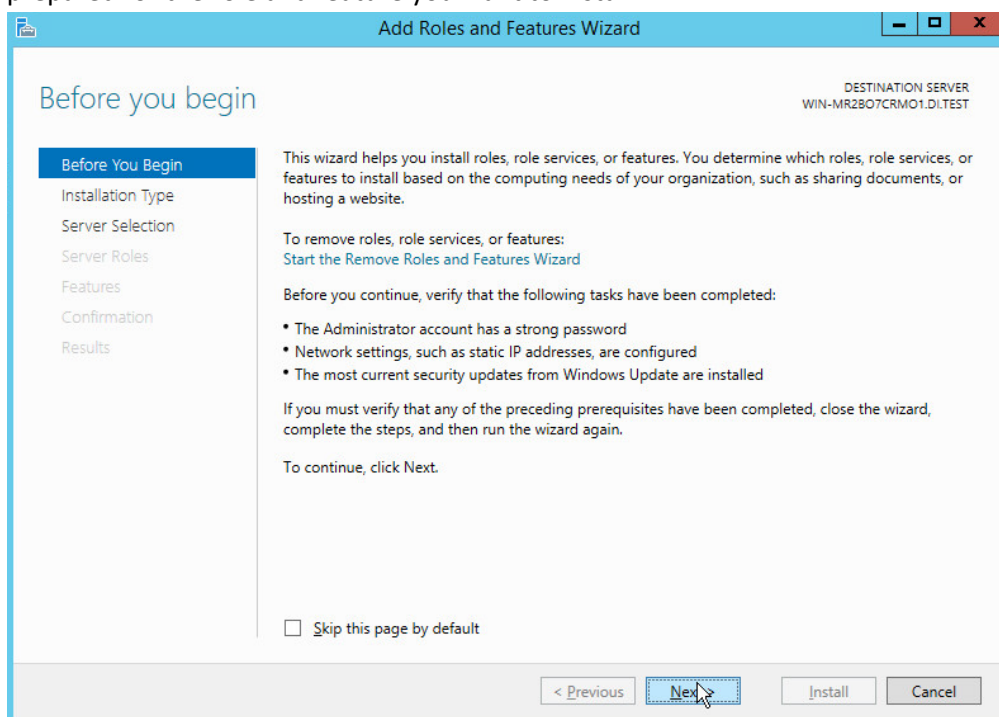
The instructions for enabling the Windows Server Hyper-V Role are retrieved from [https://technet.microsoft.com/en-us/library/hh846766\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx) and are replicated below for preservation and ease of use.

### 2.3.1 Production Installation

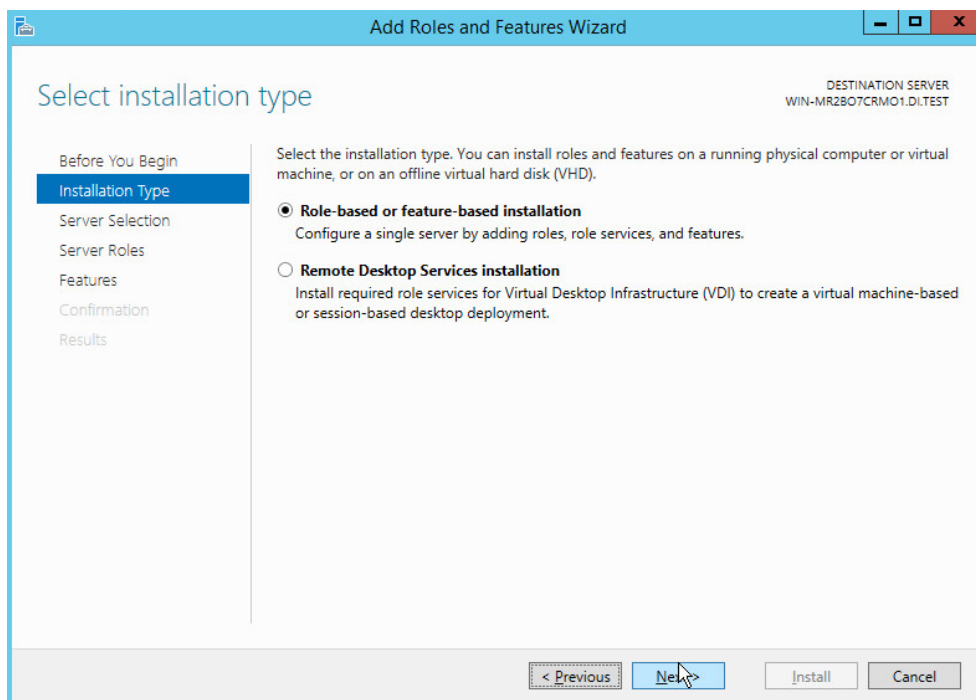
1. In **Server Manager** on the **Manage** menu, click **Add Roles and Features**.



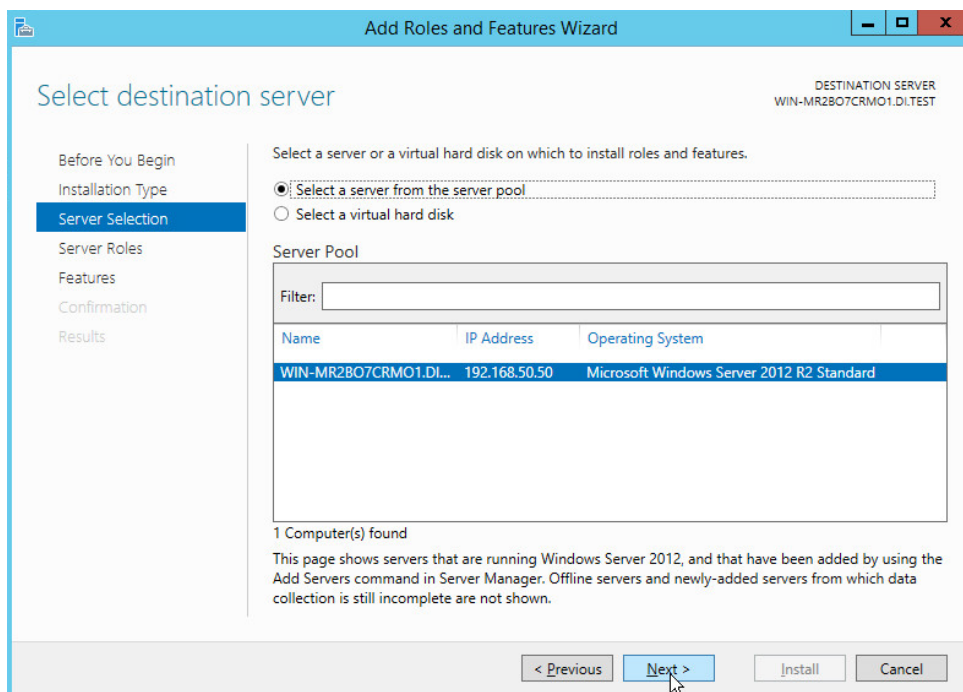
2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.



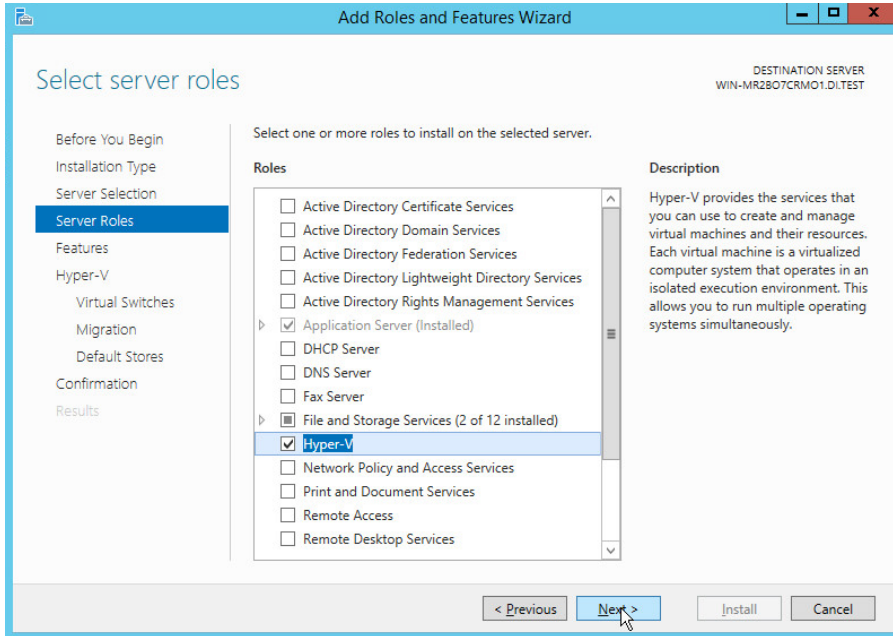
3. Click **Next**.
4. On the **Select installation type** page, select **Role-based or feature-based installation**.



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

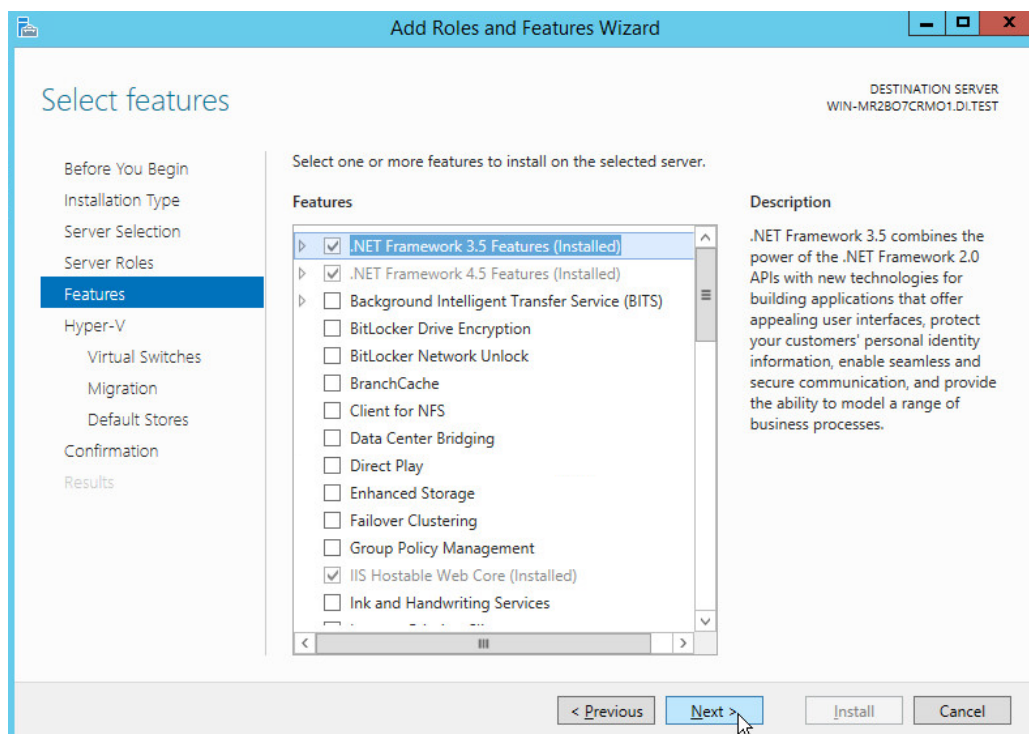


7. Click **Next**.
8. On the **Select server roles** page, select **Hyper-V**.
9. To add the tools that you use to create and manage virtual machines, click **Add Features**.

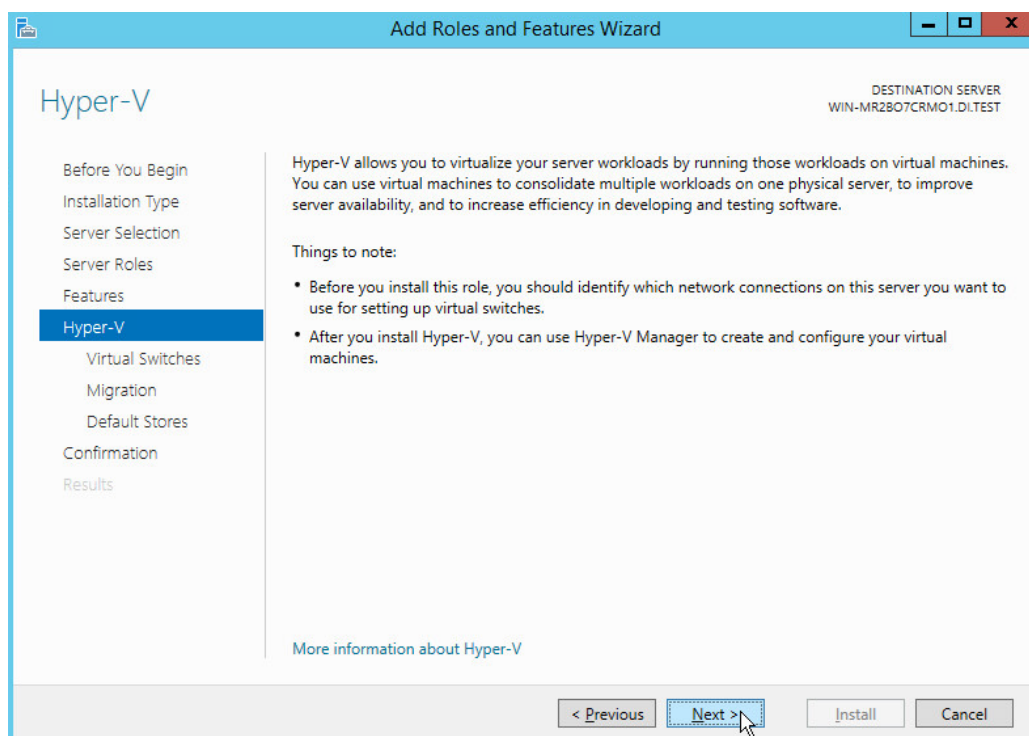


10. Click **Next**.



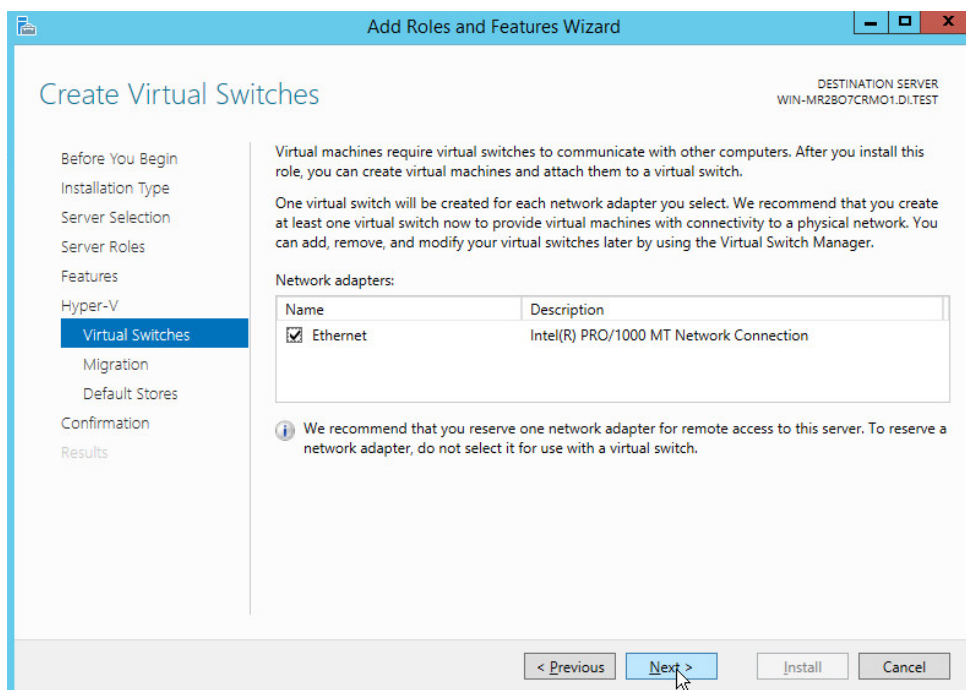


11. Click **Next**.



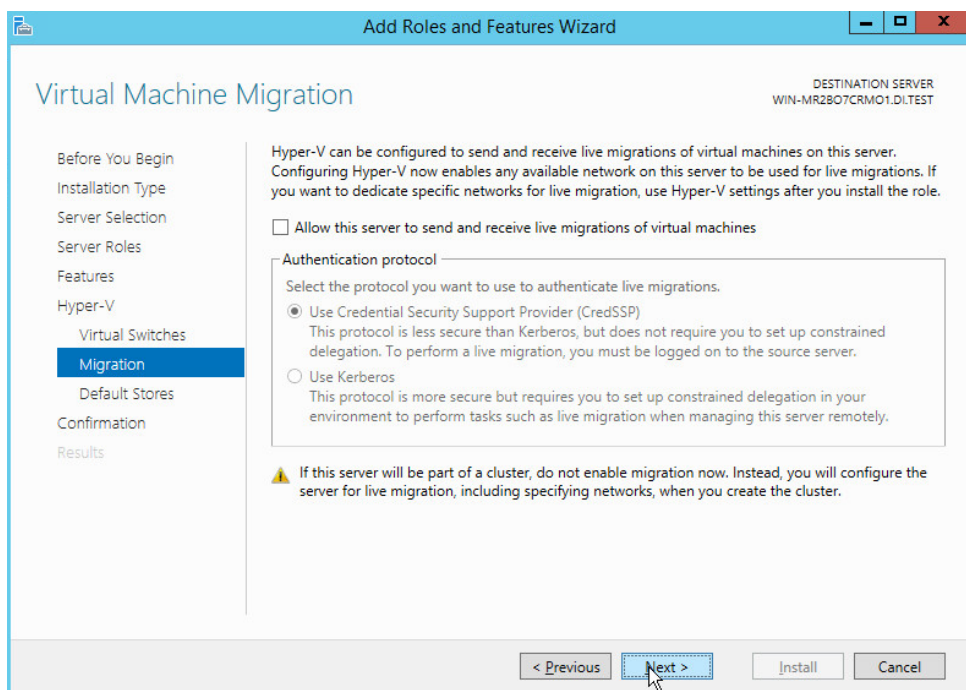
12. Click **Next**.

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



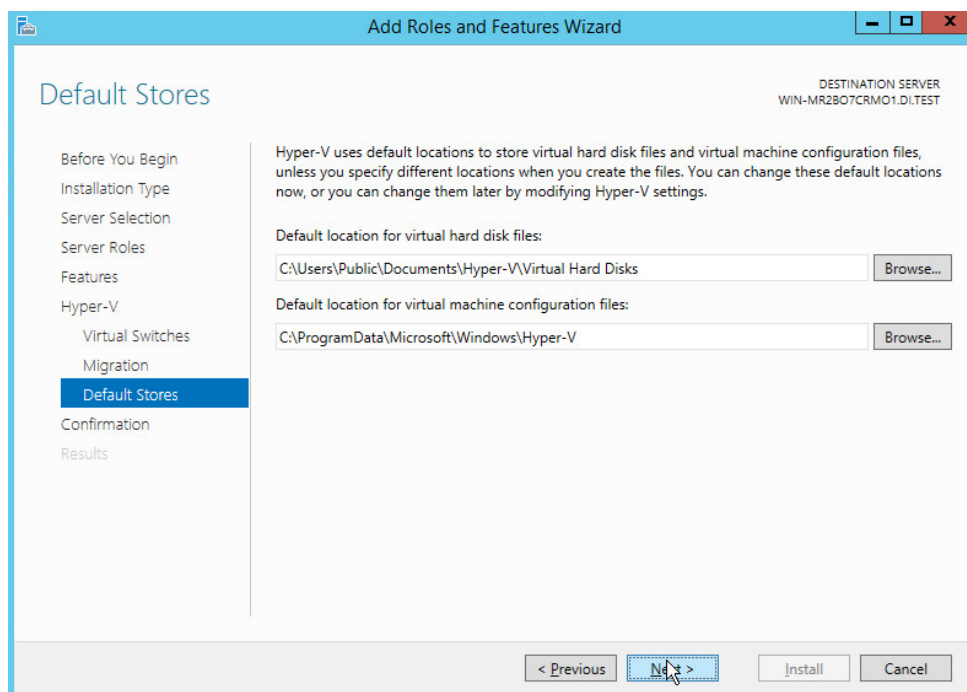
14. Click **Next**.

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



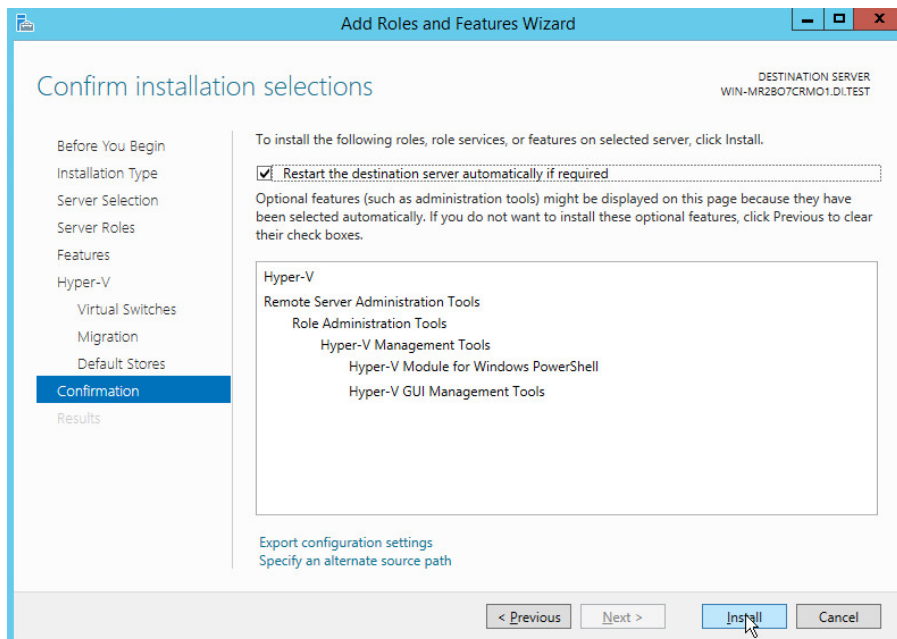
16. Click **Next**.

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



18. Click **Next**.

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



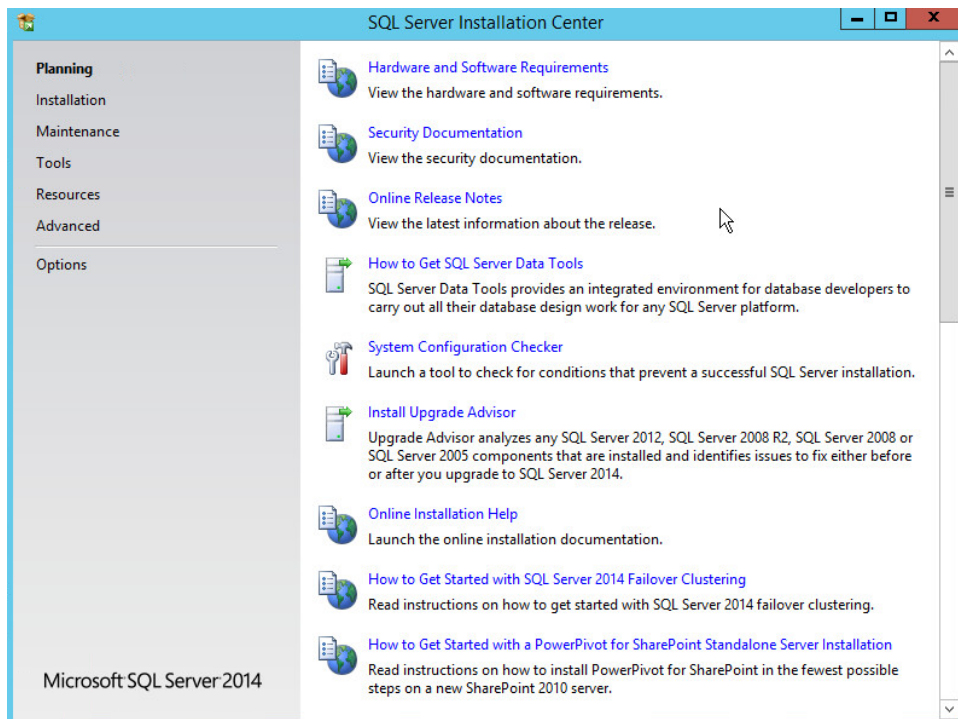
20. Click **Install**.
21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

## 2.4 MS SQL Server

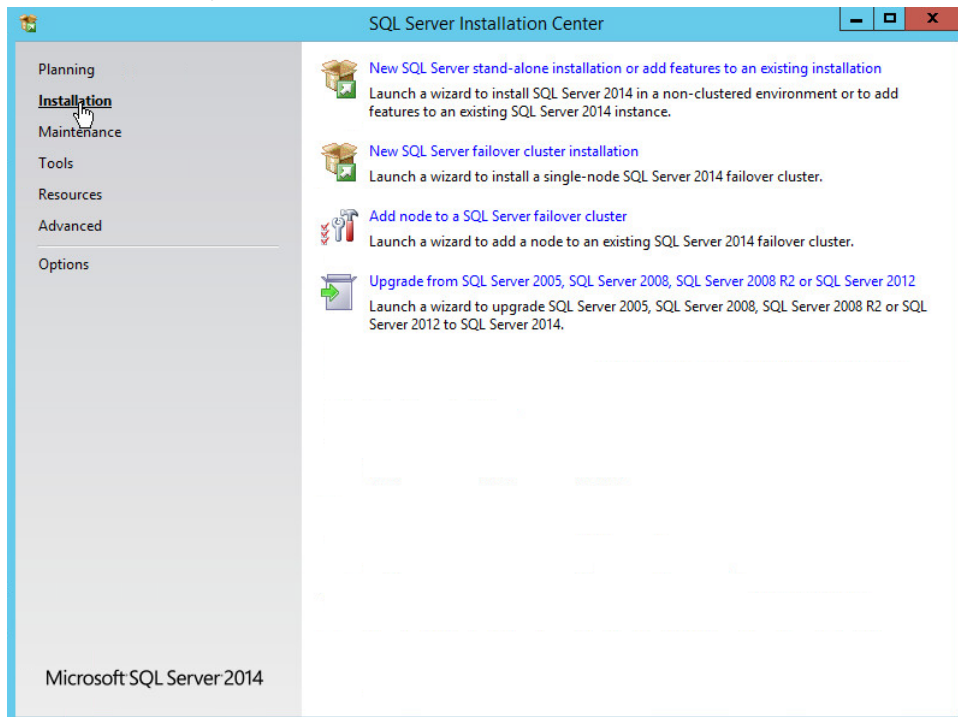
As part of both our enterprise emulation and data integrity solution, we include a Microsoft Structured Query Language (MS SQL) Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

### 2.4.1 Install and Configure MS SQL

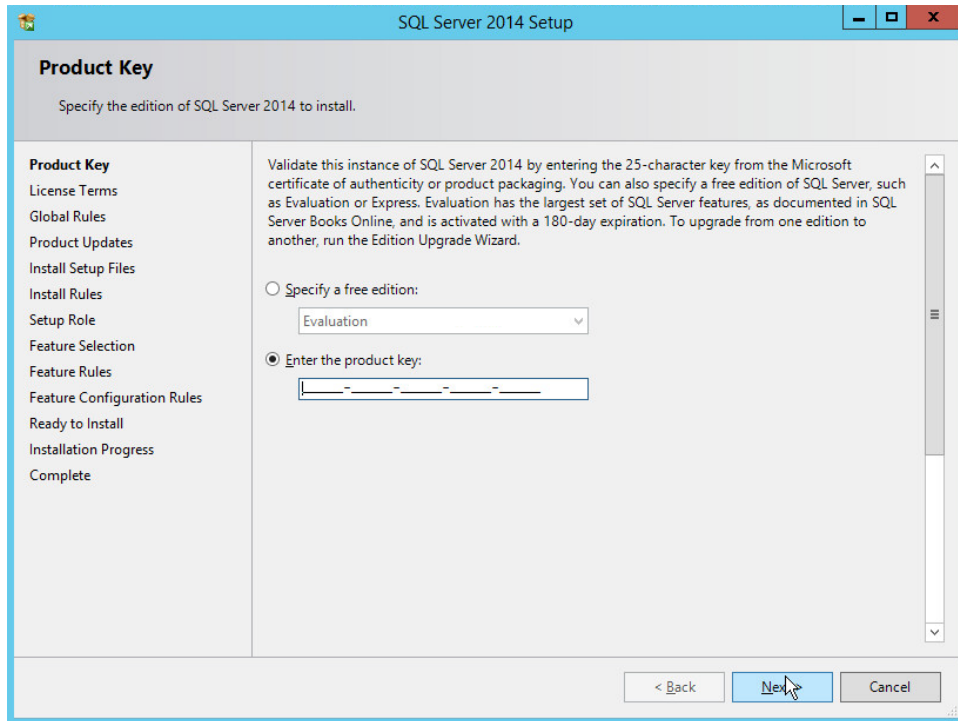
1. Acquire **SQL Server 2014 installation media**.
2. Locate the installation media in the machine and click on **SQL2014\_x64\_ENU** to launch **SQL Server Installation Center**.



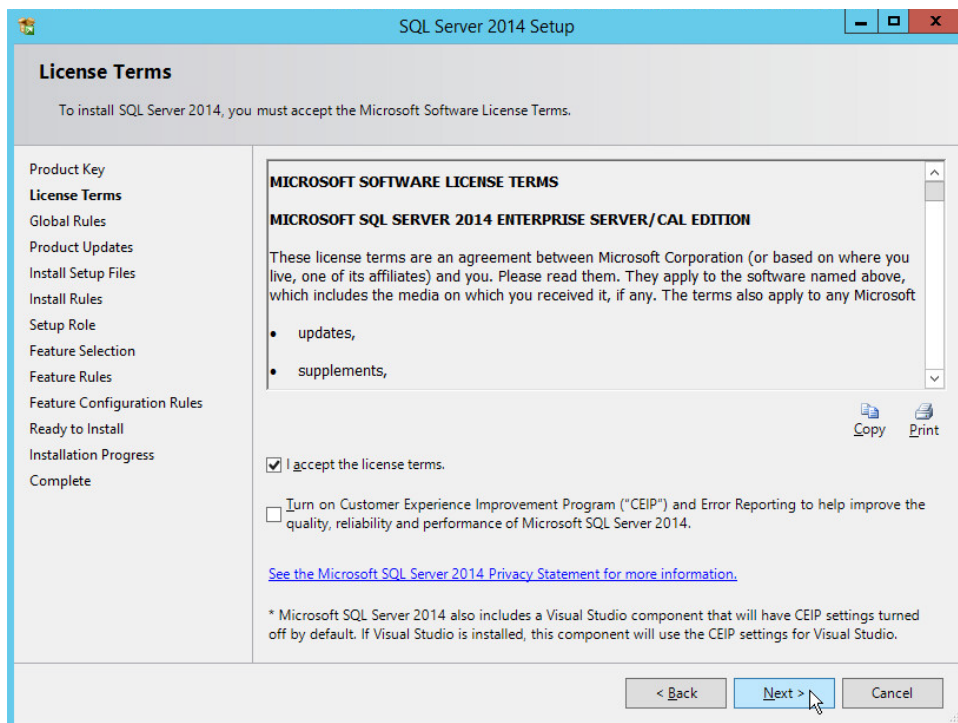
3. On the left menu, select **Installation**.



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

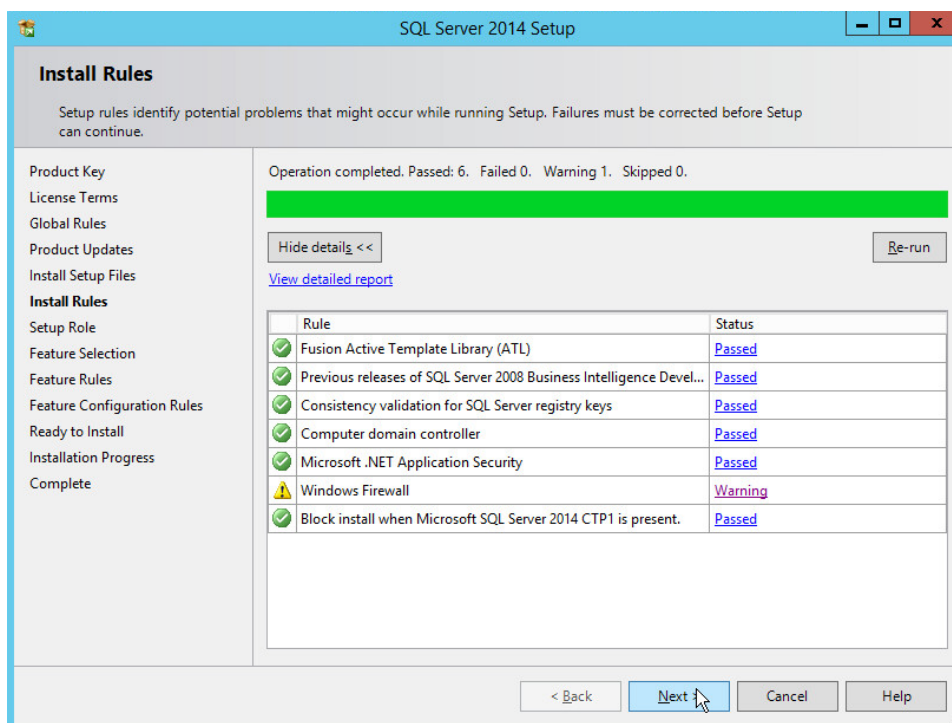


6. Click **Next**.
7. In the **License Terms** section, read and click **I accept the license terms**.



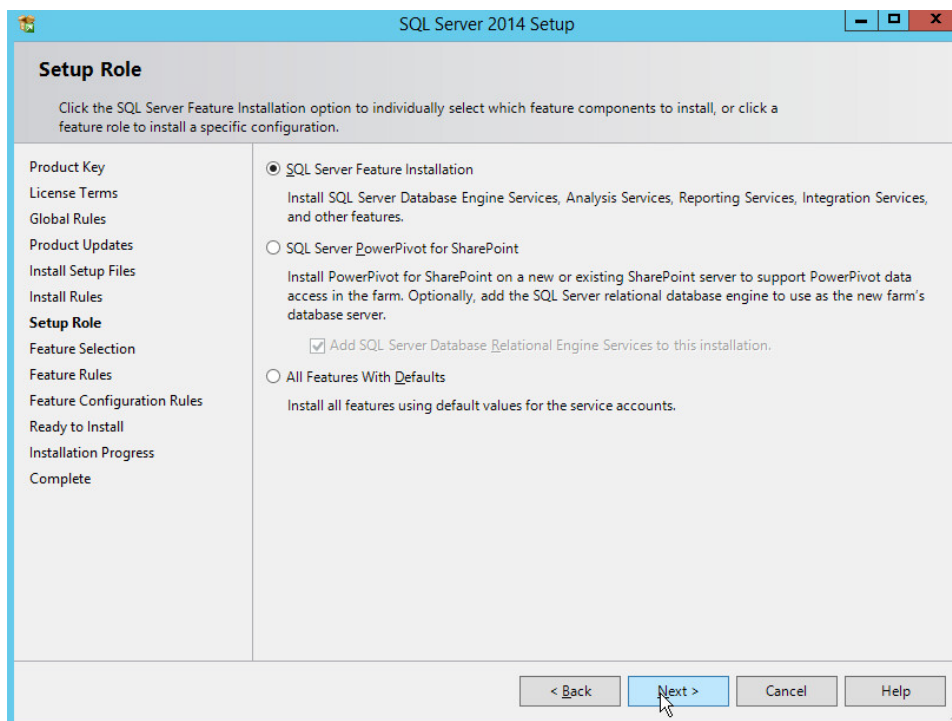
8. Click **Next**.
9. In the **Install Rules** section, note and resolve any further conflicts.





10. Click **Next**.

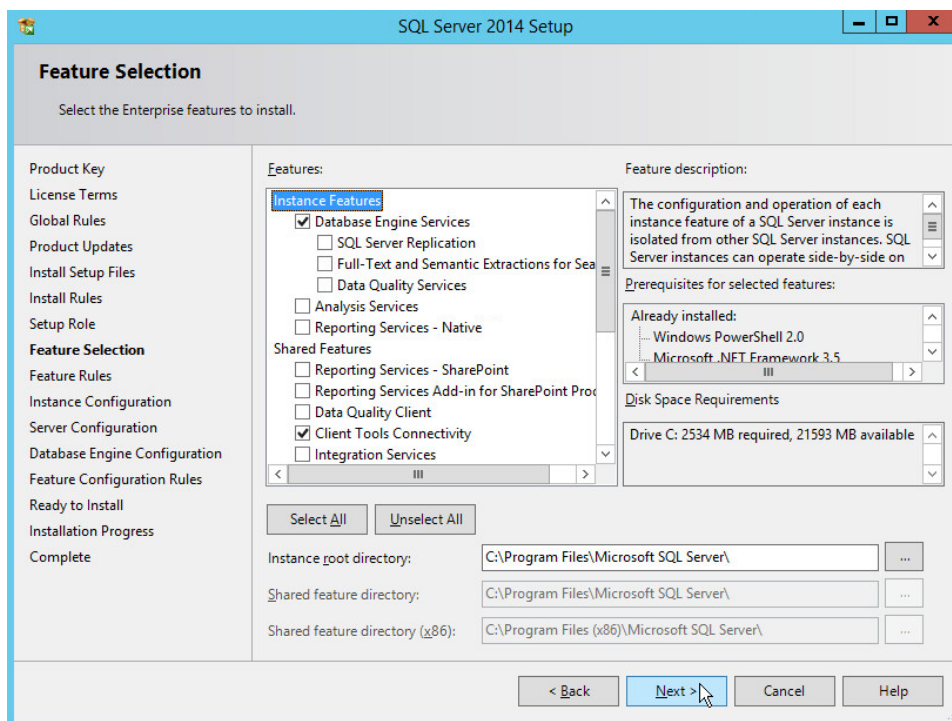
11. In the **Setup Role** section, select **SQL Server Feature Installation**.



12. Click **Next**.

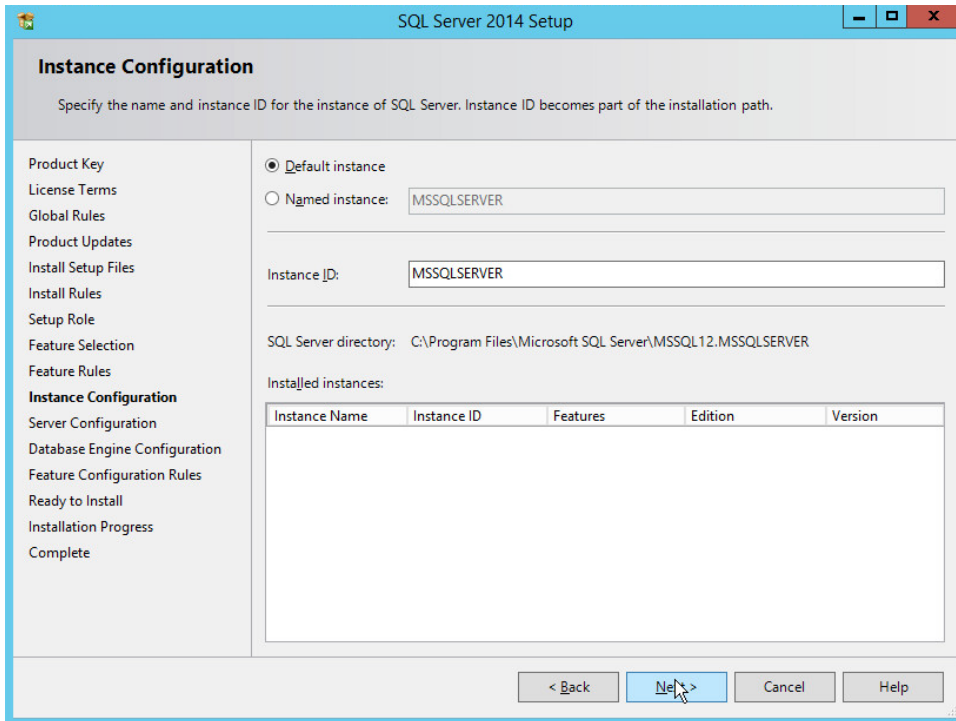
13. In the **Feature Selection** section, select the following options:

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

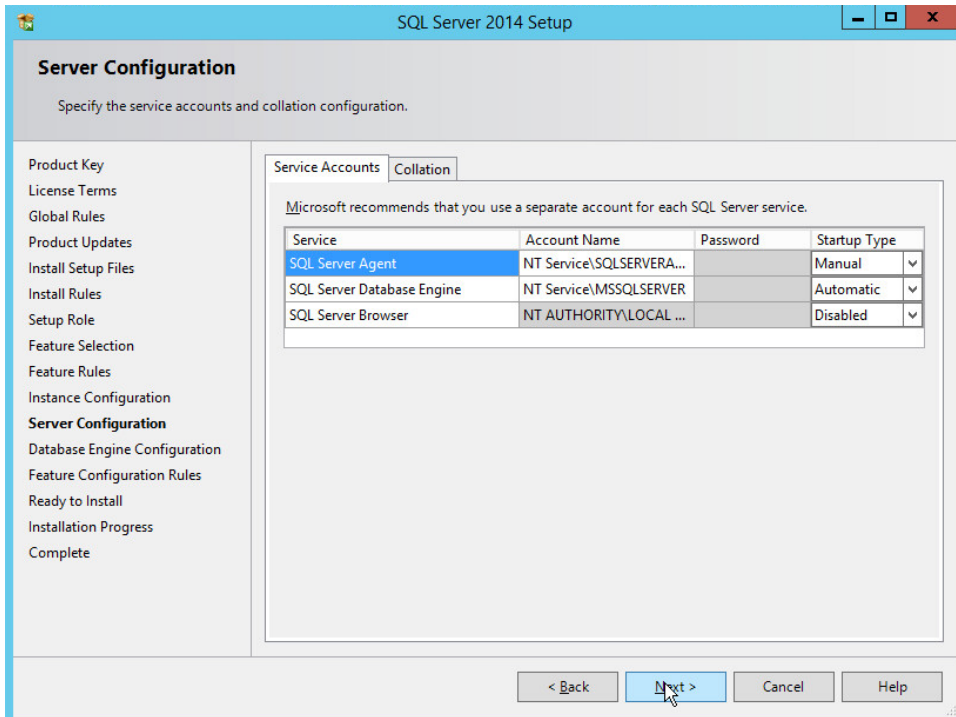


14. Click **Next**.

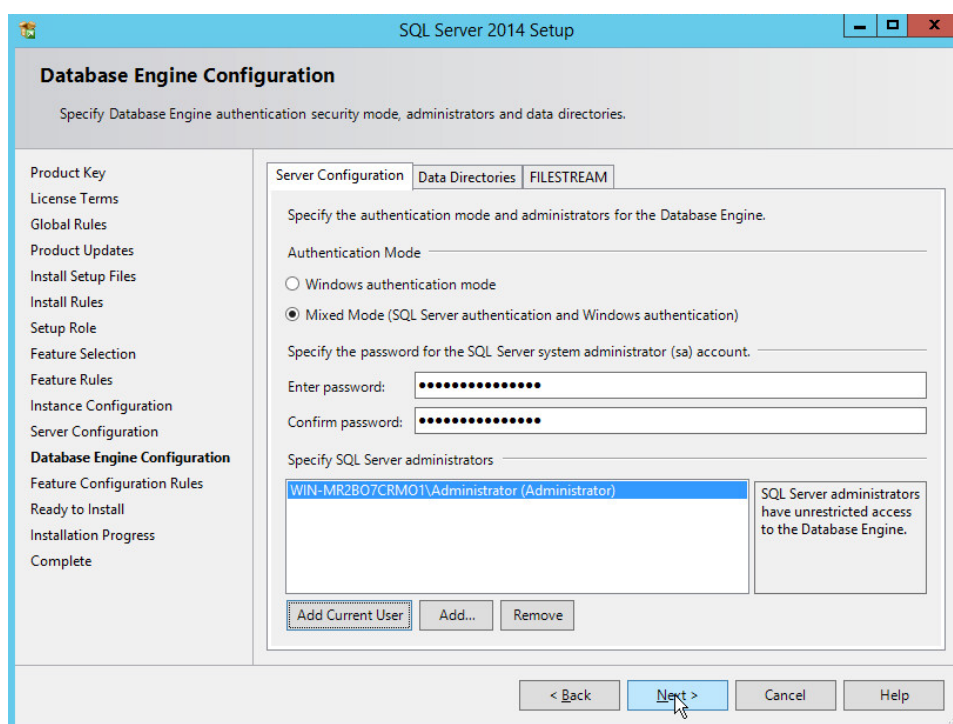
15. In the **Instance Configuration** section, select **Default instance**.



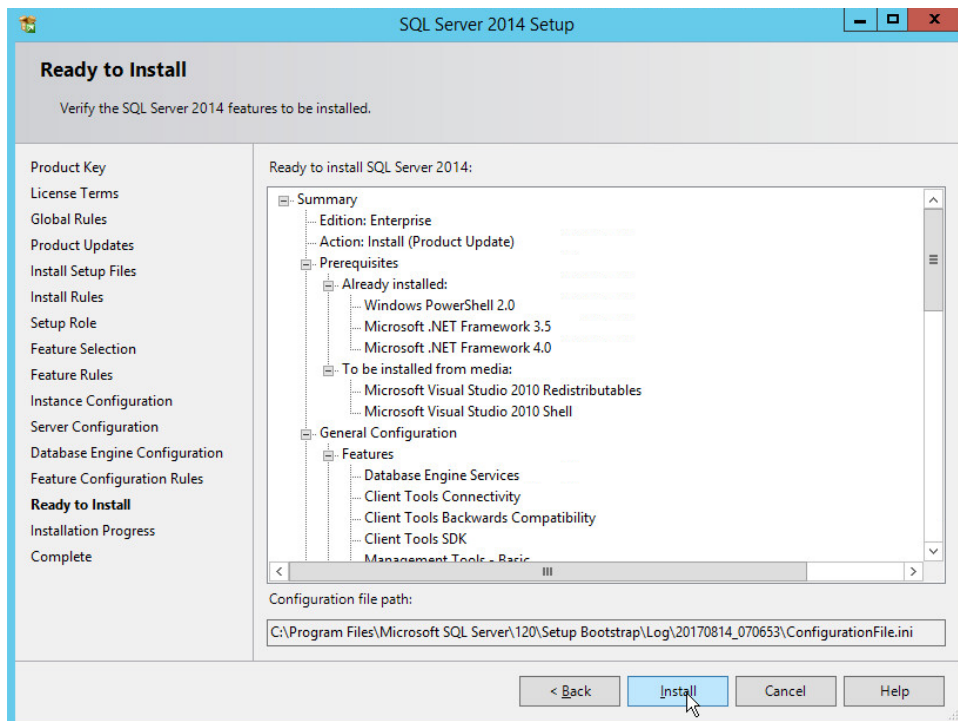
16. Click **Next**.



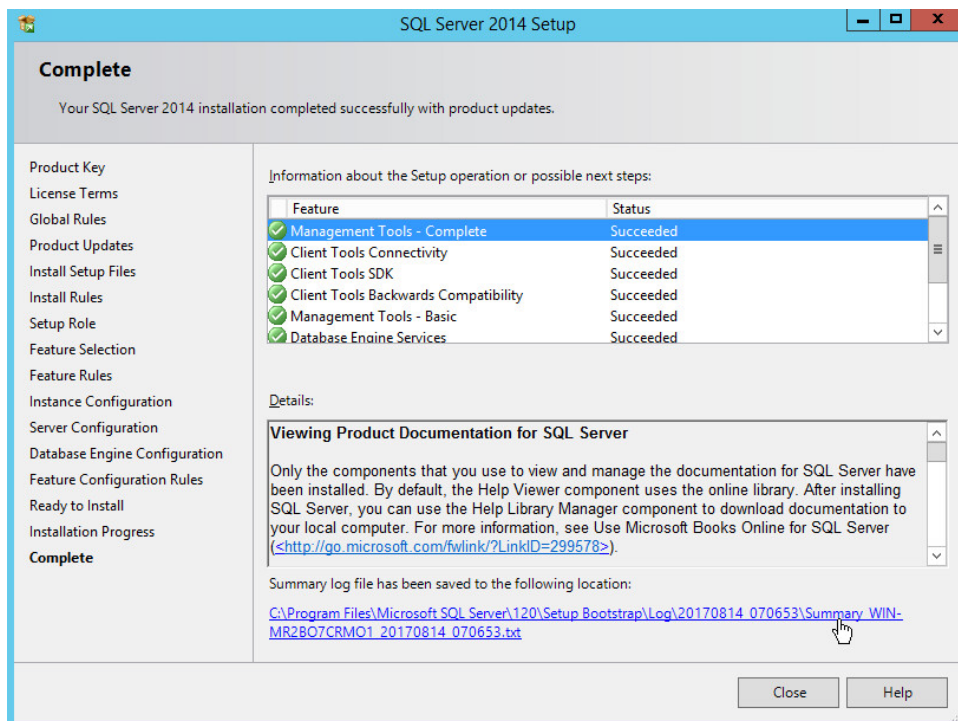
17. In the **Server Configuration** section, click **Next**.
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.
19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User**.
  - a. For Domain accounts,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



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



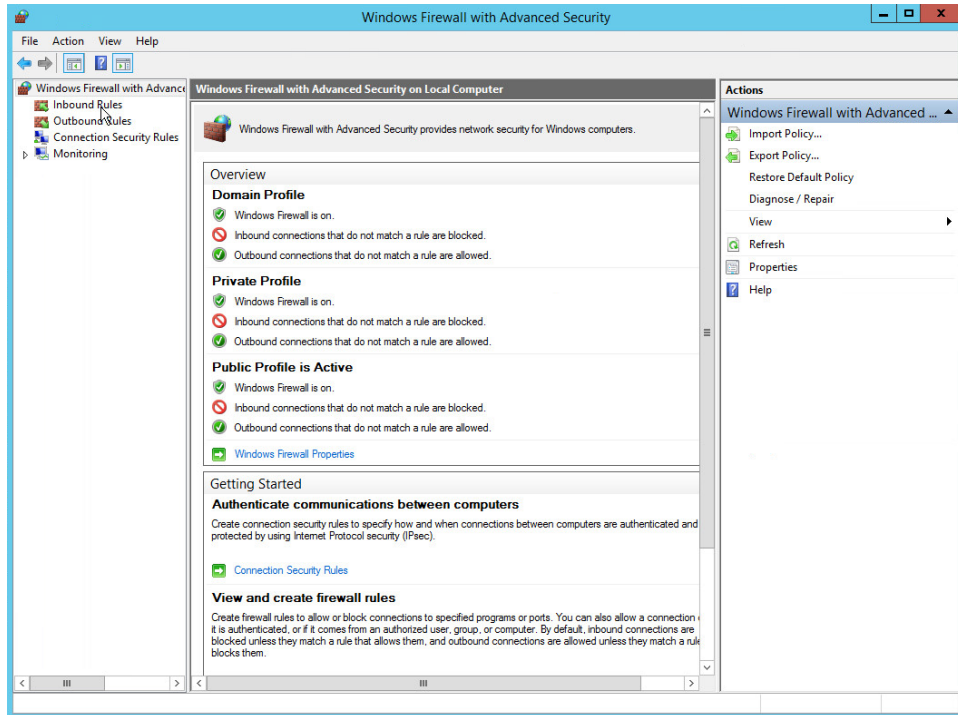
21. Wait for the installation to finish.



22. Click **Close**.

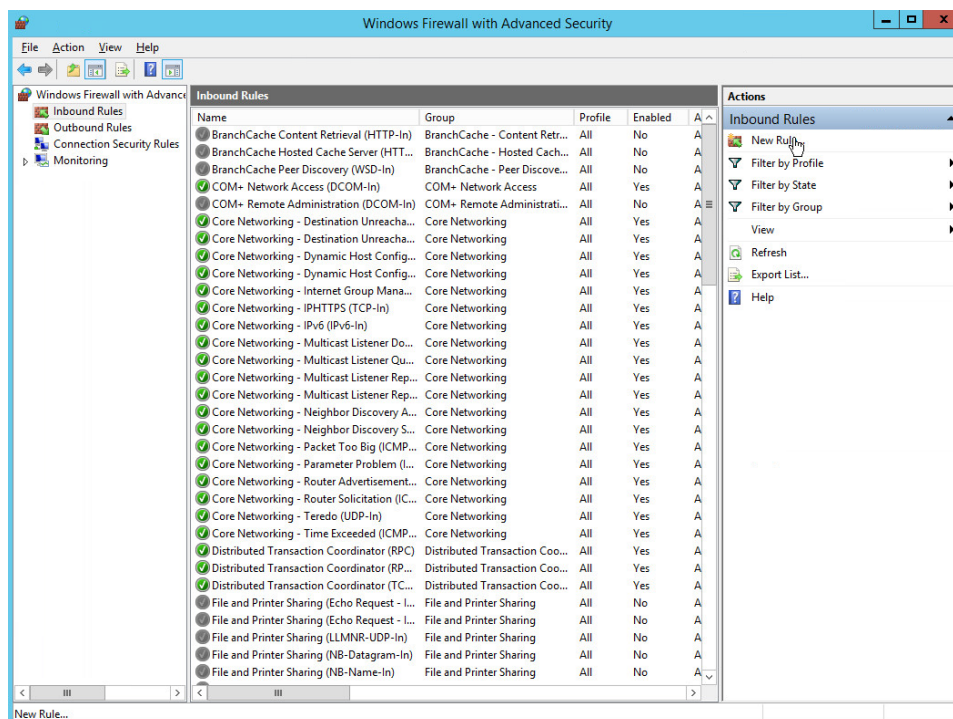
## 2.4.2 Open Port on Firewall

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



2. Click **Inbound Rules**.



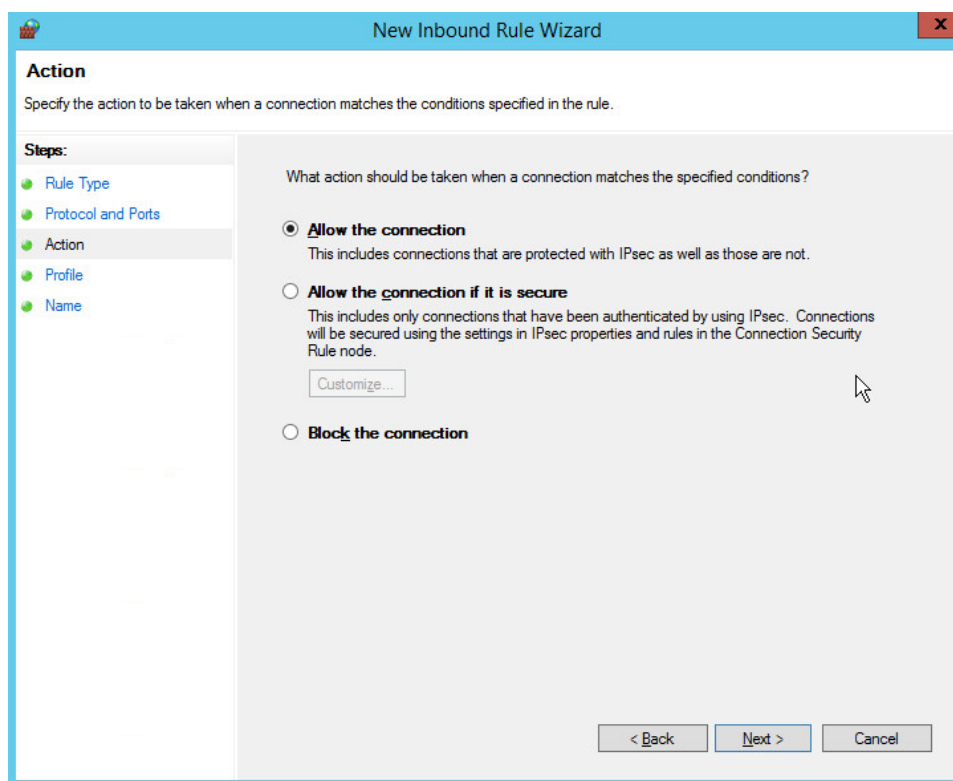


3. Click **New Rule**.
4. Select **Port**.
5. Click **Next**.
6. Select **TCP** and **Specific local ports**.
7. Type **1433** into the text field.

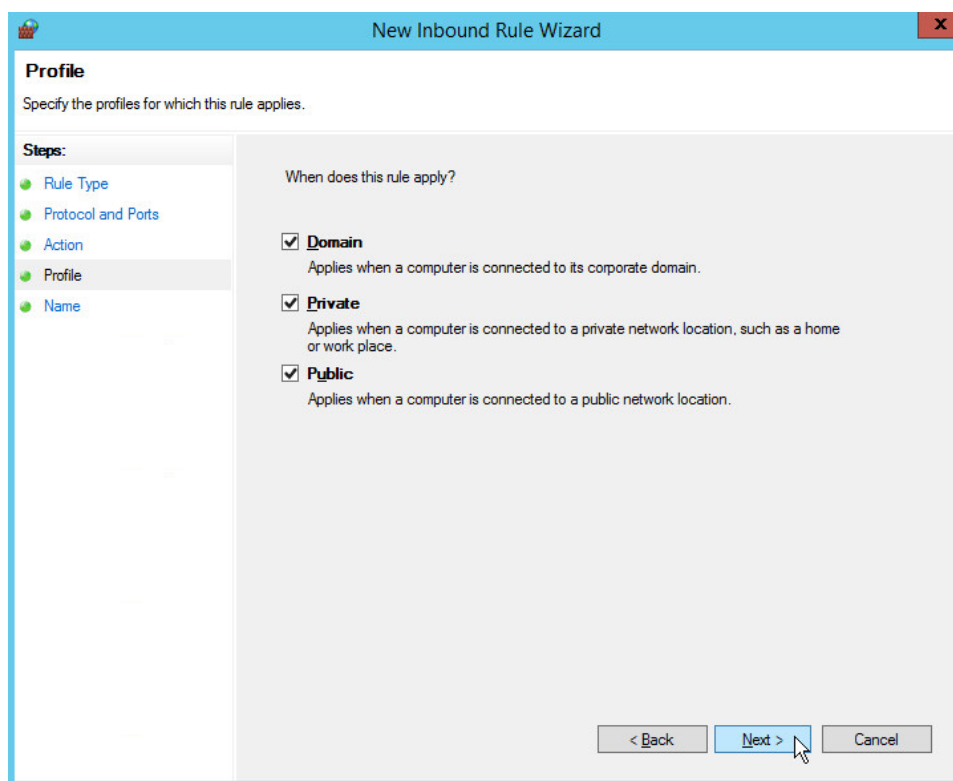


The screenshot shows the 'New Inbound Rule Wizard' window with the title bar 'New Inbound Rule Wizard' and a close button. The main area is titled 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' pane lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main content area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports' (selected). Below the 'Specific local ports' option is a text box containing '1433' and an example text 'Example: 80, 443, 5000-5010'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a mouse cursor), and 'Cancel'.

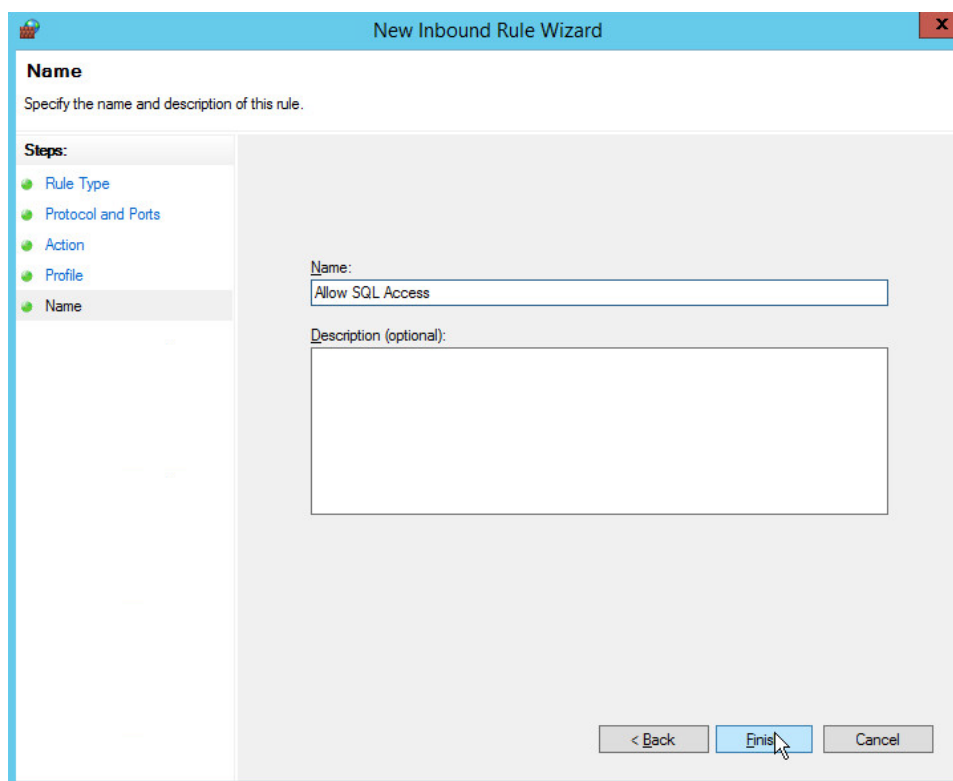
8. Click **Next**.
9. Select **Allow the connection**.



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



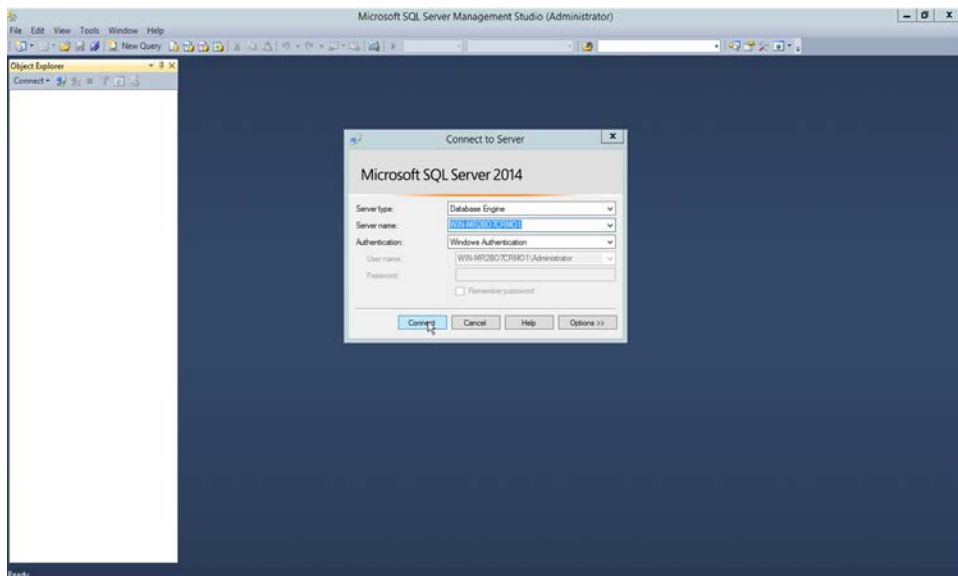
12. Click **Next**.
13. Name the rule **Allow SQL Access**.



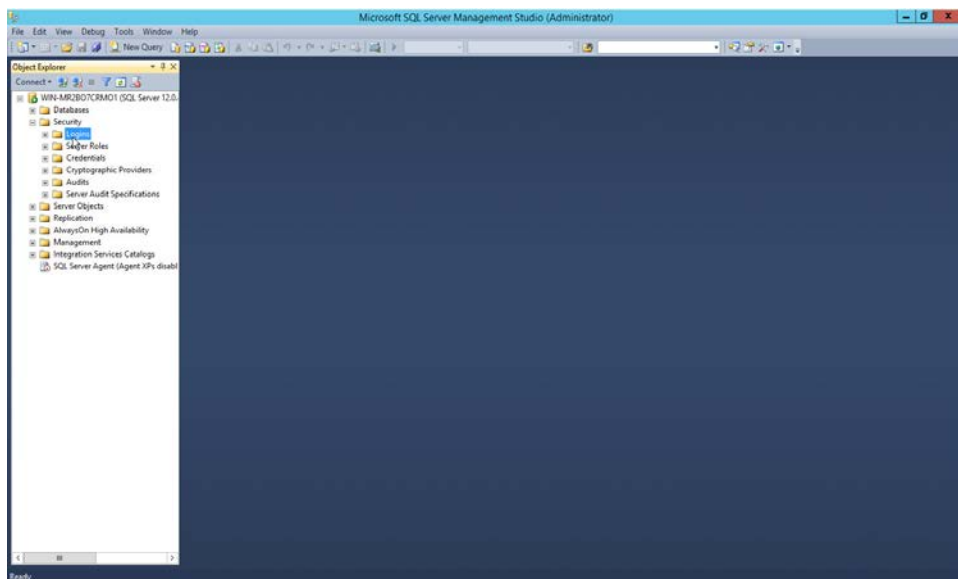
14. Click **Finish**.

### 2.4.3 Add a New Login to the Database

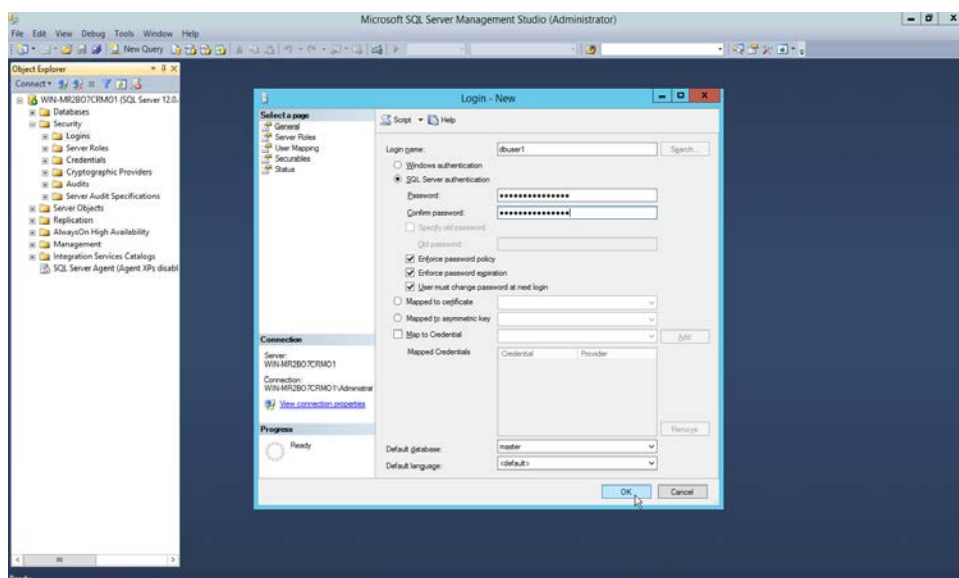
1. Open **SQL Server Management Studio**.



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



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



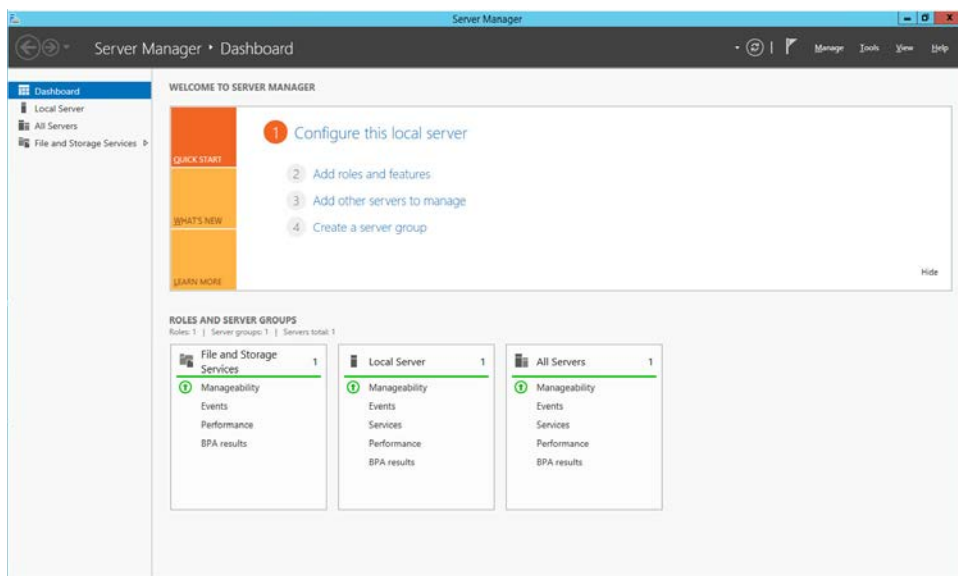
6. Click **OK**.

## 2.5 Microsoft IIS Server

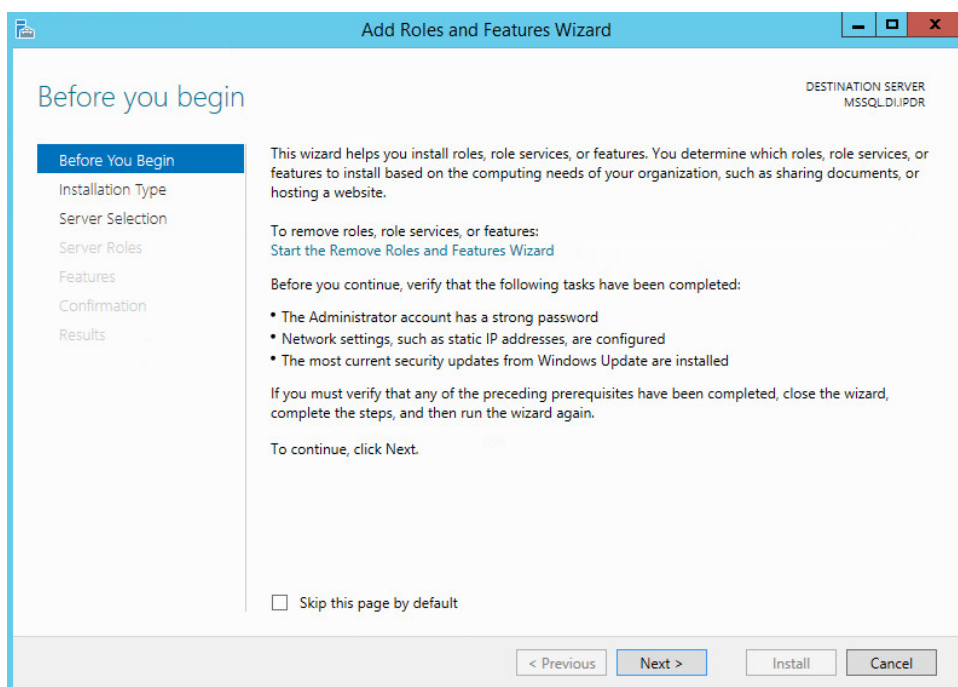
As part of our enterprise emulation, we include a Microsoft Internet Information Services (IIS) server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine. This was conducted on the same machine as in [Section 2.4](#).

### 2.5.1 Install IIS

1. Open **Server Manager**.

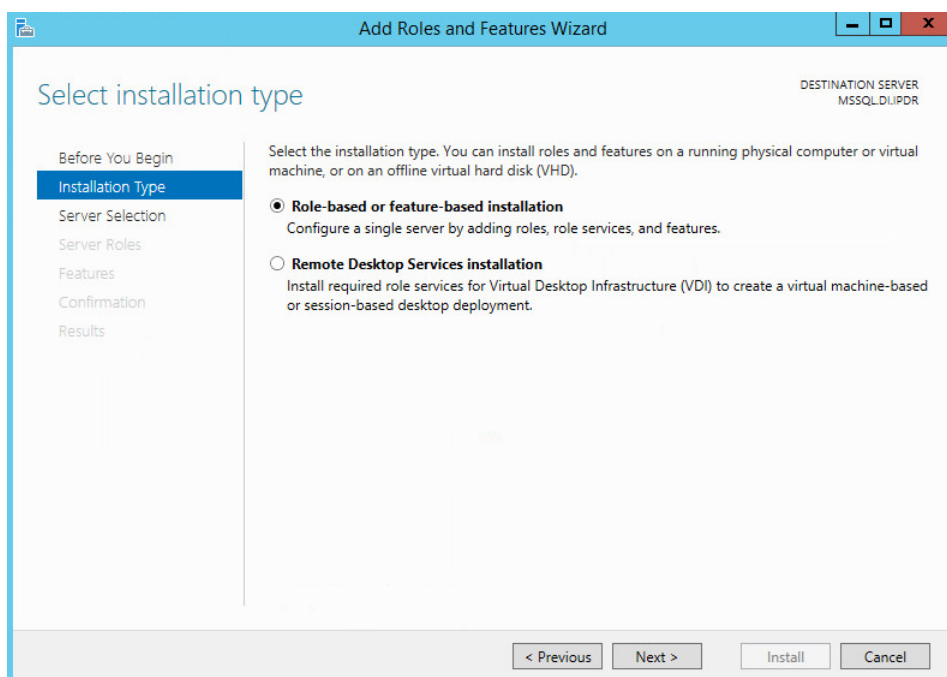


2. Click **Add Roles and Features**.



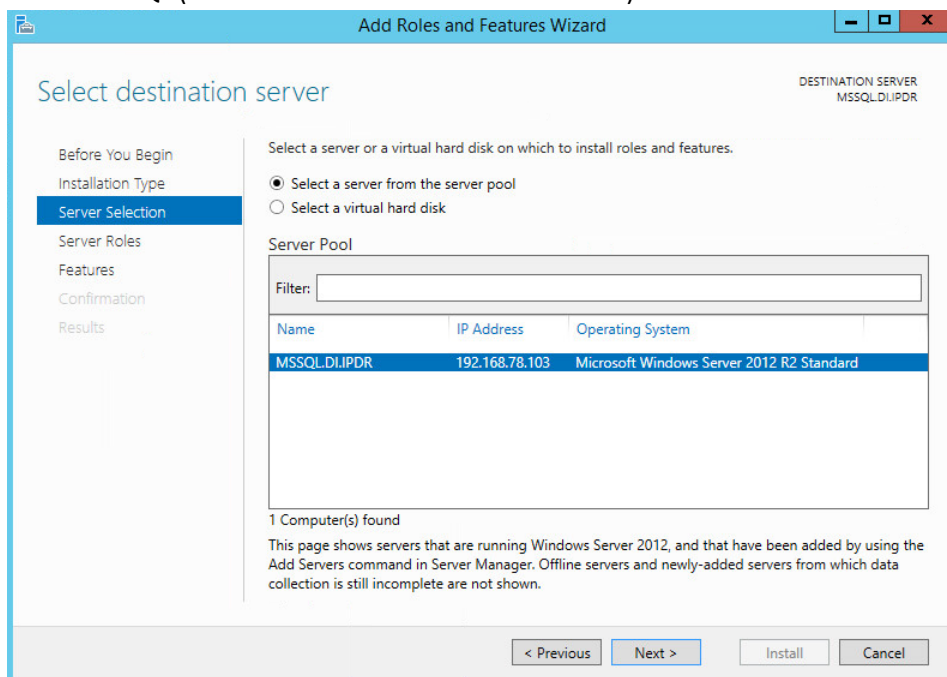
3. Click **Next**.

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



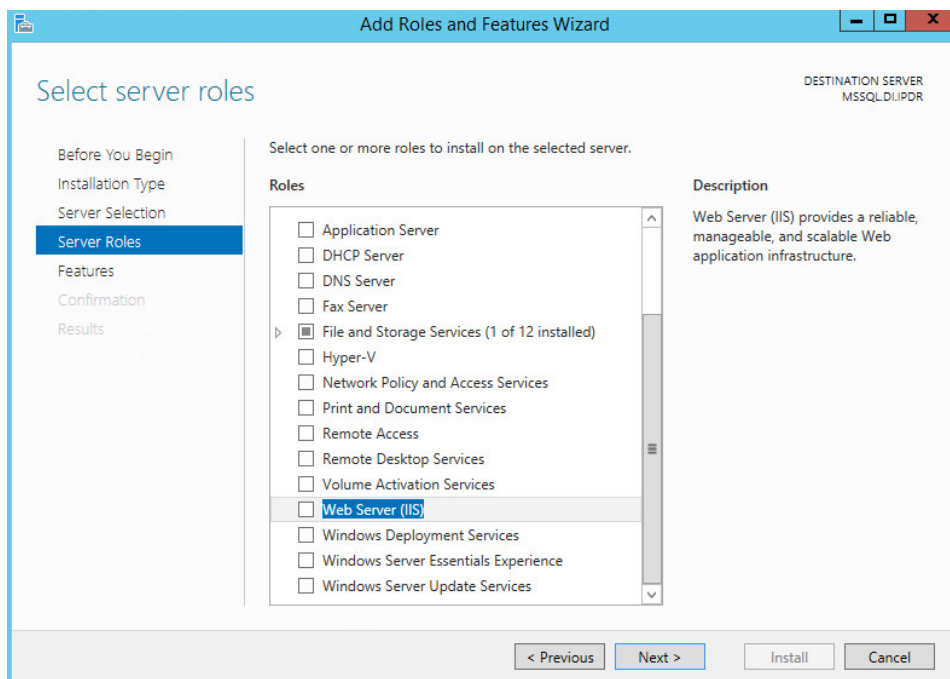
5. Click **Next**.

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

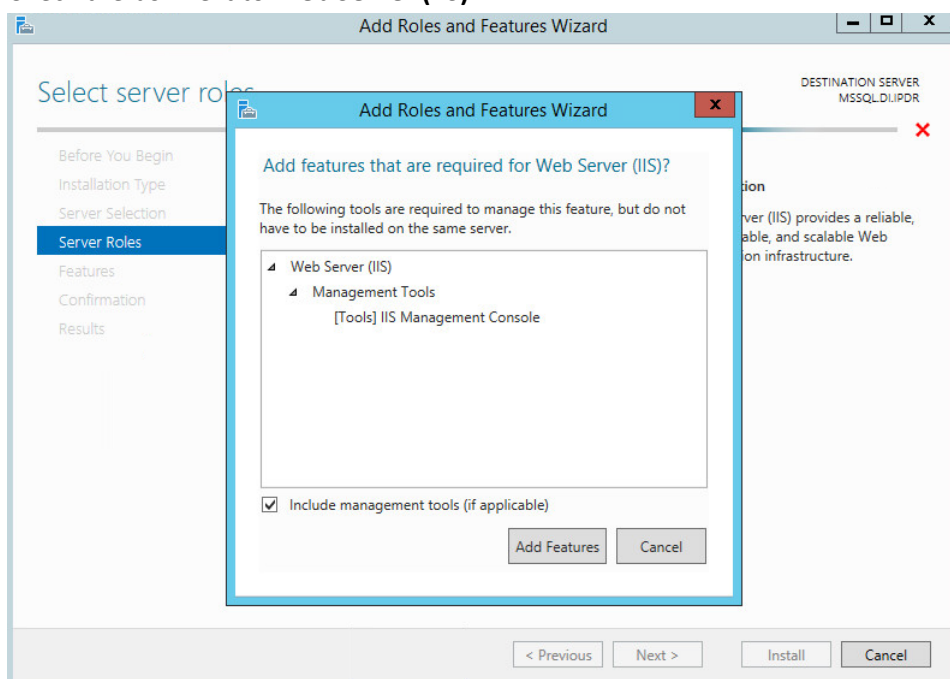


7. Click **Next**.

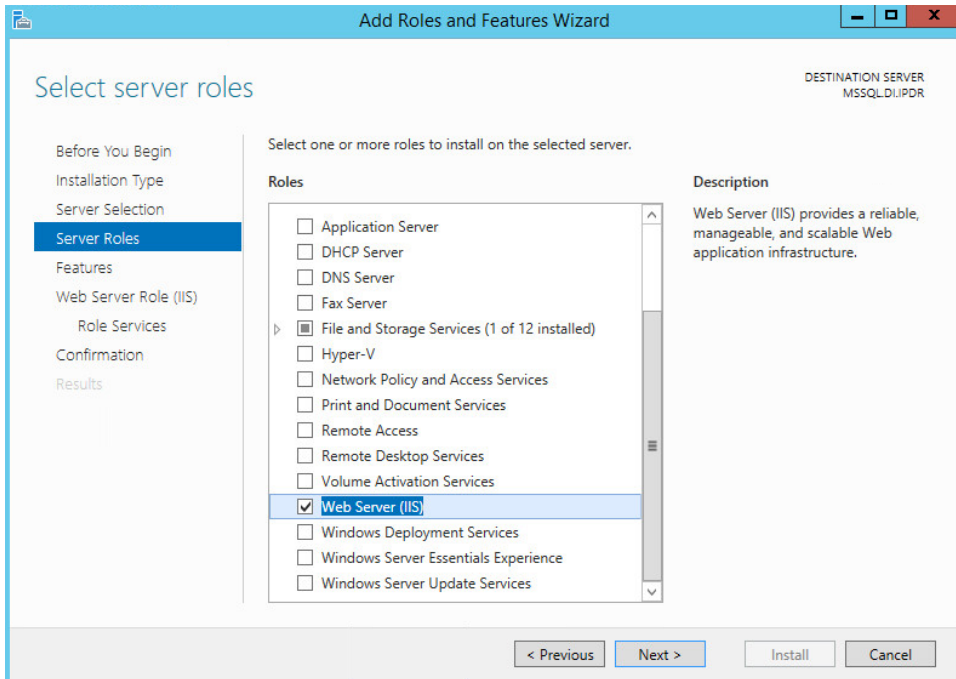




8. Check the box next to **Web Server (IIS)**.

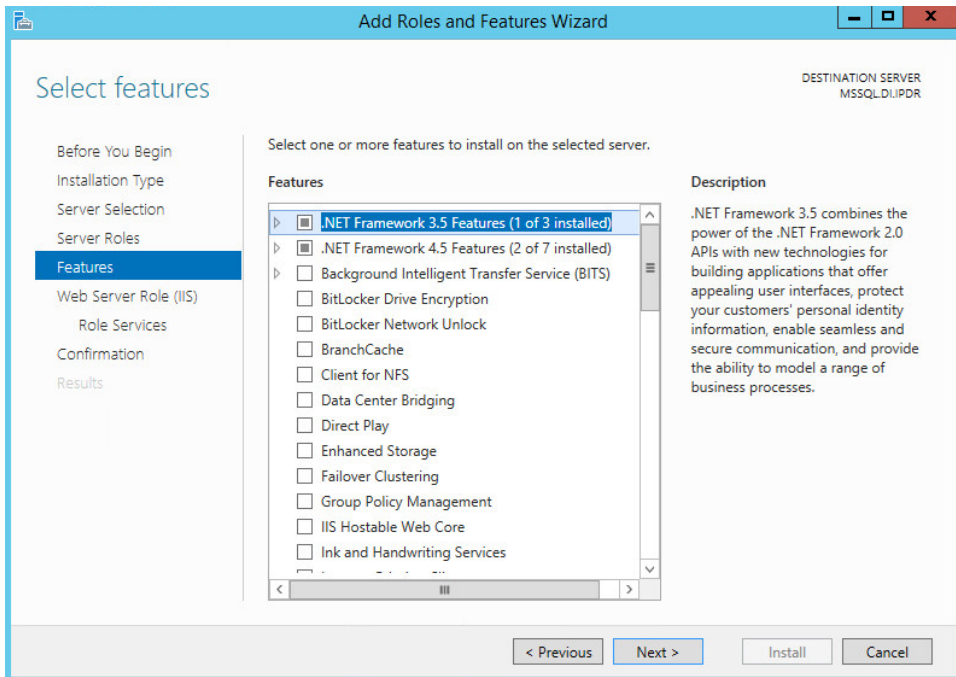


9. Click **Add Features**.

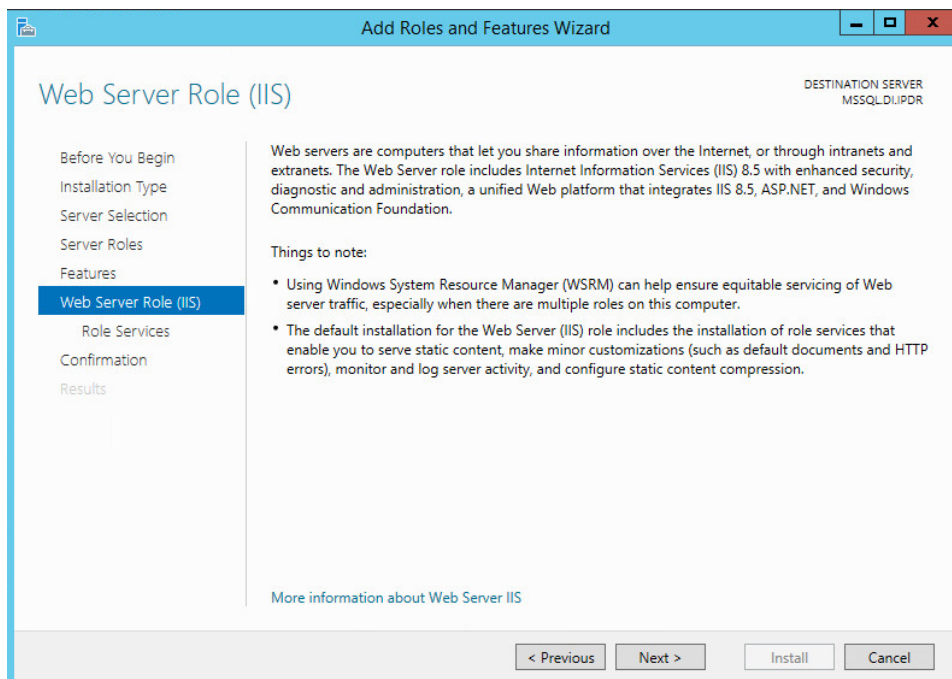


10. Click **Next**.

11. Ensure that all desired features are selected.

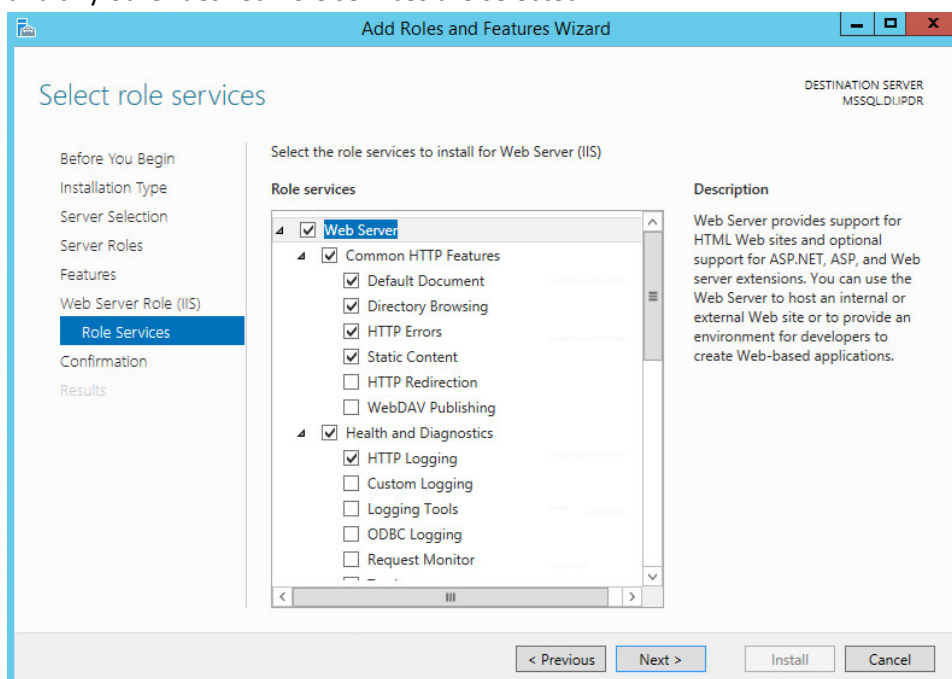


12. Click **Next**.

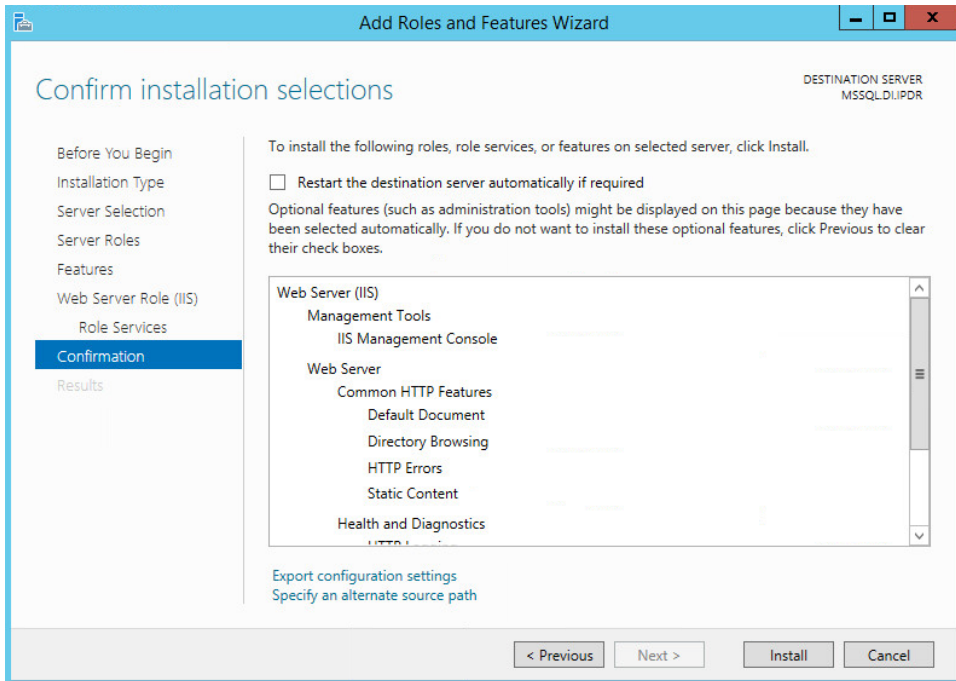


13. Click **Next**.

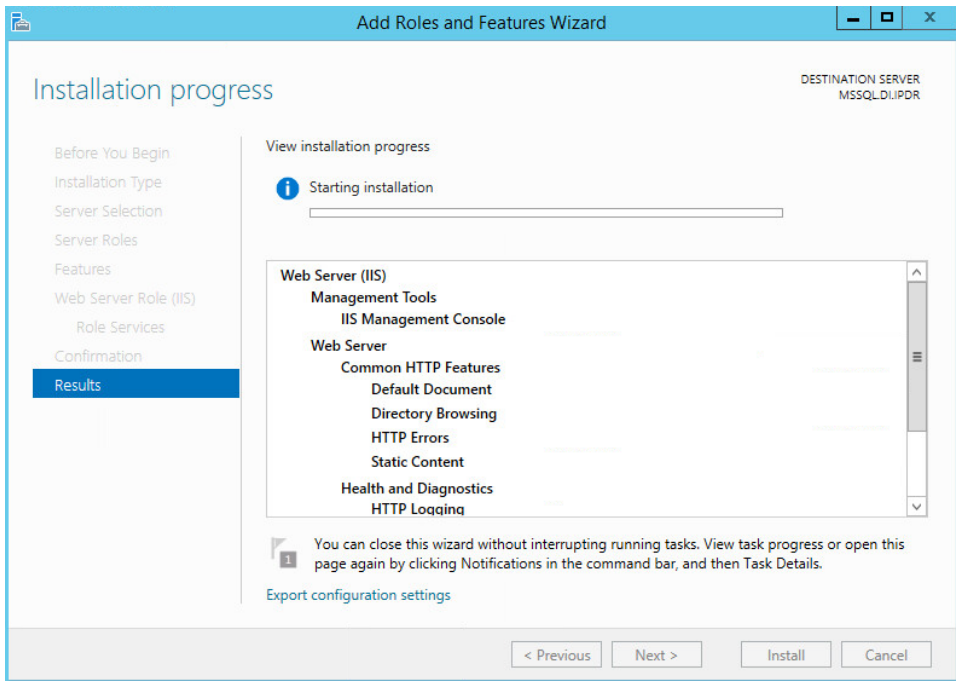
14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging**, and any other desired Role services are selected.



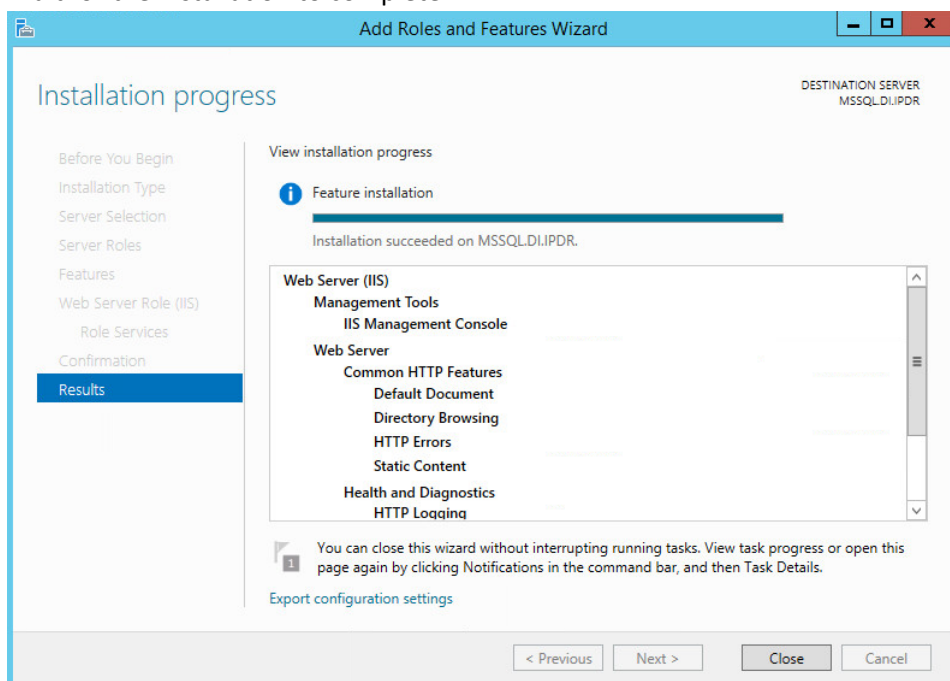
15. Click **Next**.



16. Click **Install**.



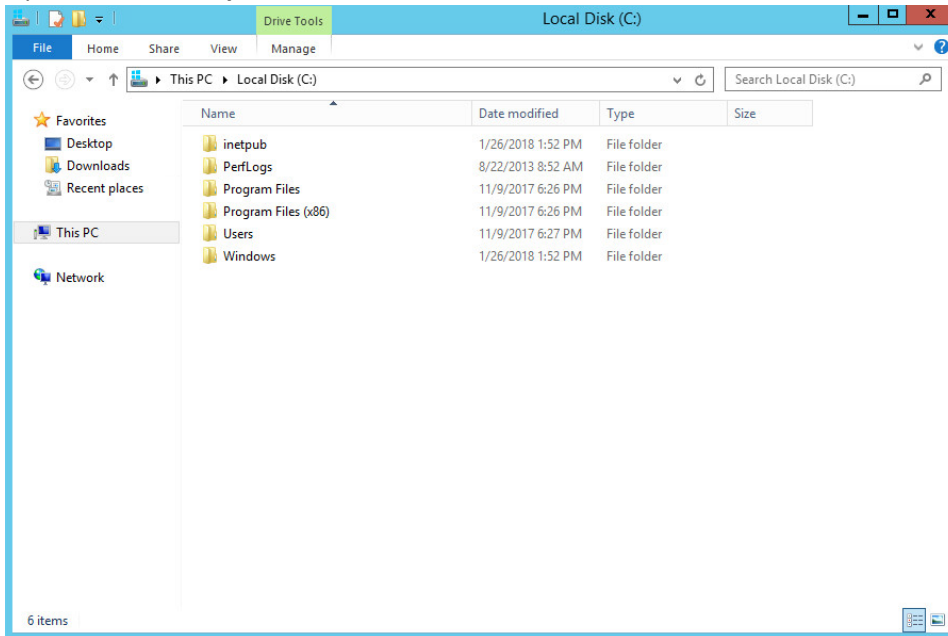
17. Wait for the installation to complete.



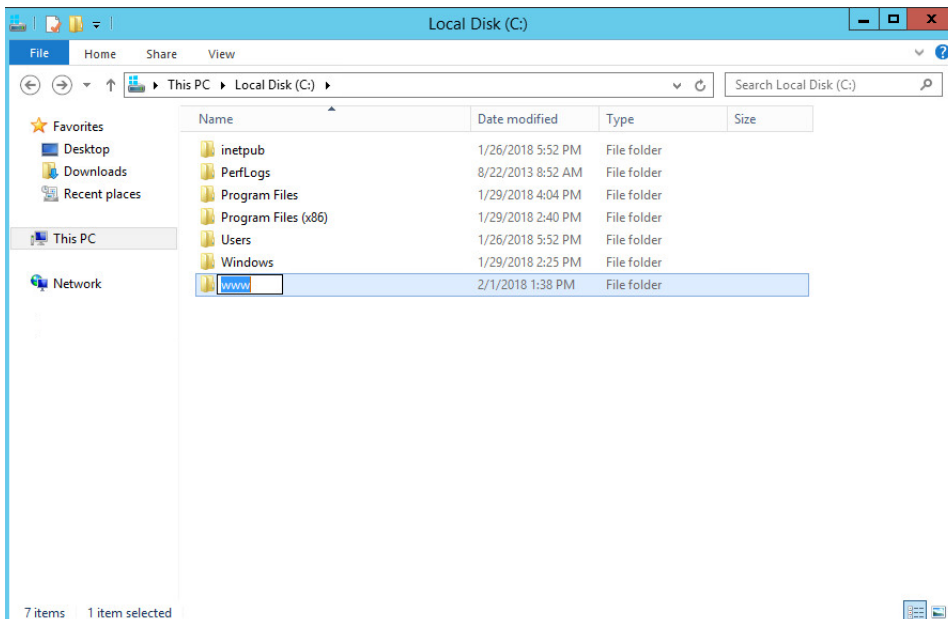
18. Click **Close**.

## 2.5.2 IIS Configuration

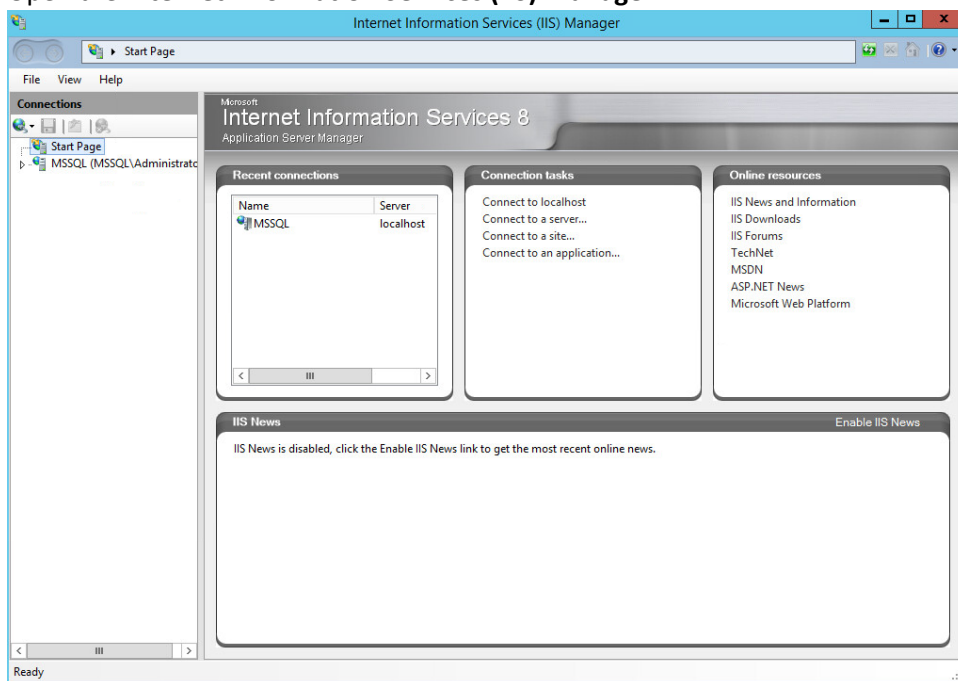
1. Open **Windows Explorer** and click **This PC**.



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

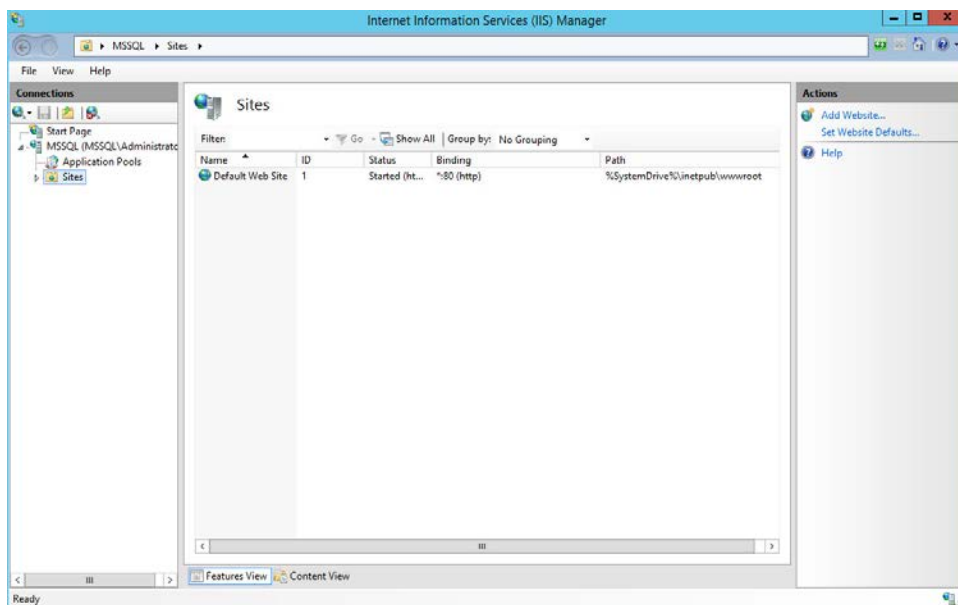


4. Open the **Internet Information Services (IIS) Manager**.



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

6. Click **Sites**.



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

**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:

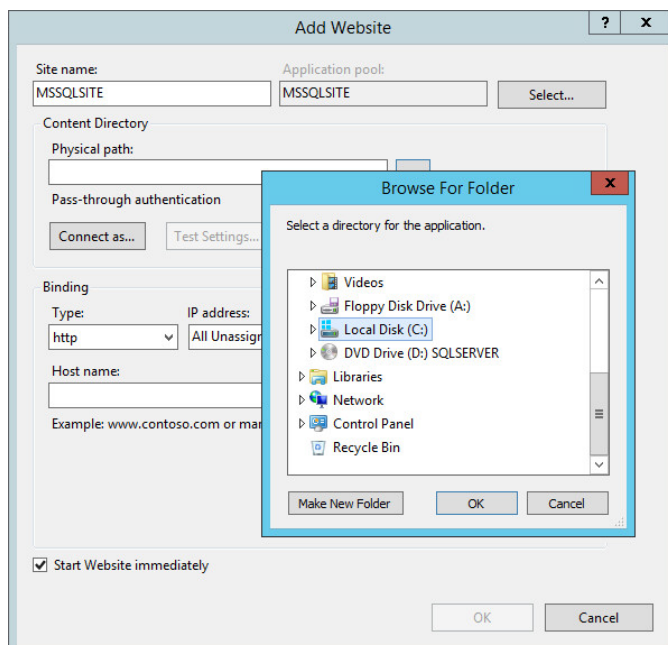
Host name:

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

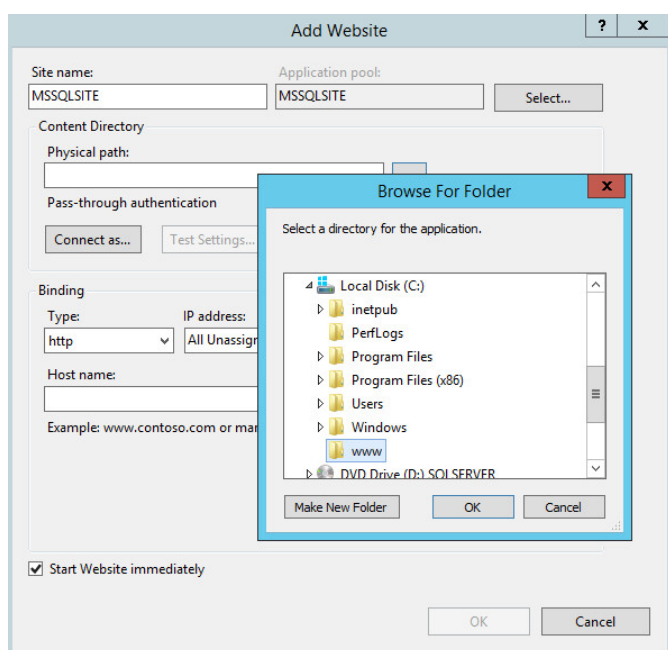
☒ Start Website immediately

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

The screenshot shows the 'Add Website' dialog box with the following fields and values:

- Site name:** MSSQLSITE
- Application pool:** MSSQLSITE
- Physical path:** C:\www
- IP address:** 192.168.81.107
- Port:** 80
- Host name:** MSSQL.di.ipdr
- Start Website immediately:** ☒

The 'OK' button is highlighted in blue.

15. Click **OK**.

## 2.6 GreenTec WORMdisks

See the *Installation of GreenTec Command Line Utilities* document, which should accompany the installation disk, for a detailed guide on how to install the GreenTec command line utilities. Furthermore, refer to the *GT\_WinStatus User Guide*, which should also accompany the installation disk, for instructions on how to effectively use GreenTec WORMdisks to preserve data. Read these instructions *carefully*, as locking GreenTec WORMdisks can result in making some or all of the disk or the entire disk unusable. Having portions of the disk or the entire disk permanently locked is sometimes desirable, but it is dependent on the needs of your organization, e.g., if you want to store backup information or logs securely.

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

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

### 2.6.1 Format GreenTec WORMdisks

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

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

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

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

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

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

```
Format successful
```

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

```
Format successful
```

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

```
Format successful
```

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

```
Format successful
```

### 2.6.2 Obtain Status Information About GreenTec WORMdisks

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

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

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

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

```
> wvlist.exe 1
```

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

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

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

> IS WORM > IS \*NOT\* Finalized

\*\*\*\* WORMdisk Volume (WDV) Info \*\*\*\*

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

### 2.6.3 Map GreenTec WORMdisks to Drive Letters

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

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

For example,

> **wvmap.exe H:**

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

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

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

For example,

> **wvmap.exe H: 1.2**

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

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

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

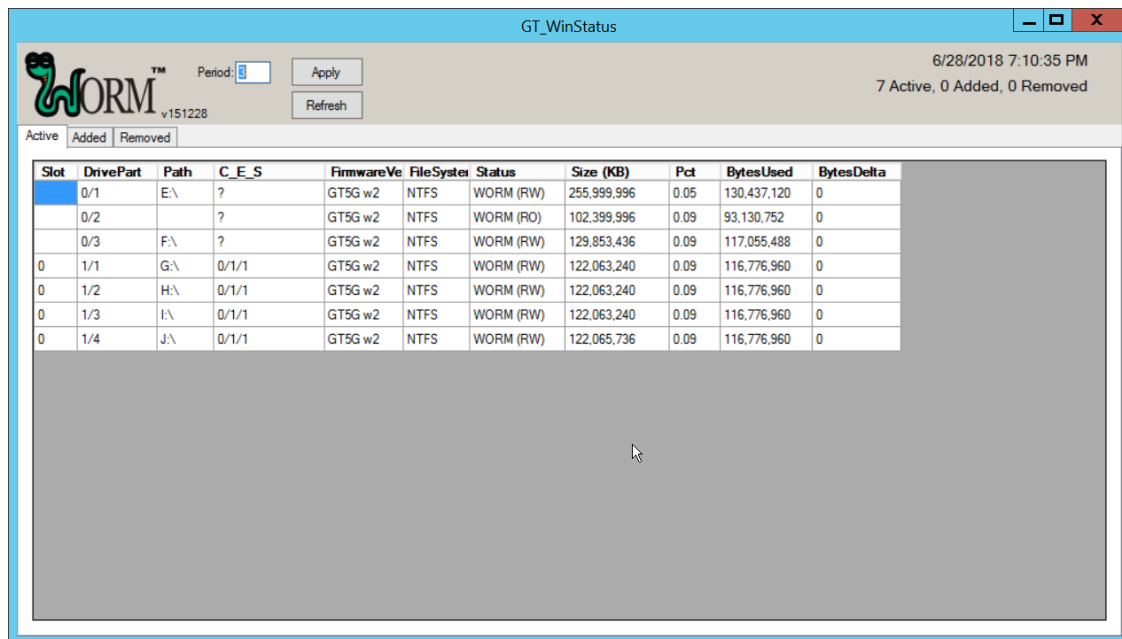
For example, if *H:* is mapped to partition 2 of drive 1 (1.2)

> `wvnext.exe H:`

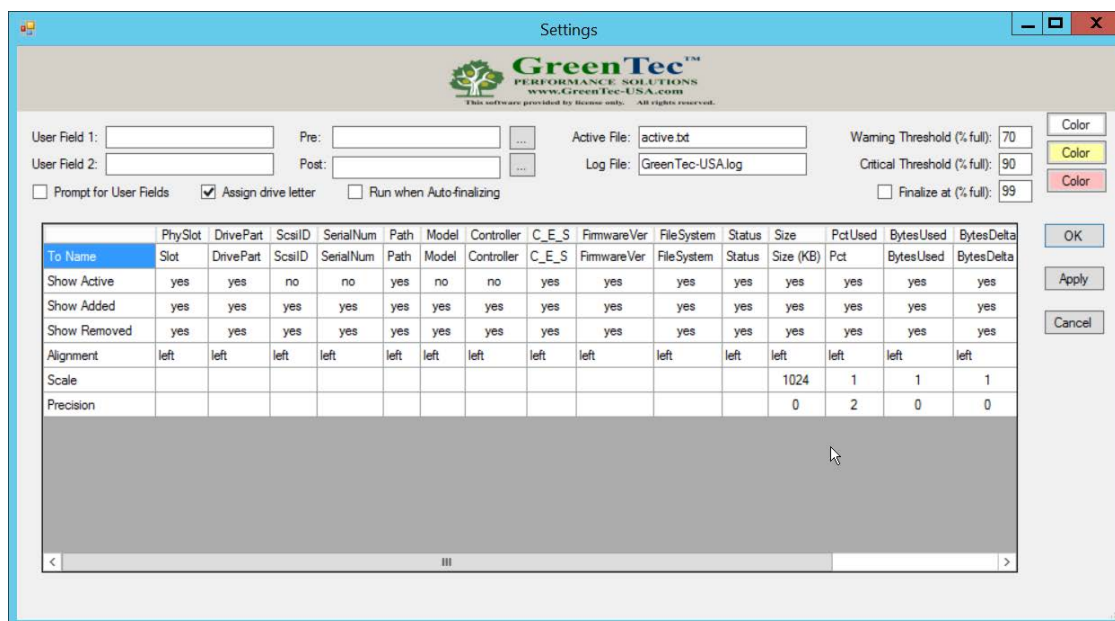
will attempt to map *H:* to partition 3 of drive 1 (1.3).

## 2.6.4 Activate Write Protection in GreenTec WORMdisks

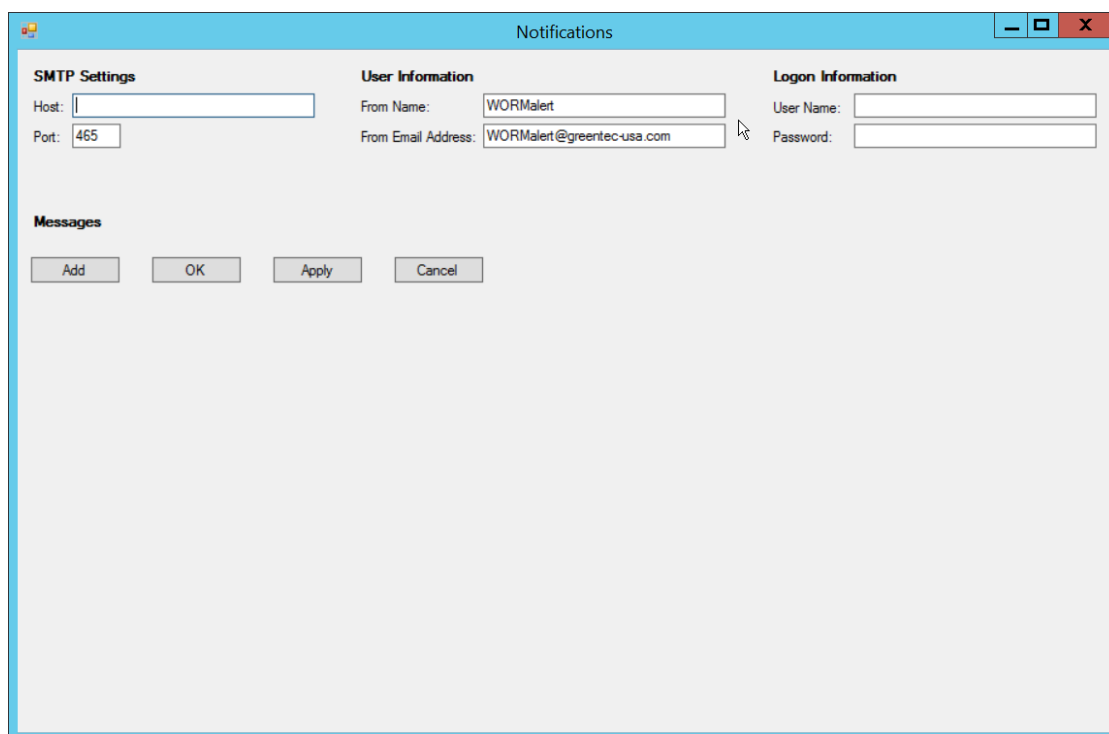
1. Running `GT_WinStatus.exe` will open the Graphical User Interface (GUI), which displays various information such as drive mappings, partitions, total space, and space used, as well as a range of other options.



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



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



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

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

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

The screenshot shows the GT\_WinStatus application window. At the top, there's a title bar 'GT\_WinStatus' and a status bar showing '6/28/2018 7:30:18 PM' and '7 Active, 0 Added, 0 Removed'. Below the title bar is a toolbar with 'Period: 3', 'Apply', and 'Refresh' buttons. The main area contains a table with columns: Slot, DrivePart, Path, C\_E\_S, FirmwareVer, FileSystem, Status, Size (KB), Pct, BytesUsed, BytesDelta, TLock, Enforce, and Finalize. The table lists several drives with their respective paths and sizes. Below the table, there are three buttons: TLock, Enforce, and Finalize.

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

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

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

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

**The Finalize function permanently locks the entire drive.**

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



## 2.7 CryptoniteNXT

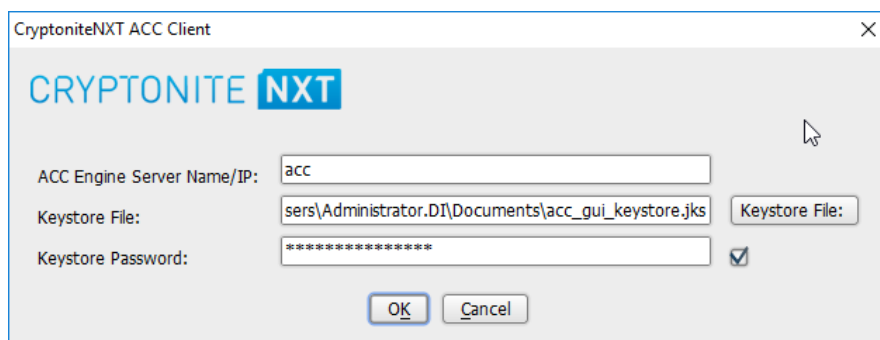
See the *CryptoniteNXT 2.6.2 Unified Installation Guide*, which should accompany the device for a detailed guide on how to install **CryptoniteNXT** on the provided device.

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

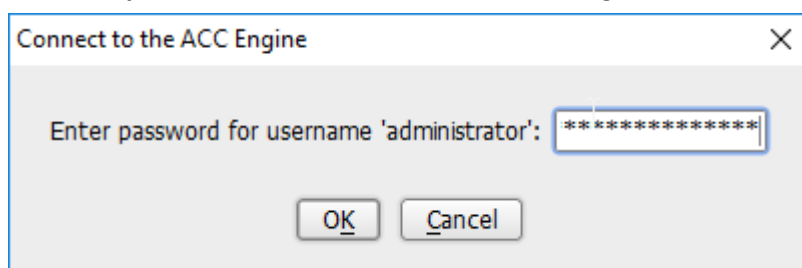
### 2.7.1 Configure Cryptonite NXT

#### 2.7.1.1 Verify a New Device

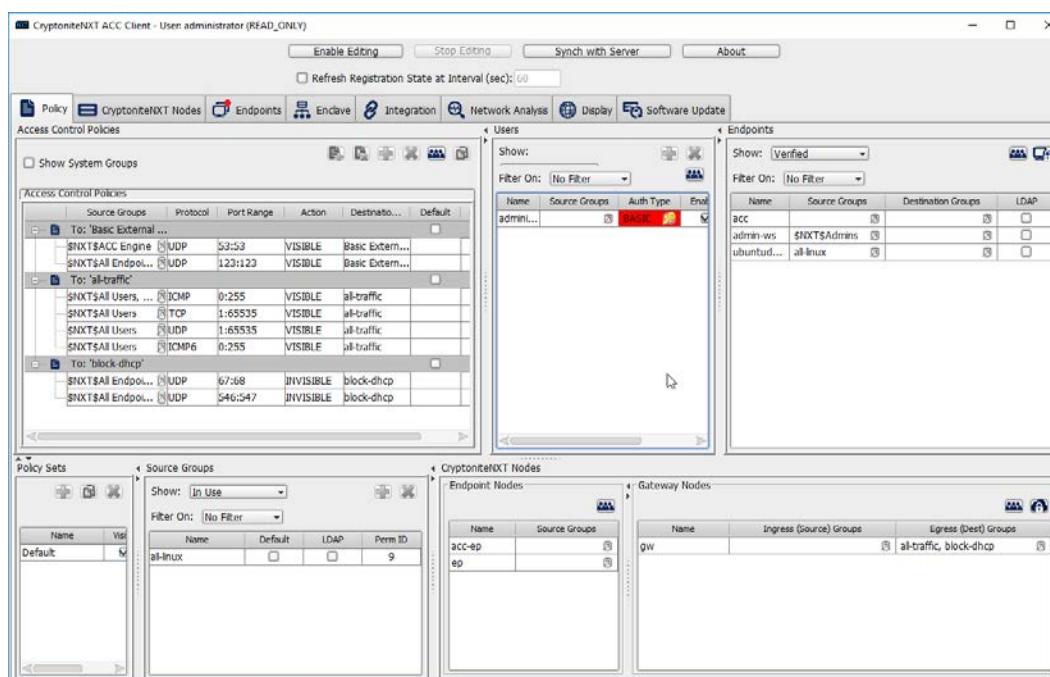
1. Open the **CryptoniteNXT ACC GUI** application.



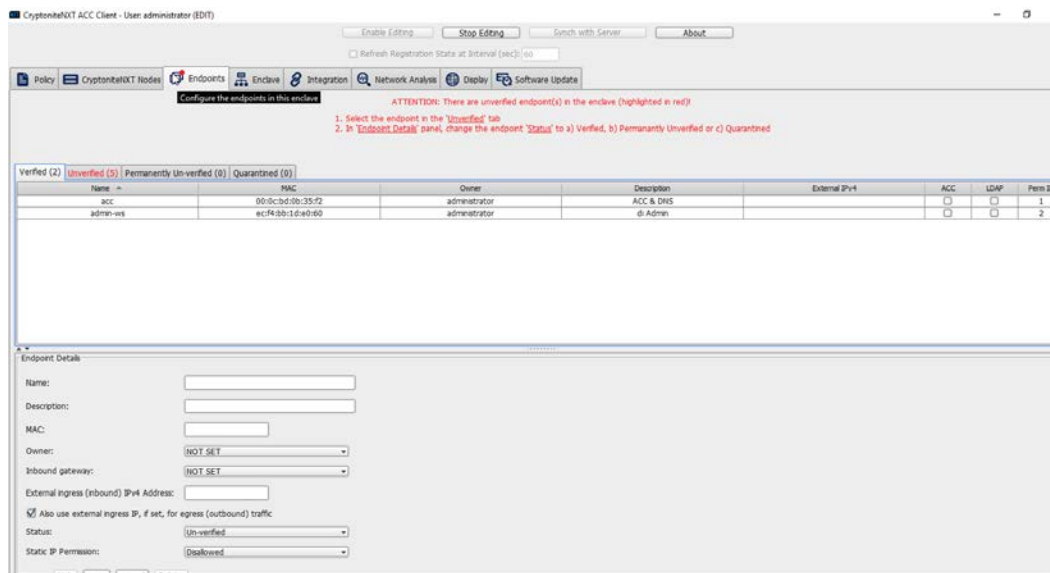
2. Click **OK**.
3. Enter the **password** for the account created during the installation.



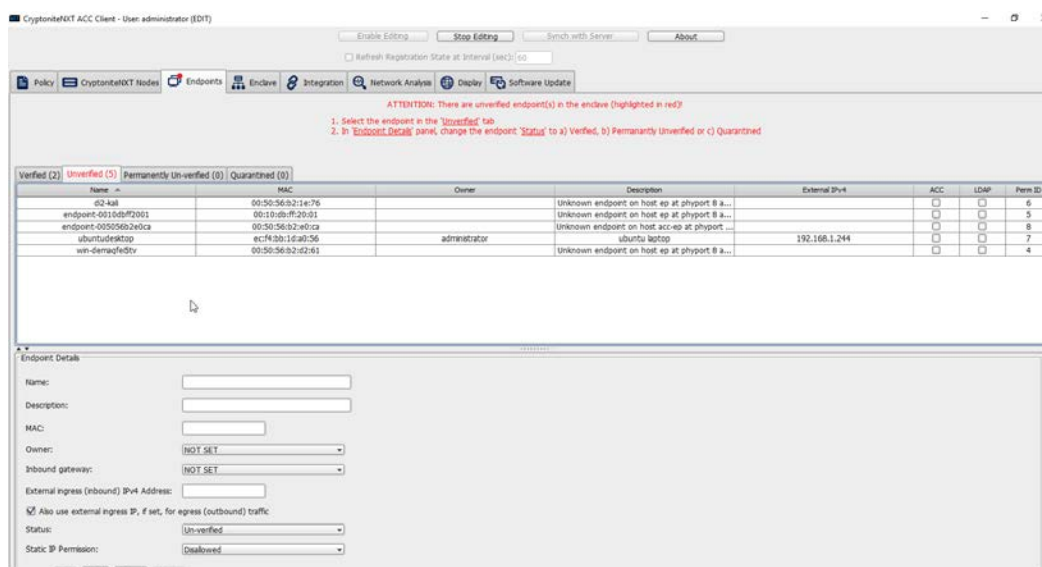
4. Click **OK**.



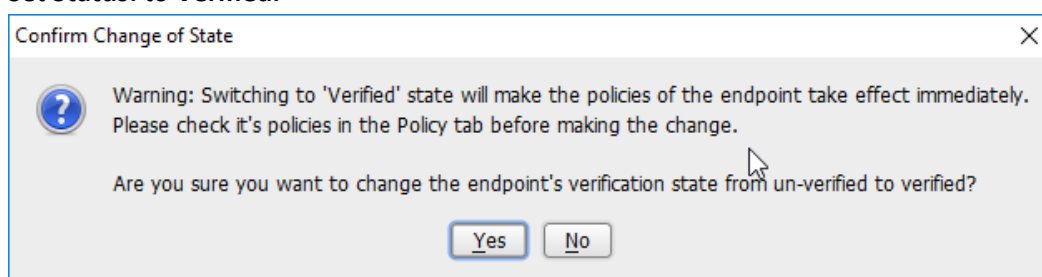
5. Click **Enable Editing** at the top of the application.
6. Click the **Endpoints** tab.



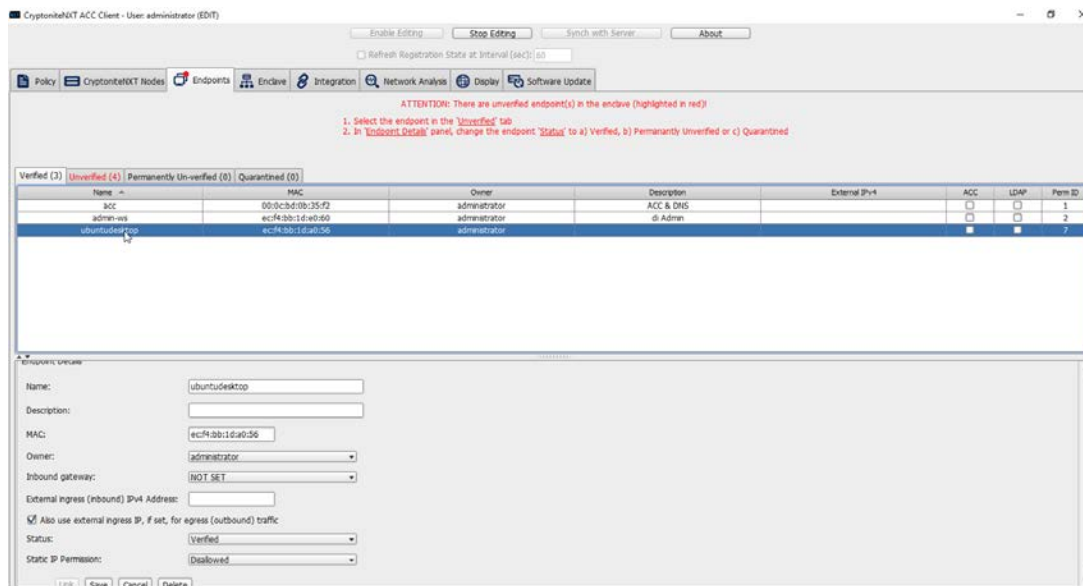
7. Click the **Unverified** tab. Any new devices connected to the network should appear here, if configured to use Dynamic Host Configuration Protocol (DHCP).



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

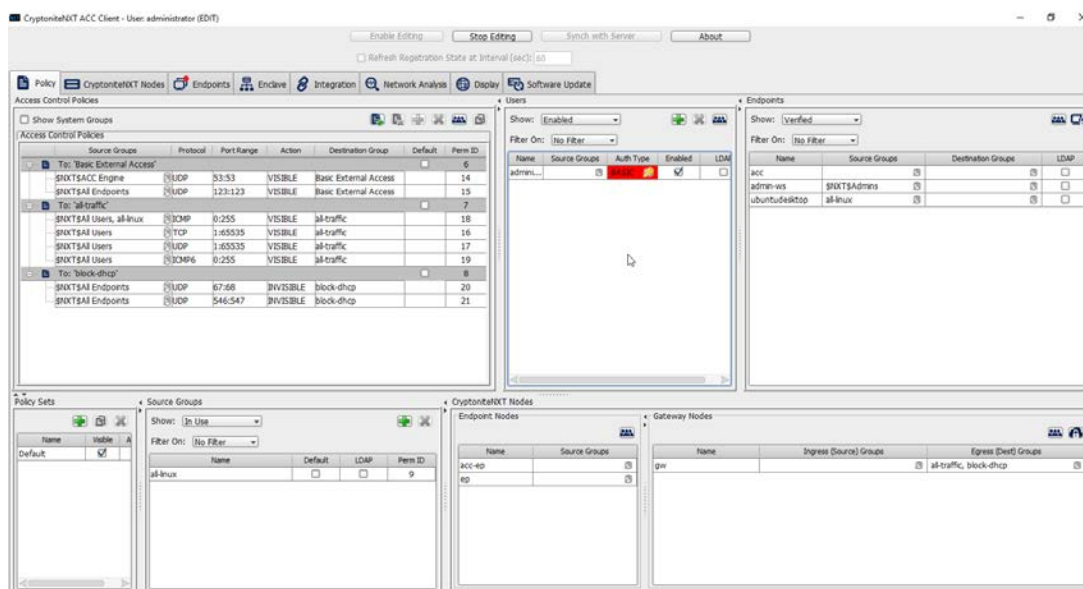


16. Click **Yes**.
17. Click **Save**.
18. The machine should now appear in the **Verified** tab.

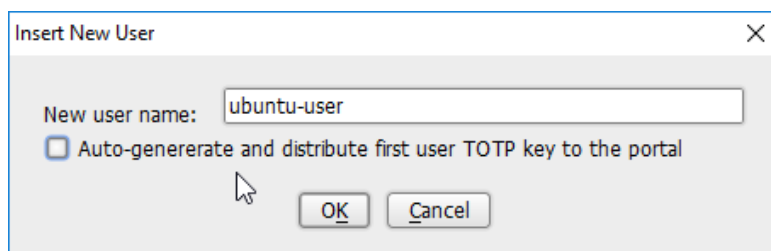


### 2.7.1.2 Create a New User

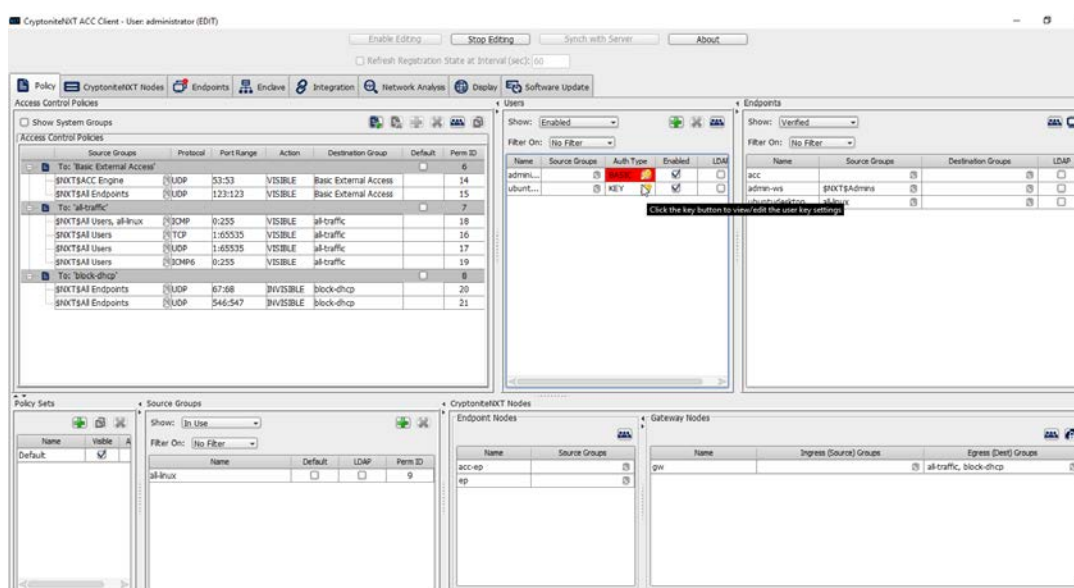
1. Go to the **Policy** tab.



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



4. Click **OK**.



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

**Modify User Authentication Key**

User name: ubuntu-user

Authentication Type:

☒ Keep current type: TOTP KEY <VALUE HIDDEN>

OR

☐ Auto-generate and distribute new TOTP key (STRONGLY RECOMMENDED if making changes)

☐ Manually enter TOTP key (for hardware tokens):

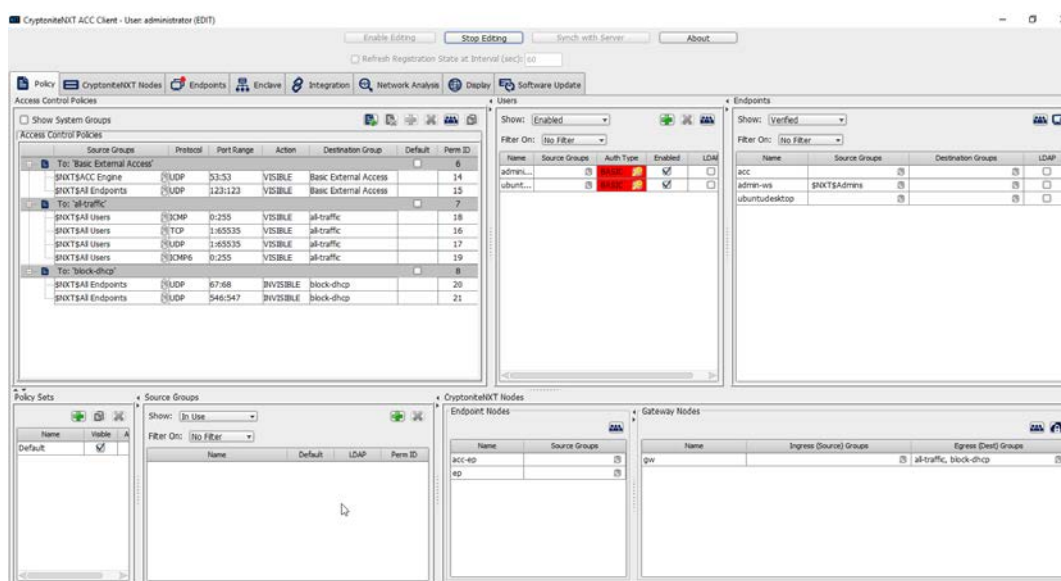
(Enter Base32 encoded key, exactly 32 characters using only A-Z, 2-7 NO zeros or ones)

☐ Basic password (WARNING: THIS IS INSECURE!):

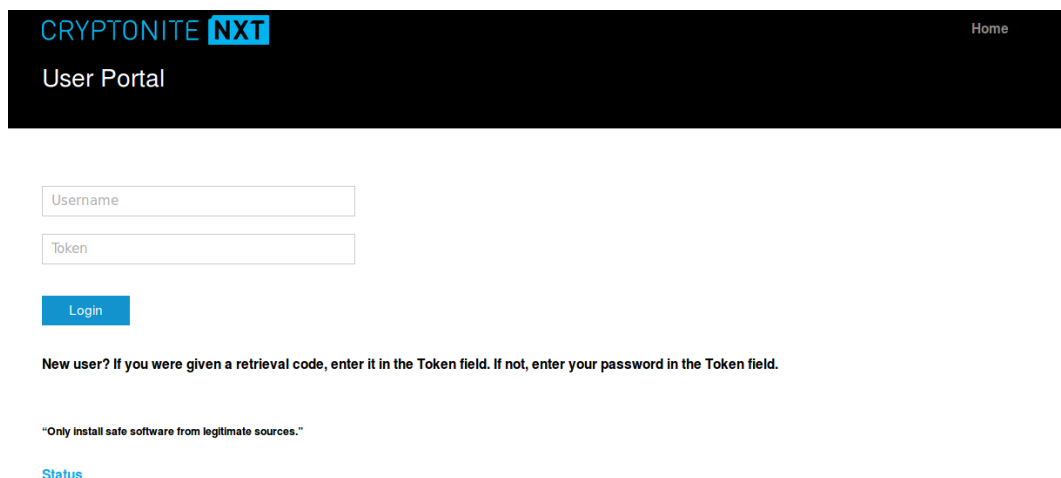
(Passwords in general can be easily replayed by malware, do not use this option!)

Save Cancel

7. Click **Save**.



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

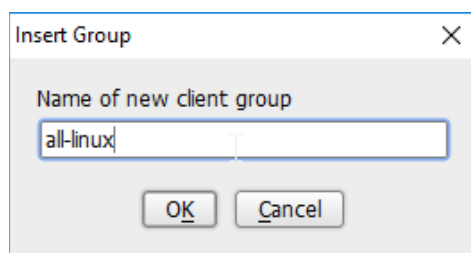


The screenshot shows the 'CRYPTONITE NXT' logo in the top left corner of a dark header bar, with a 'Home' link in the top right. Below the header, the text 'User Portal' is centered. The main content area contains two input fields: 'Username' and 'Token'. Below these fields is a blue 'Login' button. A note below the button reads: 'New user? If you were given a retrieval code, enter it in the Token field. If not, enter your password in the Token field.' Below the note is a small text string: '"Only install safe software from legitimate sources."' At the bottom of the form is a blue link labeled 'Status'.

### 2.7.1.3 Create a New Policy

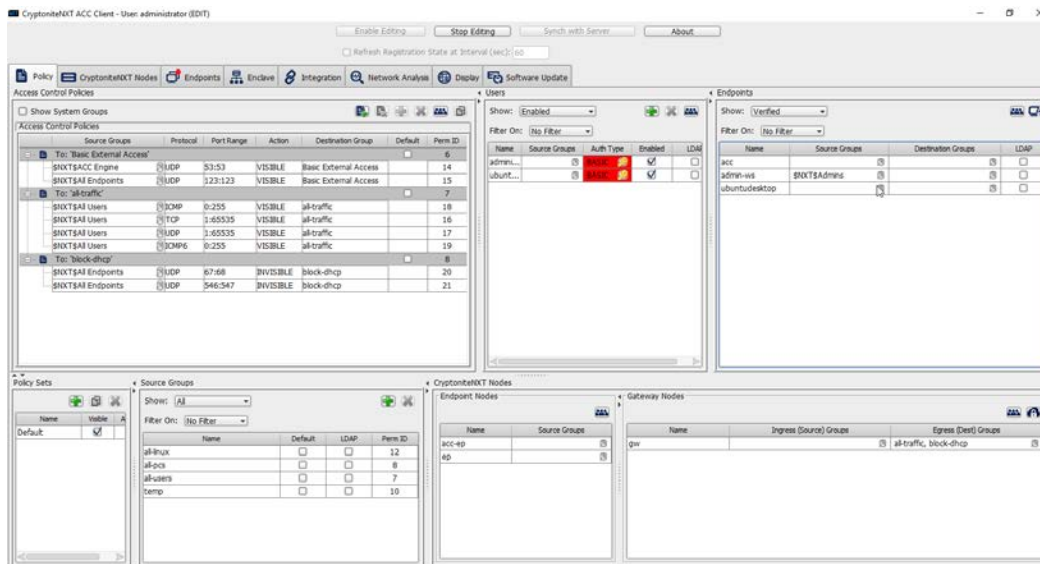
Creating policy in CryptoniteNXT essentially requires specifying allowed types of traffic. To do this, source groups and destination groups are created.

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

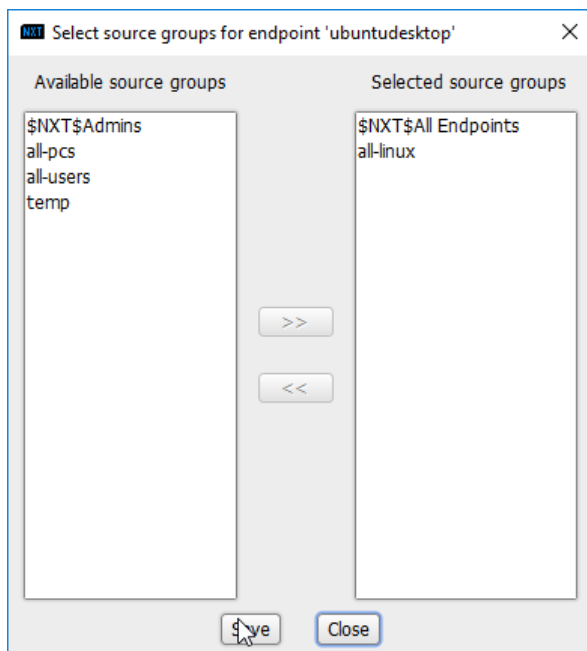


The screenshot shows a dialog box titled 'Insert Group' with a close button (X) in the top right corner. Inside the dialog, there is a label 'Name of new client group' above a text input field. The input field contains the text 'all-linux'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

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

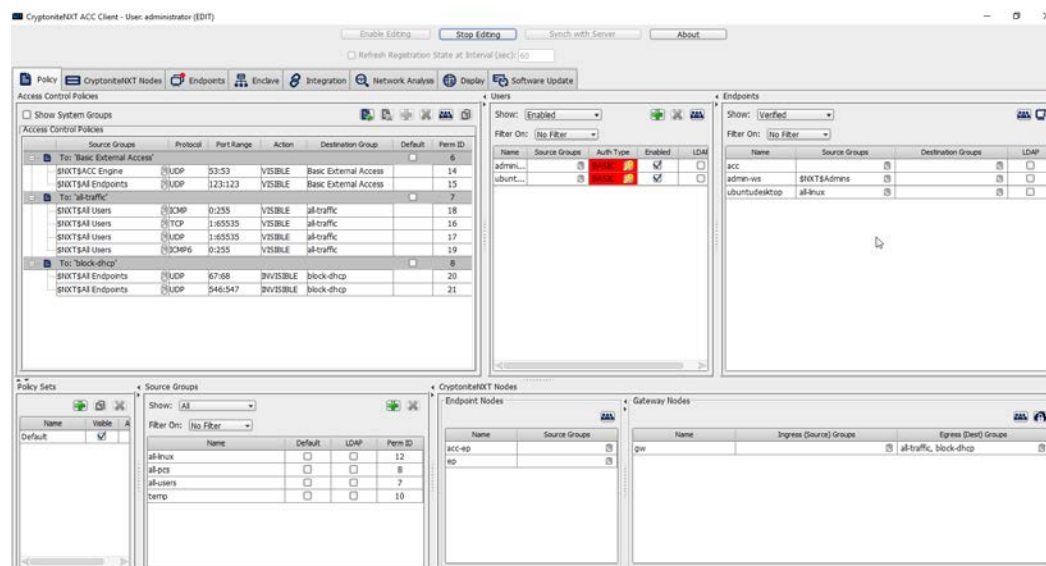


5. In the **Endpoints** window, click the arrow button under the **Source Groups** column for any machines to be added to this **Source Group**.
6. Select the newly created group (or groups).
7. Click the >> button to add the endpoint to this group.



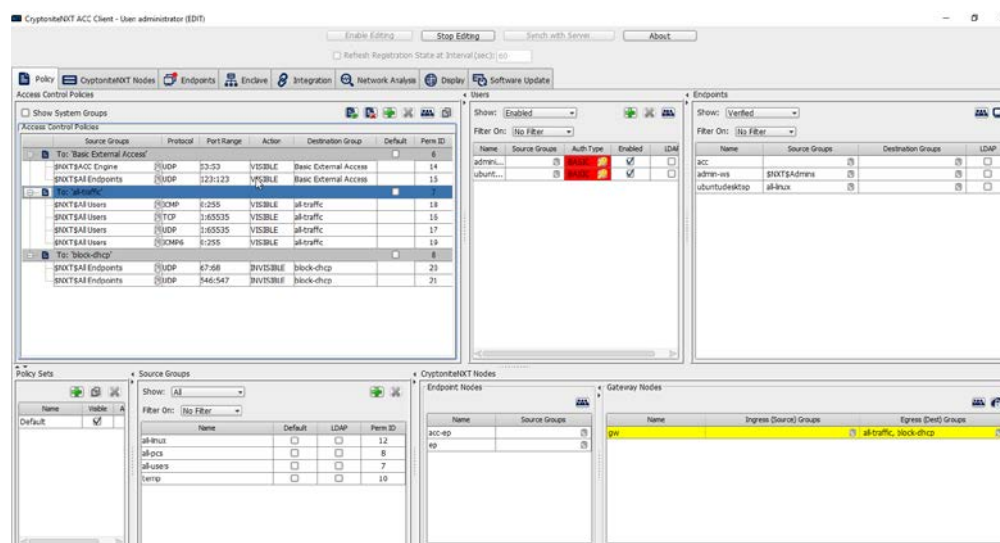
8. Click **Save**.
9. The group should show under the **Source Groups** column for those endpoints.





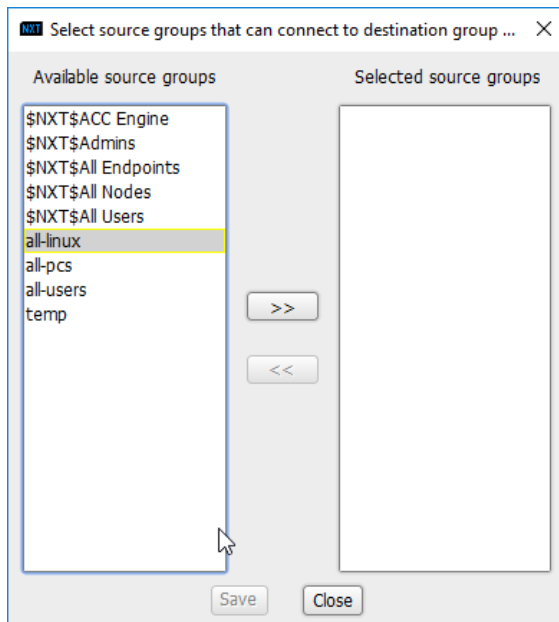
Destination groups are used to govern the allowed destinations of endpoints within certain source groups. While destination groups can be created according to organizational property, this example uses an existing group, **all-traffic**.

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

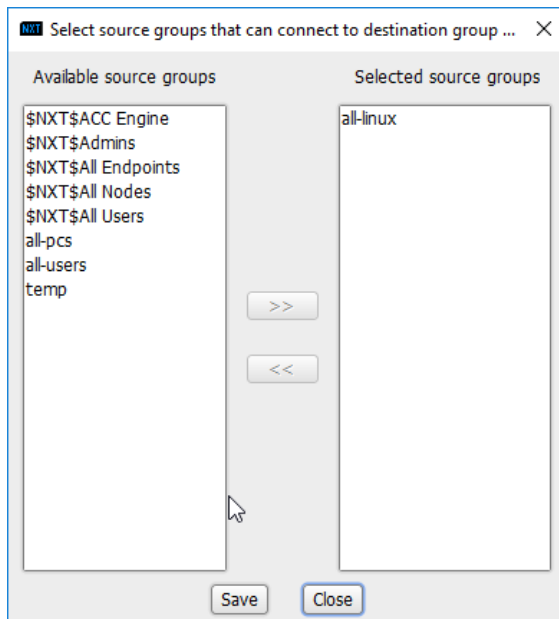


2. Click the arrow button under the **Source Groups** column.

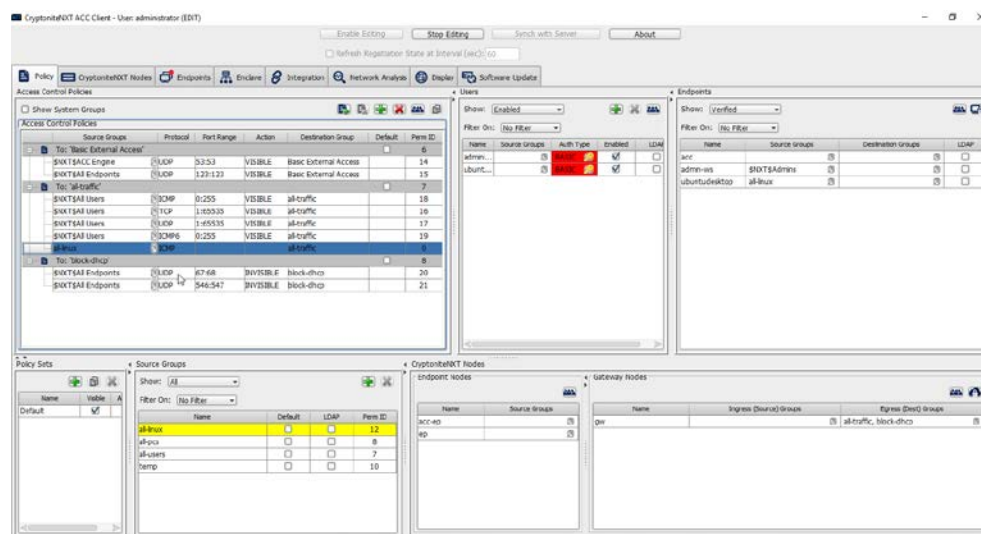
3. Select the newly created source group.



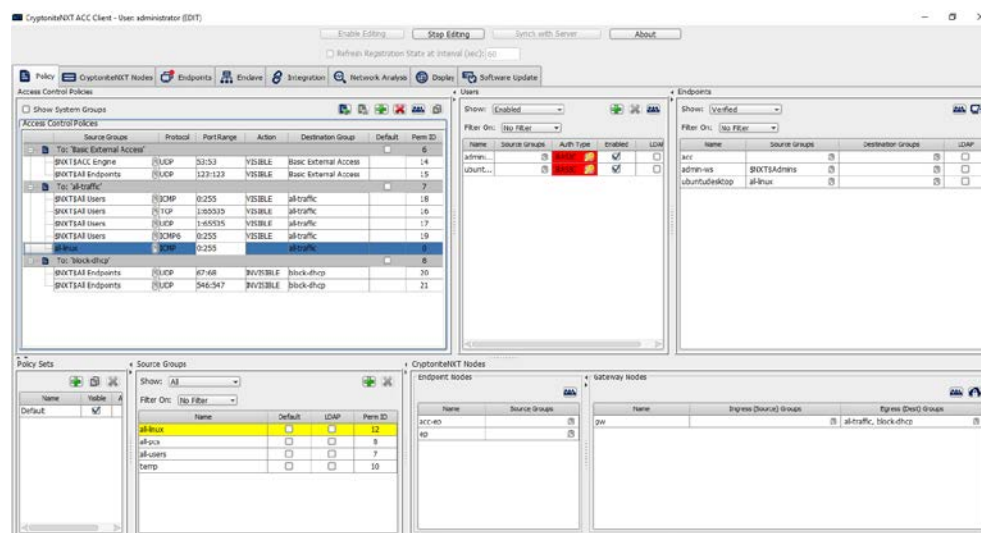
4. Click the >> button.



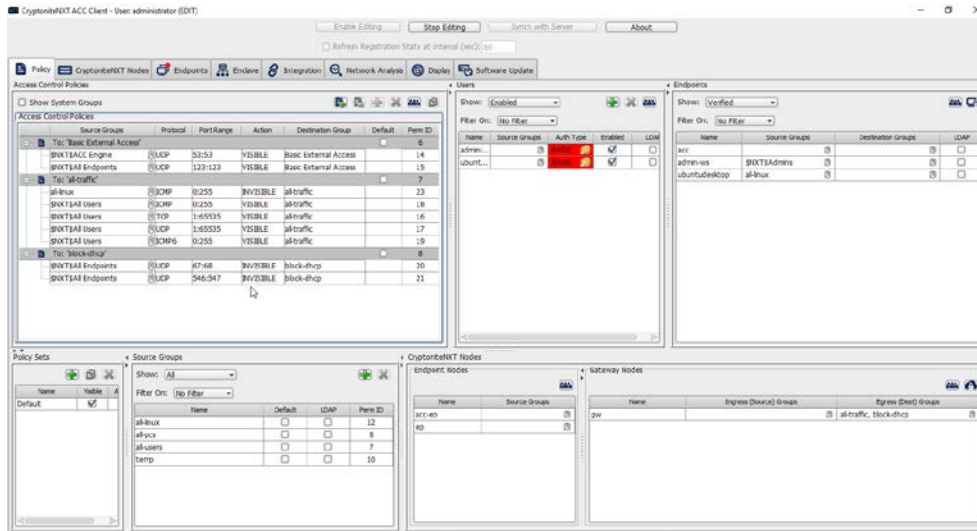
5. Click **Save**.
6. Select the **Protocol**. In this case, to prevent the machine from using ping, we choose **ICMP**.



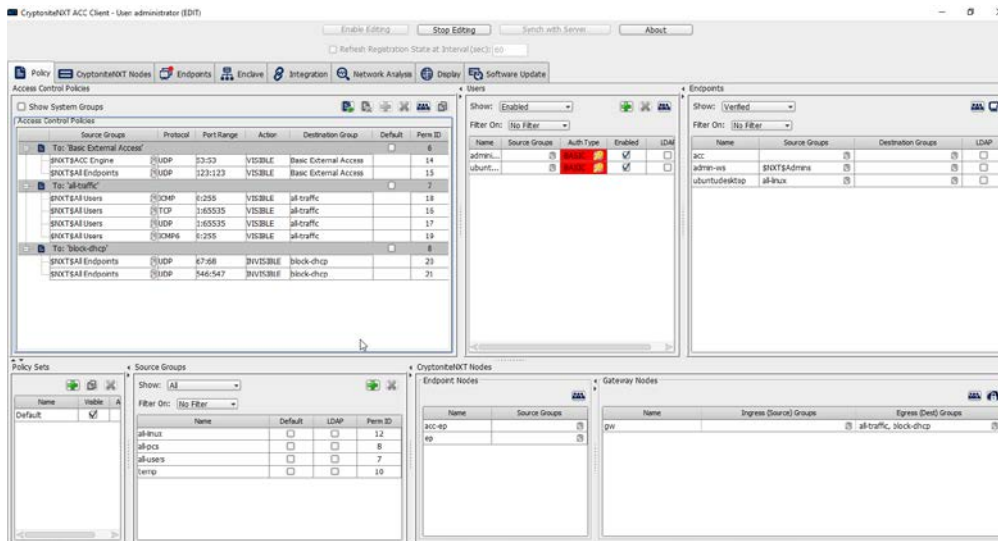
7. Enter the port range that this traffic can operate on.



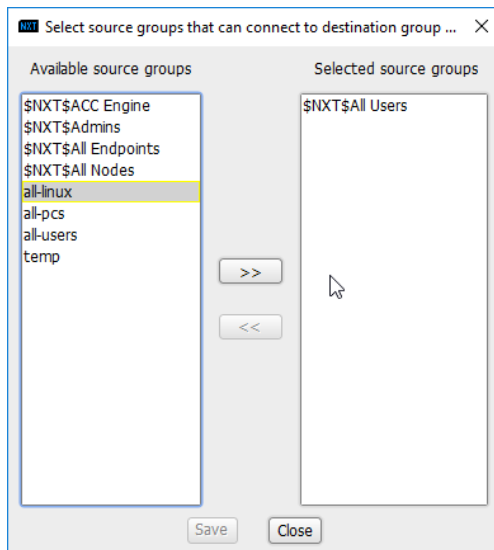
8. Select **INVISIBLE** for the **Action** column.



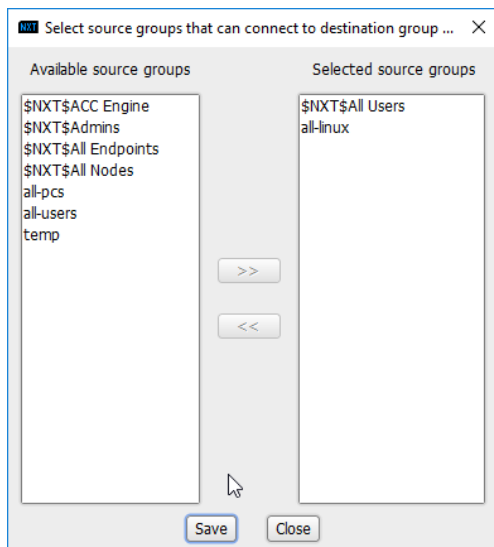
9. This will prevent the members of this group from using ping.
10. To allow the members of this group to use ping, delete this rule. Right-click the entry and select **Delete Access Control Policy Entries**.



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

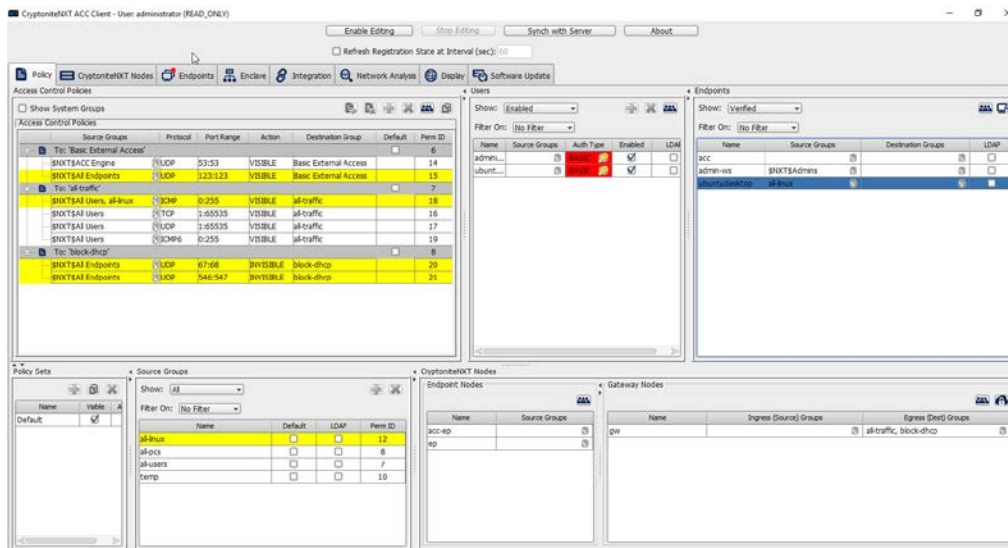


13. Click the >> button.



14. Click **Save**.

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



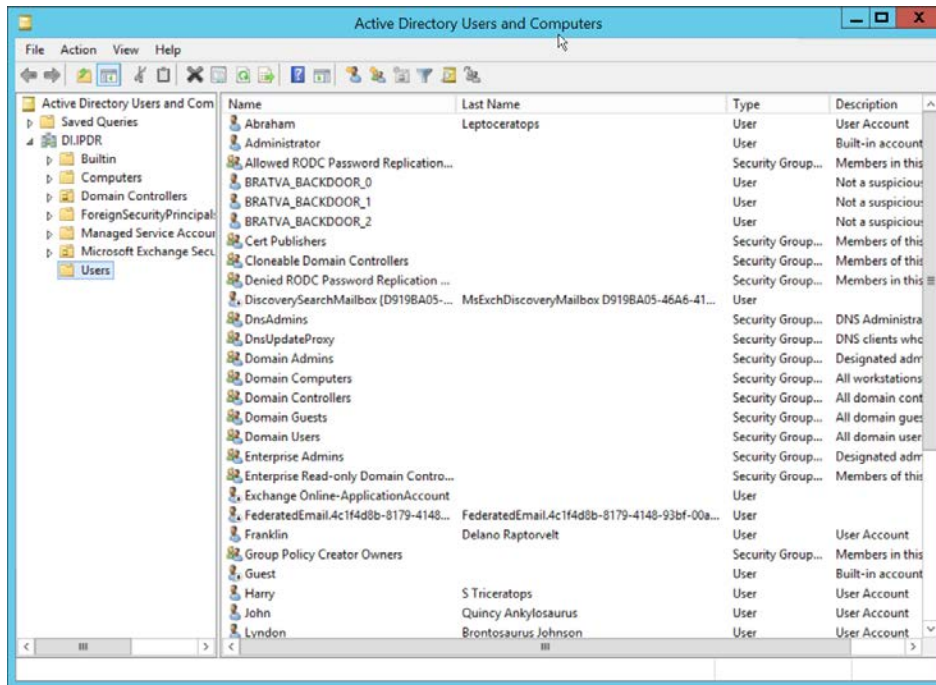
16. Now, the new machine should be allowed to use ping. With these policies it is possible to manage all traffic through the specification of groups, ports, and protocols.

## 2.7.2 Integrate CryptoniteNXT with Active Directory

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

### 2.7.2.1 Generate a Keytab File

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



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

Create in: DI.IPDR/Users

First name:  Initials:

Last name:

Full name:

User login name:  @DI.IPDR

User login name (pre-Windows 2000):

< Back Next > Cancel

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

New Object - User

Create in: DI.IPDR/Users

Password: [dots]

Confirm password: [dots]

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back   Next >   Cancel

6. Click **Next**.

New Object - User

Create in: DI.IPDR/Users

When you click Finish, the following object will be created:

Full name: NXTADMIN

User logon name: nxtadmin@DI.IPDR

The password never expires.

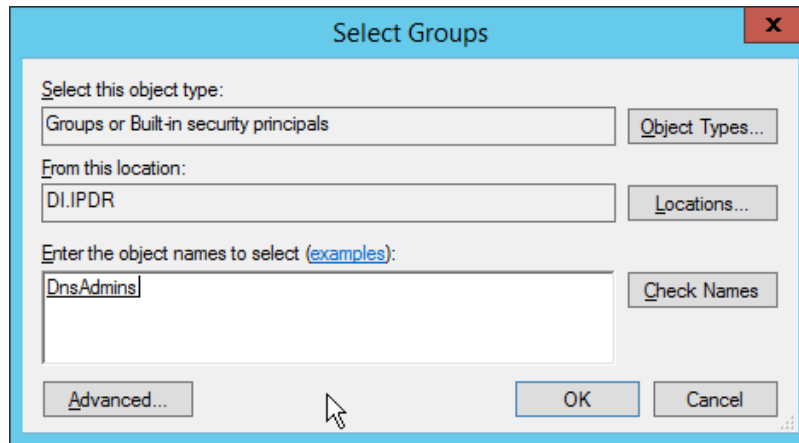
< Back   Finish   Cancel

7. Click **Finish**.

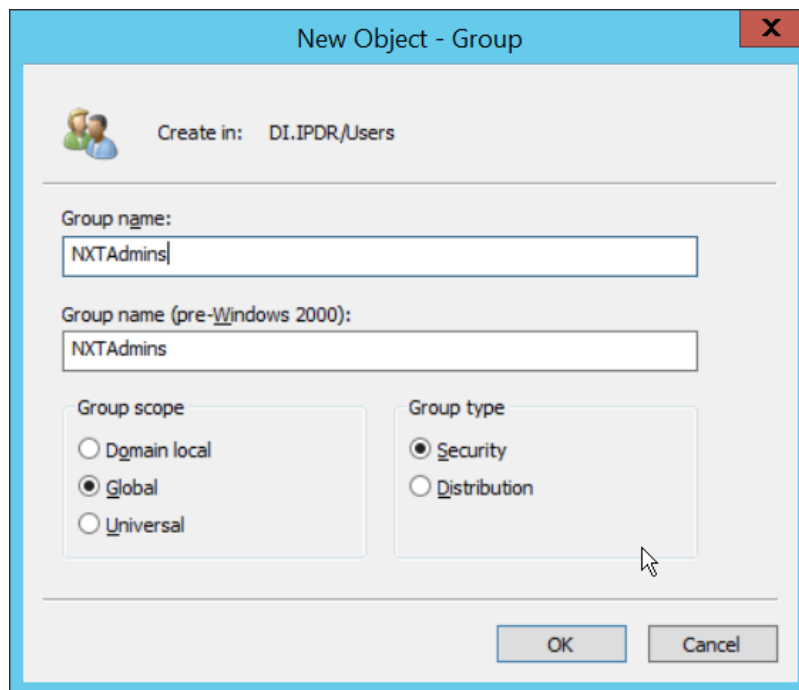
8. Right-click the newly created user and select **Add to a group....**

9. Enter **DnsAdmins**.

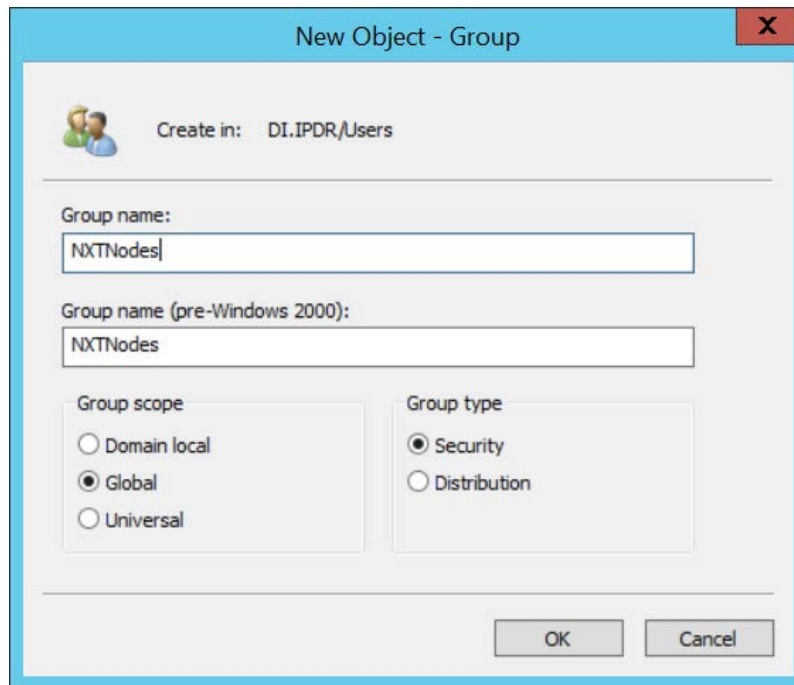




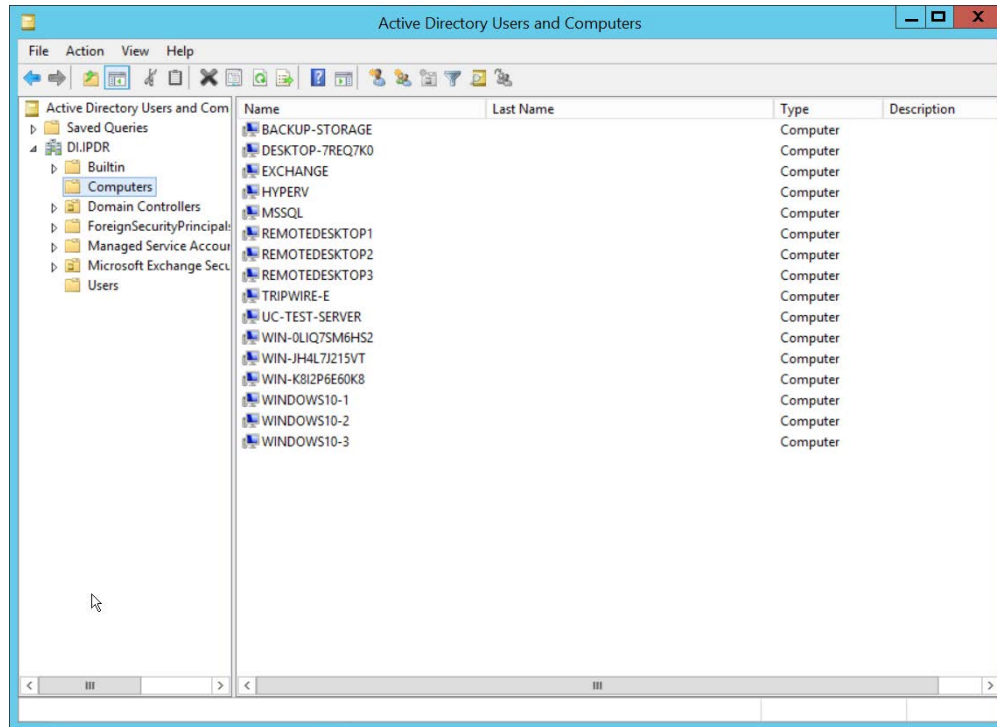
10. Click **OK**.
11. Right-click the **Users** folder in the left pane and select **New > Group**.
12. Enter **NXTAdmins** as the group name.



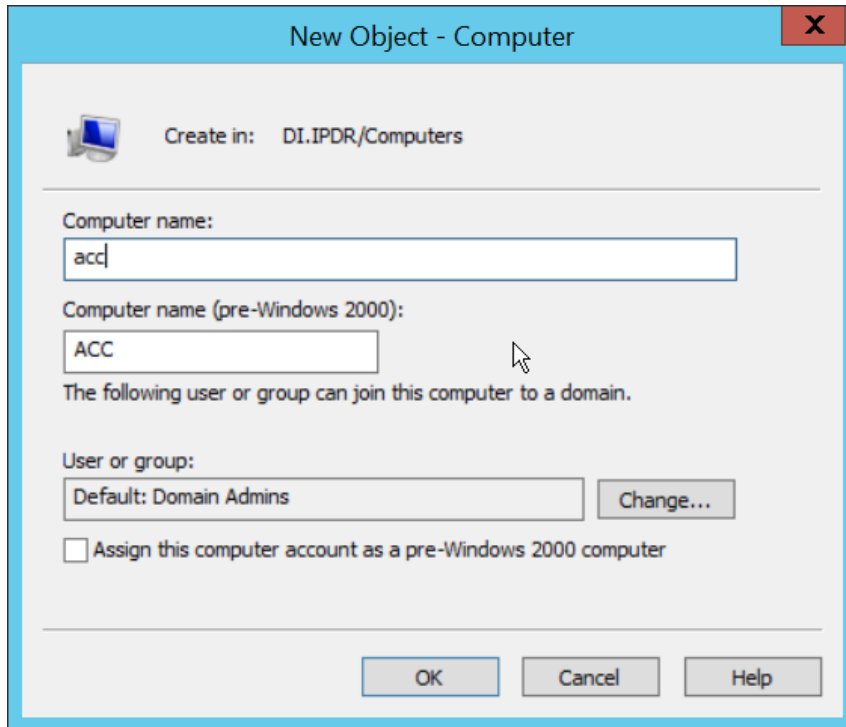
13. Click **OK**.
14. Right-click the **Users** folder in the left pane and select **New > Group**.
15. Enter **NXTNodes** as the group name.



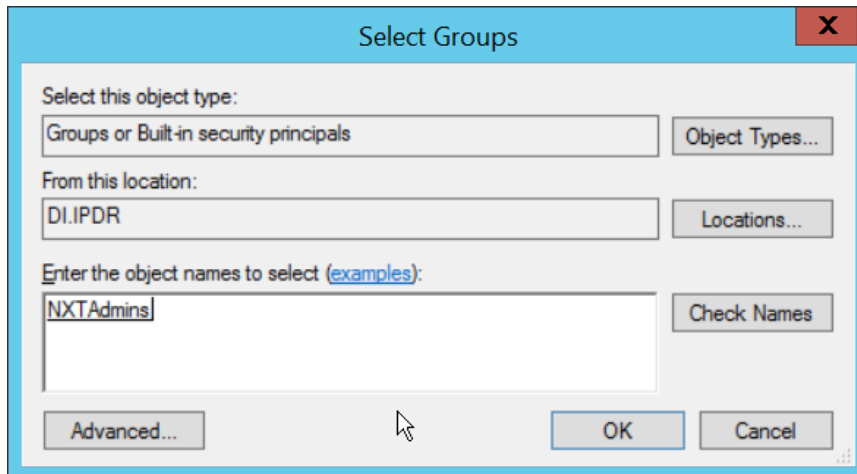
16. Click **OK**.
17. Click **Computers** in the left pane.



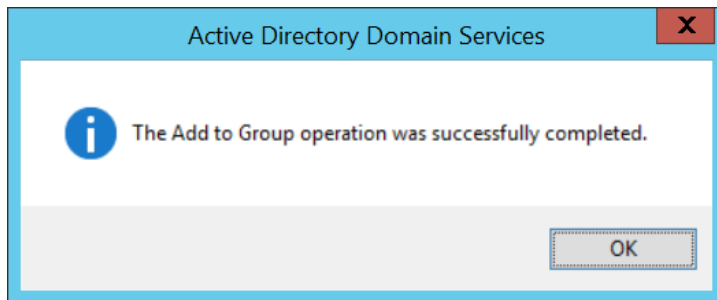
18. Right-click **Computers** in the left pane and select **New > Computer**.
19. Enter the name of the **acc** server for **CryptoniteNXT** (Node A).



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



23. Click **OK**.



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

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

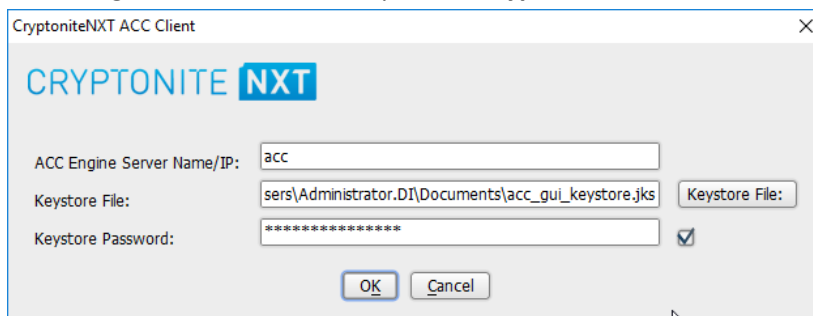
For example:

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

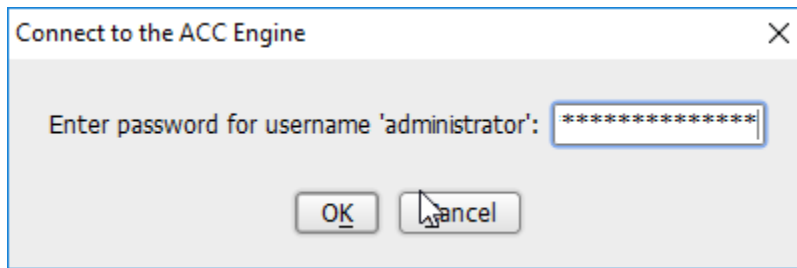
27. This will produce a keytab file. Copy this file to the CryptoniteNXT Management workstation.

### 2.7.2.2 Import Keytab File to ACC

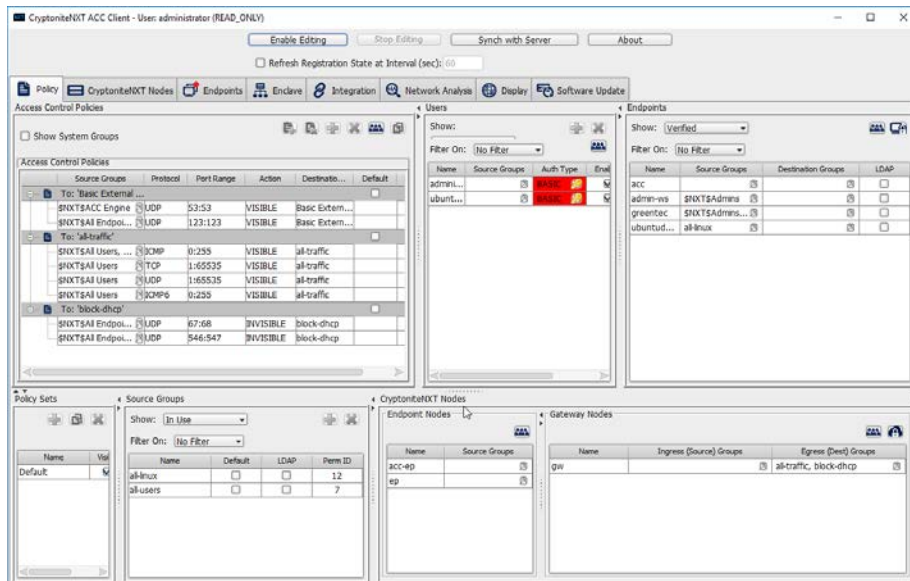
1. On the management workstation, open the **CryptoniteNXT ACC GUI**.



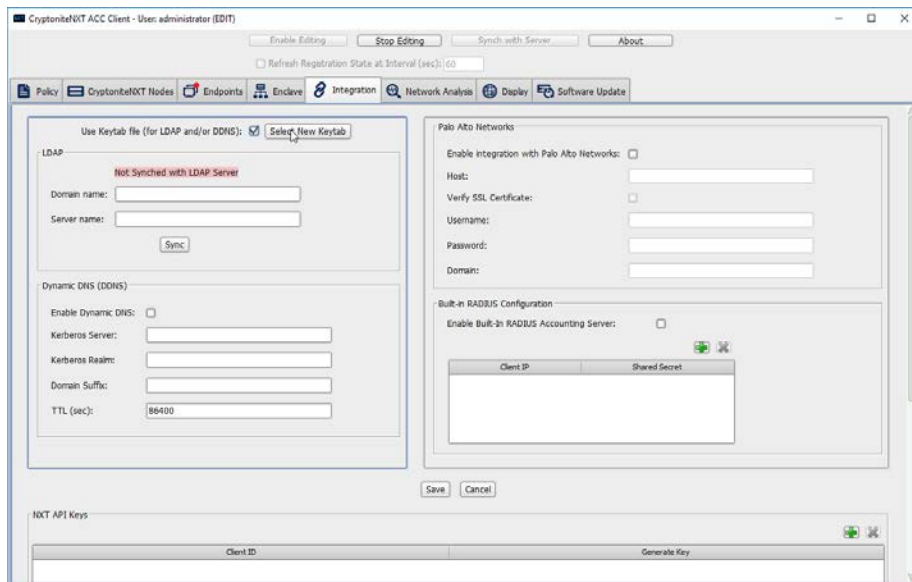
2. Click **OK**.
3. Enter the **password** configured during installation.



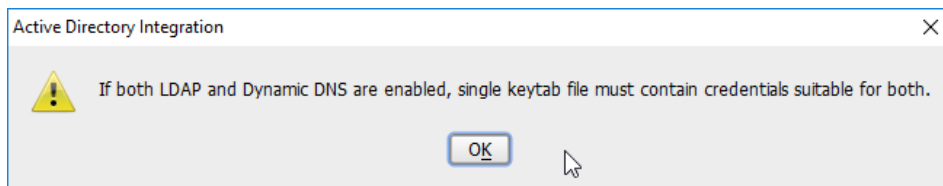
4. Click **OK**.



5. Click **Enable Editing**.
6. Click the **Integration** tab.
7. Check the box next to **Use Keytab file (for LDAP and/or DDNS):**.

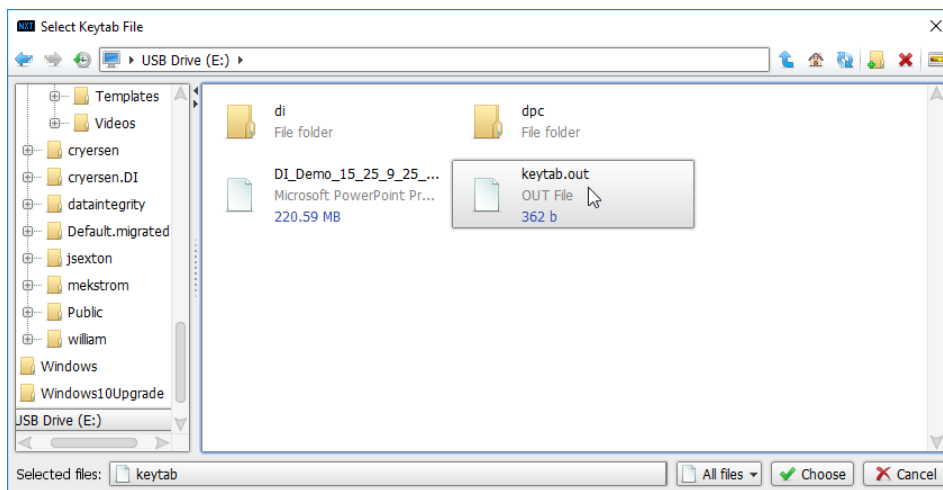


8. Click **Select New Keytab**.



9. Click **OK**.

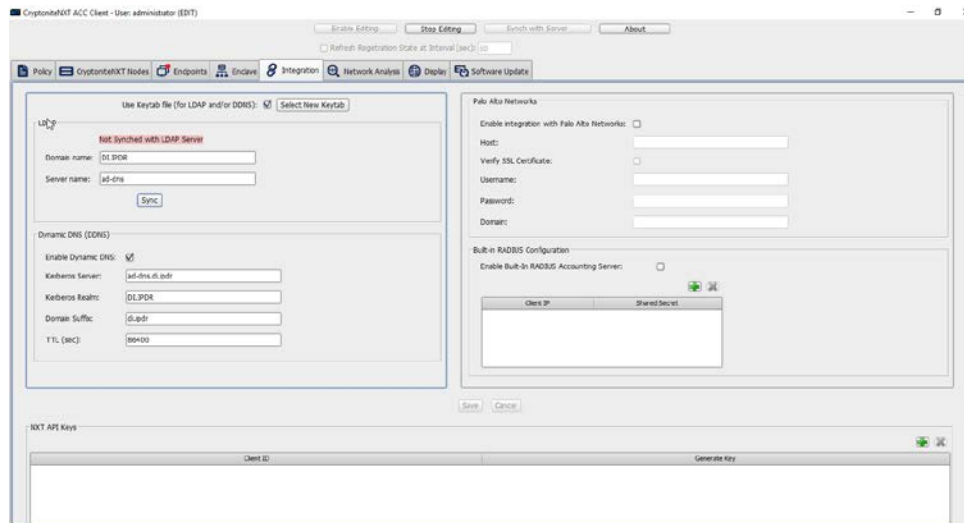
10. Navigate to the keytab file.



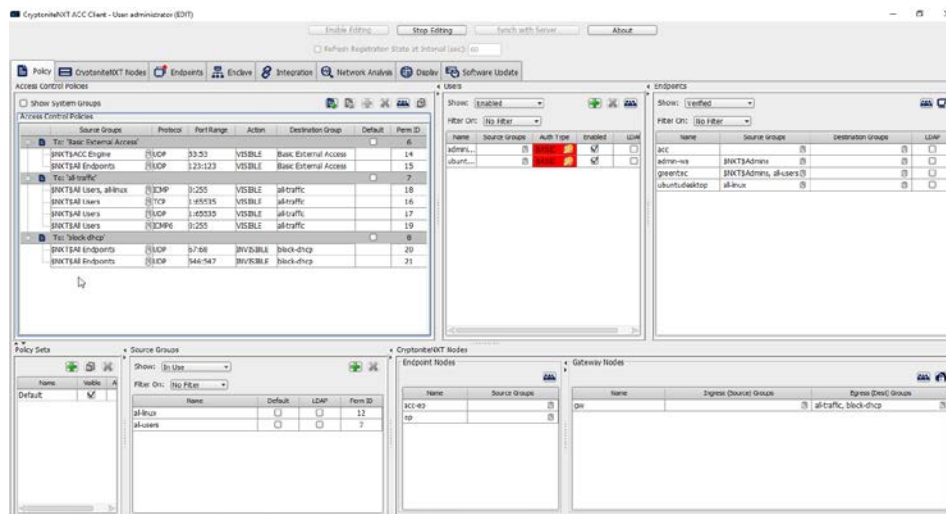
11. Click **Choose**.

12. Click **Save**.

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

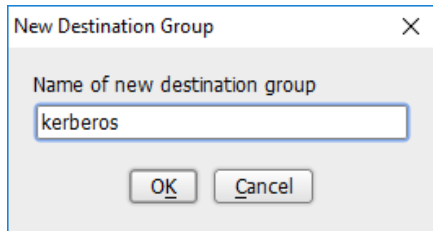


18. Click **Save**.
19. Click the **Policies** tab.

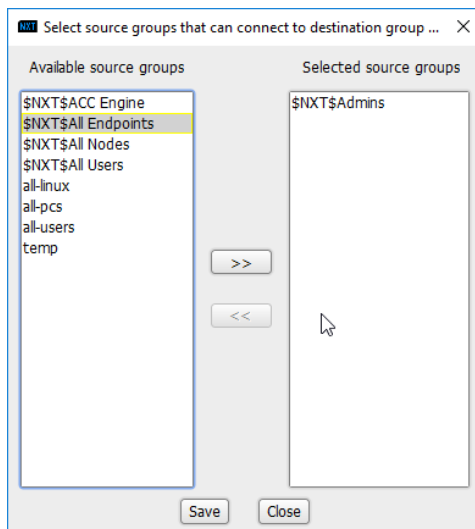


20. Right-click in the **Access Control Policies Window** and select **New Destination Group**.
21. Enter **kerberos**.

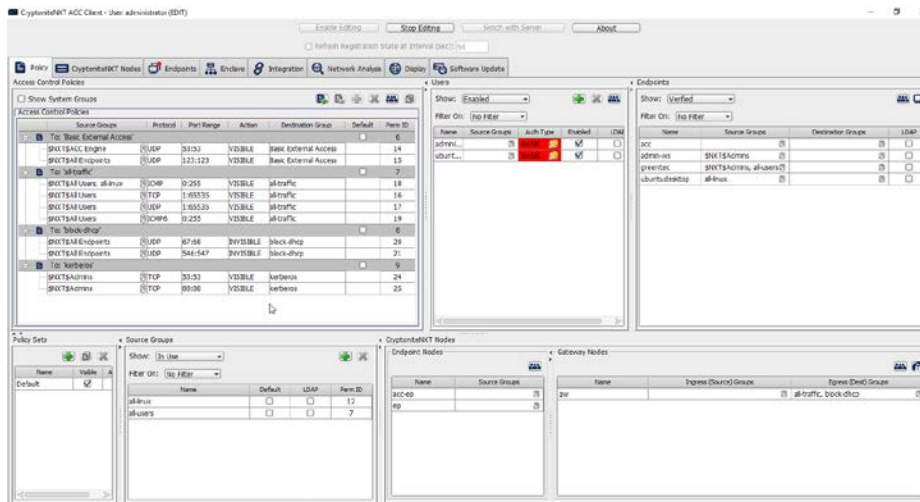




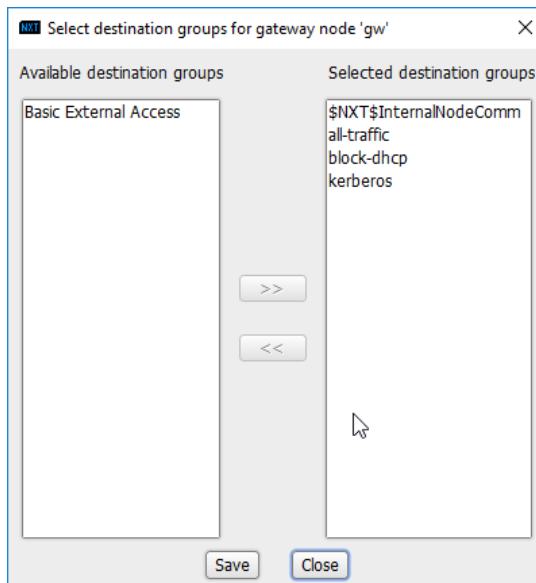
22. Click **OK**.
23. Select **TCP** under **Action**.
24. Enter 53:53 under **Port Range**.
25. Select **VISIBLE** under **Action**.
26. Click the arrow under **Source Groups**.
27. Select **\$NXT\$Admins**.
28. Click the >> button.



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



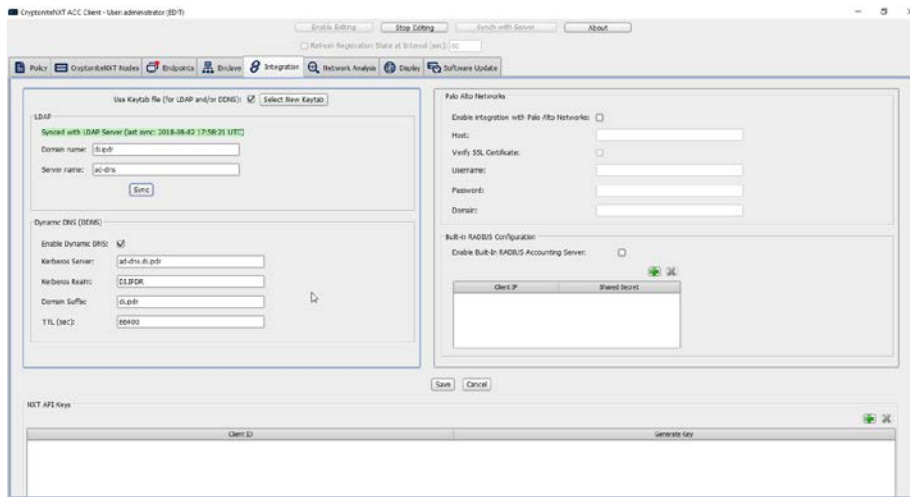
31. Repeat steps 21–29, but replace 53:53 with 88:88.
32. In the **Gateway Nodes** window, click the arrow under **Egress (Dest) Groups**.
33. Select “kerberos”.
34. Click the >> button.



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

[illegible]

NIST SP 1800-25C: Identifying and Protecting Assets Against Ransomware and Other Destructive Events



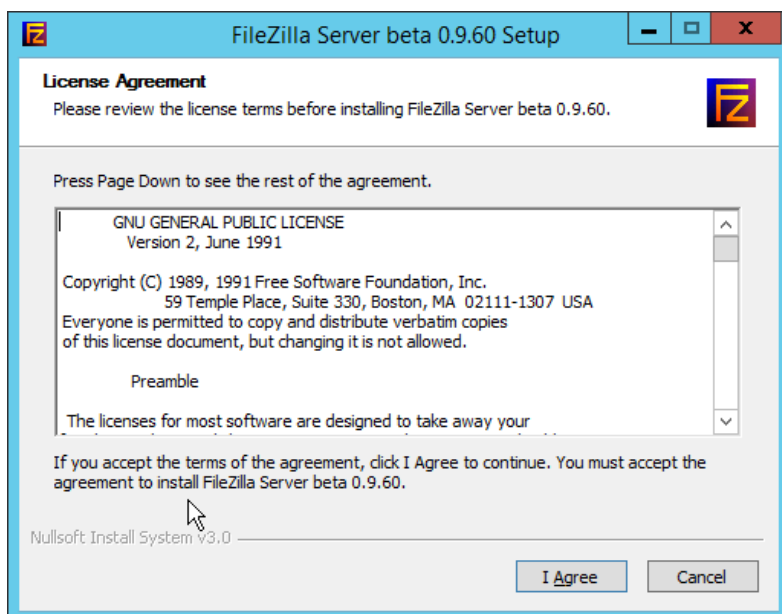
41. Click **Sync**.

## 2.8 Backups

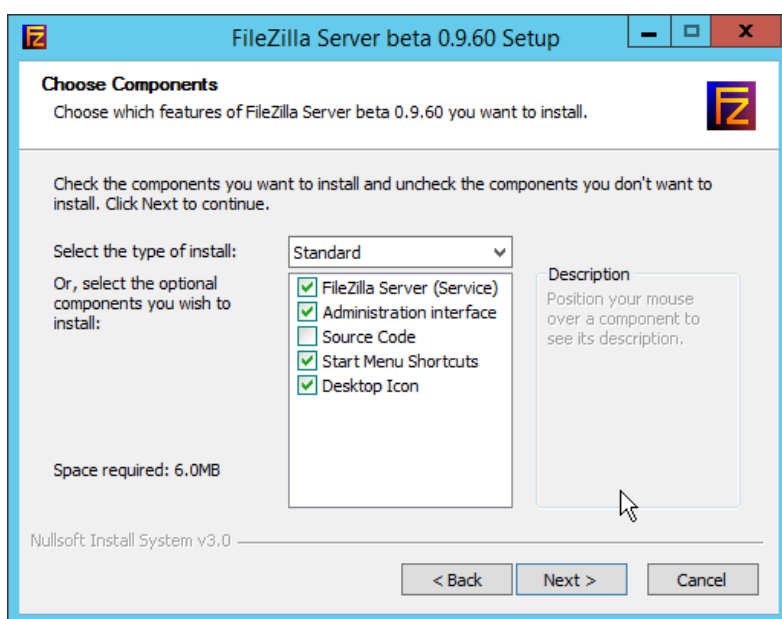
For this capability we use an integration of two open-source tools: **Duplicati** and **FileZilla**. **FileZilla** acts as a File Transfer Protocol (FTP) (over TLS) server component, while **Duplicati** acts as an encrypted backup client. This section details the installation and integration of both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

### 2.8.1 FileZilla FTPS Server Setup

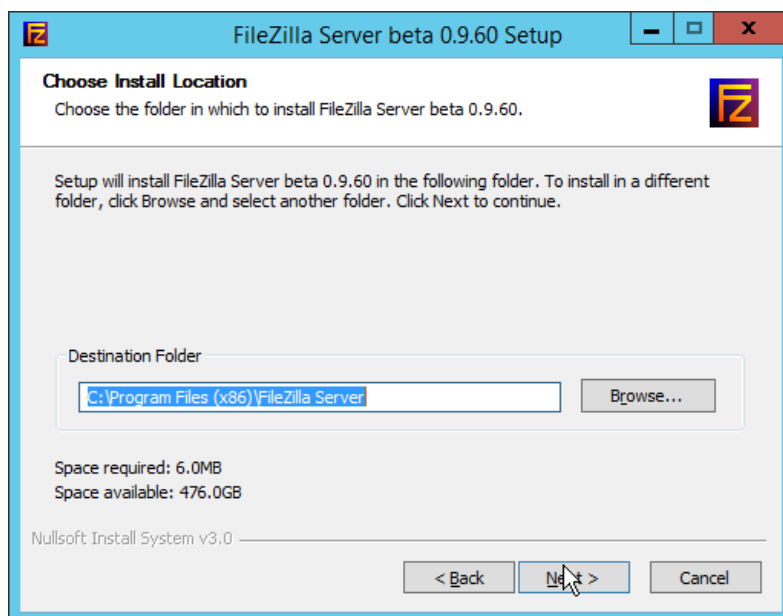
1. Run **FileZilla\_Server-0\_9\_60\_2.exe**.



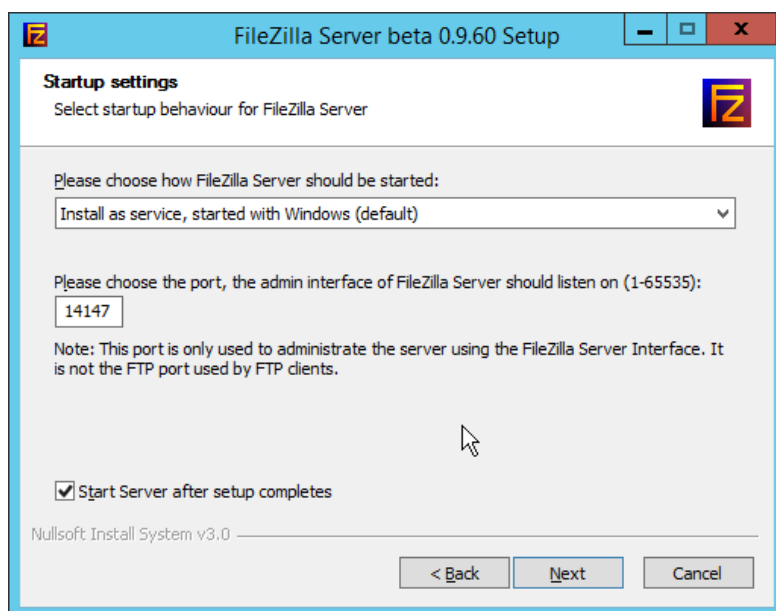
2. Click **I Agree**.
3. Select **Standard** from the drop-down menu.



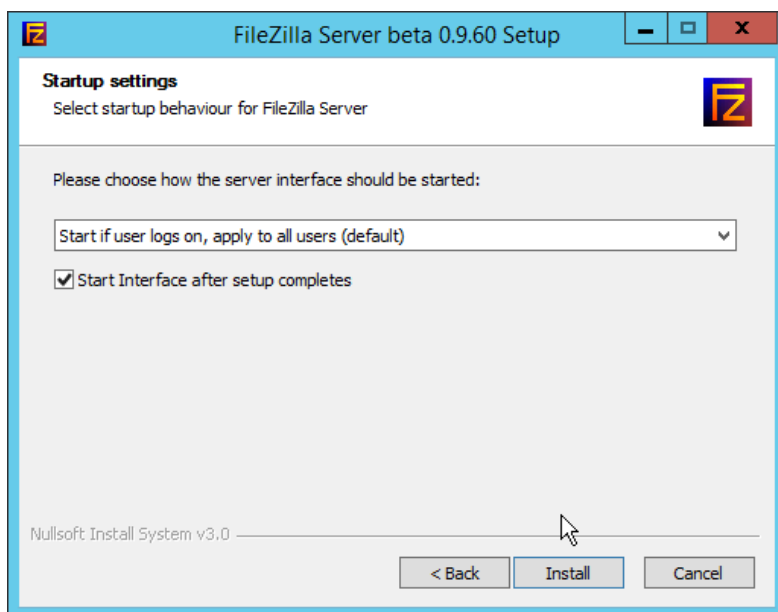
4. Click **Next**.



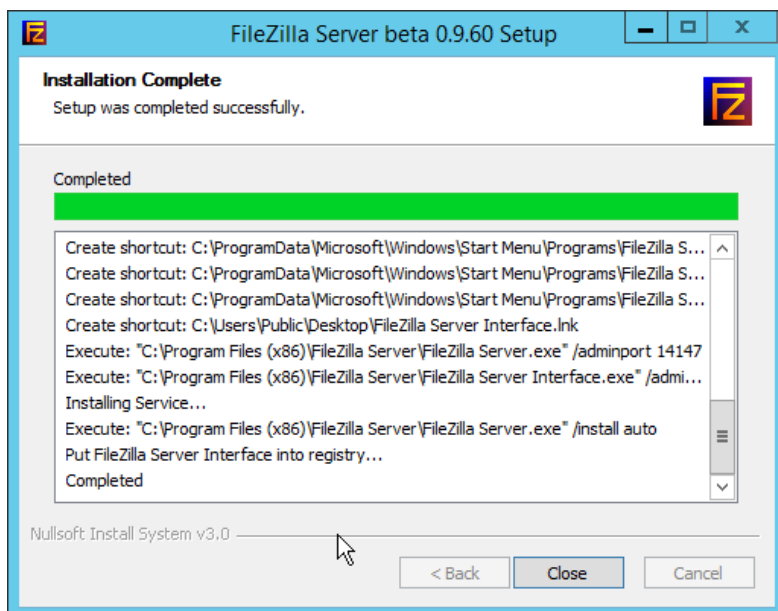
5. Click **Next**.
6. Select **Install as service, started with Windows (default)** from the drop-down.
7. Specify a port (for the administrator interface to run on) if desired (the default is 14147).
8. Ensure the box next to **Start Server after setup completes** is checked.



9. Click **Next**.



10. Click **Install**.



11. Click **Close**.

## 2.8.2 FileZilla Configuration

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

2. Click **Edit > Settings**.

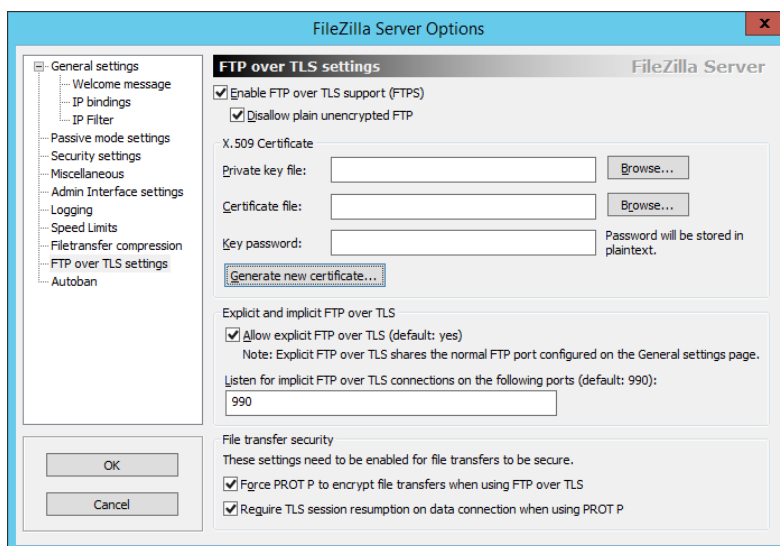
The screenshot shows the 'FileZilla Server Options' dialog box with the 'General settings' tab selected. The left sidebar lists various settings categories, with 'General settings' highlighted. The main area contains three sections: 'Connection settings' with fields for 'Listen on these ports' (21) and 'Max. number of users' (0); 'Performance settings' with 'Number of threads' (2); and 'Timeout settings' with 'Connections timeout' (120), 'No Transfer timeout' (120), and 'Login timeout' (60). Each timeout field includes a descriptive note about the range and purpose of the value. At the bottom are 'OK' and 'Cancel' buttons.

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

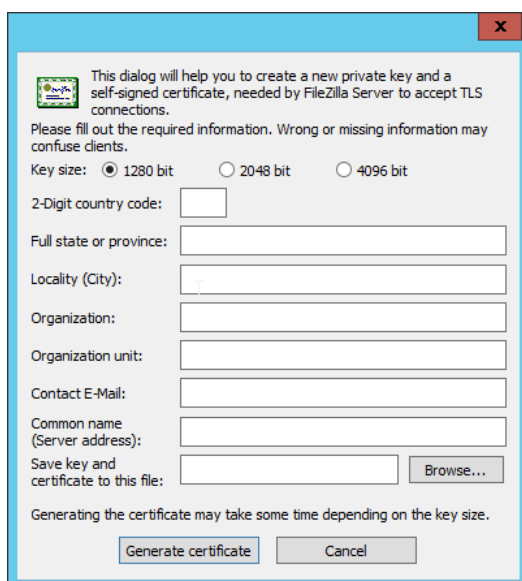
The screenshot shows the 'FileZilla Server Options' dialog box with the 'FTP over TLS settings' tab selected. The left sidebar highlights 'FTP over TLS settings'. The main area contains several sections: 'Enable FTP over TLS support (FTPS)' with a checked checkbox and an unchecked 'Disallow plain unencrypted FTP' checkbox; 'X.509 Certificate' section with fields for 'Private key file' and 'Certificate file' (each with a 'Browse...' button) and a 'Key password' field; a 'Generate new certificate...' button; 'Explicit and implicit FTP over TLS' section with a checked 'Allow explicit FTP over TLS (default: yes)' checkbox and a note; a field for 'Listen for implicit FTP over TLS connections on the following ports (default: 990)' with the value '990'; and 'File transfer security' section with two checked checkboxes: 'Force PROTP to encrypt file transfers when using FTP over TLS' and 'Require TLS session resumption on data connection when using PROTP'. At the bottom are 'OK' and 'Cancel' buttons.

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

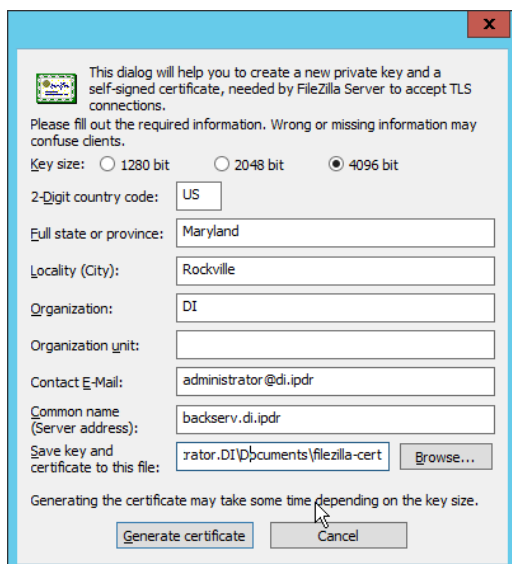




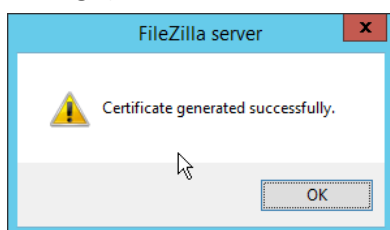
6. Click **Generate new certificate**.



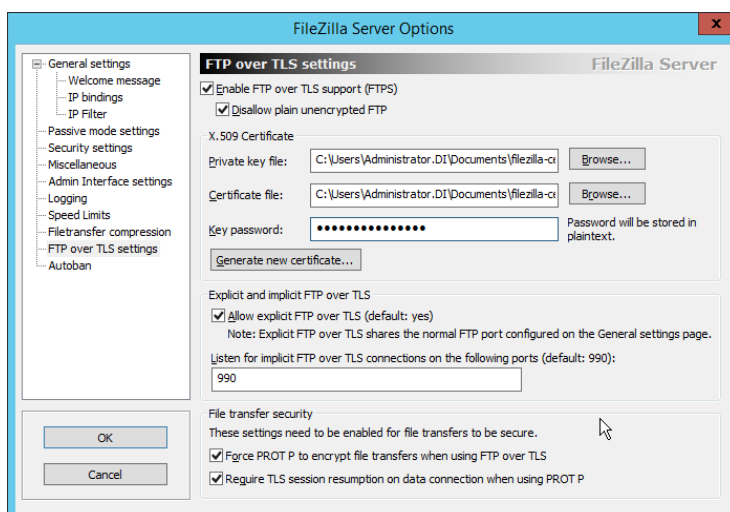
7. Select **4096 bit** for **Key Size**.
8. Enter the information for the certificate specific to your organization.
9. For the **common name**, enter the address of the server on which this is installed.
10. Click **Browse** and specify a file location for the certificate.



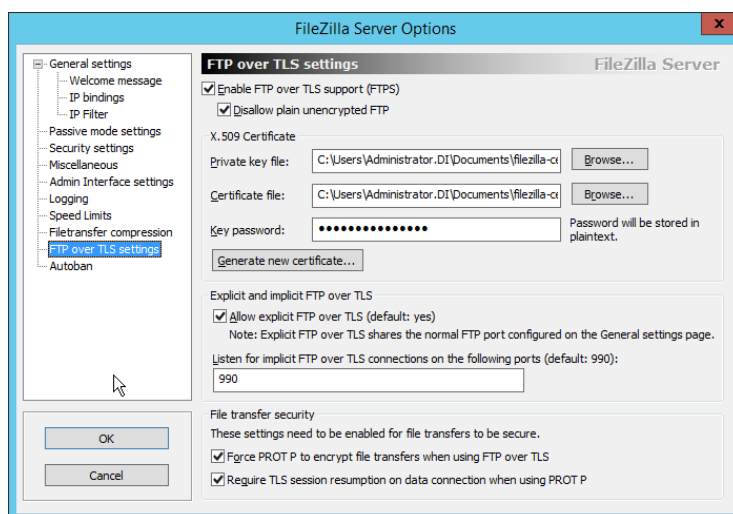
11. Click **Generate certificate**. (The file now contains both the private key and the certificate. These can be separated, for ease of use, as long as the correct file locations are specified in the settings.)



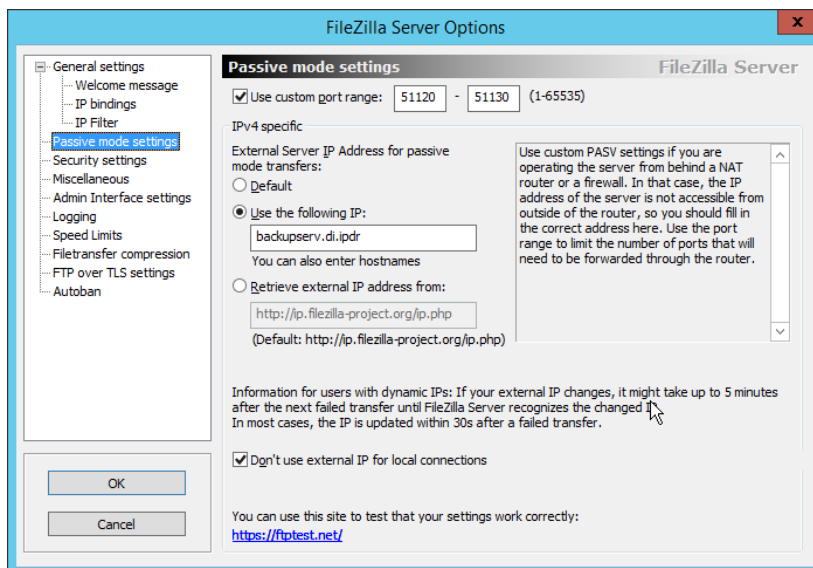
12. Click **OK**.



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



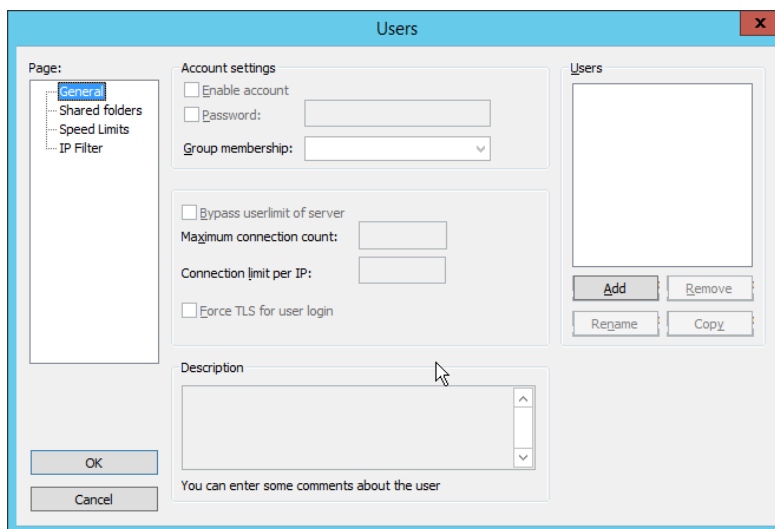
16. Click **Passive mode settings**. Check the box next to **Use custom port range**. (This is necessary in cases of a local server behind Network Address Translation (NAT) or a firewall.)
17. Enter a range of ports for passive mode to use. Ensure that these ports are allowed through the firewall.
18.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



20. Click **OK**.

## 2.8.3 Add a User to FileZilla

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

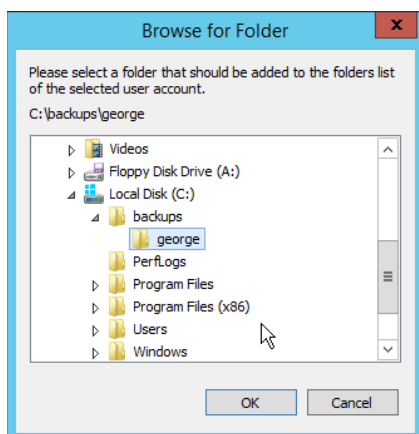


2. Click **Add**.

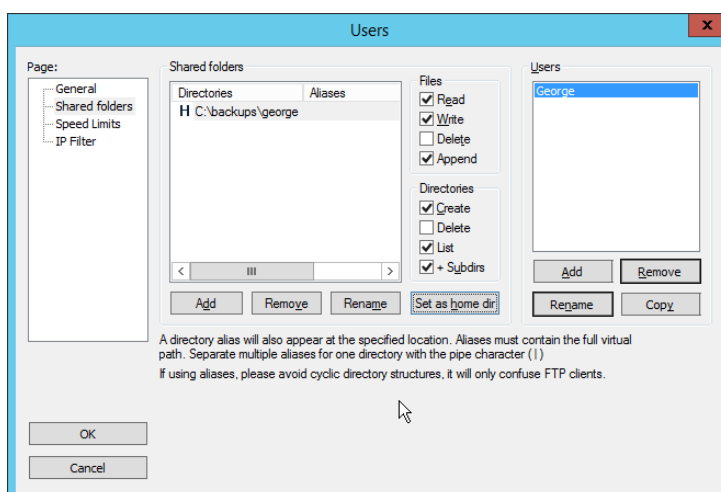
3. Enter a **name** for the user.

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

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



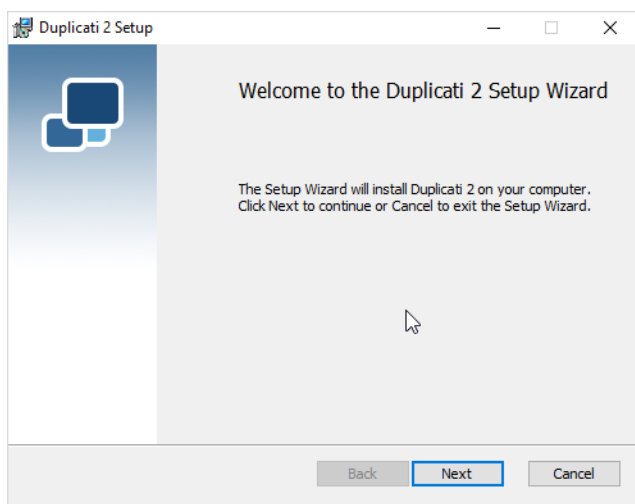
10. Select a place for backups *for this user* to be stored.
11. Check the boxes next to **Write** and **Append**, under **Files**.
12. Check the box next to **Create**, under **Directories**.
13. Select this entry and click **Set as home dir**.



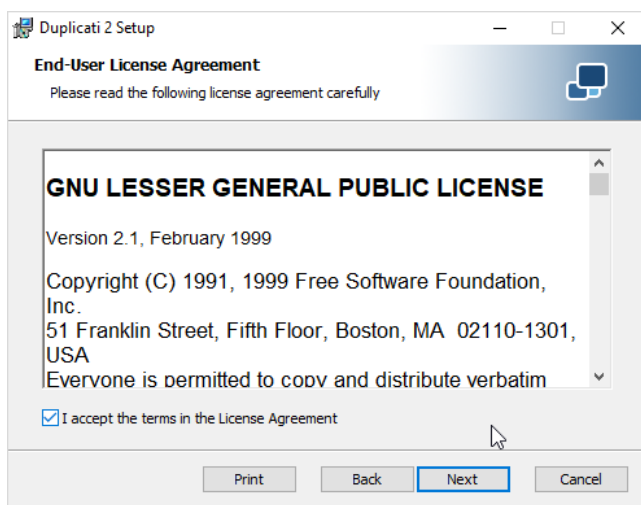
14. Click **OK**.

## 2.8.4 Duplicati Client Installation (Windows)

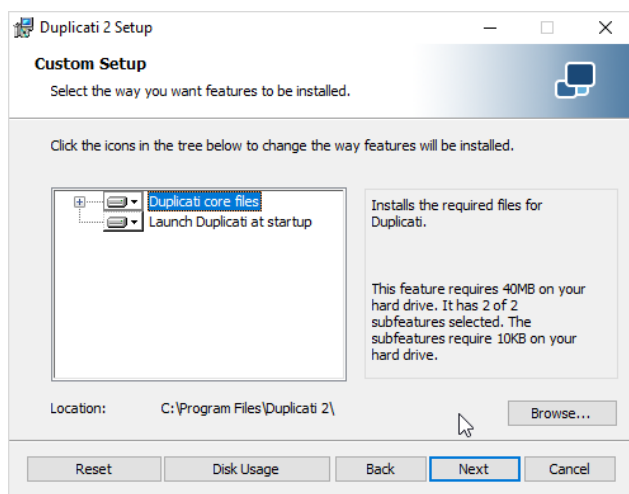
1. On the client machine, run **duplicati-2.0.3.3\_beta\_2018-04-02-x64.msi**.



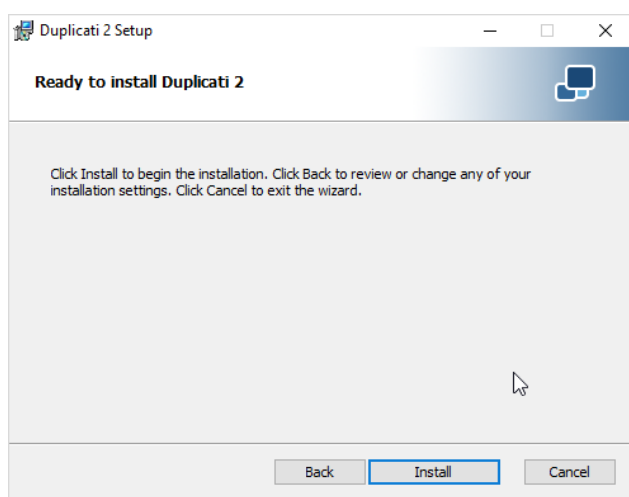
2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



4. Click **Next**.

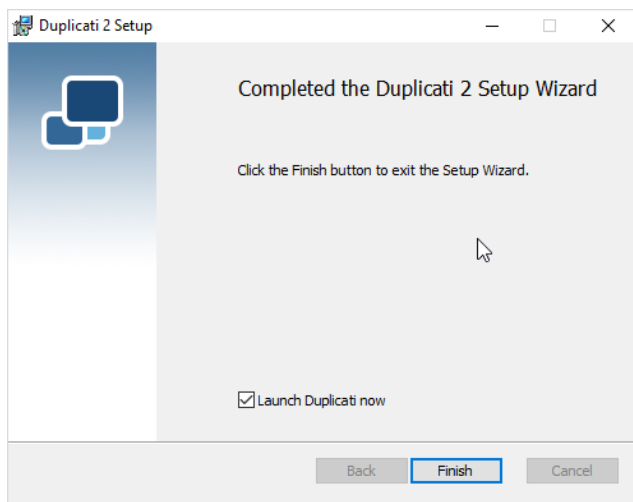


5. Click **Next**.



6. Click **Install**.





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

## 2.8.5 Duplicati Client Installation (Ubuntu)

1. Install mono by using the following command:

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

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

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

3. Install Duplicati by using the following command:

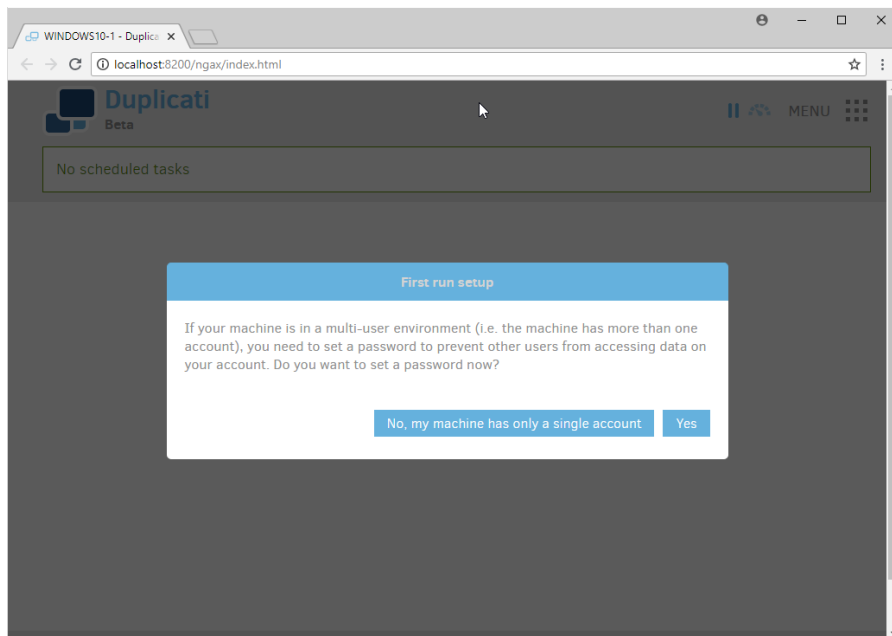
```
> sudo dpkg -i duplicati_2.0.3.9-1_all.deb
```

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

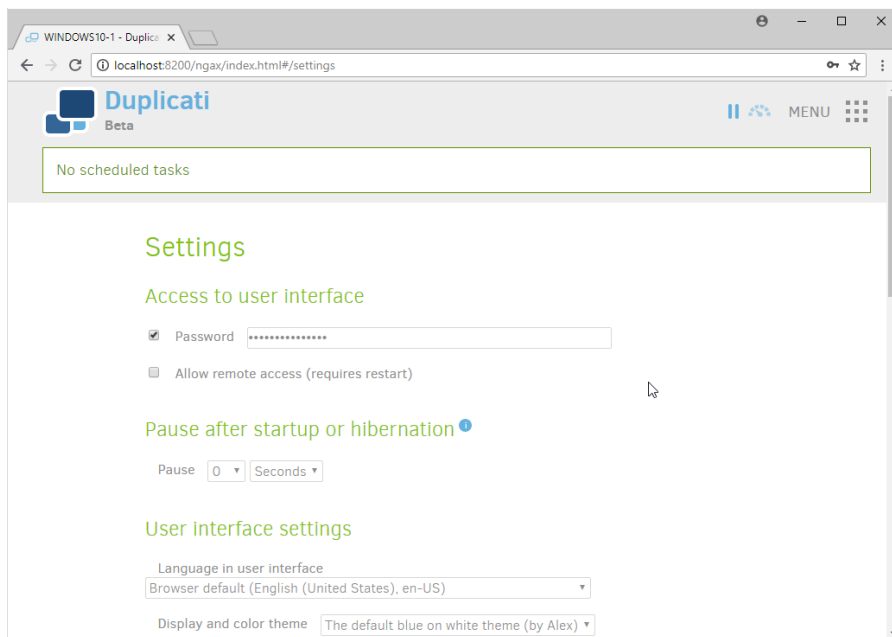
```
> sudo systemctl enable duplicati
```

## 2.8.6 Configure Duplicati

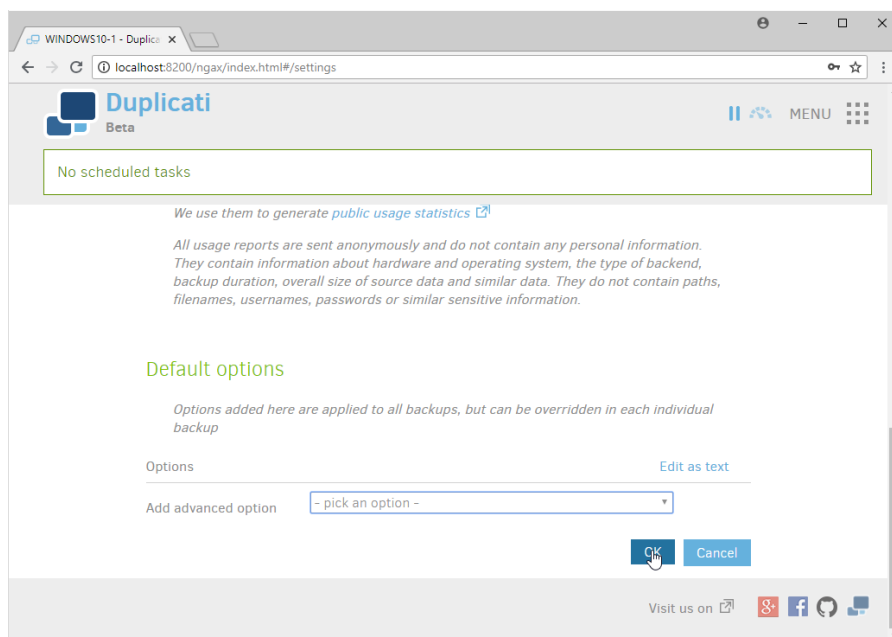
1. When it first starts, **Duplicati** will have a **First run setup**.



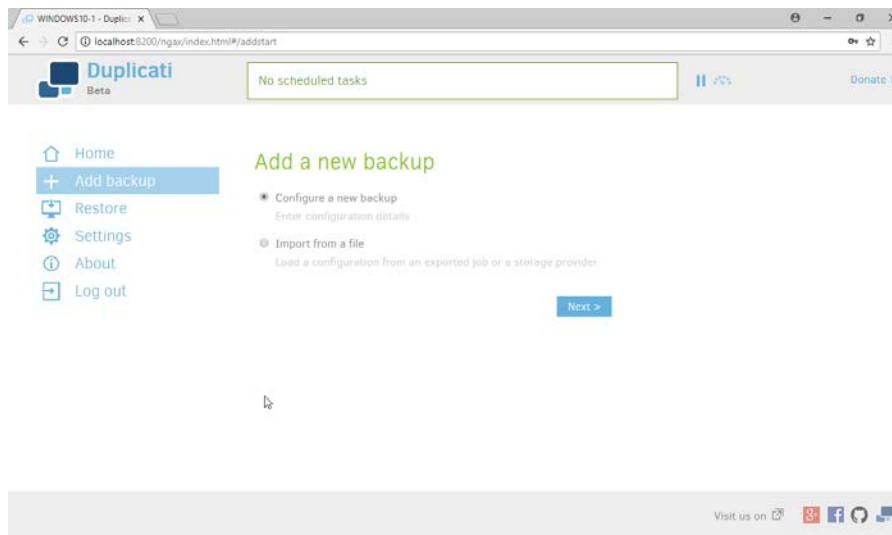
2. Click **Yes**.
3. Check the box next to **Password**.



4. Enter a **password**.



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



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

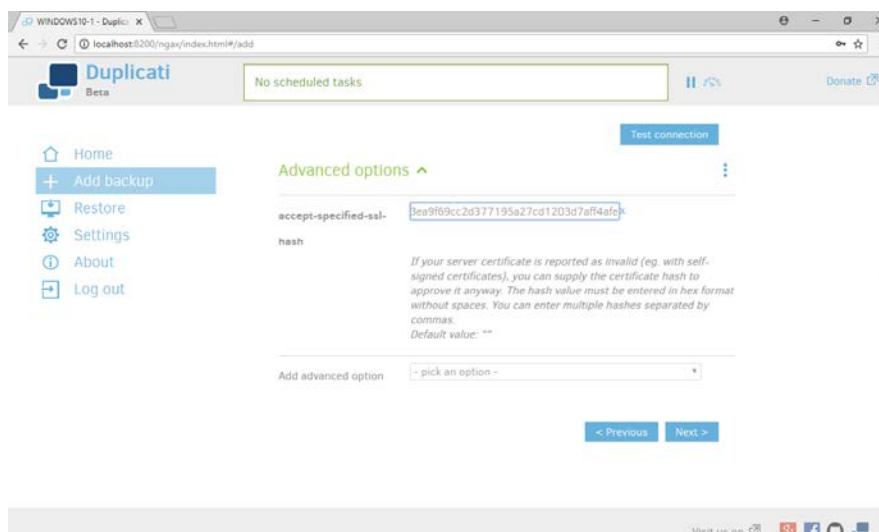
The screenshot shows the Duplicati Beta web interface in a browser window. The address bar displays 'localhost:8200/ngax/index.html#/add'. The interface has a sidebar on the left with links: Home, Add backup, Restore, Settings, About, and Log out. The main content area shows a progress bar with five steps: 1. General, 2. Destination, 3. Source Data, 4. Schedule, and 5. Options. The 'General' step is active. Below the progress bar, the 'General backup settings' section includes fields for Name (filled with 'files'), Encryption (set to 'AES-256 encryption, built in'), Passphrase (masked with dots), and Repeat Passphrase (masked with dots). There are links for 'Show', 'Generate', and 'Strength: Strong'. A 'Next >' button is at the bottom right.

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

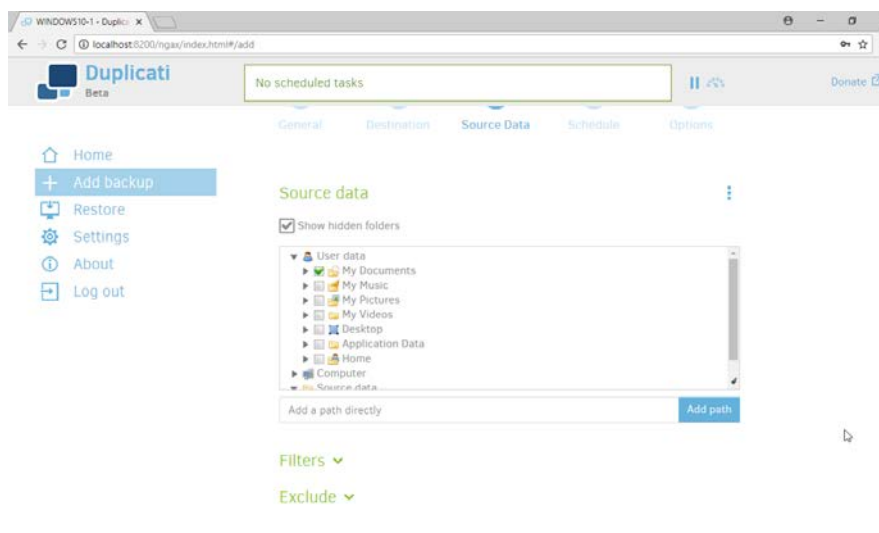
The screenshot shows the Duplicati Beta web interface in a browser window, now on the 'Backup destination' step. The sidebar is the same. The progress bar shows step 2, 'Destination', is active. The 'Backup destination' section includes a 'Storage Type' dropdown menu set to 'FTP', a checked 'Use SSL' checkbox, a 'Server and port' field with 'backupserv.di.ipdr' and a port field with '990', a 'Path on server' field with 'windows101backups', a 'Username' field with 'George', and a 'Password' field (masked). A 'Test connection' button is below these fields. An 'Advanced options' section is collapsed. At the bottom, there are '< Previous' and 'Next >' buttons.

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

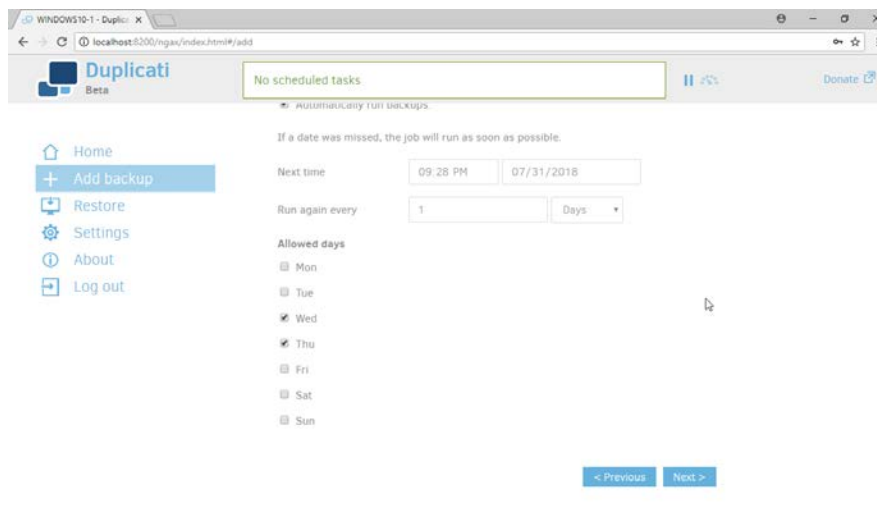
19. If you receive an error about a certificate, you can go to **Advanced Options**, select **accept-specified-ssl-hash**, and enter the **thumbprint** from the server's certificate.



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

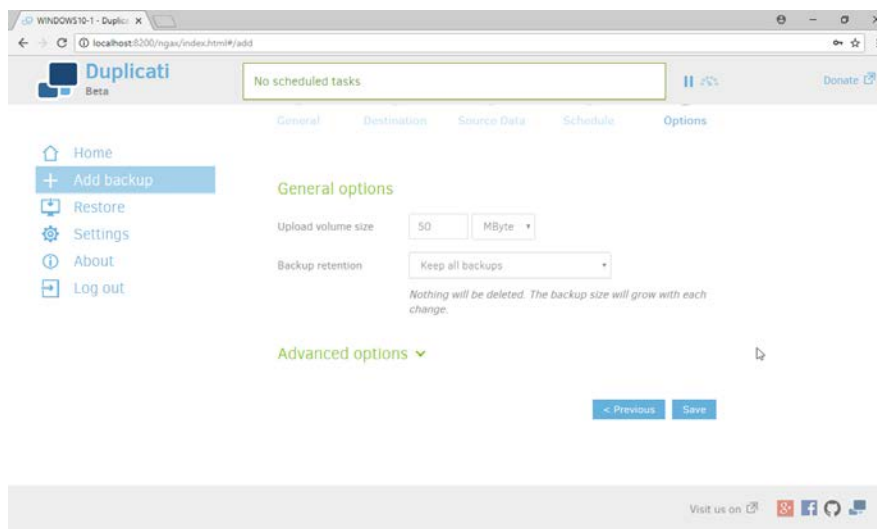


22. Click **Next**.
23. Select a backup schedule according to your organization's needs.

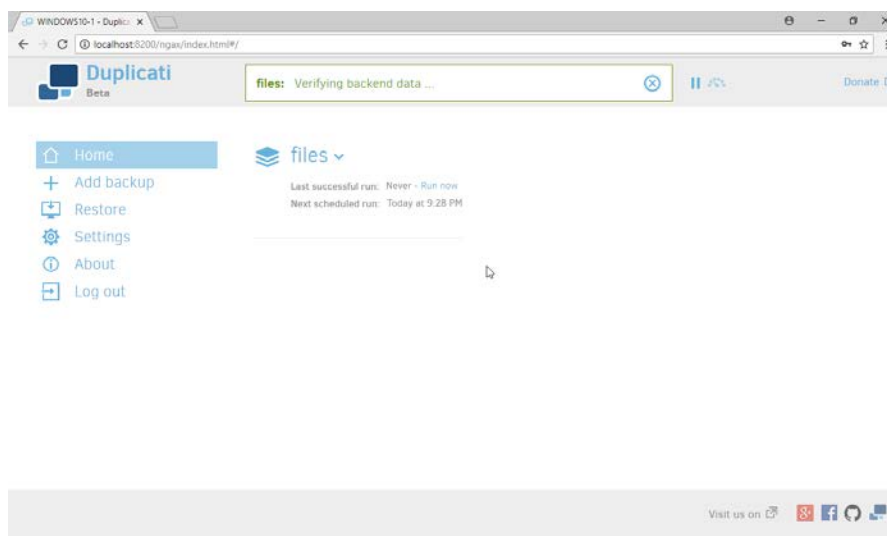


24. Click **Next**.

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



26. Click **Save**.



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

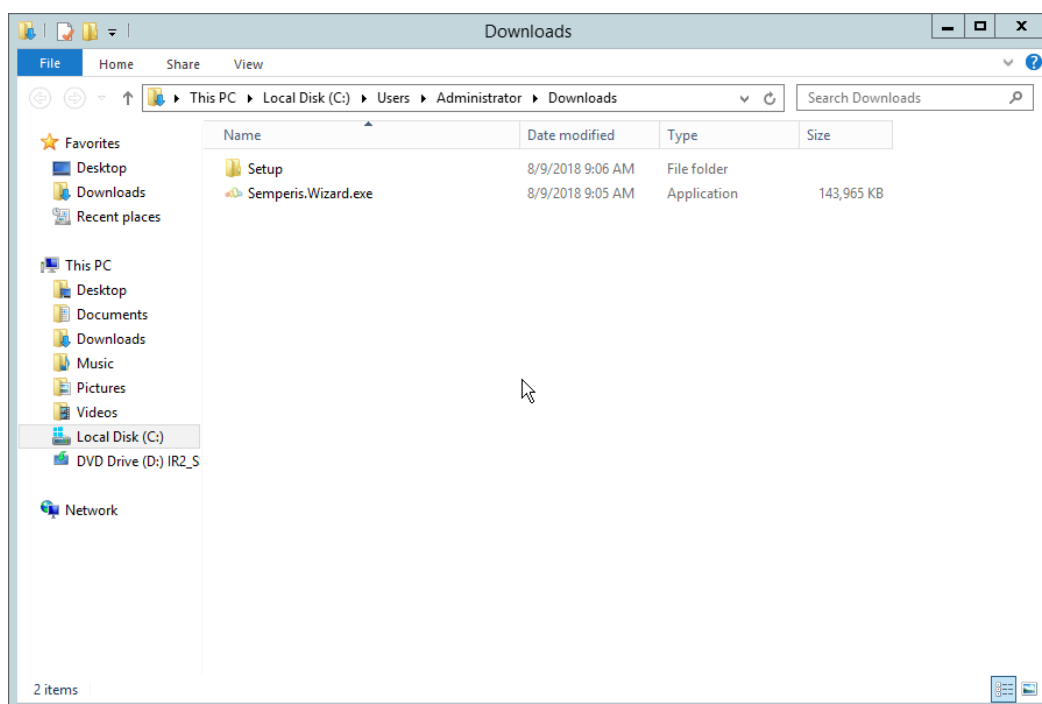
## 2.9 Semperis Active Directory Forest Recovery

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

- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- not joined to the Active Directory domain it is protecting
- SQL Express is not installed on the machine, but the installer SQLEXPRESS\_x64\_ENU.exe is downloaded.

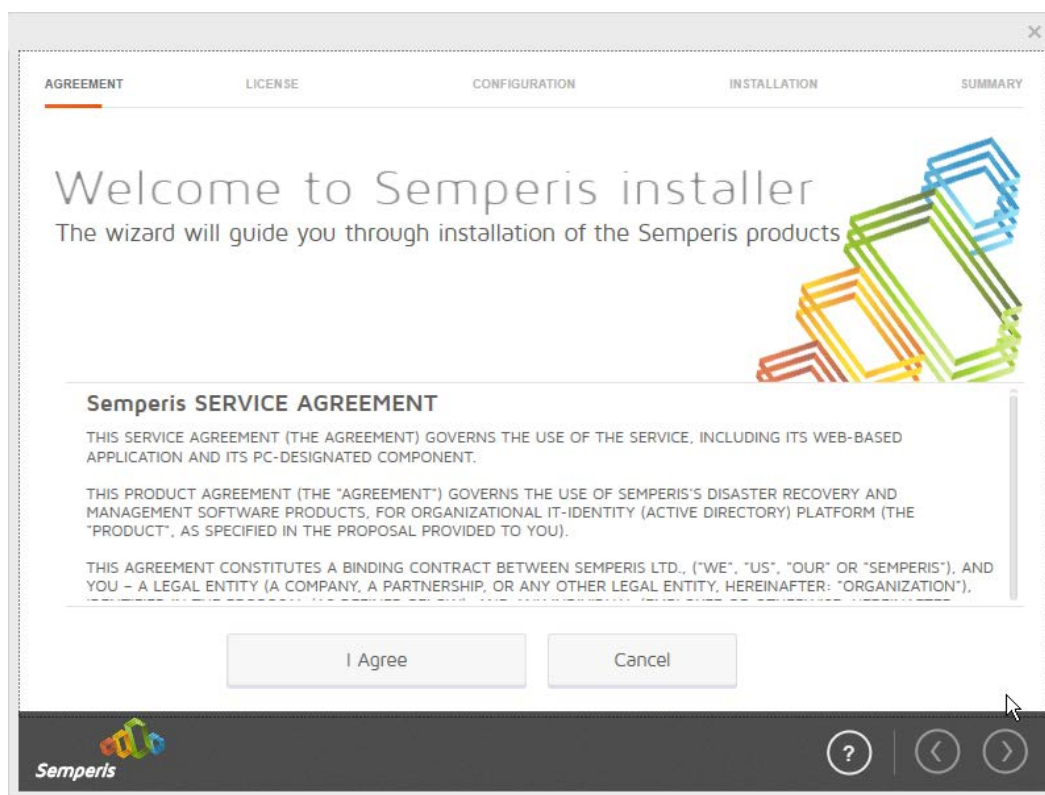
### 2.9.1 Install Semperis ADFR

1. Place the **SQLEXPRESS\_x64\_ENU.exe** installer in a directory called Setup, and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it).

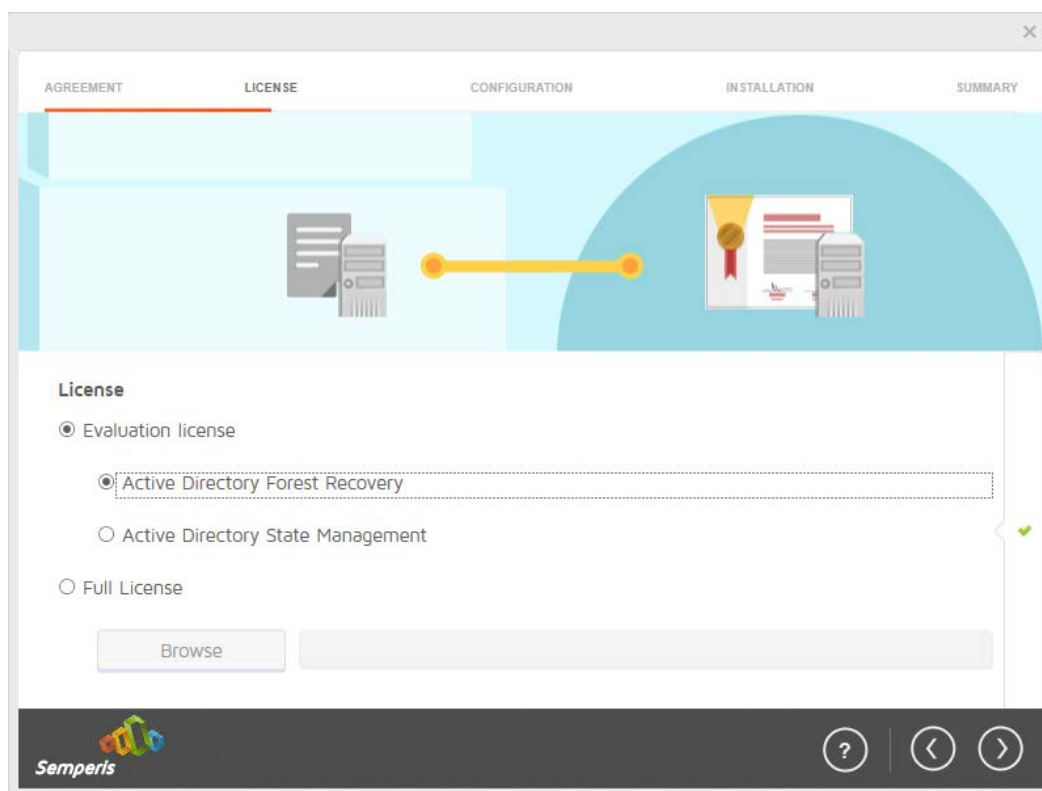


2. If prompted to restart the computer, do so.

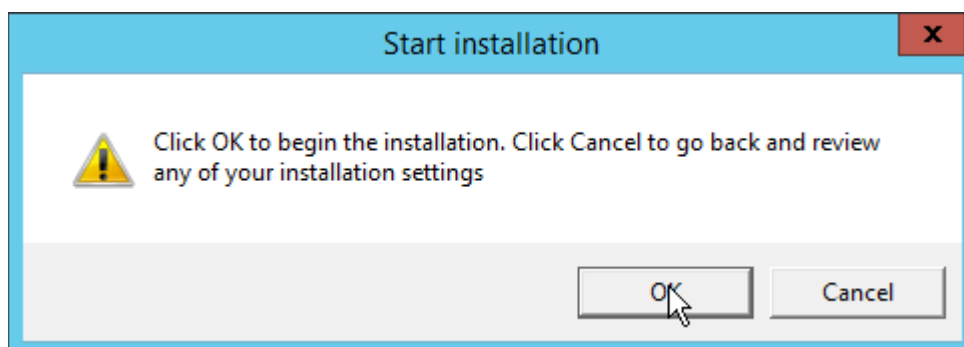




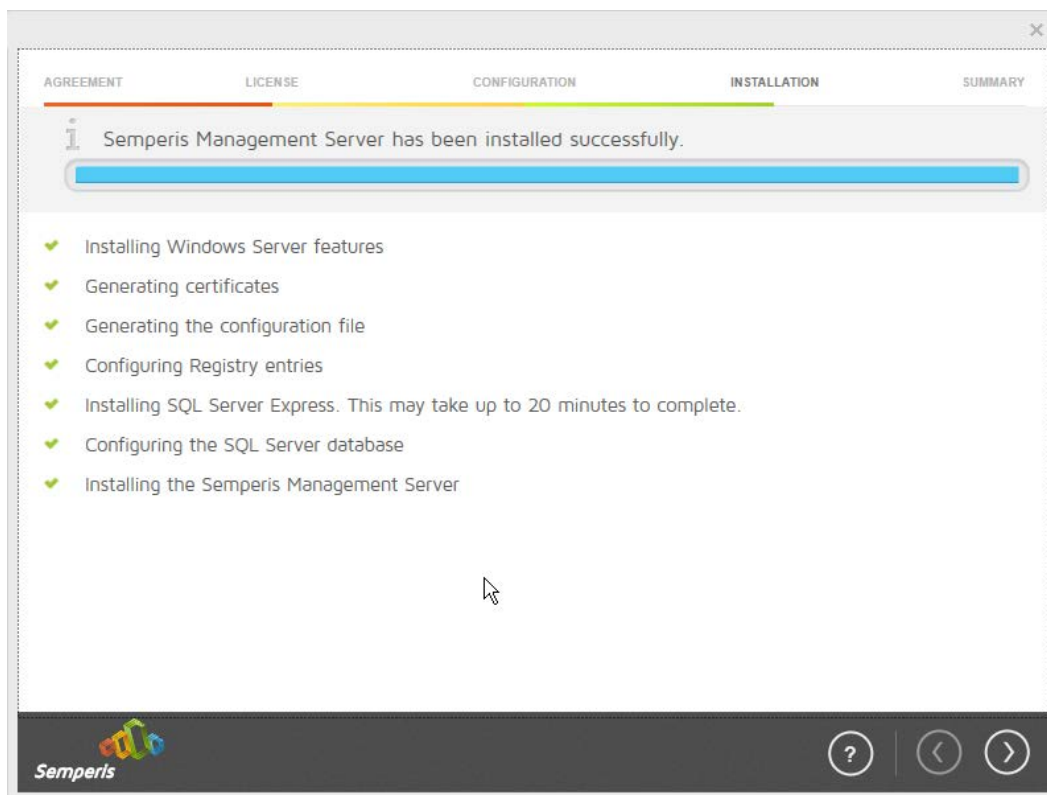
3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory Forest Recovery**.



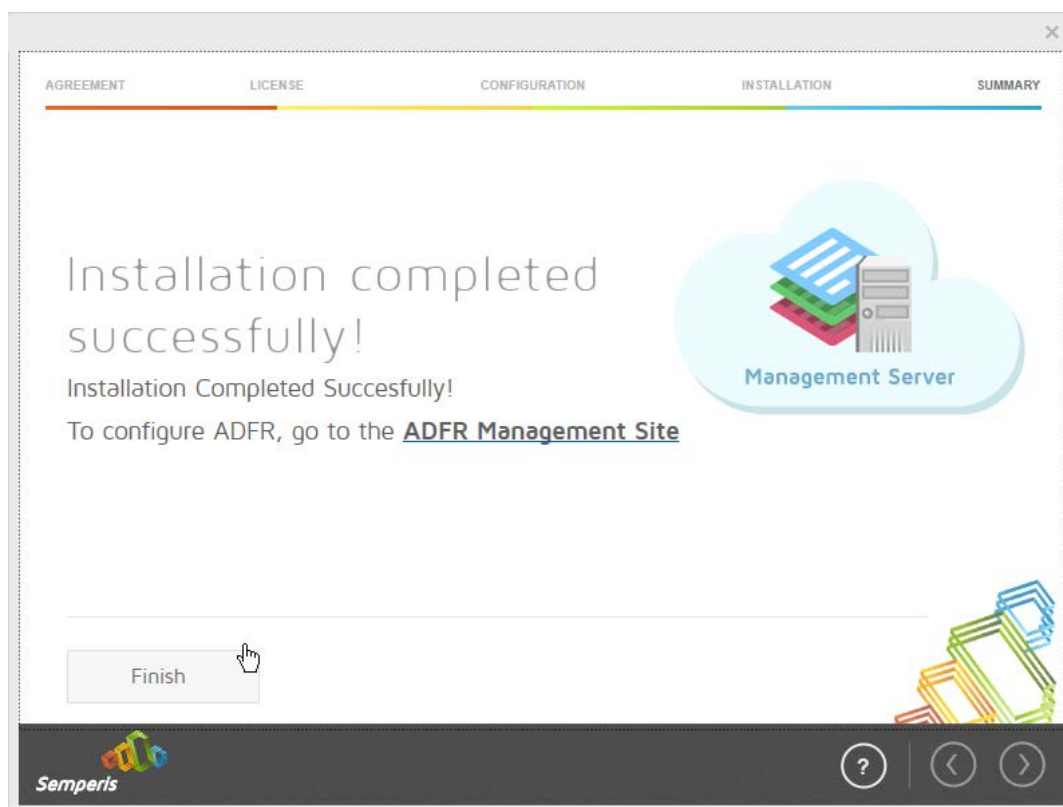
6. Click the > button.



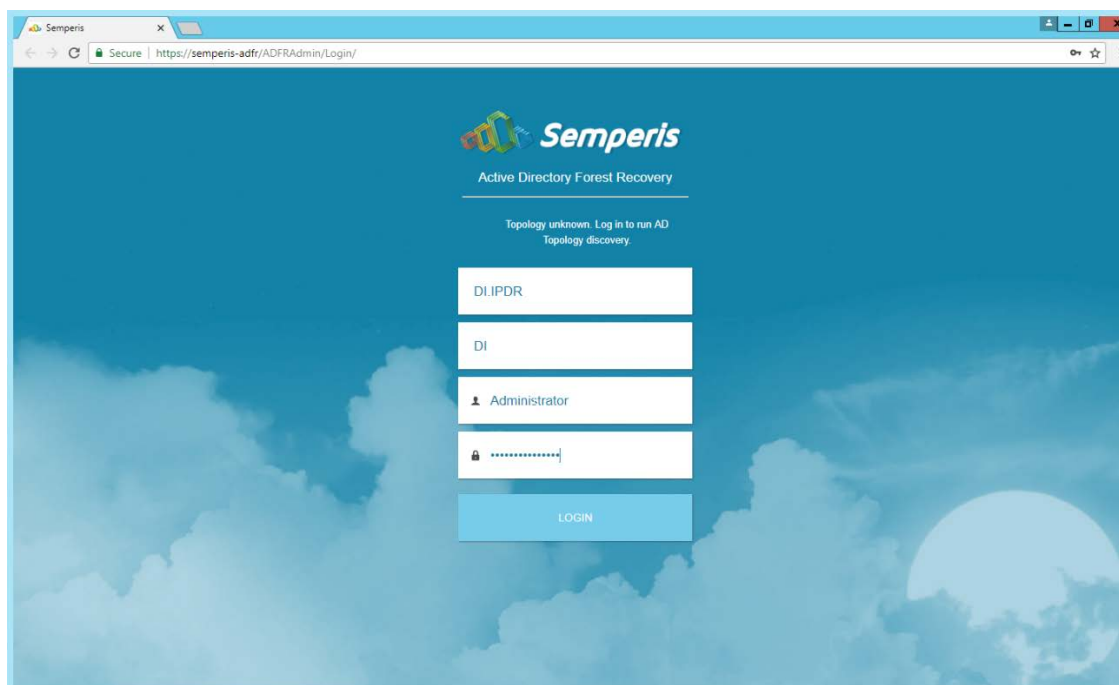
7. Click **OK**.
8. Wait for the installation to complete.



9. Click the > button.

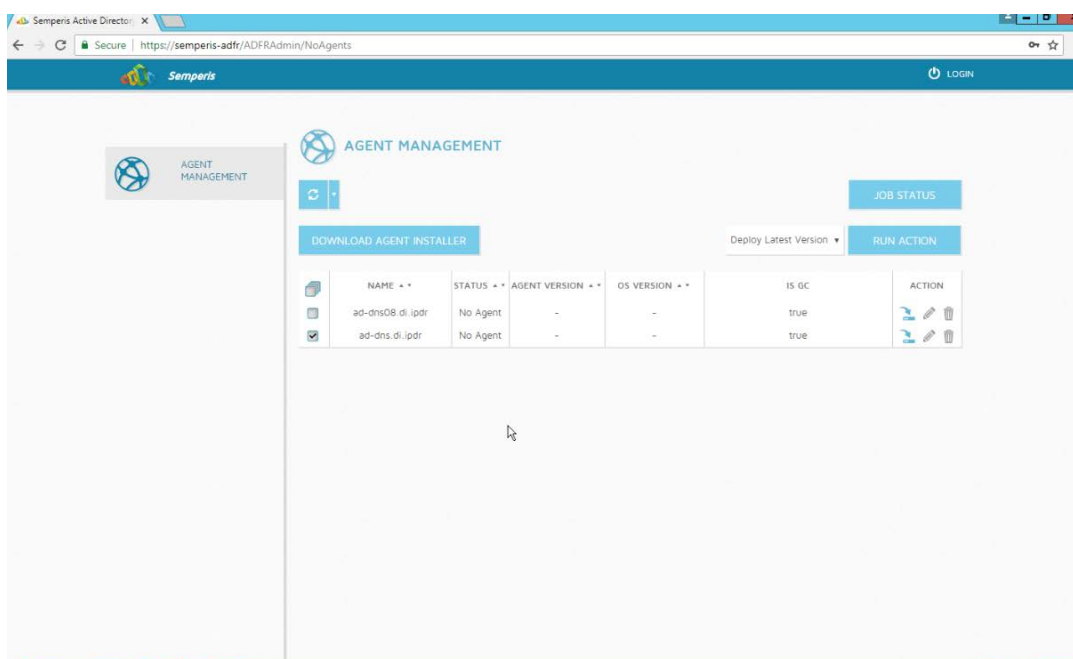


10. Click **Finish**.
11. There should now be a shortcut on the desktop linking to the web console for **Semperis ADFR**.
12. On the login page, enter the full domain as well as the NetBIOS name.
13. Enter the **username** and **password** of an administrator on the domain.



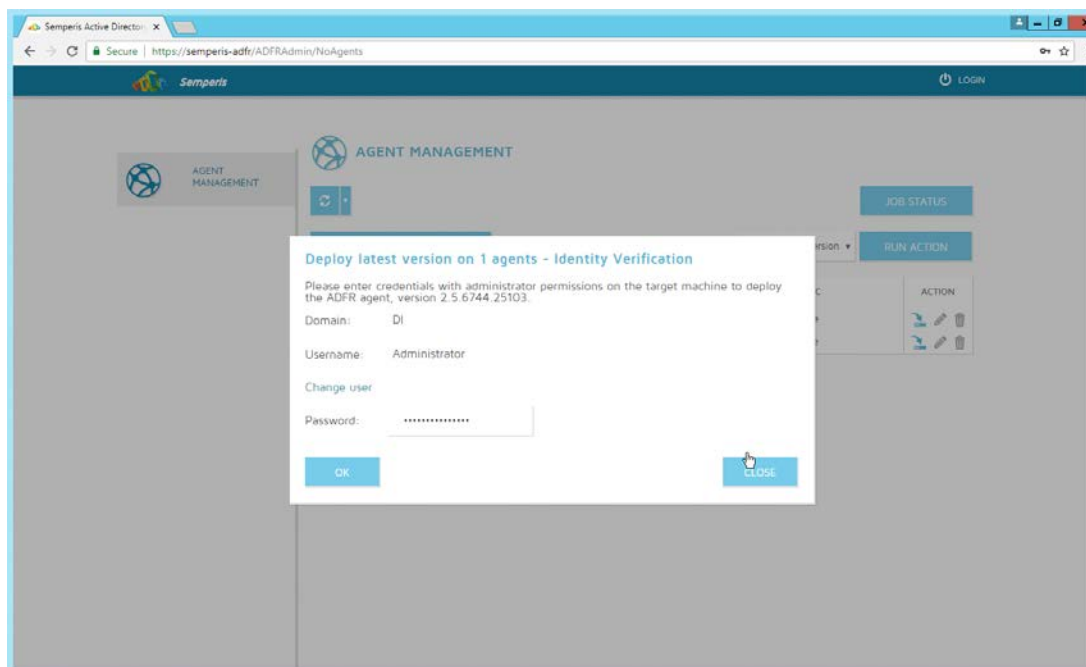
14. Click **Login**.

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

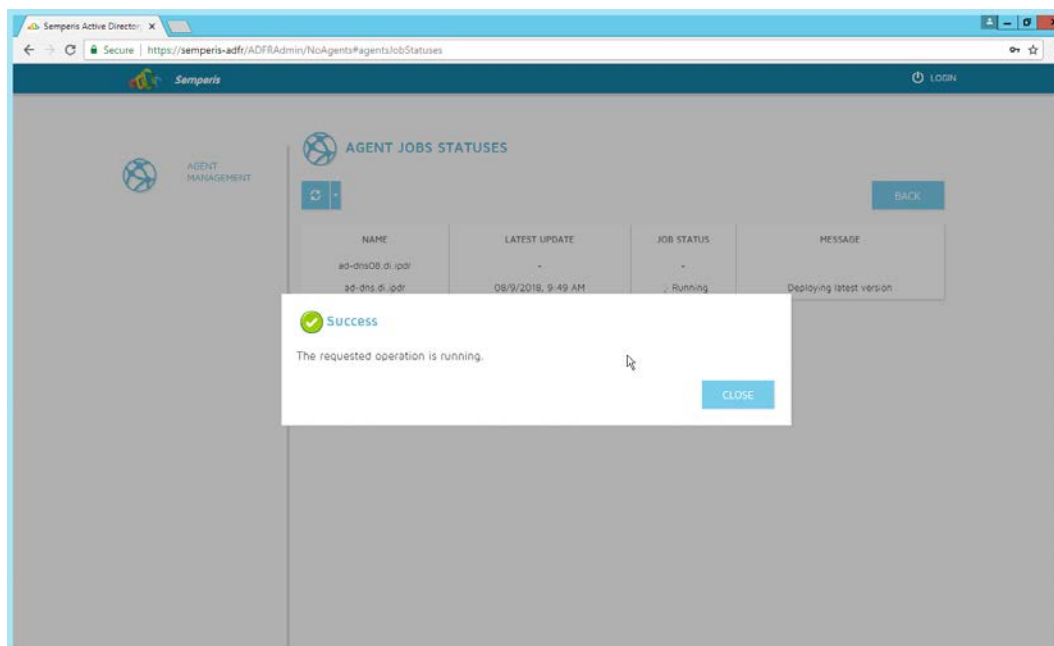


16. Click **Run Action**.

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



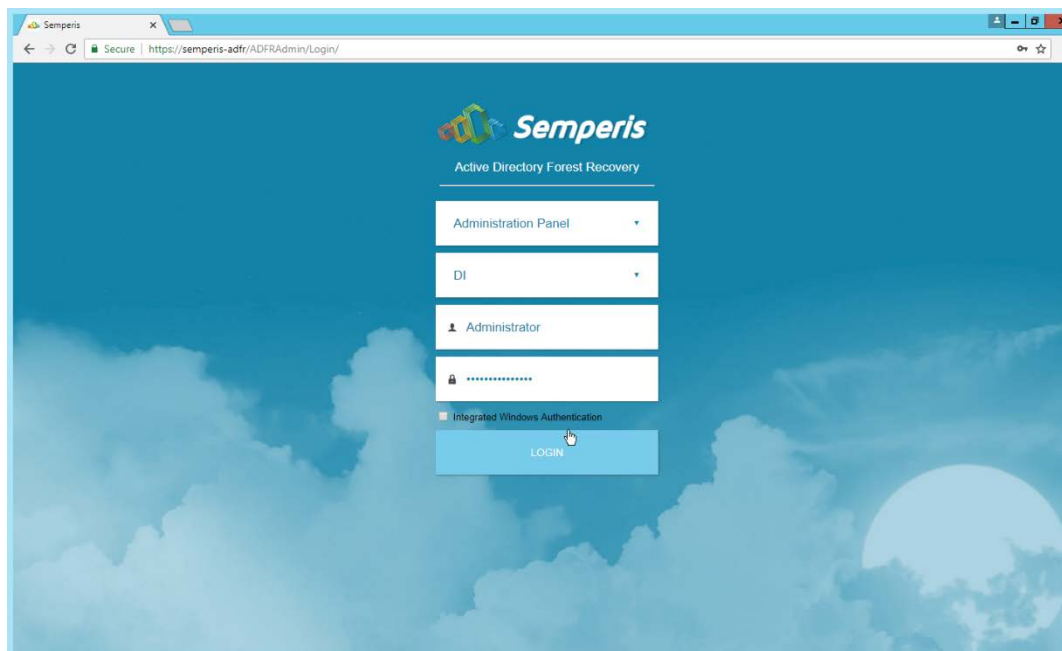
18. Click **OK**.



19. Click **Close**.

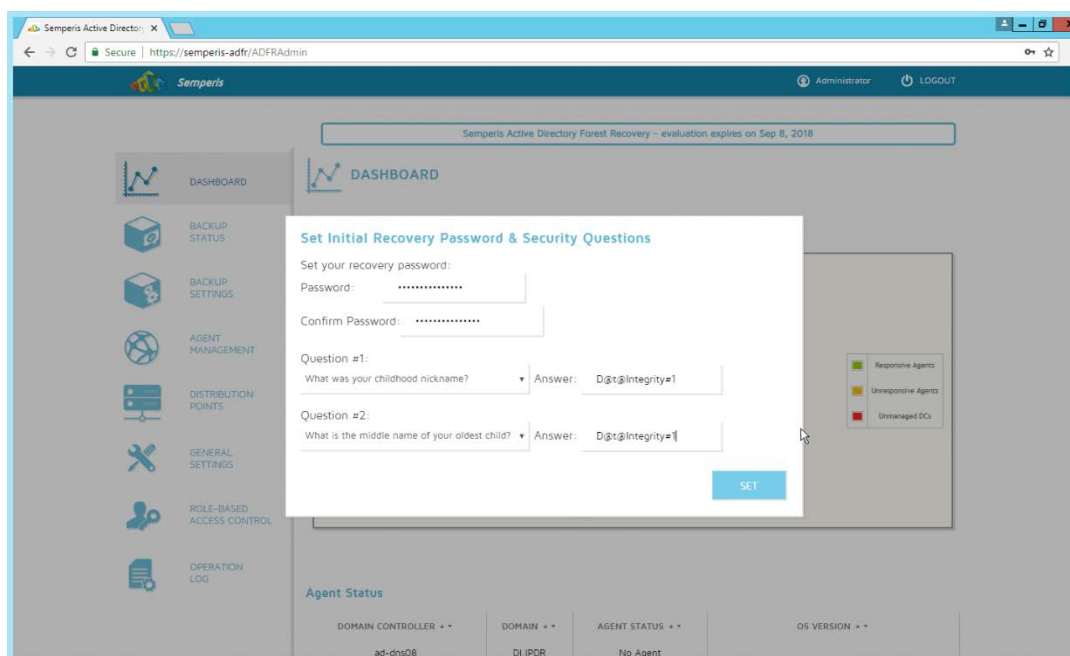
20. After the installation finishes, click **Login** at the top of the page.

21. Enter the login credentials for the domain.



22. Click **Login**.

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



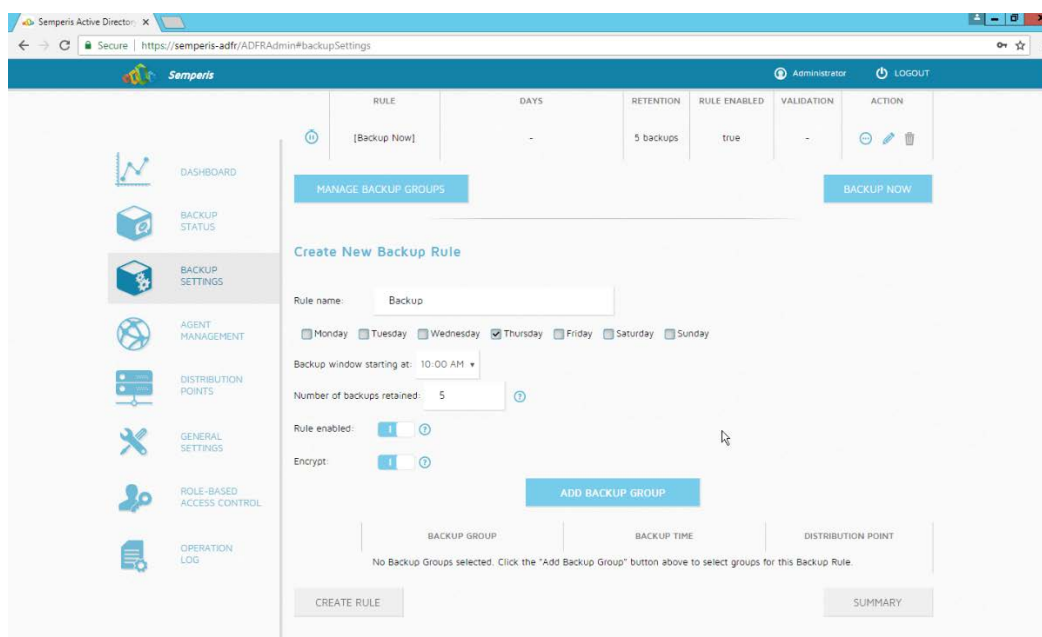
24. Set recovery questions for the password.

25. Click **Set**.

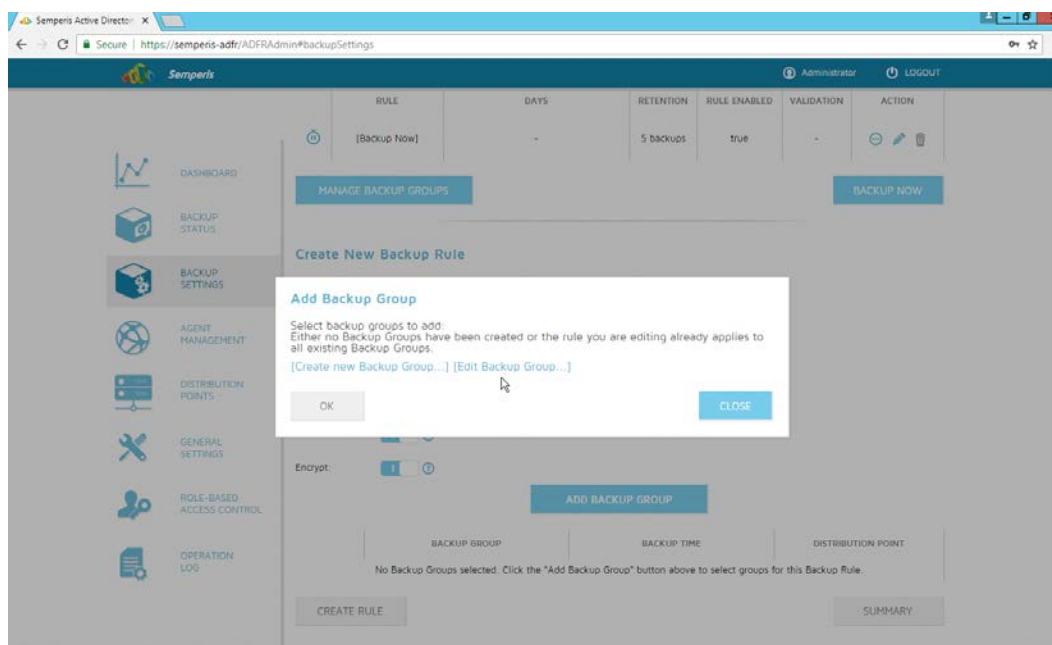
## 2.9.2 Create a Backup Schedule for the Domain Controller

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

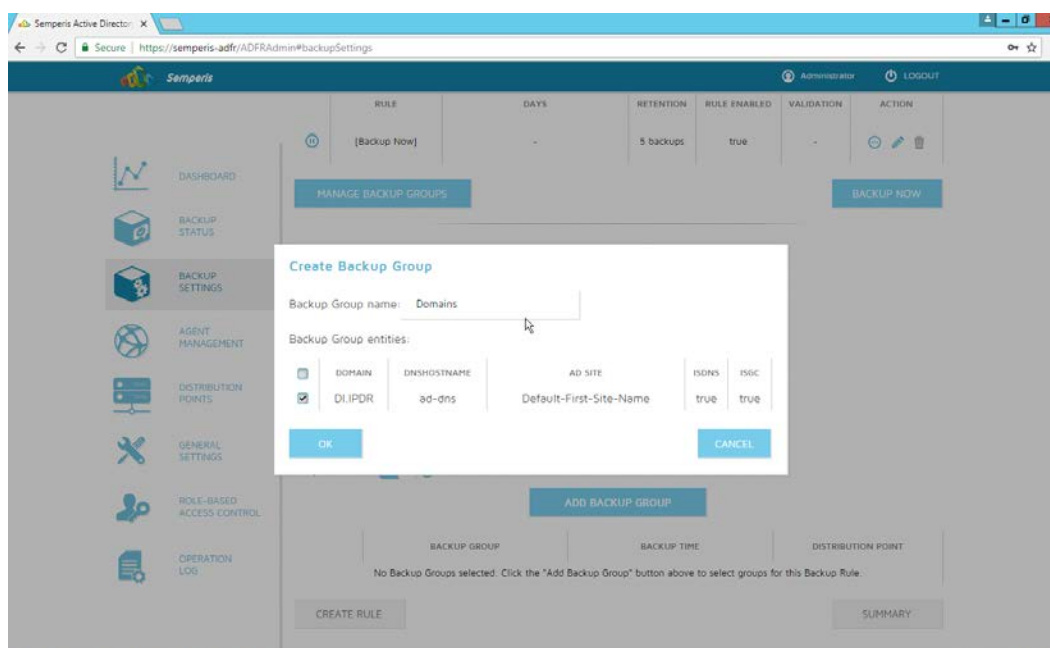




6. Click **Add Backup Group**.

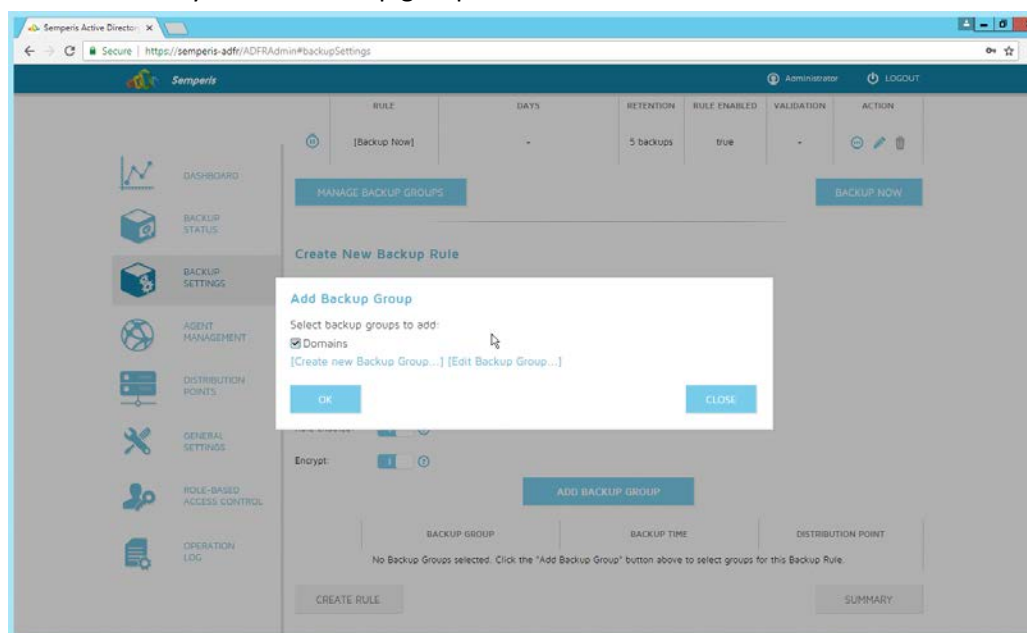


7. Click **Create new Backup Group**.
8. Enter a **name** for the backup group.
9. Select the domain controllers to be part of the backup group.

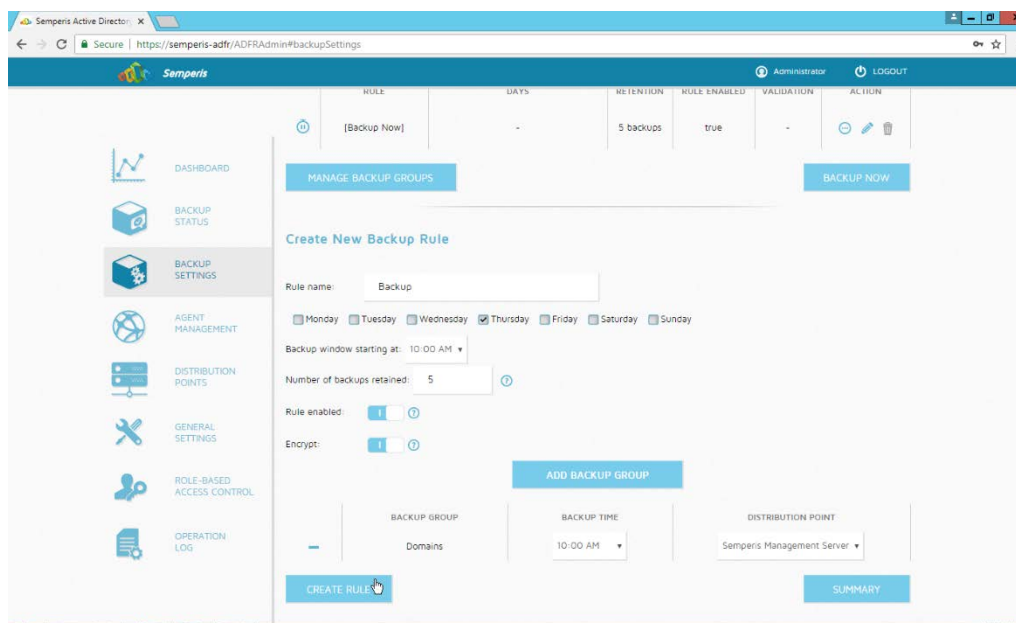


10. Click **OK**.

11. Select the newly created backup group.



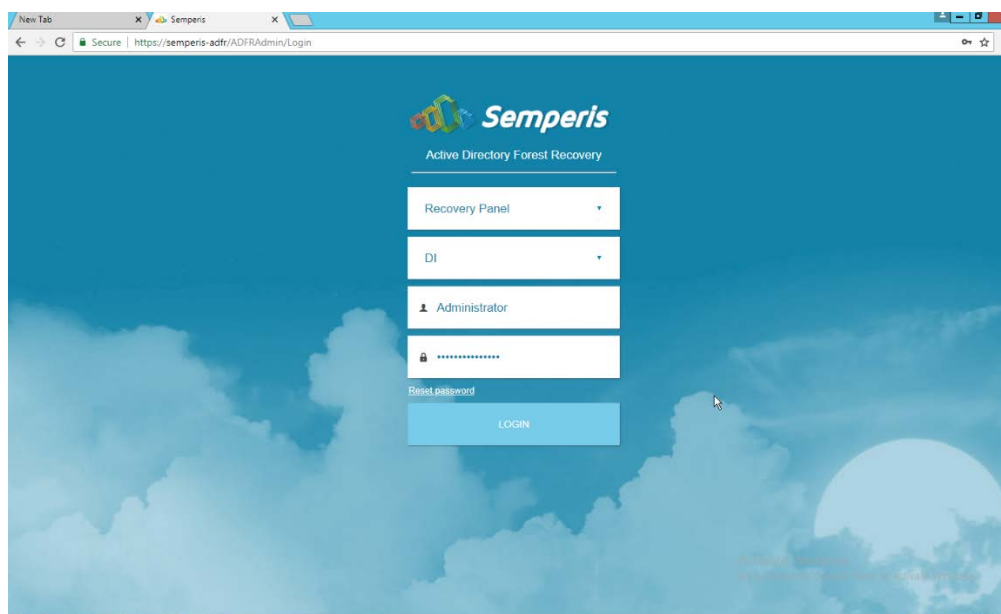
12. Click **OK**.



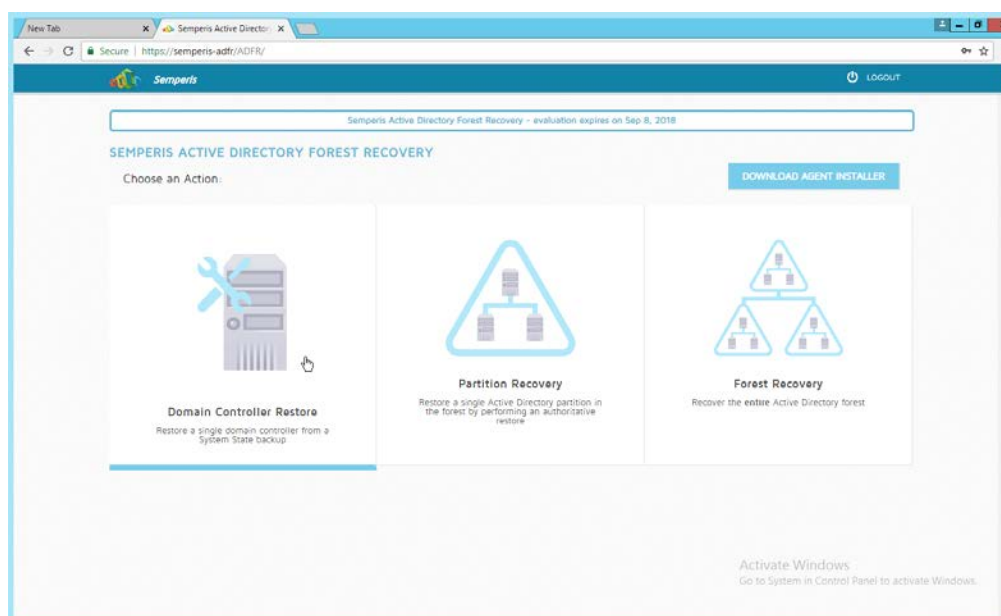
13. Click **Create Rule**.

### 2.9.3 Recover the Active Directory Forest from a Backup

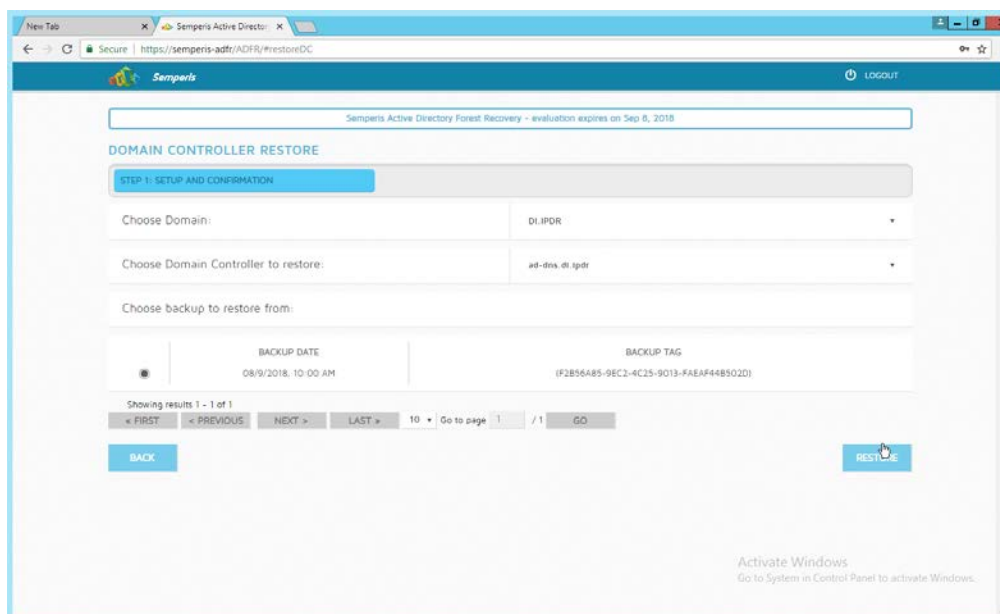
1. Open the **Semperis ADFR** web console.
2. Select **Recovery Panel** from the drop-down.
3. Select the **Domain** that you wish to recover.
4. Enter the **username** and **password**.



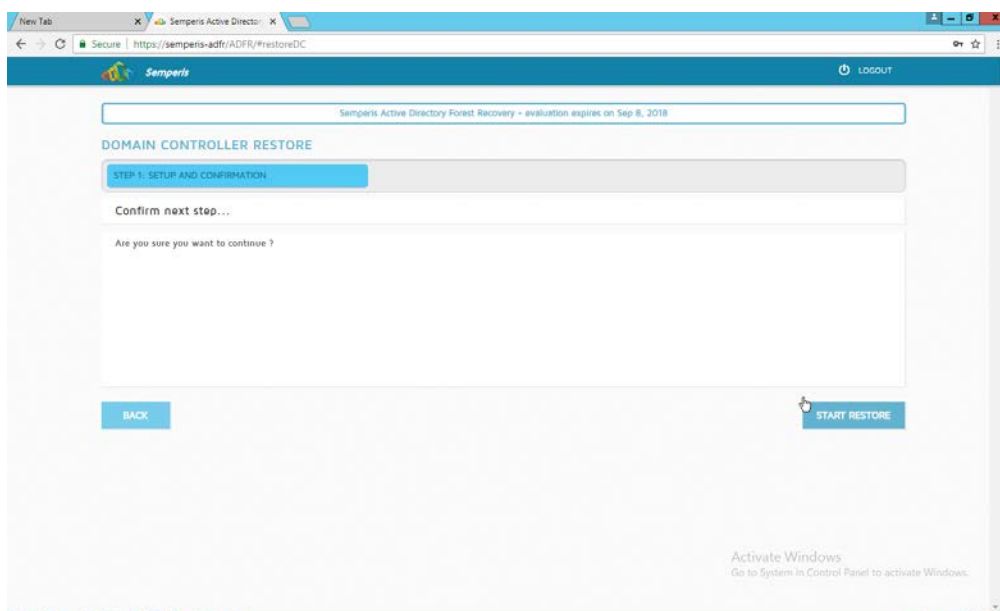
5. Click **Login**.



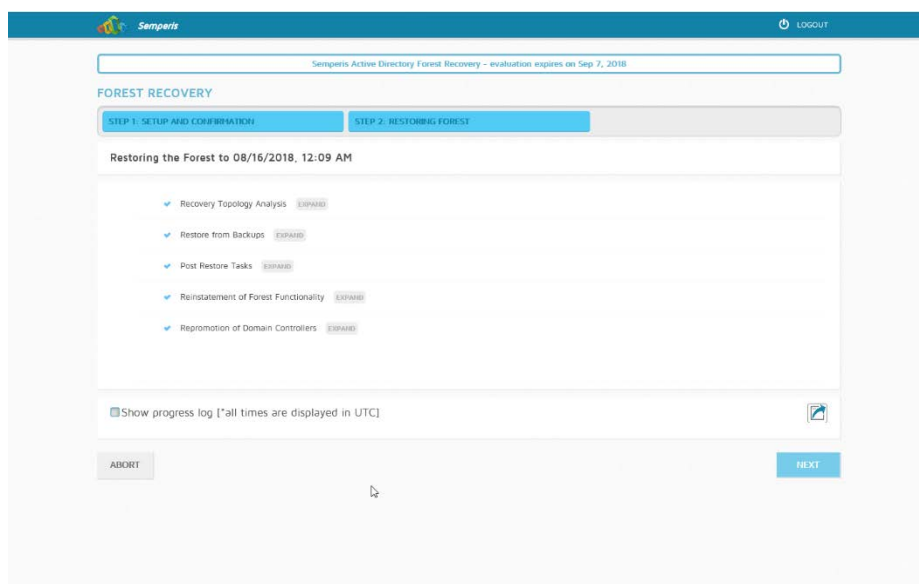
6. Select an action based on the recovery needs of the organization. In this example we select **Domain Controller Restore**.
7. Provide the information for the restoration, namely the **domain**, the **domain controller**, and which backup to use.



8. Click **Restore**.



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



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

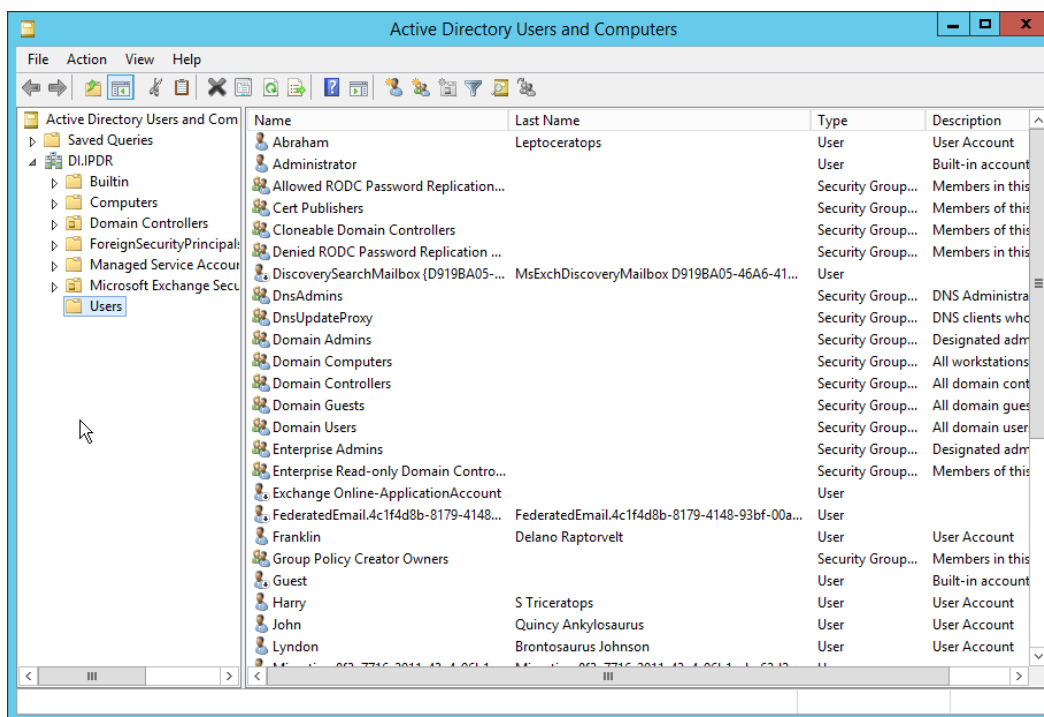
## 2.10 Semperis Directory Services Protector

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

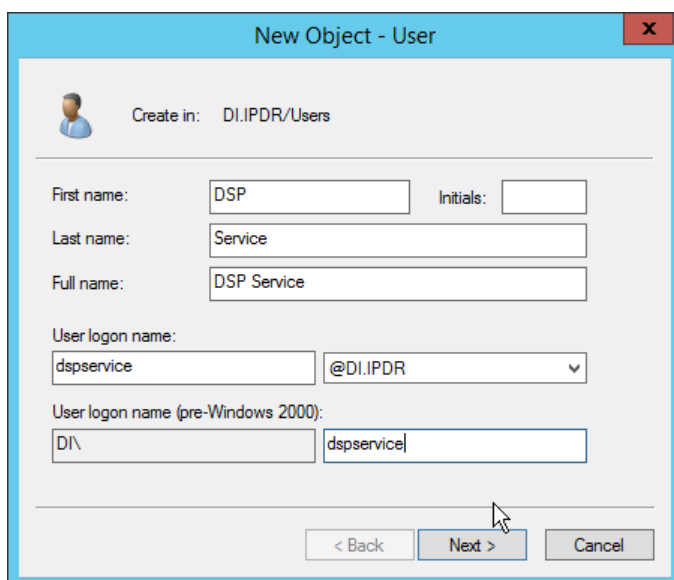
- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- joined to the Active Directory domain it is protecting
- either the installer for SQL Express Advanced or connection information and credentials for a full version of Microsoft SQL (MSSQL)

### 2.10.1 Configure Active Directory for Semperis DSP

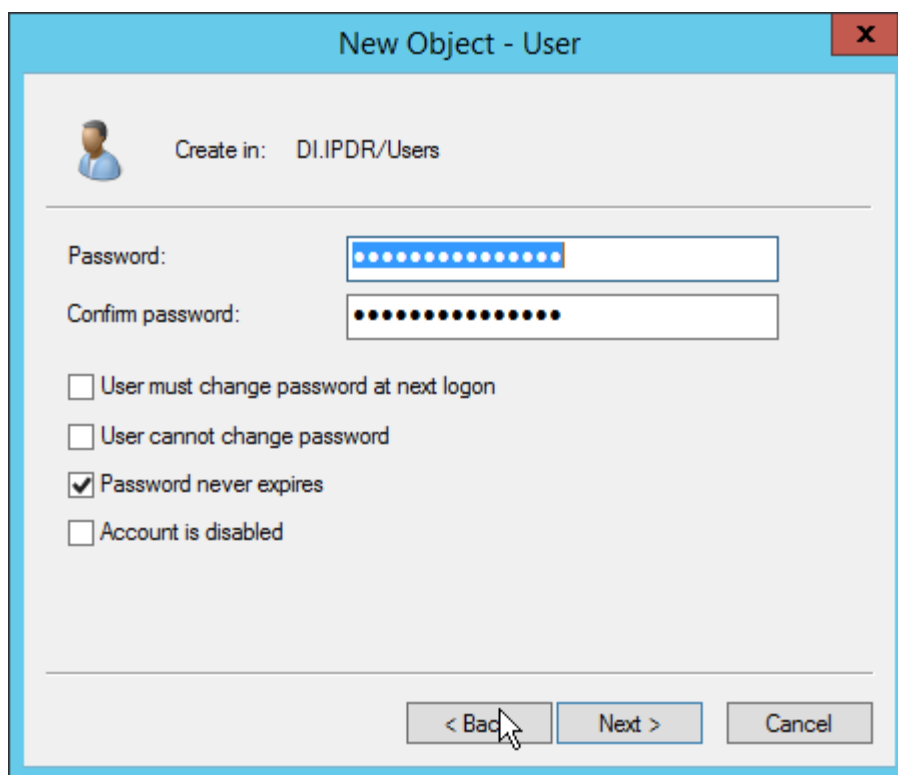
1. Open **Active Directory Users and Computers**.



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



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



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

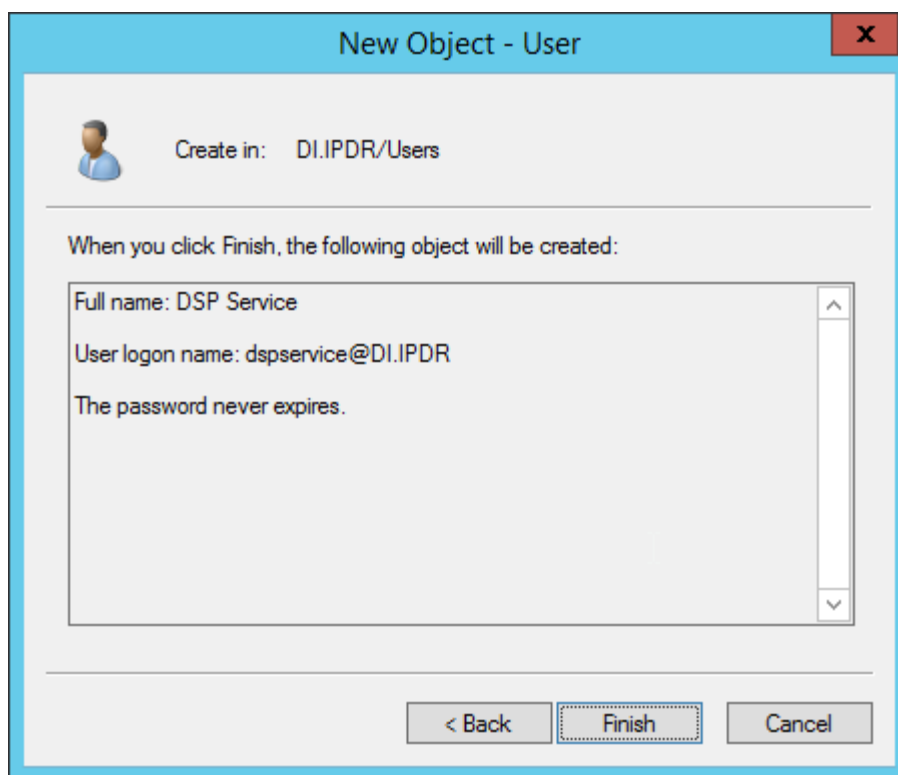
☒ Password never expires

☐ Account is disabled

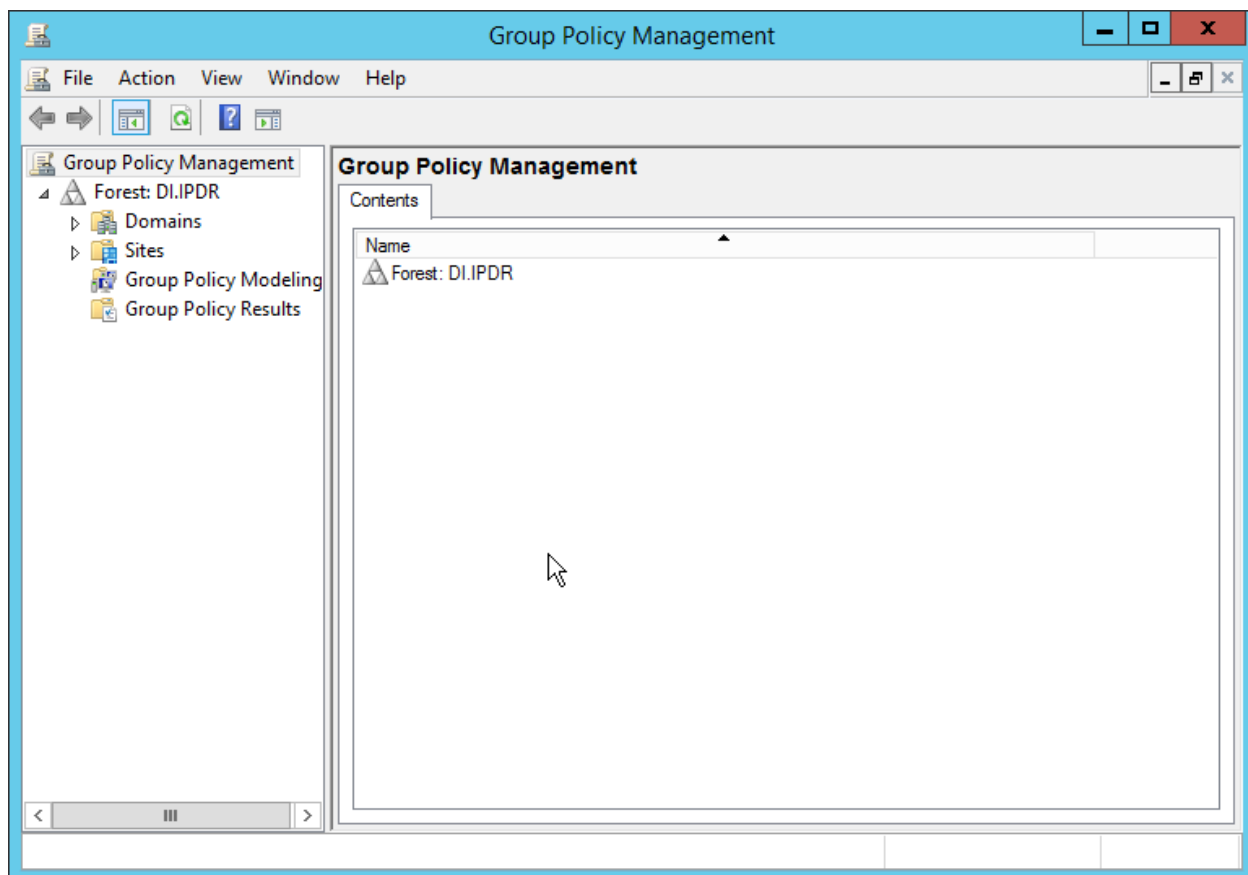
< Back   Next >   Cancel

7. Click **Next**.

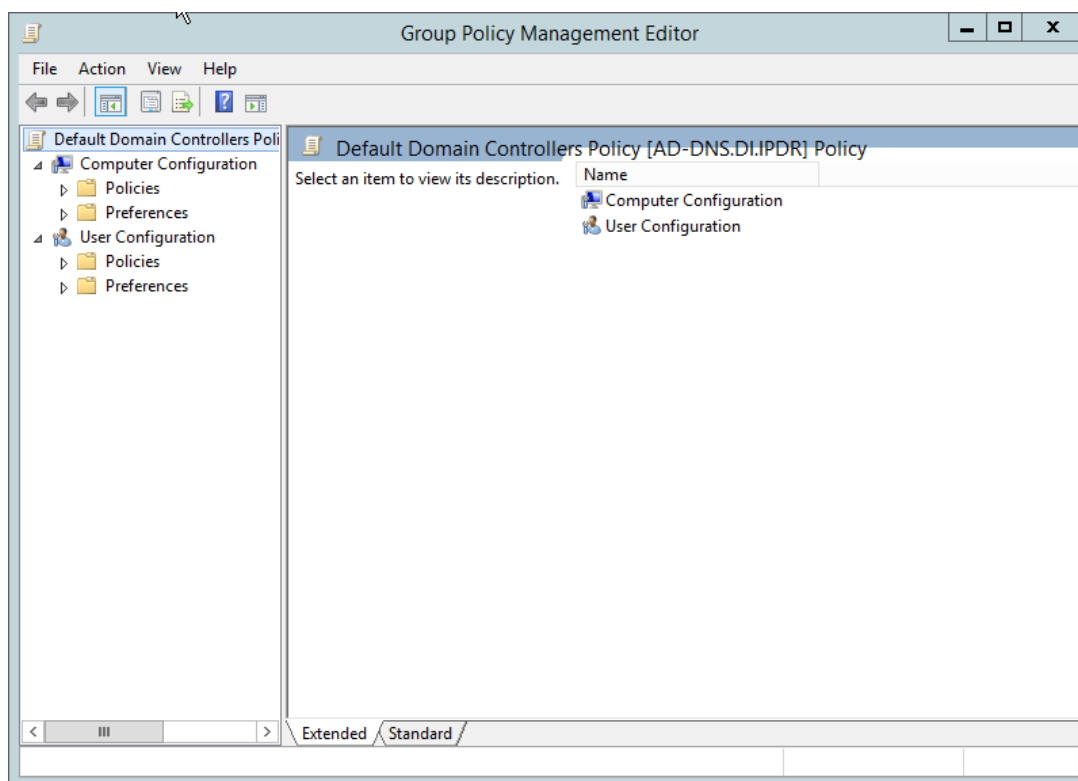




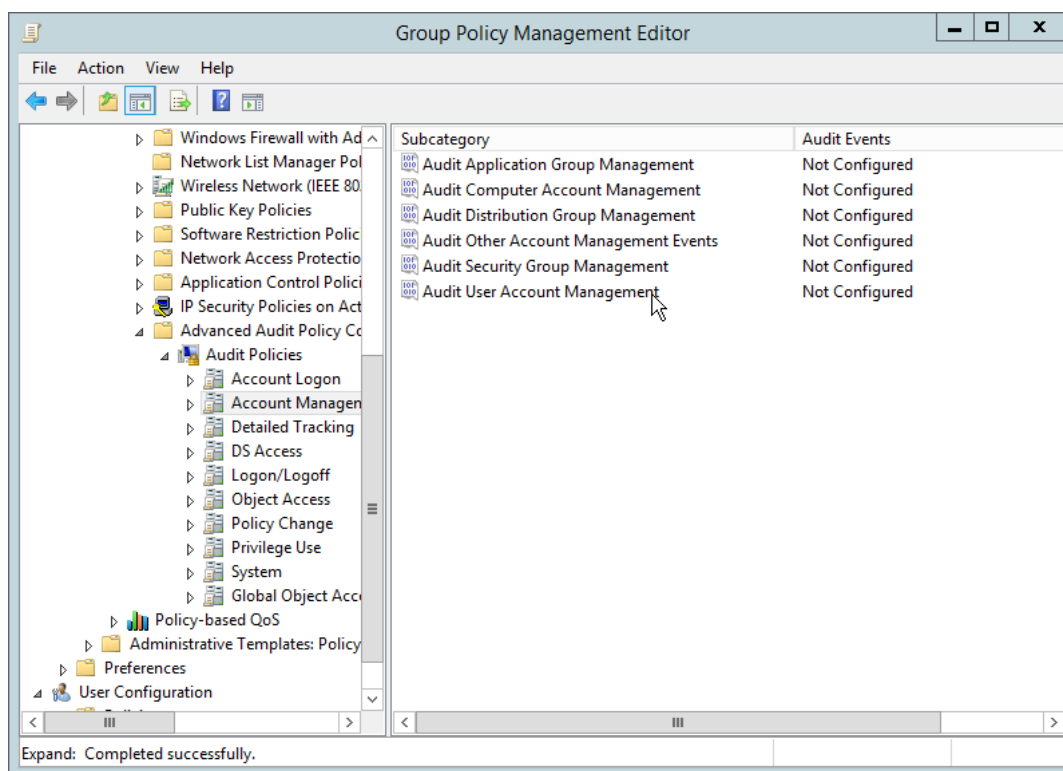
8. Click **Finish**.
9. Open **Group Policy Management**.



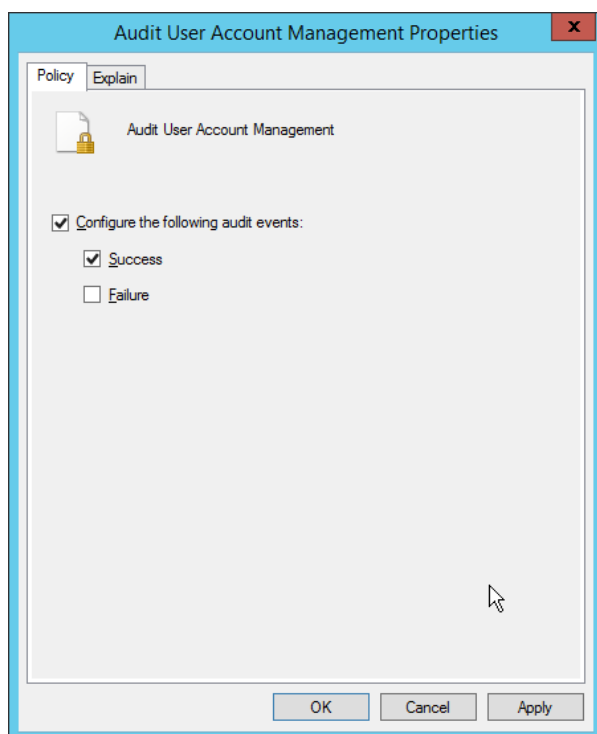
10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy** and click **Edit**.



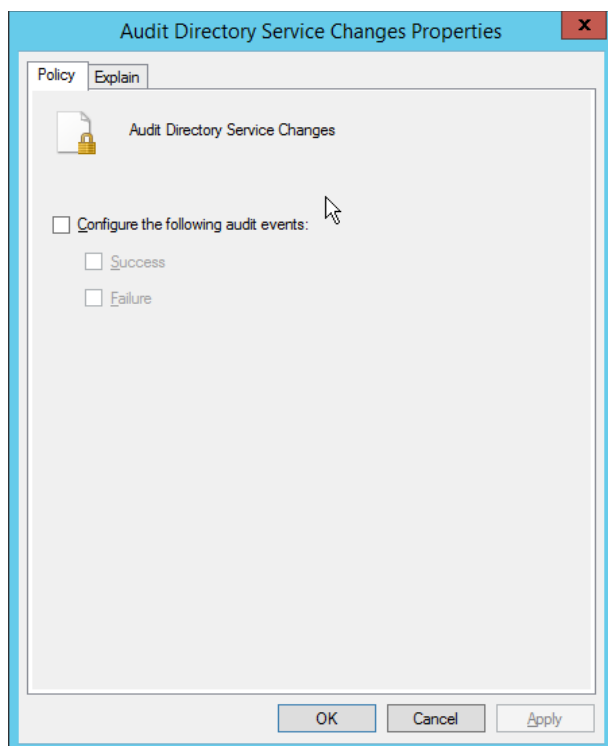
11. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management**.



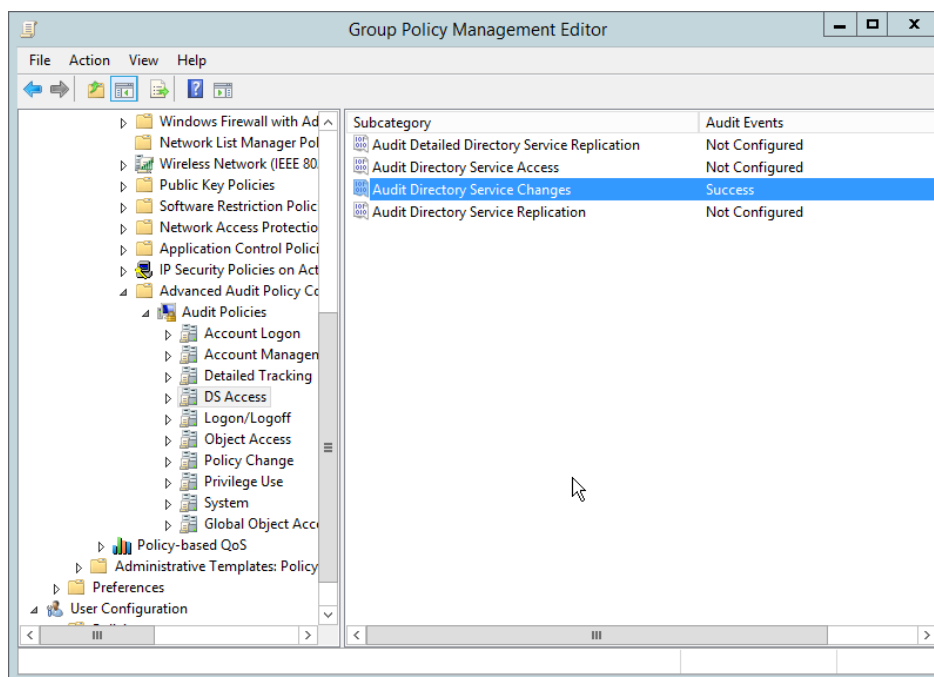
12. Edit the **Audit User Account Management** field by double-clicking it.
13. Check the box next to **Configure the following audit events**.
14. Check the box next to **Success**.



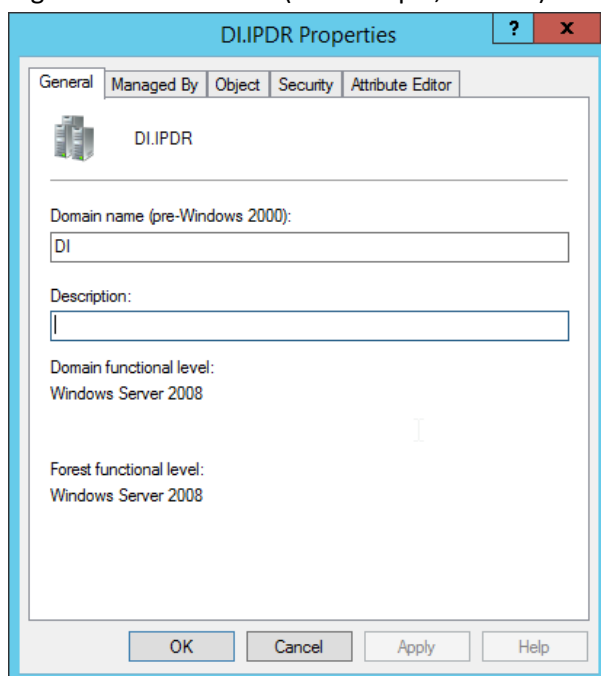
15. Click **OK**.
16. Go to **Audit Policies > DS Access**.
17. Double-click **Audit Directory Service Changes**.



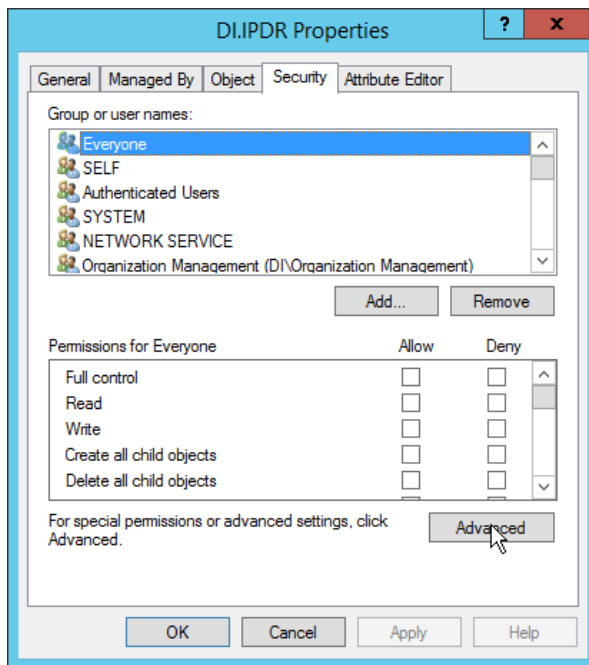
18. Check the box next to **Configure the following audit events**.
19. Check the box next to **Success**.
20. Click **OK**.



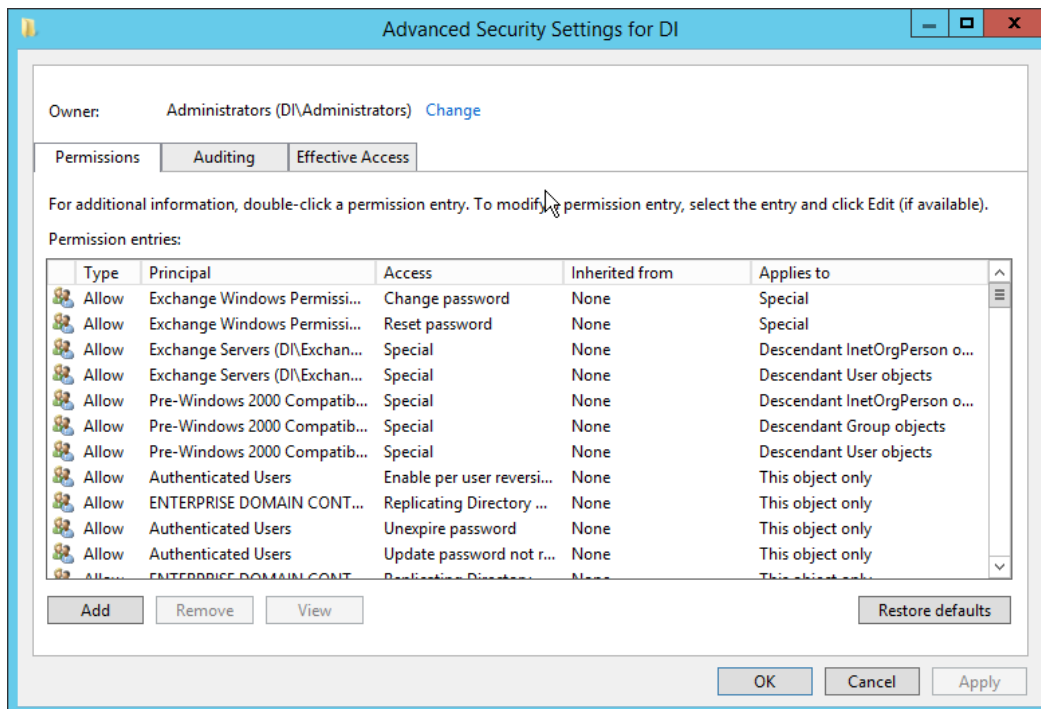
21. Open **Active Directory Users and Computers**.
22. Ensure that **View > Advanced Features** is enabled.
23. Right-click the **domain** (for example, DI.IPDR) created earlier and click **Properties**.



24. Click the **Security** tab.



25. Click **Advanced**.

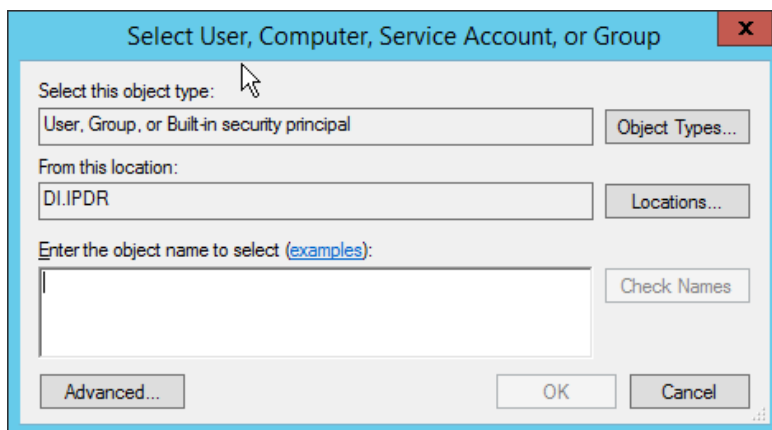


26. Click the **Auditing** tab.

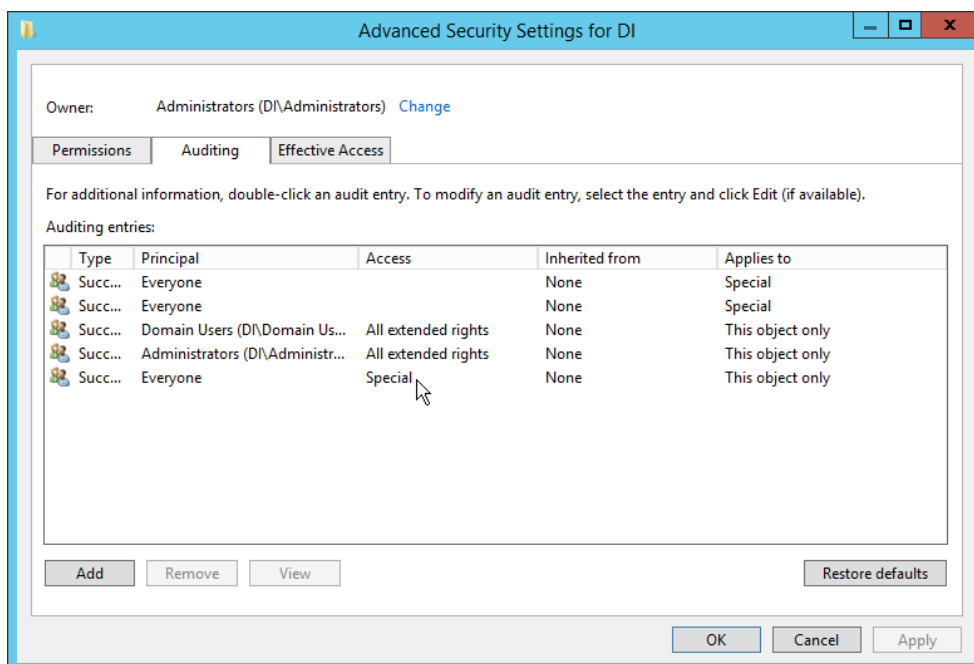
27. Click **Add**.



28. Enter **Everyone**.

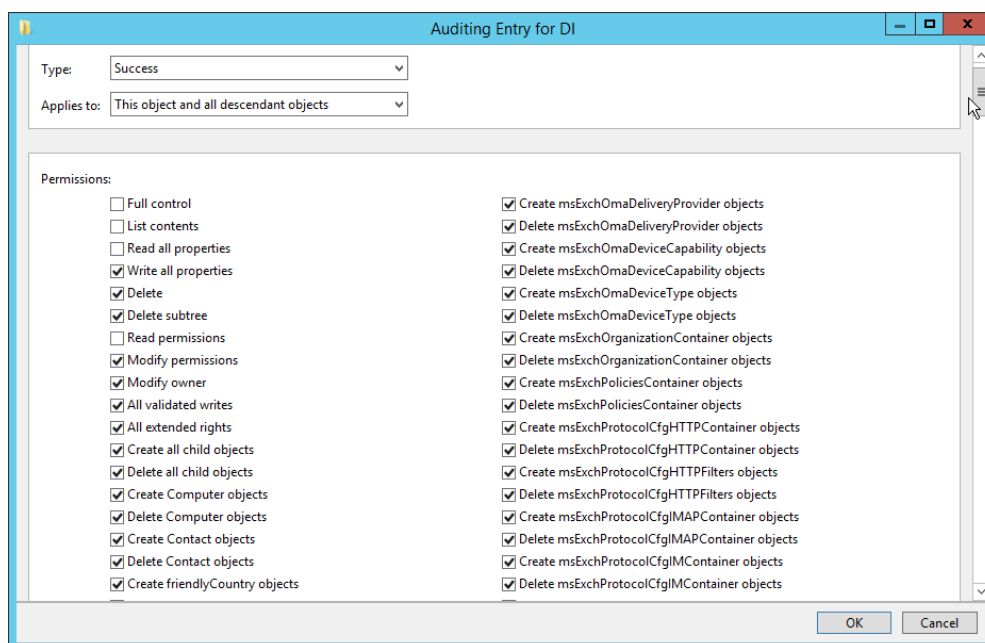


29. Click **OK**.

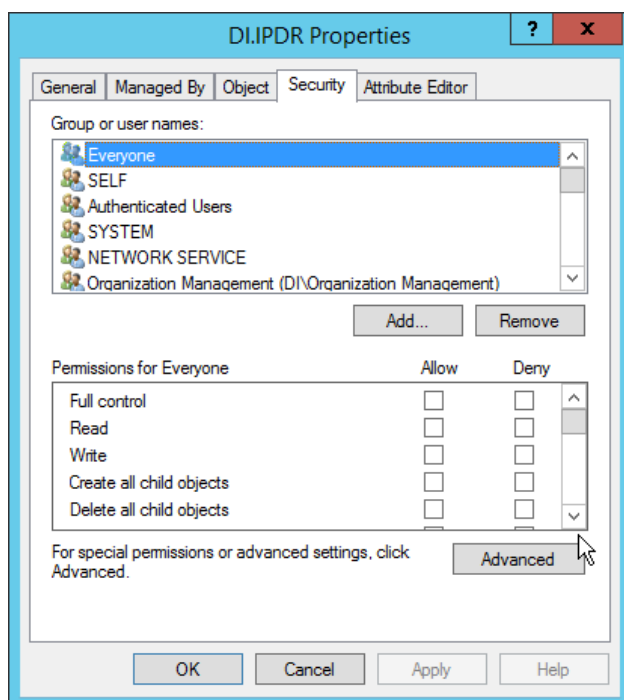


30. Double-click **Everyone**.

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



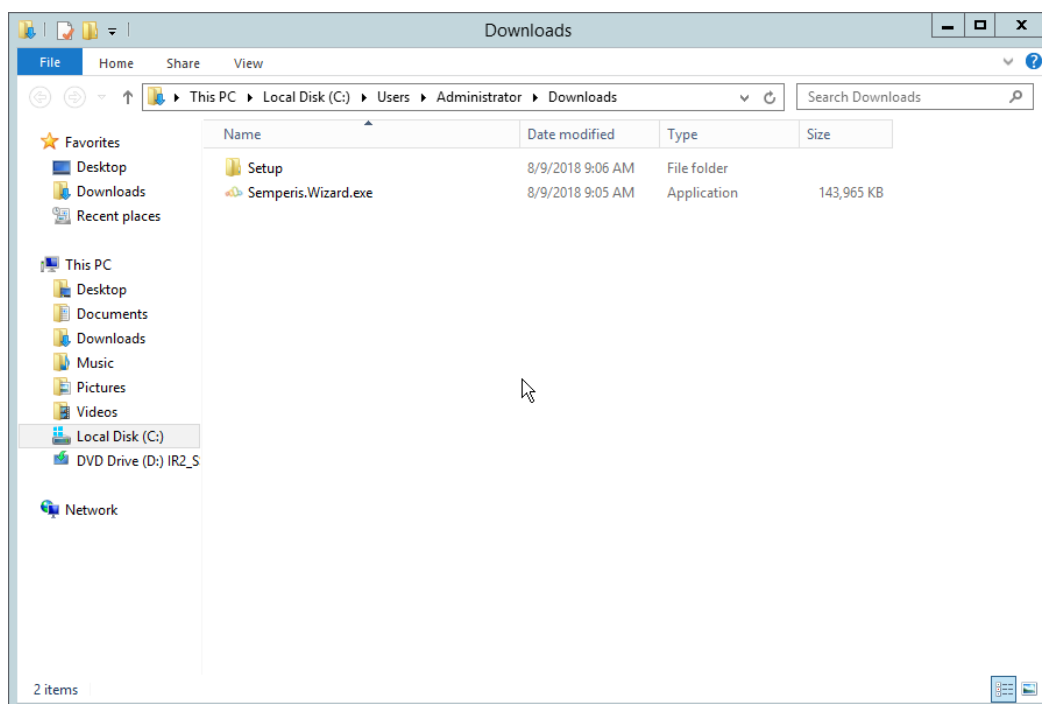
32. Click **OK**.



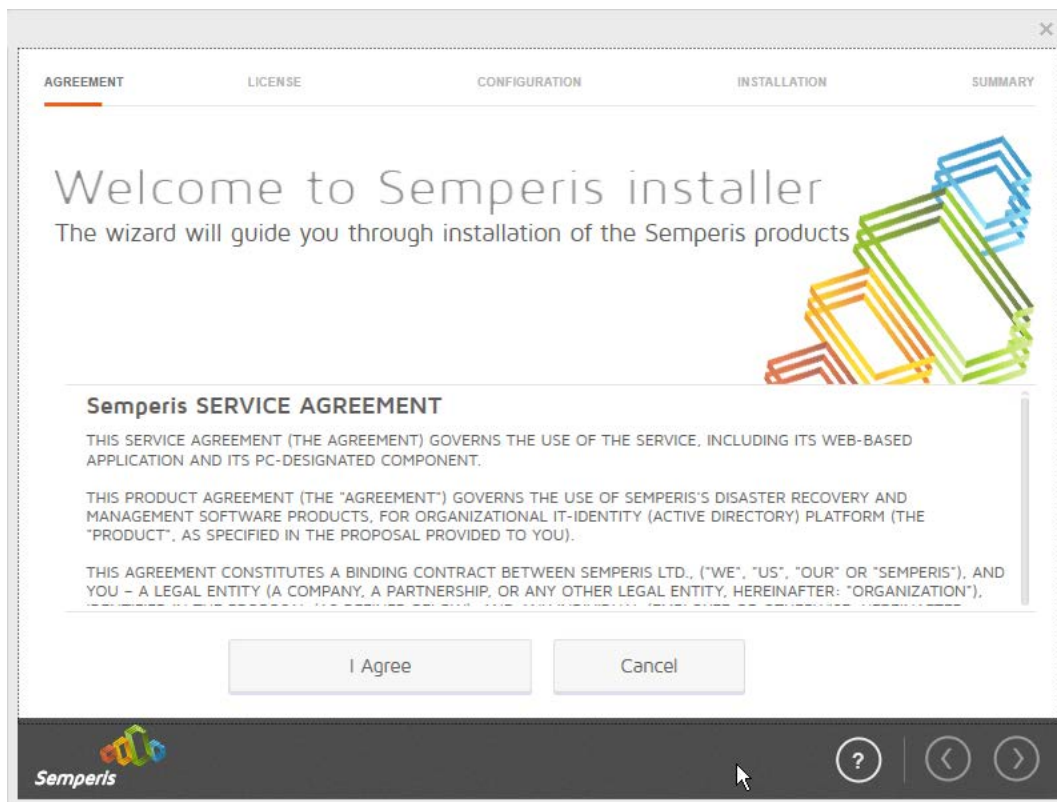
33. Click **OK**.

## 2.10.2 Install Semperis DSP

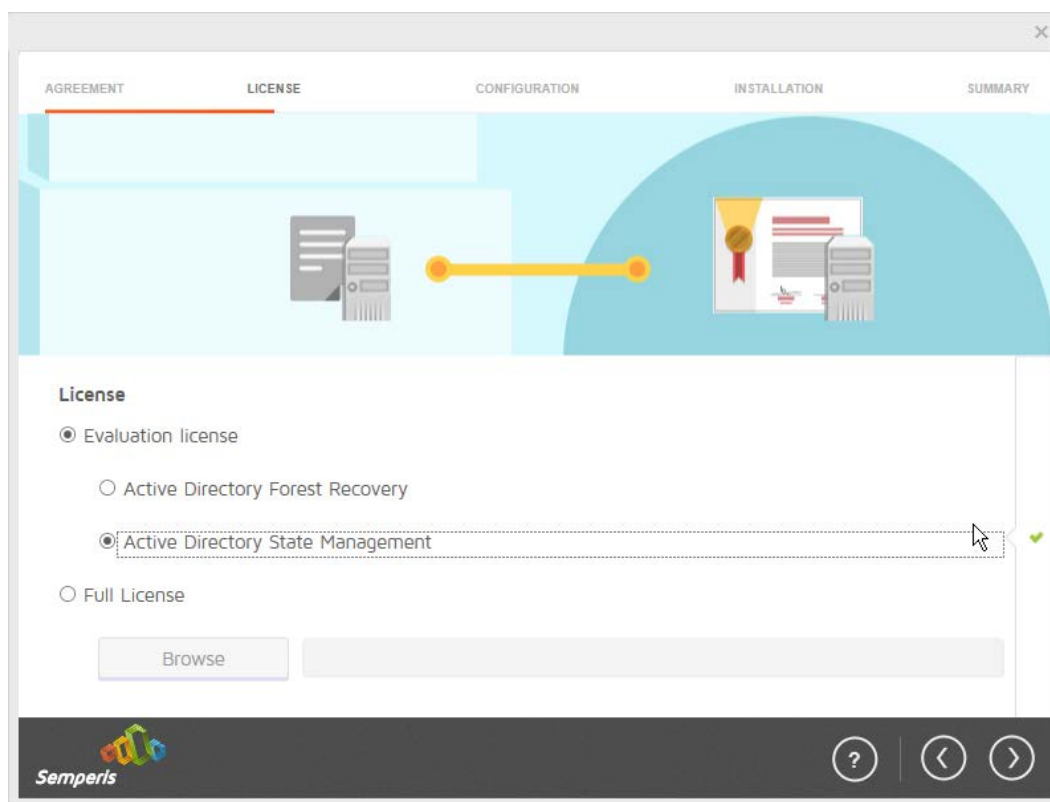
1. If you are using a local SQL Express Advanced server, place the **SQLEXPRADV\_x64\_ENU.exe** installer in a directory called **Setup**, and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it). If an SQL Express Advanced server is not being used, no **Setup** folder is required.



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

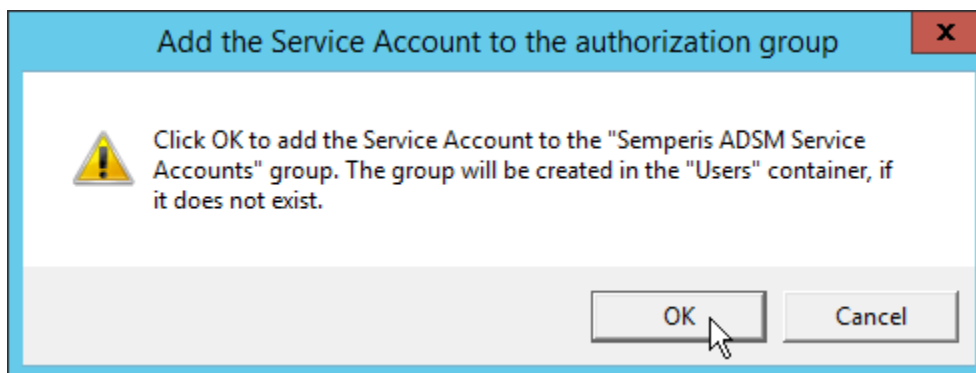


3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory State Management**.

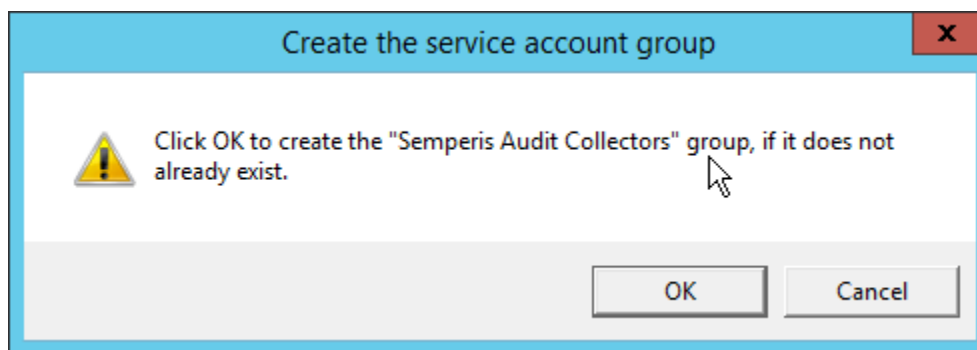


6. Click the > button.
7. Enter the **username** and **password** of the account created earlier.

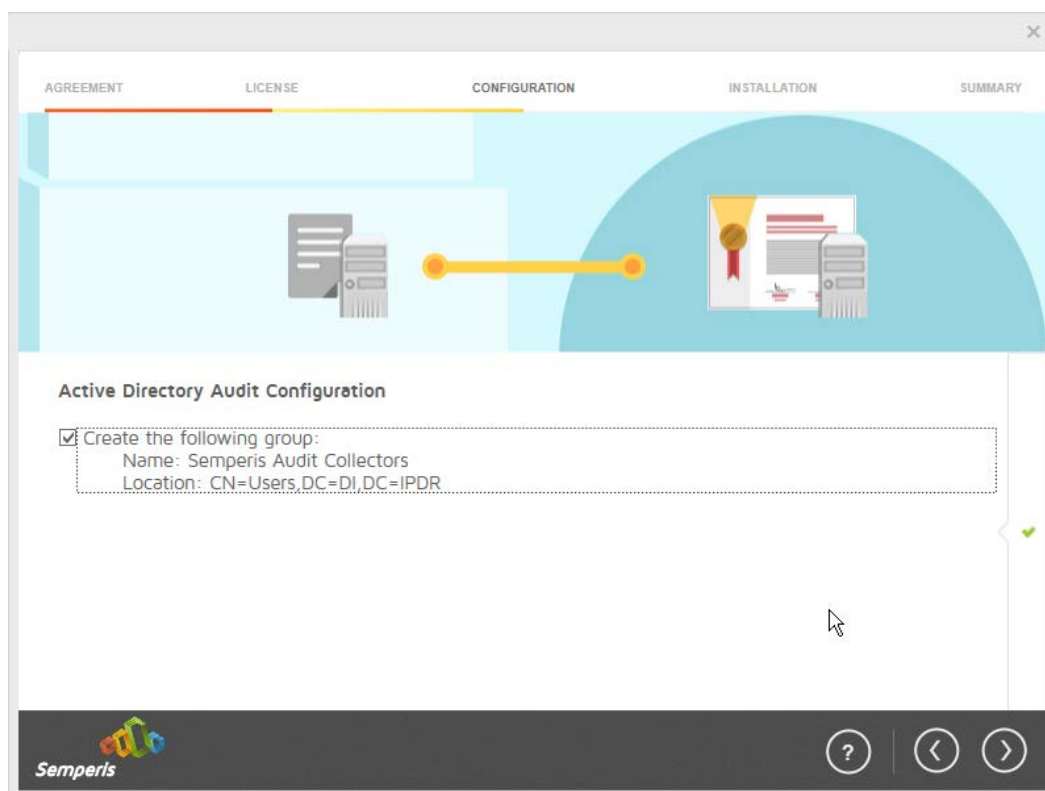
8. Click the > button.



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

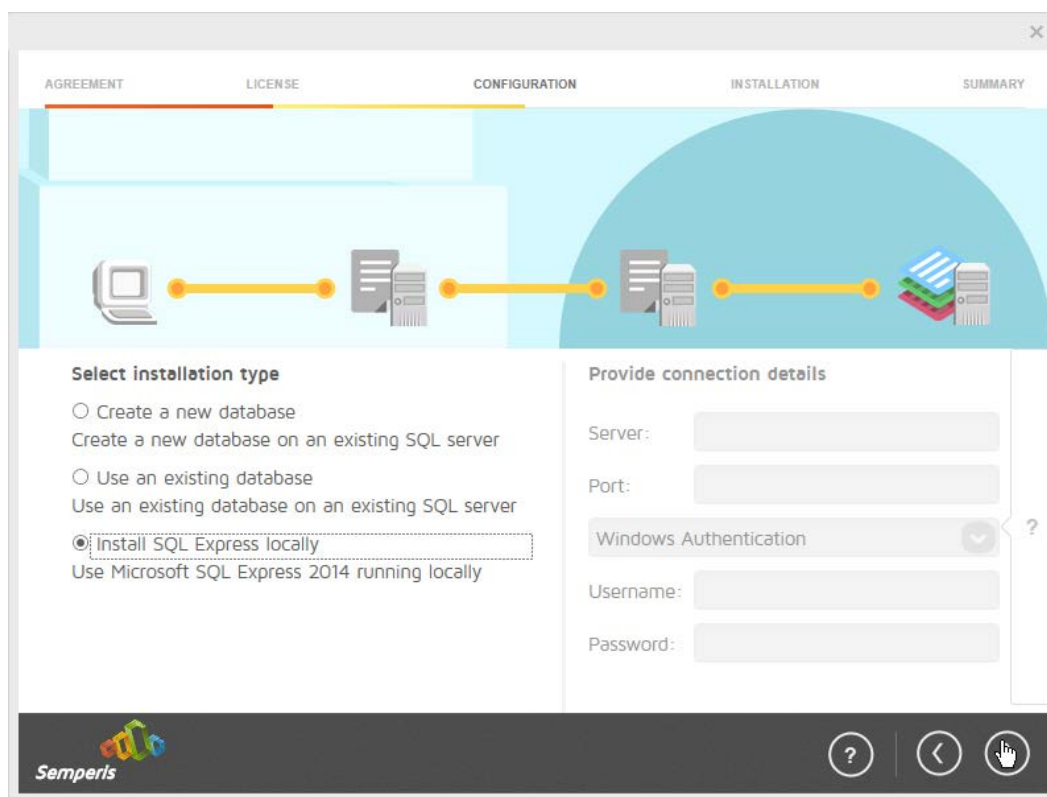


11. Click **OK**.

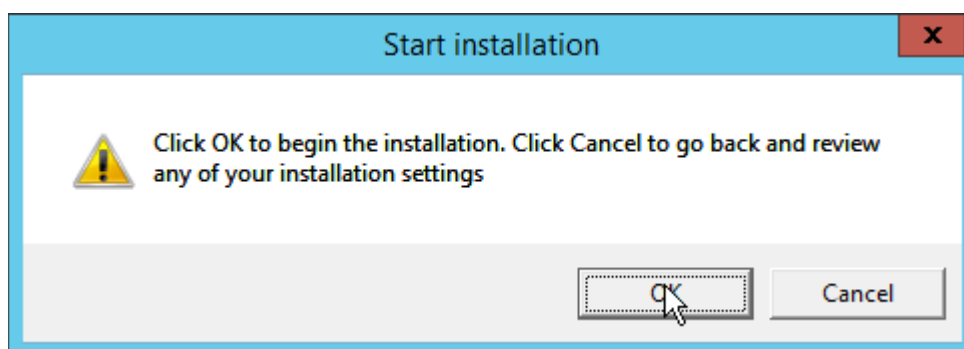


12. Click the **>** button.

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

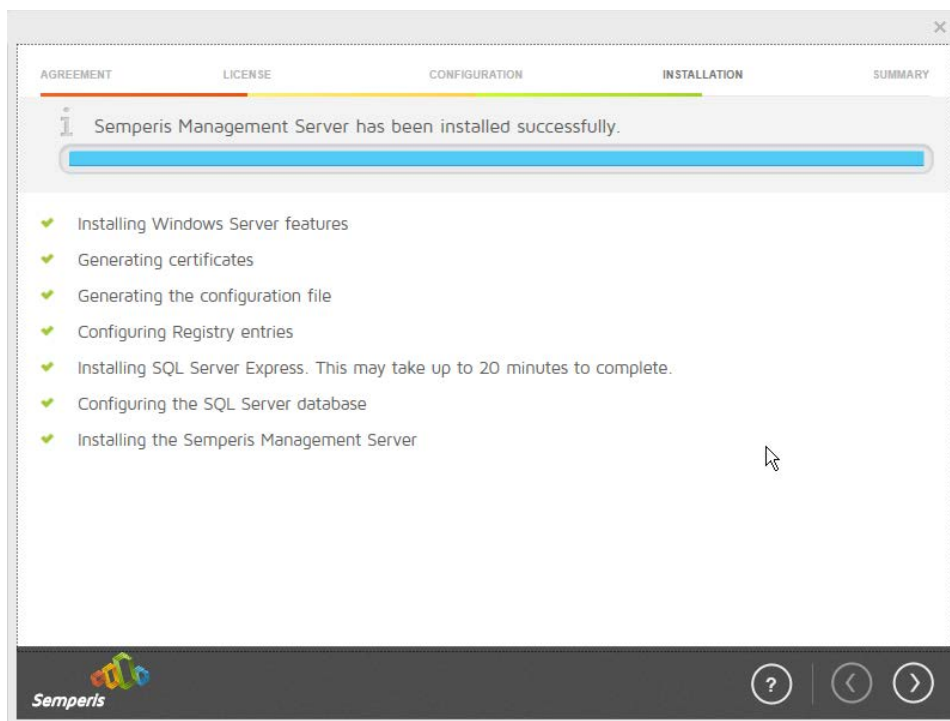


14. Click the > button.

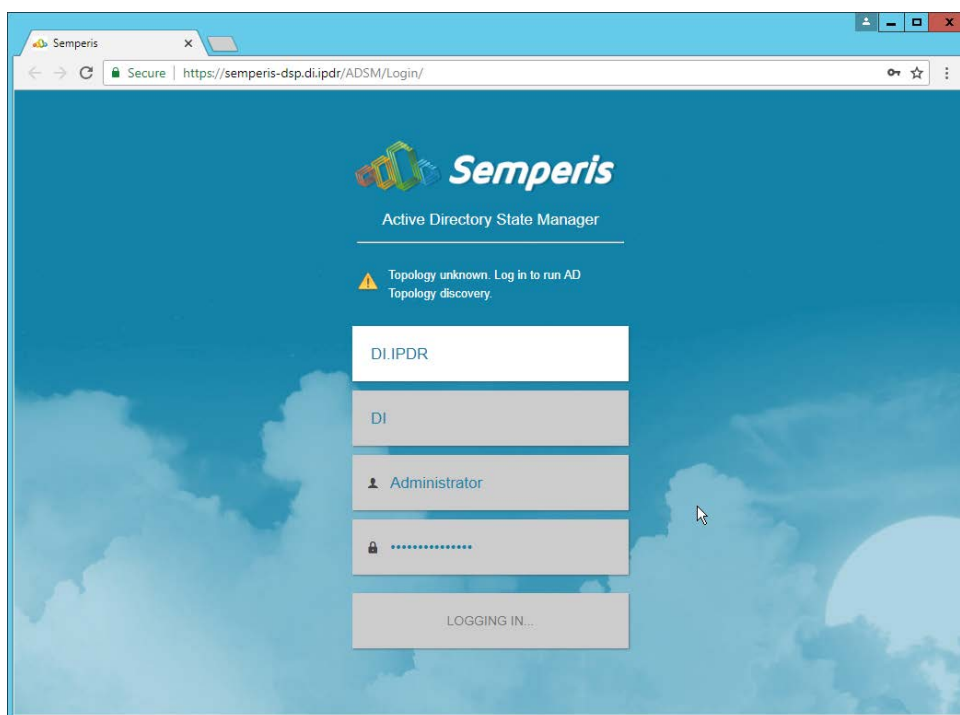


15. Click OK.



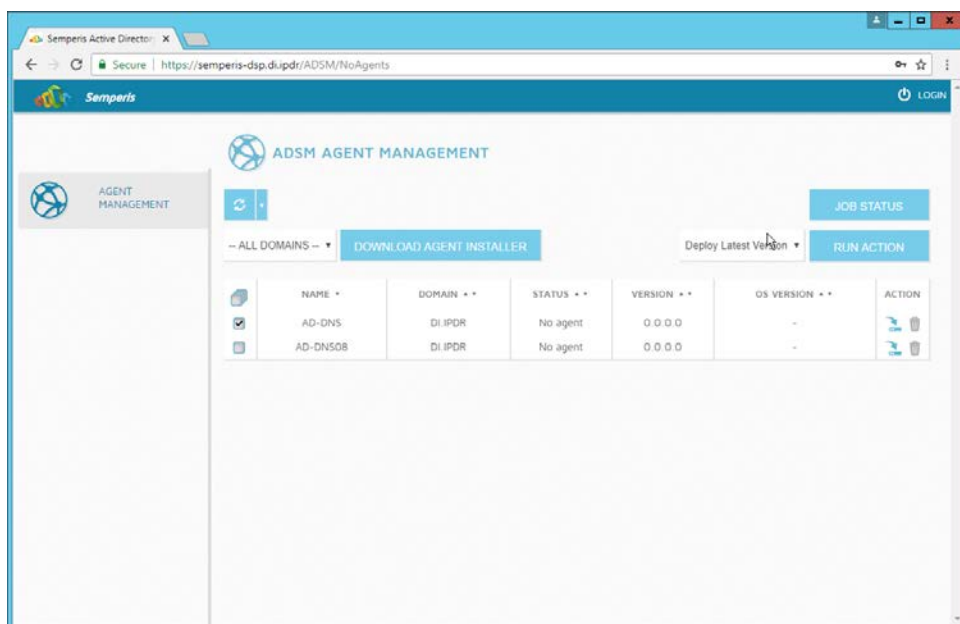


16. Click the > button after the installation completes.
17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector**.
18. On the login page, enter the full domain as well as the NetBIOS name.
19. Enter the **username** and **password** of an administrator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



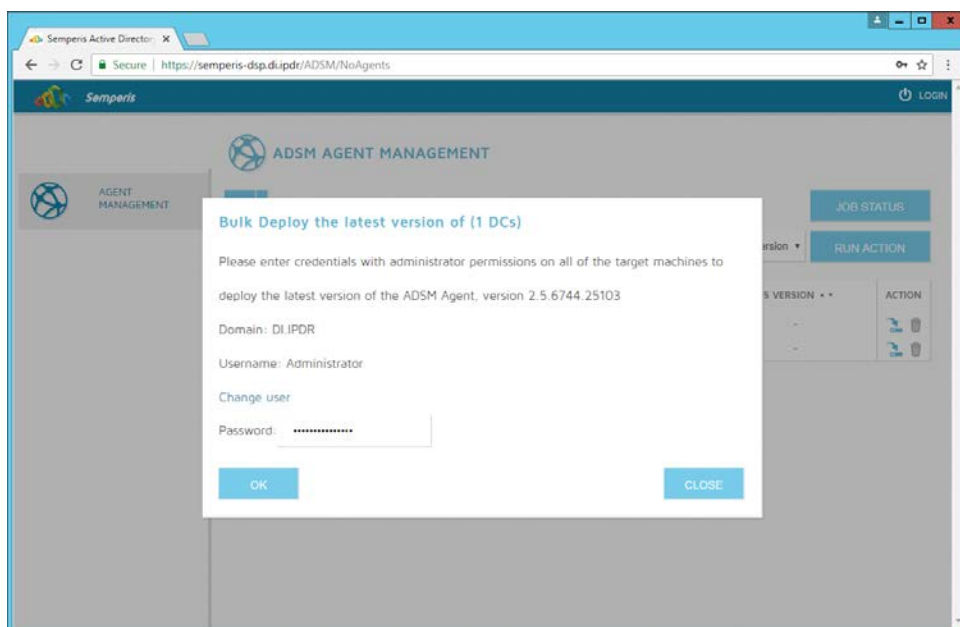
20. Click **Login**.

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

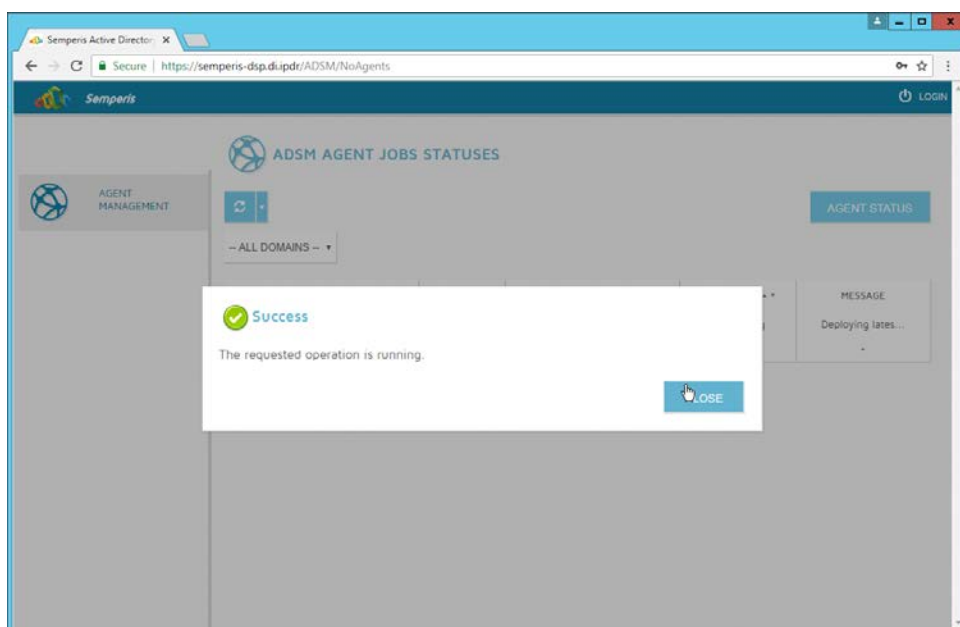


22. Click **Run Action**.

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

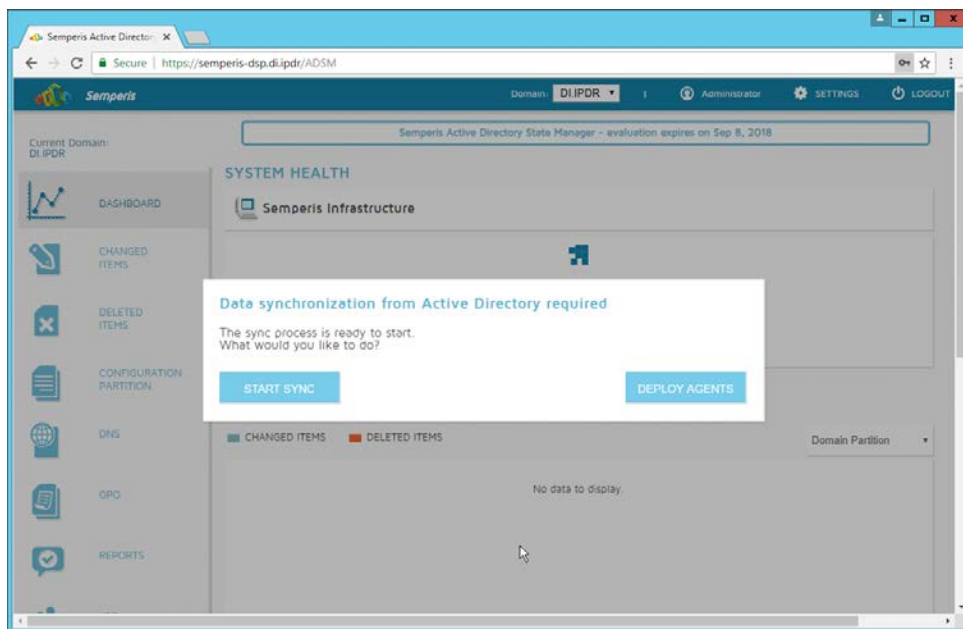


24. Click **OK**.



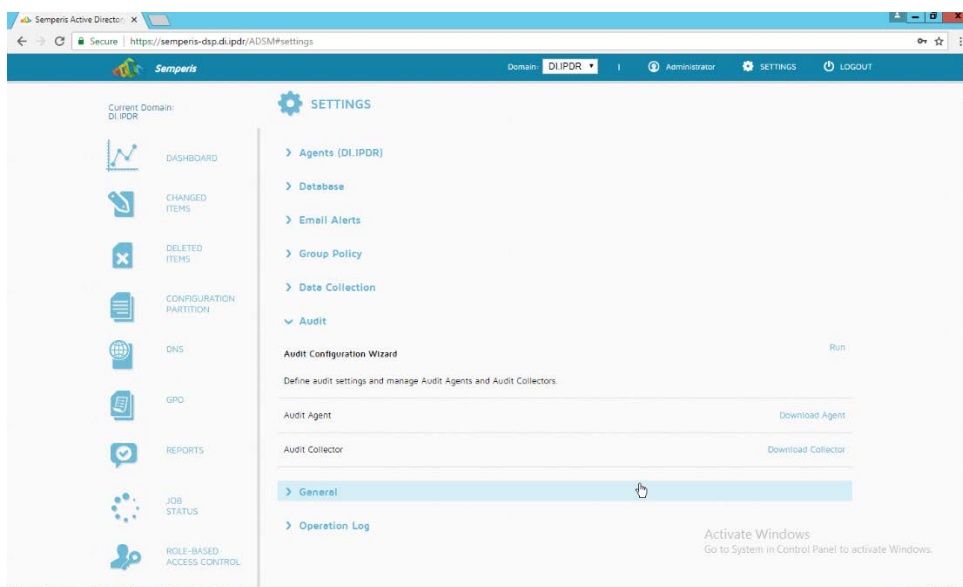
25. Click **Close**.

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



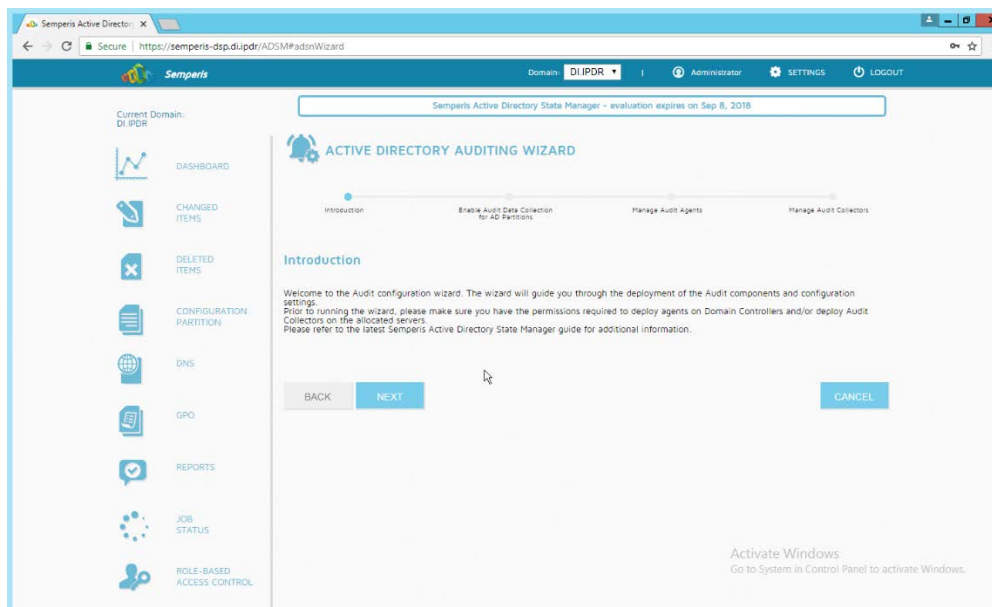
27. Click **Start Sync**.

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

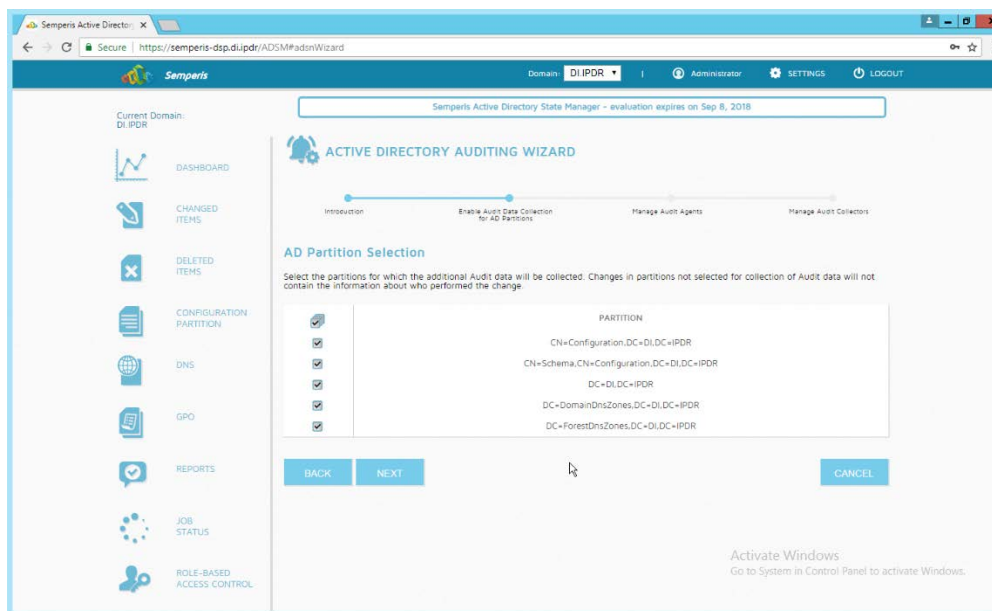


29. Click **Audit**.

30. Click **Run**.

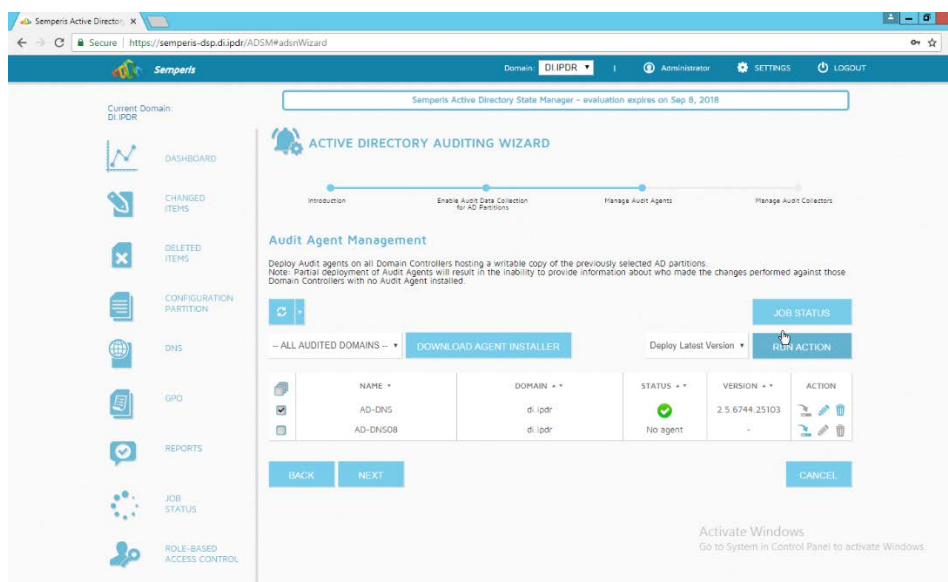


31. Click **Next**.



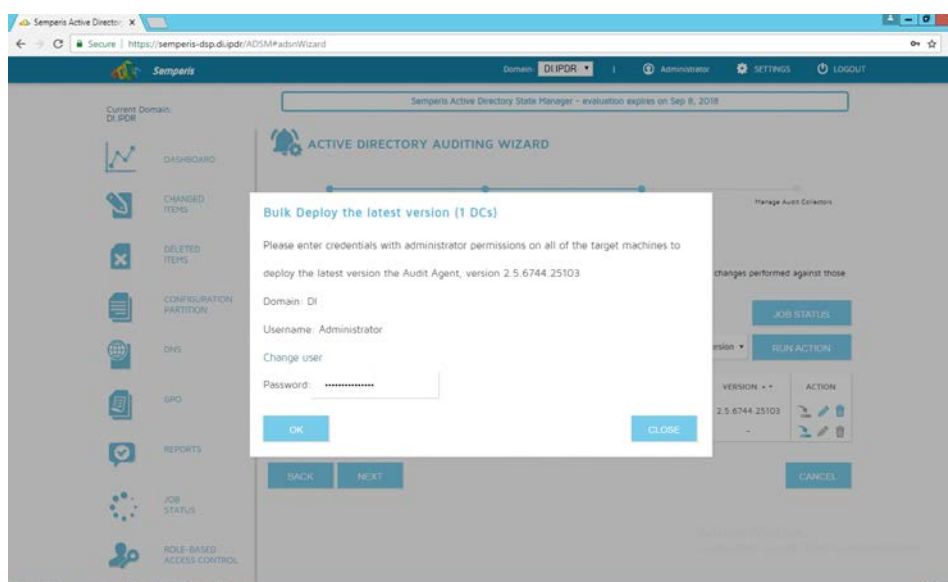
32. Click **Next**.

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



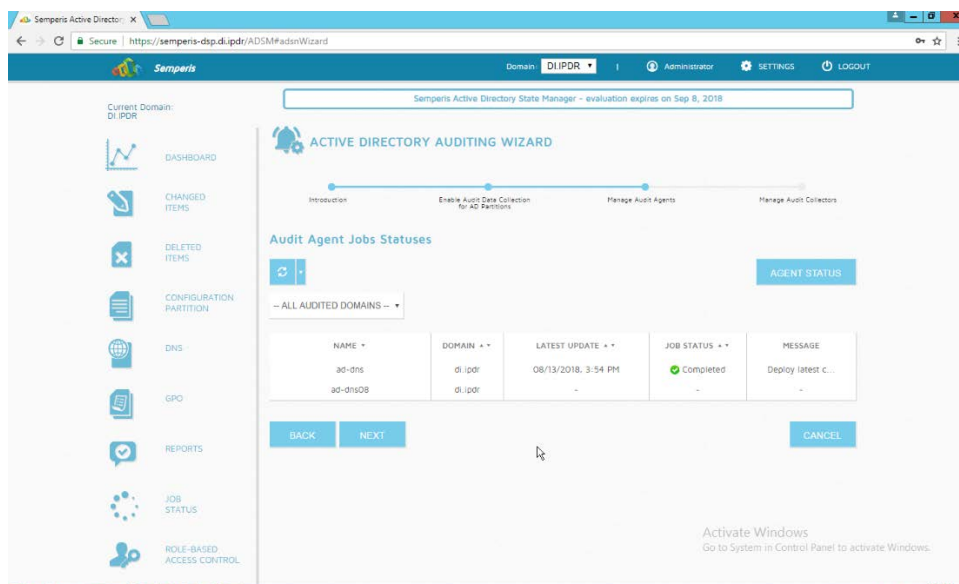
34. Click **Run Action**.

35. Enter the **password**.

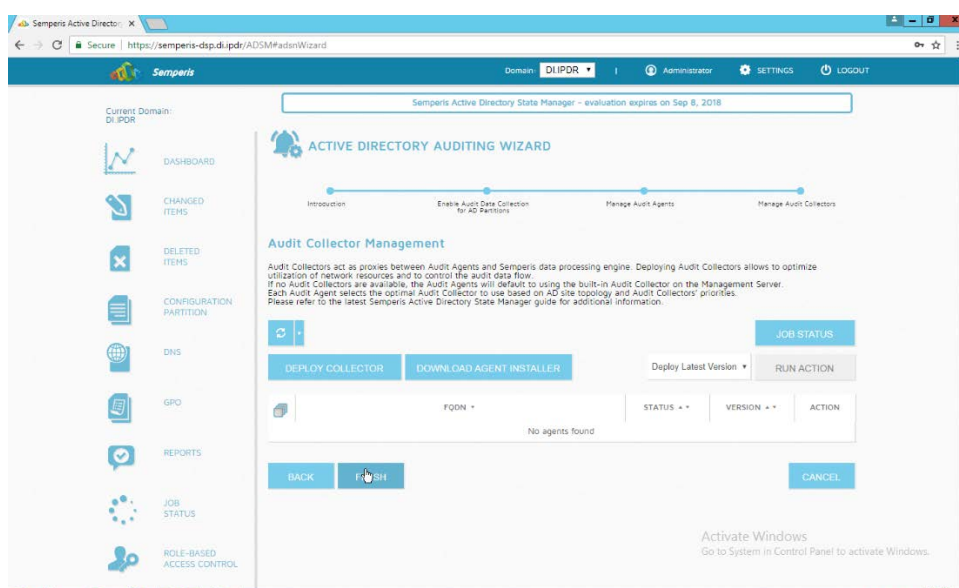


36. Click **OK**.

37. Wait for the deployment to finish.



38. Click **Next**.



39. Click **Finish**.

## 2.11 Micro Focus ArcSight Enterprise Security Manager

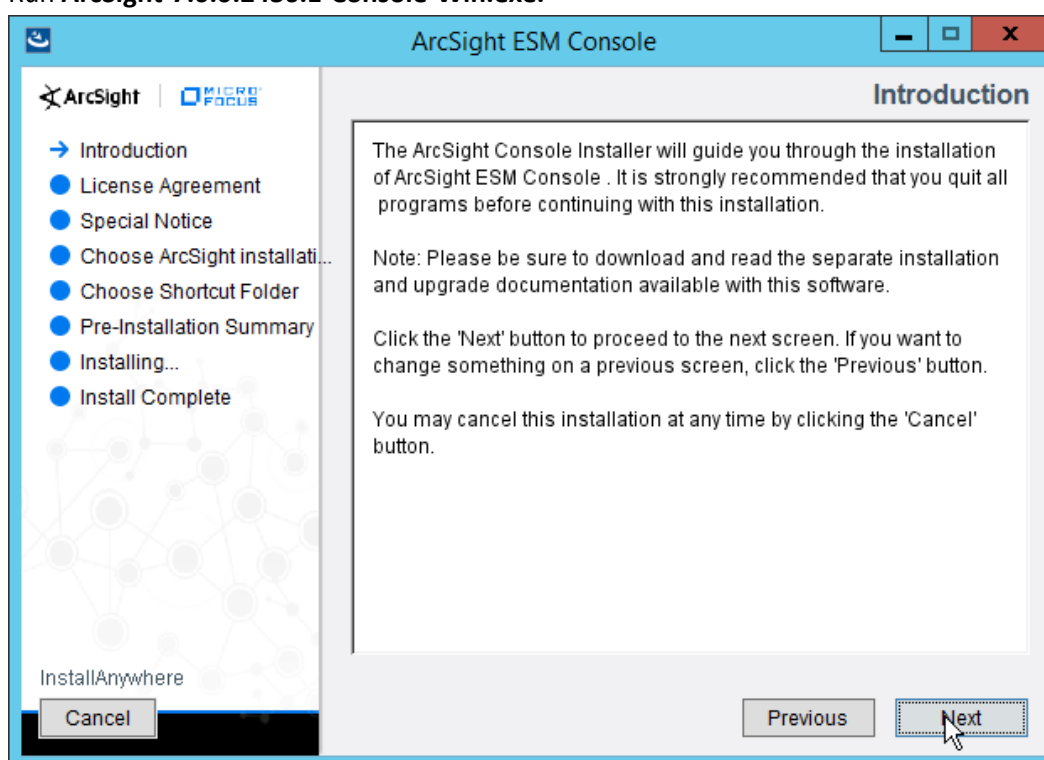
Micro Focus ArcSight Enterprise Security Manager is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

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

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

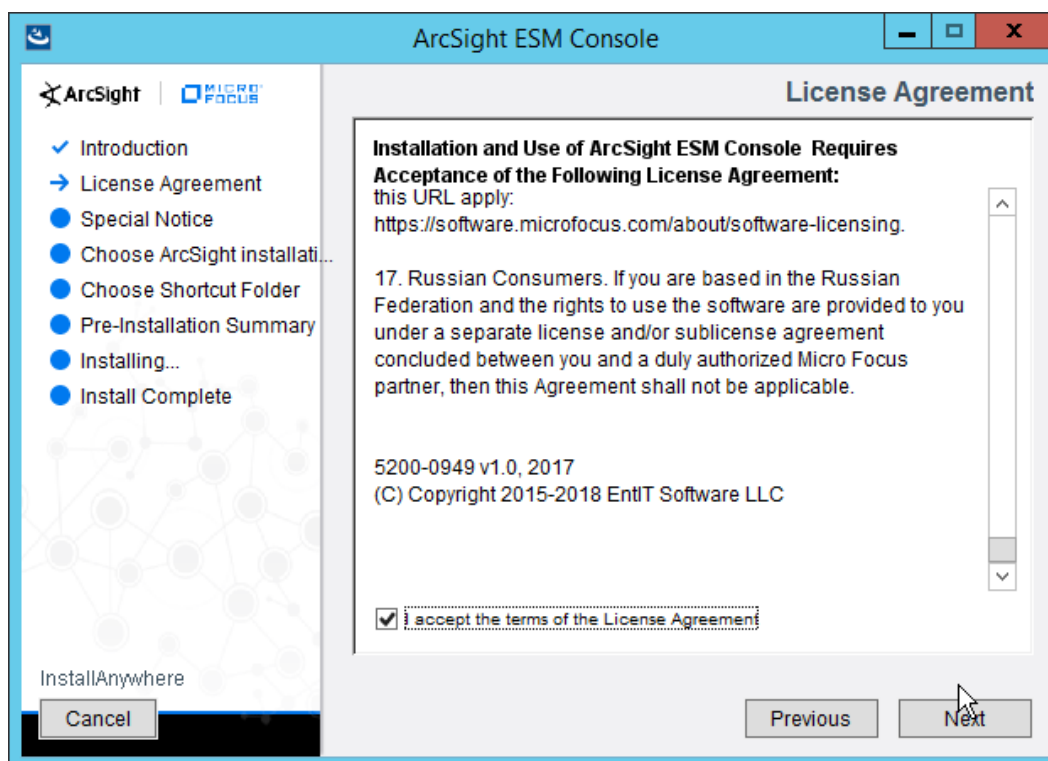
### 2.11.1 Install the ArcSight Console

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

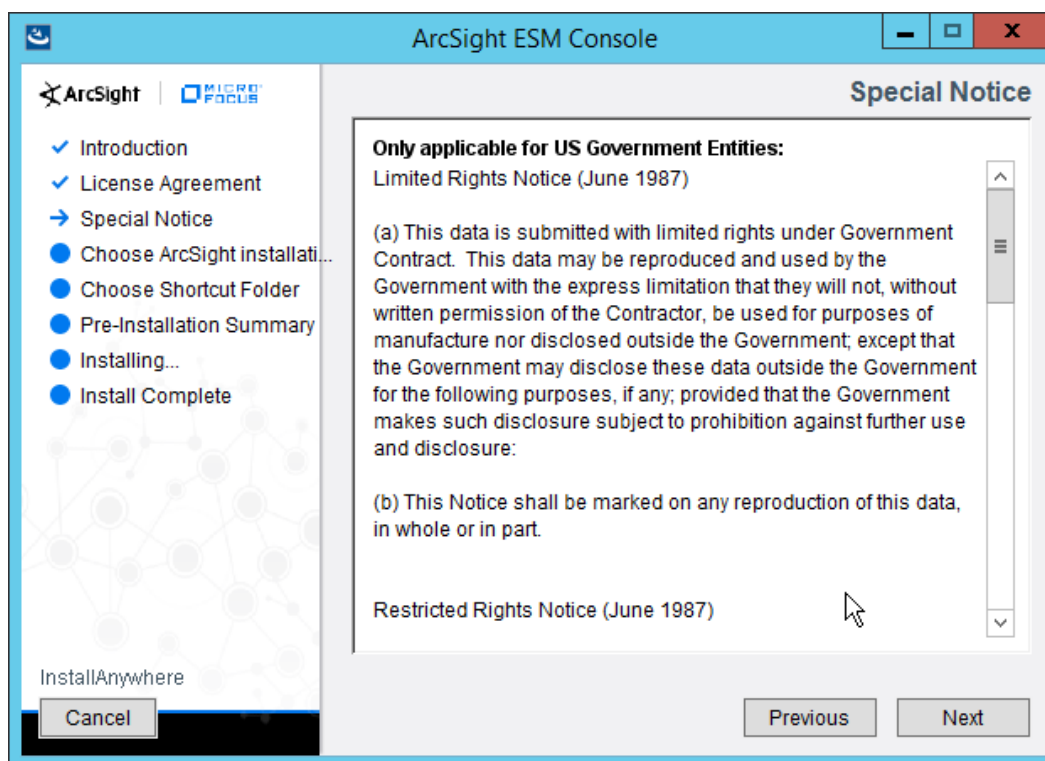


2. Click **Next**.
3. Check the box next to **I accept the License Agreement**.

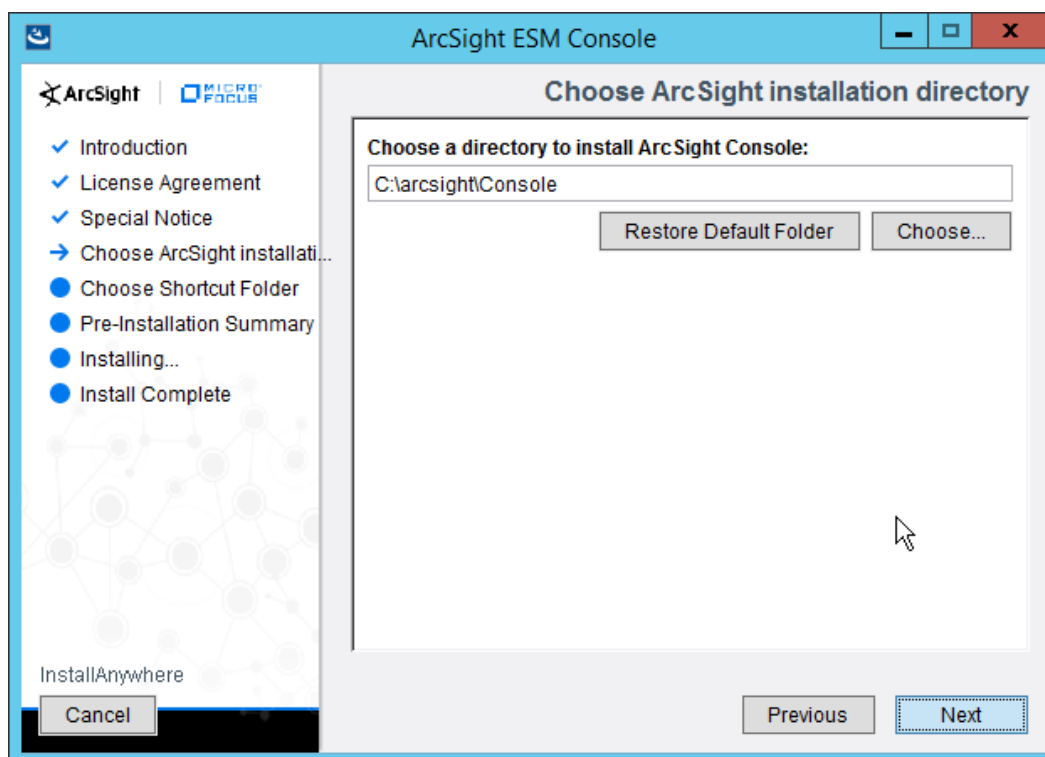




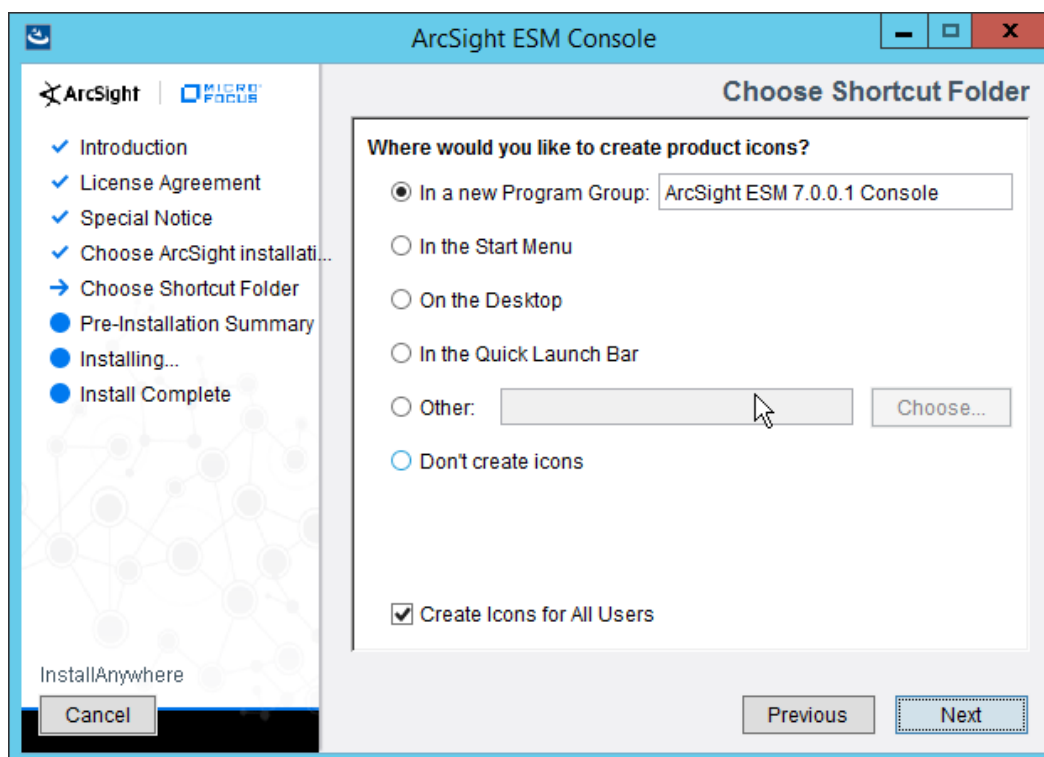
4. Click **Next**.



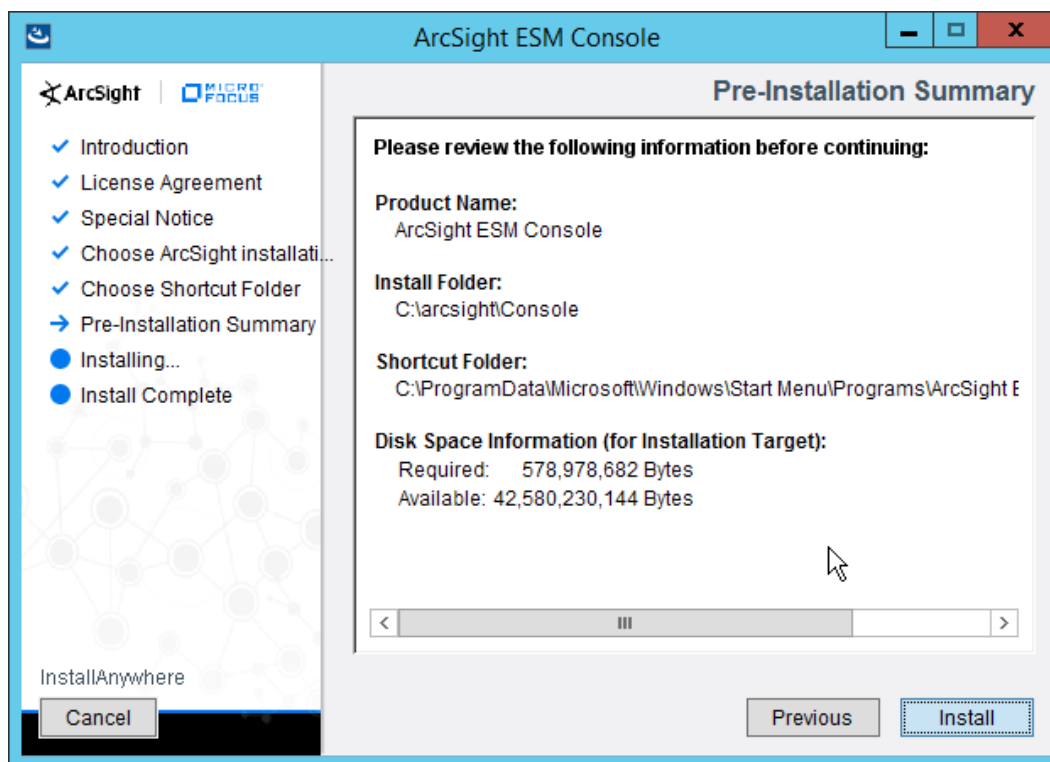
5. Click **Next**.



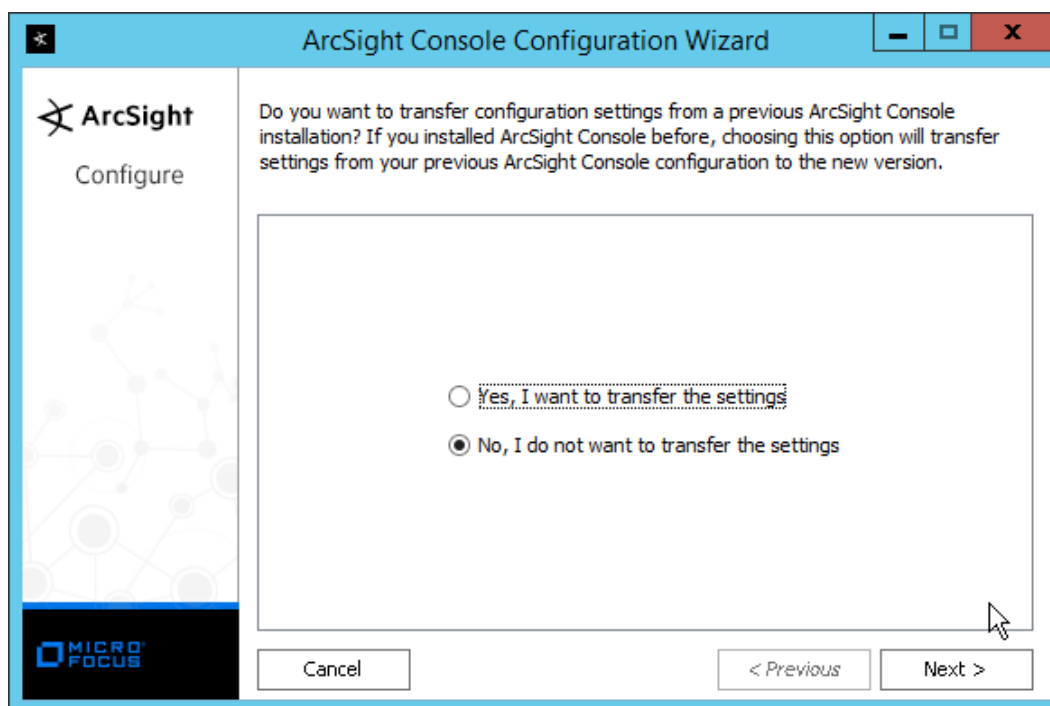
6. Click **Next**.



7. Click **Next**.

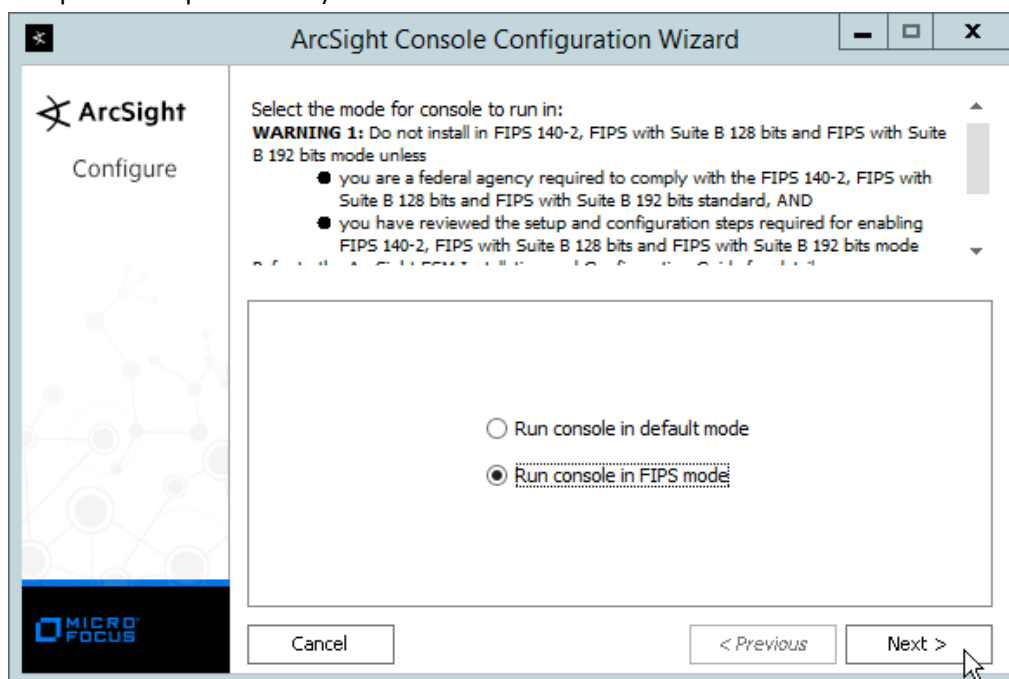


8. Click **Install**.
9. Select **No, I do not want to transfer the settings**.

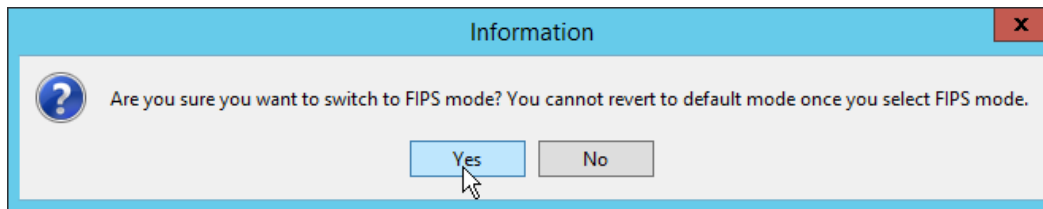


10. Click **Next**.

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

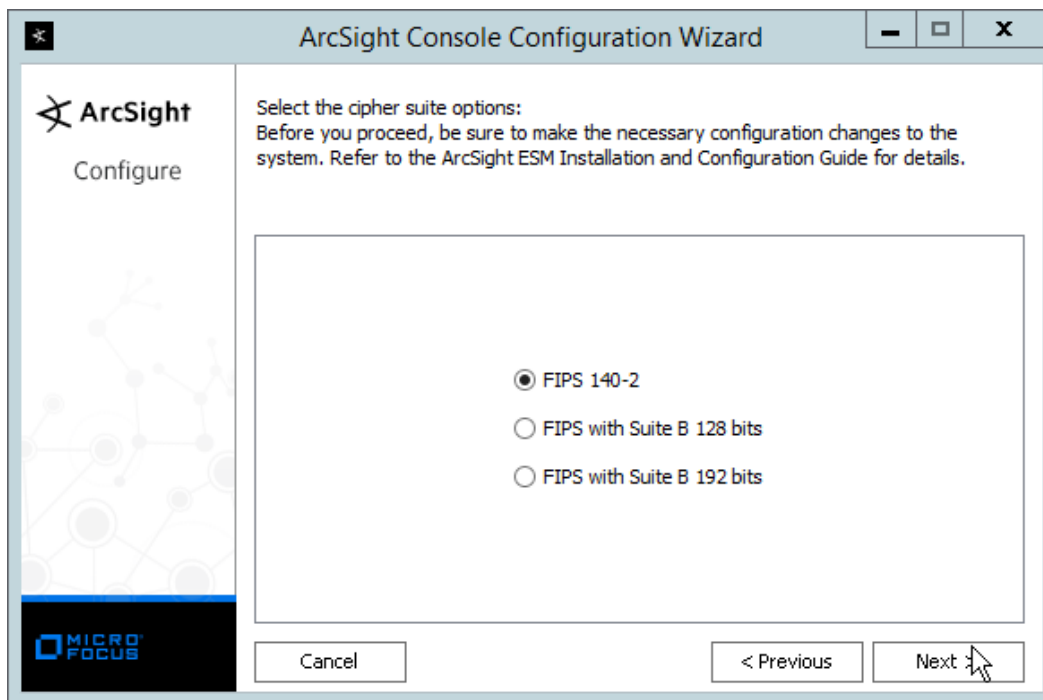


12. Click **Next**.



13. Click **Yes**.

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



15. Click **Next**.

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

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

**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

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.

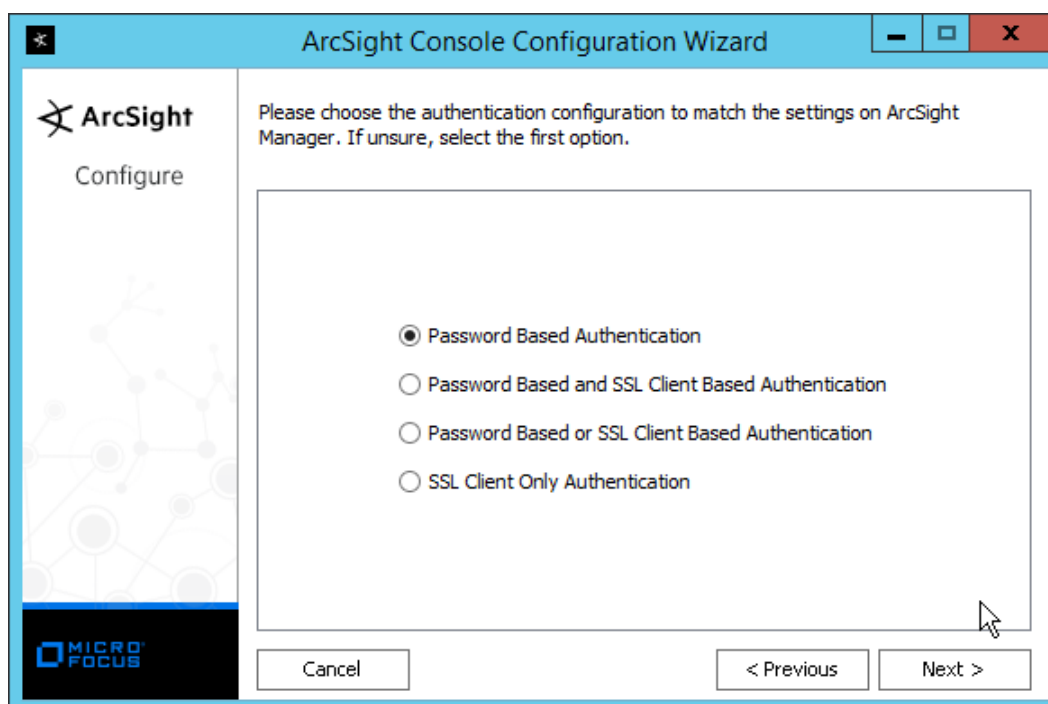
☒ Use direct connection.

☐ Use proxy server.

Cancel < Previous Next >

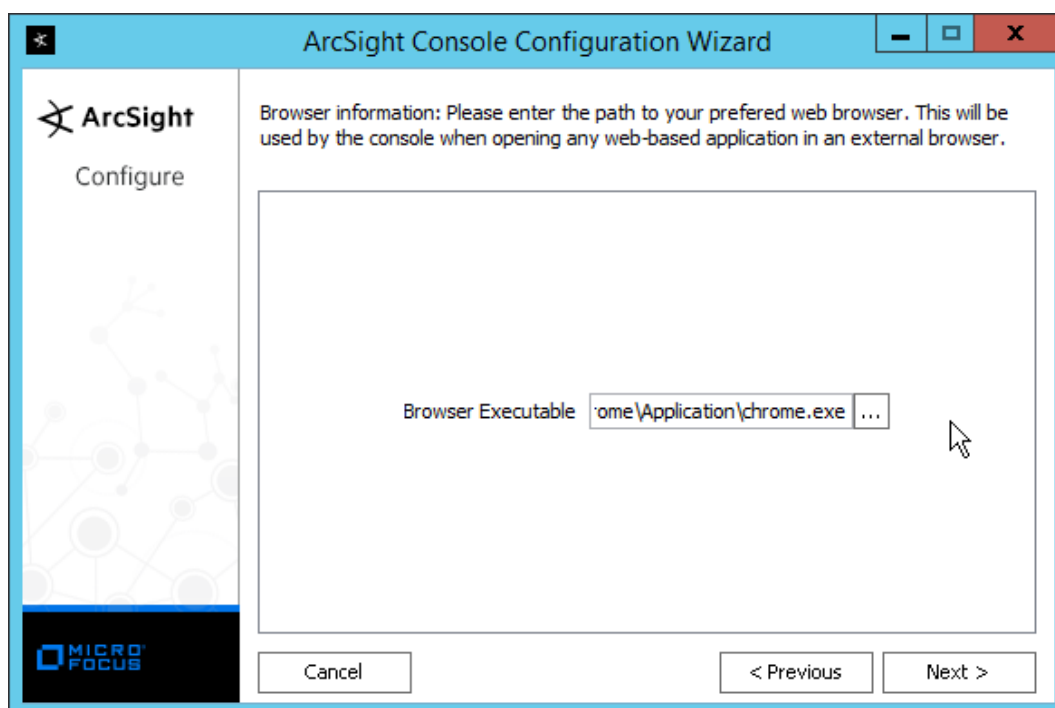


20. Click **Next**.

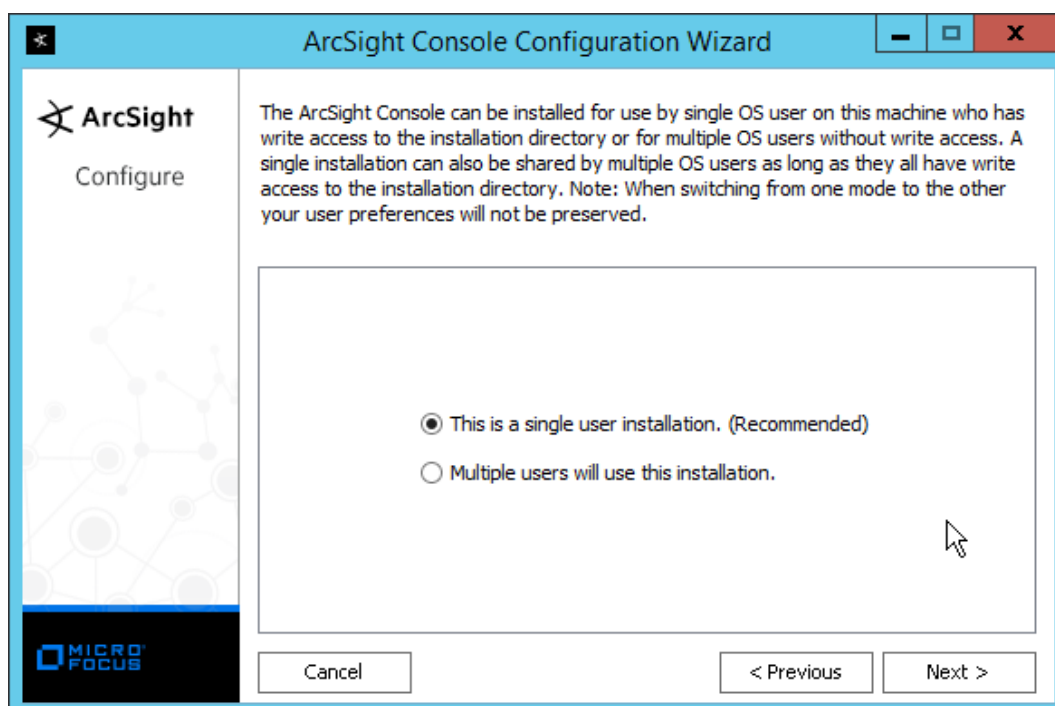


21. Click **Next**.

22. Select your preferred browser.

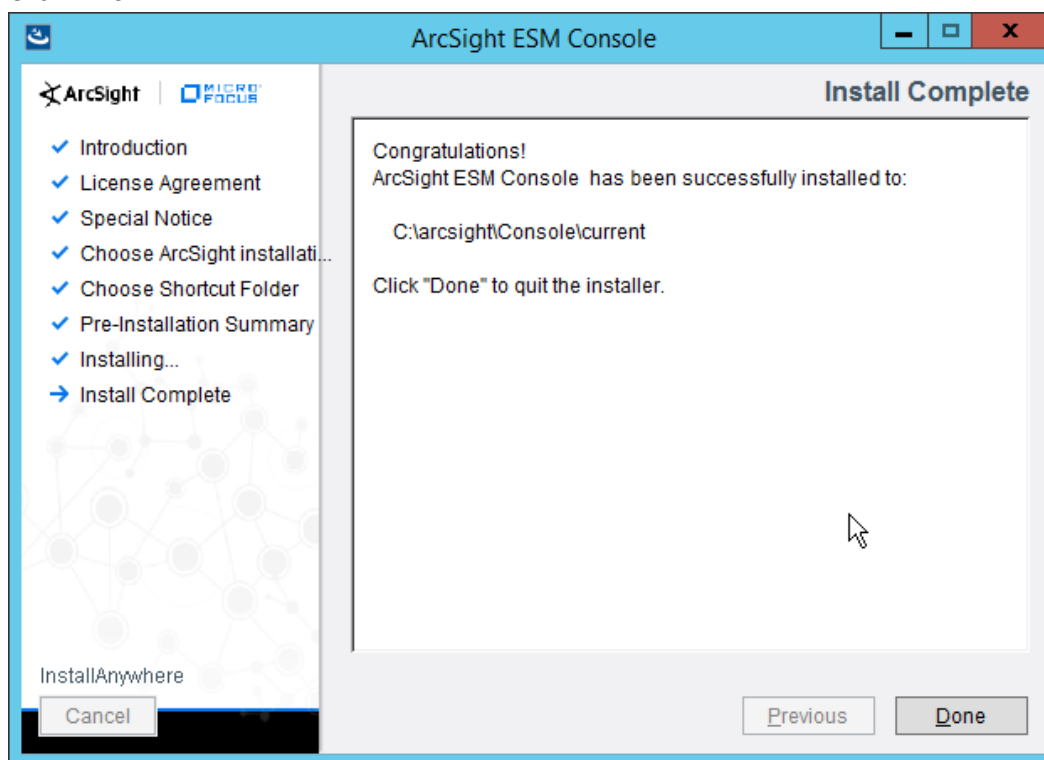


23. Click **Next**.



24. Click **Next**.

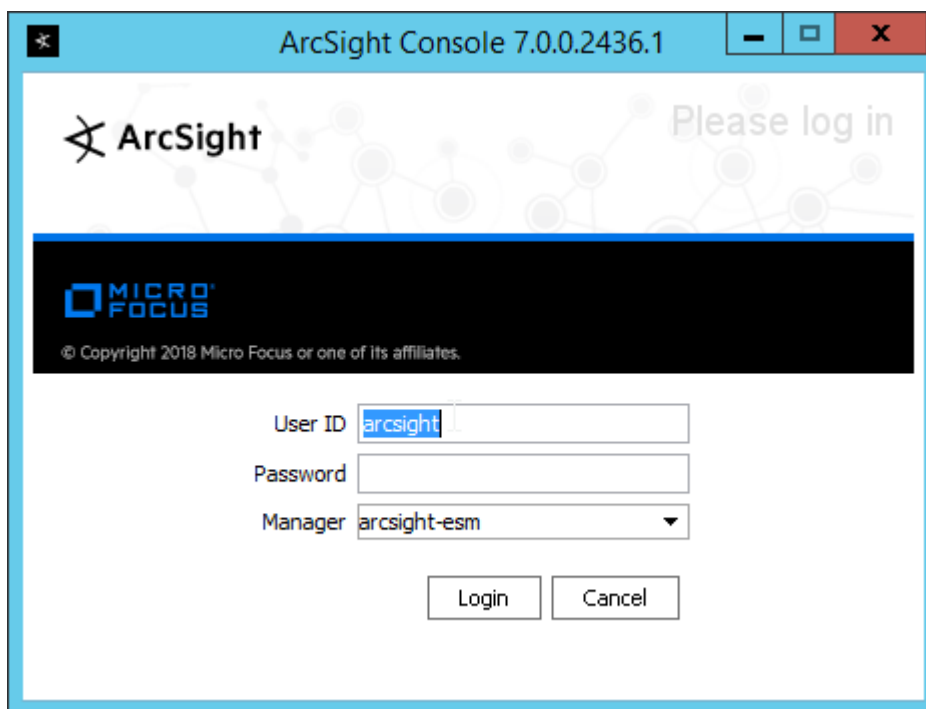
25. Click **Finish**.



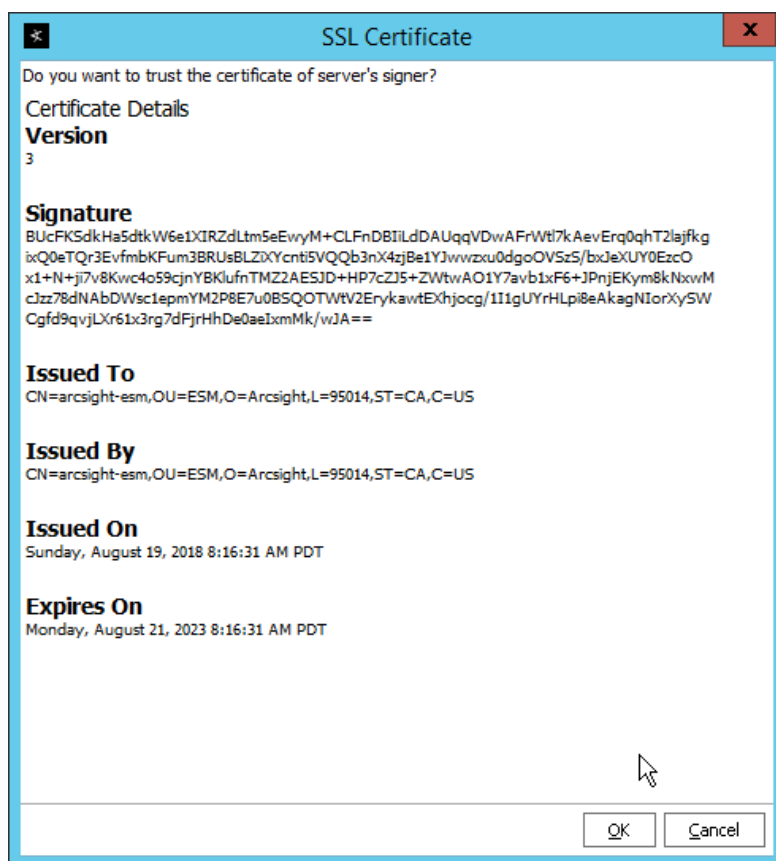
26. Click **Done**.

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

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



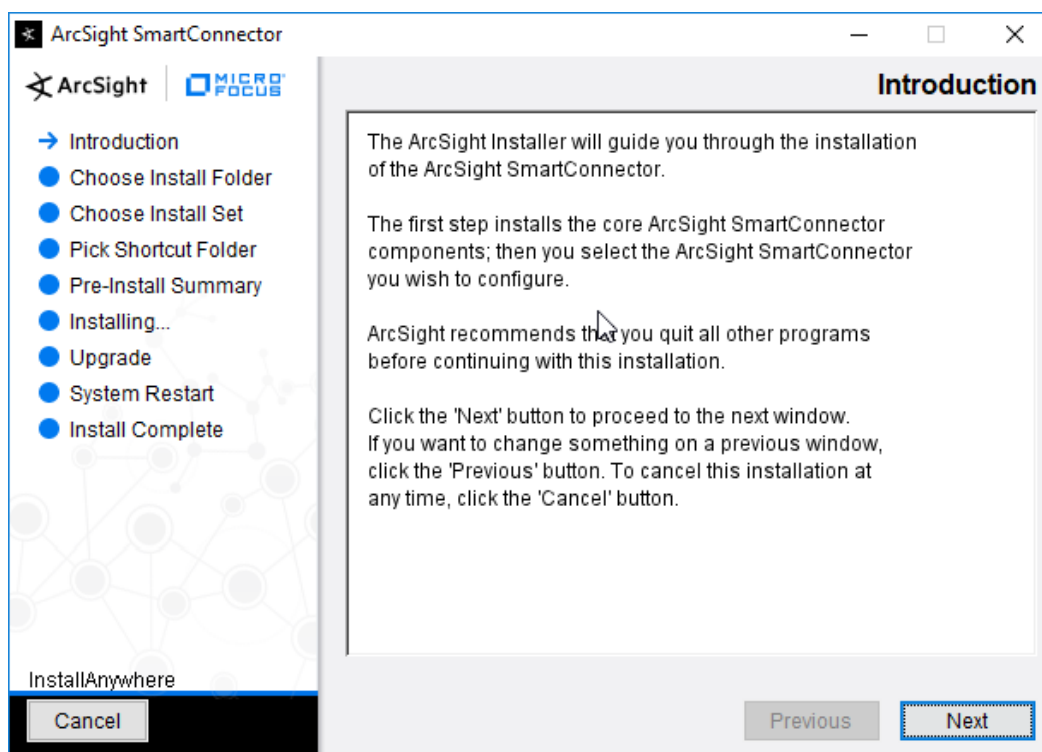
29. Click **Login**. (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)



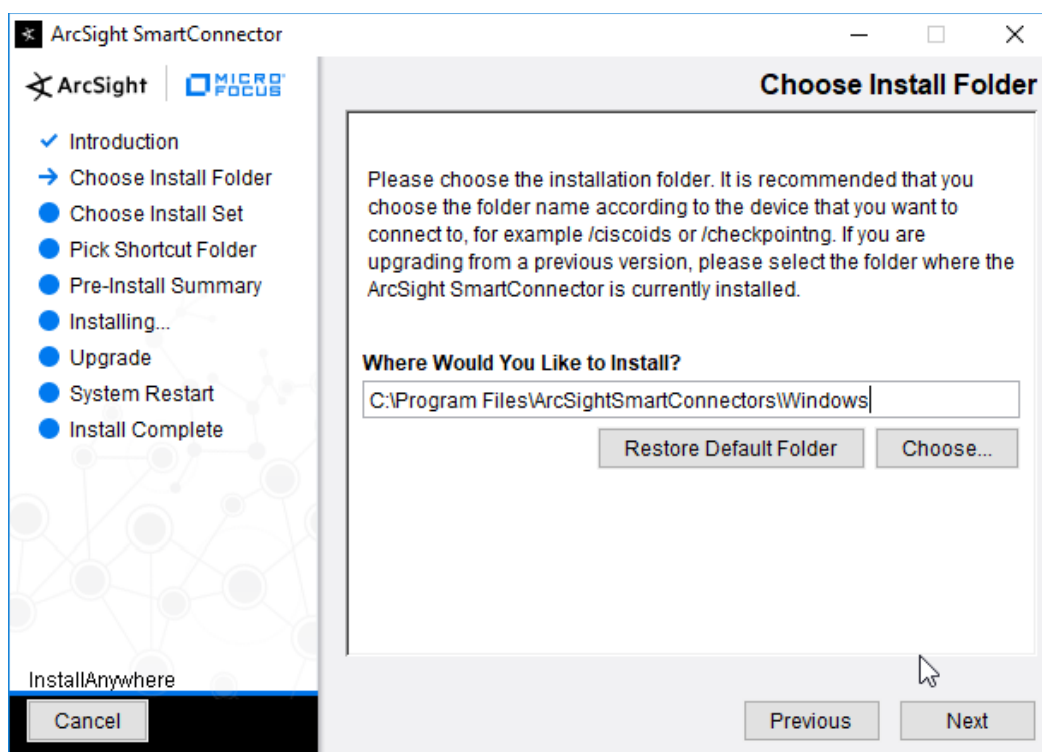
30. Click **OK**.

## 2.11.2 Install Individual ArcSight Windows Connectors

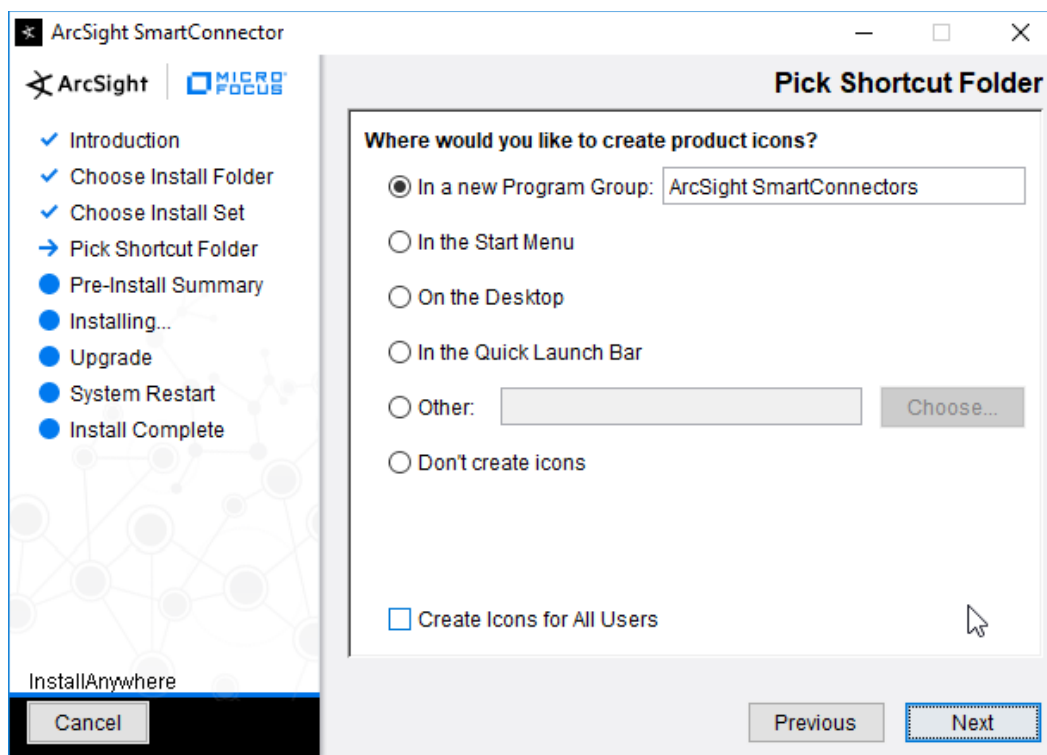
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



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

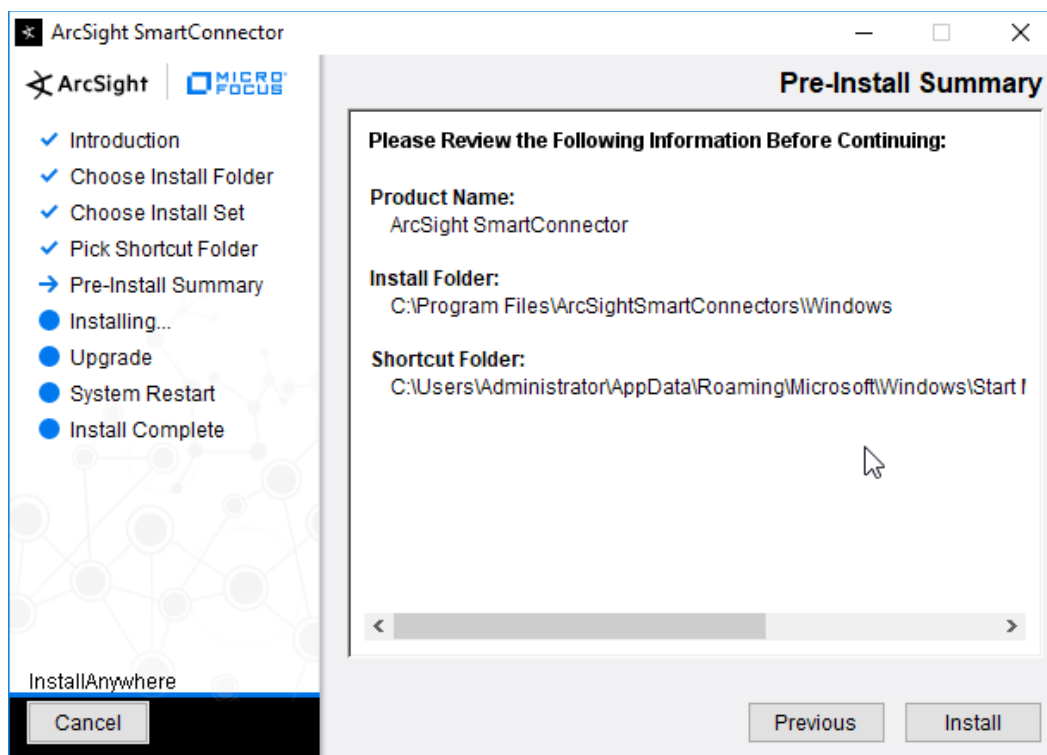


4. Click **Next**.

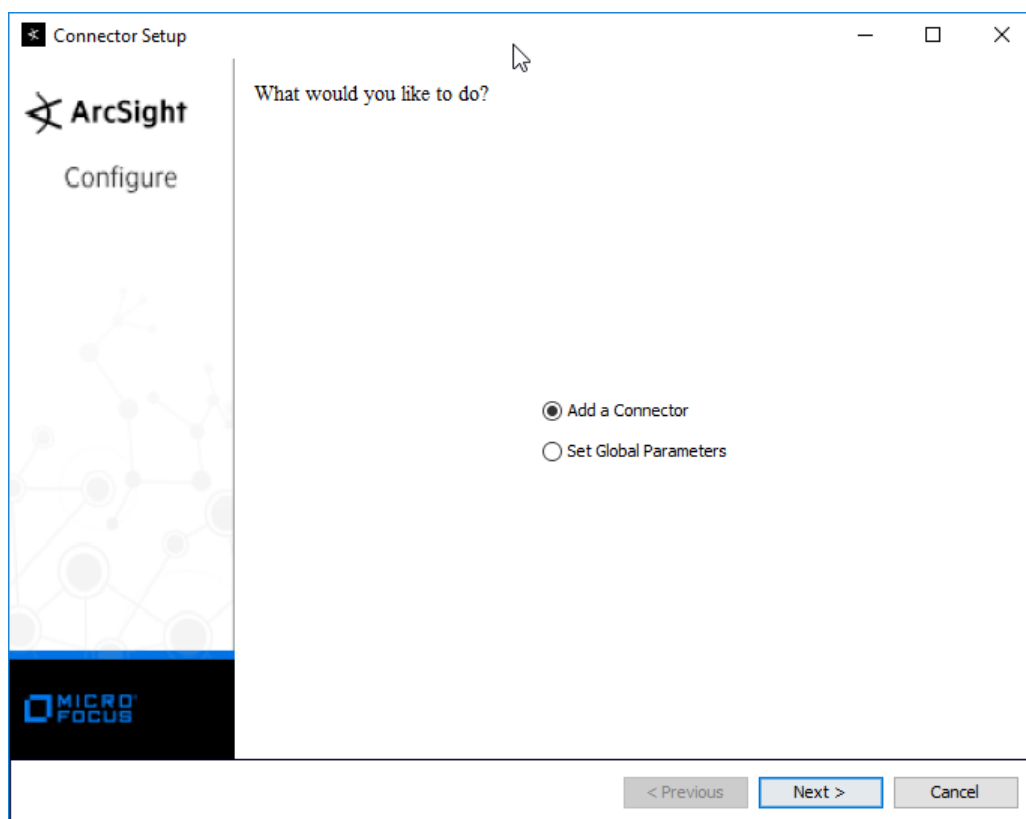


5. Click **Next**.

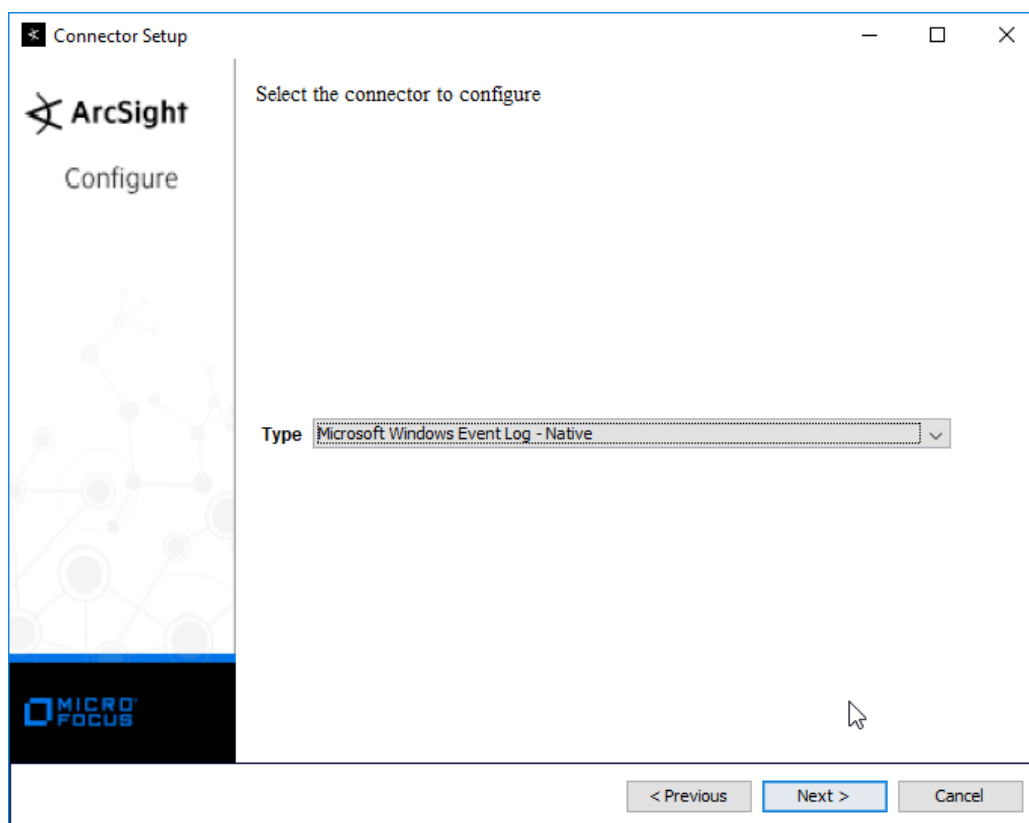




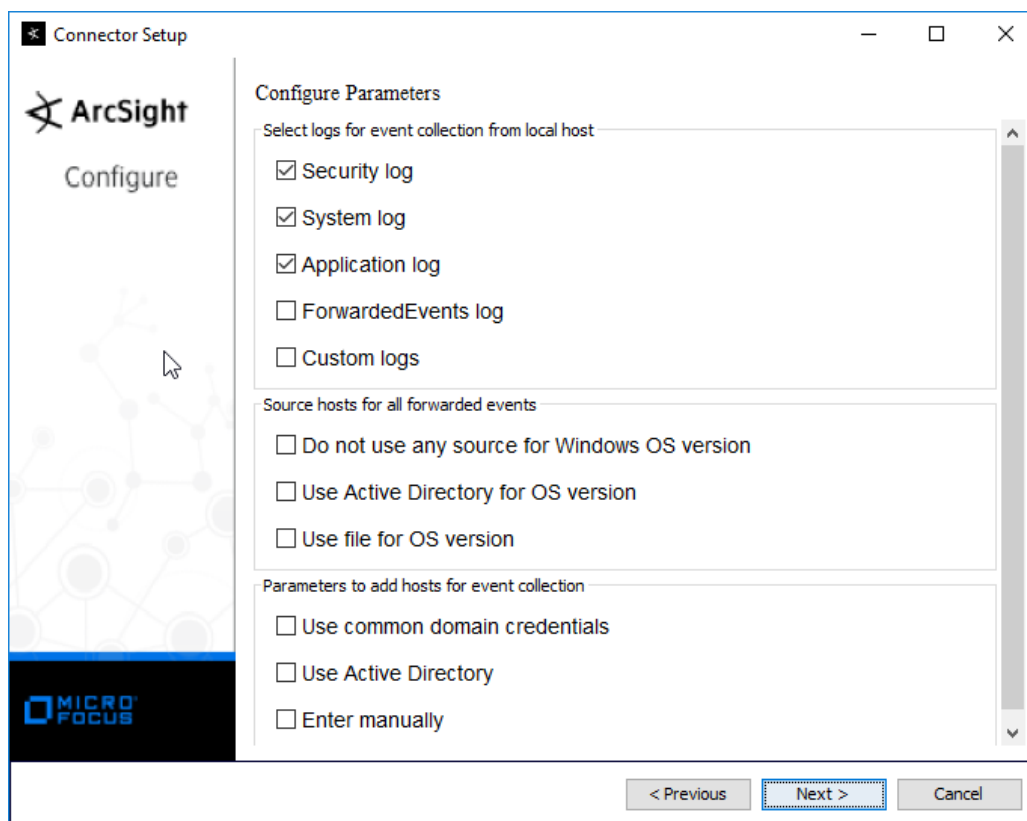
6. Click **Install**.
7. Select **Add a Connector**.



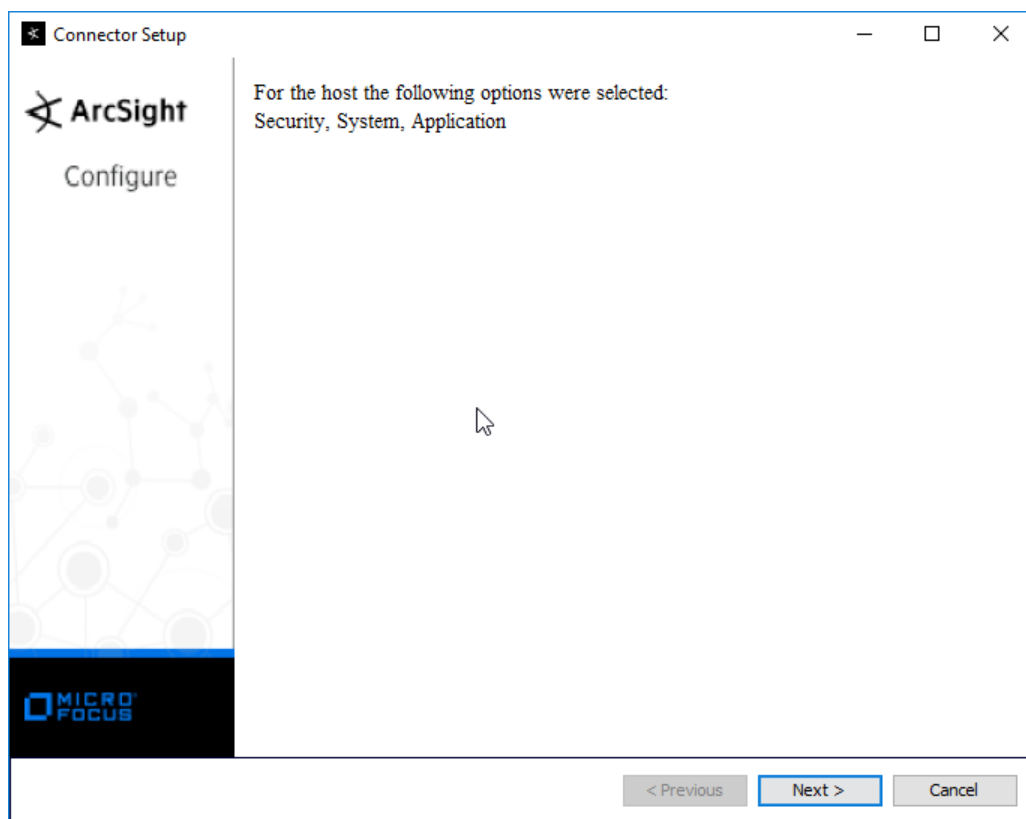
8. Click **Next**.
9. Select **Microsoft Windows Event Log–Native**.



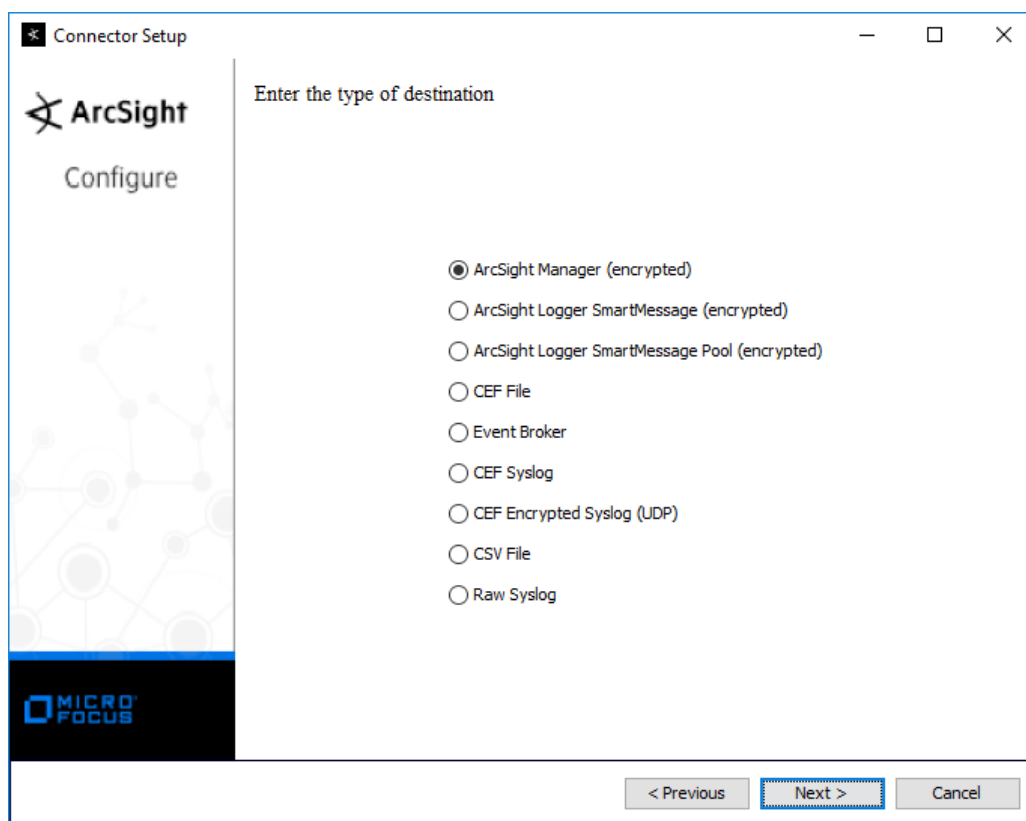
10. Click **Next**.



11. Click **Next**.



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



14. Click **Next**.

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

Connector Setup

ArcSight  
Configure

Enter the destination parameters

Manager Hostname: arcsight-esm

Manager Port: 8443

User: administrator

Password: ••••••••

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: false

< Previous   Next >   Cancel

16. Click **Next**.

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

Connector Setup

ArcSight  
Configure

Enter the connector details

Name: Windows 10-1

Location:

DeviceLocation:

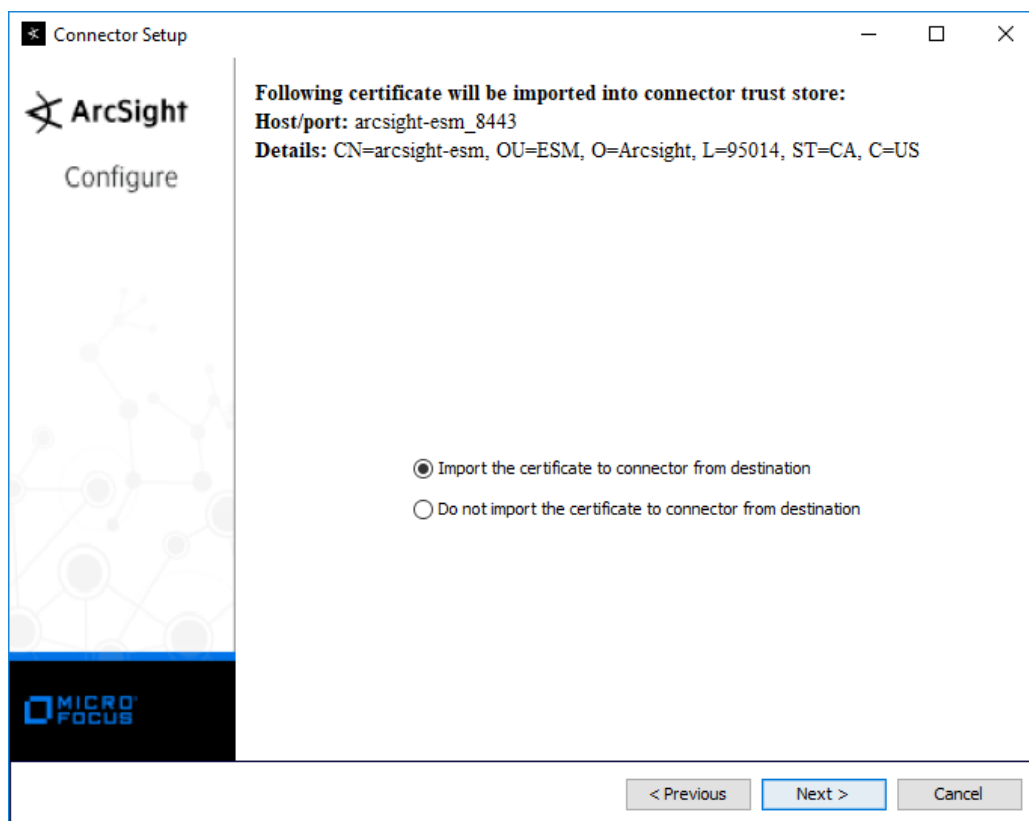
Comment: Windows 10-1 Client

< Previous   Next >   Cancel

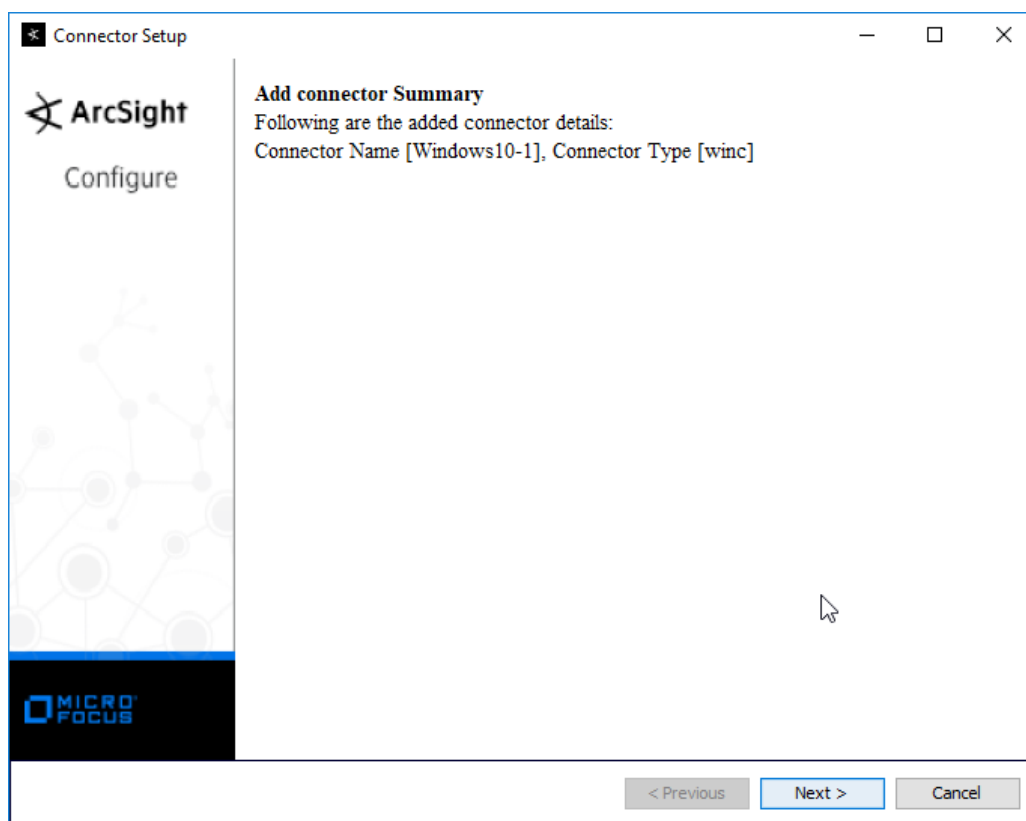
18. Click **Next**.

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

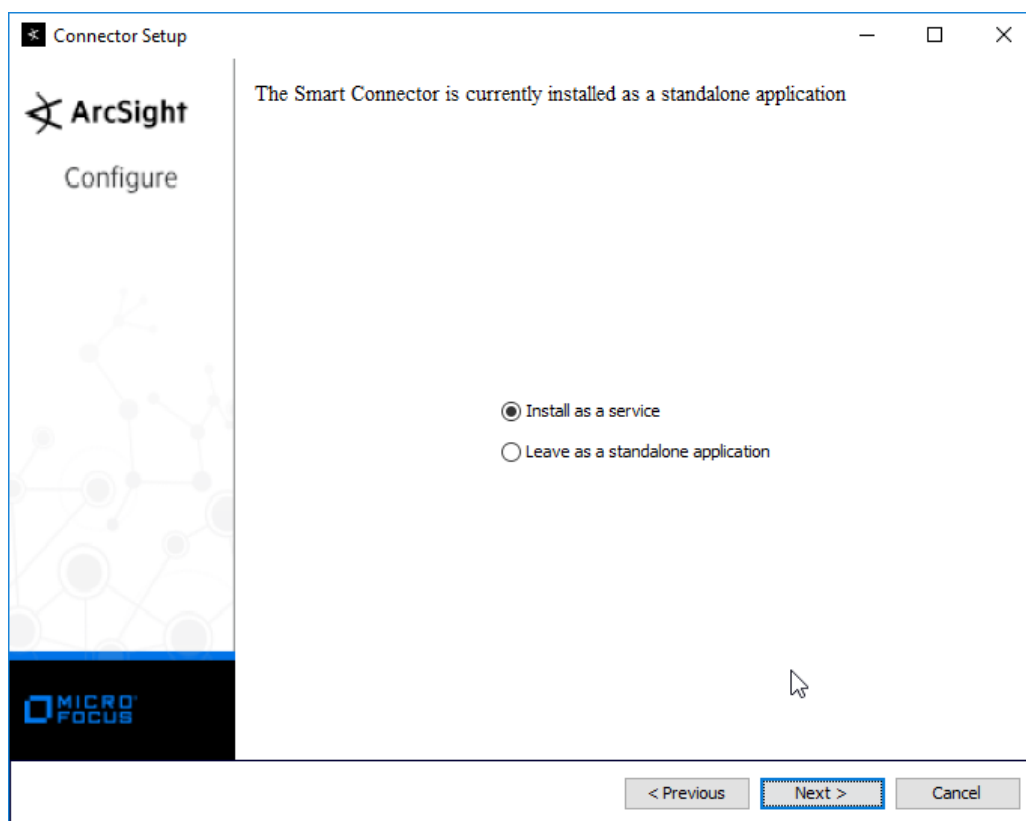




20. Click **Next**.



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

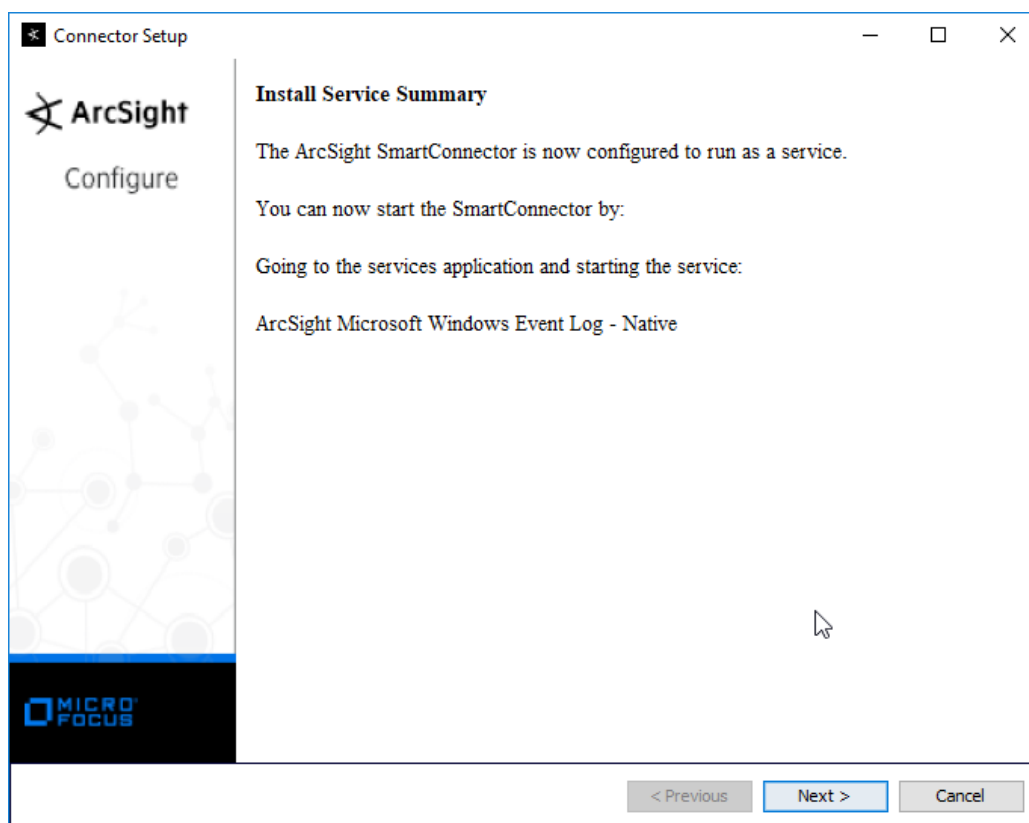


23. Click **Next**.

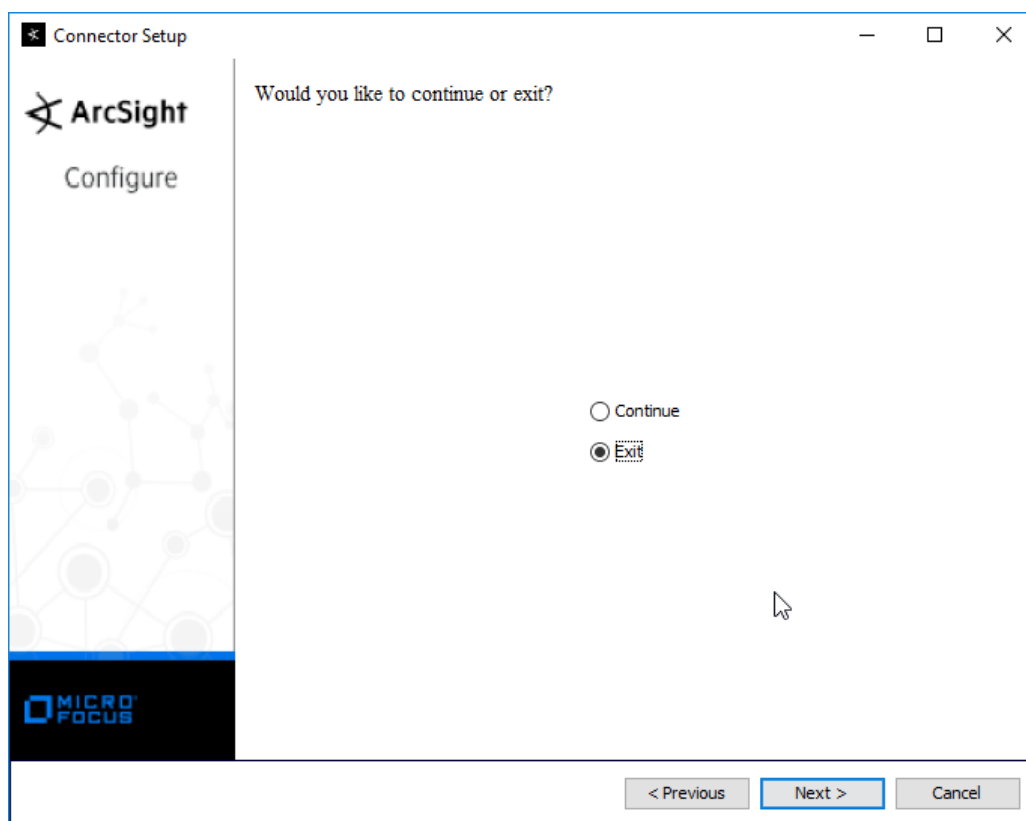
The screenshot shows a window titled "Connector Setup" with a standard Windows title bar (minimize, maximize, close buttons). On the left is a sidebar with the ArcSight logo and the word "Configure". The main area is titled "Specify the service parameters". It contains three configuration items: "Service Internal Name" with a text box containing "winc", "Service Display Name" with a text box containing "Microsoft Windows Event Log - Native", and "Start the service automatically" with a dropdown menu set to "Yes". At the bottom right are three buttons: "< Previous", "Next >" (which is highlighted with a blue dashed border), and "Cancel". A mouse cursor is visible over the "Next >" button. The Micro Focus logo is in the bottom left corner of the window.

Parameter	Value
Service Internal Name	winc
Service Display Name	Microsoft Windows Event Log - Native
Start the service automatically	Yes

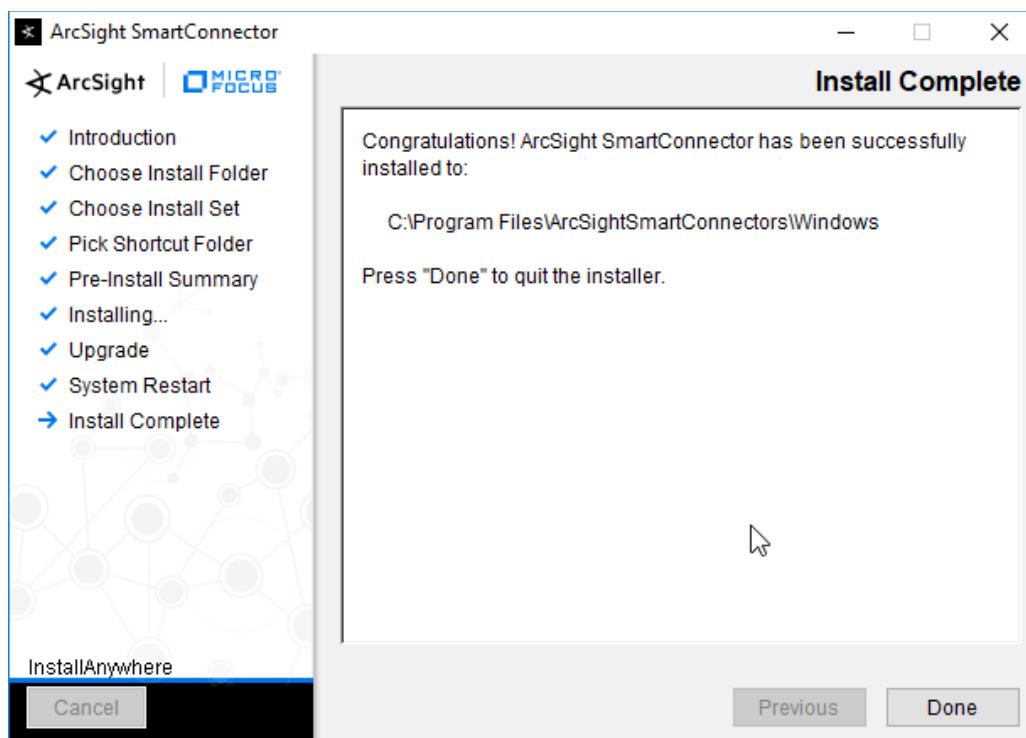
24. Click **Next**.



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



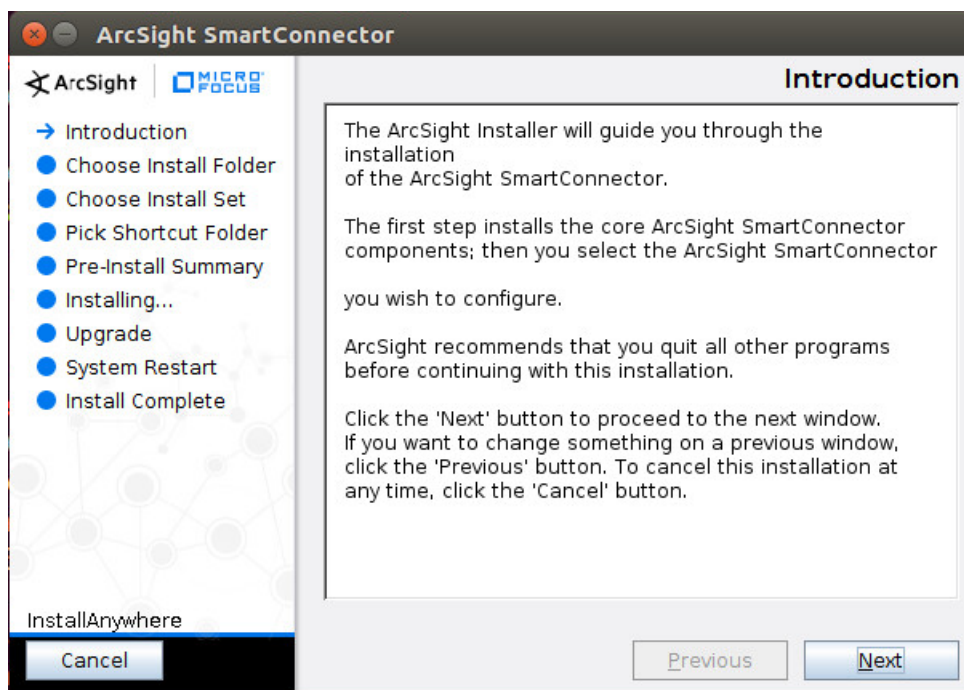
27. Click **Next**.



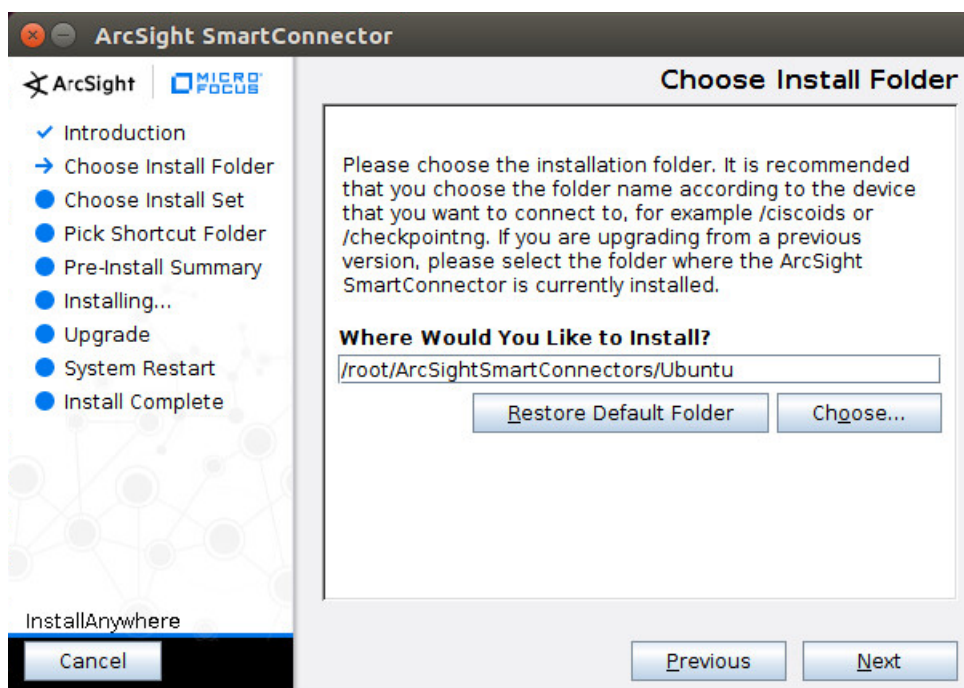
28. Click **Done**.

### 2.11.3 Install Individual ArcSight Ubuntu Connectors

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

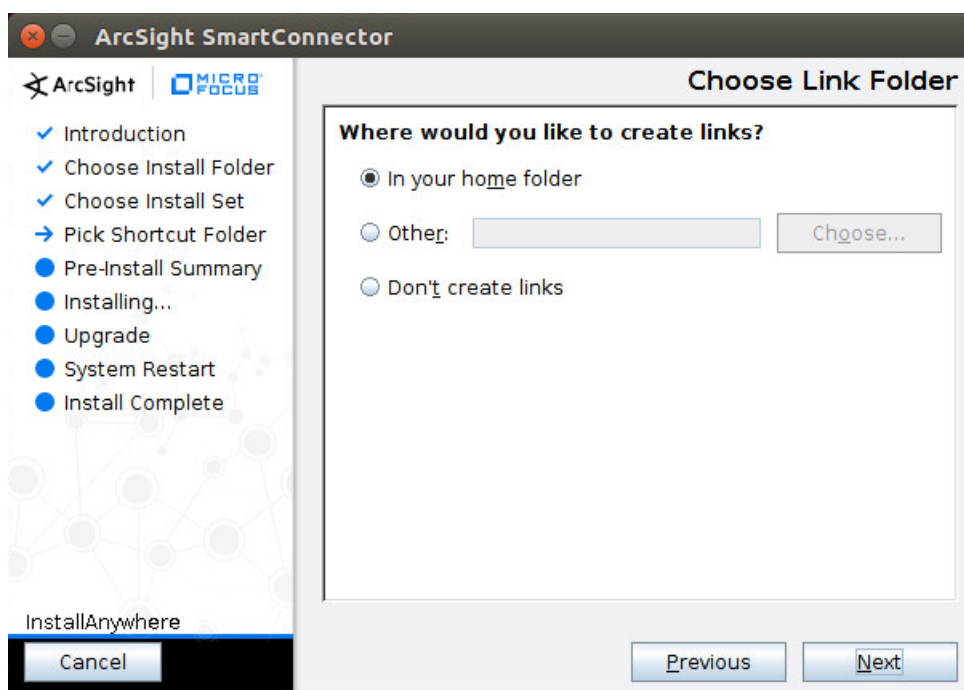


3. Click **Next**.
4. Enter `/root/ArcSightSmartConnectors/Ubuntu`.

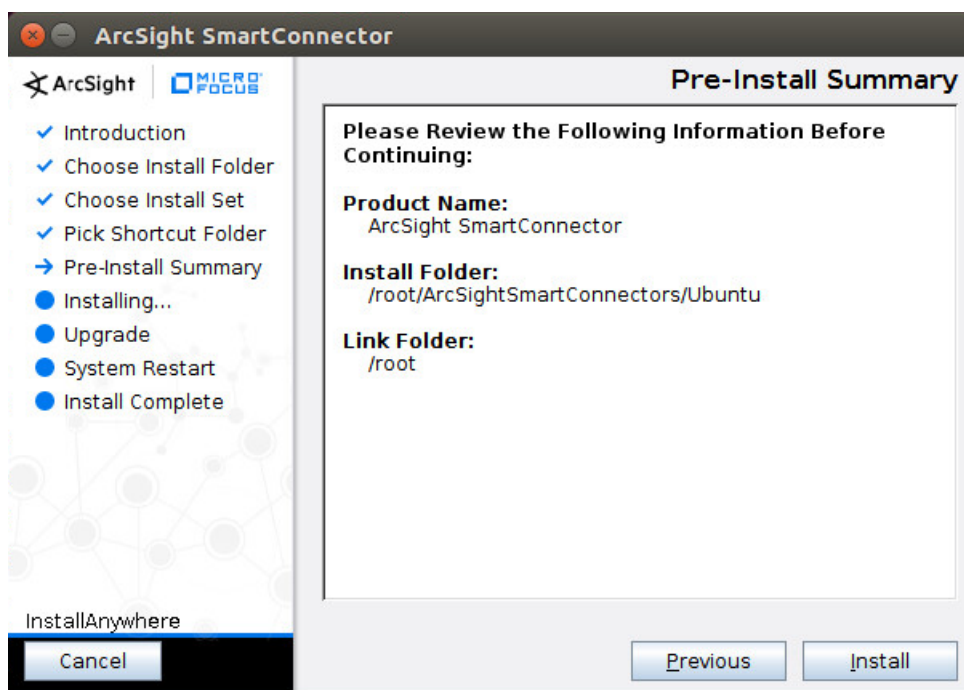




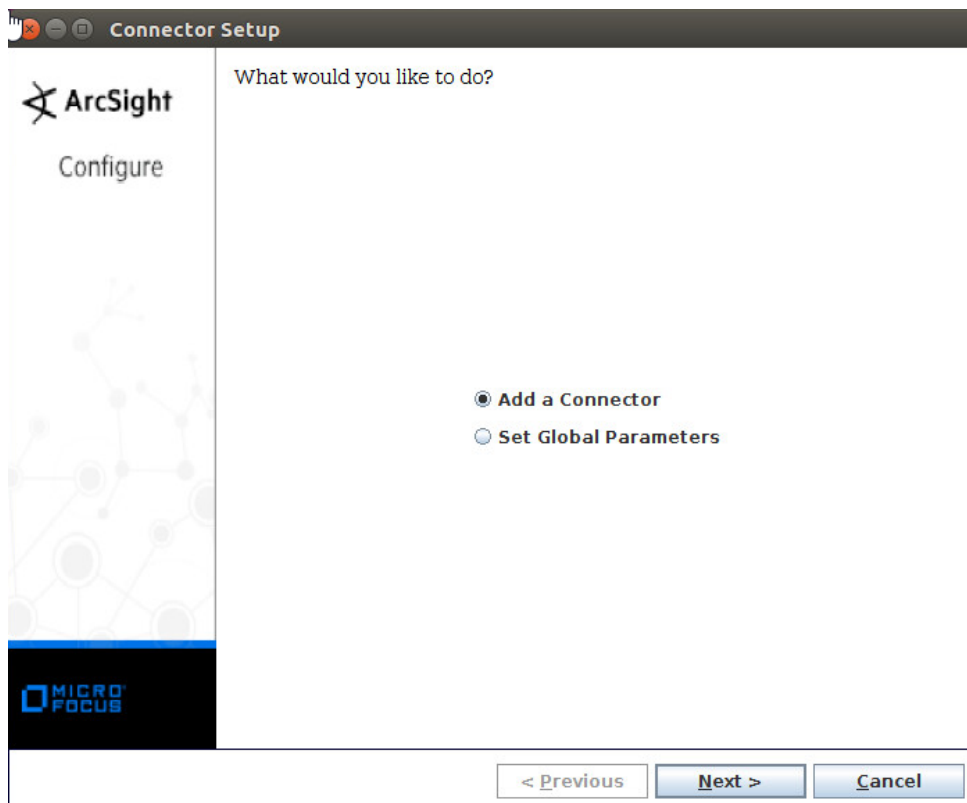
5. Click **Next**.



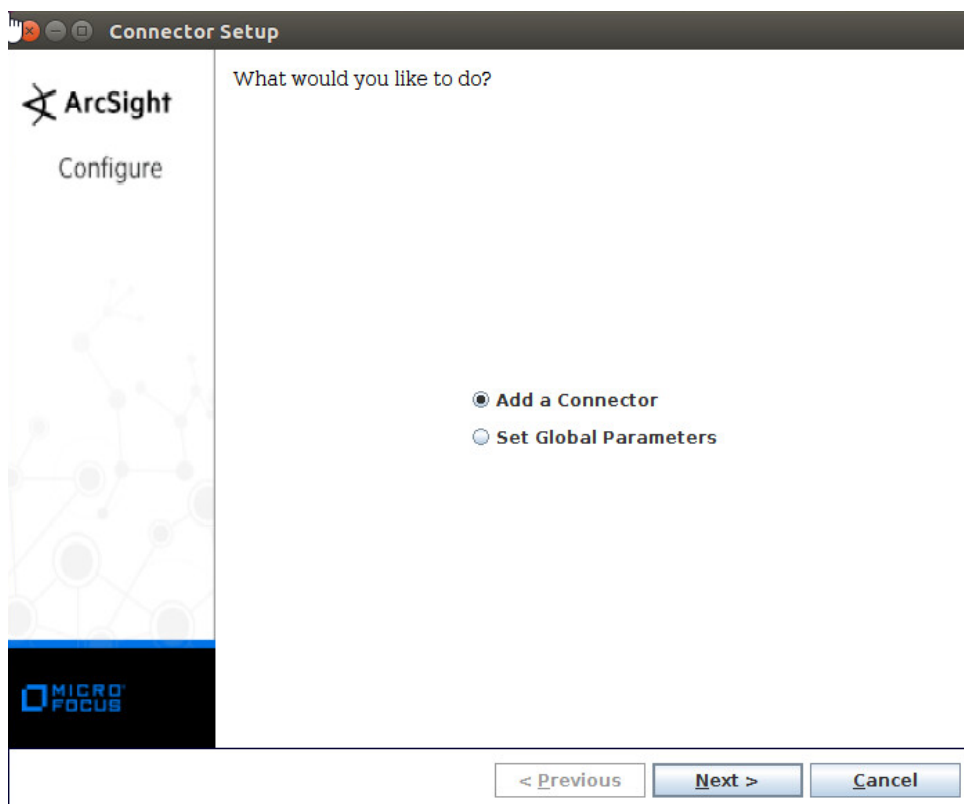
6. Click **Next**.



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



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



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

Connector Setup

ArcSight  
Configure

Enter the parameter details

File Absolute Path Name

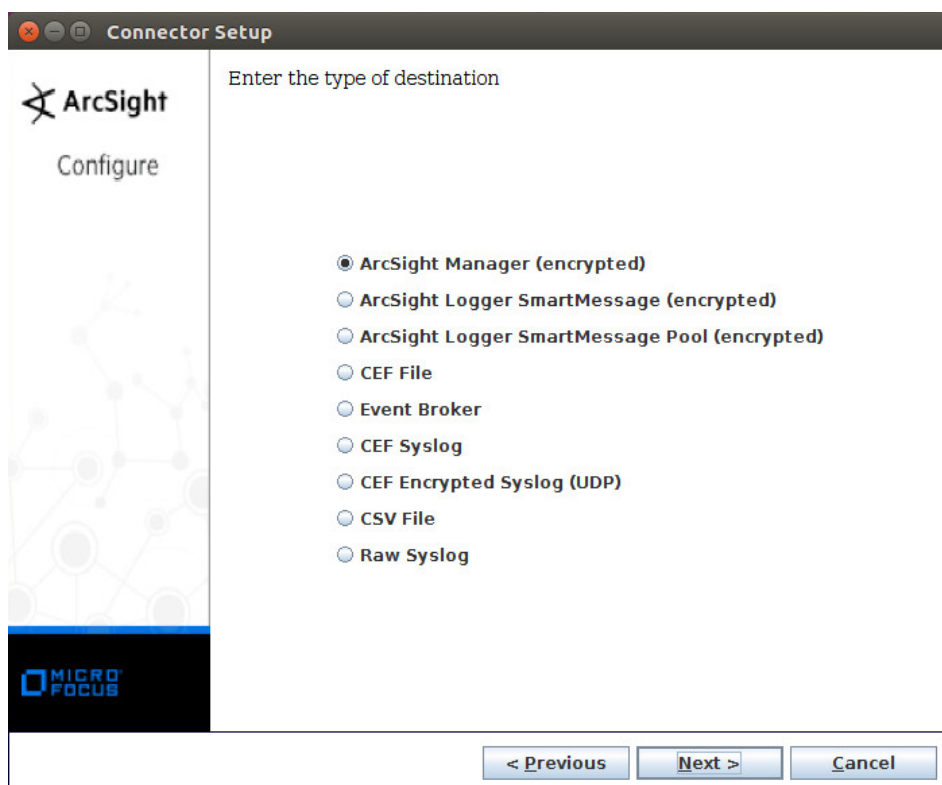
Reading Events Real Time or Batch

Action Upon Reaching EOF

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: Ubuntu Client

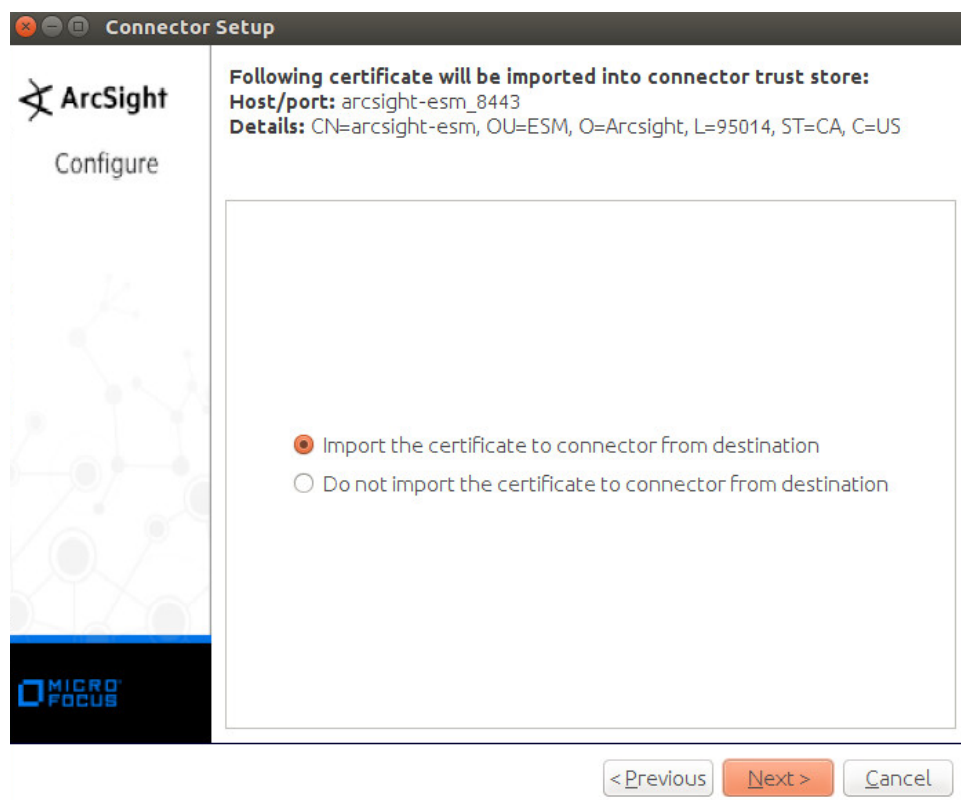
Location:

DeviceLocation:

Comment:

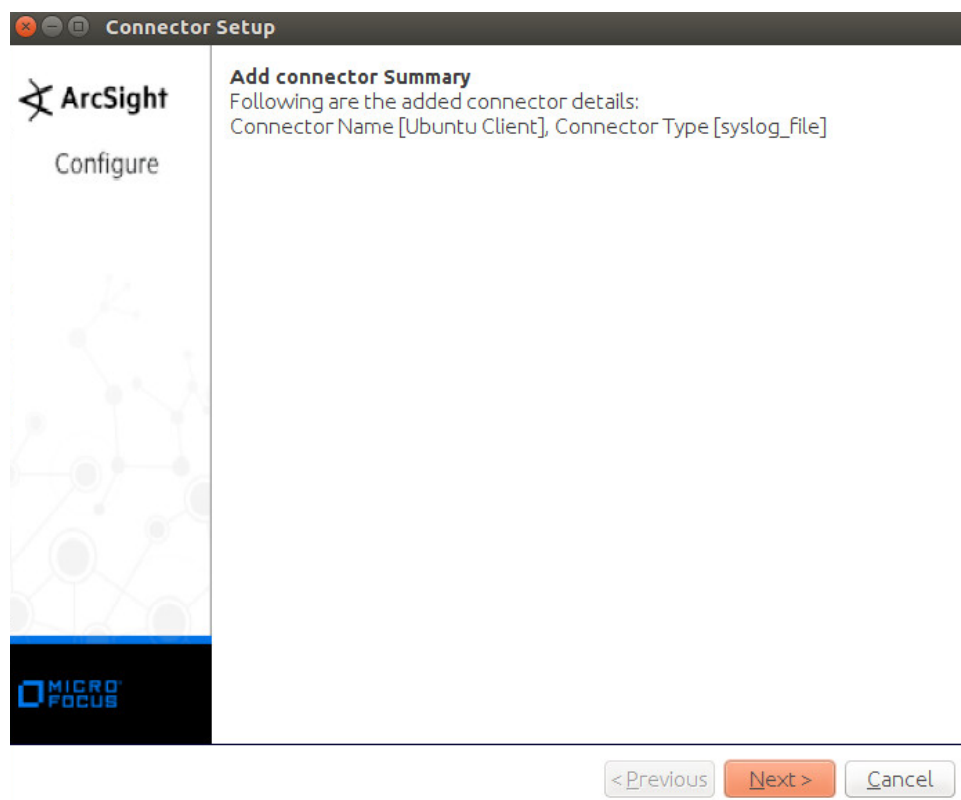
< Previous   Next >   Cancel

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

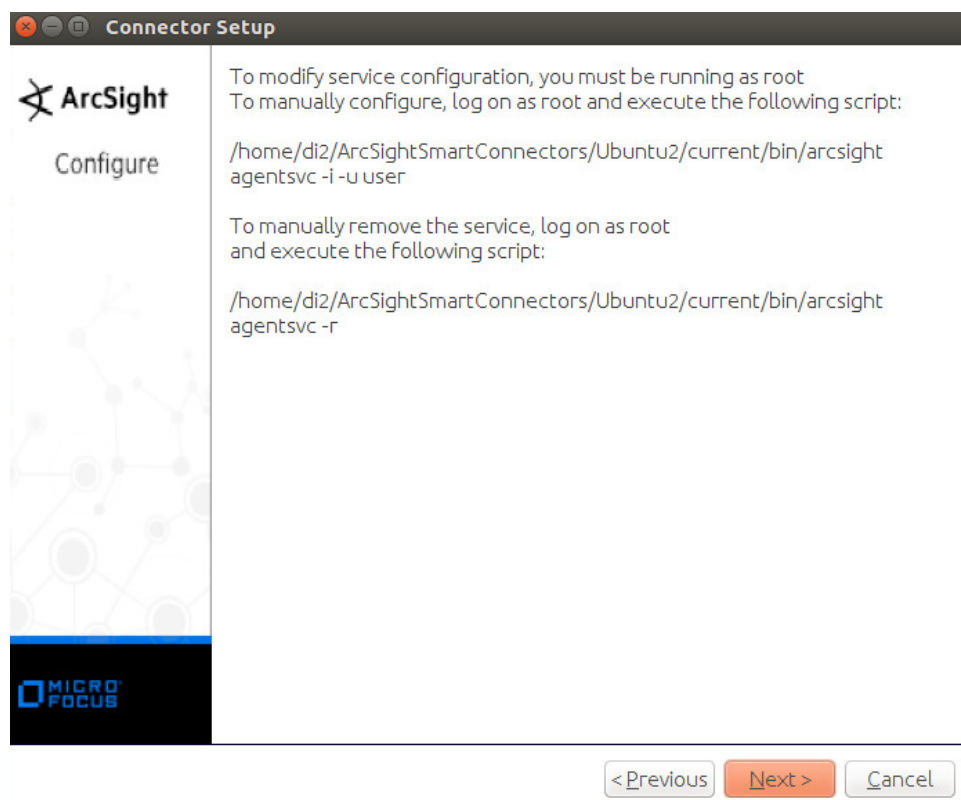


21. Click **Next**.

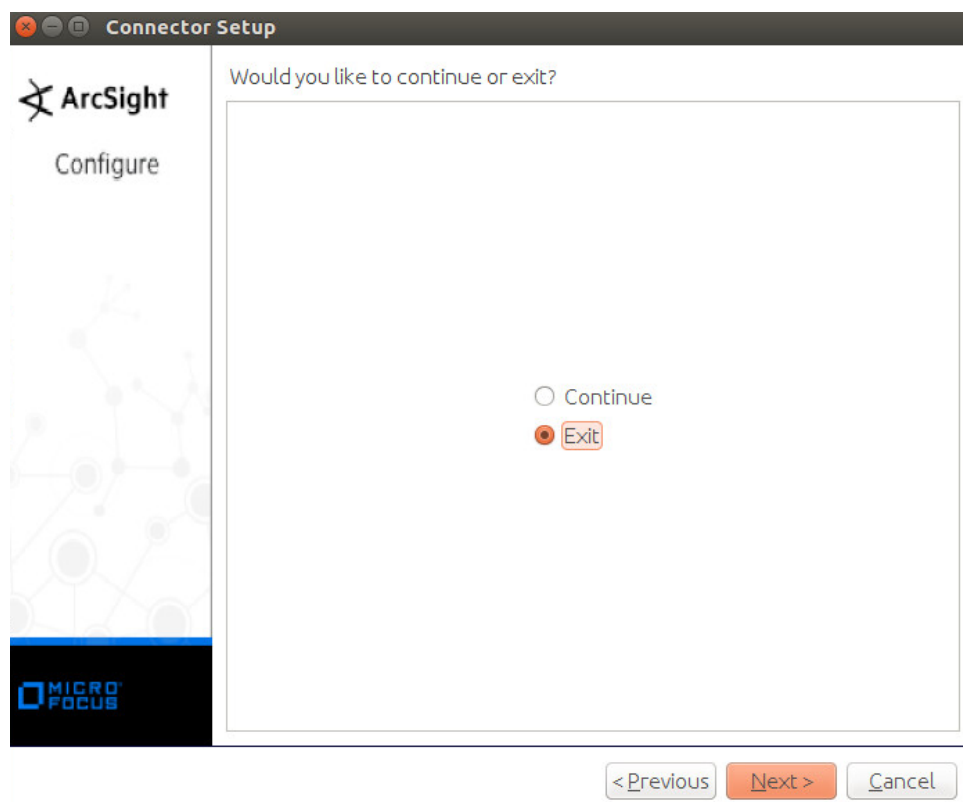




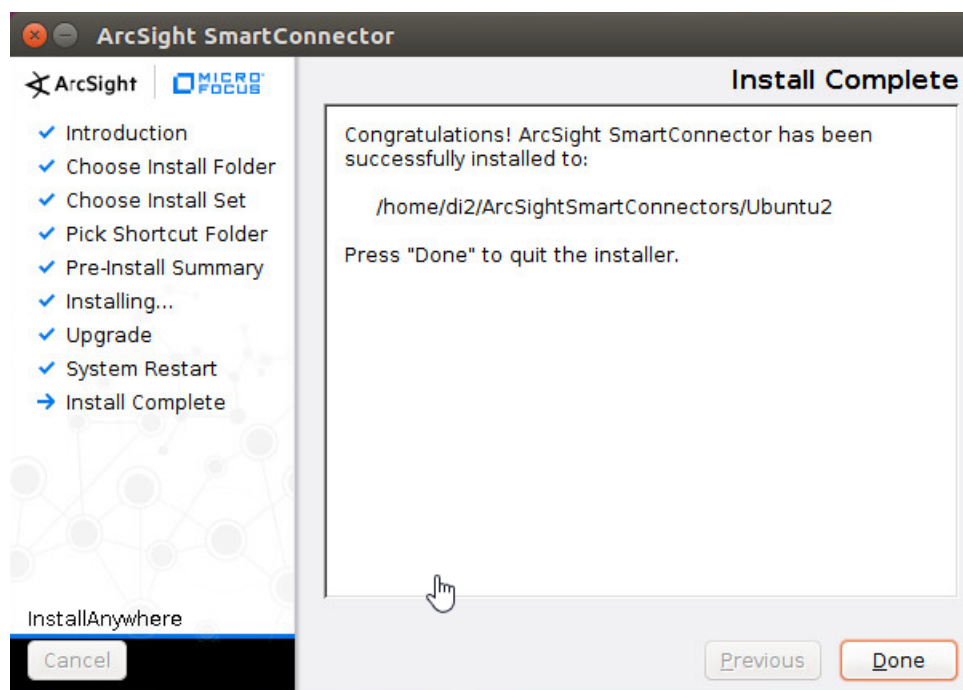
22. Click **Next**.



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



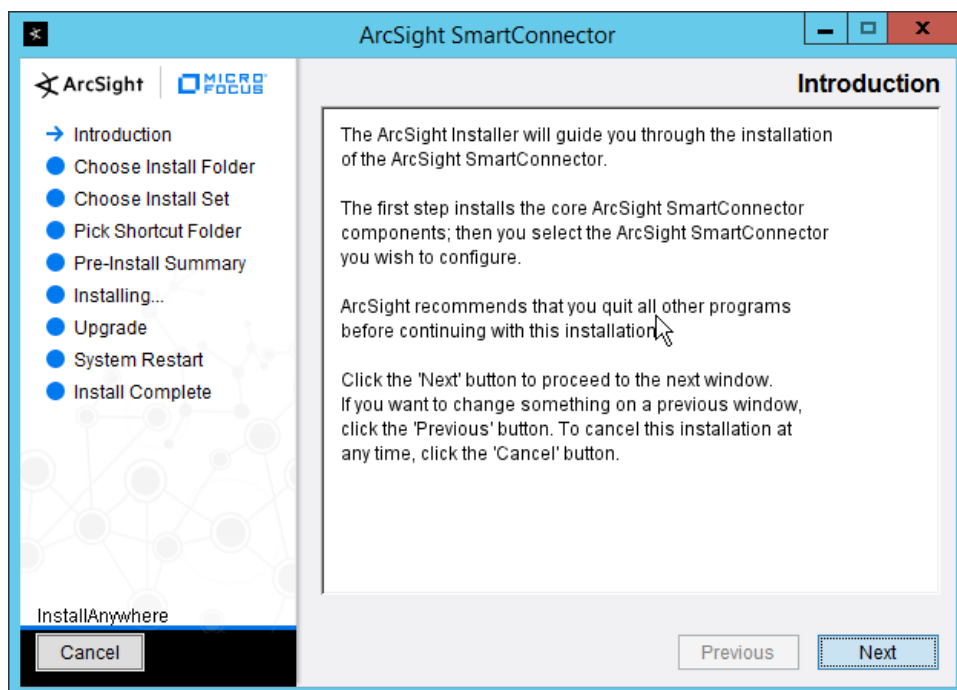
25. Click **Next**.



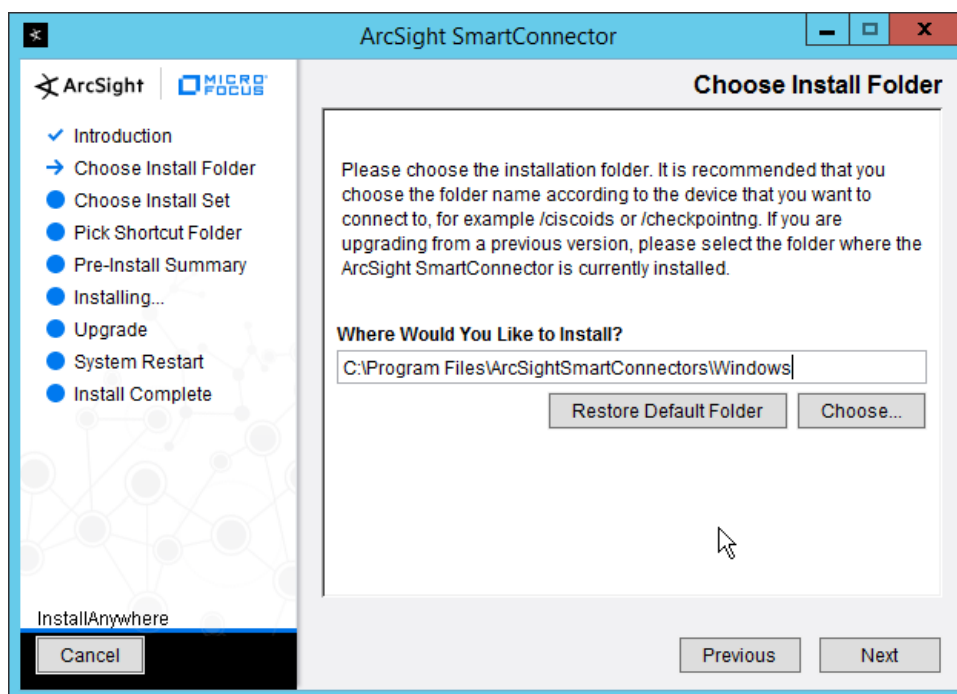
26. Click **Done**.

## 2.11.4 Install a Connector Server for ESM on Windows 2012 R2

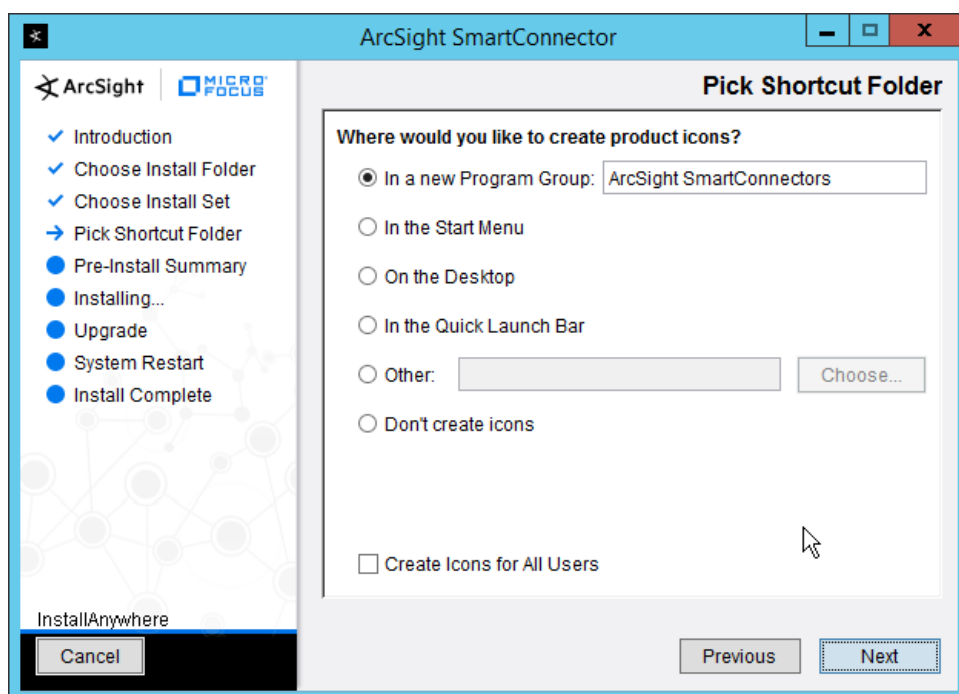
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



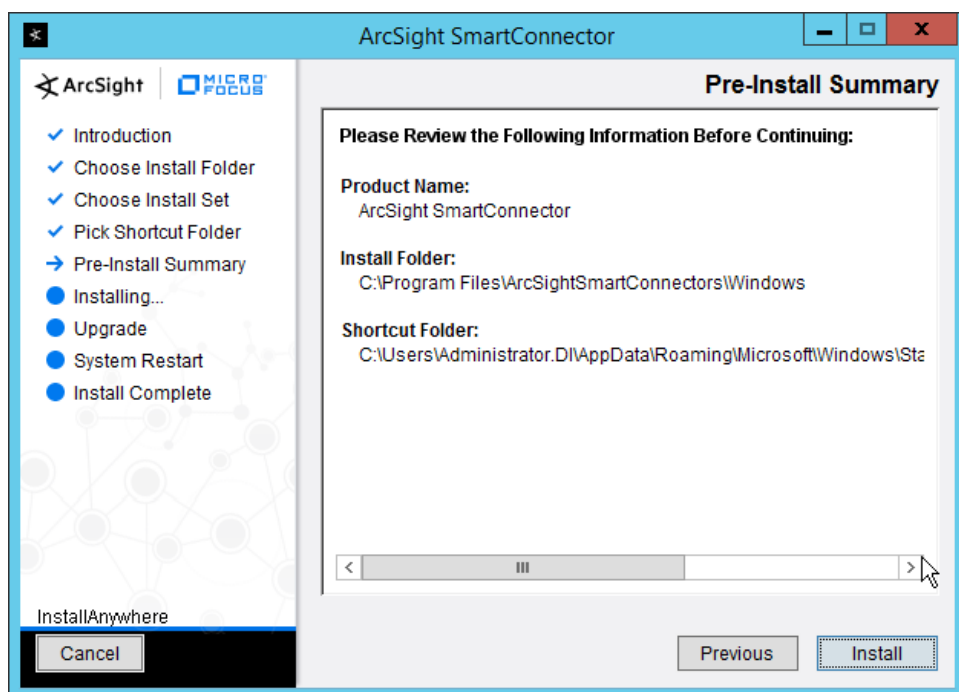
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



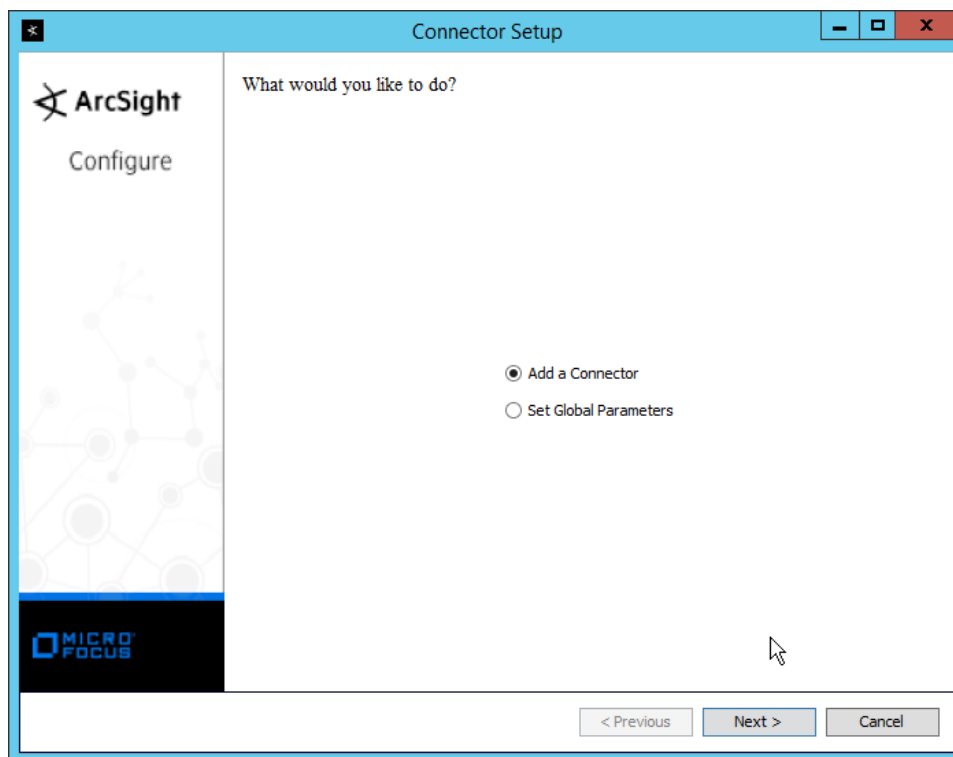
4. Click **Next**.



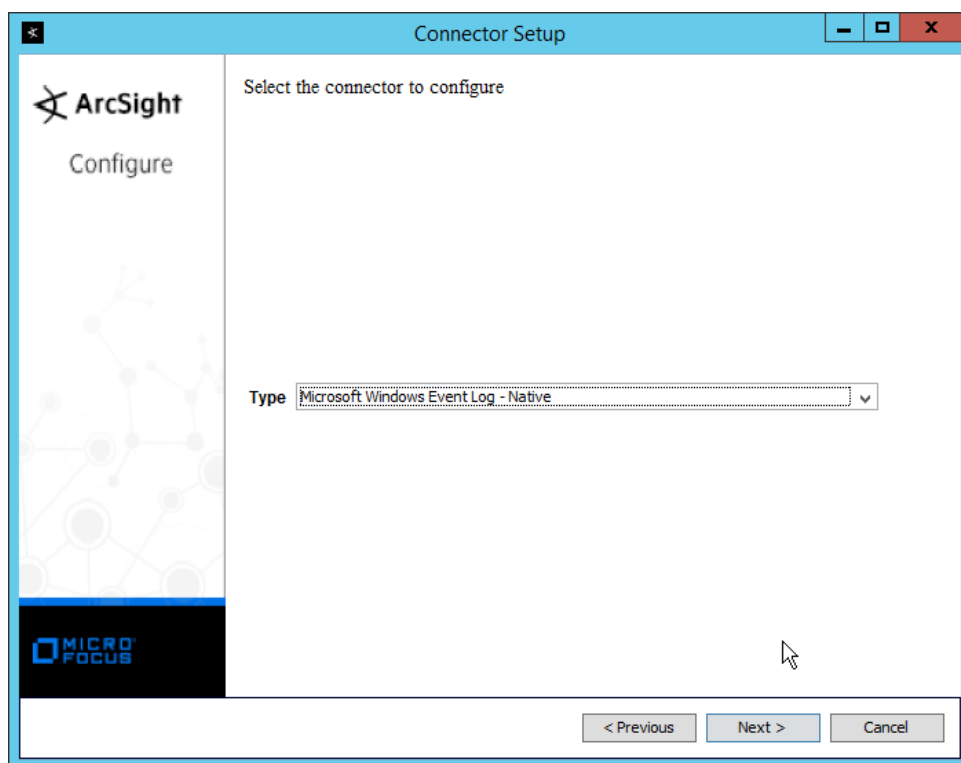
5. Click **Next**.



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

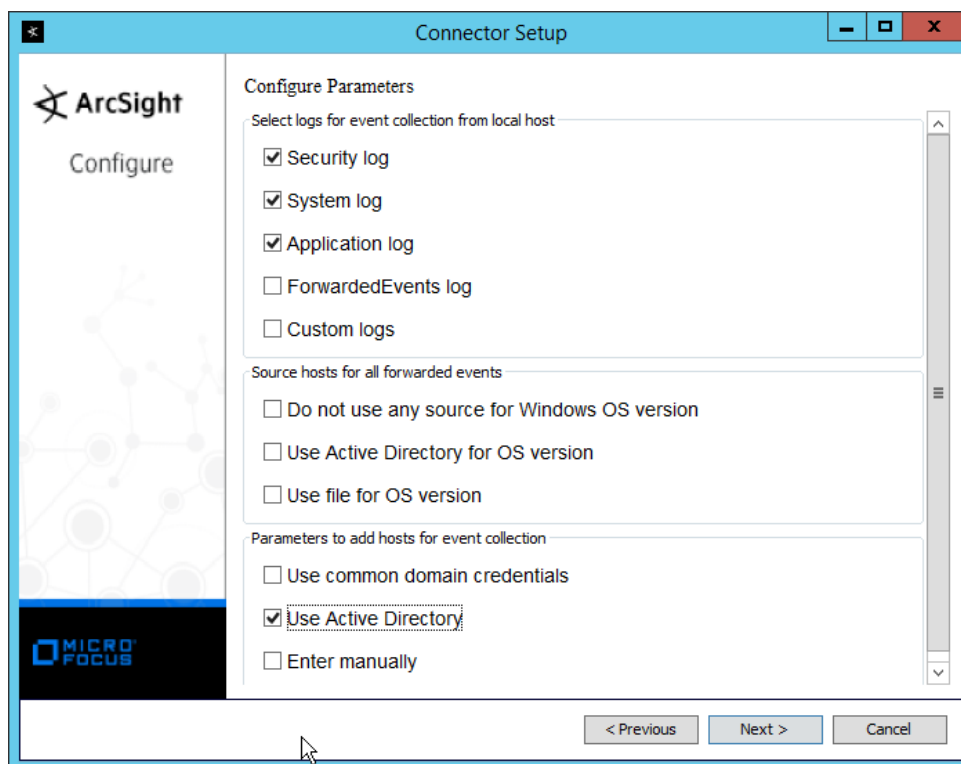


8. Click **Next**.
9. Select **Microsoft Windows Event Log–Native**.



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





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

Connector Setup

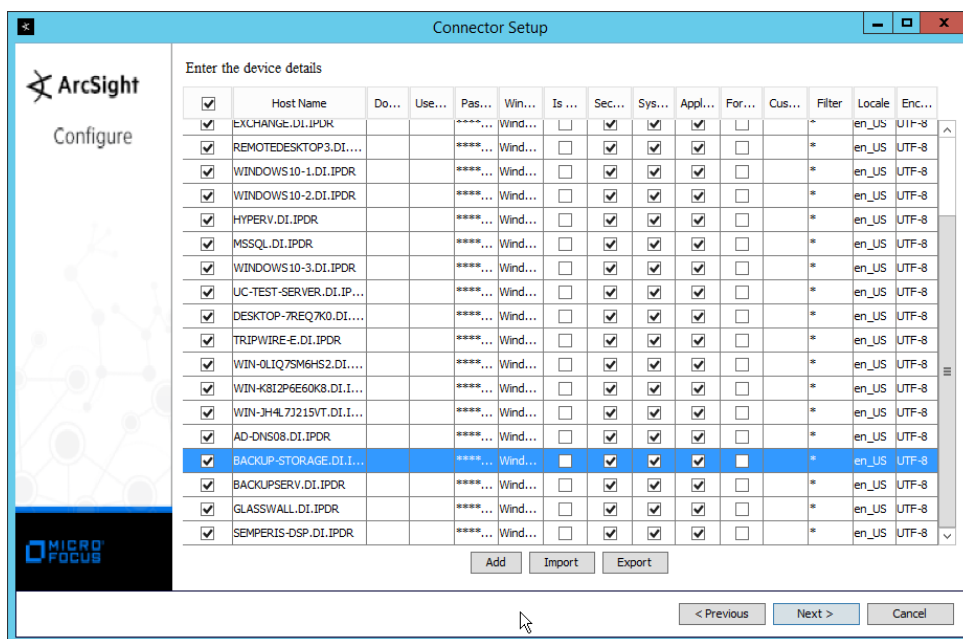
ArcSight  
Configure

Enter the parameter details

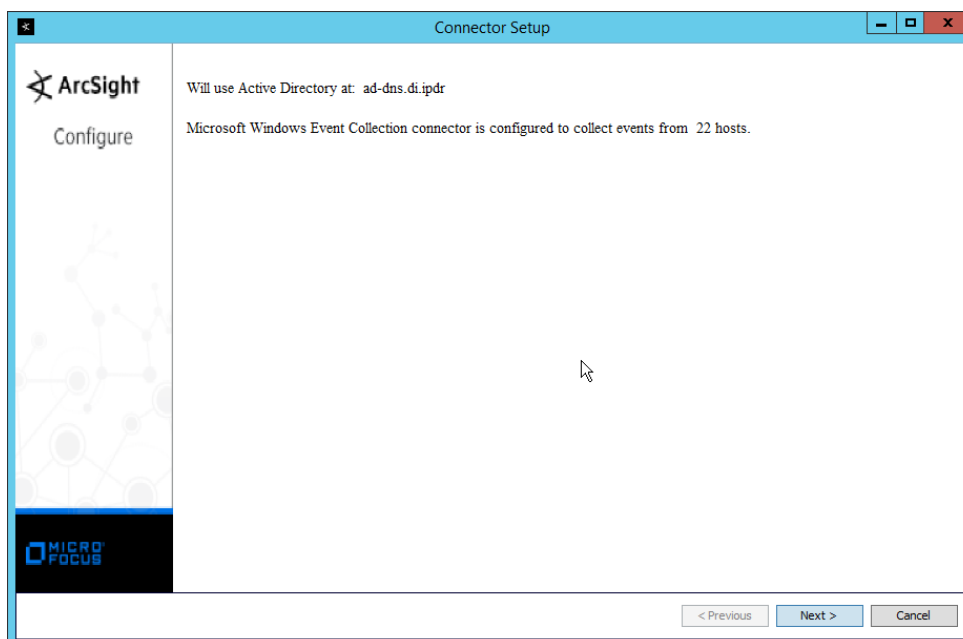
Domain Name	DI
Domain User Name	arcsight_admin
Domain User Password	.....
Active Directory Domain	DI.IPDR
Active Directory User Name	arcsight_admin
Active Directory User Password	.....
Active Directory Server	ad-dns.di.ipdr
Active Directory Filter	(&(cn=*)(operatingsystem=*)(whenevercreated=*))
Active 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, e.g., **Security, System, Application**.

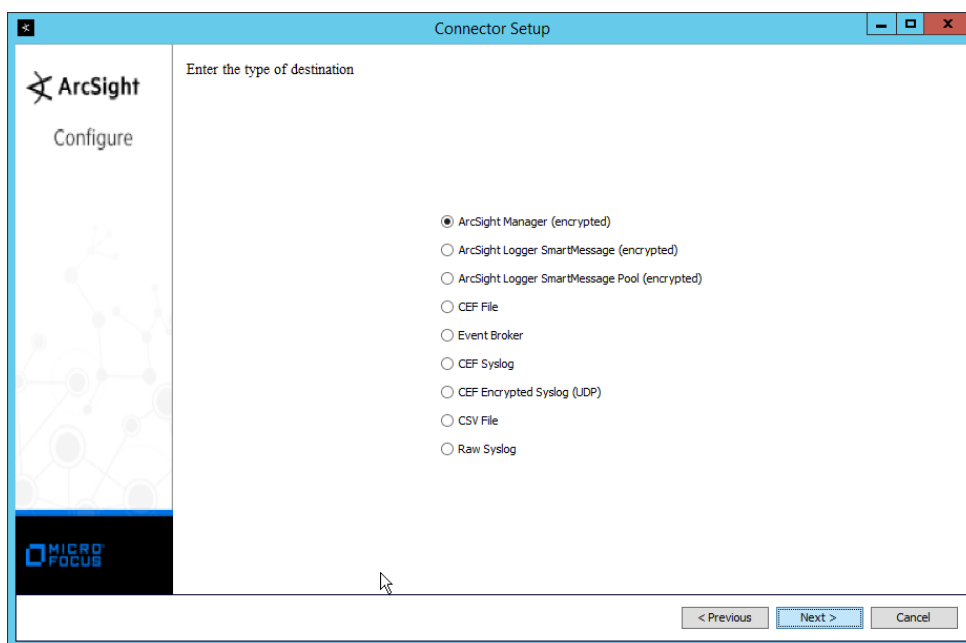


17. Click **Next**.



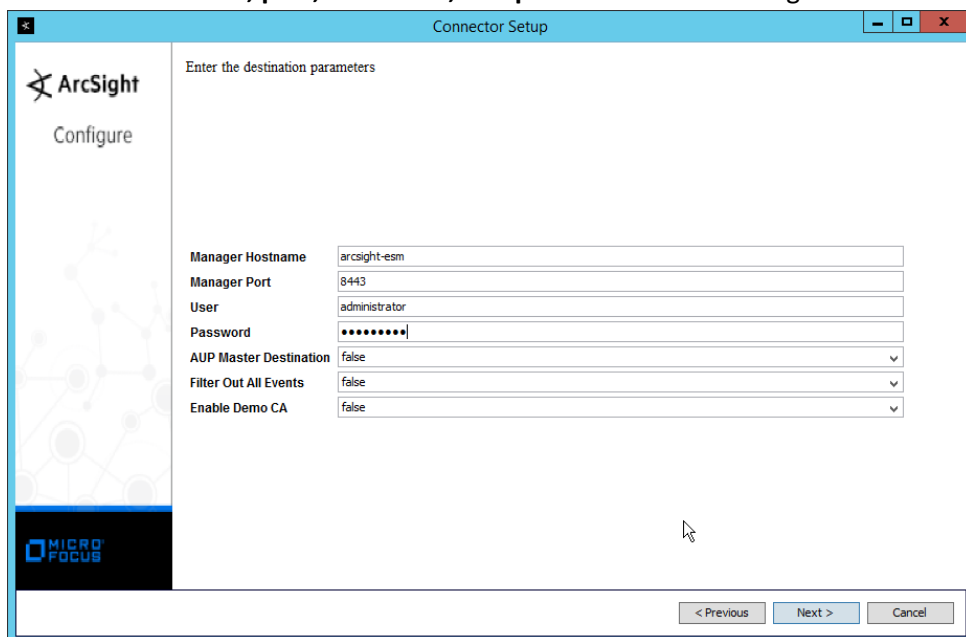
18. Click **Next**.

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



20. Click **Next**.

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



22. Click **Next**.

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

Connector Setup

ArcSight  
Configure

Enter the connector details

Name: Windows Connector Server

Location:

DeviceLocation:

Comment:

< Previous   Next >   Cancel

24. Click **Next**.

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

Connector Setup

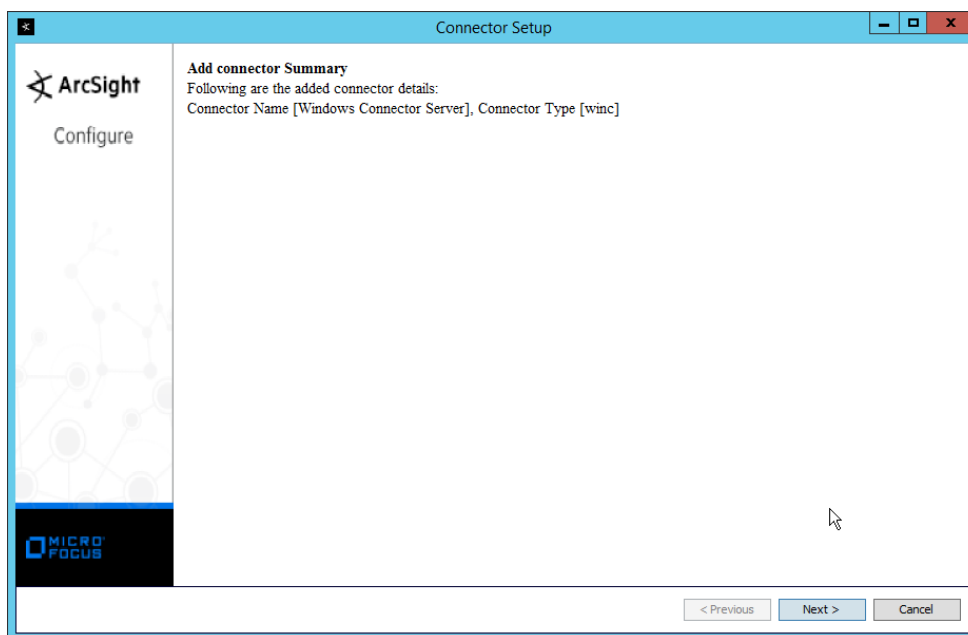
ArcSight  
Configure

Following certificate will be imported into connector trust store:  
Host/port: arcsight-esm\_8443  
Details: CN=arcsight-esm, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

☒ Import the certificate to connector from destination  
☐ Do not import the certificate to connector from destination

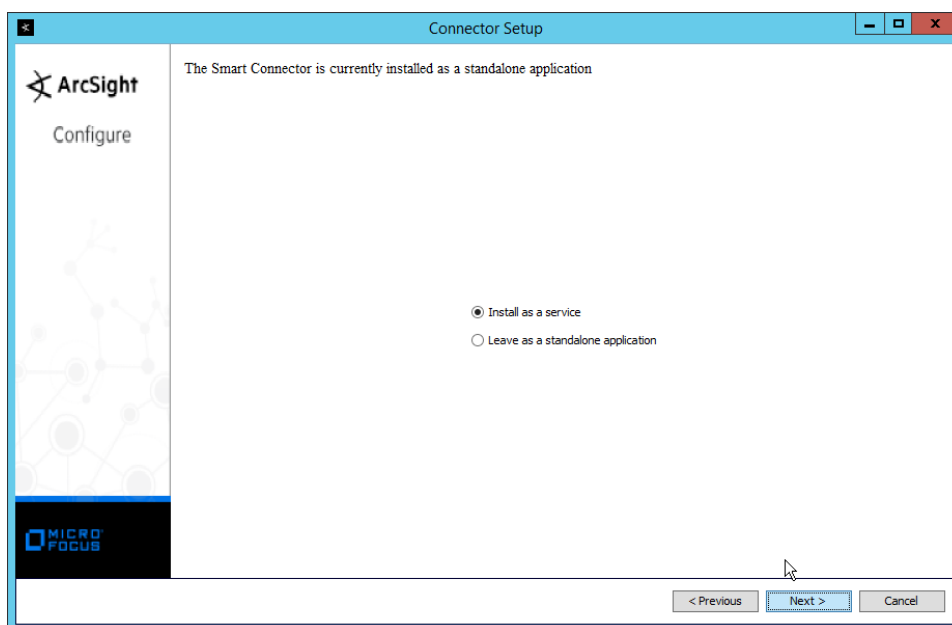
< Previous   Next >   Cancel

26. Click **Next**.

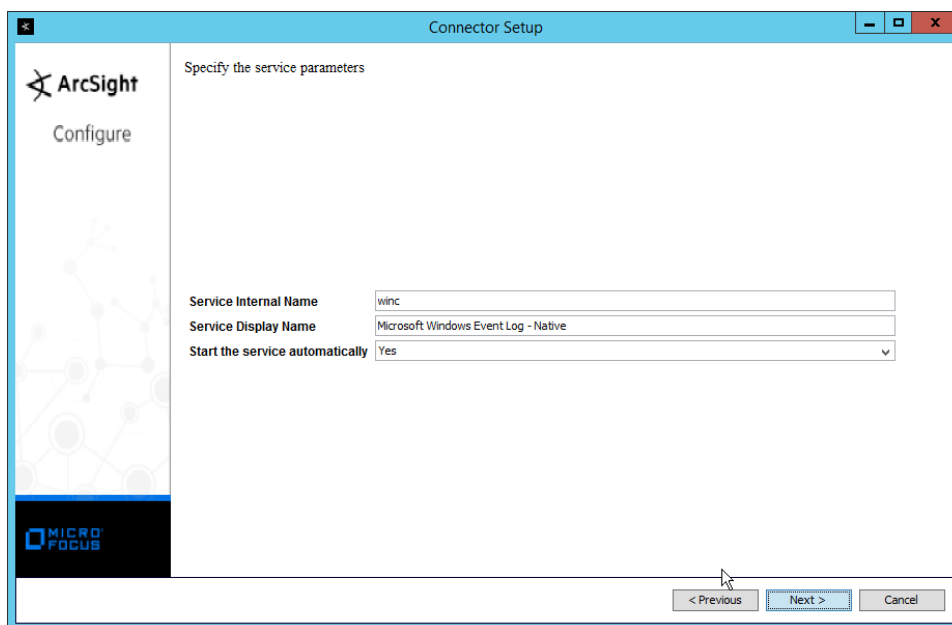


27. Click **Next**.

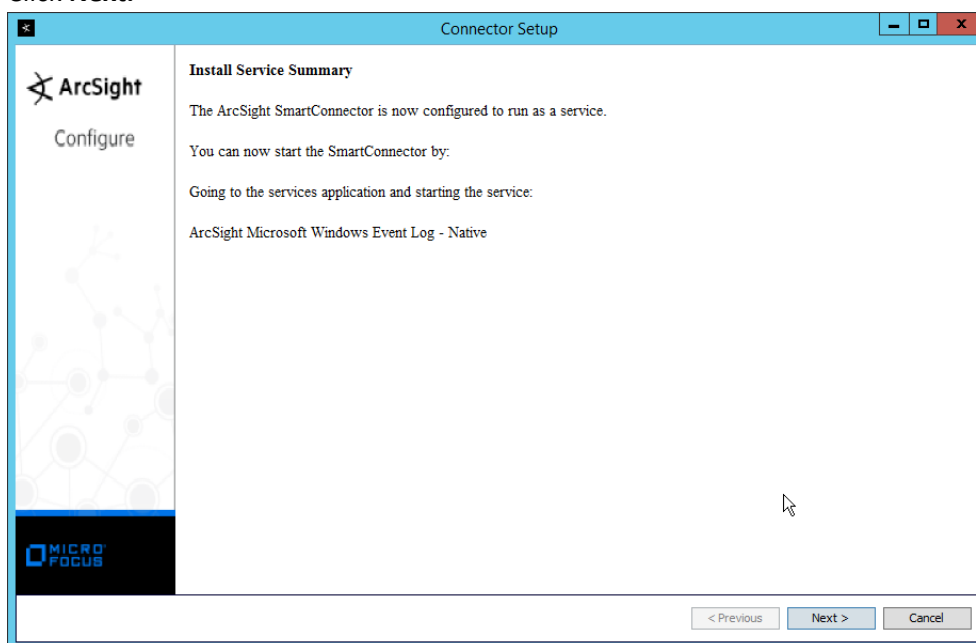
28. Select **Install as a service**.



29. Click **Next**.

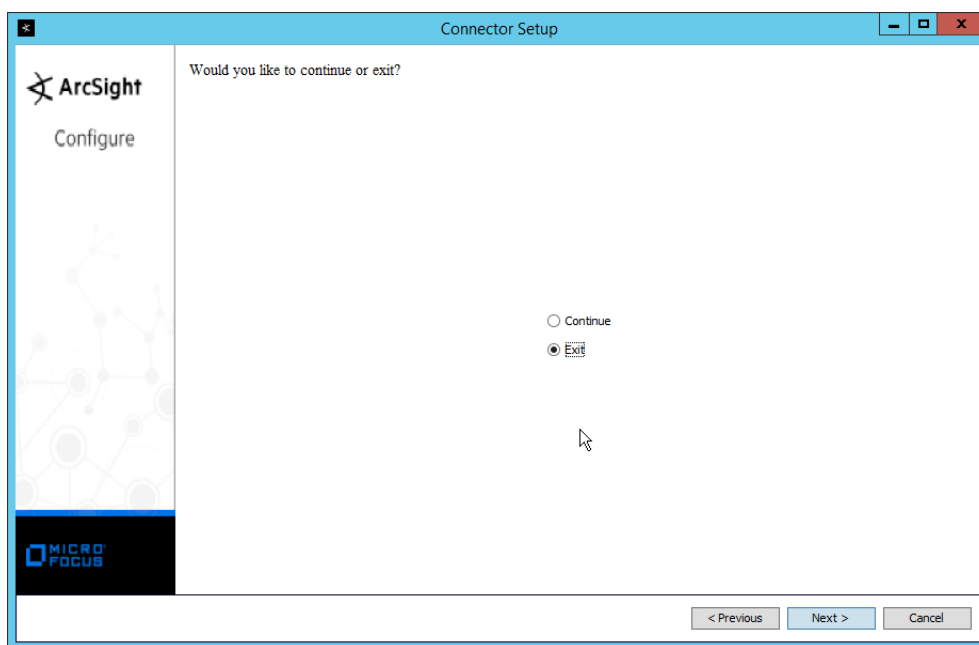


30. Click **Next**.

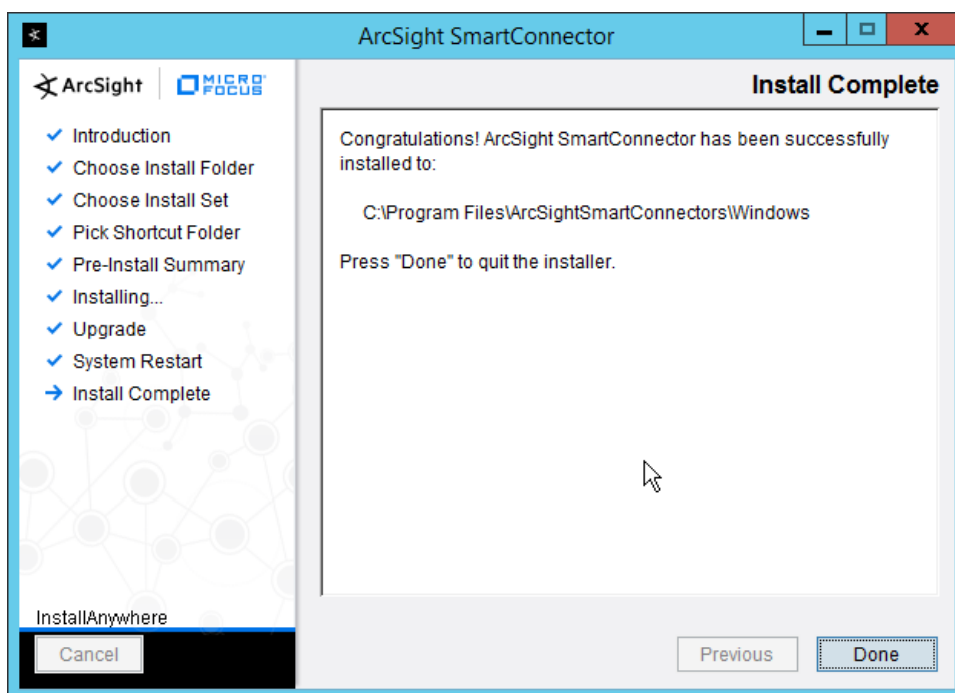


31. Click **Next**.

32. Select **Exit**.



33. Click **Next**.



34. Click **Done**.

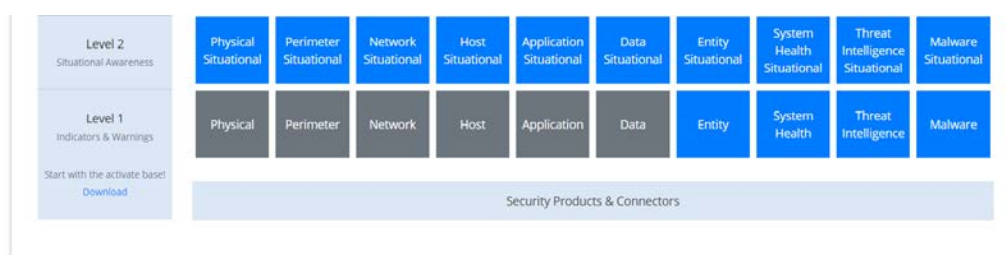
35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.



## 2.11.5 Install Preconfigured Filters for ArcSight

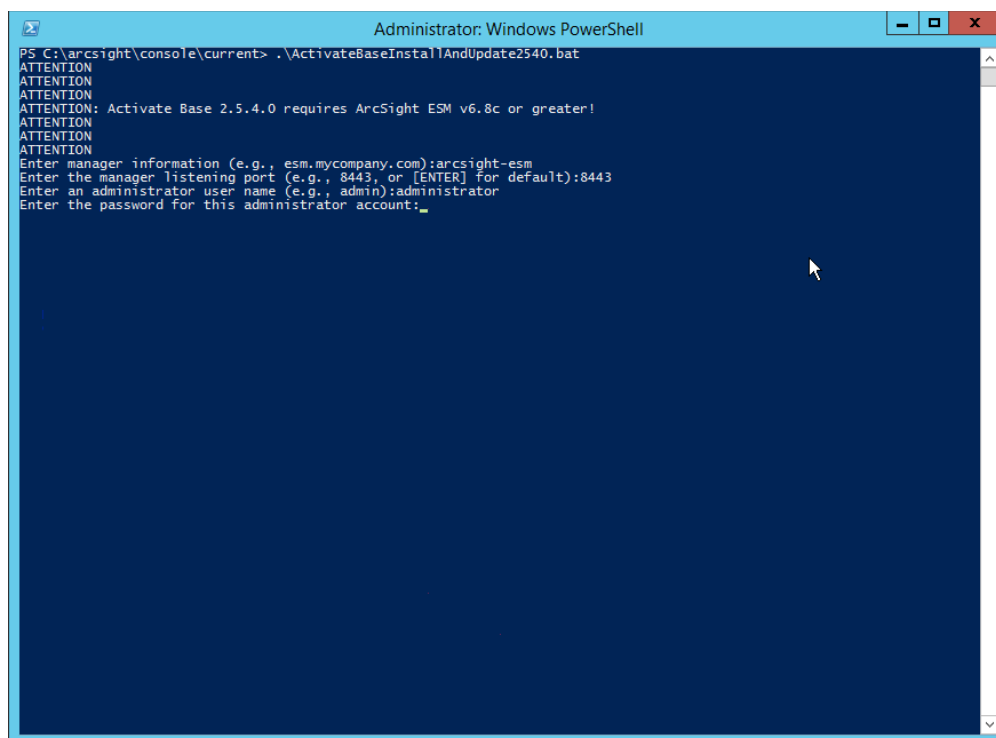
### 2.11.5.1 Install/Activate Base

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



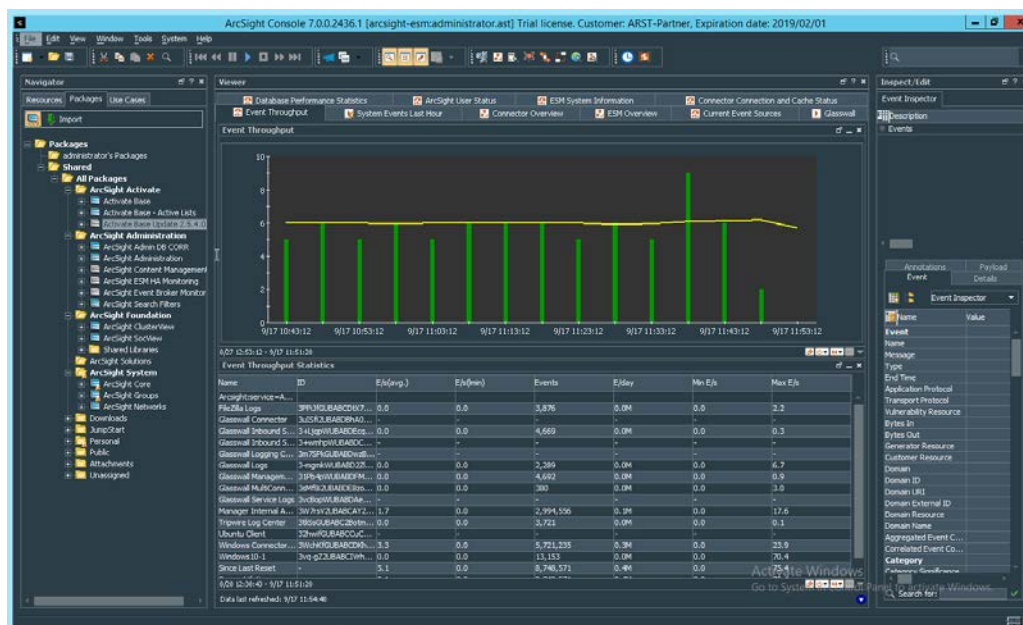
2. Click the **Download** link for the Activate Base. (Note: This package should be installed on the ArcSight Console, not on the ESM.)
3. Copy the contents of the zip file to ARCSIGHT\_HOME. The default for this is C:\arcsight\Console\current, assuming a Windows Server.
4. In PowerShell, navigate to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

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



```
Administrator: Windows PowerShell
PS C:\arcsight\console\current> .\ActivateBaseInstallAndUpdate2540.bat
ATTENTION
ATTENTION
ATTENTION: 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**.

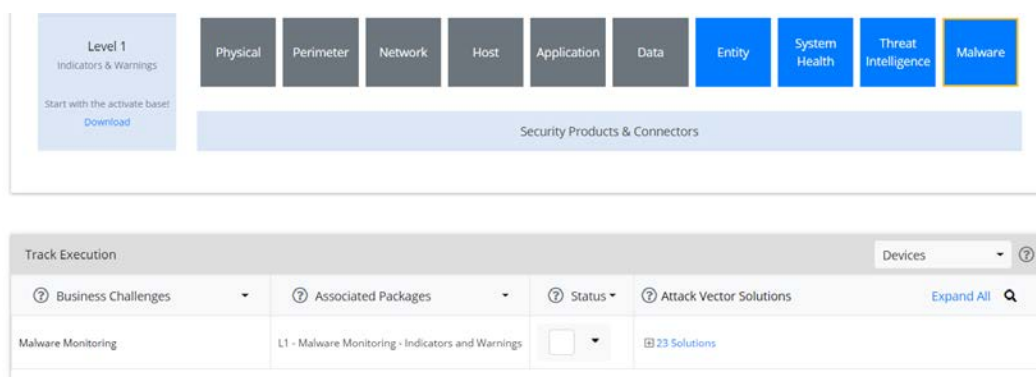


- Under **Packages > Shared > All Packages > ArcSight Activate**, right-click **Activate Base Update 2.5.4.0**, and select **Delete Package**.

### 2.11.5.2 Install Packages

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

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



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

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

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

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

```
Administrator: Windows PowerShell

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

ArcSight Package Utility starting...

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

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

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

Will now install:

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

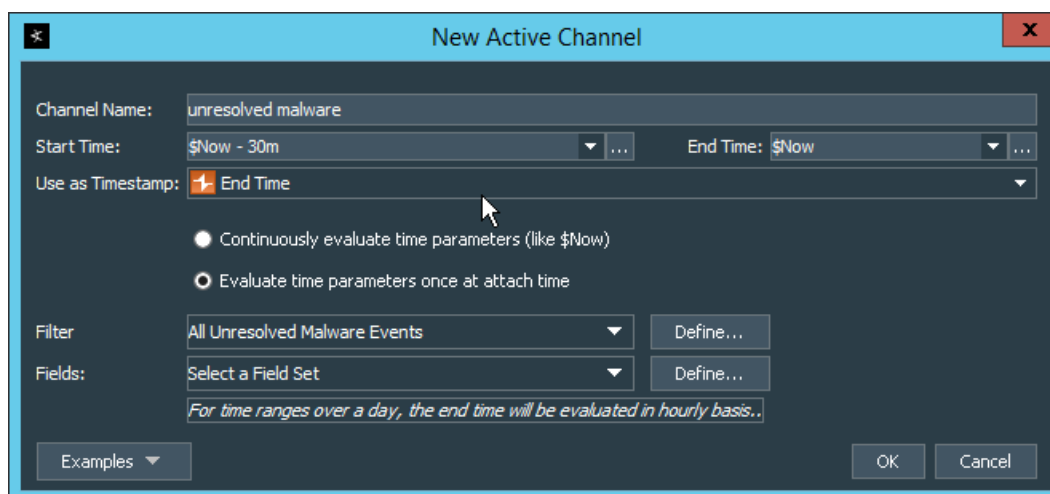
ATTENTION
ATTENTION
ATTENTION: From your ESM console UI:
ATTENTION: Please delete /All Packages/ArcSight Activate/Activate Base Update 2.5.4.0.
ATTENTION:
ATTENTION: From your ESM console's file system:
ATTENTION: Please delete Activate_Base_Updated_2.5.4.0.arb
ATTENTION:
ATTENTION
ATTENTION
ATTENTION

PS C:\arcsight\console\current> .\L1-Malware_Monitoring_1.1.0.1.bat
Enter manager information (e.g., esm.mycompany.com):arcsight-esm
Enter the manager listening port (e.g., 8443, or [ENTER] for default):8443
Enter an administrator user name (e.g., admin):administrator
Enter the password for this administrator account:
```

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

## 2.11.6 Apply Filters to a Channel

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



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

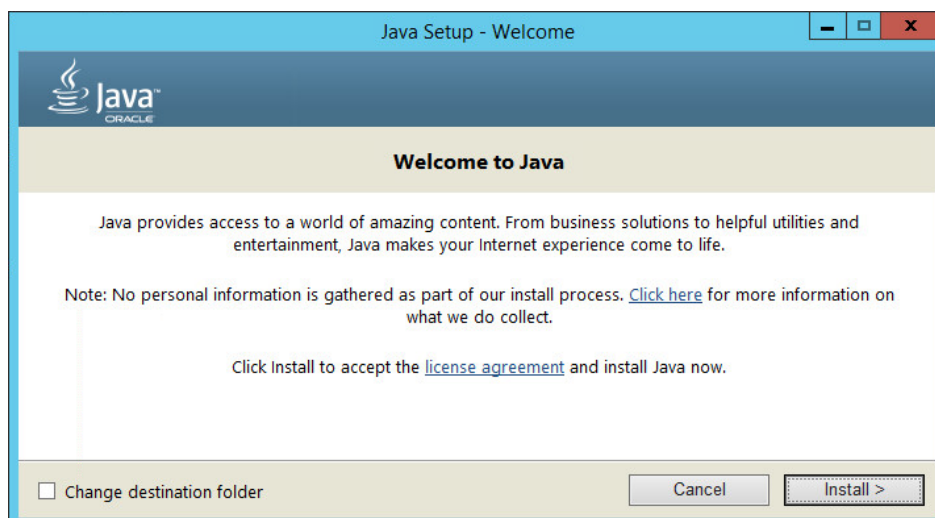
## 2.12 Tripwire Enterprise

### Notes:

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

### 2.12.1 Install Tripwire Enterprise

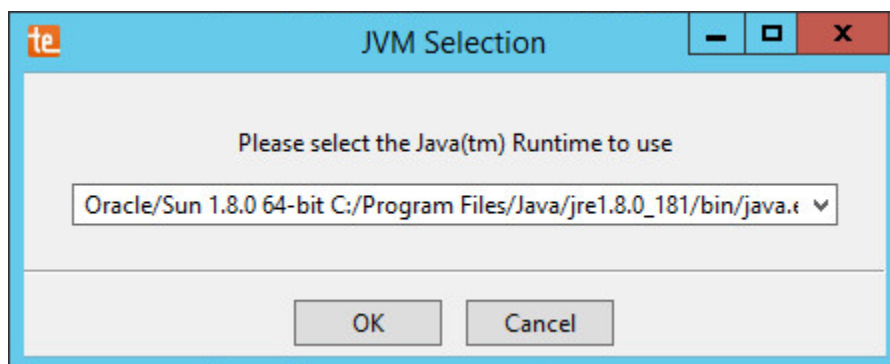
1. Ensure that you have an up-to-date version of Oracle Java. You must install both the Java Runtime Environment (JRE) and the Java Cryptography Extension (JCE).
2. Download and run the **JRE installer**.



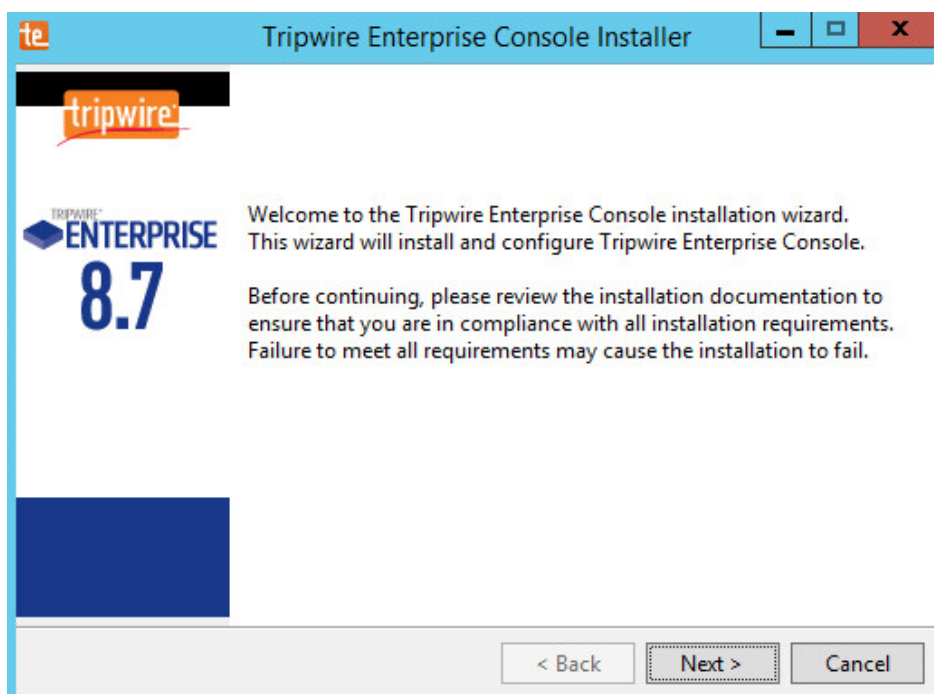
3. Click **Install**.
4. Download the JCE and extract the files.

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

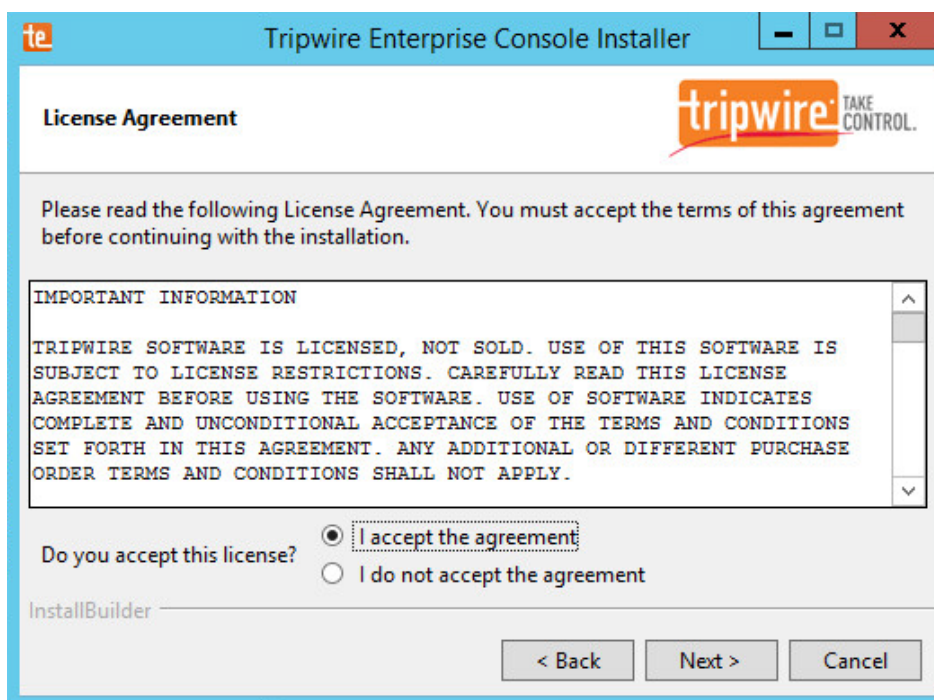
5. Copy the **local\_policy.jar** and **US\_export\_policy.jar** files to **/lib/security/Unlimited/** and **/lib/security/Limited** in the Java installation directory.
6. Run **install-server-windows-amd64**.
7. Select the Java runtime that was just installed.



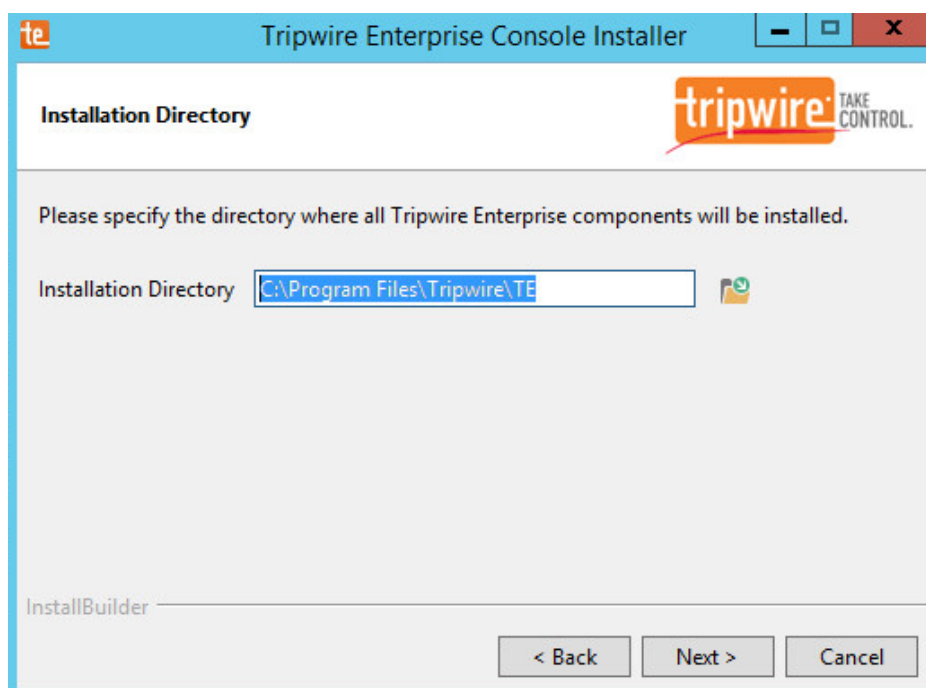
8. Click **OK**.



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



11. Click **Next**.



12. Click **Next**.

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



te Tripwire Enterprise Console Installer

Tripwire Enterprise Console Configuration Part 1 of 4

tripwire TAKE CONTROL.

Please provide the hostname of the system where Tripwire Enterprise Console will be installed.

TE Server Hostname TRIPWIRE-E

InstallBuilder

< Back Next > Cancel

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

**Tripwire Enterprise Console Configuration Part 2 of 4**

Specify the ports that Tripwire Enterprise Console uses to communicate.

This port is used for user-initiated Web console sessions.

HTTPS Web Services port

This port is used for external integrations (such as plugins).

HTTP EMS Integration Port

This port is used for Console/Agent Java communications.

Tripwire Enterprise RMI Port

InstallBuilder

< Back Next > 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.

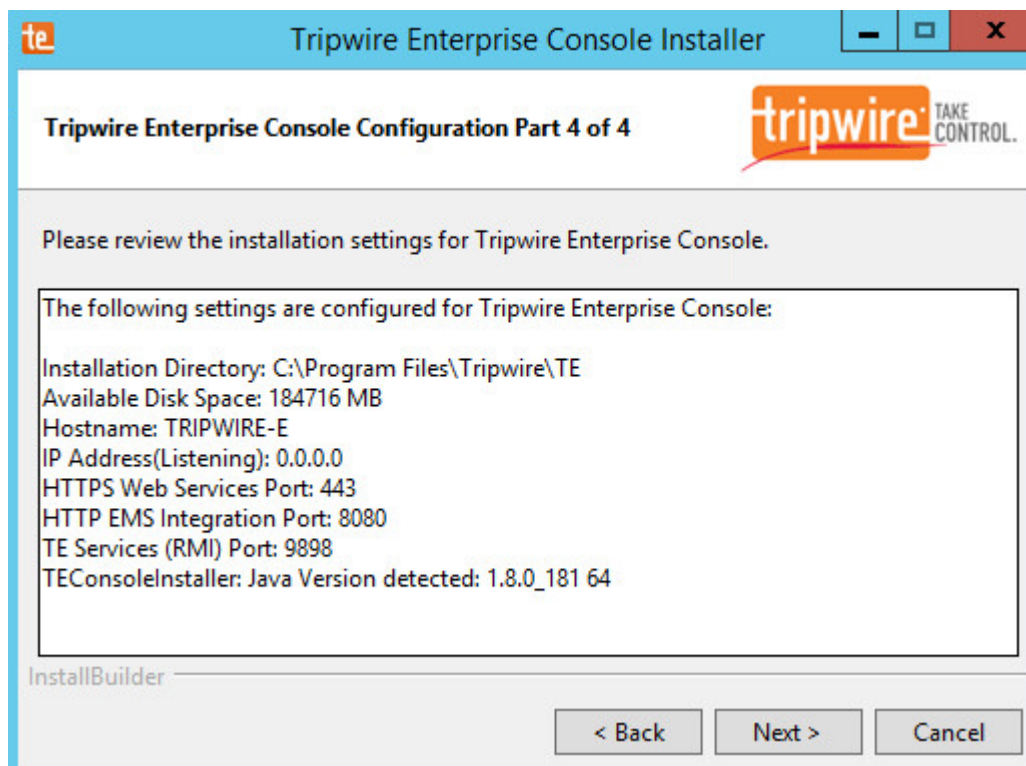
Services Passphrase

Confirm Passphrase

InstallBuilder

< Back Next > Cancel

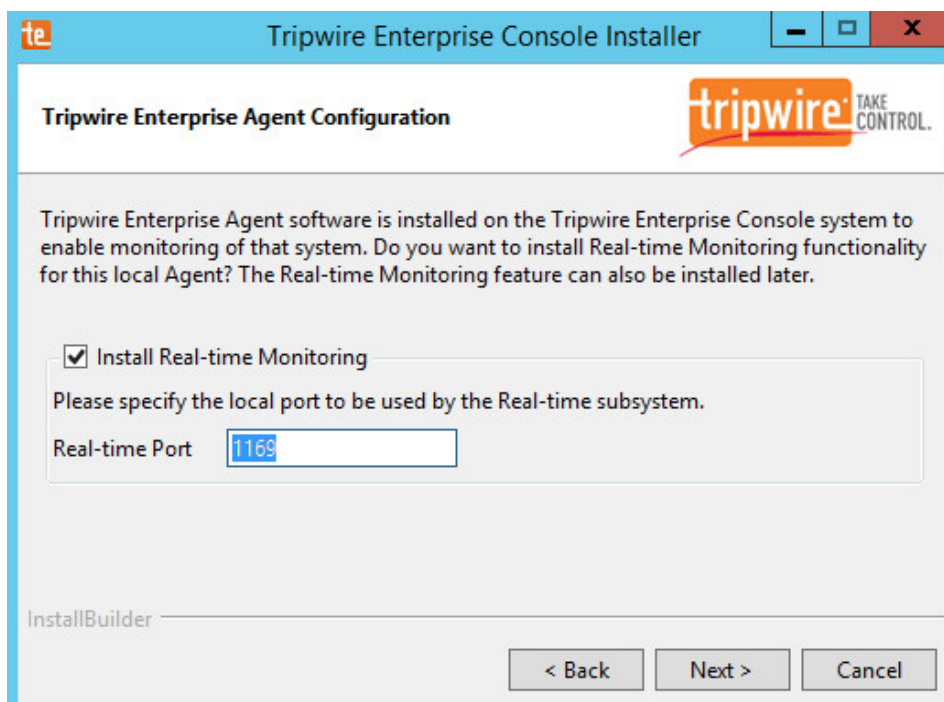
18. Click **Next**.



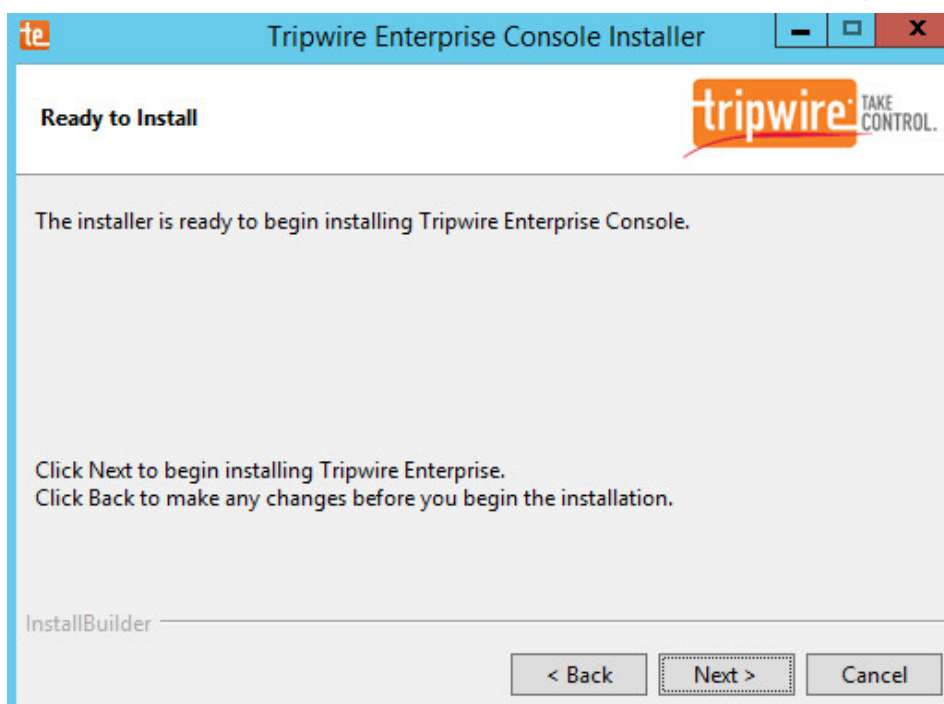
19. Click **Next**.

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

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

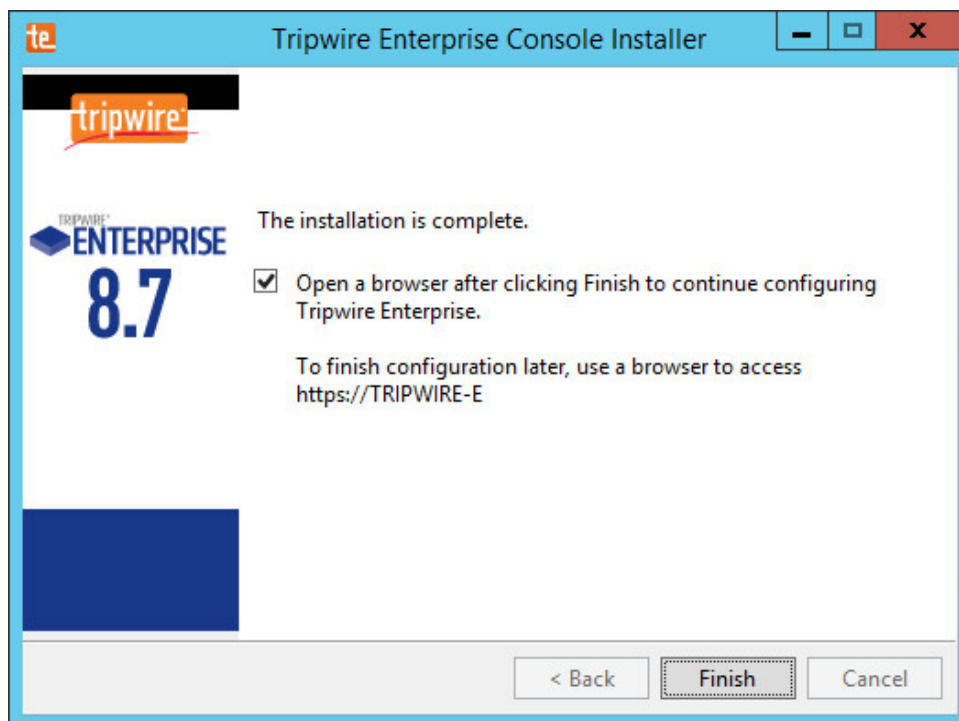


22. Click **Next**.



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.

**Tripwire Enterprise Post-Install Configuration**

Tripwire Enterprise needs additional configuration.  
To finish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created when you installed Tripwire Enterprise.

Services Passphrase:

Login

27. Click **Login**.

**Tripwire Enterprise Post-Install Configuration**

**Database Configuration Settings**

These settings control how the TE Console connects to a remote database that stores data for all TE operations. You can check the current configuration here, and make any necessary changes in the fields below.

Remote Database Type:

Microsoft SQL Server  
Microsoft SQL Server  
Oracle  
Oracle RAC  
MySQL

Remote Database Type: The type of remote database used by TE.

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

The screenshot shows the 'Authentication Type' configuration window. It contains several input fields and descriptive text:

- Authentication Type:** A dropdown menu set to 'SQL Server'. To the right, a description states: '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:** A text box containing 'twadmin'. To the right, it says: 'Login Name: The login name that TE will use to authenticate with the database.'
- Password:** A text box with masked characters. To the right, it says: 'Password: The password that TE will use to authenticate with the database.'
- Database Host:** A text box containing '192.168.78.125'. To the right, it says: 'Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.'
- Port (default 1433):** A text box containing '1433'. To the right, it says: '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:** A text box containing 'TE\_DB'. To the right, it says: '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):** An empty text box. To the right, it says: '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:** A dropdown menu set to 'Off'. To the right, it says: 'SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.' Below this, a bulleted list provides details:
  - Request - SSL will be used if available.
  - Require - SSL will always be used, and an error will occur if SSL is not available for the database.
  - Authenticate - SSL will always be used, and an error will occur if SSL is not available for the database. In addition, the certificate chain of the database server's public key will be authenticated using TE's trust store. If the certificate chain does not originate from a trusted source, an error will occur.
  - Off - SSL will never be used. This setting is not recommended.

At the bottom left is a 'Test Database Login' button with a green checkmark icon. At the bottom right, there is a watermark for 'Activate Windows' and a link to 'Go to System in Control Panel'.

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

The screenshot shows the same configuration window as before, but now the 'Test Results' section is visible. It contains a text box with the message 'Connection Succeeded.' Below this, there is a blue status bar with the text 'Tripwire Enterprise 8.7.0.b8.7.0.r20180606173604-e215728.b40'. To the right of the status bar are two buttons: 'Save Configuration and Restart Console' and 'Logout'.

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



**Tripwire Enterprise Post-Install Configuration**

**Configuration Steps Needed:**

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

**Create Administrator Password**

Passwords must:

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

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

Password:

.....

Confirm Password:

.....

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**.

NIST SP 1800-25C: Identifying and Protecting Assets Against Ransomware and Other Destructive Events

267

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

No file chosen

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

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

#### Step 2: Configure Change Auditing and/or Policy Management

Monitoring Solutions  
☒ Change Auditing  
☒ Policy Management

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

42. Select any available policies desired.

#### Step 3: Specify the platforms to monitor

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

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

Selected Platforms:

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

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

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

Change Audit Scheduling

Checks  
 How frequently would you like to run checks on your assets?  
  
 Run the checks at:

Reports  
 How frequently would you like to run reports on your assets?  
  
 Run the reports at:

Policy Scheduling

Checks  
 How frequently would you like to run checks on your assets?  
 on   
 Run the checks at:

Reports  
 How frequently would you like to run reports on your assets?  
 on   
 Run the reports at:

☐ 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 Tripwire Enterprise Console.

Preview Configuration

47. Click **Preview Configuration**.

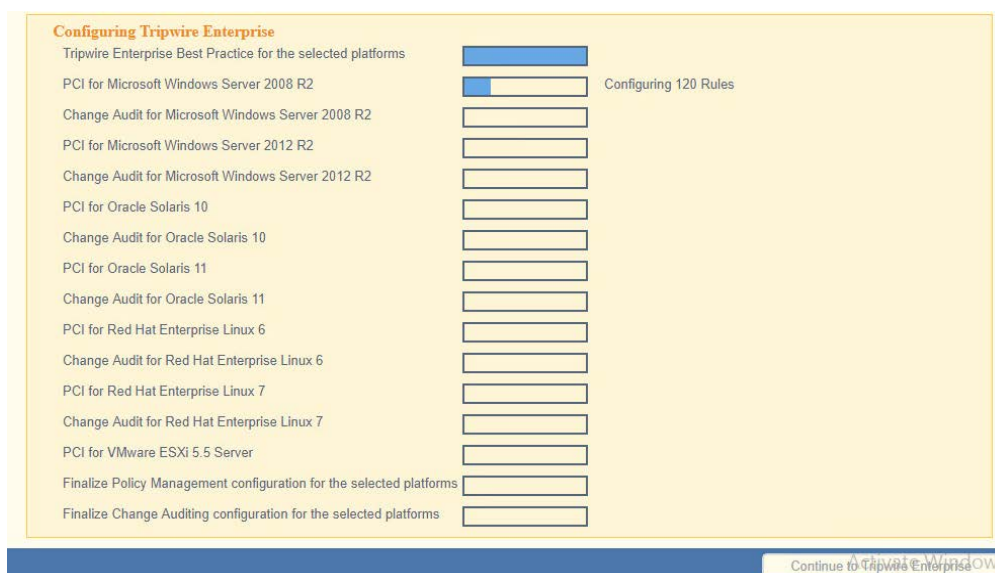
**These tasks will be applied to your configuration**

- 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.

## 2.12.2 Install the Axon Bridge

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

## 2.12.3 Install the Axon Agent (Windows)

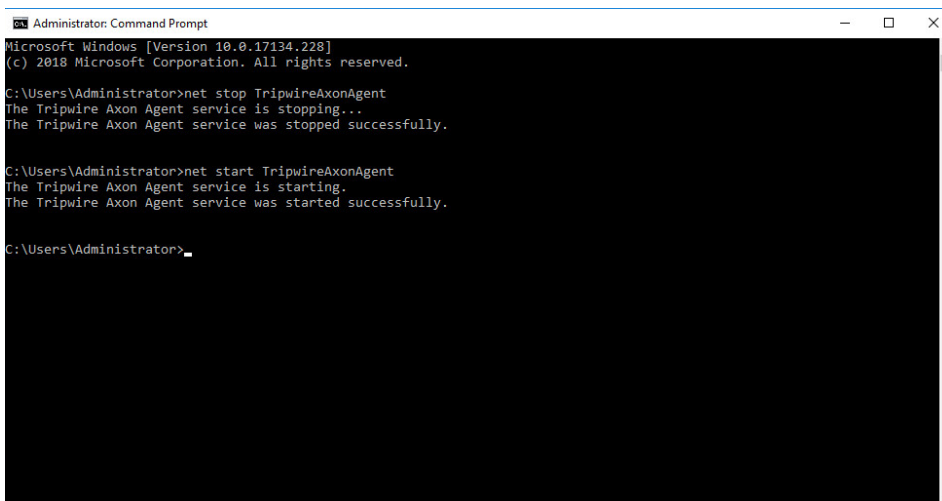
1. Download the Axon Agent zip file from the Tripwire customer website (<https://tripwireinc.force.com/customers>), under the Product Downloads tab.
2. Unzip the file.
3. To begin the installation, double-click the `.msi` file in the extracted folder. Note: No installation wizard will appear; the installation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

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

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

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

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



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

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

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

C:\Users\Administrator>
```

#### 2.12.4 Install the Axon Agent (Linux)

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

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

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

RHEL or CentOS:

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

Debian or Ubuntu:

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

## 2.12.5 Configure Tripwire Enterprise

### 2.12.5.1 Terminology

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

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

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

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

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

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

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

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

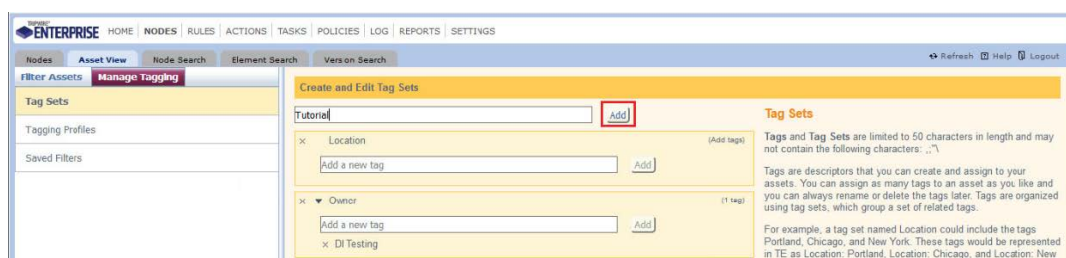
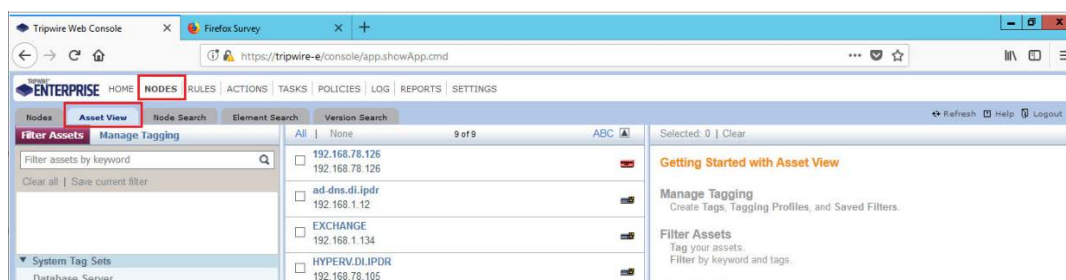
**Baseline:** the act of creating an element that reflects the current state of a monitored object (also called the **current baseline**). When a node's baseline is promoted, TE saves the former baseline as a **historic baseline**.

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

### 2.12.5.2 Tags

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

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



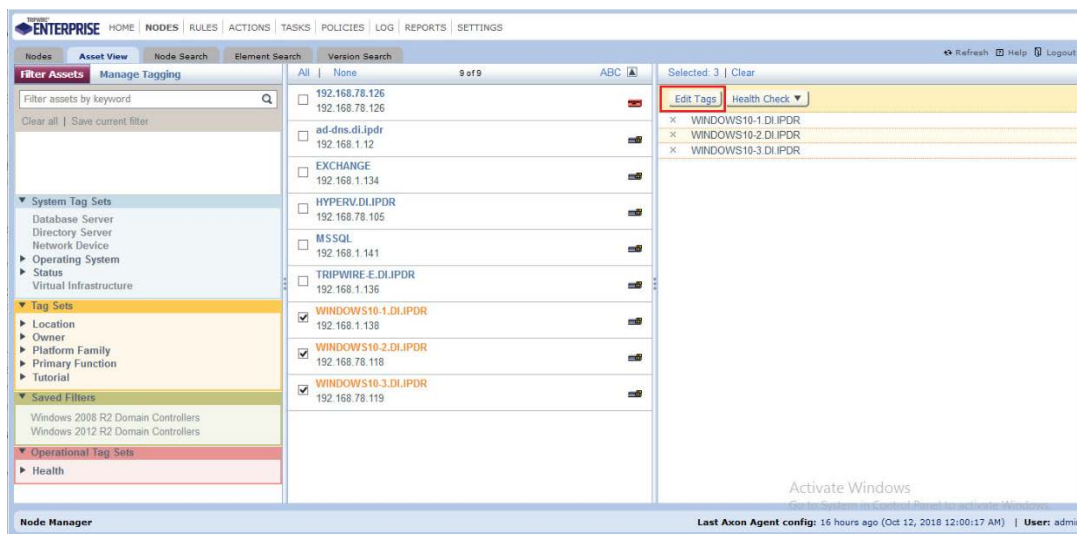
5. Under the tag set to which you wish to add a tag, enter the name of the tag.

**Create and Edit Tag Sets**

add a new tag set

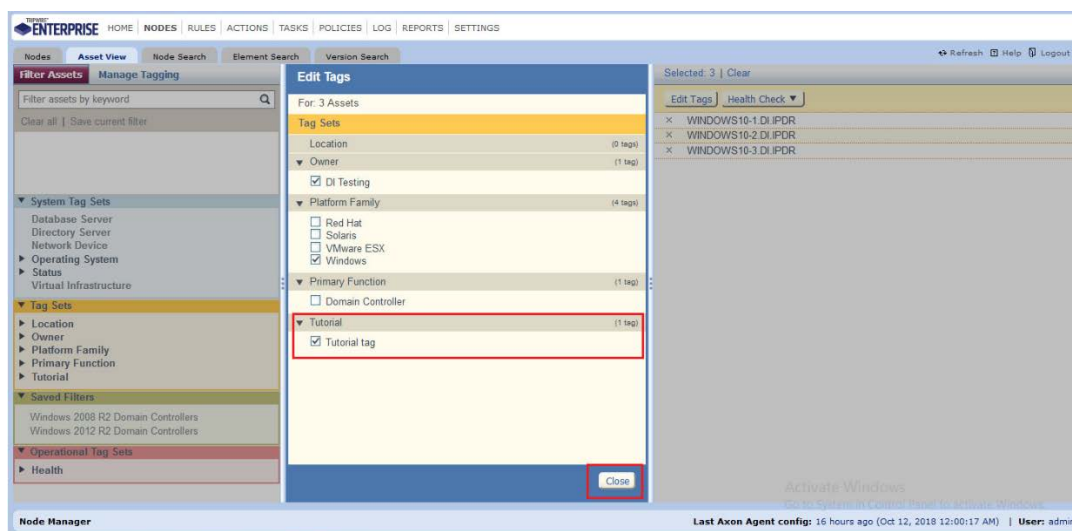
- × Location (Add tags)
- × ▼ Owner (1 tag)
  
  - × DI Testing
- × ▼ Platform Family (4 tags)
  
  - × Red Hat
  - × Solaris
  - × VMware ESX
  - × Windows
- × ▼ Primary Function (1 tag)
  
  - × Domain Controller
- × Tutorial (Add tags)

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



9. Click **Edit Tags**.

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



11. Click **Close**.

### 2.12.5.3 Rules

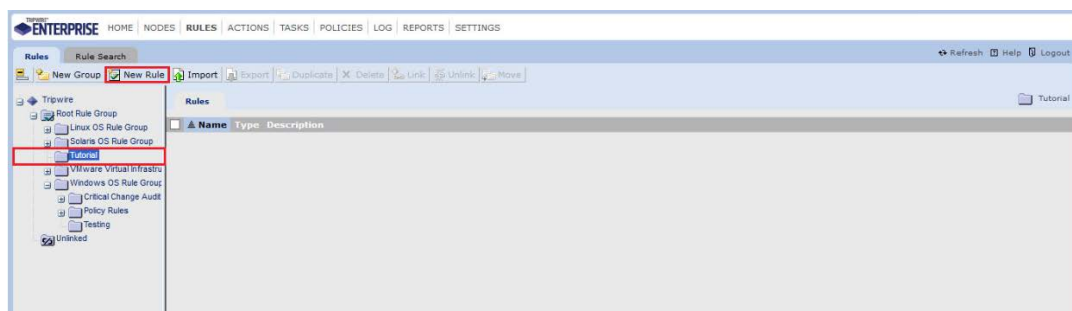
This section describes how to create a rule.

1. Click **Rules**.

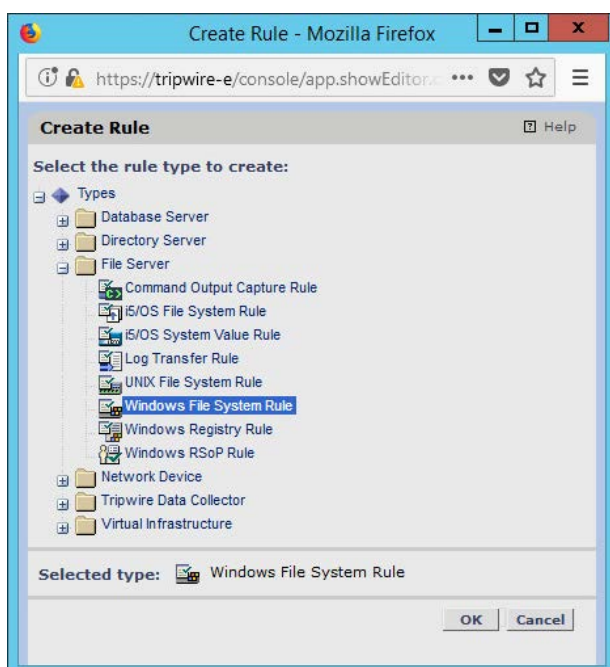




2. Select or create a rule group into which the new rule should be put.



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



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



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

<input type="checkbox"/> 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.

**New Start Point Wizard**

Specify the monitored object for the start point, and enter associated settings.

Path:

Default Severity:  (0-10,000, 0 = no severity assigned)

☐ Archive element content

☒ Recurse directory

Limit depth to  (0-100, 0 = no limit)

< Back Next > Finish Cancel

11. Click **Next**.

12. Select **Windows Content and Permissions**.

**New Start Point Wizard**

New Criteria Set New From Selected

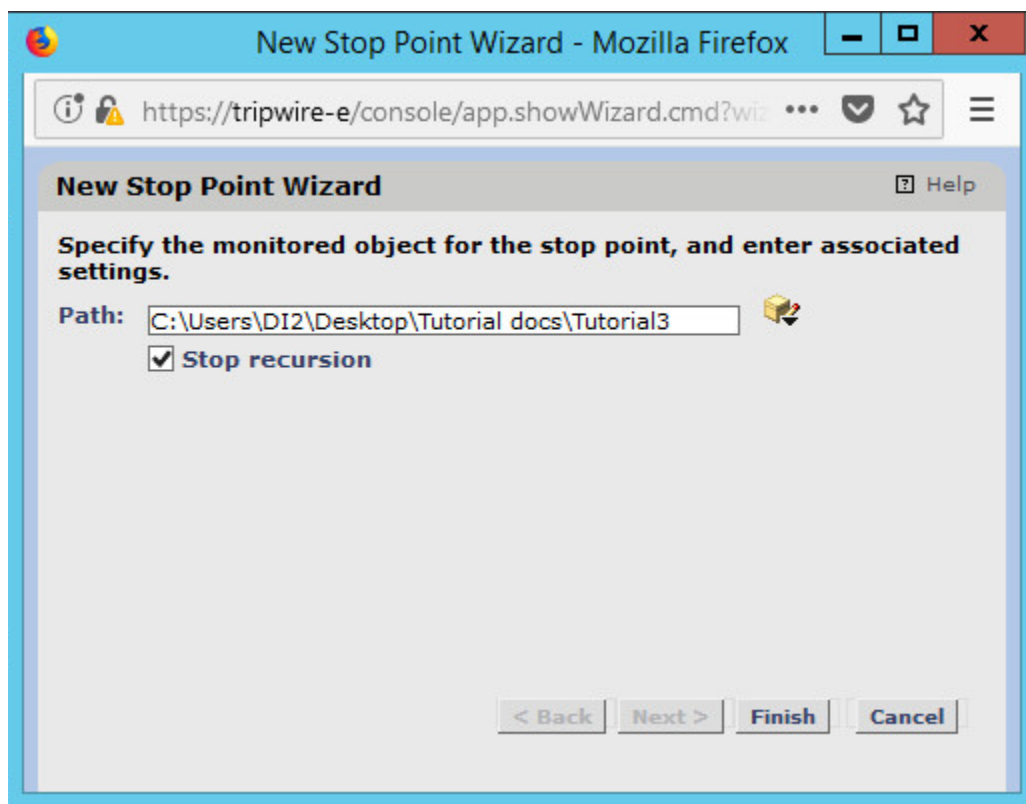
Name	Description
<input checked="" type="radio"/> Windows - Content and Permissions	
<input type="radio"/> Windows - Content Only	
<input type="radio"/> Windows - Permissions Only	

< Back Next > Finish Cancel

13. Click **Finish**.

14. Click **New Stop Point**.

15. Enter the path of any folders or files that should not be included in the scan, and indicate whether they should end the recursion.



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

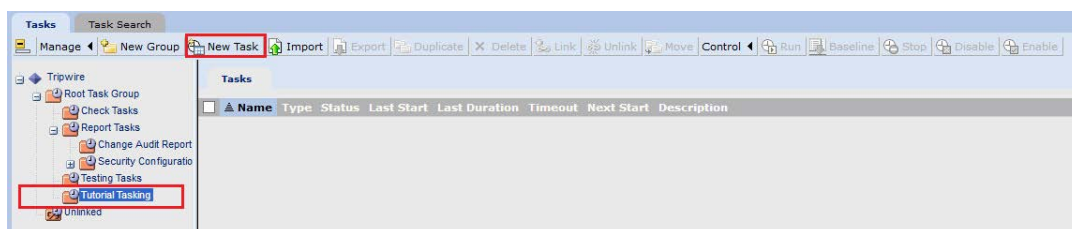
#### 2.12.5.4 Tasks

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

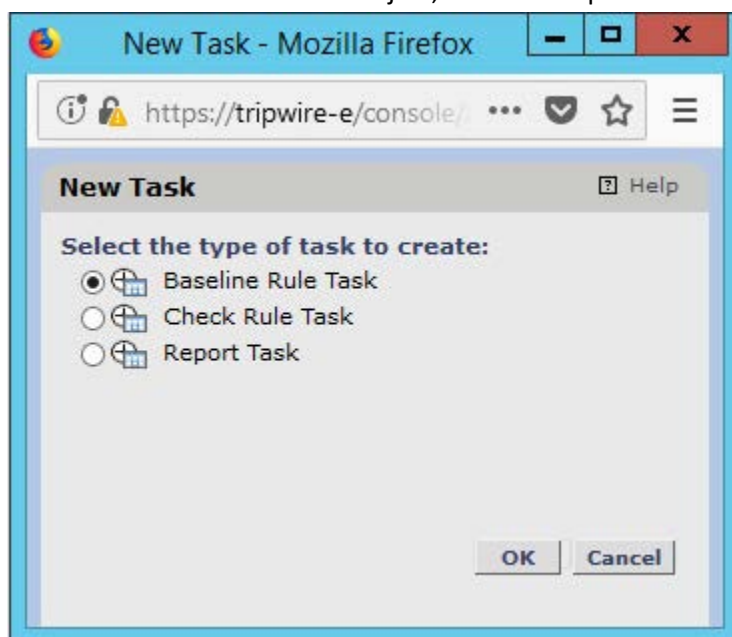
1. Click **Tasks**.



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



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



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

**New Baseline Rule Task Wizard** Help

**Enter the task name and description.**

Name:

Description:

Run as user:

☒ Use timeout:

hour(s)  minute(s)

< Back Next > Finish Cancel

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

**New Baseline Rule Task Wizard** Help

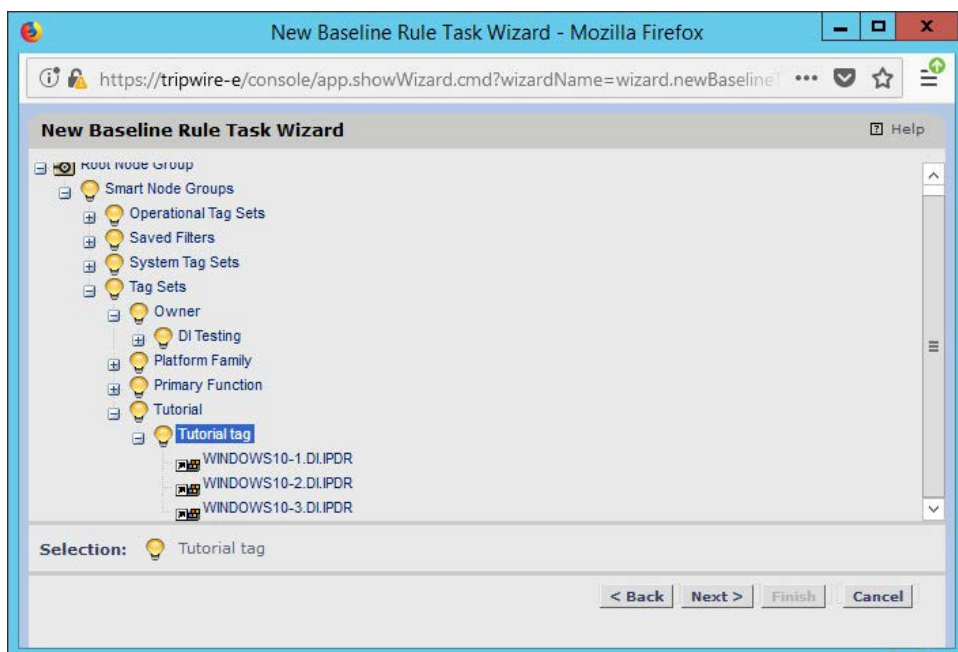
**Select the scope of the baseline operation.**

☒ New baselines only

☐ All baselines

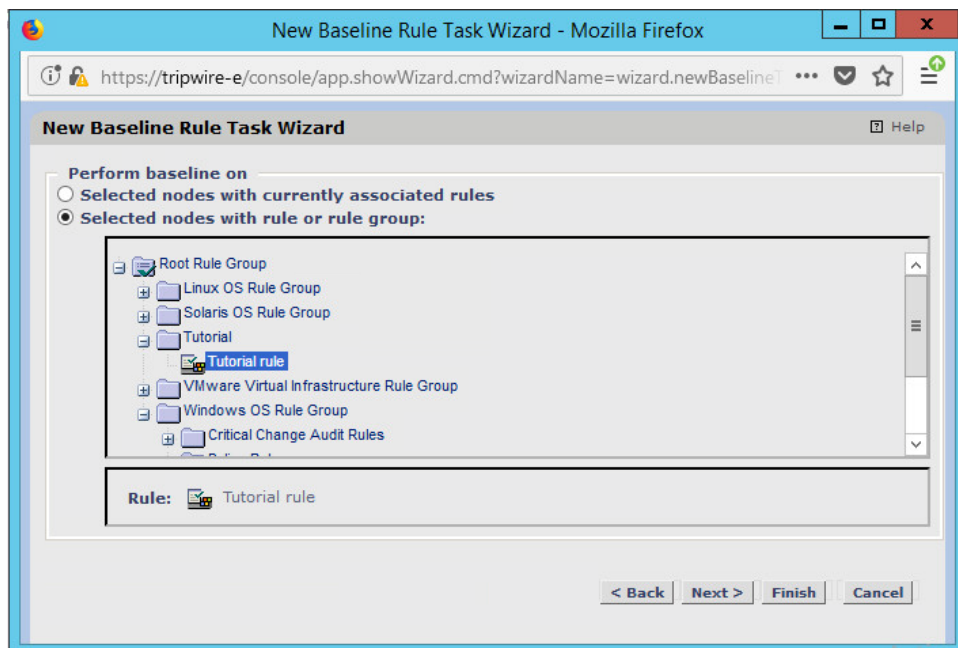
< Back Next > Finish Cancel

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



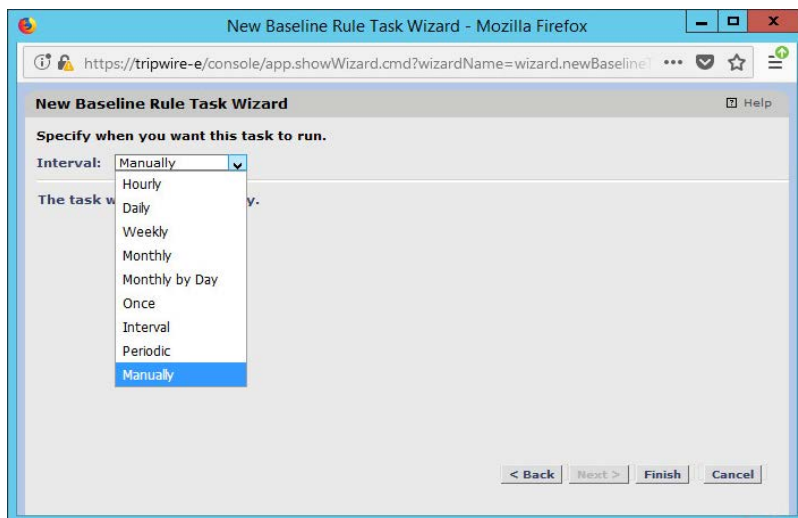
11. Click **Next**.

12. Select the rule created earlier.



13. Click **Next**.

14. Set the schedule of this task according to your organization's needs.



15. Click **Finish**.

## 2.13 Tripwire Log Center

### 2.13.1 Install Tripwire Log Center Manager

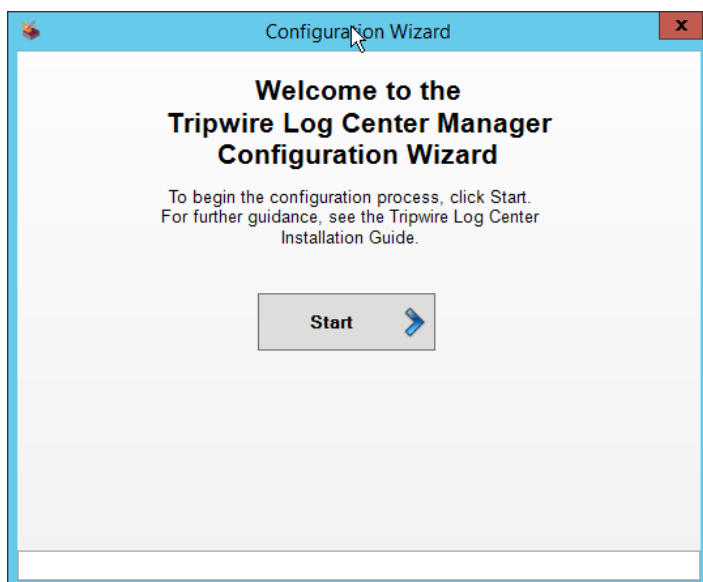
See the *Tripwire Log Center 7.3.1 Installation Guide*, which should accompany the installation media, for instructions on how to install **Tripwire Log Center**. Use the **Tripwire Log Center Manager** installer.

Notes:

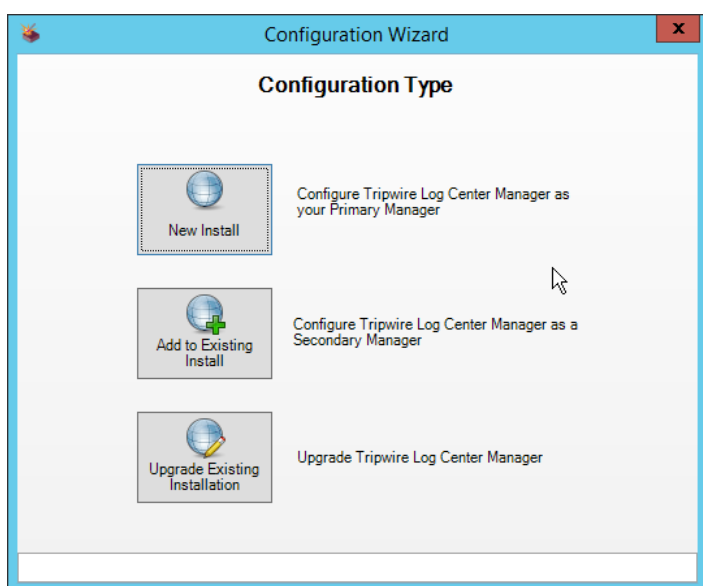
- a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise**.
- b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
- c. .NET Framework 3.5 is required for this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

### 2.13.2 Configure Tripwire Log Center Manager

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

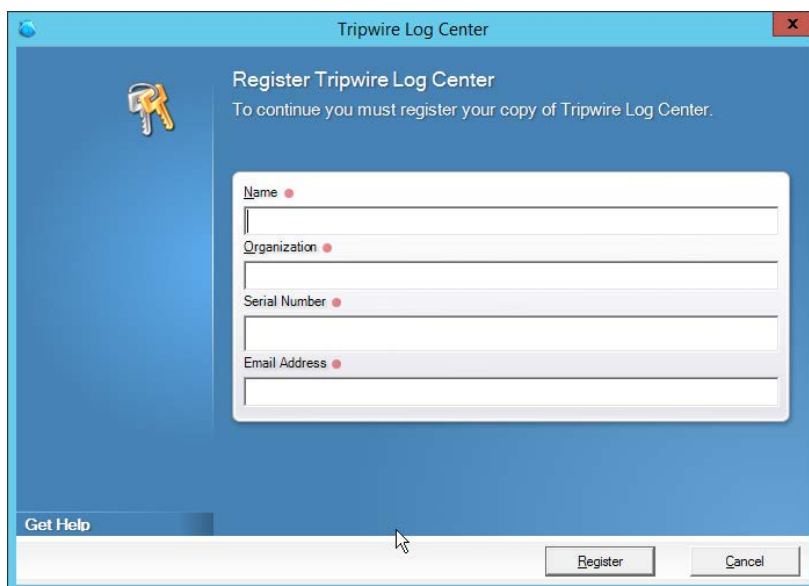


2. Click **Start**.

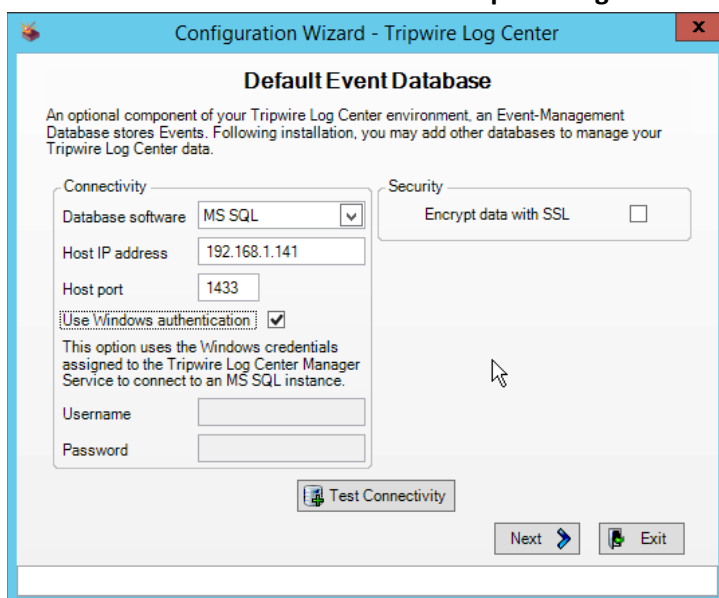


3. Click **New Install**.
4. Enter the registration details for your **Tripwire Log Center** license.

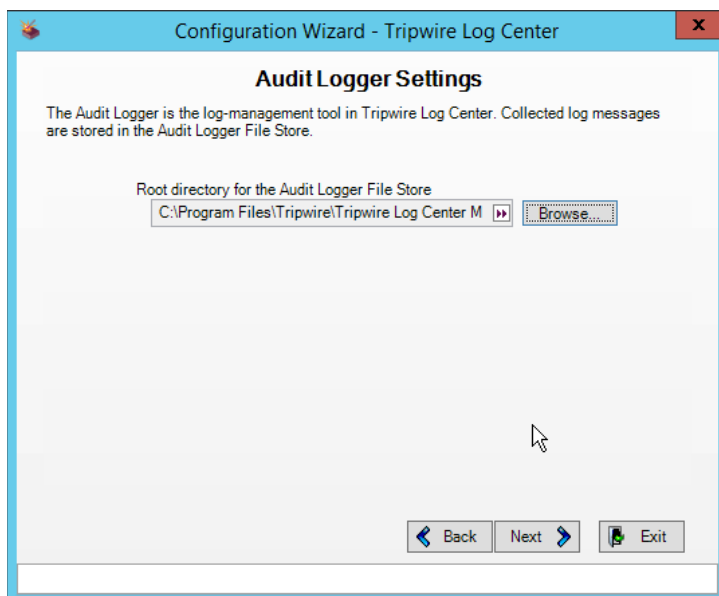




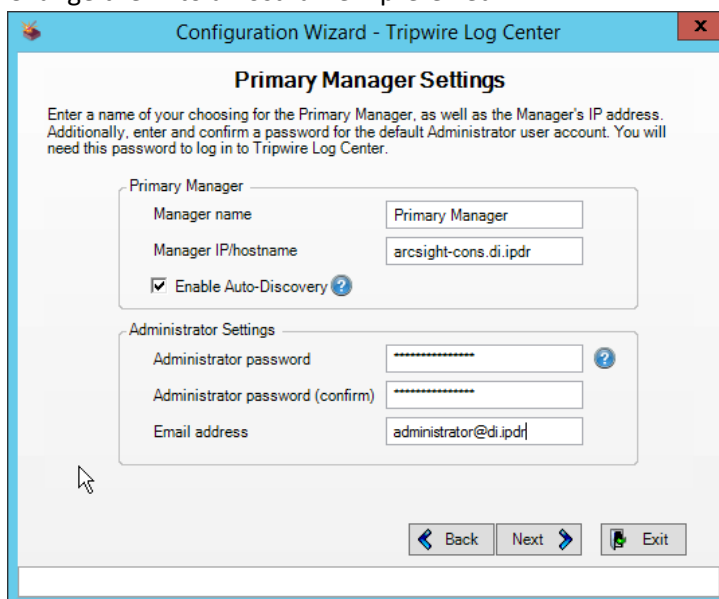
5. Click **Register**.
6. Enter details about the database that **Tripwire Log Center** should use.



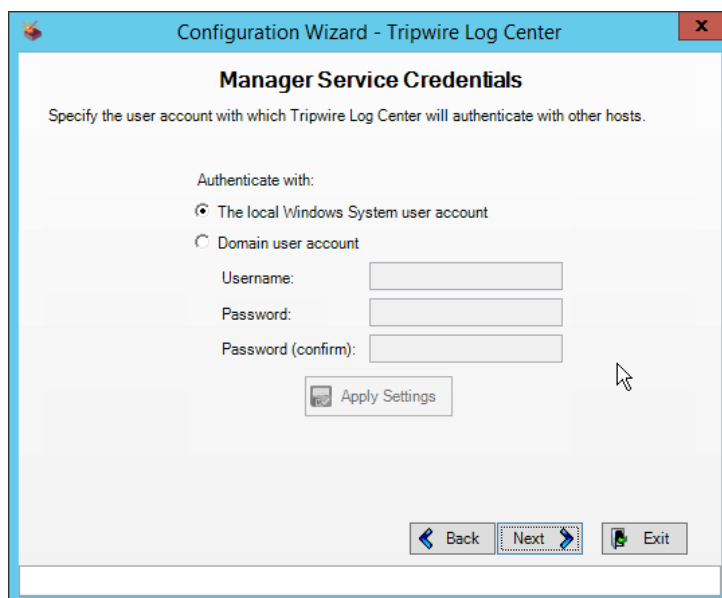
7. Click **Next**.
8. Select a directory in which to store log messages, such as C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT.



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

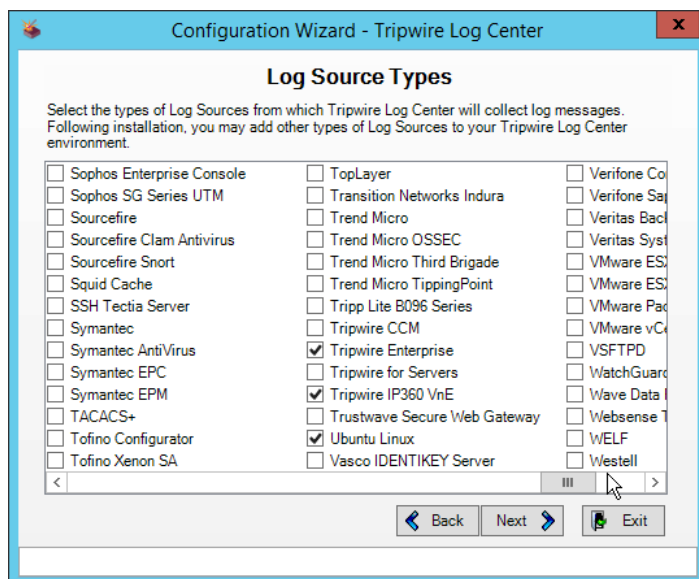


12. Click **Next**.

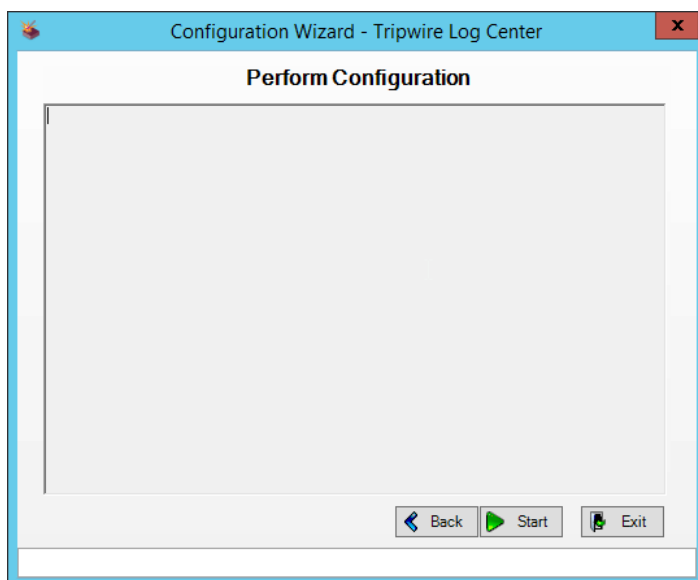


13. Click **Next**.

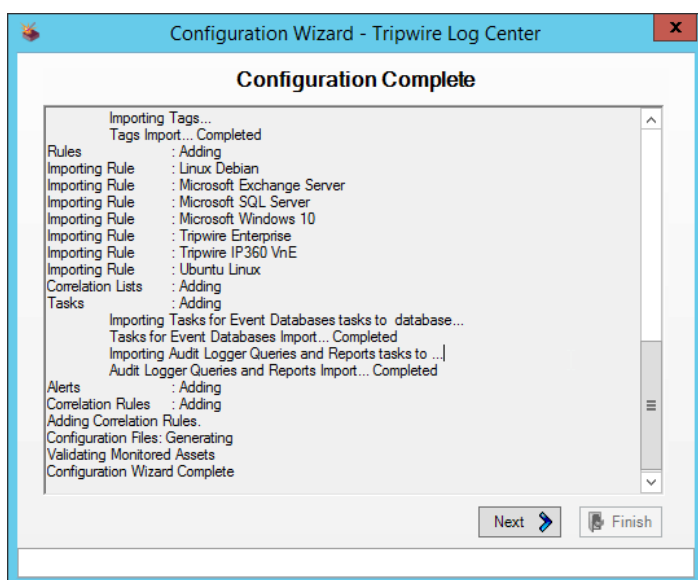
14. Select any log sources that you expect to collect with **Tripwire Log Center**. Examples: Tripwire Enterprise, Microsoft Windows 10, Tripwire IP360 VnE, Linux Debian, Ubuntu Linux, Microsoft Exchange, Microsoft SQL Server.



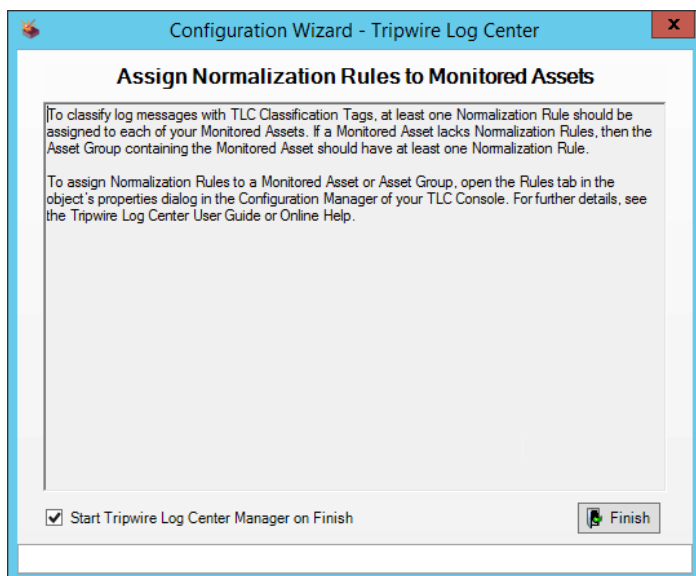
15. Click **Next**.



16. Click **Start**.



17. Click **Next**.



18. Click **Finish**.

### 2.13.3 Install Tripwire Log Center Console

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

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

## 2.14 Cisco Web Security Appliance

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

### 2.14.1 Network Configuration

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

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

## 2.14.2 System Setup

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

The screenshot shows the Cisco S000V Web Security Virtual Appliance System Setup Wizard. The wizard is at the '2. Network' step. The 'System Settings' section includes the following fields:

- Default System Hostname:** coeus.di.ipdr (with a hint: e.g. proxy.company.com)
- DNS Server(s):**
  - ☐ Use the Internet's Root DNS Servers
  - ☒ Use these DNS Servers:
    - 192.168.1.12
    - (optional)
    - (optional)
- NTP Server:** time.dmz.nccoe.nist.gov
- Time Zone:**
  - Region: America
  - Country: United States
  - Time Zone / GMT Offset: Eastern Time (New\_York)

The **Appliance Mode** section shows two options:

- ☒ **Standard**  
This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation).
- ☐ **Cloud Web Security Connector**  
This appliance will be used primarily to direct traffic to Cisco Cloud Web Security for cloud policy enforcement and threat defense (Cloud Web Security Connector installation).

Navigation buttons at the bottom include 'Prev', 'Cancel', and 'Next'.

7. Click **Next**.

The screenshot shows the Cisco S000V Web Security Virtual Appliance setup wizard. The browser address bar shows the URL: `coeus.di.ipdr:8080/system_administration/system_setup/wsassw_network_context`. The page title is "Cisco S000V Web Security Virtual Appliance". The navigation bar shows four steps: 1. Start, 2. Network (selected), 3. Security, and 4. Review. The main content area is titled "Network Context" and contains a checkbox labeled "Is there another web proxy in your network?". Below this, there is a text input field for "Proxy Group Name", an "Address" field with a hint "e.g. 10.1.1.1, 2001:420:80:1::5, example.com", and a "Port" field with the value "3128". A note states: "If another web proxy is present, the Cisco Web Security Appliance is recommended to be placed downstream of the existing proxy (closer to the client), as illustrated below:". Below the note is a diagram showing the network topology: CLIENTS, IRONPORT S-SERIES, ANOTHER WEB PROXY, FIREWALL, and INTERNET. The diagram shows the IRONPORT S-SERIES and ANOTHER WEB PROXY connected to the FIREWALL, which is connected to the INTERNET. The CLIENTS are connected to the IRONPORT S-SERIES. The bottom of the page has a copyright notice: "Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | Privacy Statement".

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

1. Start    **2. Network**    3. Security    4. Review

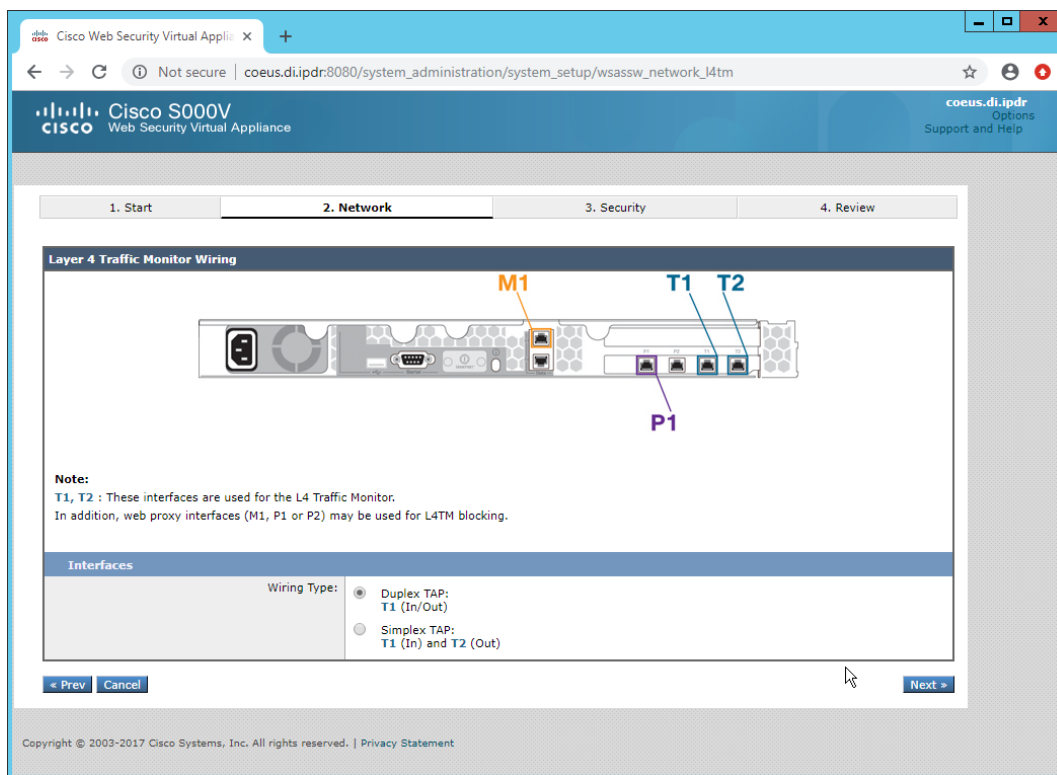
### Network Interfaces and Wiring

**Note:**  
**M1:** This interface is used to manage the appliance. Optionally, it may also handle web traffic.  
**P1:** This interface may be used to handle web traffic.

Interfaces	
Ethernet Port:	<div> <b>M1</b>  <input type="checkbox"/> Use M1 port for management only </div> <div> <b>P1</b>  <i>(Optional if M1 used for data)</i> </div>
IPv4 Address / Netmask:	<div>192.168.1.59/24</div> <div></div>
IPv6 Address / Netmask:	<div></div> <div></div>
Hostname:	<div>coeus.di.ipdr</div> <div><i>(e.g. wsa.example.com)</i></div>

10. Click **Next**.





11. Click **Next**.
12. Enter the **default gateway** and any additional gateways to use for routing.

1. Start    **2. Network**    3. Security    4. Review

**IPv4 Routes for Management and Data Traffic (Interface M1: 192.168.1.59)**

Default Gateway:   
*This will be the default route for external traffic as well as internal traffic with no static route below.*

**Static Routes Table**

Optionally, add static routes for Management access to the Cisco Web Security Appliance as well as Data traffic. Depending on the appliance functions you enable, these routes will be used for monitoring by the Secure Web Proxy and optional blocking by the L4 Traffic Monitor.

Name	Internal Network	Internal Gateway	
<input type="text"/>	<input type="text"/>	<input type="text"/>	🗑️
<i>Identifying name for route</i>	<i>IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)</i>	<i>IPv4 Address</i>	

Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

13. Click **Next**.

The screenshot shows the 'Transparent Connection Settings' screen in the Cisco S000V Web Security Virtual Appliance setup wizard. The wizard is at step 2, 'Network', with previous steps being '1. Start', '3. Security', and '4. Review'. The screen is titled 'Transparent Connection Settings' and includes a note: 'For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router.' Below this, there are two radio button options for 'Transparent Redirection Device': 'Layer 4 Switch or No Device' (selected) and 'WCCP v2 Router'. Under 'Layer 4 Switch or No Device', there is a checkbox for 'Enable standard service ID: 0 web\_cache (port 80)'. Under 'WCCP v2 Router', there is a checkbox for 'Enable router security for this service'. There are input fields for 'Router Addresses' (with a note 'Separate multiple addresses with commas or whitespace.') and 'Passphrase' (with a note 'Must be 7 or less characters.'). There is also a 'Confirm Passphrase' field. At the bottom, there are buttons for '< Prev', 'Cancel', and 'Next >'. The footer of the page shows 'Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | Privacy Statement'.

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

Cisco Web Security Virtual Appli x

Not secure | coeus.di.ipdr:8080/system\_administration/system\_setup/wsassw\_network\_admin

Cisco S000V  
Web Security Virtual Appliance

coeus.di.ipdr  
Options  
Support and Help

1. Start 2. Network 3. Security 4. Review

**Administrative Settings**

Administrator Passphrase:

☐ Generate a passphrase:

☒ Enter a passphrase of your choice

Passphrase:

Retype Passphrase:

Email system alerts to:

e.g. admin@company.com

Send Email via SMTP Relay Host (optional): ?

Port: ?

i.e., smtp.example.com, 10.0.0.3 optional

AutoSupport: ☐ Send system alerts and weekly status reports to Cisco Customer Support

**SensorBase Network Participation**

Network Participation: ☐ Allow Cisco to gather anonymous statistics on HTTP requests and report them to Cisco in order to identify and stop web-based threats.

Participation Level: ☐ Limited - Summary URL information.

☒ Standard - Full URL information. (Recommended)

Learn what information is shared...

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

The screenshot shows the Cisco S000V Web Security Virtual Appliance configuration page. The browser address bar shows the URL `coeus.di.ipdr:8080/system_administration/system_setup/wsassw_security`. The page has a blue header with the Cisco logo and the text "Cisco S000V Web Security Virtual Appliance". On the right, there are links for "Options", "Support and Help", and a user profile "coeus.di.ipdr".

The main content area has a progress bar with four steps: 1. Start, 2. Network, 3. Security (selected), and 4. Review. Below the progress bar is the "Security Settings" section, which contains several rows of configuration options:

- Global Policy Default Action:** Two radio buttons: "Monitor all traffic" (selected) and "Block all traffic". A note below states: "If block all traffic is selected, the Global Access Policy will be initially configured to block all proxied protocols (HTTP, HTTPS, FTP over HTTP, and native FTP)."
- L4 Traffic Monitor:** A label "Action for Suspect Malware Addresses" followed by two radio buttons: "Monitor only" and "Block" (selected).
- Acceptable Use Controls:** A checkbox "Enable" which is checked. A note below states: "The Global Access Policy will be initially configured to monitor all pre-defined categories."
- Reputation Filtering:** A checkbox "Enable" which is checked. A note below states: "The Global Access Policy will be initially configured to use Web Reputation Filtering and Adaptive Scanning."
- Malware and Spyware Scanning:** Two checkboxes "Enable Webroot" and "Enable Sophos" are both checked. A note below states: "The Global Access Policy and Outbound Malware Scanning Policy will be initially configured to apply the actions configured below." Below this note are two radio buttons: "Monitor only" and "Block" (selected).
- Cisco Data Security Filtering:** A checkbox "Enable" which is checked. A note below states: "The Global Cisco Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads."

At the bottom of the form, there are buttons for "< Prev", "Cancel", and "Next >". A mouse cursor is hovering over the "Next >" button. At the very bottom of the page, there is a copyright notice: "Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | Privacy Statement".

24. Click **Next**.

Management (M1)	
IPv4 Address:	192.168.1.59/24
Hostname:	coeus.di.ipdr
Use M1 port for management only:	No
<b>L4 Traffic Monitor:</b>	
Wiring Type:	Duplex TAP: T1 (In/Out)
<b>Routes</b> <span>Edit</span>	
Default IPv4 Gateway:	192.168.1.1
Static IPv4 Routes:	No static routes have been defined.
<b>Transparent Connection Settings</b> <span>Edit</span>	
Transparent Redirection Device Type:	Layer 4 Switch or No Device
<b>Administrative Settings</b> <span>Edit</span>	
Administrator Passphrase:	(hidden)
Email System Alerts To:	administrator@di.ipdr
Internal SMTP Relay Hosts:	exchange.di.ipdr:25
AutoSupport:	No
SensorBase Network Participation:	No

Security Settings	
Global Policy Default Action:	Monitor
L4 Traffic Monitor:	Monitor and Block
Acceptable Use Controls:	Enabled
Reputation Filtering:	Enabled
Cisco DVS Engine:	Webroot: Enabled McAfee: Disabled Sophos: Enabled
Cisco Data Security Filtering:	Disabled

< Previous Cancel Install This Configuration

25. Click **Install This Configuration**.

### 2.14.3 Using WSA to Proxy Traffic

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

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

### 2.14.3.1 Creating a PAC File

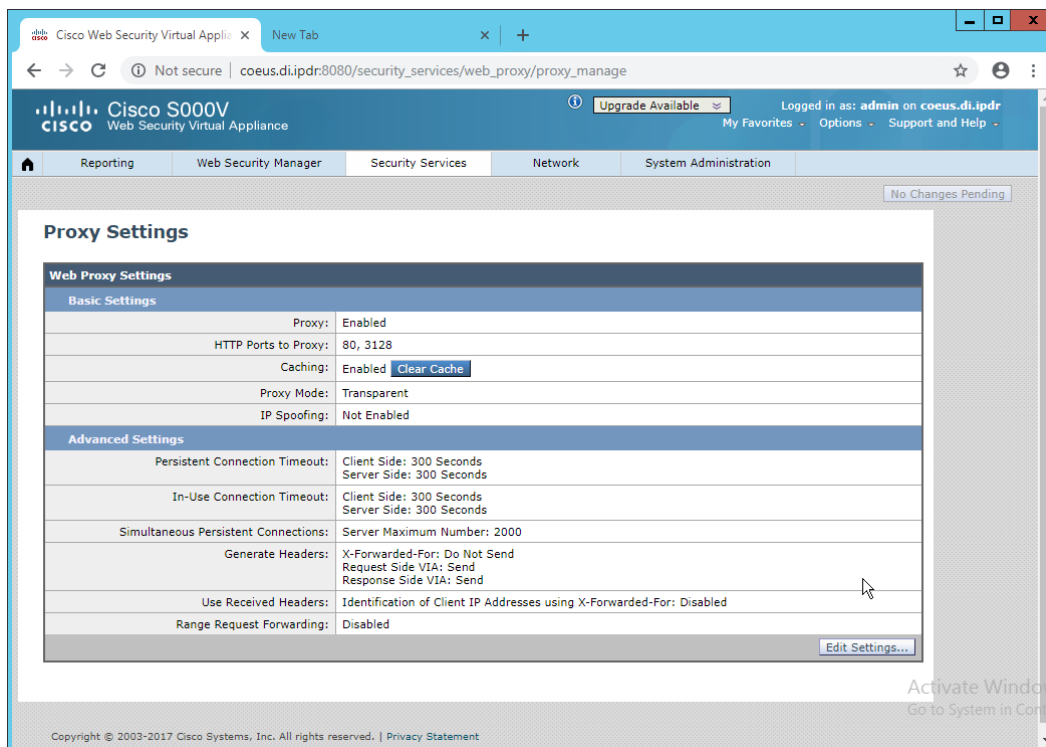
1. Create a new file named **wpad.dat** and enter the following JavaScript function:

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

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

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

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



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

The screenshot displays the 'Edit Web Proxy Settings' page of a Cisco Web Security Virtual Appliance. The browser address bar shows 'coeus.d.ipdr:8080/security\_services/web\_proxy/proxy\_manage'. The page is divided into two main sections: 'Basic Settings' and 'Advanced Settings'.

**Basic Settings:**

- Enable Proxy:** Checked.
- HTTP Ports to Proxy:** A text input field containing '3128'.
- Caching:** Checked (Enable).
- Proxy Mode:** Radio buttons for 'Transparent' (selected) and 'Forward'. A note below states: 'When in Transparent mode, the proxy can accept both transparent and explicit forward connections. Transparent connections require a transparent redirection device (see Network > Transparent Redirection). When in Forward mode, only explicit forward connections are supported.'
- IP Spoofing:** A checkbox for 'Enable IP Spoofing' is unchecked. Below it are radio buttons for 'For Transparent Connections Only' (selected) and 'For All Connections'. A note below states: 'When enabling IP spoofing in forward mode, you should ensure that you have appropriate network devices to route return packets back to the Web Security appliance.'

**Advanced Settings:**

- Persistent Connection Timeout:** Two input fields for 'Client Side' and 'Server Side', both set to '300' seconds.
- In-Use Connection Timeout:** Two input fields for 'Client Side' and 'Server Side', both set to '300' seconds.
- Simultaneous Persistent Connections:** An input field for 'Server Maximum Number' set to '2000'.
- Generate Headers:**
  - X-Forwarded-For:** Radio buttons for 'Send' and 'Do Not Send' (selected).
  - Request Side VIA:** Radio buttons for 'Send' (selected) and 'Do Not Send'.
  - Response Side VIA:** Radio buttons for 'Send' (selected) and 'Do Not Send'.
- Use Received Headers:** A checkbox for 'Enable Identification of Client IP Addresses using X-Forwarded-For' is unchecked.

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



**Edit Proxy Auto-Configuration File Hosting Settings**

**Proxy Auto-Configuration File Hosting**

☒ **Enable Proxy Auto-Config File Hosting**

**Basic Settings**

PAC Server Ports:   
Enter multiple ports separated with a comma

PAC File Expiration: ☐ Allow PAC file to expire in browser's cache  
PAC file will expire after  minutes  
If this option is enabled, some supported browsers will automatically download a new copy of the PAC file if it is available after the defined expiration schedule.

**PAC Files**

Uploaded Files		Add Row
wpad.dat	Download PAC File...	
<input type="button" value="Choose File"/>	No file chosen	

**Hostnames for Serving PAC Files Directly ?**

To serve PAC files for PAC file requests that do not include the PAC server port, enter one or more hosts here and choose a default PAC file name. You can specify hosts using hostnames or IP addresses.

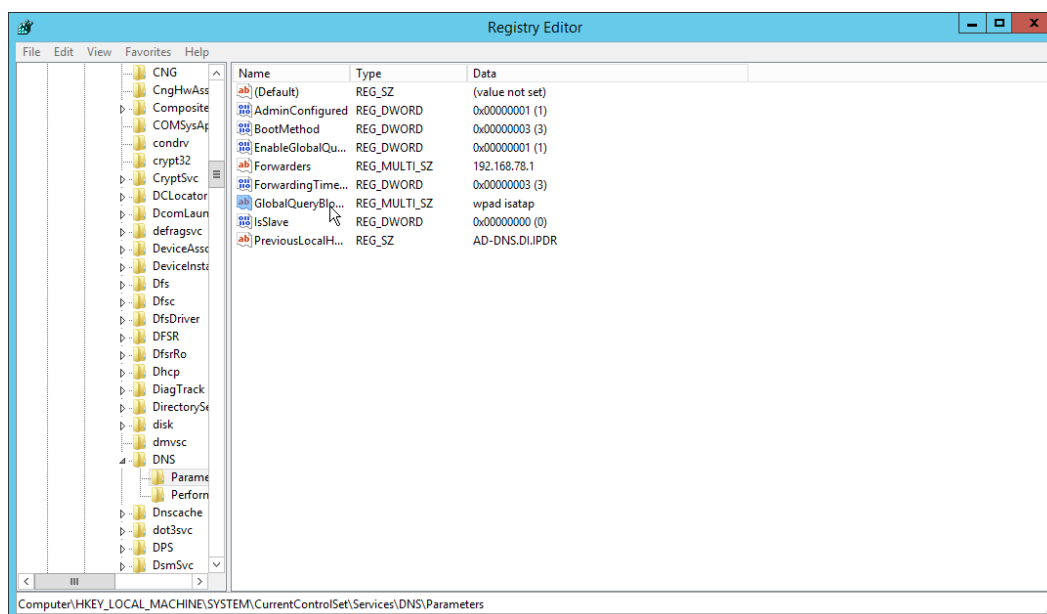
Hostname	Default PAC File for "Get/" Request through Proxy Port	Add Row
<input type="text"/>	wpad.dat	

Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | Privacy Statement

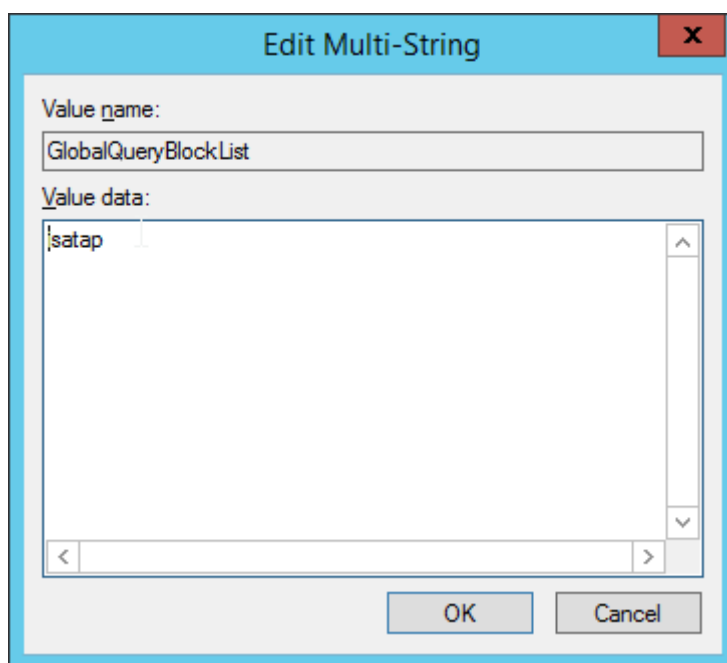
13. Click **Submit**.
14. Click **Commit Changes**.
15. Enter a comment if desired.
16. Click **Commit Changes**.

### 2.14.3.2 Setting Up Web Proxy Auto Discovery (WPAD)

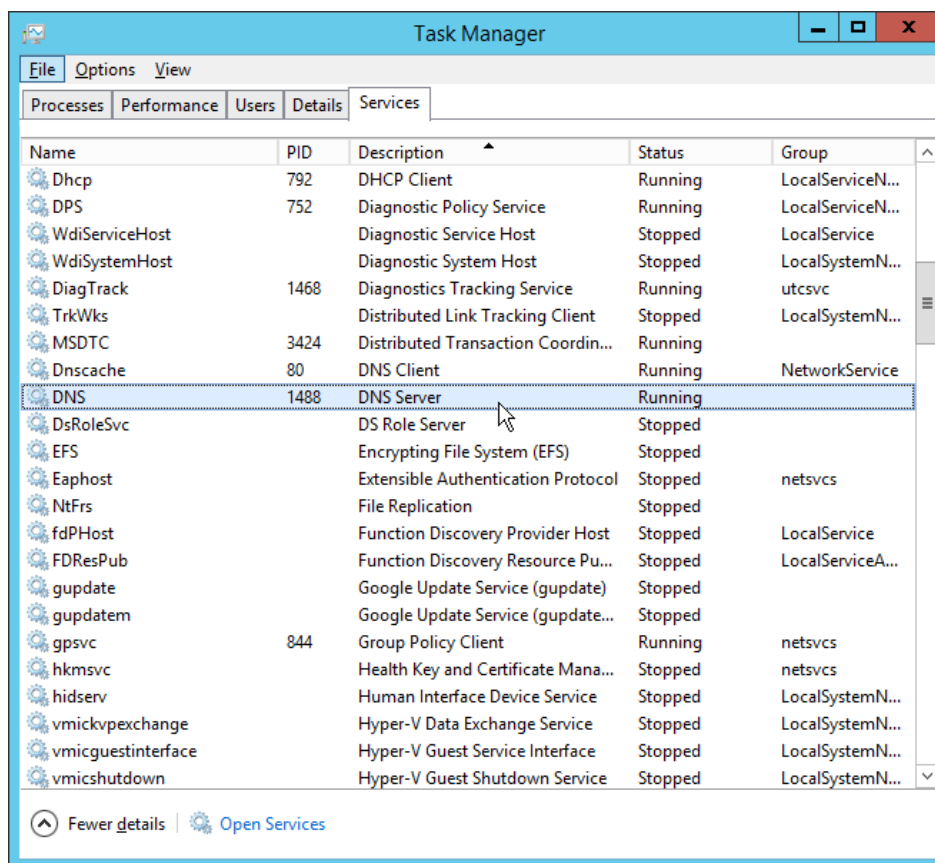
1. On the DNS server, open **regedit.exe**.
2. Navigate to **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > DNS > Parameters**.



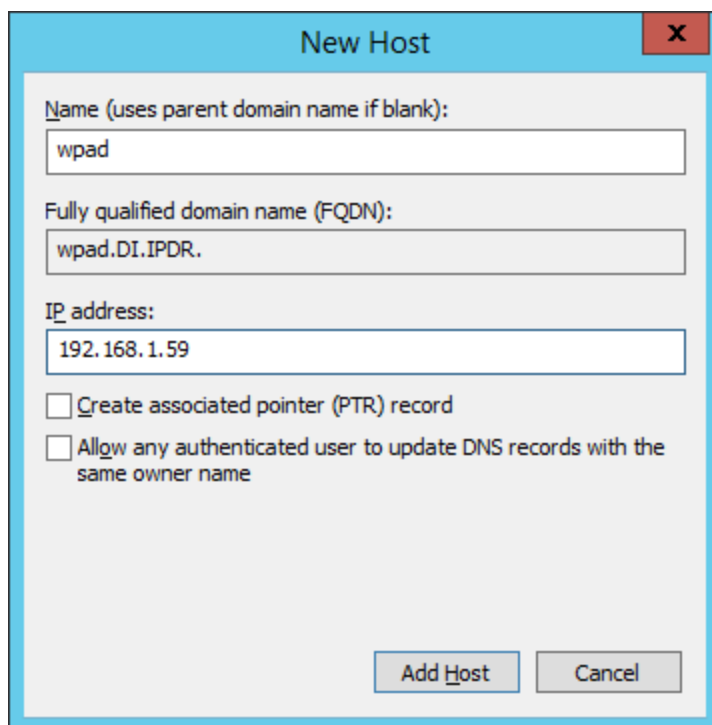
3. Double-click **GlobalQueryBlockList**.
4. Remove wpad from the list but leave isatap on the list.



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



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



13. Click **Add Host**.

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

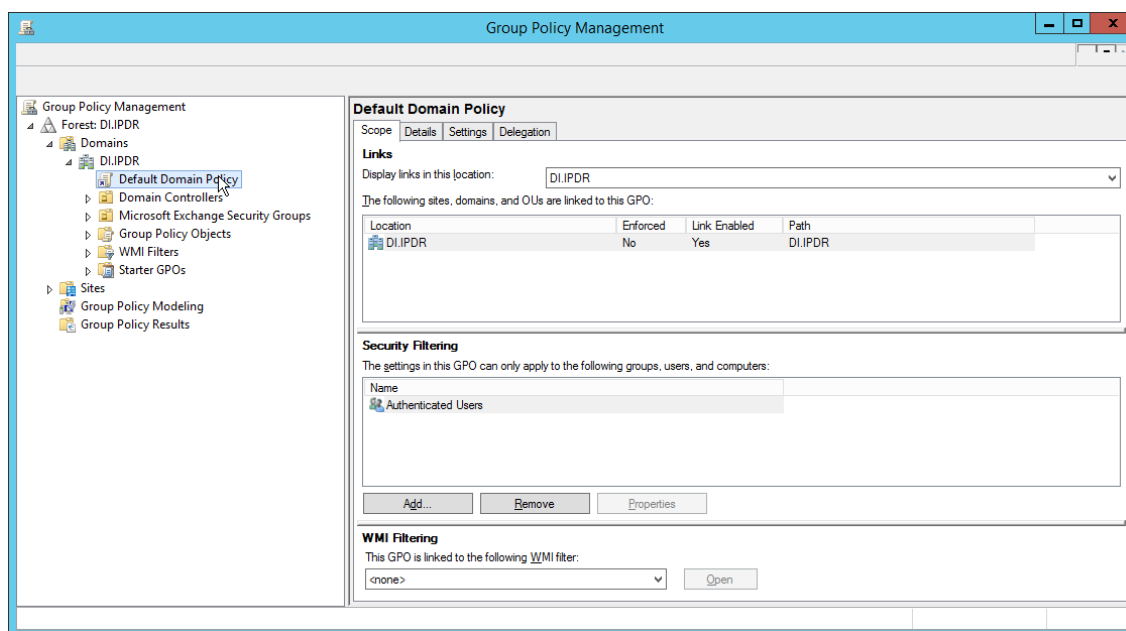
#### *2.14.3.3 Configure Group Policy to Use Explicit Proxy*

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

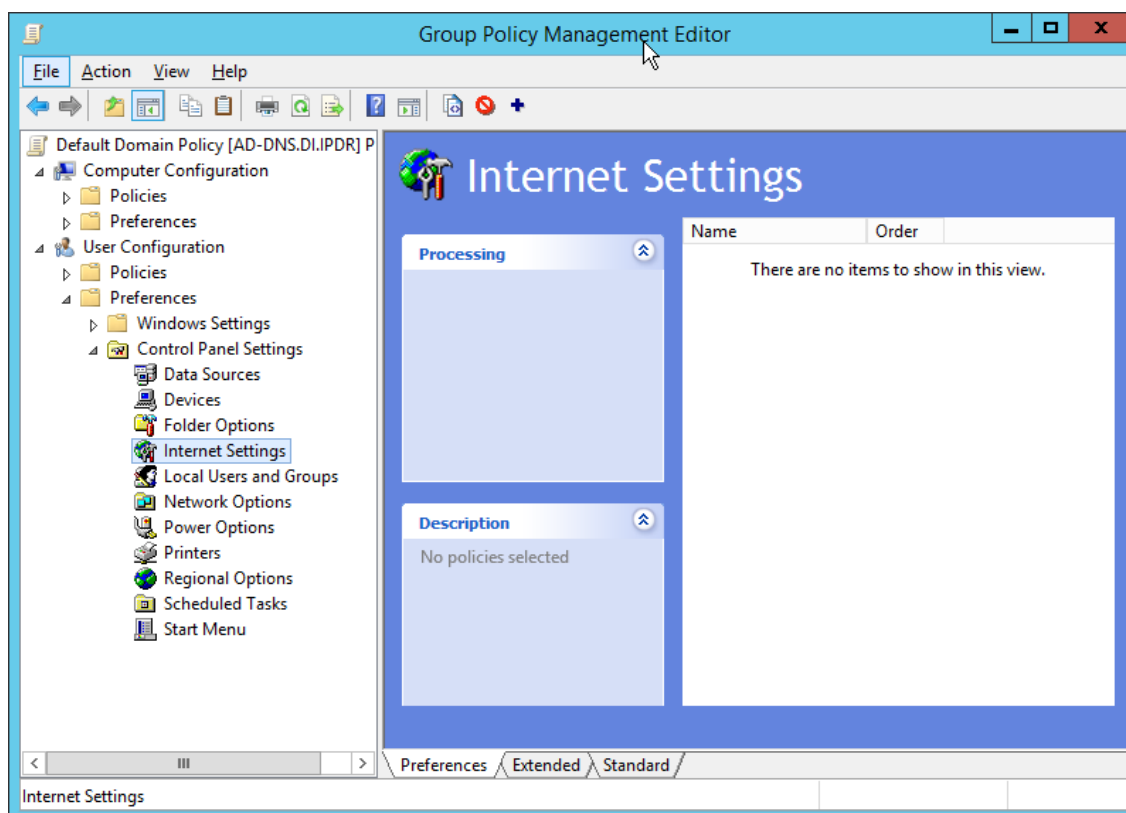
To mitigate this vulnerability, we explicitly point to this proxy file with any browsers used by clients. For Internet Explorer and Google Chrome, it is sufficient to change group policy in Active Directory to direct the change across all systems.

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

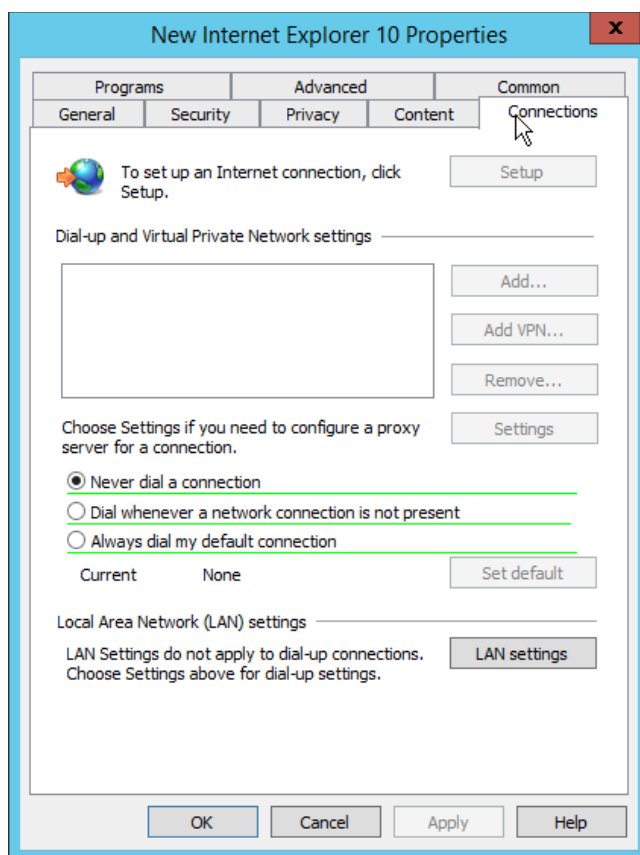
1. In **Group Policy Management**, right-click the **Default Domain Policy** and click **Edit**.



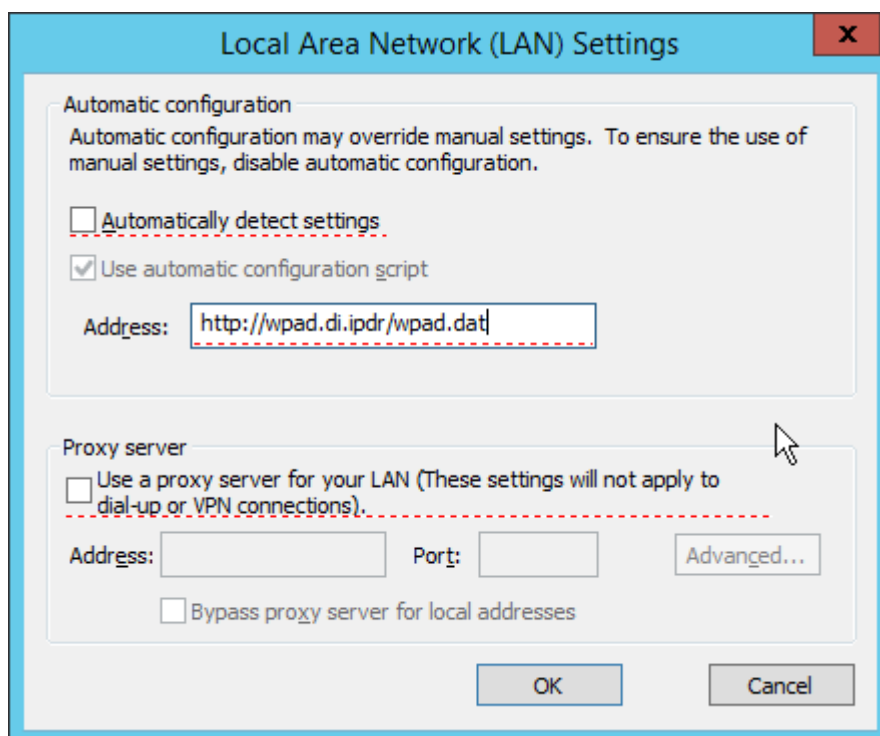
2. In Group Policy Management Editor, navigate to **User Configuration > Preferences > Control Panel Settings > Internet Settings**.



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

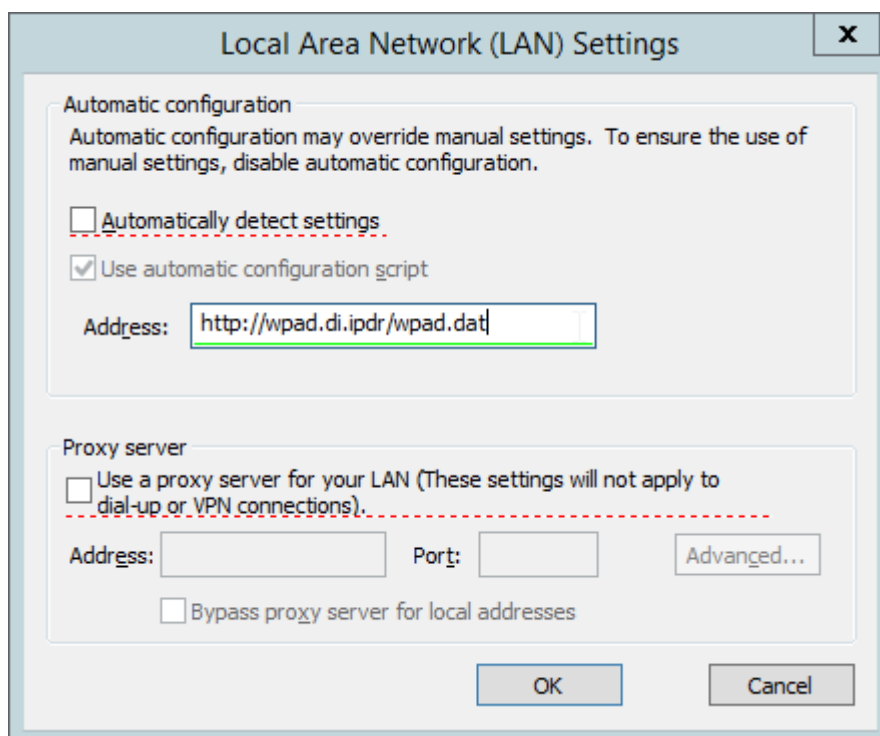


5. Click **LAN Settings**.
6. Enter the **address** of the WPAD file for address. This will likely take the form `http://wpad.my.domain/wpad.dat` if you followed these instructions for configuring the proxy file.
7. Press the **F8** key to disable all settings in this dialogue box. (Note: This should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



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



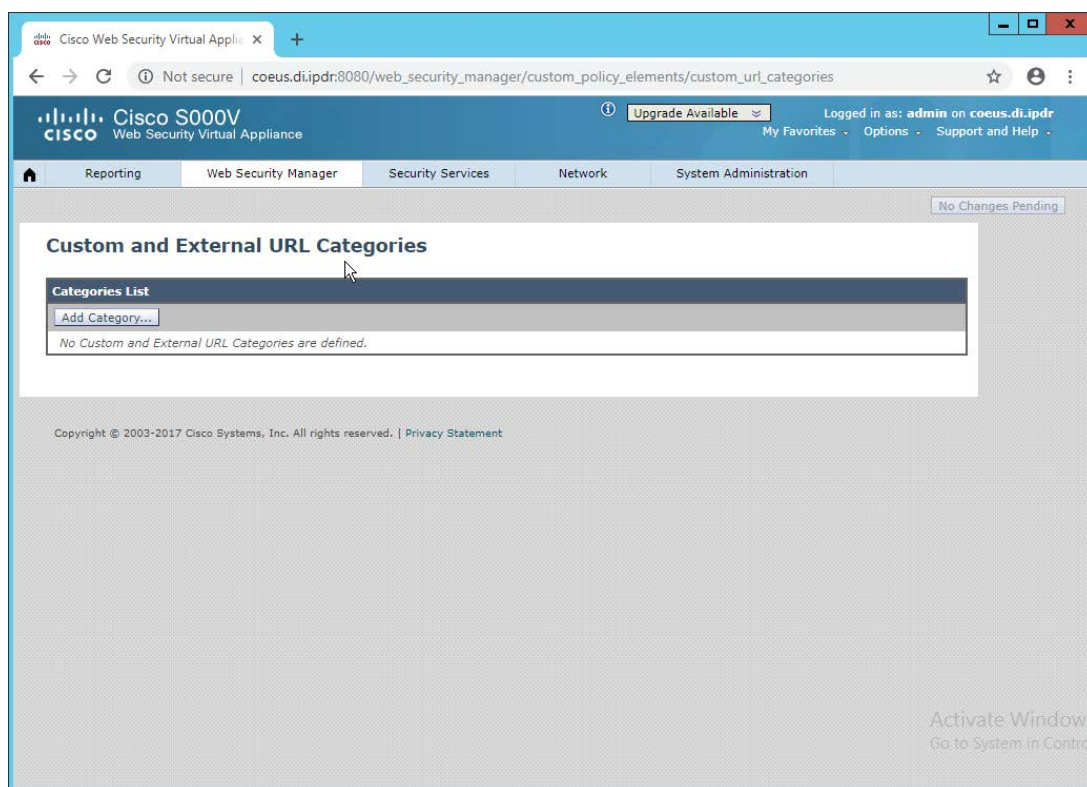


9. Press **F6** to enable this setting. (Note: The explicit WPAD address should now be underlined in green.)
10. Click **OK**.
11. Click **OK**.

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

#### 2.14.4 Denylisting

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



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

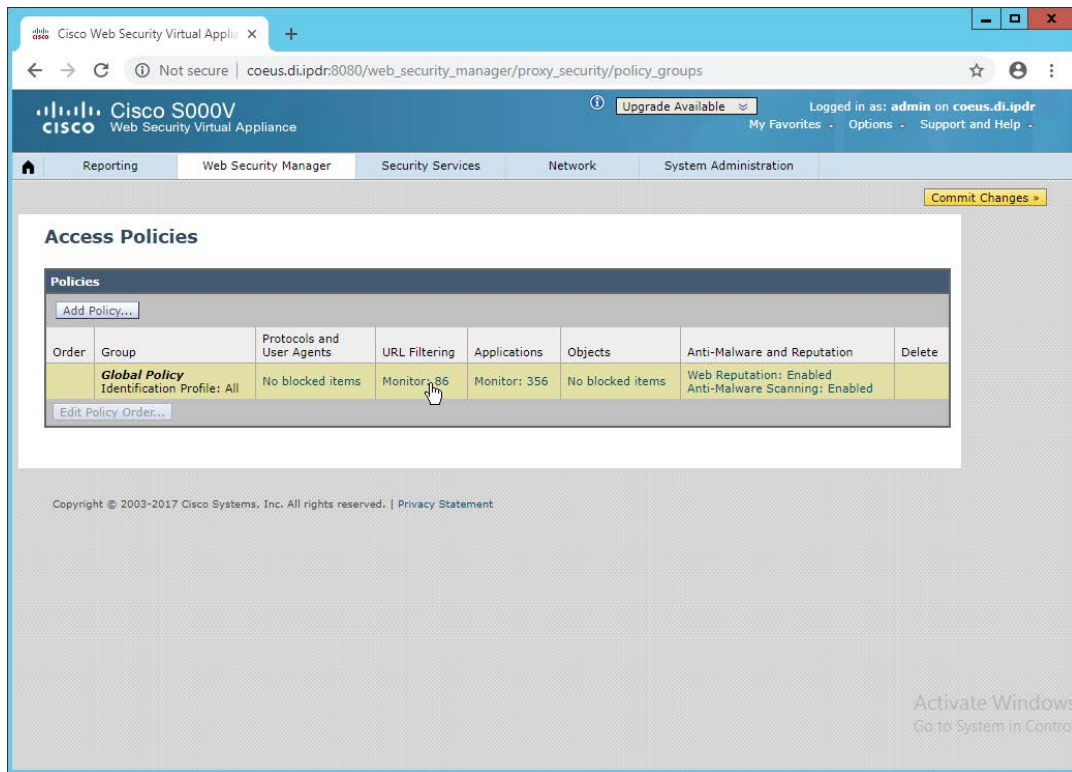
The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The browser address bar indicates the URL: `coeus.dl.ipdr:8080/web_security_manager/custom_policy_elements/custom_url_categories`. The interface is logged in as `admin` on `coeus.dl.ipdr`. The main navigation bar includes `Reporting`, `Web Security Manager`, `Security Services`, `Network`, and `System Administration`. The `Web Security Manager` tab is active, and the `Custom and External URL Categories: Add Category` form is displayed.

The form is titled `Edit Custom and External URL Category` and contains the following fields:

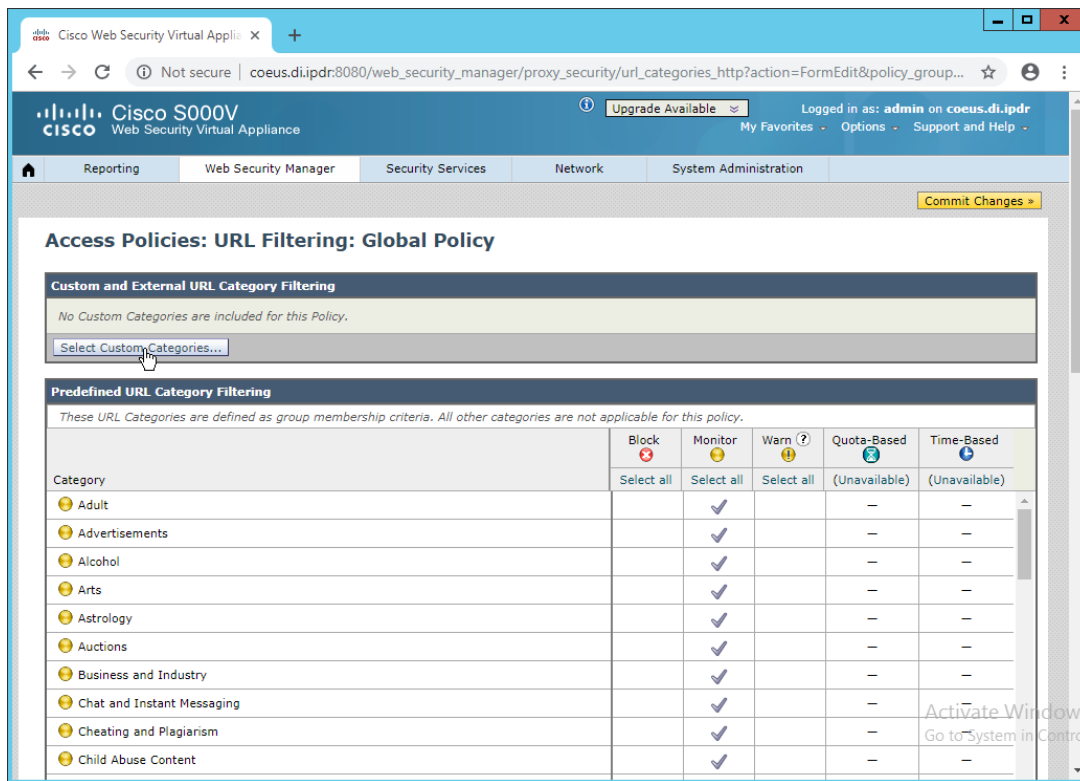
- `Category Name`: `Malicious Blacklist`
- `List Order`: `1`
- `Category Type`: `Local Custom Category` (dropdown menu)
- `Sites`: A text area containing `.evil.ko`. A `Sort URLs` button is located to the right of the text area. Below the text area, a note reads: `(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)`
- `Advanced`: A section with a `Regular Expressions` field. A note below the field reads: `Enter one regular expression per line.`

At the bottom of the form, there are `Cancel` and `Submit` buttons. A `No Changes Pending` status message is visible in the top right corner of the form area.

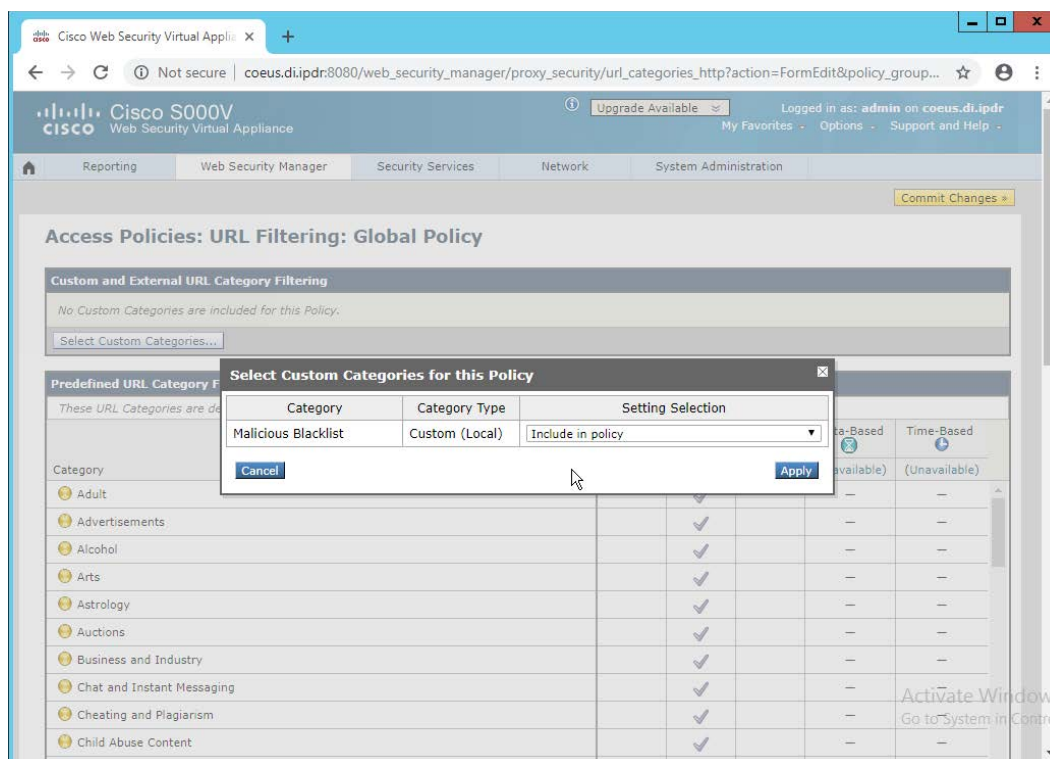
6. Click **Submit**.
7. Navigate to **Web Security Manager > Access Policies**.



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



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



11. Click **Apply**.

**Access Policies: URL Filtering: Global Policy**

**Custom and External URL Category Filtering**

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Block	Redirect	Allow (?)	Monitor	Warn (?)	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Malicious Blacklist	Custom (Local)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	—	—

Select Custom Categories...

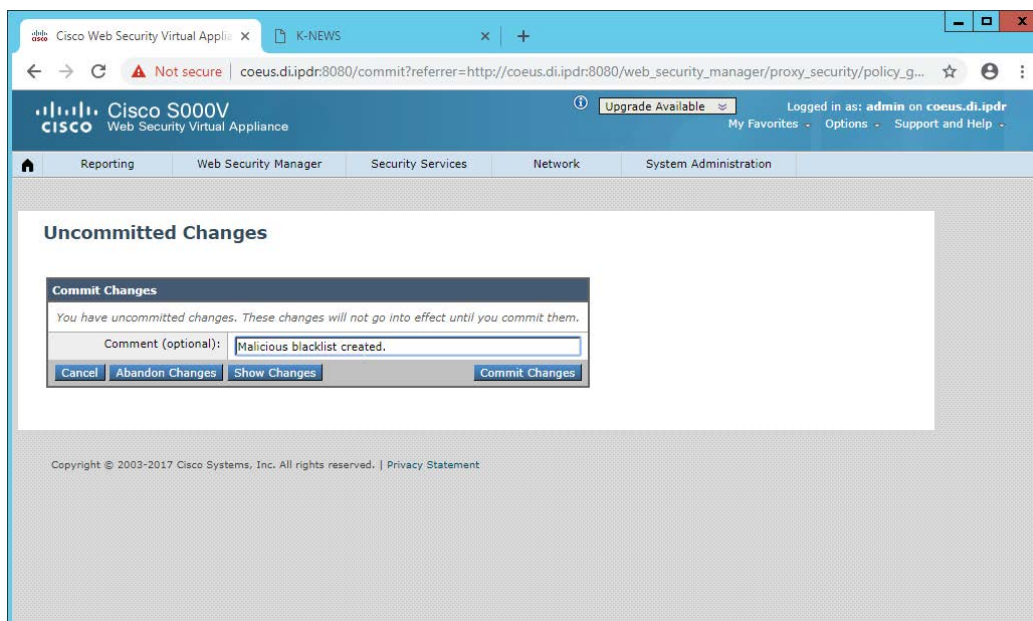
Cancel Submit

**Predefined URL Category Filtering**

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Block	Monitor	Warn (?)	Quota-Based	Time-Based
	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	—	—
Advertisements	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	—	—
Alcohol	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	—	—
Arts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	—	—
Astrology	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	—	—
Auctions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	—	—

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



16. Click **Commit Changes**.

## 2.15 Symantec Data Loss Prevention

### 2.15.1 Install Oracle 12c Enterprise

1. Unzip the Symantec DLP installation files.
2. Download the Oracle 12c installation files from <https://www.oracle.com> if they are not included with the Symantec DLP installation files.
3. Move both sets of installation files to a temporary directory, such as **C:\temp**.
4. Copy the Symantec **12.2.0.1\_64\_bit\_Installation\_Tools** folder to **C:\temp\Oracle\tools**.
5. From a command prompt, navigate to **C:\temp\Oracle\database**, assuming the Oracle installation files were unzipped to **C:\temp\Oracle**.
6. Run the following command:  

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



Oracle Database 12c Release 2 Installer - Step 1 of 10

### Configure Security Updates

Provide your email address to be informed of security issues, install the product and initiate configuration manager. [View details.](#)

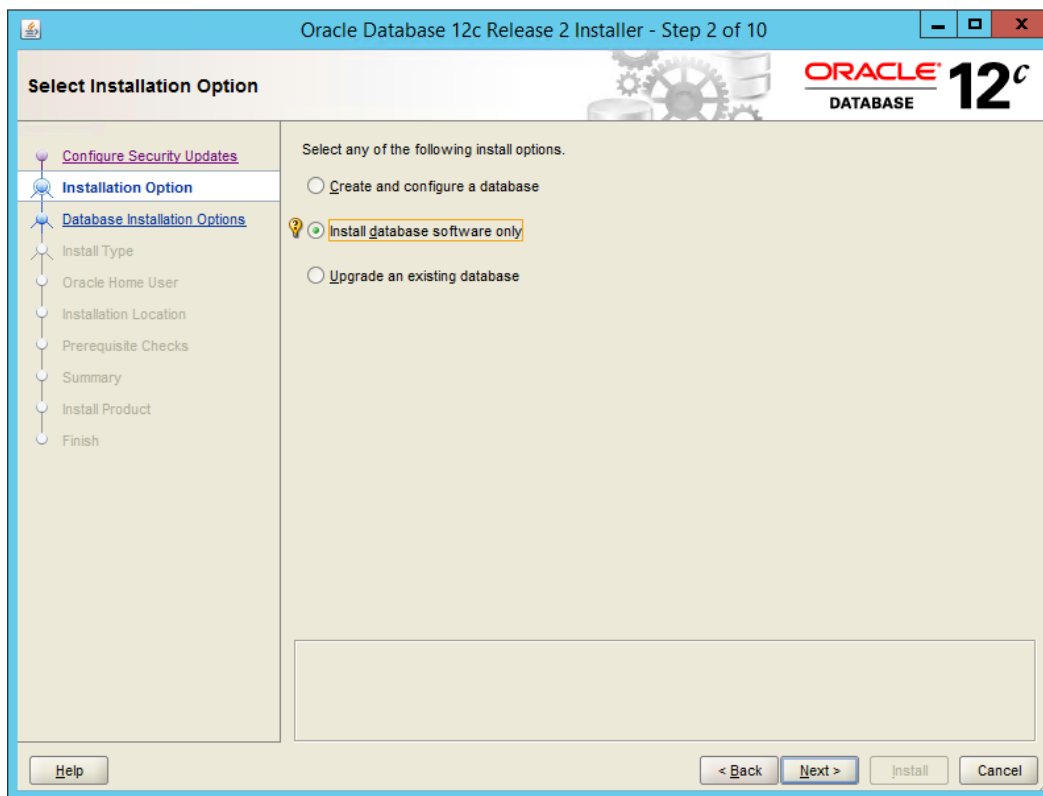
Email:

Easier for you if you use your My Oracle Support email address/username.

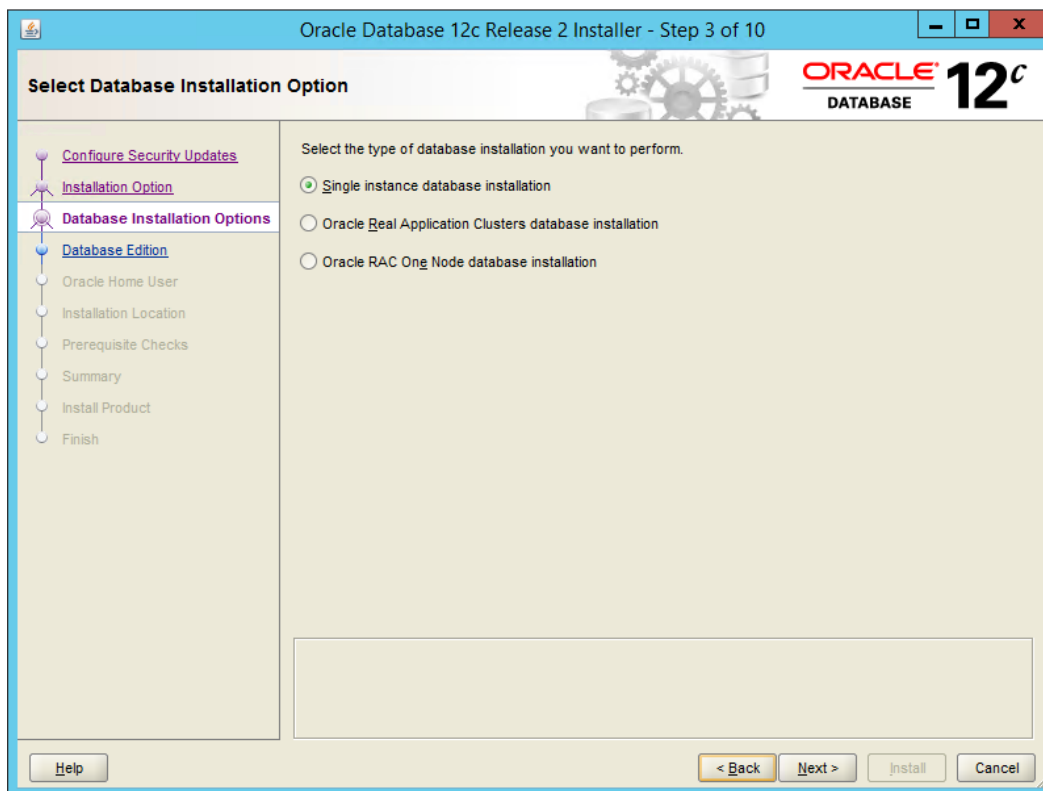
☐ I wish to receive security updates via My Oracle Support.

My Oracle Support Password:

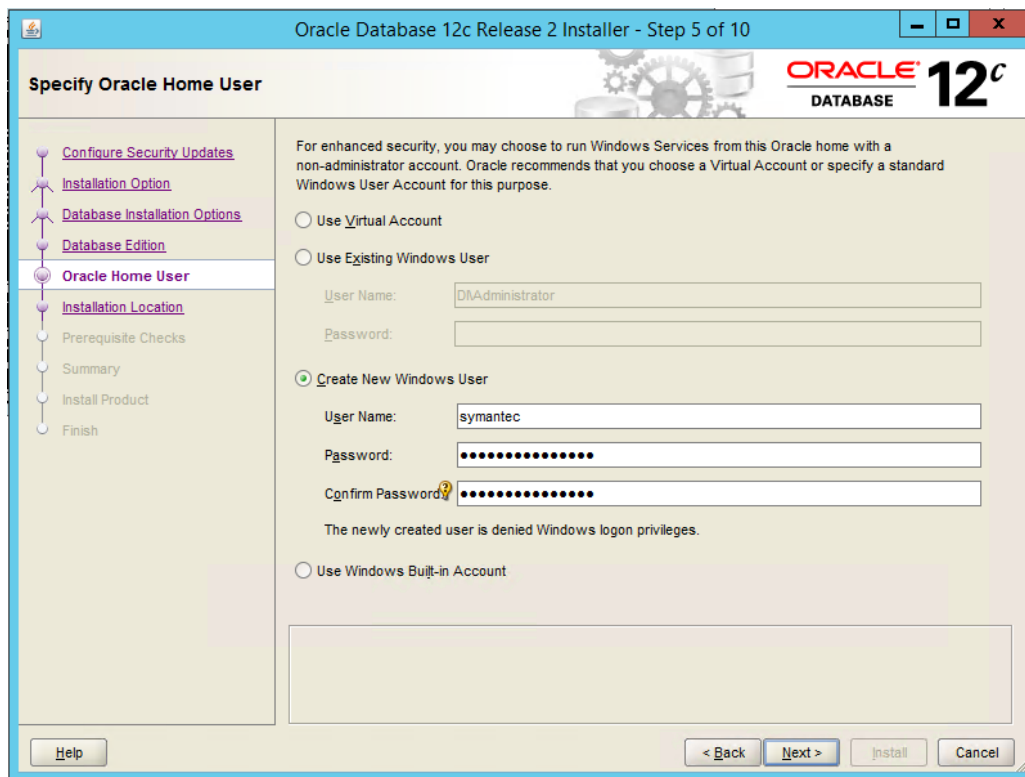
8. Click **Next**.
9. Select **Install database software only**.



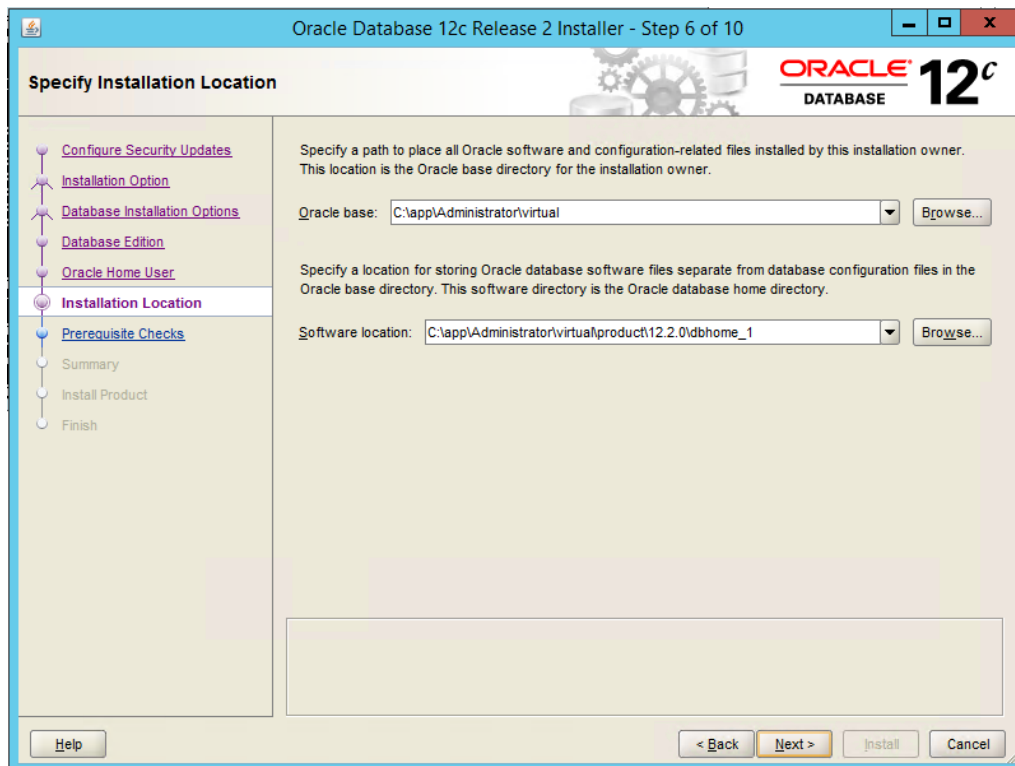
10. Click **Next**.
11. Select **Single instance database installation**.



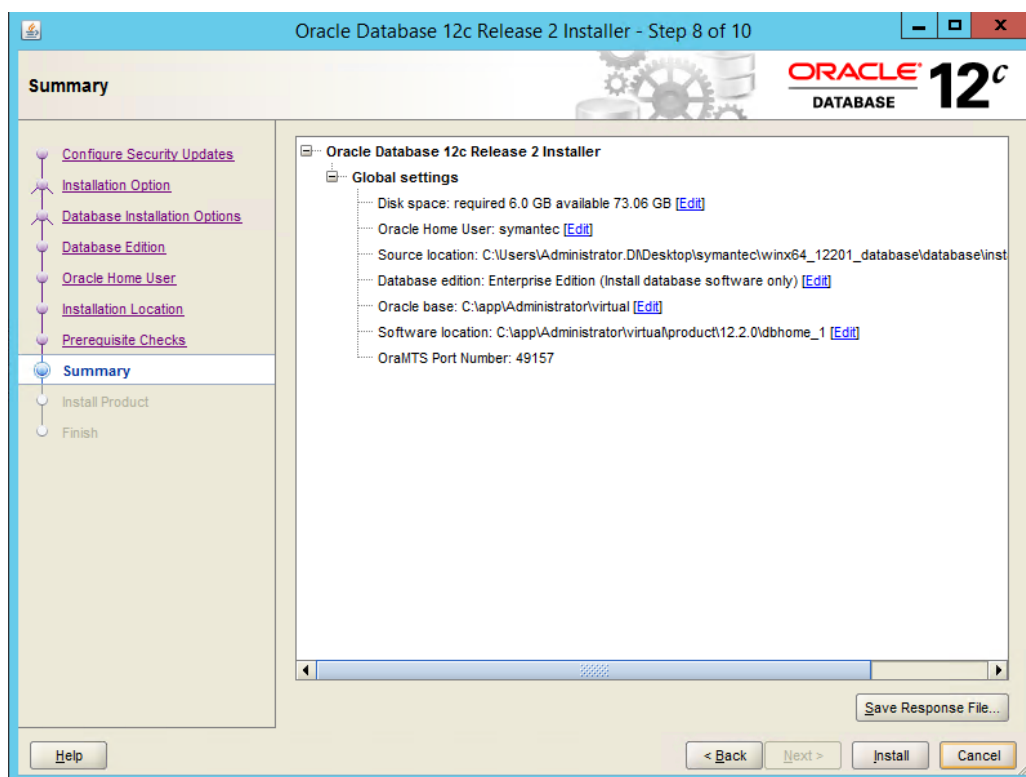
12. Click **Next**.
13. Select **Standard Edition**.
14. Click **Next**.
15. Select **Create New Windows User**.
16. Enter the **username** and **password** of a new user for Active Directory.



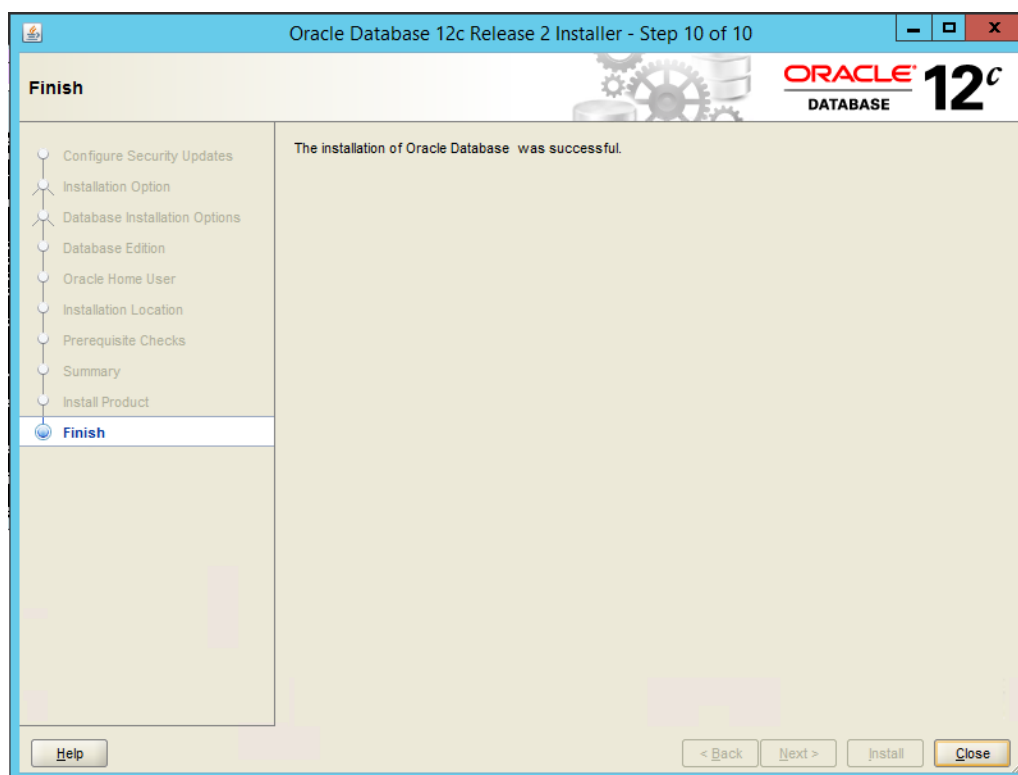
17. Click **Next**.
18. Select a location to install the software, if desired.



19. Click **Next**.



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



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

## 2.15.2 Create an Oracle Database for Symantec DLP

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

```
> set
ORACLE_HOME=C:\app\Administrator\virtual\product\12.2.0\dbhome_1
```
2. Copy the Oracle database template named **Oracle\_12.2.0.1\_Template\_for\_64\_bit\_WIN.dbt** from the Symantec DLP zip file into **C:\app\Administrator\virtual\product\12.2.0\dbhome\_1\assistants\dbca\templates**.
3. Ensure that the response file **Oracle\_12.2.0.1\_DBCA\_WIN.rsp** is located in the folder **C:\temp\Oracle\database\tools\responsefiles**.
4. Run the following command.  

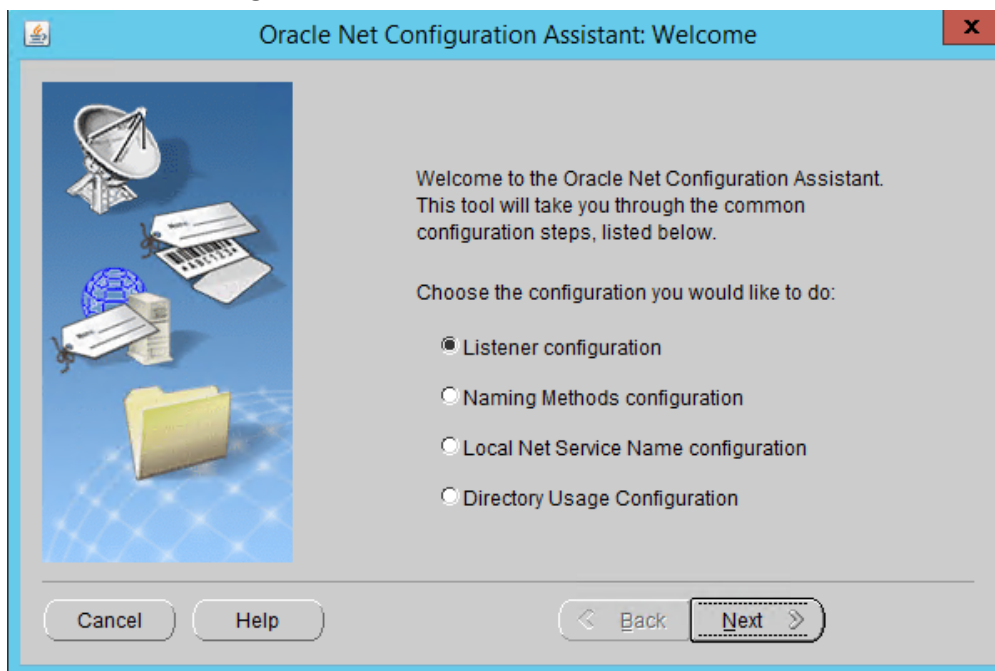
```
> %ORACLE_HOME%\bin\dbca -createDatabase -progressOnly -
responseFile
```

C:\temp\Oracle\database\tools\responsefiles\Oracle\_12.2.0.1\_DBCA\_WIN.rsp

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

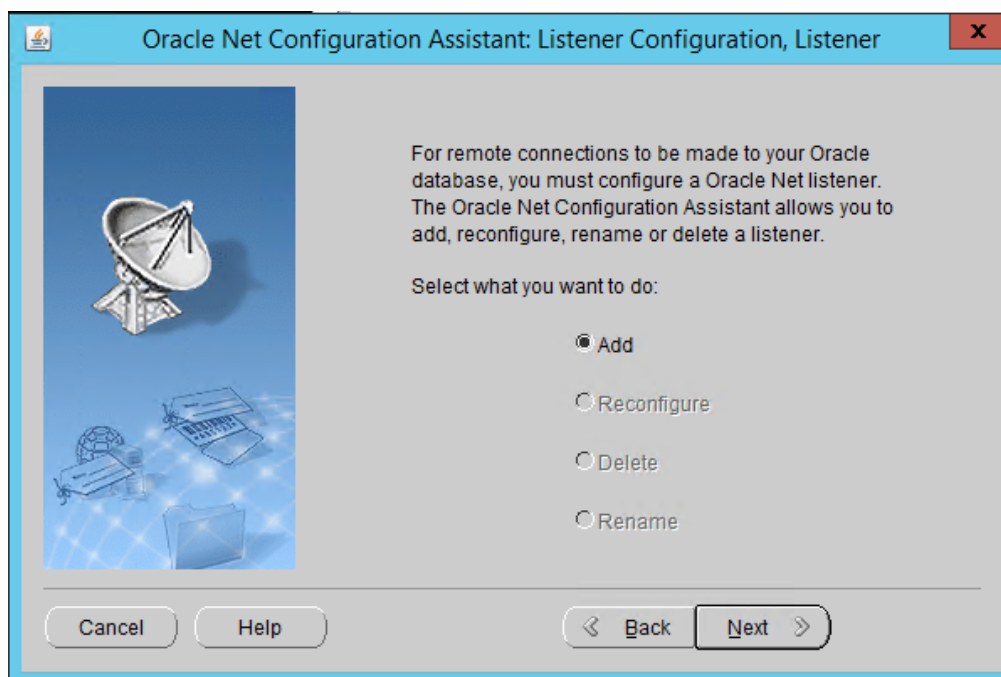
### 2.15.3 Configuring the Oracle Listener

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

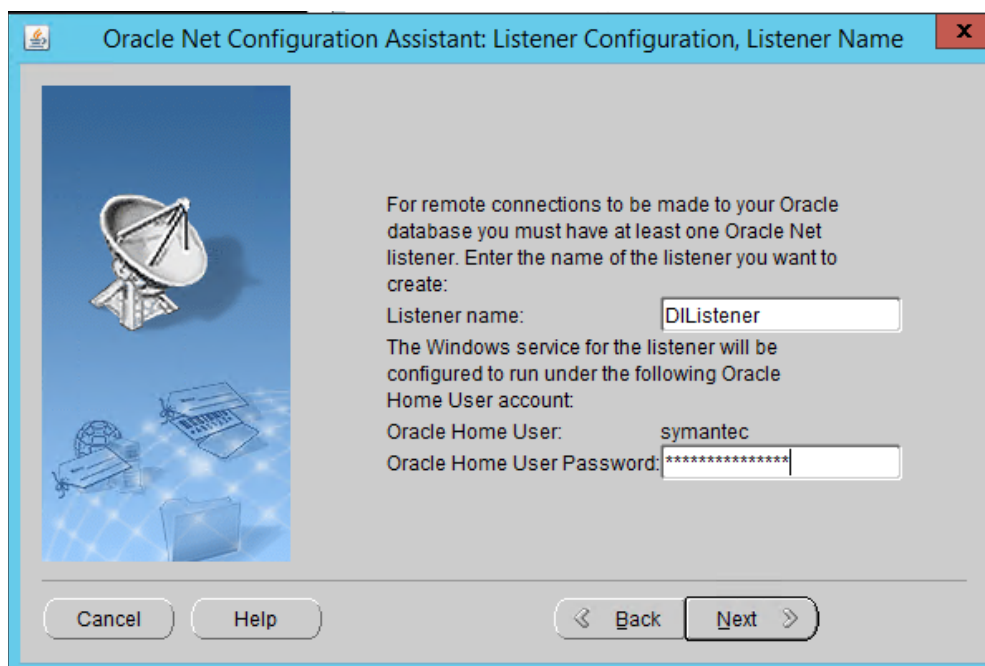


5. Click **Next**.
6. Select **Add**.





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

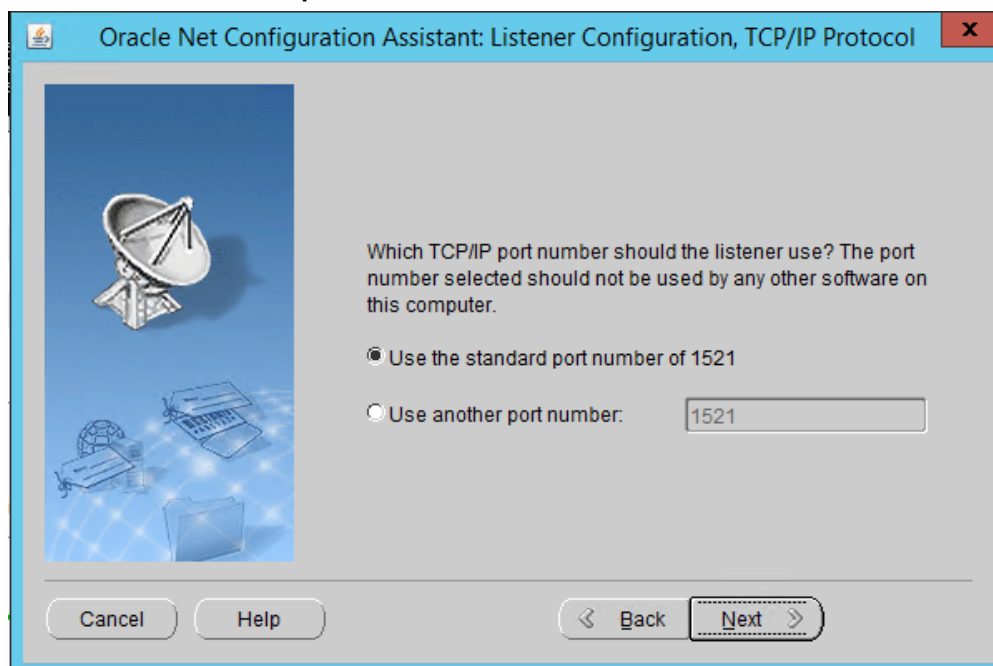


10. Click **Next**.

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

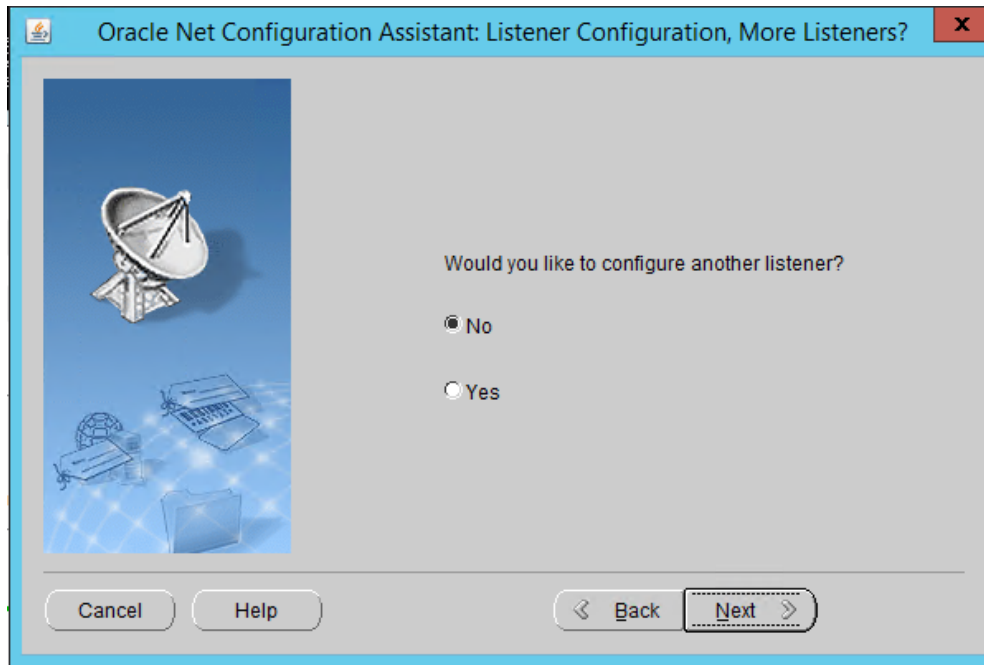


12. Click **Next**.
13. Select **Use the standard port number of 1521**.



14. Click **Next**.

15. Select **No**.

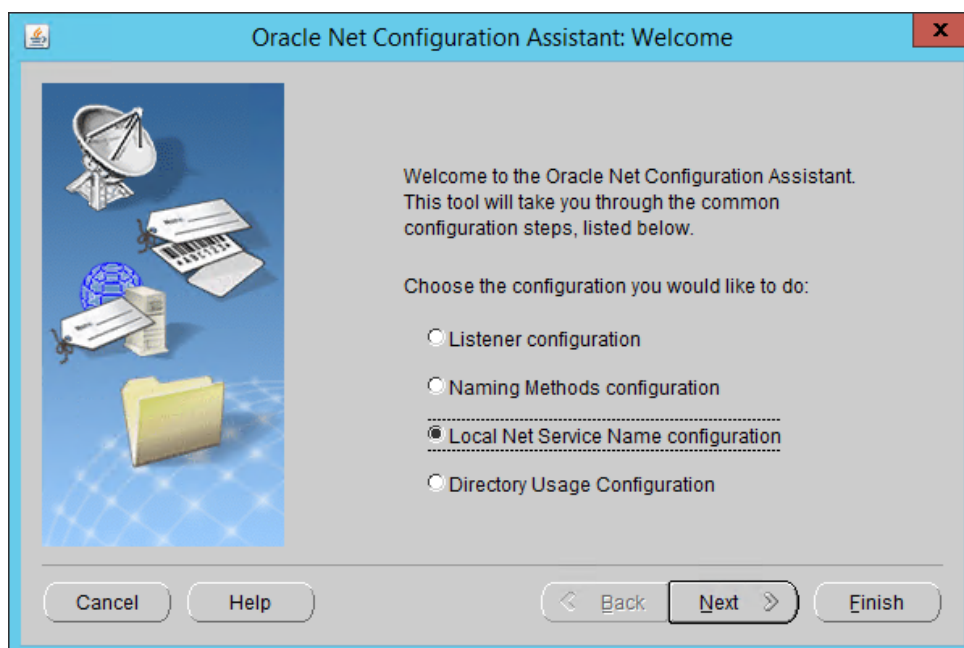


16. Click **Next**.



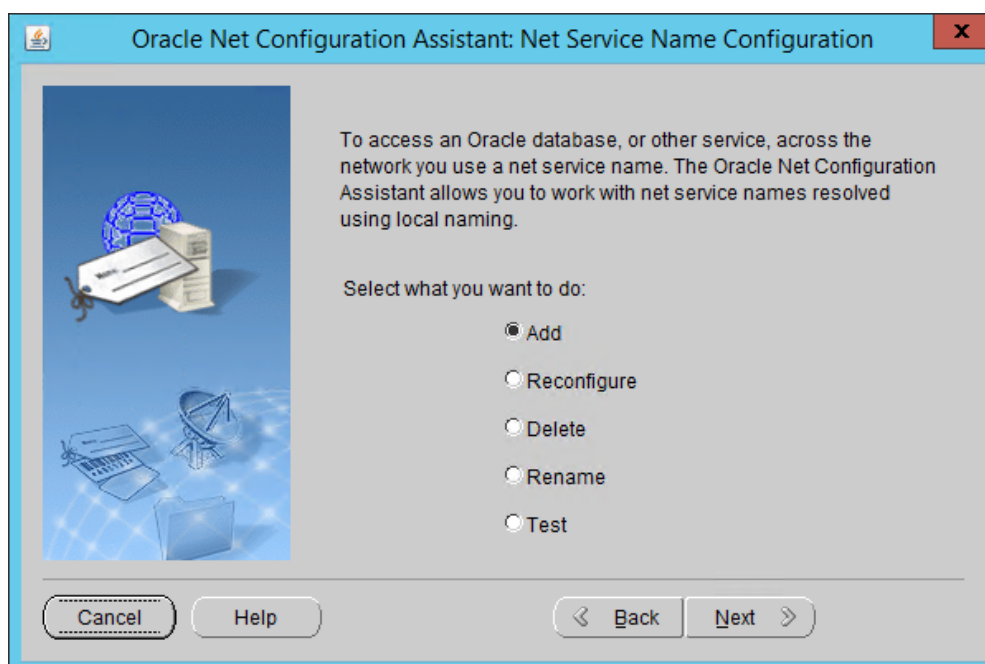
17. Click **Next**.

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



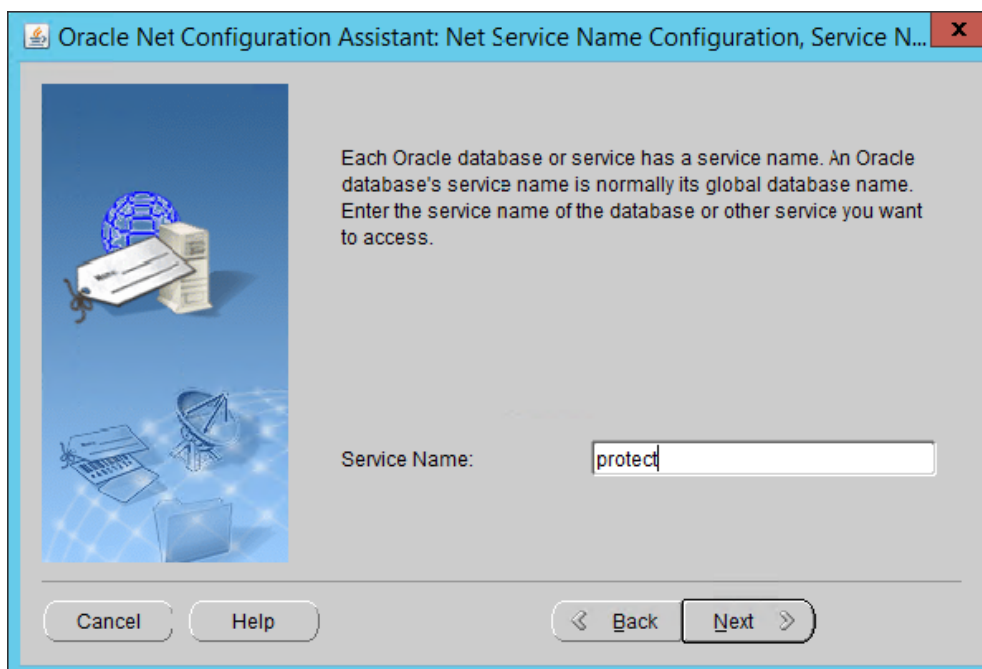
19. Click **Next**.

20. Select **Add**.



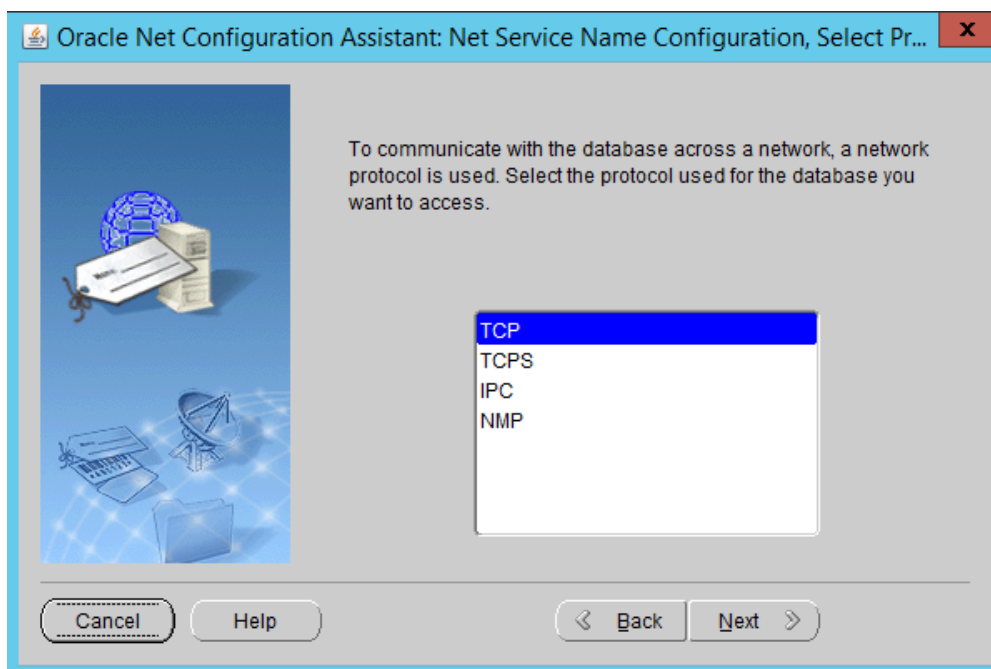
21. Click **Next**.

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



23. Click **Next**.

24. Select **TCP**.



25. Click **Next**.

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

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

Oracle Net Configuration Assistant: Net Service Name Configuration, TCP/IP Pr...

To communicate with the database using the TCP/IP protocol, the database computer's host name is required. Enter the host name for the computer where the database is located.

Host name:

A TCP/IP port number is also required. In most cases the standard port number should be used.

☒ Use the standard port number of 1521

☐ Use another port number:

Cancel Help < Back Next >

28. Click **Next**.

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

Oracle Net Configuration Assistant: Net Service Name Configuration, Test

You can verify that an Oracle database can be reached, using the information provided, by performing a connection test.

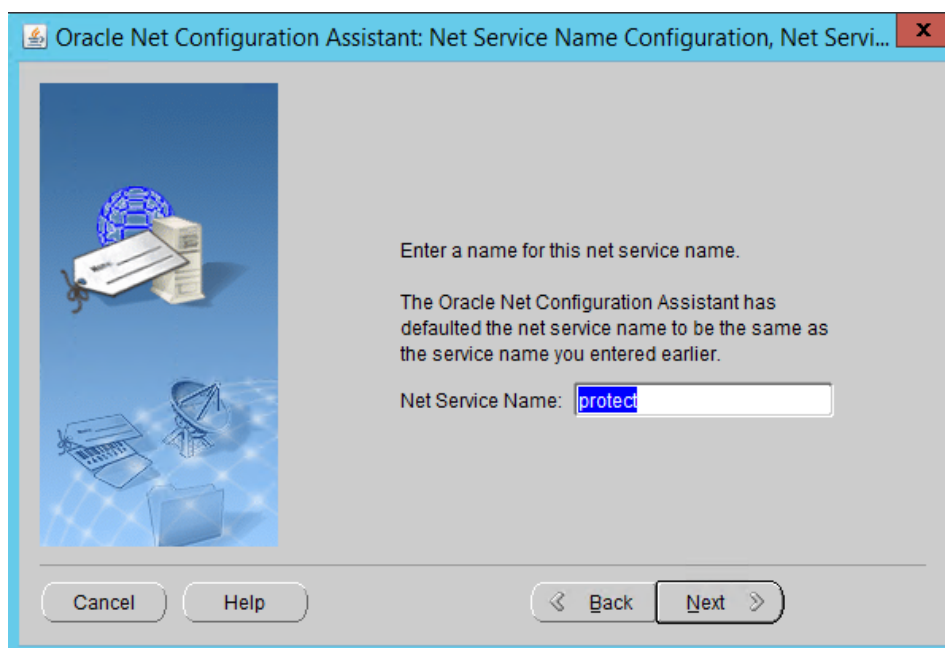
Would you like to test that a connection can be made to the database?

☒ No, do not test

☐ Yes, perform a test

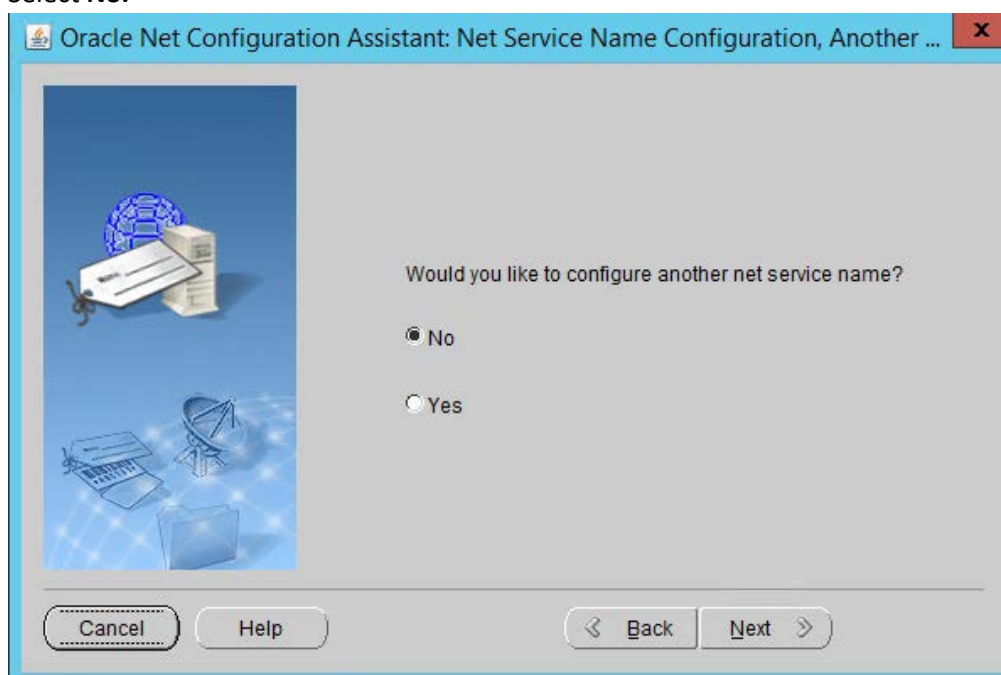
Cancel Help < Back Next >

30. Click **Next**.



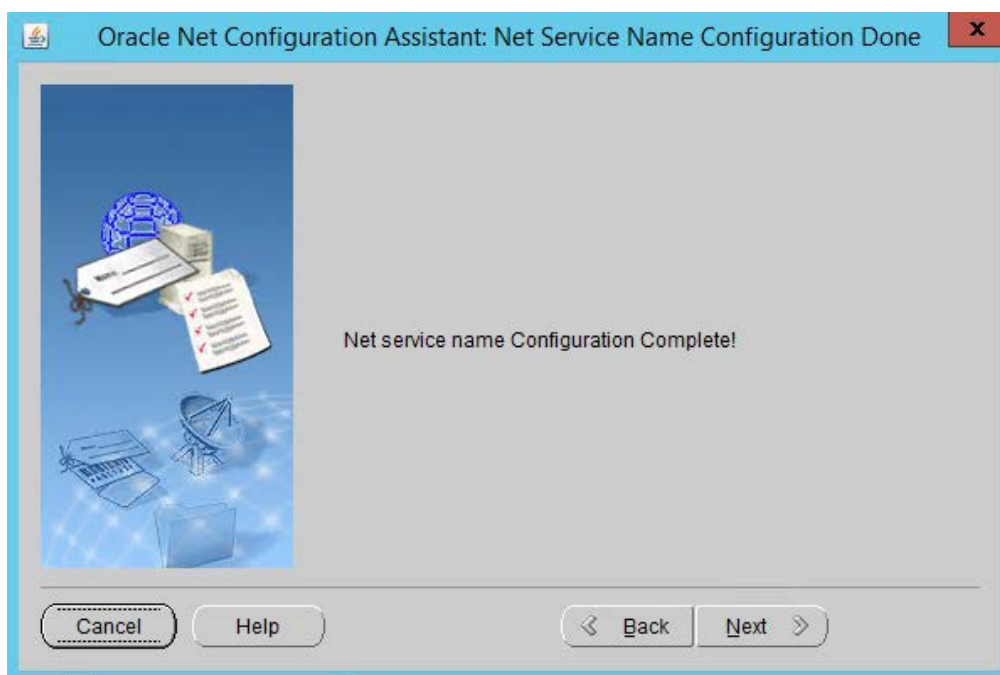
31. Click **Next**.

32. Select **No**.



33. Click **Next**.





34. Click **Next**.



35. Click **Finish**.

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



```
> lsnrctl stop
```

37. Open the file **%ORACLE\_HOME%\network\admin\listener.ora**.

38. Change (ADDRESS = (PROTOCOL = IPC)(KEY = <key\_value>)) to (ADDRESS = (PROTOCOL = IPC)(KEY = PROTECT)).

39. Add the line **SECURE\_REGISTER\_LISTENER=(IPC)** to the end of the file.



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

SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\app\Administrator\virtual\product\12.2.0\dbhome_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\app\Administrator\virtual\product\12.2.0\dbhome_1\bin\oracler12.dll")
)
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\app\Administrator\virtual\product\12.2.0\dbhome_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\app\Administrator\virtual\product\12.2.0\dbhome_1\bin\oracler12.dll")
)
)
DILISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = SYMANTEC-DLP.DE.IPDOR)(PORT = 1521))
(ADDRESS = (PROTOCOL = IPC)(KEY = PROTECT))
)
)
SECURE_REGISTER_LISTENER = (IPC) |
```

40. Save the file and exit the editor.

41. Ensure that OracleServicePROTECT and OracleVssWriterPROTECT services are running in Task Manager.

42. In an administrative command prompt, run the following command to start the listener. Replace dilistener with the name given to your listener.

```
> lsnrctl start dilistener
```

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

```
> sqlplus /nolog
```

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

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

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

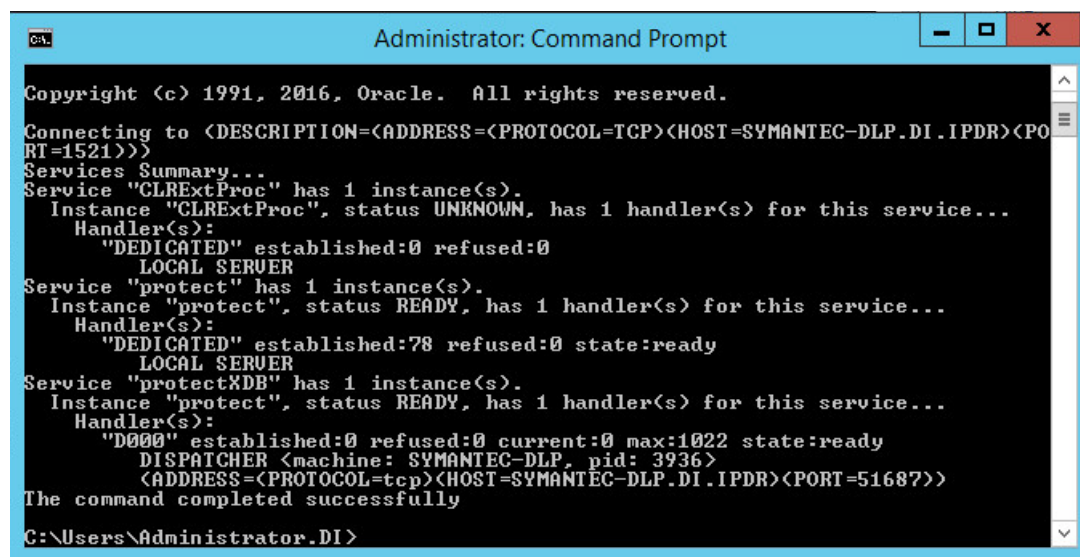
```
> ALTER SYSTEM SET local_listener = '(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=PROTECT)))' SCOPE=both;
```

```
> ALTER SYSTEM REGISTER;
```

```
> exit
```

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

```
> lsnrctl services
```



```
Administrator: Command Prompt

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

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=SYMANTEC-DLP.DI.IPDR)(PORT=1521)))
Services Summary...
Service "CLRExtProc" has 1 instance(s).
  Instance "CLRExtProc", status UNKNOWN, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:0 refused:0
      LOCAL SERVER
Service "protect" has 1 instance(s).
  Instance "protect", status READY, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:78 refused:0 state:ready
      LOCAL SERVER
Service "protectXDB" has 1 instance(s).
  Instance "protect", status READY, has 1 handler(s) for this service...
    Handler(s):
      "D0000" established:0 refused:0 current:0 max:1022 state:ready
      DISPATCHER (machine: SYMANTEC-DLP, pid: 3936)
      (ADDRESS=(PROTOCOL=tcp)(HOST=SYMANTEC-DLP.DI.IPDR)(PORT=51687))
The command completed successfully

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

46. Open a new administrative command window.

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

48. Run the following command:

```
> sqlplus /nolog
```

```
> @oracle_create_user.sql
```

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

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

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

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

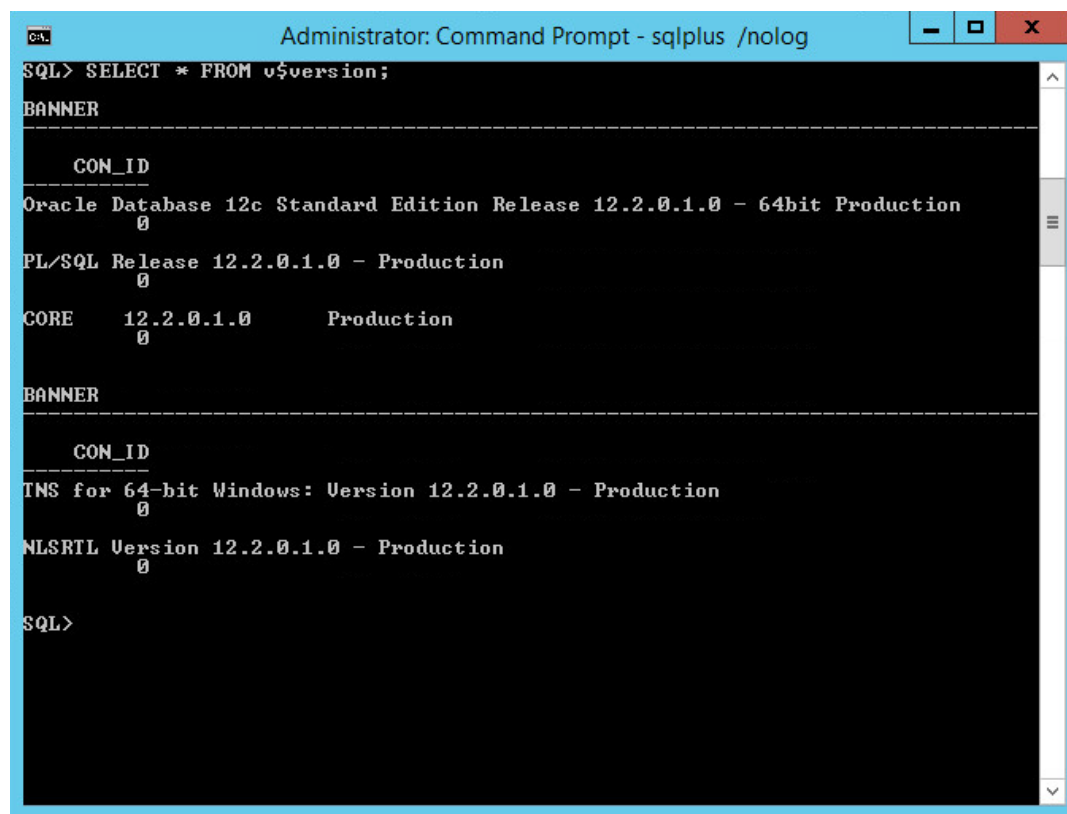
```
> sqlplus /nolog
```

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

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

55. Verify the version information with the following command.

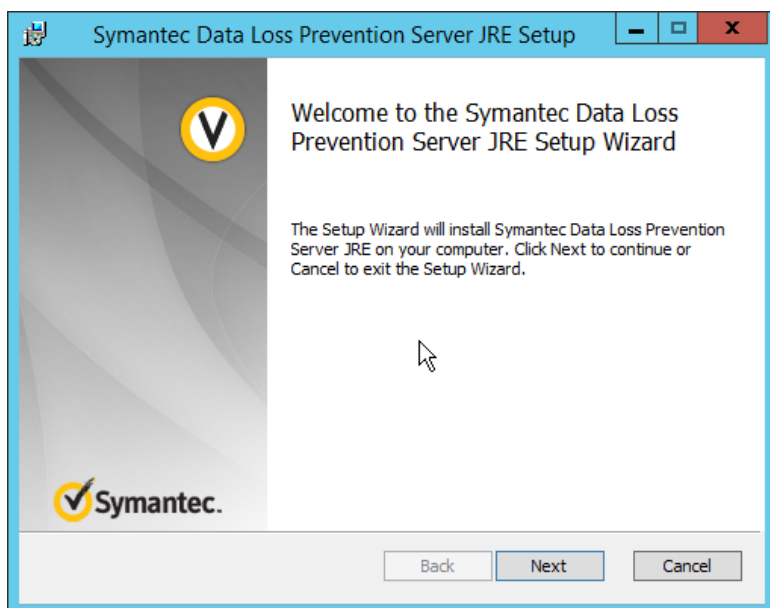
```
> SELECT * FROM v$version;
```



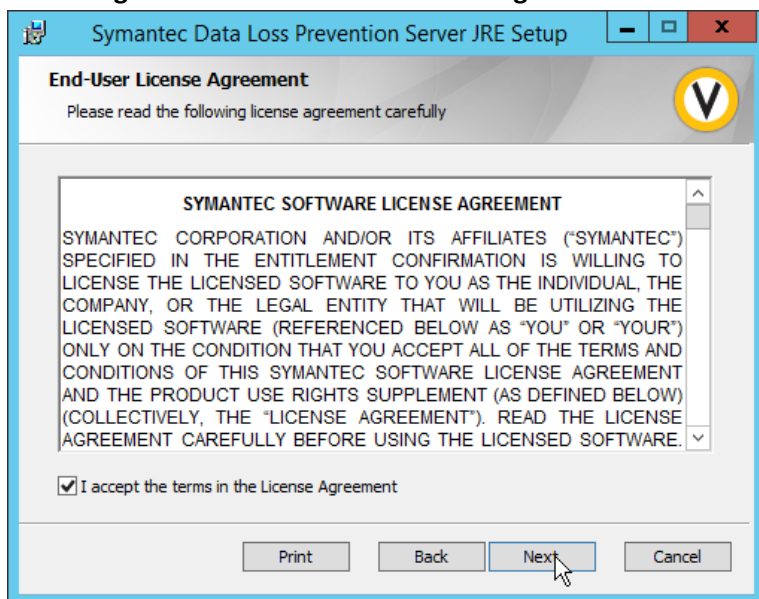
```
Administrator: Command Prompt - sqlplus /nolog
SQL> SELECT * FROM v$version;
BANNER
-----
      CON_ID
-----
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production
      0
PL/SQL Release 12.2.0.1.0 - Production
      0
CORE      12.2.0.1.0      Production
      0
BANNER
-----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

## 2.15.4 Install Symantec DLP

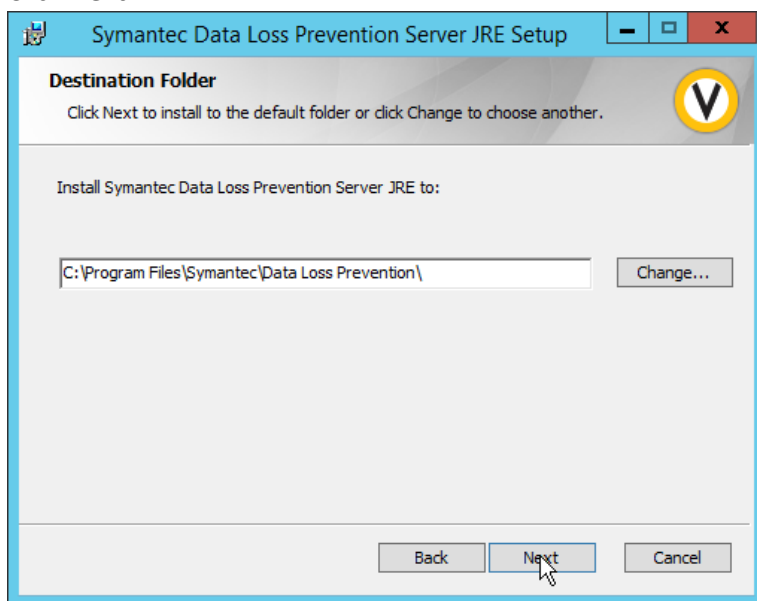
1. In the folder **DLP Installs\DLP 15.1\Symantec\_DLP\_15.1\_Platform\_Win-IN\_15.1.0.25021\DLP\15.1\New\_Installs\x64\Release**, located in the download folder for the DLP files, run **ServerJRE.msi**.



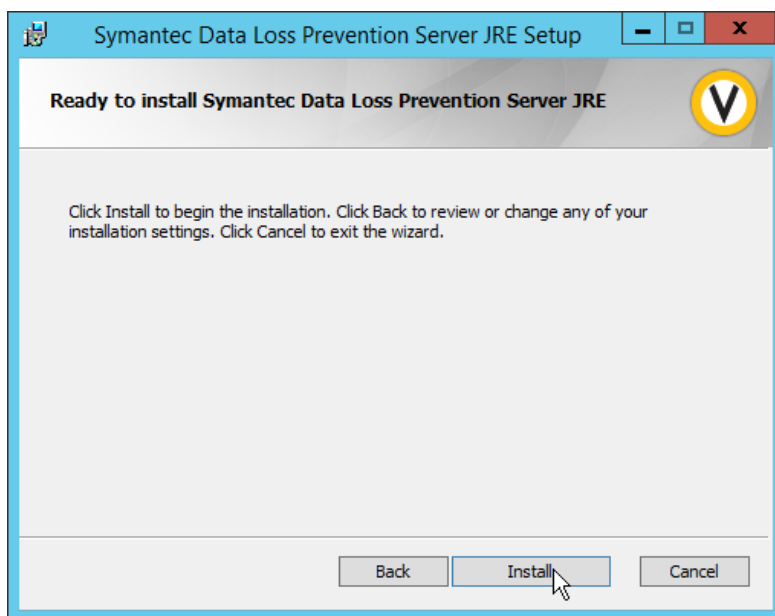
2. Click **Next**.
3. Select **I agree to the terms in the license agreement**.



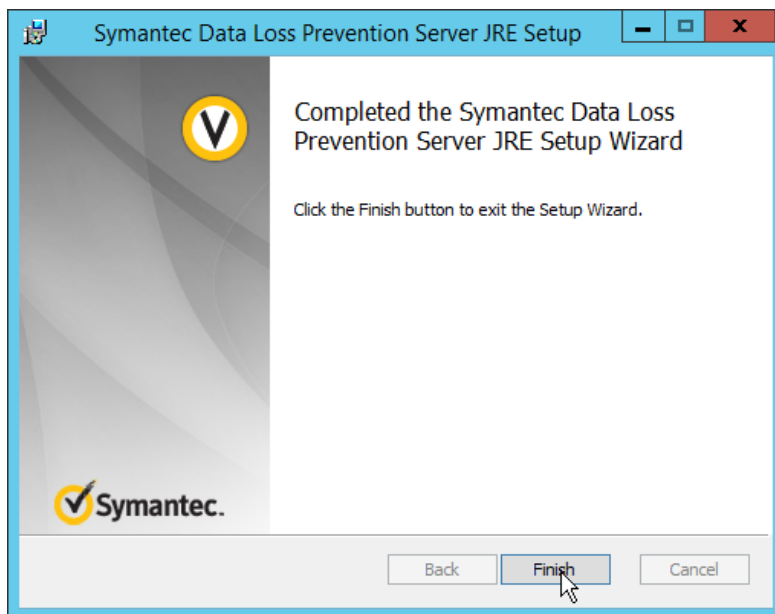
4. Click **Next**.



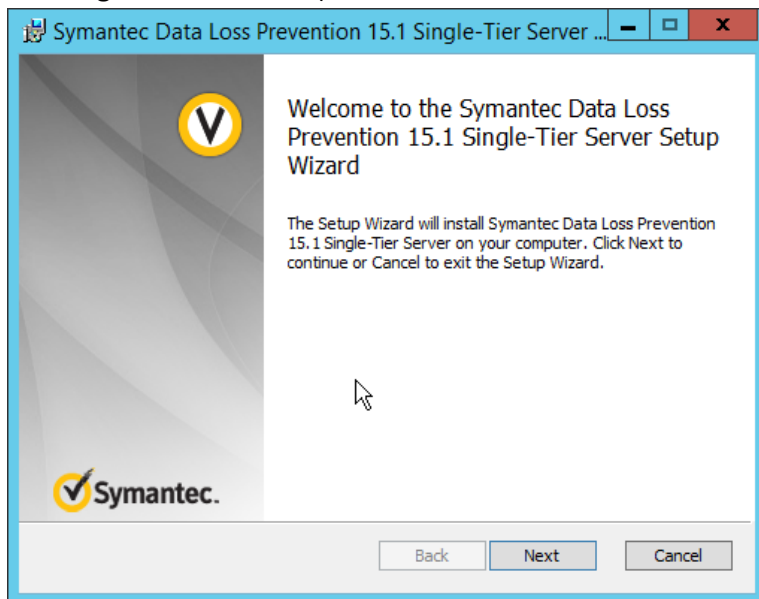
5. Click **Next**.



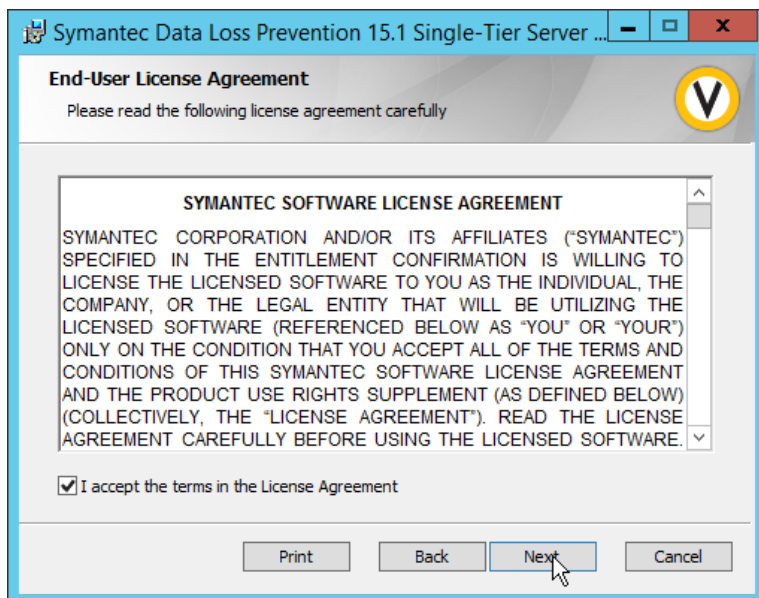
6. Click **Install**.



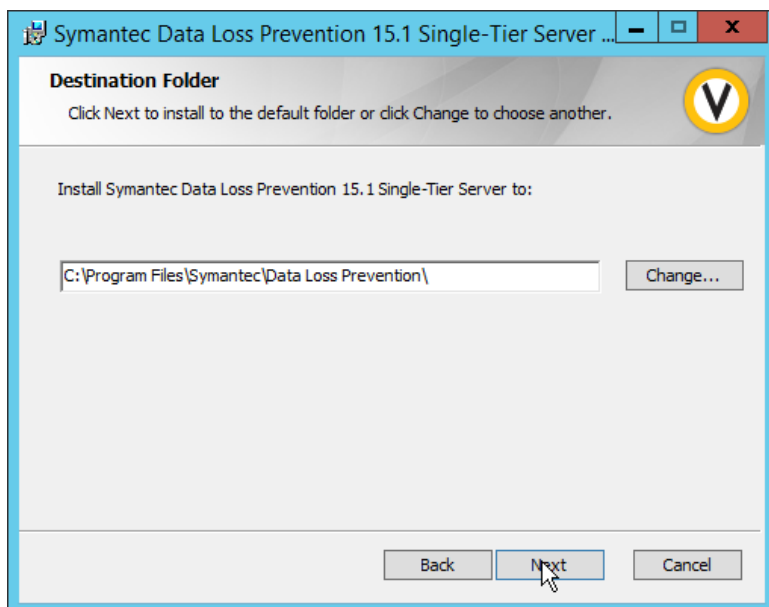
7. Click **Finish**.
8. Run **SingleTierServer.msi** (located in the same folder as **ServerJRE.msi**).



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

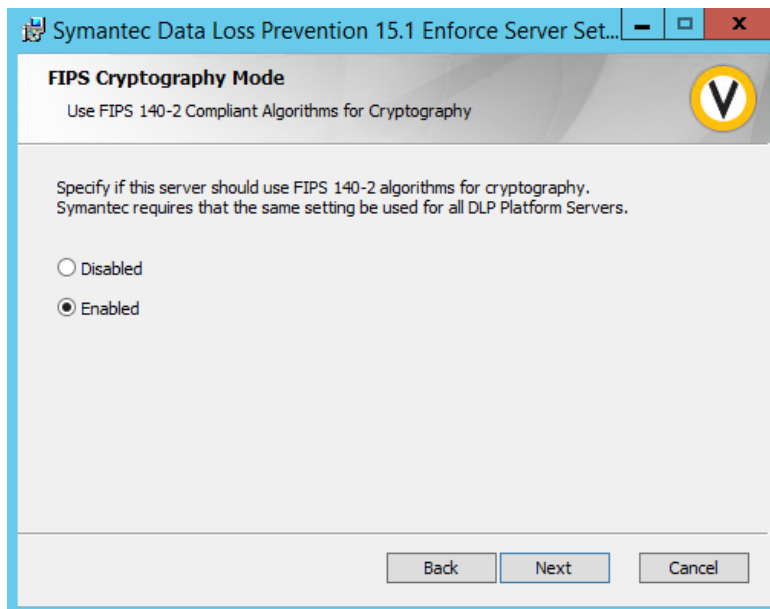


11. Click **Next**.

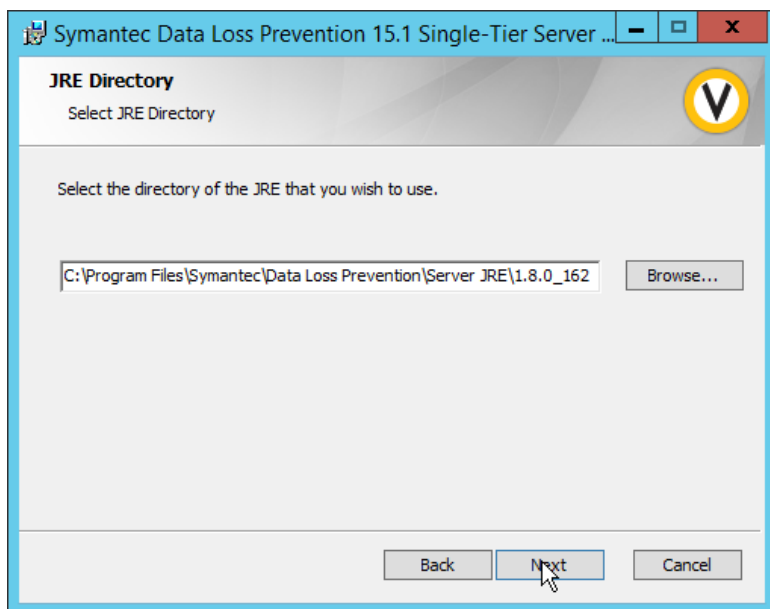


12. Click **Next**.

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



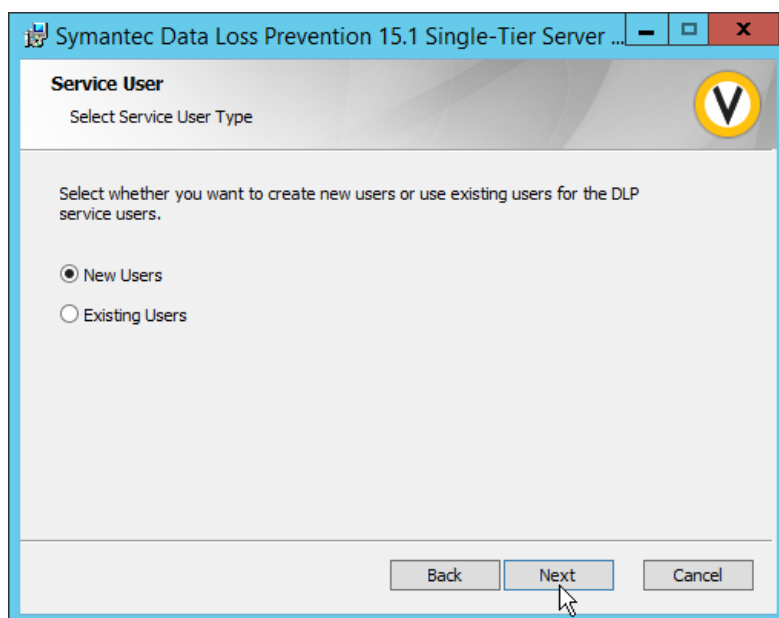
14. Click **Next**.



15. Click **Next**.

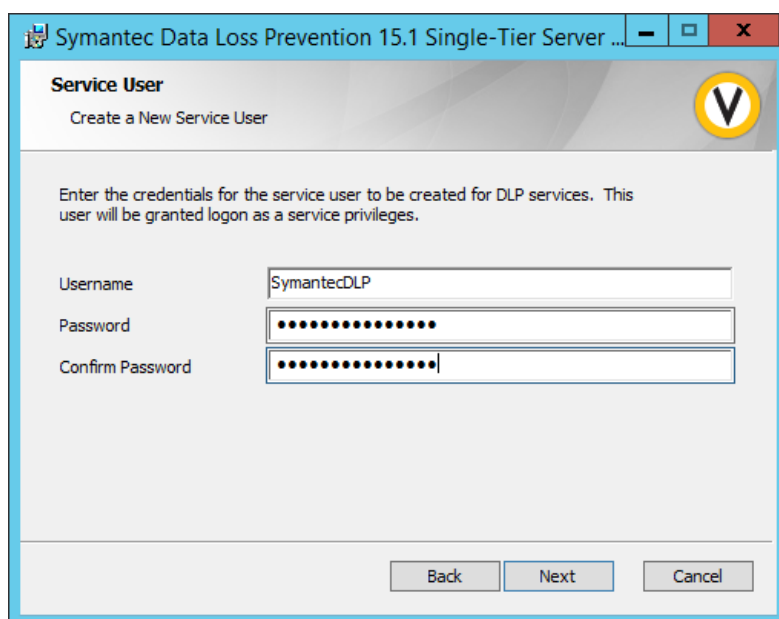
16. Click on **New Users**.





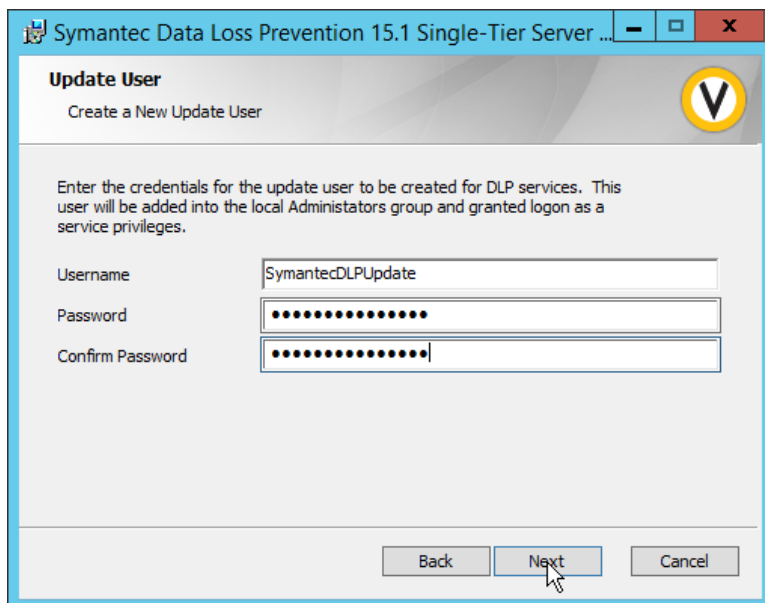
17. Click **Next**.

18. Enter a **password** and optionally a **username**.



19. Click **Next**.

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



**Symantec Data Loss Prevention 15.1 Single-Tier Server ...**

**Update User**  
Create a New Update User

Enter the credentials for the update user to be created for DLP services. This user will be added into the local Administrators group and granted logon as a service privileges.

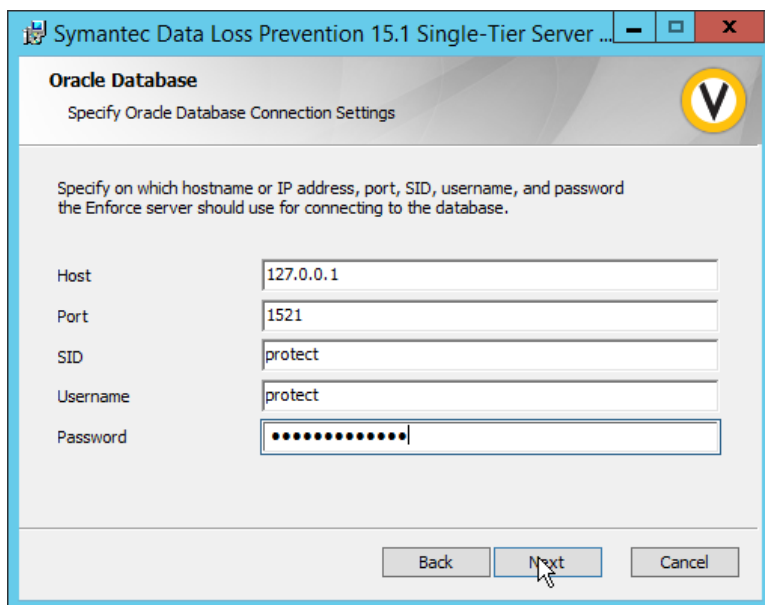
Username: SymantecDLPUpdate

Password: [masked]

Confirm Password: [masked]

Back Next Cancel

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



**Symantec Data Loss Prevention 15.1 Single-Tier Server ...**

**Oracle Database**  
Specify Oracle Database Connection Settings

Specify on which hostname or IP address, port, SID, username, and password the Enforce server should use for connecting to the database.

Host: 127.0.0.1

Port: 1521

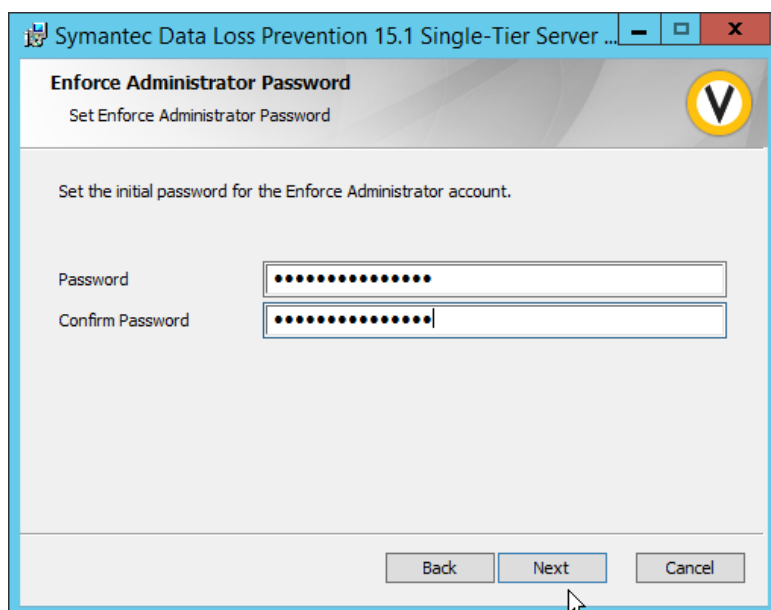
SID: protect

Username: protect

Password: [masked]

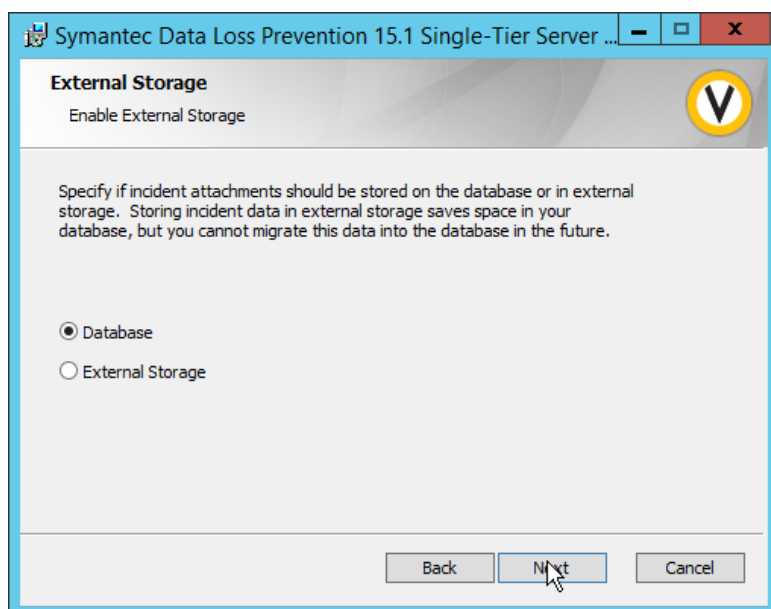
Back Next Cancel

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



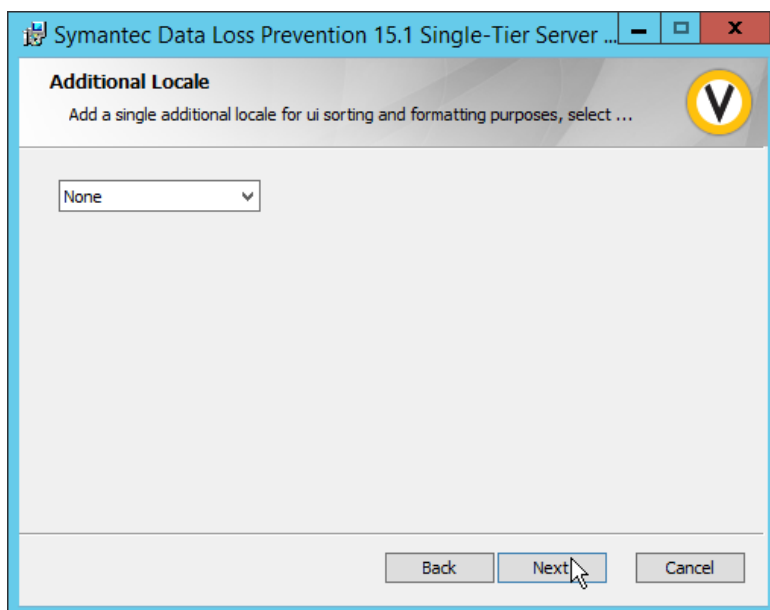
27. Click **Next**.

28. Select **Database**.

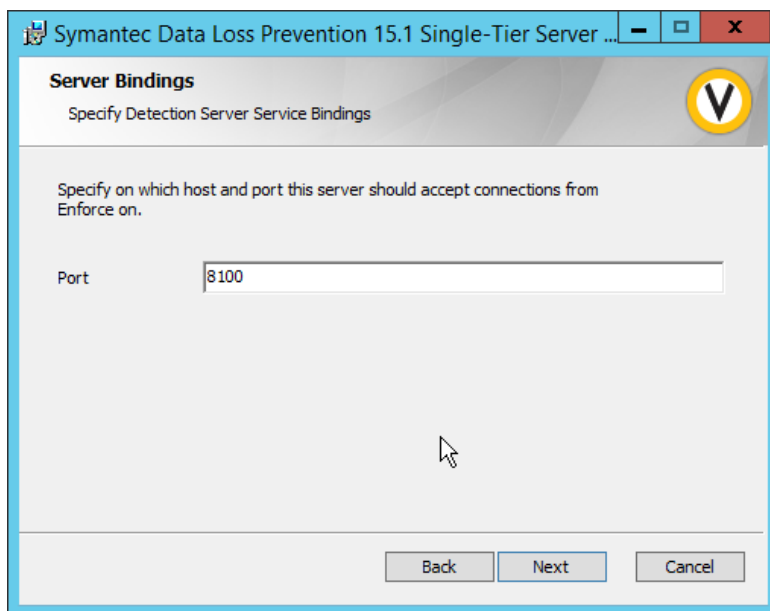


29. Click **Next**.

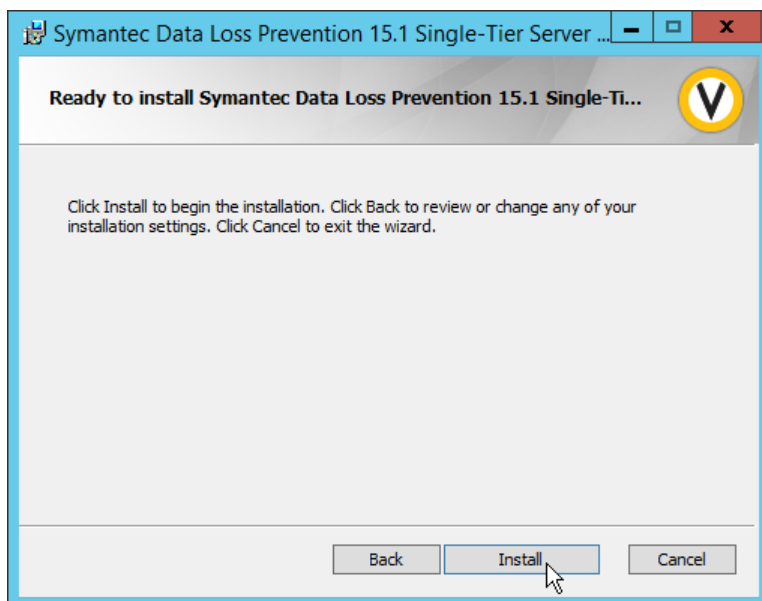
30. Select **None**.



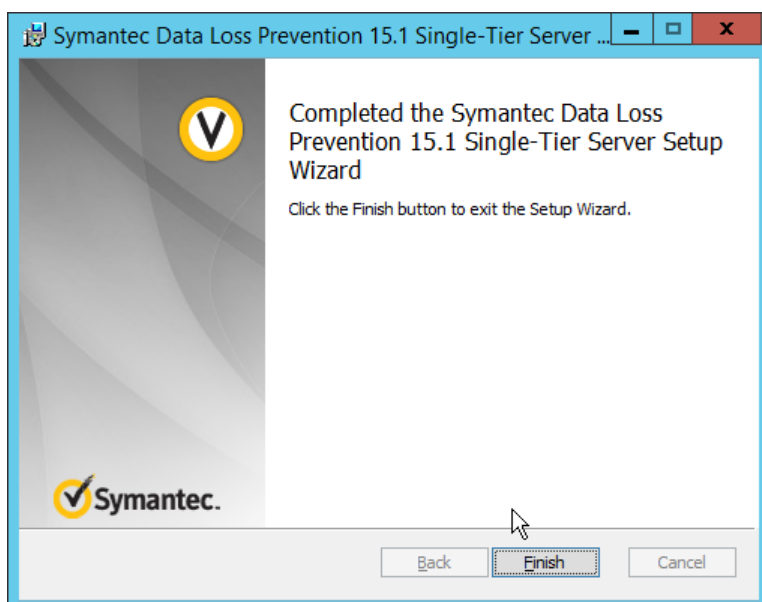
31. Click **Next**.



32. Click **Next**.



33. Click **Install**.



34. Click **Finish**.

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

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

d. SymantecDLPDetectionServer

## 2.15.5 Configure Symantec DLP

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

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

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

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

### Process Control

Advanced Process Control



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

## 2.16 Cisco Identity Services Engine

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

### 2.16.1 Initial Setup

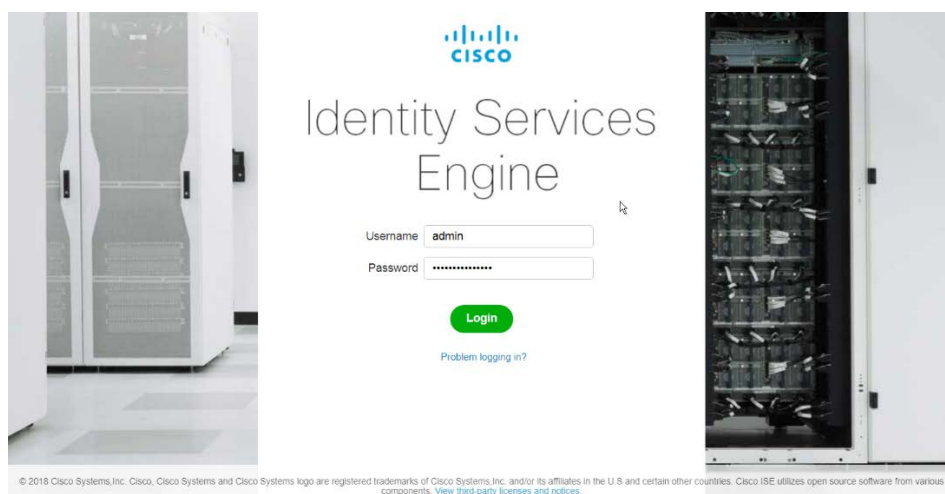
1. When prompted to log in for the first time, enter `setup`. (You can use the command `reset-config` to change these values later.)
2. Enter the desired **hostname** for the machine.
3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated with this IP address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

### 2.16.2 Inventory: Configure SNMP on Routers/Network Devices

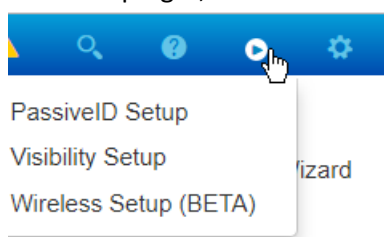
See the corresponding vendor documentation for the correct way to enable Simple Network Management Protocol (SNMP) on your network device. Ensure that the community string you choose is considered sensitive, like a password.

### 2.16.3 Inventory: Configure Device Detection

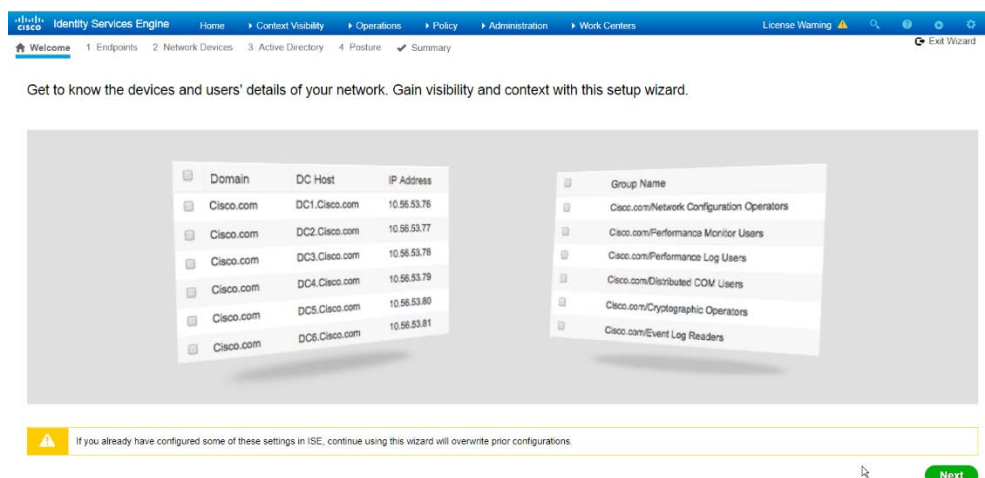
1. Log in to the web client by visiting `https://hostname/admin` but replace **hostname** with the hostname of the ISE machine.



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



3. Click **Next**.



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



Endpoints Discovery

We are going to discover the endpoints using the IP range(s) below.

IP Address Range \* 192.168.0.0/16  
e.g. 10.10.10.0/24

Active Scanning ☒

Add another range

Skip Back 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.

Add Network Device

Name \* GATEWAYROUTER

IP Address \* 192.168.1.1

Location

Device Type

Description

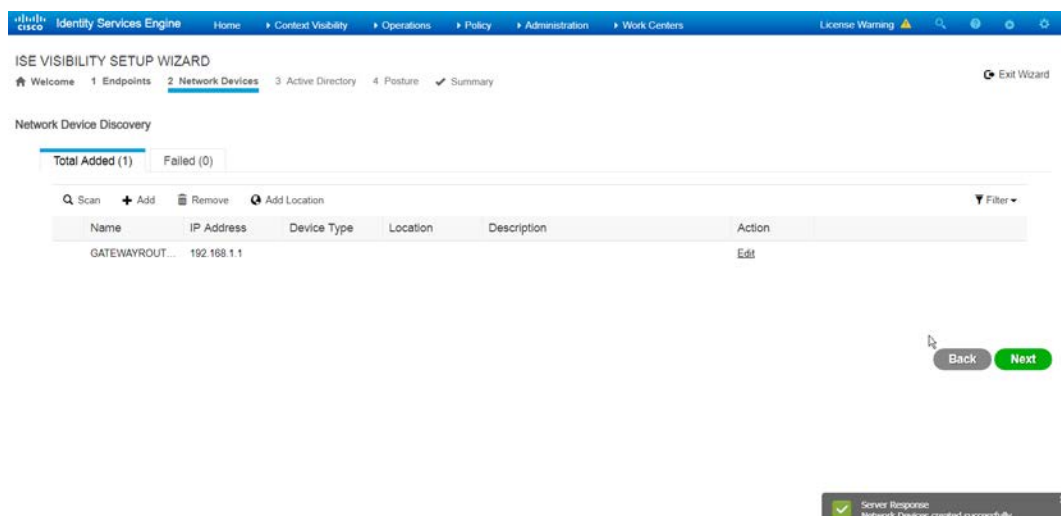
SNMP Settings

SNMP Version \* 1

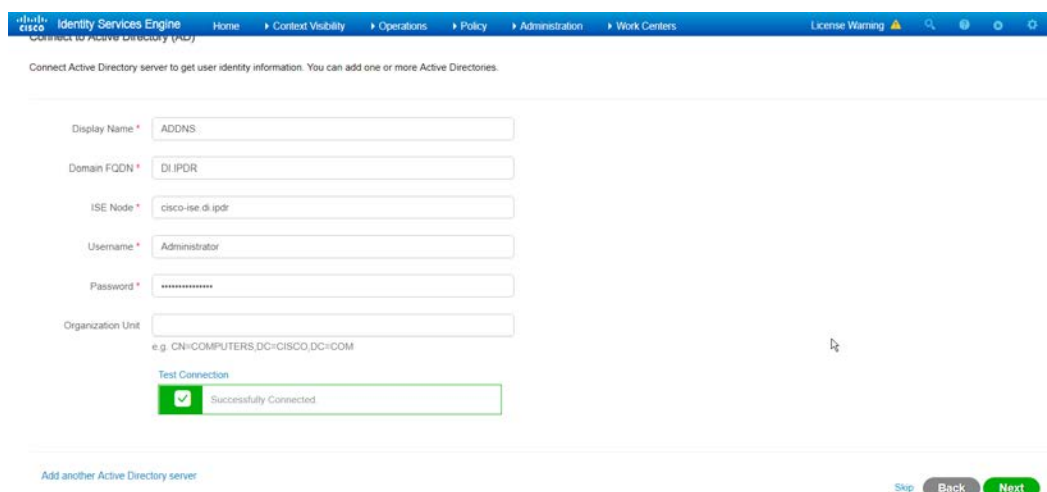
RO Community \* \*\*\*\*\* Show

Cancel OK

12. Click **OK**.



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



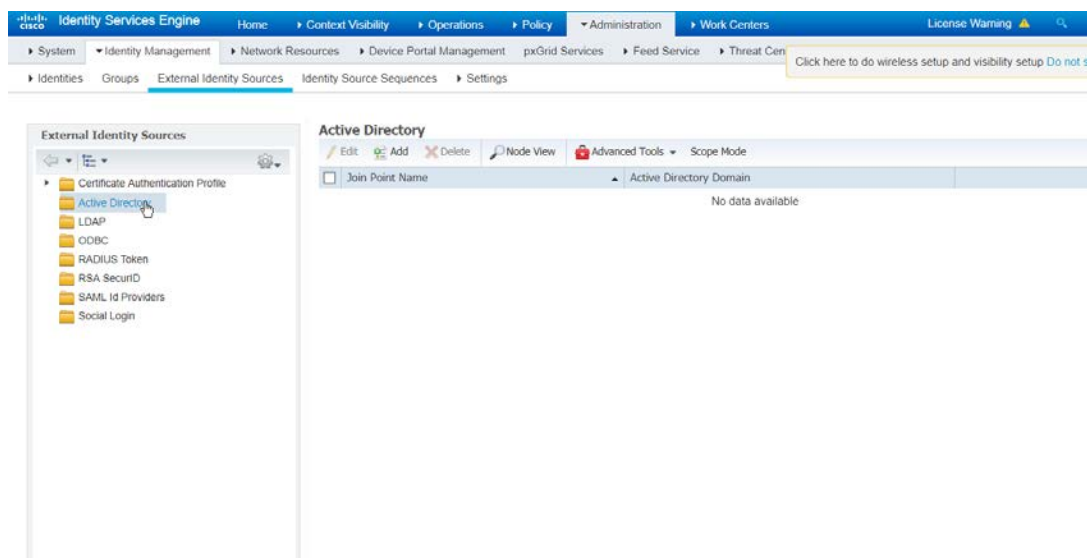
19. Click **Next**.
20. Enter a **username** and **password**.
21. Check the box next to **Enable Endpoint Logging**.
22. Check the box next to **Include Range**.

### 23. Click **Next**.

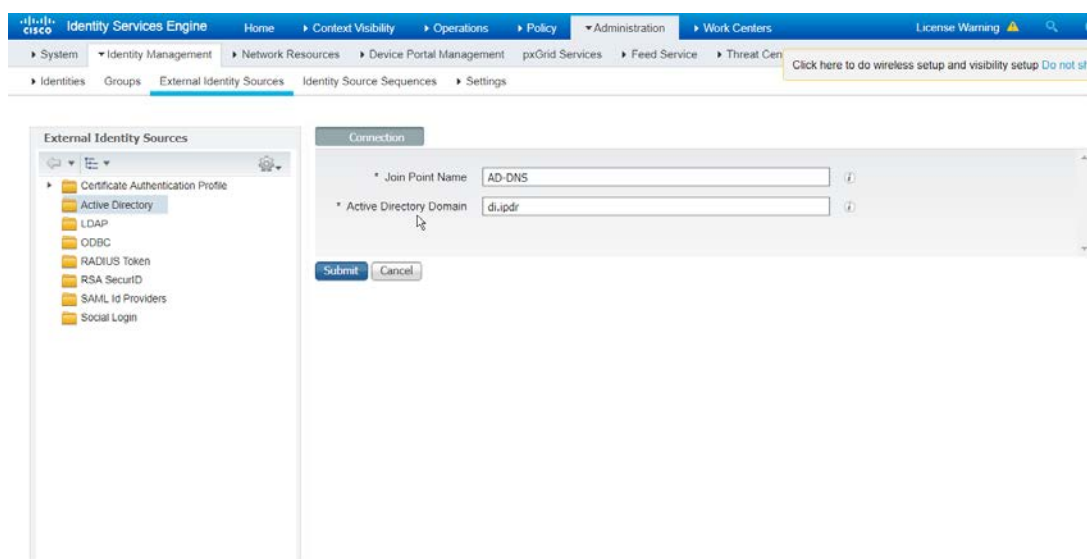
24. Verify the settings and click **Done**. (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

## 2.16.4 Policy Enforcement: Configure Active Directory Integration

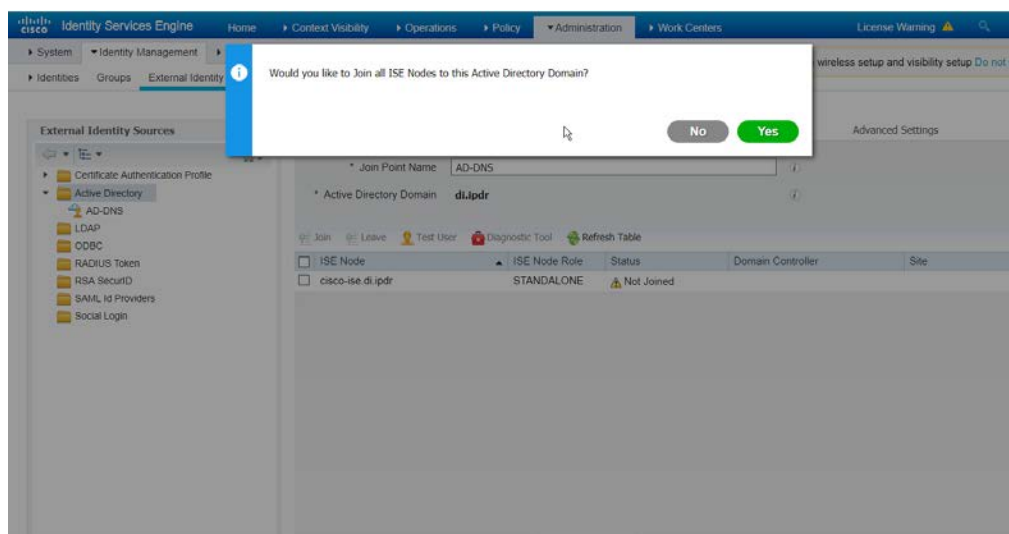
1. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.



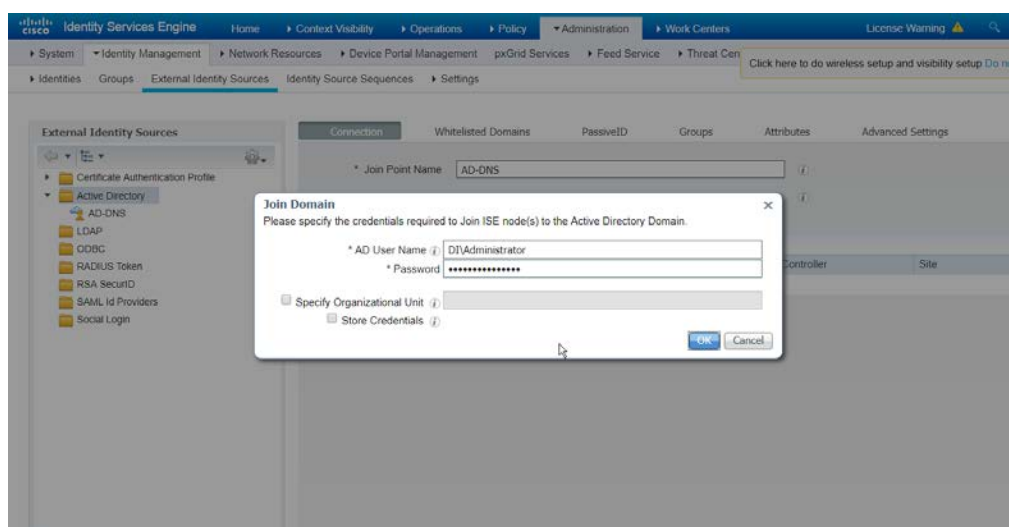
2. Click **Add**.
3. Enter a **name**.
4. Enter the **domain**.



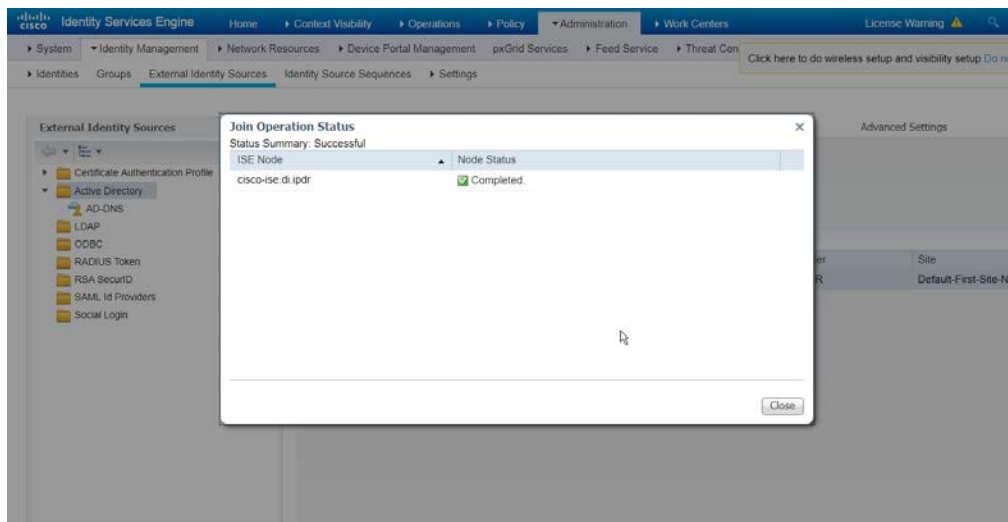
5. Click **Submit**.



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



8. Click **OK**.

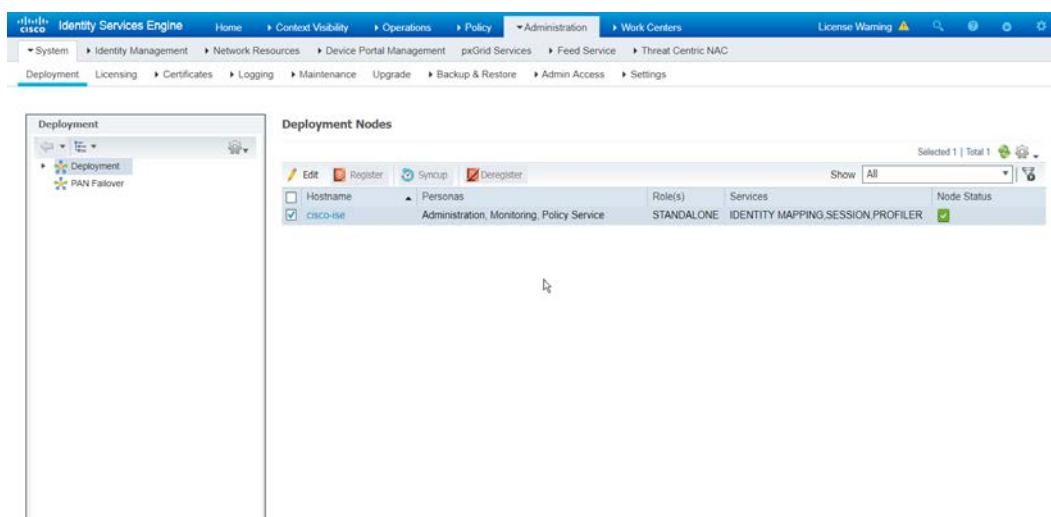


9. Click **Close** when the join is finished.

## 2.16.5 Policy Enforcement: Enable Passive Identity with AD

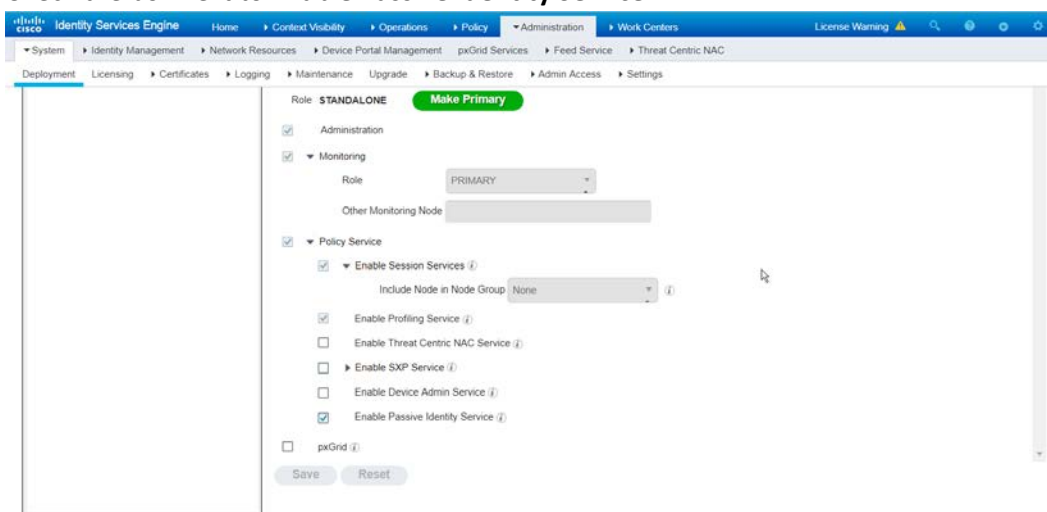
This configuration allows users to use Active Directory usernames/passwords as authentication for the portal. The web portal will allow clients to download profiling software to ensure that clients have up to date software and can be trusted on the network.

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

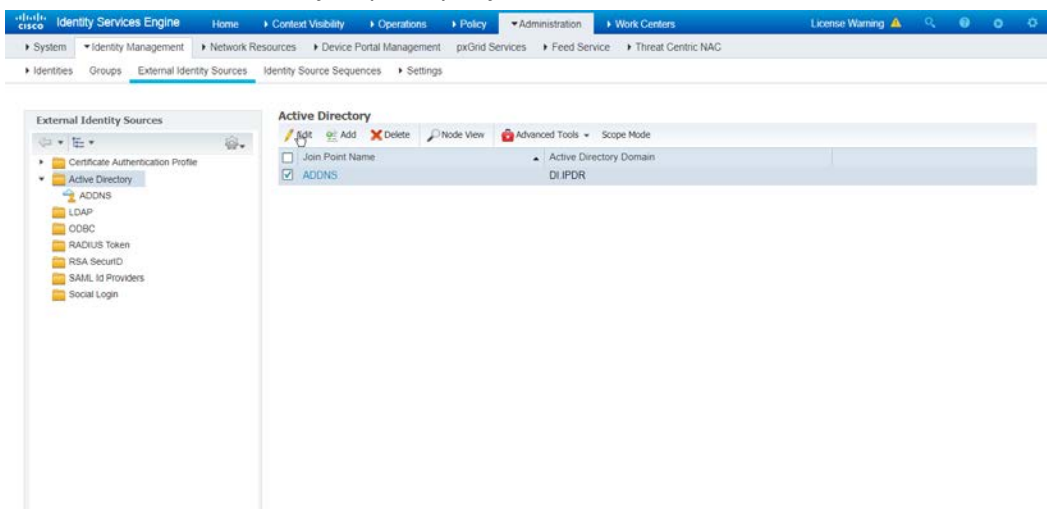


3. Click **Edit**.

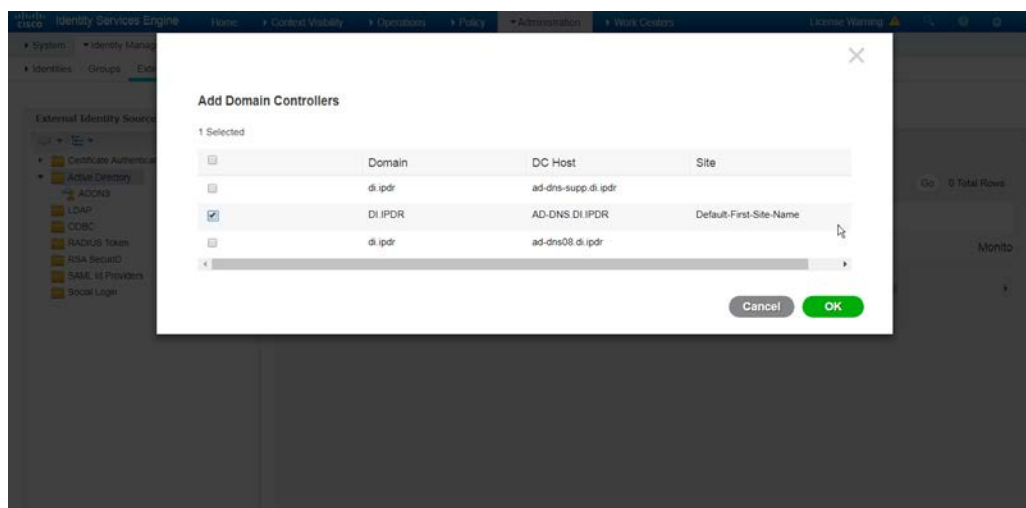
4. Check the box next to **Enable Passive Identity Service**.



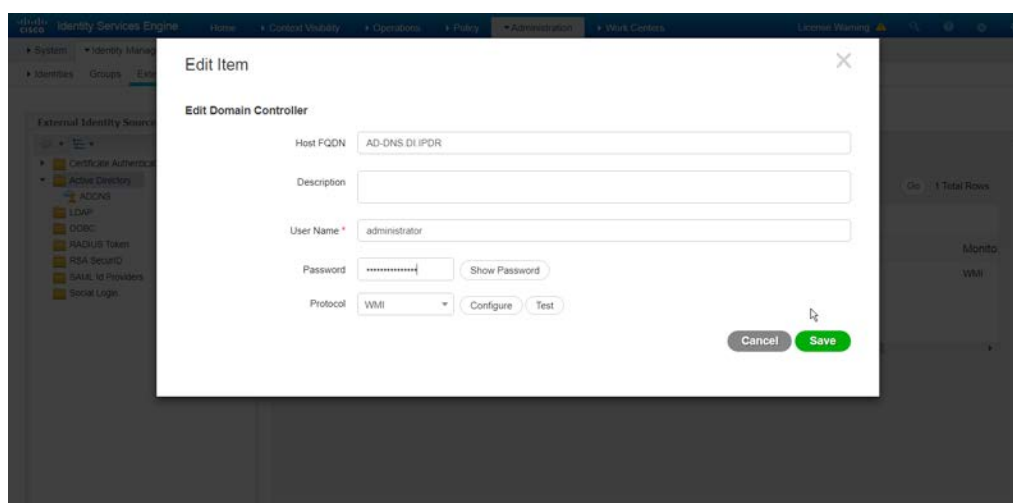
5. Click **Save**.
6. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.
7. Click the name of the Active Directory machine.
8. Check the box next to the join point you just created.



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

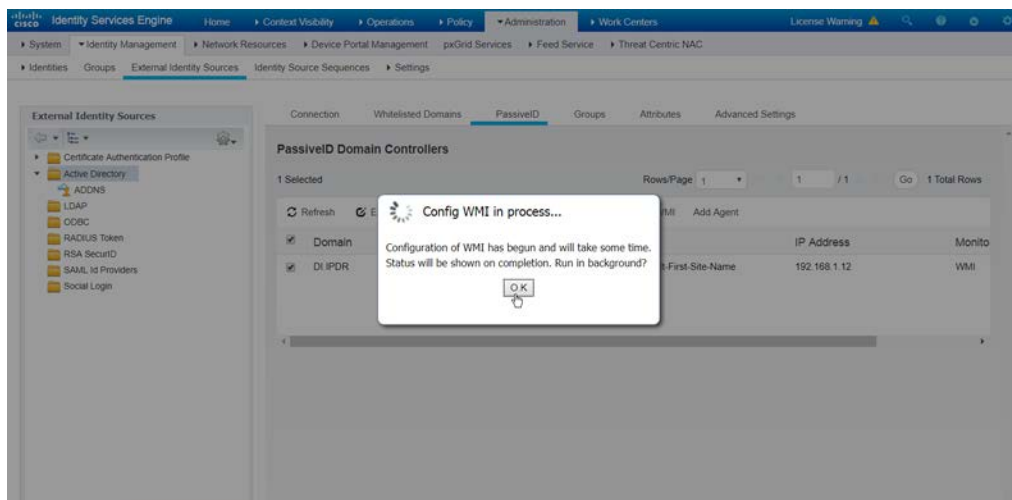


12. Select the Active Directory domain controller.
13. Click **OK**.
14. Check the box next to the selected domain controller.
15. Click **Edit**.
16. Enter credentials for an administrator account.

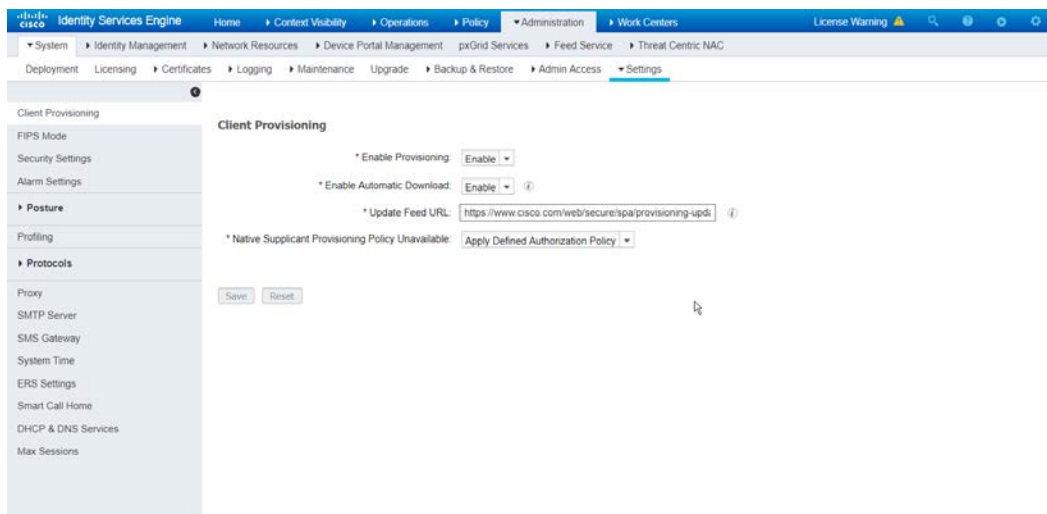


17. Click **Save**.
18. Click **Config WMI**.
19. Click **OK**.

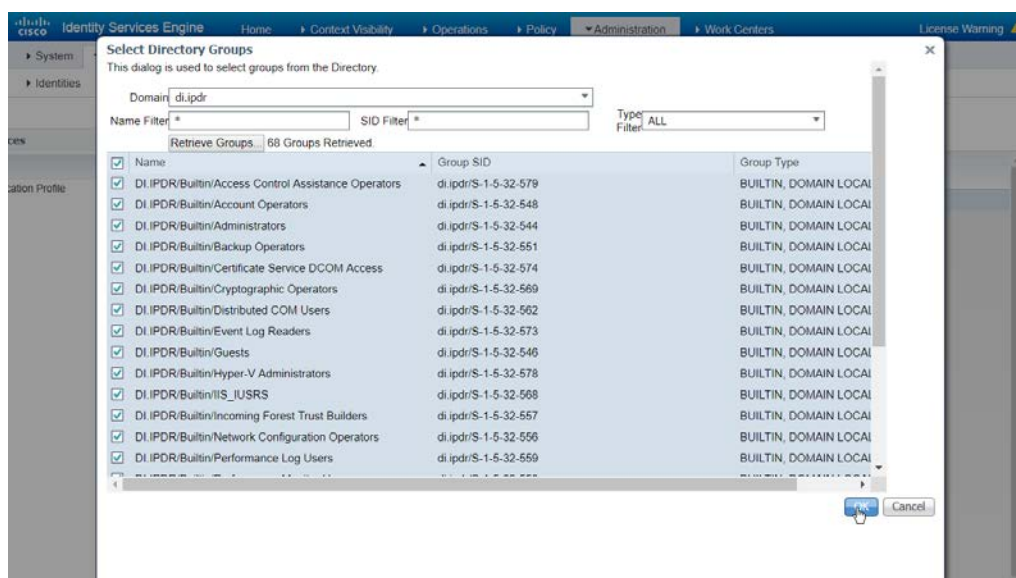




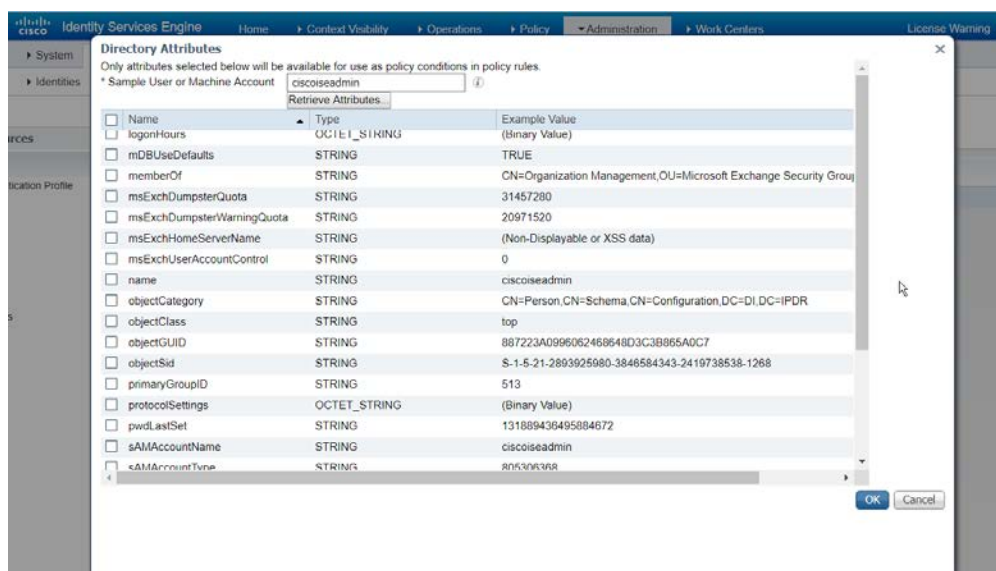
20. Click **OK** when this configuration finishes.
21. Navigate to **Administration > System > Settings > Client Provisioning**.
22. Set **Enable Automatic Download** to **Enable**.



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



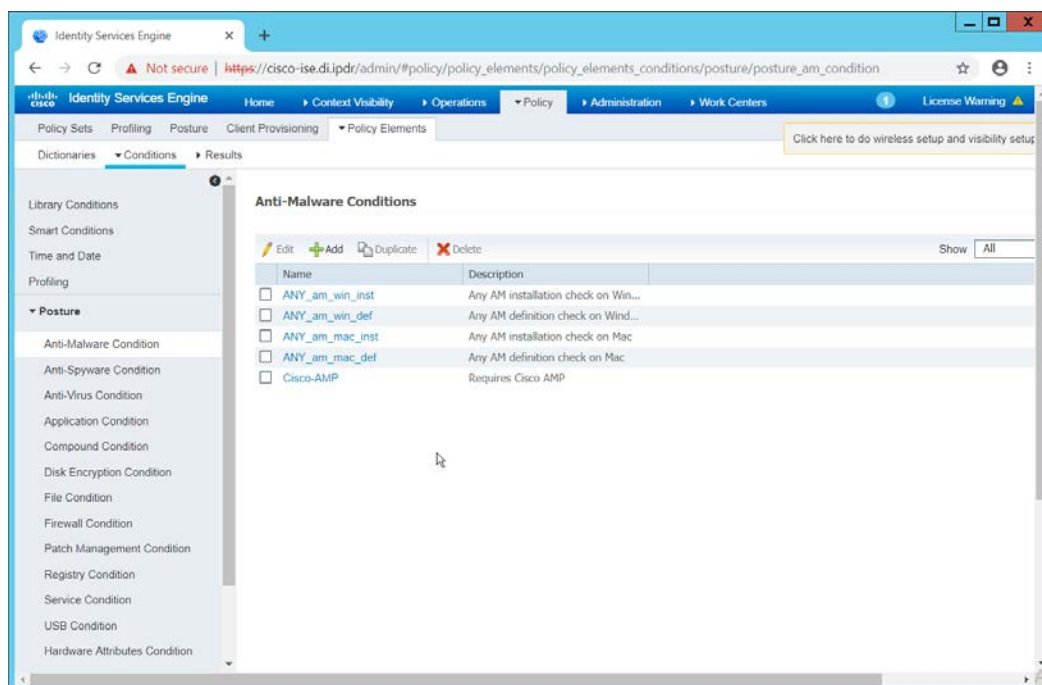
29. Click **OK**. (If you add more groups to Active Directory they can be imported in the same way in the future.)
30. Click the **Attributes** tab.
31. Click **Add > Select Attributes from Directory**.
32. Enter a **username**.
33. Click **Retrieve Attributes**. (This will populate the window with Active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



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

## 2.16.6 Policy Enforcement: Developing Policy Conditions

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



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

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Policy > Policy Elements > Results > Posture > Anti-Malware Condition. The page title is 'Anti-Malware Condition List > New Anti-Malware Condition'. The form fields are as follows:

- Name: CiscoAMP
- Description: Check for cisco AMP
- Compliance Module: 4.x or later
- Operating System: Windows All
- Vendor: Cisco Systems, Inc.
- Check Type: ☒ Installation ☐ Definition

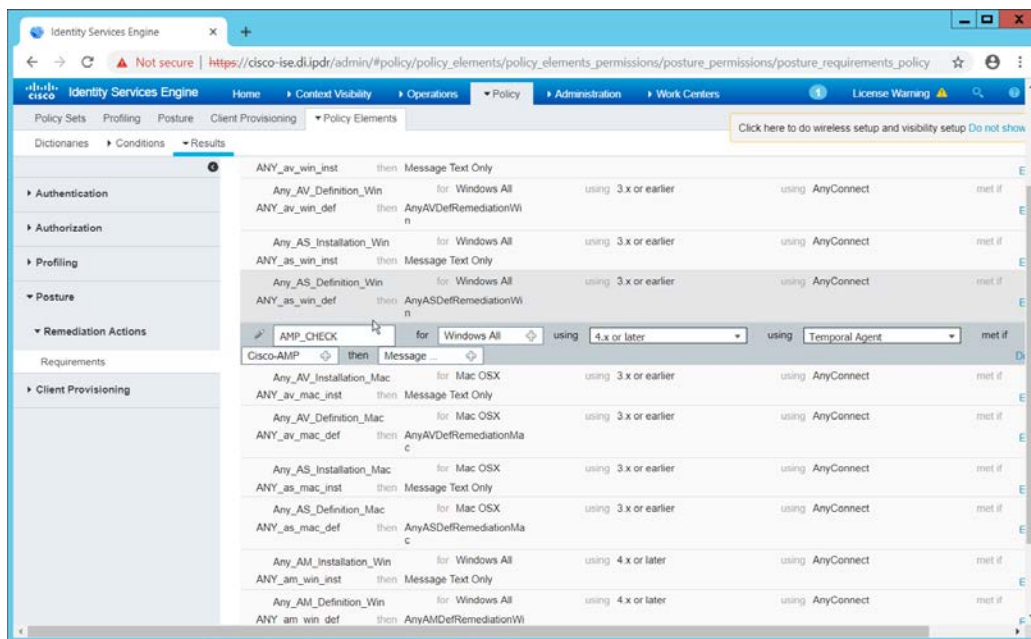
Below the form is a table titled 'Products for Selected Vendor' with the following data:

Product Name	Version	Remediation Support	Definition Check	Latest Definition Date	Latest Definition
<input type="checkbox"/> ANY	ANY	N/A	YES		
<input type="checkbox"/> Cisco Advanced Malware Protec...	5.x	NO	YES	02/19/2019	7.79603
<input checked="" type="checkbox"/> Cisco Advanced Malware Protec...	6.x	NO	YES	02/19/2019	7.79603

10. Click **Submit**.

## 2.16.7 Policy Enforcement: Developing Policy Results

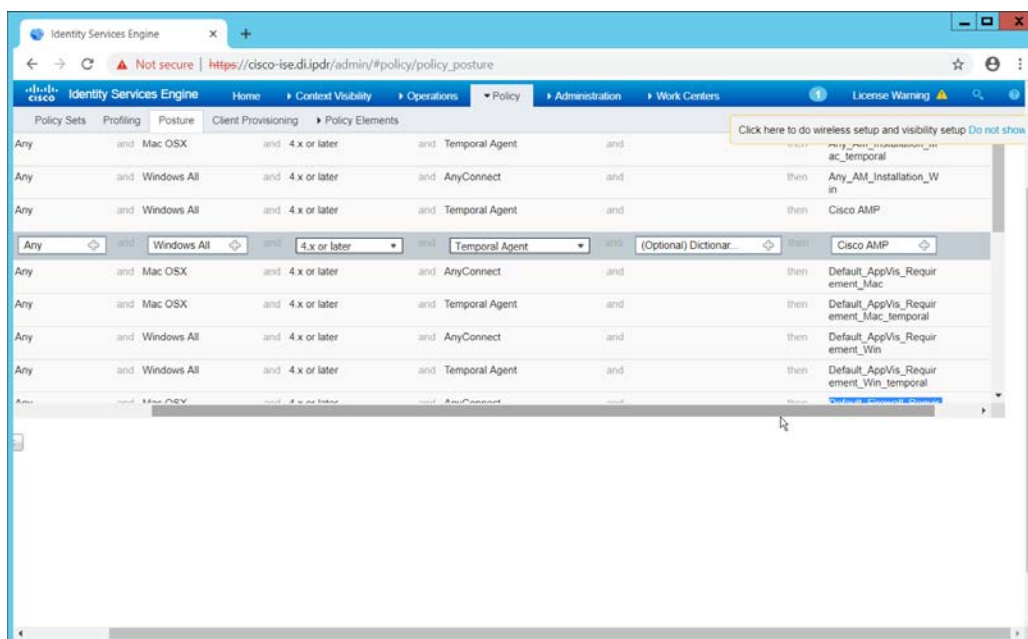
1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements**.
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement**.
3. Enter a **name**.
4. Select **Windows All** for **Operating Systems**.
5. Select **4.x or later** for **Compliance Module**.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



10. Click **Save**.

## 2.16.8 Policy Enforcement: Enforcing a Requirement in Policy

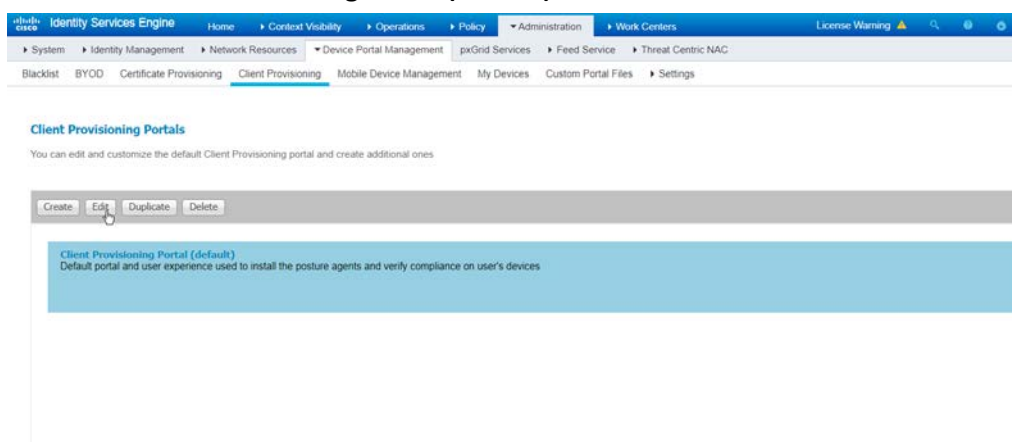
1. Navigate to **Policy > Posture**.
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Policy**.
3. Enter a **name**.
4. Select **Windows All** for **Operating Systems**.
5. Select **4.x or later** for **Compliance Module**.
6. Select **Temporal Agent** for **Posture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



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

## 2.16.9 Policy Enforcement: Configuring a Web Portal

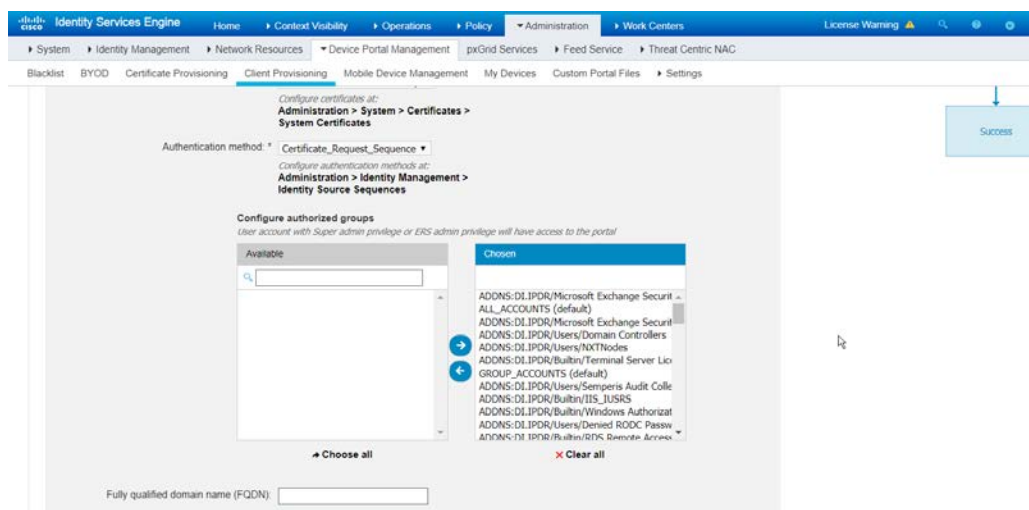
1. Navigate to **Administration > Device Portal Management > Client Provisioning**.
2. Select the **Client Provisioning Portal (default)**.



3. Click **Edit**.



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



6. Click **Save**.

## 2.16.10 Configuring RADIUS with Your Network Device

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

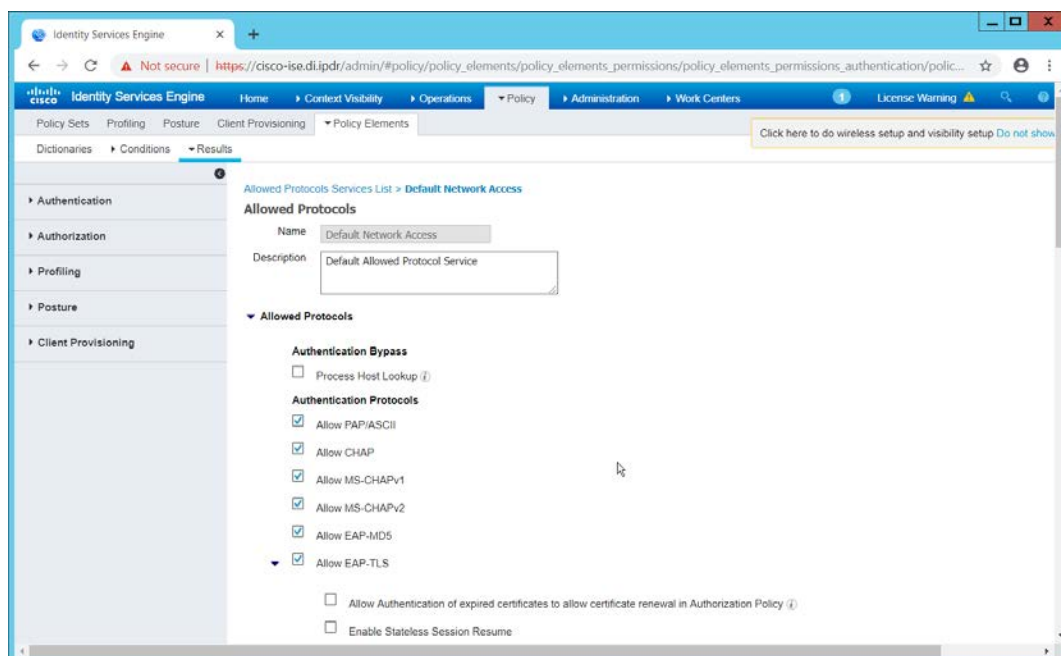
- The **Network Device** (i.e., the router or switch) must support RADIUS functions, specifically **Authentication, Authorization, and Accounting**. Furthermore, it must also support **CoA**, which is **Change of Authorization**. To configure this, you must configure your network device to use Cisco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



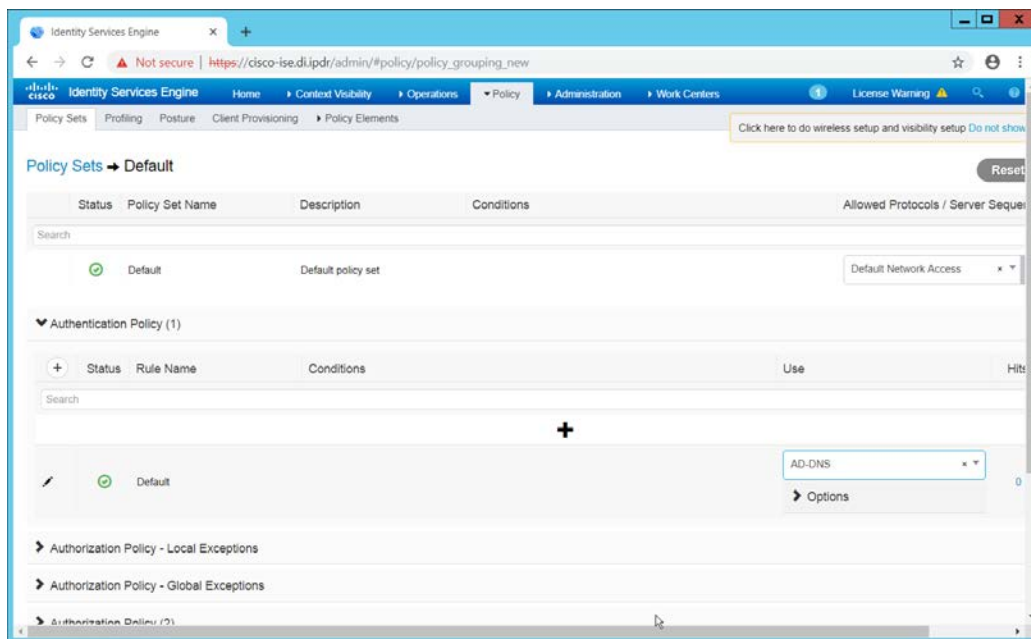
- b. There are also many switches that provide direct 802.1x username/password authentication. Note that if you choose to use this mechanism, a client is still required, and it will not be in the web browser. Windows has a built-in 802.1x client, which can be configured on network adapters under the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

### 2.16.11 Configuring an Authentication Policy

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



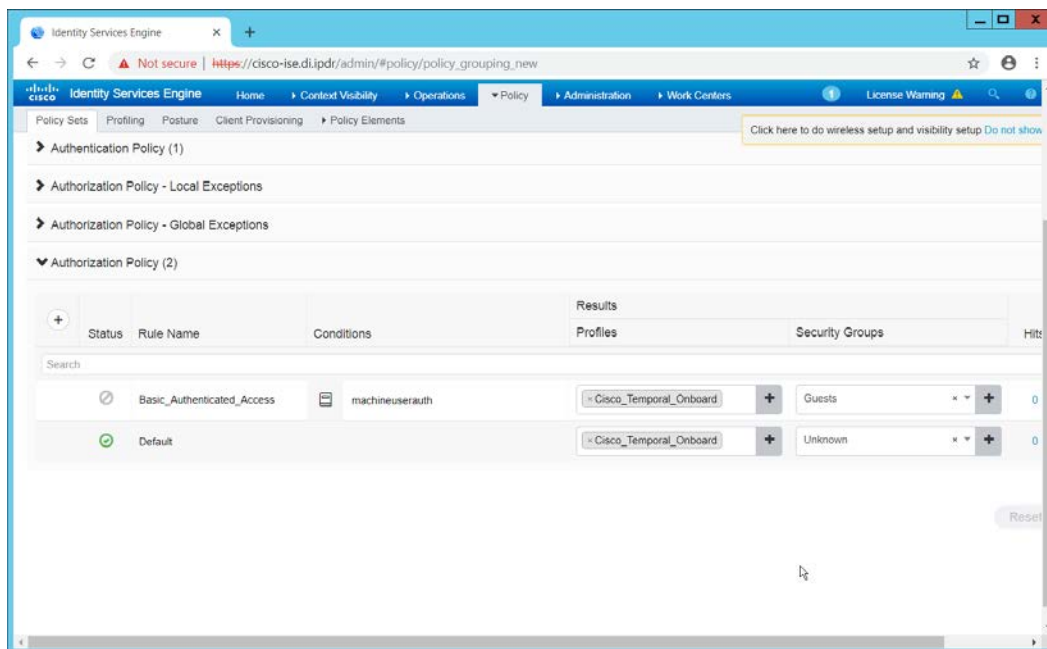
4. Click **Save**.
5. Navigate to **Policy > Policy Sets**.
6. Select the default policy.
7. Ensure that the **Allowed Protocol** selection matches the allowed protocol you just created/edited.
8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate users.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



9. Click **Save**.

### 2.16.12 Configuring an Authorization Policy

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



7. Click **Save**.

## 2.17 Tripwire IP360

This section details installation and configuration for Tripwire IP360.

### 2.17.1 Installation

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

## 2. Log in using default admin credentials.

```
Running airc-firstboot: [ OK ]
Starting postfix: [ OK ]
Running vnc-airc-firstboot: [ OK ]
Installing Ontology: [ 2789.687618] sched: RT throttling activated [ OK ]

Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Waiting for Tripwire Axon Access Point Gateway.....
Running: PID:27875
Starting HAL daemon: [ OK ]
Starting ched: [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory
Starting dbd: [ OK ]
Starting hostd: [ OK ]
Starting objectapi: [ OK ]
Starting reportd: [ OK ]
Starting vnc-php-fpm: [ OK ]
Starting vnc-airc: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] ncLib: 07.48 and libche: 04.6
Starting imageserver: [ OK ]
Starting httpd: [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cron: [ OK ]
Digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting loader: [ OK ]

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

Starting ntlmaps:

Tripwire Appliance
vnc-934358a2 login:

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

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

```
Installing Ontology: [ 2789.687618] sched: RT throttling activated [ OK ]

Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Waiting for Tripwire Axon Access Point Gateway.....
Running: PID:27875
Starting HAL daemon: [ OK ]
Starting ched: [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory
Starting dbd: [ OK ]
Starting hostd: [ OK ]
Starting objectapi: [ OK ]
Starting reportd: [ OK ]
Starting vnc-php-fpm: [ OK ]
Starting vnc-airc: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] ncLib: 07.48 and libche: 04.6
Starting imageserver: [ OK ]
Starting httpd: [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cron: [ OK ]
Digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting loader: [ OK ]

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

Starting ntlmaps:

Tripwire Appliance
vnc-934358a2 login:

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

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

```
[ 1.647400] [drm] Max dedicated hypervisor surface memory is 0 kiB
[ 1.647506] [drm] Maximum display memory size is 20400 kiB
[ 1.647799] [drm] UARM at 0xc0000000 size is 20400 kiB
[ 1.647995] [drm] PMU at 0xc0000000 size is 256 kiB
[ 1.648122] [drm] global init.
[ 1.648373] [TTM] Zone kernel: Available graphics memory: 8214352 kiB
[ 1.648544] [TTM] Zone dma32: Available graphics memory: 2897152 kiB
[ 1.648694] [TTM] Initializing pool allocator
[ 1.648837] [TTM] Initializing DMA pool allocator
[ 1.649301] [drm] Supports vblank timestamp caching Rev 2 (21.10.2013).
[ 1.649576] [drm] No driver support for vblank timestamp query.
[ 1.650530] [drm] Screen Target Display device initialized
[ 1.650551] [drm] width 1200
[ 1.650661] [drm] height 760
[ 1.650801] [drm] bpp 32
[ 1.651637] [drm] Fifo max 0x00040000 min 0x00001000 cap 0x000007ff
[ 1.652583] [drm] Using command buffers with DMA pool.
[ 1.652695] [drm] DX: no.
[ 1.656720] [drm] fbcon: aspdramfb (fb0) is primary device
[ 1.659833] Console: switching to colour frame buffer device 160x40
[ 1.672613] [drm] Initialized vmafx 2.12.0 20170221 for 0000:00:0f:0 on minor 0
[ 1.716076] random: Fast init done
[ 1.728649] Flippy device(s): f00 is 1.44M
[ 1.733327] FDC 0 is a post-1991 82077
[ 1.817166] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts: (null)
[ 1.822838] dracut: Mounted root filesystem /dev/sda2
[ 1.881043] dracut: Switching root
Welcome to Tripwire Appliance
Starting udev: [ 2.251929] udev: starting version 147
[ 2.353204] shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
[ 2.562032] random: crng init done
[ 3.043626] pinctrl_gpio: 0000:00:07:3: SMBus Host Controller not enabled!
[ 3.051650] vme_vml 0000:00:07:7: Found VML PCI device at 0x1000, irq 16
[ 3.051720] vme_vml 0000:00:07:7: Using capabilities 0xc
[ 3.051843] Guest personality initialized and is active
[ 3.051909] VML host device registered (name=vml, major=10, minor=57)
[ 3.052059] Initialized host personality
[ 3.062491] input: PC Speaker at /devices/platform/pcspkr/input/input5
[ 3.118276] FUJITSU Extended Socket Network Device Driver - version 1.1 - Copyright (c) 2015 FUJITSU LIMITED
[ 3.195277] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 3.195365] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 3.530622] e1000 0000:02:00:0 eth0: (PCI:64bit/32-bit) 00:50:56:b2:3a:b1
[ 3.530615] e1000 0000:02:00:0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.557727] ppdev: user-space parallel port driver
Setting hostname localhost.localdomain: [ OK ]
Checking filesystems [ OK ]
```

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

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

Tripwire Appliance
vme-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vme-934358a2) system hostname update tw360.d1.ipdr
Command succeeded.
vme-934358a2) network interface update eth0 192.168.1.144/255.255.255.0
[552860.264771] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552860.264771] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552860.275441] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vme-934358a2) _
```

6. Use command **network route\_default create <gateway>** to update the system's default gateway information in accordance with your environment's network.

```
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed odev events [ OK ]
Digest_proxy does not need to start
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed odev events [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory [ OK ]
Starting hostd: [ OK ]
Starting reportd: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nc11b: 07.40 and libche: 04.6
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cron: [ OK ]
Digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting monit: Cannot translate 'vne-934358a2' to FQDN name -- Name or service not known
Starting Minit 5.14 daemon with http interface at [localhost]:2812 [ OK ]

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

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

```

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

Tripwire Appliance
vne-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vne-934358a2> system hostname update tw360.di.ipdr
Command succeeded.
vne-934358a2> network interface update eth0 192.168.1.144/255.255.255.0
[552868.264771] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552868.264774] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552868.275441] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> network route default create 192.168.1.1
[552116.598551] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552116.603958] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552116.608788] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> system name server create 192.168.1.12
Add nameserver.

Usage:
system nameserver create <ip>

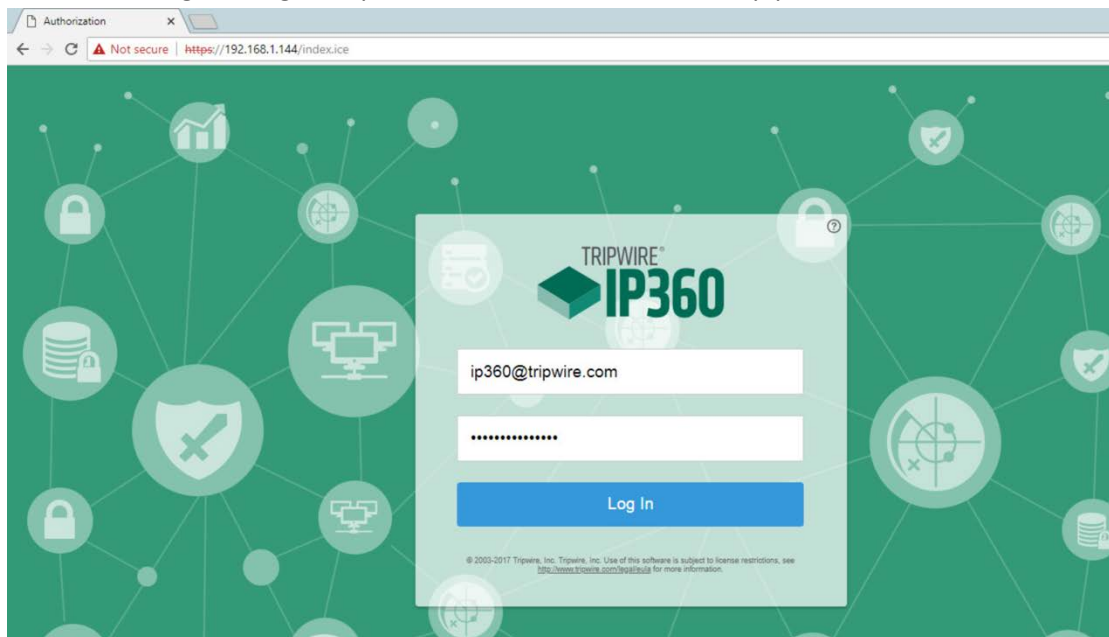
Example:
system nameserver create 192.168.1.2
tw360.di.ipdr> system nameserver create 192.168.1.12
Command succeeded.
tw360.di.ipdr> _

```

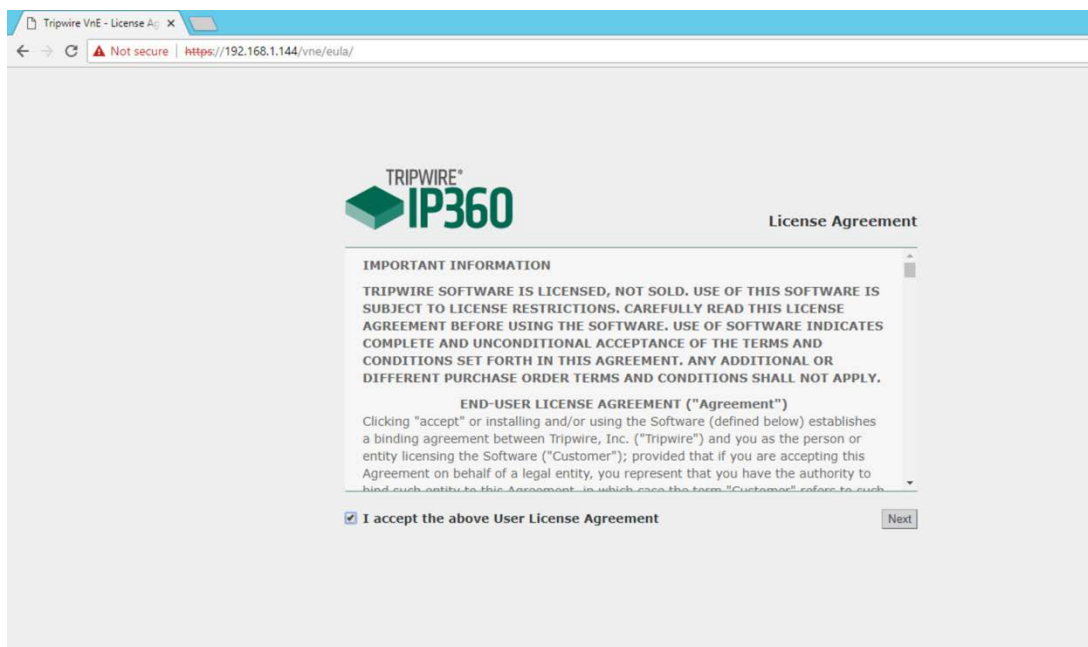


## 2.17.2 Web Portal

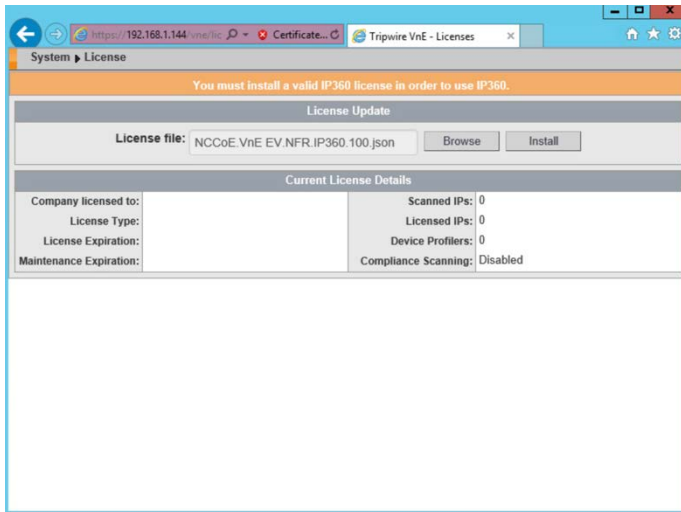
1. From a web browser that can access the newly installed machine's IP address, navigate to the IP address and log in using the updated credentials from the setup process.



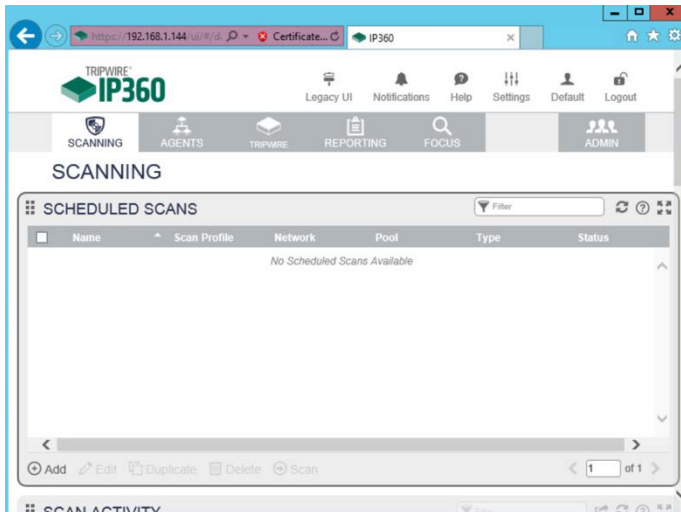
2. Check the box next to **I accept the above User License Agreement.**



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



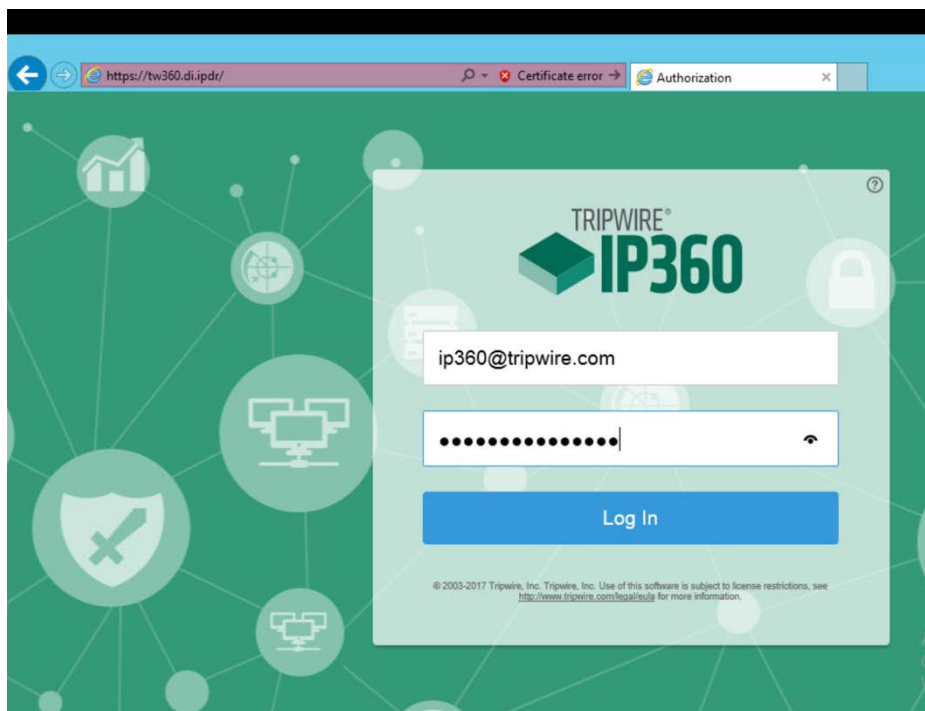
5. Click **Install**.
6. Tripwire IP360 should now be installed and running.



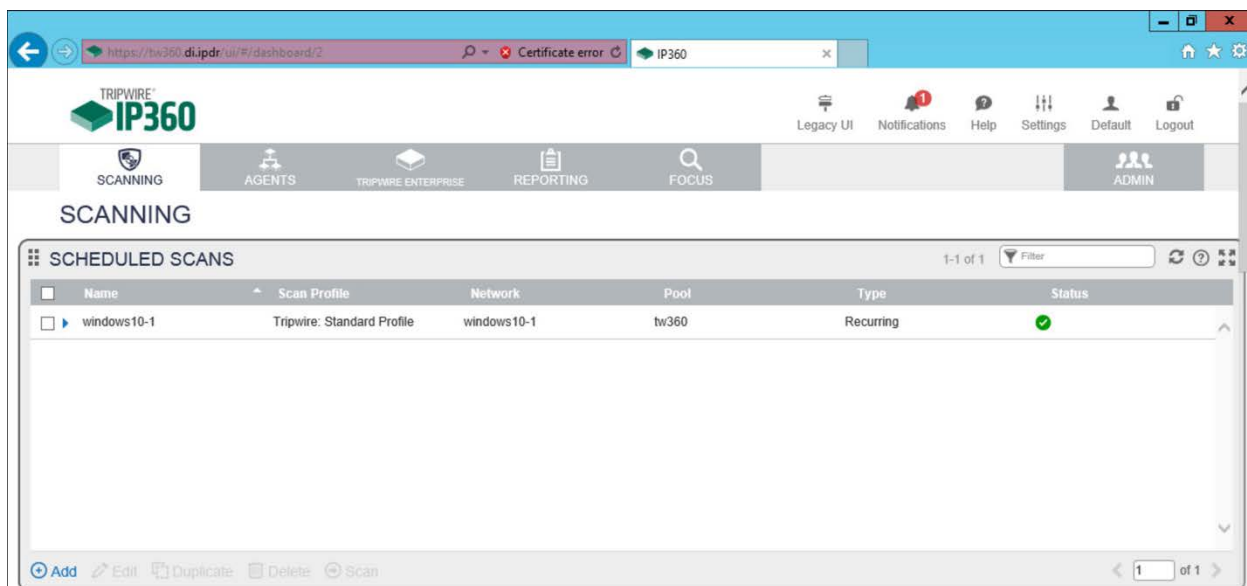
## 2.17.3 Scanning

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

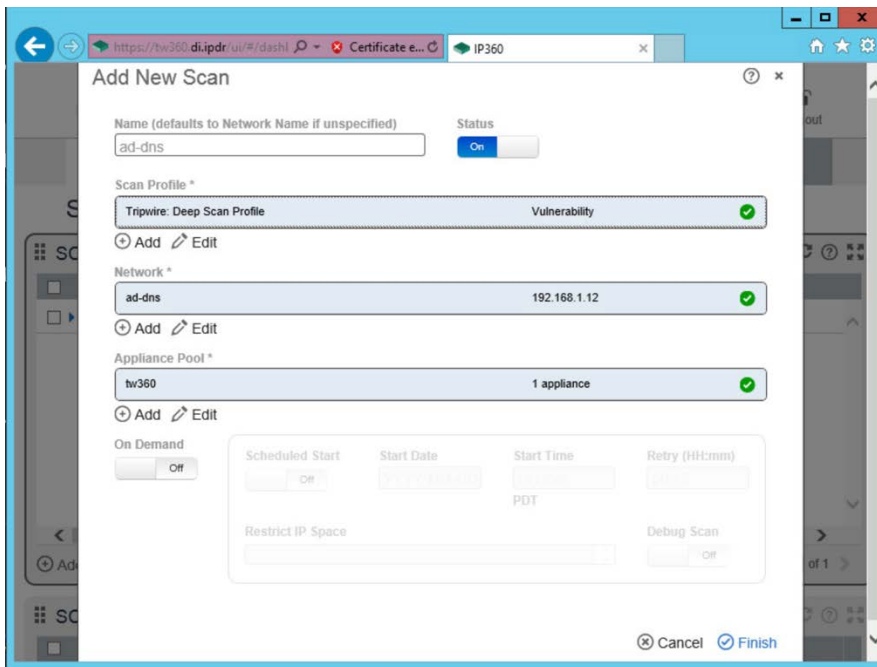
1. Navigate to the web interface and log in.



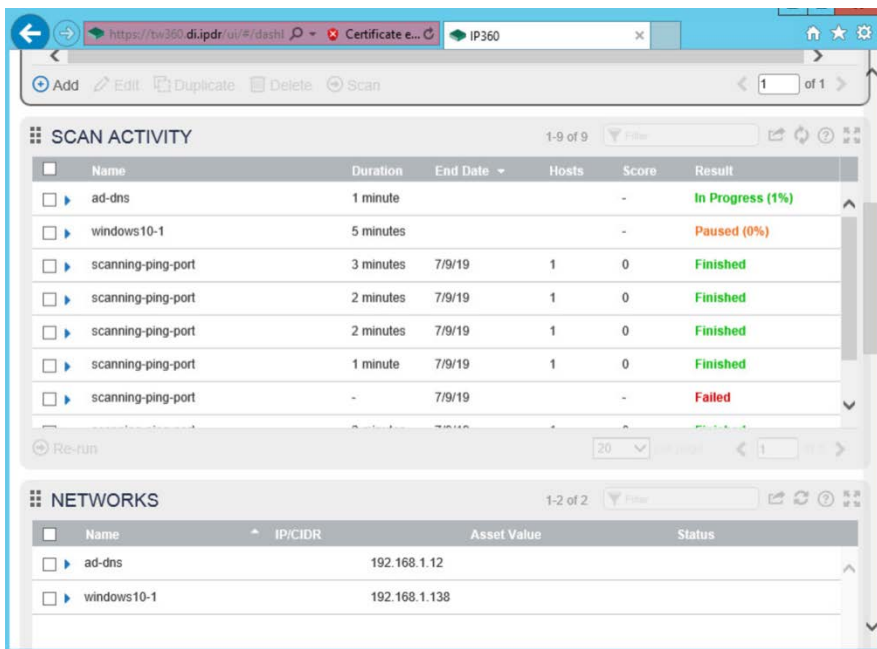
2. Navigate to the **Scanning** tab.



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

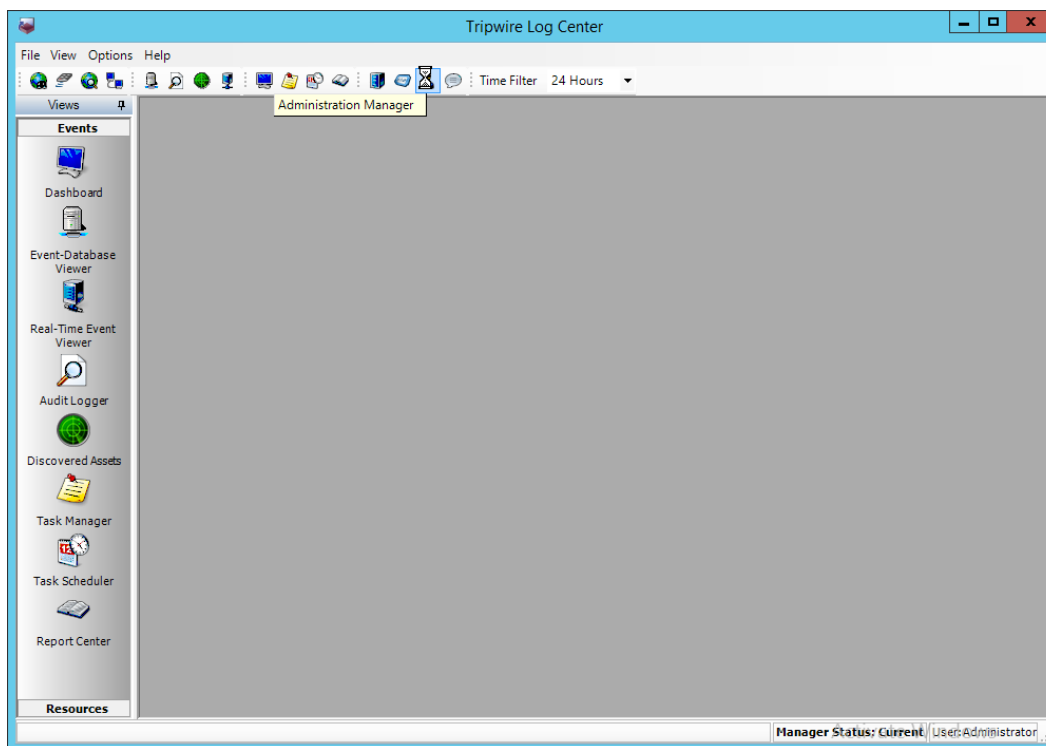


5. Observe successful scan activity.

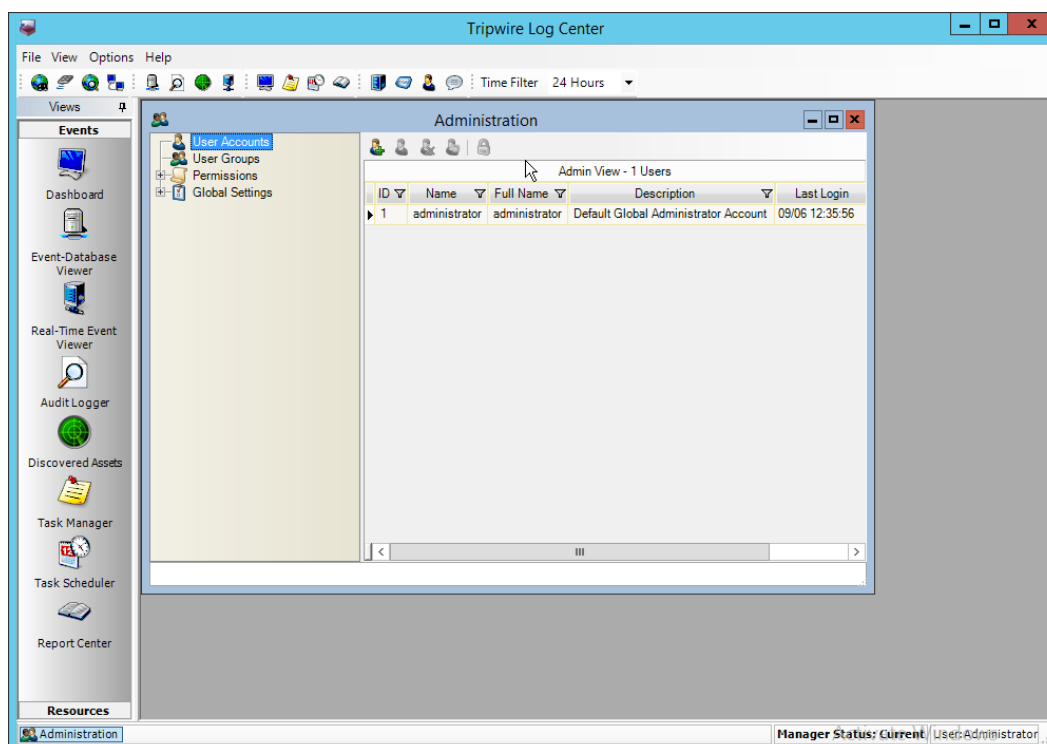


## 2.18 Integration: Tripwire Log Center and Tripwire Enterprise

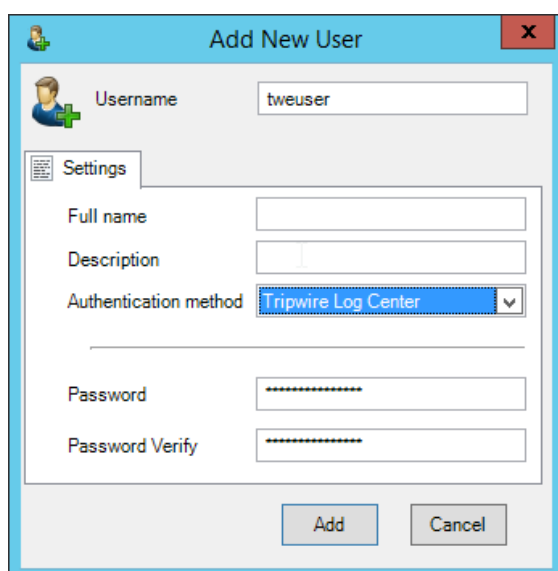
1. Create a user account in **Tripwire Log Center** by logging into **Tripwire Log Center Console**.



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



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



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

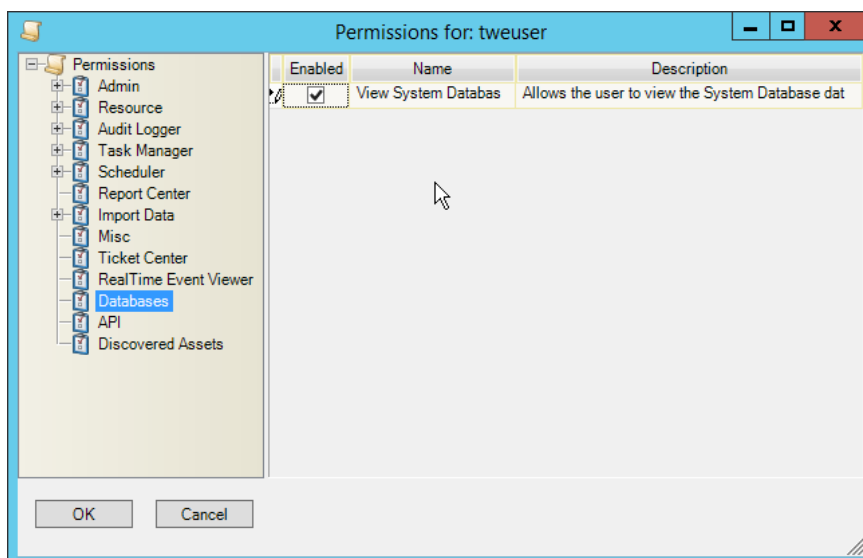
The screenshot shows the 'Edit User - tweuser' dialog box with the 'General' tab selected. The 'User Name' field contains 'tweuser'. Below the tabs, there are input fields for 'Full name', 'Description', 'Email', and two 'Phone' fields, each followed by a dropdown arrow. The 'Authentication' section includes a 'Valid IP's' 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.

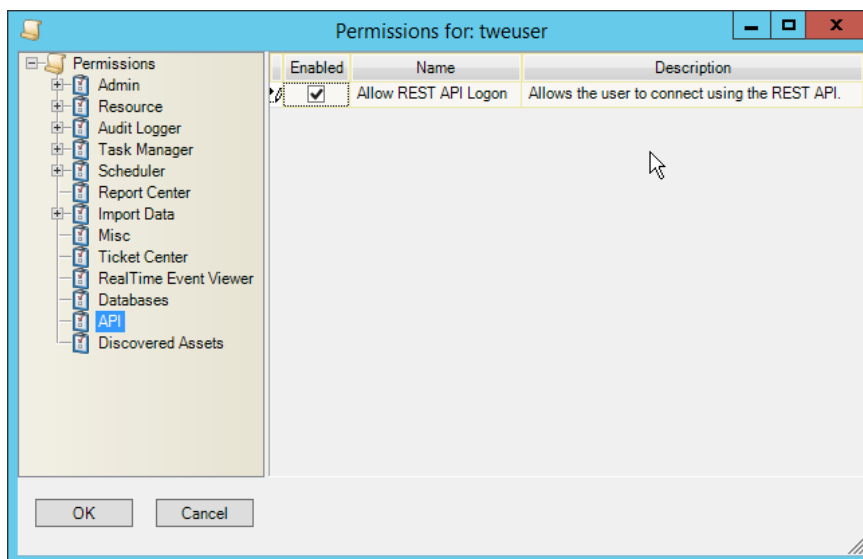
9. Click **Edit list of permissions**.

10. Select **Databases**.



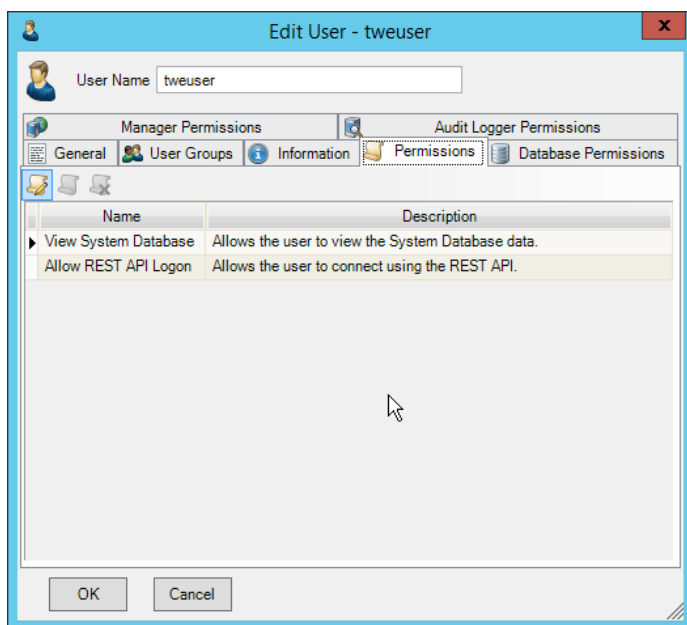
11. Check the box next to **View System Database**.

12. Select **API**.

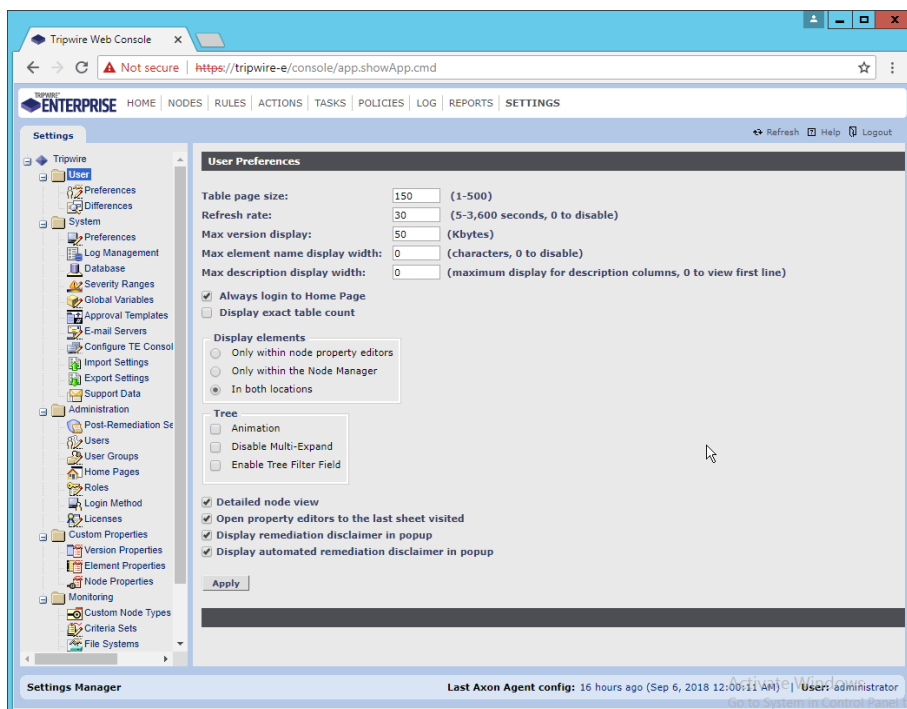


13. Check the box next to **Allow REST API Logon**.

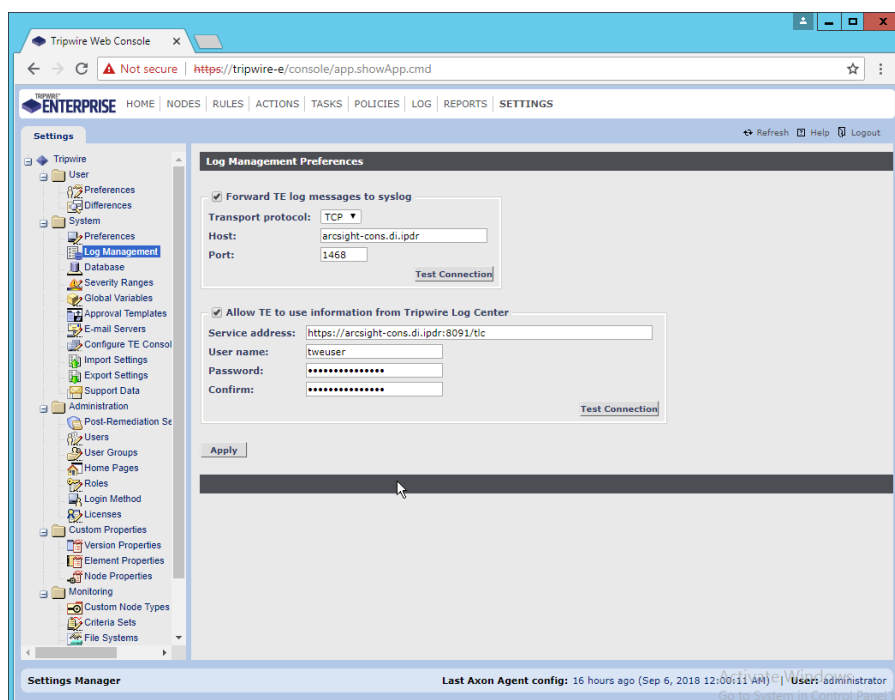




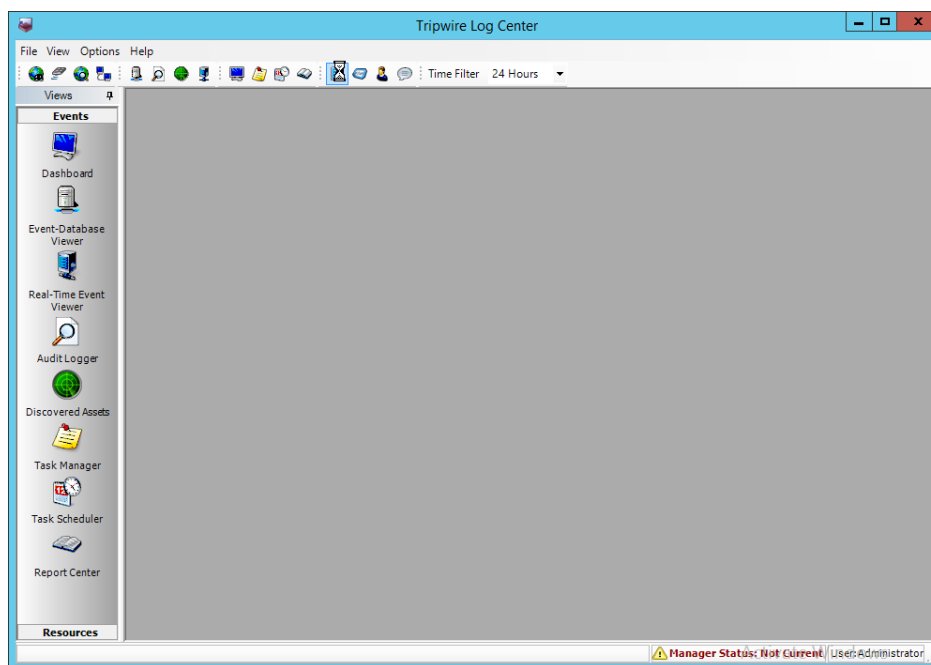
14. Click **OK**.
15. Click **OK**.
16. Log in to the **Tripwire Enterprise** web console.
17. Click **Settings**.



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`. Replace the **hostname** with the hostname of your **Tripwire Log Center** server.
23. Enter the account information of the account just created for **Tripwire Log Center**.
24. You can use **Test Connection** to verify that the connection is working.

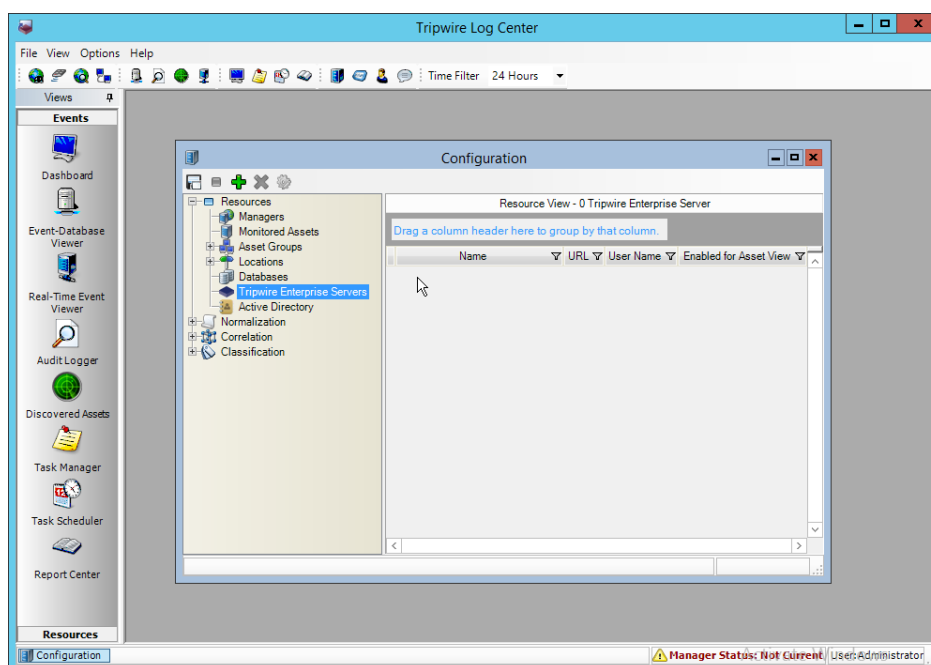


25. Click **Apply** when finished.
26. Go back to the **Tripwire Log Center Console**.



27. Click **Configuration Manager**.

28. Click **Resources > Tripwire Enterprise Servers**.



29. Click **Add**.

30. Enter a **name** for the server.

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

33. Click **Save**.

## 2.19 Integration: Tripwire Log Center and Tripwire IP360

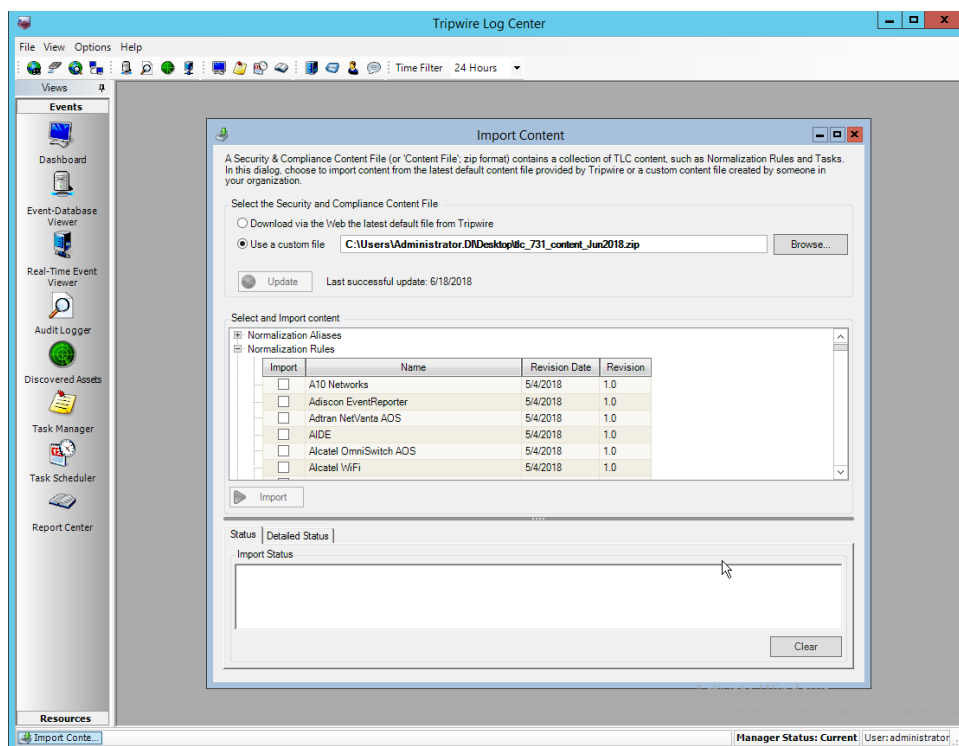
### 2.19.1 Configure IP360 and Log Center

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

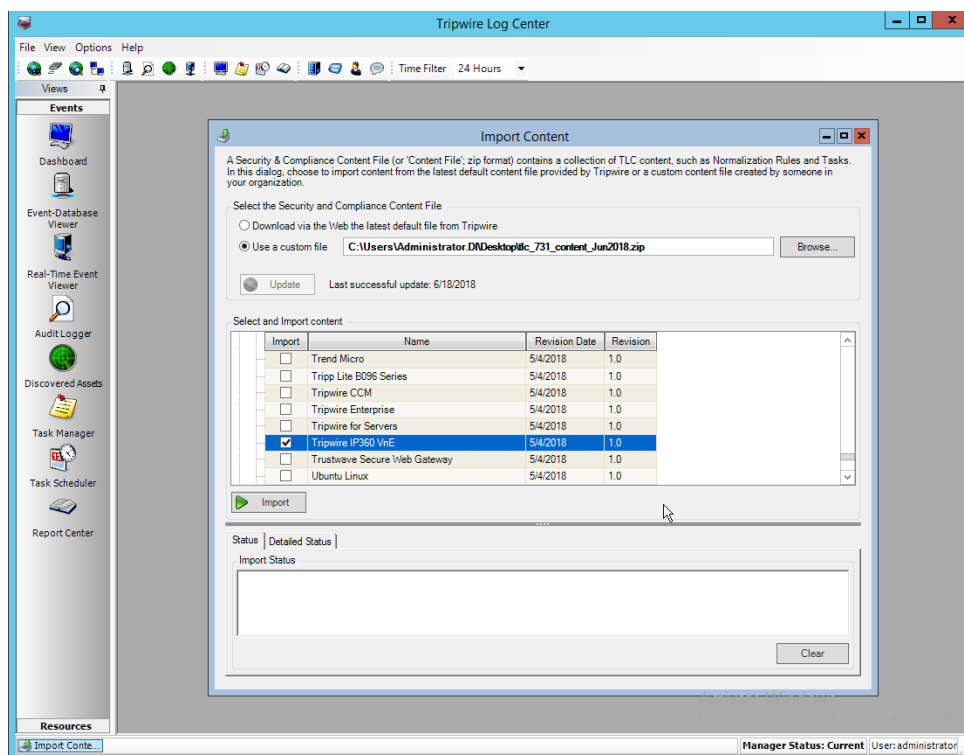
- > `tlc config bridge password update <password>`
- 8. Enter the following command to start the TLC service on the IP360 machine (this will use port 5670 on the TLC machine by default):  
> `system service tlc enable`
- 9. Download the “Content update–June 2018” package from the **Tripwire Customer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



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



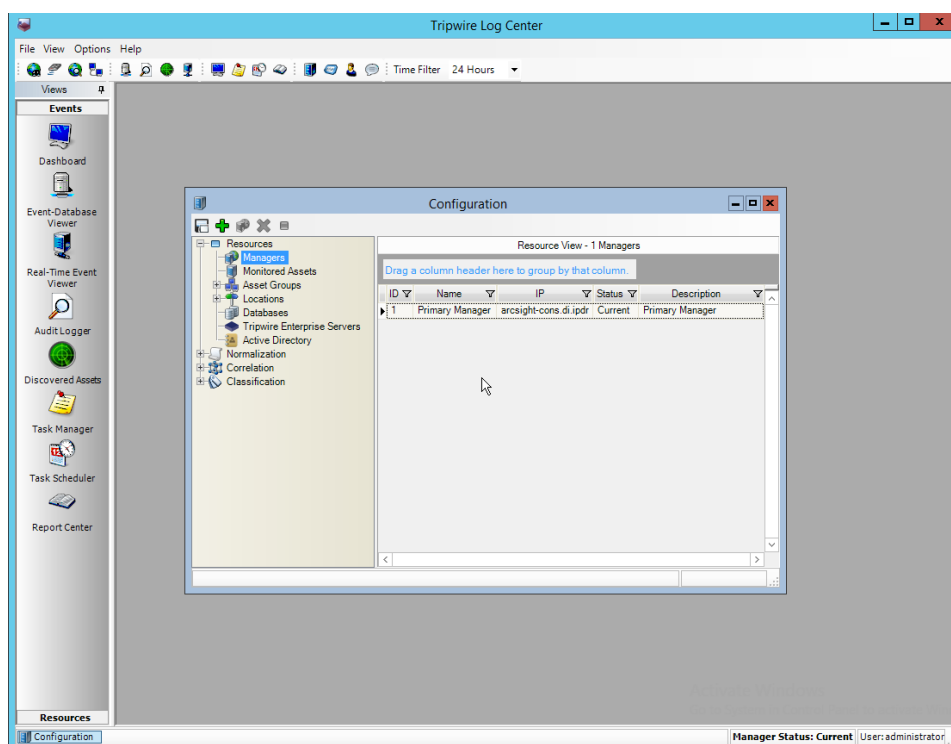
16. Expand the **Normalization Rules** section.
17. Check the box next to **Tripwire IP360 VnE**.



18. Click **Import**.

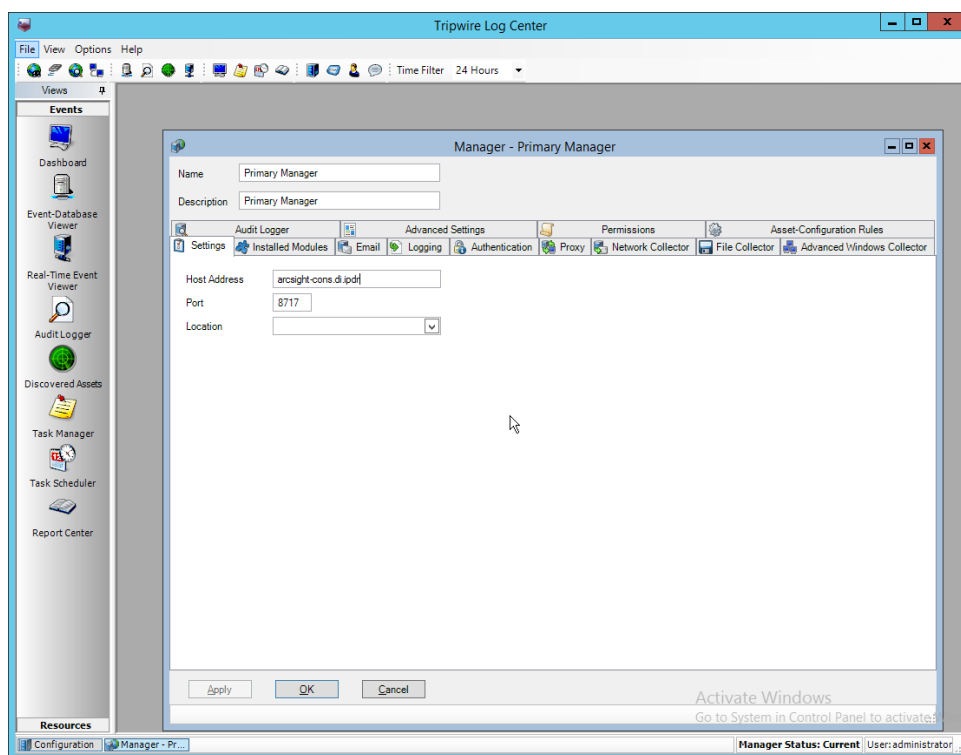
## 2.19.2 Collect Tripwire IP360 Operational Logs

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

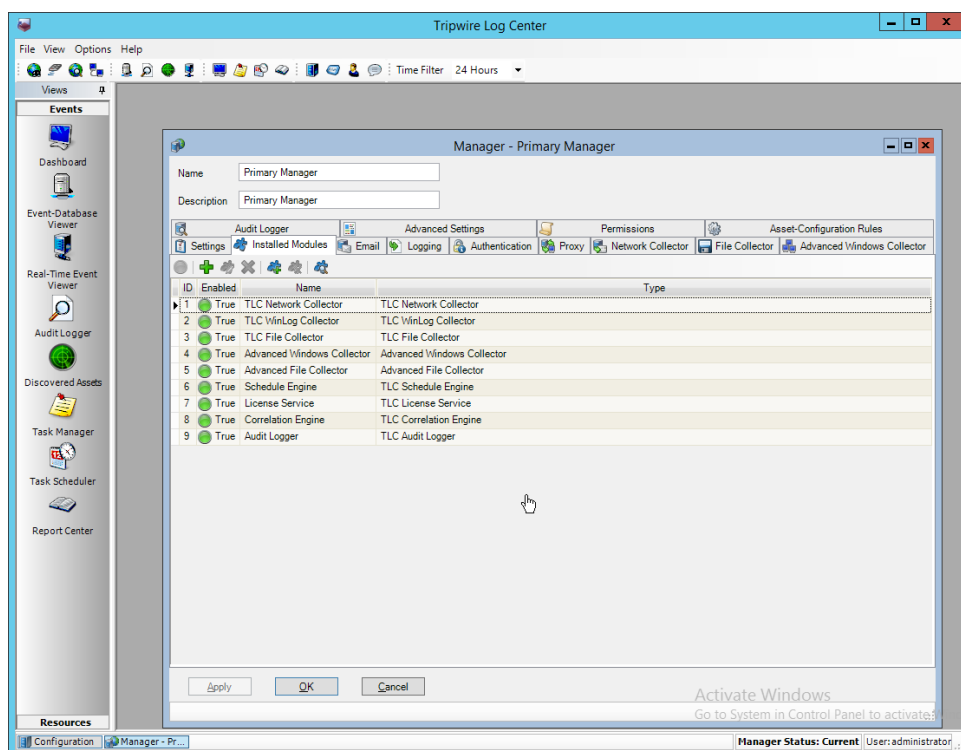


3. Double-click the **Primary Manager**.

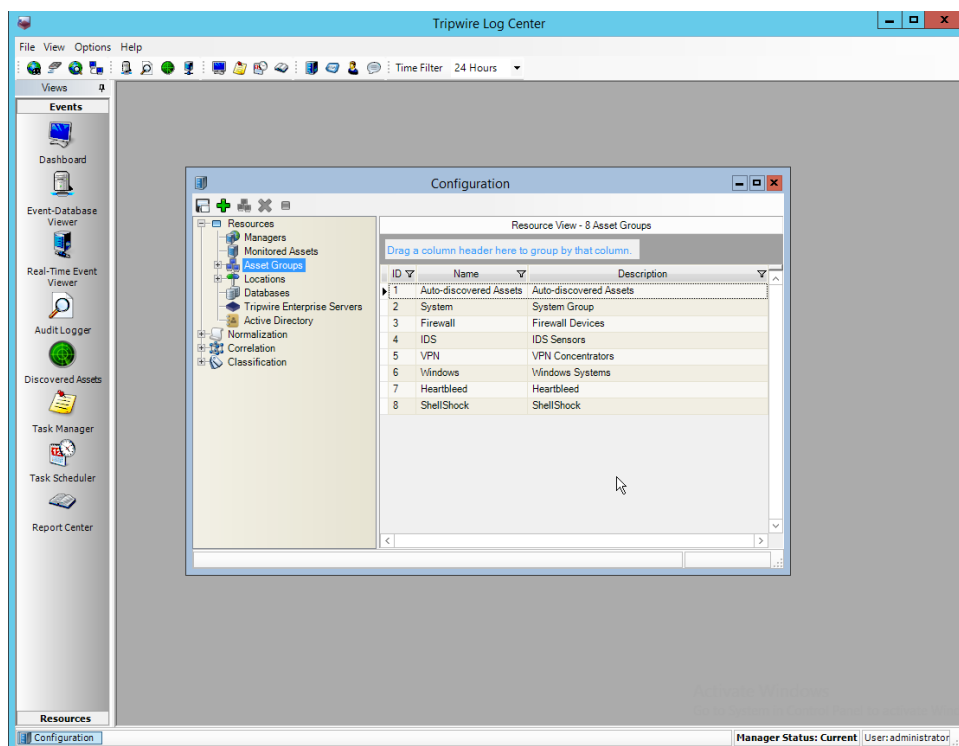




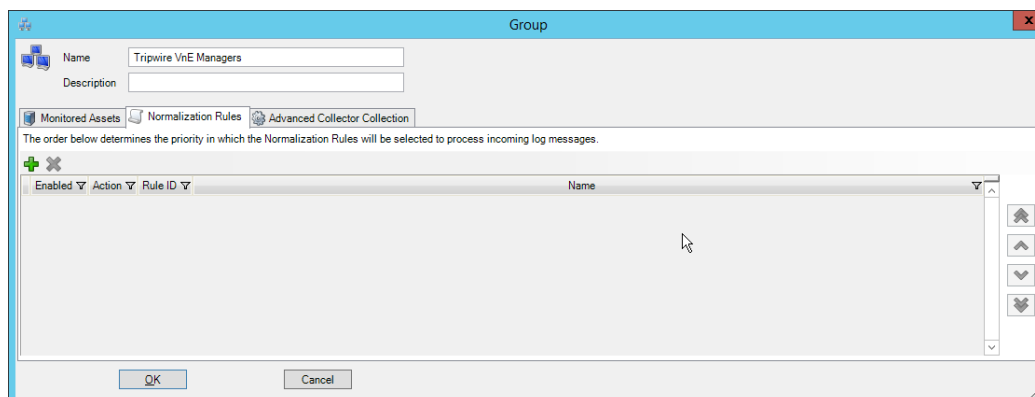
4. Click the **Installed Modules** tab.



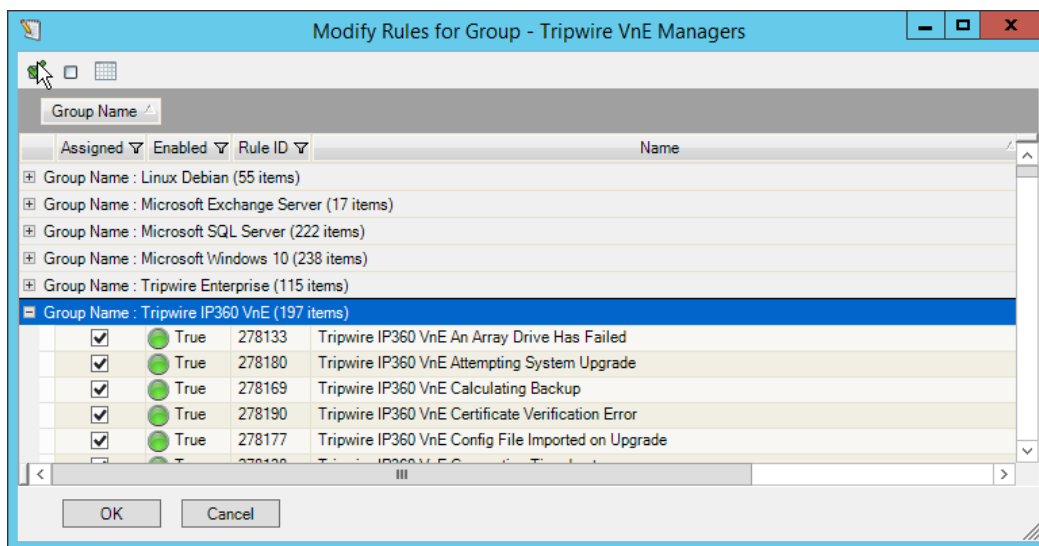
5. Ensure that there is an **Advanced File Collector**. If not, click the **Create new module** button, and specify a **name**. Set the type to **Advanced File Collector**. If there is an **Advanced File Collector**, skip this step.
6. Click **OK**.
7. Click **Resources > Asset Groups**.



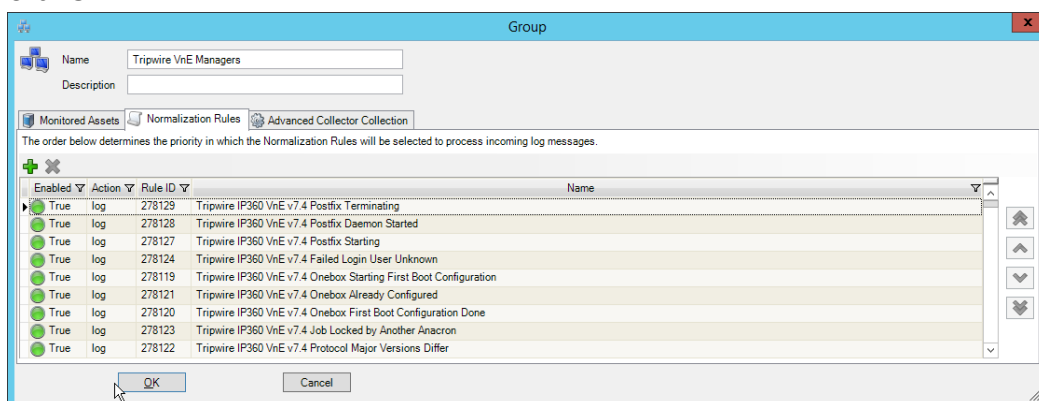
8. Click **Add**.
9. Enter **Tripwire VnE Managers** in the **Name** field.
10. Click the **Normalization Rules** tab.



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

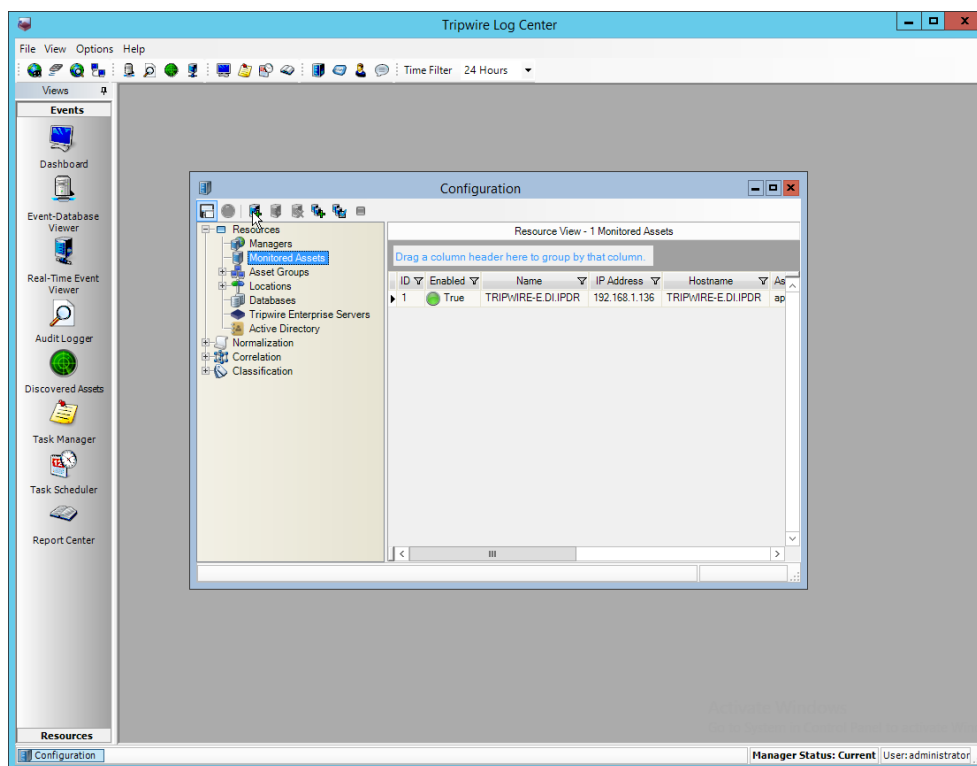


14. Click **OK**.

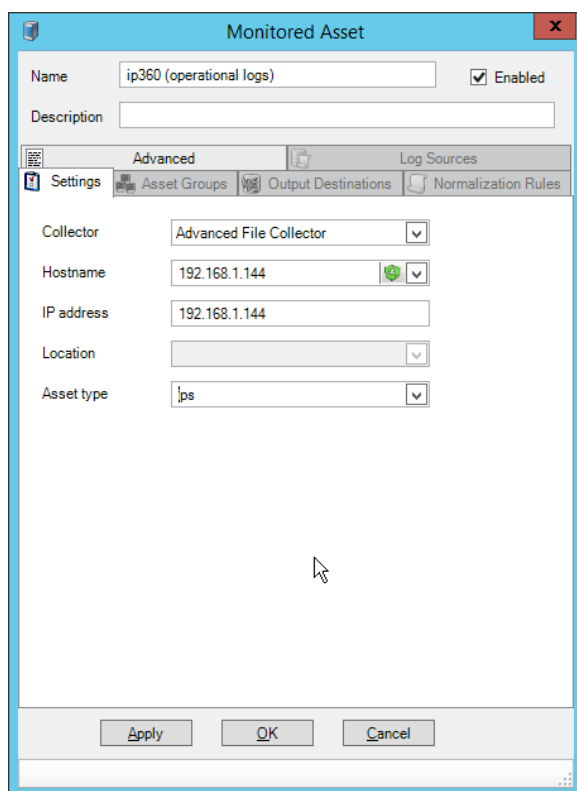


15. Click **OK**.

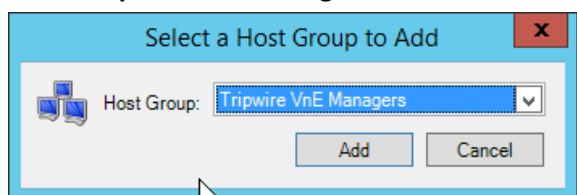
16. Click **Resources > Monitored Assets**.



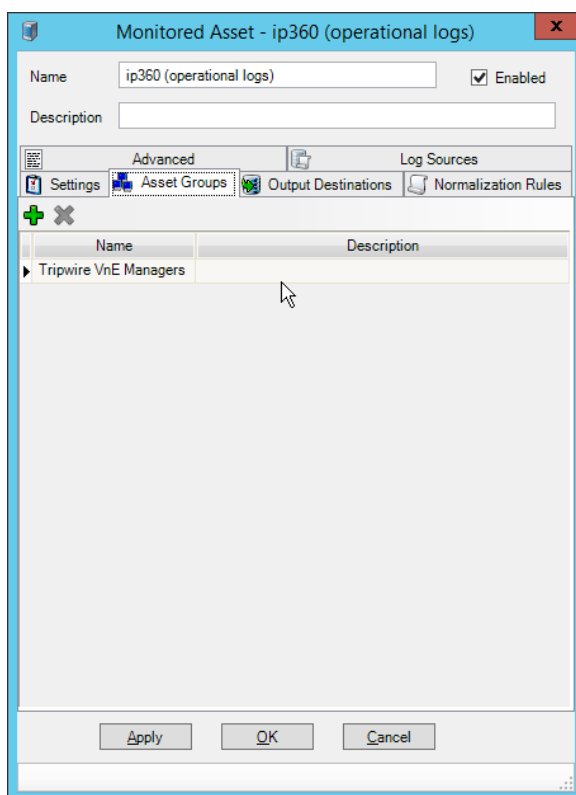
17. Click **Add Monitored Asset**.
18. Enter a **name**.
19. Select **Advanced File Collector** for **Collector**.
20. Select the IP360 server from the **Hostname** drop-down. It may appear as an IP address.
21. Enter the **IP address** of the server.
22. Select **ips** for **Asset type**.



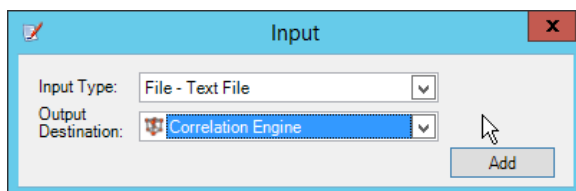
23. Click the **Asset Groups** tab.
24. Click **Add**.
25. Select **Tripwire VnE Managers**.



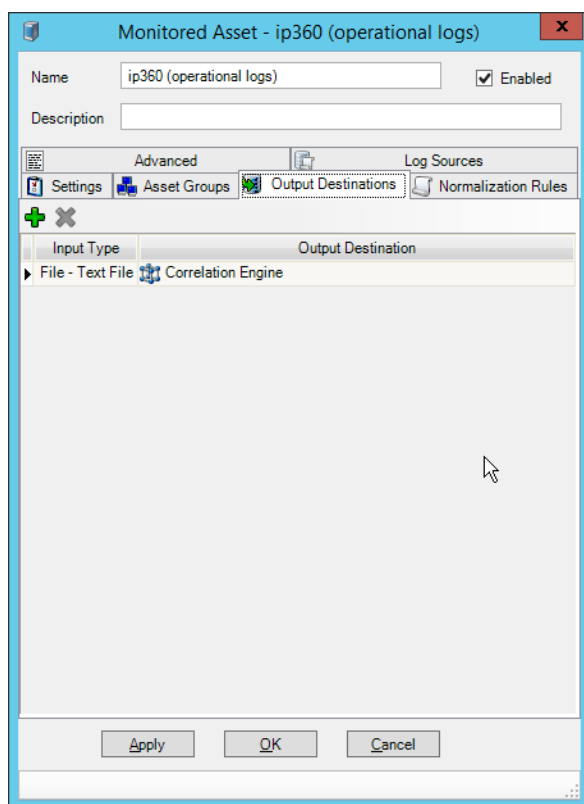
26. Click **Add**.



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

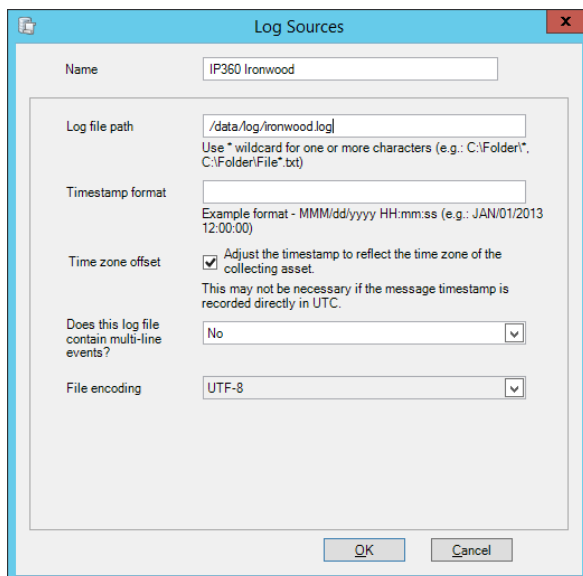


31. Click **Add**.



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





**Log Sources**

Name: IP360 Ironwood

Log file path: /data/log/ironwood.log  
Use \* wildcard for one or more characters (e.g.: C:\Folder\*, C:\Folder\File\*.txt)

Timestamp format:   
Example format - MMM/dd/yyyy HH:mm:ss (e.g.: JAN/01/2013 12:00:00)

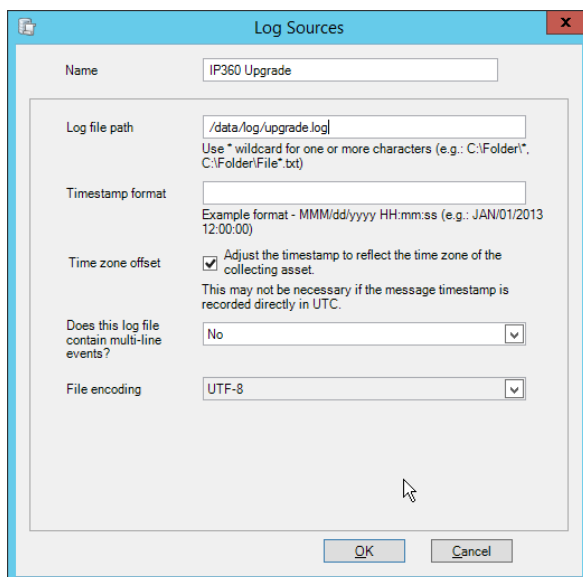
Time zone offset: ☒ Adjust the timestamp to reflect the time zone of the collecting asset.  
This may not be necessary if the message timestamp is recorded directly in UTC.

Does this log file contain multi-line events?: No

File encoding: UTF-8

OK Cancel

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



**Log Sources**

Name: IP360 Upgrade

Log file path: /data/log/upgrade.log  
Use \* wildcard for one or more characters (e.g.: C:\Folder\*, C:\Folder\File\*.txt)

Timestamp format:   
Example format - MMM/dd/yyyy HH:mm:ss (e.g.: JAN/01/2013 12:00:00)

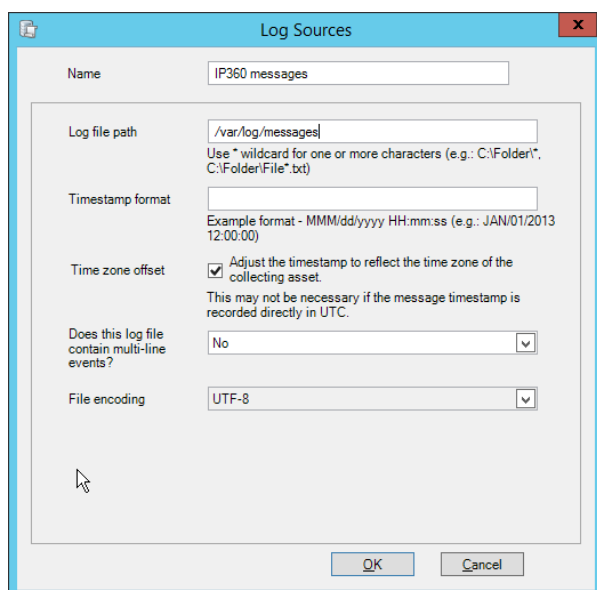
Time zone offset: ☒ Adjust the timestamp to reflect the time zone of the collecting asset.  
This may not be necessary if the message timestamp is recorded directly in UTC.

Does this log file contain multi-line events?: No

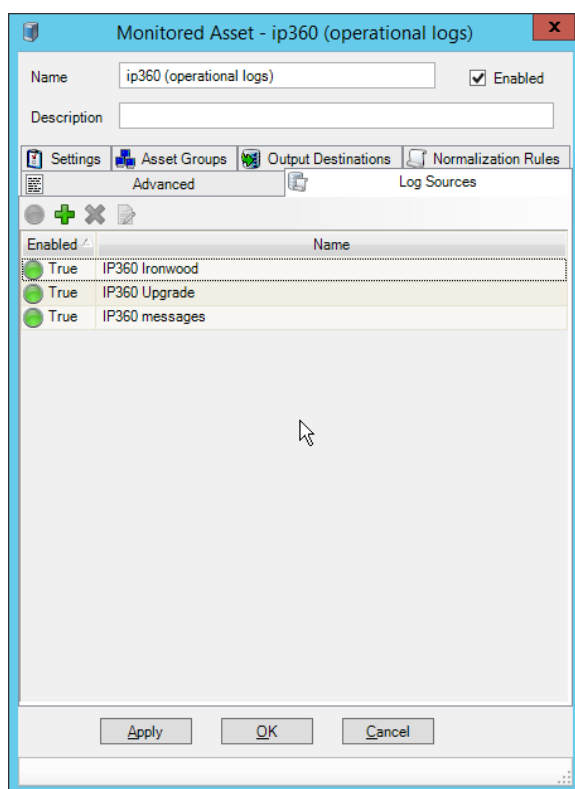
File encoding: UTF-8

OK Cancel

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

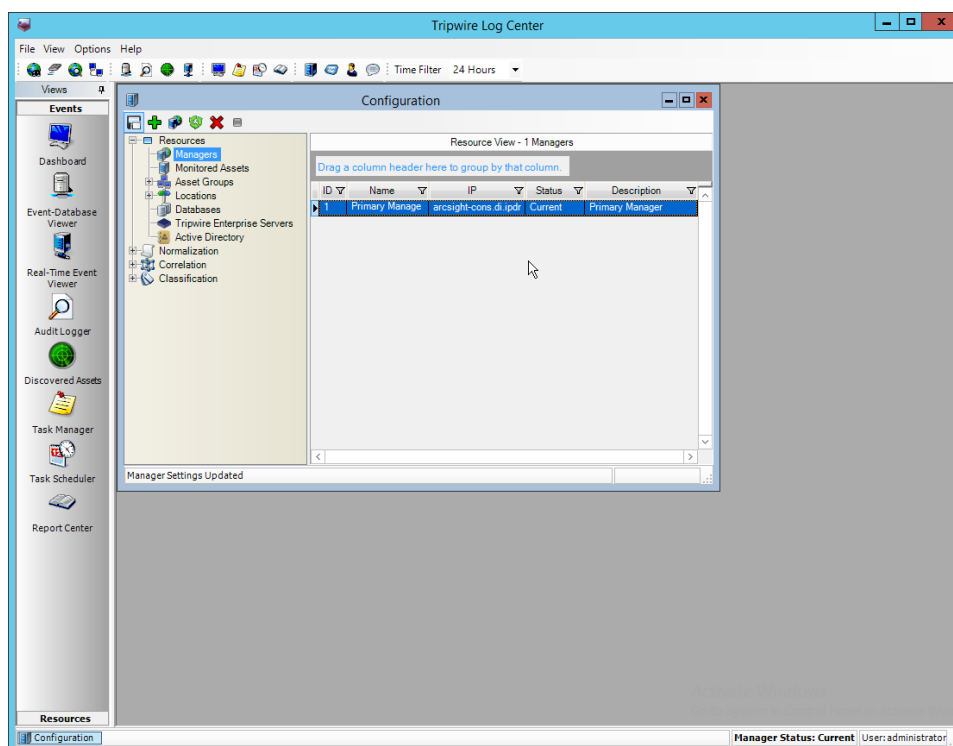


44. Click **OK**.



45. Click **OK**.

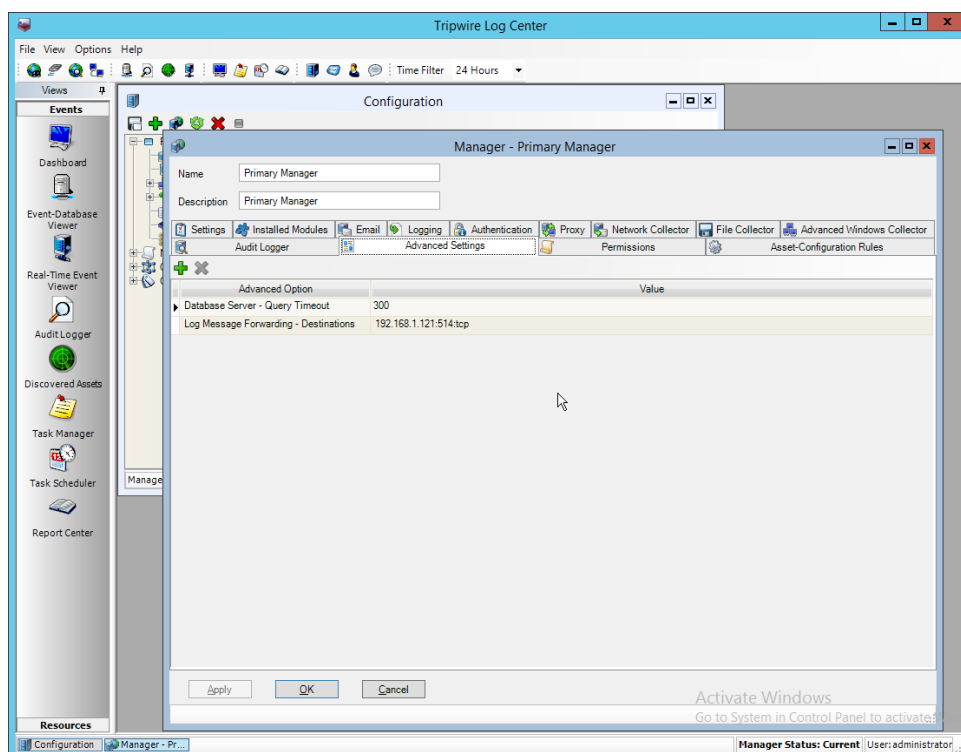
46. Click **Resources > Managers**.



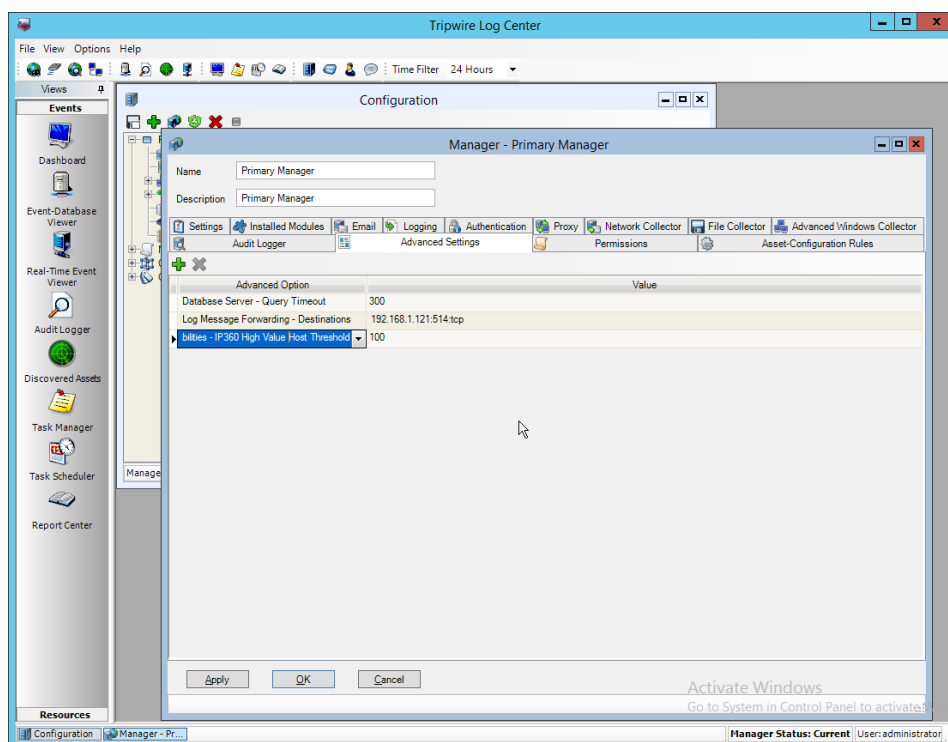
47. Select the **Primary Manager** and click **Push Updates to Manager**.

### 2.19.3 Configure Tripwire IP360 Scan Results Forwarding

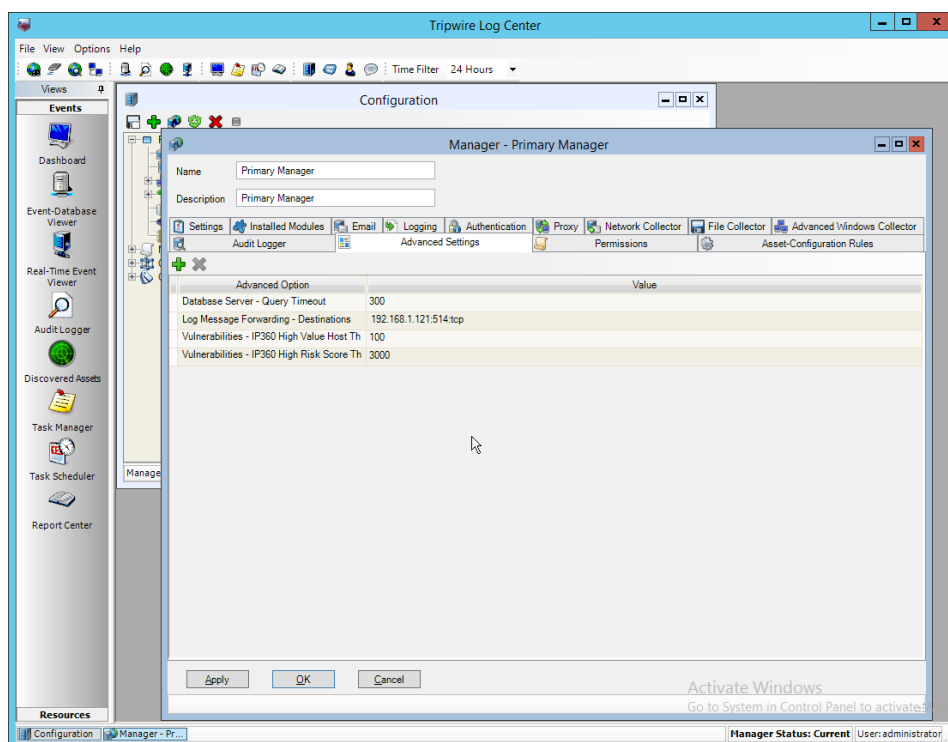
1. Click **Configuration Manager**.
2. Click **Resources > Manager**.
3. Double-click the **Primary Manager**.
4. Click the **Advanced Settings** tab.



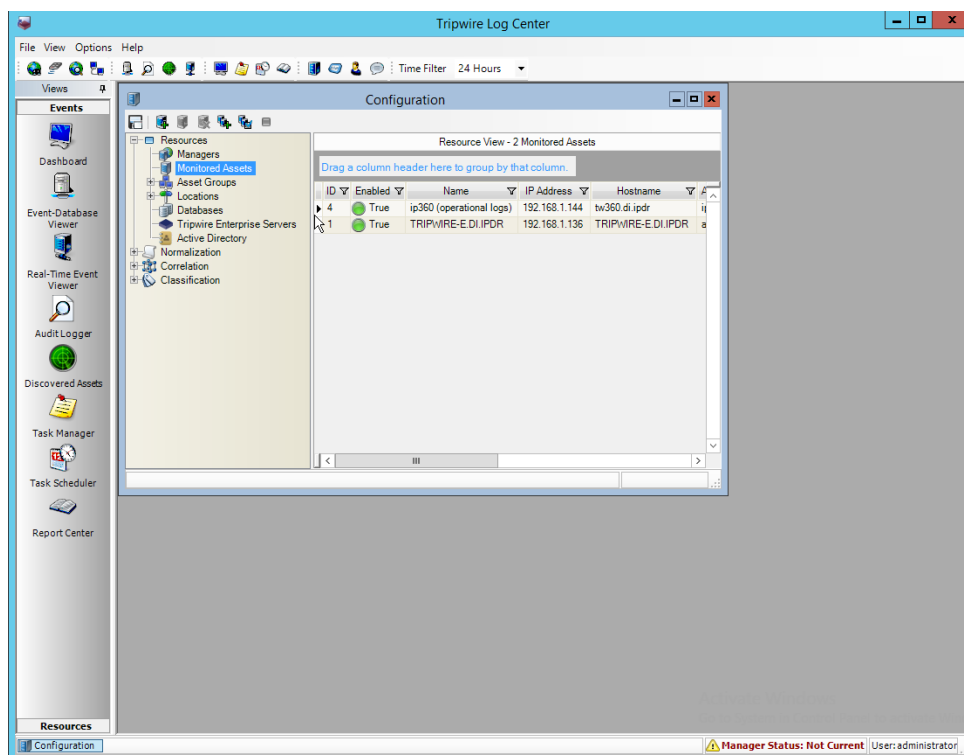
5. Click **Add**.
6. Select **Vulnerabilities–IP360 High Value Host Threshold** for the **Advanced Option**.
7. Enter a number between 0 and 999,999,999 for the **Value**. This number corresponds to the priority level of the host system being scanned. The value entered will be the minimum value for a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



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



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



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

Monitored Asset - Tripwire IP360 (Scan Results)

Name: Tripwire IP360 (Scan Results) ☒ Enabled

Description:

Advanced ☒ Schedule

Settings ☒ Asset Groups ☒ Output Destinations ☒ Normalization Rules

Collector: TLC File Collector

IP address: 192.168.1.144

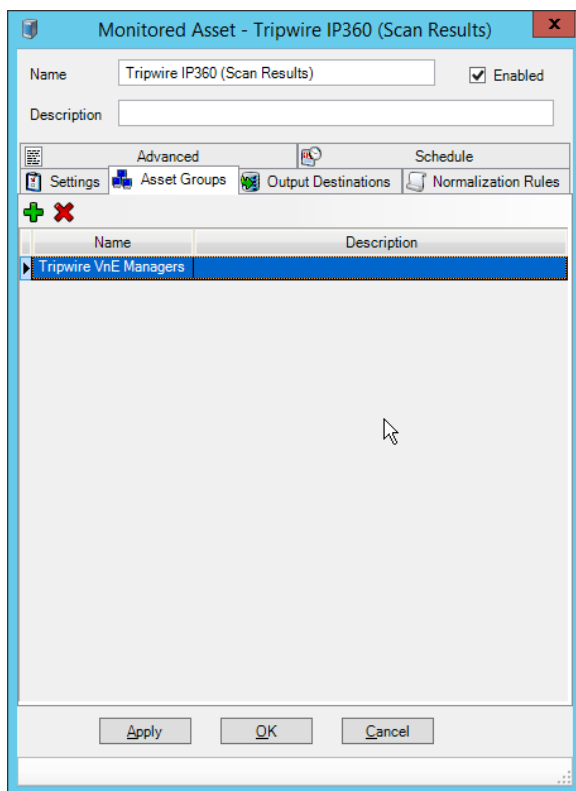
Location:

Asset type: ips

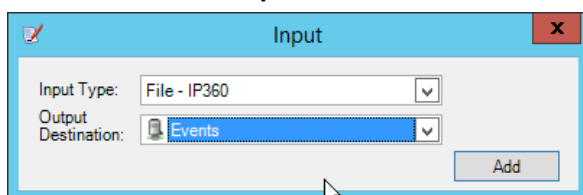
Apply OK Cancel

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

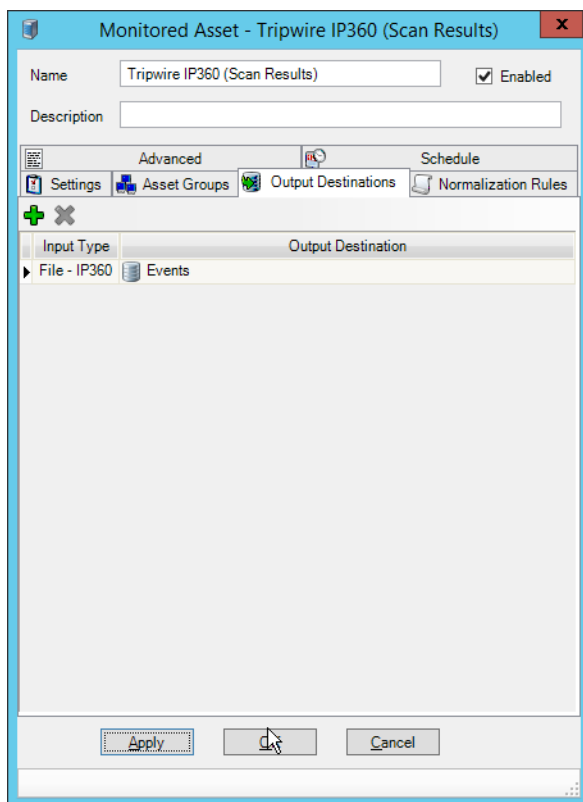




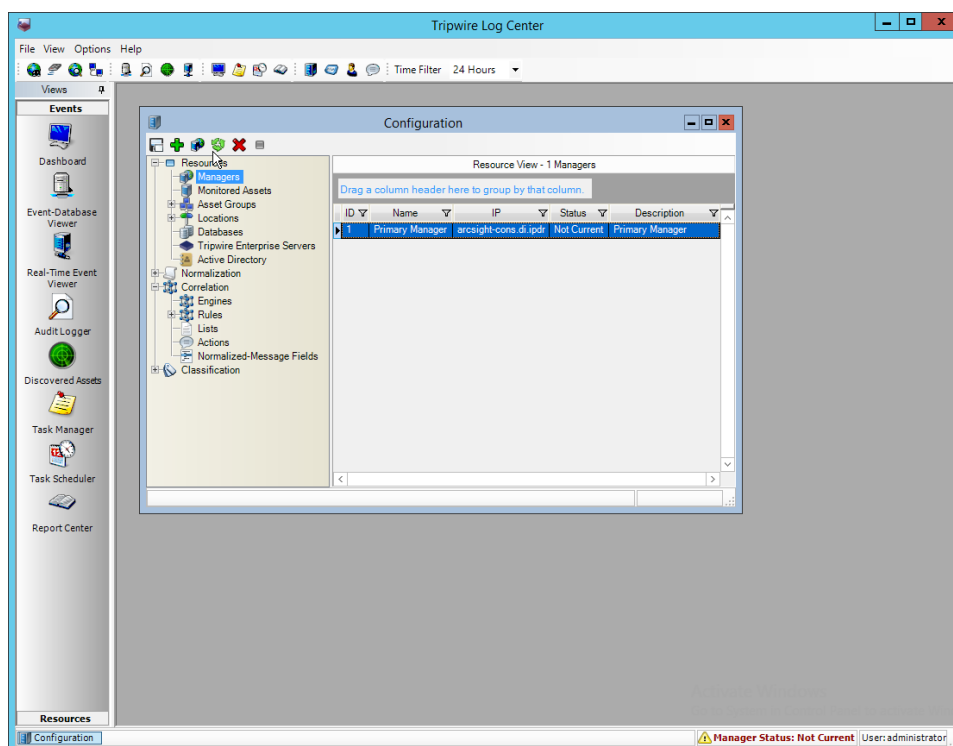
22. Click the **Output Destinations** tab.
23. Select **File—IP360** for **Input Type**.
24. Select **Events** for **Output Destination**.



25. Click **Add**.

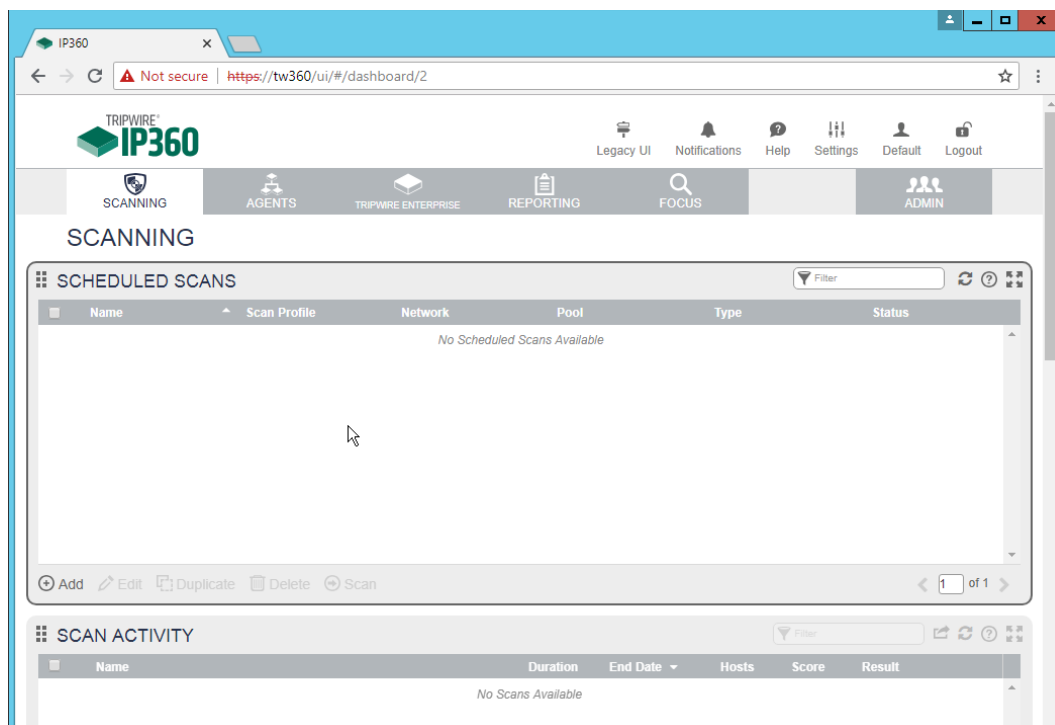


26. Click **OK**.
27. Click **Resources > Managers**.
28. Select the **Primary Manager**.

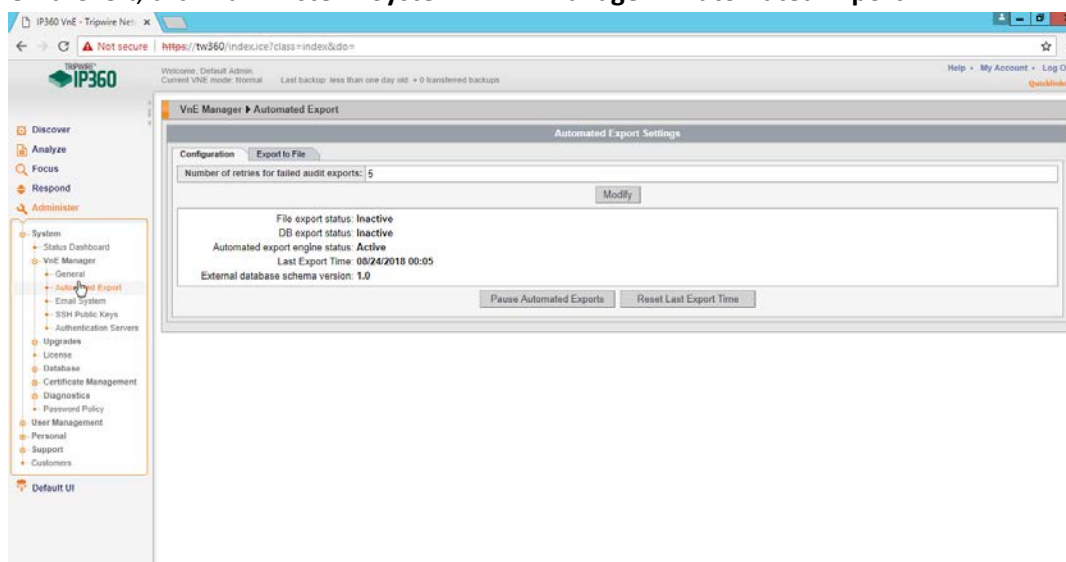


29. Click **Push Update to Manager**.

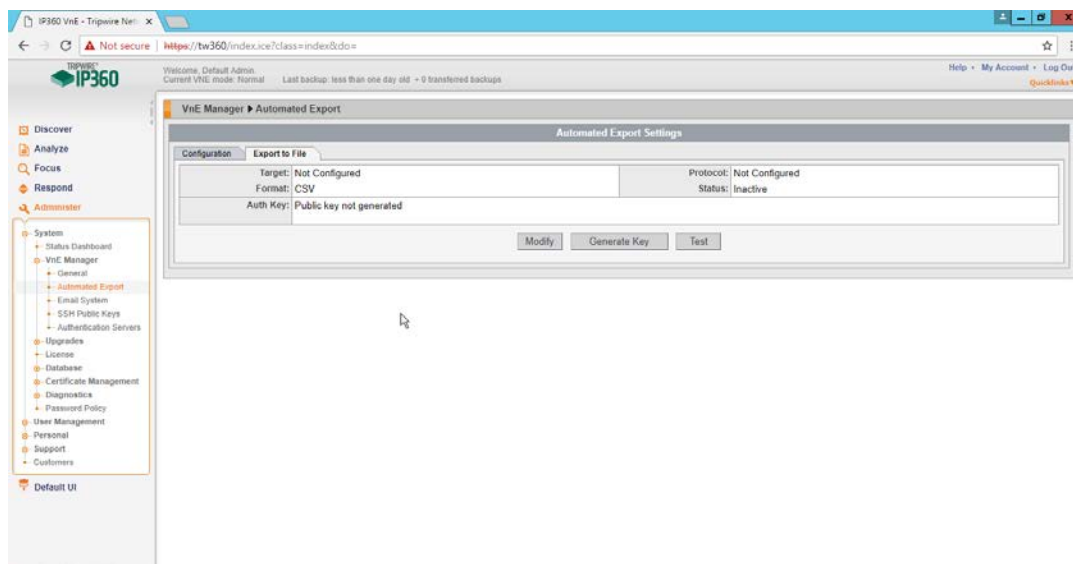
30. Log in to the **Tripwire IP360 Web Console**.



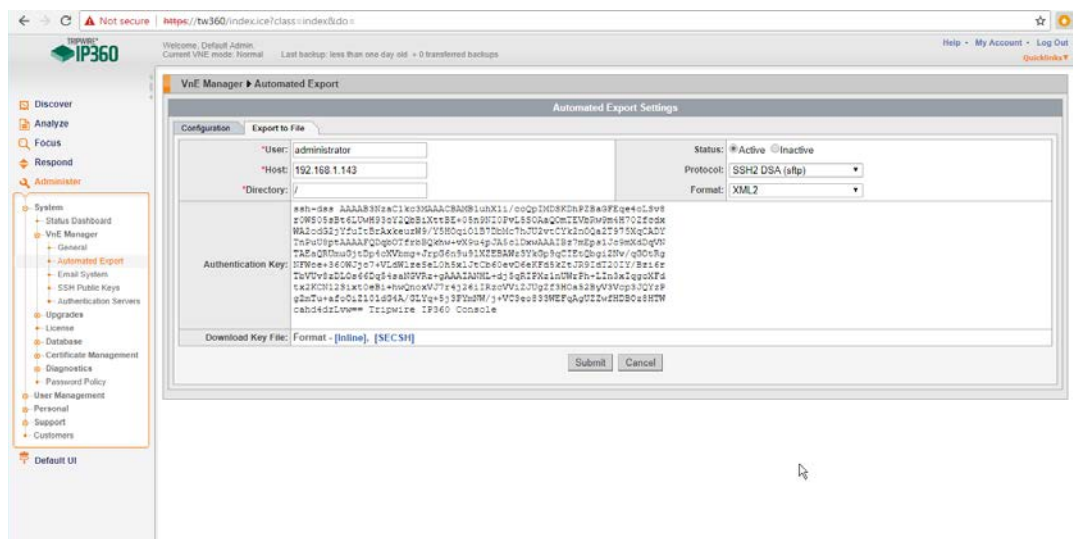
31. Click **Legacy UI** at the top.
32. On the left, click **Administer** > **System** > **VnE Manager** > **Automated Export**.



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



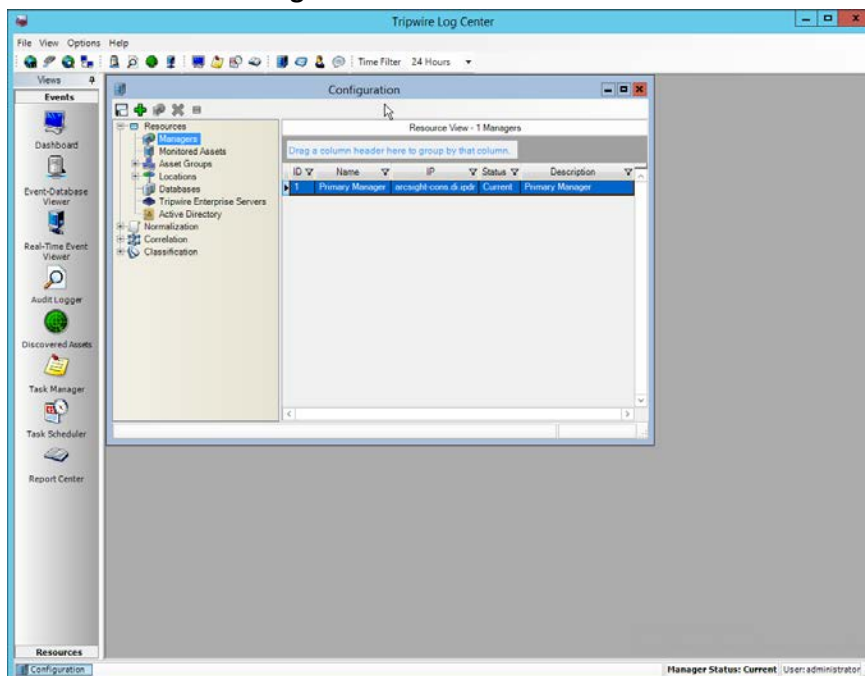
34. Click **Modify**.
35. Enter the **username** of a TLC user account for **User**.
36. Enter the **IP address** of the TLC Manager for **Host**.
37. Enter **"/"** for the **directory**.
38. Select **Active**.
39. Select **SSH2 DSA (sftp)** for **Protocol**.
40. Select **XML2** for **Format**.



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

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

44. Click **Resources > Managers**.



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

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

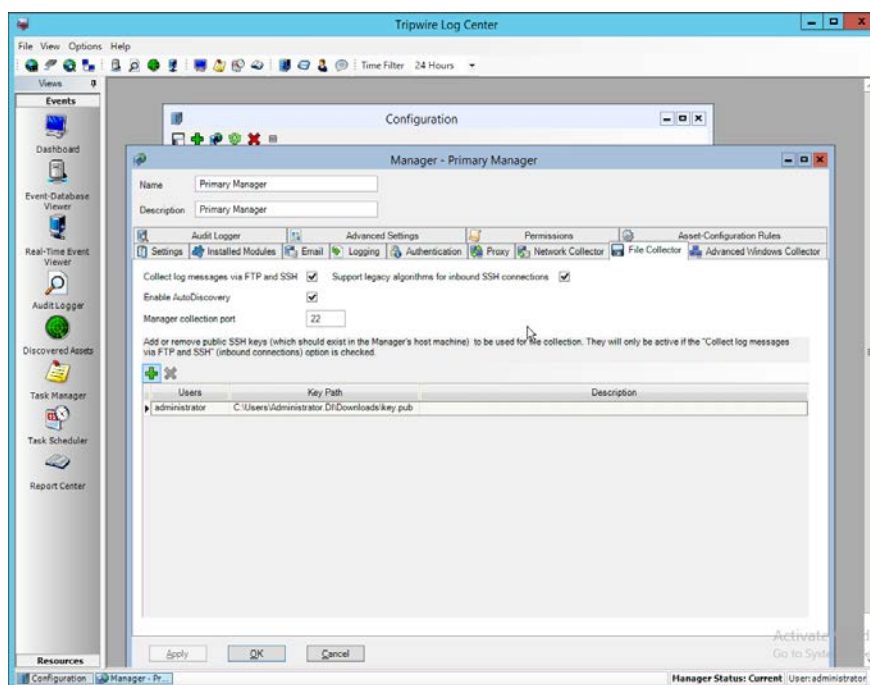
47. Ensure that the **Collect log messages via FTP and SSH** option is enabled.

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

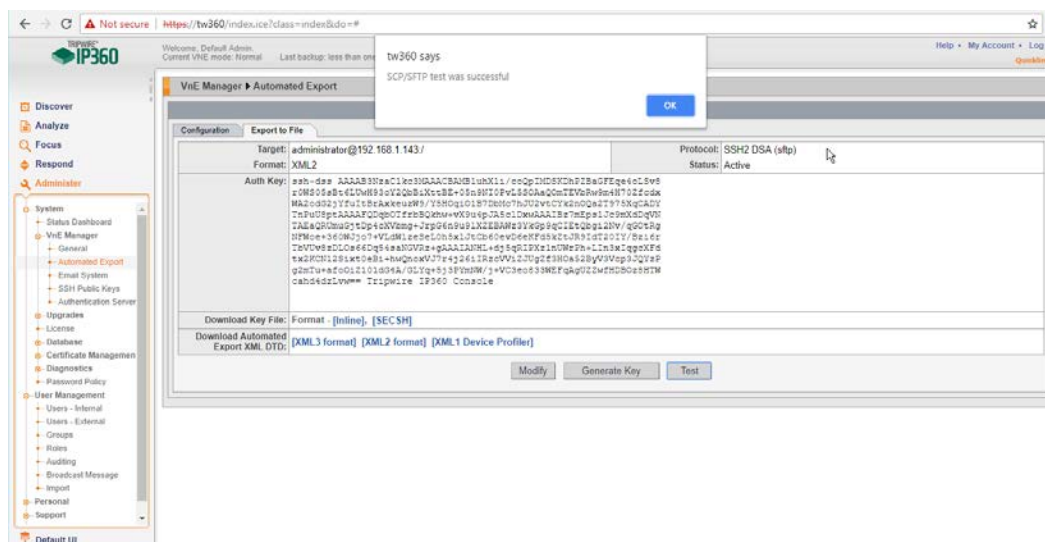
49. Click **Add**.

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

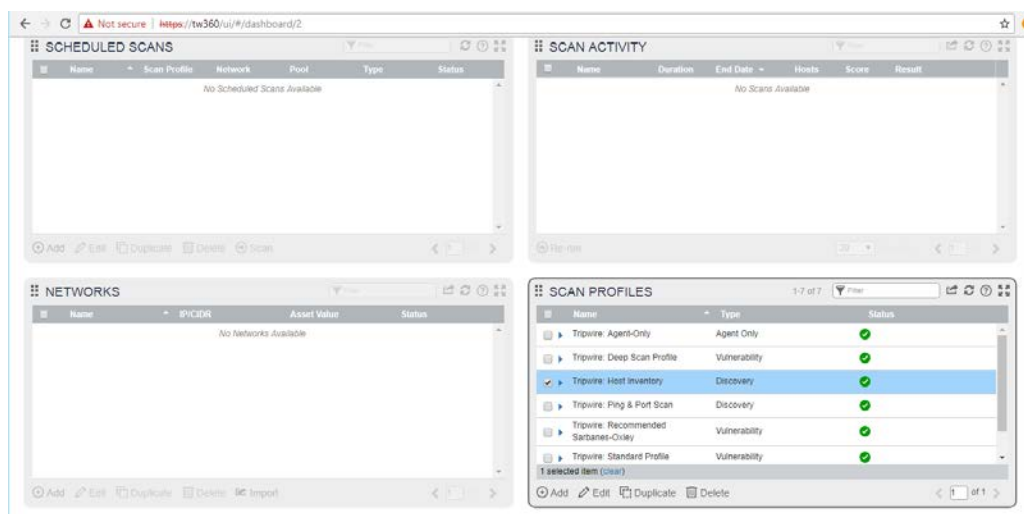
51. Under **Key Path**, enter the path to the downloaded key.



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



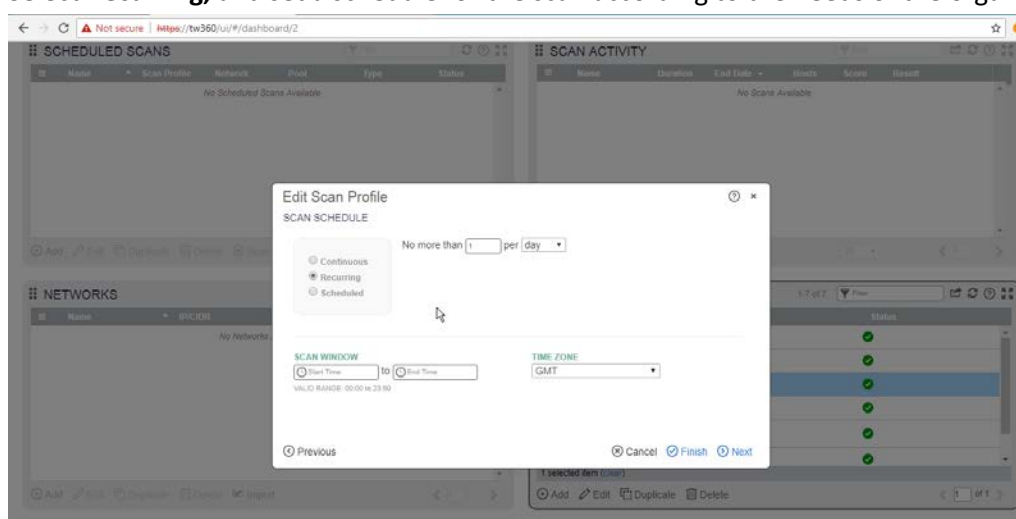
56. Any recurring scans will now forward the scan results to **Tripwire Log Center**. To ensure that a scan is recurring, select a scan in **Scan Profiles** on the main dashboard of the **IP360** web console.



57. Click **Edit**.

58. Click **Next** until the **Scan Schedule** page.

59. Select **Recurring**, and set a schedule for the scan according to the needs of the organization.



60. Click **Finish**.

## 2.20 Integration: Tripwire Enterprise and Backups

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

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



## 2.20.1 Export Configuration from Tripwire Enterprise

1. On the Tripwire Enterprise server, navigate to C:\Program Files\Tripwire\TE\Server\bin.
2. Run the following command to stop **Tripwire Services**.  

```
> twservices stop
```
3. Run the following command to export the configuration files to a backup (replace config.bak with the desired name of the backup).  

```
> tectool backup config.bak
```
4. Run the following command to restart **Tripwire Services**.  

```
> twservices start
```

## 2.20.2 Back Up the Tripwire Enterprise Configuration

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

## 2.21 Integration: Cisco ISE and CryptoniteNXT

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

### 2.21.1 Requirements for Integrating Cisco ISE and CryptoniteNXT

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

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

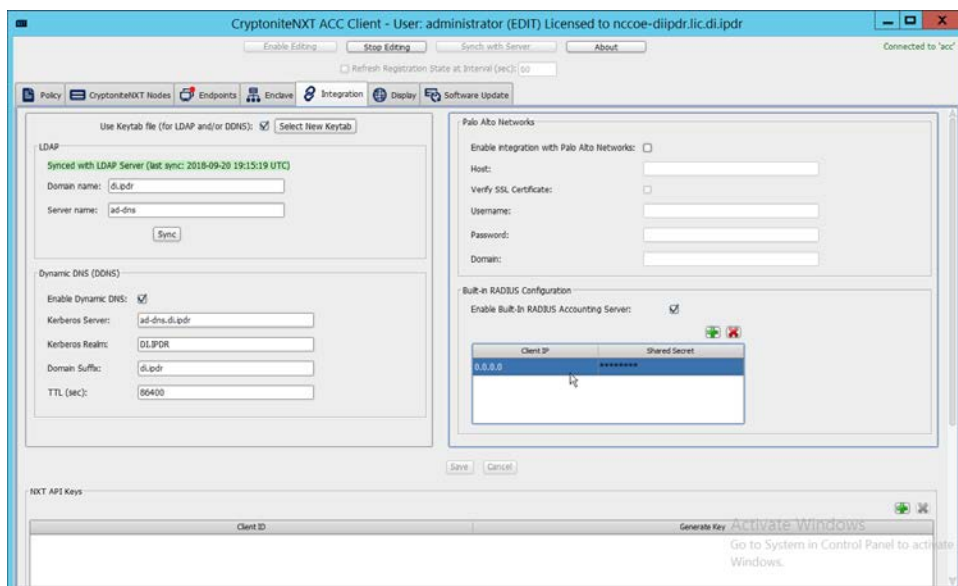
This integration requires the following:

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

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

## 2.21.2 Configuring CryptoniteNXT for RADIUS

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



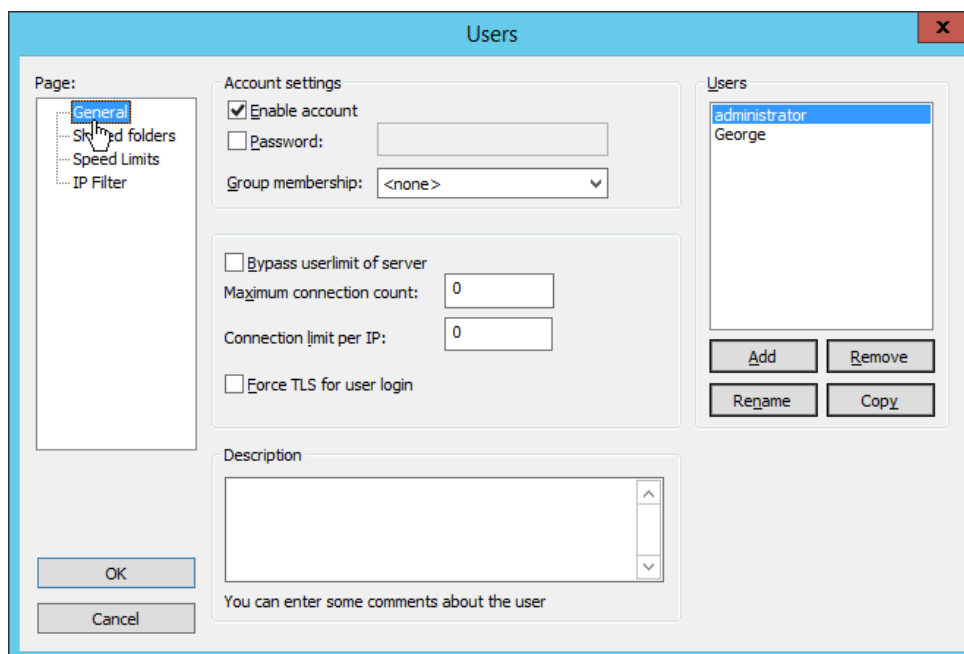
13. Click the **plus button** to add the IP of the switch as well as a shared secret. You can use 0.0.0.0/0 as the IP to accept RADIUS Accounting packets from all IPs, however this is not recommended in production.

## 2.22 Integration: Backups and GreenTec

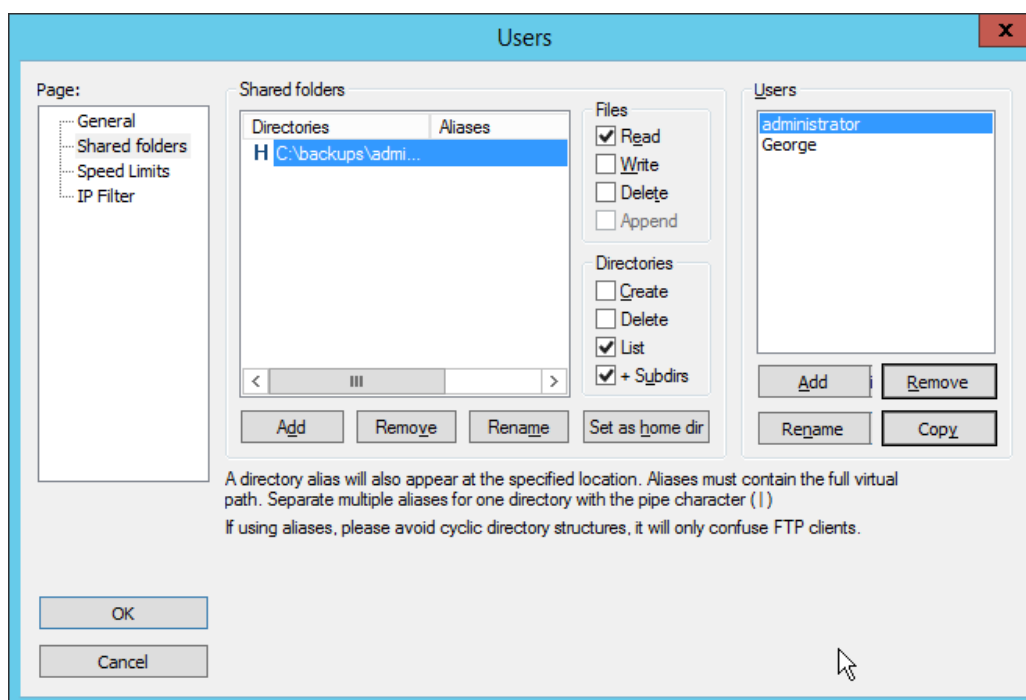
This section details integration between the backup capability and **GreenTec WORMdisks**. Because **GreenTec WORMdisks** provide write protection for files on the disk, they are an ideal place to store important backups. There are a couple options for this integration, but before these backups can be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

### 2.22.1 Locate Backups with FileZilla and Duplicati

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

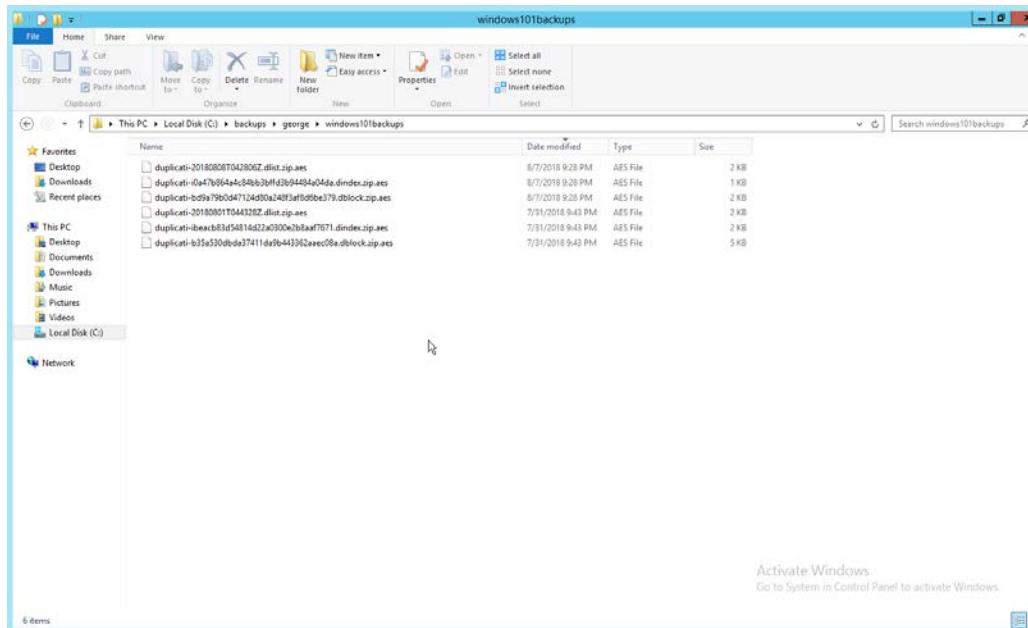


3. Click **Shared folders** in the left pane.



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

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



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

## 2.22.2 Back Up to a GreenTec Disk

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

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

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

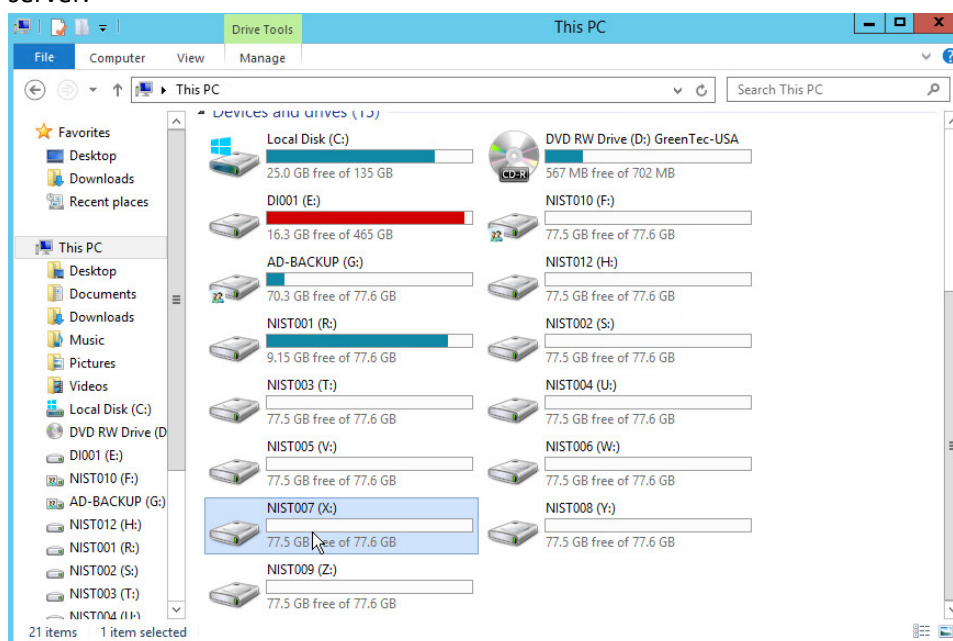
utilizing a backup schedule. This would afford protection for some basic functionality but would forfeit the secure storage capability for day-to-day data.

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

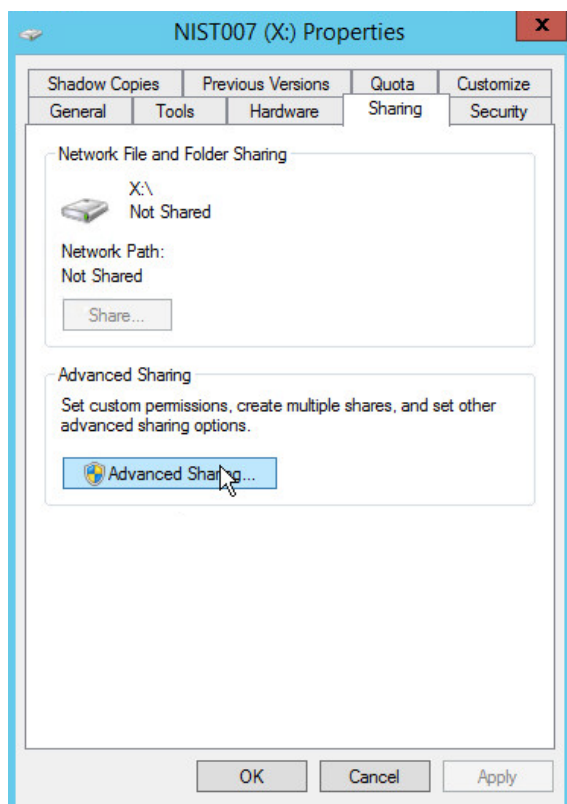
### 2.22.3 Configure Network-Accessible GreenTec Disk

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

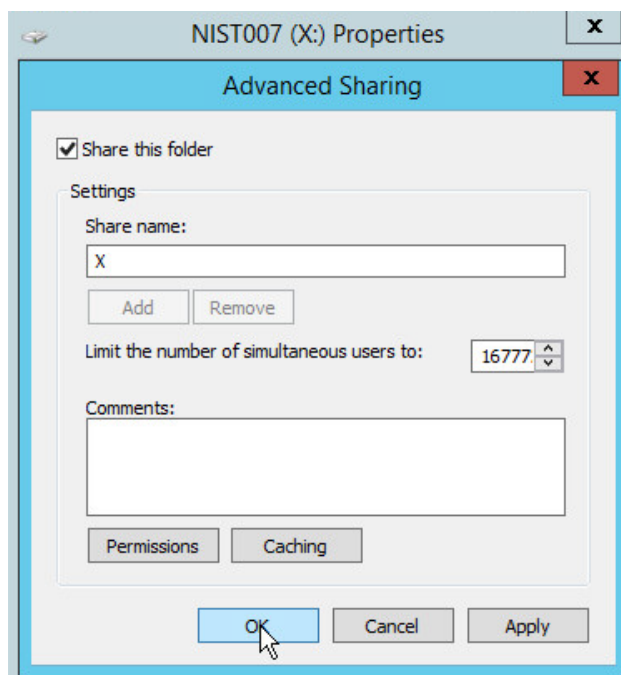
1. To configure a GreenTec disk to be network accessible, right-click the disk on the GreenTec server.



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



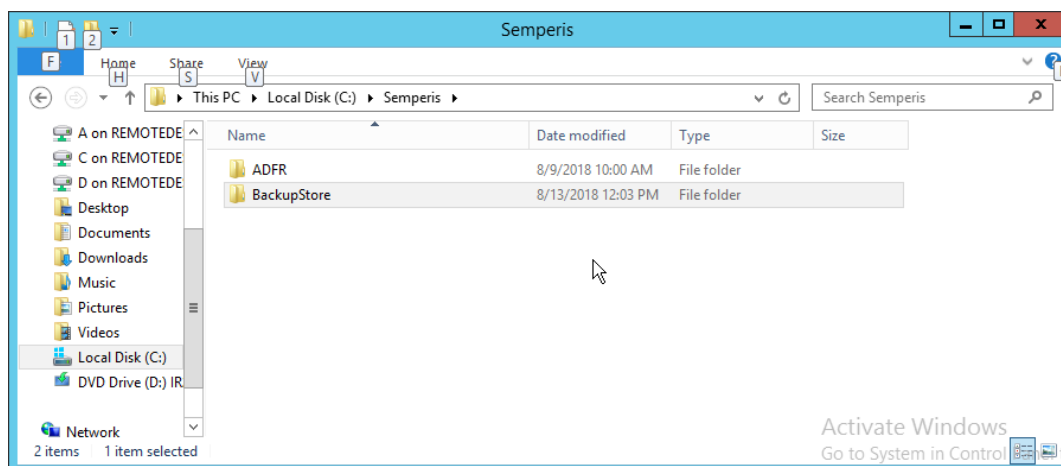
3. Click **Advanced Sharing**.
4. Check the box next to **Share this folder**.
5. Enter a name for the drive if desired.



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

## 2.22.4 Secure Storage for Semperis ADFR

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





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

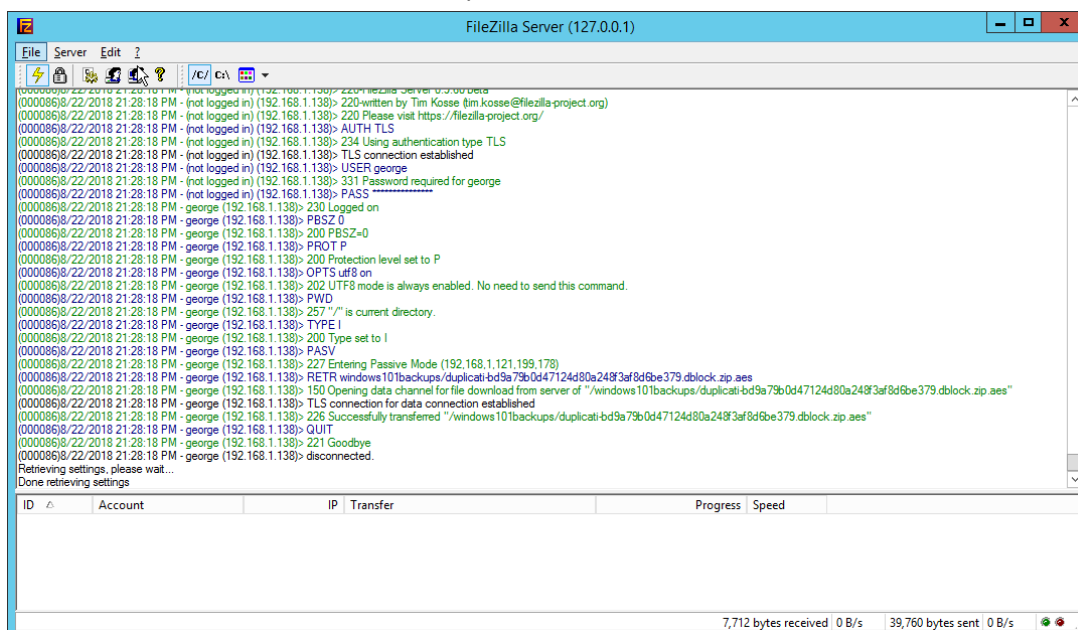
Though these backups can be replicated to WORMdisks, this is currently not supported by Semperis ADFR. Instead, Semperis ADFR offers a different type of “secure storage” by not joining to the domain, allowing the machine to be taken offline and brought online only during creation/application of a backup.

## 2.23 Integration: Micro Focus ArcSight and FileZilla

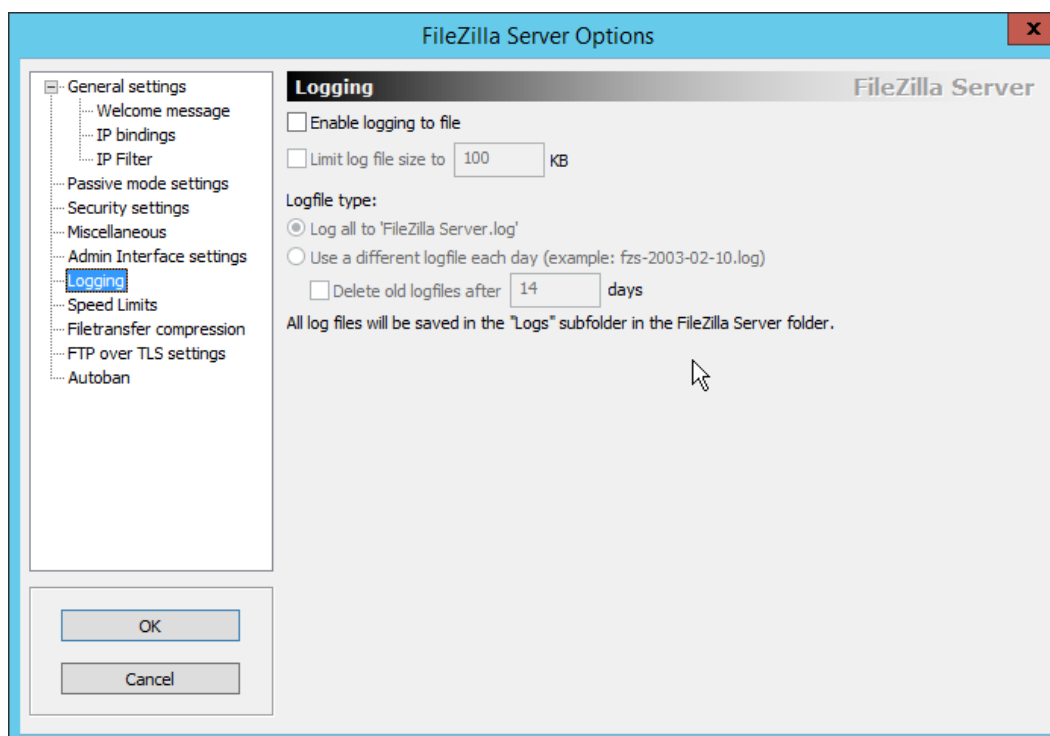
In this section an integration between ArcSight and FileZilla is detailed so that logs from FileZilla are forwarded to ArcSight by using an ArcSight syslog file connector.

### 2.23.1 Enable Logs in FileZilla

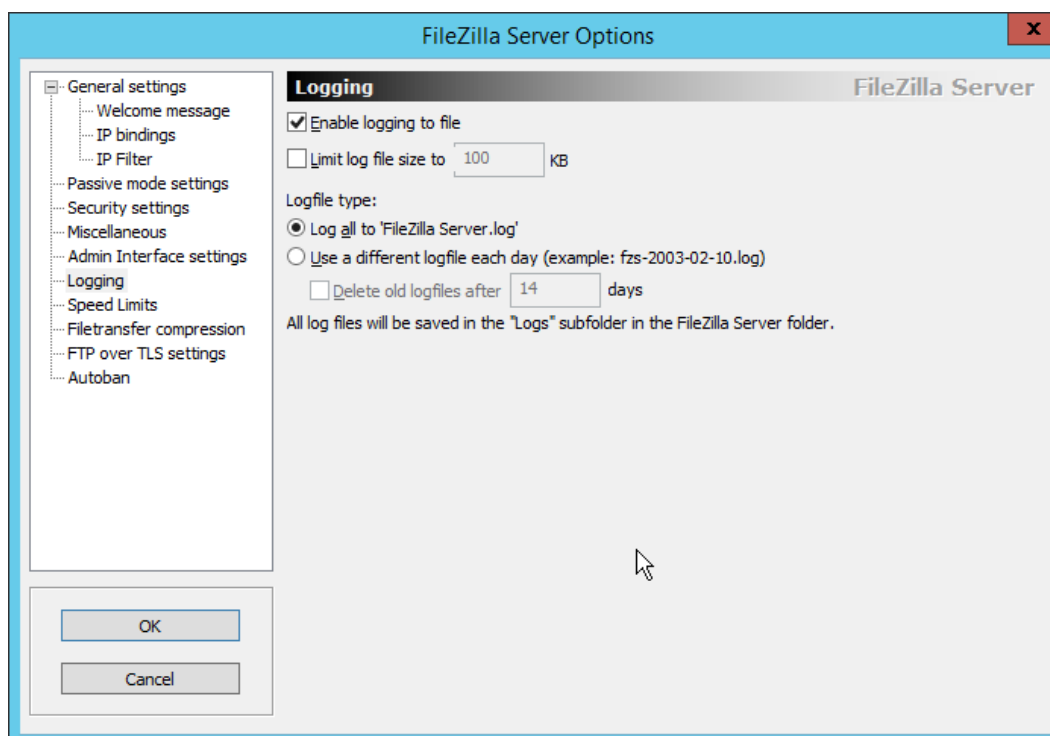
1. On the server with **FileZilla** installed, open **FileZilla Server**.



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



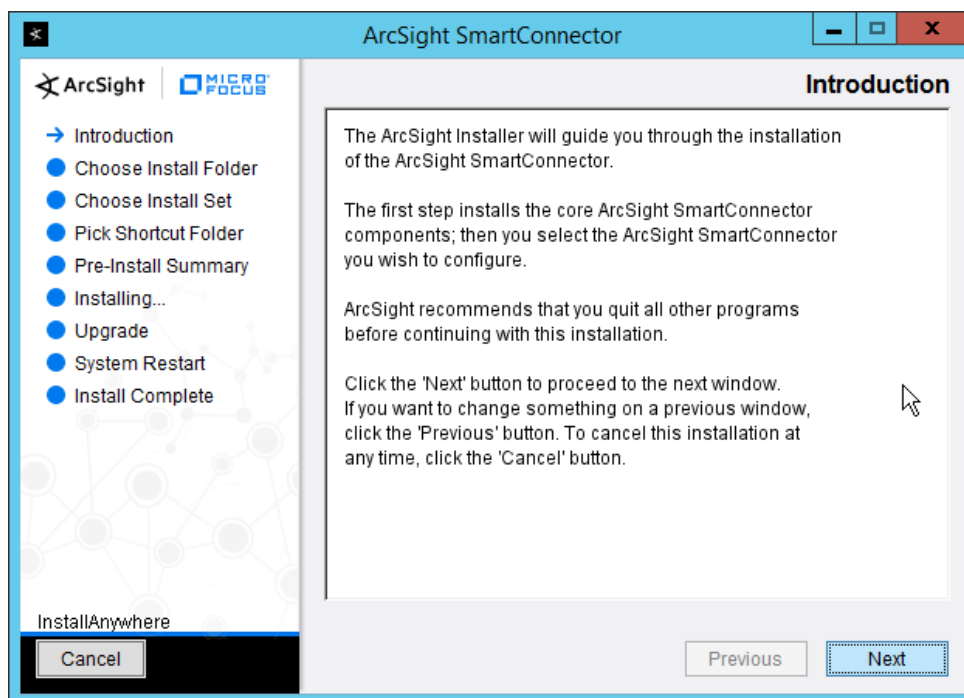
4. Check the box next to **Enable logging to file**.



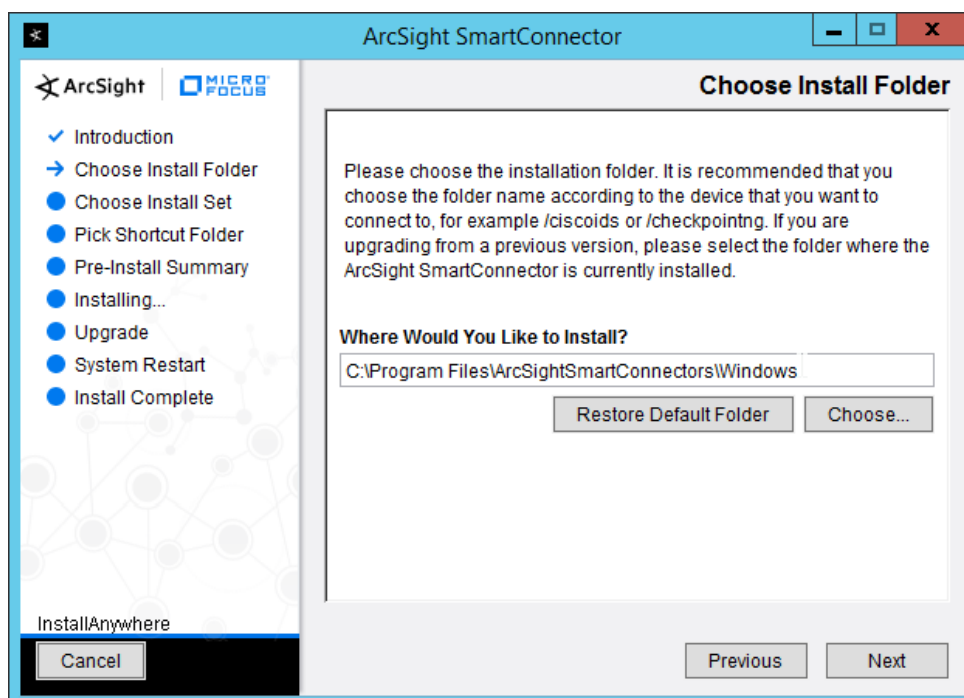
5. Click **OK**.

## 2.23.2 Install Micro Focus ArcSight

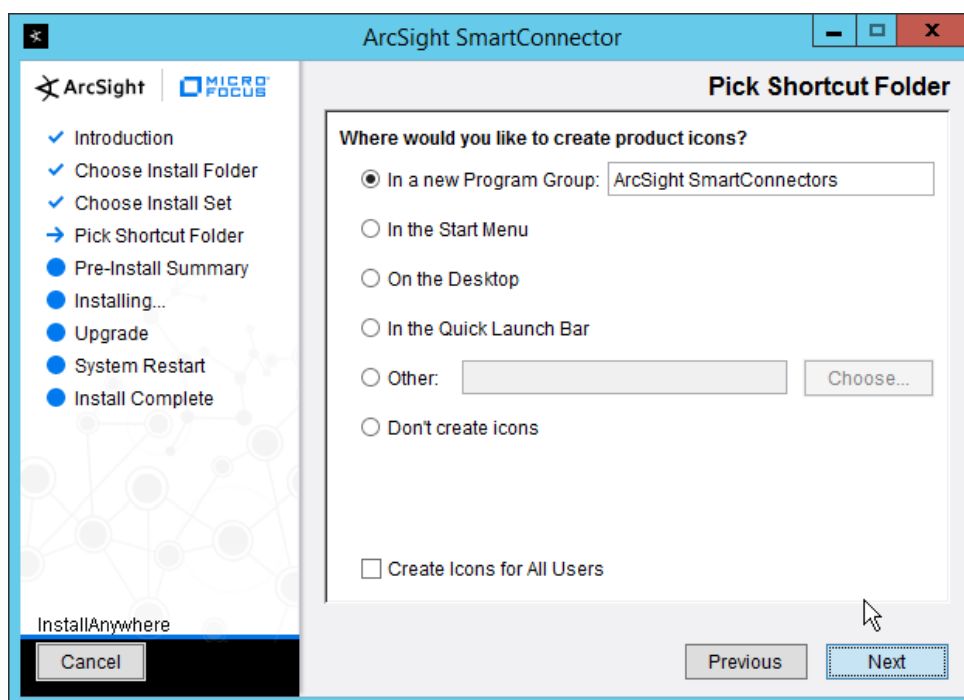
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



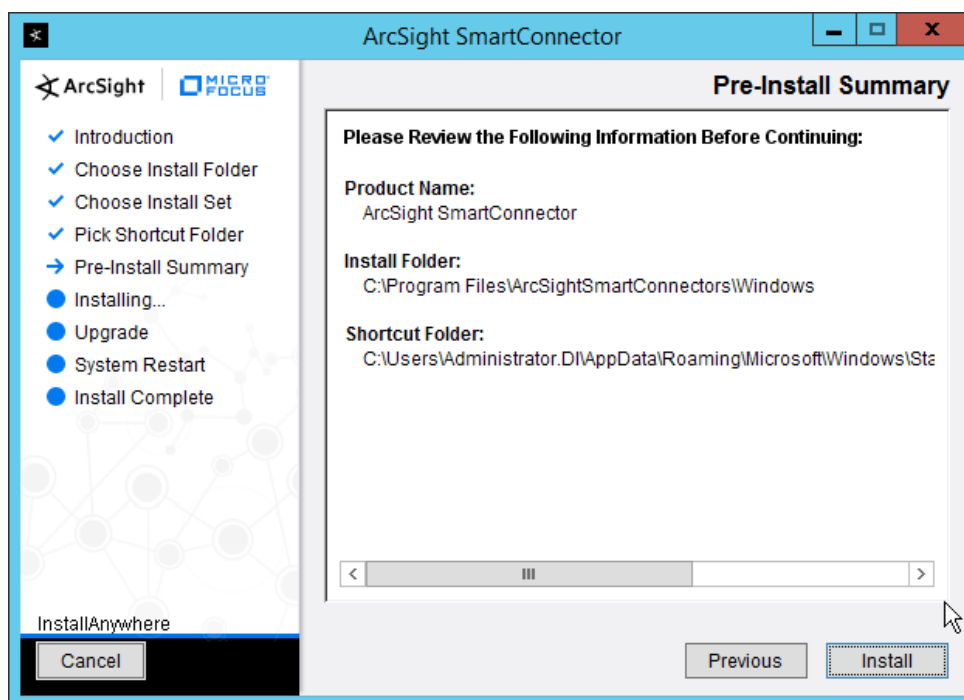
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



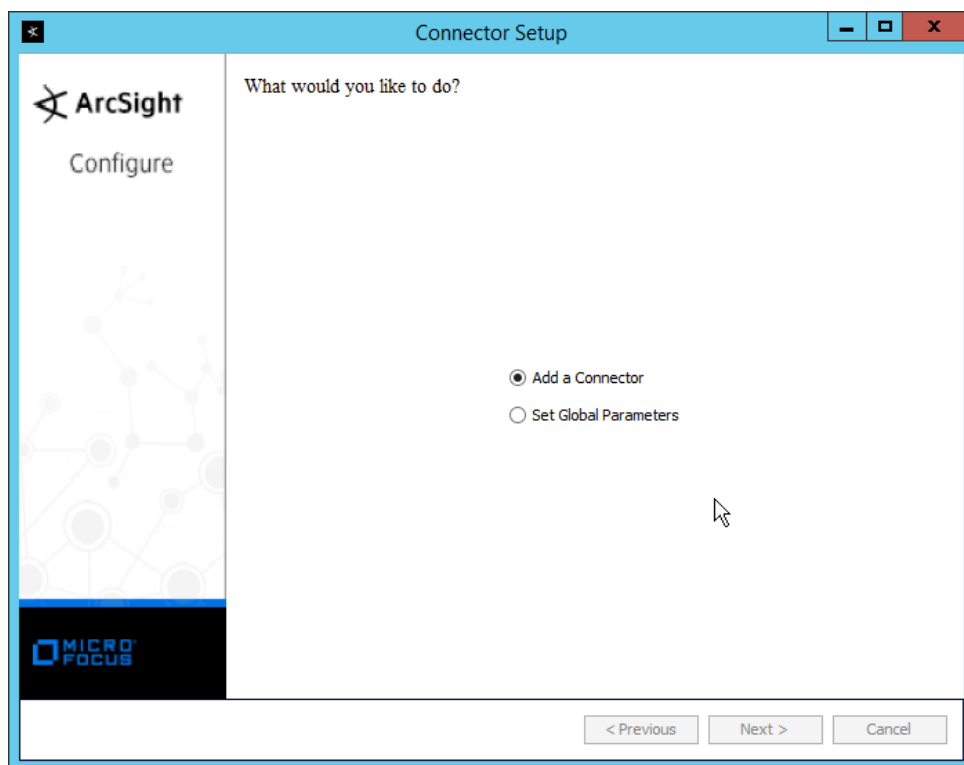
4. Click **Next**.



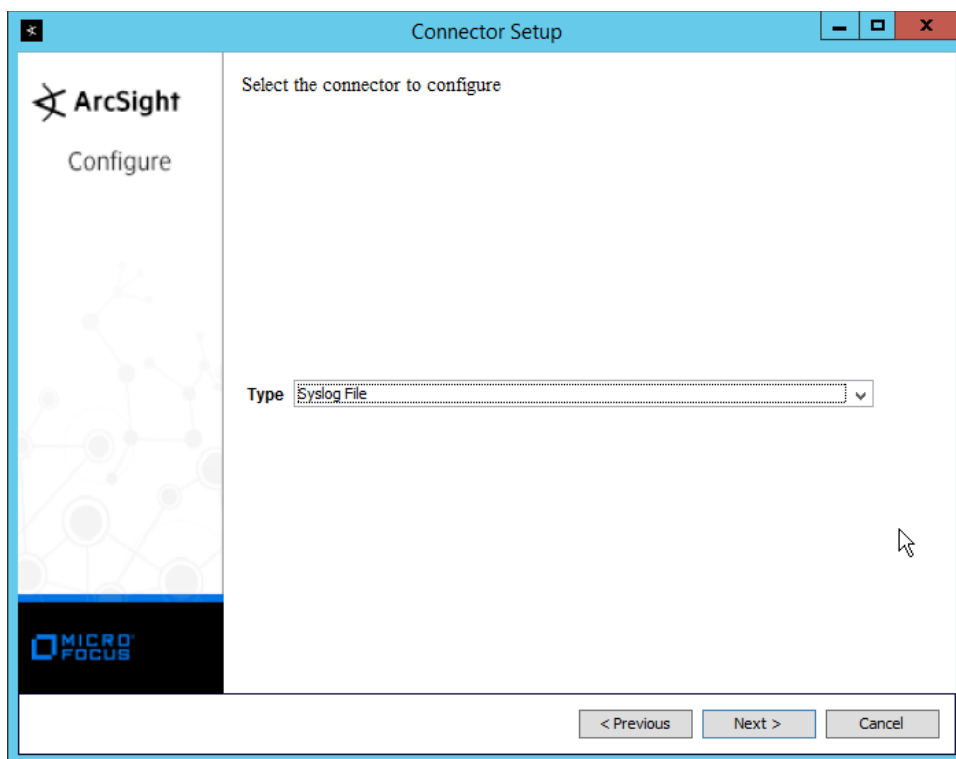
5. Click **Next**.



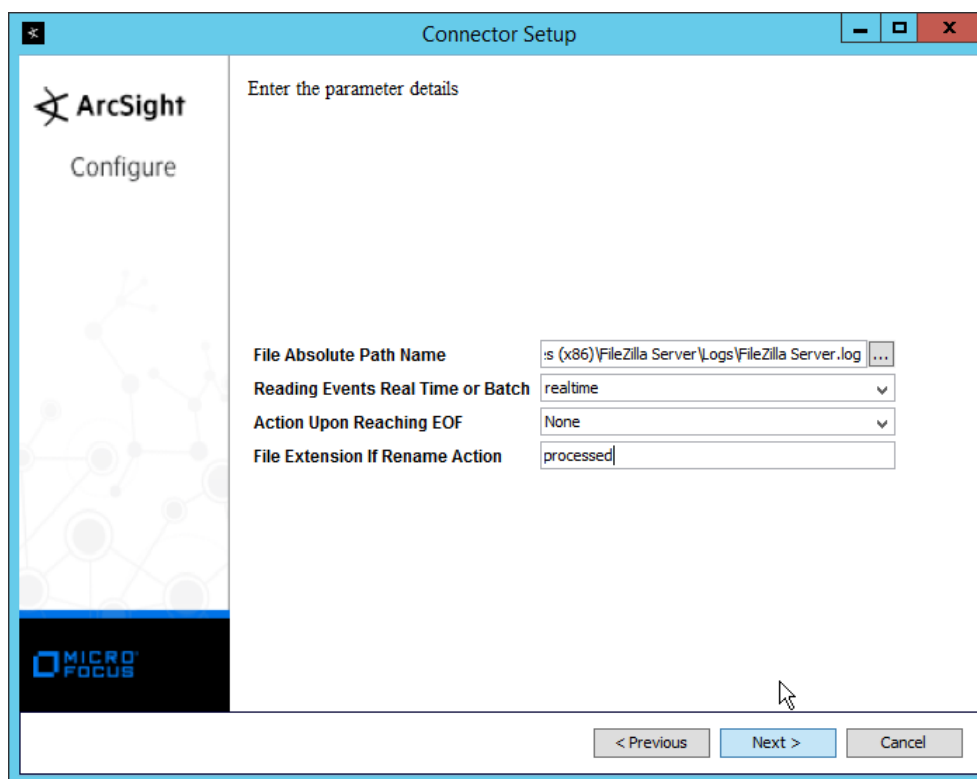
6. Click **Install**.
7. Select **Add a Connector**.



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

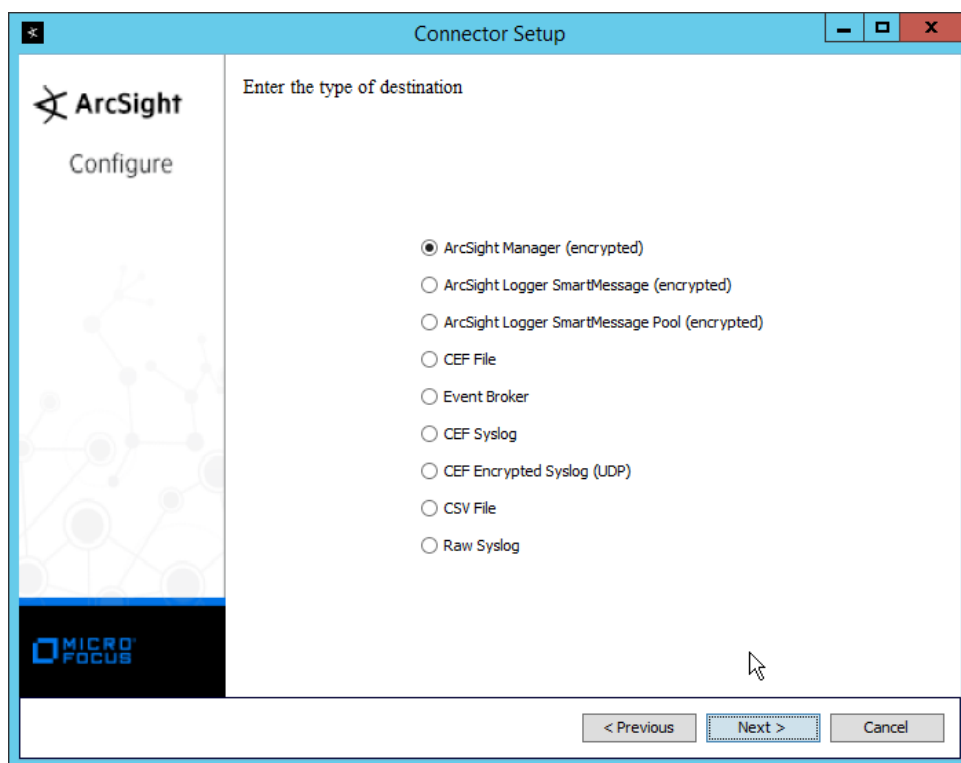


10. Click **Next**.
11. Enter C:\Program Files (x86)\FileZilla Server\Logs\FileZilla Server.log for **File Absolute Path Name**.



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





14. Click **Next**.

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

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: FileZilla Logs

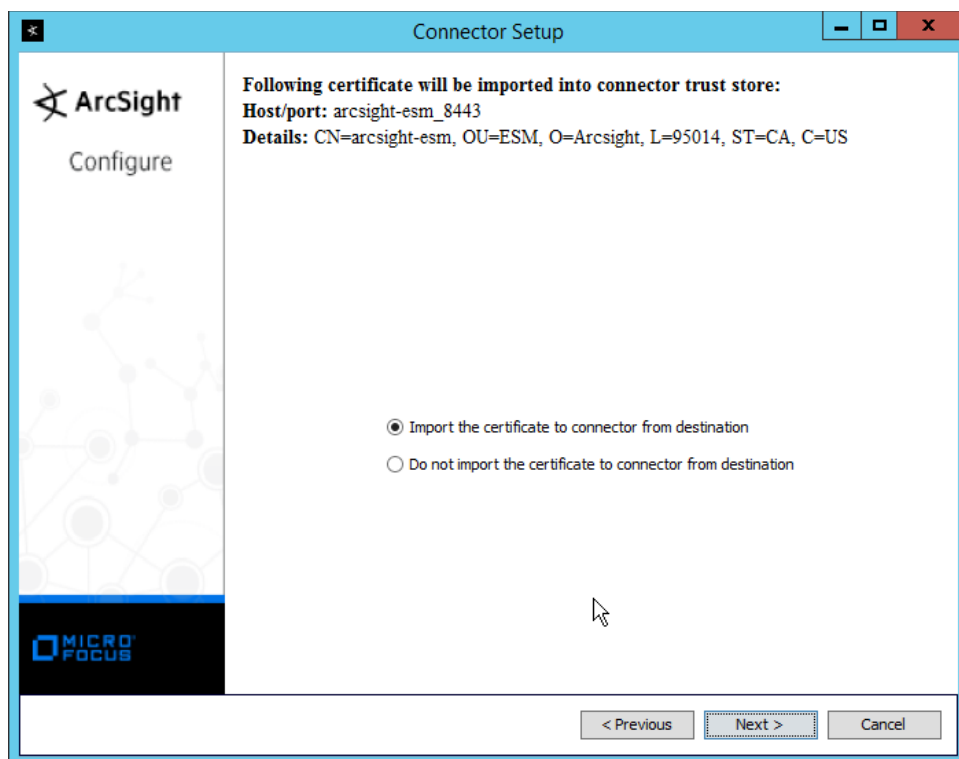
Location:

DeviceLocation:

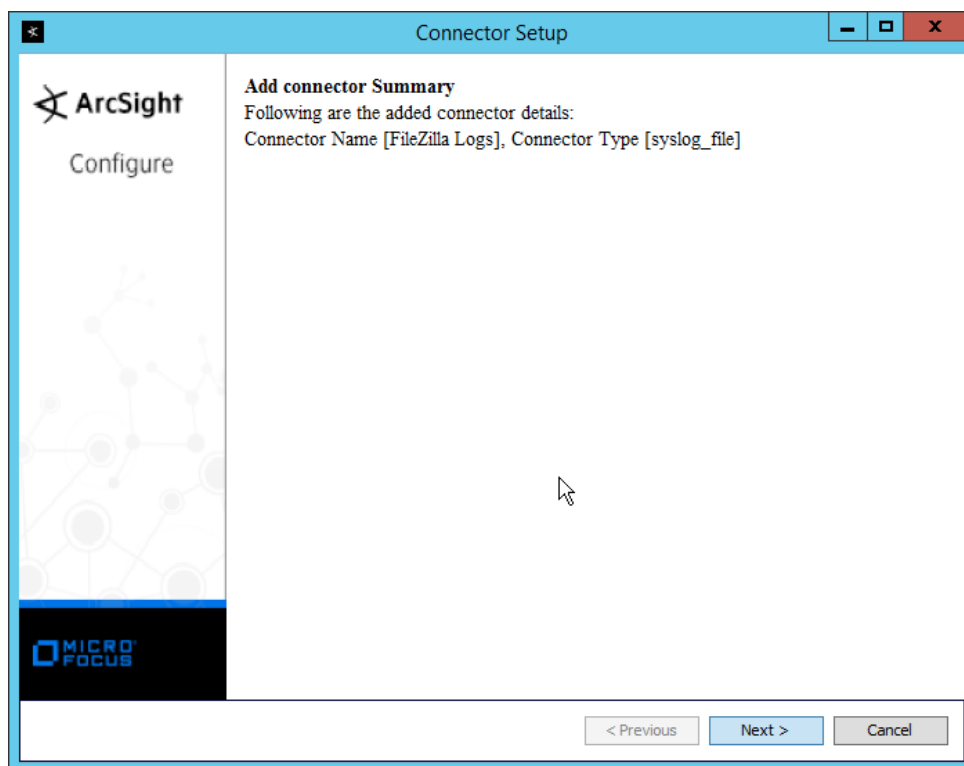
Comment:

< Previous   Next >   Cancel

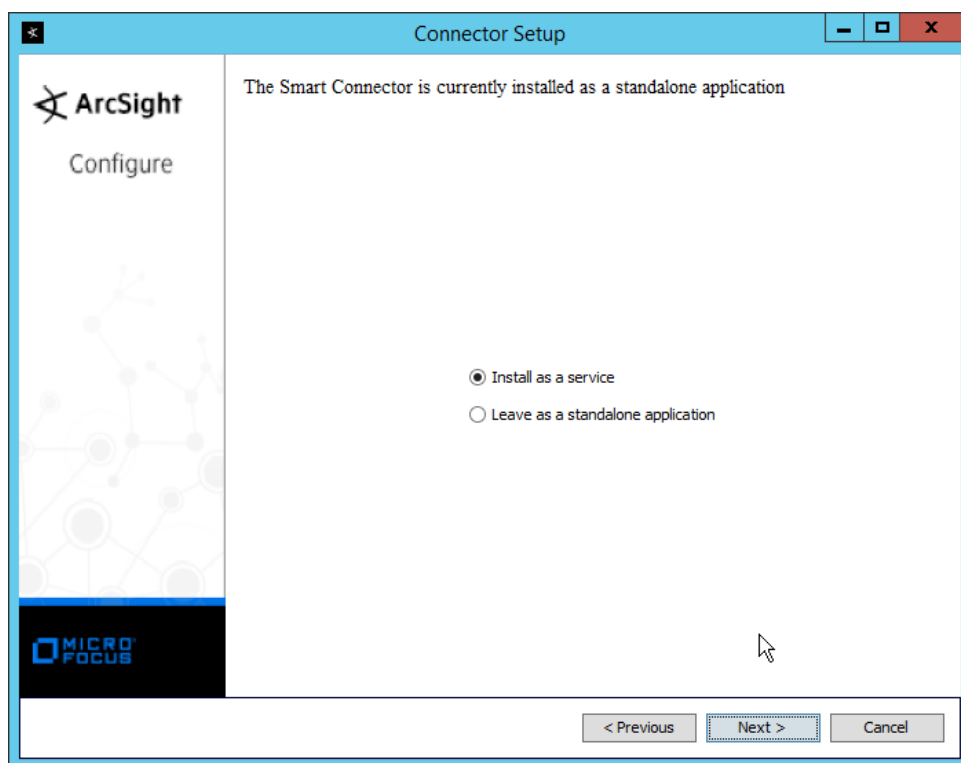
18. Click **Next**.
19. Select **Import the certificate to connector from destination**.



20. Click **Next**.



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



23. Click **Next**.

Connector Setup

ArcSight  
Configure

Specify the service parameters

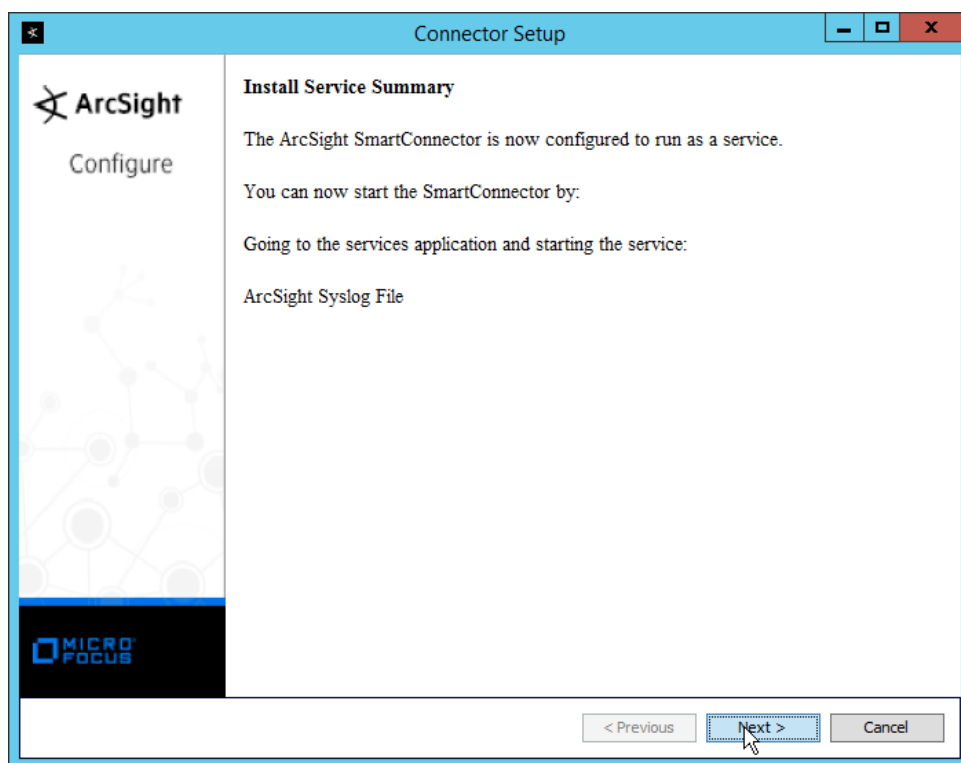
Service Internal Name: syslog\_file

Service Display Name: Syslog File

Start the service automatically: Yes

< Previous   Next >   Cancel

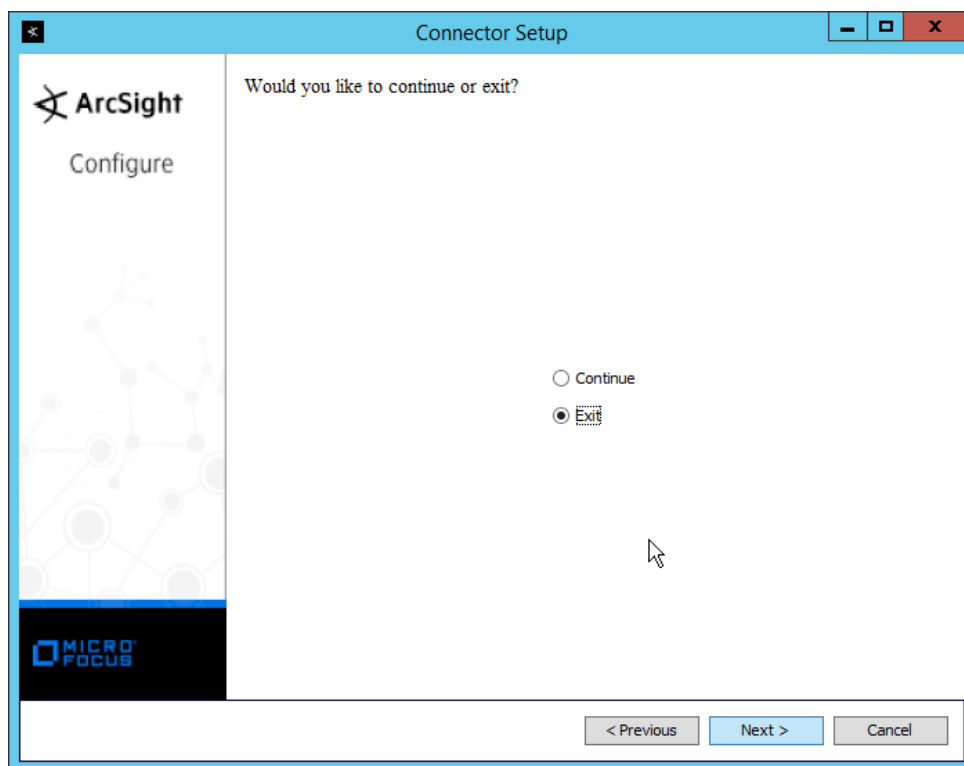
24. Click **Next**.



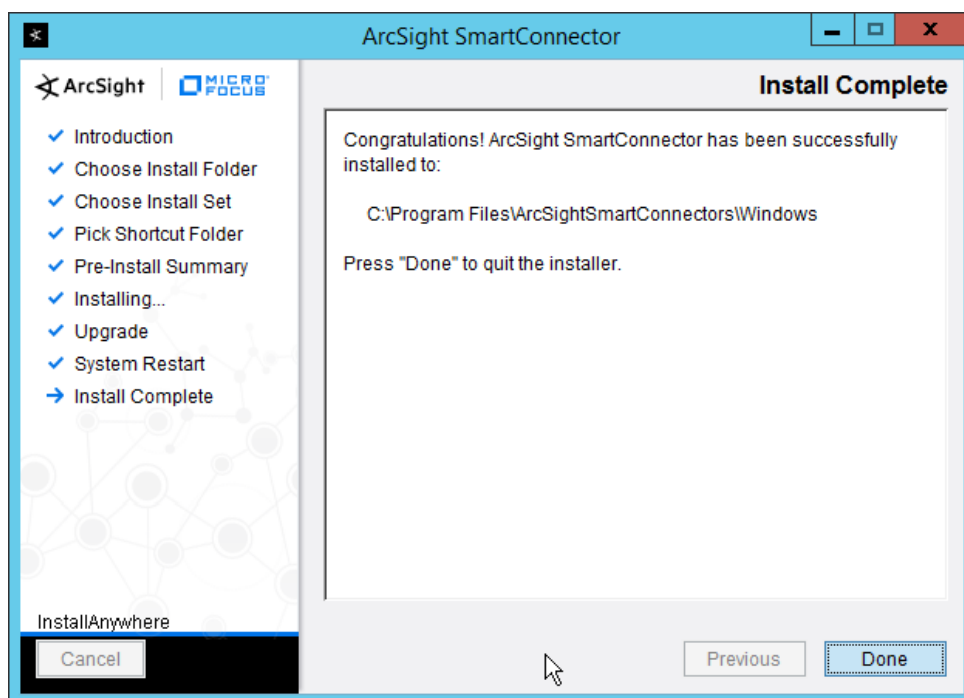
25. Click **Next**.

26. Select **Exit**.





27. Click **Next**.



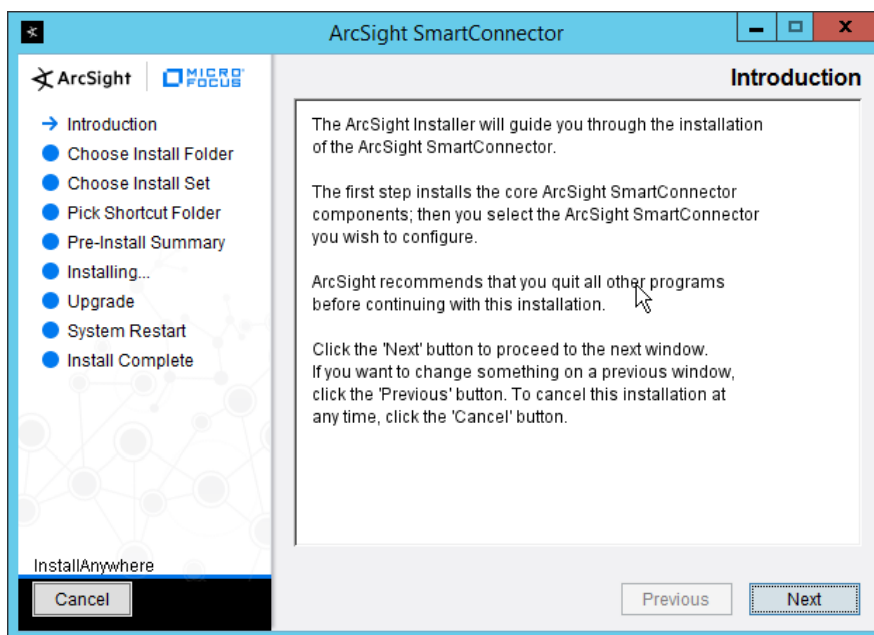
28. Click **Done**.

## 2.24 Integration: Micro Focus ArcSight and Tripwire

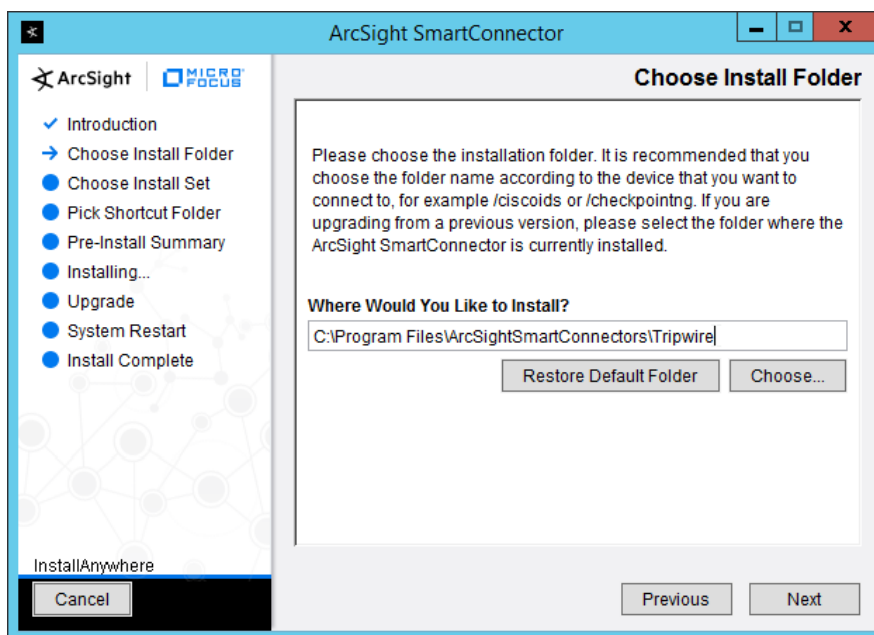
This section details forwarding logs from **Tripwire Log Center** to **Micro Focus ArcSight**. This will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight**, assuming those logs are being collected by **Tripwire Log Center**.

### 2.24.1 Install Micro Focus ArcSight

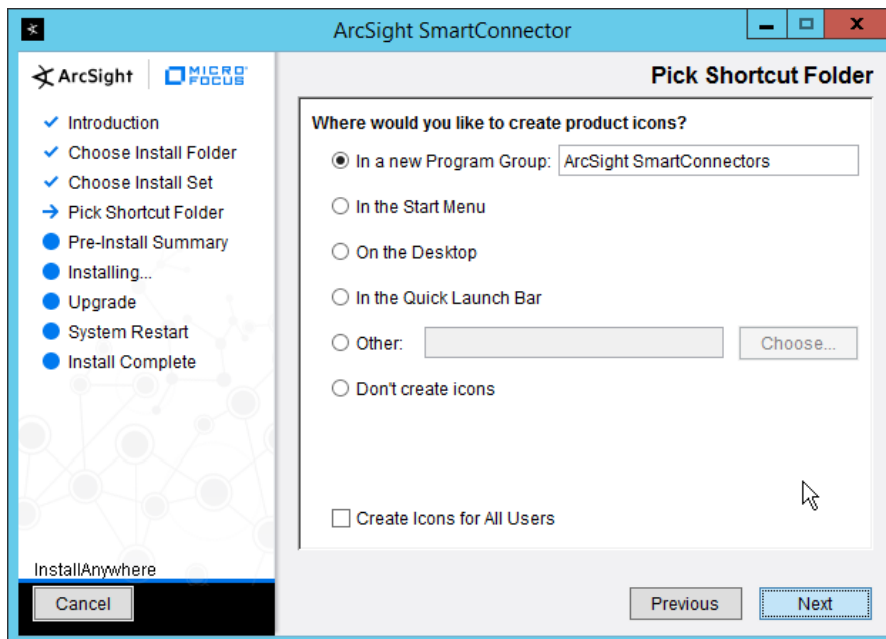
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running Tripwire Log Center.



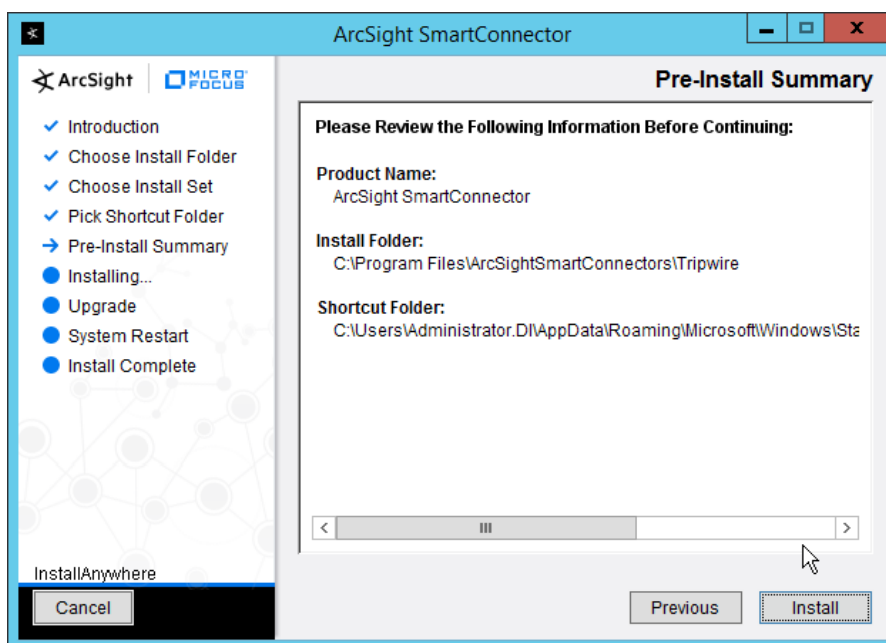
2. Click **Next**.



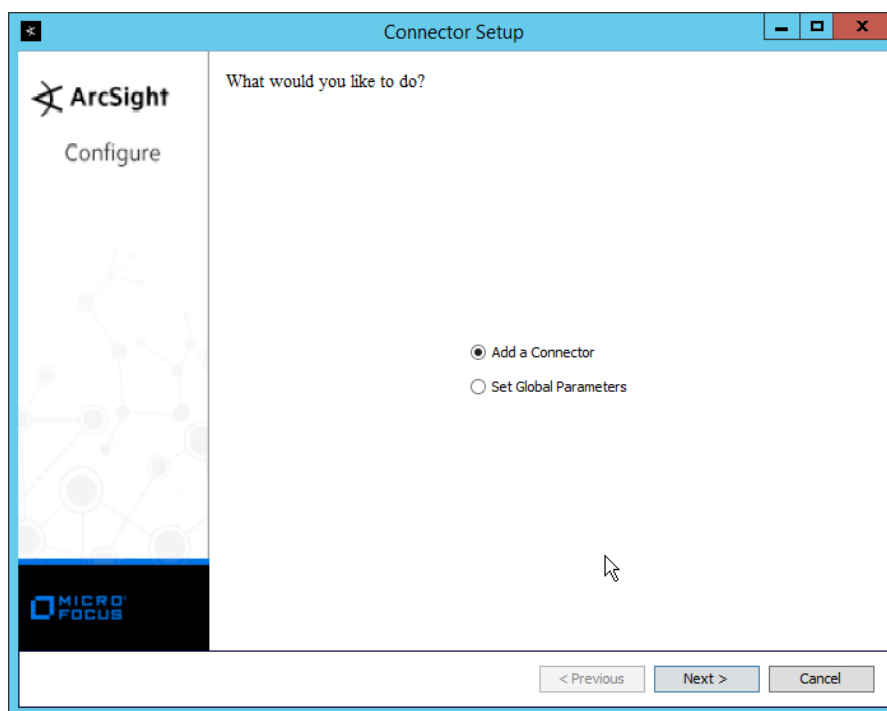
3. Enter C:\Program Files\ArcSightSmartConnectors\Tripwire.



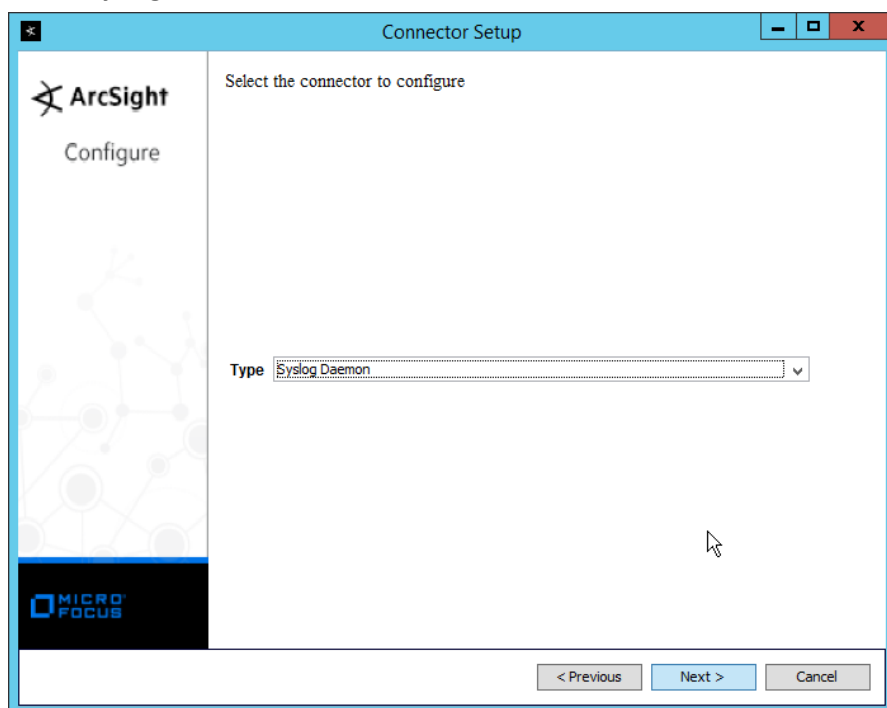
4. Click **Next**.



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



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



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

Connector Setup

ArcSight  
Configure

Enter the parameter details

Network Port: 514

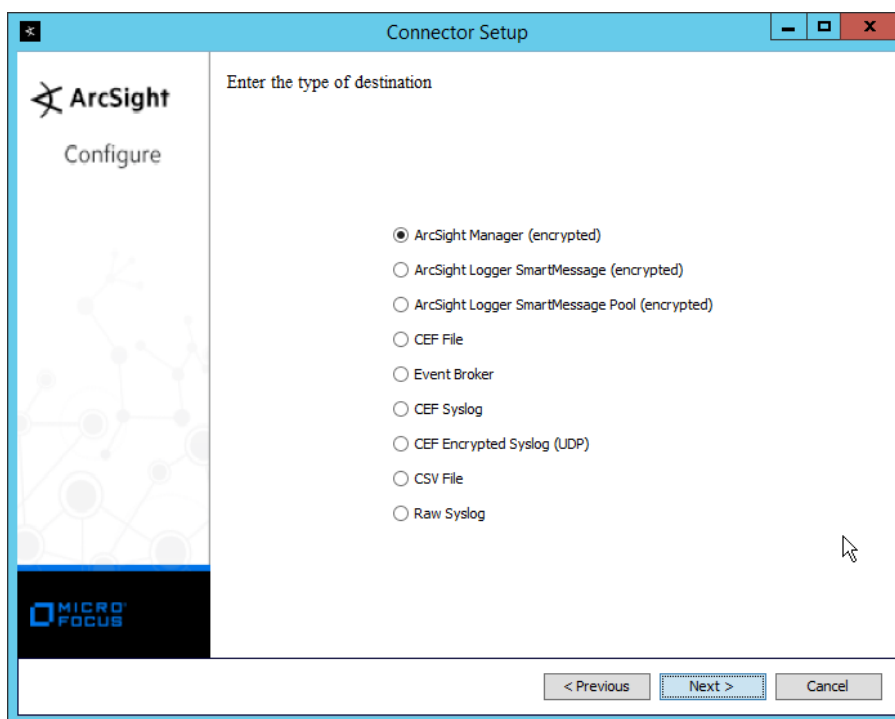
IP Address: (ALL)

Protocol: Raw TCP

Forwarder: false

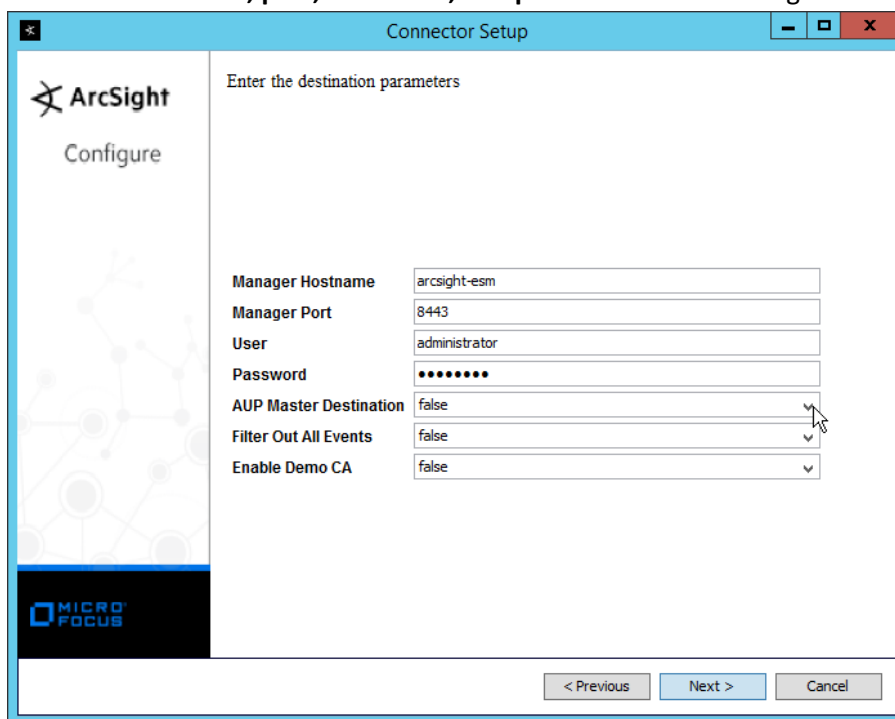
< Previous   Next >   Cancel

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

Location

DeviceLocation

Comment

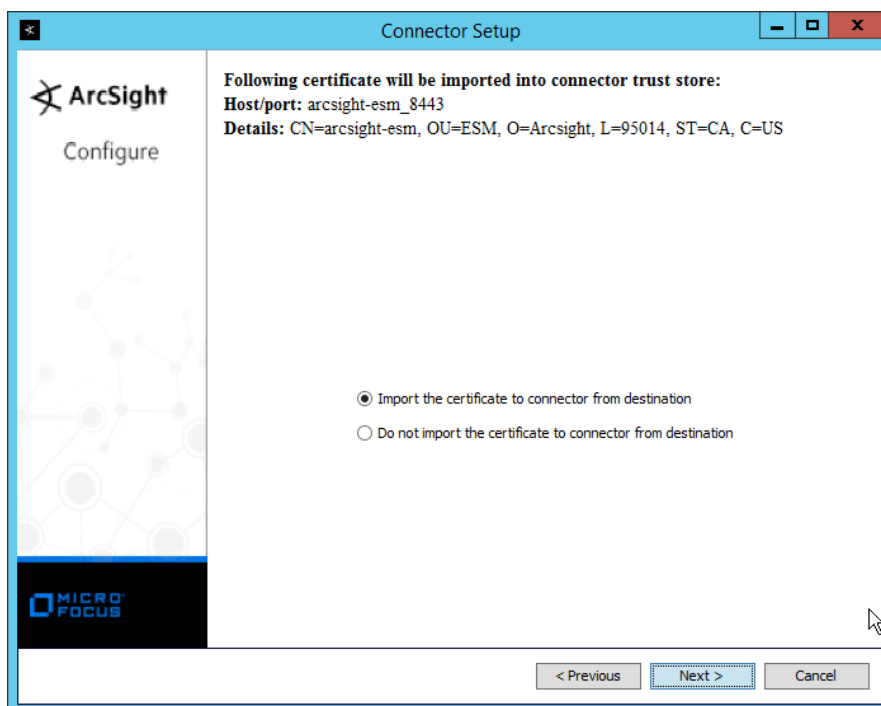
MICRO FOCUS

< Previous   Next >   Cancel

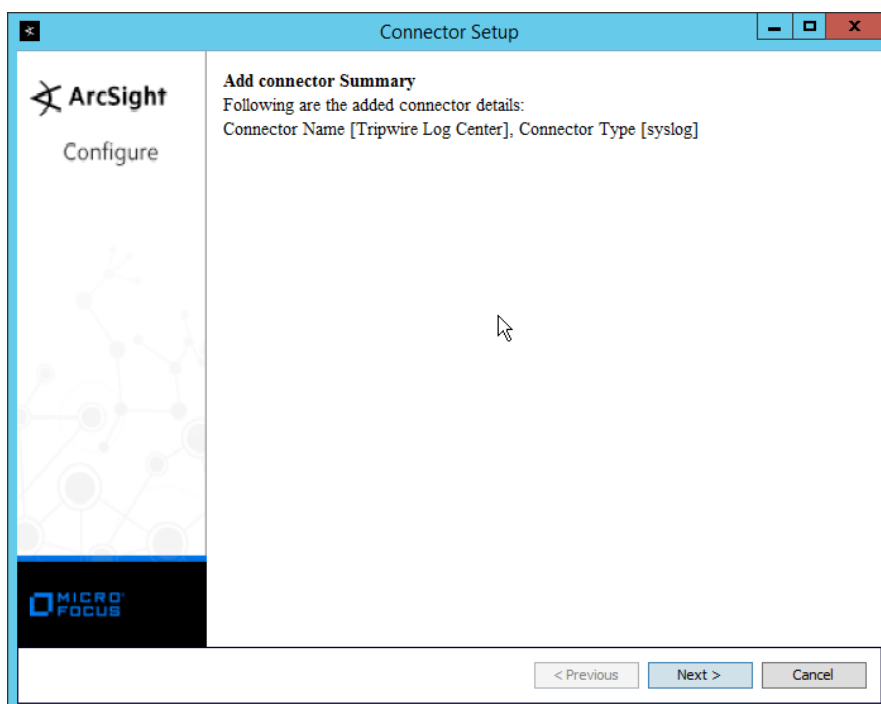
18. Click **Next**.

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



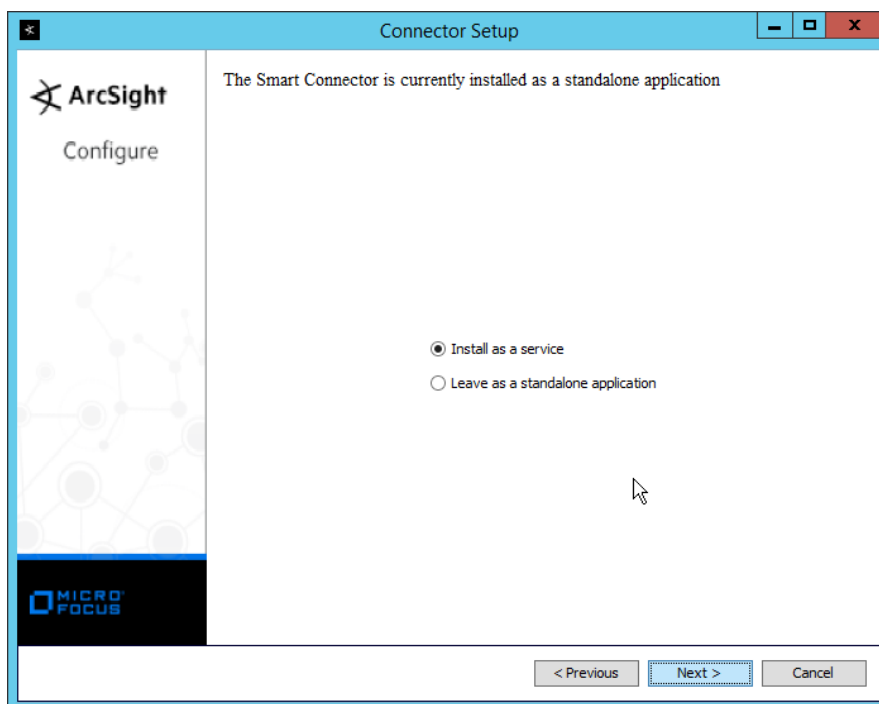


20. Click **Next**.

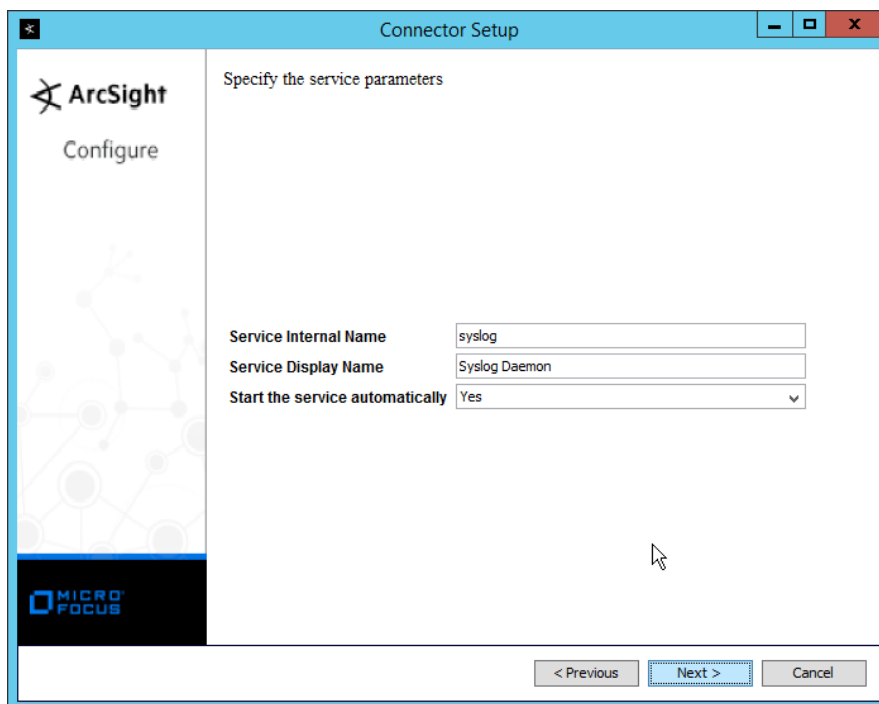


21. Click **Next**.

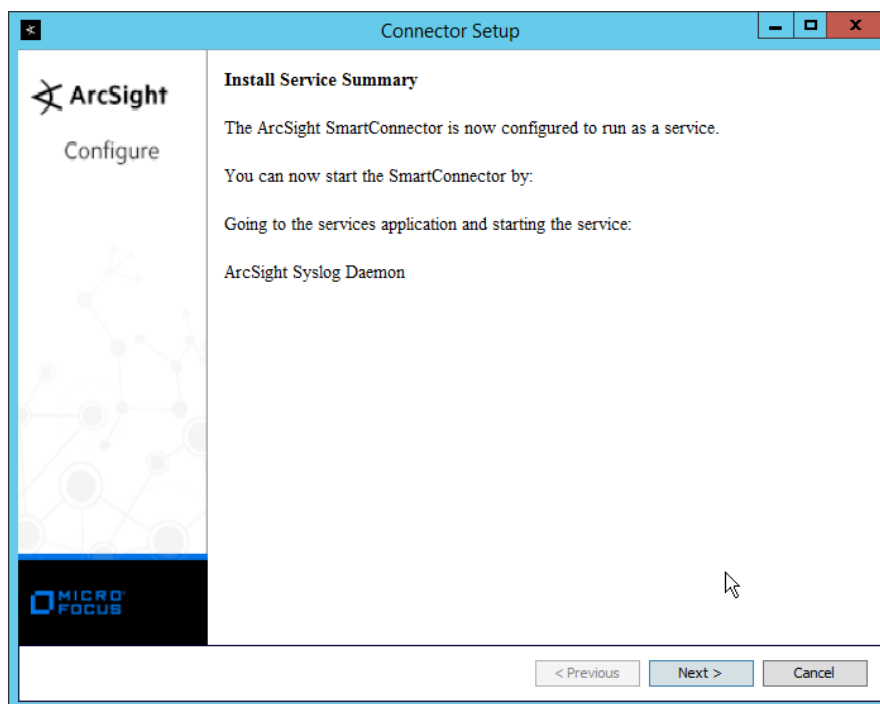
22. Select **Install as a service**.



23. Click **Next**.

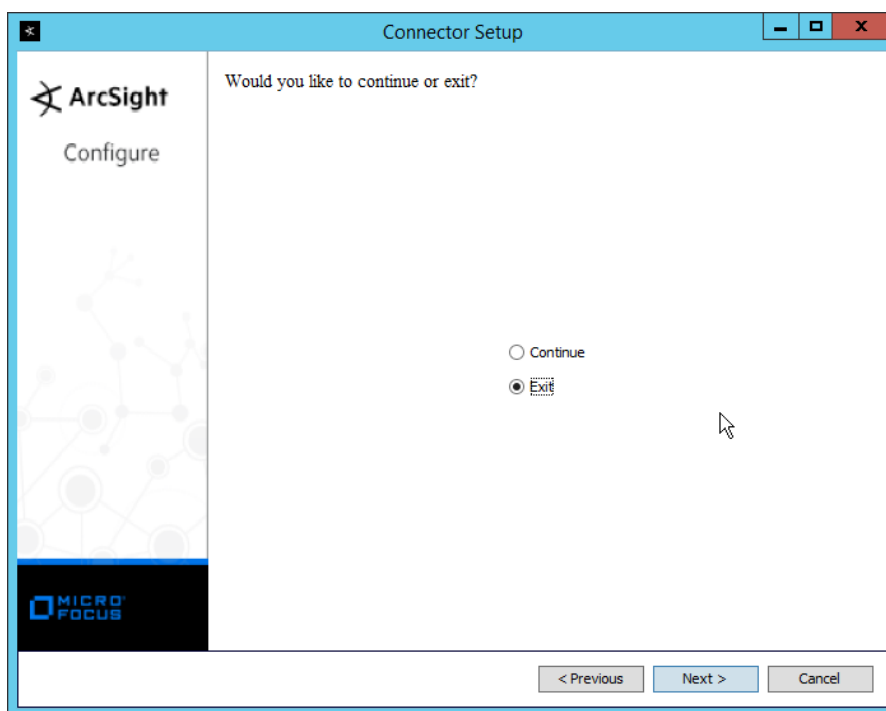


24. Click **Next**.

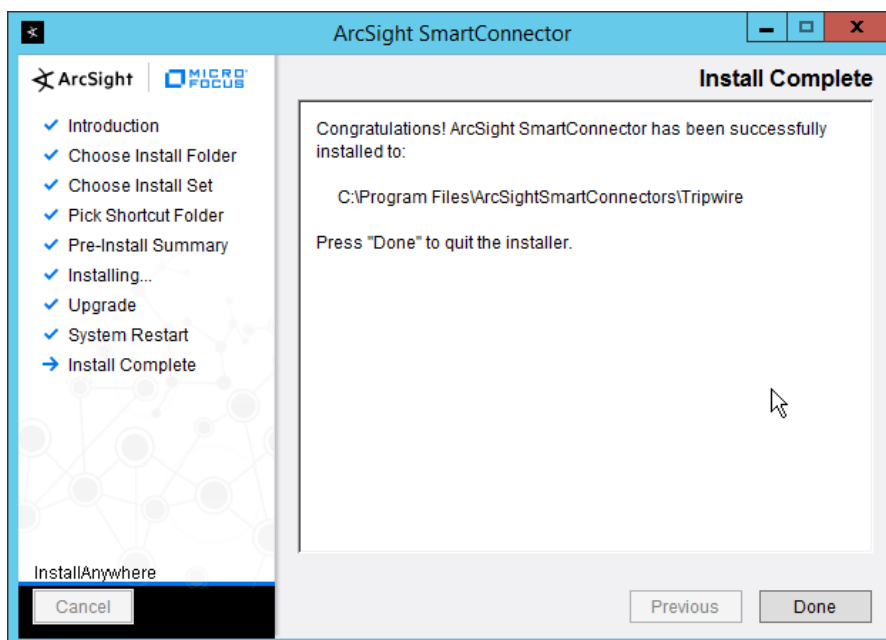


25. Click **Next**.

26. Select **Exit**.



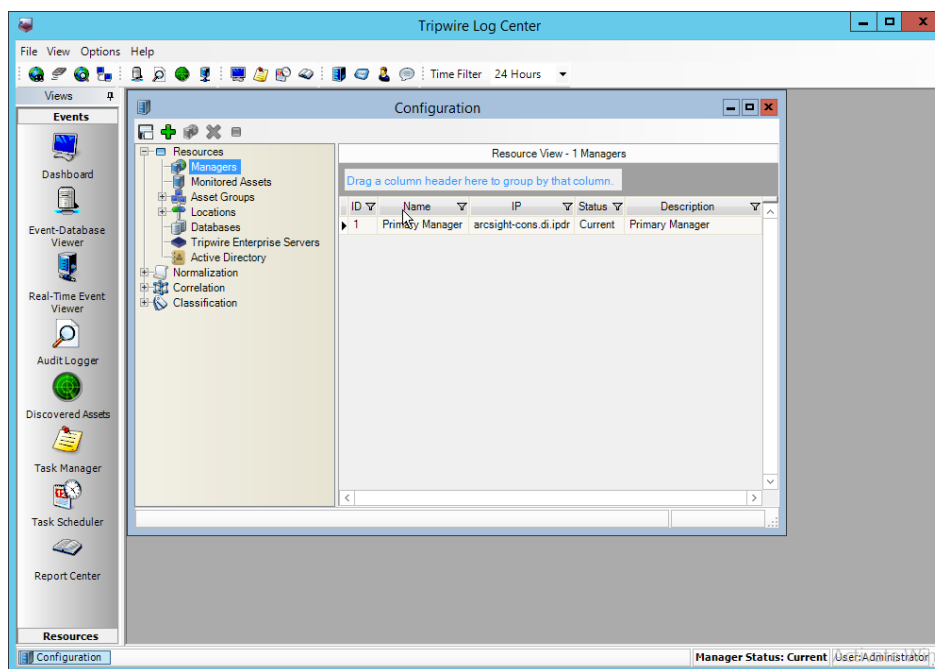
27. Click **Next**.



28. Click **Done**.

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

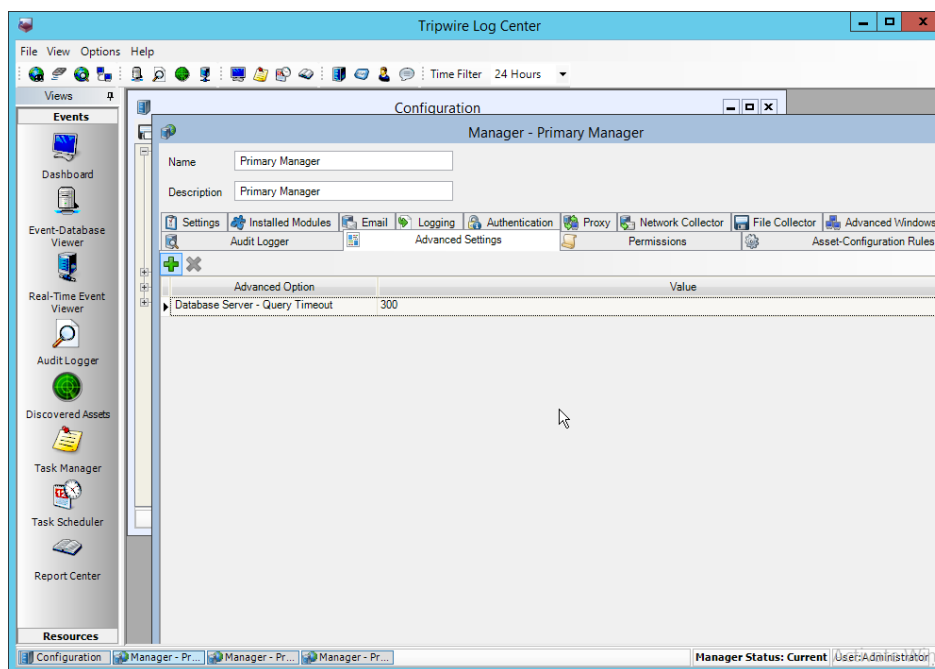
30. Go to the **Configuration Manager**.



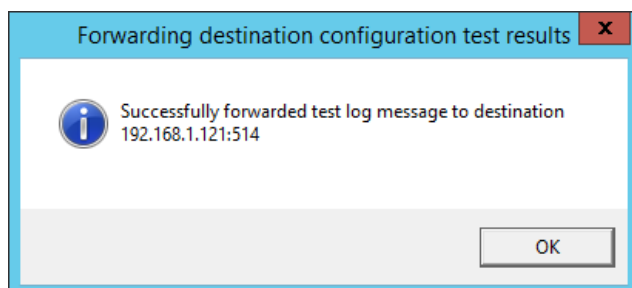
31. Select **Resources > Managers**.

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

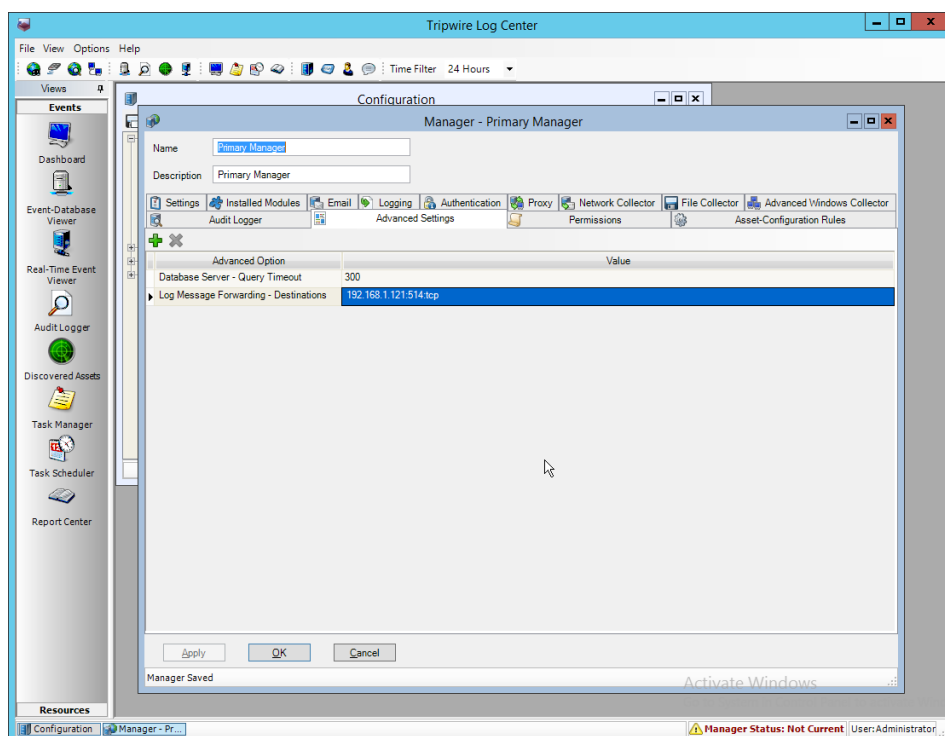
33. Click the **Advanced Settings** tab.



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



37. Click **OK**.



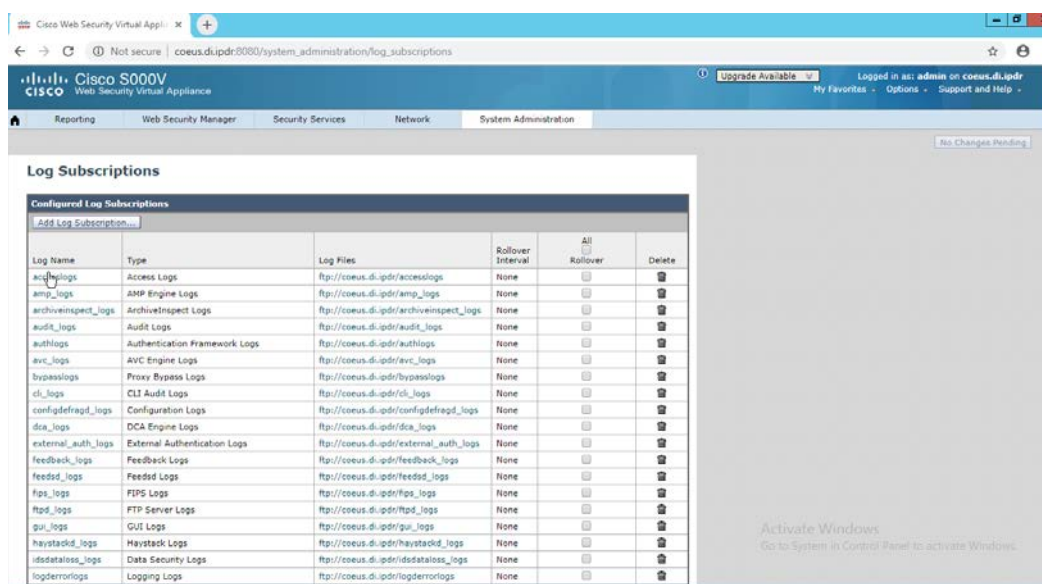
38. Click **OK**.
39. Restart the **Tripwire Log Center Manager**.

## 2.25 Integration: Micro Focus ArcSight and Cisco WSA

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

### 2.25.1 Configure Cisco WSA to Forward Logs

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



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

The screenshot shows the 'New Log Subscription' configuration page in the Cisco S000V Web Security Virtual Appliance. The page is titled 'New Log Subscription' and contains a form with various settings for log subscriptions. The form includes fields for Log Type (Access Logs), Log Name (Access Logs ArcSight Forwarding), Rollover by File Size (100M), Rollover by Time (None), Log Style (Squid), Custom Fields (optional), File Name (aclog), Log Compression (Enable), Log Exclusions (Optional), and Retrieval Method (FTP on coeus.di.ipdr). The interface also shows a navigation bar with tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. A status bar at the top indicates 'Upgrade Available' and 'Logged in as: admin on coeus.di.ipdr'.

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

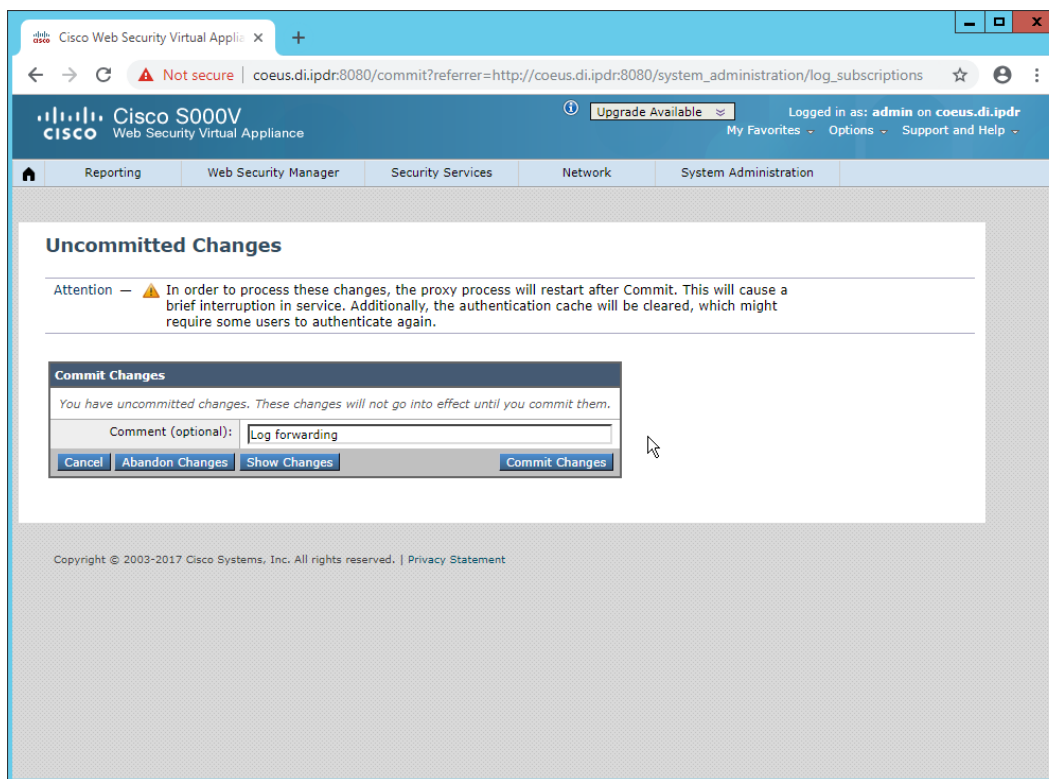


Retrieval Method:

- ☐ FTP on coeus.di.ipdr
  - Maximum Number of Files:
- ☐ FTP on Remote Server
  - FTP Host:
  - Directory:
  - Username:
  - Passphrase:
- ☐ SCP on Remote Server
  - SCP Host:  SCP Port:
  - Directory:
  - Username:
  - ☐ Enable Host Key Checking
    - ☒ Automatically Scan
    - ☐ Enter Manually
- ☒ Syslog Push
  - Hostname:
  - Protocol: ☐ UDP ☒ TCP
  - Maximum message size:
  - Facility:

Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

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



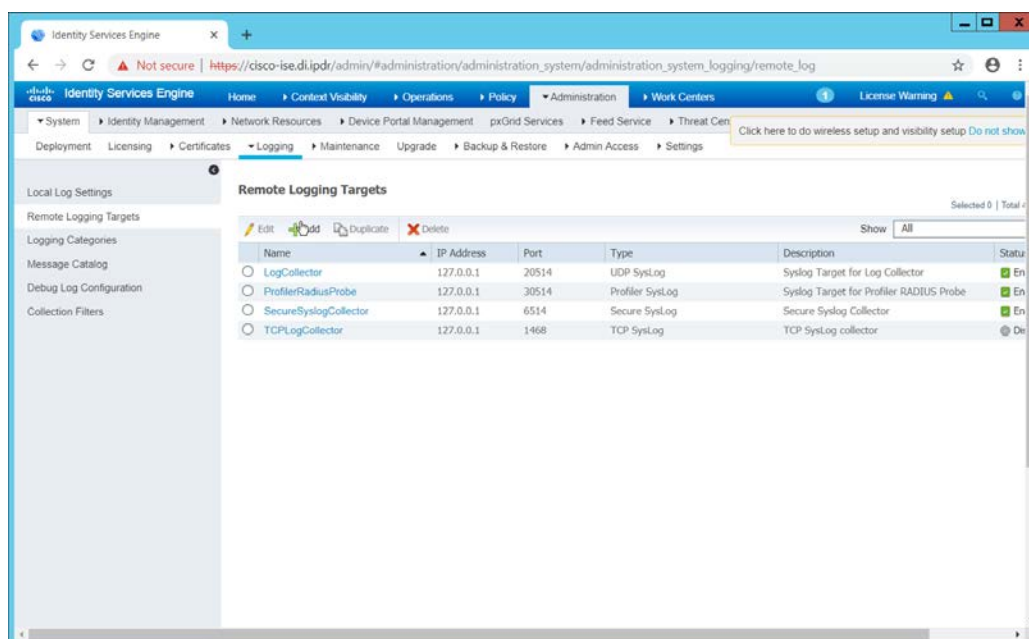
12. Click **Commit Changes**. The server will restart, so the web page connection will be temporarily lost.

## 2.26 Integration: Micro Focus ArcSight and Cisco ISE

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

### 2.26.1 Configure Cisco ISE to Forward Logs

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



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

Identity Services Engine

Not secure | [https://cisco-ise.d.ipdr/admin/#administration/administration\\_system/administration\\_system\\_logging/remote\\_log](https://cisco-ise.d.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log)

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

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.d.ipdr

\* 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.d.ipdr/admin/#administration/administration\\_system/administration\\_system\\_logging/remote\\_log](https://cisco-ise.d.ipdr/admin/#administration/administration_system/administration_system_logging/remote_log)

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

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.d.ipdr

\* 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

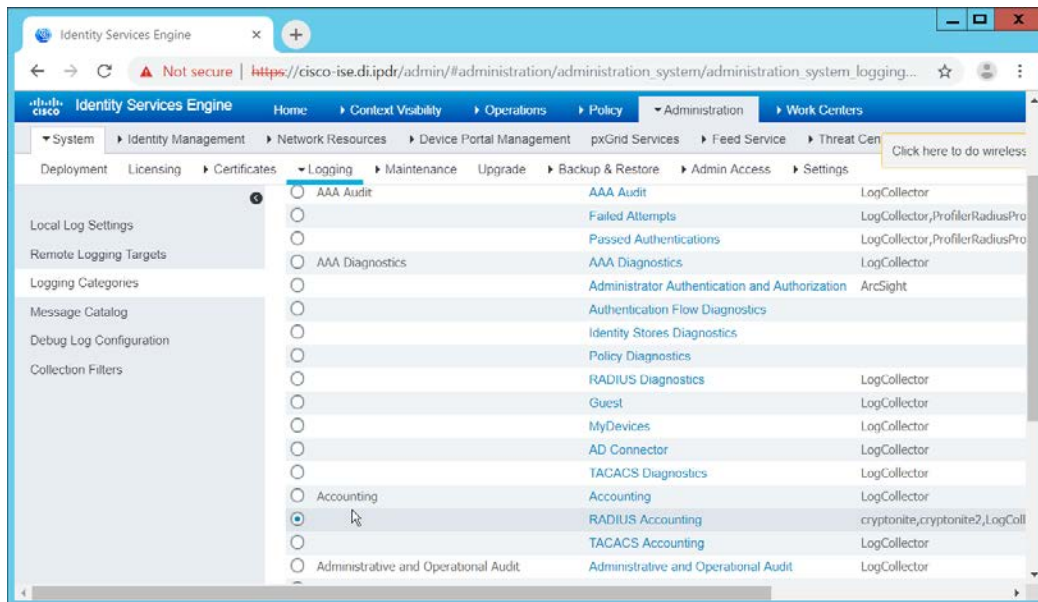
You have chosen to create an insecure (TCP/UDP) connection to the server. Are you sure you want to proceed?

No Yes

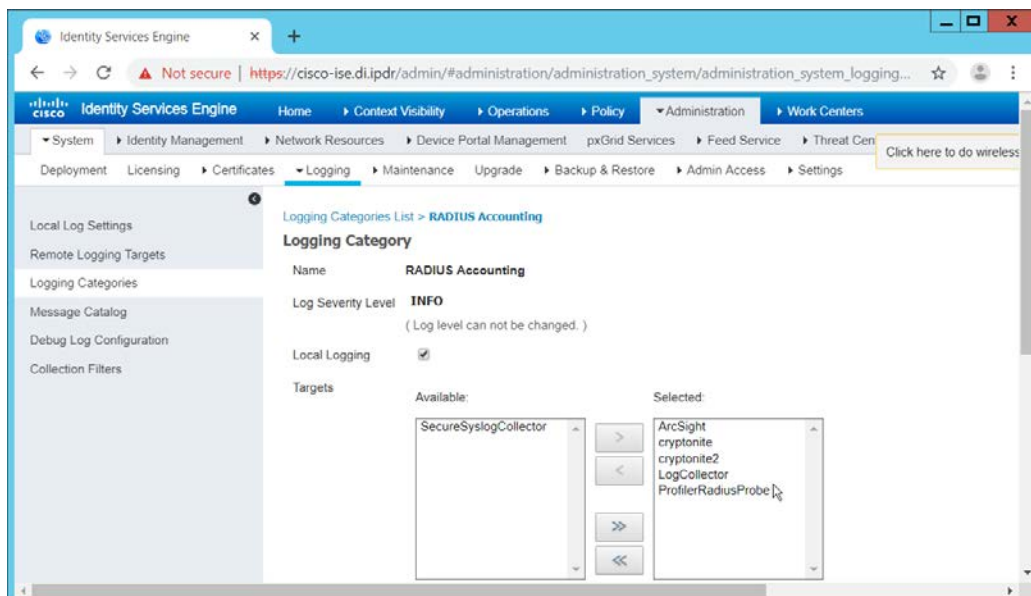
10. Click **Yes**.

## 2.26.2 Select Logs for Forwarding

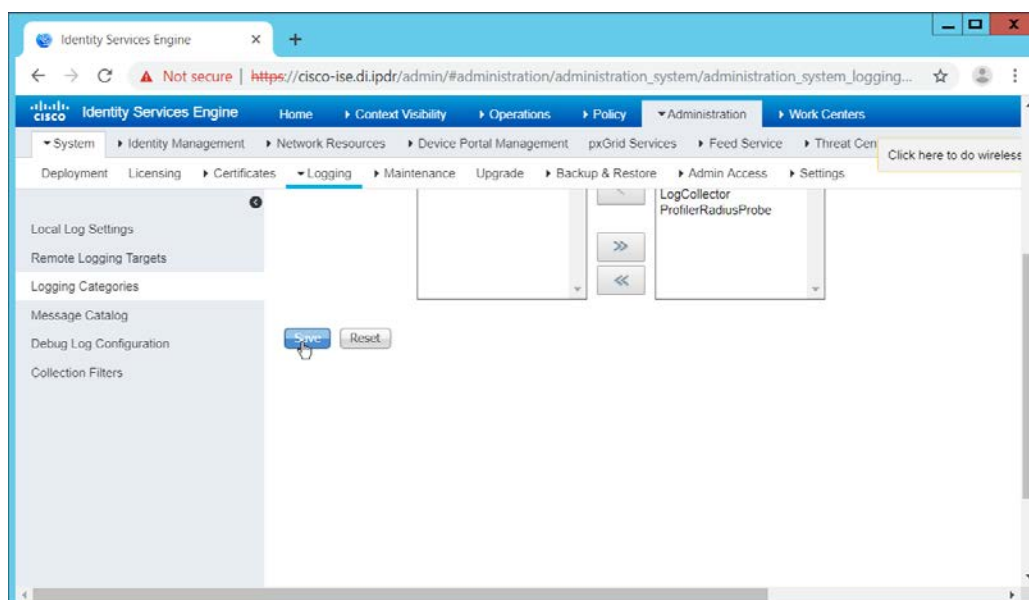
1. Navigate to **System > Logging > Logging Categories**.



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



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



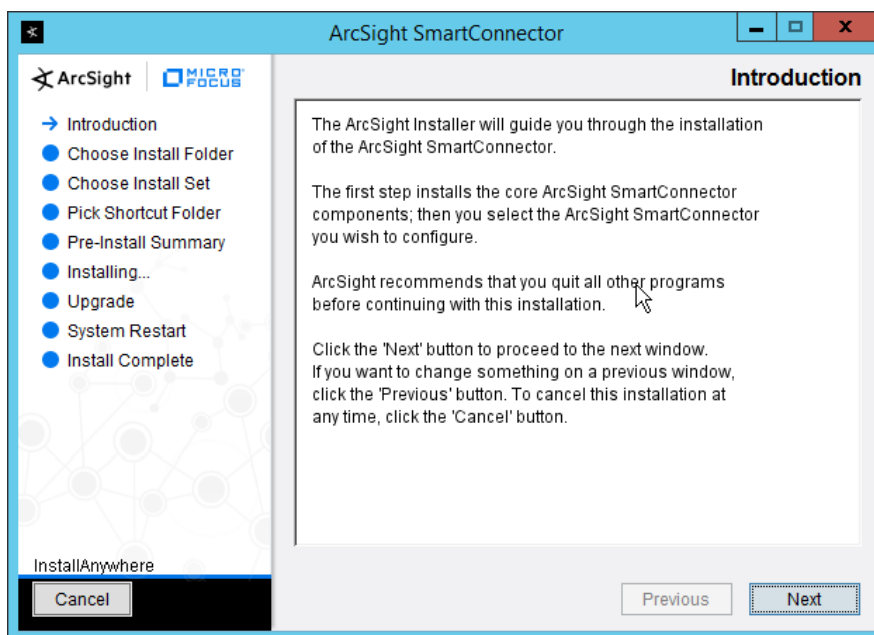
5. Click **Save**.
6. Repeat steps 1–5 for any log files you wish to forward to ArcSight.

## 2.27 Integration: Micro Focus ArcSight and Symantec DLP

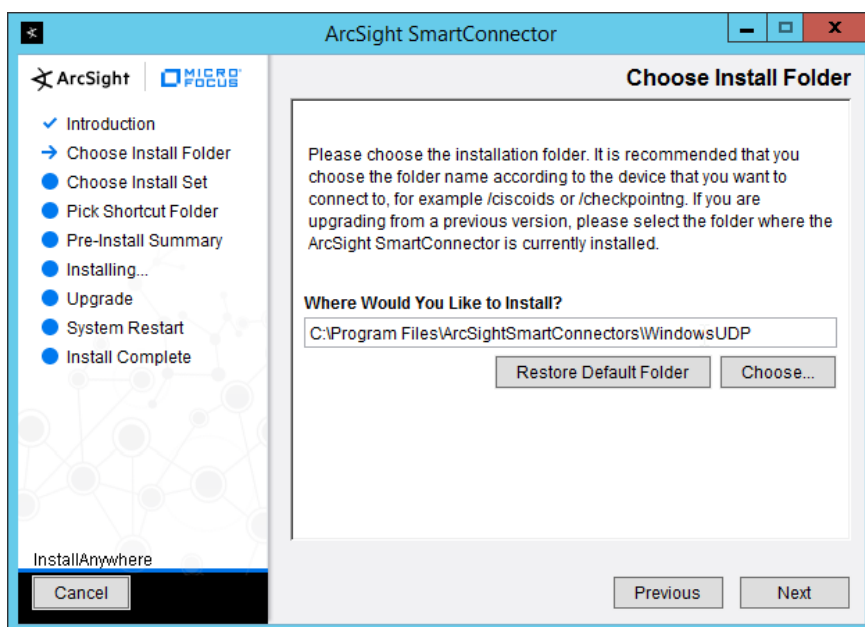
This integration briefly details how to send logs to an ArcSight syslog collector from Symantec DLP. If a server is already configured, you do not need to install a new one—simply forward logs to the address of that server. It is important to note that DLP requires a UDP server, so a TCP syslog server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

### 2.27.1 Install Micro Focus ArcSight

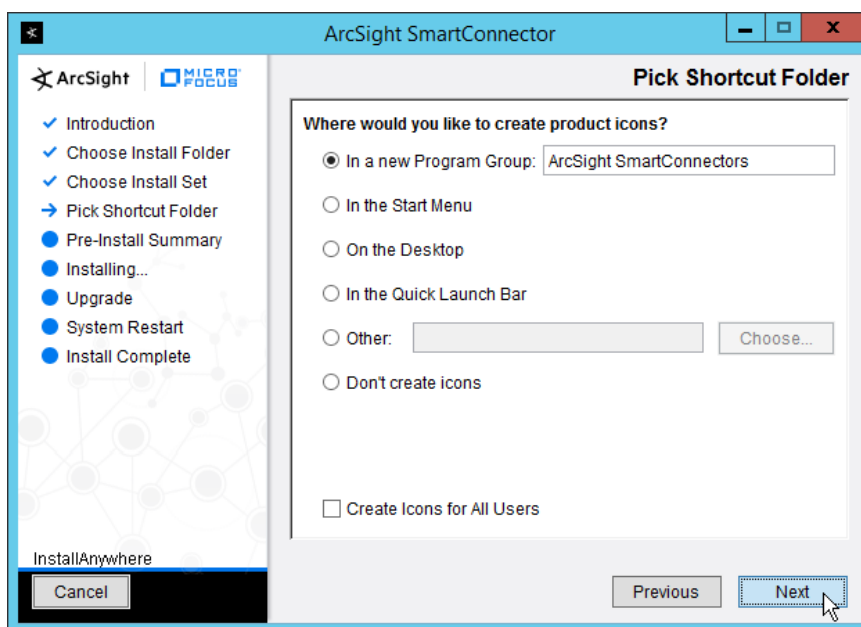
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running Cisco Stealthwatch.



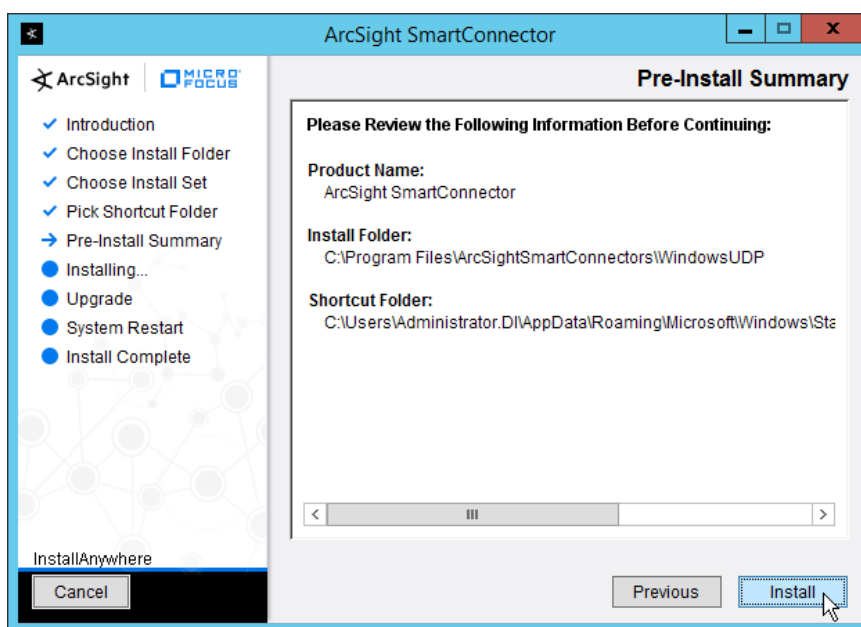
2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\WindowsUDP.



4. Click **Next**.



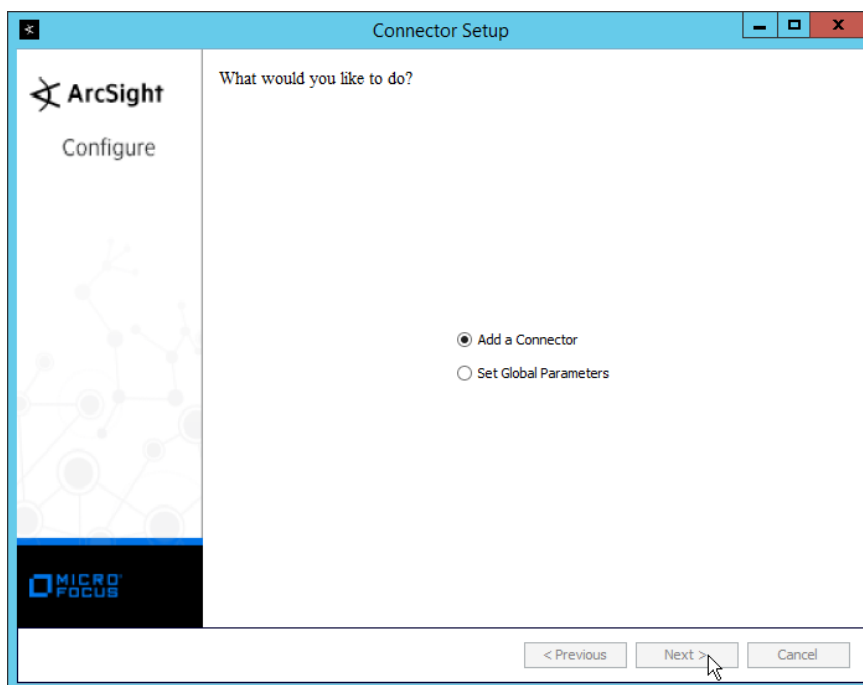
5. Click **Next**.



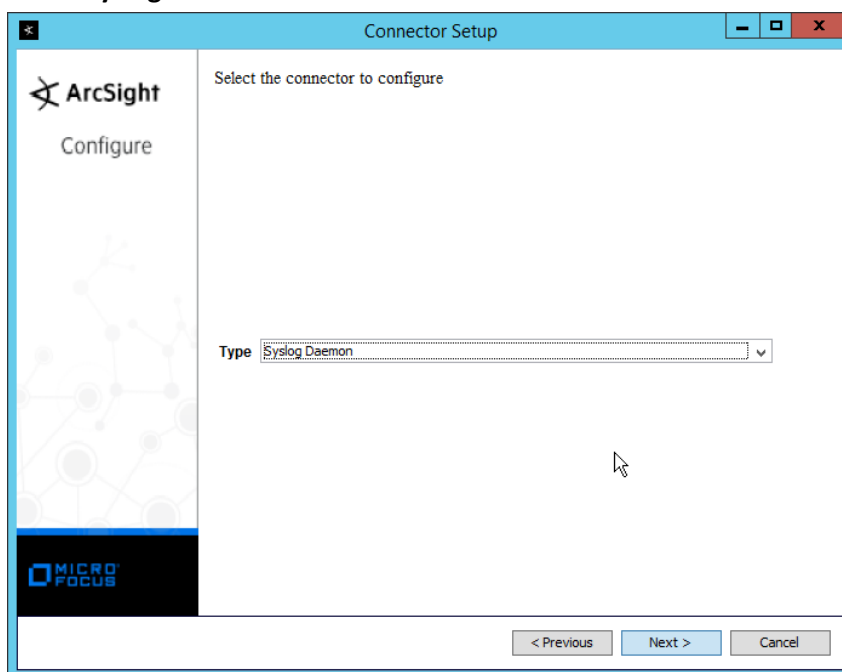
6. Click **Install**.

7. Select **Add a Connector**.



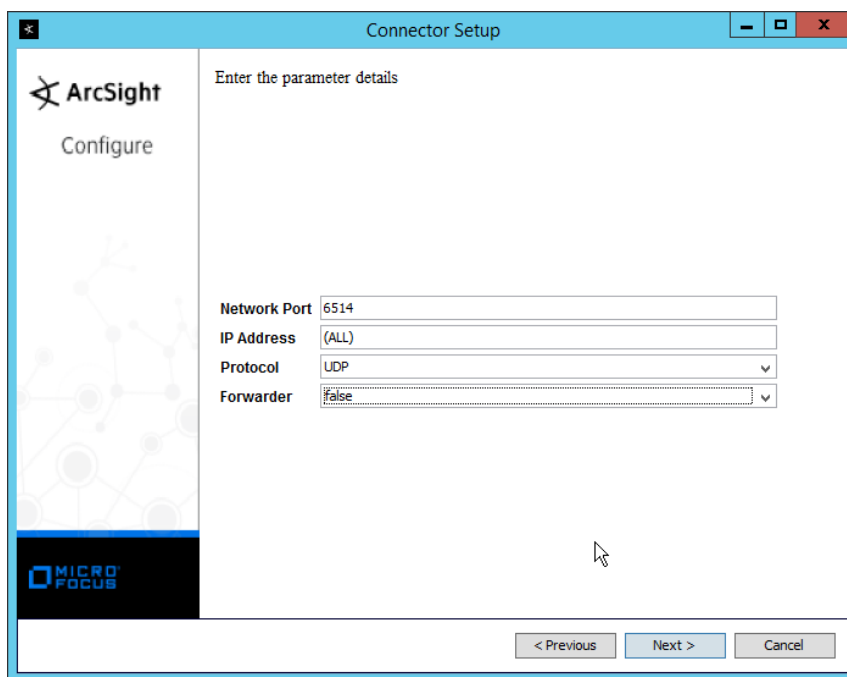


8. Click **Next**.
9. Select **Syslog Daemon**.



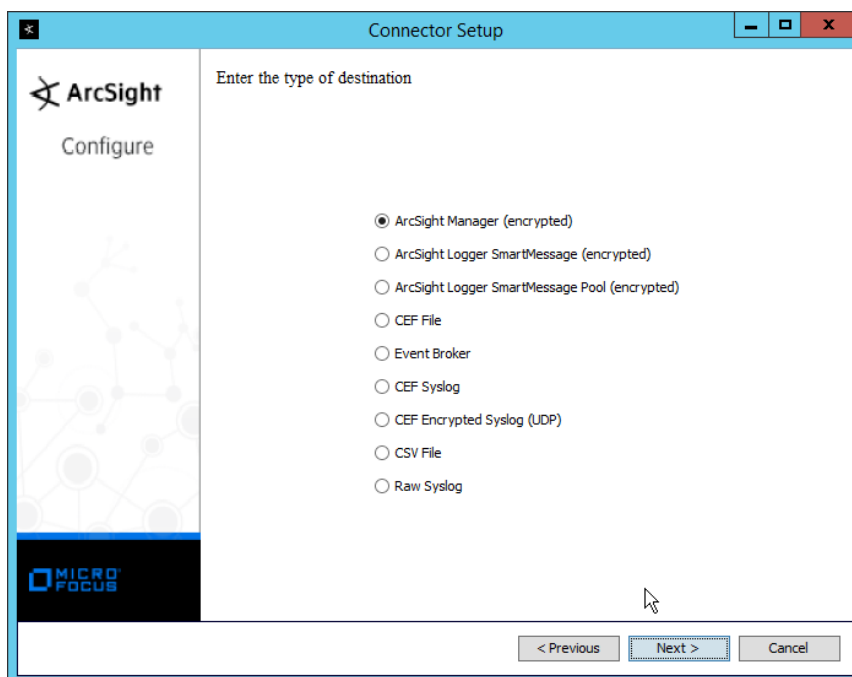
10. Click **Next**.

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



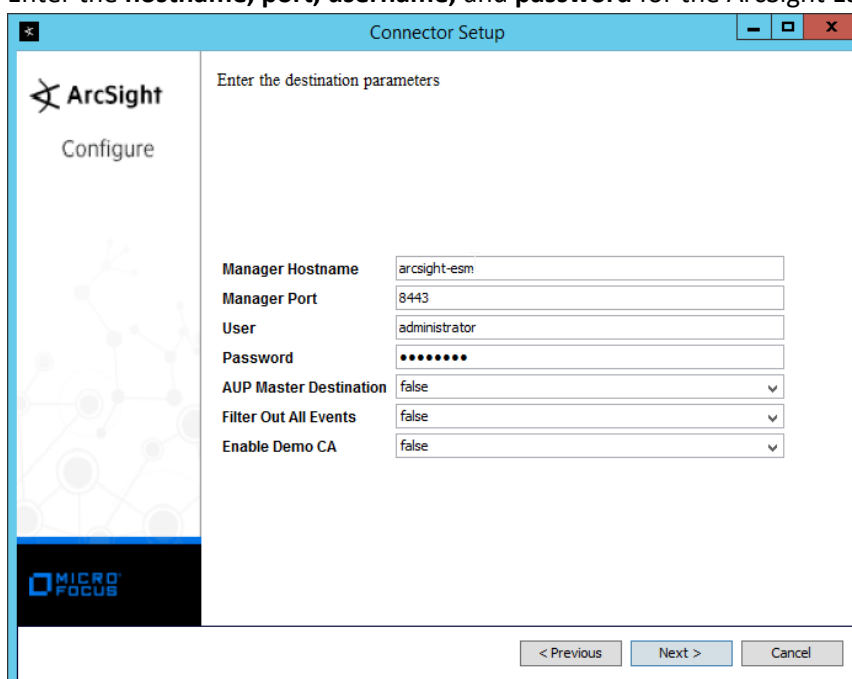
The screenshot shows the 'Connector Setup' window for ArcSight. The window has a blue title bar and a sidebar on the left with the ArcSight logo and the word 'Configure'. The main area is titled 'Enter the parameter details' and contains four configuration fields: 'Network Port' with the value '6514', 'IP Address' with the value '(ALL)', 'Protocol' with a dropdown menu showing 'UDP', and 'Forwarder' with a dropdown menu showing 'False'. At the bottom of the window are three buttons: '< Previous', 'Next >', and 'Cancel'. A mouse cursor is visible over the 'Next >' button.

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



15. Click **Next**.

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



17. Click **Next**.

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

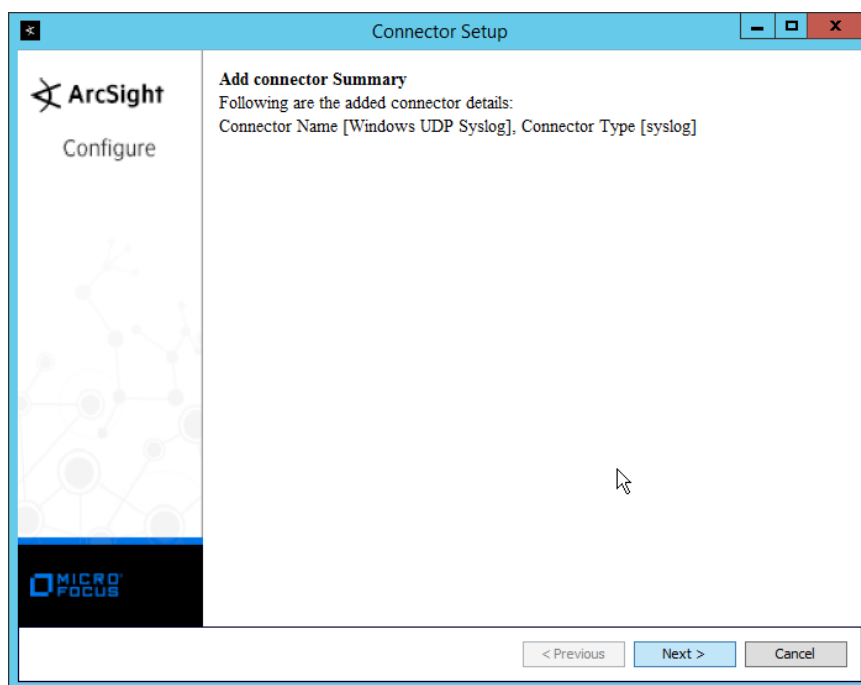
The screenshot shows the 'Connector Setup' window with the 'Configure' tab selected. The title bar reads 'Connector Setup'. The main area is titled 'Enter the connector details'. On the left, there is an ArcSight logo and the word 'Configure'. Below that is a Micro Focus logo. The main area contains four input fields: 'Name' (pre-filled with 'Windows UDP Syslog'), 'Location', 'DeviceLocation', and 'Comment'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

19. Click **Next**.

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

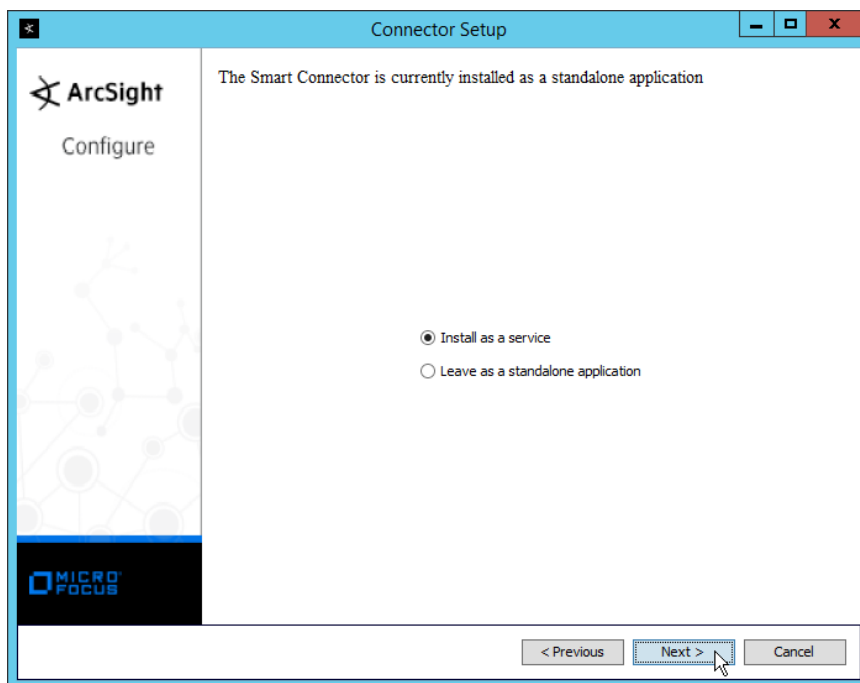
The screenshot shows the 'Connector Setup' window with the 'Configure' tab selected. The title bar reads 'Connector Setup'. The main area is titled 'Following certificate will be imported into connector trust store:'. Below this, it shows 'Host/port: arcsight-esm\_8443' and 'Details: CN=arcsight-esm, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US'. There are two radio buttons: 'Import the certificate to connector from destination' (selected) and 'Do not import the certificate to connector from destination'. A mouse cursor is pointing at the first radio button. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

21. Click **Next**.



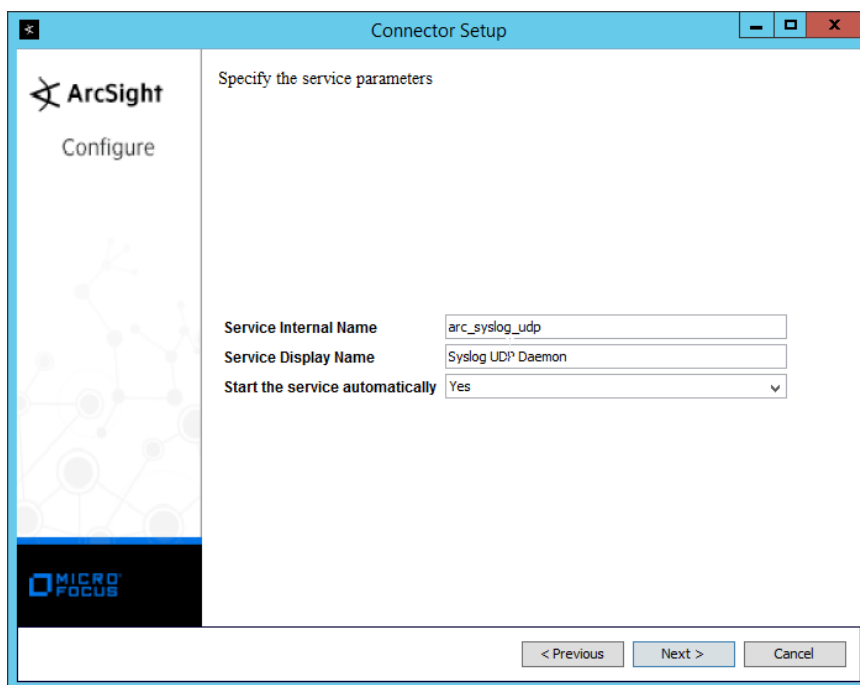
22. Click **Next**.

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

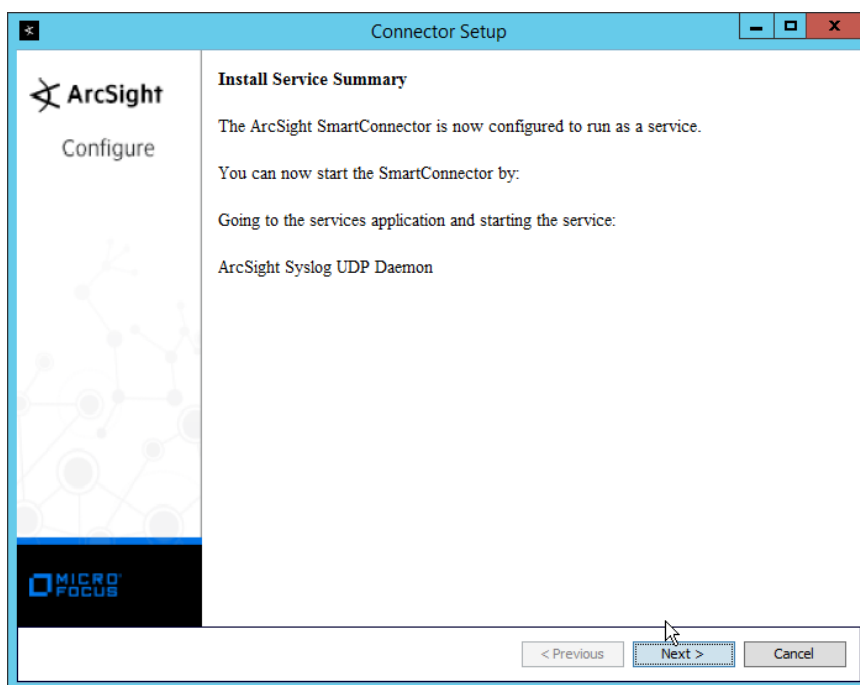


24. Click **Next**.

25. Enter a **service name** and **display name**.

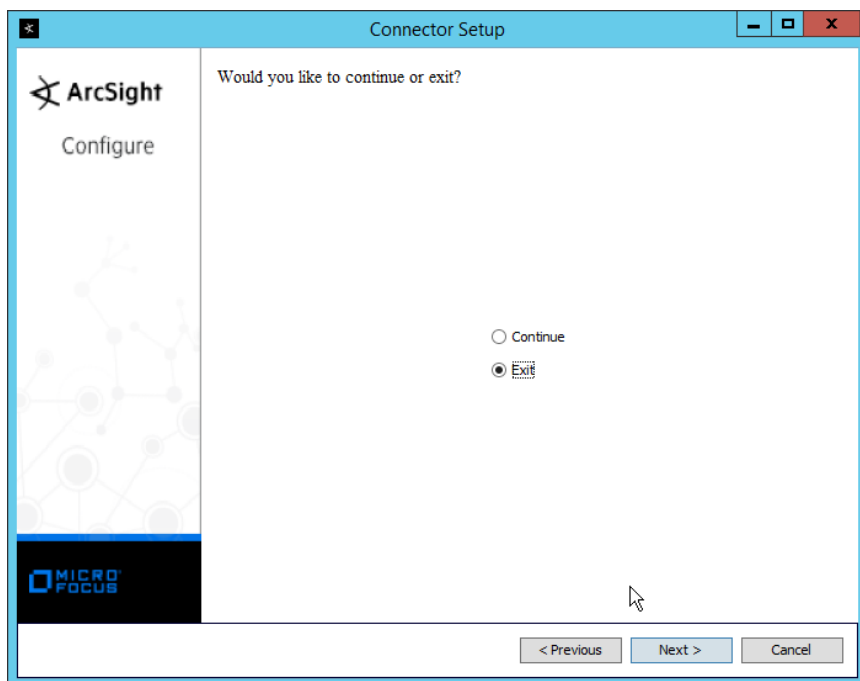


26. Click **Next**.

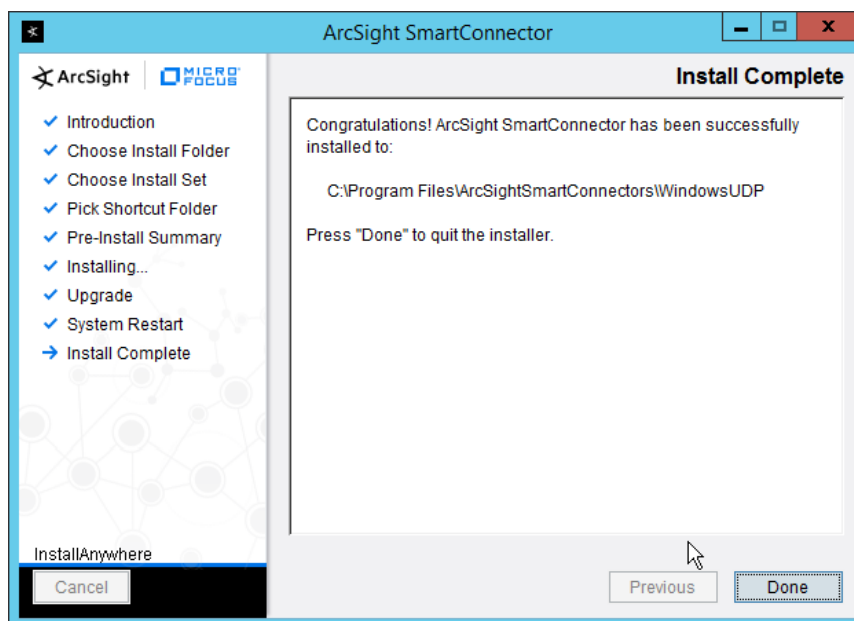


27. Click **Next**.

28. Select **Exit**.



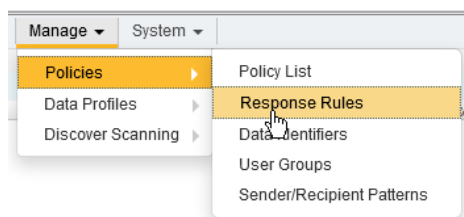
29. Click **Next**.



30. Click **Done**.

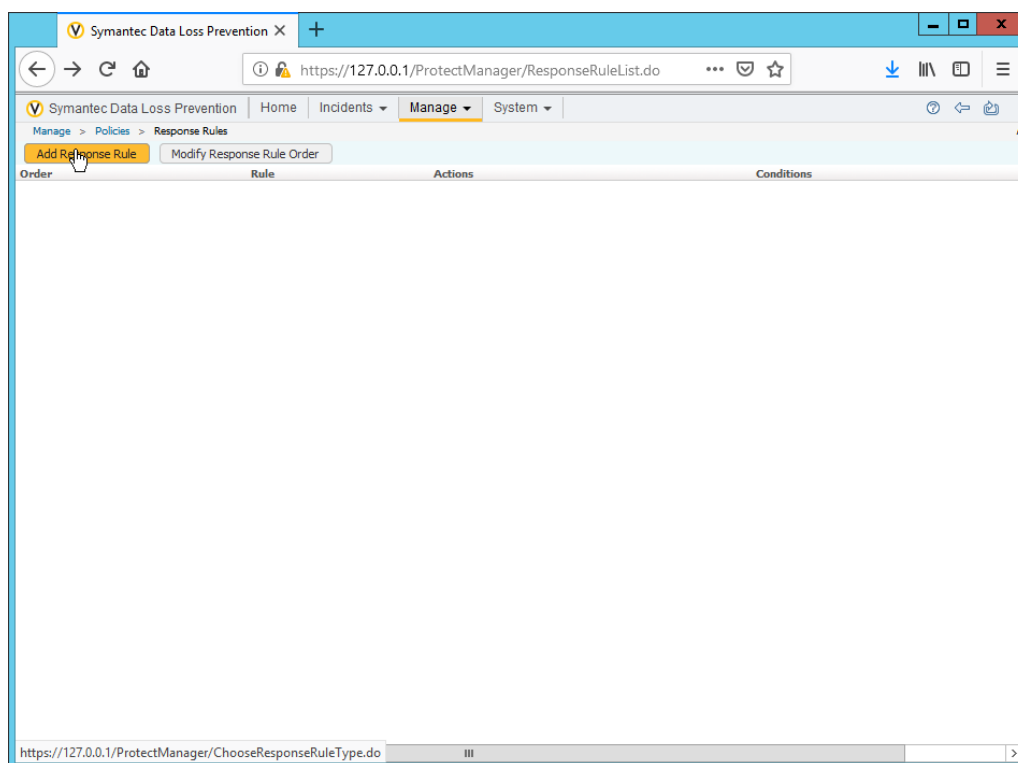
## 2.27.2 Configure Symantec DLP to Forward Logs

1. Log in to the Symantec DLP web console.

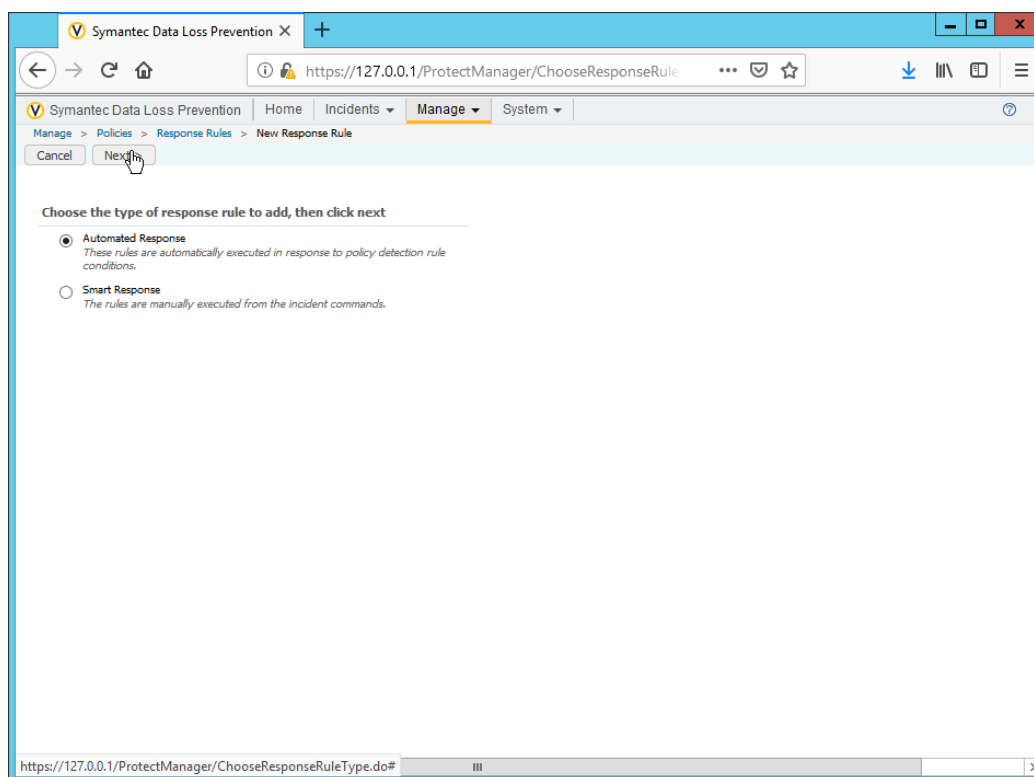


2. Navigate to **Manage > Policies > Response Rules**.

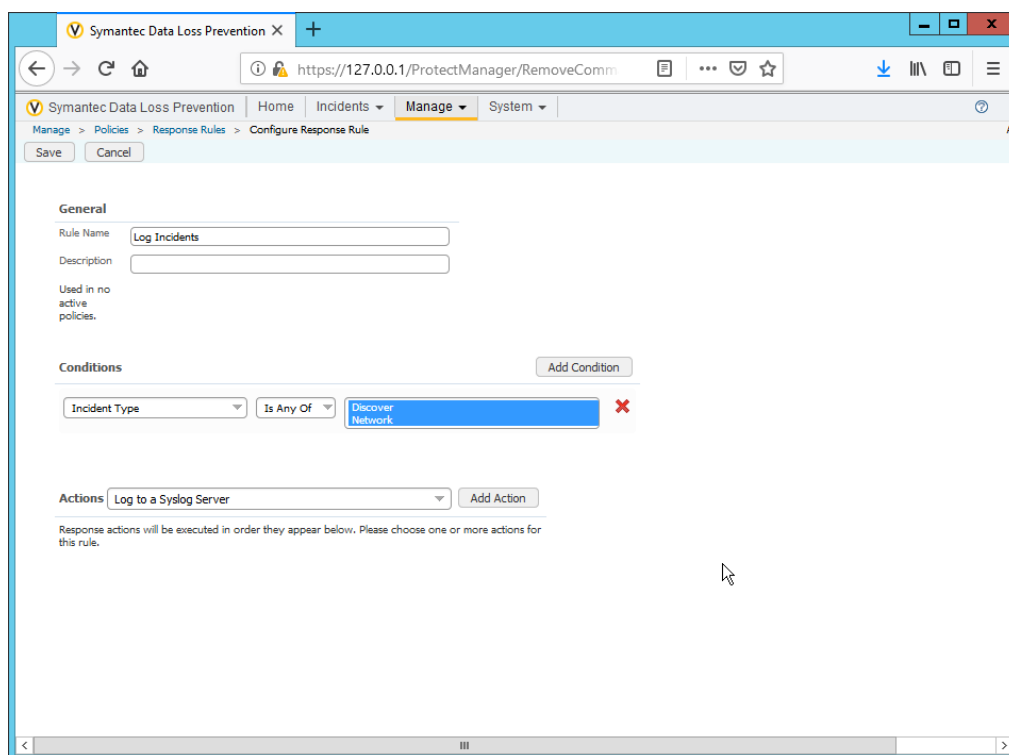




3. Click **Add Response Rule**.

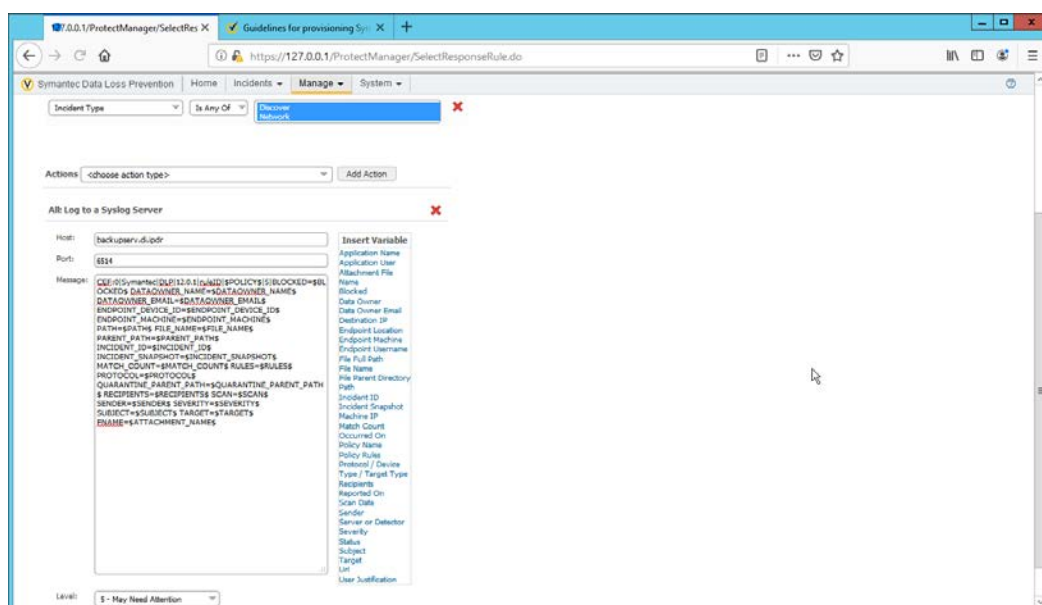


4. Click **Next**.
5. Enter a **name** for the rule.
6. Set any conditions for sending syslog messages. If you do not add conditions, all incidents will be forwarded.
7. Select **Log to a Syslog Server** for **Actions**.



8. Click **Add Action**.
9. Enter the **IP address** of the ArcSight syslog server.
10. Enter the **port** of the ArcSight syslog UDP server.
11. Select variables and format a log message to include all the information desired to be sent to the ArcSight server. Below is a sample format for the syslog message, which can potentially be parsed according to the needs of your organization.

```
CEF:0|Symantec|DLP|12.0.1|ruleID|$POLICY$|5|BLOCKED=$BLOCKED$
DATAOWNER_NAME=$DATAOWNER_NAME$ DATAOWNER_EMAIL=$DATAOWNER_EMAIL$
ENDPOINT_DEVICE_ID=$ENDPOINT_DEVICE_ID$
ENDPOINT_MACHINE=$ENDPOINT_MACHINE$ PATH=$PATH$
FILE_NAME=$FILE_NAME$ PARENT_PATH=$PARENT_PATH$
INCIDENT_ID=$INCIDENT_ID$ INCIDENT_SNAPSHOT=$INCIDENT_SNAPSHOT$
MATCH_COUNT=$MATCH_COUNT$ RULES=$RULES$ PROTOCOL=$PROTOCOL$
QUARANTINE_PARENT_PATH=$QUARANTINE_PARENT_PATH$
RECIPIENTS=$RECIPIENTS$ SCAN=$SCAN$ SENDER=$SENDER$
SEVERITY=$SEVERITY$ SUBJECT=$SUBJECT$ TARGET=$TARGET$
FNAME=$ATTACHMENT_NAME$
```



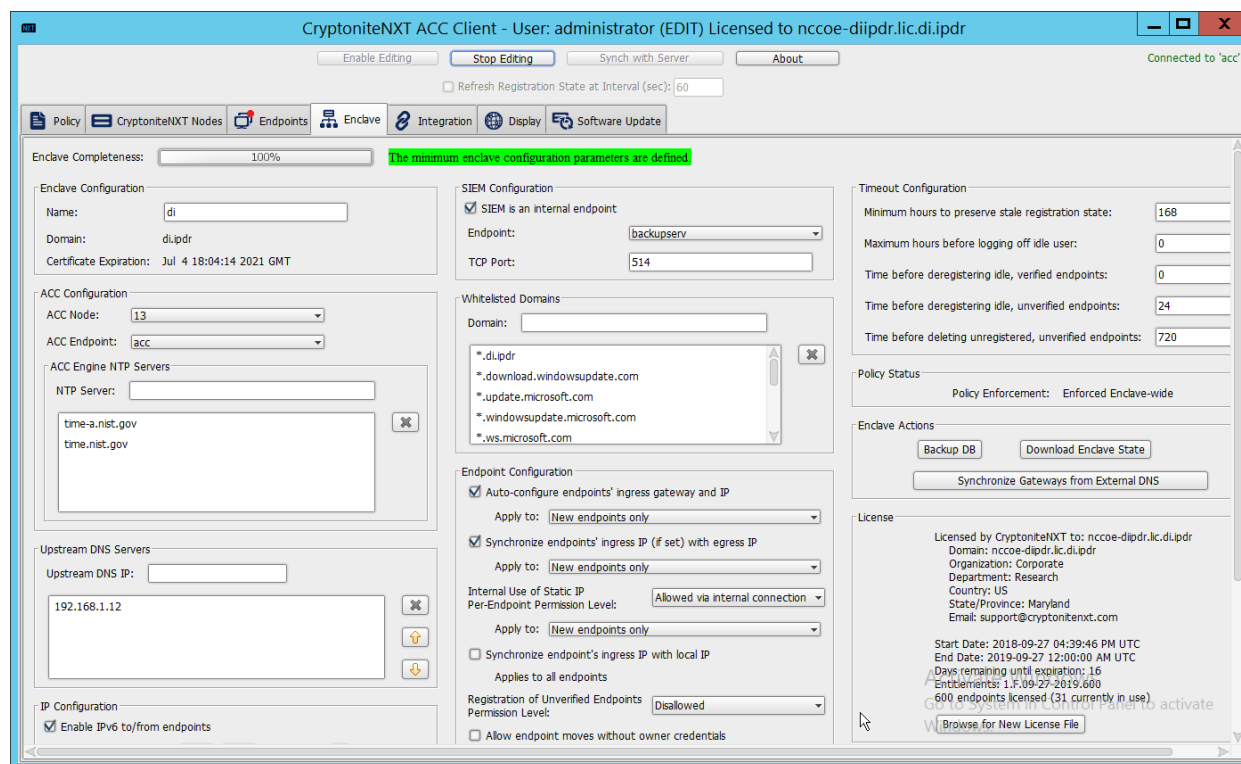
12. Click **Save**.

## 2.28 Integration: Micro Focus ArcSight and CryptoniteNXT

This integration briefly details how to send logs to an ArcSight syslog collector from CryptoniteNXT. Please see [Section 2.24](#) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one— simply forward logs to the address of that server. Ensure that you are using a TCP syslog collector. This section assumes that the collector is already under CryptoniteNXT’s network protection.

### 2.28.1 Configure CryptoniteNXT to Forward Logs to ArcSight

1. Navigate to the **Enclave** tab in the **CryptoniteNXT ACC GUI**.
2. Under **SIEM Configuration**, check the box next to **SIEM is an internal endpoint**.
3. Select the endpoint running the TCP syslog collector.
4. Enter the port used.



5. Click **Save**.

## 2.29 Integration: Micro Focus ArcSight and Semperis DSP

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

Note: This integration requires Semperis DSP version 2.6.

### 2.29.1 Configure Semperis DSP to Forward Logs

1. In Semperis DSP, navigate to **Settings > SIEM Integration**.
2. Check the box next to **Enable SysLog**.
3. Under **Syslog Server**, enter the **hostname** for the ArcSight syslog collector, as well as the **port**.
4. Select **TCP**.
5. Enter a value for **Change Event Polling Frequency** based on the needs of your organization—this is how often it will poll for new logs to forward.

6. Under **Change Event Filtering**, select **AD Changed Items**, and **Send Operation Log to SysLog**. Ensure that **All** is selected for **Partitions**.
7. You can also select any specific **operations**, **classes**, and **attributes** to be forwarded or simply leave as **All**.

8. Click **Save**.

9. Click **Close**.

## 2.30 Integrations: CryptoniteNXT

For the architecture, it is necessary to create the following source groups. If your organization's desired architecture is different from the one described in this document, it is necessary to adapt the following instructions to avoid loss of network or security function. This section will describe the creation of source groups and destination groups used in this enterprise.

Create the following destination groups and source groups and apply them to the correct endpoints to allow these products and integrations to communicate under CryptoniteNXT.

### 2.30.1 Active Directory and DNS

This guide assumes the use of Active Directory and DNS on the same Windows 2012 server. The following ports may vary for other products.

Destination Group Name	Source Group Name	Protocol	Port Range
ad-dns	ad-dns-clients	TCP	389
ad-dns	ad-dns-clients	UDP	389
ad-dns	ad-dns-clients	UDP	53
ad-dns	ad-dns-clients	TCP	88
ad-dns	ad-dns-clients	UDP	88
ad-dns	ad-dns-clients	TCP	25
ad-dns	ad-dns-clients	TCP	42
ad-dns	ad-dns-clients	TCP	137
ad-dns	ad-dns-clients	TCP	139
ad-dns	ad-dns-clients	TCP	53
ad-dns	ad-dns-clients	TCP	636
ad-dns	ad-dns-clients	TCP	3268:3269
ad-dns	ad-dns-clients	TCP	445
ad-dns	ad-dns-clients	UDP	445
ad-dns	ad-dns-clients	TCP	9389
ad-dns	ad-dns-clients	TCP	5722
ad-dns	ad-dns-clients	TCP	464
ad-dns	ad-dns-clients	UDP	464
ad-dns	ad-dns-clients	UDP	123
ad-dns	ad-dns-clients	UDP	137:138
ad-dns	ad-dns-clients	UDP	67
ad-dns	ad-dns-clients	UDP	2535

Destination Group Name	Source Group Name	Protocol	Port Range
ad-dns	ad-dns-clients	UDP	49152:65535
ad-dns	ad-dns-clients	TCP	49152:65535

Endpoint	Source Groups	Destination Groups
(all endpoints that need access to AD/DNS)	ad-dns-clients	
AD/DNS server		ad-dns

### 2.30.2 Microsoft Exchange

This guide assumes the use of Microsoft Exchange. The following ports may vary for other products.

Destination Group Name	Source Group Name	Protocol	Port Range
exchange	exchange-clients	TCP	443
exchange	exchange-clients	TCP	80
exchange	exchange-clients	TCP	25
exchange	exchange-clients	TCP	379
exchange	exchange-clients	TCP	3268:3269
exchange	exchange-clients	TCP	636
exchange	exchange-clients	TCP	143
exchange	exchange-clients	TCP	993
exchange	exchange-clients	TCP	110
exchange	exchange-clients	TCP	995
exchange	exchange-clients	TCP	119
exchange	exchange-clients	TCP	563
exchange	exchange-clients	TCP	465
exchange	exchange-clients	TCP	443691
exchange	exchange-clients	TCP	102
exchange	exchange-clients	TCP	135



Destination Group Name	Source Group Name	Protocol	Port Range
exchange	exchange-clients	TCP	389:390
exchange	exchange-clients	TCP	53
exchange	exchange-clients	UDP	53
exchange	exchange-clients	TCP	2525
exchange	exchange-clients	TCP	475

Endpoint	Source Groups	Destination Groups
MS Exchange	exchange-clients	exchange
(all email clients)	exchange-clients	
AD/DNS server	exchange-clients	

### 2.30.3 FileZilla

The default port for FileZilla is 21.

1. To determine the ports being used for your instance, open the FileZilla console.
2. Navigate to **Edit > Settings > General Settings > Listen on these ports**, and allow any ports listed here.
3. If your server listens in passive mode, navigate to **Edit > Settings > Passive mode settings > Use custom port range**, and allow any ports listed here.

Destination Group Name	Source Group Name	Protocol	Port Range
FileZilla	BackupClients	TCP	21 (default—see instructions)
FileZilla	BackupClients	TCP	51120-511230 (passive mode—see instructions)

Endpoint	Source Groups	Destination Groups
(any endpoints that need to perform backups)	BackupClients	
FileZilla server		FileZilla

## 2.30.4 GreenTec

If GreenTec is configured to use a FileZilla server, refer to the above section. If GreenTec is configured to use Windows Network Share, see below for ports required.

Destination Group Name	Source Group Name	Protocol	Port Range
NetworkShare	GreenTecClients	TCP	80
NetworkShare	GreenTecClients	TCP	135-139
NetworkShare	GreenTecClients	TCP	445

Endpoint	Source Groups	Destination Groups
(any endpoints that need access to GreenTec disks)	GreenTecClients	
GreenTec server		NetworkShare

## 2.30.5 Tripwire Enterprise

In Tripwire, the Axon Bridge is used for Tripwire Enterprise to contact endpoints. Therefore, the port 5670 must be allowed on endpoints to allow TE to initiate communications. Furthermore, TE requires MSSQL to function, so it must be granted access to that as well.

Destination Group Name	Source Group Name	Protocol	Port Range
TripwireEnterprise	TEClients	TCP	443
TripwireEnterprise	TEClients	TCP	8080
TripwireEnterprise	TEClients	TCP	9898
TripwireEnterprise	TEClients	TCP	1169
TEAxon	TripwireE	TCP	5670
MSSQL	MSSQLClients	TCP	1433

Endpoint	Source Groups	Destination Groups
(any endpoints that need to be monitored by Tripwire Enterprise)	TEClients	TEAxon
Tripwire Enterprise server	TripwireE, MSSQLClients	TripwireEnterprise
MSSQL server		MSSQL

### 2.30.6 ArcSight ESM

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSight	ArcSightConnectors	TCP	8443

Endpoint	Source Groups	Destination Groups
(any endpoints with an ArcSight Connector installed)	ArcSightConnectors	
ArcSight ESM server		ArcSight

### 2.30.7 Cisco ISE

Please see the *CryptoniteNXT Generic RADIUS Integration Guide* for instructions on how ISE should be integrated with CryptoniteNXT.

To access the web console for ISE, allow port 443 for any machines that should be able to access the ISE administrative console.

To access the portal for ISE, allow port 8443 (default) for any machines that will need to access the portal. You can find this value by looking at your portal configuration in ISE.

Furthermore, if RADIUS is configured for the posture integration, you will need to add any ports used in RADIUS for both ISE and the internal switch. The default for these is 1812 (Authentication), 1813 (Accounting), and 1700 (CoA). RADIUS can be TCP or UDP, so you can restrict this to your organization's configuration.

Destination Group Name	Source Group Name	Protocol	Port Range
ISE	ISEConsole	TCP	443
ISE	ISEClients	TCP	8443
radius	ISESwitch, ISEServer	TCP	1812
radius	ISESwitch, ISEServer	UDP	1812
radius	ISESwitch, ISEServer	TCP	1813
radius	ISESwitch, ISEServer	UDP	1813
radius	ISESwitch, ISEServer	TCP	1700
radius	ISESwitch, ISEServer	UDP	1700

Endpoint	Source Groups	Destination Groups
(any endpoints that need to do posture under ISE)	ISEClients	
(any endpoints that need to access the ISE web console)	ISEConsole	
ISE server	ISEServer	ISE, radius
(internal switches or RADIUS servers used for ISE Posture)	ISESwitch, ISEClients	radius
Cryptonite ACC Node		radius

### 2.30.8 Semperis DSP

Semperis DSP recommends allowing full network access during the initial database sync. After that, the following ports should be left open for communication.

Destination Group Name	Source Group Name	Protocol	Port Range
dsp	dsp-admin	TCP	443
dsp	dsp-agents	TCP	8903
dsp	dsp-agents	TCP	135
dsp	dsp-agents	TCP	445

Destination Group Name	Source Group Name	Protocol	Port Range
dsp	dsp-agents	TCP	1024:1034
ad-dsp	dsp-client	TCP	8772
ad-dsp	dsp-client	TCP	8750
ad-dsp	dsp-client	ICMP	0:255

Endpoint	Source Groups	Destination Groups
(any endpoints that need admin access to DSP)	dsp-admin	
Semperis DSP	ad-dns-clients, dsp-client, exchange-clients	dsp
Active Directory server	dsp-agents	ad-dsp

### 2.30.9 Symantec DLP

This largely depends on how distributed the setup of DLP is. See here for a list of ports required by Symantec DLP: <https://support.symantec.com/us/en/article.tech220846.html>.

For this build, we used a single server that contained the database, so only the agents and administrative clients needed to be allowed to communicate through Cryptonite.

Destination Group Name	Source Group Name	Protocol	Port Range
dlp	dlp-admin	TCP	443
dlp	dlp-clients	TCP	10443

### 2.30.10 Cisco WSA

WSA uses a proprietary command line, which means it does not have a way of authenticating to the CryptoniteNXT portal. For devices such as this, there are two options.

1. The device can be left outside CryptoniteNXT.
2. The device can be placed under CryptoniteNXT on a CryptoniteNXT Endpoint Node with the portal disabled.

To prevent MAC spoofing, by default Cryptonite pins MAC addresses to the port + VLAN (Virtual LAN) to which a device is connected, so a malicious device connecting to the end-point node with the same MAC as an already connected IP360 would still be required to authenticate. Physical security for the end-point node can further mitigate concerns about MAC spoofing.

If you can find a way to authenticate WSA to CryptoniteNXT or decide to use the disabled portal option with strong physical security, we provide the ports below for integration.

To access the web console for WSA, allow port 8080 for any machines that should be able to access the ISE administrative console.

To access the proxy, allow port 80 and port 3128 for any machines that will need to go through the proxy, which will likely be most clients in the enterprise. Port 80 is for the *wpad.dat* file, and port 3128 is for the proxy itself.

Destination Group Name	Source Group Name	Protocol	Port Range
wsa	wsa-clients	TCP	80
wsa	wsa-clients	TCP	3128
wsa	wsa-admin	TCP	8080

Endpoint	Source Groups	Destination Groups
(any endpoints that need to use the proxy to connect to the internet)	wsa-clients	
(any endpoints that need to access the WSA web console)	wsa-admin	
Cisco WSA		wsa

### 2.30.11 Tripwire IP360

IP360 uses a proprietary command line, which means it does not have a way of authenticating to the CryptoniteNXT portal. For devices such as this, there are two options.

1. The device can be left outside CryptoniteNXT.
2. The device can be placed under CryptoniteNXT on a CryptoniteNXT Endpoint Node with the portal disabled.

To prevent MAC spoofing, by default Cryptonite pins MAC addresses to the port+VLAN to which a device is connected, so a malicious device connecting to the end-point node with the same MAC as an already connected IP360 would still be required to authenticate. Physical security for the end-point node can further mitigate concerns about MAC spoofing.

If you can find a way to authenticate IP360 to CryptoniteNXT or decide to use the disabled portal option with strong physical security, we provide the ports below for integration.

To access the web console for IP360, allow port 443 for any machines that should be able to access the IP360 administrative console.

IP360 should have access to all ports of the client machines it needs to scan. Another option is to simply add IP360 to all the source groups present in your enterprise, and it will give an overview of the vulnerabilities of clients on ports that CryptoniteNXT is not actively protecting. Alternatively, you can disable policy enforcement temporarily on the CryptoniteNXT Endpoint Node to which IP360 is connected, but you should do this only during scans.

Destination Group Name	Source Group Name	Protocol	Port Range
ip360	ip360admin	TCP	443
scantarget	ip360scanner	TCP	1:65535
scantarget	ip360scanner	UDP	1:65535
scantarget	ip360scsanner	ICMP	0:255

Endpoint	Source Groups	Destination Groups
(any endpoints need to access the IP360 web console)	ip360admin	
(any endpoints to be fully scanned by IP360)		scantarget
IP360	ip360scanner	ip360

### *2.30.11.1 Tripwire Log Center, Tripwire IP360, Tripwire Enterprise, and ArcSight ESM*

The guide details an integration among Tripwire IP360, Tripwire Enterprise, Tripwire Log Center, and ArcSight ESM. This section describes the ports needed to allow the integrations through Cryptonite.

First, traffic must be allowed from Tripwire Log Center to the MSSQL server. To do this, ensure that Tripwire Log Center can access 1433 on the MSSQL server. (Note: Tripwire Enterprise also has access to this port, as described above in the Tripwire Enterprise section.)

Then traffic from Tripwire Enterprise to Tripwire Log Center should be allowed on ports 8091 and 1468.

Traffic from IP360 to Tripwire Log Center should be allowed on port 22 for the SFTP (Secure FTP) transfer. Also, traffic from Tripwire Log Center to 5670 on Tripwire IP360 should be allowed. If you chose to leave IP360 out of the Cryptonite NXT enclave, Tripwire Log Center will need to be able to reach it externally.

Traffic from Tripwire Log Center to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514). As a last note, the server running the ArcSight syslog connector requires an IP and not a hostname for its integration with Tripwire Log Center—you must set a static IP for the connector server in Cryptonite and enter this IP in the appropriate place in Tripwire Log Center’s configuration.

Destination Group Name	Source Group Name	Protocol	Port Range
MSSQL	MSSQLClients	TCP	1443
TLC	TLCClients	TCP	8091
TLC	TLCClients	TCP	1468
TLC	TLCClients	TCP	22
ArcSightTCPSysConn	TCPSysClients	TCP	514
ip360	ip360admin	TCP	5670

Endpoint	Source Groups	Destination Groups
Tripwire Log Center	TCPSysClients, MSSQLClients, ip360admin	TLC
Tripwire Enterprise	TLCClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn
MSSQL		MSSQL
IP360	TLCClients	ip360



### 2.30.12 FileZilla and ArcSight

The guide details an integration between FileZilla and ArcSight ESM to forward logs from FileZilla to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Because this integration involves the use of an ArcSight Connector directly on the FileZilla server, only one port is needed. The FileZilla server should be able to directly communicate with 8443 on the ArcSight ESM server.

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSight	ArcSightConnectors	TCP	8443

Endpoint	Source Groups	Destination Groups
FileZilla	ArcSightConnectors	
ArcSight ESM		ArcSight

### 2.30.13 Cisco ISE and ArcSight

The guide details an integration between Cisco ISE and ArcSight ESM to forward logs from ISE to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Cisco ISE to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

Endpoint	Source Groups	Destination Groups
Cisco ISE	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

### 2.30.14 Cisco WSA and ArcSight

The guide details an integration between Cisco WSA and ArcSight ESM to forward logs from WSA to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Cisco WSA to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

Endpoint	Source Groups	Destination Groups
Cisco WSA	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

### 2.30.15 Semperis DSP and ArcSight

The guide details an integration between Semperis DSP and ArcSight ESM to forward logs from DSP to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Semperis DSP to the machine containing the ArcSight TCP syslog container should be allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

Endpoint	Source Groups	Destination Groups
Semperis DSP	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

### 2.30.16 Symantec DLP and ArcSight

The guide details an integration between Symantec DLP and ArcSight ESM to forward logs from DLP to ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

Traffic from Symantec DLP to the machine containing the ArcSight UDP syslog container should be allowed on the port configured (in the guide, we use UDP and port 6514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	UDP	6514

Endpoint	Source Groups	Destination Groups
Symantec DLP	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

## Appendix A List of Acronyms

<b>ACC</b>	Administration Control Center
<b>AD</b>	Active Directory
<b>ADFR</b>	Active Directory Forest Recovery
<b>CoA</b>	Change of Authorization
<b>DDNS</b>	Dynamic Domain Name System
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domain Name System
<b>DSP</b>	Directory Services Protector
<b>ESM</b>	Enterprise Security Manager
<b>FTP</b>	File Transfer Protocol
<b>FTPS</b>	File Transfer Protocol over TLS
<b>GUI</b>	Graphical User Interface
<b>IIS</b>	Internet Information Services
<b>ISE</b>	Identity Services Engine
<b>IT</b>	Information Technology
<b>JCE</b>	Java Cryptography Extension
<b>JRE</b>	Java Runtime Environment
<b>LAN</b>	Local Area Network
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MSSQL</b>	Microsoft SQL
<b>NAT</b>	Network Address Translation
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>PAC</b>	Proxy Auto Config
<b>RADIUS</b>	Remote Authentication Dial-In User Service
<b>SDK</b>	Software Developer Kit
<b>SFTP</b>	Secure FTP
<b>SNMP</b>	Simple Network Management Protocol
<b>SQL</b>	Structured Query Language
<b>TE</b>	Tripwire Enterprise
<b>TLC</b>	Tripwire Log Center
<b>VLAN</b>	Virtual LAN
<b>WDV</b>	WORM Disk Volume
<b>WORM</b>	Write Once Read Many
<b>WPAD</b>	Web Proxy Auto Discovery

**WSA**      Web Security Appliance