NIST SPECIAL PUBLICATION 1800-26

Data Integrity

Detecting and Responding to 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

DRAFT

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-26

Data Integrity: Detecting and Responding to 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

DRAFT

January 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 1800-26A

Data Integrity

Detecting and Responding to 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

January 2020

DRAFT

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

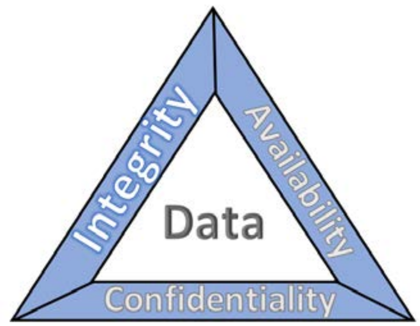
National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 (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 quickly detect and respond to an event that impacts data integrity. Businesses must be confident that these events are detected quickly and responded to appropriately.
- 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 NIST built a laboratory environment to explore methods to effectively detect and respond to a data integrity event in various information technology (IT) enterprise environments, to immediately react to the event in an effort to prevent a complete compromise.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and implement appropriate actions during 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, leaving it modified in an unusable state. Other data integrity attacks may be more dynamic, targeting machines, spreading laterally across networks, and continuing to cause damage throughout an organization. In either case, behaviors are exhibited—such as files inexplicably becoming encrypted or network activity—that provide an ability to immediately detect the occurrence and respond in a timely fashion to curtail the ramifications.

SOLUTION

NIST published version 1.1 of the Cybersecurity Framework in April 2018 to provide guidance on protecting and developing resiliency for 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 v1.1.]

Applying the Cybersecurity Framework to data integrity, this practice guide informs organizations of how to quickly **detect** and **respond** to data integrity attacks by implementing appropriate activities that immediately inform about the data integrity events.

The NCCoE developed and implemented a solution that incorporates multiple systems working in concert to **detect** an ongoing data integrity cybersecurity event. Additionally, the solution provides guidance on how to **respond** to the detected event. Addressing these functions together enables organizations to have the necessary tools to act during a data integrity attack.

The NCCoE sought existing technologies that provided the following capabilities:

- event detection
- forensics/analysis
- integrity monitoring
- logging
- mitigation and containment
- reporting

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

The NCCoE's practice guide to Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events can help your organization:

- develop a strategy for detecting and responding to a data integrity cybersecurity event
- facilitate effective detection and response to adverse events, maintain operations, and ensure the integrity and availability 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/detect-respond. 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.

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.

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, easily 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
301-975-0200

NIST SPECIAL PUBLICATION 1800-26B

Data Integrity

Detecting and Responding to 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

January 2020

DRAFT

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

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-26B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-26B, 53 pages, (January 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

losses due to data integrity events. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, has built an example solution to address these data integrity challenges. This project details methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network. It also identifies tools and strategies to aid in a security team's response to such an event.

KEYWORDS

attack vector; data integrity; malicious actor; malware; malware detection; malware response; ransomware.

ACKNOWLEDGMENTS

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

Name	Organization
Kyle Black	Bay Dynamics
Sunjeet Randhawa	Broadcom Inc.
Peter Romness	Cisco Systems
Matthew Hyatt	Cisco Systems
Matthew Shabat	Glasswall Government Solutions
Justin Rowland	Glasswall Government Solutions
Greg Rhein	Glasswall Government Solutions
Steve Roberts	Micro Focus
Timothy McBride	NIST
Christopher Lowde	Semperis

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

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Information Centric Analytics v6.5.2 Symantec Security Analytics v8.0.1
Cisco Systems	Cisco Identity Services Engine v2.4, Cisco Advanced Malware Protection v5.4, Cisco Stealthwatch v7.0.0
Glasswall Government Solutions	Glasswall FileTrust ATP for Email v6.90.2.5
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Semperis	Semperis Directory Services Protector v2.7

Contents

1 Summary 1

1.1 Challenge 2

1.2 Solution 2

1.3 Benefits 3

2 How to Use This Guide 4

2.1 Typographic Conventions 5

3 Approach 6

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 13

4 Architecture 16

4.1 Architecture Description 16

4.1.1 High-Level Architecture 16

4.1.2 Architecture Components 17

5 Security Characteristic Analysis 20

5.1 Assumptions and Limitations 20

5.2 Build Testing 20

5.3 Scenarios and Findings 20

5.3.1 Ransomware via Web Vector and Self-Propagation 21

5.3.2 Destructive Malware via USB Vector 22

5.3.3 Accidental VM Deletion via Maintenance Script 23

5.3.4 Backdoor Creation via E-mail Vector 24

5.3.5 Database Modification via Malicious Insider 25

5.3.6 File Modification via Malicious Insider 26
5.3.7 Backdoor Creation via Compromised Update Server 26
6 Future Build Considerations 27
Appendix A List of Acronyms 28
Appendix B Glossary 29
Appendix C References 33
Appendix D Functional Evaluation 35
D.1 Data Integrity Functional Test Plan 35
D.2 Data Integrity Use Case Requirements 36
D.3 Test Case: Data Integrity DR -1....................43
D.4 Test Case: Data Integrity DR -2....................45
D.5 Test Case: Data Integrity DR -3....................46
D.6 Test Case: Data Integrity DR -4....................47
D.7 Test Case: Data Integrity DR -5....................49
D.8 Test Case: Data Integrity DR -6....................50
D.9 Test Case: Data Integrity DR -7....................51

List of Figures

Figure 4-1 DI Detect & Respond High-Level Architecture 16

List of Tables

Table 3--1 DI Reference Design Cybersecurity Framework Core Components Map 10
Table 3-2 Products and Technologies 13
Table 6-1 Test Case Fields 35
Table 6-2 Capability Requirements 36
Table 6-3 Test Case ID: Data Integrity DR -1 43
Table 6-4 Test Case ID: Data Integrity DR -2 45
Table 6-5 Test Case ID: Data Integrity DR -3 46
Table 6-6 Test Case ID: Data Integrity DR -4 47
Table 6-7 Test Case ID: Data Integrity DR -5 49
Table 6-8 Test Case ID: Data Integrity DR -6 50
Table 6-9 Test Case ID: Data Integrity DR -7 51

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 detect and respond to DI 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 detect and respond to 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 detection and mitigation of DI events while facilitating analysis of these events.

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

- detect malicious and suspicious activity generated on the network, by users, or from applications that could indicate a DI event
- mitigate and contain the effects of events that can cause a loss of DI
- monitor the integrity of the enterprise for detection of events and after-the-fact analysis
- utilize logging and reporting features to speed response time to DI events
- analyze DI events for the scope of their impact on the network, enterprise devices, and enterprise data
- analyze DI events to inform and improve the enterprise's defenses against future attacks

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

- 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; the benefits of the solution; and the technology partners that participated in building, demonstrating, and documenting the solution. 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 Characteristic 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 that NIST is considering consistent with Cybersecurity Framework Core Functions: Identify, Protect, Detect, Respond, and Recover.

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, such an attack can impact 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.

When DI events occur, organizations should have the capabilities to detect and respond in real time. Early detection and mitigation can reduce the potential impact of events, including damage to enterprise files, infection of systems, and account compromise. Furthermore, organizations should be able to learn from DI events to improve their defenses. Analysis of malicious behavior at the network level, user level, and file level can reveal flaws in the security of the enterprise. Resolution of these flaws, though out of scope of this guide, is often only possible once they have been exploited and with the right solution in place.

1.2 Solution

The NCCoE implemented a solution that incorporates appropriate actions during and directly after a DI event. The solution is composed of multiple systems working together to detect and respond to data corruption events in standard enterprise components. These components include mail servers, databases, end-user machines, virtual infrastructure, and file share servers. Furthermore, an important function of the Respond Category of the Cybersecurity Framework is improvement of defenses—this guide includes components that aid in analysis of DI events and for improving defenses against them.

The NCCoE sought existing technologies that provided the following capabilities:

- Event Detection
- Integrity Monitoring

- Logging
- Reporting
- Mitigation and Containment
- Forensics/Analytics

In developing our solution, we used standards and guidance from the following, 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 140-2: 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 an implementation plan for detecting and responding to cybersecurity events
- facilitate detection, response, and analysis of DI events to improve defenses and mitigate impact

- maintain integrity and availability of data that is 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 detection and response solution. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-26A: *Executive Summary*
- NIST SP 1800-26B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-26C: *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 1800-26A, which describes the following topics:

- challenges that enterprises face in detecting and responding to data integrity events
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-26B, which describes what we did and why. The following sections will be of particular interest:

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

You might share the *Executive Summary,* NIST SP 1800-26A, with your leadership team members to help them understand the importance of adopting a standards-based solution to detect and respond to data integrity events.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-26C, to replicate all or parts of the build created in our lab. The how-to 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 detection and response solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that 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.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

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 Detect and Respond, which consist of detecting and responding to DI attacks. Compromise can come from malicious websites, targeted emails, insider threats, and honest mistakes. Monitoring solutions should be in place to detect these events. Once detected, swift response to a threat is critical to mitigate the need for recovery action after an event occurs. 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 is intended to provide practical guidance to any organization interested in implementing a solution for detecting and responding to 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 capability to comprehensively detect, mitigate, and learn from cybersecurity events. The platforms demonstrated by this project and the implementation information provided in this practice guide permit integration of products to implement a data integrity detection and response 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 Volume 1, specifically the Core Functions of Detect and Respond. Detecting emphasizes developing and implementing the appropriate activities to detect events in real time, compare the current system state to a norm, and produce audit logs for use during and after the event. Responding emphasizes real-time mitigation of events, forensic analysis during and after the event, and reporting. Examples of outcomes within these functions are integrity monitoring, event detection, logging, reporting, forensics, and mitigation.

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 basic organization's IT enterprise. It does not reflect the complexity of a production environment: for example, building across numerous physical locations, accommodating 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 skill sets and resources required to implement an event detection and response system.
- A DI event is taking place, and the organization is seeking to detect and mitigate the damage that an event is causing.

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*—publicly available material. The Risk Management Framework (RMF) guidance, as a whole, proved 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 assessment:

- Initial analysis of the risk factors discussed with financial, retail, and hospitality institutions. This analysis led to creation of the DI project and the desired security posture. See NISTIR 8050, Executive Technical Workshop, 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. Having produced *Data Integrity: Recovering from Ransomware and Other Destructive Events,* which primarily focused on the recovery aspect of DI, we identified a need for guidance in the areas of detecting and responding to cybersecurity events in real time.

When considering risk from the perspective of detecting and responding to cybersecurity events during their execution, 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 these:

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

The types of vulnerabilities we consider in relation to these threats include:

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

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

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

Analysis of the threats, vulnerabilities, and potential impact to an organization has given us an understanding of the risk for organizations 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 is a summary of 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 event detection and response 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 the damage caused by active events and facilitates the information needed to learn from the events.
- 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 security Functions and Subcategories that we wanted the reference design to support through a risk analysis process. This was a critical first step in drafting 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 that 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 Detect/Respond capabilities, also uses PR.DS-6, a Protect Subcategory. This is primarily because creation of integrity baselines is used for comparison when detecting attacks but is created prior to the start of an attack.
- Not all the Cybersecurity Framework Subcategories guidance 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 called Respond are processes and policies that should be developed prior to implementing recommendations.

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

Cybersecurity Framework v1.1				Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
PROTECT (PR)	Data Security (PR.DS)	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
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	AC-4, CA-3, CM-2, SI-4	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	SP-ARC-001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6, CA-7, IR-4, SI-4	A.12.4.1, A.16.1.1, A.16.1.4	PR-CDA-001
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	A.12.4.1, A.16.1.7	CO-OPS-001, PR-CIR-001
		DE.AE-4: Impact of events is determined.	CP-2, IR-4, RA-3, SI-4	A.16.1.4	PR-INF-001

Cybersecurity Framework v1.1				Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
		DE.AE-5: Incident alert thresholds are established.	IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events.	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4		OM-NET-001
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	A.12.4.1, A.12.4.3	AN-TWA-001
		DE.CM-4: Malicious code is detected.	SI-3, SI-8	A.12.2.1	SP-DEV-001
		DE.CM-5: Unauthorized mobile code is detected.	SC-18, SI-4, SC-44	A.12.5.1, A.12.6.2	SP-DEV-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	A.12.4.1, A.14.2.7, A.15.2.1	AN-TWA-001
	Detection Processes (DE.DP)	DE.DP-2: Detection activities comply with all applicable requirements.	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	A.18.1.4, A.18.2.2, A.18.2.3	PR-CDA-001
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or after an incident.	CP-2, CP-10, IR-4, IR-8	A.16.1.5	PR-CIR-001

Cybersecurity Framework v1.1				Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
	Communications (RS.CO)	RS.CO-2: Incidents are reported consistent with established criteria.	AU-6, IR-6, IR-8	A.6.1.3, A.16.1.2	IN-FOR-002
	Analysis (RS.AN)	RS.AN-1: Notifications from detection systems are investigated.	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	A.12.4.1, A.12.4.3, A.16.1.5	PR-CDA-001
		RS.AN-2: The impact of the incident is understood.	CP-2, IR-4	A.16.1.4, A.16.1.6	PR-CIR-001
		RS.AN-3: Forensics are performed.	AU-7, IR-4	A.16.1.7	IN-FOR-002
		RS.AN-4: Incidents are categorized consistent with response plans.	CP-2, IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
	Mitigation (RS.MI)	RS.MI-1: Incidents are contained.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001
		RS.MI-2: Incidents are mitigated.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001

3.5 Technologies

Table 3-2 lists all of 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.

Table 3-2 Products and Technologies

<table>
<tr><th>Component</th><th>Product</th><th>Function</th><th>Cybersecurity Framework Subcategories</th></tr>
<tr><td rowspan="2">Integrity Monitoring</td><td>Tripwire Enterprise v8.7</td><td rowspan="2">Provides file hashes and integrity checks for files and software, regardless of file type.
Provides integrity monitoring for data.
Provides integrity monitoring for Active Directory.</td><td rowspan="2">PR.DS-6, DE.AE-1, DE.CM-3, DE.CM-7</td></tr>
<tr><td>Semperis Directory Services Protector (DSP) v2.7</td></tr>
<tr><td rowspan="3">Event Detection</td><td>Cisco Advanced Malware Protection (AMP) v5.4</td><td rowspan="3">Provides the ability to receive information about new threats.
Provides the ability to statically detect malicious software.</td><td rowspan="3">DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-7</td></tr>
<tr><td>Glasswall FileTrust ATP for Email v6.90.2.5</td></tr>
<tr><td>Cisco Stealthwatch v7.0.0</td></tr>
</table>

Component	Product	Function	Cybersecurity Framework Subcategories
	Semperis DSP v2.7	• Provides ability to dynamically detect malicious software. • Provides ability to detect malicious email attachments. • Provides ability to scan the network for anomalies. • Provides the ability to monitor user behavior for anomalies. • Provides ability to scan email attachments for deviations from file type specifications or organizational policy.	
Logging	Micro Focus ArcSight Enterprise Security Manager (ESM) v7.0 Patch 2 Tripwire Log Center v7.3.1	• Provides auditing and logging capabilities configurable to organizational policy. • Correlates logs of cybersecurity events with user information. • Provides automation for logging.	DE.AE-1, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-3, DE.CM-7, RS.AN-2
Forensics/Analytics	Cisco AMP v5.4 Symantec Security Analytics v8.0.1 Micro Focus ArcSight ESM v7.0 Patch 2 Symantec Information Centric Analytics (ICA) v6.5.2	• Provides forensics to track effects of malware retrospectively. • Provides network traffic analysis. • Provides ability to analyze files sent over the network. • Provides analysis capabilities for finding anomalies in enterprise activity.	DE.AE-2, DE.AE-4, DE.CM-1, RS.RP-1, RS.AN-1, RS.AN-2, RS.AN-3
	Cisco AMP v5.4		

Component	Product	Function	Cybersecurity Framework Subcategories
Mitigation and Containment	Cisco Identity Services Engine (ISE) v2.4 Glasswall FileTrust ATP for Email v6.90.2.5 Semperis DSP v2.7	• Provides ability to sandbox files locally. • Provides ability to enforce policy across the enterprise. • Provides ability to quarantine devices across the enterprise. • Provides ability to sanitize files through file reconstruction. • Provides ability to revert changes to domain services.	DE.CM-5, RS.RP-1, RS.MI-1, RS.MI-2
Reporting	Micro Focus ArcSight ESM v7.0 Patch 2	• Provides ability to send security alerts based on organizational policy. • Provides ability to provide reports of enterprise health. • Provides ability to provide reports of malware detection across the enterprise.	DE.AE-5, RS.RP-1, RS.CO-2

4 Architecture

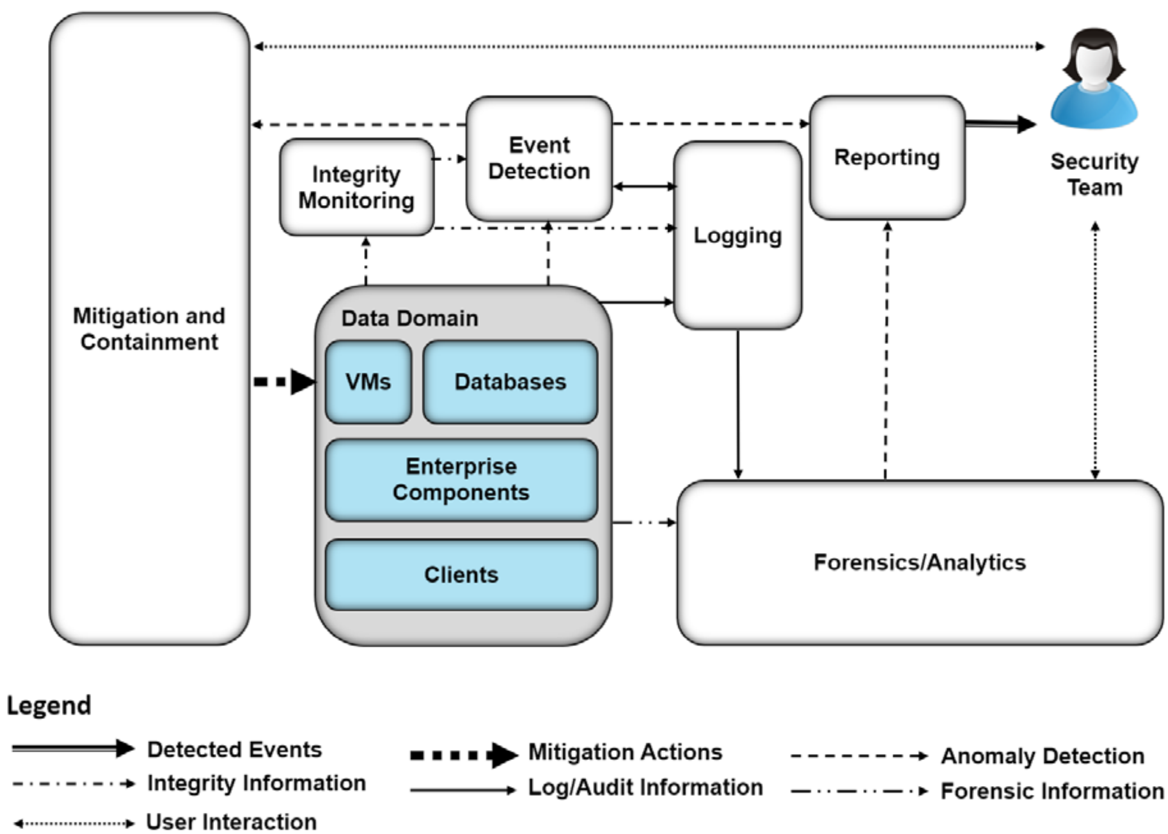
This section presents the high-level architecture used for implementation of a DI solution that detects and responds to ransomware and other destructive events.

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 Detect & Respond High-Level Architecture



- Integrity Monitoring provides capabilities for comparing current system states against established baselines.

- Event Detection provides capabilities for detecting ongoing events and can be composed of intrusion detection, malware detection, user anomaly detection, and others, depending on the established threat model of the organization.
- Logging records and stores all the log files produced by components within the enterprise.
- Forensics/Analytics provides the capability to probe/analyze logs and machines within the enterprise to learn from DI events.
- Mitigation and Containment allows responding to DI events by containing and limiting the threat's ability to affect the system.
- Reporting provides the capability to report on all activities within the enterprise and within the reference architecture for analysis by a security team.

These capabilities work together to provide the Detect and Respond Functions for DI. The integrity monitoring capability collects integrity information prior to attacks so that when an attack happens, records of all file/system changes are preserved. In combination with event detection, these records not only function as a tool to inform recovery but also as early indicators of compromise. Event detection uses these records and its own mechanisms to actively detect events as they happen and to take appropriate action through other components of the reference architecture. Logging collects information from event detection and integrity monitoring for use in response functions. Mitigation and Containment provides capabilities to stop ongoing attacks and limit their effect on the system. Forensics/Analytics allow analysis of logs and threat behavior to aid the organization in learning from the attack. Reporting provides capabilities for reporting information from analysis and logging to the appropriate parties both during and after an attack. The information gained from these attacks can be used to inform products that fall in the Identify Function of the Cybersecurity Framework to indicate vulnerabilities in the enterprise that need to be remediated.

4.1.2 Architecture Components

4.1.2.1 Integrity Monitoring

The Integrity Monitoring component 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 detecting and responding to an active attack, being able to track changes to files is critical. Asset integrity changes can provide an early detection mechanism by tracking changes made at abnormal times or by tracking users who typically do not make such changes. Furthermore, the changes tracked during a DI event can be used to inform the 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.

Integrity Monitoring typically requires an operation baseline to be taken prior to the start of a DI event—this baseline is used for comparison against the system's state during an attack.

For the Integrity Monitoring capability, we use a combination of two tools: Tripwire Enterprise and Semperis DSP. Once a baseline is taken prior to an attack, Tripwire Enterprise stores integrity information for selected data across all systems. When a “check” is run, Tripwire collects all the changes that occurred to monitored files on those systems. These changes are forwarded to the Logging component, which can then report and alert on them, becoming an indicator of a DI event. Furthermore, these collected changes can be used to help remediate the effects of malware on a system.

Semperis DSP provides a similar function but with a focus on Active Directory. Changes to Active Directory users, groups, and other services are collected and can be used to notify administrators of potentially malicious activity. Given the sensitive nature of Active Directory, Semperis DSP does not rely on a single source of information but instead monitors multiple aspects of Active Directory. This helps ensure that any change to permissions or privileged credentials is captured, including changes that attackers attempt to hide (for example, by circumventing security auditing).

4.1.2.2 Event Detection

The Event Detection component provides the ability to detect events as they happen. This can be achieved through a combination of mechanisms, depending on the needs of the organization. Analysis of integrity monitoring logs can indicate malicious activity. Malware detection, behavior-based anomaly detection, and intrusion detection are all potential examples of event detection. The goal of this component is to detect events as they happen, to trigger the appropriate responses, and to provide information about the attack to the security team.

For the event detection capability, we use a combination of tools. Cisco AMP is used to detect malicious files. Glasswall FileTrust ATP for Email is used to identify malicious email attachments that do not conform to file standards and organizational policies. Cisco Stealthwatch is used to detect malicious network activity. Finally, Semperis DSP is used to detect changes in Active Directory. Information from these four can be correlated to identify malicious patterns of behavior from users.

4.1.2.3 Logging

Logging from each component serves several functions in an architecture that aims to detect and respond to active DI events. Logs are produced through integrity monitoring and event detection, which aid other components in responding to active events. Both Mitigation and Containment and Forensics/Analytics use logs to inform their actions—logs tell them what systems are being affected and what programs are causing the event. Further, these logs help decide what steps should be taken to remediate the attack and protect against it going forward.

For the Logging capability, we use a combination of two tools: Micro Focus ArcSight and Tripwire Log Center. While Tripwire Log Center’s purpose in this build is primarily to collect, transform, and forward logs from Tripwire Enterprise to ArcSight, ArcSight performs a wider function. ArcSight collects logs from various sources in the enterprise, such as Event Detection and Integrity Monitoring, as well as Windows event logs and Ubuntu syslogs. The goal of this widespread collection is to provide a base for the Forensics/Analytics component.

4.1.2.4 Mitigation and Containment

The Mitigation and Containment component provides the ability to limit a destructive event's effect on the enterprise. This component may be able to interact with a security team for greater effectiveness and may have the option to provide automated response to certain DI events. This response can involve stopping execution of associated programs, disabling user accounts, disconnecting a system from the network, and more, depending on the threat. Other actions may involve removing software from a system, restarting services, or copying the threat to a safe environment for analysis.

For the Mitigation and Containment capability, we use a combination of tools. Cisco AMP provides the ability to remove malicious files on sight—combined with its event detection capability, this can be leveraged to quickly respond to malware on user systems. Cisco ISE provides quarantine functions that can be used to respond to detected malware and poor machine posture as well as to network events in Stealthwatch. Semperis DSP provides the ability to quickly and automatically revert detected changes in Active Directory, mitigating the use of backdoors and other malicious domain changes. Semperis DSP can also disable user accounts to prevent further changes from compromised or maliciously created accounts. Glasswall provides the ability to sanitize malicious or noncompliant email attachments before they ever reach the user's inbox, thereby eliminating malicious content in email attachments.

4.1.2.5 Forensics/Analytics

The Forensics/Analytics component uses the logs generated by event detection and the enterprise to discover the source and effects of the DI event and learn about how to prevent similar events in the future, if possible. This component will typically allow an organization to analyze malware or logs related to the malware's execution and produce information such as: the servers that the malware communicates with, or the executable's signature, to improve detection of the malware in the future. Furthermore, the ability to examine machines affected by malware for lasting effects may be desirable. The information gained from forensic analysis can also be used to enhance the organization's protections against malware and potentially reform policy in the organization.

For the Forensics/Analytics capability, we use a combination of tools. Cisco AMP provides the ability to review the history of malicious files to determine the source and movement across the enterprise. Symantec Security Analytics provides the ability to analyze network traffic in a similar manner. ArcSight ESM provides event correlation capabilities for logs collected from almost all the other capabilities, allowing processing of events before they are reported to the security team. Symantec ICA provides additional analysis capabilities for logs as well as aggregation and visualization of certain potentially malicious movements within the enterprise. These products aid in the future prevention of such attacks as well as determine the scope of the event's effect on the system.

4.1.2.6 Reporting

The Reporting component is primarily an interface between various components of the architecture and the security team. It allows alerting based on events through email and dashboards, depending on the organization's need. The reporting capabilities are best used throughout the entirety of an event—they can be used to alert the security team when an event starts as well as to provide regular status updates when events are not happening or have just finished.

For the Reporting capability, we use Micro Focus ArcSight. ArcSight can send email alerts and generate reports based on the log correlation and analysis that it performs. By ensuring integration of as many relevant logs as possible with ArcSight's logging capabilities, we can use various indicators to trigger alerts when certain logs or sets of logs are received by ArcSight.

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 detect-and-respond 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 detecting and responding to DI events. Furthermore, the project aims to facilitate analysis of these events during and after an attack. In addition, it seeks to understand the security benefits and drawbacks of the reference design.

5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that 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 are 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 to which it propagated and demands payment in exchange for decryption of these files.

5.3.1.2 Resolution

The build provides a significant defense in depth against this use case.

The **Event Detection** capability provides the ability to detect malicious software on the system and generate logs and alerts based on this activity. It also allows for the detection of suspicious network behavior, such as propagation.

The **Mitigation and Containment** capability provides the ability to halt execution of the ransomware and remove it from the system. Furthermore, it allows quarantine of the affected machine(s) from the network after detection of malicious activity.

The **Integrity Monitoring** capability provides the ability to collect changes to files, including changes made by the ransomware as well as the ransomware's first creation or download onto the system.

When forwarded to the **Logging** capability, these logs in combination with others can be used to identify the scope of the attack.

The **Reporting** capability uses logs from the above capabilities to report on malicious activity and to increase response time.

The **Forensics/Analytics** capability analyzes logs related to the event to provide information that can be used to strengthen defenses against the attack in the future. This includes the websites it communicated with or was downloaded from, the signature of the executable, and the scope of the attack.

5.3.1.3 Other Considerations

Because malware comes in many forms, it is imperative to have multiple layers of defense against it while also working to actively improve these defenses. An early defense against malware means blacklisting known malicious sites. However, because this must be done entirely before the attack takes place, it is out of scope of this build.

This build suggests a Forensics/Analytics capability specifically for informing and strengthening the enterprise's defenses against future attacks. This is a function of the Respond Category—learning from attacks can inform defense of such attacks in the future, both in the Protect and Detect phases of the attack. Blacklisting is one such defense that can be informed by the Respond Category, and Event Detection is another.

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 his or her 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

The build provides several mechanisms to detect and mitigate this use case.

The **Integrity Monitoring** capability provides the ability to detect changes to the file system, allowing the changes and deletions to be detected and logged. Furthermore, information about what program (and by extension, where the program was located—that is, on a USB drive) is included in the logs.

The **Logging** capability is used to collect logs from the integrity monitoring capability for posterity, as well as from Windows event logs to monitor usage of external drives in comparison to normal usage.

The **Event Detection** capability provides the ability to detect malicious files on the USB inserted into the system. It also can detect execution of these files.

The **Mitigation and Containment** capability provides the ability to stop malicious files from executing as well as delete the files on the USB drive.

5.3.2.3 Other Considerations

USB attacks do not always come in the form of disguised file-based malware. As USB attacks allow direct interfacing with the hardware of the system, they can aim to destroy the system via electrical attacks or involve impersonation of a keyboard or other devices to avoid detection and gain privileges. These attacks may be better mitigated through a thorough physical security policy and restrictions on the types of allowed connected devices. Advanced attacks that involve manipulation of hardware can become increasingly difficult to detect once plugged into the system. A prevention solution involving backups, physical security, and employee education is often more effective.

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 data integrity events that occur on virtual machines.

A routine maintenance script on the system causes an error. During a move operation in the Hyper-V system, the script deletes an important virtual machine (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. It is expected that the build will mitigate the damage caused to virtual machines in such an incident.

5.3.3.2 Resolution

The build provides several methods for detecting and analyzing this use case. Errors in custom code are often difficult to detect at run time and because they are usually run by privileged programs. Classifying them as malware or even as "unintended" changes is often undesirable.

The **Integrity Monitoring** capability provides the ability to detect changes to VM configurations, allowing the VM deletion to be detected and logged. Furthermore, information about what program (i.e., the routine maintenance script) is included in the logs.

The **Logging** capability provides the ability to collect these events for posterity.

The **Forensics/Analytics** capability provides the ability to analyze the events after the fact to enable the security team to understand the impact, resolve the error in the script, and inform the restoration process.

5.3.3.3 Other Considerations

This solution will aid in identifying the script that causes a configuration change or deletion, but ultimately some things cannot be automated by the solution. Understanding the impact of the event requires a security team, and this build aims to provide the tools for a security team to do so.

Resolving an error in a maintenance script will also typically require effort on the part of the system administrators. Judgment on whether a script should be deleted, disabled, or left running during the remediation process is necessary and can depend on the size of the script, the affected assets, and the availability of resources to put toward resolving the error. Because of these considerations, the organization is left to decide whether a malfunctioning script should be treated like malware (see other scenarios that deal with malware) or as a part of the enterprise as it is possible that the remediation process is lengthy and exceeds the scope of the Detect/Respond Categories of the NIST Cybersecurity Framework.

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 that was 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. It is expected that the build will 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 forwards logs of file changes and Active Directory changes to the Logging capability, allowing recording and detection of both the malicious attachment's download and the changes it makes to the system account structure.

The **Logging** and **Reporting** capabilities provide the ability to generate alerts based on events for the security team to quickly take action to resolve them.

The **Event Detection** capability provides detection at two points in time—both before the attachment reaches the user's inbox and, should this fail, after the attachment downloads to the system.

The **Mitigation and Containment** capability provides mitigation before the attachment reaches the user's inbox, as well as when it is on the user's system.

The **Forensics/Analytics** capability provides the ability to view the network traffic generated by the spreadsheet when fetching its malicious files from the web server. This can inform defense of the enterprise in the Protect Category of the Cybersecurity Framework before any similar events happen in the future.

5.3.4.3 Other Considerations

Another defense that can partially prevent this use case is detection of the email as spam. However, as this is often a function of the email provider and not a separate security solution, it is out of scope for this build.

This build suggests a Forensics/Analytics capability specifically for informing and strengthening the defenses of the enterprise against future attacks. This is a function of the Respond Category—learning from attacks can inform the defense of such attacks in the future, both in the Protect and Detect phases of the attack.

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. It is expected that the build will mitigate the impact that a user can have on the database.

5.3.5.2 Resolution

The build provides several layers of defense against this use case. The **Integrity Monitoring** capability is used to detect changes to the database.

These changes are forwarded to the **Logging** capability, which also collects information about web requests.

The **Reporting** capability provides the ability to generate alerts and quickly inform the security team of an anomaly, based on the logs.

The **Forensics/Analytics** capability is used to investigate the malicious access as well as identify the page with the vulnerability. Because this vulnerability is a vulnerability in custom code, it is important for information-gathering mechanisms to be in place to provide ample information for the resolution of this vulnerability.

5.3.5.3 Other Considerations

This use case highlights the need for a response-oriented build to collaborate with an identify-oriented build. Identification and resolution of vulnerabilities in custom code are sometimes feasible only through gathering information after the vulnerability has been exploited. This build provides the mechanisms to gather such information, but it is ultimately up to the security team to resolve the vulnerability and learn from the attack.

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 non-technical means. The insider, using these credentials, uses remote Windows PowerShell sessions to uniformly modify employee stock information to their benefit across several machines. This attack will also target the enterprise's backup system to modify all records of the previous stock information. It is expected that the aspects of the build described above will 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 has several layers of defense against this use case. The **Integrity Monitoring** capability detects changes to files and backups caused by a malicious insider.

When forwarded to the **Logging** and **Reporting** capabilities, the build can report on these changes. Irregularities or differences from the normal backup schedule are important indicators of a compromise.

When the security team is alerted to a malicious insider, they can use the **Mitigation and Containment** capability to disable the insider's access.

5.3.6.3 Other Considerations

Malicious insiders are powerful adversaries, because they already have some level of access to the system. The existence of malicious insiders widens the threat surface of an enterprise to needing defense against internal machines as well as external machines. For this reason, this build includes mitigations against threats already present inside the enterprise and not just threats that originate externally. This includes the ability to disable user accounts, quarantine machines, and monitor network traffic originating from within the enterprise.

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 an attacker root access into the machine updated by the compromised server. It is expected that the build will mitigate the impact of a compromised update server.

5.3.7.2 Resolution

The build has several layers of defense against this use case. **Integrity Monitoring** detects changes to programs, providing information about how and when the program was changed. It also detects changes to any files made by an intruder.

The **Event Detection** capability is used to detect the malicious update through signature detection. Furthermore, it detects the connection to the open port by an attacker.

The **Mitigation and Containment** capability is used to delete/quarantine the malicious update, stopping the port from being accessible. It can also be used to quarantine the machine from the network, to prevent the spread of the intrusion and remove the attacker's access.

5.3.7.3 Other Considerations

The use of the Event Detection capability to detect largely assumes that the update has been reported as vulnerable, either through a well-known history of being vulnerable or through intelligence-sharing channels. As such, an event detection capability would, in some cases of new custom attacks, be unable to detect this at first sight. However, the build provides other tools, such as monitoring network activity, that can alert security staff to such attacks.

Using a data integrity identify-and-protect build to incorporate Blacklisting and Network Protection as part of the defense is beneficial, as a use case that involves connecting to an unused port would be entirely defeated by a network protection white list of allowed ports.

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 share 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

AMP	Advanced Malware Protection
COI	Community of Interest
DE	Detect
DI	Data Integrity
DSP	Directory Services Protector
ESM	Enterprise Security Manager
ICA	Information Centric Analytics
ISE	Identity Services Engine
IT	Information Technology
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
PR	Protect
RMF	Risk Management Framework
RS	Respond
SP	Special Publication
USB	Universal Serial Bus
VM	Virtual Machine
vsftpd	Very Secure File Transfer Protocol Daemon

Glossary

Access Control	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) SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009
Architecture	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). SOURCE: FIPS 201-2
Audit	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. SOURCE: CNSSI 4009-2015
Backdoor	An undocumented way of gaining access to a computer system. A backdoor is a potential security risk. SOURCE: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2
Backup	A copy of files and programs made to facilitate recovery if necessary. SOURCE: NIST SP 800-34 Rev. 1
Compromise	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. SOURCE: NIST SP 800-32

Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. SOURCE: NIST SP 800-137
Cybersecurity	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)
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. SOURCE: CNSSI-4009
Information Security	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)
Information Security Risk	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)
Information System	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)
Insider	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)

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

Appendix B References

[1] A. 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. Availabe: 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.

Appendix C 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 detecting and responding to DI events. Furthermore, this project aims to analyze the events to aid recovery and protection of the enterprise against future attacks. The evaluation verified that the example implementation could perform the following functions:

- Detect malicious network activity, malicious mobile code, malicious code execution, and unauthorized user behavior.
- Contain and analyze these types of incidents.
- Mitigate the impact of these incidents as they occur.
- Report relevant details for use in mitigation and protection against future events.

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.

C.1 Data Integrity Functional Test Plan

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that 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.

Test Case Field	Description
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
Description	Describes the objective of the test case.
Associated Cybersecurity Framework Subcategories	Lists the National Institute of Standards and Technology Special Publication 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-case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

C.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	Subrequirement 1	Test Case
CR 1	The DI example implementation shall detect and respond to malware that encrypts files and displays notice demanding payment.		Data Integrity DR-1

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 1.a		File integrity changes are collected and logged.	Data Integrity DR-1
CR 1.b		Access is halted.	Data Integrity DR-1
CR 1.c		Executable is identified as malicious, using a blacklist.	Data Integrity DR-1
CR 1.d		Executable is identified as malicious through analysis, and blacklist is updated.	Data Integrity DR-1
CR 1.e		Execution is halted.	Data Integrity DR-1
CR 1.f		Downloads are identified as malicious, using a blacklist.	Data Integrity DR-1
CR 1.g		Downloads are identified as malicious through analysis, and blacklist is updated.	Data Integrity DR-1
CR 1.h		Downloads are prevented.	Data Integrity DR-1
CR 1.i		Attempts to propagate are detected.	Data Integrity DR-1
CR 1.j		Machines attempting to propagate are prevented from propagating.	Data Integrity DR-1
CR 1.k		Suspicious network traffic is detected, and blacklist is updated.	Data Integrity DR-1

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 2	The DI example implementation shall detect and respond to malware inserted via Universal Serial Bus (USB) that modifies and deletes user data.		Data Integrity DR-2
CR 2.a		File integrity changes are collected and logged.	Data Integrity DR-2
CR 2.b		The insertion of a USB device is detected and logged.	Data Integrity DR-2
CR 2.c		The executable is identified as malicious, using a blacklist.	Data Integrity DR-2
CR 2.d		The executable is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-2
CR 2.e		Malicious executable is halted or deleted.	Data Integrity DR-2
CR 3	The DI example implementation shall detect and respond to virtual machine deletion.		Data Integrity DR-3
CR 3.a		Virtual machine integrity changes are collected and logged.	Data Integrity DR-3

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 3.b		The event causing deletion of the virtual machine is analyzed.	Data Integrity DR-3
CR 4	The DI example implementation shall detect and respond to malware received via phishing email.		Data Integrity DR-4
CR 4.a		Configuration integrity changes are collected and logged.	Data Integrity DR-4
CR 4.b		Email is identified as malicious, using a blacklist.	Data Integrity DR-4
CR 4.c		Email is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-4
CR 4.d		Email is deleted or sorted into spam.	Data Integrity DR-4
CR 4.e		The attachment is identified as malicious, using a blacklist.	Data Integrity DR-4
CR 4.f		The attachment is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-4
CR 4.g		Execution of the spreadsheet is stopped, and the blacklist updated if necessary.	Data Integrity DR-4

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 4.h		The downloads are identified as malicious, using a blacklist.	Data Integrity DR-4
CR 4.i		The downloads are identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-4
CR 4.j		The malicious executable is halted or deleted.	Data Integrity DR-4
CR 4.k		Suspicious network traffic is detected, and blacklist is updated.	Data Integrity DR-4
CR 5	The DI example implementation shall detect and respond to changes to the database made through a web server vulnerability in custom code.		Data Integrity DR-5
CR 5.a		Database integrity changes are collected and logged.	Data Integrity DR-5
CR 5.b		Information about the client interacting with the web service is collected and logged.	Data Integrity DR-5
CR 5.c		Information from the attack is reported for use in protection against future events.	Data Integrity DR-5

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 6	The DI example implementation shall detect and respond to targeted modification by malicious insiders with elevated privileges.		Data Integrity DR-6
CR 6.a		File integrity changes are collected and logged.	Data Integrity DR-6
CR 6.b		Backup integrity changes are collected and logged.	Data Integrity DR-6
CR 6.c		Detected changes are reported.	Data Integrity DR-6
CR 6.d		Associated user accounts are contained.	Data Integrity DR-6
CR 7	The DI example implementation shall detect and respond to an intrusion via compromised update server.		Data Integrity DR-7
CR 7.a		Program integrity changes are collected and logged.	Data Integrity DR-7
CR 7.b		The downloaded service is identified as malicious, using a blacklist.	Data Integrity DR-7
CR 7.c		The downloaded service is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-7

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 7.d		The service is halted and reverted or deleted.	Data Integrity DR-7
CR 7.e		The download site is temporarily added to the blacklist.	Data Integrity DR-7
CR 7.f		The port opened by the service is detected.	Data Integrity DR-7
CR 7.g		The opened port is closed.	Data Integrity DR-7
CR 7.h		The intrusion into the infected machine is detected.	Data Integrity DR-7
CR 7.i		The intrusion into the infected machine is contained.	Data Integrity DR-7

C.3 Test Case: Data Integrity DR-1

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

Parent requirement	(CR 1) The DI example implementation shall detect and respond to malware that encrypts files and displays notice demanding payment.
Testable requirement	(CR 1.a) Integrity Monitoring, Logging, Reporting, (CR 1.c, CR 1.d, CR 1.f, CR 1.g, CR 1.i) Event Detection, (CR 1.b, CR 1.e, CR 1.j) Mitigation and Containment, (CR 1.h, CR 1.k) Forensics and Analytics
Description	Show that the DI solution has capabilities to detect behaviors typical of ransomware, and mitigate these behaviors appropriately.
Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2,DE.CM-4, DE.CM-7, DE.DP-2, DE.AE-1, DE.CM-1
Preconditions	User navigates to a malicious website and clicks on an ad for a virus cleaner. The virus cleaner is ransomware, which propagates across the domain and encrypts user files.
Procedure	The **Integrity Monitoring** capability is used to monitor and log changes to the integrity of files. The **Logging** capability and the **Reporting** capability are used to notify the security team of changes to the integrity of files and of potentially malicious events. The **Event Detection** capability is used to detect the ransomware in real time before or during its execution. It is also used to detect propagation of the ransomware. The **Mitigation and Containment** capability is used to halt the ransomware's execution and delete it from the system. It is also used to quarantine affected machines once a breach is discovered. The **Forensics/Analytics** capability is used to discover malicious hosts and websites accessed by the ransomware.
Expected Results (pass)	The build can monitor and report changes to the integrity of files (CR 1.a). The machine is quarantined when malware is detected (CR 1.b).

	Malicious executables are identified through signature detection or analysis (CR 1.c, CR 1.d). Malicious executables are prevented from executing (CR 1.e). Malicious downloads are identified through signature detection or analysis (CR 1.f, CR 1.g). Malicious downloads are prevented (CR 1.h). Propagation of malicious executables is detected (CR 1.i). Propagation of malicious executables is prevented (CR 1.j). Network traffic is captured and analyzed for suspicious activity (CR 1.k).
Actual Results	**Tripwire Enterprise (Integrity Monitoring)** is used to successfully detect changes to files on the affected systems. **ArcSight ESM (Logging)** is used to successfully log events from Event Detection and Integrity Monitoring for use in Reporting and Forensics/Analytics. **ArcSight ESM (Reporting)** is used to successfully report on malicious activity detected in logs. **Cisco AMP (Event Detection)** is used to successfully detect the malicious executable. **Cisco AMP (Mitigation and Containment)** is used to successfully remove malicious executables from the affected systems. **Cisco Stealthwatch (Event Detection)** is used to successfully capture malicious or suspicious network traffic from the executable. **Cisco ISE (Mitigation and Containment)** is used to successfully quarantine affected machines. **Symantec Security Analytics (Forensics/Analytics)** is used to successfully review network traffic generated by the ransomware for potentially malicious hosts and websites.

	Symantec ICA (Forensics/Analytics) successfully displays relevant events from ArcSight for analysis to aid in identifying the malicious files for use in future Event Detection as well as for removal by the security team.
Overall Result	Pass. All requirements for this use case are met.

870 ## C.4 Test Case: Data Integrity DR-2

871 **Table 6-4 Test Case ID: Data Integrity DR-2**

Parent requirement	(CR 2) The DI example implementation shall detect and respond to malware inserted via USB that modifies and deletes user data.
Testable requirement	(CR 2.a) Integrity Monitoring, (CR 2.b, CR 2.c) Event Detection, (CR 2.d) Forensics and Analytics, (CR 2.e) Mitigation and Containment
Description	Show that the DI solution can detect behaviors of destructive malware and can mitigate these behaviors appropriately.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
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	The **Integrity Monitoring** capability is used to monitor integrity changes to the system. The **Logging** capability is used to collect logs from the integrity monitoring capability. The **Event Detection** capability is used to detect malicious files on the USB inserted into the system. The **Mitigation and Containment** capability is used to prevent malicious files from executing.
Expected Results (pass)	The build can monitor and report changes to the integrity of files (CR 2.a). The build can detect insertion of a USB (CR 2.b). Malicious executables are identified through signature detection or analysis (CR 2.c, CR 2.d).

	Malicious executables are prevented from executing (CR 2.e).
Actual Results	**Tripwire Enterprise (Integrity Monitoring)** successfully detects changes made by an executable running from a USB. **ArcSight ESM (Logging)** successfully collects logs from the integrity monitoring capability. Furthermore, USB insertions can be collected by using Windows group policy. **Cisco AMP (Event Detection)** successfully detects malicious files on the USB drive. **Cisco AMP (Mitigation and Containment)** immediately deletes these malicious files on the system if they are copied. It also prevents execution if the file is run from the USB drive.
Overall Result	Pass (partial). Cisco AMP does not immediately delete the file from the USB drive when it is plugged in if the user does not make any action (copy or execution). However, because both these actions trigger deletion, this is not a significant shortcoming as the file is otherwise harmless.

C.5 Test Case: Data Integrity DR-3

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

Parent requirement	(CR 3) The DI example implementation shall detect and respond to virtual machine deletion.
Testable requirement	(CR 3.a) Integrity Monitoring, (CR 3.b) Forensics and Analytics
Description	Show that the DI solution can detect and analyze DI events that involve virtual machines.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A routine maintenance script contains an error that accidentally deletes a virtual machine.
Procedure	The **Integrity Monitoring** capability is used to monitor integrity changes to the system. The **Logging** capability is used to collect logs from the integrity monitoring capability.

	The **Forensics/Analytics** capability is used to analyze logs and determine the cause of integrity events.
Expected Results (pass)	The build can monitor and report changes to the integrity of virtual machines (CR 3.a). The build can analyze the impact of DI events (CR 3.b).
Actual Results	**Tripwire Enterprise (Integrity Monitoring)** successfully monitors and logs changes to configurations of virtual machines. **ArcSight ESM (Logging)** successfully collects logs and reports on the events generated by the Integrity Monitoring capability, enabling faster response time. **Symantec ICA (Forensics/Analytics)** successfully displays relevant events from ArcSight for analysis to aid in identifying the file that causes the deletion.
Overall Result	Pass. All requirements for this use case are met.

874 ## C.6 Test Case: Data Integrity DR-4

875 **Table 6-6 Test Case ID: Data Integrity DR-4**

Parent requirement	(CR 4) The DI example implementation shall detect and respond to malware received via phishing email.
Testable requirement	(CR 4.a) Integrity Monitoring and Logging, (CR 4.b, CR4.e, CR 4.h, CR 4.k) Event Detection, (CR 4.c, CR 4.f, CR 4.i) Forensics and Analytics, (CR 4.d, CR 4.g, CR 4.j) Mitigation and Containment
Description	Show that the DI solution can detect malicious attachments and respond to malicious configuration changes.
Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	The user receives a phishing email with a malicious spreadsheet attached. The spreadsheet is downloaded and opened, causing account changes in Active Directory.
Procedure	The **Integrity Monitoring** capability is used to detect and log the account creation.

	This information is forwarded to the **Logging** capability, along with other available Active Directory information. The email attachment is detected as malicious by the **Event Detection** capability and mitigated by the **Mitigation and Containment** capability, both when the file is in the inbox and when it is on the user's system. The solution can review the network traffic generated by the file when it calls out to the malicious web server to download files through **Forensics/Analytics**.
Expected Results (pass)	The build can monitor and report changes to the integrity of configurations (CR 4.a). Malicious emails are identified through signature detection or analysis (CR 4.b, CR 4.c). Emails identified as malicious are sorted into spam or deleted (CR 4.d). Malicious attachments are identified through signature detection or analysis (CR 4.e, CR 4.f). Malicious attachments are prevented from executing (CR 4.g). Malicious downloads are identified through signature detection or analysis (CR 4.h, CR 4.i). Malicious executables are prevented from executing (CR 4.j). Network traffic is captured and analyzed for suspicious activity (CR 4.k).
Actual Results	**Semperis DSP (Integrity Monitoring)** successfully monitors and logs changes to Active Directory. **ArcSight ESM (Logging)** successfully collects logs and reports on the events generated by the Integrity Monitoring capability, enabling faster response time. **Glasswall FileTrust (Event Detection)** successfully identifies the malicious attachment before it reaches the user's inbox.

	Glasswall FileTrust (Mitigation and Containment) successfully mitigates the malicious attachment before it reaches the user's inbox. The malicious file is successfully uploaded to **Cisco AMP (Event Detection)** for signature detection. **Cisco AMP (Event Detection)** successfully mitigates the file when found on user workstations. **Symantec Security Analytics (Forensics/Analytics)** is used to successfully detect network traffic involving download of files from the malicious server.
Overall Result	Pass (partial). Emails are not sorted into spam (CR 4.b–d); rather, the attachment is mitigated before reaching the user's inbox. Sorting emails into spam is often a function of the email infrastructure.

876 ## C.7 Test Case: Data Integrity DR-5

877 **Table 6-7 Test Case ID: Data Integrity DR-5**

Parent requirement	(CR 5) The DI example implementation shall detect and respond to changes to the database made through a web server vulnerability in custom code.
Testable requirement	(CR 5.a) Integrity Monitoring, (CR 5.b) Logging, (CR 5.c) Reporting
Description	Show that the DI solution can detect and respond to an exploitation a vulnerability in custom code that leads to an attack on the database.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A vulnerability in the source code of an intranet web page is discovered by a malicious insider. The insider exploits this vulnerability to delete significant portions of the database.
Procedure	The **Integrity Monitoring** capability is used to detect changes to the database. The **Logging** capability is used to monitor changes to the database and to log web requests.

	The **Reporting** capability is used to alert the security team of significant changes to the database. The **Forensics/Analytics** capability is used to investigate the malicious access as well as identify the page with the vulnerability.
Expected Results (pass)	The build can monitor and report changes to the integrity of the database (CR 5.a). Malicious interaction with the web server is detected (CR 5.b). Information about the attack is reported for use in maintaining the enterprise systems (CR 5.c).
Actual Results	**Tripwire Enterprise (Integrity Monitoring)** successfully monitors changes to the database configuration. **ArcSight ESM (Logging)** successfully logs changes to the database and web requests. **ArcSight ESM (Reporting)** successfully alerts the security team of changes to the database. **Symantec Security Analytics (Forensics/Analytics)** allows identification of web requests that could have caused the deletion, helping identify the web server's vulnerability in custom code.
Overall Result	Pass. All requirements for this use case are met.

878 ## C.8 Test Case: Data Integrity DR-6

879 **Table 6-8 Test Case ID: Data Integrity DR-6**

Parent requirement	(CR 6) The DI example implementation shall detect and respond to targeted modification by malicious insiders with elevated privileges.
Testable requirement	(CR 6.a, 6.b) Integrity monitoring, (CR 6.c) Reporting, (CR 6.d) Mitigation and Containment
Description	Show that the DI solution can detect and respond to targeted modification of assets and backups by malicious insiders.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2

Preconditions	A malicious insider attempts to modify targeted information in both the enterprise systems and the backup systems by using elevated credentials obtained extraneously.
Procedure	The **Integrity Monitoring** capability is used to detect changes to the file system. The **Reporting** capability is used to notify the security team of changes to critical data assets. The **Mitigation and Containment** capability is used to prevent the malicious user from making further modifications.
Expected Results (pass)	The build can monitor and report changes to the integrity of files and backups (CR 6.a, CR 6.b). Information about the attack is reported for use in responding to the threat (CR 6.c). User accounts associated with the attack are contained (CR 6.d).
Actual Results	**Tripwire Enterprise (Integrity Monitoring)** successfully detects changes to files and backups caused by a malicious insider. **ArcSight ESM (Reporting)** successfully reports and alerts administrators via email on changes made to files by a malicious insider. **Semperis DSP (Mitigation and Containment)** successfully disables the user accounts associated with malicious insider activity.
Overall Result	Pass. All requirements for this use case are met.

880 ## C.9 Test Case: Data Integrity DR-7

881 **Table 6-9 Test Case ID: Data Integrity DR-7**

Parent requirement	(CR 7) The DI example implementation shall detect and respond to an intrusion via compromised update server.
Testable requirement	(CR 7.a) Integrity Monitoring, (CR 7.b) Event Detection, (CR 7.c) Forensics and Analytics, (CR 7.d, CR 7.e) Mitigation and Containment
Description	Show that the DI solution can detect a malicious update from a compromised update server as well as detect and respond to a resulting intrusion.

Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2, DE.CM-4, DE.CM-7, DE.AE-1, DE.CM-1,
Preconditions	An external update server has been compromised, and a user workstation attempts to update from this server.
Procedure	The **Integrity Monitoring** capability is used to detect changes to the integrity of programs and files. The **Event Detection** capability is used to detect the malicious update. It is also used to detect the connection to the machine. The **Mitigation and Containment** capability is used to halt execution of the update and delete it. It is also used to contain the intrusion.
Expected Results (pass)	The build can monitor and report changes to the integrity of programs (CR 7.a). The malicious update is identified through signature detection or analysis (CR 7.b, CR 7.c). The malicious service is halted and reverted or deleted (CR 7.d). Other users are temporarily prevented from accessing this update server (CR 7.e). The port opened by the service is detected (CR 7.f). The port opened by the service is closed (CR 7.g). The intrusion is detected (CR 7.h). The intrusion is contained (CR 7.i).
Actual Results	**Tripwire Enterprise (Integrity Monitoring)** is used to identify changes in programs on the system as well as any changes made by the attacker. **Cisco AMP (Event Detection)** is used to detect the malicious update. **Cisco Stealthwatch (Event Detection)** is used to detect a connection to the machine via an unusual port.

	Cisco AMP (Mitigation and Containment) is used to halt the execution of the file and delete it, thereby closing the vulnerable port. **Cisco ISE (Mitigation and Containment)** is used to disconnect the affected machines from the network to prevent the spread of the intrusion.
Overall Result	Pass (partial). Cisco AMP does not seem to support network blocking for Unix machines at the time this practice guide was written—it supports only detection (it does support network blocking for Windows use cases, though, so a similar use case on Windows machines would potentially work). Instead, we rely on network protection, a DI Protect capability, to prevent further access to the update server; and on Cisco AMP's mitigation capabilities to remedy any known malicious files downloaded from the server.

NIST SPECIAL PUBLICATION 1800-26C

Data Integrity

Detecting and Responding to Ransomware and Other Destructive Events

Volume C:
How-To Guides

Jennifer Cawthra
National Cybersecurity Center of Excellence
NIST

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

January 2020

DRAFT

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

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

NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-26C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-26C, 440 pages, (January 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

losses due to data integrity events. The NCCoE, in collaboration with members of the business community and vendors of cybersecurity solutions, has built an example solution to address these data integrity challenges. This project details methods and potential tool sets that can detect, mitigate, and contain data integrity events in the components of an enterprise network. It also identifies tools and strategies to aid in a security team's response to such an event.

KEYWORDS

attack vector; data integrity; malicious actor; malware; malware detection; malware response; ransomware.

ACKNOWLEDGMENTS

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

Name	Organization
Kyle Black	Bay Dynamics
Sunjeet Randhawa	Broadcom Inc.
Peter Romness	Cisco Systems
Matthew Hyatt	Cisco Systems
Matthew Shabat	Glasswall Government Solutions
Justin Rowland	Glasswall Government Solutions
Greg Rhein	Glasswall Government Solutions
Steve Roberts	Micro Focus
Timothy McBride	NIST
Christopher Lowde	Semperis

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

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Information Centric Analytics v6.5.2 Symantec Security Analytics v8.0.1
Cisco Systems	Cisco Identity Services Engine v2.4, Cisco Advanced Malware Protection v5.4, Cisco Stealthwatch v7.0.0
Glasswall Government Solutions	Glasswall FileTrust ATP for Email v6.90.2.5
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Semperis	Semperis Directory Services Protector v2.7

Contents

1 Introduction 1

1.1 Practice Guide Structure 1

1.2 Build Overview 2

1.3 Typographical Conventions 3

2 Product Installation Guides 3

2.1 Active Directory and Domain Name System Server 3

2.1.1 Install Features 3

2.1.2 Create a Certificate Authority 17

2.1.3 Configure Account to Add Computers to Domain 30

2.1.4 Add Machines to the Domain 36

2.1.5 Configure Active Directory to Audit Account Activity 41

2.1.6 Configure Reverse Lookup Zones 43

2.2 Microsoft Exchange Server 48

2.2.1 Install Microsoft Exchange 49

2.3 Windows Server Hyper-V Role 59

2.3.1 Production Installation 59

2.4 MS SQL Server 65

2.4.1 Install and Configure MS SQL 65

2.4.2 Open Port on Firewall 73

2.4.3 Add a New Login to the Database 78

2.5 Microsoft IIS Server 80

2.5.1 Install IIS 80

2.5.2 IIS Configuration 87

2.6 Semperis Directory Services Protector 91

2.6.1 Configure Active Directory for Semperis DSP 91

2.6.2 Install Semperis DSP 103

2.6.3 Roll Back Changes with Semperis DSP 116

2.6.4 Configure Reporting with Semperis DSP 117

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

2.8.5 Install Pre-Configured Filters for ArcSight 221
2.8.5.1 Install Activate Base 221
2.8.5.2 Install Packages 223
2.8.6 Apply Filters to a Channel 224
2.8.7 Configure Email Alerts in ArcSight 225
2.8.7.1 Configure a New Destination 225
2.8.7.2 Configure a New Rule 226
2.9 Tripwire Enterprise 229
2.9.1 Install Tripwire Enterprise 230
2.9.2 Install the Axon Bridge 242
2.9.3 Install the Axon Agent (Windows) 242
2.9.4 Install the Axon Agent (Linux) 243
2.9.5 Configure Tripwire Enterprise 244
2.9.5.1 Terminology 244
2.9.5.2 Tags 245
2.9.5.3 Rules 247
2.9.5.4 Tasks 251
2.10 Tripwire Log Center 254
2.10.1 Install Tripwire Log Center Manager 254
2.10.2 Configure Tripwire Log Center Manager 255
2.10.3 Install Tripwire Log Center Console 260
2.11 Cisco Identity Services Engine 261
2.11.1 Initial Setup 261
2.11.2 Inventory: Configure SNMP on Routers/Network Devices 261
2.11.3 Inventory: Configure Device Detection 261
2.11.4 Policy Enforcement: Configure Active Directory Integration 265
2.11.5 Policy Enforcement: Enable Passive Identity with AD 268
2.11.6 Policy Enforcement: Developing Policy Conditions 273

2.11.7 Policy Enforcement: Developing Policy Results 274
2.11.8 Policy Enforcement: Enforcing a Requirement in Policy 275
2.11.9 Policy Enforcement: Configuring a Web Portal 276
2.11.10 Configuring RADIUS with your Network Device 277
2.11.11 Configuring an Authentication Policy 278
2.11.12 Configuring an Authorization Policy 279
2.12 Cisco Advanced Malware Protection 280
2.12.1 Dashboard Configuration...280
2.12.2 Installing the Connector on a Windows Server 281
2.12.3 Installing the Connector on a Windows 10 Machine...282
2.12.4 Scanning using AMP...283
2.12.5 Configure AMP Policy 284
2.13 Cisco Stealthwatch 286
2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor 286
2.13.2 Change Default Stealthwatch Console Passwords 291
2.13.3 Configure the Stealthwatch Management Console Web Interface 295
2.13.4 Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces 298
2.14 Symantec Analytics.. 301
2.14.1 Initial Setup 301
2.14.2 Capturing Data 307
2.15 Symantec Information Centric Analytics.. 308
2.15.1 Installing MS SQL 2017 308
2.15.2 Install Windows Services 316
2.15.3 Installing Symantec ICA...324
2.15.4 Configuring Symantec ICA for Analysis 331

2.15.4.1 Installing Integration Packs 331
2.15.4.2 Create a View 332
2.15.4.3 Open an Existing View 333
2.15.4.4 Viewing Detailed Analyzer Data 335
2.16 Integration: Cisco Identity Services Engine and Cisco Stealthwatch 335
2.16.1 Configuring Certificates for pxGrid 335
2.16.2 Configuring Stealthwatch to Quarantine through ISE 347
2.17 Integration: Tripwire Log Center and Tripwire Enterprise 352
2.18 Integration: Symantec ICA and ArcSight ESM 359
2.18.1 Export the CSV File from ArcSight Console 359
2.18.2 Import the CSV File to Symantec ICA 361
2.18.3 Create a Mapping between ArcSight events and Symantec ICA 365
2.18.4 View ArcSight Events in the Analyzer 370
2.19 Integration: Micro Focus ArcSight and Tripwire 371
2.19.1 Install Micro Focus ArcSight 371
2.20 Integration: Micro Focus ArcSight and Cisco AMP 383
2.20.1 Create API Credentials for ArcSight to access AMP 383
2.20.2 Install Micro Focus ArcSight 384
2.20.3 Create a Parser for Cisco AMP REST events 392
2.21 Integration: Micro Focus ArcSight and Cisco ISE 393
2.21.1 Configure Cisco ISE to Forward Logs 394
2.21.2 Select Logs for Forwarding 395
2.22 Integration: Micro Focus ArcSight and Semperis DSP 397
2.22.1 Configure Semperis DSP to Forward Logs 397
2.23 Integration: Micro Focus ArcSight and Symantec Analytics 398
2.23.1 Configure Symantec Analytics to Forward Logs 398
2.23.2 Install Symantec Analytics Package for ArcSight 400
2.24 Integration: Micro Focus ArcSight and Glasswall FileTrust 408
2.24.1 Install Micro Focus ArcSight 408

2.25 Integration: Micro Focus ArcSight and Cisco Stealthwatch 423
2.25.1 Install Micro Focus ArcSight..423
2.25.2 Configure Cisco Stealthwatch 432
Appendix A List of Acronyms 440

1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

- NIST SP 1800-26a: *Executive Summary*
- NIST SP 1800-26b: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-26c: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers will be interested in the *Executive Summary (NIST SP 1800-26a)*, which describes the:

- challenges enterprises face in detecting and responding to data integrity events
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-26b,* which describes what we did and why. The following sections will be of particular interest:

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

You might share the *Executive Summary, NIST SP 1800-26a,* with your leadership team members to help them understand the importance of adopting standards-based data integrity solutions.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-26c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

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

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

1.2 Build Overview

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively detect and respond to a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also explored the issues of analysis and reporting to support incident response. The servers in the virtual environment were built to the hardware specifications of their specific software components.

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

1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

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

2 Product Installation Guides

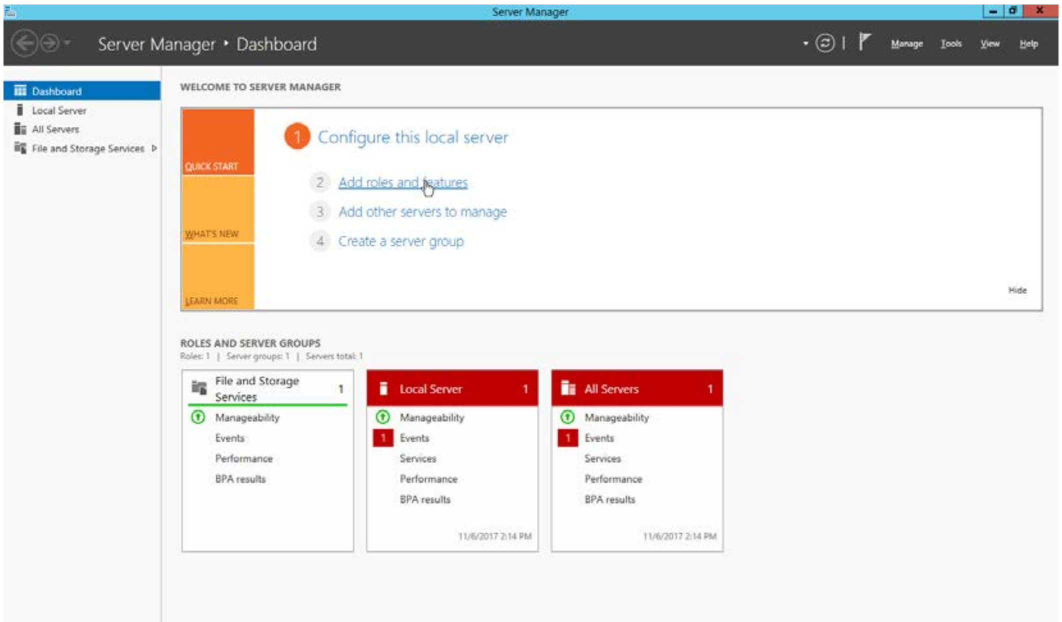
This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution.

2.1 Active Directory and Domain Name System Server

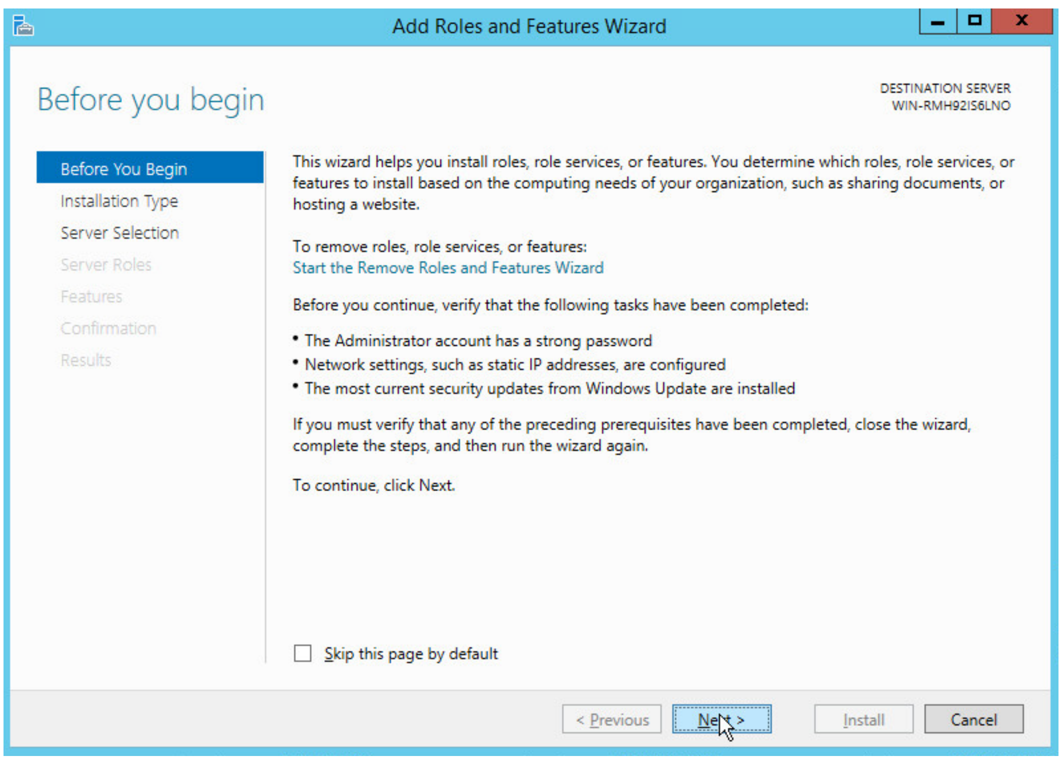
As part of our enterprise emulation, we included an Active Directory server that doubles as a Domain Name System (DNS) server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

2.1.1 Install Features

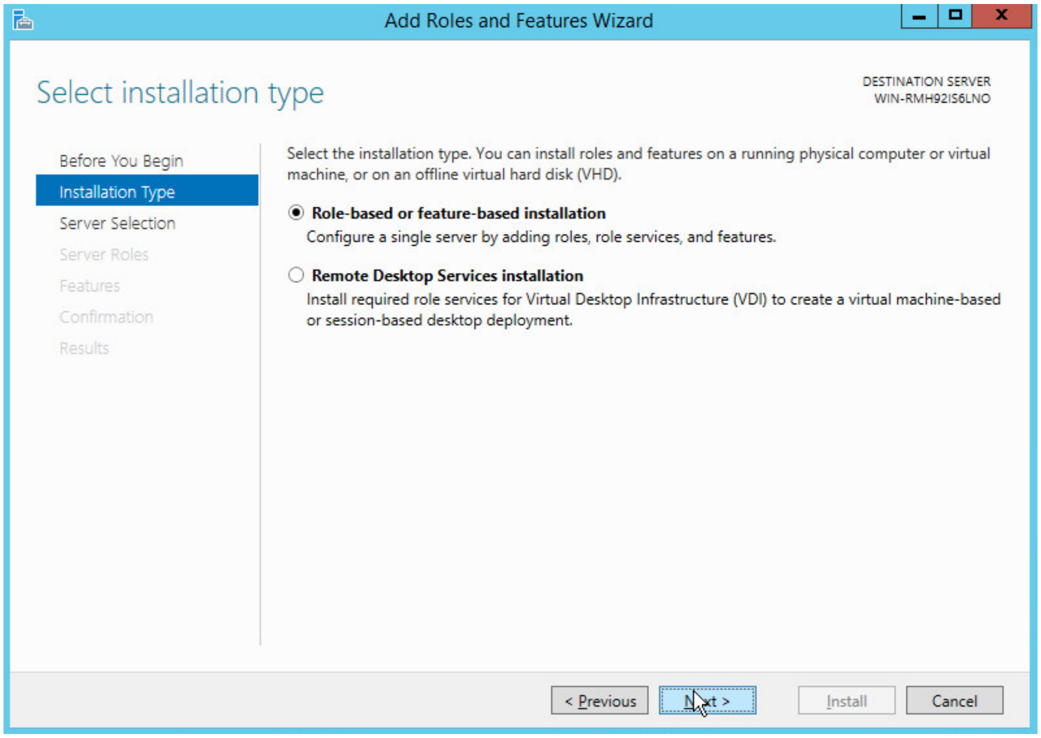
1. Open **Server Manager.**



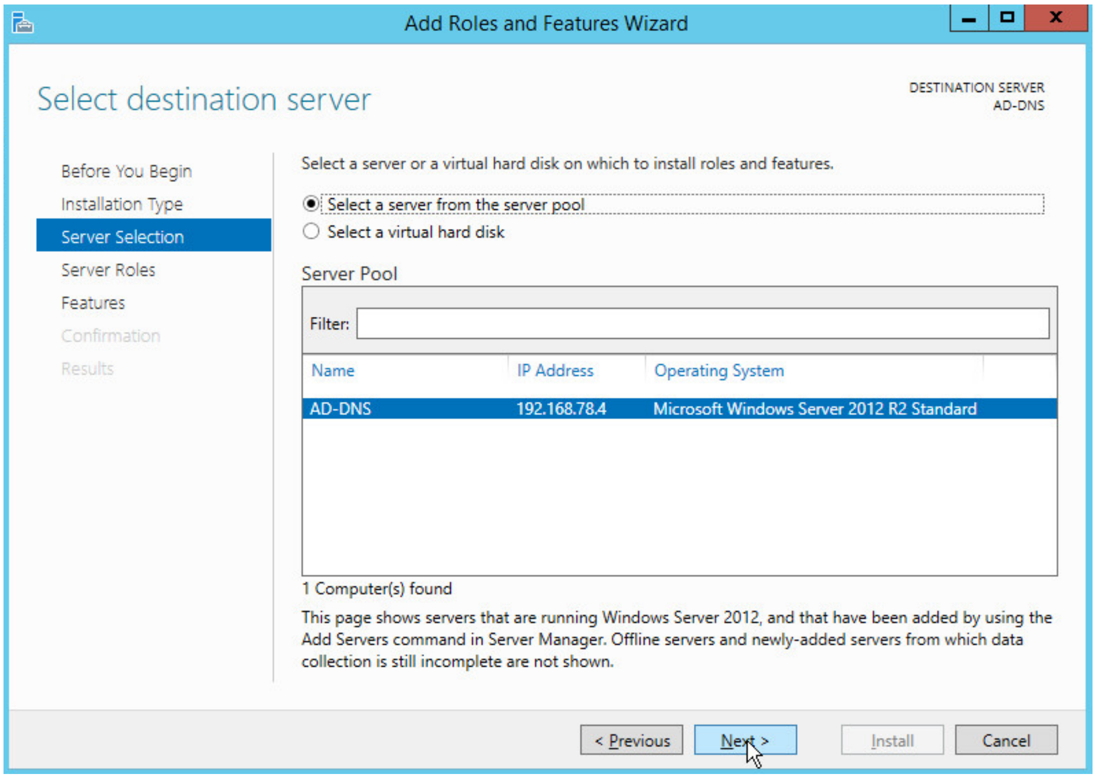
2. Click the link **Add roles and features.**



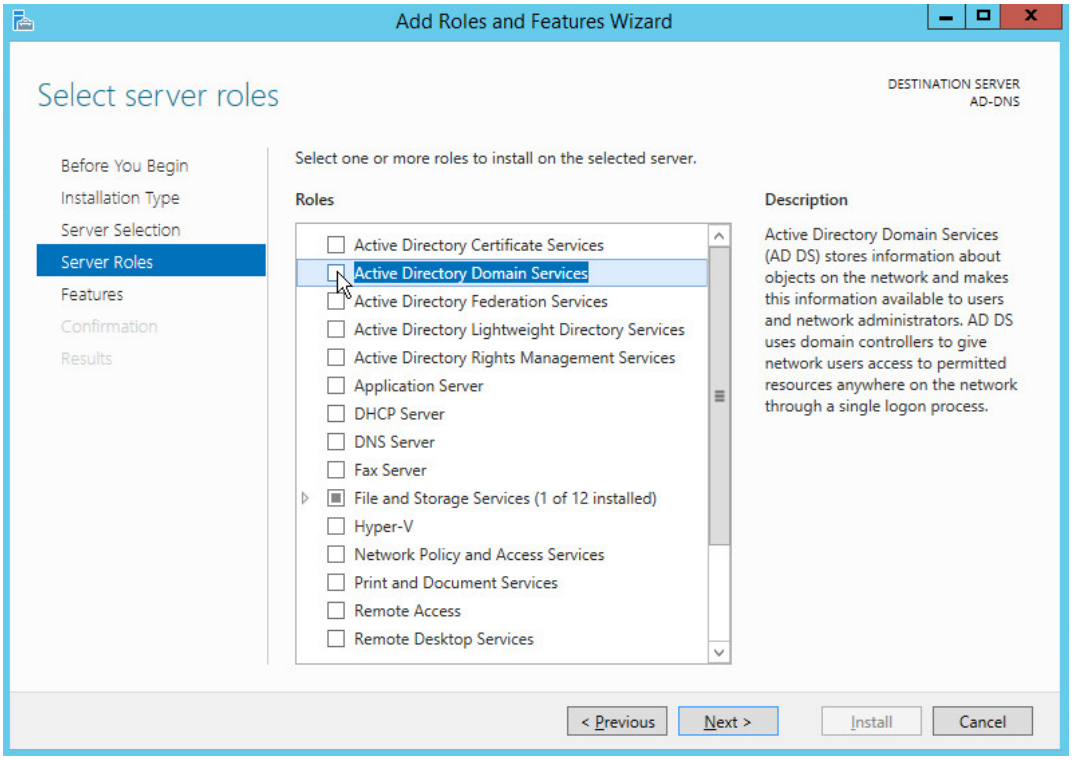
3. Click **Next.**
4. Select **Role-based or feature-based installation.**



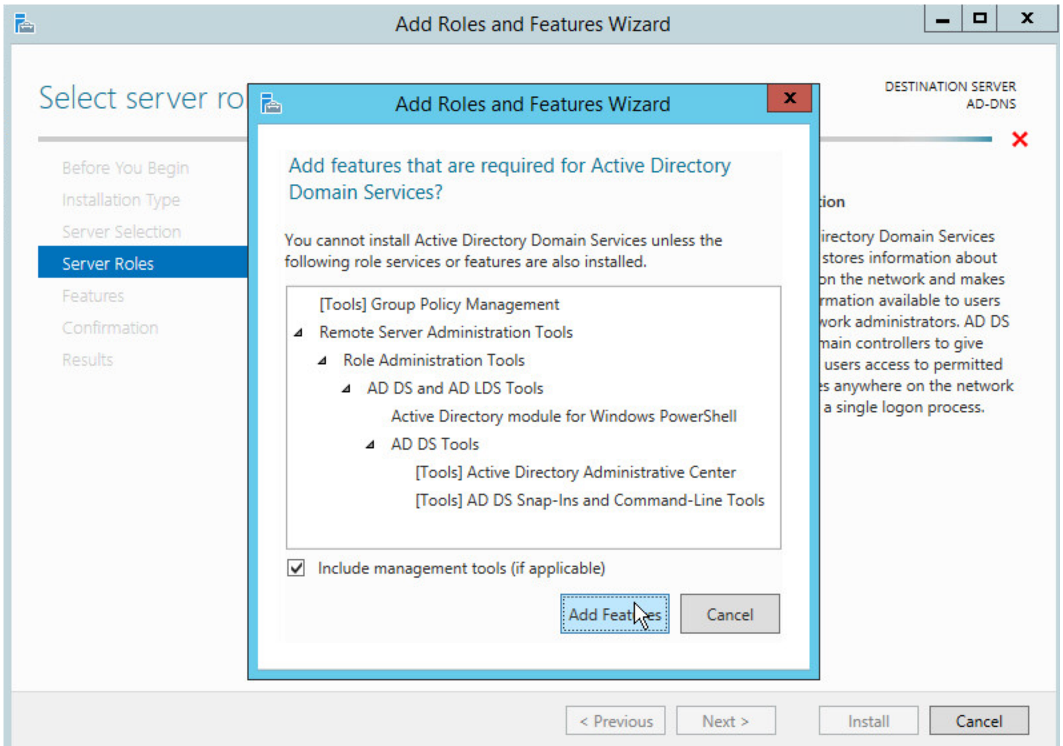
5. Click **Next.**
6. Select **Select a server from the server pool.**
7. Select the intended active directory server.


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

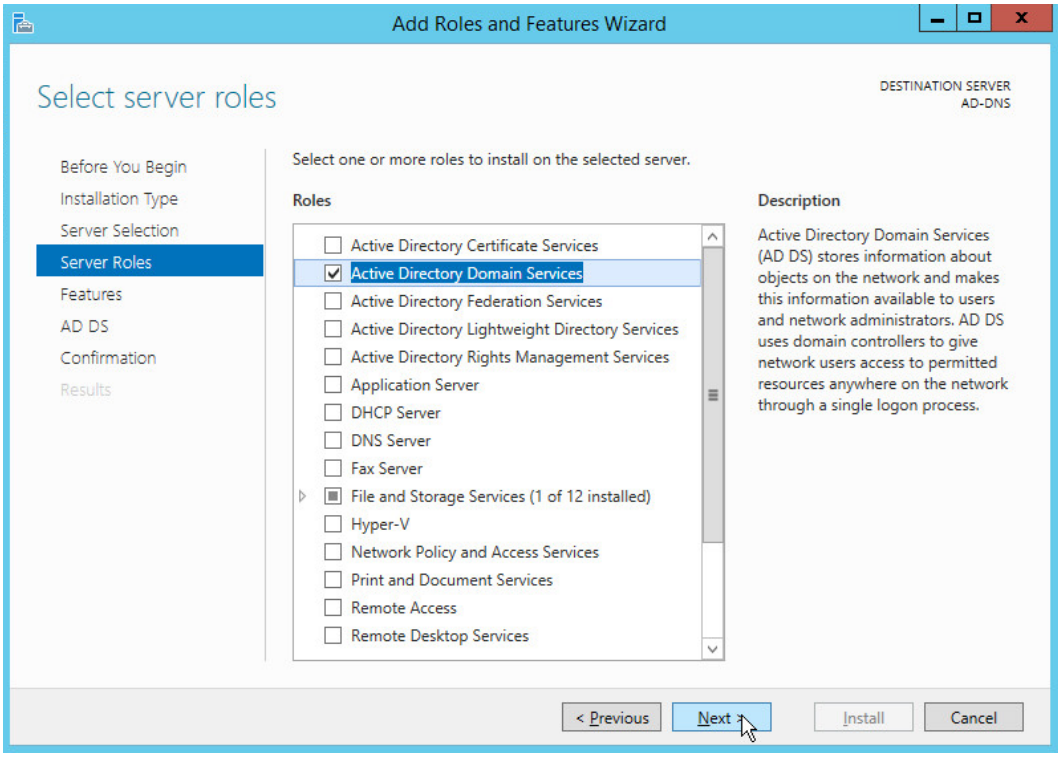
8. Click **Next.**



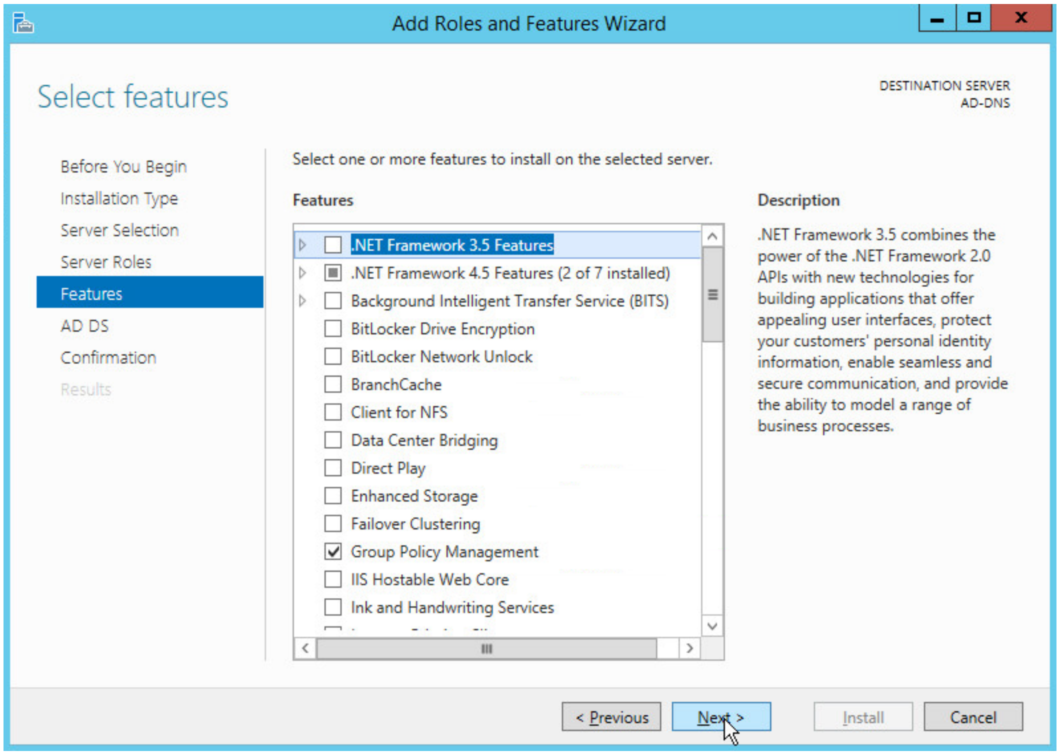
9. Check the box next to **Active Directory Domain Services.**



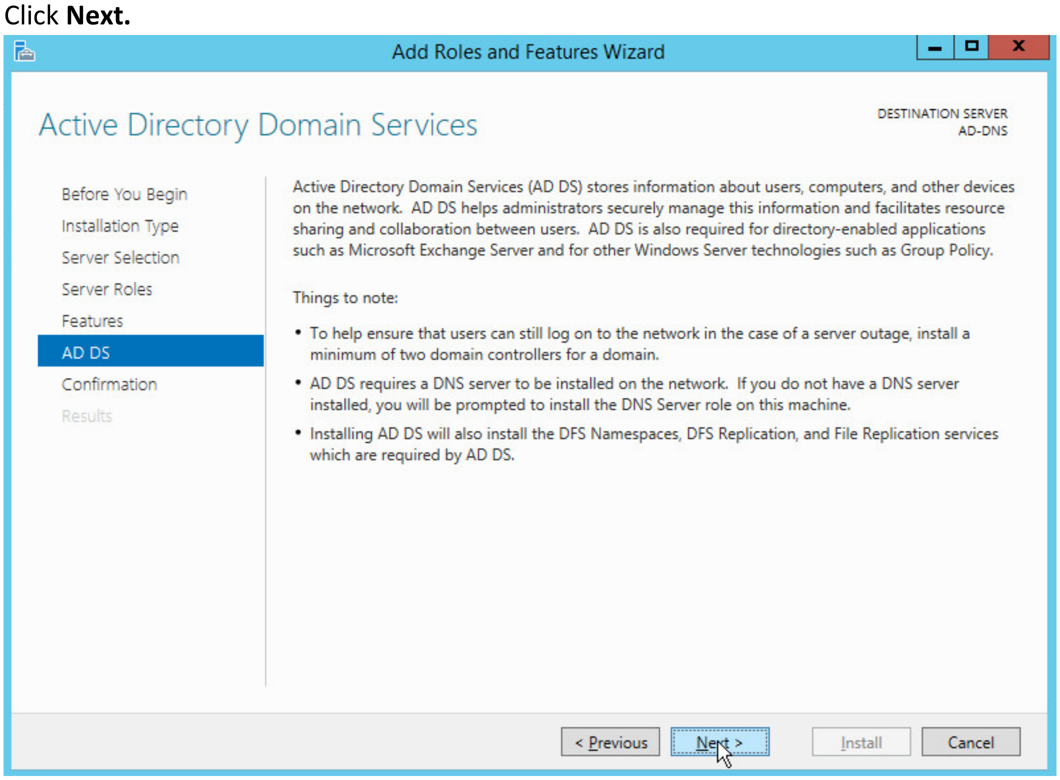
10. Click **Add Features.**

298 

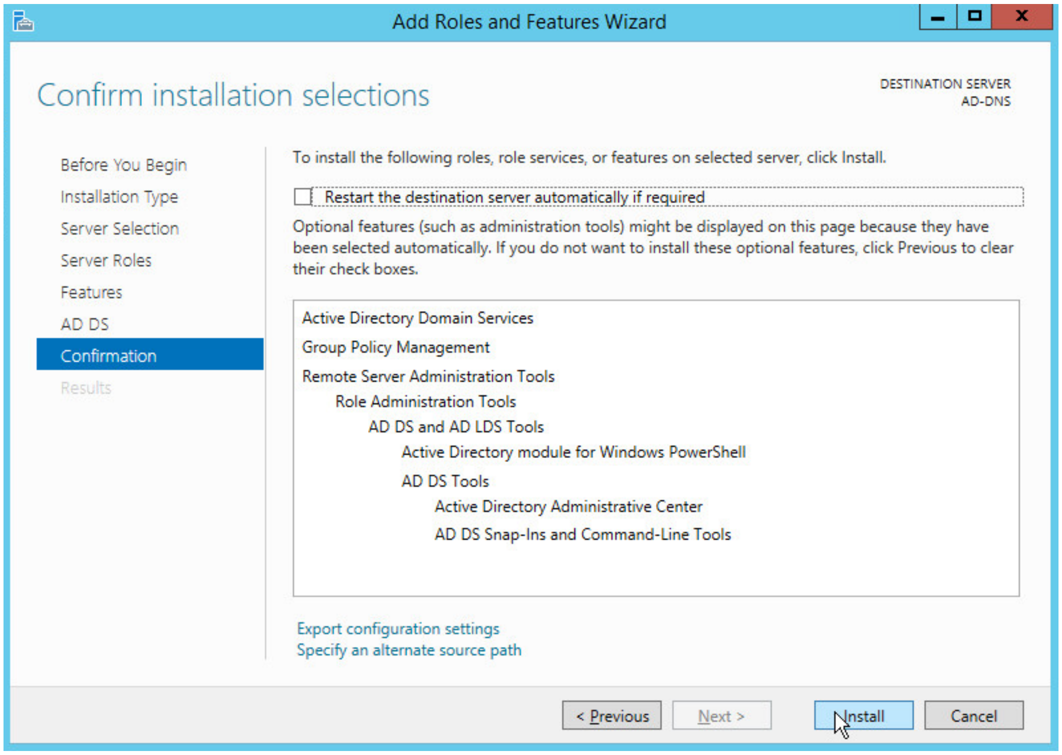
299 11. Click **Next.**



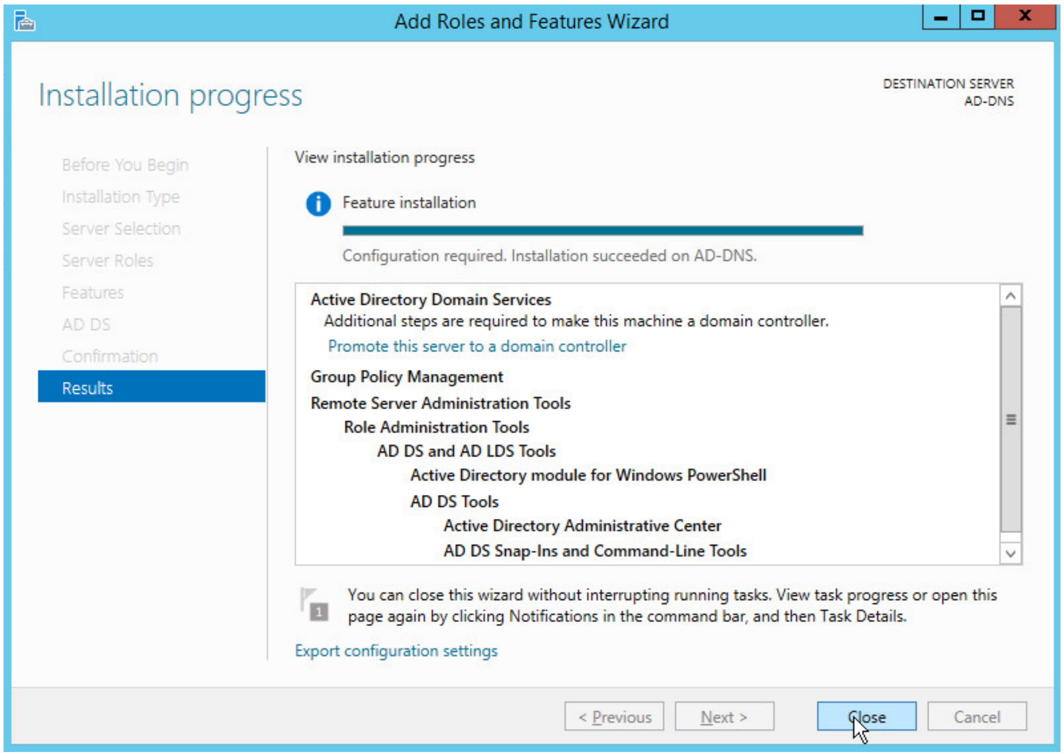
12. Click **Next.**



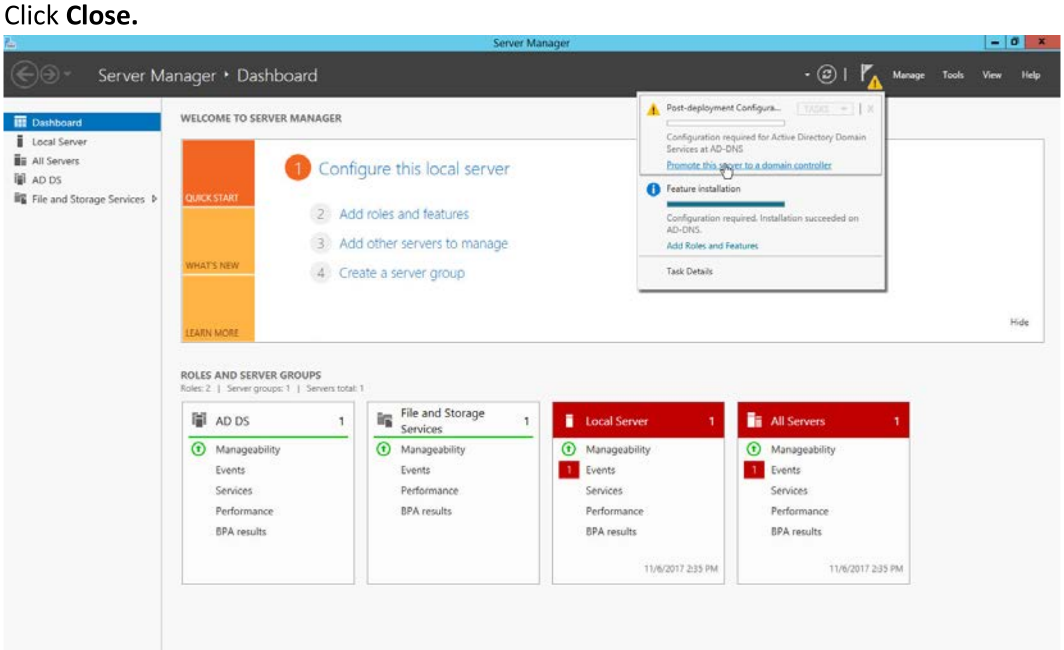
13. Click **Next.**



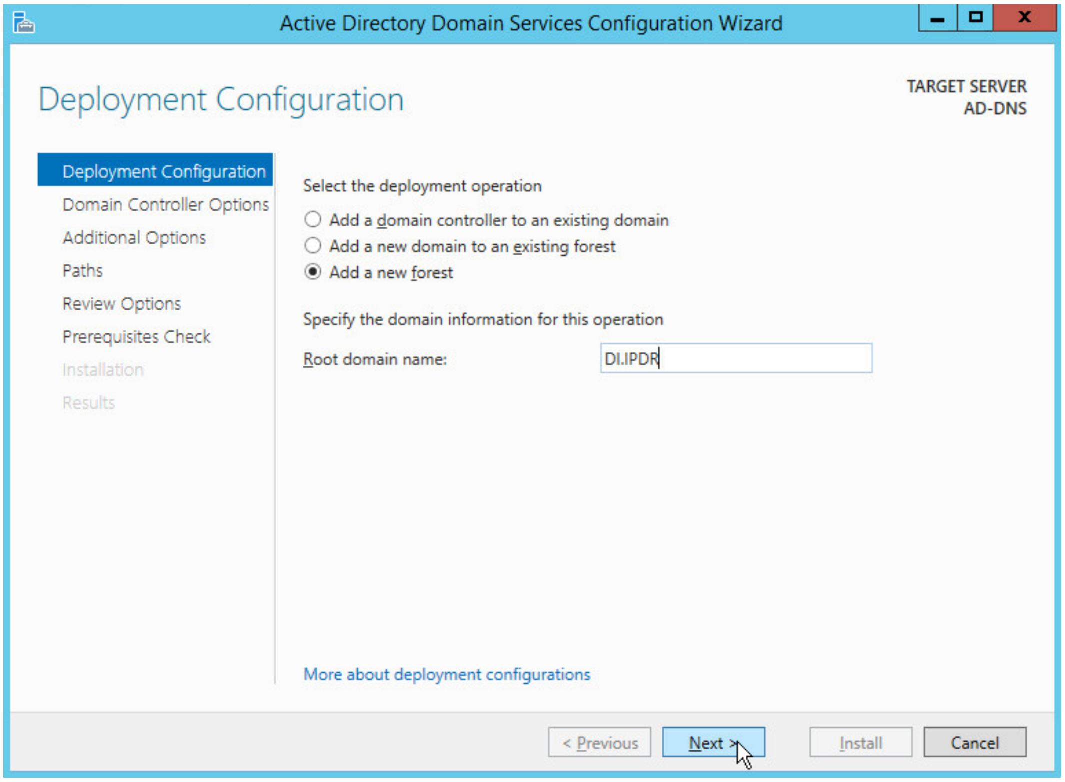
14. Click **Install.**
15. Wait for the installation to complete.



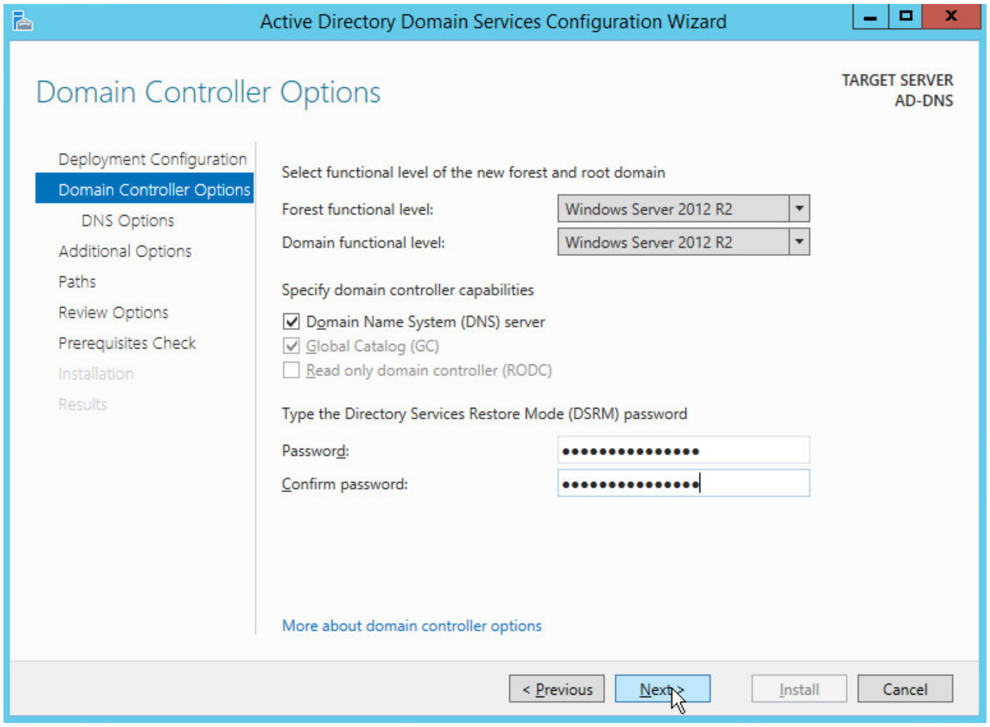
16. Click **Close.**



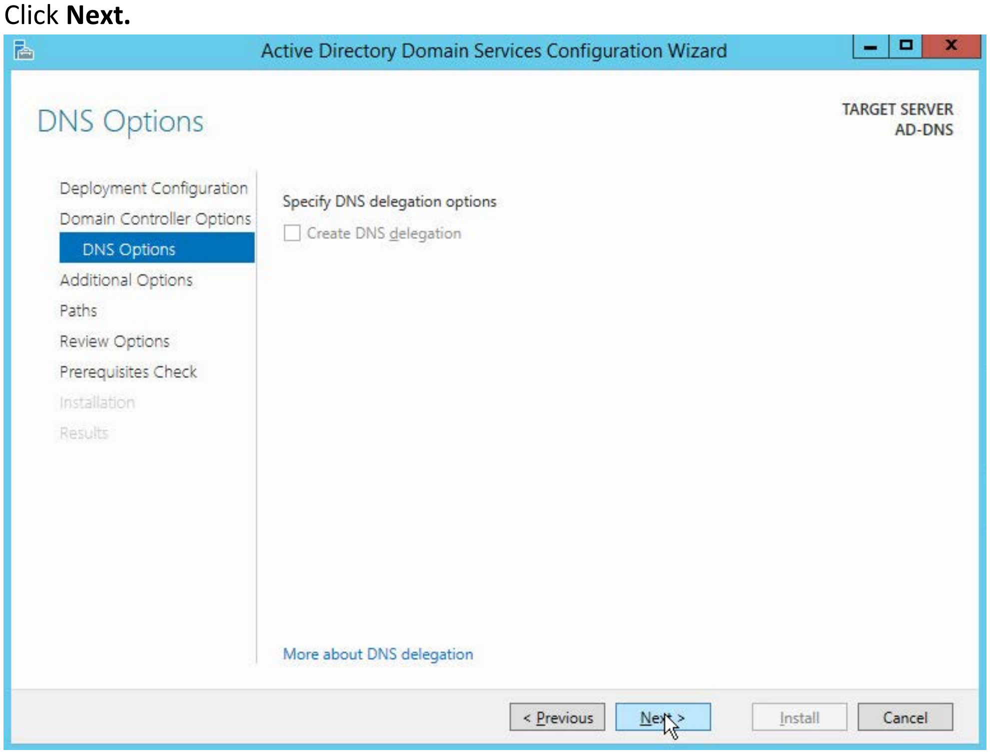
17. Click **Promote this server to a domain controller.**
18. Select **Add a new forest.**
19. Enter a **Root domain name.**



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

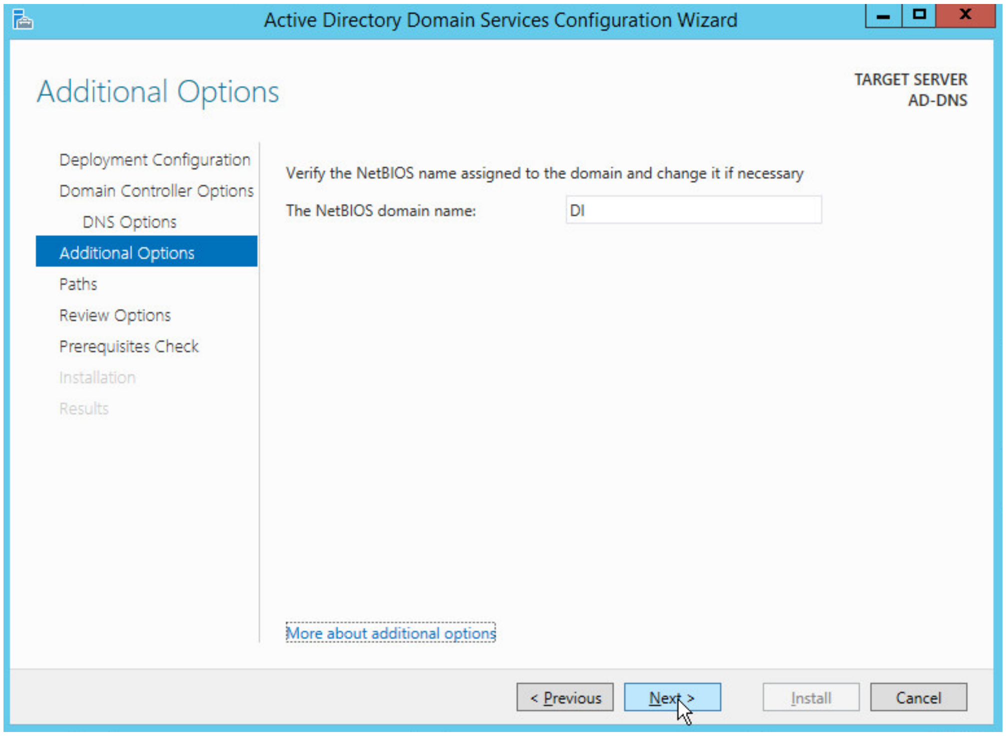


24. Click **Next.**

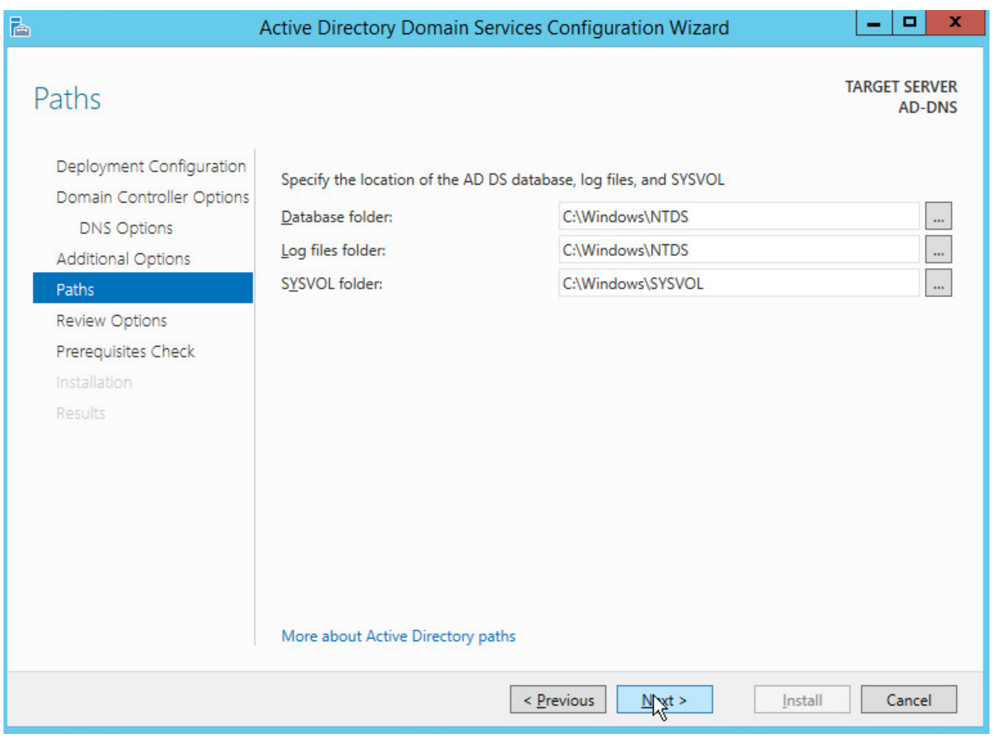


25. Click **Next.**

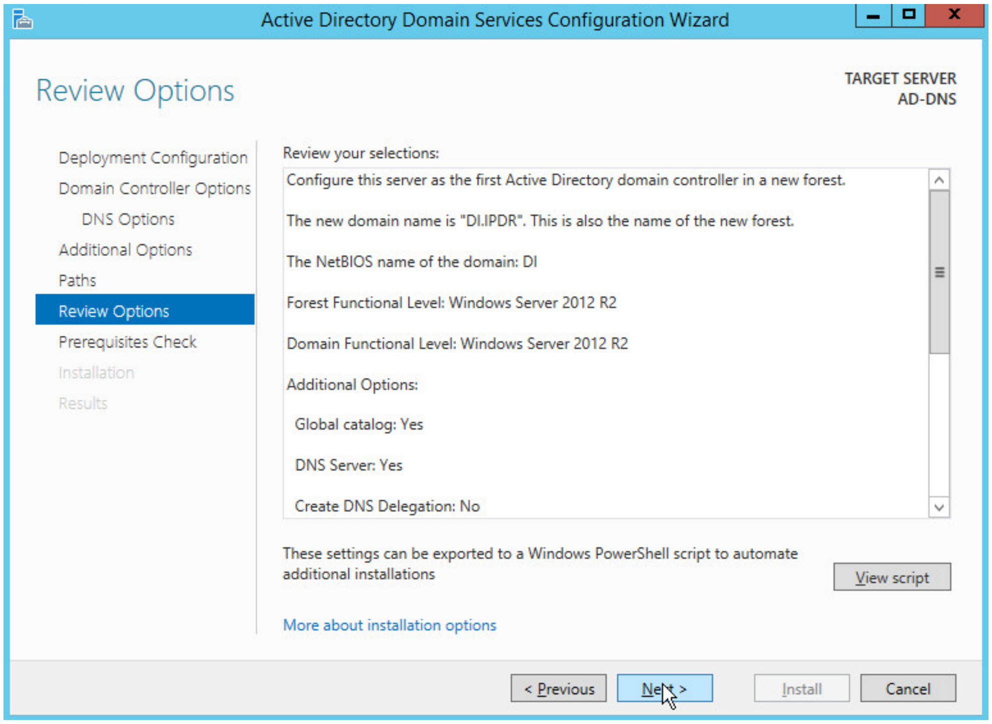
26. Verify the domain name.



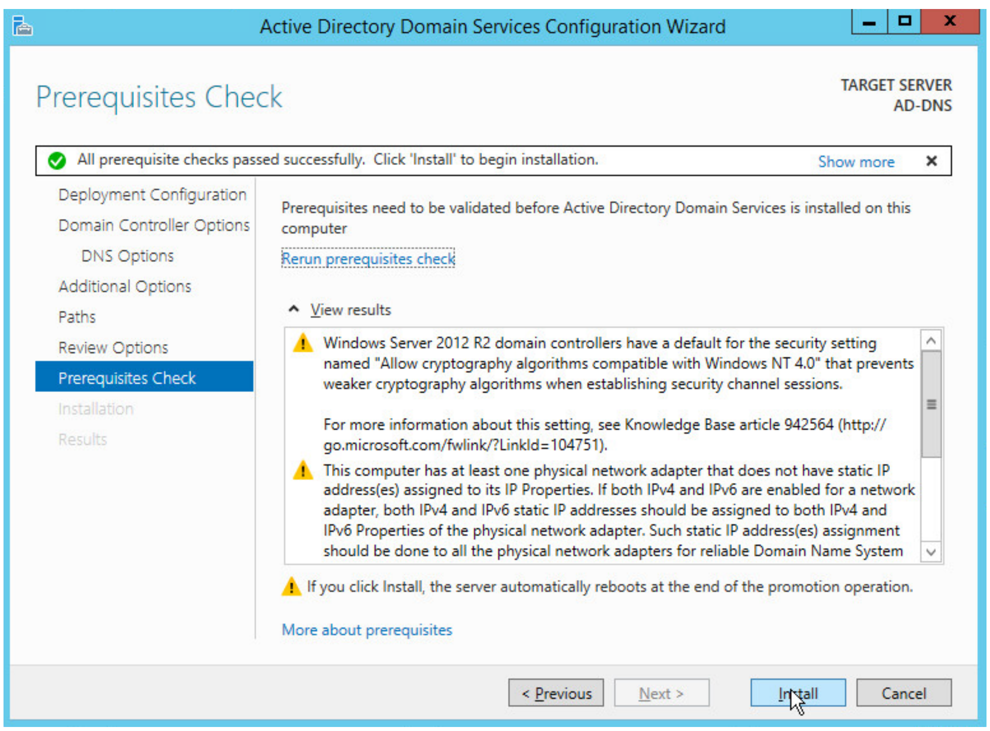
27. Click **Next.**



28. Click **Next.**



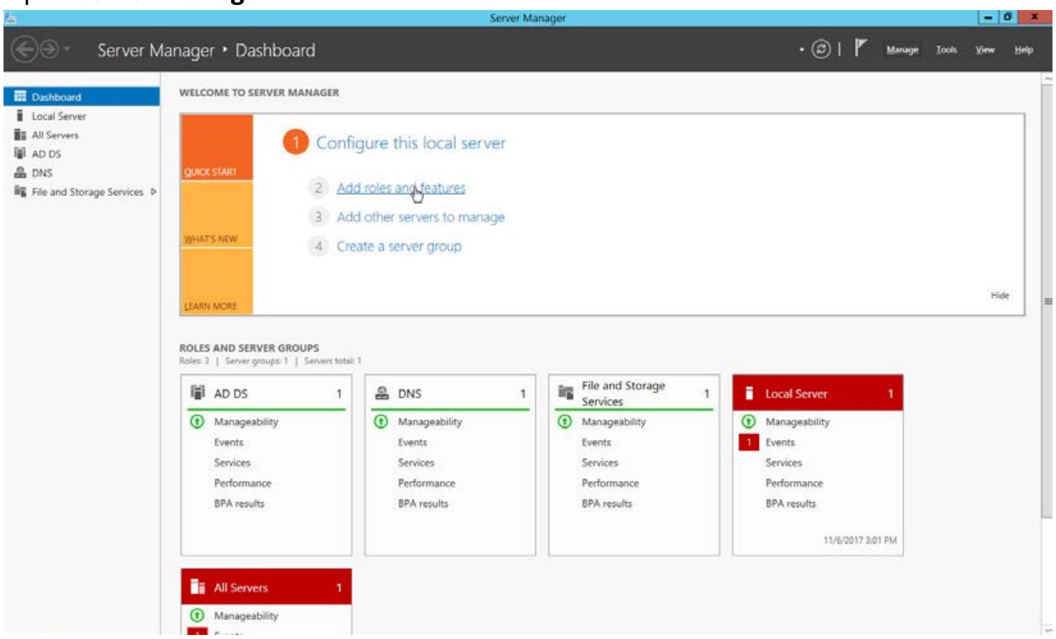
29. Click **Next.**



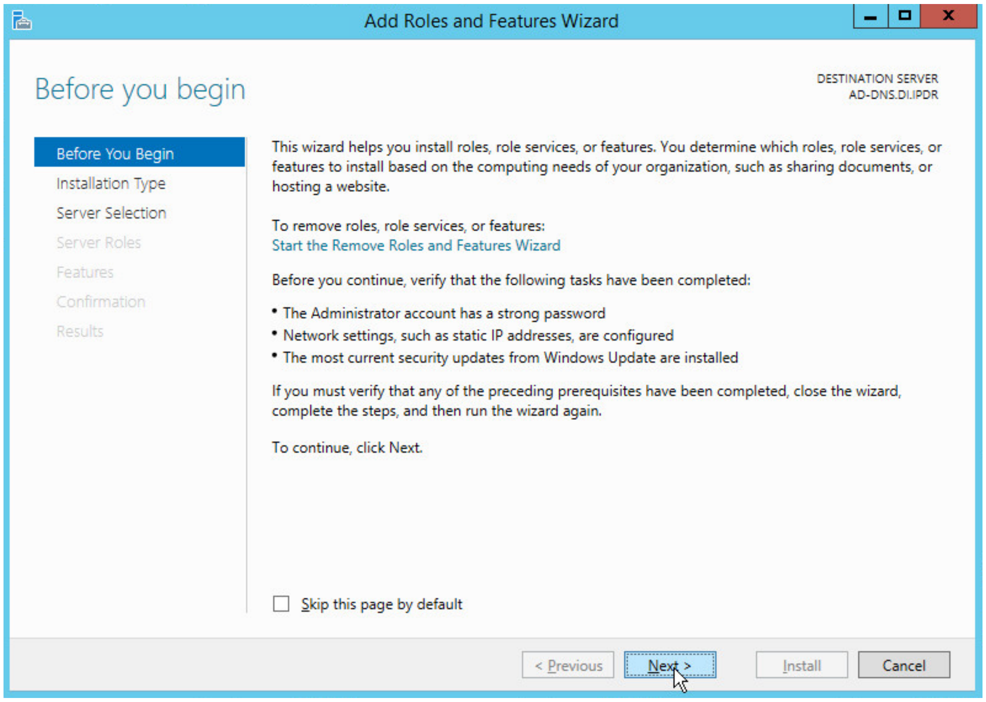
30. Click **Install.**
31. Wait for the installation to complete.
32. The server automatically reboots.

2.1.2 Create a Certificate Authority

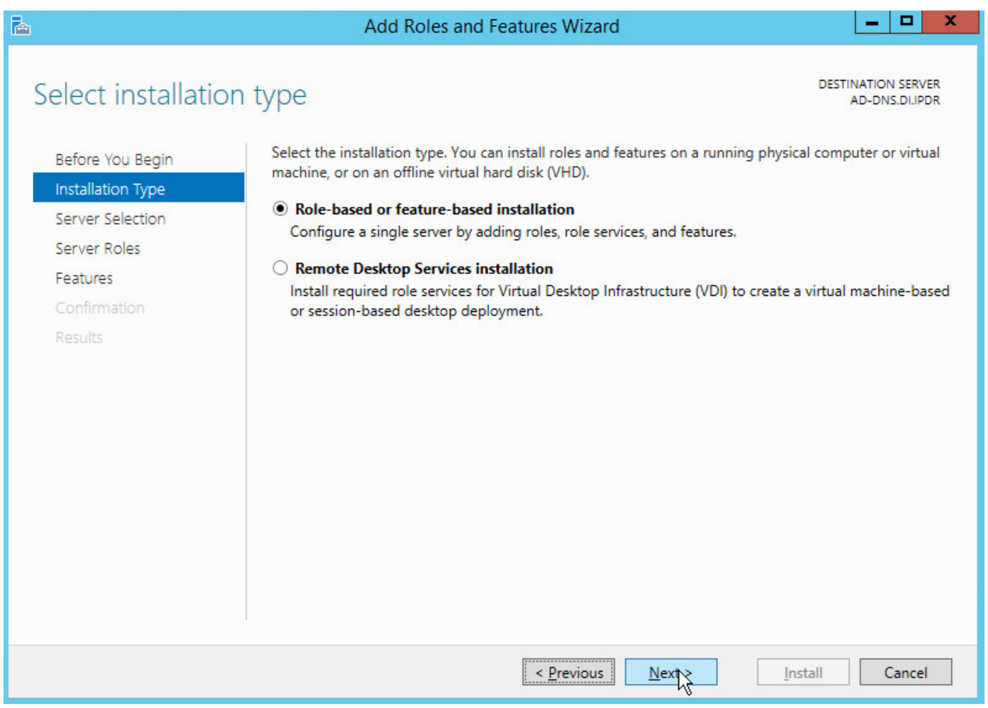
1. Open **Server Manager.**



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

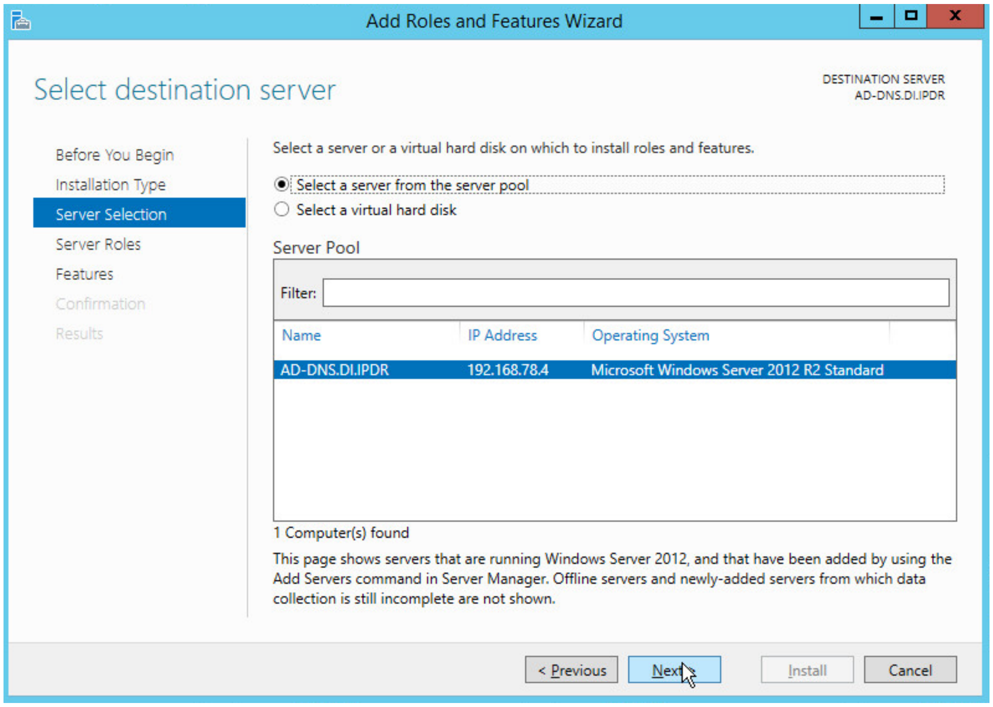


3. Click **Next.**
4. Select **Role-based or feature-based installation.**

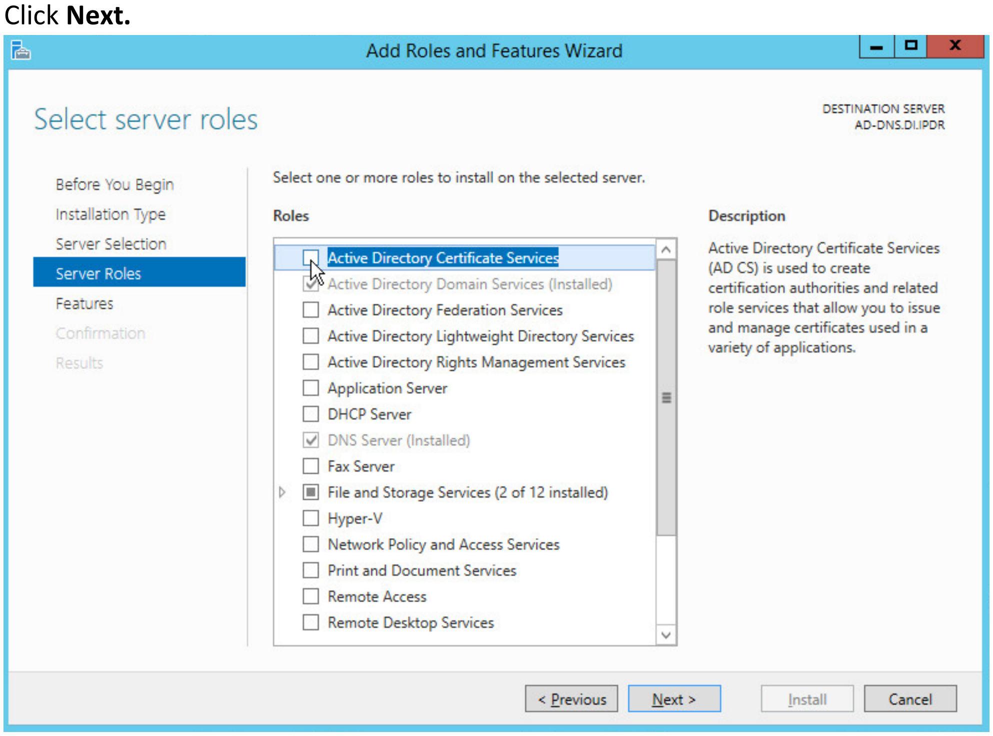


5. Click **Next.**

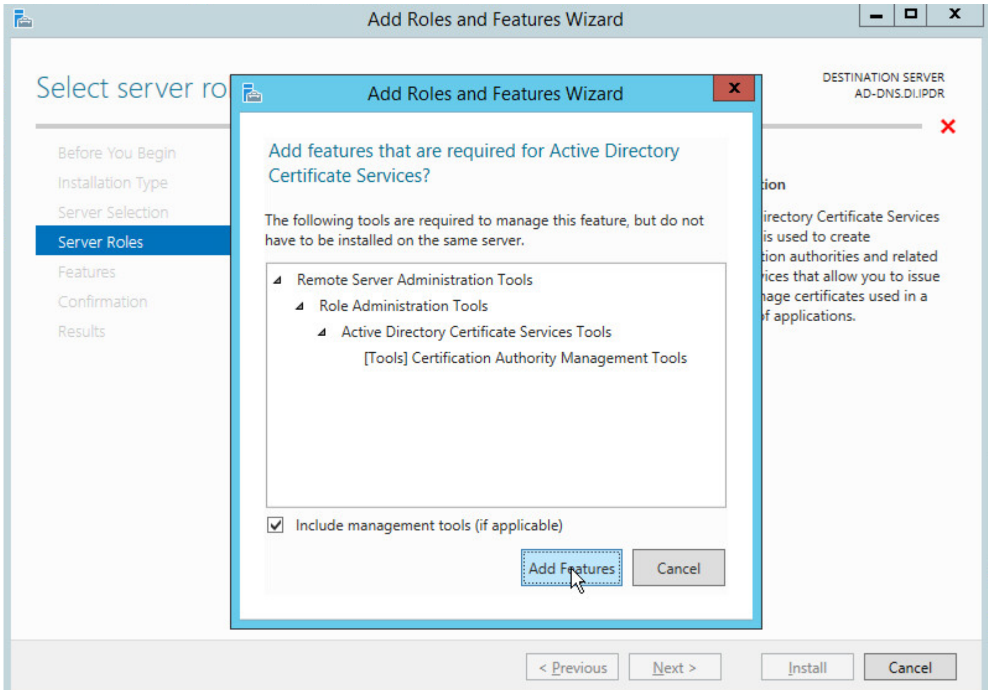
6. Select **Select a server from the server pool.**
7. Select the intended Active Directory server.



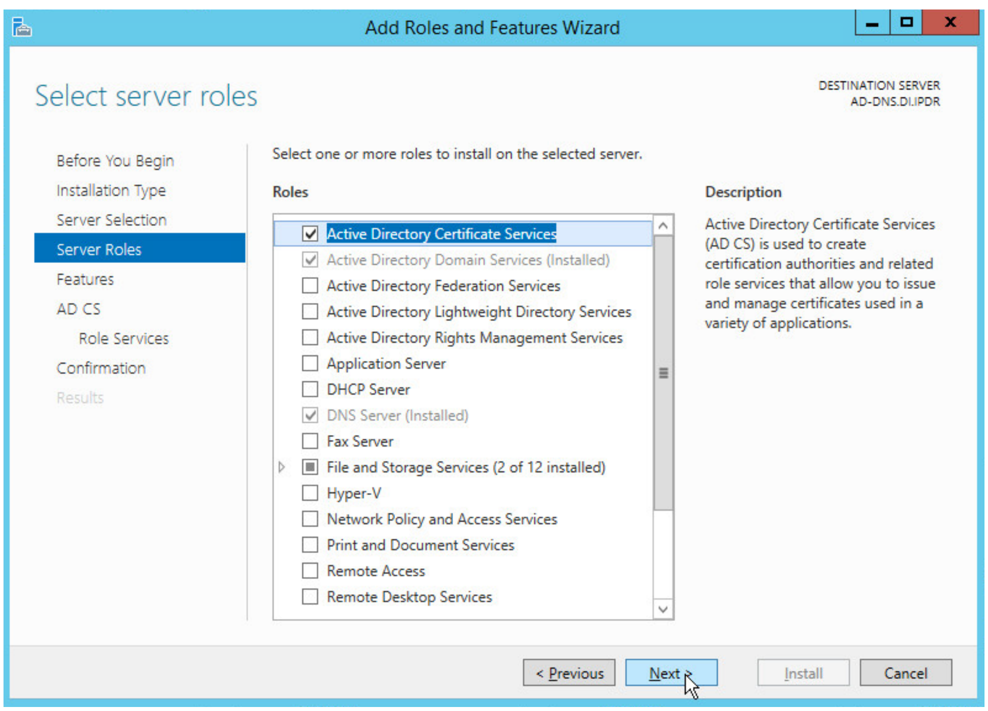
8. Click **Next.**



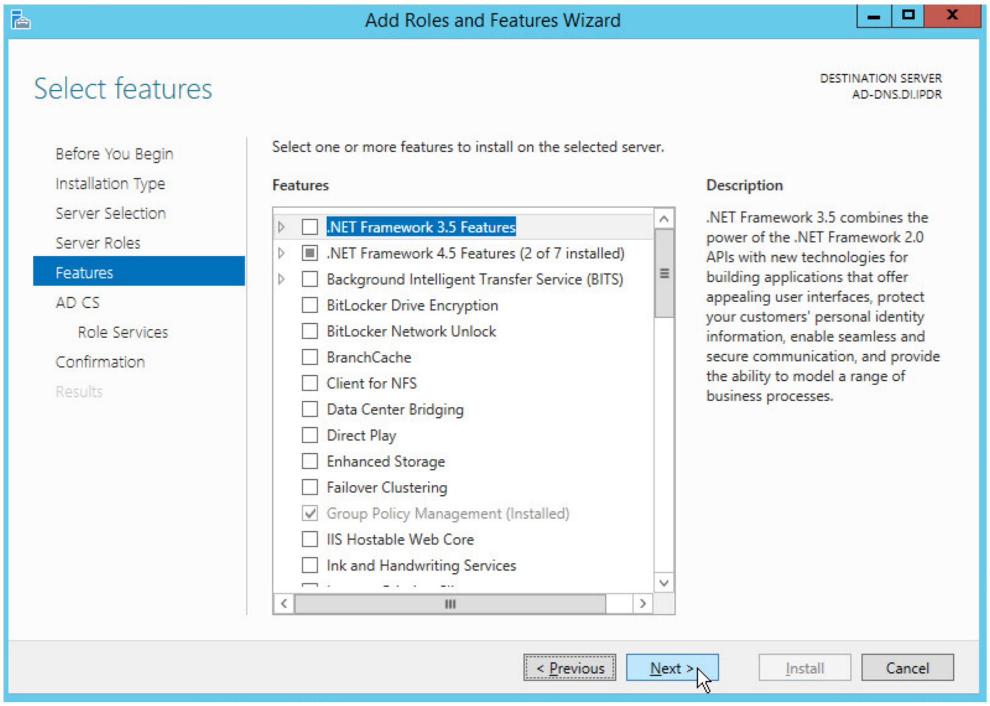
9. Check the box next to **Active Directory Certificate Services.**



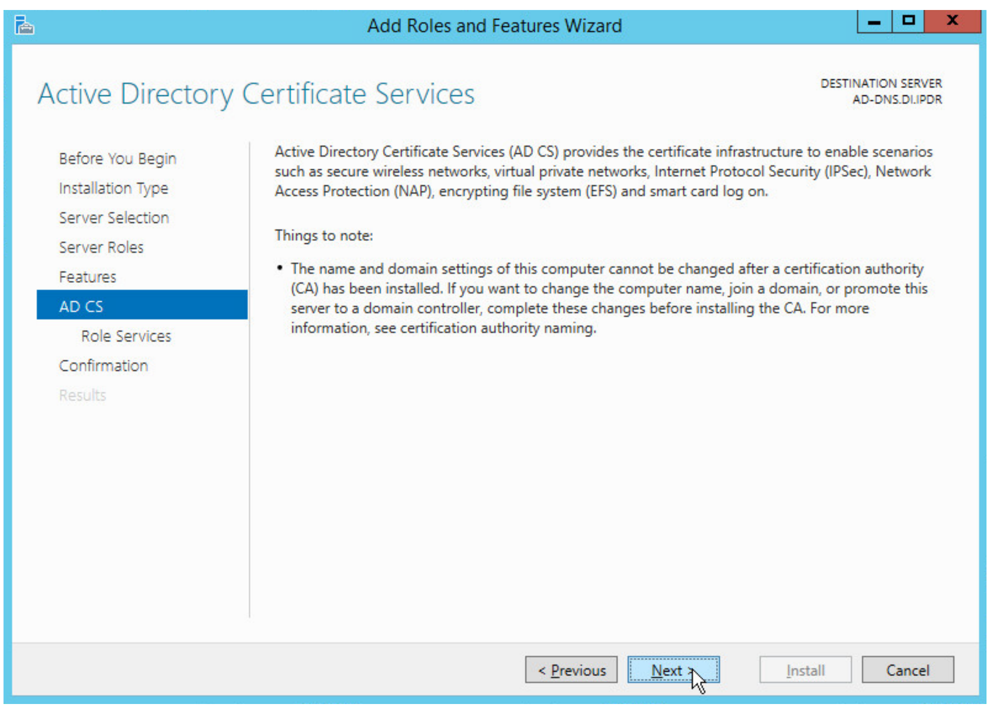
10. Click **Add Features.**



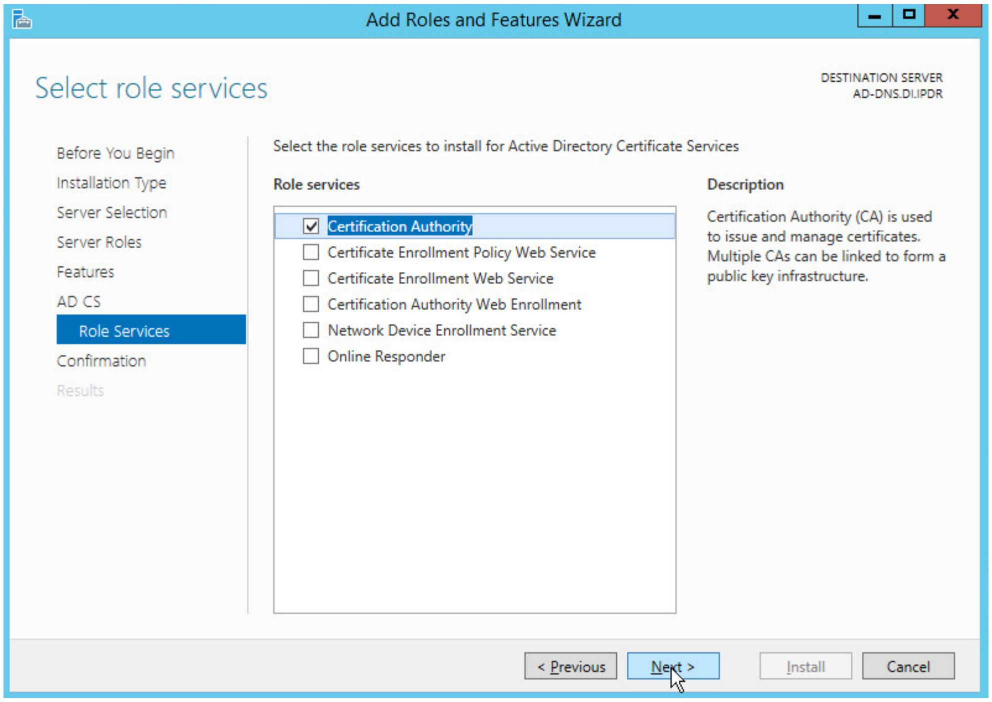
11. Click **Next.**



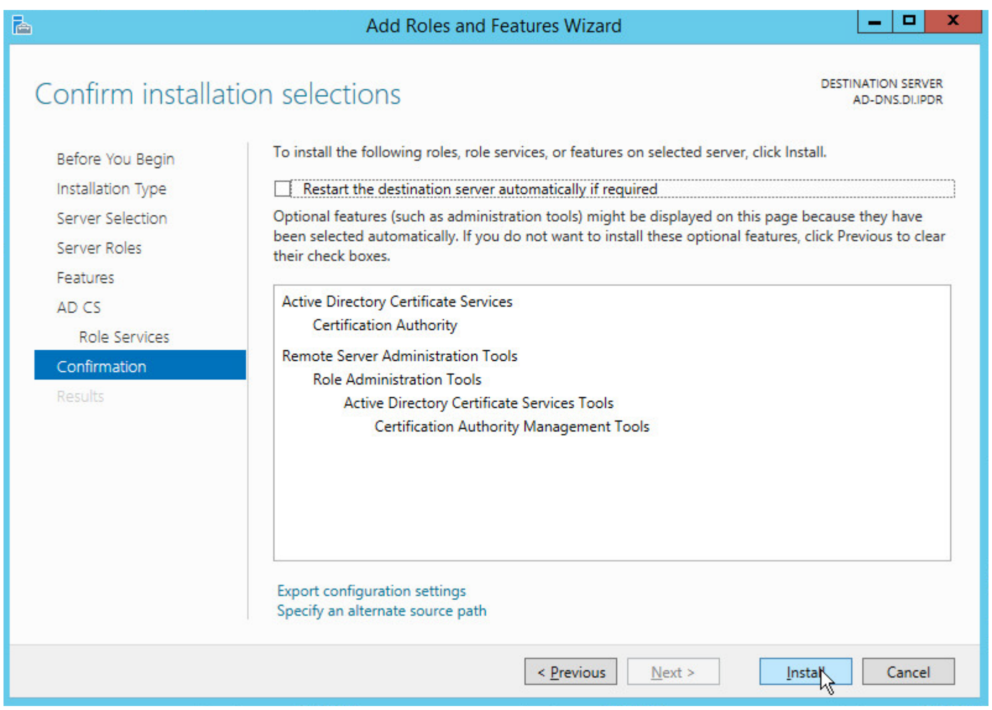
12. Click **Next.**



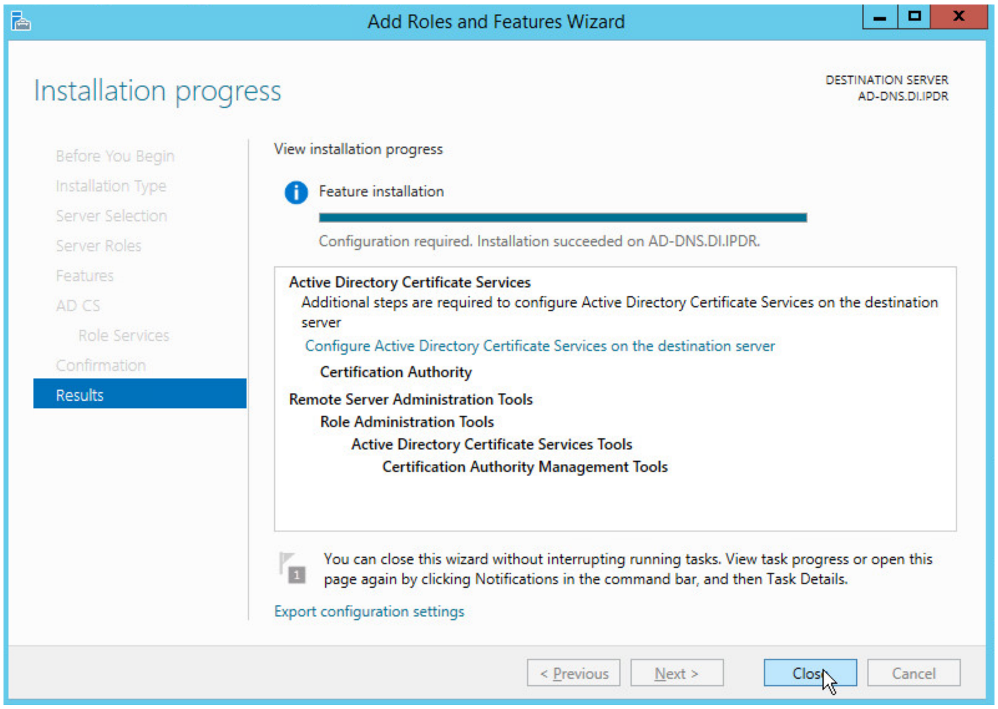
13. Click **Next.**
14. Check the box next to **Certification Authority.**



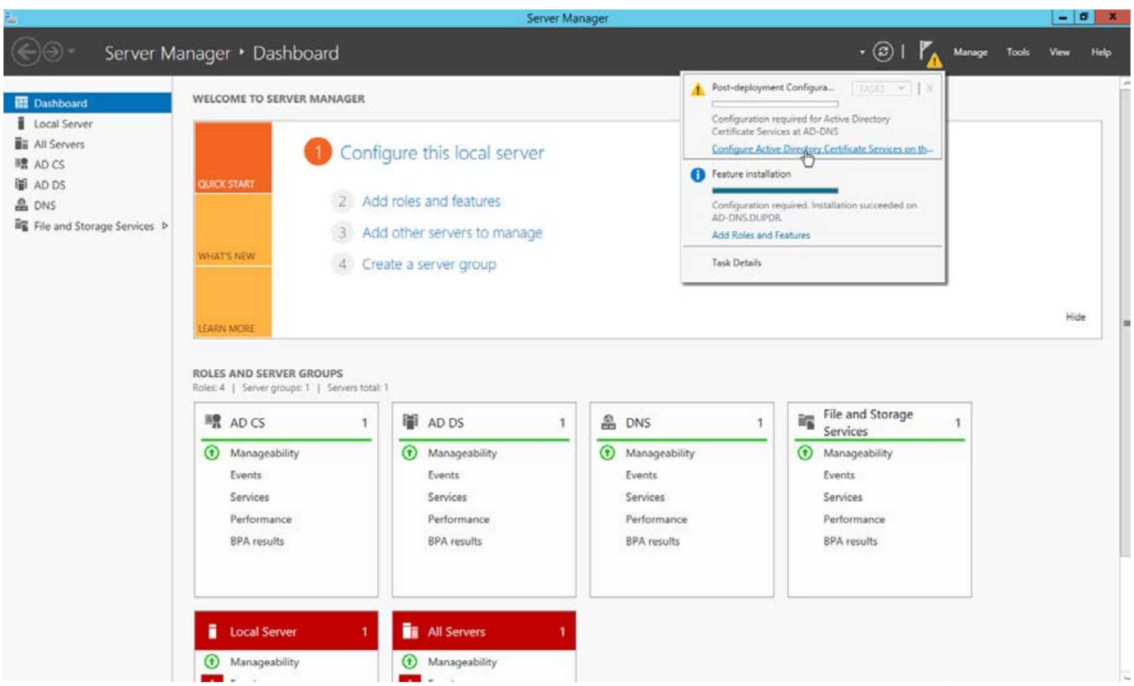
15. Click **Next.**



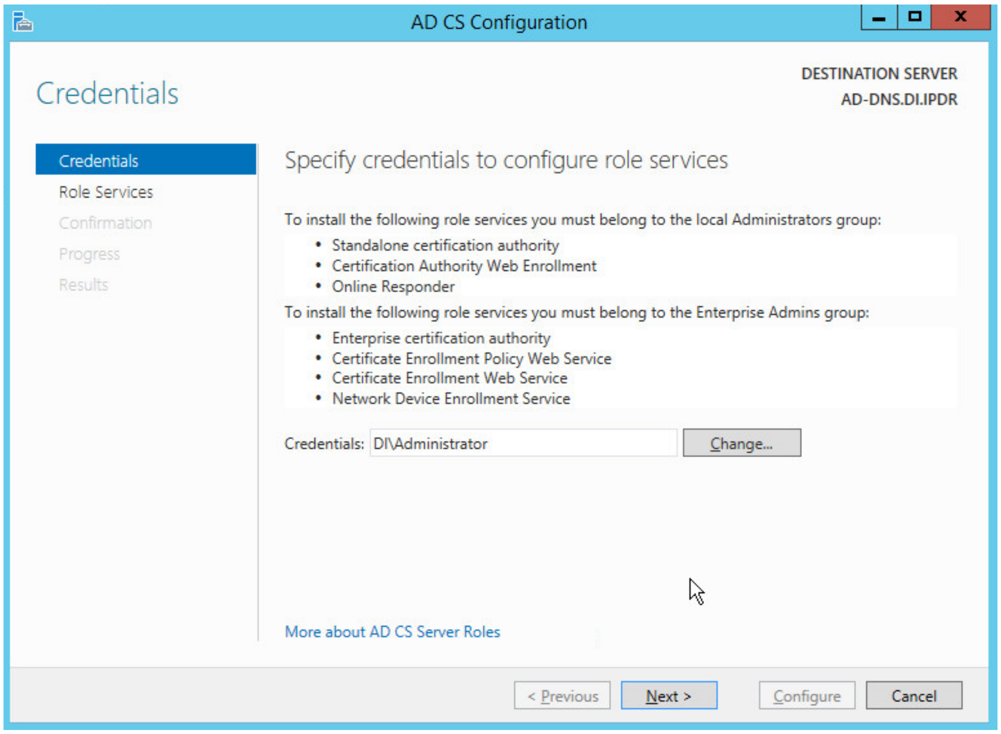
16. Click **Install.**
17. Wait for the installation to complete.



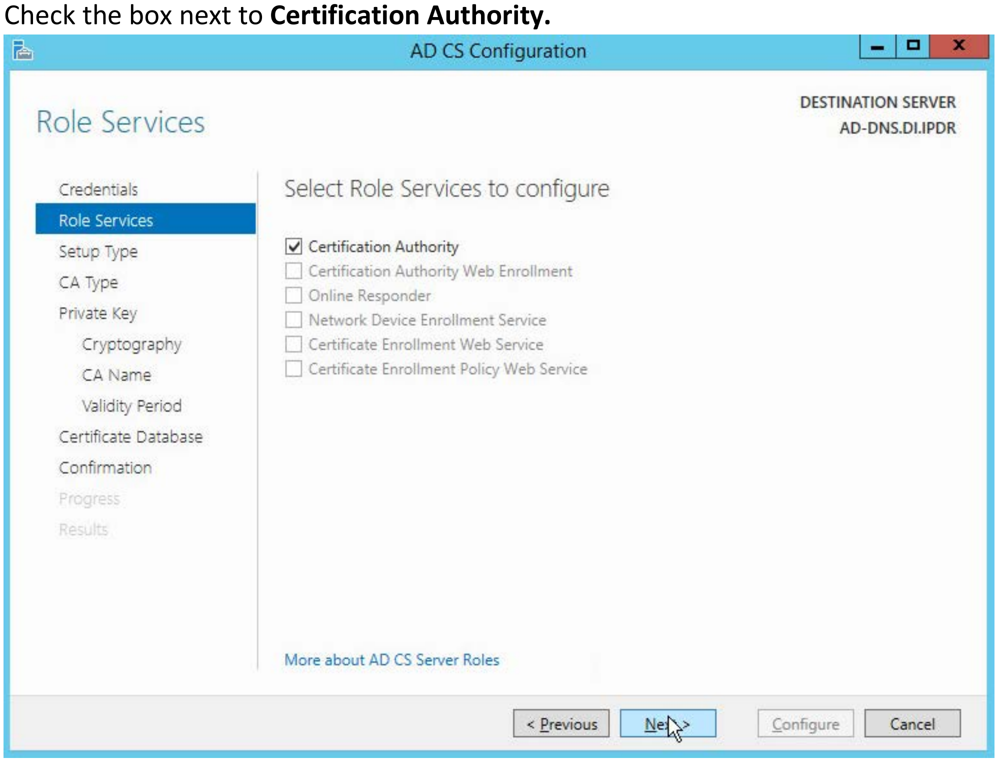
18. Click **Close.**



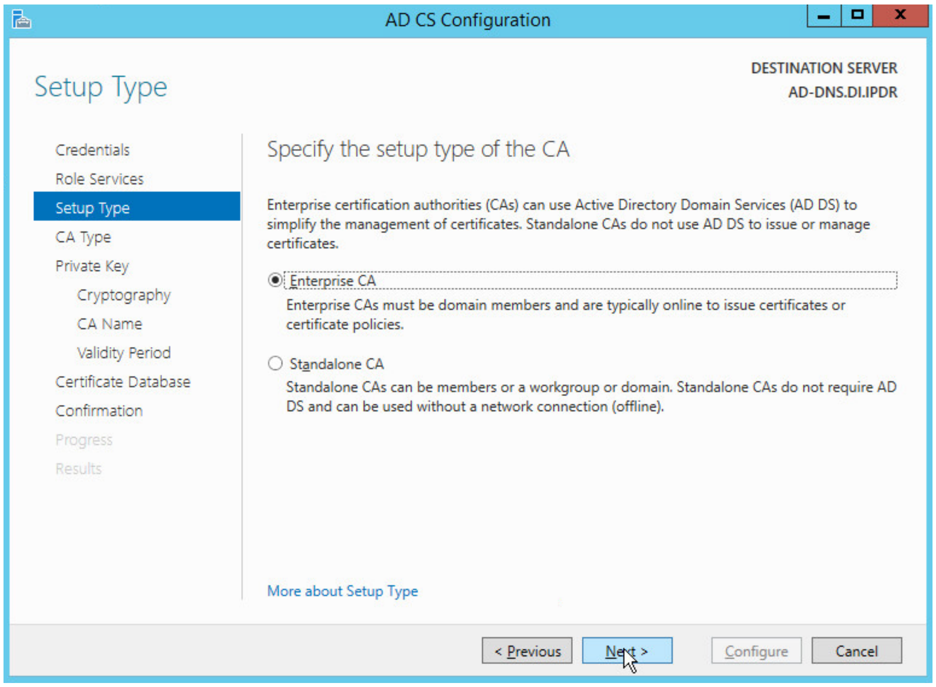
19. Click **Configure Active Directory Certificate Serves on the destination server.**



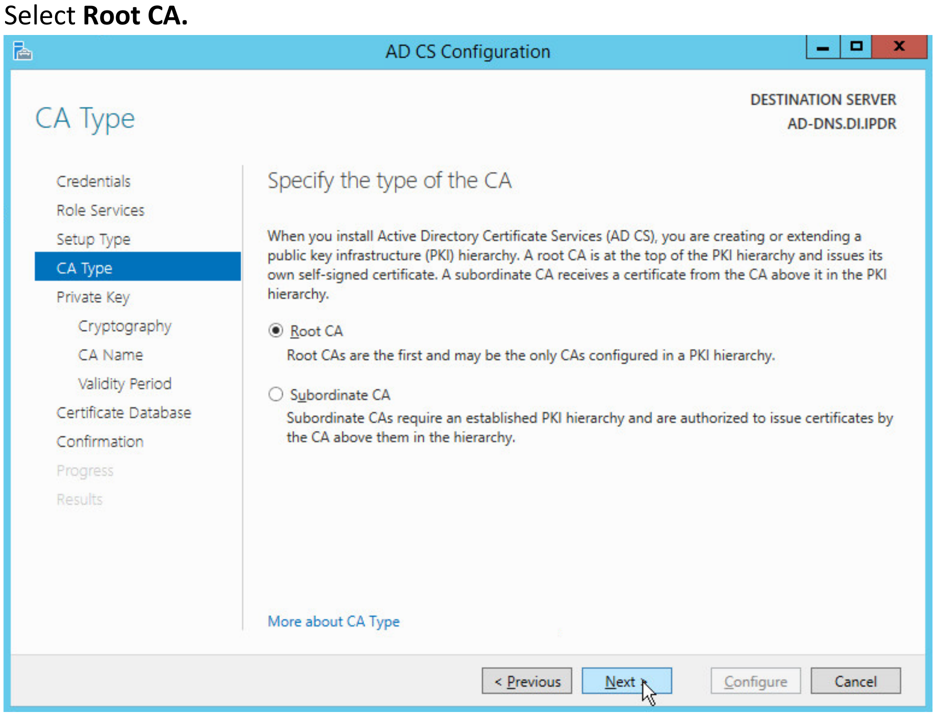
20. Click **Next.**
21. Check the box next to **Certification Authority.**



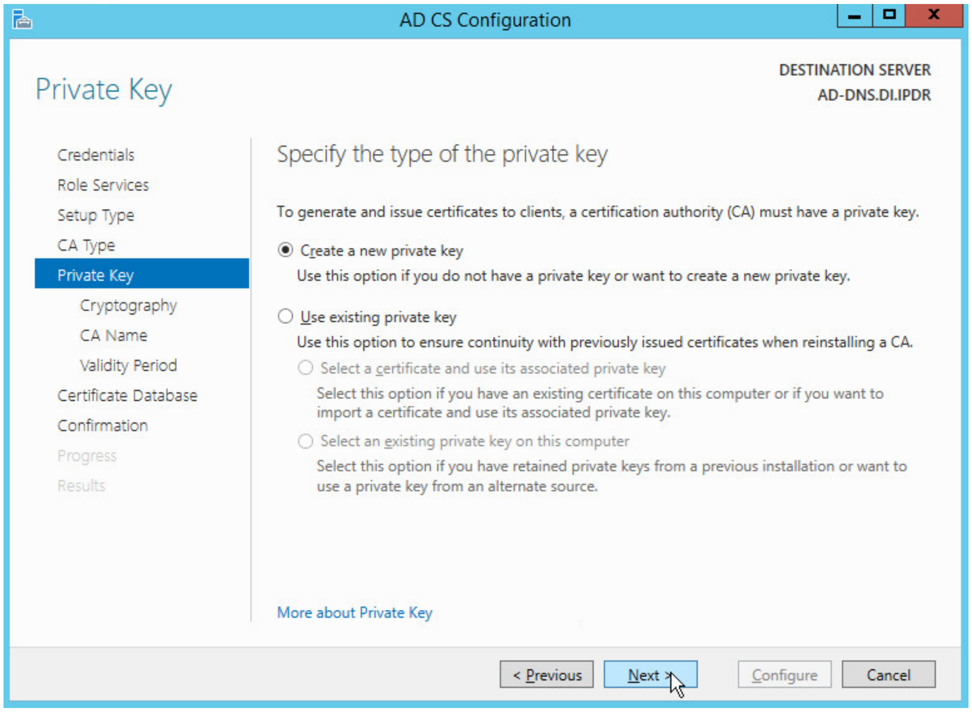
22. Click **Next.**
23. Select **Enterprise CA.**



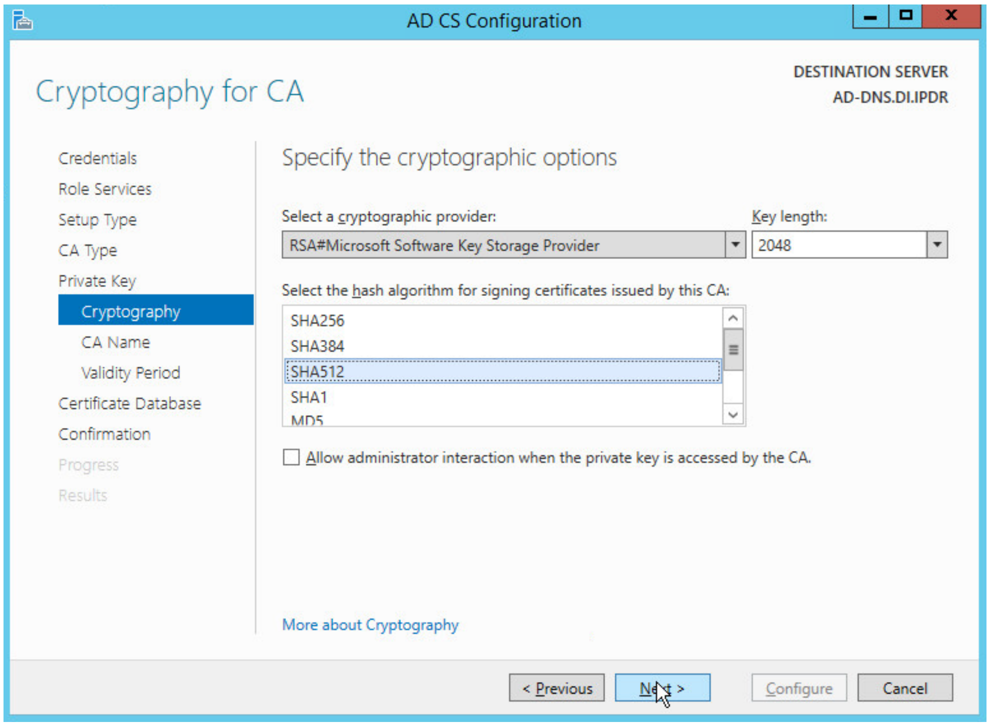
24. Click **Next.**
25. Select **Root CA.**



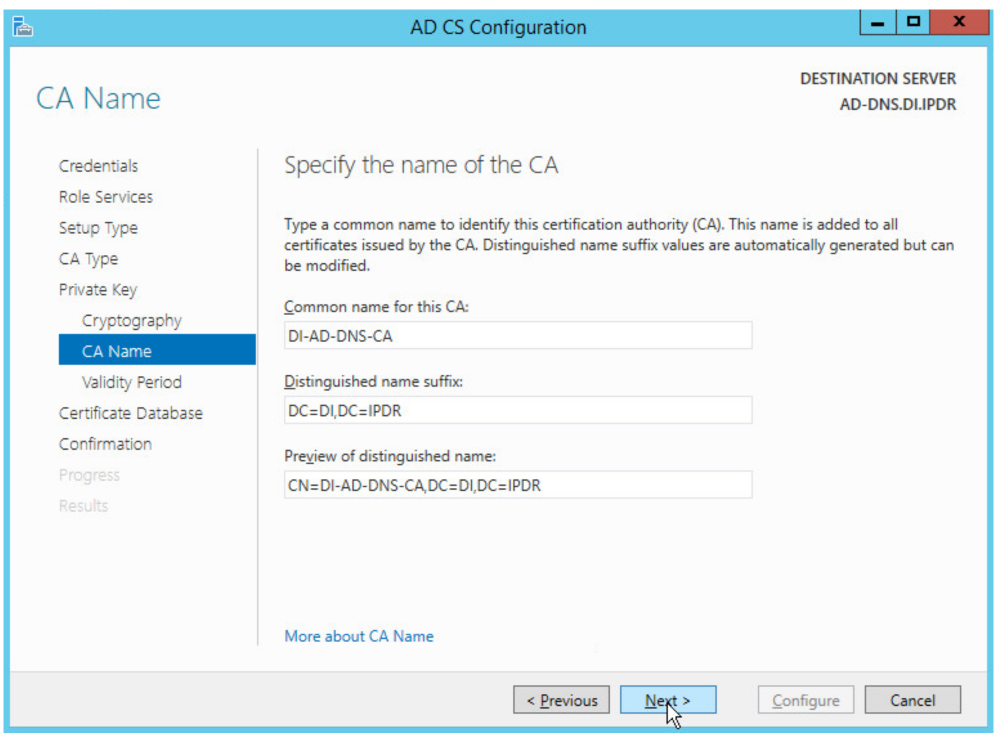
26. Click **Next.**
27. Select **Create a new private key.**



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

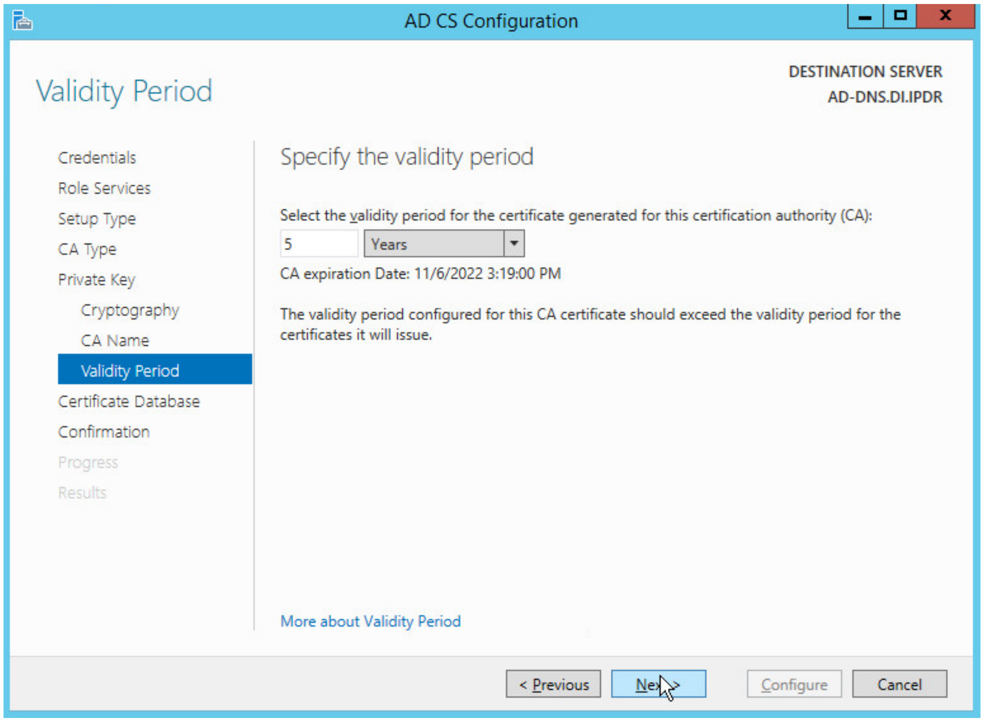


32. Click **Next.**

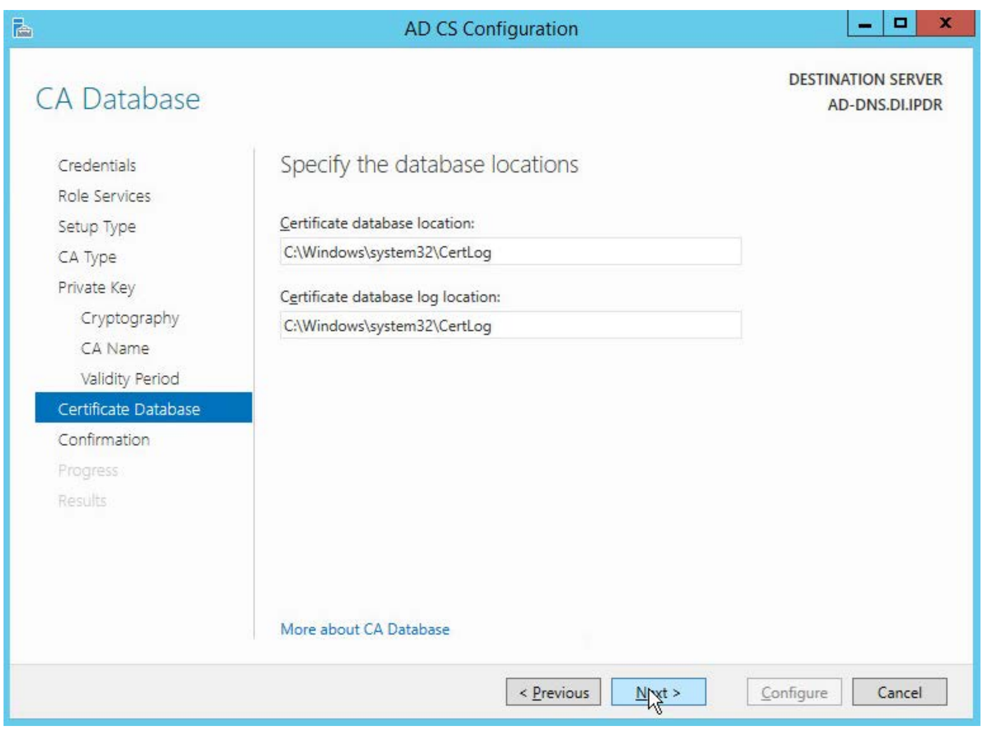


33. Click **Next.**

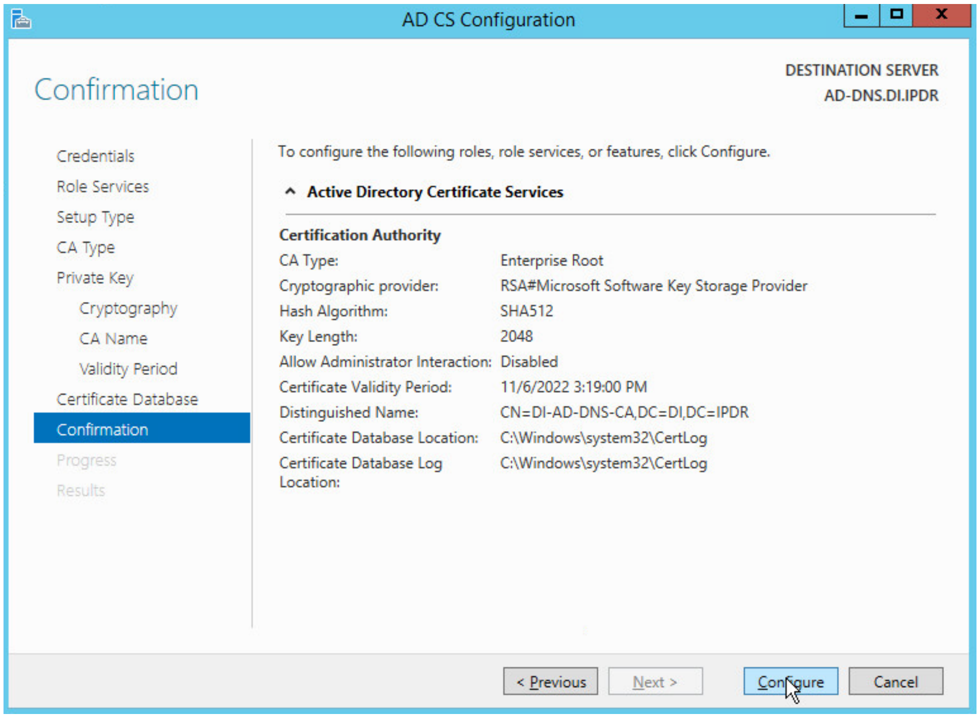
34. Set the validity period of the certificate according to the needs of your organization.



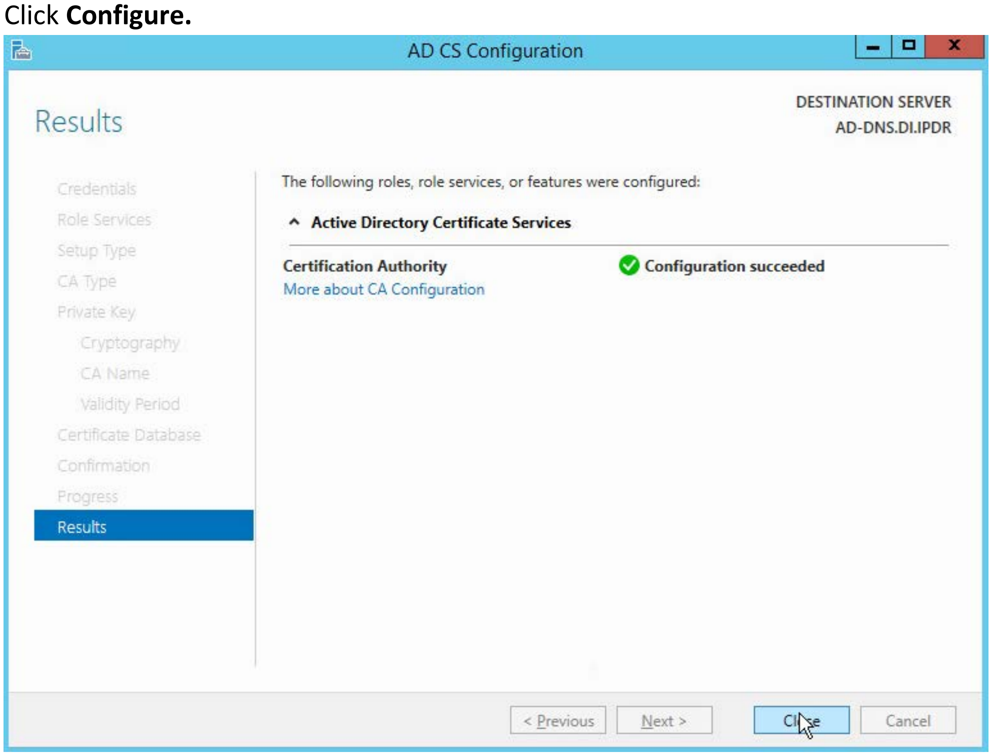
35. Click **Next.**



36. Click **Next.**



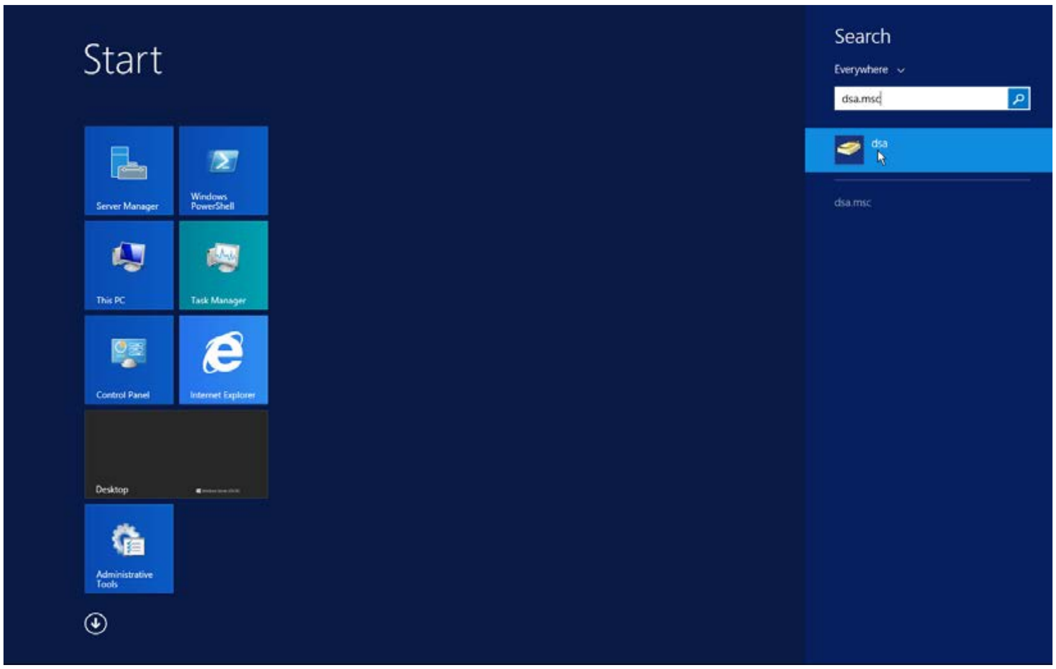
37. Click **Configure.**



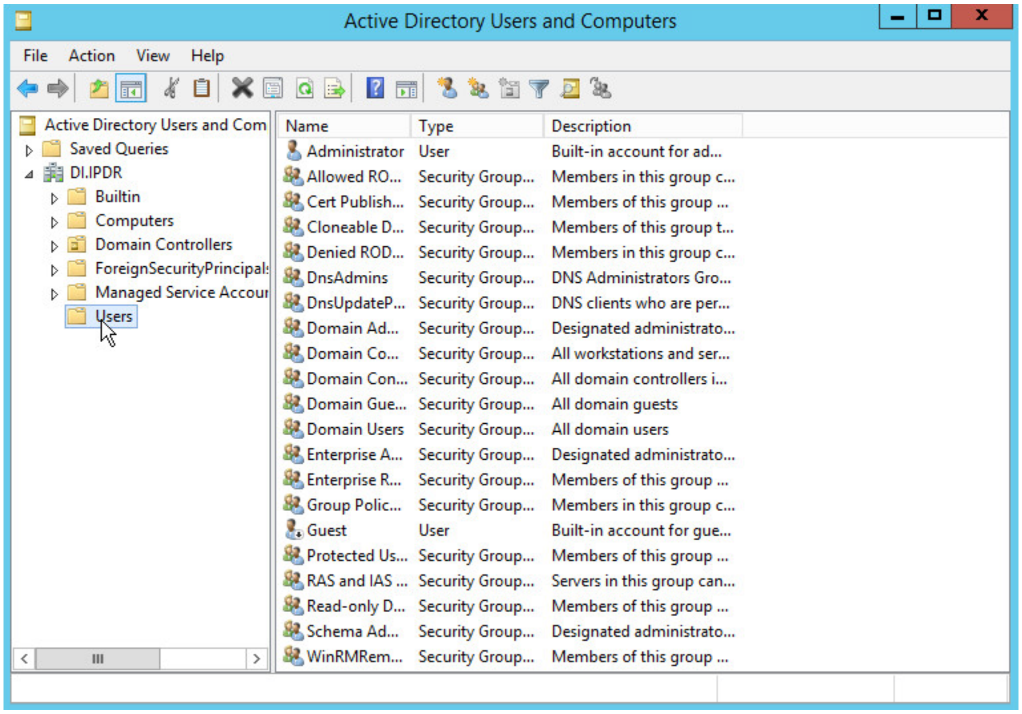
38. Click **Close.**

2.1.3 Configure Account to Add Computers to Domain

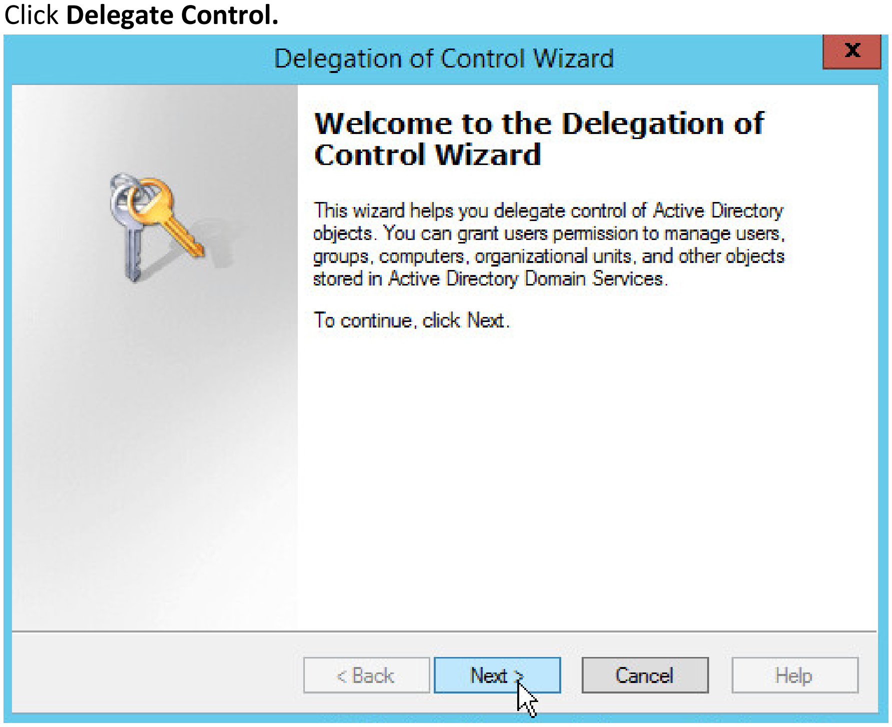
1. Open the **Start** menu.
2. Enter **dsa.msc,** and run the program.



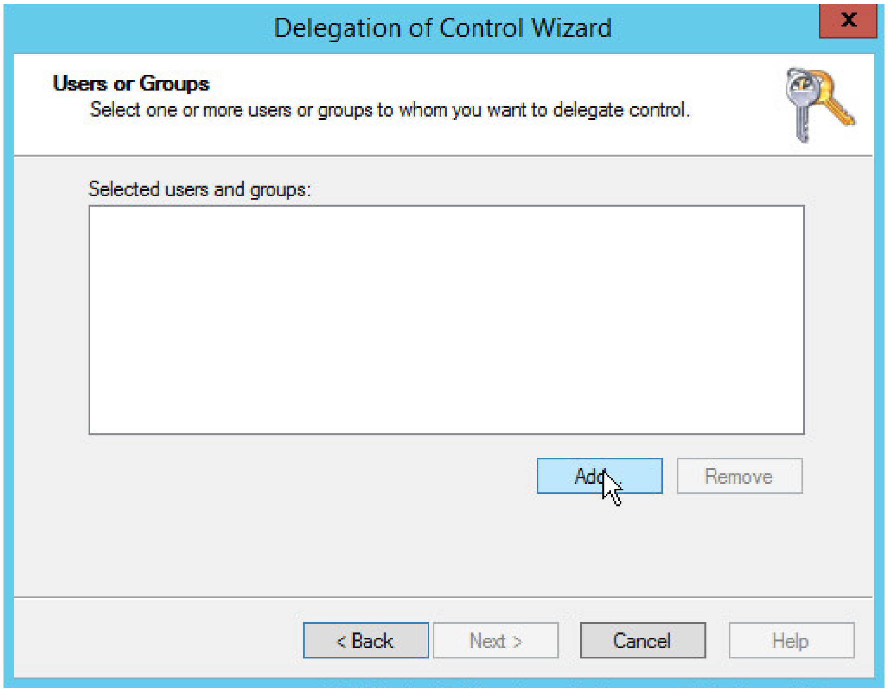
3. Right-click on **Users** in the left panel.



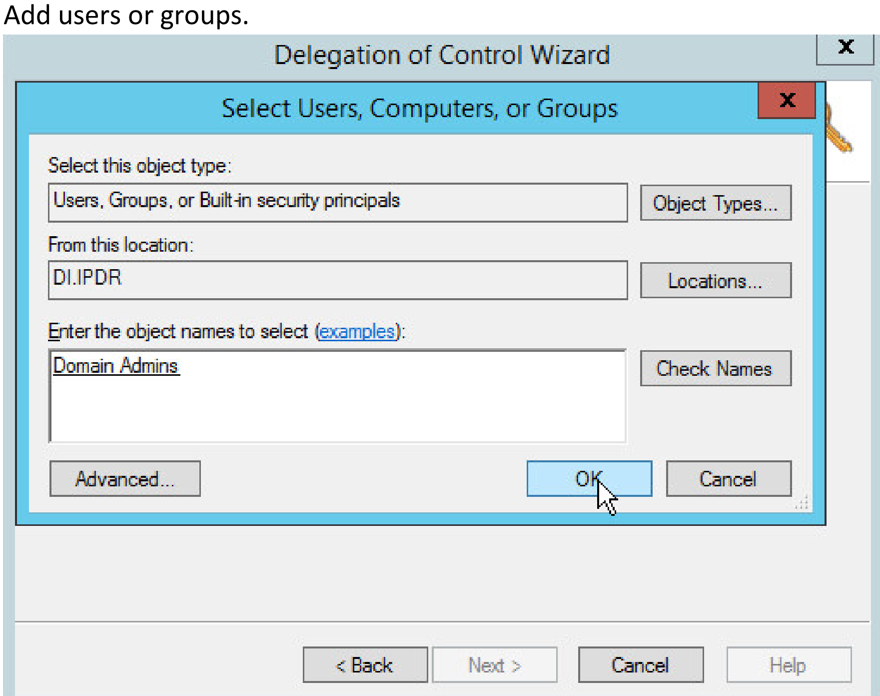
4. Click **Delegate Control.**



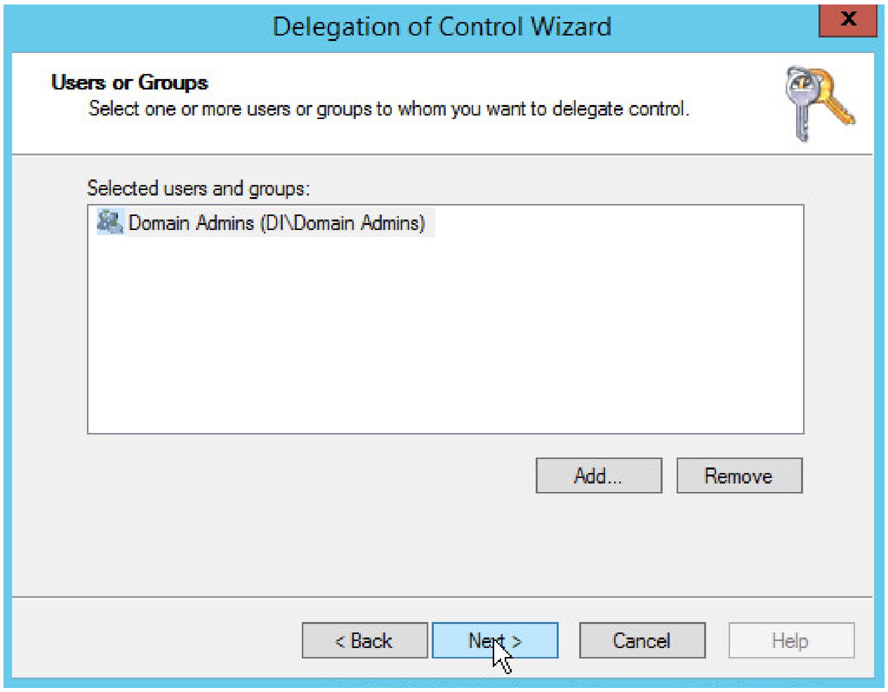
5. Click **Next.**



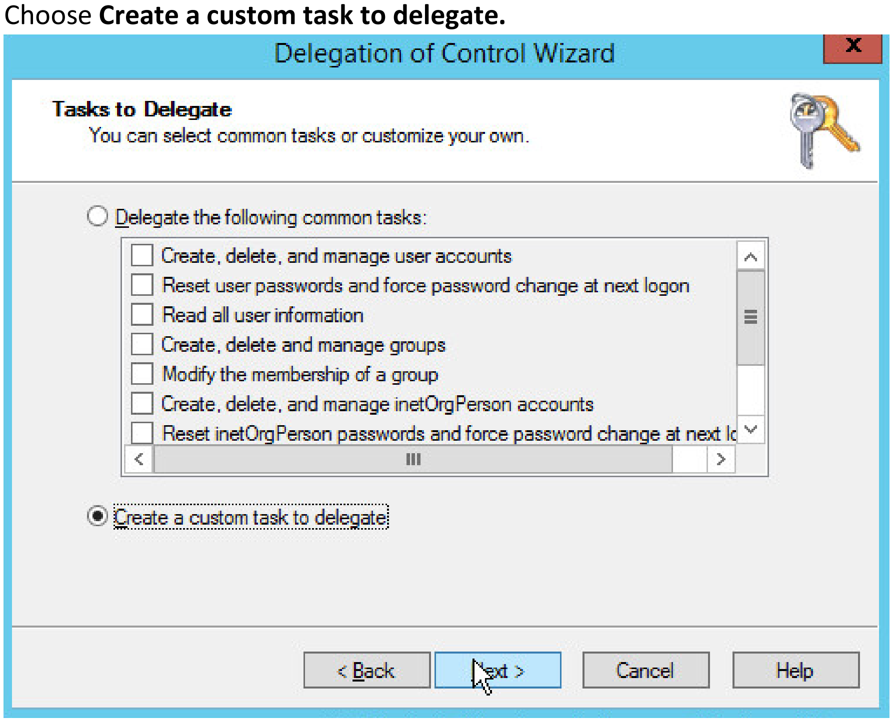
6. Click **Add** to select users or groups.
7. Add users or groups.



8. Click **OK.**

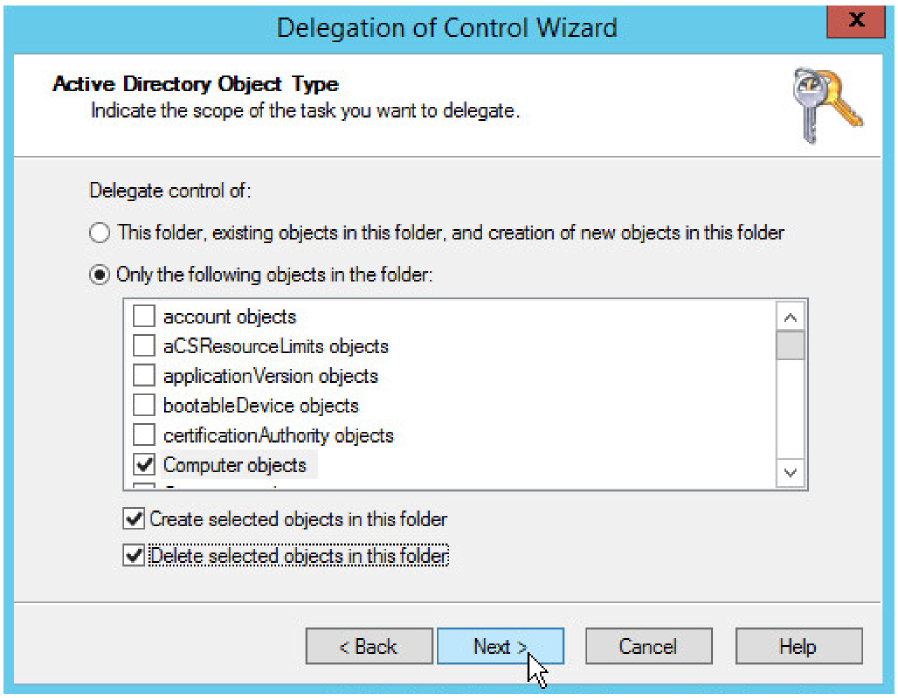


9. Click **Next.**
10. Choose **Create a custom task to delegate.**

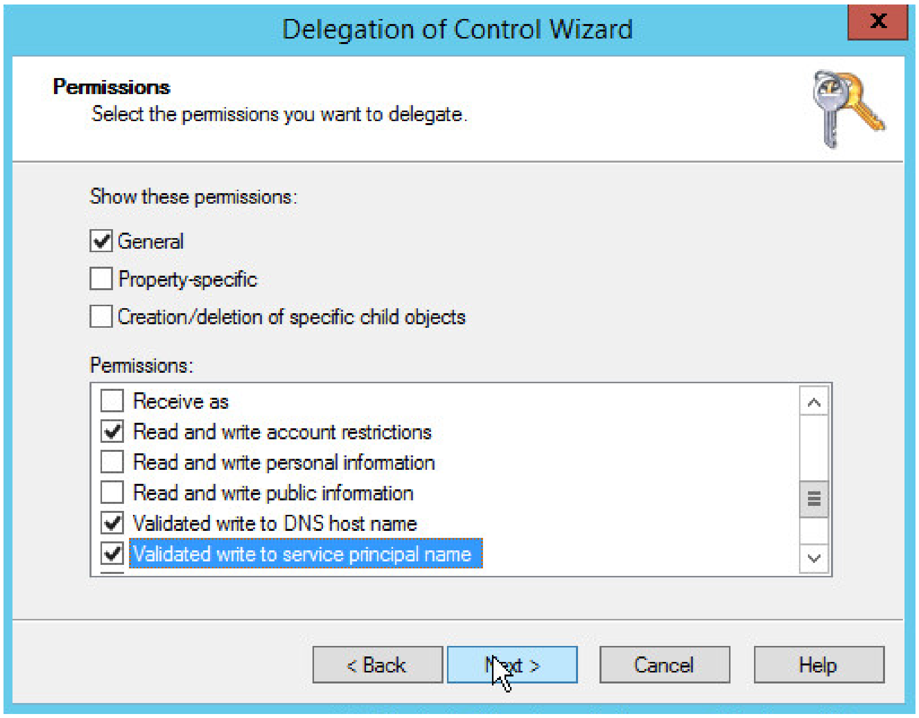


11. Click **Next.**
12. Choose **Only the following objects in the folder.**

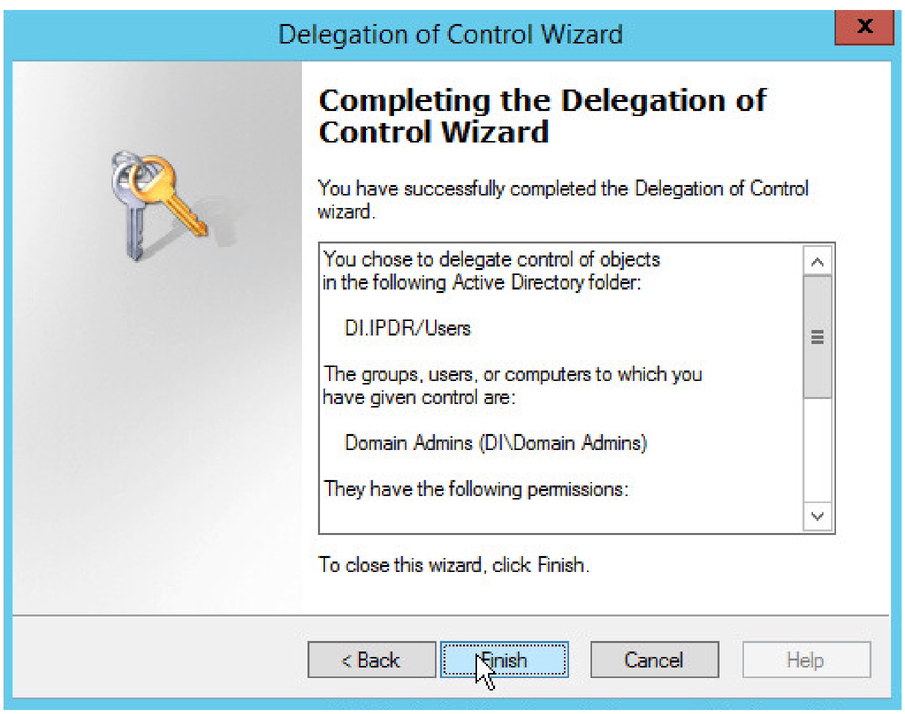
13. Check the box next to **Computer objects.**
14. Check the box next to **Create selected objects in this folder.**
15. Check the box next to **Delete selected objects in this folder.**



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



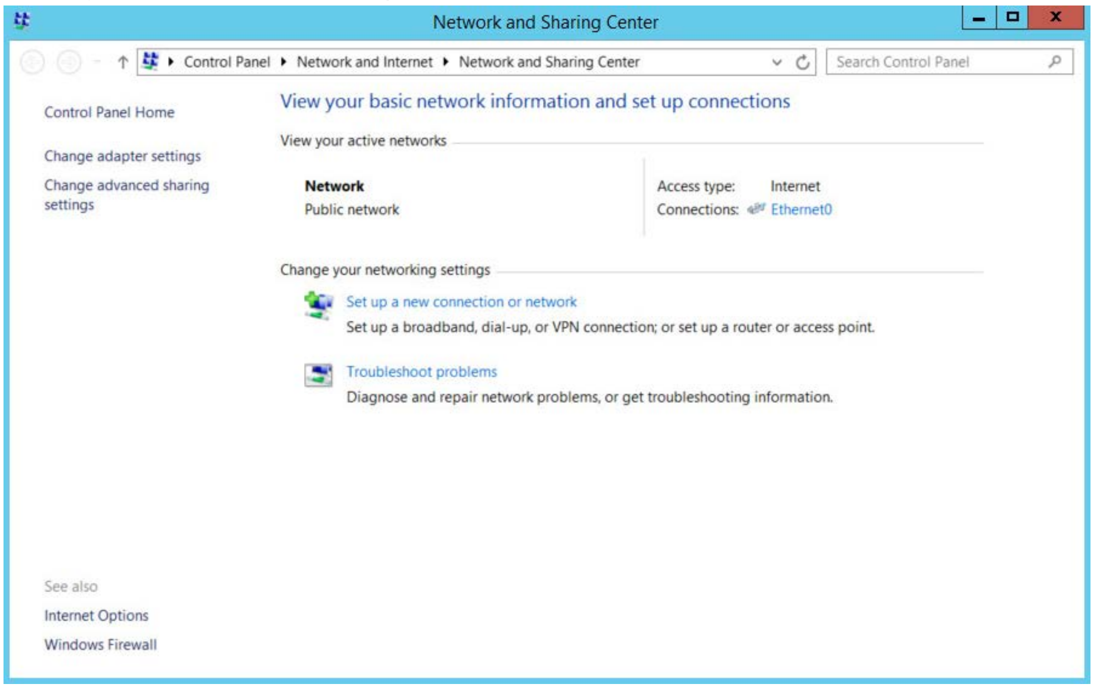
18. Click **Next.**



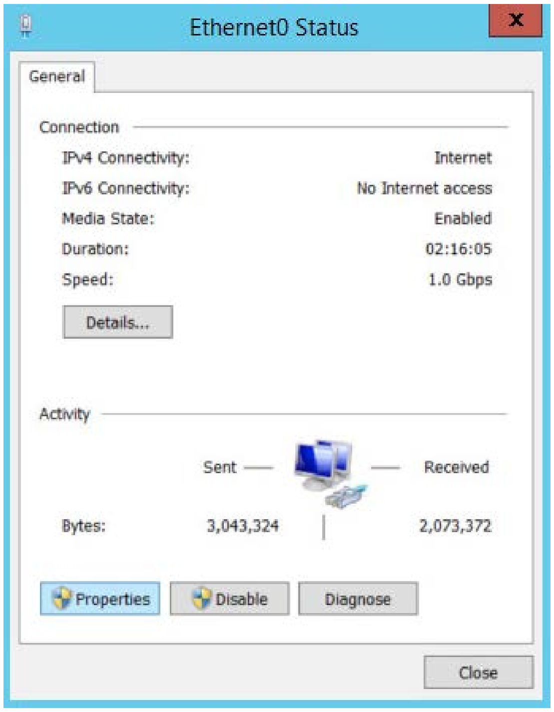
19. Click **Finish.**

2.1.4 Add Machines to the Domain

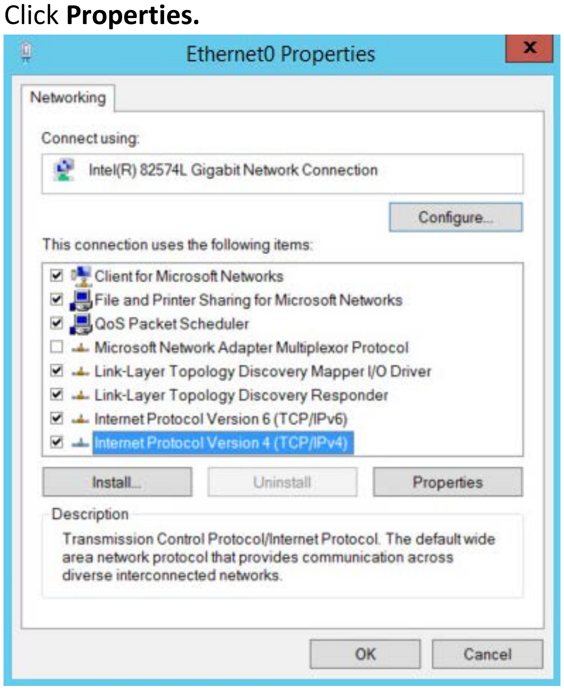
1. Right-click the network icon in the task bar, on a computer that you wish to add to the domain.
2. Click **Open Network and Sharing Center.**



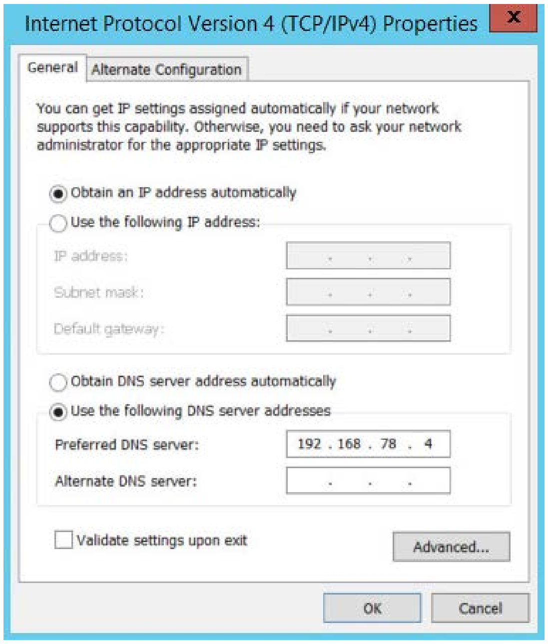
3. Click the name of the internet adapter.



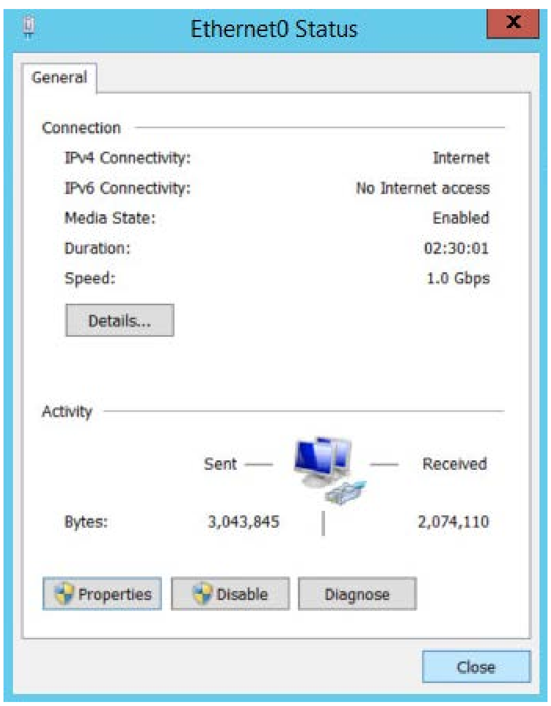
4. Click **Properties.**



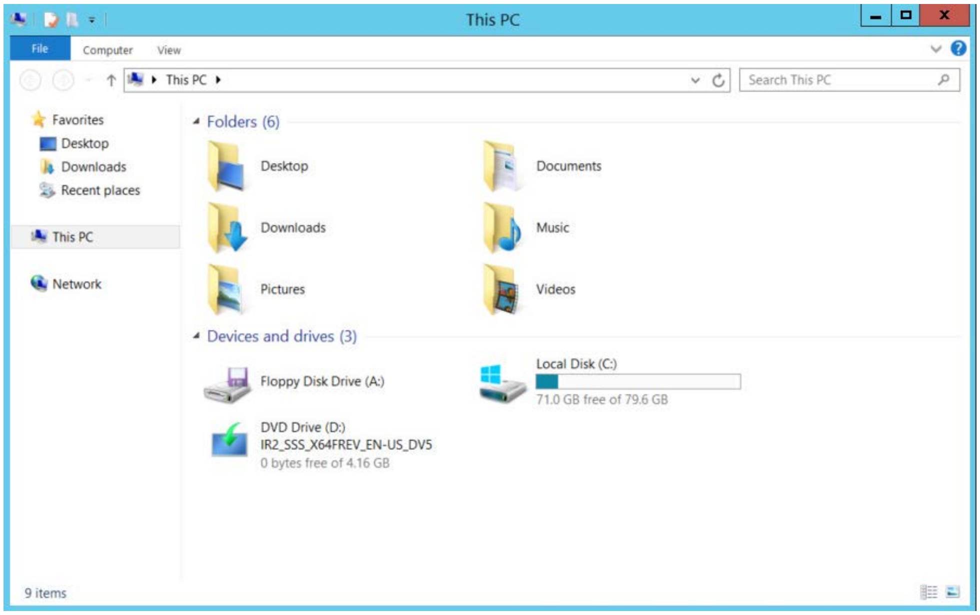
5. Double-click **Internet Protocol Version 4 (TCP/IPv4).**
6. Select **Use the following DNS server addresses.**
7. Enter the **IP address** of the DNS server.



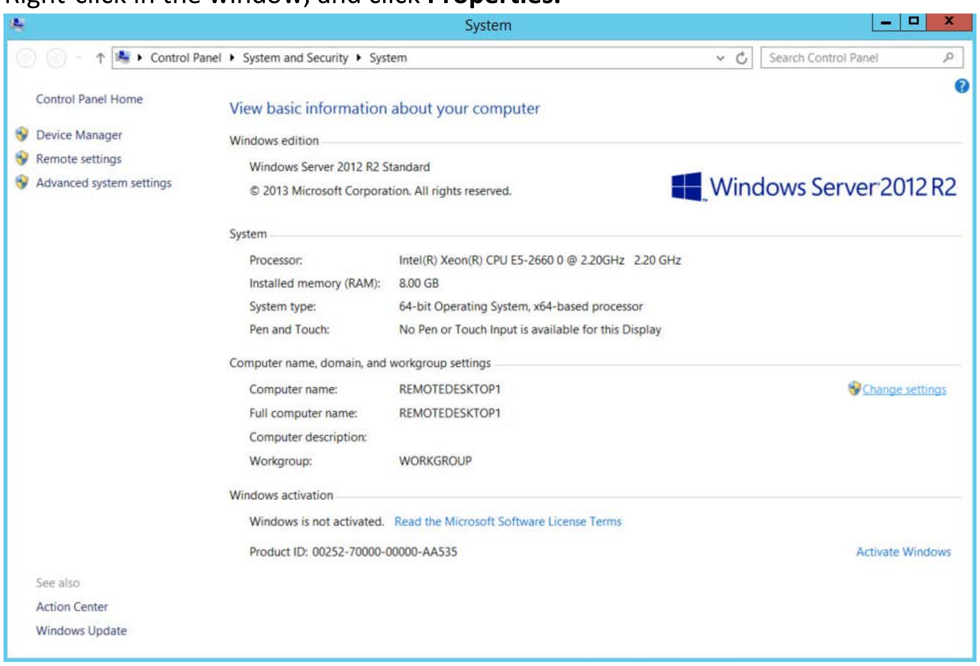
8. Click **OK.**
9. Click **OK.**



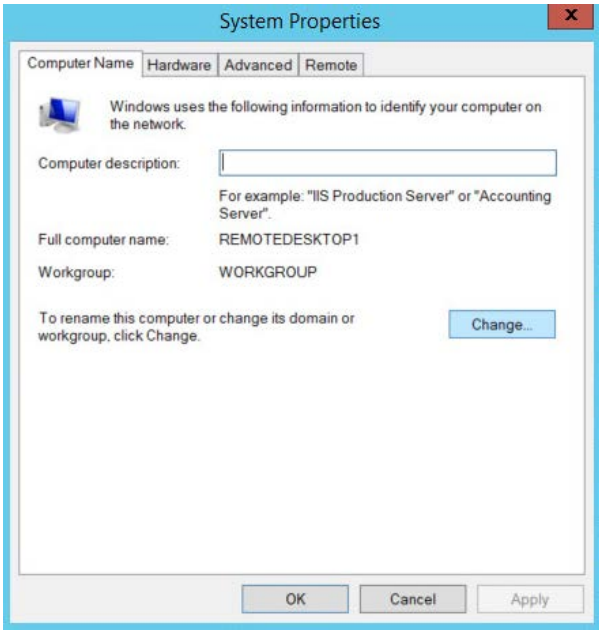
10. Click **Close.**
11. Navigate to **This PC.**



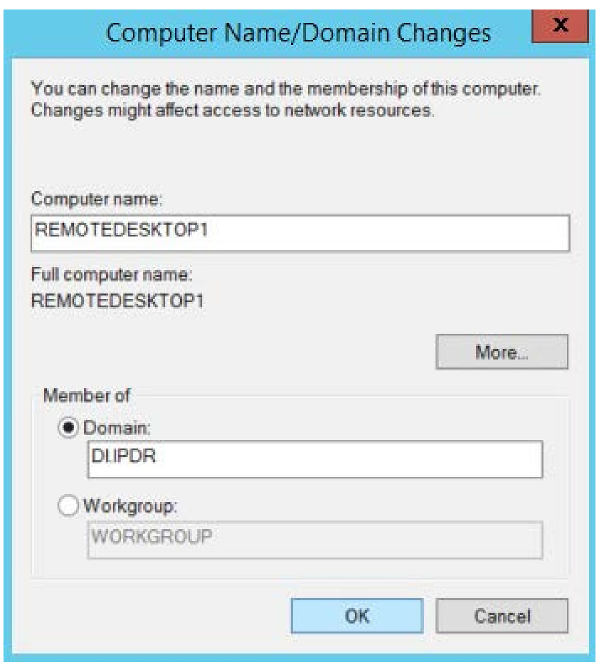
12. Right-click in the window, and click **Properties.**



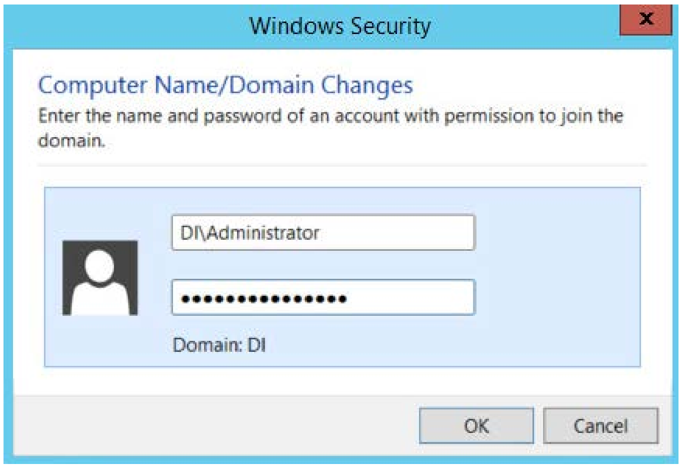
13. Click **Change Settings.**



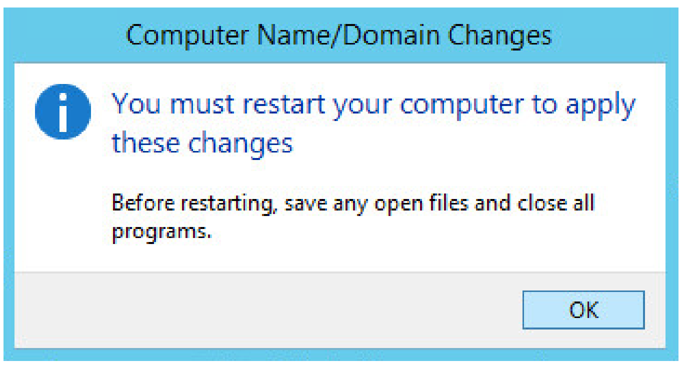
14. Click **Change.**
15. Select **Domain.**
16. Enter the domain.



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



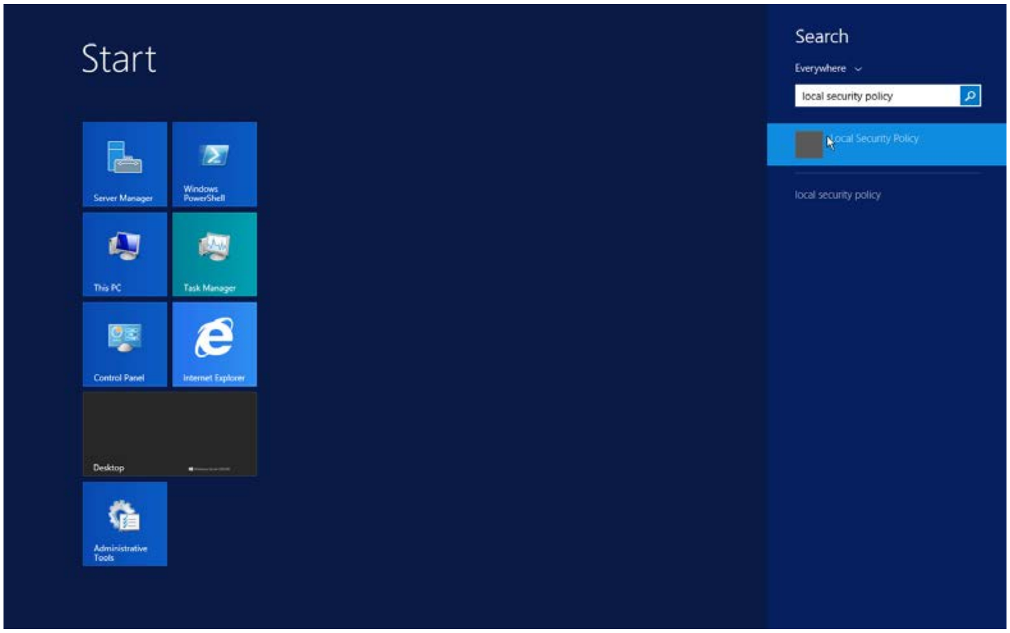
19. Click **OK.**



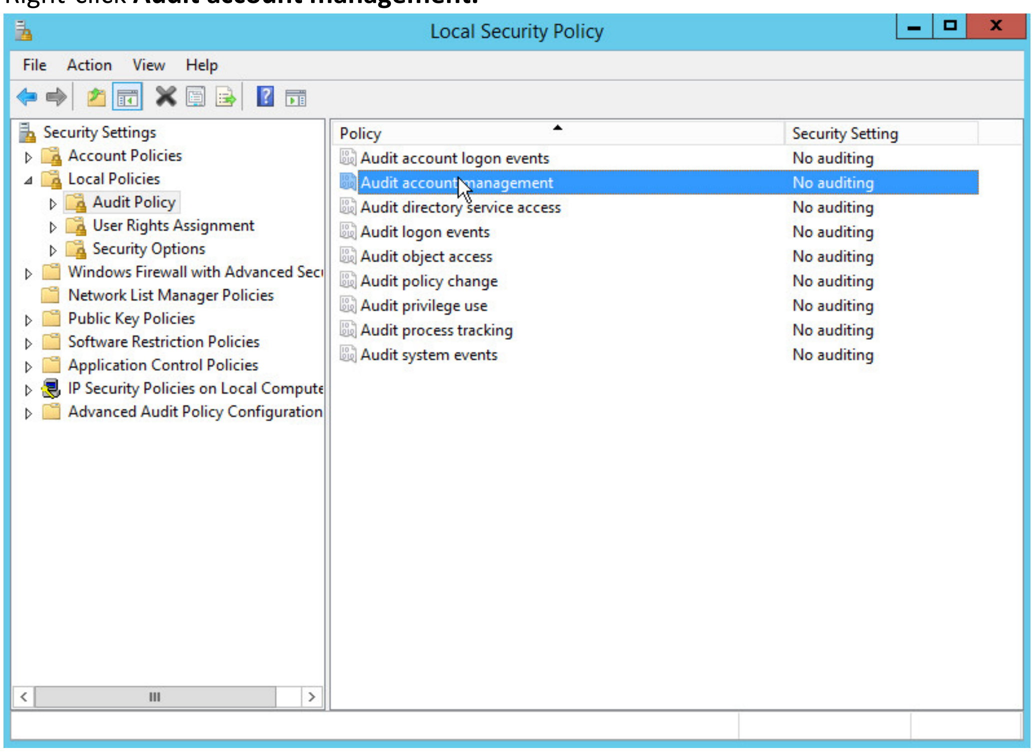
20. Click **OK** when prompted to restart the computer.

2.1.5 Configure Active Directory to Audit Account Activity

1. Open the **Start** Menu.

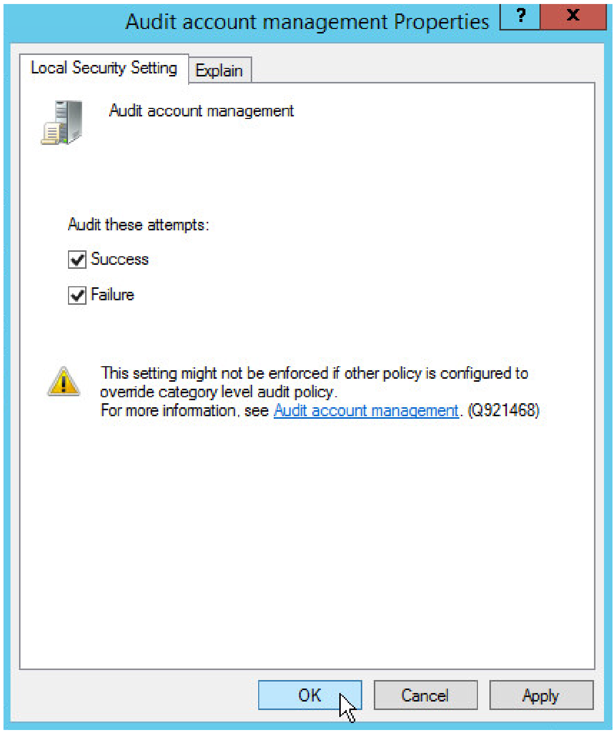


2. Enter Local Security Policy in the search bar, and open the program.
3. Navigate to **Local Policies > Audit Policy.**
4. Right-click **Audit account management.**



5. Click **Properties.**

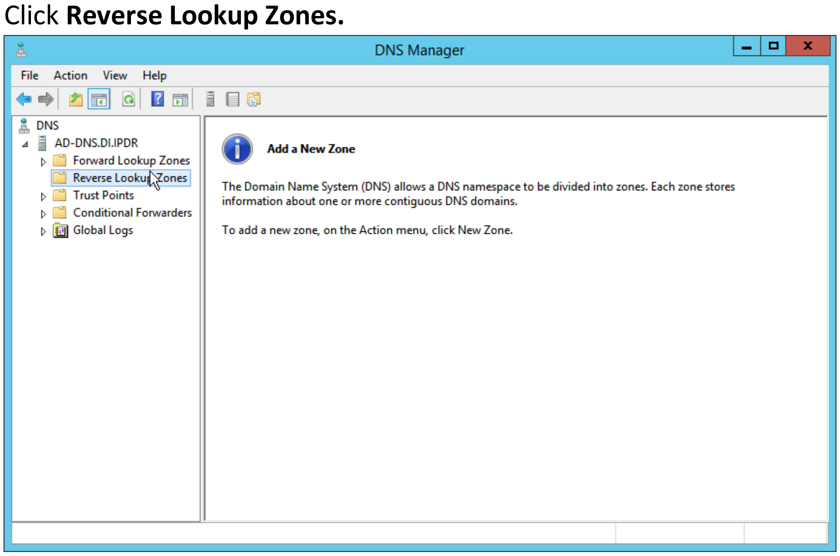
6. Check the boxes next to **Success** and **Failure.**



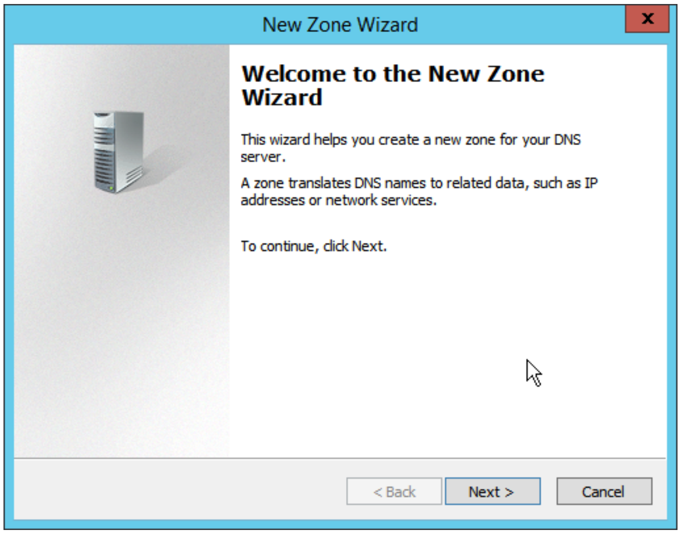
7. Click **OK.**

2.1.6 Configure Reverse Lookup Zones

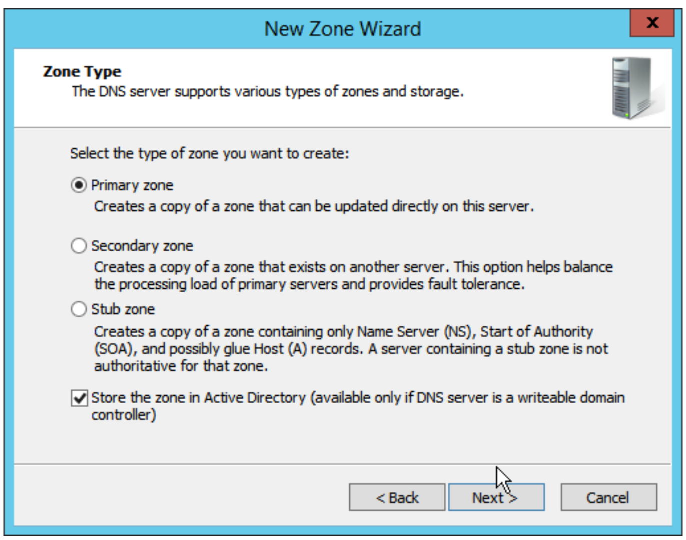
1. Open **DNS Manager** by right-clicking the DNS server in **Server Manager.**
2. Click **Reverse Lookup Zones.**



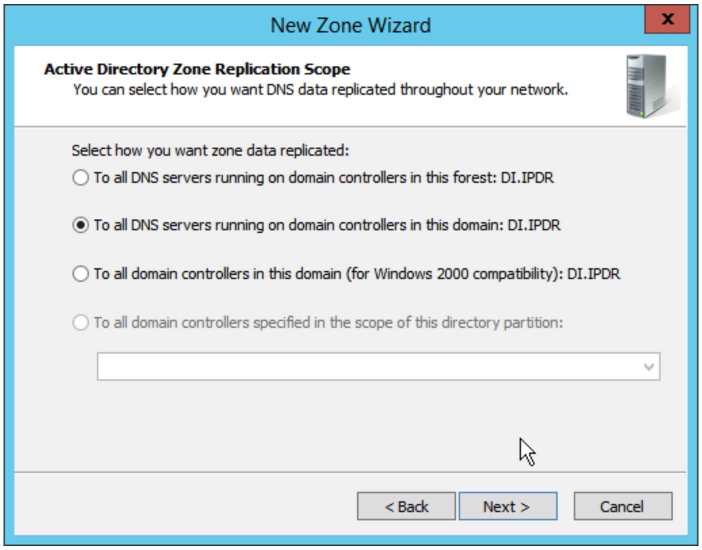
3. Click **Action > New Zone.**



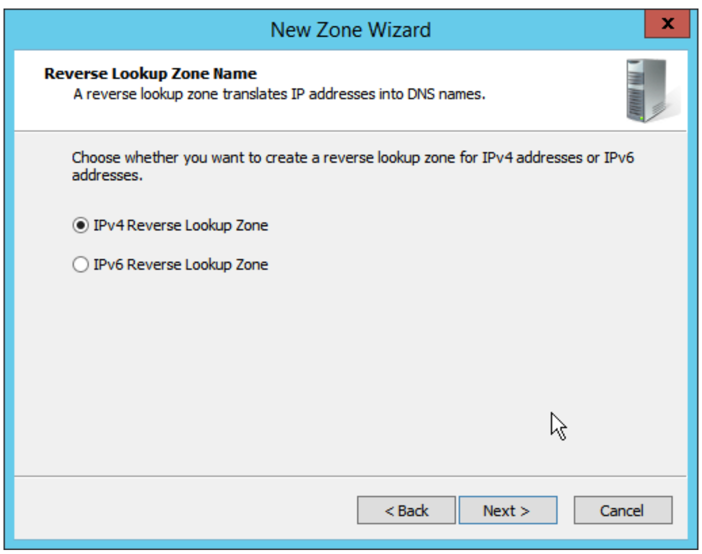
4. Click **Next.**



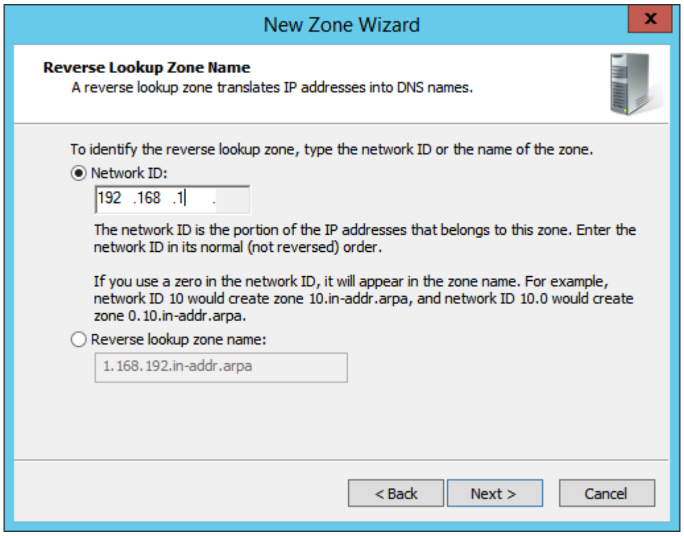
5. Click **Next.**



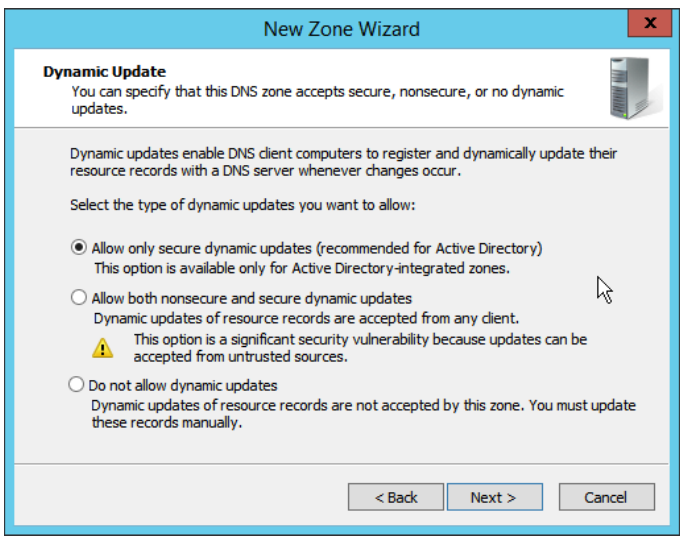
6. Click **Next.**



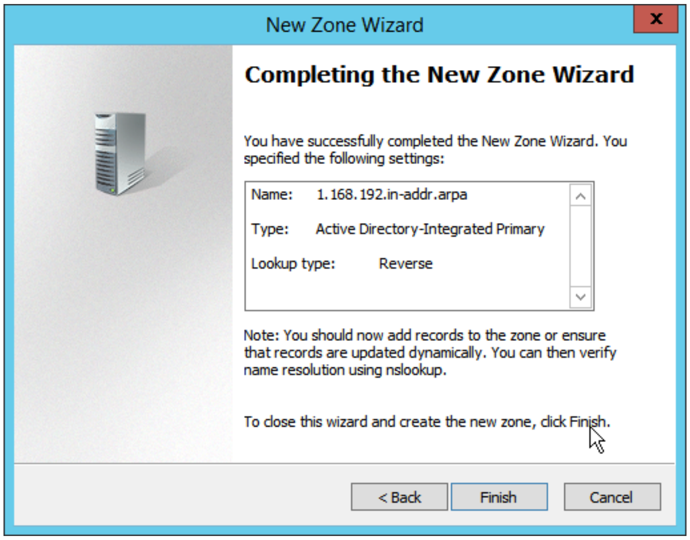
7. Click **Next.**
8. Enter the first three parts of the IP address of the AD/DNS server (for example, 192.168.1).



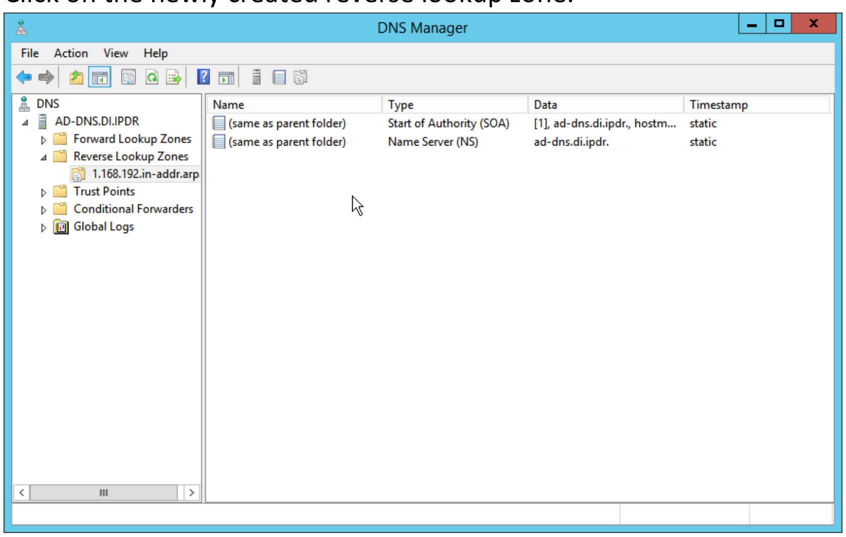
9. Click **Next.**



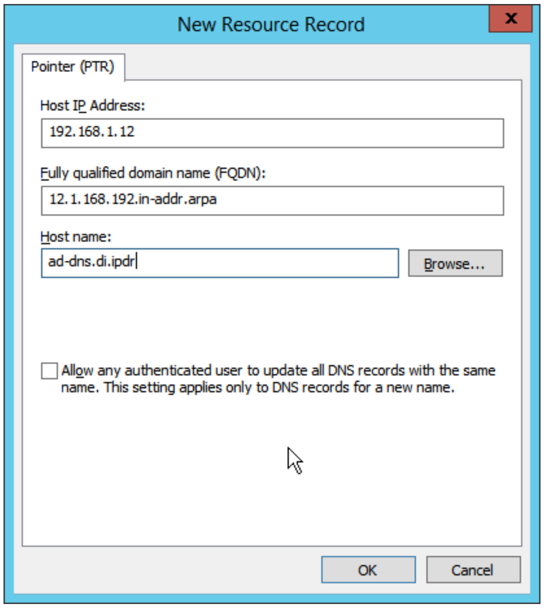
10. Click **Next.**



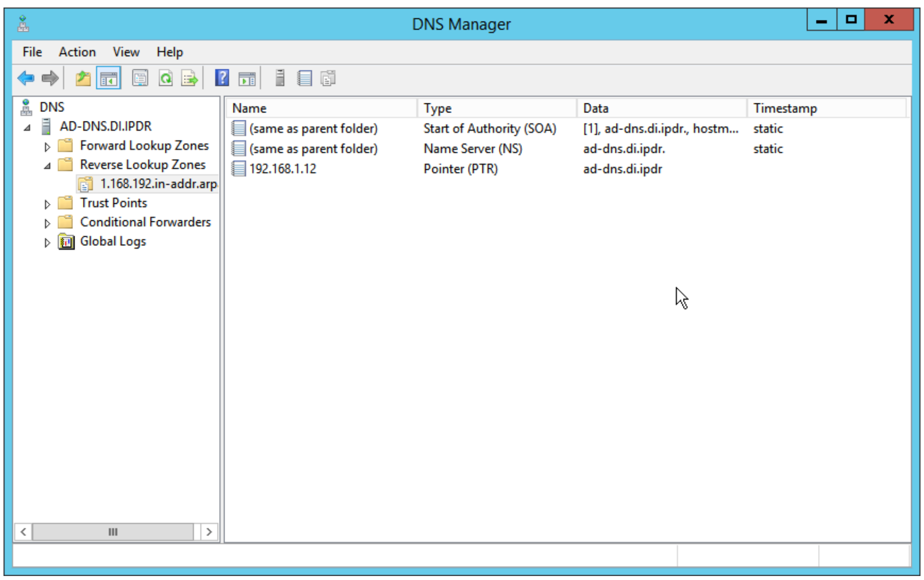
11. Click **Finish.**
12. Click on the newly created reverse lookup zone.



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



16. Click **OK.**

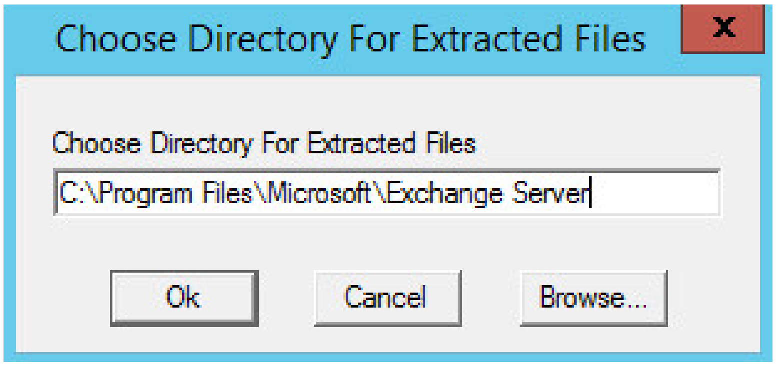


2.2 Microsoft Exchange Server

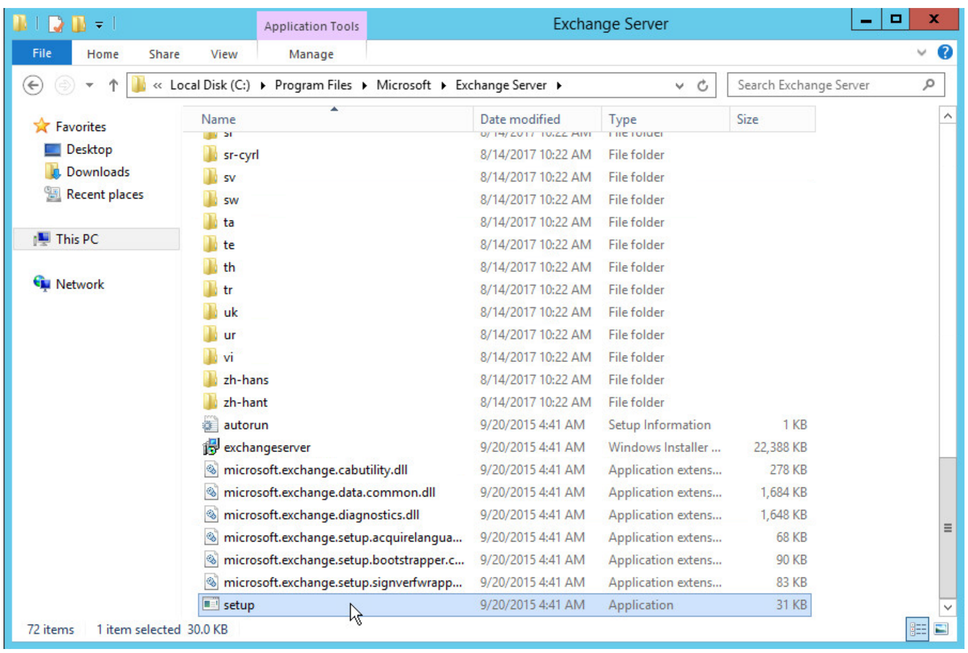
As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

2.2.1 Install Microsoft Exchange

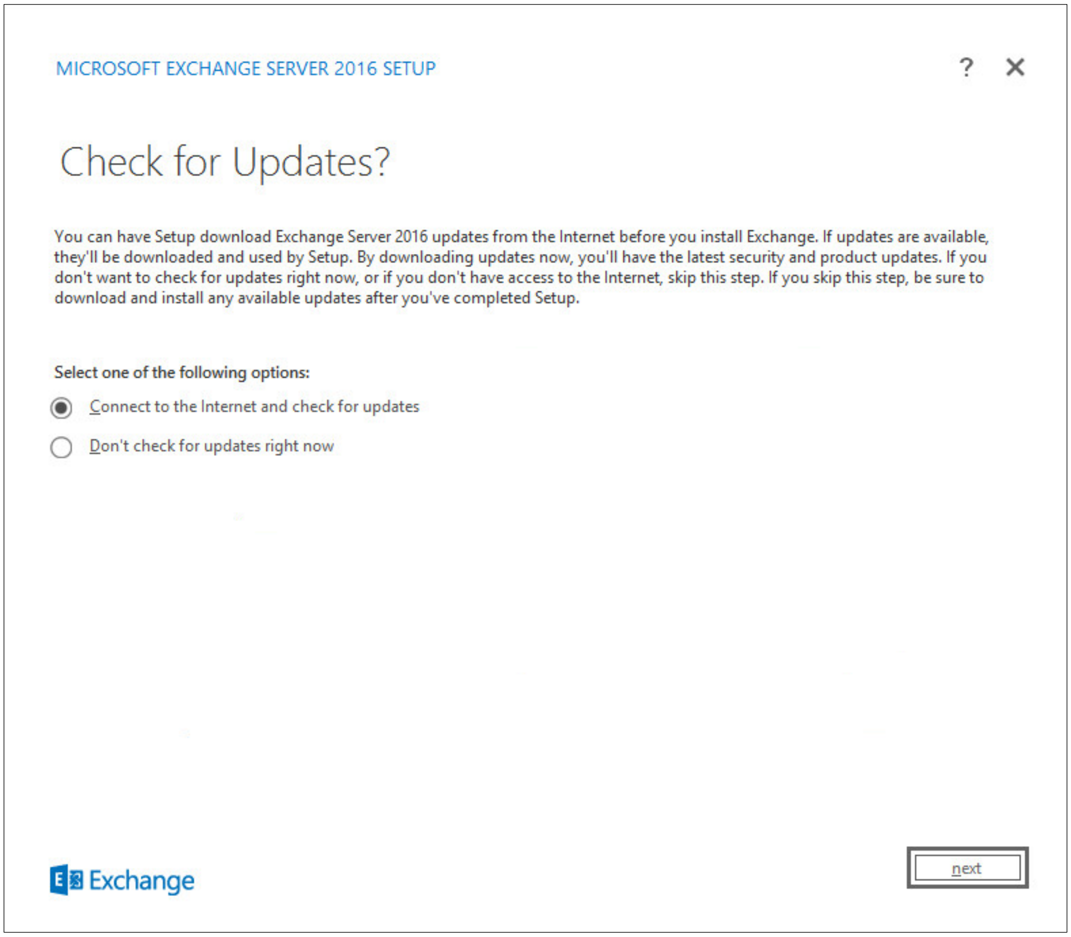
1. Run **Exchange2016-x64.exe.**
2. Choose the directory for the extracted files.



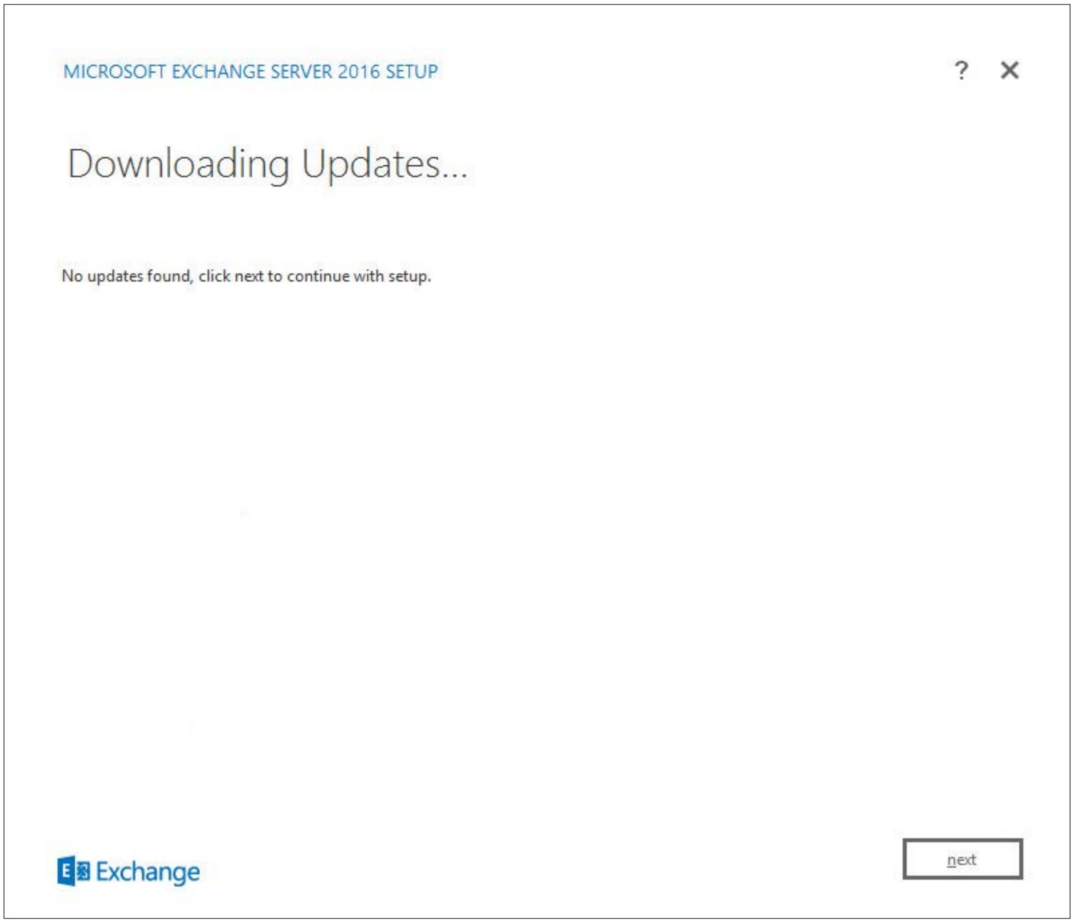
3. Click **OK.**



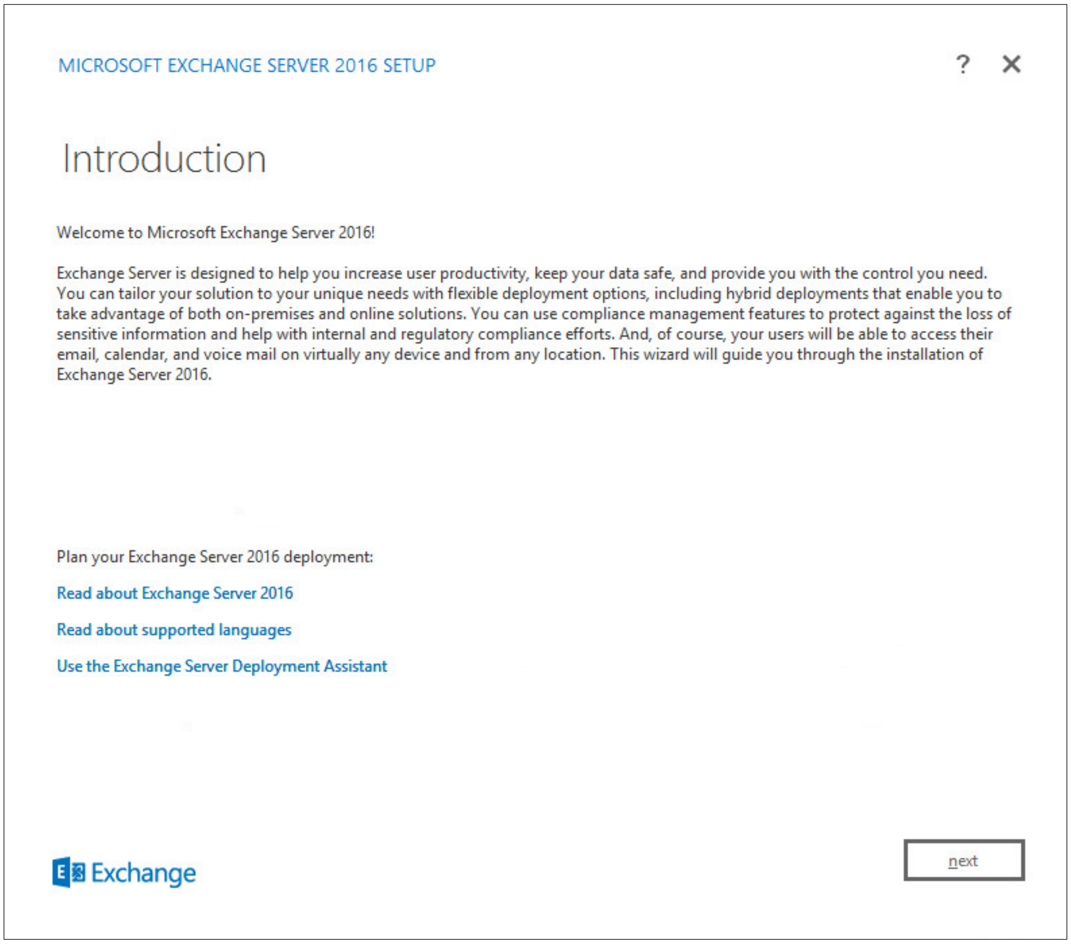
4. Enter the directory and run **setup.exe.**
5. Select **Connect to the Internet and check for updates.**



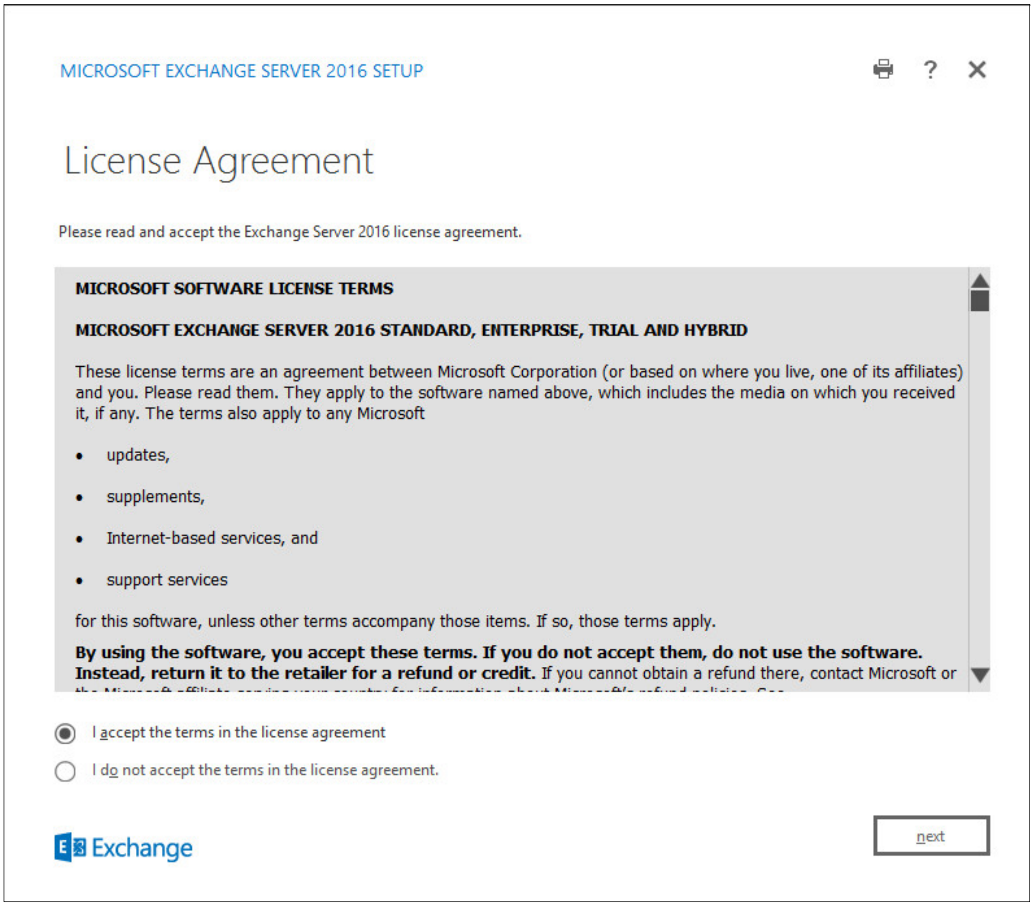
6. Click **Next.**
7. Wait for the check to finish.



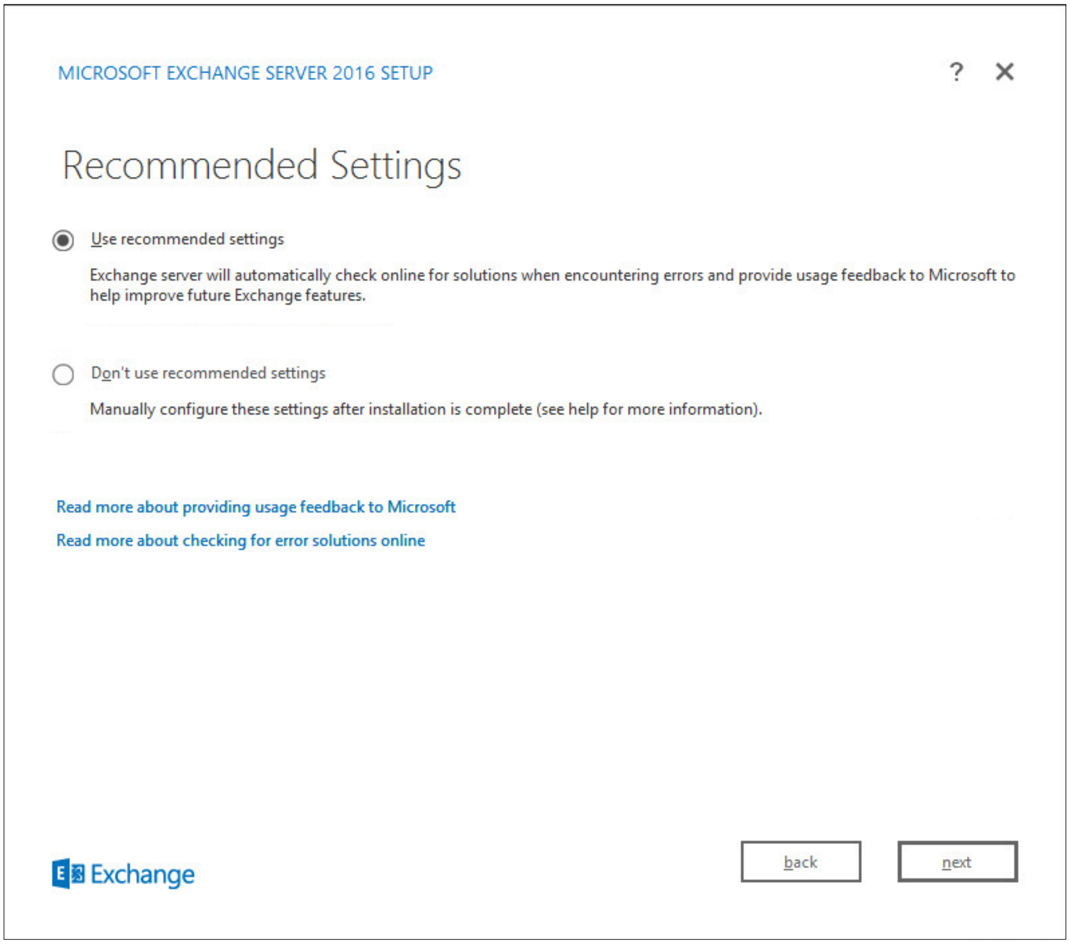
8. Click **Next.**
9. Wait for the copying to finish.



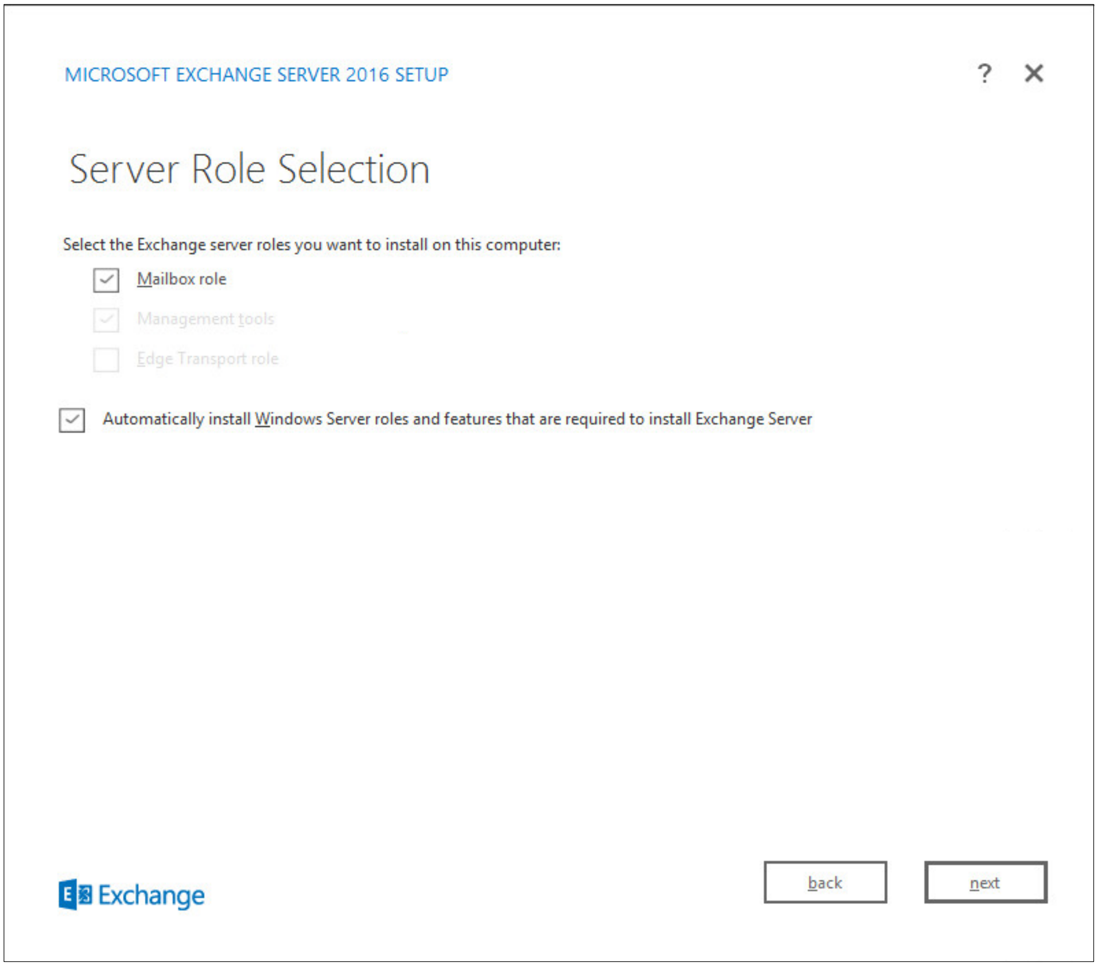
10. Click **Next.**
11. Click **I accept the terms in the license agreement.**



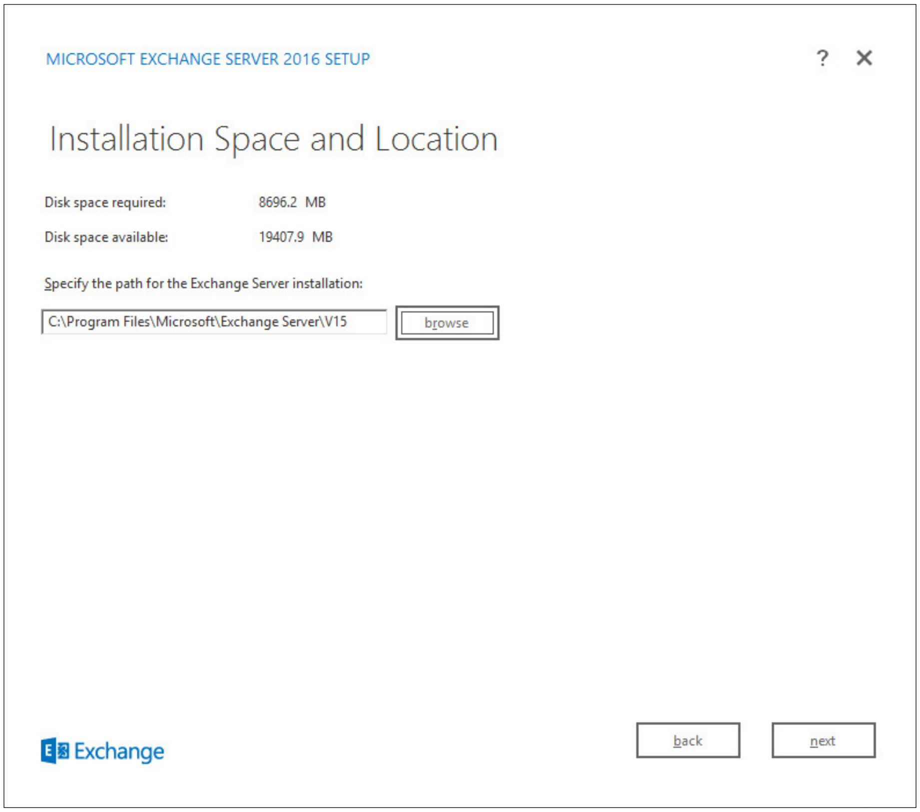
12. Click **Next.**
13. Click **Use Recommended Settings.**



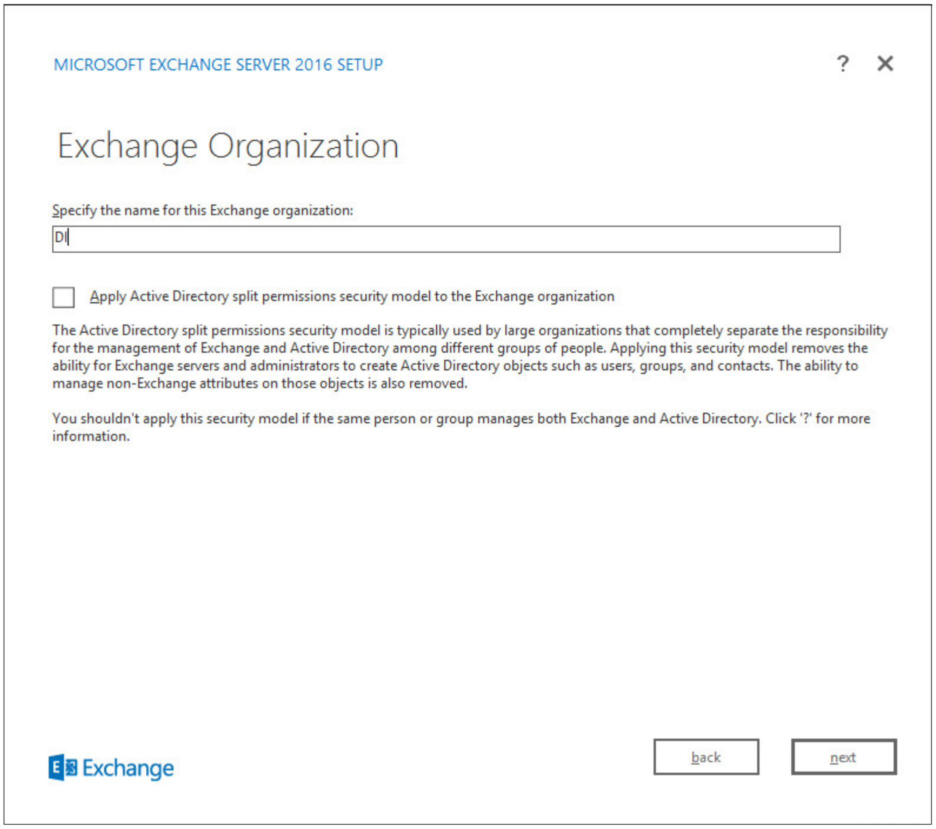
14. Click **Next.**
15. Check **Mailbox role.**
16. Check **Automatically install Windows Server roles and features that are required to install Exchange Server.**



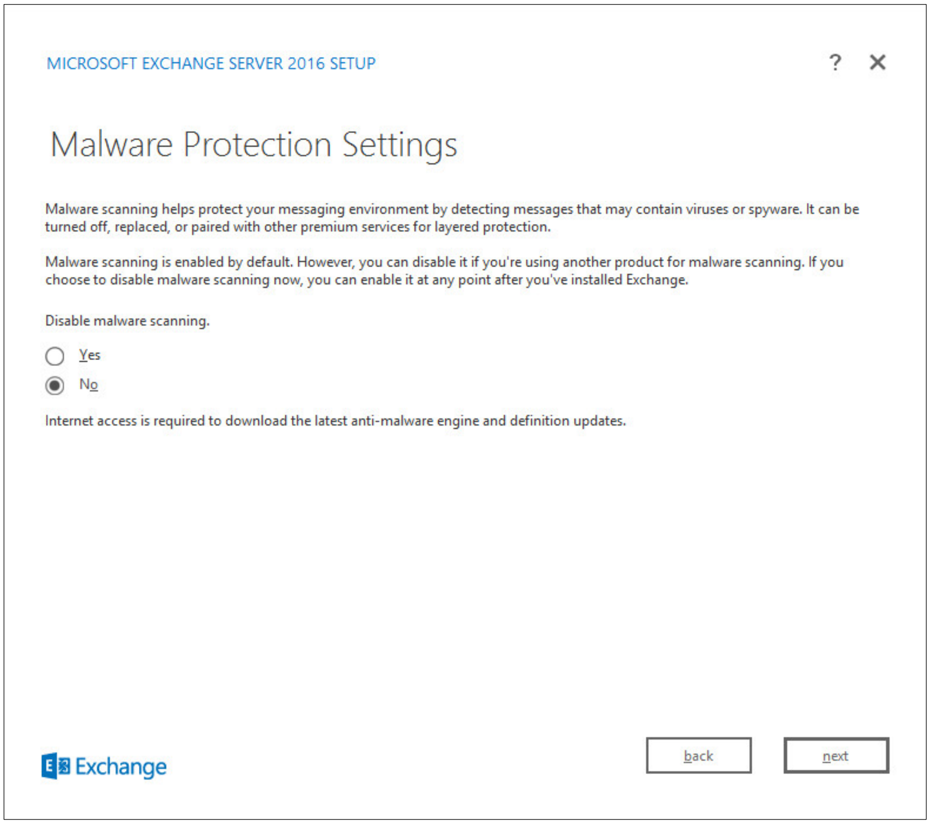
17. Click **Next.**
18. Specify the installation path for MS Exchange.



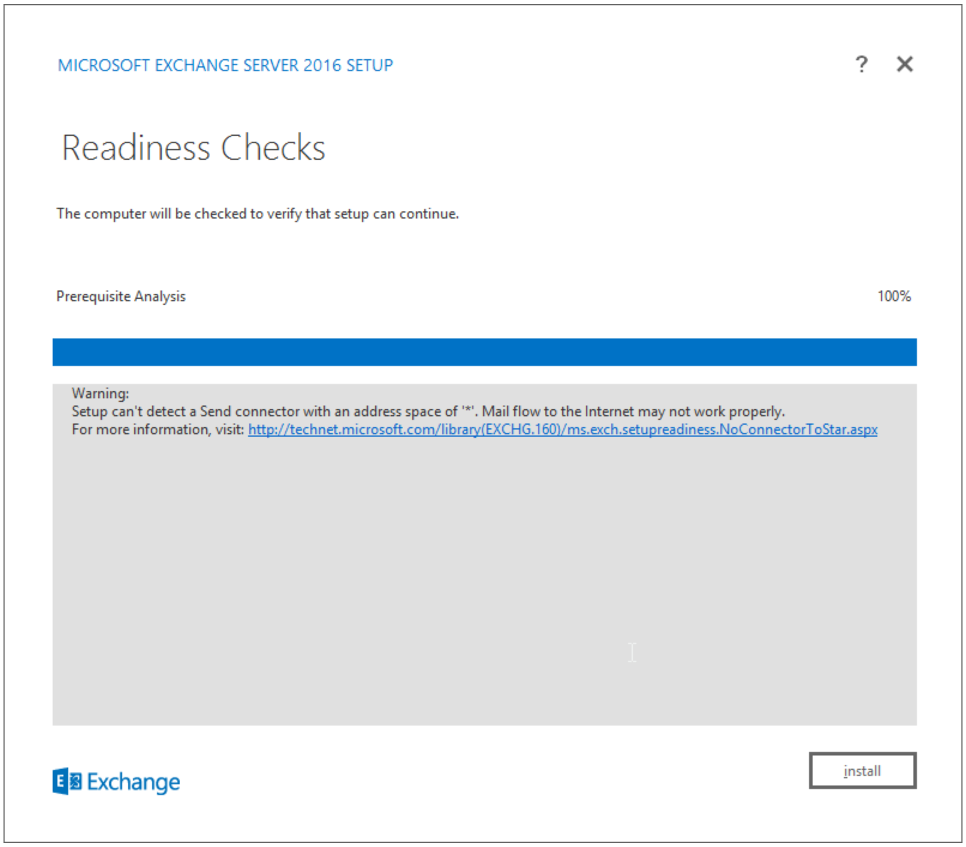
19. Click **Next.**
20. Specify the name for the Exchange organization, for example, DI.
21. Decide whether to apply split permissions, based on the needs of the enterprise.



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



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



27. Click **Install.**

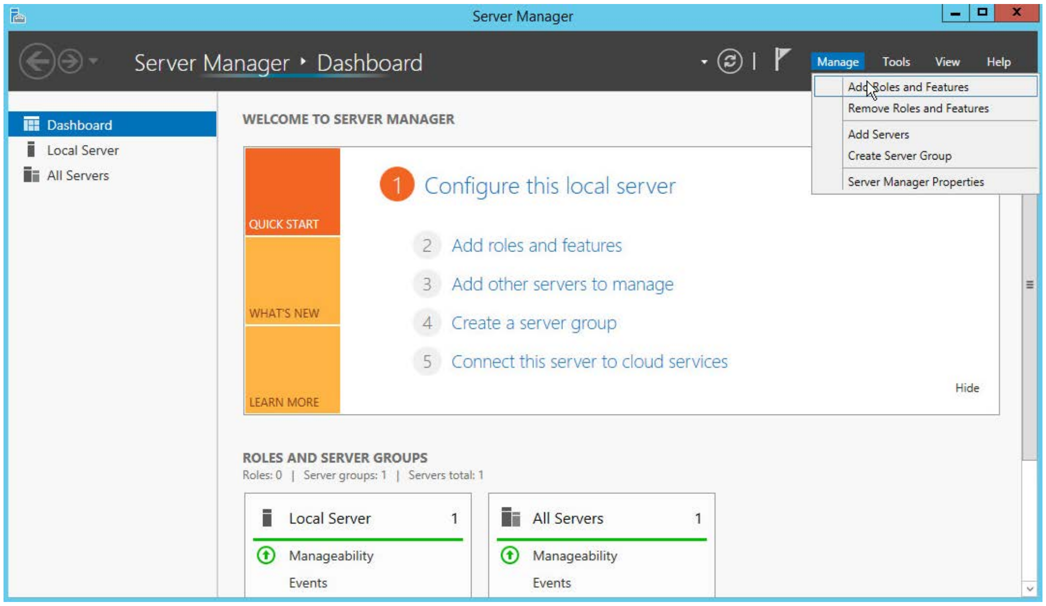
2.3 Windows Server Hyper-V Role

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

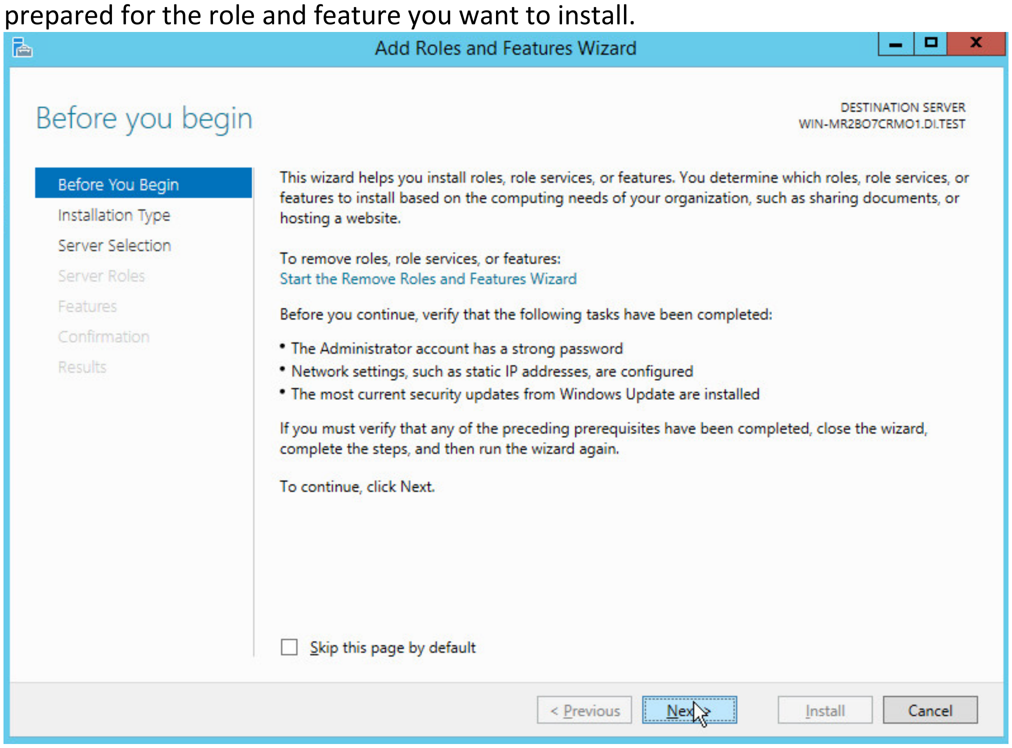
The instructions for enabling the Windows Server Hyper-V Role are retrieved from https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx and are replicated below for preservation and ease of use.

2.3.1 Production Installation

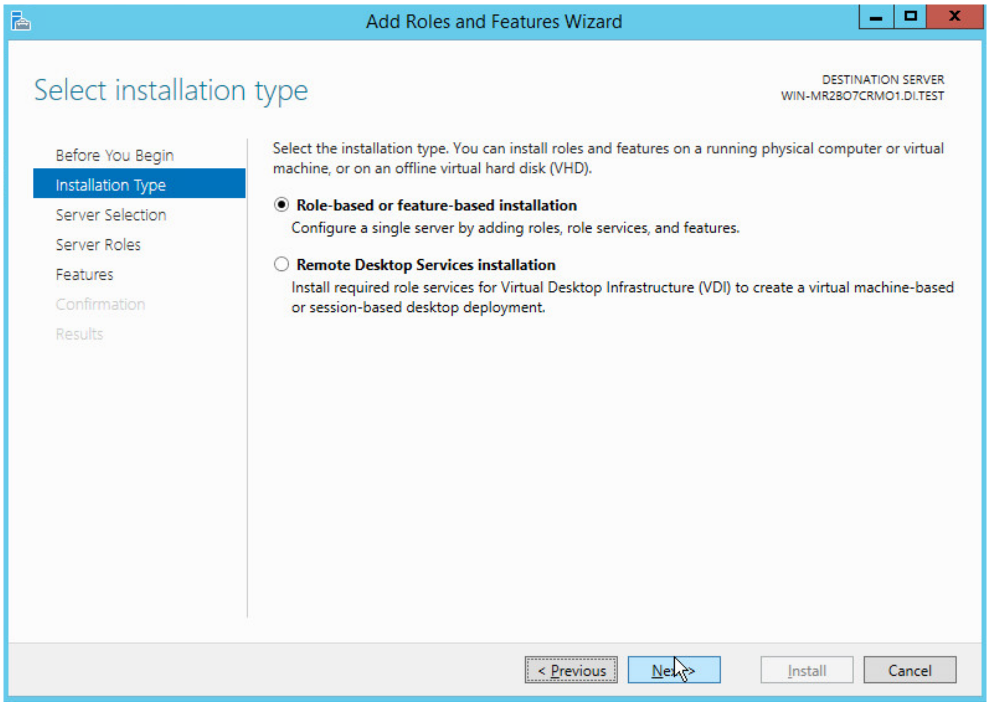
1. In **Server Manager,** on the **Manage** menu, click **Add Roles and Features.**



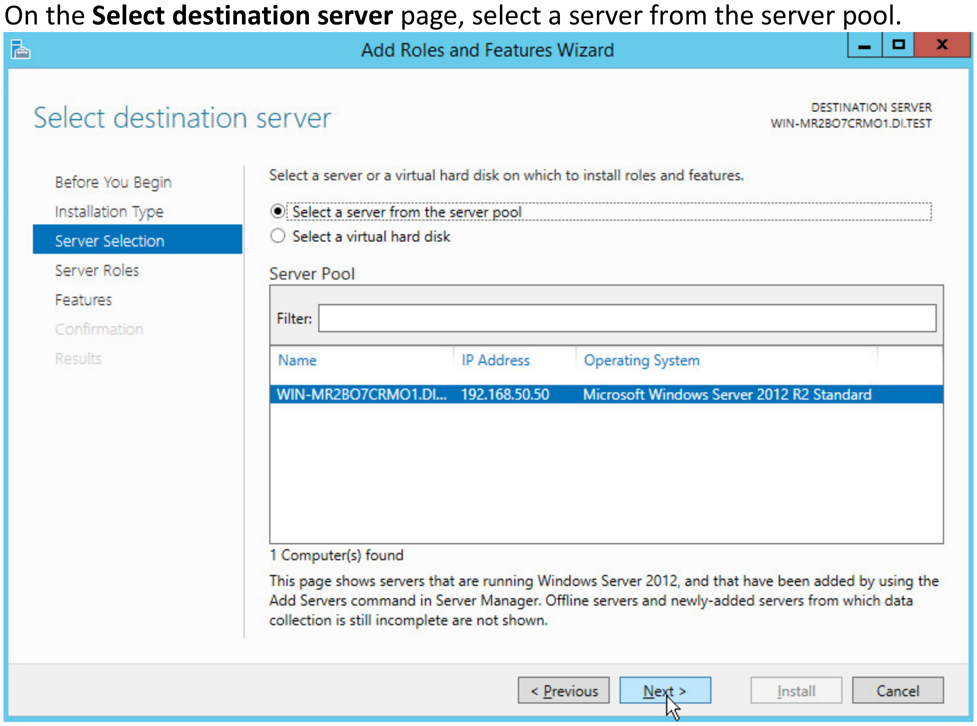
2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.



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

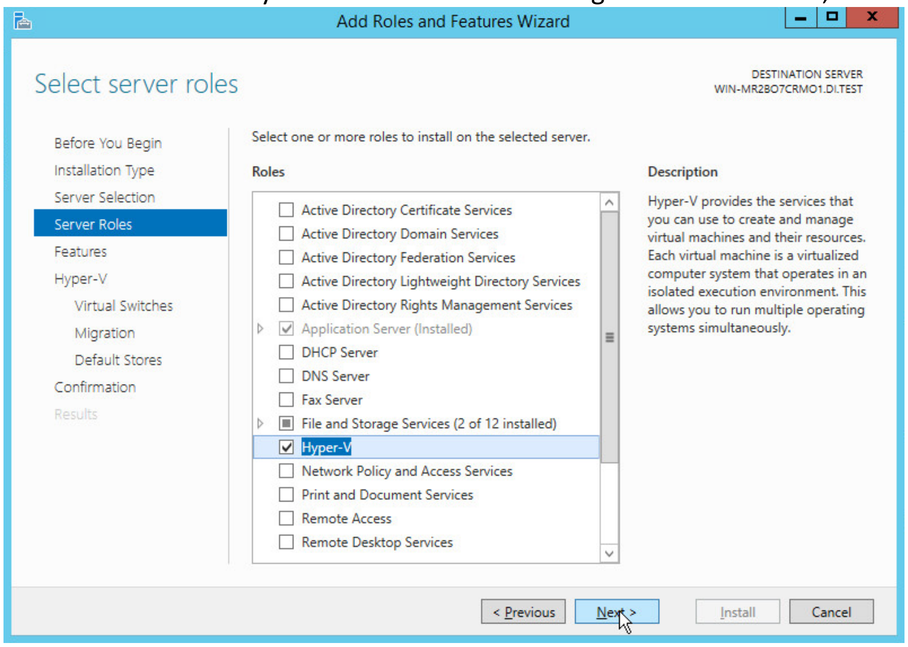


5. Click **Next.**
6. On the **Select destination server** page, select a server from the server pool.

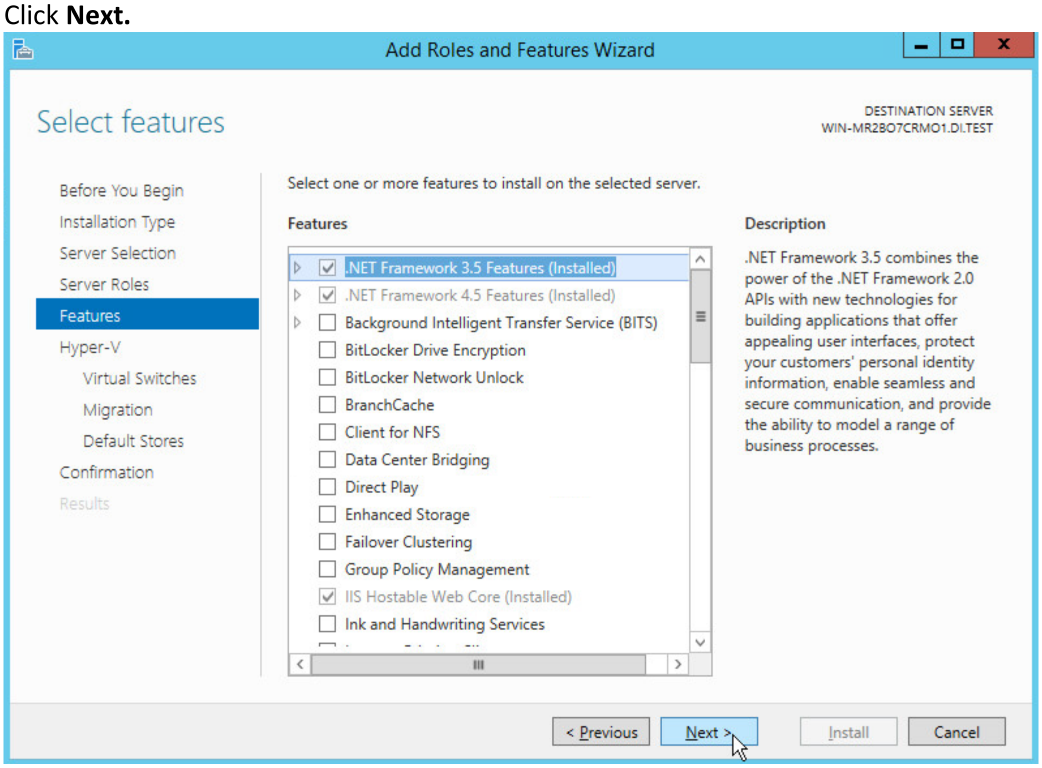


7. Click **Next.**
8. On the **Select server roles** page, select **Hyper-V.**

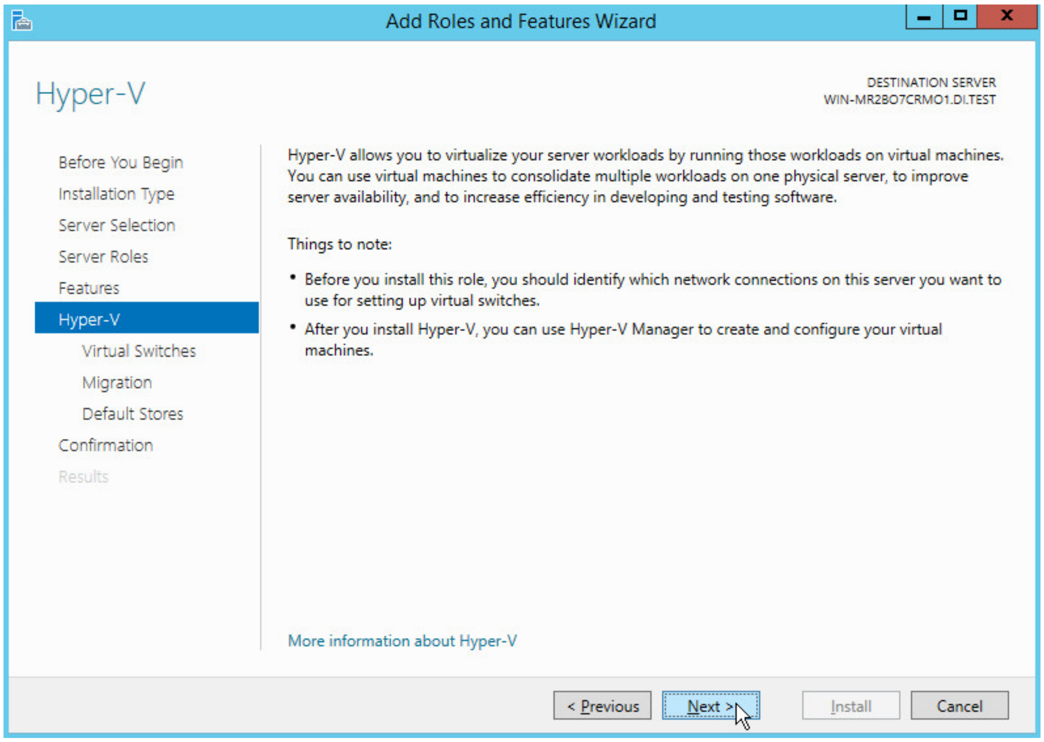
9. To add the tools that you use to create and manage virtual machines, click **Add Features.**



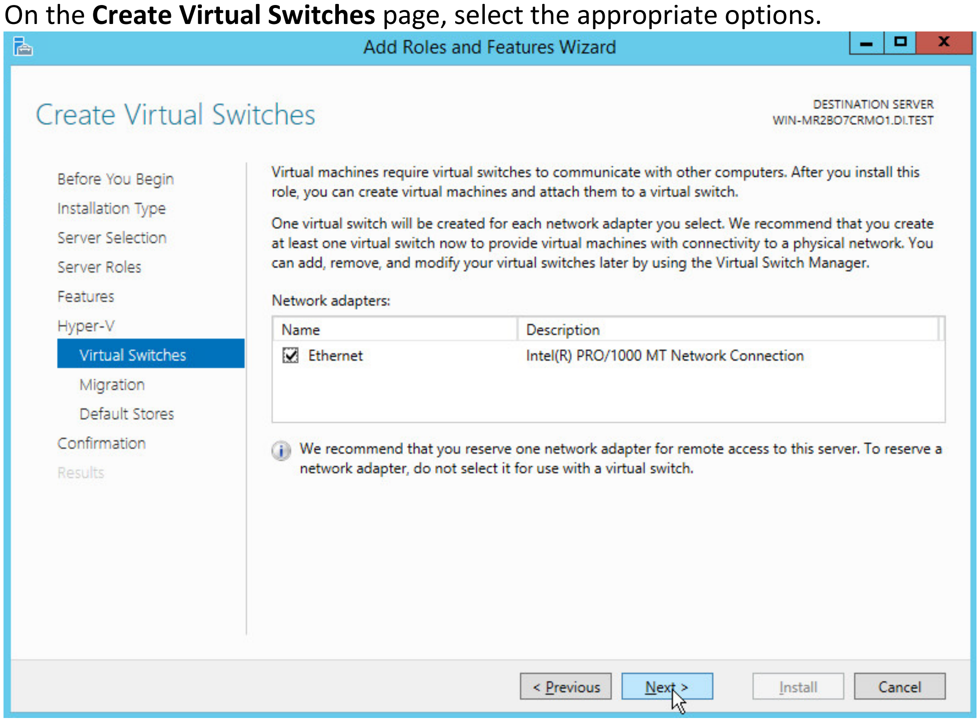
10. Click **Next.**



11. Click **Next.**

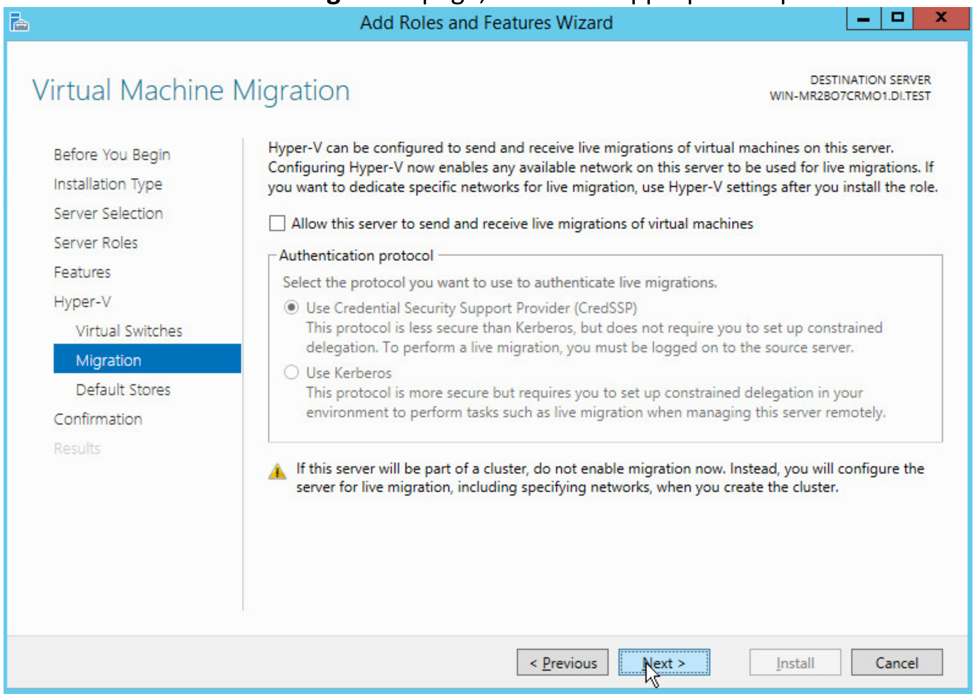


12. Click **Next.**
13. On the **Create Virtual Switches** page, select the appropriate options.



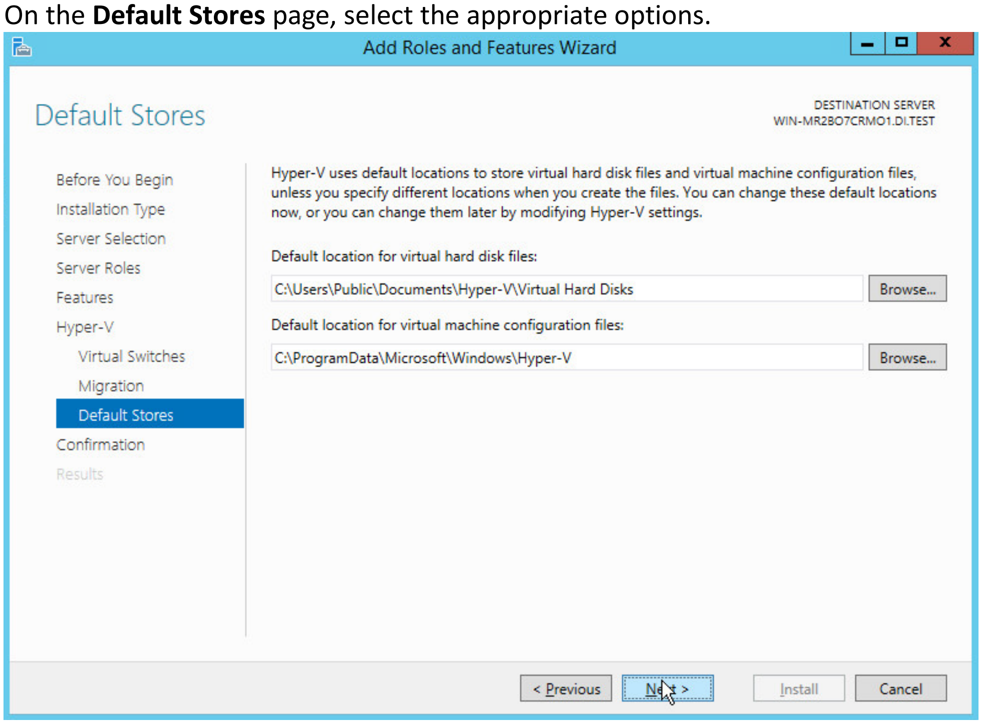
14. Click **Next.**

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



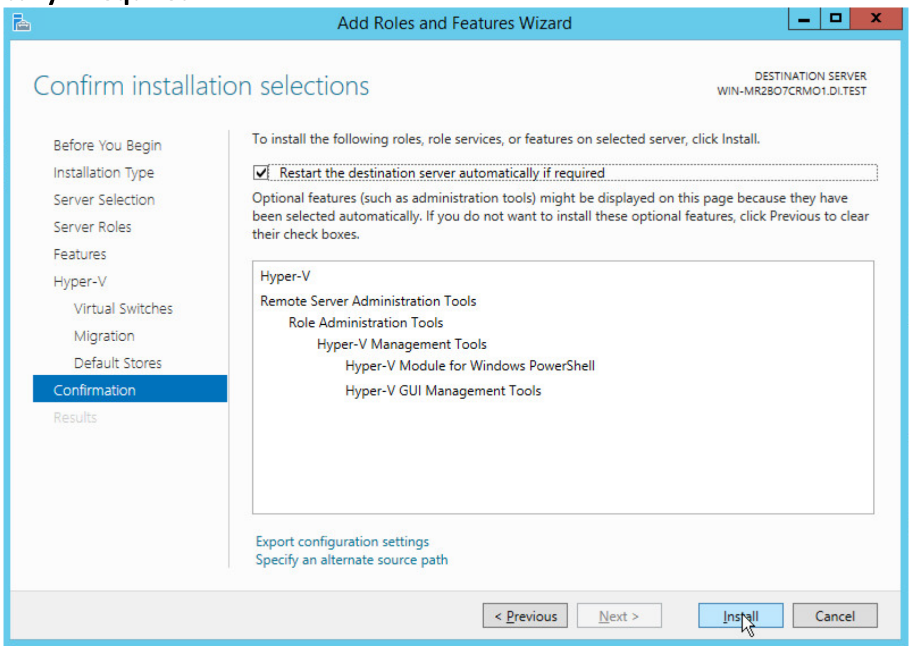
16. Click **Next.**

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.**



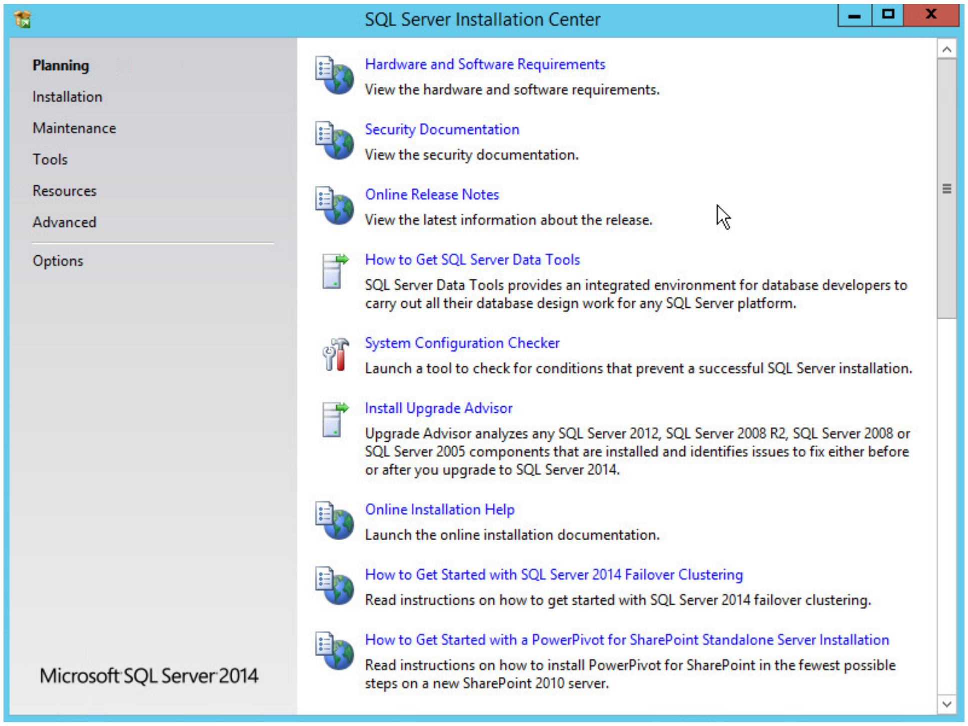
20. Click **Install.**
21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

2.4 MS SQL Server

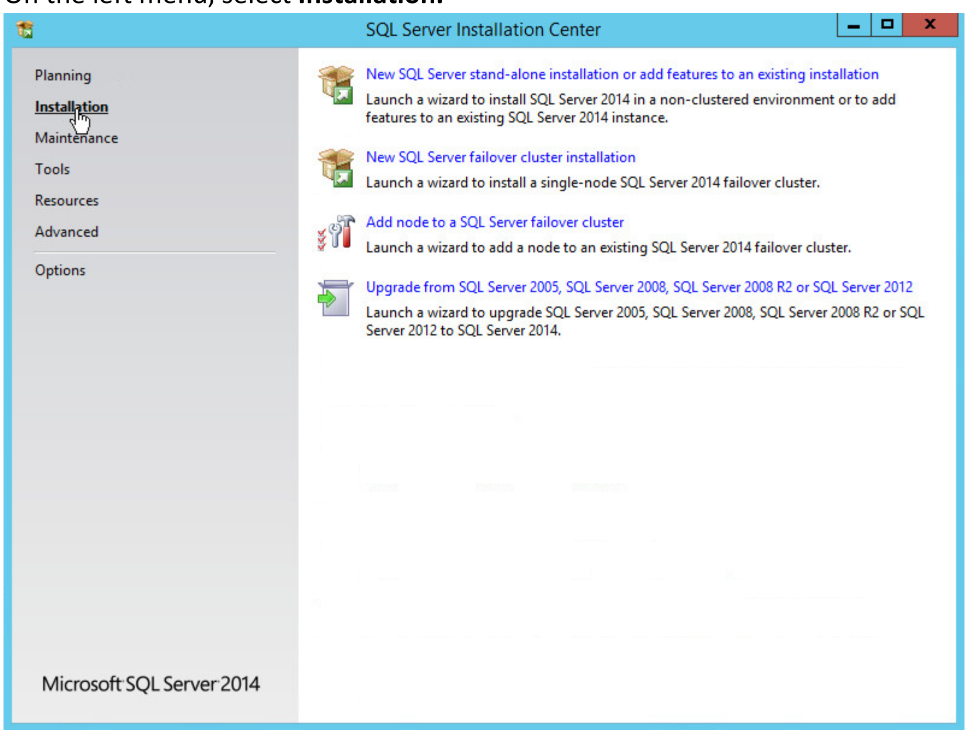
As part of both our enterprise emulation and data integrity solution, we include a Microsoft SQL Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

2.4.1 Install and Configure MS SQL

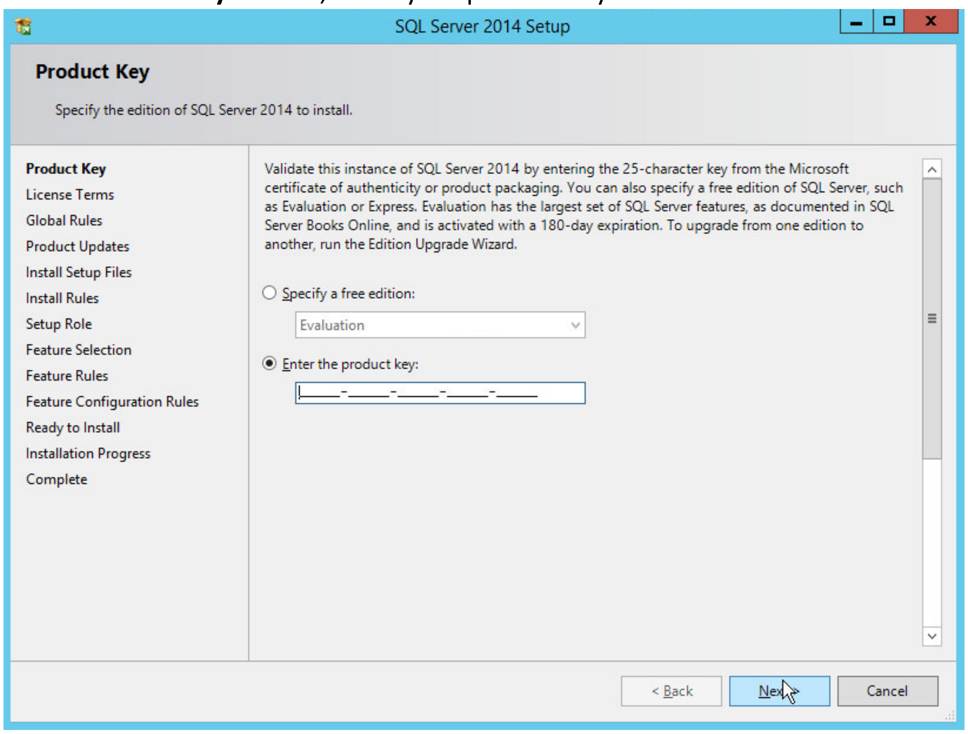
1. Acquire **SQL Server 2014 Installation Media.**
2. Locate the installation media in the machine and click on **SQL2014_x64_ENU** to launch **SQL Server Installation Center.**



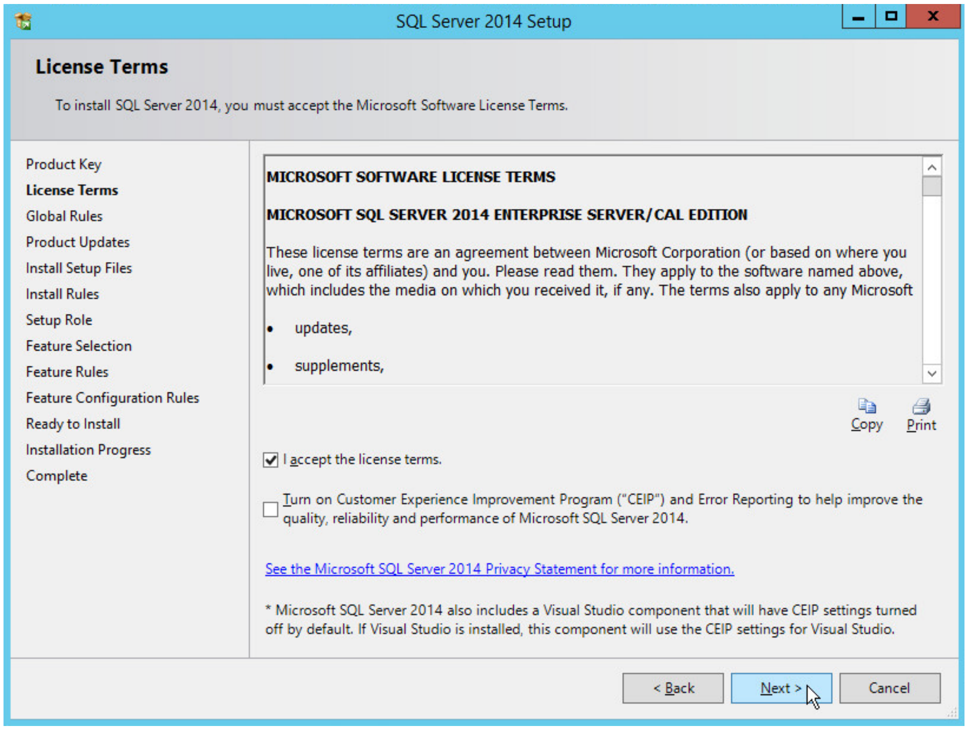
3. On the left menu, select **Installation.**



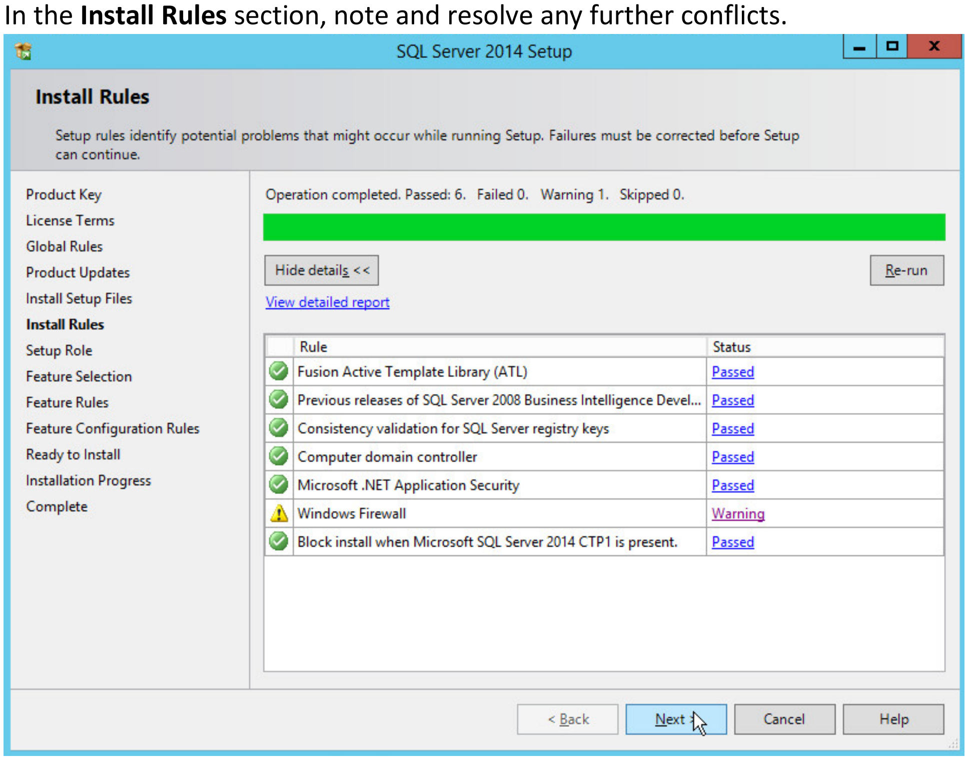
4. Select **New SQL Server stand-alone installation or add features to an existing installation.** This will launch the SQL Server 2014 setup.
5. In the **Product Key** section, enter your product key.



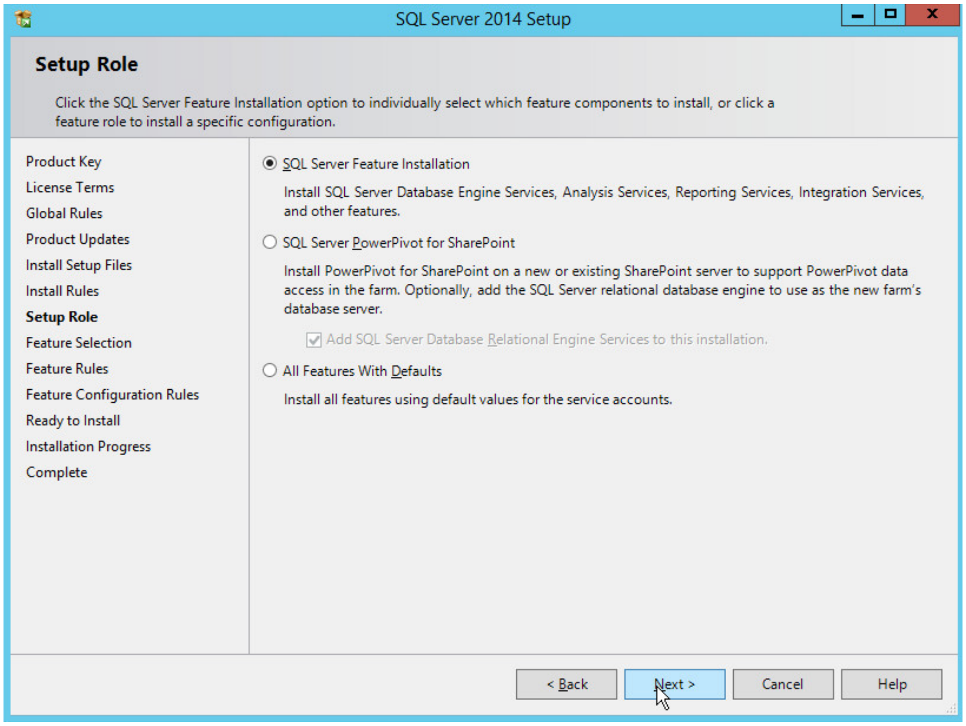
6. Click **Next.**
7. In the **License Terms** section, read and click **I accept the license terms.**



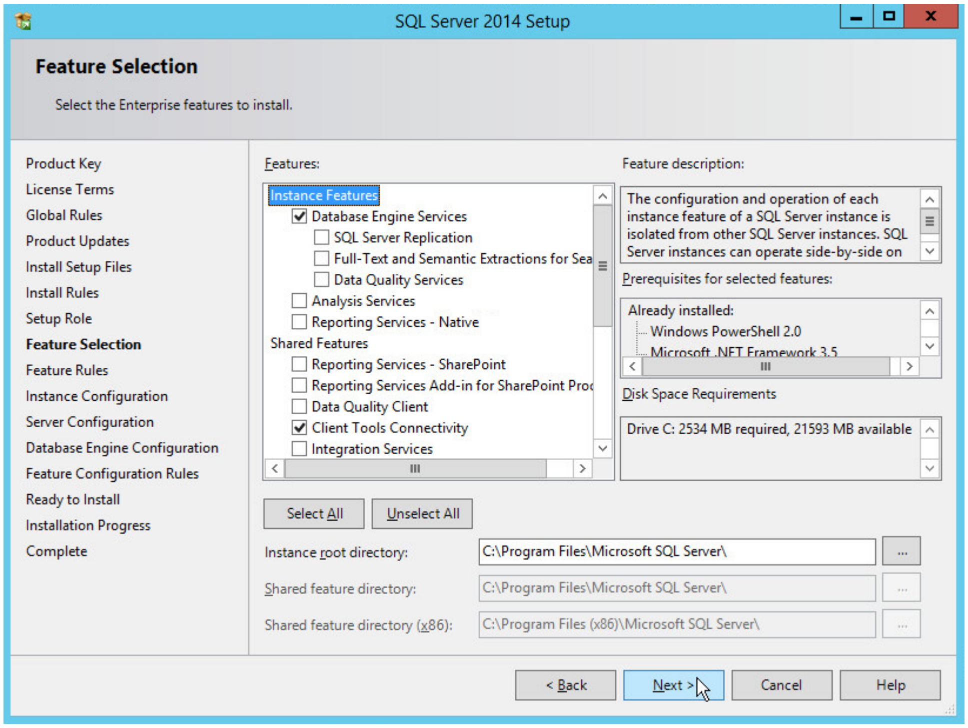
8. Click **Next.**
9. In the **Install Rules** section, note and resolve any further conflicts.



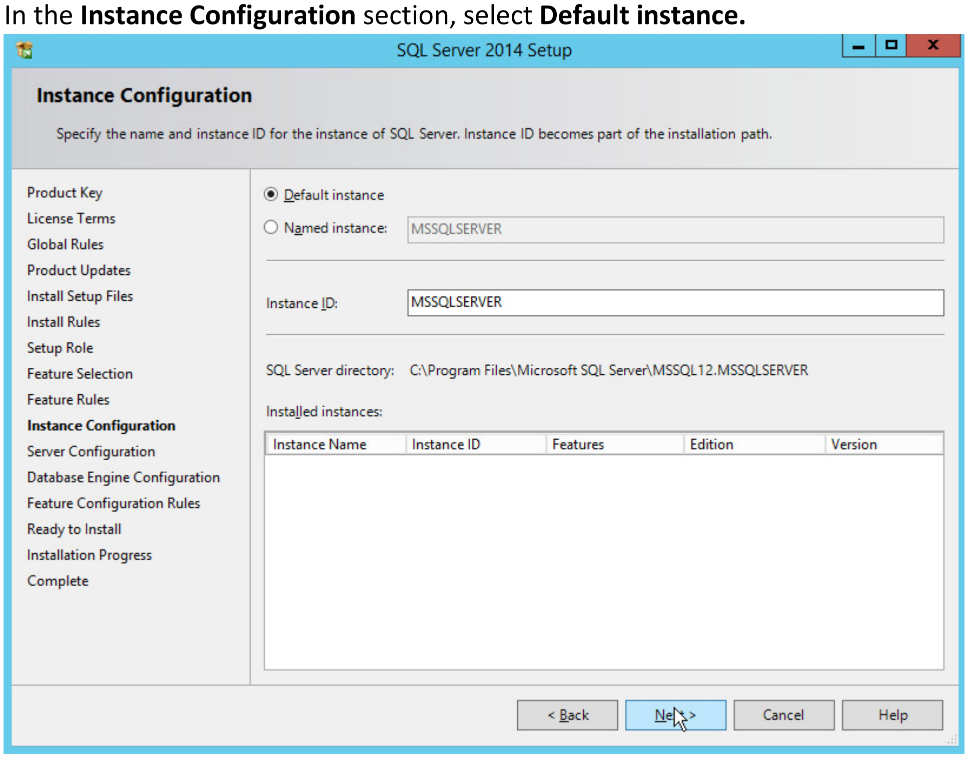
10. Click **Next.**
11. In the **Setup Role** section, select **SQL Server Feature Installation.**



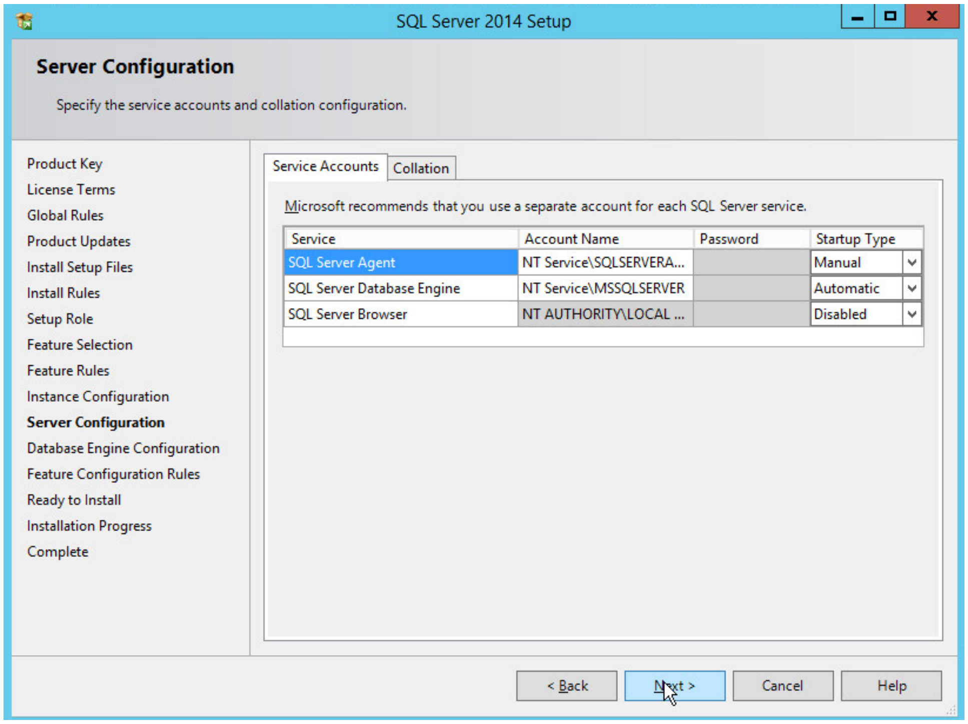
12. Click **Next.**
13. In the **Feature Selection** section, select the following:
    a. **Database Engine Services**
    b. **Client Tools Connectivity**
    c. **Client Tools Backwards Compatibility**
    d. **Client Tools SDK**
    e. **Management Tools – Basic**
    f. **Management Tools – Complete**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



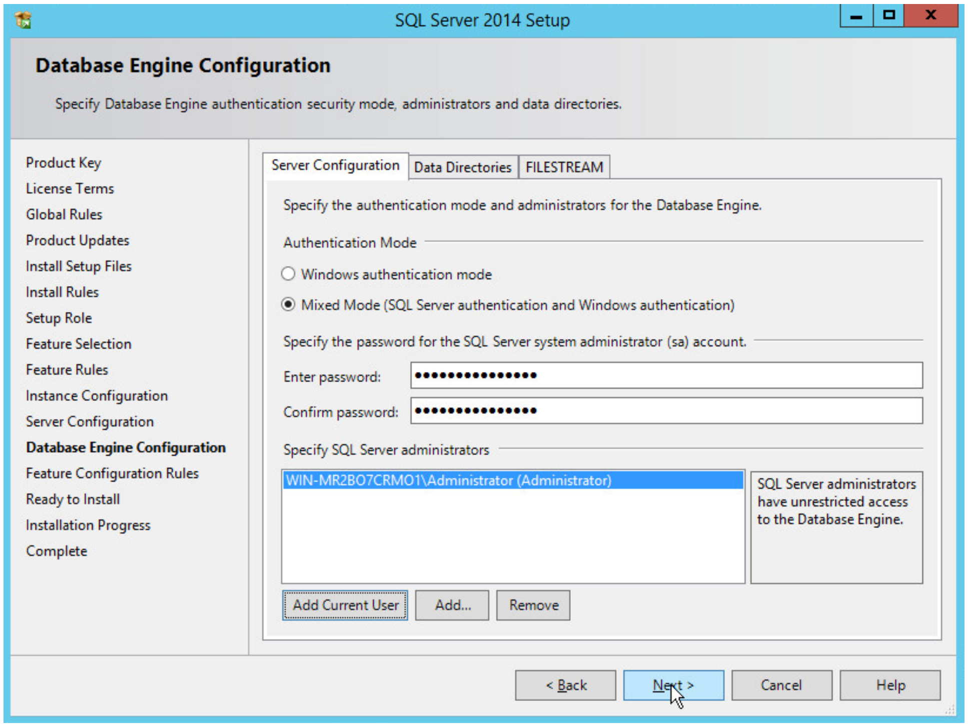
14. Click **Next.**
15. In the **Instance Configuration** section, select **Default instance.**



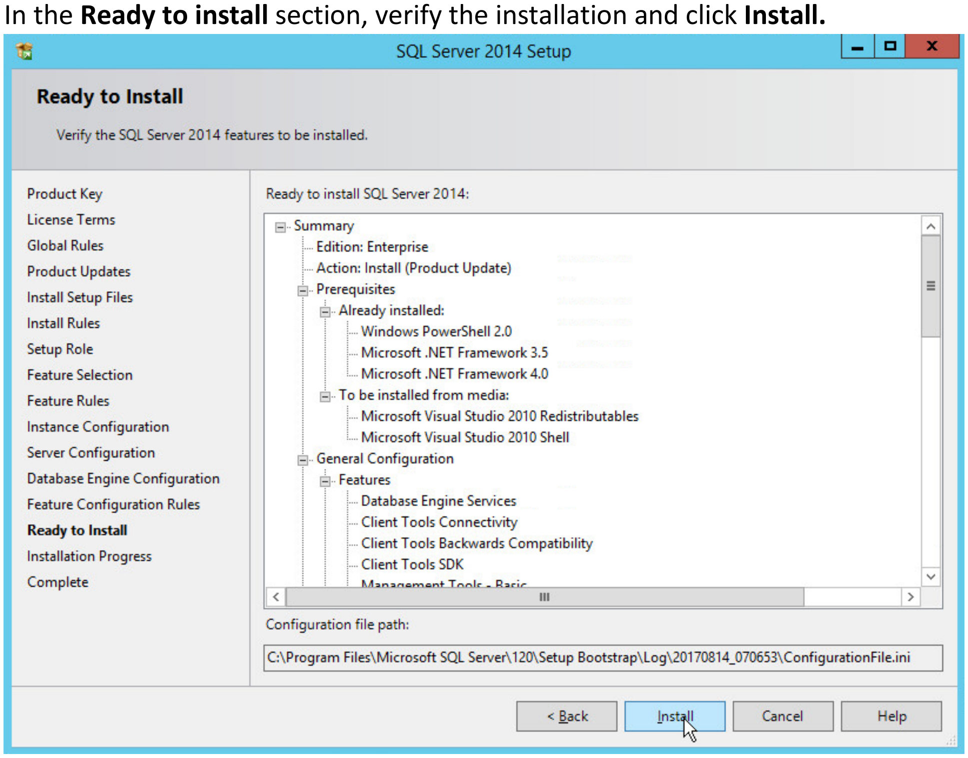
16. Click **Next.**



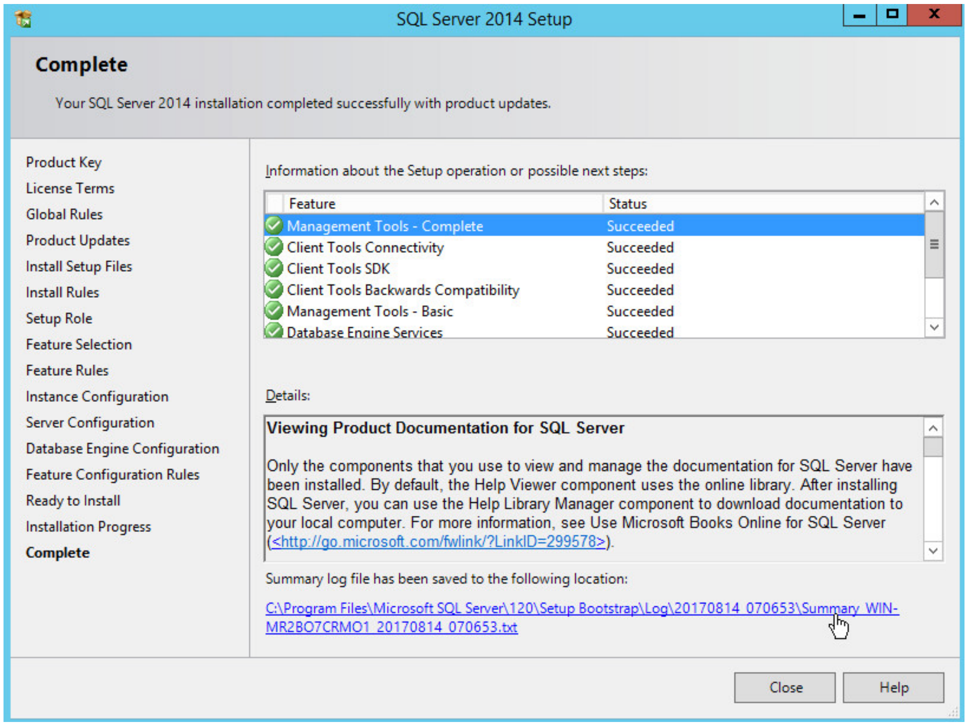
17. In the **Server Configuration** section, click **Next.**
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.
19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User.**
    a. For Domain accounts,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



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



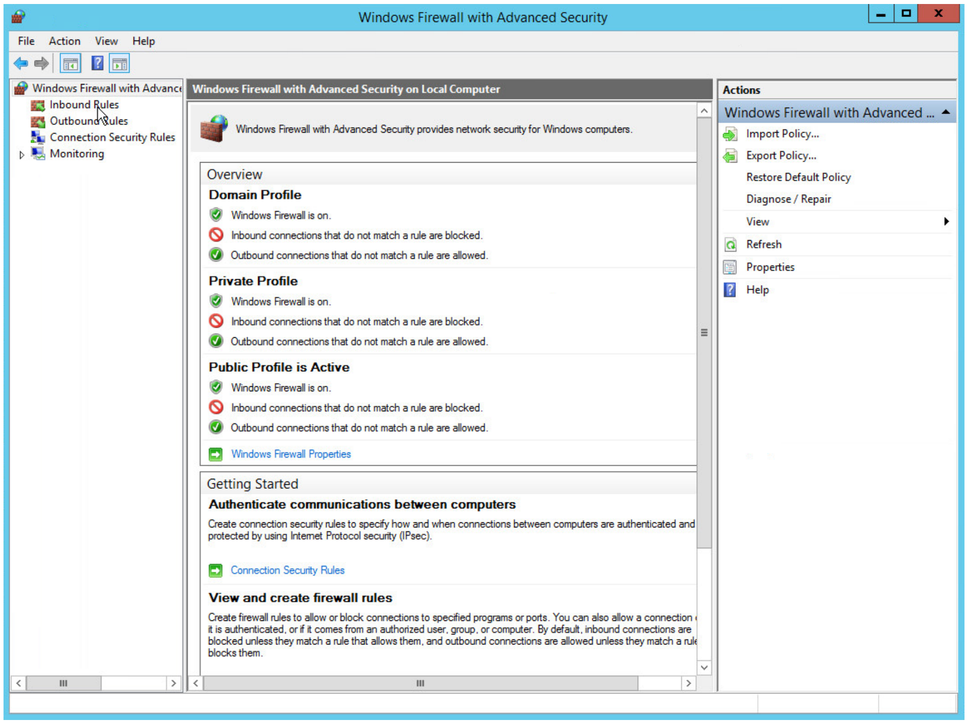
21. Wait for the install to finish.



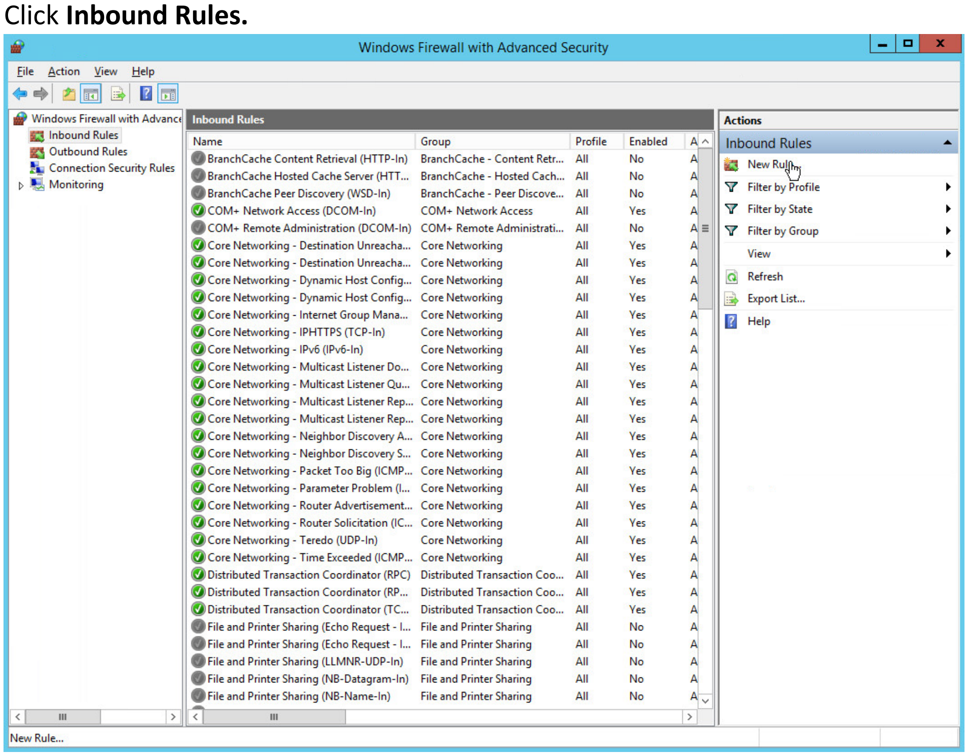
22. Click **Close.**

2.4.2 Open Port on Firewall

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

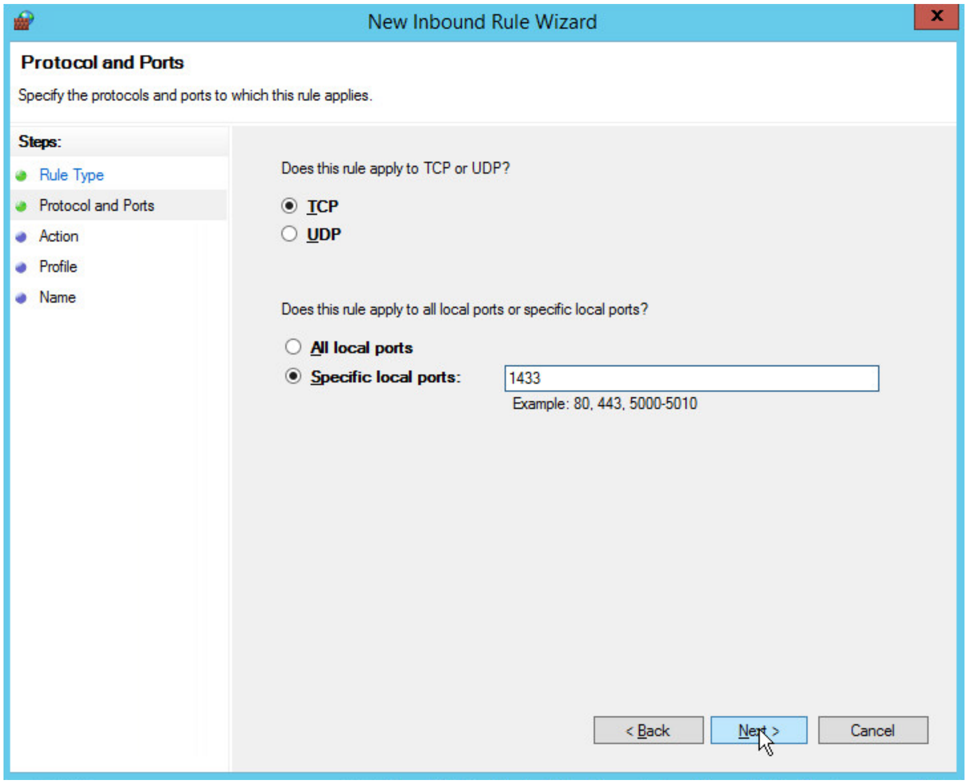


2. Click **Inbound Rules.**

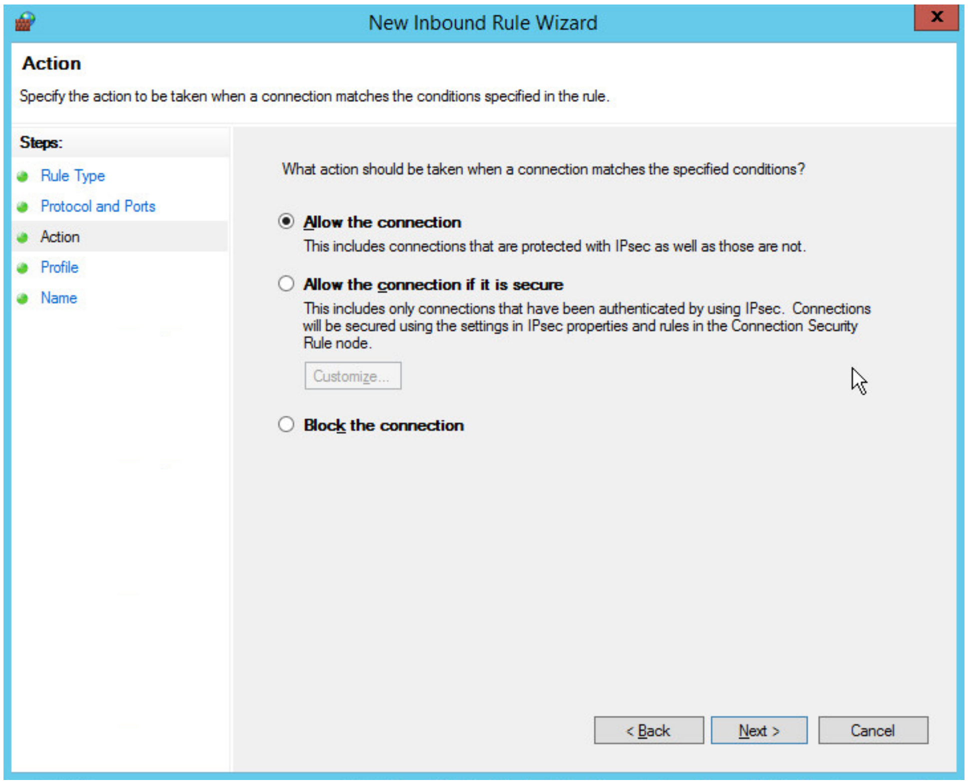


3. Click **New Rule.**

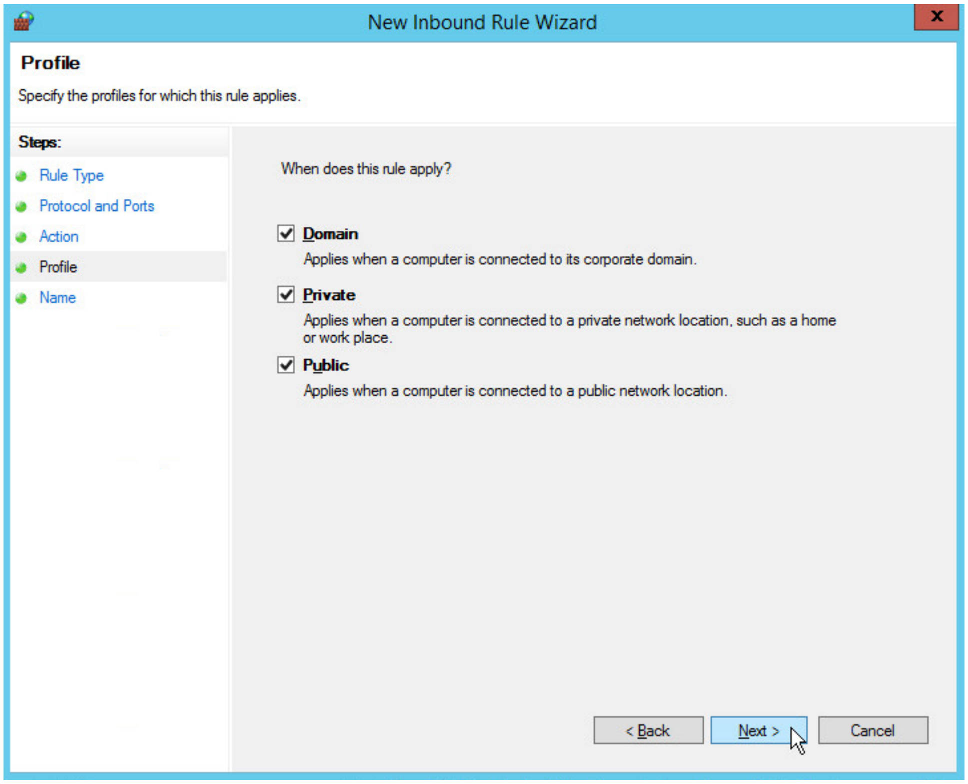
4. Select **Port.**
5. Click **Next.**
6. Select **TCP** and **Specific local ports.**
7. Type **1433** into the text field.



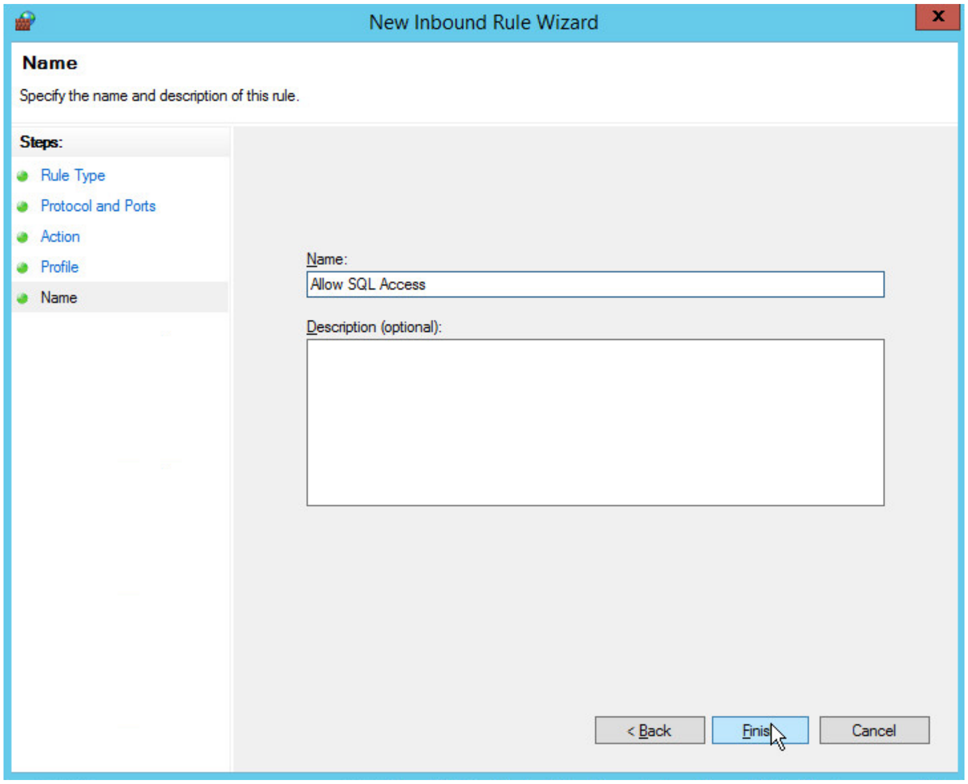
8. Click **Next.**
9. Select **Allow the connection.**



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



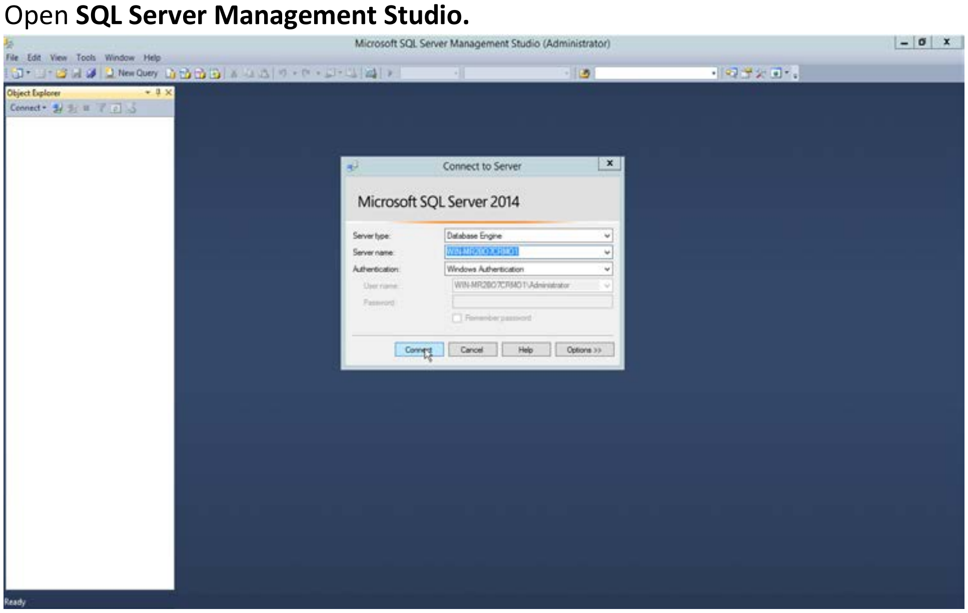
12. Click **Next.**
13. Name the rule **Allow SQL Access.**



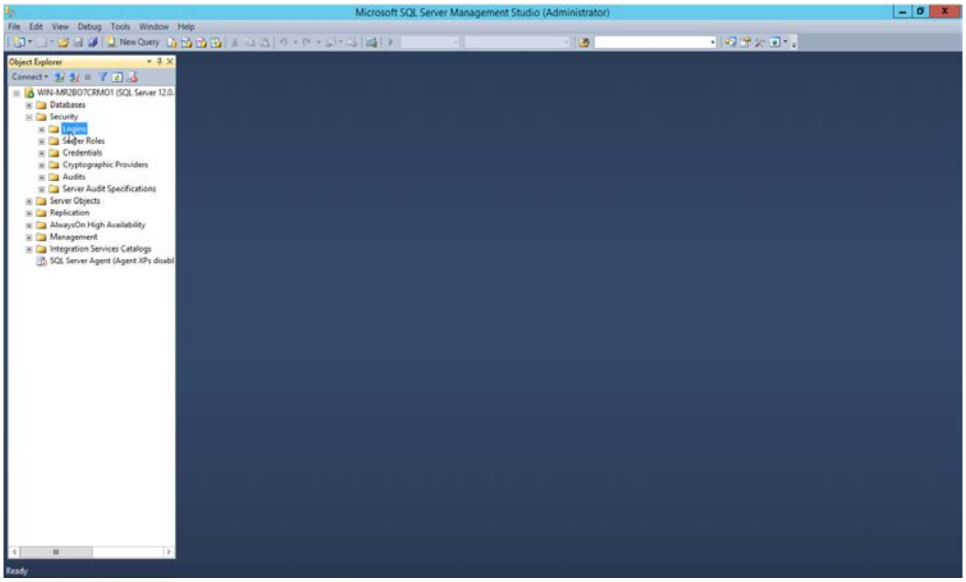
14. Click **Finish.**

2.4.3 Add a New Login to the Database

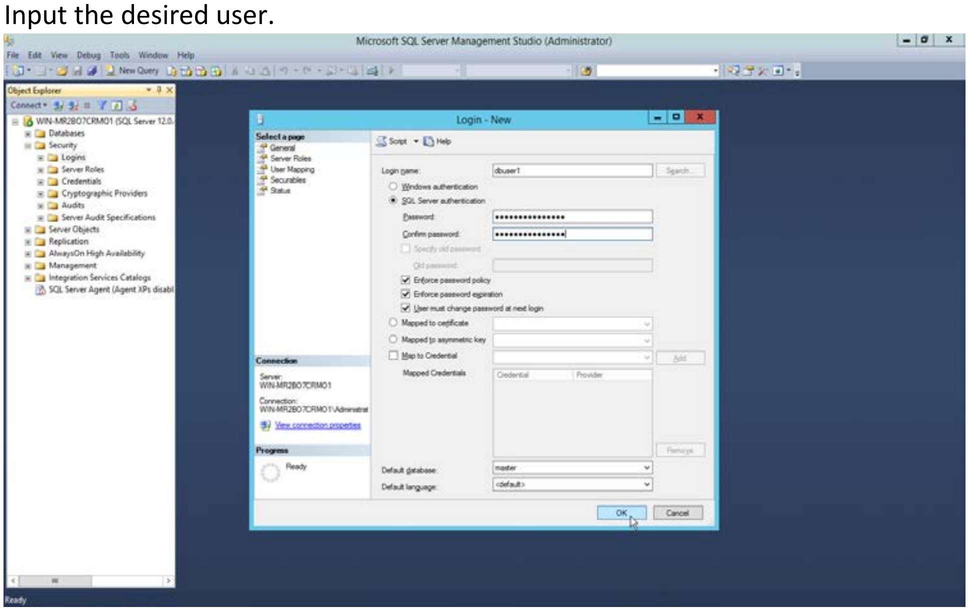
1. Open **SQL Server Management Studio.**



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.



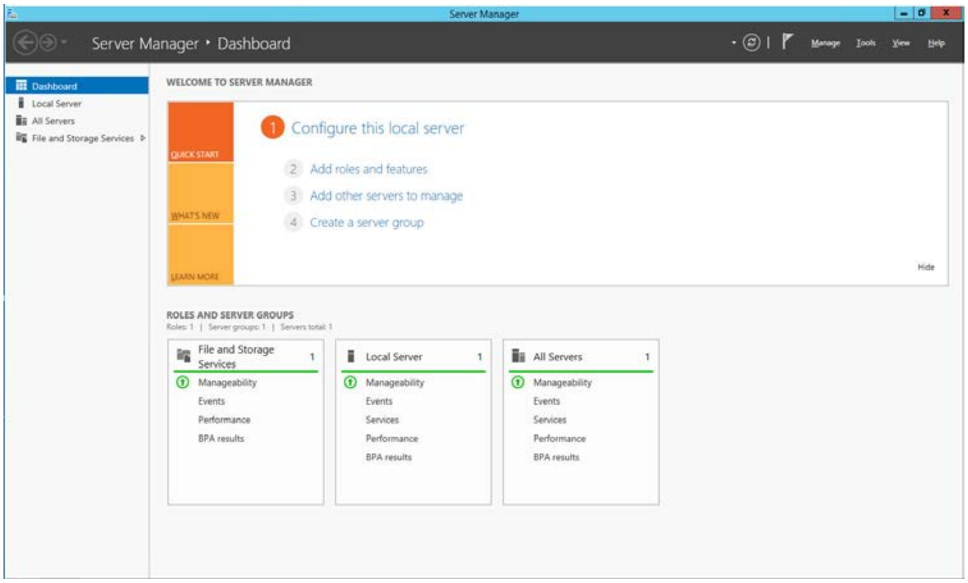
6. Click **OK.**

2.5 Microsoft IIS Server

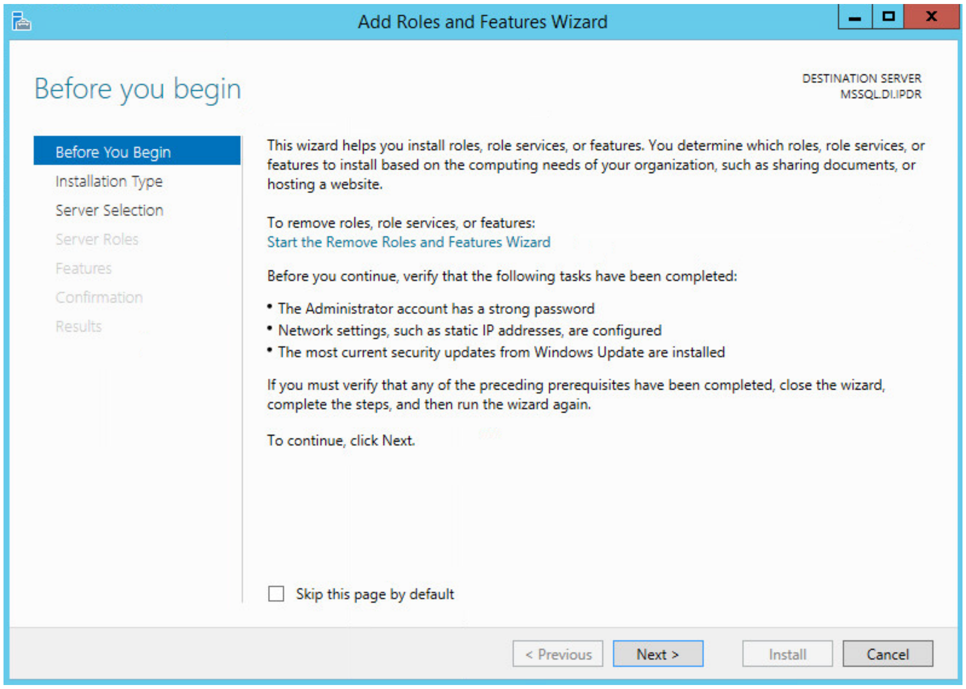
As part of our enterprise emulation, we include a Microsoft IIS server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine. This was conducted on the same machine as section 2.4.

2.5.1 Install IIS

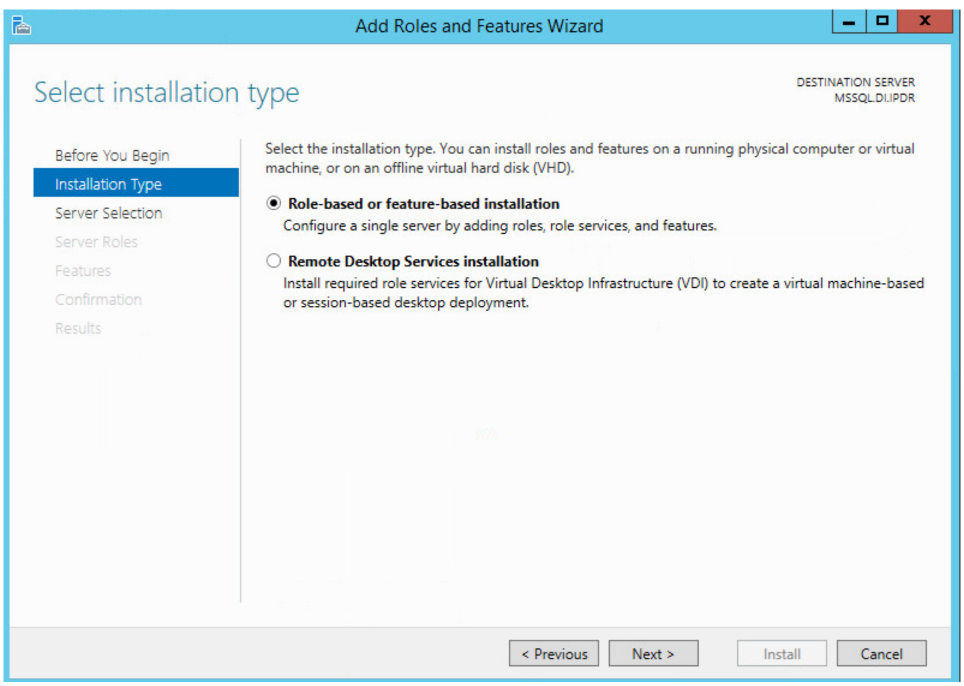
1. Open **Server Manager.**



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

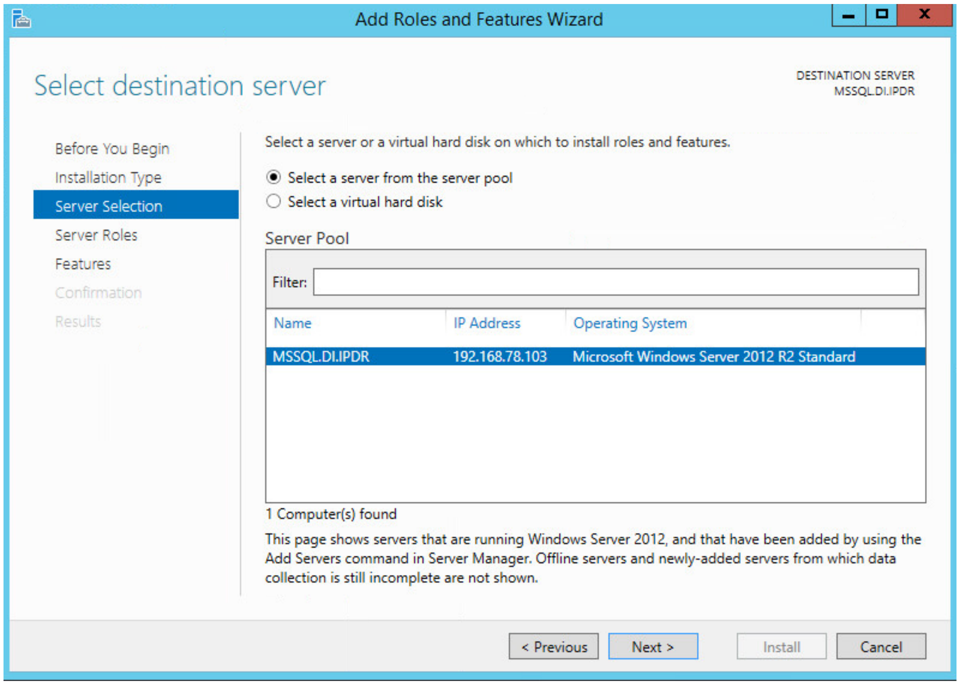


3. Click **Next.**
4. Select **Role-based or feature-based installation.**

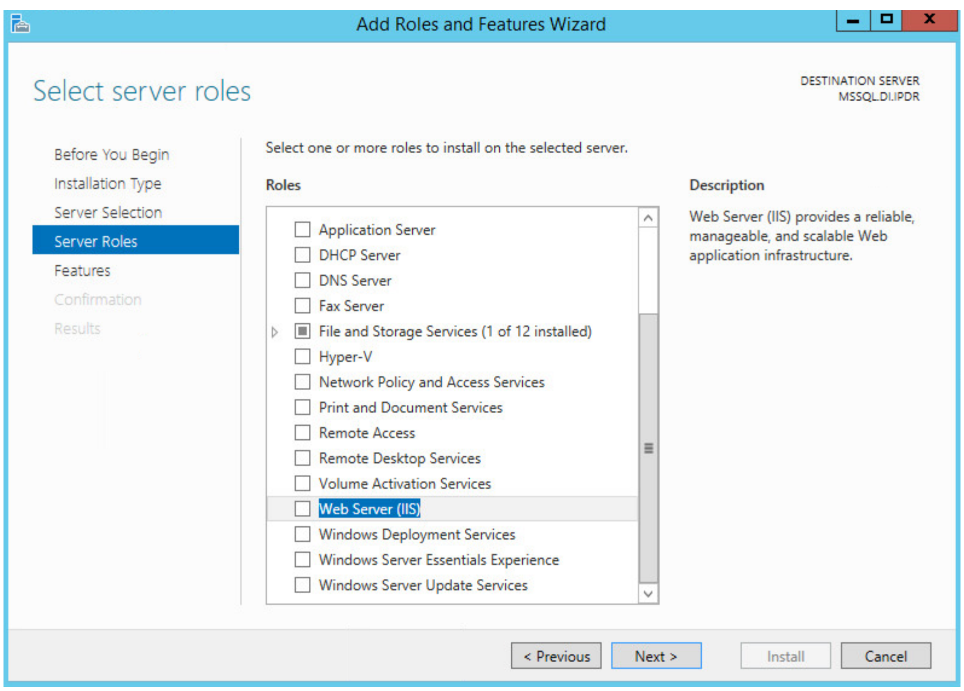


5. Click **Next.**

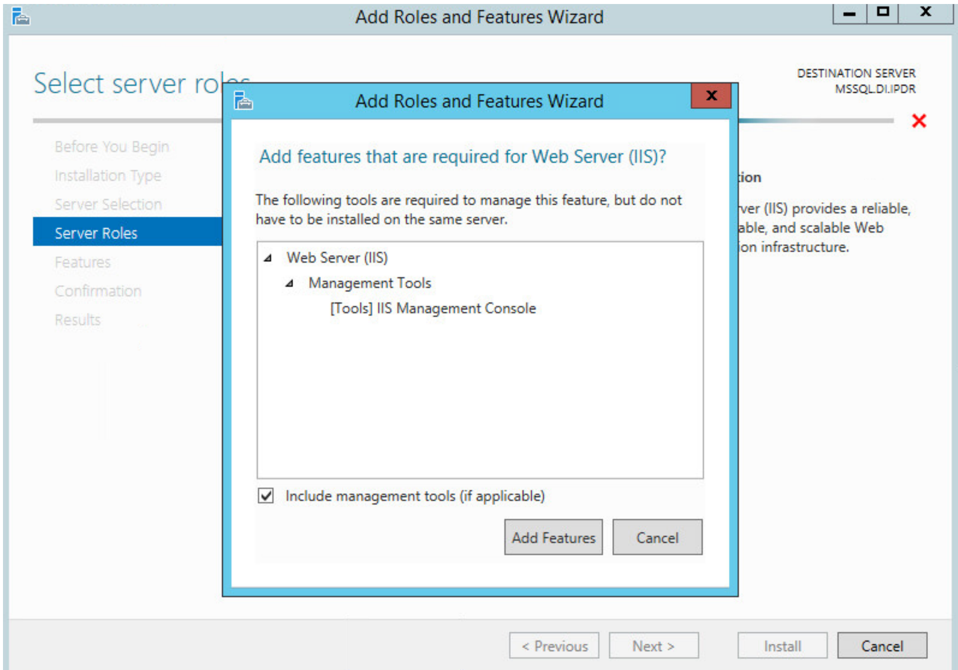
6. Select **MSSQL** (or the correct Windows Server name) from the list.



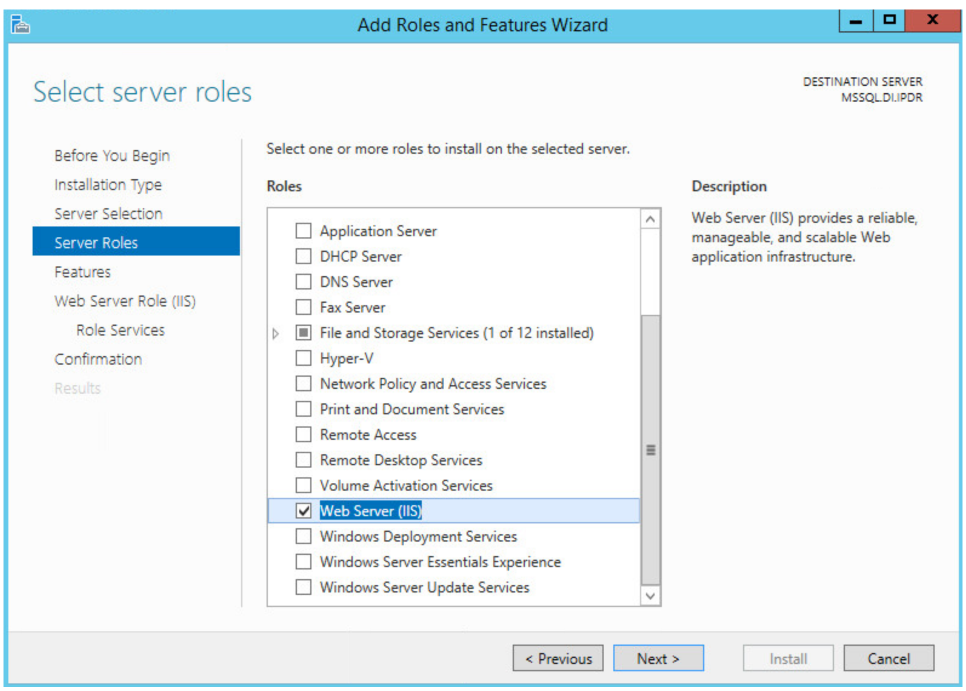
7. Click **Next.**



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

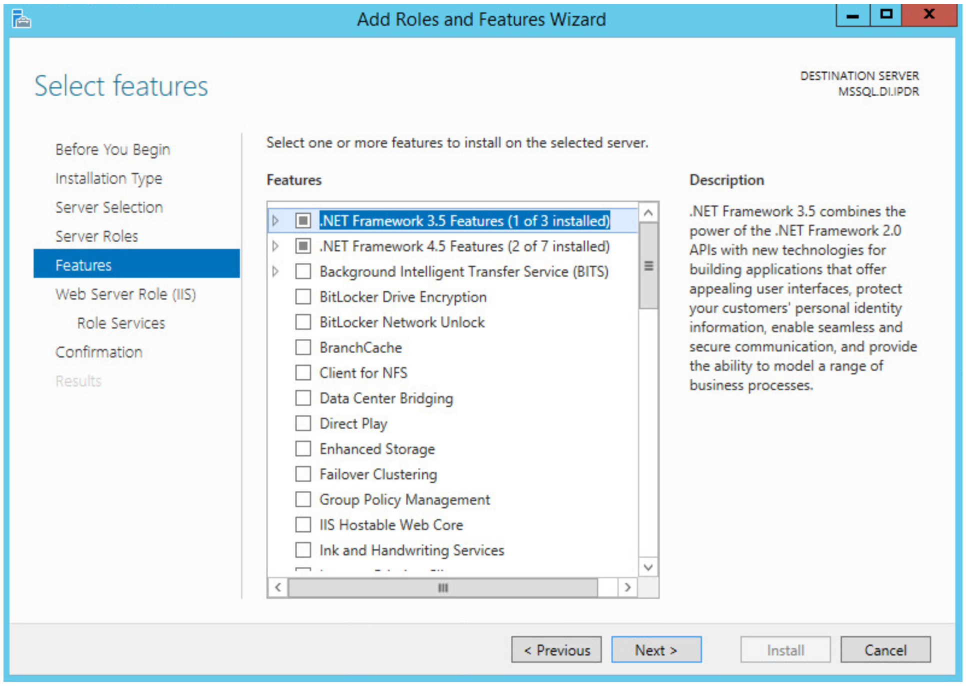


9. Click **Add Features.**

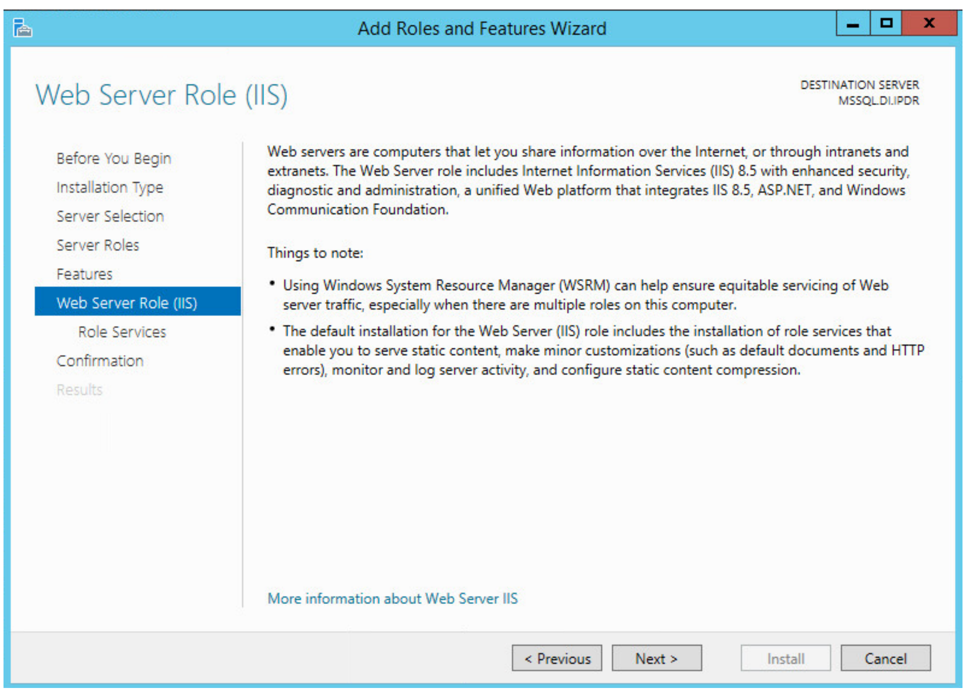


10. Click **Next.**

11. Ensure that all desired features are selected.

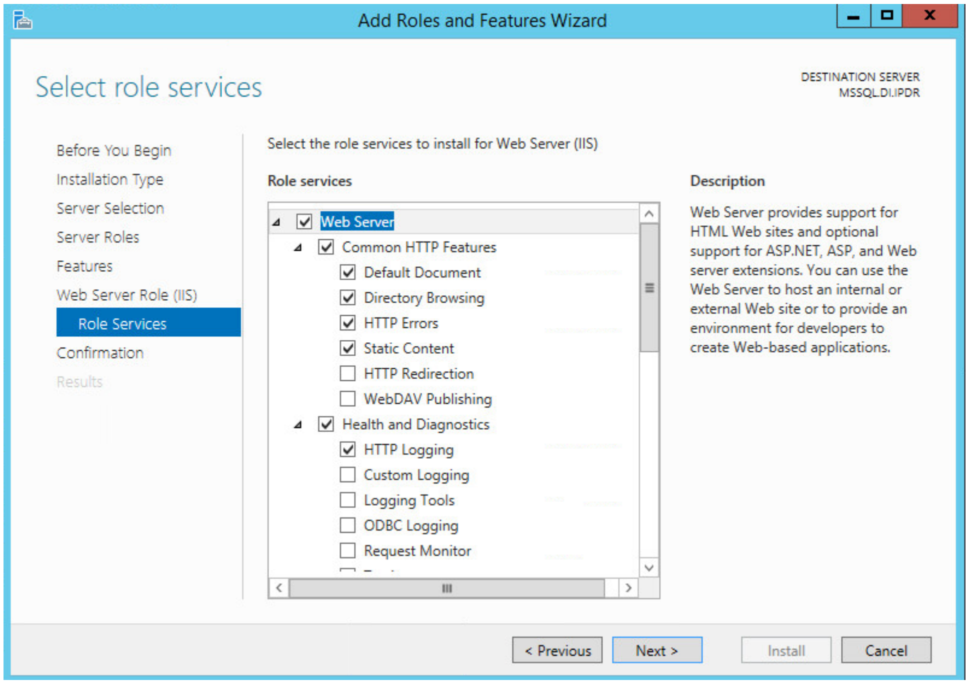


12. Click **Next.**

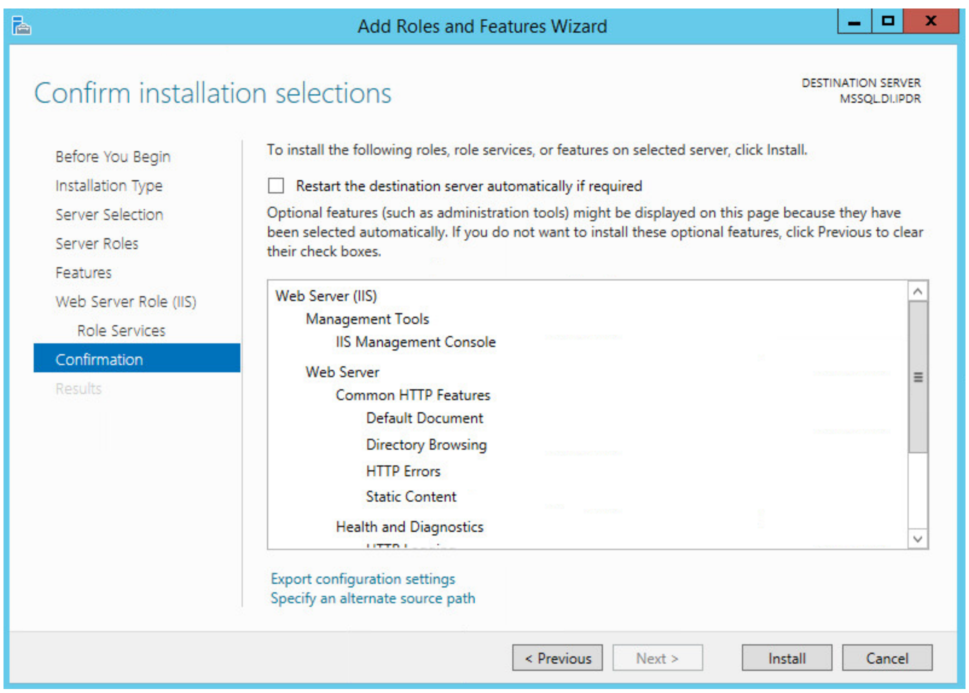


13. Click **Next.**

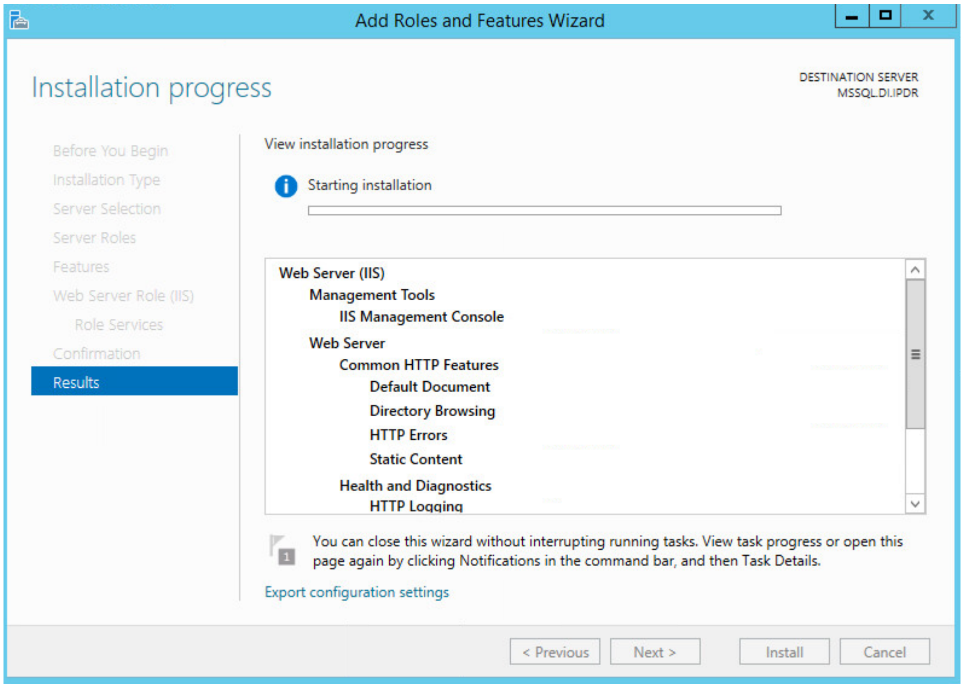
14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging,** and any other desired Role services are selected.



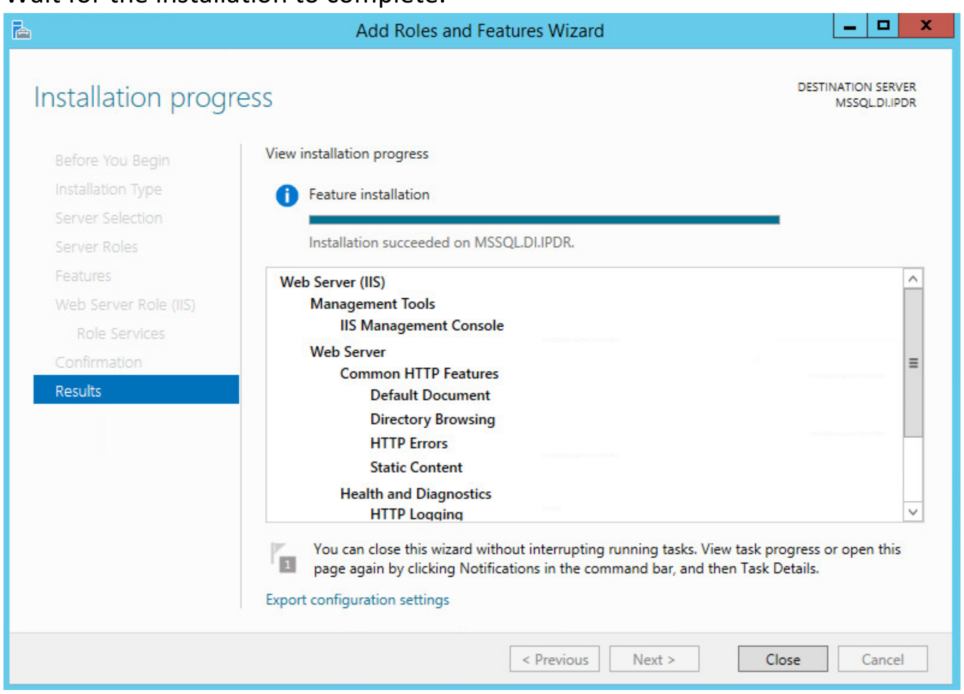
15. Click **Next.**



16. Click **Install.**



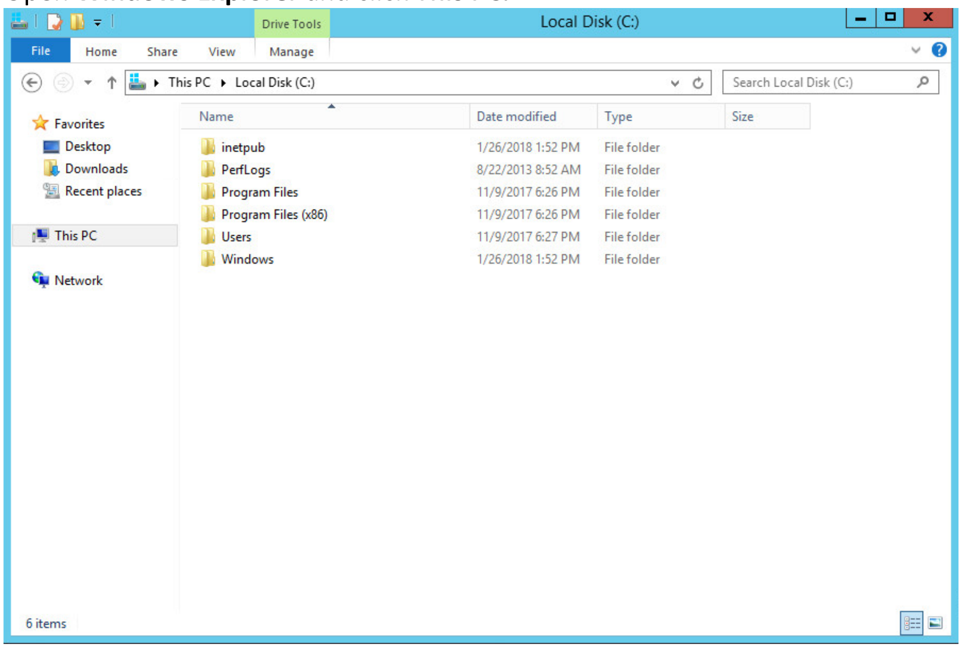
17. Wait for the installation to complete.



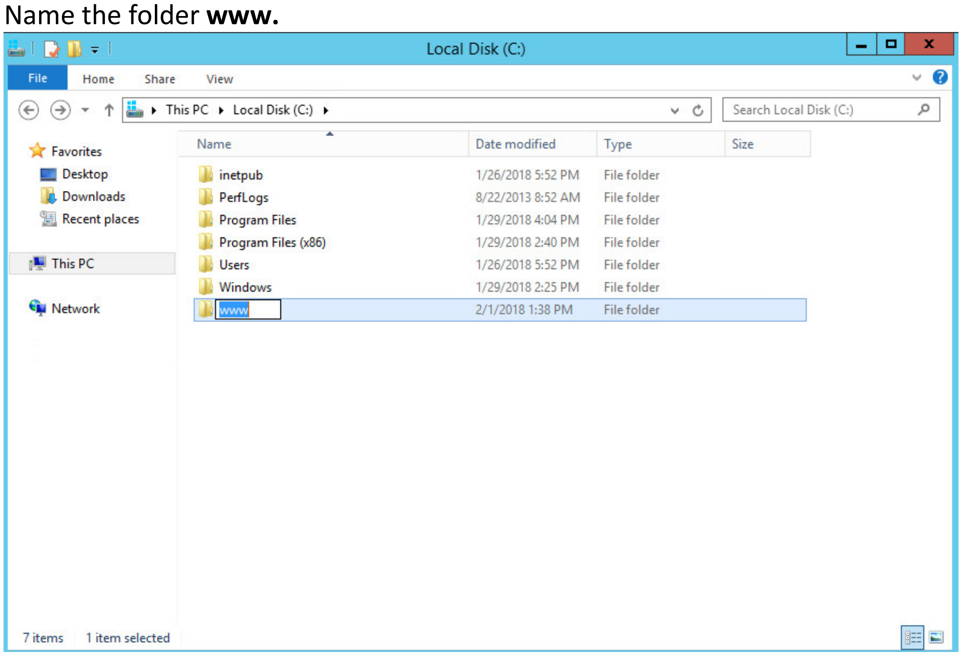
18. Click **Close.**

2.5.2 IIS Configuration

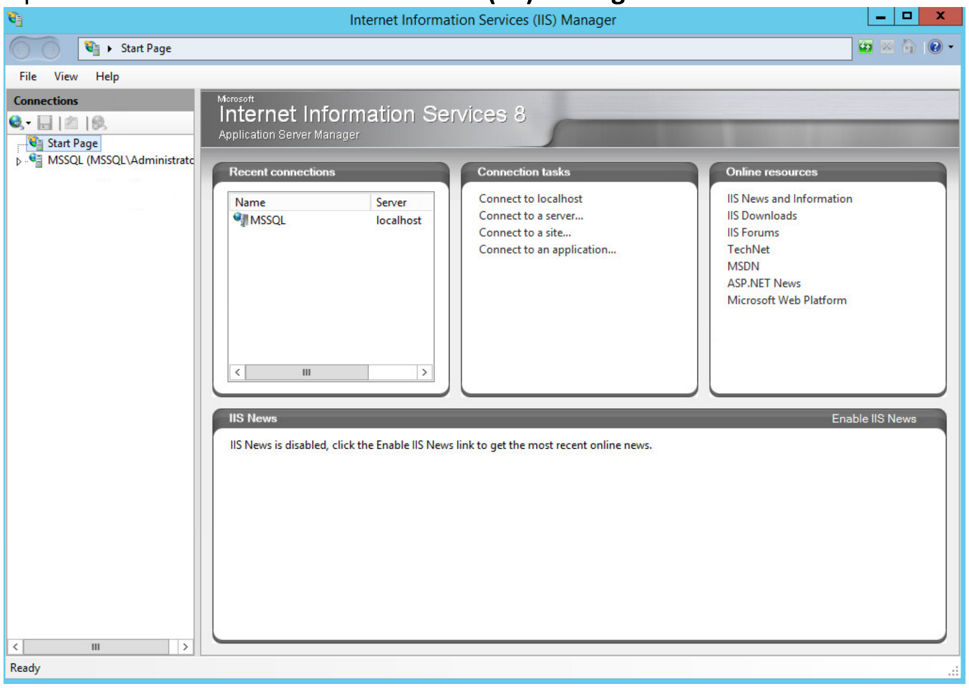
1. Open **Windows Explorer** and click **This PC.**



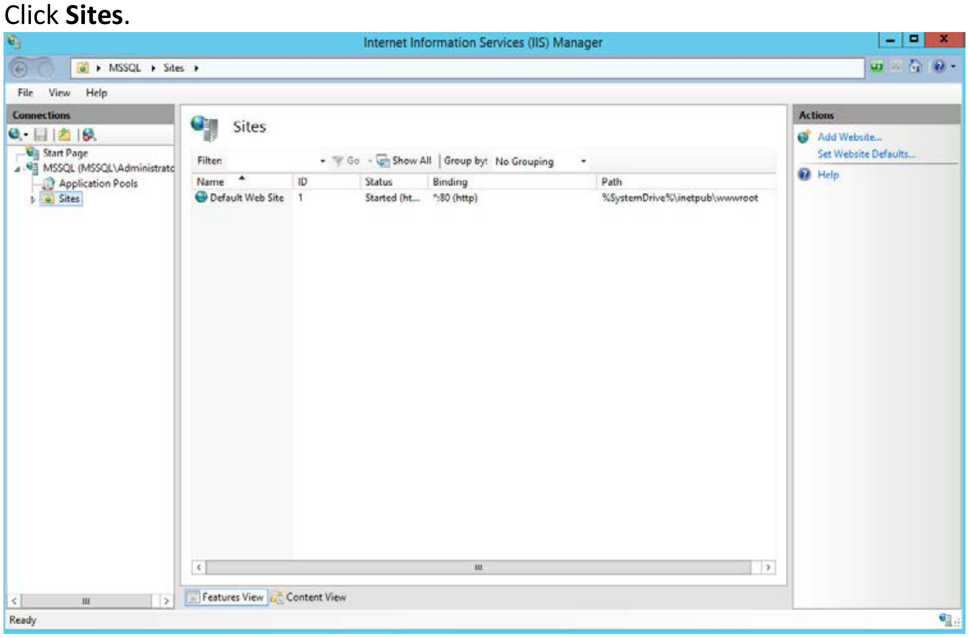
2. Right-click, and select **Create Folder.**
3. Name the folder **www.**



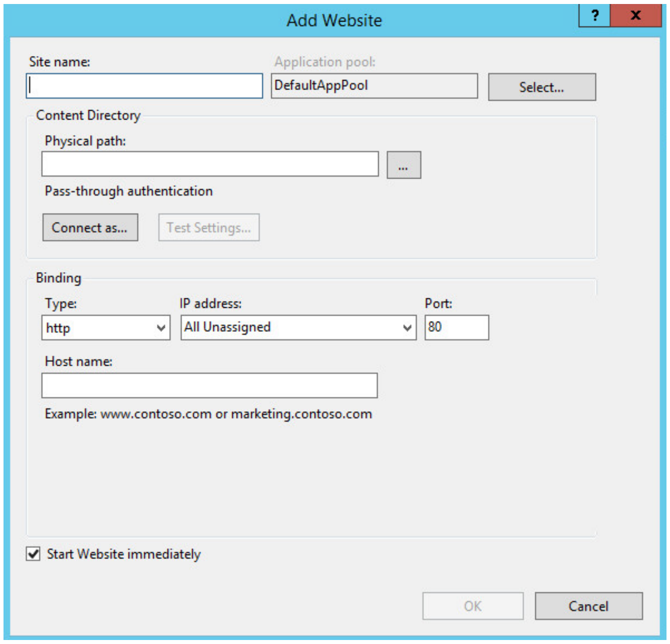
4. Open the **Internet Information Services (IIS) Manager.**



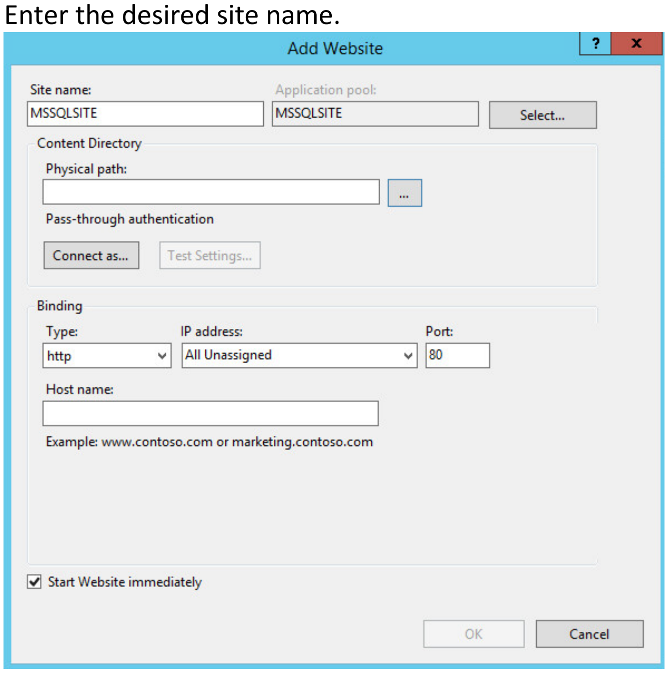
5. Click the arrow next to **MSSQL** (or the chosen name of the server).
6. Click **Sites**.



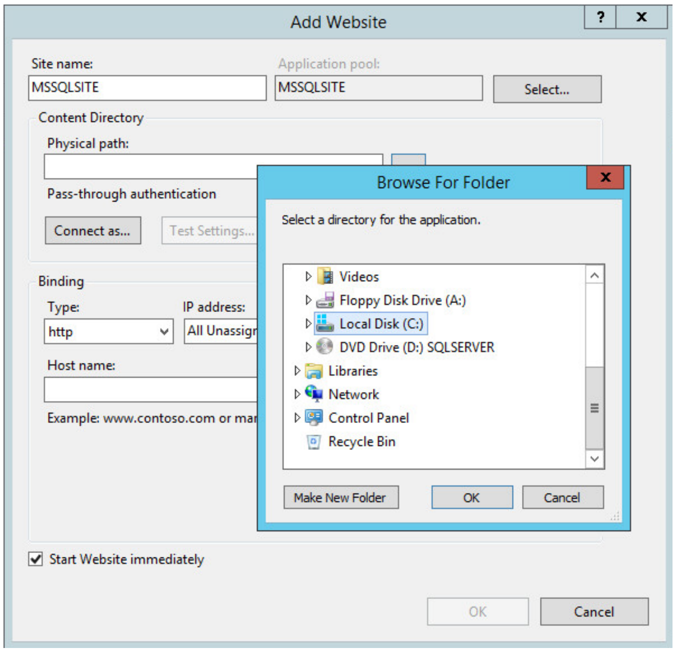
7. Click **Add Website…**.



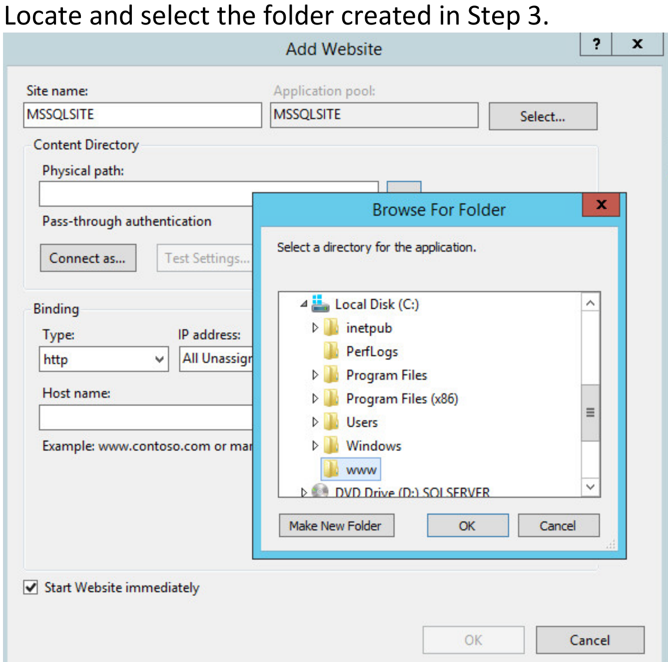
8. Enter the desired site name.



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

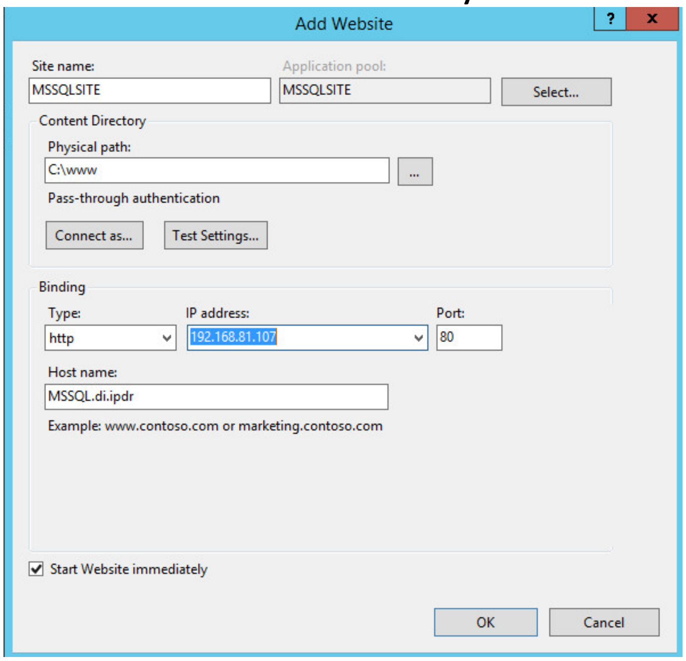


10. Locate and select the folder created in Step 3.



11. Click **OK.**
12. Set **Type** to **http** and **Port** to **80.**
13. Ensure the **IP address** and **Host name** fields are filled in with the correct information for the machine.

14. Ensure that **Start Website immediately** is selected.



15. Click **OK.**

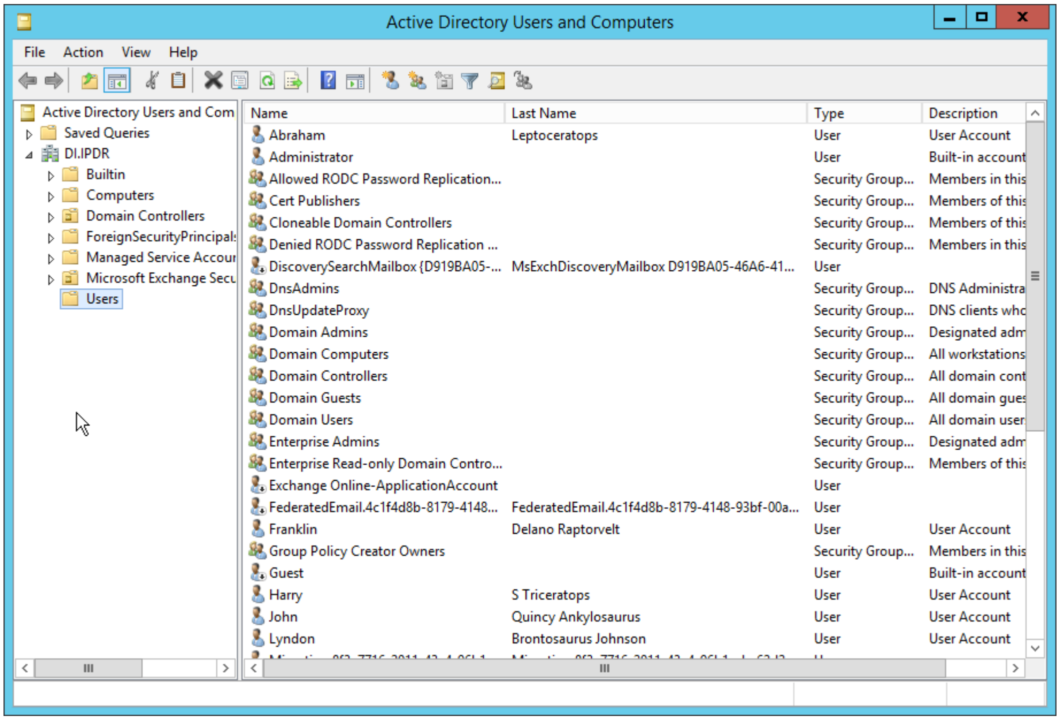
2.6 Semperis Directory Services Protector

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

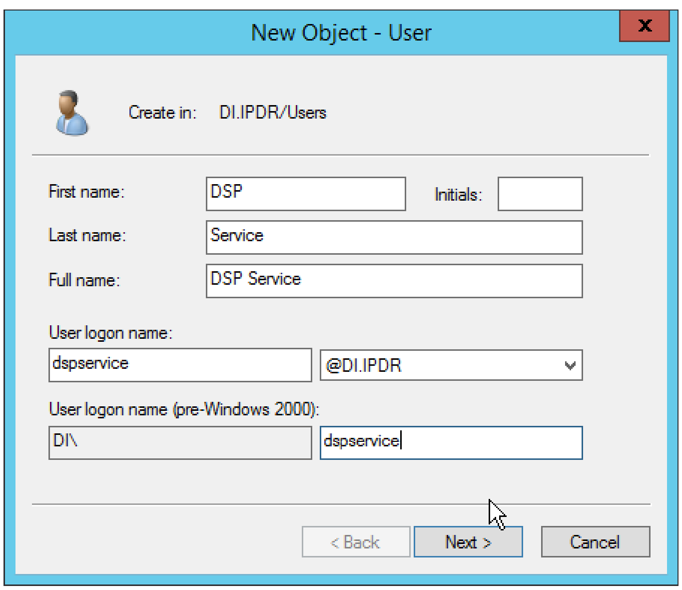
- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- Joined to the Active Directory Domain it is protecting
- Either the installer for SQL Express Advanced or connection information and credentials for a full version of Microsoft SQL (MSSQL)

2.6.1 Configure Active Directory for Semperis DSP

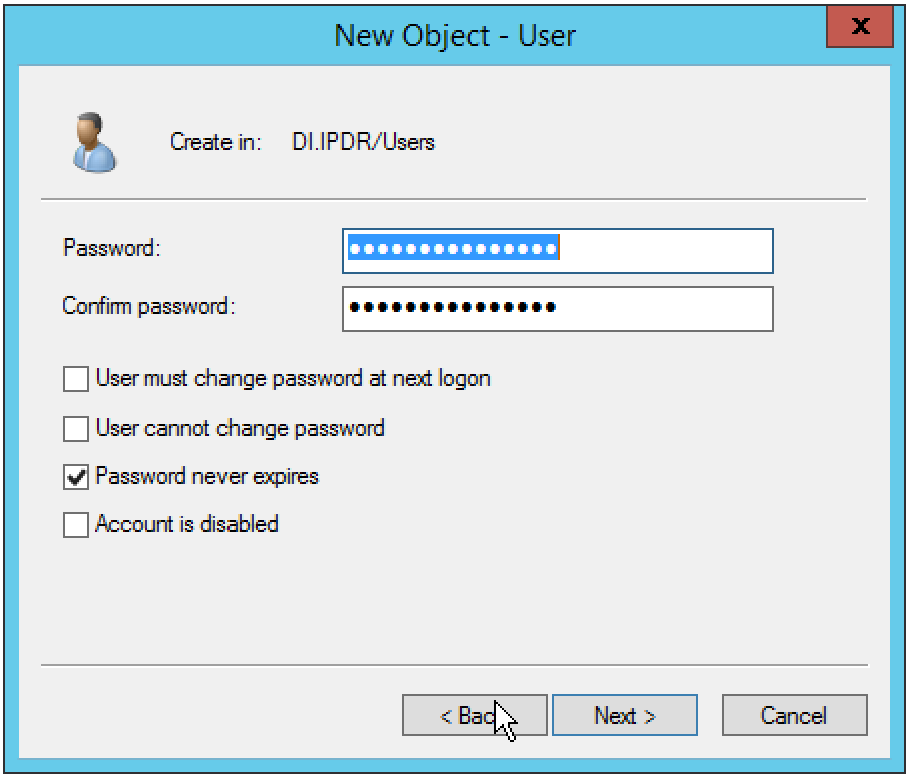
1. Open **Active Directory Users and Computers.**



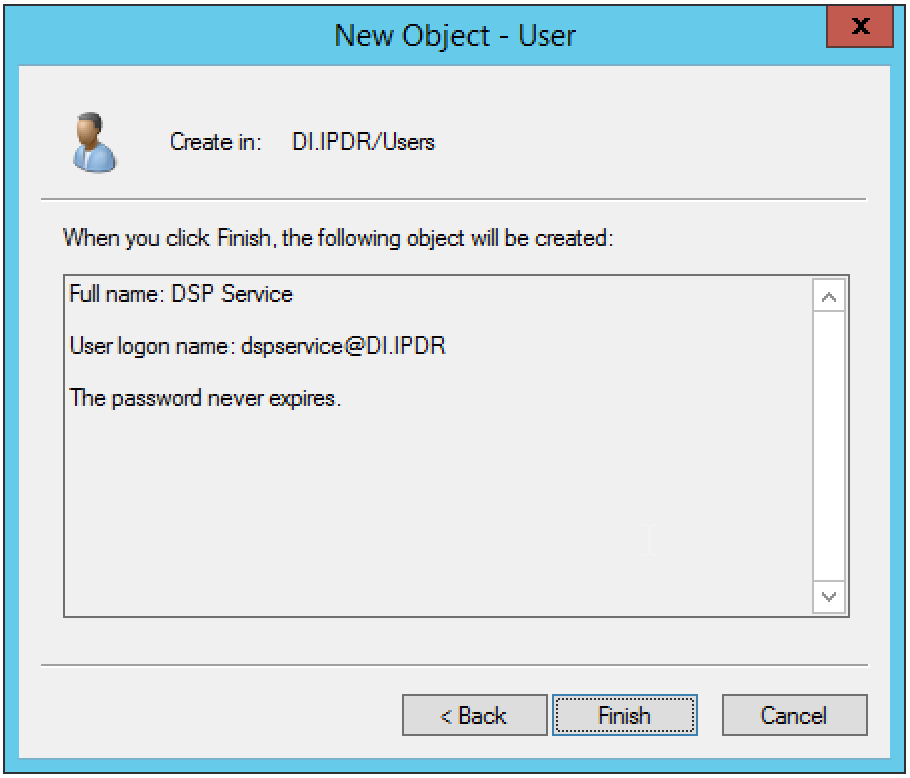
2. Right-click **Users** in the left pane, and select **New > User.**
3. Enter the information for a new user for the DSP service.



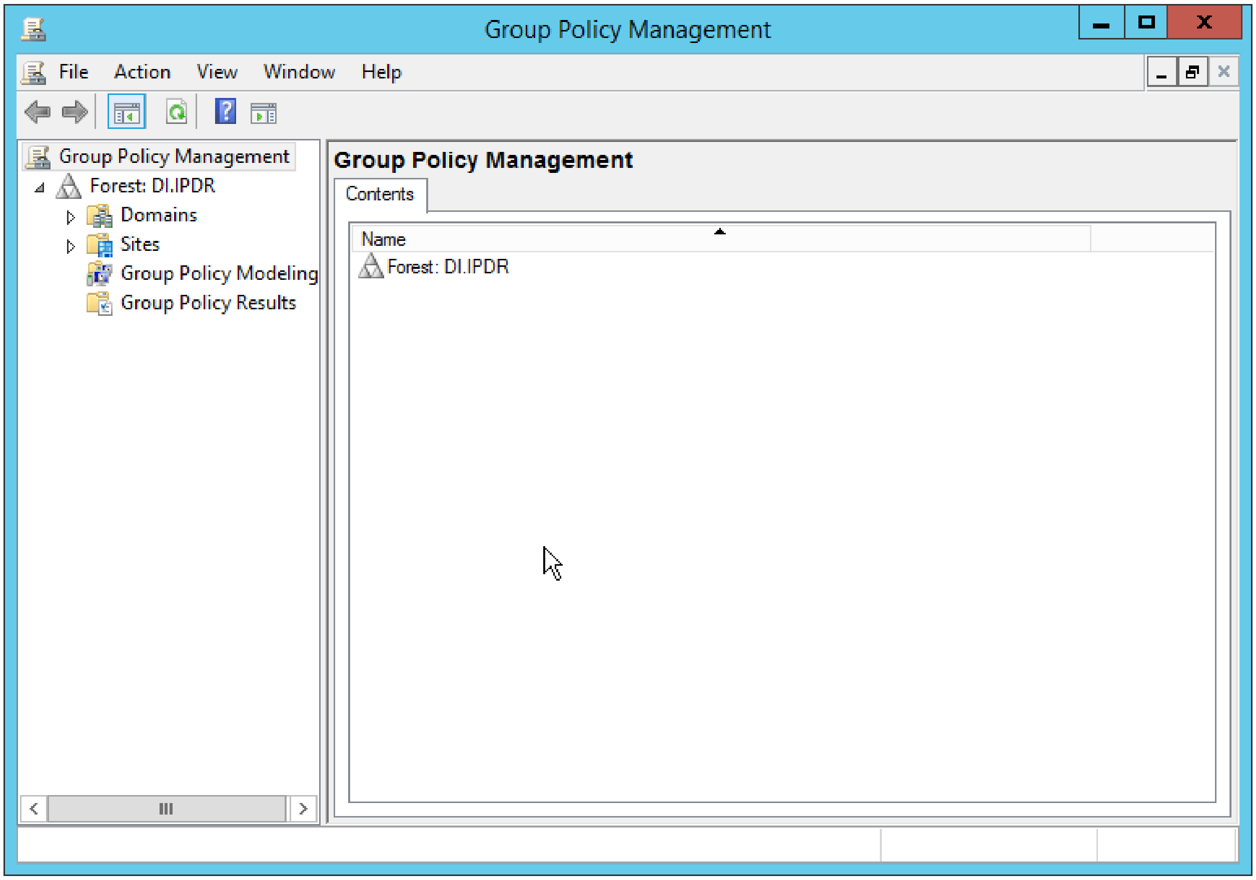
4. Click **Next.**
5. Enter a **password** twice for this user.
6. Set the password policy.


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

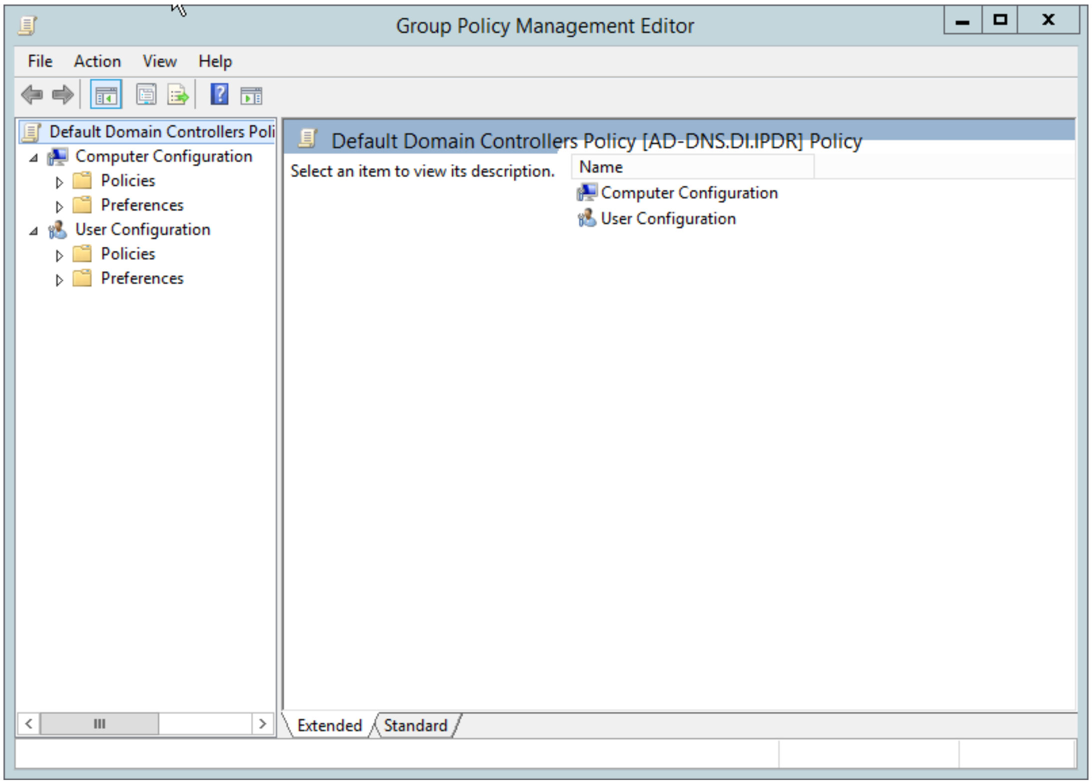
7. Click **Next.**



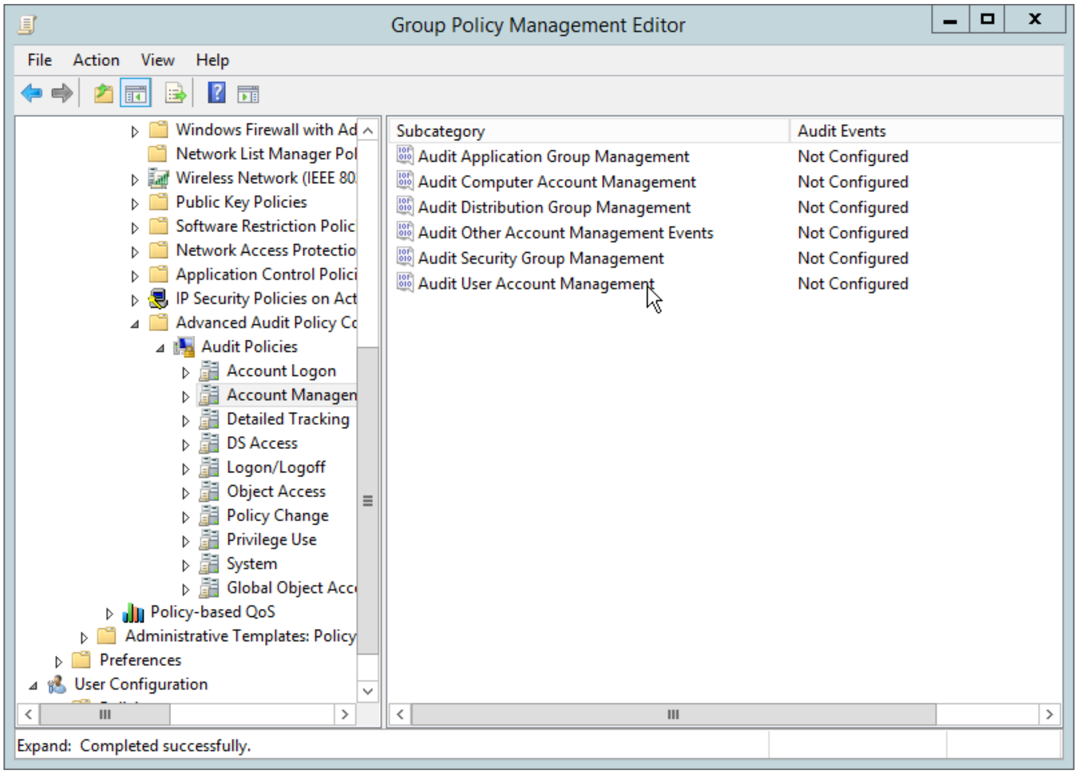
8. Click **Finish.**
9. Open **Group Policy Management.**



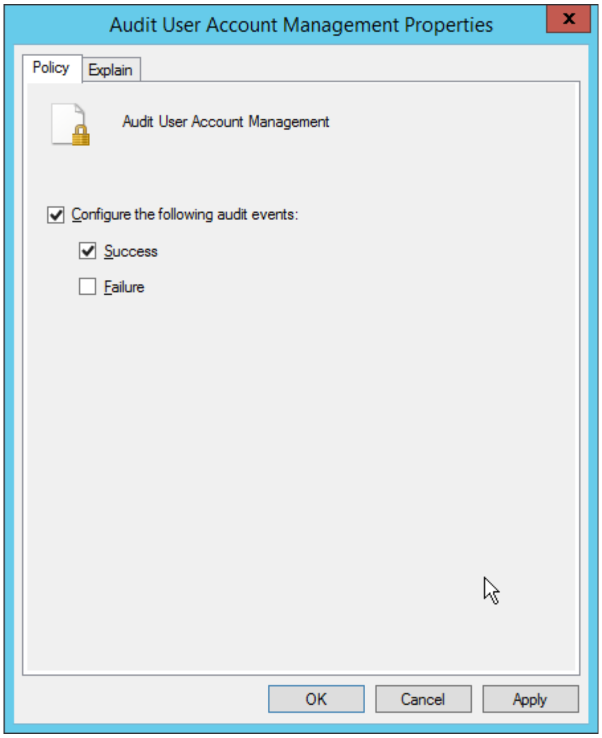
10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy,** and click **Edit.**



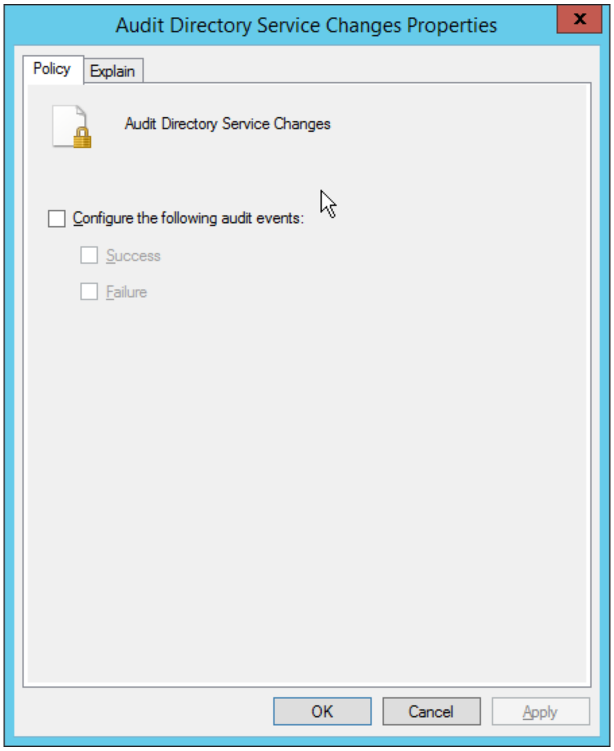
11. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management.**



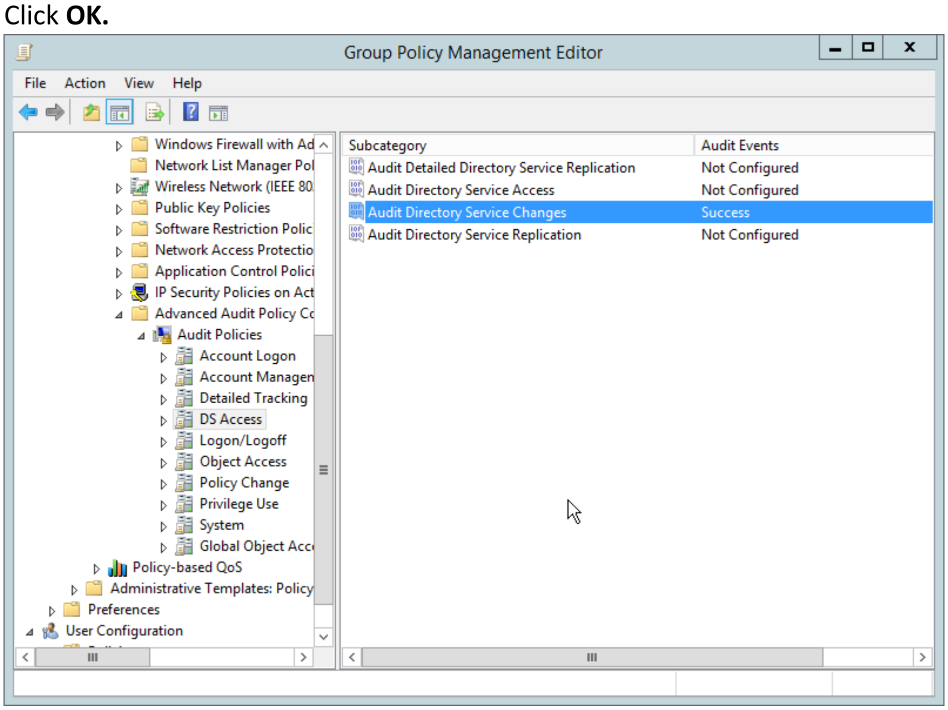
12. Edit the **Audit User Account Management** field by double-clicking it.
13. Check the box next to **Configure the following audit events.**
14. Check the box next to **Success.**



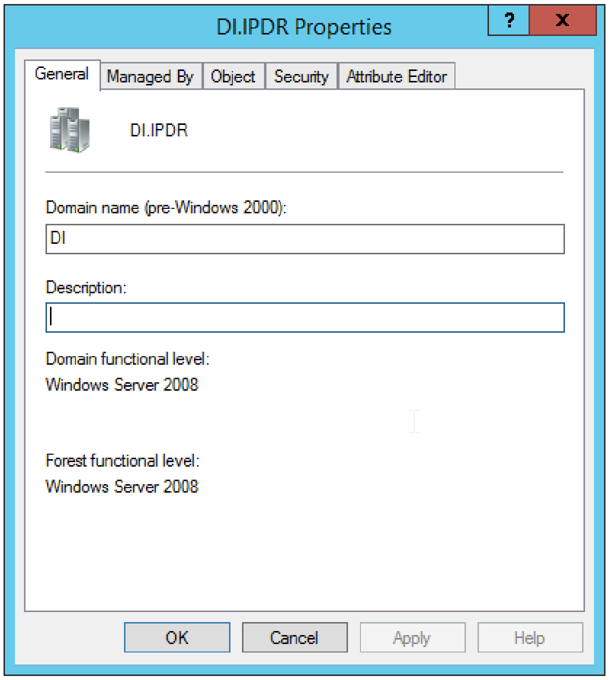
15. Click **OK.**
16. Go to **Audit Policies > DS Access.**
17. Double-click **Audit Directory Services Changes.**



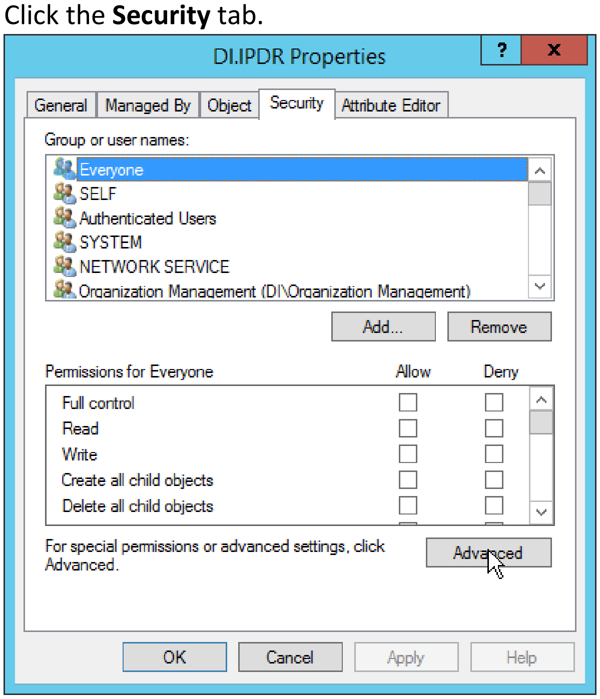
18. Check the box next to **Configure the following audit events.**
19. Check the box next to **Success.**
20. Click **OK.**



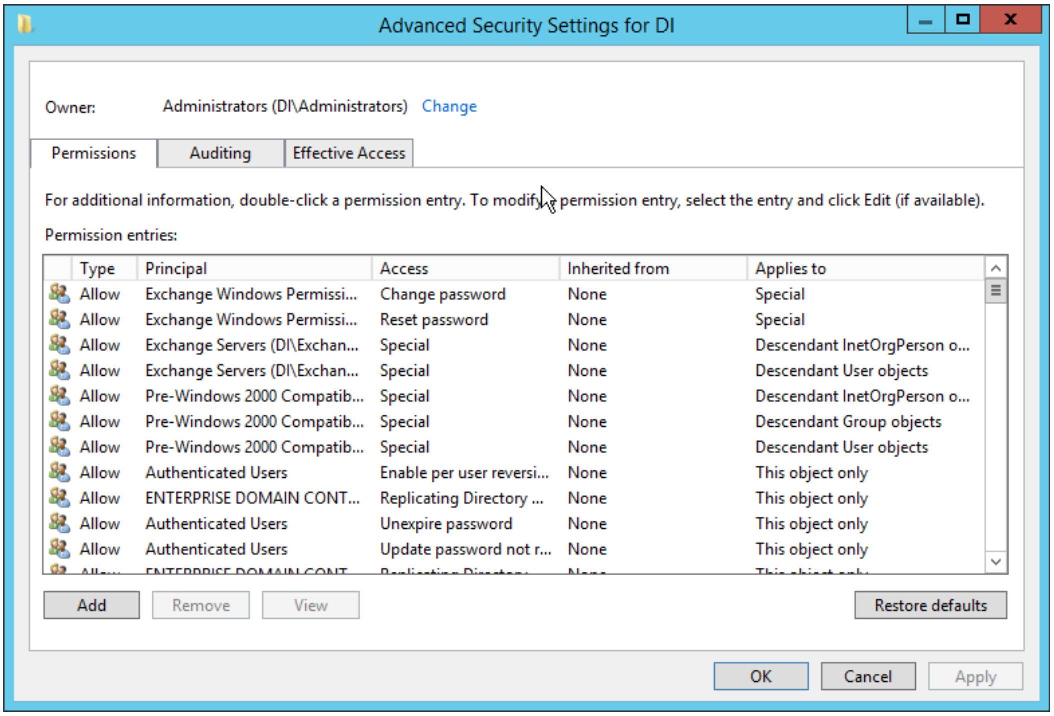
21. Open **Active Directory Users and Computers.**
22. Ensure **View > Advanced Features** is enabled.
23. Right-click the **domain** (for example, DI.IPDR) created earlier, and click **Properties.**



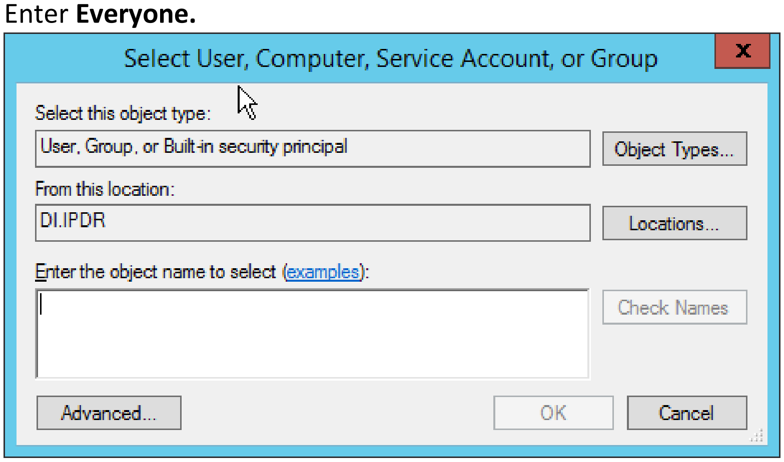
24. Click the **Security** tab.



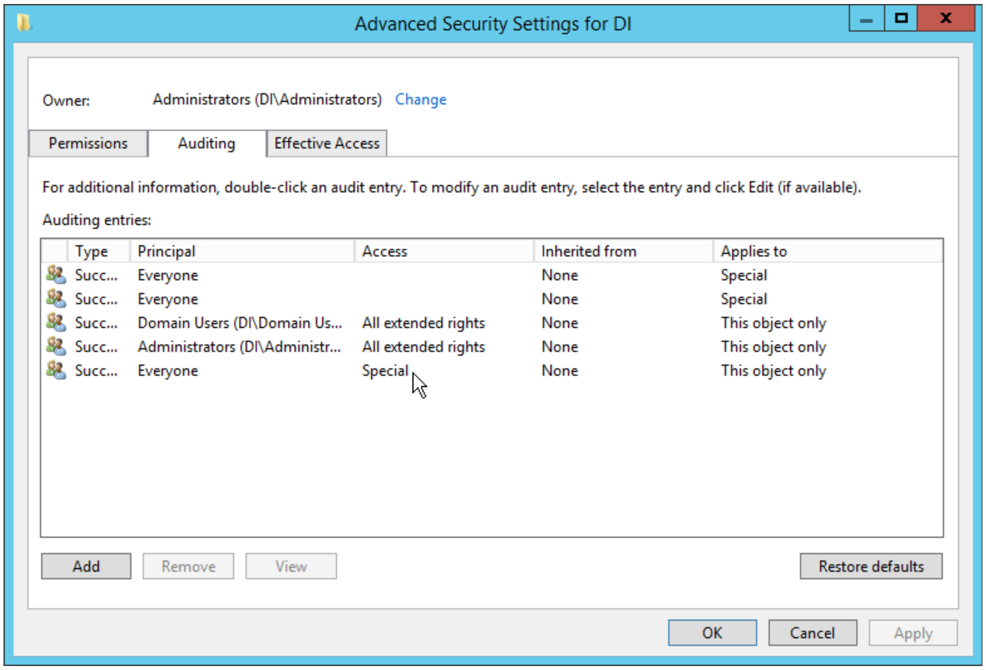
25. Click **Advanced.**



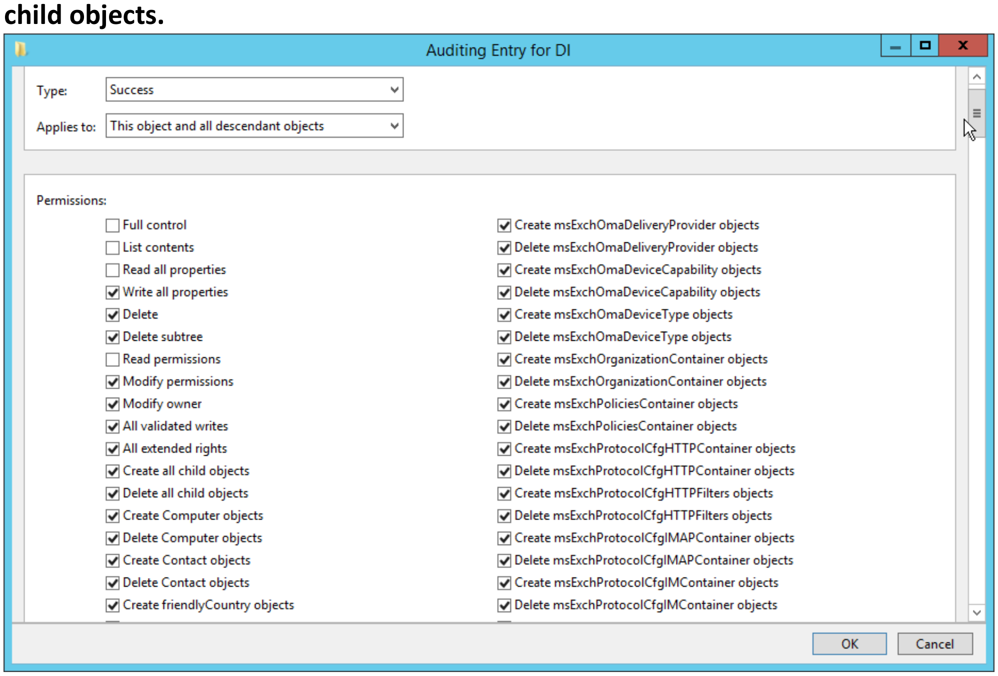
26. Click the **Auditing** tab.
27. Click **Add.**
28. Enter **Everyone.**



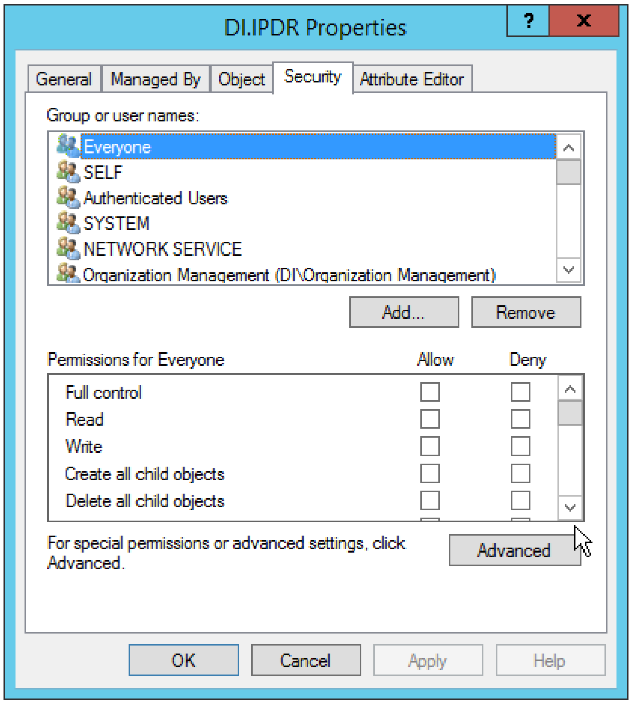
29. Click **OK.**



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



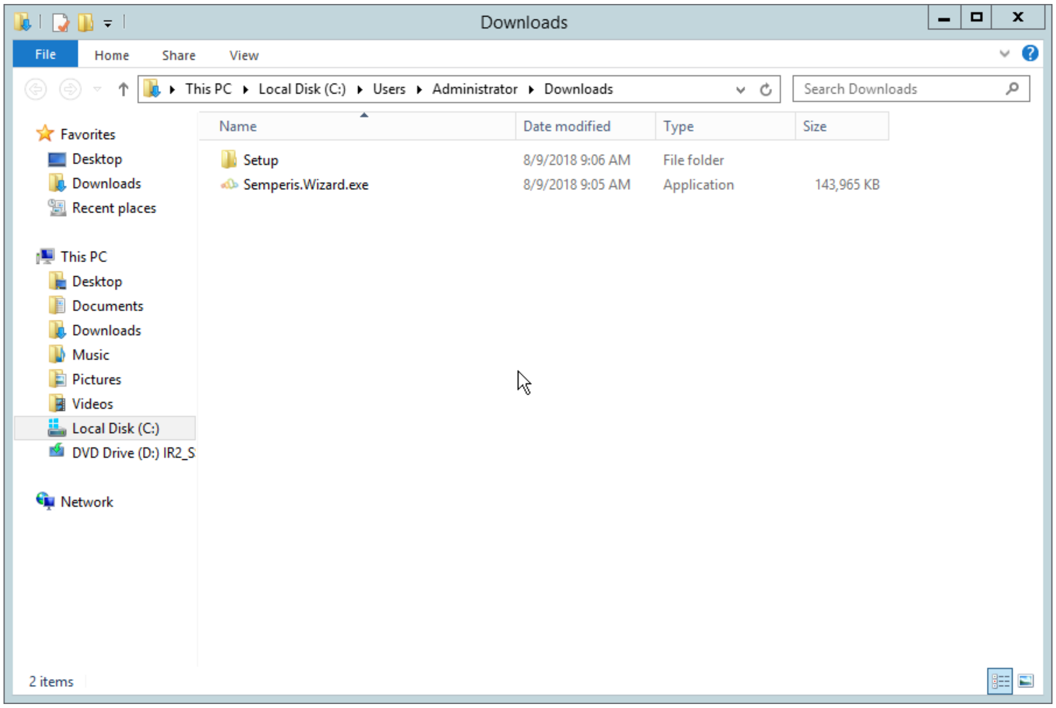
32. Click **OK.**



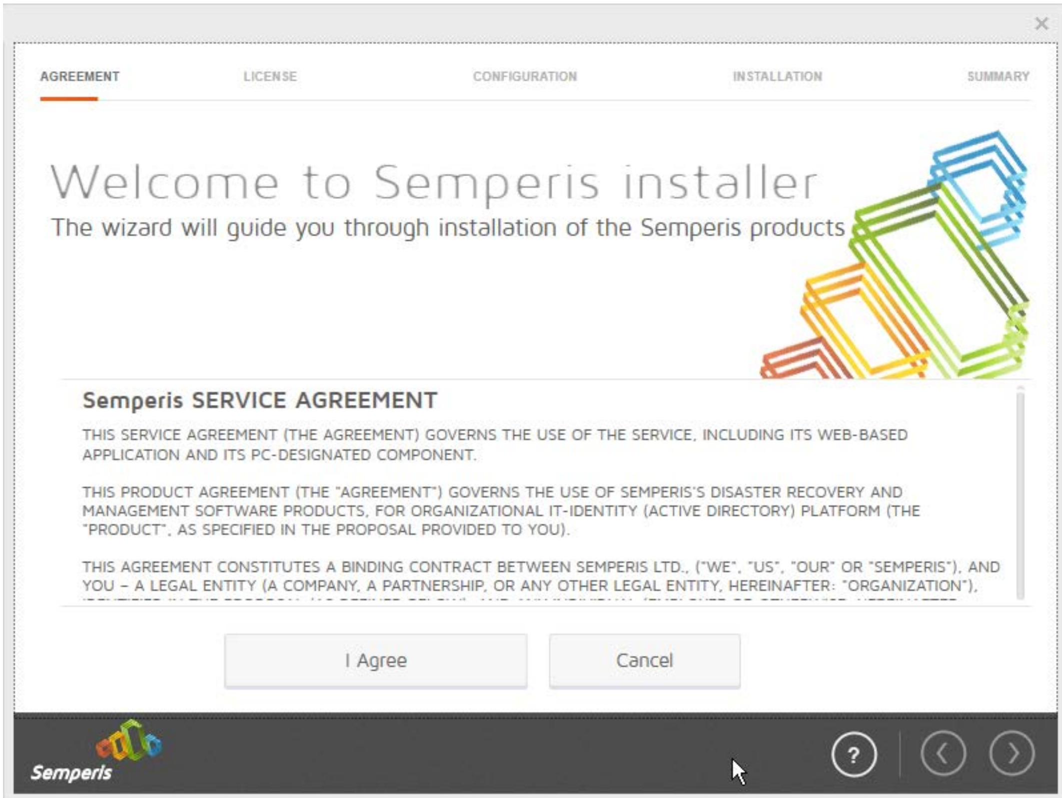
33. Click **OK.**

2.6.2 Install Semperis DSP

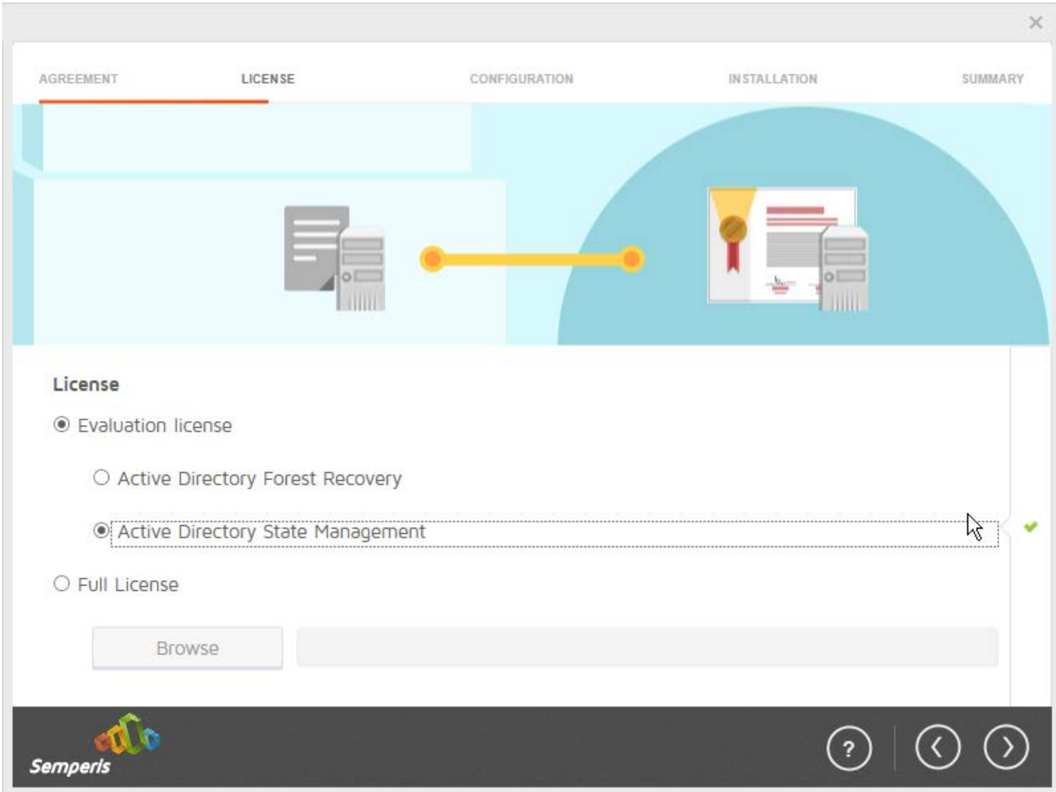
1. If you are using a local SQL Express Advanced server, place the **SQLEXPRADV_x64_ENU.exe** installer in a directory called *Setup,* and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it). If a SQL Express Advanced server is not being used, no **Setup** folder is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



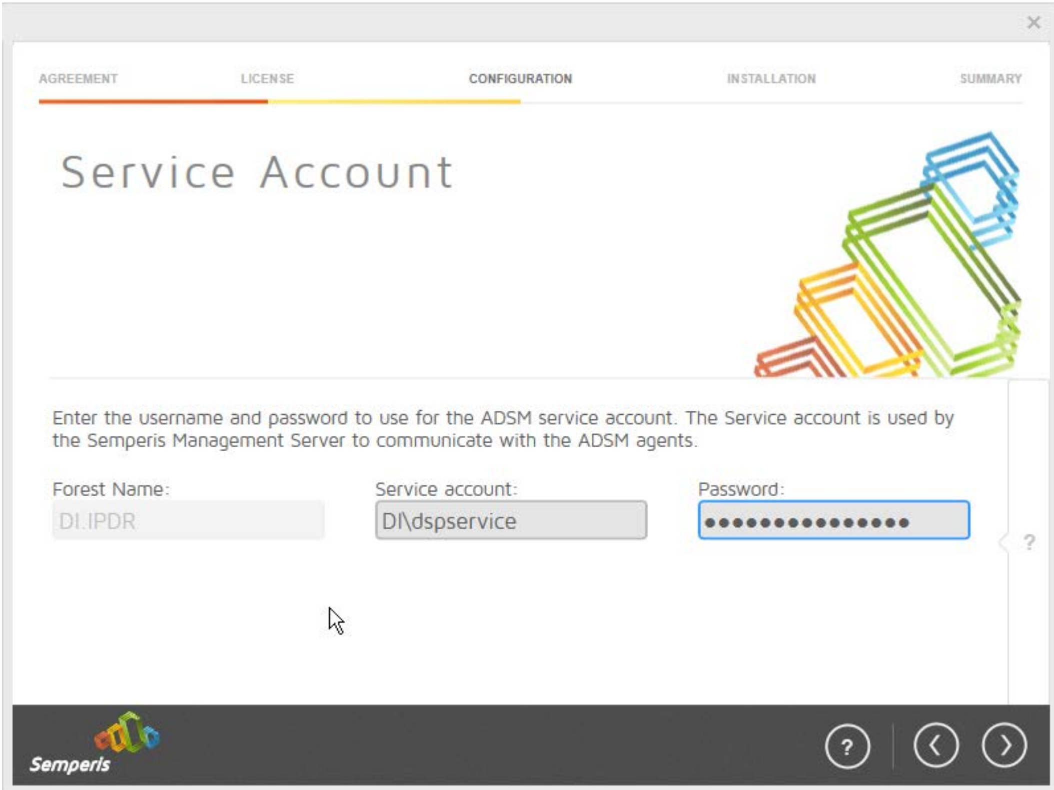
2. If prompted to restart the computer, do so.



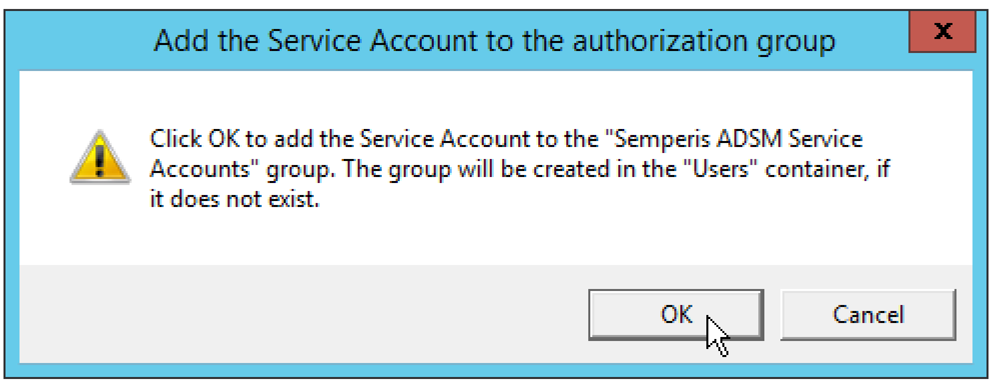
3. Click **I Agree.**
4. Select **Evaluation License.**
5. Select **Active Directory State Management.**



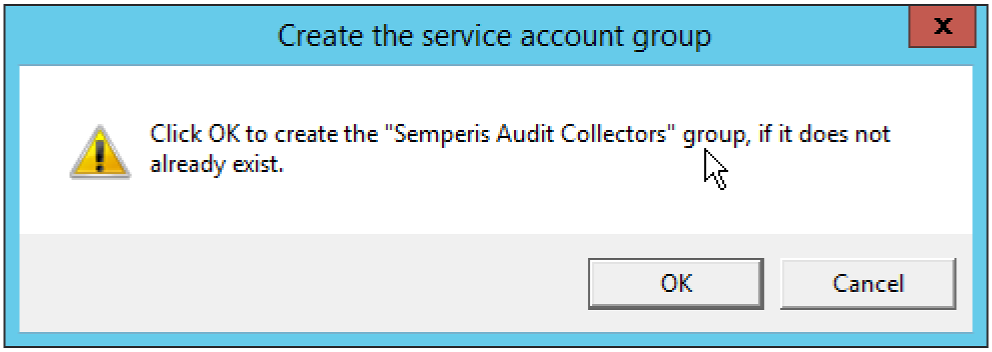
814
815 6. Click the **>** button.
816 7. Enter the **username** and **password** of the account created earlier.



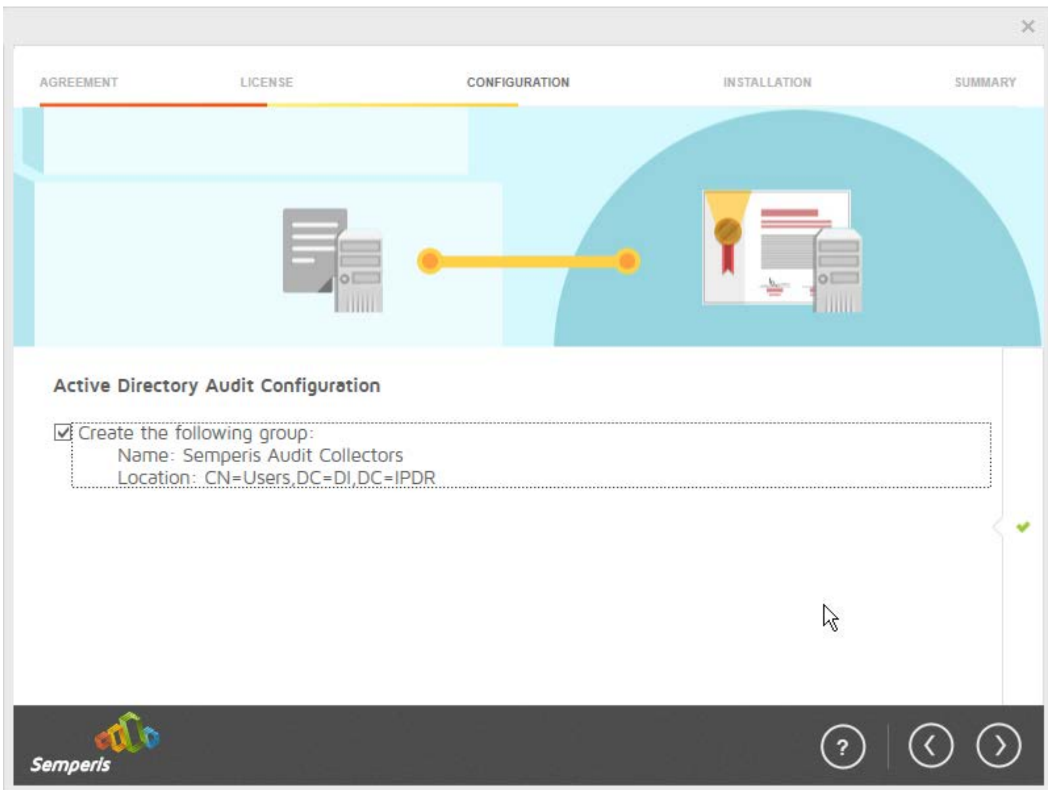
8. Click the **>** button.



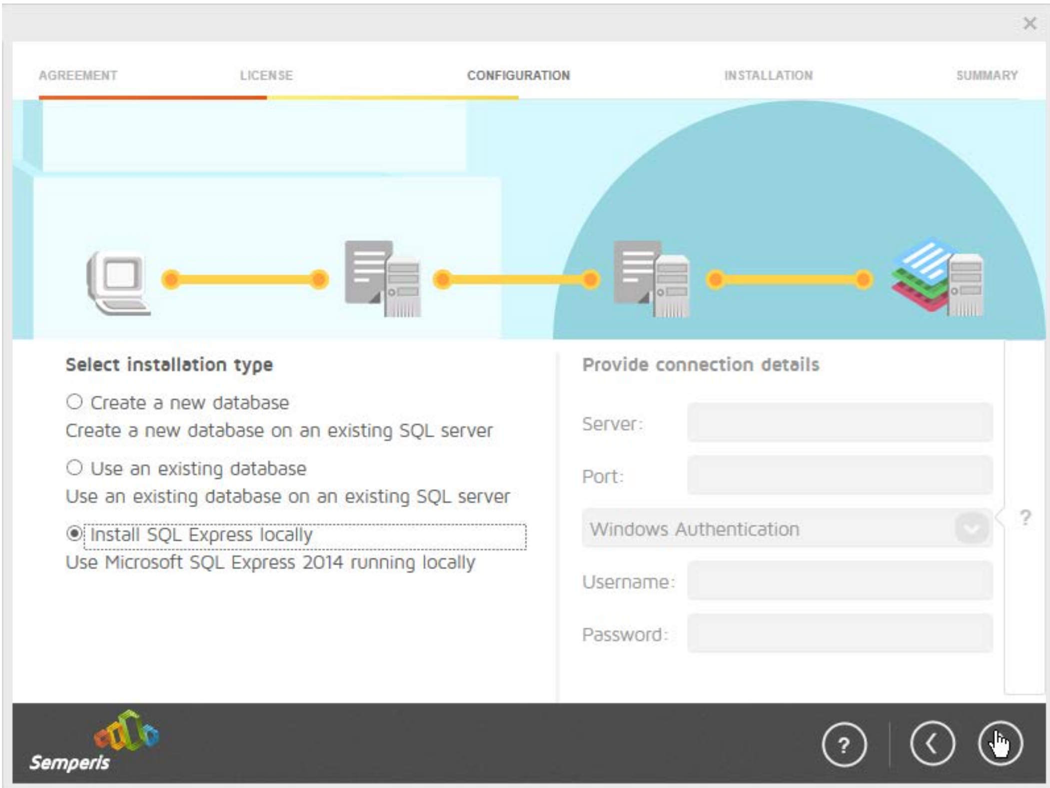
9. Click **OK.**
10. Check the box next to **Create the following group.**



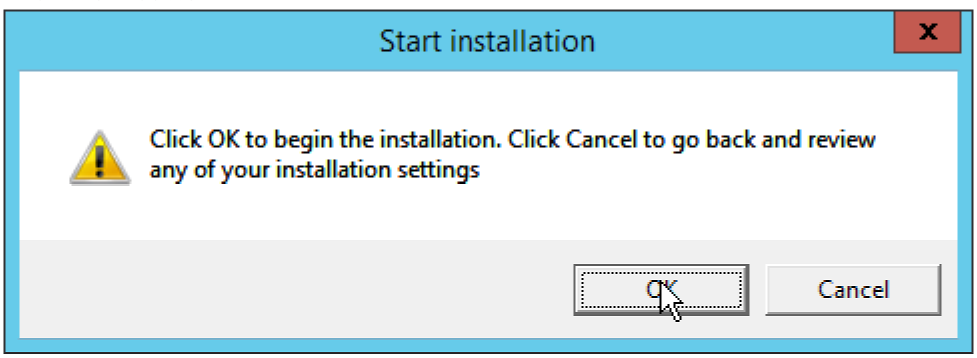
11. Click **OK.**



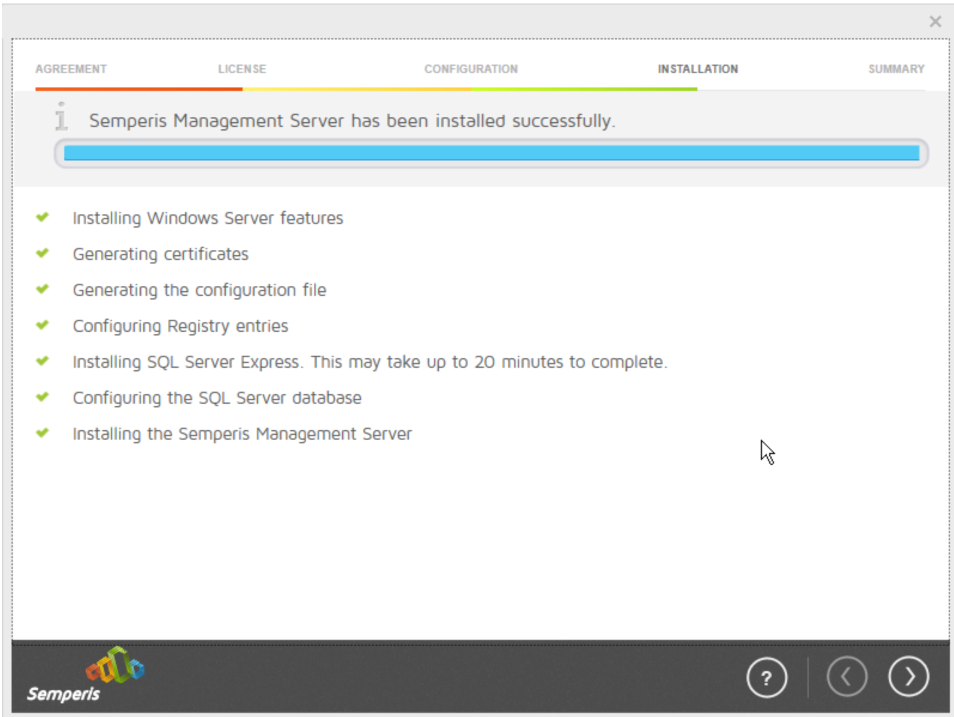
12. Click the **>** button.
13. Select the appropriate database option, and enter any required information.



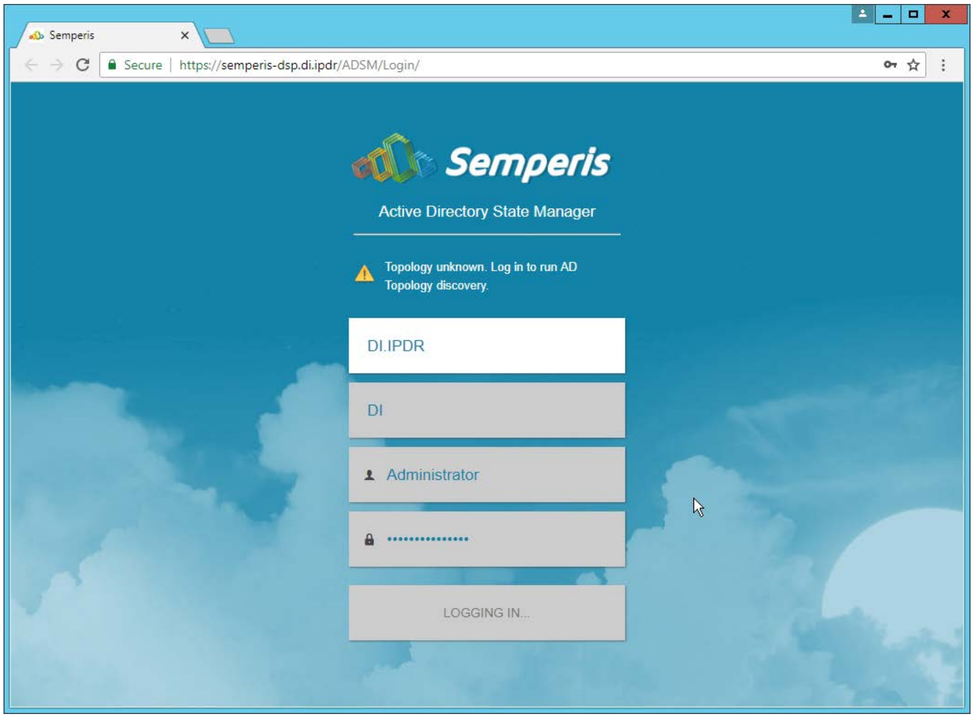
14. Click the **>** button.



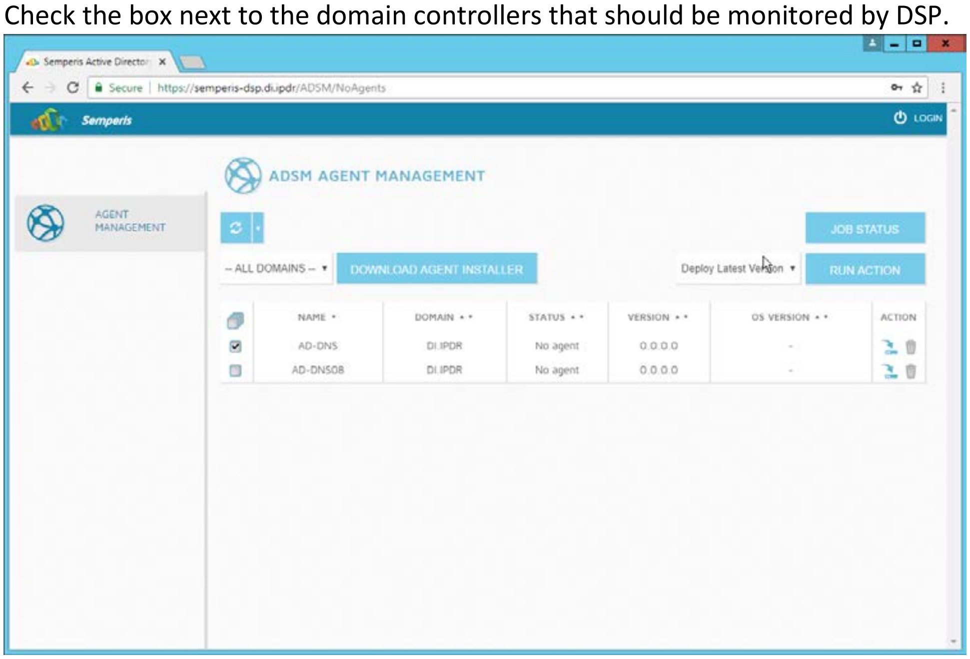
15. Click **OK.**



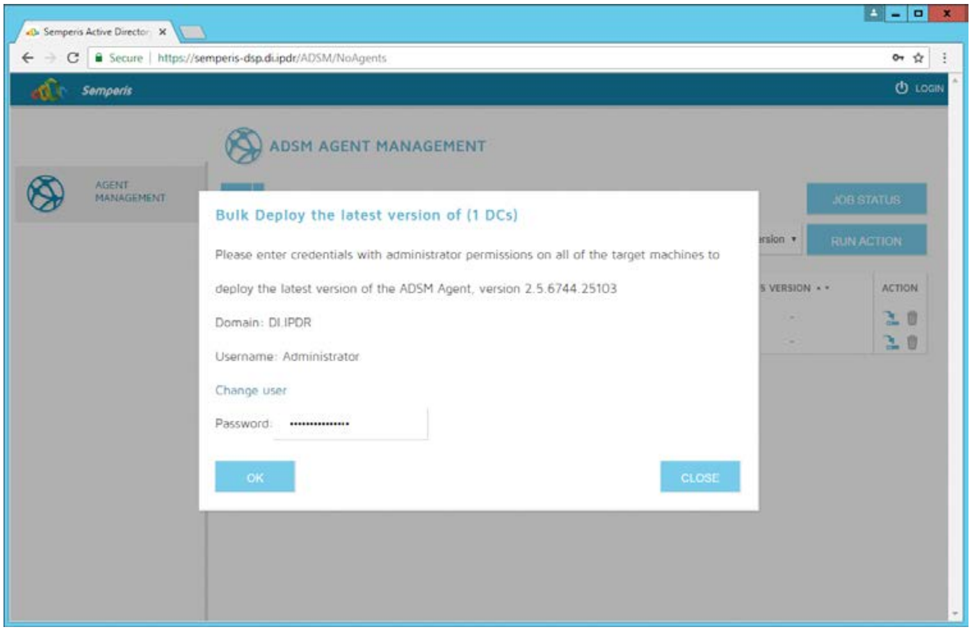
16. Click the **>** button after the installation completes.
17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector.**
18. On the login page, enter the full domain as well as the NetBIOS name.
19. Enter the **username** and **password** of an administrator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



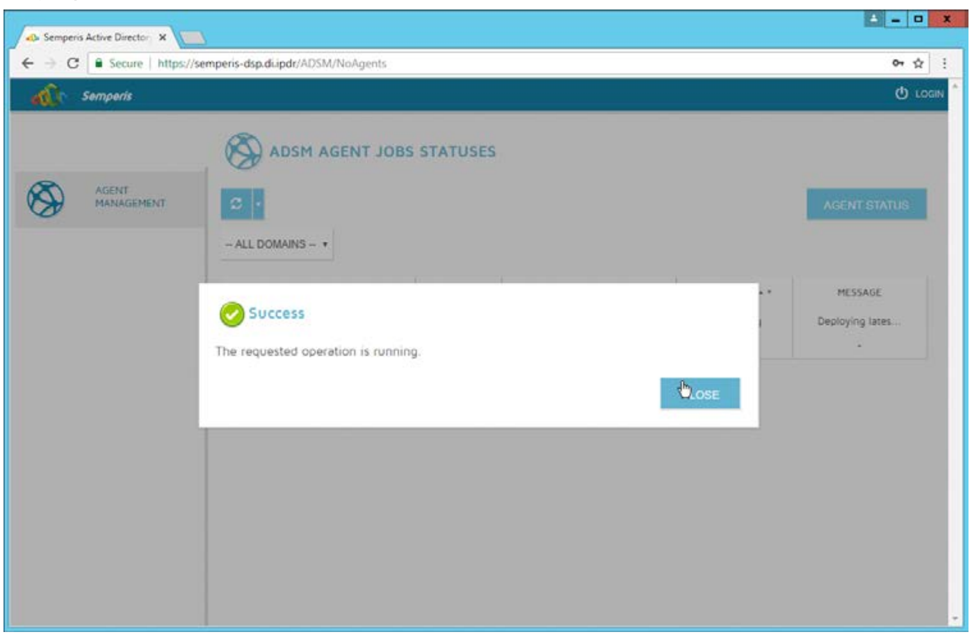
20. Click **Login.**
21. Check the box next to the domain controllers that should be monitored by DSP.



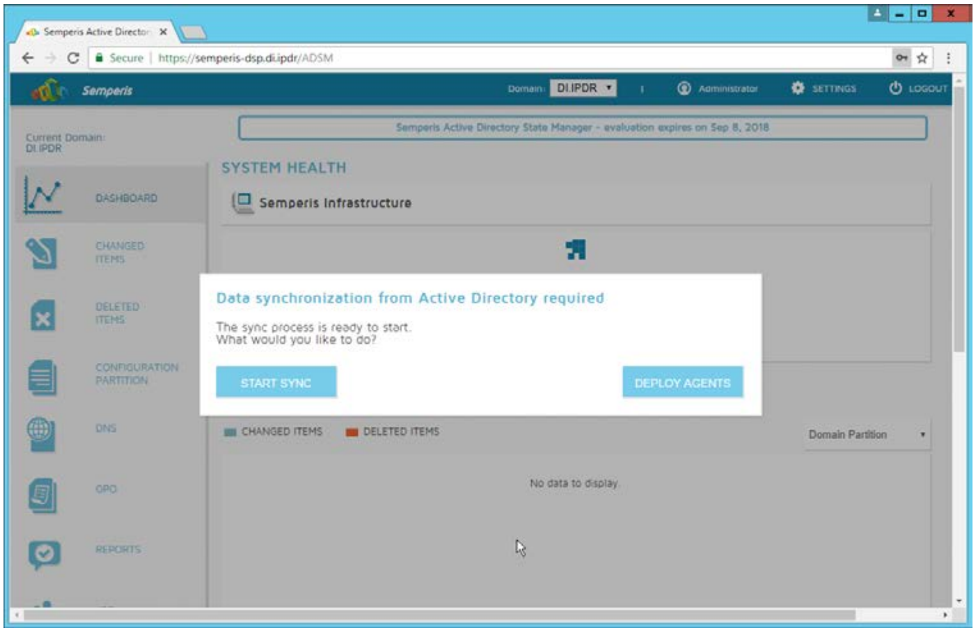
22. Click **Run Action.**
23. Enter the **password** for the account.



24. Click **OK.**



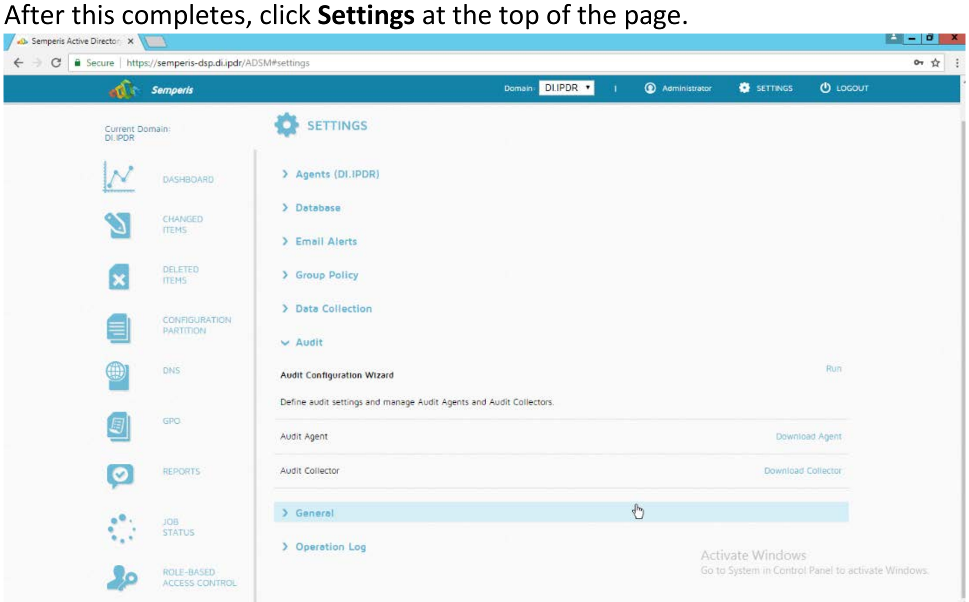
25. Click **Close.**
26. After the agent finishes deploying, click **Login** at the top of the page, and log in.



848

849 27. Click **Start Sync.**

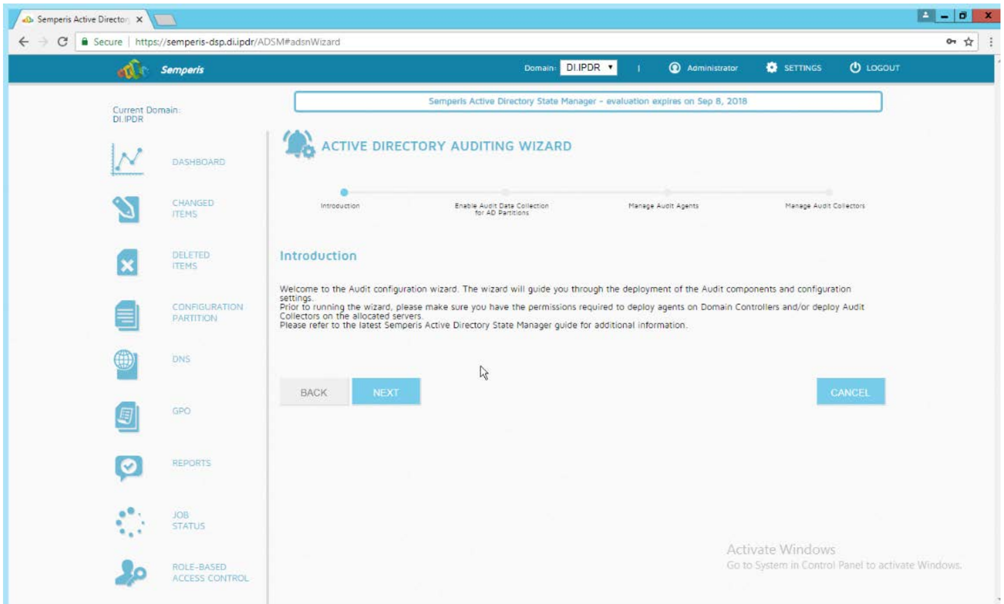
850 28. After this completes, click **Settings** at the top of the page.



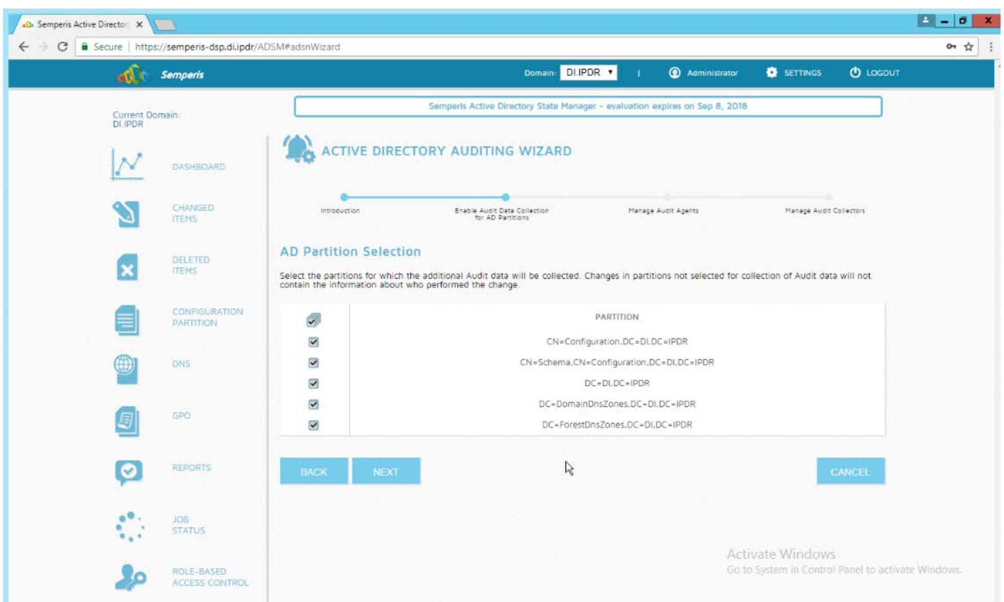
851

852 29. Click **Audit.**

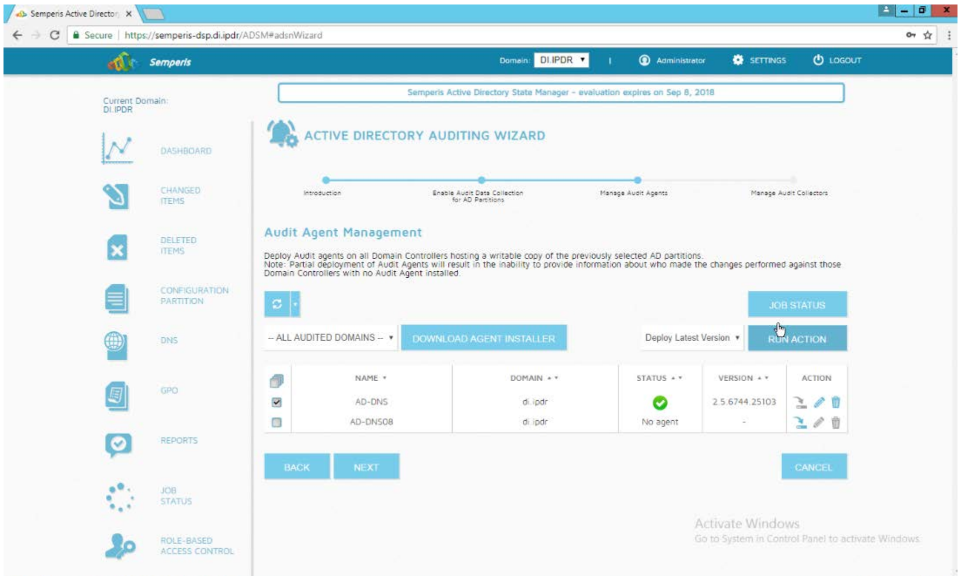
853 30. Click **Run.**



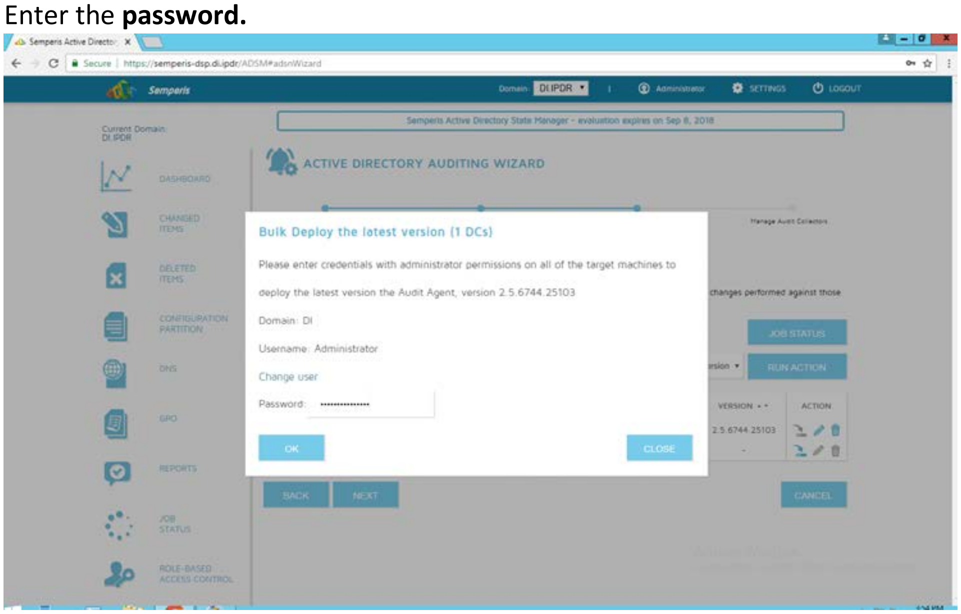
31. Click **Next.**



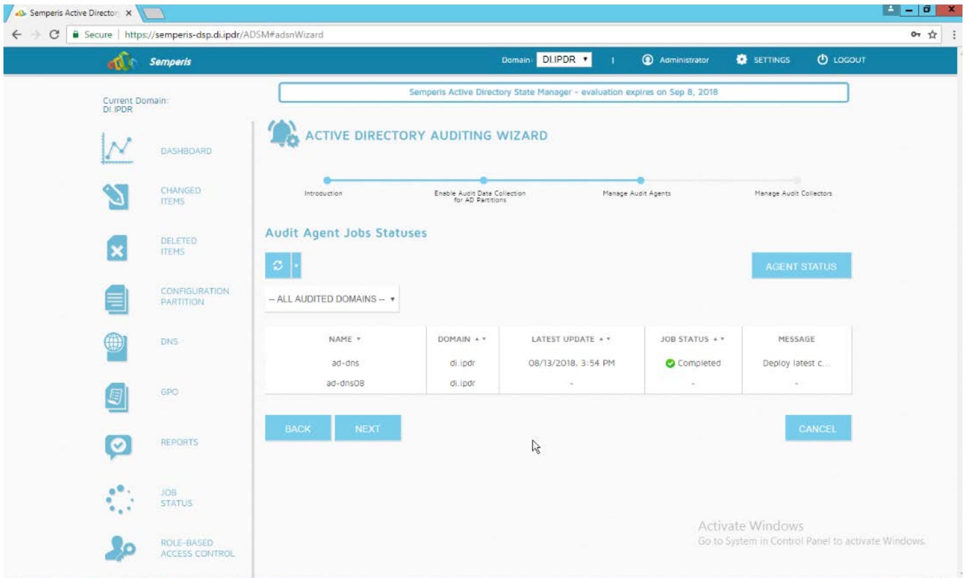
32. Click **Next.**
33. Check the boxes next to any Domain Controllers that should be monitored.



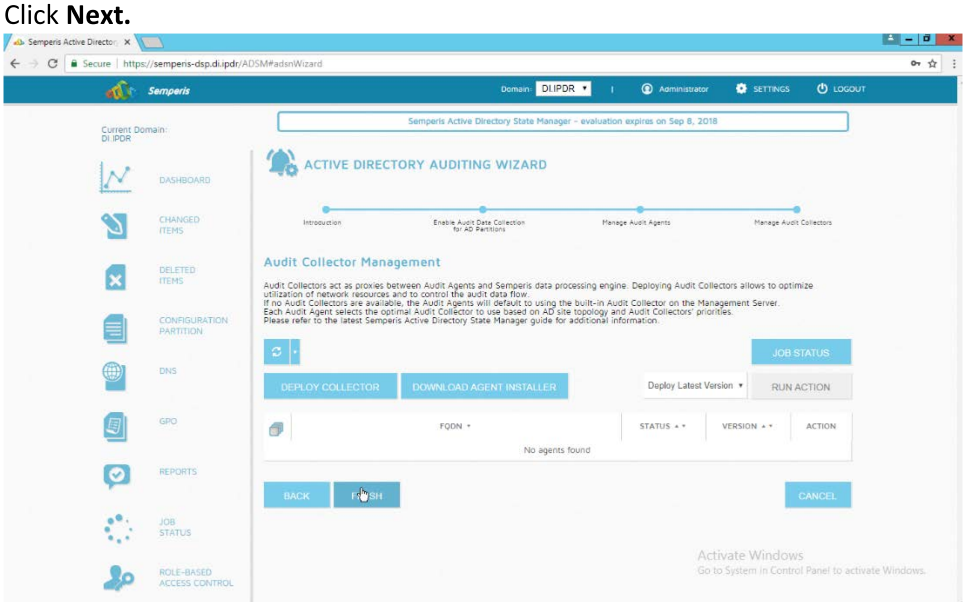
34. Click **Run Action.**
35. Enter the **password.**



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



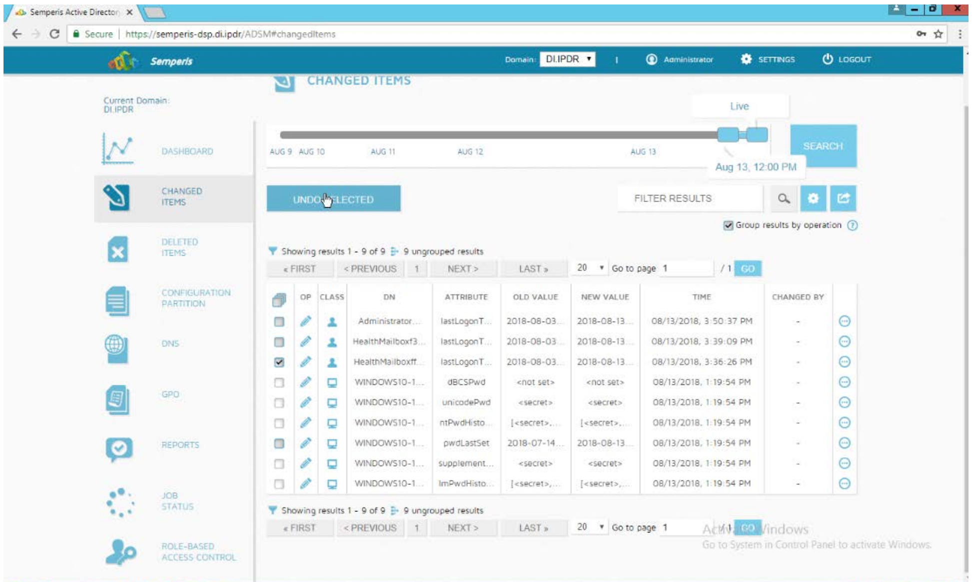
38. Click **Next.**



39. Click **Finish.**

2.6.3 Roll Back Changes with Semperis DSP

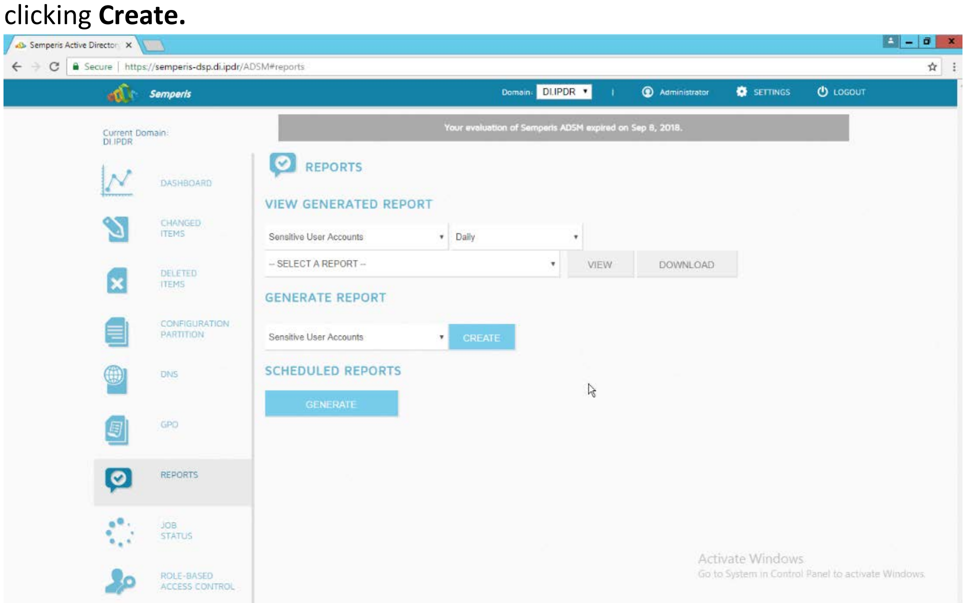
1. Go to **Changed Items** on the left navigation bar.
2. Check the box next to any undesired Active Directory changes.
3. Click the **…** button to view more details about the change.



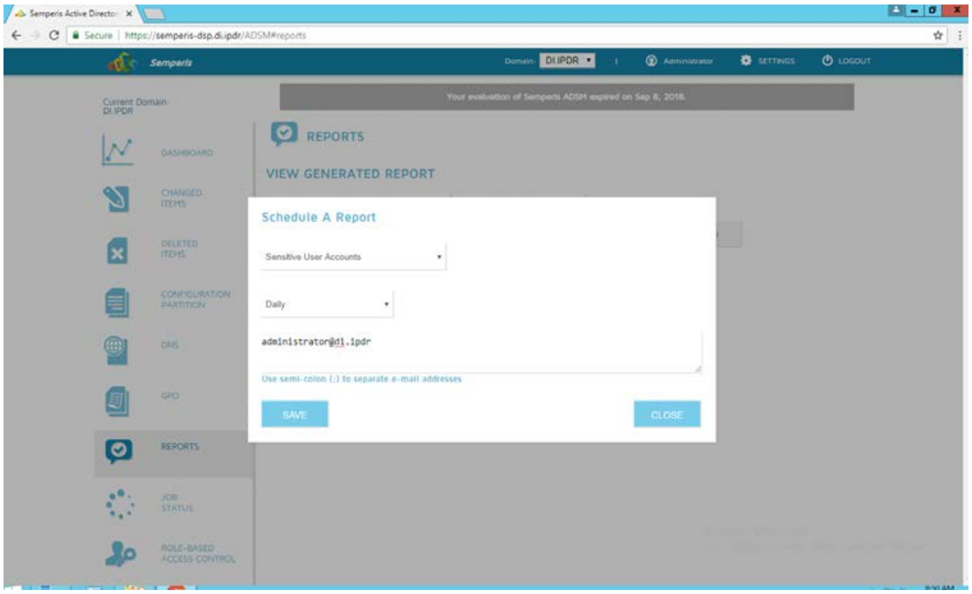
4. Click **Undo Selected** to roll back these changes.

2.6.4 Configure Reporting with Semperis DSP

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



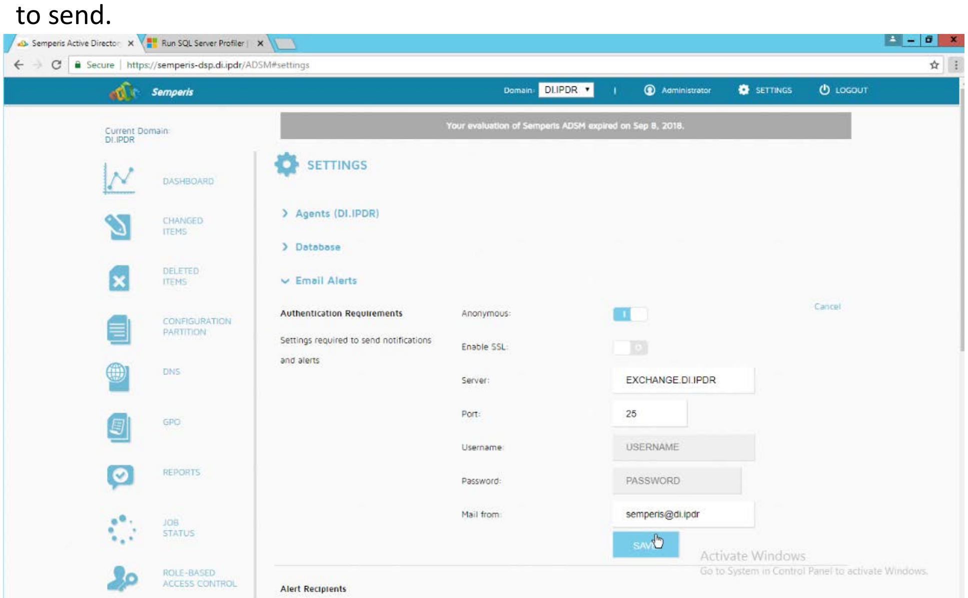
3. Under **Scheduled Reports,** click **Generate** to automatically email specific reports.
4. Select a report type and a schedule.
5. Enter the email addresses of anyone who should receive this report.



6. Click **Save.**

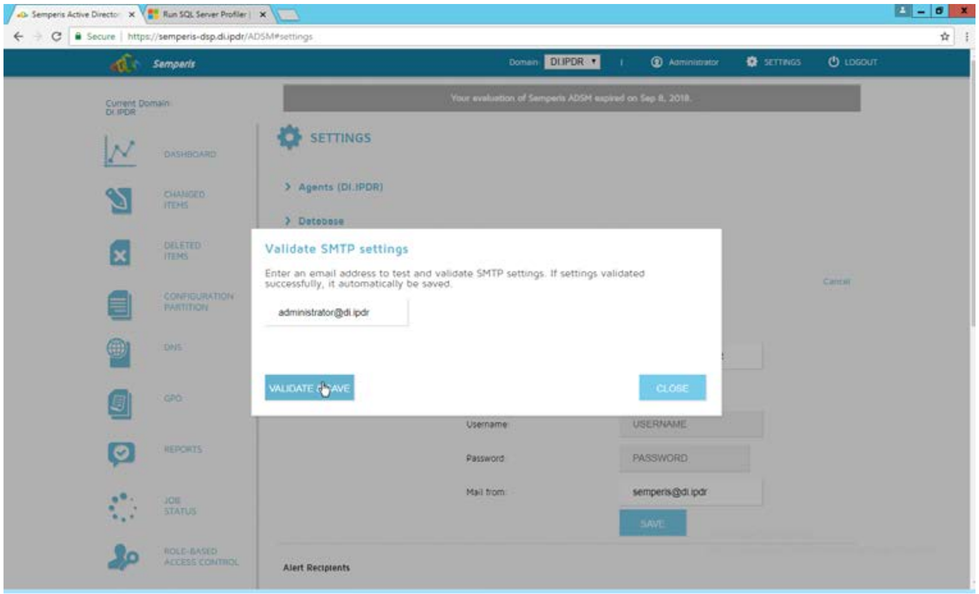
2.6.5 Configure Email Alerts with Semperis DSP

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

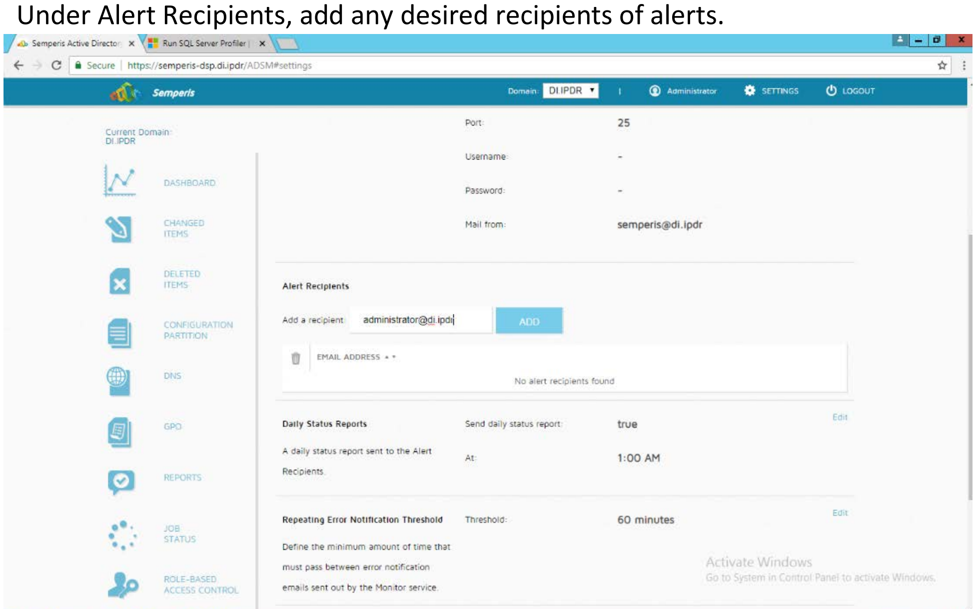


5. Click **Save.**

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



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



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

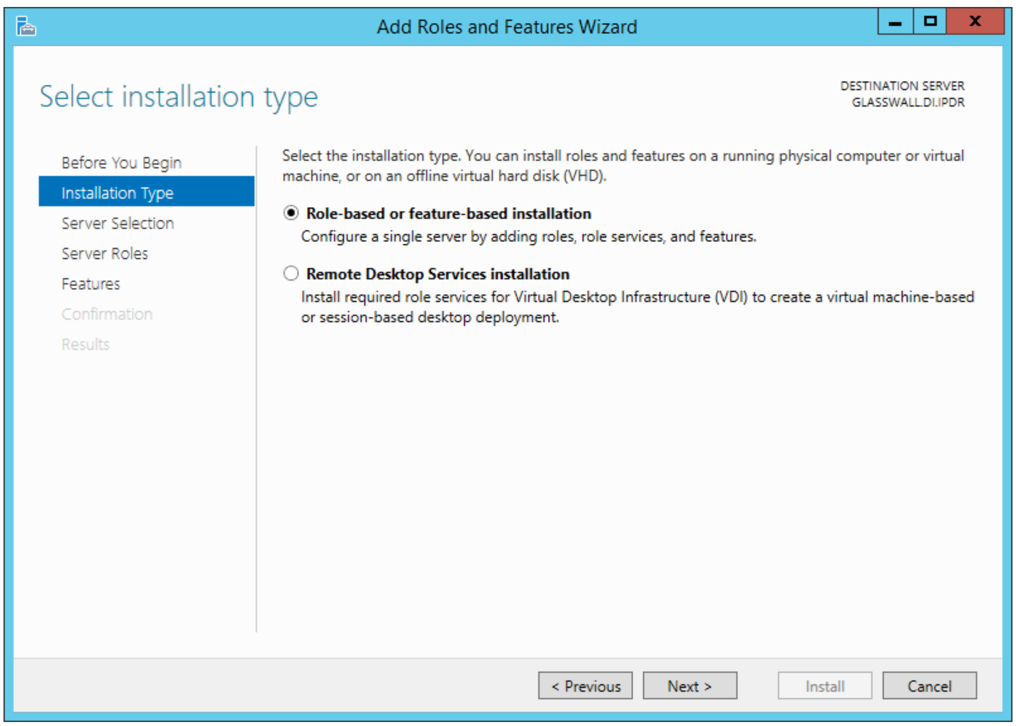
2.7 Glasswall FileTrust™ for Email

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

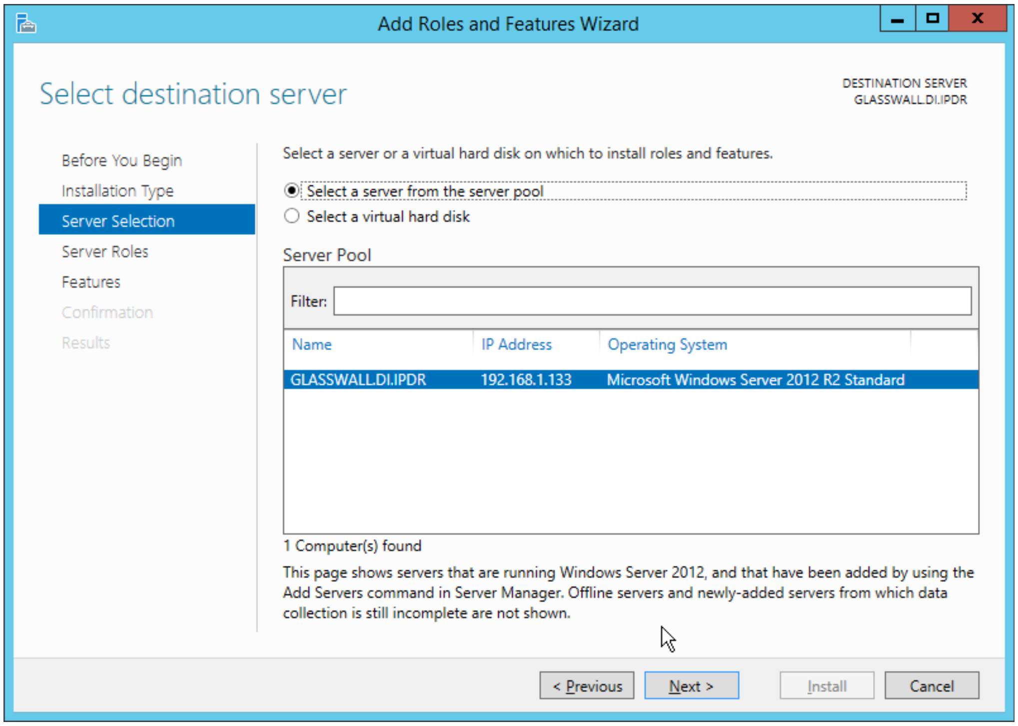
2.7.1 Install Prerequisites

2.7.1.1 *Install the IIS web server*

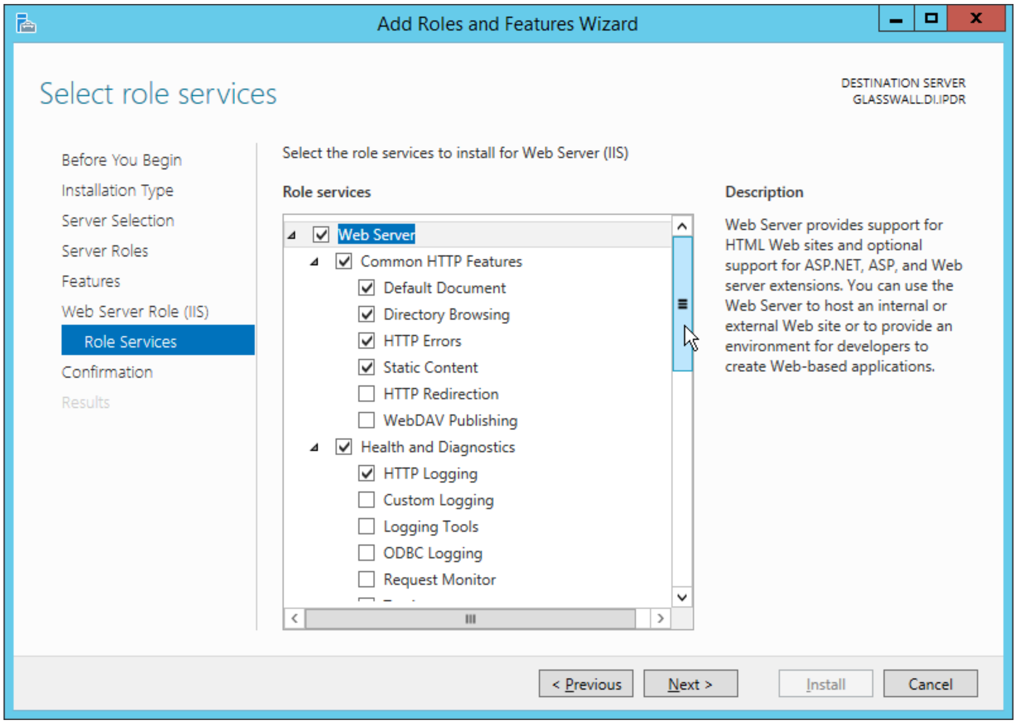
1. In **Server Manager,** click **Add Roles and Features.**
2. Click **Next.**
3. Select **Role-based or feature-based installation.**



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



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



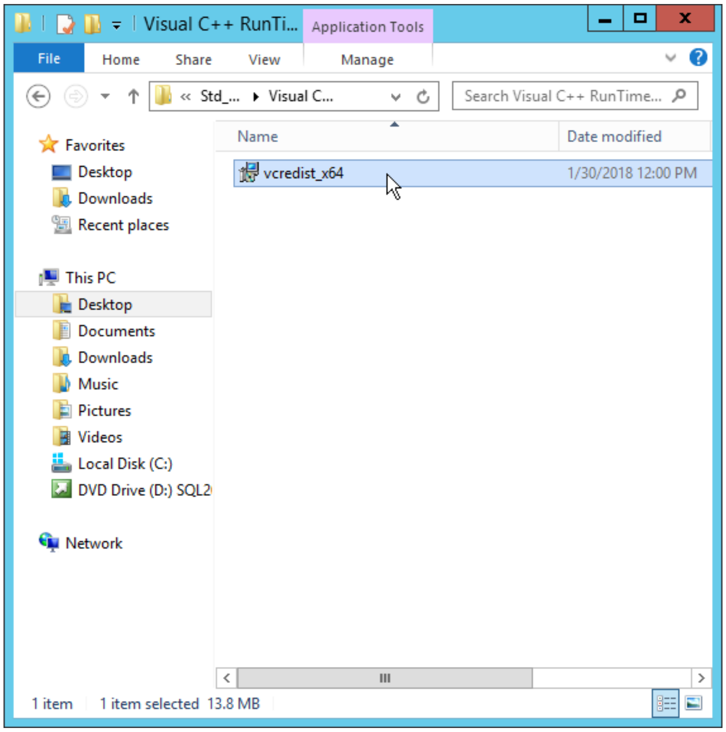
12. Click **Next.**
13. Check the box next to **Restart the destination server automatically if required.**
14. Click **Install.**

2.7.1.2 *Install Microsoft SQL 2014 Enterprise*

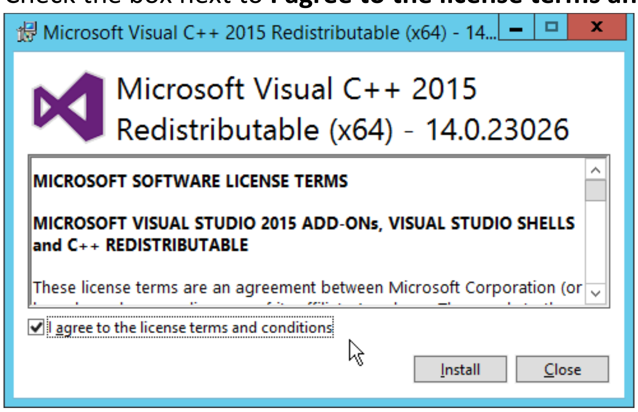
Please see Section 2.4 for an installation guide for MS SQL 2014; for simplicity it should be installed on the same server as Glasswall FileTrust. Ensure that Mixed Mode authentication is selected when installing.

2.7.1.3 *Install Microsoft Visual C++ 2015*

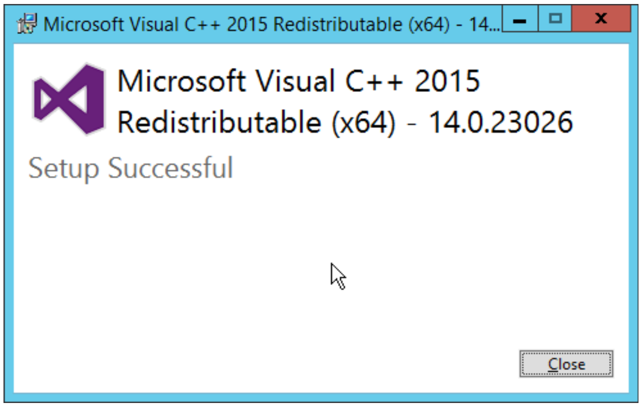
1. Run the **vcredist_x64** installer.



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



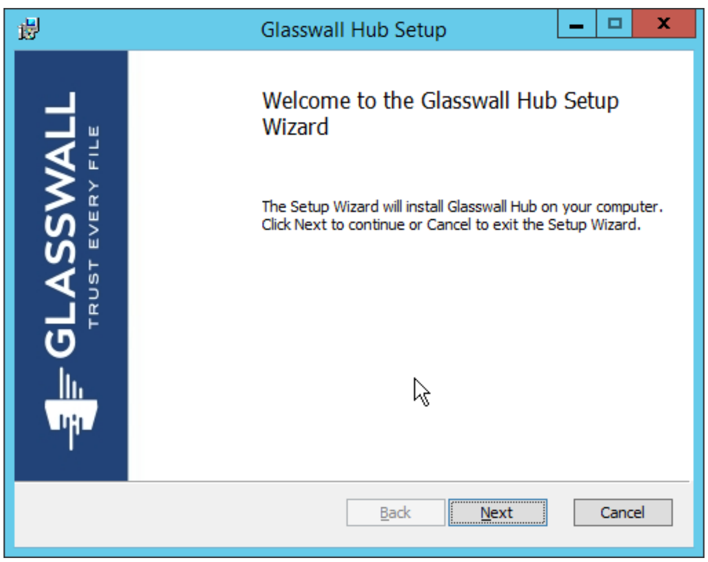
3. Click **Install.**
4. After the installation is complete, click **Close.**



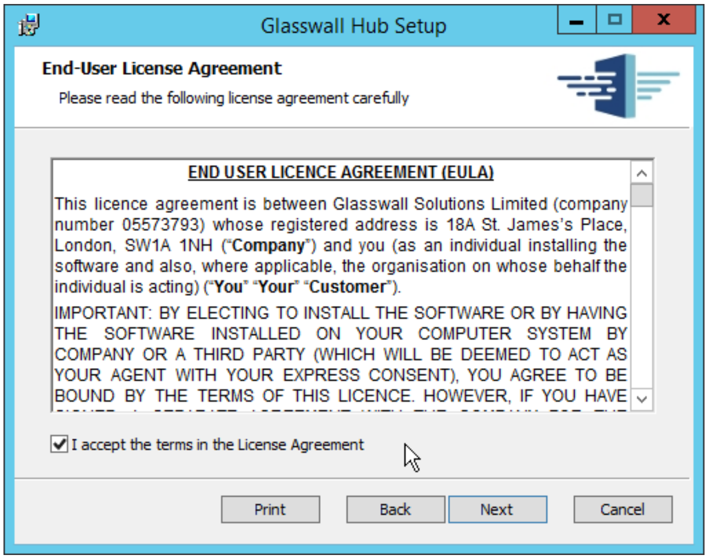
2.7.2 Install the Glasswall FileTrust Server Component

2.7.2.1 *Install Glasswall Hub*

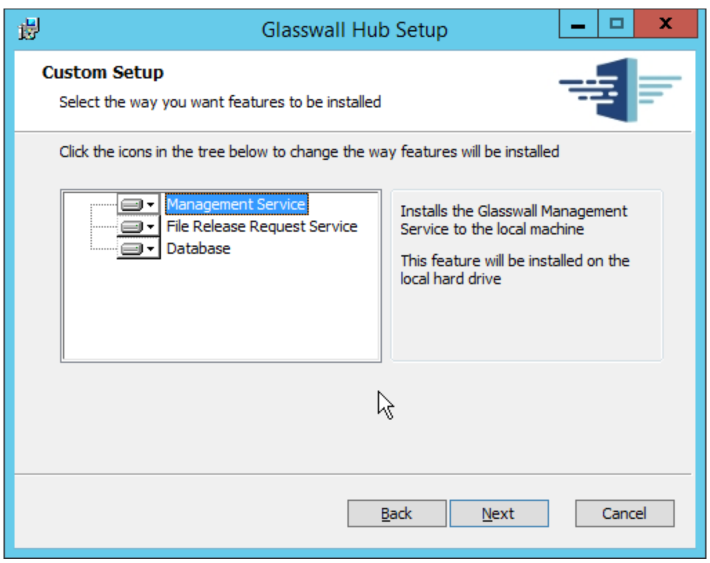
1. Run **HubInstaller.msi.**



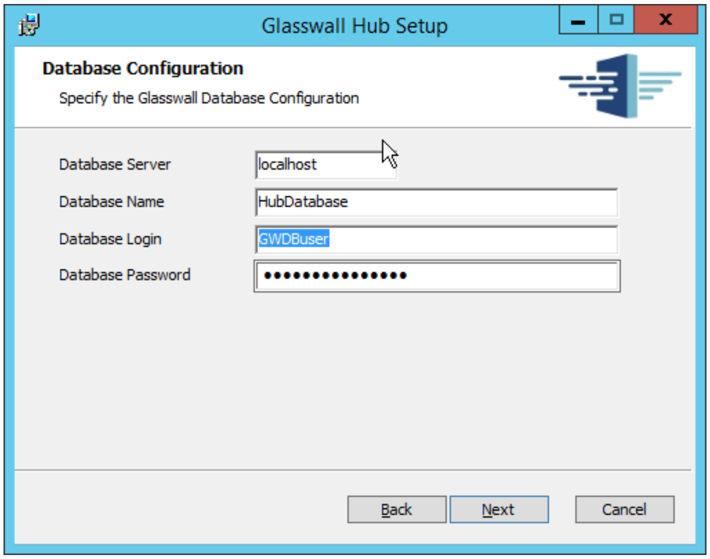
2. Click **Next.**



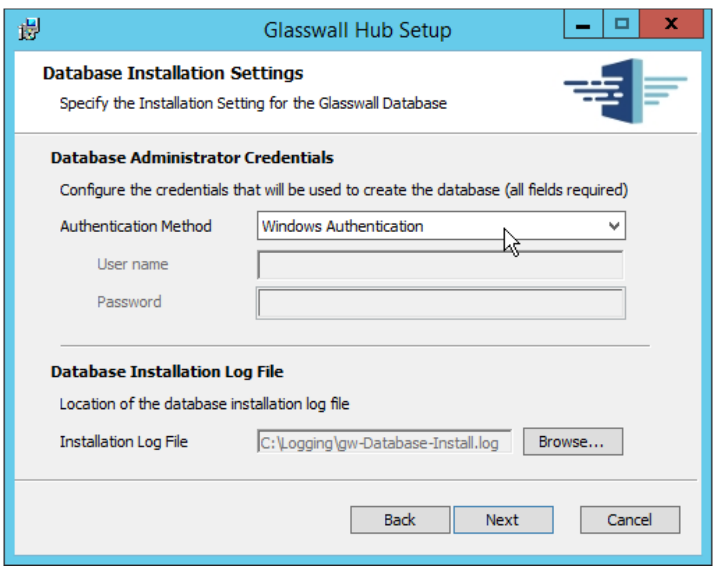
3. Check the box next to **I accept the terms in the License Agreement.**
4. Click **Next.**



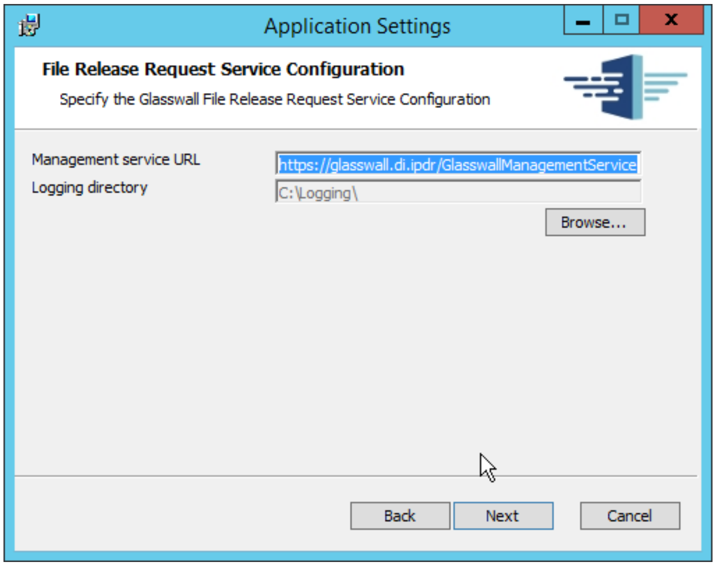
5. Click **Next.**
6. Enter **localhost** for the **Database Server**.
7. Enter **HubDatabase** for the **Database Name.**
8. Enter a **username** and **password** (and take note of these for later).



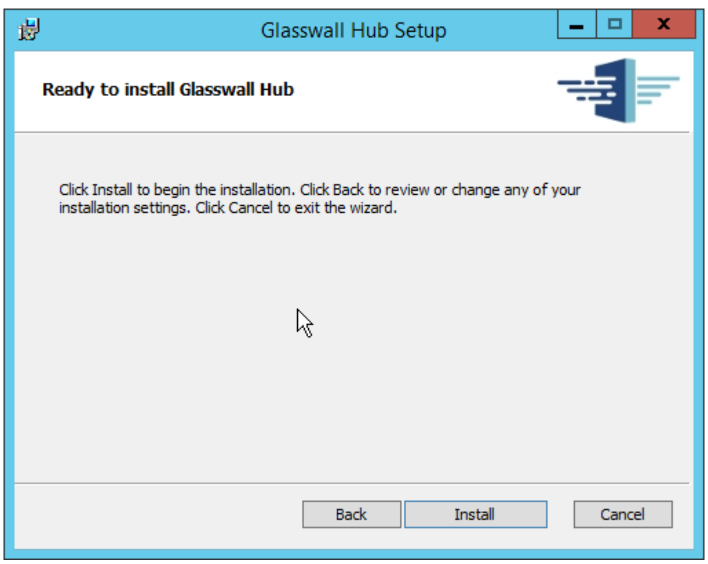
9. Click **Next.**
10. Select **Windows Authentication.**



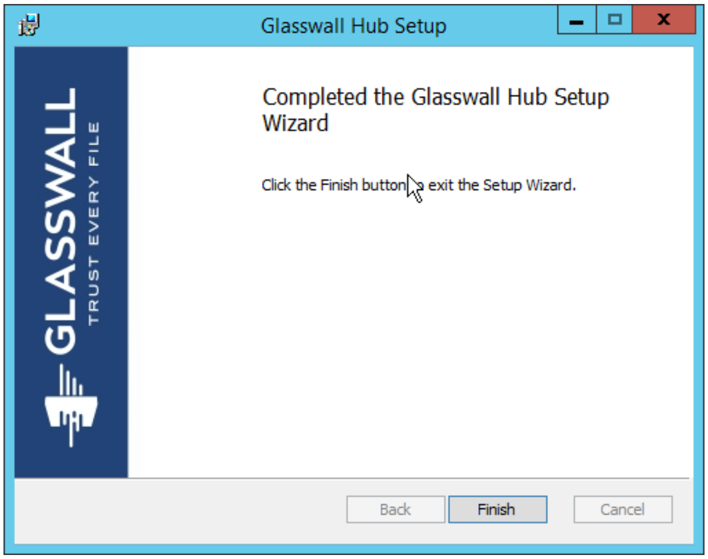
11. Click **Next.**
12. Replace the domain of the **management service URL** with the address of the current machine, such as **glasswall.di.ipdr.**



13. Click **Next.**



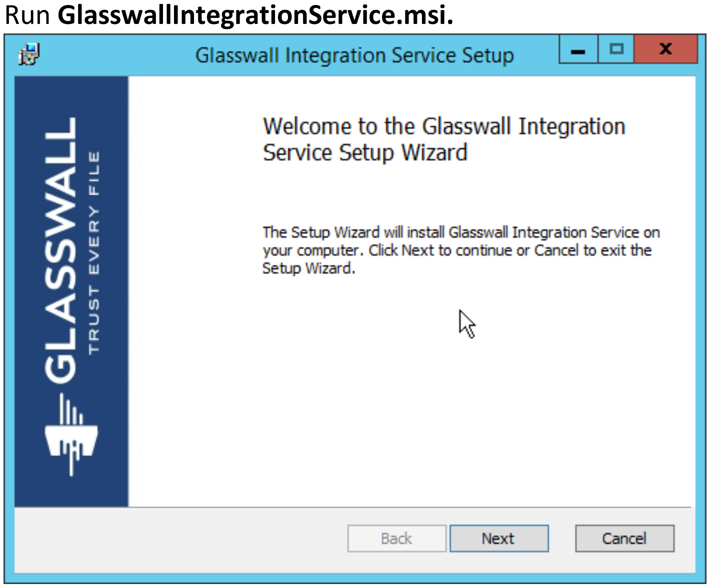
14. Click **Install.**



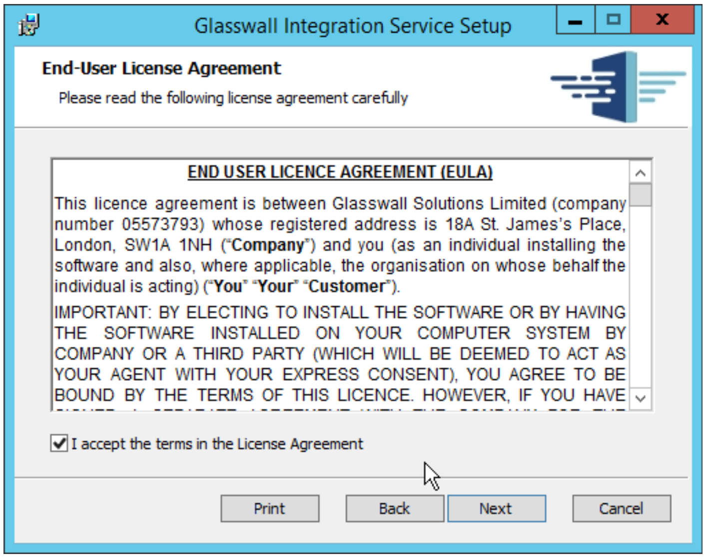
15. Click **Finish.**

2.7.2.2 *Install Glasswall Integration Service*

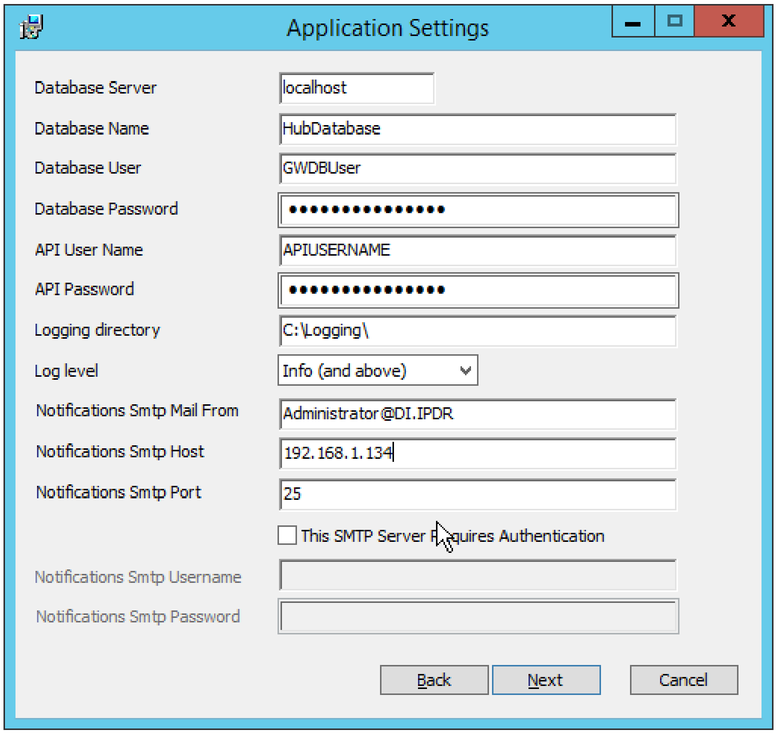
1. Run **GlasswallIntegrationService.msi.**



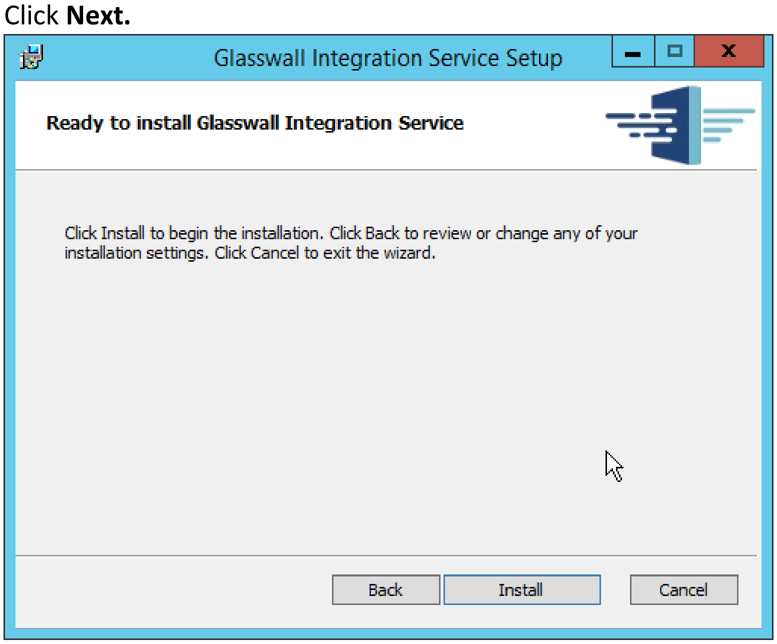
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**



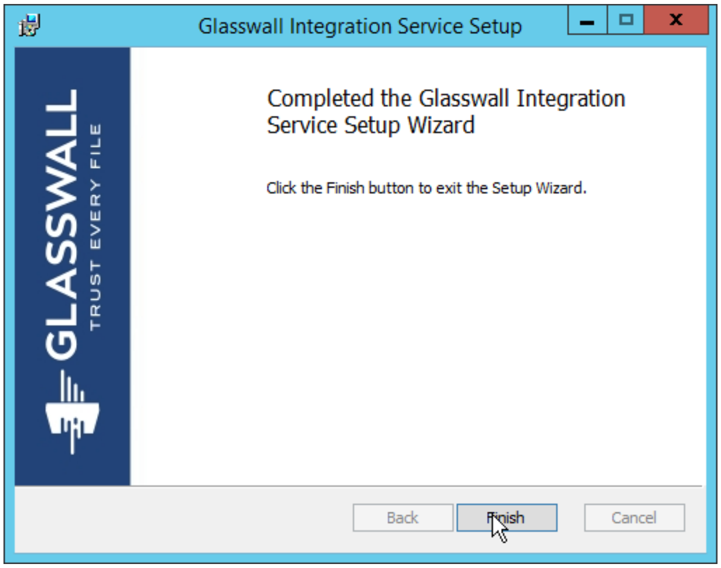
4. Click **Next.**
5. For **Database Server, Database Name, Database User,** and **Database Password,** enter the information entered in the **Glasswall Hub Installer.**
6. Create a **username** and **password** for **API User Name** and **API Password.**
7. Enter an email address to be used for notifications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



10. Click **Next.**



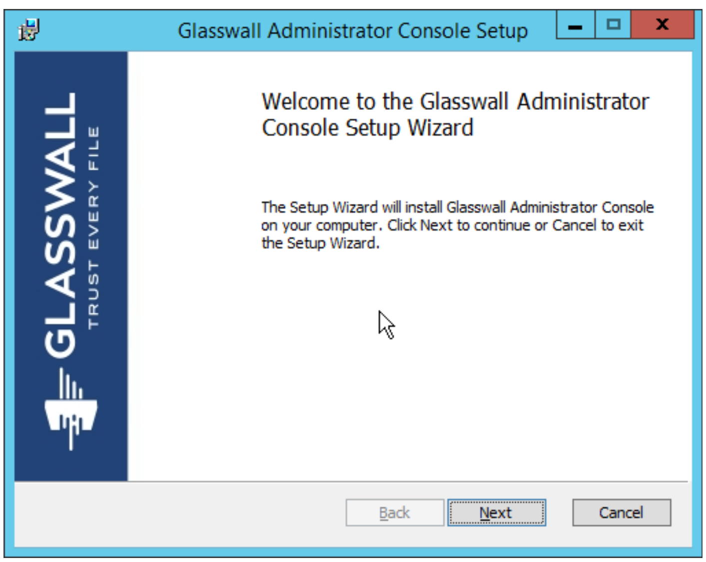
11. Click **Install.**



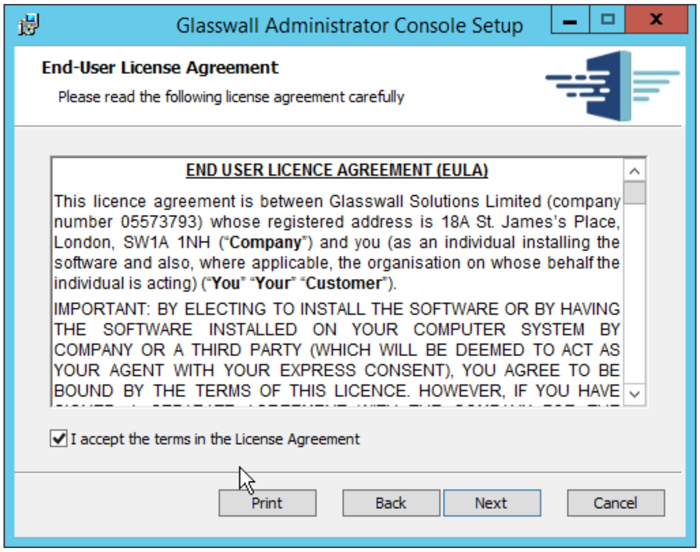
12. Click **Finish.**

2.7.2.3 *Install Glasswall Administrator Console*

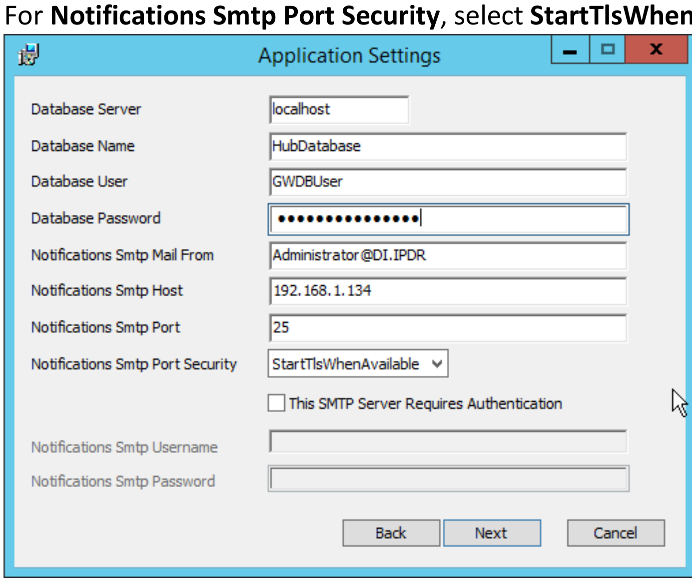
1. Run **AdministratorConsoleInstaller.msi.**



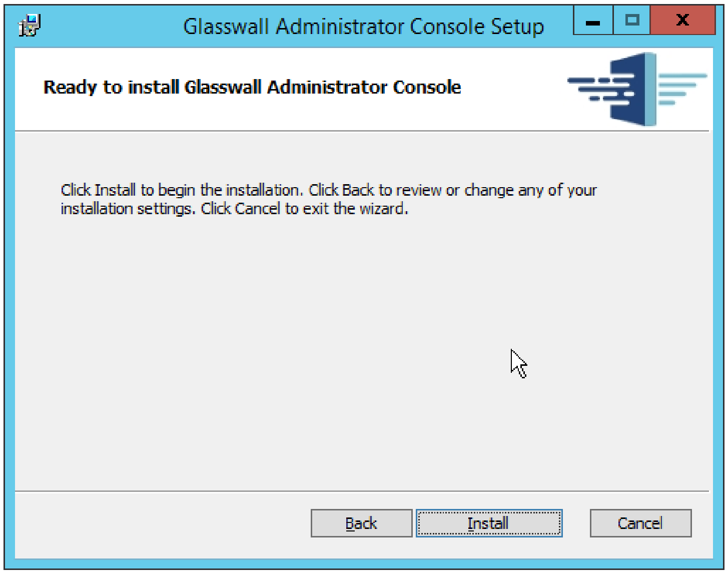
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**



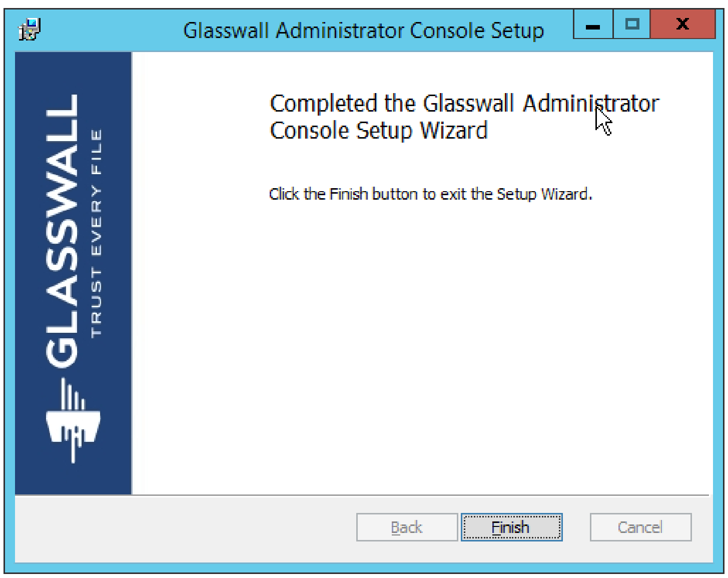
4. Click **Next.**
5. For **Database Server, Database Name, Database User,** and **Database Password,** enter the information entered in the **Glasswall Hub Installer.**
6. For **Notifications Smtp Mail From, Notifications Smtp Host, Notifications Smtp Port,** enter the information entered in the **Glasswall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



8. Click **Next.**



9. Click **Install.**

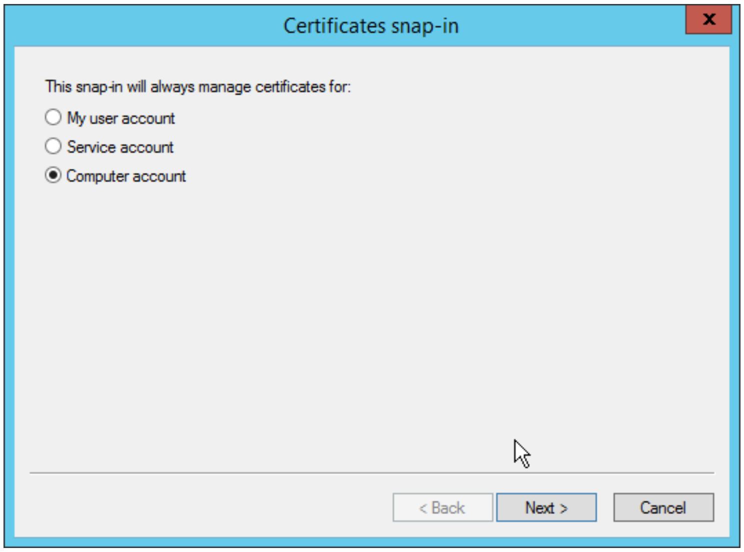


10. Click **Finish.**

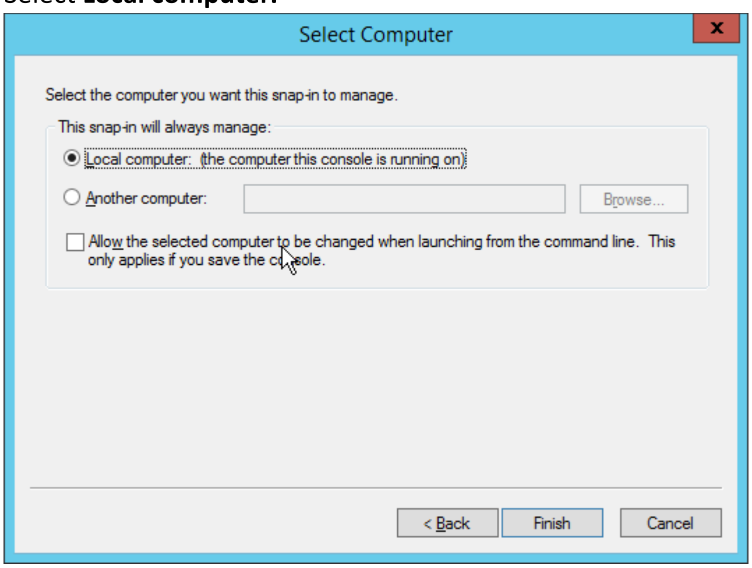
2.7.2.4 *Add the Server's Certificate*

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

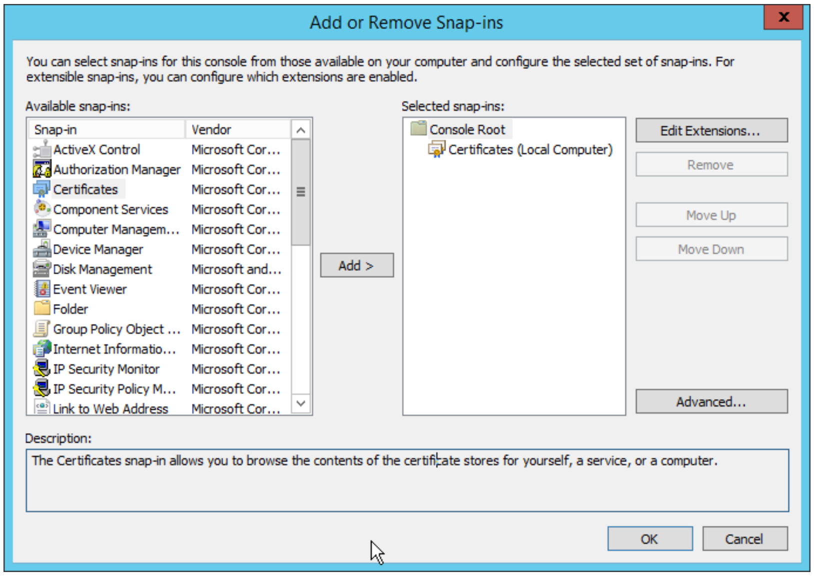
5. Select **Computer Account.**



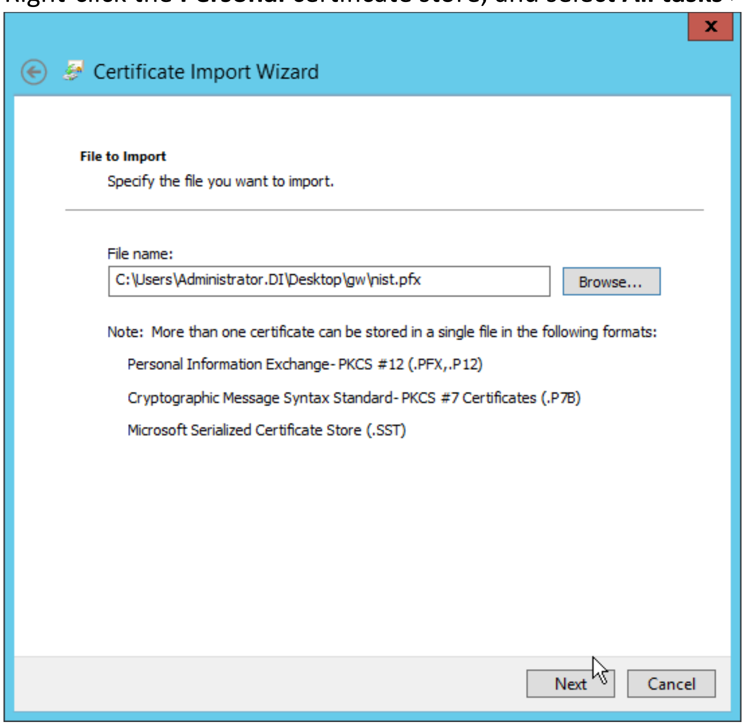
6. Click **Next.**
7. Select **Local computer.**



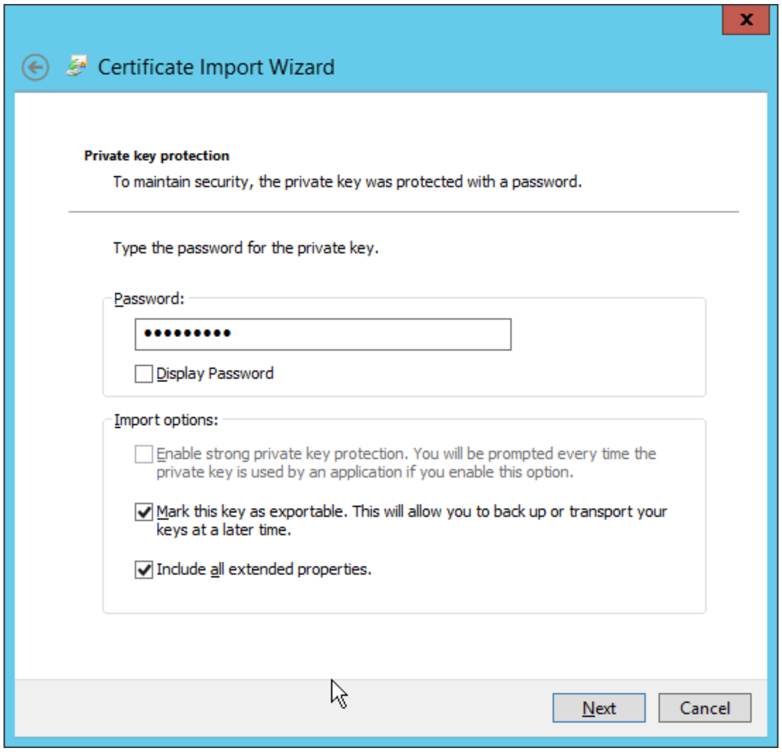
8. Click **Finish.**



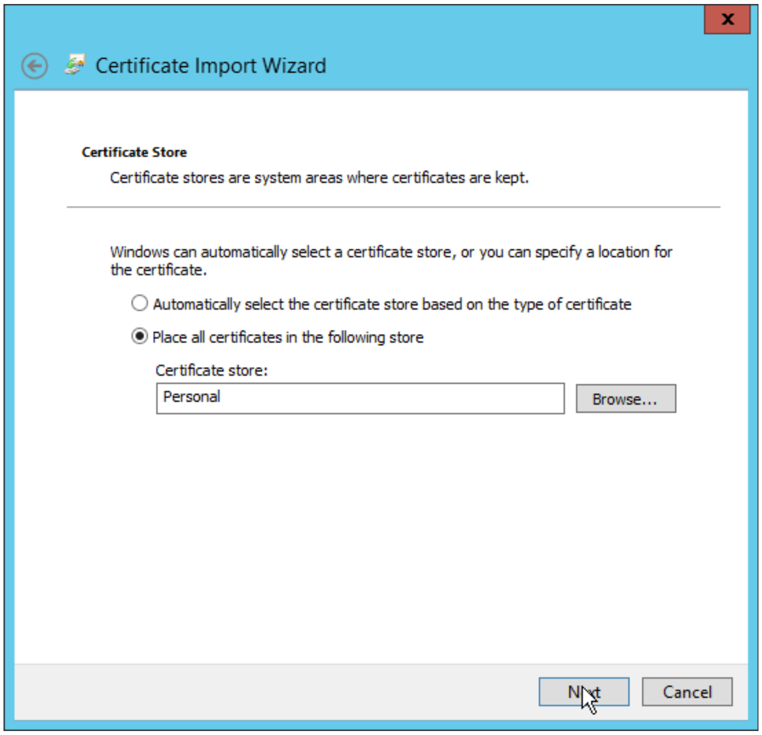
9. Click **OK.**
10. Right-click the **Personal** certificate store, and select **All tasks > Import….**



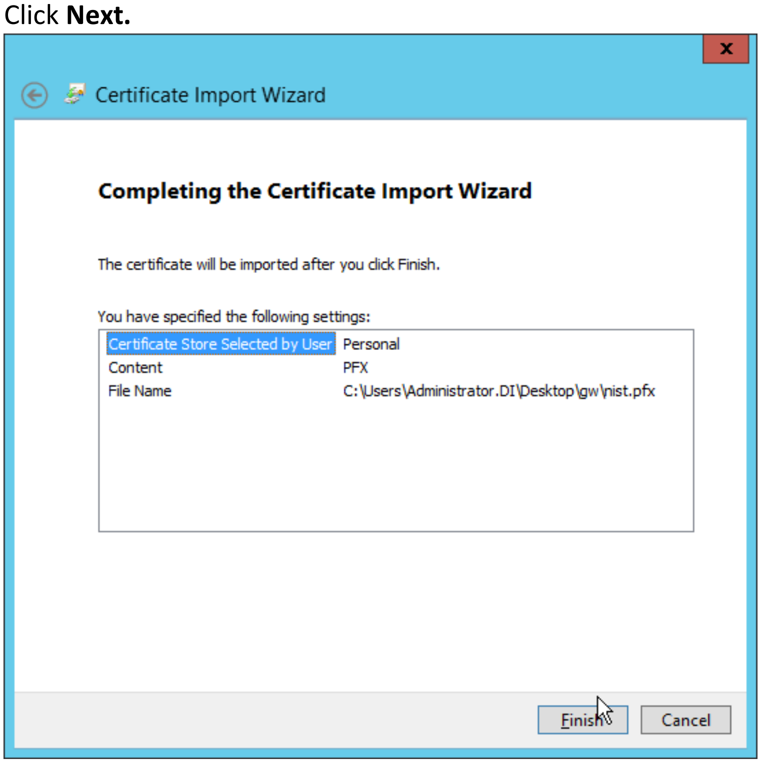
11. Enter the **file name** of the certificate.
12. Click **Next.**
13. Enter the **password** for the certificate.
14. Check the box next to **Mark this key as exportable.**



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

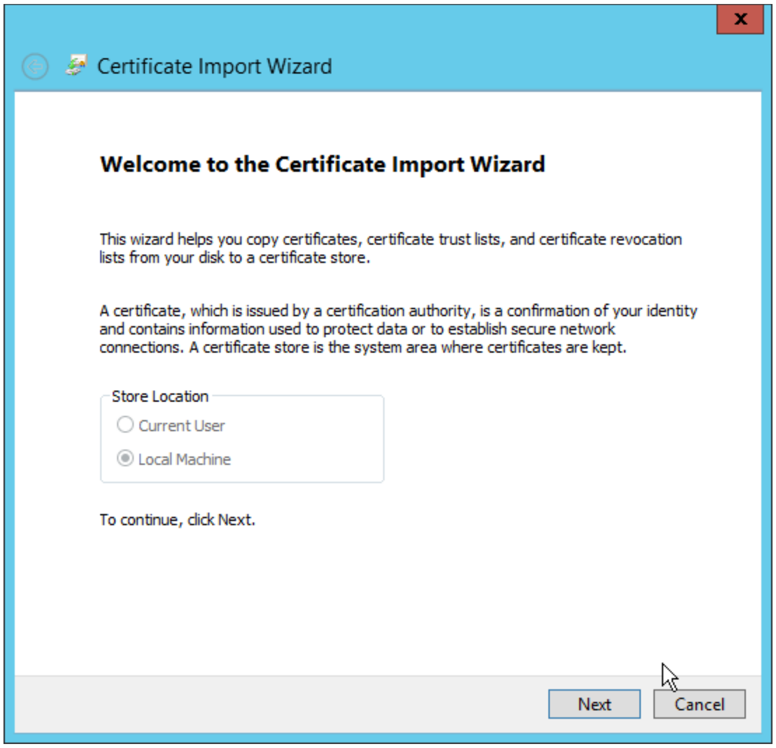


17. Click **Next.**

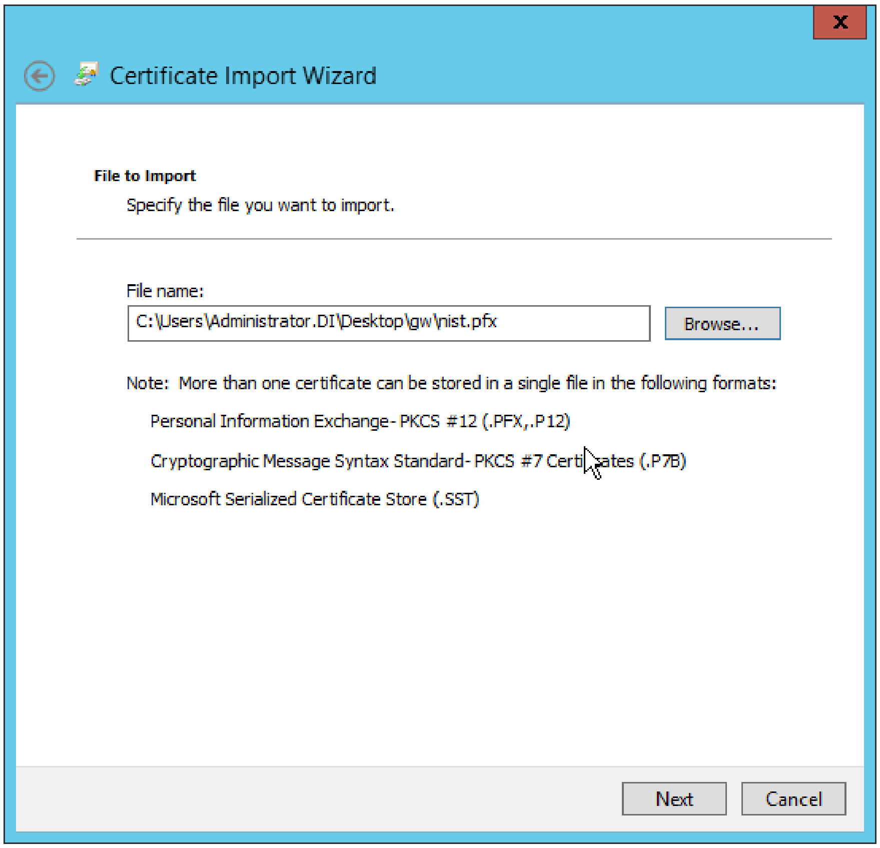


18. Click **Finish.**

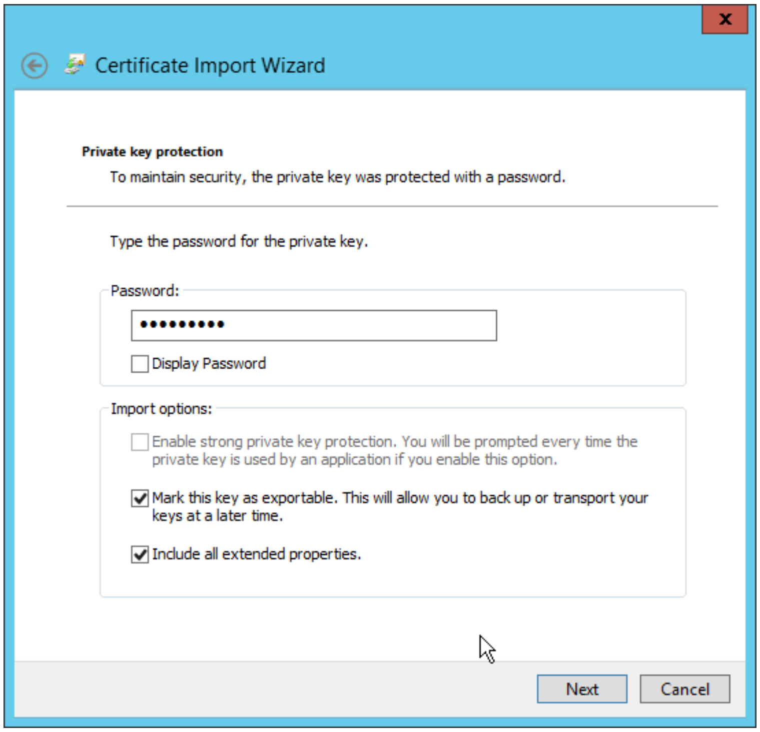
19. Re-open the certificate import wizard but this time for **Trusted Root Certification Authorities.**



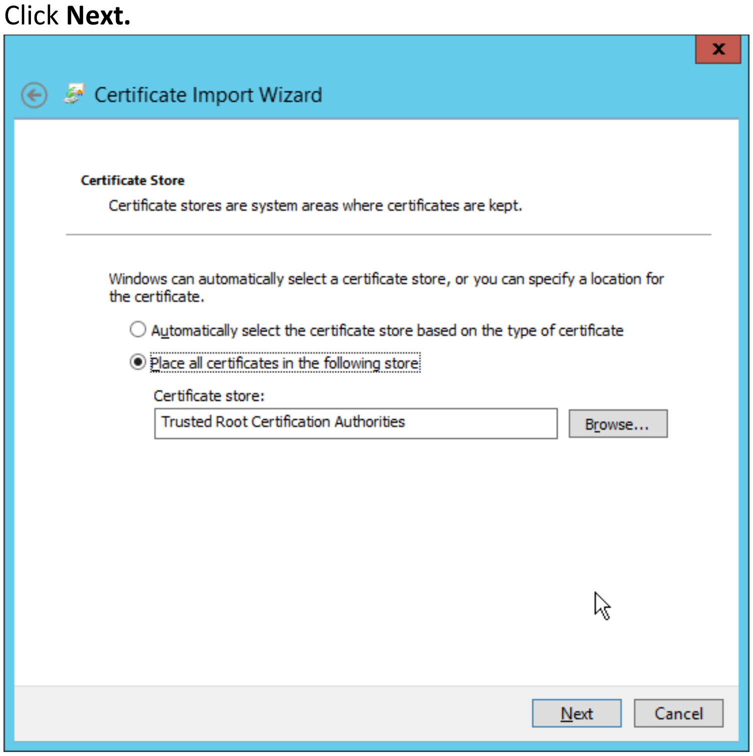
20. Click **Next.**
21. Select the same certificate.



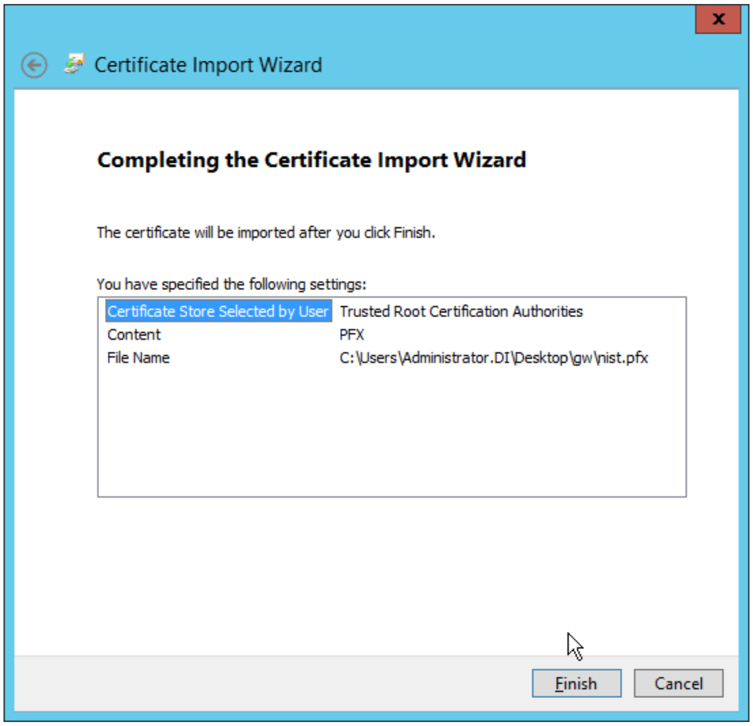
22. Click **Next.**
23. Enter the certificate's **password.**
24. Check the box next to **Mark this key as exportable.**



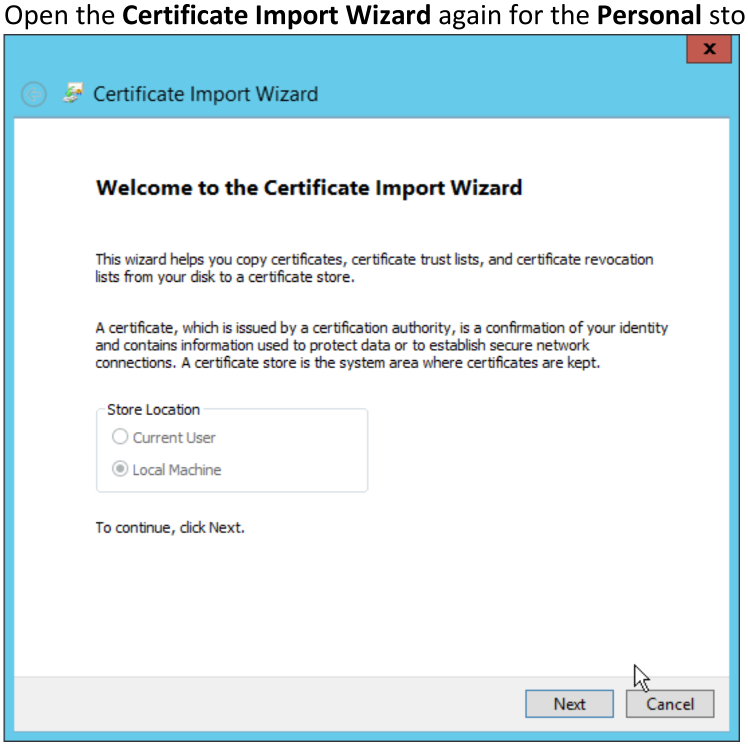
25. Click **Next.**



26. Click **Next.**

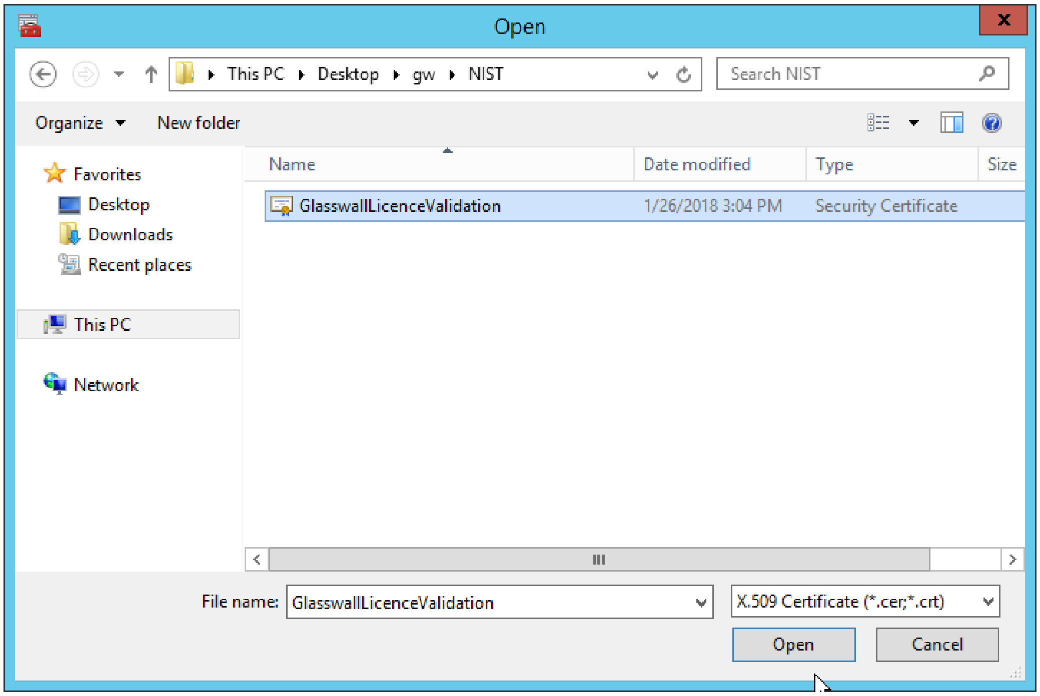


27. Click **Finish.**
28. Open the **Certificate Import Wizard** again for the **Personal** store**.**



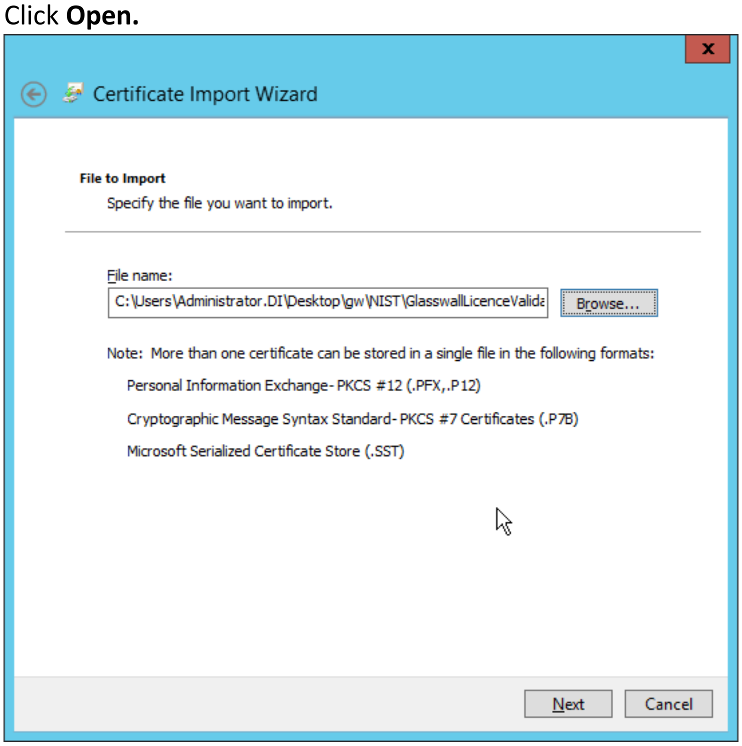
1047 29. Click **Next.**

1048 30. Browse to the **GlasswallLicenseValidation** certificate.



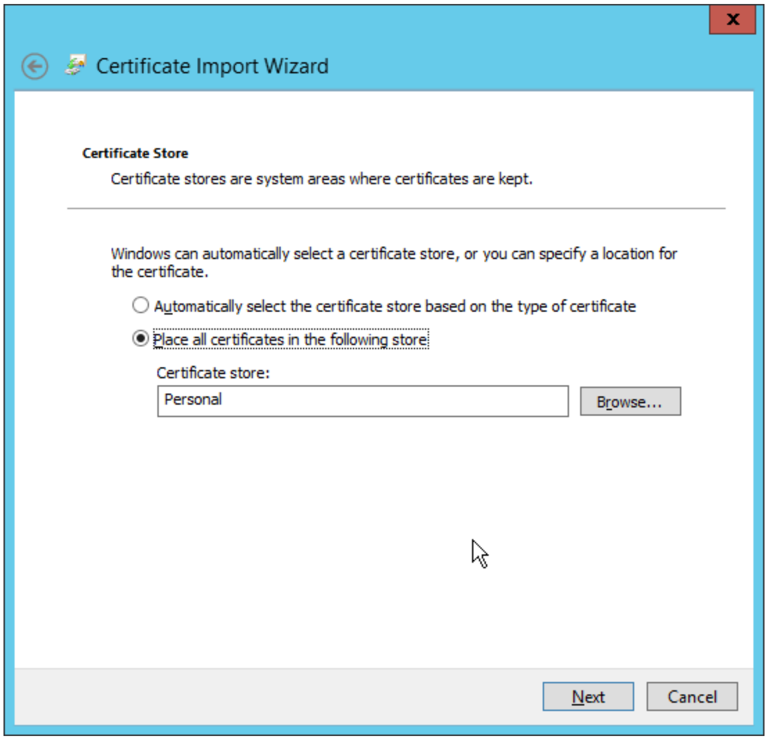
1049

1050 31. Click **Open.**



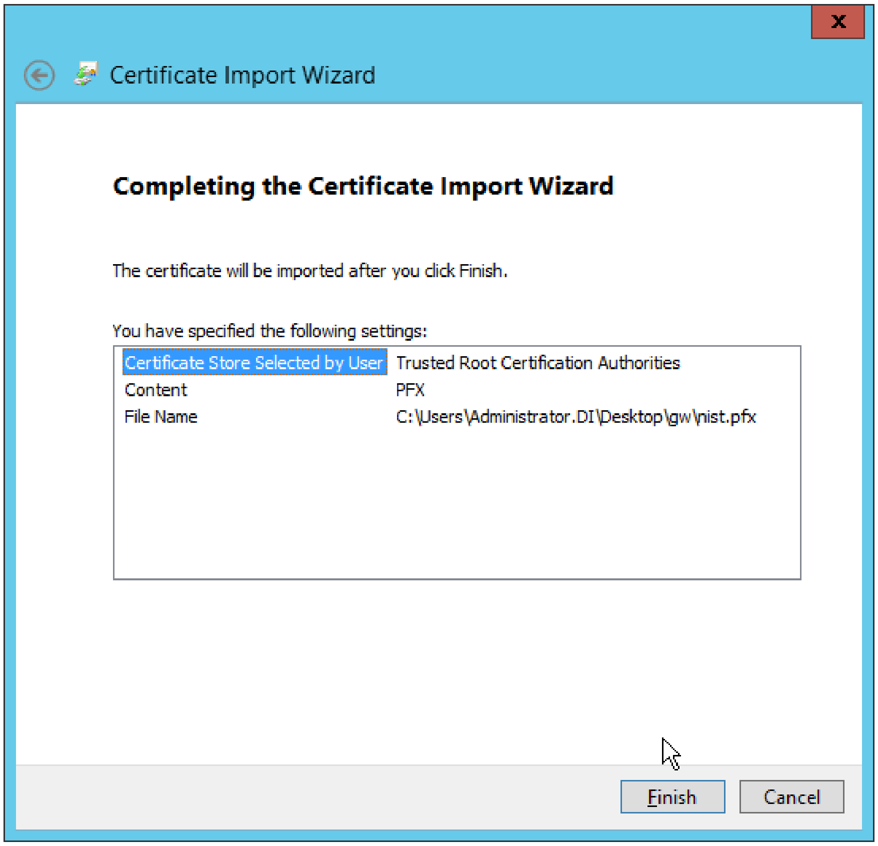
1051

1052 32. Click **Next.**

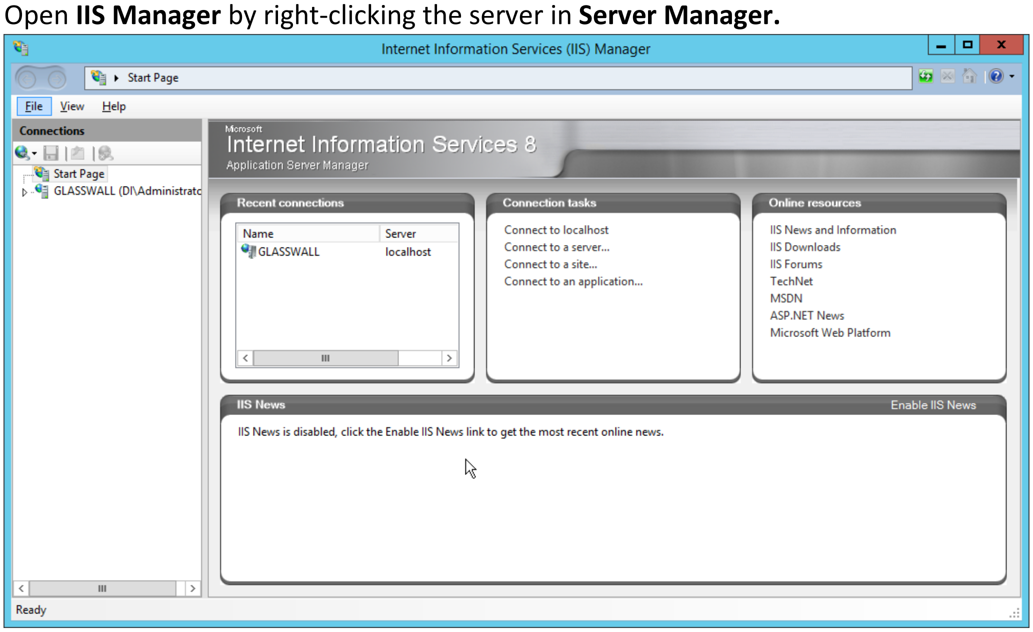


1053

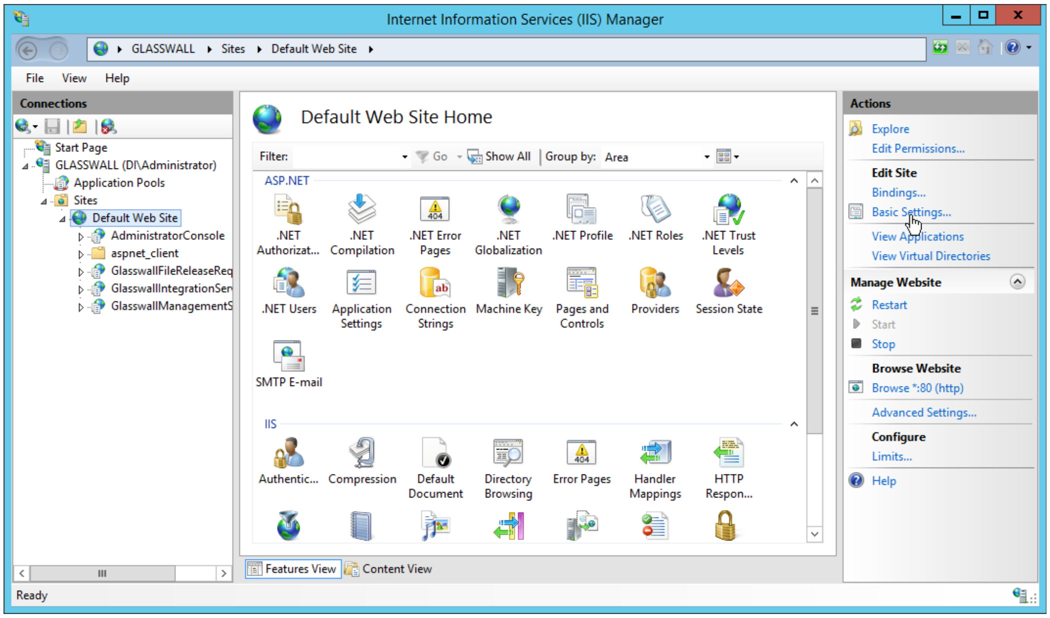
1054 33. Click **Next.**



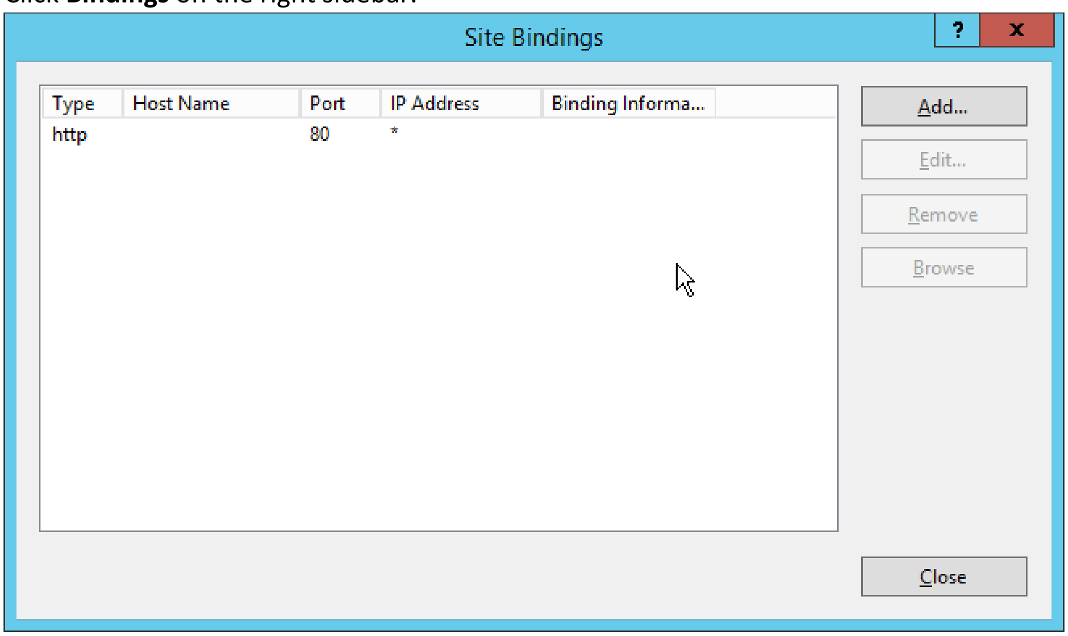
34. Click **Finish.**
35. Open **IIS Manager** by right-clicking the server in **Server Manager.**



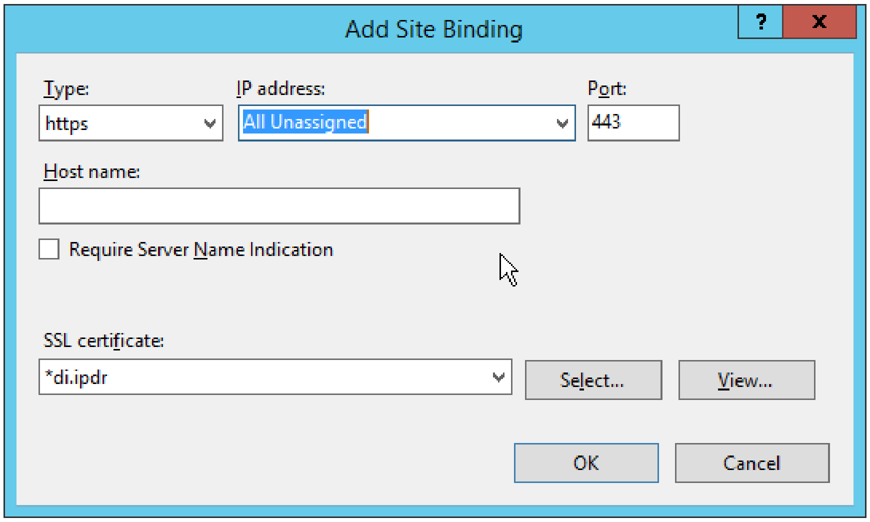
36. Navigate to the **Default Website** in the tree.



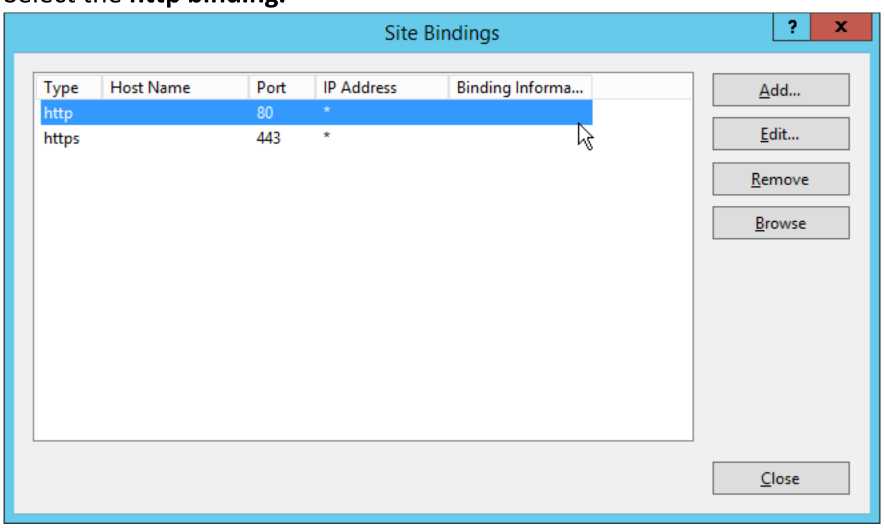
37. Click **Bindings** on the right sidebar.



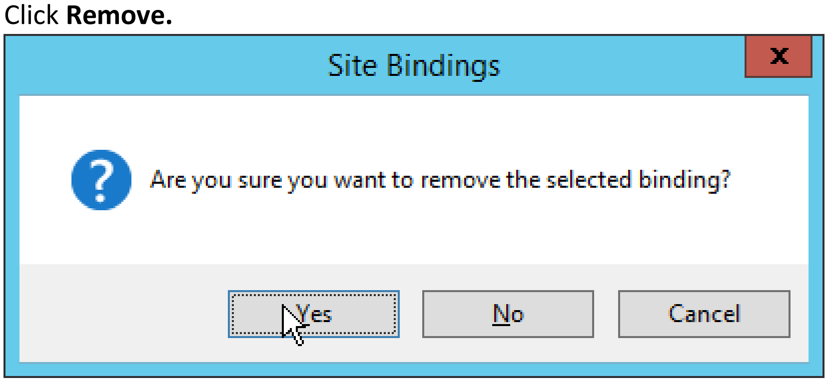
38. Click **Add.**
39. Select **https** for the **Type.**
40. Select **All Unassigned** for **IP address.**
41. Select the **domain certificate** for **SSL certificate.**



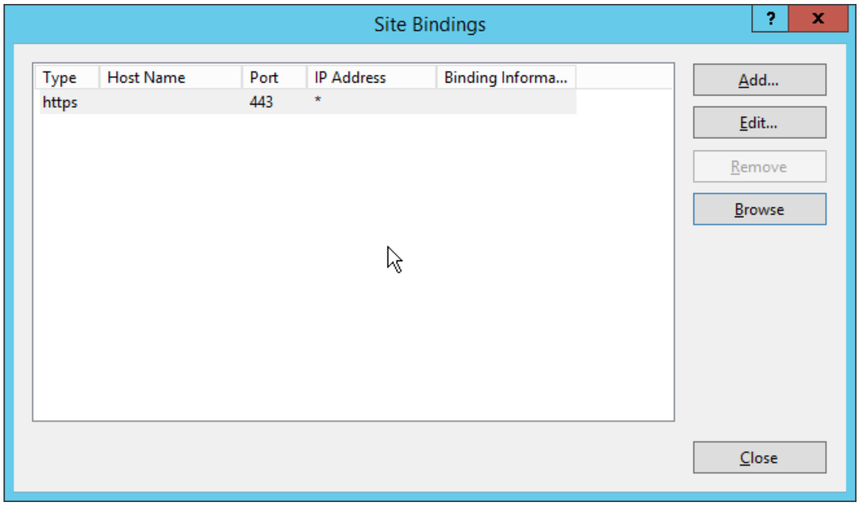
42. Click **OK.**
43. Select the **http binding.**



44. Click **Remove.**



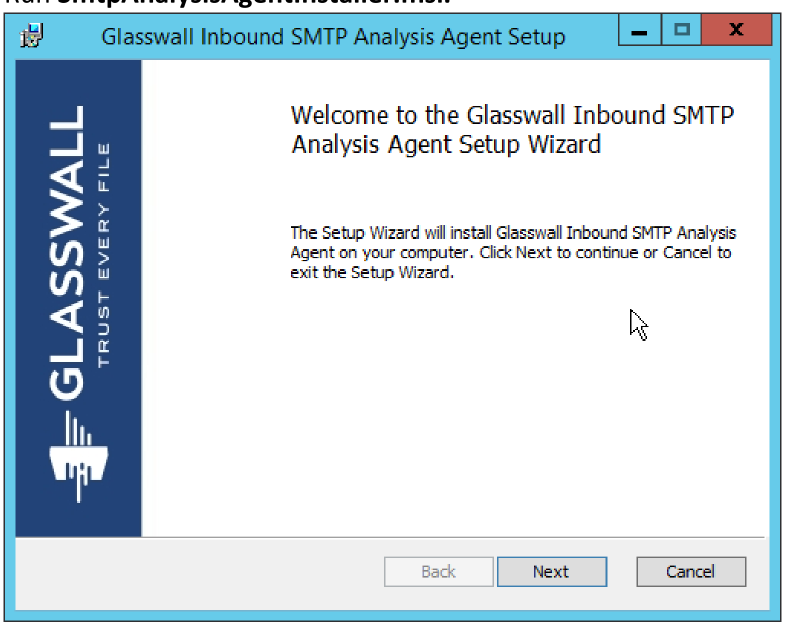
45. Click **Yes.**



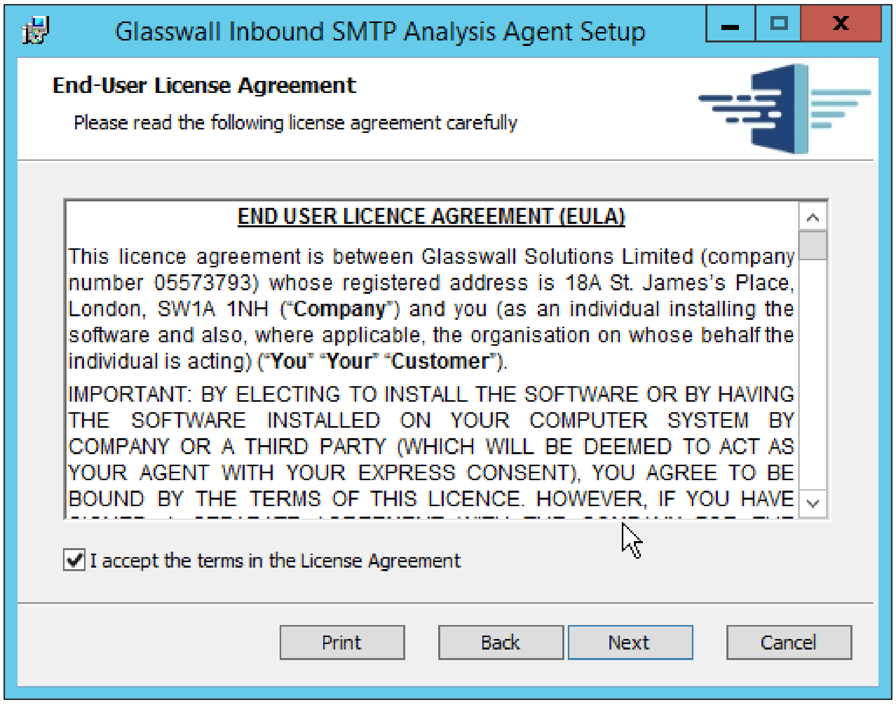
46. Click **Close.**
47. Restart the IIS server. The Glasswall FileTrust console should now be accessible through a browser. (For example, https://glasswall.di.ipdr/AdministratorConsole). Ensure that there are no certificate errors.

2.7.2.5 *Install the Smtp Analysis Agent*

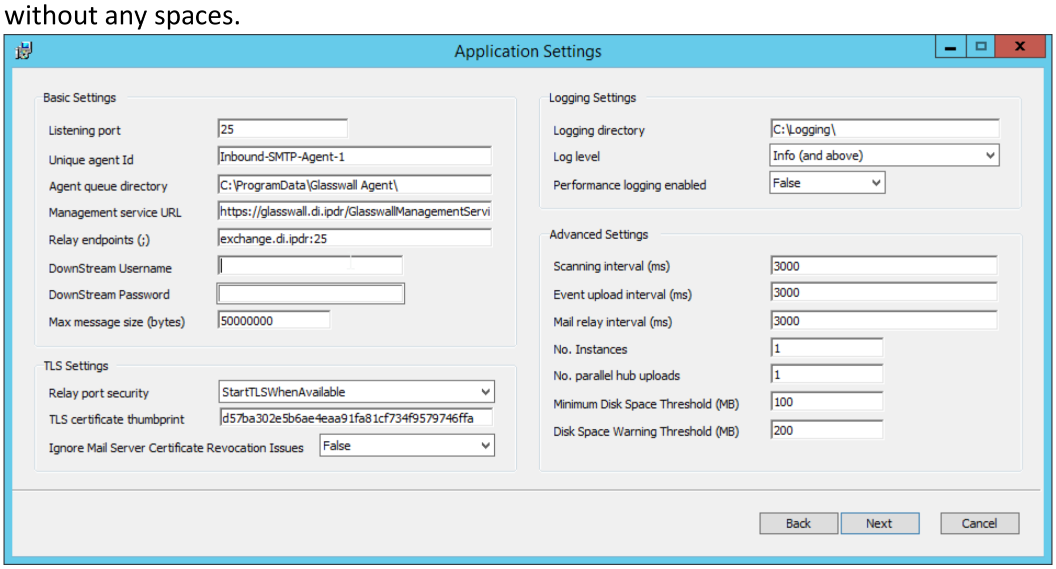
1. Run **SmtpAnalysisAgentInstaller.msi.**



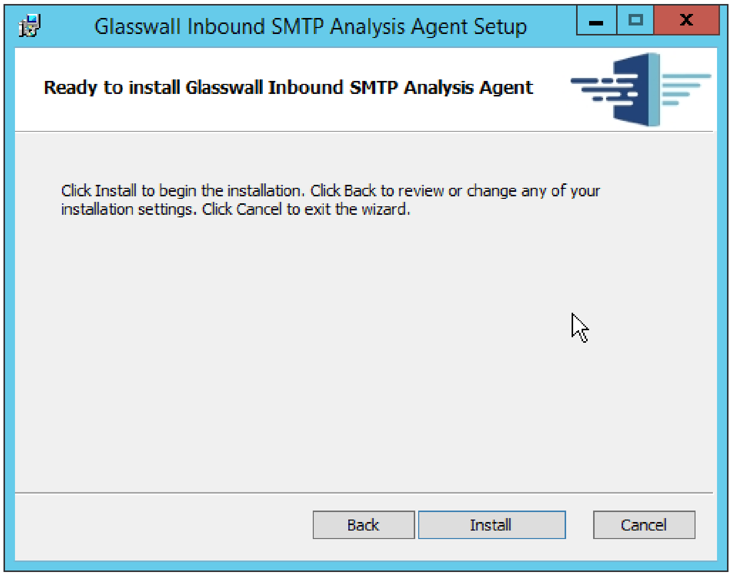
2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**



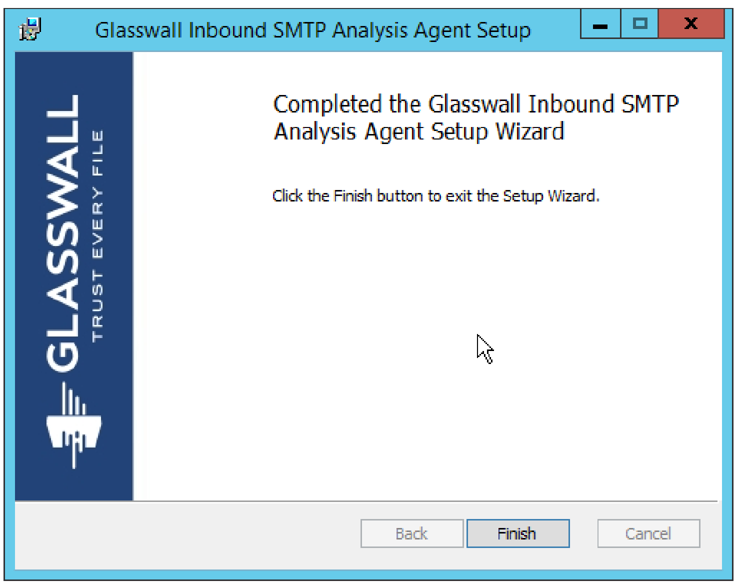
4. Click **Next.**
5. For **Listening** port, enter **25.**
6. For **Management service URL,** correct the domain to be the web domain of the IIS server (for example, glasswall.di.ipdr).
7. For the **Relay endpoints,** enter the address of the Exchange server, followed by the port (for example, exchange.di.ipdr:25).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



9. Click **Next.**



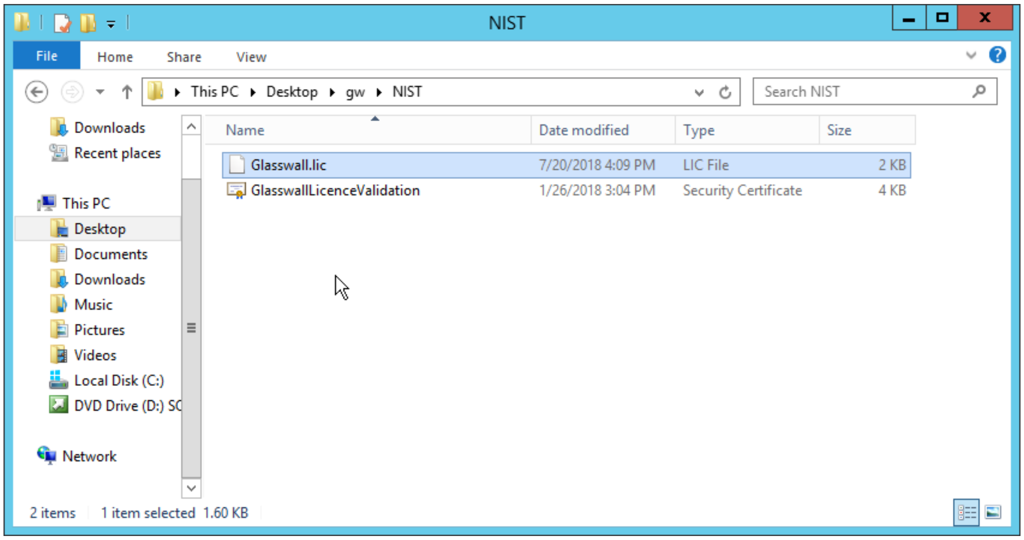
10. Click **Install.**



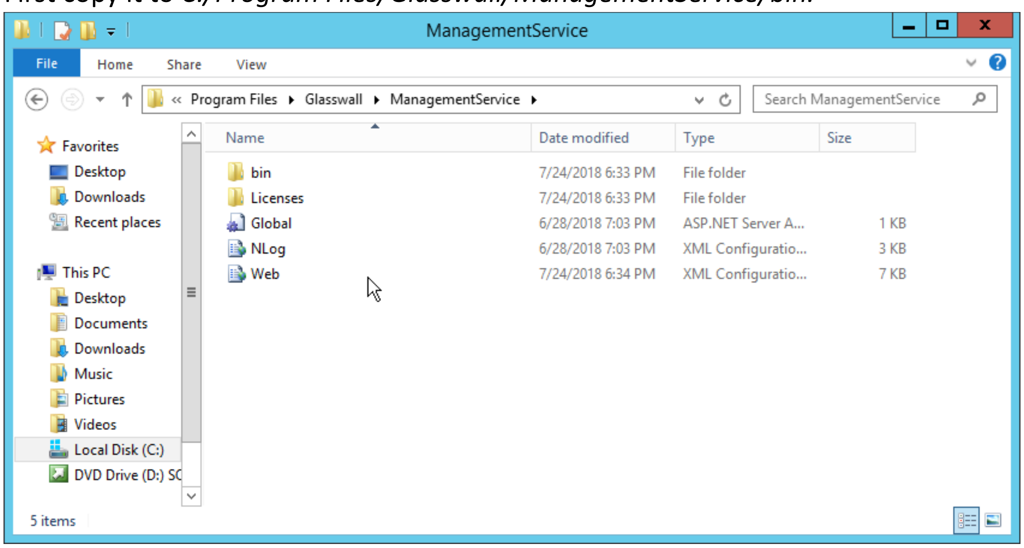
11. Click **Finish.**

2.7.2.6 *Distribute the Glasswall License File*

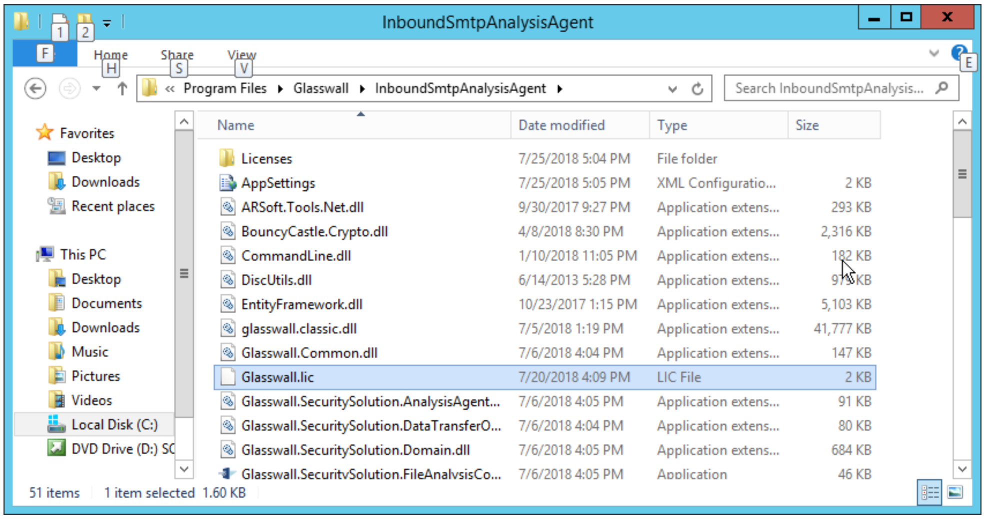
1. Copy the **Glasswall License** file to the following locations, assuming **Glasswall** was installed to *C:/Program Files/Glasswall.*



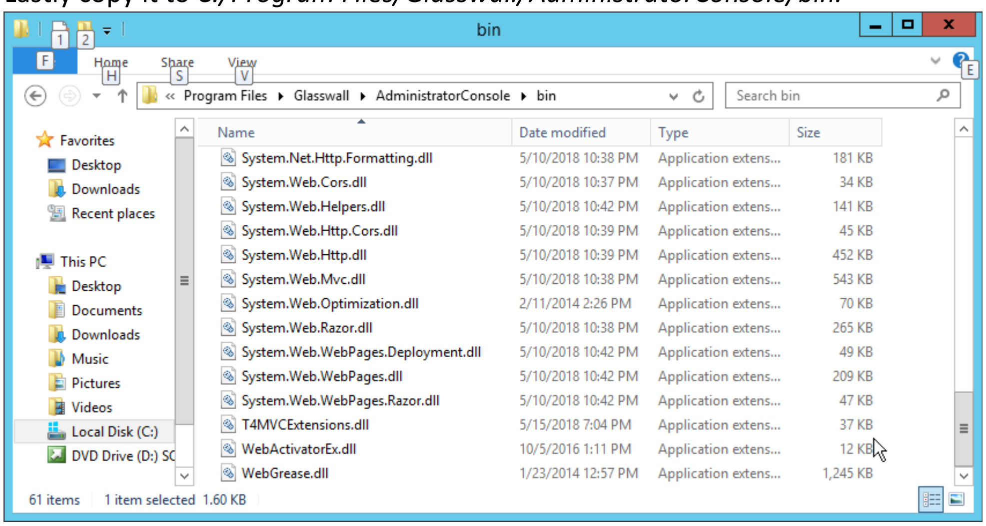
2. First copy it to *C:/Program Files/Glasswall/ManagementService/bin.*



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



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



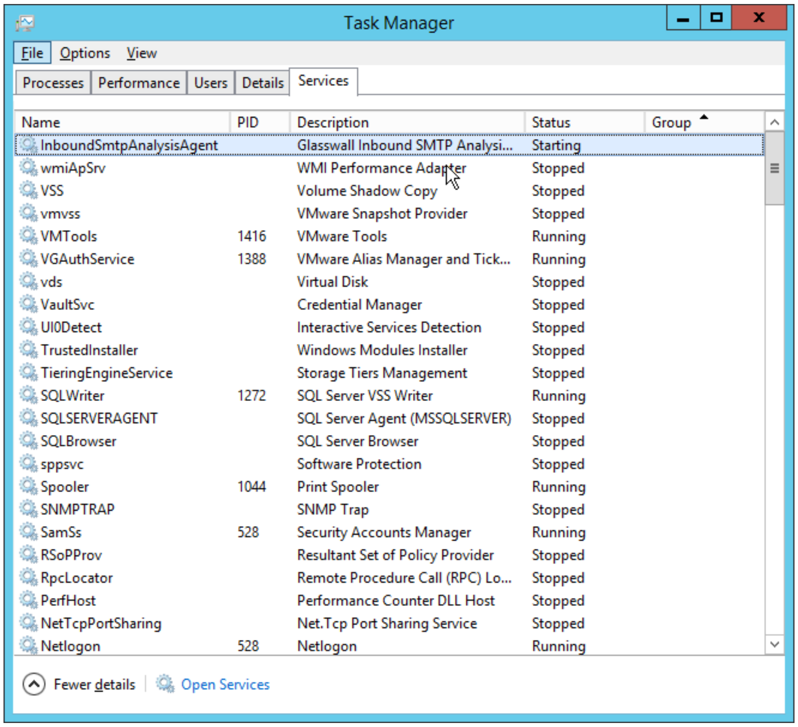
2.7.3 Configure Glasswall FileTrust

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

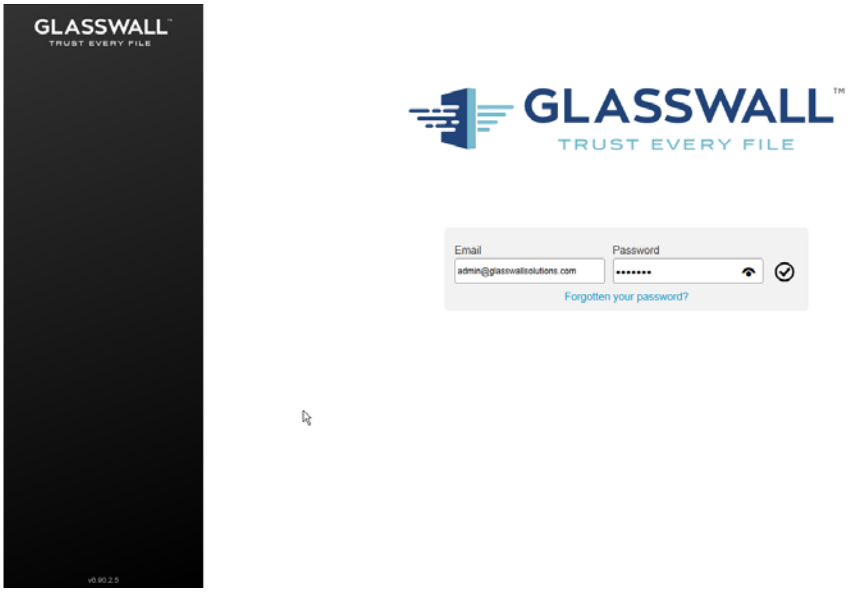
Instead, to achieve the goal of routing email through Glasswall, we redirect local MX records to Glasswall FileTrust. We implemented it this way because of limitations of the lab environment, but organizations should consult with the vendor for the best solution to route email through the email sanitization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

2.7.3.1 *Create a New Administrator Account*

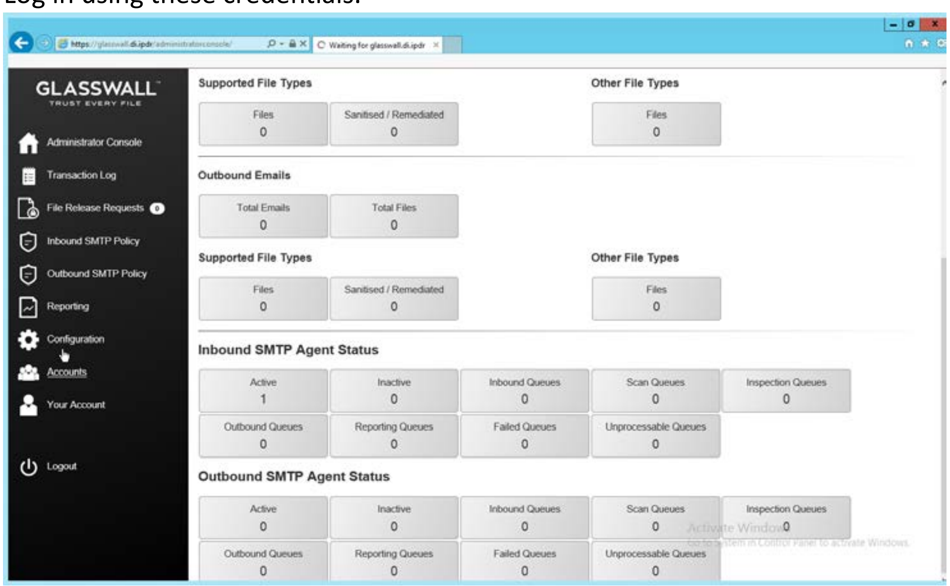
1. Open **Task Manager.**
2. In the **Services** tab, start the **InboundSmtpAnalysisAgent** service.



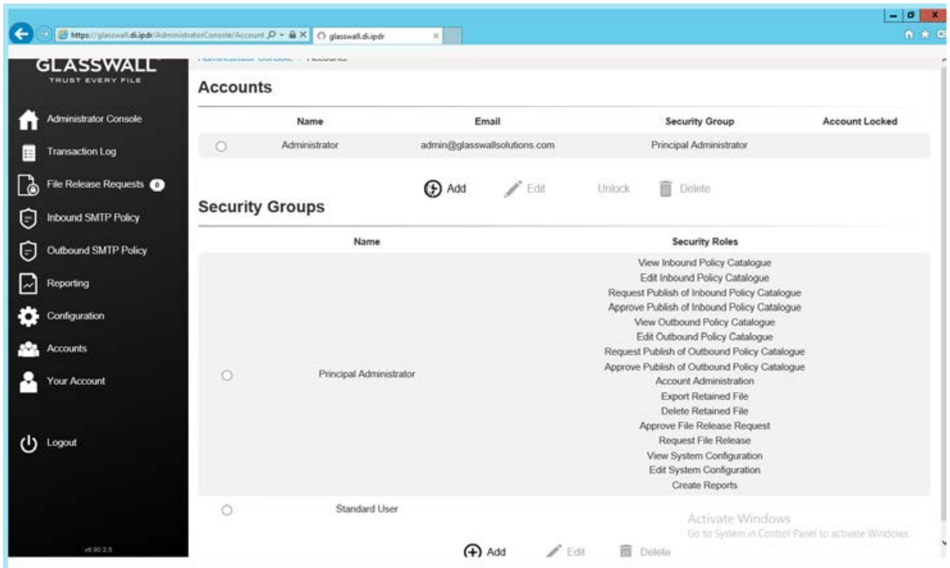
3. Close **Task Manager.**
4. Open a browser and navigate to the **Glasswall Administration Console** (for example, http://glasswall.di.ipdr/AdministratorConsole).
5. If this is the first time logging in, the default account will be **admin@glasswallsolutions.com,** and the password is **Welcome1?**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



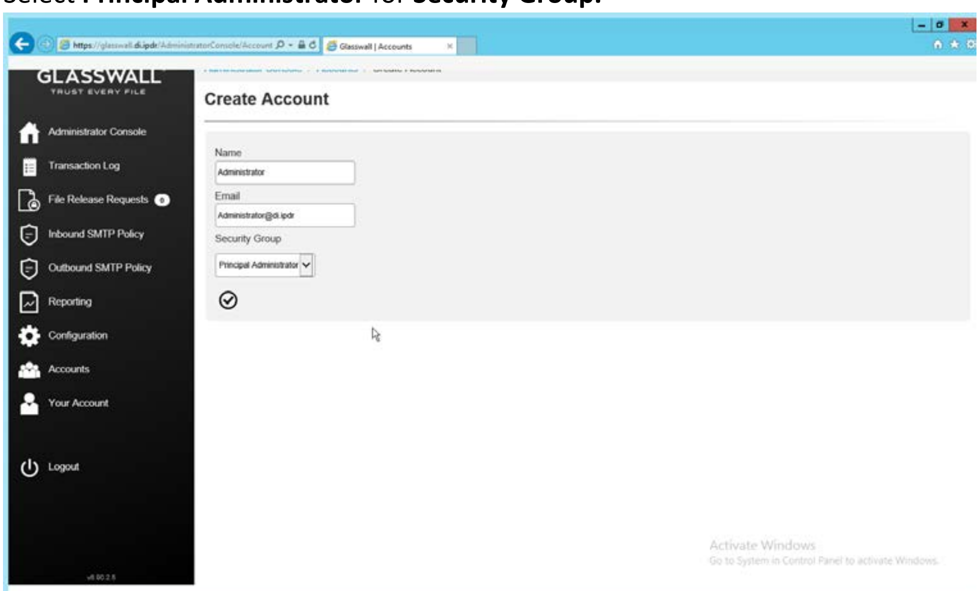
6. Log in using these credentials.



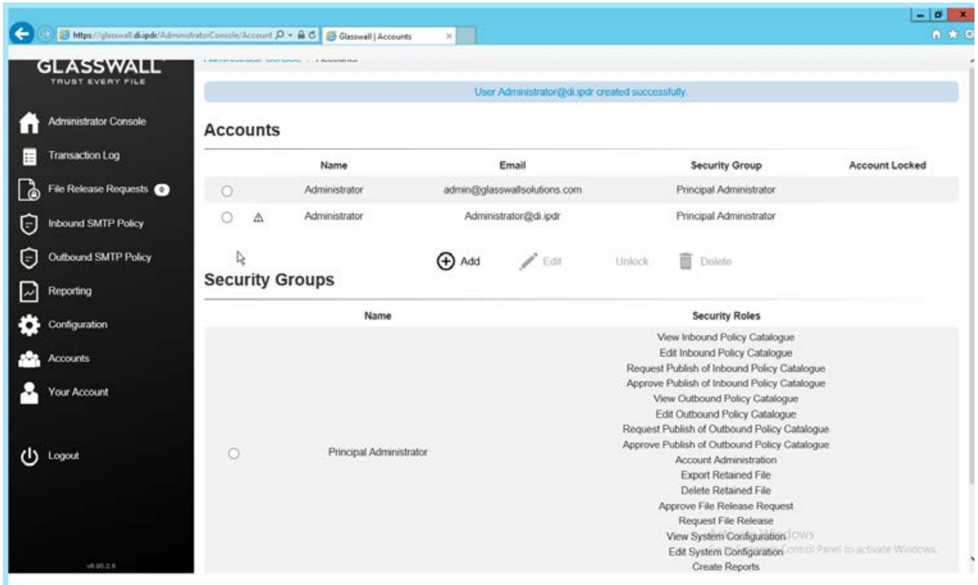
7. On the left sidebar, click **Accounts.**



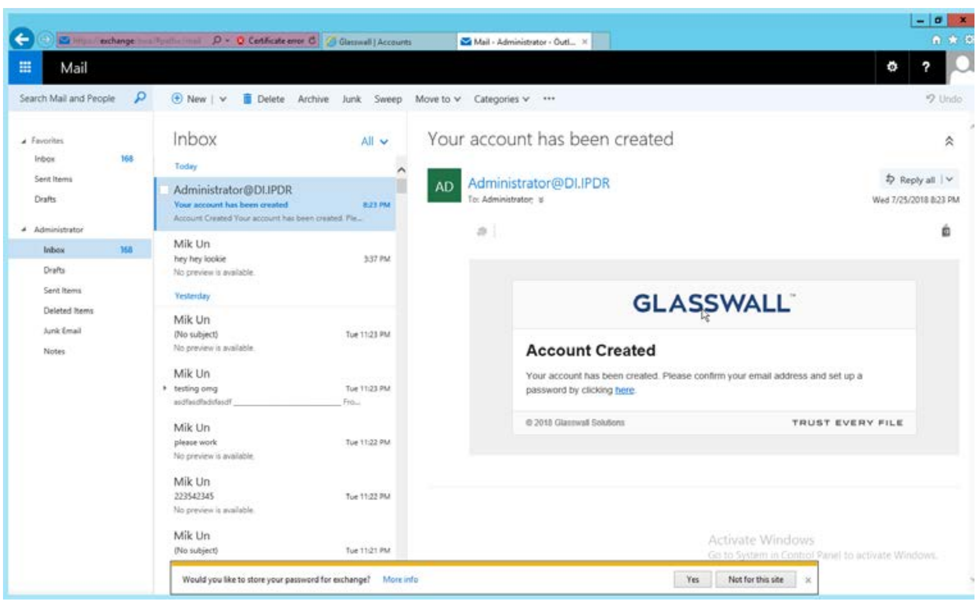
8. Under **Accounts**, click **Add.**
9. Enter the **name** and **email address** of an administrator account from the email server.
10. Select **Principal Administrator** for **Security Group.**



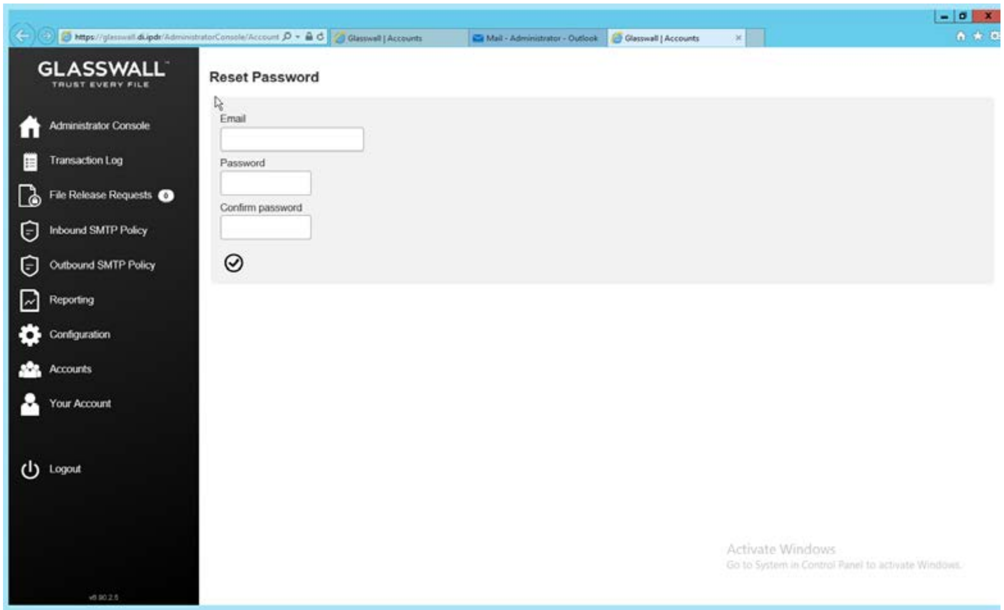
11. Click the **checkmark** button when finished.



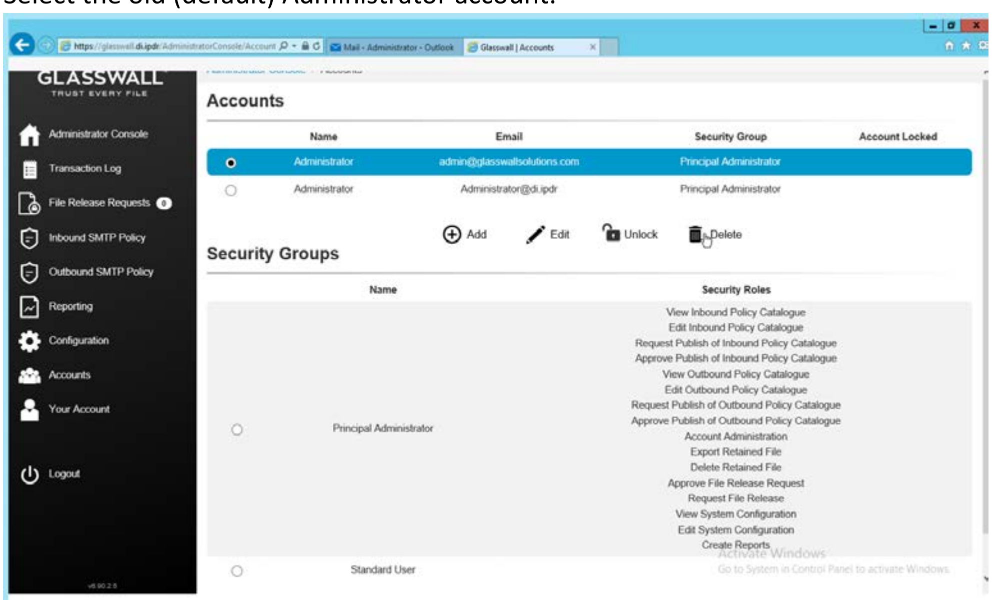
12. The new administrator account should be created.



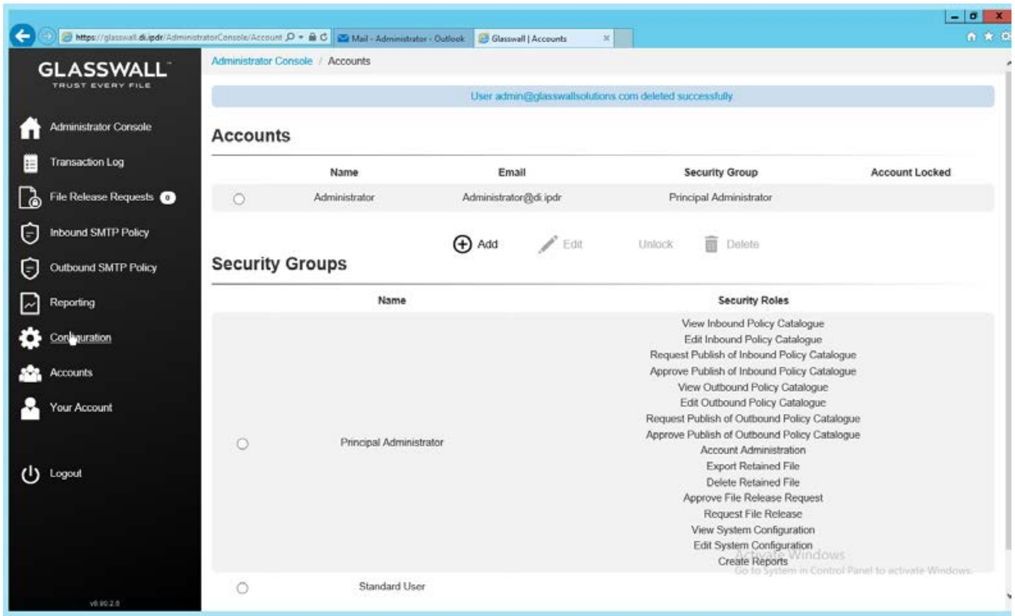
13. Check the email inbox of the specified email address for a confirmation email, and click the link in the email.



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



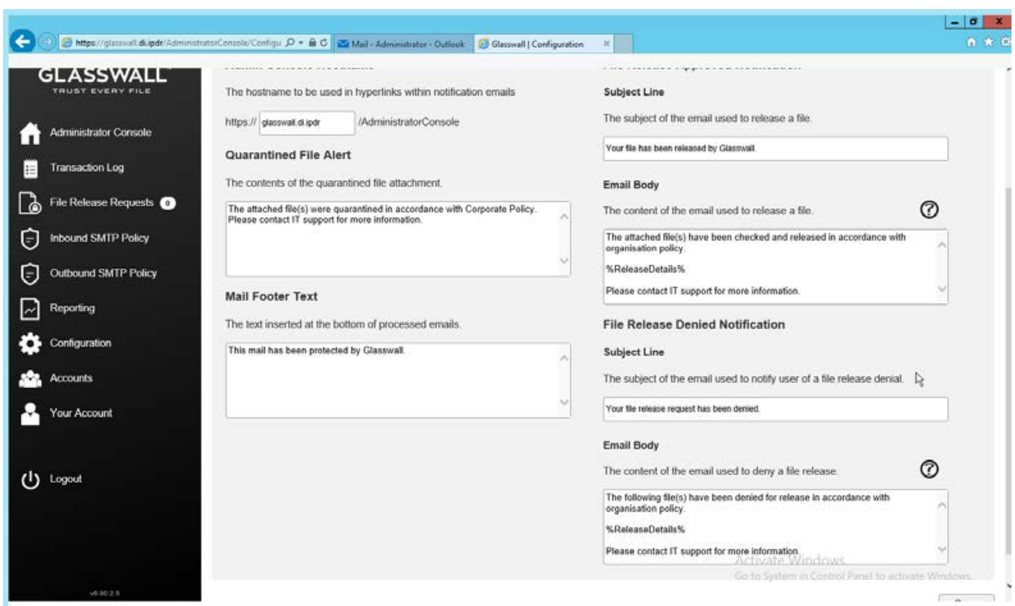
17. Click **Delete.**



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

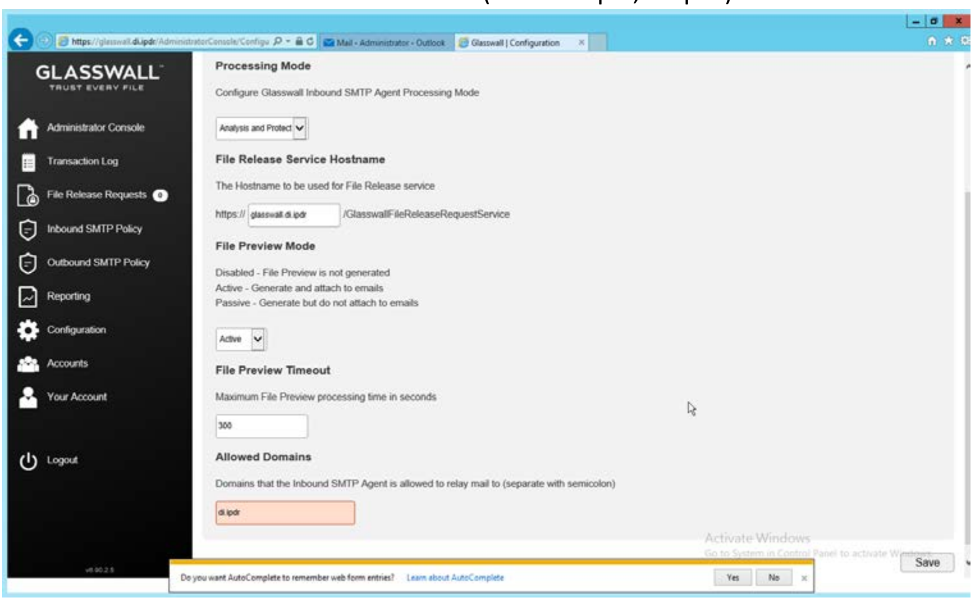
2.7.3.2 *Configure Notifications and Policies*

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



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

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



9. Click **Save.**

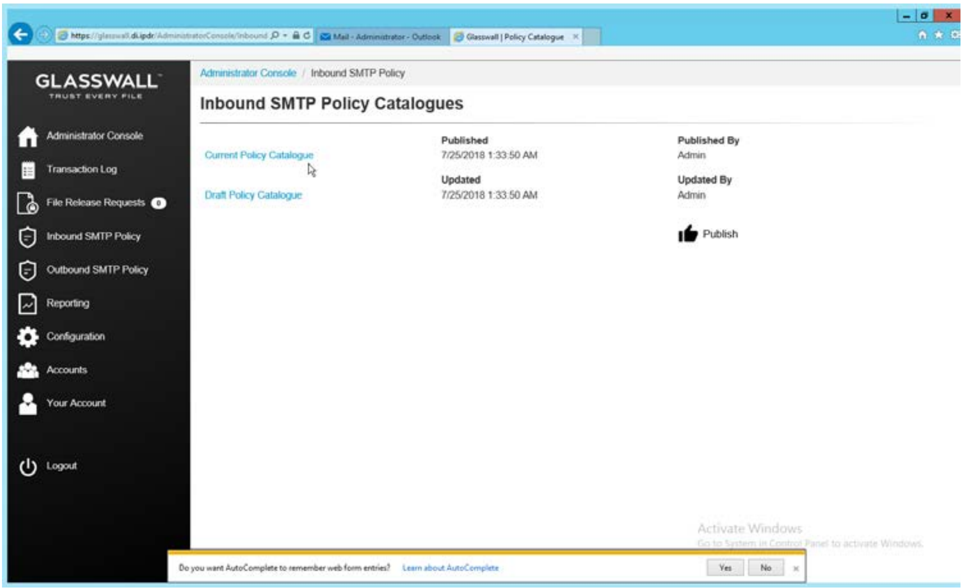
2.7.3.3 *Configure Inbound SMTP Policy*

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

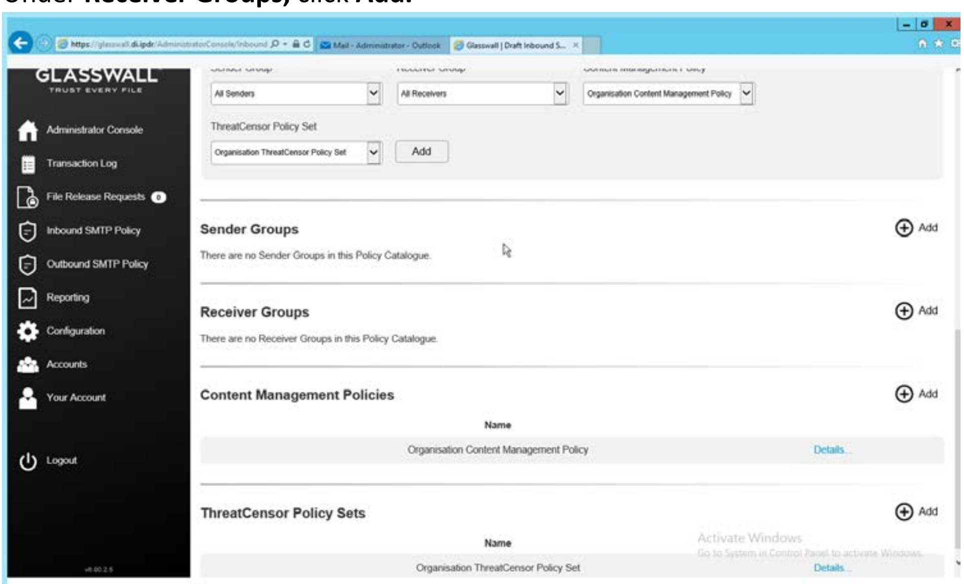
Policy in Glasswall FileTrust consists of **Sender Groups, Receiver Groups, Content Management Policies,** and **ThreatCensor Policy Sets. Receiver groups** allow for the specification of users who receive email. **Sender groups** allow for the specification of emails received from specific senders.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

2.7.3.4 *Create a Receiver Group*

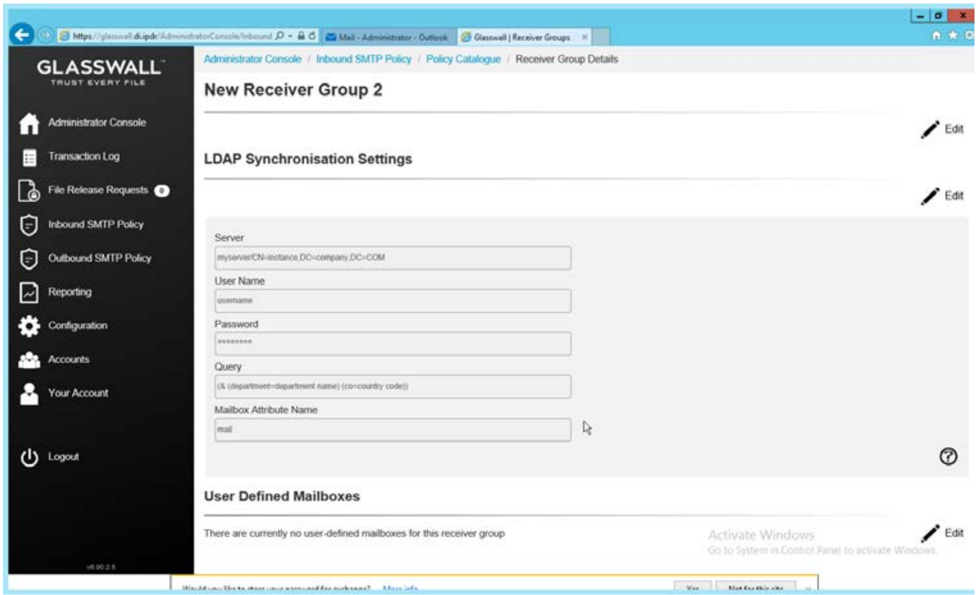
1. On the left sidebar, click **Inbound SMTP Policy.**
2. Click **Draft Policy Catalogue.**



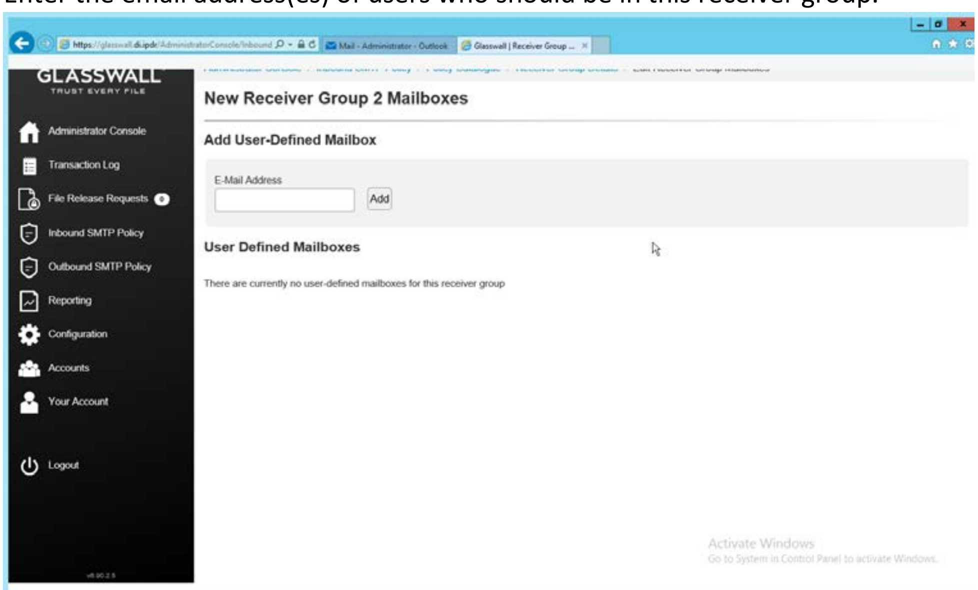
3. Under **Receiver Groups,** click **Add.**



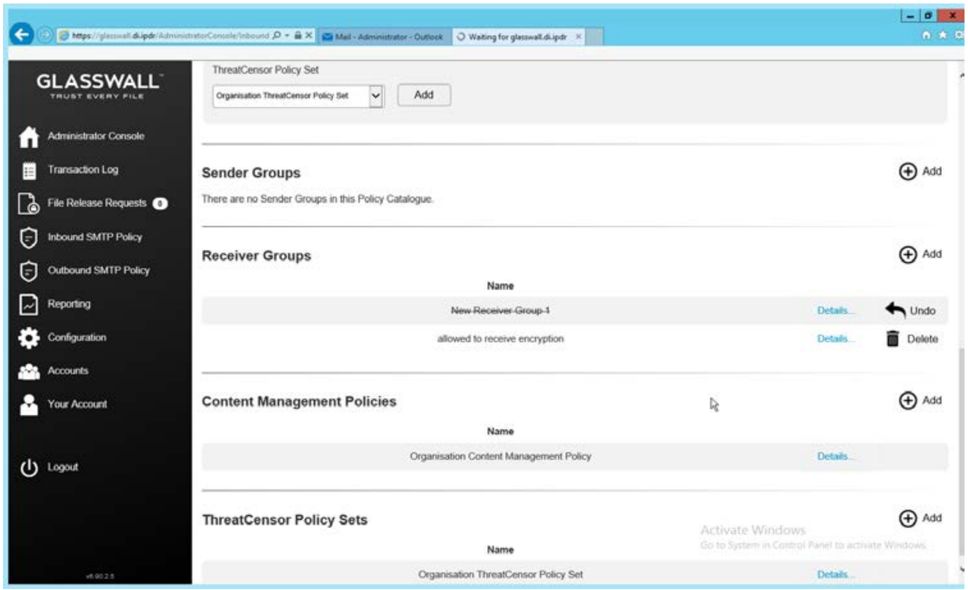
4. Under **User Defined Mailboxes,** click **Edit.**



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

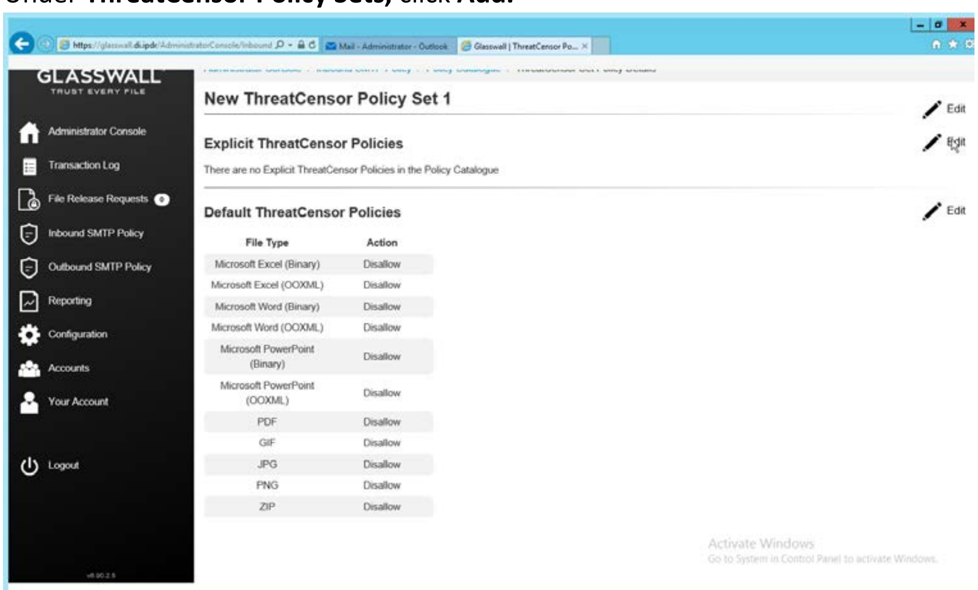


6. Click **Add.**
7. When finished, return to the **Policy Catalogue** page.

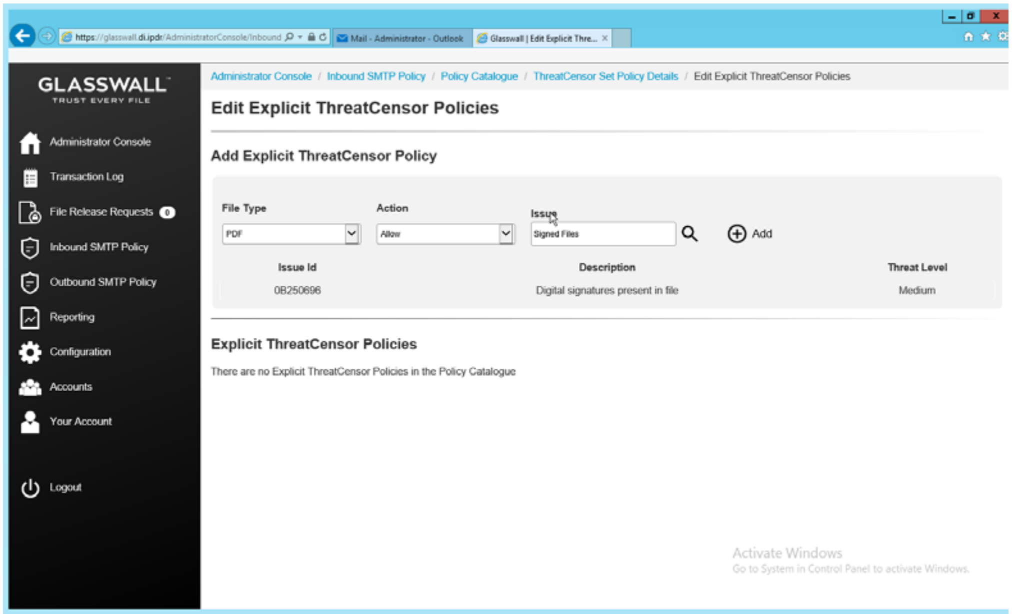


2.7.3.5 *Create a ThreatCensor Policy Set*

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



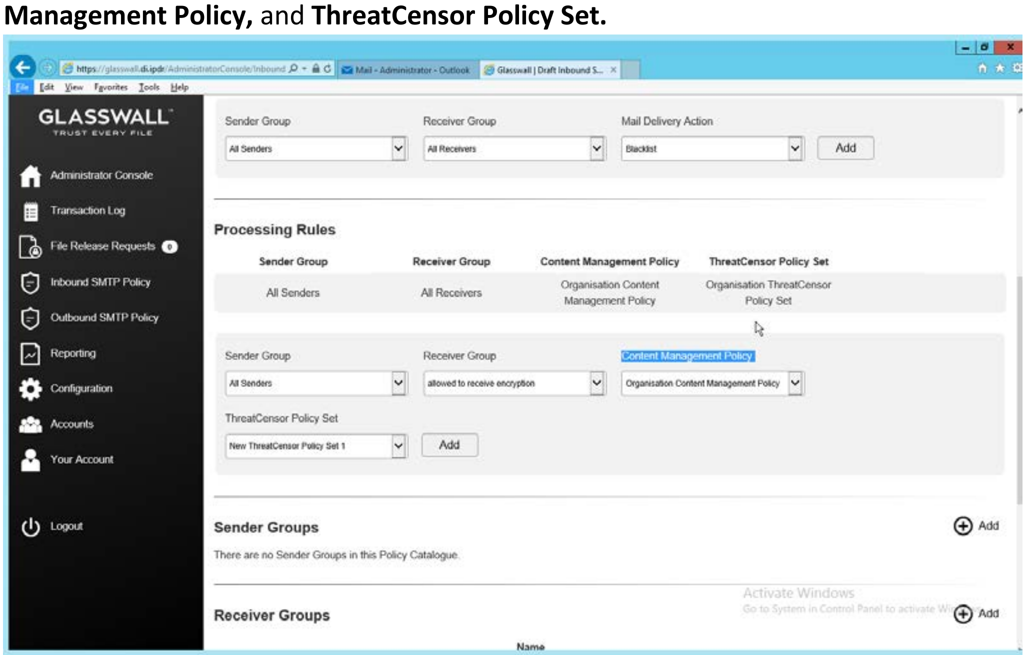
2. Under **Explicit ThreatCensor Policies,** click **Edit.**



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

2.7.3.6 *Create a Processing Rule*

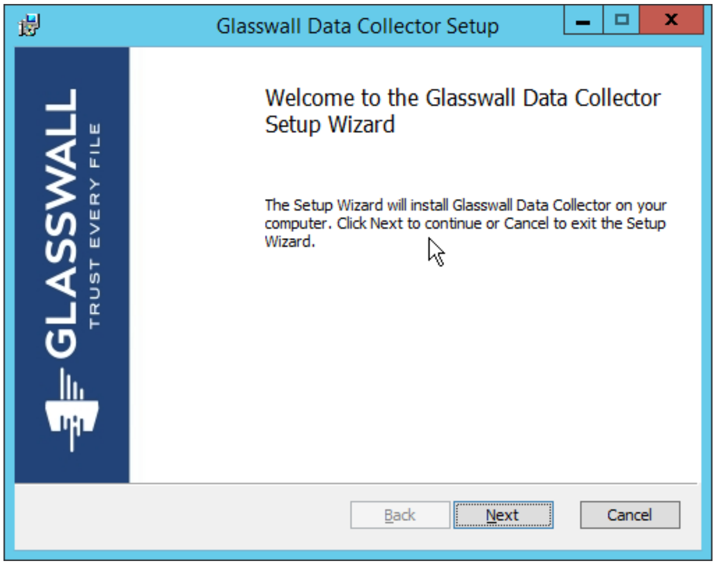
1. Under Processing Rules, select the appropriate **Sender Group, Receiver Group, Content Management Policy,** and **ThreatCensor Policy Set.**



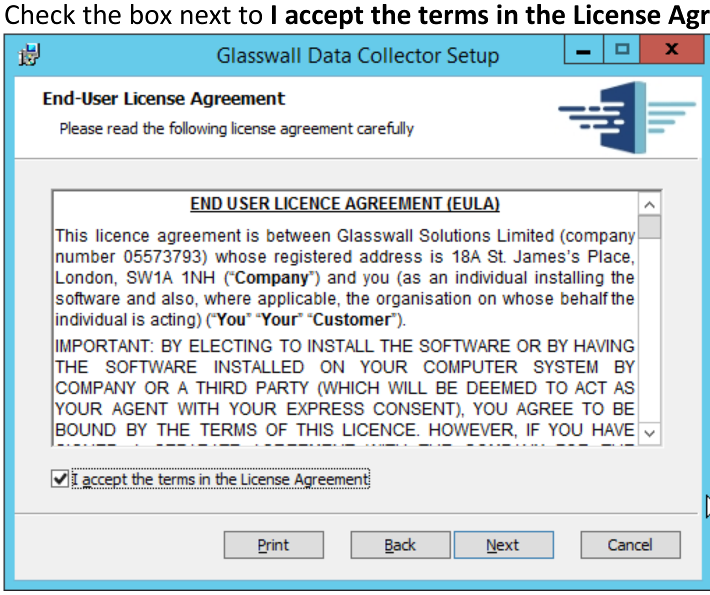
2. Click **Add.**
3. This allows for granular policy for email inspection, quarantine, and reconstruction.

2.7.4 Configure Intelligence Sharing

1. Run **DataCollectorInstaller.msi.**

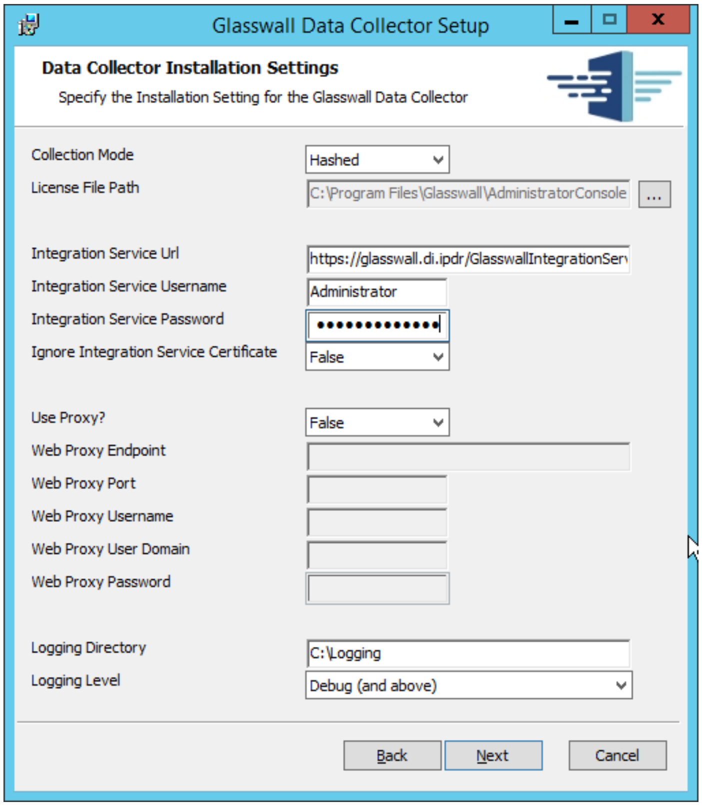


2. Click **Next.**
3. Check the box next to **I accept the terms in the License Agreement.**

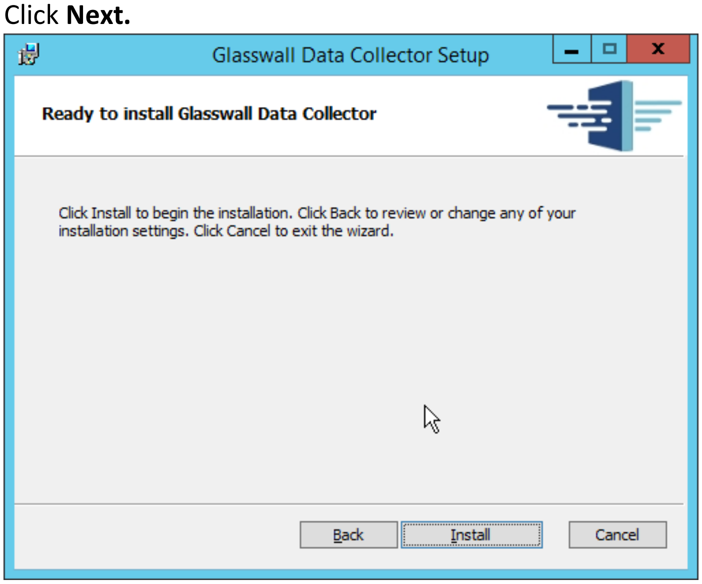


4. Click **Next.**
5. Select **Hashed** for **Collection Mode** (especially if your data is sensitive; this will prevent the release of any identifying information).

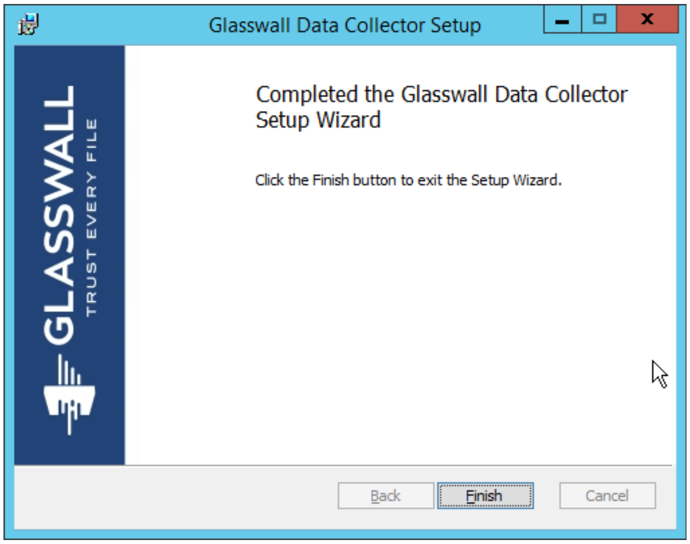
6. For **Integration Service Url** replace **localhost** with the name of the computer running the **Integration Service.**
7. Enter the **username** and **password.**



8. Click **Next.**



9. Click **Install.**



10. Click **Finish.**

2.8 Micro Focus ArcSight Enterprise Security Manager

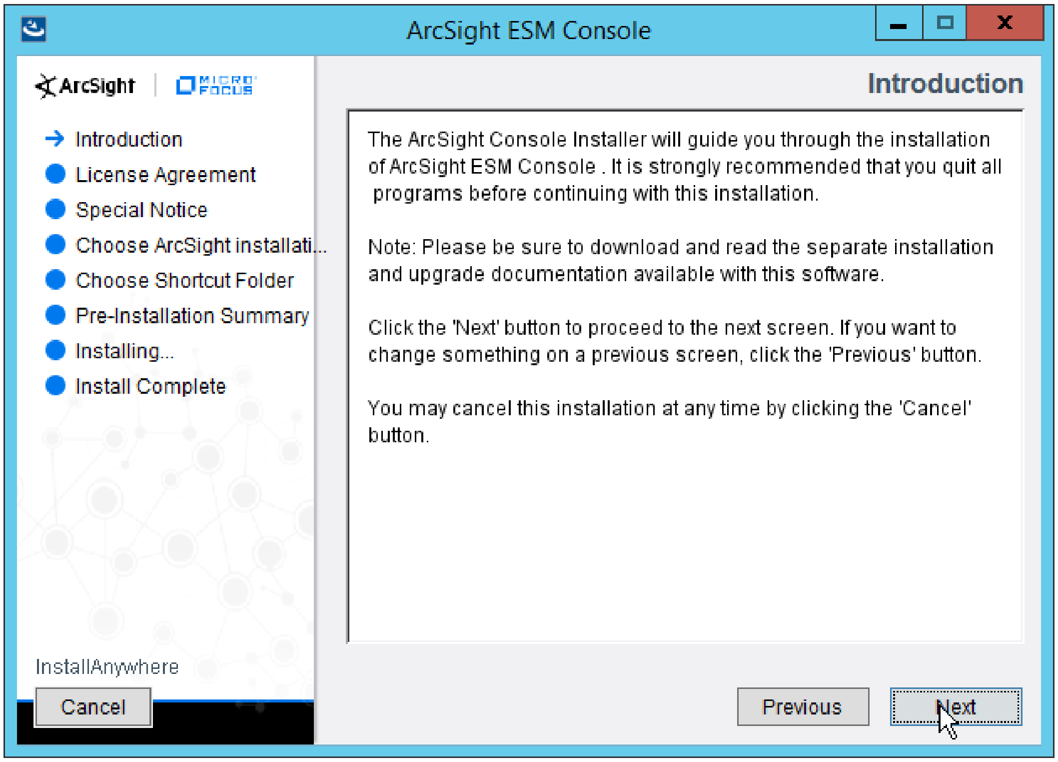
Micro Focus ArcSight Enterprise Security Manager (ESM) is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

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

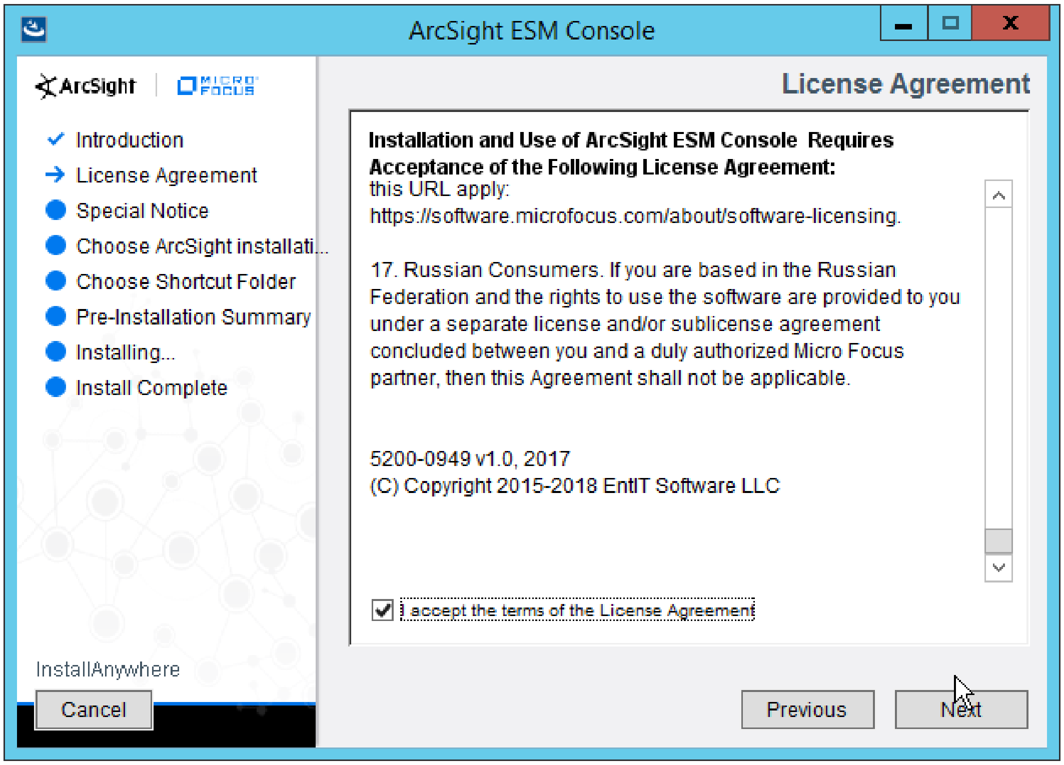
Installation instructions are included for both Windows and UNIX machines, as well as for collecting from multiple machines. Furthermore, integrations with other products in the build are included in later sections.

2.8.1 Install the ArcSight Console

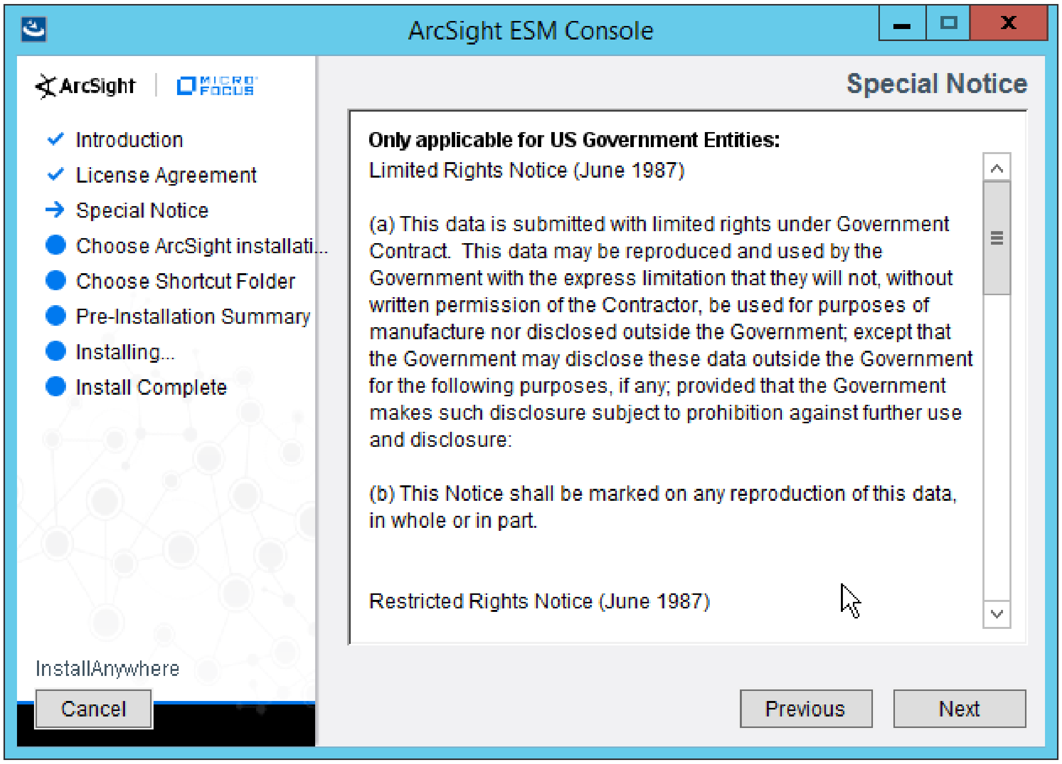
1. Run **ArcSight-7.0.0.2436.1-Console-Win.exe.**



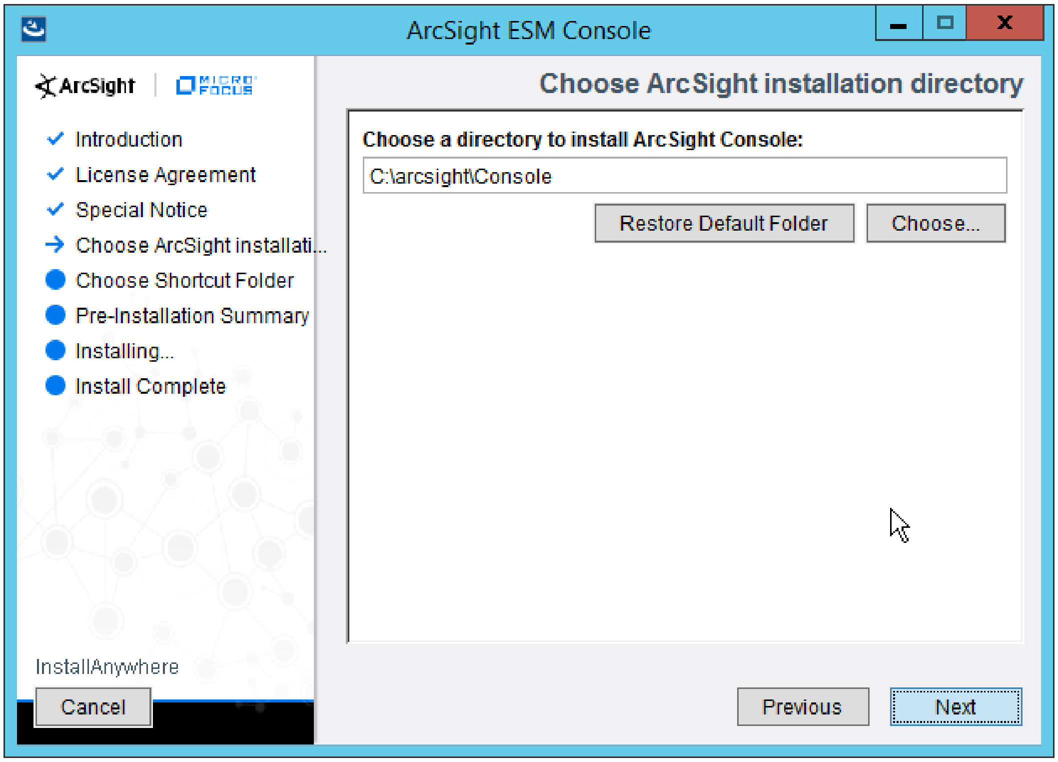
2. Click **Next.**
3. Check the box next to **I accept the License Agreement.**



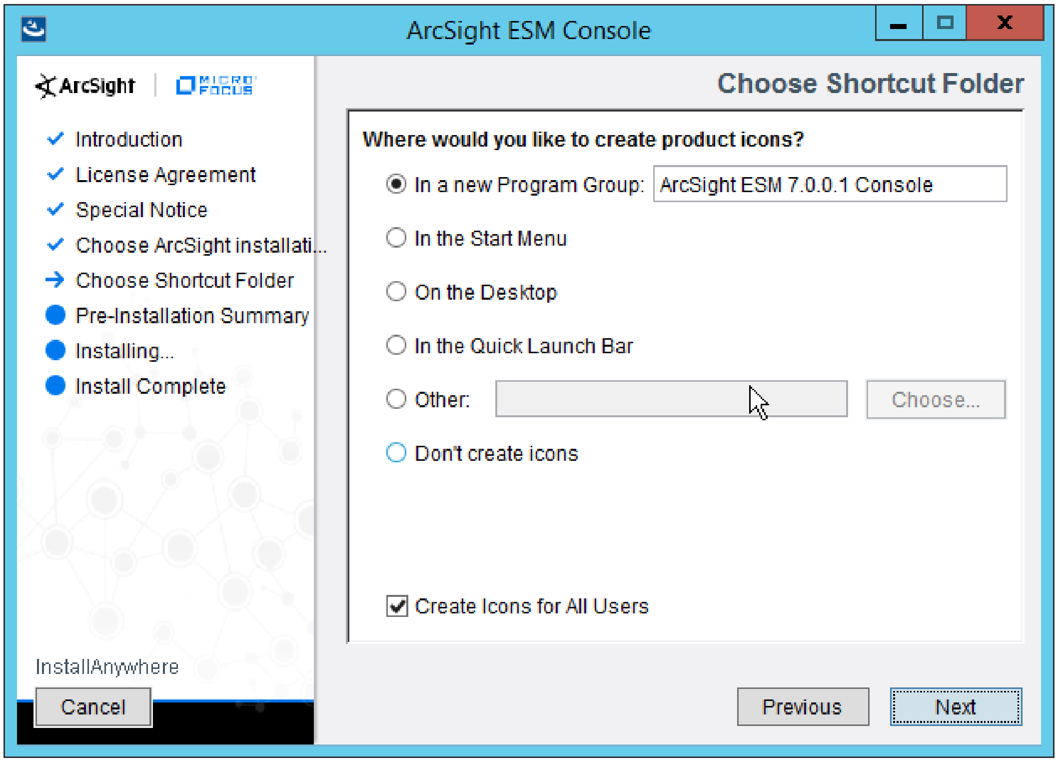
1237
1238 4. Click **Next.**


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

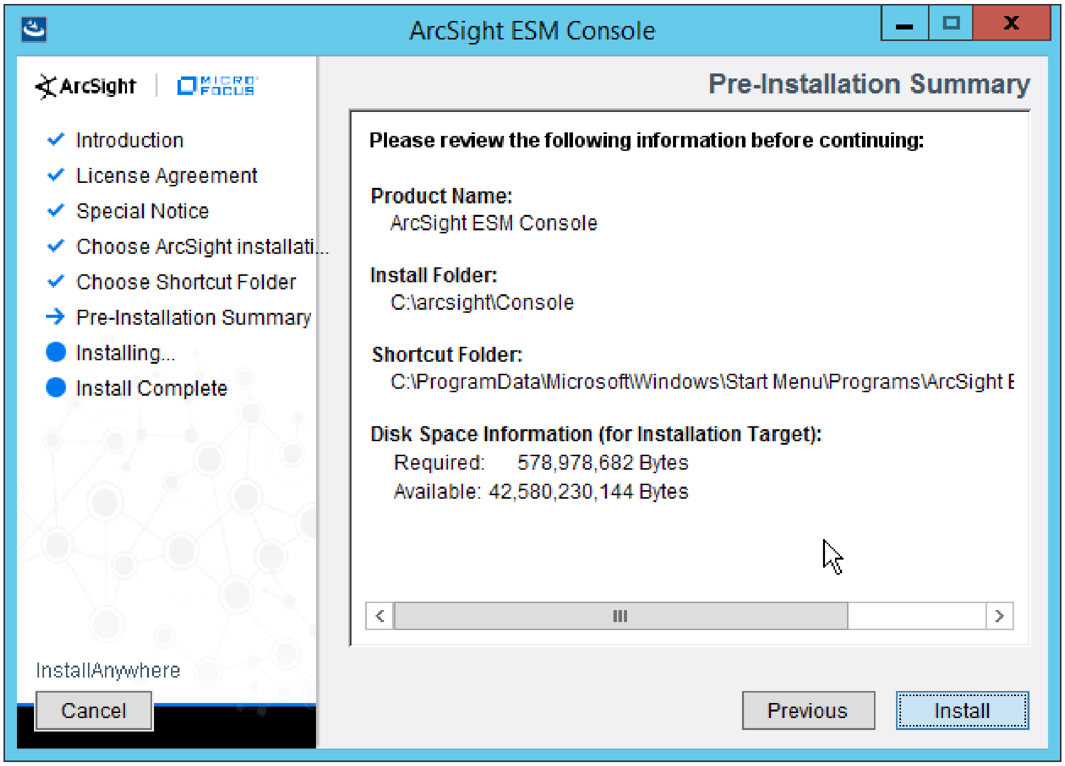
5. Click **Next.**


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

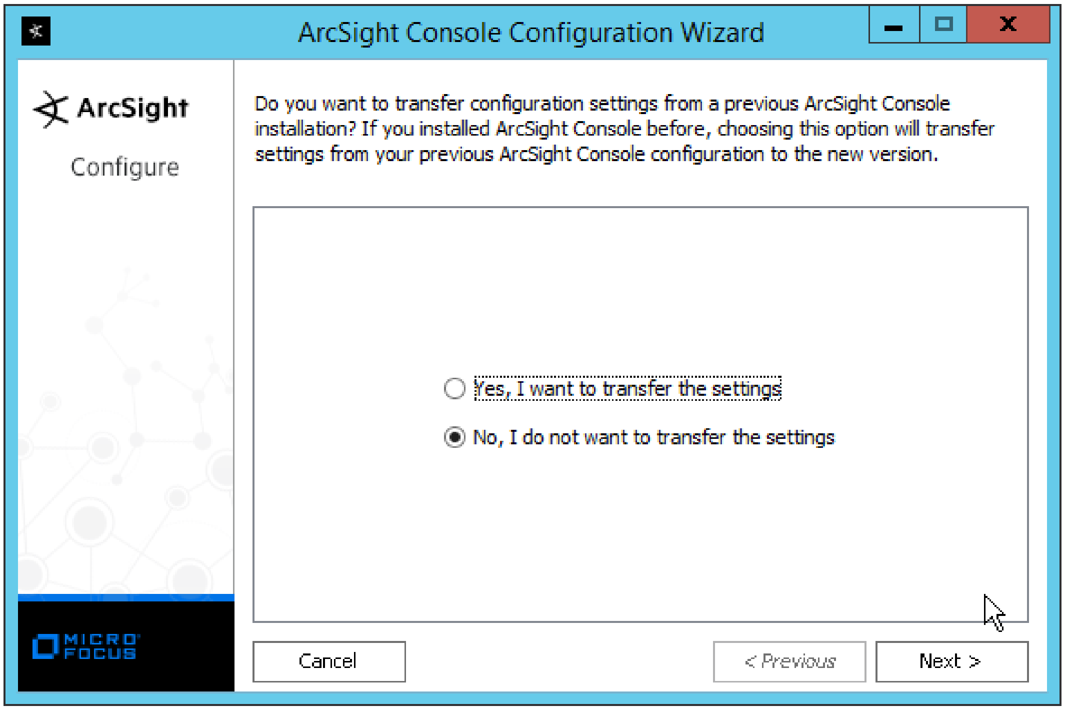
6. Click **Next.**


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

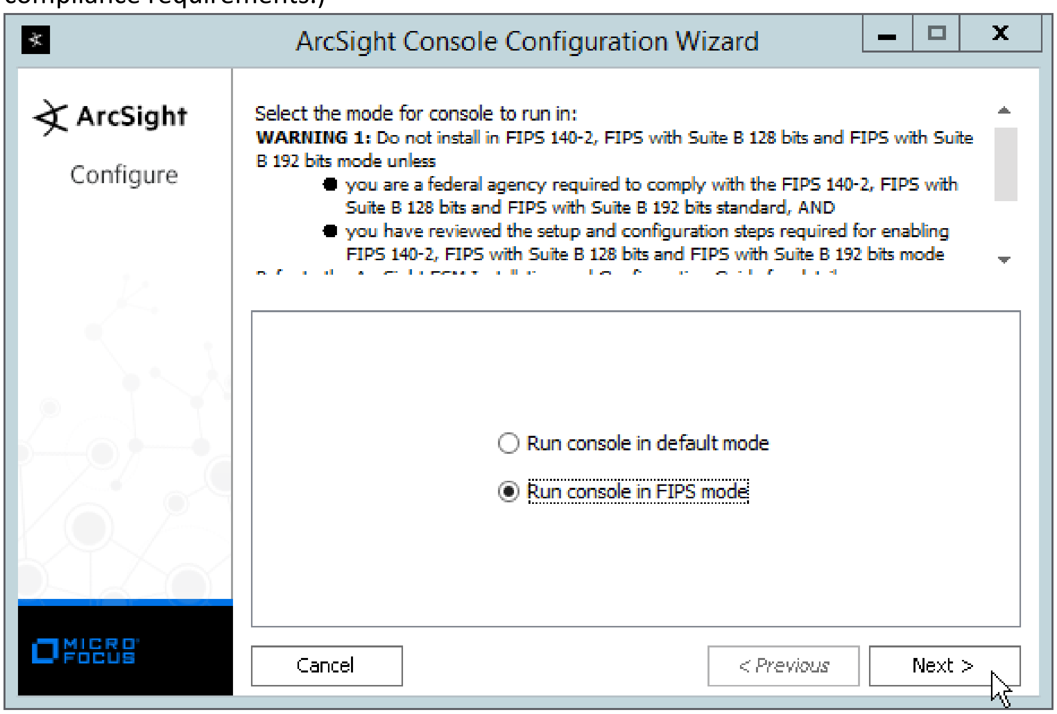
7. Click **Next.**



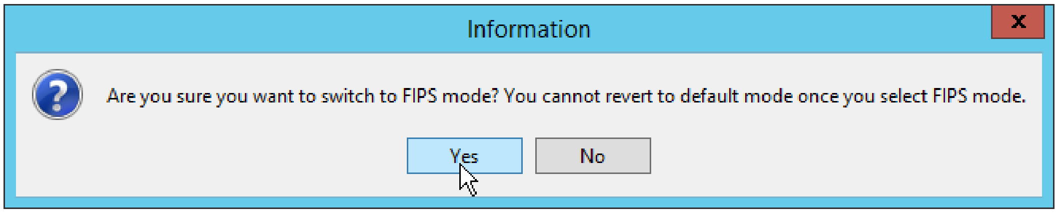
8. Click **Install.**
9. Select **No, I do not want to transfer the settings.**



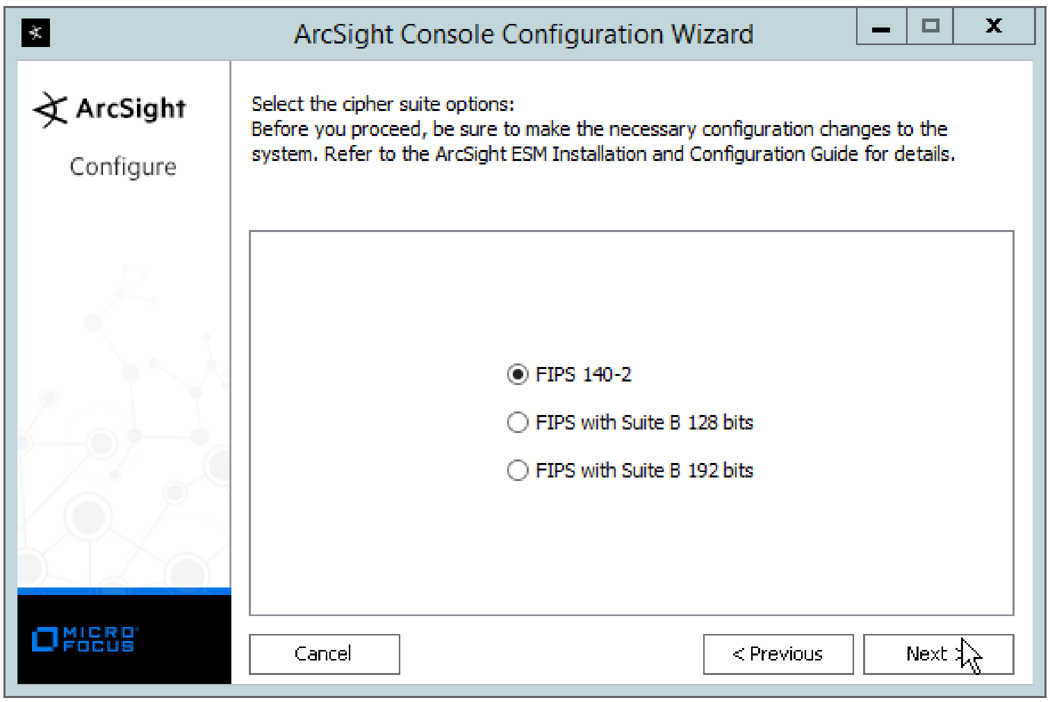
10. Click **Next.**
11. Select **Run console in default mode.** (This can be changed later according to your organization's compliance requirements.)



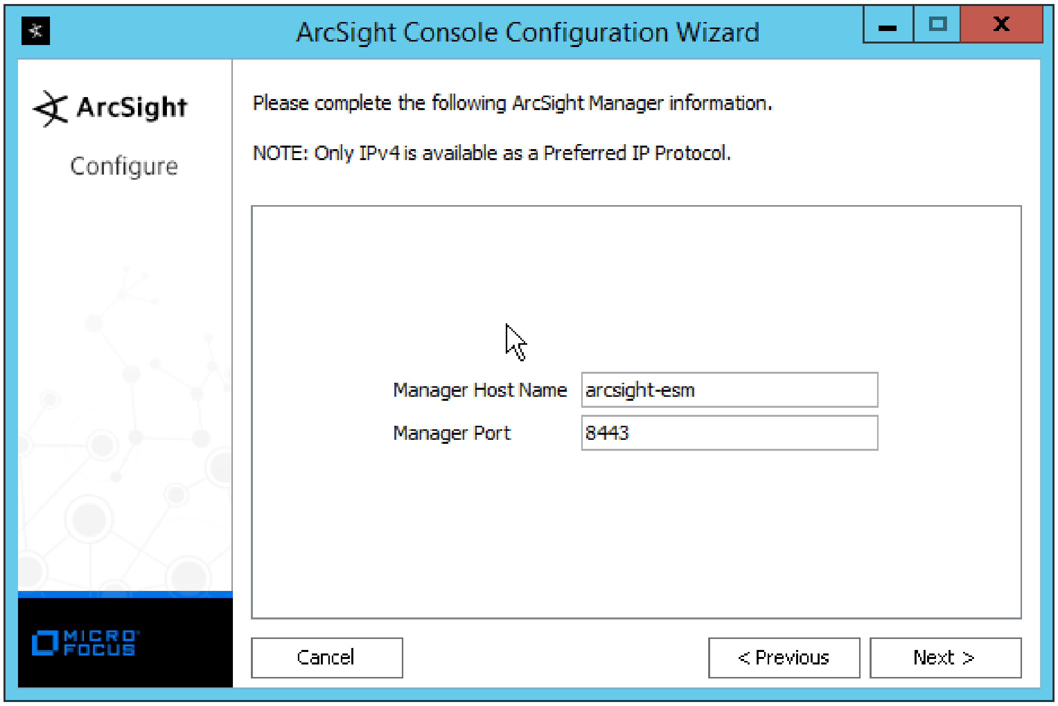
12. Click **Next.**



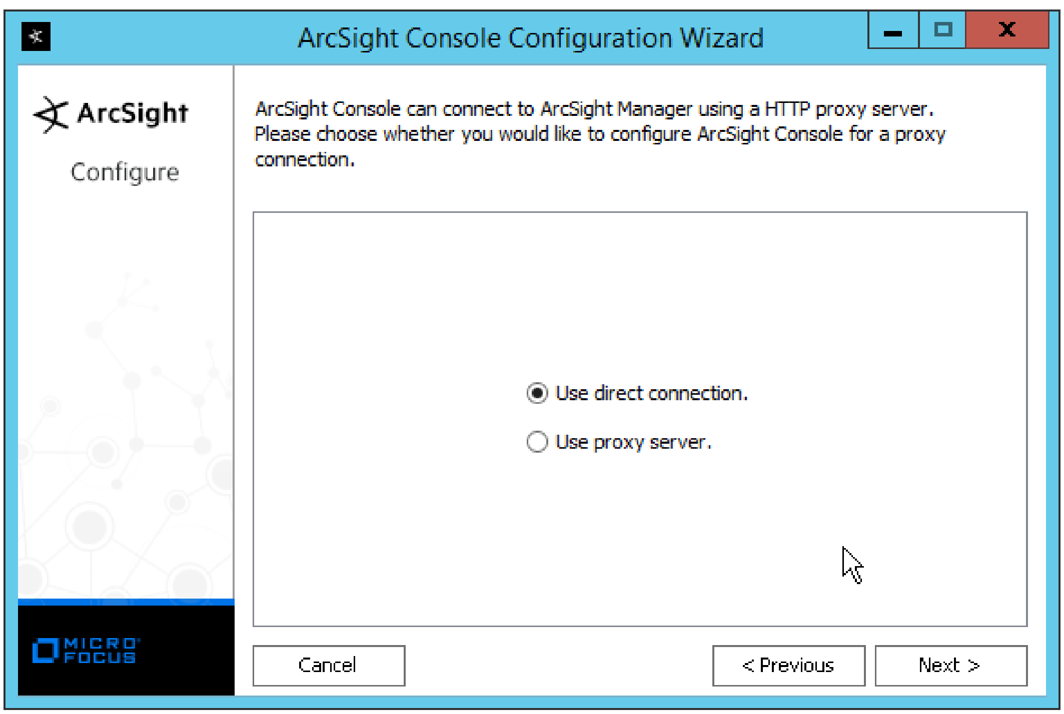
13. Click **Yes.**
14. Select **FIPS 140-2.**



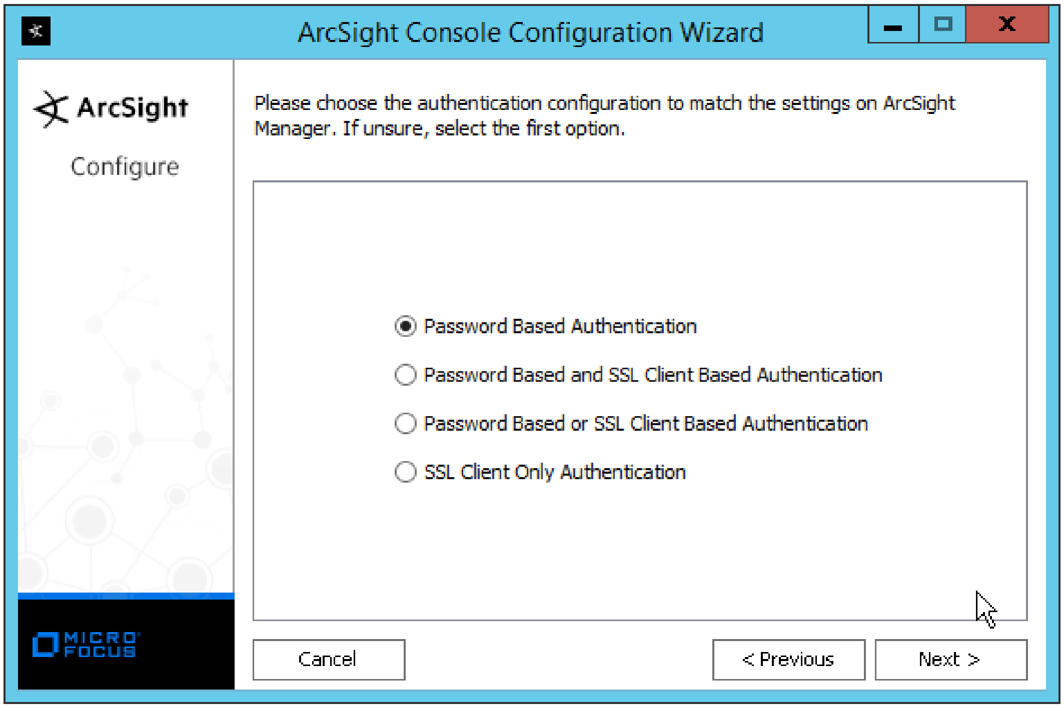
15. Click **Next.**
16. Enter the **hostname** of the ESM server for **Manager Host Name.**
17. Enter the **port** that ESM is running on for **Manager Port** (default: **8443**).



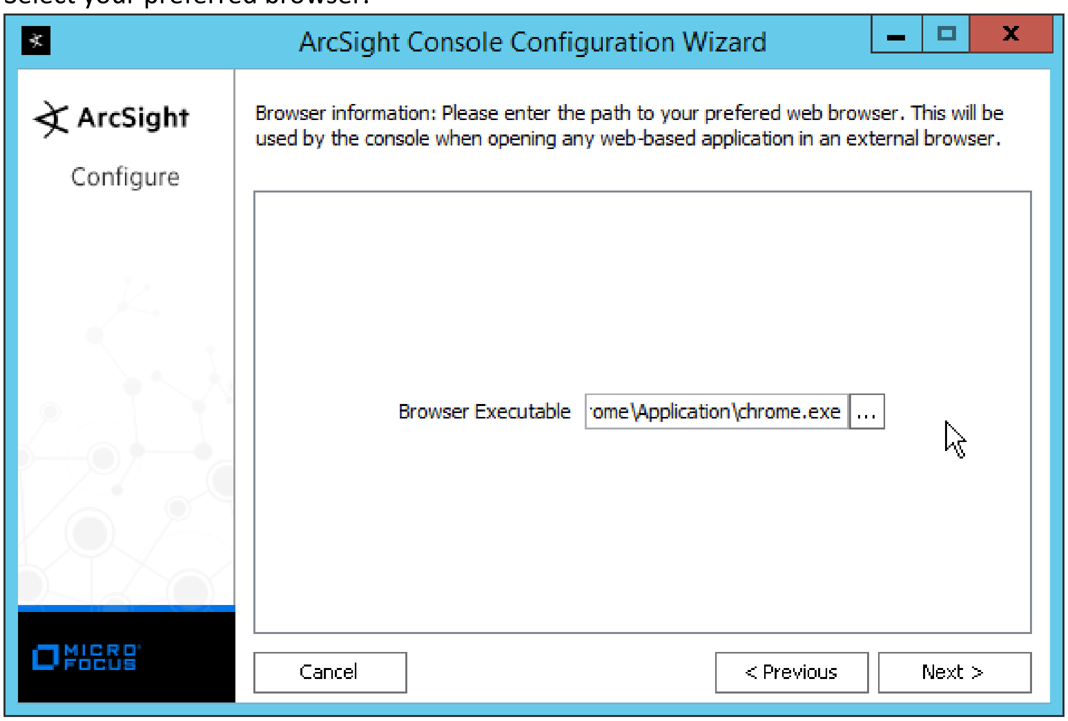
18. Click **Next.**
19. Select **Use direct connection.**



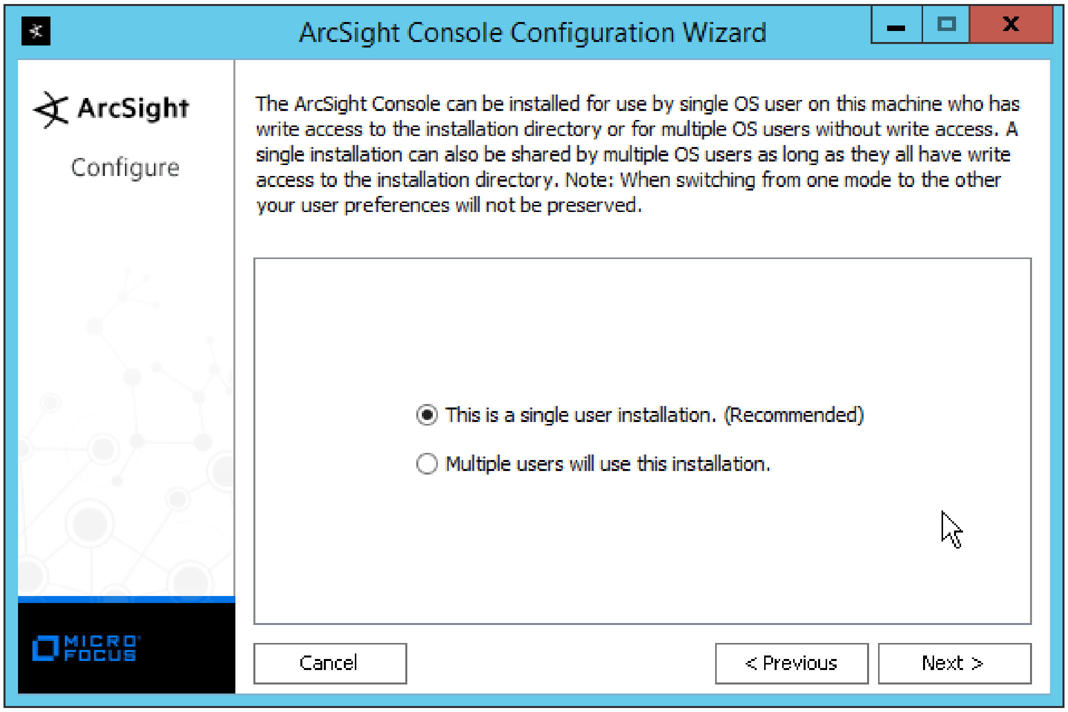
20. Click **Next.**



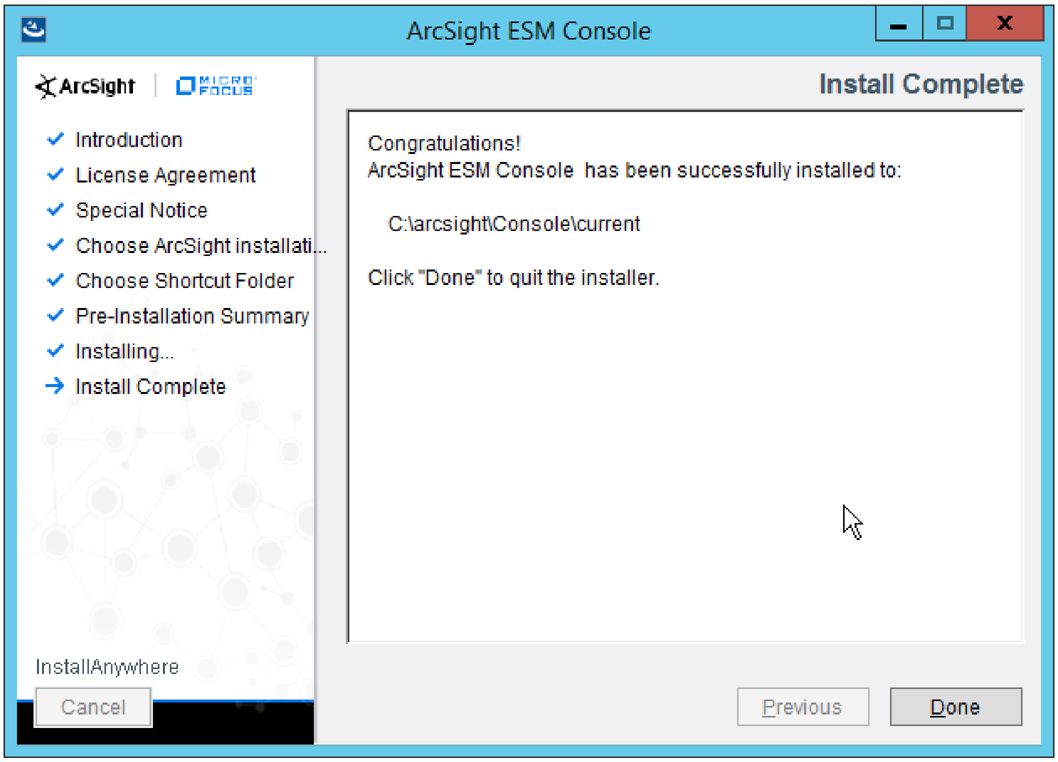
21. Click **Next.**
22. Select your preferred browser.



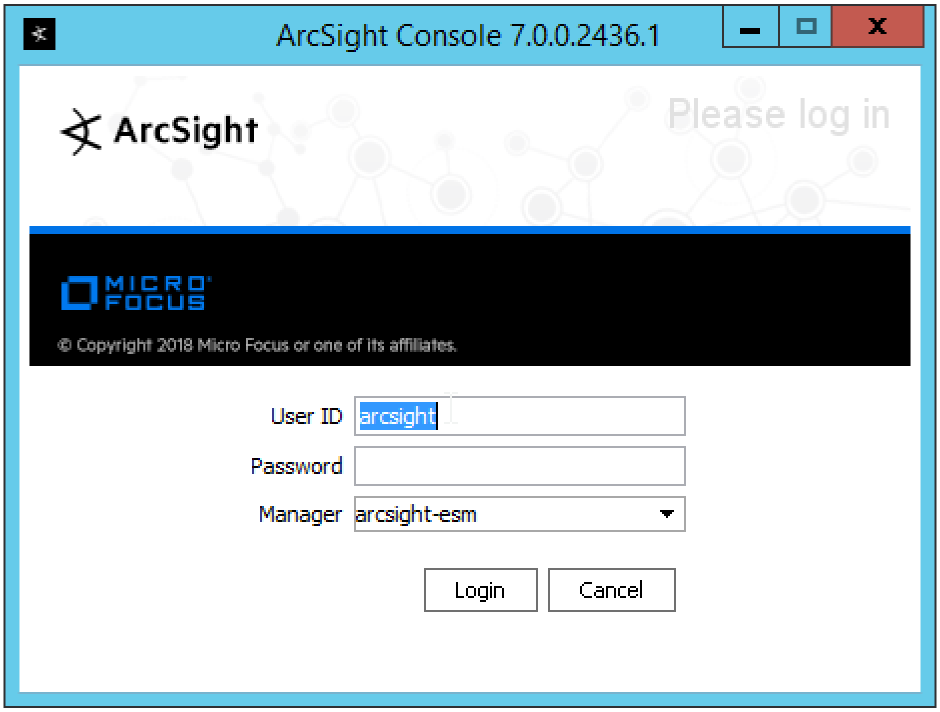
23. Click **Next.**



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



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

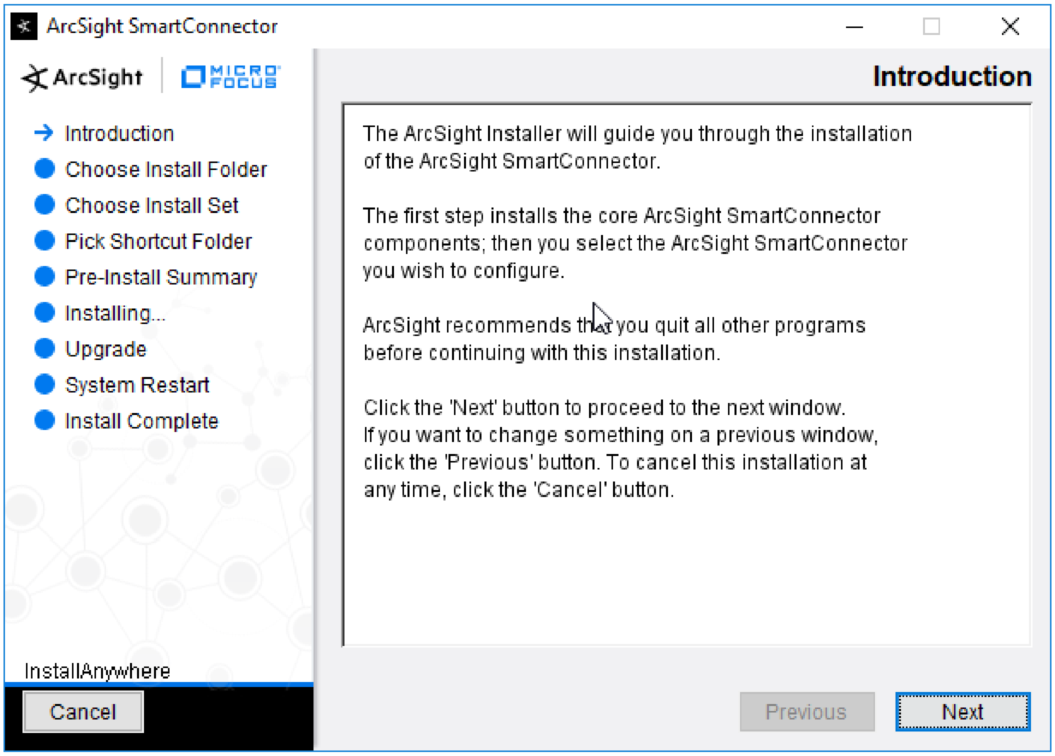


29. Click **Login.** (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)

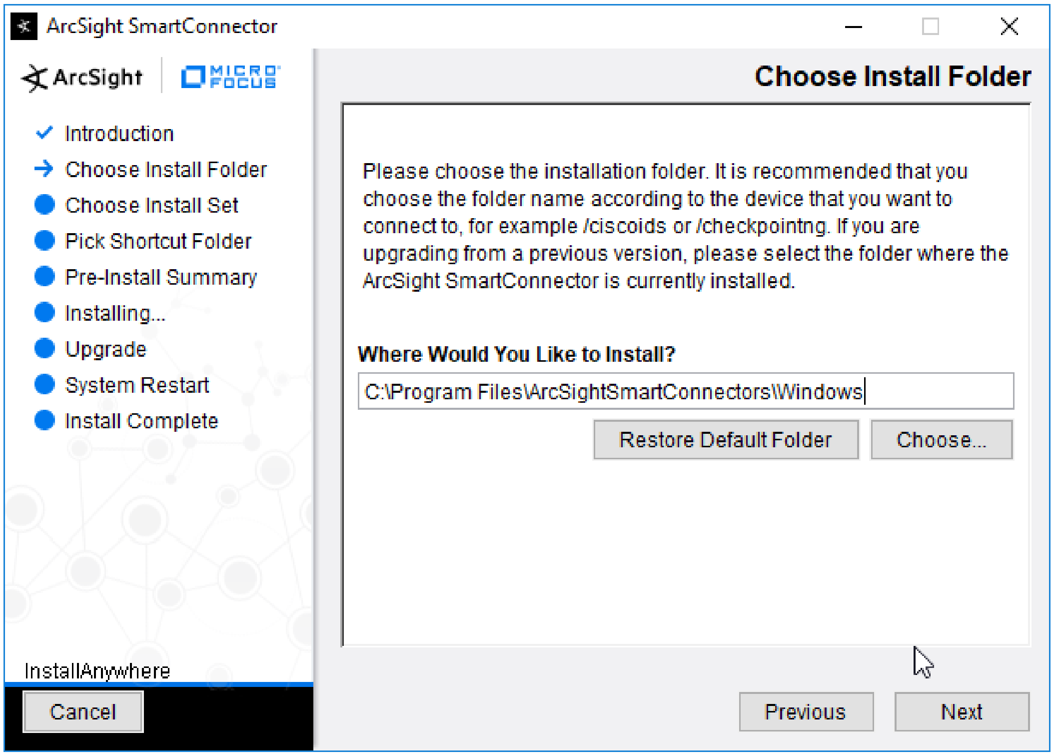
30. Click **OK.**

2.8.2 Install Individual ArcSight Windows Connectors

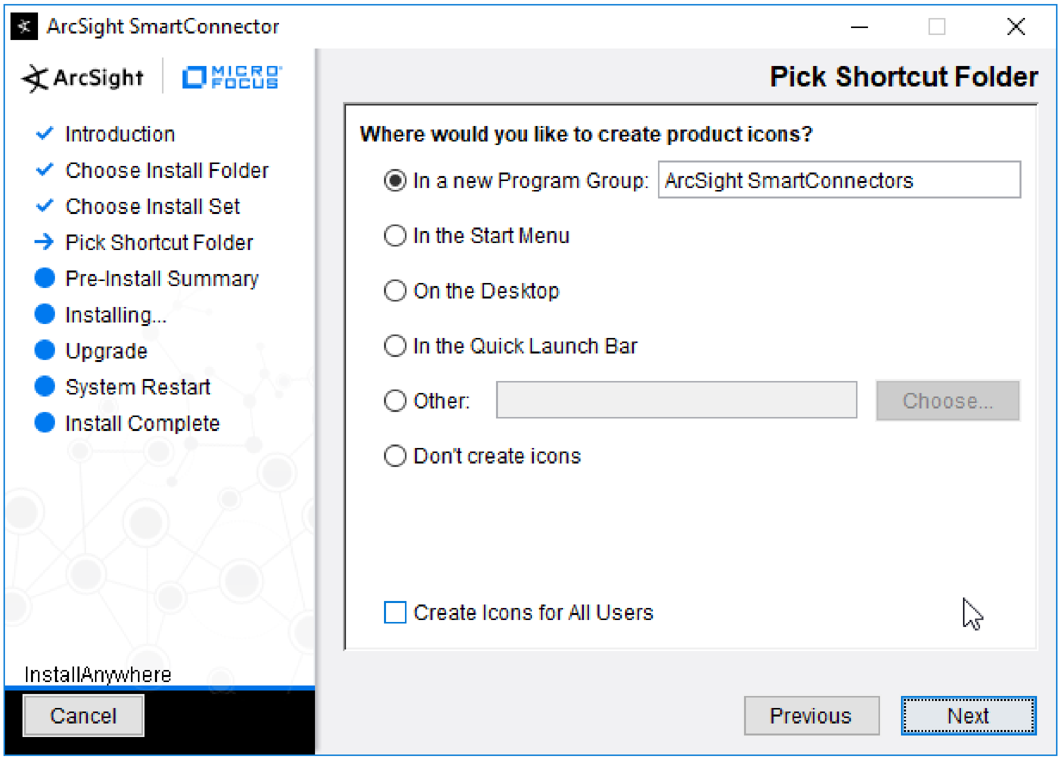
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe.**



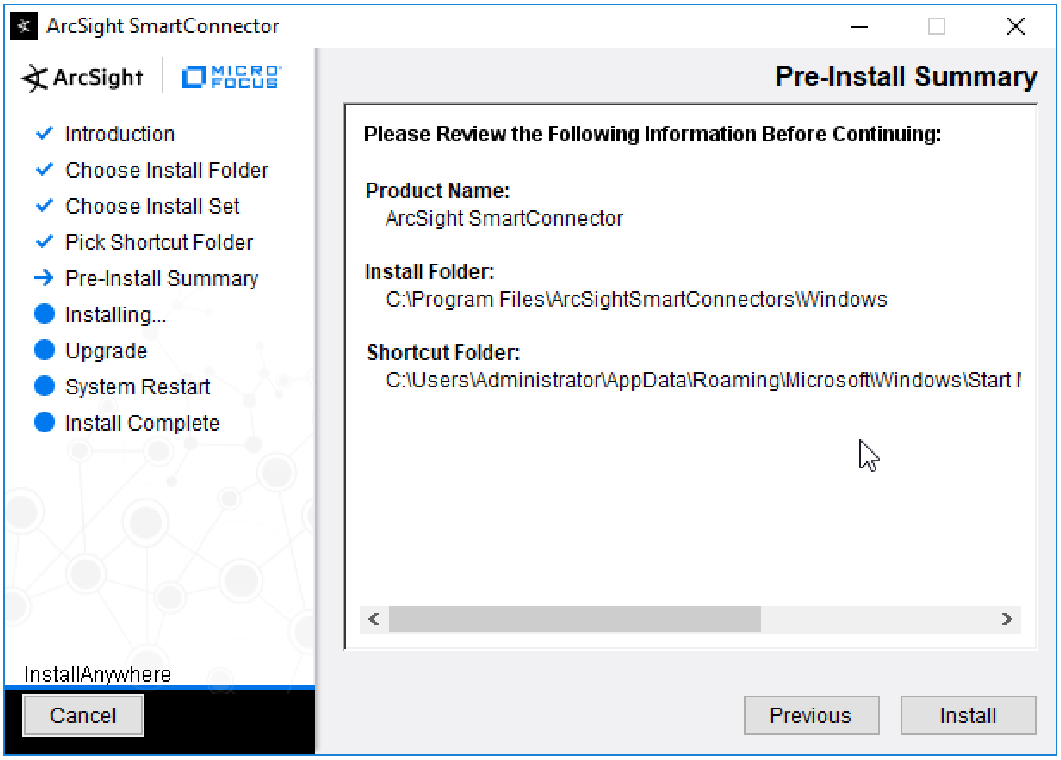
2. Click **Next.**
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.


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

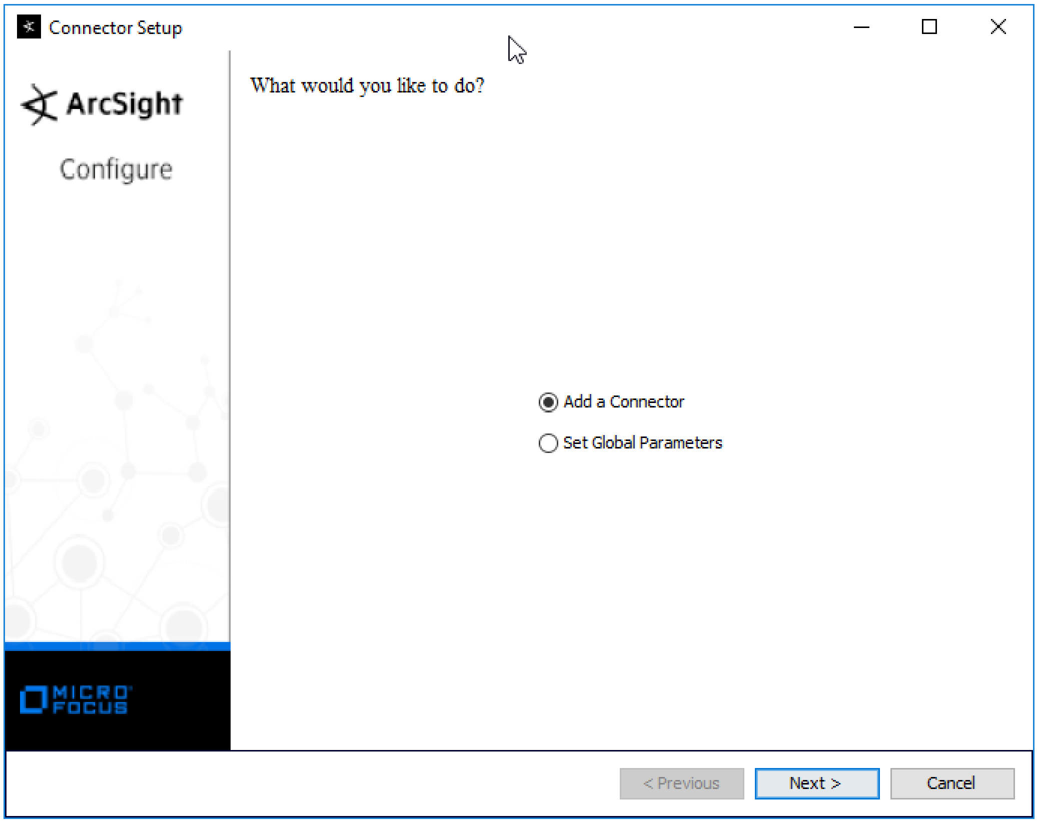
4. Click **Next.**


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

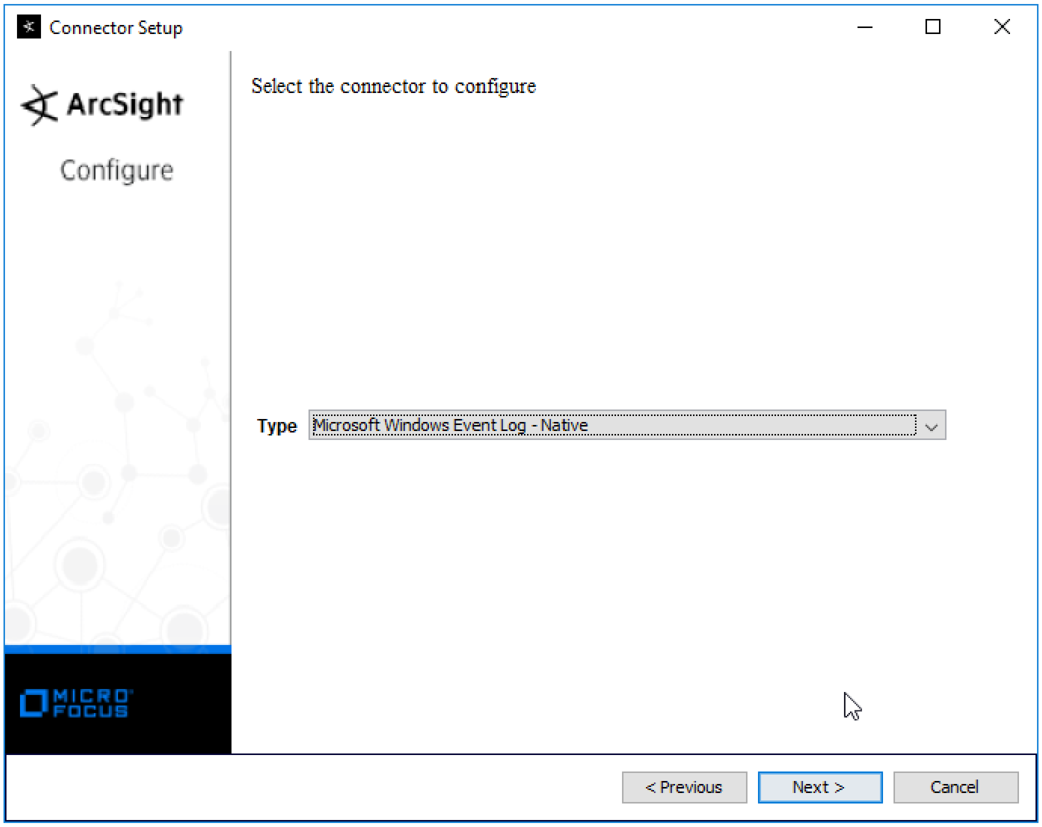
5. Click **Next.**



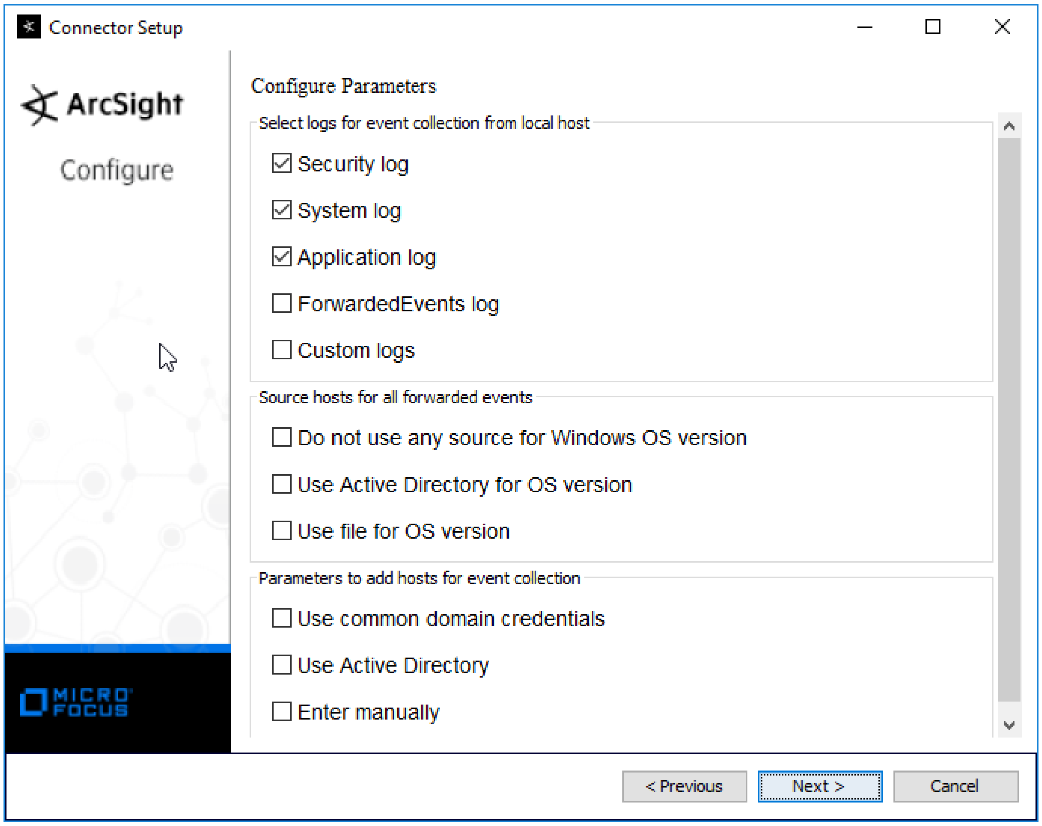
6. Click **Install.**
7. Select **Add a Connector.**



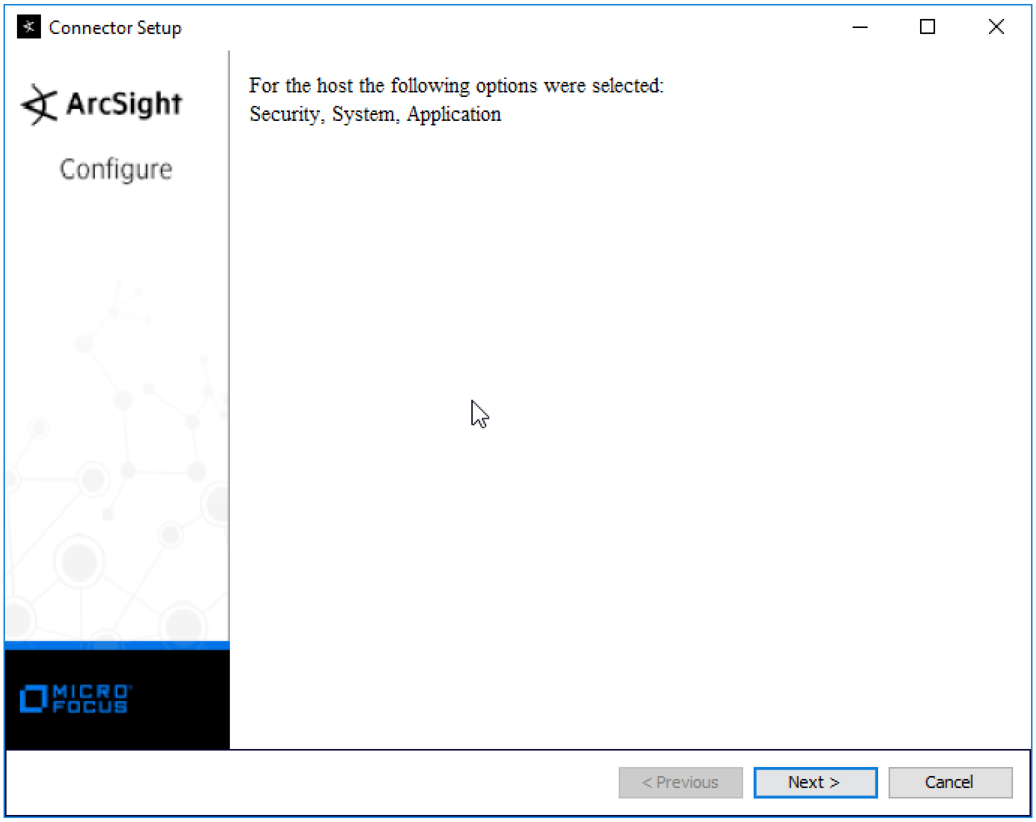
8. Click **Next.**
9. Select **Microsoft Windows Event Log – Native.**



10. Click **Next.**



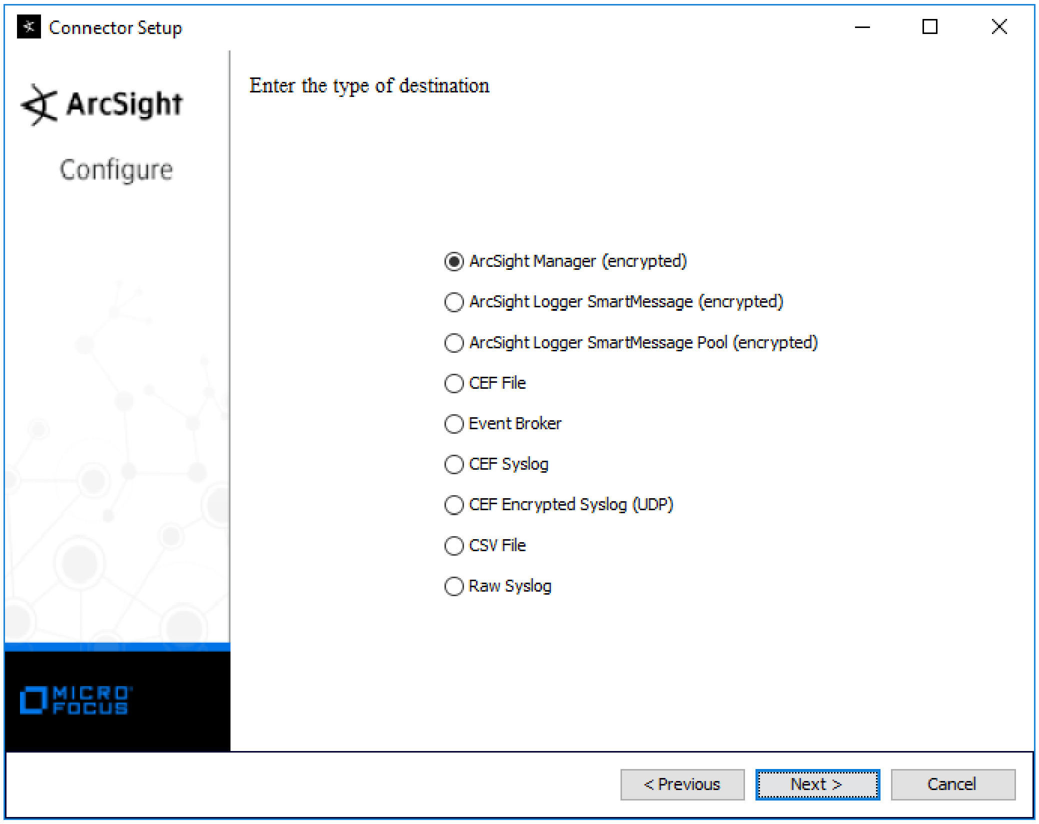
1300
1301 11. Click **Next.**



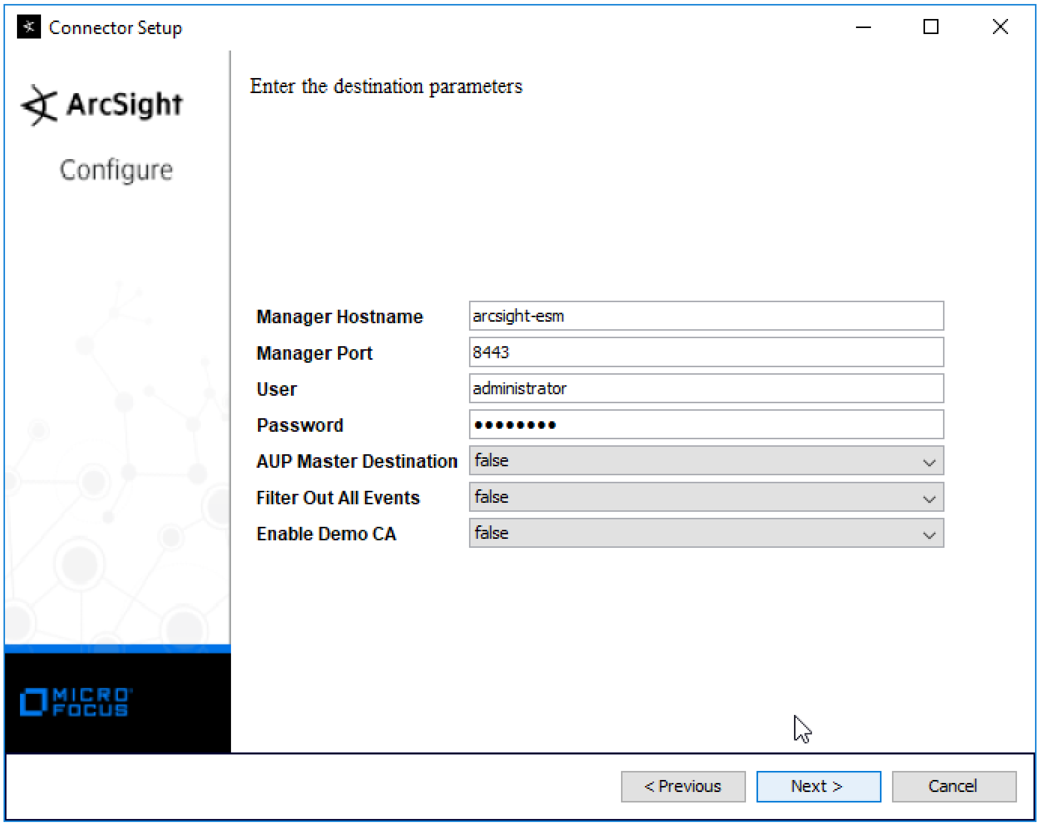
1302

1303 12. Click **Next.**

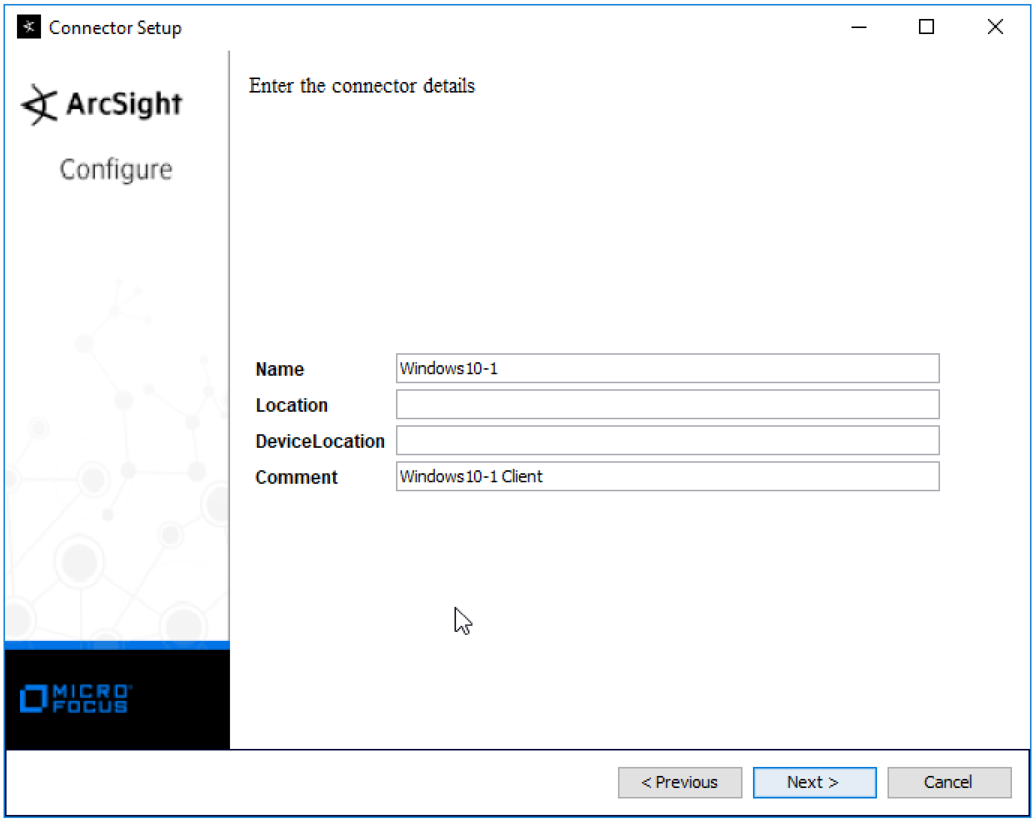
1304 13. Select **ArcSight Manager (encrypted).**



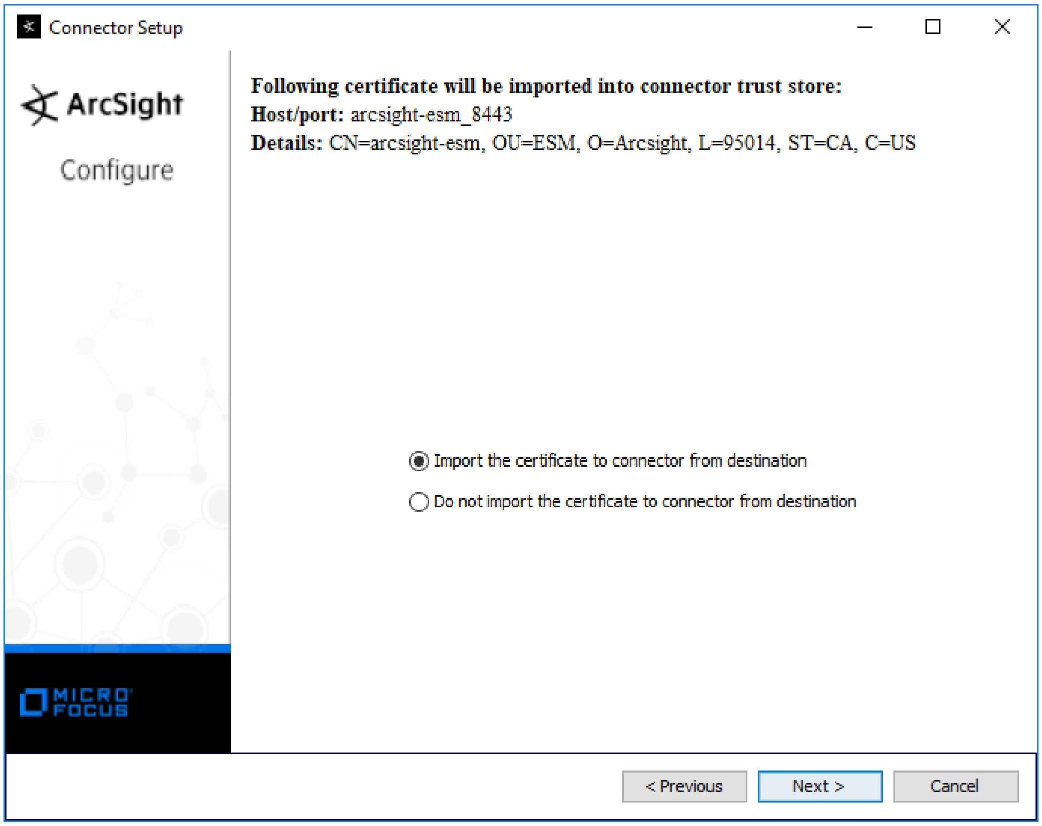
14. Click **Next.**
15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



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

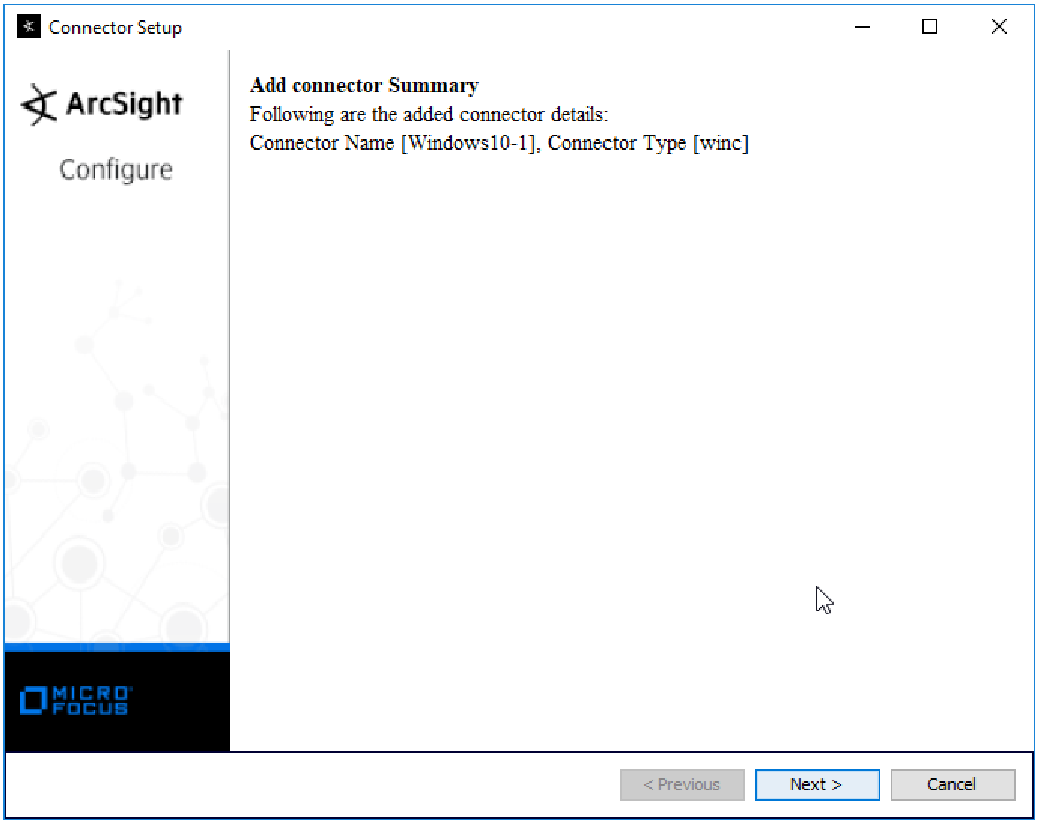


18. Click **Next.**
19. Select **Import the certificate to connector from destination.**

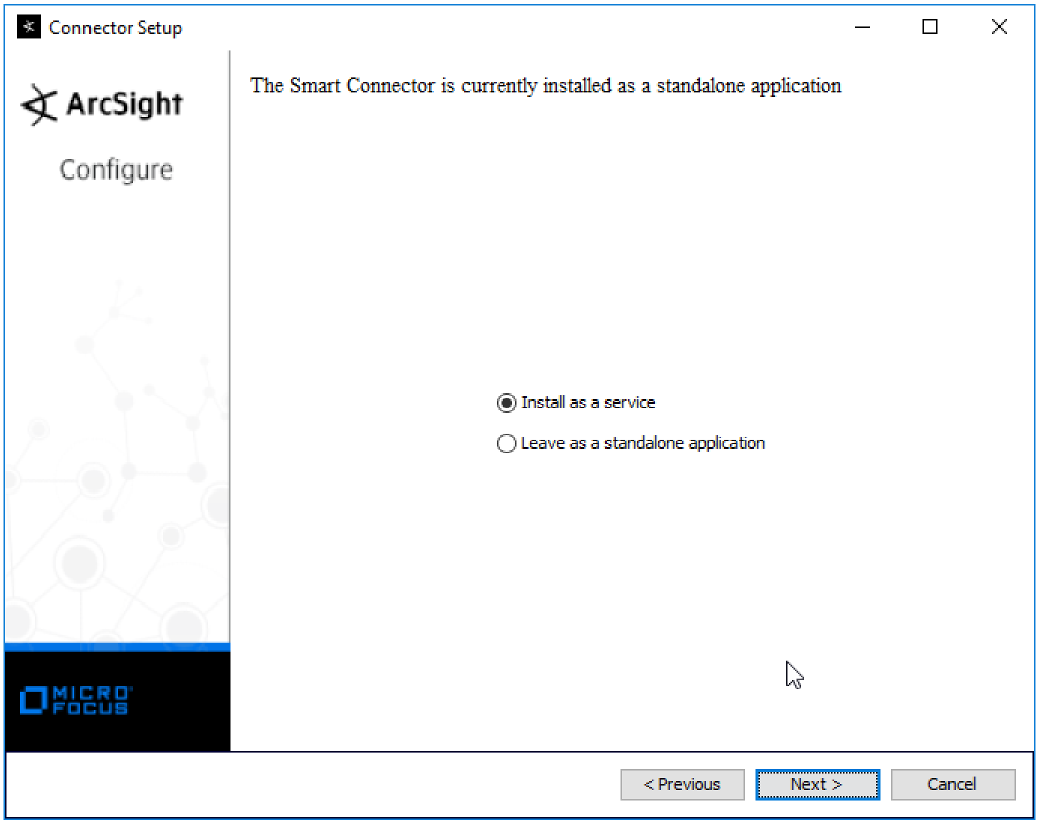


1314

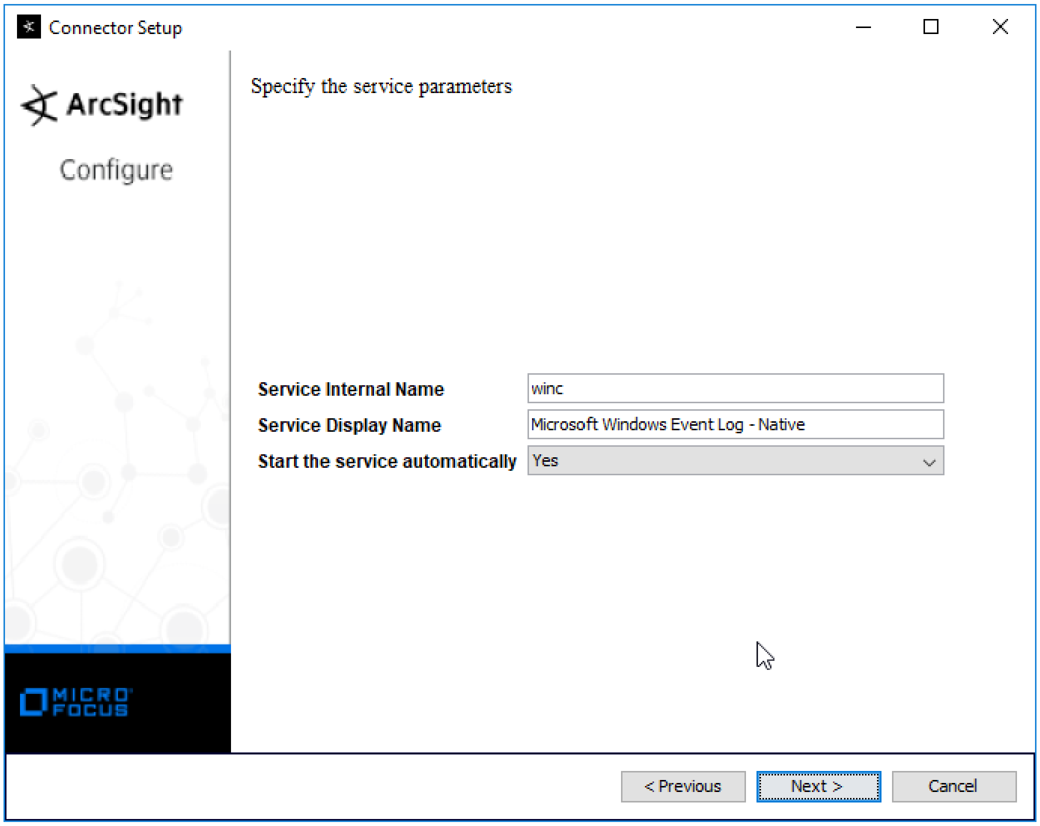
1315 20. Click **Next.**



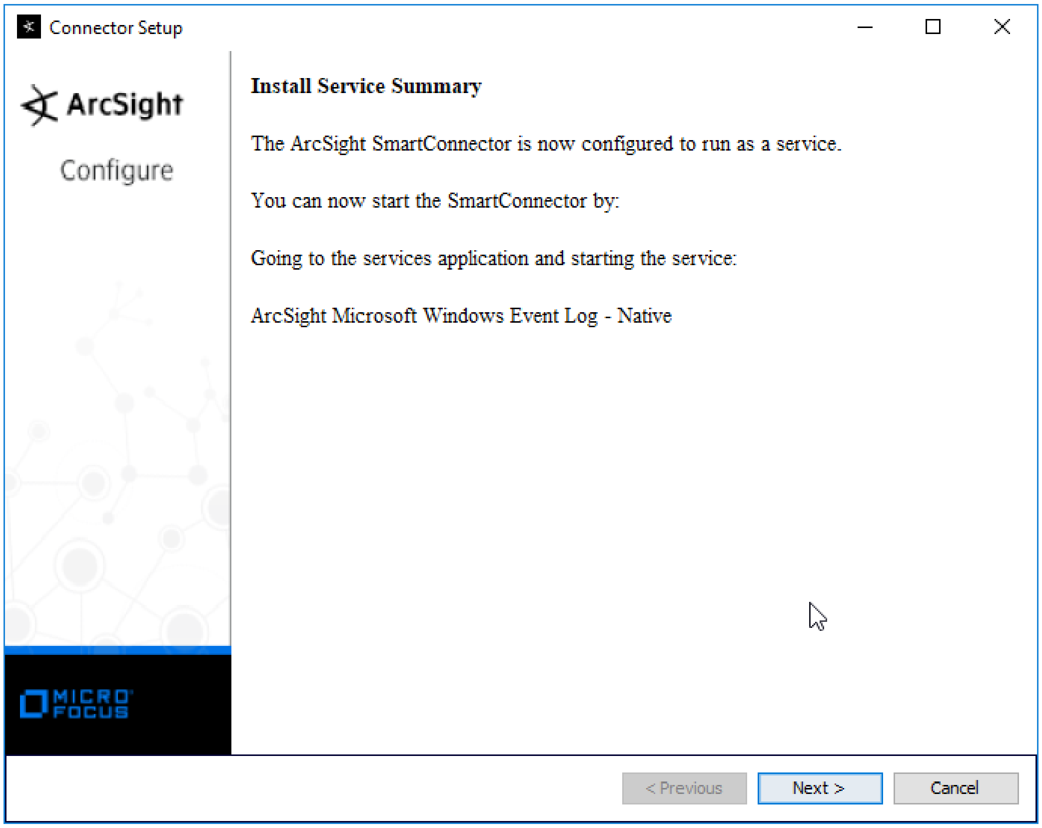
21. Click **Next.**
22. Select **Install as a service.**



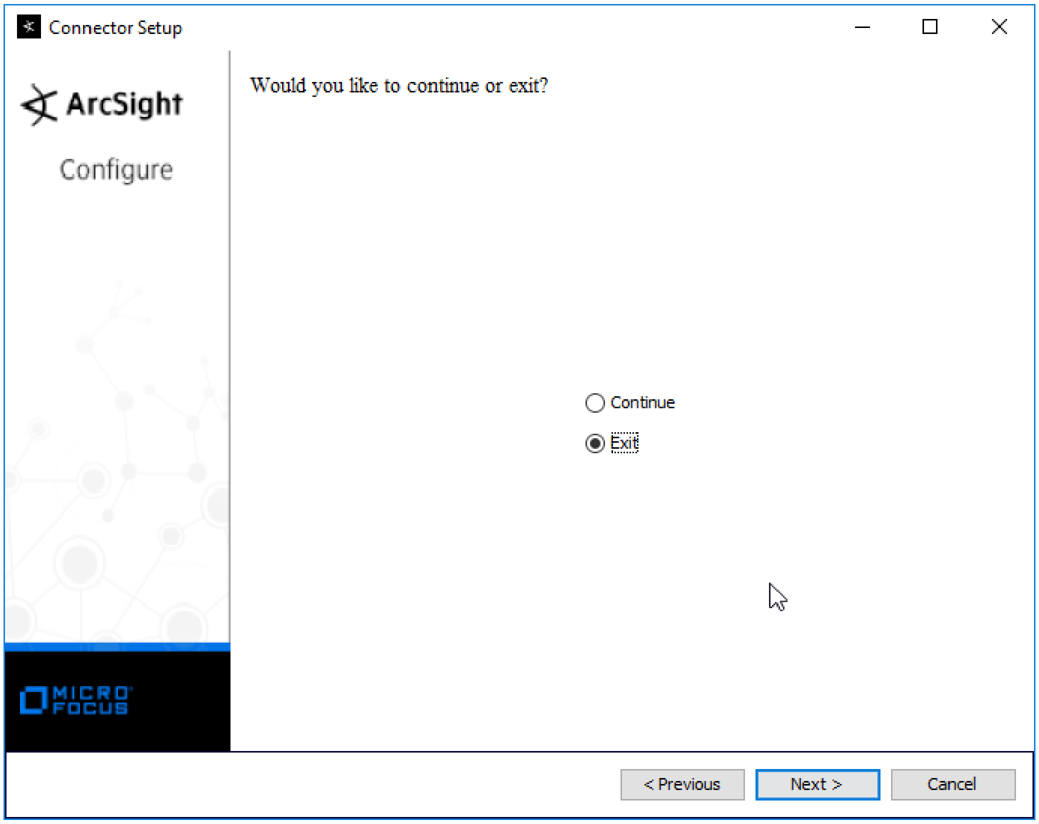
23. Click **Next.**



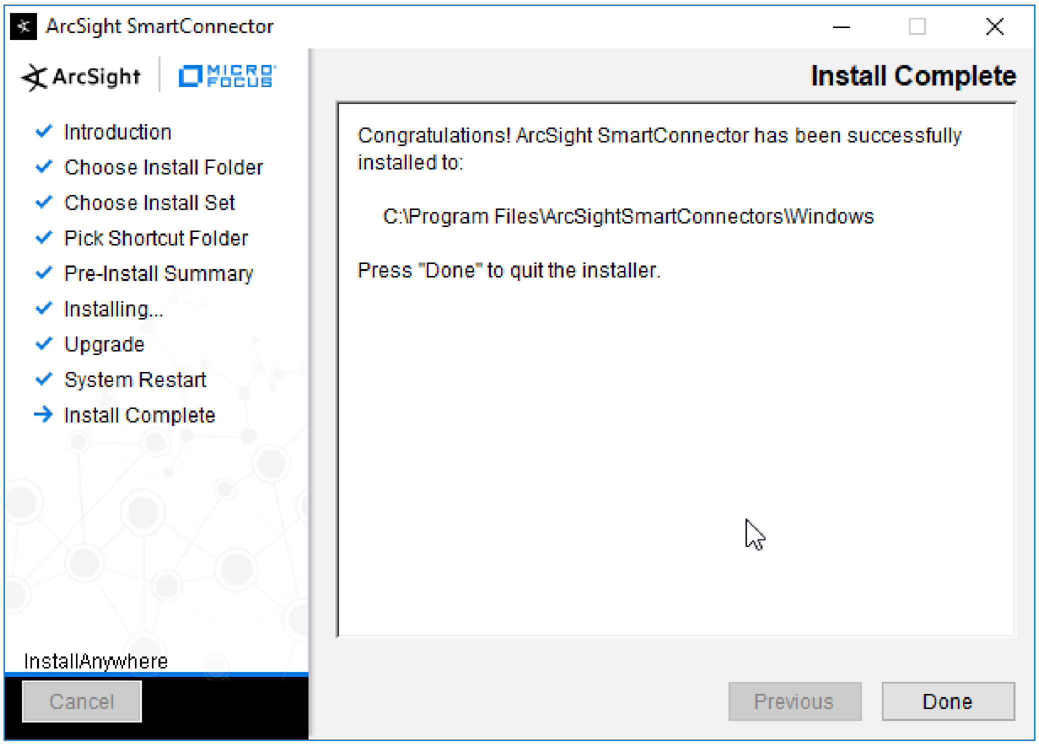
1321
1322 24. Click **Next.**



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



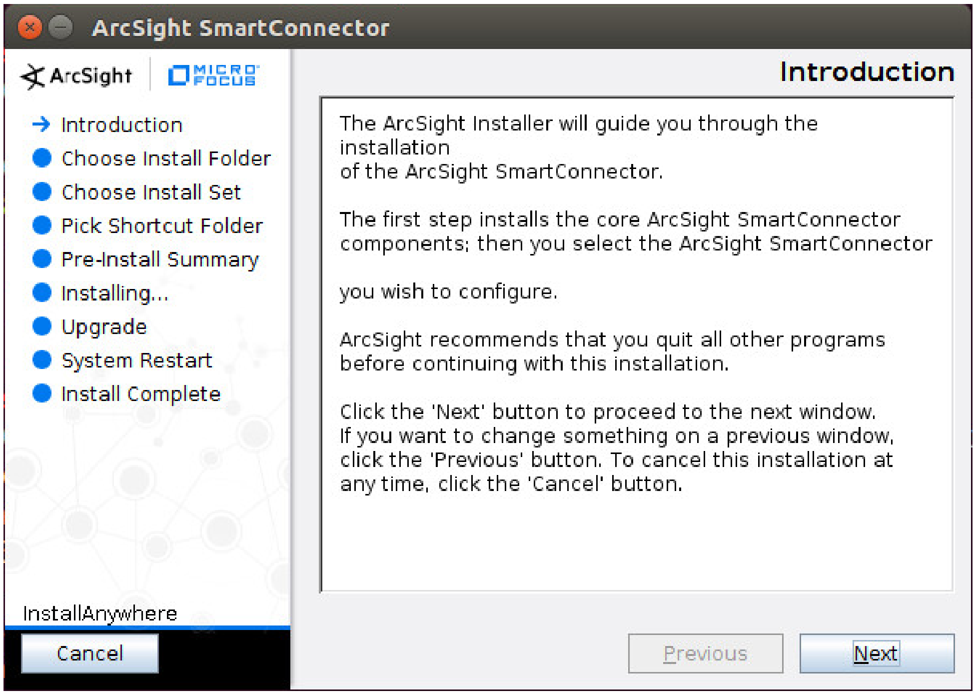
27. Click **Next.**



28. Click **Done.**

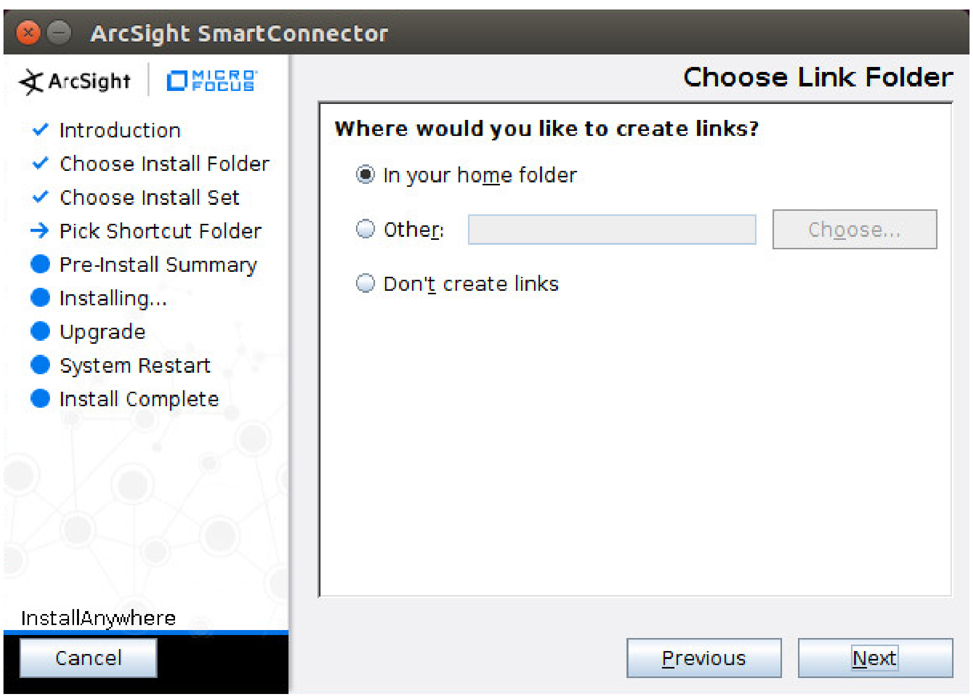
2.8.3 Install Individual ArcSight Ubuntu Connectors

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

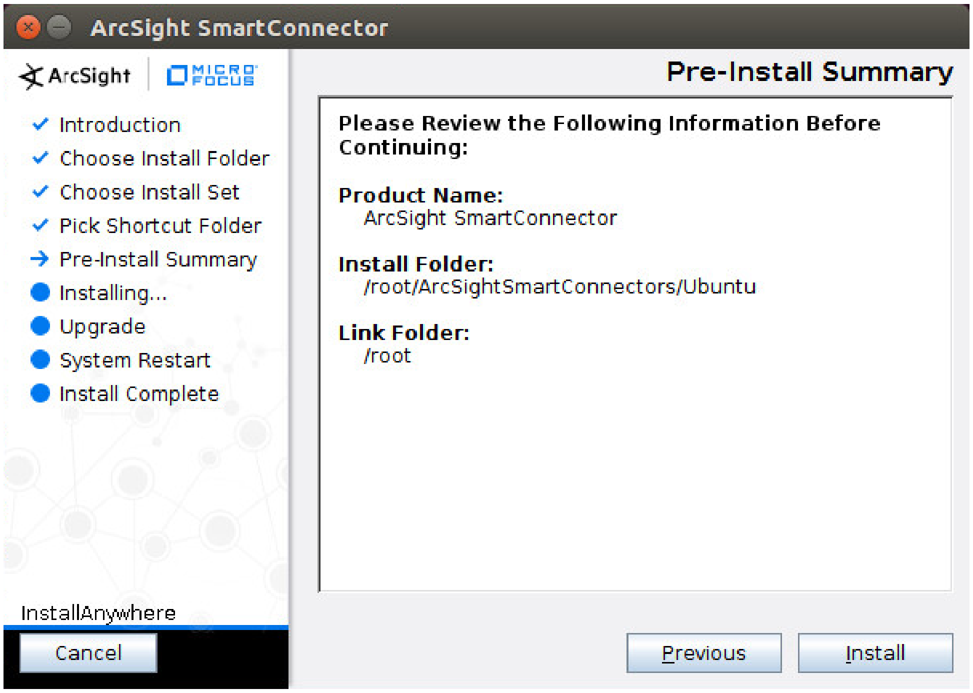


3. Click **Next.**
4. Enter */root/ArcSightSmartConnectors/Ubuntu.*

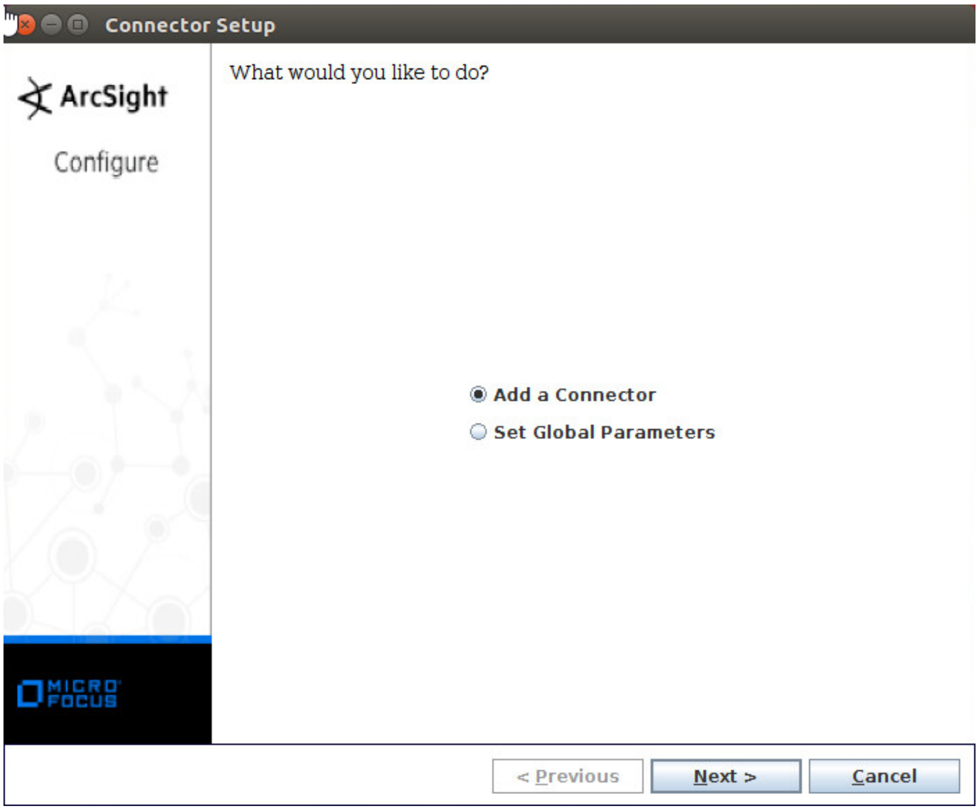
5. Click **Next.**



6. Click **Next.**



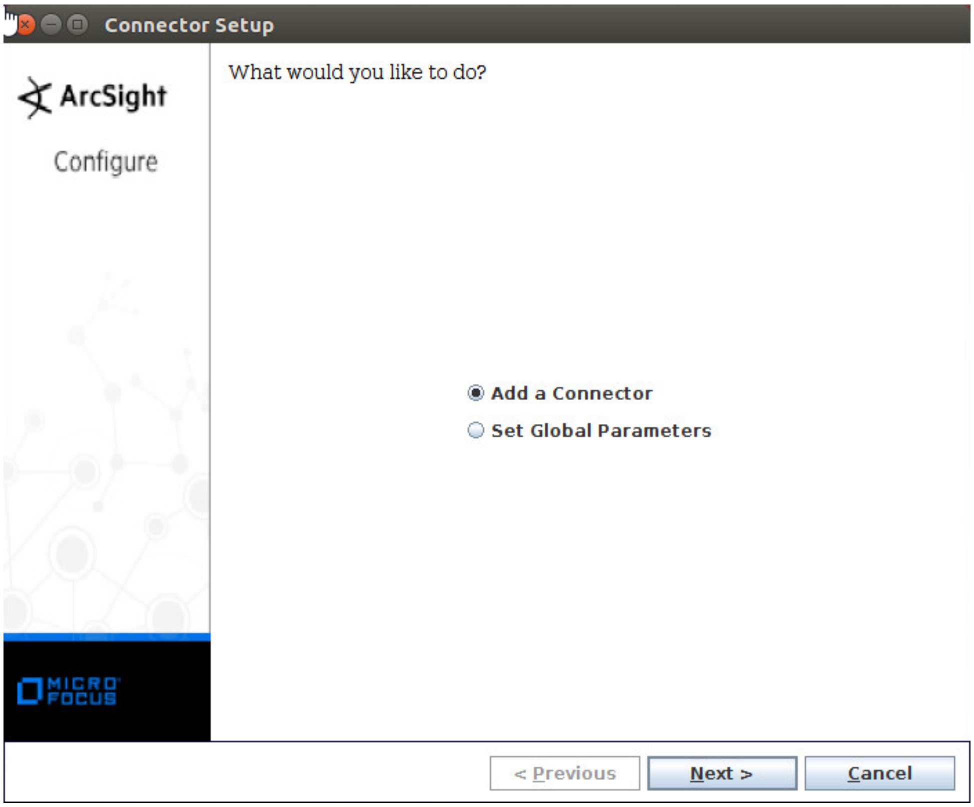
7. Click **Install.**
8. Select **Add a Connector.**



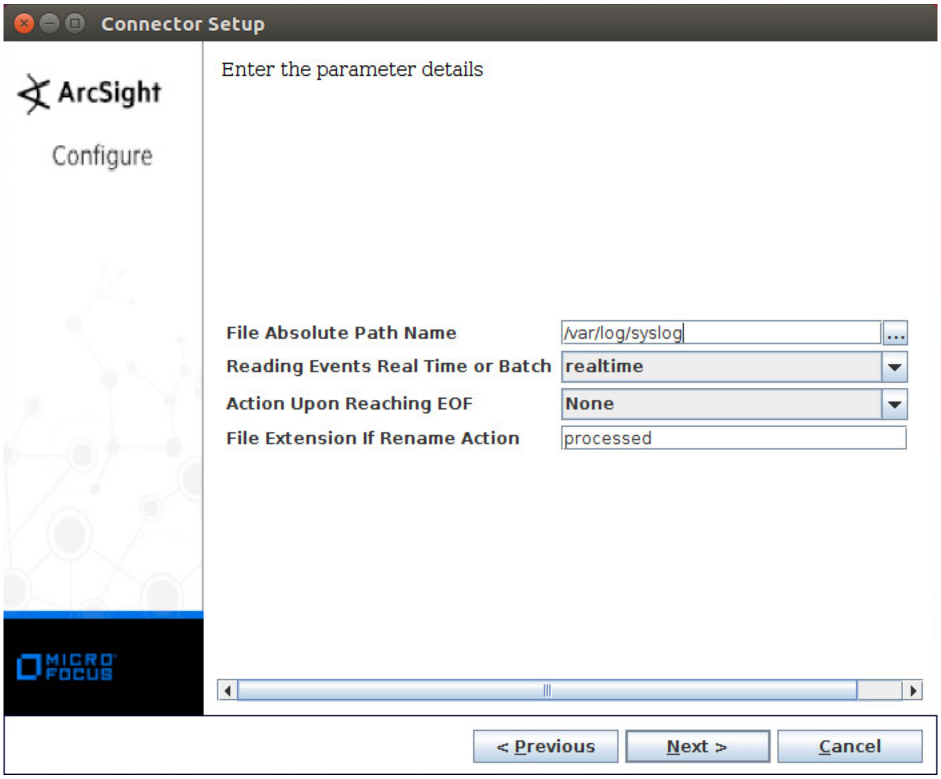
1344

1345 9. Click **Next.**

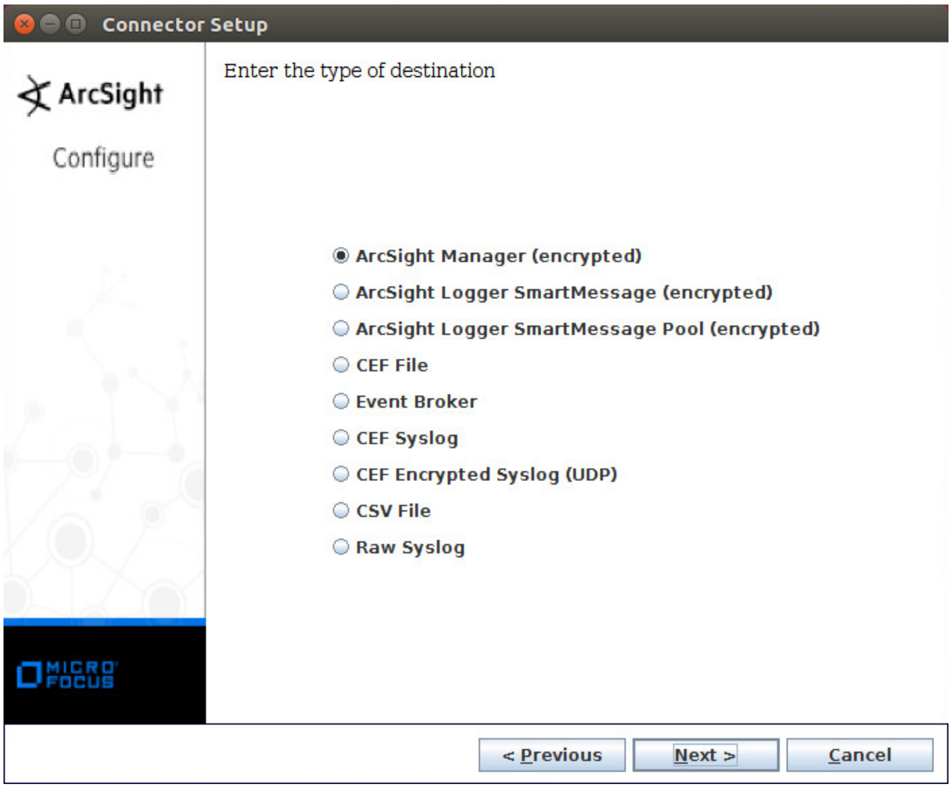
1346 10. Select **Syslog File.**



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



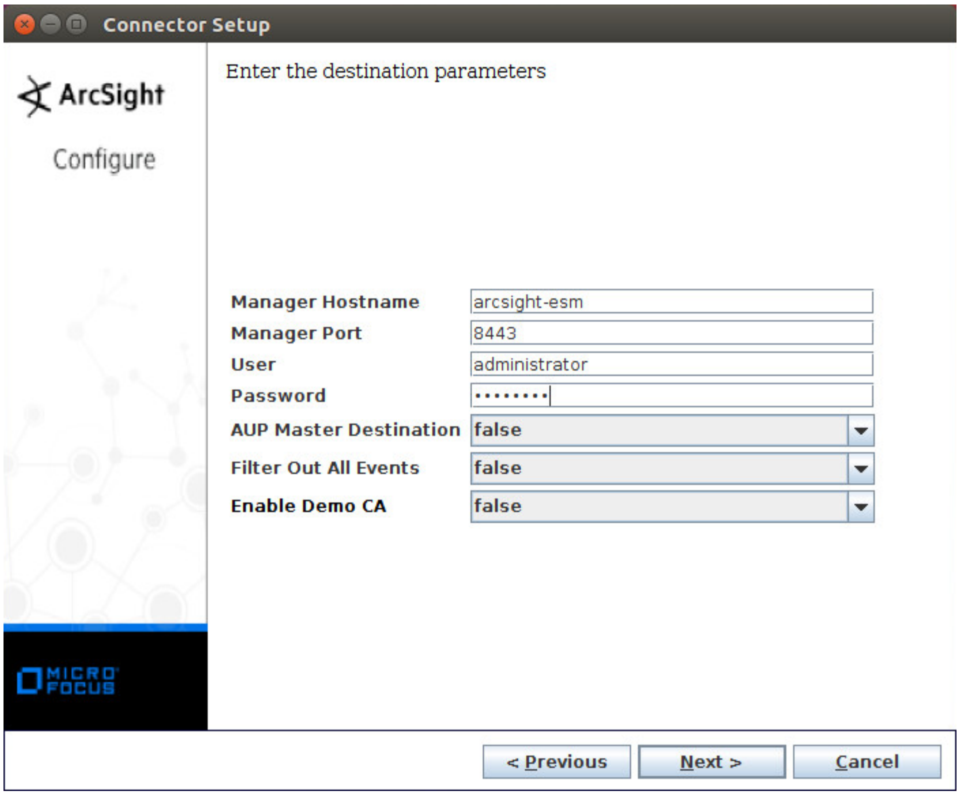
13. Click **Next.**
14. Select **ArcSight Manager** (encrypted).



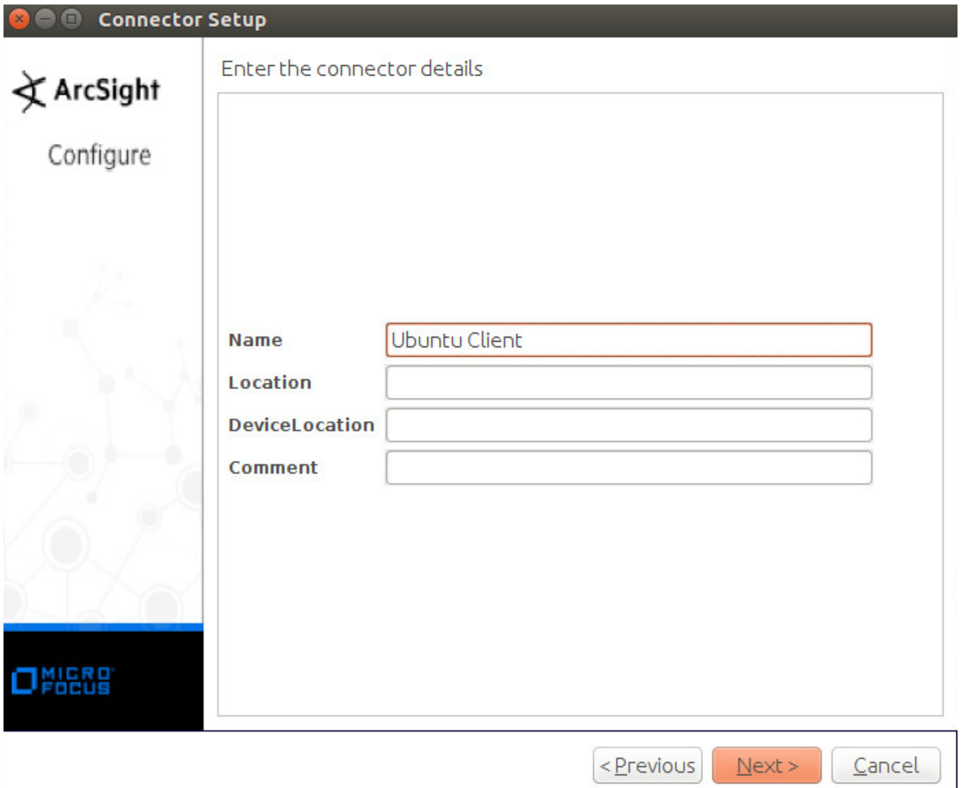
1353

1354 15. Click **Next.**

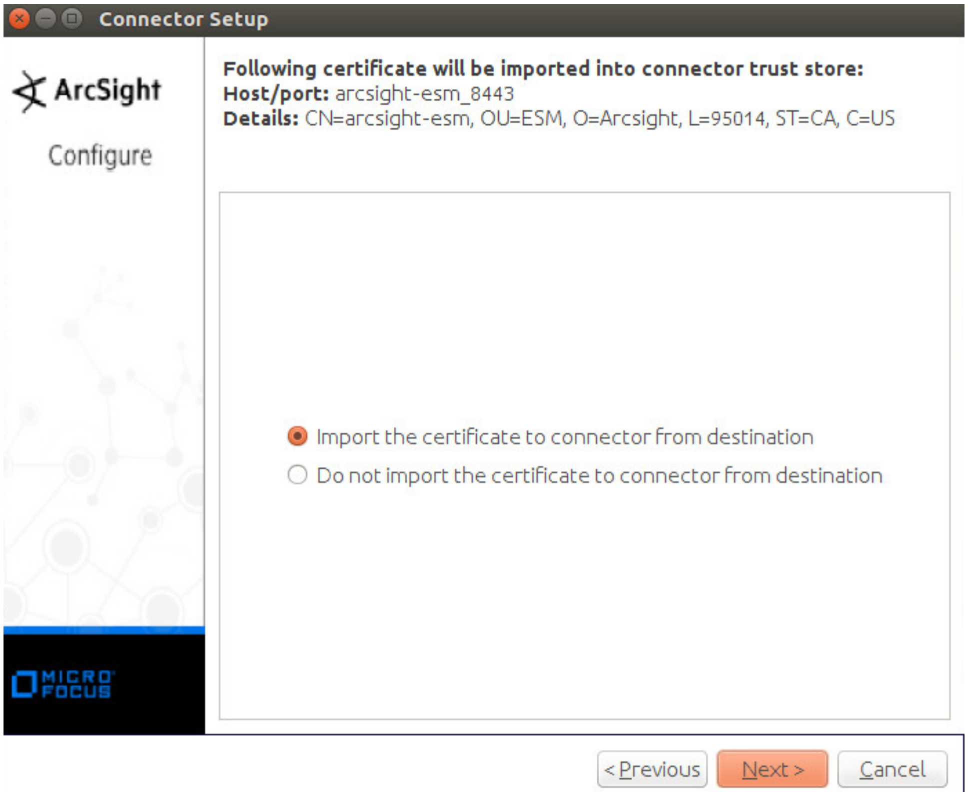
1355 16. Enter the **hostname, port, username,** and **password** for ArcSight ESM.



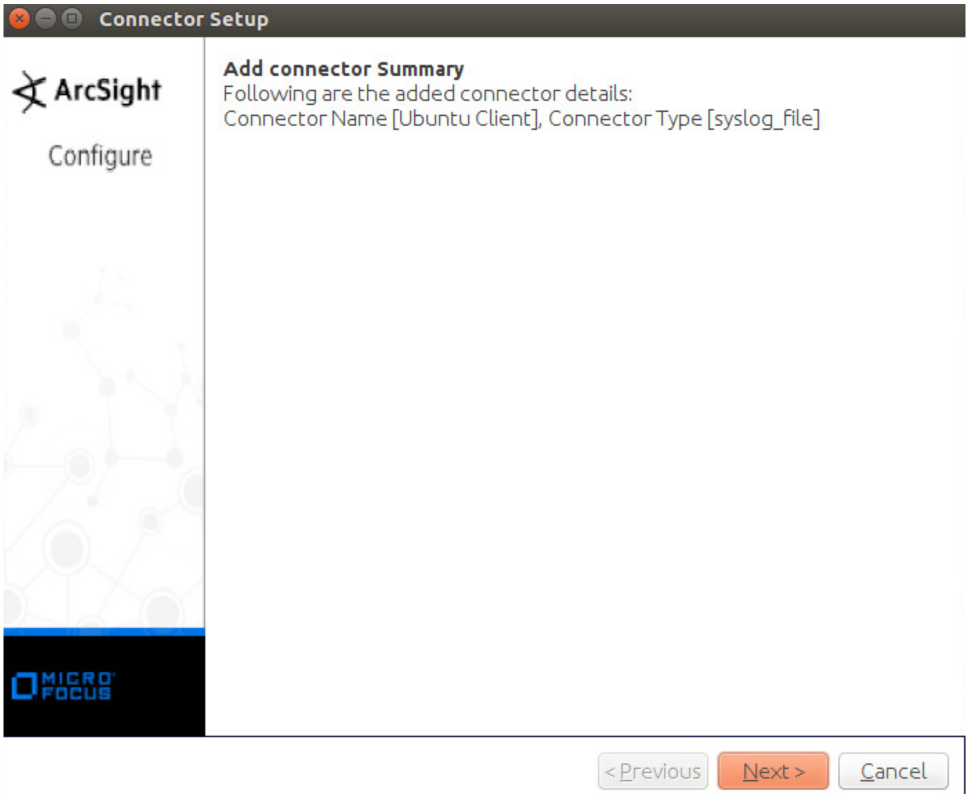
17. Click **Next.**
18. Enter identifying details about the system (only **Name** is required).



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



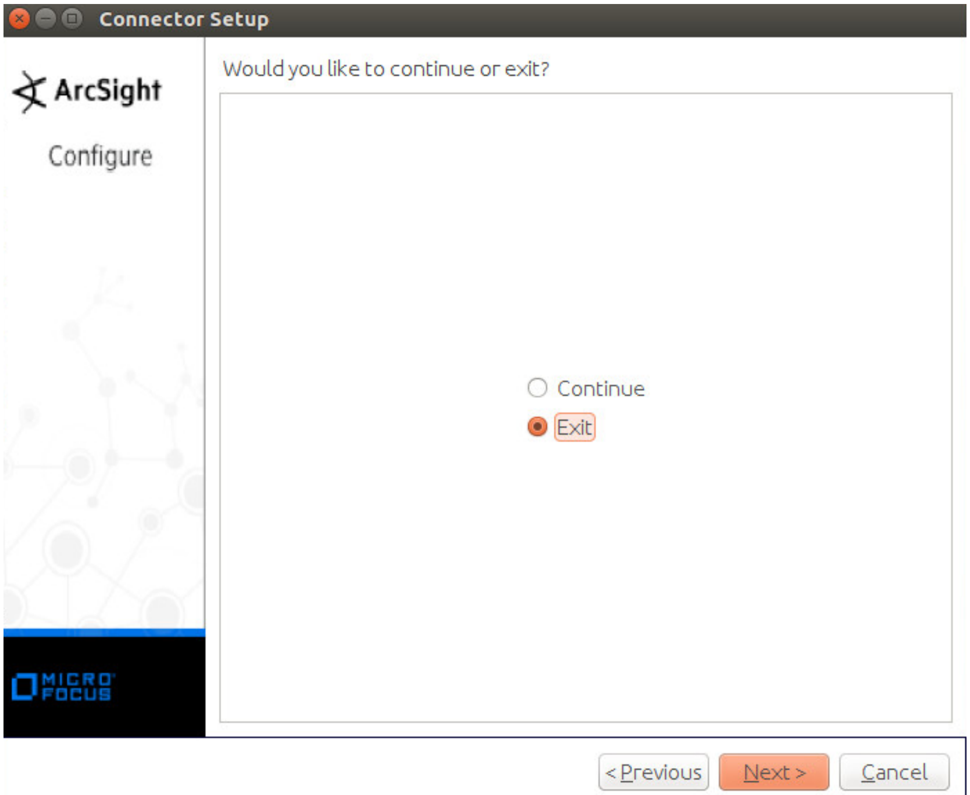
21. Click **Next.**



1364

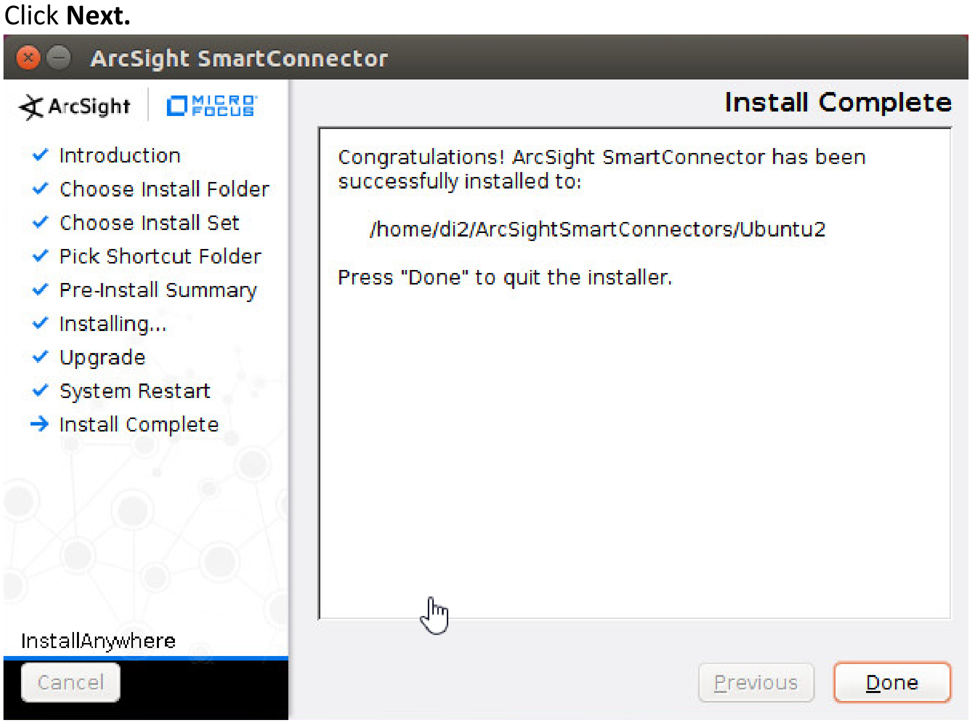
1365 22. Click **Next.**

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



1369

1370 25. Click **Next.**

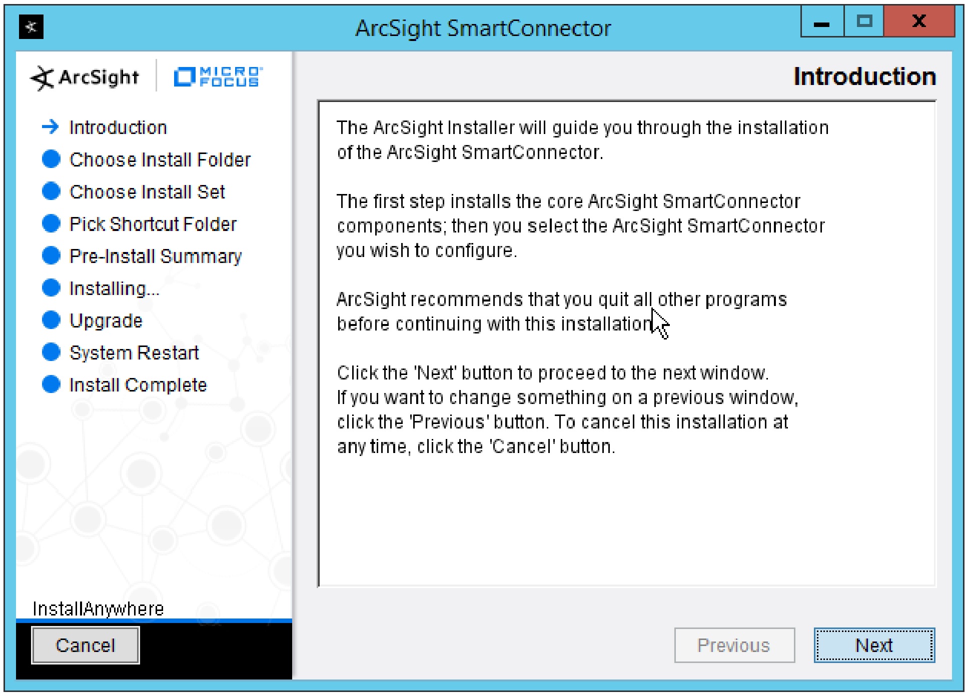


1371

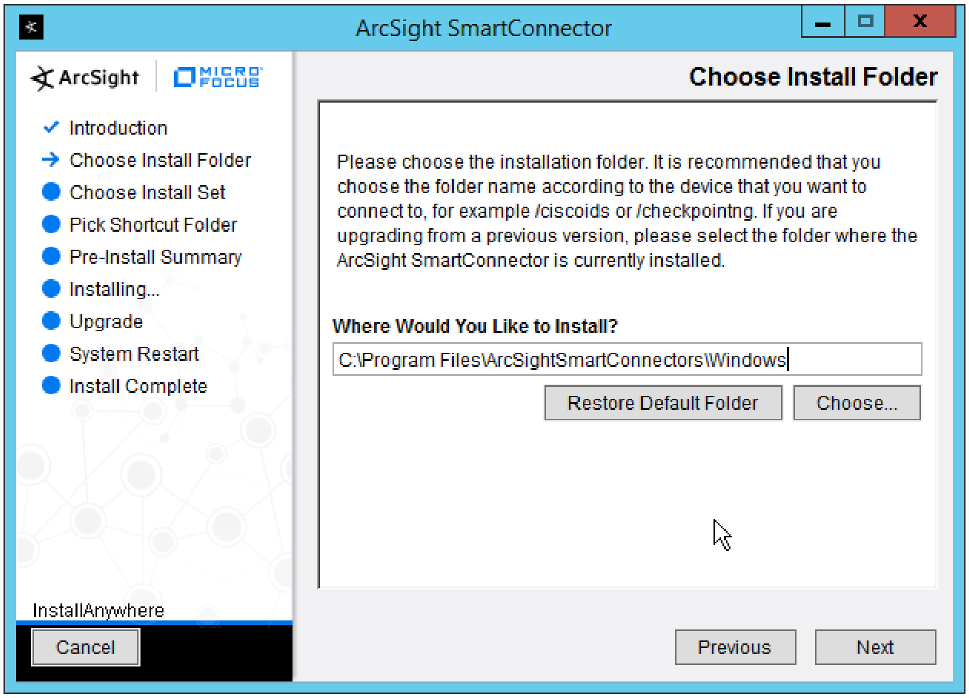
26. Click **Done.**

2.8.4 Install a Connector Server for ESM on Windows 2012 R2

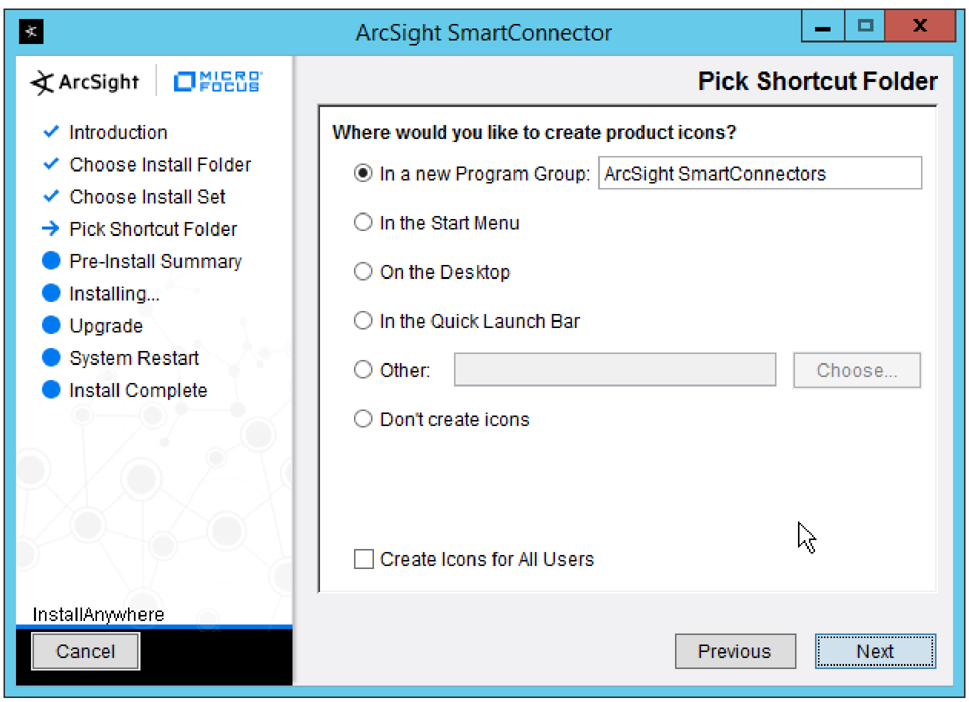
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe.**



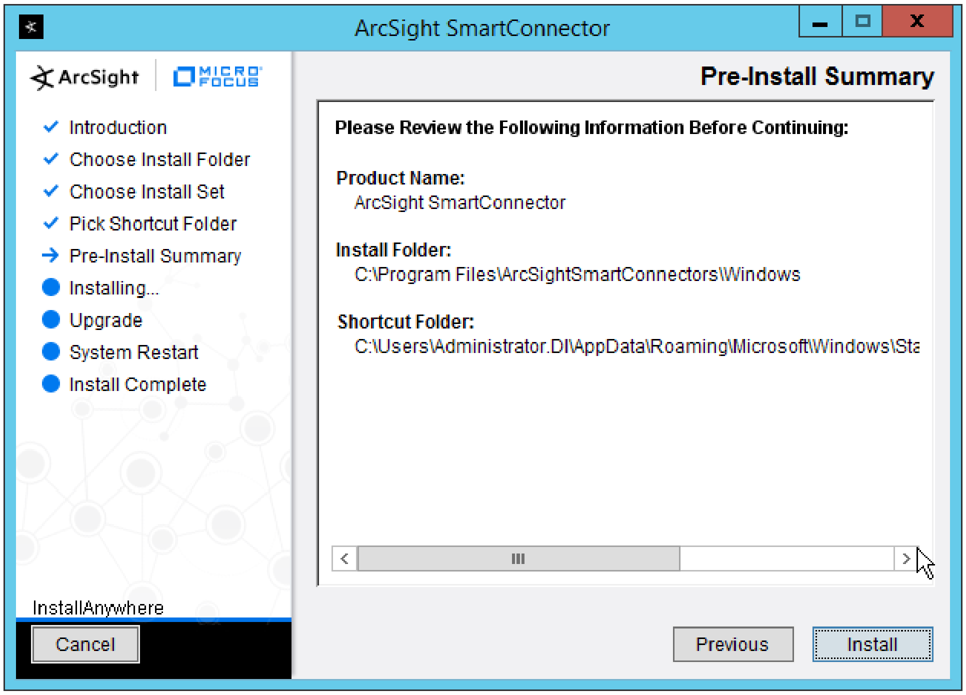
2. Click **Next.**
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows.*



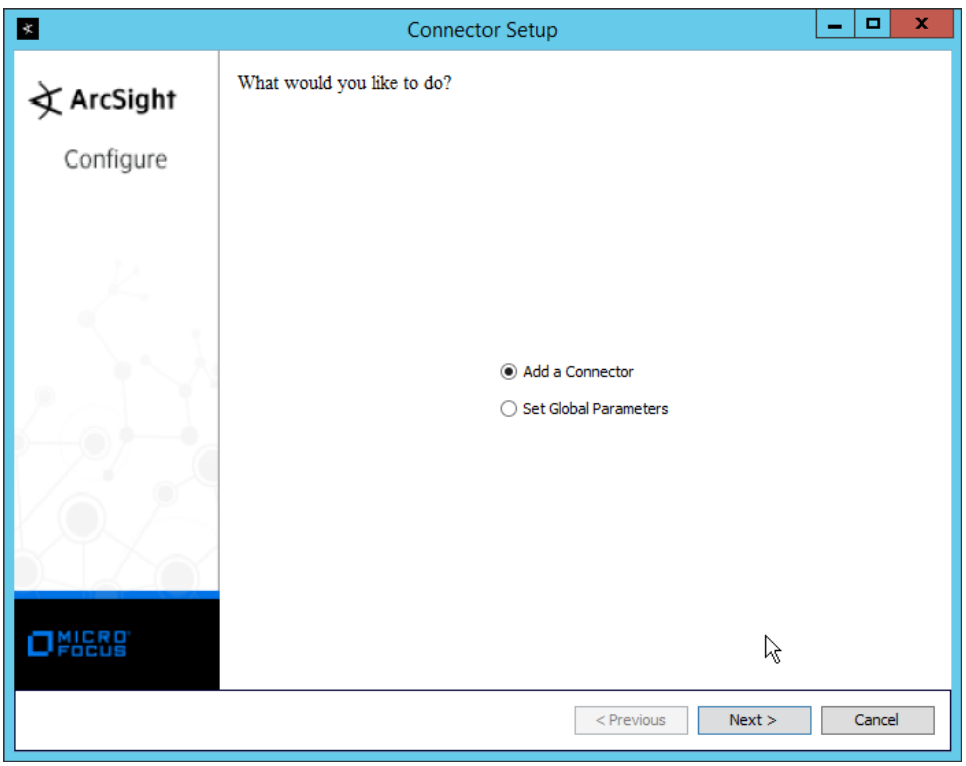
4. Click **Next.**



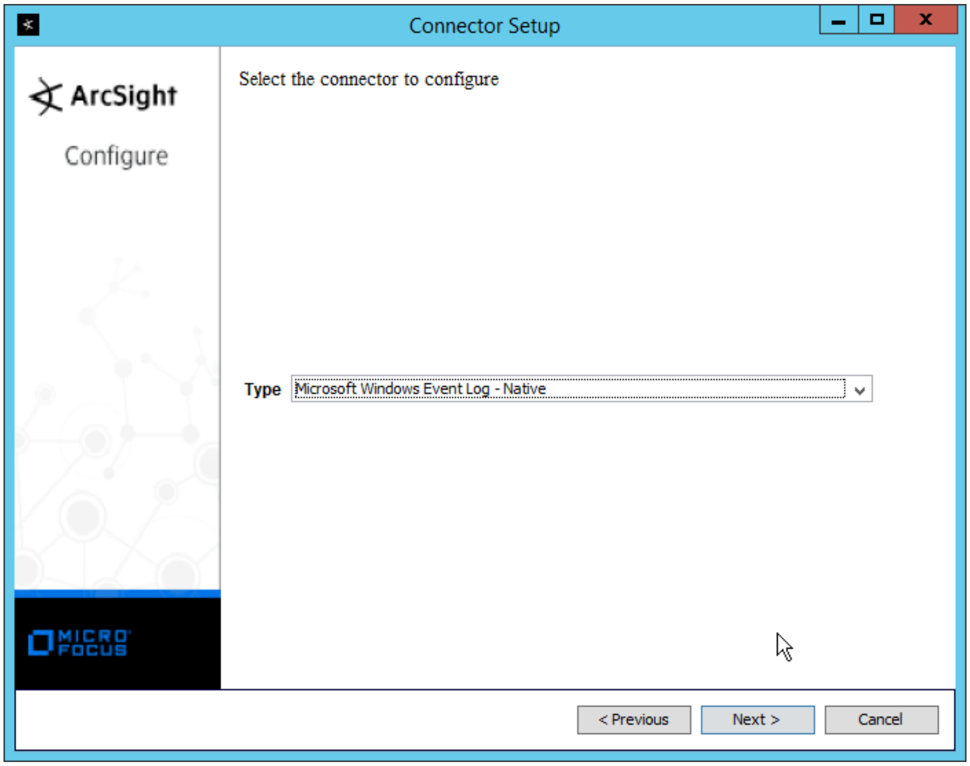
5. Click **Next.**



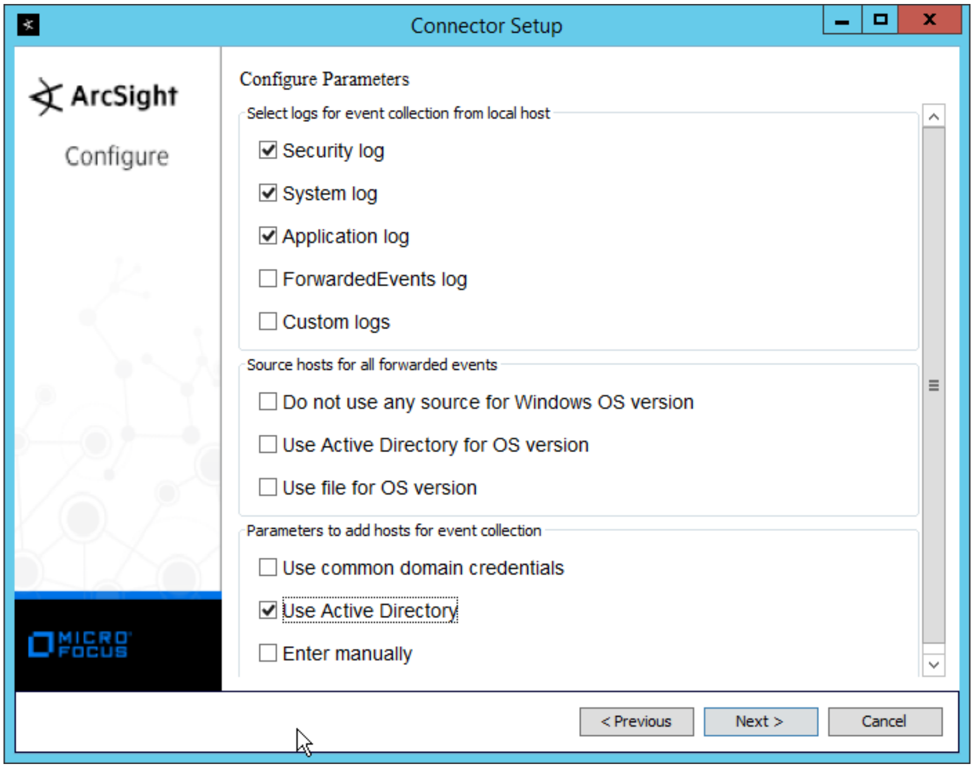
6. Click **Install.**
7. Select **Add a Connector.**



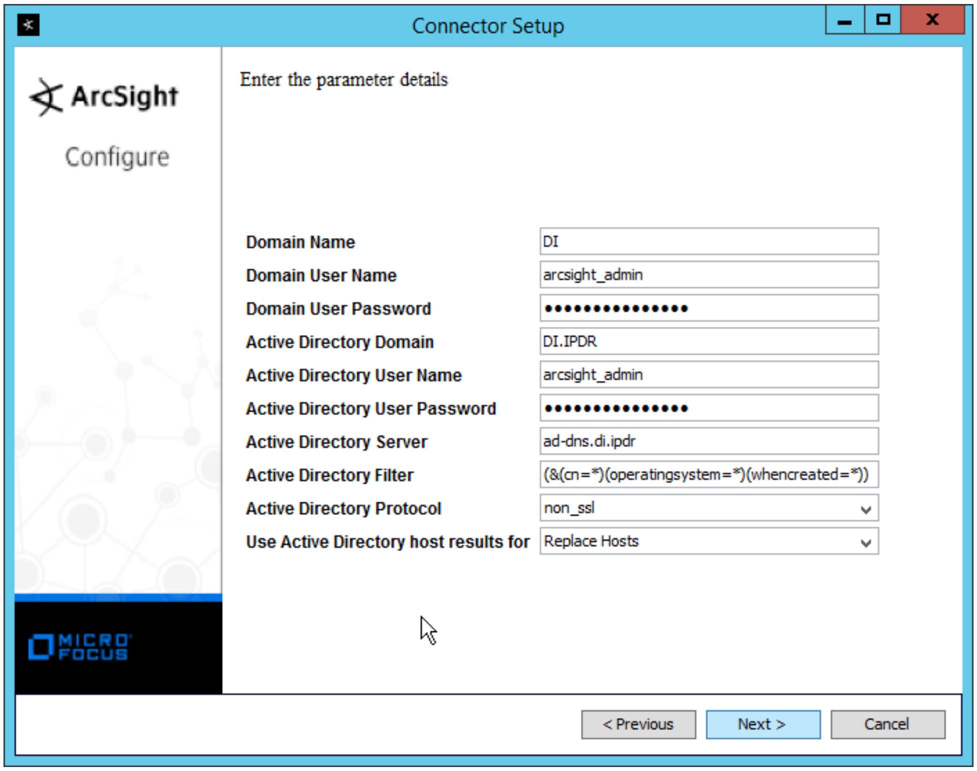
8. Click **Next.**
9. Select **Microsoft Windows Event Log – Native.**



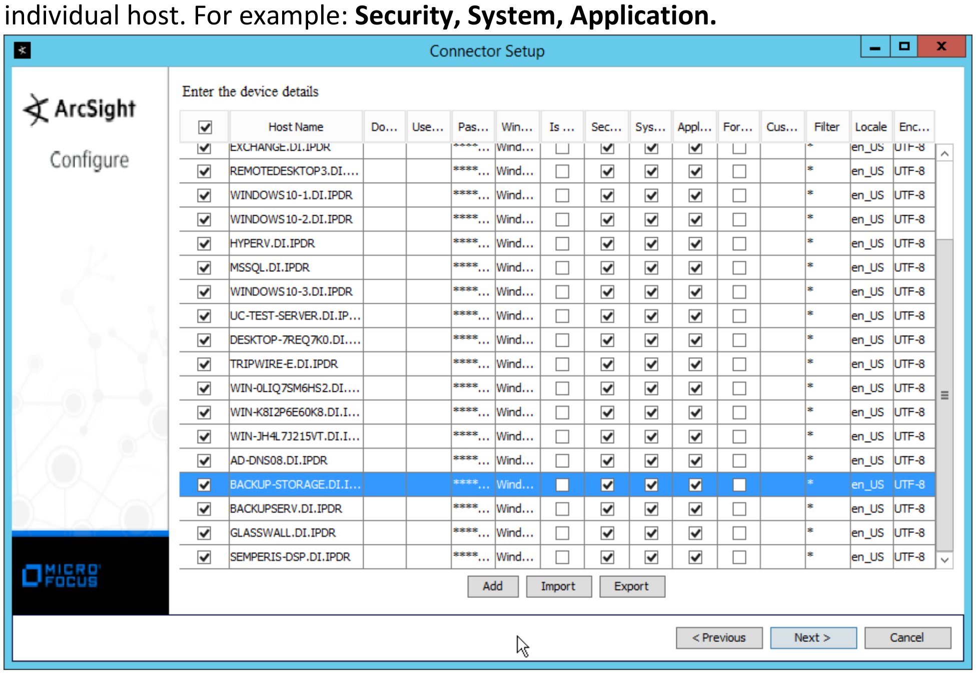
10. Click **Next.**
11. Check the box next to **Use Active Directory.**



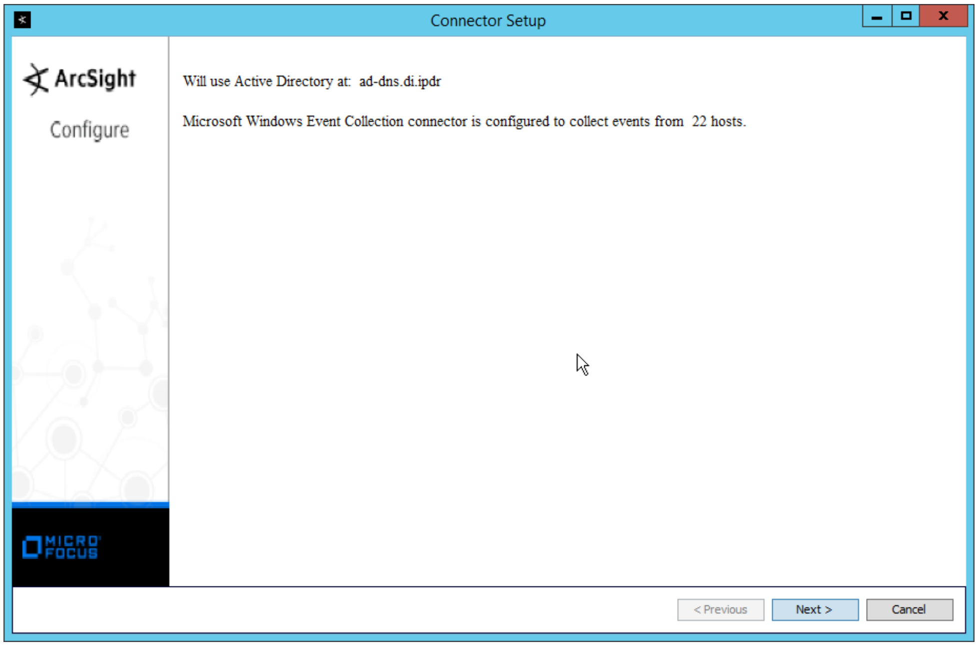
12. Click **Next.**
13. Enter information about your Active Directory server (it is recommended to create a new administrator account for ArcSight to use).
14. Set **Use Active Directory host results for** to **Replace Hosts**.



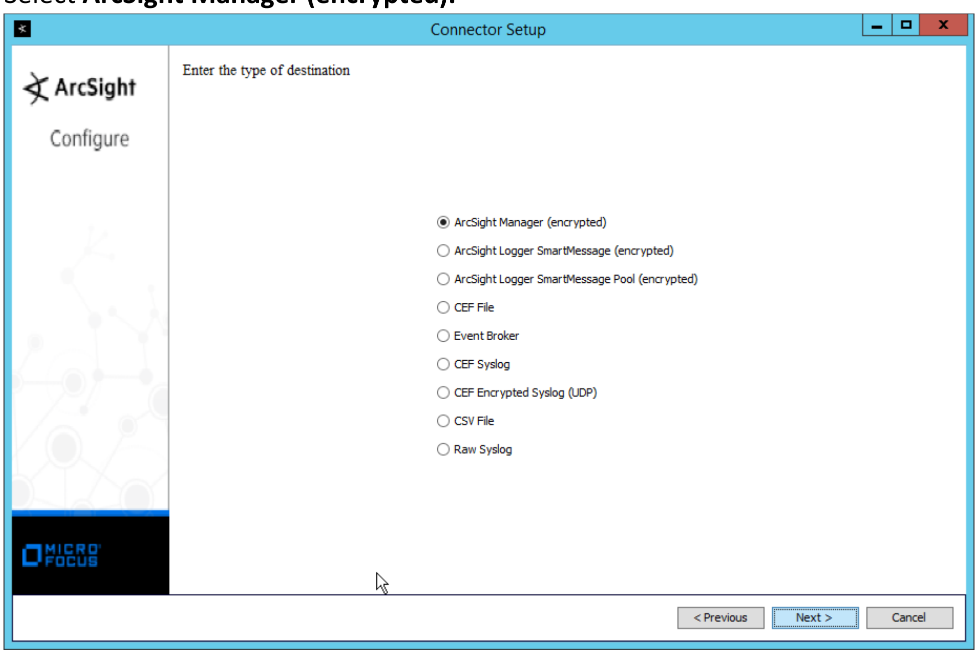
15. Click **Next.**
16. Check the boxes under any event types that should be forwarded to this connector, for each individual host. For example: **Security, System, Application.**



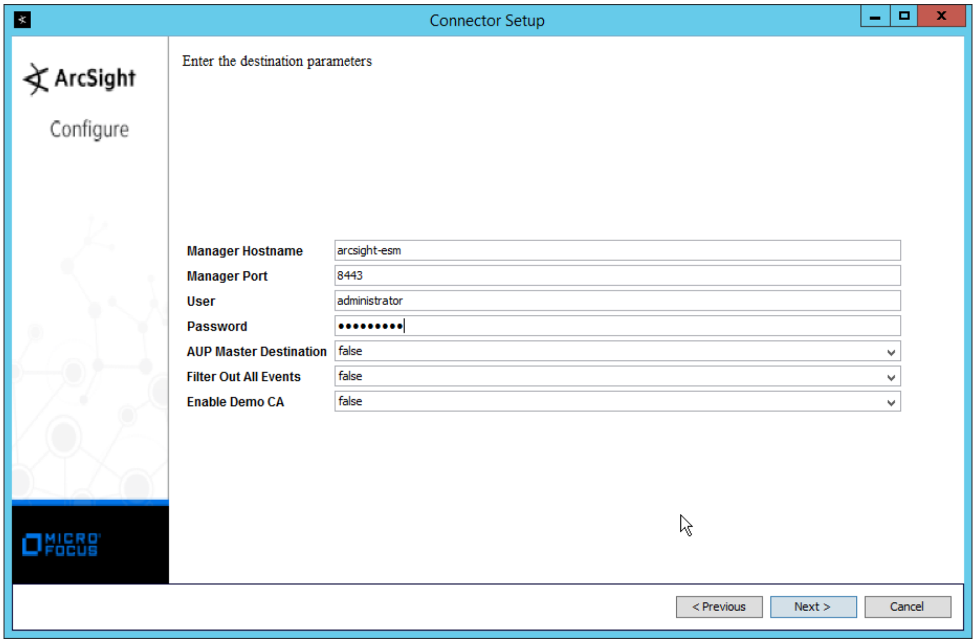
17. Click **Next.**



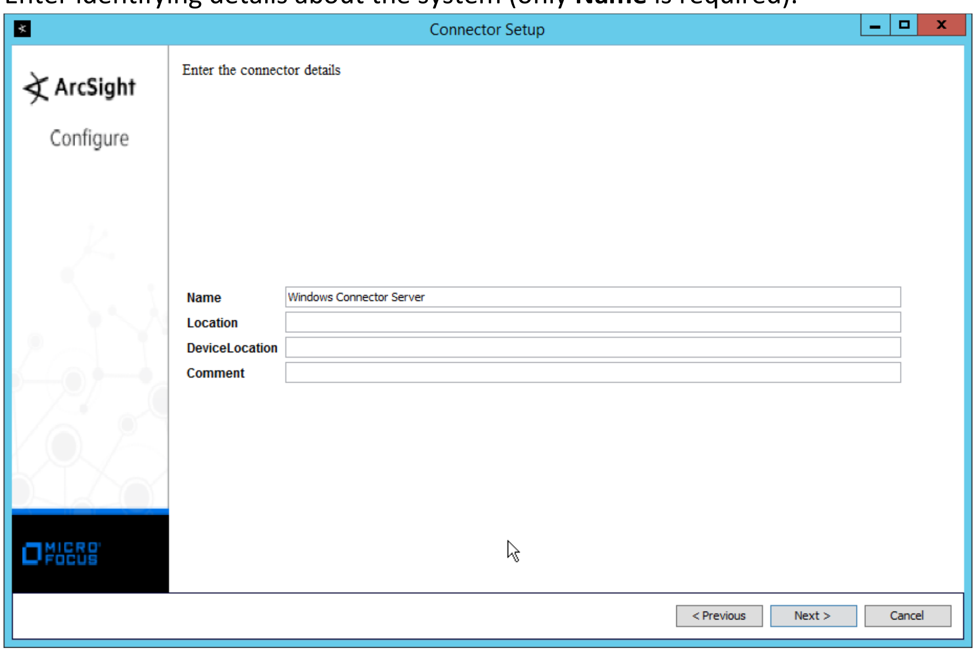
18. Click **Next.**
19. Select **ArcSight Manager (encrypted).**



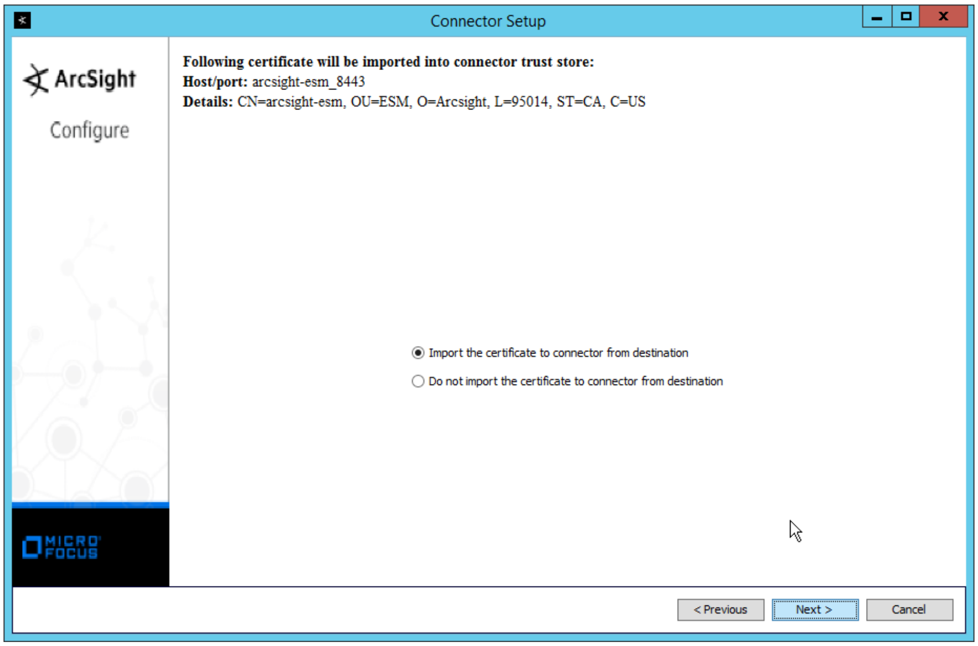
20. Click **Next.**
21. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



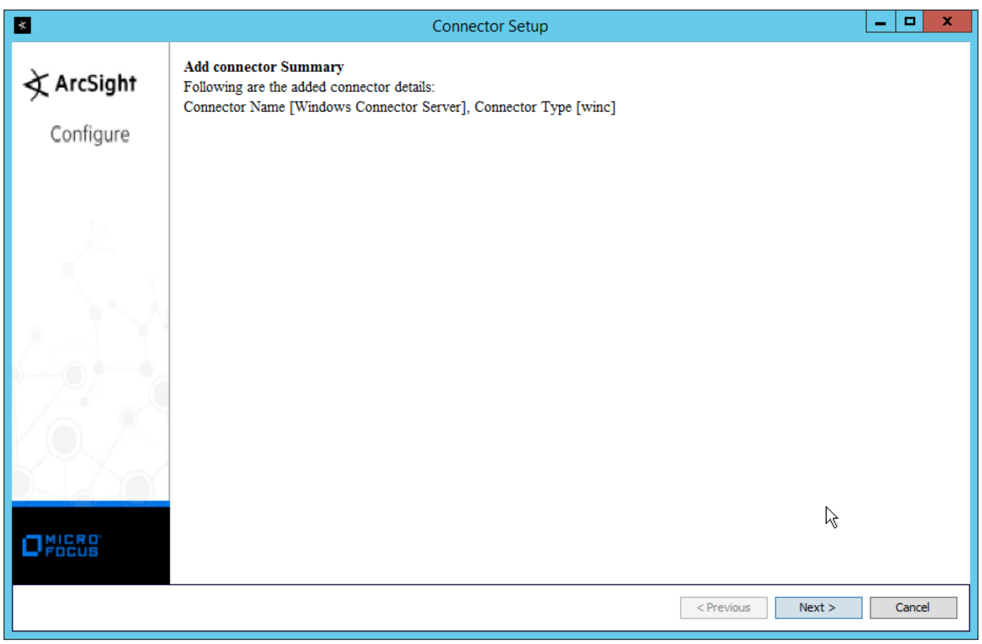
22. Click **Next.**
23. Enter identifying details about the system (only **Name** is required).



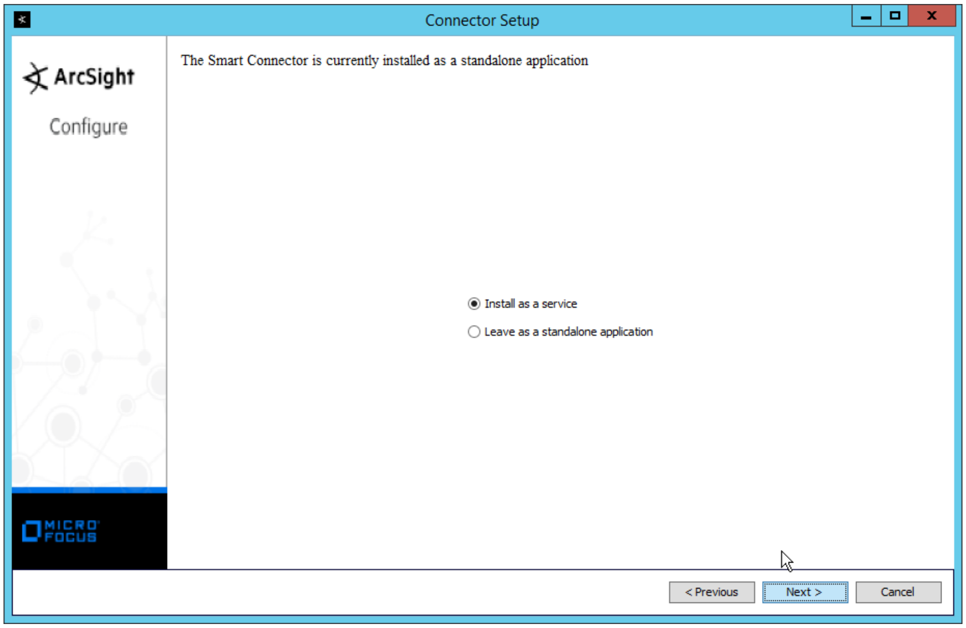
24. Click **Next.**
25. Select **Import the certificate to connector from destination.**



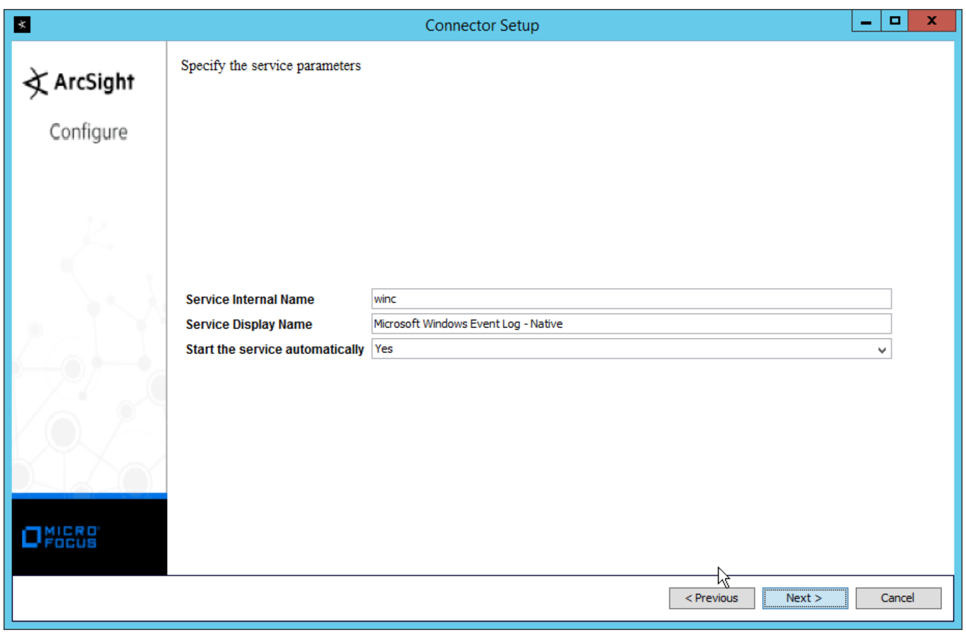
26. Click **Next.**



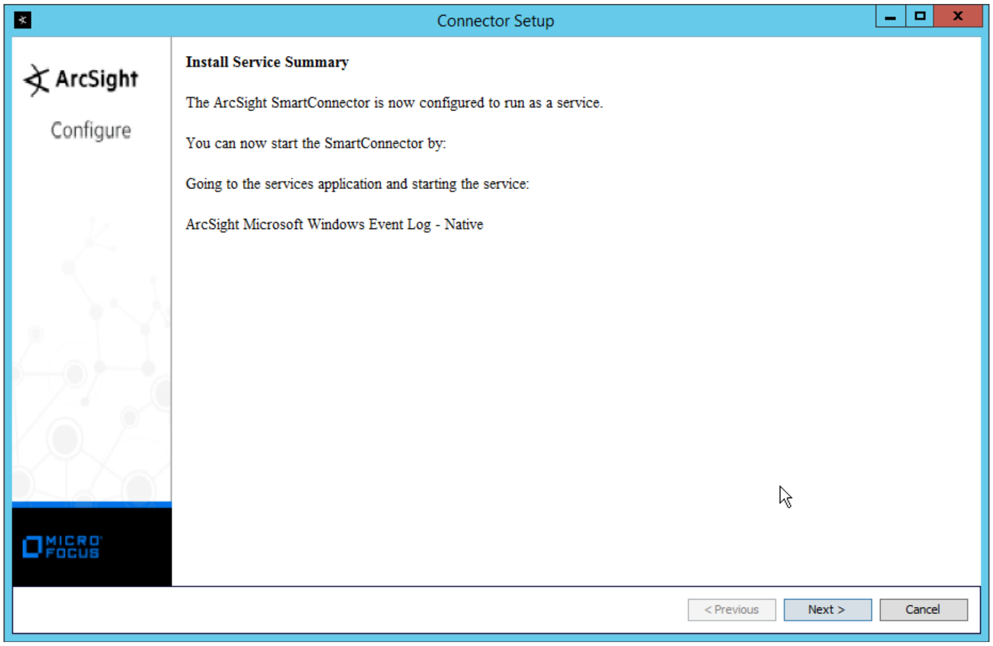
27. Click **Next.**
28. Select **Install as a service.**



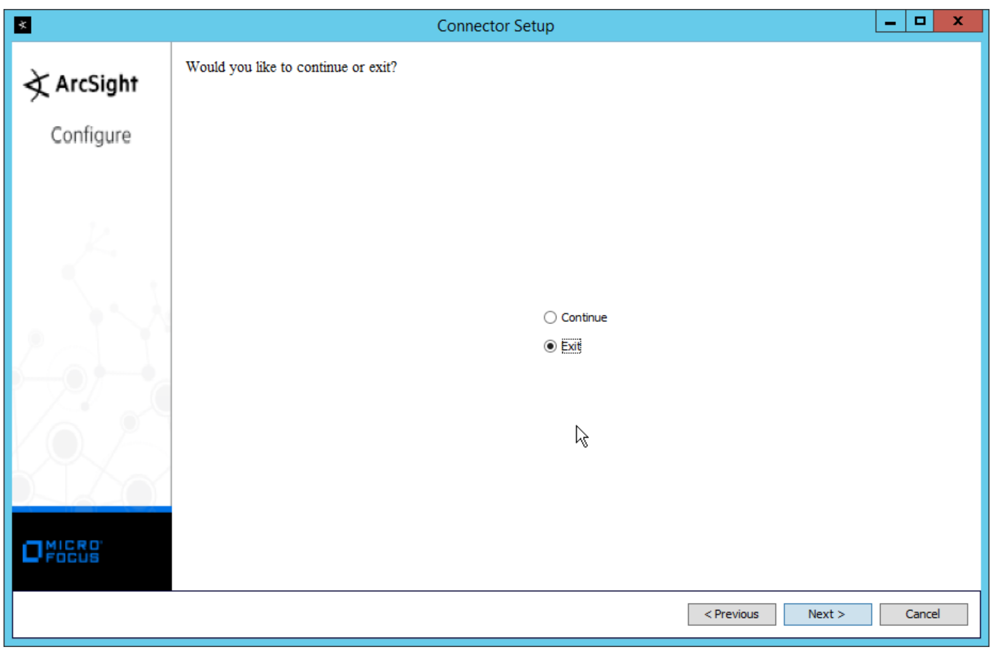
29. Click **Next.**



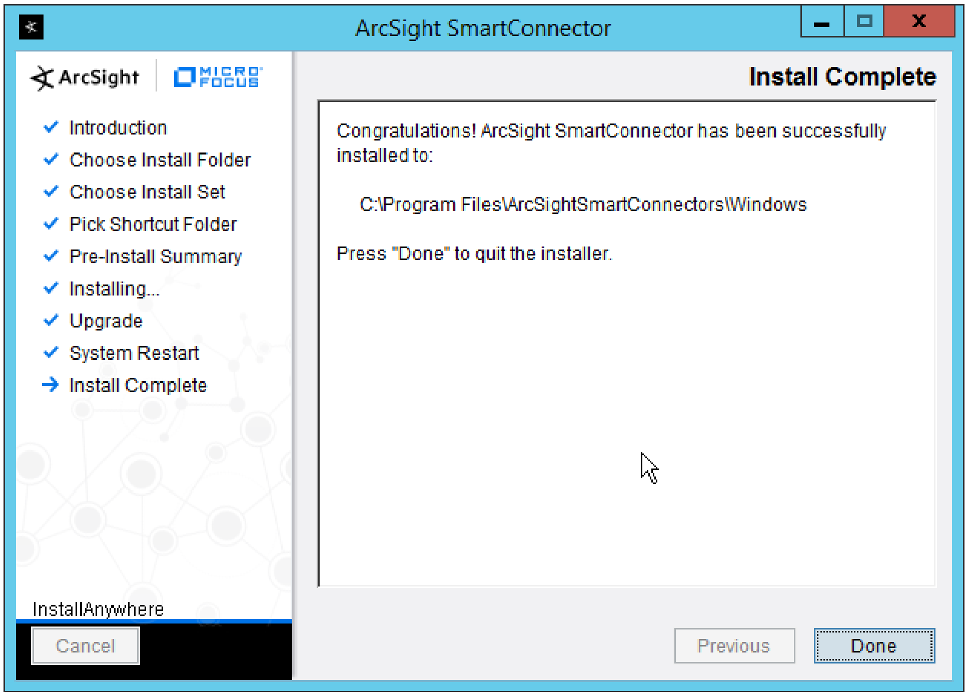
30. Click **Next.**



31. Click **Next.**
32. Select **Exit.**



33. Click **Next.**

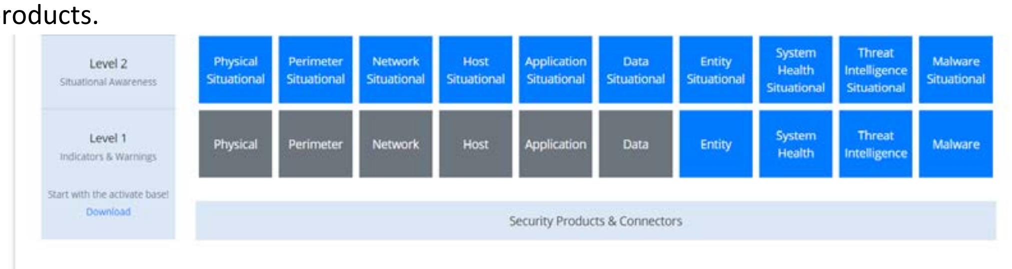


34. Click **Done.**
35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.

2.8.5 Install Pre-Configured Filters for ArcSight

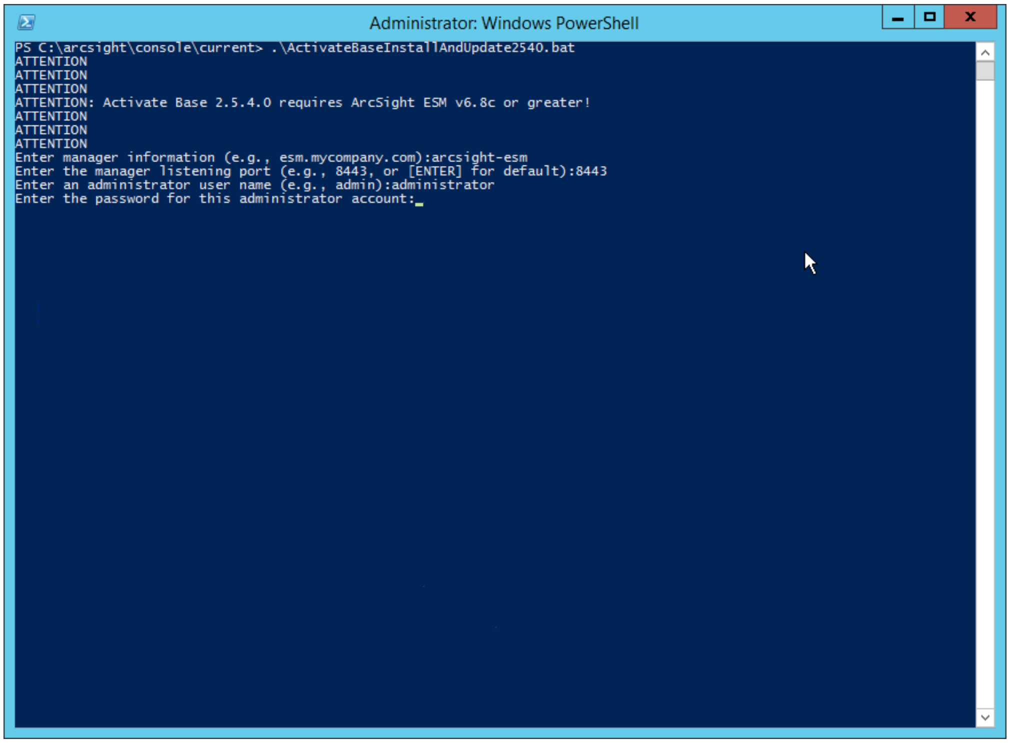
2.8.5.1 *Install Activate Base*

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

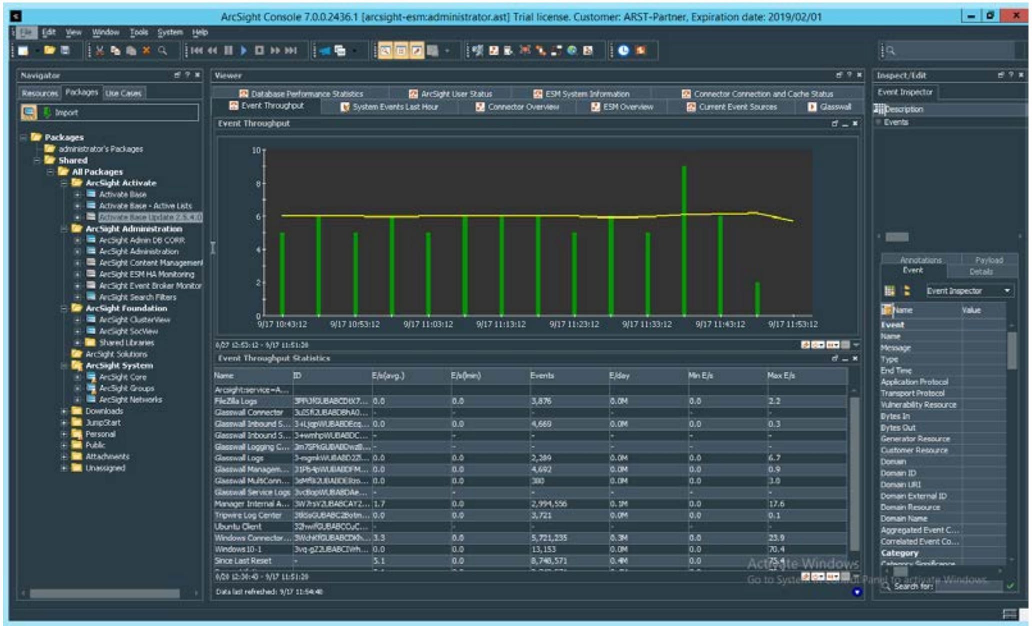


2. Click the **Download** link for the activate base. (Note: This package should be installed on the Arcsight Console, not on the ESM.)
3. Copy the contents of the zip file to *ARCSIGHT_HOME*. The default for this is *C:\arcsight\Console\current*, assuming a Windows Server.

4. In PowerShell, navigate to the *ARCSIGHT_HOME* directory *(C:\arcsight\Console\current),* and run:
`> .\ActivateBaseInstallAndUpdate2540.bat`



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

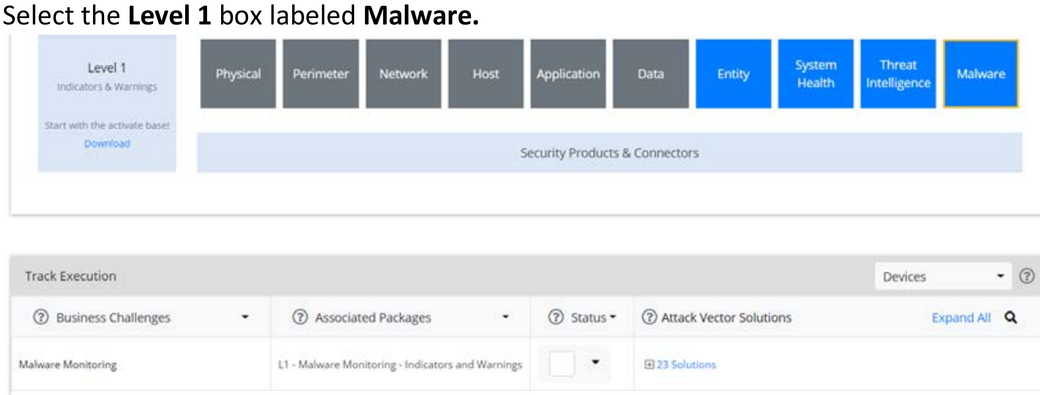


8. Under **Packages > Shared > All Packages > ArcSight Activate,** right-click **Activate Base Update 2.5.4.0,** and select **Delete Package.**

2.8.5.2 *Install Packages*

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

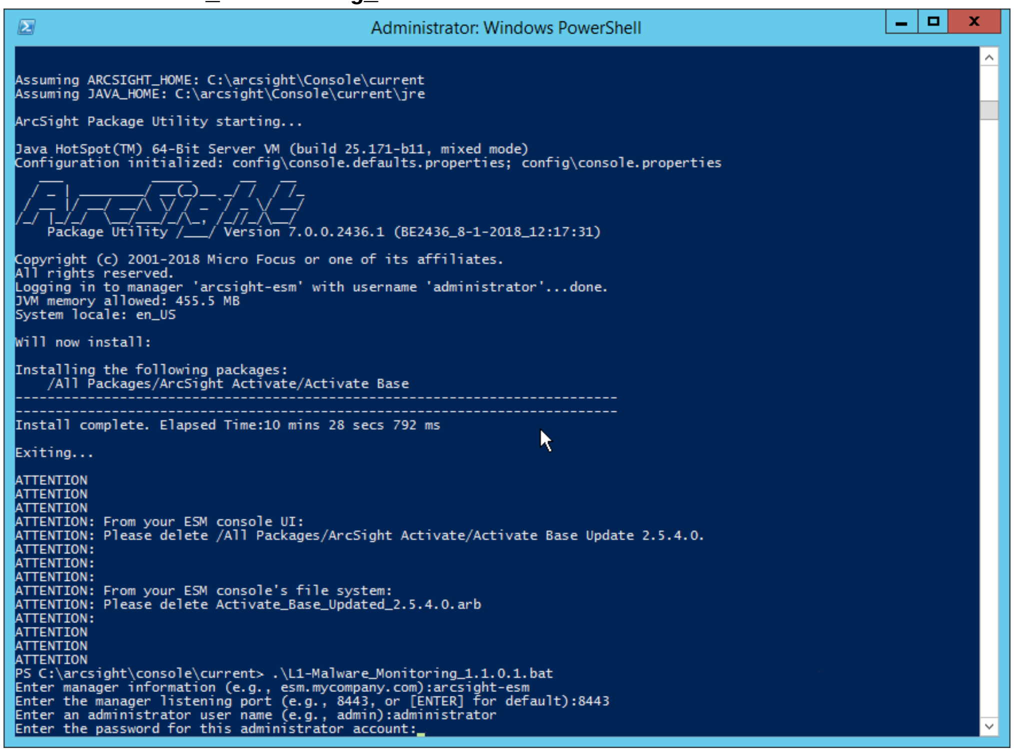
1. Navigate to the **ArcSight Content Brain** web app.
2. Select the **Level 1** box labeled **Malware.**



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

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

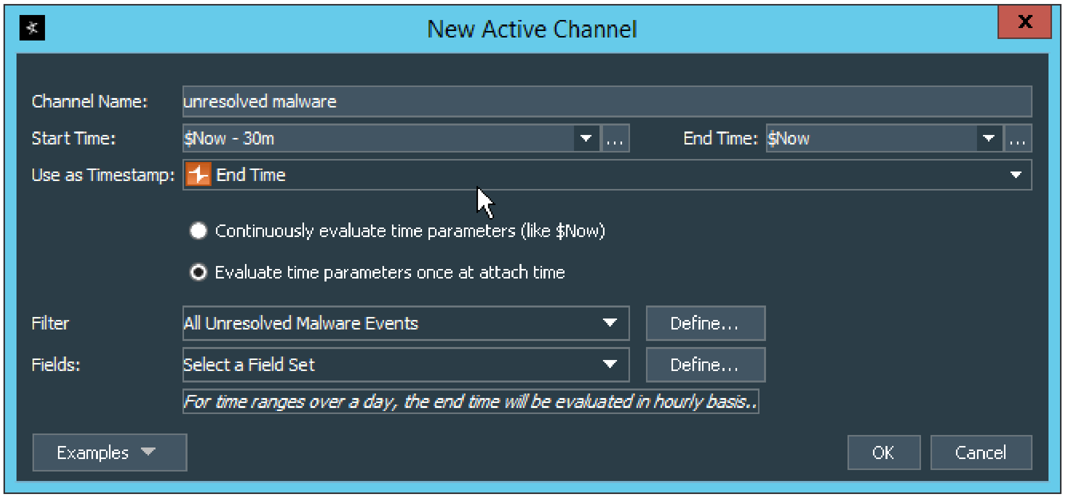
```
> .\L1-Malware_Monitoring_1.1.0.1.bat
```



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

2.8.6 Apply Filters to a Channel

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

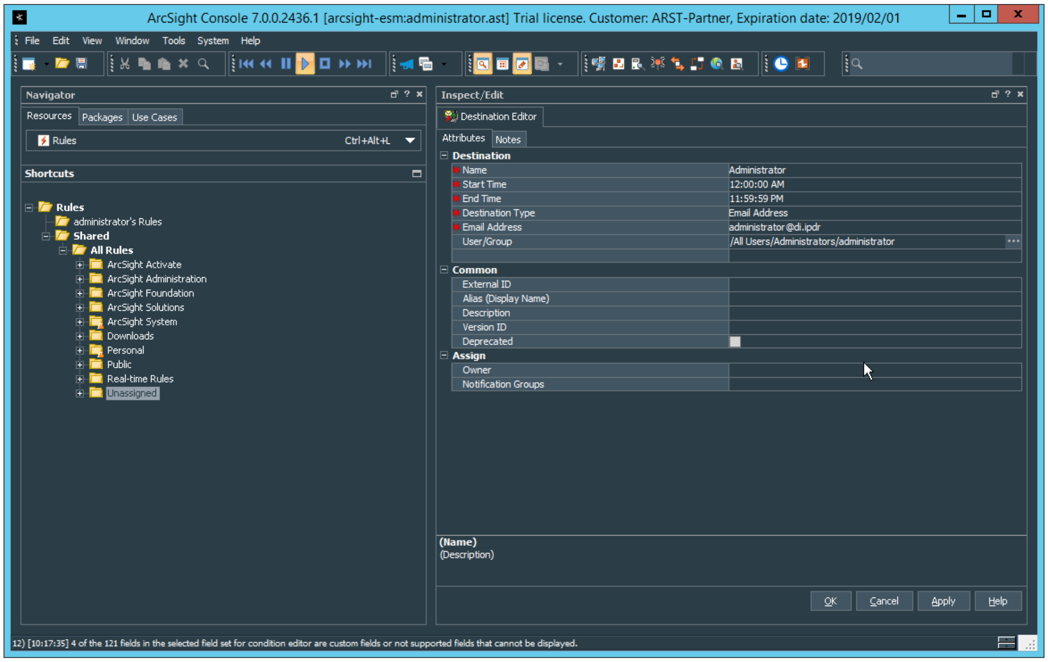


5. Click **OK.** All events that match the filter can be displayed in the newly created channel. Filters from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate > Solutions.**

2.8.7 Configure Email Alerts in ArcSight

2.8.7.1 Configure a New Destination

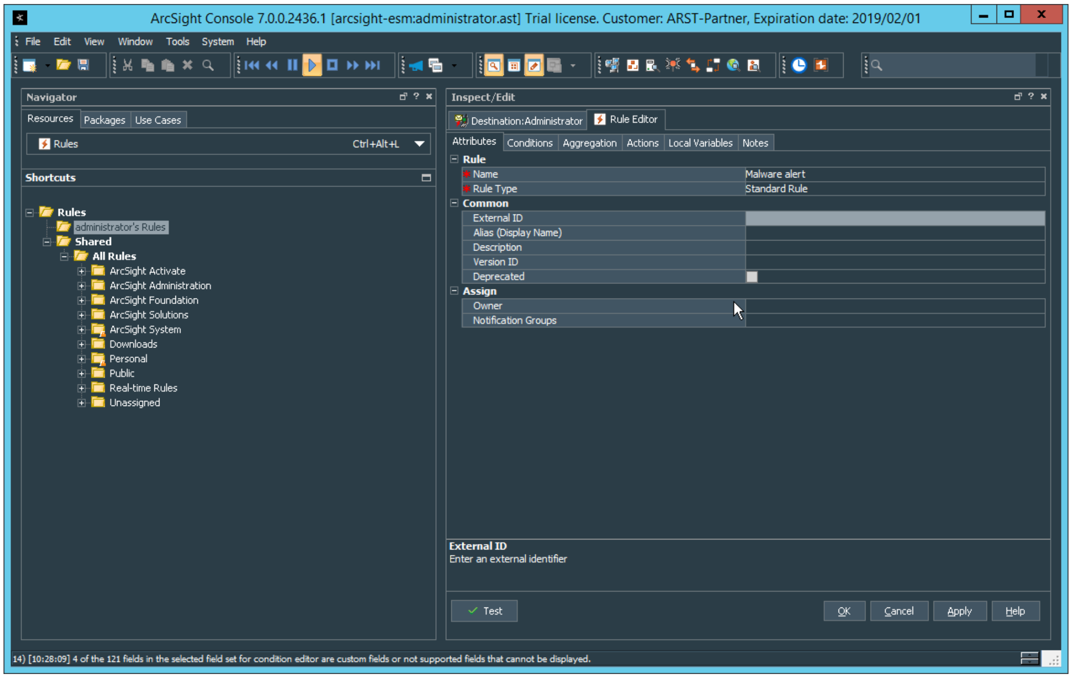
1. In **ArcSight Console,** click **File > New > Destination.**
2. Enter a name for the **Destination.**
3. For **Destination Type,** select **Email Address.**
4. For **Email Address,** enter the email that should be associated with this destination.



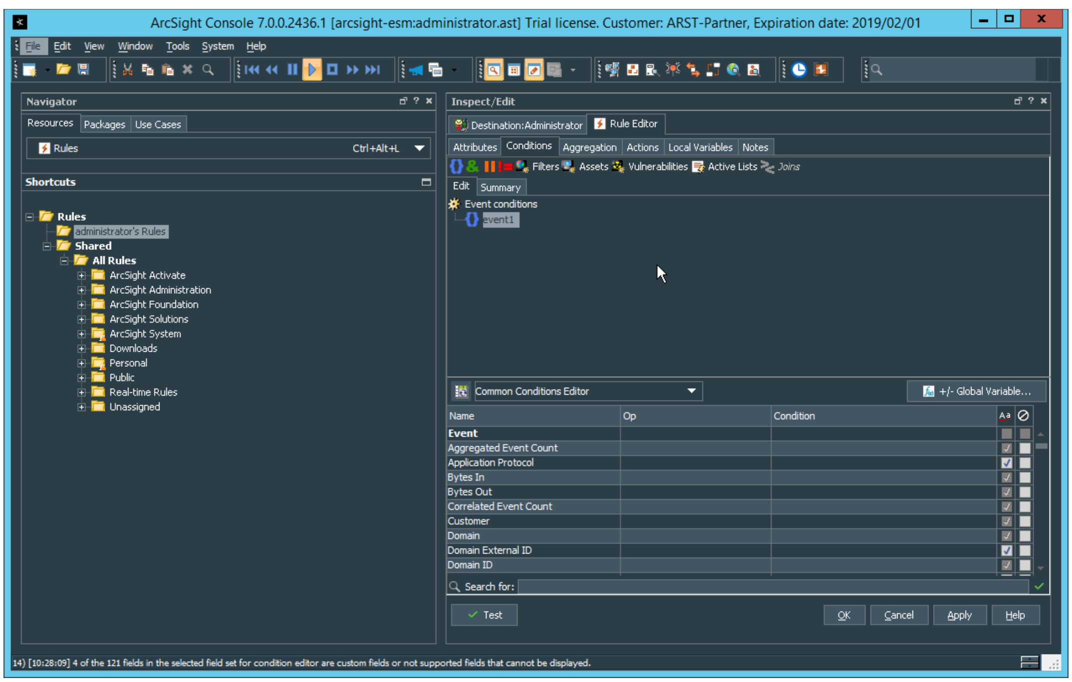
5. Click **OK.**
6. Select a place to save the new **Destination.**
7. Click **OK.**

2.8.7.2 *Configure a New Rule*

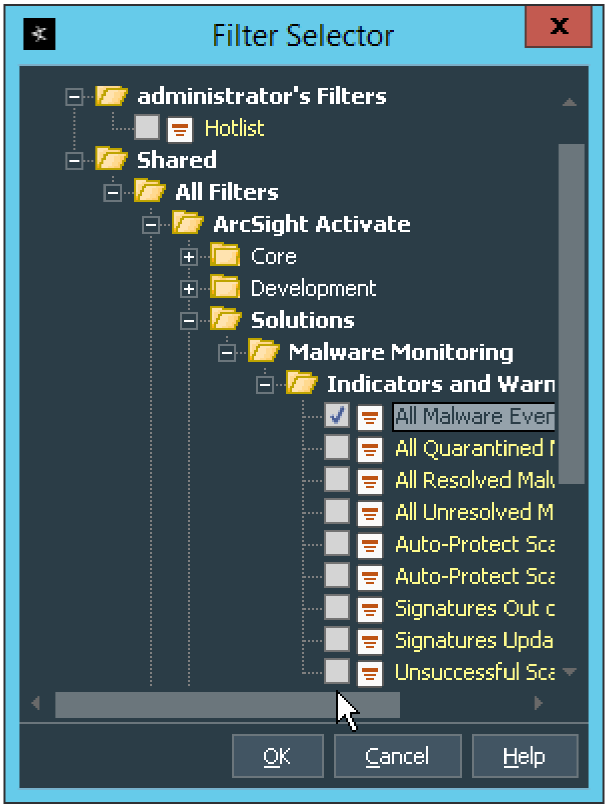
1. Click **File > New > Rule > Standard Rule.**
2. Enter a name for the rule.



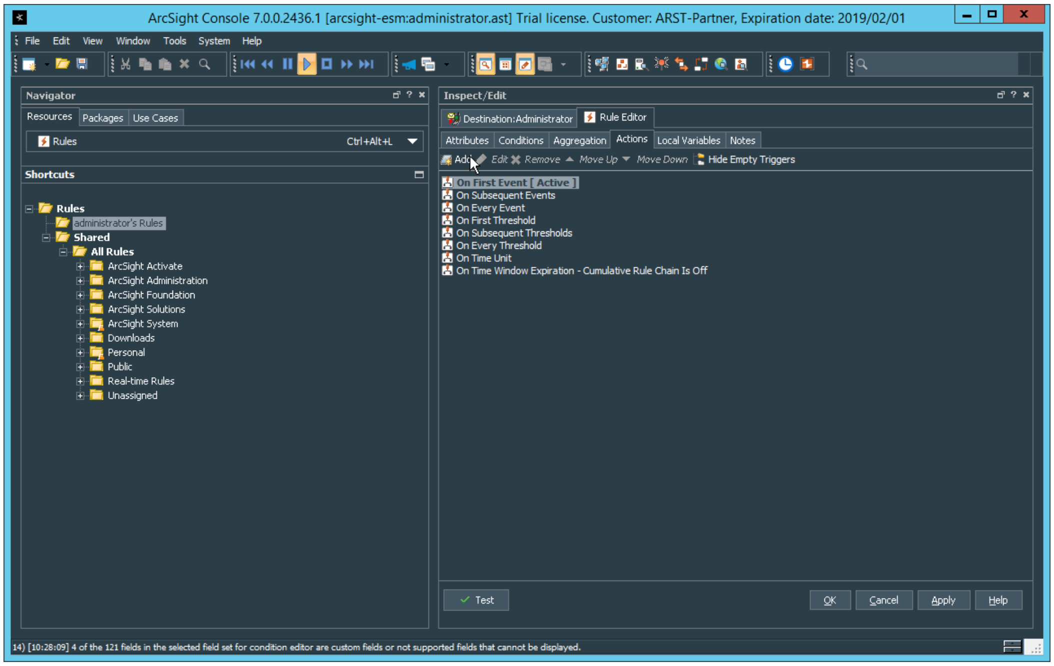
3. Click the **Conditions** tab.



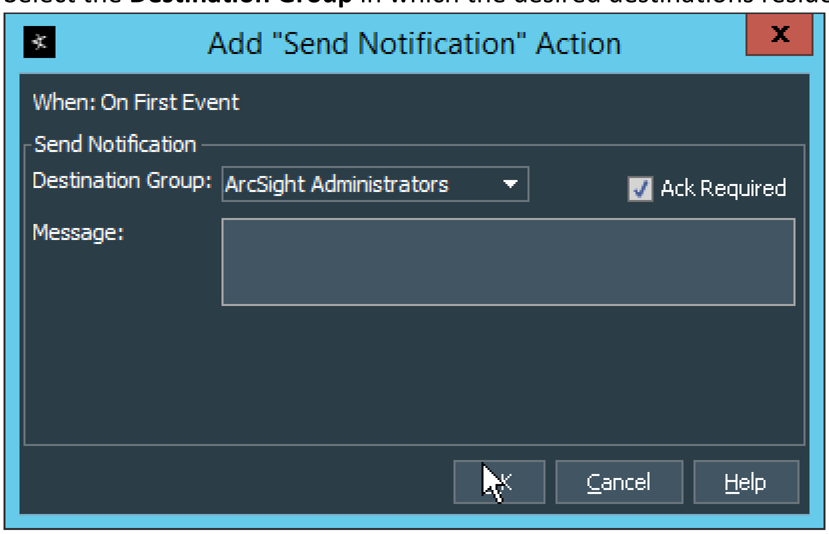
4. Either create a custom condition for the rule or click the **Filters** button to select a pre-configured Filter. (Ensure you check the box next to desired filters if you choose to select a pre-configured filter.)



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



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



9. Click **OK.**

2.9 Tripwire Enterprise

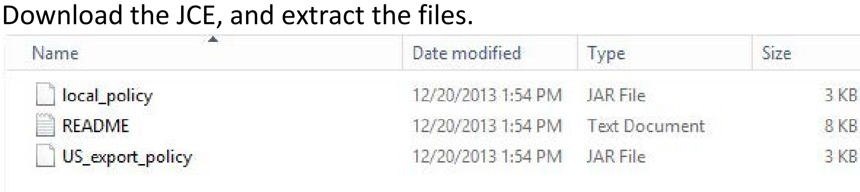
Notes:

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

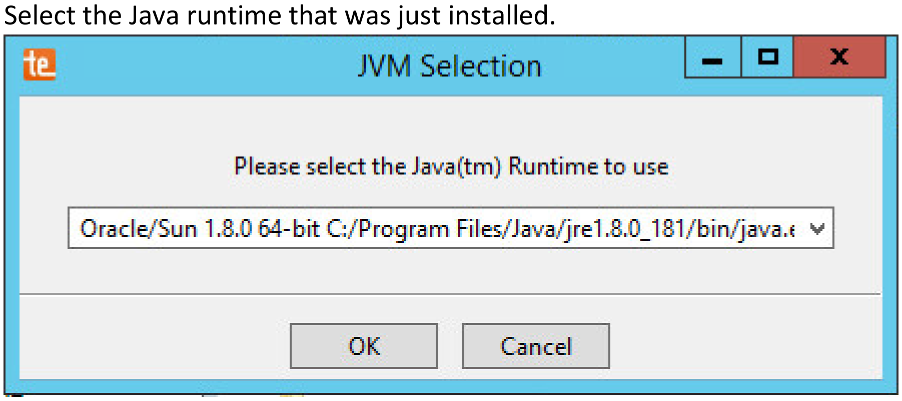
2.9.1 Install Tripwire Enterprise

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

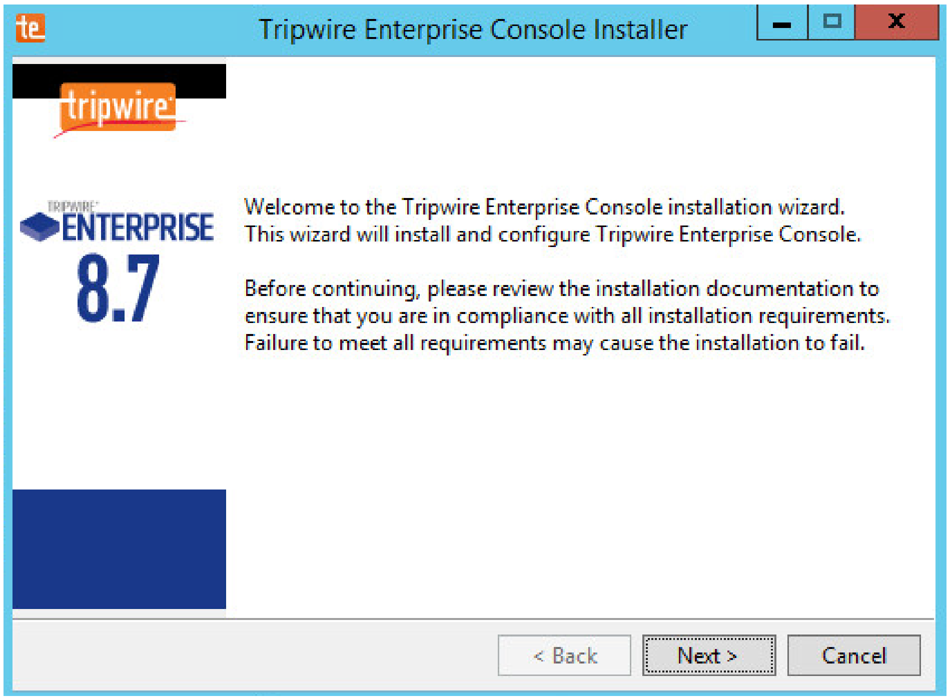
3. Click **Install.**
4. Download the JCE, and extract the files.



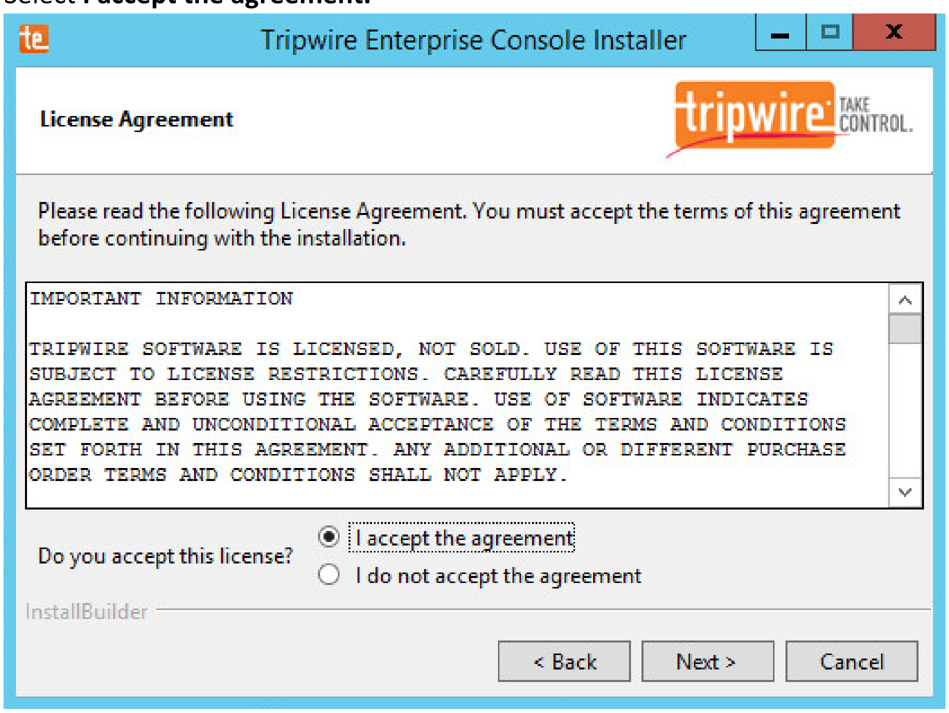
5. Copy the **local_policy.jar** and **US_export_policy.jar** files to */lib/security/Unlimited/* and */lib/security/Limited* in the Java installation directory.
6. Run **install-server-windows-amd64.**
7. Select the Java runtime that was just installed.



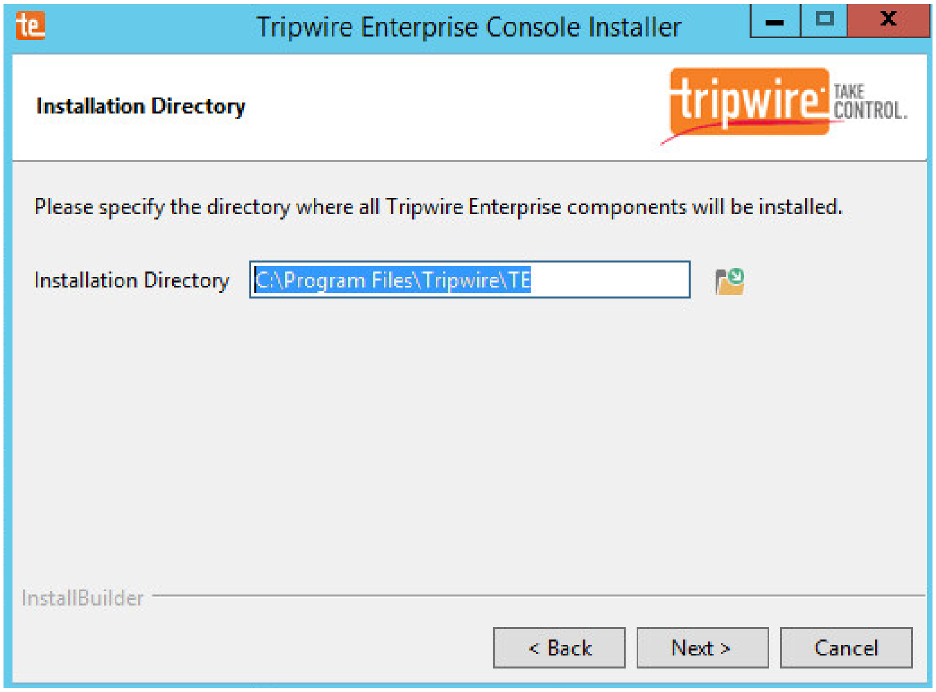
8. Click **OK.**



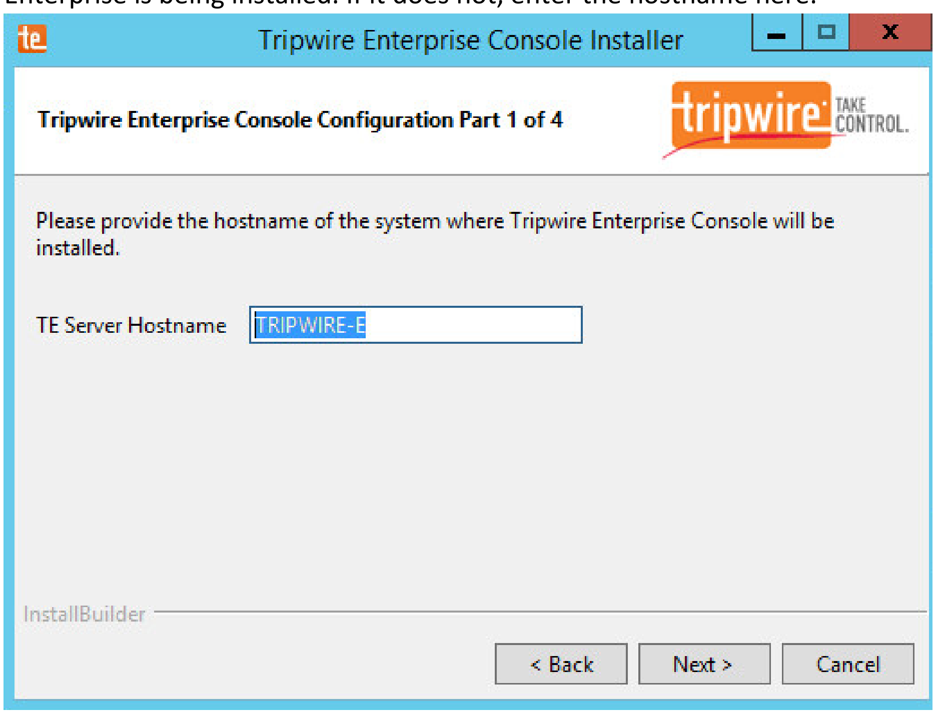
9. Click **Next.**
10. Select **I accept the agreement.**



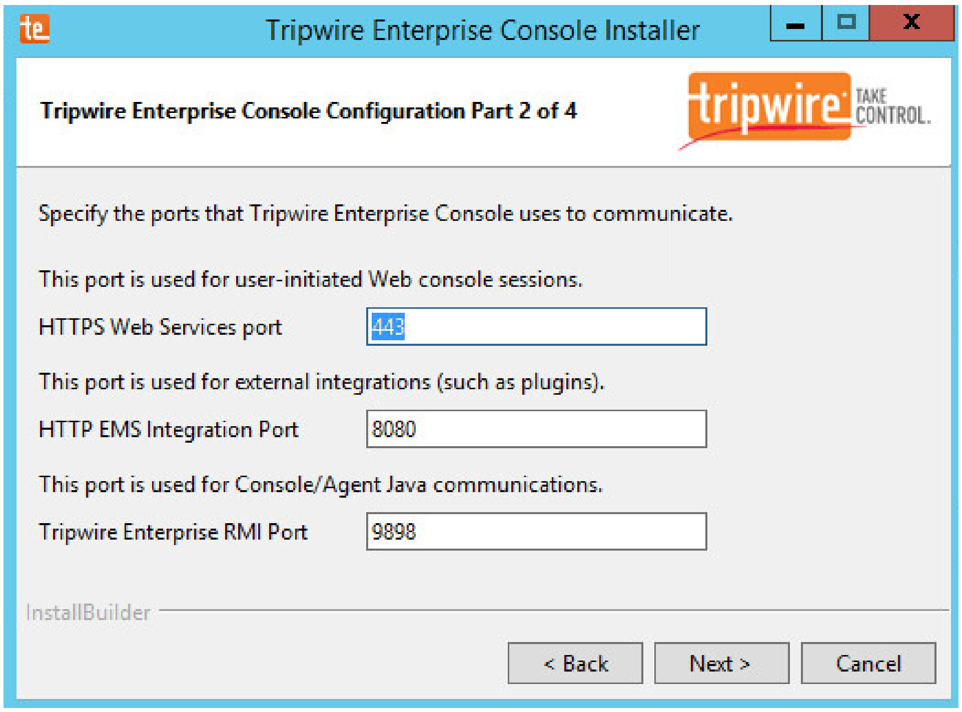
11. Click **Next.**



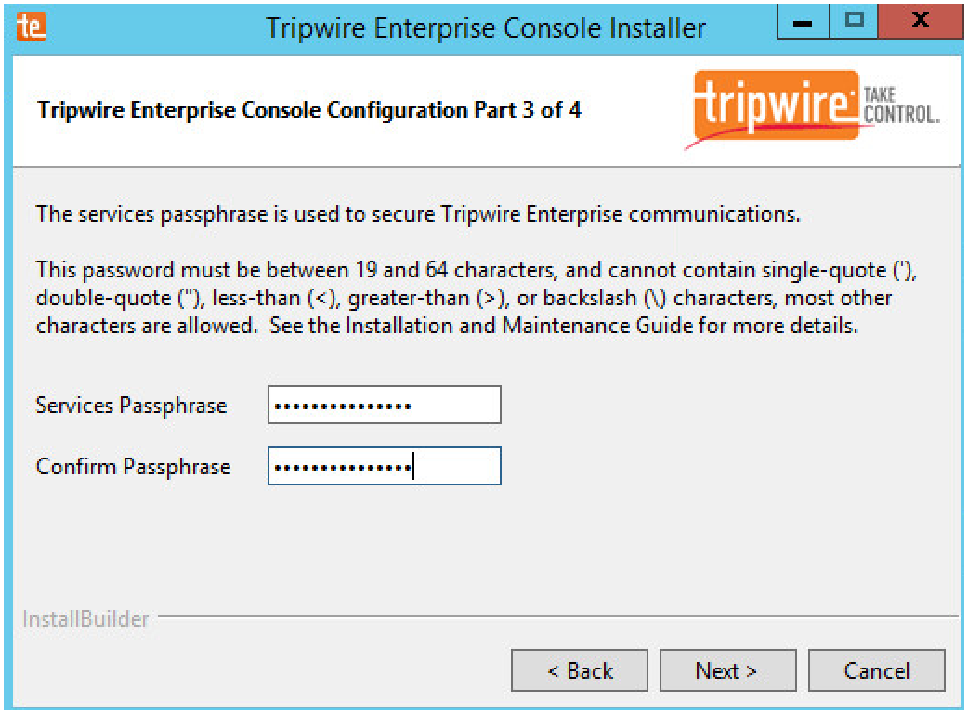
12. Click **Next.**
13. The installer should automatically detect the hostname of the system on which Tripwire Enterprise is being installed. If it does not, enter the hostname here.



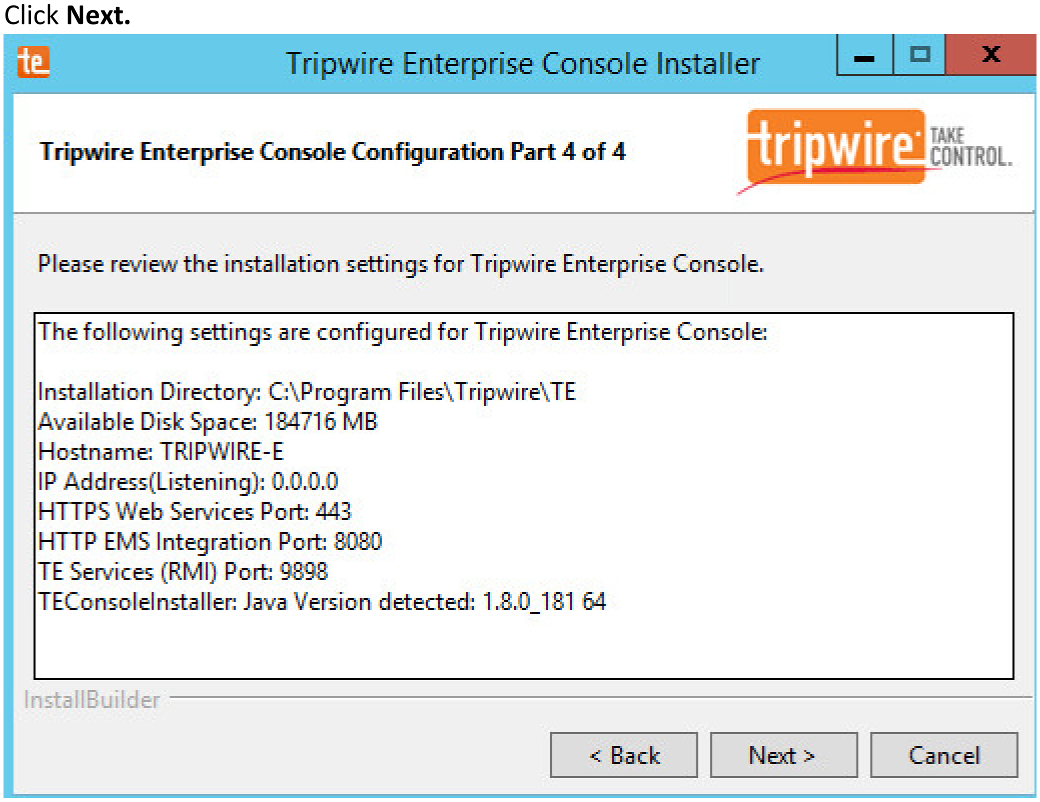
14. Click **Next.**
15. Enter the port numbers to use for each of the **HTTPS Web Services port, HTTP EMS Integration Port,** and **Tripwire Enterprise RMI port.** The RMI port is used for inbound communication from Tripwire agents to the server, so ensure that it is allowed through the firewall.



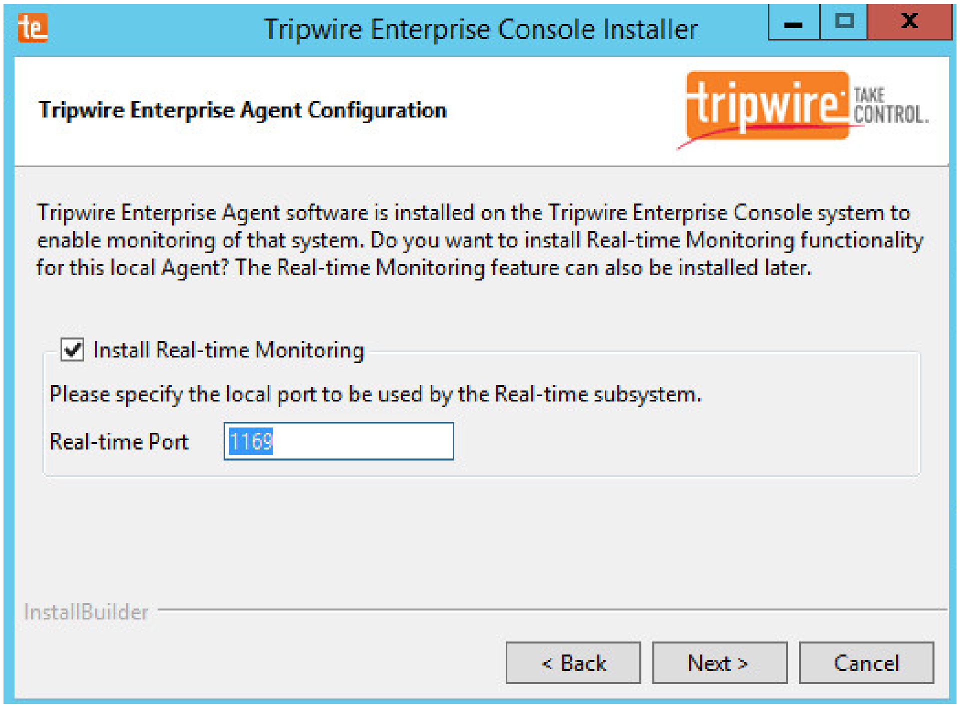
16. Click **Next.**
17. Enter a passphrase to use.



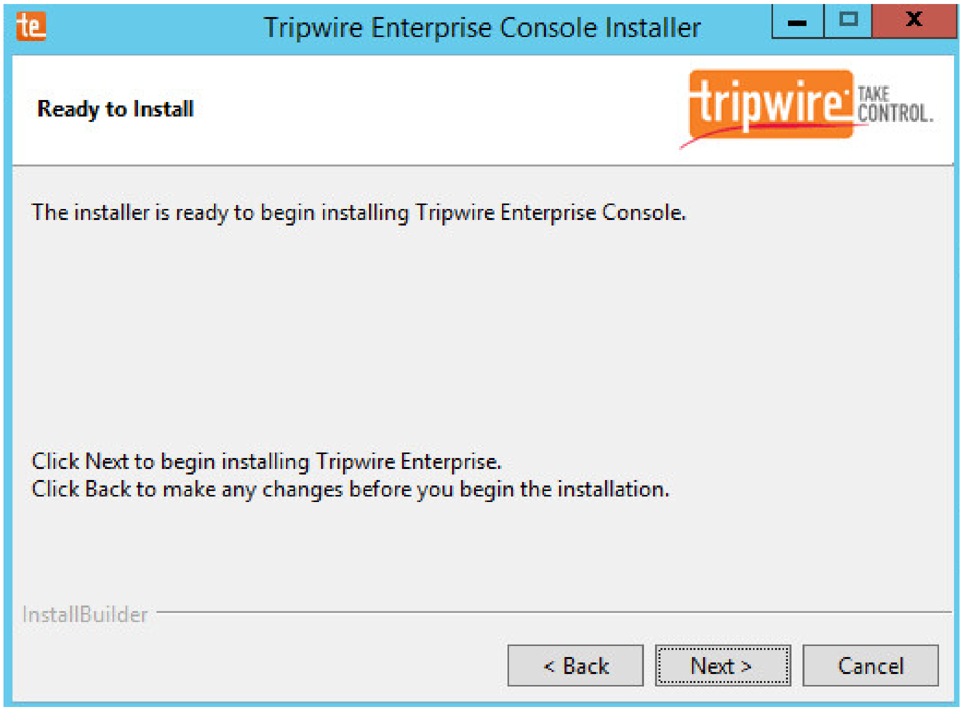
18. Click **Next.**



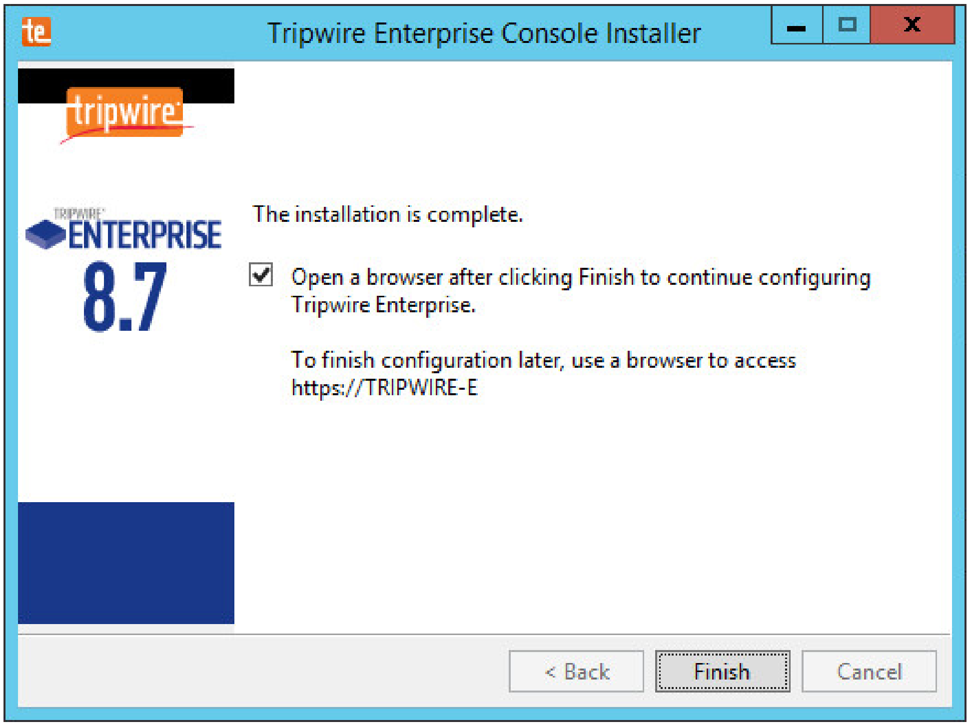
19. Click **Next.**
20. Check the box next to **Install Real-time Monitoring.**
21. Enter **1169** for **Real-time Port.**



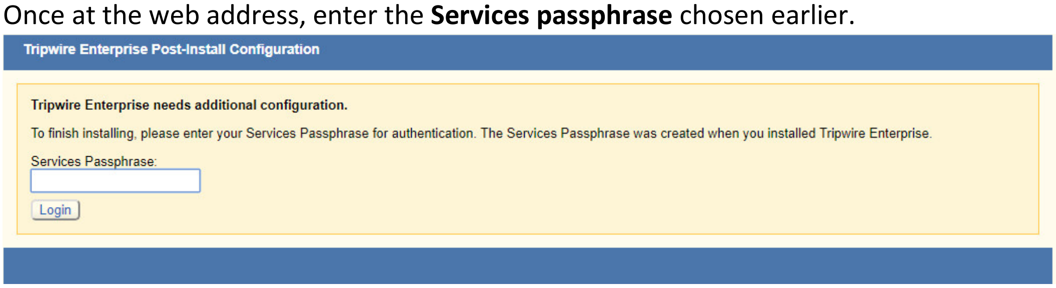
22. Click **Next.**



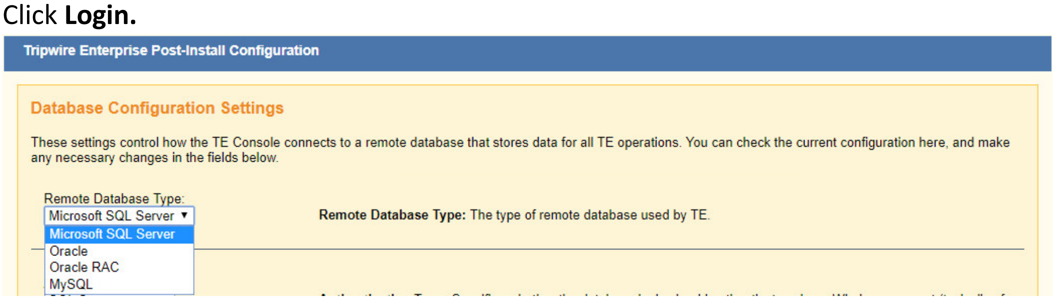
23. Click **Next.**
24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise.**



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

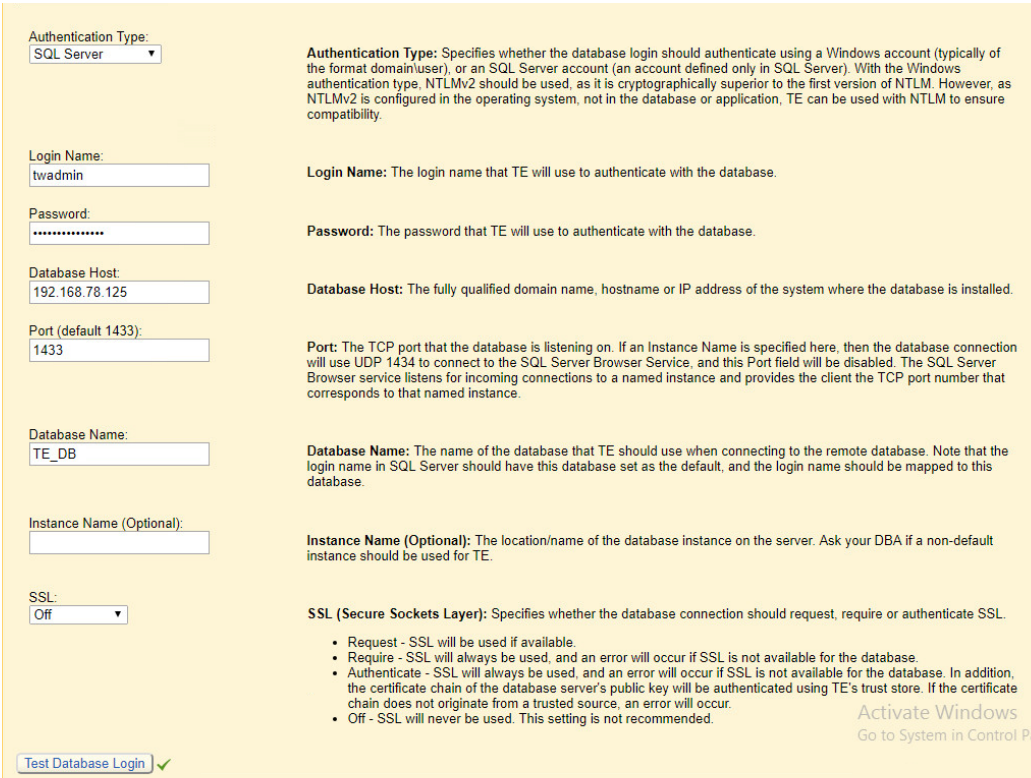


27. Click **Login.**

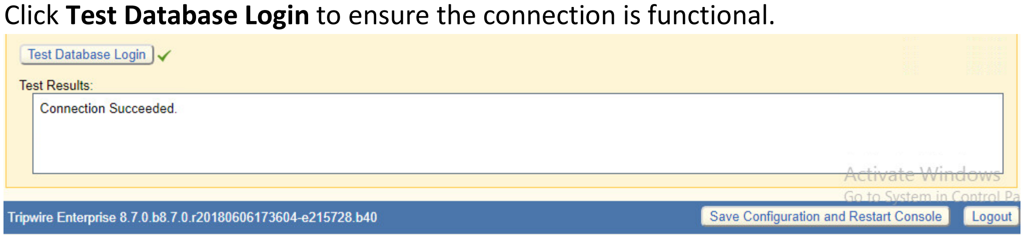


28. Select **Microsoft SQL Server** for **Remote Database Type.**
29. Select **SQL Server** for **Authentication Type.**
30. Enter login details for the account created during the MSSQL setup.
31. Enter the **hostname** or **IP** of the database server.

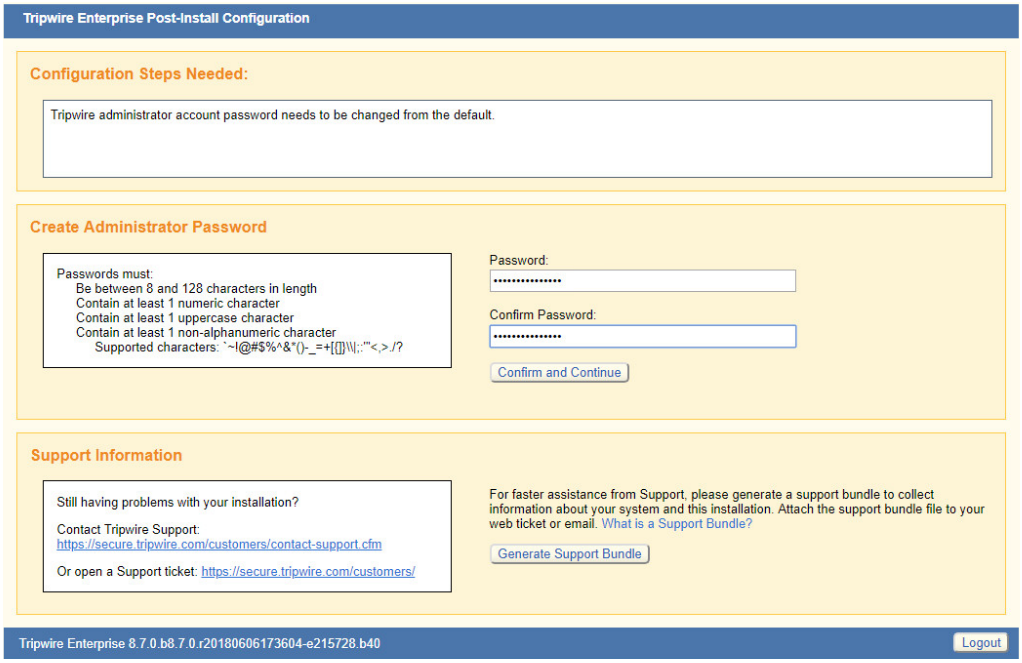
32. Enter the **port** on which the database is operating.
33. Enter the **name** of the database to be used for Tripwire Enterprise.
34. Select the appropriate setting for **SSL** according to your organization's needs.



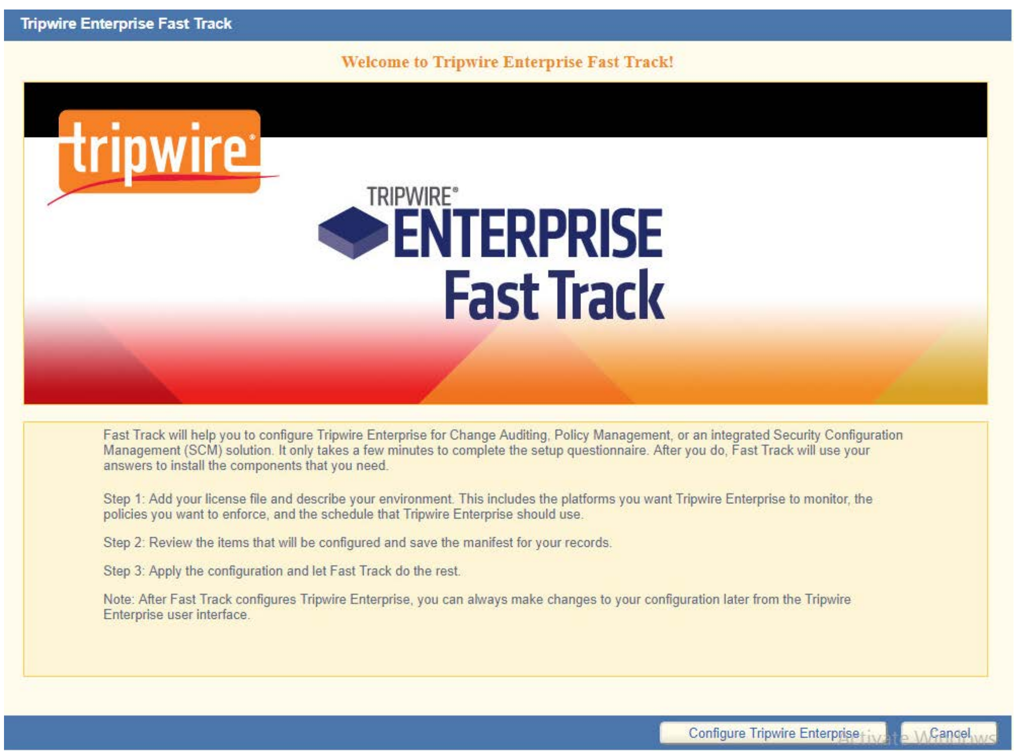
35. Click **Test Database Login** to ensure the connection is functional.



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



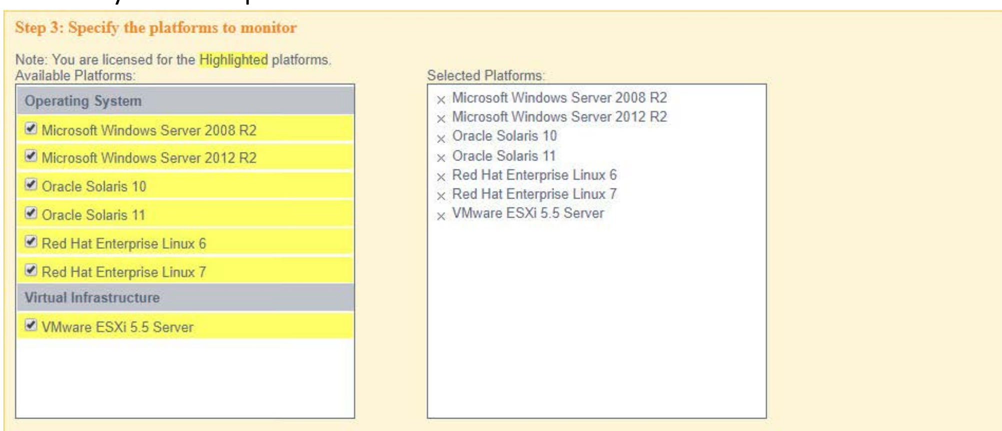
38. Click **Confirm and Continue.**



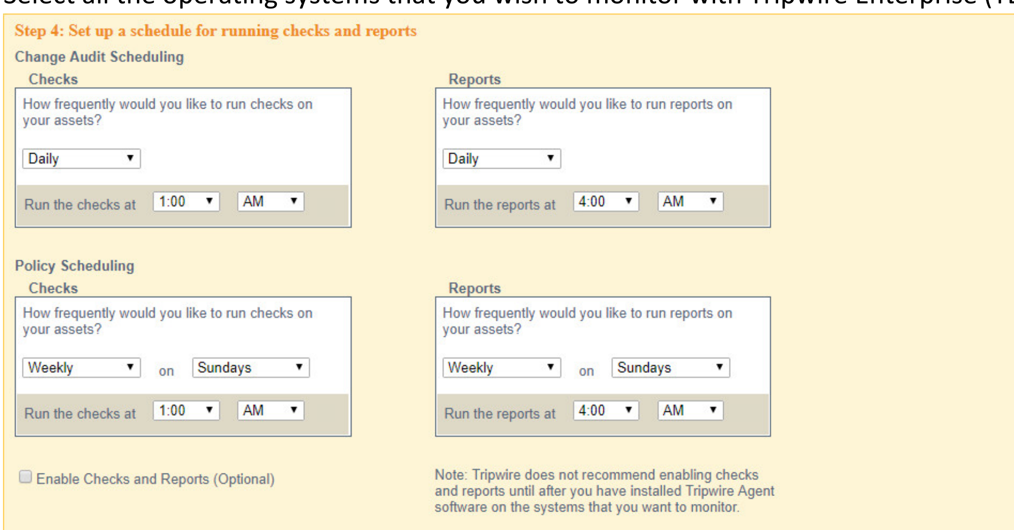
39. Click **Configure Tripwire Enterprise.**

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

42. Select any available policies desired.



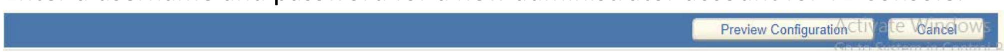
43. Select all the operating systems that you wish to monitor with Tripwire Enterprise (TE).



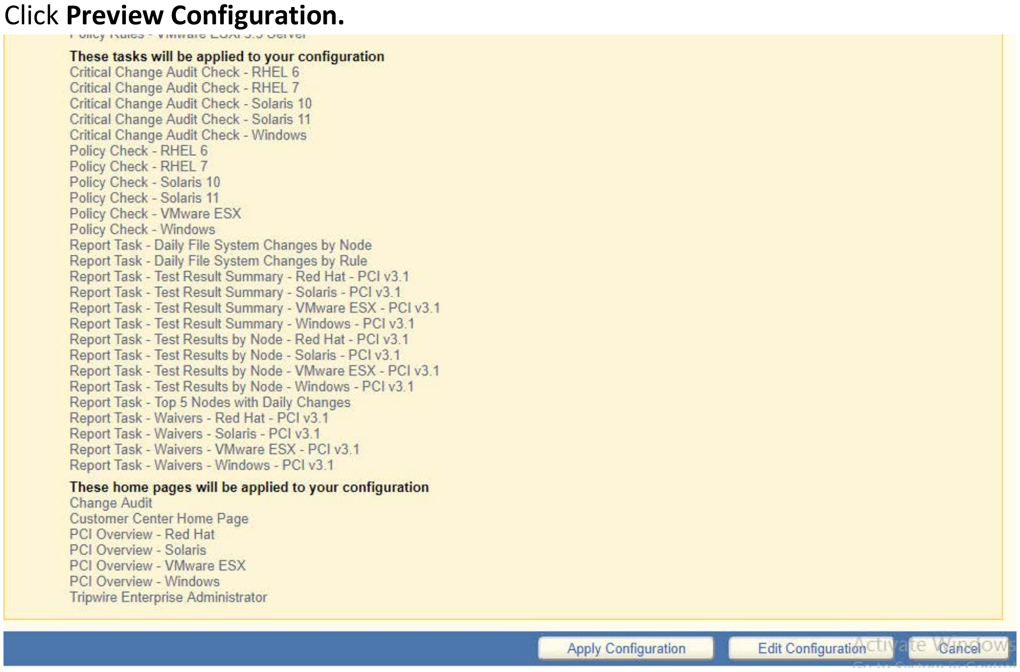
44. Set up a schedule for running checks and reports according to your organization's needs. Leave the box next to **Enable Checks and Reports** unchecked for now.

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

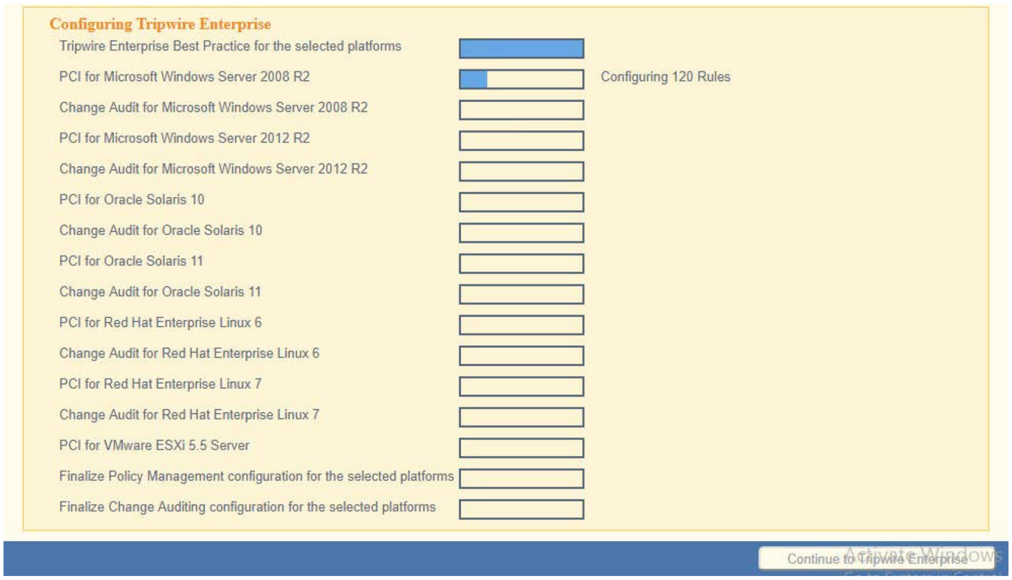
46. Enter a username and password for a new administrator account for TE Console.



47. Click **Preview Configuration.**



48. Click **Apply Configuration.**



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

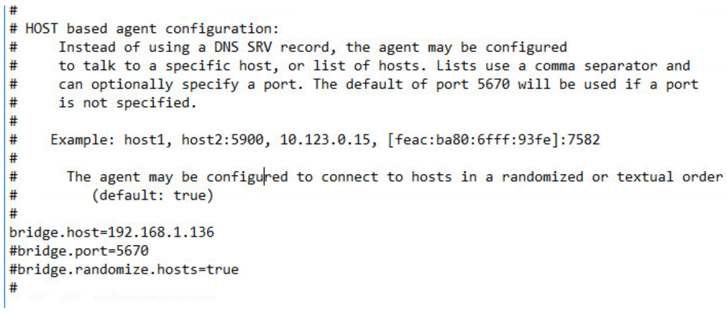
2.9.2 Install the Axon Bridge

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

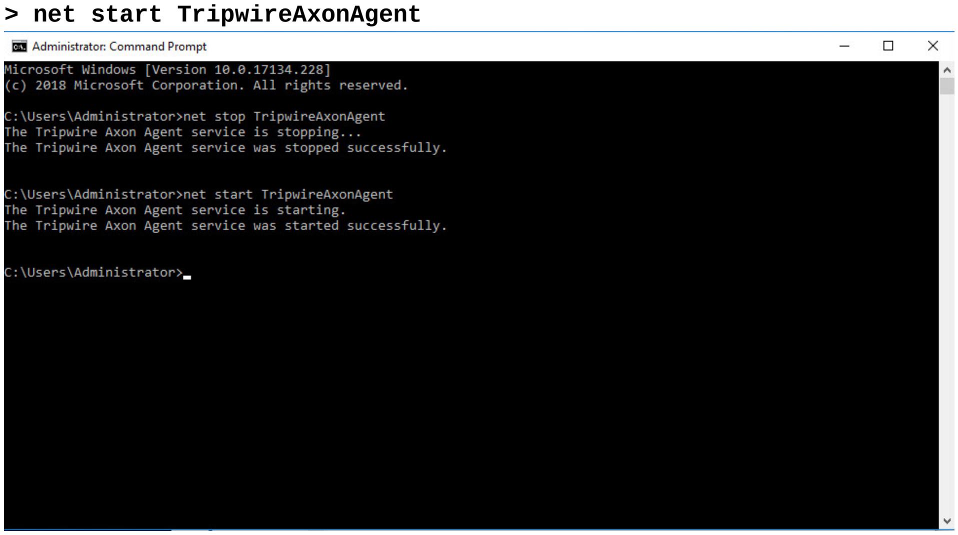
```
> <te_root>/server/bin/twserver restart
```

2.9.3 Install the Axon Agent (Windows)

1. Download the *Axon Agent .zip* file from the Tripwire customer website (https://tripwireinc.force.com/customers), under the **Product Downloads** tab.
2. Unzip the file.
3. To begin the installation, double-click the *.msi* file in the extracted folder. Note: No installation wizard will appear; the installation happens automatically.
4. After the Axon Agent is installed, navigate to *C:\ProgramData\Tripwire\agent\config,* and copy *twagent_sample.conf* to *twagent.conf.*



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



2.9.4 Install the Axon Agent (Linux)

1. Download the Axon Agent *.tgz* file from the Tripwire customer website (https://tripwireinc.force.com/customers), under the **Product Downloads** tab.
2. To install the software, run the following commands:
   RHEL or CentOS: **> rpm -ivh <installer_file>**
   Debian or Ubuntu: **> dpkg -i <installer_file>**
3. Navigate to */etc/tripwire/* and copy *twagent_sample.conf* to *twagent.conf.*
4. Open *twagent.conf,* and find the line that says `bridge.host`. Remove the **#** character, and enter the hostname or IP address of the Axon Bridge server.

5. In a file called *registration_pre_shared_key.txt,* enter the value of the pre-shared key that was set in the Axon Bridge.
6. Restart the Axon Agent Service by opening a command prompt and running the following commands:

   RHEL or CentOS:
   ```
   > /sbin/service tripwire-axon-agent stop
   > /sbin/service tripwire-axon-agent start
   ```

   Debian or Ubuntu:
   ```
   > /usr/sbin/service tripwire-axon-agent stop
   > /usr/sbin/service tripwire-axon-agent start
   ```

2.9.5 Configure Tripwire Enterprise

2.9.5.1 *Terminology*

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

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

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

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

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

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

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

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

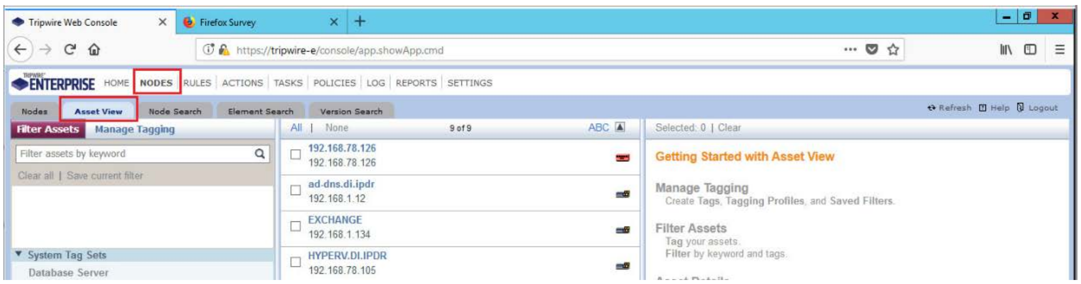
Baseline: The act of creating an element that reflects the current state of a monitored object (also called the **current baseline.** When a node's baseline is promoted, TE saves the former baseline as a **historic baseline.**

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

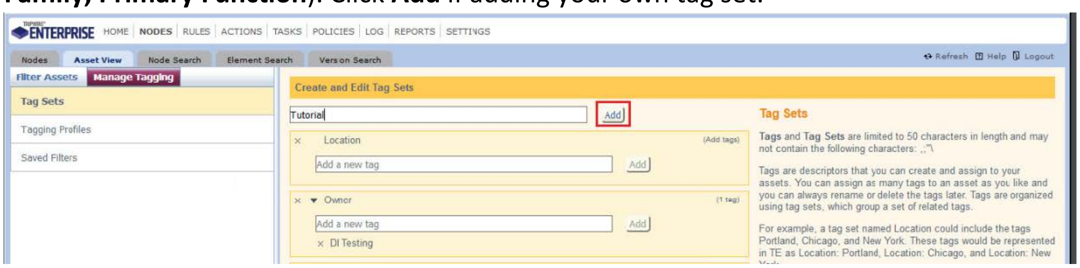
2.9.5.2 *Tags*

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

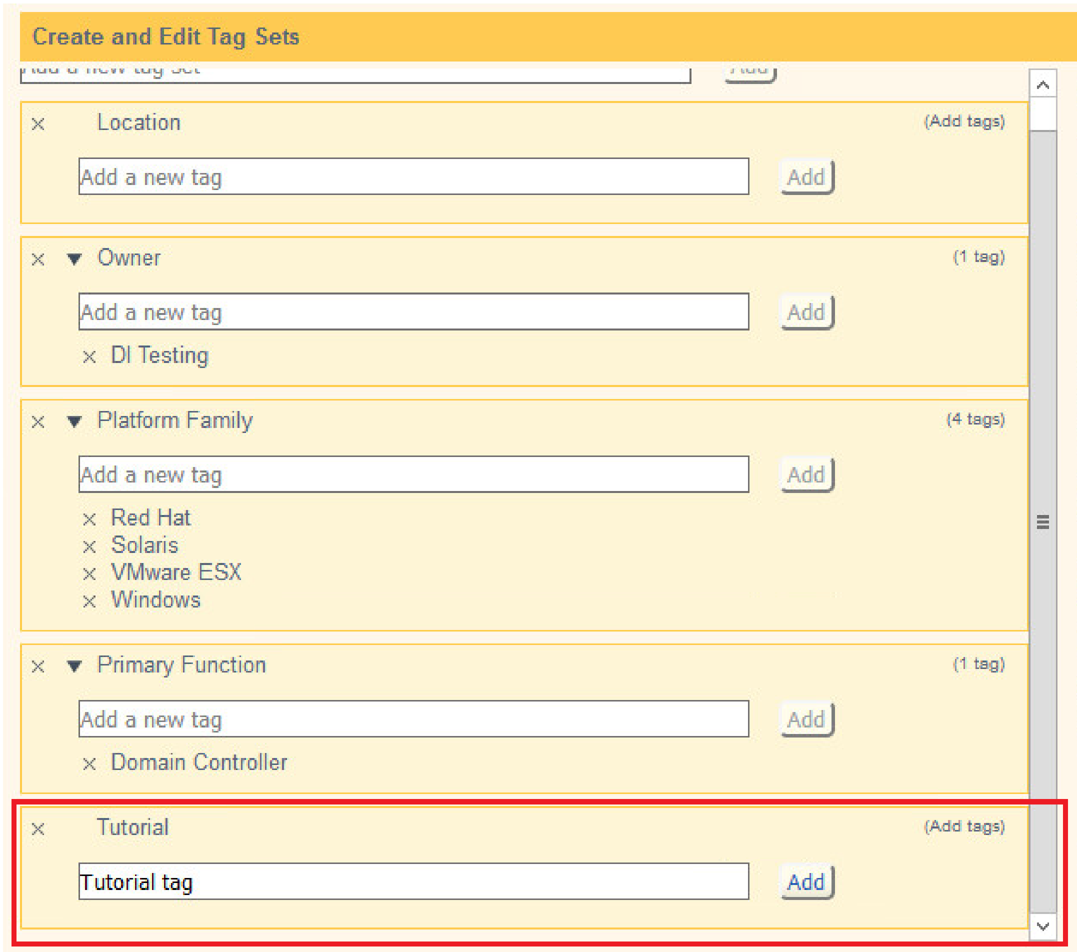
1. Navigate to the TE Console in your browser.
2. Click **Asset View.**



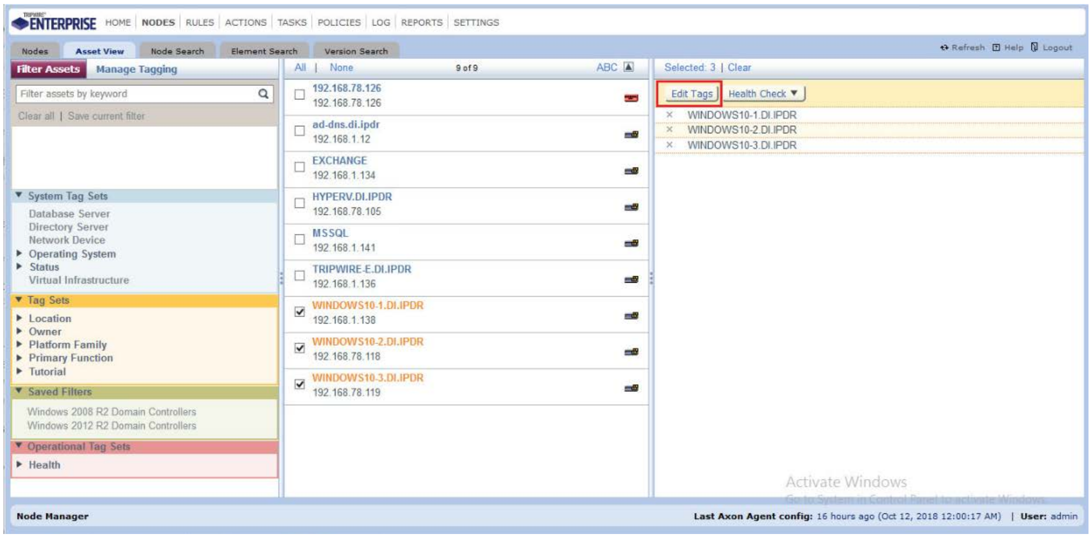
3. Click the **Manage Tagging** tab.
4. Enter the name of a tag set or use one of the four existing ones (**Location, Owner, Platform Family, Primary Function**). Click **Add** if adding your own tag set.



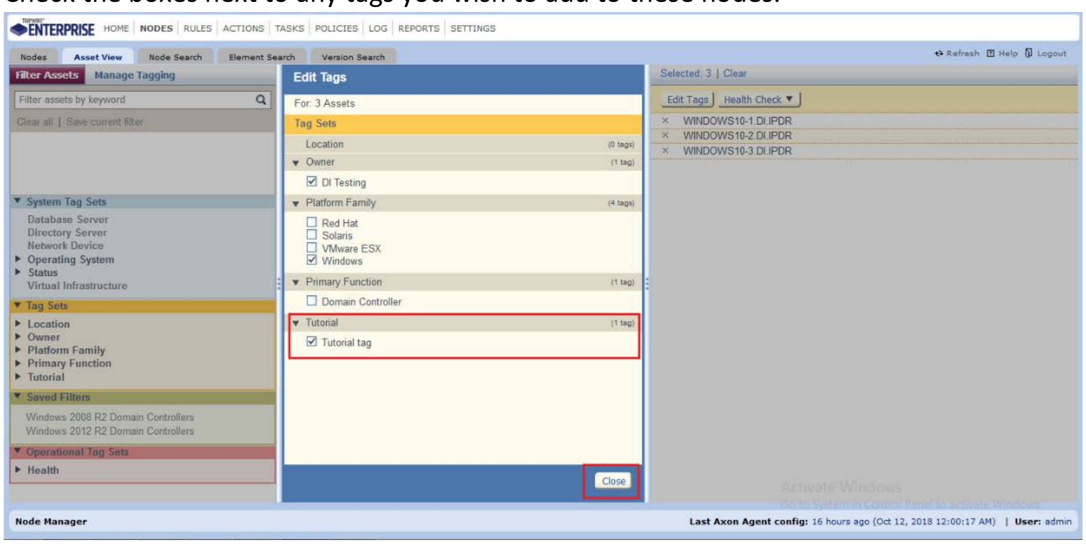
5. Under the tag set you wish to add a tag to, enter the name of the tag.



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



9. Click **Edit Tags.**
10. Check the boxes next to any tags you wish to add to these nodes.



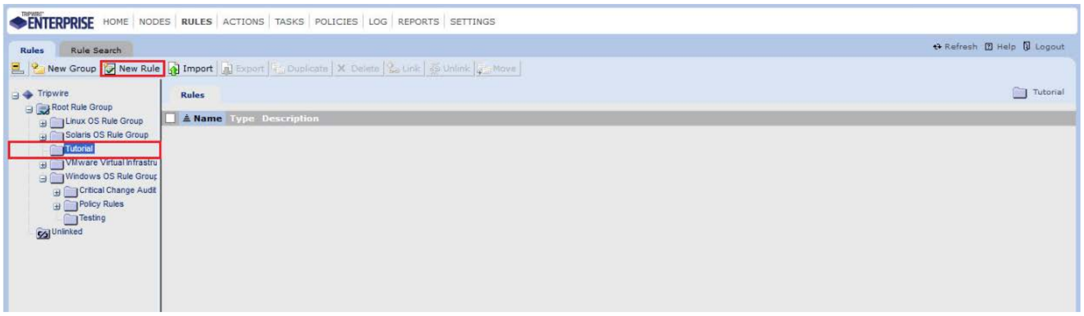
11. Click **Close.**

2.9.5.3 *Rules*

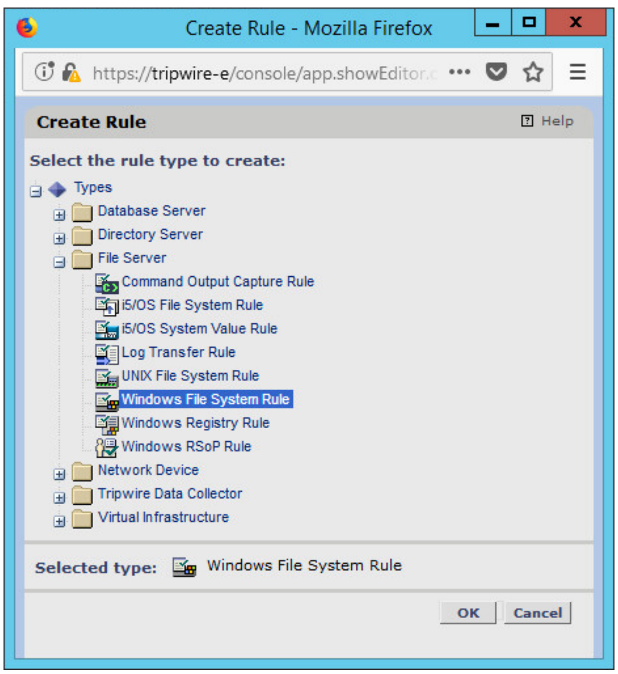
This section will describe how to create a rule.

1. Click **Rules.**

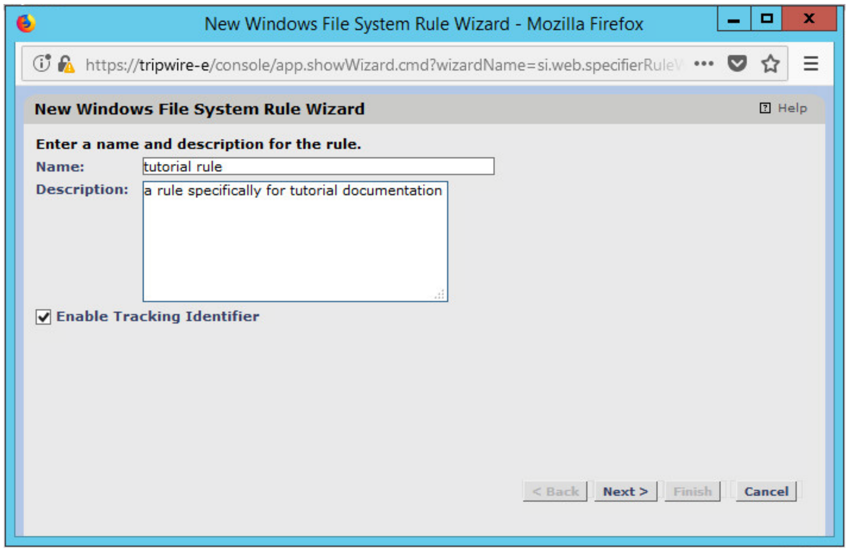
2. Select or create a rule group in which to put the new rule.



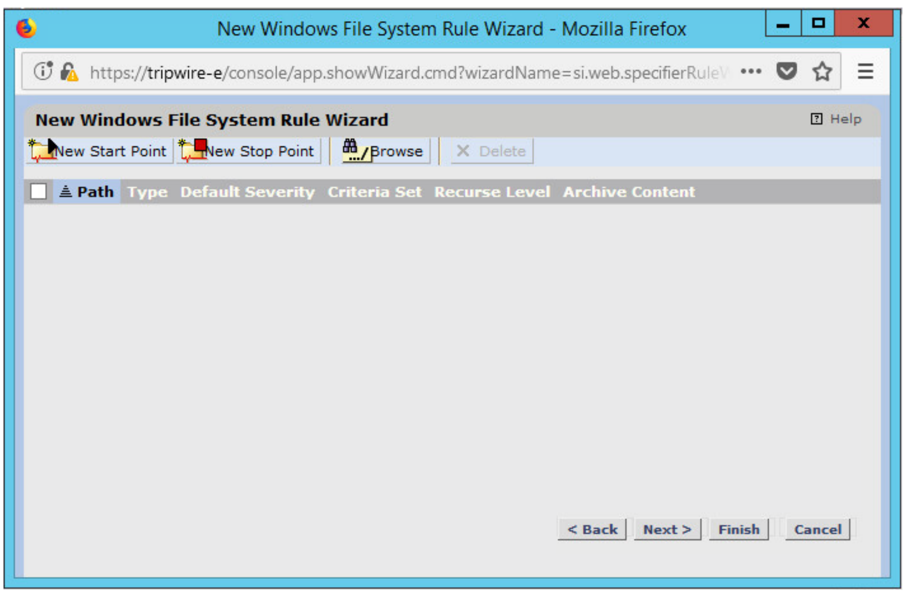
3. Click **New Rule.**
4. Select the type of rule. For monitoring Windows filesystems, we choose **Windows File System Rule.**



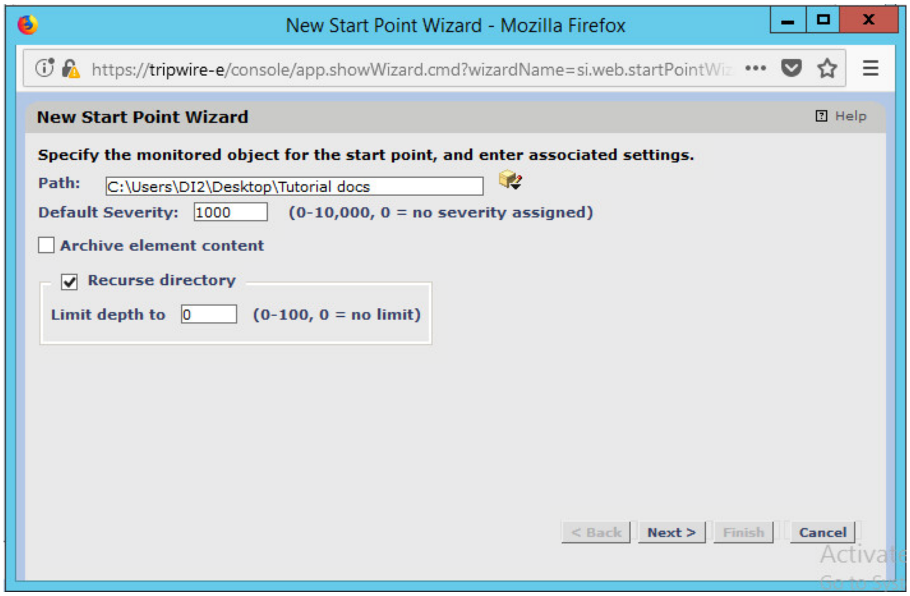
5. Click **OK.**
6. Enter a **name** and **description** for the rule.



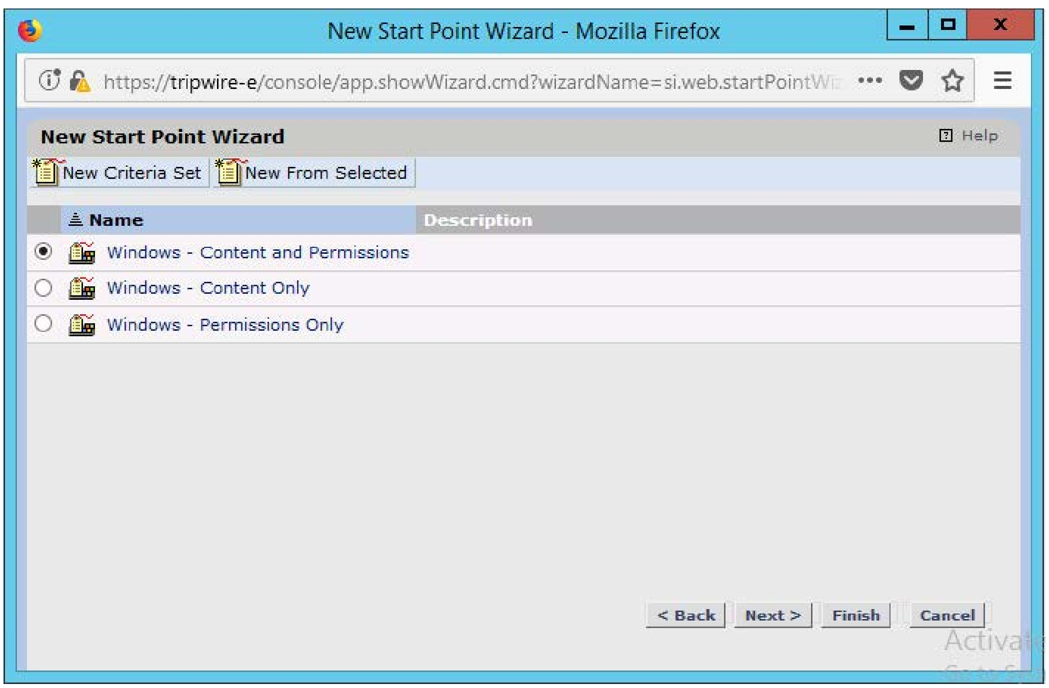
7. Click **Next.**



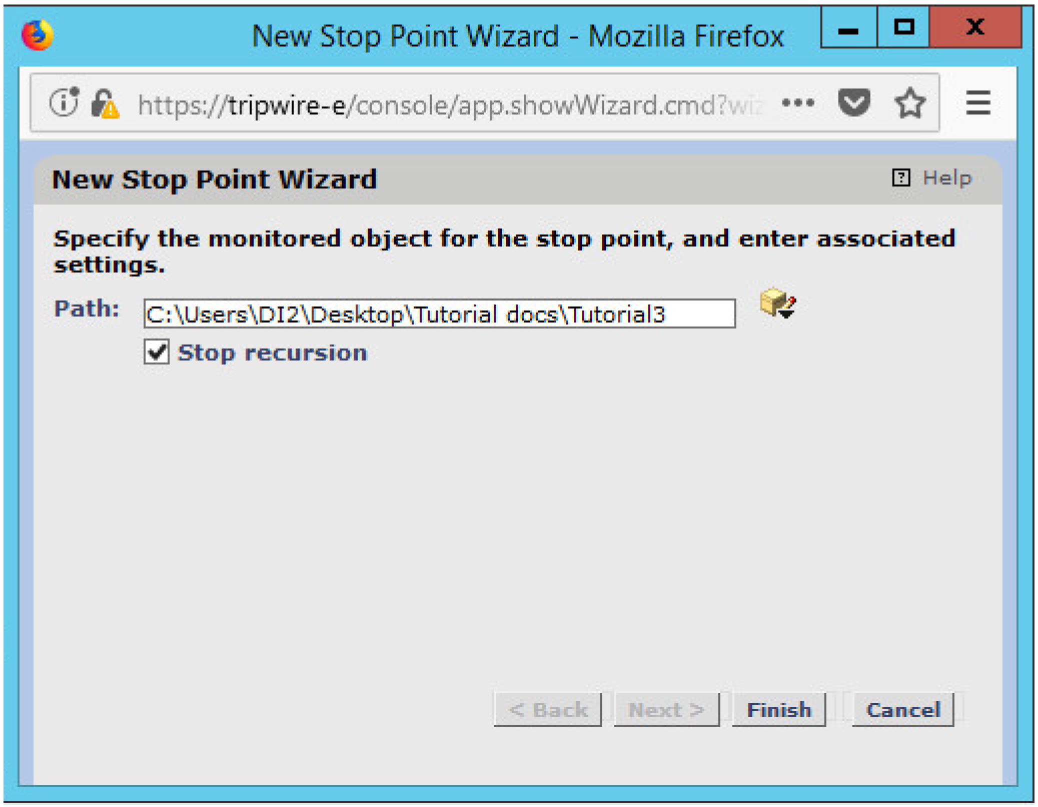
8. Click **New Start Point.**
9. For **Path**, enter a directory that represents the scope of the scan. It can be limited to the documents folder or be wide enough to encompass all the files on a system. Note that the latter will take much longer to scan.
10. Check the box next to **Recurse directory**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



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



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



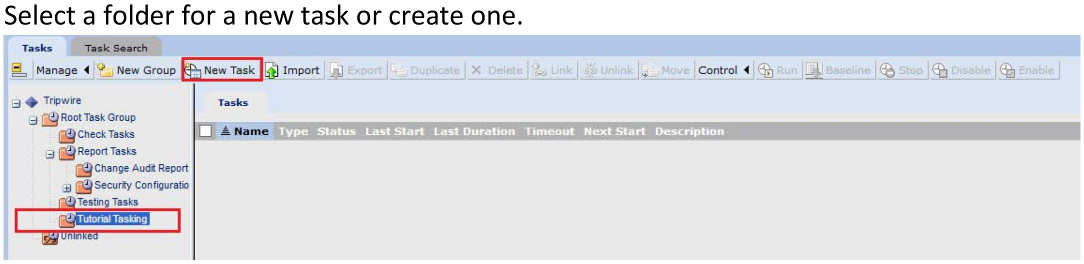
16. Click **Finish.**
17. Click **Next.**
18. Click **Next.**
19. Click **Finish.**

2.9.5.4 *Tasks*

This section will describe how to create a task.

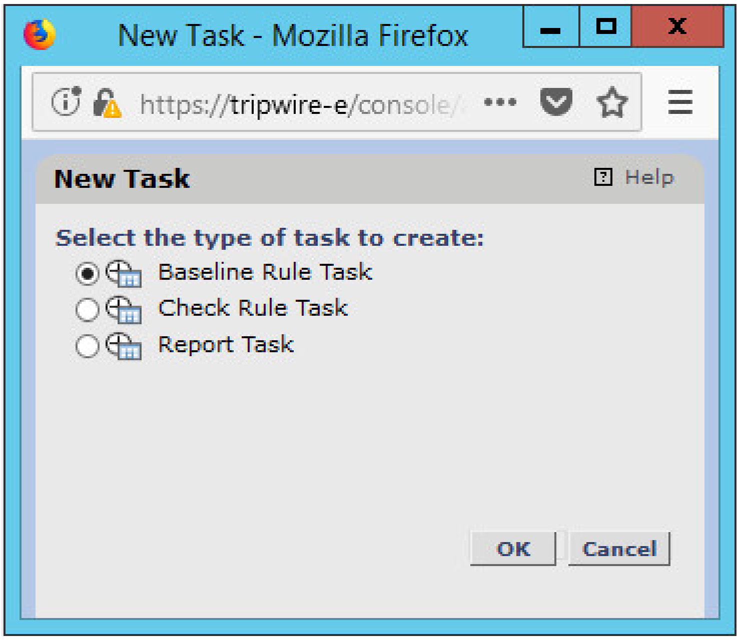
1. Click **Tasks.**

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

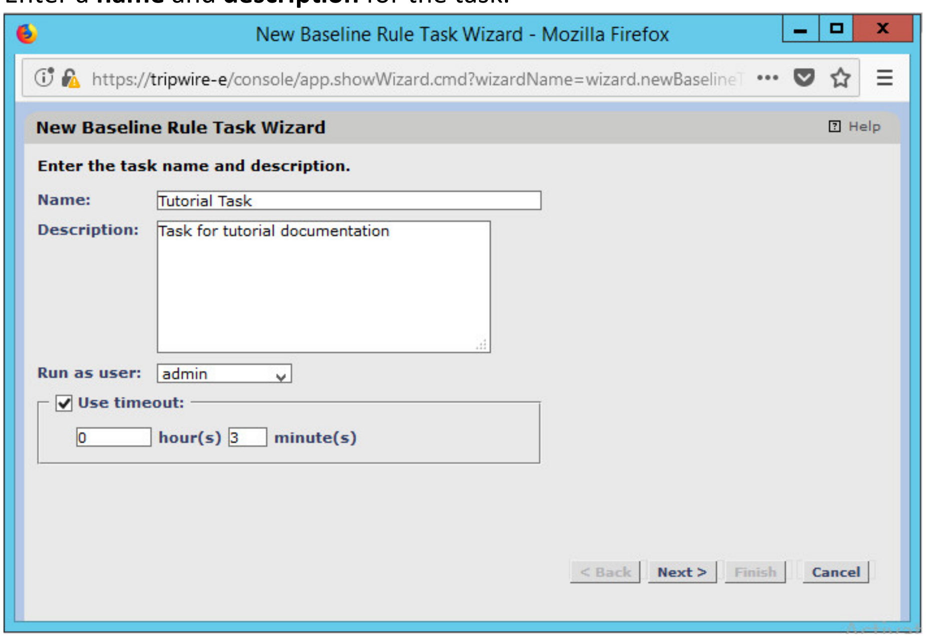


3. Click **New Task.**

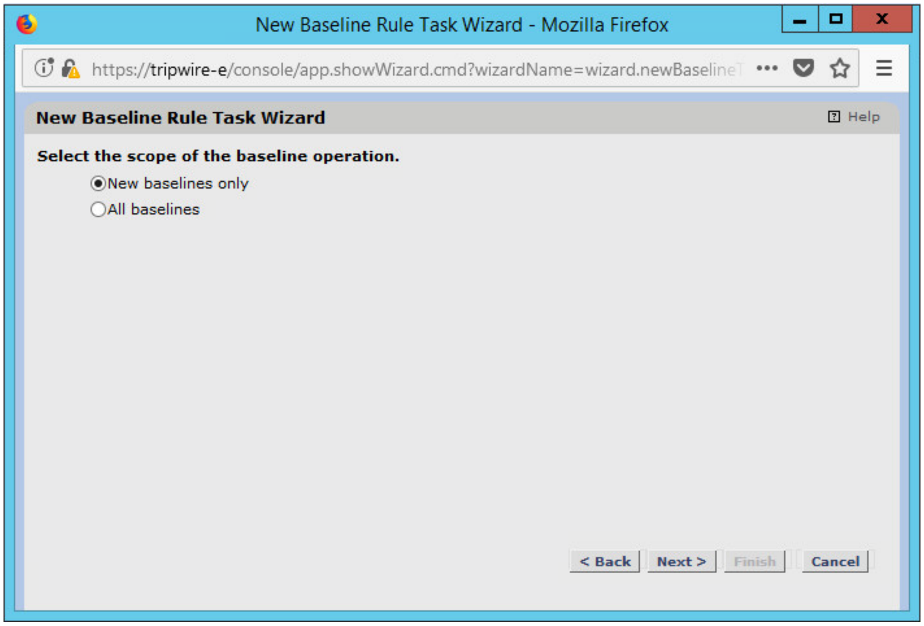
4. Select **Baseline Rule Task** or **Check Rule Task** (Note: Both are needed: baseline creates the initial state of the monitored object, and check updates the state and reports any changes).



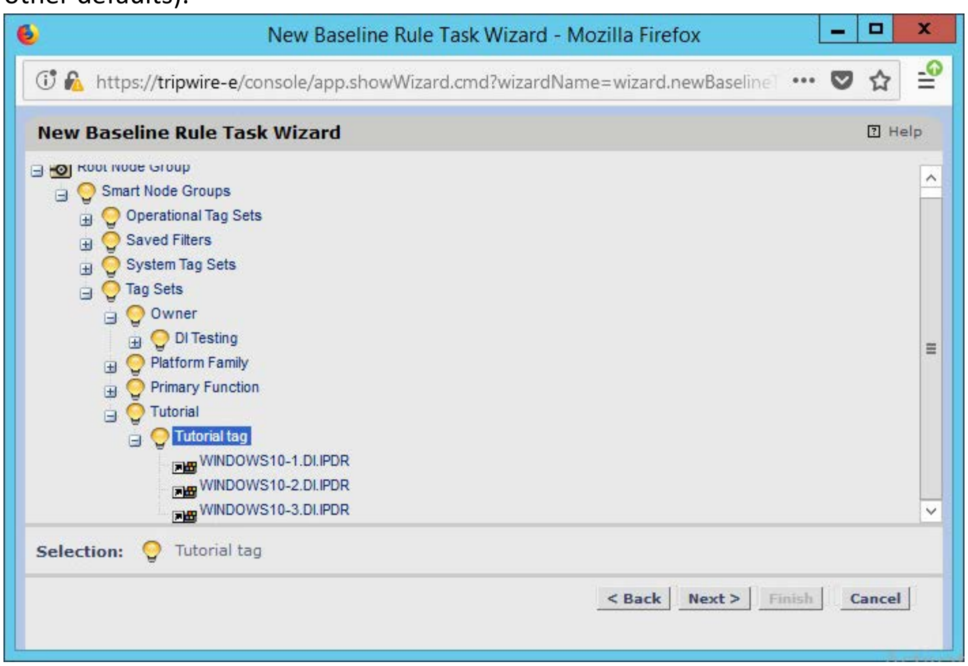
5. Click **OK.**
6. Enter a **name** and **description** for the task.



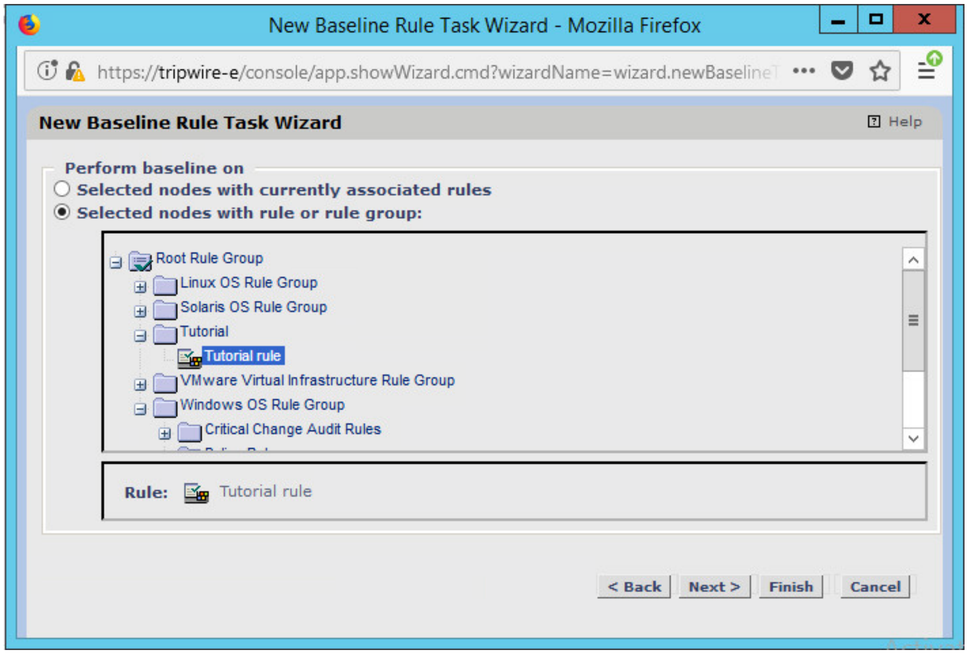
7. Click **Next.**
8. Select whether you want all baselines to be updated or to only create new baselines.



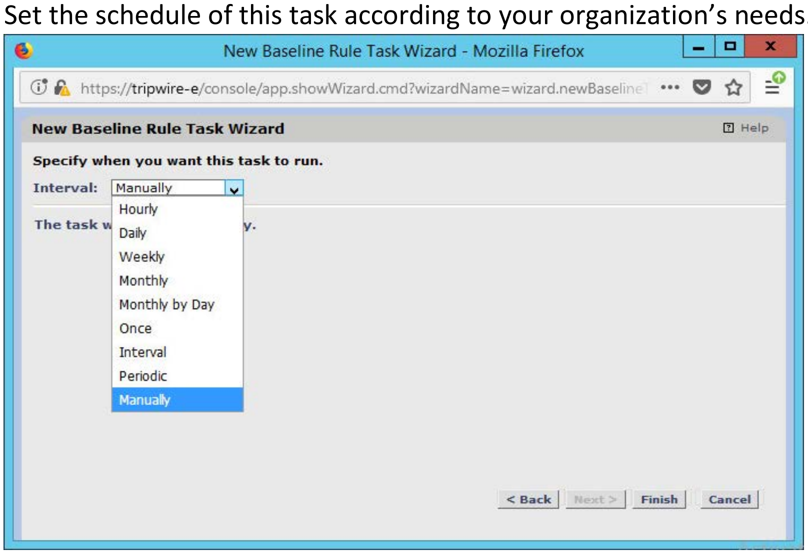
9. Click **Next.**
10. Select the systems to be included in the task. You can use tags or select by operating system (or other defaults).



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



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



15. Click **Finish.**

2.10 Tripwire Log Center

2.10.1 Install Tripwire Log Center Manager

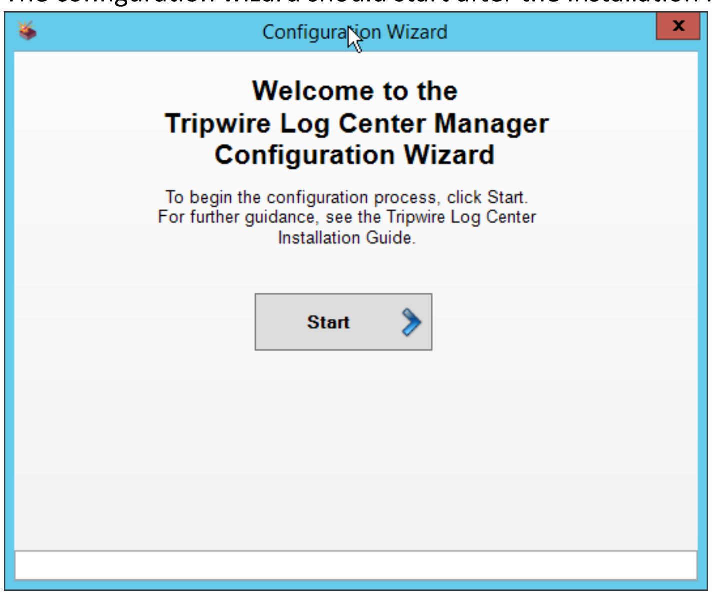
See the *Tripwire Log Center 7.3.1 Installation Guide* that should accompany the installation media for instructions on how to install **Tripwire Log Center.** Use the **Tripwire Log Center Manager** installer.

Notes:

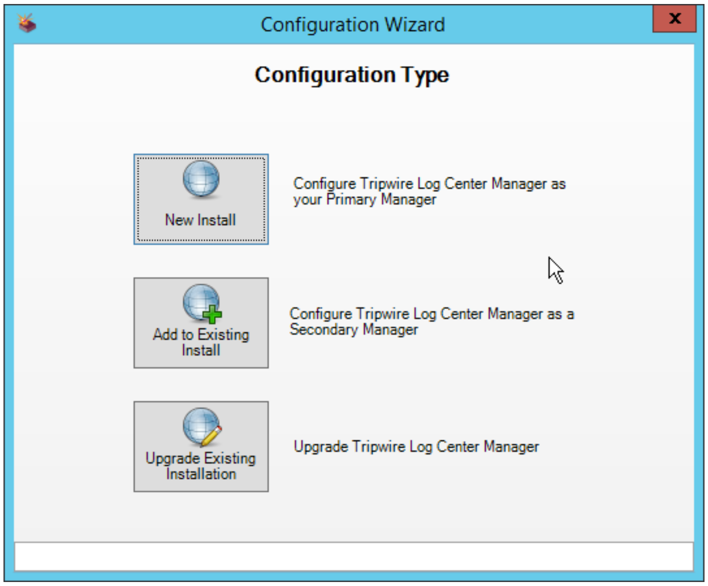
a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise.**
b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
c. .NET Framework 3.5 is required for this installation;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

2.10.2 Configure Tripwire Log Center Manager

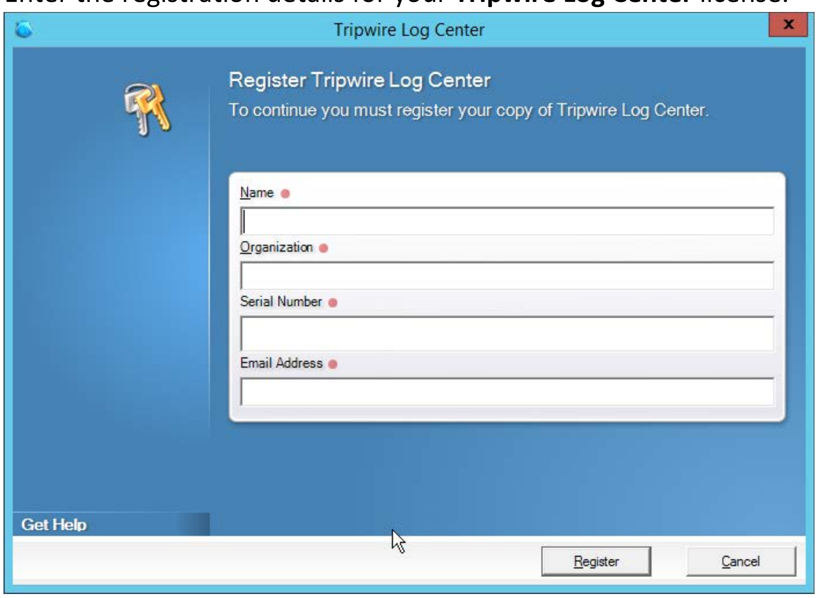
1. The configuration wizard should start after the installation is complete.



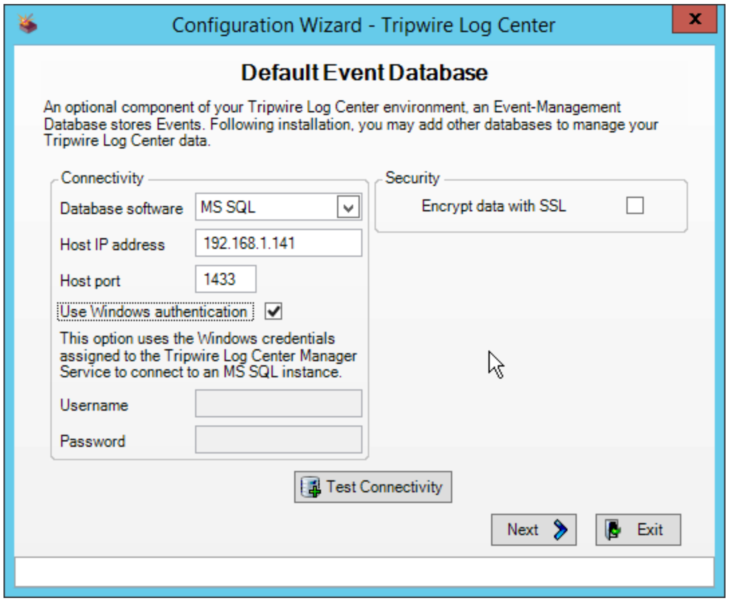
2. Click **Start.**



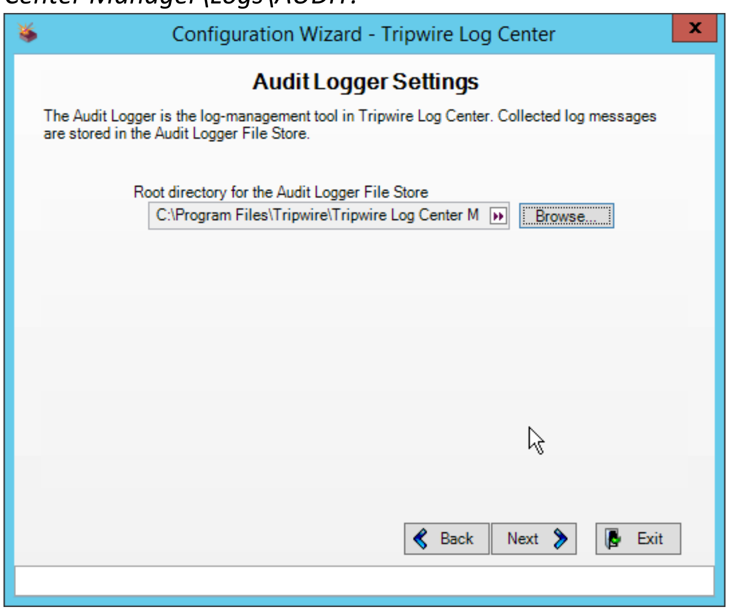
3. Click **New Install.**
4. Enter the registration details for your **Tripwire Log Center** license.



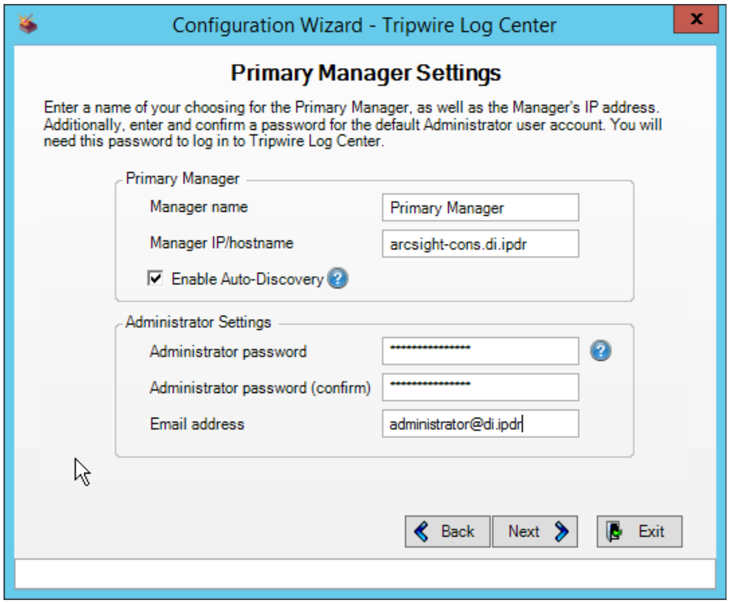
5. Click **Register.**
6. Enter details about the database that **Tripwire Log Center** should use.



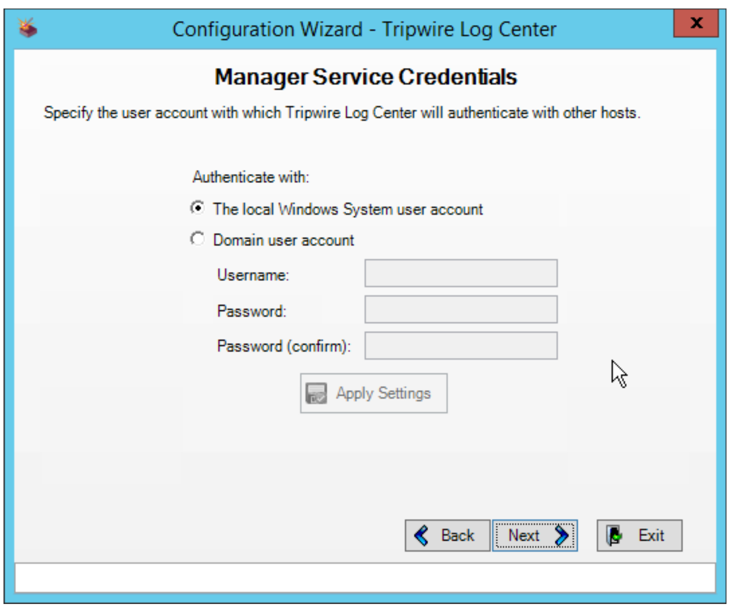
7. Click **Next.**
8. Select a directory to store log messages in, such as *C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT.*



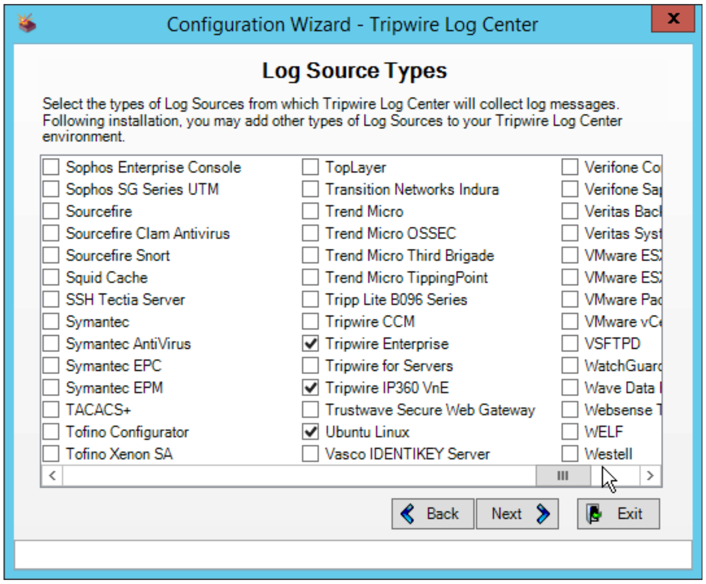
9. Click **Next.**
10. Enter a **password** and an **email**.
11. Change the IP to a hostname, if preferred.



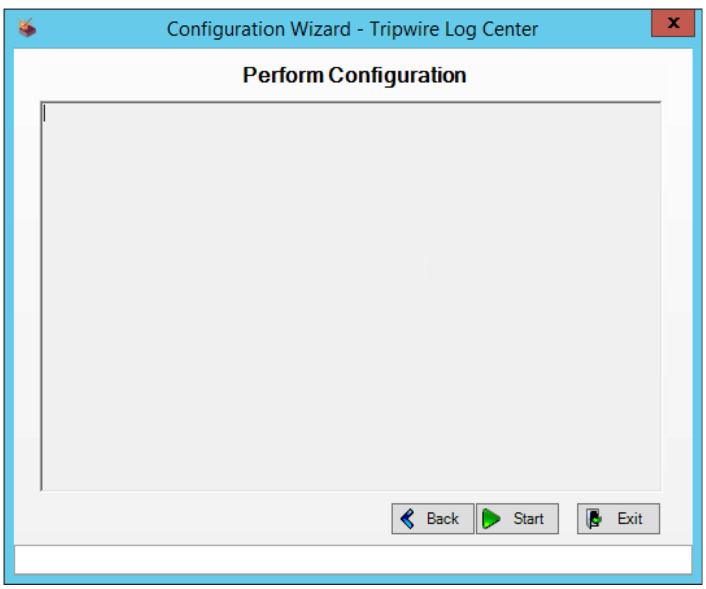
12. Click **Next.**



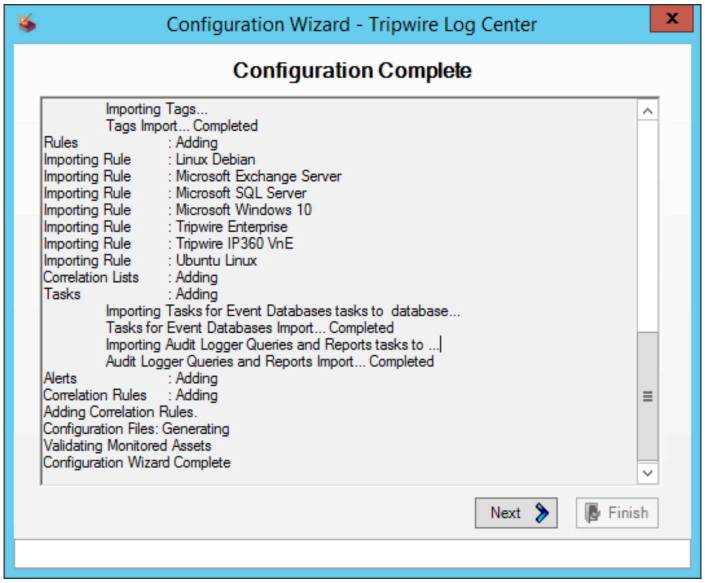
13. Click **Next.**
14. Select any log sources that you expect to collect with **Tripwire Log Center.** Examples: **Tripwire Enterprise, Microsoft Windows 10, Tripwire IP360 VnE, Linux Debian, Ubuntu Linux, Microsoft Exchange, Microsoft SQL Server.**



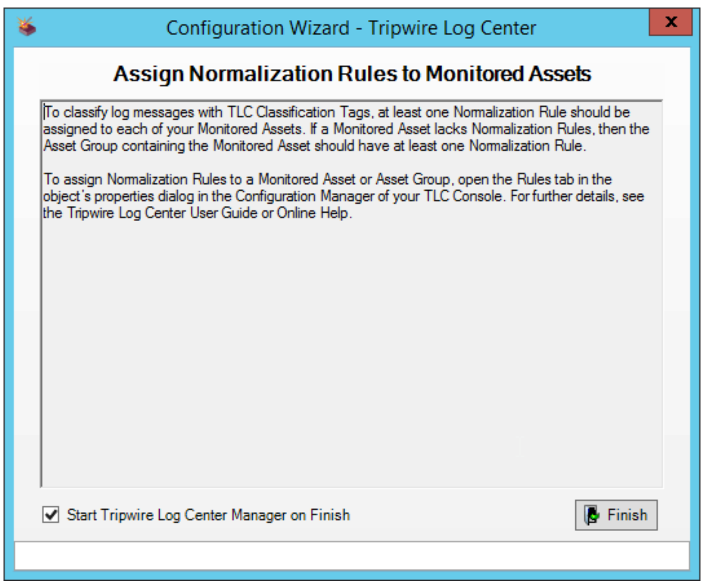
15. Click **Next.**



16. Click **Start.**



17. Click **Next.**



18. Click **Finish.**

2.10.3 Install Tripwire Log Center Console

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

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

2.11 Cisco Identity Services Engine

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

2.11.1 Initial Setup

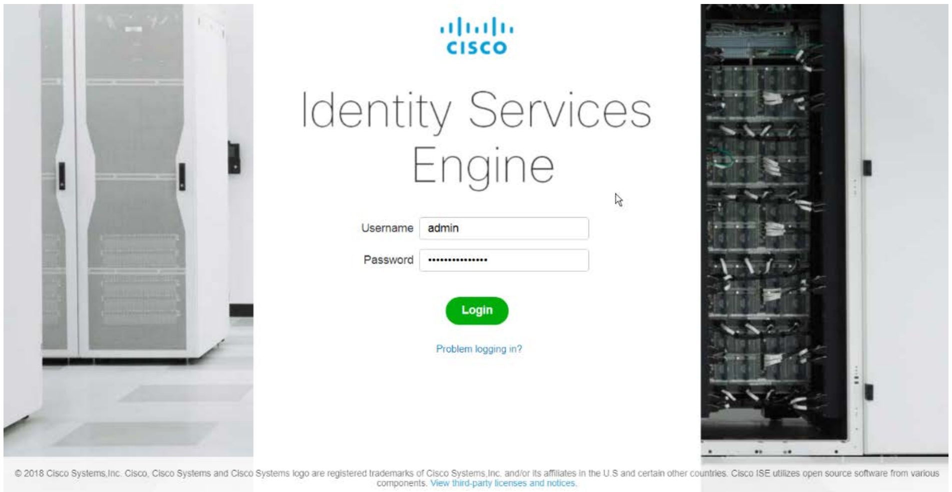
1. When prompted to log in for the first time, enter `setup`. (You can use the command `reset-config` to change these values later.)
2. Enter the desired **hostname** for the machine.
3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated with this IP address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

2.11.2 Inventory: Configure SNMP on Routers/Network Devices

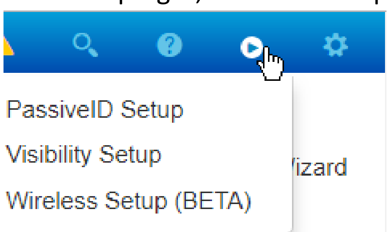
See the corresponding vendor documentation for the correct way to enable SNMP on your network device. Ensure that the community string you choose is considered sensitive, like a password.

2.11.3 Inventory: Configure Device Detection

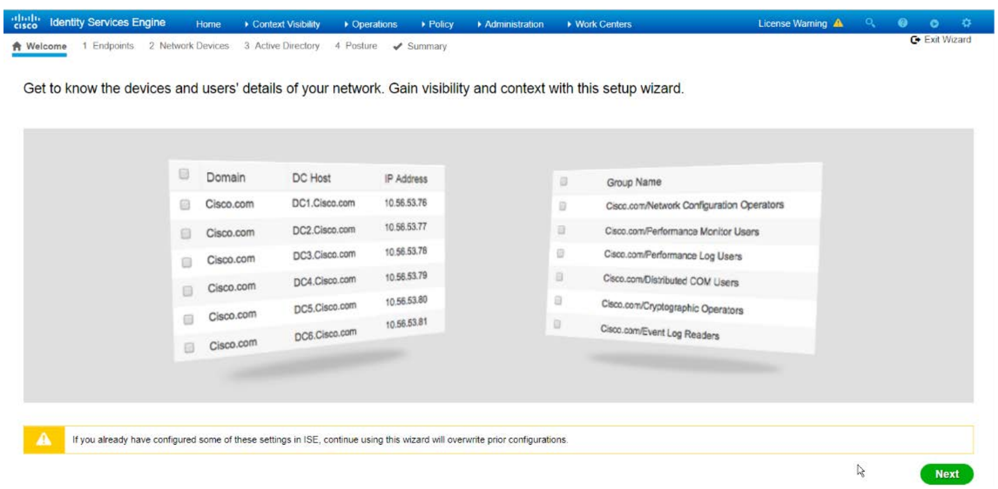
1. Log in to the web client by visiting https://hostname/admin, but replace **hostname** with the hostname of the ISE machine.



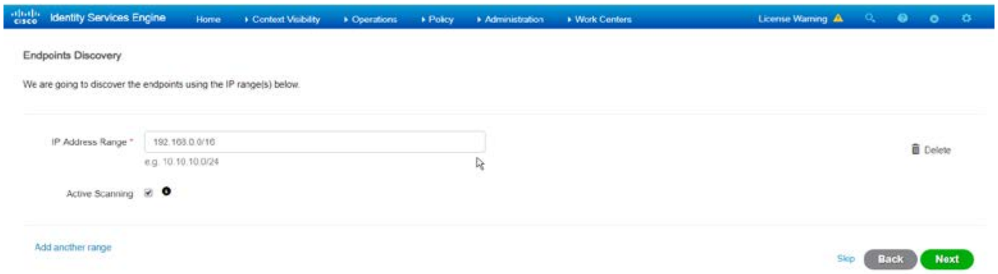
2. On the top right, use the small play button to select **Visibility Setup.**



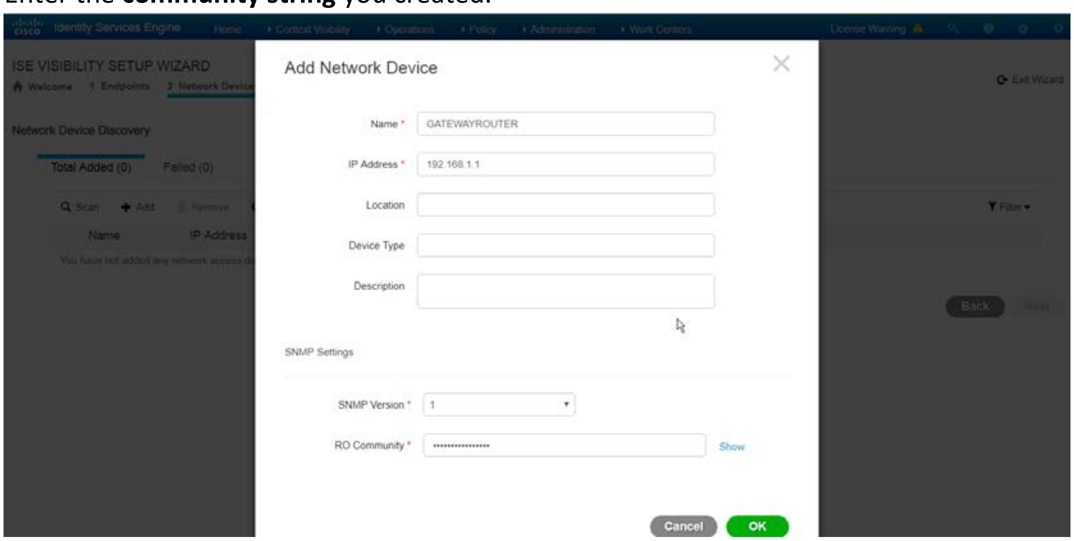
3. Click **Next.**



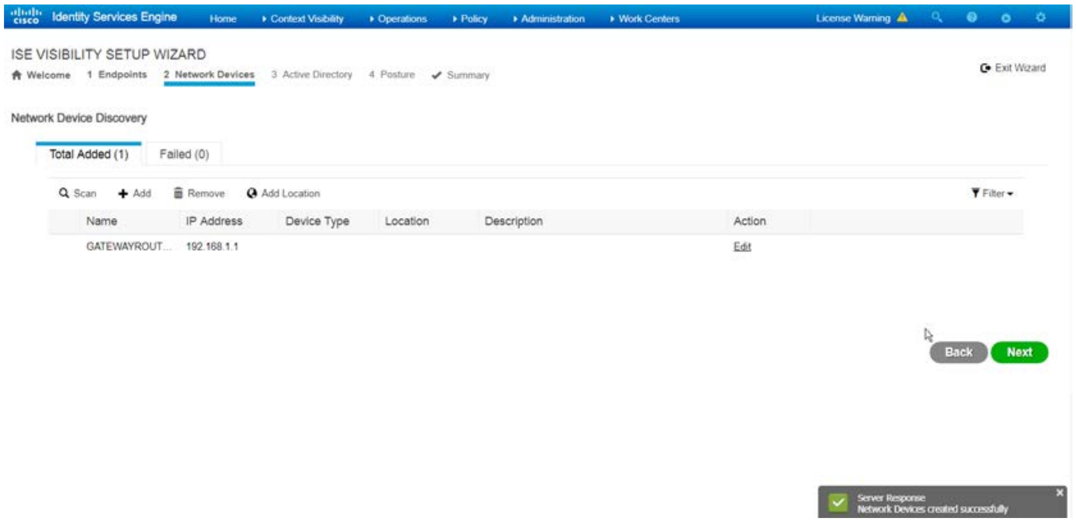
4. Enter the range of IP addresses to add to ISE's inventory.
5. Ensure that **Active Scanning** is checked.



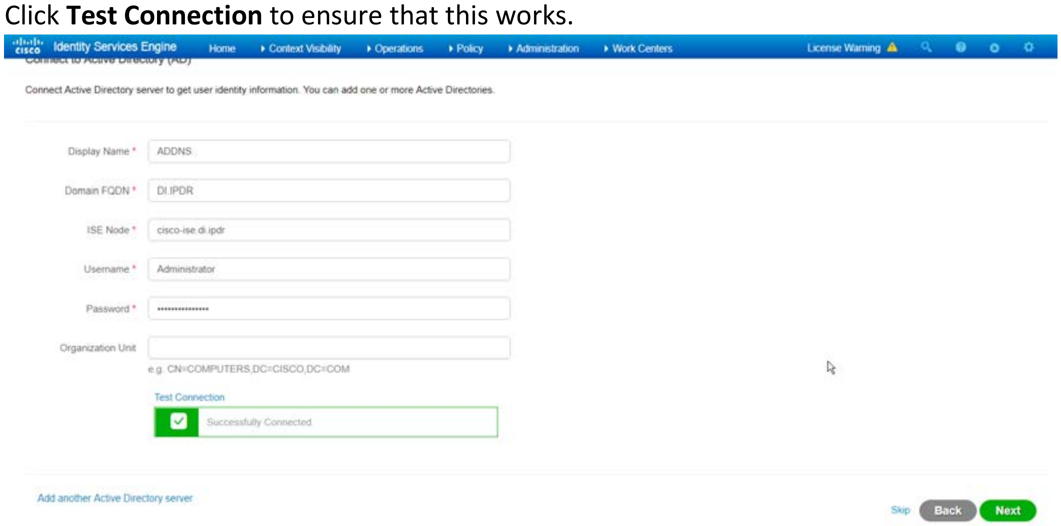
6. Click **Next.**
7. Click the **Add Device Manually** link.
8. Enter a **name.**
9. Enter the **IP address** of the network device you configured for SNMP.
10. Select **1** for **SNMP version.**
11. Enter the **community string** you created.



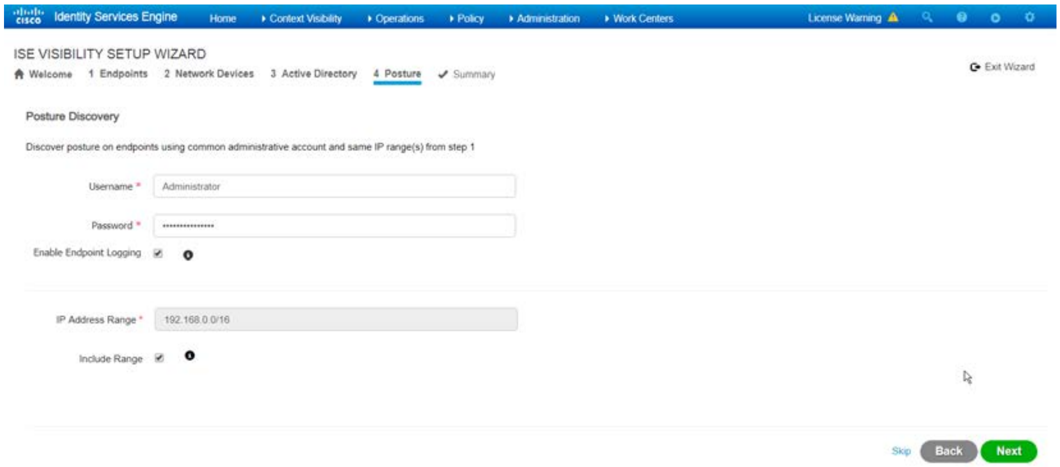
12. Click **OK.**



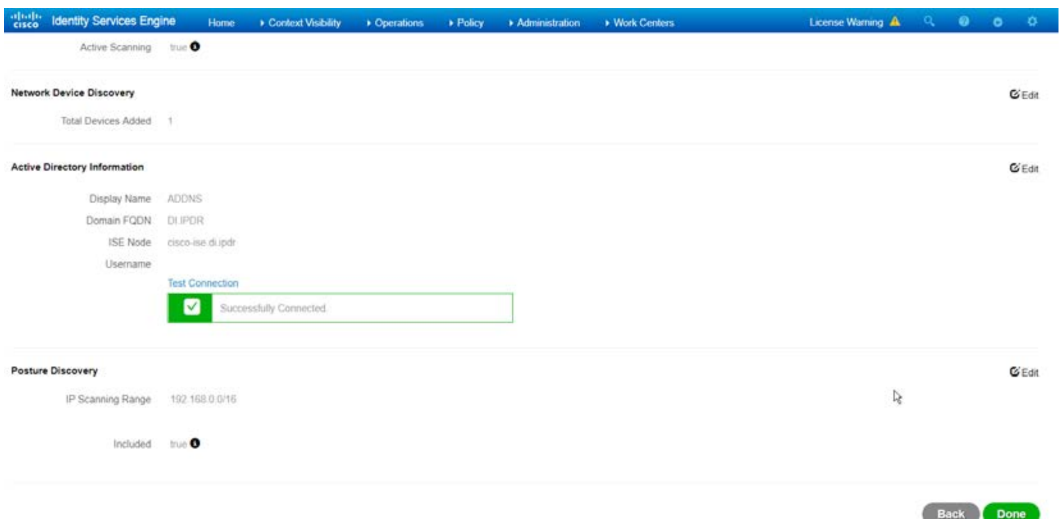
13. Click **Next.**
14. Enter a **display name.**
15. Enter the **domain name.**
16. Enter the **hostname** of **Cisco ISE.**
17. Enter a **username** and **password.**
18. Click **Test Connection** to ensure that this works.



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



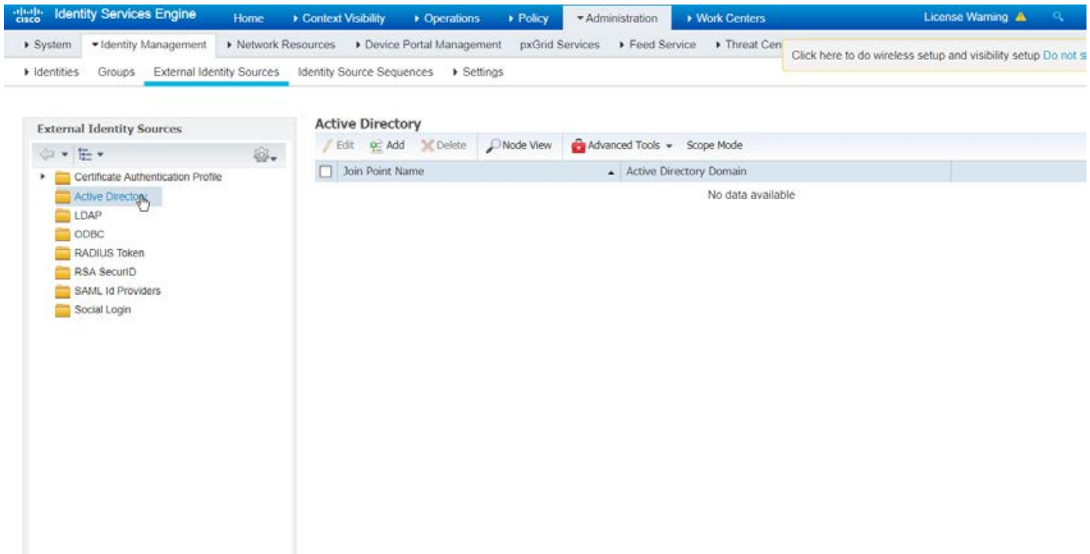
23. Click **Next.**



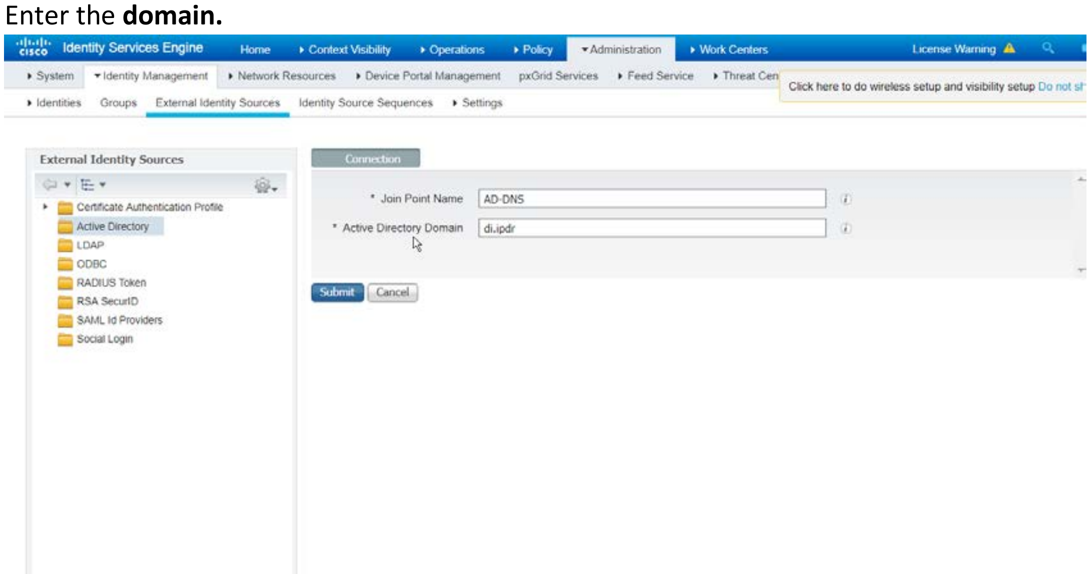
24. Verify the settings, and click **Done.** (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

2.11.4 Policy Enforcement: Configure Active Directory Integration

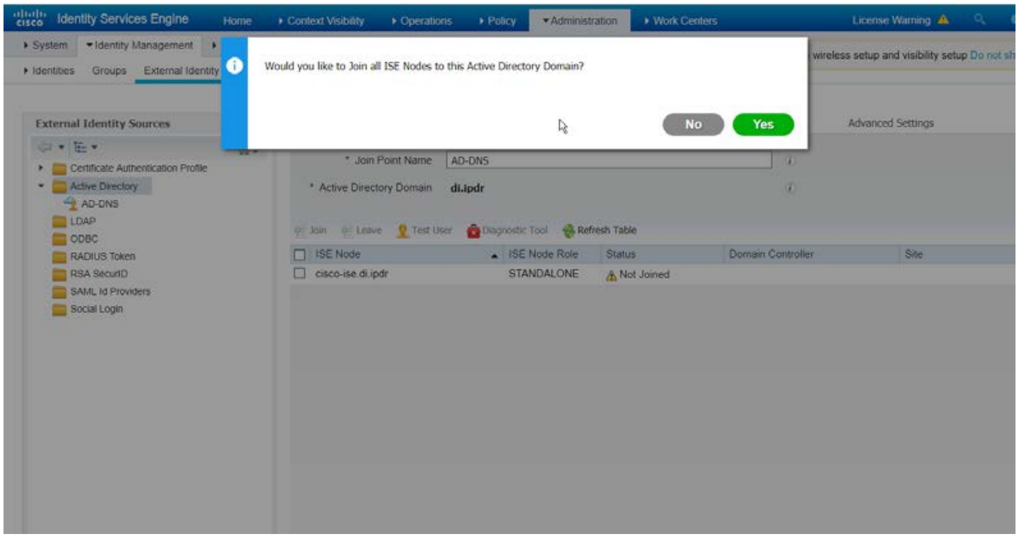
1. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory.*



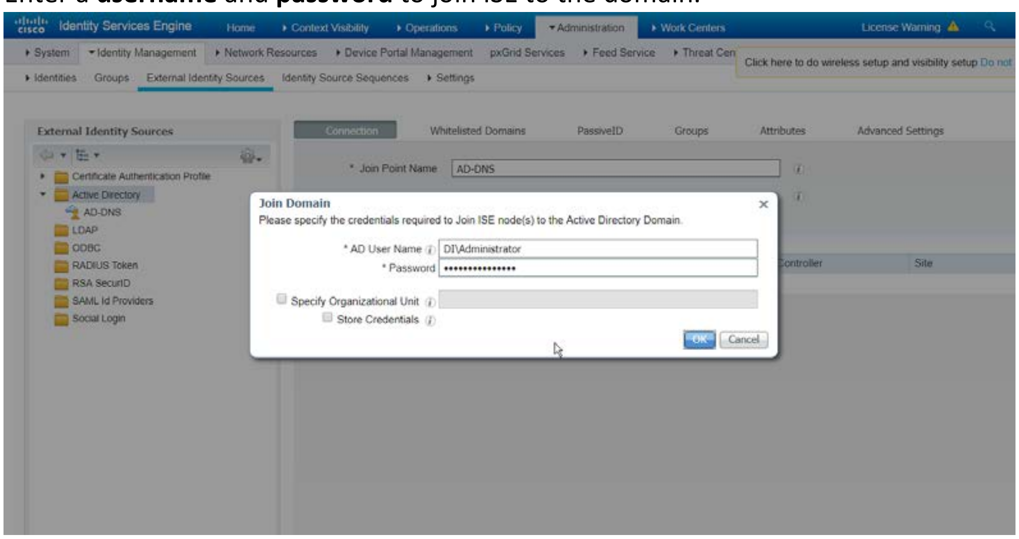
2. Click **Add.**
3. Enter a **name.**
4. Enter the **domain.**



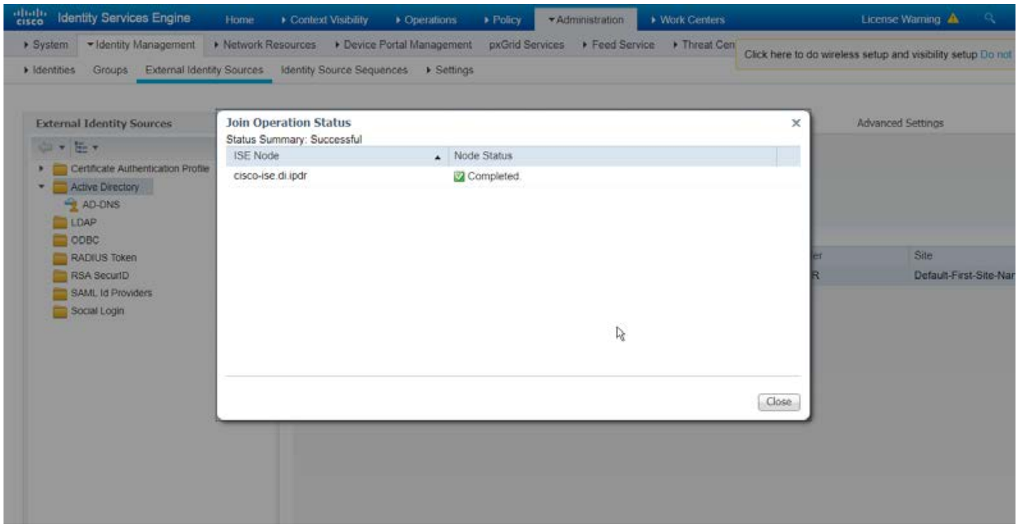
5. Click **Submit.**



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



8. Click **OK.**

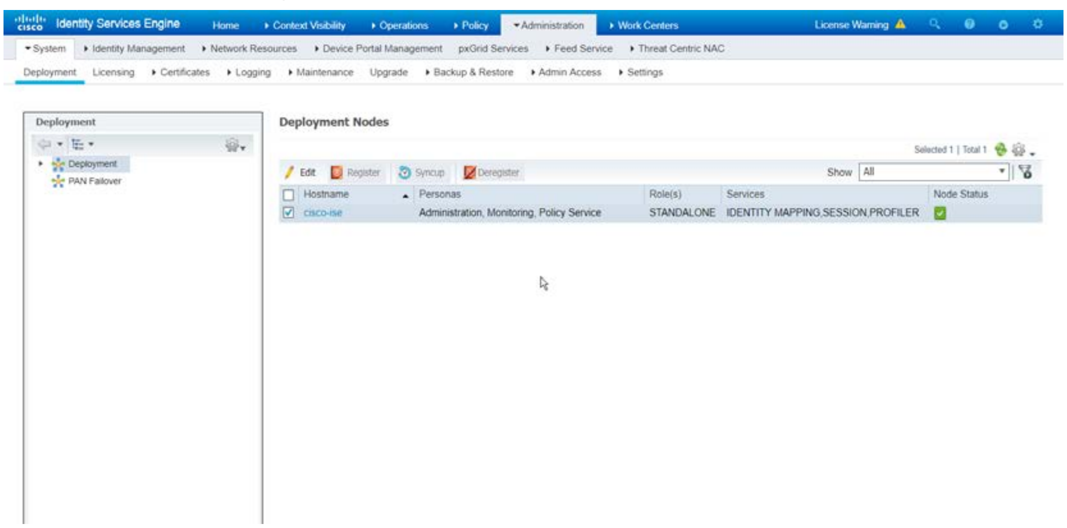


9. Click **Close** when the join is finished.

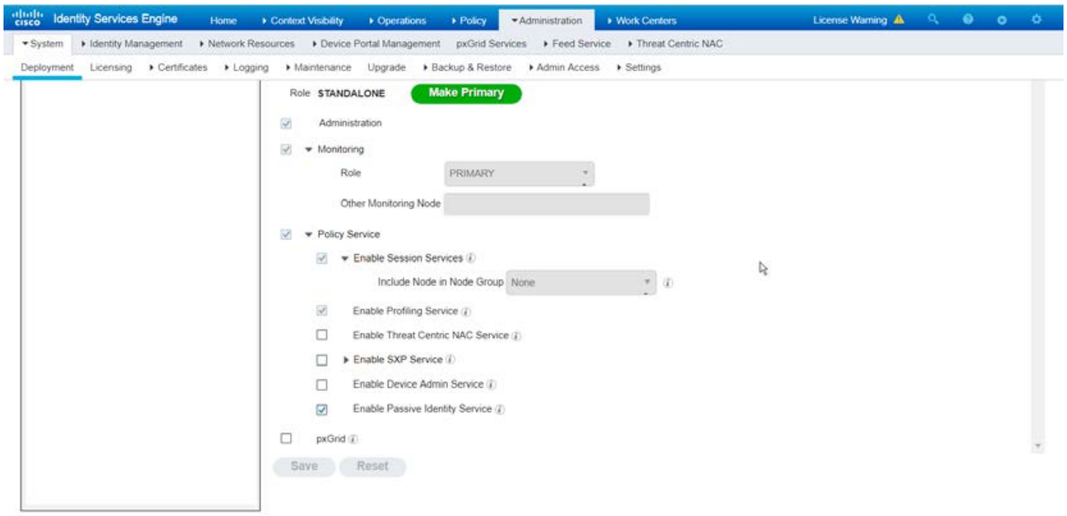
2.11.5 Policy Enforcement: Enable Passive Identity with AD

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

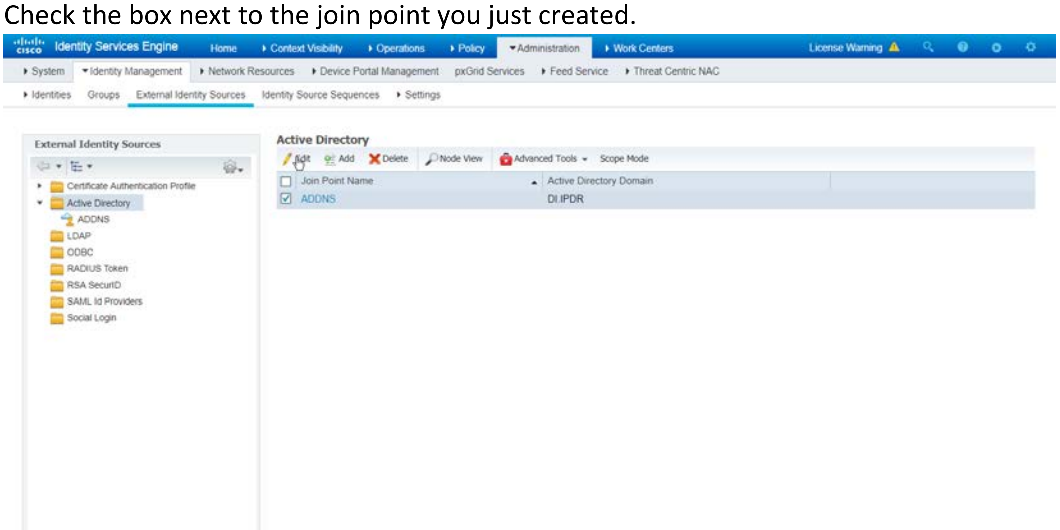
1. Navigate to **Administration > System > Deployment.**
2. Check the box next to **ISE.**



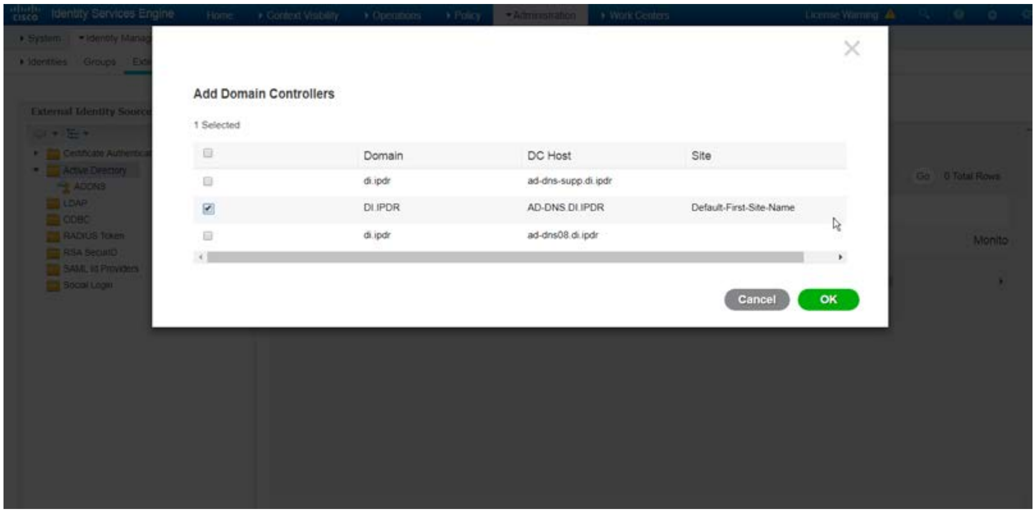
3. Click **Edit.**
4. Check the box next to **Enable Passive Identity Service.**



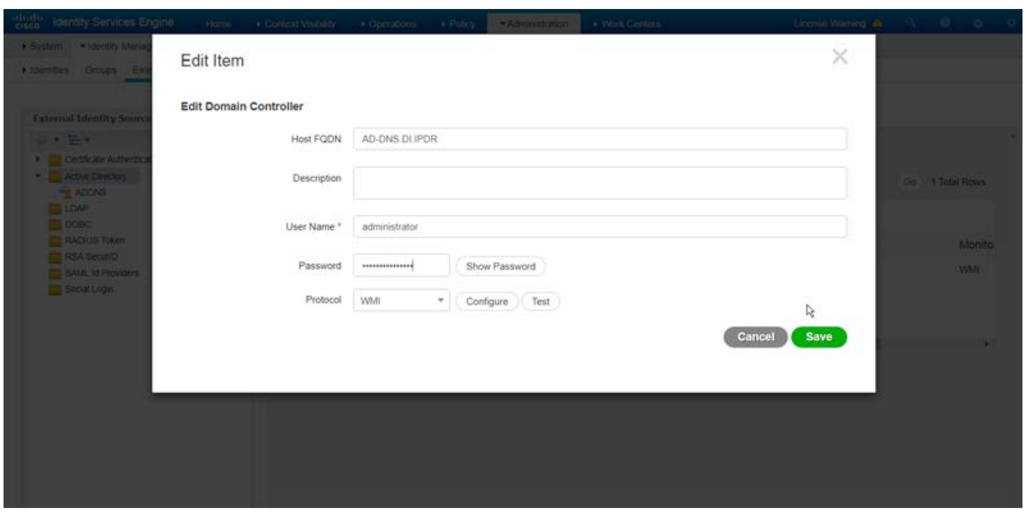
5. Click **Save.**
6. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory.*
7. Click the name of the Active Directory machine.
8. Check the box next to the join point you just created.



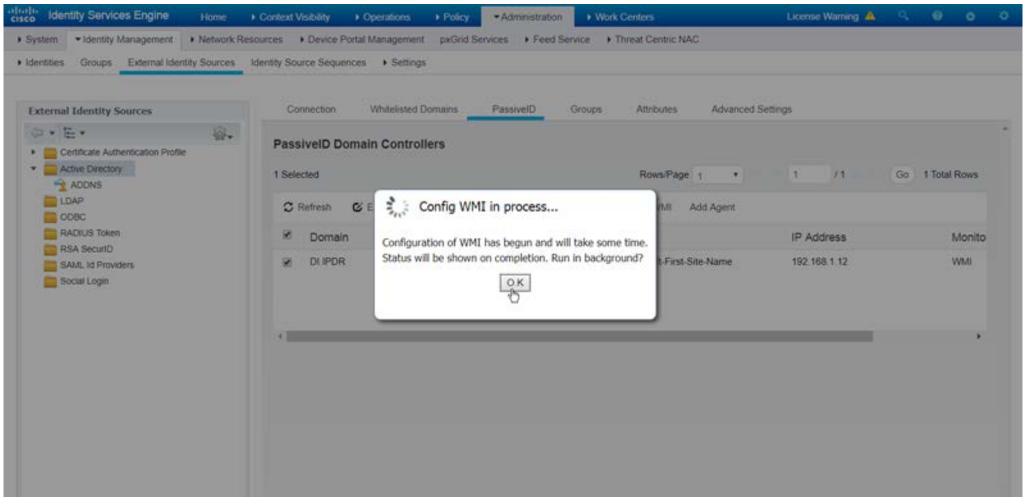
9. Click **Edit.**
10. Click the **PassiveID** tab.
11. Click **Add DCs** if there are no domain controllers listed.



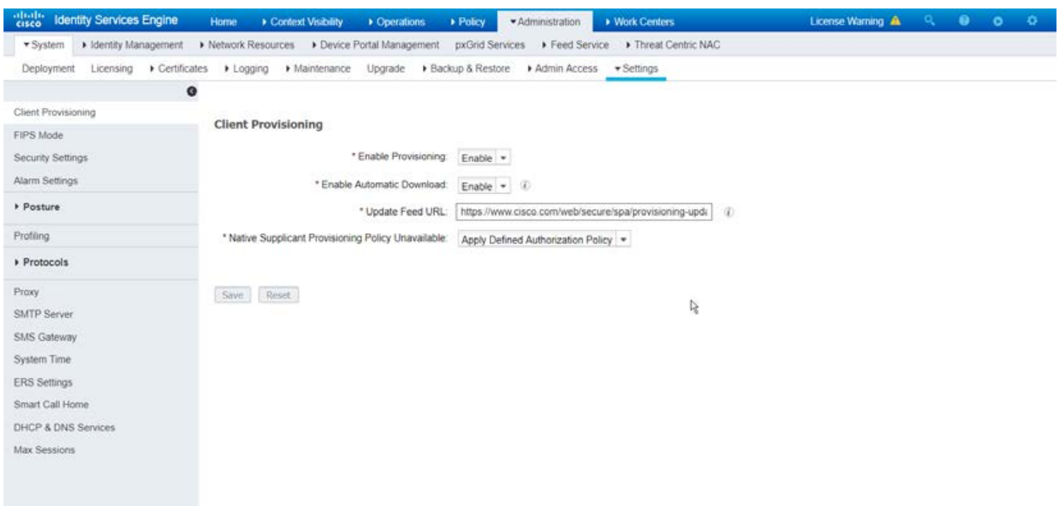
12. Select the Active Directory domain controller.
13. Click **OK.**
14. Check the box next to the selected domain controller.
15. Click **Edit.**
16. Enter credentials for an administrator account.



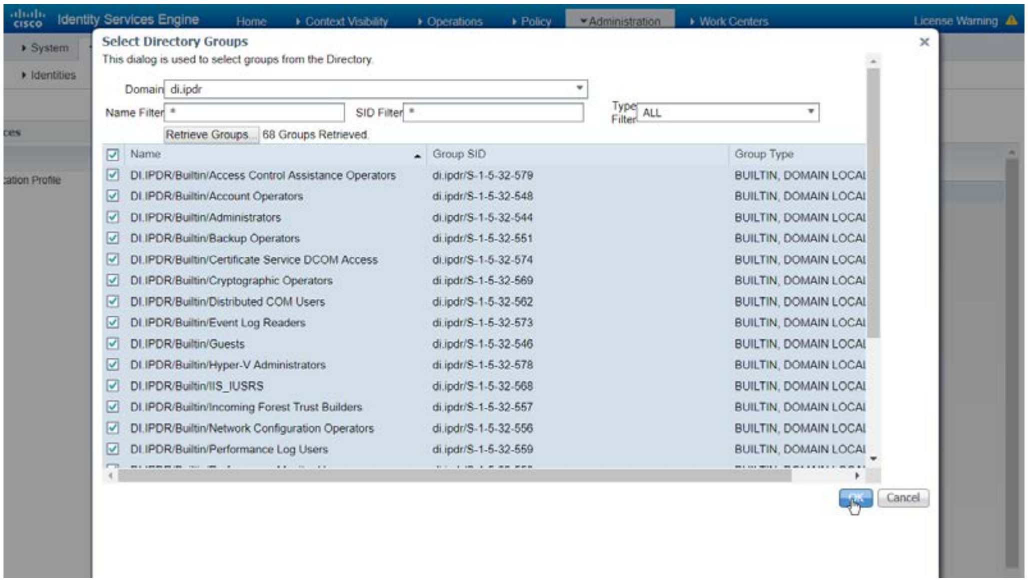
17. Click **Save.**
18. Click **Config WMI.**
19. Click **OK.**



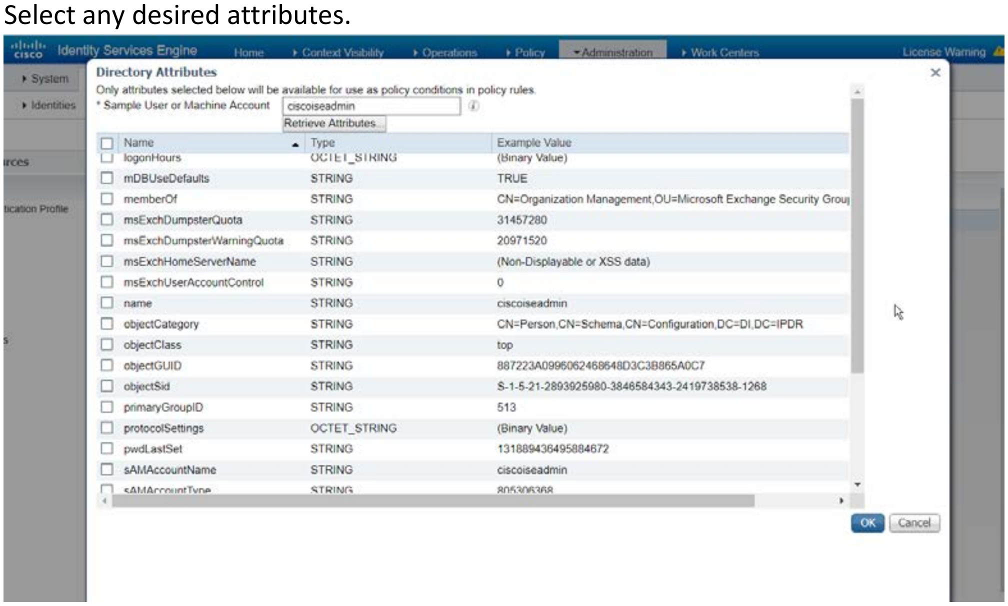
20. Click **OK** when this configuration finishes.
21. Navigate to *Administration > System > Settings > Client Provisioning.*
22. Set Enable **Automatic Download** to **Enable.**



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



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

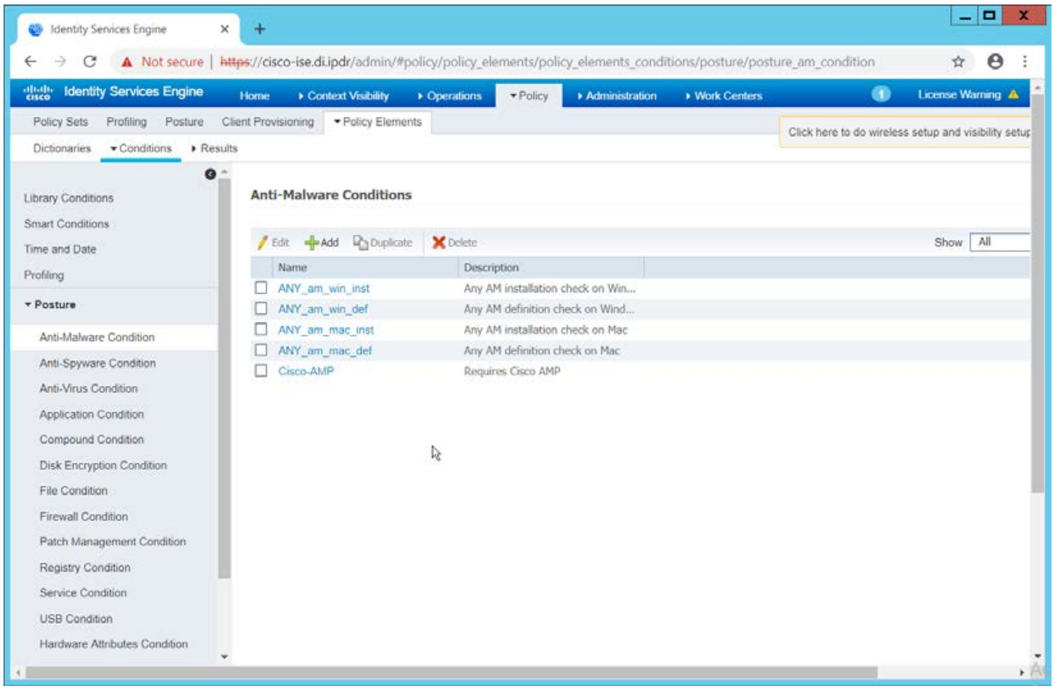


36. Click **OK.**

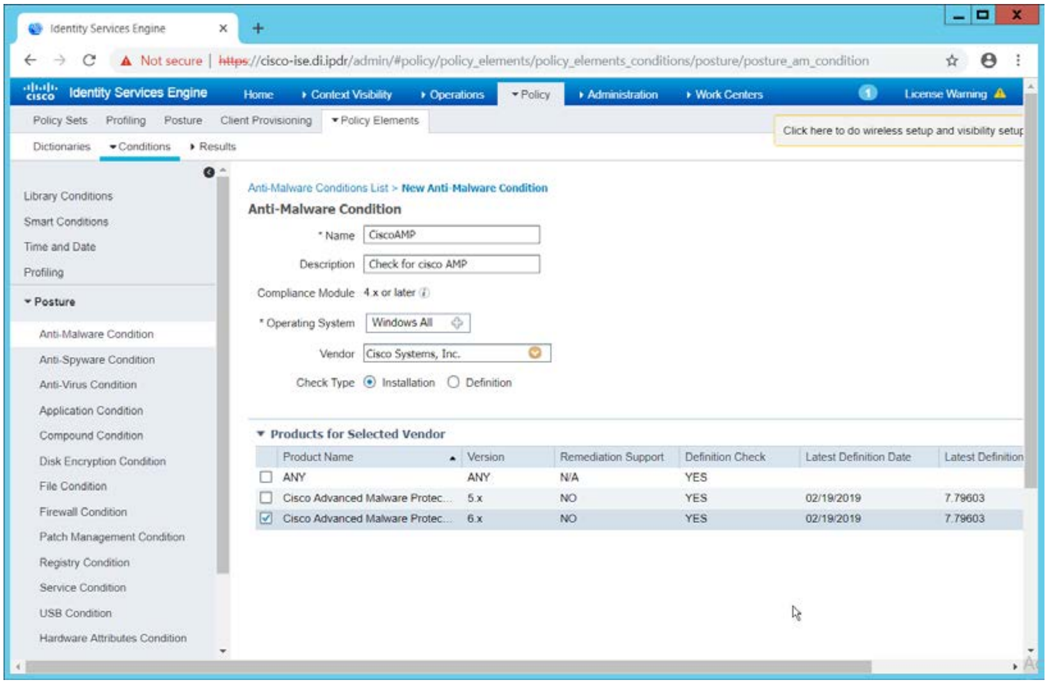
37. Click **Save.**

2.11.6 Policy Enforcement: Developing Policy Conditions

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



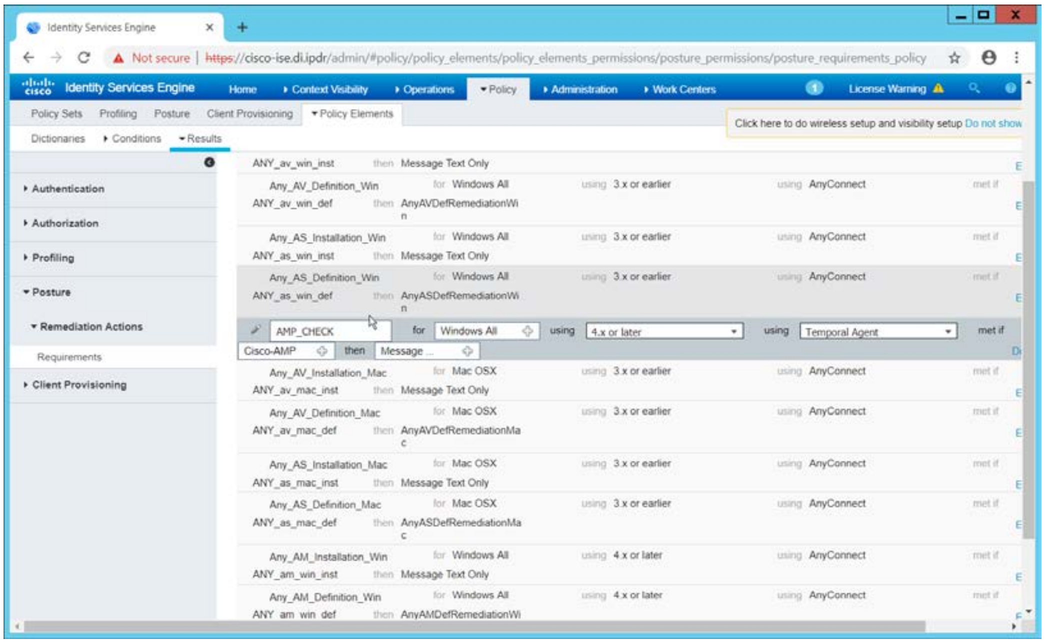
4. Click **Add.**
5. Enter a **name.**
6. Enter a **description** if desired.
7. Select **Windows All** for **Operating System.**
8. Select **Cisco Systems, Inc.** for **Vendor.**
9. Under **Products for Selected Vendor,** check the box next to **Cisco Advanced Malware Protection,** with the version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



10. Click **Submit.**

2.11.7 Policy Enforcement: Developing Policy Results

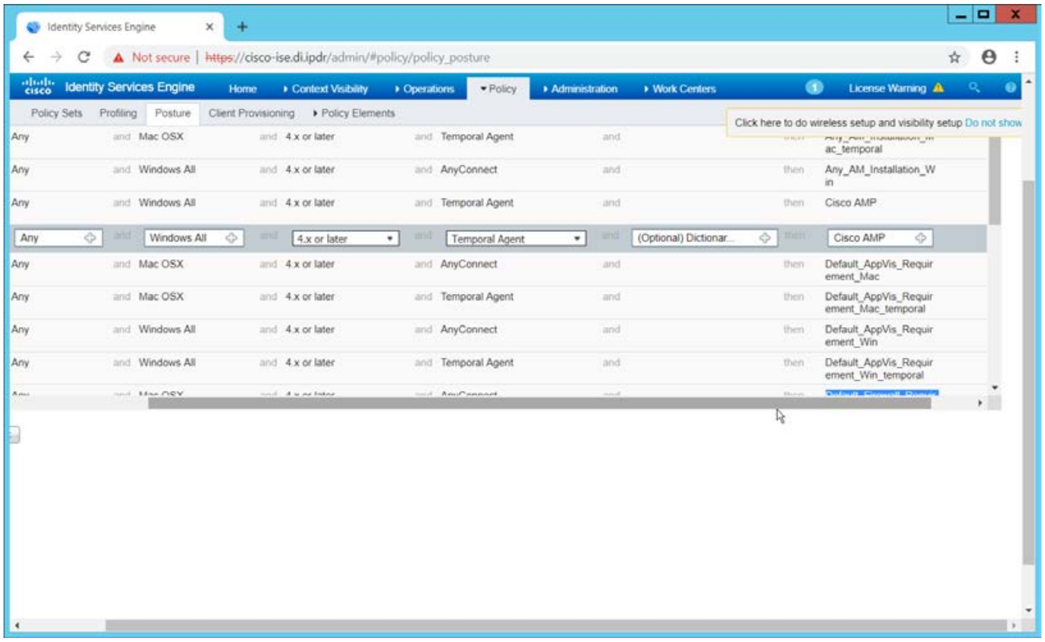
1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements.**
2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement.**
3. Enter a **name.**
4. Select **Windows All** for **Operating Systems.**
5. Select **4.x or later** for **Compliance Module.**
6. Select **Temporal Agent** for **Posture.**
7. Select **User Defined Conditions > Anti-Malware Condition > Cisco AMP** (substitute “Cisco AMP” with the name of the condition you just created).
8. Select **Message Text Only** for the **Remediation Action.** (Other remediation actions can be defined by going to **Policy > Policy Elements > Results > Posture > Remediation Actions,** but there is no option for Cisco AMP to be installed, so we leave the default for now.)
9. Enter a **Message** to show to the user to inform them that they must install Cisco AMP.



10. Click **Save.**

2.11.8 Policy Enforcement: Enforcing a Requirement in Policy

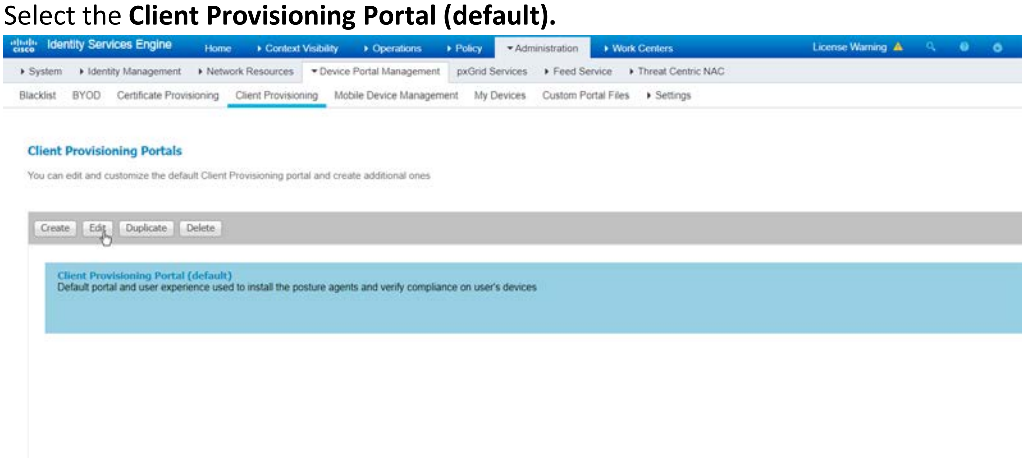
1. Navigate to **Policy > Posture.**
2. Click one of the black arrows next to the **Edit** link and select **Insert New Policy.**
3. Enter a **name.**
4. Select **Windows All** for **Operating Systems.**
5. Select **4.x or later** for **Compliance Module.**
6. Select **Temporal Agent** for **Posture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



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

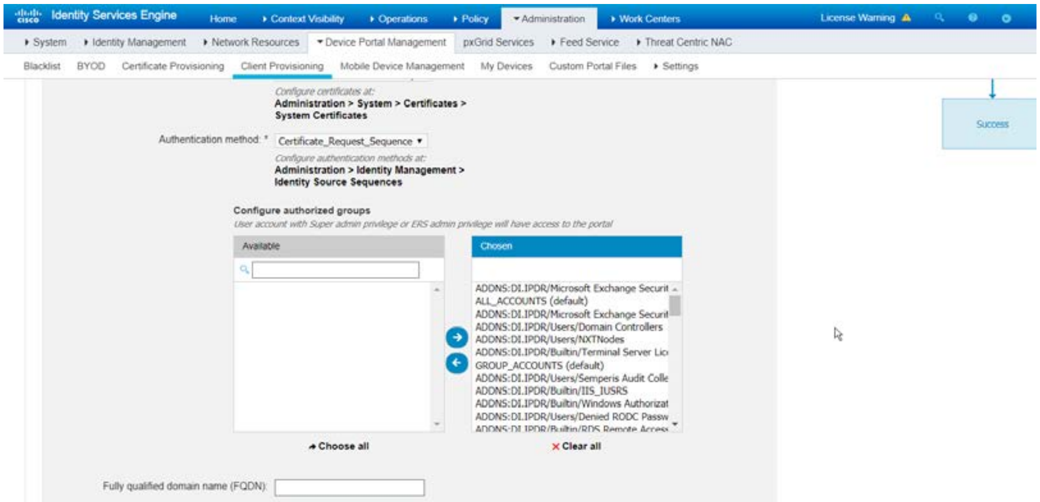
2.11.9 Policy Enforcement: Configuring a Web Portal

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



3. Click **Edit.**

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



6. Click **Save.**

2.11.10 Configuring RADIUS with your Network Device

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

1. The **Network Device** (i.e. the router or switch) must support RADIUS functions, specifically **Authentication, Authorization,** and **Accounting.** Furthermore, it must also support **CoA,** which is **Change of Authorization.**
    a. To configure this, you must configure your network device to use Cisco ISE as a Radius Server. What this means is that your network device will forward authentication requests to Cisco ISE, and Cisco ISE will respond with an "accept" or "reject."
2. The **Network Device** must support some form of **802.1x.** Note that this is not supported on certain routers, even if RADIUS is supported. **802.1x** is a mechanism for authenticating the end workstation to the network device, potentially over wireless or through ethernet.
    a. This can take various forms, such as a captive web portal, MAC address authentication, or user authentication. A captive web portal, if the device supports it, may be ideal for configuration without the correct hardware.
    b. There are also many switches that provide direct 802.1x username/password authentication. Note that if you choose to use this mechanism, a client is still required,

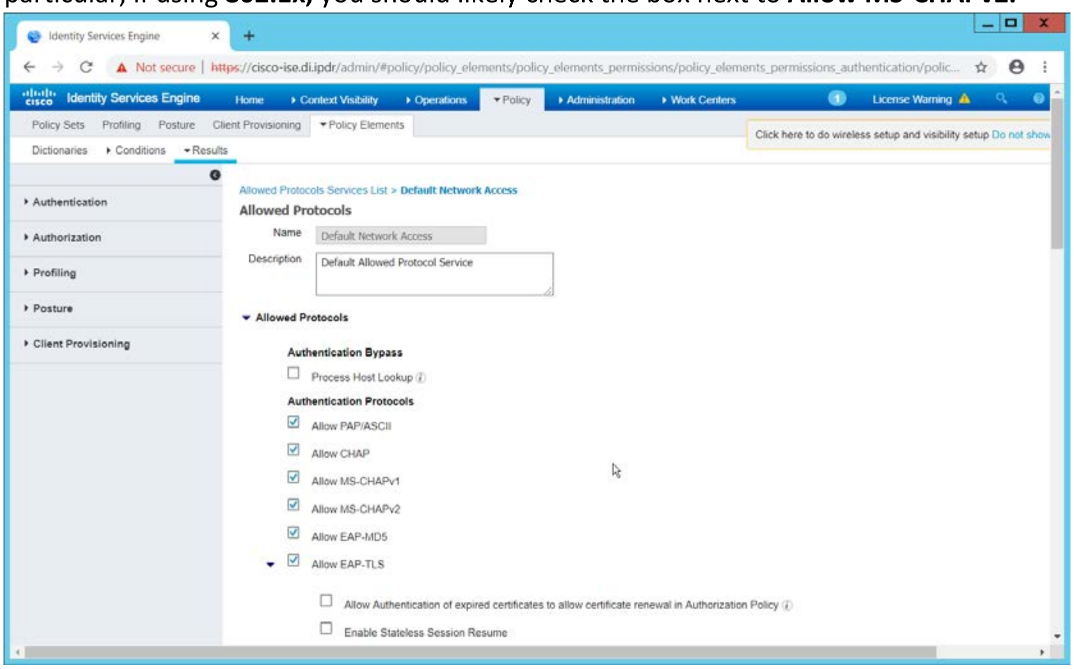
and it will not be in the web browser. Windows has a built-in **802.1x** client that can be configured on Network adapters under the **Authentication** tab. To enable it, you must first start the service **Wired AutoConfig,** and then the **Authentication** tab will become available for configuration.

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

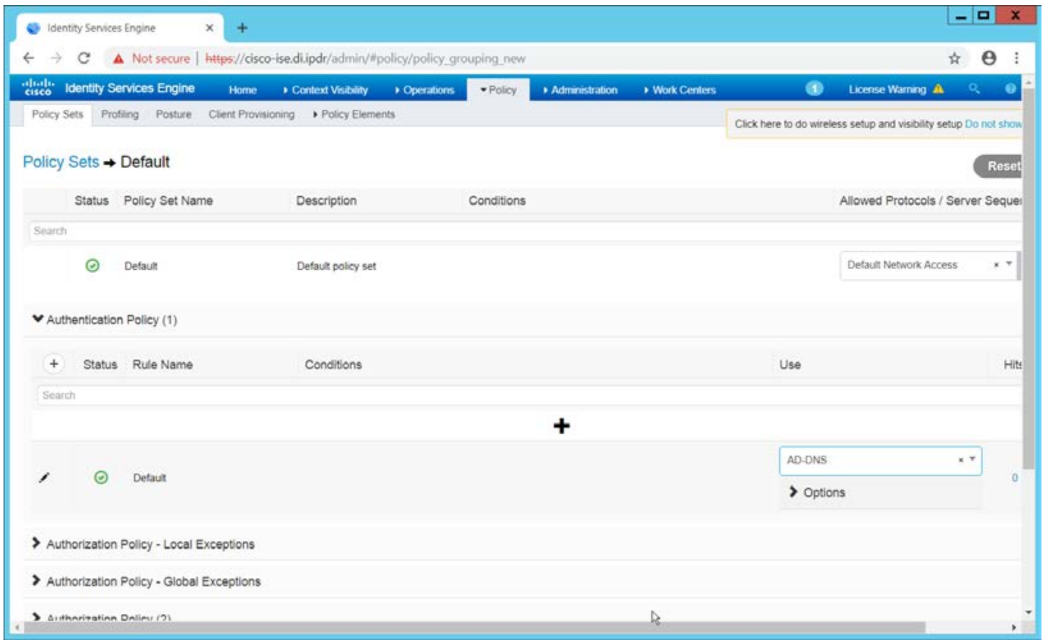
3. The two steps above detail the **authentication** phase. Once authenticated, the network device must redirect the user to the client provisioning portal (or to a guest portal), depending on the setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.
4. The user will then authenticate to the **Guest Portal** or **Client Provisioning Portal** (depending on your setup). The portal will prompt the user to download an executable, which will run posture.
5. The executable will *first* check for the existence of a RADIUS session in Cisco ISE for the user who downloaded the executable. It will primarily check the MAC address that visited the ISE web portal against the MAC addresses of existing sessions. *If and only if a session exists*, it will run posture based on the policy you set up. You can verify that a session exists by navigating to **Operations > RADIUS > Live Sessions.**

2.11.11 Configuring an Authentication Policy

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



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

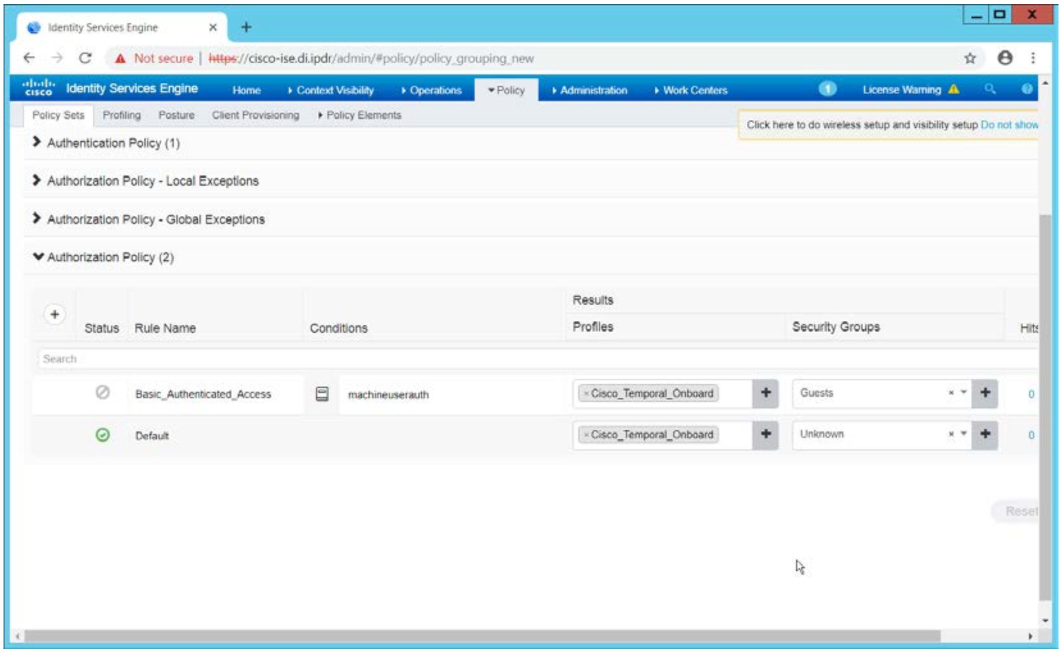


9. Click **Save.**

2.11.12 Configuring an Authorization Policy

1. The Authorization Profile is likely dependent on your network device, but it is possible that the **Cisco_Temporal_Onboard** profile will work even for non-Cisco devices. You can edit the authorization policy by navigating to **Policy > Policy Elements > Results > Authorization > Authorization Profiles.**
2. The temporal onboard profile will attempt to redirect the user to a client provisioning portal– this redirection will most likely only happen automatically on compatible Cisco network devices. If another device is used, the device may need to manually redirect the user to the client provisioning portal after authentication. (We accomplished this in PFSense for our build using a "Post-authentication redirection" feature in the Captive Portal.)
3. Once you are finished configuring the **Authorization Profile,** navigate to **Policy > Policy Sets.**
4. Select the default policy.
5. Expand the **Authorization Policy** section.

6. Note that you can configure this for as many groups and conditions as desired, potentially specifying different authorization profiles for various user groups or levels of authentication, including unauthenticated access. Under **Results > Profiles,** you can select the authorization profiles you configured.



7. Click **Save.**

2.12 Cisco Advanced Malware Protection

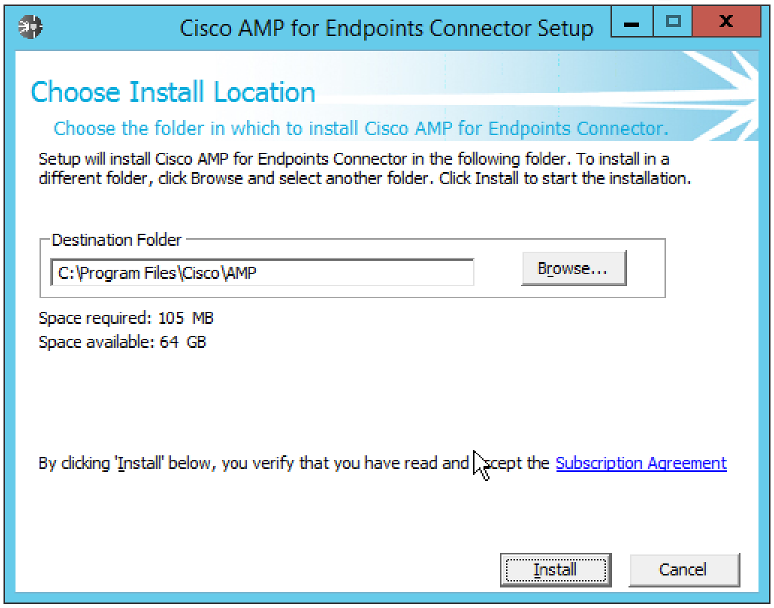
This section assumes the use of the Cisco Advanced Malware Protection (AMP) Console, a cloud-based server that connects to clients on individual machines. There is some configuration to be done on this cloud-based server, which may impact the installation. Cisco provides best practices guides online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

2.12.1 Dashboard Configuration

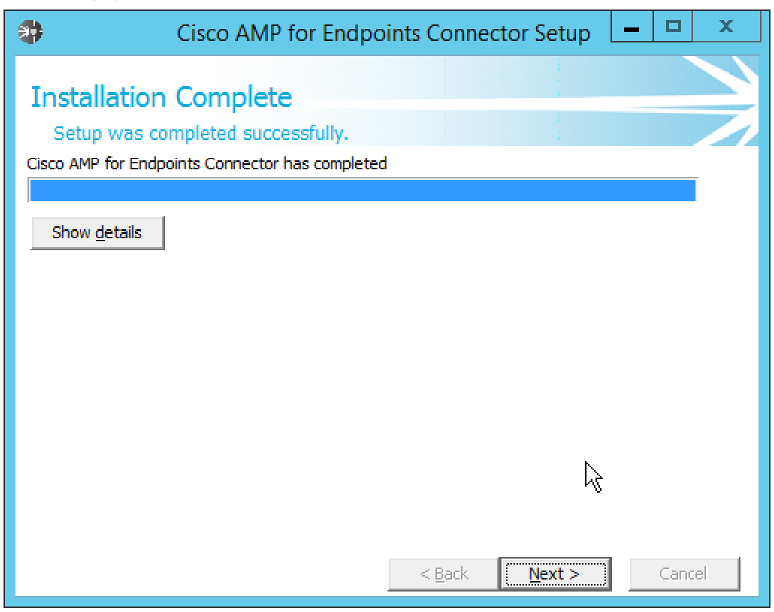
1. From the Cisco AMP dashboard, located at https://console.amp.cisco.com/dashboard, click **Set Up Windows Connector.**
2. The configuration of this will be different for each enterprise, so consult your Cisco representative for the proper way to set this up. For the purposes of this build, we accepted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

2.12.2 Installing the Connector on a Windows Server

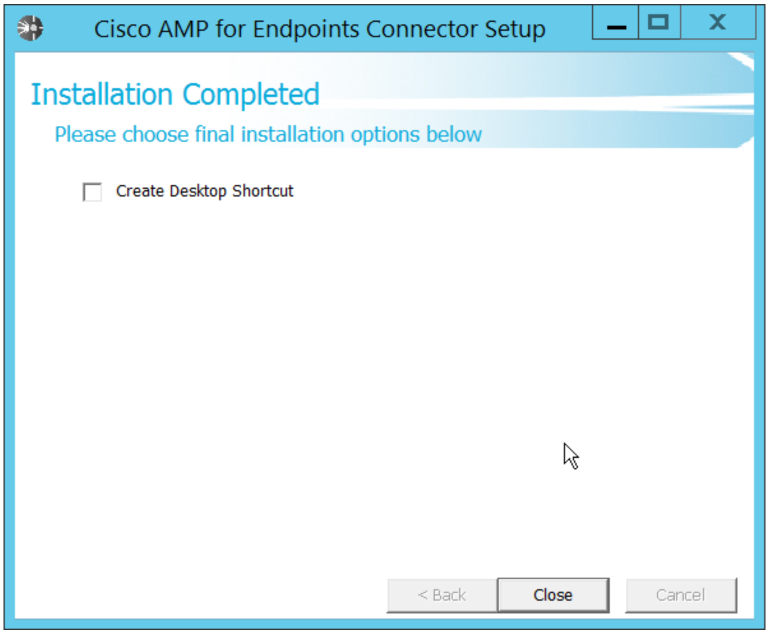
1. On the Cisco AMP dashboard, navigate to **Management > Download Connector.**
2. Select the AMP group in which to put the machine. For example, when installing on an Active Directory machine, we chose **Domain Controller.**
3. Find the correct OS version of the installer, and click **Download.**
4.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



5. Click **Install.**



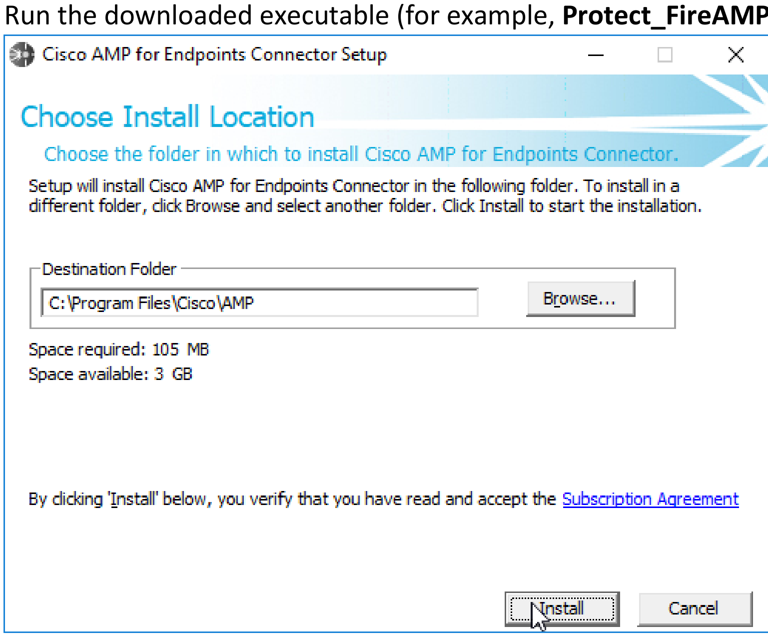
6. Click **Next.**



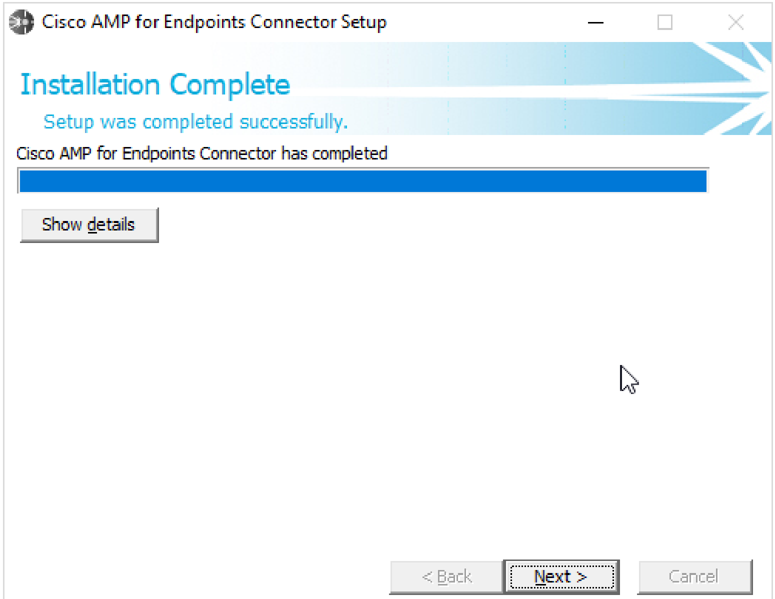
7. Click **Close.**

2.12.3 Installing the Connector on a Windows 10 Machine

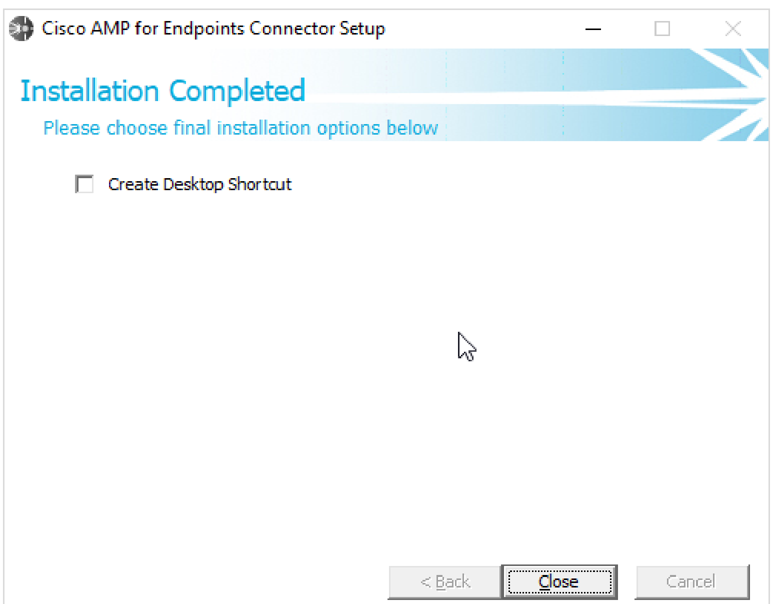
1. On the Cisco AMP dashboard, navigate to **Management > Download Connector.**
2. Select the AMP group in which to put the machine. For this installation we chose **Protect.**
3. Find the correct OS version of the installer, and click **Download.**
4. Run the downloaded executable (for example, **Protect_FireAMPSetup.exe**).



5. Click **Install.**



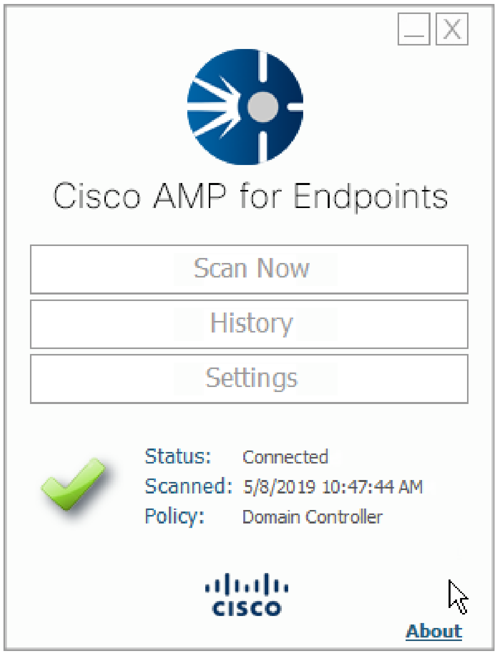
6. Click **Next.**



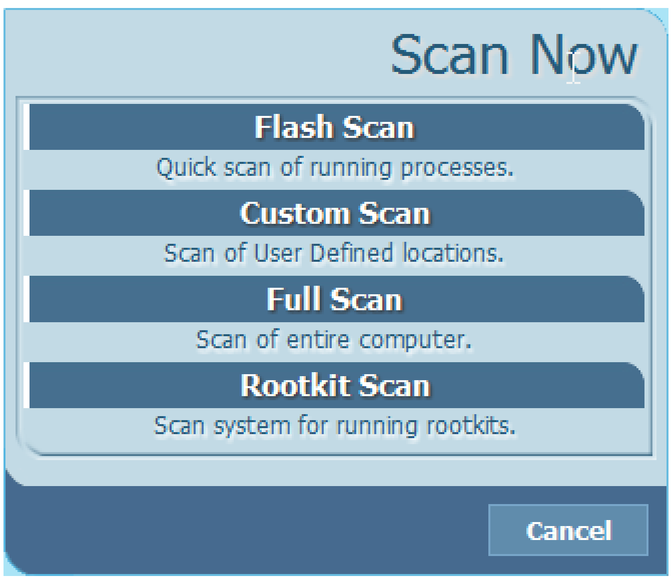
7. Click **Close.**

2.12.4 Scanning using AMP

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



2. Click **Scan Now.**

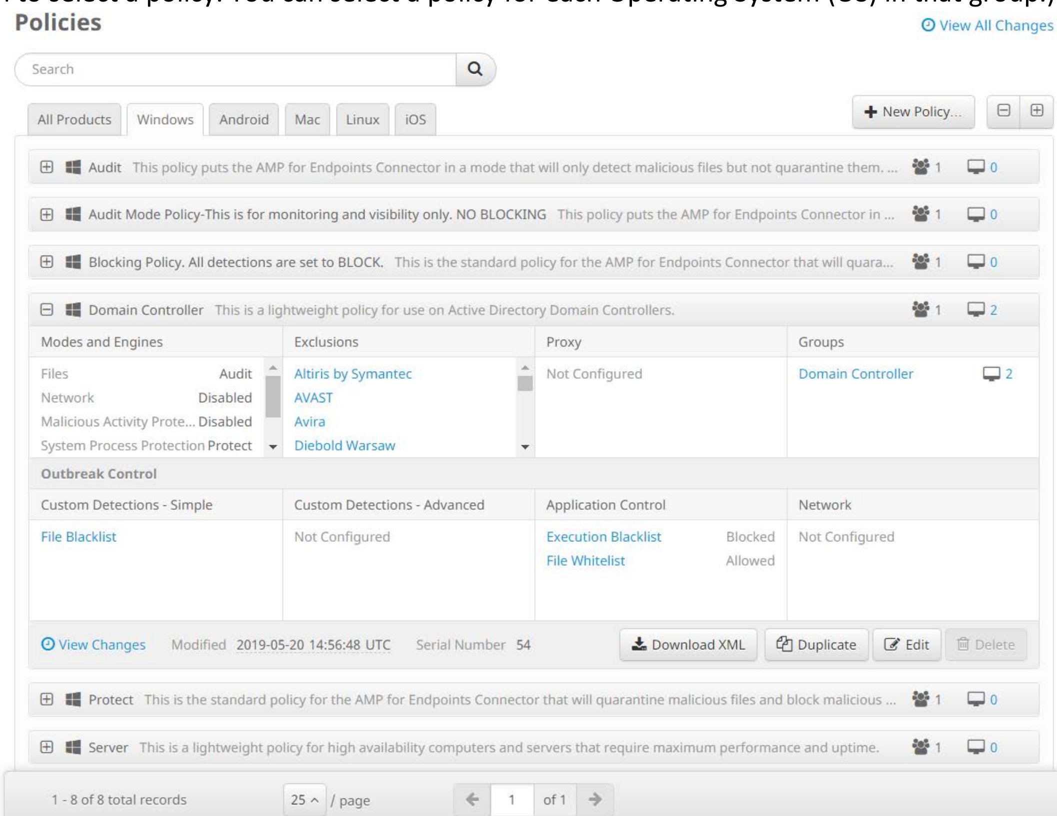


3. Click **Full Scan.**
4. A scan should begin.

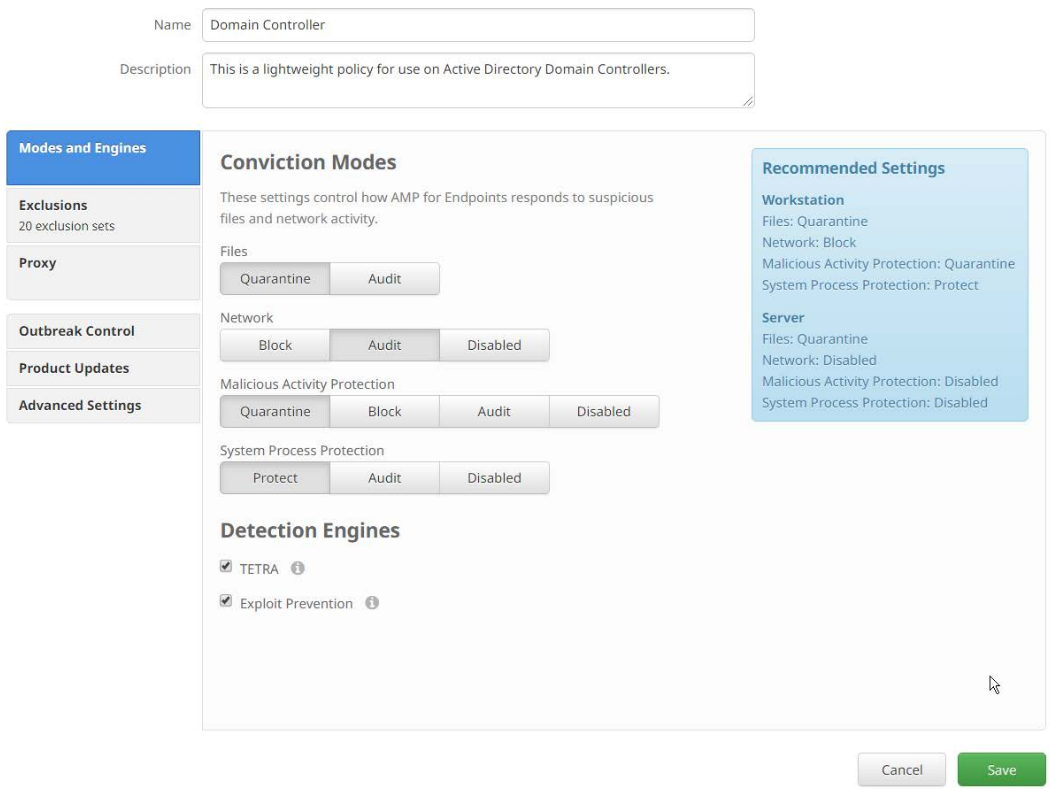
2.12.5 Configure AMP Policy

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

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



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



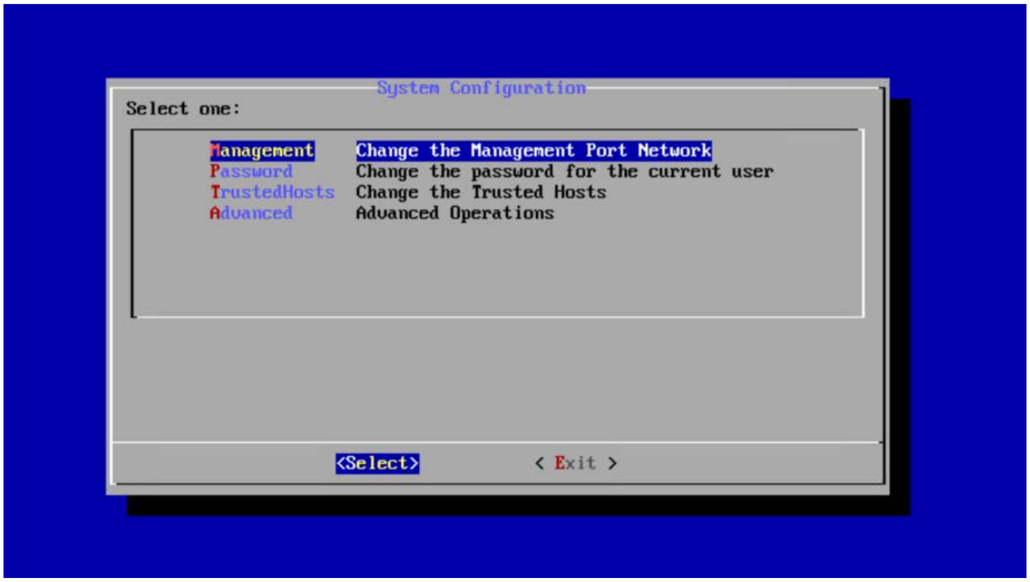
6. Click **Save.**

2.13 Cisco Stealthwatch

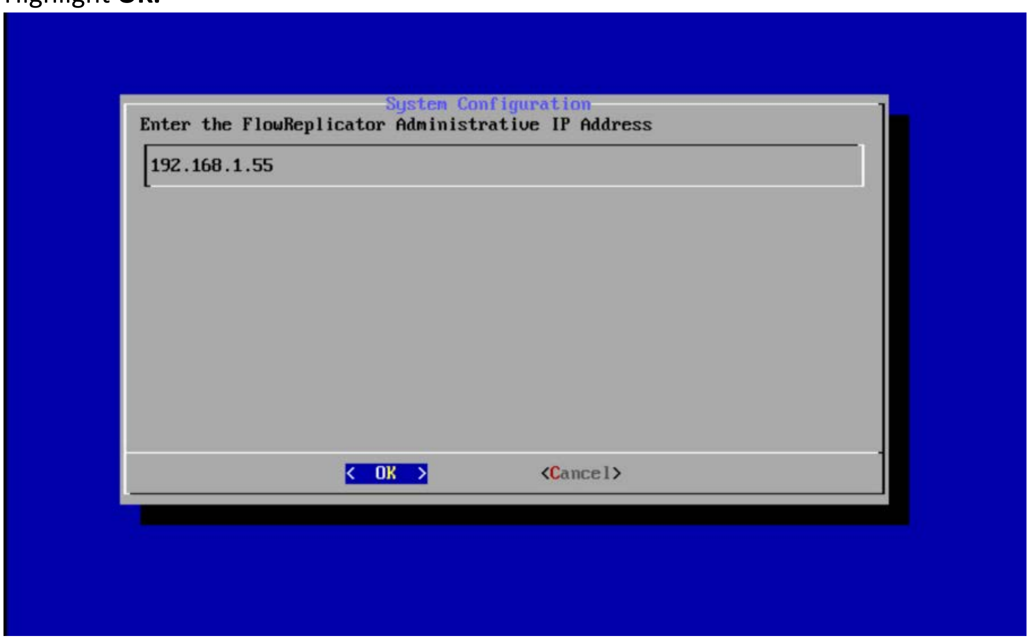
This section will describe the setup and configuration of Cisco Stealthwatch, a network monitoring solution. This guide assumes the use of the Stealthwatch virtual machines.

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

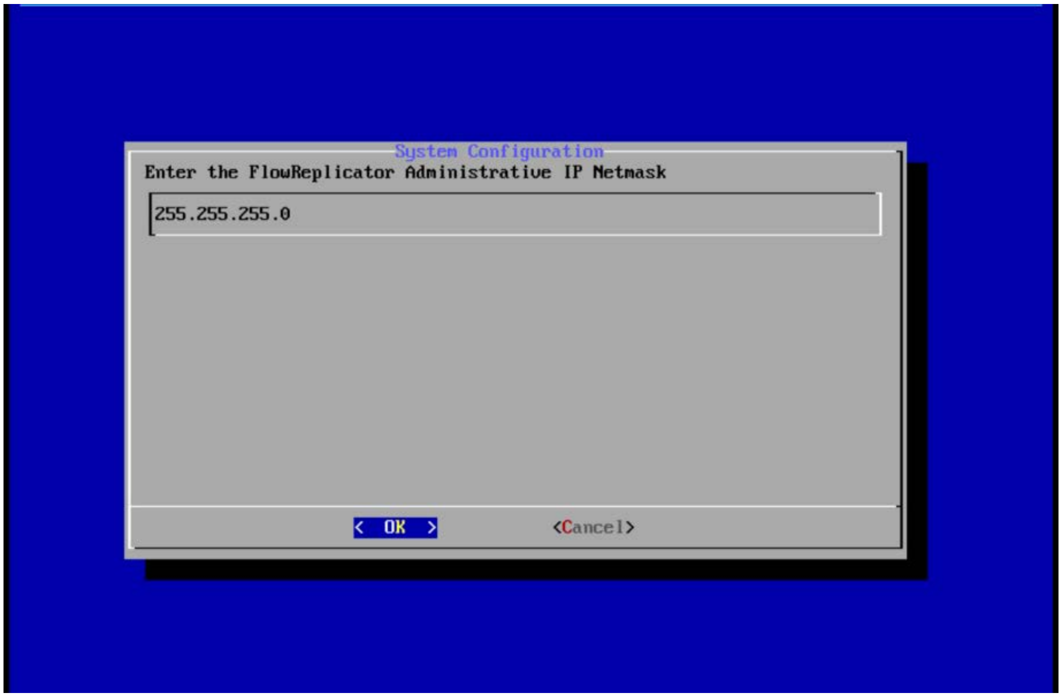
1. Log in to the console of **Stealthwatch Flow UDP Director.**
2. Navigate the menu to highlight **Management** and **Select.**



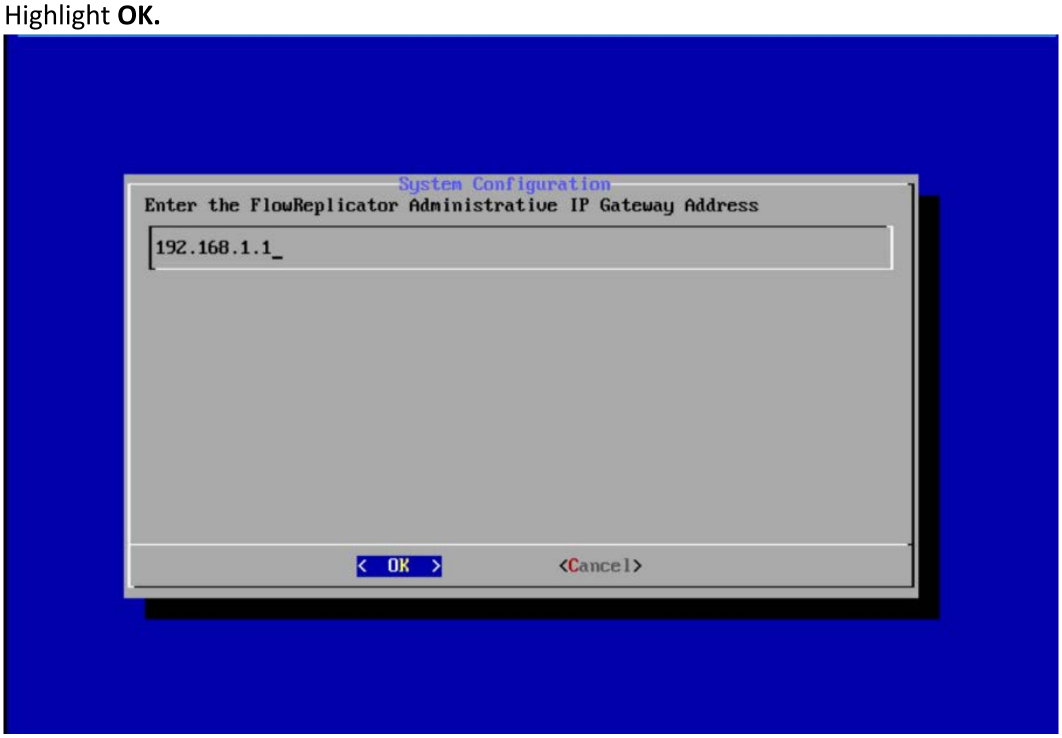
3. Press **Enter.**
4. Enter an **IP Address** for this machine.
5. Highlight **OK.**



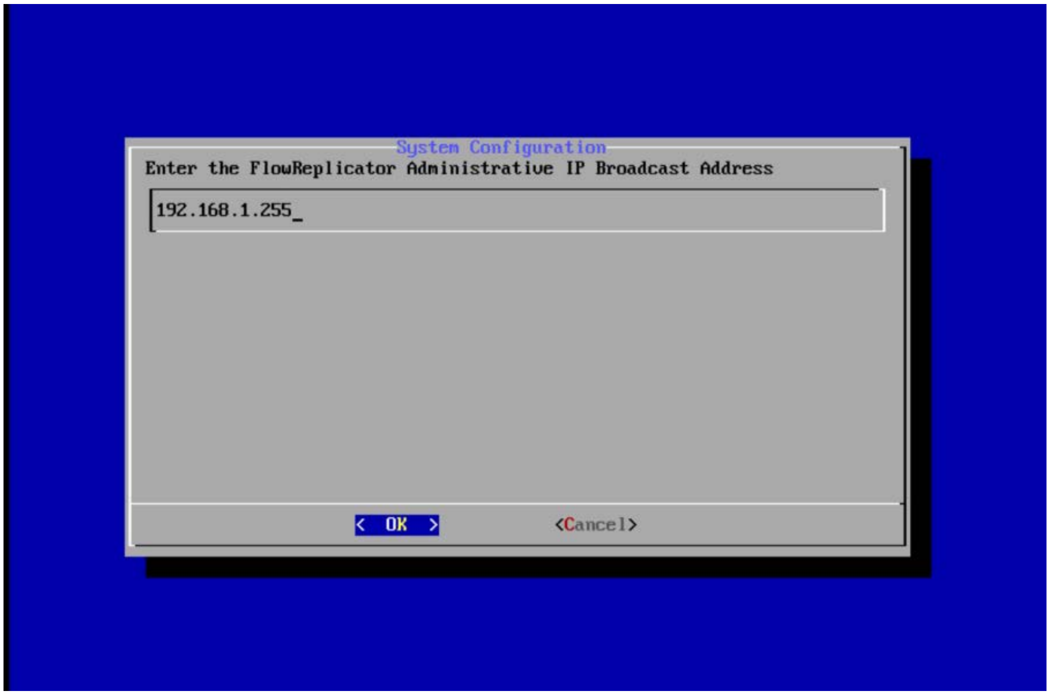
6. Press **Enter.**
7. Enter a **network mask** for the IP Address.
8. Highlight **OK.**



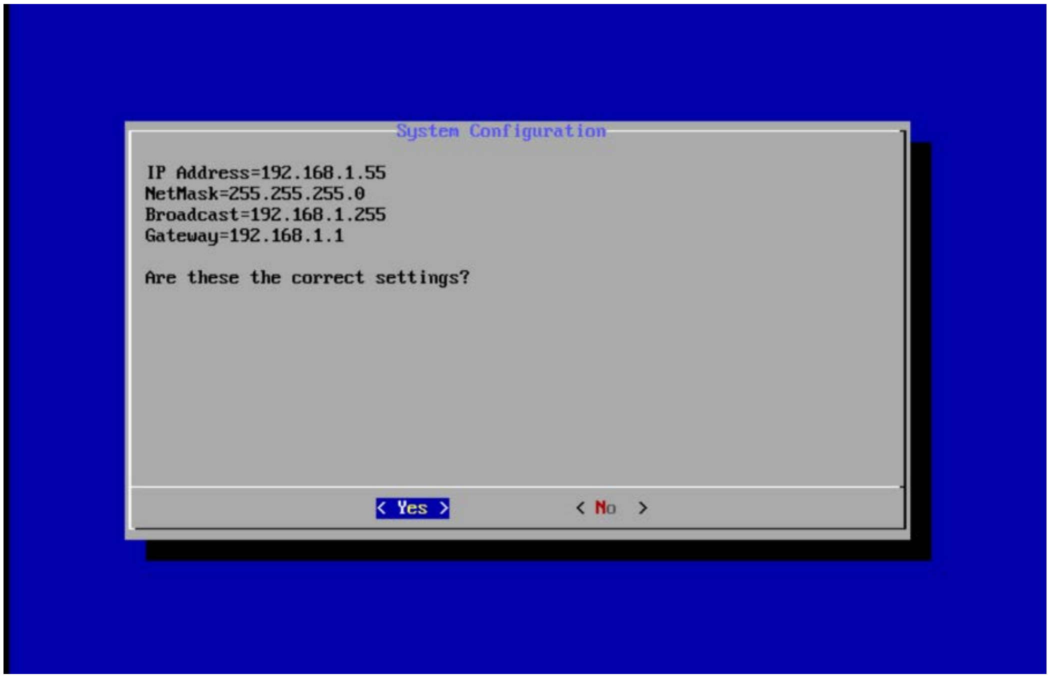
9. Press **Enter.**
10. Enter the network **gateway.**
11. Highlight **OK.**



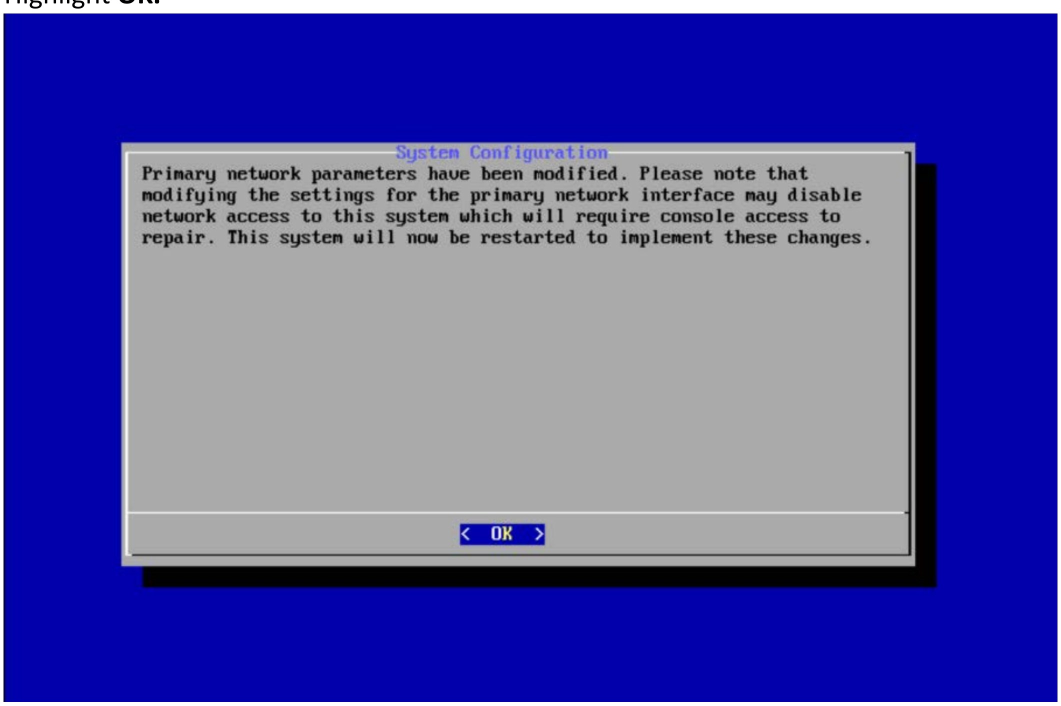
12. Press **Enter.**
13. Enter the network **broadcast address.**
14. Highlight **OK.**



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



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

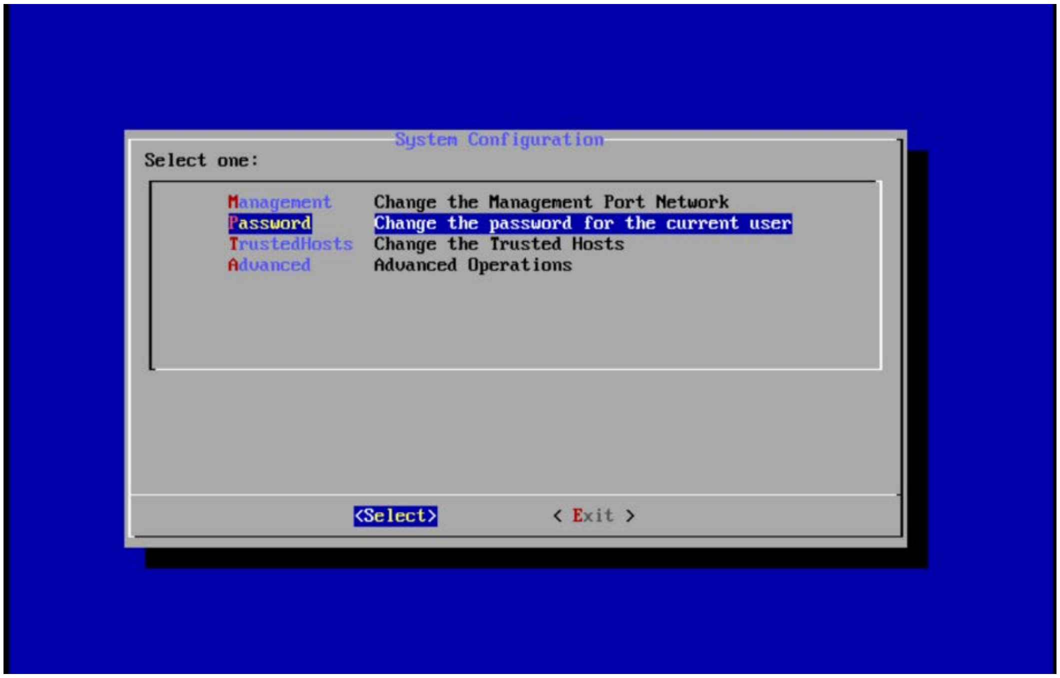


19. Press **Enter.**

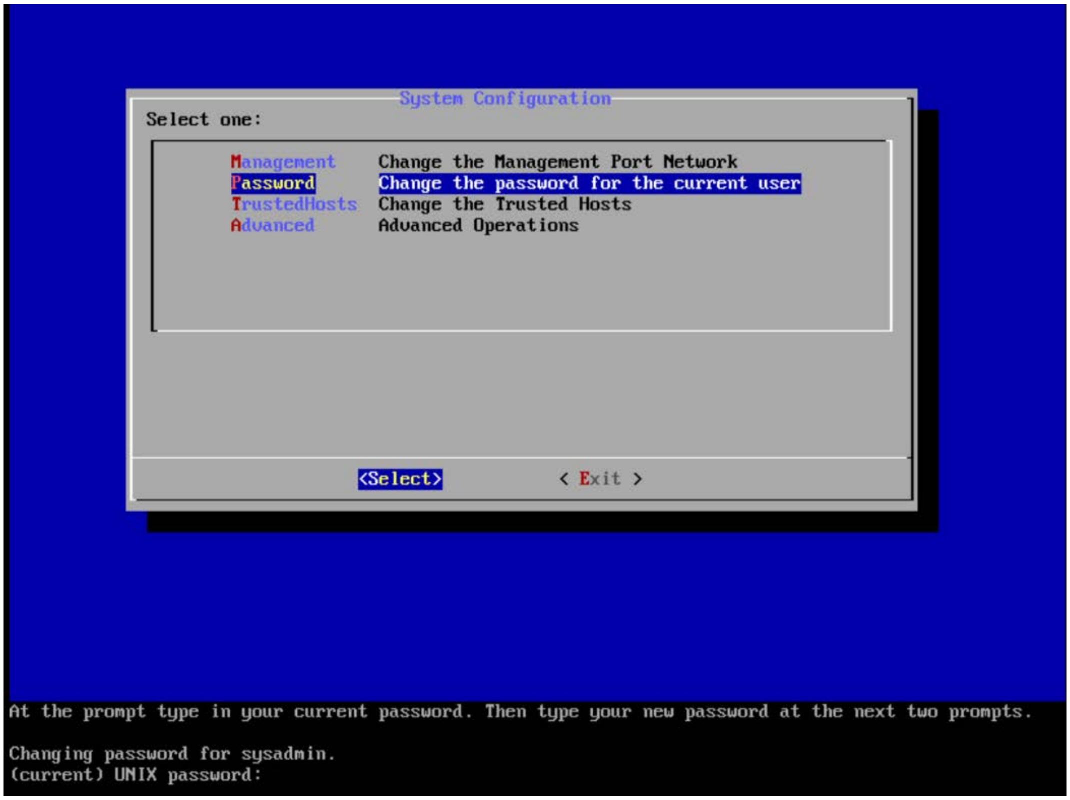
20. Repeat steps 1-19 for each of the **Stealthwatch Management Console, Stealthwatch UDP Director, Stealthwatch Flow Sensor,** and **Stealthwatch Flow Collector.**

2.13.2 Change Default Stealthwatch Console Passwords

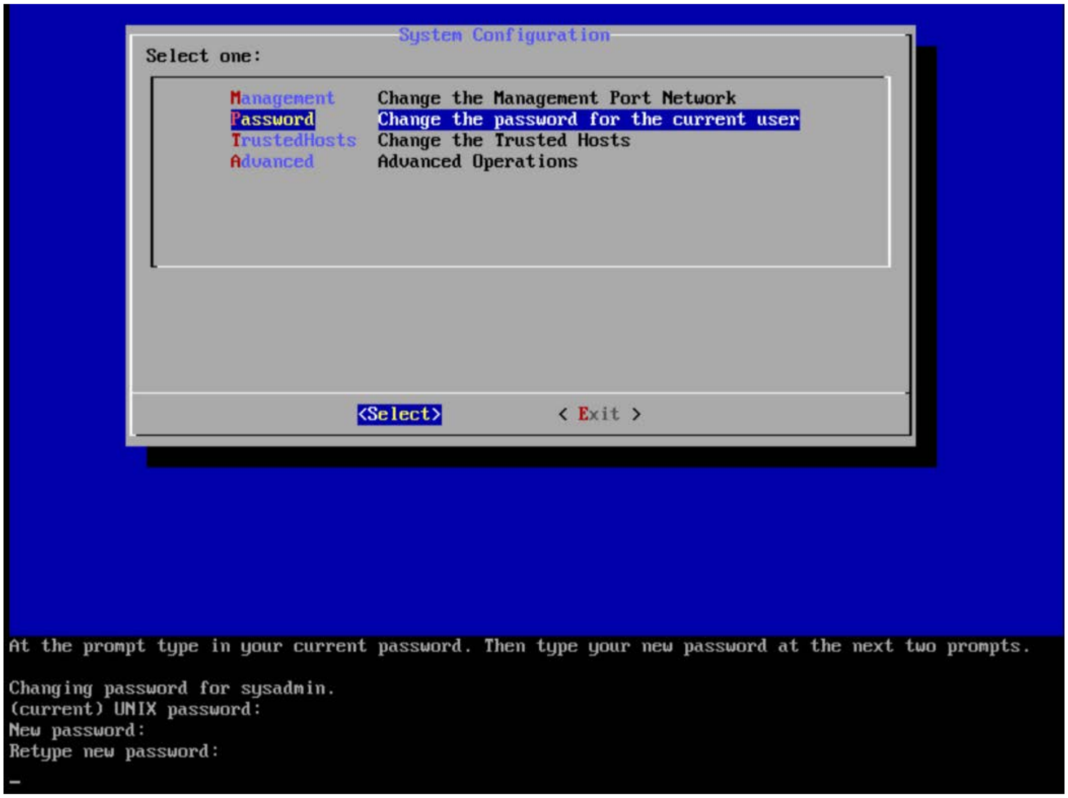
1. In the **System Configuration** menu, highlight **Password** and **Select.**



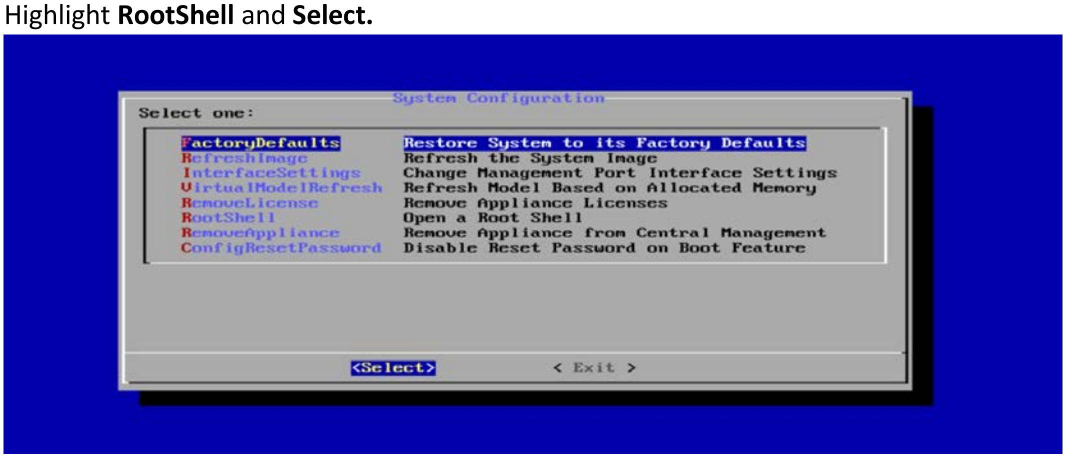
2. Press **Enter.**
3. Enter the original password.



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



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



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

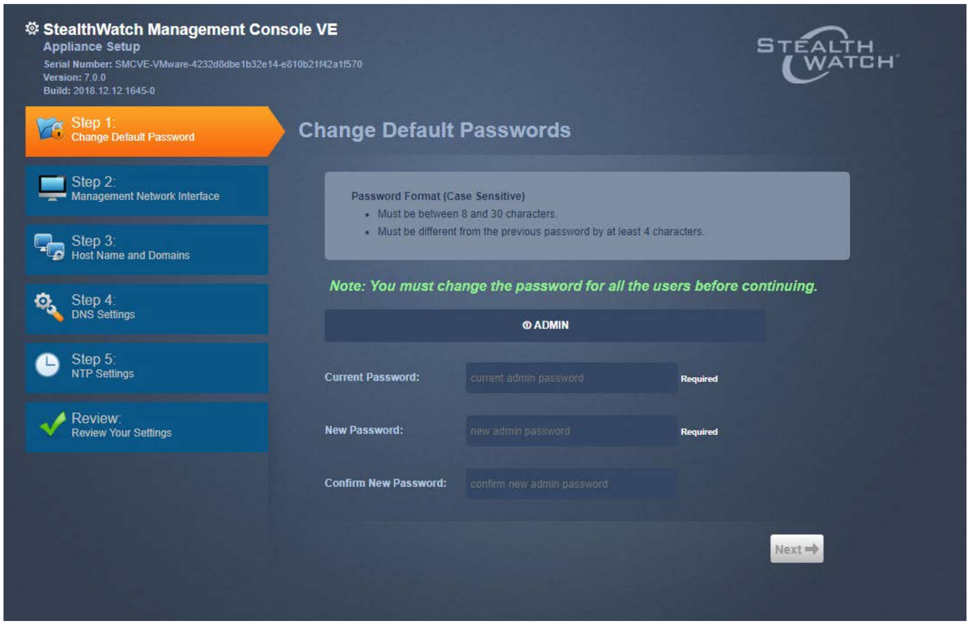
12. Enter the command **`root.`**
13. Type the new password, and confirm it.

.

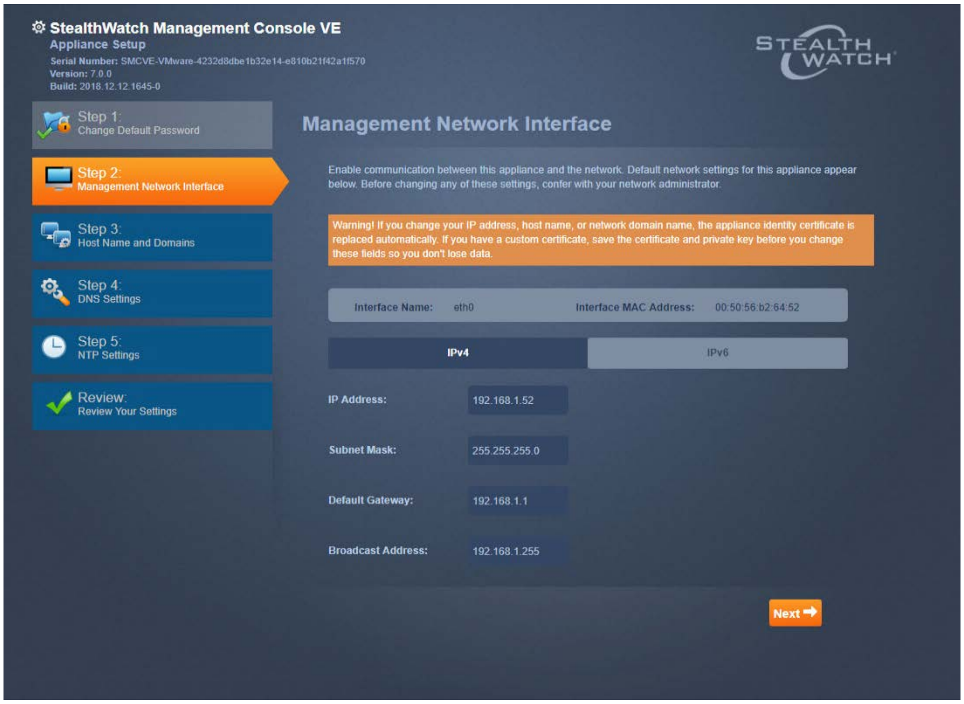
14. Press **Enter.**
15. Repeat steps 1-14 for each console.

2.13.3 Configure the Stealthwatch Management Console Web Interface

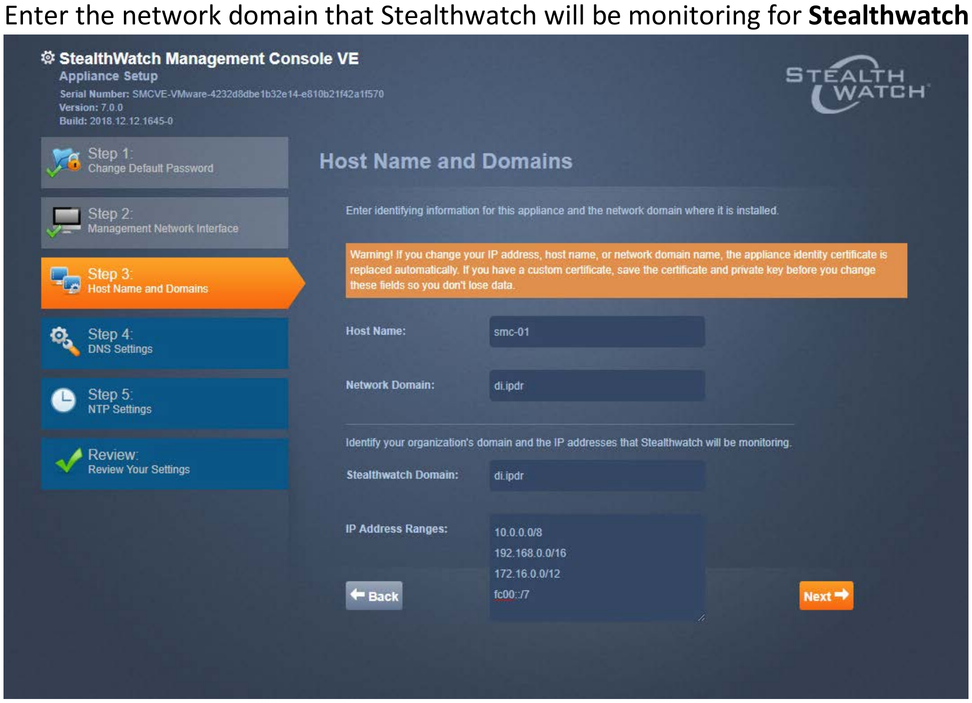
1. Change the default password by filling in the fields for **Current Password, New Password,** and **Confirm New Password.**



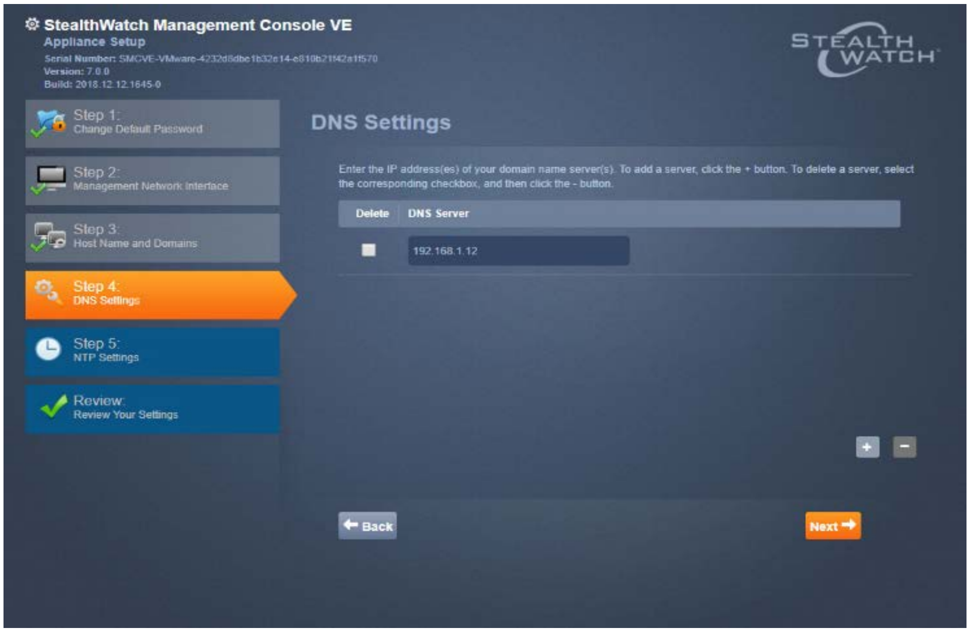
2. Click **Next.**
3. Fill in the fields for **IP Address, Subnet Mask, Default Gateway** and **Broadcast Address** according to your network topology.



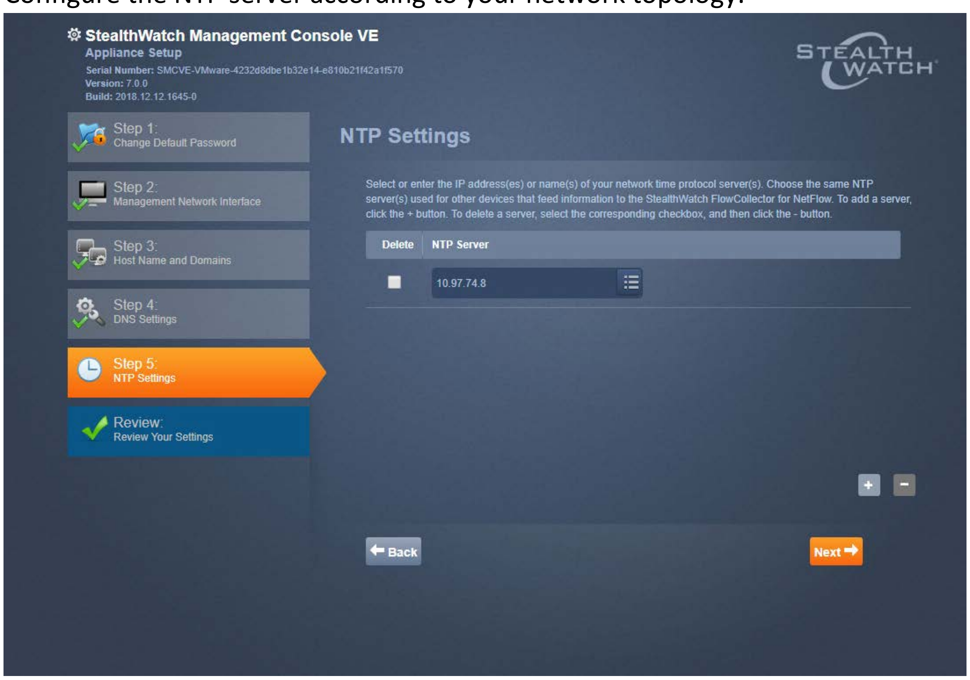
4. Click **Next.**
5. Enter a **host name.**
6. Enter the network domain that Stealthwatch is in for **Network Domain.**
7. Enter the network domain that Stealthwatch will be monitoring for **Stealthwatch Domain.**



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

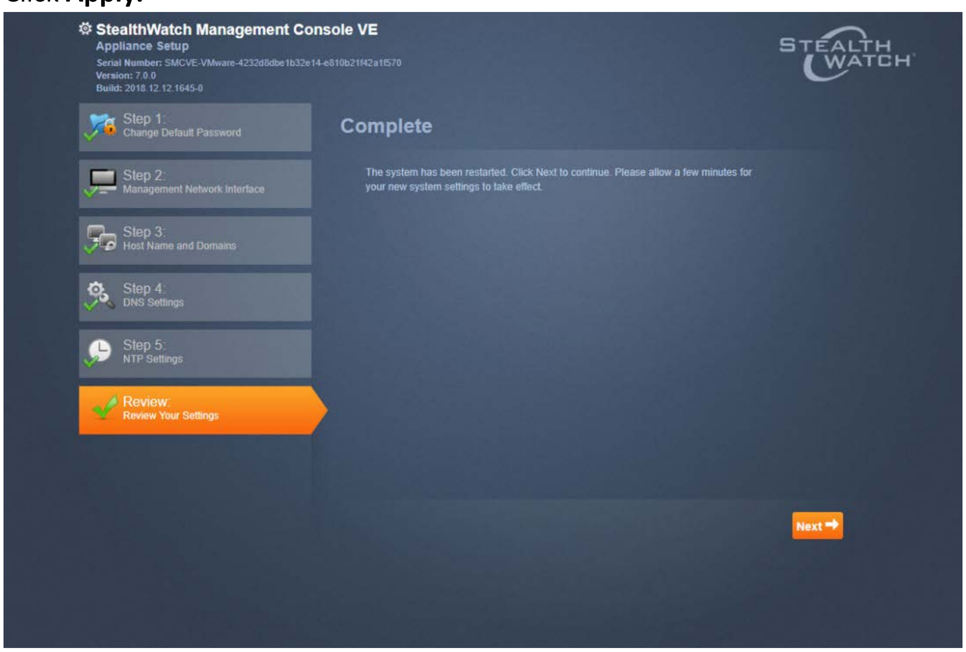


10. Click **Next.**
11. Configure the NTP server according to your network topology.



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

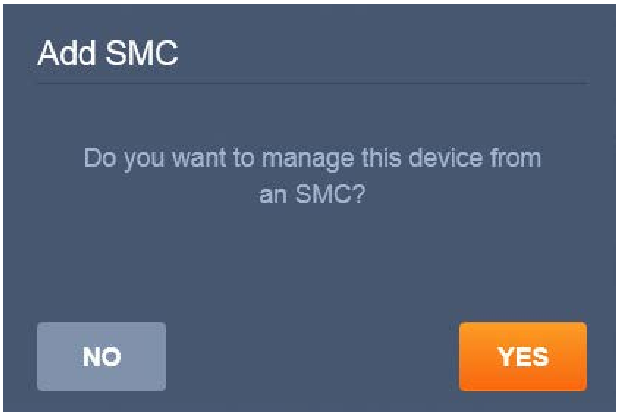
14. Click **Apply.**



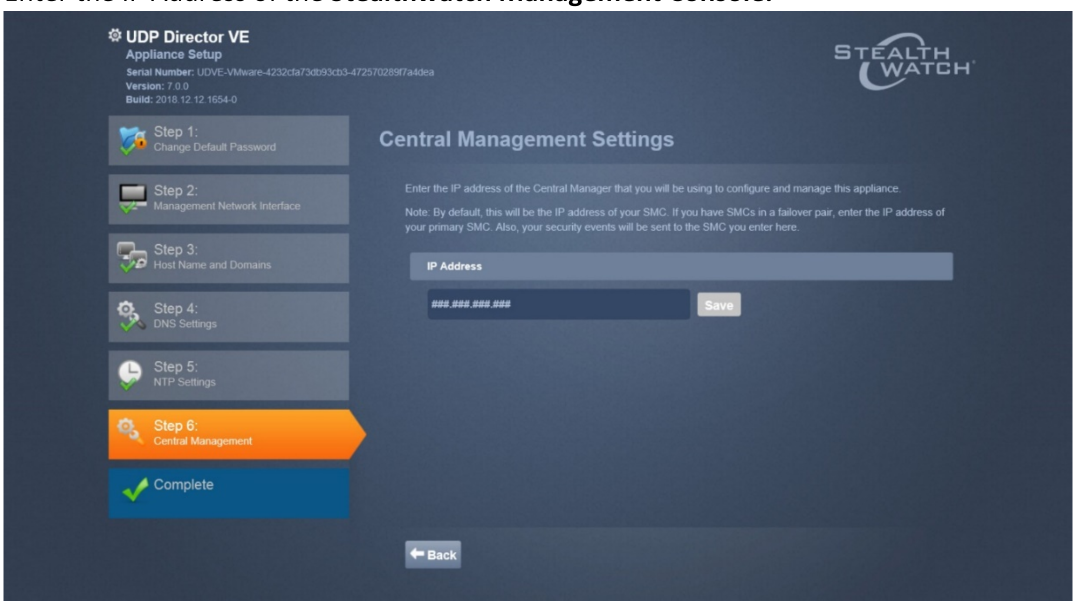
15. After the restart, click **Next.**

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

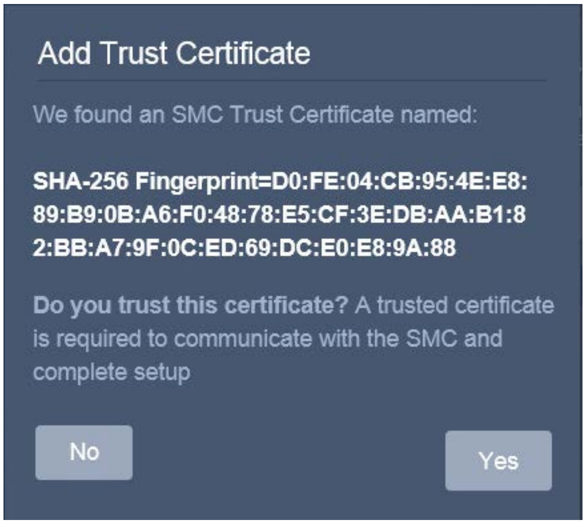
1. Repeat steps 1-12 from *Configure the Stealthwatch Management Console Web Interface.*



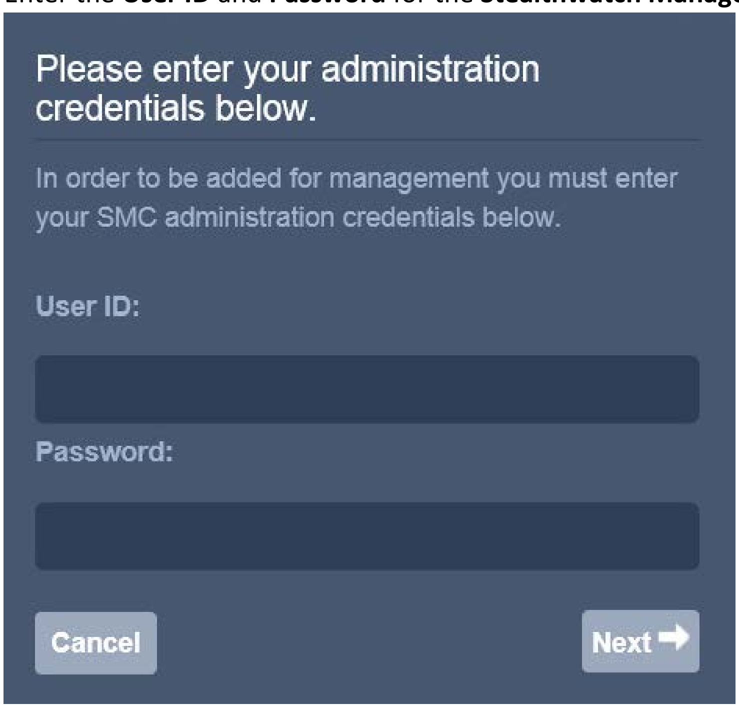
2. When prompted to manage this device from an SMC, click **Yes.**
3. Enter the IP Address of the **Stealthwatch Management Console.**



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



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



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

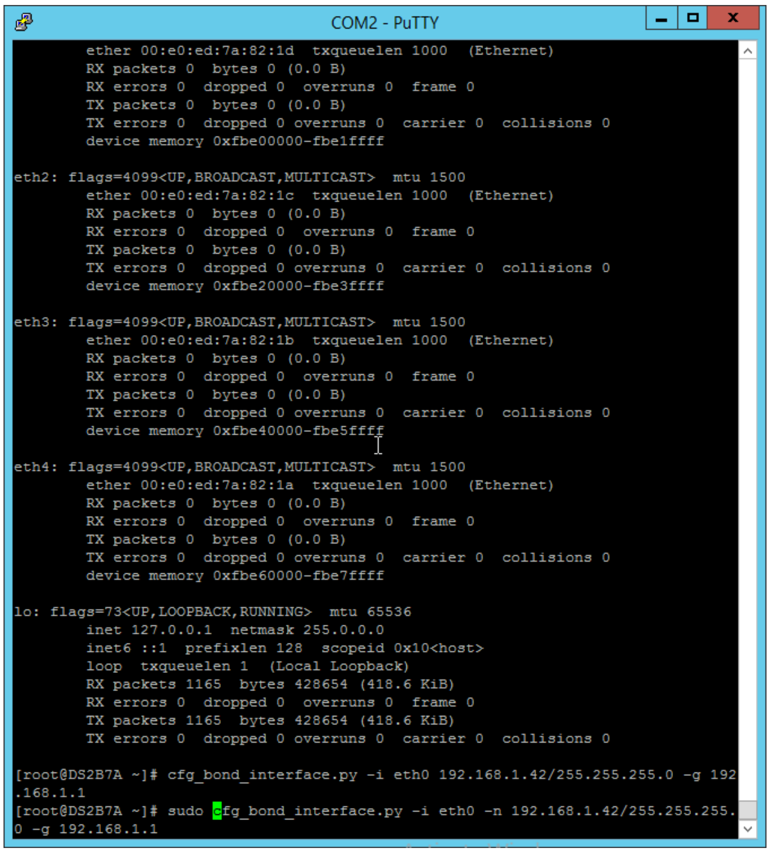
2.14 Symantec Analytics

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

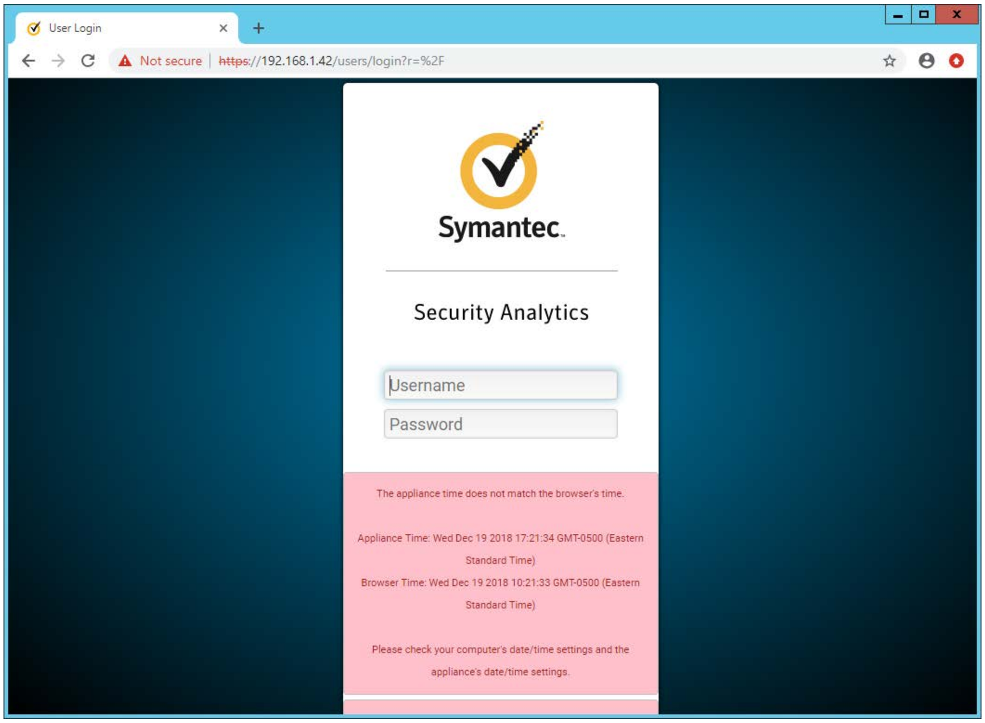
2.14.1 Initial Setup

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

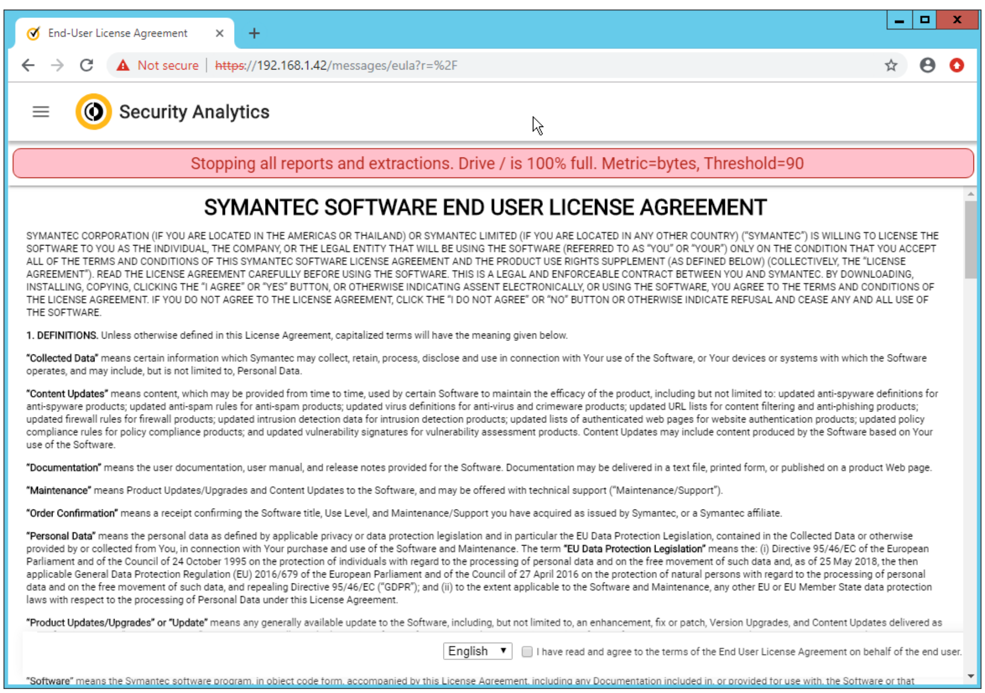
   `sudo cfg_bond_interface.py -i eth0 -n 192.168.1.42/255.255.255.0 -g 192.168.1.1`



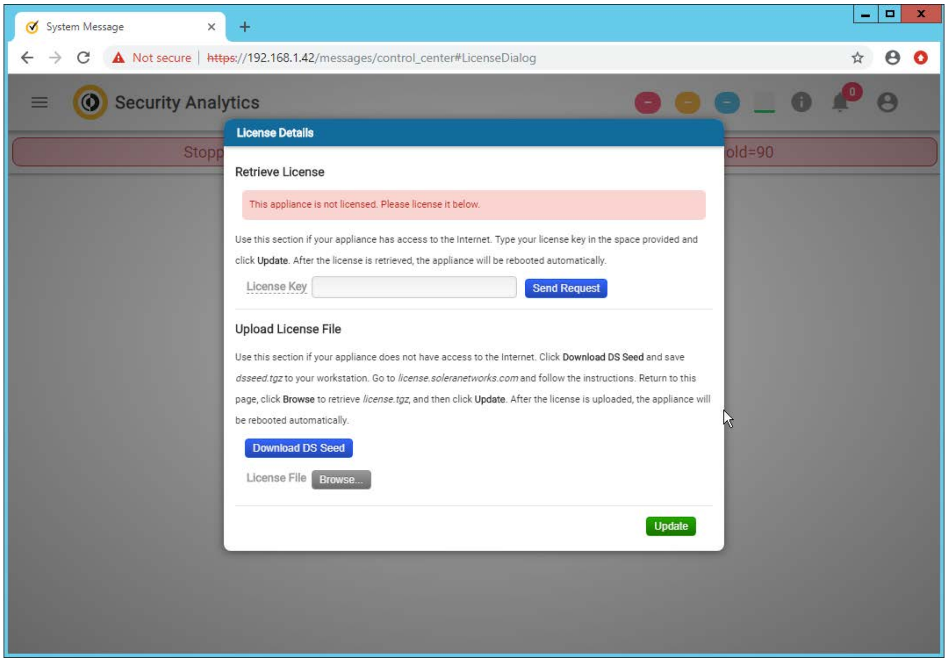
3. Navigate to the IP you assigned in a browser.



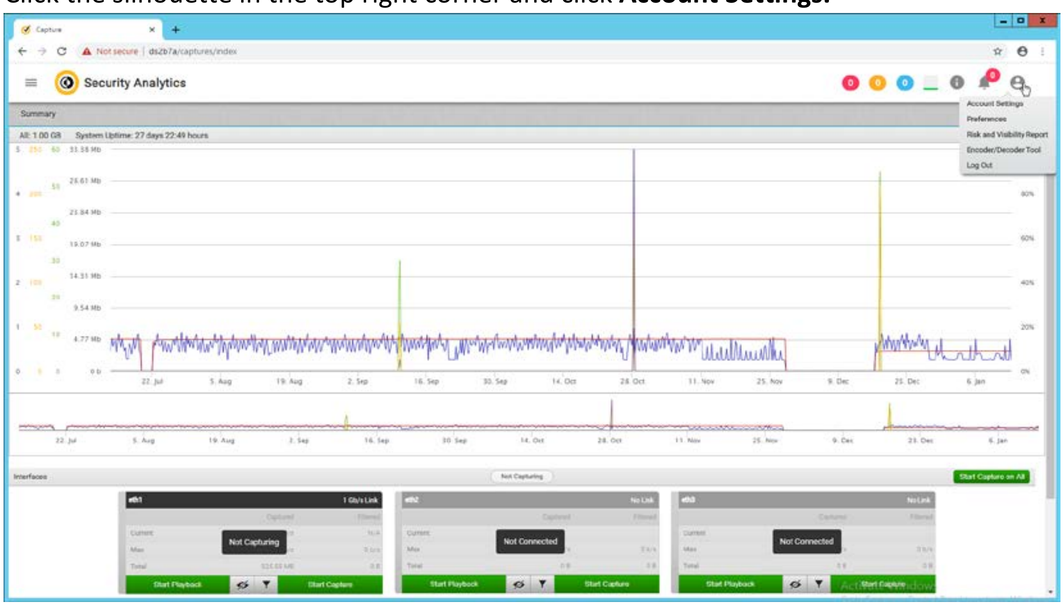
4. Enter the username and password to log in. The default is **(Admin/Solera).**
5. Check the box next to **I have read and agreed to the terms of the End User License Agreement on behalf of the end user.**



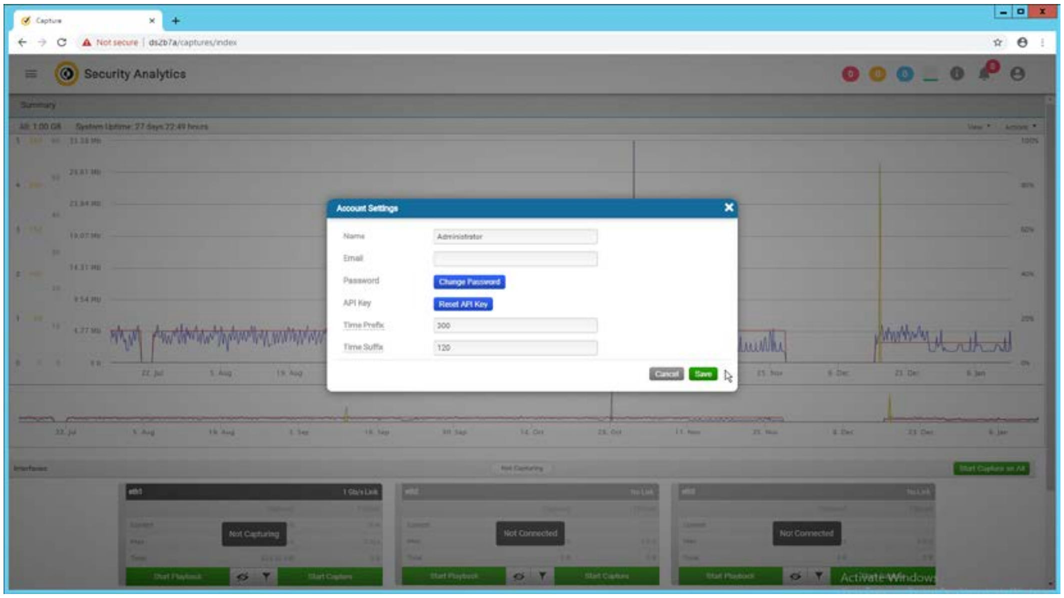
6. Click **Next.**
7. Enter the license key.
8. If you do not have internet connectivity, follow the instructions under **Upload License File.** Otherwise, click **Send Request.**



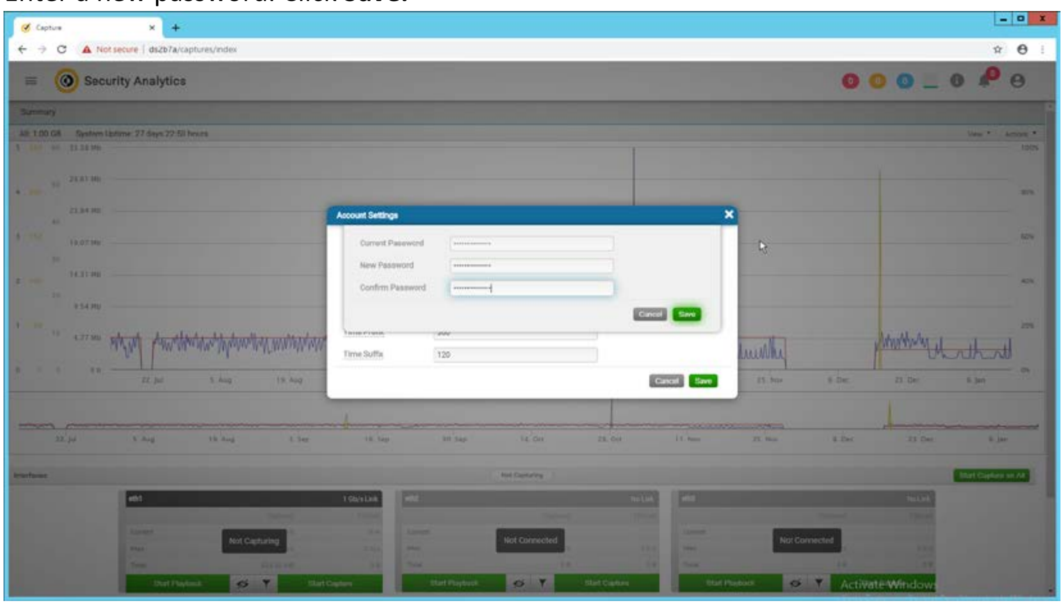
9. Click **Update.** The device will reboot.
10. Log in to the web page again.
11. Click the silhouette in the top right corner and click **Account Settings.**



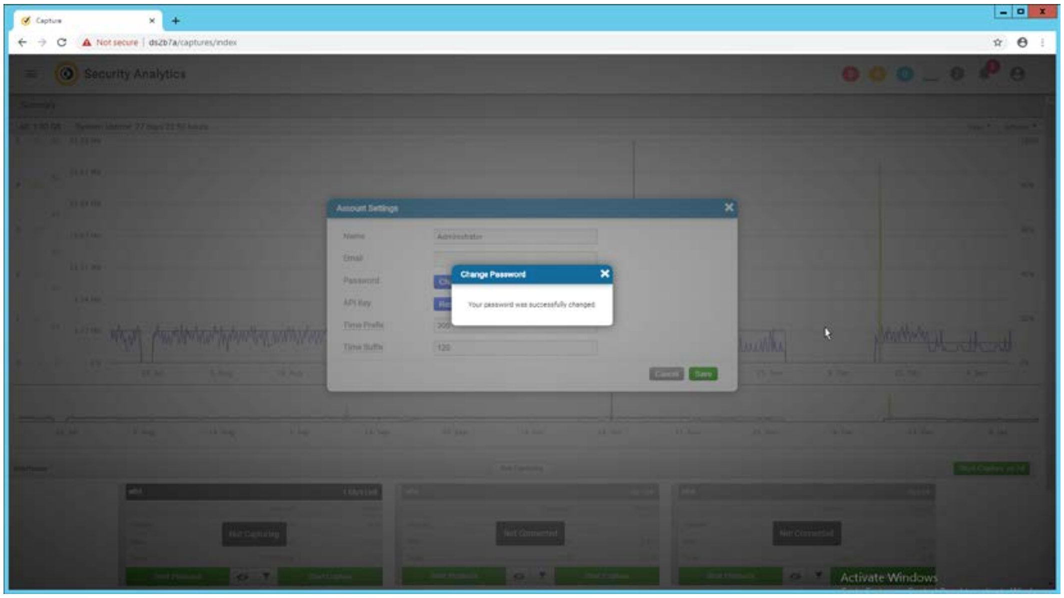
12. Click **Change Password.**



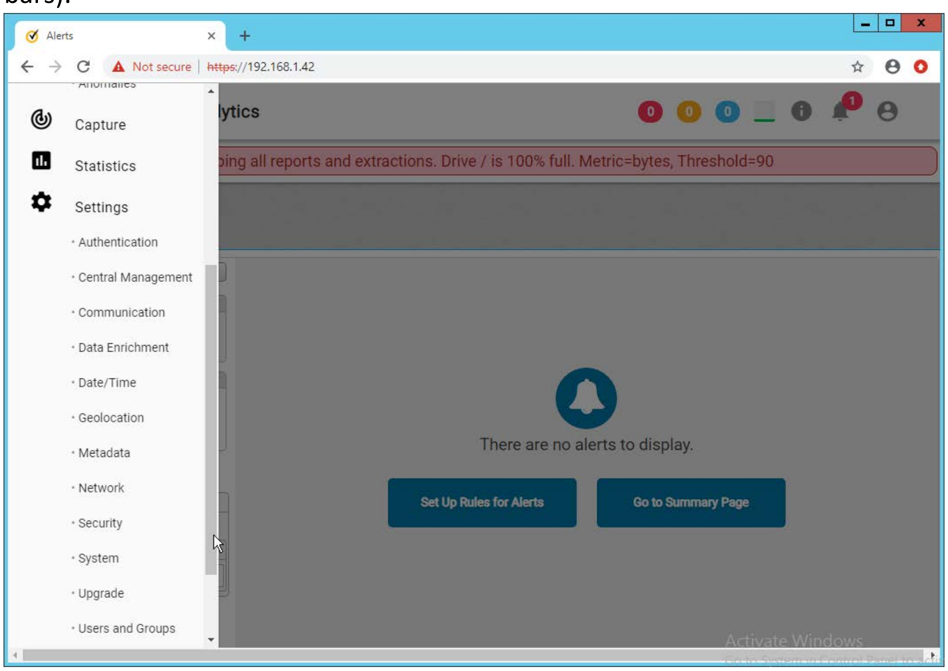
13. Enter a new password. Click **Save.**



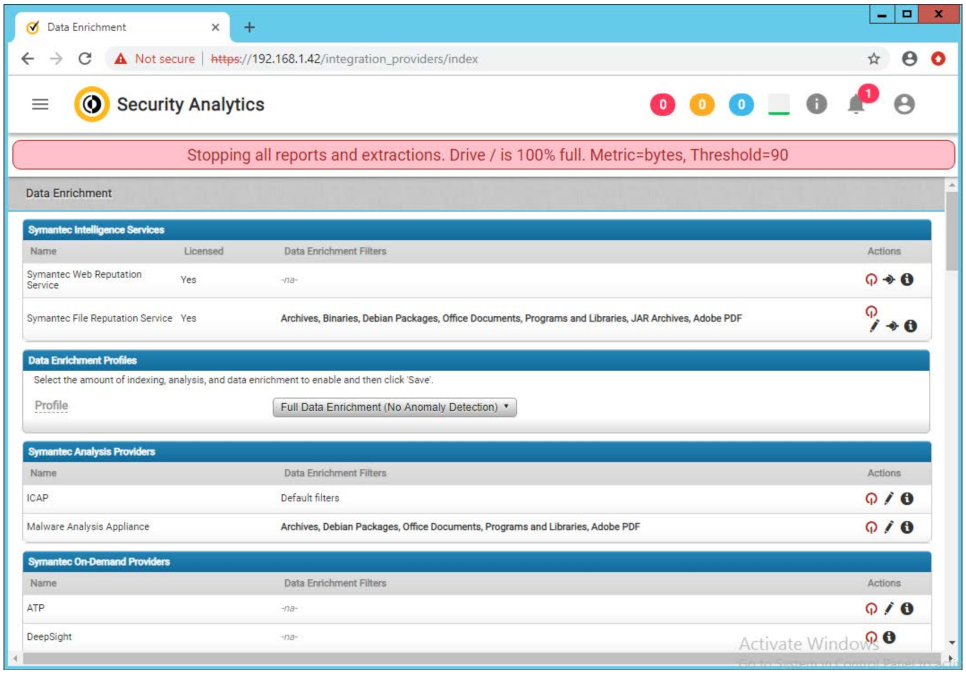
14. The screen should reflect that the password has been changed. Close out of both windows and return to the main web console.



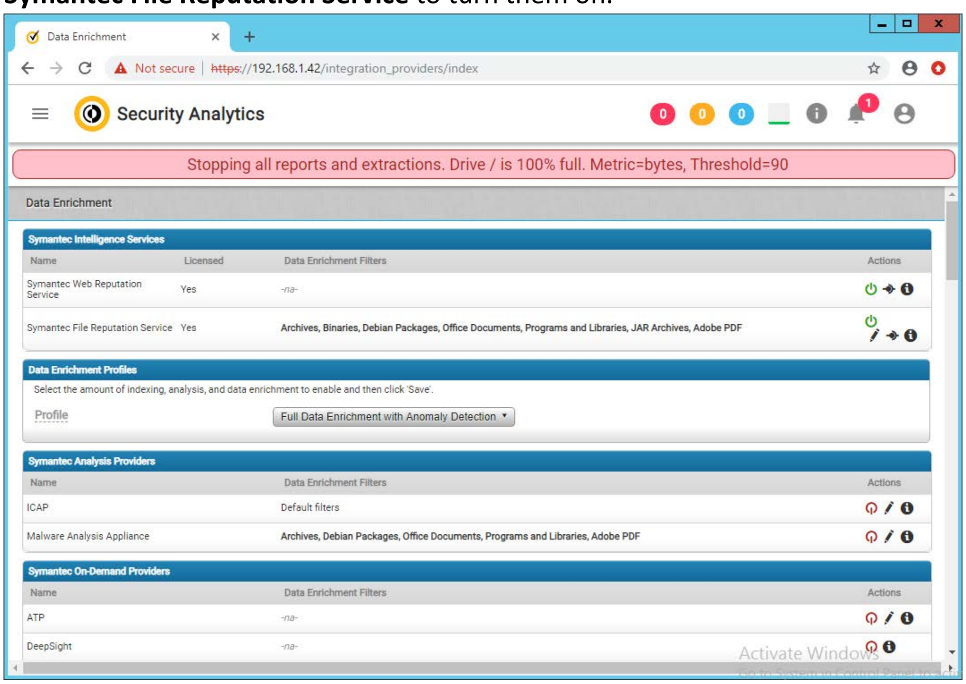
15. In the top left corner of the web console, click the menu button. (It shows as three horizontal bars).



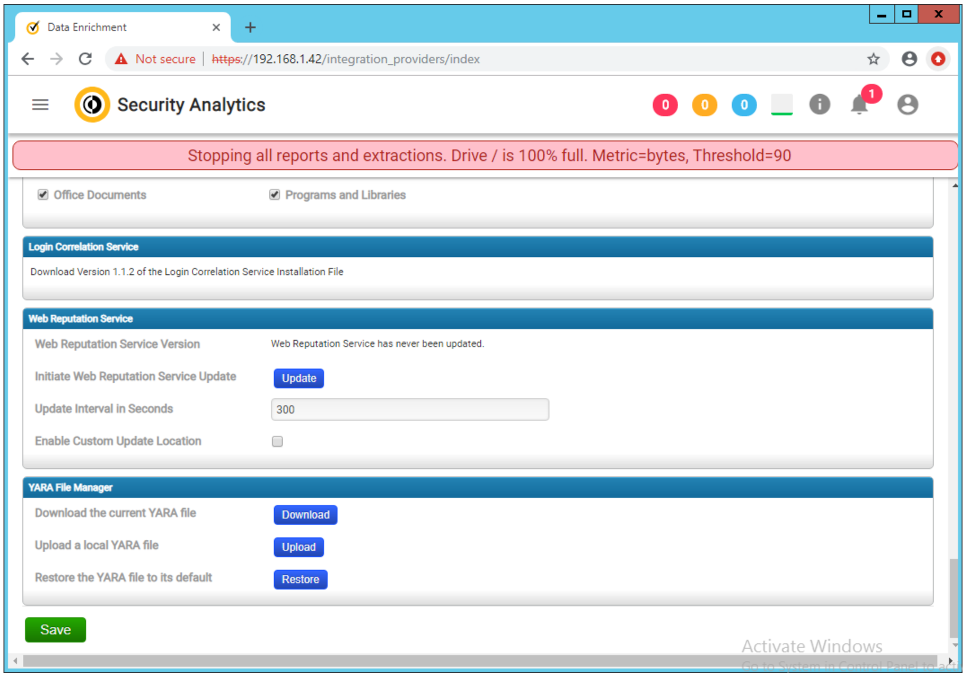
16. Navigate to **Settings > Data Enrichment.**



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



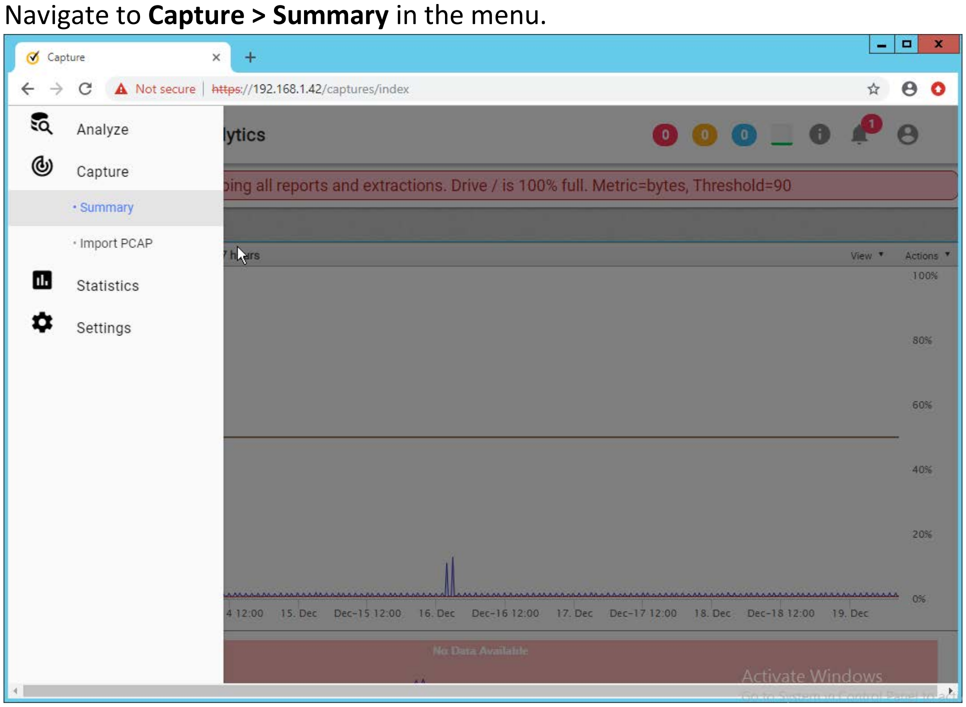
18. Select **Full Data Enrichment (with Anomaly Protection)** for the profile under **Data Enrichment Profiles.**



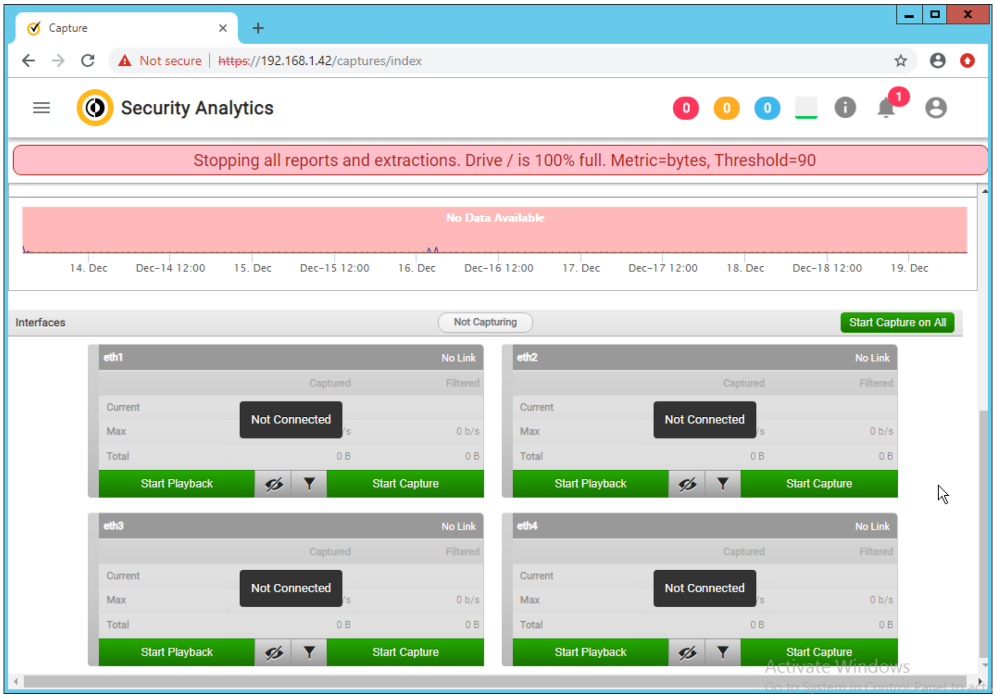
19. Click **Save.**

2.14.2 Capturing Data

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



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

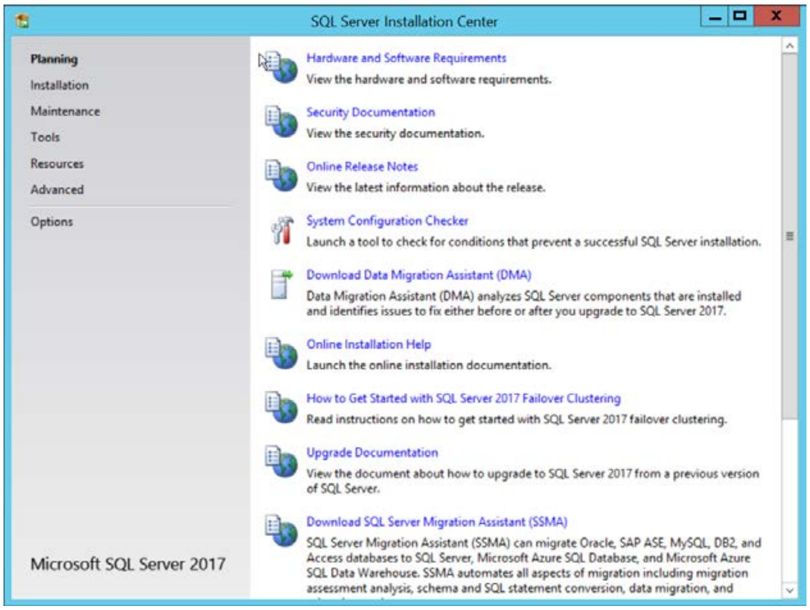


2.15 Symantec Information Centric Analytics

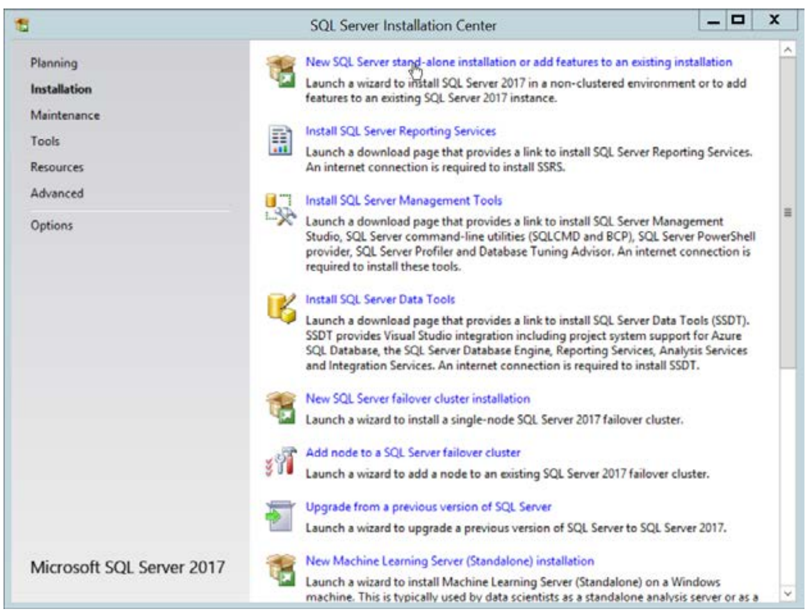
This section describes the installation and configuration of Symantec Information Centric Analytics (ICA).

2.15.1 Installing MS SQL 2017

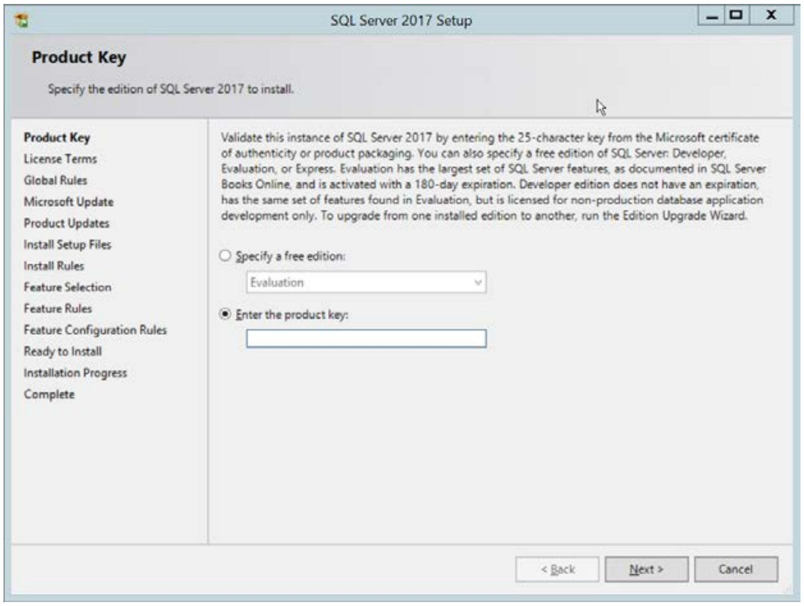
1. Launch the SQL Setup Wizard.



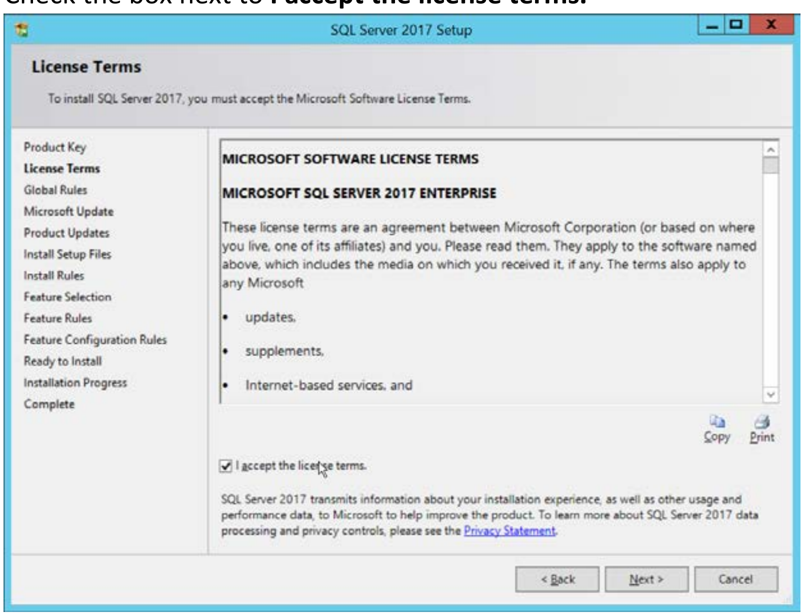
2. Click **Installation.**



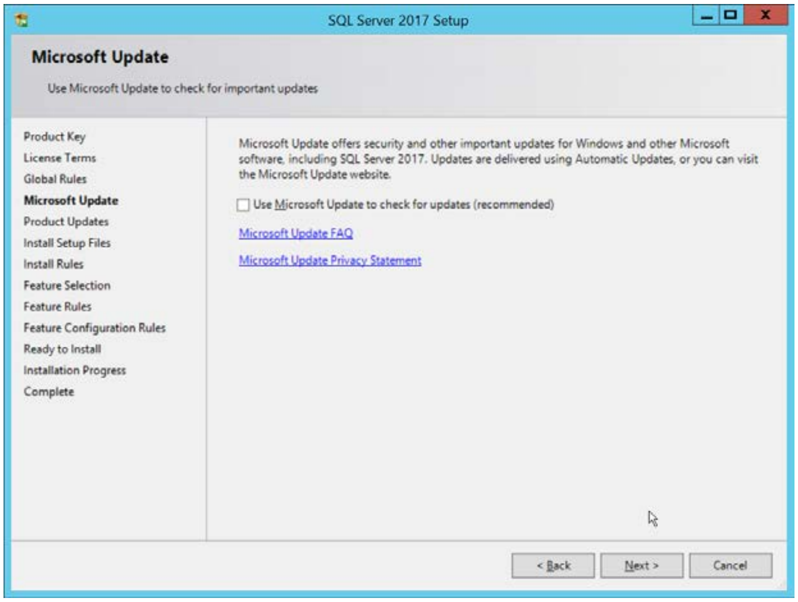
3. Click **New SQL Server stand-alone installation or add features to an existing installation.**
4. Enter a **product key.**



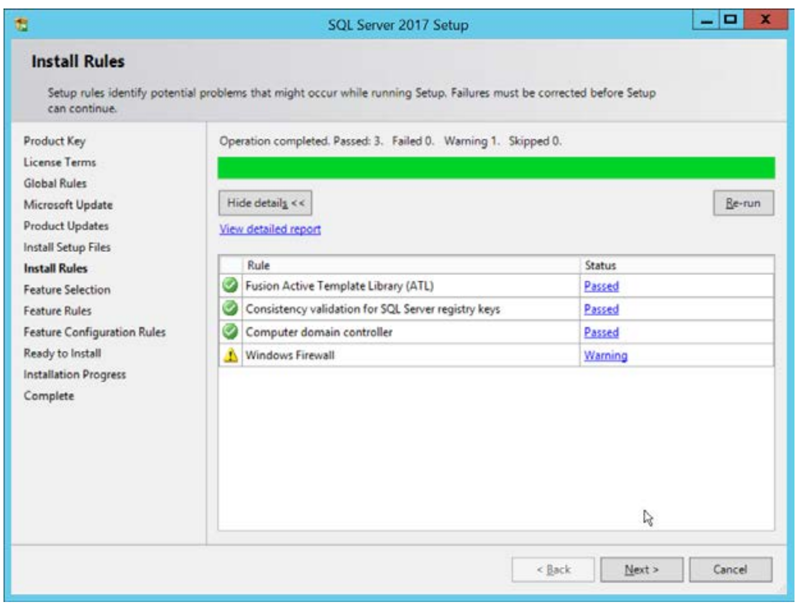
5. Click **Next.**
6. Check the box next to **I accept the license terms.**



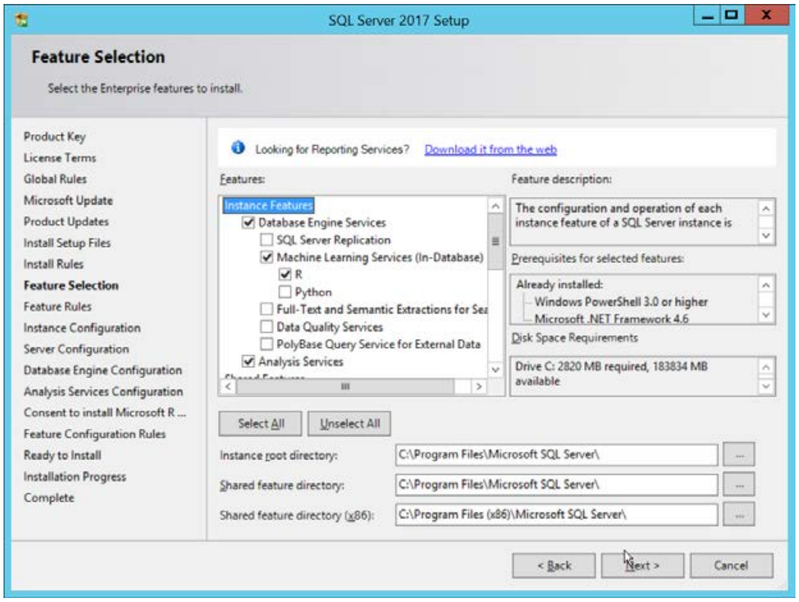
7. Click **Next.**



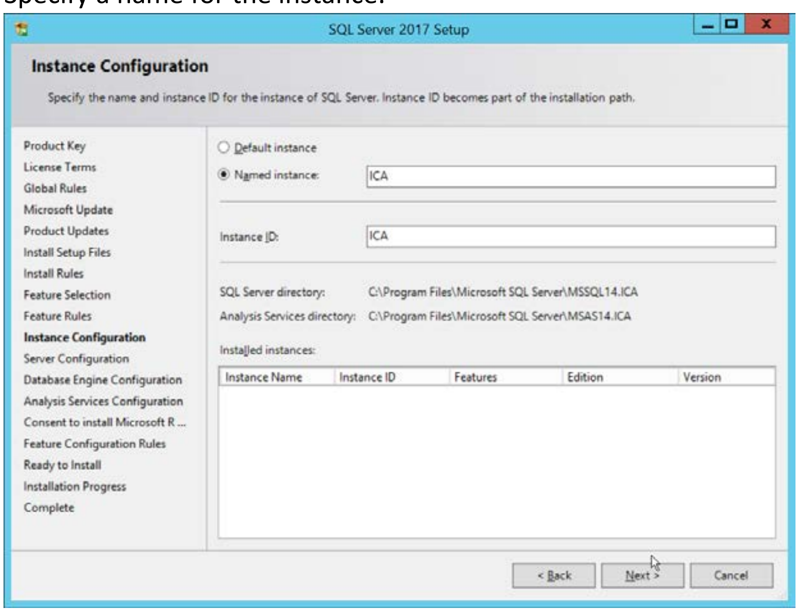
8. Click **Next.**



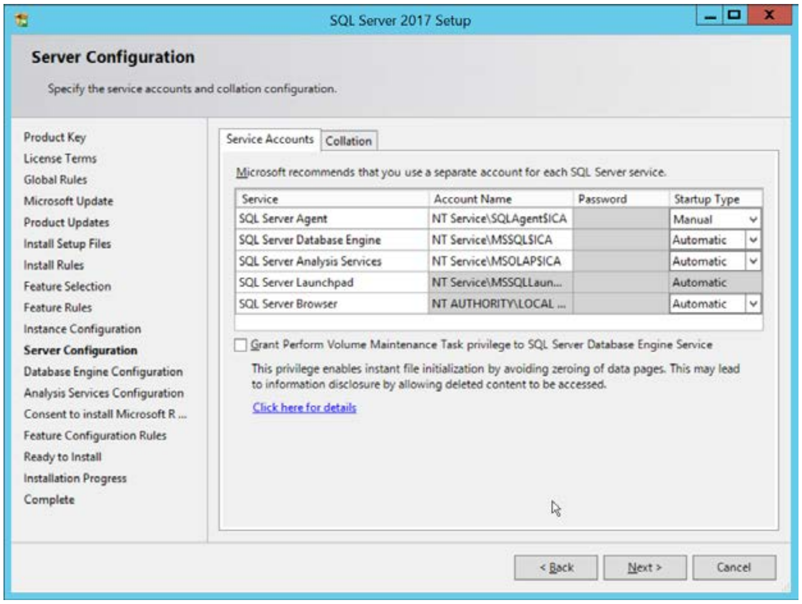
9. Click **Next.**
10. Ensure that box next to **R** and the box next to **Analysis Services** is checked.



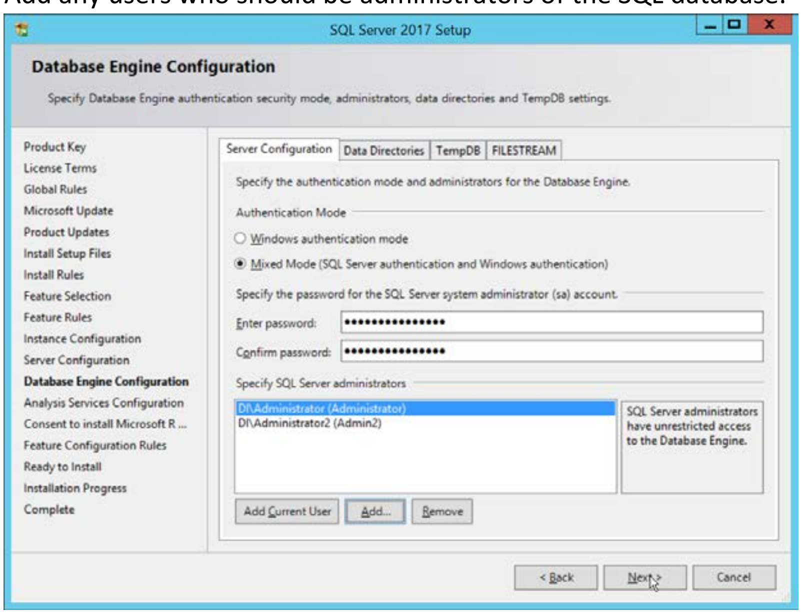
11. Click **Next.**
12. Select **Named instance.**
13. Specify a name for the instance.



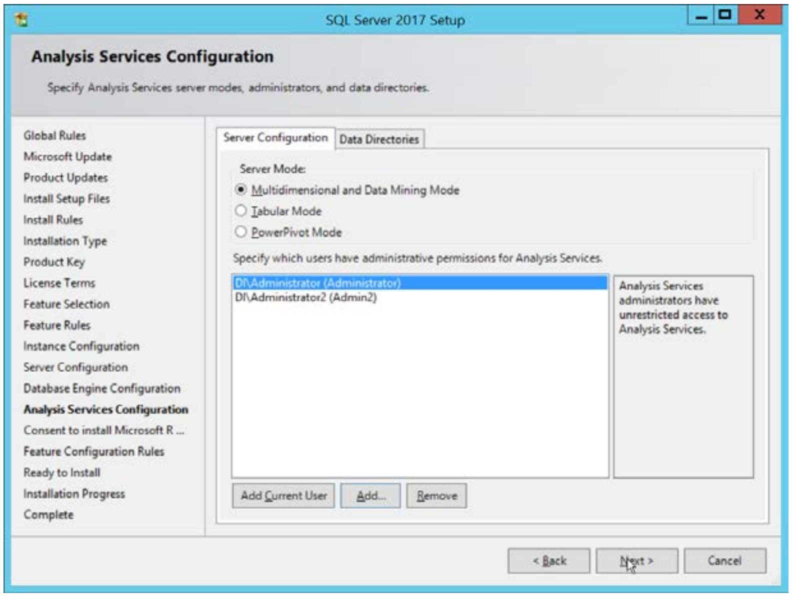
14. Click **Next.**



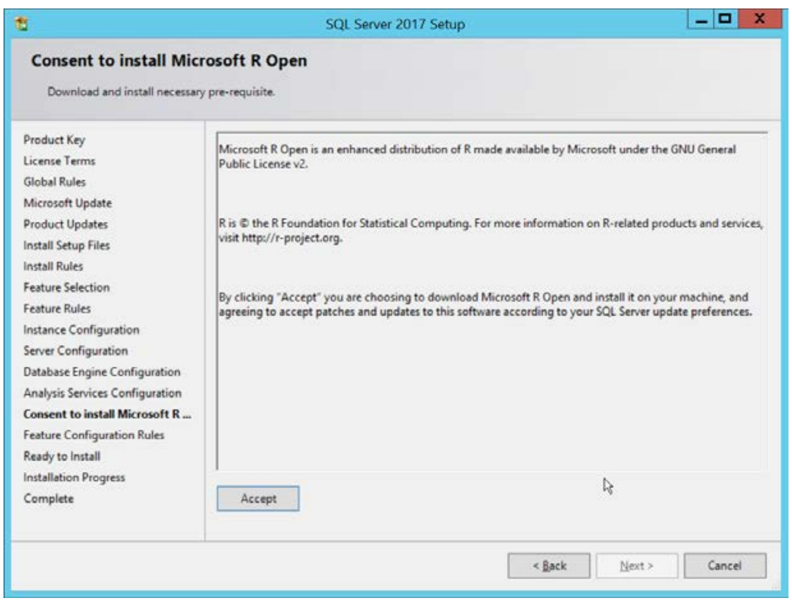
15. Click **Next.**
16. Select **Mixed Mode (SQL Server authentication and Windows authentication).**
17. Enter a **password.**
18. Add any users who should be administrators of the SQL database.



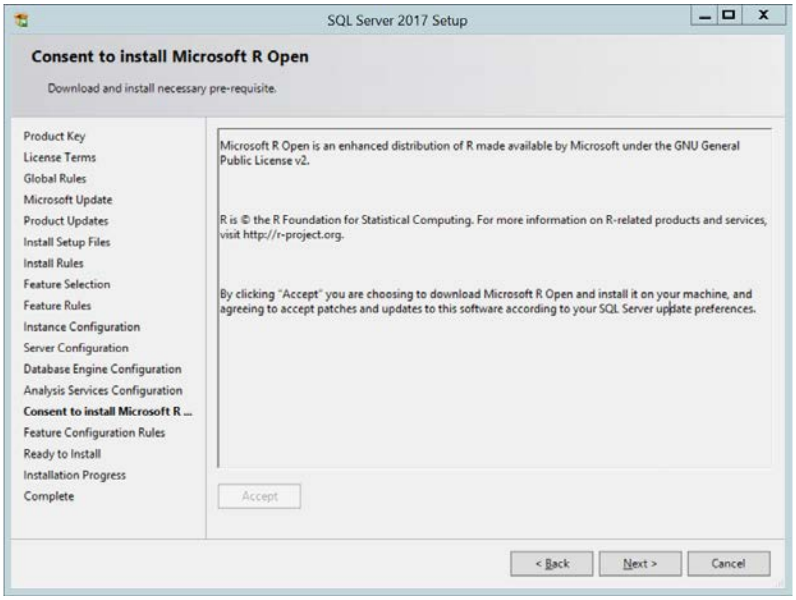
19. Click **Next.**
20. Select **Multidimensional and Data Mining Mode.**
21. Add any users who should be administrators of the Analysis Services.



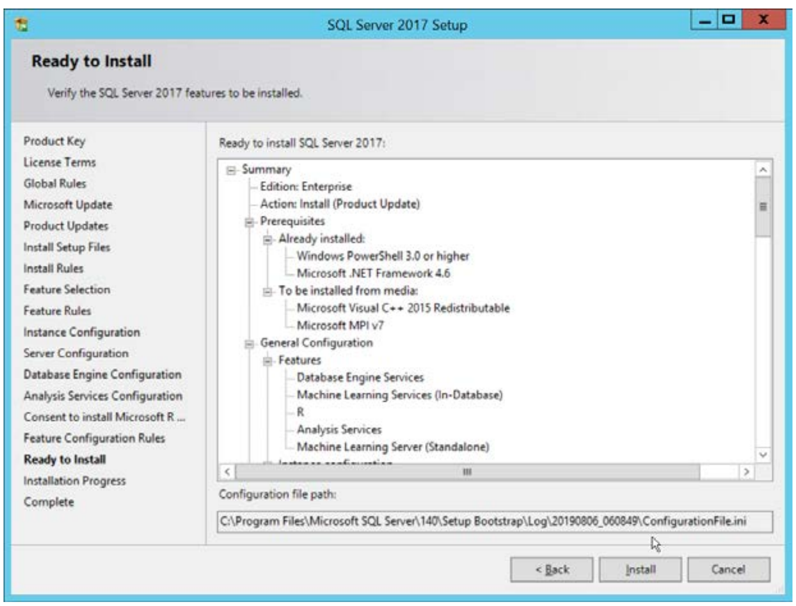
22. Click **Next.**



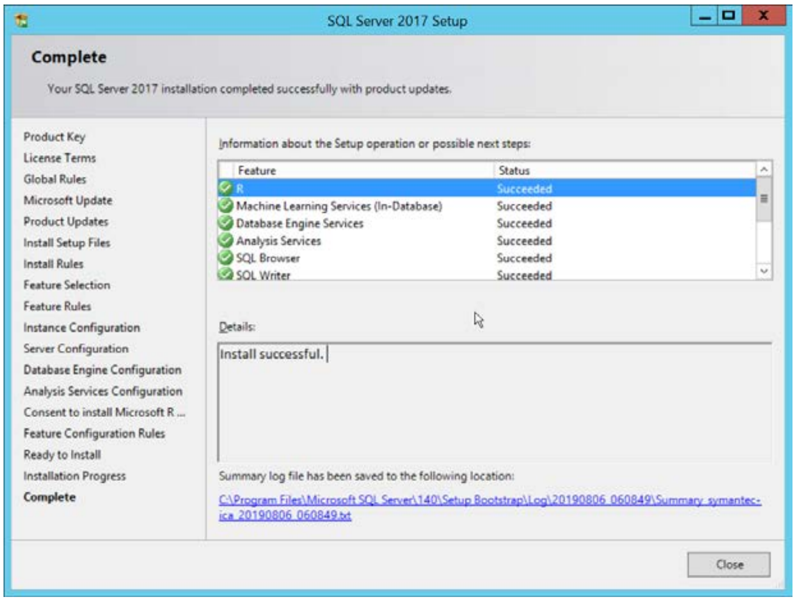
23. Click **Accept.**



24. Click **Next.**



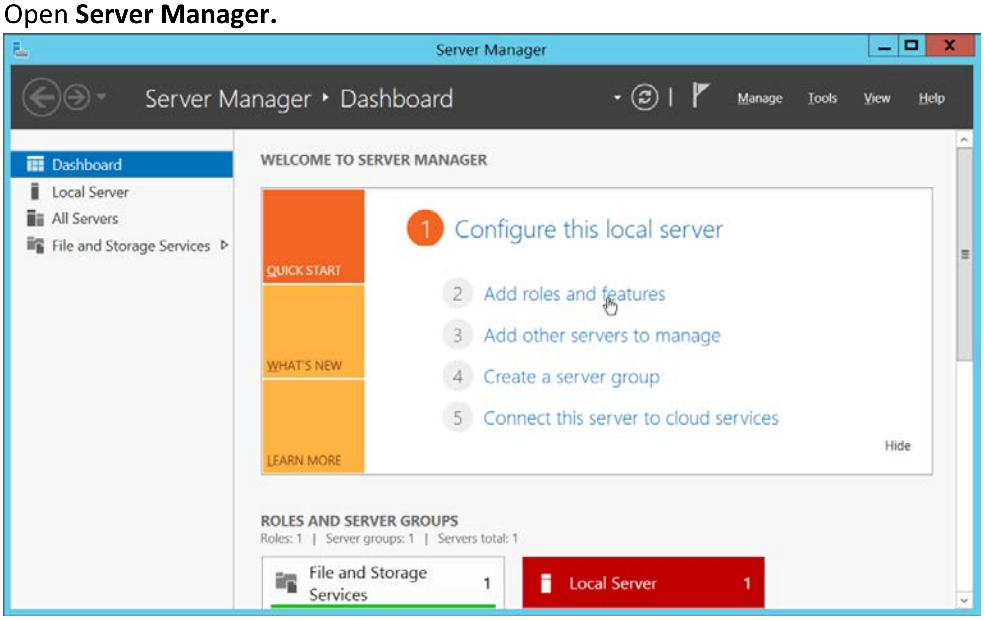
25. Click **Install.**



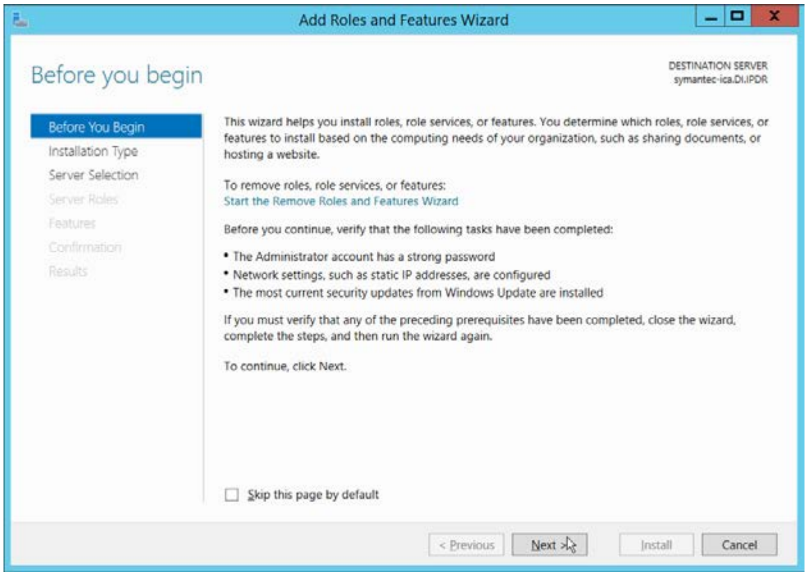
26. Click **Close.**

2.15.2 Install Windows Services

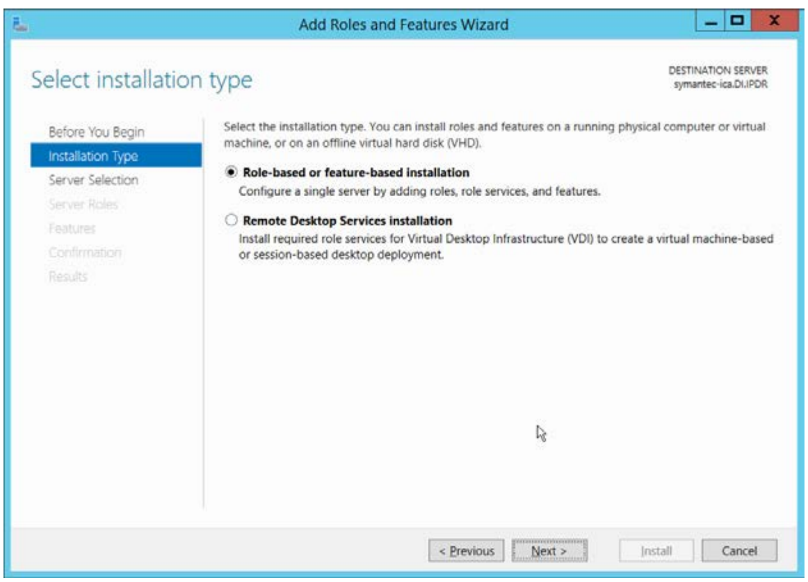
1. Open **Server Manager.**



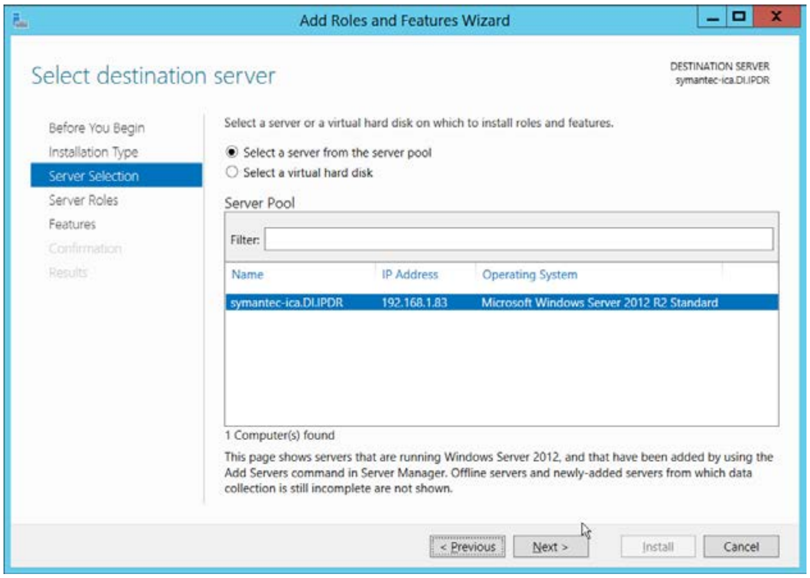
2. Click **Add Roles and Features.**



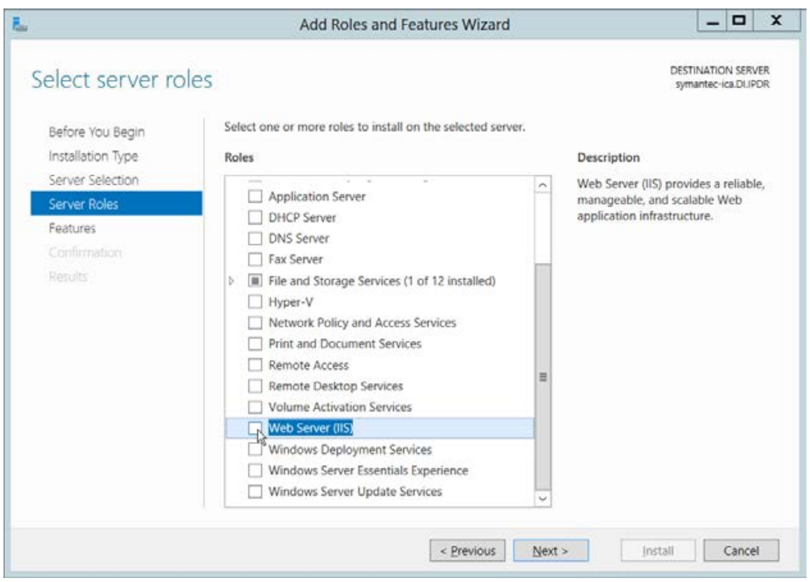
3. Click **Next.**



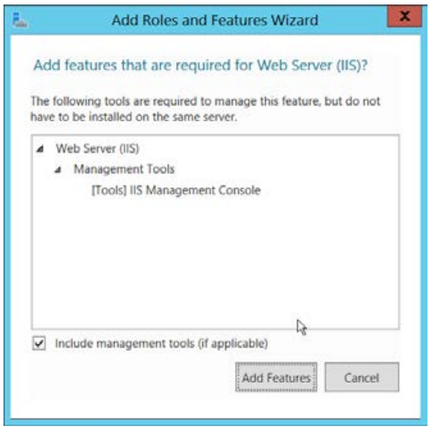
4. Click **Next.**



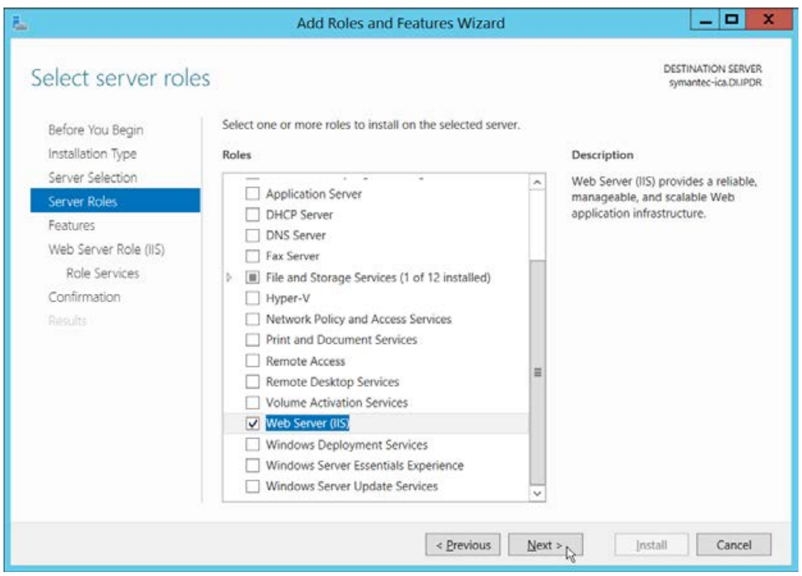
5. Click **Next.**



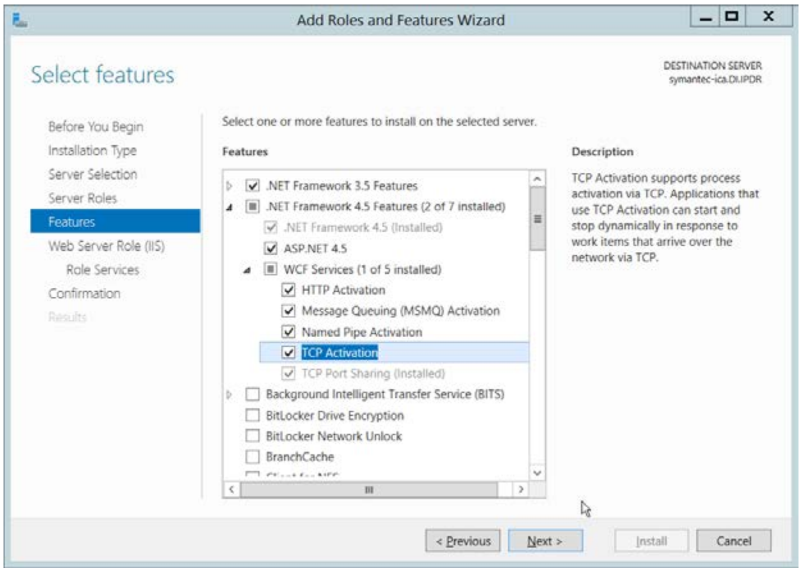
6. Select **Web Server (IIS).**



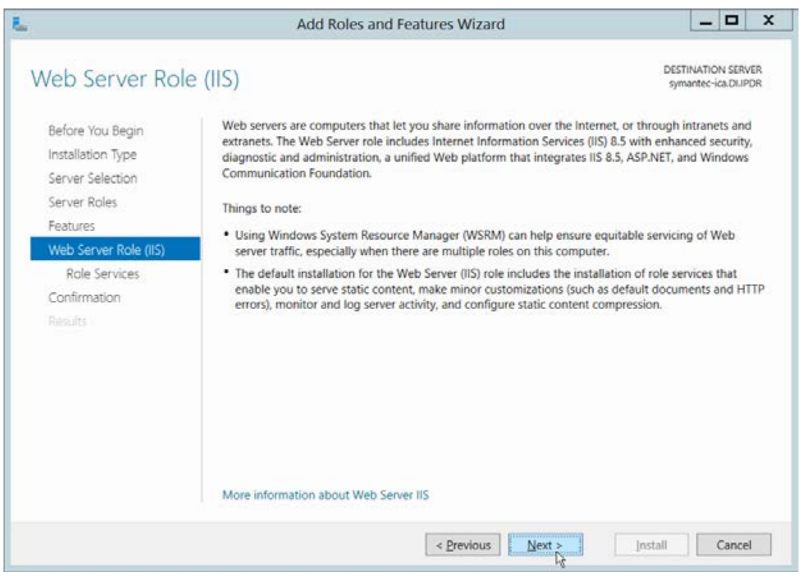
7. Click **Add Features.**



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



11. Click **Next.**



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

            i. **Static Content Compression**

      d. **Security**

            i. **Windows Authentication**

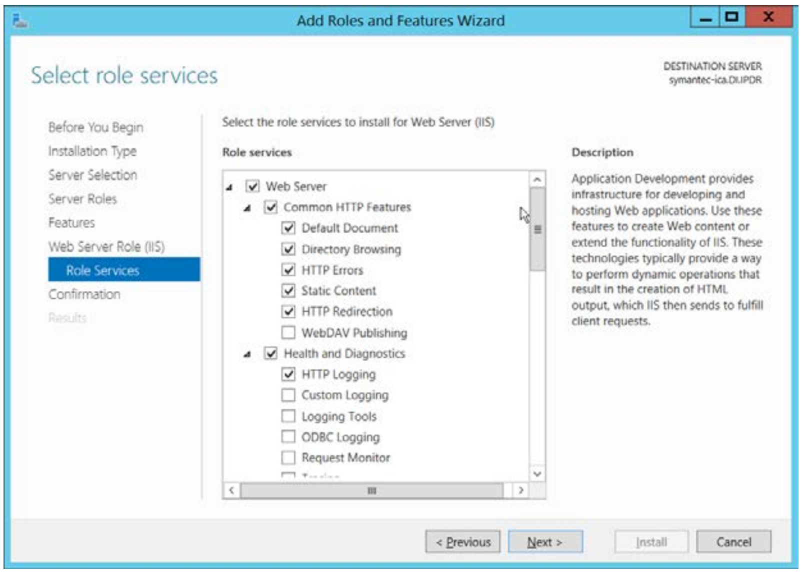
      e. **Application Development**

            i. **.NET Extensibility 4.5**

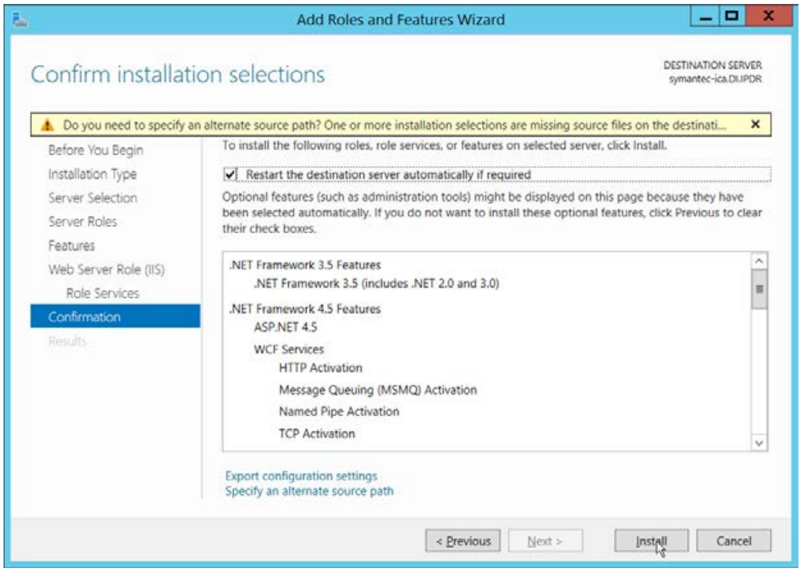
            ii. **ASP.NET 4.5**

            iii. **ISAPI Extensions**

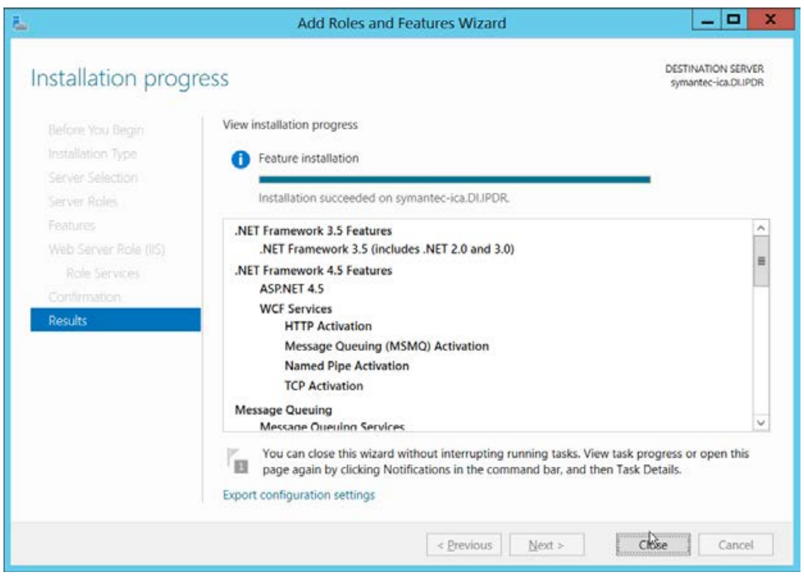
            iv. **ISAPI Filters**



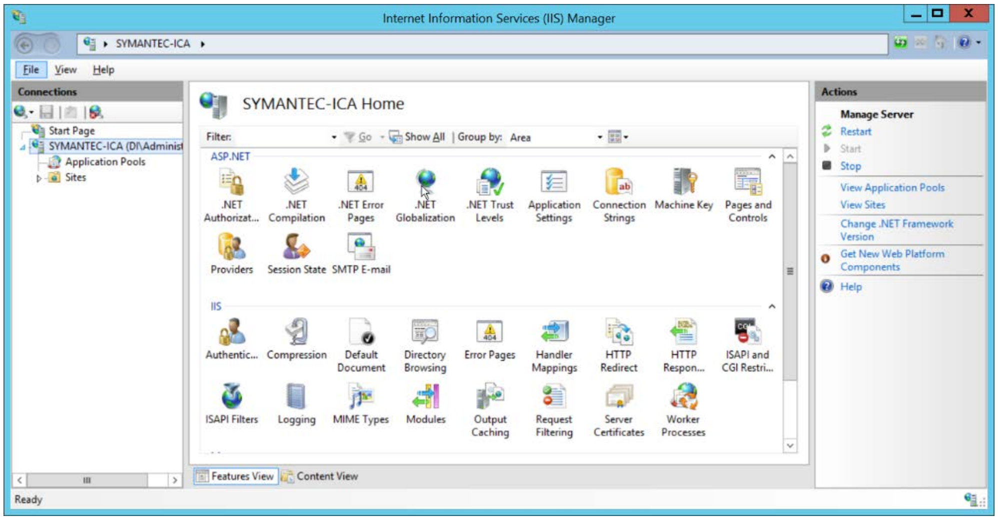
14. Click **Next.**
15. If necessary, specify a path to **/Sources/SxS,** which is found in the Windows Installation Media.
16. Check the box next to **Restart the destination server automatically if required.**



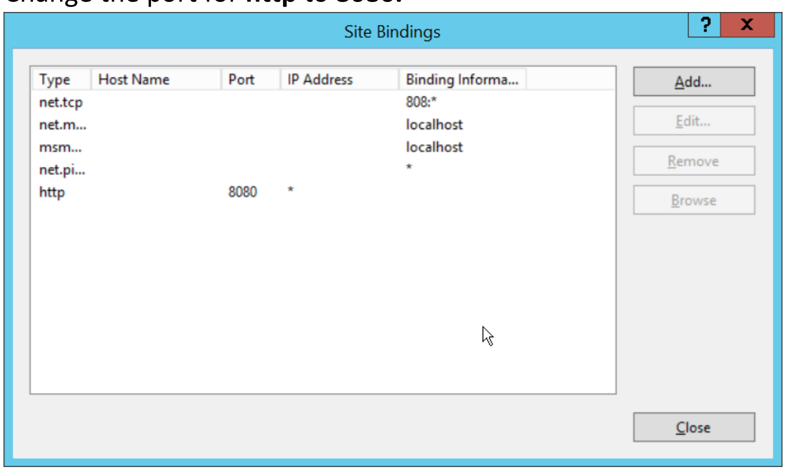
17. Click **Install.**



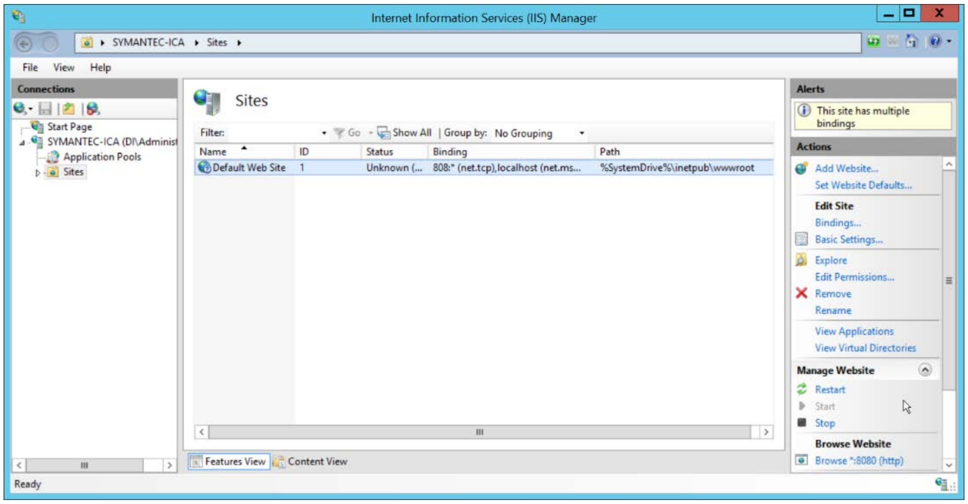
18. Click **Close** when the installation finishes.
19. Open **Internet Information Services Manager.**



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



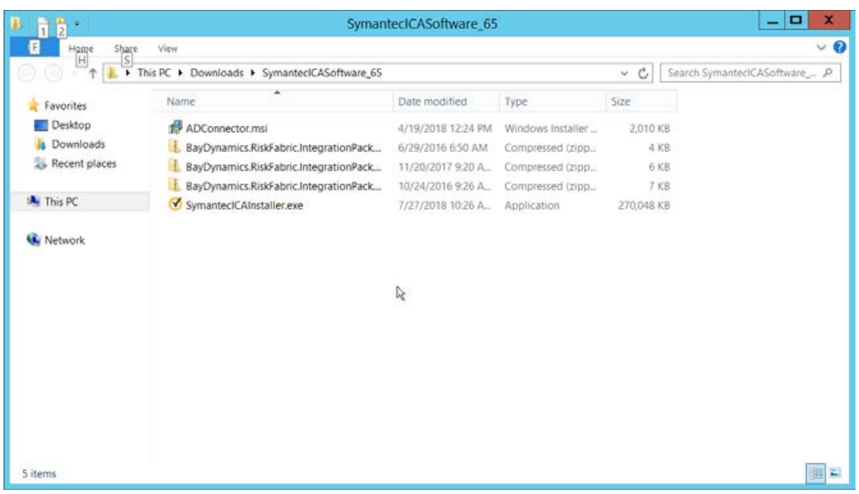
23. Click **Close.**



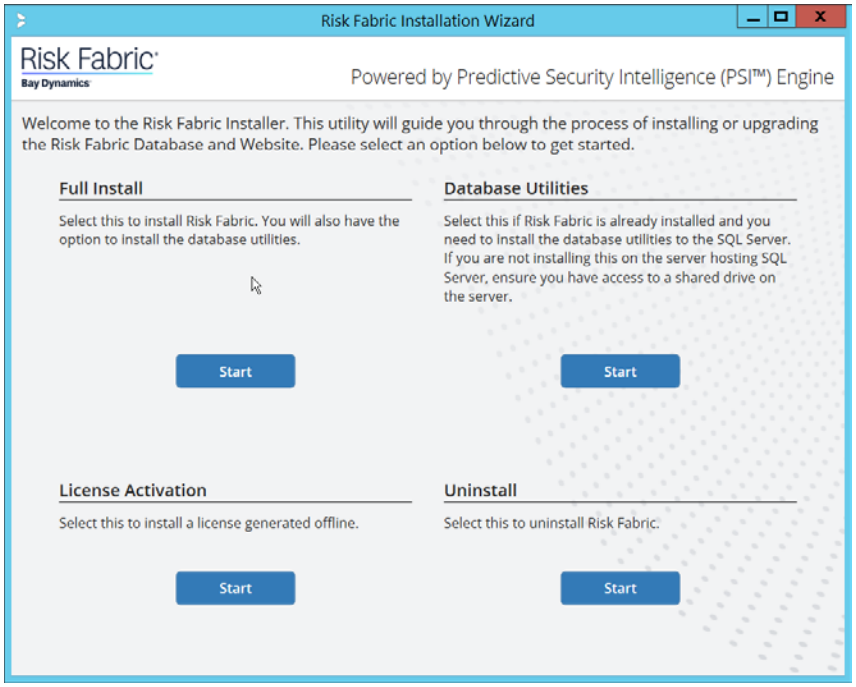
24. Click **Restart** under **Manage Website.**

2.15.3 Installing Symantec ICA

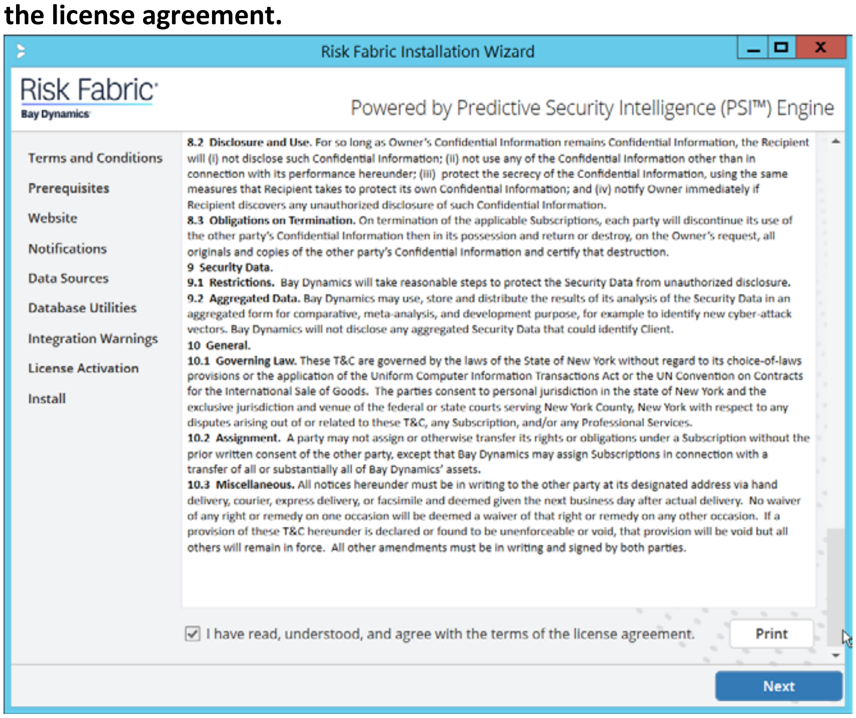
1. In Task Manager, verify that the **SQL Server Agent** service is running.
2. Copy the installation media **SymantecICASoftware_65.zip** onto the server.
3. Extract the installation media.



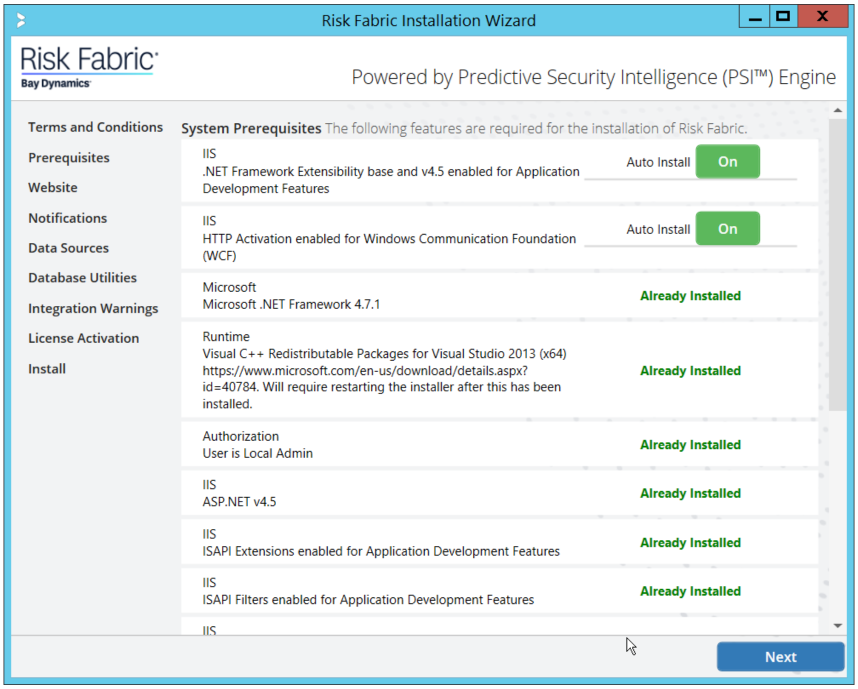
4. Run **SymantecICAInstaller.exe.**



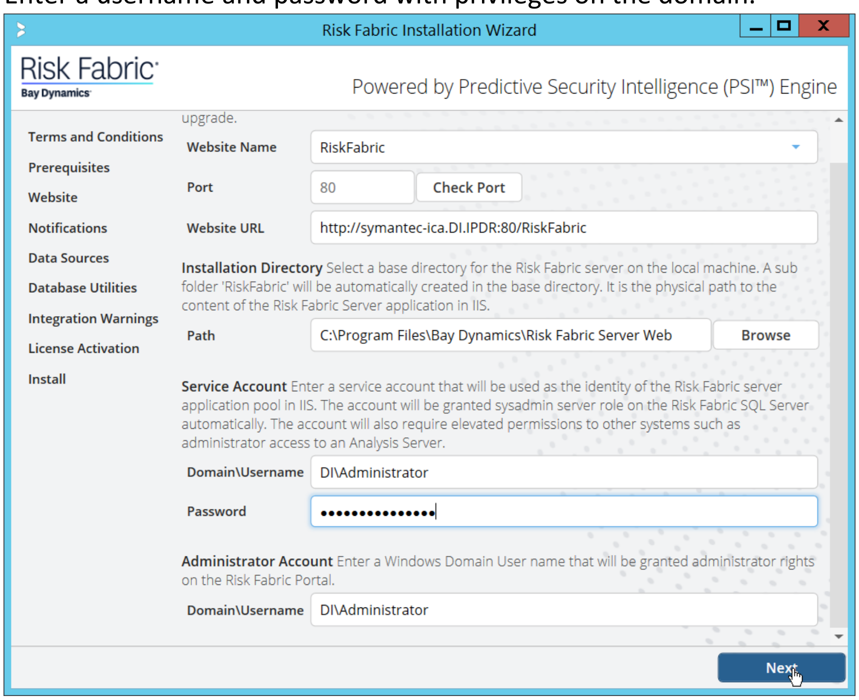
5. Under **Full Install,** click **Start.**
6. Scroll down and check the box next to **I have read, understood, and agree with the terms of the license agreement.**



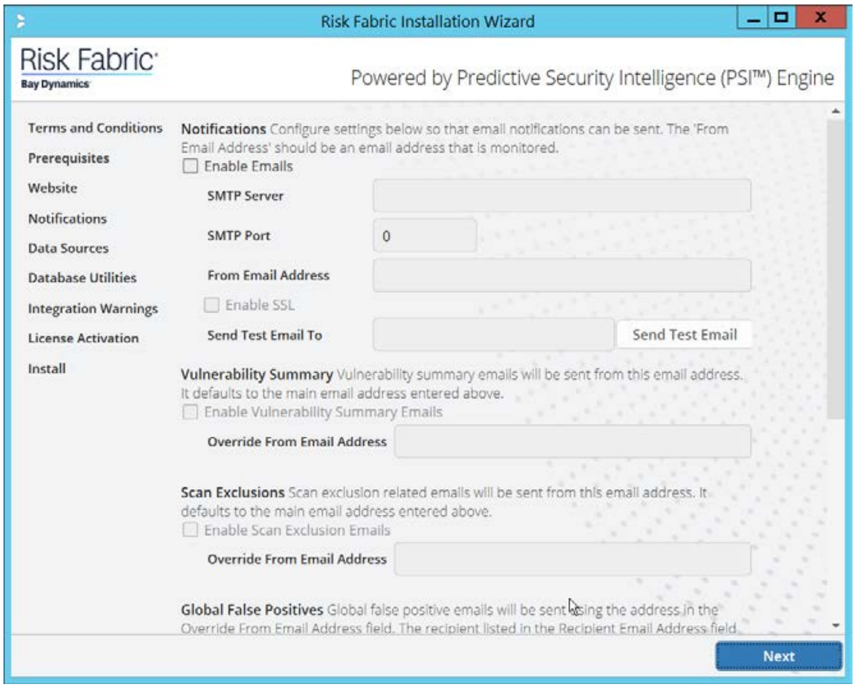
7. Click **Next.**



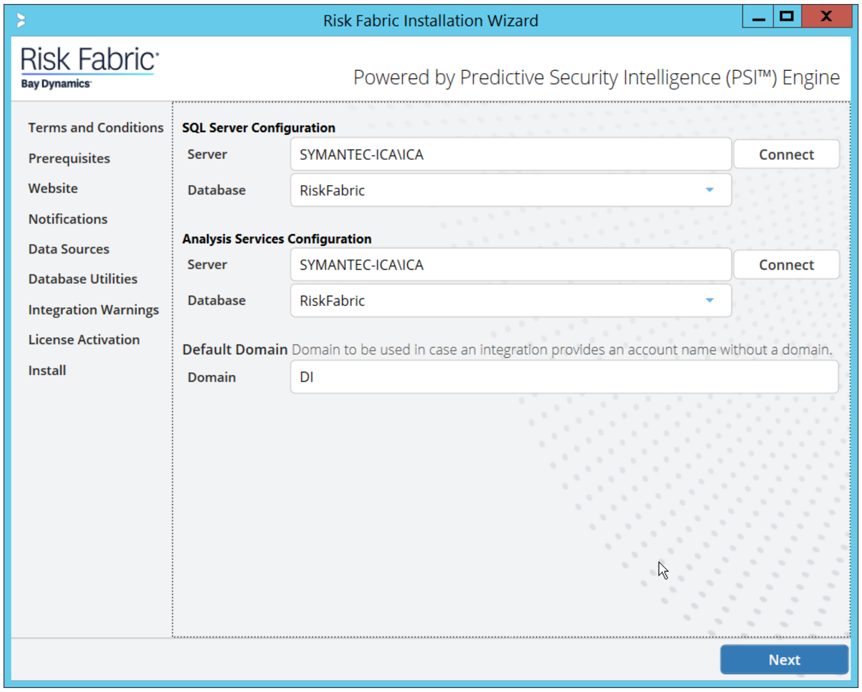
8. Click **Next.**
9. Enter a username and password with privileges on the domain.



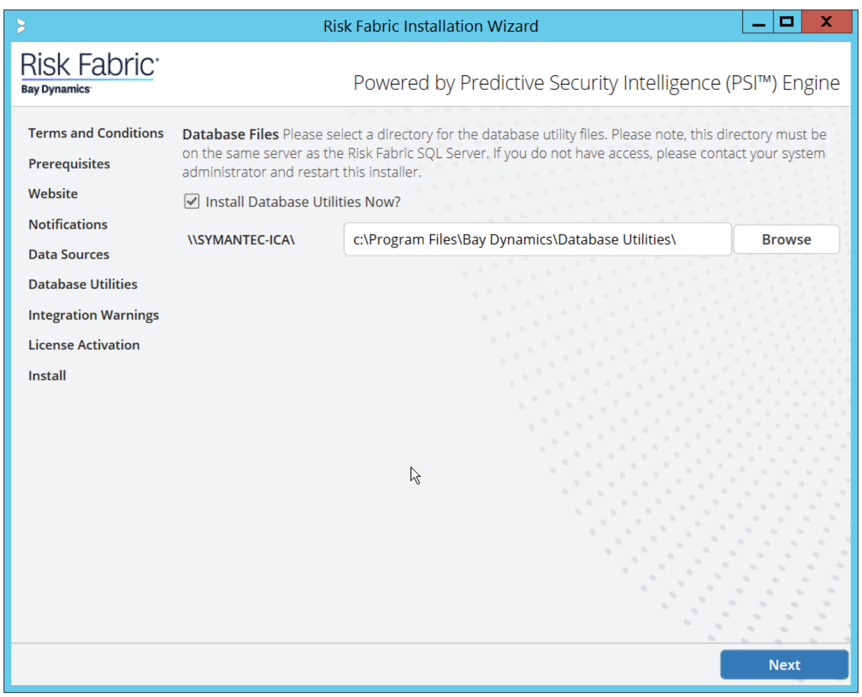
10. Click **Next.**
11. Configure any alert settings desired; these can be changed later.



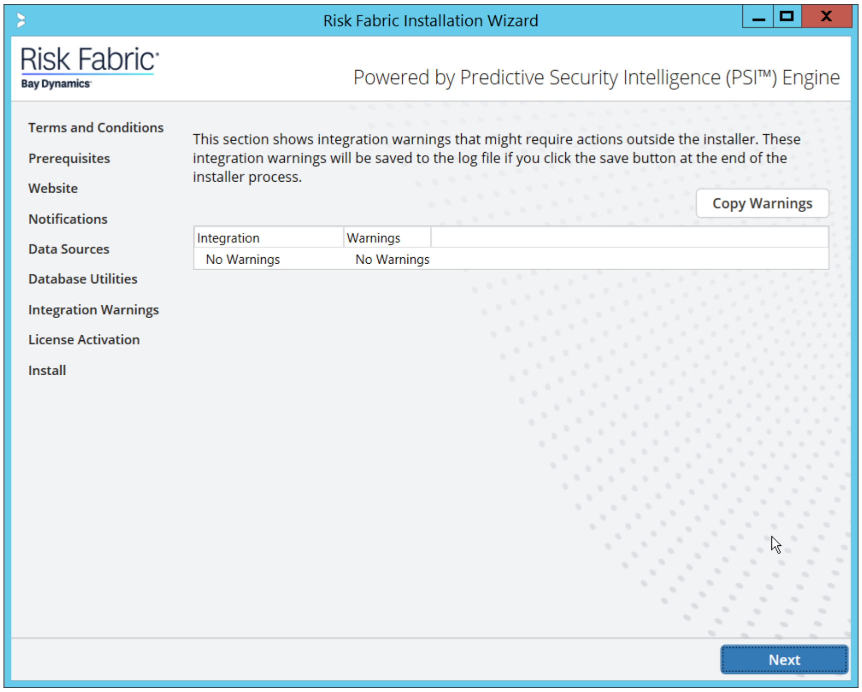
12. Click **Next.**
13. Enter the name of the SQL Server you created in the format **<SERVER-DOMAIN-NAME>\<SQL-SERVER-NAME>.**
14. Click **Connect,** and verify that there are no connection issues.
15. Enter the name of the SQL Analysis Services server you created in the format **<SERVER-DOMAIN-NAME>\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



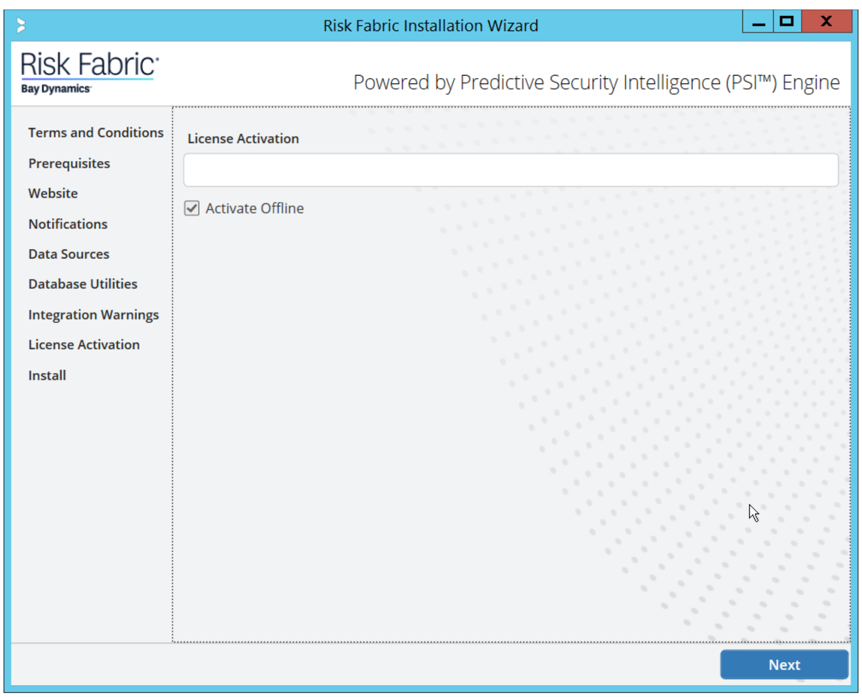
17. Click **Next.**



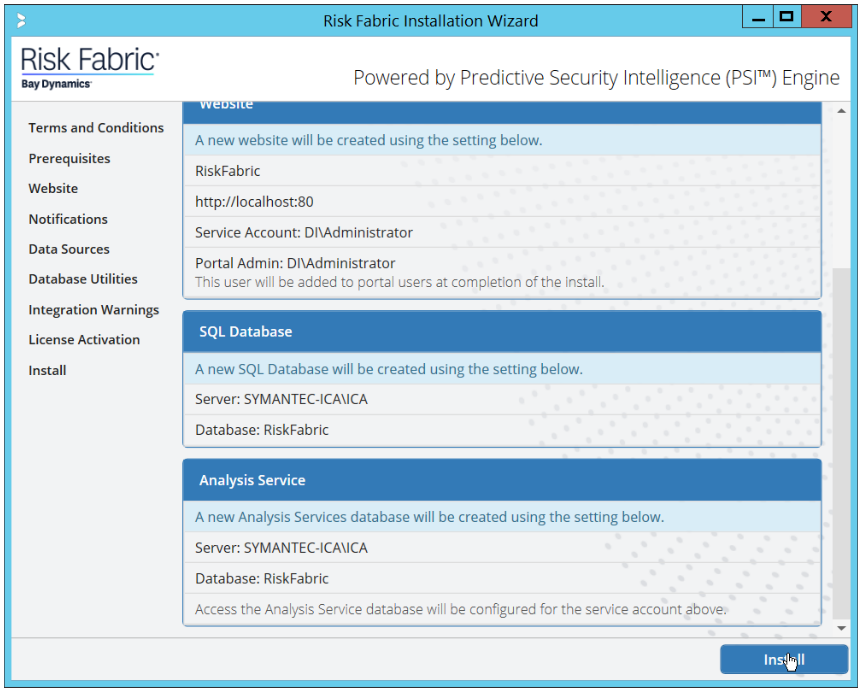
18. Click **Next.**



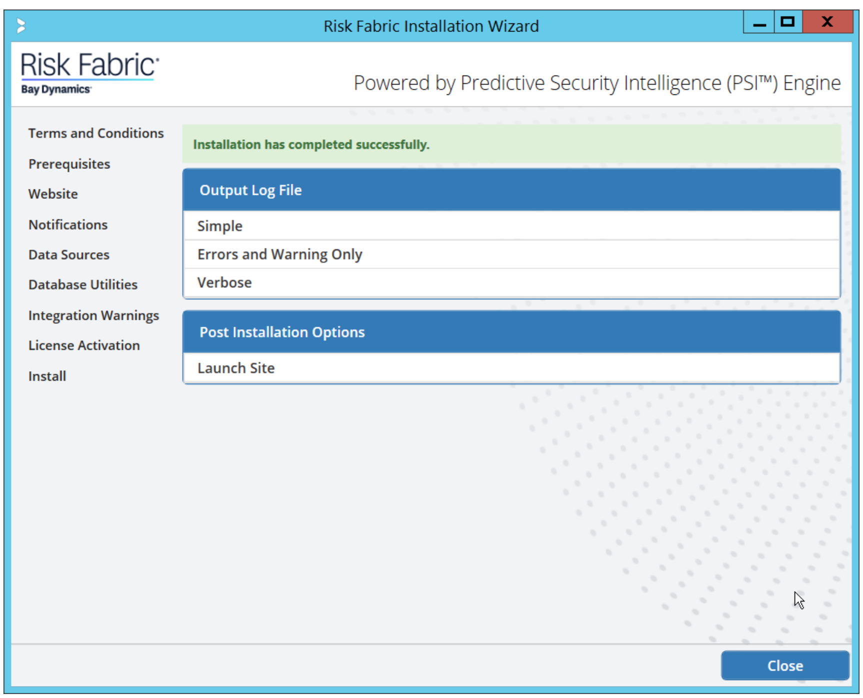
19. Click **Next.**
20. Check the box next to **Activate Offline.**



21. Click **Next.**



22. Click **Install.**



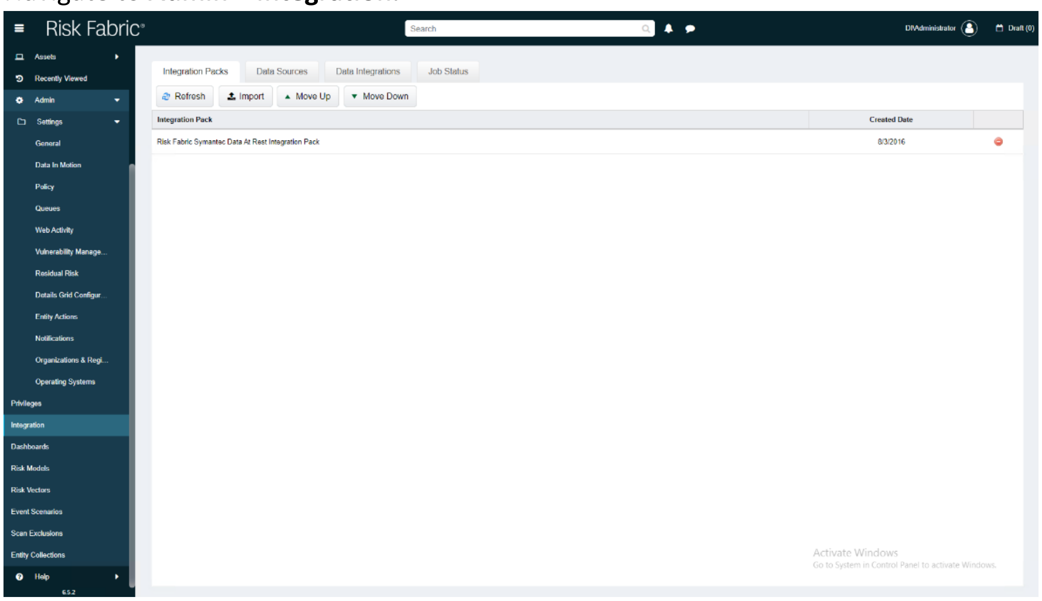
23. Click **Close.**

2.15.4 Configuring Symantec ICA for Analysis

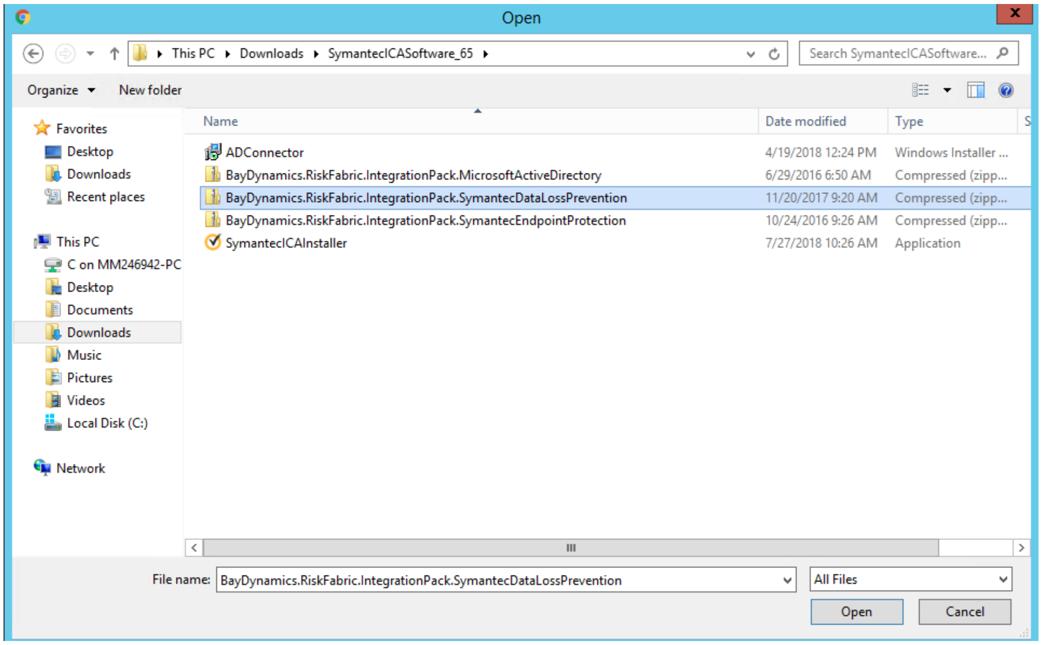
This section will contain instructions for navigating some aspects of the ICA admin console and dashboards, though this largely depends on the specific data your organization has identified and is trying to analyze.

2.15.4.1 *Installing Integration Packs*

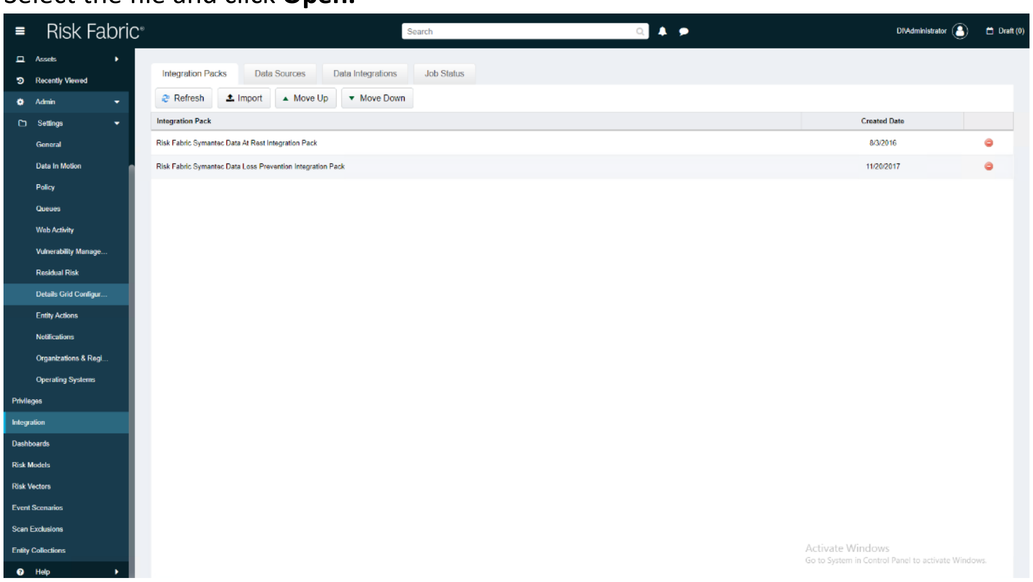
1. Download the relevant integration packs to someone on the local system. These are typically provided by Symantec, in a zip file. The zip file should be titled in the format of *BayDynamics.RiskFabric.IntegrationPack.<productName>.*
2. Log in to the Risk Fabric web interface.
3. Navigate to **Admin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



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

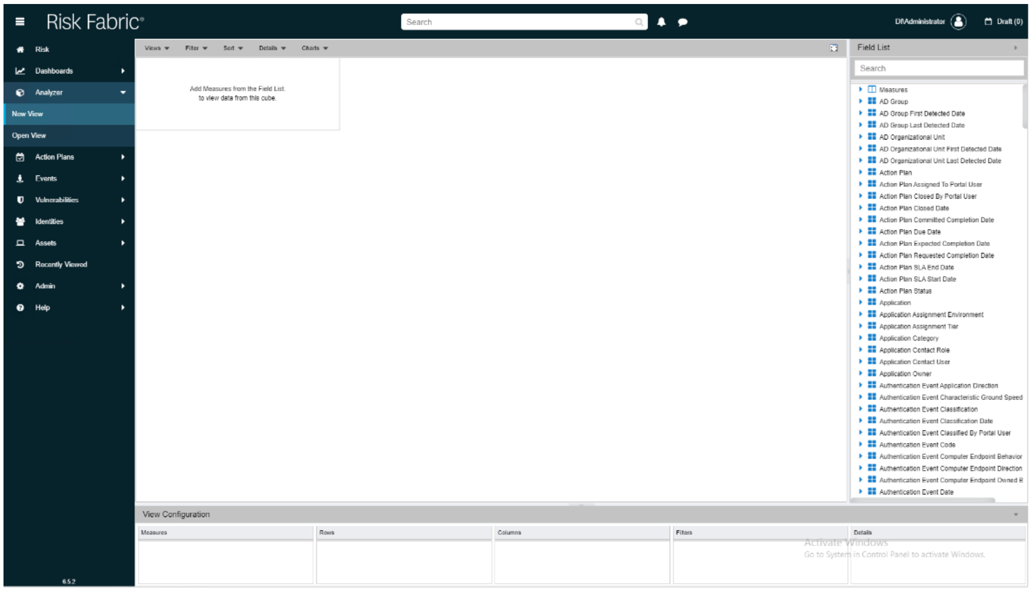


6. Select the file and click **Open**.

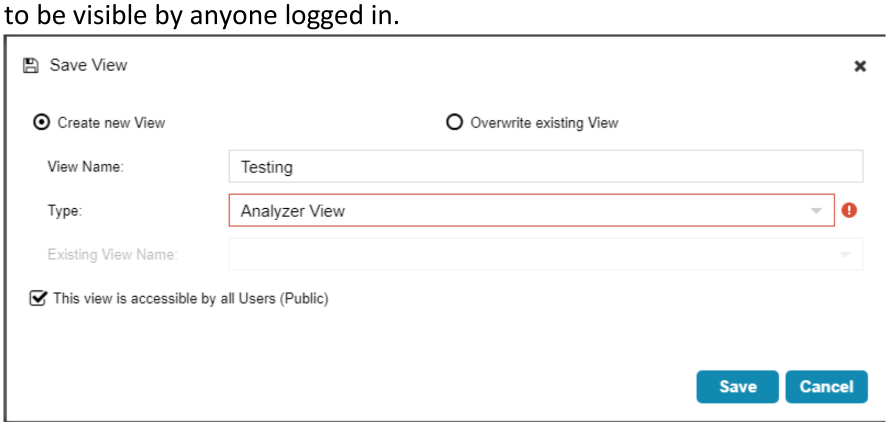


2.15.4.2 *Create a View*

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



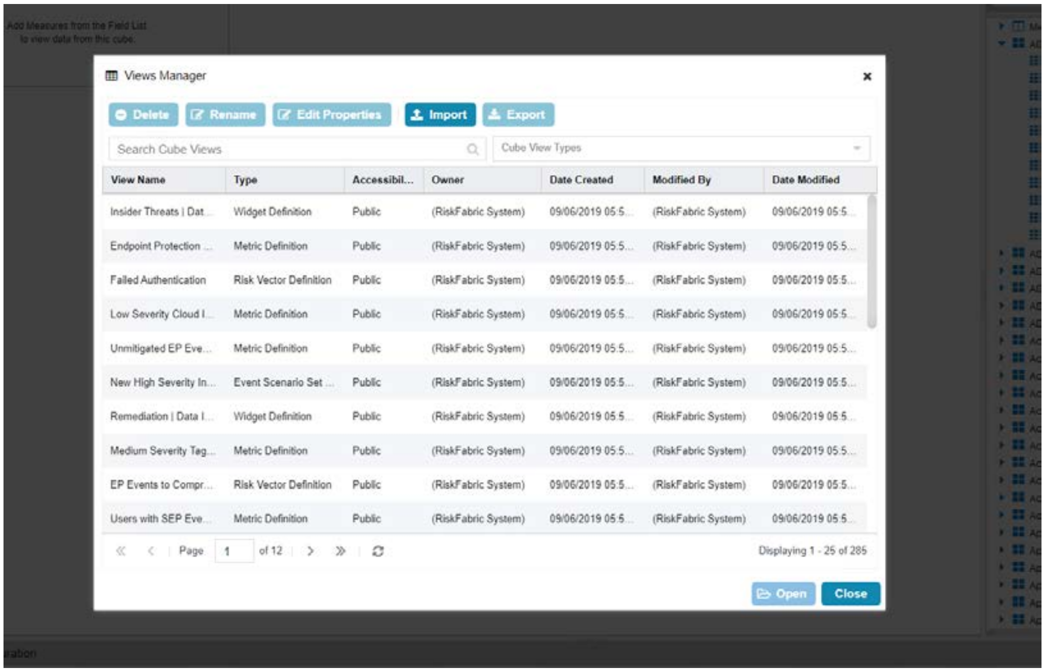
2. In the field list on the right, manually select or search for the data fields desired.
3. The fields can be added either by dragging the field onto the screen or by right-clicking on the field and selecting where it should be added. Ultimately, which views to select depends on the needs and preferences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



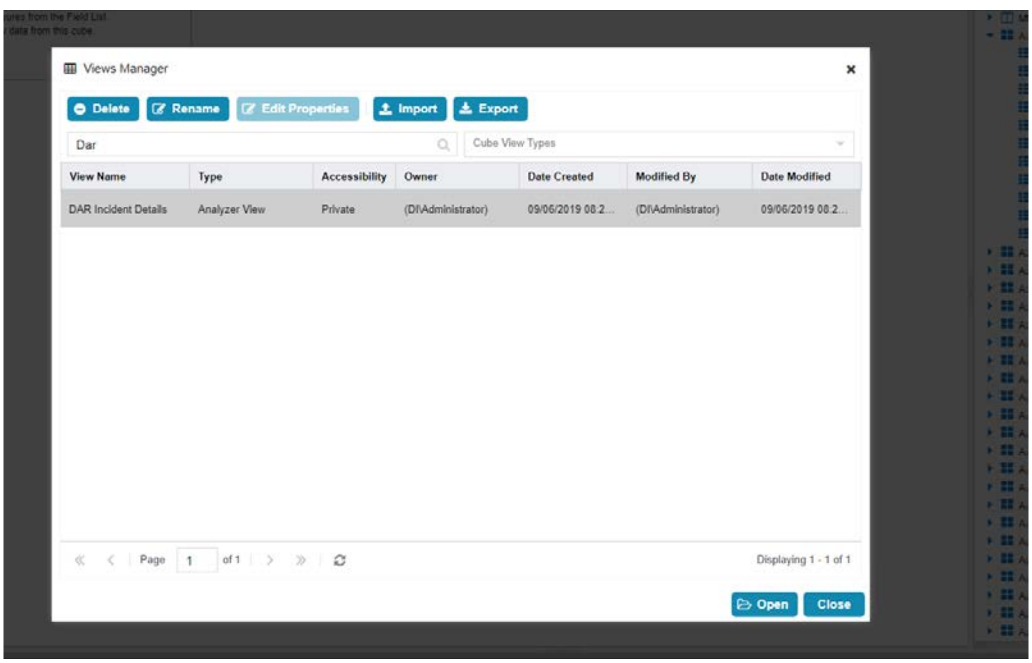
8. Click **Save.**

2.15.4.3 *Open an Existing View*

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



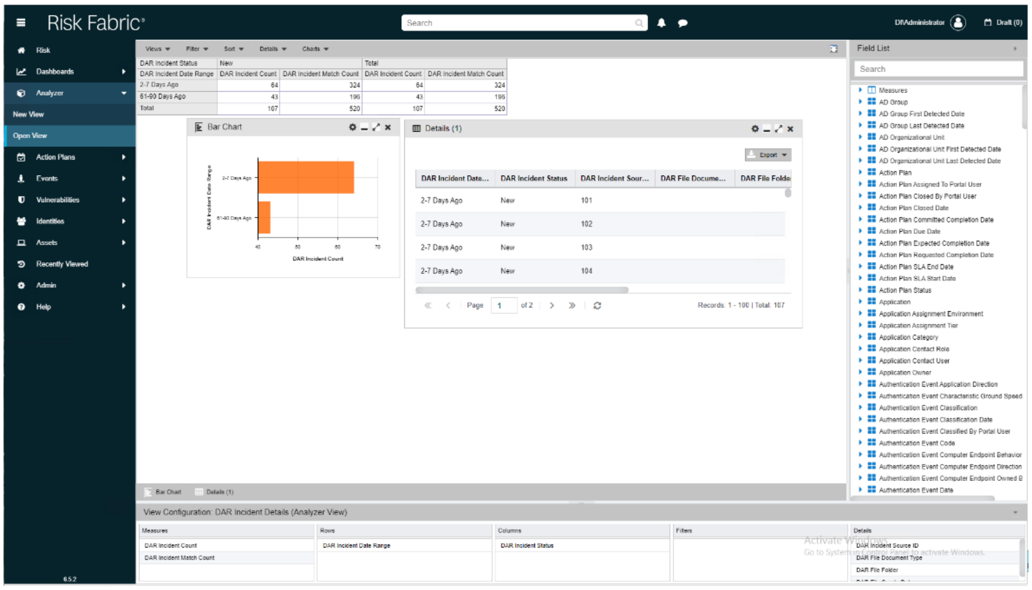
2. Begin to search for the view you want by typing a search term into **Search Cube Views.** (Note: if you created a view, it will also be present in this list).
3. Click the **Search** icon.
4. Select a view.



5. Click **Open.**

2.15.4.4 *Viewing Detailed Analyzer Data*

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



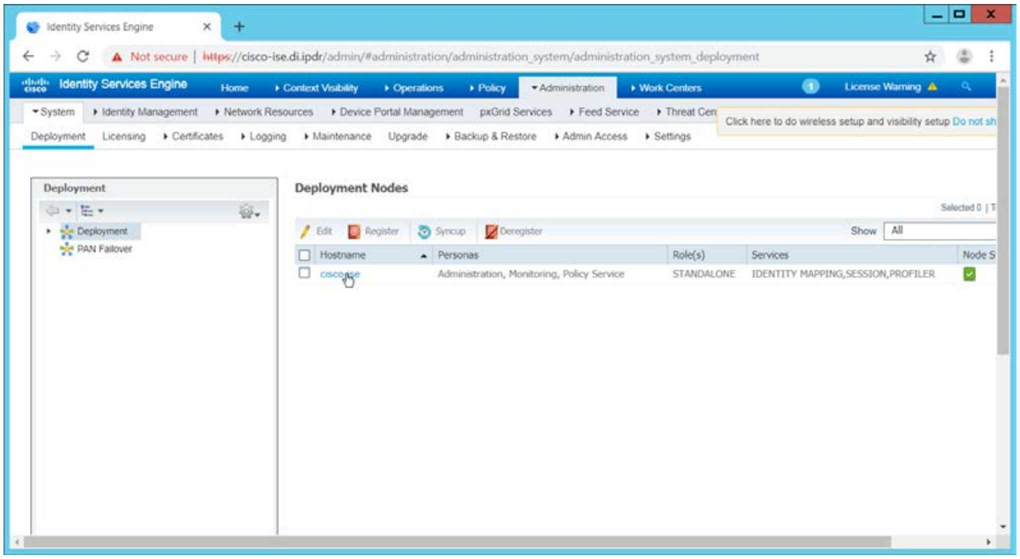
2. Charts can be added or removed using the **Charts** dropdown menu near the top of the analyzer.
3. Any data in the **Field List** on the right side can be added to or removed from the view and will be automatically incorporated into its relevant rows or columns.
4. The entire view format can be exported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

2.16 Integration: Cisco Identity Services Engine and Cisco Stealthwatch

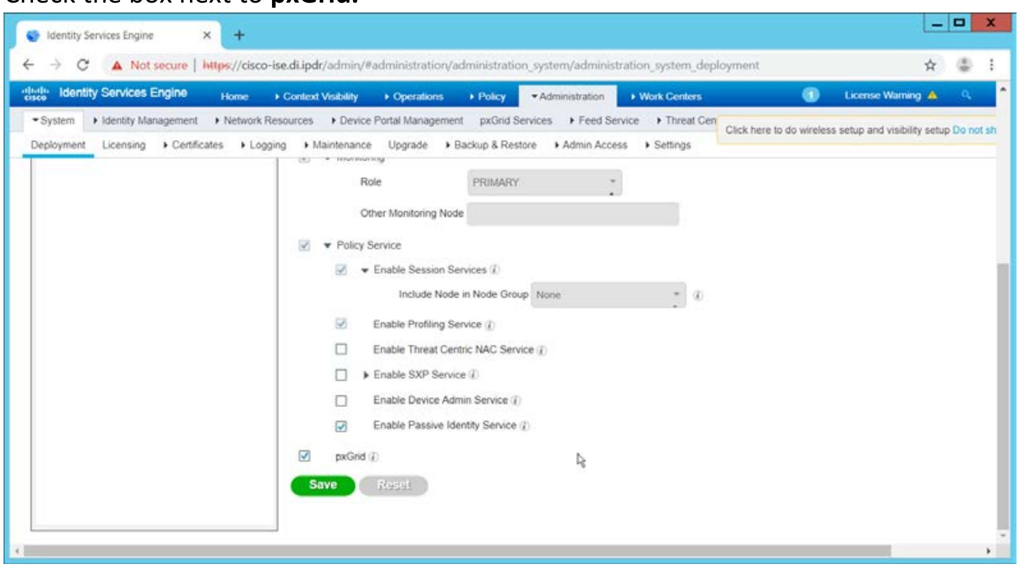
This section will detail an integration between Cisco Identity Services Engine (ISE) and Cisco Stealthwatch, allowing Stealthwatch to apply certain policies to hosts in ISE. Stealthwatch acts as a network monitoring solution and can be integrated with ISE to enable mitigation capabilities in response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

2.16.1 Configuring Certificates for pxGrid

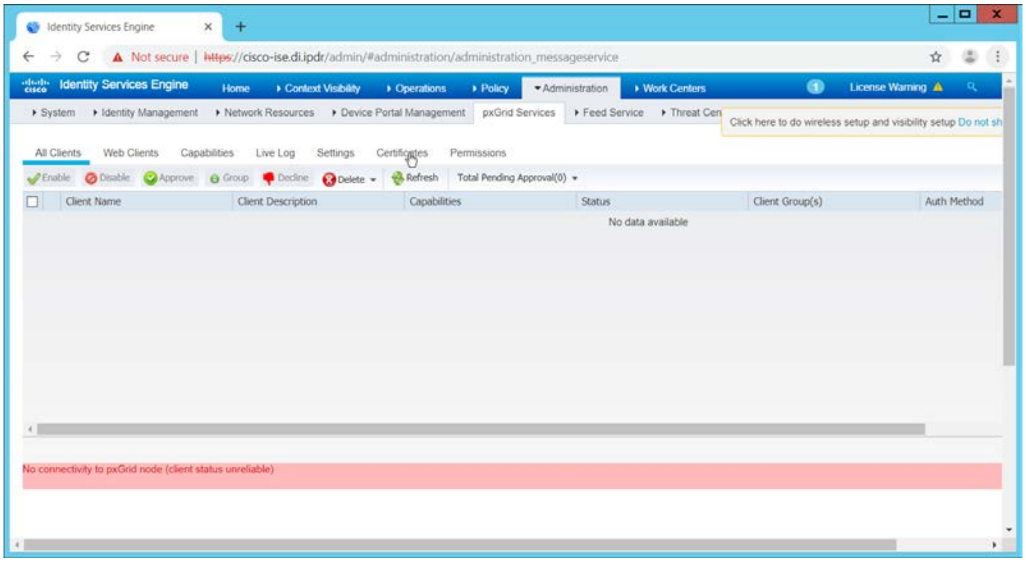
1. Log in to the Cisco ISE web console in a browser.
2. Navigate to **Administration > System > Deployment.**



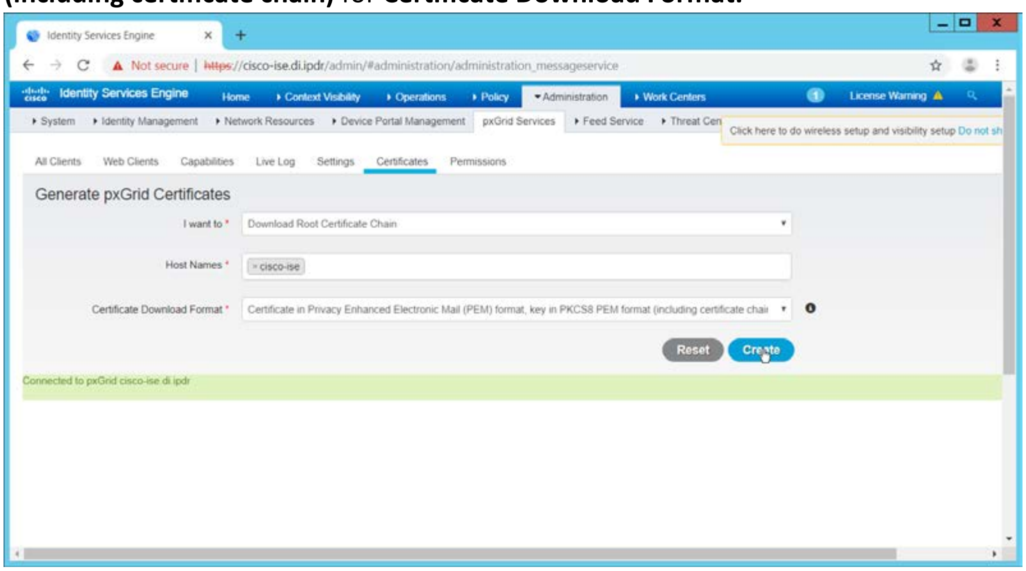
3. Click the hostname of the Cisco ISE machine.
4. Check the box next to **pxGrid.**



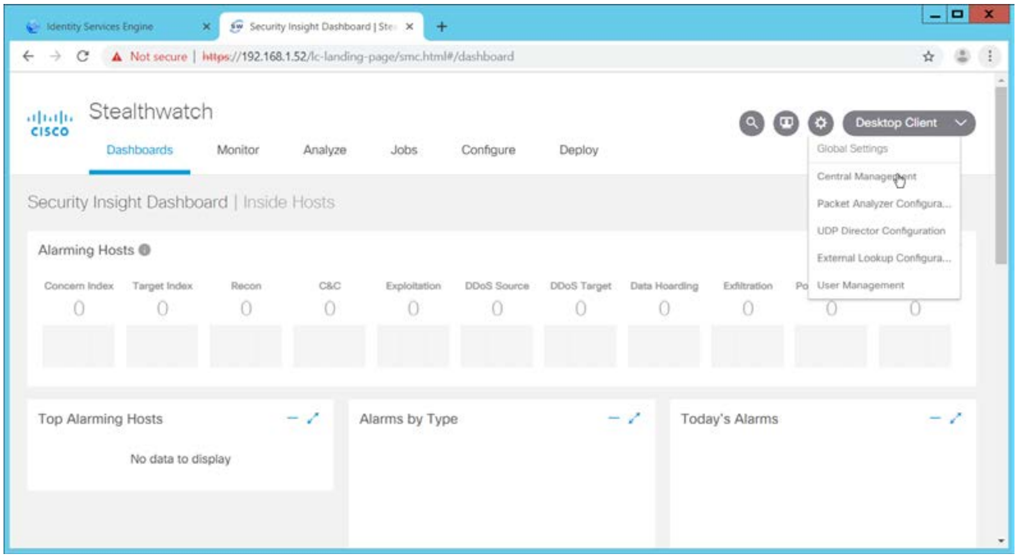
5. Click **Save.**
6. Navigate to **Administration > pxGrid Services.**



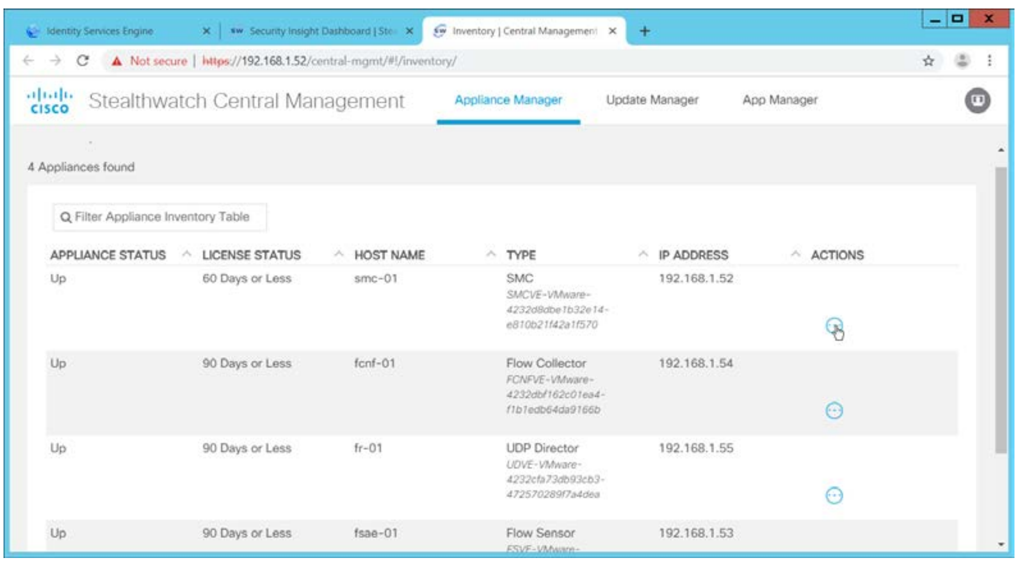
7. Click **Certificates.**
8. Select **Download Root Certificate Chain** for **I want to.**
9. Select the hostname of the Cisco ISE server for **Host Names.**
10. Select **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PLCS8 PEM format (including certificate chain)** for **Certificate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



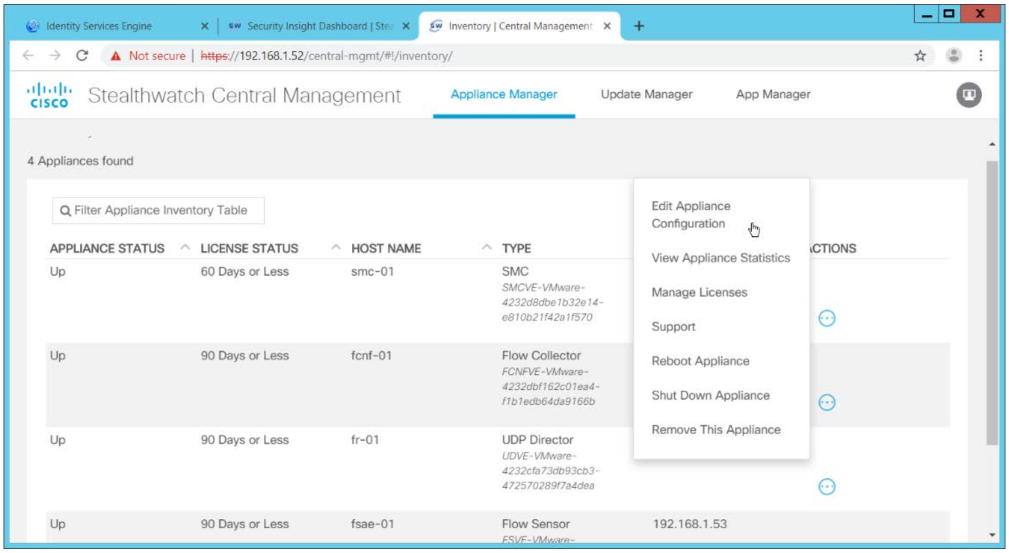
11. Click **Create.** This will download a zip file containing the certificate.
12. Extract the zip file—it may contain several files—the one we are interested in is the Root CA.
13. Log in to the **Stealthwatch Management Console** through the browser.



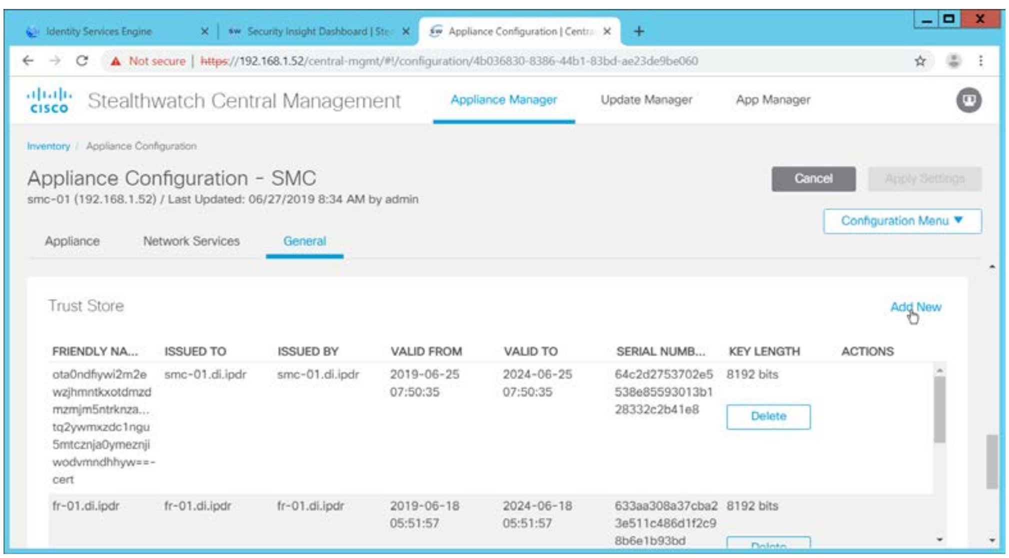
14. In the top right corner of the console, hover over the **gear icon** and select **Central Management** from the submenu.



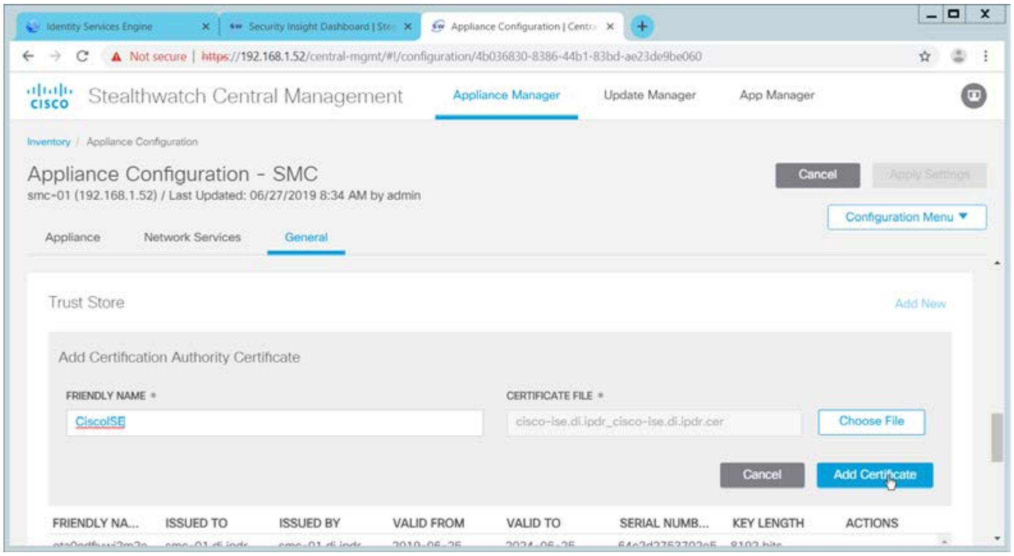
15. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.



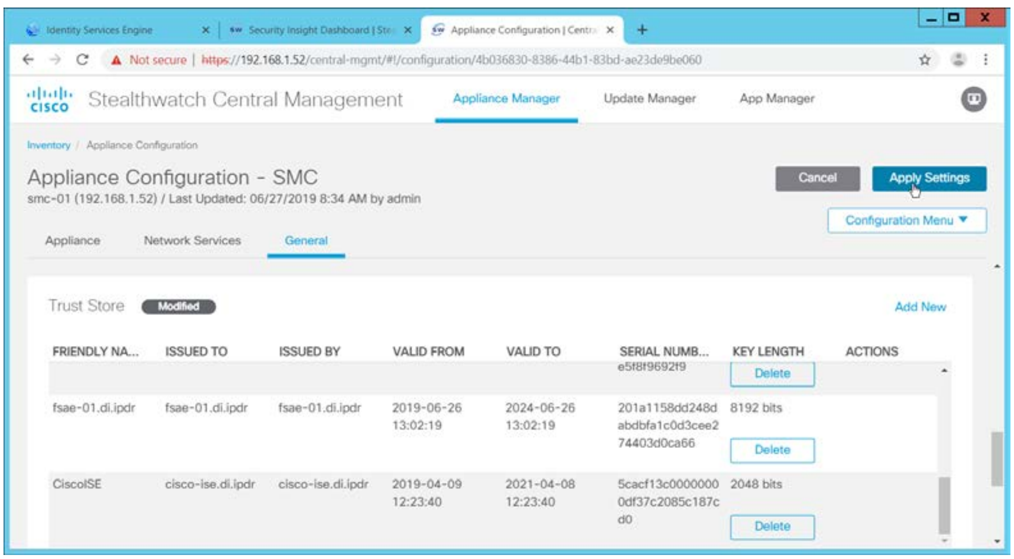
16. This will open a submenu. Select **Edit Appliance Configurations.**
17. Click the **General** tab.
18. Scroll down to the **Trust Store** section.



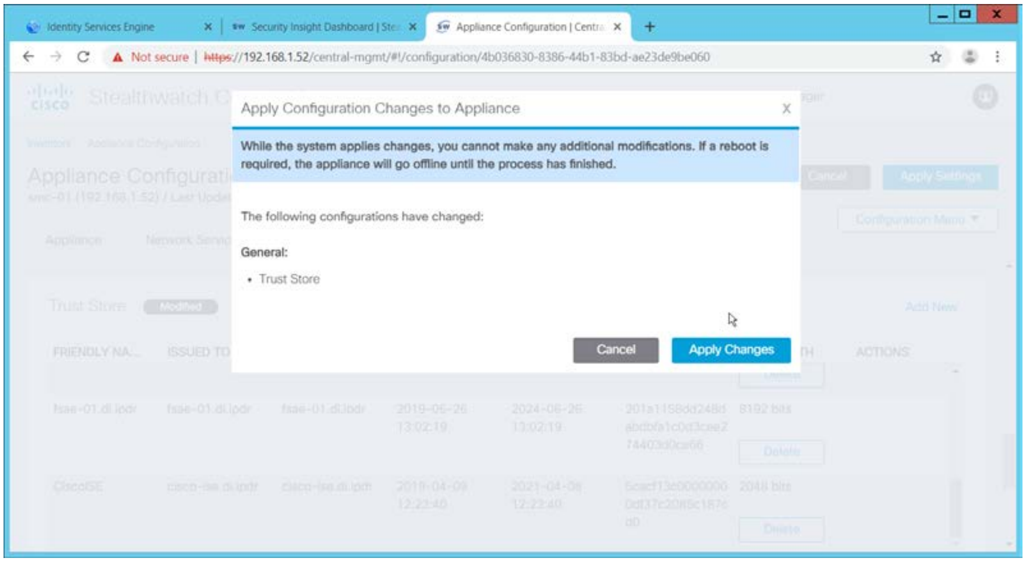
19. Click **Add New.**
20. Enter a **name.**
21. Click **Choose File.**
22. Select the Cisco ISE Root certificate from the files downloaded earlier.



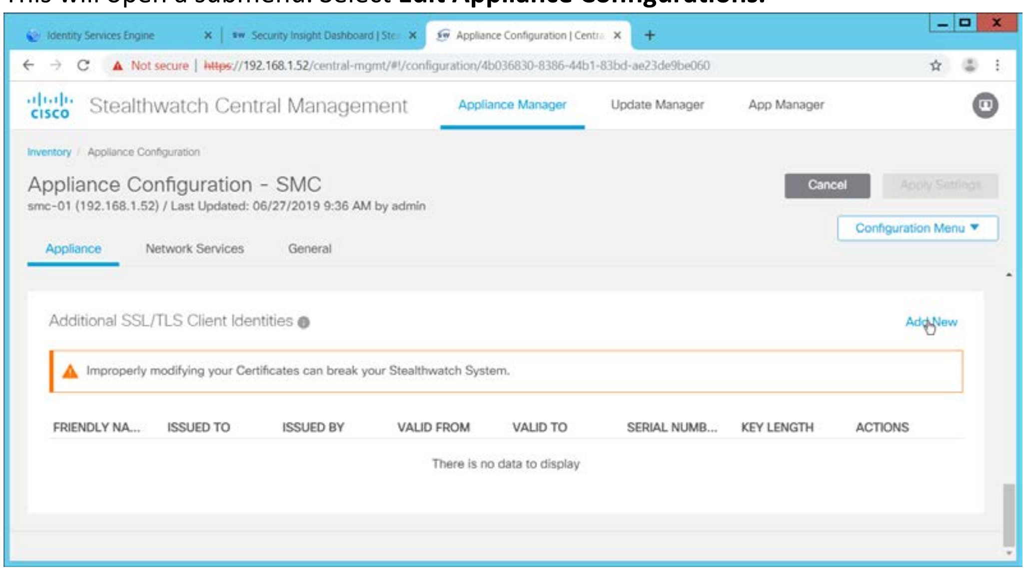
23. Click **Add Certificate.**



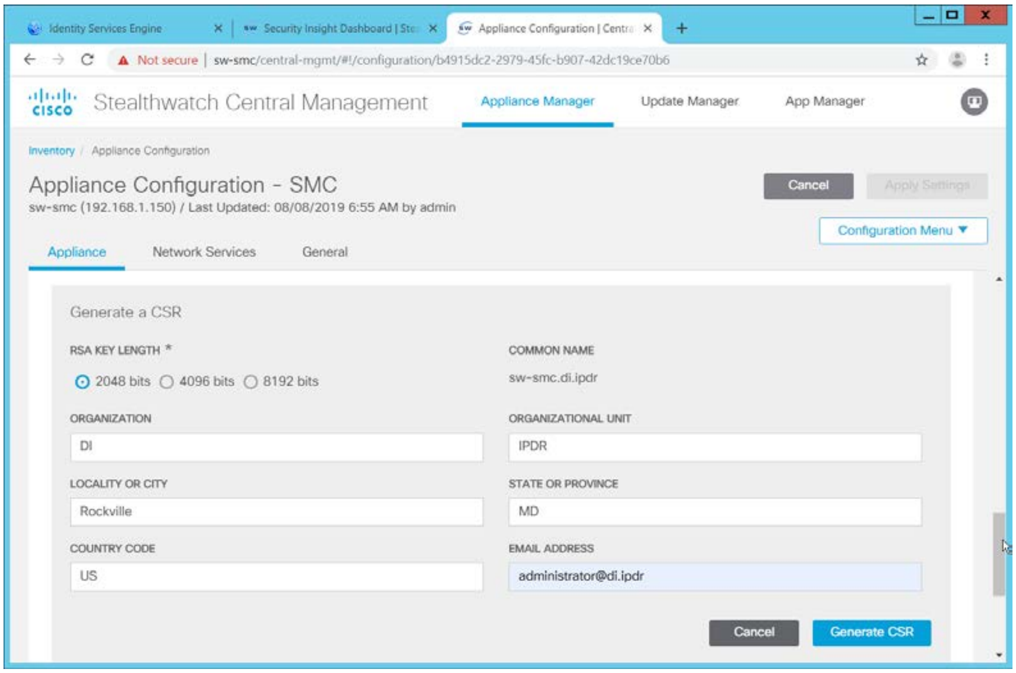
24. Click **Apply Settings.**



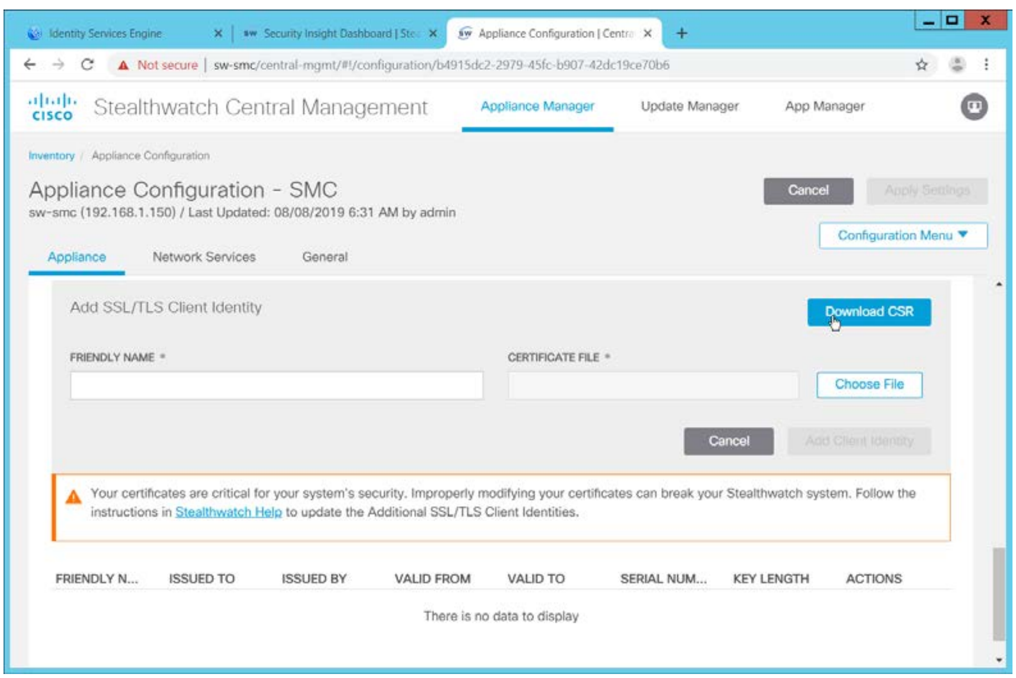
25. Click **Apply Changes** if prompted to confirm the changes.
26. When that finishes, navigate back to the **Appliance Configurations** section.
27. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.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



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

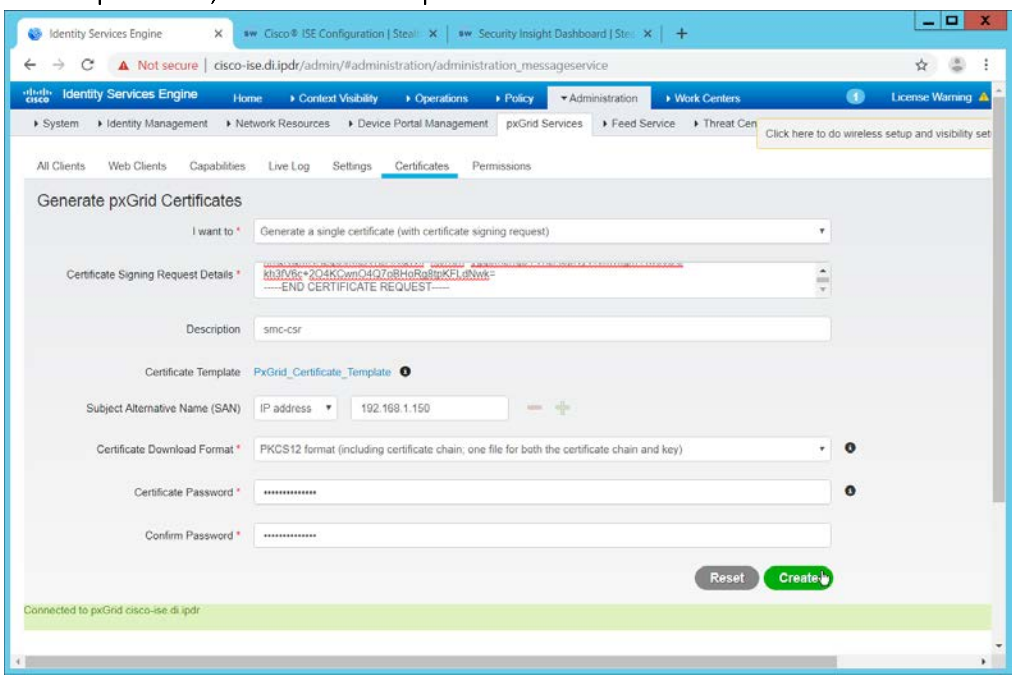


32. Click **Generate CSR.**

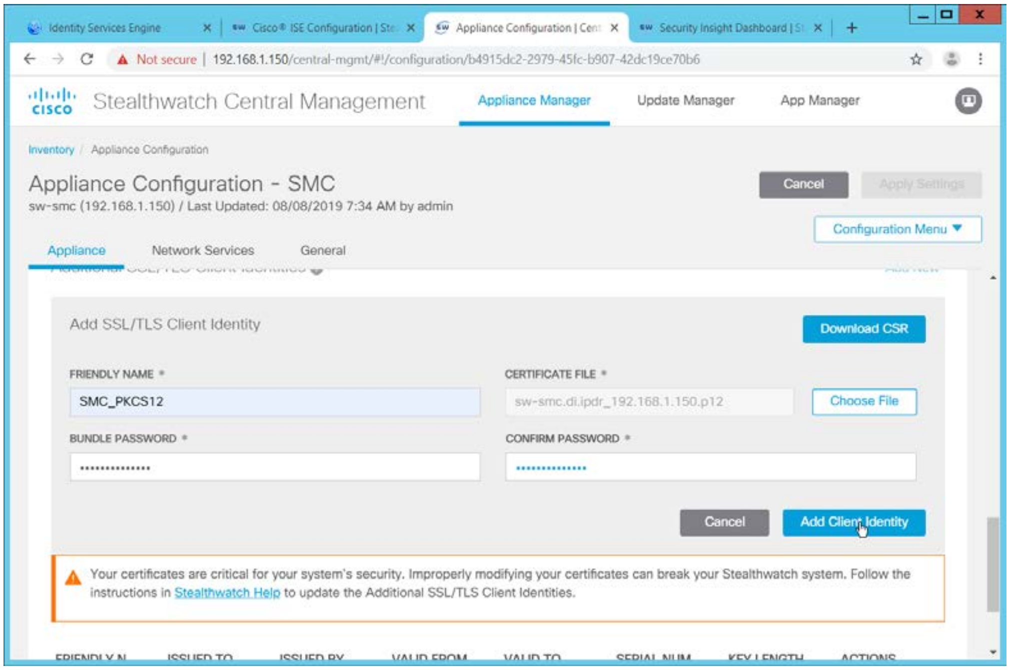


33. When this finishes, click **Download CSR.**
34. Open the CSR in a text file, and copy all the contents.
35. On the ISE web console, navigate to **Administration > pxGrid Services > Certificates > Generate pxGrid Certificates.**

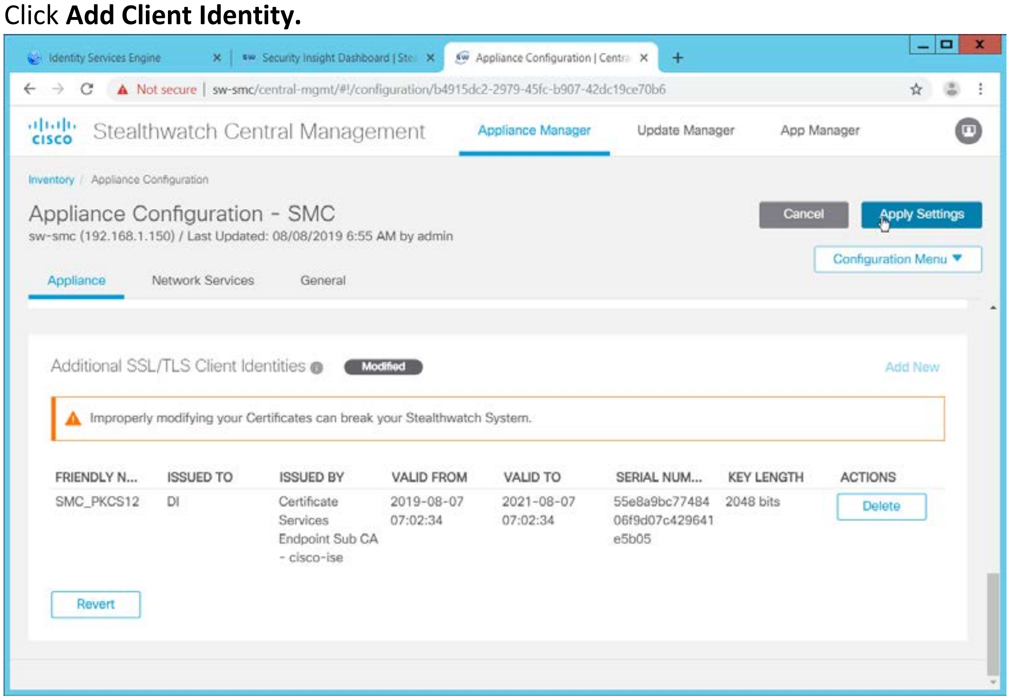
36. Select **Generate a single certificate (with certificate signing request)** for **I want to.**
37. Paste the copied text into the **Certificate Signing Request Details.**
38. Enter a description such as **SMC** for the **Description.**
39. Select **IP Address** for **Subject Alternative Name (SAN).**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



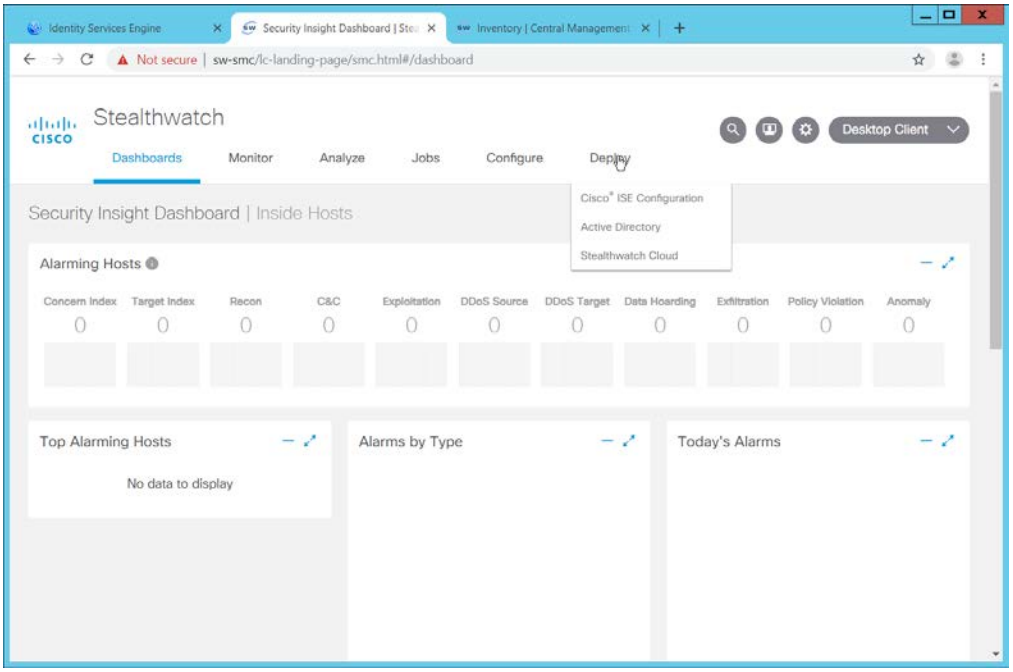
43. Click **Create.**
44. This will download a zip file. Unzip the file.
45. On the Stealthwatch Management Console (SMC) web console, under **Additional SSL/TLS Client Identities** (where you downloaded the CSR), click **Choose File.**
46. Upload the certificate file from the zip file that has the hostname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



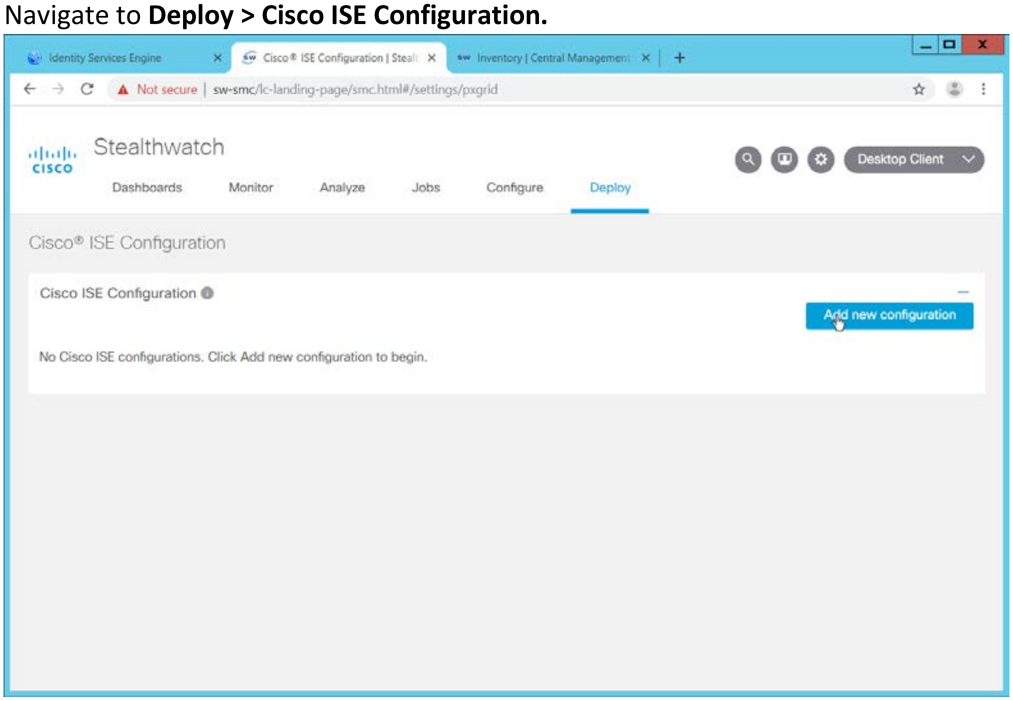
49. Click **Add Client Identity.**



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

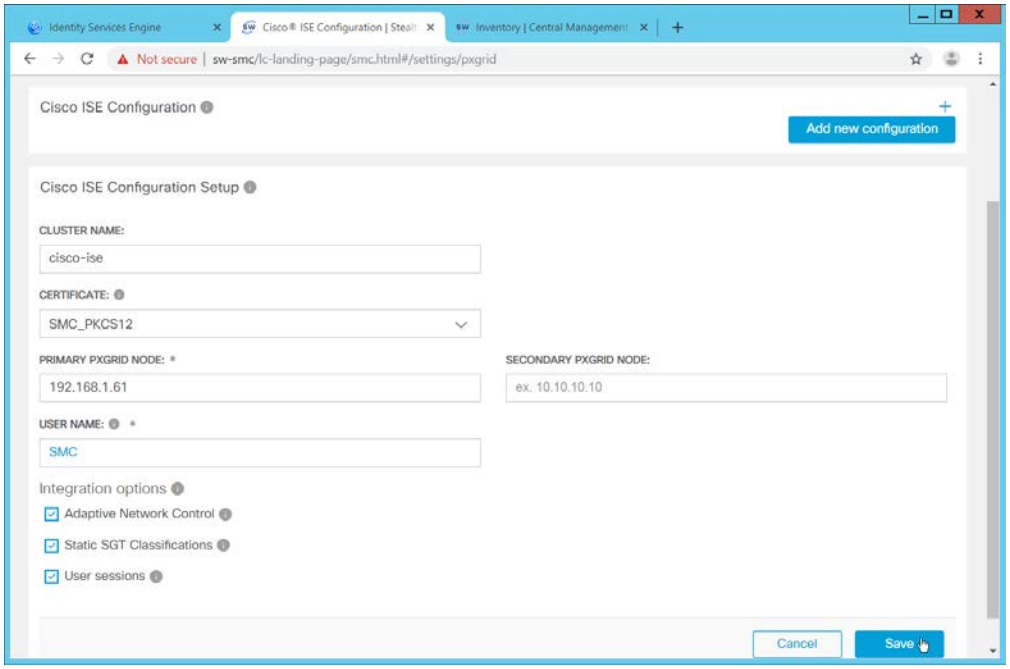


52. Navigate to **Deploy > Cisco ISE Configuration.**



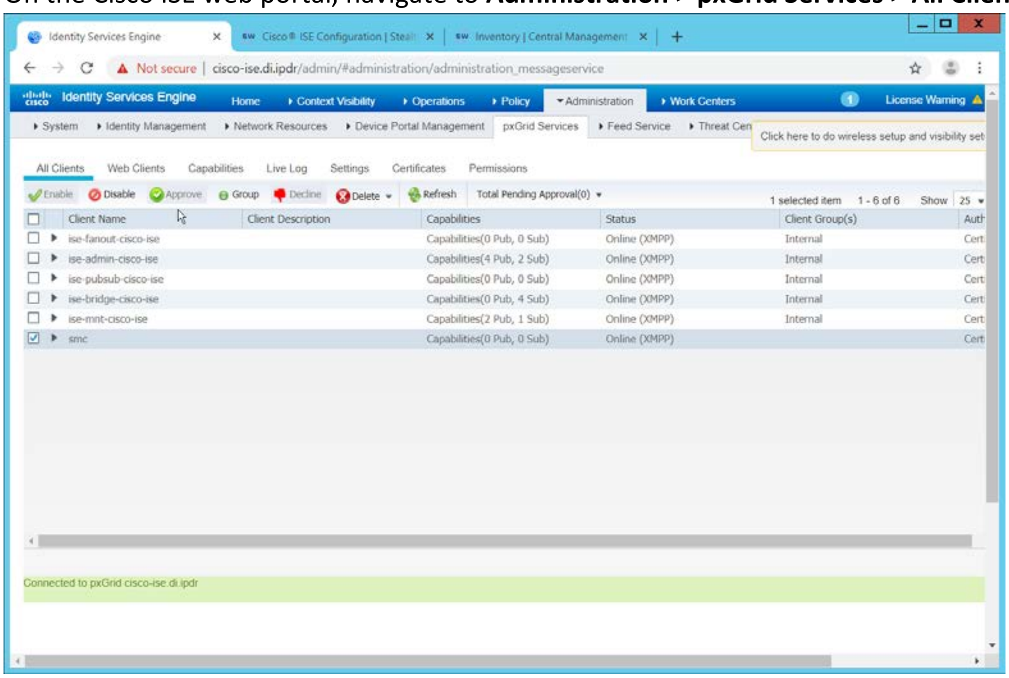
53. Click **Add New Configuration.**
54. Enter a Cisco ISE cluster name.
55. Select the certificate you just uploaded for **Certificate.**
56. Enter the **IP Address** of Cisco ISE for **Primary pxGrid Node.**

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

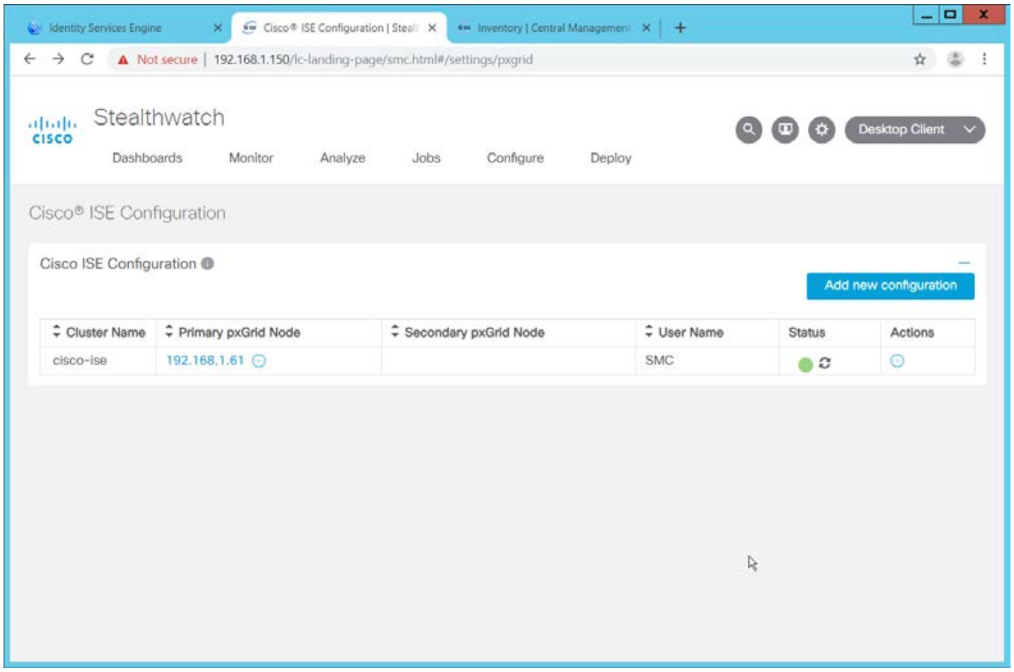


58. Click **Save.**

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



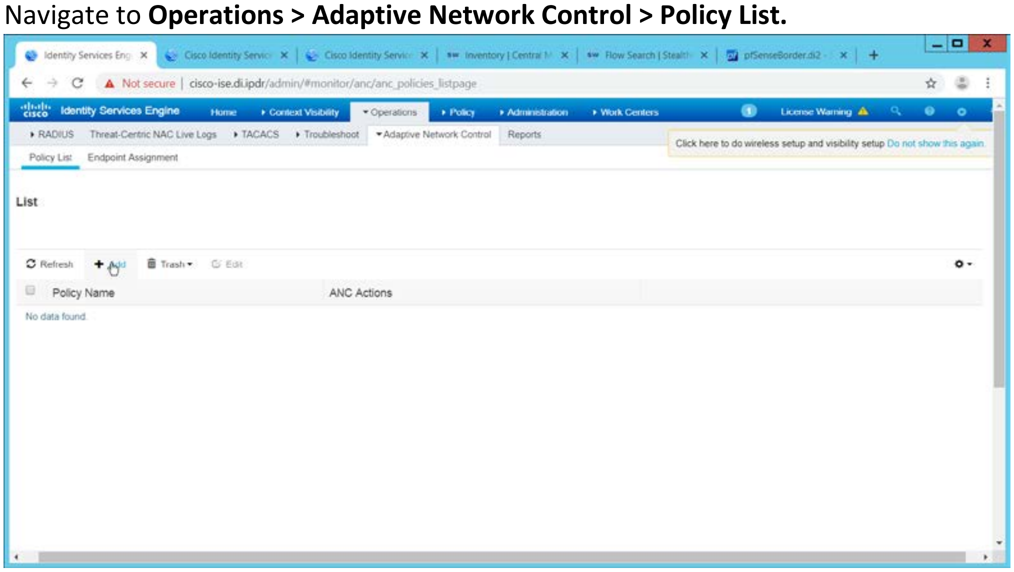
60. If the SMC client you just created says **Pending,** check the box next to it and click **Approve.**



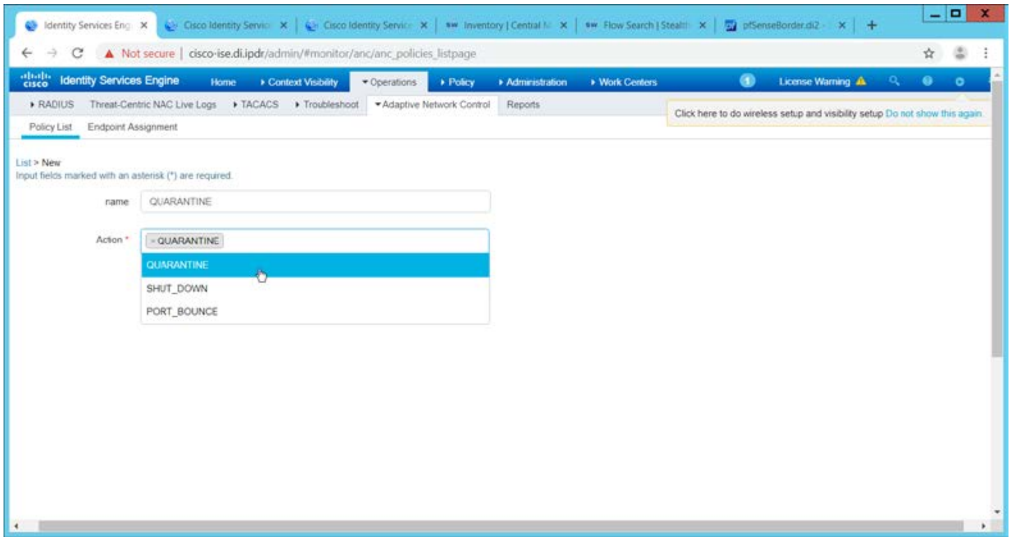
61. The SMC Cisco ISE Configuration page will have a green status icon if it can successfully authenticate to ISE.

2.16.2 Configuring Stealthwatch to Quarantine through ISE

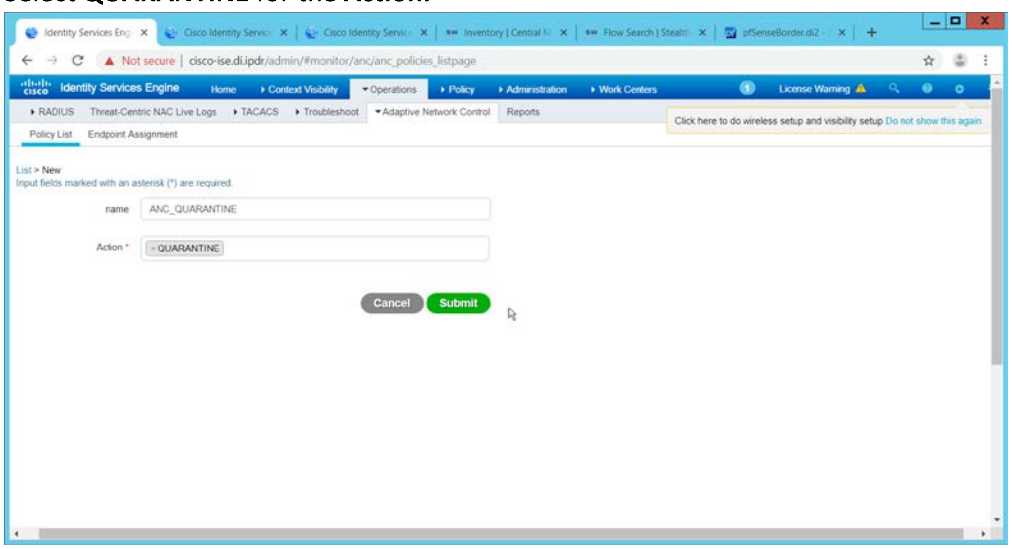
1. Navigate to **Operations > Adaptive Network Control > Policy List.**



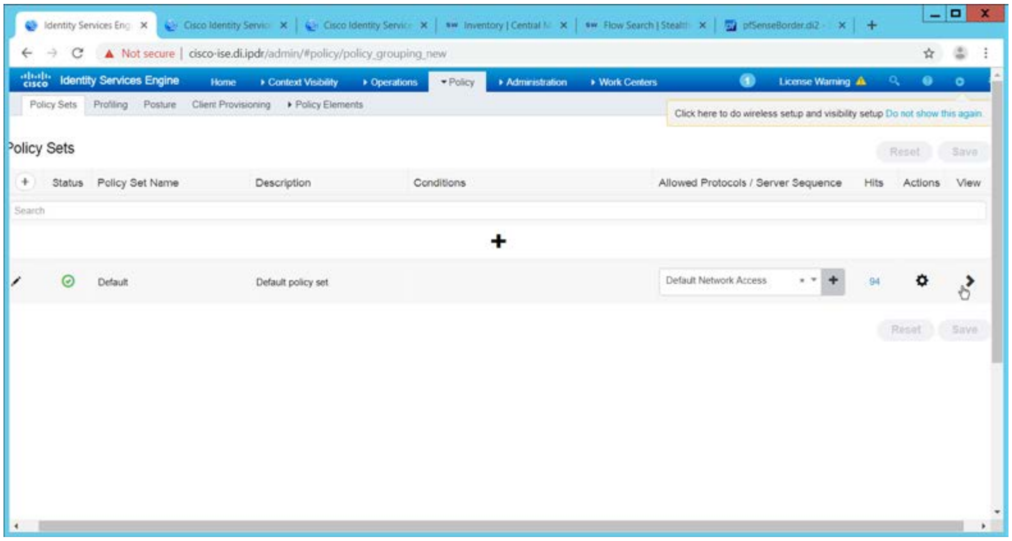
2. Click **Add.**
3. Enter a name for a quarantine action.



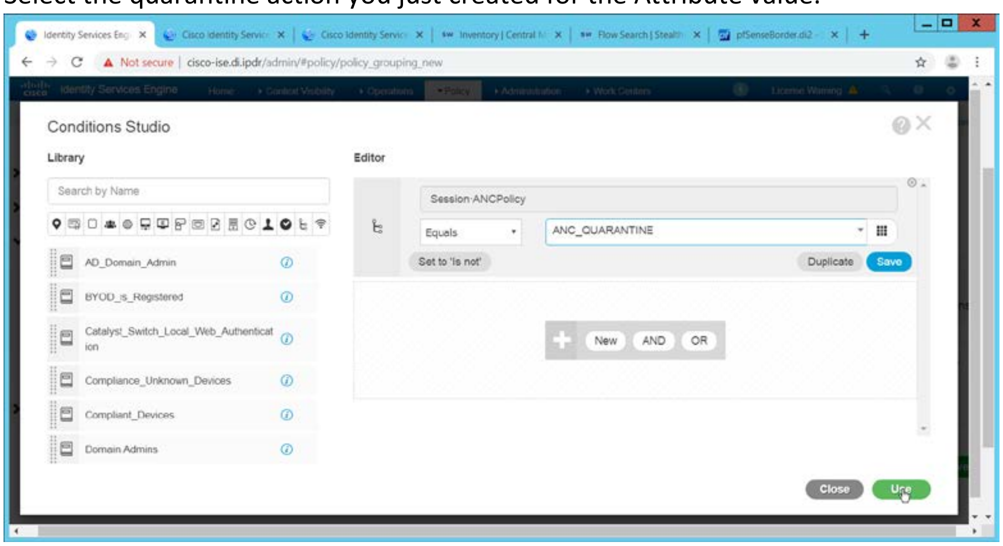
4. Select **QUARANTINE** for the **Action.**



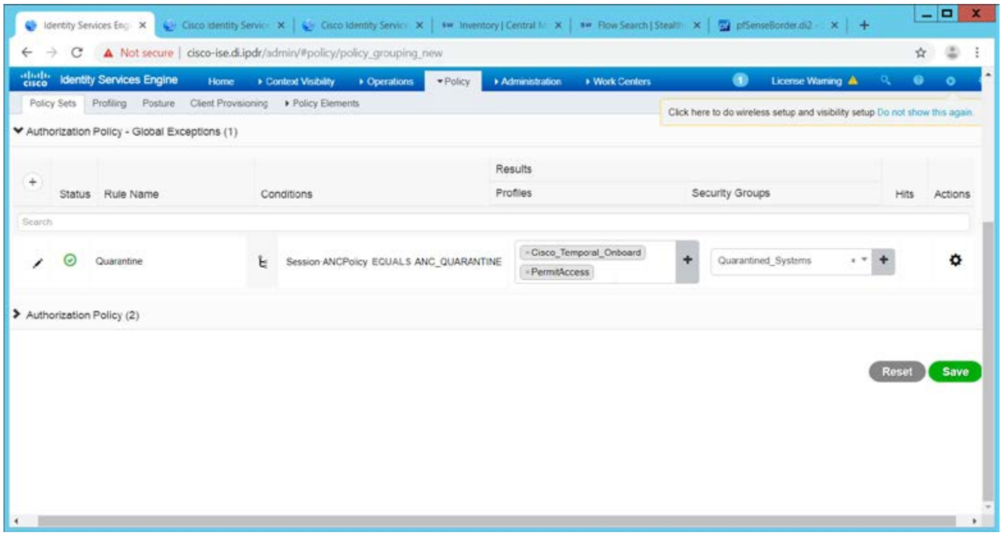
5. Click **Submit.**
6. Navigate to **Policy > Policy Sets.**



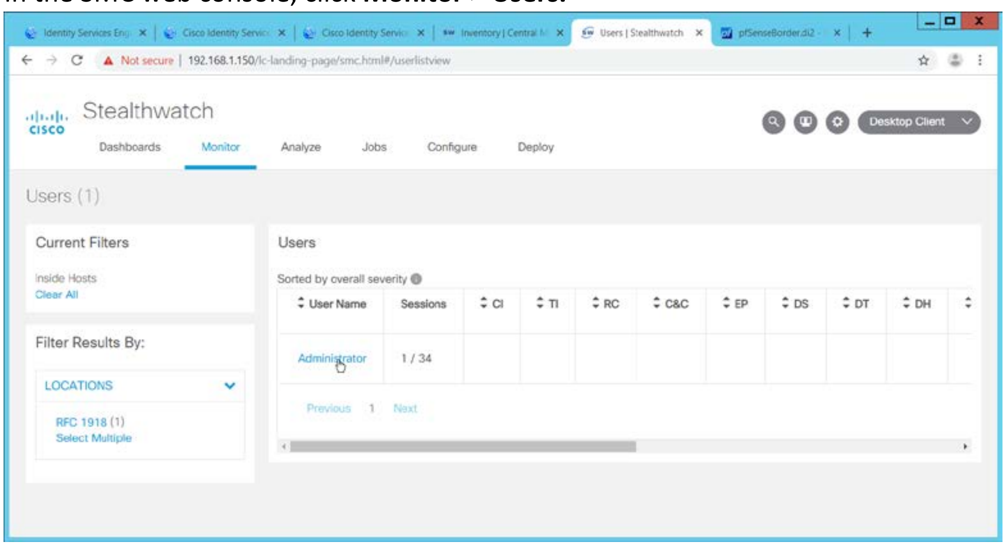
7. Click the **>** arrow next to the default policy set.
8. Expand the **Authorization Policy - Global Exceptions** section.
9. Click the **+** plus sign to add a new policy.
10. Click the **+** plus sign under **Conditions.**
11. Select the field **Session – ANCPolicy.**
12. Select the quarantine action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



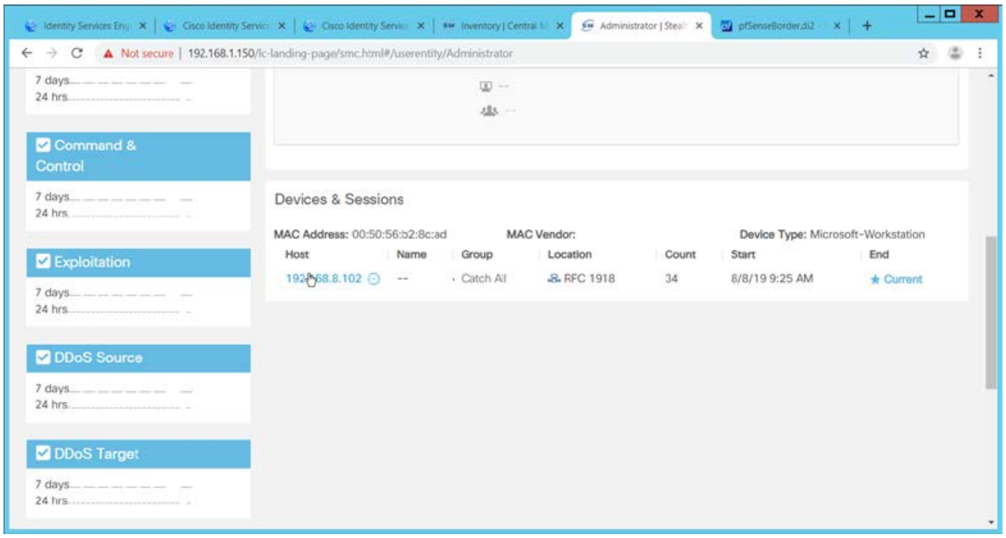
13. Click **Use.**
14. Select the **Deny Access** profile; the profile selected here will be applied to the machine when the machine is added to the quarantine group.
15. Select **Quarantined_Systems** for **Security Groups.**



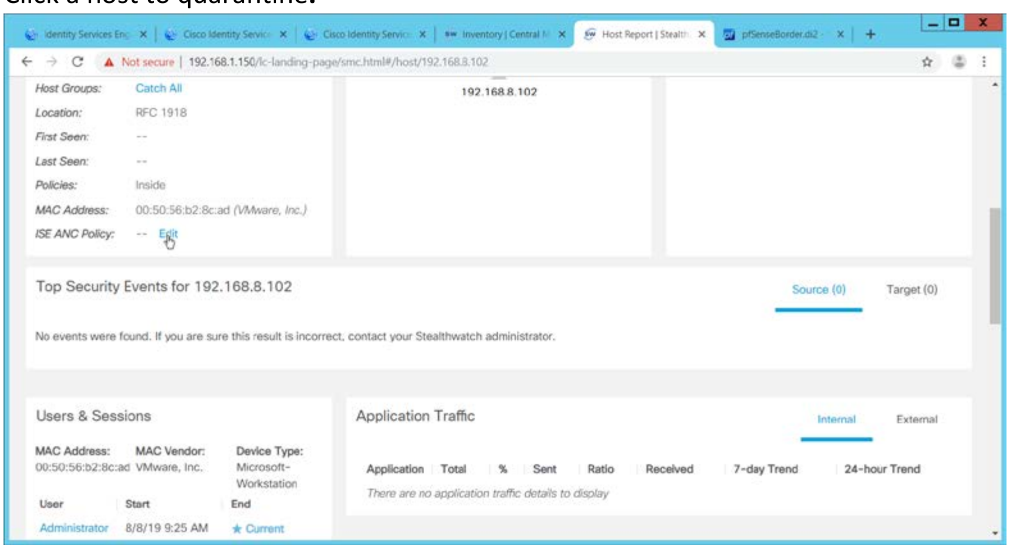
16. Click **Save.**
17. In the SMC web console, click **Monitor > Users.**



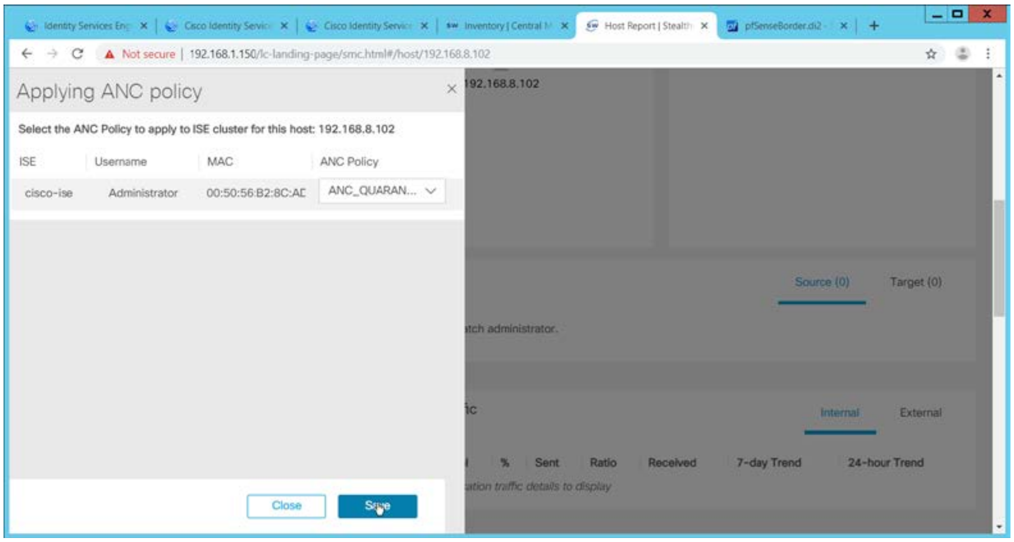
18. Select a user to quarantine.



19. Click a host to quarantine.



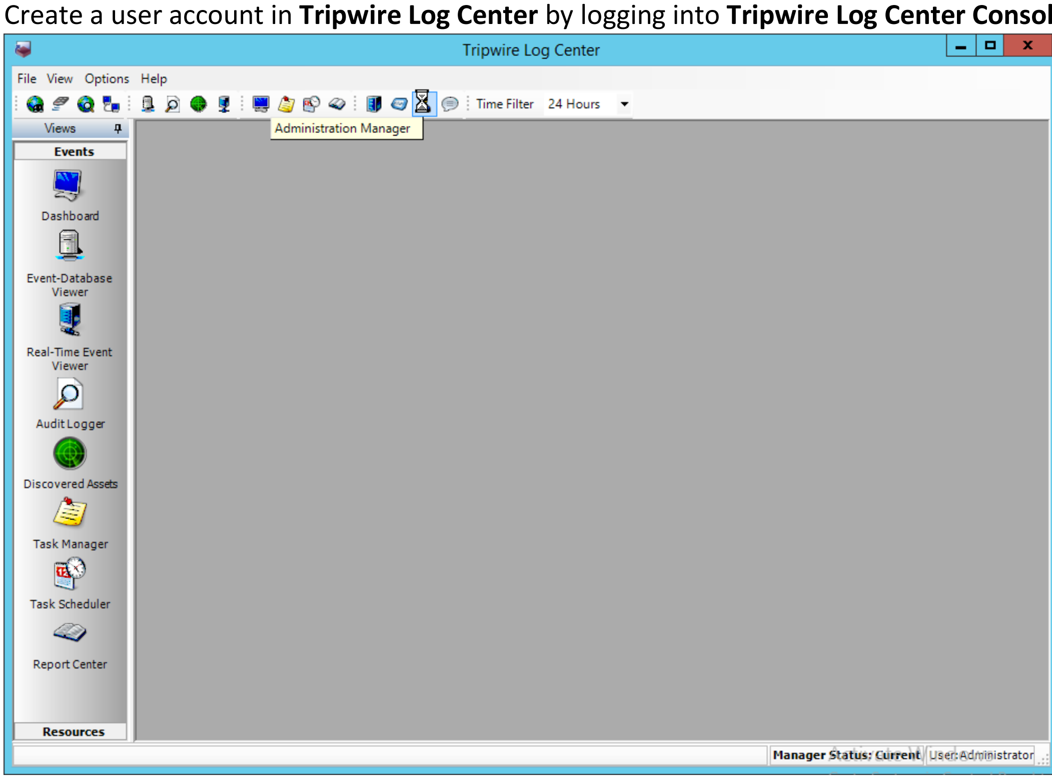
20. Click **Edit** next to **ISE ANC Policy.**
21. From the drop down, select the quarantine action you created earlier.



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

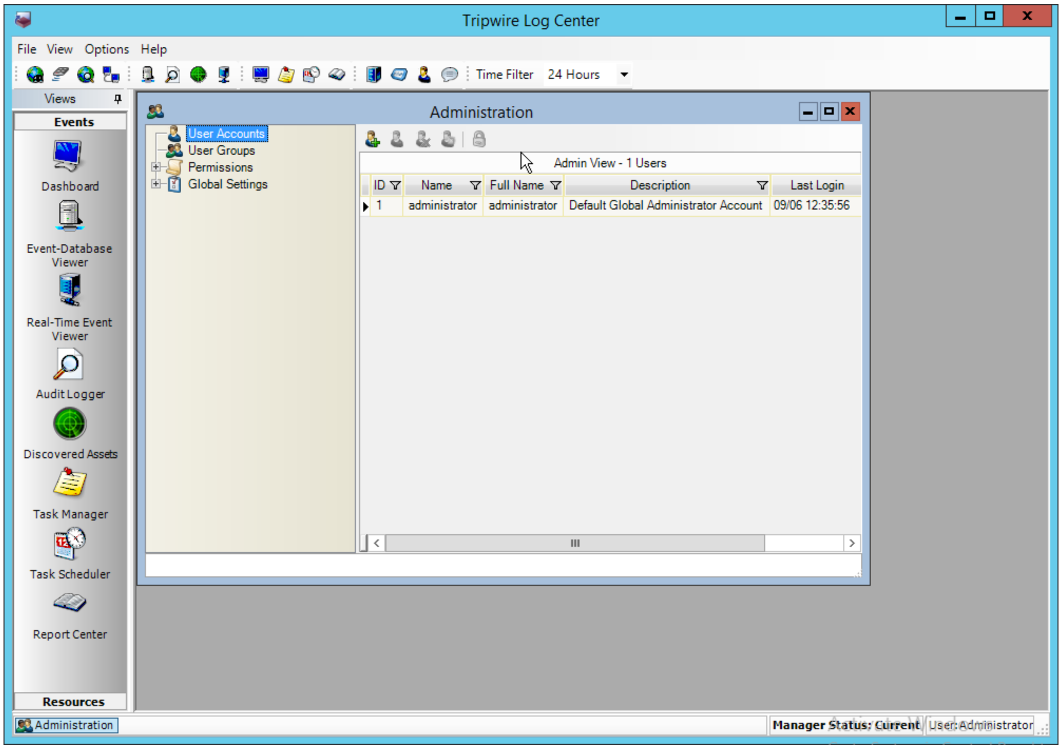
2.17 Integration: Tripwire Log Center and Tripwire Enterprise

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

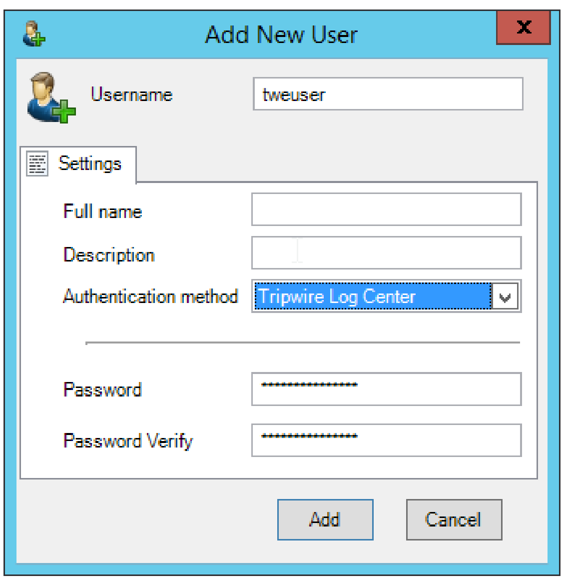


2. Click the **Administration Manager** button.

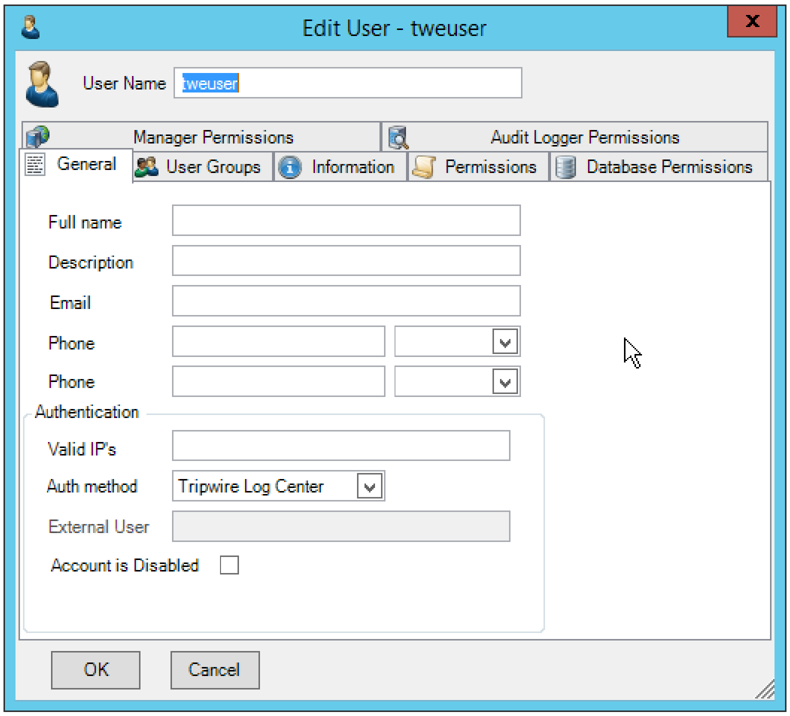
3. Click **User Accounts.**



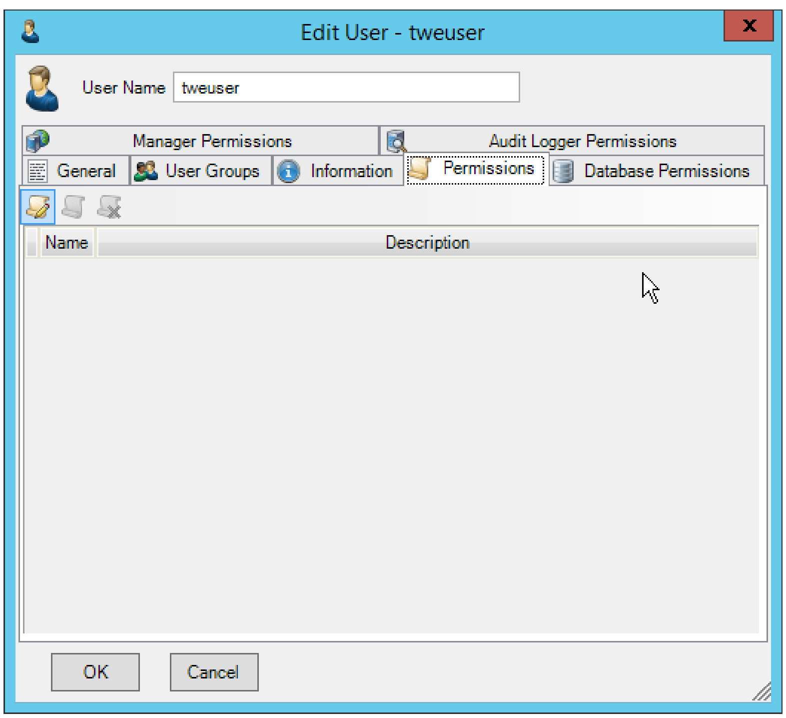
4. Click the **Add** button.
5. Enter the details of the user.



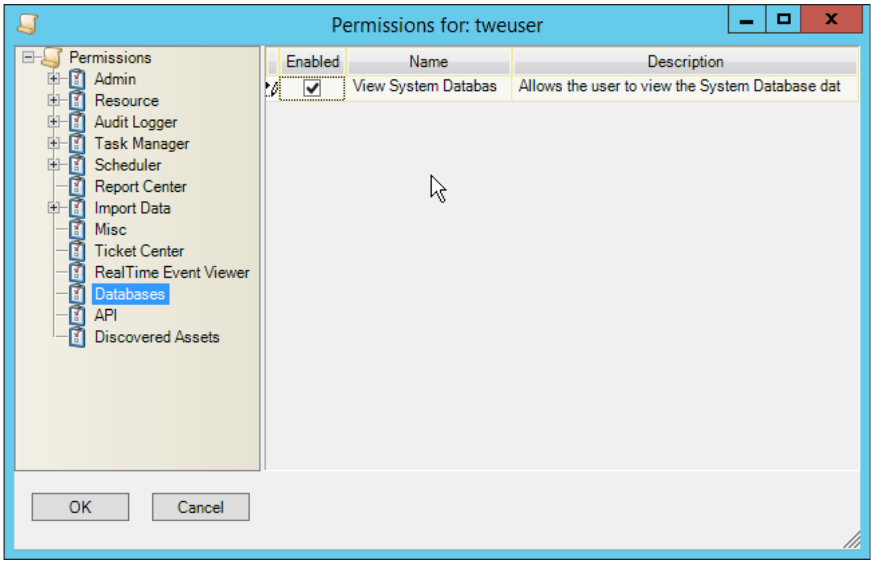
6. Click **Add.**
7. Double-click the user account.



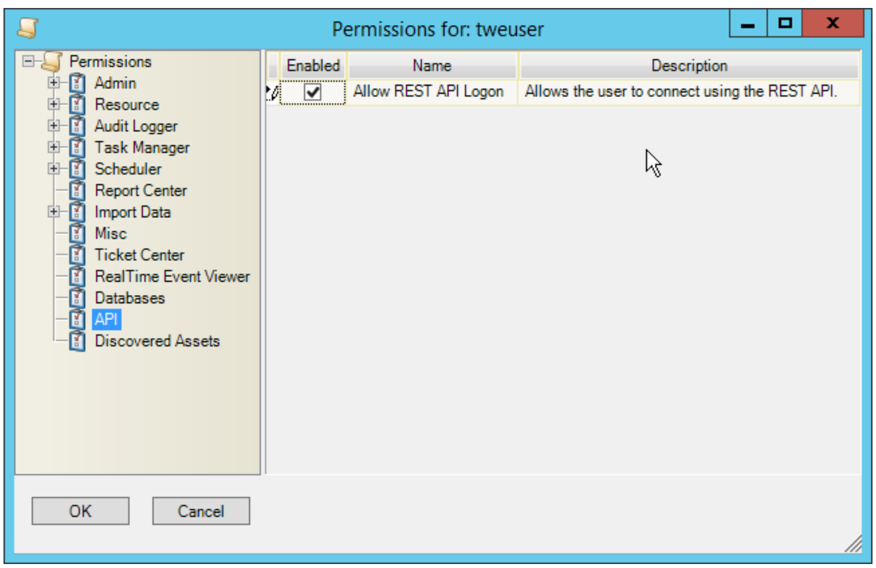
8. Click the **Permissions** tab.



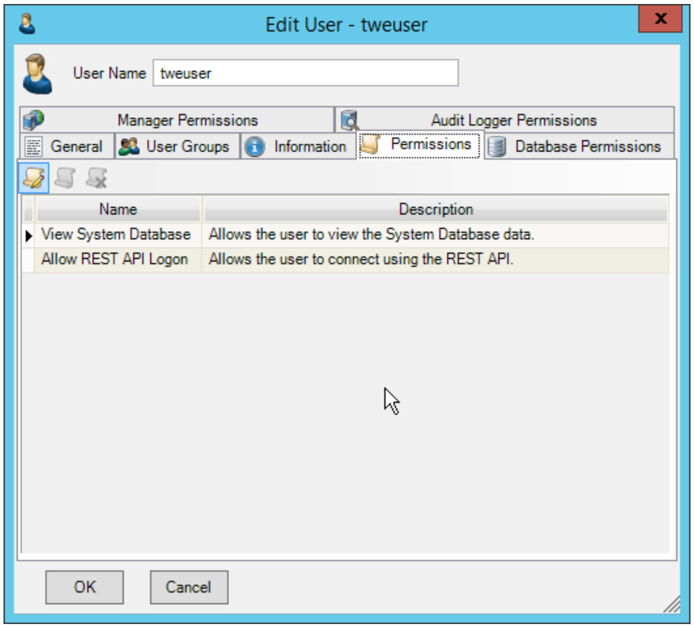
9. Click **Edit list of permissions.**
10. Select **Databases.**



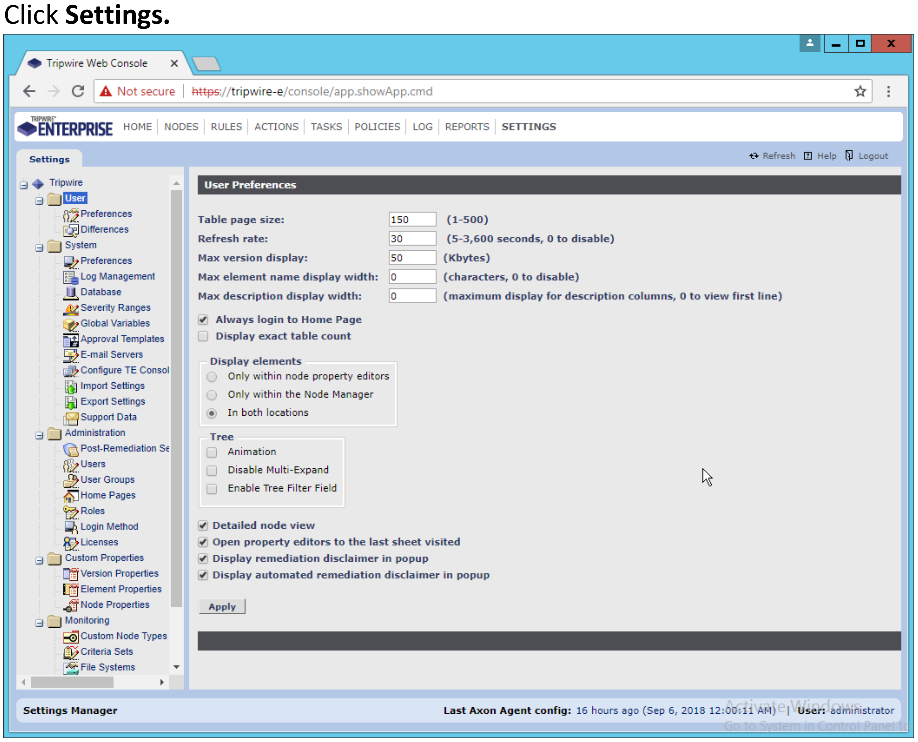
11. Check the box next to **View System Database.**
12. Select **API.**



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

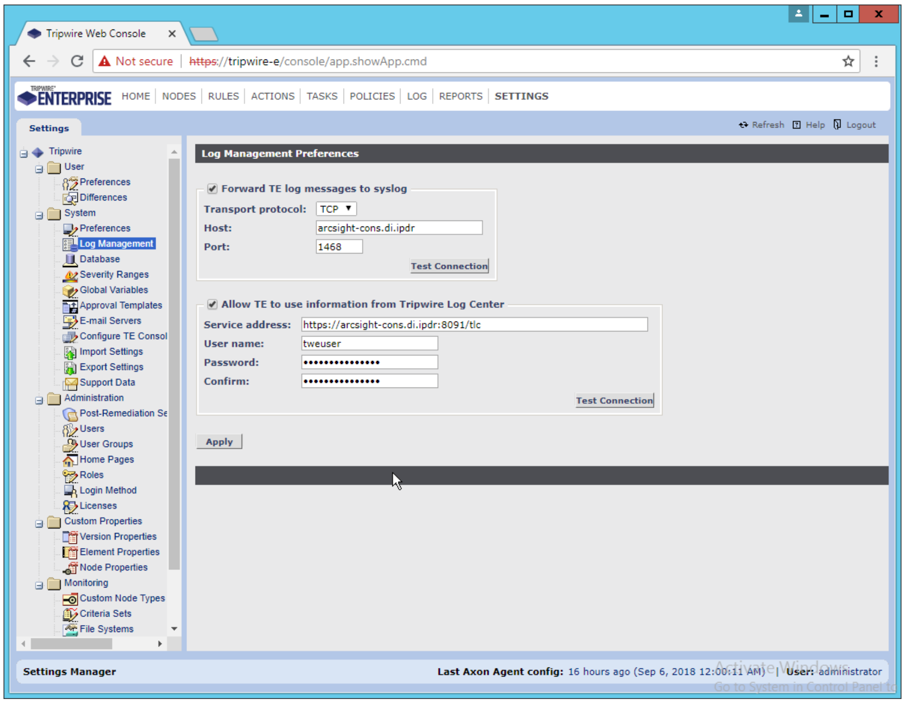


14. Click **OK.**
15. Click **OK.**
16. Log in to the **Tripwire Enterprise** web console.
17. Click **Settings.**

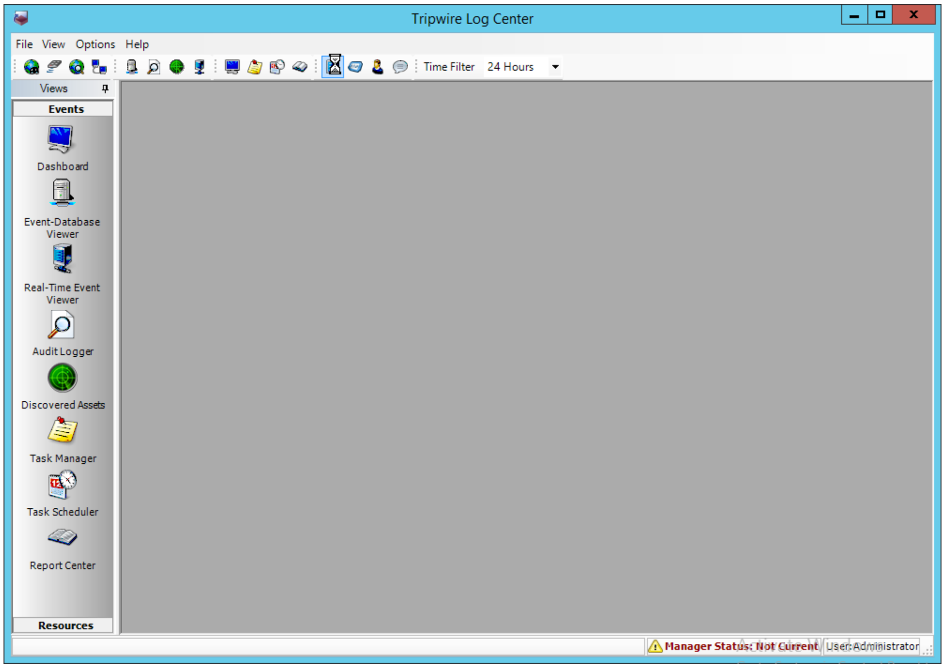


18. Go to **System** > **Log Management.**

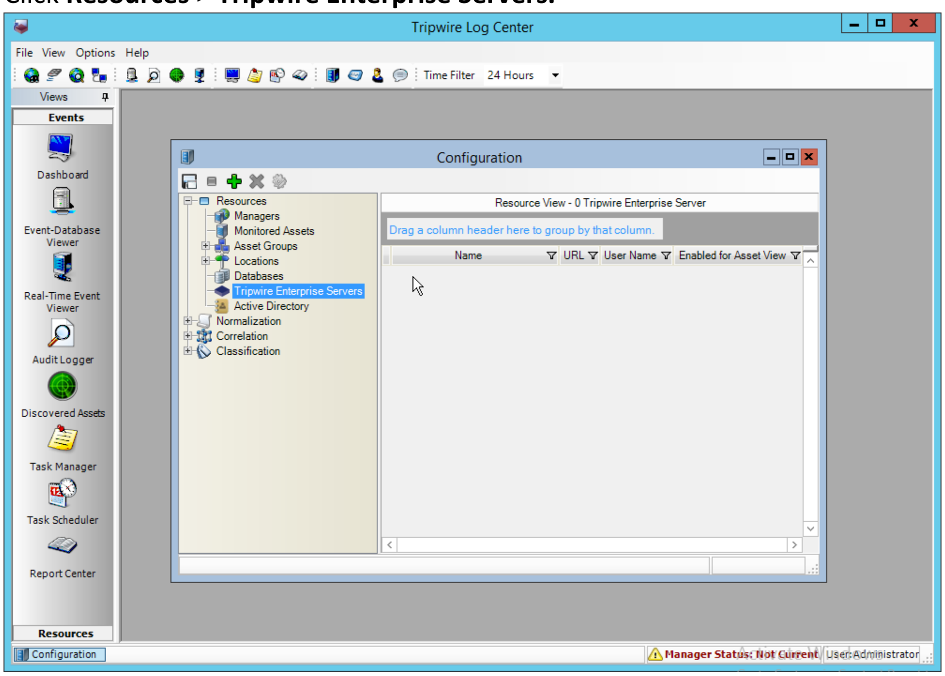
19. Check the box next to **Forward TE log messages to syslog.**
20. Enter the **hostname** and **port** of the **Tripwire Log Center** server. The default port is **1468.**
21. Check the box next to **Allow TE to use information from Tripwire Log Center.**
22. Enter the **service address** like this: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



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

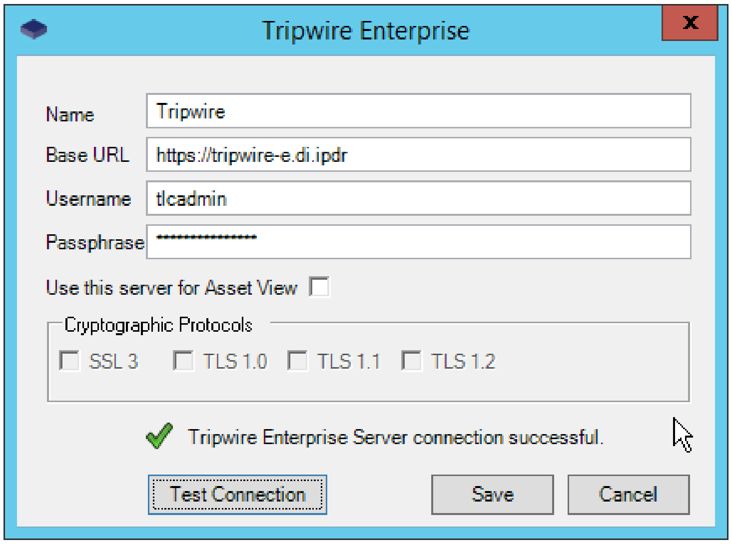


27. Click **Configuration Manager.**
28. Click **Resources** > **Tripwire Enterprise Servers.**



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

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



33. Click **Save.**

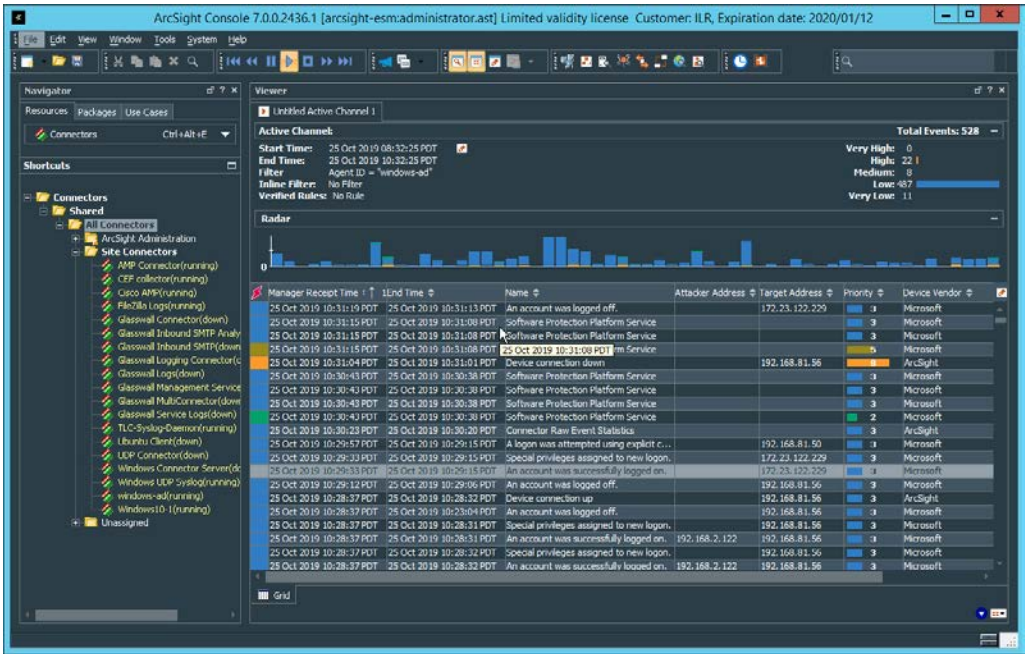
2.18 Integration: Symantec ICA and ArcSight ESM

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

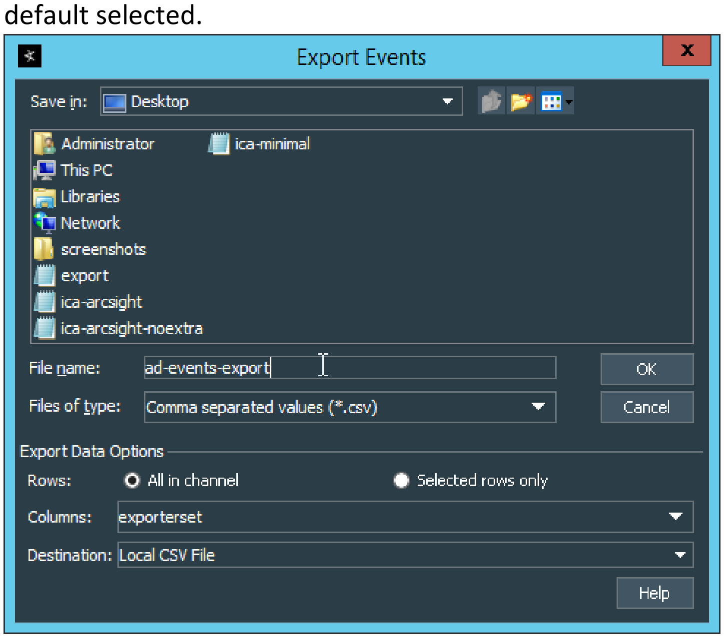
- On the version of Symantec ICA we are using, it is required to replace empty fields in the CSV with NULL. This may be unnecessary in future updates.
- The CSV file should be in a location accessible to the ICA server. You can replace this file with a new CSV file on a daily basis, and Symantec ICA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

2.18.1 Export the CSV File from ArcSight Console

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



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

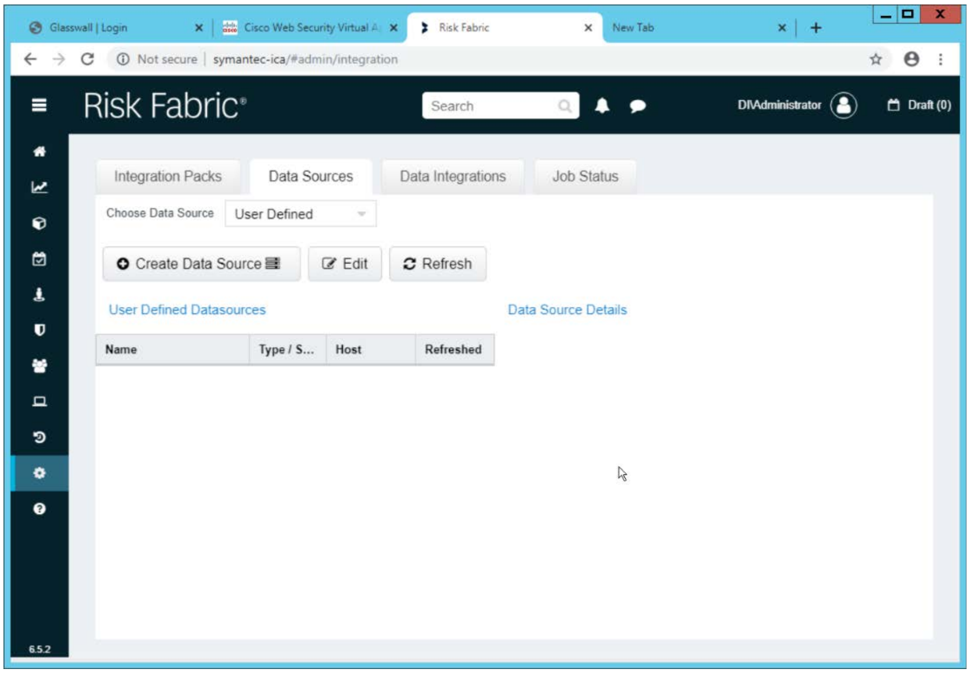


7. Click **OK.**

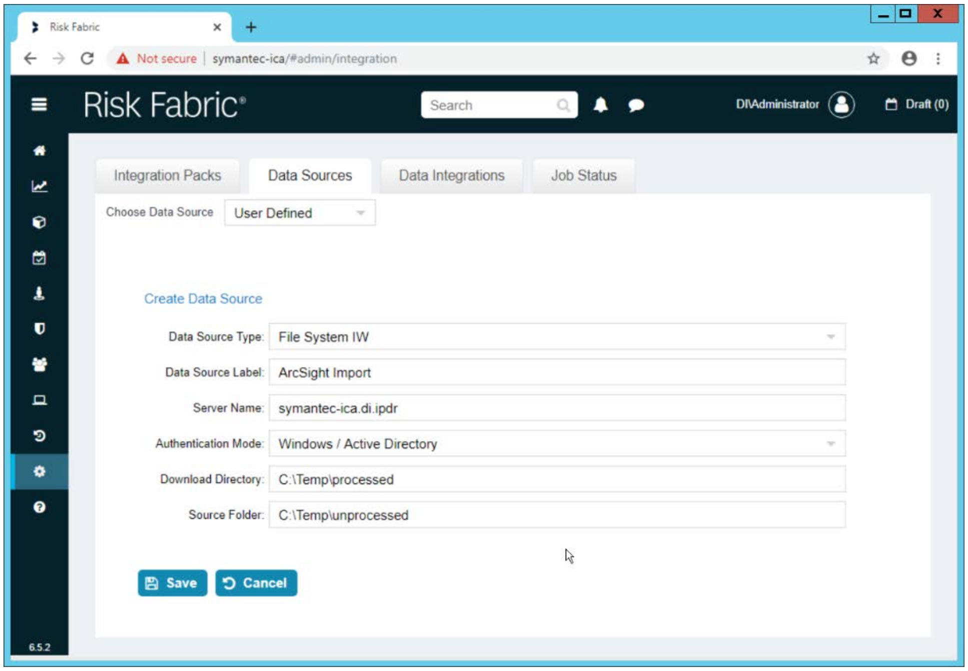
8. Move the file to the desired location for ICA to collect. (Ensure that if required for your version of Symantec ICA, all empty fields are replaced with "NULL") For the purposes of this demonstration, we moved it to *C:\Temp\unprocessed* on the Symantec ICA server.

2.18.2 Import the CSV File to Symantec ICA

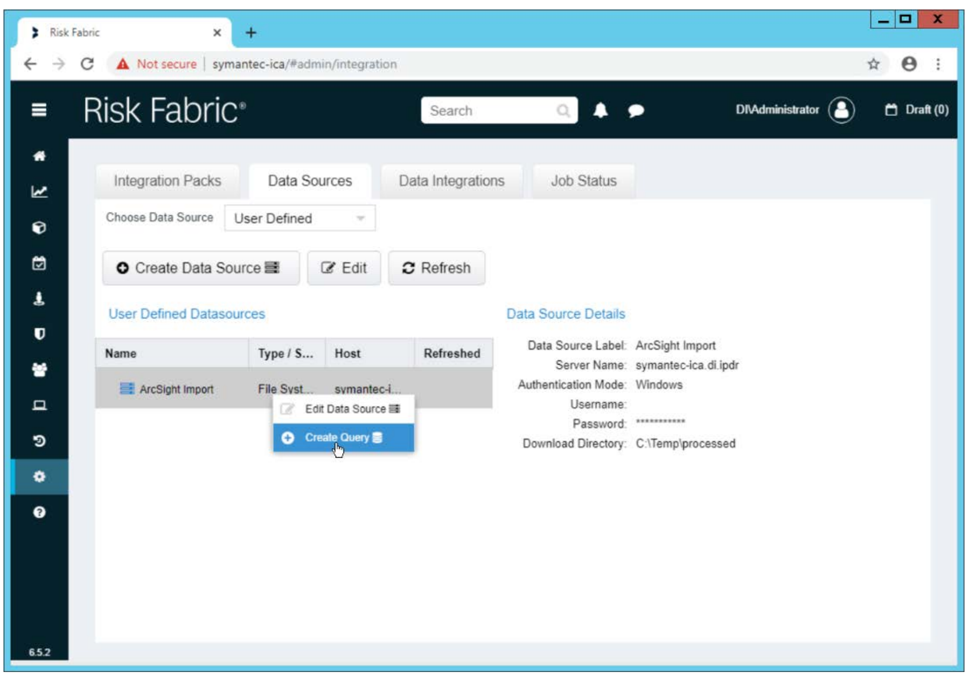
1. On the Symantec ICA web console, navigate to **Gear Icon > Integration.**
2. Click the **Data Sources** tab.



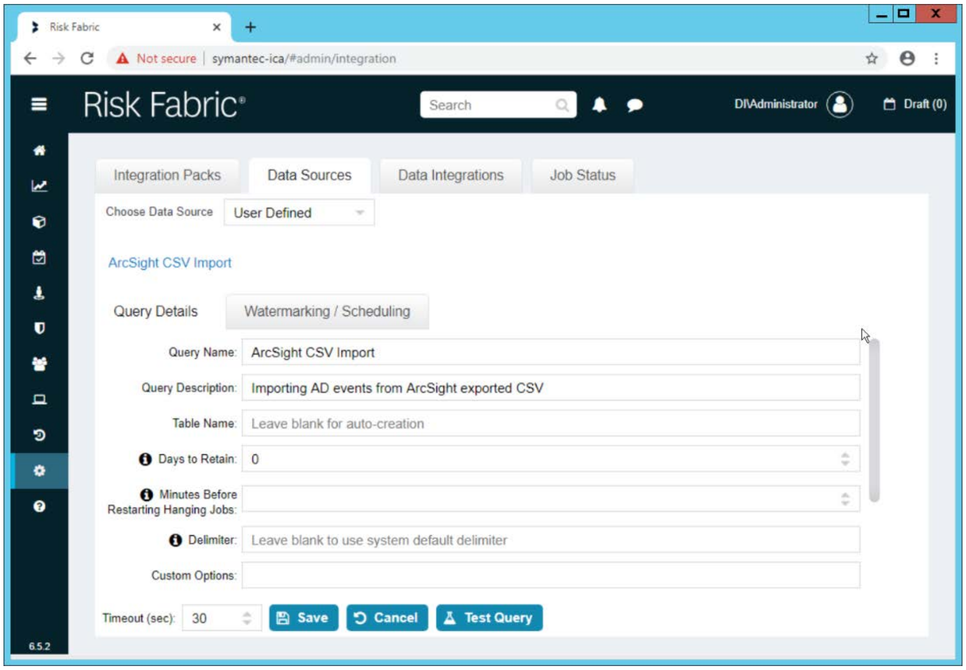
3. Select **User Defined** for **Choose Data Source.**
4. Click **Create Data Source.**
5. Select **File System IW** for the **Data Source Type.**
6. Enter a name for the data source for **Data Source Label.**
7. Enter the hostname of the Symantec ICA server for **Server Name.**
8. Select **Windows/Active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



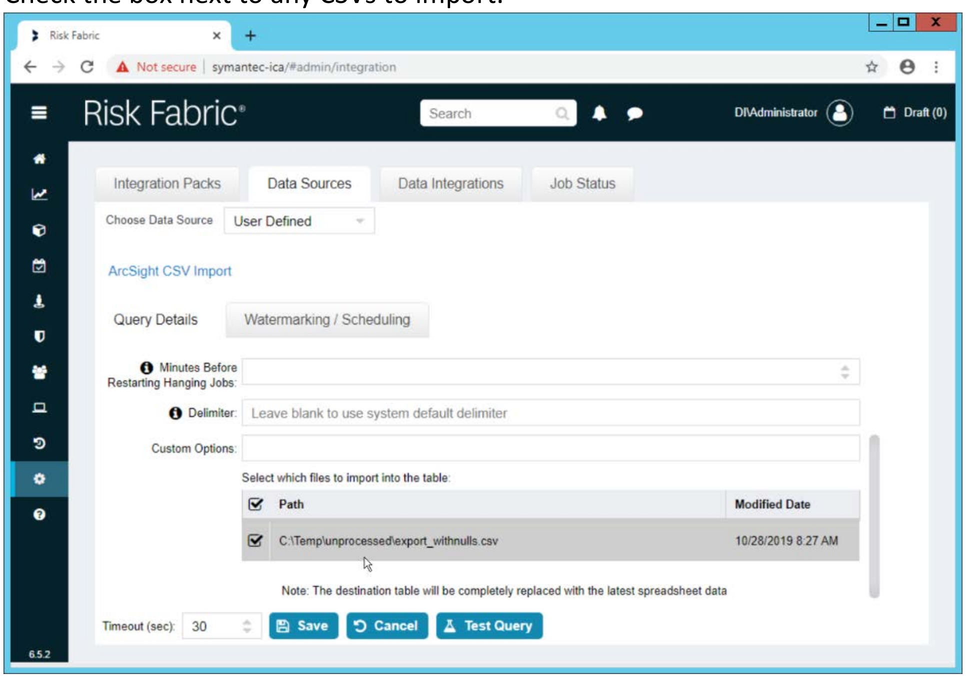
11. Click **Save.**



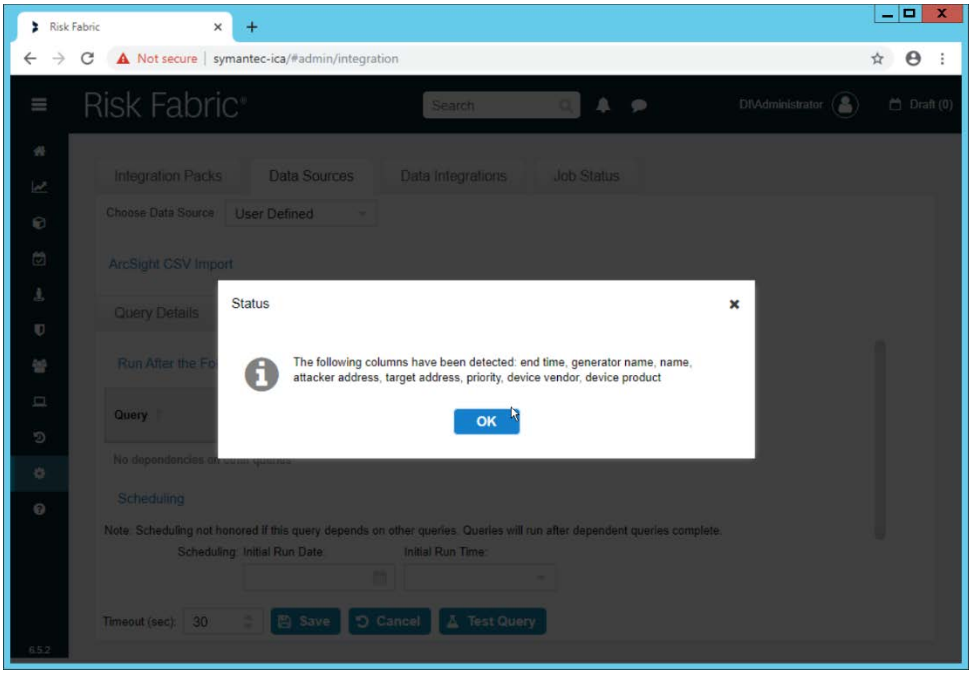
12. Right-click the newly created data source and select **Create Query.**
13. Enter a **Query Name** and **Query Description.**



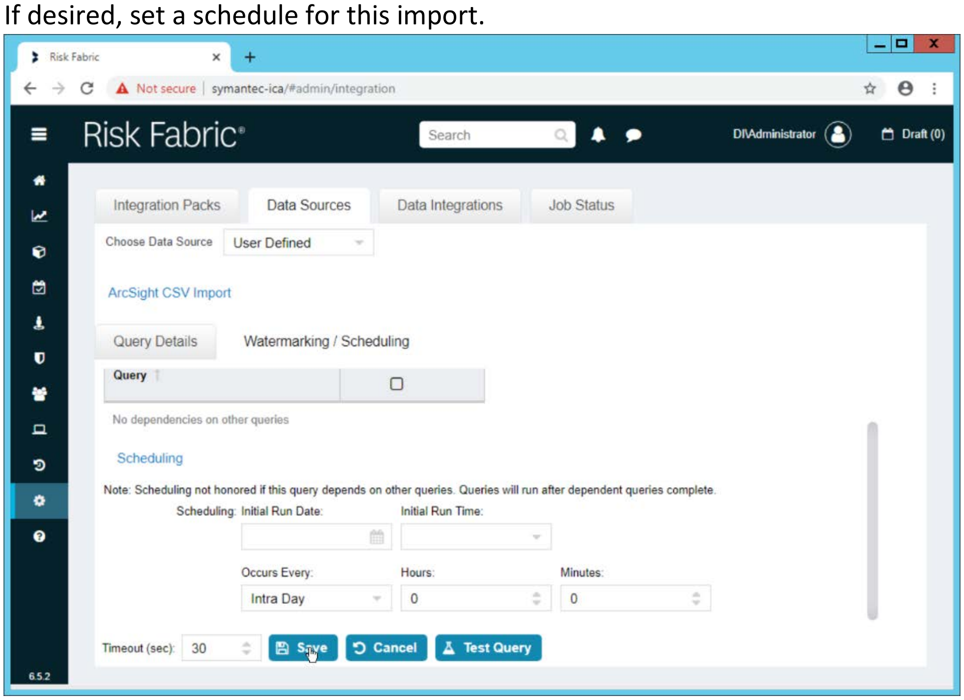
14. If you specified the **Source Folder** correctly, you will see the CSV file listed.
15. Check the box next to any CSVs to import.



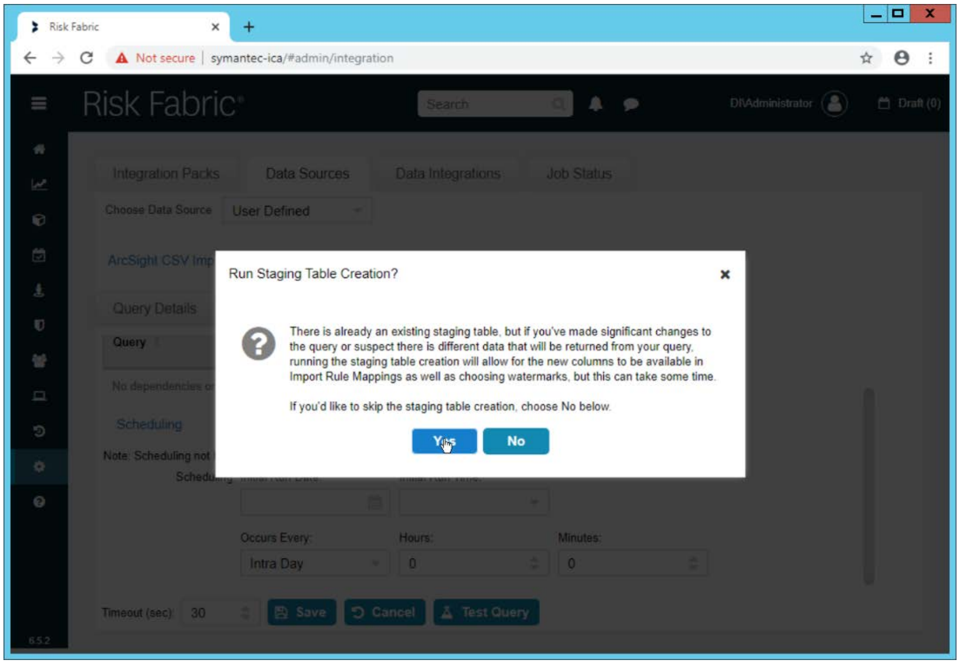
16. Click **Save.**



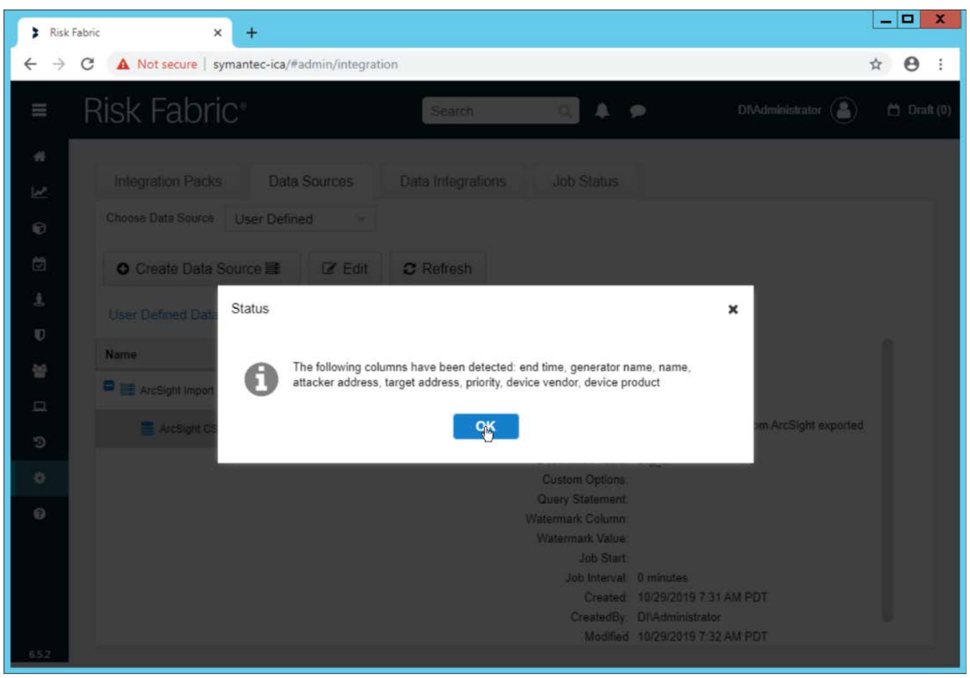
17. Click **OK.**
18. If desired, set a schedule for this import.



19. Click **Save.**



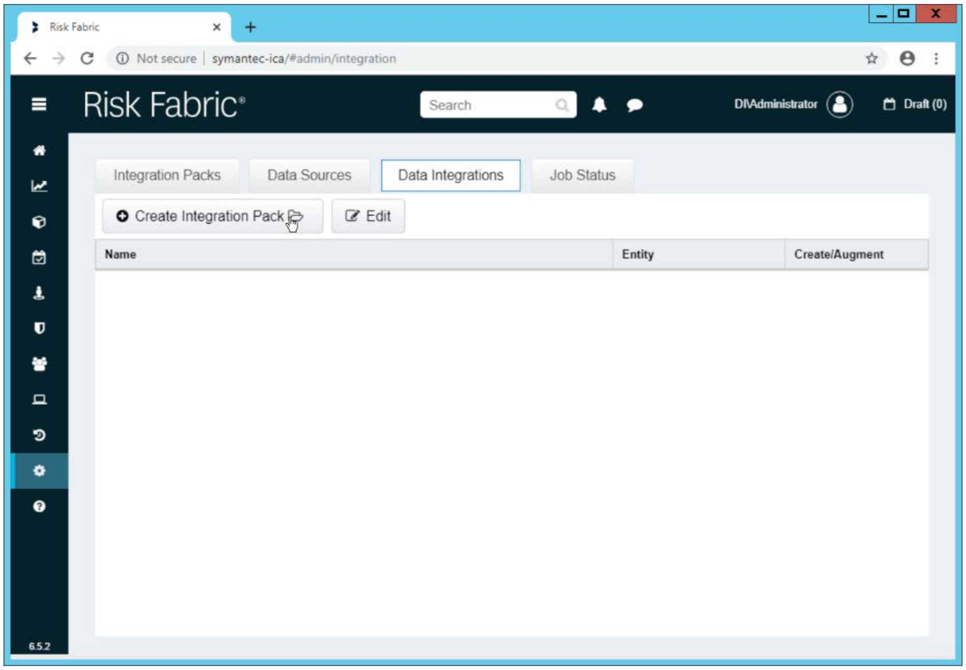
20. Click **Yes.**



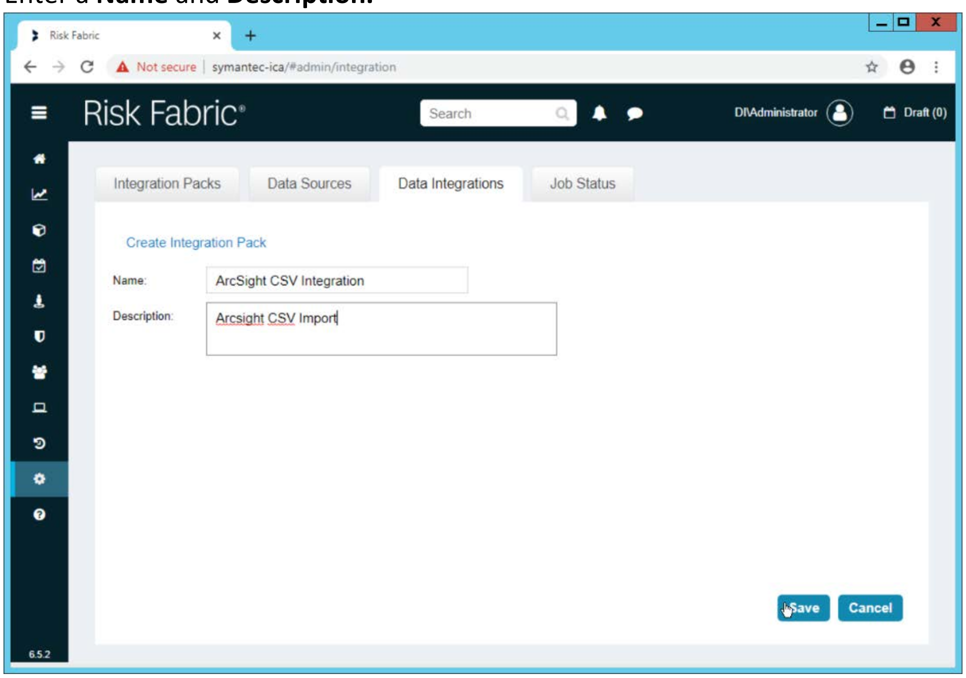
21. Click **OK.**

2.18.3 Create a Mapping between ArcSight events and Symantec ICA

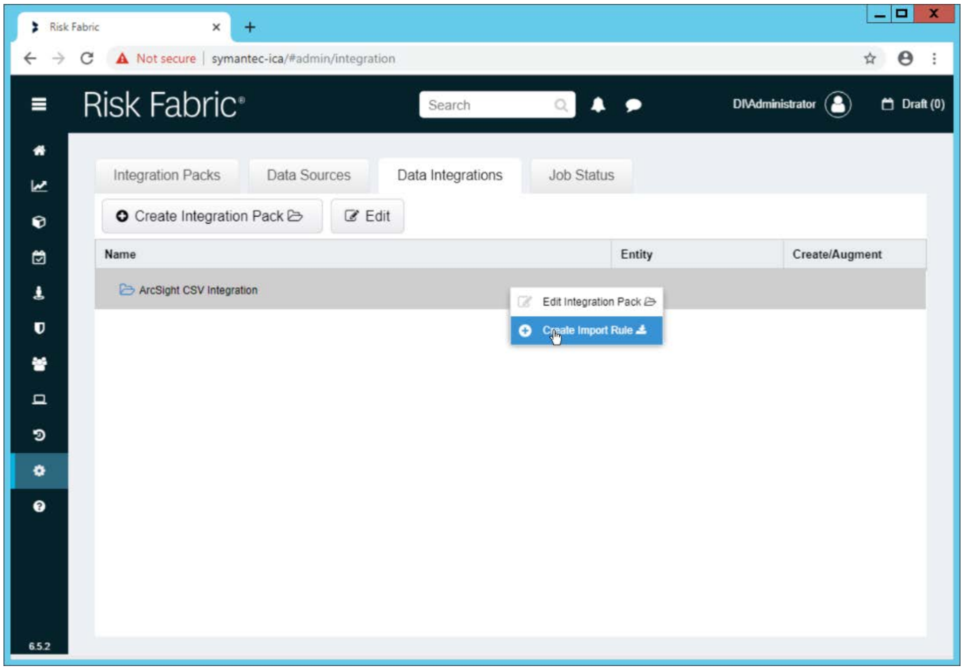
1. Navigate to the **Data Integrations** tab.



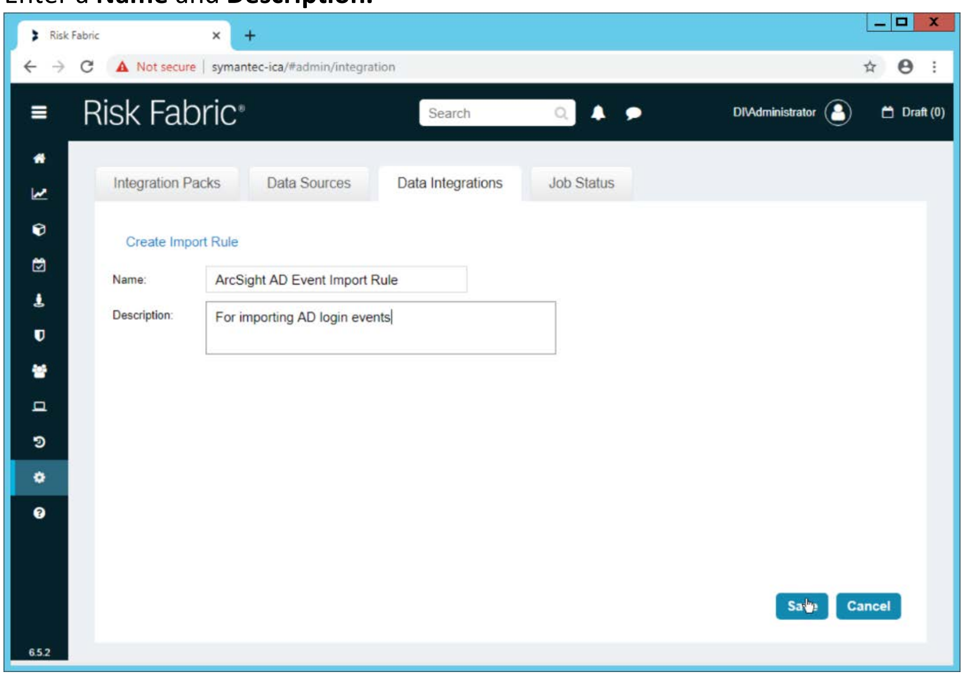
2. Click **Create Integration Pack.**
3. Enter a **Name** and **Description.**



4. Click **Save.**

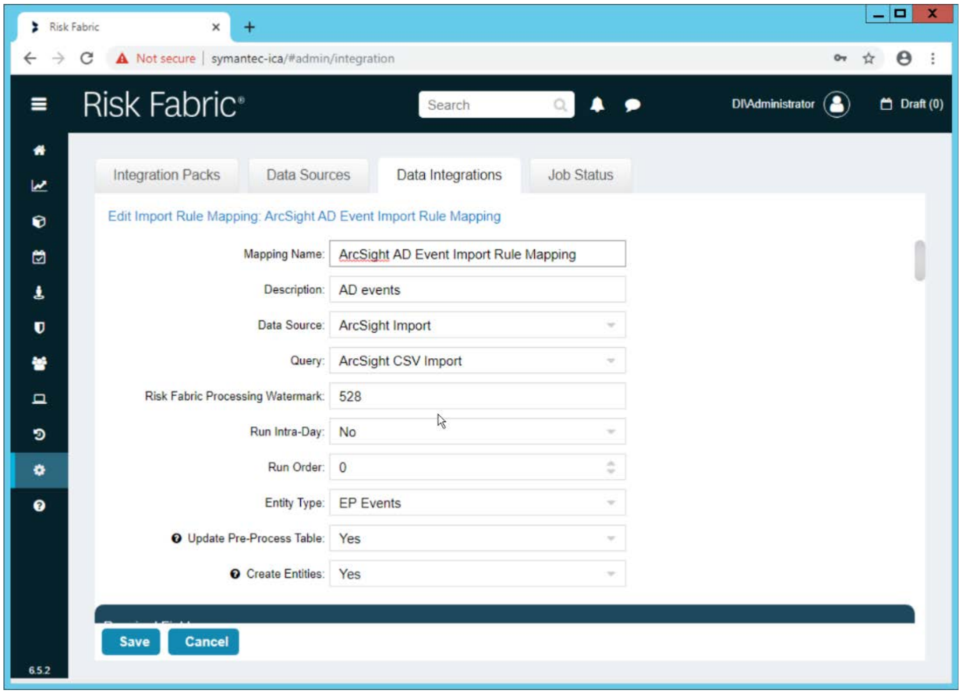


5. Right-click the newly created Integration Pack, and select **Create Import Rule.**
6. Enter a **Name** and **Description.**

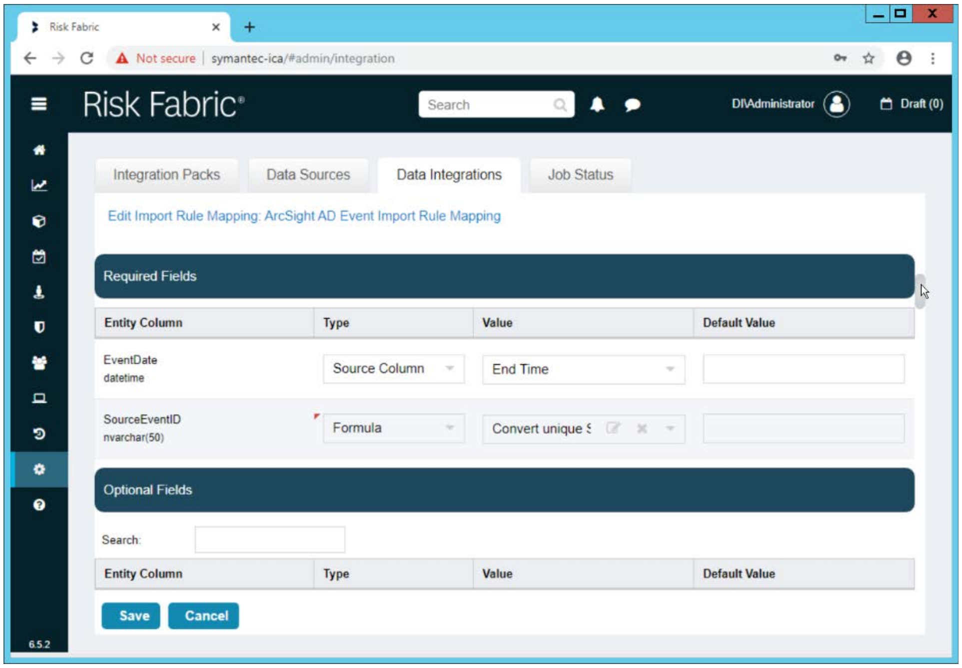


7. Click **Save.**
8. Right-click the newly created **Import Rule** and select **Create Import Rule Mapping.**
9. Enter a **Name** for the mapping.

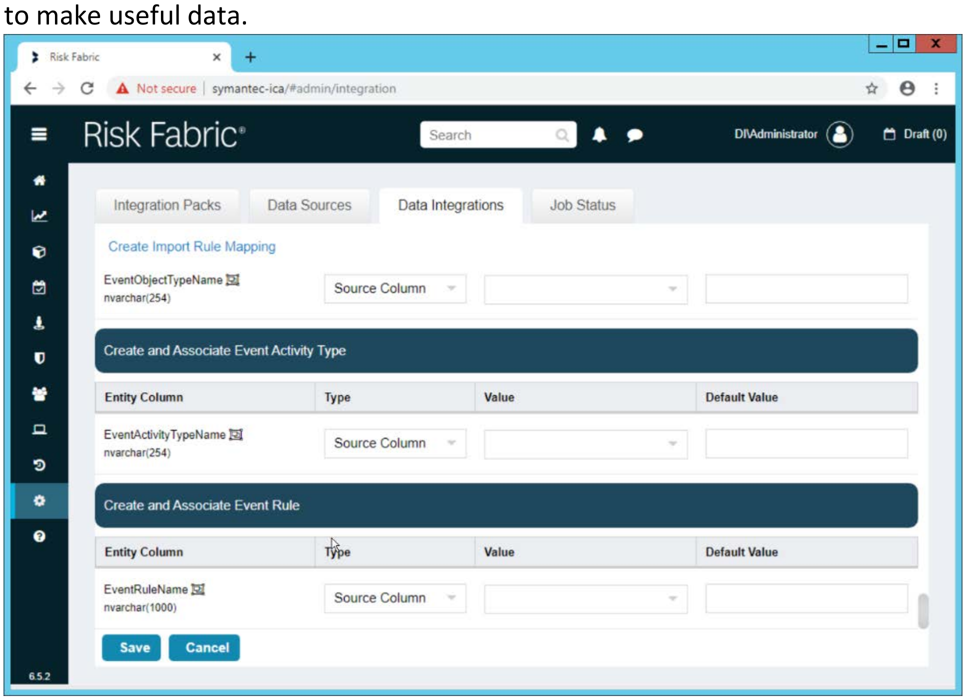
10. Enter a **Description.**
11. Select the **Data Source** created earlier.
12. Select the **Query** created earlier.
13. Select **EP Events** for the **Entity Type** (or explore other Entity Types that may better match the events you are importing).



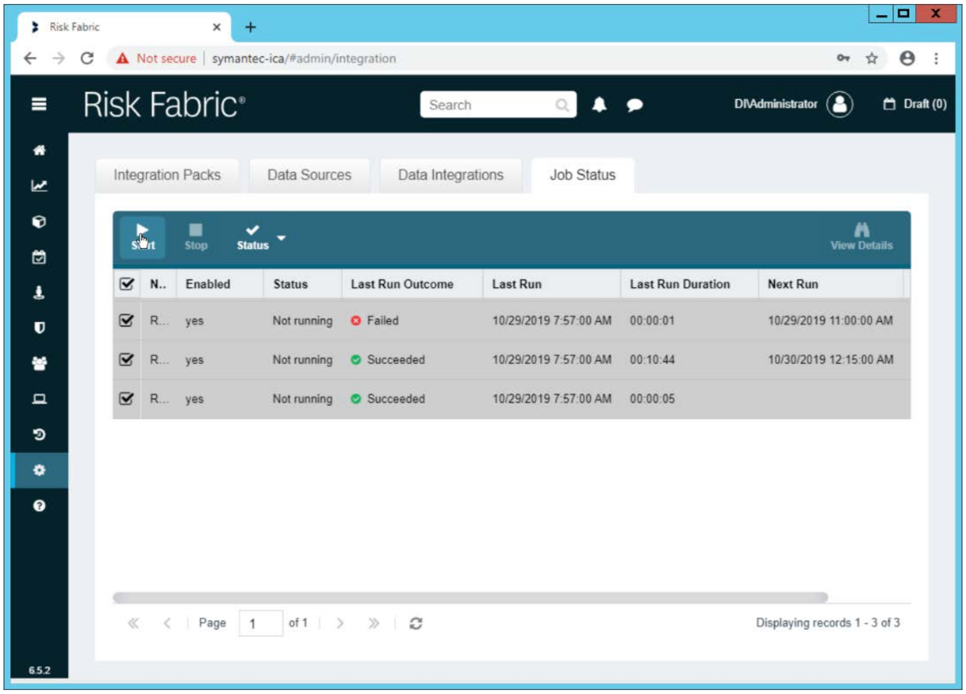
14. Below, the **Entity Column** refers to the target field in ICA to which a field is being mapped. Map event fields from the CSV to fields in the Entity Column.
15. For example, **EventDate** in ICA corresponds directly to the **End Time** in ArcSight, so we select that value directly as a **Source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



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



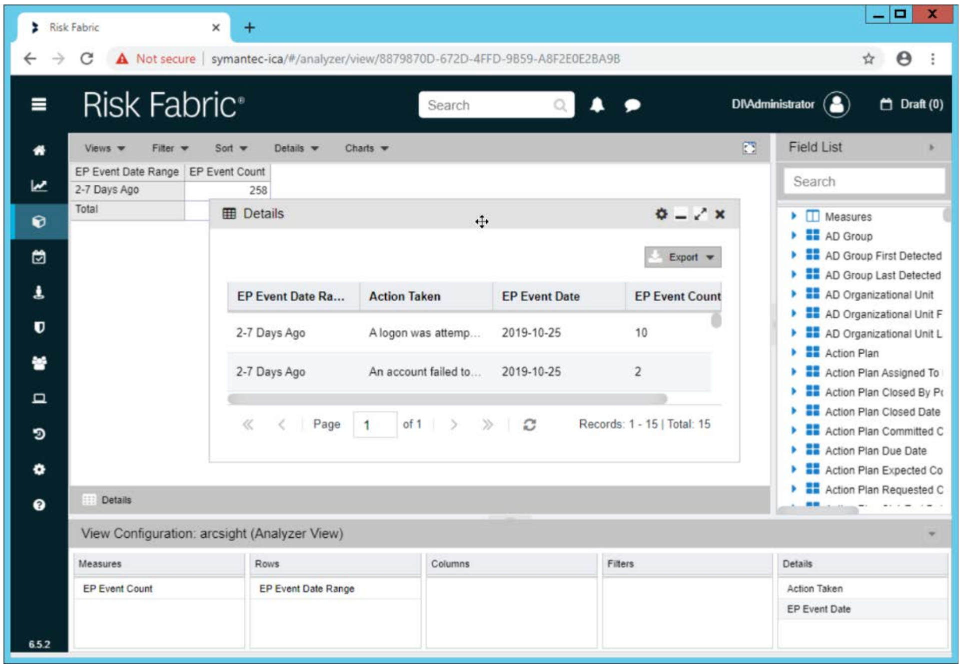
18. Click **Save** when finished.
19. Navigate to the **Job Status** tab.



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

2.18.4 View ArcSight Events in the Analyzer

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



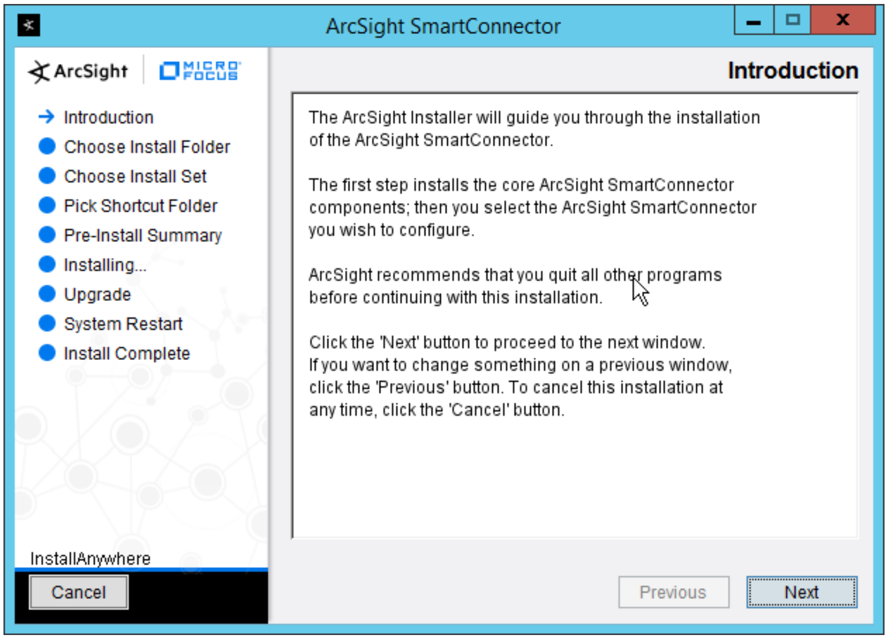
2. Drag mapped columns (from the import rule mapping you created) from the list on the right to view them in the analyzer.

2.19 Integration: Micro Focus ArcSight and Tripwire

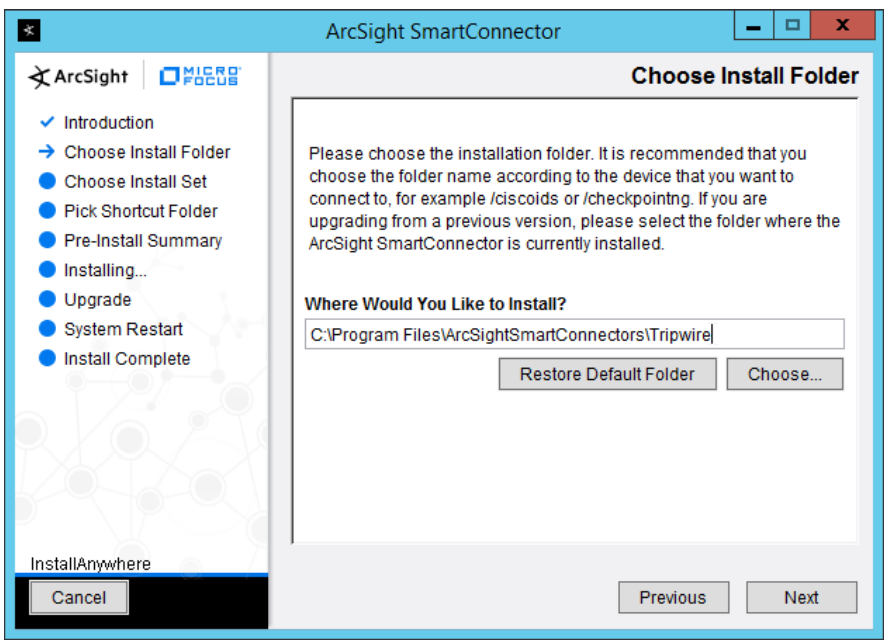
This section will detail the forwarding of logs from **Tripwire Log Center** to **Micro Focus ArcSight.** This will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight,** assuming those logs are being collected by **Tripwire Log Center.**

2.19.1 Install Micro Focus ArcSight

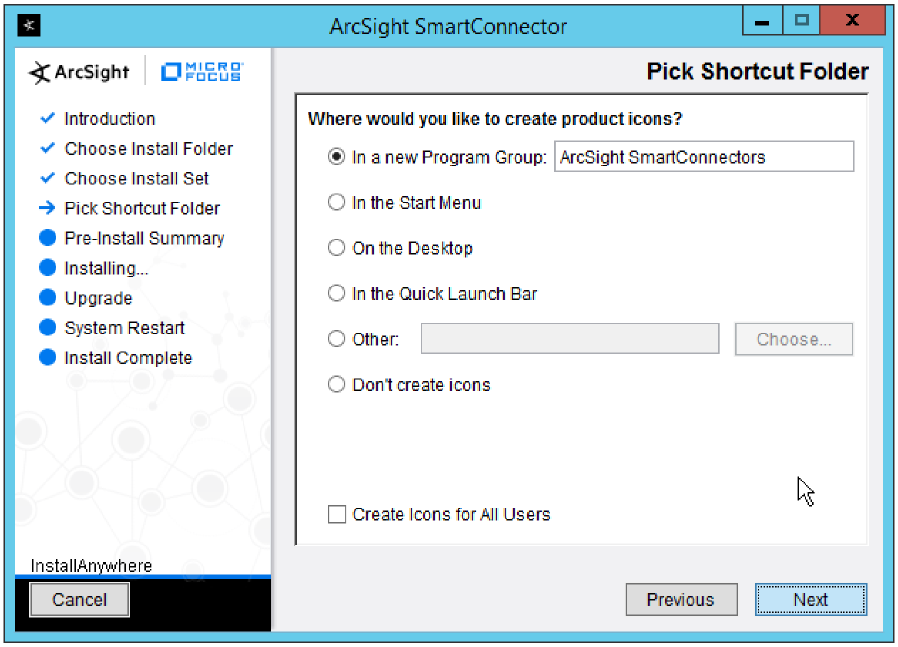
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Tripwire Log Center.**



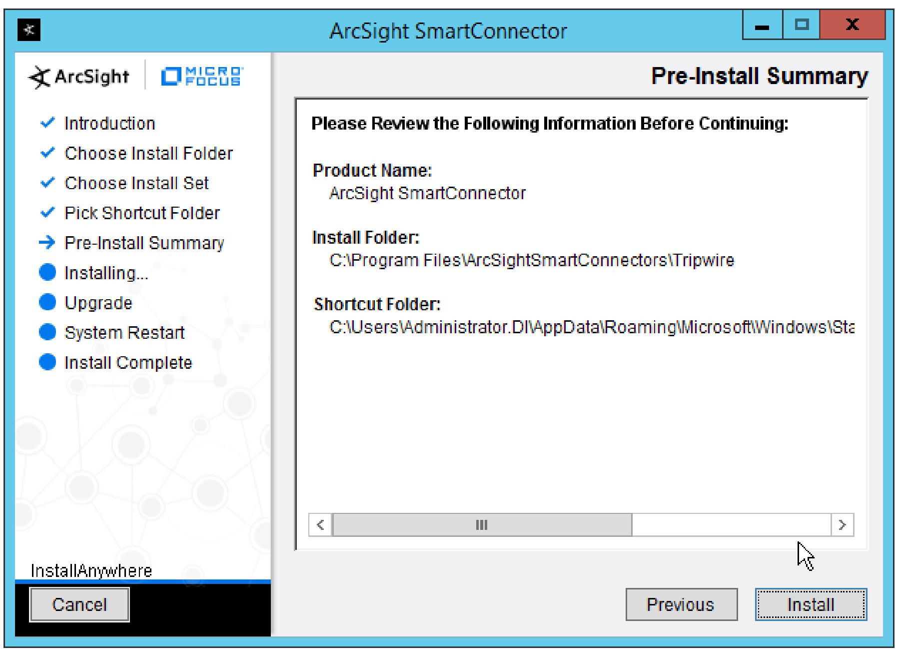
2. Click **Next.**



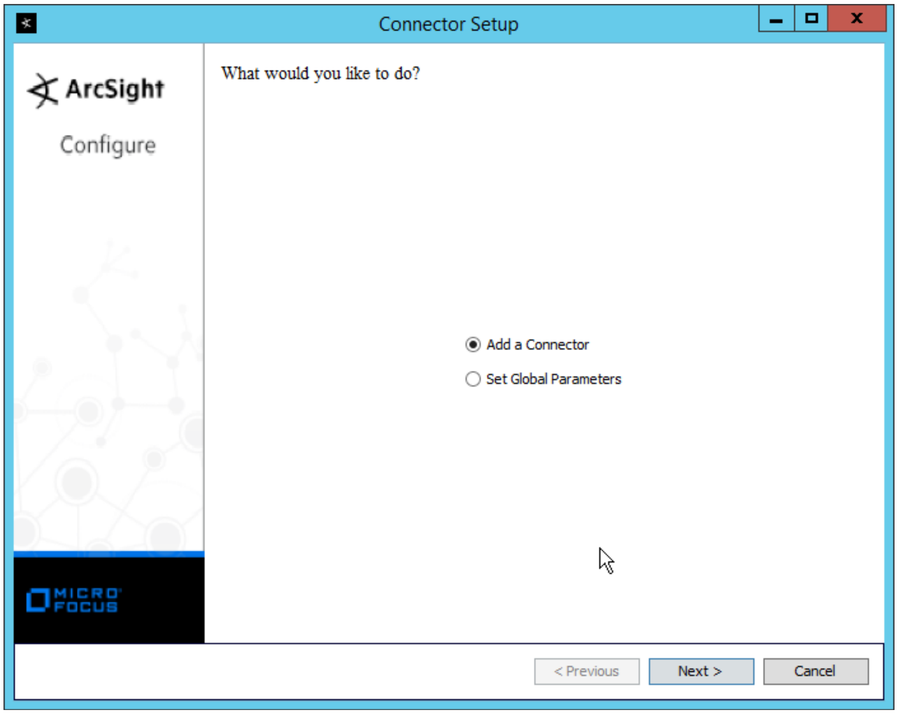
3. Enter *C:\Program Files\ArcSightSmartConnectors\Tripwire.*



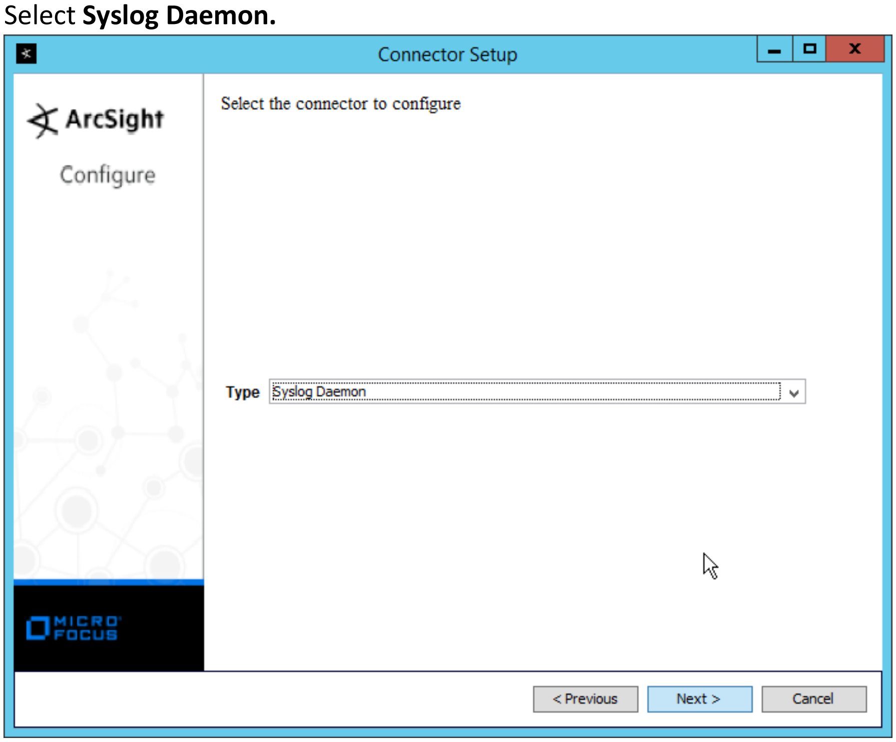
4. Click **Next.**



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

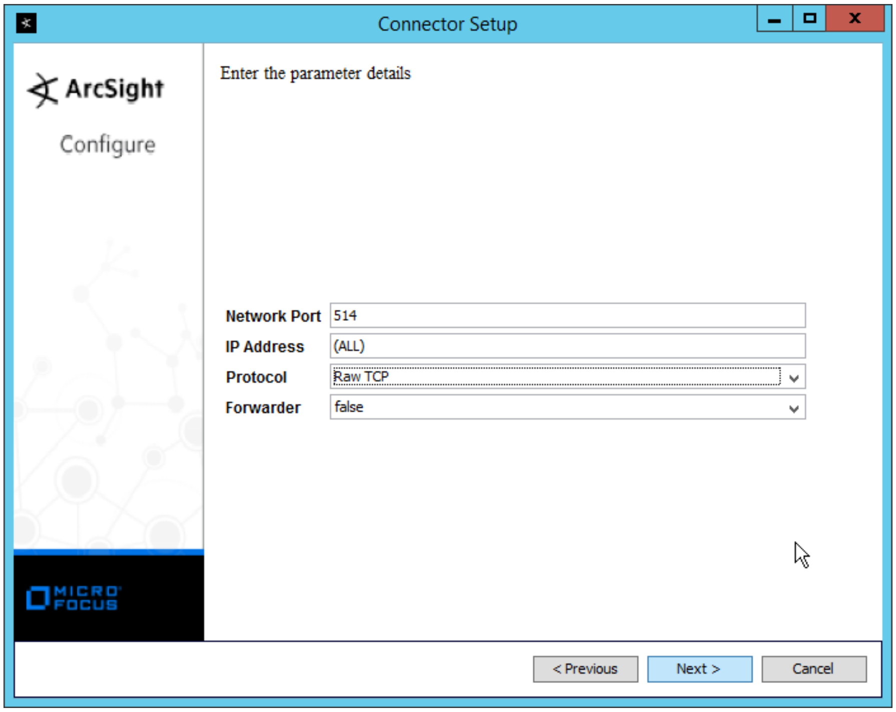


7. Click **Next.**
8. Select **Syslog Daemon.**

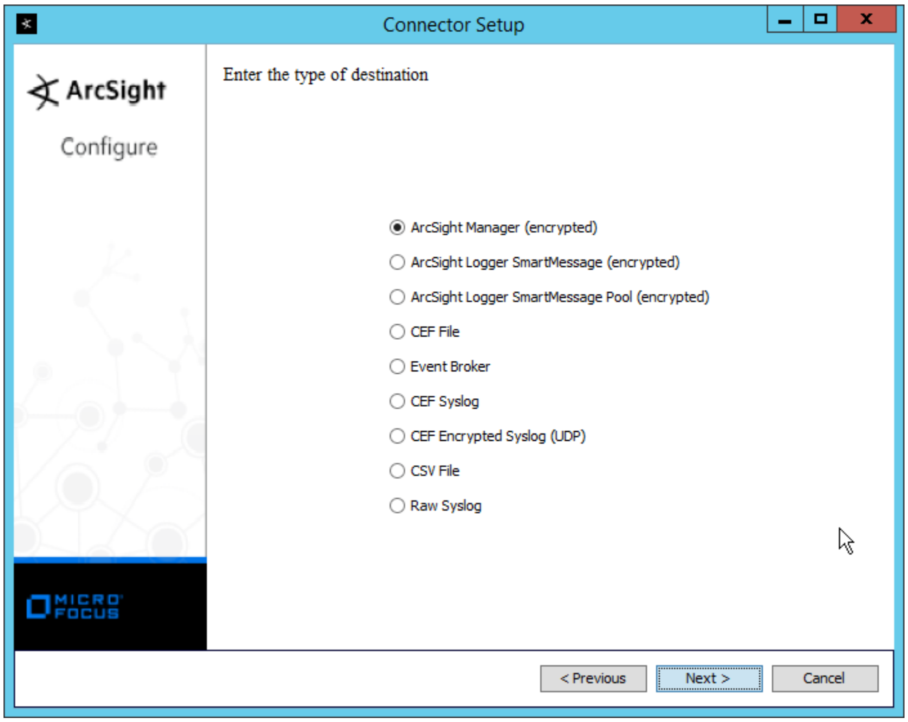


9. Click **Next.**

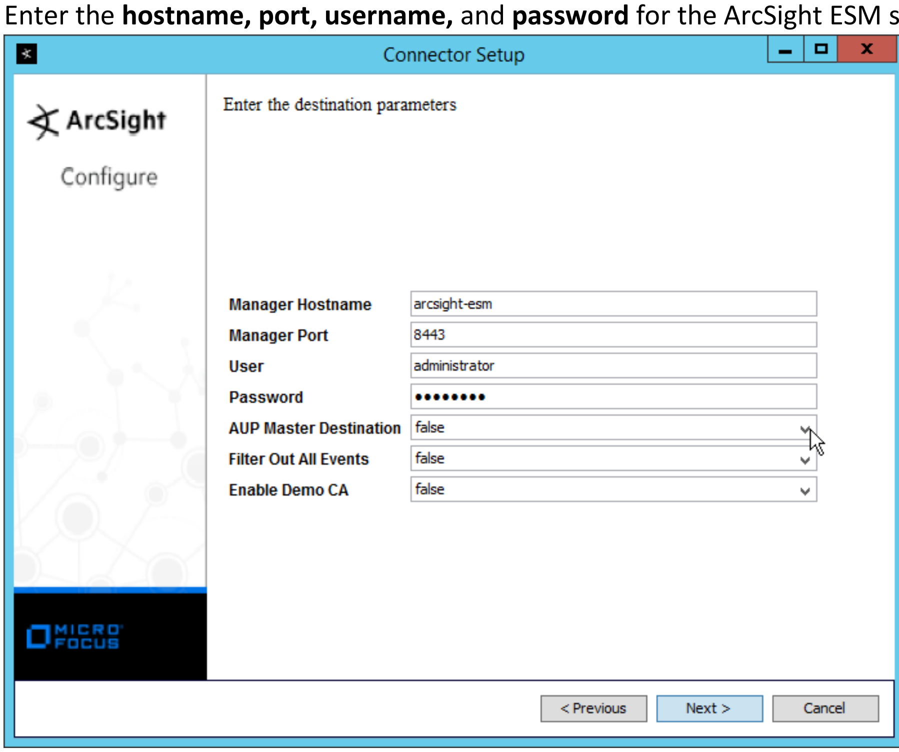
10. Enter a port for the daemon to run on.
11. Select **Raw TCP** for **Protocol.**



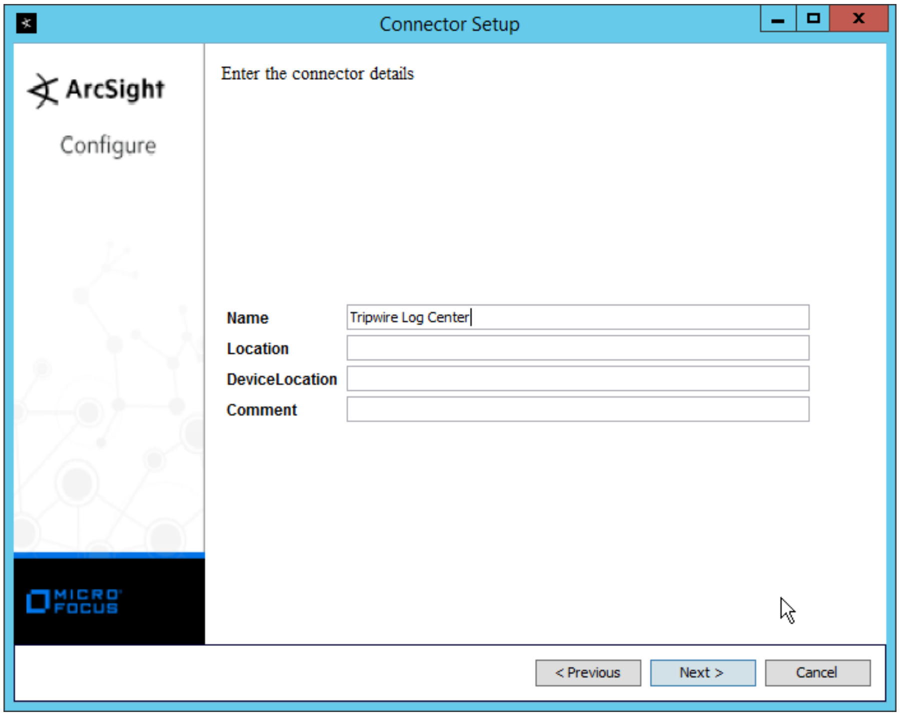
12. Click **Next.**
13. Select **ArcSight Manager (encrypted).**



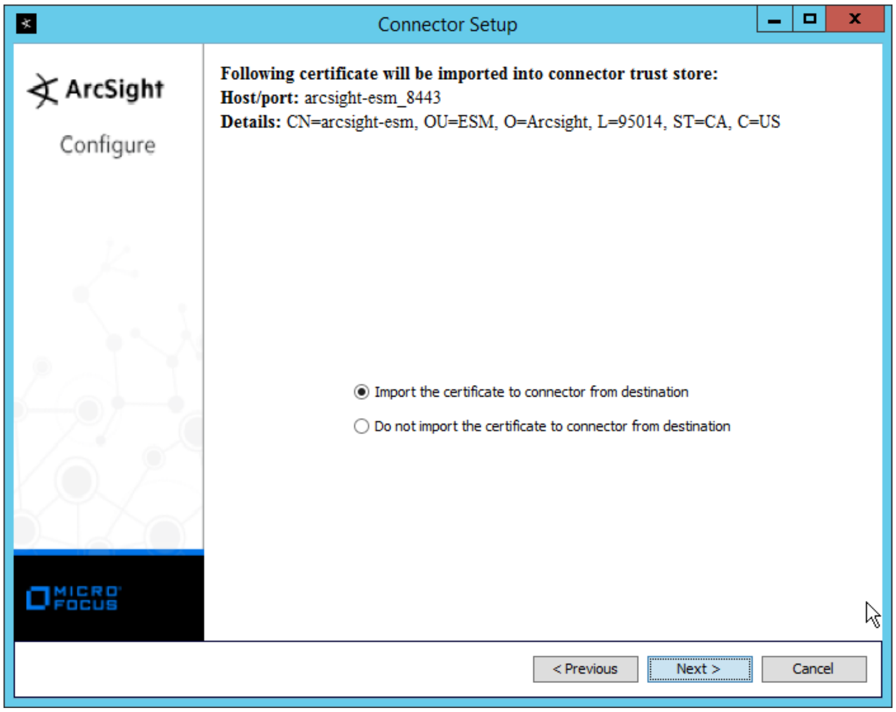
14. Click **Next.**
15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



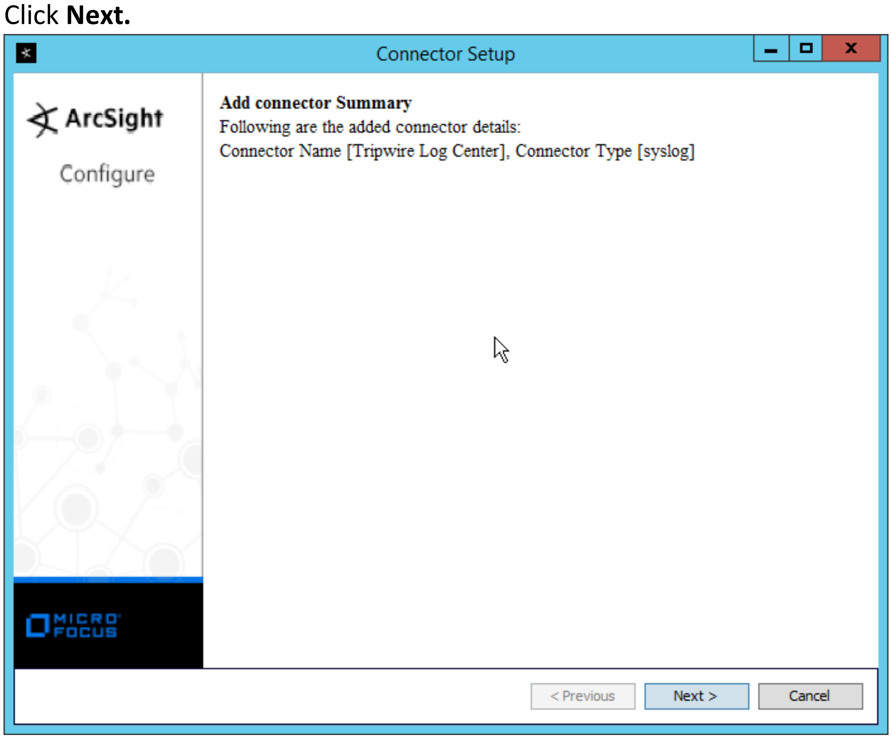
16. Click **Next.**
17. Enter identifying details about the system (only **Name** is required).



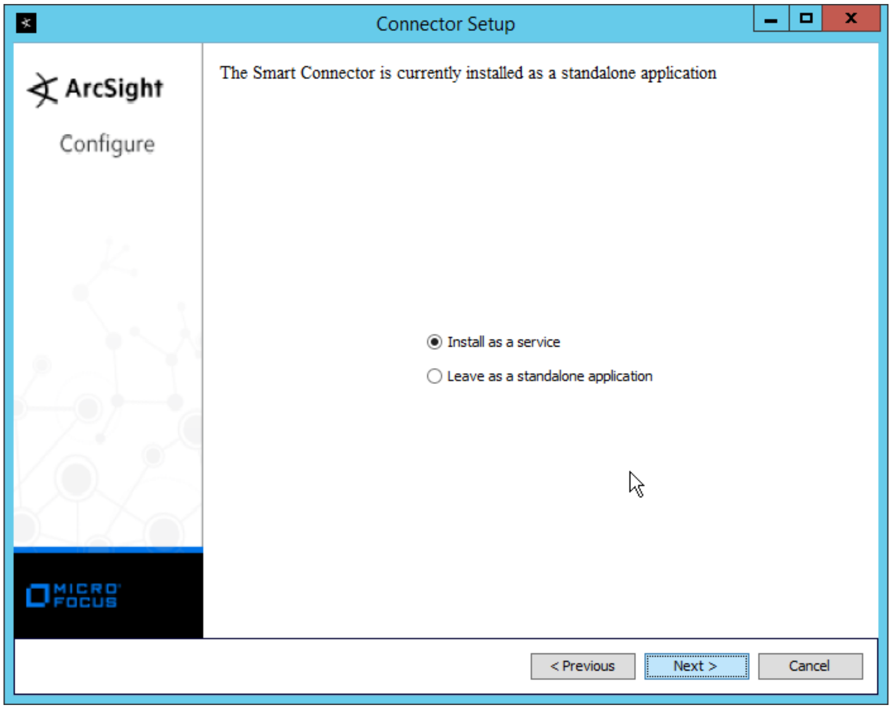
18. Click **Next.**
19. Select **Import the certificate to connector from destination.**



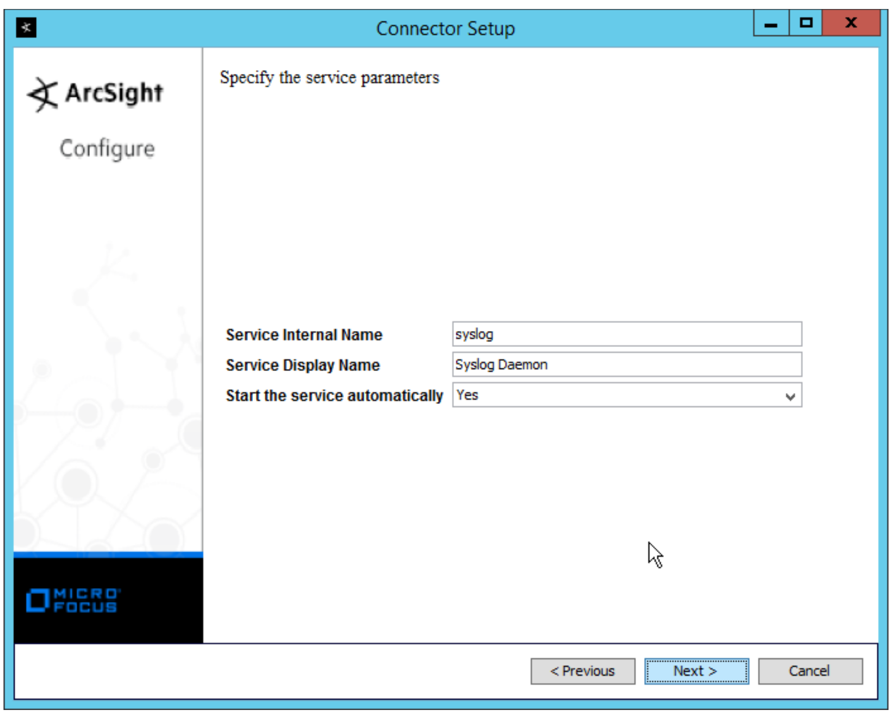
20. Click **Next.**



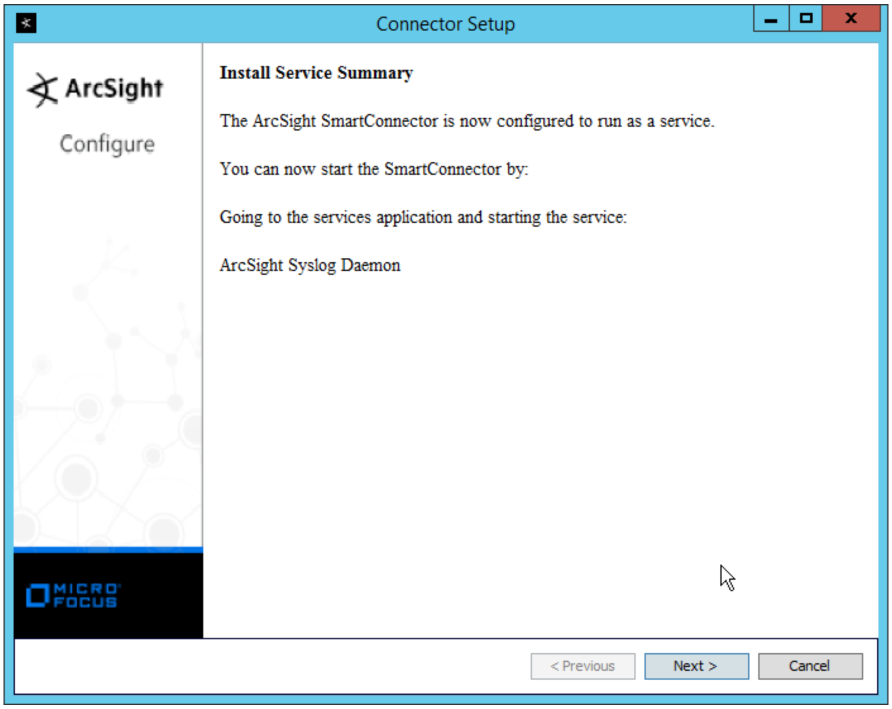
21. Click **Next.**
22. Select **Install as a service.**



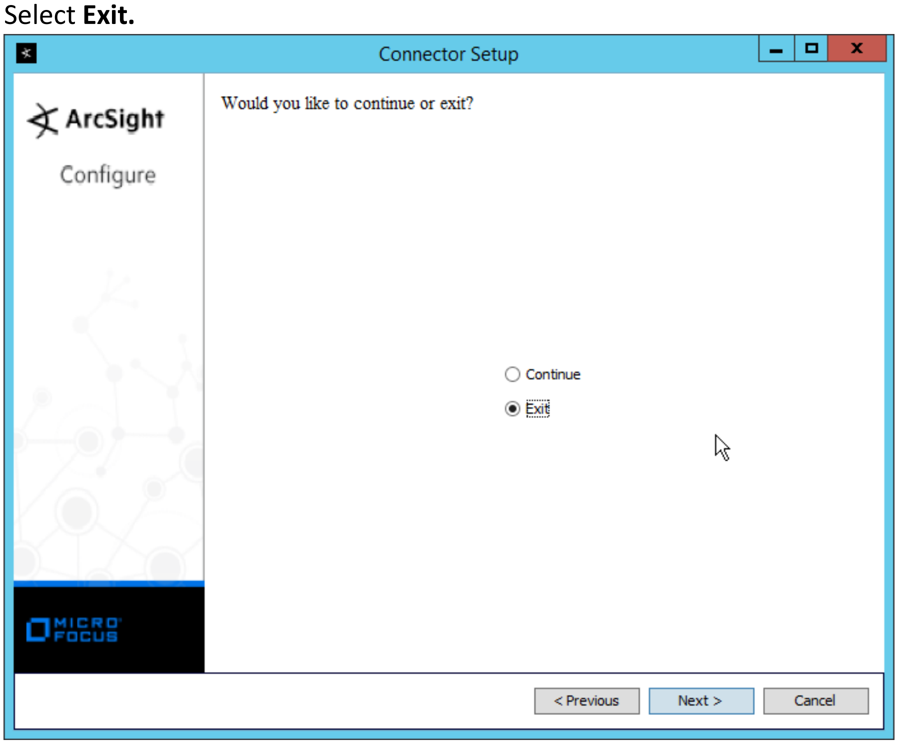
23. Click **Next.**



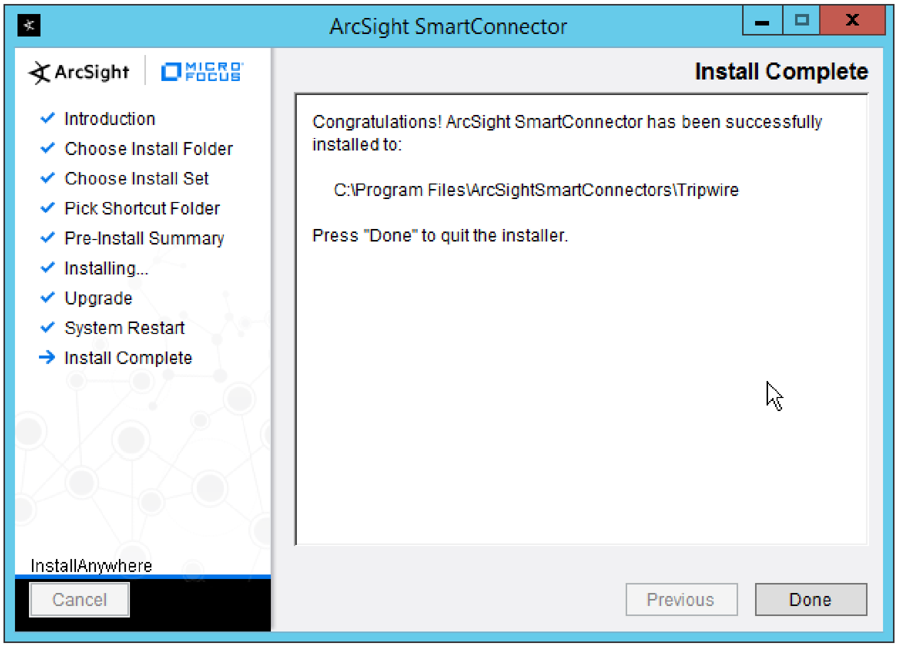
24. Click **Next.**



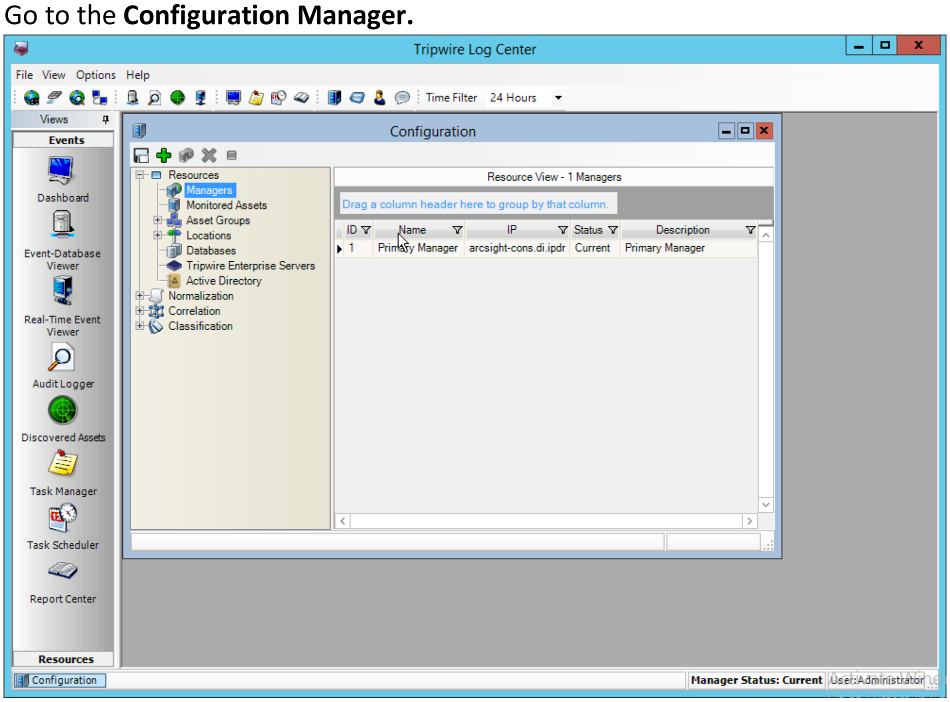
25. Click **Next.**
26. Select **Exit.**



27. Click **Next.**

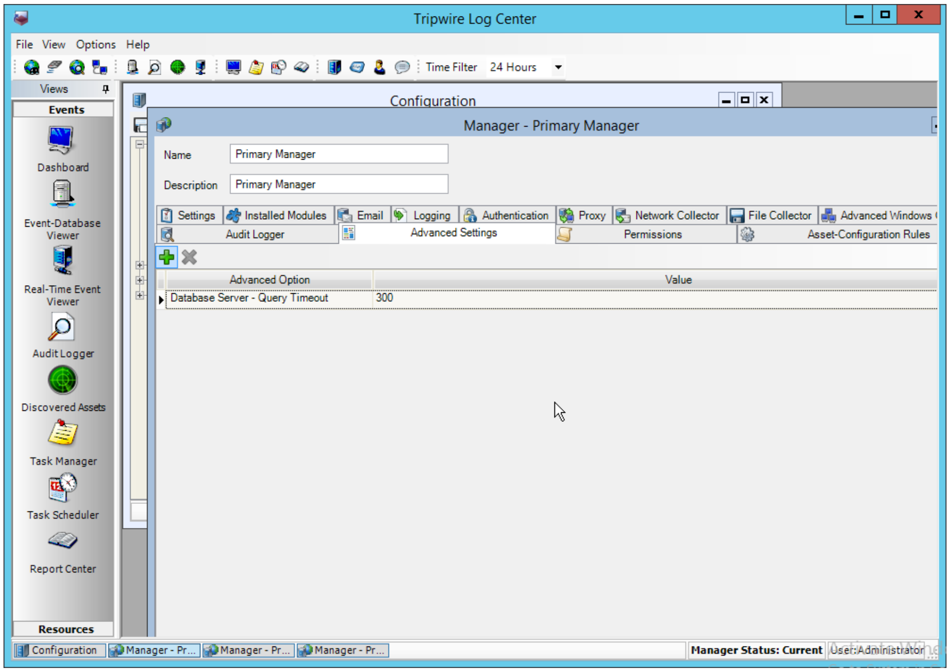


28. Click **Done.**
29. Open the **Tripwire Log Center Console.**
30. Go to the **Configuration Manager.**

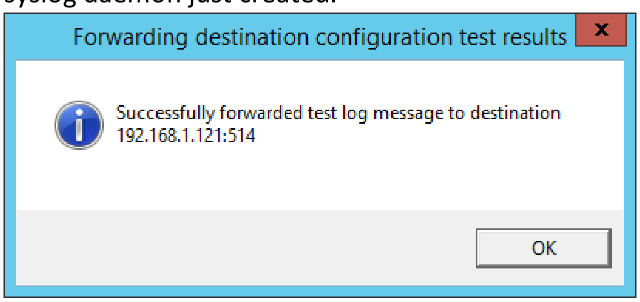


31. Select **Resources** > **Managers.**
32. Double-click the **Primary Manager.**

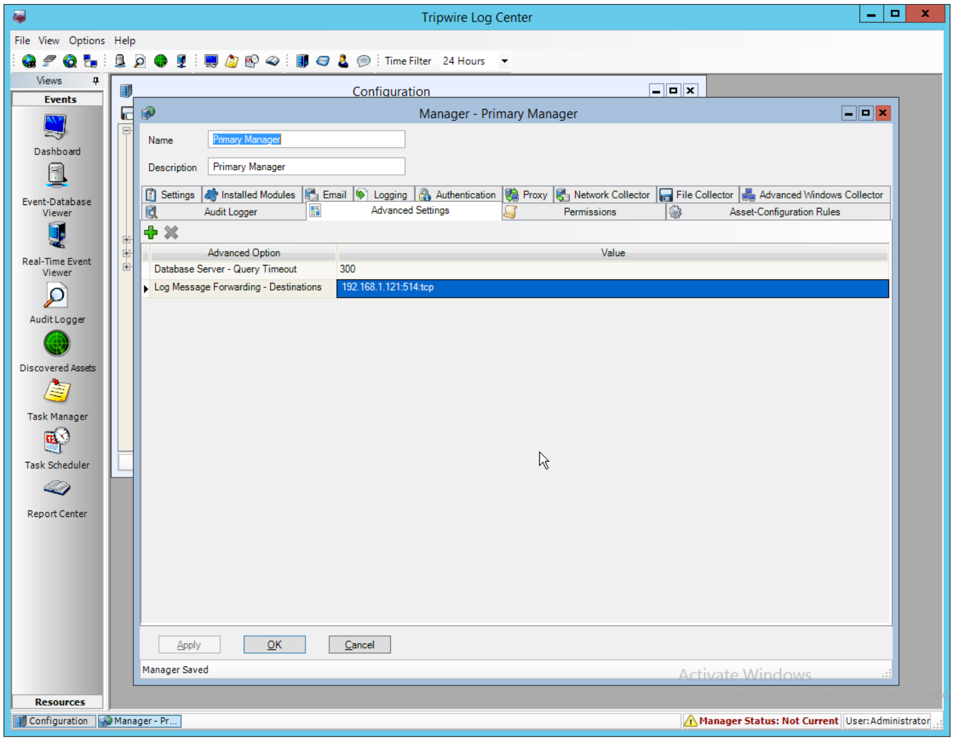
33. Click the **Advanced Settings** tab.



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



37. Click **OK**.



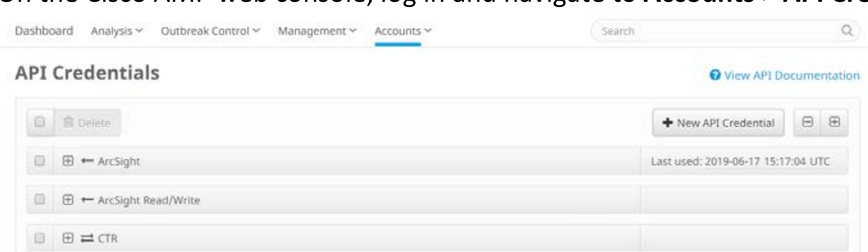
38. Click **OK.**
39. Restart the **Tripwire Log Center Manager.**

2.20 Integration: Micro Focus ArcSight and Cisco AMP

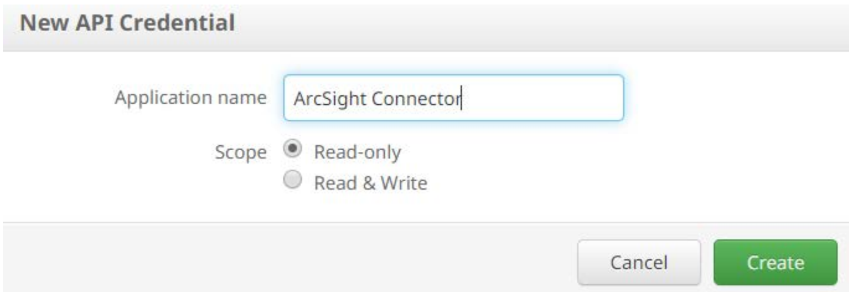
This section will detail the collection of logs from **Cisco AMP's** REST APIs using **Micro Focus ArcSight.**

2.20.1 Create API Credentials for ArcSight to access AMP

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



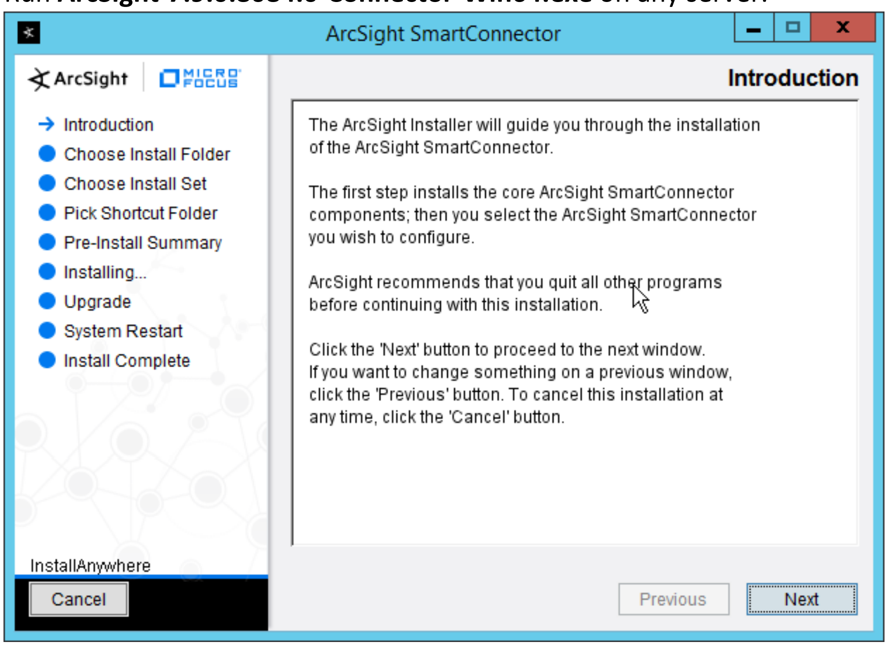
2. Click **New API Credential.**
3. Enter a name for the credential.
4. Select **Read-only.**



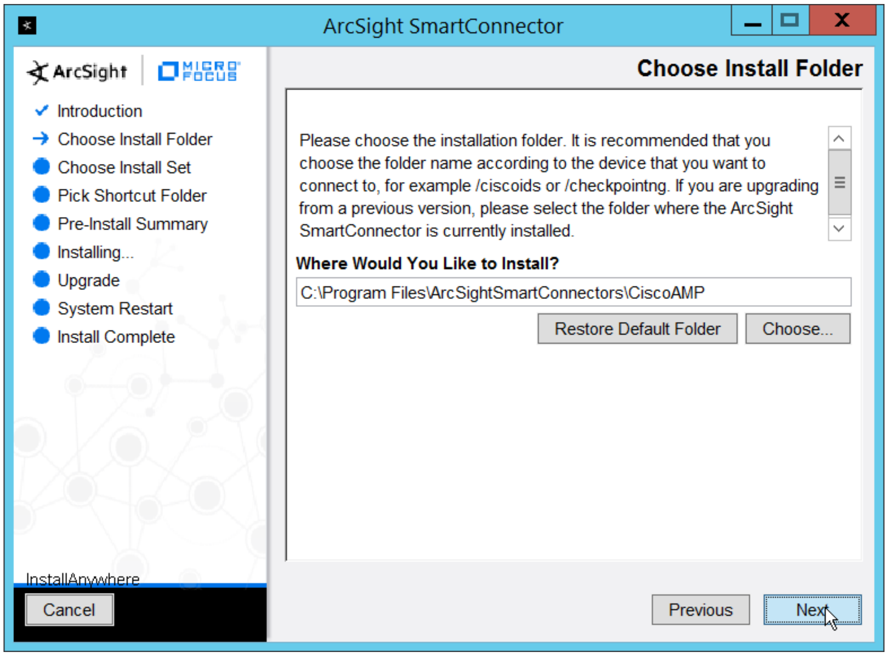
5. Click **Create.**
6. This will direct you to a page with an **ID** and **API Key.** Keep track of these, as you will need them in the setup for the ArcSight Connector, and Cisco AMP may not let you view them again.

2.20.2 Install Micro Focus ArcSight

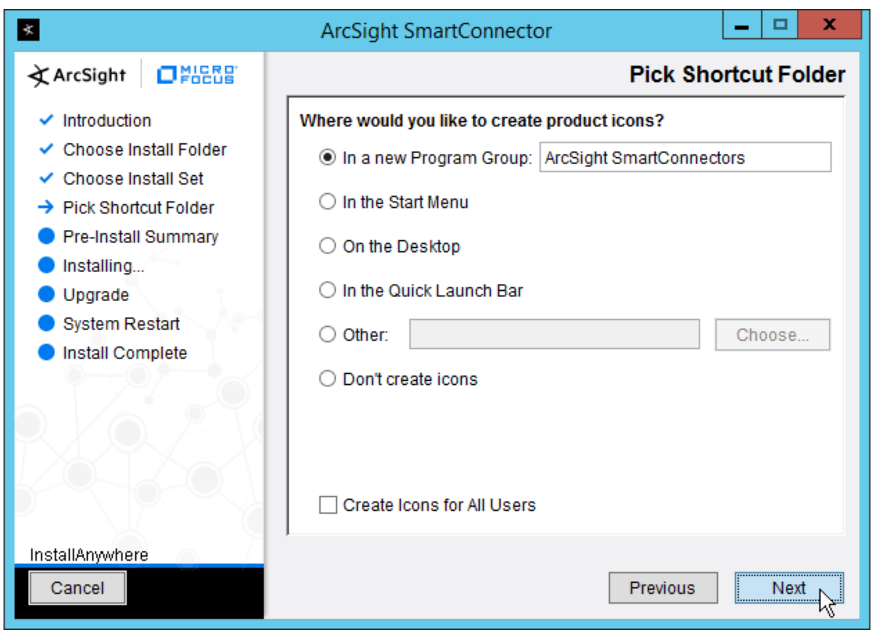
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server.



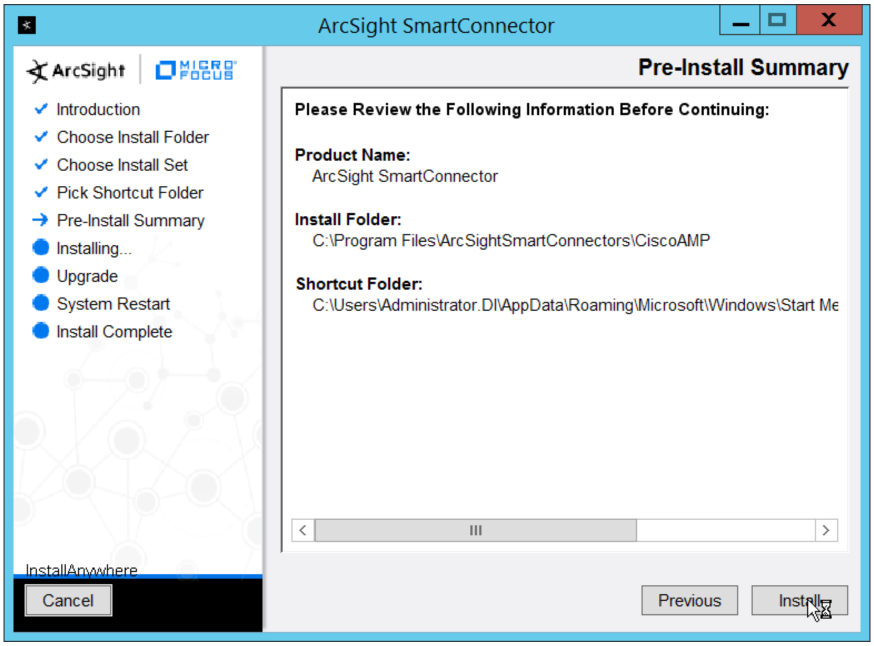
2. Click **Next.**
3. Enter *C:\Program Files\ArcSightSmartConnectors\CiscoAMP.*



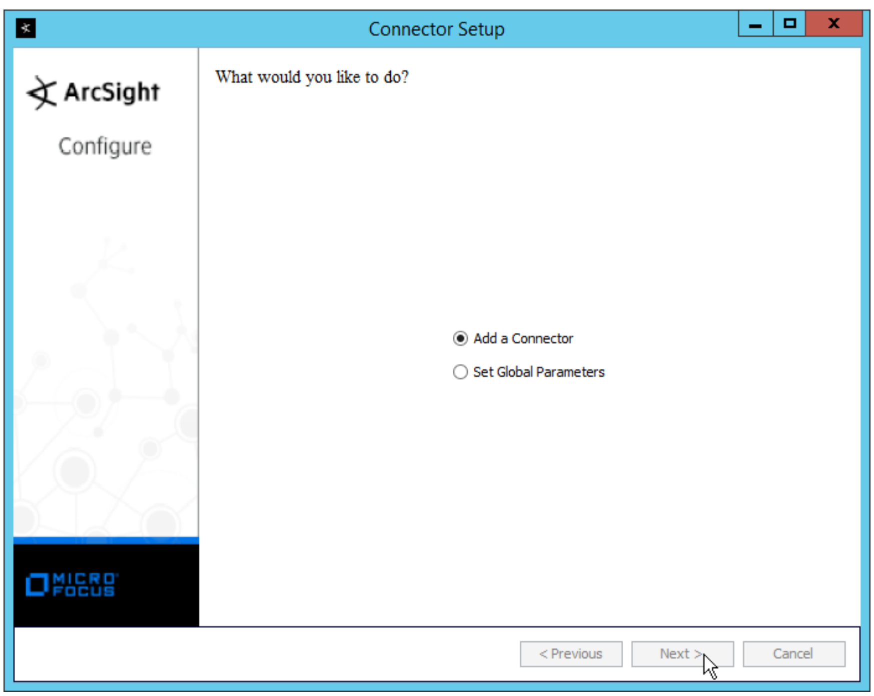
4. Click **Next.**



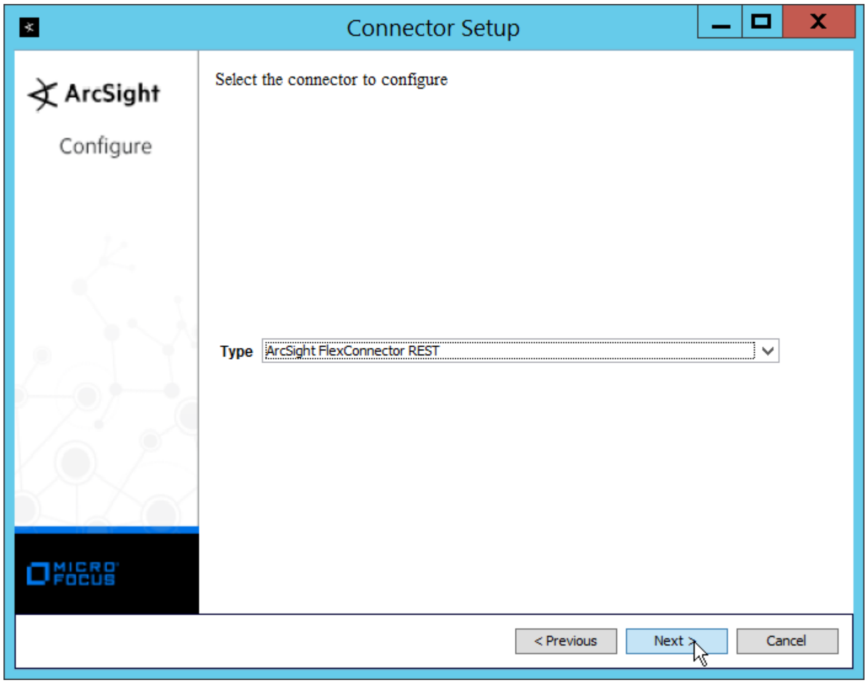
5. Click **Next.**



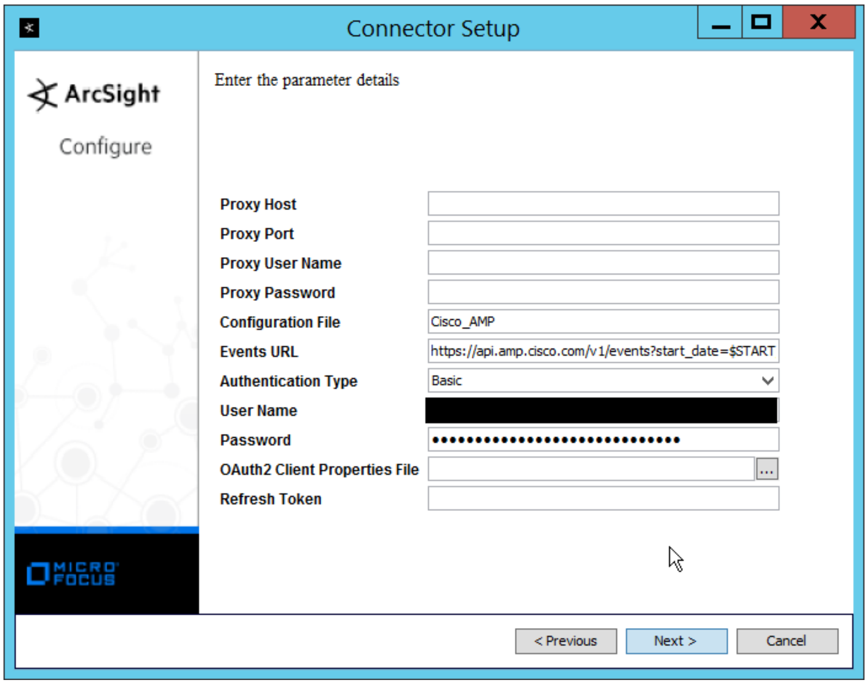
6. Click **Install.**
7. Select **Add a Connector.**



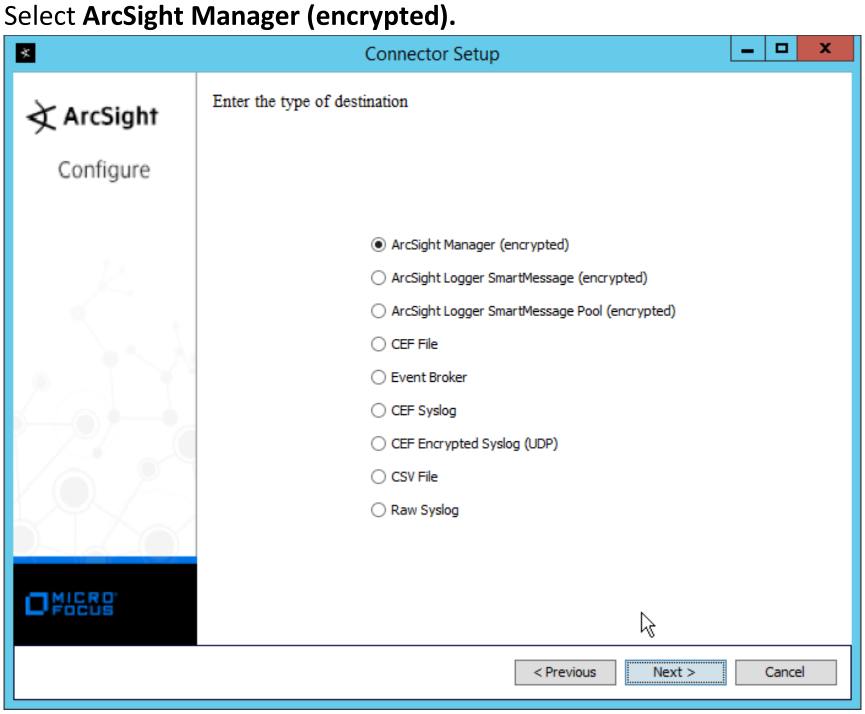
8. Click **Next.**
9. Select **ArcSight FlexConnector REST.**



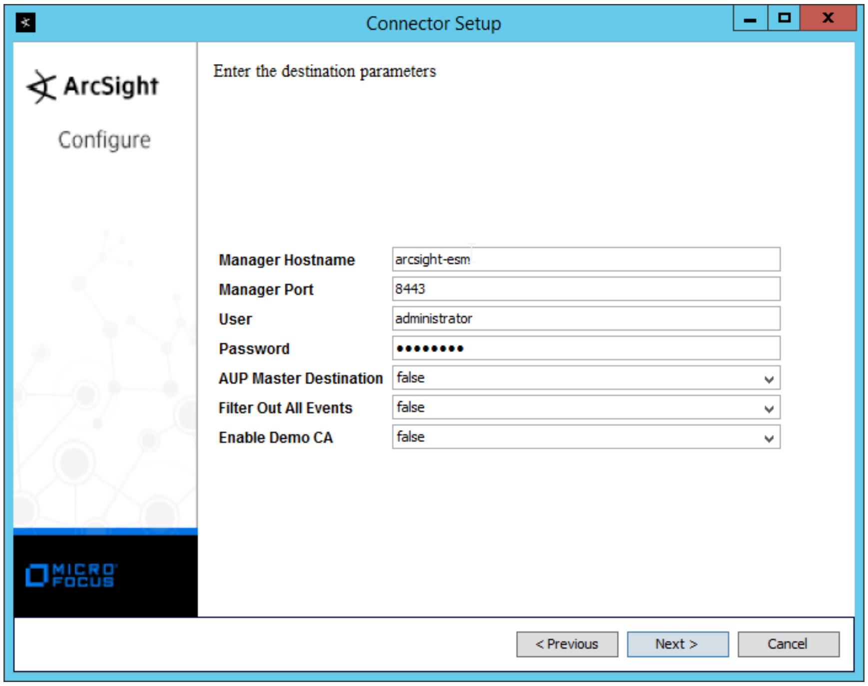
10. Click **Next.**
11. Enter *Cisco_AMP* for the **Configuration File.**
12. Enter https://api.amp.cisco.com/v1/events?start_date=$START_AT_TIME for the **Events URL.** (Note: You can see the Cisco AMP REST API documentation for more information on how to formulate this URL for things other than events.)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



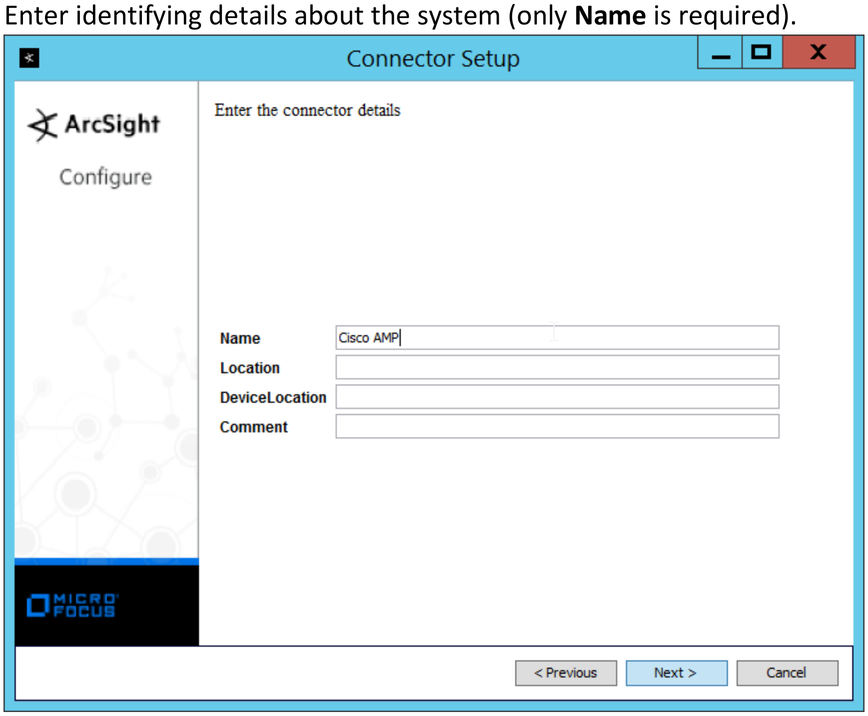
14. Click **Next.**
15. Select **ArcSight Manager (encrypted).**



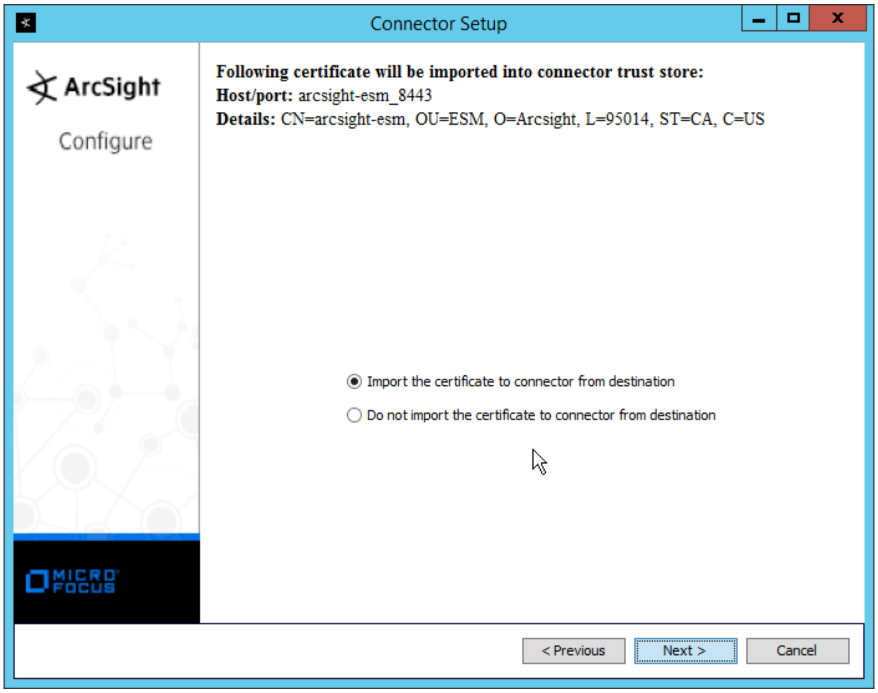
16. Click **Next.**
17. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



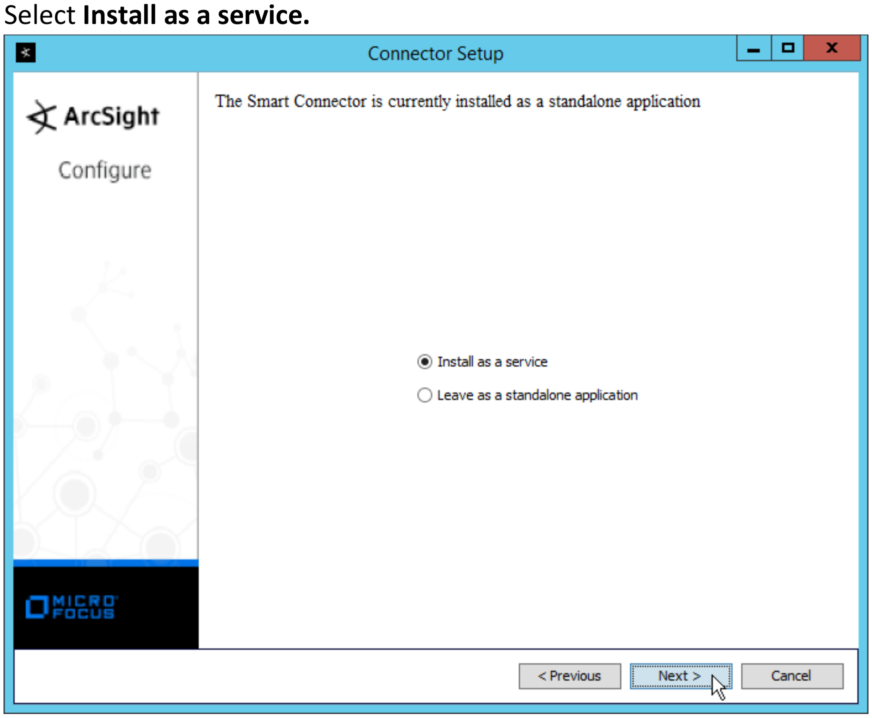
18. Click **Next.**
19. Enter identifying details about the system (only **Name** is required).



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

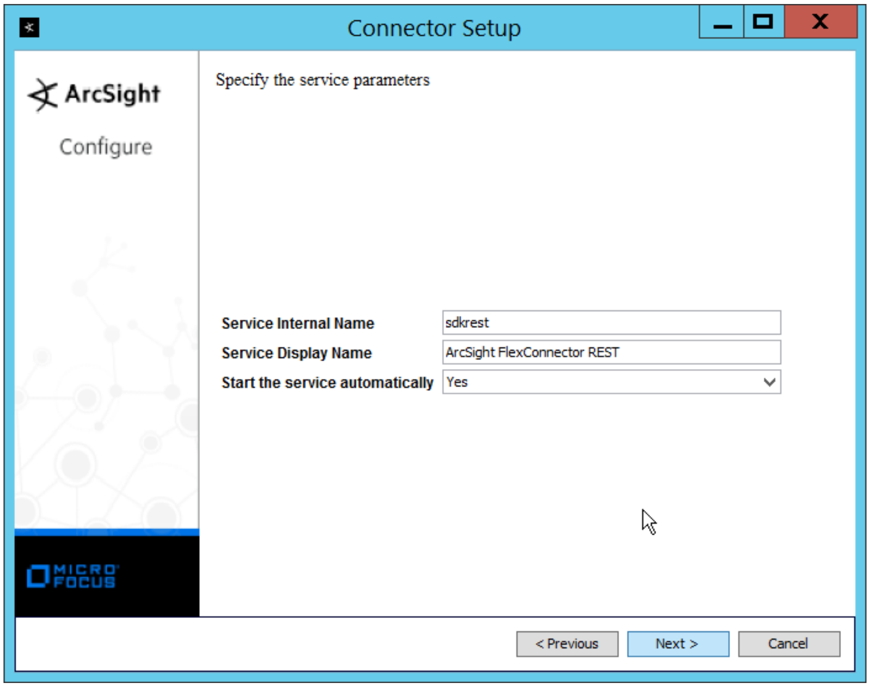


22. Click **Next.**
23. Click **Next.**
24. Select **Install as a service.**

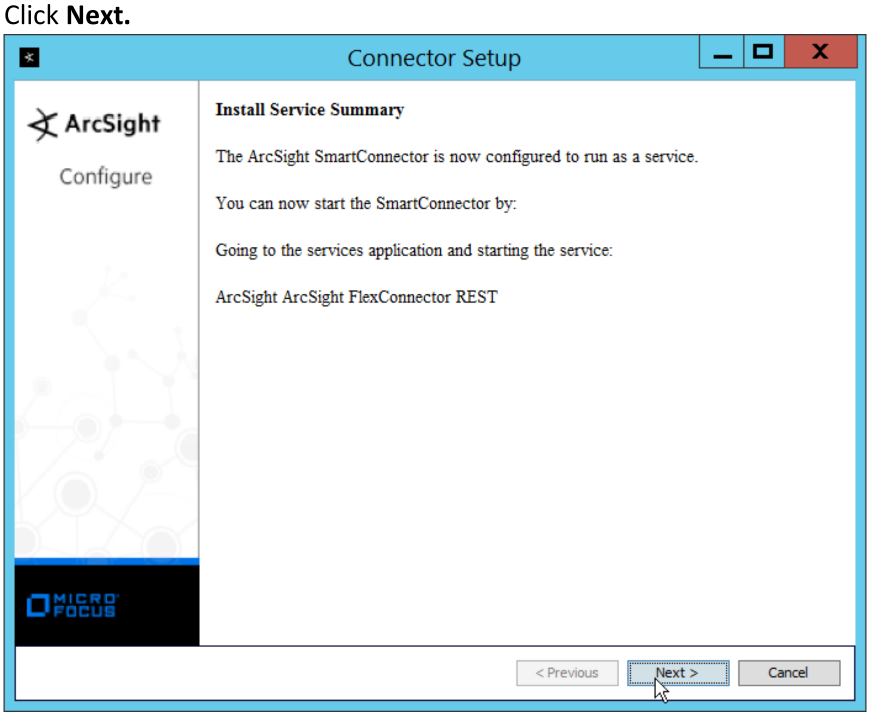


25. Click **Next.**

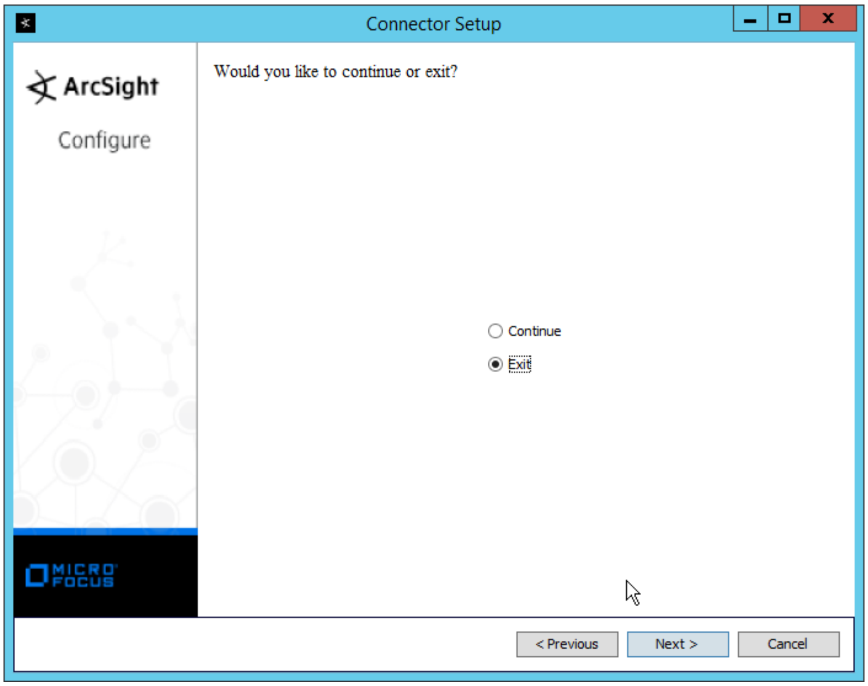
26. Enter a service name and display name.



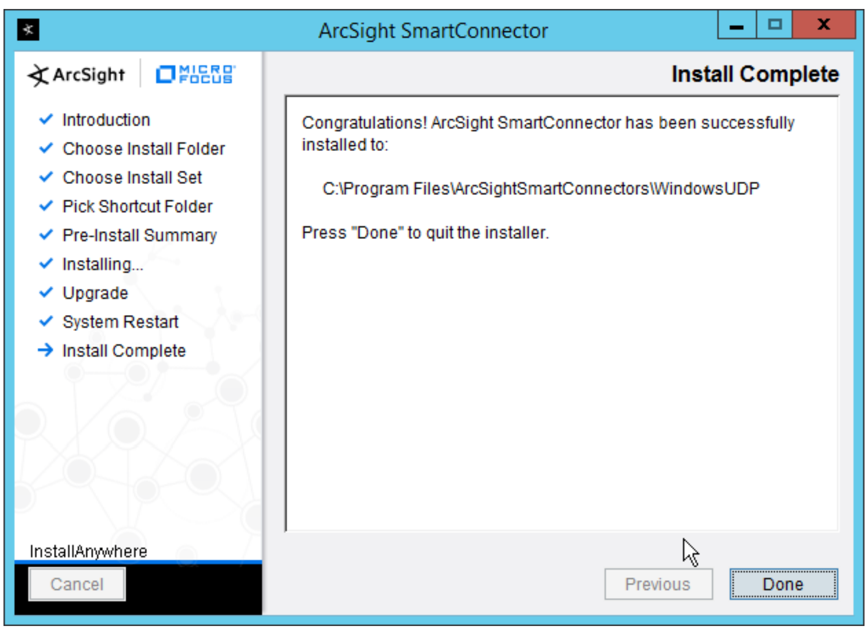
27. Click **Next.**



28. Click **Next.**
29. Select **Exit.**



30. Click **Next.**



31. Click **Done.**

2.20.3 Create a Parser for Cisco AMP REST events

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

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

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

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

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

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

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

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

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

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

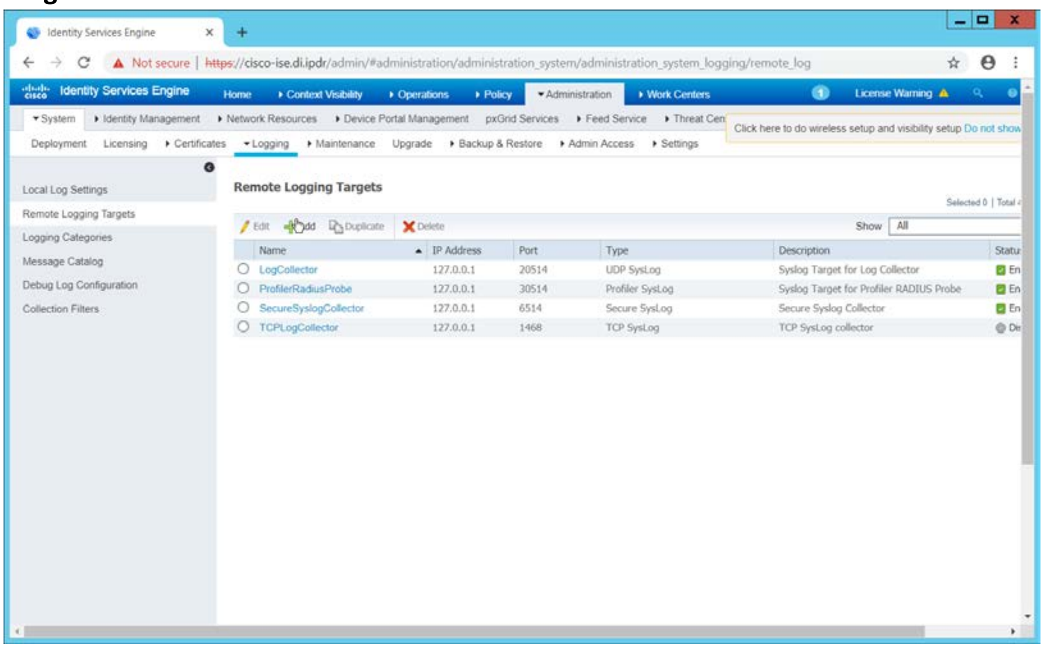
4. This parser will allow for details of Cisco AMP events to be shown in ArcSight. Custom parsers are a functionality of ArcSight. For more information on the creation of custom parsers, please see the *ArcSight FlexConnector Developer’s Guide* as well as the *FlexConnector REST Developer’s Guide*. You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

2.21 Integration: Micro Focus ArcSight and Cisco ISE

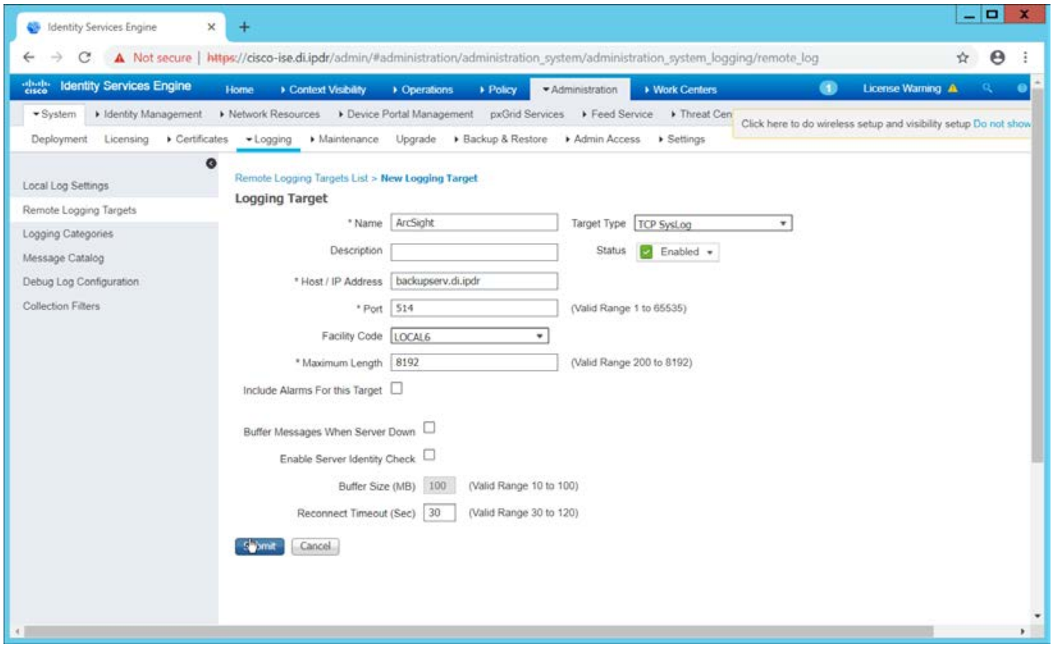
This integration will briefly detail how to send logs to an ArcSight syslog collector from Cisco ISE. Please see Section 2.18 (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one—simply use the address of that server to which to forward logs.

2.21.1 Configure Cisco ISE to Forward Logs

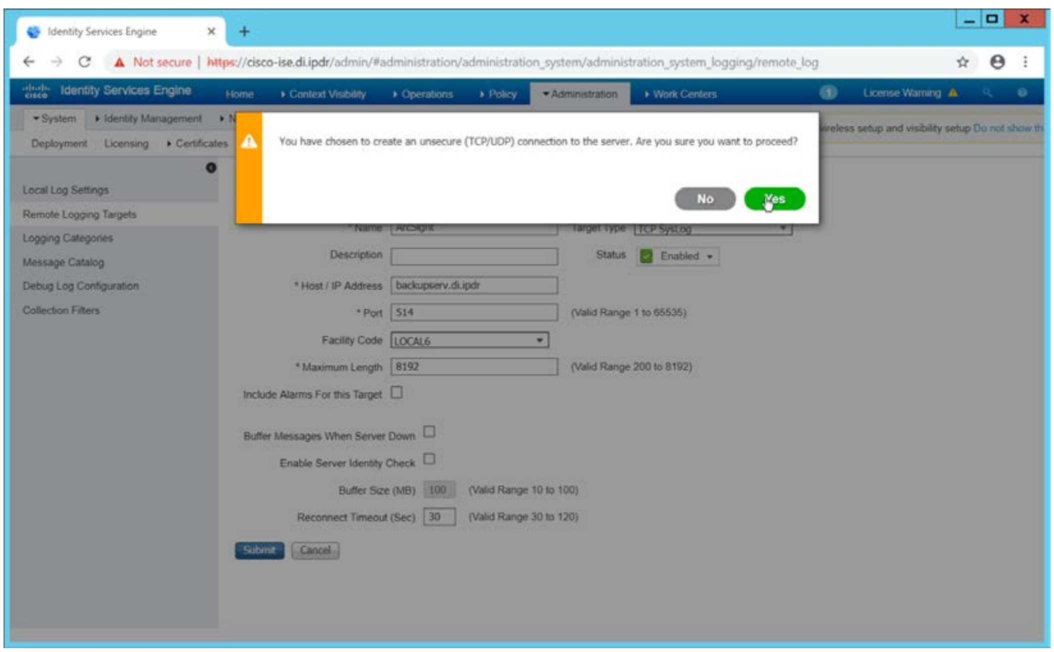
1. In the Cisco ISE web client, navigate to **Administration > System > Logging > Remote Logging Targets.**



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



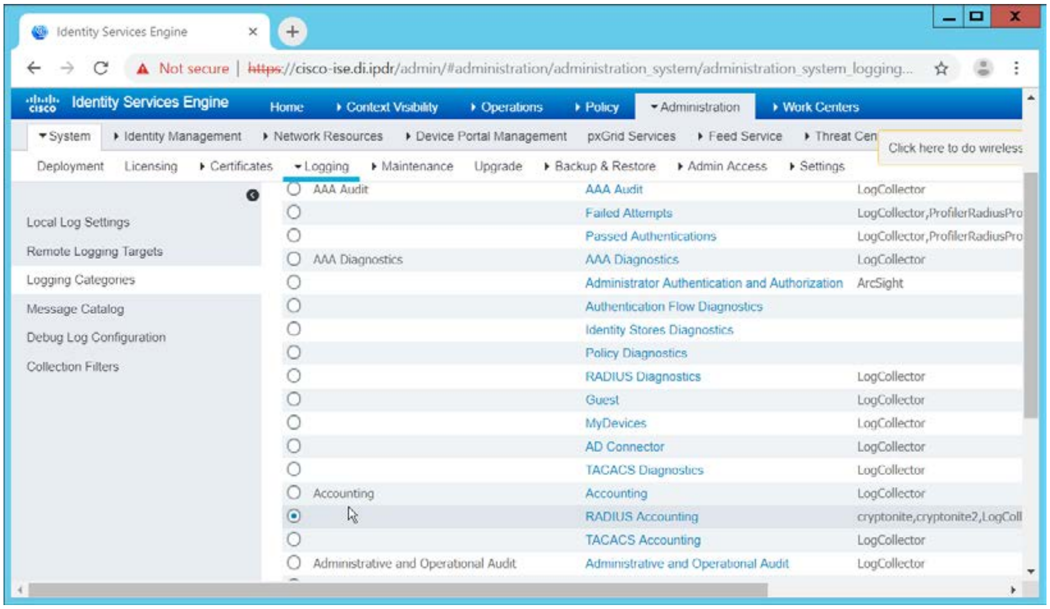
9. Click **Submit.**



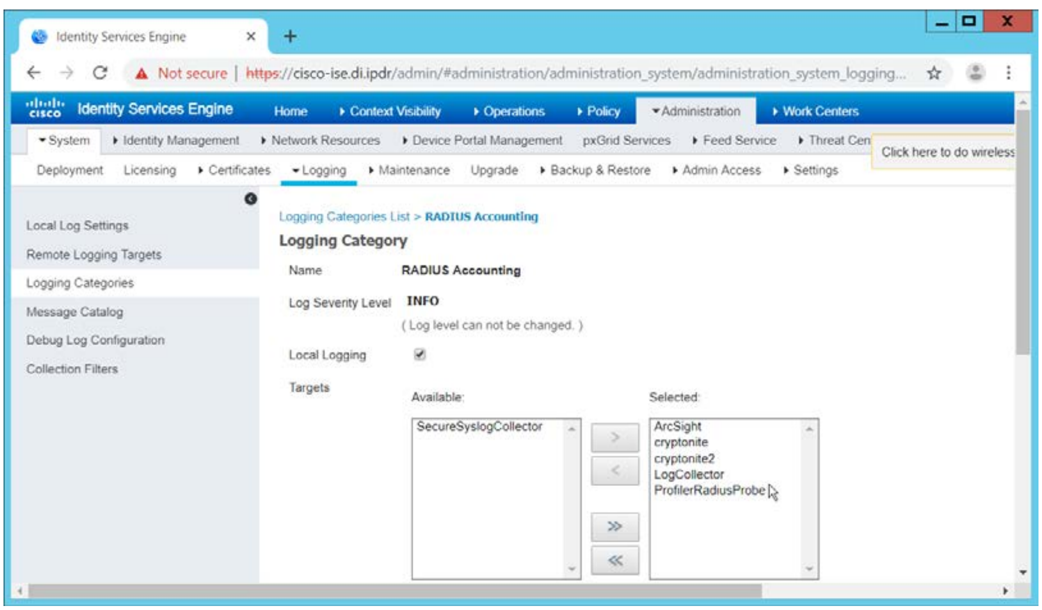
10. Click **Yes.**

2.21.2 Select Logs for Forwarding

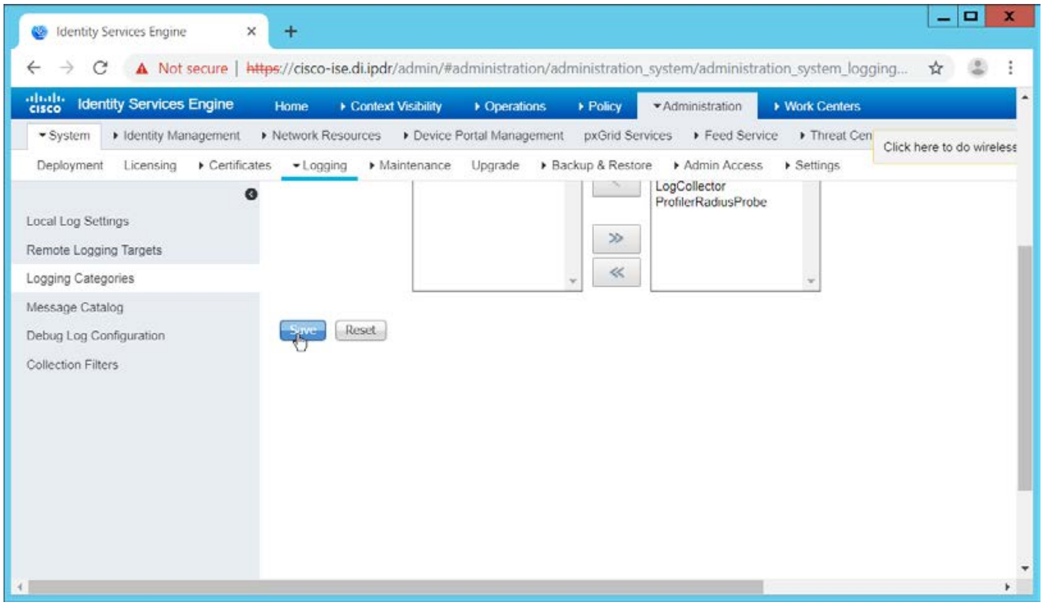
1. Navigate to **System > Logging > Logging Categories.**



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



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



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

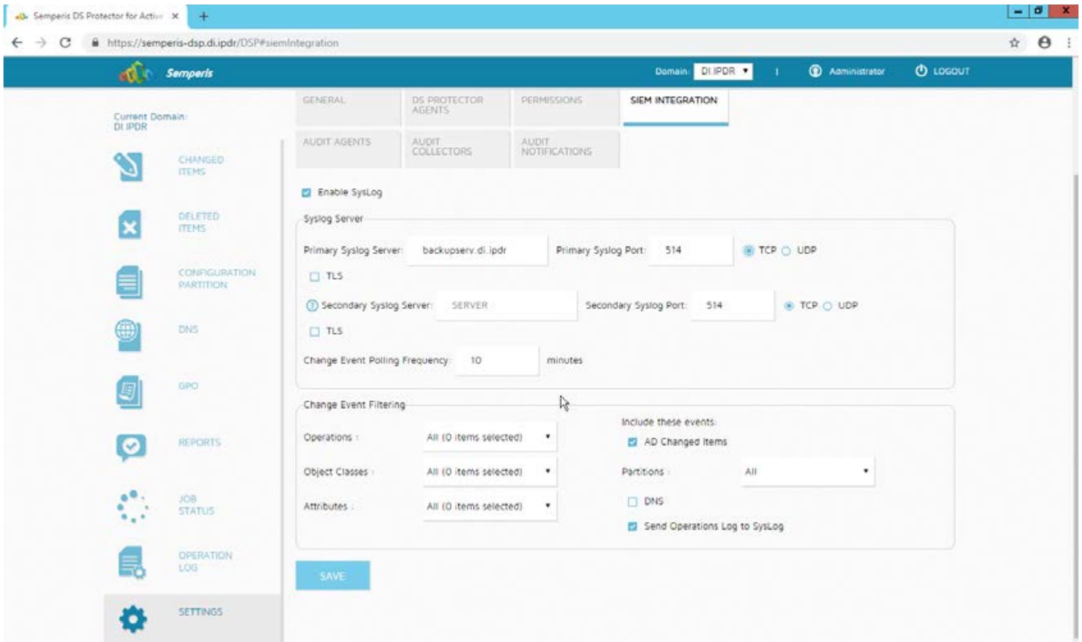
2.22 Integration: Micro Focus ArcSight and Semperis DSP

This integration will briefly detail how to send logs to an ArcSight syslog collector from Semperis DSP. Please see Section 2.18 (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one—simply use the address of that server to which to forward logs.

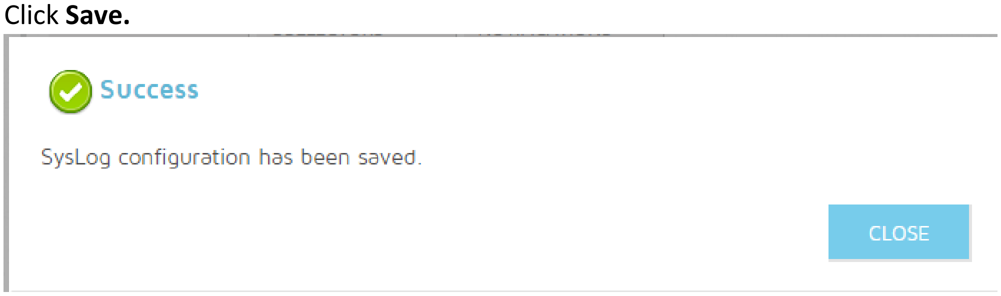
Note: This integration requires Semperis DSP version 2.6.

2.22.1 Configure Semperis DSP to Forward Logs

1. In Semperis DSP, navigate to **Settings** > **SIEM Integration.**
2. Check the box next to **Enable SysLog.**
3. Under **Syslog Server,** enter the **hostname** for the ArcSight syslog collector, as well as the **port.**
4. Select **TCP.**
5. Enter a value for **Change Event Polling Frequency** based on the needs of your organization; this is how often it will poll for new logs to forward.
6. Under **Change Event Filtering,** select **AD Changed Items,** and **Send Operation Log to SysLog.** Ensure that **All** is selected for **Partitions.**
7. You can also select any specific **operations, classes,** and **attributes** to be forwarded or simply leave it as **All.**



8. Click **Save.**



9. Click **Close.**

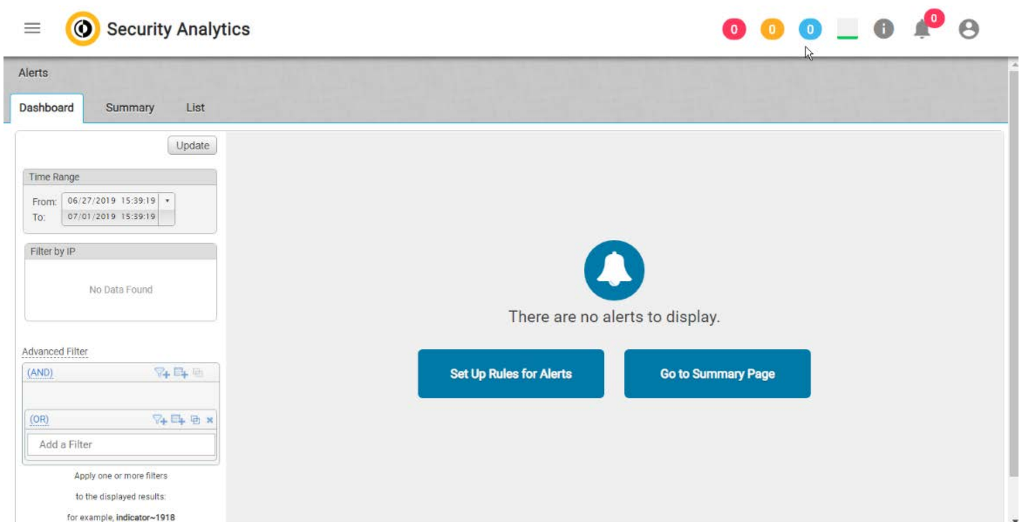
2.23 Integration: Micro Focus ArcSight and Symantec Analytics

This section will first detail the forwarding of logs from **Symantec Analytics** to **Micro Focus ArcSight**. Please see section **2.18** (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog collector. If a server is already configured, you do not need to install a new one; simply use the address of that server to which to forward logs.

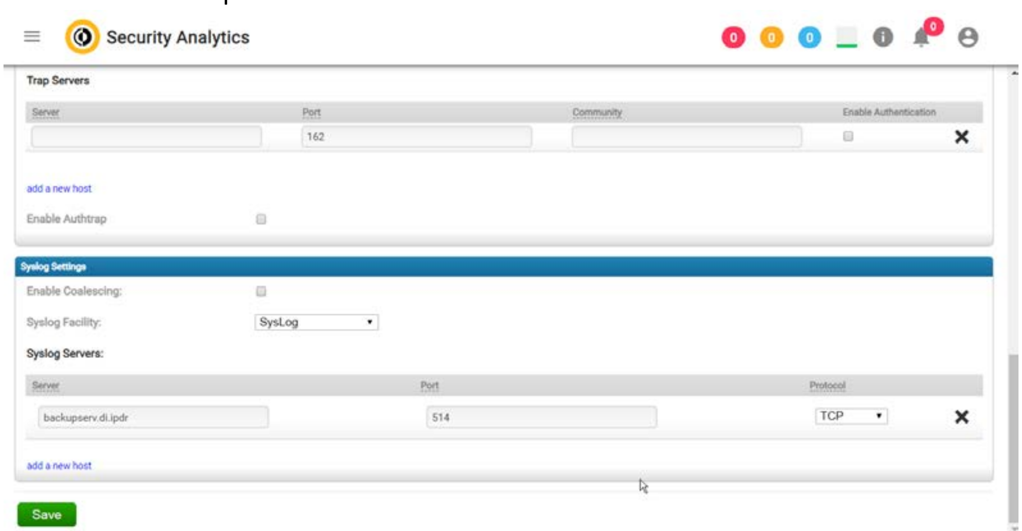
The second part of this section will detail a further integration for ArcSight that allows ArcSight to better analyze network packets received from Symantec Analytics.

2.23.1 Configure Symantec Analytics to Forward Logs

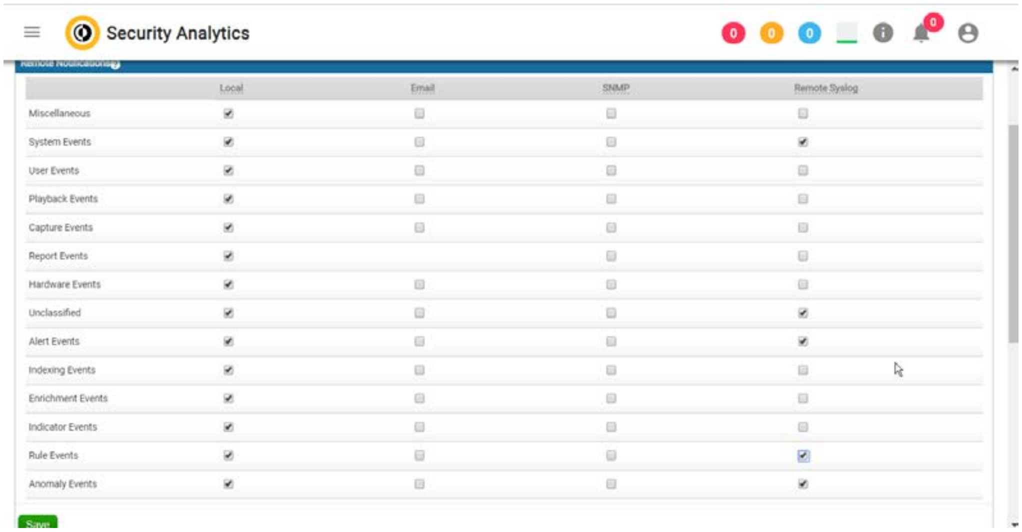
1. Log in to the Symantec Analytics web console.



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



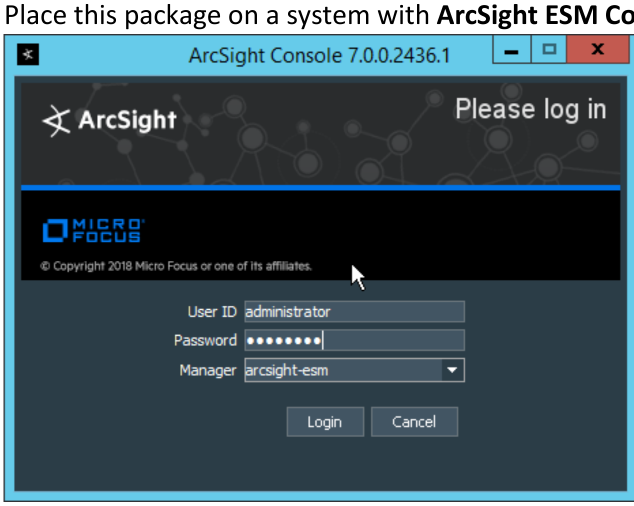
9. Click **Save.**
10. Click the **Advanced** tab.
11. Select the box under **Remote Syslog** column for any events that you wish to forward to ArcSight, for example, **System Events**, **Unclassified Events**, **Alert Events**, **Rule Events**, **Anomaly Events.**



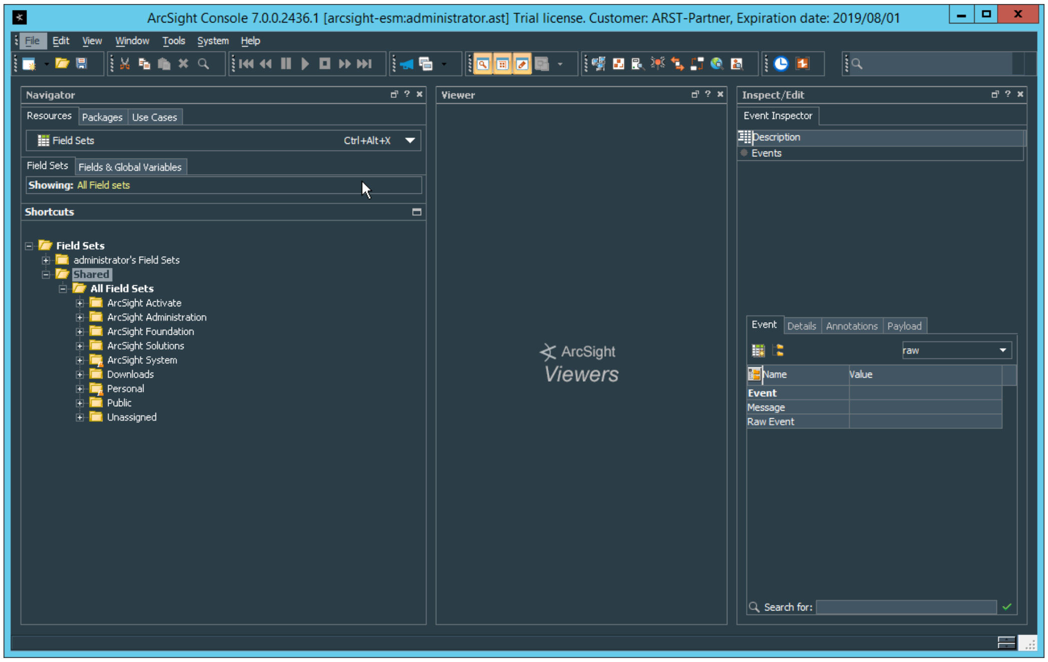
12. Click **Save.**

2.23.2 Install Symantec Analytics Package for ArcSight

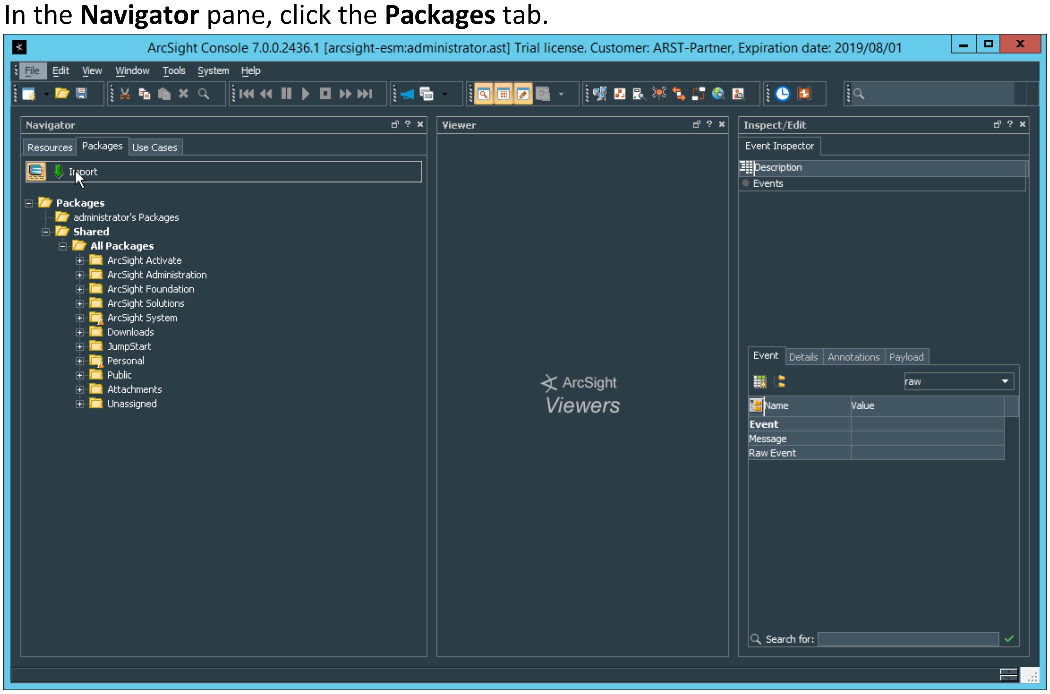
1. Navigate to the ArcSight marketplace. Look for the “Blue Coat Security Analytics” package for ArcSight. It may be available here: https://marketplace.microfocus.com/arcsight/content/blue-coat-security-analytics-platform but not please contact your ArcSight representative to get the package. The package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



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

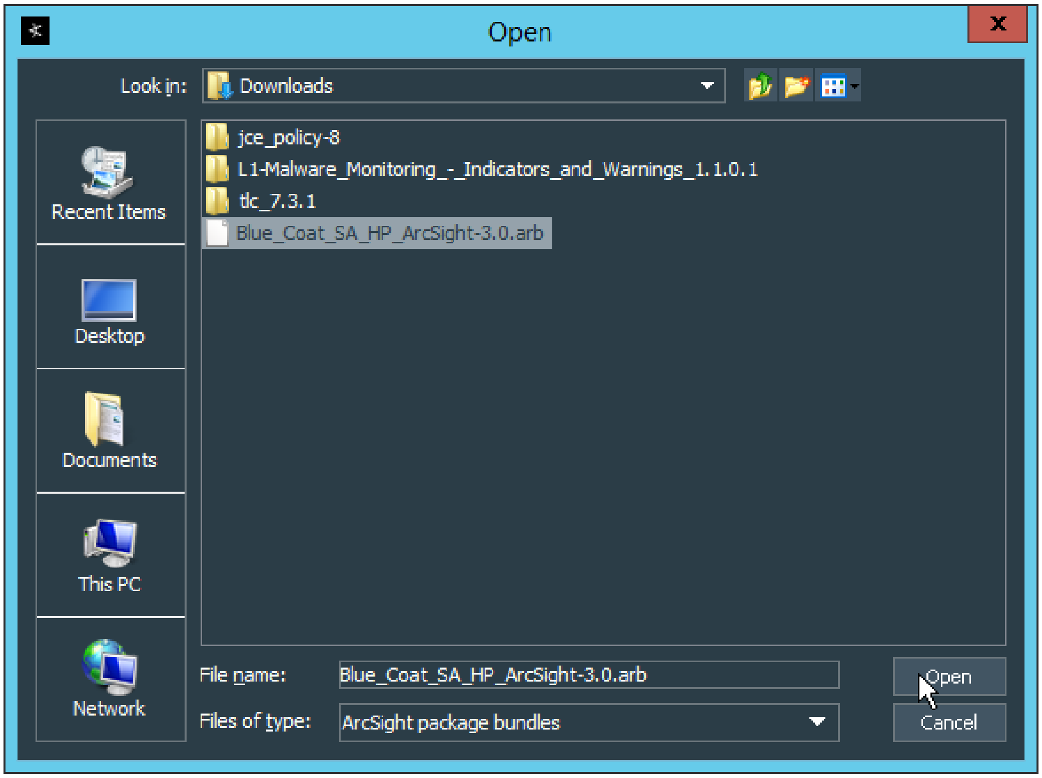


4. In the **Navigator** pane, click the **Packages** tab.

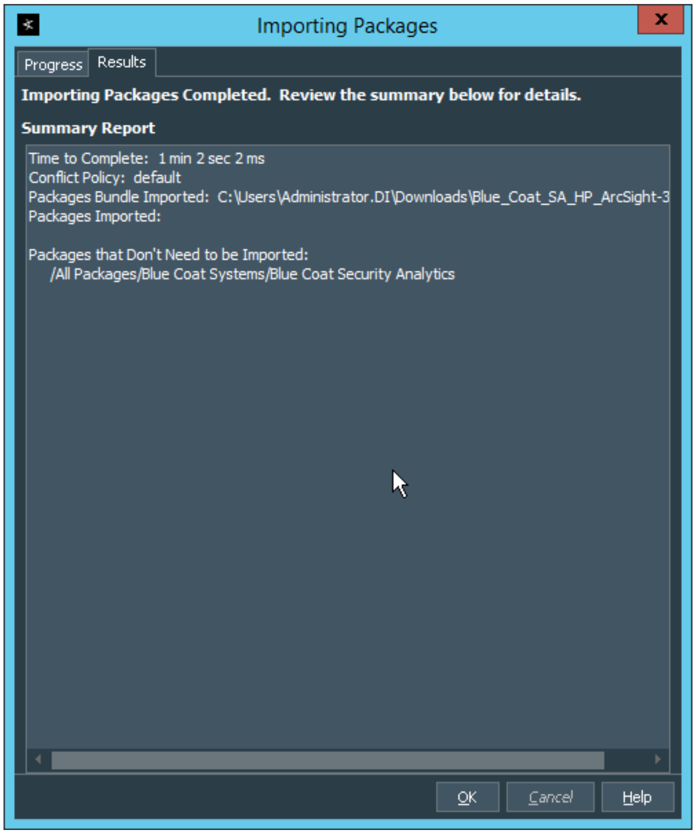


5. Click **Import.**

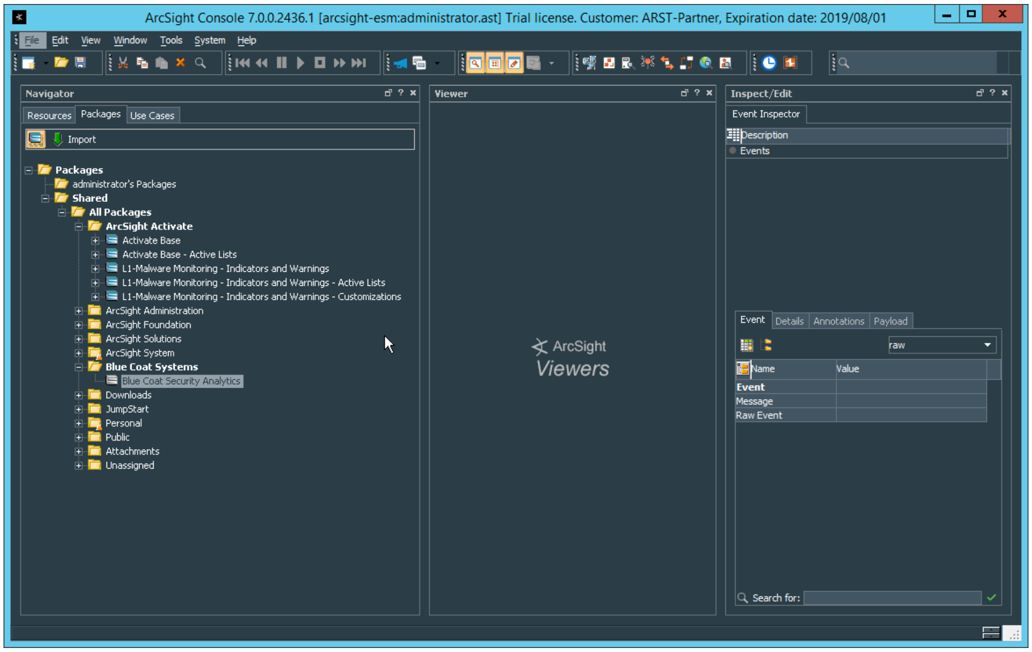
6. In the window that it opens, find and select the package you downloaded.


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

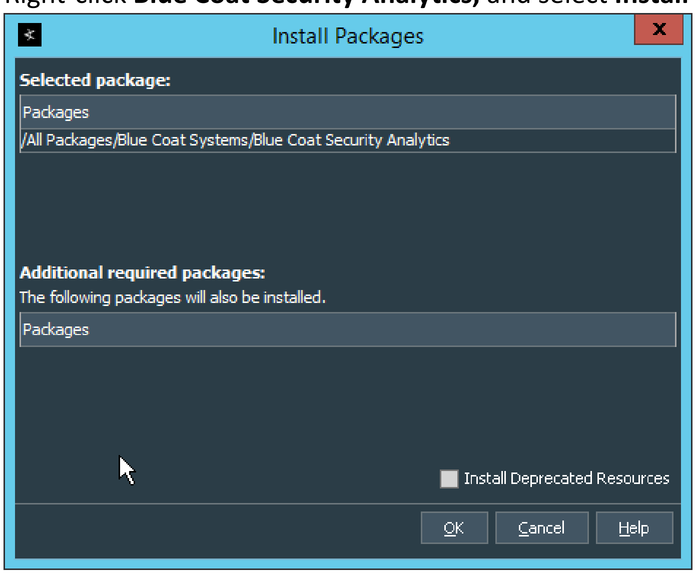
7. Click **Open.**



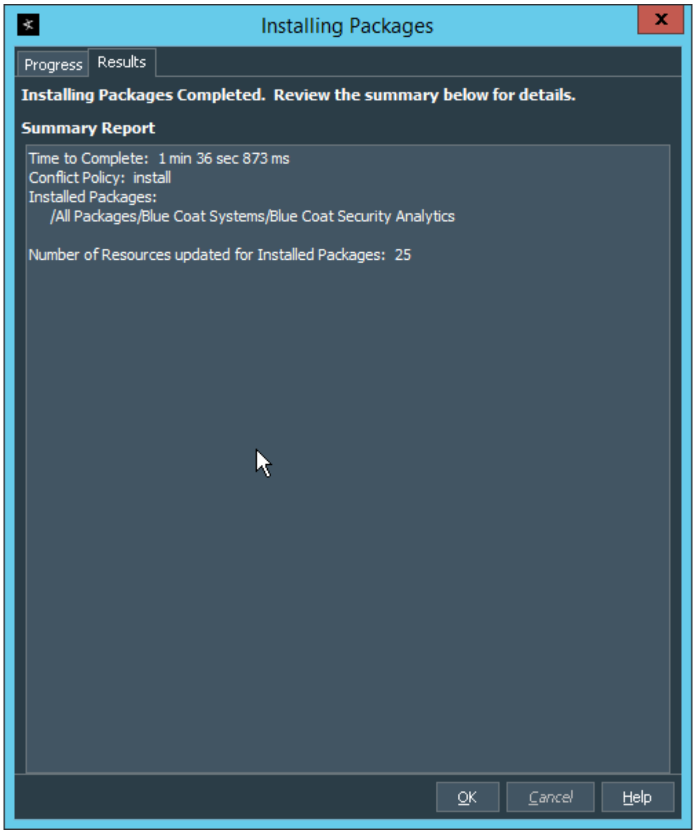
8. Click **OK** when the import finishes.
9. Under the **Packages** tab in the **Navigator** pane, navigate to **Packages > Shared > All Packages > Blue Coat Systems > Blue Coat Security Analytics.**



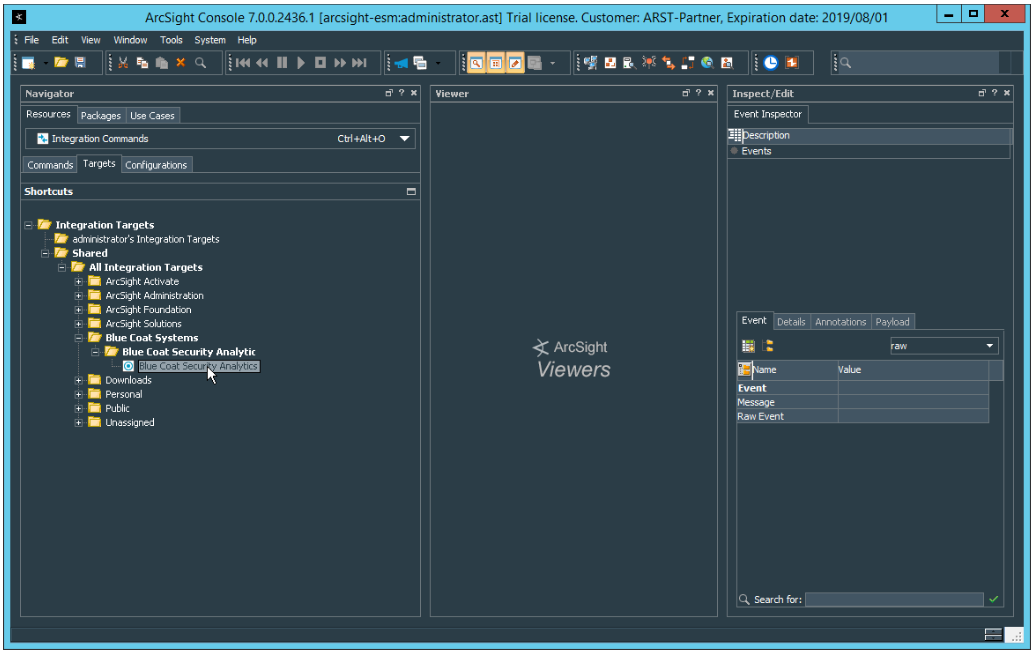
10. Right-click **Blue Coat Security Analytics,** and select **Install Package.**



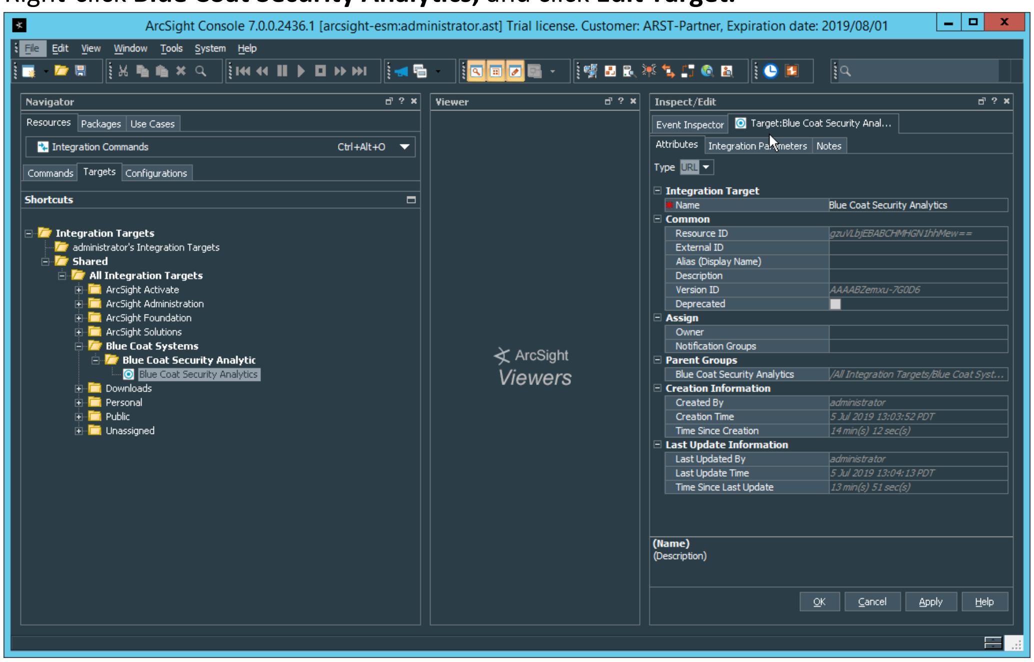
11. Click **OK.**



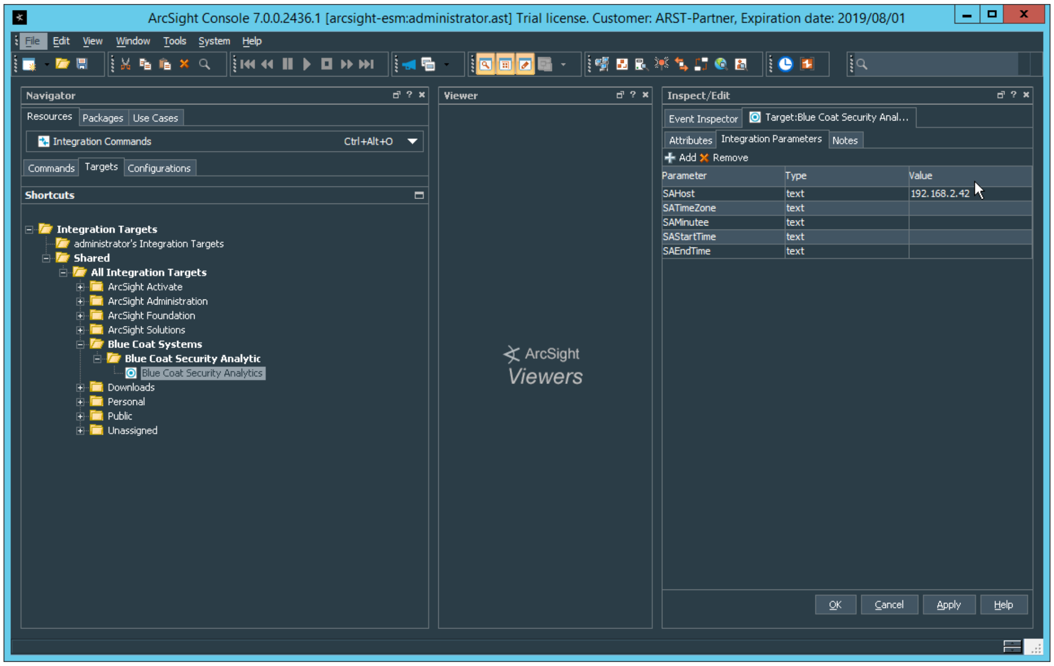
12. Click **OK.**
13. When this completes, you can verify that the installation was successful by the existence of a **Blue Coat Systems** folder when you navigate to **Resources > Integration Commands > Commands > Shared > All Integration Commands.**
14. In the **Resources** tab of the **Navigation**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



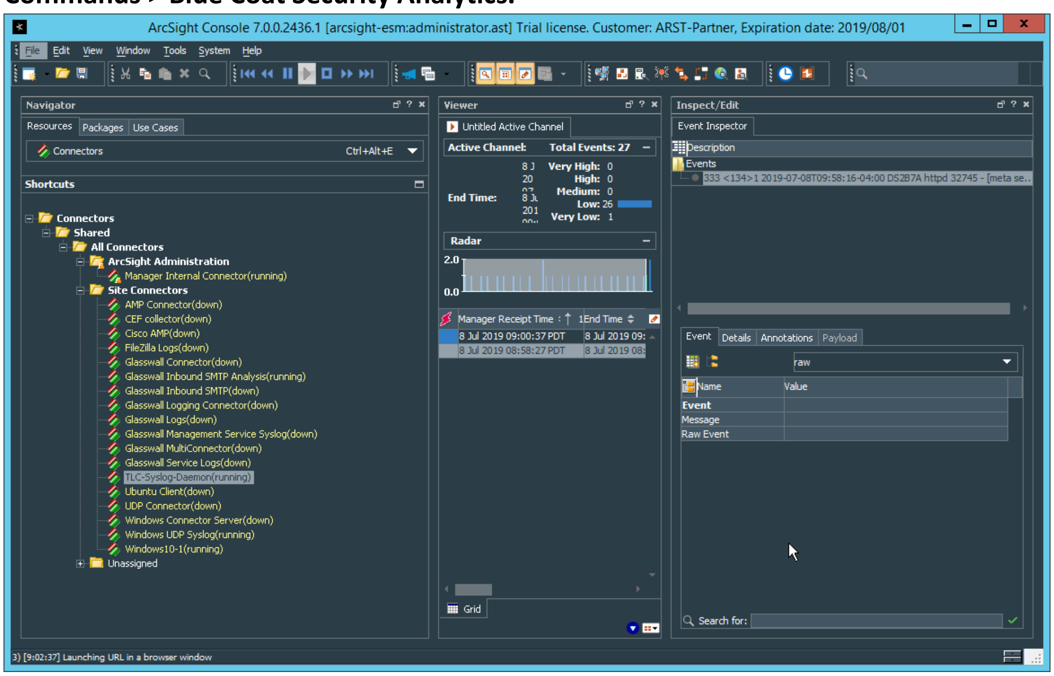
16. Right-click **Blue Coat Security Analytics,** and click **Edit Target.**



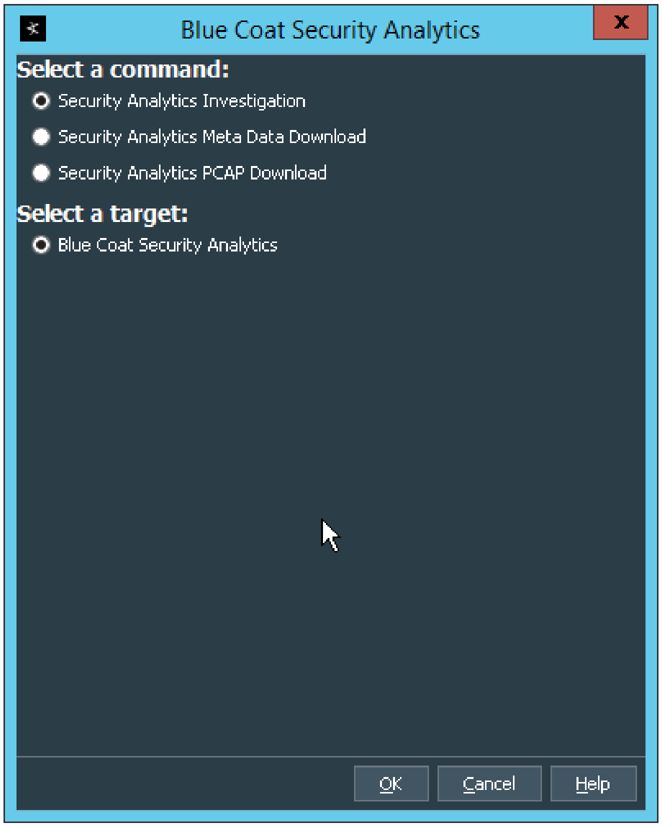
17. Click the **Integration Parameters** tab.
18. Replace the **SAHost** value with the IP address of Symantec Analytics.



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



21. Select **Security Analytics Investigation.**



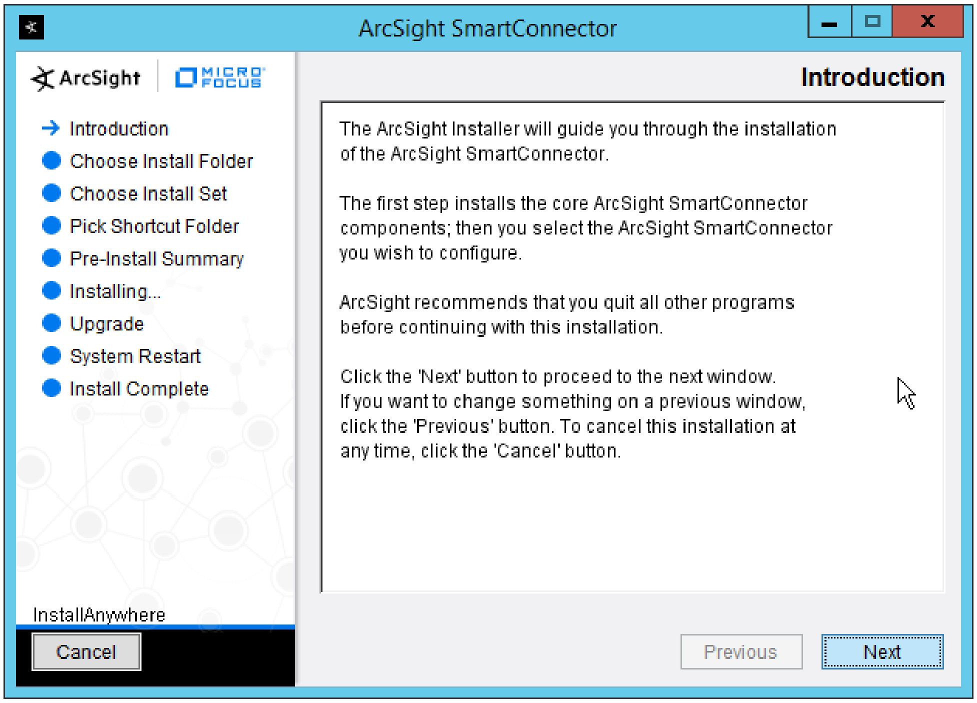
22. Click **OK.** This will open Security Analytics in the browser and perform a packet search based on the event parameters.

2.24 Integration: Micro Focus ArcSight and Glasswall FileTrust

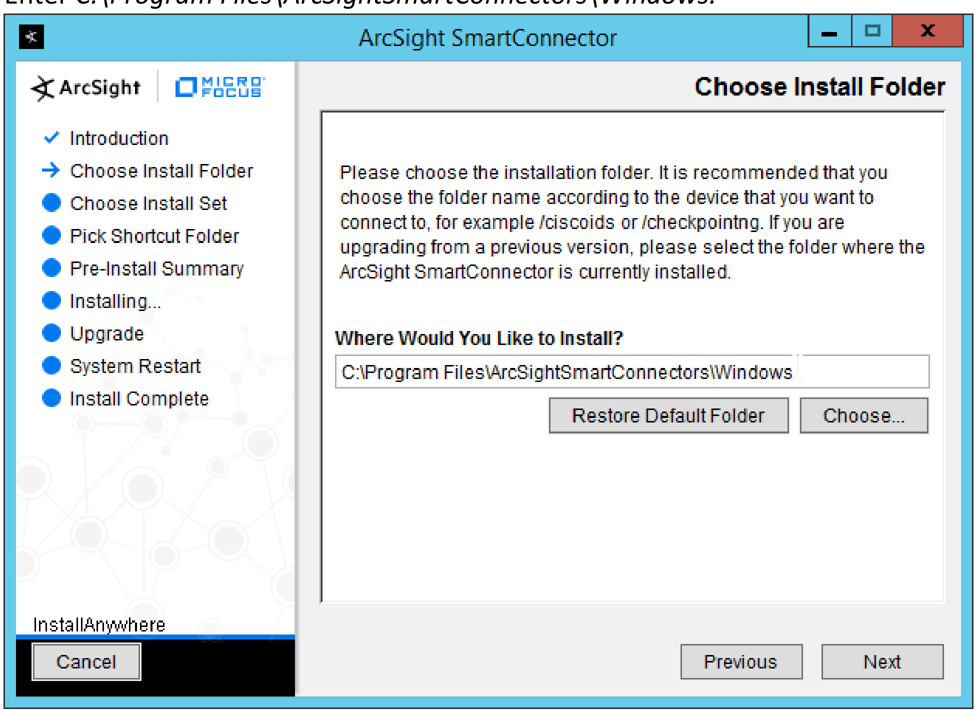
Glasswall FileTrust for Email stores its logs in *C:\Logging*, on the server running the **Glasswall** services.

2.24.1 Install Micro Focus ArcSight

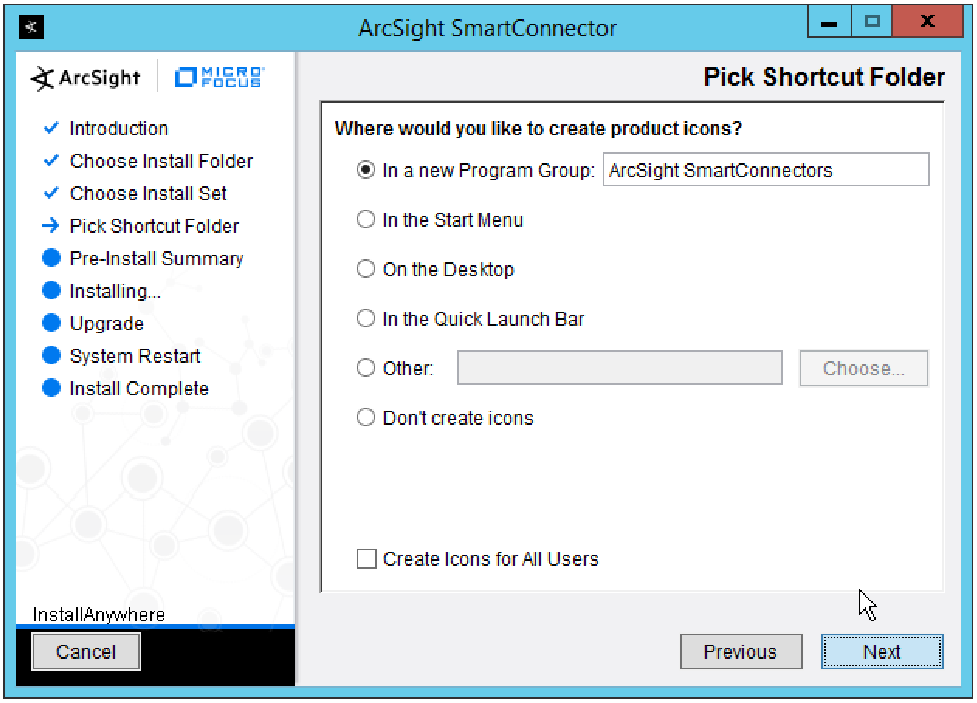
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on the same server as **Glasswall FileTrust.**



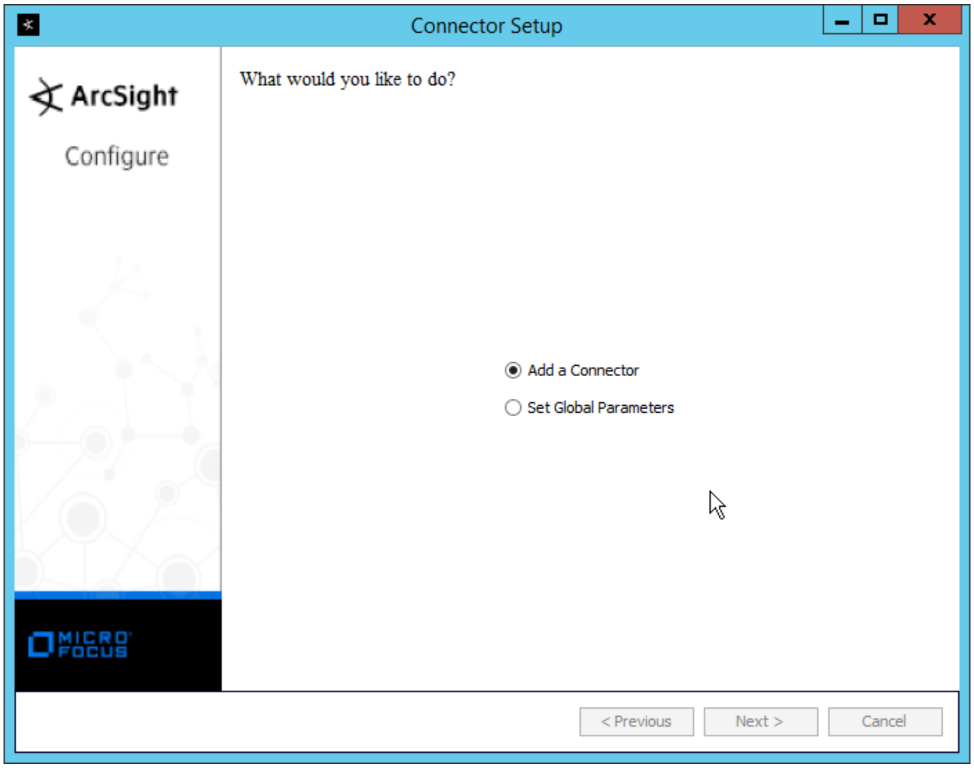
2. Click **Next.**
3. *Enter C:\Program Files\ArcSightSmartConnectors\Windows.*



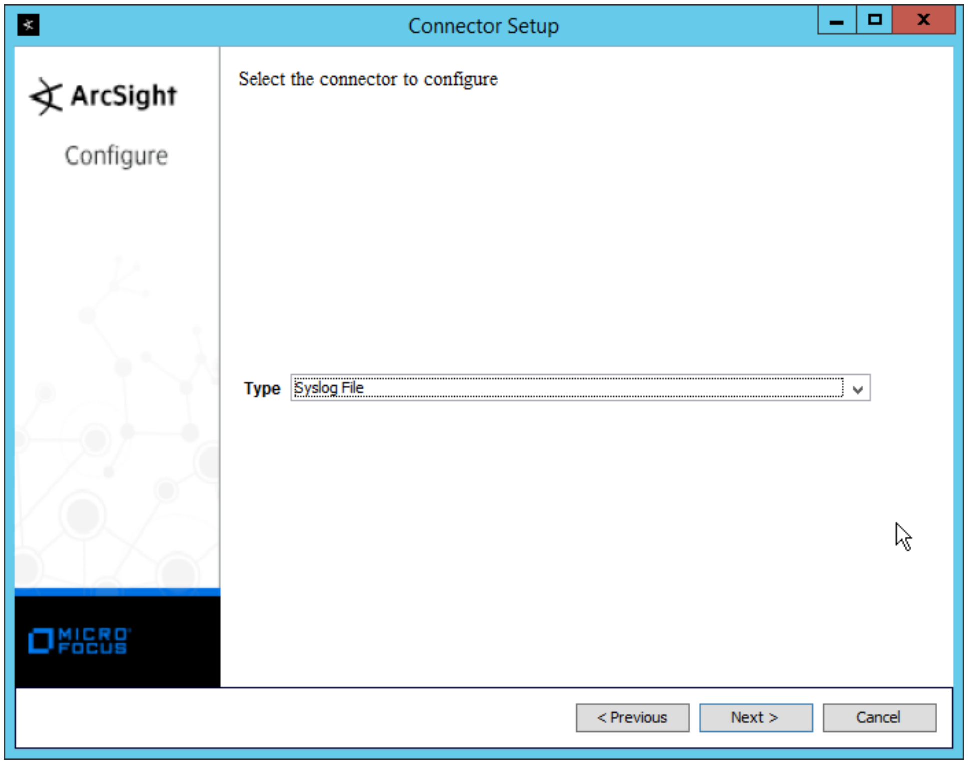
4. Click **Next.**



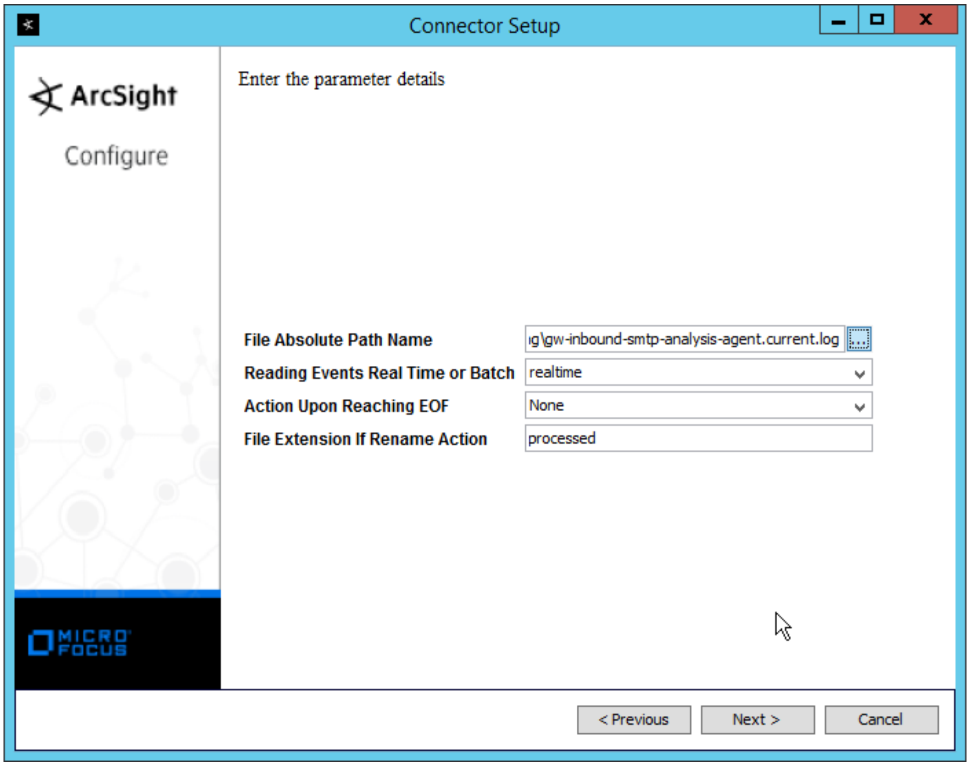
5. Click **Next.**
6. Click **Install.**
7. Select **Add a Connector.**



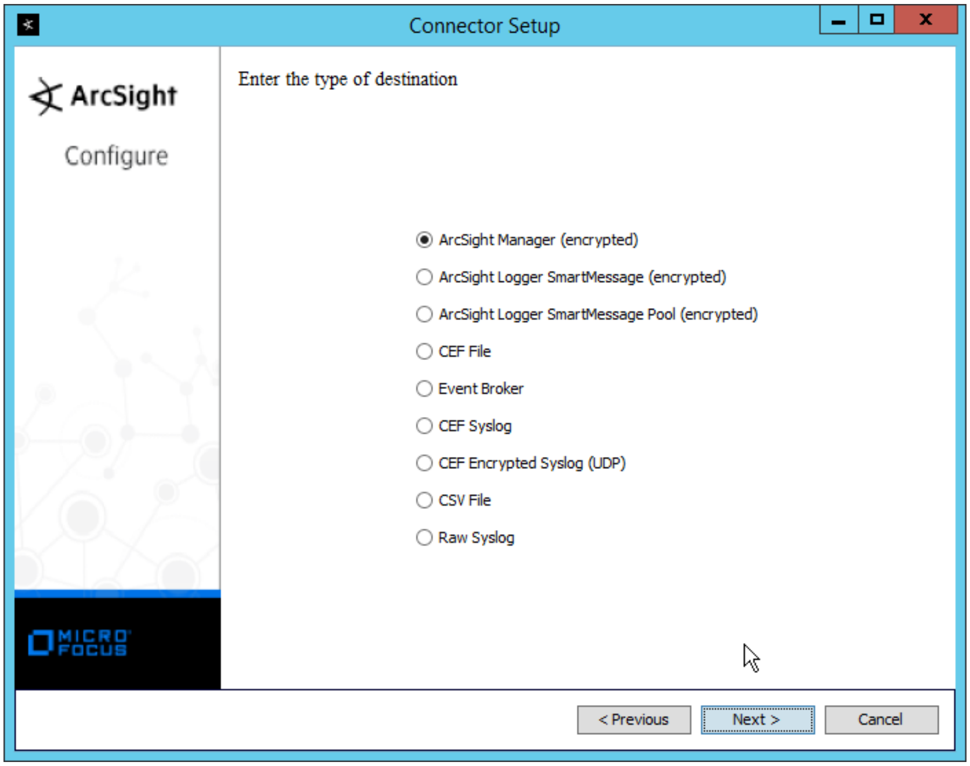
3050
3051 8. Click **Next.**
3052 9. Select **Syslog File.**



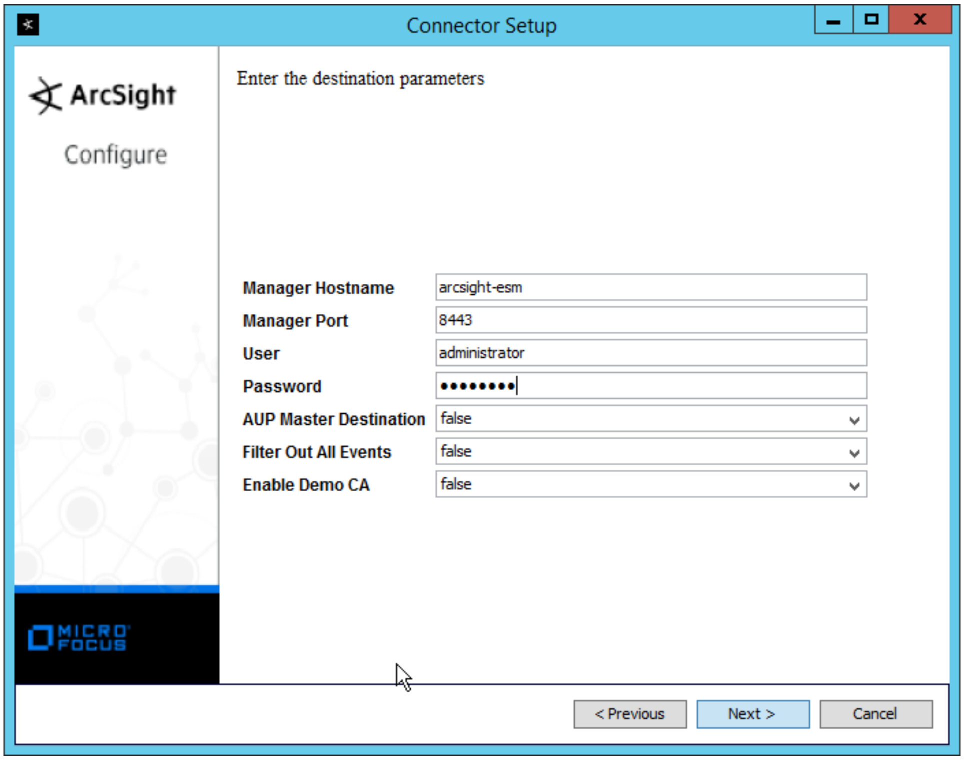
10. Click **Next.**
11. Enter *C:\Logging\gw-inbound-smtp-analysis-agent.current.log* for **File Absolute Path Name.**



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



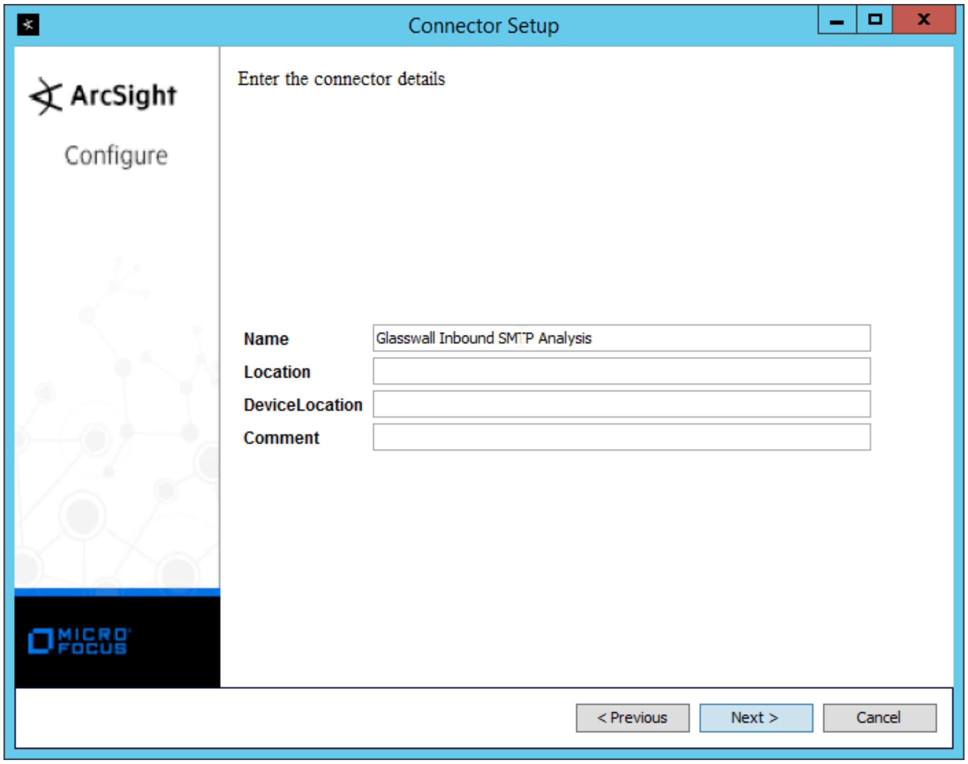
14. Click **Next.**
15. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.



3062

3063 16. Click **Next.**

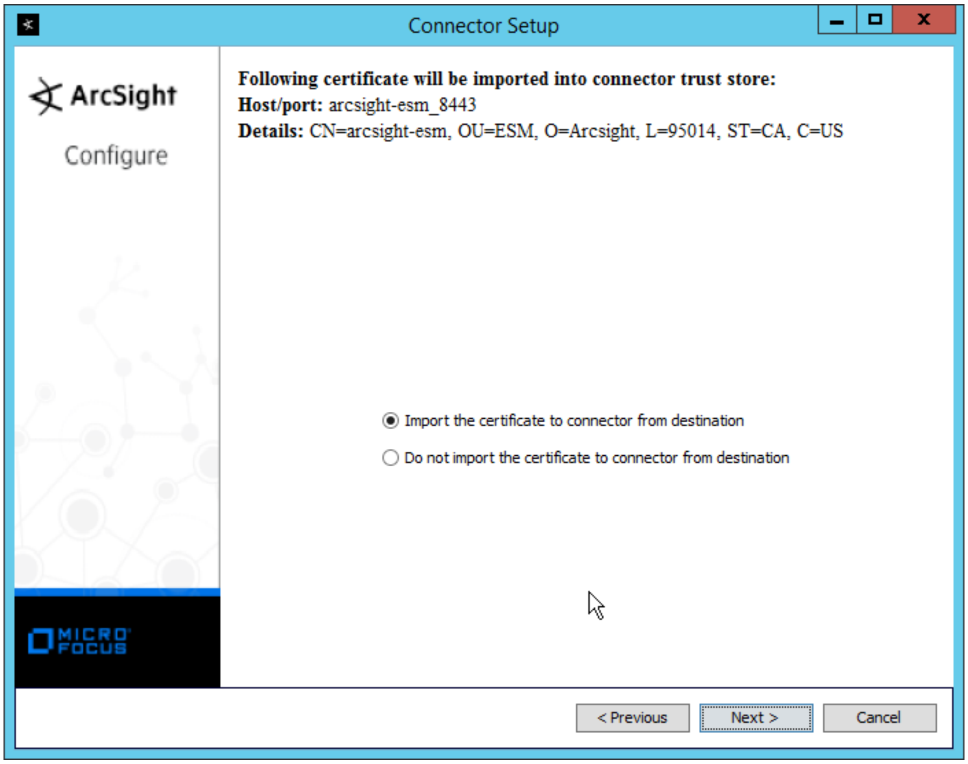
3064 17. Enter identifying details about the system (only **Name** is required).



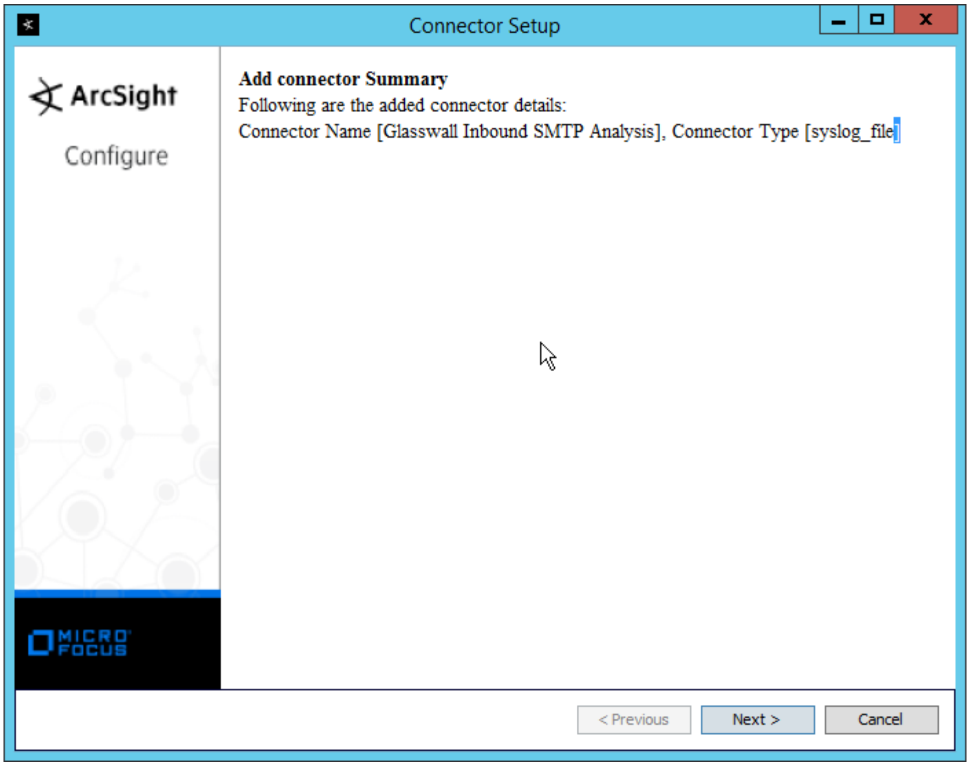
3065

3066 18. Click **Next.**

3067 19. Select **Import the certificate to connector from destination.**



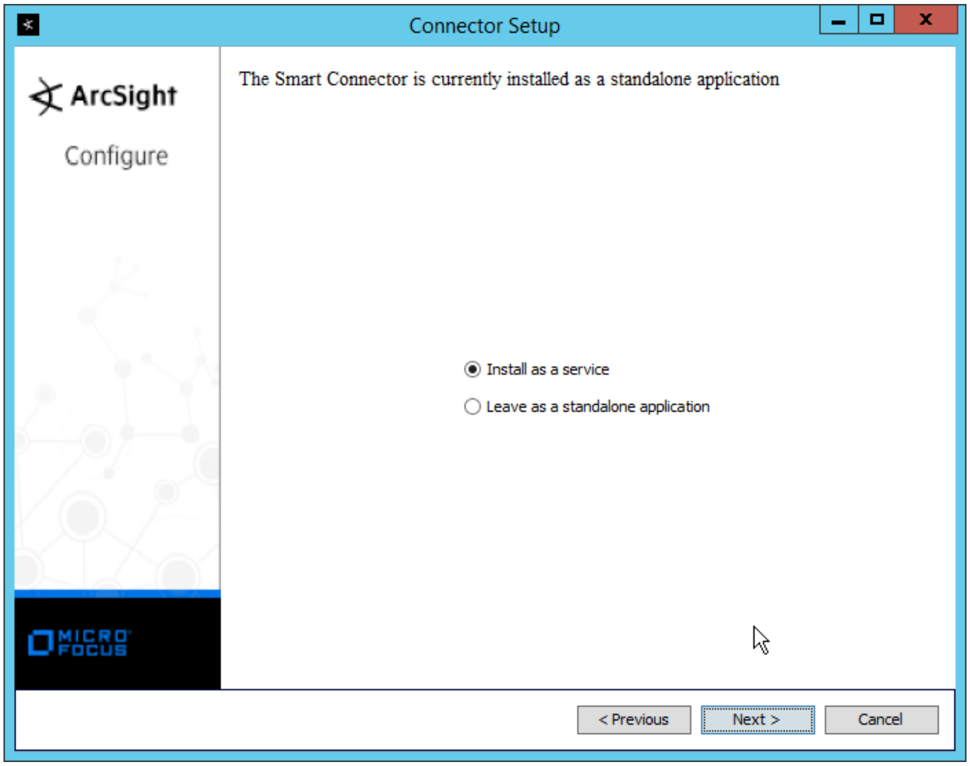
20. Click **Next.**



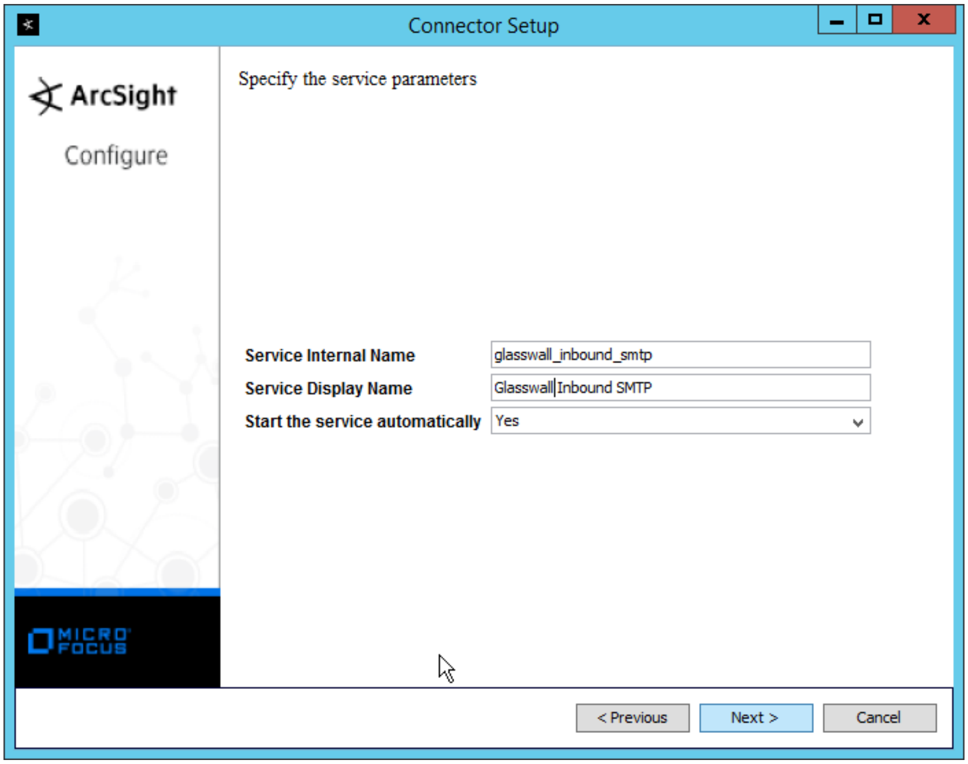
3070

3071 21. Click **Next.**

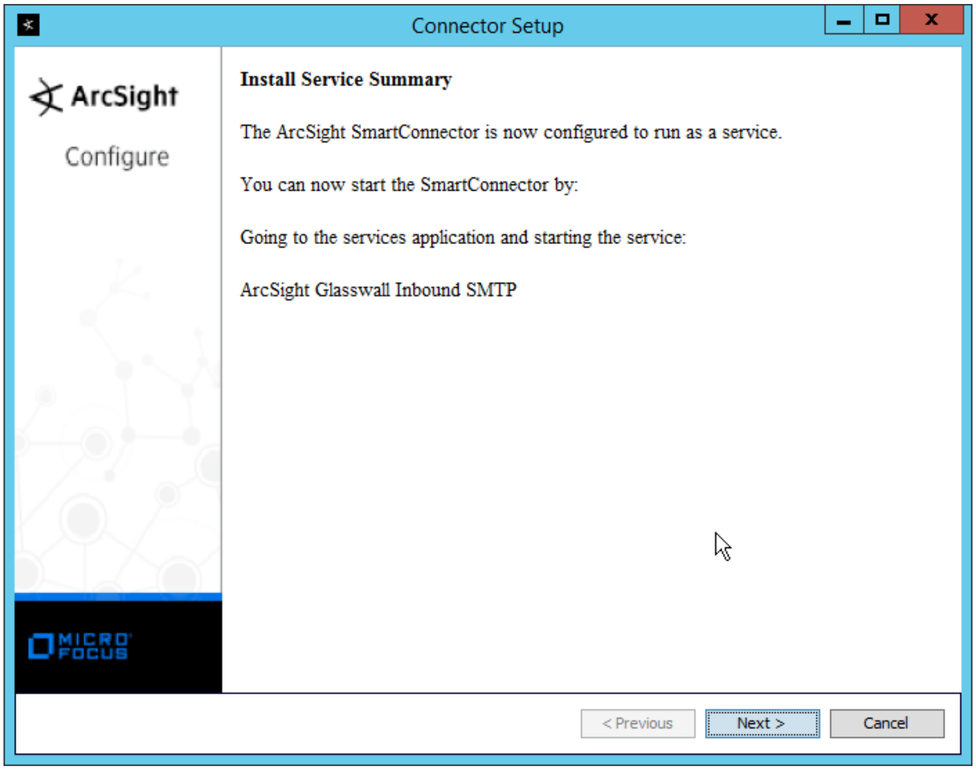
3072 22. Select **Install as a service.**



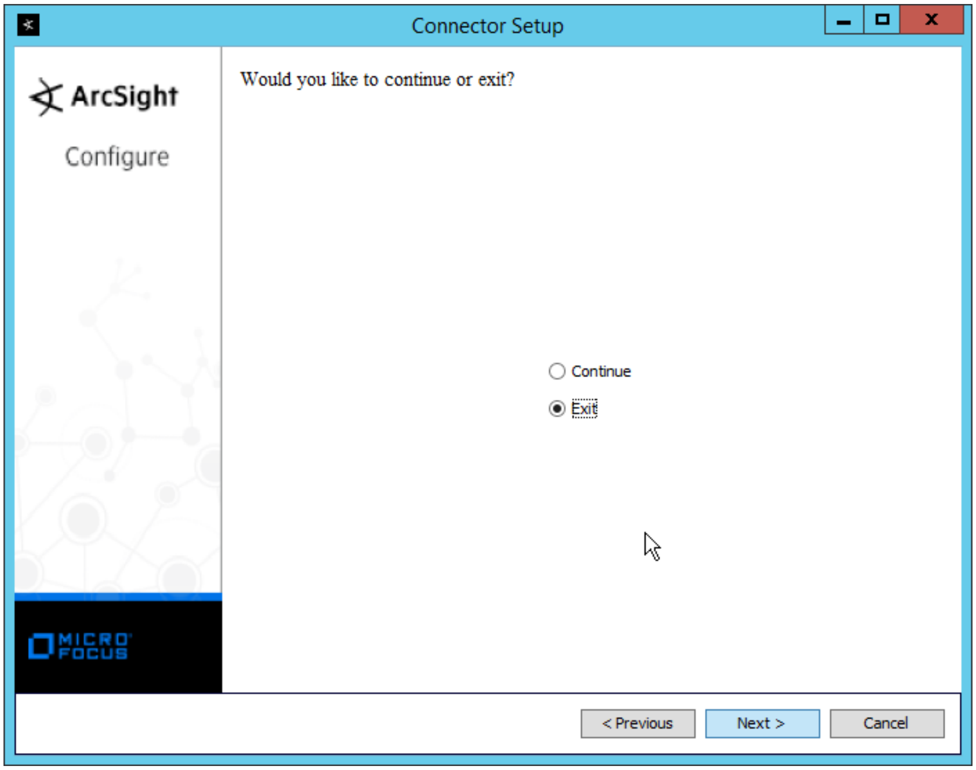
23. Click **Next.**
24. Change the service parameters to more appropriate names, because multiple connectors need to be installed on this server.



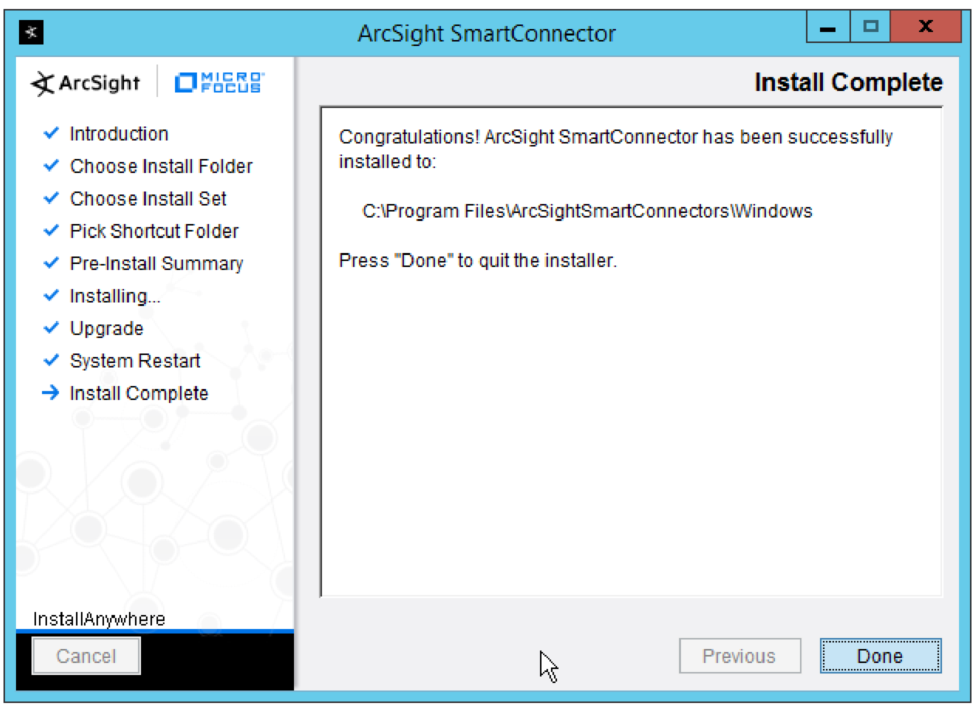
3077
3078 25. Click **Next.**



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



28. Click **Next.**



29. Click **Done.**

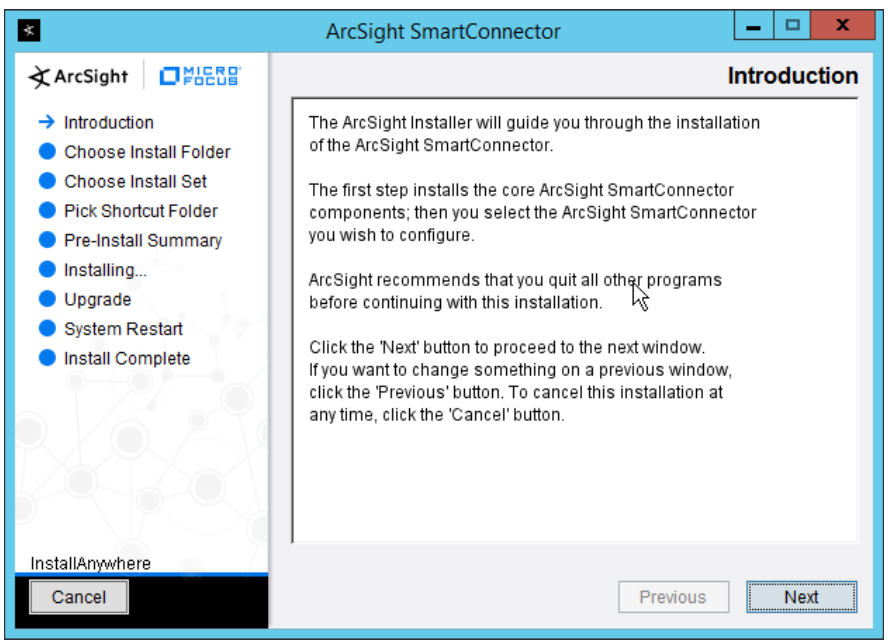
30. Repeat steps 1-29 for the other three “current” log files in *C:\Logging,* with the following caveats:
    a. Replace *C:\Program Files\ArcSightSmartConnectors\Windows* with a different folder name for each connector.
    b. Replace *C:\Logging\gw-inbound-smtp-analysis-agent.current.log* with the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

2.25 Integration: Micro Focus ArcSight and Cisco Stealthwatch

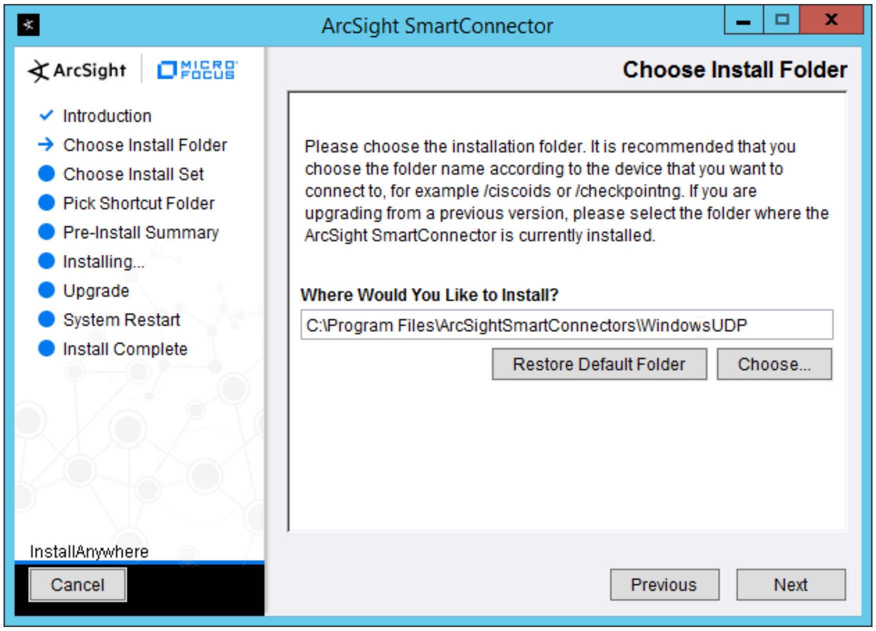
This section will detail the forwarding of logs from **Cisco Stealthwatch** to **Micro Focus ArcSight.**

2.25.1 Install Micro Focus ArcSight

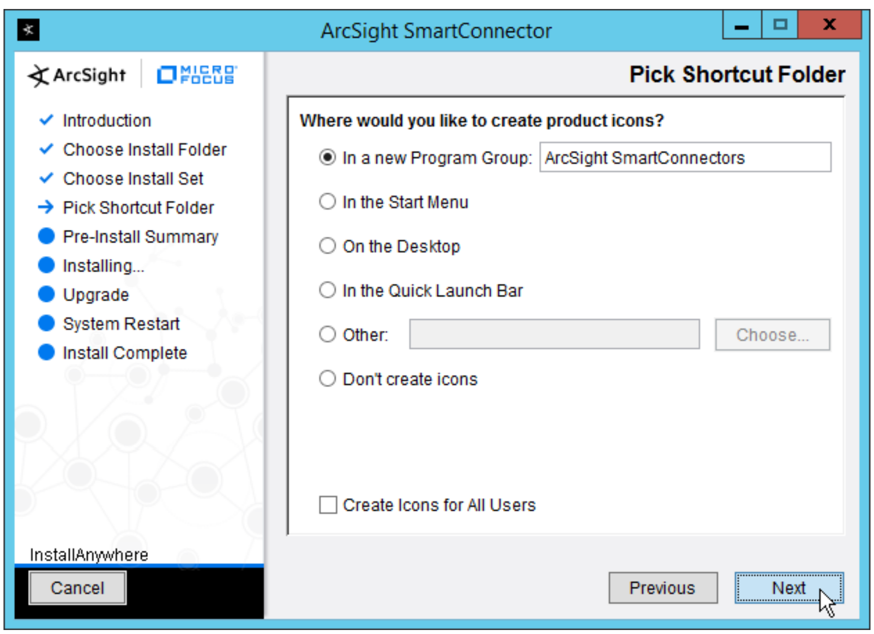
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Cisco Stealthwatch.**



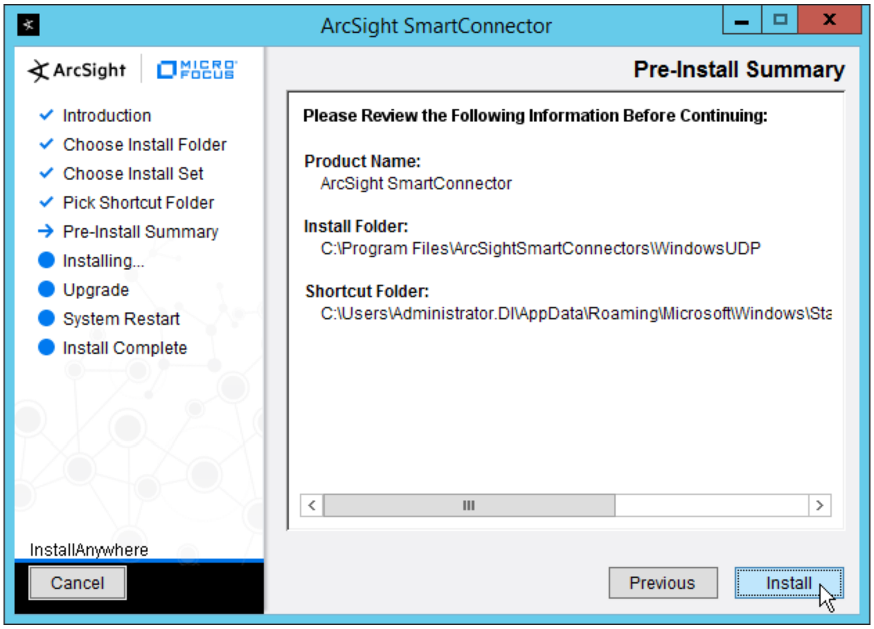
2. Click **Next.**
3. Enter C:*Program Files\ArcSightSmartConnectors\WindowsUDP.*



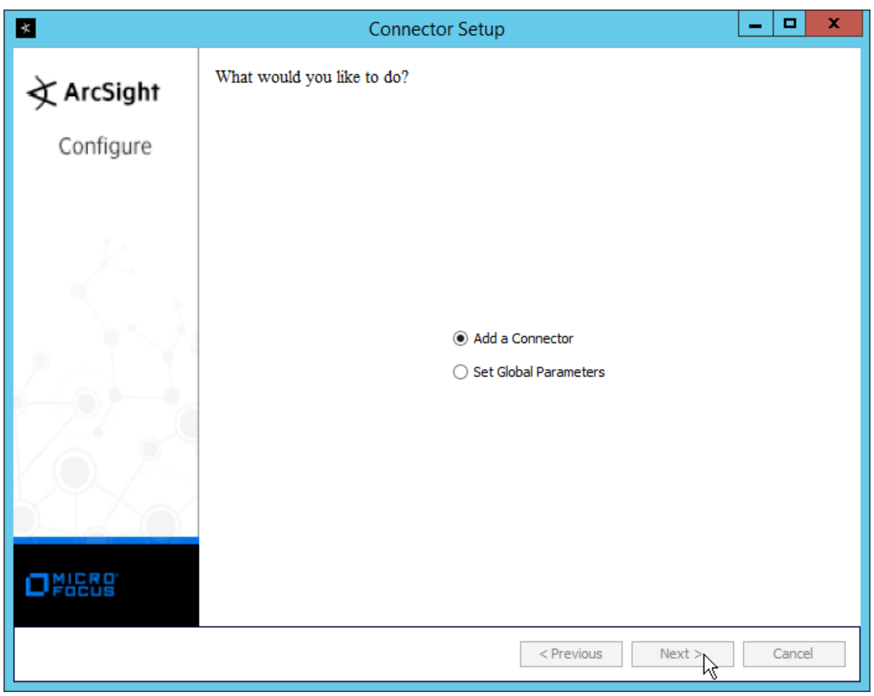
4. Click **Next.**



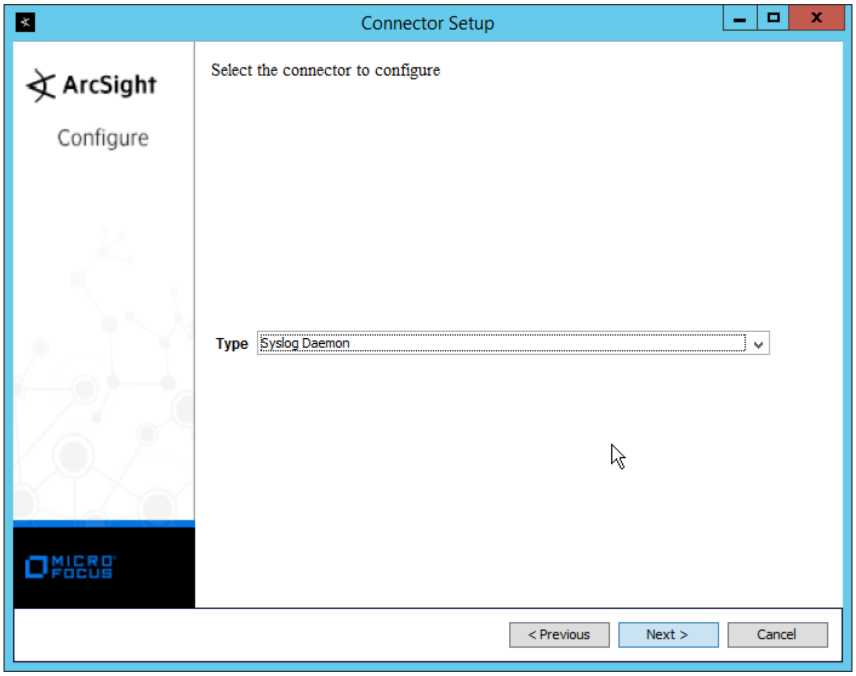
5. Click **Next.**



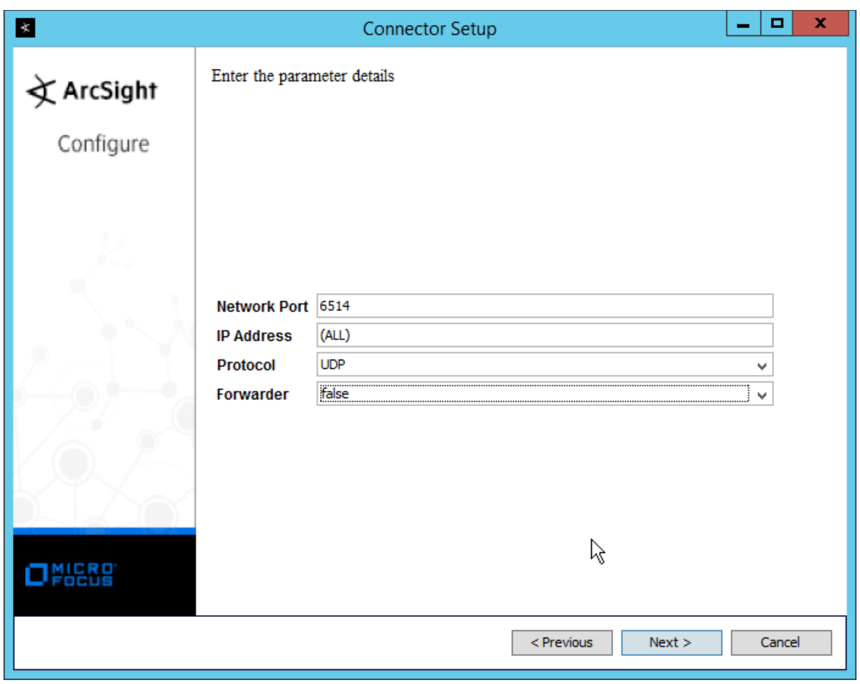
6. Click **Install.**
7. Select **Add a Connector.**



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

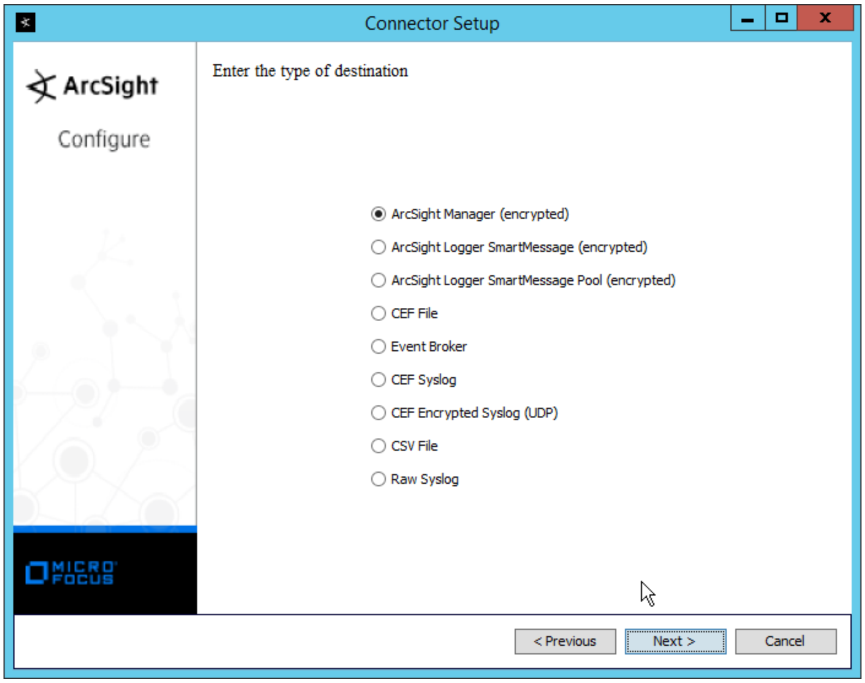


10. Click **Next.**
11. Enter an unused port for the daemon to run on. (Ensure that this port is allowed through the firewall.)
12. Select **UDP** for **Protocol.**

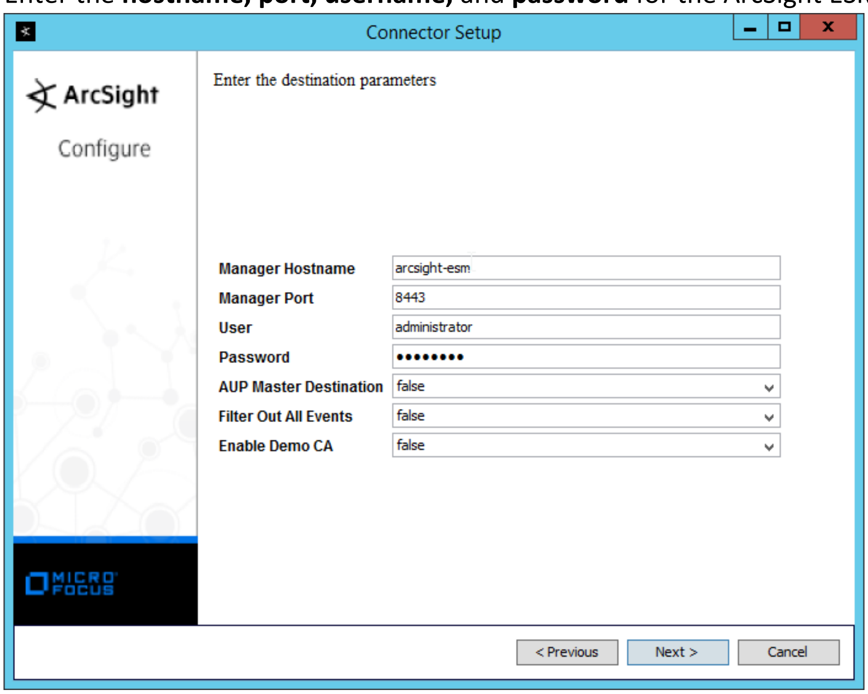


13. Click **Next.**

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

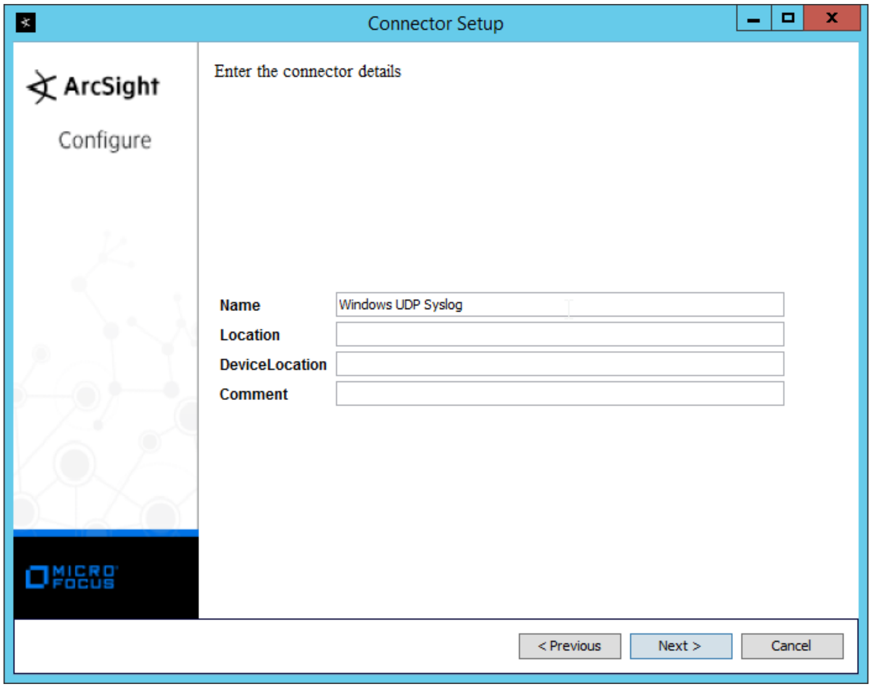


15. Click **Next.**
16. Enter the **hostname, port, username,** and **password** for the ArcSight ESM server.

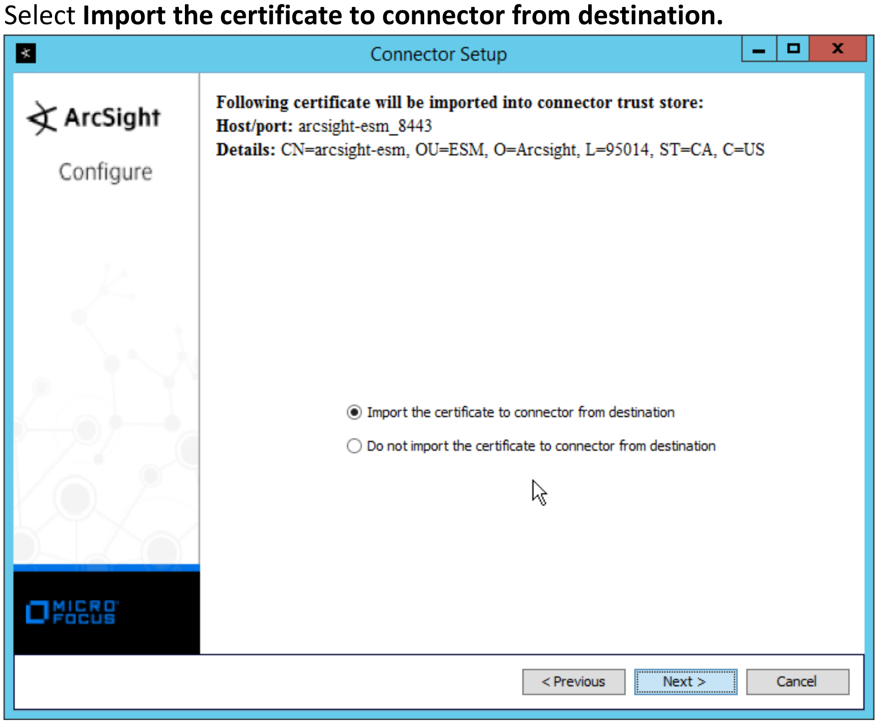


17. Click **Next.**

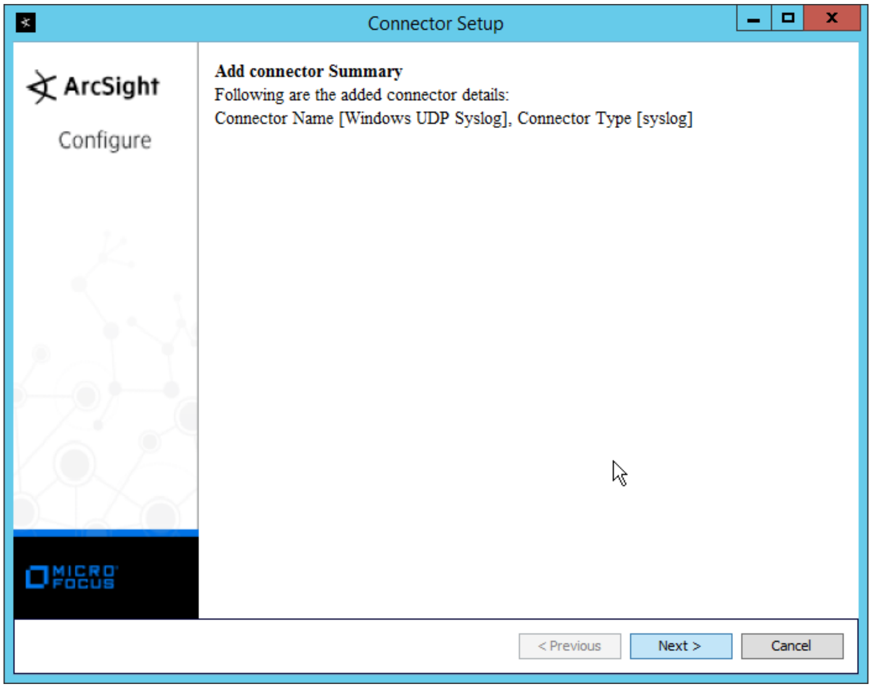
18. Enter identifying details about the system (only **Name** is required).



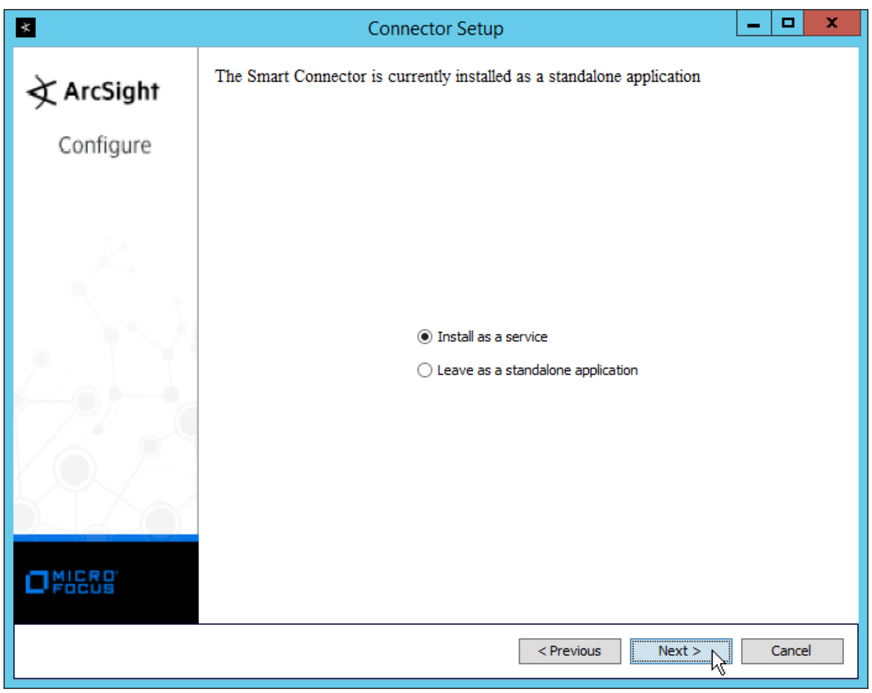
19. Click **Next.**
20. Select **Import the certificate to connector from destination.**



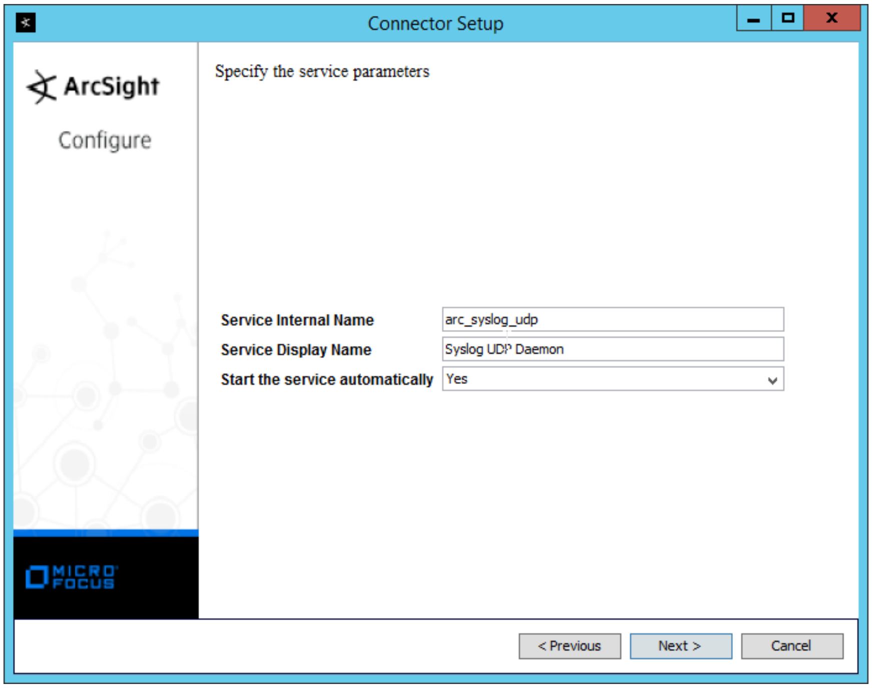
21. Click **Next.**



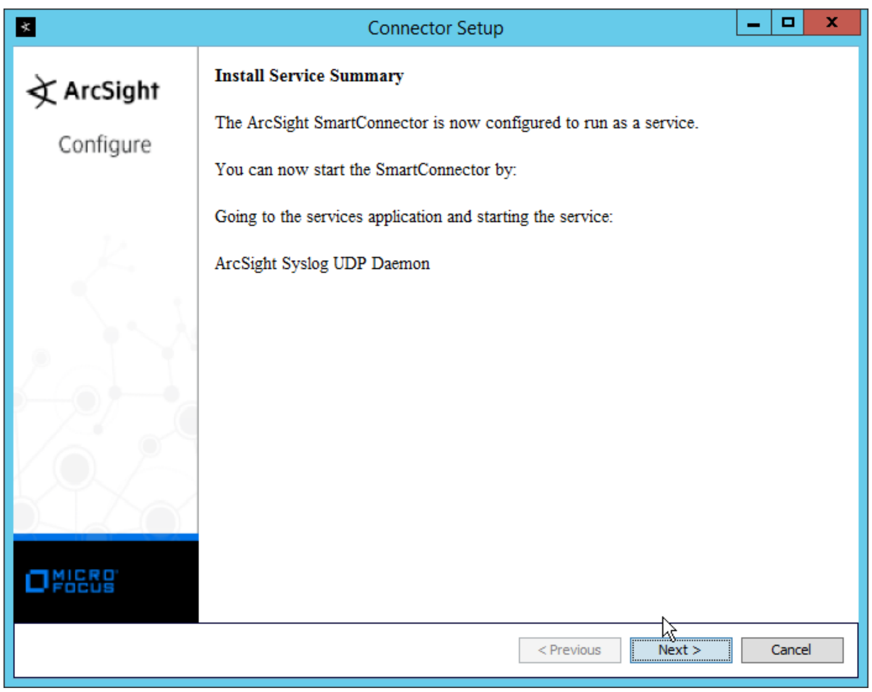
22. Click **Next.**
23. Select **Install as a service.**



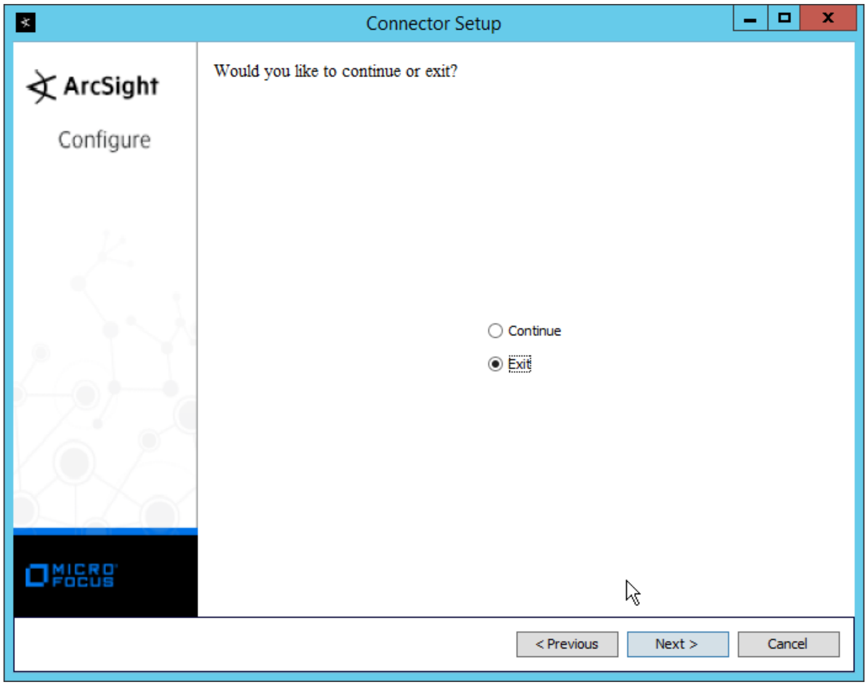
24. Click **Next.**
25. Enter a service name and display name.



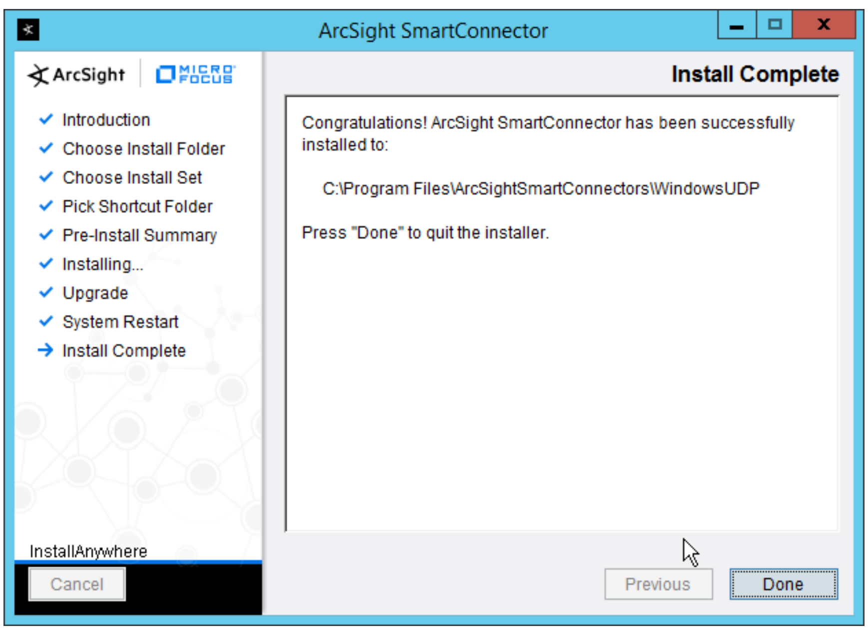
26. Click **Next.**



27. Click **Next.**
28. Select **Exit.**



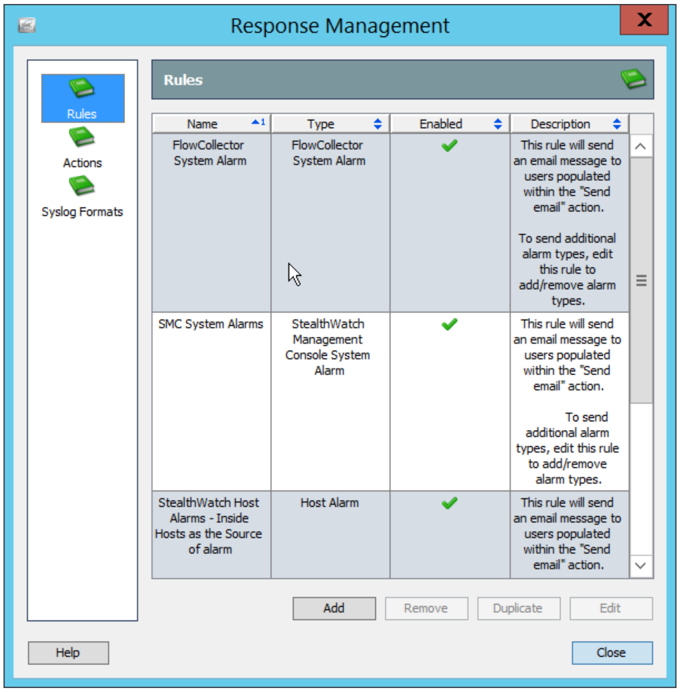
29. Click **Next.**



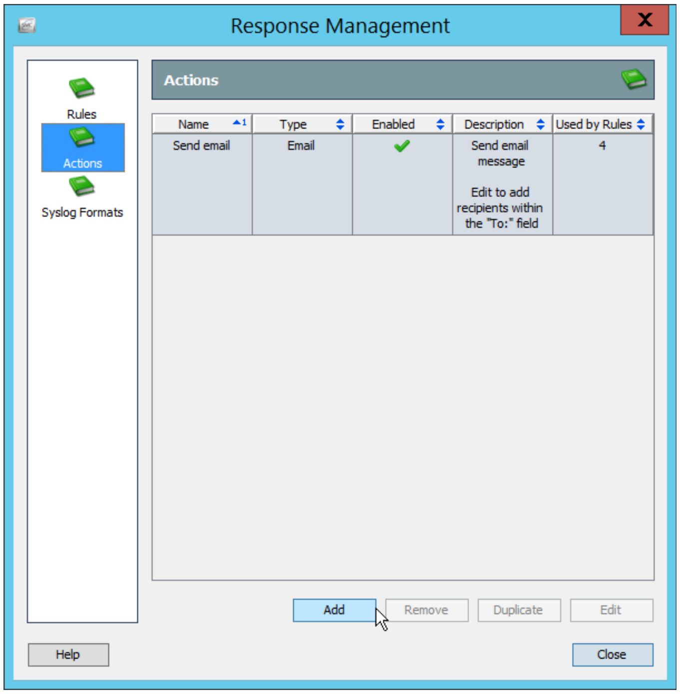
30. Click **Done.**

2.25.2 Configure Cisco Stealthwatch

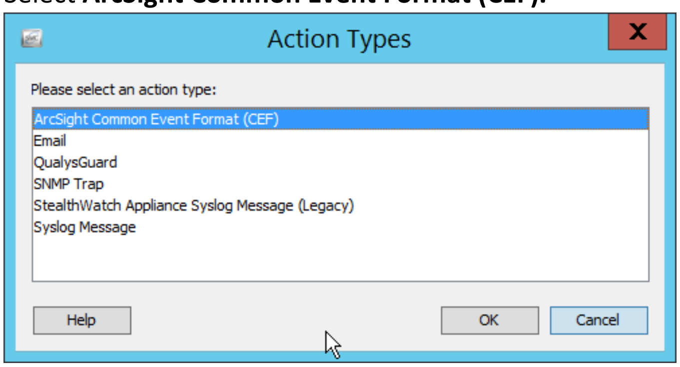
1. Log in to the **Cisco Stealthwatch Management Console** desktop interface. (This can be downloaded from the web interface and run using **javaws.exe.** You may need to add the site to your Java exceptions in **Control Panel > Java.**)
2. Click **Configuration > Response Management.**



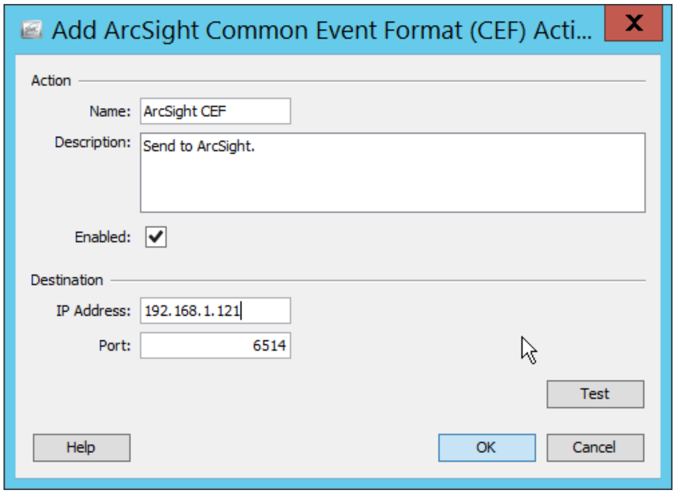
3. Click **Actions.**



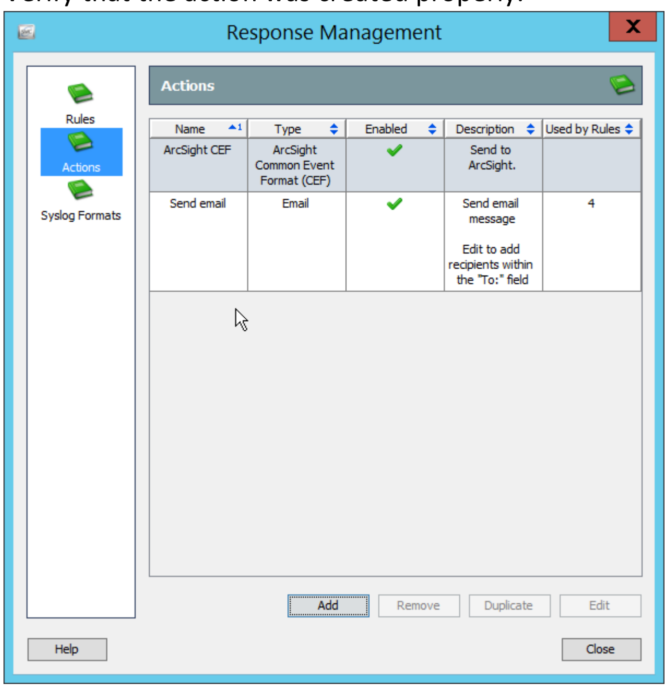
4. Click **Add.**
5. Select **ArcSight Common Event Format (CEF).**



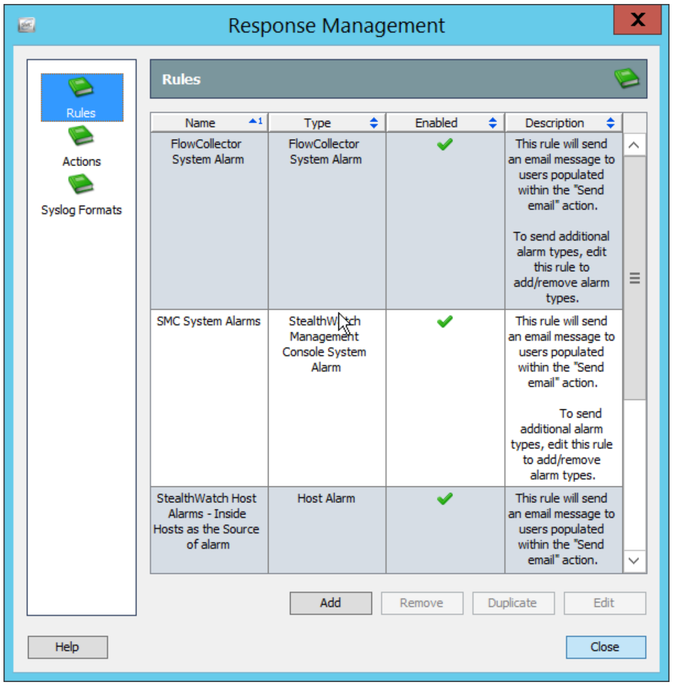
6. Click **OK.**
7. Enter a **name** for the **Action.**
8. Enter a **description.**
9. Enter the **IP address** of the server with the UDP ArcSight Connector that you just created.
10. Enter the **port** used in the UDP ArcSight Connector that you just created.
11. (Optional) Click **Test** to send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



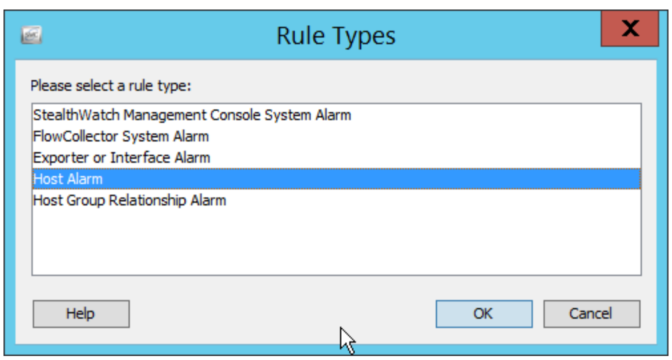
12. Click **OK.**
13. Verify that the action was created properly.



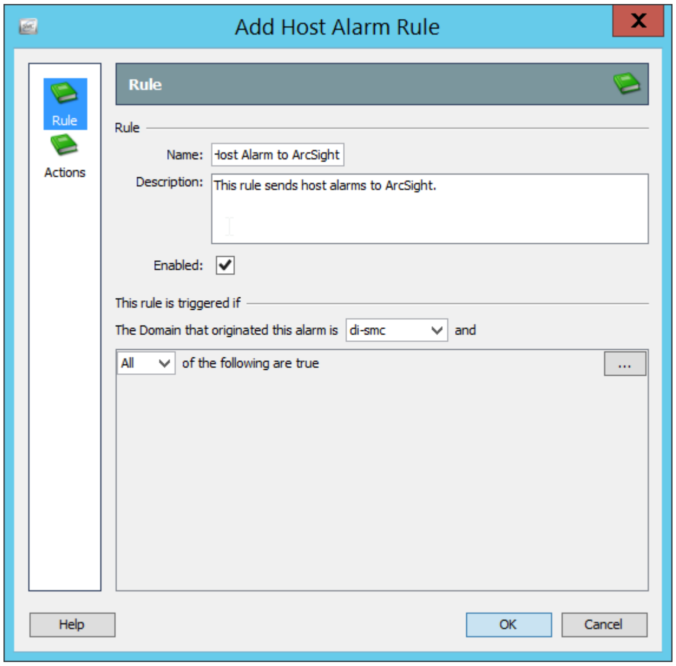
14. Click **Rules.**



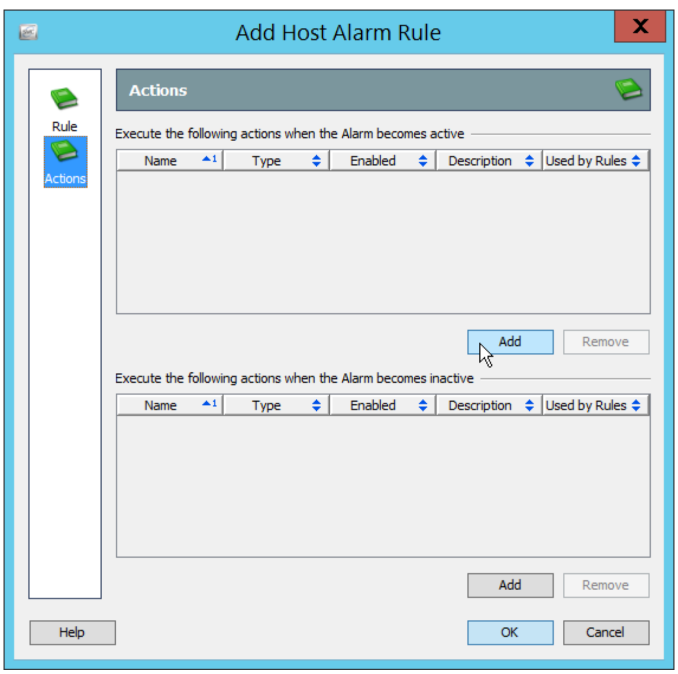
15. Click **Add.**
16. Select **Host Alarm.**



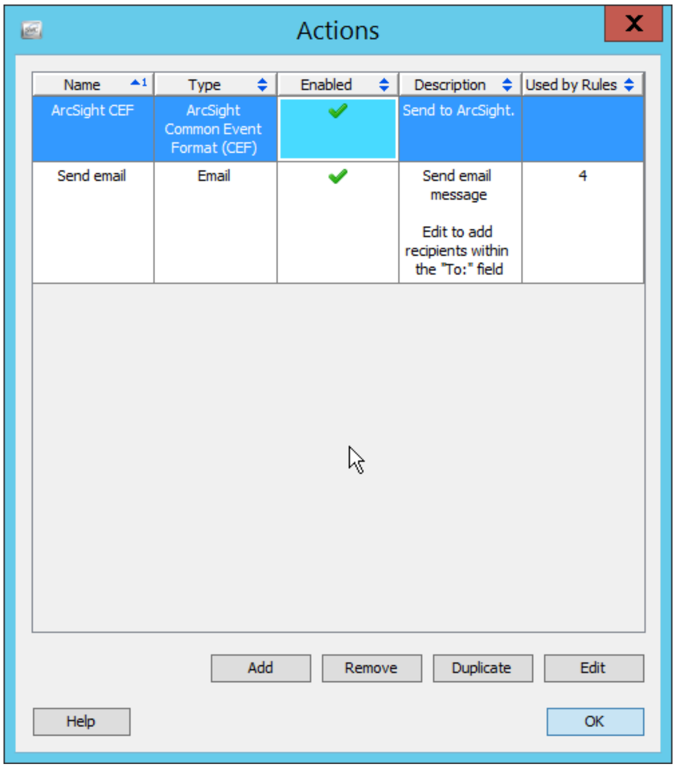
17. Click **OK.**
18. Enter a **name.**
19. Enter a **description.**



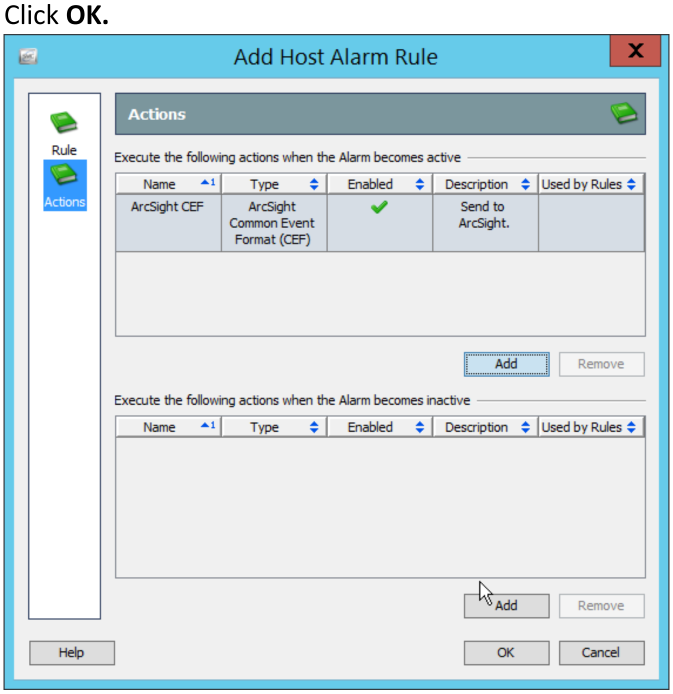
20. Click **Actions.**



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

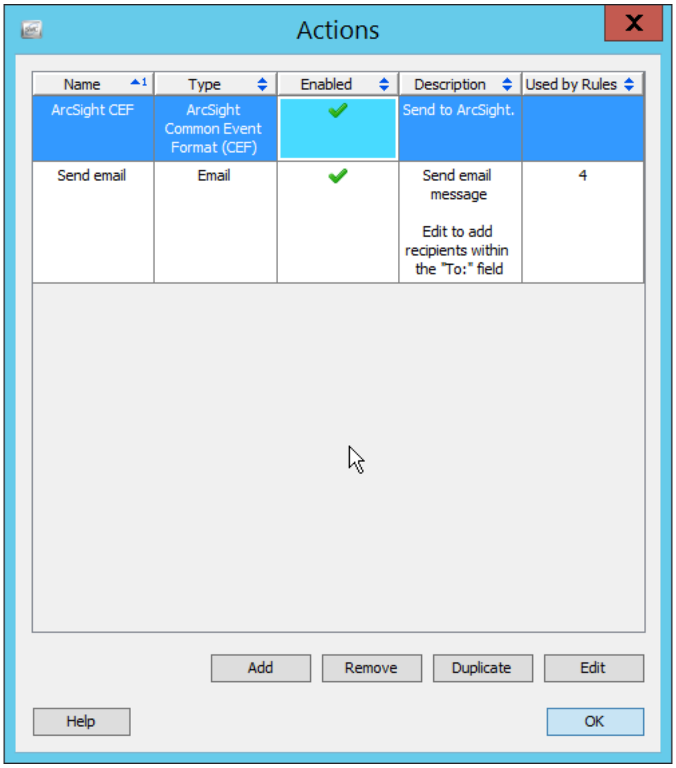


23. Click **OK.**

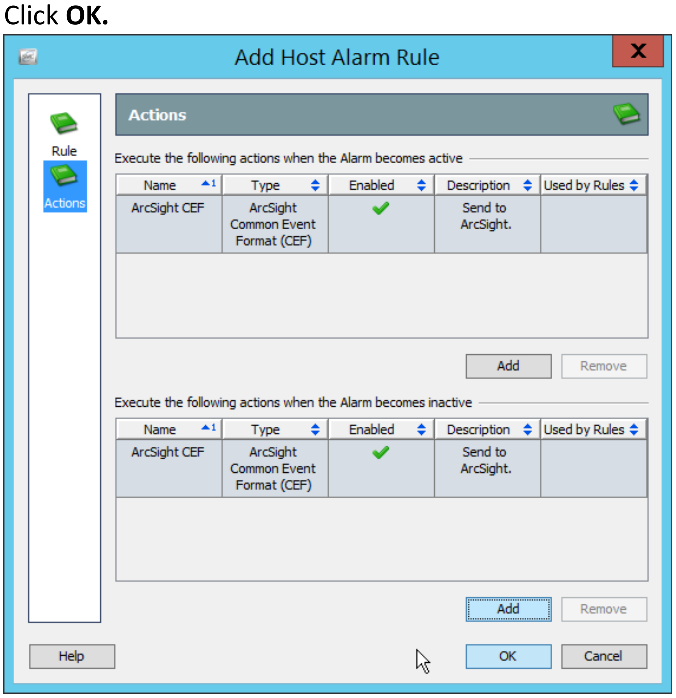


24. Click the **Add** button for the bottom section; this adds an action when the alarm becomes inactive.

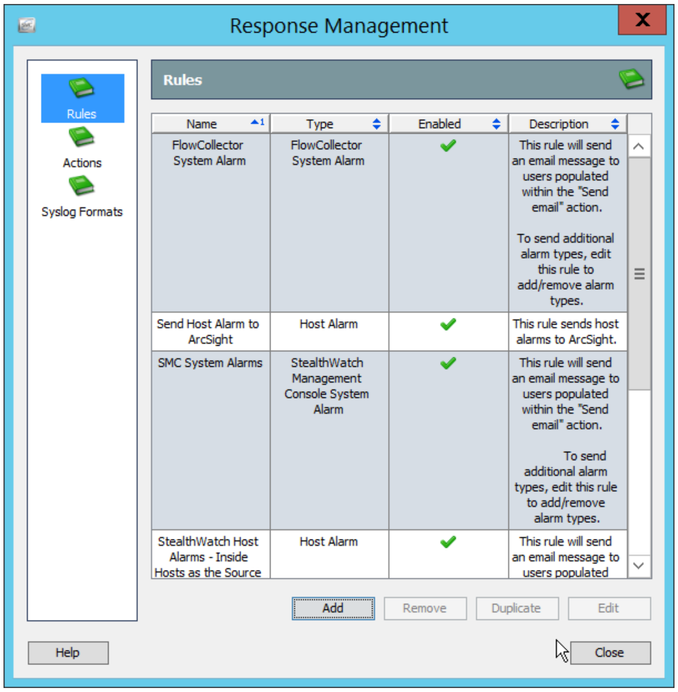
25. Select the ArcSight CEF rule you just created.



26. Click **OK.**



3175 27. Click **OK.**



3176 **28.** Click **Close.**

Appendix A List of Acronyms

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