NIST SPECIAL PUBLICATION 1800-11C

Data Integrity

Recovering from Ransomware and Other Destructive Events

Volume C:
How-to Guides

Timothy McBride
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Ekstrom
Lauren Lusty
Julian Sexton
Anne Townsend
The MITRE Corporation
McLean, VA

September 2020

FINAL

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-11

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-11C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-11C, 378 pages, (September 2020), CODEN: NSPUE2

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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 data corruption events could cause a significant loss to a company's reputation, business operations, and bottom line.

These types of adverse events, that ultimately impact data integrity, can compromise critical corporate information including emails, employee records, financial records, and customer data. It is imperative for organizations to recover from a data integrity attack and trust the accuracy and precision of the recovered data.

The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to explore methods to effectively recover from a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also implemented auditing and reporting IT system use to support incident recovery and investigations.

This NIST Cybersecurity Practice Guide demonstrates how organizations can implement technologies to take immediate action following a data corruption event. The example solution outlined in this guide encourages effective monitoring and detection of data corruption in standard, enterprise components as well as custom applications and data composed of open-source and commercially available components.

KEYWORDS

business continuity; data integrity; data recovery; malware; ransomware

ACKNOWLEDGMENTS

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

Name	Organization
Steve Petruzzo	GreenTec USA
Steve Roberts	Hewlett Packard Enterprise
Dave Larimer	IBM Corporation
John Unthank	IBM Corporation
Jim Wachhaus	Tripwire
Donna Koschalk	Veeam Software Corporation
Dewain Smith	Veeam Software Corporation
Lisa Ignosci	Veeam Software Corporation

Name	Organization
Brian Abe	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Josh Klosterman	The MITRE Corporation
Susan Urban	The MITRE Corporation
Mary Yang	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
GreenTec USA	GreenTec WORMdisk, v151228
Hewlett Packard Enterprise	HPE ArcSight ESM, v6.9.1 HPE ArcSight Connector, v7.4.0
IBM Corporation	IBM Spectrum Protect, v8.1.0
Tripwire	Tripwire Enterprise, v8.5 Tripwire Log Center, v7.2.4.80
Veeam Software Corporation	Veeam Availability Suite 9.5

Contents

1 Introduction

The following guides show IT professionals and security engineers how we implemented this data integrity solution example. We cover all 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 integrated the products into 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 solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-11A: *Executive Summary*
- NIST SP 1800-11B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-11C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary (NIST SP 1800-11A)*, which describes the:

- challenges enterprises face in protecting their data from loss or corruption
- example solution built at the National Cybersecurity Center of Excellence (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 1800-11B,* which describes what we did and why. The following sections will be of particular interest:

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

Consider sharing the *Executive Summary (NIST SP 1800-11A)* with your leadership team 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 1800-11C)* to replicate all or parts of the build created in our lab. The guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we integrated the products in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we 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 the data integrity 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.

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 recover from a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also explored the issues of auditing and reporting that IT systems use to support incident recovery and investigations. 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 5.1. 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, configuring, and integrating all the products used to build an instance of the example solution.

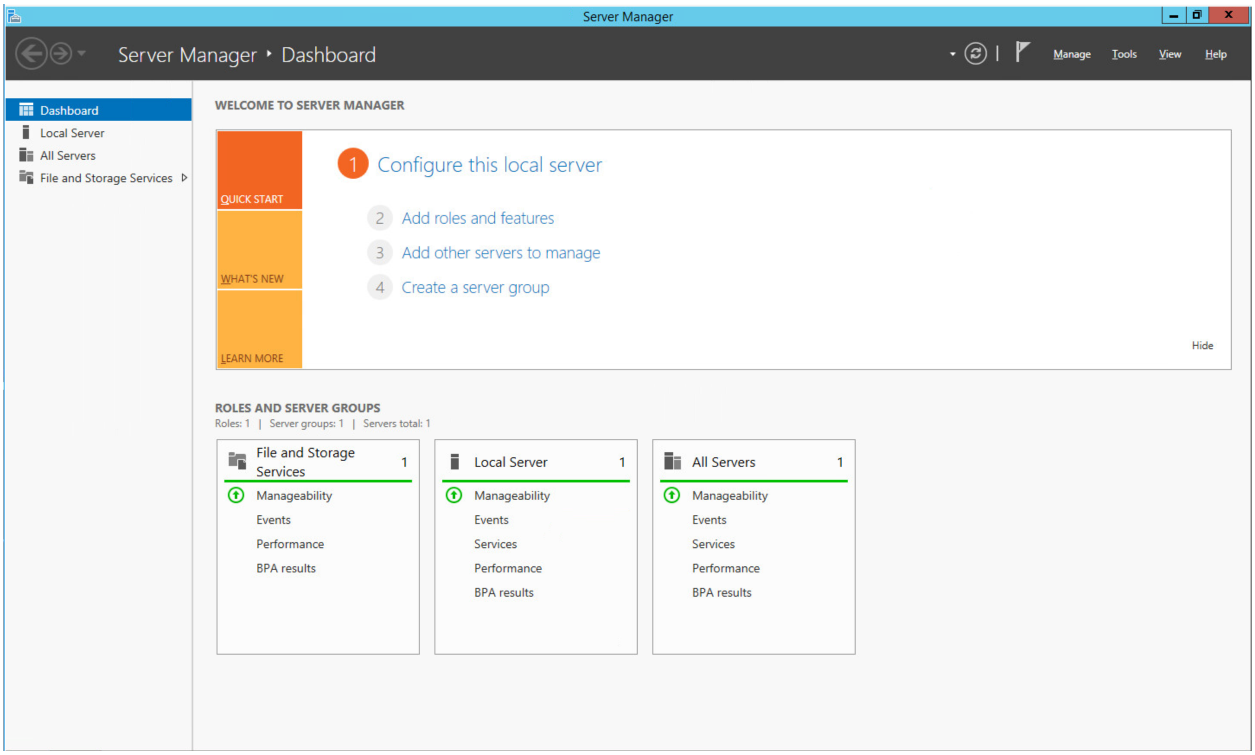
The products presented in this document have the potential to change both interfaces and functionality. This document aims to highlight the core configurations an organization could use along with visual representations of those configurations.

2.1 Active Directory and Domain Name System (DNS) Server

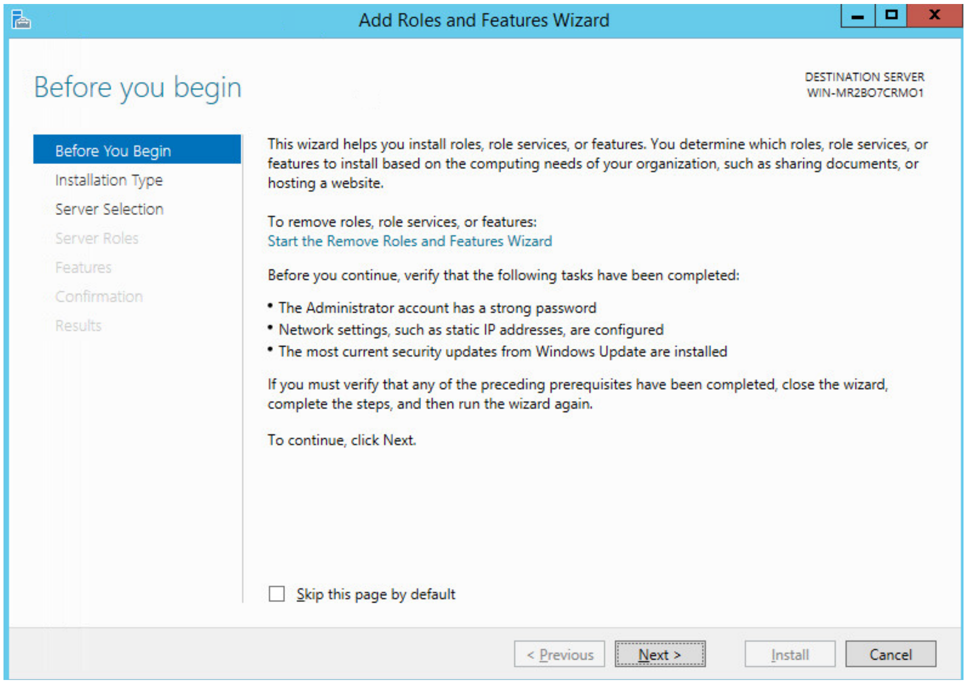
As part of our enterprise emulation, we included an Active Directory server that doubles as a DNS server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

2.1.1 Installing Features

1. Open **Server Manager**.



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



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

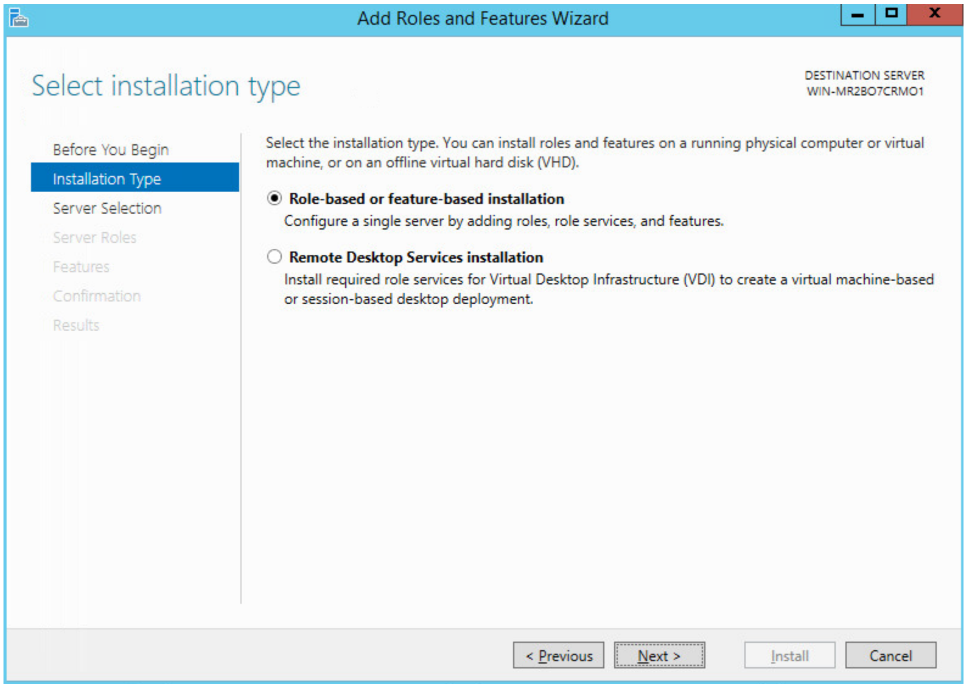
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

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

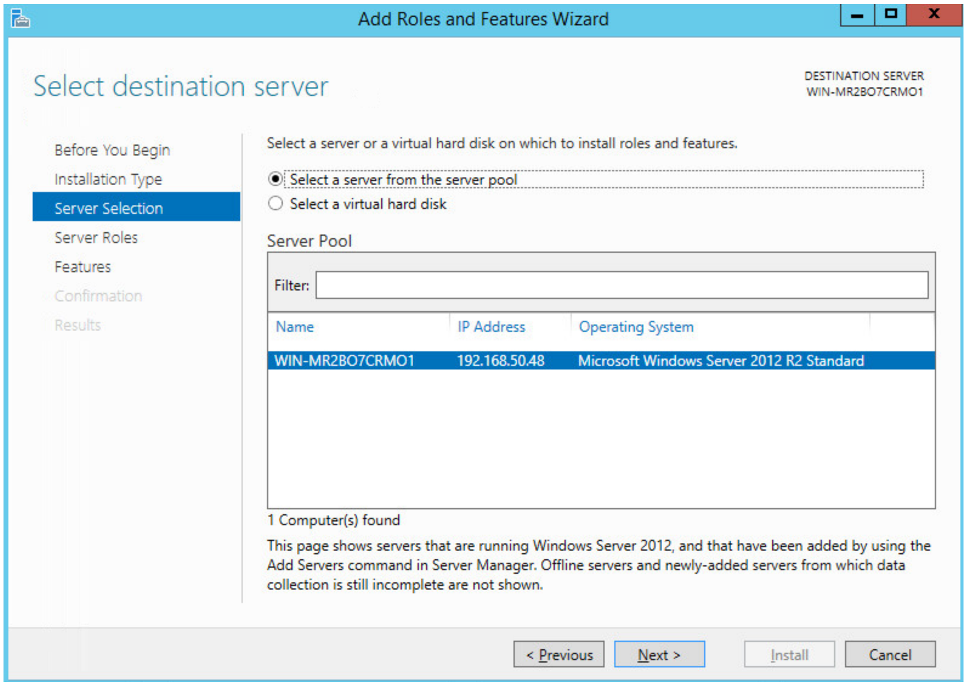


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

5. Click **Next**.



Select destination server

DESTINATION SERVER
WIN-MR2BO7CRMO1

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

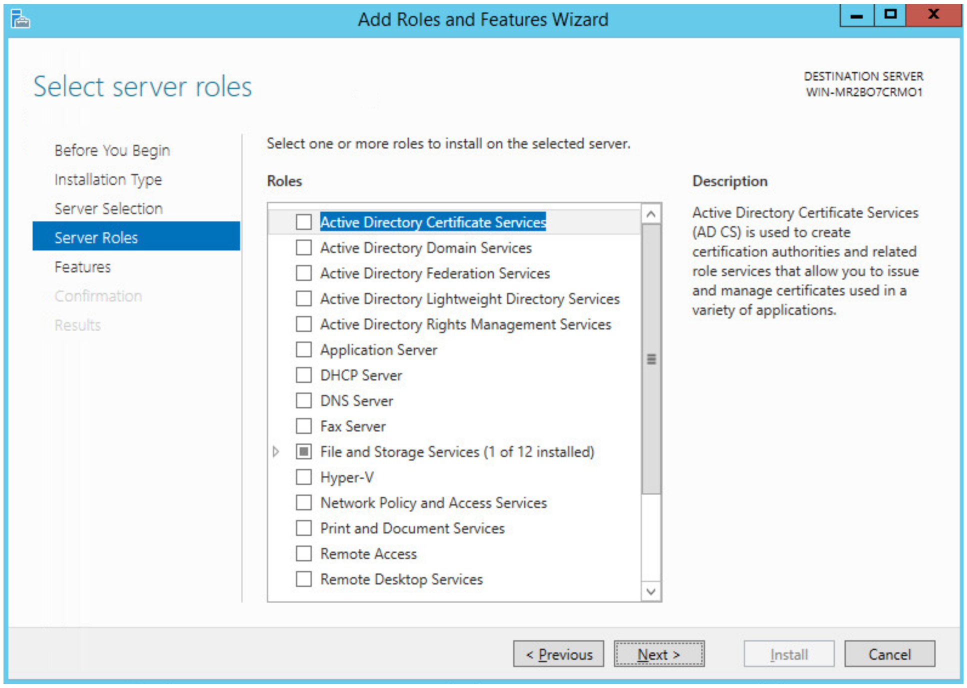
Filter:

Name	IP Address	Operating System
WIN-MR2BO7CRMO1	192.168.50.48	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.

6. Select **ADDNS** (or the correct Windows Server name) from the list.
7. Click **Next**.



Select server roles

DESTINATION SERVER
WIN-MR2BO7CRMO1

Select one or more roles to install on the selected server.

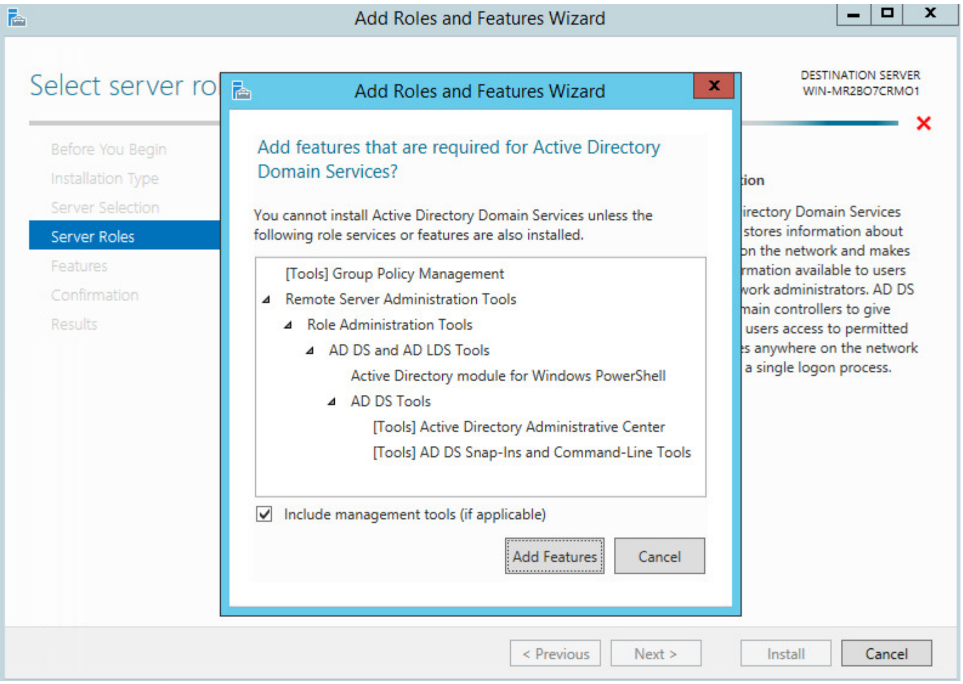
Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

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



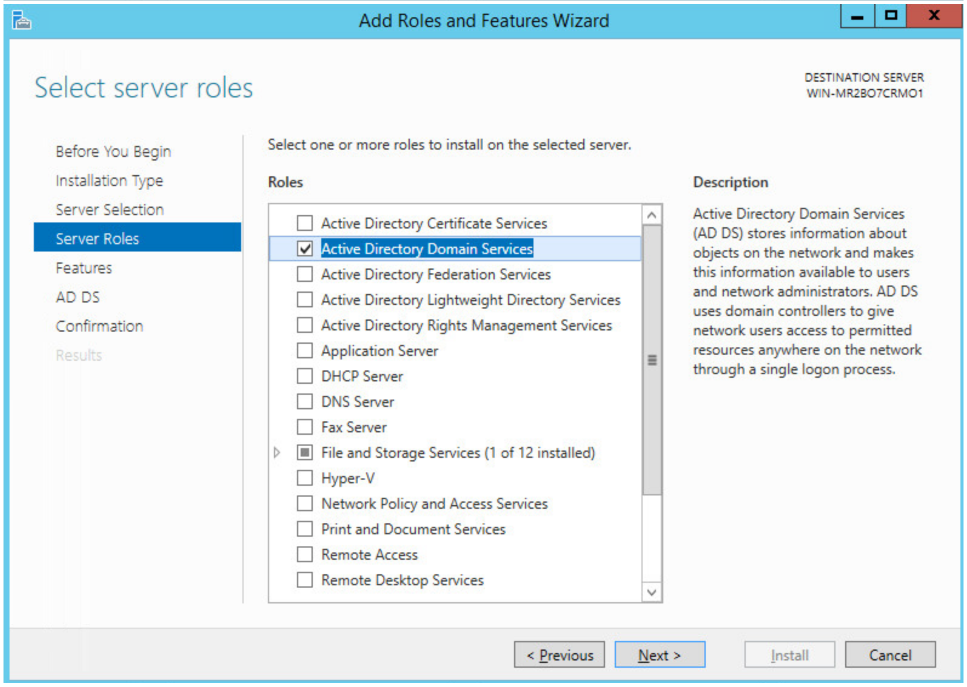
Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools

☑ Include management tools (if applicable)



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-MR2BO7CRMO1

Select one or more roles to install on the selected server.

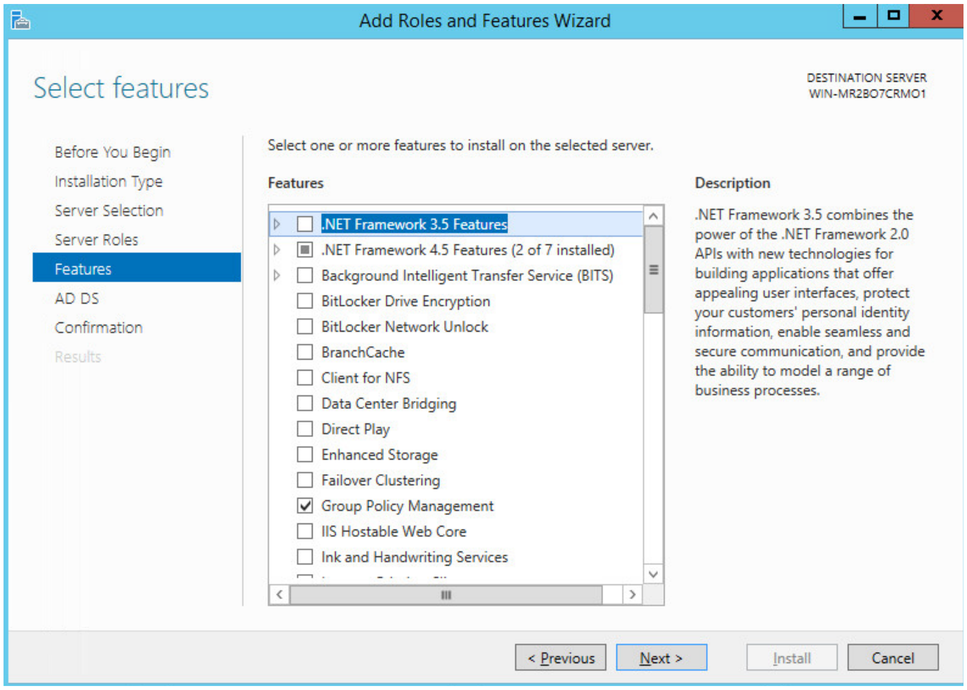
Roles

□ Active Directory Certificate Services
☑ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
□ DNS Server
□ Fax Server
▣ File and Storage Services (1 of 12 installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

9. Click **Add Features**.
10. Click **Next**.



Select one or more features to install on the selected server.

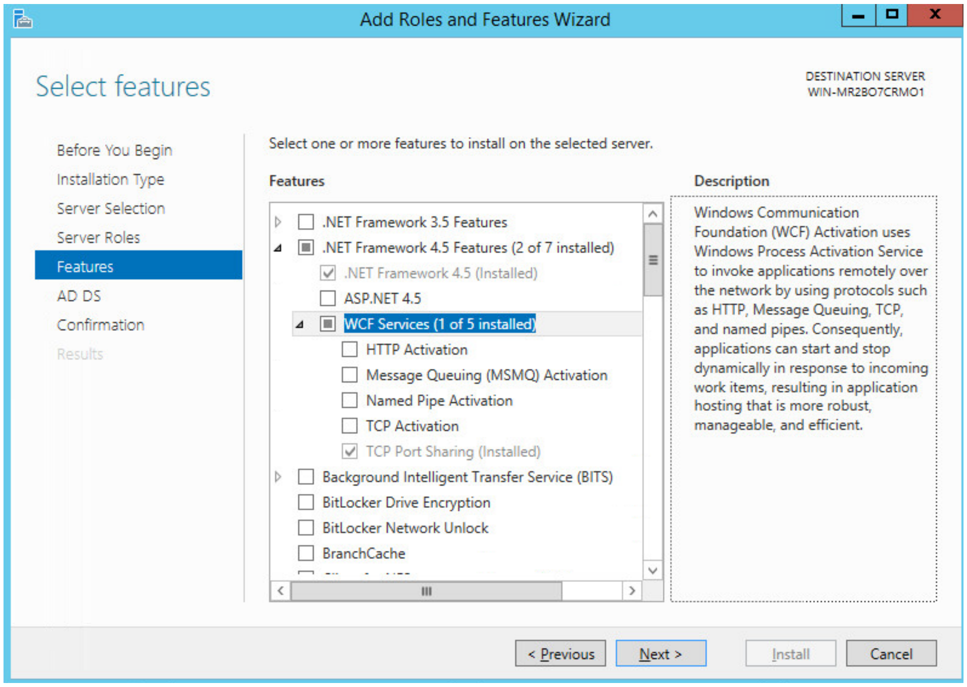
Features

- □ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

11. Ensure that **Group Policy Management**, **.NET Framework 4.5**, **TCP Port Sharing**, **Remote Server Administration Tools**, and **Windows PowerShell** are selected.



Select one or more features to install on the selected server.

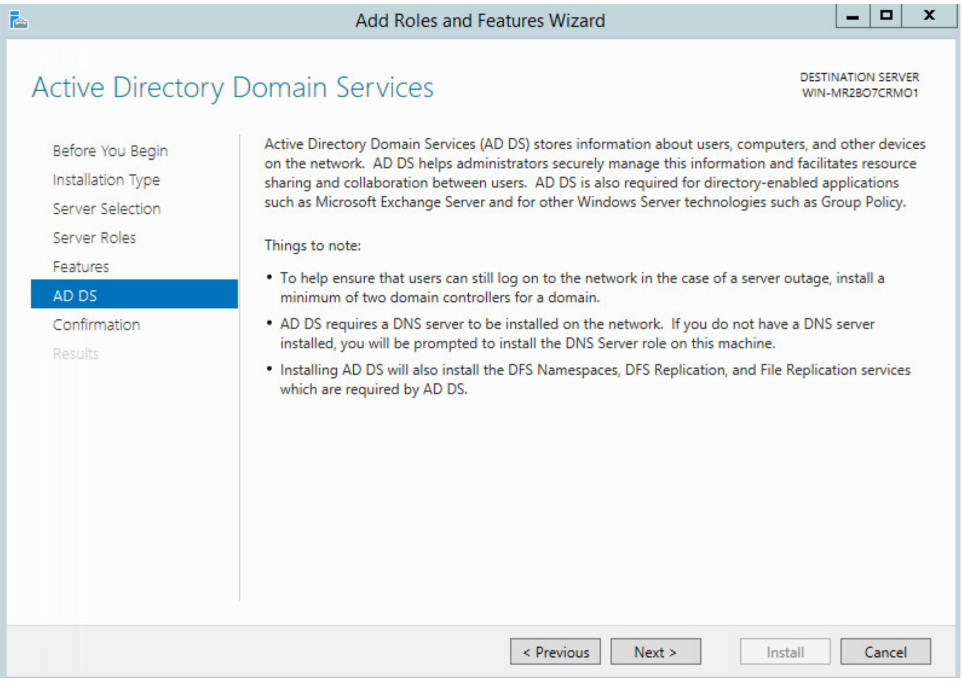
Features

- □ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
  - ☑ .NET Framework 4.5 (Installed)
  - □ ASP.NET 4.5
  - ▣ WCF Services (1 of 5 installed)
    - □ HTTP Activation
    - □ Message Queuing (MSMQ) Activation
    - □ Named Pipe Activation
    - □ TCP Activation
    - ☑ TCP Port Sharing (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache

Description

Windows Communication Foundation (WCF) Activation uses Windows Process Activation Service to invoke applications remotely over the network by using protocols such as HTTP, Message Queuing, TCP, and named pipes. Consequently, applications can start and stop dynamically in response to incoming work items, resulting in application hosting that is more robust, manageable, and efficient.

12. Select any additional features and click **Add Features** on the popup.
13. Click **Next**.



Active Directory Domain Services

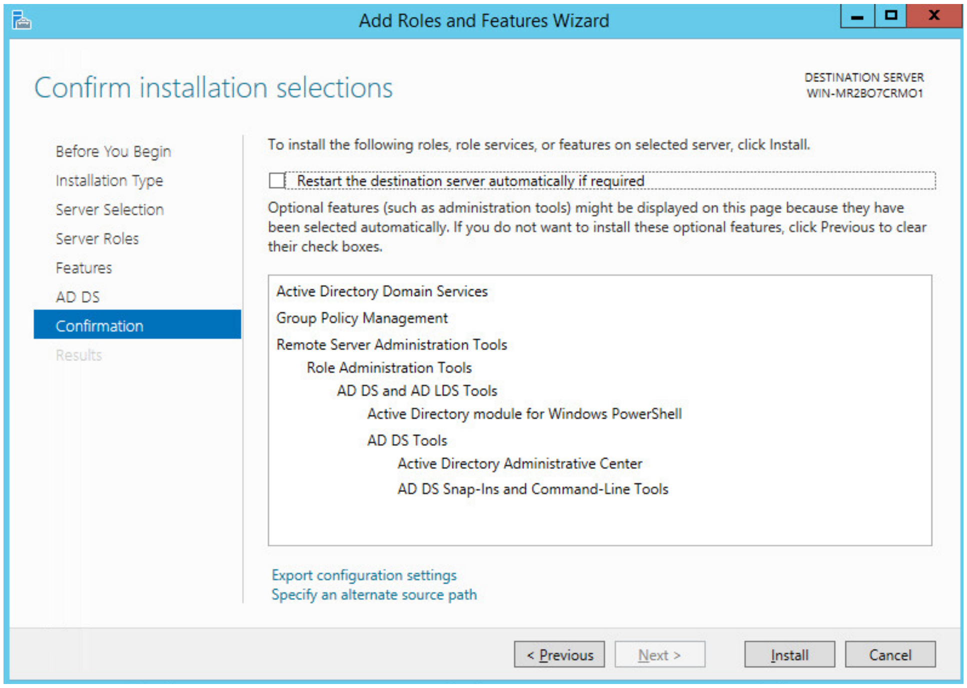
DESTINATION SERVER
WIN-MR2BO7CRMO1

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
- Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.

14. Click **Next**.



Confirm installation selections

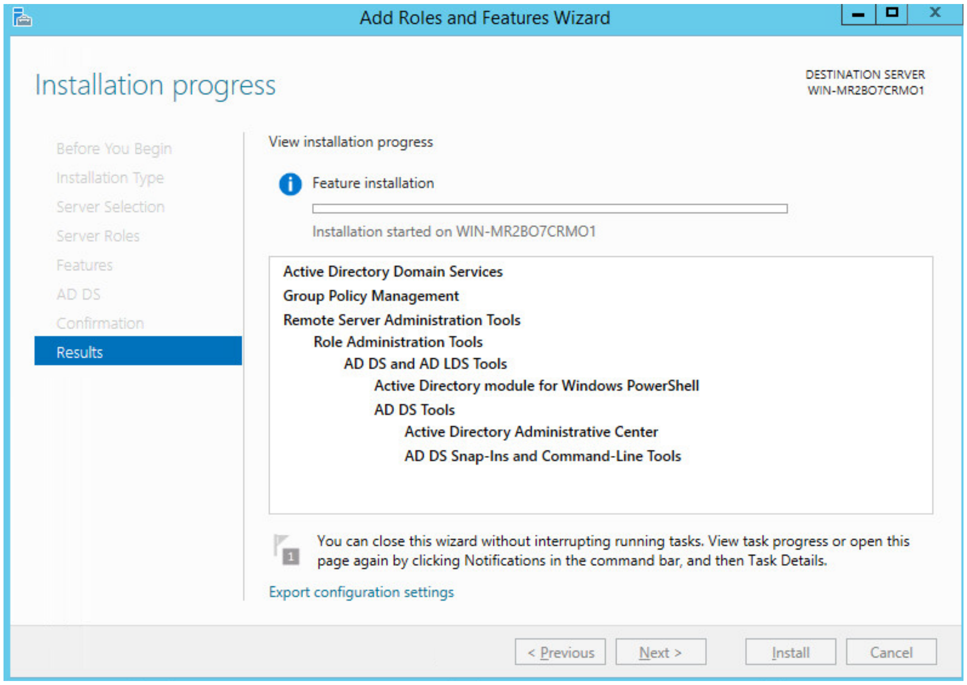
DESTINATION SERVER
WIN-MR2BO7CRMO1

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - AD DS Tools
        - Active Directory Administrative Center
        - AD DS Snap-Ins and Command-Line Tools



View installation progress

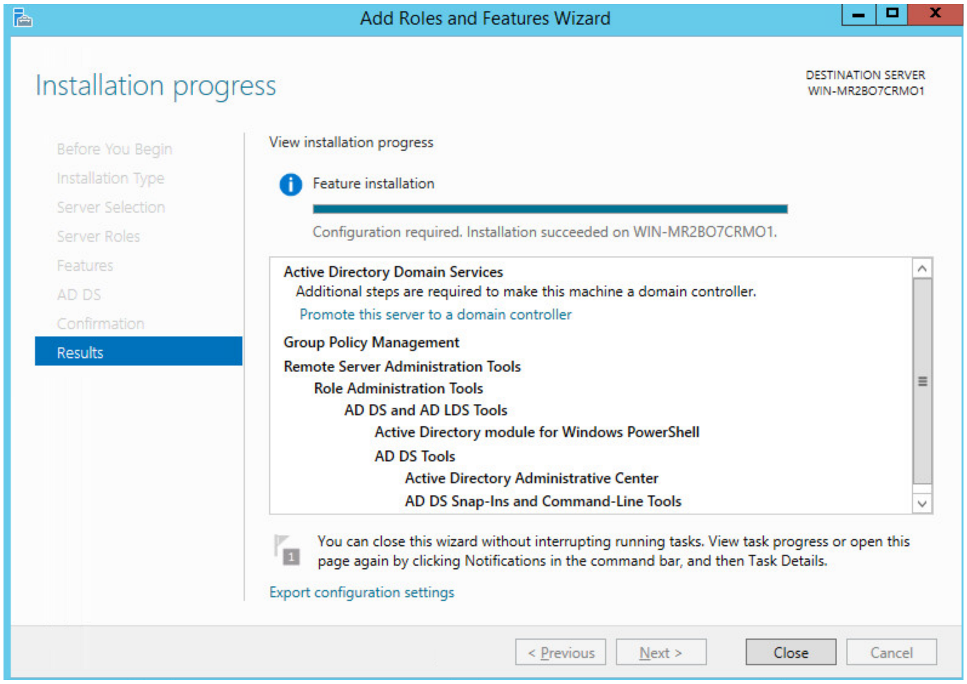
Feature installation

Installation started on WIN-MR2BO7CRMO1

Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

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



View installation progress

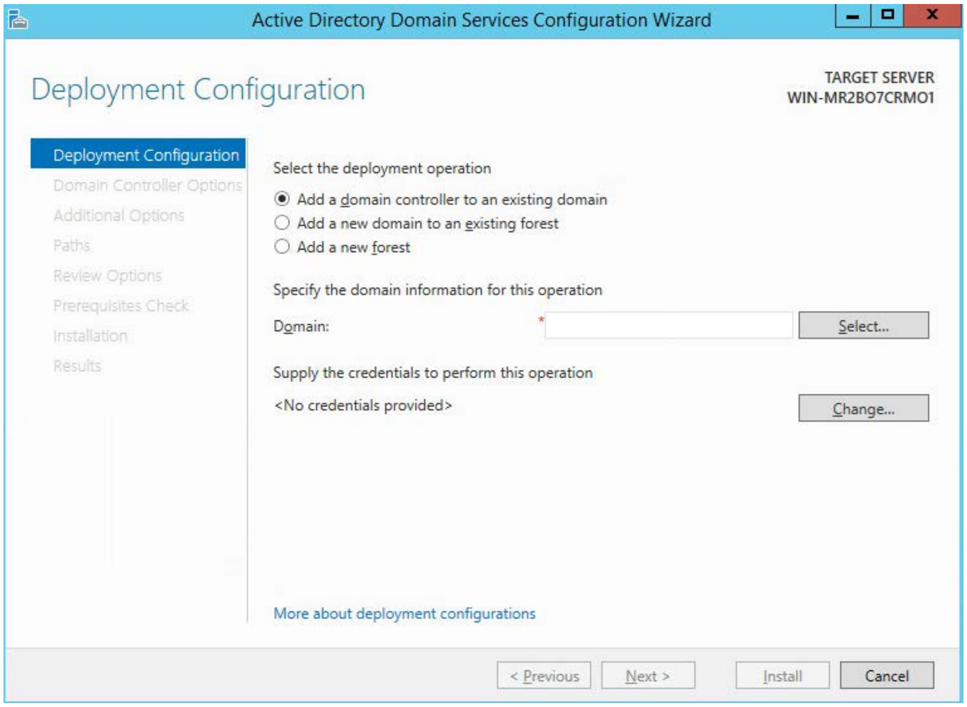
Feature installation

Configuration required. Installation succeeded on WIN-MR2BO7CRMO1.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

17. Select **Post-Deployment Configuration** or **Promote this server to a domain controller**.



Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

Domain: *

Select...

Supply the credentials to perform this operation

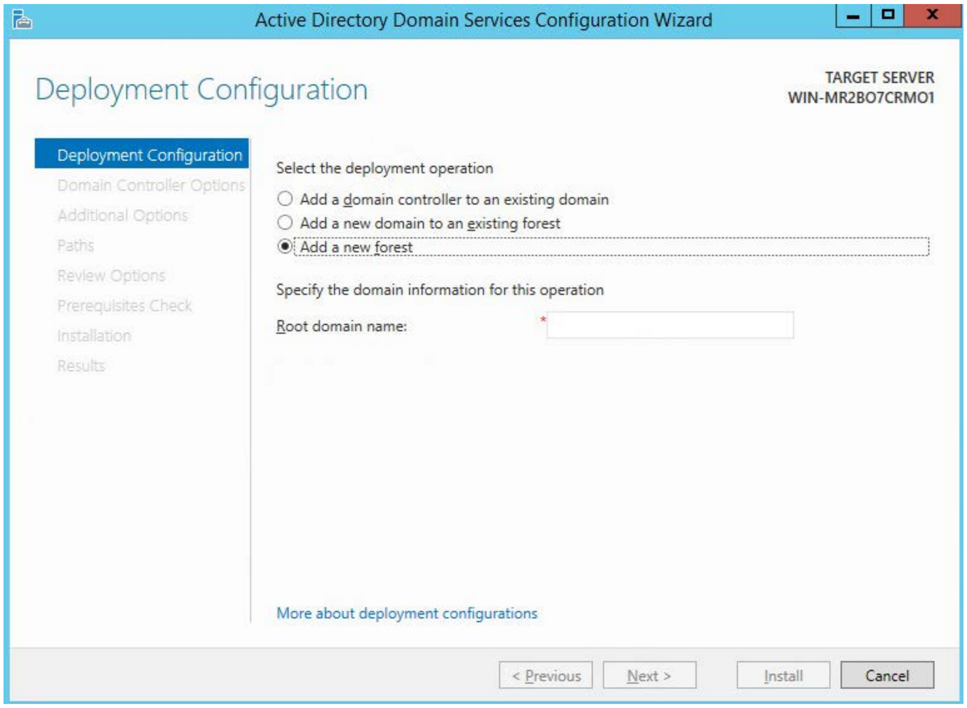
<No credentials provided>

Change...

More about deployment configurations

< Previous | Next > | Install | Cancel

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



Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

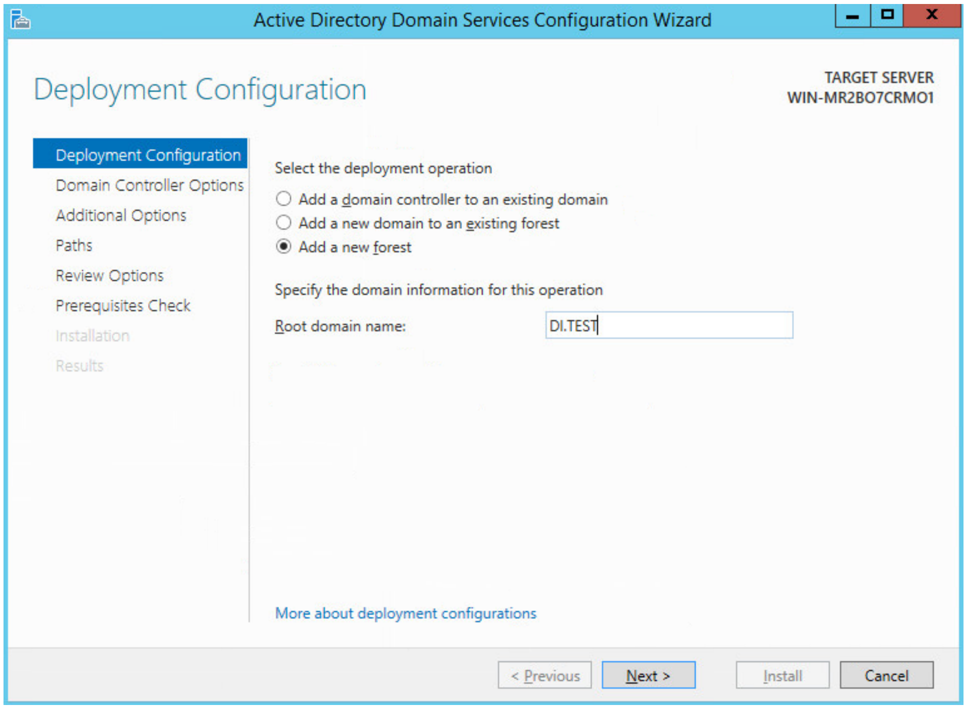
Specify the domain information for this operation

Root domain name: *

More about deployment configurations

< Previous | Next > | Install | Cancel

19. Enter a **Root domain name**. Example: DI.TEST.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-MR2BO7CRMO1

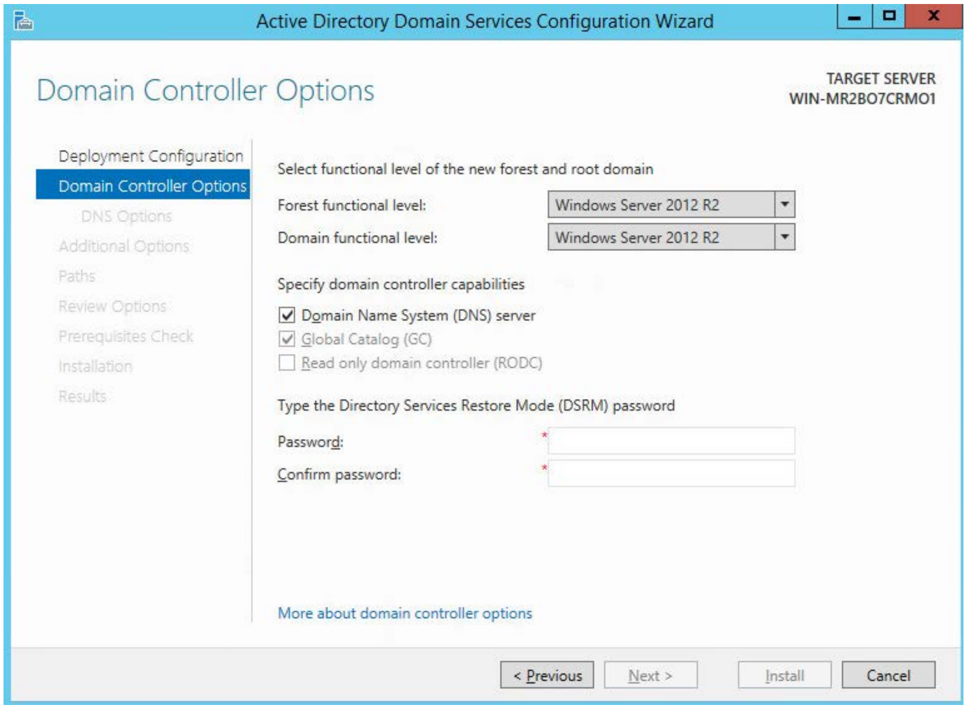
Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: DI.TEST

20. Click **Next.**



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-MR2BO7CRMO1

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

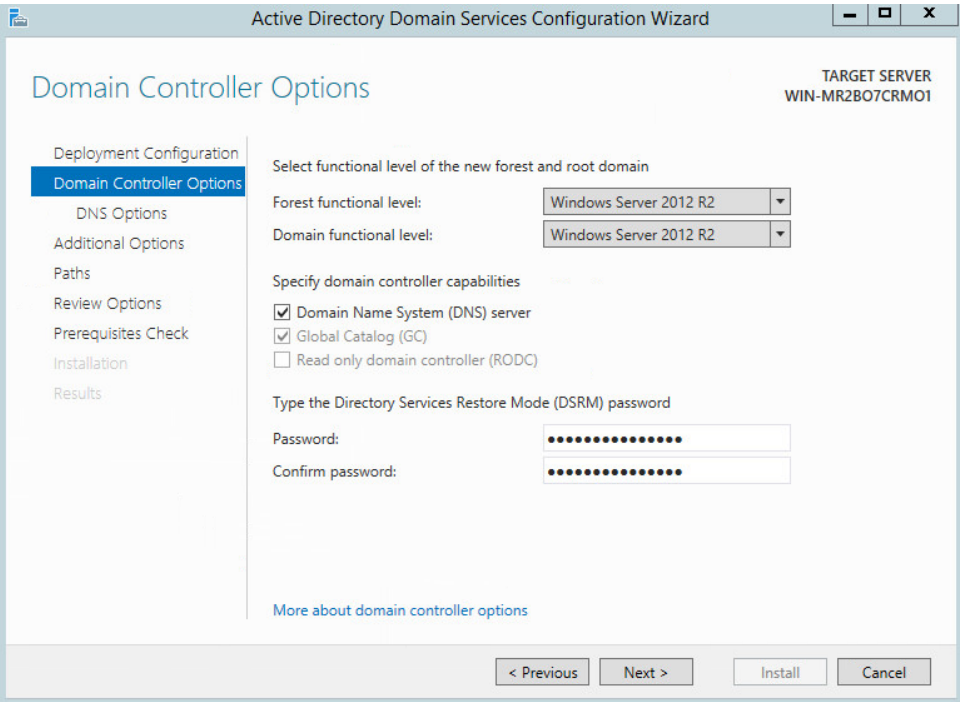
Type the Directory Services Restore Mode (DSRM) password

Password: *

Confirm password: *

21. Select **Windows Server 2012 R2** for the **Forest Functional Level**.

22. Select **Windows Server 2012 R2** for the **Domain Functional Level**.
23. Check the box next to **DNS server** and **Global Catalog**.
24. Do not check the box next to **read-only domain controller**.
25. Specify a password for **DSRM**.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-MR2BO7CRMO1

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

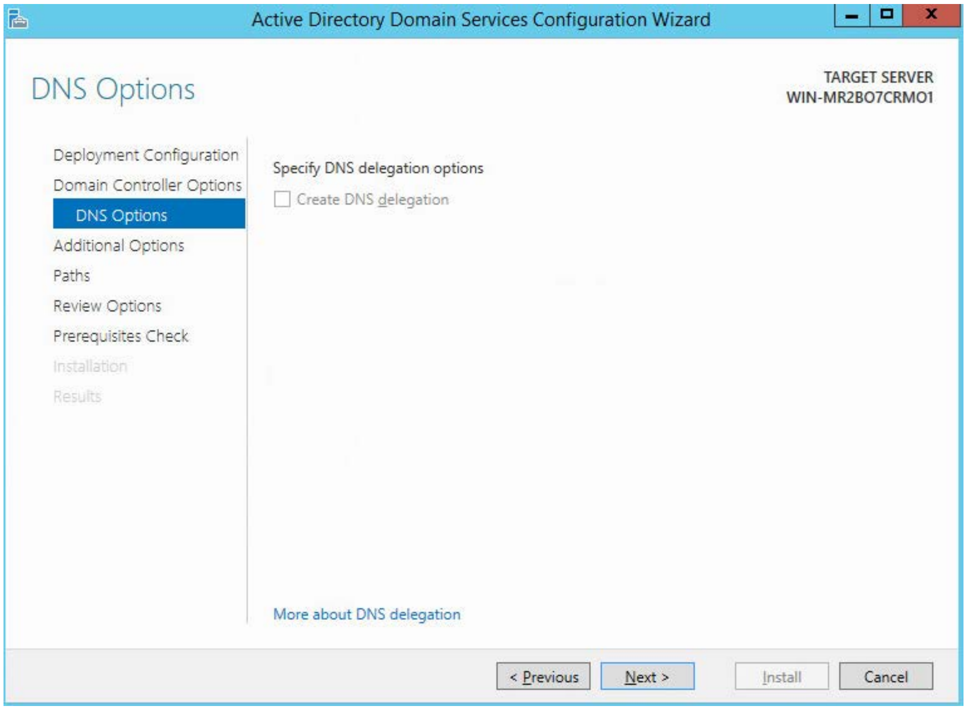
Type the Directory Services Restore Mode (DSRM) password

Password: •••••••••••••••

Confirm password: •••••••••••••••

More about domain controller options

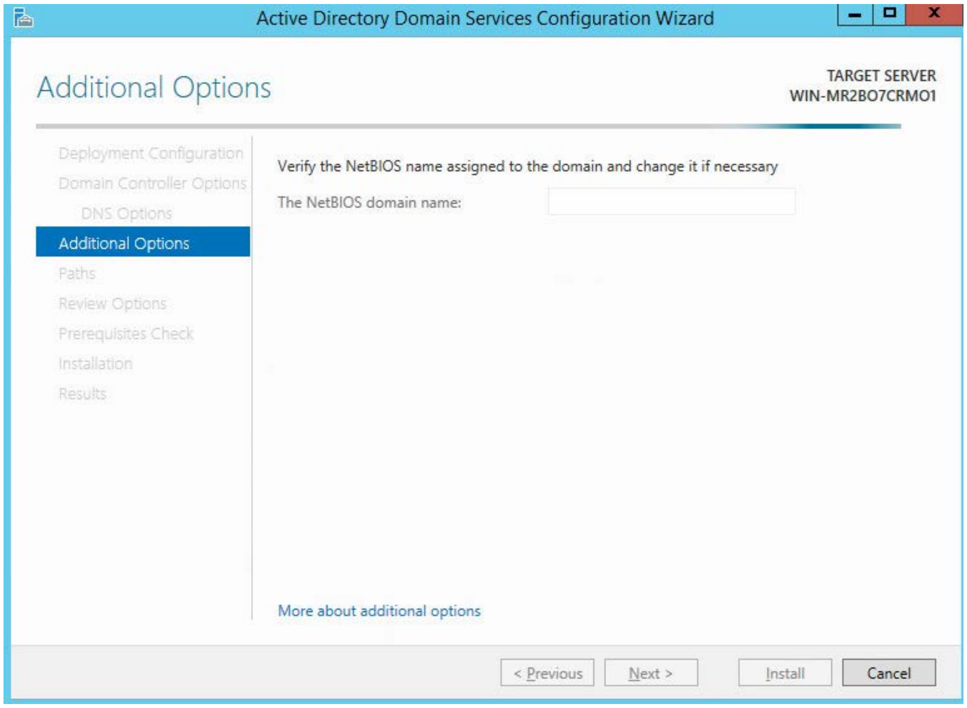
26. Click **Next**.



Specify DNS delegation options

□ Create DNS delegation

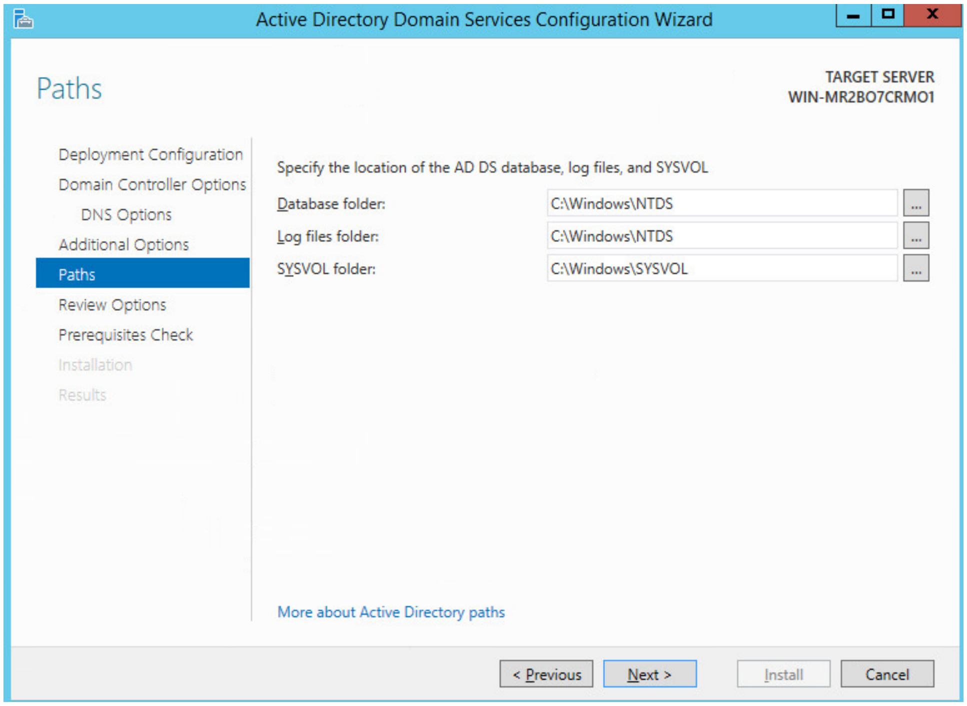
27. Click **Next**.



Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

28. Verify the NetBIOS name.
29. Click **Next**.



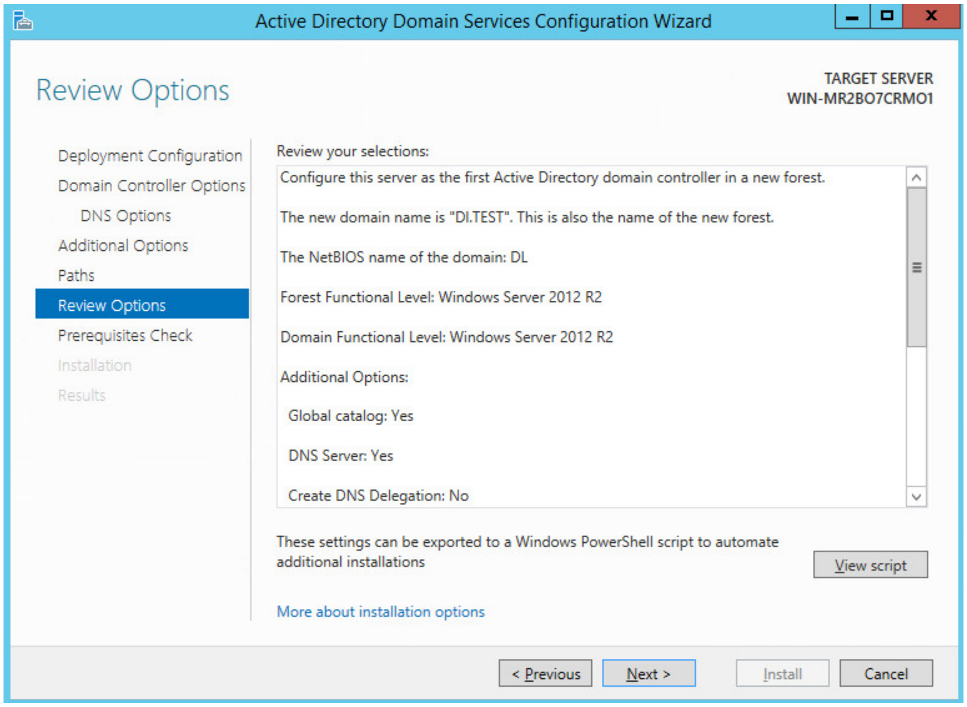
Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

30. Click **Next**.



Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "DI.TEST". This is also the name of the new forest.

The NetBIOS name of the domain: DL

Forest Functional Level: Windows Server 2012 R2

Domain Functional Level: Windows Server 2012 R2

Additional Options:

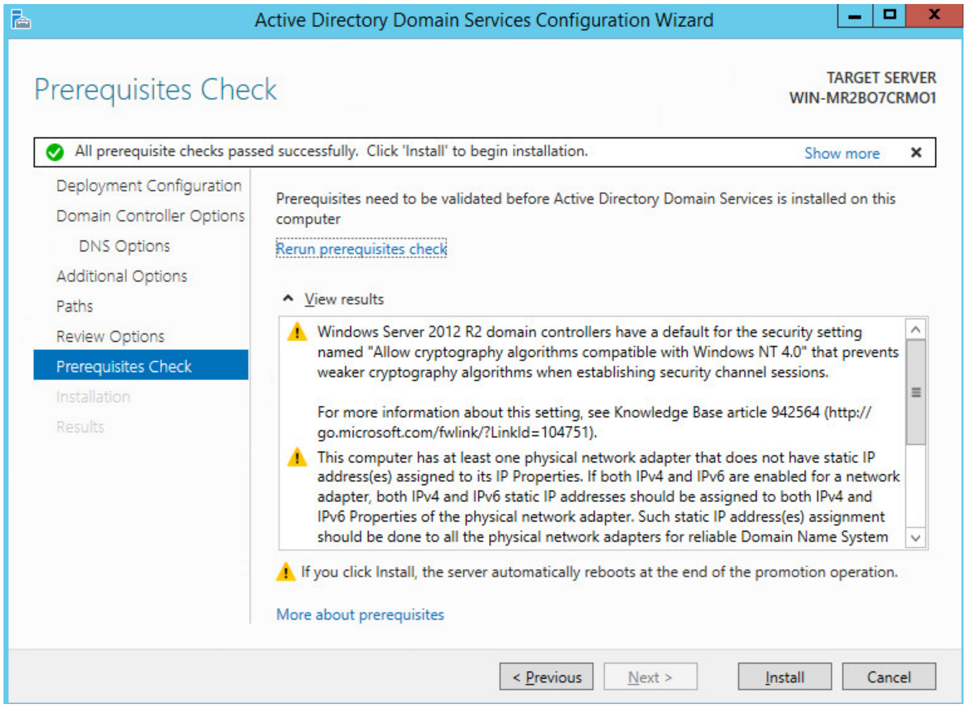
Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

31. Click **Next**.



All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

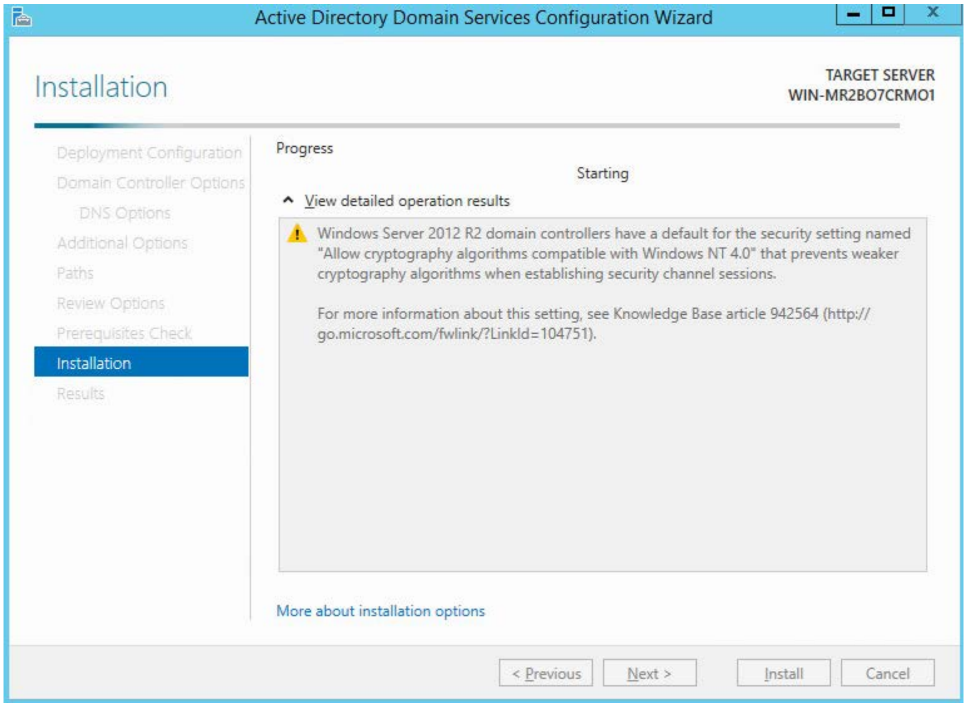
Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System

If you click Install, the server automatically reboots at the end of the promotion operation.

32. Click **Install**.



Starting

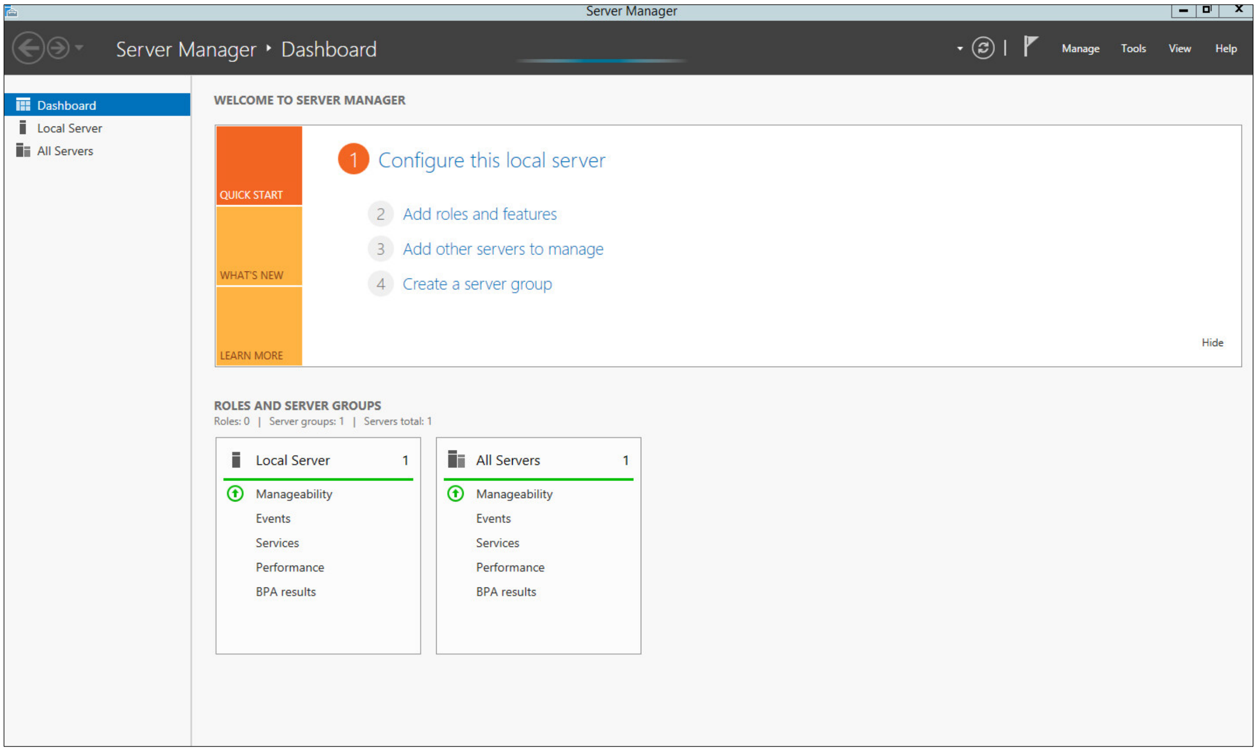
Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

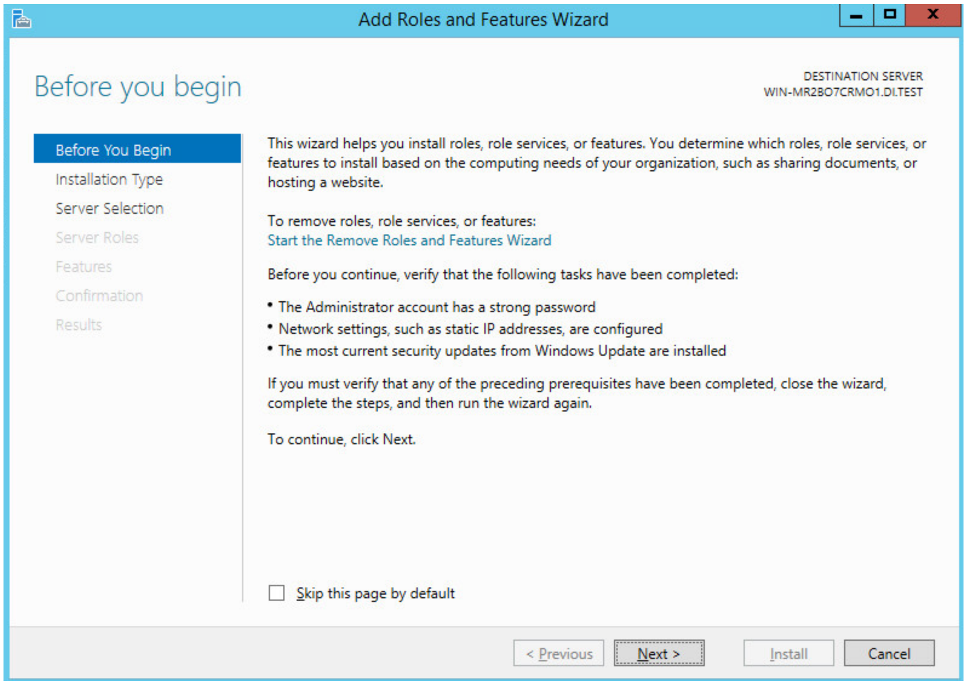
33. The server automatically reboots.

2.1.2 Creating a Certificate Authority

1. Open **Server Manager**.



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



Before you begin

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

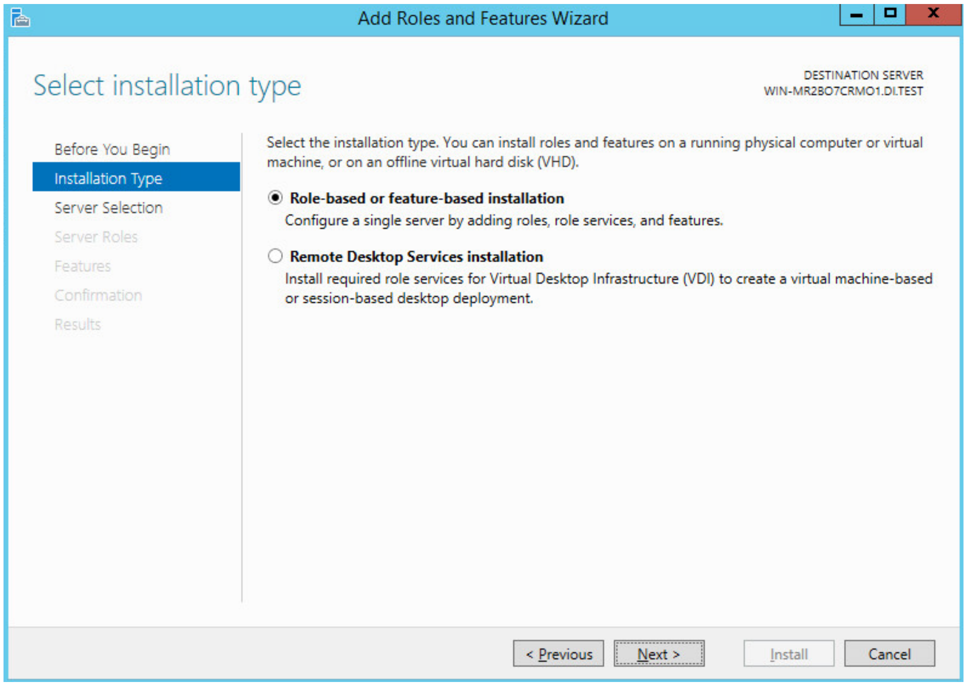
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

3. Click **Next**.



Select installation type

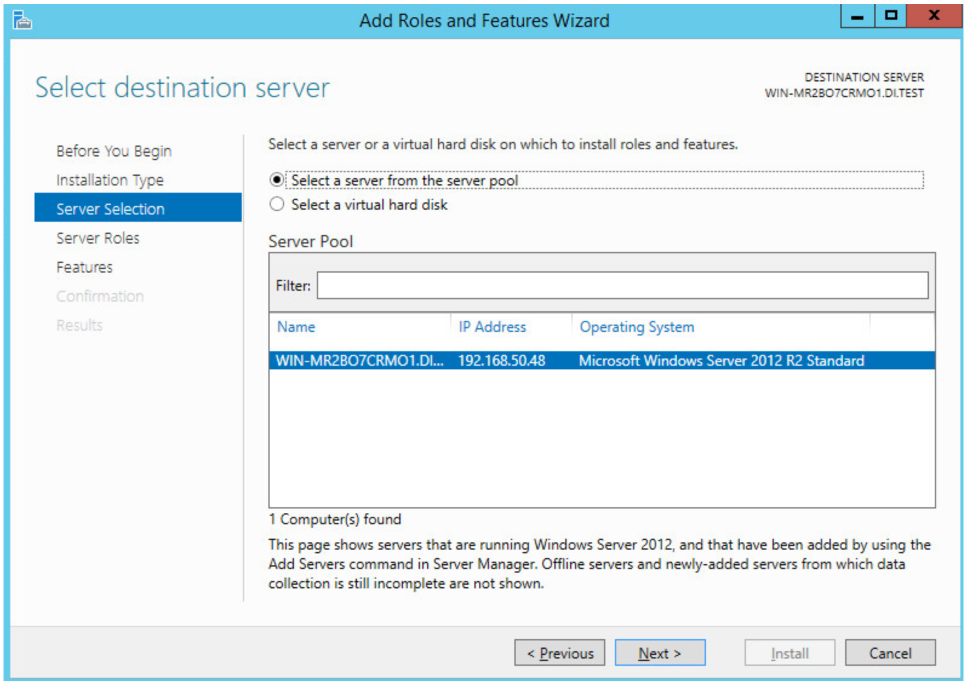
DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Select destination server

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

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

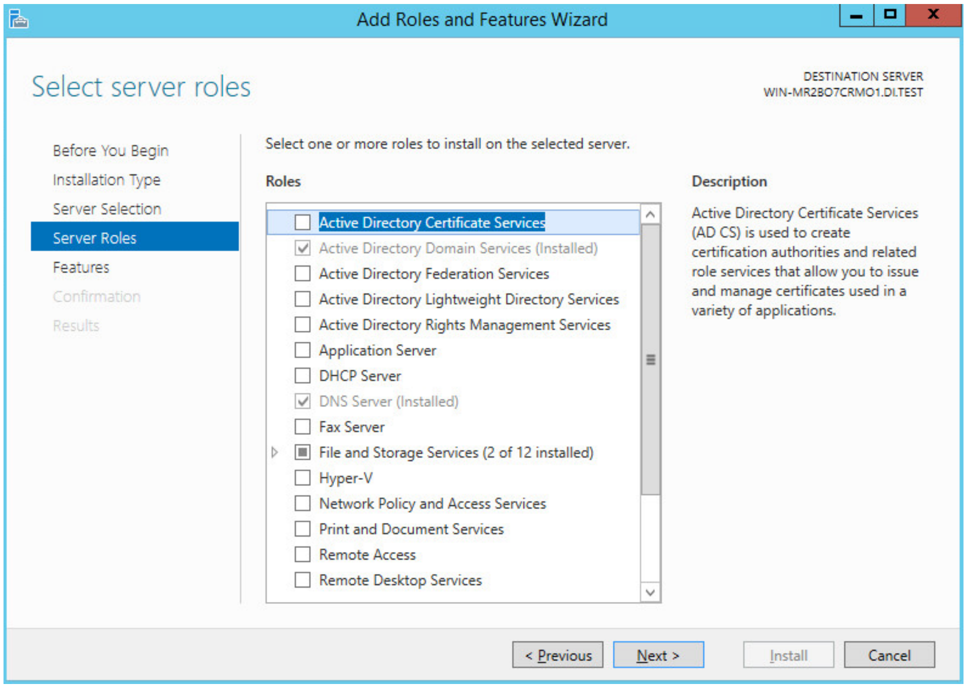
Filter:

Name	IP Address	Operating System
WIN-MR2BO7CRMO1.DI...	192.168.50.48	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.

6. Select **ADDNS** (or the correct Windows Server name) from the list.
7. Click **Next**.



Select server roles

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Select one or more roles to install on the selected server.

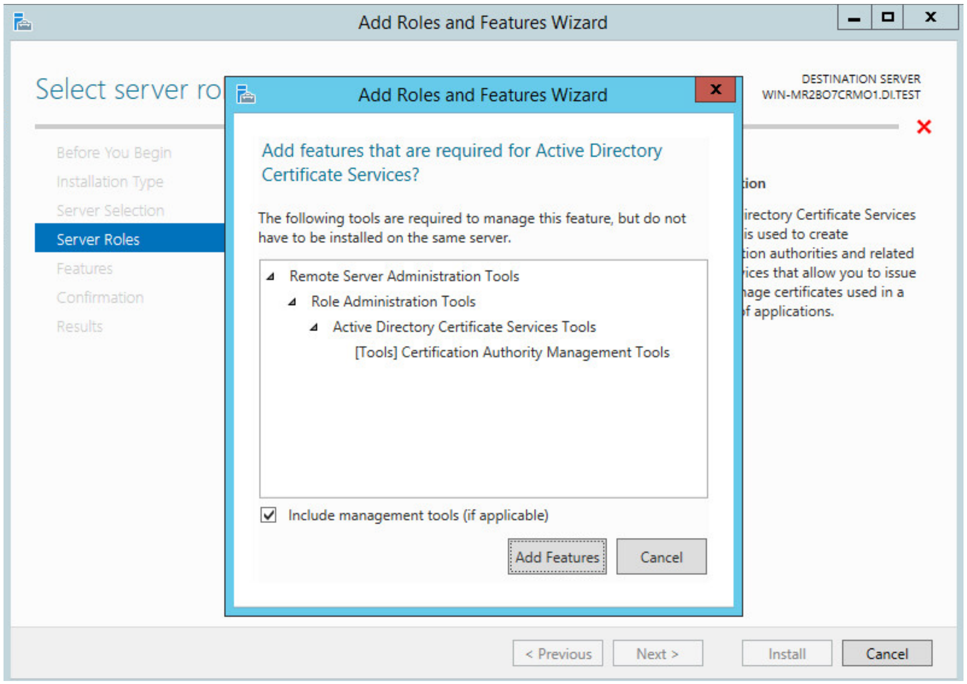
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ▣ File and Storage Services (2 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

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



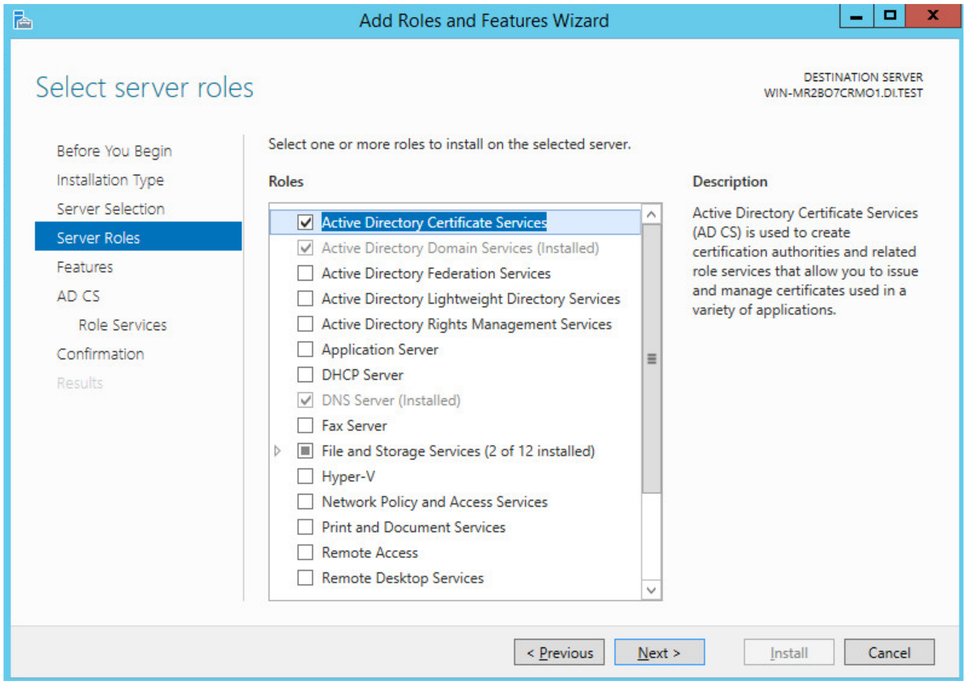
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

9. Click **Add Features**.



Select server roles

Select one or more roles to install on the selected server.

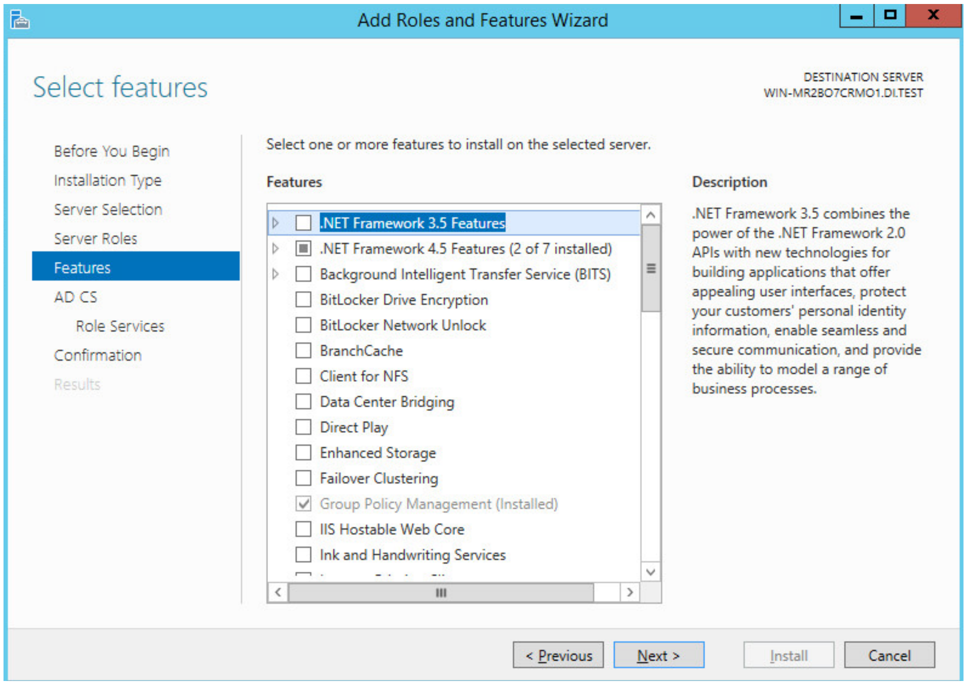
Roles

☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Application Server
☐ DHCP Server
☑ DNS Server (Installed)
☐ Fax Server
▣ File and Storage Services (2 of 12 installed)
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

10. Click **Next**.


Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Select one or more features to install on the selected server.

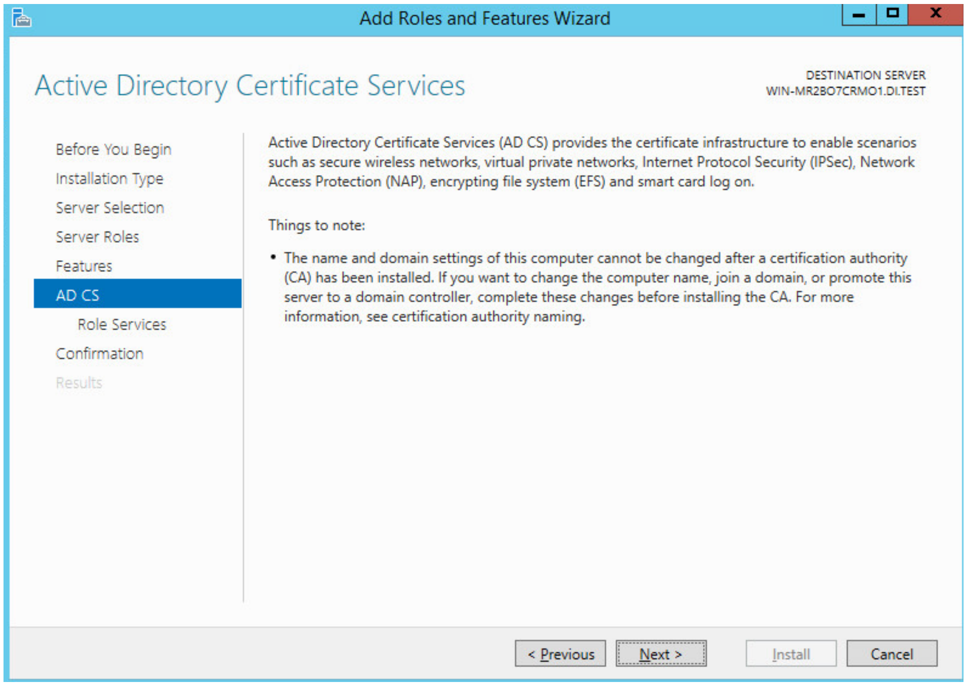
Features

- □ .NET Framework 3.5 Features
- ▪ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

11. Click **Next**.


Add Roles and Features Wizard

Active Directory Certificate Services

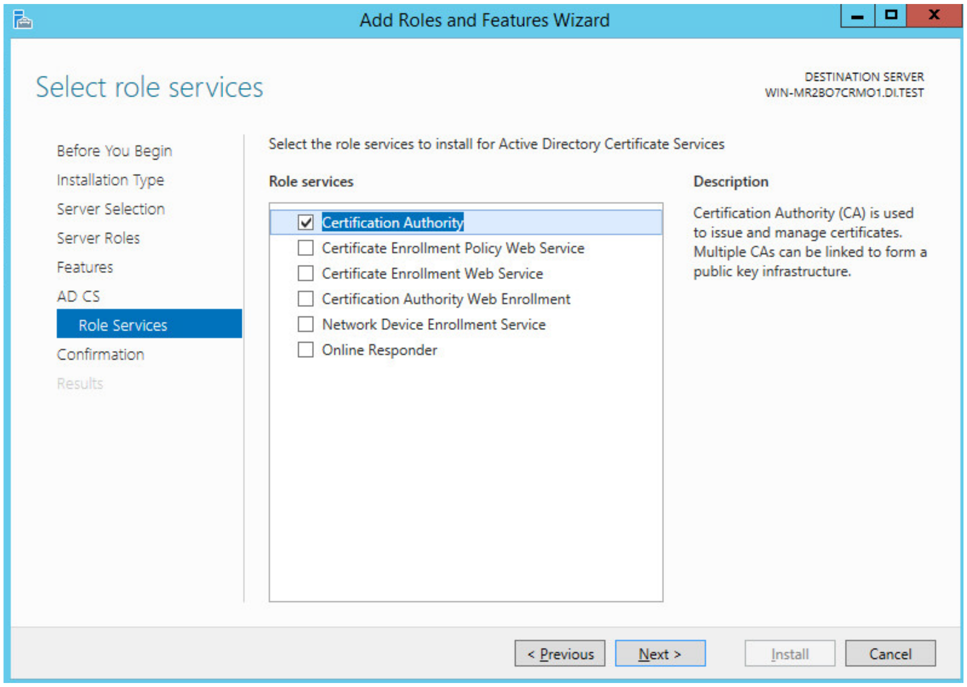
DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

12. Click **Next**.



Select the role services to install for Active Directory Certificate Services

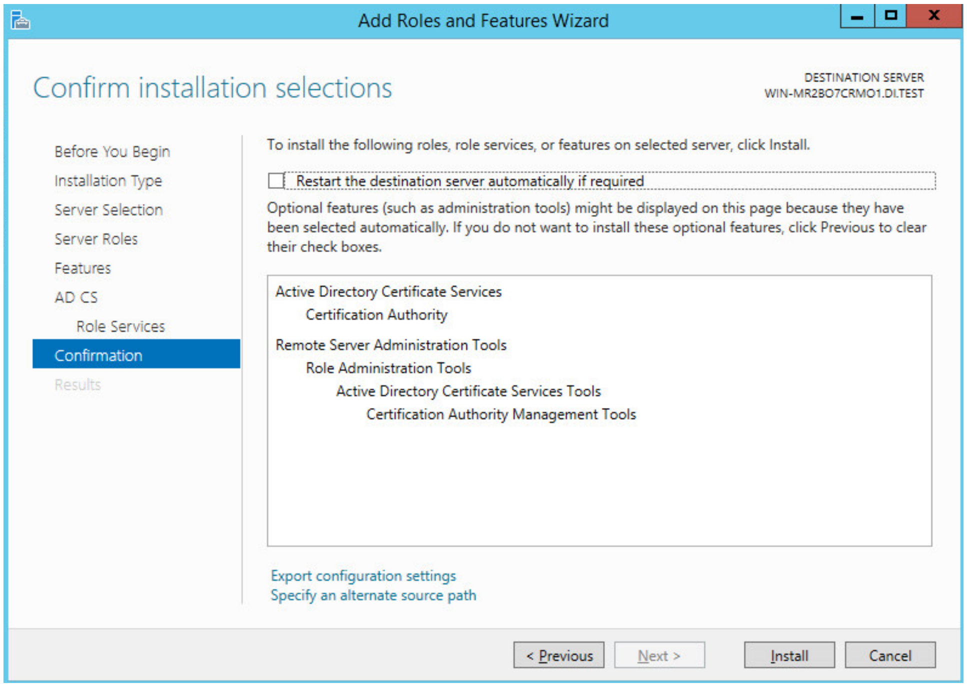
Role services

- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

13. Select **Certification Authority** on the **Role Services** list.
14. Click **Next**.

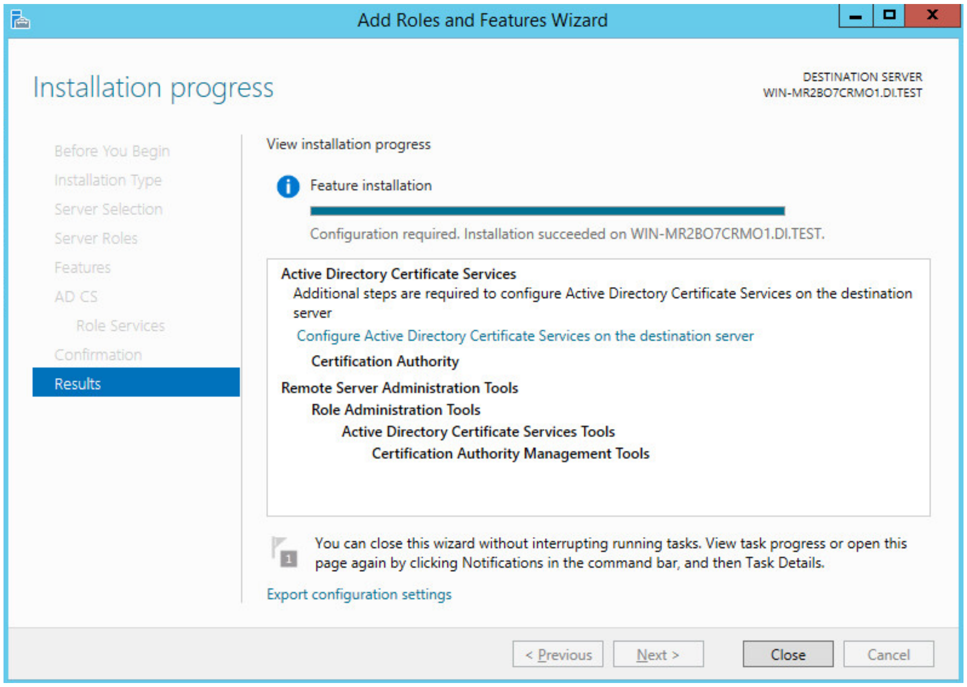


To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
    Certification Authority
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools



View installation progress

Feature installation

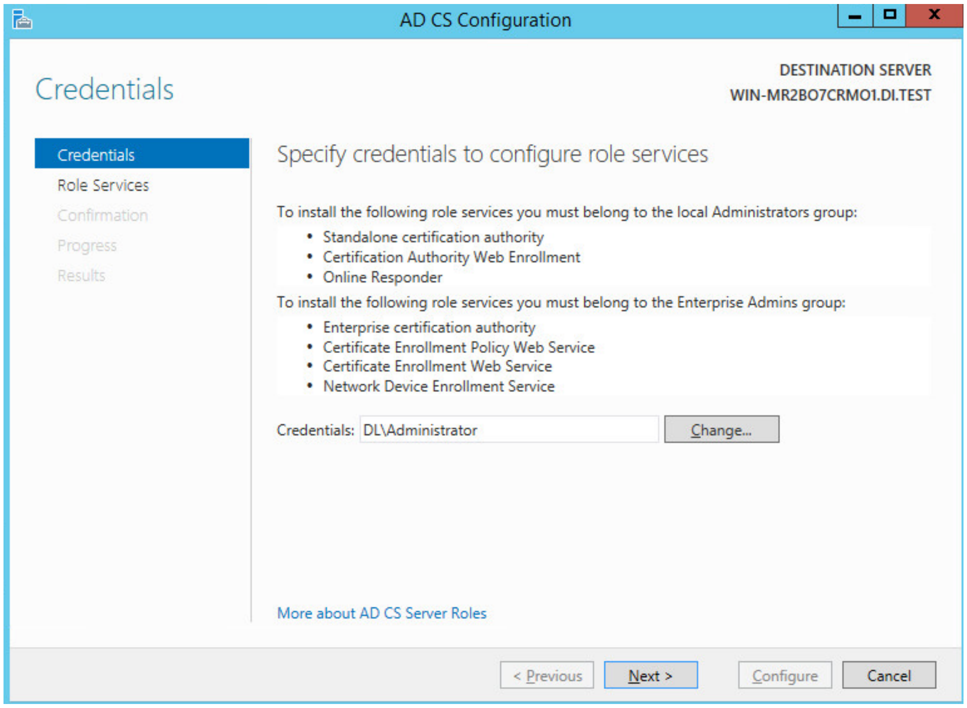
Configuration required. Installation succeeded on WIN-MR2BO7CRMO1.DI.TEST.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

15. Click **Install**.
16. Select **Configure Active Directory Certificate Services on the destination server**.



Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

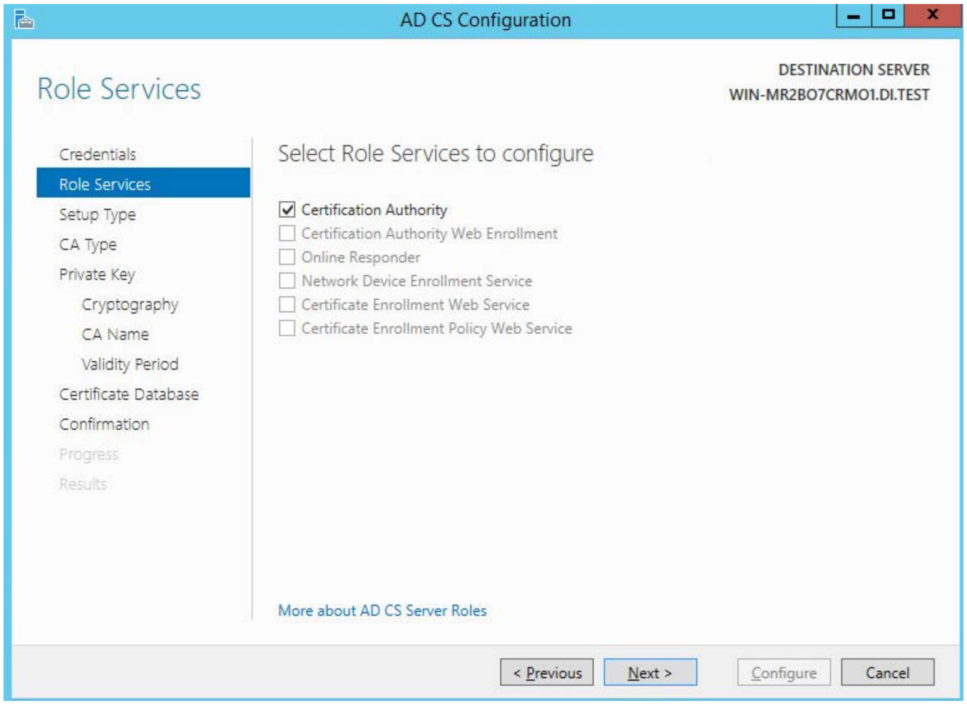
To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: DL\Administrator

17. Click **Next**.

18. Select **Certification Authority**.



Role Services

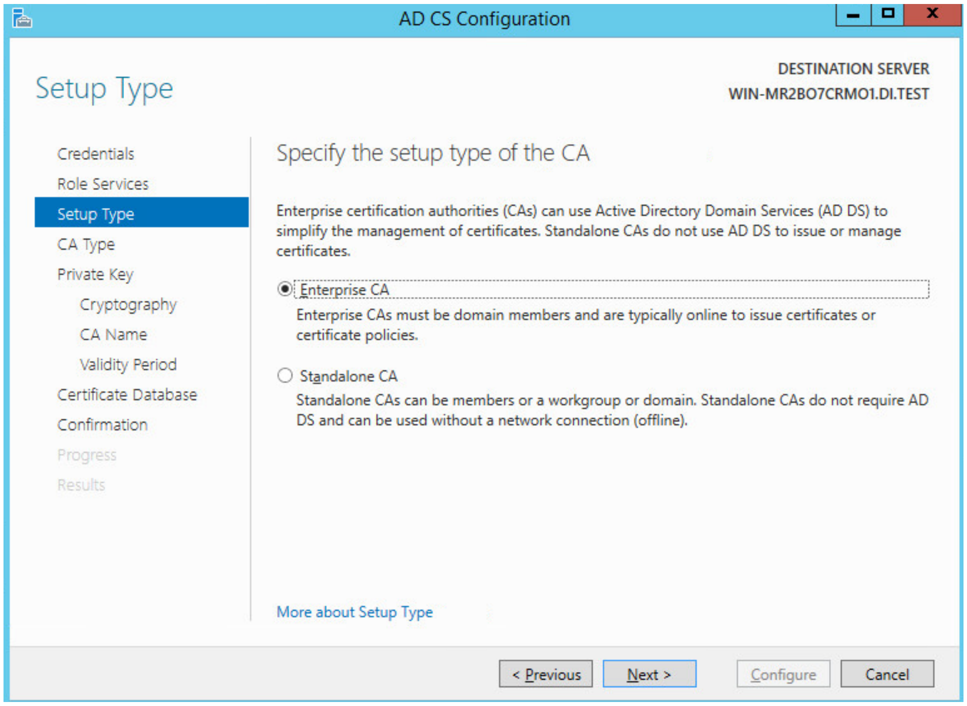
DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Select Role Services to configure

- ☑ Certification Authority
- □ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service
- □ Certificate Enrollment Web Service
- □ Certificate Enrollment Policy Web Service

More about AD CS Server Roles

19. Click **Next**.



Setup Type

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

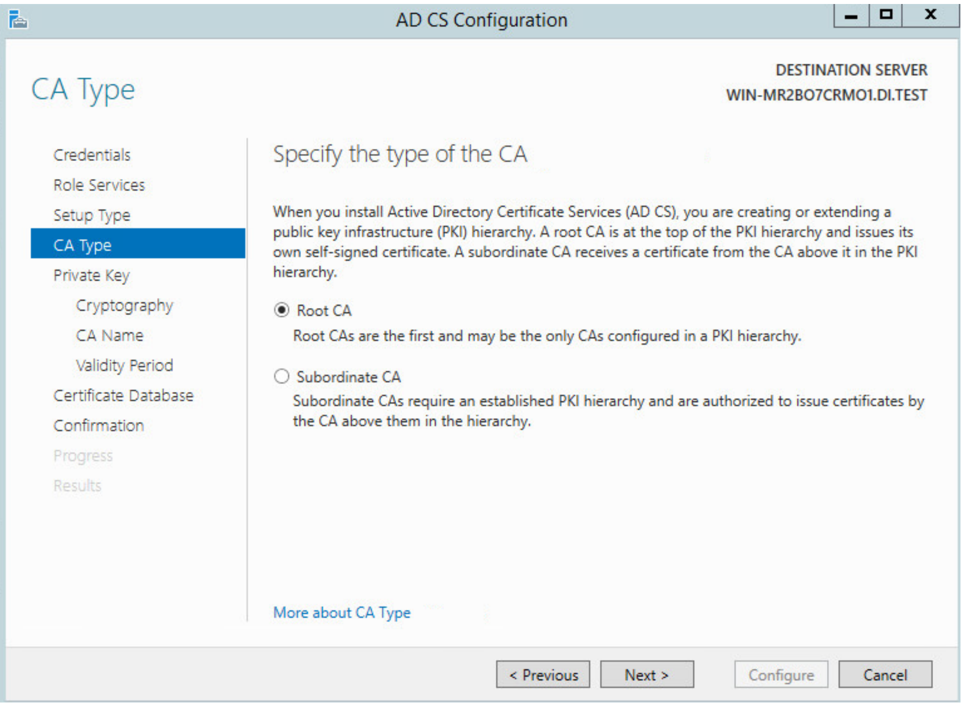
● Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

20. Select **Enterprise CA**.

21. Click **Next**.



AD CS Configuration

CA Type

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

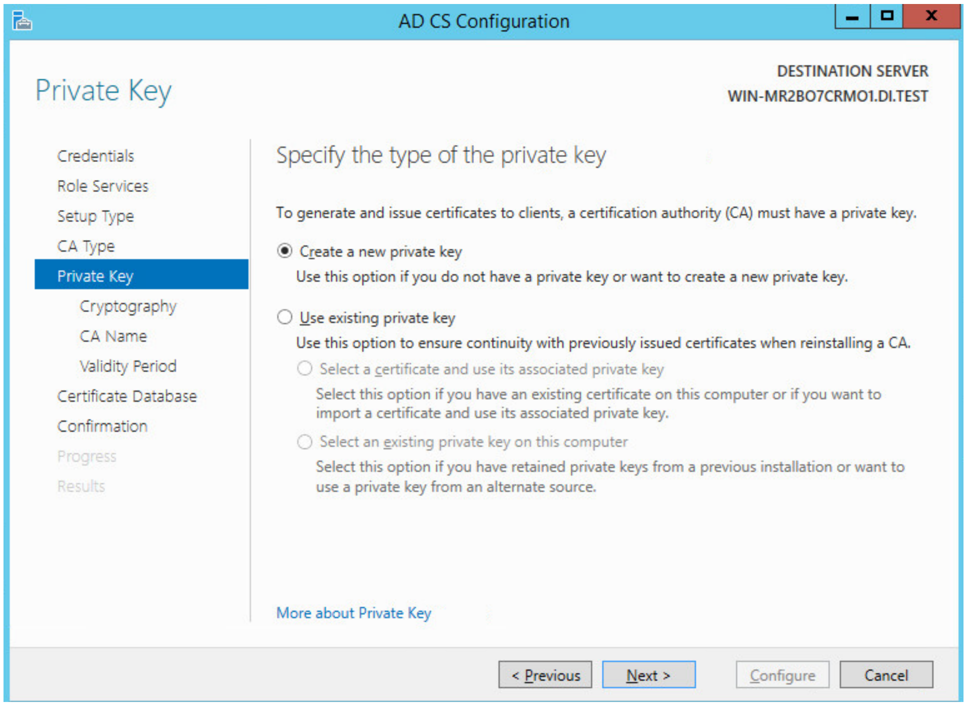
● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

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

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



Private Key

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key

Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key

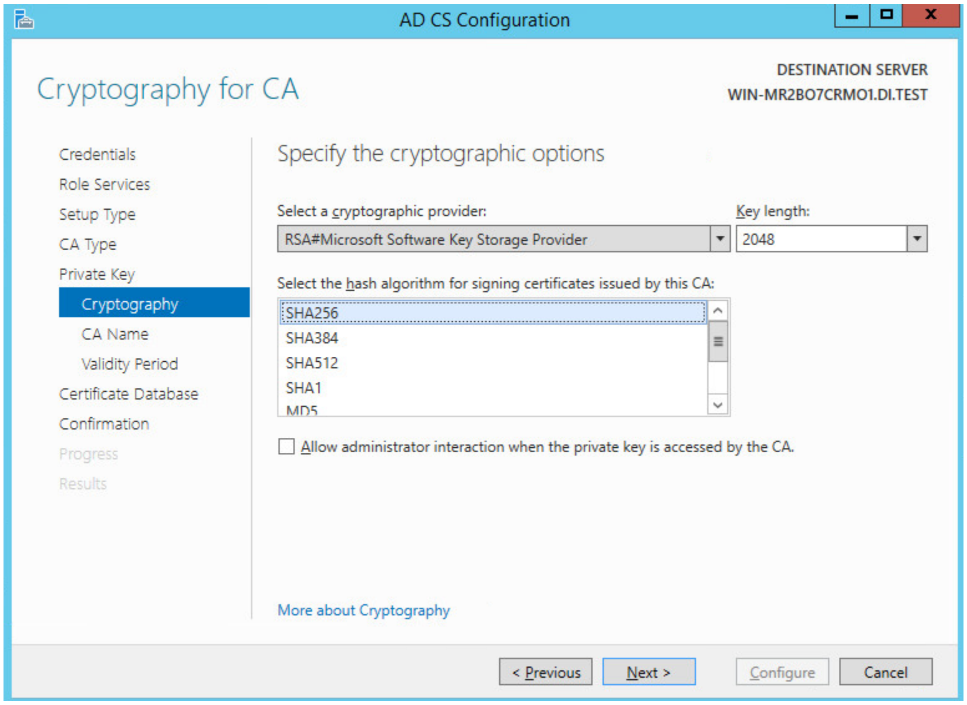
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

25. Click **Next**.
26. Select **RSA#Microsoft Software Key Storage Provider**.
27. Enter **2048** in the box.

28. Select **SHA256** from the list.



Cryptography for CA

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

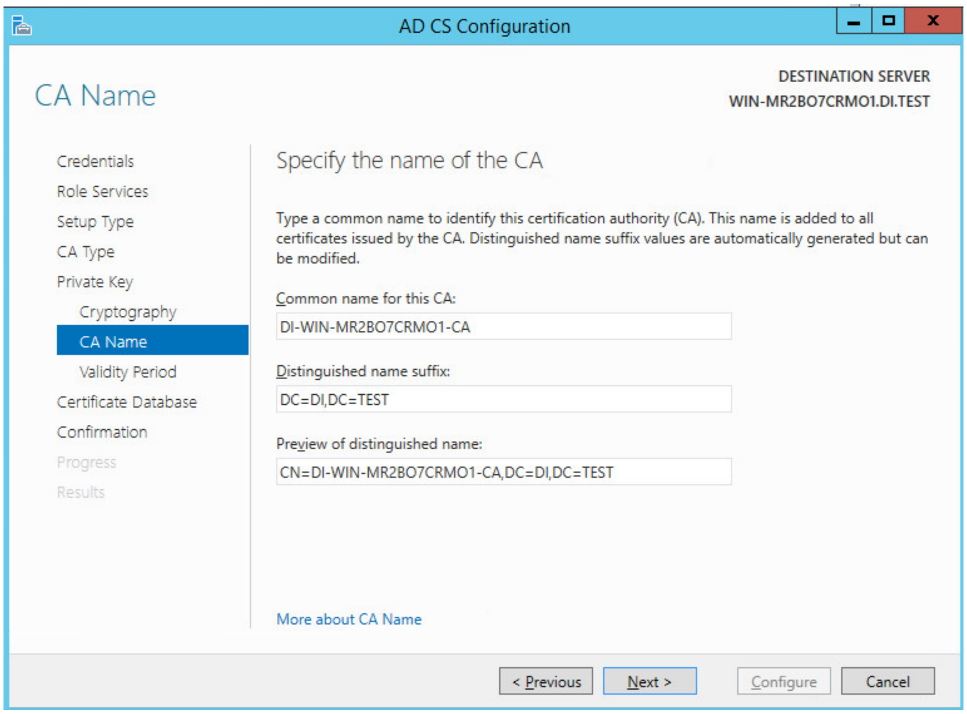
Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

29. Click **Next**.



CA Name

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

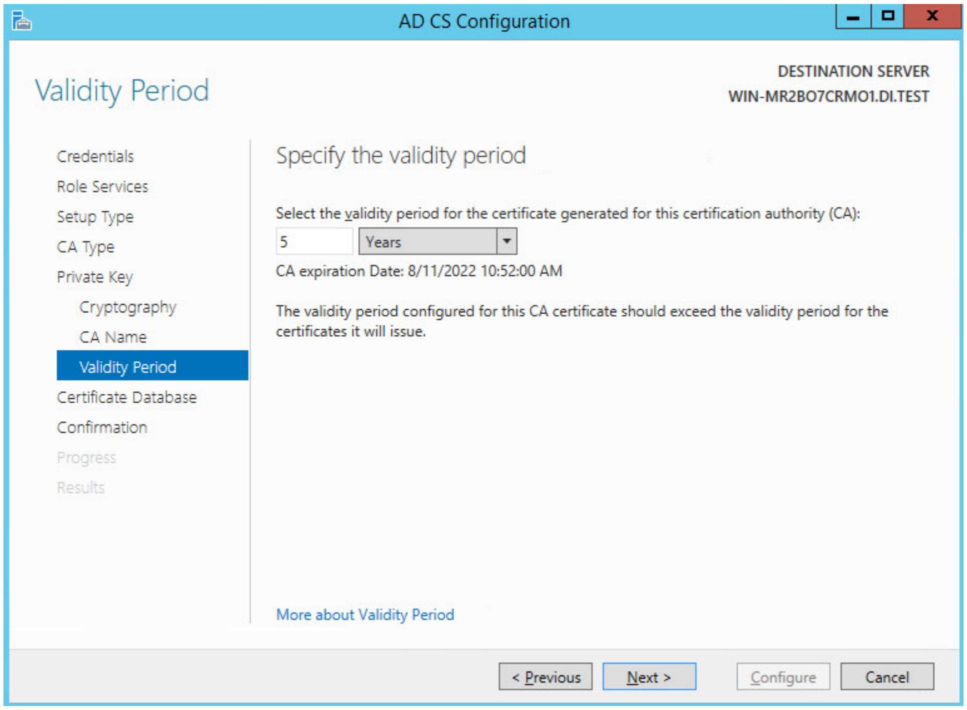
Common name for this CA: DI-WIN-MR2BO7CRMO1-CA

Distinguished name suffix: DC=DI,DC=TEST

Preview of distinguished name: CN=DI-WIN-MR2BO7CRMO1-CA,DC=DI,DC=TEST

30. Click **Next**.

31. Specify a validity period specific to your organization's needs.



AD CS Configuration

Validity Period

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the validity period

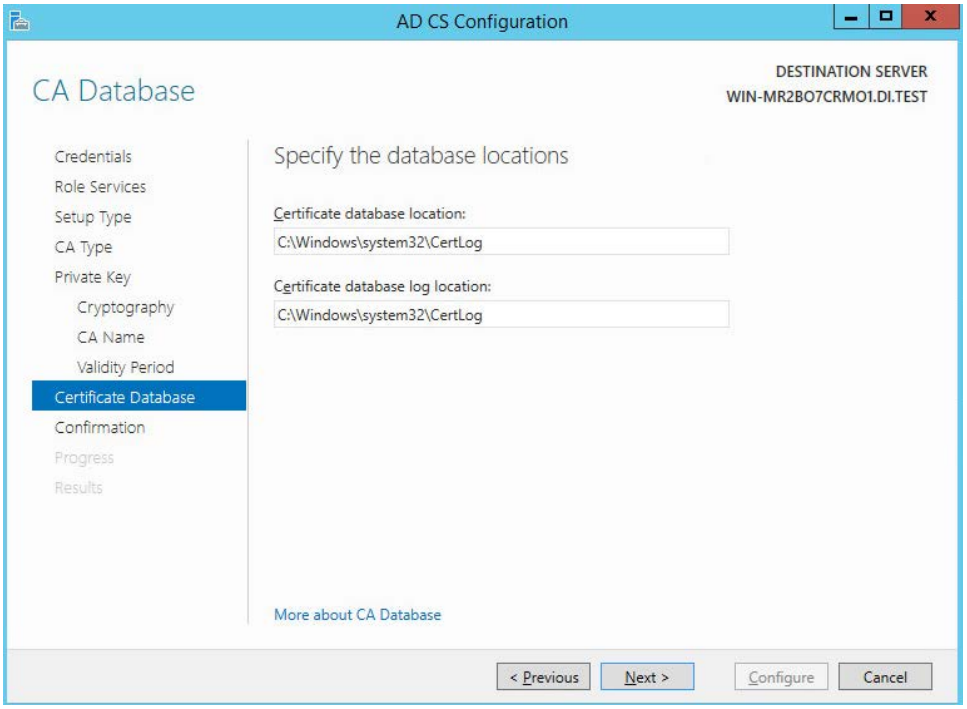
Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 8/11/2022 10:52:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

32. Click **Next**.



AD CS Configuration

CA Database

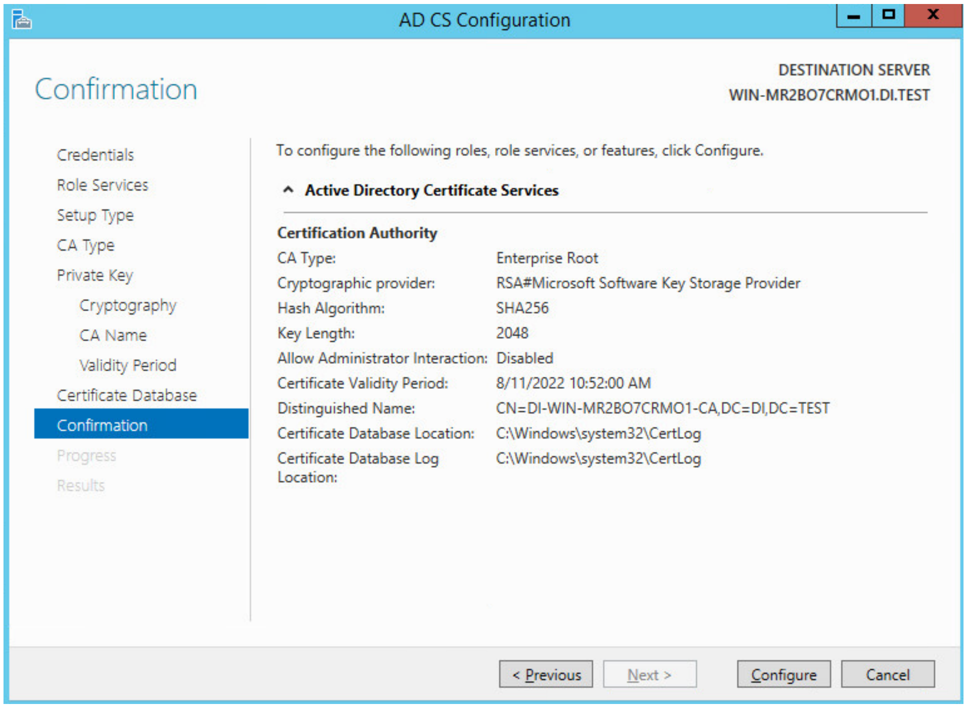
DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Specify the database locations

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

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

33. Click **Next**.



Confirmation

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

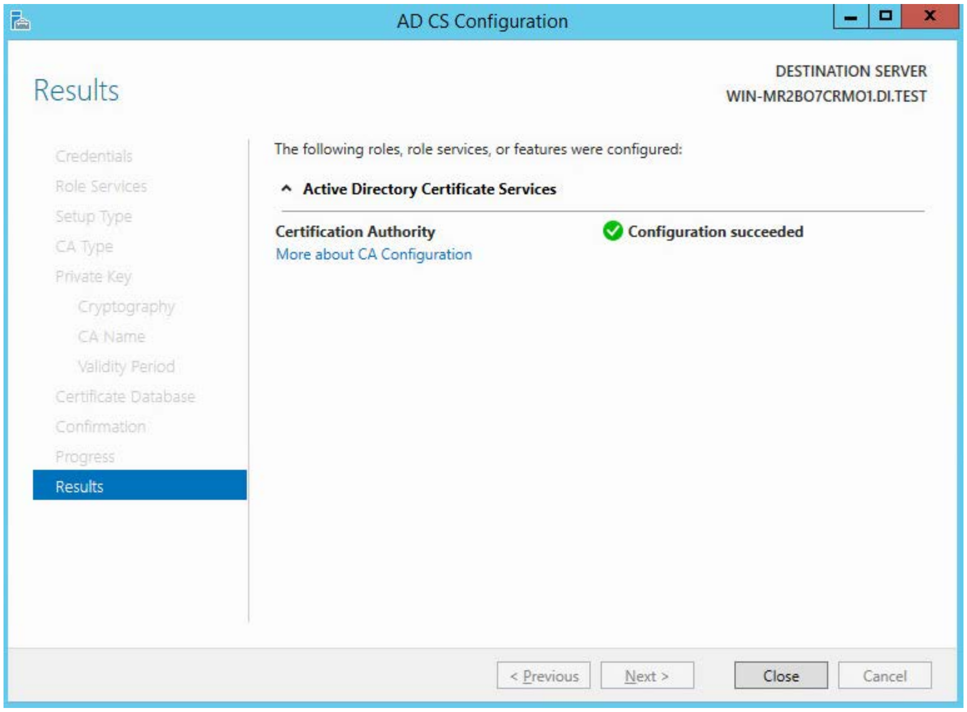
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	8/11/2022 10:52:00 AM
Distinguished Name:	CN=DI-WIN-MR2BO7CRMO1-CA,DC=DI,DC=TEST
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

34. Click **Configure**.



Results

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

The following roles, role services, or features were configured:

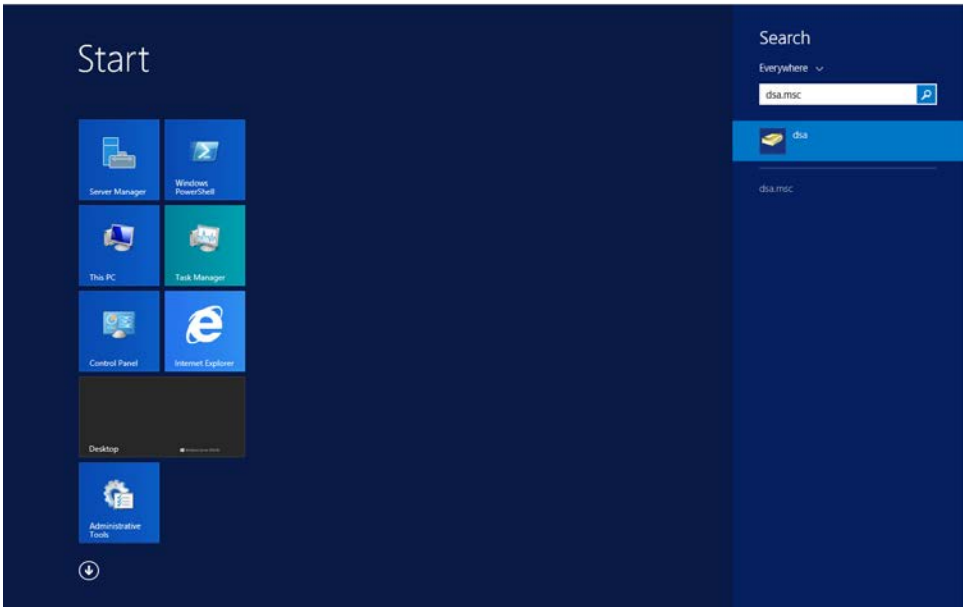
Active Directory Certificate Services

Certification Authority — ✓ Configuration succeeded

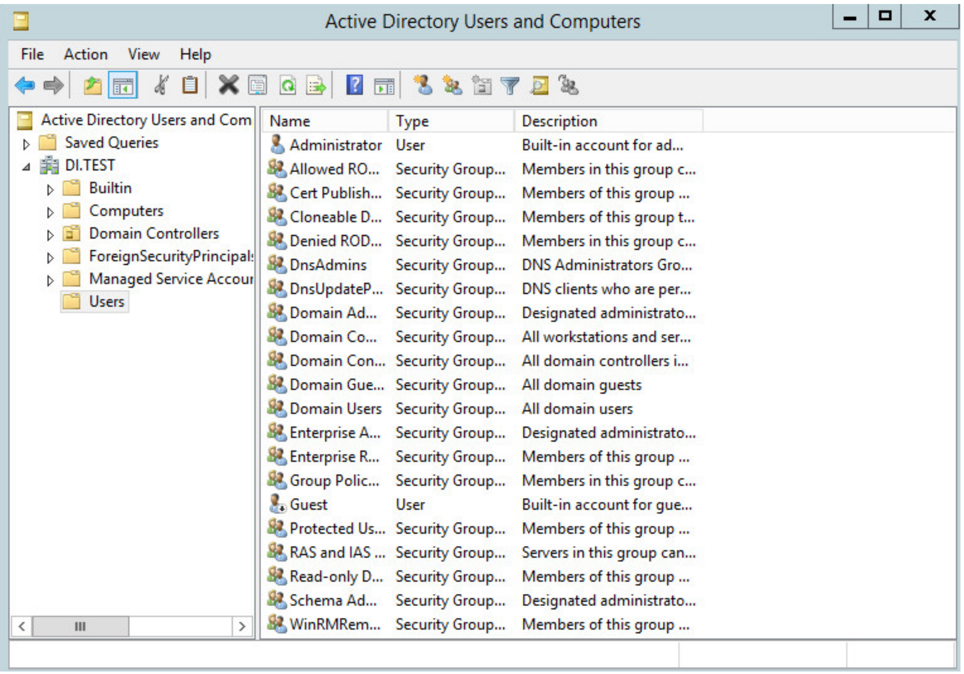
More about CA Configuration

2.1.3 Configure Account to Add Computers to Domain

1. Open the **start menu**.
2. Type **dsa.msc** and run the program.

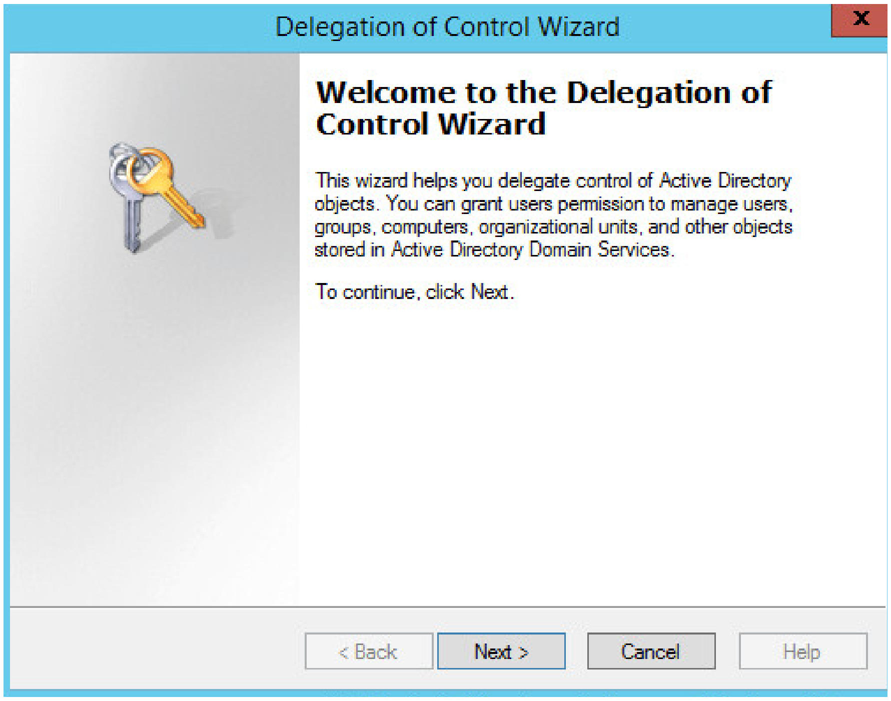


3. Right click on **Users** in the left pane.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
WinRMRem...	Security Group...	Members of this group ...

4. Click **Delegate Control**.



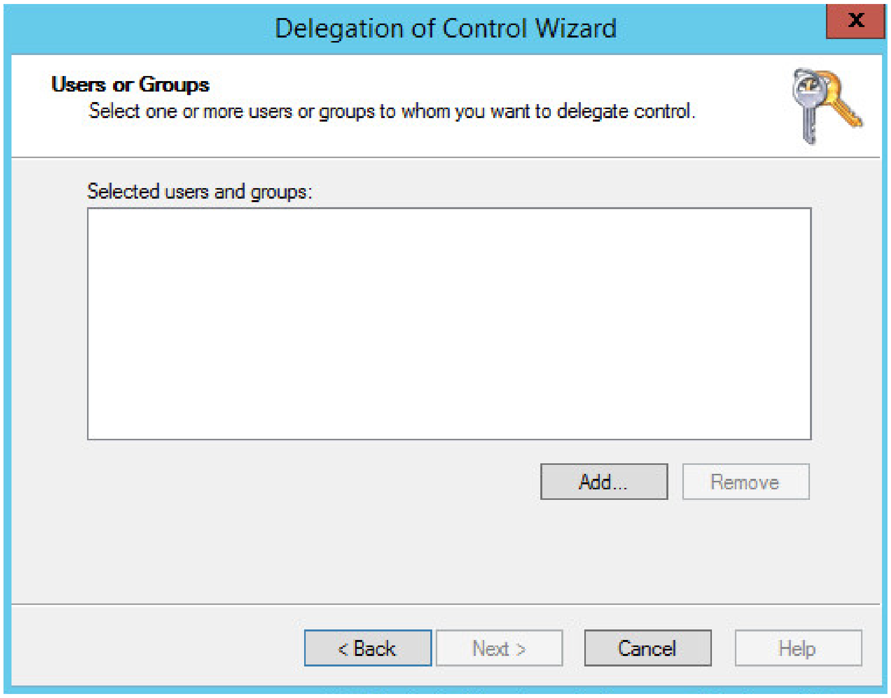
Delegation of Control Wizard

Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

5. Click **Next**.



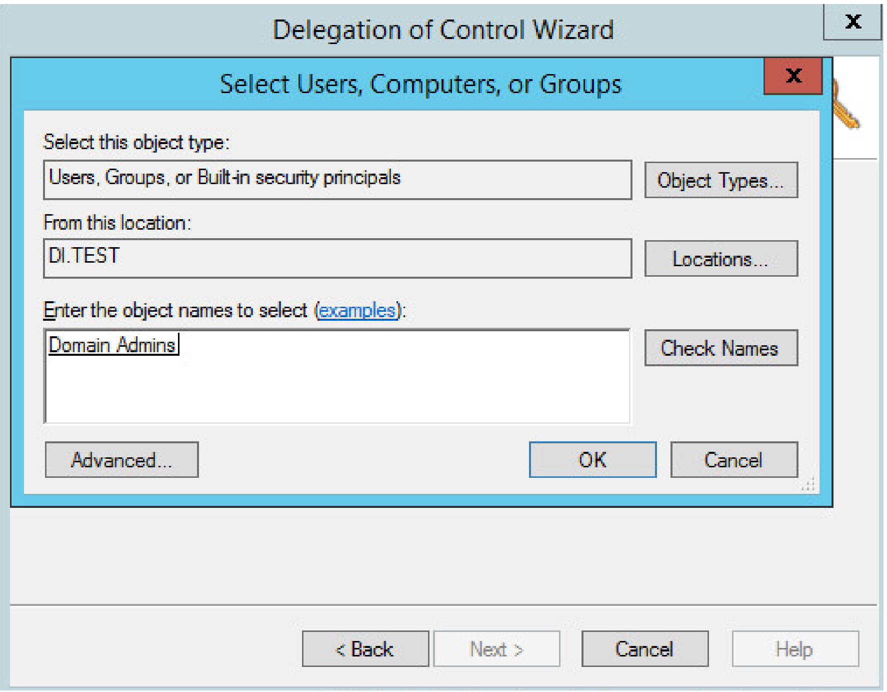
Delegation of Control Wizard

Users or Groups

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

6. Click **Add** to add a user or group. Example: **Domain Admins**.



Delegation of Control Wizard

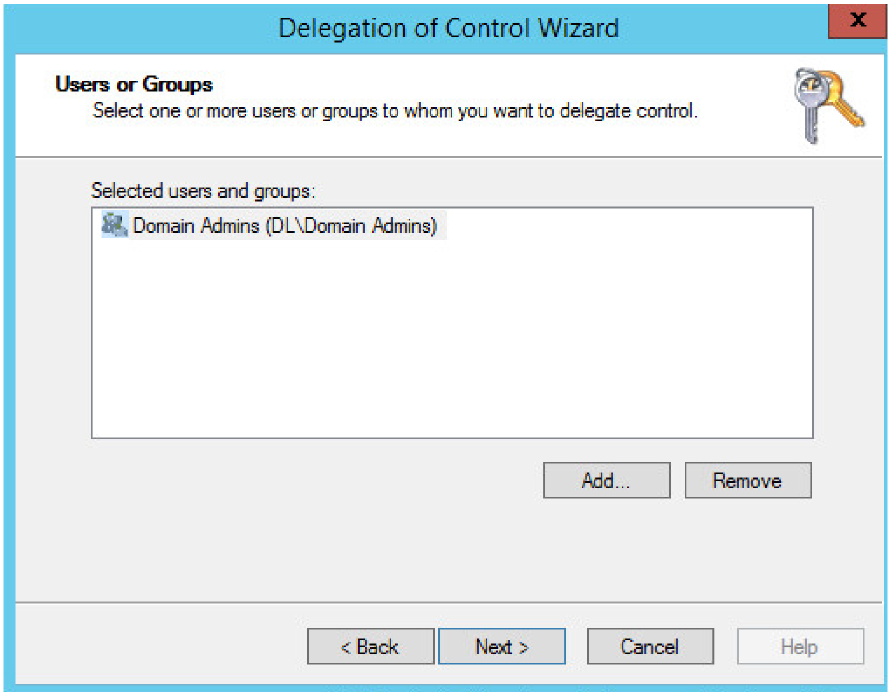
Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
DI.TEST

Enter the object names to select (examples):
Domain Admins

7. When finished adding users or groups, click **OK**.



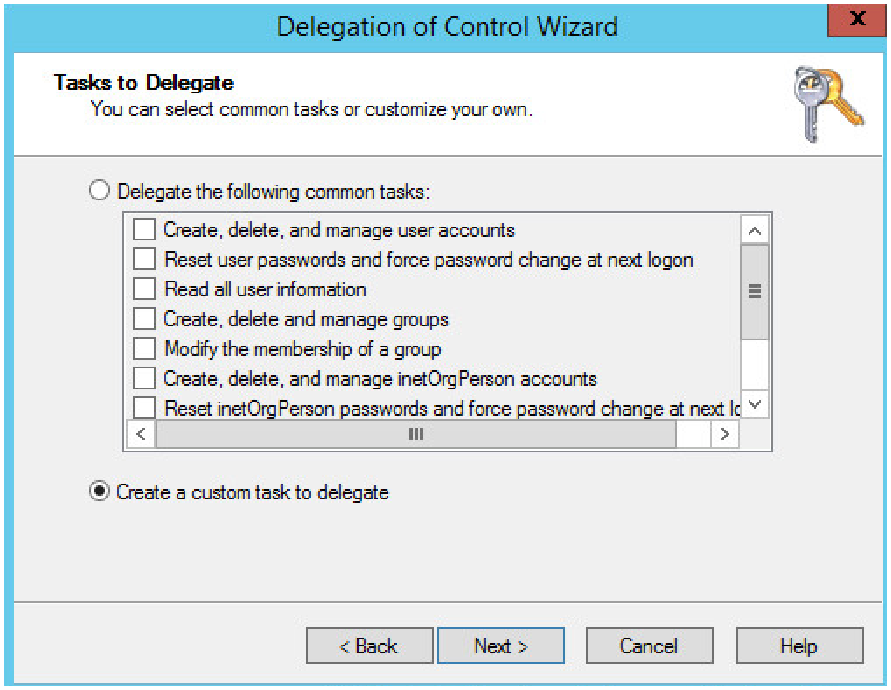
Delegation of Control Wizard

Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:
Domain Admins (DL\Domain Admins)

8. Click **Next**.

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



Delegation of Control Wizard

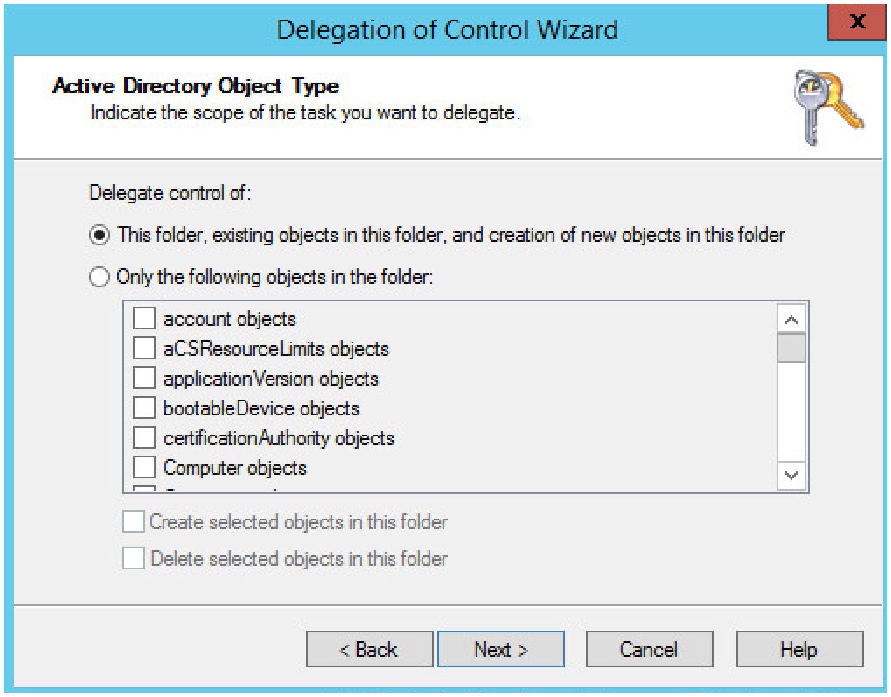
Tasks to Delegate
You can select common tasks or customize your own.

○ Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Create, delete, and manage inetOrgPerson accounts
- □ Reset inetOrgPerson passwords and force password change at next lo

● Create a custom task to delegate

10. Click **Next**.



Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

● This folder, existing objects in this folder, and creation of new objects in this folder

○ Only the following objects in the folder:

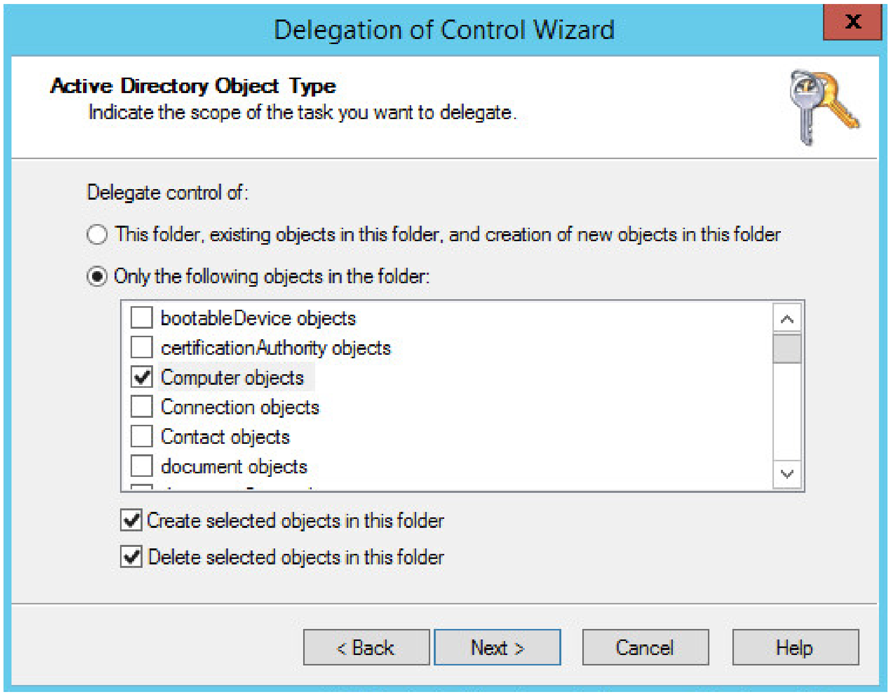
- □ account objects
- □ aCSResourceLimits objects
- □ applicationVersion objects
- □ bootableDevice objects
- □ certificationAuthority objects
- □ Computer objects

□ Create selected objects in this folder

□ Delete selected objects in this folder

11. Choose **Only the following objects in the folder**.
12. Select the **Computer Objects** check box.

13. Check the box for **Create selected objects in this folder**.
14. Check the box for **Delete selected objects in this folder**.



Delegation of Control Wizard

Active Directory Object Type

Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

● Only the following objects in the folder:

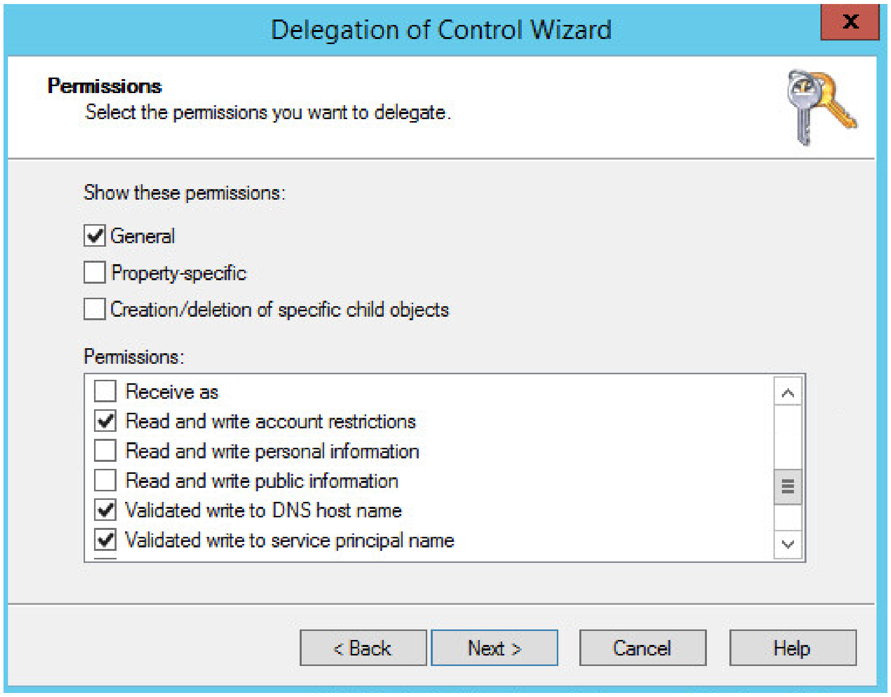
□ bootableDevice objects
□ certificationAuthority objects
☑ Computer objects
□ Connection objects
□ Contact objects
□ document objects

☑ Create selected objects in this folder

☑ Delete selected objects in this folder

15. Click **Next**.

16. In the **Permissions List**, choose **Reset Password**, **Read and write Account Restrictions**, **Validated write to DNS host name, Validated write to service principal name.**



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

☐ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

☐ Receive as

☑ Read and write account restrictions

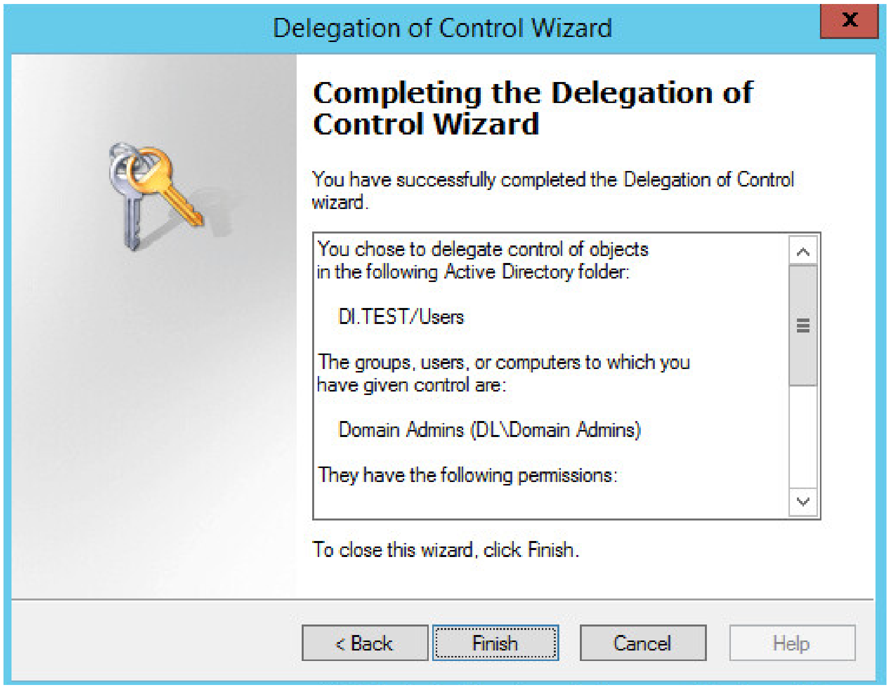
☐ Read and write personal information

☐ Read and write public information

☑ Validated write to DNS host name

☑ Validated write to service principal name

17. Click **Next**.



Delegation of Control Wizard

Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

You chose to delegate control of objects in the following Active Directory folder:

DI.TEST/Users

The groups, users, or computers to which you have given control are:

Domain Admins (DL\Domain Admins)

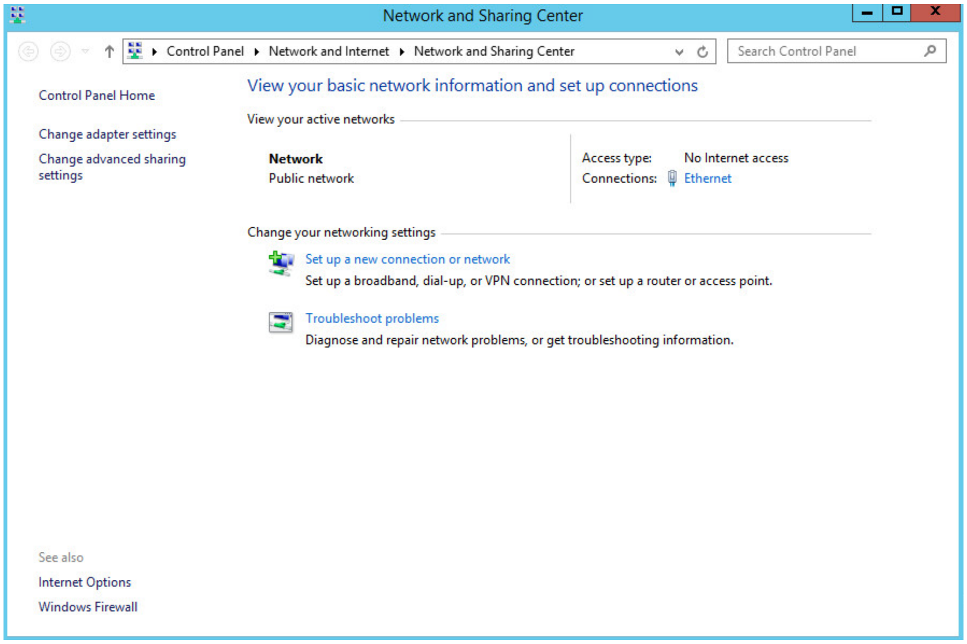
They have the following permissions:

To close this wizard, click Finish.

18. Observe the successful installation and click **Finish**.

2.1.4 Adding Machines to the Correct Domain

1. Right click network icon in task bar.
2. Click **Open Network and Sharing center**.



Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Internet Options
Windows Firewall

View your basic network information and set up connections

View your active networks

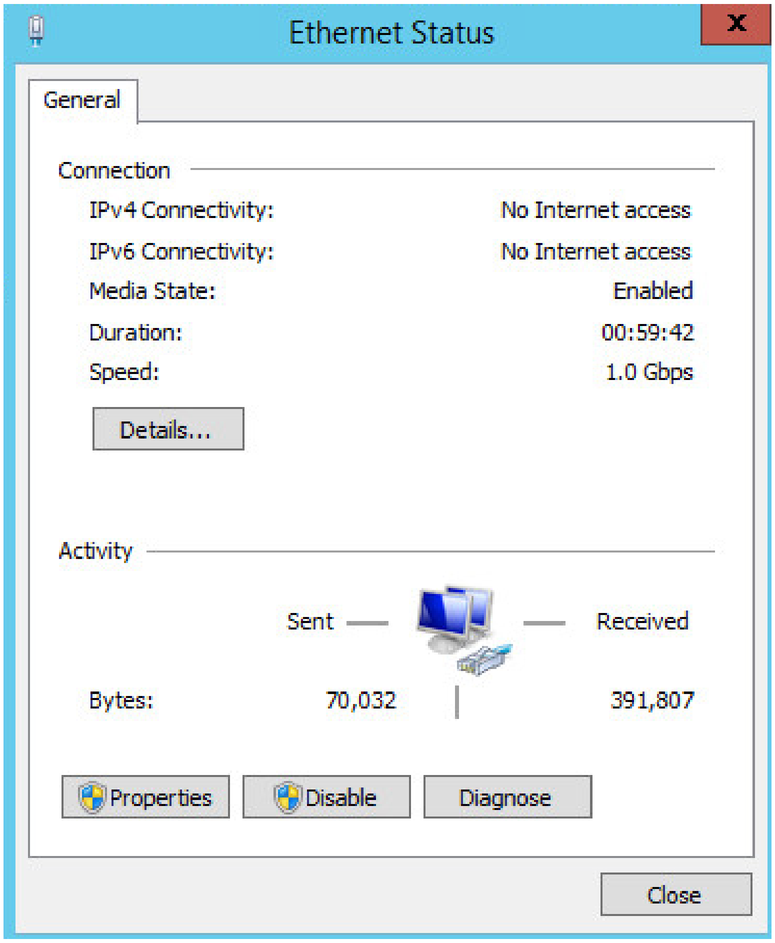
Network Public network	Access type: No Internet access Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Click the link for editing the network interface under **Connections**.



Ethernet Status

Connection

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 00:59:42

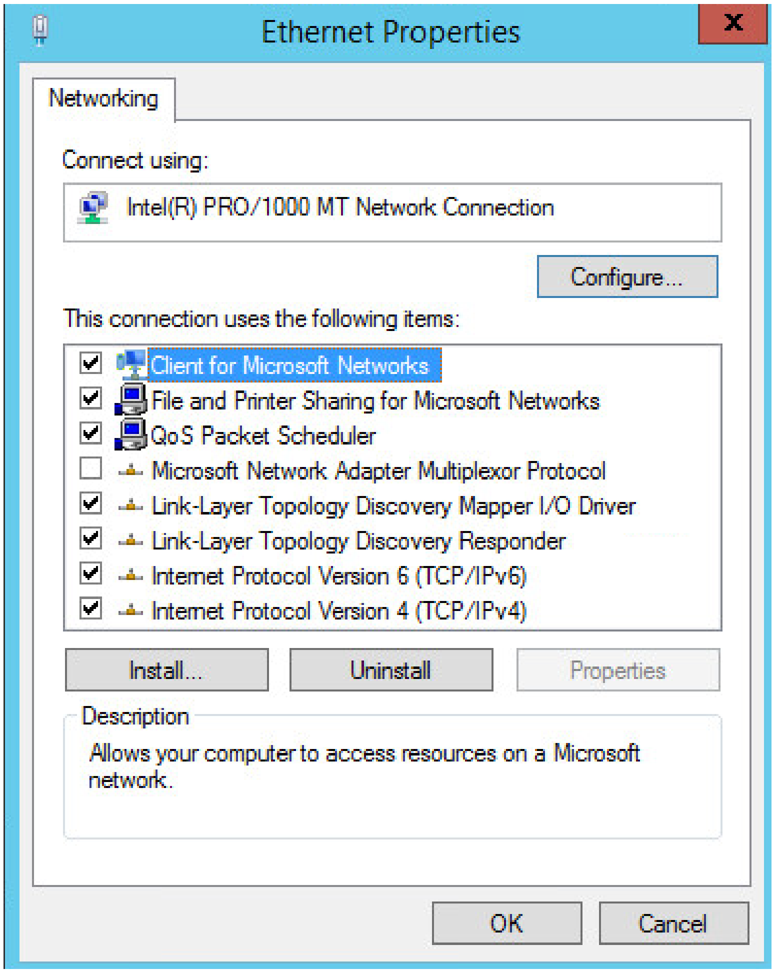
Speed: 1.0 Gbps

Activity

Sent — Received

Bytes: 70,032 | 391,807

4. Click **Properties**.



Connect using:

Intel(R) PRO/1000 MT Network Connection

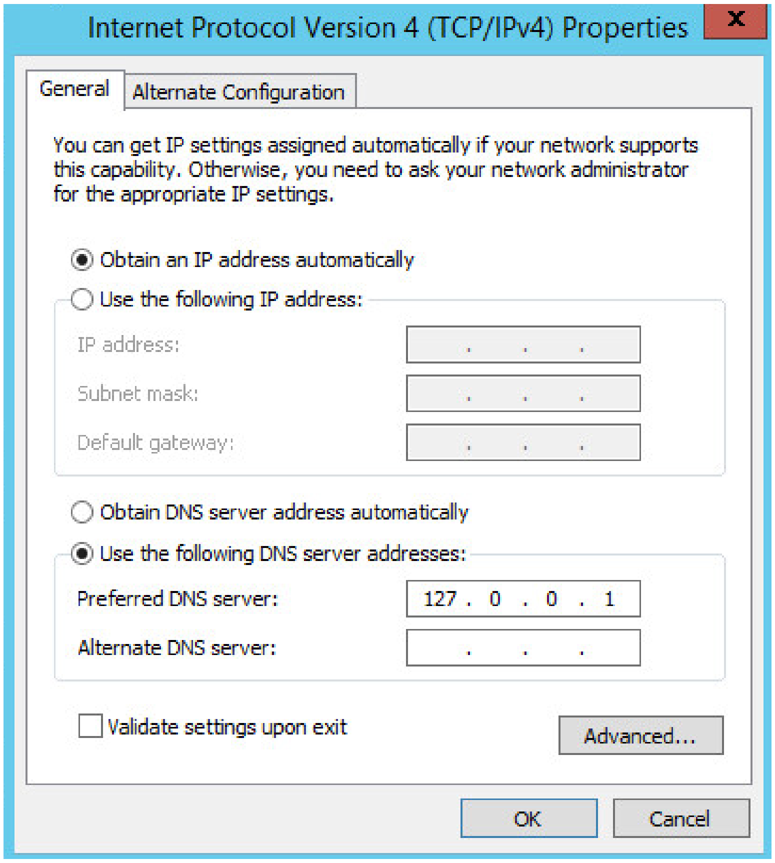
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Allows your computer to access resources on a Microsoft network.

5. Click **Internet Protocol Version 4**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

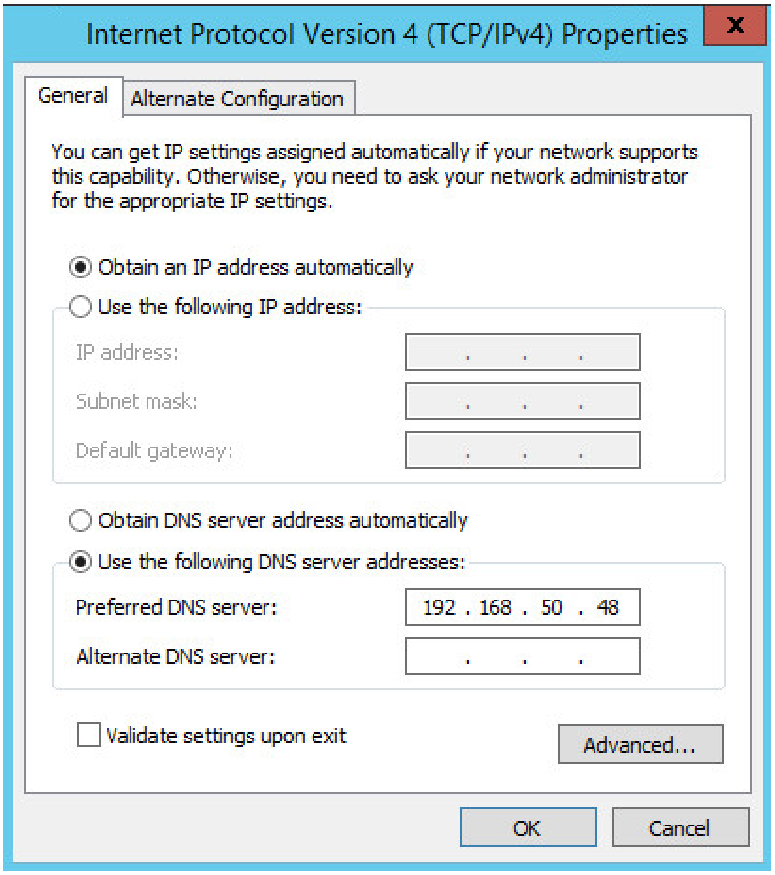
Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

6. Click **Properties**.

7. Set the **DNS** field to the IP address of the AD/DNS server.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

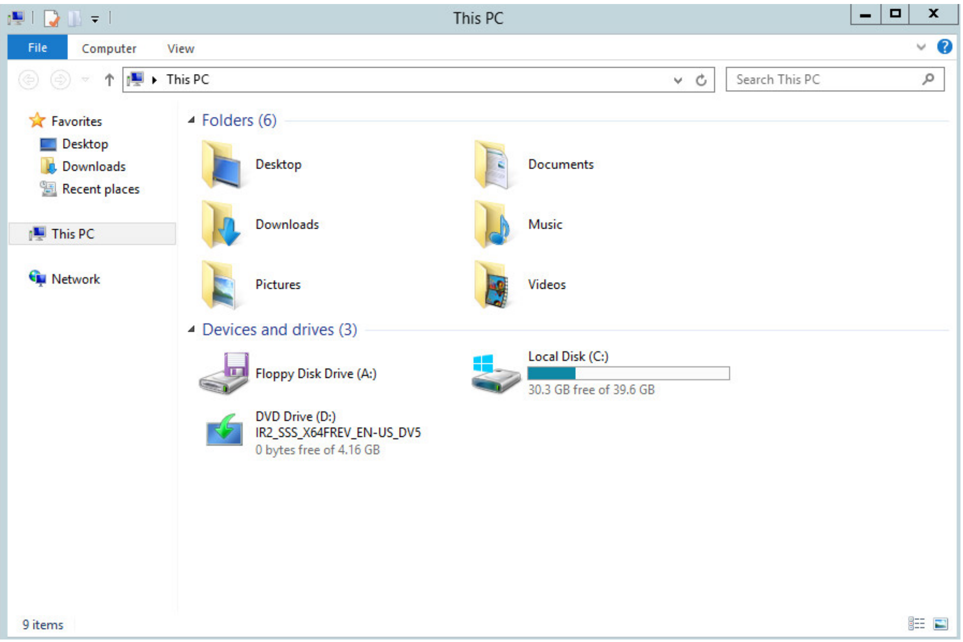
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 50 . 48

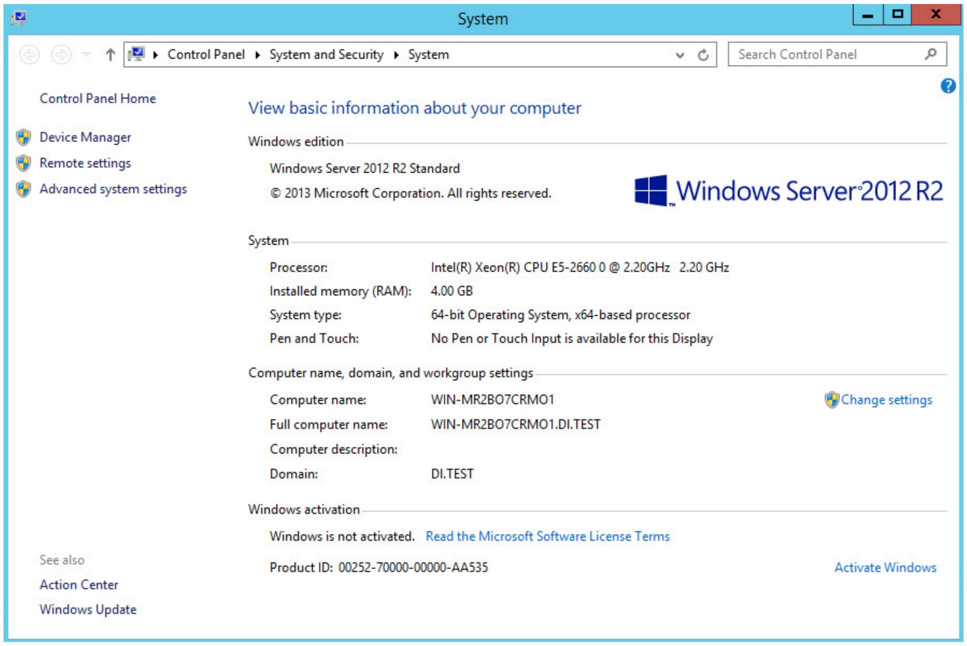
Alternate DNS server: . . .

□ Validate settings upon exit

8. Click **OK**.
9. Exit out of the **Network and Sharing Center**
10. Push the **start menu** button.



11. Go to **This PC**.
12. Right click in the window and choose **Properties**.



View basic information about your computer

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz 2.20 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	WIN-MR2BO7CRMO1
Full computer name:	WIN-MR2BO7CRMO1.DI.TEST
Computer description:	
Domain:	DI.TEST

Change settings

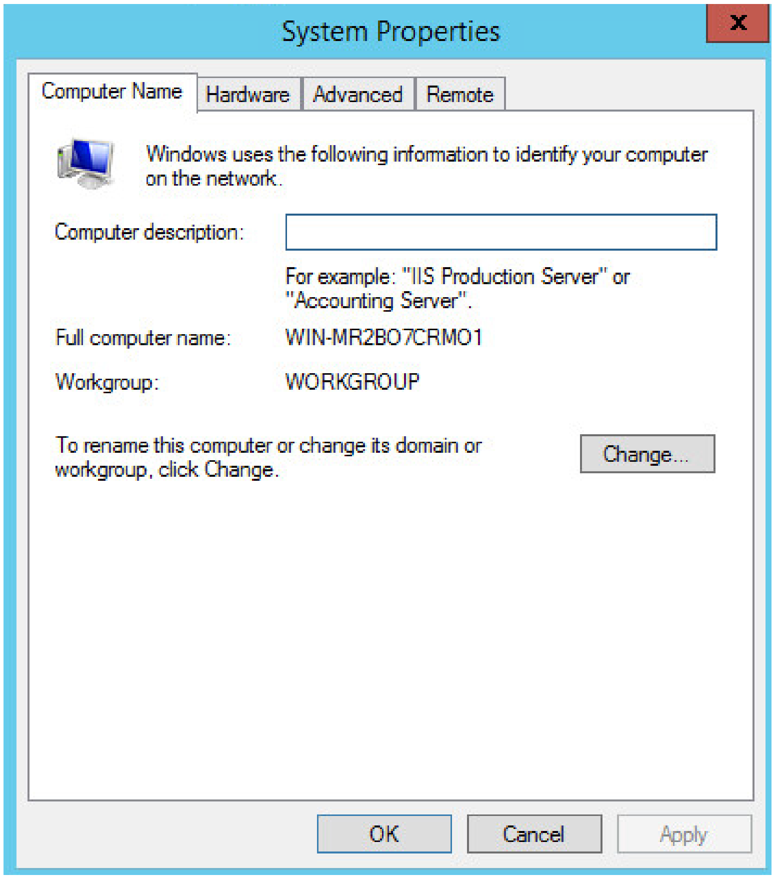
Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00252-70000-00000-AA535

Activate Windows

13. Under **Name, domain, and workgroup settings**, click **Change settings**.



System Properties

Computer Name | Hardware | Advanced | Remote

Windows uses the following information to identify your computer on the network.

Computer description:

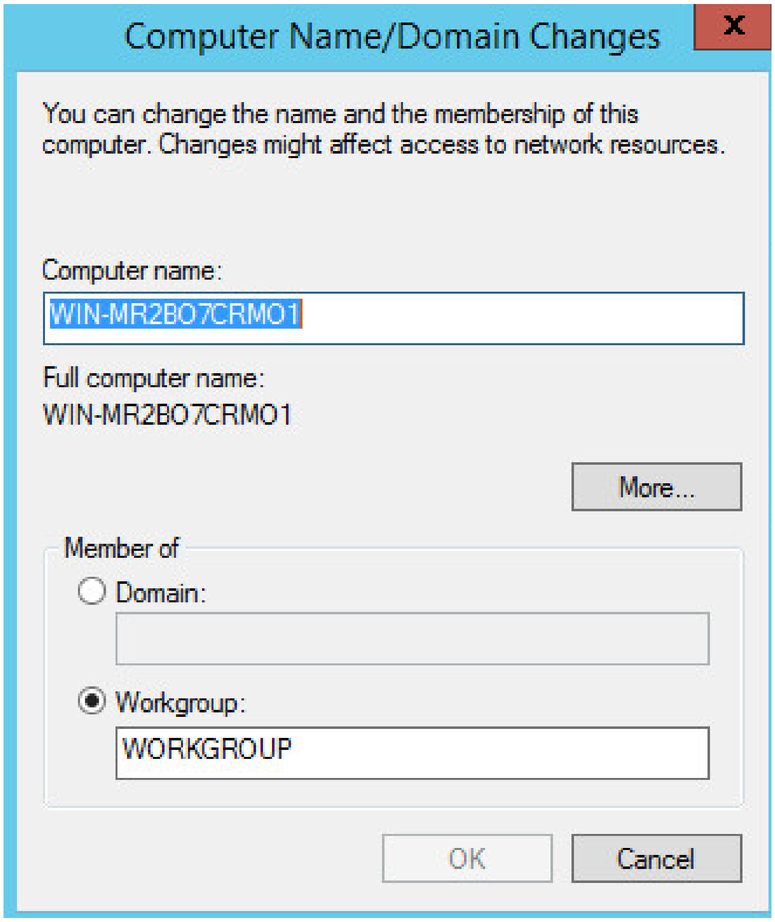
For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-MR2BO7CRMO1

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

14. Click **Change...**.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: WIN-MR2BO7CRMO1

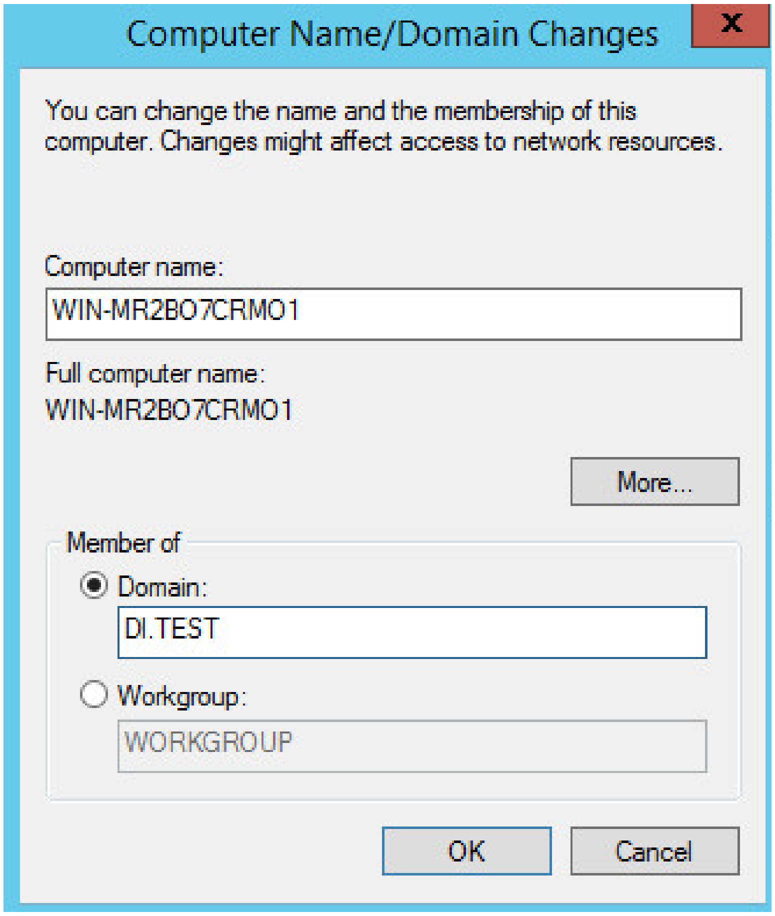
Full computer name: WIN-MR2BO7CRMO1

Member of

○ Domain:

● Workgroup: WORKGROUP

15. Select **Domain** and enter the domain specified on the AD/DNS server.



Computer Name/Domain Changes

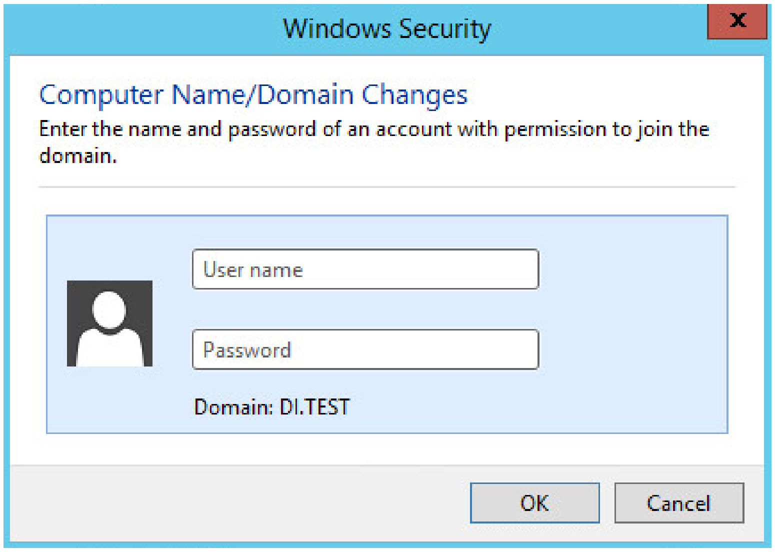
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
WIN-MR2BO7CRMO1

Full computer name:
WIN-MR2BO7CRMO1

Member of
● Domain:
DI.TEST
○ Workgroup:
WORKGROUP

16. Click **OK**.



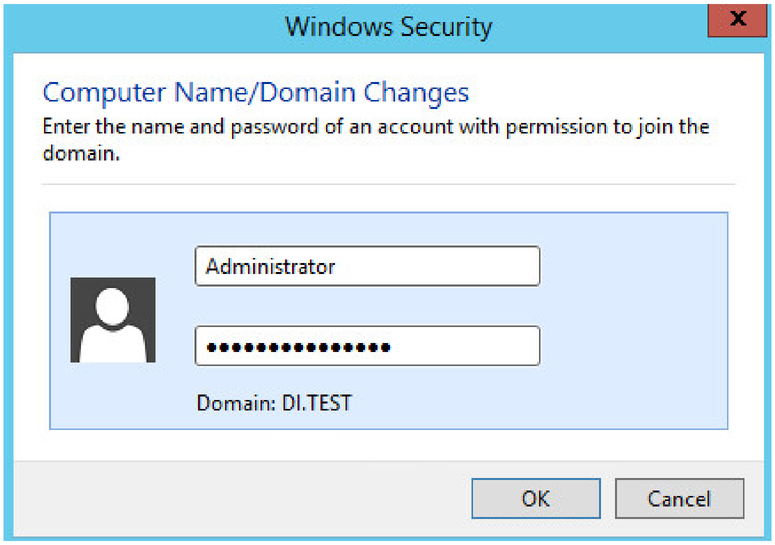
Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

User name
Password
Domain: DI.TEST

17. Enter the credentials of an account in AD which has the right permissions to add a group to the domain.



Computer Name/Domain Changes

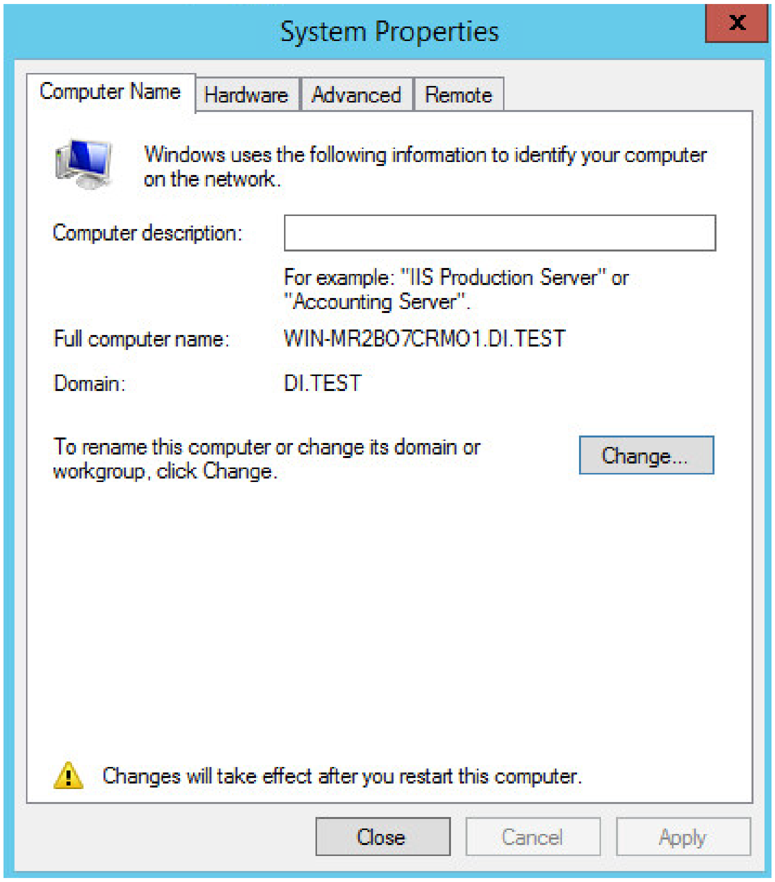
Enter the name and password of an account with permission to join the domain.

Administrator

•••••••••••••••

Domain: DI.TEST

18. Click **OK** a few times and restart the server when prompted.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-MR2BO7CRMO1.DI.TEST

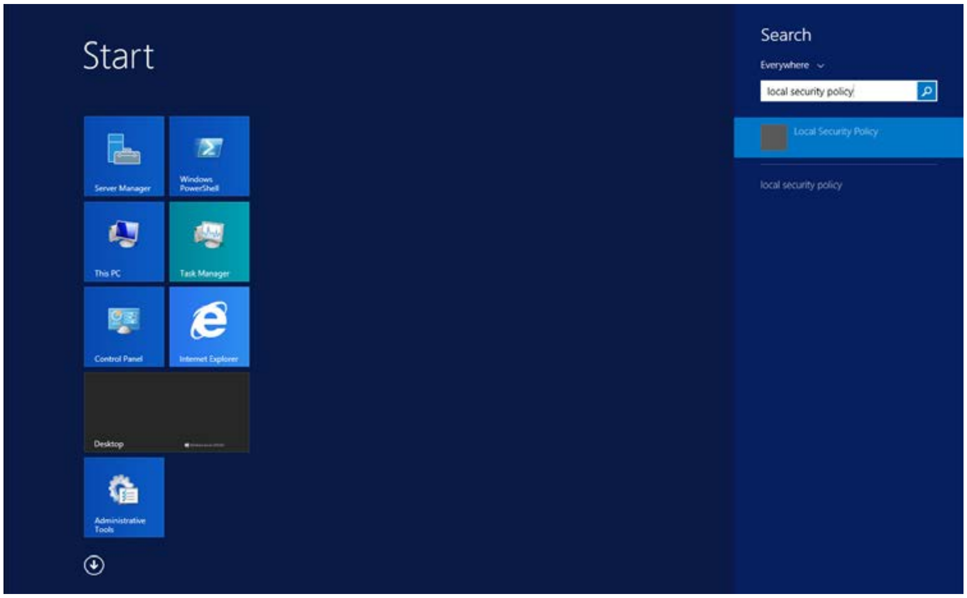
Domain: DI.TEST

To rename this computer or change its domain or workgroup, click Change.

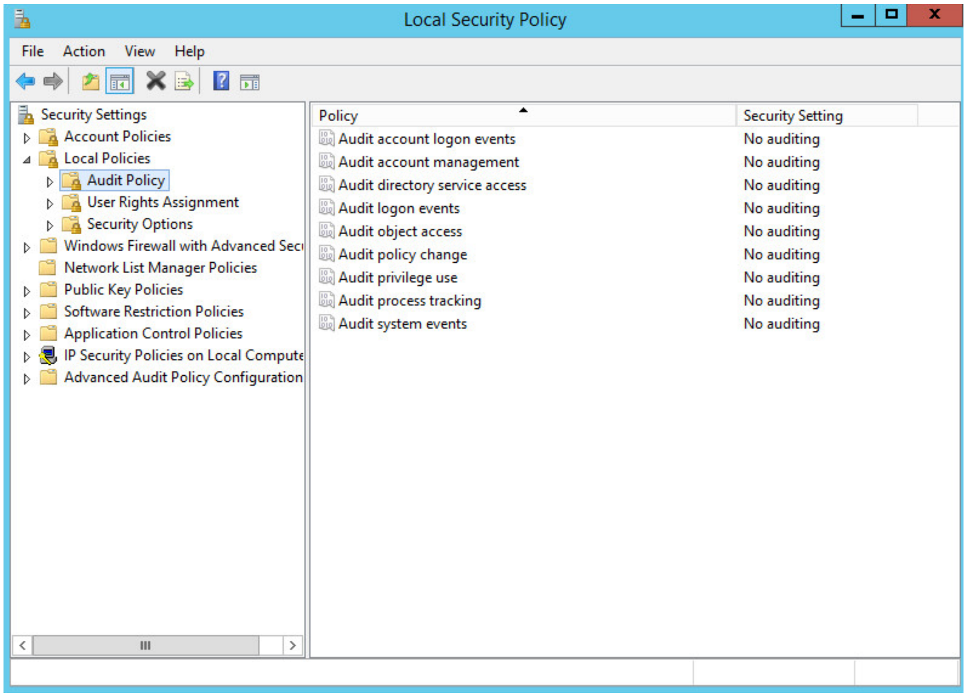
Changes will take effect after you restart this computer.

2.1.5 Configuring Active Directory to Audit Account Activity

1. Open **Local Security Policy** from the Start Menu.

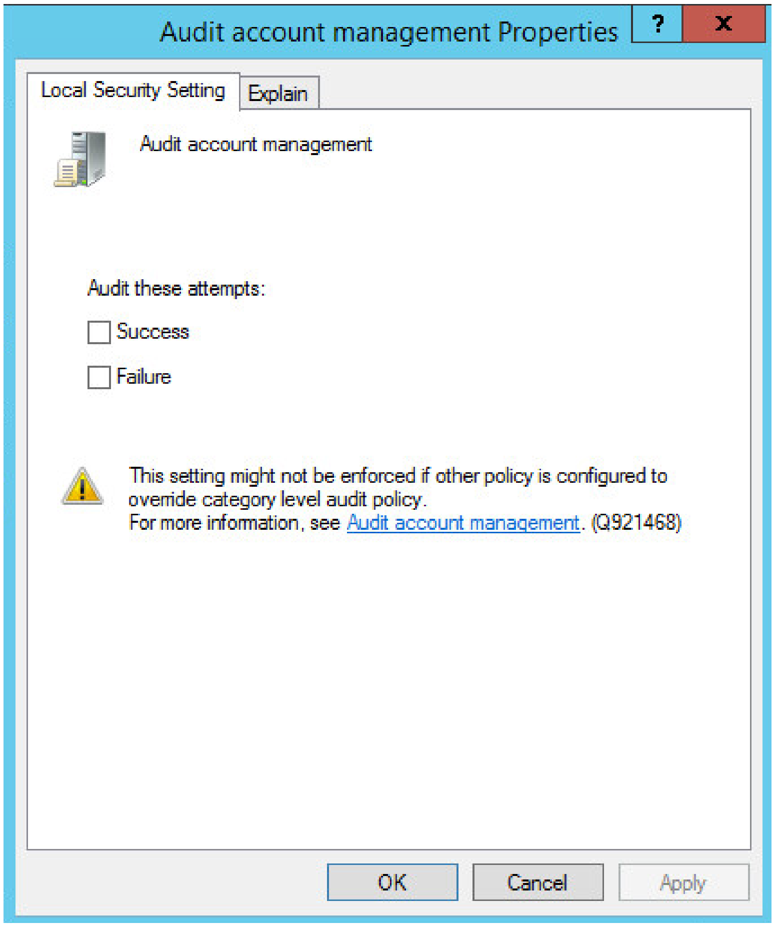


2. Open **Local Policies** > **Audit Policy**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

3. Right click **Audit account management**.
4. Select **Properties**.



Audit account management Properties

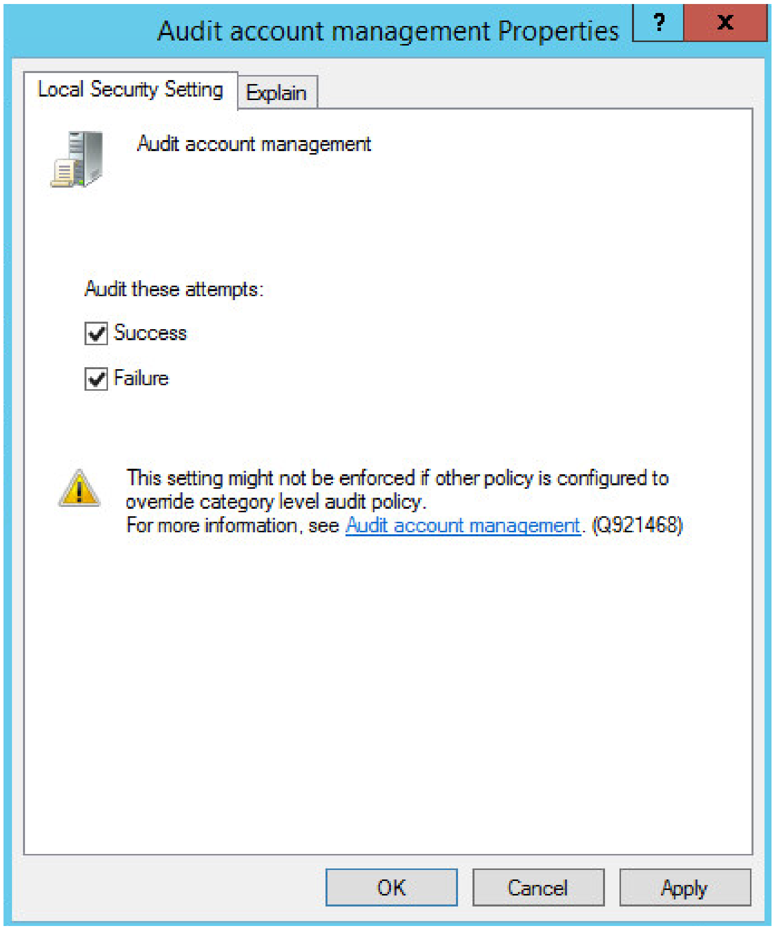
Audit account management

Audit these attempts:

□ Success

□ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account management. (Q921468)



Audit account management

Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account management. (Q921468)

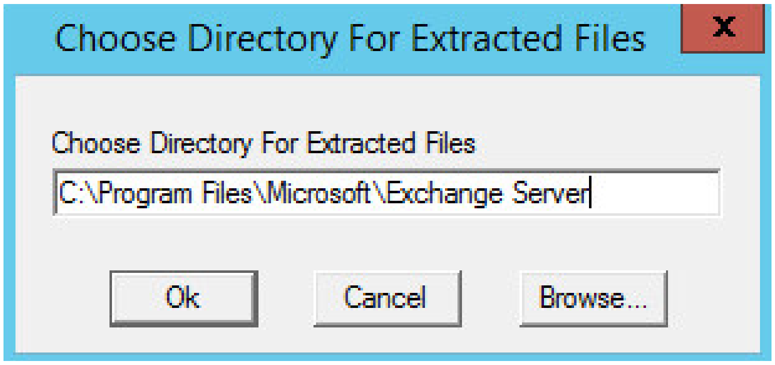
5. Check the boxes next to **Success** and **Failure**.
6. Click **OK**.
7. Account management activities will now be reported to **Windows Event Log – Security**.

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

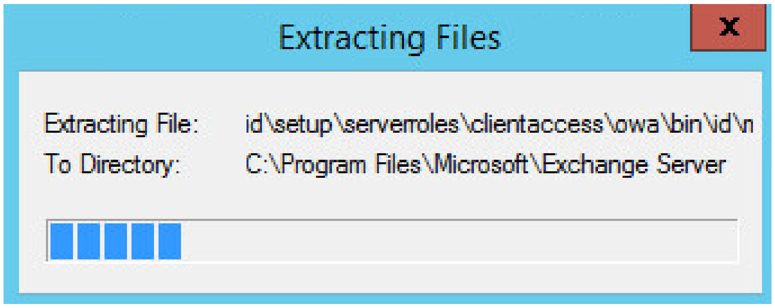
1. Run **Exchange2016-x64.exe**.



Choose Directory For Extracted Files

C:\Program Files\Microsoft\Exchange Server

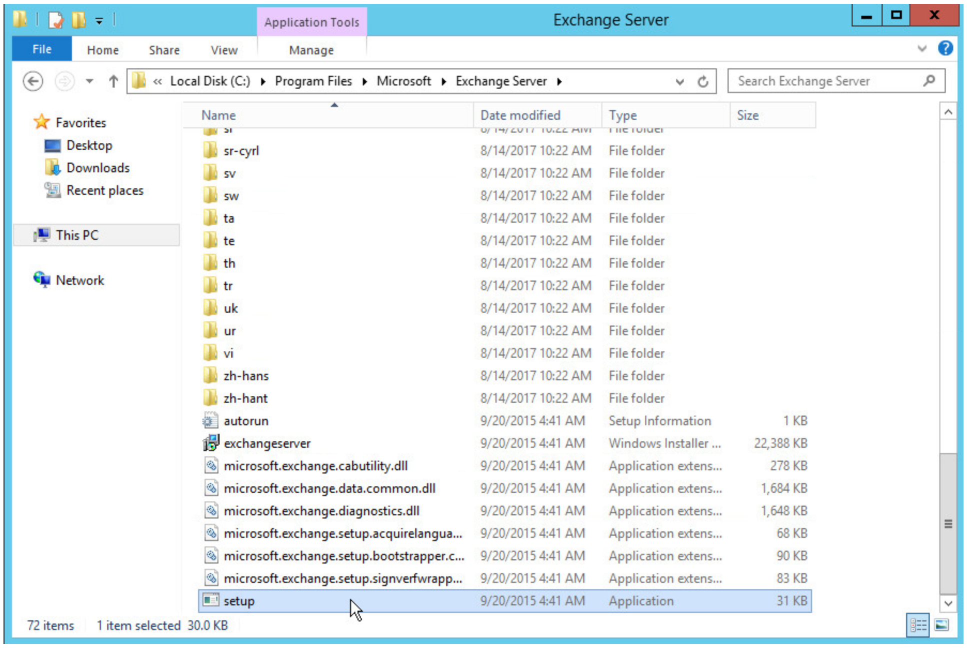
2. Choose the directory for the extracted files and press **OK**.



Extracting File: id\setup\serverroles\clientaccess\owa\bin\id\n

To Directory: C:\Program Files\Microsoft\Exchange Server

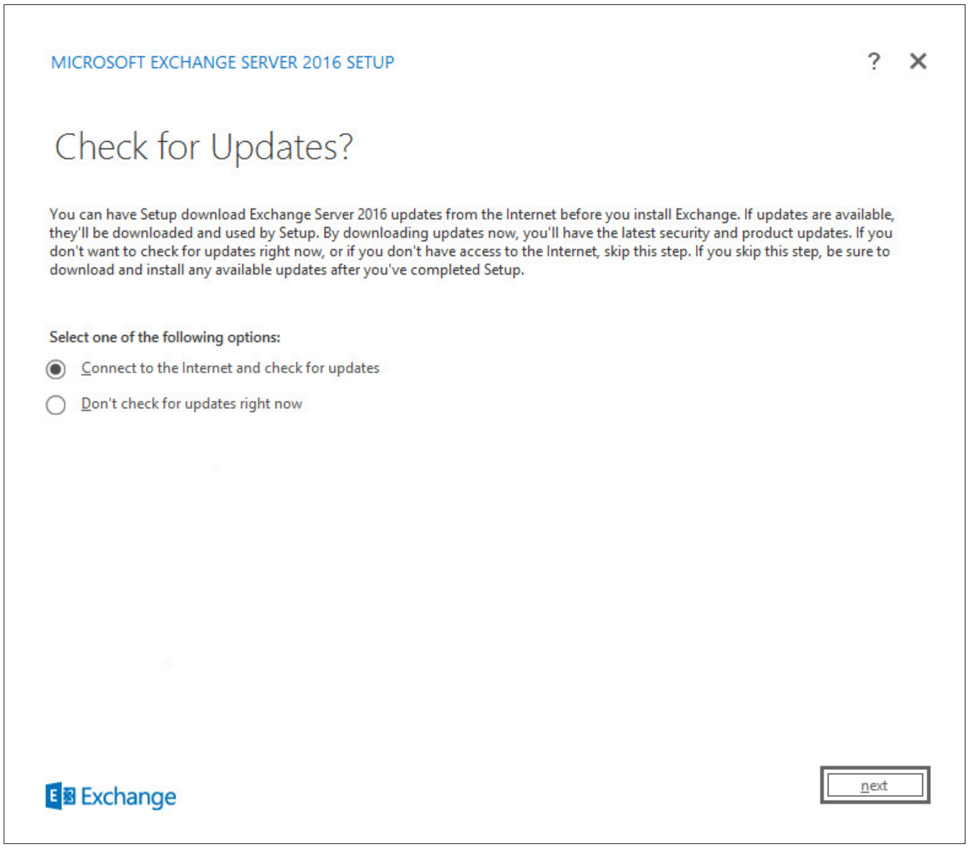
3. Enter the directory and run **setup.exe**.



Name	Date modified	Type	Size
sr-cyrl	8/14/2017 10:22 AM	File folder	
sv	8/14/2017 10:22 AM	File folder	
sw	8/14/2017 10:22 AM	File folder	
ta	8/14/2017 10:22 AM	File folder	
te	8/14/2017 10:22 AM	File folder	
th	8/14/2017 10:22 AM	File folder	
tr	8/14/2017 10:22 AM	File folder	
uk	8/14/2017 10:22 AM	File folder	
ur	8/14/2017 10:22 AM	File folder	
vi	8/14/2017 10:22 AM	File folder	
zh-hans	8/14/2017 10:22 AM	File folder	
zh-hant	8/14/2017 10:22 AM	File folder	
autorun	9/20/2015 4:41 AM	Setup Information	1 KB
exchangeserver	9/20/2015 4:41 AM	Windows Installer ...	22,388 KB
microsoft.exchange.cabutility.dll	9/20/2015 4:41 AM	Application extens...	278 KB
microsoft.exchange.data.common.dll	9/20/2015 4:41 AM	Application extens...	1,684 KB
microsoft.exchange.diagnostics.dll	9/20/2015 4:41 AM	Application extens...	1,648 KB
microsoft.exchange.setup.acquirelangua...	9/20/2015 4:41 AM	Application extens...	68 KB
microsoft.exchange.setup.bootstrapper.c...	9/20/2015 4:41 AM	Application extens...	90 KB
microsoft.exchange.setup.signverfwrapp...	9/20/2015 4:41 AM	Application extens...	83 KB
setup	9/20/2015 4:41 AM	Application	31 KB

72 items 1 item selected 30.0 KB

4. Select **Connect to the Internet and check for updates**.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Check for Updates?

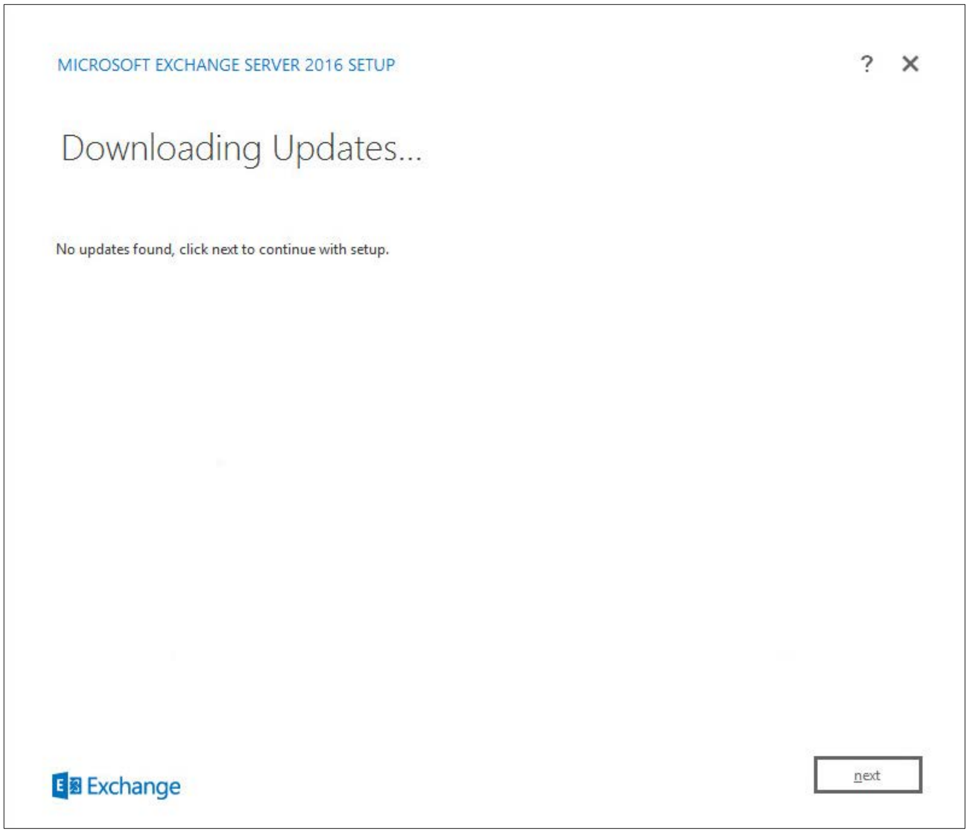
You can have Setup download Exchange Server 2016 updates from the Internet before you install Exchange. If updates are available, they'll be downloaded and used by Setup. By downloading updates now, you'll have the latest security and product updates. If you don't want to check for updates right now,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

Select one of the following options:

● Connect to the Internet and check for updates

○ Don't check for updates right now

5. Wait for the check to finish.

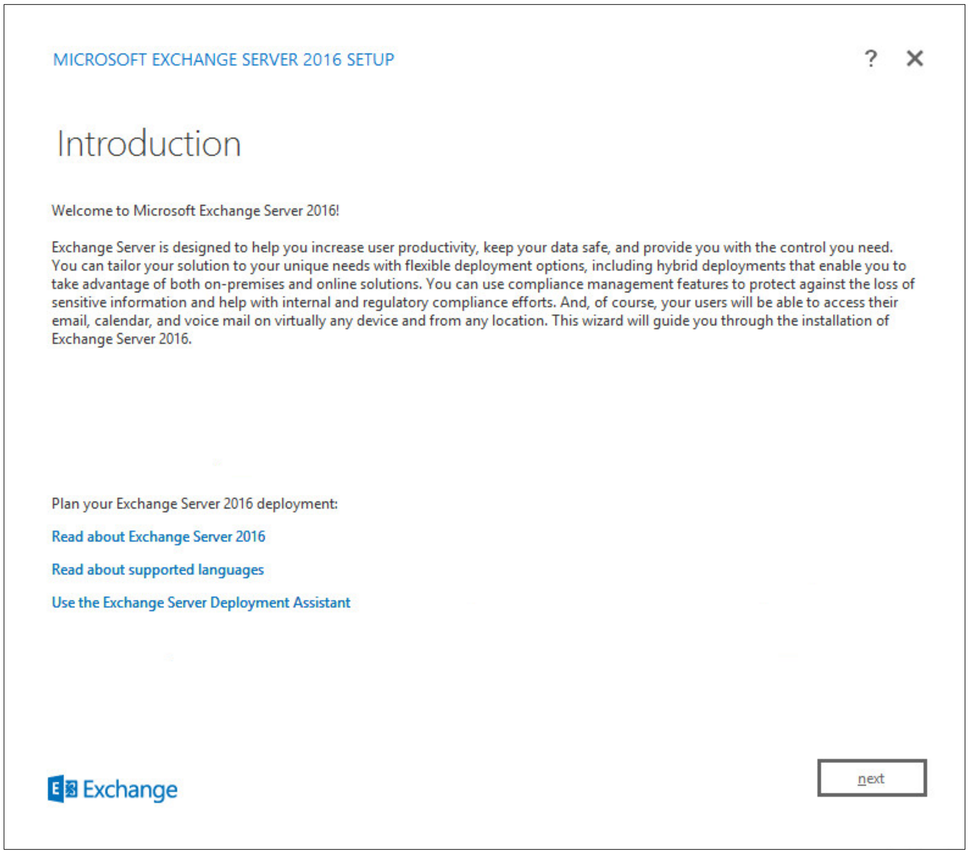


MICROSOFT EXCHANGE SERVER 2016 SETUP

Downloading Updates...

No updates found, click next to continue with setup.

6. Click **Next**.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Introduction

Welcome to Microsoft Exchange Server 2016!

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

Plan your Exchange Server 2016 deployment:

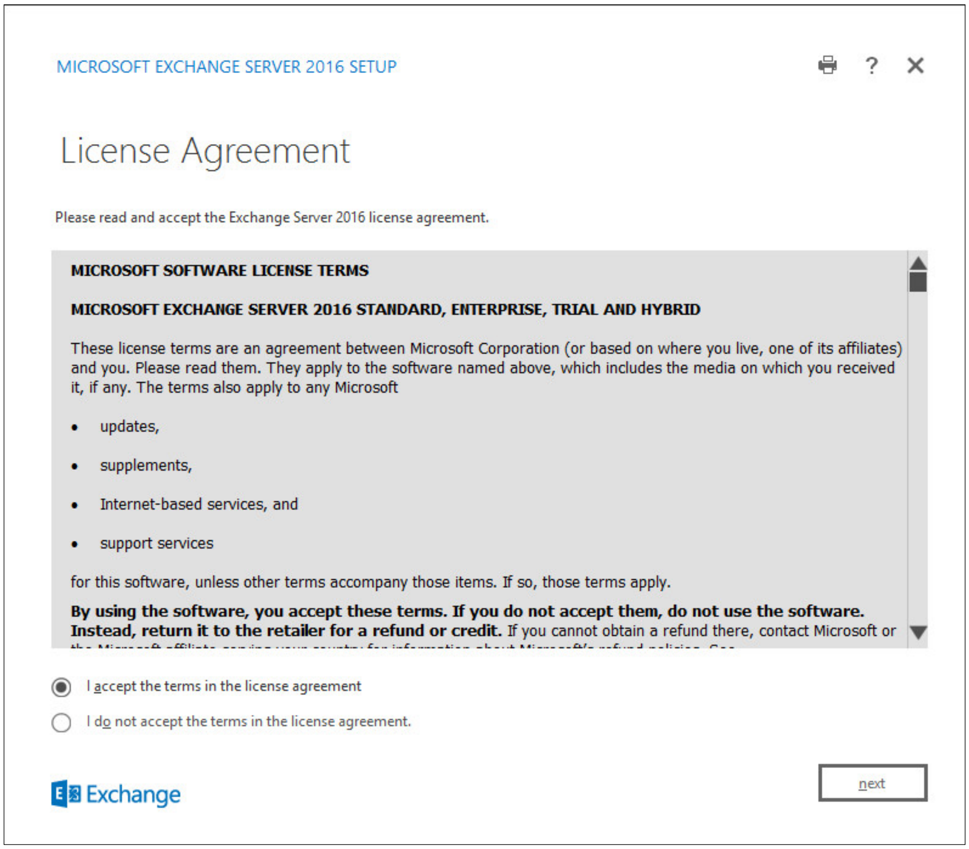
Read about Exchange Server 2016

Read about supported languages

Use the Exchange Server Deployment Assistant

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

9. Click **I accept the terms in the license agreement**.



MICROSOFT EXCHANGE SERVER 2016 SETUP

License Agreement

Please read and accept the Exchange Server 2016 license agreement.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT EXCHANGE SERVER 2016 STANDARD, ENTERPRISE, TRIAL AND HYBRID

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

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

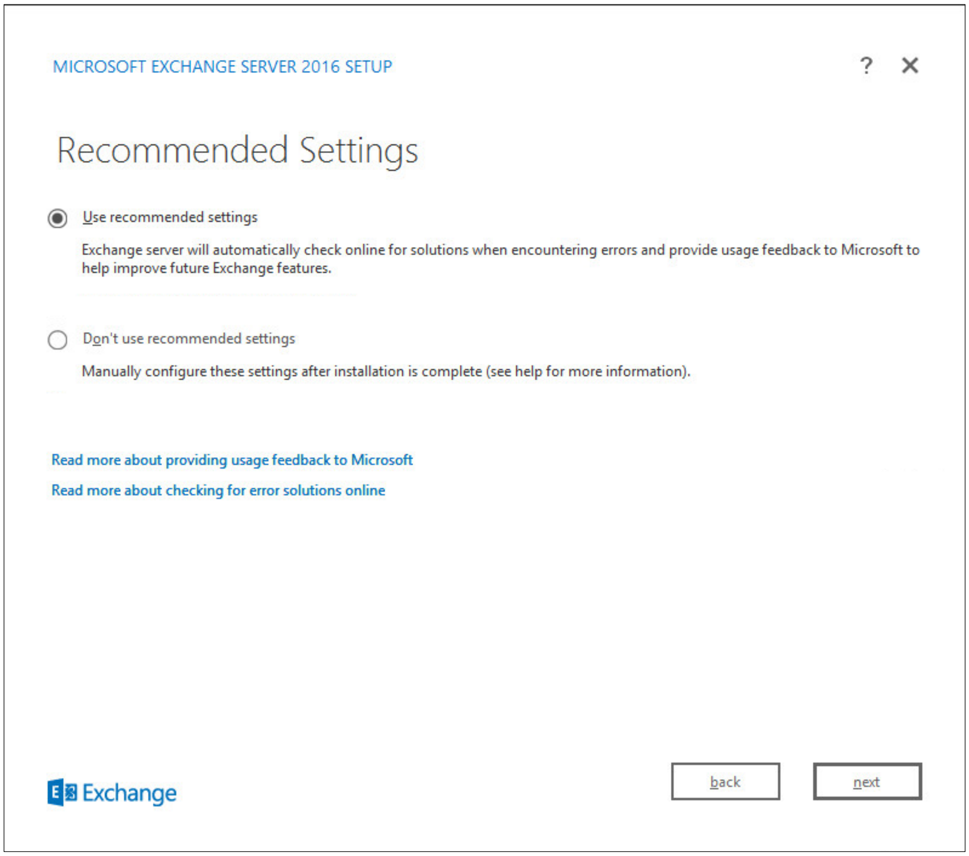
for this software, unless other terms accompany those items. If so, those terms apply.

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

● I accept the terms in the license agreement

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

10. Click **Next**.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Recommended Settings

● Use recommended settings

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

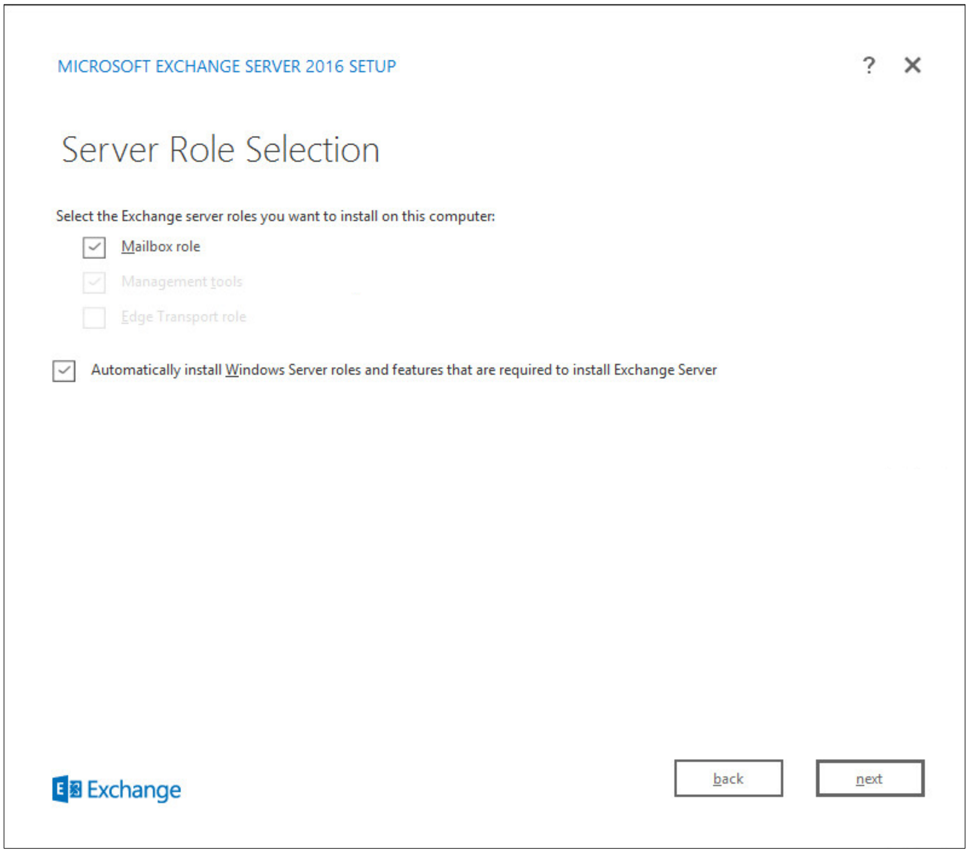
○ Don't use recommended settings

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

Read more about providing usage feedback to Microsoft

Read more about checking for error solutions online

11. Click **Use Recommended Settings**.
12. Click **Next**.
13. Check **Mailbox role**.
14. Check **Automatically install Windows Server roles and features that are required to install Exchange Server**.


MICROSOFT EXCHANGE SERVER 2016 SETUP

Server Role Selection

Select the Exchange server roles you want to install on this computer:

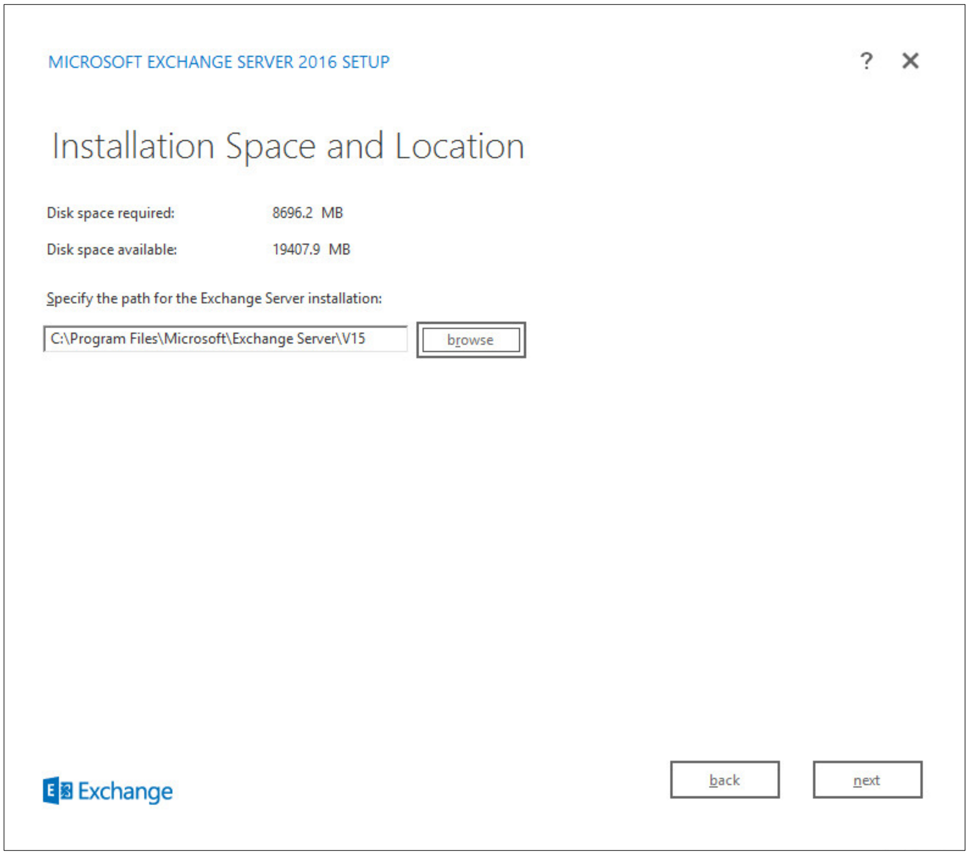
☑ Mailbox role

☑ Management tools

□ Edge Transport role

☑ Automatically install Windows Server roles and features that are required to install Exchange Server

15. Click **Next**.
16. Specify the installation path for MS Exchange.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Installation Space and Location

Disk space required: 8696.2 MB

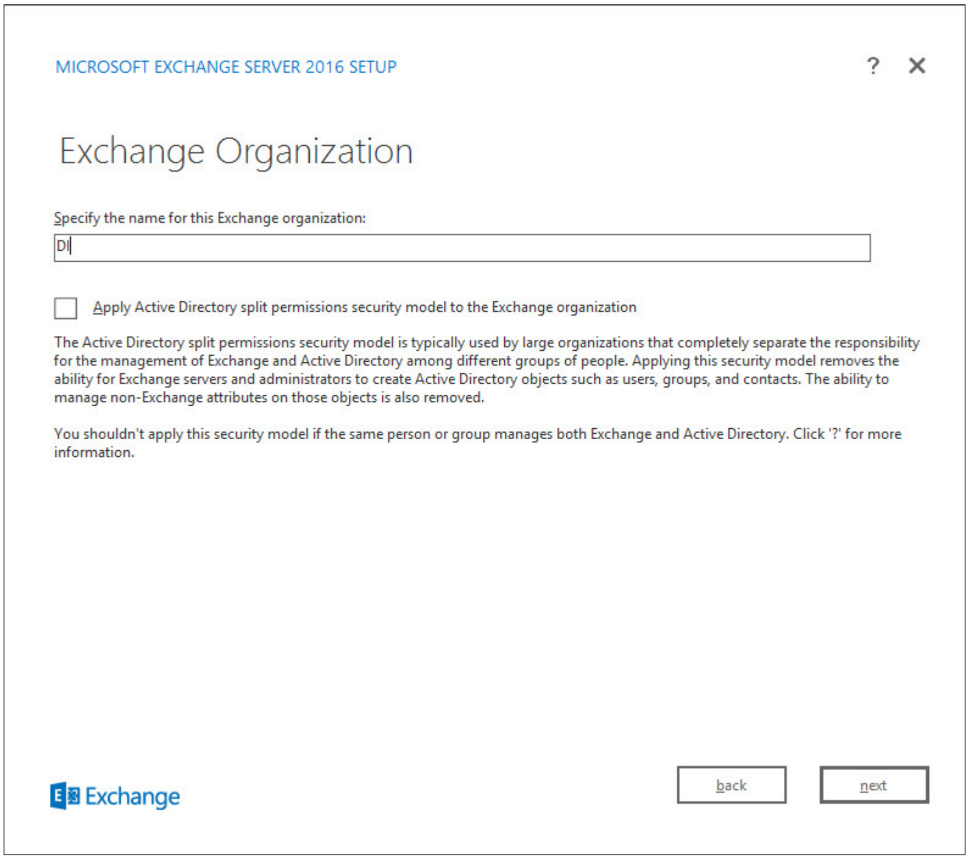
Disk space available: 19407.9 MB

Specify the path for the Exchange Server installation:

C:\Program Files\Microsoft\Exchange Server\V15

17. Click **Next**.
18. Specify the name for the Exchange organization. Example: DI.

19. Decide whether to apply split permissions based on the needs of the enterprise.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Exchange Organization

Specify the name for this Exchange organization:

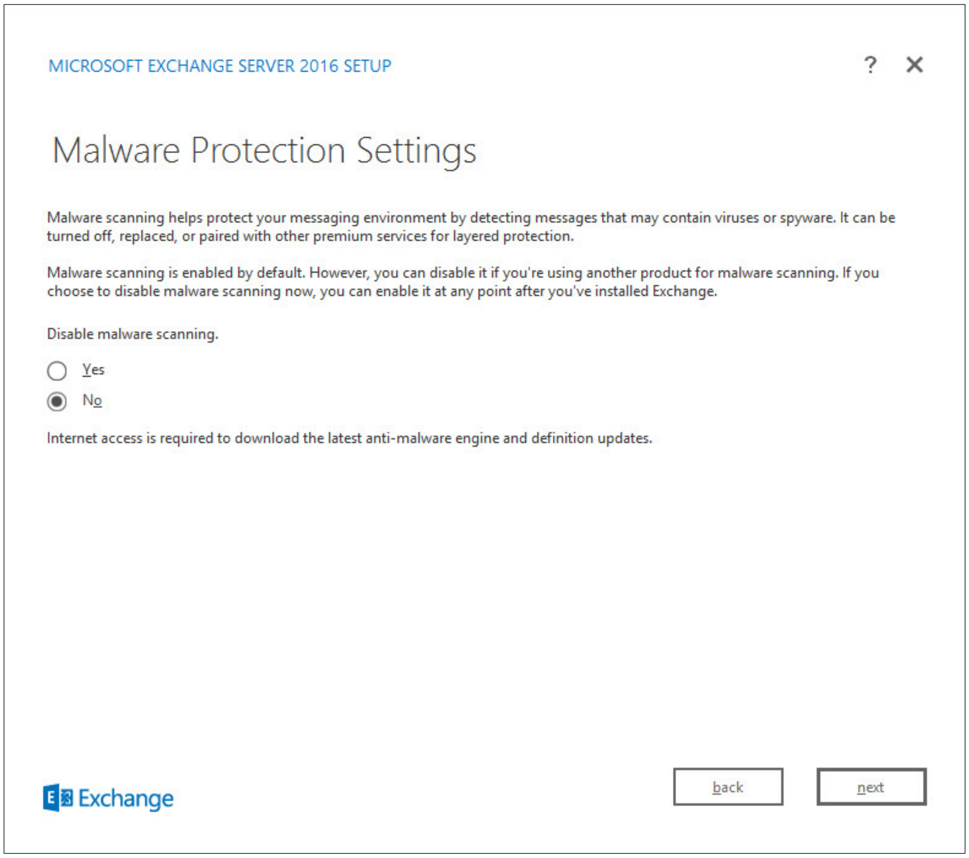
DI

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

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

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

20. Click **Next**.
21. Click **No**.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Malware Protection Settings

Malware scanning helps protect your messaging environment by detecting messages that may contain viruses or spyware. It can be turned off, replaced, or paired with other premium services for layered protection.

Malware scanning is enabled by default. However, you can disable it if you're using another product for malware scanning. If you choose to disable malware scanning now, you can enable it at any point after you've installed Exchange.

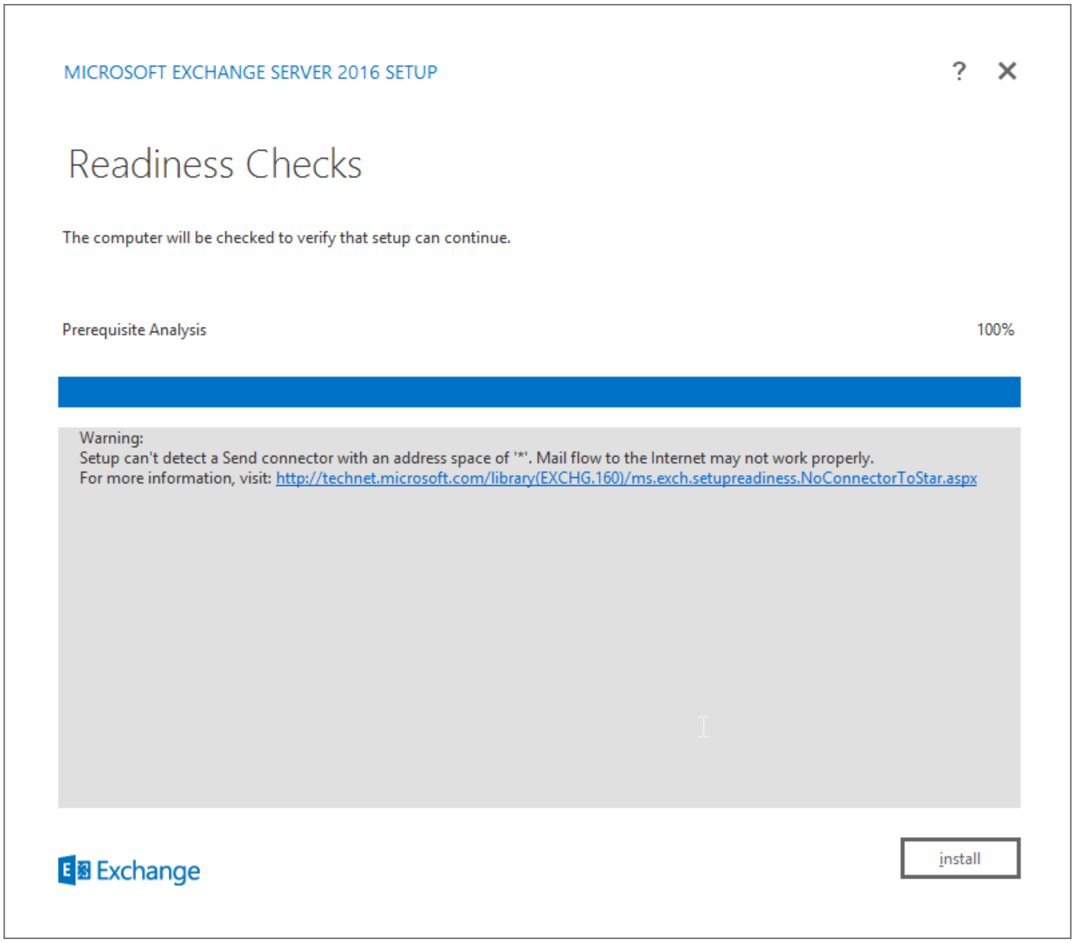
Disable malware scanning.

○ Yes

● No

Internet access is required to download the latest anti-malware engine and definition updates.

22. Click **Next**.
23. Install any **prerequisites** listed.
24. If necessary, restart the server and re-run **setup.exe**, following through steps 3 to 22 again.


MICROSOFT EXCHANGE SERVER 2016 SETUP

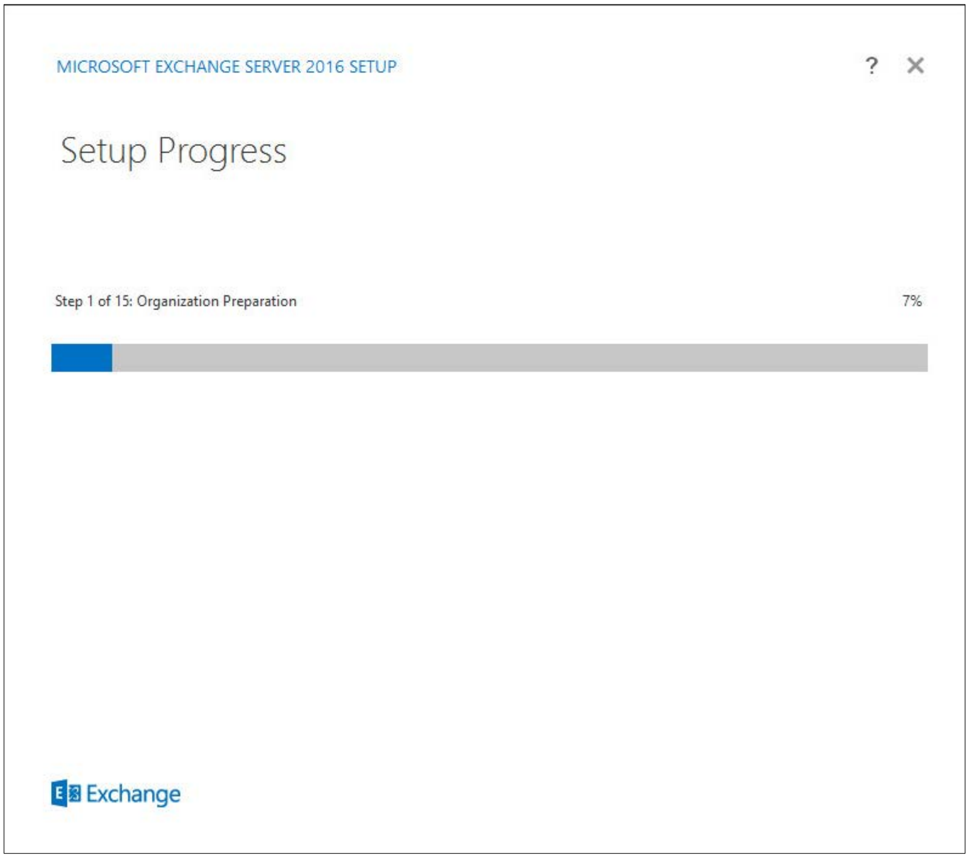
Readiness Checks

The computer will be checked to verify that setup can continue.

Prerequisite Analysis 100%

Warning:
Setup can't detect a Send connector with an address space of '*'. Mail flow to the Internet may not work properly.
For more information, visit: http://technet.microsoft.com/library(EXCHG.160)/ms.exch.setupreadiness.NoConnectorToStar.aspx

25. Click **Install**.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Setup Progress

Step 1 of 15: Organization Preparation 7%

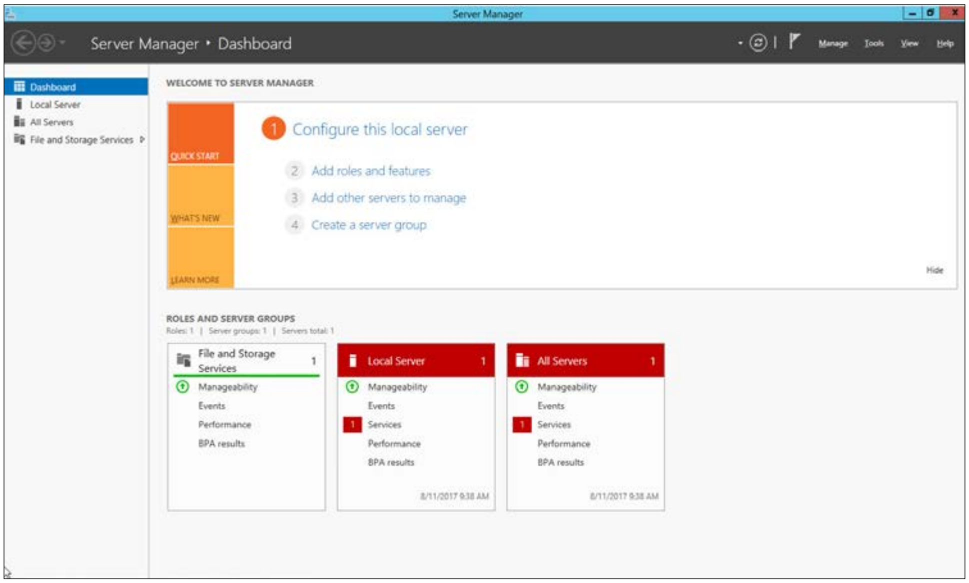
26. Wait for setup to complete.

2.3 SharePoint Server

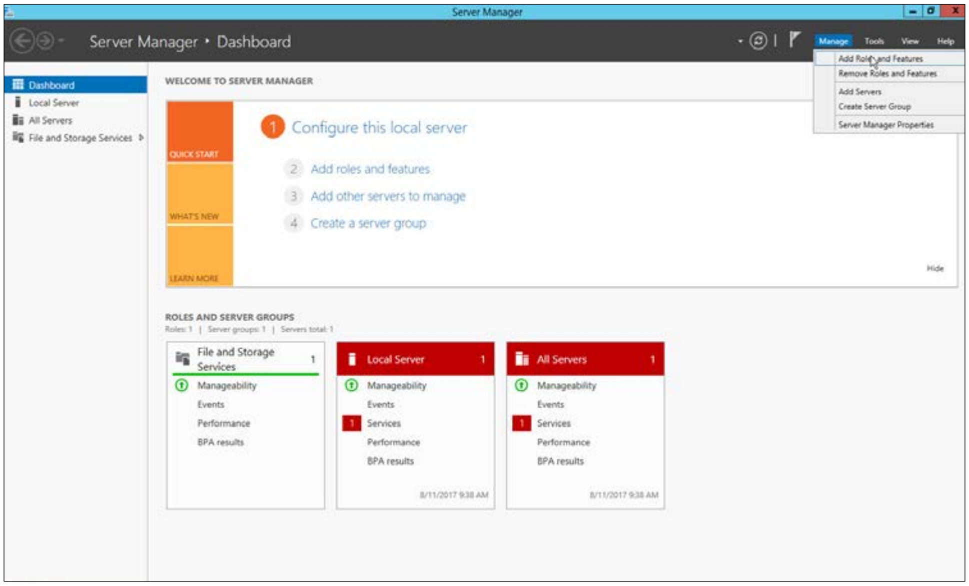
As part of our enterprise emulation, we include a Microsoft SharePoint server. This section covers the installation and configuration process used to set up SharePoint on a Windows Server 2012 R2 machine.

2.3.1 Install Roles and Features

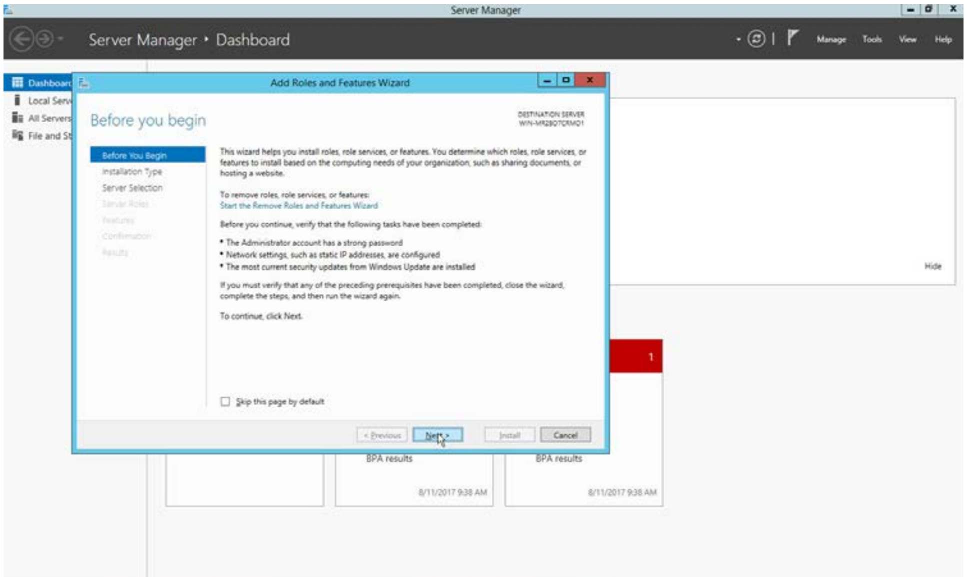
1. Open **Server Manager**.



2. Click **Manage**.



3. Click **Add Roles and Features**.



Before you begin

DESTINATION SERVER
WIN-MR2BOTCRMO1

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

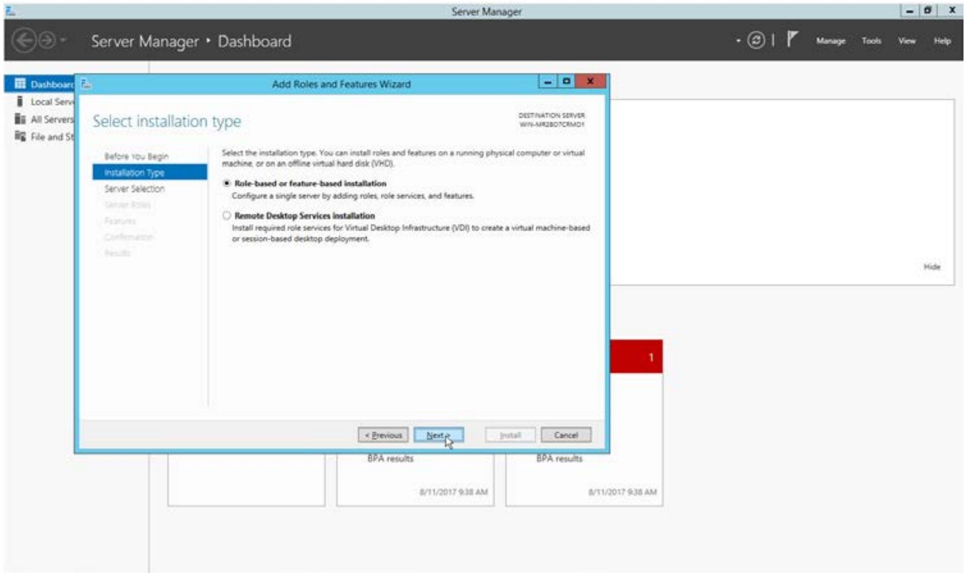
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

4. Click **Next**.
5. Choose **Role-based or feature-based installation**.



Select installation type

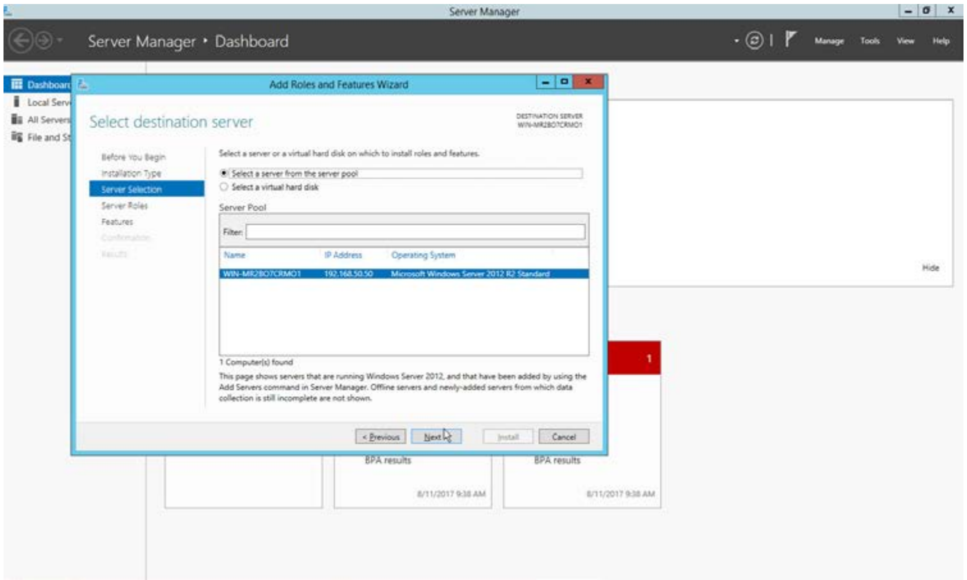
DESTINATION SERVER
WIN-MR2BO7CRMO1

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

6. Click **Next**.
7. Choose **Select a server from the server pool**.
8. Choose the SharePoint server from the list.



Select destination server

DESTINATION SERVER
WIN-MR2BO7CRMO1

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

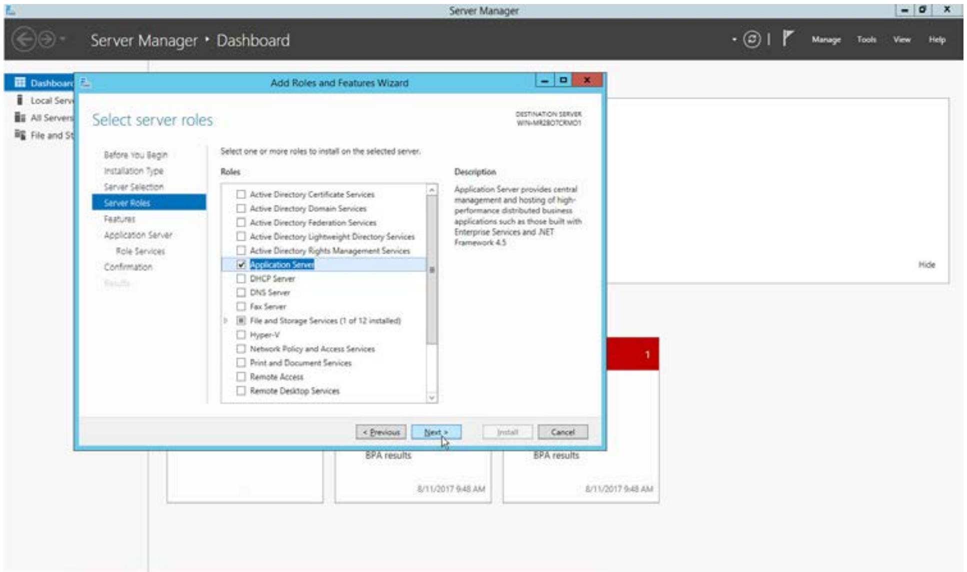
Filter:

Name	IP Address	Operating System
WIN-MR2BO7CRMO1	192.168.50.50	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.

9. Click **Next**.
10. Check **Application Server Role**.



Select server roles

DESTINATION SERVER
WIN-MR2BO7CRMO1

Select one or more roles to install on the selected server.

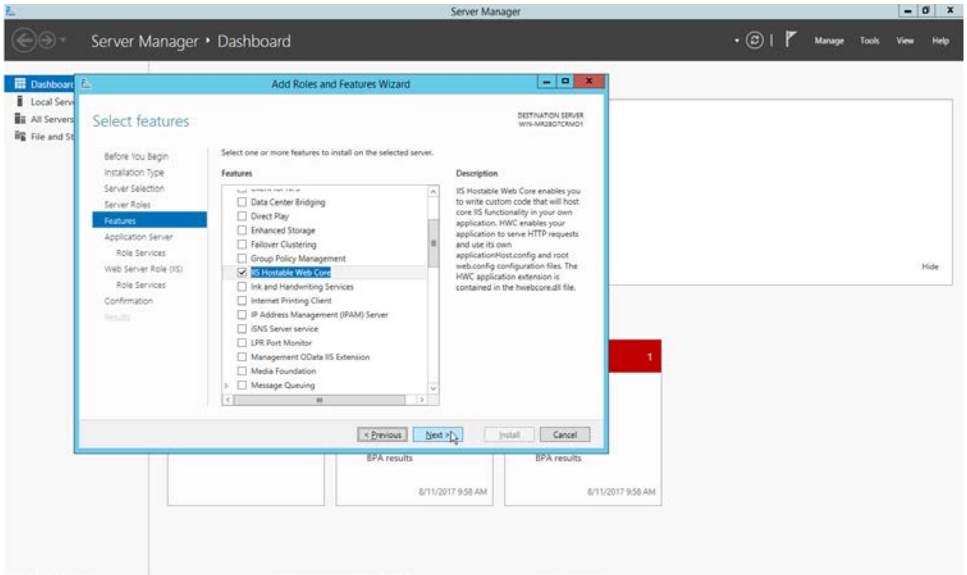
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☑ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Application Server provides central management and hosting of high-performance distributed business applications such as those built with Enterprise Services and .NET Framework 4.5

11. Click **Next**.
12. Check **IIS Hostable Web Core**.



Select features

DESTINATION SERVER
WIN-MR2BOTCRMO1

Select one or more features to install on the selected server.

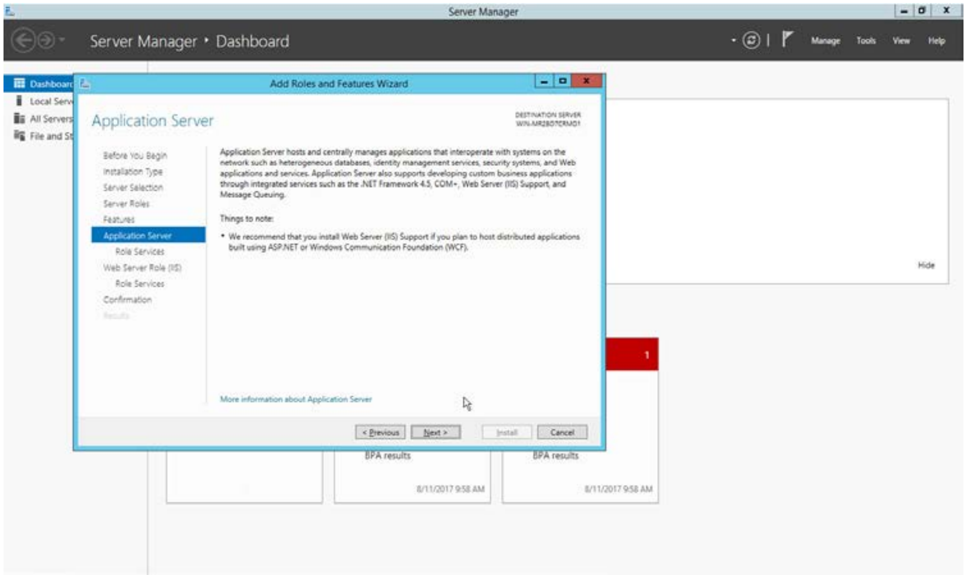
Features

- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☐ Group Policy Management
- ☑ IIS Hostable Web Core
- ☐ Ink and Handwriting Services
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ iSNS Server service
- ☐ LPR Port Monitor
- ☐ Management OData IIS Extension
- ☐ Media Foundation
- ☐ Message Queuing

Description

IIS Hostable Web Core enables you to write custom code that will host core IIS functionality in your own application. HWC enables your application to serve HTTP requests and use its own applicationHost.config and root web.config configuration files. The HWC application extension is contained in the hwebcore.dll file.

13. Click **Next**.



Application Server

DESTINATION SERVER
WIN-MR2BOTCRMO1

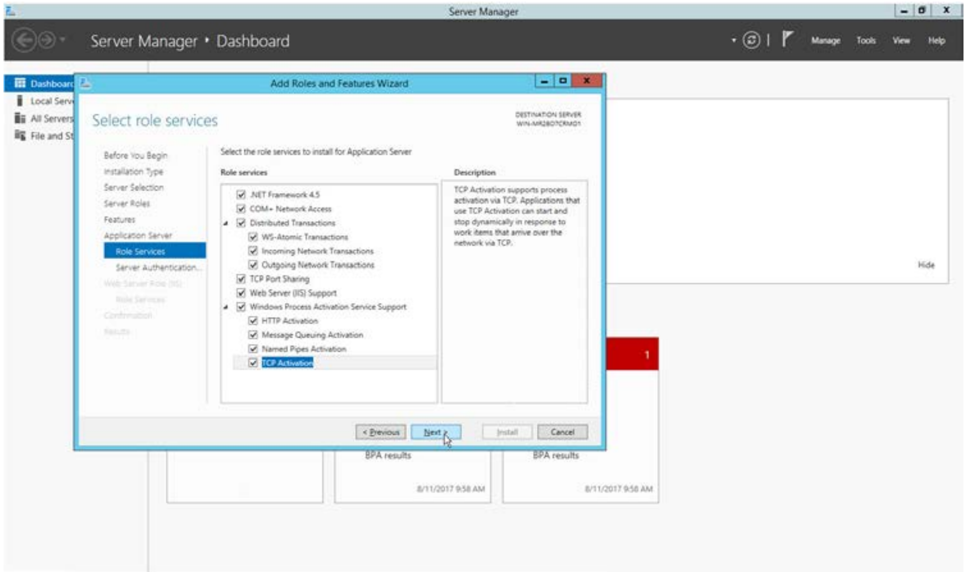
Application Server hosts and centrally manages applications that interoperate with systems on the network such as heterogeneous databases, identity management services, security systems, and Web applications and services. Application Server also supports developing custom business applications through integrated services such as the .NET Framework 4.5, COM+, Web Server (IIS) Support, and Message Queuing.

Things to note:

- We recommend that you install Web Server (IIS) Support if you plan to host distributed applications built using ASP.NET or Windows Communication Foundation (WCF).

More information about Application Server

14. Click **Next**.
15. Check all boxes under **Application Server Role Services**.



Select role services

DESTINATION SERVER
WIN-MR2BO7CRMO1

Select the role services to install for Application Server

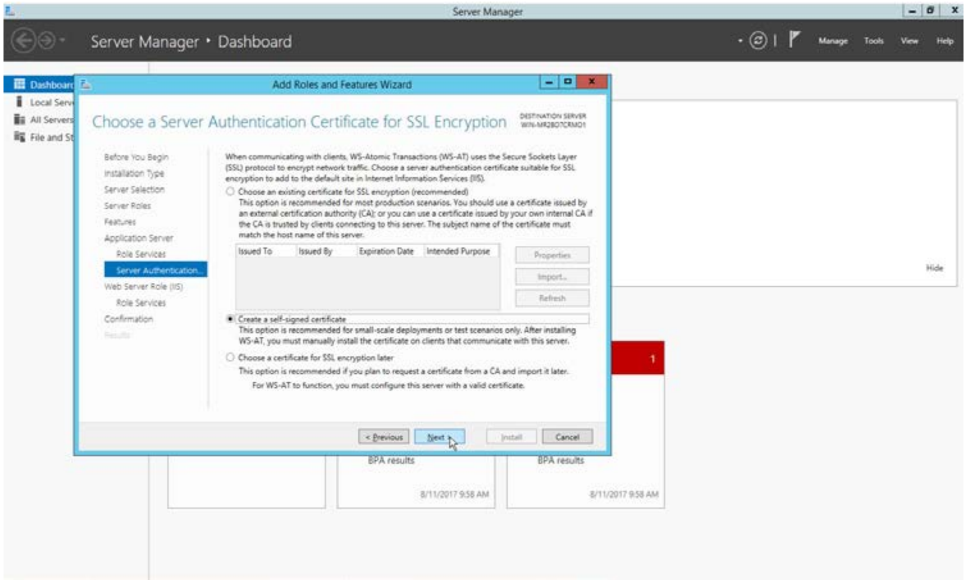
Role services

- ☑ .NET Framework 4.5
- ☑ COM+ Network Access
- ☑ Distributed Transactions
  - ☑ WS-Atomic Transactions
  - ☑ Incoming Network Transactions
  - ☑ Outgoing Network Transactions
- ☑ TCP Port Sharing
- ☑ Web Server (IIS) Support
- ☑ Windows Process Activation Service Support
  - ☑ HTTP Activation
  - ☑ Message Queuing Activation
  - ☑ Named Pipes Activation
  - ☑ TCP Activation

Description

TCP Activation supports process activation via TCP. Applications that use TCP Activation can start and stop dynamically in response to work items that arrive over the network via TCP.

16. Click **Next**.
17. Choose **Create a self-signed certificate**.



Choose a Server Authentication Certificate for SSL Encryption

DESTINATION SERVER
WIN-MR2BO7CRMO1

When communicating with clients, WS-Atomic Transactions (WS-AT) uses the Secure Sockets Layer (SSL) protocol to encrypt network traffic. Choose a server authentication certificate suitable for SSL encryption to add to the default site in Internet Information Services (IIS).

○ Choose an existing certificate for SSL encryption (recommended)
This option is recommended for most production scenarios. You should use a certificate issued by an external certification authority (CA); or you can use a certificate issued by your own internal CA if the CA is trusted by clients connecting to this server. The subject name of the certificate must match the host name of this server.

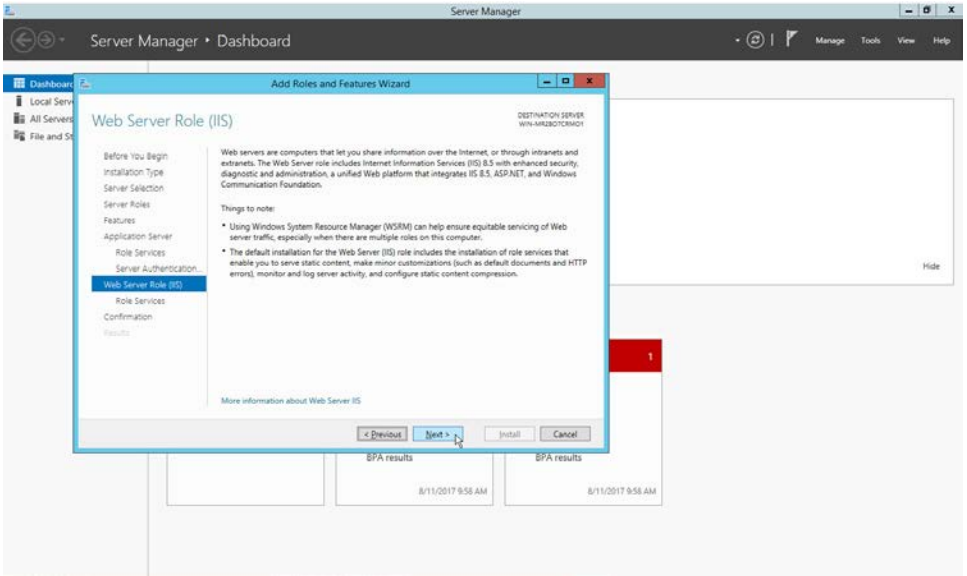
Issued To	Issued By	Expiration Date	Intended Purpose

● Create a self-signed certificate
This option is recommended for small-scale deployments or test scenarios only. After installing WS-AT, you must manually install the certificate on clients that communicate with this server.

○ Choose a certificate for SSL encryption later
This option is recommended if you plan to request a certificate from a CA and import it later.

For WS-AT to function, you must configure this server with a valid certificate.

18. Click **Next**.



Web Server Role (IIS)

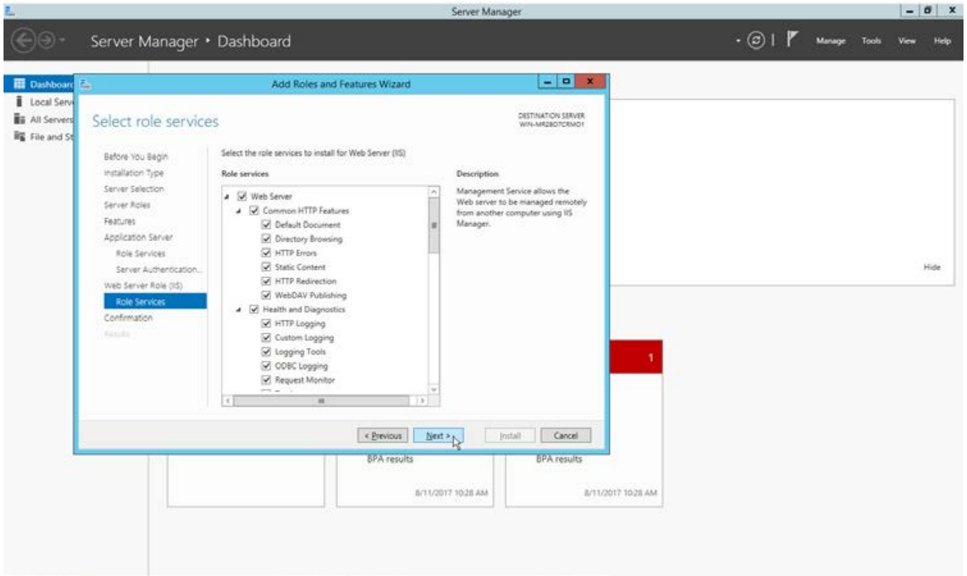
DESTINATION SERVER
WIN-MR2BOTCRMO1

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 8.5 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 8.5, ASP.NET, and Windows Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

19. Click **Next**.
20. Check all boxes under **Web Server (IIS) Role Services**.



Select role services

DESTINATION SERVER
WIN-MR2BOTCRMO1

Select the role services to install for Web Server (IIS)

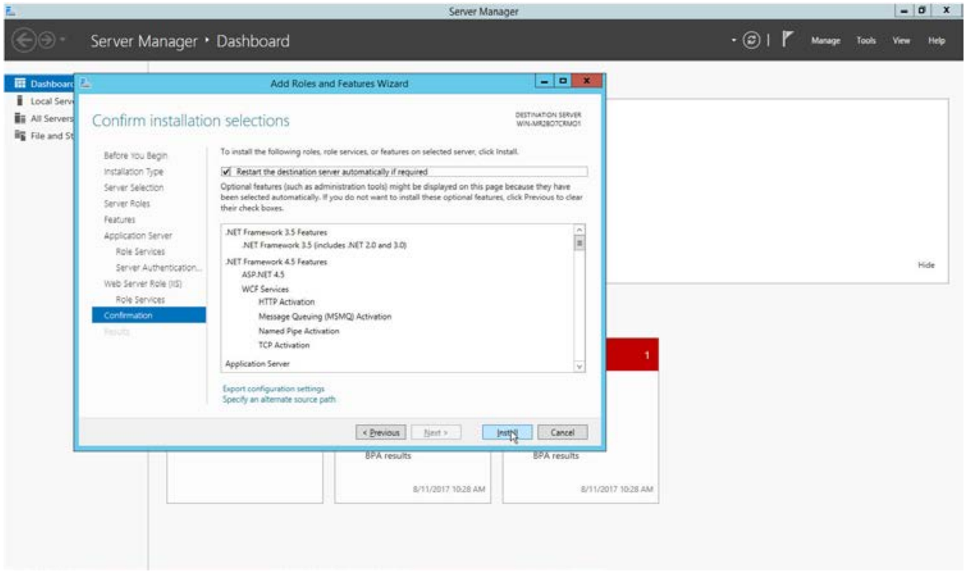
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - ☑ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Custom Logging
    - ☑ Logging Tools
    - ☑ ODBC Logging
    - ☑ Request Monitor

Description

Management Service allows the Web server to be managed remotely from another computer using IIS Manager.

21. Click **Next**.
22. Check **Restart the destination server automatically if required**.



To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

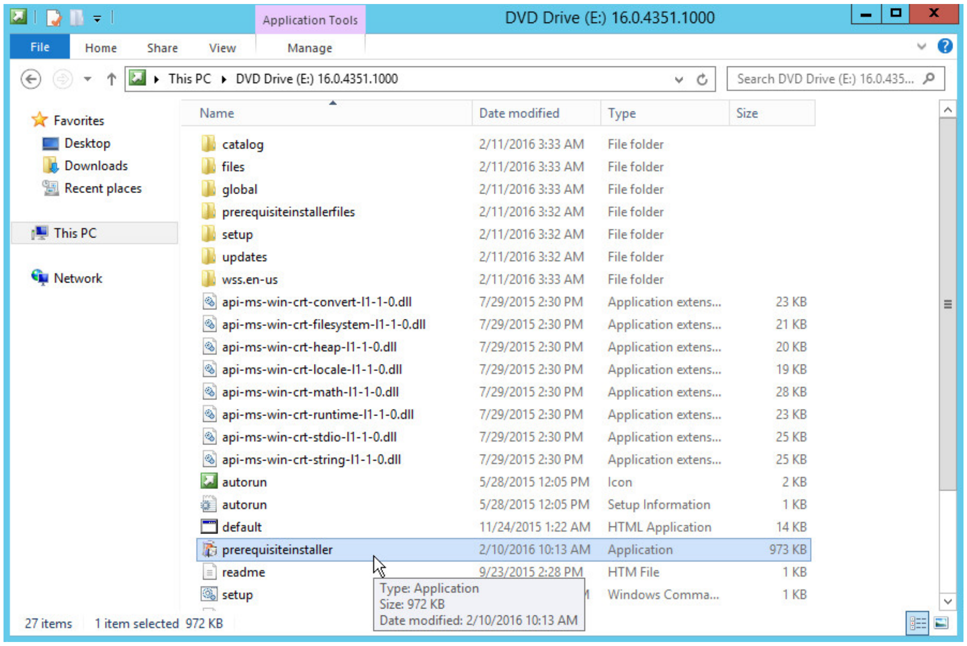
```
.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.5 Features
    ASP.NET 4.5
    WCF Services
        HTTP Activation
        Message Queuing (MSMQ) Activation
        Named Pipe Activation
        TCP Activation
Application Server
```

Export configuration settings
Specify an alternate source path

23. Click **Install**.
24. The server may automatically restart.
25. Right click the **.ISO file** for **SharePoint Server**.
26. Choose **Mount**.

2.3.2 Install SharePoint

1. Navigate to the main directory of the ISO.

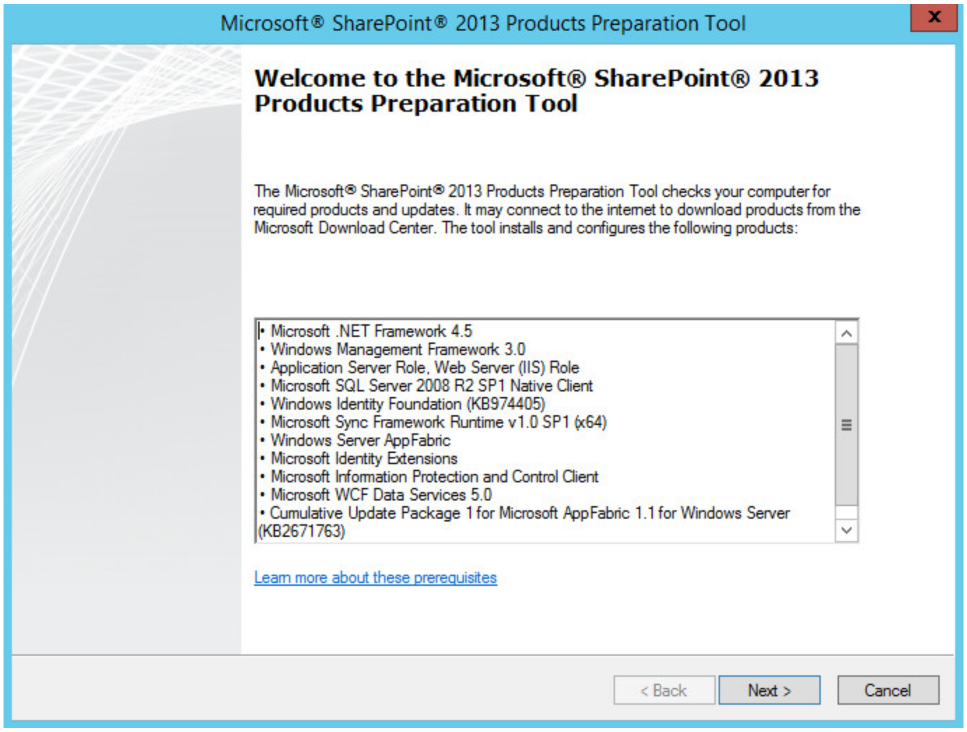

Application Tools
DVD Drive (E:) 16.0.4351.1000
File
Home
Share
View
Manage
This PC ‣ DVD Drive (E:) 16.0.4351.1000
Search DVD Drive (E:) 16.0.435...
Favorites
Desktop
Downloads
Recent places
This PC
Network

Name	Date modified	Type	Size
catalog	2/11/2016 3:33 AM	File folder	
files	2/11/2016 3:33 AM	File folder	
global	2/11/2016 3:33 AM	File folder	
prerequisiteinstallerfiles	2/11/2016 3:32 AM	File folder	
setup	2/11/2016 3:32 AM	File folder	
updates	2/11/2016 3:32 AM	File folder	
wss.en-us	2/11/2016 3:33 AM	File folder	
api-ms-win-crt-convert-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	23 KB
api-ms-win-crt-filesystem-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	21 KB
api-ms-win-crt-heap-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	20 KB
api-ms-win-crt-locale-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	19 KB
api-ms-win-crt-math-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	28 KB
api-ms-win-crt-runtime-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	23 KB
api-ms-win-crt-stdio-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	25 KB
api-ms-win-crt-string-l1-1-0.dll	7/29/2015 2:30 PM	Application extens...	25 KB
autorun	5/28/2015 12:05 PM	Icon	2 KB
autorun	5/28/2015 12:05 PM	Setup Information	1 KB
default	11/24/2015 1:22 AM	HTML Application	14 KB
prerequisiteinstaller	2/10/2016 10:13 AM	Application	973 KB
readme	9/23/2015 2:28 PM	HTM File	1 KB
setup		Windows Comma...	1 KB

Type: Application
Size: 972 KB
Date modified: 2/10/2016 10:13 AM

27 items 1 item selected 972 KB

2. Double click **pre-requisite installer**.



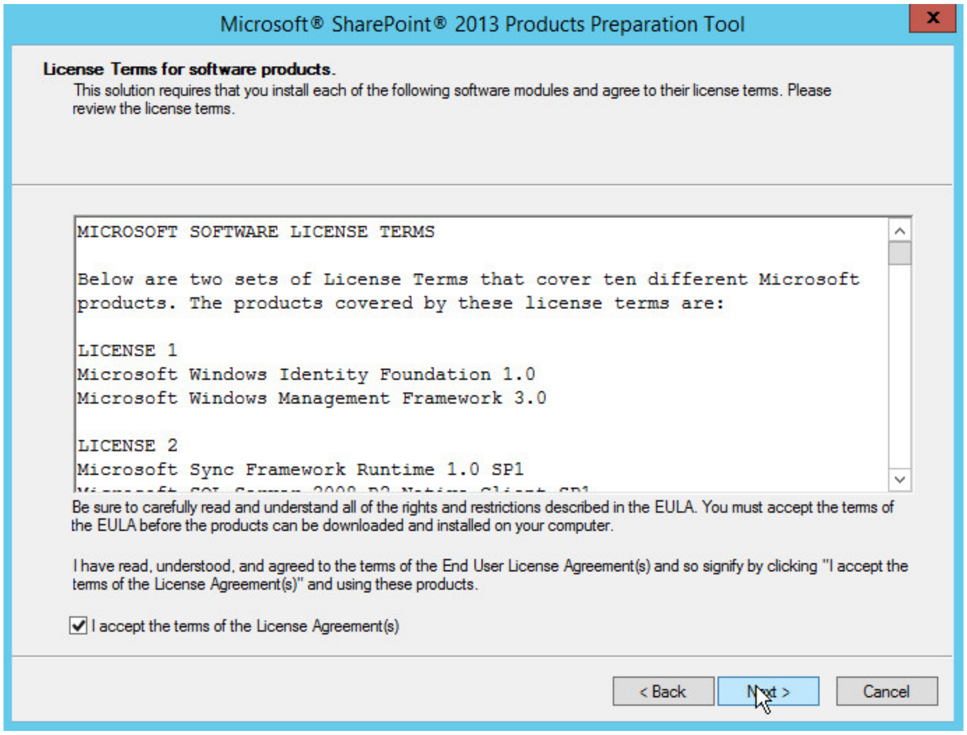
Microsoft® SharePoint® 2013 Products Preparation Tool

Welcome to the Microsoft® SharePoint® 2013 Products Preparation Tool

The Microsoft® SharePoint® 2013 Products Preparation Tool checks your computer for required products and updates. It may connect to the internet to download products from the Microsoft Download Center. The tool installs and configures the following products:

- Microsoft .NET Framework 4.5
- Windows Management Framework 3.0
- Application Server Role, Web Server (IIS) Role
- Microsoft SQL Server 2008 R2 SP1 Native Client
- Windows Identity Foundation (KB974405)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64)
- Windows Server AppFabric
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client
- Microsoft WCF Data Services 5.0
- Cumulative Update Package 1 for Microsoft AppFabric 1.1 for Windows Server (KB2671763)

3. Click **Next**.
4. Click **I accept the terms of the License agreement**.



License Terms for software products.

This solution requires that you install each of the following software modules and agree to their license terms. Please review the license terms.

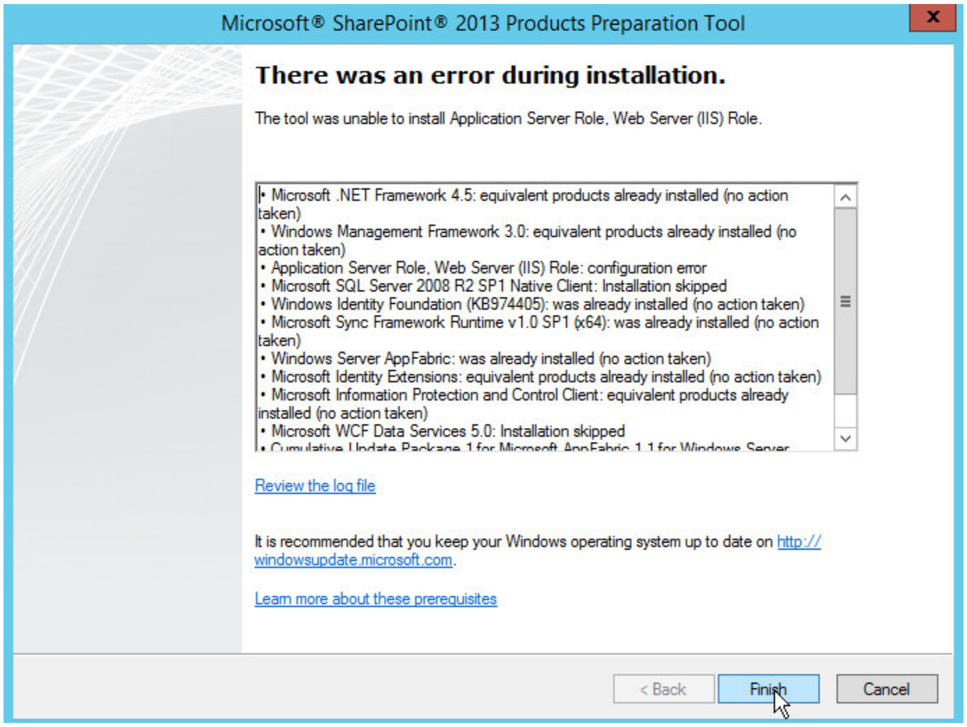
```
MICROSOFT SOFTWARE LICENSE TERMS

Below are two sets of License Terms that cover ten different Microsoft
products. The products covered by these license terms are:

LICENSE 1
Microsoft Windows Identity Foundation 1.0
Microsoft Windows Management Framework 3.0

LICENSE 2
Microsoft Sync Framework Runtime 1.0 SP1
```

Be sure to carefully read and understand all of the rights and restrictions described in the EULA. You must accept the terms of the EULA before the products can be downloaded and installed on your computer.

I have read, understood, and agreed to the terms of the End User License Agreement(s) and so signify by clicking "I accept the terms of the License Agreement(s)" and using these products.

☑ I accept the terms of the License Agreement(s)

5. Click **Next**.
6. Resolve any dependencies and repeat steps 2-5.



There was an error during installation.

The tool was unable to install Application Server Role, Web Server (IIS) Role.

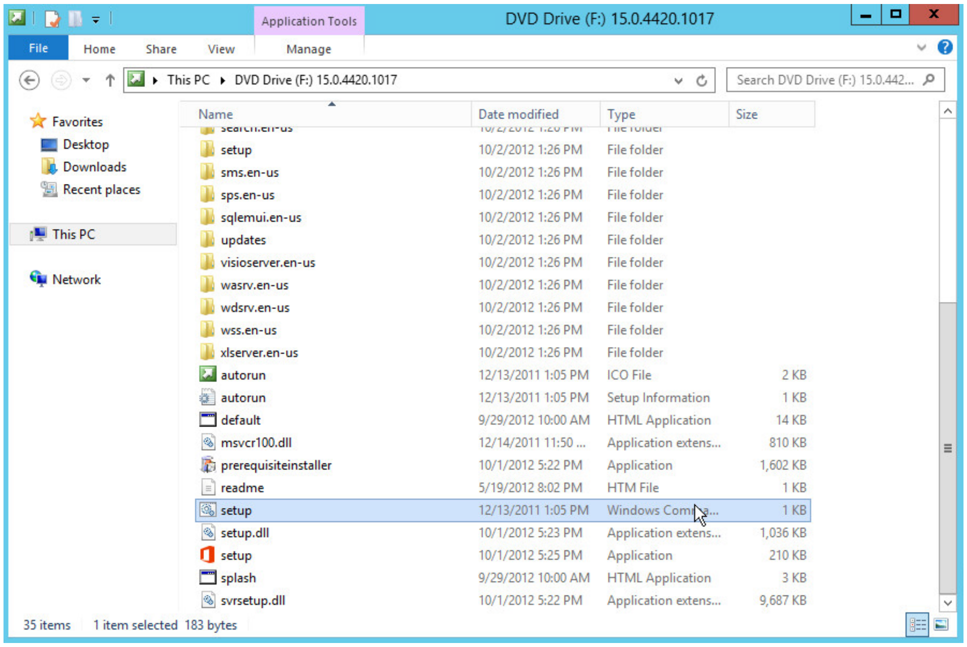
- Microsoft .NET Framework 4.5: equivalent products already installed (no action taken)
- Windows Management Framework 3.0: equivalent products already installed (no action taken)
- Application Server Role, Web Server (IIS) Role: configuration error
- Microsoft SQL Server 2008 R2 SP1 Native Client: Installation skipped
- Windows Identity Foundation (KB974405): was already installed (no action taken)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64): was already installed (no action taken)
- Windows Server AppFabric: was already installed (no action taken)
- Microsoft Identity Extensions: equivalent products already installed (no action taken)
- Microsoft Information Protection and Control Client: equivalent products already installed (no action taken)
- Microsoft WCF Data Services 5.0: Installation skipped

Review the log file

It is recommended that you keep your Windows operating system up to date on http://windowsupdate.microsoft.com.

Learn more about these prerequisites

7. After the successful installation, click **Finish**.
8. The server may automatically restart.
9. Remount the .**ISO file** for **SharePoint Server**.
10. Navigate to the main directory of the **.ISO file**.

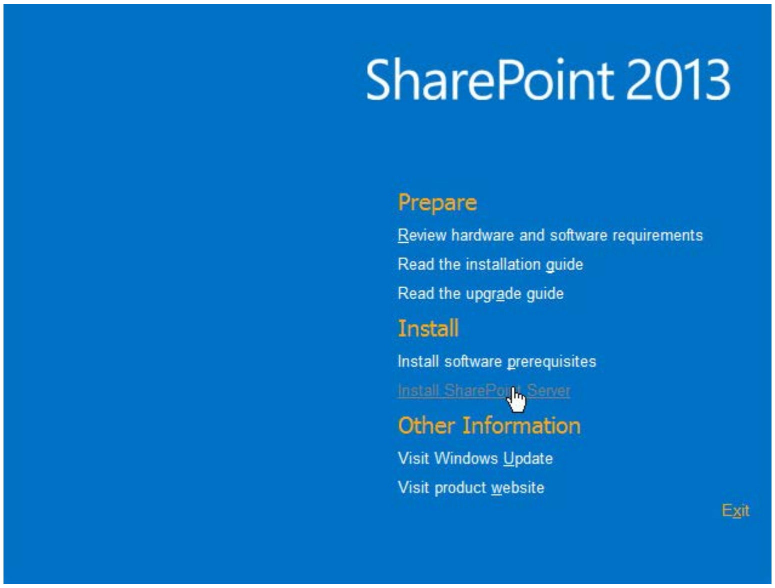


Application Tools
DVD Drive (F:) 15.0.4420.1017
File
Home
Share
View
Manage
This PC ▸ DVD Drive (F:) 15.0.4420.1017
Search DVD Drive (F:) 15.0.442...
Favorites
Desktop
Downloads
Recent places
This PC
Network

Name	Date modified	Type	Size
search.en-us	10/2/2012 1:26 PM	File folder	
setup	10/2/2012 1:26 PM	File folder	
sms.en-us	10/2/2012 1:26 PM	File folder	
sps.en-us	10/2/2012 1:26 PM	File folder	
sqlemui.en-us	10/2/2012 1:26 PM	File folder	
updates	10/2/2012 1:26 PM	File folder	
visioserver.en-us	10/2/2012 1:26 PM	File folder	
wasrv.en-us	10/2/2012 1:26 PM	File folder	
wdsrv.en-us	10/2/2012 1:26 PM	File folder	
wss.en-us	10/2/2012 1:26 PM	File folder	
xlserver.en-us	10/2/2012 1:26 PM	File folder	
autorun	12/13/2011 1:05 PM	ICO File	2 KB
autorun	12/13/2011 1:05 PM	Setup Information	1 KB
default	9/29/2012 10:00 AM	HTML Application	14 KB
msvcr100.dll	12/14/2011 11:50 ...	Application extens...	810 KB
prerequisiteinstaller	10/1/2012 5:22 PM	Application	1,602 KB
readme	5/19/2012 8:02 PM	HTM File	1 KB
setup	12/13/2011 1:05 PM	Windows Com...a...	1 KB
setup.dll	10/1/2012 5:23 PM	Application extens...	1,036 KB
setup	10/1/2012 5:25 PM	Application	210 KB
splash	9/29/2012 10:00 AM	HTML Application	3 KB
svrsetup.dll	10/1/2012 5:22 PM	Application extens...	9,687 KB

35 items 1 item selected 183 bytes

11. Double click the program called **setup**.



SharePoint 2013

Prepare

Review hardware and software requirements

Read the installation guide

Read the upgrade guide

Install

Install software prerequisites

Install SharePoint Server

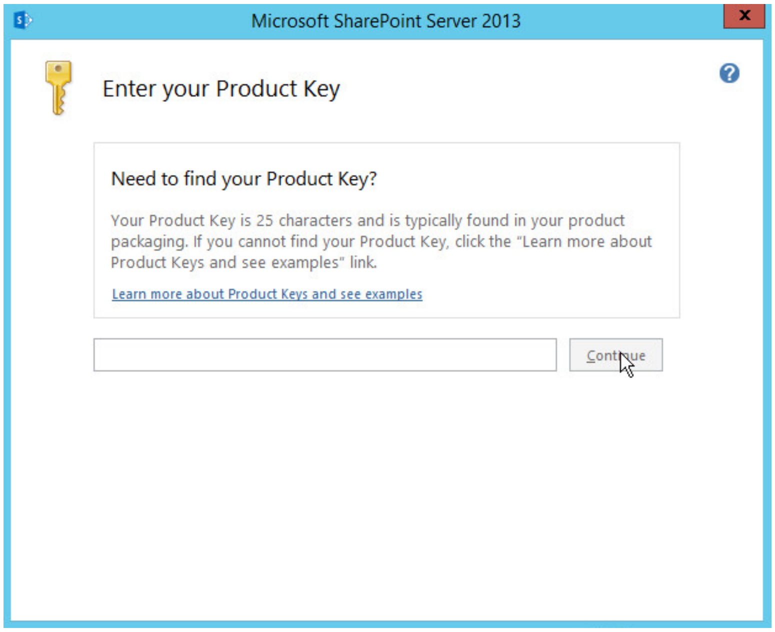
Other Information

Visit Windows Update

Visit product website

Exit

12. Click **Install SharePoint Server**.
13. Enter your product key when prompted.



Microsoft SharePoint Server 2013

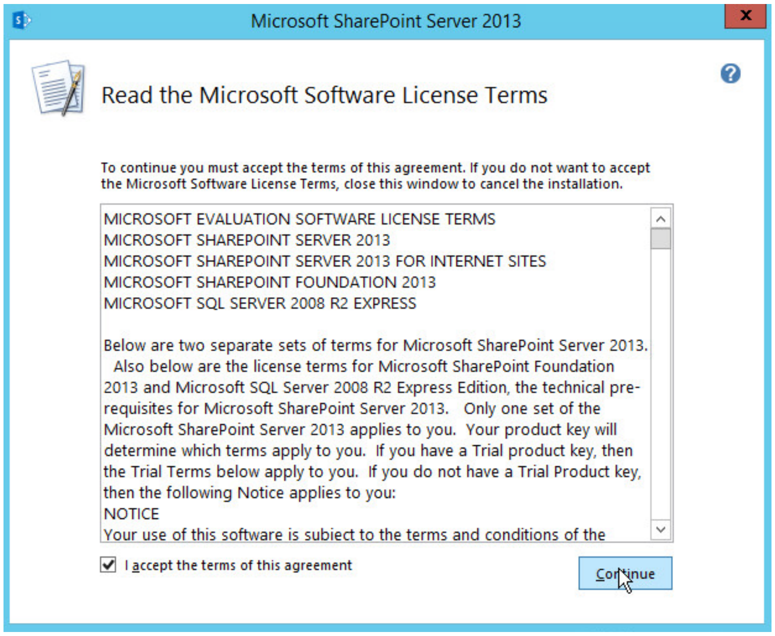
Enter your Product Key

Need to find your Product Key?

Your Product Key is 25 characters and is typically found in your product packaging. If you cannot find your Product Key, click the "Learn more about Product Keys and see examples" link.

Learn more about Product Keys and see examples
Continue

14. Click **Continue**.
15. Check **I accept the terms of this agreement**.



Read the Microsoft Software License Terms

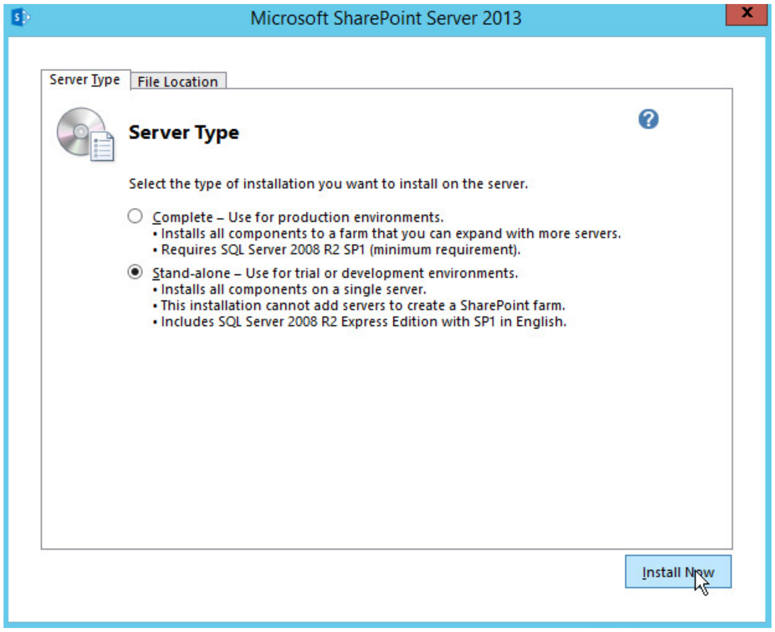
To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation.

MICROSOFT EVALUATION SOFTWARE LICENSE TERMS
MICROSOFT SHAREPOINT SERVER 2013
MICROSOFT SHAREPOINT SERVER 2013 FOR INTERNET SITES
MICROSOFT SHAREPOINT FOUNDATION 2013
MICROSOFT SQL SERVER 2008 R2 EXPRESS

Below are two separate sets of terms for Microsoft SharePoint Server 2013. Also below are the license terms for Microsoft SharePoint Foundation 2013 and Microsoft SQL Server 2008 R2 Express Edition, the technical pre-requisites for Microsoft SharePoint Server 2013. Only one set of the Microsoft SharePoint Server 2013 applies to you. Your product key will determine which terms apply to you. If you have a Trial product key, then the Trial Terms below apply to you. If you do not have a Trial Product key, then the following Notice applies to you:
NOTICE
Your use of this software is subject to the terms and conditions of the

☑ I accept the terms of this agreement

16. Click **Continue**.
17. Choose which **Server Type** fits your organization's purposes.



Microsoft SharePoint Server 2013

Server Type | File Location

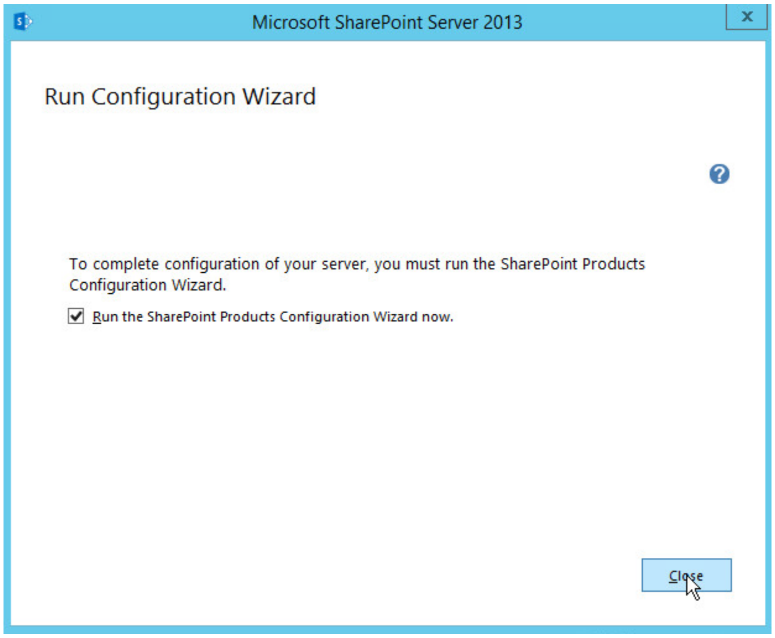
Server Type

Select the type of installation you want to install on the server.

○ Complete – Use for production environments.
• Installs all components to a farm that you can expand with more servers.
• Requires SQL Server 2008 R2 SP1 (minimum requirement).

● Stand-alone – Use for trial or development environments.
• Installs all components on a single server.
• This installation cannot add servers to create a SharePoint farm.
• Includes SQL Server 2008 R2 Express Edition with SP1 in English.

18. Click **Install Now**.
19. Wait for the installation to finish.
20. Check **Run the SharePoint Products Configuration Wizard now**.



Microsoft SharePoint Server 2013

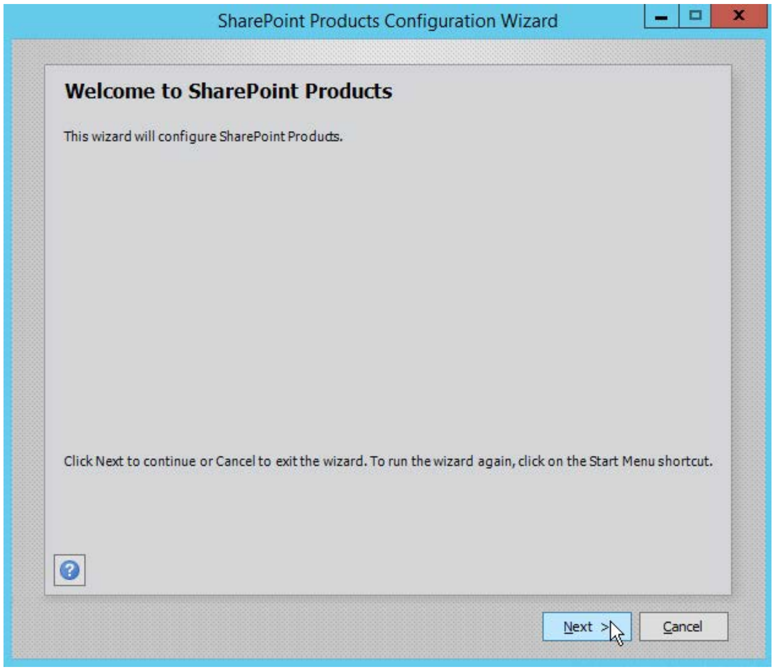
Run Configuration Wizard

To complete configuration of your server, you must run the SharePoint Products Configuration Wizard.

☑ Run the SharePoint Products Configuration Wizard now.

21. Click **Close**.

2.3.3 SharePoint Products Configuration Wizard

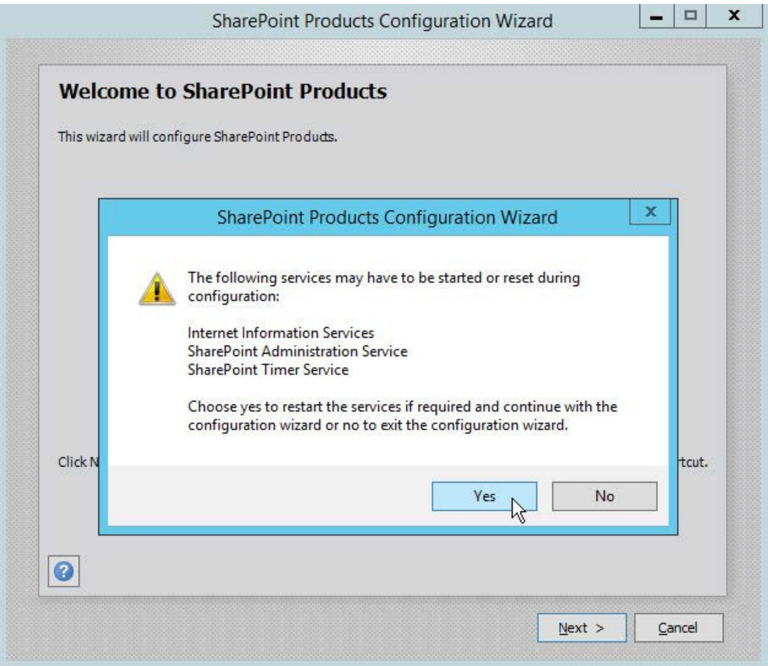


Welcome to SharePoint Products

This wizard will configure SharePoint Products.

Click Next to continue or Cancel to exit the wizard. To run the wizard again, click on the Start Menu shortcut.

1. Click **Next**.


SharePoint Products Configuration Wizard
Welcome to SharePoint Products
This wizard will configure SharePoint Products.
SharePoint Products Configuration Wizard

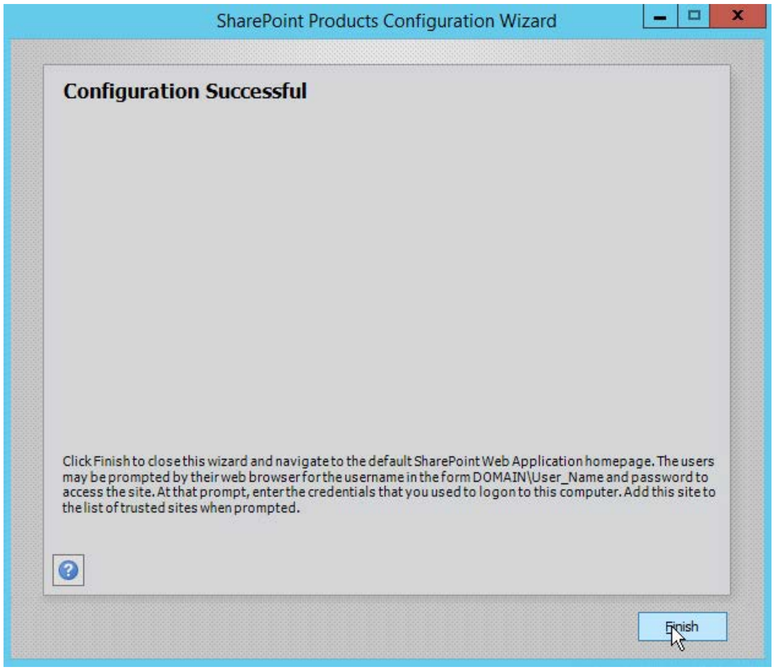
The following services may have to be started or reset during configuration:

Internet Information Services
SharePoint Administration Service
SharePoint Timer Service

Choose yes to restart the services if required and continue with the configuration wizard or no to exit the configuration wizard.

2. Click **Yes**.
3. Click **Next**.

4. Wait for the configuration to complete (it may take up to 30 minutes depending on your system).



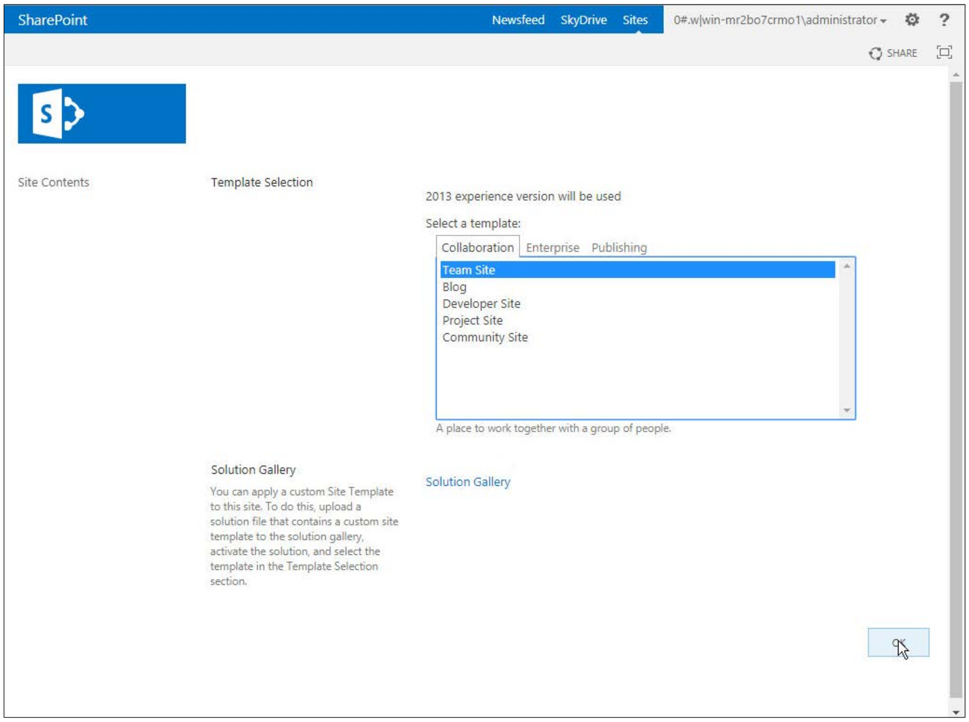
Configuration Successful

Click Finish to close this wizard and navigate to the default SharePoint Web Application homepage. The users may be prompted by their web browser for the username in the form DOMAIN\User_Name and password to access the site. At that prompt, enter the credentials that you used to logon to this computer. Add this site to the list of trusted sites when prompted.

5. Click **Finish**.

2.3.4 Configure SharePoint

1. **Open** a browser and navigate to *http://sharepoint* (replace **sharepoint** with the hostname or IP address of the SharePoint server)**.**
2. Choose the type of SharePoint template that fits your business needs. Example: Enterprise > Document Center.



Template Selection

2013 experience version will be used

Select a template:

Collaboration | Enterprise | Publishing

- Team Site
- Blog
- Developer Site
- Project Site
- Community Site

A place to work together with a group of people.

Solution Gallery

You can apply a custom Site Template to this site. To do this, upload a solution file that contains a custom site template to the solution gallery, activate the solution, and select the template in the Template Selection section.

Solution Gallery

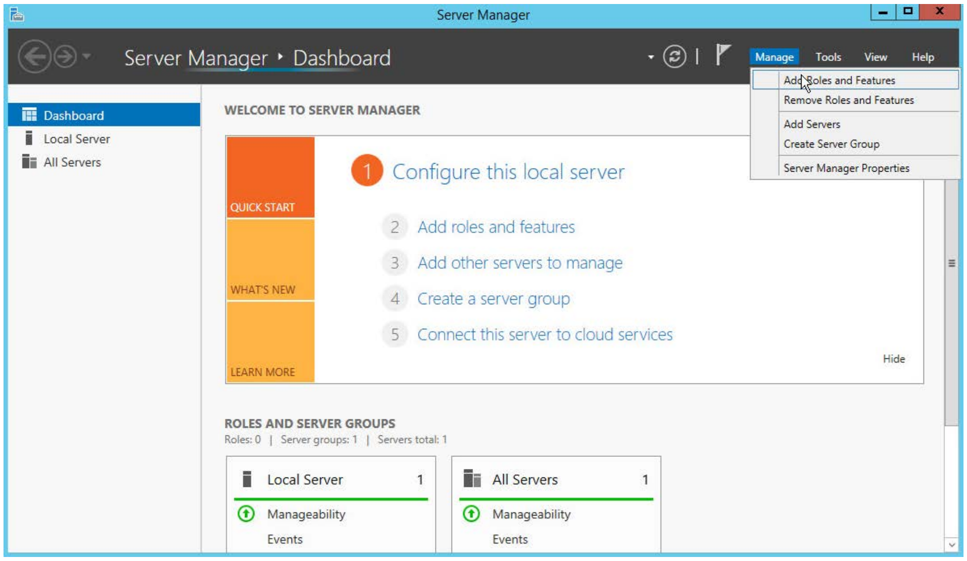
2.4 Windows Server Hyper-V Role

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.

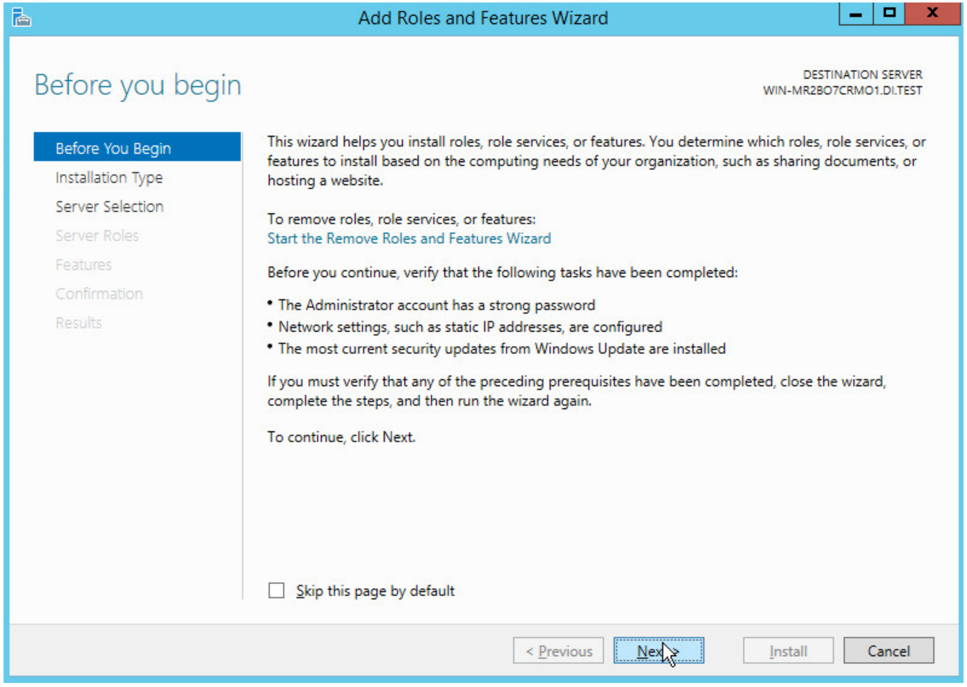
The instructions for enabling the Windows Server Hyper-V Role are retrieved from https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx and are replicated below for preservation and ease of use.

2.4.1 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.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

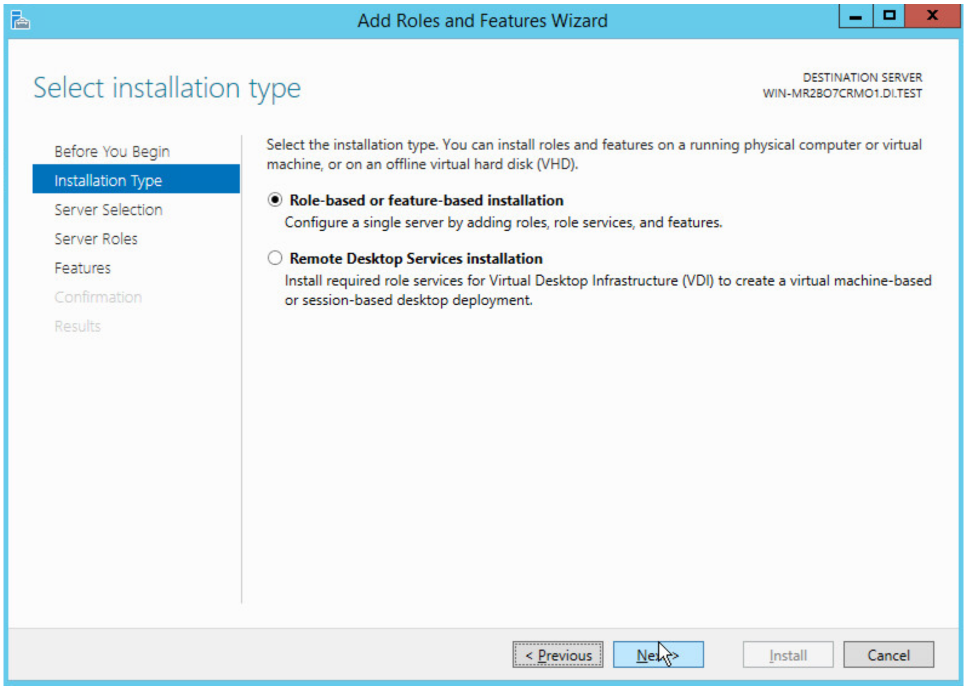
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

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



Select installation type

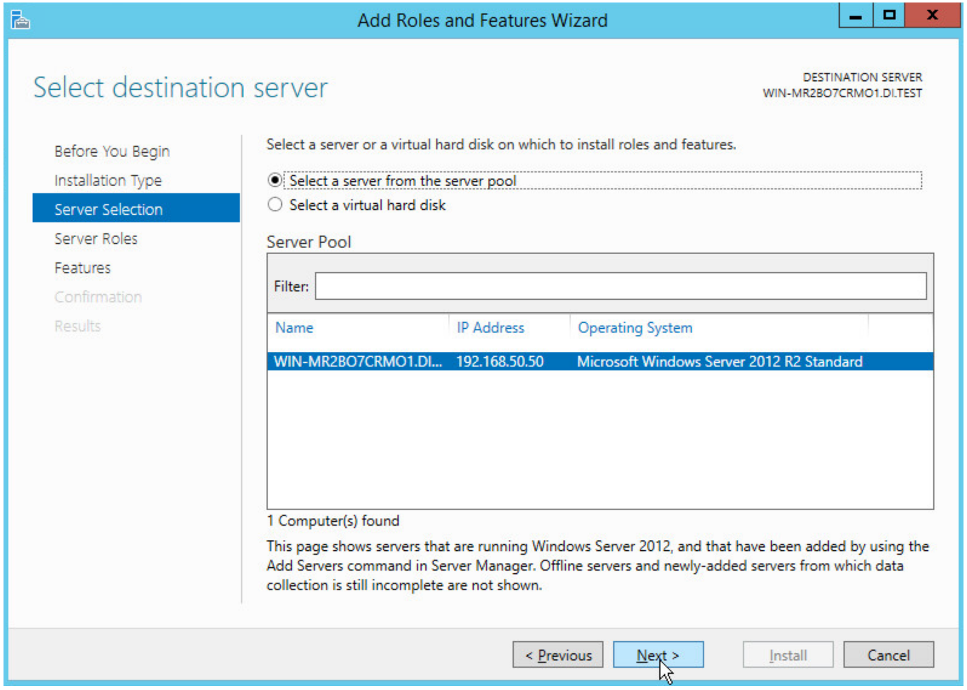
DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Select destination server

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

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:

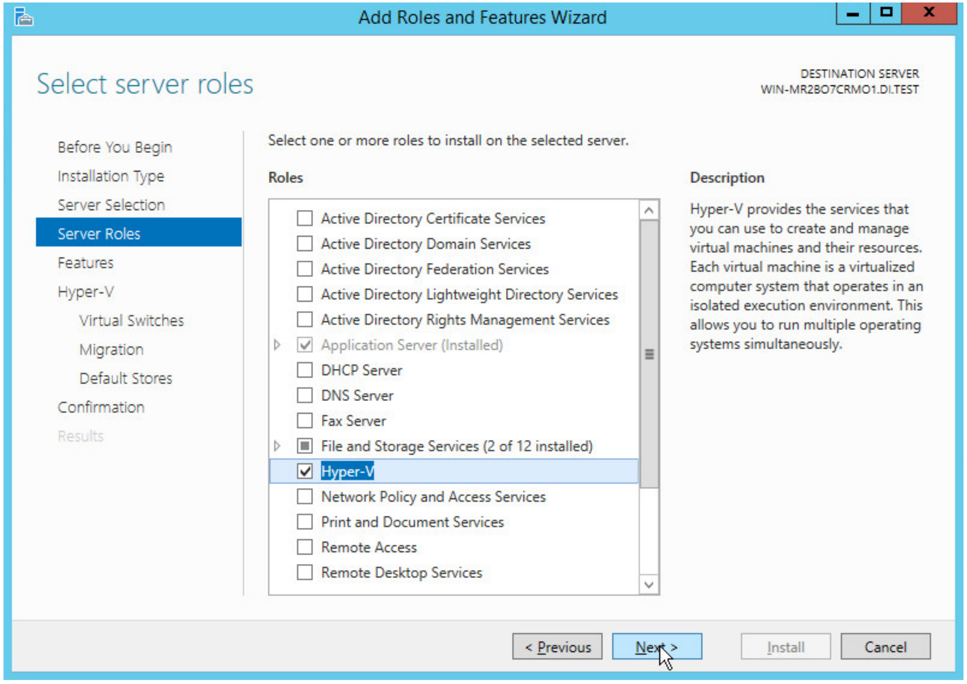
Name	IP Address	Operating System
WIN-MR2BO7CRMO1.DI...	192.168.50.50	Microsoft Windows Server 2012 R2 Standard

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.

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**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Hyper-V
  - Virtual Switches
  - Migration
  - Default Stores
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

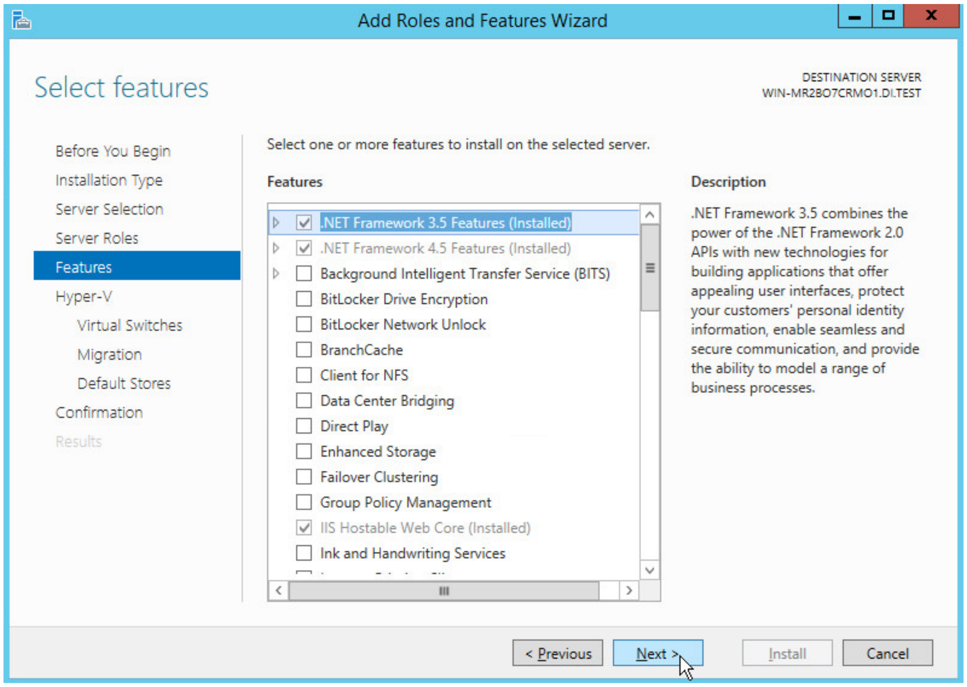
- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☑ Application Server (Installed)
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- ☑ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Hyper-V provides the services that you can use to create and manage virtual machines and their resources. Each virtual machine is a virtualized computer system that operates in an isolated execution environment. This allows you to run multiple operating systems simultaneously.

< Previous | Next > | Install | Cancel

10. Click **Next**.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Hyper-V
  - Virtual Switches
  - Migration
  - Default Stores
- Confirmation
- Results

Select one or more features to install on the selected server.

Features

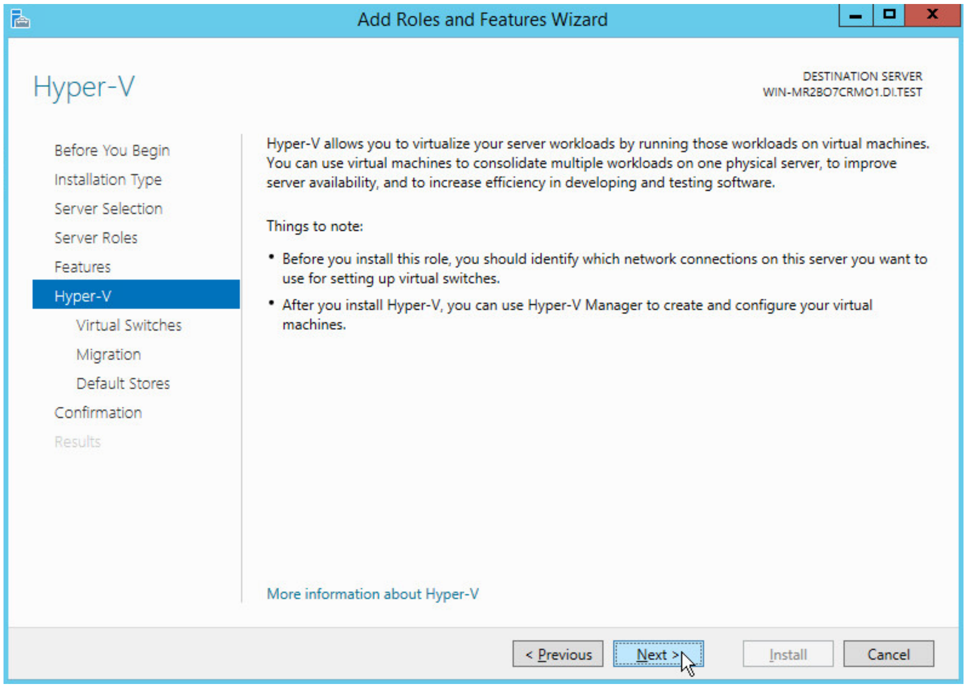
- ☑ .NET Framework 3.5 Features (Installed)
- ☑ .NET Framework 4.5 Features (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☐ Group Policy Management
- ☑ IIS Hostable Web Core (Installed)
- ☐ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous | Next > | Install | Cancel

11. Click **Next**.



Hyper-V

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

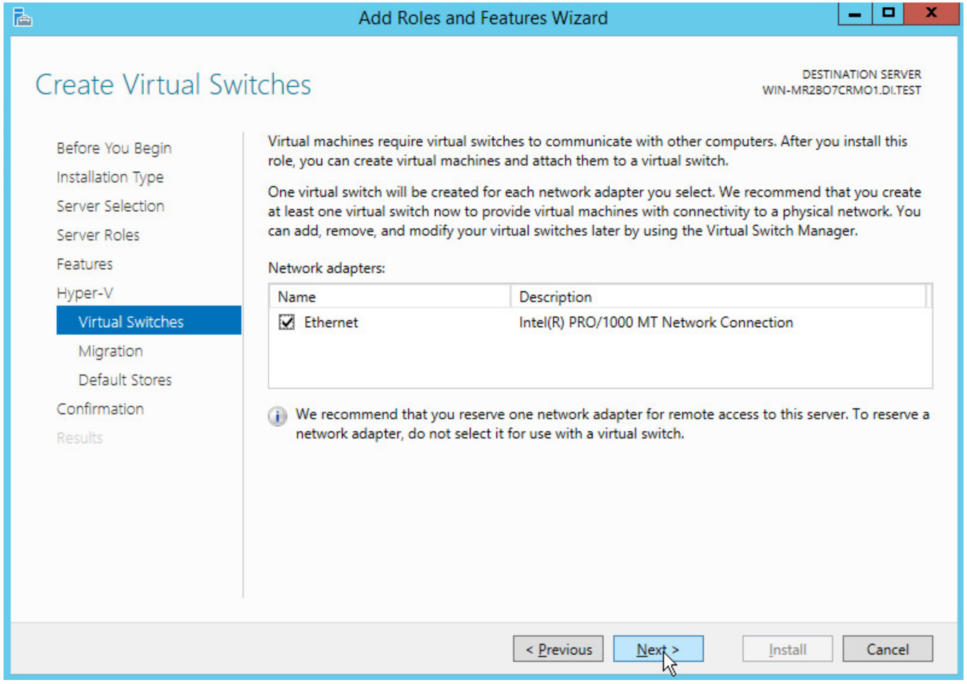
Hyper-V allows you to virtualize your server workloads by running those workloads on virtual machines. You can use virtual machines to consolidate multiple workloads on one physical server, to improve server availability, and to increase efficiency in developing and testing software.

Things to note:

- Before you install this role, you should identify which network connections on this server you want to use for setting up virtual switches.
- After you install Hyper-V, you can use Hyper-V Manager to create and configure your virtual machines.

More information about Hyper-V

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



Create Virtual Switches

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Virtual machines require virtual switches to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual switch.

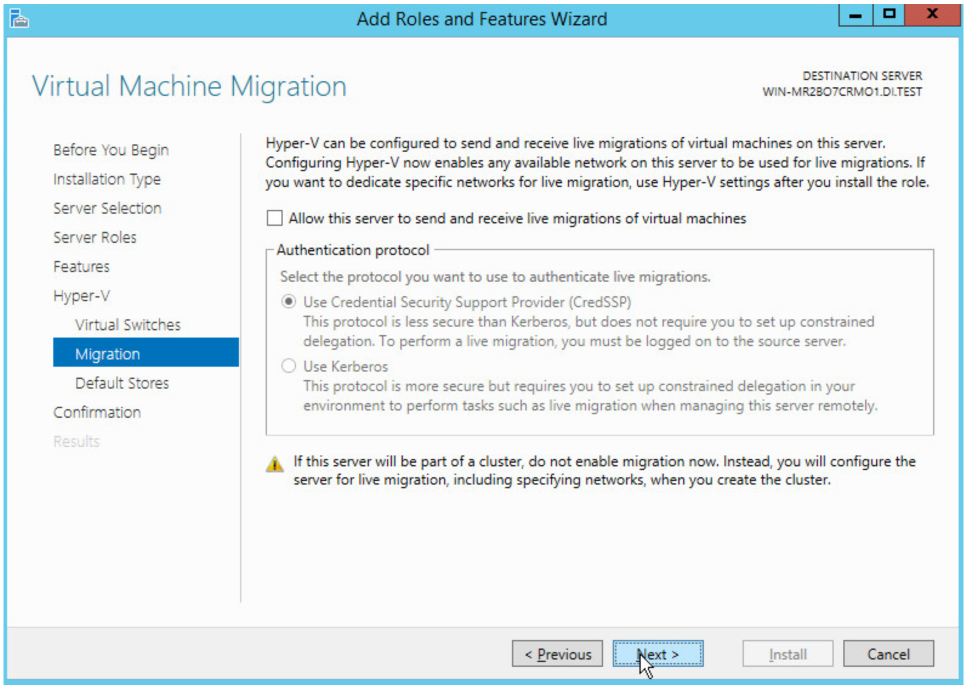
One virtual switch will be created for each network adapter you select. We recommend that you create at least one virtual switch now to provide virtual machines with connectivity to a physical network. You can add, remove, and modify your virtual switches later by using the Virtual Switch Manager.

Network adapters:

Name	Description
☑ Ethernet	Intel(R) PRO/1000 MT Network Connection

We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual switch.

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



Virtual Machine Migration

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migrations. If you want to dedicate specific networks for live migration, use Hyper-V settings after you install the role.

□ Allow this server to send and receive live migrations of virtual machines

Authentication protocol

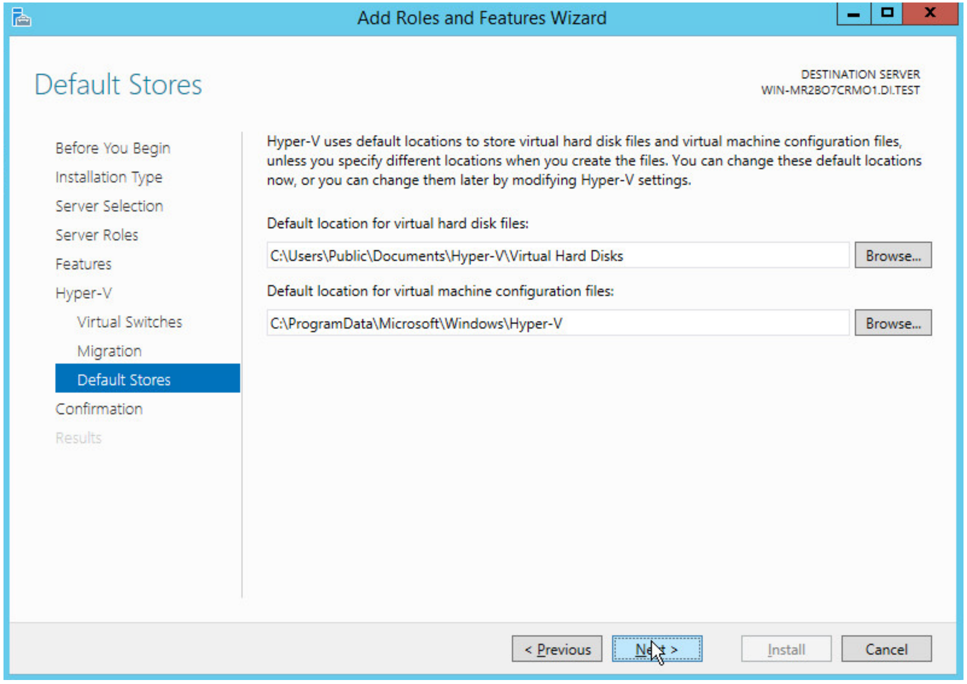
Select the protocol you want to use to authenticate live migrations.

● Use Credential Security Support Provider (CredSSP)
This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.

○ Use Kerberos
This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.

If this server will be part of a cluster, do not enable migration now. Instead, you will configure the server for live migration, including specifying networks, when you create the cluster.

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



Default Stores

DESTINATION SERVER
WIN-MR2BO7CRMO1.DI.TEST

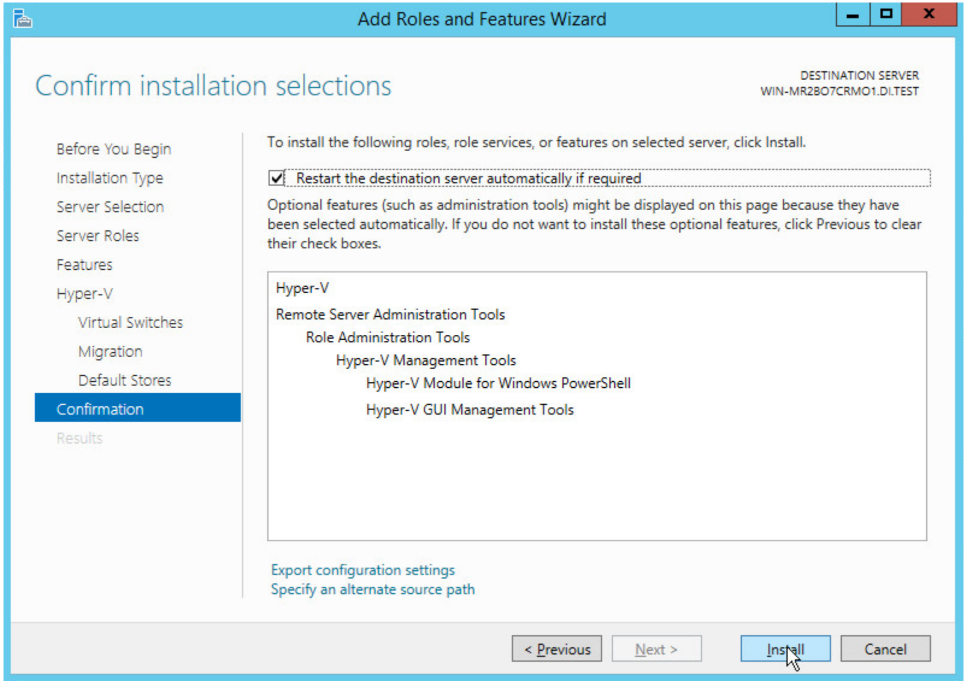
Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

Default location for virtual hard disk files:
C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:
C:\ProgramData\Microsoft\Windows\Hyper-V

18. Click **Next**.

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



To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Hyper-V
Remote Server Administration Tools
Role Administration Tools
Hyper-V Management Tools
Hyper-V Module for Windows PowerShell
Hyper-V GUI Management Tools

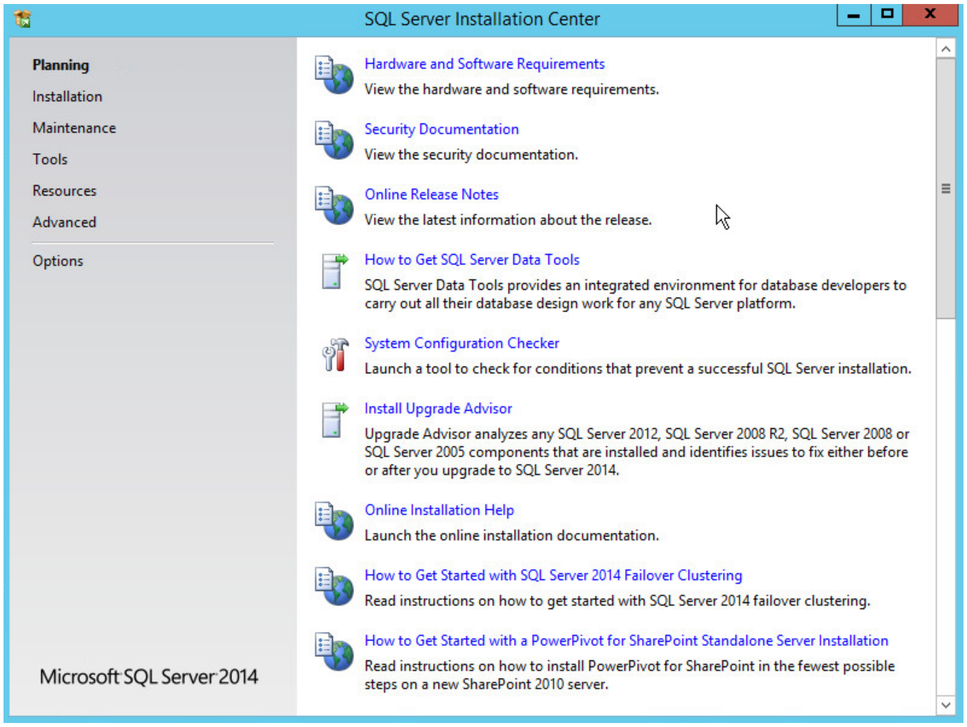
20. Click **Install**.
21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

2.5 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.

2.5.1 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.**



Hardware and Software Requirements
View the hardware and software requirements.

Security Documentation
View the security documentation.

Online Release Notes
View the latest information about the release.

How to Get SQL Server Data Tools
SQL Server Data Tools provides an integrated environment for database developers to carry out all their database design work for any SQL Server platform.

System Configuration Checker
Launch a tool to check for conditions that prevent a successful SQL Server installation.

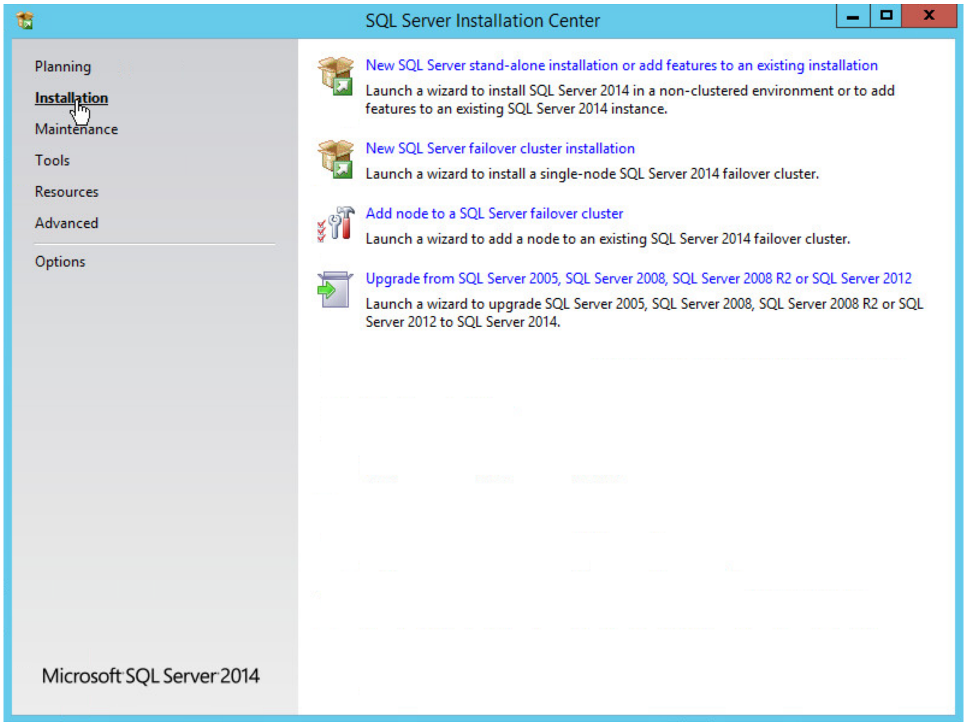
Install Upgrade Advisor
Upgrade Advisor analyzes any SQL Server 2012, SQL Server 2008 R2, SQL Server 2008 or SQL Server 2005 components that are installed and identifies issues to fix either before or after you upgrade to SQL Server 2014.

Online Installation Help
Launch the online installation documentation.

How to Get Started with SQL Server 2014 Failover Clustering
Read instructions on how to get started with SQL Server 2014 failover clustering.

How to Get Started with a PowerPivot for SharePoint Standalone Server Installation
Read instructions on how to install PowerPivot for SharePoint in the fewest possible steps on a new SharePoint 2010 server.

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



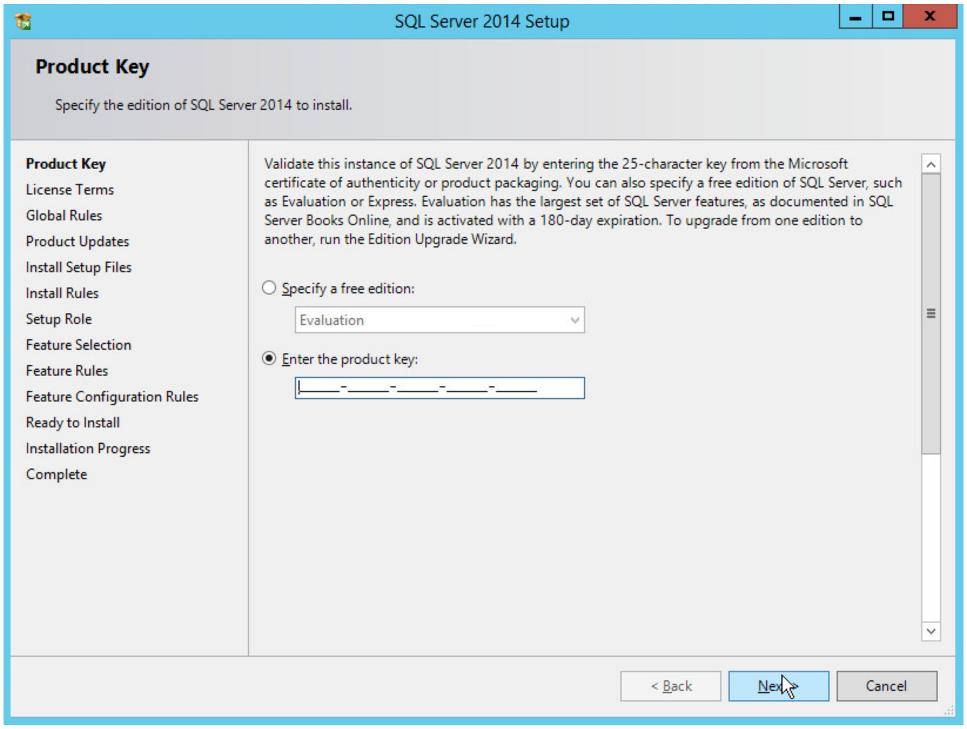
New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance.

New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2014 failover cluster.

Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2014 failover cluster.

Upgrade from SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012
Launch a wizard to upgrade SQL Server 2005, SQL Server 2008, SQL Server 2008 R2 or SQL Server 2012 to SQL Server 2014.

4. Select **New SQL Server stand-alone installation or add features to an existing installation**. This will launch the SQL Server 2014 setup.



Product Key

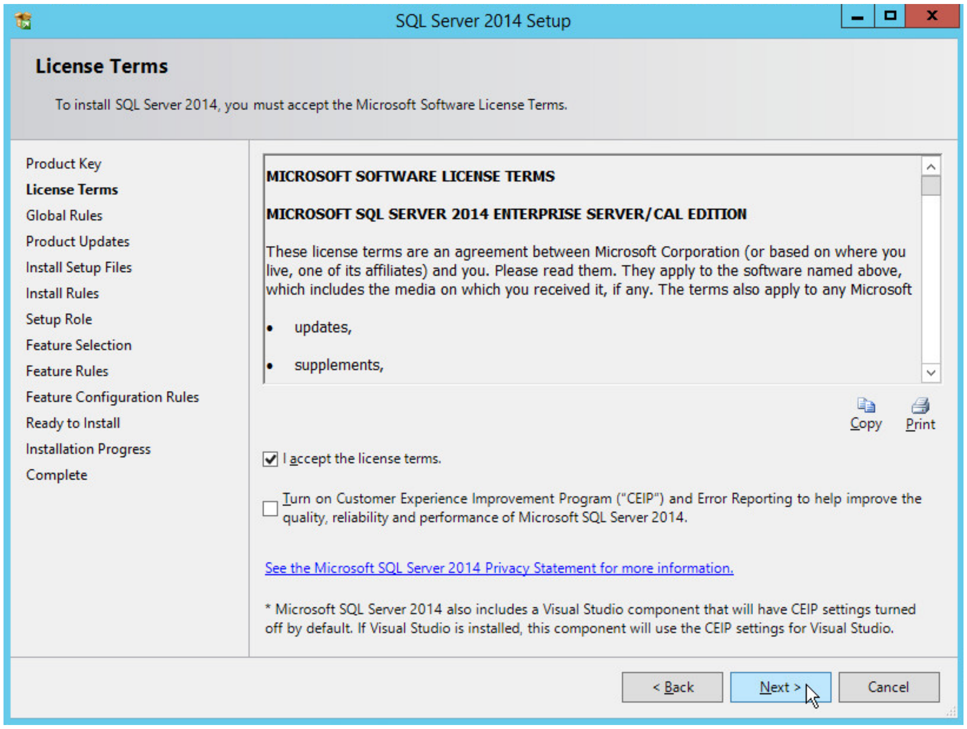
Specify the edition of SQL Server 2014 to install.

Validate this instance of SQL Server 2014 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server, such as Evaluation or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. To upgrade from one edition to another, run the Edition Upgrade Wizard.

○ Specify a free edition: Evaluation

● Enter the product key: _____-_____-_____-_____-_____

5. In the **Product Key** section, enter your product key.
6. Click **Next**.



License Terms

To install SQL Server 2014, you must accept the Microsoft Software License Terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2014 ENTERPRISE SERVER/CAL EDITION

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

- updates,
- supplements,

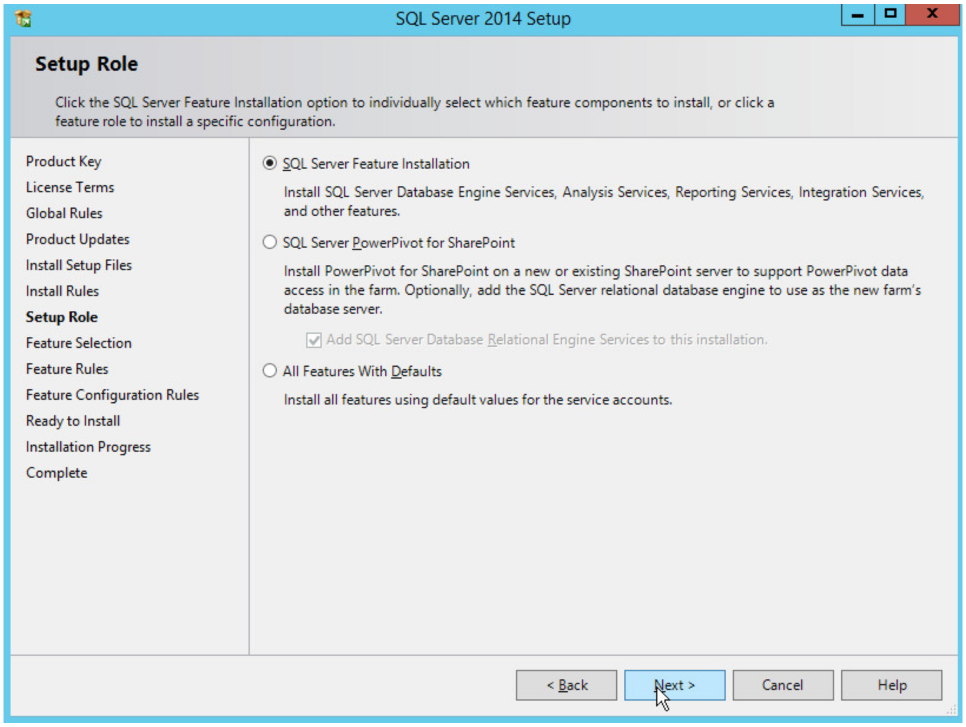
☑ I accept the license terms.

☐ Turn on Customer Experience Improvement Program ("CEIP") and Error Reporting to help improve the quality, reliability and performance of Microsoft SQL Server 2014.

See the Microsoft SQL Server 2014 Privacy Statement for more information.

* Microsoft SQL Server 2014 also includes a Visual Studio component that will have CEIP settings turned off by default. If Visual Studio is installed, this component will use the CEIP settings for Visual Studio.

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**.



SQL Server 2014 Setup

Setup Role

Click the SQL Server Feature Installation option to individually select which feature components to install, or click a feature role to install a specific configuration.

● SQL Server Feature Installation

Install SQL Server Database Engine Services, Analysis Services, Reporting Services, Integration Services, and other features.

○ SQL Server PowerPivot for SharePoint

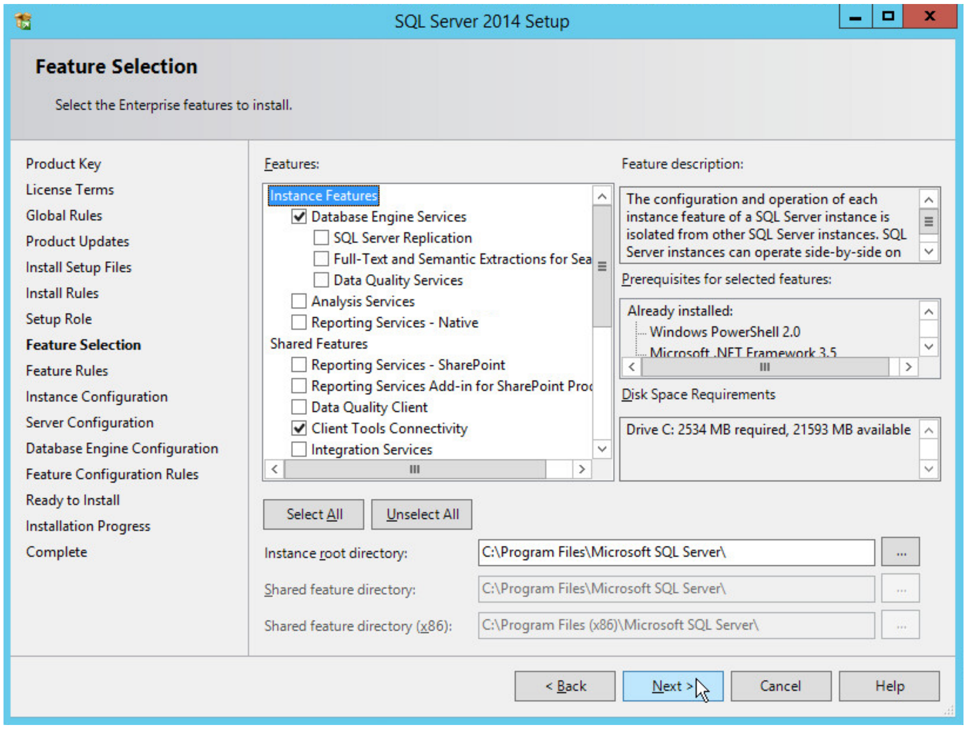
Install PowerPivot for SharePoint on a new or existing SharePoint server to support PowerPivot data access in the farm. Optionally, add the SQL Server relational database engine to use as the new farm's database server.

☑ Add SQL Server Database Relational Engine Services to this installation.

○ All Features With Defaults

Install all features using default values for the service accounts.

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**



SQL Server 2014 Setup

Feature Selection

Select the Enterprise features to install.

Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

Features:

Instance Features
- ☑ Database Engine Services
  - ☐ SQL Server Replication
  - ☐ Full-Text and Semantic Extractions for Sea
  - ☐ Data Quality Services
- ☐ Analysis Services
- ☐ Reporting Services - Native

Shared Features
- ☐ Reporting Services - SharePoint
- ☐ Reporting Services Add-in for SharePoint Proc
- ☐ Data Quality Client
- ☑ Client Tools Connectivity
- ☐ Integration Services

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on

Prerequisites for selected features:

Already installed:
Windows PowerShell 2.0
Microsoft .NET Framework 3.5

Disk Space Requirements

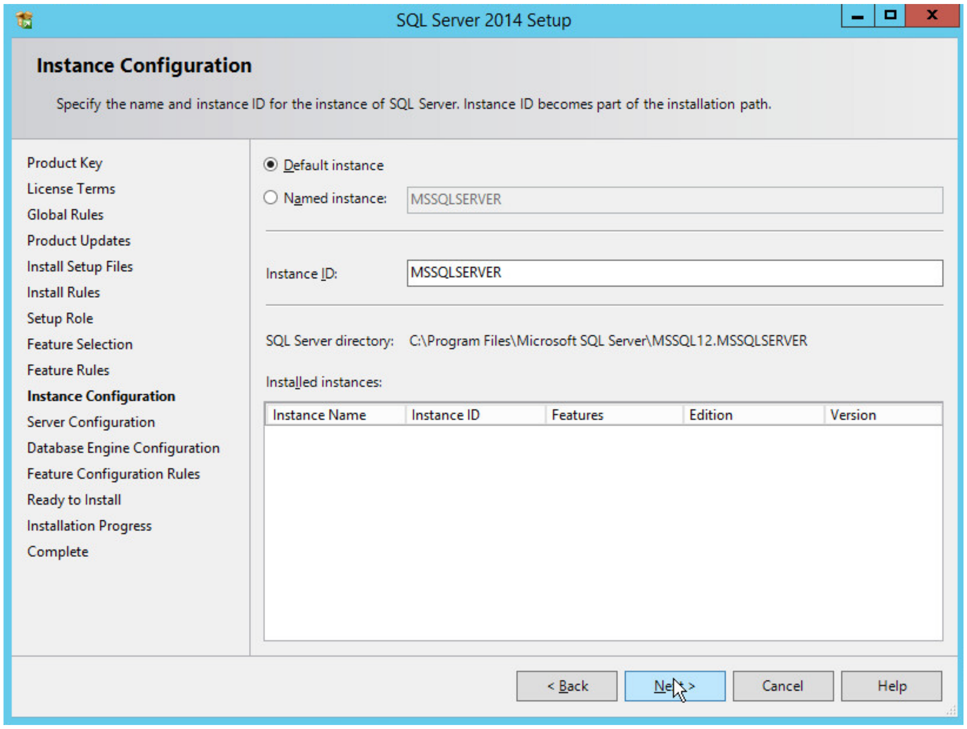
Drive C: 2534 MB required, 21593 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

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



SQL Server 2014 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete

● Default instance

○ Named instance: MSSQLSERVER

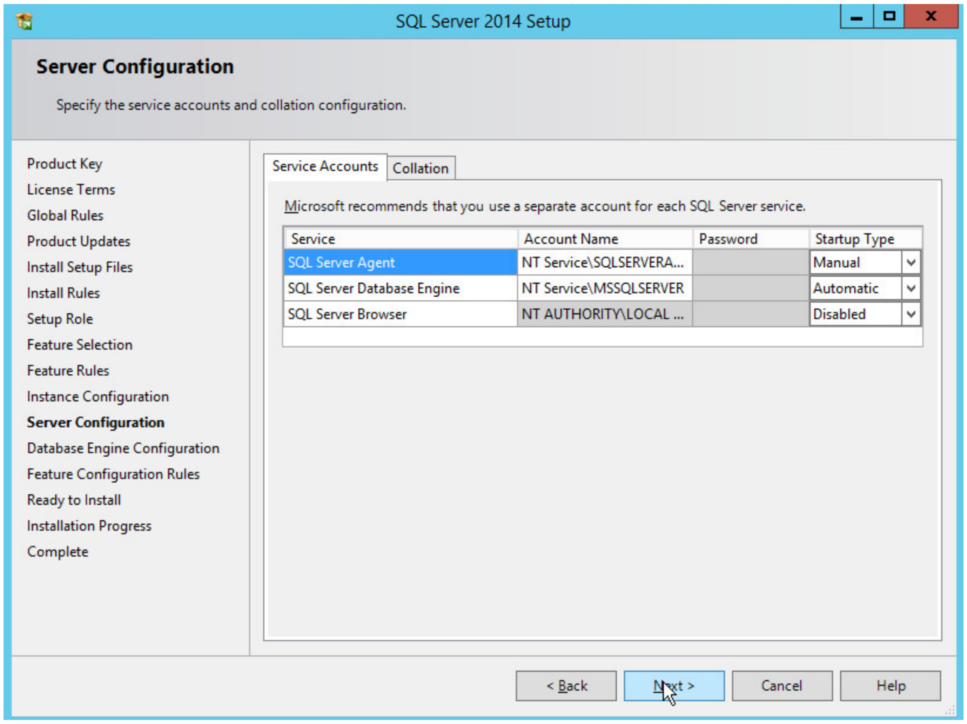
Instance ID: MSSQLSERVER

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

16. Click **Next**.



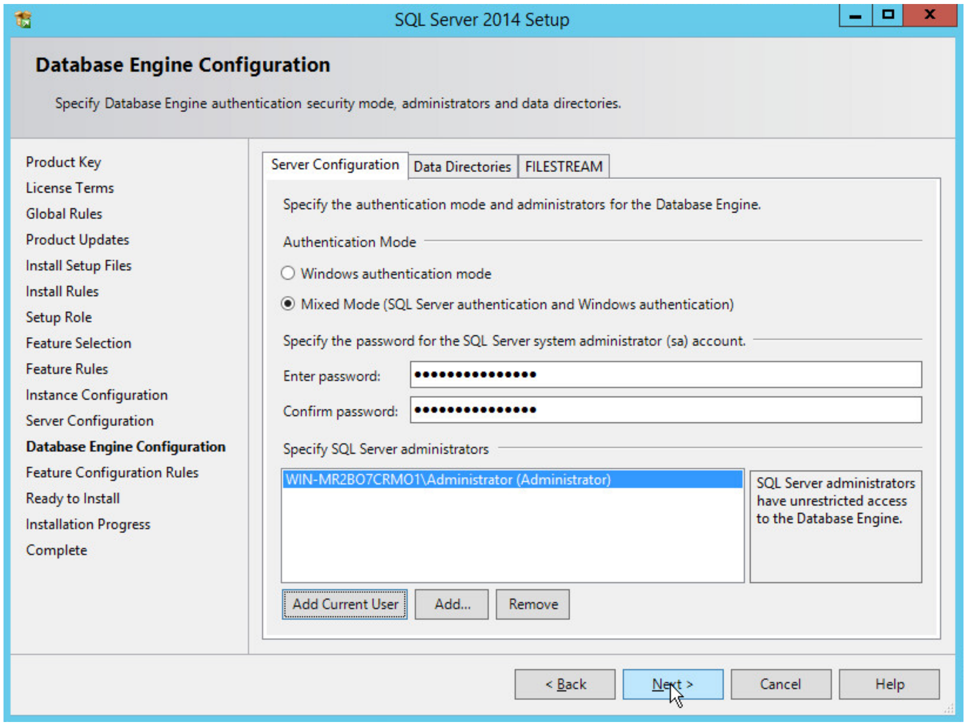
Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	NT Service\SQLSERVERA...		Manual
SQL Server Database Engine	NT Service\MSSQLSERVER		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled

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, 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 computers 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**.



Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: •••••••••••••••

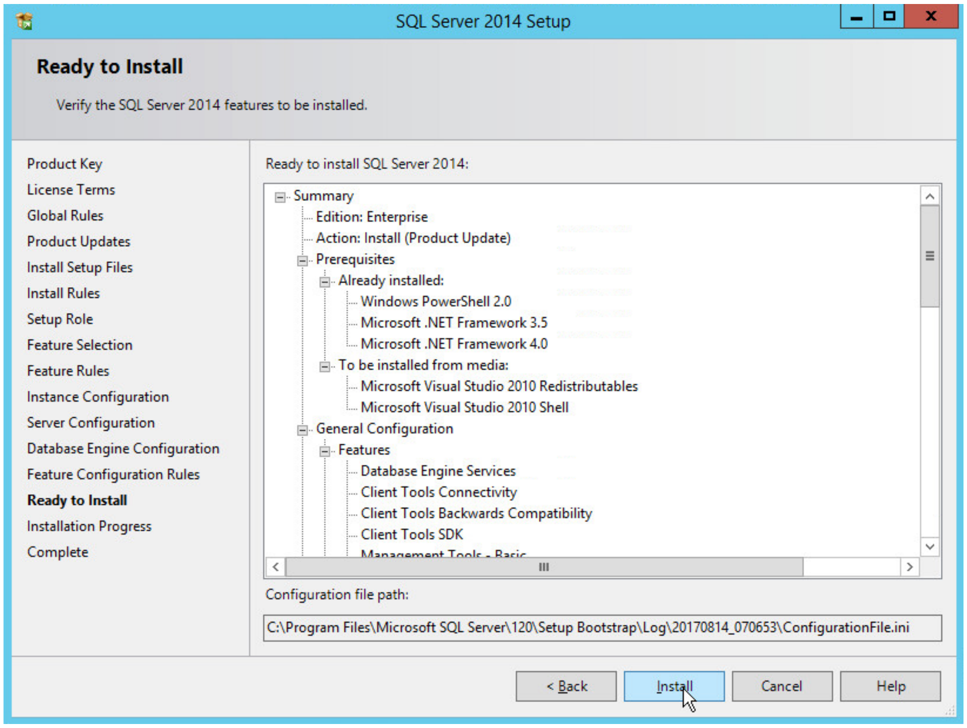
Confirm password: •••••••••••••••

Specify SQL Server administrators

WIN-MR2BO7CRMO1\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

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



Ready to Install

Verify the SQL Server 2014 features to be installed.

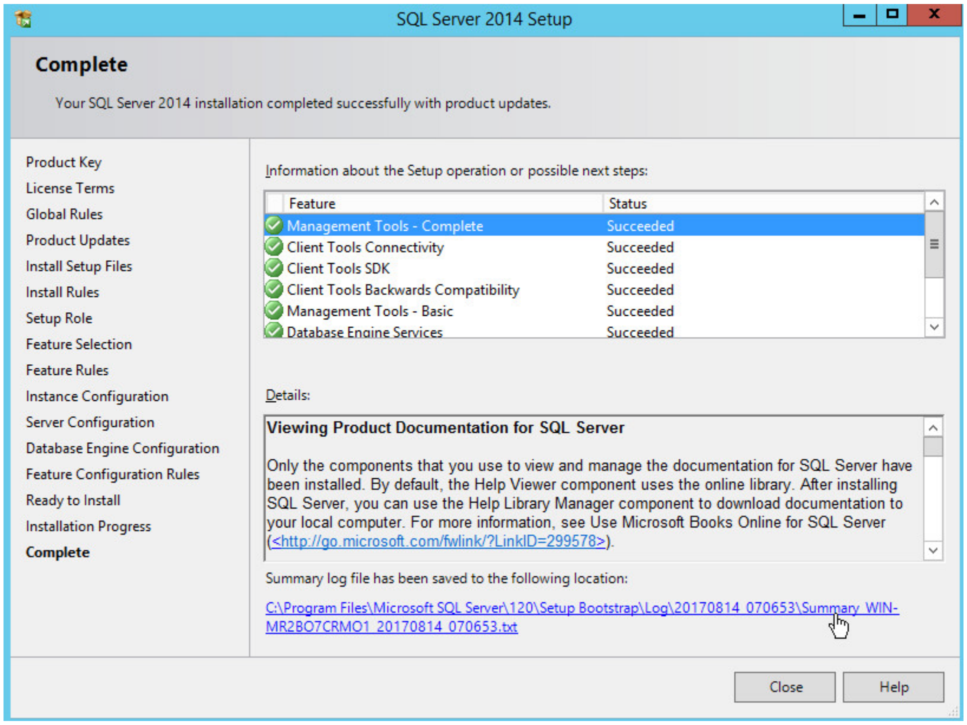
Ready to install SQL Server 2014:

```
Summary
  Edition: Enterprise
  Action: Install (Product Update)
  Prerequisites
    Already installed:
      Windows PowerShell 2.0
      Microsoft .NET Framework 3.5
      Microsoft .NET Framework 4.0
    To be installed from media:
      Microsoft Visual Studio 2010 Redistributables
      Microsoft Visual Studio 2010 Shell
  General Configuration
    Features
      Database Engine Services
      Client Tools Connectivity
      Client Tools Backwards Compatibility
      Client Tools SDK
      Management Tools - Basic
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\120\Setup Bootstrap\Log\20170814_070653\ConfigurationFile.ini

21. Wait for the install to finish.



Complete

Your SQL Server 2014 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Management Tools - Complete	Succeeded
Client Tools Connectivity	Succeeded
Client Tools SDK	Succeeded
Client Tools Backwards Compatibility	Succeeded
Management Tools - Basic	Succeeded
Database Engine Services	Succeeded

Details:

Viewing Product Documentation for SQL Server

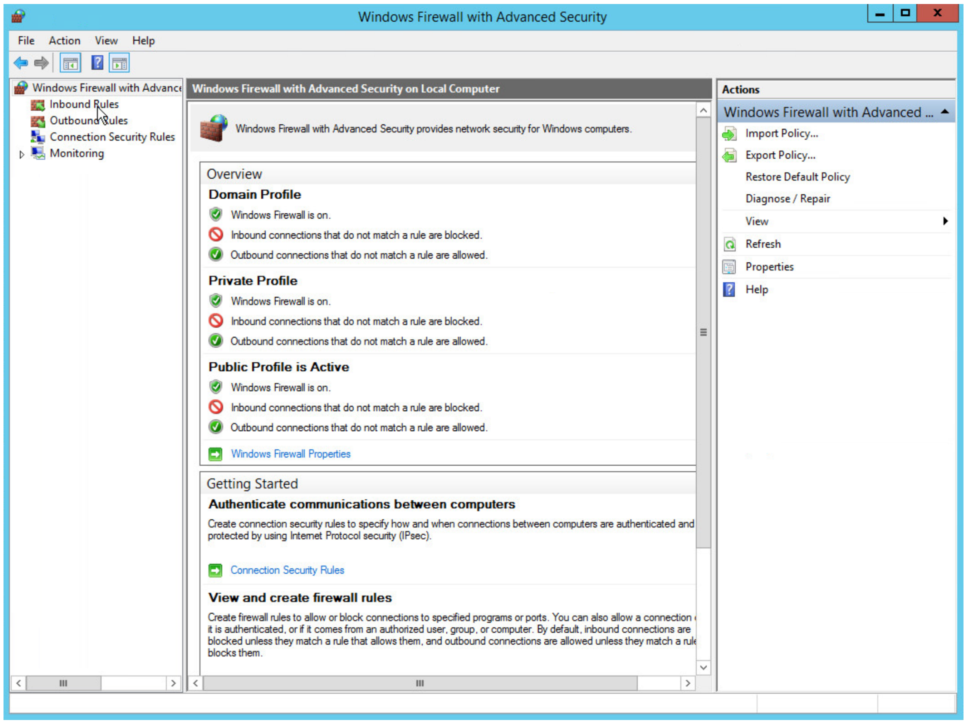
Only the components that you use to view and manage the documentation for SQL Server have been installed. By default, the Help Viewer component uses the online library. After installing SQL Server, you can use the Help Library Manager component to download documentation to your local computer. For more information, see Use Microsoft Books Online for SQL Server (<http://go.microsoft.com/fwlink/?LinkID=299578>).

Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\120\Setup Bootstrap\Log\20170814_070653\Summary_WIN-MR2BO7CRMO1_20170814_070653.txt

2.5.2 Open Port on Firewall

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



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Private Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Public Profile is Active

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

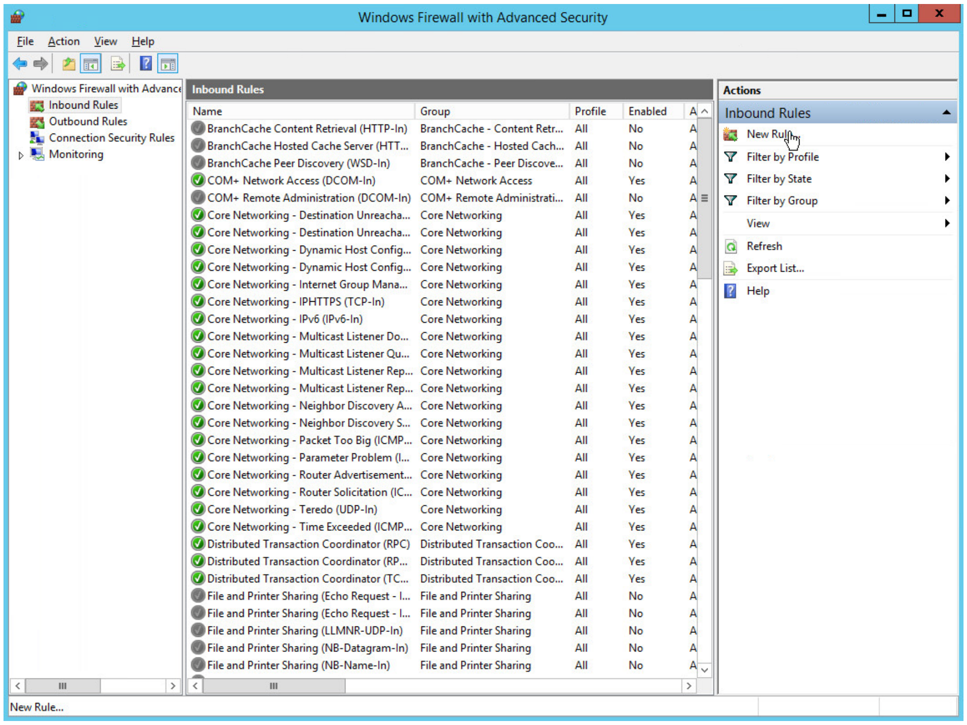
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection i it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rul blocks them.

2. Click **Inbound Rules** and then **New Rule.**

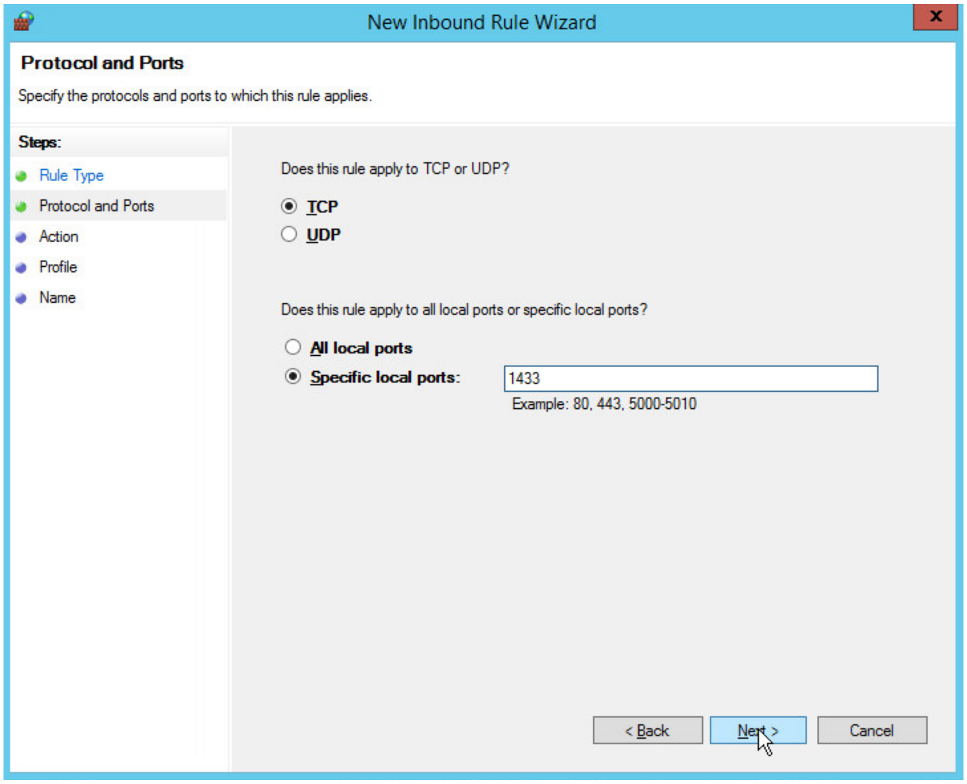


Inbound Rules

Name	Group	Profile	Enabled	A
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	A
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	A
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	A
COM+ Network Access (DCOM-In)	COM+ Network Access	All	Yes	A
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	A
Core Networking - Destination Unreacha...	Core Networking	All	Yes	A
Core Networking - Destination Unreacha...	Core Networking	All	Yes	A
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	A
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	A
Core Networking - Internet Group Mana...	Core Networking	All	Yes	A
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	A
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	A
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	A
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	A
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	A
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	A
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	A
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	A
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	A
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	A
Core Networking - Router Advertisement...	Core Networking	All	Yes	A
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	A
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	A
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	A
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	Yes	A
Distributed Transaction Coordinator (RP...	Distributed Transaction Coo...	All	Yes	A
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	All	Yes	A
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	A
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	A
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	A
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No	A
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No	A

3. Select **Port**.

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



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

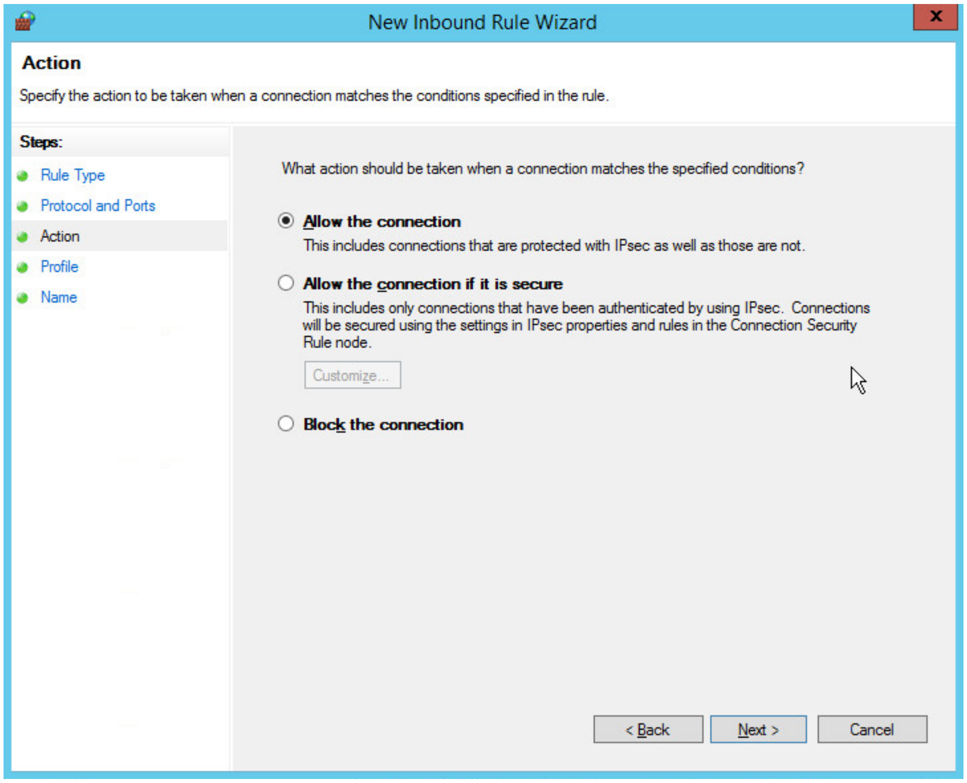
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 1433

Example: 80, 443, 5000-5010

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


New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

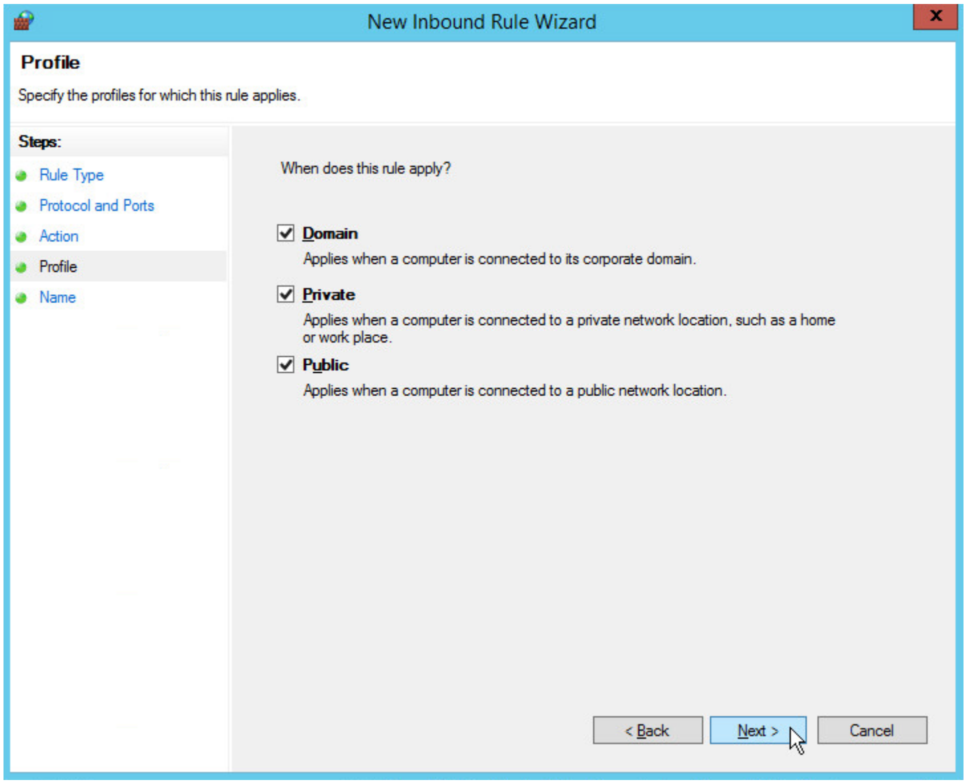
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

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



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**

Applies when a computer is connected to its corporate domain.

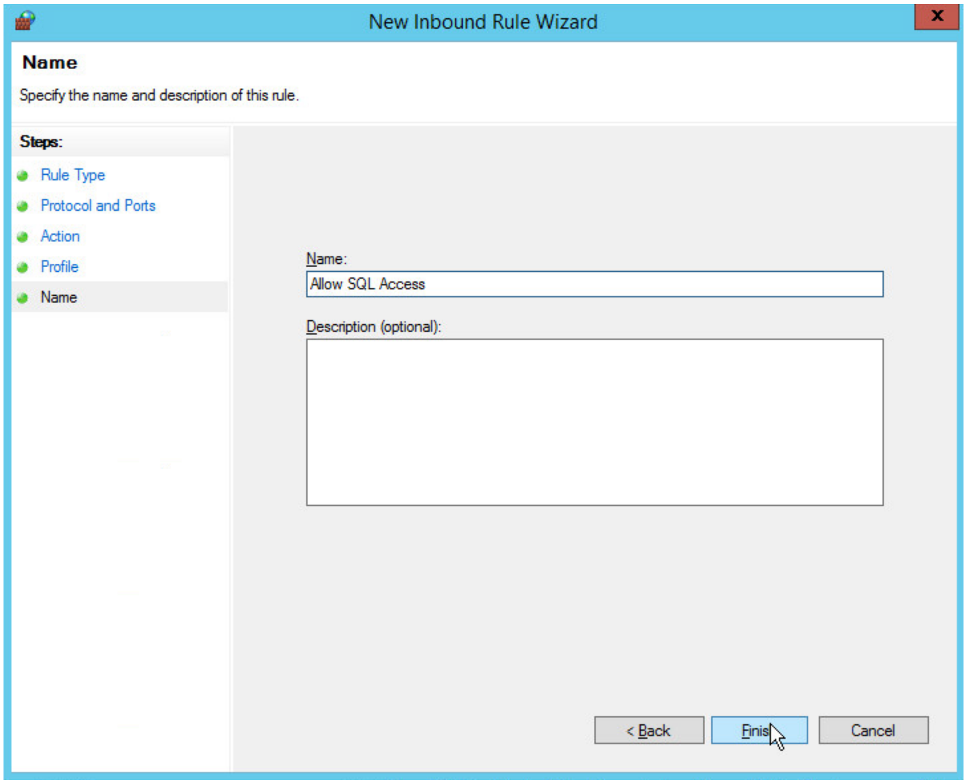
☑ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**

Applies when a computer is connected to a public network location.

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



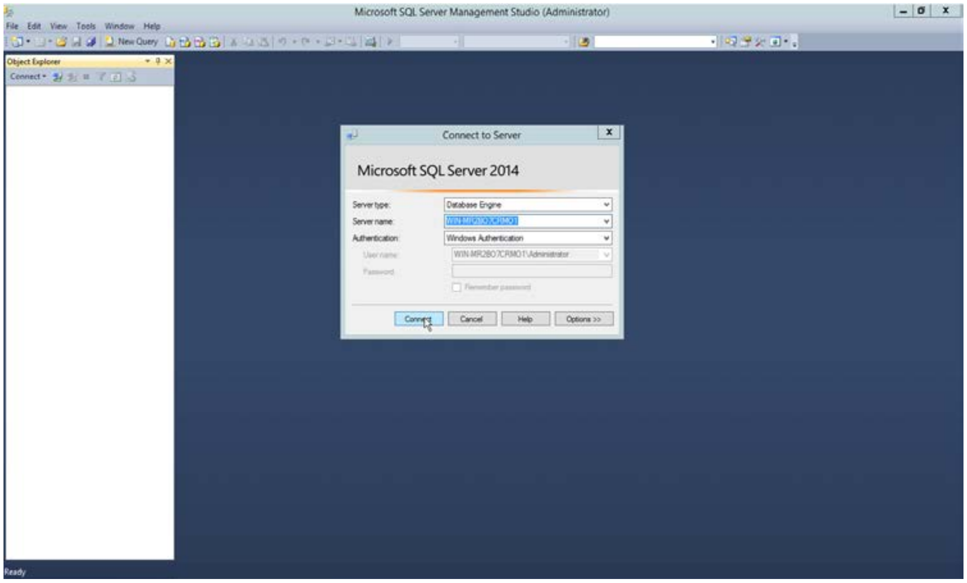
Name: Allow SQL Access

Description (optional):

13. Click **Finish**.

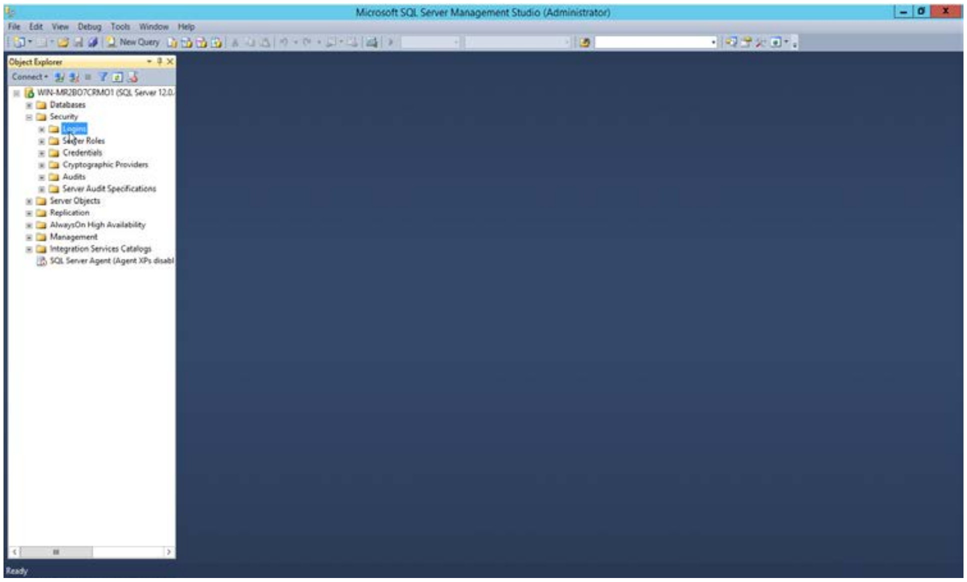
2.5.3 Add a New Login to the Database

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

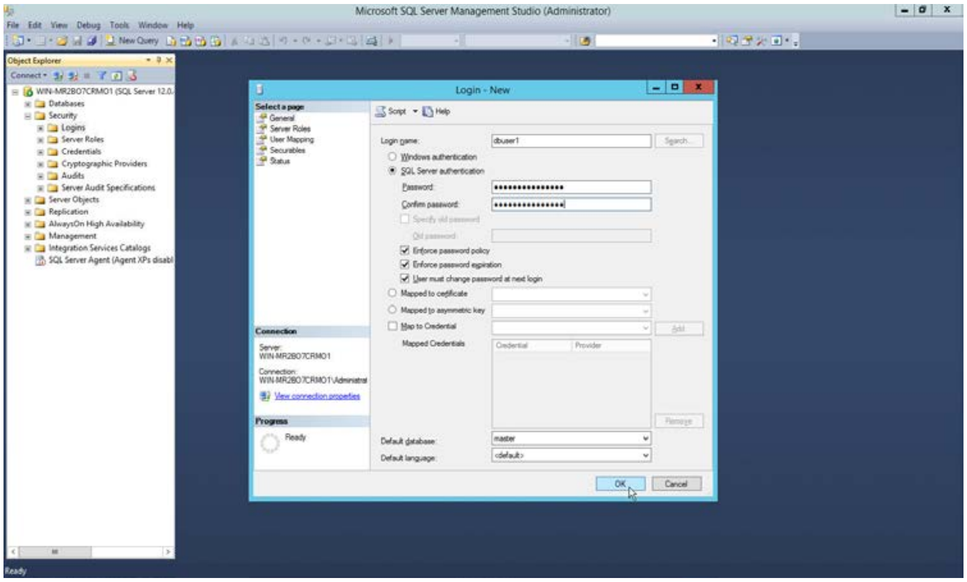

Microsoft SQL Server Management Studio (Administrator)
File Edit View Tools Window Help
New Query
Object Explorer
Connect
Ready
Connect to Server
Microsoft SQL Server 2014
Connect
Cancel
Help
Options >>

Server type: Database Engine
Server name: WIN-MR2BO7CRMO1
Authentication: Windows Authentication
User name: WIN-MR2BO7CRMO1\Administrator
Password:
□ Remember password

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


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
WIN-MR2BO7CRMO1 (SQL Server 12.0.
Databases
Security
Logins
Server Roles
Credentials
Cryptographic Providers
Audits
Server Audit Specifications
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent (Agent XPs disabl
Ready

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



Login name: dbuser1

○ Windows authentication

● SQL Server authentication

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

□ Specify old password

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Server: WIN-MR2BO7CRMO1

Connection: WIN-MR2BO7CRMO1\Administrat

Progress: Ready

Default database: master

Default language: <default>

6. Click **OK**.

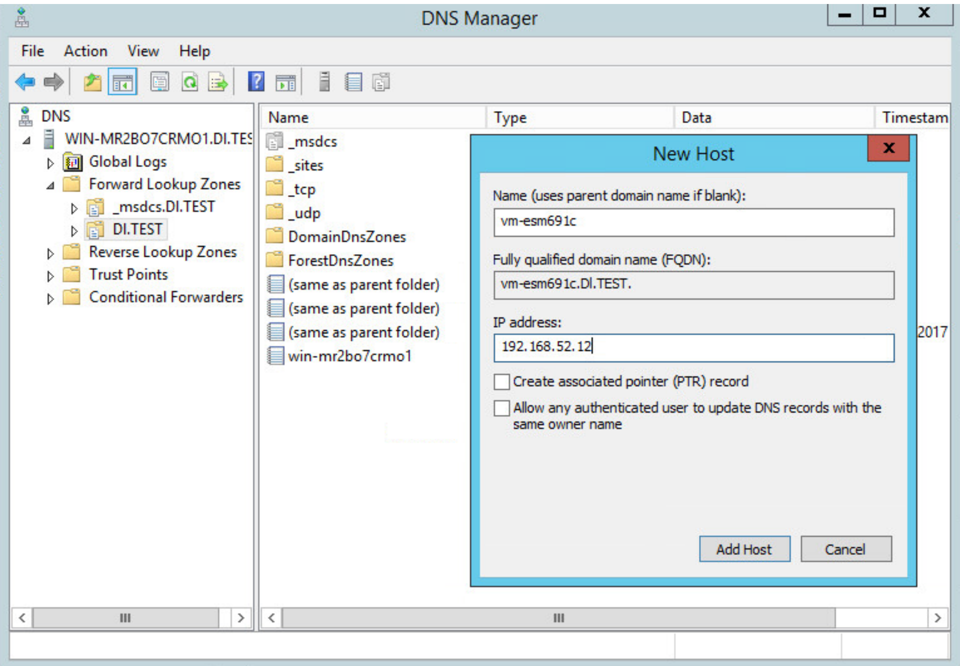
2.6 HPE ArcSight Enterprise Security Manager (ESM)

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

This installation guide assumes a pre-configured CentOS 7 Virtual Machine with ESM already installed and licensed. This section covers the installation and configuration process used to set up ArcSight agents on various machines.

2.6.1 Install Individual ArcSight Windows Connectors

1. Log in to your DNS server.



New Host

Name (uses parent domain name if blank): vm-esm691c

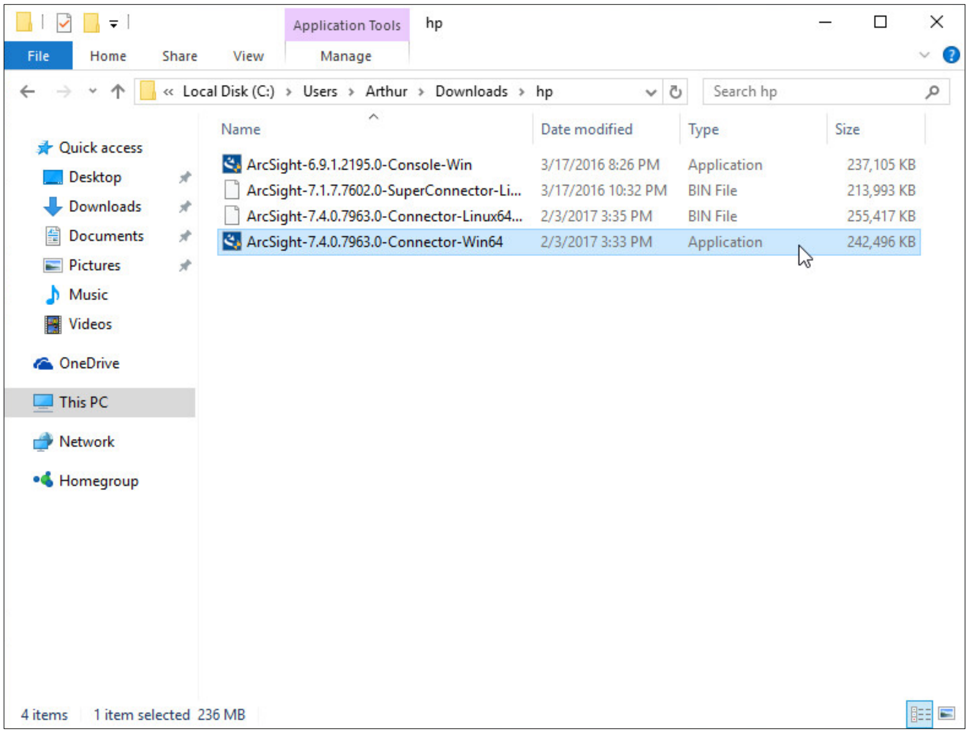
Fully qualified domain name (FQDN): vm-esm691c.DI.TEST.

IP address: 192.168.52.12

□ Create associated pointer (PTR) record

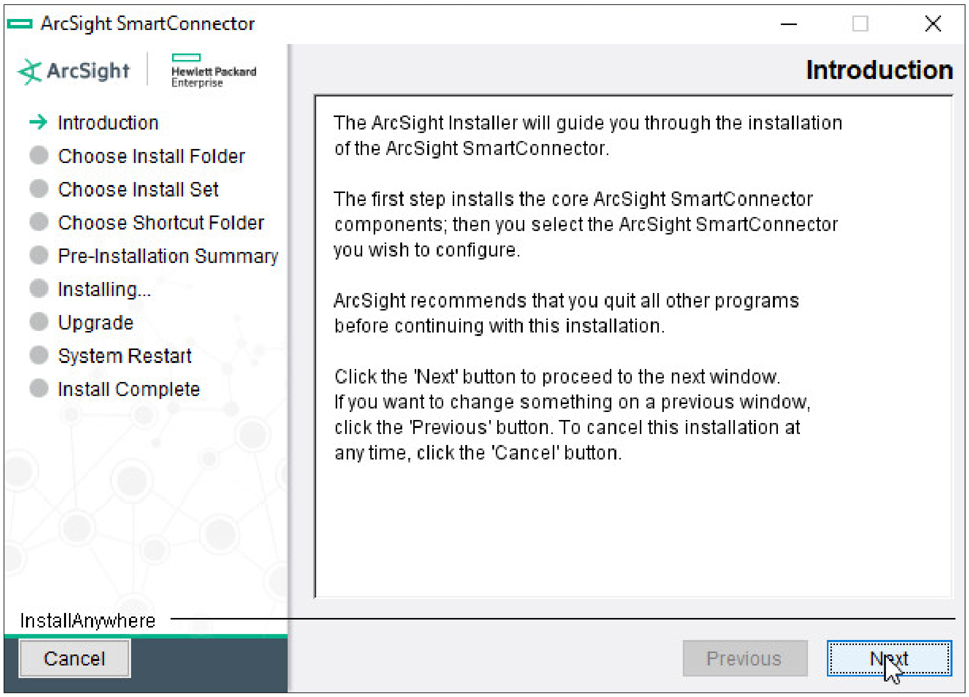
□ Allow any authenticated user to update DNS records with the same owner name

2. Add the host name of the ESM server *vm-esm691c* to the DNS list and associate it with the IP address of the ESM server.
3. Run the installation file **ArcSight-7.4.0.7963.0-Connector-Win64**.



Name	Date modified	Type	Size
ArcSight-6.9.1.2195.0-Console-Win	3/17/2016 8:26 PM	Application	237,105 KB
ArcSight-7.1.7.7602.0-SuperConnector-Li...	3/17/2016 10:32 PM	BIN File	213,993 KB
ArcSight-7.4.0.7963.0-Connector-Linux64...	2/3/2017 3:35 PM	BIN File	255,417 KB
ArcSight-7.4.0.7963.0-Connector-Win64	2/3/2017 3:33 PM	Application	242,496 KB

4. Wait for the initial setup to finish.



Introduction

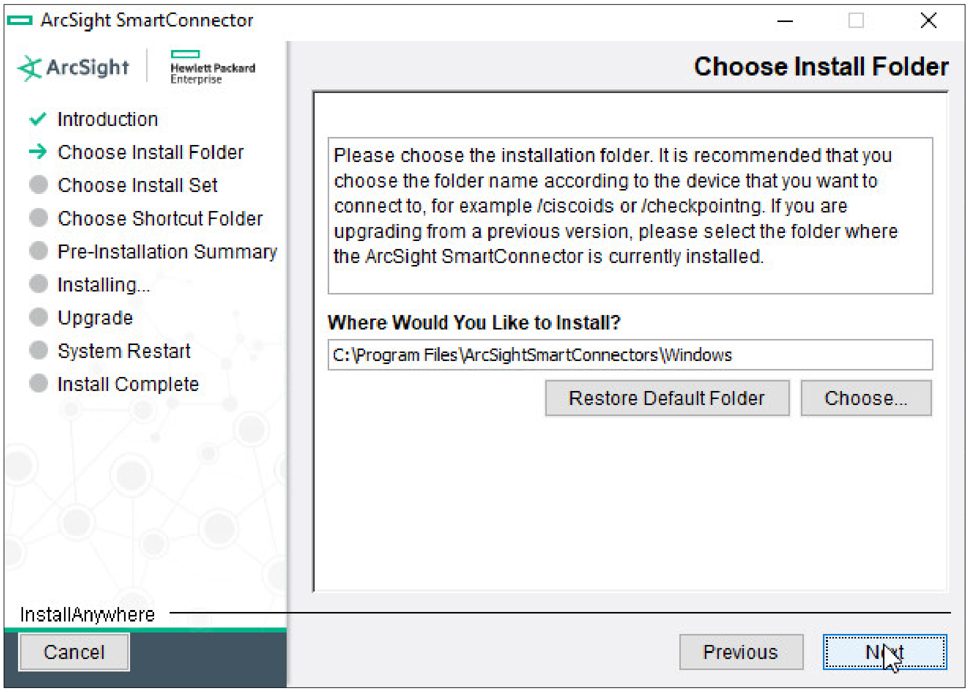
The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector.

The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.

5. Click **Next**.
6. Choose a destination folder. Note: It is recommended to change the default destination folder to `<default>\Windows`. This is to avoid conflicts if you wish to install more than one connector.

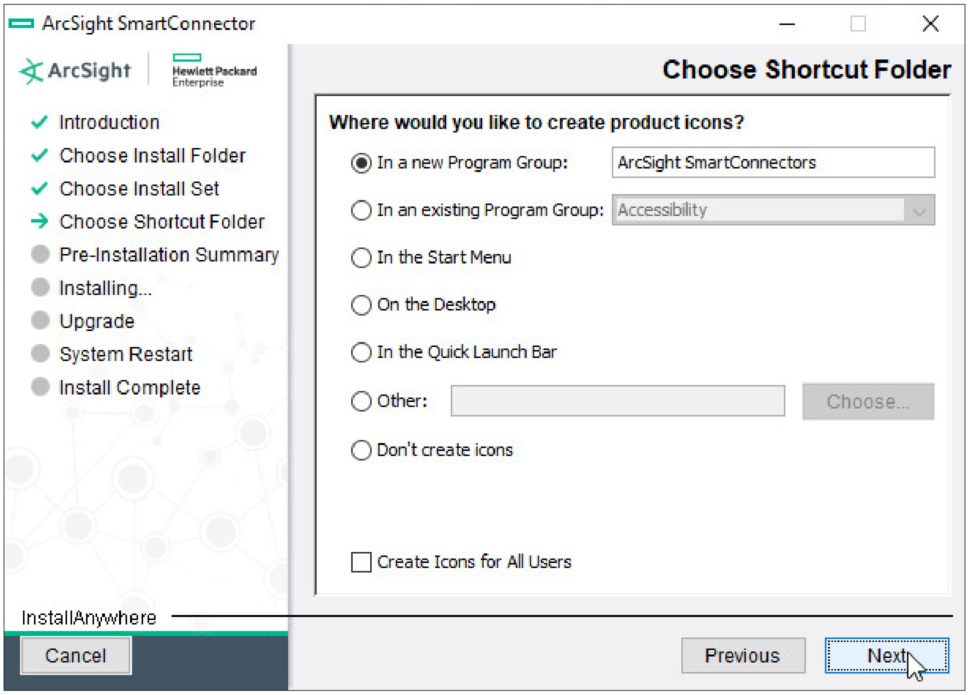


Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.

Where Would You Like to Install?

C:\Program Files\ArcSightSmartConnectors\Windows

7. Click **Next**.



Where would you like to create product icons?

● In a new Program Group: ArcSight SmartConnectors

○ In an existing Program Group: Accessibility

○ In the Start Menu

○ On the Desktop

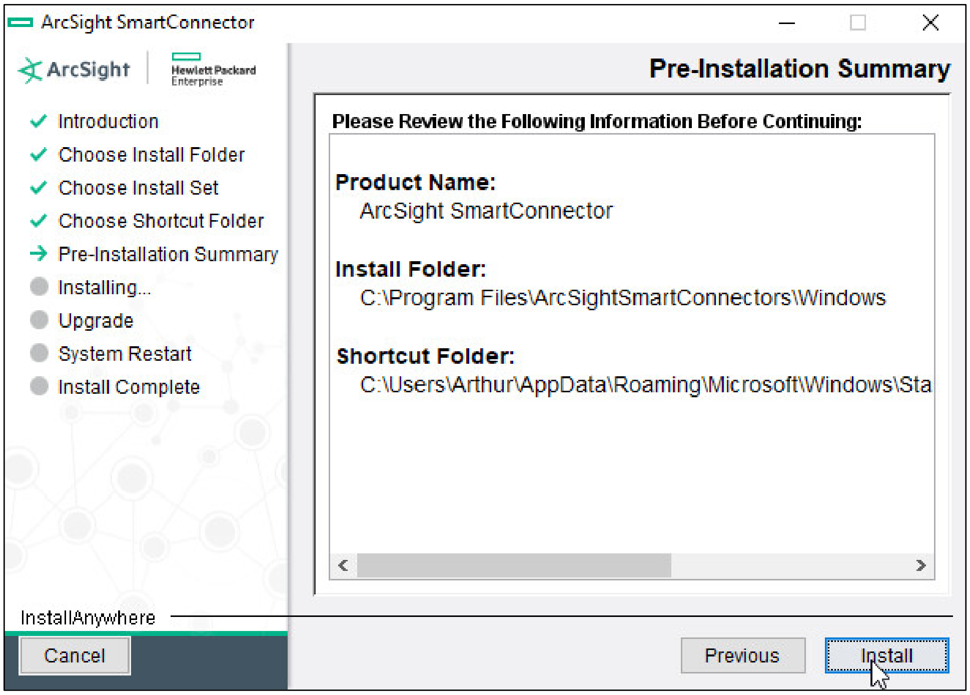
○ In the Quick Launch Bar

○ Other:

○ Don't create icons

□ Create Icons for All Users

8. Click **Next**.



Pre-Installation Summary

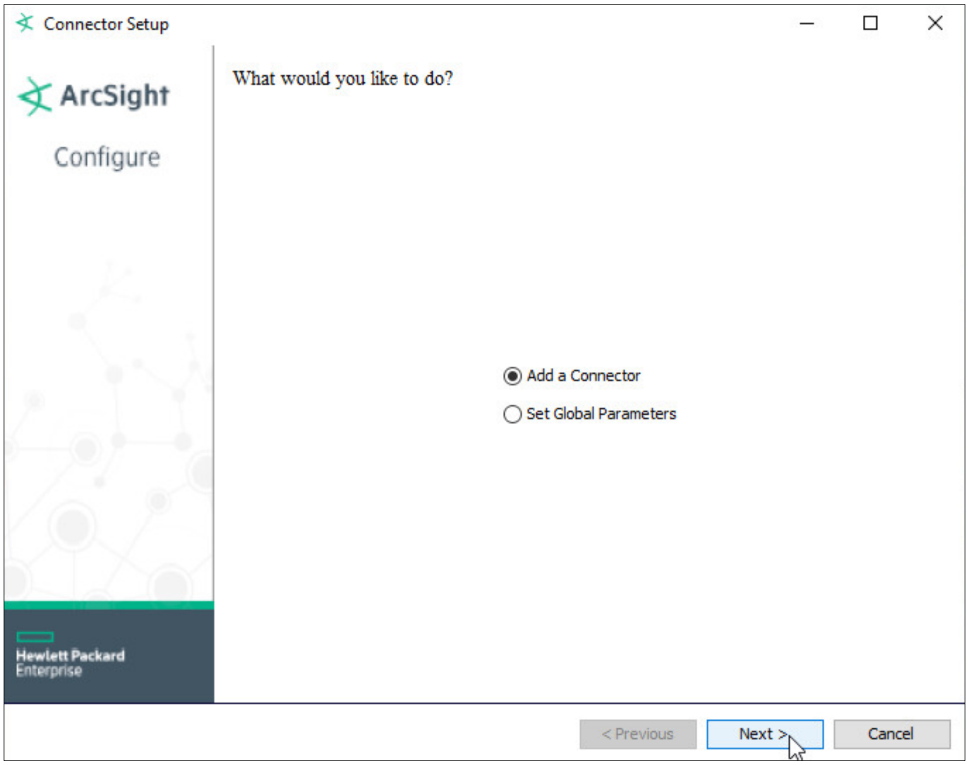
Please Review the Following Information Before Continuing:

Product Name:
ArcSight SmartConnector

Install Folder:
C:\Program Files\ArcSightSmartConnectors\Windows

Shortcut Folder:
C:\Users\Arthur\AppData\Roaming\Microsoft\Windows\Sta

9. Click **Install**.
10. Wait for the installation to finish.

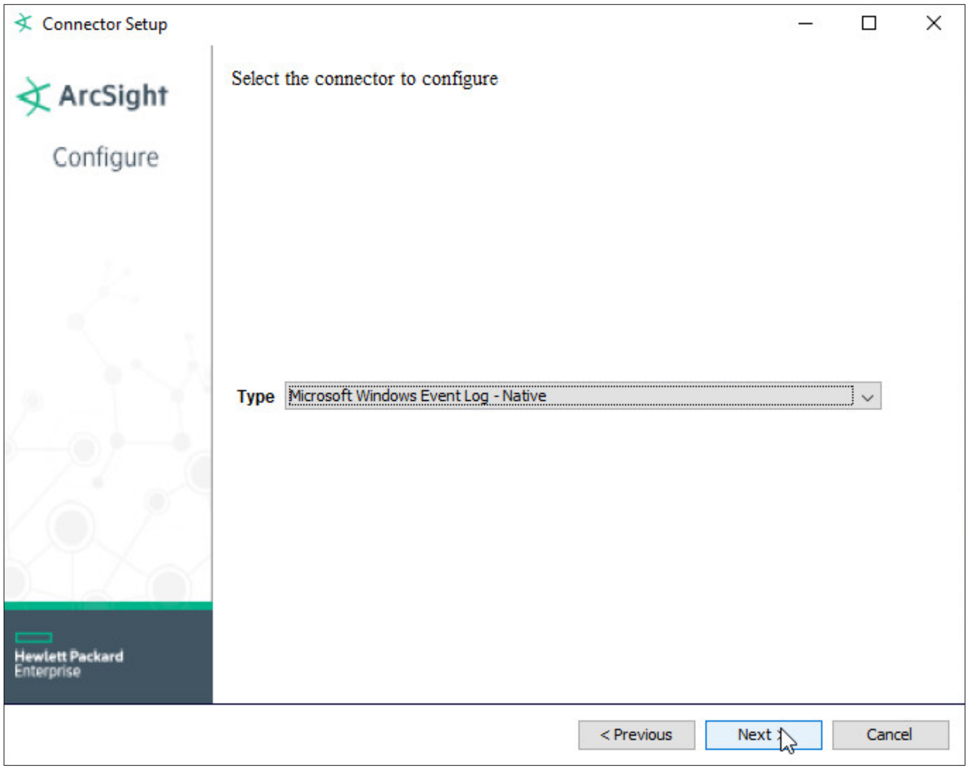


What would you like to do?

● Add a Connector

○ Set Global Parameters

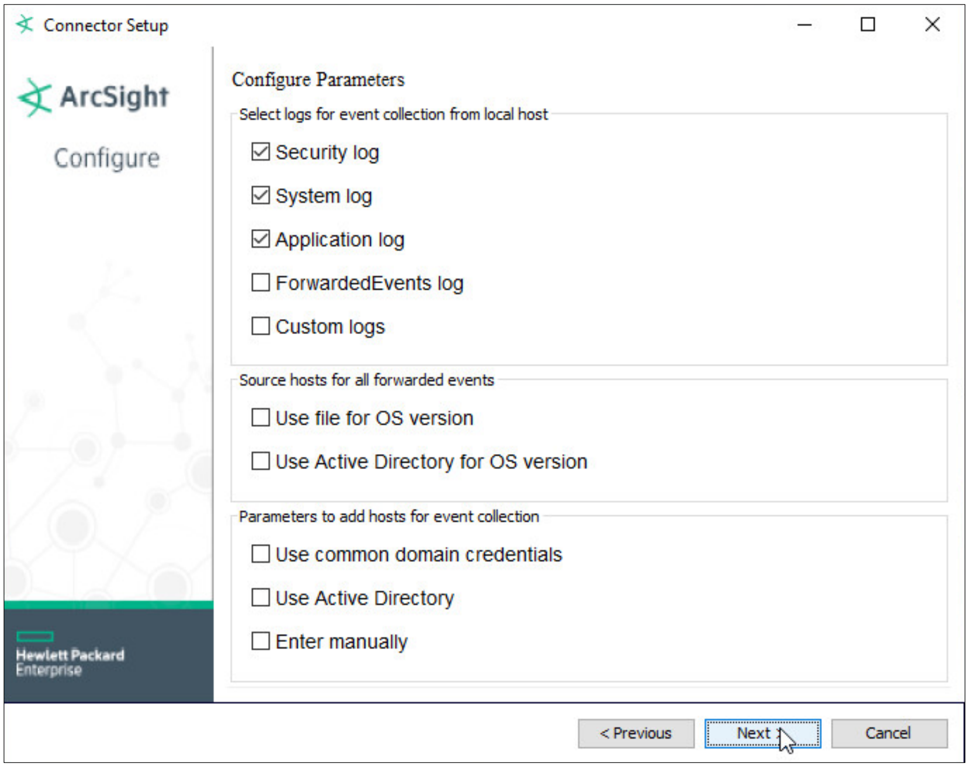
11. Select **Add a Connector**.
12. Click **Next**.
13. Choose **Microsoft Windows Event Log - Native** from the list.



Select the connector to configure

Type Microsoft Windows Event Log - Native

14. Click **Next**.
15. Check **Security log**, **System log**, and **Application Log**.



Connector Setup

Configure Parameters

Select logs for event collection from local host

☑ Security log

☑ System log

☑ Application log

□ ForwardedEvents log

□ Custom logs

Source hosts for all forwarded events

□ Use file for OS version

□ Use Active Directory for OS version

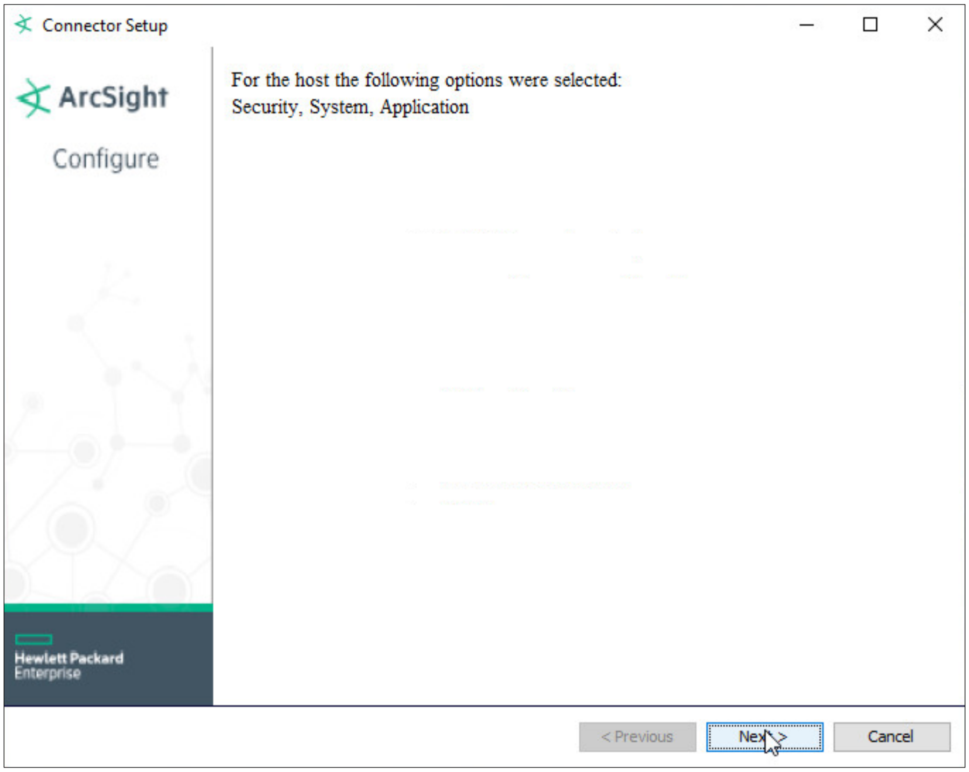
Parameters to add hosts for event collection

□ Use common domain credentials

□ Use Active Directory

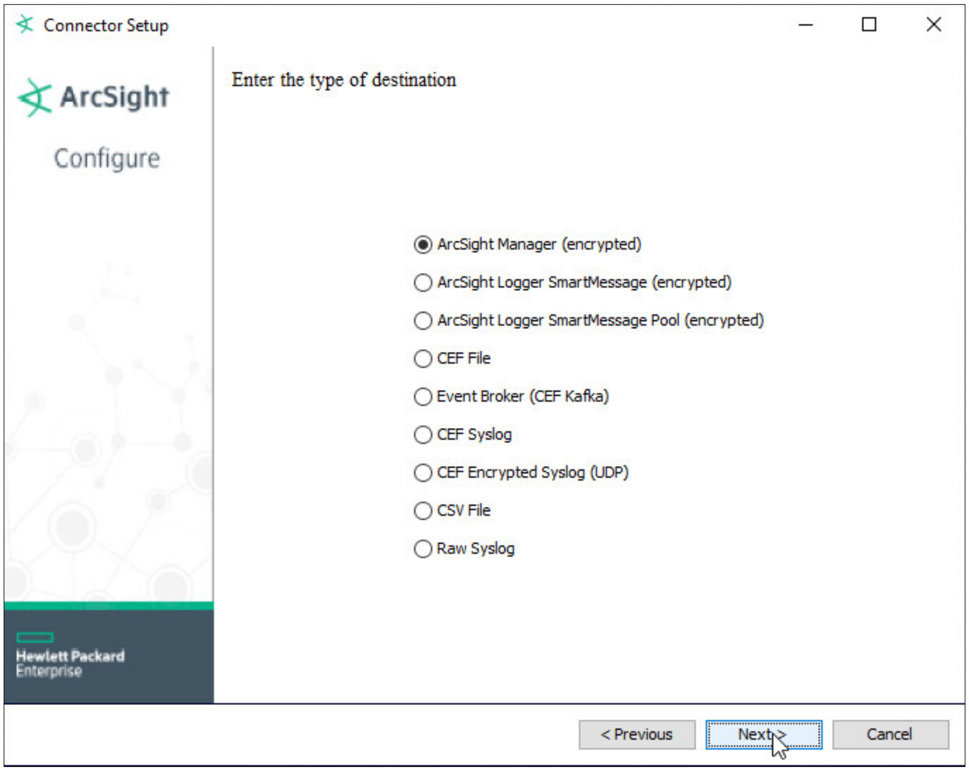
□ Enter manually

16. Click **Next**.



For the host the following options were selected:
Security, System, Application

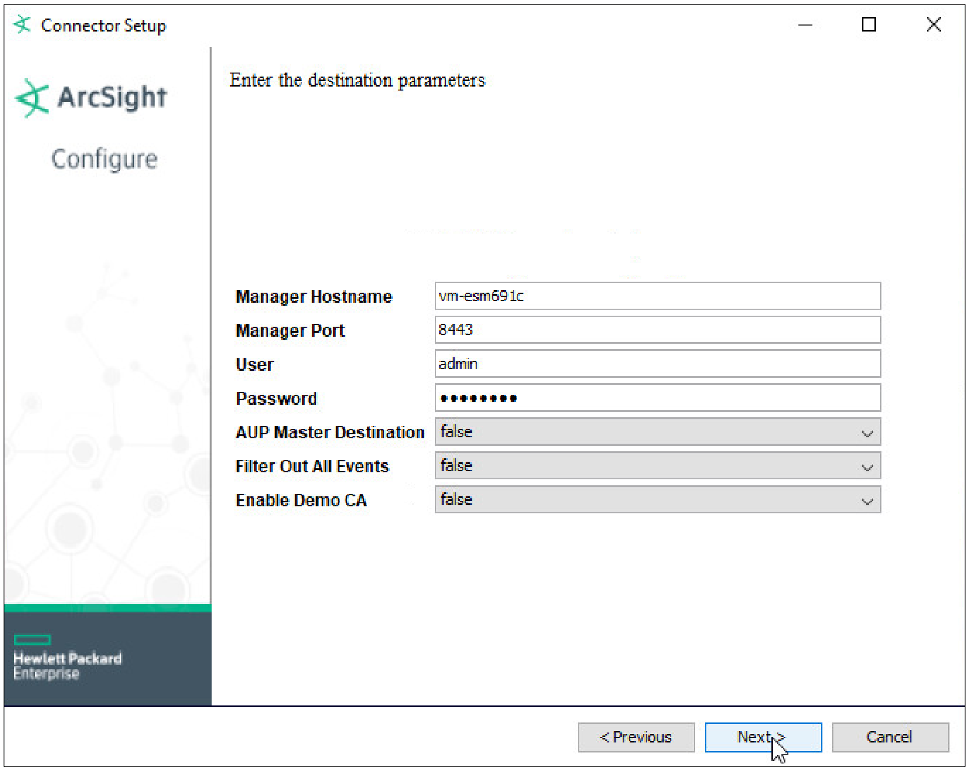
17. Click **Next**.
18. Choose **ArcSight Manager (encrypted)**.



Enter the type of destination

- ● ArcSight Manager (encrypted)
- ○ ArcSight Logger SmartMessage (encrypted)
- ○ ArcSight Logger SmartMessage Pool (encrypted)
- ○ CEF File
- ○ Event Broker (CEF Kafka)
- ○ CEF Syslog
- ○ CEF Encrypted Syslog (UDP)
- ○ CSV File
- ○ Raw Syslog

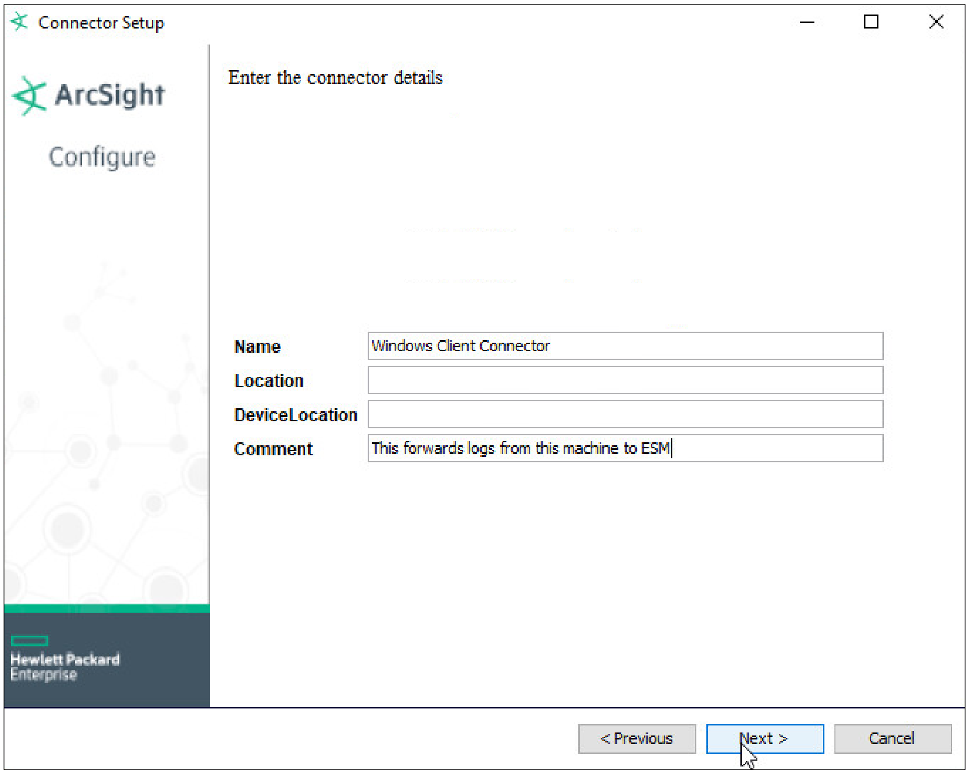
19. Click **Next**.
20. For **Manager Hostname**, put **vm-esm691c**, or the hostname of your ESM server.
21. For **Manager Port**, put **8443** (or the port that ESM is running on) on the ESM server.
22. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)



Enter the destination parameters

Manager Hostname	vm-esm691c
Manager Port	8443
User	admin
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

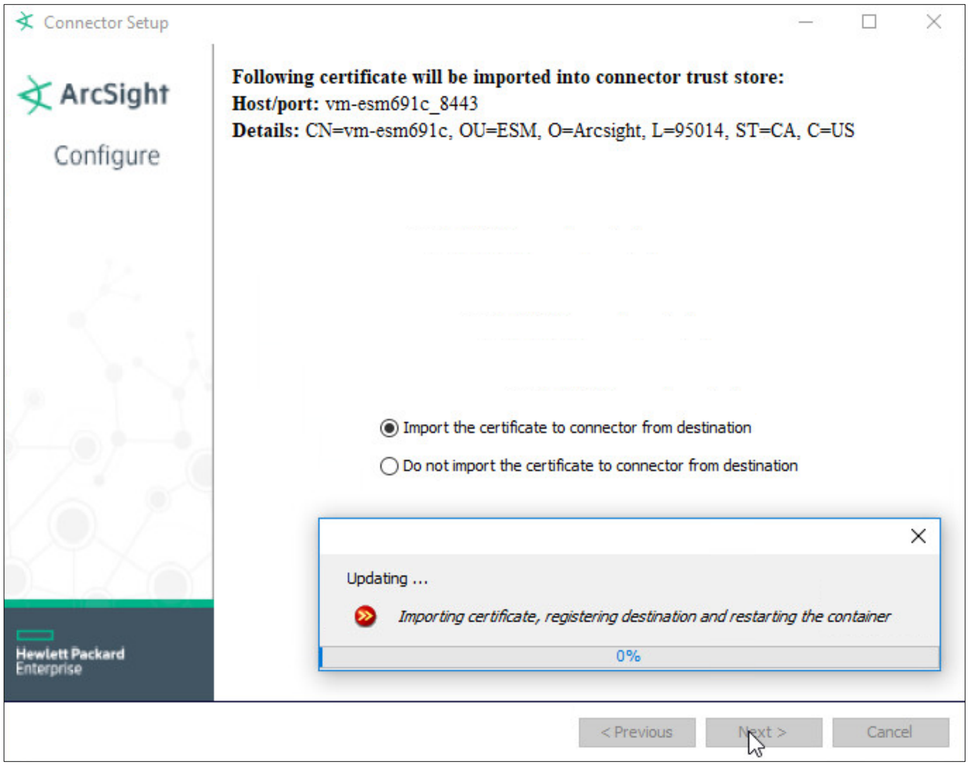
23. Click **Next**.
24. Set identifying details about the system to help identify the connector (include a value for **Name**; the rest is optional).



Enter the connector details

Name	Windows Client Connector
Location	
DeviceLocation	
Comment	This forwards logs from this machine to ESM

25. Click **Next**.
26. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the Virtual Machine.



Following certificate will be imported into connector trust store:
Host/port: vm-esm691c_8443
Details: CN=vm-esm691c, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

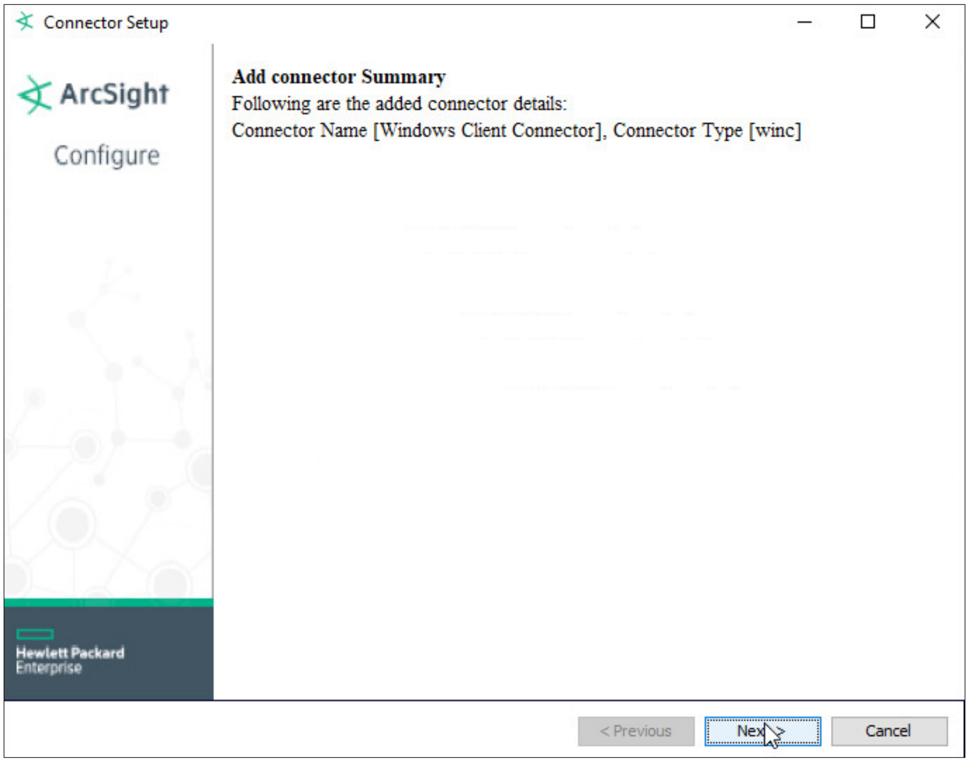
● Import the certificate to connector from destination
○ Do not import the certificate to connector from destination

Updating ...

Importing certificate, registering destination and restarting the container

0%

27. Click **Next**.

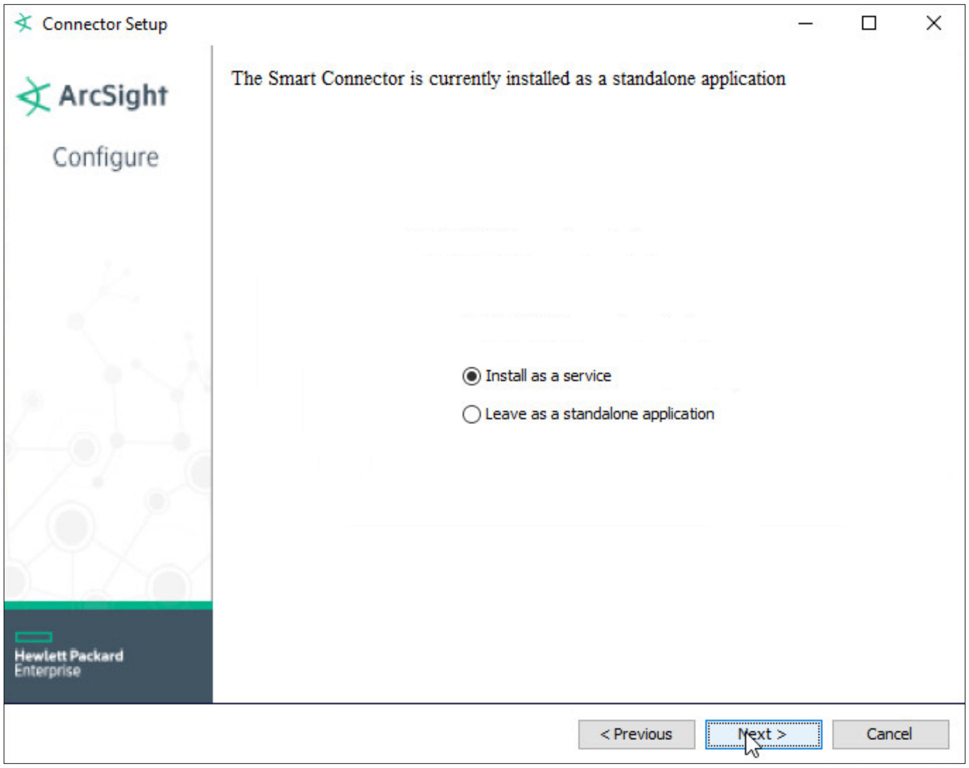


Add connector Summary

Following are the added connector details:

Connector Name [Windows Client Connector], Connector Type [winc]

28. Click **Next**.
29. Choose **Install as a service**.

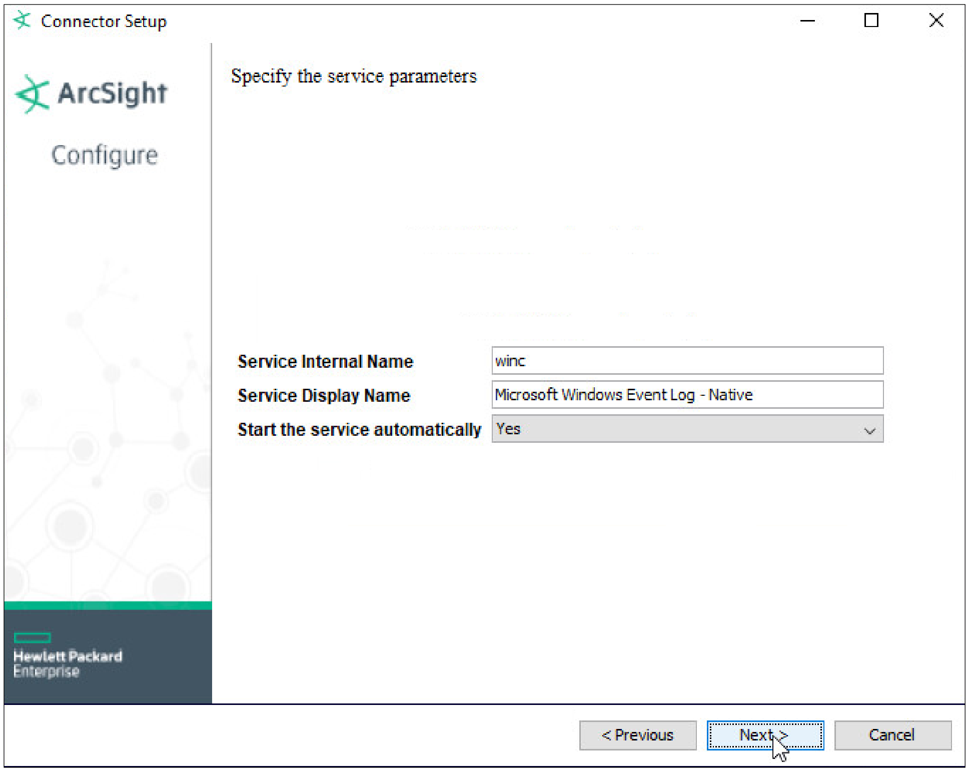


The Smart Connector is currently installed as a standalone application

● Install as a service

○ Leave as a standalone application

30. Click **Next**.



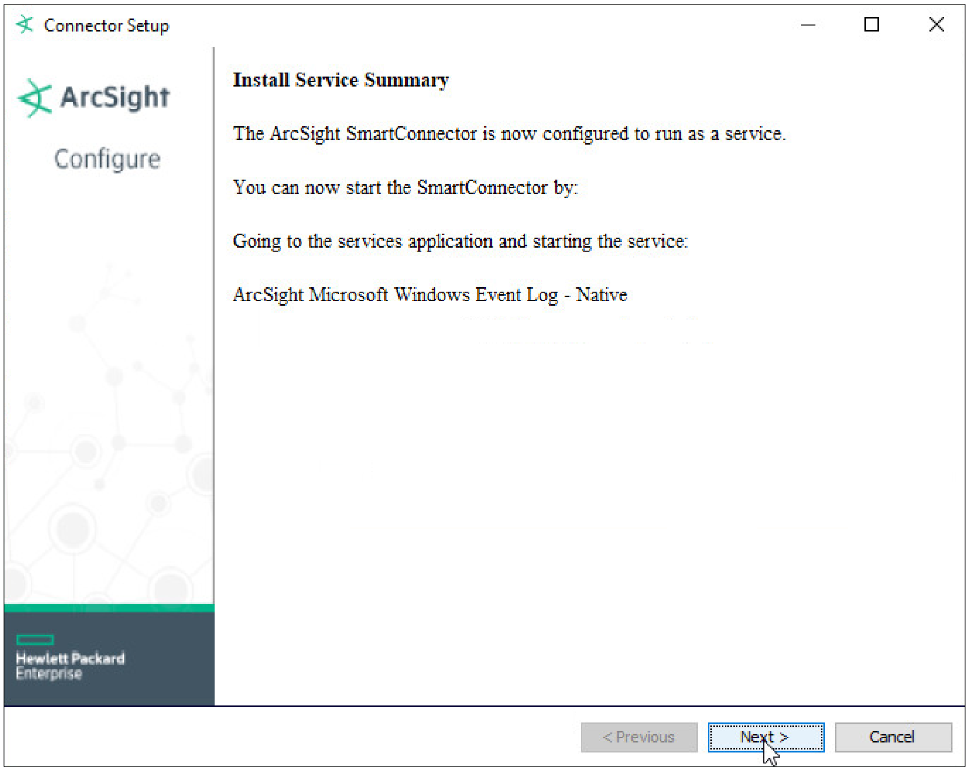
Specify the service parameters

Service Internal Name: winc

Service Display Name: Microsoft Windows Event Log - Native

Start the service automatically: Yes

31. Click **Next**.



Install Service Summary

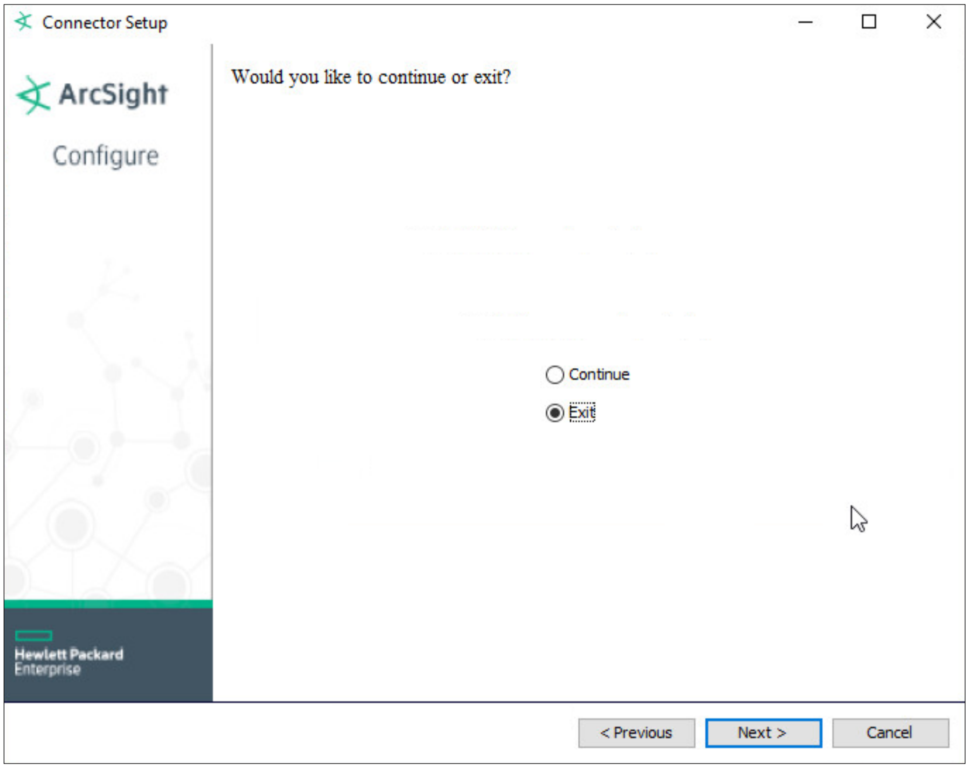
The ArcSight SmartConnector is now configured to run as a service.

You can now start the SmartConnector by:

Going to the services application and starting the service:

ArcSight Microsoft Windows Event Log - Native

32. Click **Next**.
33. Choose **Exit**.

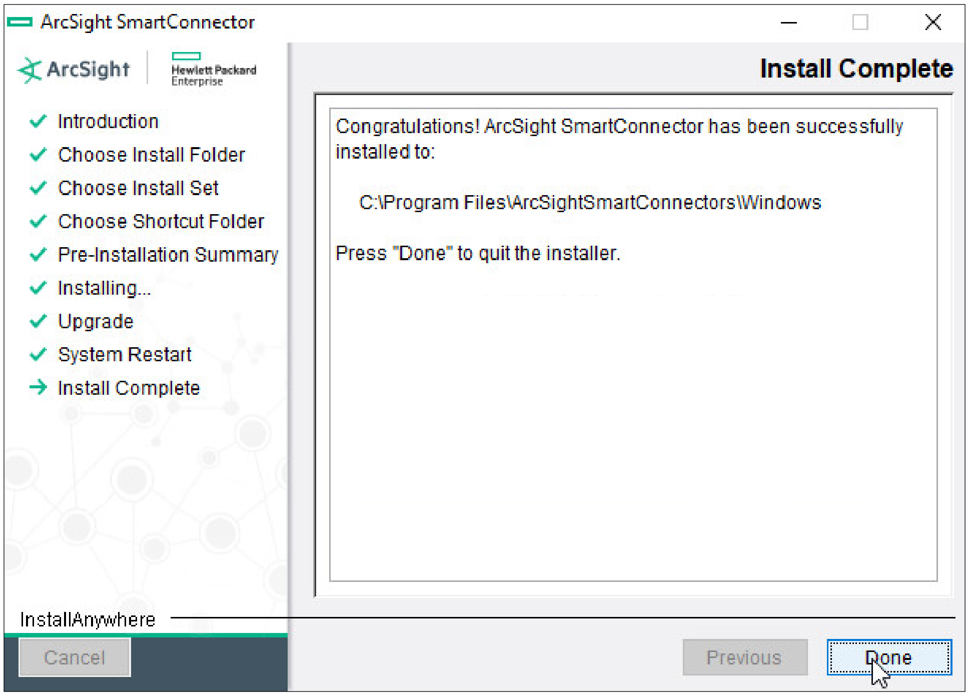


Would you like to continue or exit?

○ Continue

● Exit

34. Click **Next**.



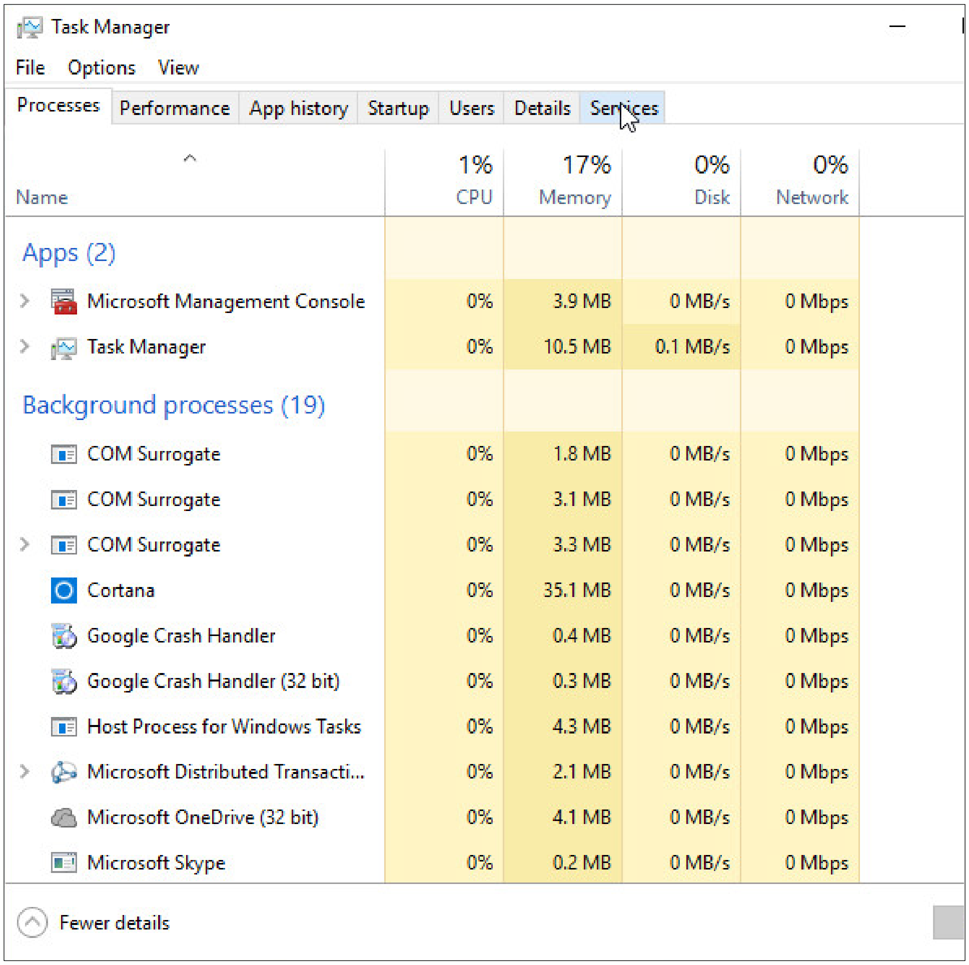
Install Complete

Congratulations! ArcSight SmartConnector has been successfully installed to:

C:\Program Files\ArcSightSmartConnectors\Windows

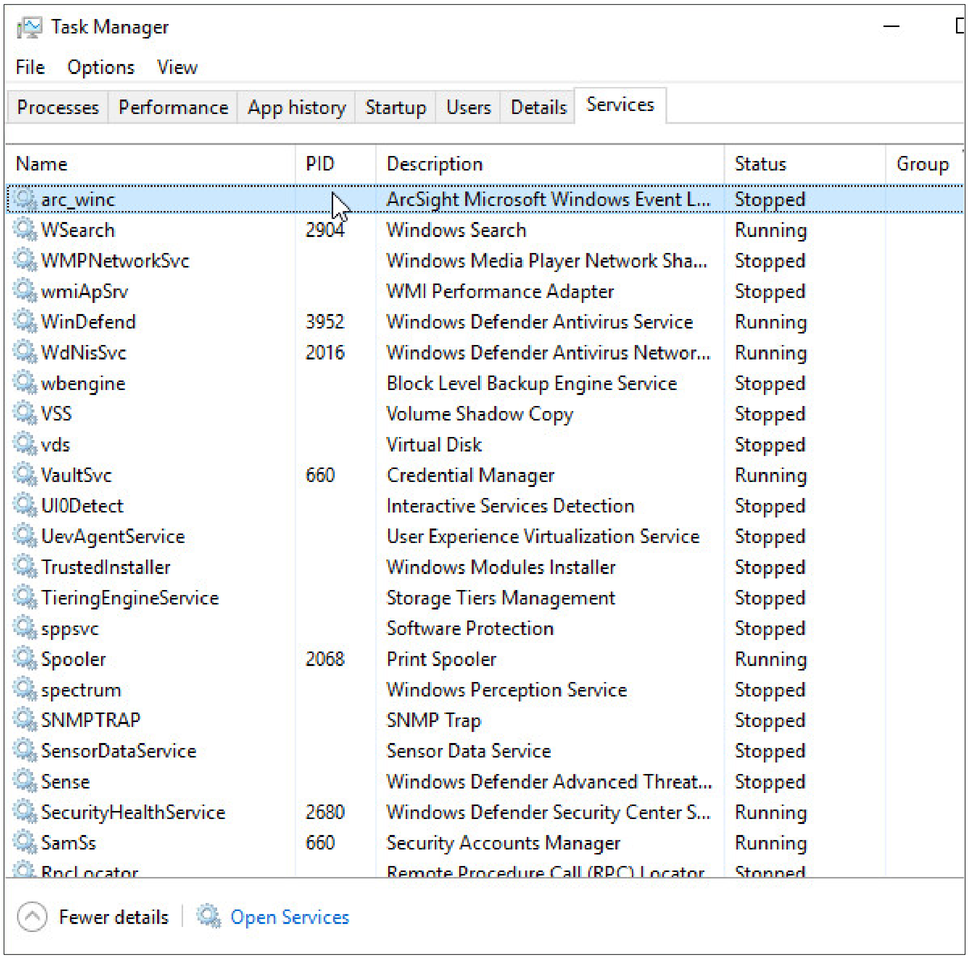
Press "Done" to quit the installer.

35. Click **Done**.
36. Open **Task Manager**.
37. Click **More Details**.



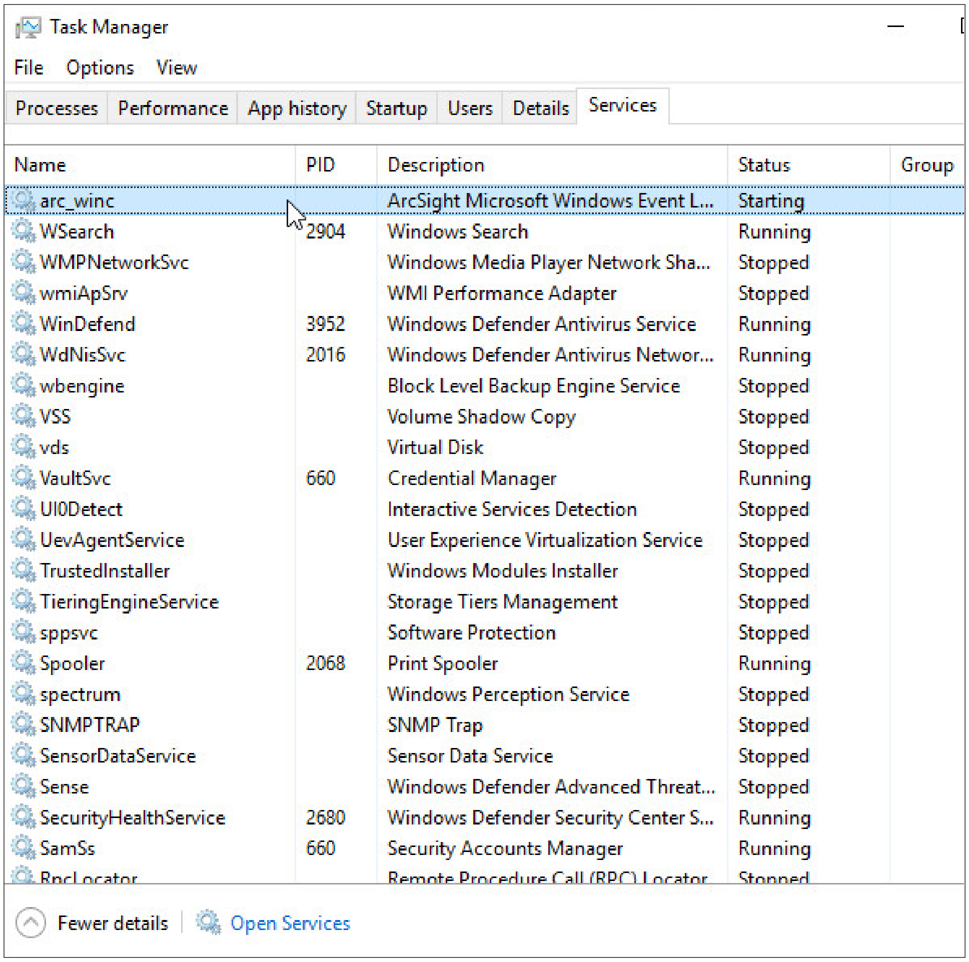
	1%	17%	0%	0%
Name	CPU	Memory	Disk	Network
Apps (2)				
Microsoft Management Console	0%	3.9 MB	0 MB/s	0 Mbps
Task Manager	0%	10.5 MB	0.1 MB/s	0 Mbps
Background processes (19)				
COM Surrogate	0%	1.8 MB	0 MB/s	0 Mbps
COM Surrogate	0%	3.1 MB	0 MB/s	0 Mbps
COM Surrogate	0%	3.3 MB	0 MB/s	0 Mbps
Cortana	0%	35.1 MB	0 MB/s	0 Mbps
Google Crash Handler	0%	0.4 MB	0 MB/s	0 Mbps
Google Crash Handler (32 bit)	0%	0.3 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	4.3 MB	0 MB/s	0 Mbps
Microsoft Distributed Transacti...	0%	2.1 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)	0%	4.1 MB	0 MB/s	0 Mbps
Microsoft Skype	0%	0.2 MB	0 MB/s	0 Mbps

38. Go to the **Services** tab.
39. Find the service just created for ArcSight and right click it.



Name	PID	Description	Status	Group
arc_winc		ArcSight Microsoft Windows Event L...	Stopped	
WSearch	2904	Windows Search	Running	
WMPNetworkSvc		Windows Media Player Network Sha...	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	3952	Windows Defender Antivirus Service	Running	
WdNisSvc	2016	Windows Defender Antivirus Networ...	Running	
wbengine		Block Level Backup Engine Service	Stopped	
VSS		Volume Shadow Copy	Stopped	
vds		Virtual Disk	Stopped	
VaultSvc	660	Credential Manager	Running	
UI0Detect		Interactive Services Detection	Stopped	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	2068	Print Spooler	Running	
spectrum		Windows Perception Service	Stopped	
SNMPTRAP		SNMP Trap	Stopped	
SensorDataService		Sensor Data Service	Stopped	
Sense		Windows Defender Advanced Threat...	Stopped	
SecurityHealthService	2680	Windows Defender Security Center S...	Running	
SamSs	660	Security Accounts Manager	Running	
RpcLocator		Remote Procedure Call (RPC) Locator	Stopped	

40. Choose **Start**.

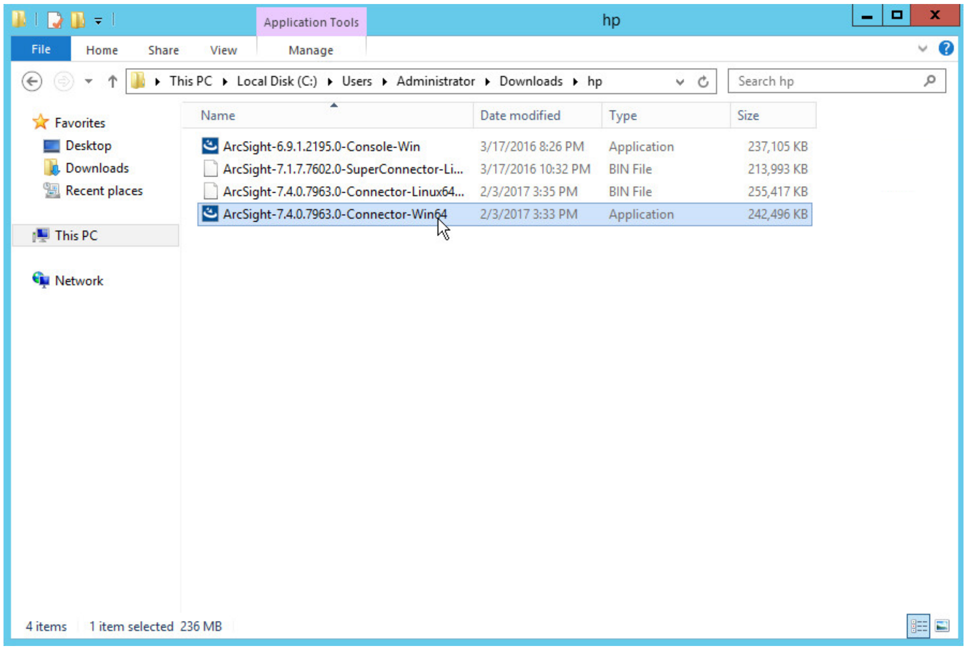


Name	PID	Description	Status	Group
arc_winc		ArcSight Microsoft Windows Event L...	Starting	
WSearch	2904	Windows Search	Running	
WMPNetworkSvc		Windows Media Player Network Sha...	Stopped	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend	3952	Windows Defender Antivirus Service	Running	
WdNisSvc	2016	Windows Defender Antivirus Networ...	Running	
wbengine		Block Level Backup Engine Service	Stopped	
VSS		Volume Shadow Copy	Stopped	
vds		Virtual Disk	Stopped	
VaultSvc	660	Credential Manager	Running	
UI0Detect		Interactive Services Detection	Stopped	
UevAgentService		User Experience Virtualization Service	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	2068	Print Spooler	Running	
spectrum		Windows Perception Service	Stopped	
SNMPTRAP		SNMP Trap	Stopped	
SensorDataService		Sensor Data Service	Stopped	
Sense		Windows Defender Advanced Threat...	Stopped	
SecurityHealthService	2680	Windows Defender Security Center S...	Running	
SamSs	660	Security Accounts Manager	Running	
RpcLocator		Remote Procedure Call (RPC) Locator	Stopped	

41. The machine will now report its logs to ArcSight ESM.

2.6.2 Install a Connector Server for ESM on Windows 2012 R2

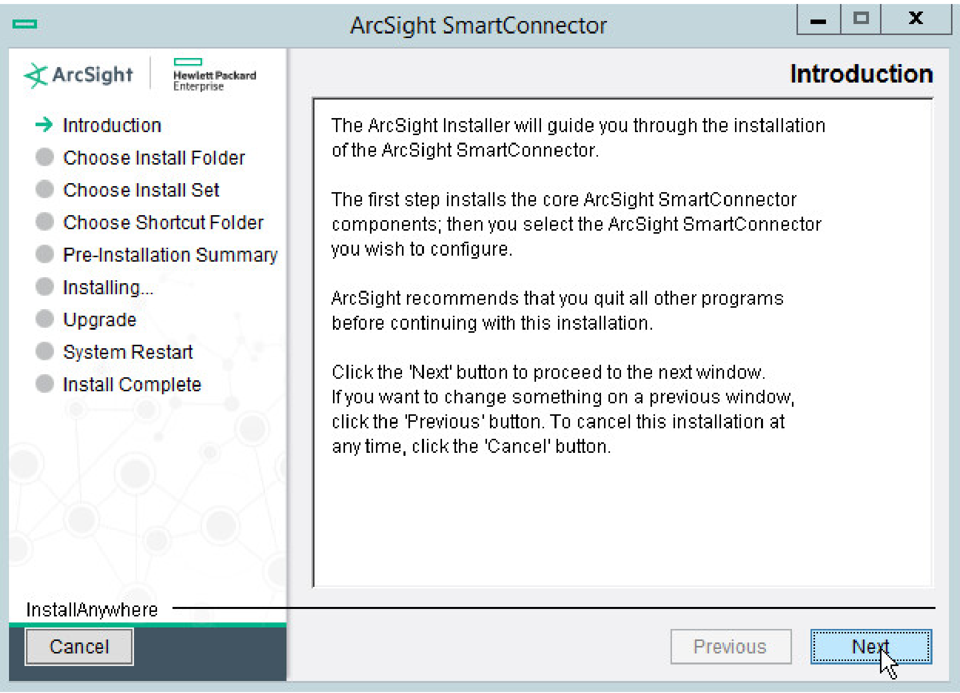
1. Run the installation file **ArcSight-7.4.0.7963.0-Connector-Win64**.



Name	Date modified	Type	Size
ArcSight-6.9.1.2195.0-Console-Win	3/17/2016 8:26 PM	Application	237,105 KB
ArcSight-7.1.7.7602.0-SuperConnector-Li...	3/17/2016 10:32 PM	BIN File	213,993 KB
ArcSight-7.4.0.7963.0-Connector-Linux64...	2/3/2017 3:35 PM	BIN File	255,417 KB
ArcSight-7.4.0.7963.0-Connector-Win64	2/3/2017 3:33 PM	Application	242,496 KB

4 items 1 item selected 236 MB

2. Wait for the initial setup to finish.



Introduction

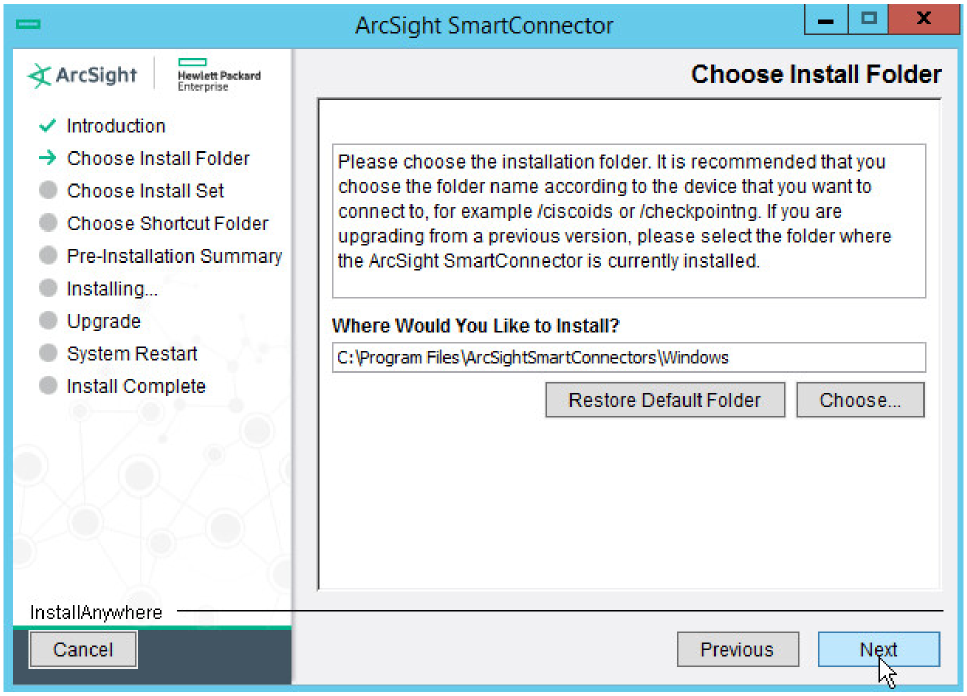
The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector.

The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.

3. Click **Next**.
4. Choose a destination folder. Note: It is recommended to change the default destination folder to `<default>\Windows`. This is to avoid conflicts if you wish to install more than one connector.



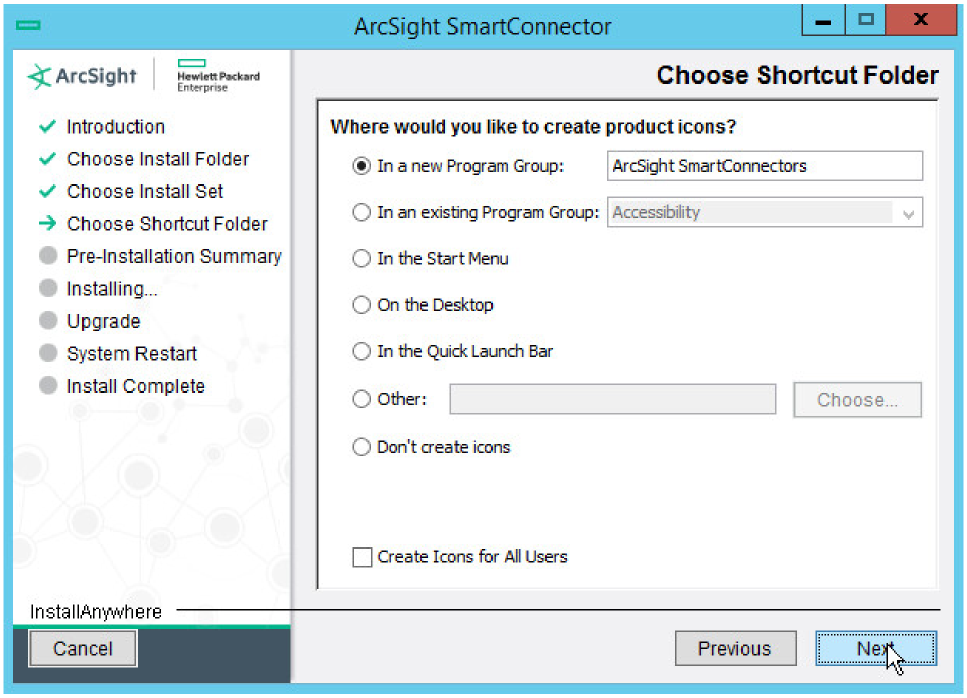
Choose Install Folder

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

5. Click **Next**.



Choose Shortcut Folder

Where would you like to create product icons?

● In a new Program Group: ArcSight SmartConnectors

○ In an existing Program Group: Accessibility

○ In the Start Menu

○ On the Desktop

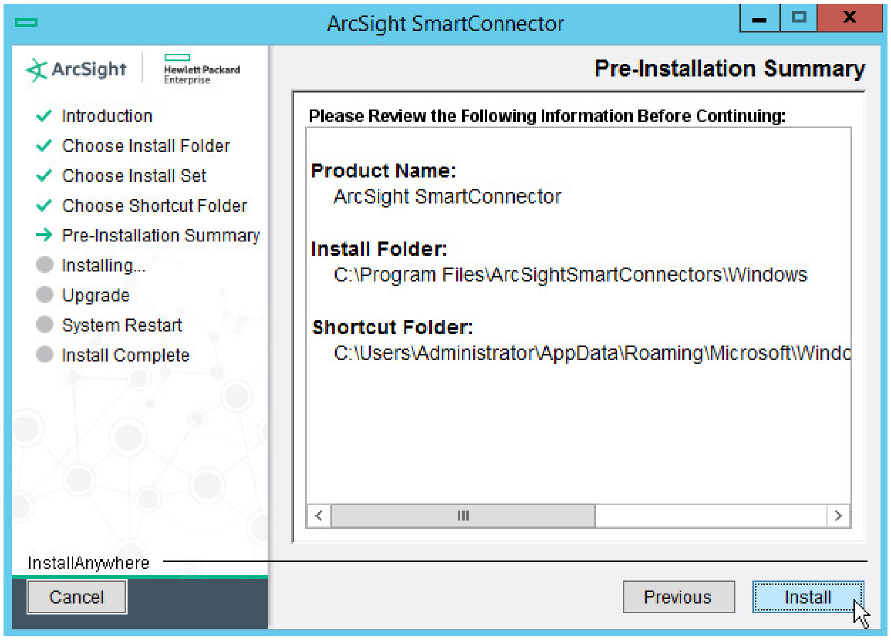
○ In the Quick Launch Bar

○ Other:

○ Don't create icons

□ Create Icons for All Users

6. Click **Next**.



Pre-Installation Summary

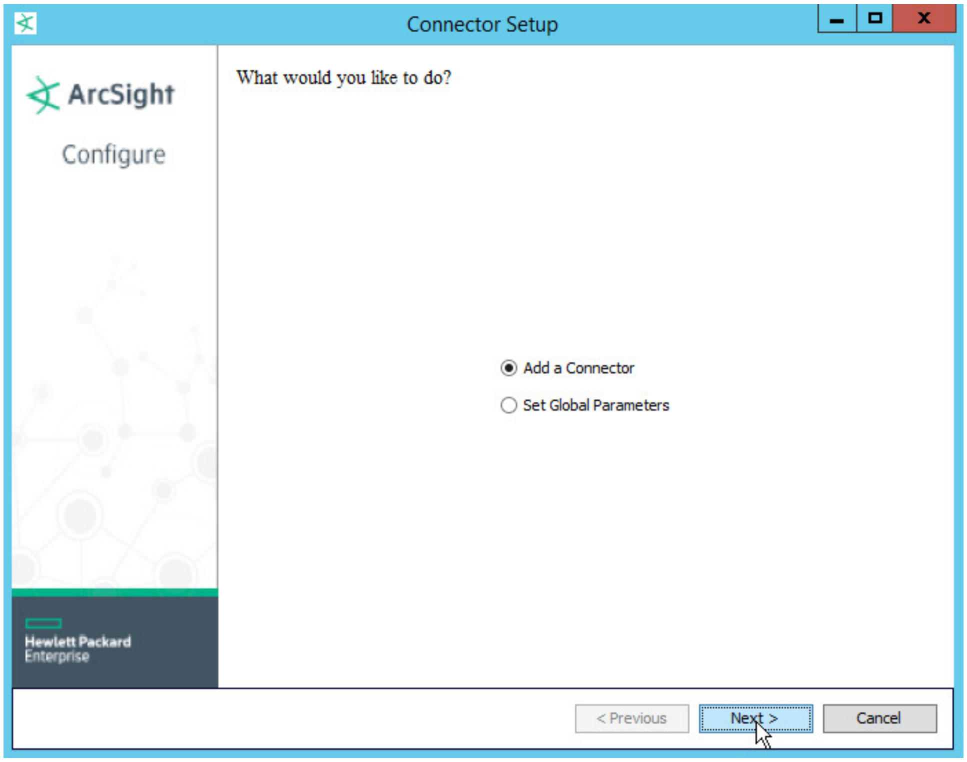
Please Review the Following Information Before Continuing:

Product Name:
ArcSight SmartConnector

Install Folder:
C:\Program Files\ArcSightSmartConnectors\Windows

Shortcut Folder:
C:\Users\Administrator\AppData\Roaming\Microsoft\Windo

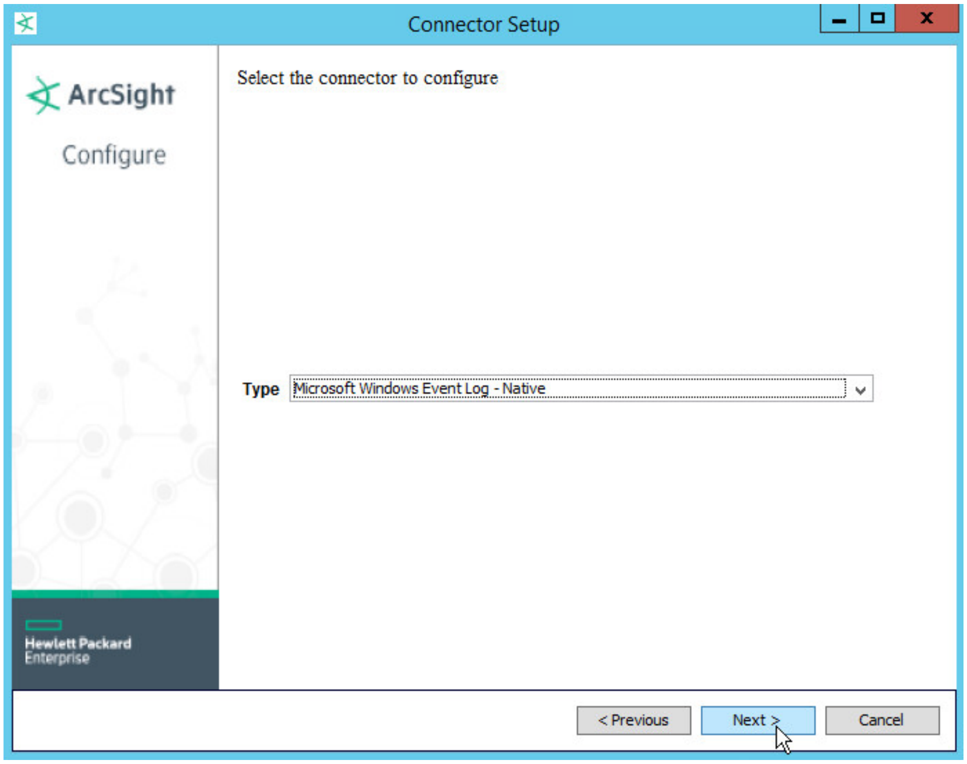
7. Click **Install**.
8. Wait for the installation to finish.
9. Select **Add a Connector**.



What would you like to do?

● Add a Connector
○ Set Global Parameters

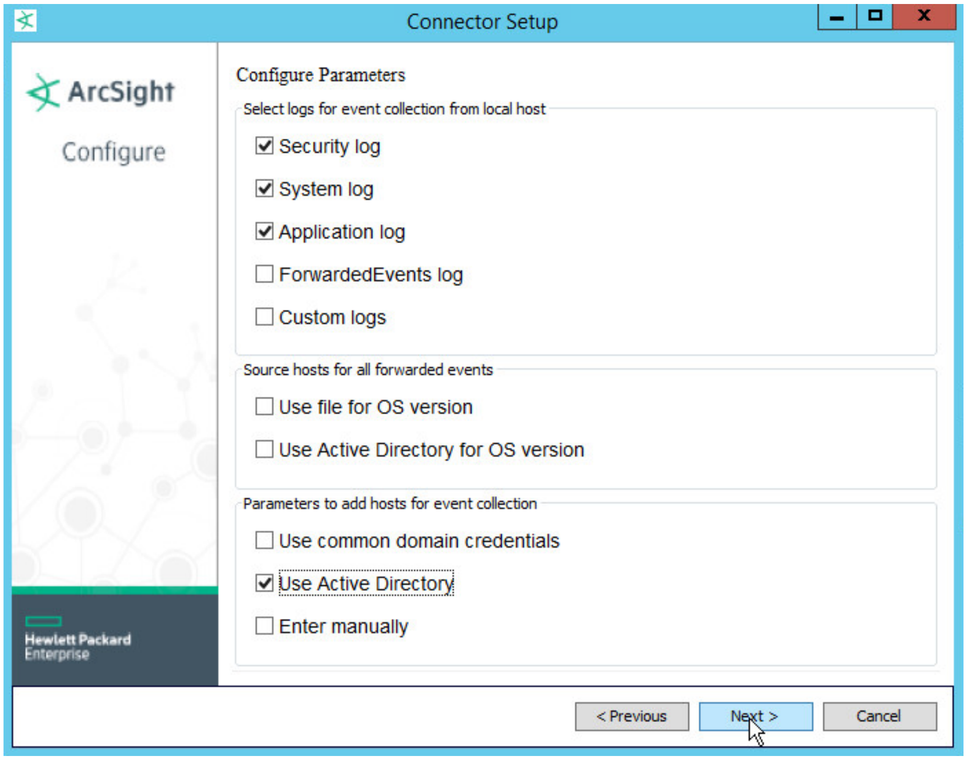
10. Click **Next**.
11. Choose **Microsoft Windows Event Log - Native** from the list.



Select the connector to configure

Type Microsoft Windows Event Log - Native

12. Click **Next**.
13. Check **Security log**, **System log**, **Application Log**.
14. Check **Use Active Directory**.



Configure Parameters

Select logs for event collection from local host

- ☑ Security log
- ☑ System log
- ☑ Application log
- □ ForwardedEvents log
- □ Custom logs

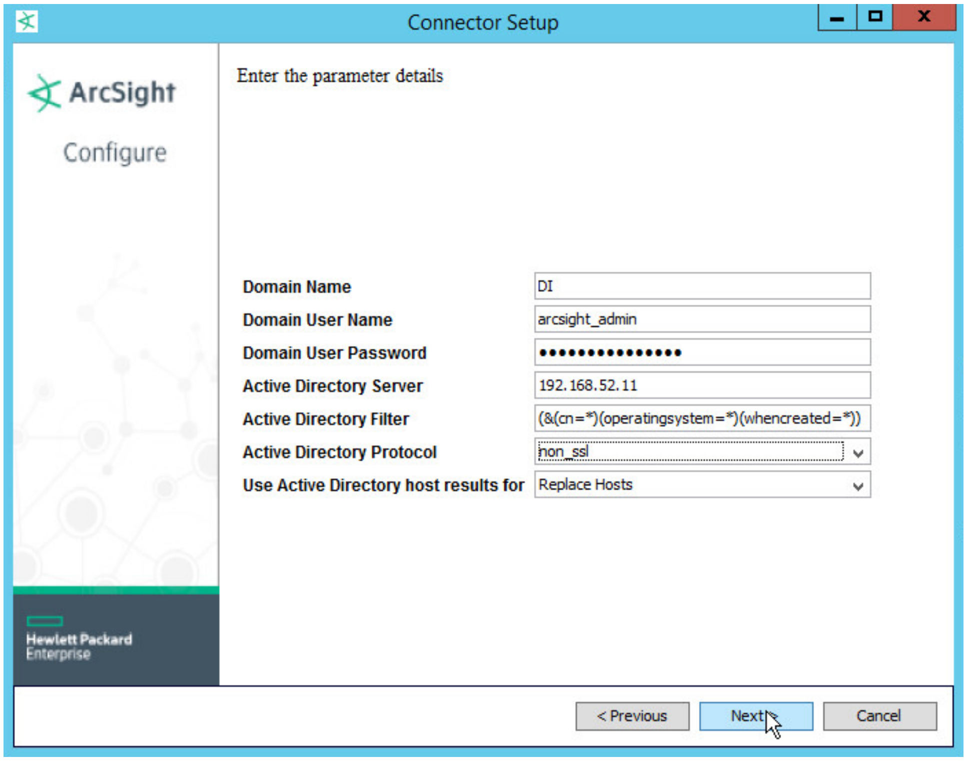
Source hosts for all forwarded events

- □ Use file for OS version
- □ Use Active Directory for OS version

Parameters to add hosts for event collection

- □ Use common domain credentials
- ☑ Use Active Directory
- □ Enter manually

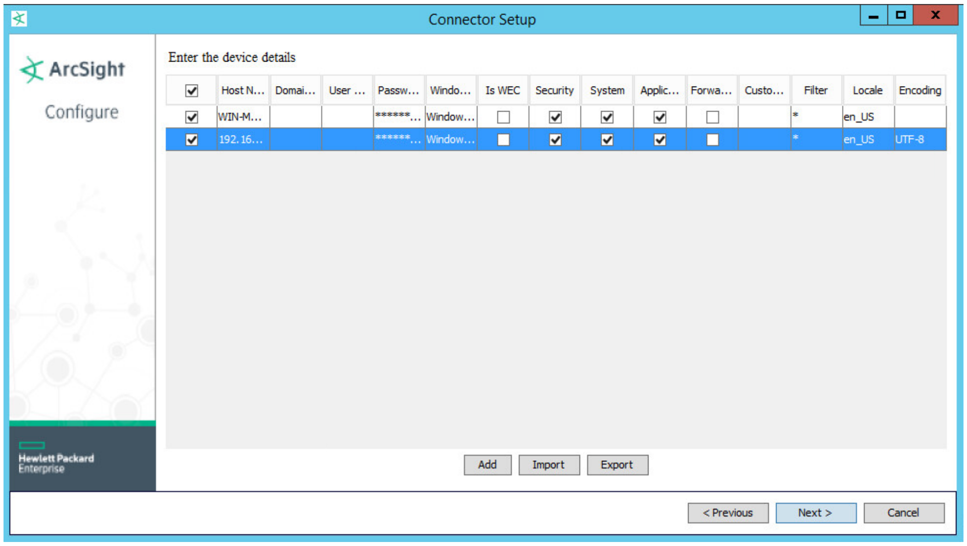
15. Click **Next**.
16. Fill out the form with the appropriate information for your Active Directory server. It is recommended to create an account on Active Directory specifically for ArcSight.
17. Select **Replace Hosts** for **Use Active Directory host results for**.



Enter the parameter details

Domain Name	DI
Domain User Name	arcsight_admin
Domain User Password	•••••••••••••••
Active Directory Server	192.168.52.11
Active Directory Filter	(&(cn=*)(operatingsystem=*)(whencreated=*))
Active Directory Protocol	non_ssl
Use Active Directory host results for	Replace Hosts

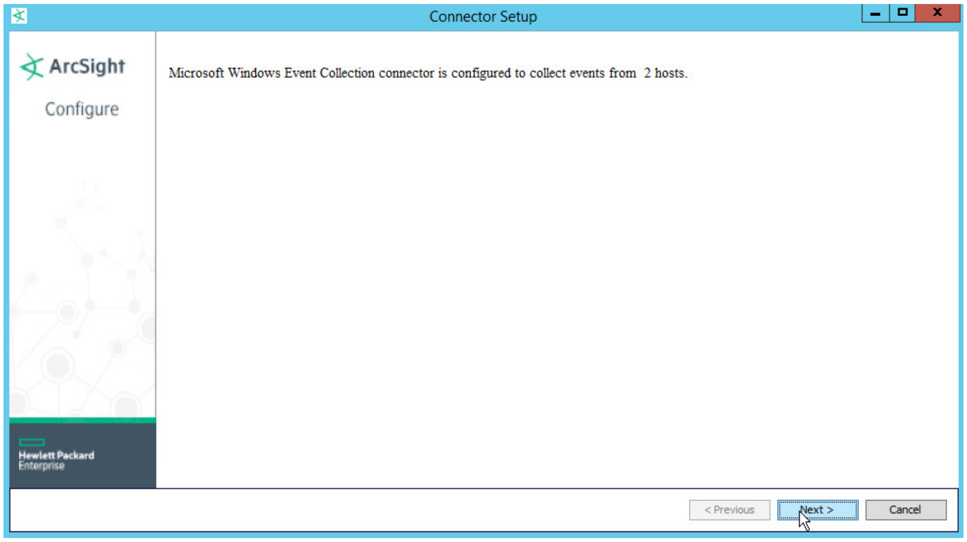
18. Click **Next**.
19. Select all the event types you would like forwarded from each machine.



Enter the device details

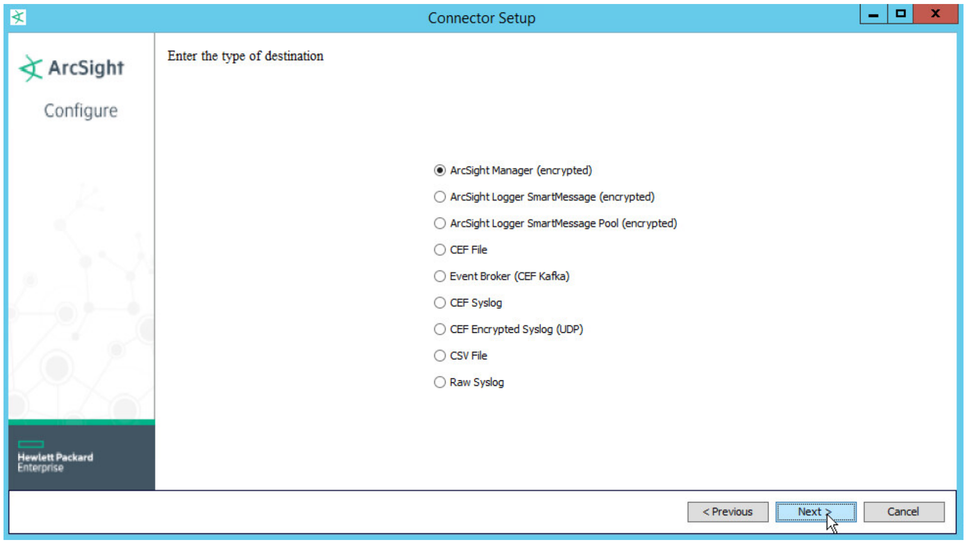
☑	Host N...	Domai...	User ...	Passw...	Windo...	Is WEC	Security	System	Applic...	Forwa...	Custo...	Filter	Locale	Encoding
☑	WIN-M...			******...	Window...	☐	☑	☑	☑	☐		*	en_US	
☑	192.16...			******...	Window...	☐	☑	☑	☑	☐		*	en_US	UTF-8

20. Click **Next**.



Microsoft Windows Event Collection connector is configured to collect events from 2 hosts.

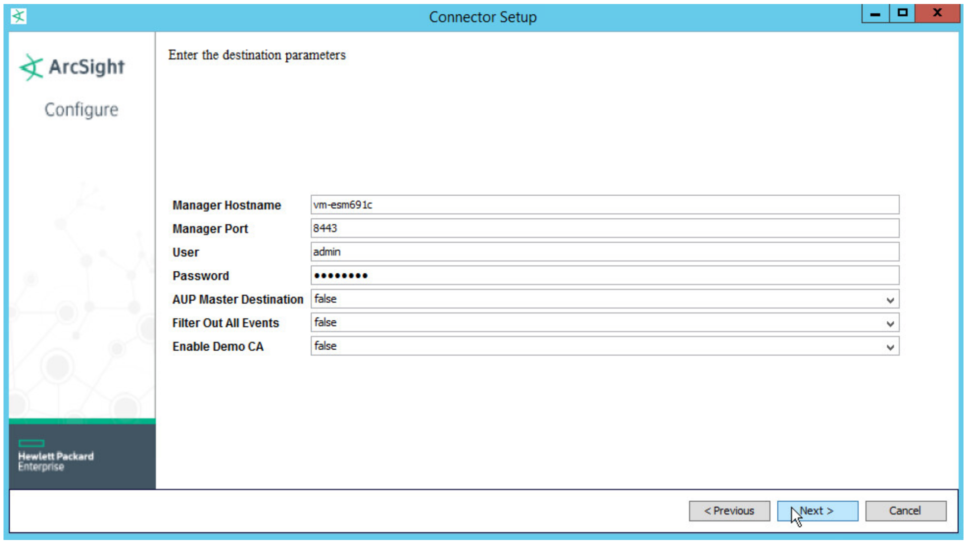
21. Click **Next**.
22. Choose **ArcSight Manager (encrypted)**.



Enter the type of destination

● ArcSight Manager (encrypted)
○ ArcSight Logger SmartMessage (encrypted)
○ ArcSight Logger SmartMessage Pool (encrypted)
○ CEF File
○ Event Broker (CEF Kafka)
○ CEF Syslog
○ CEF Encrypted Syslog (UDP)
○ CSV File
○ Raw Syslog

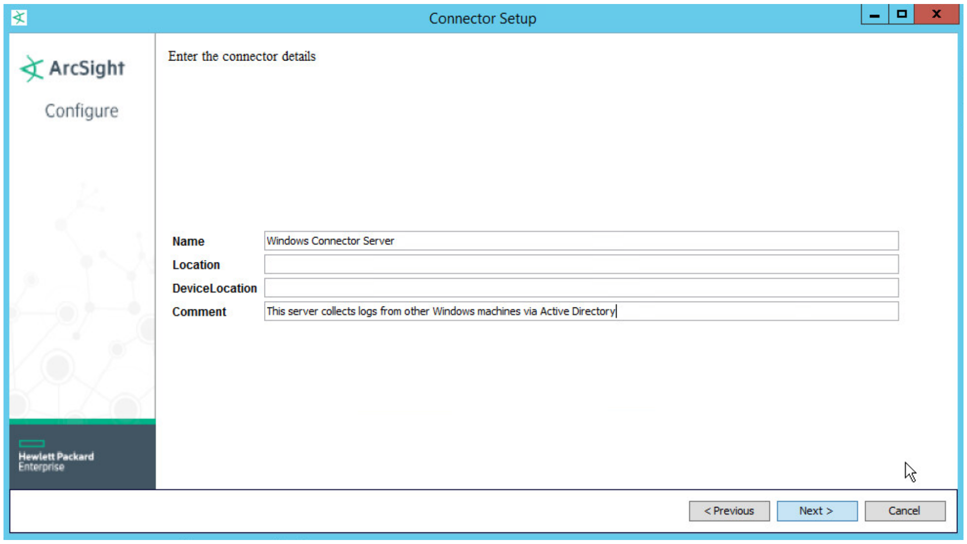
23. Click **Next**.
24. For **Manager Hostname**, use **vm-esm691c** or the hostname of your ESM server.
25. For **Manager Port**, use **8443** (or the port that ESM is running on) on the ESM server.
26. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)



Enter the destination parameters

Manager Hostname	vm-esm691c
Manager Port	8443
User	admin
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

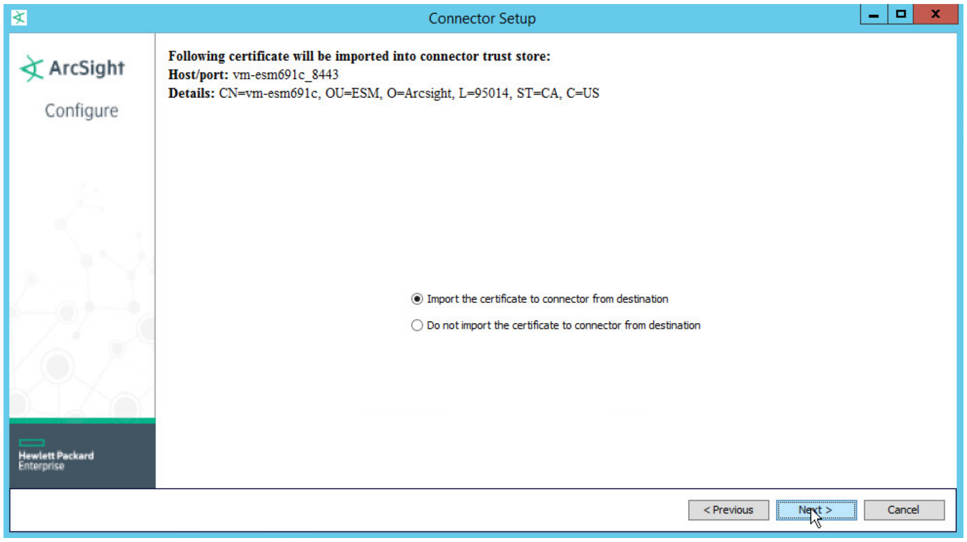
27. Click **Next**.
28. Set identifying details about the system to help identify the connector (include **Name;** the rest is optional).



Enter the connector details

Name	Windows Connector Server
Location	
DeviceLocation	
Comment	This server collects logs from other Windows machines via Active Directory

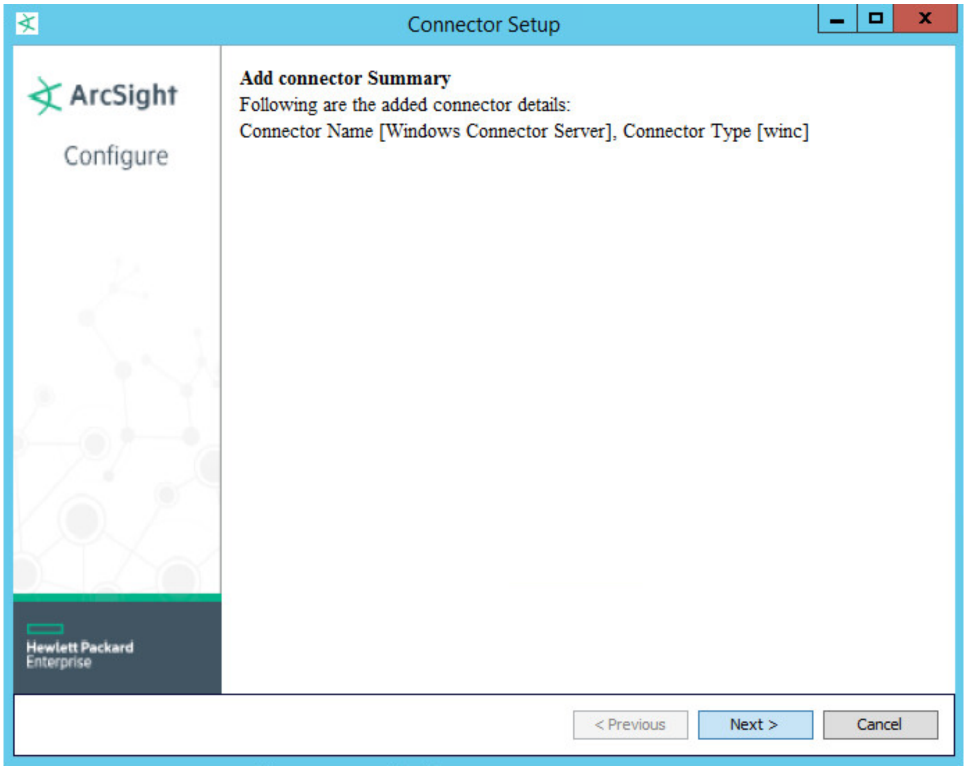
29. Click **Next**.
30. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the VM.



Following certificate will be imported into connector trust store:
Host/port: vm-esm691c_8443
Details: CN=vm-esm691c, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

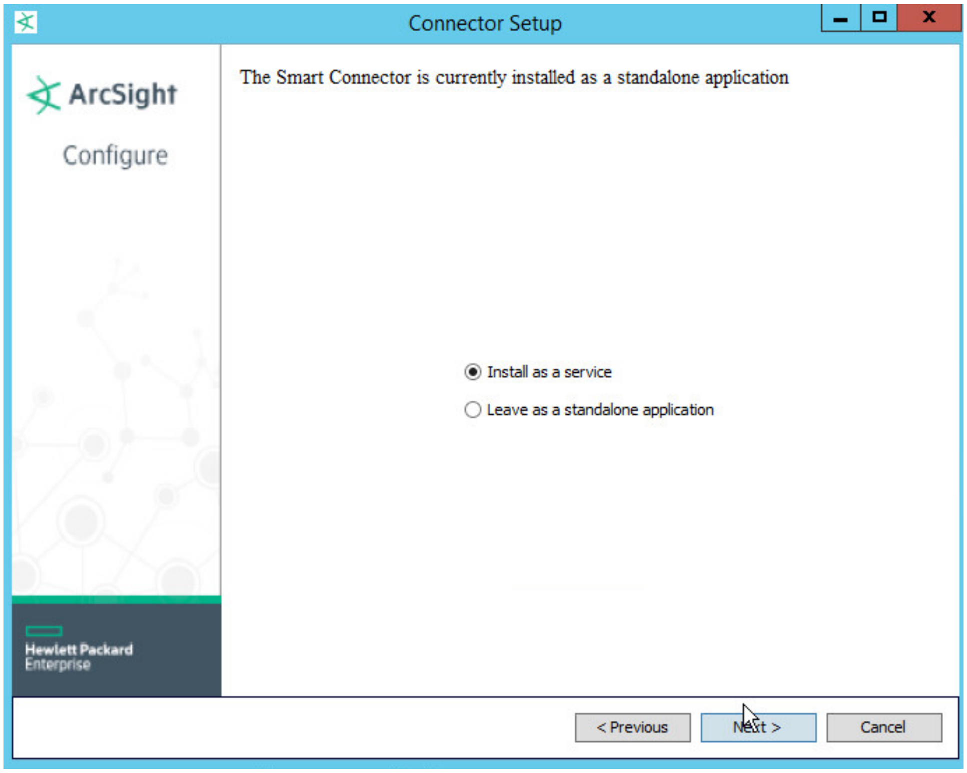
● Import the certificate to connector from destination
○ Do not import the certificate to connector from destination

31. Click **Next**.



Add connector Summary
Following are the added connector details:
Connector Name [Windows Connector Server], Connector Type [winc]

32. Click **Next**.
33. Choose **Install as a service**.

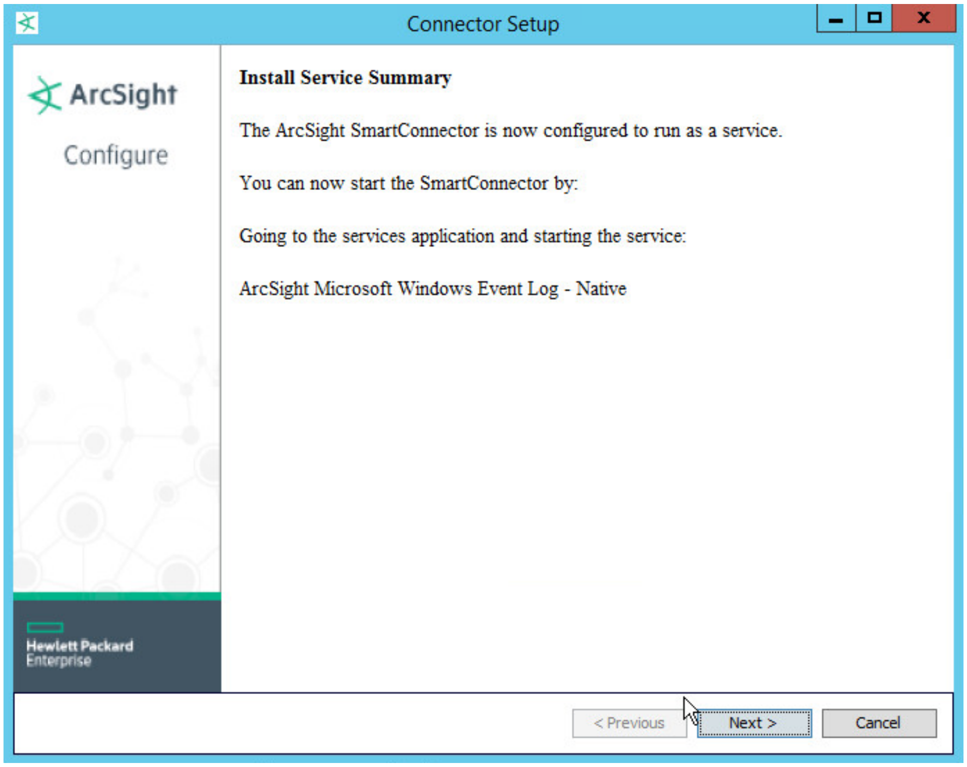


The Smart Connector is currently installed as a standalone application

● Install as a service

○ Leave as a standalone application

34. Click **Next**.



Install Service Summary

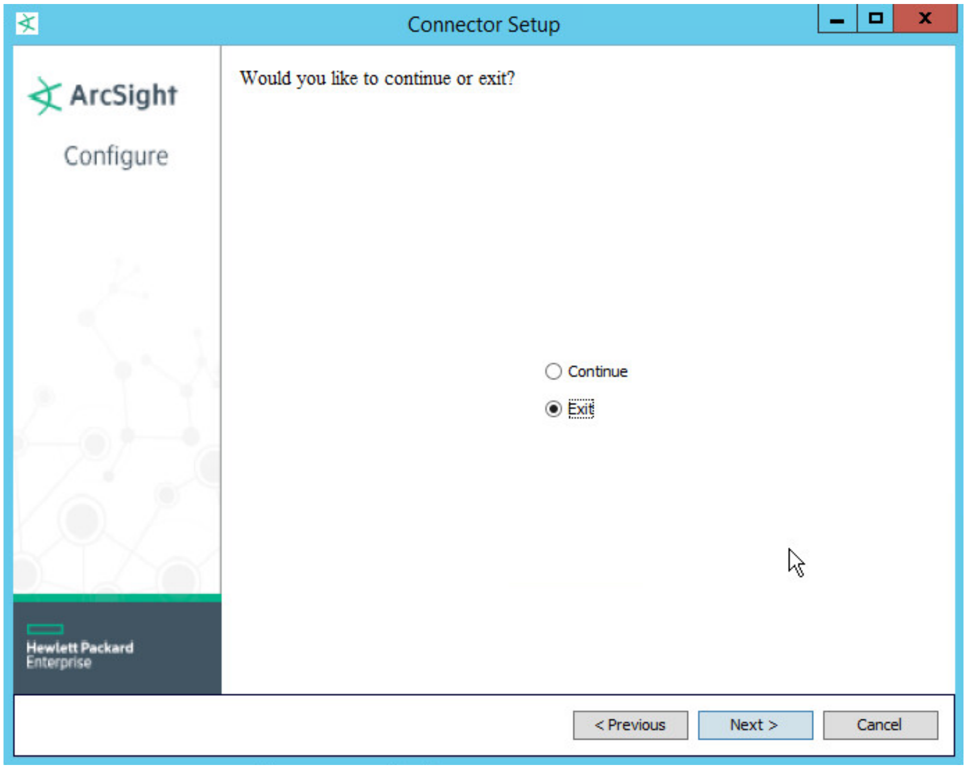
The ArcSight SmartConnector is now configured to run as a service.

You can now start the SmartConnector by:

Going to the services application and starting the service:

ArcSight Microsoft Windows Event Log - Native

35. Click **Next**.
36. Choose **Exit**.

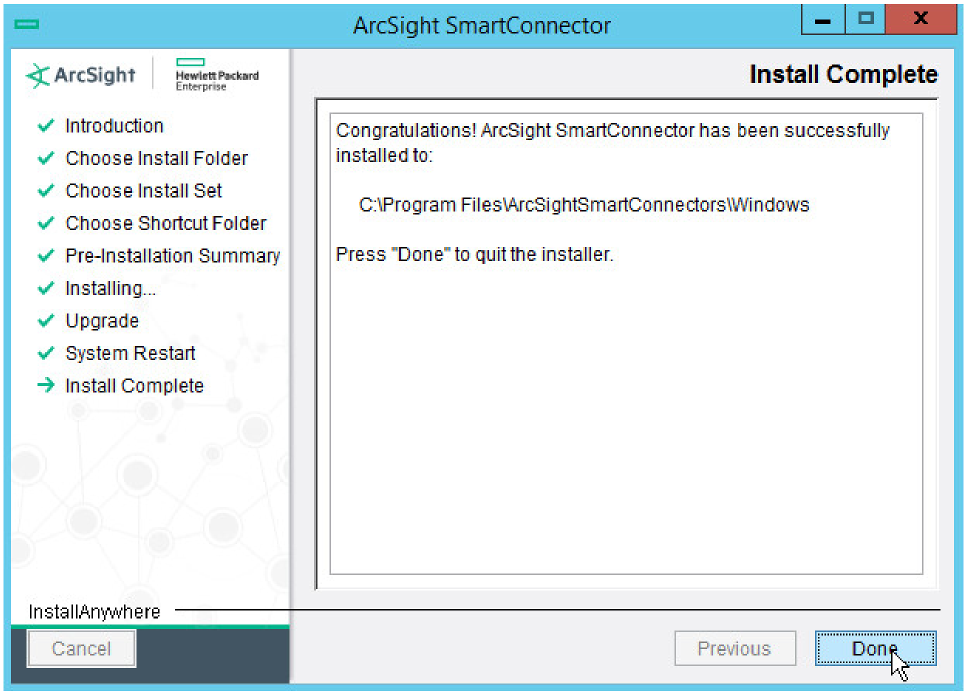


Would you like to continue or exit?

○ Continue

● Exit

37. Click **Next**.



Install Complete

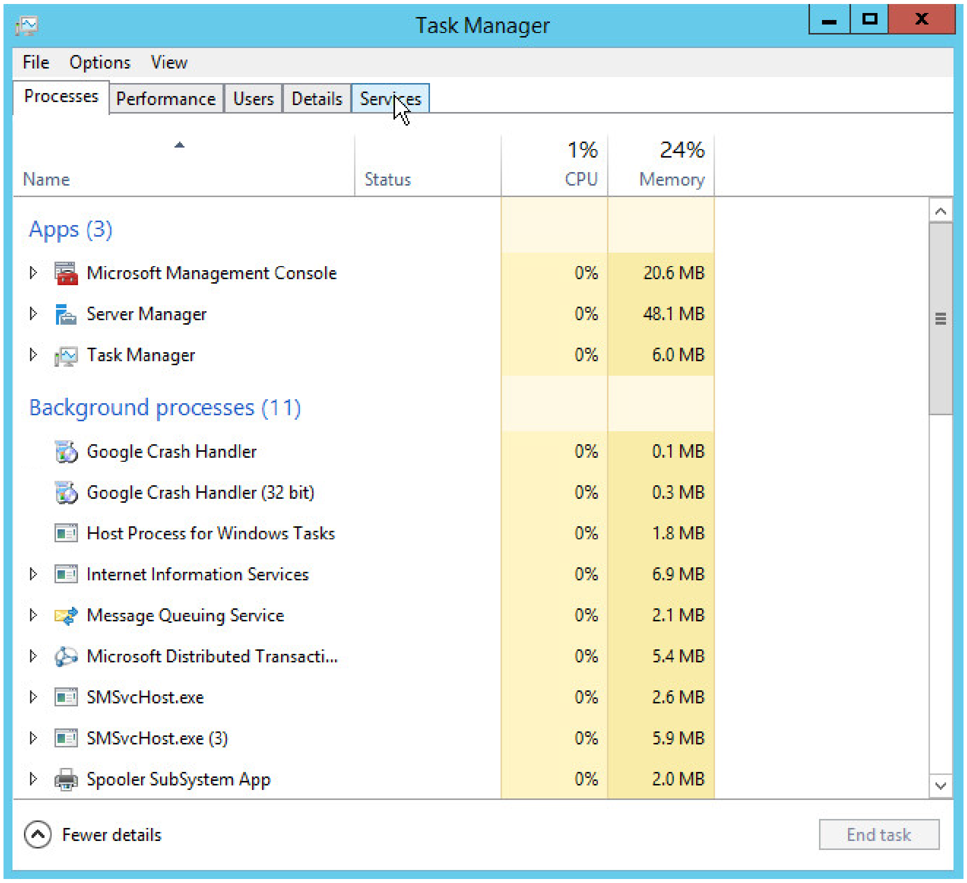
Congratulations! ArcSight SmartConnector has been successfully installed to:

C:\Program Files\ArcSightSmartConnectors\Windows

Press "Done" to quit the installer.

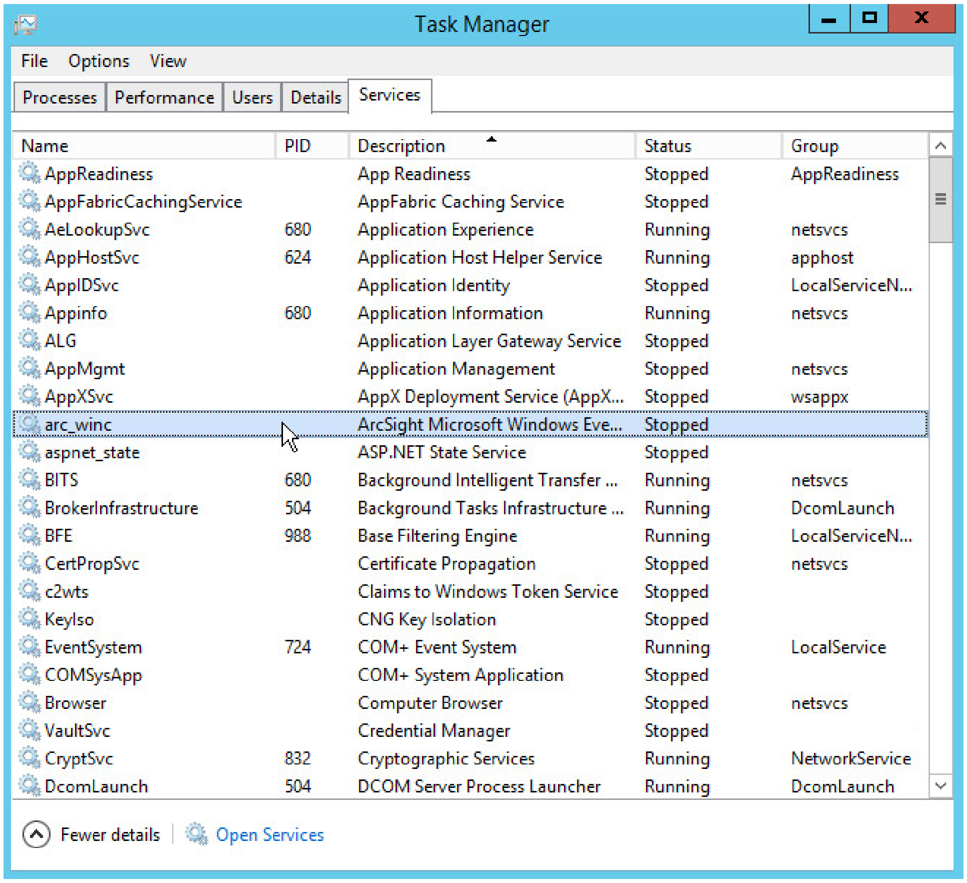
38. Click **Done**.

39. Open **Task Manager**.
40. Click **More Details**.



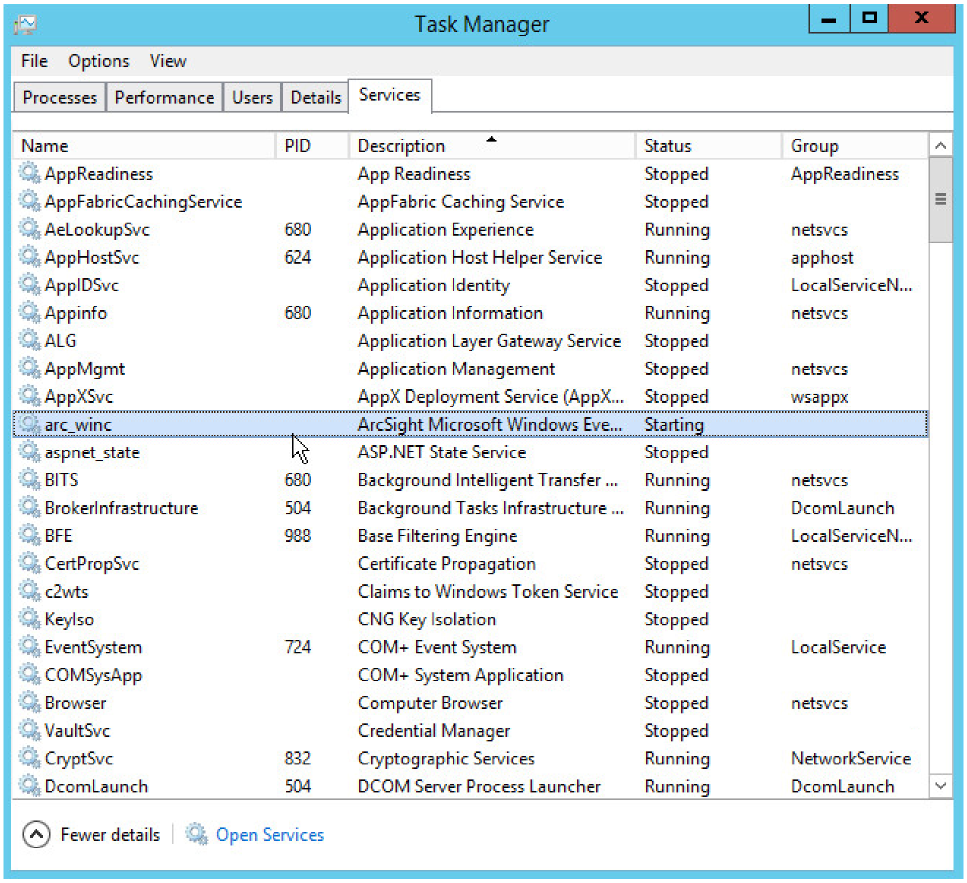
Name	Status	1% CPU	24% Memory
Apps (3)			
Microsoft Management Console		0%	20.6 MB
Server Manager		0%	48.1 MB
Task Manager		0%	6.0 MB
Background processes (11)			
Google Crash Handler		0%	0.1 MB
Google Crash Handler (32 bit)		0%	0.3 MB
Host Process for Windows Tasks		0%	1.8 MB
Internet Information Services		0%	6.9 MB
Message Queuing Service		0%	2.1 MB
Microsoft Distributed Transacti...		0%	5.4 MB
SMSvcHost.exe		0%	2.6 MB
SMSvcHost.exe (3)		0%	5.9 MB
Spooler SubSystem App		0%	2.0 MB

41. Go to the **Services** tab.
42. Find the service just created for ArcSight and right click it.



Name	PID	Description	Status	Group
AppReadiness		App Readiness	Stopped	AppReadiness
AppFabricCachingService		AppFabric Caching Service	Stopped	
AeLookupSvc	680	Application Experience	Running	netsvcs
AppHostSvc	624	Application Host Helper Service	Running	apphost
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo	680	Application Information	Running	netsvcs
ALG		Application Layer Gateway Service	Stopped	
AppMgmt		Application Management	Stopped	netsvcs
AppXSvc		AppX Deployment Service (AppX...	Stopped	wsappx
arc_winc		ArcSight Microsoft Windows Eve...	Stopped	
aspnet_state		ASP.NET State Service	Stopped	
BITS	680	Background Intelligent Transfer ...	Running	netsvcs
BrokerInfrastructure	504	Background Tasks Infrastructure ...	Running	DcomLaunch
BFE	988	Base Filtering Engine	Running	LocalServiceN...
CertPropSvc		Certificate Propagation	Stopped	netsvcs
c2wts		Claims to Windows Token Service	Stopped	
KeyIso		CNG Key Isolation	Stopped	
EventSystem	724	COM+ Event System	Running	LocalService
COMSysApp		COM+ System Application	Stopped	
Browser		Computer Browser	Stopped	netsvcs
VaultSvc		Credential Manager	Stopped	
CryptSvc	832	Cryptographic Services	Running	NetworkService
DcomLaunch	504	DCOM Server Process Launcher	Running	DcomLaunch

43. Choose **Start**.

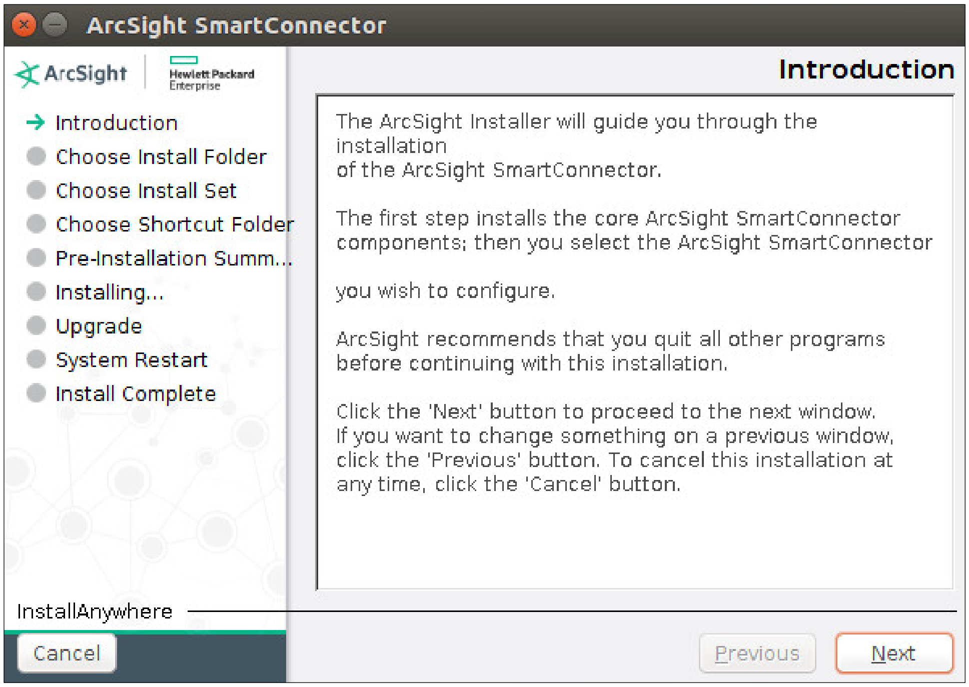


Name	PID	Description	Status	Group
AppReadiness		App Readiness	Stopped	AppReadiness
AppFabricCachingService		AppFabric Caching Service	Stopped	
AeLookupSvc	680	Application Experience	Running	netsvcs
AppHostSvc	624	Application Host Helper Service	Running	apphost
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo	680	Application Information	Running	netsvcs
ALG		Application Layer Gateway Service	Stopped	
AppMgmt		Application Management	Stopped	netsvcs
AppXSvc		AppX Deployment Service (AppX...	Stopped	wsappx
arc_winc		ArcSight Microsoft Windows Eve...	Starting	
aspnet_state		ASP.NET State Service	Stopped	
BITS	680	Background Intelligent Transfer ...	Running	netsvcs
BrokerInfrastructure	504	Background Tasks Infrastructure ...	Running	DcomLaunch
BFE	988	Base Filtering Engine	Running	LocalServiceN...
CertPropSvc		Certificate Propagation	Stopped	netsvcs
c2wts		Claims to Windows Token Service	Stopped	
KeyIso		CNG Key Isolation	Stopped	
EventSystem	724	COM+ Event System	Running	LocalService
COMSysApp		COM+ System Application	Stopped	
Browser		Computer Browser	Stopped	netsvcs
VaultSvc		Credential Manager	Stopped	
CryptSvc	832	Cryptographic Services	Running	NetworkService
DcomLaunch	504	DCOM Server Process Launcher	Running	DcomLaunch

44. The machine will now report all collected Windows logs to ArcSight ESM.

2.6.3 Install Syslog Connector for Ubuntu

1. Run `./ArcSight-7.4.0.7963.0-Connector-Linux64.bin`.



The ArcSight Installer will guide you through the
installation
of the ArcSight SmartConnector.

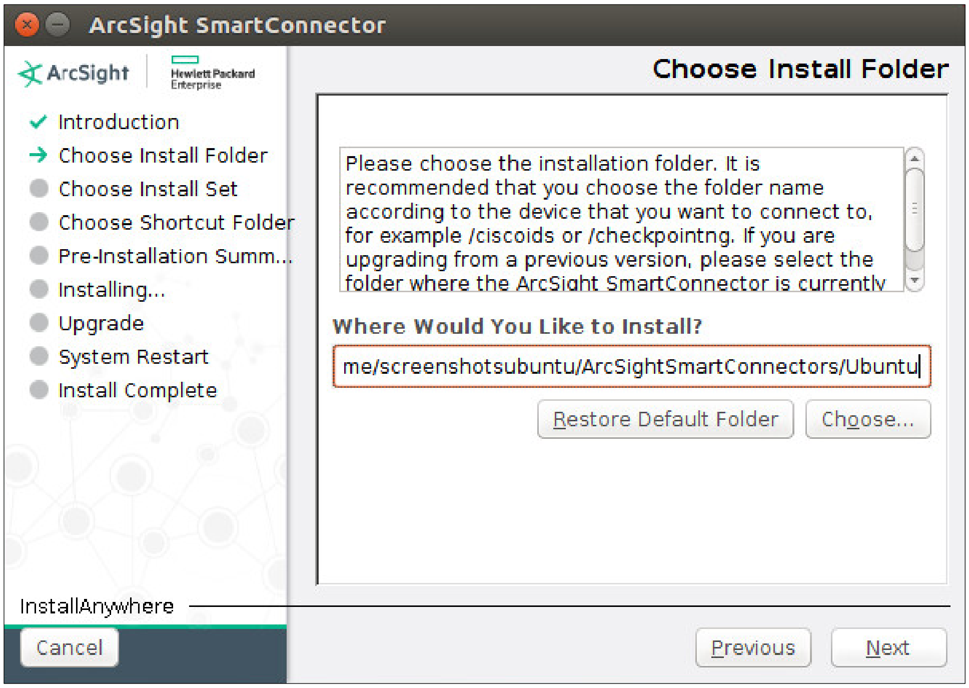
The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector

you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.

2. Click **Next**.
3. Choose a folder to install the connector in.

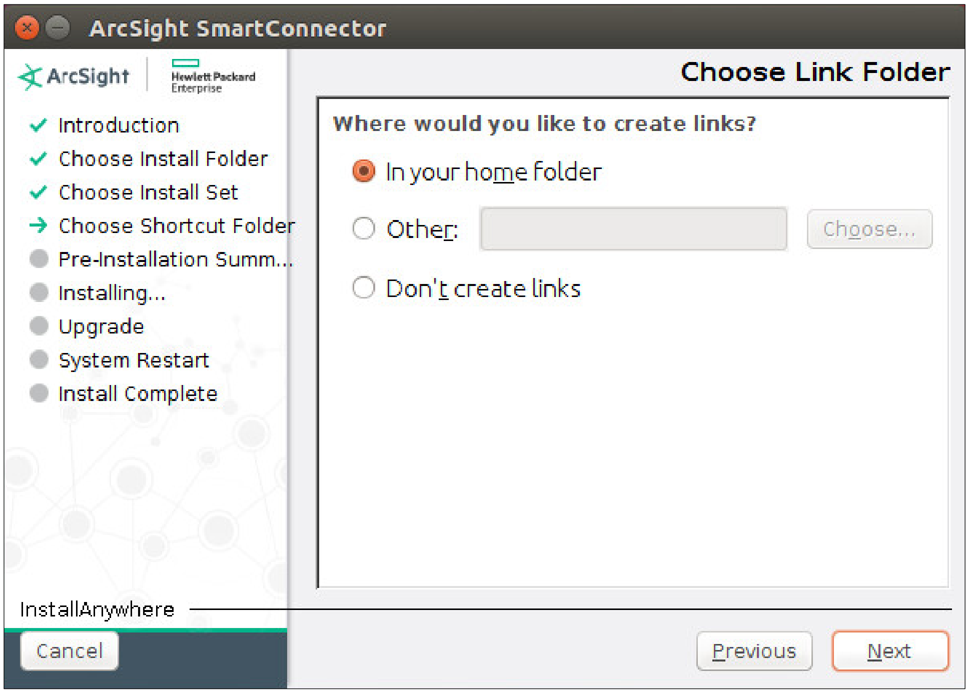


Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently

Where Would You Like to Install?

me/screenshotsubuntu/ArcSightSmartConnectors/Ubuntu

4. Click **Next**.



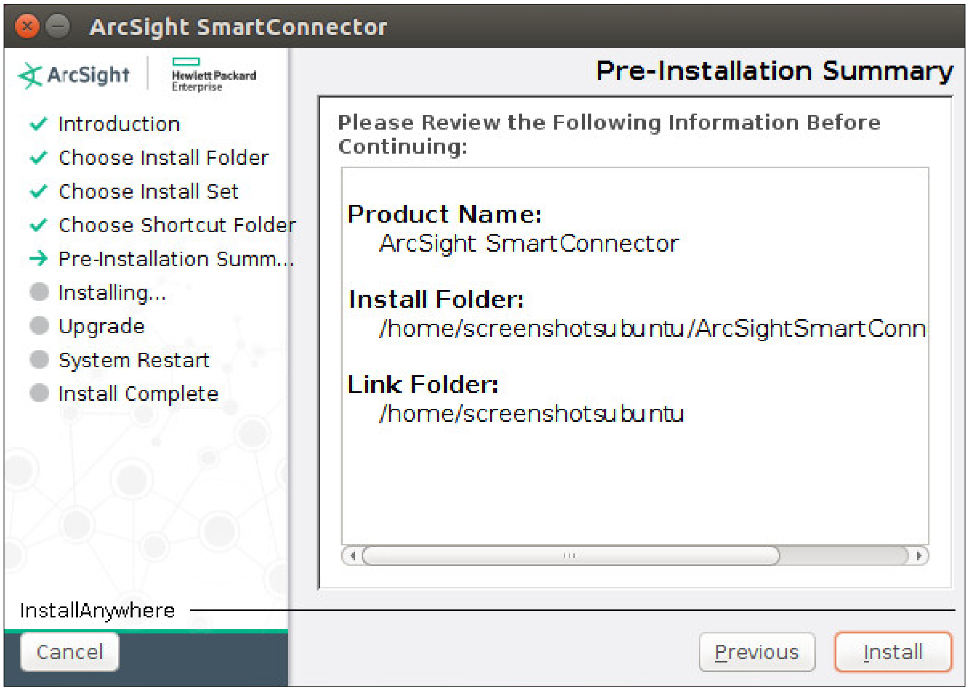
Where would you like to create links?

● In your home folder

○ Other: Choose...

○ Don't create links

5. Click **Next**.



Please Review the Following Information Before Continuing:

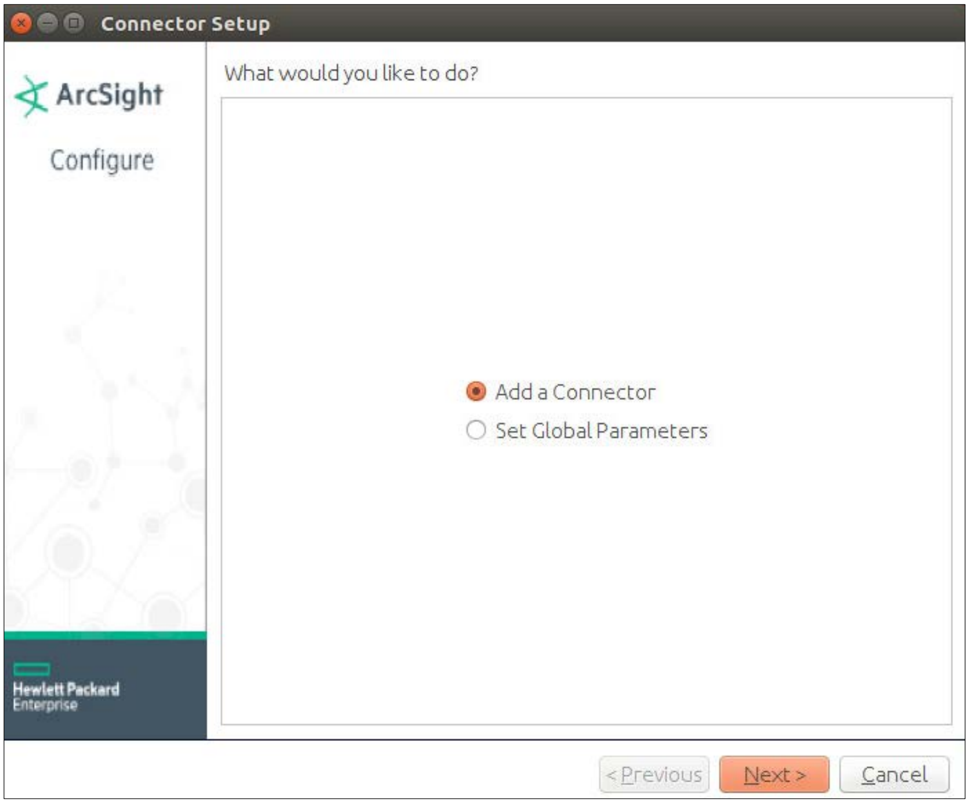
Product Name:
ArcSight SmartConnector

Install Folder:
/home/screenshotsubuntu/ArcSightSmartConn

Link Folder:
/home/screenshotsubuntu

6. Click **Install**.

7. Choose **Add a Connector.**

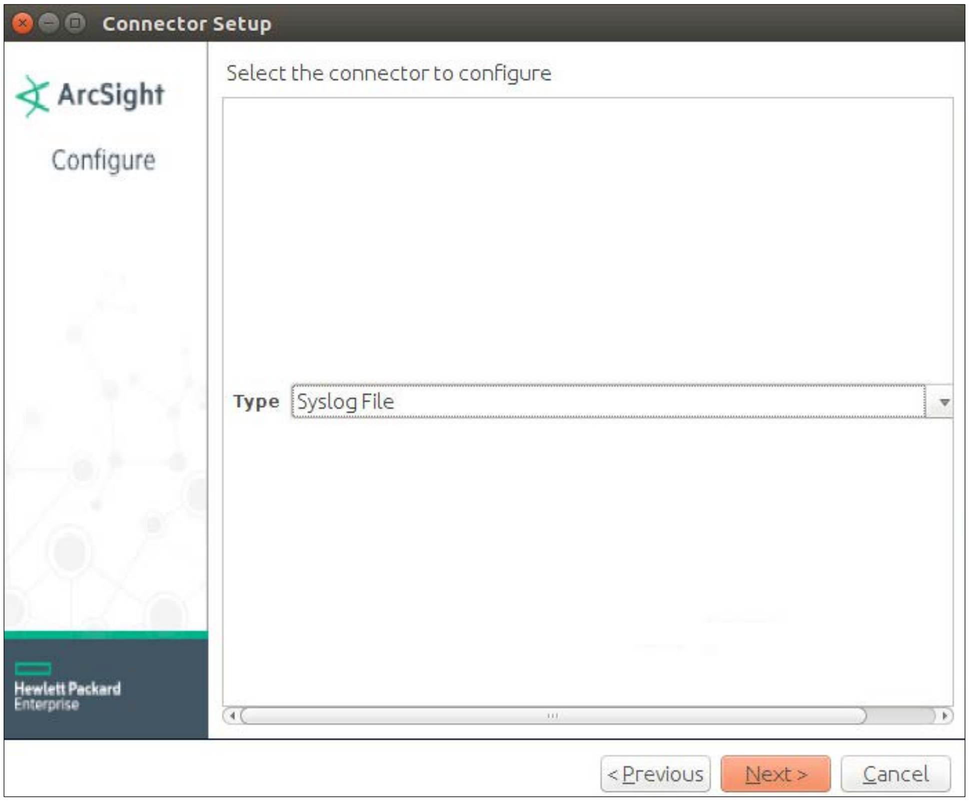


What would you like to do?

● Add a Connector

○ Set Global Parameters

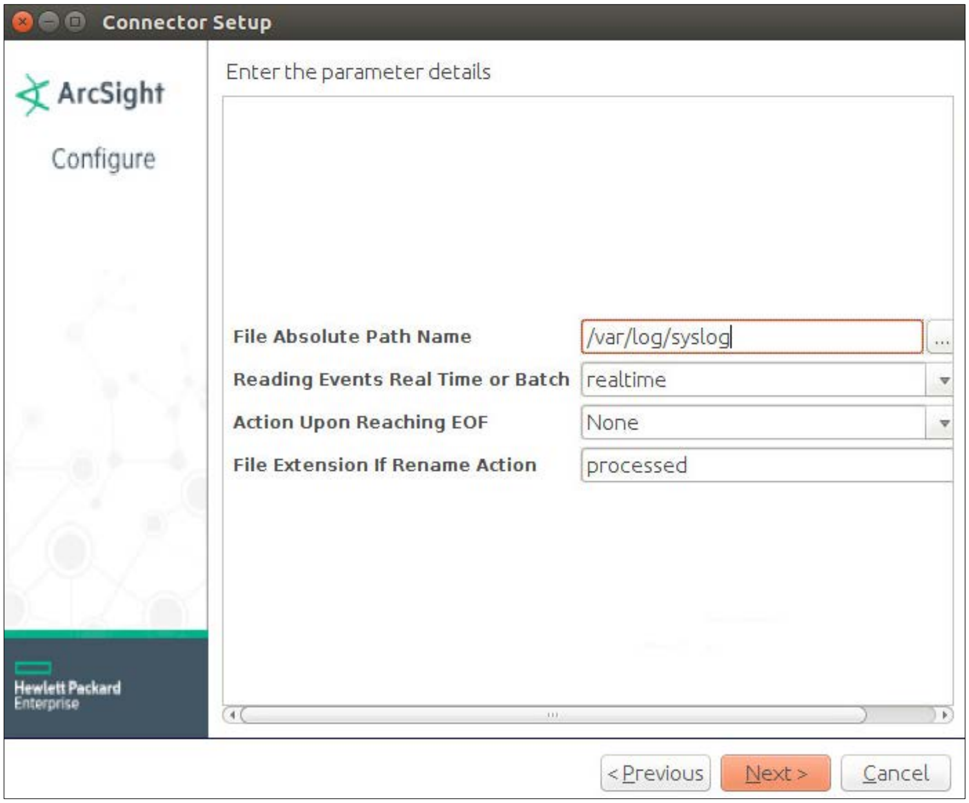
8. Click **Next**.
9. Choose **Syslog File.**



Select the connector to configure

Type: Syslog File

10. Click **Next**.
11. For **File Absolute Path Name**, select a log file from which to forward events to ESM. Example: */var/log/syslog*
12. Select **realtime** to have events be streamed or **batch** to have events sent over in sets.
13. For **Action upon Reaching EOF**, select **None**.



Enter the parameter details

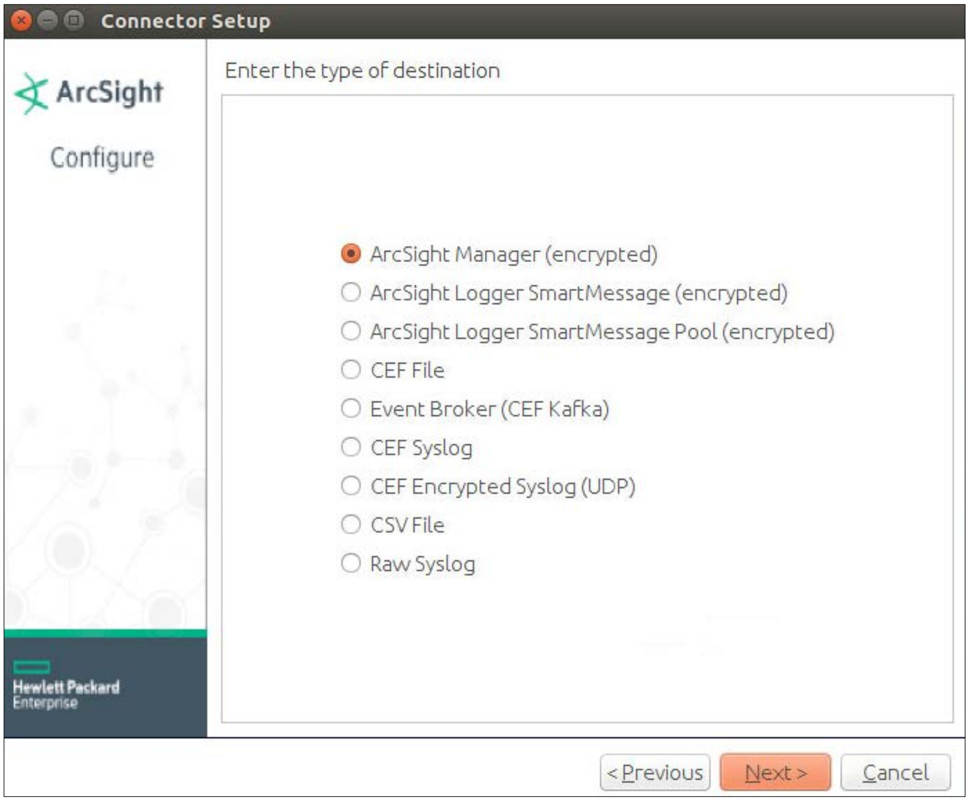
File Absolute Path Name: /var/log/syslog

Reading Events Real Time or Batch: realtime

Action Upon Reaching EOF: None

File Extension If Rename Action: processed

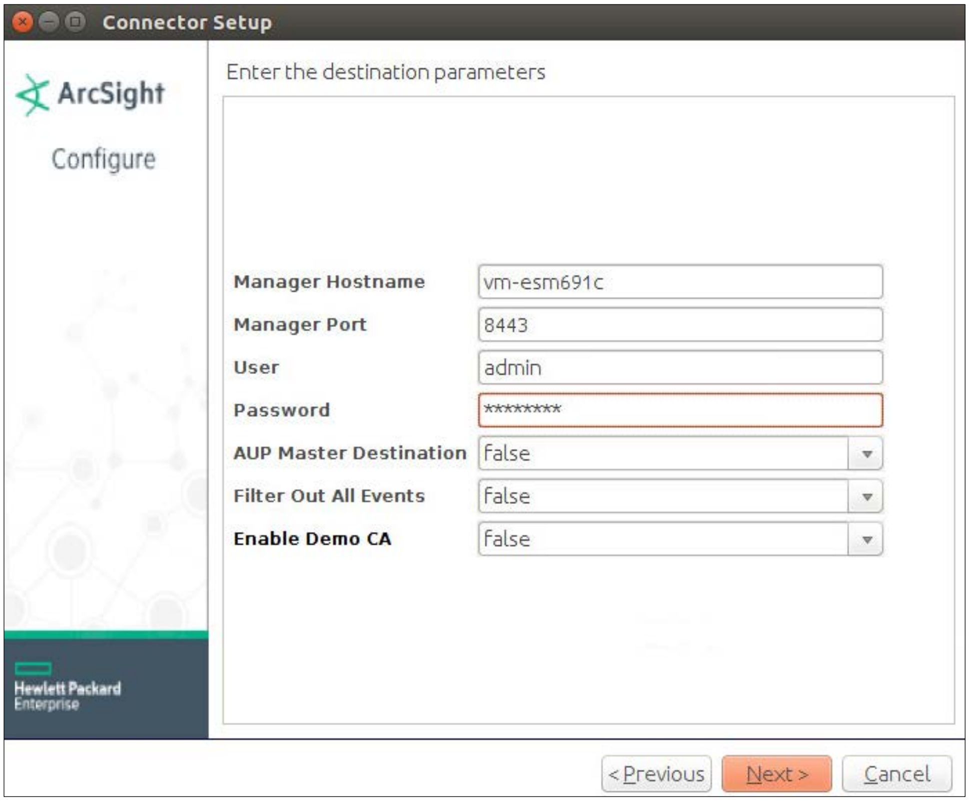
14. Click **Next**.
15. Select **ArcSight Manager (encrypted)**.



Enter the type of destination

● ArcSight Manager (encrypted)
○ ArcSight Logger SmartMessage (encrypted)
○ ArcSight Logger SmartMessage Pool (encrypted)
○ CEF File
○ Event Broker (CEF Kafka)
○ CEF Syslog
○ CEF Encrypted Syslog (UDP)
○ CSV File
○ Raw Syslog

16. Click **Next**.
17. For **Manager Hostname**, put **vm-esm691c** or the hostname of your ESM server. (You may need to add *dns-search.di.test* to */etc/network/interfaces* if the hostname does not resolve on its own. For example, vm-esm691c.di.test may resolve but vm-esm691c may not.)
18. For **Manager Port**, put **8443** (or the port that ESM is running on) on the ESM server.
19. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)

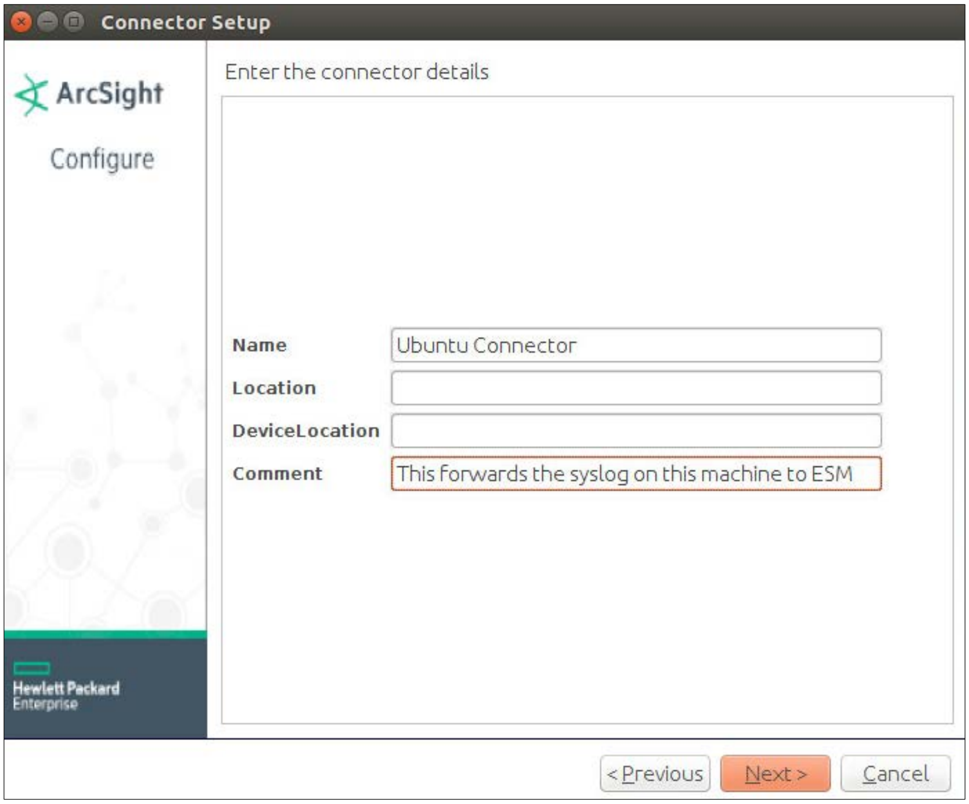


Connector Setup

Enter the destination parameters

Manager Hostname	vm-esm691c
Manager Port	8443
User	admin
Password	*********
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

20. Click **Next**.
21. Set identifying details about the system to help identify the connector (include **Name;** the rest is optional).



Enter the connector details

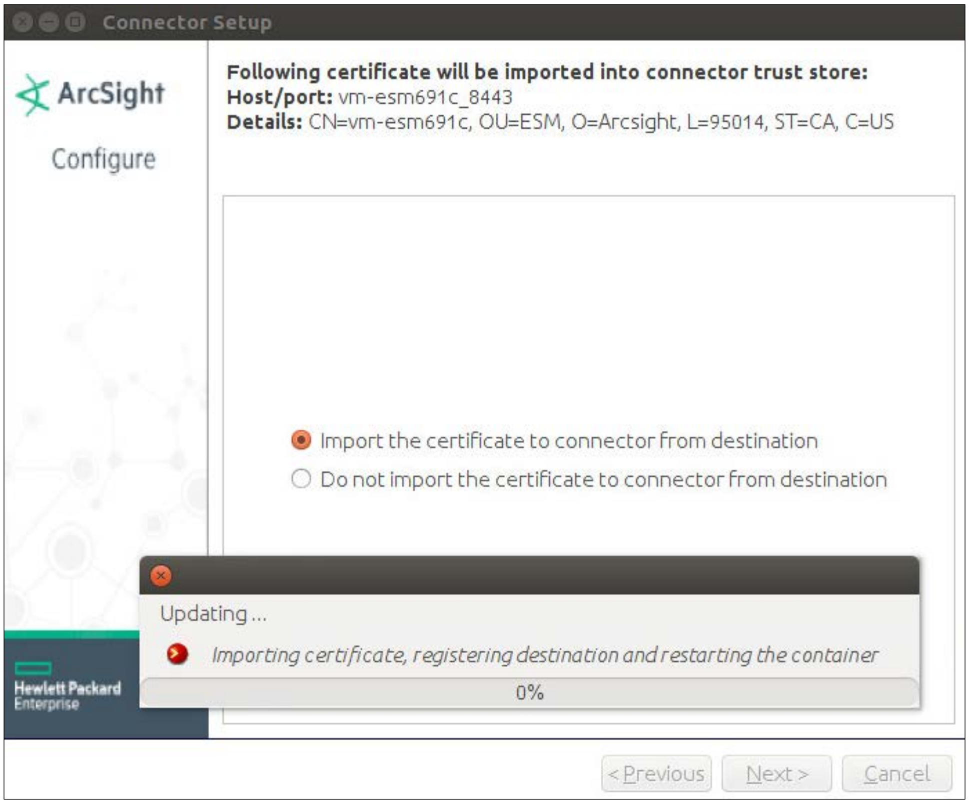
Name: Ubuntu Connector

Location:

DeviceLocation:

Comment: This forwards the syslog on this machine to ESM

22. Click **Next**.
23. Choose **Import the certificate to connector from destination**.



Following certificate will be imported into connector trust store:
Host/port: vm-esm691c_8443
Details: CN=vm-esm691c, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

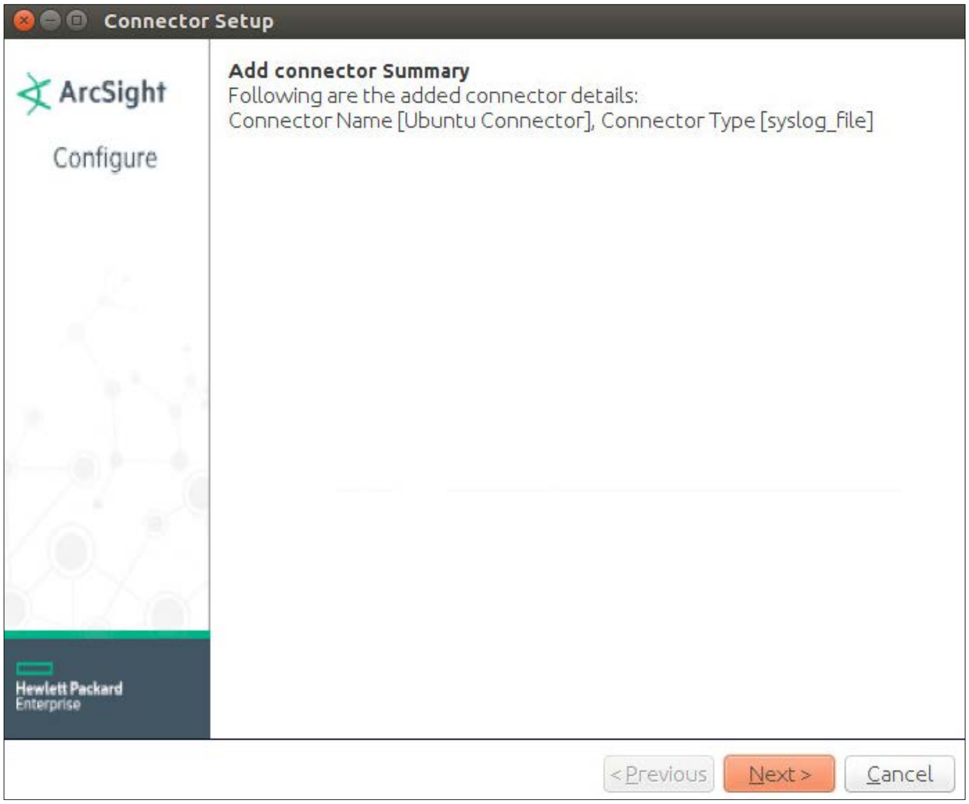
● Import the certificate to connector from destination
○ Do not import the certificate to connector from destination

Updating ...

Importing certificate, registering destination and restarting the container

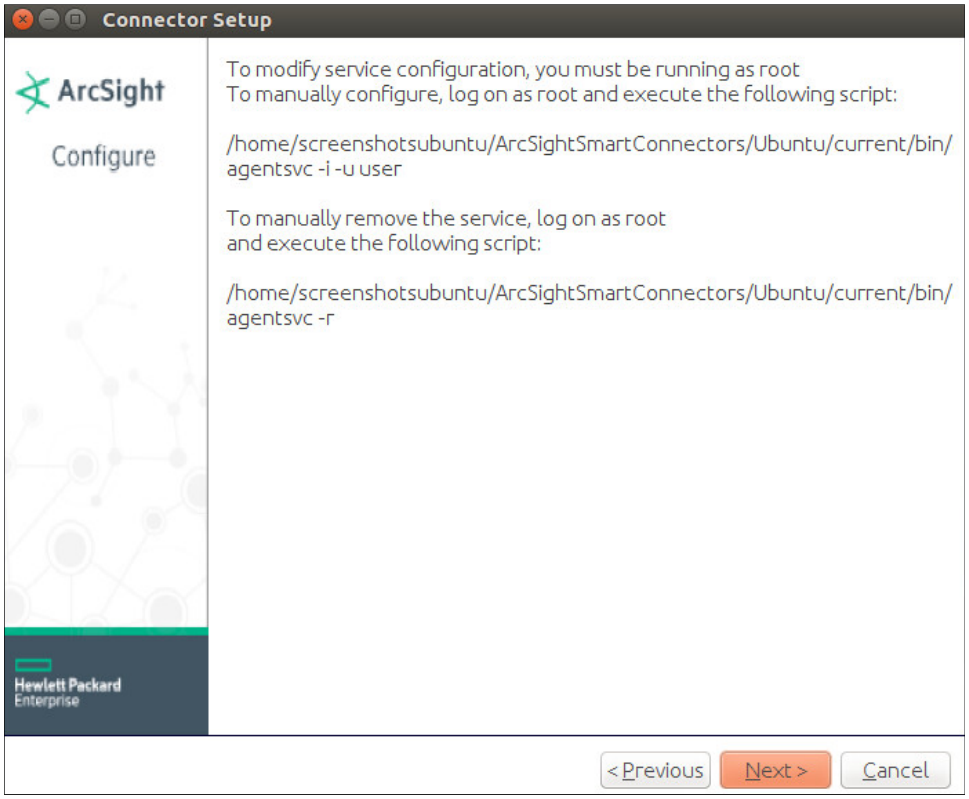
0%

24. Click **Next**.



Add connector Summary
Following are the added connector details:
Connector Name [Ubuntu Connector], Connector Type [syslog_file]

25. Click **Next**.



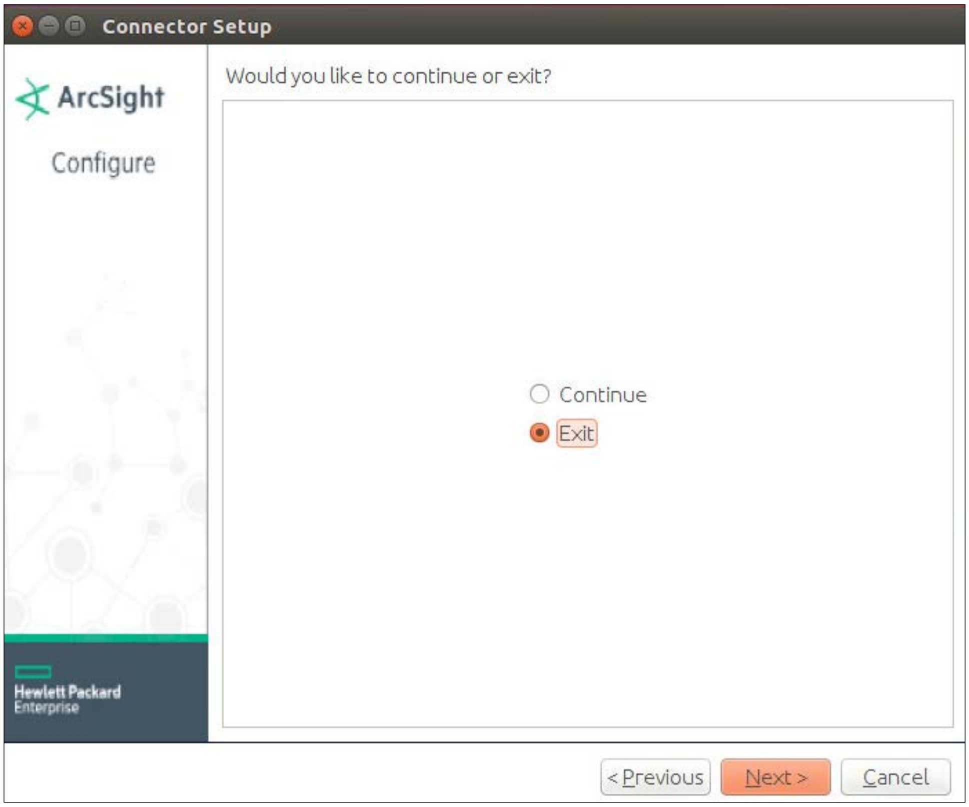
To modify service configuration, you must be running as root
To manually configure, log on as root and execute the following script:

```
/home/screenshotsubuntu/ArcSightSmartConnectors/Ubuntu/current/bin/
agentsvc -i -u user
```

To manually remove the service, log on as root
and execute the following script:

```
/home/screenshotsubuntu/ArcSightSmartConnectors/Ubuntu/current/bin/
agentsvc -r
```

26. Click **Next**.
27. Choose **Exit**.

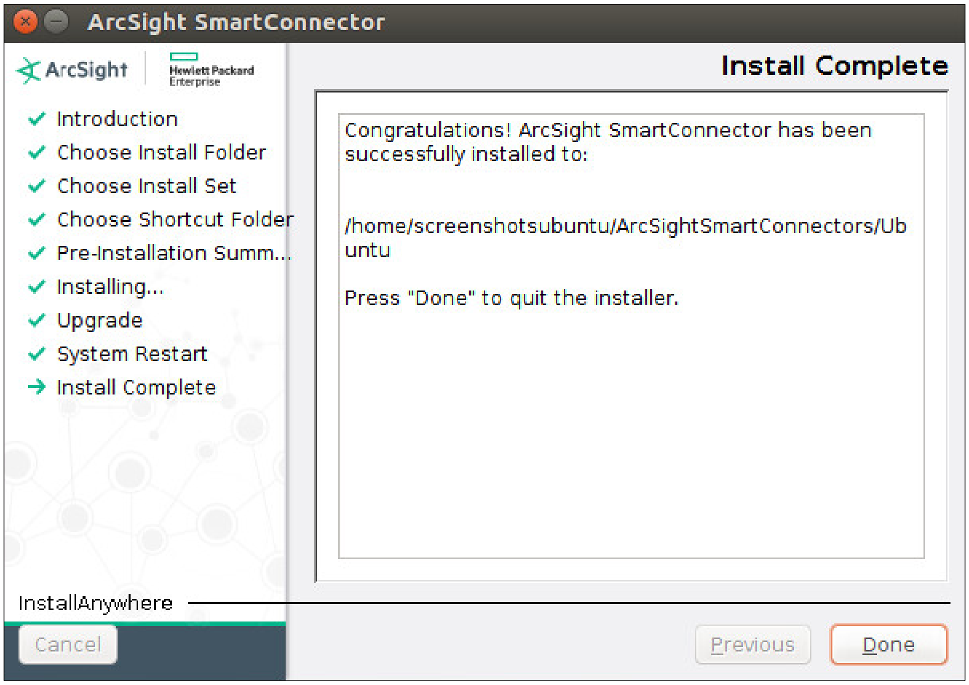


Would you like to continue or exit?

○ Continue

● Exit

28. Click **Next**.



Install Complete

Congratulations! ArcSight SmartConnector has been successfully installed to:

/home/screenshotsubuntu/ArcSightSmartConnectors/Ubuntu

Press "Done" to quit the installer.

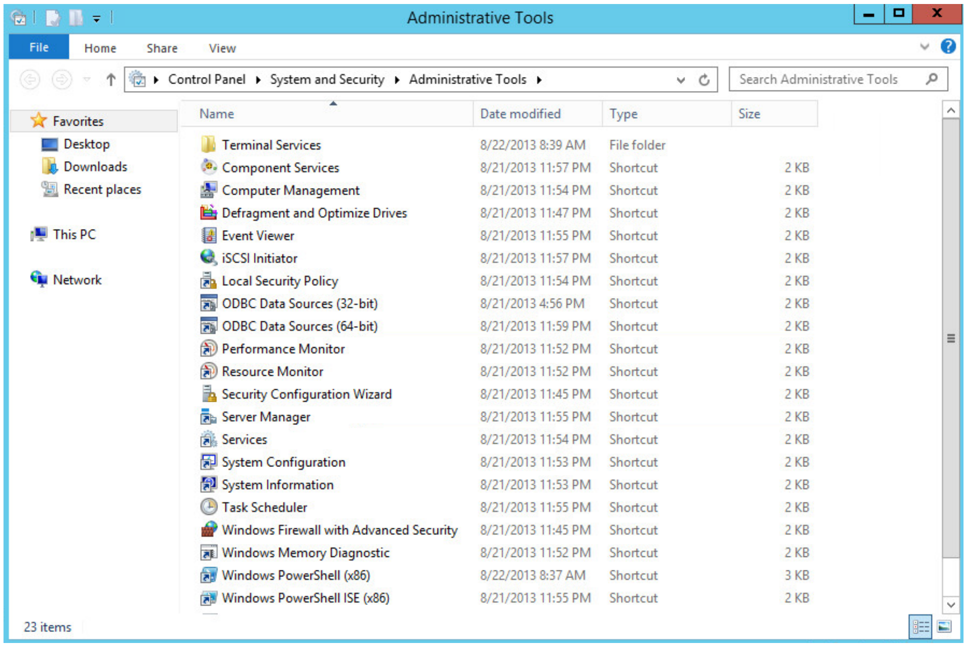
29. Click **Done**.

2.7 IBM Spectrum Protect

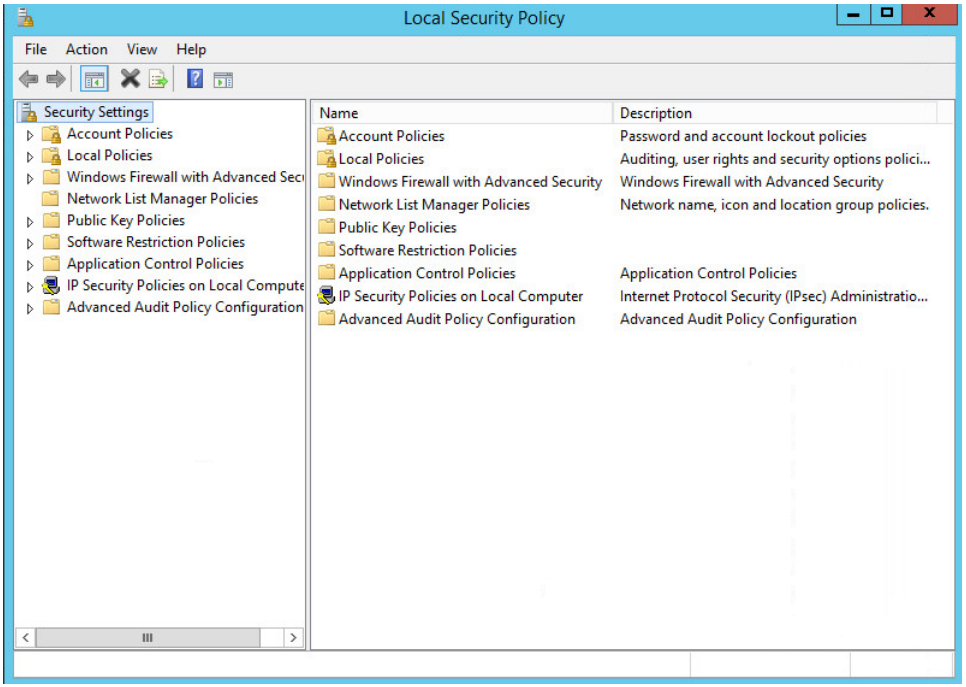
IBM Spectrum Protect is a backup/restore solution that makes use of cloud-based object storage. It allows for administrative management of backups across an enterprise, providing users with mechanisms to restore their data on a file level. This section covers the installation and configuration process used to set up IBM Spectrum Protect on a Windows Server 2012 R2 machine, as well as the installation and configuration processes required for installing the backup/archive client on various machines.

2.7.1 Install IBM Spectrum Protect Server

1. You may need to disable **Run all administrators in Admin Approval Mode**. To do this go to **Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options**. Double click the **User Account Control: Run all administrators in Admin Approval Mode** section. Select **Disable** and click **OK**. Restart the computer.

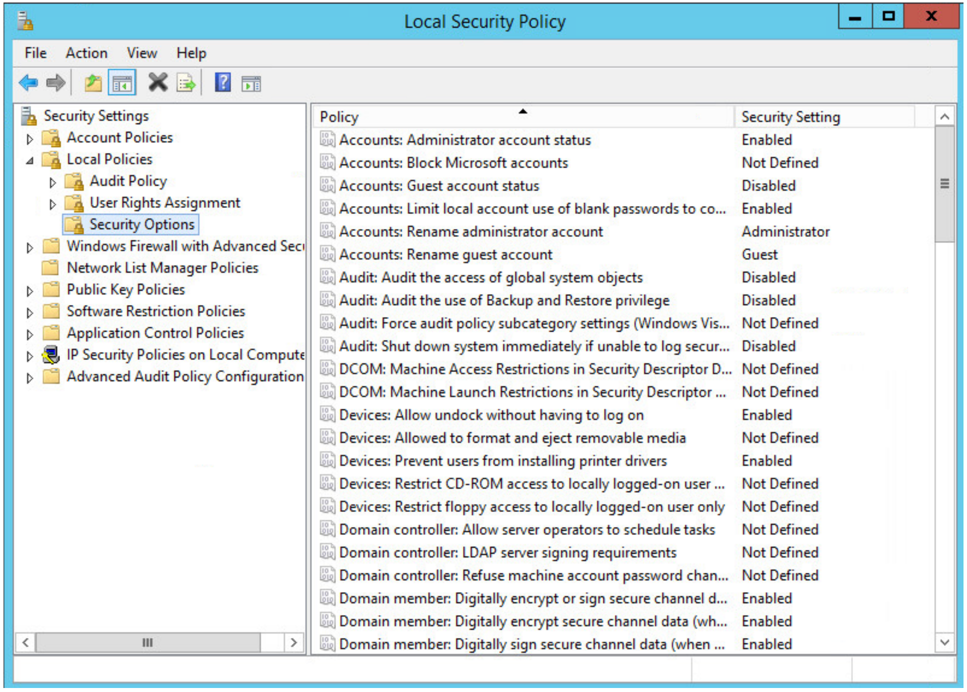


Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Security Configuration Wizard	8/21/2013 11:45 PM	Shortcut	2 KB
Server Manager	8/21/2013 11:55 PM	Shortcut	2 KB
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:53 PM	Shortcut	2 KB
System Information	8/21/2013 11:53 PM	Shortcut	2 KB
Task Scheduler	8/21/2013 11:55 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	8/21/2013 11:45 PM	Shortcut	2 KB
Windows Memory Diagnostic	8/21/2013 11:52 PM	Shortcut	2 KB
Windows PowerShell (x86)	8/22/2013 8:37 AM	Shortcut	3 KB
Windows PowerShell ISE (x86)	8/21/2013 11:55 PM	Shortcut	2 KB



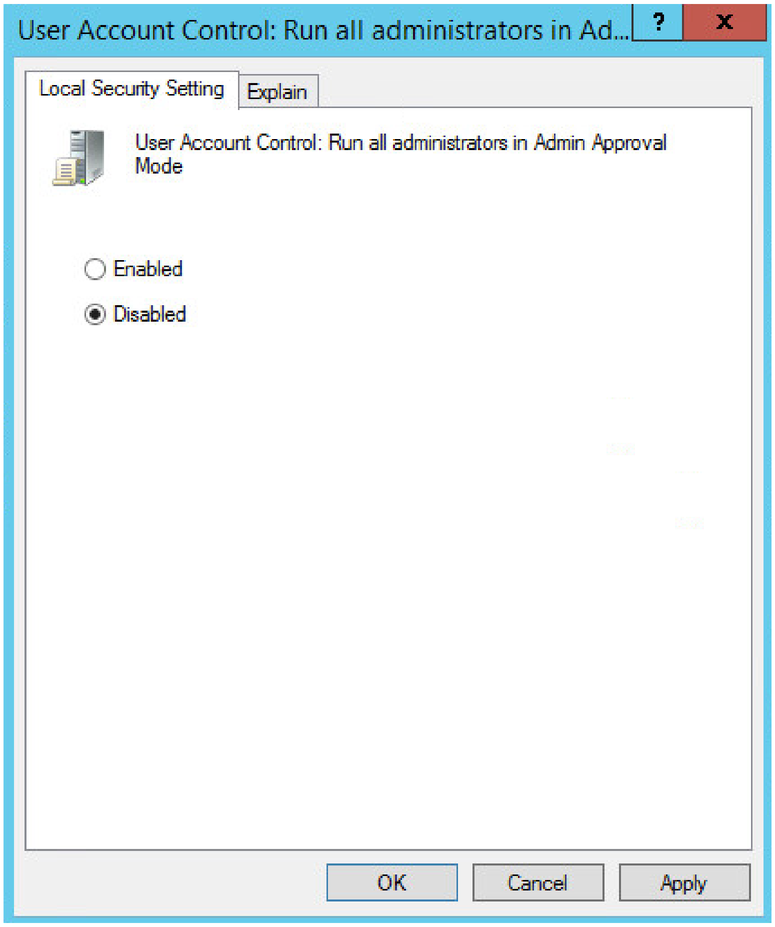
- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled



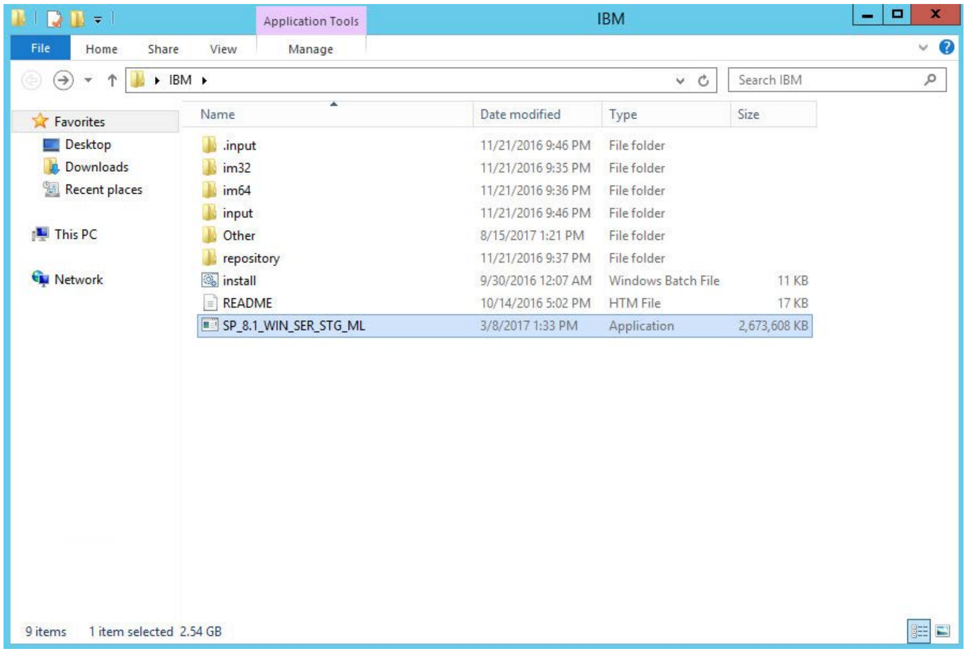
User Account Control: Run all administrators in Ad...

User Account Control: Run all administrators in Admin Approval Mode

○ Enabled

● Disabled

2. Run **WIN_SER_STG_ML** in its own folder to extract the contents.

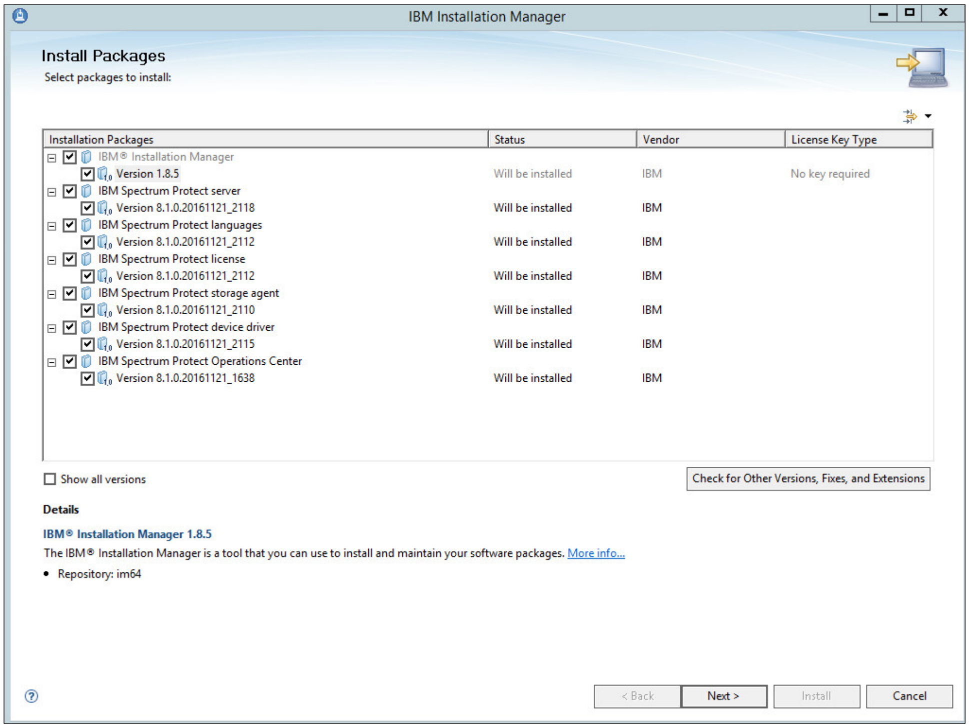


Name	Date modified	Type	Size
.input	11/21/2016 9:46 PM	File folder	
im32	11/21/2016 9:35 PM	File folder	
im64	11/21/2016 9:36 PM	File folder	
input	11/21/2016 9:46 PM	File folder	
Other	8/15/2017 1:21 PM	File folder	
repository	11/21/2016 9:37 PM	File folder	
install	9/30/2016 12:07 AM	Windows Batch File	11 KB
README	10/14/2016 5:02 PM	HTM File	17 KB
SP_8.1_WIN_SER_STG_ML	3/8/2017 1:33 PM	Application	2,673,608 KB

9 items   1 item selected 2.54 GB

3. Run the **install** script.

4. Make sure all the boxes are checked.



Installation Packages	Status	Vendor	License Key Type
⊟ ☑ IBM® Installation Manager			
☑ Version 1.8.5	Will be installed	IBM	No key required
⊟ ☑ IBM Spectrum Protect server			
☑ Version 8.1.0.20161121_2118	Will be installed	IBM	
⊟ ☑ IBM Spectrum Protect languages			
☑ Version 8.1.0.20161121_2112	Will be installed	IBM	
⊟ ☑ IBM Spectrum Protect license			
☑ Version 8.1.0.20161121_2112	Will be installed	IBM	
⊟ ☑ IBM Spectrum Protect storage agent			
☑ Version 8.1.0.20161121_2110	Will be installed	IBM	
⊟ ☑ IBM Spectrum Protect device driver			
☑ Version 8.1.0.20161121_2115	Will be installed	IBM	
⊟ ☑ IBM Spectrum Protect Operations Center			
☑ Version 8.1.0.20161121_1638	Will be installed	IBM	

☐ Show all versions   Check for Other Versions, Fixes, and Extensions

Details

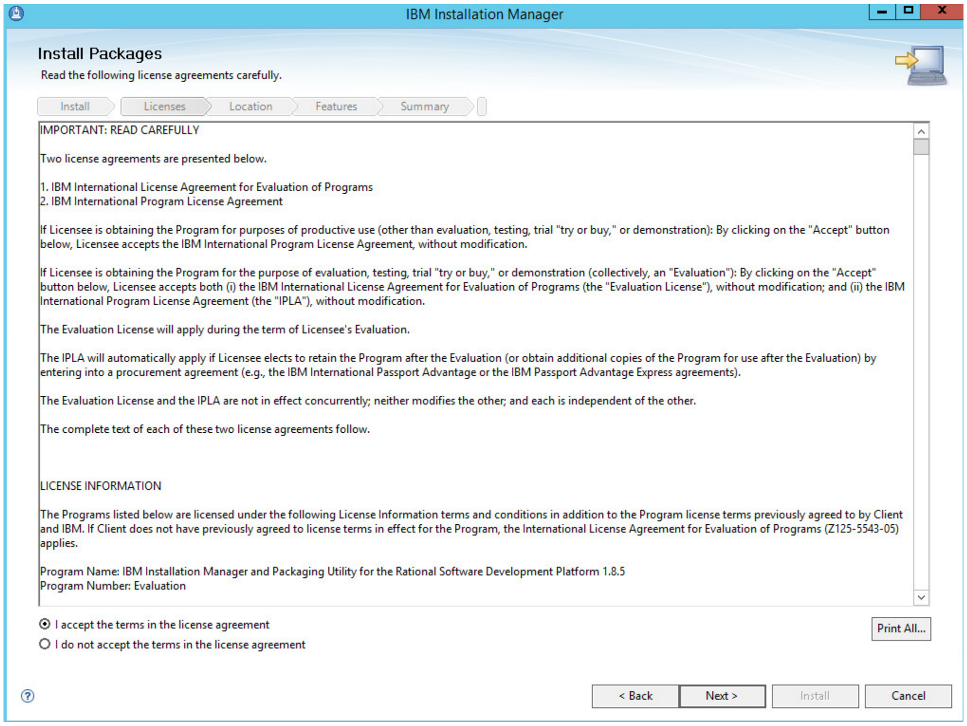
IBM® Installation Manager 1.8.5

The IBM® Installation Manager is a tool that you can use to install and maintain your software packages. More info...

- Repository: im64

5. Click **Next**.

6. Read and select **I accept the terms in the license agreement**.



IMPORTANT: READ CAREFULLY

Two license agreements are presented below.

1. IBM International License Agreement for Evaluation of Programs
2. IBM International Program License Agreement

If Licensee is obtaining the Program for purposes of productive use (other than evaluation, testing, trial "try or buy," or demonstration): By clicking on the "Accept" button below, Licensee accepts the IBM International Program License Agreement, without modification.

If Licensee is obtaining the Program for the purpose of evaluation, testing, trial "try or buy," or demonstration (collectively, an "Evaluation"): By clicking on the "Accept" button below, Licensee accepts both (i) the IBM International License Agreement for Evaluation of Programs (the "Evaluation License"), without modification; and (ii) the IBM International Program License Agreement (the "IPLA"), without modification.

The Evaluation License will apply during the term of Licensee's Evaluation.

The IPLA will automatically apply if Licensee elects to retain the Program after the Evaluation (or obtain additional copies of the Program for use after the Evaluation) by entering into a procurement agreement (e.g., the IBM International Passport Advantage or the IBM Passport Advantage Express agreements).

The Evaluation License and the IPLA are not in effect concurrently; neither modifies the other; and each is independent of the other.

The complete text of each of these two license agreements follow.

LICENSE INFORMATION

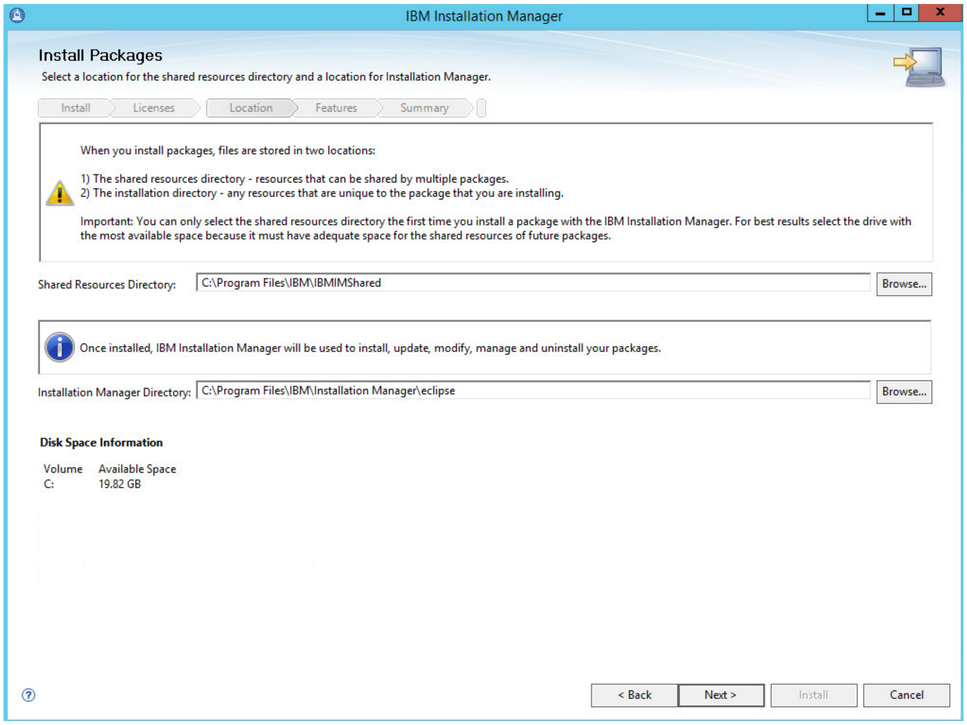
The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International License Agreement for Evaluation of Programs (Z125-5543-05) applies.

Program Name: IBM Installation Manager and Packaging Utility for the Rational Software Development Platform 1.8.5
Program Number: Evaluation

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

7. Click **Next**.

8. Select the location for files to be installed to.



Install Packages

Select a location for the shared resources directory and a location for Installation Manager.

When you install packages, files are stored in two locations:

1) The shared resources directory - resources that can be shared by multiple packages.
2) The installation directory - any resources that are unique to the package that you are installing.

Important: You can only select the shared resources directory the first time you install a package with the IBM Installation Manager. For best results select the drive with the most available space because it must have adequate space for the shared resources of future packages.

Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

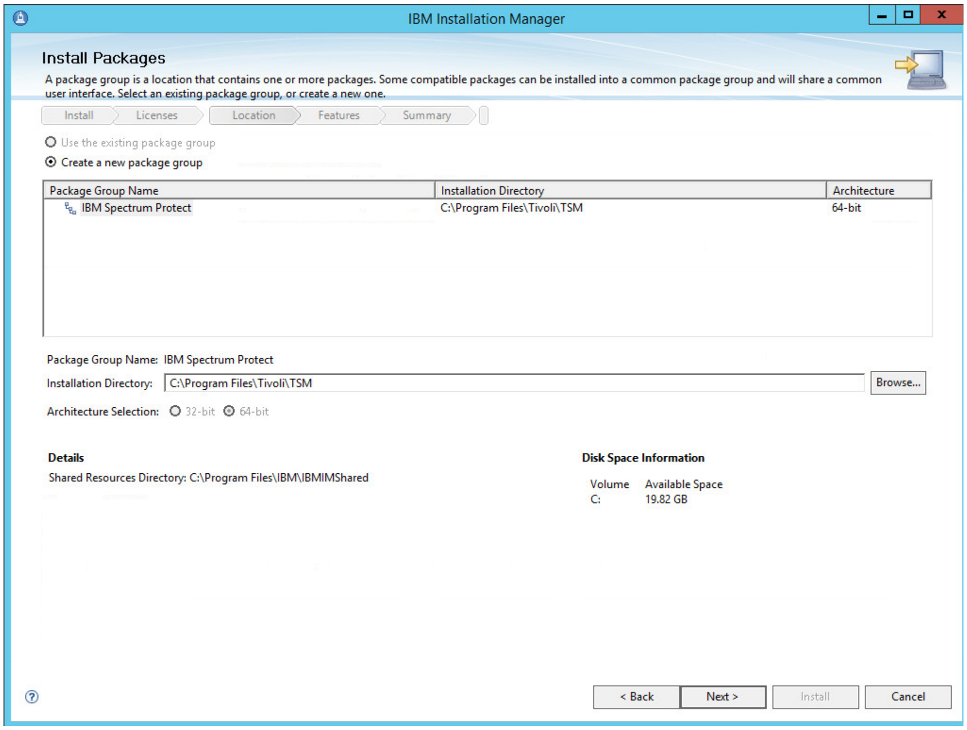
Once installed, IBM Installation Manager will be used to install, update, modify, manage and uninstall your packages.

Installation Manager Directory: C:\Program Files\IBM\Installation Manager\eclipse

Disk Space Information

Volume	Available Space
C:	19.82 GB

9. Click **Next**.



Install Packages

A package group is a location that contains one or more packages. Some compatible packages can be installed into a common package group and will share a common user interface. Select an existing package group, or create a new one.

○ Use the existing package group

● Create a new package group

Package Group Name	Installation Directory	Architecture
IBM Spectrum Protect	C:\Program Files\Tivoli\TSM	64-bit

Package Group Name: IBM Spectrum Protect

Installation Directory: C:\Program Files\Tivoli\TSM

Architecture Selection: ○ 32-bit ● 64-bit

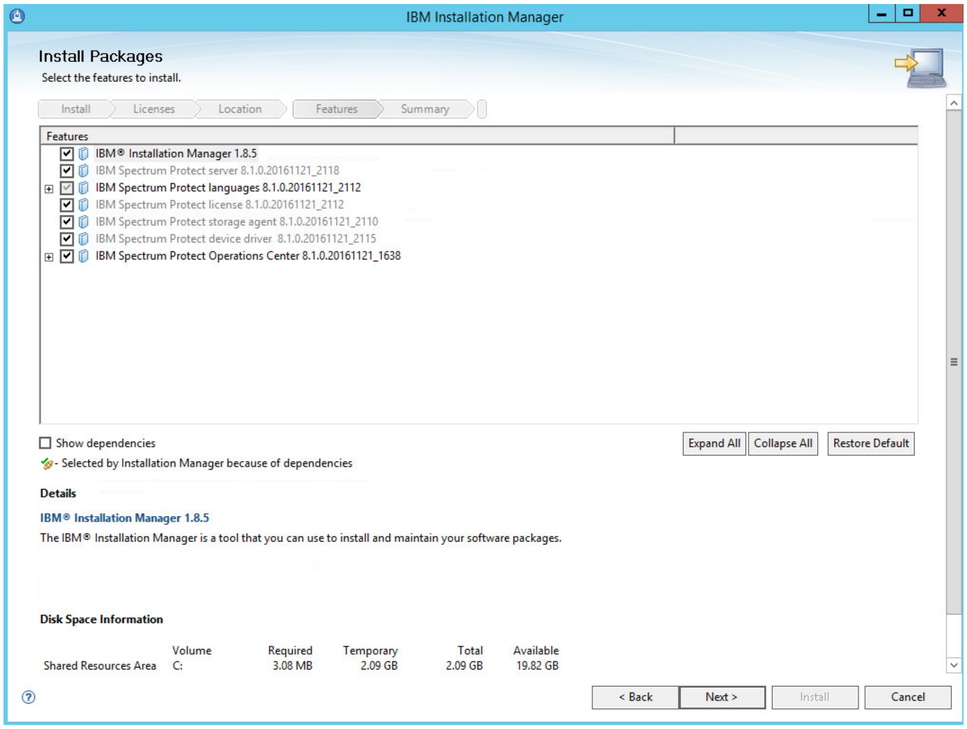
Details

Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

Disk Space Information

Volume	Available Space
C:	19.82 GB

10. Click **Next**.
11. Make sure all the packages are checked.



☑ IBM® Installation Manager 1.8.5
☑ IBM Spectrum Protect server 8.1.0.20161121_2118
☑ IBM Spectrum Protect languages 8.1.0.20161121_2112
☑ IBM Spectrum Protect license 8.1.0.20161121_2112
☑ IBM Spectrum Protect storage agent 8.1.0.20161121_2110
☑ IBM Spectrum Protect device driver 8.1.0.20161121_2115
☑ IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

□ Show dependencies
- Selected by Installation Manager because of dependencies

Details

IBM® Installation Manager 1.8.5

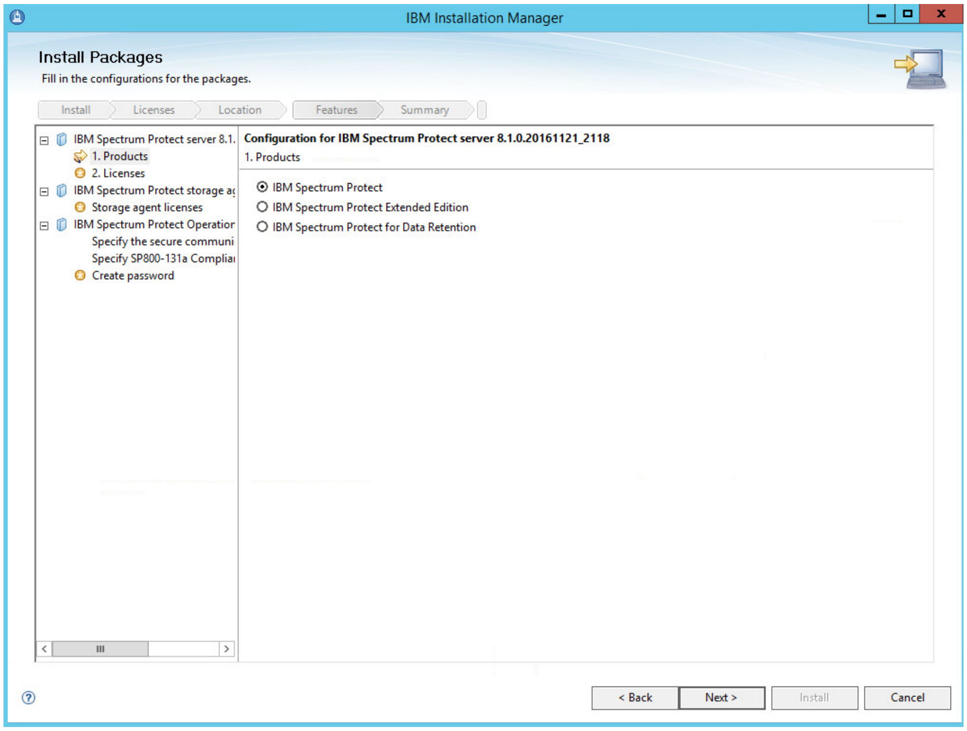
The IBM® Installation Manager is a tool that you can use to install and maintain your software packages.

Disk Space Information

	Volume	Required	Temporary	Total	Available
Shared Resources Area	C:	3.08 MB	2.09 GB	2.09 GB	19.82 GB

12. Click **Next**.

13. Select **IBM Spectrum Protect**.



IBM Installation Manager

Install Packages

Fill in the configurations for the packages.

Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage ag
Storage agent licenses
IBM Spectrum Protect Operation
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

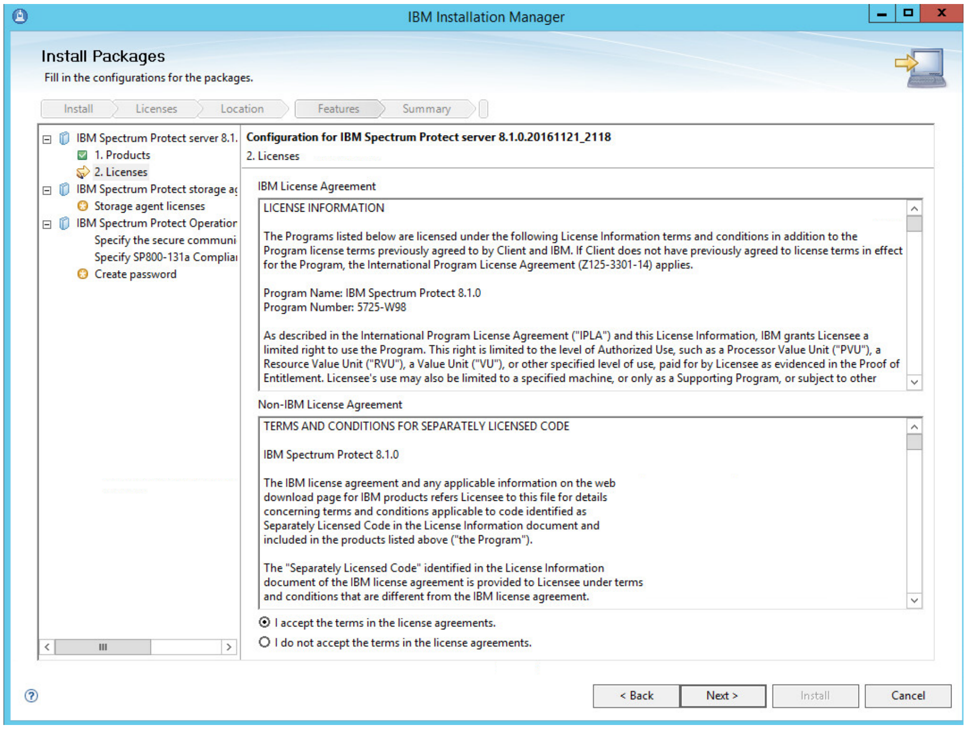
Configuration for IBM Spectrum Protect server 8.1.0.20161121_2118

1. Products

● IBM Spectrum Protect
○ IBM Spectrum Protect Extended Edition
○ IBM Spectrum Protect for Data Retention

14. Click **Next**.

15. Read and select **I accept the terms in the license agreement**.



IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage ag
Storage agent licenses
IBM Spectrum Protect Operatior
Specify the secure communi
Specify SP800-131a Complia
Create password

Configuration for IBM Spectrum Protect server 8.1.0.20161121_2118

2. Licenses

IBM License Agreement

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International Program License Agreement (Z125-3301-14) applies.

Program Name: IBM Spectrum Protect 8.1.0
Program Number: 5725-W98

As described in the International Program License Agreement ("IPLA") and this License Information, IBM grants Licensee a limited right to use the Program. This right is limited to the level of Authorized Use, such as a Processor Value Unit ("PVU"), a Resource Value Unit ("RVU"), a Value Unit ("VU"), or other specified level of use, paid for by Licensee as evidenced in the Proof of Entitlement. Licensee's use may also be limited to a specified machine, or only as a Supporting Program, or subject to other

Non-IBM License Agreement

TERMS AND CONDITIONS FOR SEPARATELY LICENSED CODE

IBM Spectrum Protect 8.1.0

The IBM license agreement and any applicable information on the web download page for IBM products refers Licensee to this file for details concerning terms and conditions applicable to code identified as Separately Licensed Code in the License Information document and included in the products listed above ("the Program").

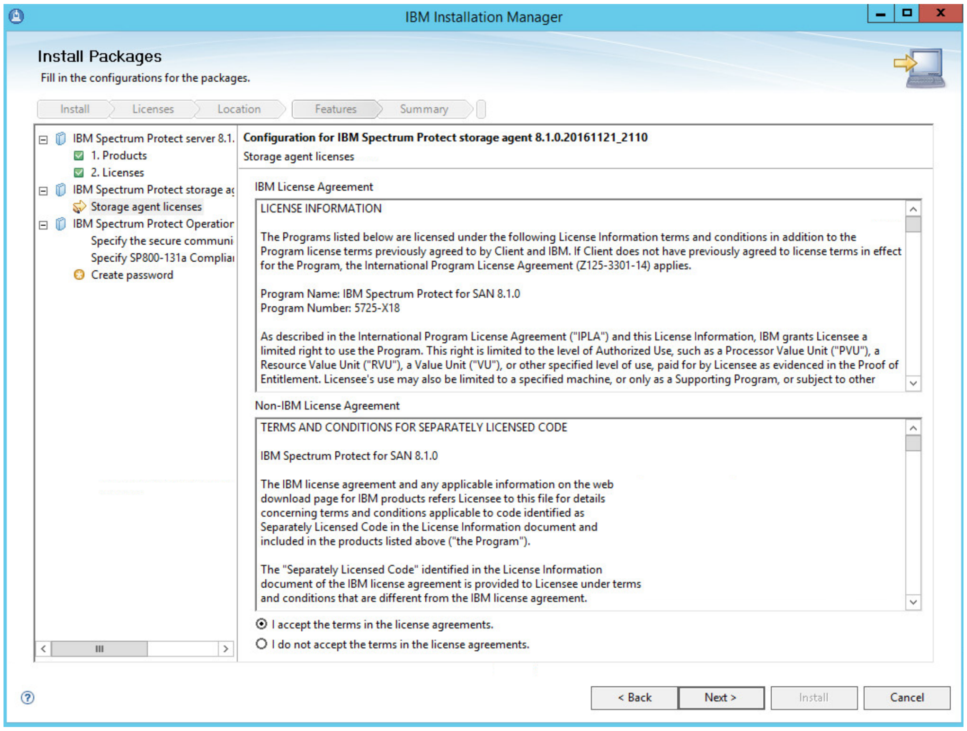
The "Separately Licensed Code" identified in the License Information document of the IBM license agreement is provided to Licensee under terms and conditions that are different from the IBM license agreement.

● I accept the terms in the license agreements.

○ I do not accept the terms in the license agreements.

16. Click **Next**.

17. Read and select **I accept the terms in the license agreement**.



IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage a
Storage agent licenses
IBM Spectrum Protect Operatior
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect storage agent 8.1.0.20161121_2110

Storage agent licenses

IBM License Agreement

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International Program License Agreement (Z125-3301-14) applies.

Program Name: IBM Spectrum Protect for SAN 8.1.0
Program Number: 5725-X18

As described in the International Program License Agreement ("IPLA") and this License Information, IBM grants Licensee a limited right to use the Program. This right is limited to the level of Authorized Use, such as a Processor Value Unit ("PVU"), a Resource Value Unit ("RVU"), a Value Unit ("VU"), or other specified level of use, paid for by Licensee as evidenced in the Proof of Entitlement. Licensee's use may also be limited to a specified machine, or only as a Supporting Program, or subject to other

Non-IBM License Agreement

TERMS AND CONDITIONS FOR SEPARATELY LICENSED CODE

IBM Spectrum Protect for SAN 8.1.0

The IBM license agreement and any applicable information on the web download page for IBM products refers Licensee to this file for details concerning terms and conditions applicable to code identified as Separately Licensed Code in the License Information document and included in the products listed above ("the Program").

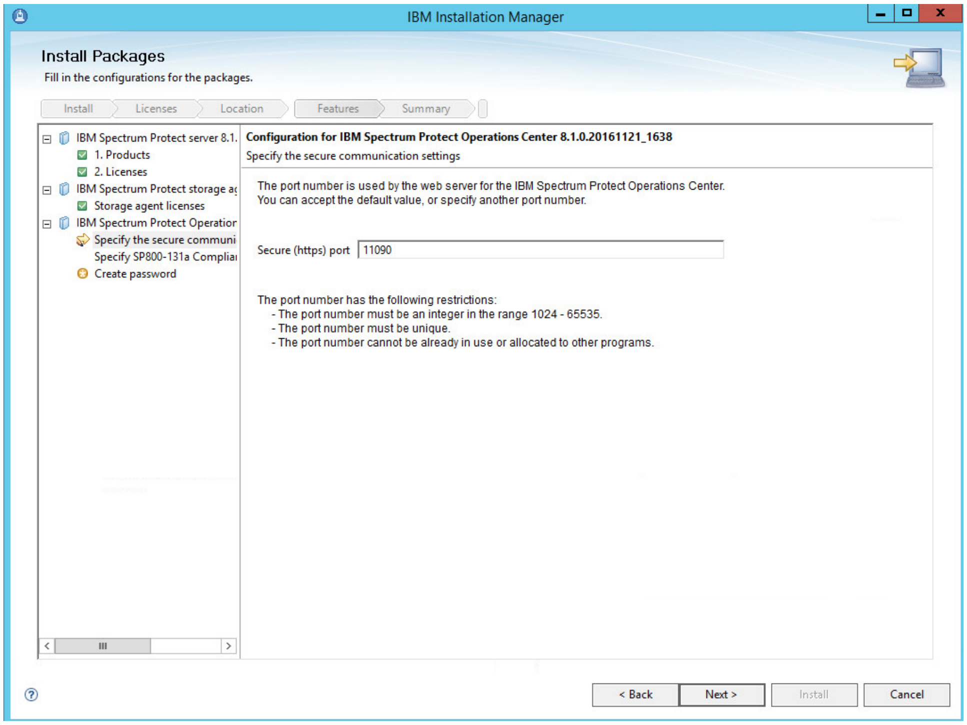
The "Separately Licensed Code" identified in the License Information document of the IBM license agreement is provided to Licensee under terms and conditions that are different from the IBM license agreement.

● I accept the terms in the license agreements.

○ I do not accept the terms in the license agreements.

18. Click **Next**.

19. Specify **11090** for the port.



IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage ag
Storage agent licenses
IBM Spectrum Protect Operation
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

Specify the secure communication settings

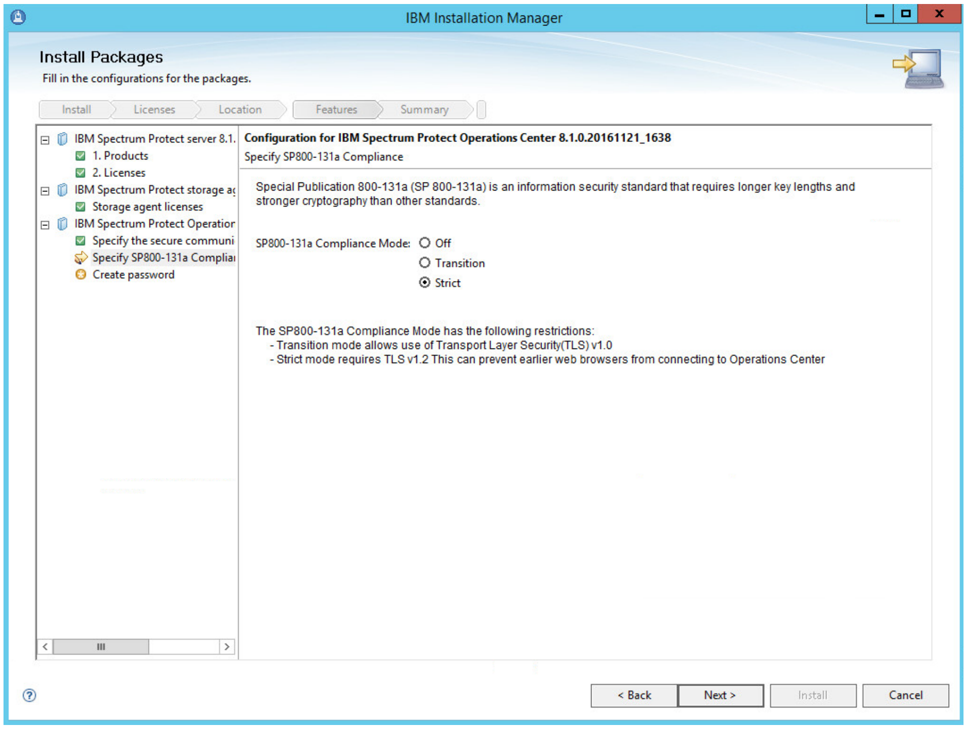
The port number is used by the web server for the IBM Spectrum Protect Operations Center.
You can accept the default value, or specify another port number.

Secure (https) port 11090

The port number has the following restrictions:
- The port number must be an integer in the range 1024 - 65535.
- The port number must be unique.
- The port number cannot be already in use or allocated to other programs.

20. Click **Next**.

21. Select **Strict** for the **SP800-131a Compliance**.


IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage a
Storage agent licenses
IBM Spectrum Protect Operatior
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

Specify SP800-131a Compliance

Special Publication 800-131a (SP 800-131a) is an information security standard that requires longer key lengths and stronger cryptography than other standards.

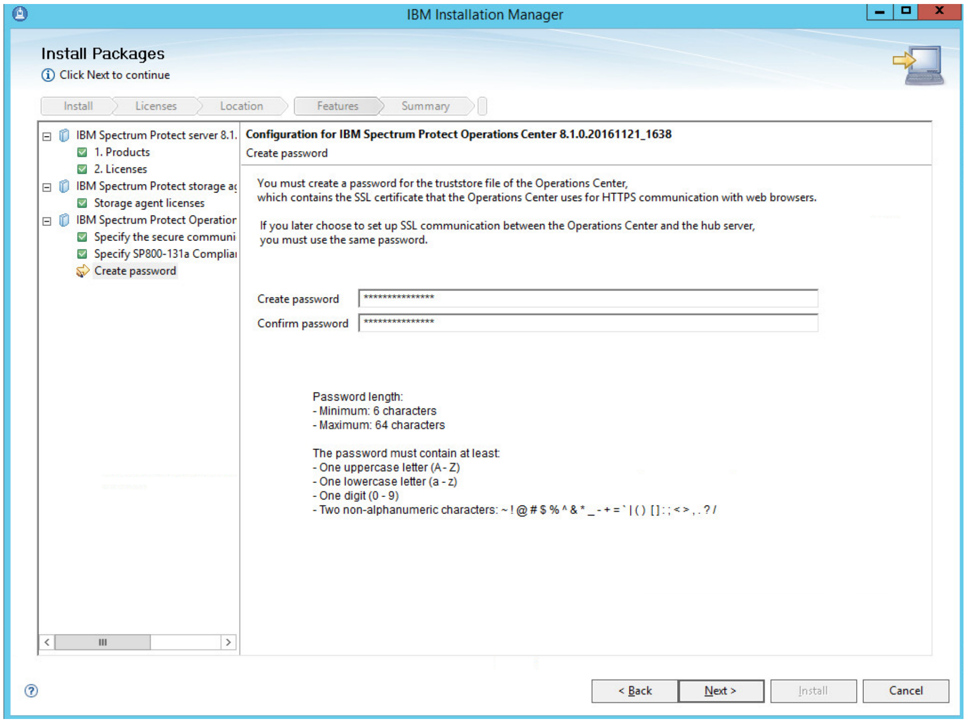
SP800-131a Compliance Mode: ○ Off

○ Transition

● Strict

The SP800-131a Compliance Mode has the following restrictions:
- Transition mode allows use of Transport Layer Security(TLS) v1.0
- Strict mode requires TLS v1.2 This can prevent earlier web browsers from connecting to Operations Center

22. Click **Next**.
23. Create a password.



Configuration for IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

Create password

You must create a password for the truststore file of the Operations Center,
which contains the SSL certificate that the Operations Center uses for HTTPS communication with web browsers.

If you later choose to set up SSL communication between the Operations Center and the hub server,
you must use the same password.

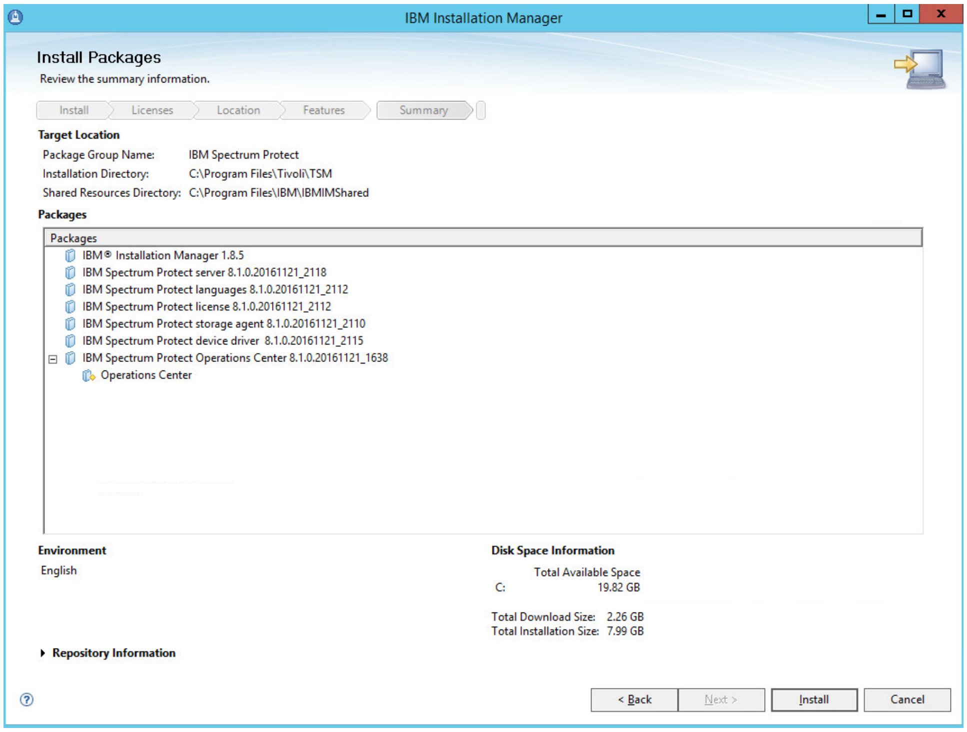
Create password ***************

Confirm password ***************

Password length:
- Minimum: 6 characters
- Maximum: 64 characters

The password must contain at least:
- One uppercase letter (A - Z)
- One lowercase letter (a - z)
- One digit (0 - 9)
- Two non-alphanumeric characters: ~ ! @ # $ % ^ & * _ - + = ` | ( ) [ ] : ; < > , . ? /

24. Click **Next**.



Target Location

Package Group Name: IBM Spectrum Protect
Installation Directory: C:\Program Files\Tivoli\TSM
Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

Packages

Packages
- IBM® Installation Manager 1.8.5
- IBM Spectrum Protect server 8.1.0.20161121_2118
- IBM Spectrum Protect languages 8.1.0.20161121_2112
- IBM Spectrum Protect license 8.1.0.20161121_2112
- IBM Spectrum Protect storage agent 8.1.0.20161121_2110
- IBM Spectrum Protect device driver 8.1.0.20161121_2115
- IBM Spectrum Protect Operations Center 8.1.0.20161121_1638
  - Operations Center

Environment

English

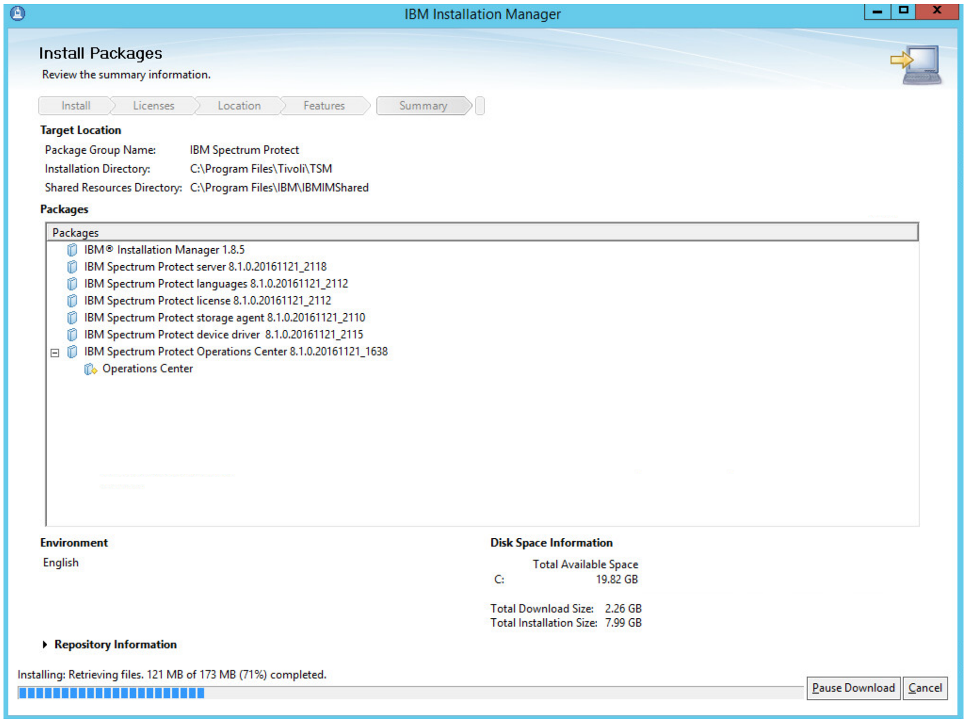
Disk Space Information

	Total Available Space
C:	19.82 GB

Total Download Size: 2.26 GB
Total Installation Size: 7.99 GB

25. Click **Install**.

26. Wait for the **install** to finish.



Install Packages

Review the summary information.

Target Location

Package Group Name: IBM Spectrum Protect

Installation Directory: C:\Program Files\Tivoli\TSM

Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

Packages

Packages
IBM® Installation Manager 1.8.5
IBM Spectrum Protect server 8.1.0.20161121_2118
IBM Spectrum Protect languages 8.1.0.20161121_2112
IBM Spectrum Protect license 8.1.0.20161121_2112
IBM Spectrum Protect storage agent 8.1.0.20161121_2110
IBM Spectrum Protect device driver 8.1.0.20161121_2115
IBM Spectrum Protect Operations Center 8.1.0.20161121_1638
Operations Center

Environment

English

Disk Space Information

	Total Available Space
C:	19.82 GB

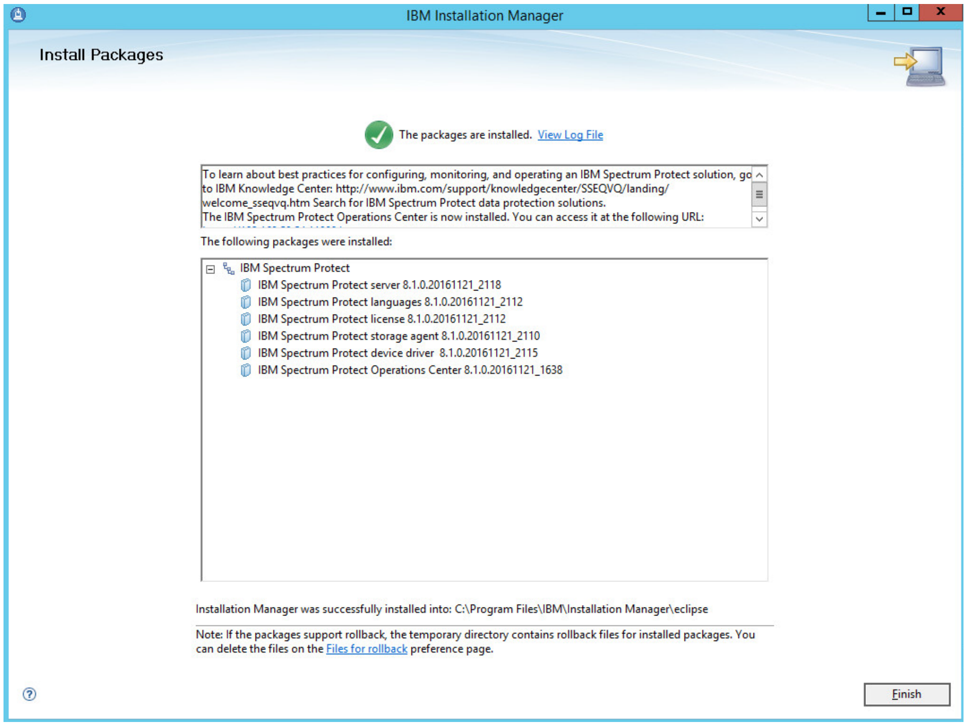
Total Download Size: 2.26 GB

Total Installation Size: 7.99 GB

Repository Information

Installing: Retrieving files. 121 MB of 173 MB (71%) completed.

27. Click **Finish**.



The packages are installed. View Log File

To learn about best practices for configuring, monitoring, and operating an IBM Spectrum Protect solution, go to IBM Knowledge Center: http://www.ibm.com/support/knowledgecenter/SSEQVQ/landing/welcome_sseqvq.htm Search for IBM Spectrum Protect data protection solutions.
The IBM Spectrum Protect Operations Center is now installed. You can access it at the following URL:

The following packages were installed:

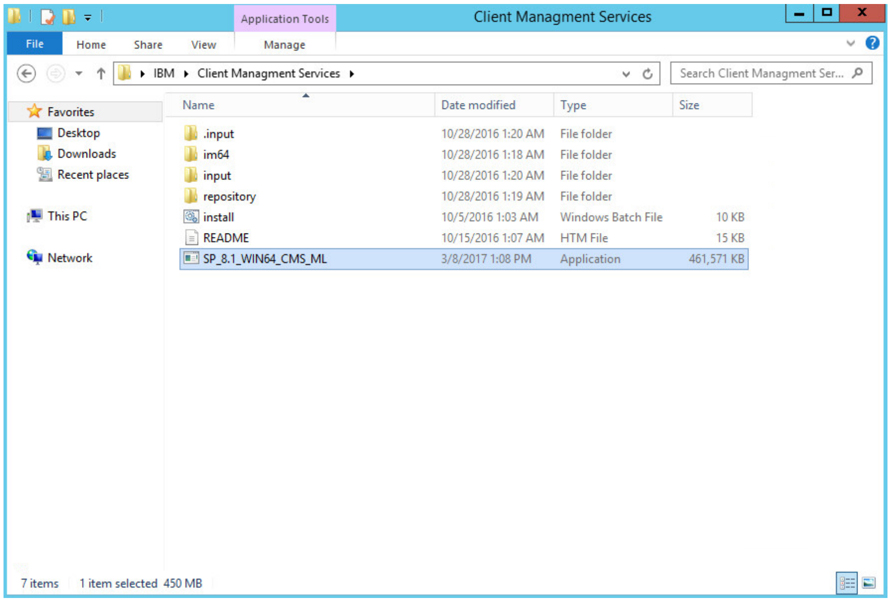
- IBM Spectrum Protect
  - IBM Spectrum Protect server 8.1.0.20161121_2118
  - IBM Spectrum Protect languages 8.1.0.20161121_2112
  - IBM Spectrum Protect license 8.1.0.20161121_2112
  - IBM Spectrum Protect storage agent 8.1.0.20161121_2110
  - IBM Spectrum Protect device driver 8.1.0.20161121_2115
  - IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

Installation Manager was successfully installed into: C:\Program Files\IBM\Installation Manager\eclipse

Note: If the packages support rollback, the temporary directory contains rollback files for installed packages. You can delete the files on the Files for rollback preference page.

2.7.2 Install IBM Spectrum Protect Client Management Services

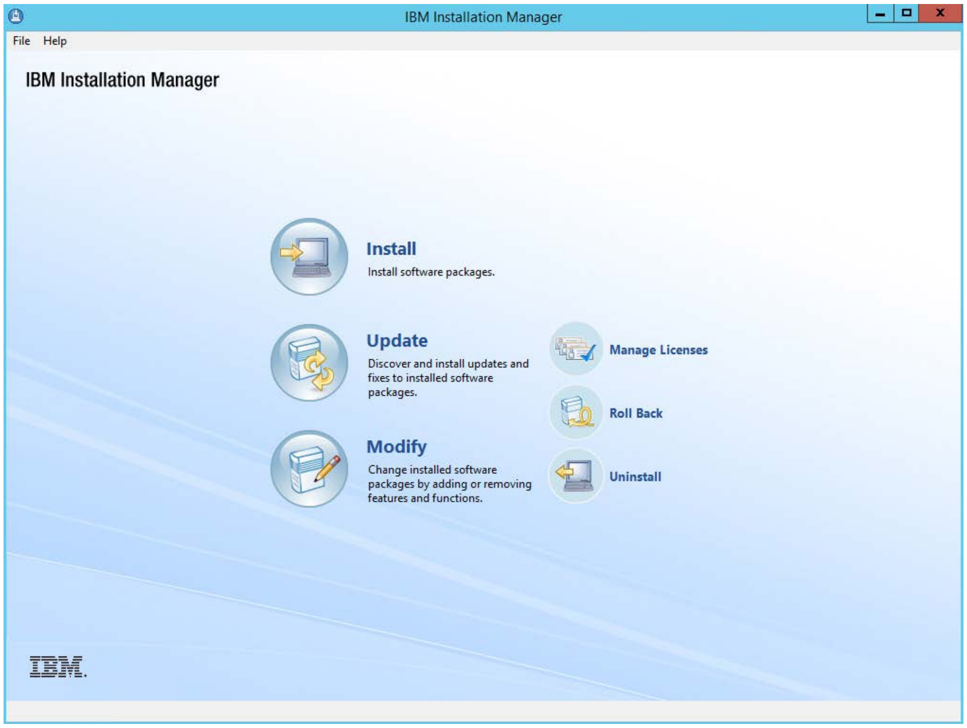
1. Run **WIN64_CMS_ML** in its own folder to extract the contents.



Name	Date modified	Type	Size
.input	10/28/2016 1:20 AM	File folder	
im64	10/28/2016 1:18 AM	File folder	
input	10/28/2016 1:20 AM	File folder	
repository	10/28/2016 1:19 AM	File folder	
install	10/5/2016 1:03 AM	Windows Batch File	10 KB
README	10/15/2016 1:07 AM	HTM File	15 KB
SP_8.1_WIN64_CMS_ML	3/8/2017 1:08 PM	Application	461,571 KB

7 items   1 item selected 450 MB

2. Run the install script.

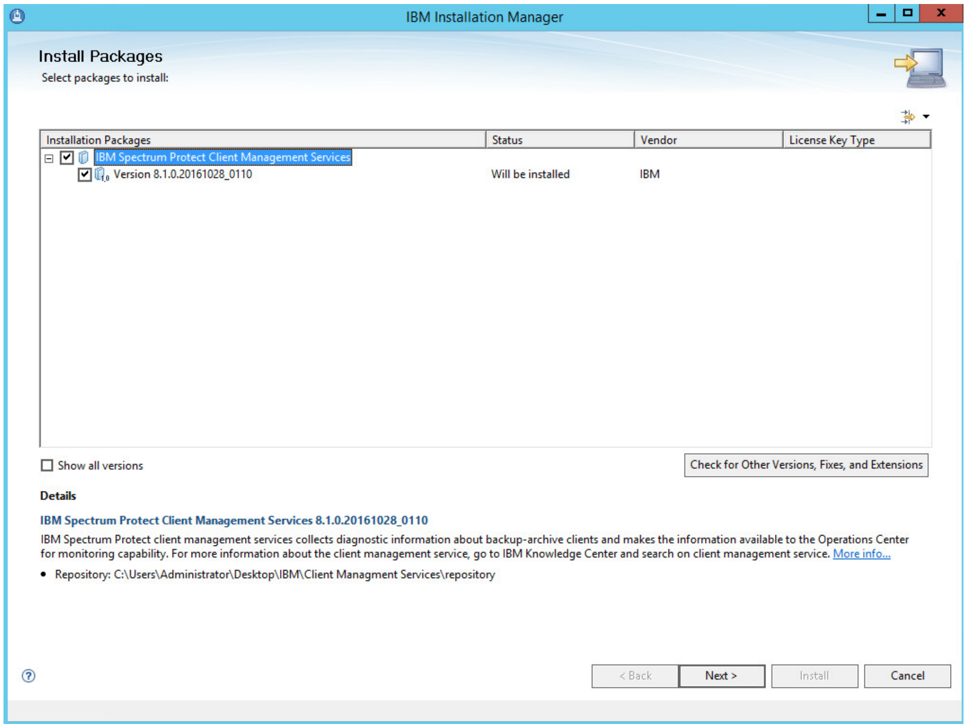


Install software packages.

Discover and install updates and fixes to installed software packages.

Change installed software packages by adding or removing features and functions.

3. Click **Install**.
4. Check the box next to **IBM Spectrum Protect Client Management Services**.



Install Packages

Select packages to install:

Installation Packages	Status	Vendor	License Key Type
☑ IBM Spectrum Protect Client Management Services			
☑ Version 8.1.0.20161028_0110	Will be installed	IBM	

☐ Show all versions

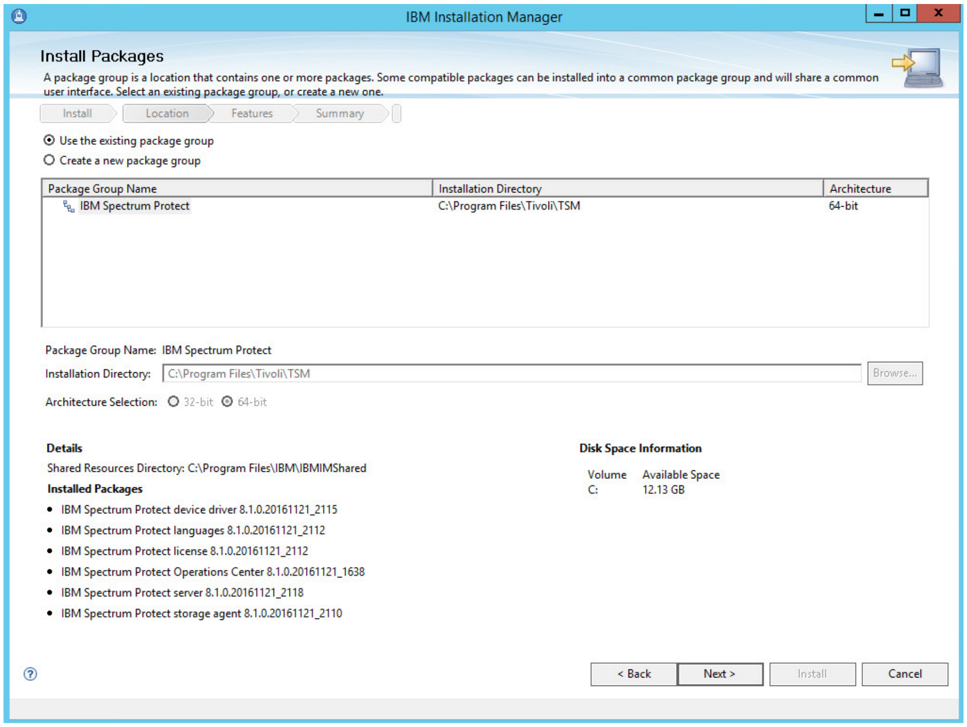
Details

IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110

IBM Spectrum Protect client management services collects diagnostic information about backup-archive clients and makes the information available to the Operations Center for monitoring capability. For more information about the client management service, go to IBM Knowledge Center and search on client management service. More info...

- Repository: C:\Users\Administrator\Desktop\IBM\Client Managment Services\repository

5. Click **Next**.
6. Select **Use the existing package group**.



Install Packages

A package group is a location that contains one or more packages. Some compatible packages can be installed into a common package group and will share a common user interface. Select an existing package group, or create a new one.

● Use the existing package group
○ Create a new package group

Package Group Name	Installation Directory	Architecture
IBM Spectrum Protect	C:\Program Files\Tivoli\TSM	64-bit

Package Group Name: IBM Spectrum Protect

Installation Directory: C:\Program Files\Tivoli\TSM

Architecture Selection: ○ 32-bit ● 64-bit

Details

Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

Installed Packages

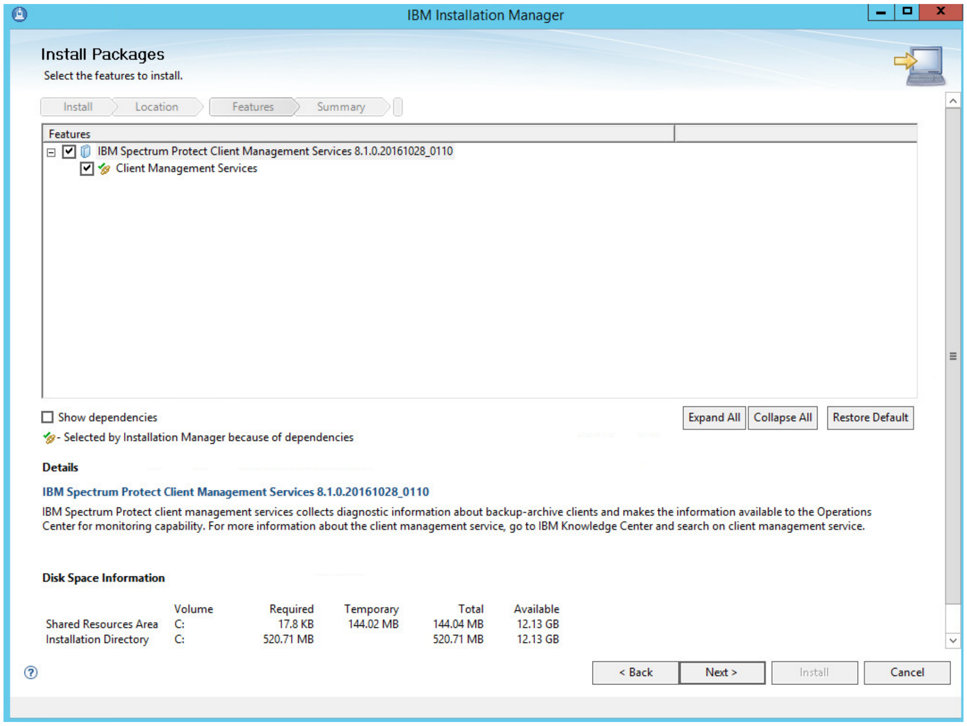
- IBM Spectrum Protect device driver 8.1.0.20161121_2115
- IBM Spectrum Protect languages 8.1.0.20161121_2112
- IBM Spectrum Protect license 8.1.0.20161121_2112
- IBM Spectrum Protect Operations Center 8.1.0.20161121_1638
- IBM Spectrum Protect server 8.1.0.20161121_2118
- IBM Spectrum Protect storage agent 8.1.0.20161121_2110

Disk Space Information

Volume	Available Space
C:	12.13 GB

7. Click **Next**.

8. Make sure all the boxes next to the package Client Management Services are checked.



IBM Installation Manager

Install Packages

Select the features to install.

Features

☑ IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110

☑ Client Management Services

□ Show dependencies

- Selected by Installation Manager because of dependencies

Details

IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110

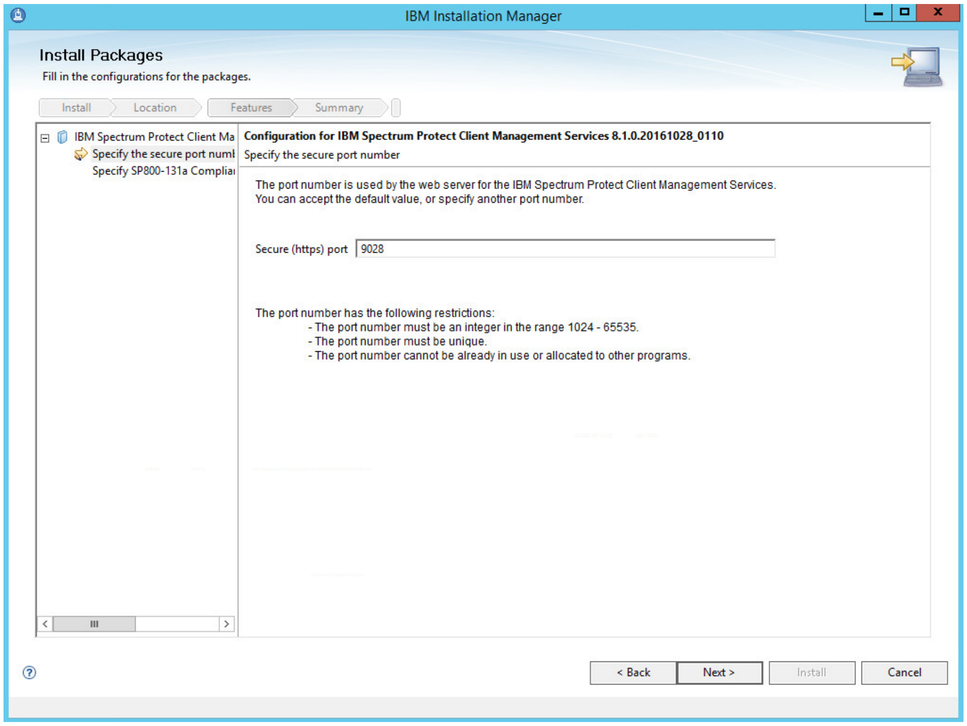
IBM Spectrum Protect client management services collects diagnostic information about backup-archive clients and makes the information available to the Operations Center for monitoring capability. For more information about the client management service, go to IBM Knowledge Center and search on client management service.

Disk Space Information

	Volume	Required	Temporary	Total	Available
Shared Resources Area	C:	17.8 KB	144.02 MB	144.04 MB	12.13 GB
Installation Directory	C:	520.71 MB		520.71 MB	12.13 GB

9. Click **Next**.

10. Set the port to **9028**.



IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Location
Features
Summary
IBM Spectrum Protect Client Ma
Specify the secure port numl
Specify SP800-131a Complia
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110

Specify the secure port number

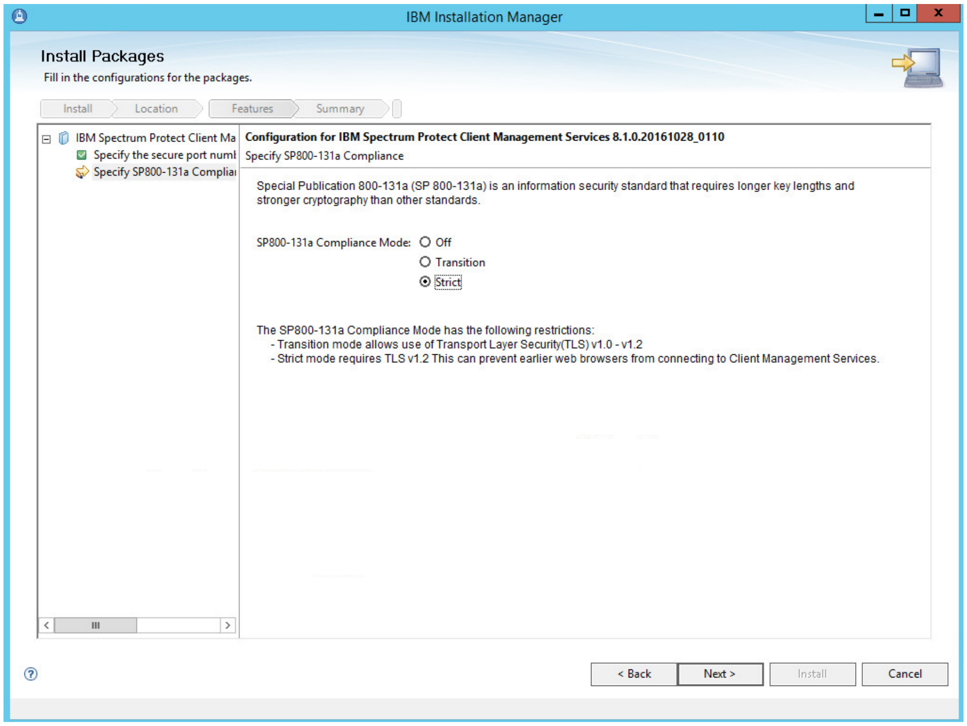
The port number is used by the web server for the IBM Spectrum Protect Client Management Services. You can accept the default value, or specify another port number.

Secure (https) port 9028

The port number has the following restrictions:
- The port number must be an integer in the range 1024 - 65535.
- The port number must be unique.
- The port number cannot be already in use or allocated to other programs.

11. Click **Next**.

12. Click **Strict** for **SP800-131a compliance**.



Install Packages

Fill in the configurations for the packages.

IBM Spectrum Protect Client Ma
Specify the secure port numl
Specify SP800-131a Complia

Configuration for IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110

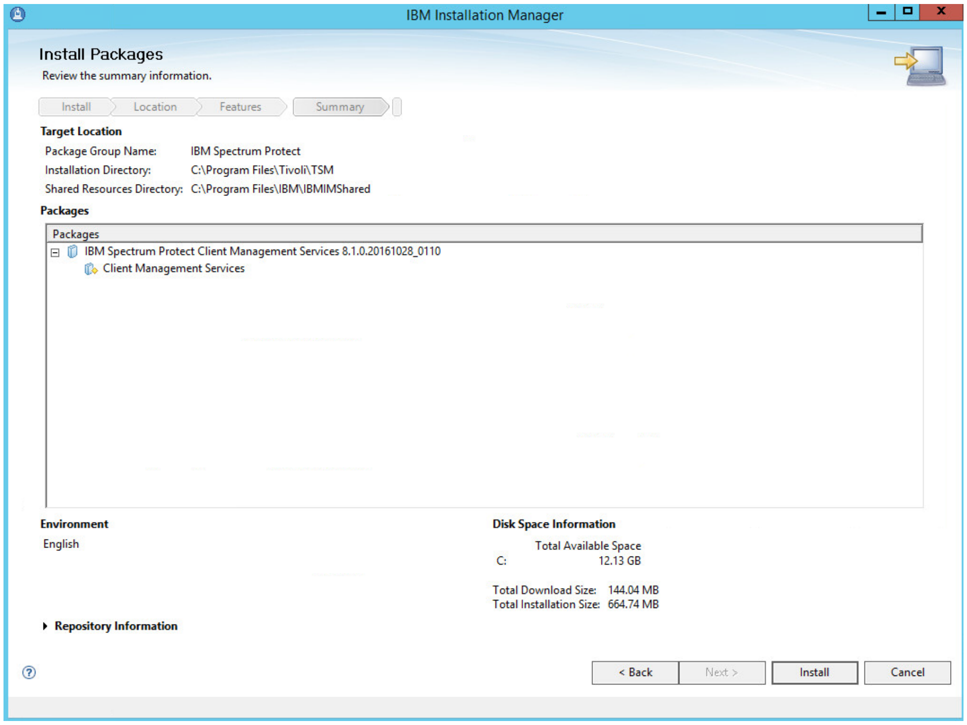
Specify SP800-131a Compliance

Special Publication 800-131a (SP 800-131a) is an information security standard that requires longer key lengths and stronger cryptography than other standards.

SP800-131a Compliance Mode: ○ Off
○ Transition
● Strict

The SP800-131a Compliance Mode has the following restrictions:
- Transition mode allows use of Transport Layer Security(TLS) v1.0 - v1.2
- Strict mode requires TLS v1.2 This can prevent earlier web browsers from connecting to Client Management Services.

13. Click **Next**.



Install Packages

Review the summary information.

Target Location

Package Group Name:	IBM Spectrum Protect
Installation Directory:	C:\Program Files\Tivoli\TSM
Shared Resources Directory:	C:\Program Files\IBM\IBMIMShared

Packages

Packages
IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110
Client Management Services

Environment

English

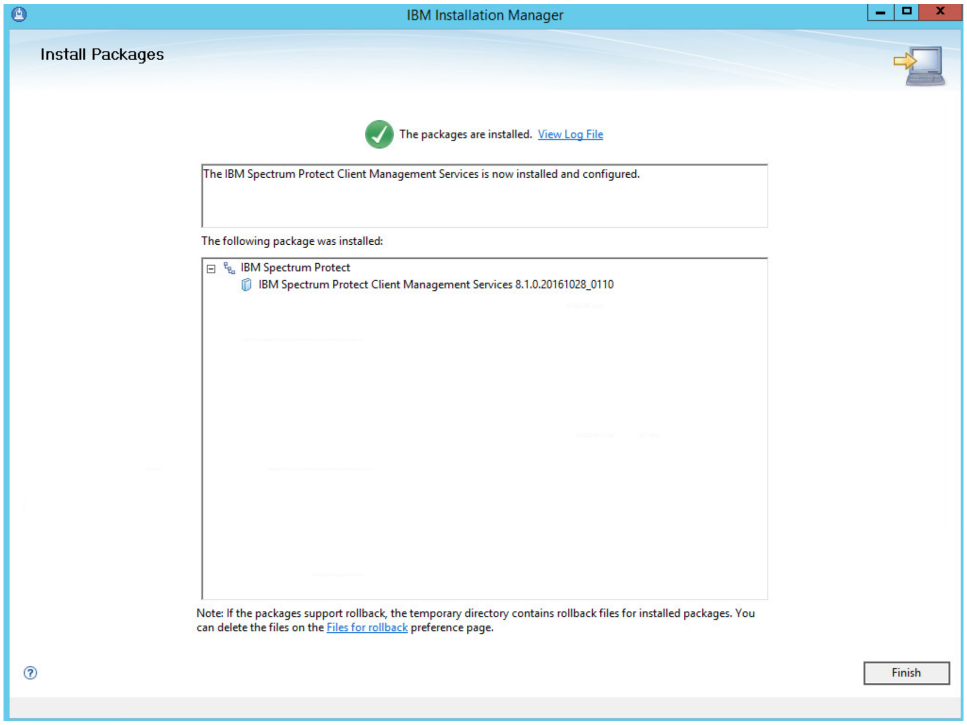
Disk Space Information

	Total Available Space
C:	12.13 GB

Total Download Size: 144.04 MB
Total Installation Size: 664.74 MB

Repository Information

14. Click **Install**.



The packages are installed. View Log File

The IBM Spectrum Protect Client Management Services is now installed and configured.

The following package was installed:

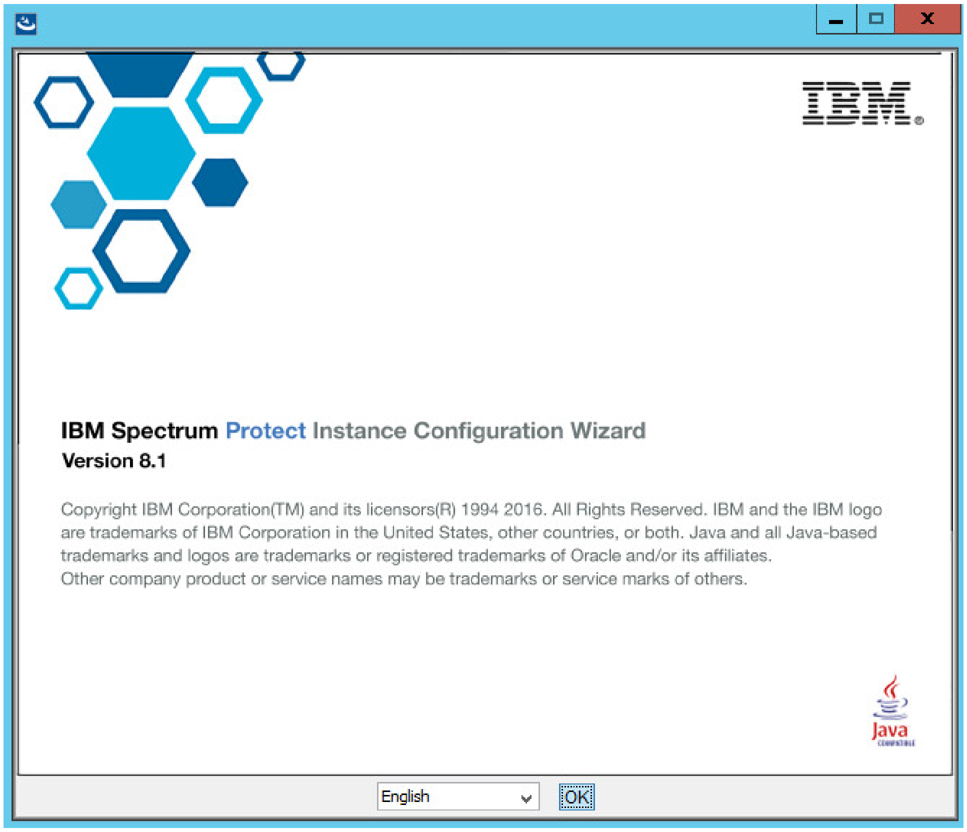
IBM Spectrum Protect
IBM Spectrum Protect Client Management Services 8.1.0.20161028_0110

Note: If the packages support rollback, the temporary directory contains rollback files for installed packages. You can delete the files on the Files for rollback preference page.

15. Observe the successful installation and click **Finish**.

2.7.3 Configure IBM Spectrum Protect

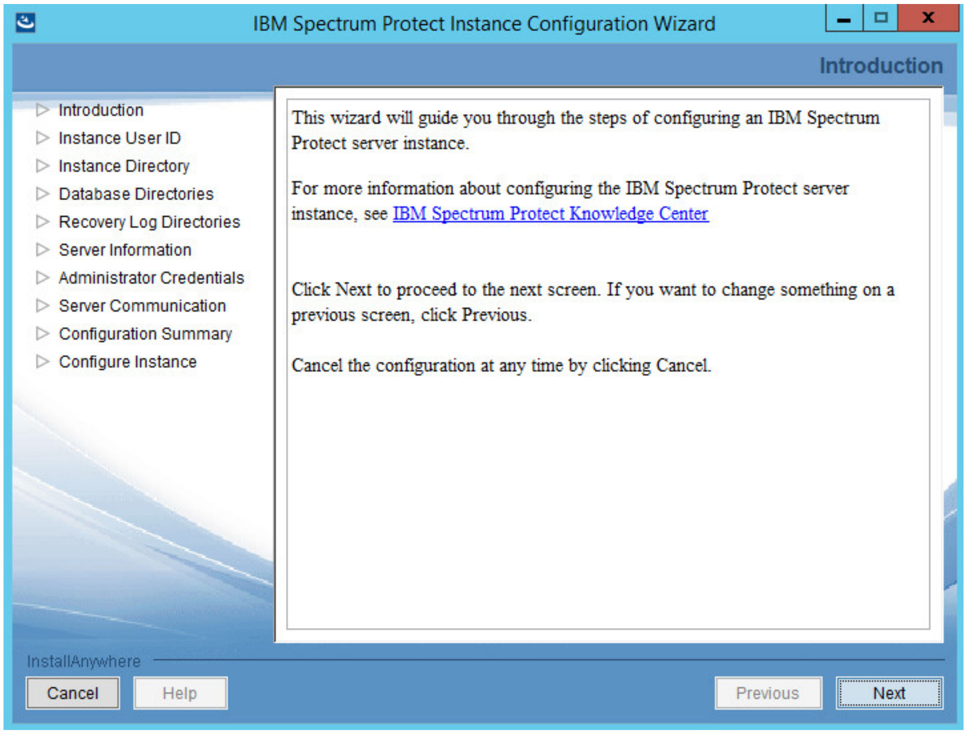
1. Go to **Start > IBM Spectrum Protect Configuration Wizard**.



IBM Spectrum Protect Instance Configuration Wizard
Version 8.1

Copyright IBM Corporation(TM) and its licensors(R) 1994 2016. All Rights Reserved. IBM and the IBM logo are trademarks of IBM Corporation in the United States, other countries, or both. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Other company product or service names may be trademarks or service marks of others.

2. Click **OK**.



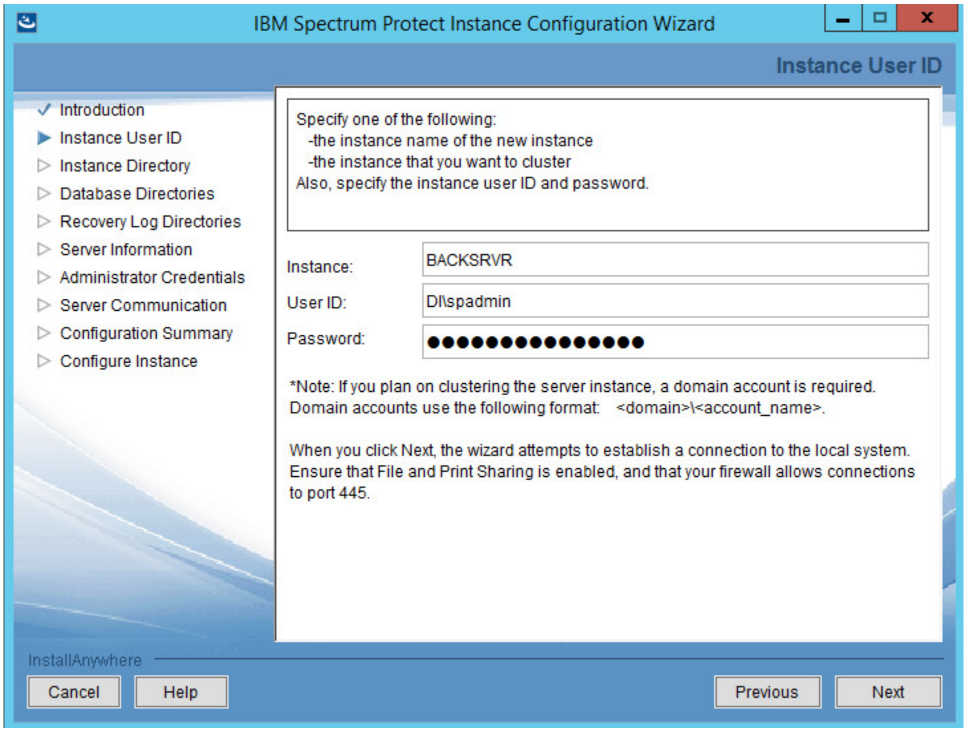
This wizard will guide you through the steps of configuring an IBM Spectrum Protect server instance.

For more information about configuring the IBM Spectrum Protect server instance, see IBM Spectrum Protect Knowledge Center

Click Next to proceed to the next screen. If you want to change something on a previous screen, click Previous.

Cancel the configuration at any time by clicking Cancel.

3. Click **Next**.
4. Specify a name and an account for the IBM server to use. Example: (name: BACKSRVR, User ID: DI\spadmin).



Specify one of the following:
-the instance name of the new instance
-the instance that you want to cluster
Also, specify the instance user ID and password.

Instance: BACKSRVR

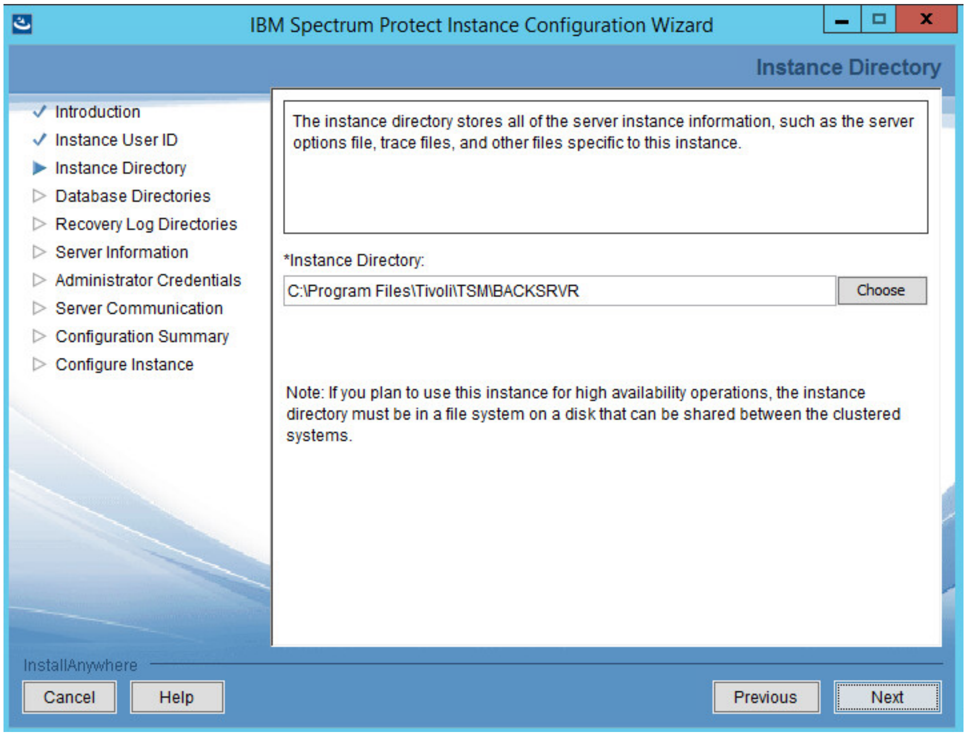
User ID: DI\spadmin

Password: ●●●●●●●●●●●●●●●

*Note: If you plan on clustering the server instance, a domain account is required. Domain accounts use the following format: <domain>\<account_name>.

When you click Next, the wizard attempts to establish a connection to the local system. Ensure that File and Print Sharing is enabled, and that your firewall allows connections to port 445.

5. Click **Next**.
6. Choose a directory.



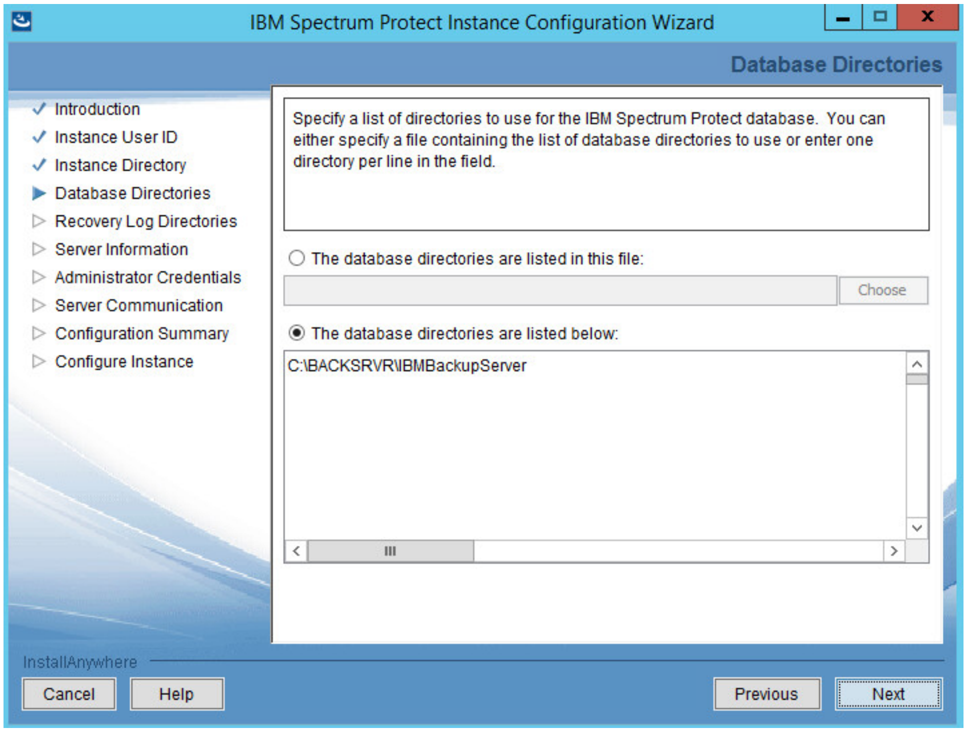
The instance directory stores all of the server instance information, such as the server options file, trace files, and other files specific to this instance.

*Instance Directory:

C:\Program Files\Tivoli\TSM\BACKSRVR

Note: If you plan to use this instance for high availability operations, the instance directory must be in a file system on a disk that can be shared between the clustered systems.

7. Click **Next**.
8. Click **Yes** if prompted to create the directory.
9. Choose **The database directories are listed below**.
10. Create a directory to contain the database. Example: *C:\BACKSRVR\IBMBackupServer.*
11. Enter the directory in the space provided.



Specify a list of directories to use for the IBM Spectrum Protect database. You can either specify a file containing the list of database directories to use or enter one directory per line in the field.

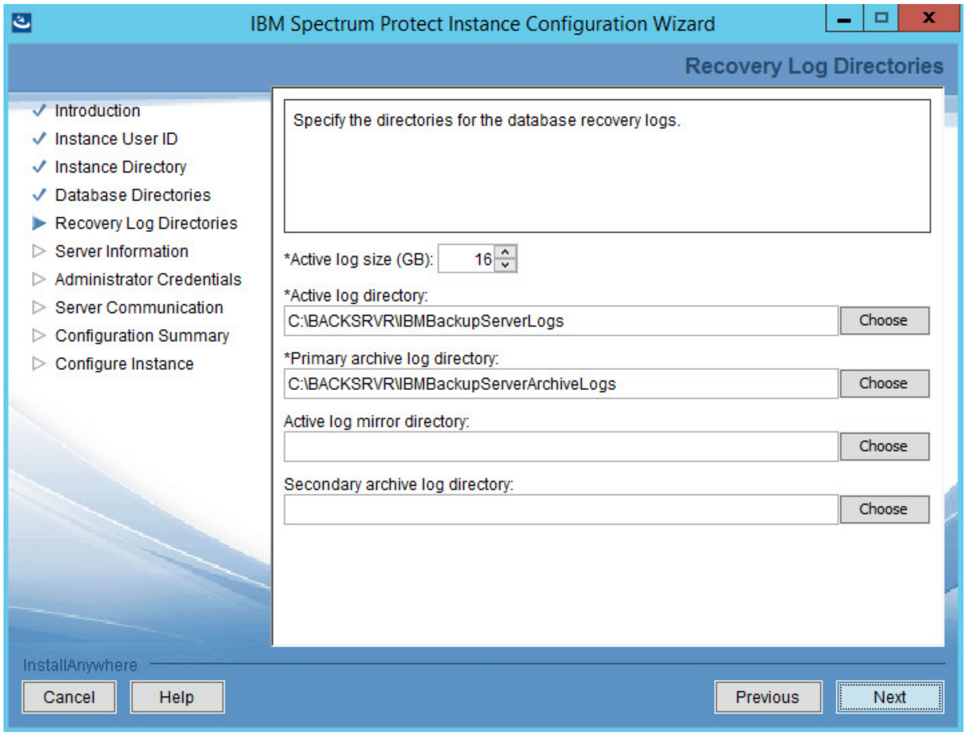
○ The database directories are listed in this file:

● The database directories are listed below:

C:\BACKSRVR\IBMBackupServer

12. Click **Next**.
13. Create directories for **logs** and **archive logs**. Example: *C:\BACKSRVR\IBMBackupServerLogs*, *C:\BACKSRVR\IBMBackupServerArchiveLogs*.

14. Enter the directories in their respective fields.



Specify the directories for the database recovery logs.

*Active log size (GB): 16

*Active log directory: C:\BACKSRVR\IBMBackupServerLogs

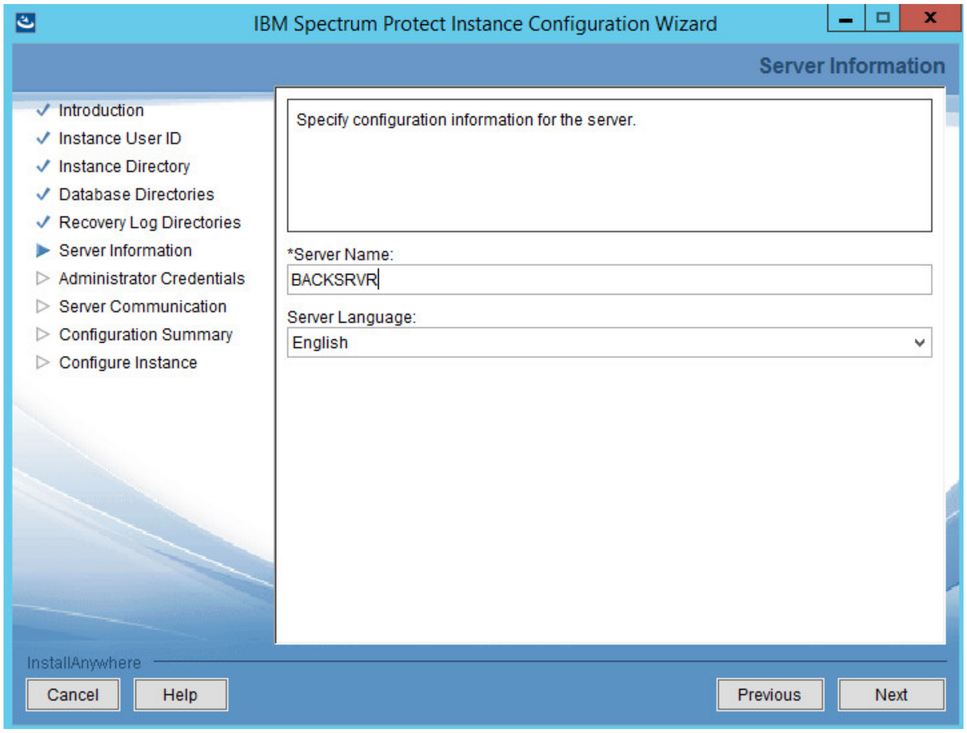
*Primary archive log directory: C:\BACKSRVR\IBMBackupServerArchiveLogs

Active log mirror directory:

Secondary archive log directory:

15. Click **Next**.

16. Specify the **server name**.



IBM Spectrum Protect Instance Configuration Wizard

Server Information

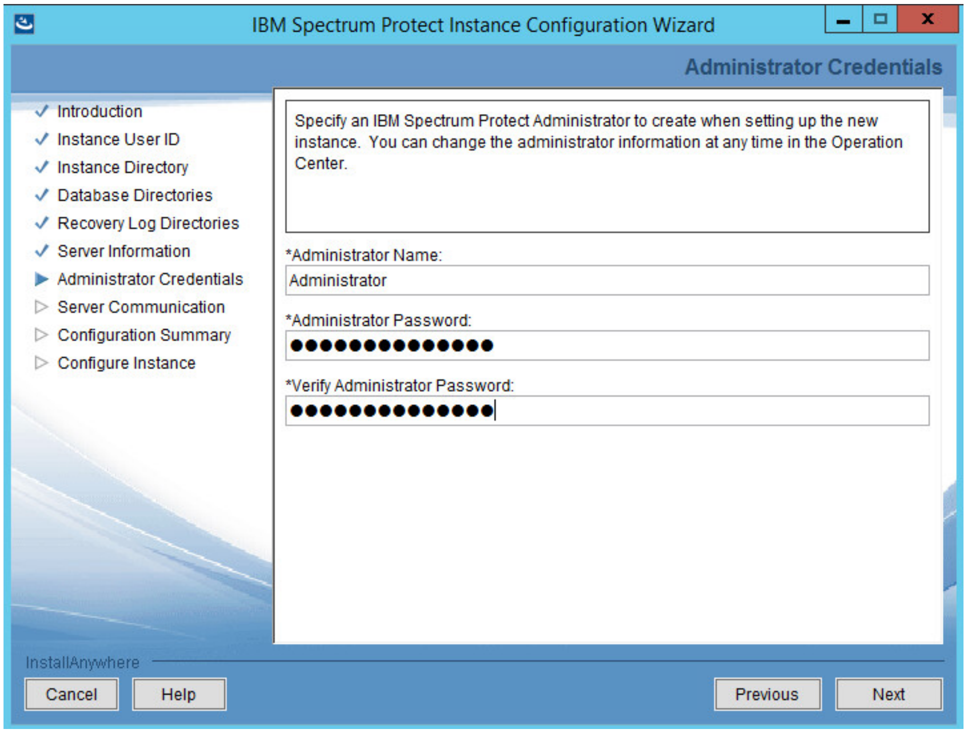
Specify configuration information for the server.

*Server Name: BACKSRVR

Server Language: English

17. Click **Next**.

18. Specify an **Administrator account**.



Specify an IBM Spectrum Protect Administrator to create when setting up the new instance. You can change the administrator information at any time in the Operation Center.

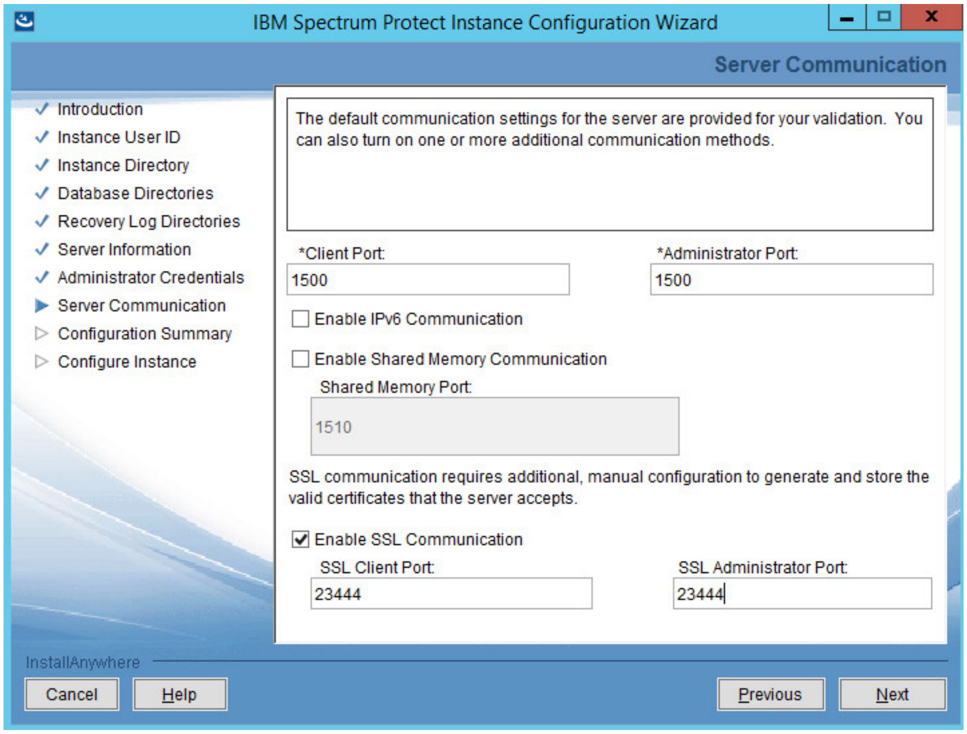
*Administrator Name: Administrator

*Administrator Password: ●●●●●●●●●●●●●●

*Verify Administrator Password: ●●●●●●●●●●●●●●

19. Click **Next**.
20. Select a **port.** Example: 1500.

21. Check the box next to **Enable SSL Communication** and enter a **port**. Example: 23444.



The default communication settings for the server are provided for your validation. You can also turn on one or more additional communication methods.

*Client Port: 1500

*Administrator Port: 1500

☐ Enable IPv6 Communication

☐ Enable Shared Memory Communication

Shared Memory Port: 1510

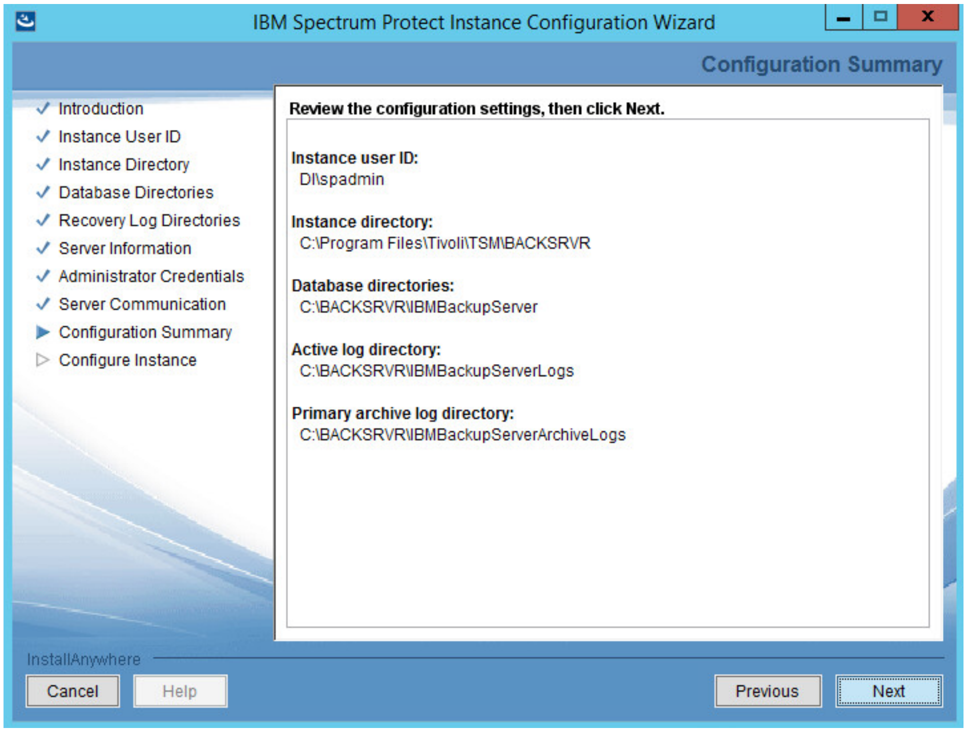
SSL communication requires additional, manual configuration to generate and store the valid certificates that the server accepts.

☑ Enable SSL Communication

SSL Client Port: 23444

SSL Administrator Port: 23444

22. Click **Next**.



Review the configuration settings, then click Next.

Instance user ID:
DI\spadmin

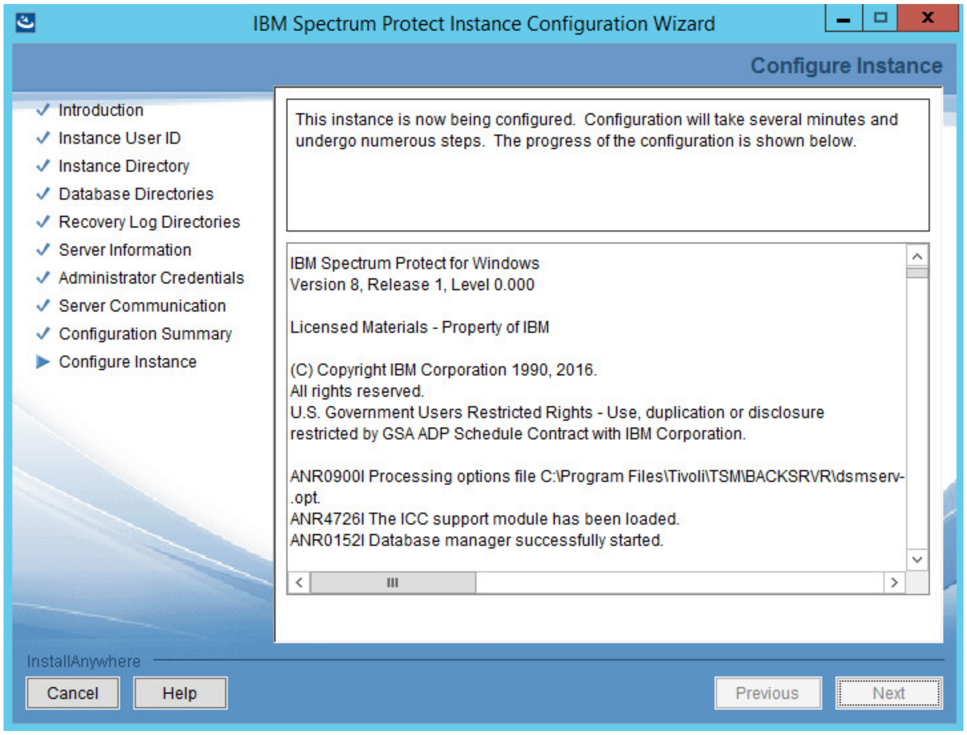
Instance directory:
C:\Program Files\Tivoli\TSM\BACKSRVR

Database directories:
C:\BACKSRVR\IBMBackupServer

Active log directory:
C:\BACKSRVR\IBMBackupServerLogs

Primary archive log directory:
C:\BACKSRVR\IBMBackupServerArchiveLogs

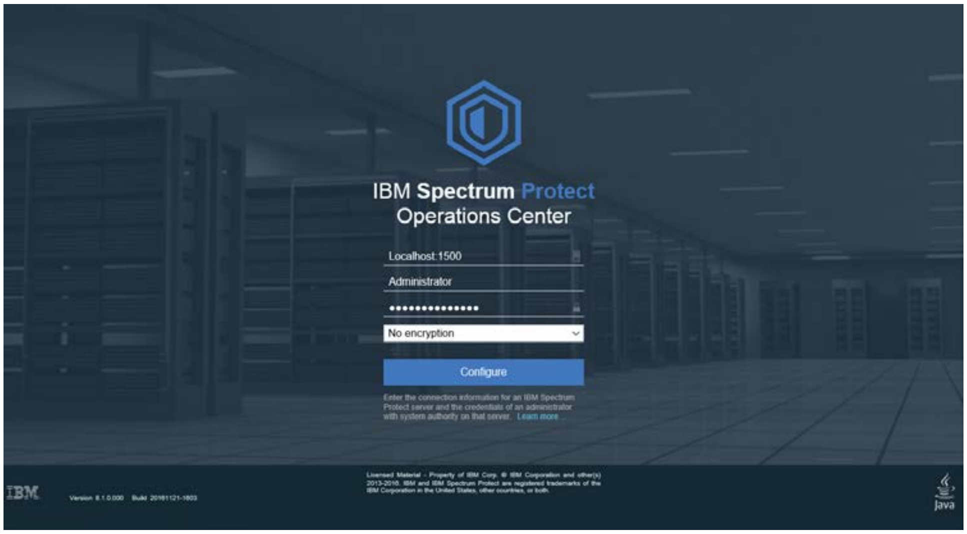
23. Click **Next**.
24. Wait for the installation to finish.



This instance is now being configured. Configuration will take several minutes and undergo numerous steps. The progress of the configuration is shown below.

```
IBM Spectrum Protect for Windows
Version 8, Release 1, Level 0.000

Licensed Materials - Property of IBM

(C) Copyright IBM Corporation 1990, 2016.
All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corporation.

ANR0900I Processing options file C:\Program Files\Tivoli\TSM\BACKSRVR\dsmserv-
.opt.
ANR4726I The ICC support module has been loaded.
ANR0152I Database manager successfully started.
```

25. Click **Next**.
26. Click **Done**.
27. Log in to **Operations Center** by going to **localhost:11090/oc/**. If issues occur, check firewall permissions for ports 1500 and 23444 (or whichever ports were designated in steps 20 and 21).



Localhost:1500
Administrator
•••••••••••••••
No encryption

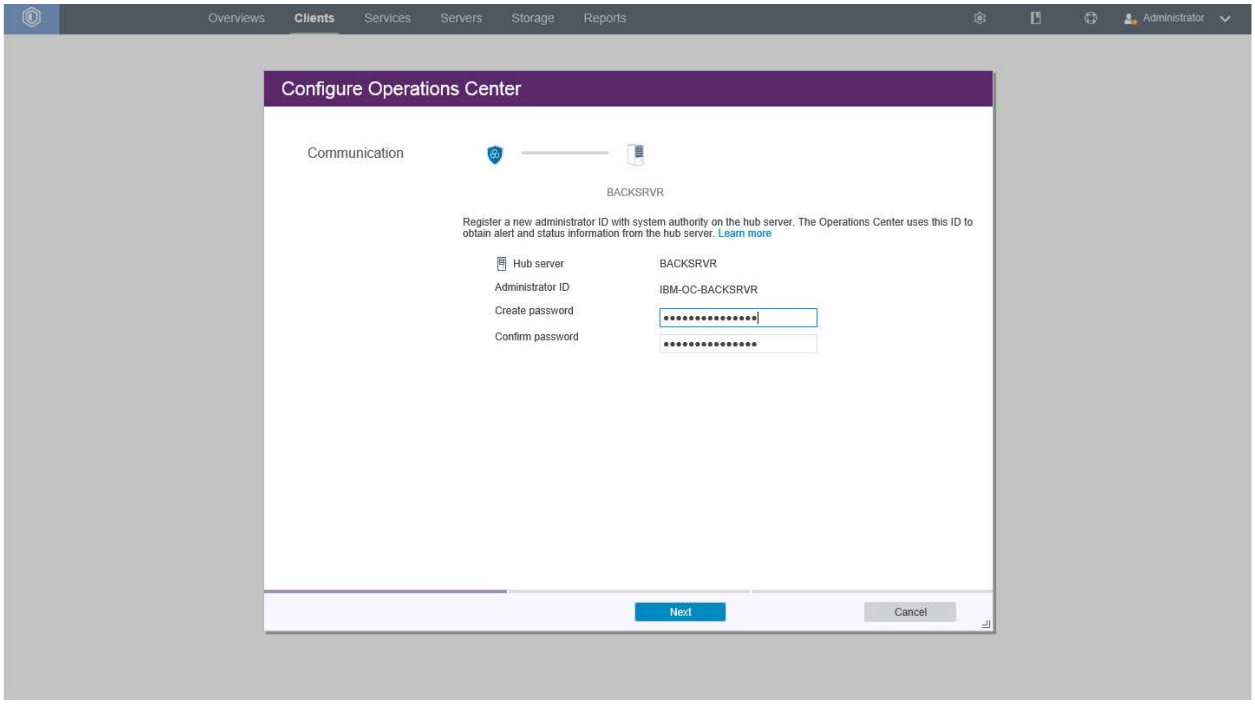
Enter the connection information for an IBM Spectrum Protect server and the credentials of an administrator with system authority on that server. Learn more ...

Version 8.1.0.000 Build 20161121-1603

Licensed Material - Property of IBM Corp. © IBM Corporation and other(s) 2013-2016. IBM and IBM Spectrum Protect are registered trademarks of the IBM Corporation in the United States, other countries, or both.

28. Log in using the credentials provided in the **Configuration Wizard**.

29. Enter the password for a new account to be created on the system.



Configure Operations Center

Communication

BACKSRVR

Register a new administrator ID with system authority on the hub server. The Operations Center uses this ID to obtain alert and status information from the hub server. Learn more

Hub server BACKSRVR

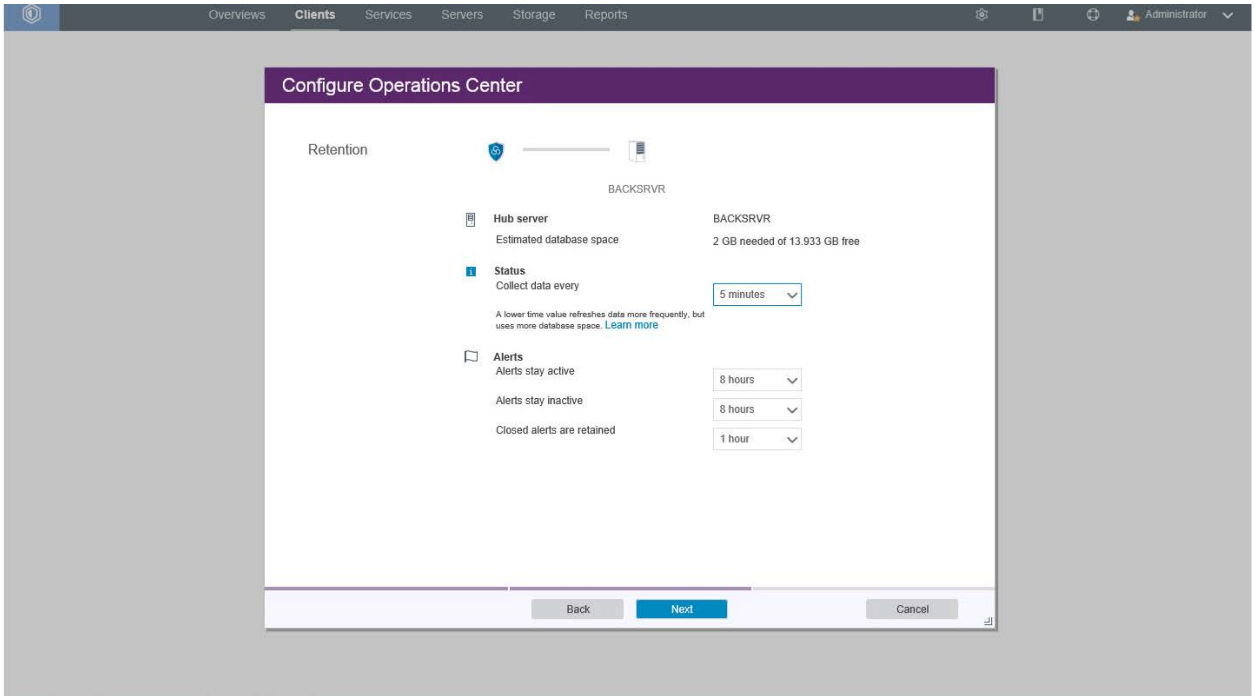
Administrator ID IBM-OC-BACKSRVR

Create password •••••••••••••••

Confirm password •••••••••••••••

30. Click **Next**.

31. Select the time interval for data collection.



Configure Operations Center

Retention

BACKSRVR

Hub server BACKSRVR

Estimated database space 2 GB needed of 13.933 GB free

Status

Collect data every 5 minutes

A lower time value refreshes data more frequently, but uses more database space. Learn more

Alerts

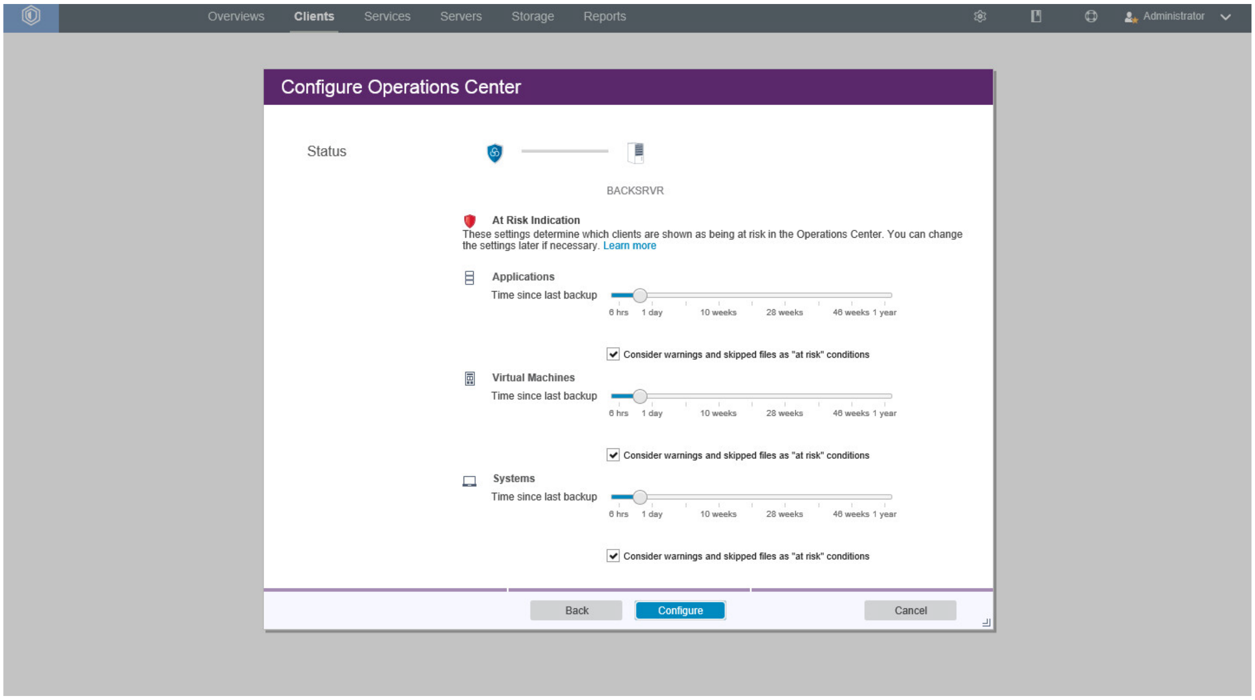
Alerts stay active 8 hours

Alerts stay inactive 8 hours

Closed alerts are retained 1 hour

32. Click **Next**.

33. Select time intervals that suit your organization's needs.



Configure Operations Center

Status

BACKSRVR

At Risk Indication

These settings determine which clients are shown as being at risk in the Operations Center. You can change the settings later if necessary. Learn more

Applications

Time since last backup

6 hrs 1 day 10 weeks 28 weeks 46 weeks 1 year

☑ Consider warnings and skipped files as "at risk" conditions

Virtual Machines

Time since last backup

6 hrs 1 day 10 weeks 28 weeks 46 weeks 1 year

☑ Consider warnings and skipped files as "at risk" conditions

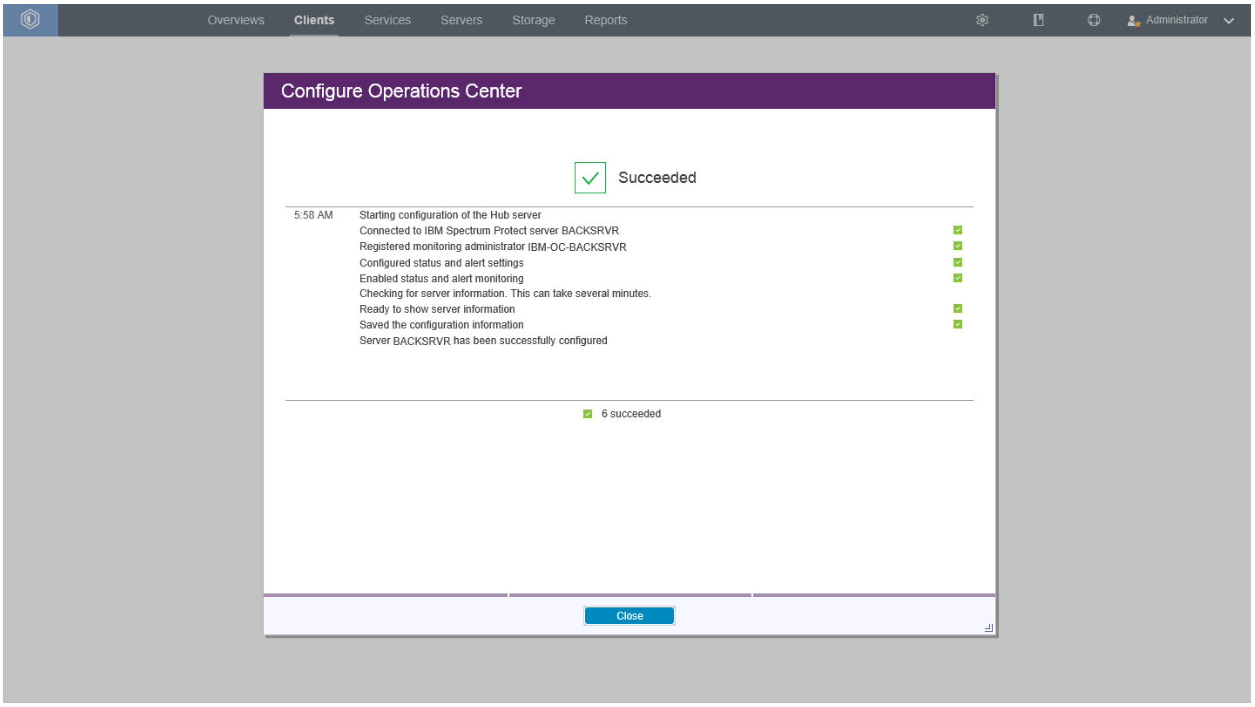
Systems

Time since last backup

6 hrs 1 day 10 weeks 28 weeks 46 weeks 1 year

☑ Consider warnings and skipped files as "at risk" conditions

34. Click **Configure**.



Configure Operations Center

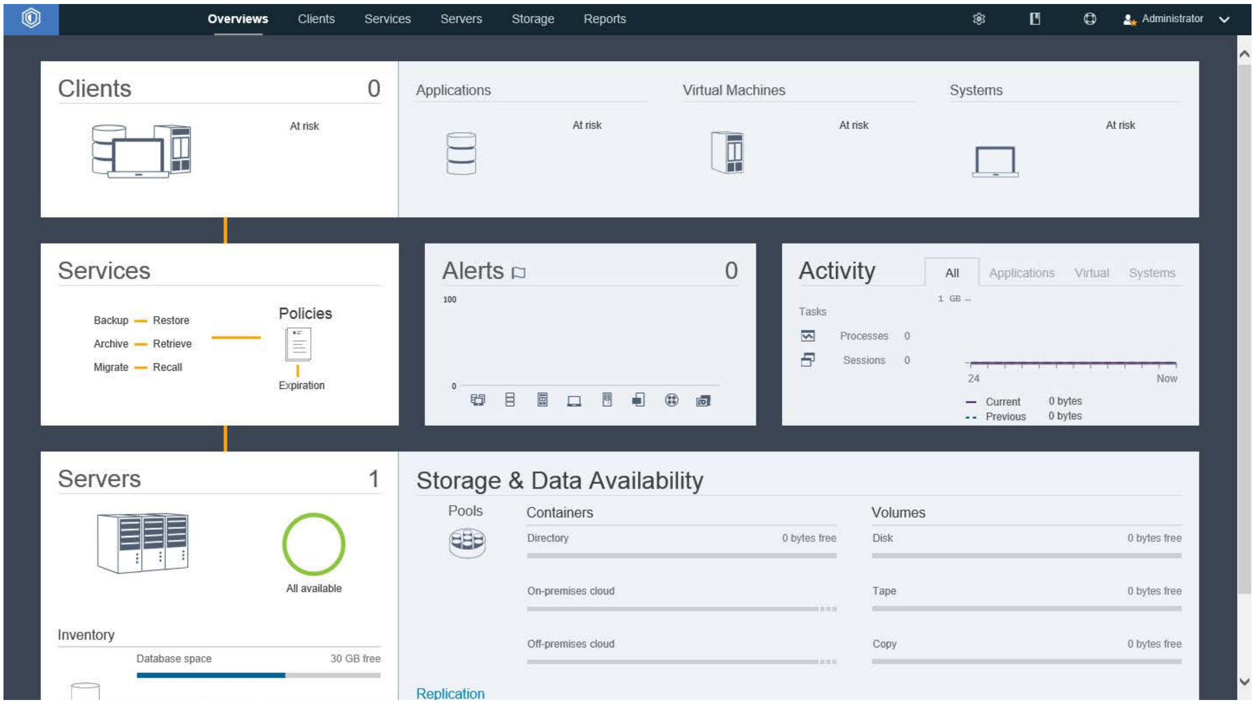
✓ Succeeded

```
5:58 AM   Starting configuration of the Hub server
          Connected to IBM Spectrum Protect server BACKSRVR                        ✓
          Registered monitoring administrator IBM-OC-BACKSRVR                      ✓
          Configured status and alert settings                                     ✓
          Enabled status and alert monitoring                                      ✓
          Checking for server information. This can take several minutes.
          Ready to show server information                                         ✓
          Saved the configuration information                                      ✓
          Server BACKSRVR has been successfully configured
```

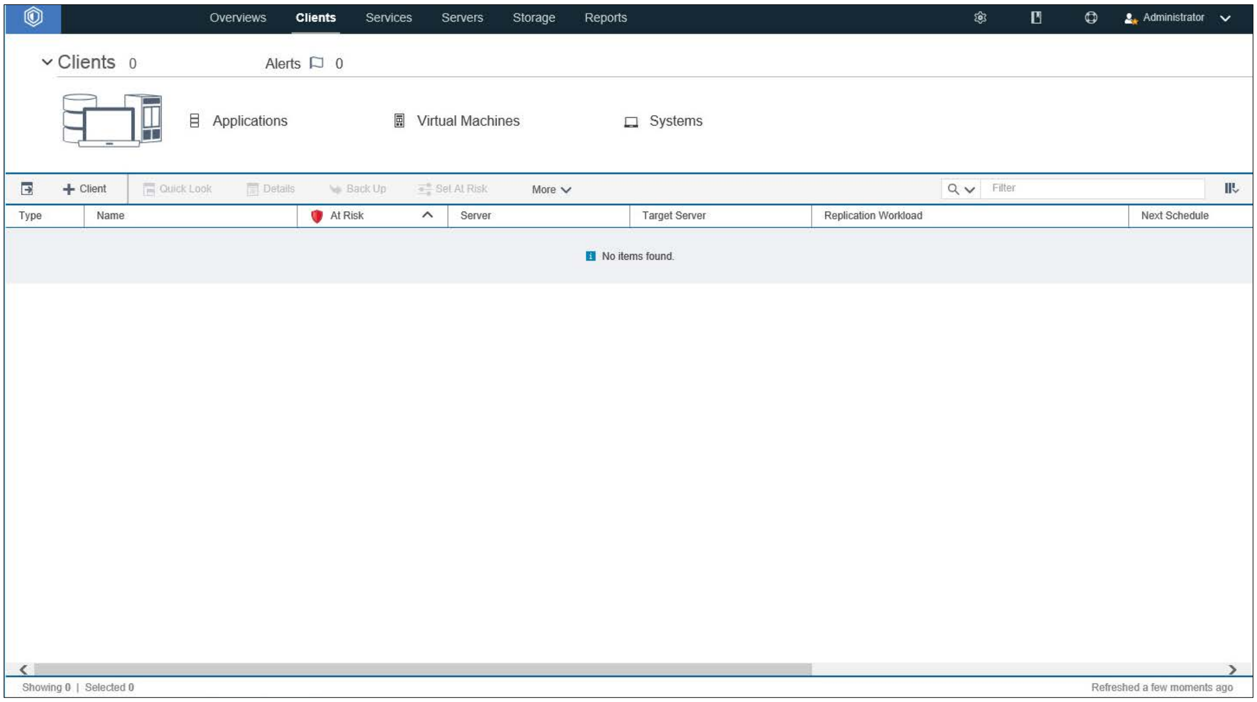
✓ 6 succeeded

2.7.4 Adding Clients to IBM Spectrum Protect

1. Log in to **Operations Center**.



2. Add clients by clicking the **Clients** tab.



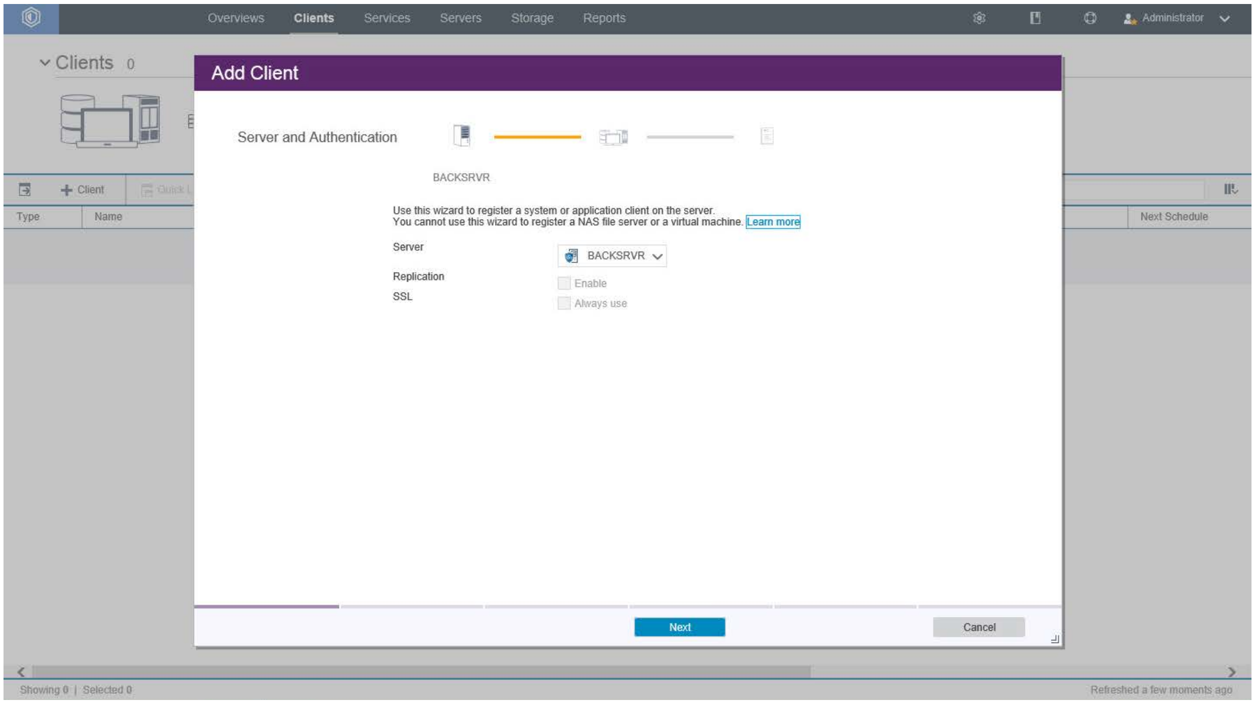
Type	Name	At Risk	Server	Target Server	Replication Workload	Next Schedule

No items found.

Showing 0 | Selected 0

Refreshed a few moments ago

3. Click **+Client**.



Add Client

Server and Authentication

BACKSRVR

Use this wizard to register a system or application client on the server.
You cannot use this wizard to register a NAS file server or a virtual machine. Learn more

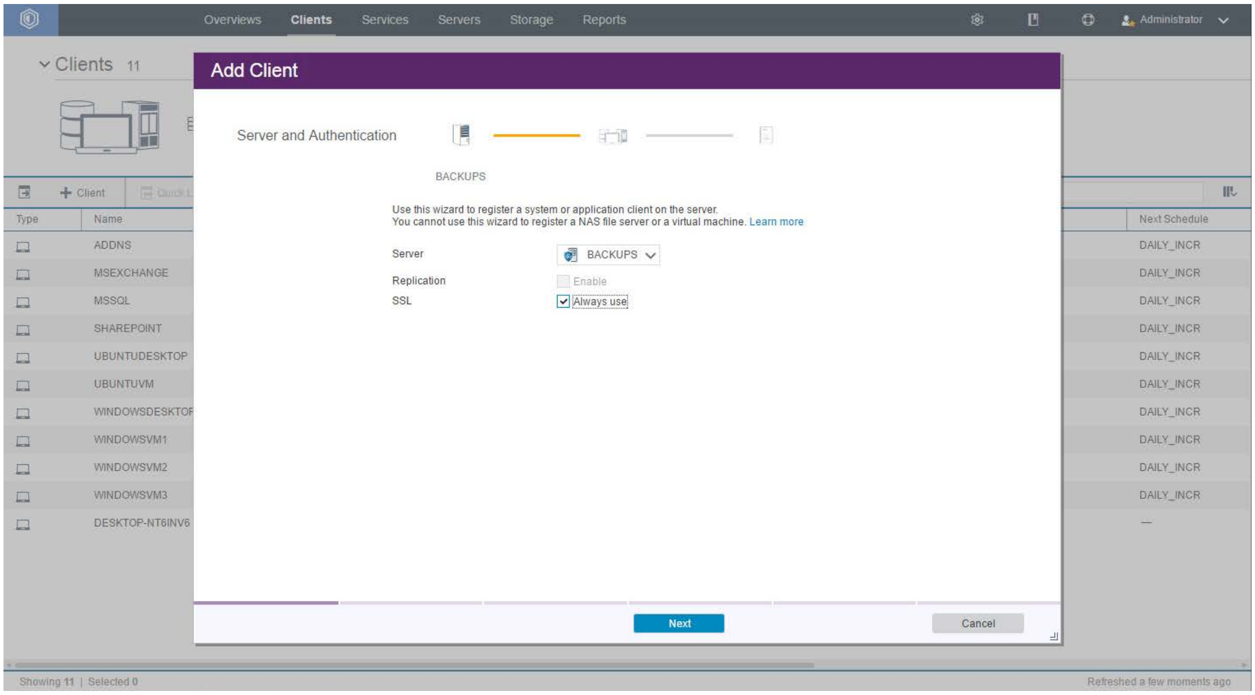
Server: BACKSRVR

Replication: ☐ Enable

SSL: ☐ Always use

4. Select the server running the IBM backup capabilities.

5. Check the box next to **Always use** for **SSL**.



BACKUPS

Use this wizard to register a system or application client on the server.
You cannot use this wizard to register a NAS file server or a virtual machine. Learn more

Server: BACKUPS

Replication: □ Enable

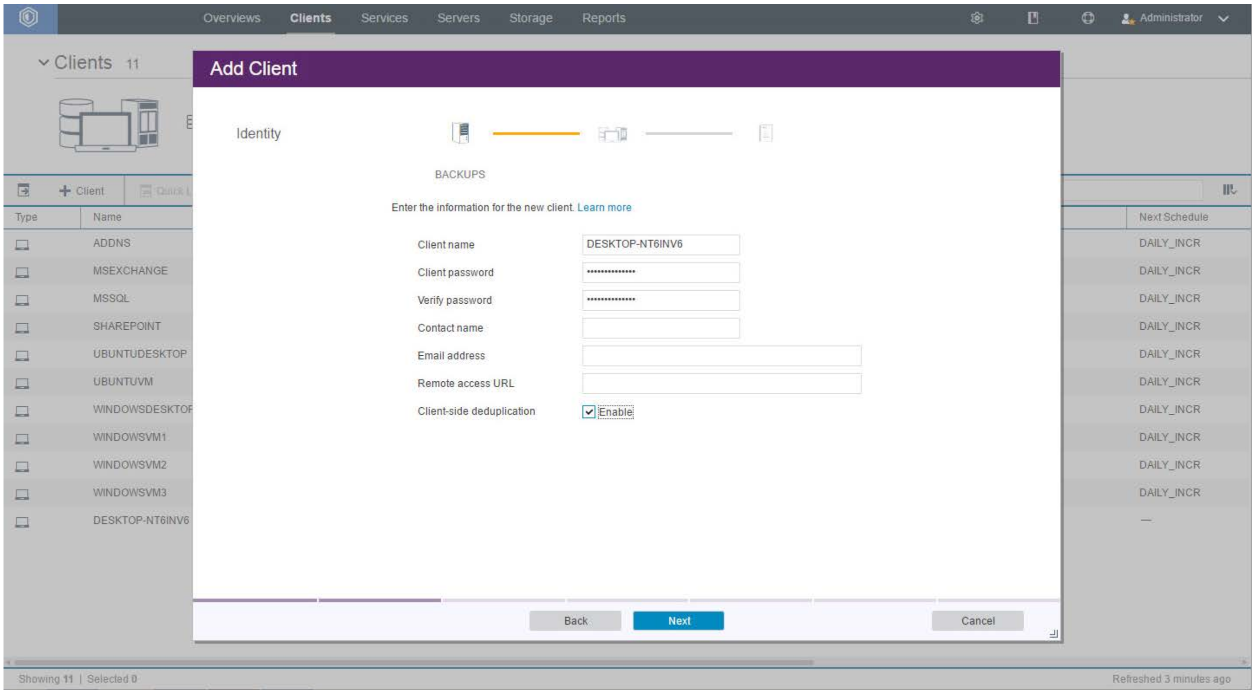
SSL: ☑ Always use

Name	Next Schedule
ADDNS	DAILY_INCR
MSEXCHANGE	DAILY_INCR
MSSQL	DAILY_INCR
SHAREPOINT	DAILY_INCR
UBUNTUDESKTOP	DAILY_INCR
UBUNTUVM	DAILY_INCR
WINDOWSDESKTOF	DAILY_INCR
WINDOWSVM1	DAILY_INCR
WINDOWSVM2	DAILY_INCR
WINDOWSVM3	DAILY_INCR
DESKTOP-NT6INV6	—

Showing 11 | Selected 0

Refreshed a few moments ago

6. Click **Next**.
7. Enter the name of a client machine that you want to be able to backup data from and a password.
8. Decide whether to use **Client-side deduplication** (it reduces the required storage space for backups).



Add Client

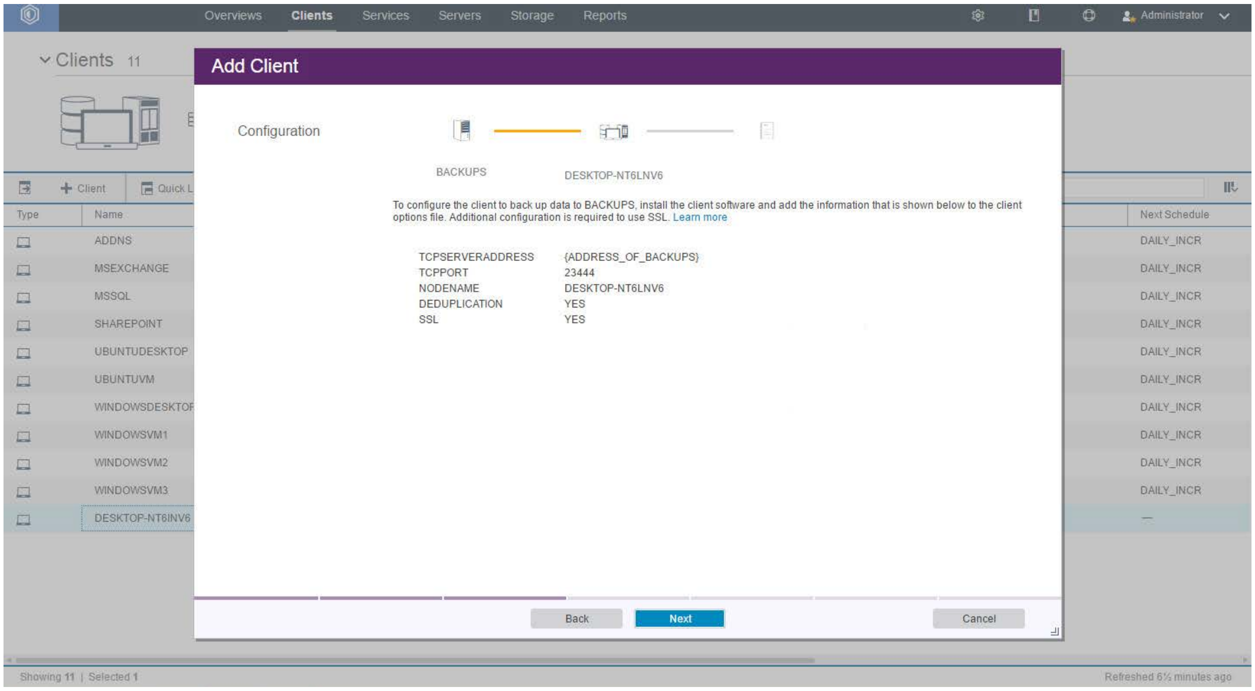
Identity

BACKUPS

Enter the information for the new client. Learn more

Client name	DESKTOP-NT6INV6
Client password	••••••••••••••
Verify password	••••••••••••••
Contact name	
Email address	
Remote access URL	
Client-side deduplication	☑ Enable

9. Click **Next**. Note the information on the next page as it is required to connect the server to the client.



Add Client

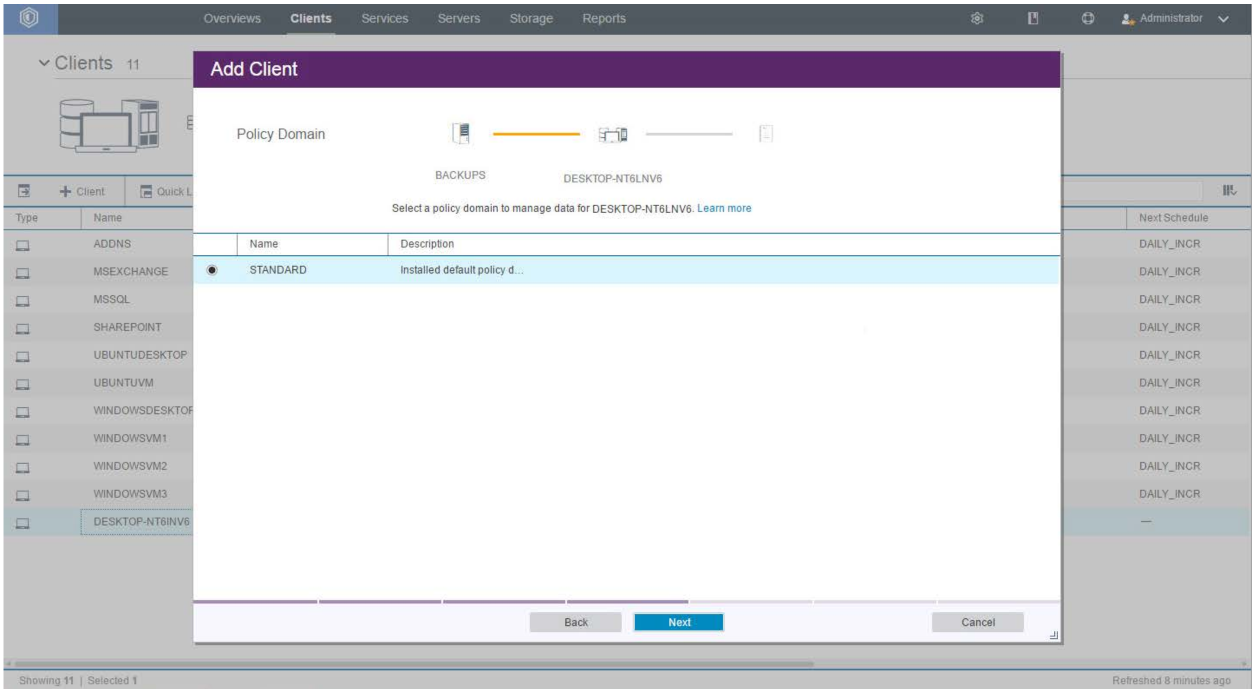
Configuration

BACKUPS DESKTOP-NT6LNV6

To configure the client to back up data to BACKUPS, install the client software and add the information that is shown below to the client options file. Additional configuration is required to use SSL. Learn more

```
TCPSERVERADDRESS     {ADDRESS_OF_BACKUPS}
TCPPORT              23444
NODENAME             DESKTOP-NT6LNV6
DEDUPLICATION        YES
SSL                  YES
```

10. Click **Next**.



Add Client

Policy Domain

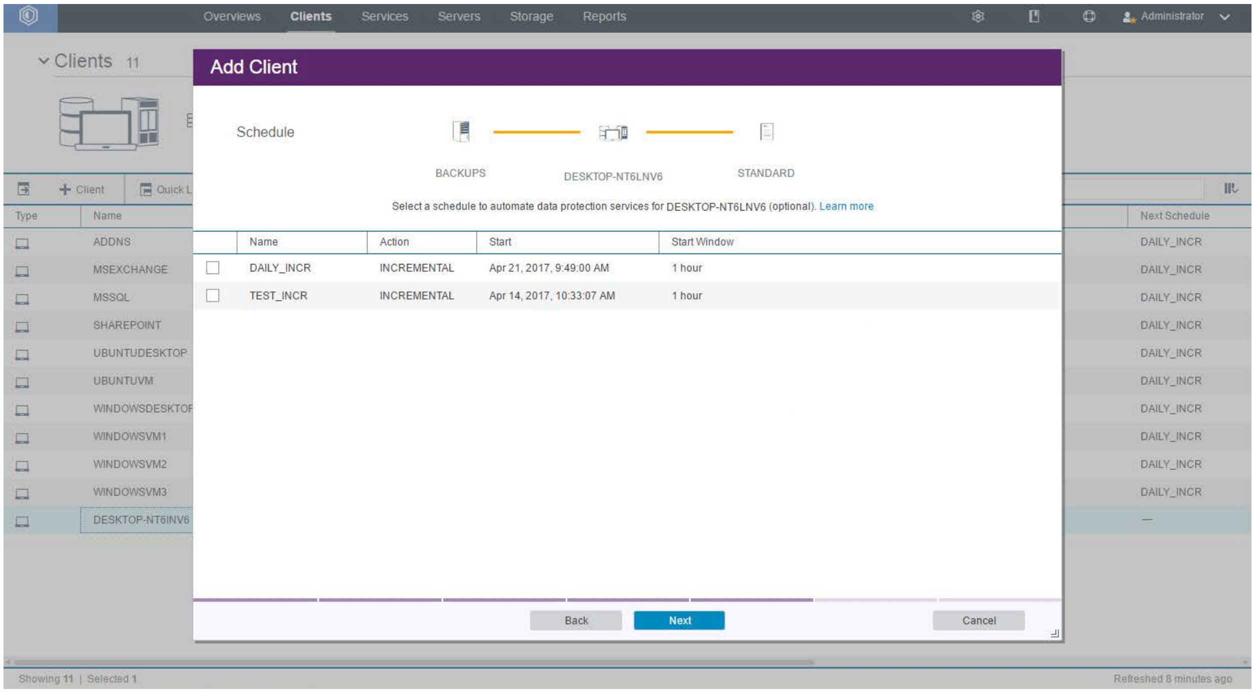
BACKUPS — DESKTOP-NT6LNV6

Select a policy domain to manage data for DESKTOP-NT6LNV6. Learn more

	Name	Description
●	STANDARD	Installed default policy d...

Type	Name	Next Schedule
	ADDNS	DAILY_INCR
	MSEXCHANGE	DAILY_INCR
	MSSQL	DAILY_INCR
	SHAREPOINT	DAILY_INCR
	UBUNTUDESKTOP	DAILY_INCR
	UBUNTUVM	DAILY_INCR
	WINDOWSDESKTOF	DAILY_INCR
	WINDOWSVM1	DAILY_INCR
	WINDOWSVM2	DAILY_INCR
	WINDOWSVM3	DAILY_INCR
	DESKTOP-NT6INV6	—

11. Click **Next**.



Add Client

Schedule

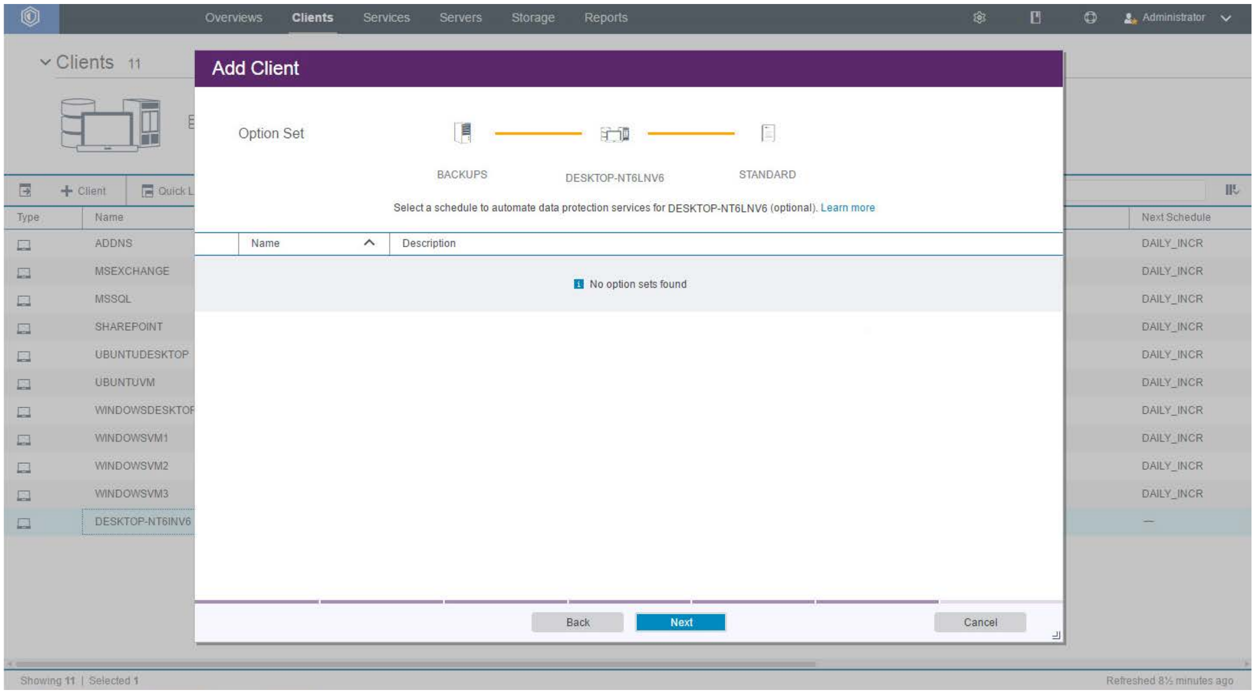
BACKUPS — DESKTOP-NT6LNV6 — STANDARD

Select a schedule to automate data protection services for DESKTOP-NT6LNV6 (optional). Learn more

	Name	Action	Start	Start Window
□	DAILY_INCR	INCREMENTAL	Apr 21, 2017, 9:49:00 AM	1 hour
□	TEST_INCR	INCREMENTAL	Apr 14, 2017, 10:33:07 AM	1 hour

Type	Name	Next Schedule
	ADDNS	DAILY_INCR
	MSEXCHANGE	DAILY_INCR
	MSSQL	DAILY_INCR
	SHAREPOINT	DAILY_INCR
	UBUNTUDESKTOP	DAILY_INCR
	UBUNTUVM	DAILY_INCR
	WINDOWSDESKTOF	DAILY_INCR
	WINDOWSVM1	DAILY_INCR
	WINDOWSVM2	DAILY_INCR
	WINDOWSVM3	DAILY_INCR
	DESKTOP-NT6INV6	—

12. Click **Next**.



Add Client

Option Set

BACKUPS — DESKTOP-NT6LNV6 — STANDARD

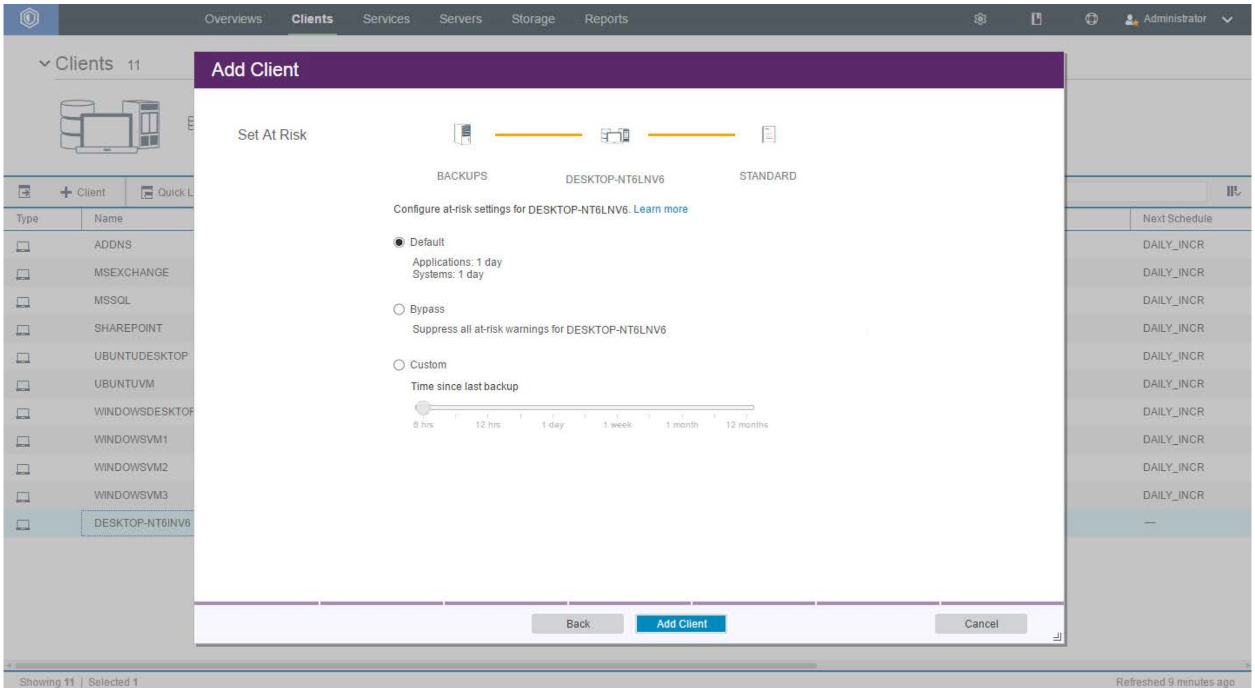
Select a schedule to automate data protection services for DESKTOP-NT6LNV6 (optional). Learn more

Name	Description

No option sets found

Type	Name	Next Schedule
	ADDNS	DAILY_INCR
	MSEXCHANGE	DAILY_INCR
	MSSQL	DAILY_INCR
	SHAREPOINT	DAILY_INCR
	UBUNTUDESKTOP	DAILY_INCR
	UBUNTUVM	DAILY_INCR
	WINDOWSDESKTOF	DAILY_INCR
	WINDOWSVM1	DAILY_INCR
	WINDOWSVM2	DAILY_INCR
	WINDOWSVM3	DAILY_INCR
	DESKTOP-NT6INV6	—

13. Click **Next**.
14. Select **Default**.



Add Client

Set At Risk

BACKUPS — DESKTOP-NT6LNV6 — STANDARD

Configure at-risk settings for DESKTOP-NT6LNV6. Learn more

● Default

Applications: 1 day
Systems: 1 day

○ Bypass

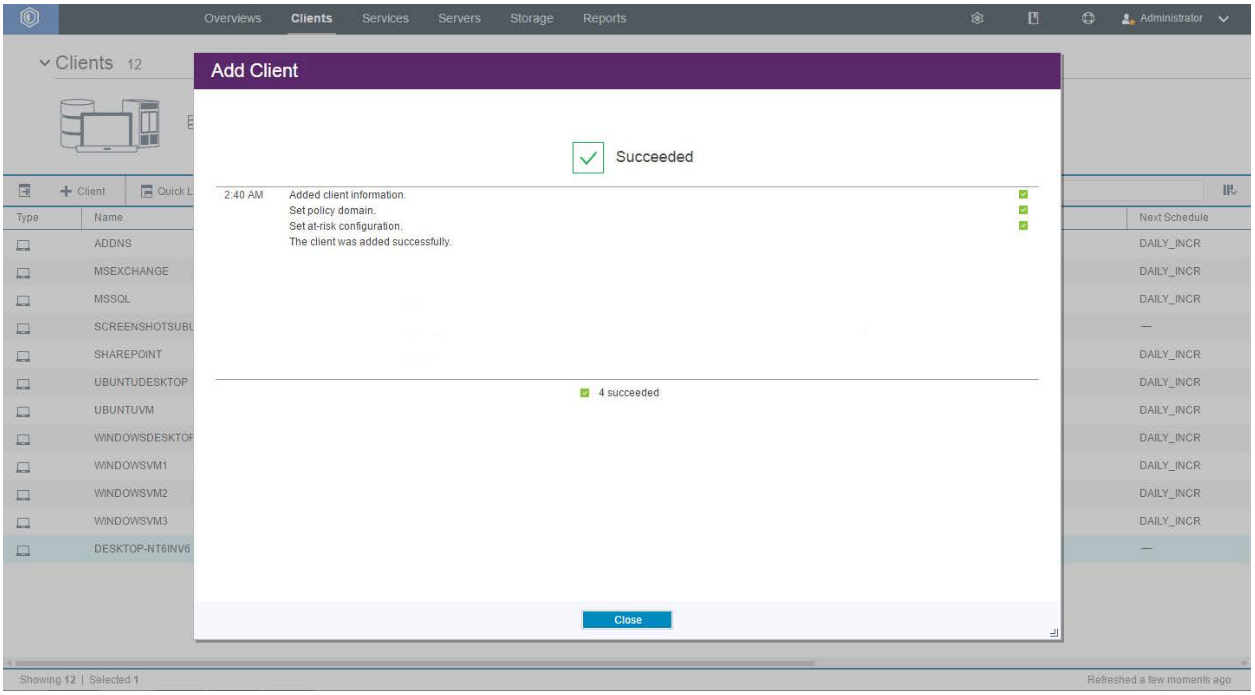
Suppress all at-risk warnings for DESKTOP-NT6LNV6

○ Custom

Time since last backup

Type	Name	Next Schedule
	ADDNS	DAILY_INCR
	MSEXCHANGE	DAILY_INCR
	MSSQL	DAILY_INCR
	SHAREPOINT	DAILY_INCR
	UBUNTUDESKTOP	DAILY_INCR
	UBUNTUVM	DAILY_INCR
	WINDOWSDESKTOF	DAILY_INCR
	WINDOWSVM1	DAILY_INCR
	WINDOWSVM2	DAILY_INCR
	WINDOWSVM3	DAILY_INCR
	DESKTOP-NT6INV6	—

15. Click **Add Client**.



Add Client

☑ Succeeded

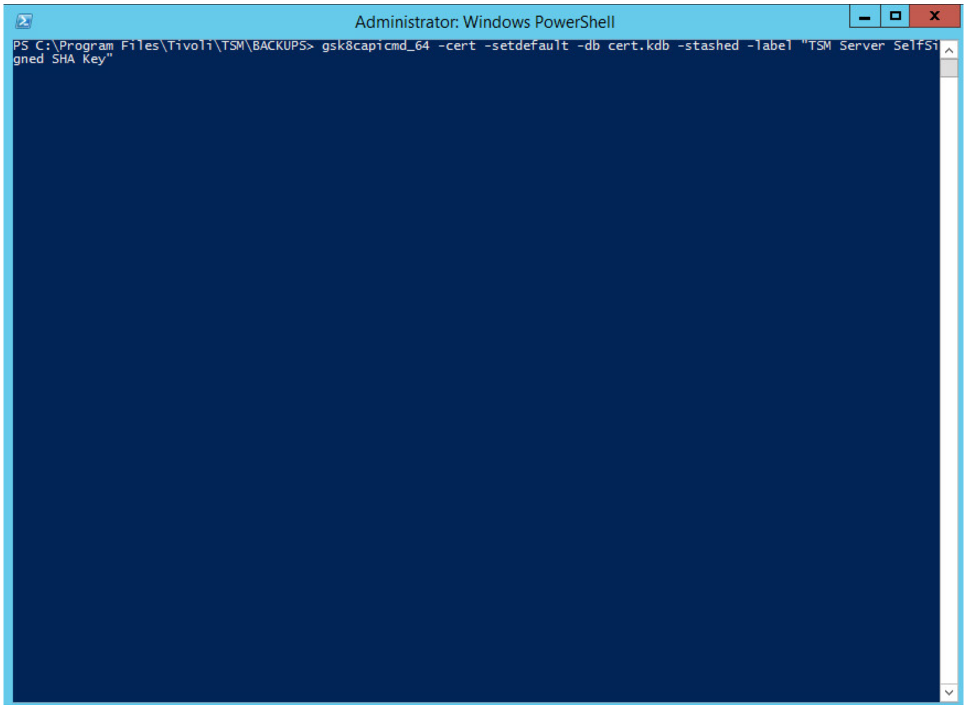
```
2:40 AM   Added client information.        ☑
          Set policy domain.               ☑
          Set at-risk configuration.       ☑
          The client was added successfully.
```

☑ 4 succeeded

16. Make sure to allow the ports for SSL and TCP traffic through the firewall (23444, 1500).
17. Run the following command to set **cert256.arm** as the default certificate on the IBM Backup server. Execute this command from the root server directory. Example: *C:\Program Files\Tivoli\TSM\BACKSRVR*

```
> gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server
SelfSigned SHA Key"
```

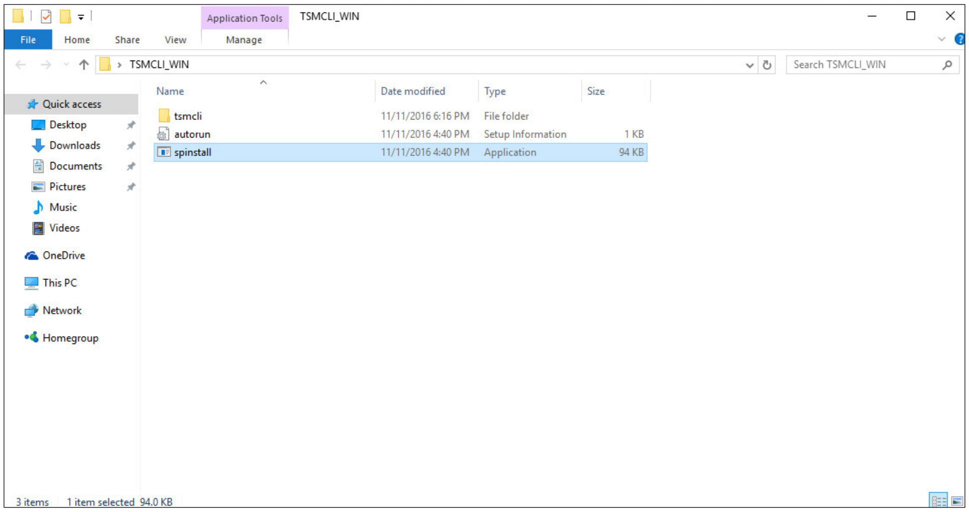
Note: By default, gsk8capicmd_64 is located at *C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin.*



```
PS C:\Program Files\Tivoli\TSM\BACKUPS> gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSi
gned SHA Key"
```

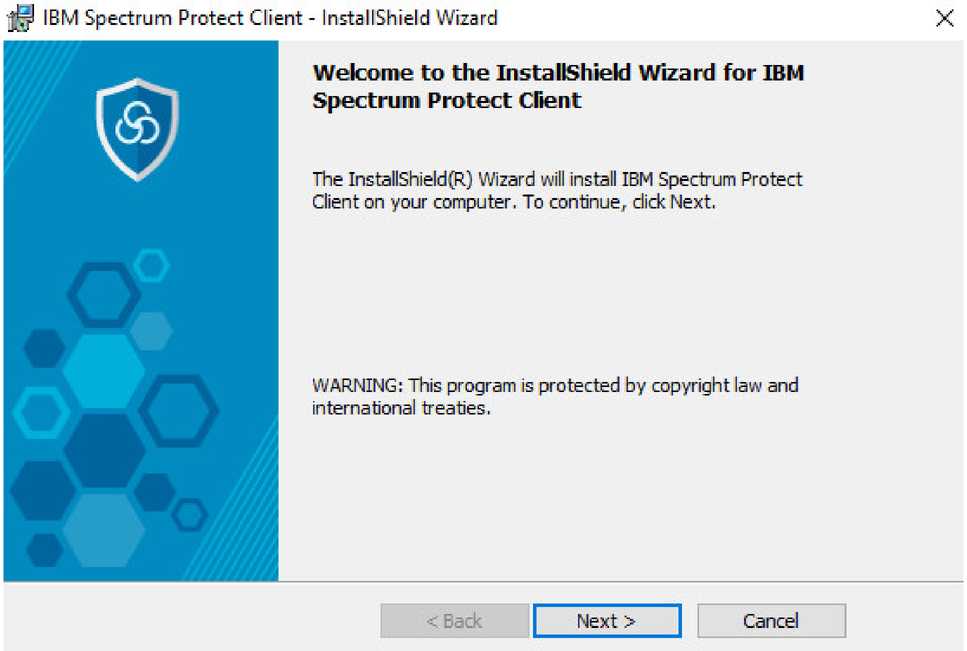
2.7.5 Install the Spectrum Protect Client on Windows

1. Extract **SP_CLIENT_8.1_WIN_ML**



Name	Date modified	Type	Size
tsmcli	11/11/2016 6:16 PM	File folder	
autorun	11/11/2016 4:40 PM	Setup Information	1 KB
spinstall	11/11/2016 4:40 PM	Application	94 KB

2. Run the **spinstall** script (install any prerequisites required).



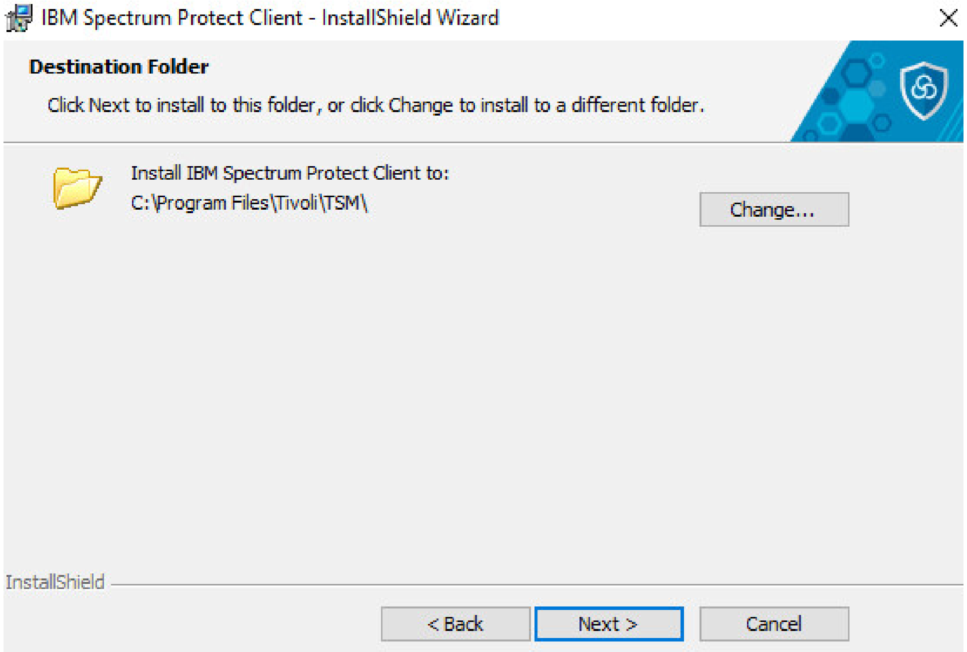
IBM Spectrum Protect Client - InstallShield Wizard

Welcome to the InstallShield Wizard for IBM Spectrum Protect Client

The InstallShield(R) Wizard will install IBM Spectrum Protect Client on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. Click **Next**.
4. Specify an installation path.



IBM Spectrum Protect Client - InstallShield Wizard

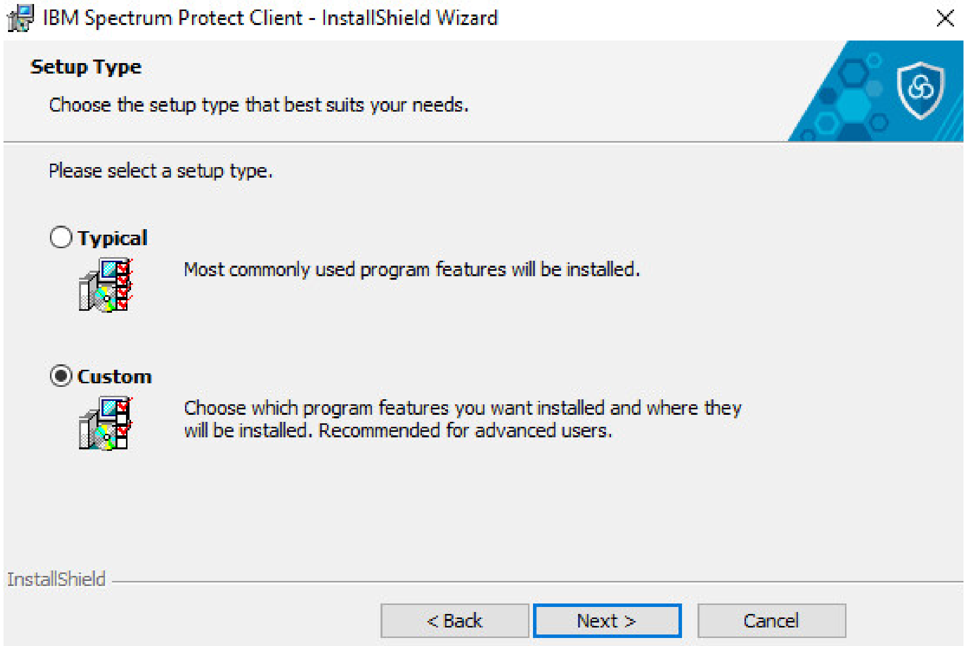
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install IBM Spectrum Protect Client to:
C:\Program Files\Tivoli\TSM\

5. Click **Next**.

6. Select **Custom Install**.



IBM Spectrum Protect Client - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

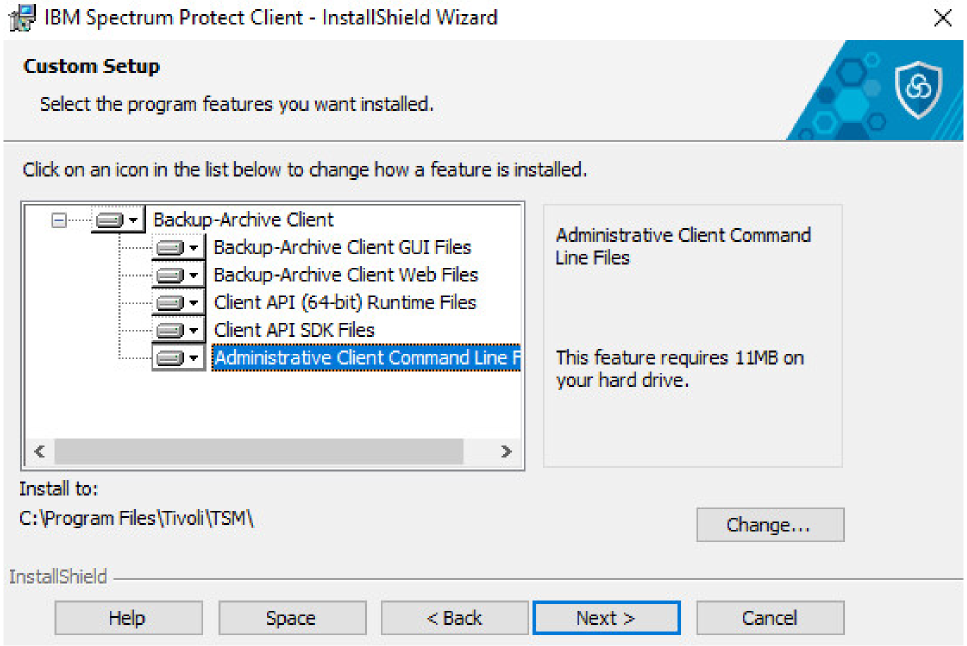
○ **Typical**

Most commonly used program features will be installed.

● **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

7. Click **Next**. Make sure that all packages are selected for installation.



IBM Spectrum Protect Client - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Backup-Archive Client
  - Backup-Archive Client GUI Files
  - Backup-Archive Client Web Files
  - Client API (64-bit) Runtime Files
  - Client API SDK Files
  - Administrative Client Command Line F

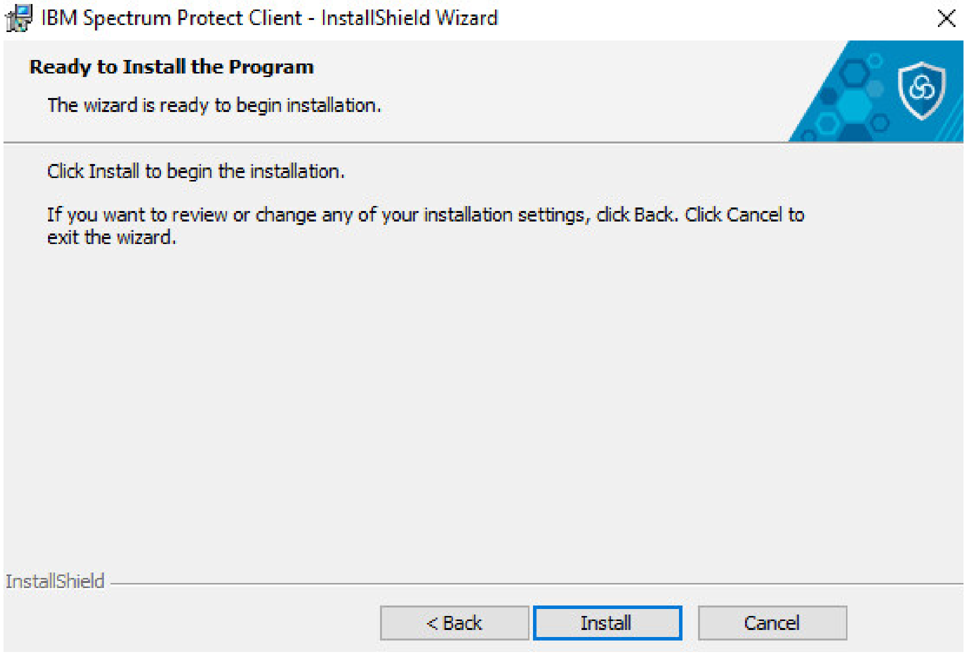
Administrative Client Command Line Files

This feature requires 11MB on your hard drive.

Install to:

C:\Program Files\Tivoli\TSM\

8. Click **Next**.



IBM Spectrum Protect Client - InstallShield Wizard

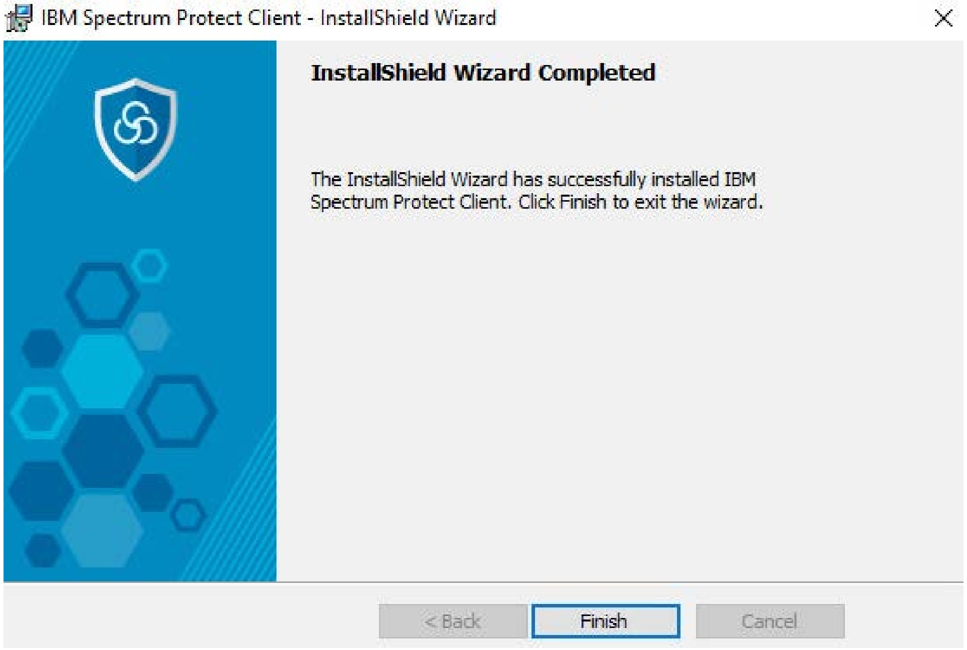
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

9. Click **Install**.



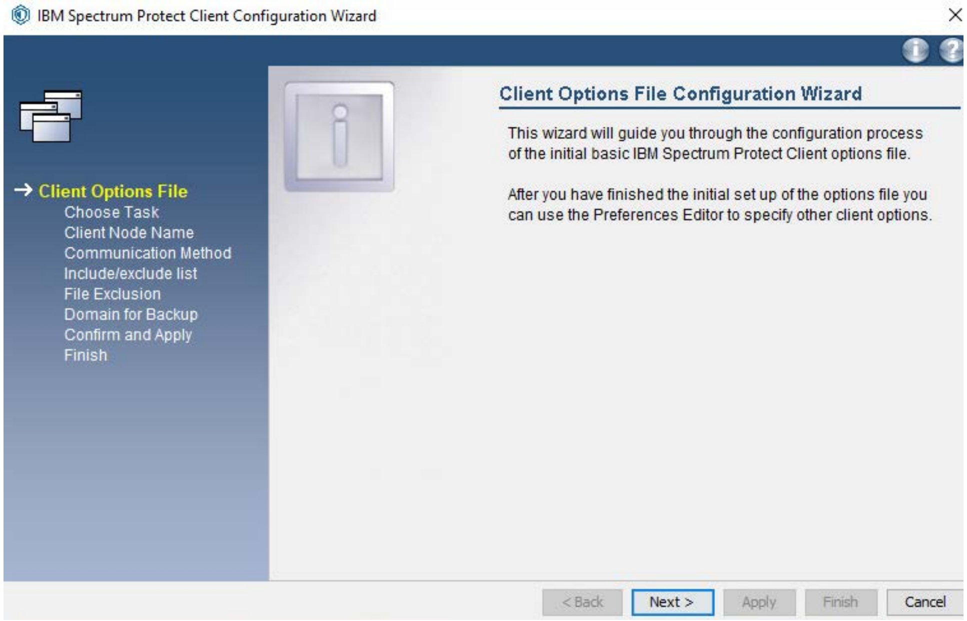
IBM Spectrum Protect Client - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed IBM Spectrum Protect Client. Click Finish to exit the wizard.

10. Click **Finish**.

11. Run **Backup-Archive GUI** from the **Start menu**. This should open the **IBM Spectrum Protect Client Configuration Wizard**.



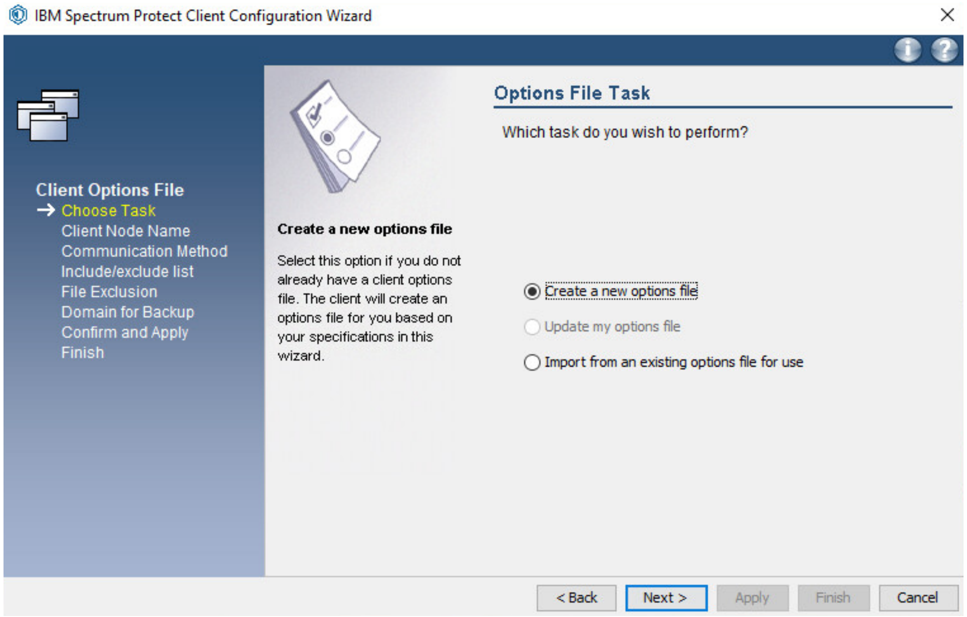
IBM Spectrum Protect Client Configuration Wizard

Client Options File Configuration Wizard

This wizard will guide you through the configuration process of the initial basic IBM Spectrum Protect Client options file.

After you have finished the initial set up of the options file you can use the Preferences Editor to specify other client options.

12. Click **Next**.
13. Select **Create a new options file**.



IBM Spectrum Protect Client Configuration Wizard

Options File Task

Which task do you wish to perform?

Create a new options file

Select this option if you do not already have a client options file. The client will create an options file for you based on your specifications in this wizard.

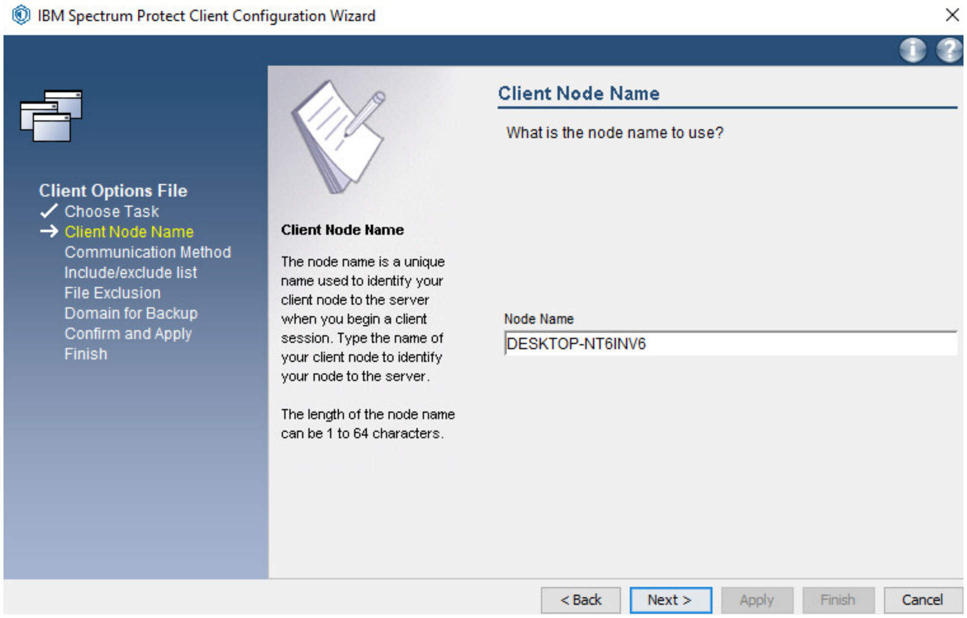
● Create a new options file

○ Update my options file

○ Import from an existing options file for use

14. Click **Next**.

15. Enter the **Node Name** that you created in the **Operations Center**.



Client Node Name

What is the node name to use?

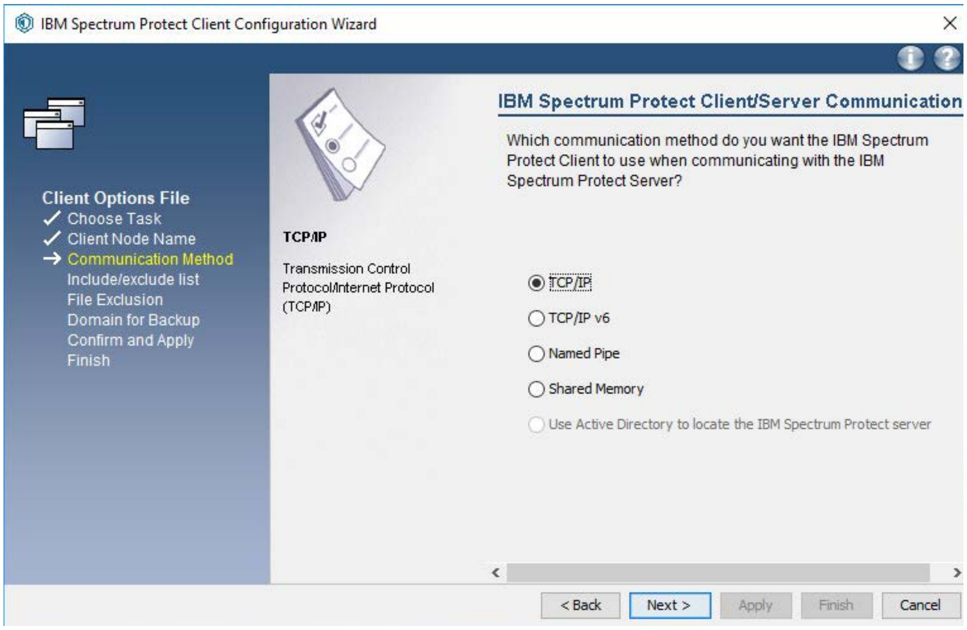
Client Node Name

The node name is a unique name used to identify your client node to the server when you begin a client session. Type the name of your client node to identify your node to the server.

The length of the node name can be 1 to 64 characters.

Node Name: DESKTOP-NT6INV6

16. Click **Next**.
17. If prompted, allow the program through the firewall.
18. Select **TCP/IP** for the communication method.



IBM Spectrum Protect Client/Server Communication

Which communication method do you want the IBM Spectrum Protect Client to use when communicating with the IBM Spectrum Protect Server?

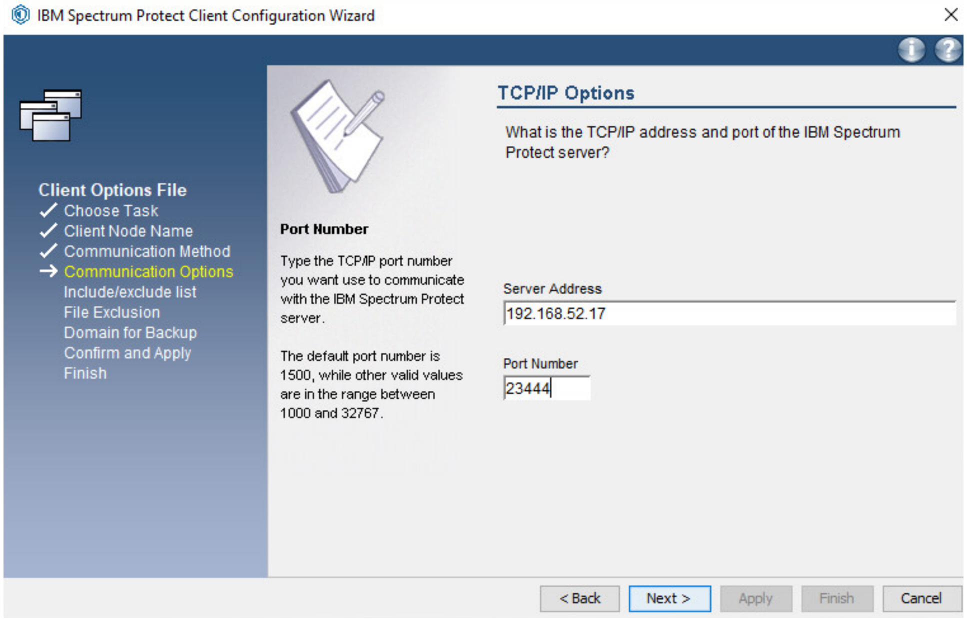
TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP)

● TCP/IP
○ TCP/IP v6
○ Named Pipe
○ Shared Memory
○ Use Active Directory to locate the IBM Spectrum Protect server

19. Click **Next**.
20. Specify the **IP address** of the server running the IBM backup server.

21. Specify the **port** that the server is accepting connections on (Example: 23444).



IBM Spectrum Protect Client Configuration Wizard

TCP/IP Options

What is the TCP/IP address and port of the IBM Spectrum Protect server?

Port Number

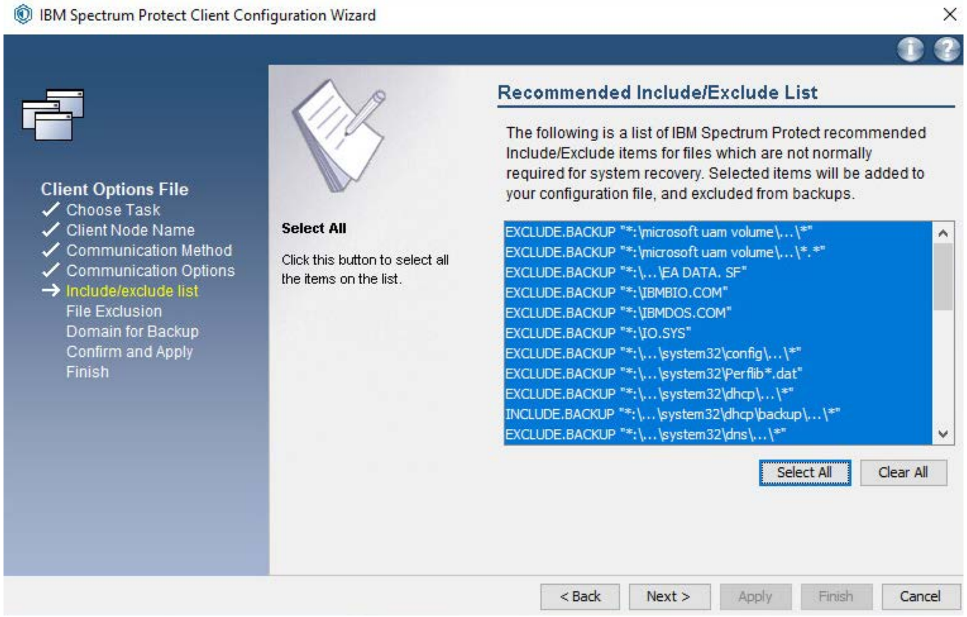
Type the TCP/IP port number you want use to communicate with the IBM Spectrum Protect server.

The default port number is 1500, while other valid values are in the range between 1000 and 32767.

Server Address: 192.168.52.17

Port Number: 23444

22. Click **Next**.
23. Click **Select All** or choose specific items from the recommended list of inclusions/exclusions.



IBM Spectrum Protect Client Configuration Wizard

Recommended Include/Exclude List

The following is a list of IBM Spectrum Protect recommended Include/Exclude items for files which are not normally required for system recovery. Selected items will be added to your configuration file, and excluded from backups.

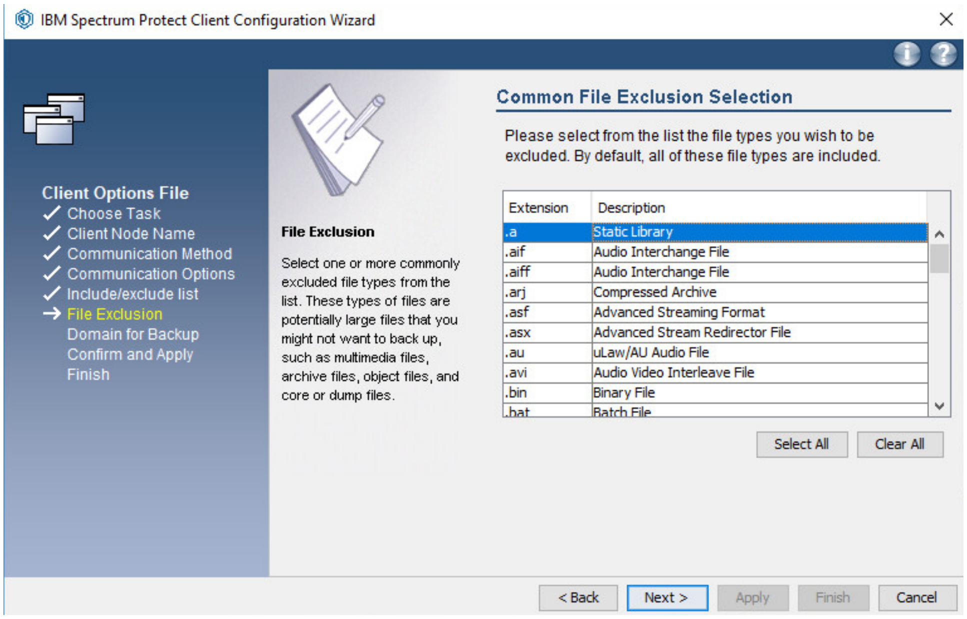
Select All

Click this button to select all the items on the list.

```
EXCLUDE.BACKUP "*:\microsoft uam volume\...\*"
EXCLUDE.BACKUP "*:\microsoft uam volume\...\*.*"
EXCLUDE.BACKUP "*:\...\EA DATA. SF"
EXCLUDE.BACKUP "*:\IBMBIO.COM"
EXCLUDE.BACKUP "*:\IBMDOS.COM"
EXCLUDE.BACKUP "*:\IO.SYS"
EXCLUDE.BACKUP "*:\...\system32\config\...\*"
EXCLUDE.BACKUP "*:\...\system32\Perflib*.dat"
EXCLUDE.BACKUP "*:\...\system32\dhcp\...\*"
INCLUDE.BACKUP "*:\...\system32\dhcp\backup\...\*"
EXCLUDE.BACKUP "*:\...\system32\dns\...\*"
```

24. Click **Next**.

25. Select certain file types to exclude from backup, if any.



IBM Spectrum Protect Client Configuration Wizard

Client Options File
✓ Choose Task
✓ Client Node Name
✓ Communication Method
✓ Communication Options
✓ Include/exclude list
→ File Exclusion
Domain for Backup
Confirm and Apply
Finish

File Exclusion

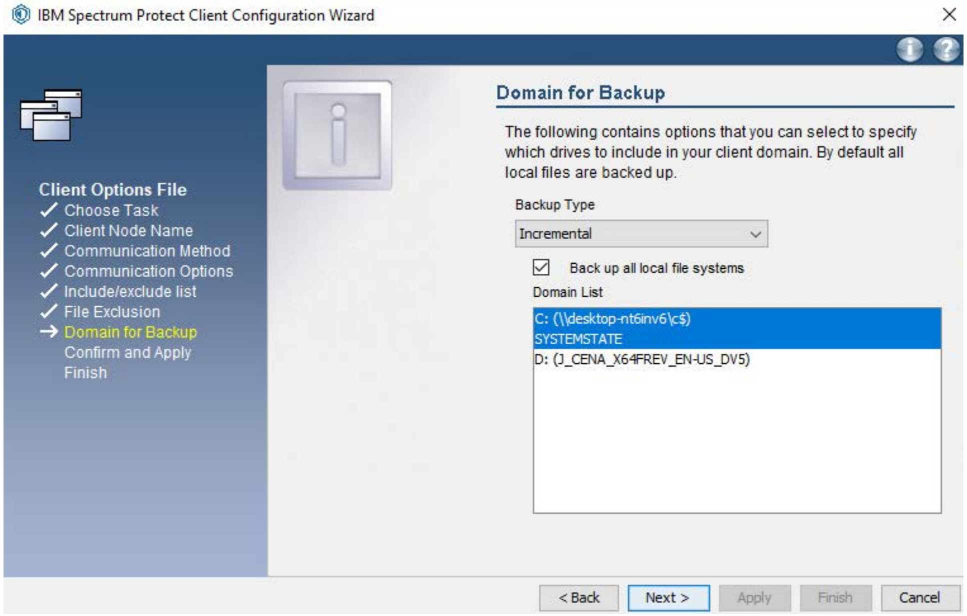
Select one or more commonly excluded file types from the list. These types of files are potentially large files that you might not want to back up, such as multimedia files, archive files, object files, and core or dump files.

Common File Exclusion Selection

Please select from the list the file types you wish to be excluded. By default, all of these file types are included.

Extension	Description
.a	Static Library
.aif	Audio Interchange File
.aiff	Audio Interchange File
.arj	Compressed Archive
.asf	Advanced Streaming Format
.asx	Advanced Stream Redirector File
.au	uLaw/AU Audio File
.avi	Audio Video Interleave File
.bin	Binary File
.bat	Batch File

26. Click **Next**.
27. Check the box next to **Backup all local file systems**.
28. Select **Incremental** for the **Backup Type**.



IBM Spectrum Protect Client Configuration Wizard

Client Options File
✓ Choose Task
✓ Client Node Name
✓ Communication Method
✓ Communication Options
✓ Include/exclude list
✓ File Exclusion
→ Domain for Backup
Confirm and Apply
Finish

Domain for Backup

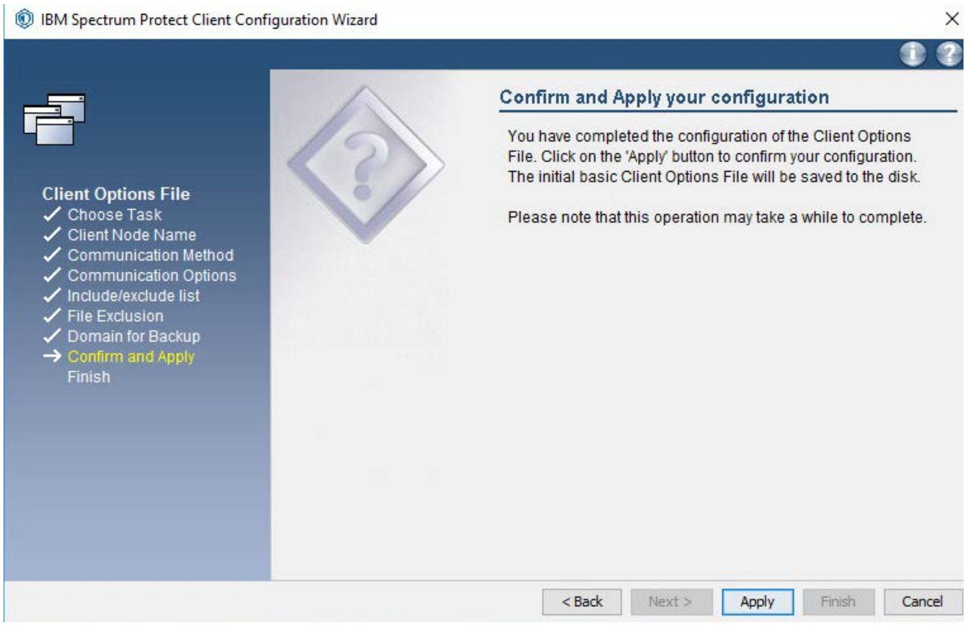
The following contains options that you can select to specify which drives to include in your client domain. By default all local files are backed up.

Backup Type: Incremental

☑ Back up all local file systems

Domain List
C: (\\desktop-nt6inv6\c$)
SYSTEMSTATE
D: (J_CENA_X64FREV_EN-US_DV5)

29. Click **Next**.

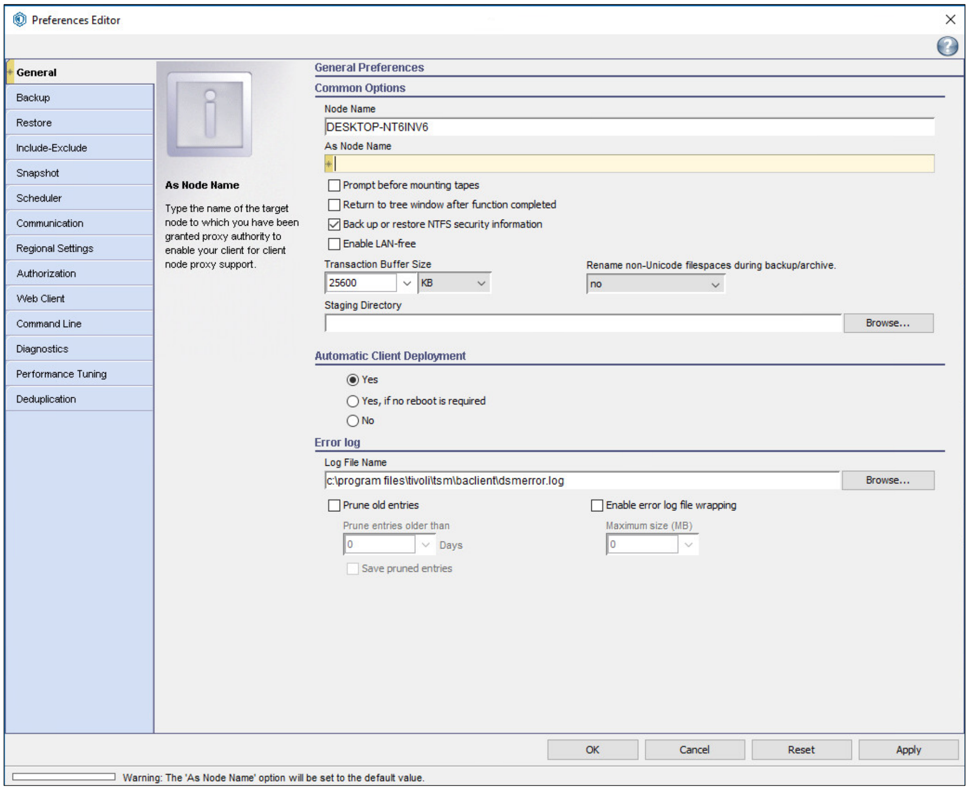


Confirm and Apply your configuration

You have completed the configuration of the Client Options File. Click on the 'Apply' button to confirm your configuration. The initial basic Client Options File will be saved to the disk.

Please note that this operation may take a while to complete.

30. Click **Apply**.
31. Click **Finish**.
32. In the **Backup-Archive GUI** (you may have to log in using the credentials specified on the server or you may have to choose to ignore a warning that you couldn't connect), go to **Edit > Client Preferences**.



As Node Name

Type the name of the target node to which you have been granted proxy authority to enable your client for client node proxy support.

General Preferences

Common Options

Node Name: DESKTOP-NT6INV6

As Node Name:

□ Prompt before mounting tapes

□ Return to tree window after function completed

☑ Back up or restore NTFS security information

□ Enable LAN-free

Transaction Buffer Size: 25600 KB

Rename non-Unicode filespaces during backup/archive.: no

Staging Directory:

Automatic Client Deployment

● Yes

○ Yes, if no reboot is required

○ No

Error log

Log File Name: c:\program files\tivoli\tsm\baclient\dsmerror.log

□ Prune old entries

Prune entries older than: 0 Days

□ Save pruned entries

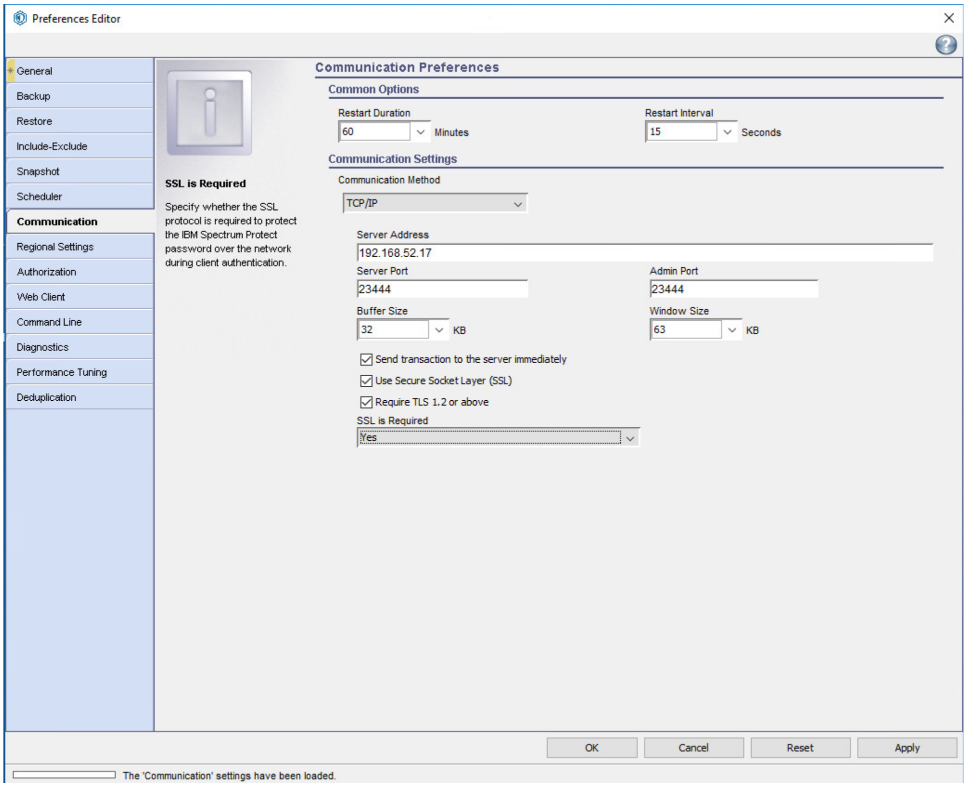
□ Enable error log file wrapping

Maximum size (MB): 0

Warning: The 'As Node Name' option will be set to the default value.

33. Click **Communication**.
34. Ensure that the **server address** is correct and that the **ports** point to your SSL port (23444).
35. Check the boxes next to **Send transaction to the server immediately**, **Use Secure Sockets Layer (SSL)**, and **Require TLS 1.2 or above**.

36. Select **Yes** for **SSL is Required**.



SSL is Required

Specify whether the SSL protocol is required to protect the IBM Spectrum Protect password over the network during client authentication.

Communication Preferences

Common Options

Restart Duration: 60 Minutes

Restart Interval: 15 Seconds

Communication Settings

Communication Method: TCP/IP

Server Address: 192.168.52.17

Server Port: 23444

Admin Port: 23444

Buffer Size: 32 KB

Window Size: 63 KB

☑ Send transaction to the server immediately

☑ Use Secure Socket Layer (SSL)

☑ Require TLS 1.2 or above

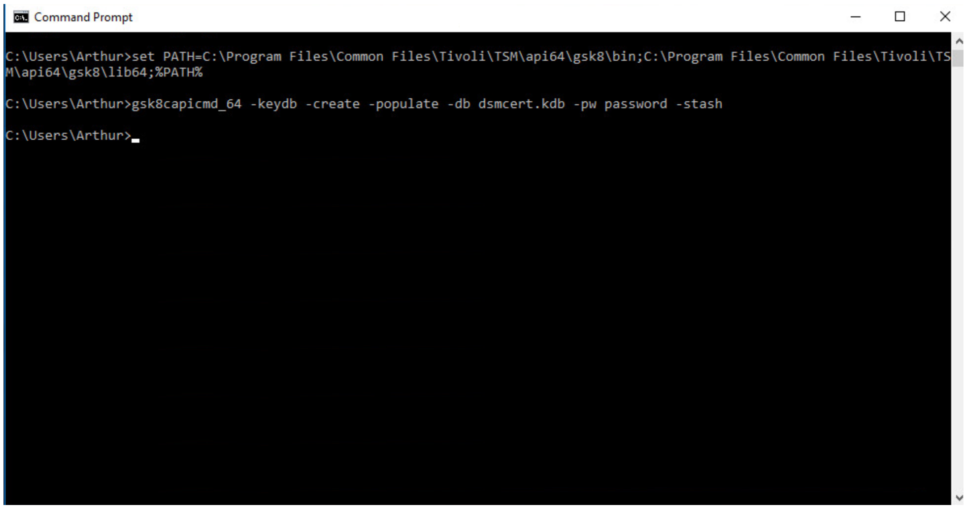
SSL is Required: Yes

The 'Communication' settings have been loaded.

37. Click **OK.**
38. Retrieve **cert256.arm** from the server.
39. On the client machine, create a new key database by running the following commands:

```
> set PATH=C:\Program Files\Common
Files\Tivoli\TSM\api64\gsk8\bin\;C:\Program Files\Common
Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```

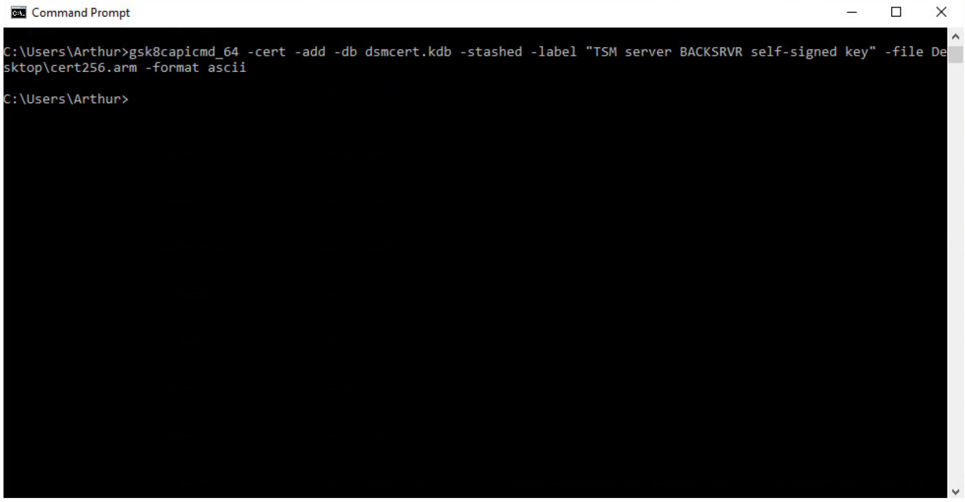
```
> gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -
stash
```



```
C:\Users\Arthur>set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin;C:\Program Files\Common Files\Tivoli\TS
M\api64\gsk8\lib64;%PATH%

C:\Users\Arthur>gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash

C:\Users\Arthur>
```

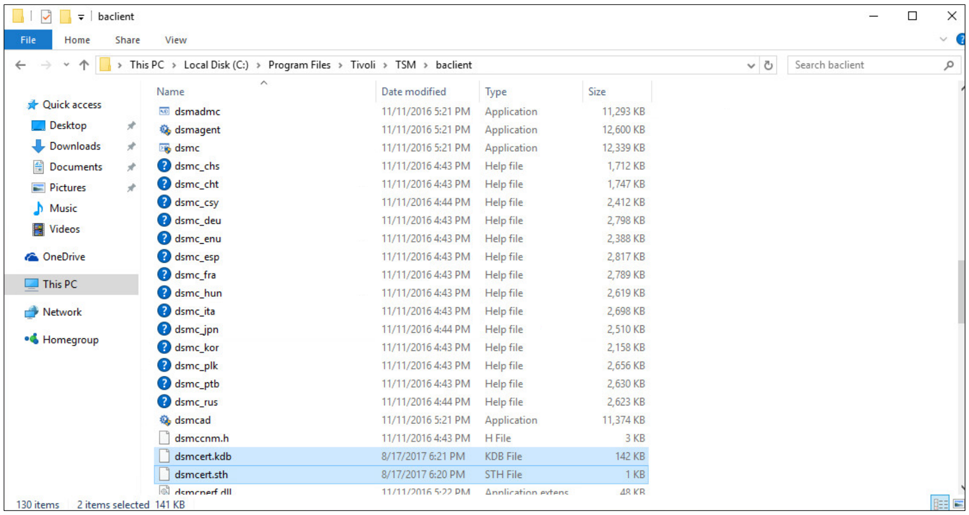
40. Import **cert256.arm** by running the command:

```
> gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "TSM server
BACKSRVR self-signed key" -file <path-to-cert256.arm> -format asci
```



```
C:\Users\Arthur>gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "TSM server BACKSRVR self-signed key" -file De
sktop\cert256.arm -format ascii

C:\Users\Arthur>
```

41. Copy the resulting *dsmcert.kdb* and *dsmcert.sth* to *C:\Program Files\Tivoli\TSM\baclient*.

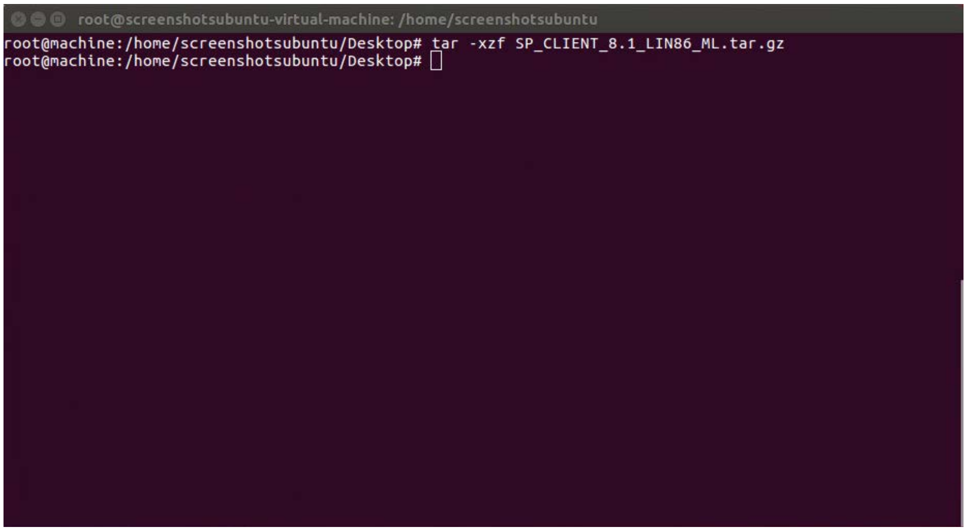


Name	Date modified	Type	Size
dsmadmc	11/11/2016 5:21 PM	Application	11,293 KB
dsmagent	11/11/2016 5:21 PM	Application	12,600 KB
dsmc	11/11/2016 5:21 PM	Application	12,339 KB
dsmc_chs	11/11/2016 4:43 PM	Help file	1,712 KB
dsmc_cht	11/11/2016 4:43 PM	Help file	1,747 KB
dsmc_csy	11/11/2016 4:44 PM	Help file	2,412 KB
dsmc_deu	11/11/2016 4:43 PM	Help file	2,798 KB
dsmc_enu	11/11/2016 4:43 PM	Help file	2,388 KB
dsmc_esp	11/11/2016 4:43 PM	Help file	2,817 KB
dsmc_fra	11/11/2016 4:43 PM	Help file	2,789 KB
dsmc_hun	11/11/2016 4:43 PM	Help file	2,619 KB
dsmc_ita	11/11/2016 4:43 PM	Help file	2,698 KB
dsmc_jpn	11/11/2016 4:44 PM	Help file	2,510 KB
dsmc_kor	11/11/2016 4:43 PM	Help file	2,158 KB
dsmc_plk	11/11/2016 4:43 PM	Help file	2,656 KB
dsmc_ptb	11/11/2016 4:43 PM	Help file	2,630 KB
dsmc_rus	11/11/2016 4:44 PM	Help file	2,623 KB
dsmcad	11/11/2016 5:21 PM	Application	11,374 KB
dsmccnm.h	11/11/2016 4:43 PM	H File	3 KB
dsmcert.kdb	8/17/2017 6:21 PM	KDB File	142 KB
dsmcert.sth	8/17/2017 6:20 PM	STH File	1 KB
dsmcperf.dll	11/11/2016 5:22 PM	Application extens	48 KB

130 items 2 items selected 141 KB

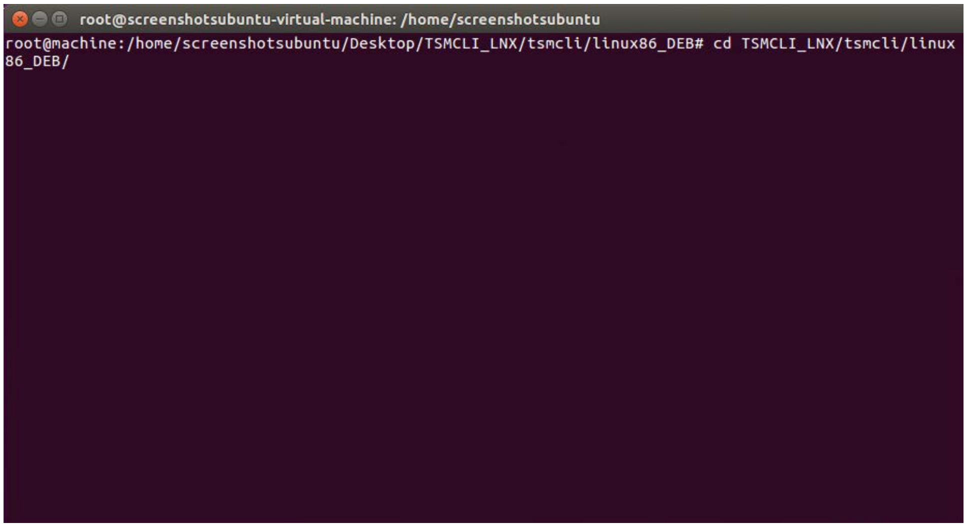
2.7.6 Install the Spectrum Protect Client on Ubuntu

1. Extract **SP_CLIENT_8.1_LIN86_ML.tar.gz**.


root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

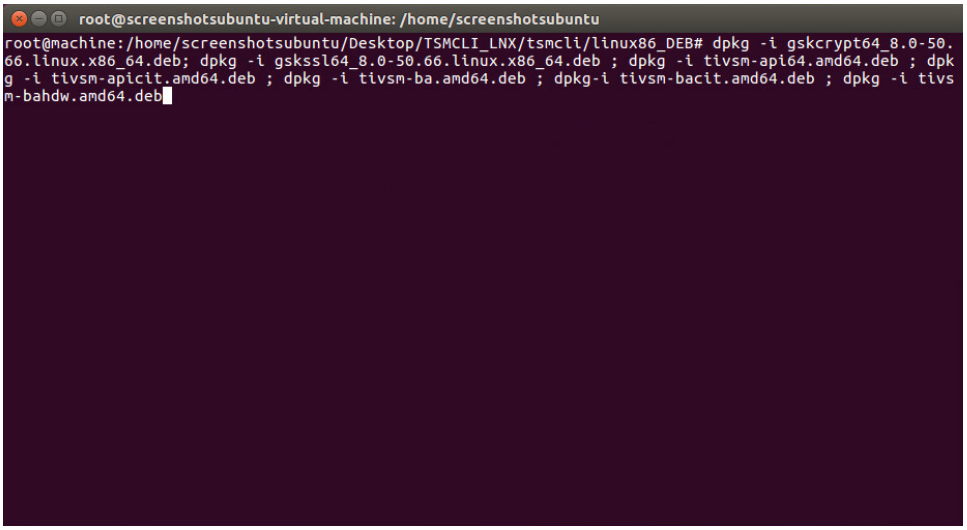
```
root@machine:/home/screenshotsubuntu/Desktop# tar -xzf SP_CLIENT_8.1_LIN86_ML.tar.gz
root@machine:/home/screenshotsubuntu/Desktop# 
```

2. Navigate to **TSMCLI_LNX/tsmcli/linux86_DEB**.


root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

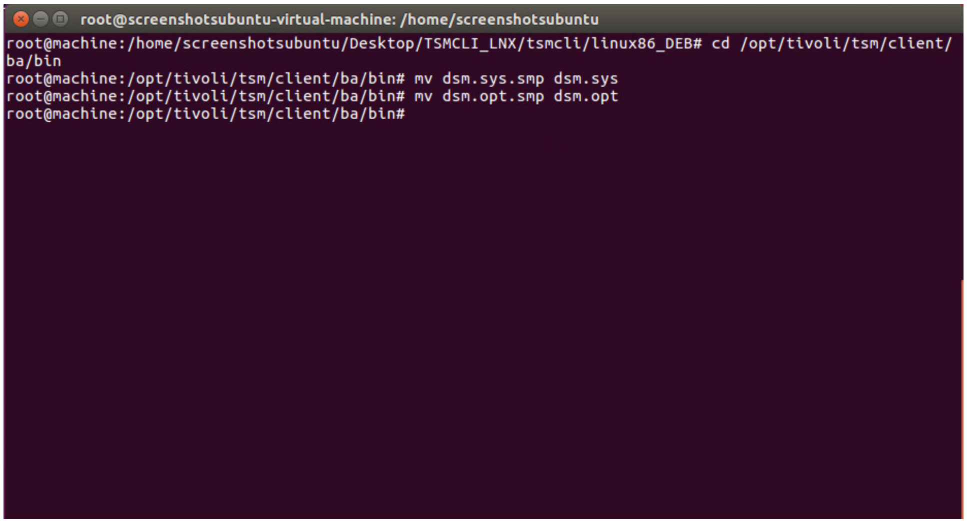
```
root@machine:/home/screenshotsubuntu/Desktop/TSMCLI_LNX/tsmcli/linux86_DEB# cd TSMCLI_LNX/tsmcli/linux
86_DEB/
```

3. Install all the **.deb** files in this directory, except tivsm-jbb.amd64.deb, by running the following command (they must be dpkg'd individually since they have interdependencies):
    a. `dpkg -i [name of package].deb`


root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:/home/screenshotsubuntu/Desktop/TSMCLI_LNX/tsmcli/linux86_DEB# dpkg -i gskcrypt64_8.0-50.
66.linux.x86_64.deb; dpkg -i gskssl64_8.0-50.66.linux.x86_64.deb ; dpkg -i tivsm-api64.amd64.deb ; dpk
g -i tivsm-apicit.amd64.deb ; dpkg -i tivsm-ba.amd64.deb ; dpkg-i tivsm-bacit.amd64.deb ; dpkg -i tivs
m-bahdw.amd64.deb
```

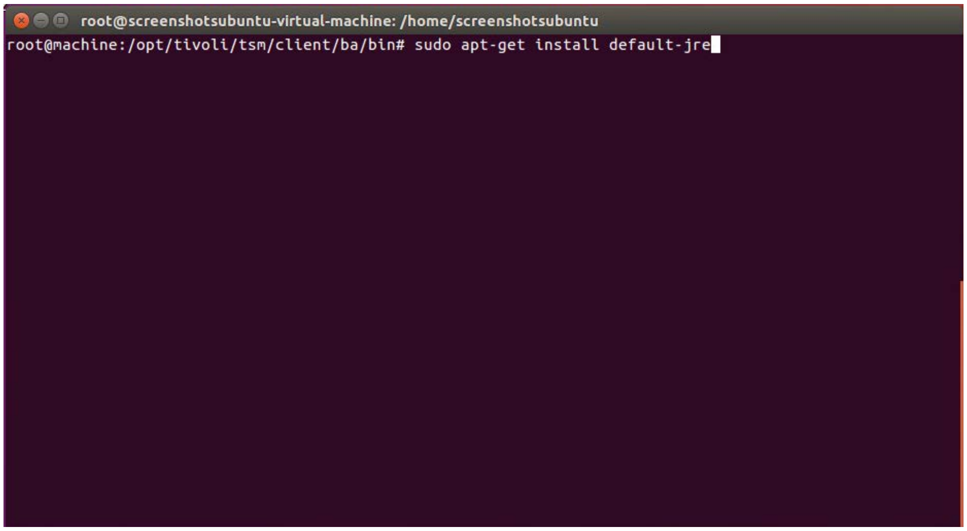
4. Issue the following commands to setup the options files:
    a. `cd /opt/tivoli/tsm/client/ba/bin`
    b. `mv dsm.sys.smp dsm.sys`
    c. `mv dsm.opt.smp dsm.opt`



```
root@machine:/home/screenshotsubuntu/Desktop/TSMCLI_LNX/tsmcli/linux86_DEB# cd /opt/tivoli/tsm/client/
ba/bin
root@machine:/opt/tivoli/tsm/client/ba/bin# mv dsm.sys.smp dsm.sys
root@machine:/opt/tivoli/tsm/client/ba/bin# mv dsm.opt.smp dsm.opt
root@machine:/opt/tivoli/tsm/client/ba/bin#
```

root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

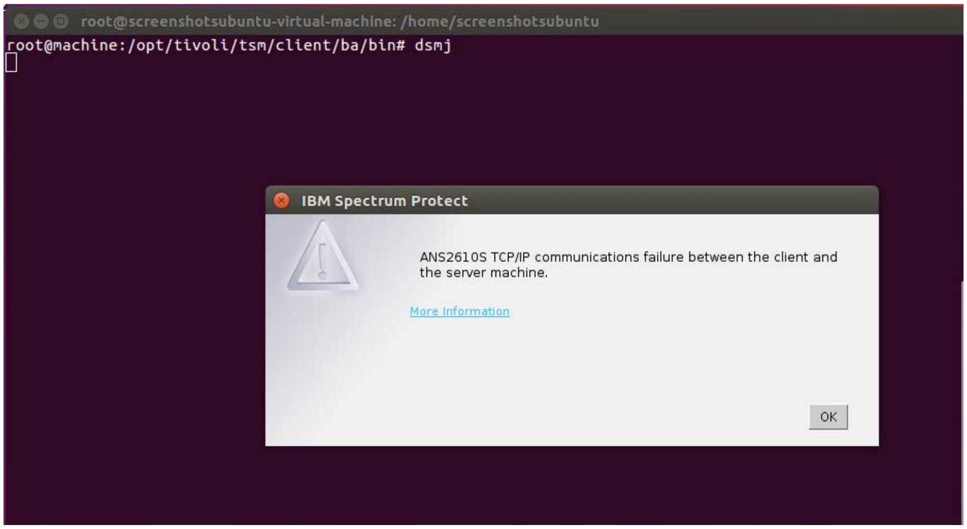
5. Install Java with:
    a. `sudo apt-get install default-jre`



```
root@machine:/opt/tivoli/tsm/client/ba/bin# sudo apt-get install default-jre
```

root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

6. Run **dsmj** to start the Java **BAClient**.



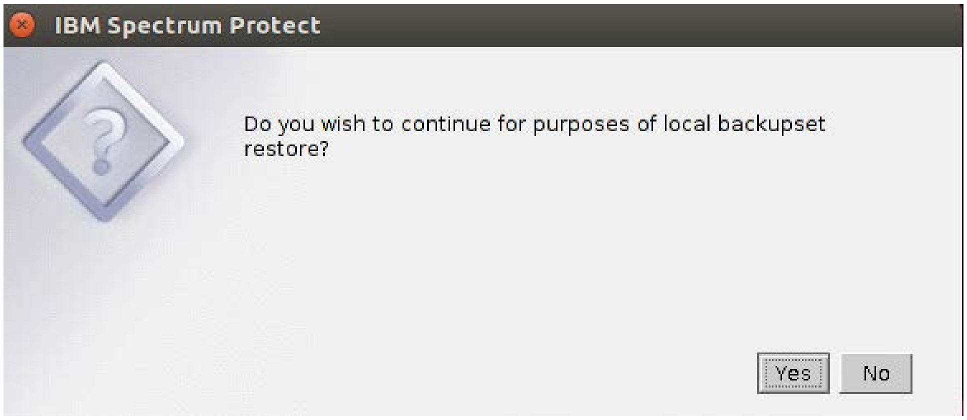
root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:/opt/tivoli/tsm/client/ba/bin# dsmj
```

IBM Spectrum Protect

ANS2610S TCP/IP communications failure between the client and the server machine.

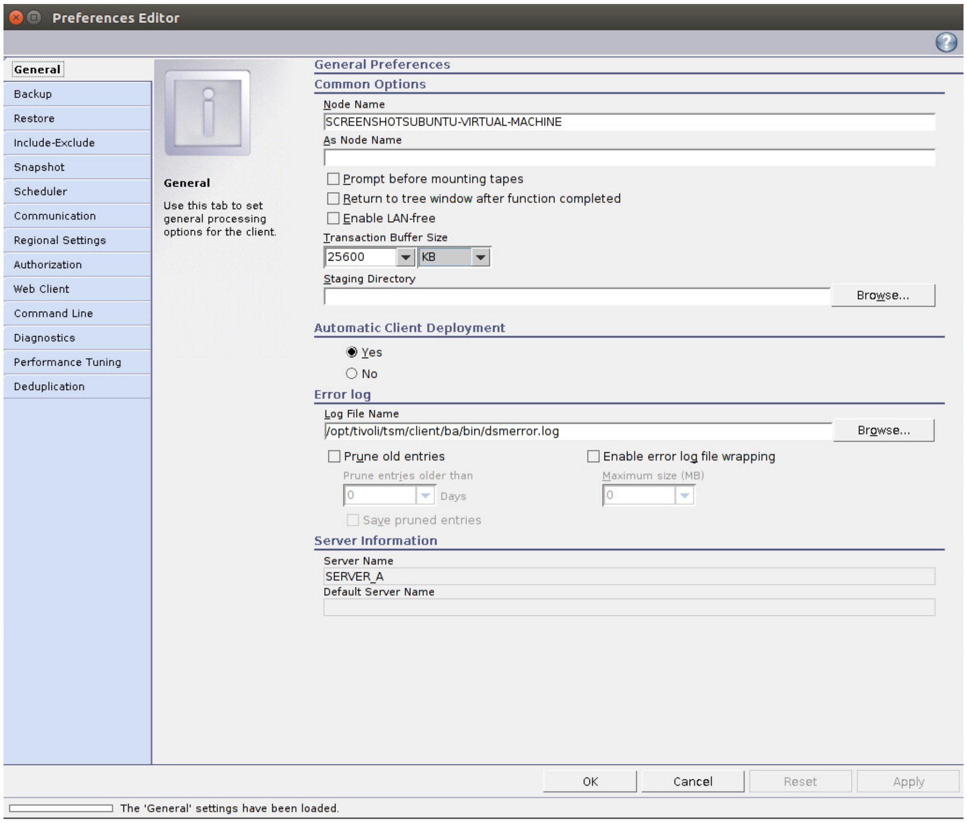
7. After about 5 minutes, it will be unable to connect and will ask if you wish to start the client anyway. Click **Yes**.



IBM Spectrum Protect

Do you wish to continue for purposes of local backupset restore?

8. Open **Edit > Client Preferences**. Enter the node name as the name of the client you added to the Spectrum Protect server.



General

Use this tab to set general processing options for the client.

General Preferences

Common Options

Node Name: SCREENSHOTSUBUNTU-VIRTUAL-MACHINE

As Node Name:

□ Prompt before mounting tapes

□ Return to tree window after function completed

□ Enable LAN-free

Transaction Buffer Size: 25600 KB

Staging Directory:

Automatic Client Deployment

● Yes

○ No

Error log

Log File Name: /opt/tivoli/tsm/client/ba/bin/dsmerror.log

□ Prune old entries

Prune entries older than: 0 Days

□ Save pruned entries

□ Enable error log file wrapping

Maximum size (MB): 0

Server Information

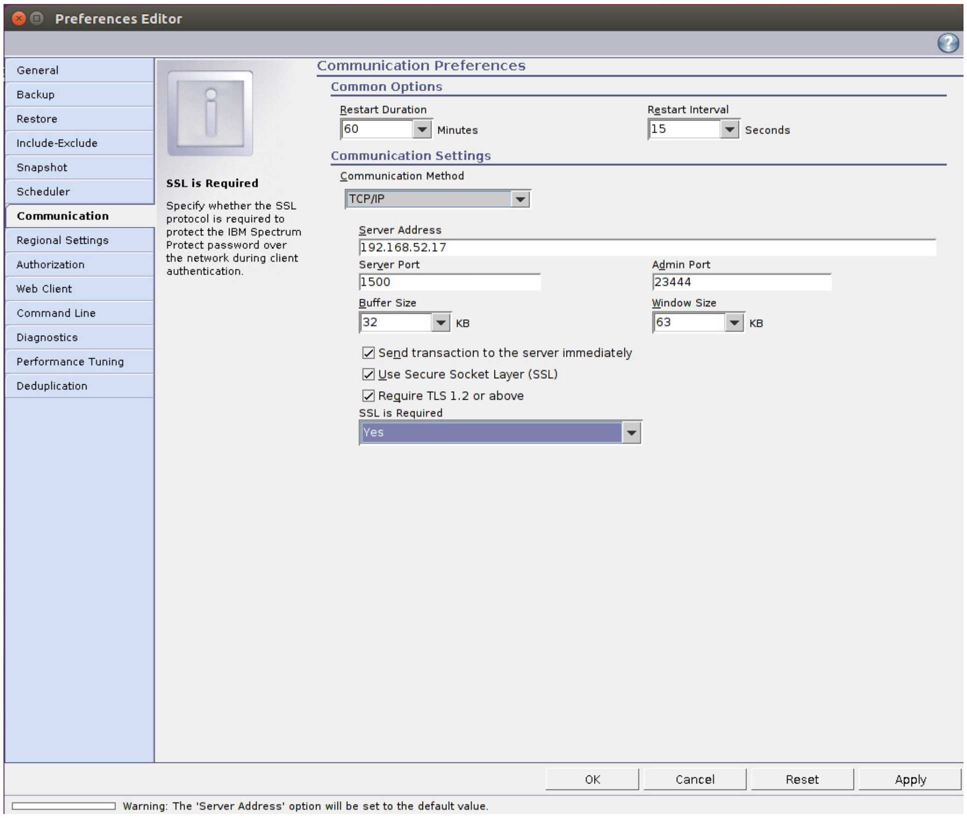
Server Name: SERVER_A

Default Server Name:

The 'General' settings have been loaded.

9. Click the **Communication** tab.
10. Enter the **IP Address** for the server.
11. Enter the **Server port** and **Admin port** (23444).
12. Check the boxes next to **Send transaction to the server immediately**, **Use Secure Sockets Layer (SSL)**, and **Require TLS 1.2 or above.**

13. Select **Yes** for **SSL is Required**.



SSL is Required

Specify whether the SSL protocol is required to protect the IBM Spectrum Protect password over the network during client authentication.

Communication Preferences

Common Options

Restart Duration: 60 Minutes

Restart Interval: 15 Seconds

Communication Settings

Communication Method: TCP/IP

Server Address: 192.168.52.17

Server Port: 1500

Admin Port: 23444

Buffer Size: 32 KB

Window Size: 63 KB

☑ Send transaction to the server immediately

☑ Use Secure Socket Layer (SSL)

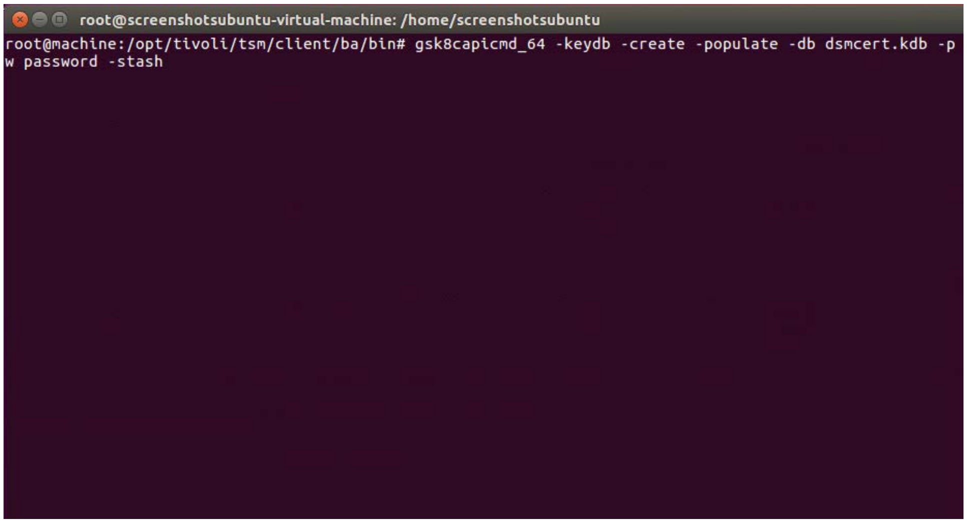
☑ Require TLS 1.2 or above

SSL is Required: Yes

Warning: The 'Server Address' option will be set to the default value.

14. Click **OK**.
15. Retrieve **cert256.arm** from the server.
16. On the client machine create a new key database by running the following commands:

```
> gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -
stash
```

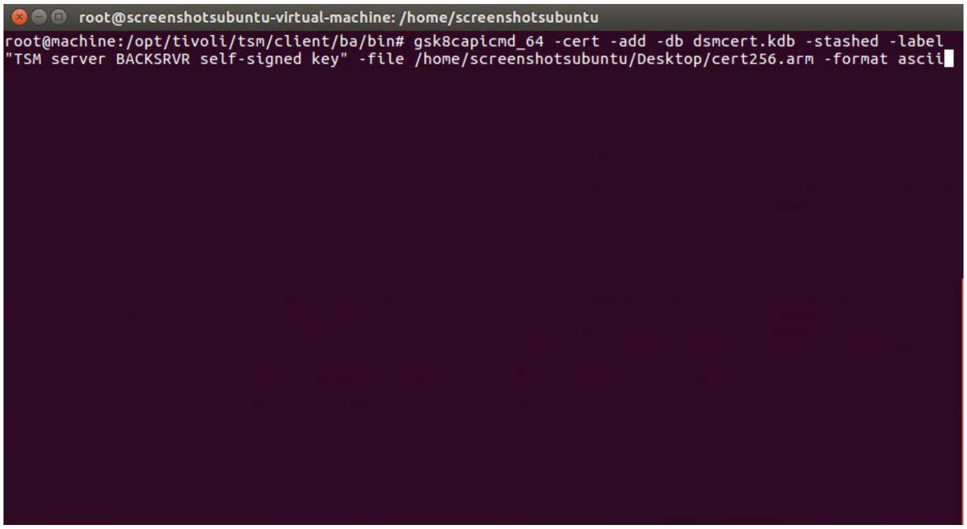


root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:/opt/tivoli/tsm/client/ba/bin# gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -p
w password -stash
```

17. Import **cert256.arm** by running the command:

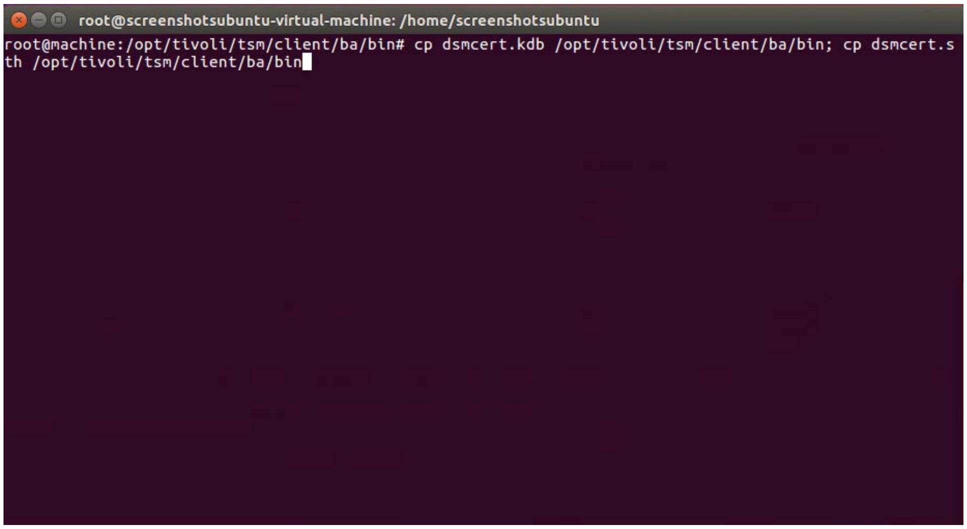
```
> gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "TSM server
BACKSRVR self-signed key" -file <path-to-cert256.arm> -format asci
```



root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:/opt/tivoli/tsm/client/ba/bin# gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label
"TSM server BACKSRVR self-signed key" -file /home/screenshotsubuntu/Desktop/cert256.arm -format ascii
```

18. Copy the resulting "dsmcert.kdb" and "dsmcert.sth" to */opt/tivoli/tsm/client/ba/bin*.

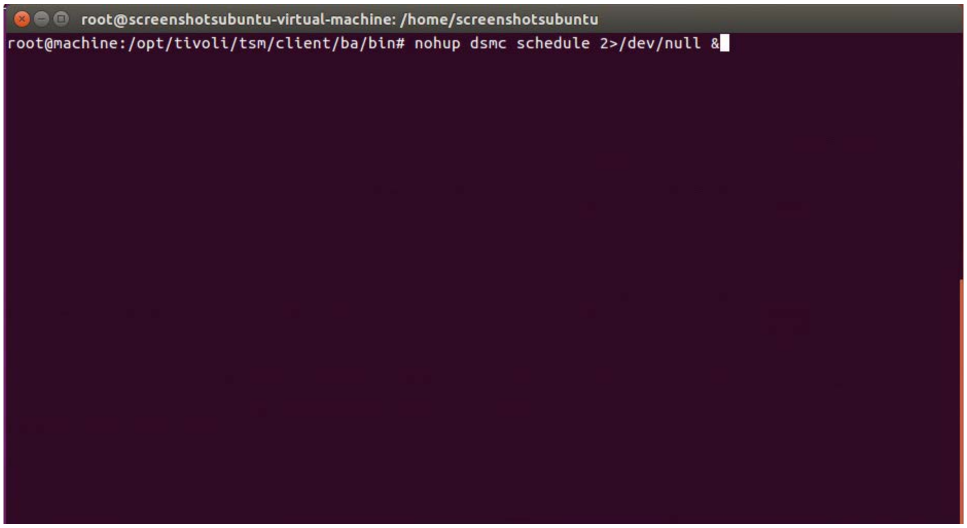


root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:/opt/tivoli/tsm/client/ba/bin# cp dsmcert.kdb /opt/tivoli/tsm/client/ba/bin; cp dsmcert.s
th /opt/tivoli/tsm/client/ba/bin
```

19. You may be asked to reconfigure the **dsm.opt** file when setting up the scheduler but the options should be filled out already.
20. To start the scheduler as a background process, run the following command:

```
> nohup dsmc schedule 2>/dev/null &
```



root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:/opt/tivoli/tsm/client/ba/bin# nohup dsmc schedule 2>/dev/null &
```

21. You can add this command to the startup programs in Ubuntu to make it start automatically.

2.8 GreenTec WORMdisks

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

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

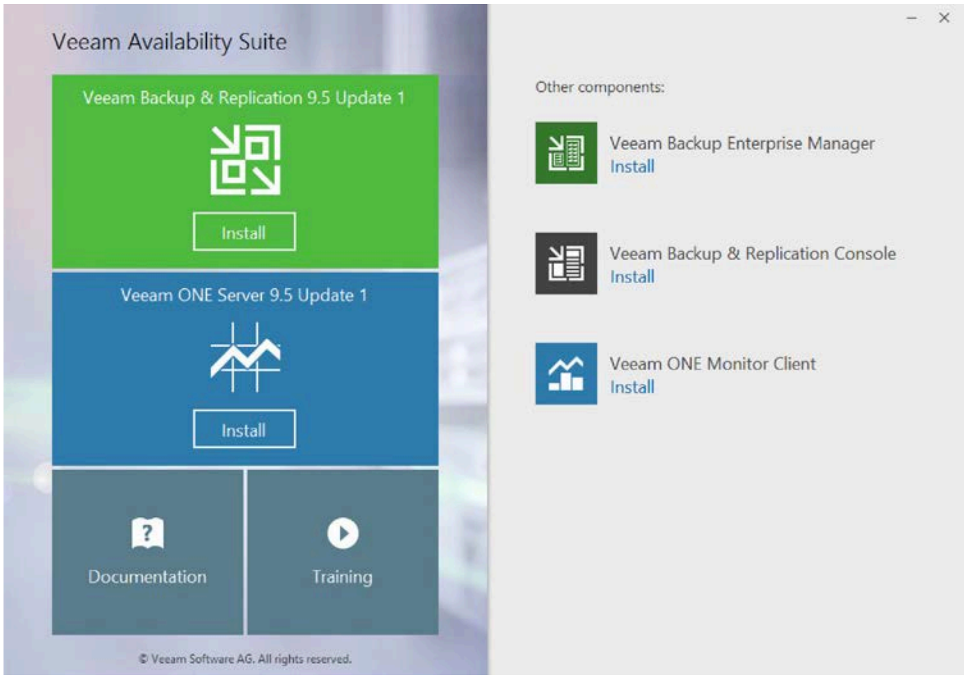
The *GT_WinStatus User Guide* provides instructions for locking and temporarily locking disk sectors. In this practice guide, we will not include instructions on when or how to lock GreenTec disks. However, in some cases, we will provide instructions detailing how to save data to these disks and leave locking them to the implementing parties.

2.9 Veeam Backup & Replication

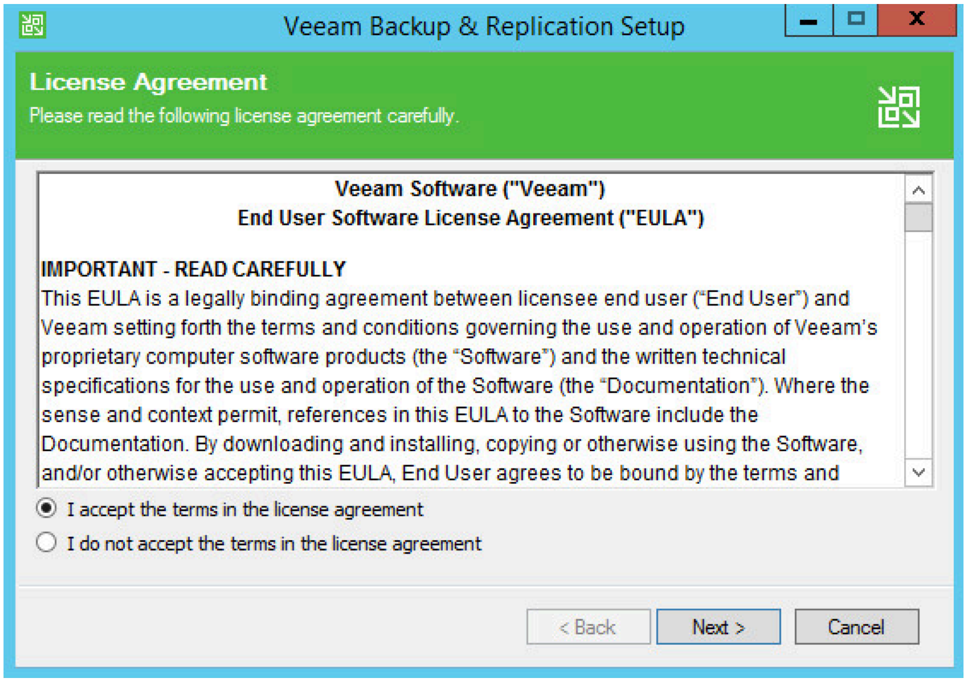
Veeam's Backup & Replication tool provides backup and restore capabilities. In the data integrity solution, Veeam is used to back up and restore virtual machines residing within Windows Server Hyper-V. In this section is the installation and configuration process for Veeam Backup & Replication on a Windows Server 2012 R2 machine. Additional installation and configuration instructions can be found at https://helpcenter.veeam.com/docs/backup/hyperv/install_vbr.html?ver=95.

2.9.1 Production Installation

1. Start the **Veeam Setup Wizard** and click to begin the installation process for **Veeam Backup & Replication** with the appropriate version number.


Veeam Availability Suite
Veeam Backup & Replication 9.5 Update 1
Install
Veeam ONE Server 9.5 Update 1
Install
Documentation
Training
© Veeam Software AG. All rights reserved.
Other components:
Veeam Backup Enterprise Manager
Install
Veeam Backup & Replication Console
Install
Veeam ONE Monitor Client
Install

2. Read and **accept** the license agreement.

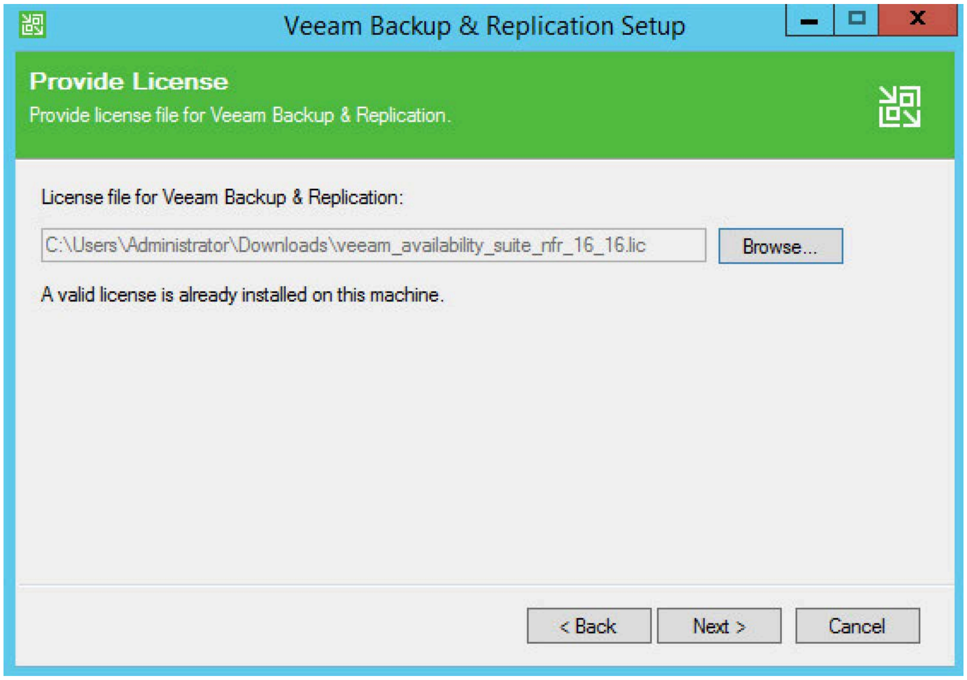

Veeam Backup & Replication Setup
License Agreement
Please read the following license agreement carefully.
< Back
Next >
Cancel

Veeam Software ("Veeam")
End User Software License Agreement ("EULA")

IMPORTANT - READ CAREFULLY
This EULA is a legally binding agreement between licensee end user ("End User") and Veeam setting forth the terms and conditions governing the use and operation of Veeam's proprietary computer software products (the "Software") and the written technical specifications for the use and operation of the Software (the "Documentation"). Where the sense and context permit, references in this EULA to the Software include the Documentation. By downloading and installing, copying or otherwise using the Software, and/or otherwise accepting this EULA, End User agrees to be bound by the terms and

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

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


Veeam Backup & Replication Setup

Provide License

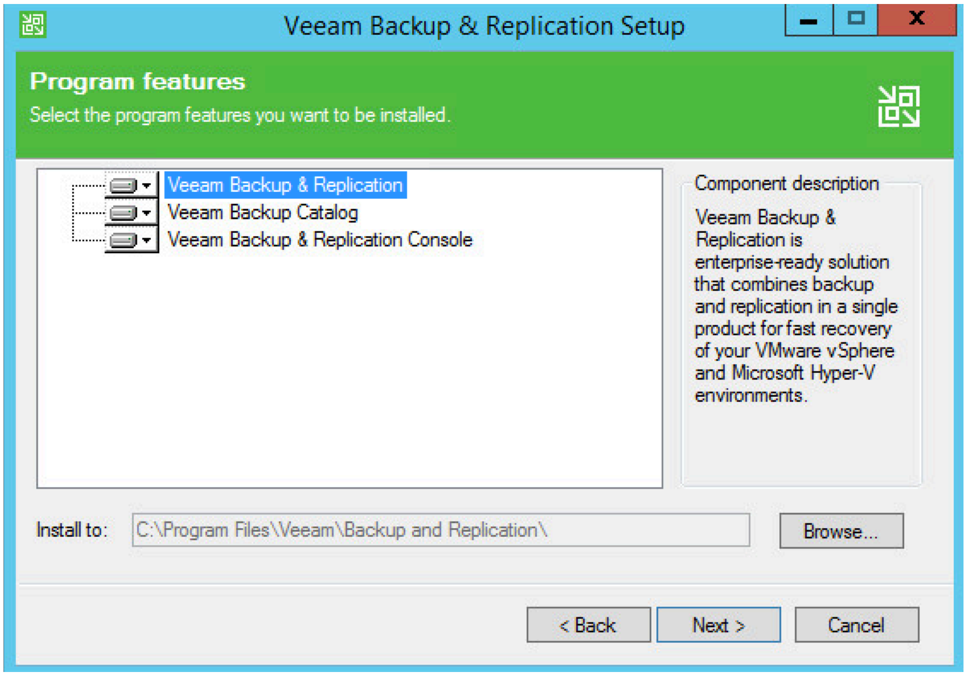
Provide license file for Veeam Backup & Replication.

License file for Veeam Backup & Replication:

C:\Users\Administrator\Downloads\veeam_availability_suite_nfr_16_16.lic

A valid license is already installed on this machine.

5. Click **Next**.
6. Select installation components required by your organization.


Veeam Backup & Replication Setup

Program features

Select the program features you want to be installed.

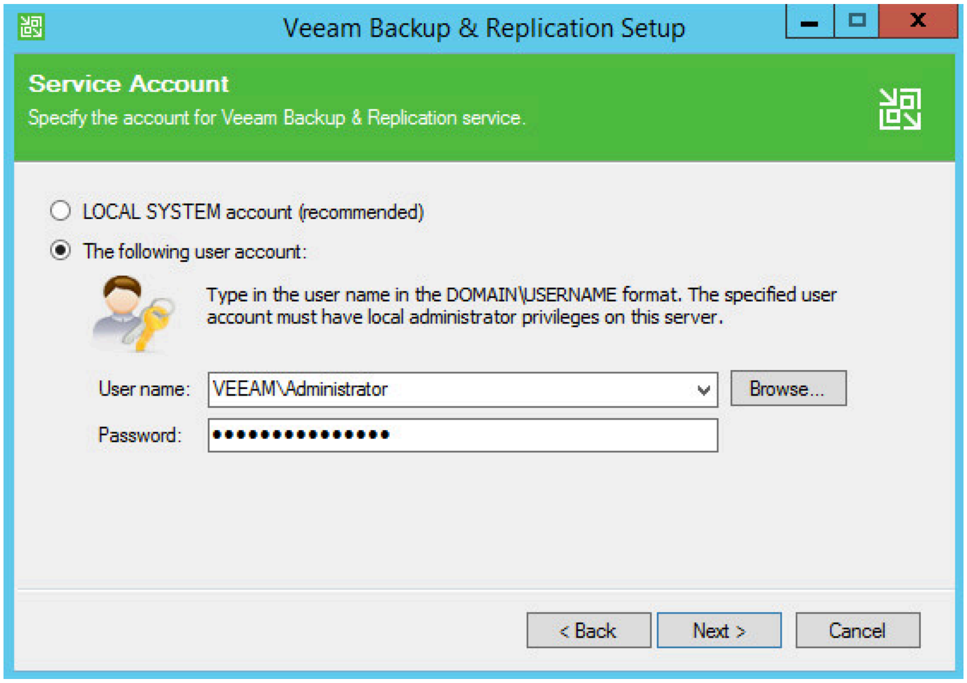
- Veeam Backup & Replication
- Veeam Backup Catalog
- Veeam Backup & Replication Console

Component description

Veeam Backup & Replication is enterprise-ready solution that combines backup and replication in a single product for fast recovery of your VMware vSphere and Microsoft Hyper-V environments.

Install to: C:\Program Files\Veeam\Backup and Replication\

7. Click **Next**.
8. Specify account credentials for **Service** account.


Veeam Backup & Replication Setup

Service Account

Specify the account for Veeam Backup & Replication service.

○ LOCAL SYSTEM account (recommended)

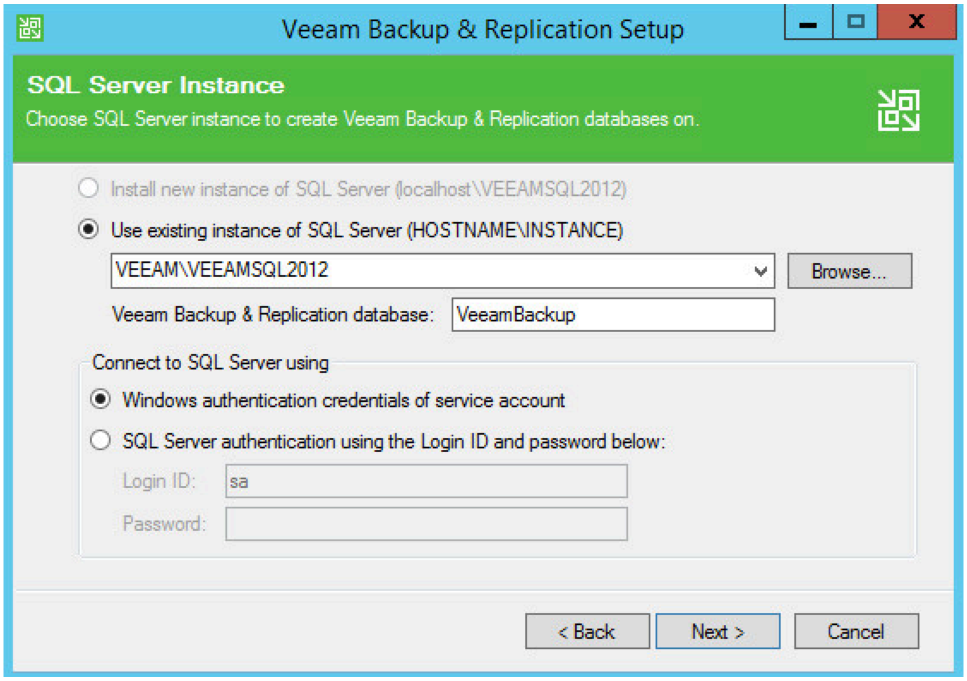
● The following user account:

Type in the user name in the DOMAIN\USERNAME format. The specified user account must have local administrator privileges on this server.

User name: VEEAM\Administrator

Password: •••••••••••••••

9. Click **Next**.
10. Specify details of the **SQL Server Instance**.


Veeam Backup & Replication Setup

SQL Server Instance

Choose SQL Server instance to create Veeam Backup & Replication databases on.

○ Install new instance of SQL Server (localhost\VEEAMSQL2012)

● Use existing instance of SQL Server (HOSTNAME\INSTANCE)

VEEAM\VEEAMSQL2012

Veeam Backup & Replication database: VeeamBackup

Connect to SQL Server using

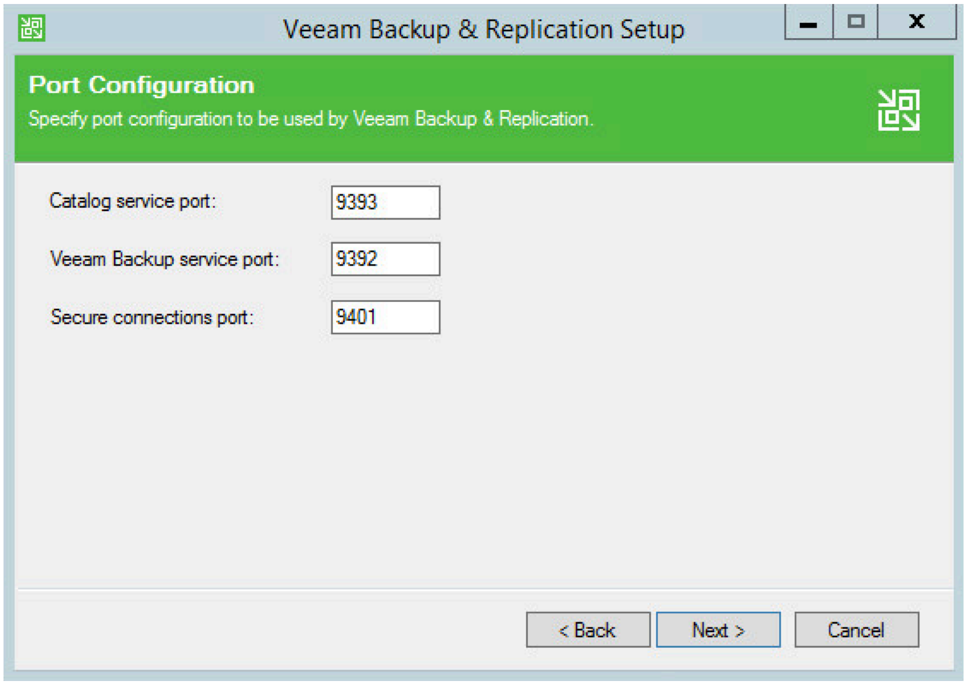
● Windows authentication credentials of service account

○ SQL Server authentication using the Login ID and password below:

Login ID: sa

Password:

11. Click **Next**.
12. Specify **port numbers** for **Veaam Backup & Replication** services.



Veeam Backup & Replication Setup

Port Configuration

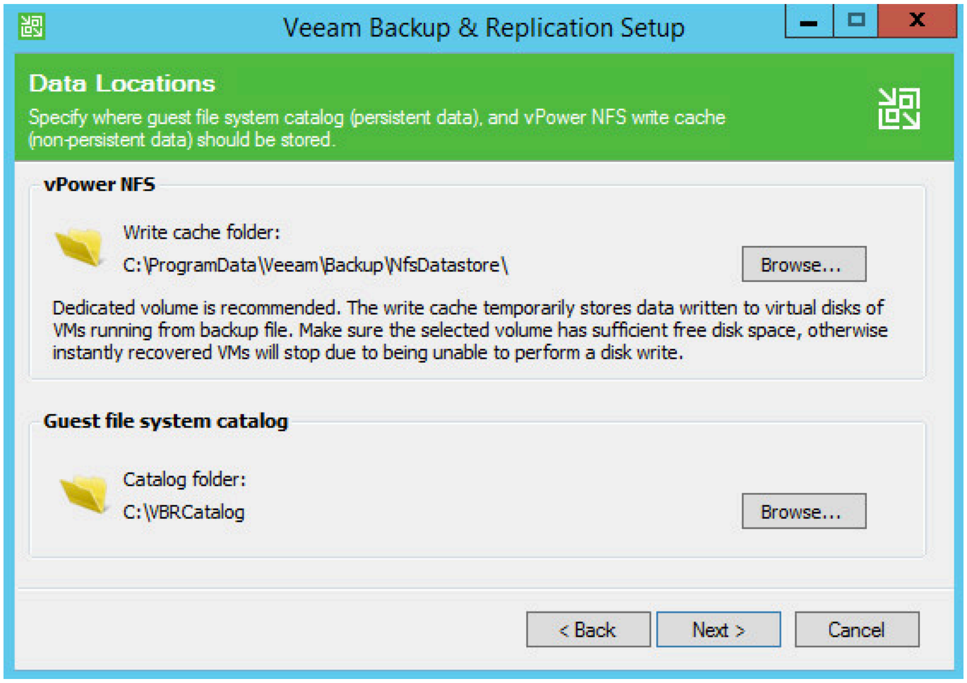
Specify port configuration to be used by Veeam Backup & Replication.

Catalog service port: 9393

Veeam Backup service port: 9392

Secure connections port: 9401

13. Click Next.
14. Specify **data storage locations.**



Veeam Backup & Replication Setup

Data Locations

Specify where guest file system catalog (persistent data), and vPower NFS write cache (non-persistent data) should be stored.

vPower NFS

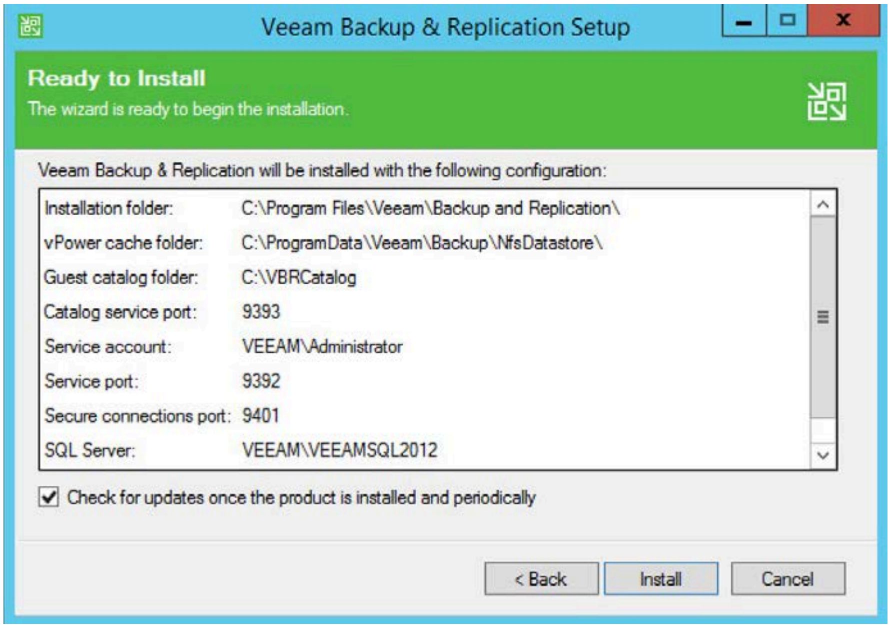
Write cache folder:
C:\ProgramData\Veeam\Backup\NfsDatastore\

Dedicated volume is recommended. The write cache temporarily stores data written to virtual disks of VMs running from backup file. Make sure the selected volume has sufficient free disk space, otherwise instantly recovered VMs will stop due to being unable to perform a disk write.

Guest file system catalog

Catalog folder:
C:\VBRCatalog

15. Click **Next**.
16. Review installation and configuration details and click **Install.**



Veeam Backup & Replication Setup

Ready to Install

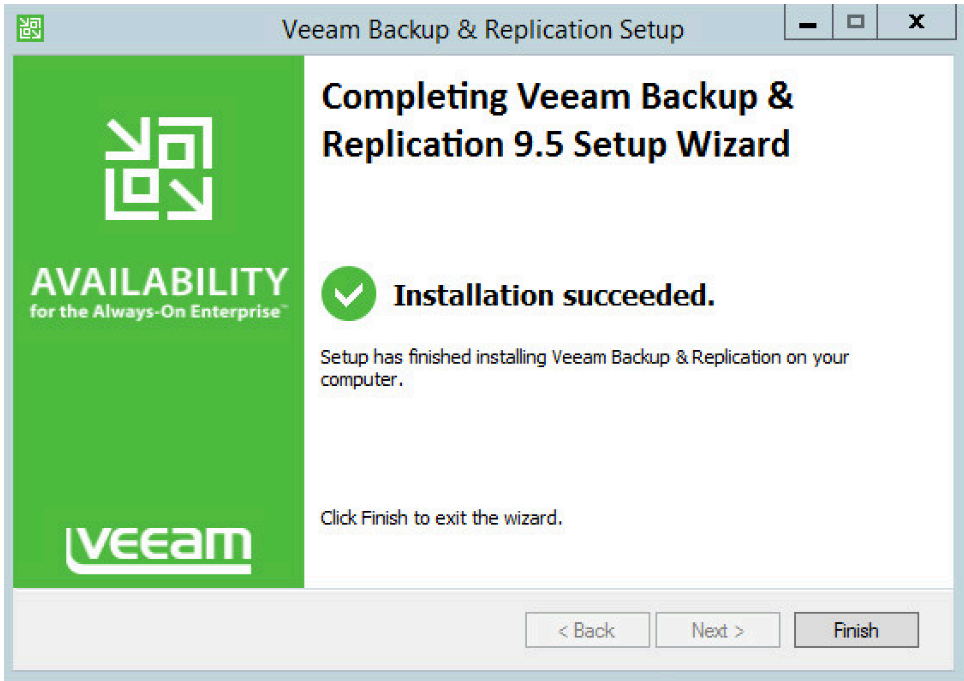
The wizard is ready to begin the installation.

Veeam Backup & Replication will be installed with the following configuration:

Installation folder:	C:\Program Files\Veeam\Backup and Replication\
vPower cache folder:	C:\ProgramData\Veeam\Backup\NfsDatastore\
Guest catalog folder:	C:\VBRCatalog
Catalog service port:	9393
Service account:	VEEAM\Administrator
Service port:	9392
Secure connections port:	9401
SQL Server:	VEEAM\VEEAMSQL2012

☑ Check for updates once the product is installed and periodically

17. Observe the successful installation and click **Finish.**



Veeam Backup & Replication Setup

Completing Veeam Backup & Replication 9.5 Setup Wizard

Installation succeeded.

Setup has finished installing Veeam Backup & Replication on your computer.

Click Finish to exit the wizard.

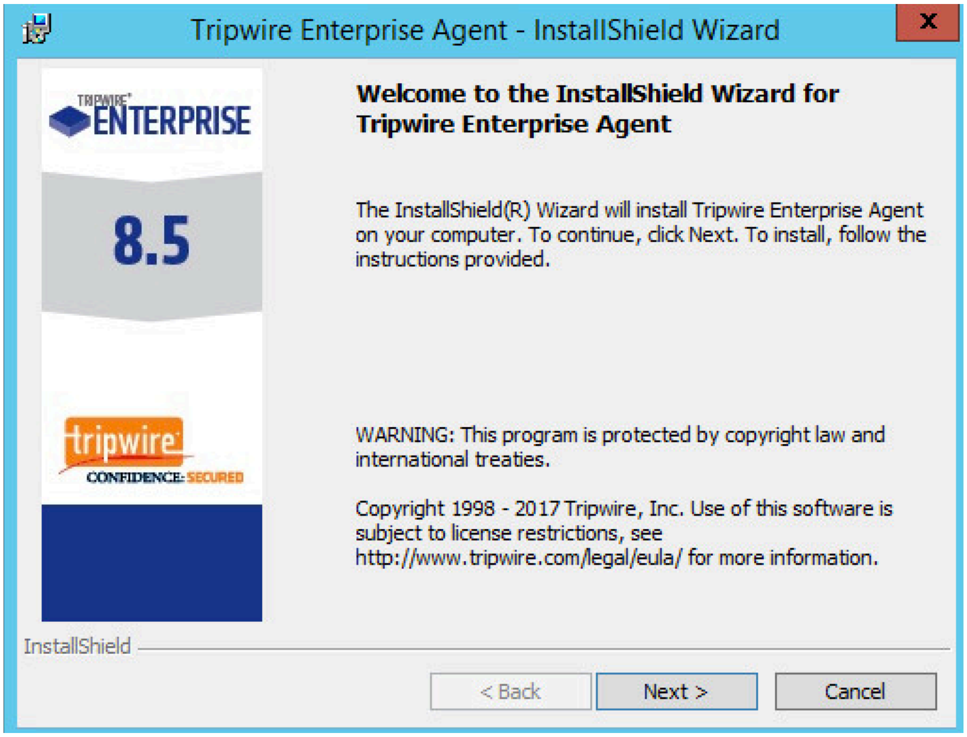
2.10 Tripwire Enterprise and Tripwire Log Center (TLC)

Tripwire Enterprise is a data integrity solution that monitors file activity and associated information across an enterprise. In this solution, we use it to monitor both a MS SQL database and file changes in certain folders. Tripwire Log Center allows for the collection and standardization of logs produced by Tripwire Enterprise.

Please see the *Tripwire Enterprise Install and Maintenance Guide*, accessible from Tripwire for a detailed, illustrated guide to the installation. The only addition to this documentation is that the MS SQL Server should be in “Mixed Mode” for authentication purposes. This section covers the installation and configuration process we used to set up Tripwire Agents on various machines as well as the installation and integration of Tripwire Log Center with Tripwire Enterprise. The result of this integration is the generation and forwarding of events from Tripwire Enterprise to Tripwire Log Center.

2.10.1 Install Tripwire Agent on Windows

1. Run **te_agent.msi** on the client machine.



Tripwire Enterprise Agent - InstallShield Wizard

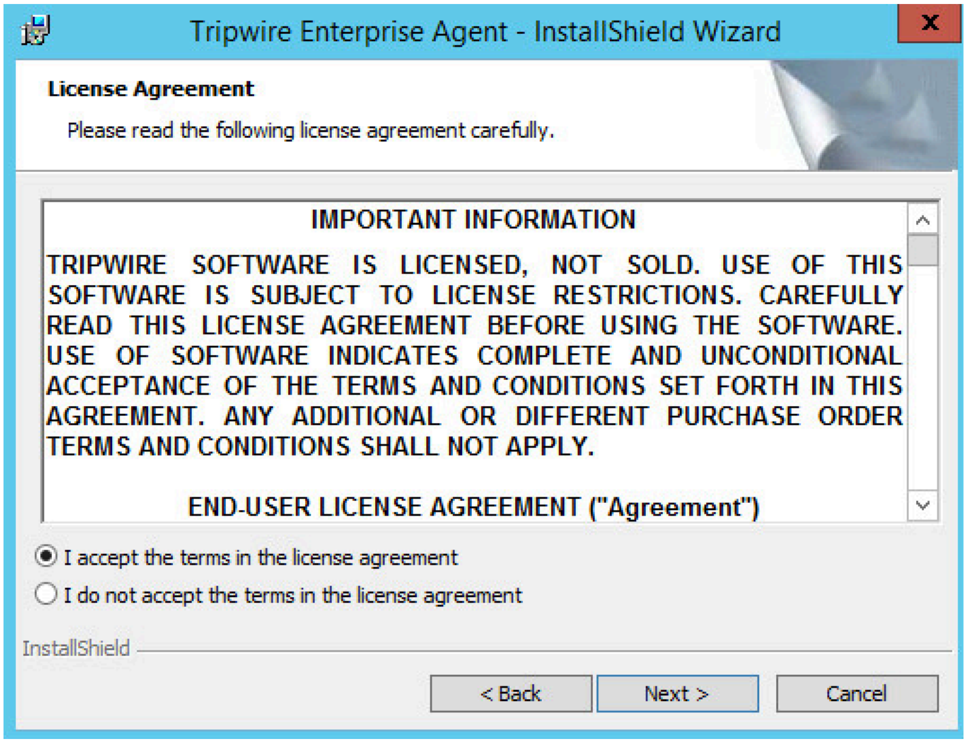
Welcome to the InstallShield Wizard for Tripwire Enterprise Agent

The InstallShield(R) Wizard will install Tripwire Enterprise Agent on your computer. To continue, click Next. To install, follow the instructions provided.

WARNING: This program is protected by copyright law and international treaties.

Copyright 1998 - 2017 Tripwire, Inc. Use of this software is subject to license restrictions, see http://www.tripwire.com/legal/eula/ for more information.

2. Click **Next**.
3. **Accept** the license agreement.



License Agreement

Please read the following license agreement carefully.

IMPORTANT INFORMATION

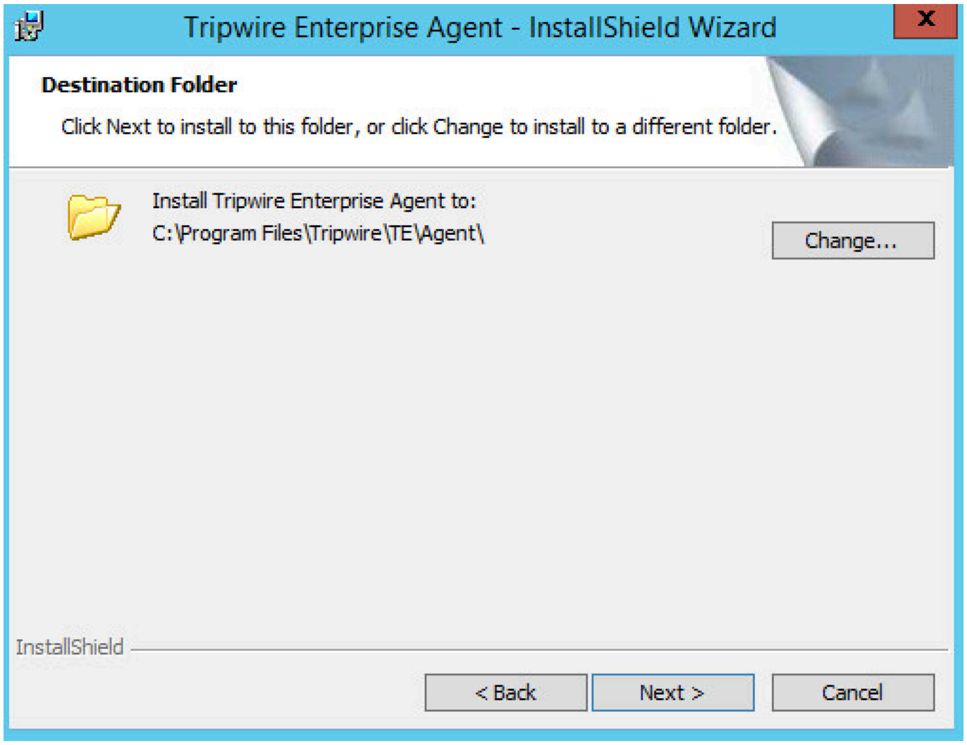
TRIPWIRE SOFTWARE IS LICENSED, NOT SOLD. USE OF THIS SOFTWARE IS SUBJECT TO LICENSE RESTRICTIONS. CAREFULLY READ THIS LICENSE AGREEMENT BEFORE USING THE SOFTWARE. USE OF SOFTWARE INDICATES COMPLETE AND UNCONDITIONAL ACCEPTANCE OF THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. ANY ADDITIONAL OR DIFFERENT PURCHASE ORDER TERMS AND CONDITIONS SHALL NOT APPLY.

END-USER LICENSE AGREEMENT ("Agreement")

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. Click **Next**.
5. Specify the installation path.

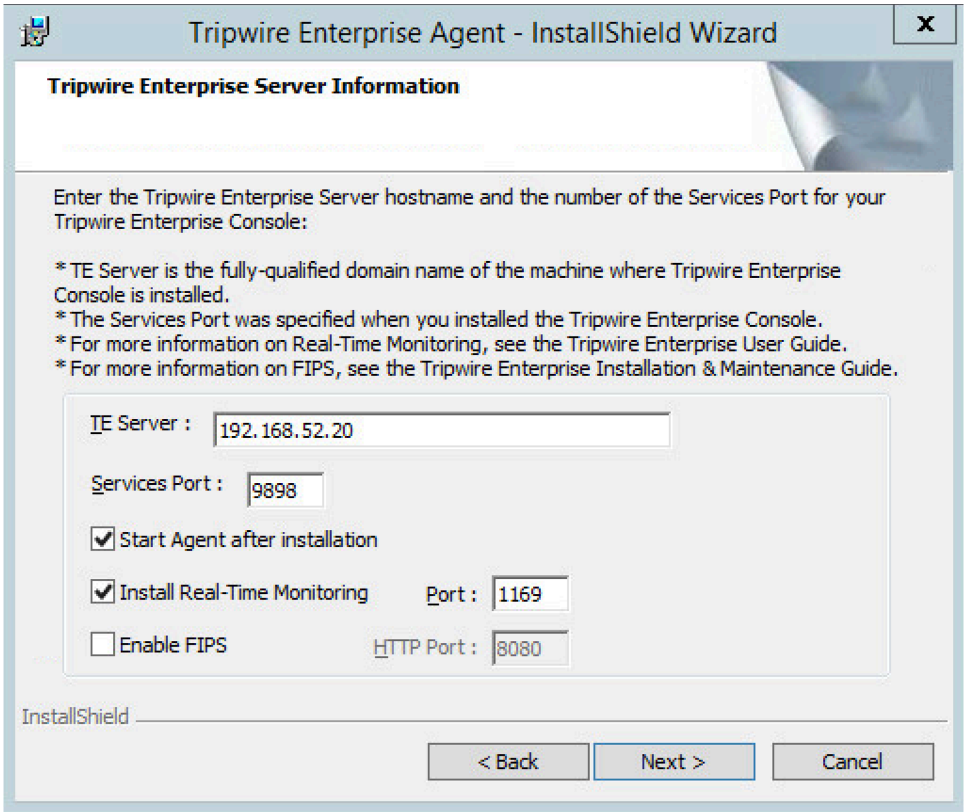


Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Tripwire Enterprise Agent to:
C:\Program Files\Tripwire\TE\Agent\

6. Click **Next**.
7. Enter the **IP address** of the Tripwire server.



Tripwire Enterprise Agent - InstallShield Wizard

Tripwire Enterprise Server Information

Enter the Tripwire Enterprise Server hostname and the number of the Services Port for your Tripwire Enterprise Console:

* TE Server is the fully-qualified domain name of the machine where Tripwire Enterprise Console is installed.
* The Services Port was specified when you installed the Tripwire Enterprise Console.
* For more information on Real-Time Monitoring, see the Tripwire Enterprise User Guide.
* For more information on FIPS, see the Tripwire Enterprise Installation & Maintenance Guide.

TE Server : 192.168.52.20

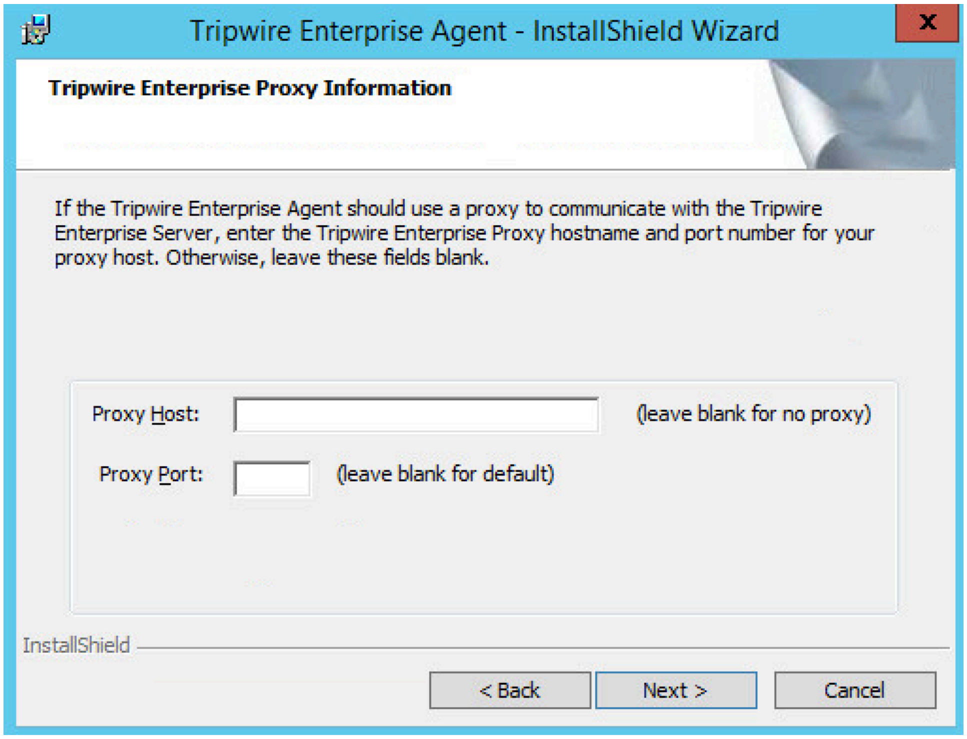
Services Port : 9898

☑ Start Agent after installation

☑ Install Real-Time Monitoring Port : 1169

☐ Enable FIPS HTTP Port : 8080

8. Click **Next**.
9. Leave the proxy settings blank.



Tripwire Enterprise Agent - InstallShield Wizard

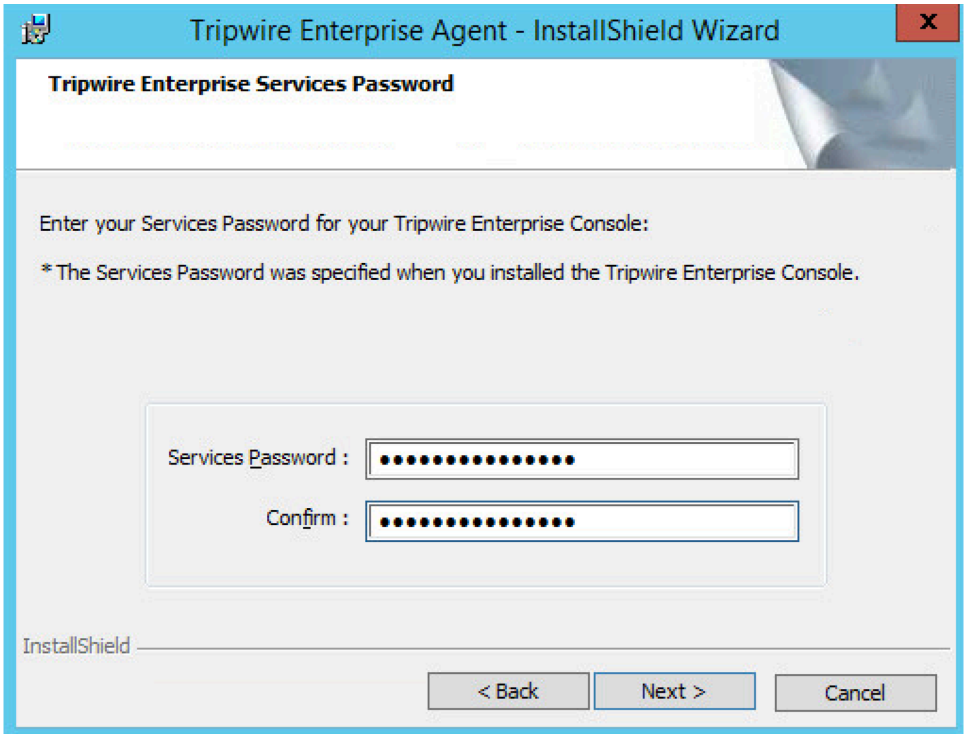
Tripwire Enterprise Proxy Information

If the Tripwire Enterprise Agent should use a proxy to communicate with the Tripwire Enterprise Server, enter the Tripwire Enterprise Proxy hostname and port number for your proxy host. Otherwise, leave these fields blank.

Proxy Host: (leave blank for no proxy)

Proxy Port: (leave blank for default)

10. Click **Next**.
11. Enter the **services password** specified in the server upon installation twice.


Tripwire Enterprise Agent - InstallShield Wizard

Tripwire Enterprise Services Password

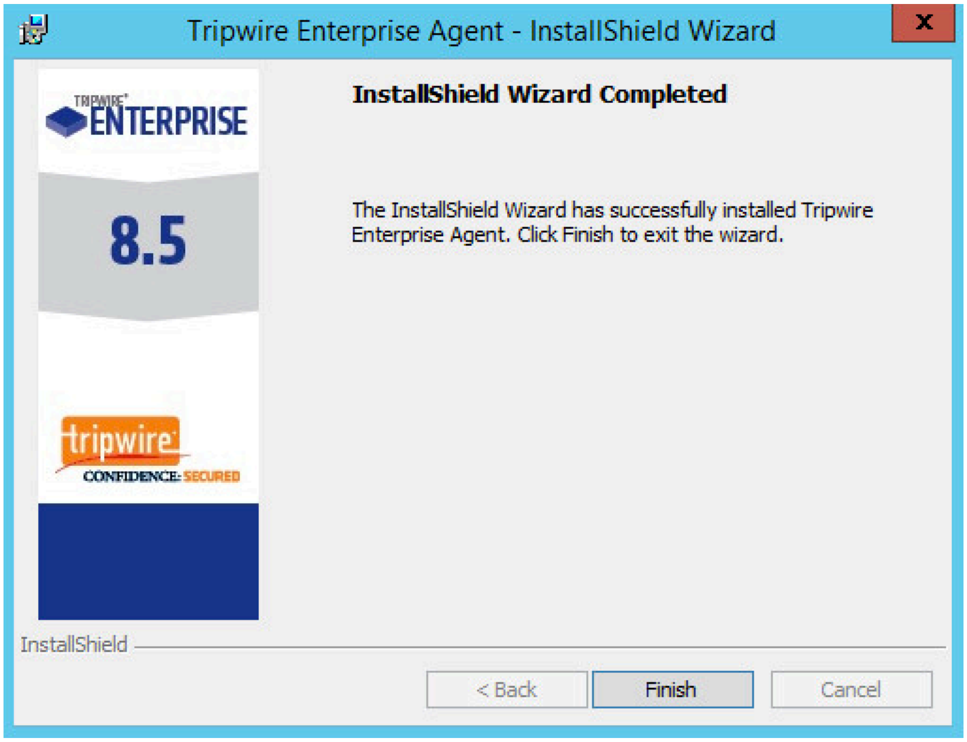
Enter your Services Password for your Tripwire Enterprise Console:

* The Services Password was specified when you installed the Tripwire Enterprise Console.

Services Password : ●●●●●●●●●●●●●●●

Confirm : ●●●●●●●●●●●●●●●

12. Click **Next**.


Tripwire Enterprise Agent - InstallShield Wizard

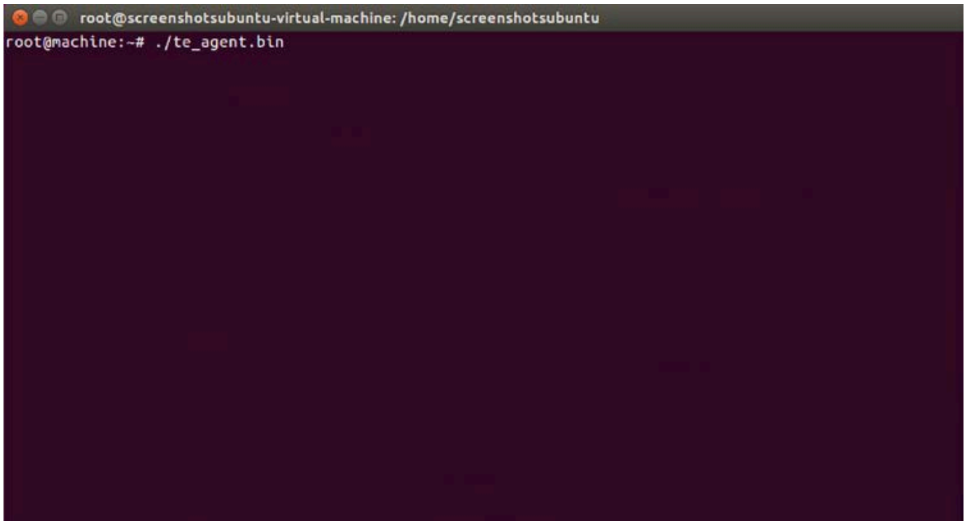
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Tripwire Enterprise Agent. Click Finish to exit the wizard.

13. Click **Install**.
14. Start **Tripwire Agent** from the start menu (on some systems it may start automatically - check **services.msc** to verify that it is running).

2.10.2 Install Tripwire Agent on Ubuntu

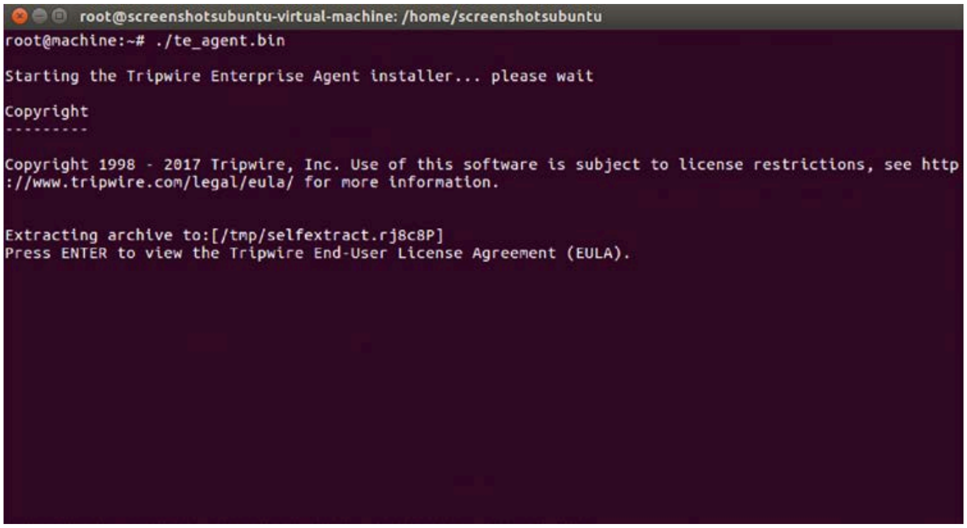
1. Execute the following commands as root.
2. Run **te_agent.bin** by issuing the command:
    a. `./te_agent.bin`



root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
root@machine:~# ./te_agent.bin
```

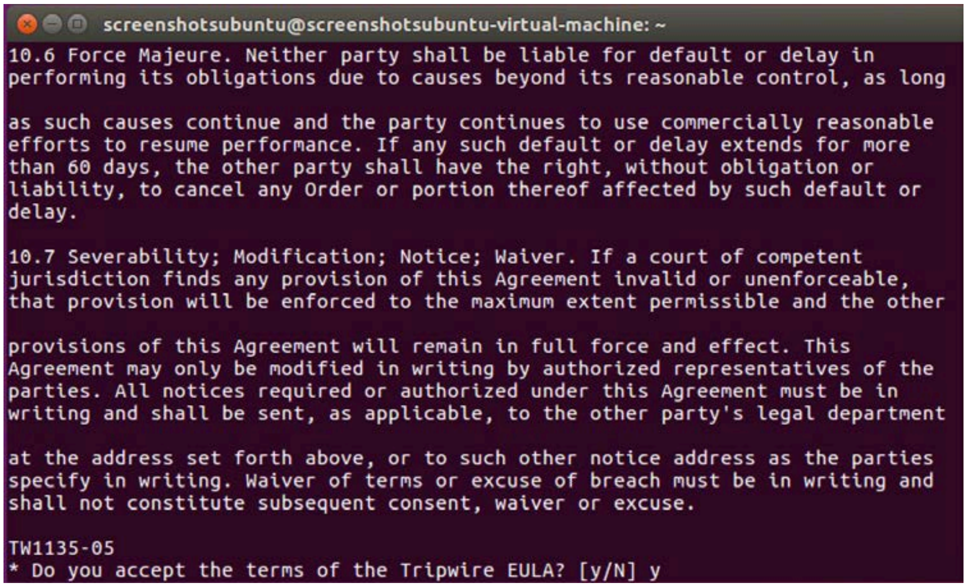
3. Press **Enter** repeatedly to read through the EULA.



root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

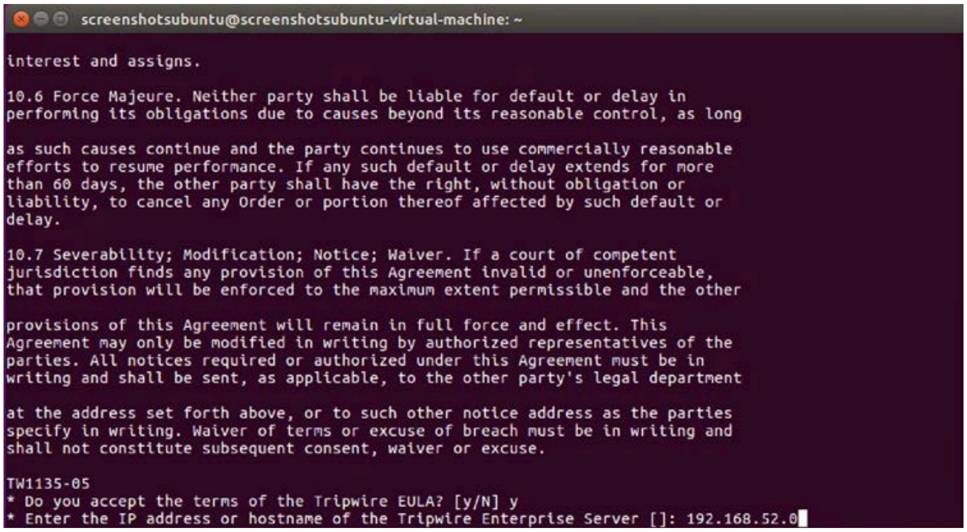
```
root@machine:~# ./te_agent.bin

Starting the Tripwire Enterprise Agent installer... please wait

Copyright
---------

Copyright 1998 - 2017 Tripwire, Inc. Use of this software is subject to license restrictions, see http
://www.tripwire.com/legal/eula/ for more information.


Extracting archive to:[/tmp/selfextract.rj8c8P]
Press ENTER to view the Tripwire End-User License Agreement (EULA).
```

4. Enter **Y** to accept the EULA.



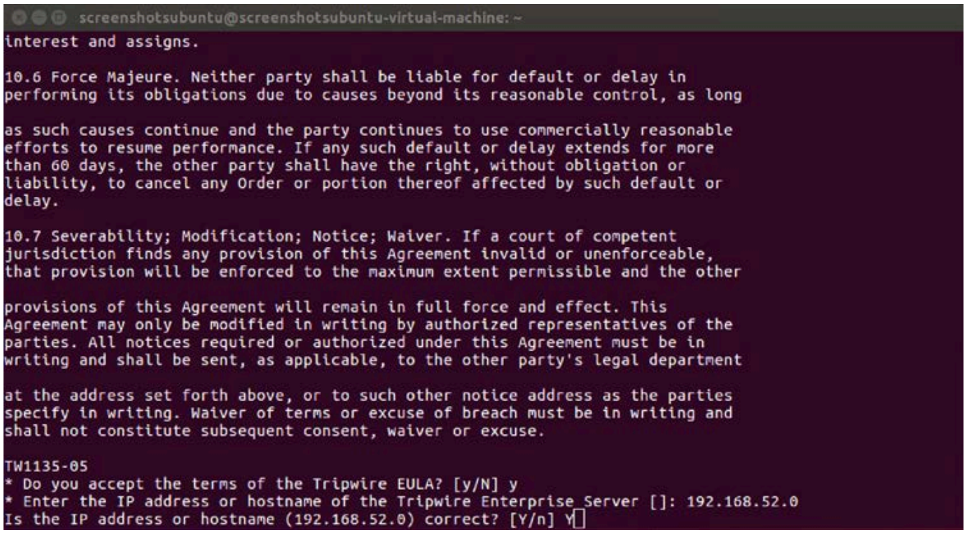
```
10.6 Force Majeure. Neither party shall be liable for default or delay in
performing its obligations due to causes beyond its reasonable control, as long

as such causes continue and the party continues to use commercially reasonable
efforts to resume performance. If any such default or delay extends for more
than 60 days, the other party shall have the right, without obligation or
liability, to cancel any Order or portion thereof affected by such default or
delay.

10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
```

5. Press **Enter**.
6. Enter the **IP address** of the Tripwire server.



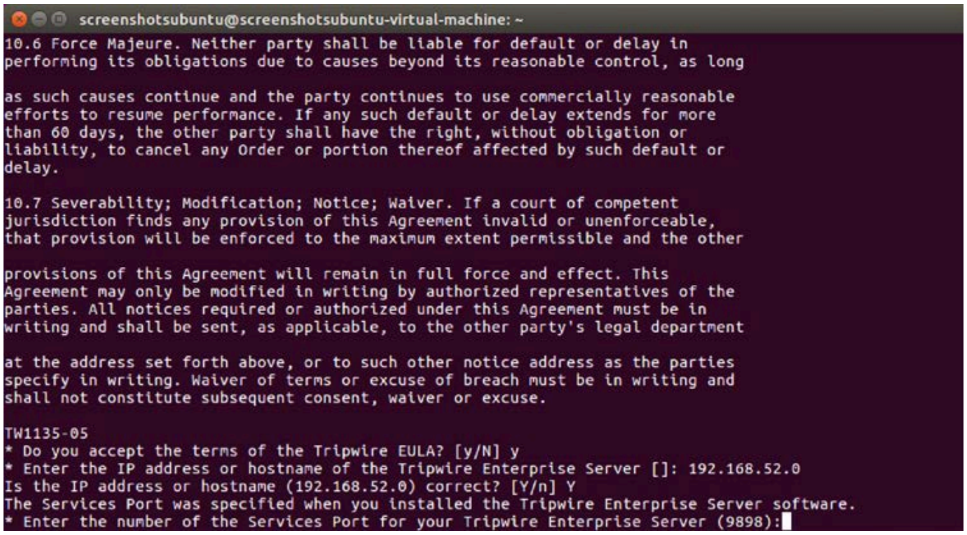
```
interest and assigns.

10.6 Force Majeure. Neither party shall be liable for default or delay in
performing its obligations due to causes beyond its reasonable control, as long

as such causes continue and the party continues to use commercially reasonable
efforts to resume performance. If any such default or delay extends for more
than 60 days, the other party shall have the right, without obligation or
liability, to cancel any Order or portion thereof affected by such default or
delay.

10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
```

7. Press **Enter**.
8. Enter **Y** if the address was entered correctly.



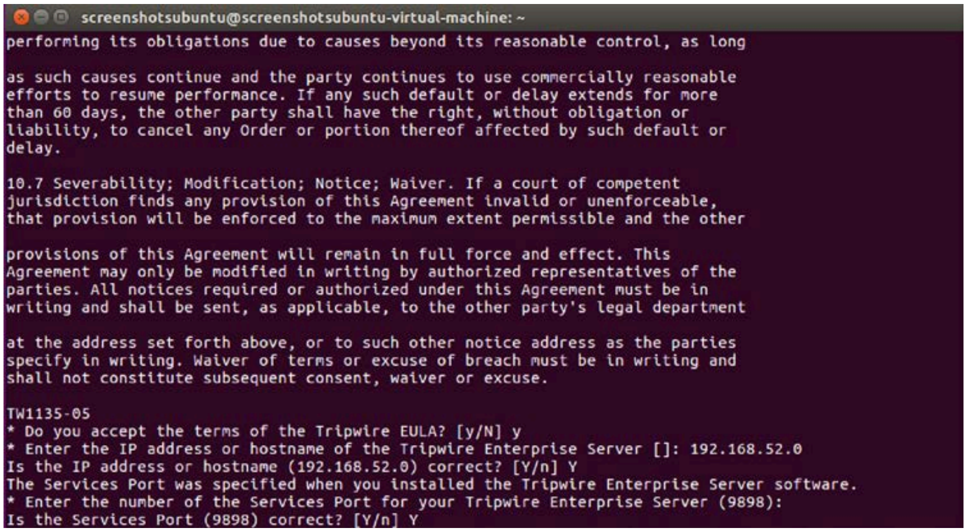
```
screenshotsubuntu@screenshotsubuntu-virtual-machine: ~
interest and assigns.

10.6 Force Majeure. Neither party shall be liable for default or delay in
performing its obligations due to causes beyond its reasonable control, as long

as such causes continue and the party continues to use commercially reasonable
efforts to resume performance. If any such default or delay extends for more
than 60 days, the other party shall have the right, without obligation or
liability, to cancel any Order or portion thereof affected by such default or
delay.

10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
```

9. Press **Enter**.



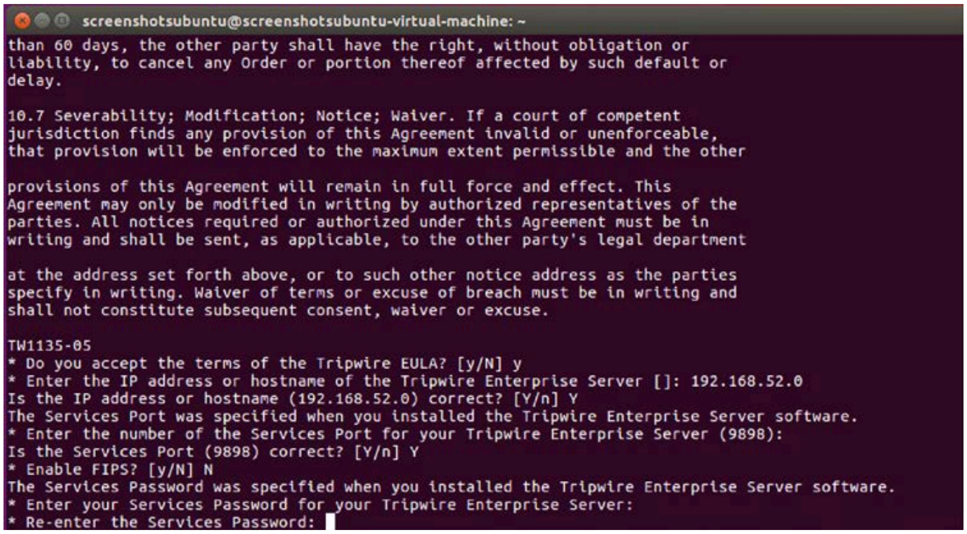
```
screenshotsubuntu@screenshotsubuntu-virtual-machine: ~
10.6 Force Majeure. Neither party shall be liable for default or delay in
performing its obligations due to causes beyond its reasonable control, as long

as such causes continue and the party continues to use commercially reasonable
efforts to resume performance. If any such default or delay extends for more
than 60 days, the other party shall have the right, without obligation or
liability, to cancel any Order or portion thereof affected by such default or
delay.

10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
```

10. Press **Enter**.
11. Enter **Y** to use the default port number.



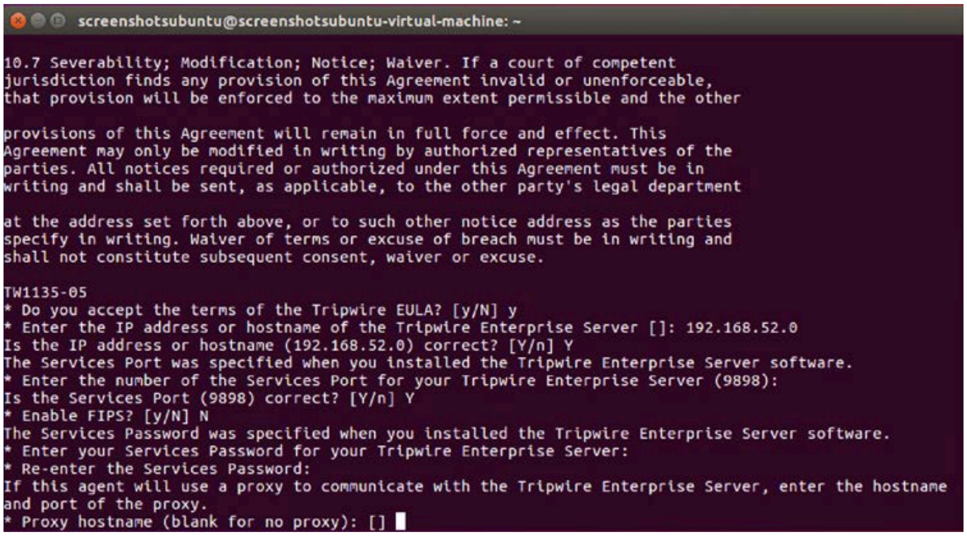
```
performing its obligations due to causes beyond its reasonable control, as long

as such causes continue and the party continues to use commercially reasonable
efforts to resume performance. If any such default or delay extends for more
than 60 days, the other party shall have the right, without obligation or
liability, to cancel any Order or portion thereof affected by such default or
delay.

10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
```

12. Press **Enter**.
13. Use the Federal Information Processing Standard (FIPS) setting that best fits your organizational needs.
14. Press **Enter**.
15. Enter the **services password** twice, pressing **Enter** after each time. Note that no text will appear while typing the password.



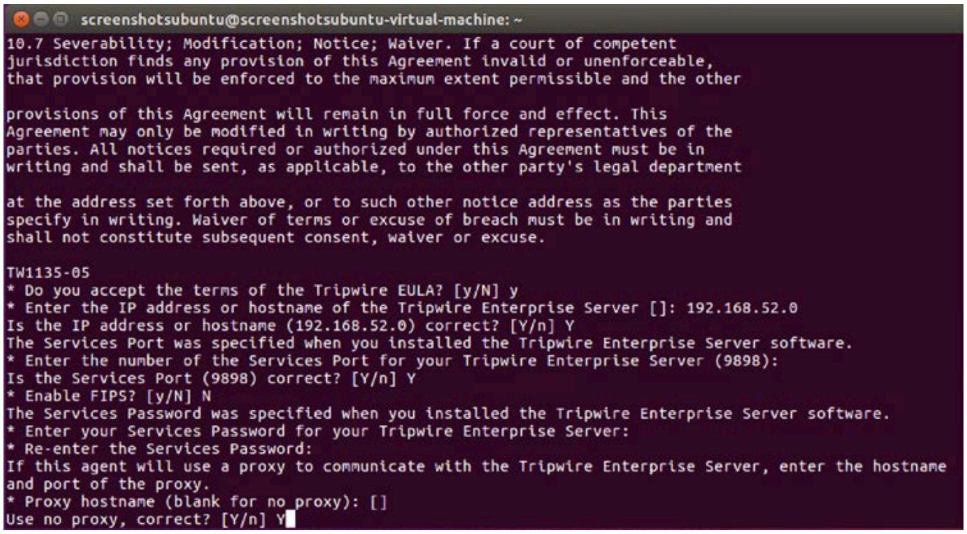
```
than 60 days, the other party shall have the right, without obligation or
liability, to cancel any Order or portion thereof affected by such default or
delay.

10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
* Enable FIPS? [y/N] N
The Services Password was specified when you installed the Tripwire Enterprise Server software.
* Enter your Services Password for your Tripwire Enterprise Server:
* Re-enter the Services Password:
```

16. Press **Enter** to skip using a proxy.



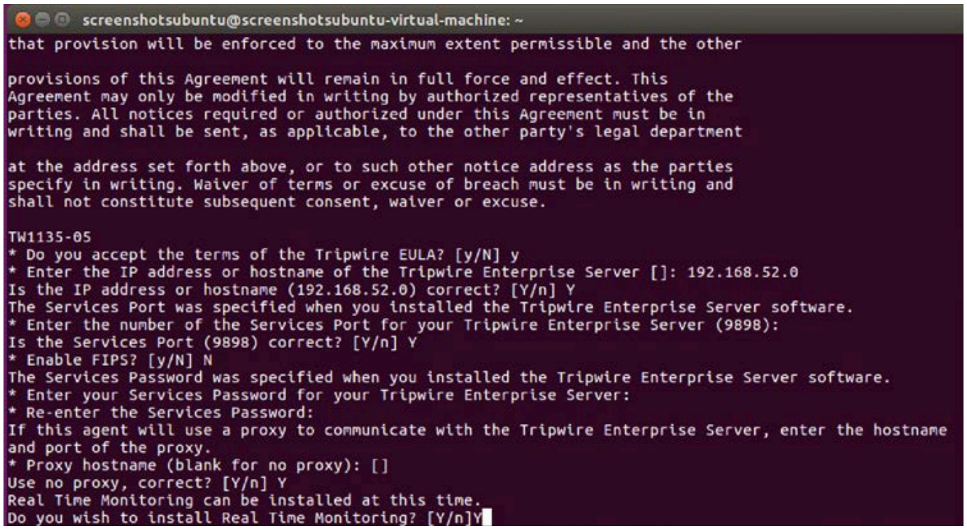
```
10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
* Enable FIPS? [y/N] N
The Services Password was specified when you installed the Tripwire Enterprise Server software.
* Enter your Services Password for your Tripwire Enterprise Server:
* Re-enter the Services Password:
If this agent will use a proxy to communicate with the Tripwire Enterprise Server, enter the hostname
and port of the proxy.
* Proxy hostname (blank for no proxy): []
```

17. Press **Y**.



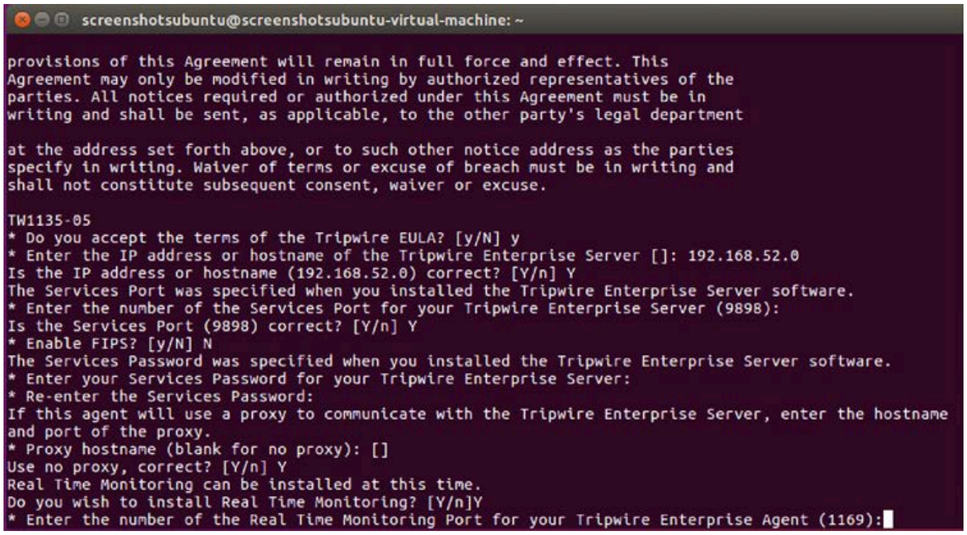
```
10.7 Severability; Modification; Notice; Waiver. If a court of competent
jurisdiction finds any provision of this Agreement invalid or unenforceable,
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
* Enable FIPS? [y/N] N
The Services Password was specified when you installed the Tripwire Enterprise Server software.
* Enter your Services Password for your Tripwire Enterprise Server:
* Re-enter the Services Password:
If this agent will use a proxy to communicate with the Tripwire Enterprise Server, enter the hostname
and port of the proxy.
* Proxy hostname (blank for no proxy): []
Use no proxy, correct? [Y/n] Y
```

18. Press **Enter**.
19. Press **Y** to install **Real Time Monitoring**.



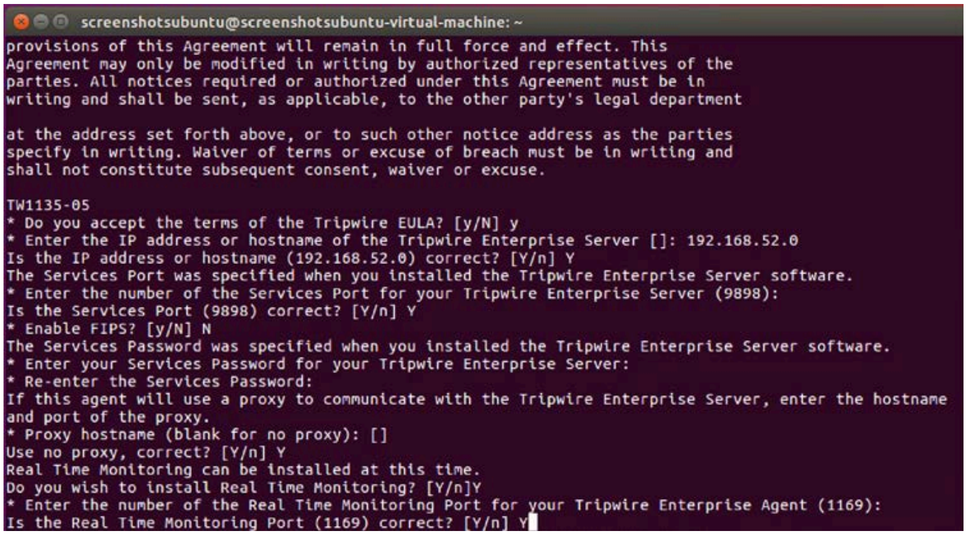
```
that provision will be enforced to the maximum extent permissible and the other

provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
* Enable FIPS? [y/N] N
The Services Password was specified when you installed the Tripwire Enterprise Server software.
* Enter your Services Password for your Tripwire Enterprise Server:
* Re-enter the Services Password:
If this agent will use a proxy to communicate with the Tripwire Enterprise Server, enter the hostname
and port of the proxy.
* Proxy hostname (blank for no proxy): []
Use no proxy, correct? [Y/n] Y
Real Time Monitoring can be installed at this time.
Do you wish to install Real Time Monitoring? [Y/n]Y
```

20. Press **Enter**.



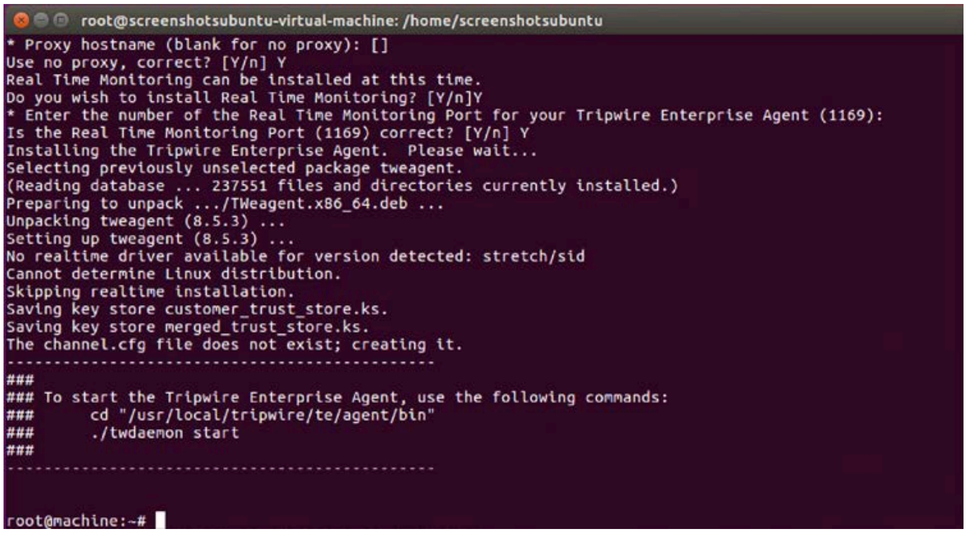
```
provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
* Enable FIPS? [y/N] N
The Services Password was specified when you installed the Tripwire Enterprise Server software.
* Enter your Services Password for your Tripwire Enterprise Server:
* Re-enter the Services Password:
If this agent will use a proxy to communicate with the Tripwire Enterprise Server, enter the hostname
and port of the proxy.
* Proxy hostname (blank for no proxy): []
Use no proxy, correct? [Y/n] Y
Real Time Monitoring can be installed at this time.
Do you wish to install Real Time Monitoring? [Y/n]Y
* Enter the number of the Real Time Monitoring Port for your Tripwire Enterprise Agent (1169):
```

21. Press **Enter** to accept the default port.
22. Press **Y**.



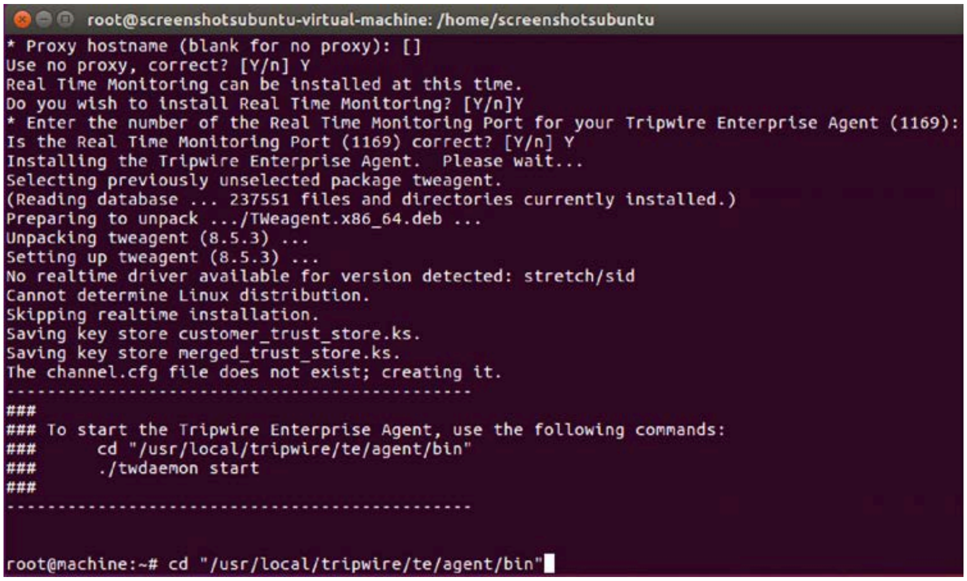
```
screenshotsubuntu@screenshotsubuntu-virtual-machine: ~
provisions of this Agreement will remain in full force and effect. This
Agreement may only be modified in writing by authorized representatives of the
parties. All notices required or authorized under this Agreement must be in
writing and shall be sent, as applicable, to the other party's legal department

at the address set forth above, or to such other notice address as the parties
specify in writing. Waiver of terms or excuse of breach must be in writing and
shall not constitute subsequent consent, waiver or excuse.

TW1135-05
* Do you accept the terms of the Tripwire EULA? [y/N] y
* Enter the IP address or hostname of the Tripwire Enterprise Server []: 192.168.52.0
Is the IP address or hostname (192.168.52.0) correct? [Y/n] Y
The Services Port was specified when you installed the Tripwire Enterprise Server software.
* Enter the number of the Services Port for your Tripwire Enterprise Server (9898):
Is the Services Port (9898) correct? [Y/n] Y
* Enable FIPS? [y/N] N
The Services Password was specified when you installed the Tripwire Enterprise Server software.
* Enter your Services Password for your Tripwire Enterprise Server:
* Re-enter the Services Password:
If this agent will use a proxy to communicate with the Tripwire Enterprise Server, enter the hostname
and port of the proxy.
* Proxy hostname (blank for no proxy): []
Use no proxy, correct? [Y/n] Y
Real Time Monitoring can be installed at this time.
Do you wish to install Real Time Monitoring? [Y/n]Y
* Enter the number of the Real Time Monitoring Port for your Tripwire Enterprise Agent (1169):
Is the Real Time Monitoring Port (1169) correct? [Y/n] Y
```

23. Press **Enter**.
24. The agent should install.



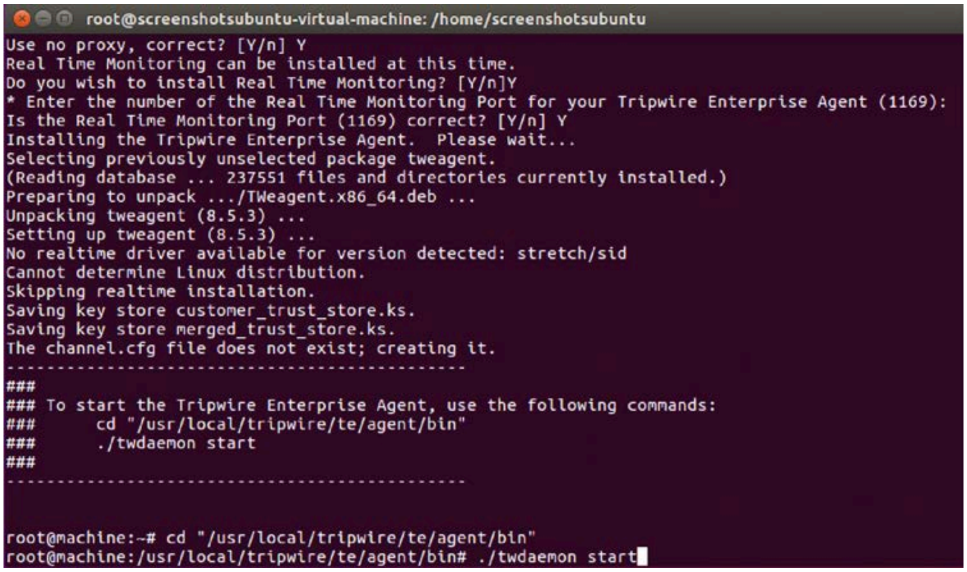
```
root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu
* Proxy hostname (blank for no proxy): []
Use no proxy, correct? [Y/n] Y
Real Time Monitoring can be installed at this time.
Do you wish to install Real Time Monitoring? [Y/n]Y
* Enter the number of the Real Time Monitoring Port for your Tripwire Enterprise Agent (1169):
Is the Real Time Monitoring Port (1169) correct? [Y/n] Y
Installing the Tripwire Enterprise Agent.  Please wait...
Selecting previously unselected package tweagent.
(Reading database ... 237551 files and directories currently installed.)
Preparing to unpack .../TWeagent.x86_64.deb ...
Unpacking tweagent (8.5.3) ...
Setting up tweagent (8.5.3) ...
No realtime driver available for version detected: stretch/sid
Cannot determine Linux distribution.
Skipping realtime installation.
Saving key store customer_trust_store.ks.
Saving key store merged_trust_store.ks.
The channel.cfg file does not exist; creating it.
---------------------------------------------
###
### To start the Tripwire Enterprise Agent, use the following commands:
###      cd "/usr/local/tripwire/te/agent/bin"
###      ./twdaemon start
###
---------------------------------------------


root@machine:~#
```

25. Run the following commands as root:
    a. **`cd "/usr/local/tripwire/te/agent/bin"`**



```
root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu
* Proxy hostname (blank for no proxy): []
Use no proxy, correct? [Y/n] Y
Real Time Monitoring can be installed at this time.
Do you wish to install Real Time Monitoring? [Y/n]Y
* Enter the number of the Real Time Monitoring Port for your Tripwire Enterprise Agent (1169):
Is the Real Time Monitoring Port (1169) correct? [Y/n] Y
Installing the Tripwire Enterprise Agent.  Please wait...
Selecting previously unselected package tweagent.
(Reading database ... 237551 files and directories currently installed.)
Preparing to unpack .../TWeagent.x86_64.deb ...
Unpacking tweagent (8.5.3) ...
Setting up tweagent (8.5.3) ...
No realtime driver available for version detected: stretch/sid
Cannot determine Linux distribution.
Skipping realtime installation.
Saving key store customer_trust_store.ks.
Saving key store merged_trust_store.ks.
The channel.cfg file does not exist; creating it.
---------------------------------------------
###
### To start the Tripwire Enterprise Agent, use the following commands:
###      cd "/usr/local/tripwire/te/agent/bin"
###      ./twdaemon start
###
---------------------------------------------


root@machine:~# cd "/usr/local/tripwire/te/agent/bin"
```

b. `./twdaemon start`



```
root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu
Use no proxy, correct? [Y/n] Y
Real Time Monitoring can be installed at this time.
Do you wish to install Real Time Monitoring? [Y/n]Y
* Enter the number of the Real Time Monitoring Port for your Tripwire Enterprise Agent (1169):
Is the Real Time Monitoring Port (1169) correct? [Y/n] Y
Installing the Tripwire Enterprise Agent.  Please wait...
Selecting previously unselected package tweagent.
(Reading database ... 237551 files and directories currently installed.)
Preparing to unpack .../TWeagent.x86_64.deb ...
Unpacking tweagent (8.5.3) ...
Setting up tweagent (8.5.3) ...
No realtime driver available for version detected: stretch/sid
Cannot determine Linux distribution.
Skipping realtime installation.
Saving key store customer_trust_store.ks.
Saving key store merged_trust_store.ks.
The channel.cfg file does not exist; creating it.
---------------------------------------------
###
### To start the Tripwire Enterprise Agent, use the following commands:
###      cd "/usr/local/tripwire/te/agent/bin"
###      ./twdaemon start
###
---------------------------------------------


root@machine:~# cd "/usr/local/tripwire/te/agent/bin"
root@machine:/usr/local/tripwire/te/agent/bin# ./twdaemon start
```

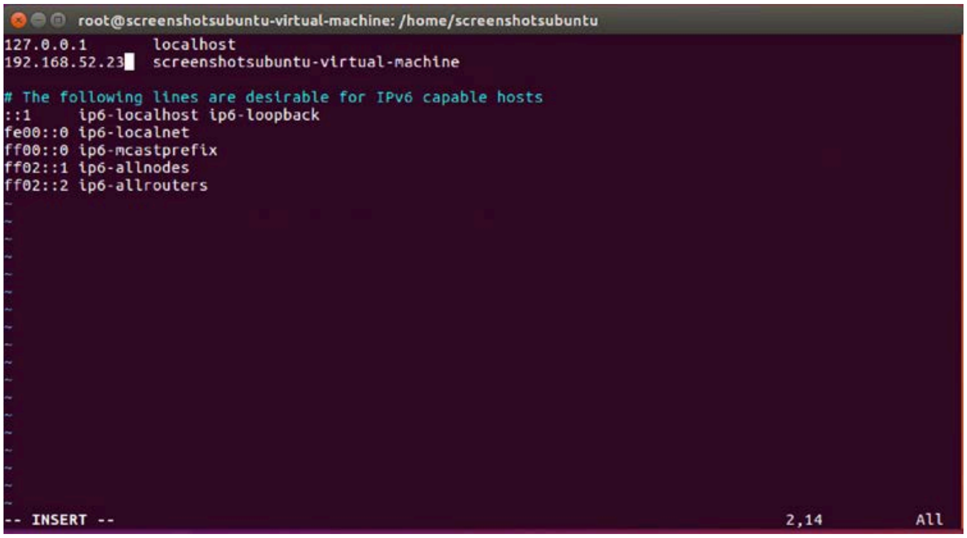
26. You may need to change /etc/hosts in Debian systems if there is a line which looks like this:

```
127.0.1.1    <hostname>
```

Change this to:

```
<IP of machine>    <hostname>
```

Otherwise, Tripwire Enterprise may consider multiple Debian machines as the same machine in the assets view of Tripwire Enterprise.



root@screenshotsubuntu-virtual-machine: /home/screenshotsubuntu

```
127.0.0.1       localhost
192.168.52.23   screenshotsubuntu-virtual-machine

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                                2,14          All
```

2.10.3 Install Tripwire Log Center

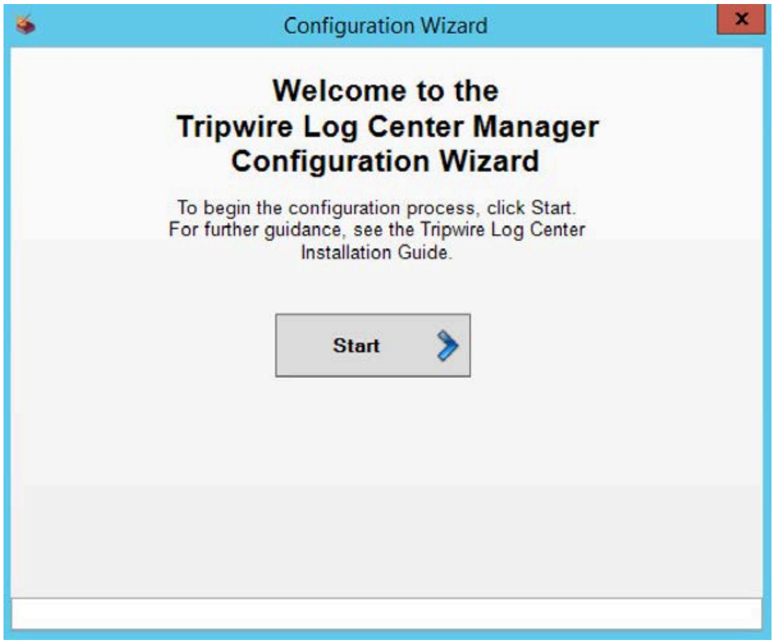
See the *Tripwire Log Center 7.2.4 Installation Guide* that should accompany the installation media for instructions on how to install TLC. Use the Tripwire Log Center Manager installer.

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 Installation Guide.*
c. You may need to unblock port 9898 on your firewall for the Tripwire enterprise agents.
d. Do not install PostgreSQL if you wish to use a database on another system.
e. When it finishes installing there should be a configuration wizard.

2.10.4 Configure Tripwire Log Center

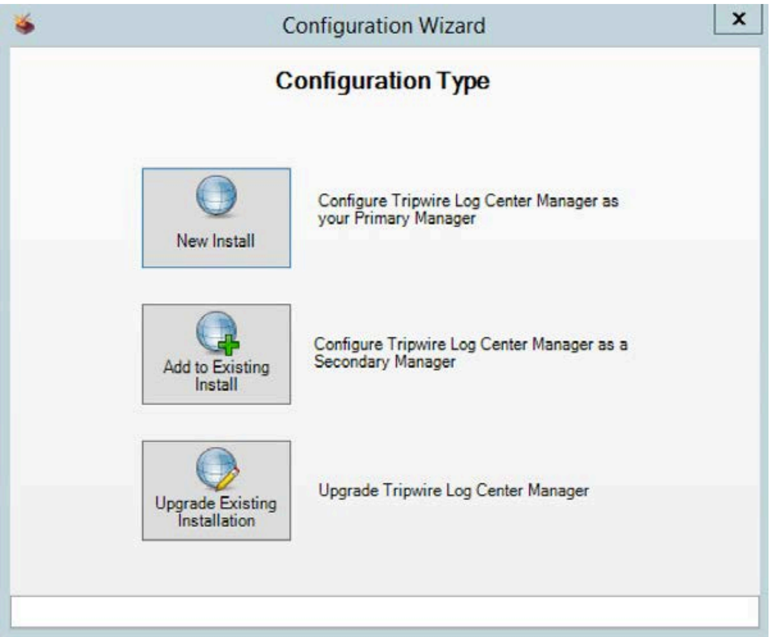
1. Click **Start**.


Configuration Wizard

Welcome to the
Tripwire Log Center Manager
Configuration Wizard

To begin the configuration process, click Start.
For further guidance, see the Tripwire Log Center
Installation Guide.

2. Click **New Install**.

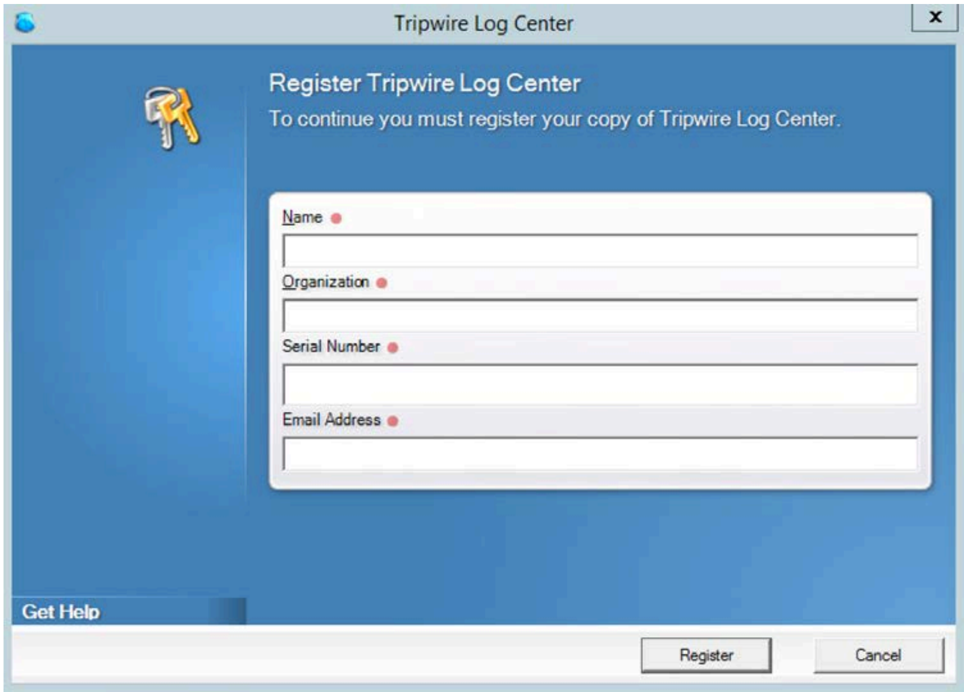

Configuration Wizard

Configuration Type

New Install
Configure Tripwire Log Center Manager as your Primary Manager
Add to Existing Install
Configure Tripwire Log Center Manager as a Secondary Manager
Upgrade Existing Installation
Upgrade Tripwire Log Center Manager

3. Click **Authorize**.
4. An error may appear asking you to install **.NET 3.5**.
5. To do this, open **Server Manager**.
6. Click **Manage**.
7. Click **Add Roles and Features**.

8. Click **Next**.
9. Select **Role-based or feature-based installation**.
10. Click **Next**.
11. Select the current server from the list.
12. Click **Next**.
13. Click **Next**.
14. Check the box next to **.NET Framework 3.5 Features**.
15. Click **Install**.
16. Wait for the installation to finish.
17. If prompted, enter **Name**, **Organization**, **Serial Number**, and **email address** in the fields. Click **Register**. This step will not appear if the software has already been registered



Tripwire Log Center

Register Tripwire Log Center

To continue you must register your copy of Tripwire Log Center.

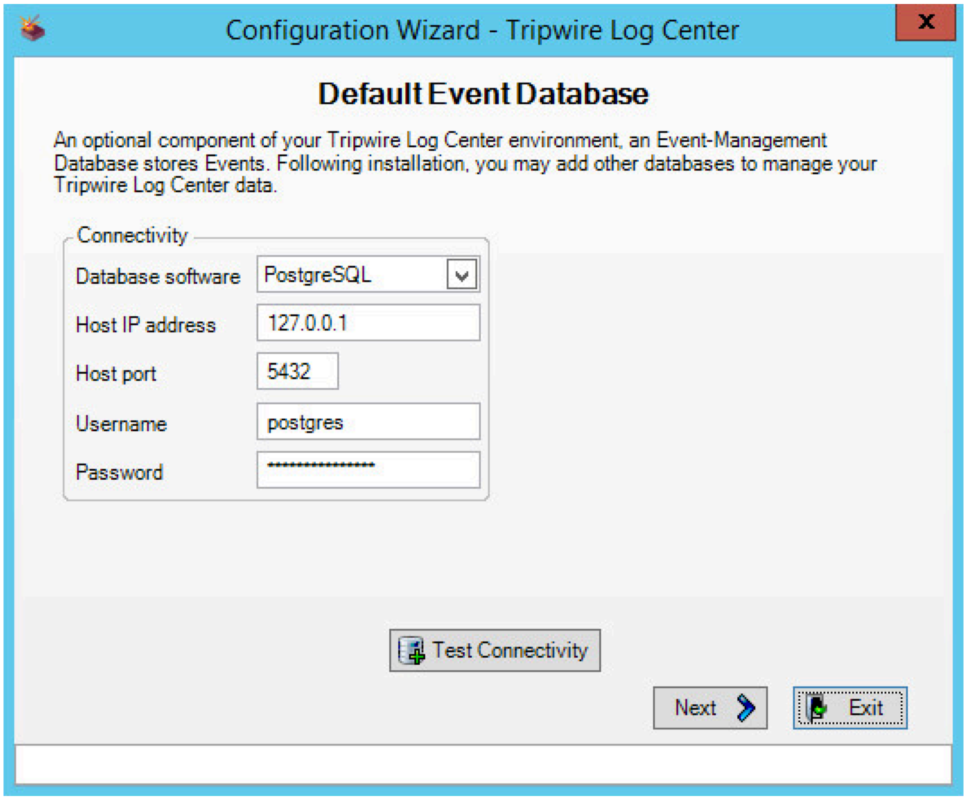
Name ●

Organization ●

Serial Number ●

Email Address ●

18. Click **Close**.
19. Continue with the **configuration wizard**.
20. Enter appropriate details for your **Database Software**.



Configuration Wizard - Tripwire Log Center

Default Event Database

An optional component of your Tripwire Log Center environment, an Event-Management Database stores Events. Following installation, you may add other databases to manage your Tripwire Log Center data.

Connectivity

Database software: PostgreSQL

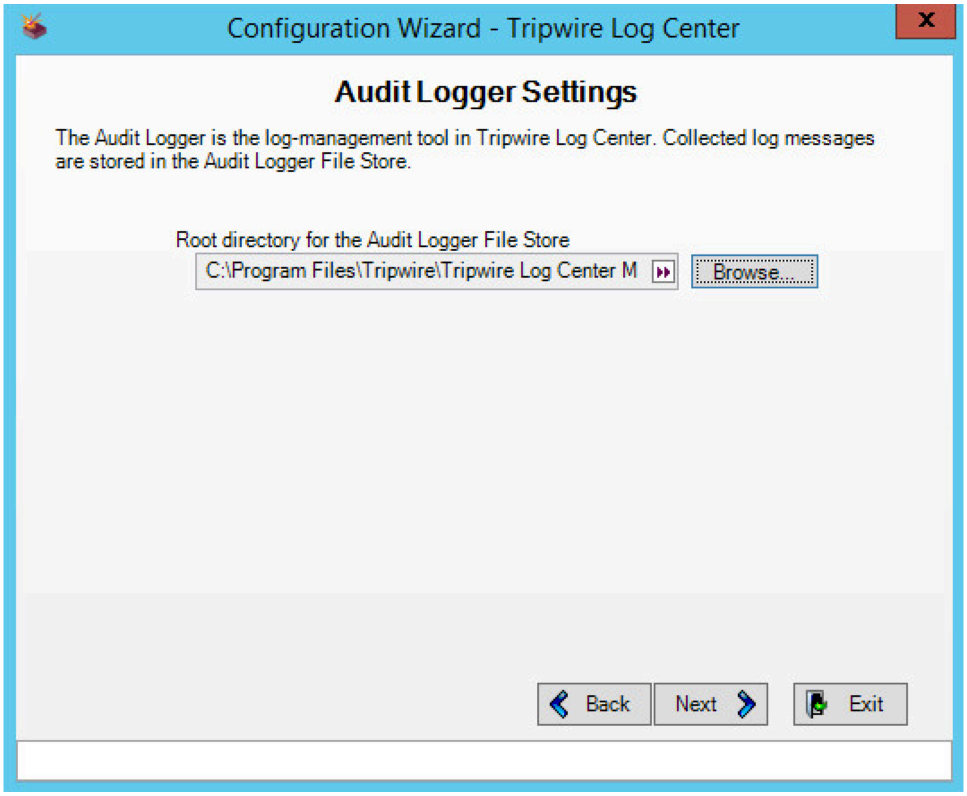
Host IP address: 127.0.0.1

Host port: 5432

Username: postgres

Password: ****************

21. Select **Use Windows Authentication**.
22. Click **Next**.
23. Select a directory to store log messages in. Example*: C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT*



Configuration Wizard - Tripwire Log Center

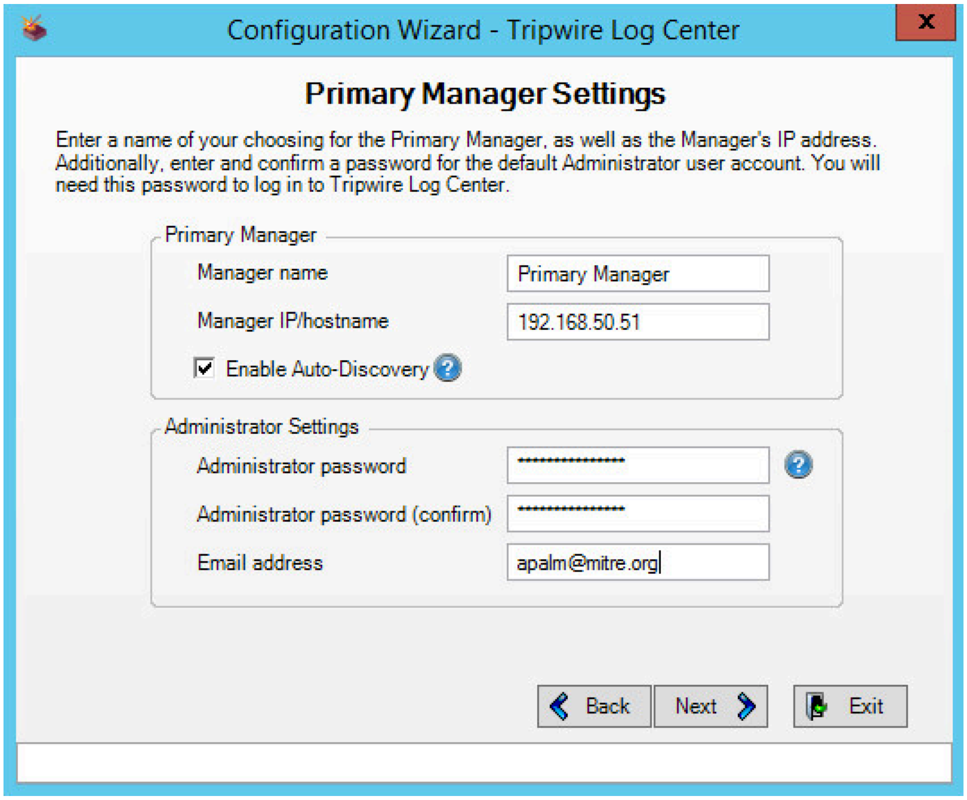
Audit Logger Settings

The Audit Logger is the log-management tool in Tripwire Log Center. Collected log messages are stored in the Audit Logger File Store.

Root directory for the Audit Logger File Store

C:\Program Files\Tripwire\Tripwire Log Center M

24. Click **Next**.
25. Create an Administrator password and enter it twice.
26. Enter your **email address**.



Primary Manager Settings

Enter a name of your choosing for the Primary Manager, as well as the Manager's IP address. Additionally, enter and confirm a password for the default Administrator user account. You will need this password to log in to Tripwire Log Center.

Primary Manager

Manager name: Primary Manager

Manager IP/hostname: 192.168.50.51

☑ Enable Auto-Discovery

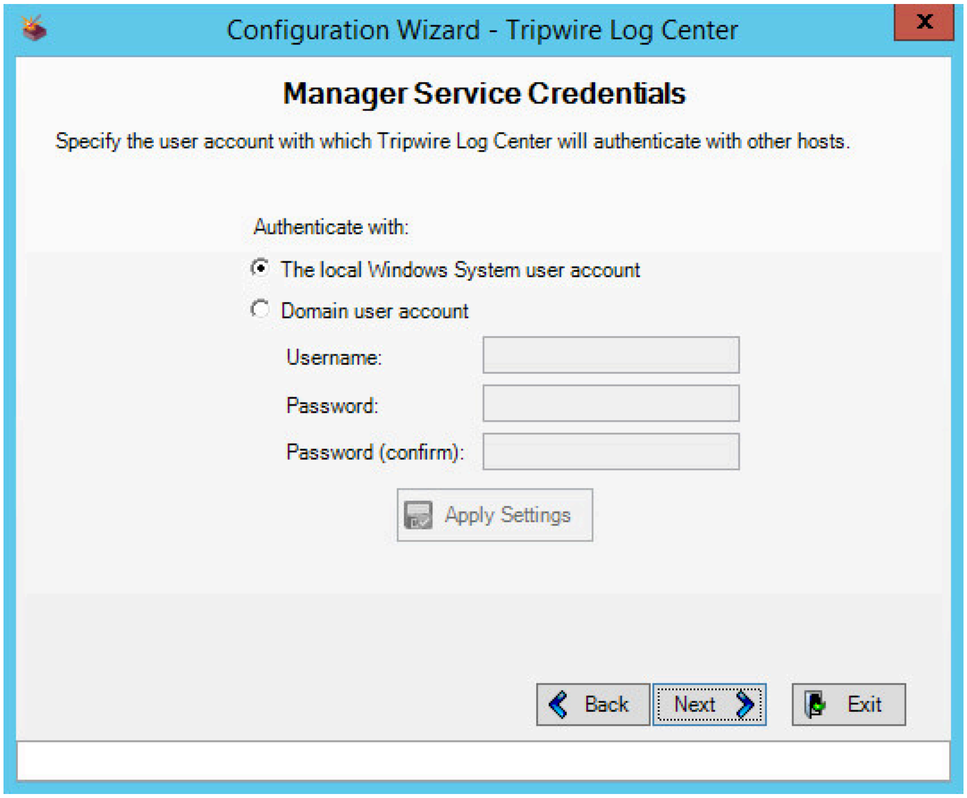
Administrator Settings

Administrator password: ****************

Administrator password (confirm): ****************

Email address: apalm@mitre.org

27. Click **Next**.
28. Select **authenticate with the local windows system user account**.



Manager Service Credentials

Specify the user account with which Tripwire Log Center will authenticate with other hosts.

Authenticate with:

● The local Windows System user account

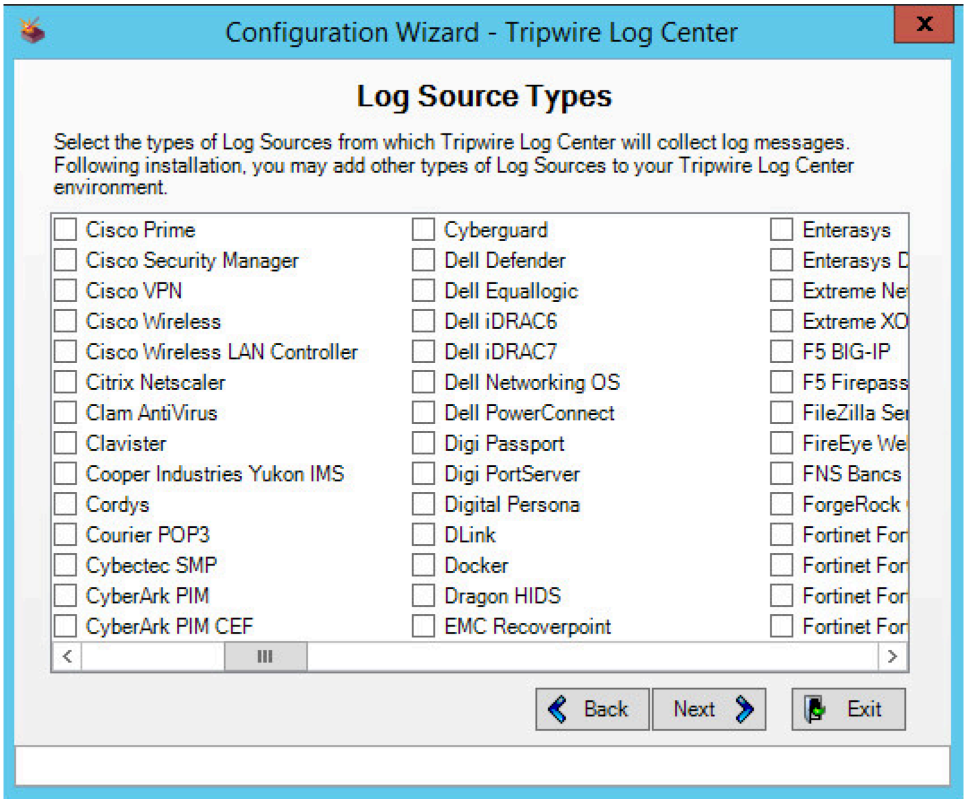
○ Domain user account

Username:

Password:

Password (confirm):

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

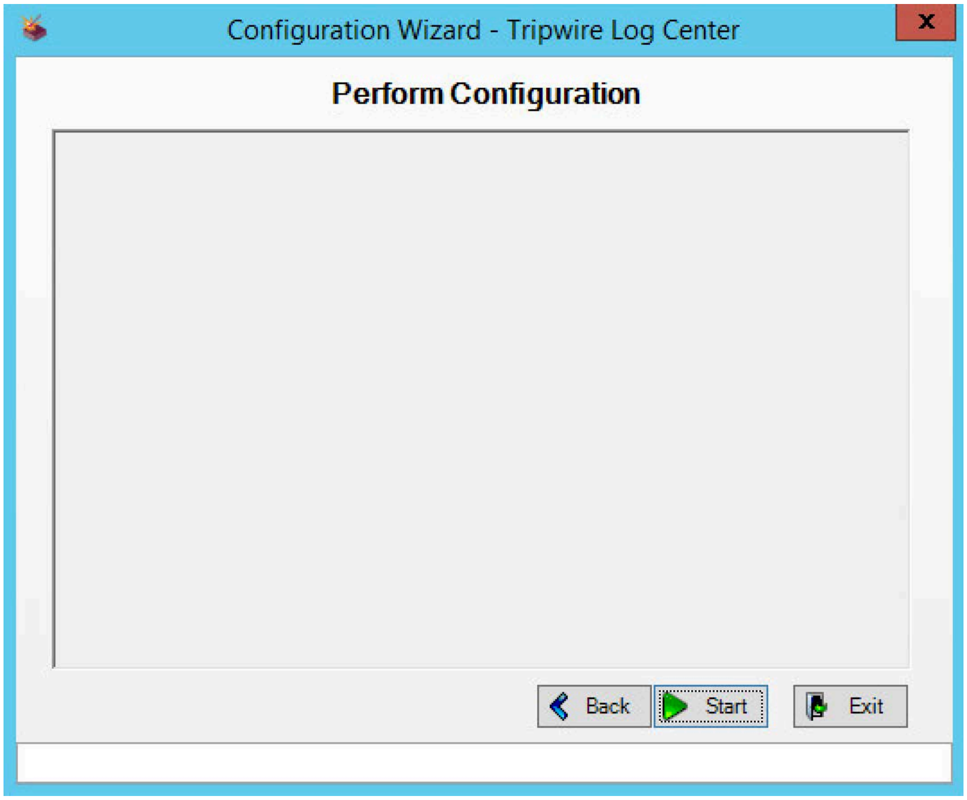


Log Source Types

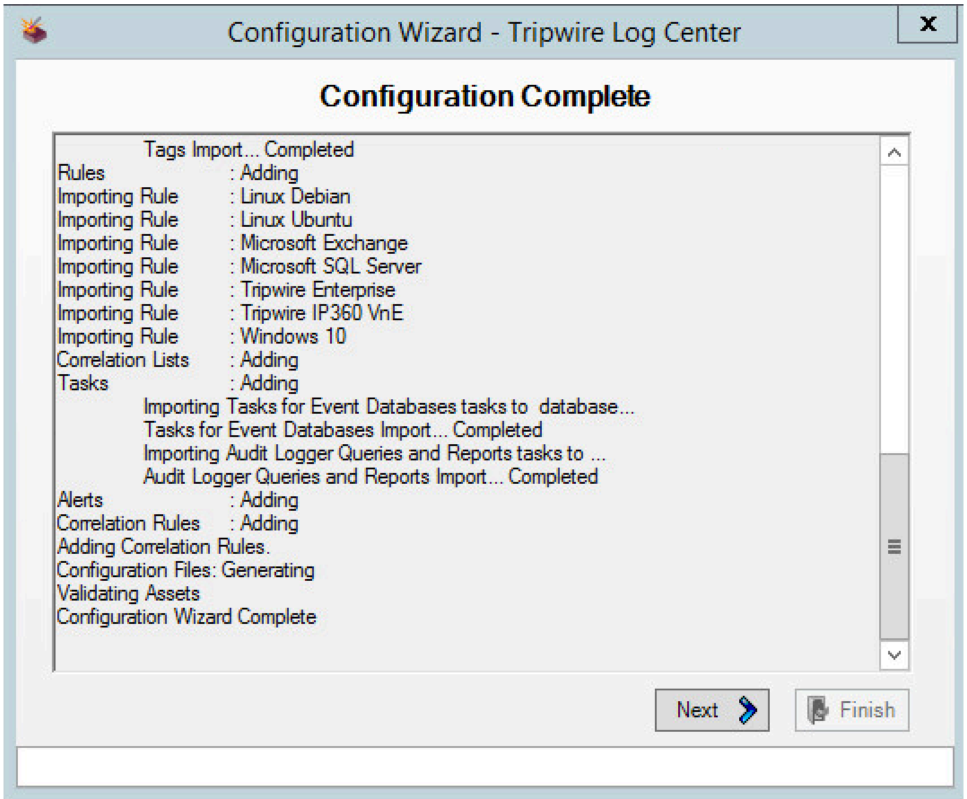
Select the types of Log Sources from which Tripwire Log Center will collect log messages. Following installation, you may add other types of Log Sources to your Tripwire Log Center environment.

- □ Cisco Prime
- □ Cisco Security Manager
- □ Cisco VPN
- □ Cisco Wireless
- □ Cisco Wireless LAN Controller
- □ Citrix Netscaler
- □ Clam AntiVirus
- □ Clavister
- □ Cooper Industries Yukon IMS
- □ Cordys
- □ Courier POP3
- □ Cybectec SMP
- □ CyberArk PIM
- □ CyberArk PIM CEF
- □ Cyberguard
- □ Dell Defender
- □ Dell Equallogic
- □ Dell iDRAC6
- □ Dell iDRAC7
- □ Dell Networking OS
- □ Dell PowerConnect
- □ Digi Passport
- □ Digi PortServer
- □ Digital Persona
- □ DLink
- □ Docker
- □ Dragon HIDS
- □ EMC Recoverpoint
- □ Enterasys
- □ Enterasys D
- □ Extreme Ne
- □ Extreme XO
- □ F5 BIG-IP
- □ F5 Firepass
- □ FileZilla Se
- □ FireEye We
- □ FNS Bancs
- □ ForgeRock
- □ Fortinet For
- □ Fortinet For
- □ Fortinet For
- □ Fortinet For

31. Click **Next**.

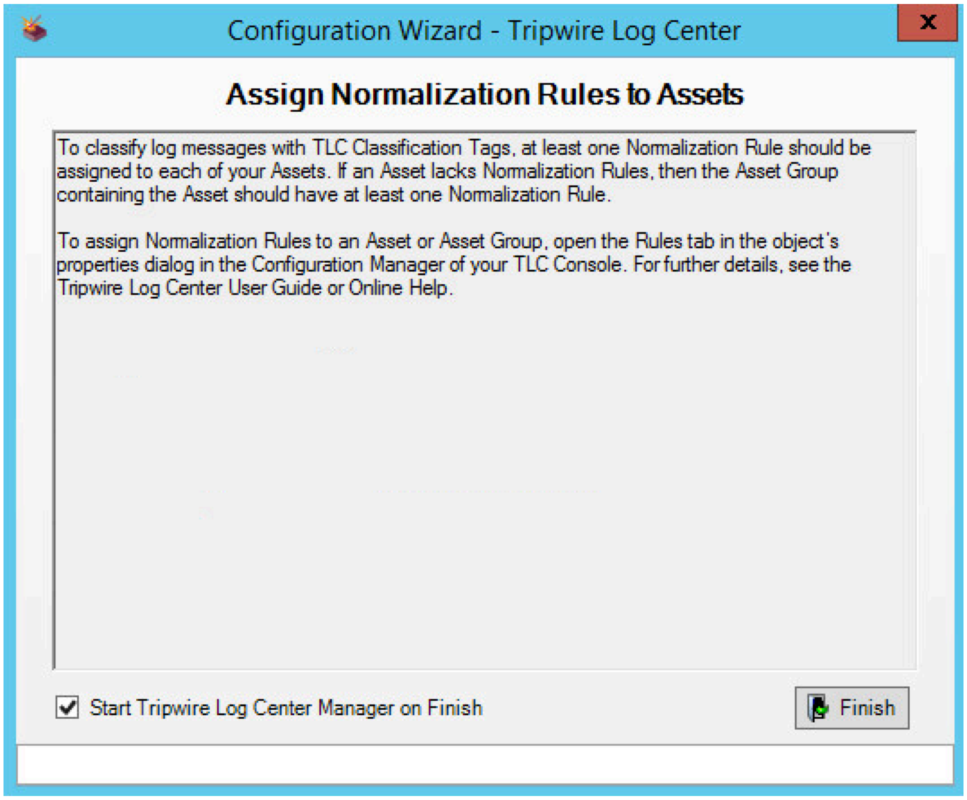


32. Click **Start**.



```
            Tags Import... Completed
Rules                   : Adding
Importing Rule          : Linux Debian
Importing Rule          : Linux Ubuntu
Importing Rule          : Microsoft Exchange
Importing Rule          : Microsoft SQL Server
Importing Rule          : Tripwire Enterprise
Importing Rule          : Tripwire IP360 VnE
Importing Rule          : Windows 10
Correlation Lists       : Adding
Tasks                   : Adding
            Importing Tasks for Event Databases tasks to  database...
            Tasks for Event Databases Import... Completed
            Importing Audit Logger Queries and Reports tasks to ...
            Audit Logger Queries and Reports Import... Completed
Alerts                  : Adding
Correlation Rules       : Adding
Adding Correlation Rules.
Configuration Files: Generating
Validating Assets
Configuration Wizard Complete
```

33. Click **Next** when the configuration finishes.



Assign Normalization Rules to Assets

To classify log messages with TLC Classification Tags, at least one Normalization Rule should be assigned to each of your Assets. If an Asset lacks Normalization Rules, then the Asset Group containing the Asset should have at least one Normalization Rule.

To assign Normalization Rules to an Asset or Asset Group, open the Rules tab in the object's properties dialog in the Configuration Manager of your TLC Console. For further details, see the Tripwire Log Center User Guide or Online Help.

☑ Start Tripwire Log Center Manager on Finish

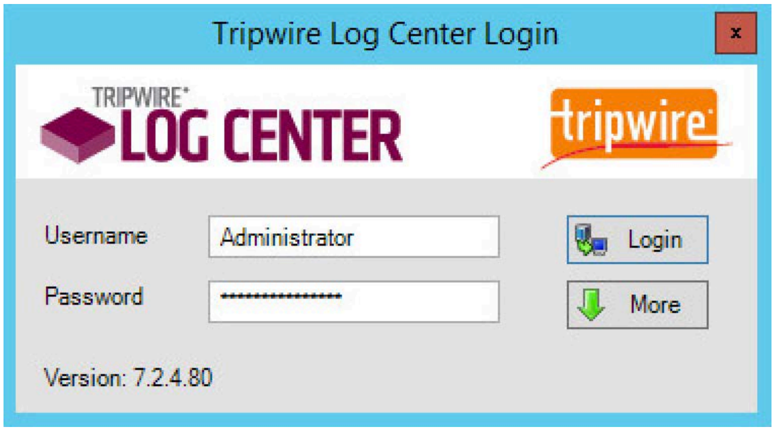
34. Observe the successful installation and click **Finish**.

2.10.5 Install Tripwire Log Center Console

See chapter 4 of Tripwire Log Center 7.2.4 installation guide for instructions on how to install **Tripwire Log Center Console**. Use the **Tripwire Log Center Console installer**. This can be done on any system, even the system running.

2.10.6 Integrate Tripwire Log Center Tripwire Log Center with Tripwire Enterprise

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



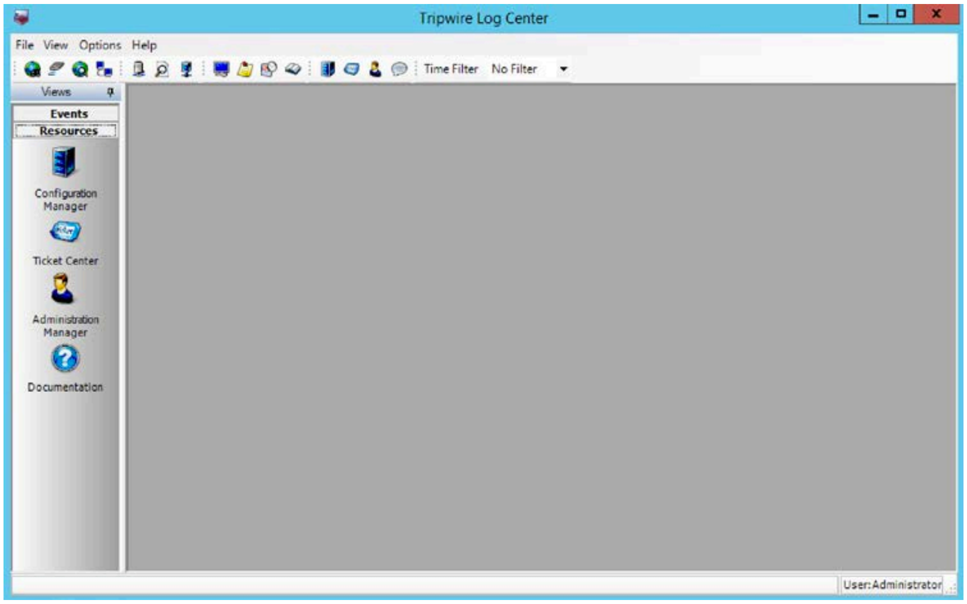
Tripwire Log Center Login

Username: Administrator

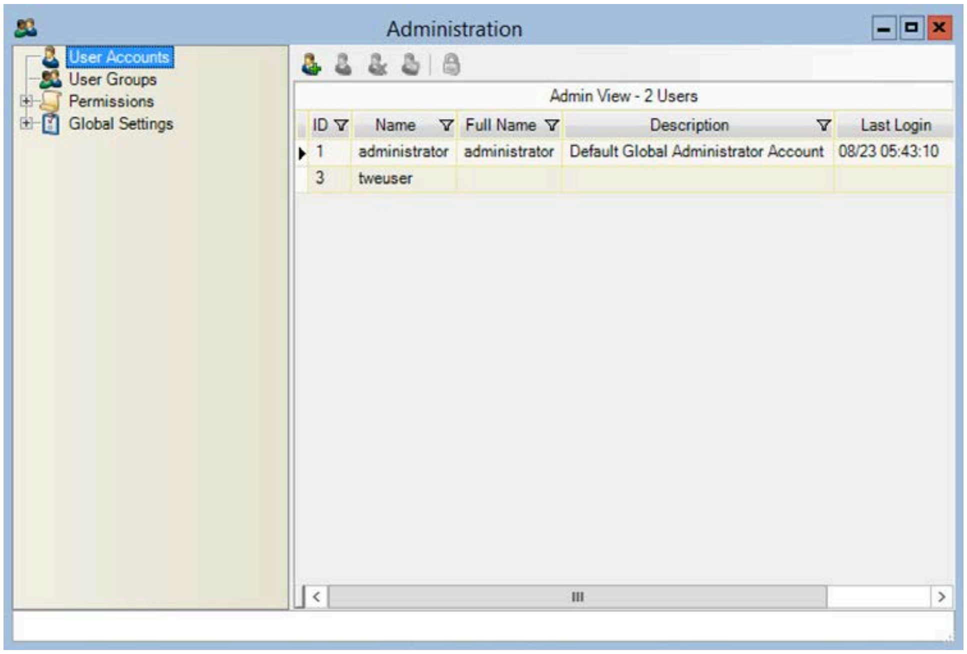
Password: ****************

Version: 7.2.4.80

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



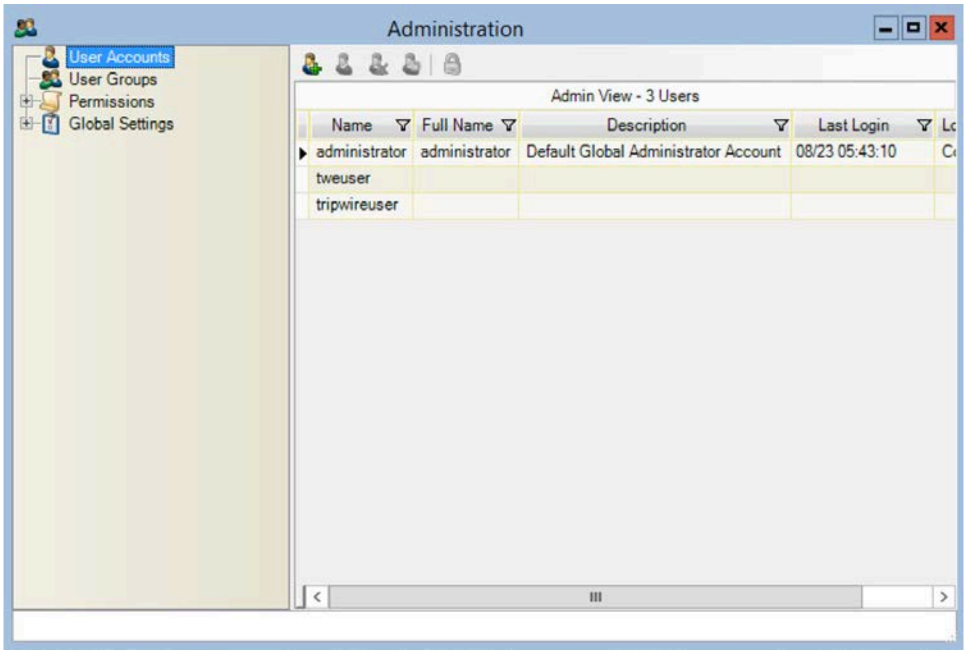
3. On the side bar, click **User Accounts**.



Admin View - 2 Users

ID	Name	Full Name	Description	Last Login
1	administrator	administrator	Default Global Administrator Account	08/23 05:43:10
3	tweuser			

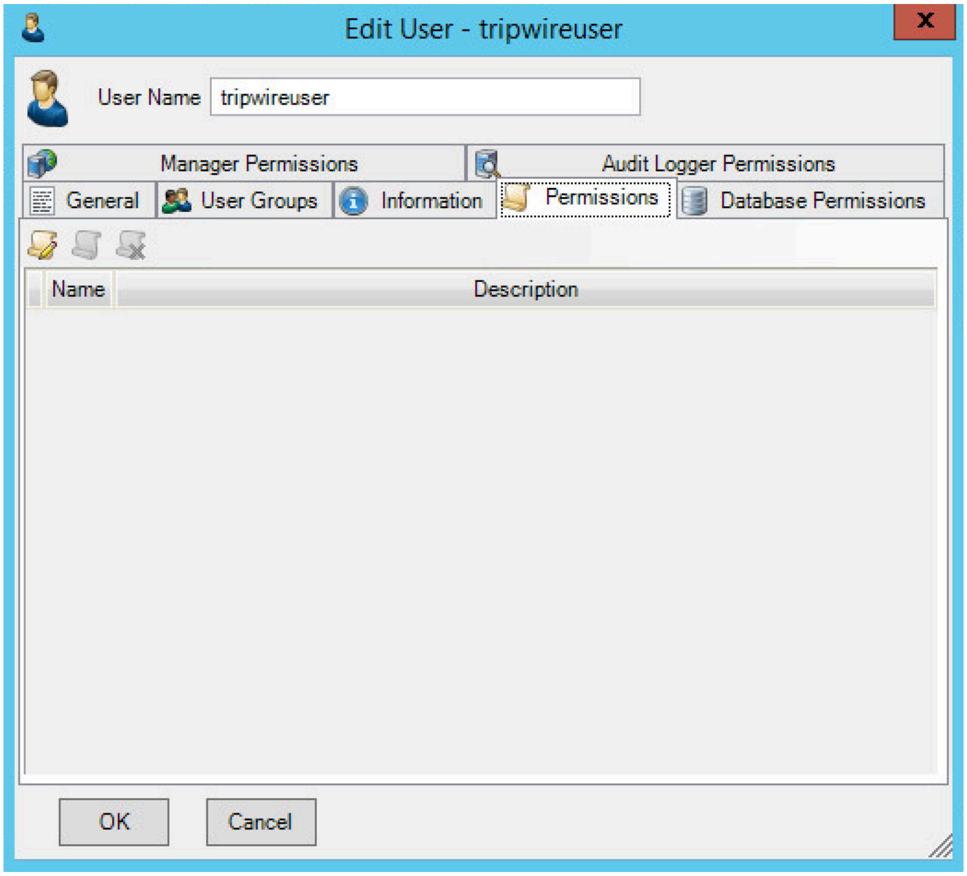
4. Click the **Add** button.
5. Enter the details of the user.



Admin View - 3 Users

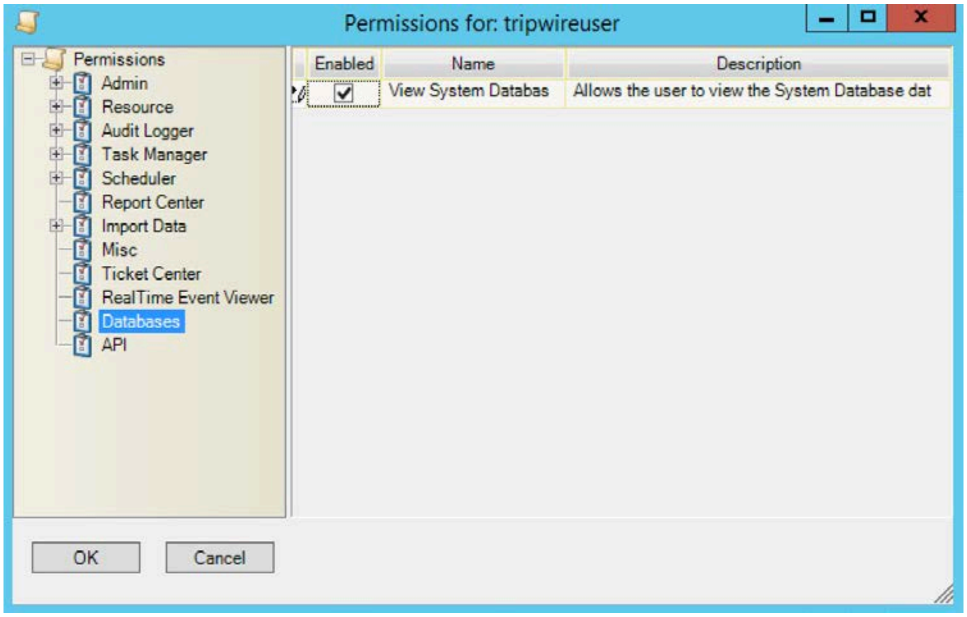
Name	Full Name	Description	Last Login	Lo
administrator	administrator	Default Global Administrator Account	08/23 05:43:10	C
tweuser				
tripwireuser				

6. Double click the user account.
7. Select the **Permissions** tab.



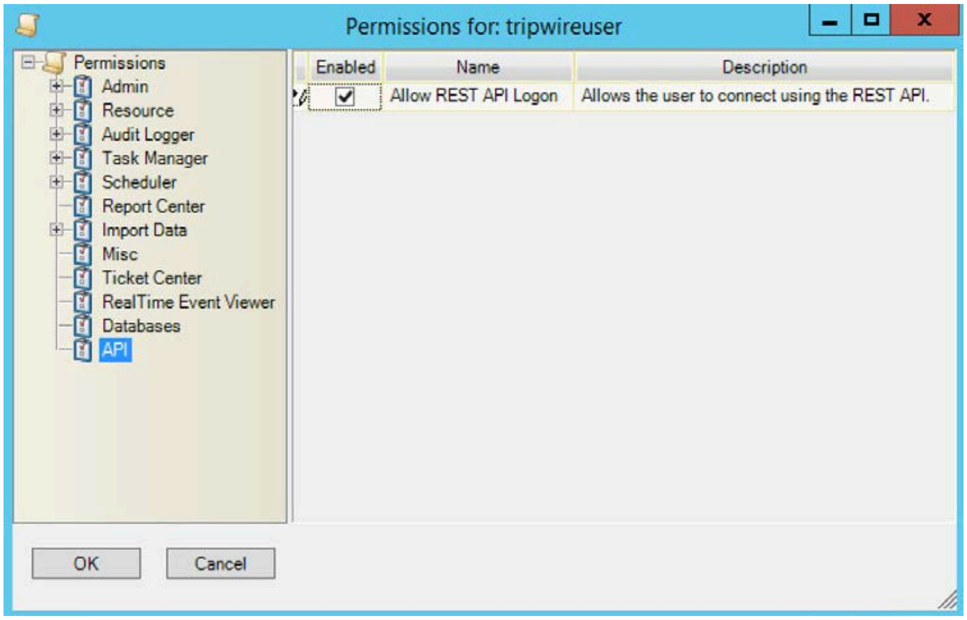
User Name: tripwireuser

8. Click **Change User Permissions**.
9. Select **Databases** and check the box.



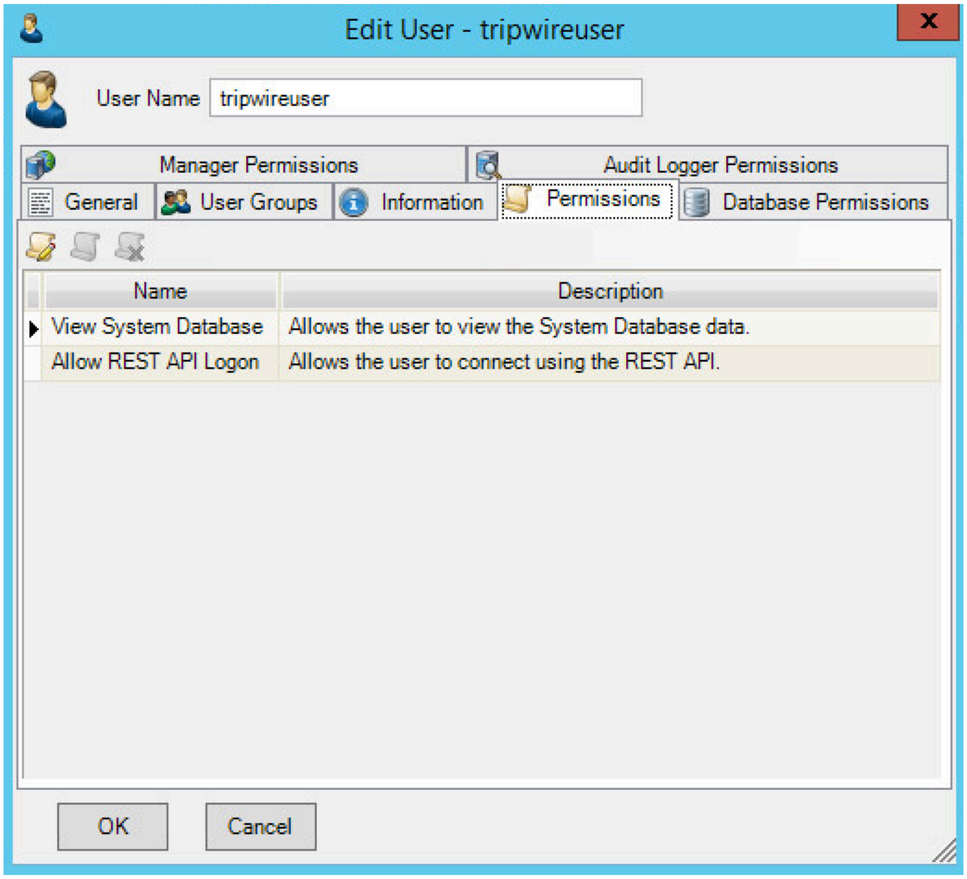
Enabled	Name	Description
☑	View System Databas	Allows the user to view the System Database dat

10. Select **API** and check the box.



Enabled	Name	Description
☑	Allow REST API Logon	Allows the user to connect using the REST API.

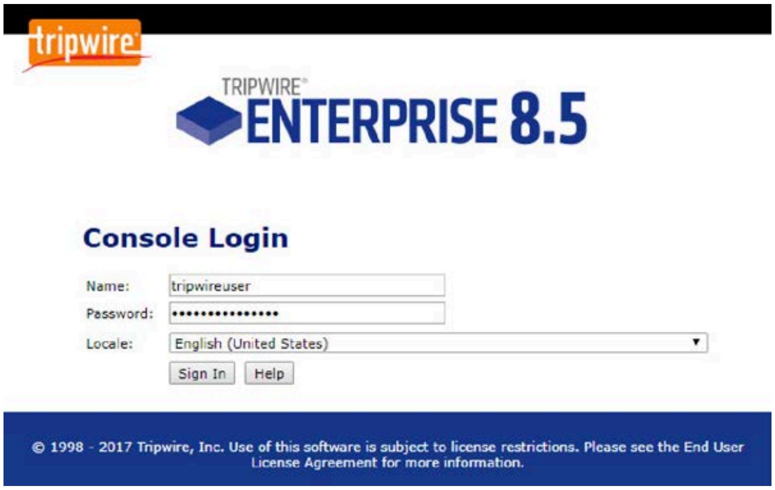
11. Click **OK**.
12. Click **OK**.
13. Click **OK**.



User Name: tripwireuser

Name	Description
View System Database	Allows the user to view the System Database data.
Allow REST API Logon	Allows the user to connect using the REST API.

14. Open **Tripwire Enterprise** by going to https://tripwire.com/
15. Log in to the **Tripwire Enterprise Console**.

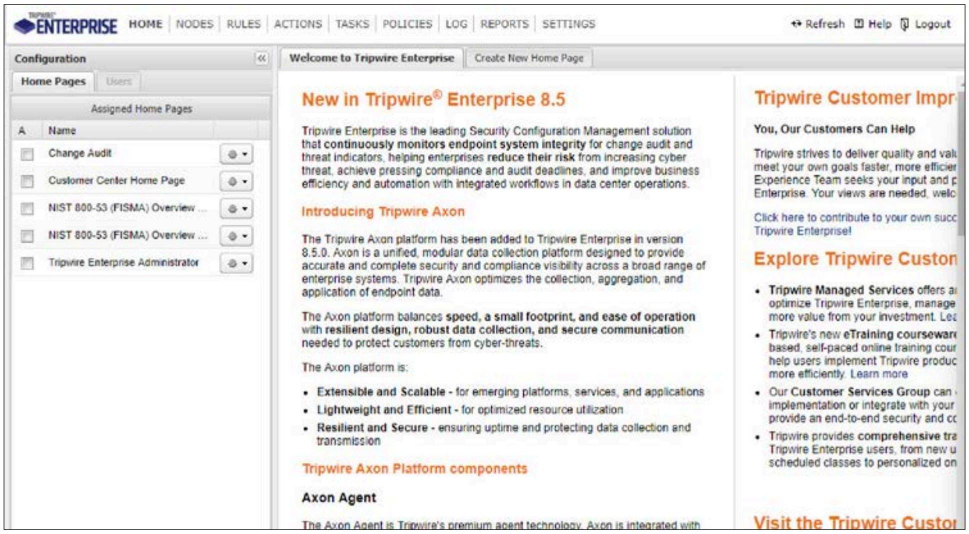


Console Login

Name: tripwireuser
Password: •••••••••••••••
Locale: English (United States)

© 1998 - 2017 Tripwire, Inc. Use of this software is subject to license restrictions. Please see the End User License Agreement for more information.

16. Click **Settings**.



Assigned Home Pages

A	Name
☐	Change Audit
☐	Customer Center Home Page
☐	NIST 800-53 (FISMA) Overview ...
☐	NIST 800-53 (FISMA) Overview ...
☐	Tripwire Enterprise Administrator

New in Tripwire® Enterprise 8.5

Tripwire Enterprise is the leading Security Configuration Management solution that **continuously monitors endpoint system integrity** for change audit and threat indicators, helping enterprises **reduce their risk** from increasing cyber threat, achieve pressing compliance and audit deadlines, and improve business efficiency and automation with integrated workflows in data center operations.

Introducing Tripwire Axon

The Tripwire Axon platform has been added to Tripwire Enterprise in version 8.5.0. Axon is a unified, modular data collection platform designed to provide accurate and complete security and compliance visibility across a broad range of enterprise systems. Tripwire Axon optimizes the collection, aggregation, and application of endpoint data.

The Axon platform balances **speed, a small footprint, and ease of operation** with **resilient design, robust data collection, and secure communication** needed to protect customers from cyber-threats.

The Axon platform is:

- **Extensible and Scalable** - for emerging platforms, services, and applications
- **Lightweight and Efficient** - for optimized resource utilization
- **Resilient and Secure** - ensuring uptime and protecting data collection and transmission

Tripwire Axon Platform components

Axon Agent

The Axon Agent is Tripwire's premium agent technology. Axon is integrated with

Tripwire Customer Impr

You, Our Customers Can Help

Tripwire strives to deliver quality and valu meet your own goals faster, more efficien Experience Team seeks your input and p Enterprise. Your views are needed, welc

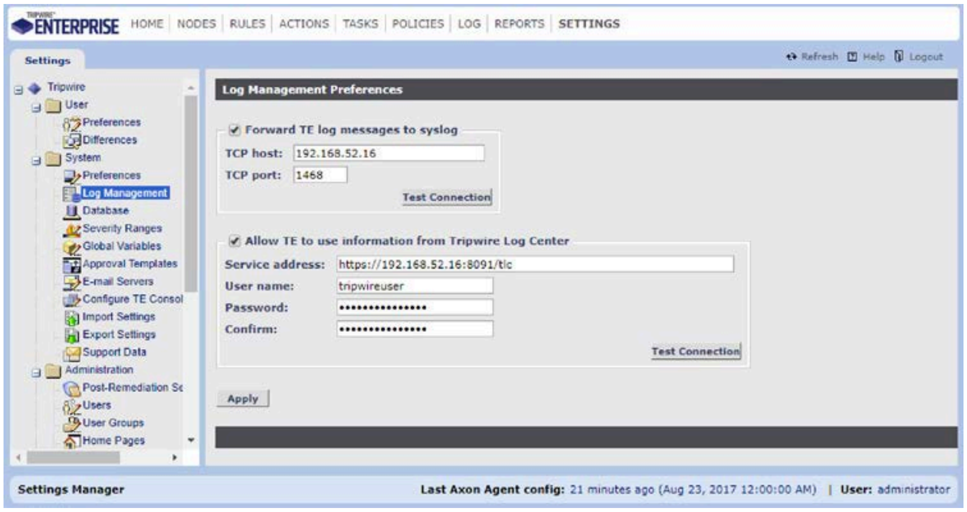
Click here to contribute to your own succ Tripwire Enterprise!

Explore Tripwire Custon

- **Tripwire Managed Services** offers a optimize Tripwire Enterprise, manage more value from your investment. Lea
- Tripwire's new **eTraining courseware** based, self-paced online training cour help users implement Tripwire produc more efficiently. Learn more
- Our **Customer Services Group** can implementation or integrate with your provide an end-to-end security and cc
- Tripwire provides **comprehensive tra** Tripwire Enterprise users, from new u scheduled classes to personalized on

Visit the Tripwire Custor

17. Go to **System > Log Management.**
18. Check the box next to **Forward TE log messages to syslog**.
19. Enter the **IP address** and **port** of the Tripwire Log Center server. The default port is 1468.
20. Check the box next to **Allow TE to use information from Tripwire Log Center**.
21. Enter the **service address** like this: *https://192.168.50.44:8091/tlc*, replacing the IP address with the IP address of the Tripwire Log Center server.
22. Enter the account information for the account created with the **Databases** and **API** permissions.



Log Management Preferences

☑ Forward TE log messages to syslog

TCP host: 192.168.52.16

TCP port: 1468

☑ Allow TE to use information from Tripwire Log Center

Service address: https://192.168.52.16:8091/tlc

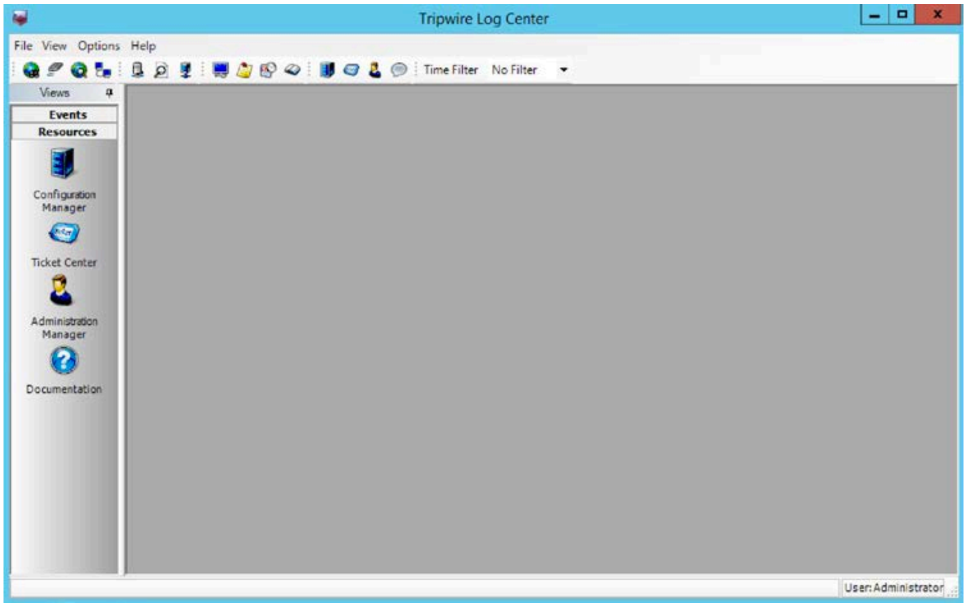
User name: tripwireuser

Password: •••••••••••••••

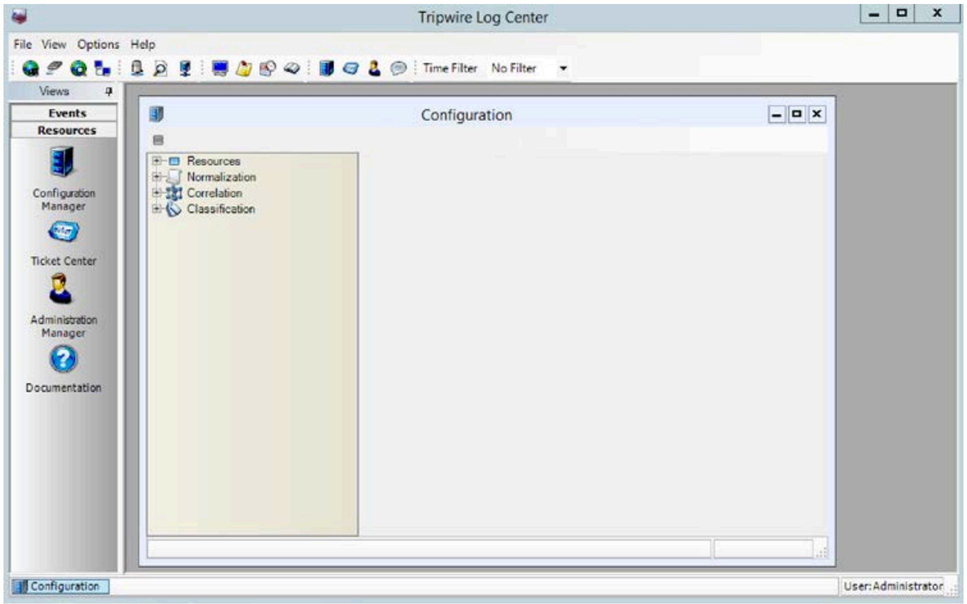
Confirm: •••••••••••••••

Last Axon Agent config: 21 minutes ago (Aug 23, 2017 12:00:00 AM) | **User:** administrator

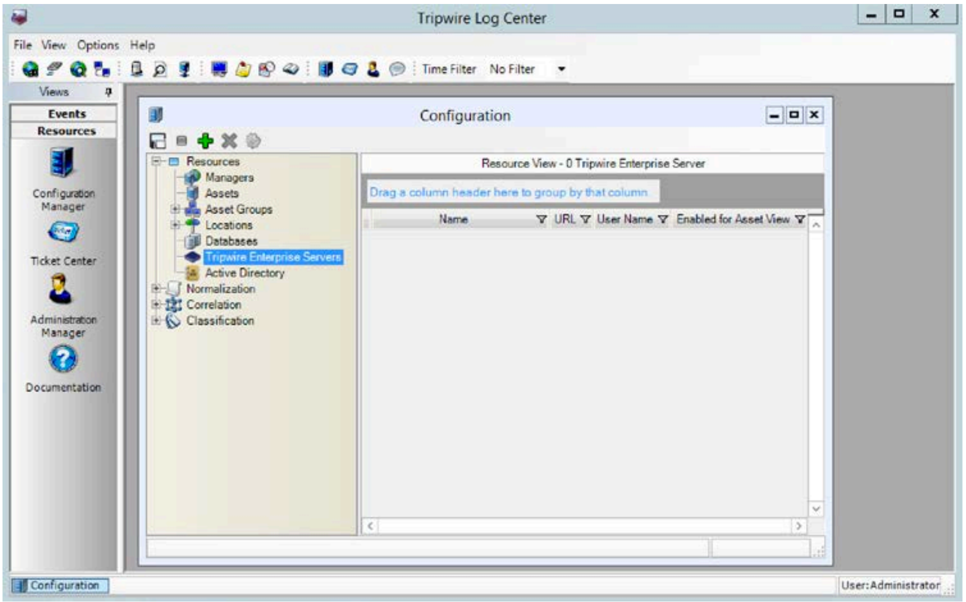
23. Click **Apply**.
24. Click **OK**.
25. Go back to the **Tripwire Log Center Console**.



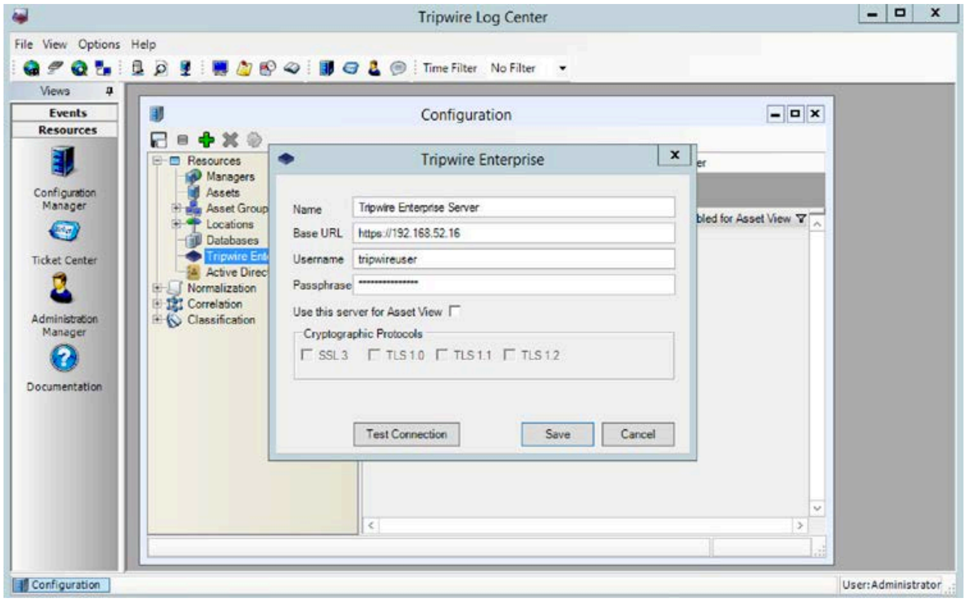
26. Click **Configuration Manager**.



27. Click **Resources > Tripwire Enterprise Servers**.



28. Click **Add**.
29. Enter a **name** for the Tripwire Enterprise server.
30. Enter the **IP address** and **port** for the Tripwire Enterprise server. By default, Tripwire Log Center and Tripwire Enterprise will communicate on port 443. (*https://192.168.50.43*)
31. Enter the name of a user account on the Tripwire Enterprise server. The account must have the following permissions: **create, delete, link, load, update, view.**


Tripwire Enterprise

Name: Tripwire Enterprise Server
Base URL: https://192.168.52.16
Username: tripwireuser
Passphrase: ***************
Use this server for Asset View ☐
Cryptographic Protocols: ☐ SSL 3 ☐ TLS 1.0 ☐ TLS 1.1 ☐ TLS 1.2

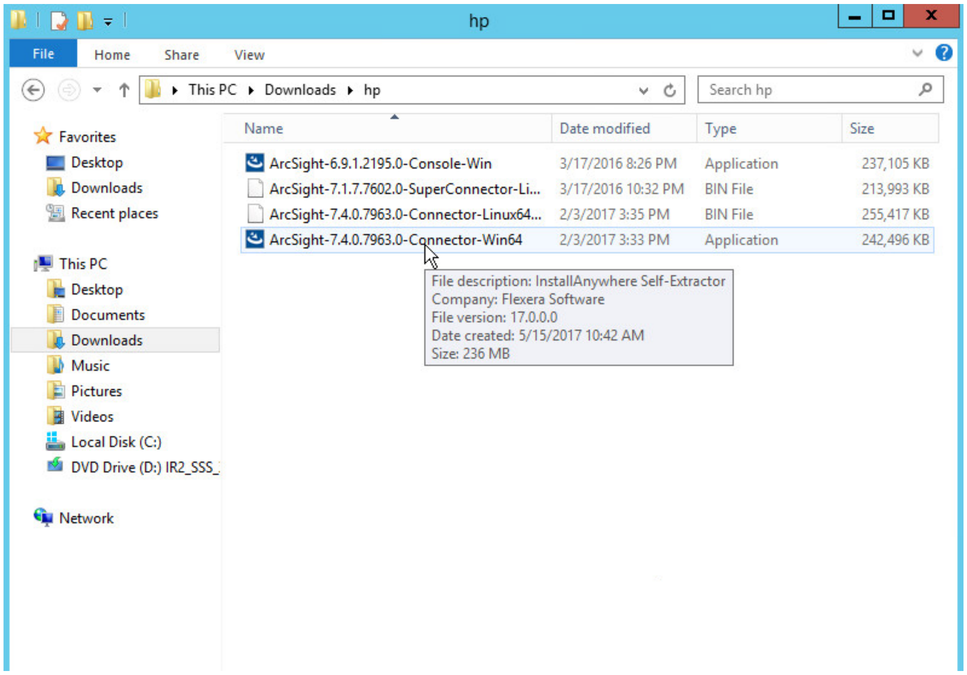
32. Click **Save**.

2.11 Integration: Tripwire Log Center (TLC) and HPE ArcSight ESM

In this section is a process for integrating Tripwire Log Center and HPE ArcSight ESM. This integration assumes the correct implementation of Tripwire and ArcSight as described in earlier sections. The result of this integration is the forwarding of logs generated by Tripwire Enterprise to ArcSight ESM as well as a method for filtering specifically for file change events in ArcSight ESM.

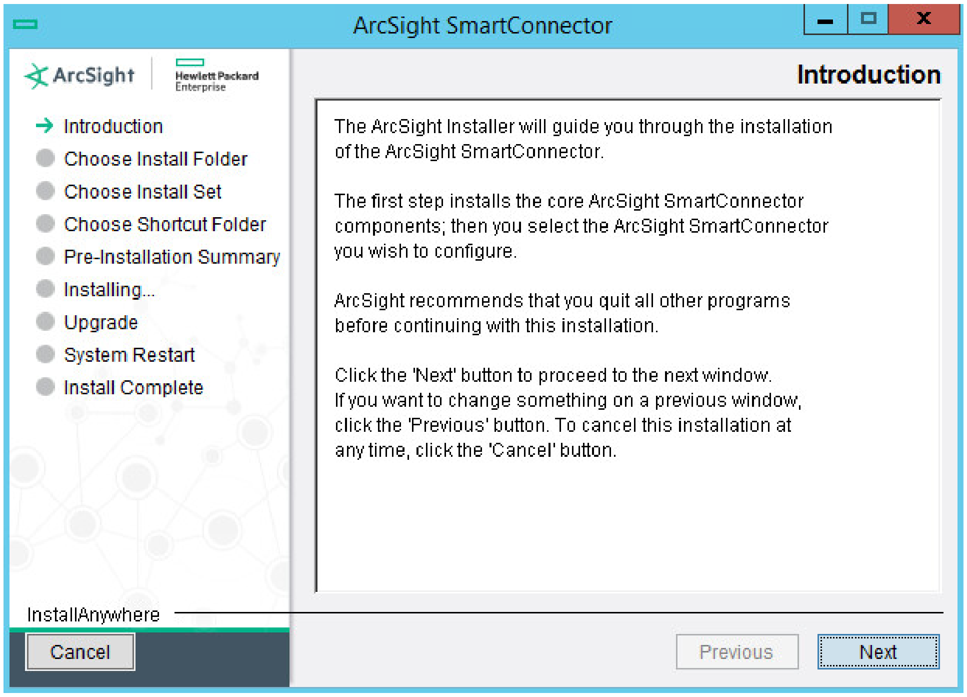
2.11.1 Integrating TLC and ESM

1. Run **ArcSight-7.4.0.7963.0-Connector-Win64** on any Windows server (*except* for the server running the Tripwire Log Center).



Name	Date modified	Type	Size
ArcSight-6.9.1.2195.0-Console-Win	3/17/2016 8:26 PM	Application	237,105 KB
ArcSight-7.1.7.7602.0-SuperConnector-Li...	3/17/2016 10:32 PM	BIN File	213,993 KB
ArcSight-7.4.0.7963.0-Connector-Linux64...	2/3/2017 3:35 PM	BIN File	255,417 KB
ArcSight-7.4.0.7963.0-Connector-Win64	2/3/2017 3:33 PM	Application	242,496 KB

File description: InstallAnywhere Self-Extractor
Company: Flexera Software
File version: 17.0.0.0
Date created: 5/15/2017 10:42 AM
Size: 236 MB



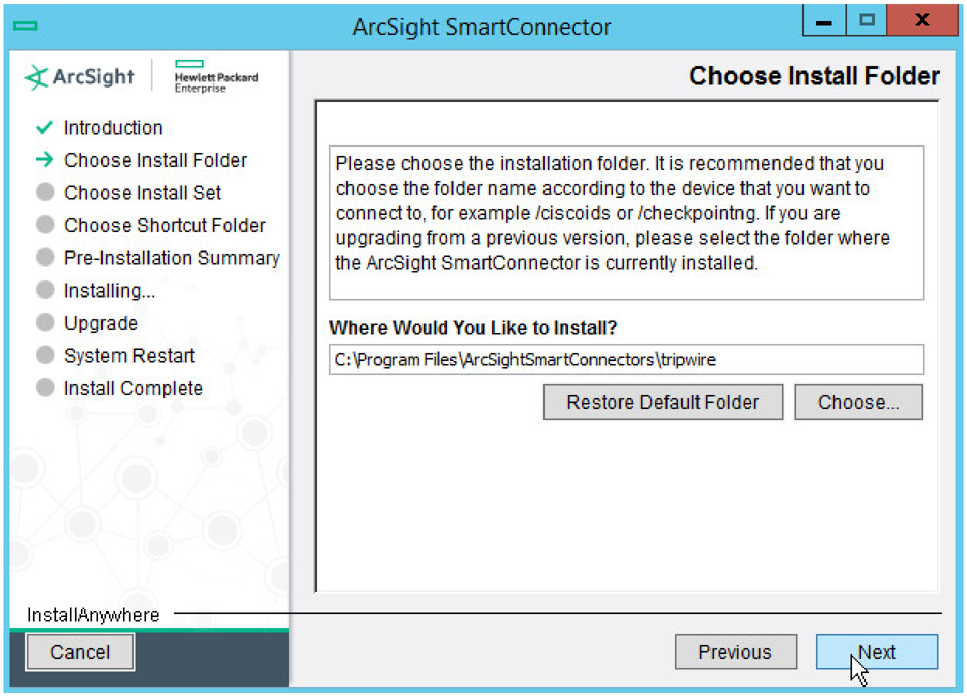
The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector.

The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.

2. Click **Next**.
3. Specify a folder to install the connector.

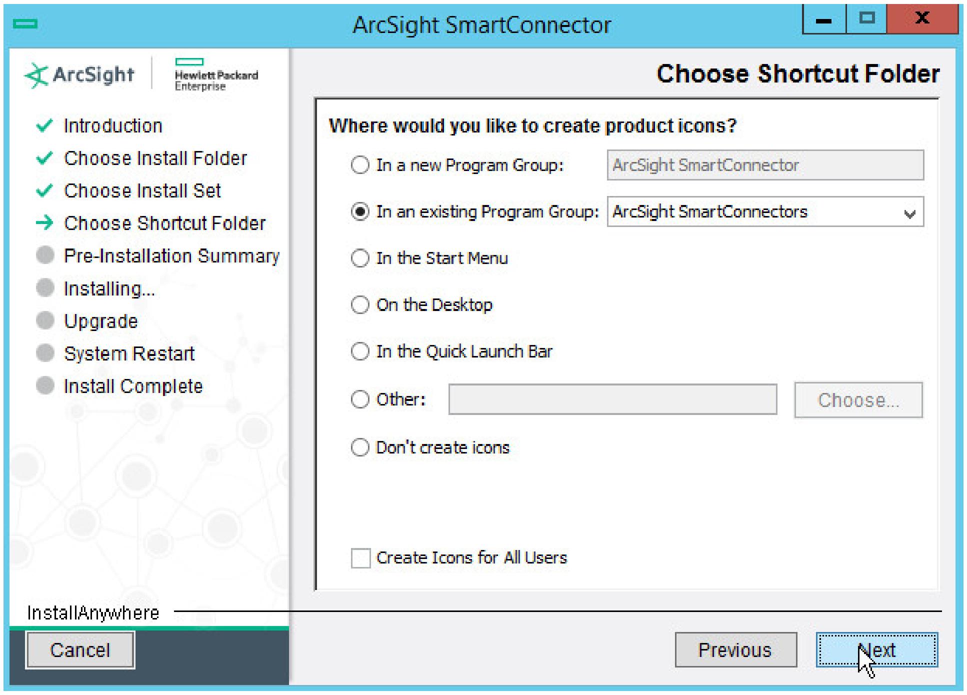


Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.

Where Would You Like to Install?

C:\Program Files\ArcSightSmartConnectors\tripwire

4. Click **Next**.



Choose Shortcut Folder

Where would you like to create product icons?

○ In a new Program Group: ArcSight SmartConnector

● In an existing Program Group: ArcSight SmartConnectors

○ In the Start Menu

○ On the Desktop

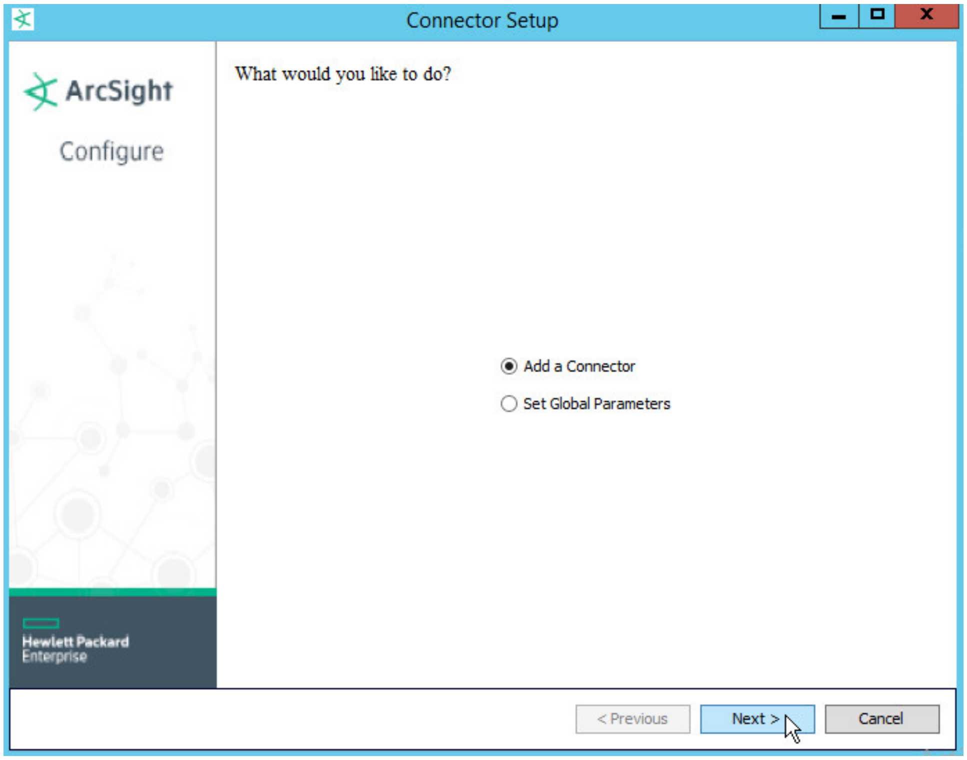
○ In the Quick Launch Bar

○ Other: Choose...

○ Don't create icons

□ Create Icons for All Users

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

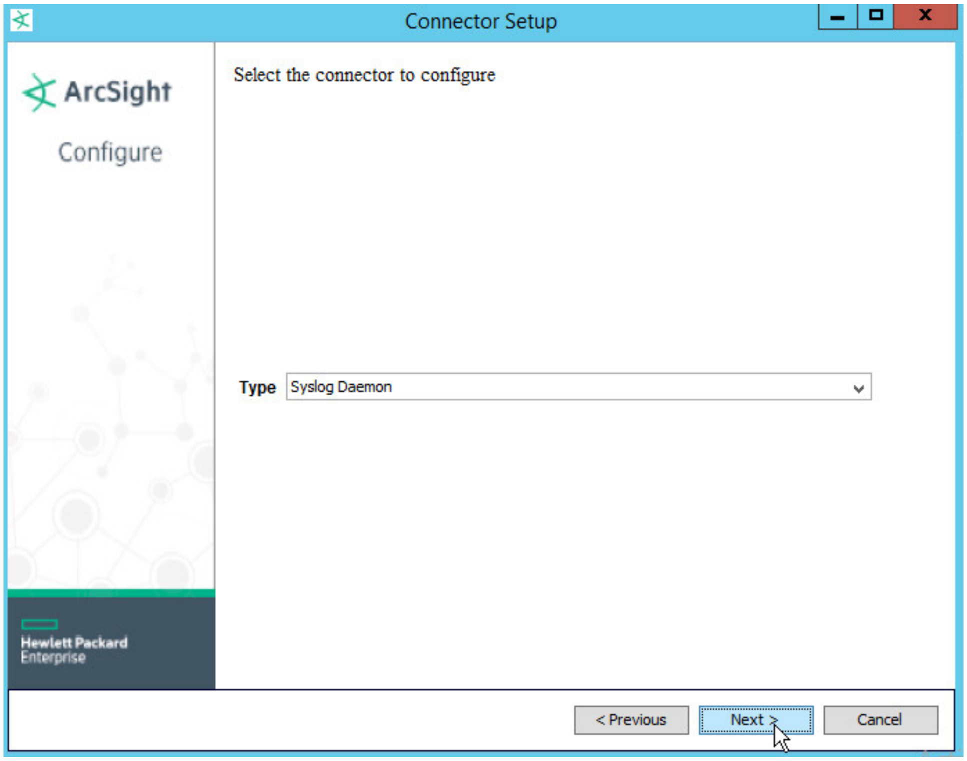


What would you like to do?

● Add a Connector

○ Set Global Parameters

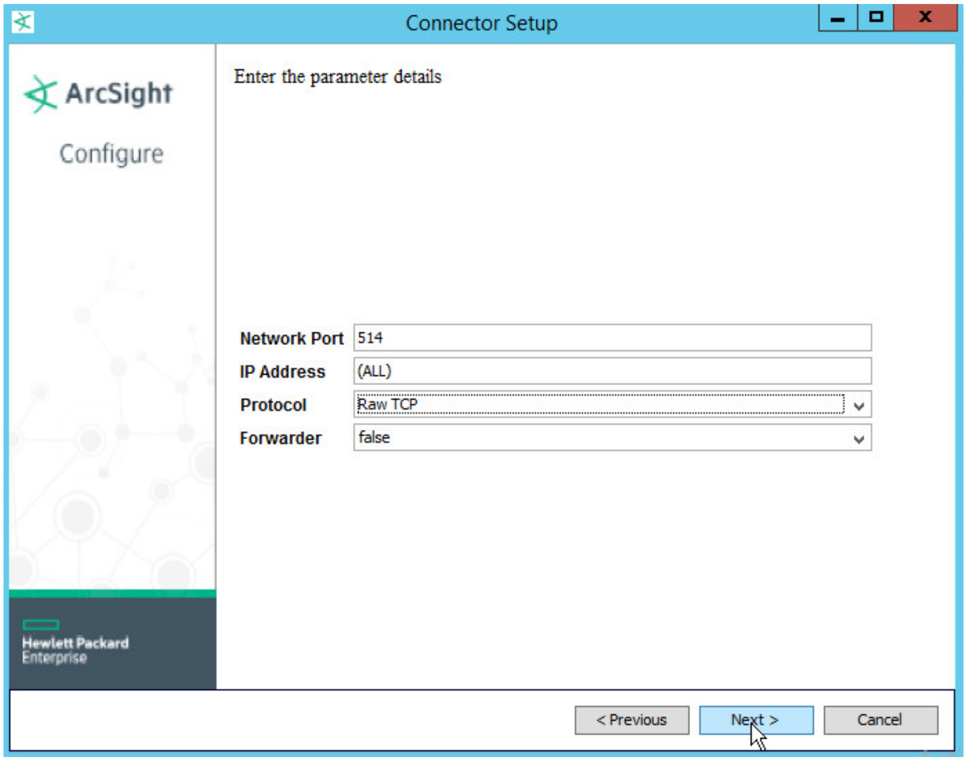
8. Click **Next**.
9. Select **Syslog daemon**.



Select the connector to configure

Type Syslog Daemon

10. Click **Next**.
11. Select a **port** for the daemon to run on.
12. Leave **IP address** as **(ALL)**.
13. Select **Raw TCP** for **Protocol**.
14. Select **False** for **Forwarder**.



Enter the parameter details

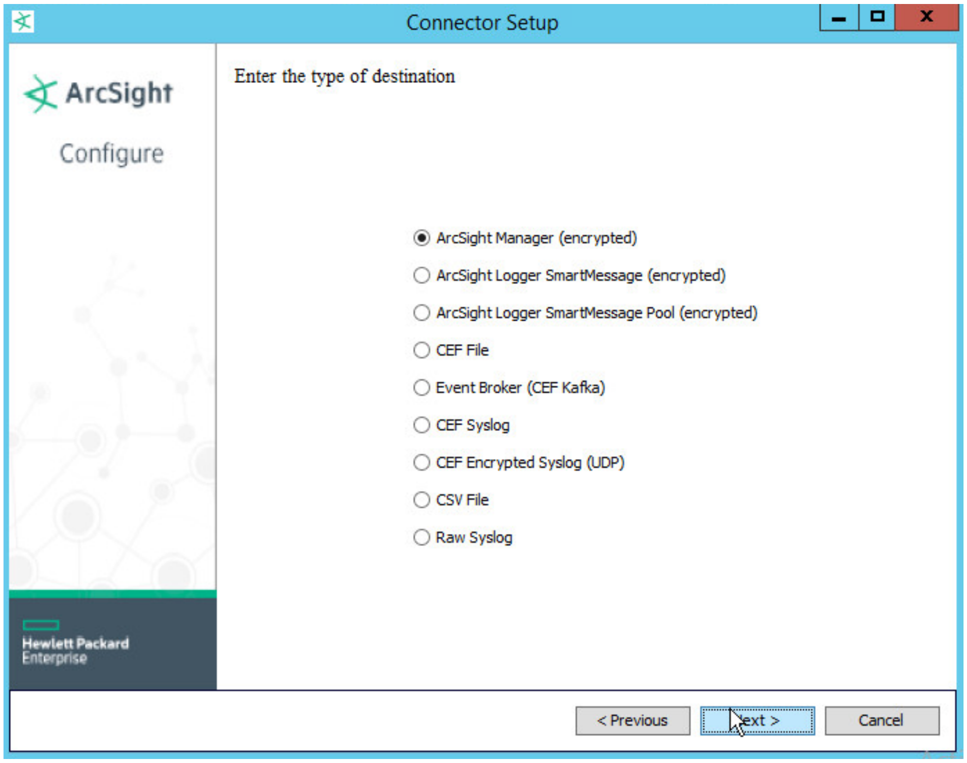
Network Port 514

IP Address (ALL)

Protocol Raw TCP

Forwarder false

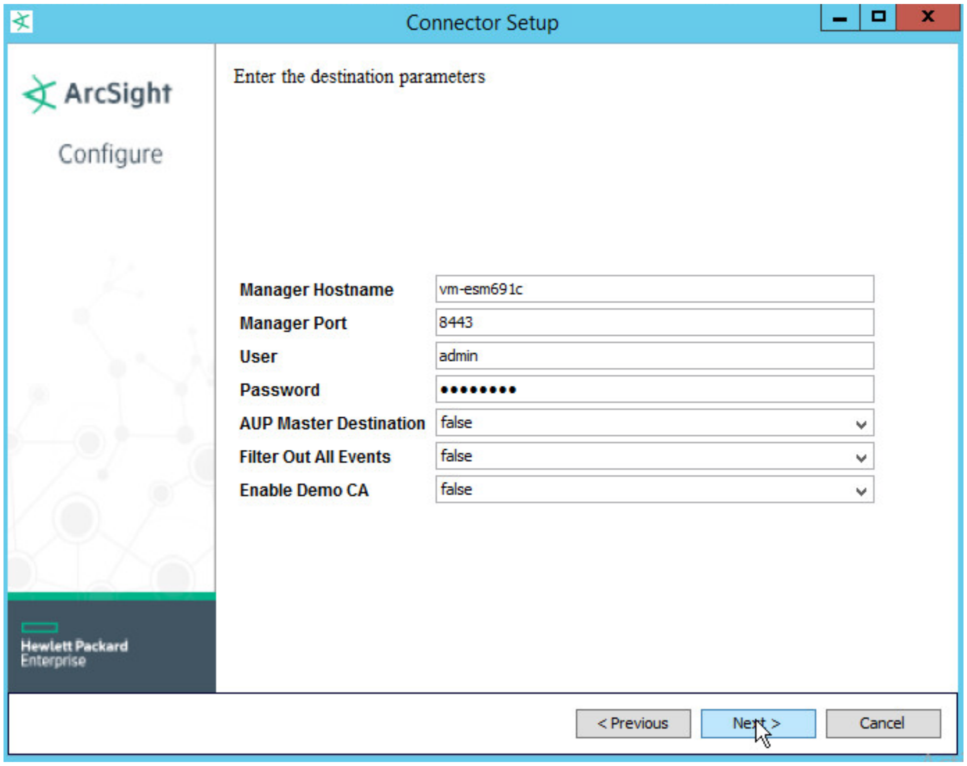
15. Click **Next**.
16. Choose **ArcSight Manager (encrypted)**.



Enter the type of destination

● ArcSight Manager (encrypted)
○ ArcSight Logger SmartMessage (encrypted)
○ ArcSight Logger SmartMessage Pool (encrypted)
○ CEF File
○ Event Broker (CEF Kafka)
○ CEF Syslog
○ CEF Encrypted Syslog (UDP)
○ CSV File
○ Raw Syslog

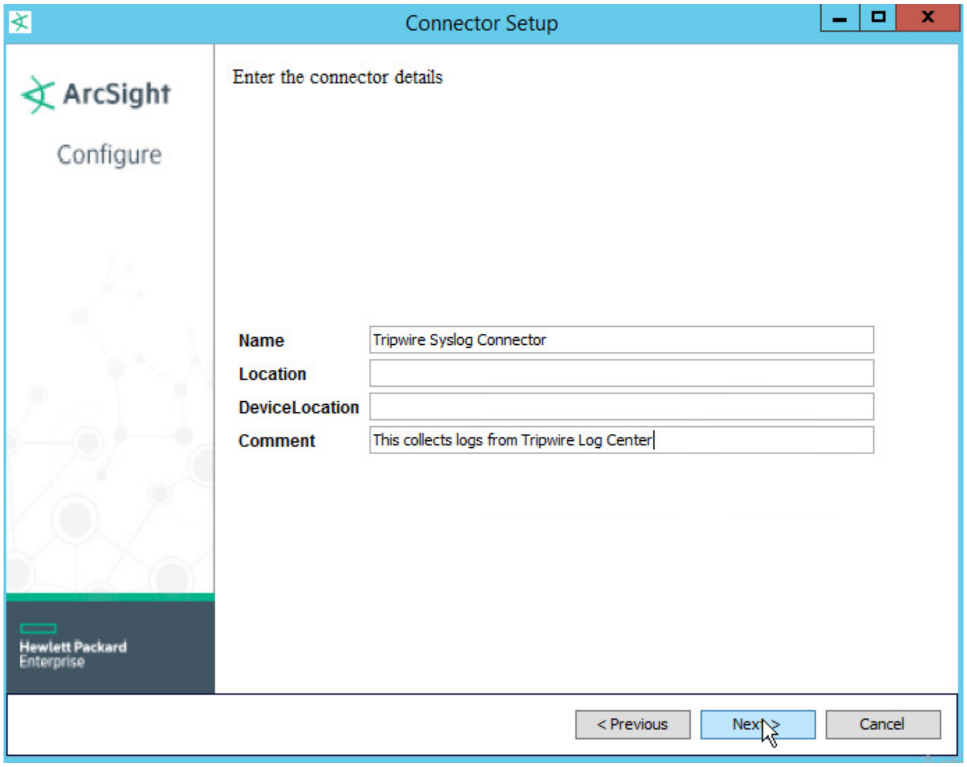
17. Click **Next**.
18. For **Manager Hostname**, put *vm-esm691c* or the hostname of your ESM server.
19. For **Manager Port**, put **8443** (or the port that ESM is running on).
20. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)



Enter the destination parameters

Manager Hostname	vm-esm691c
Manager Port	8443
User	admin
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

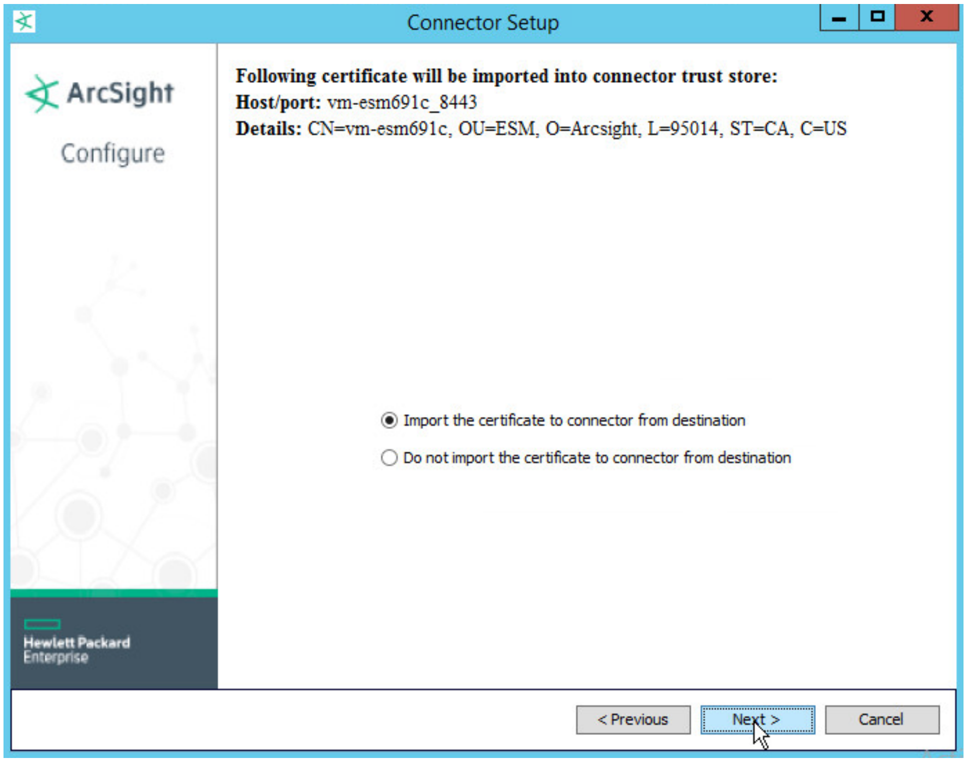
21. Click **Next**.
22. Set identifying details about the system to help identify the connector (include **Name;** the rest is optional).



Enter the connector details

Name	Tripwire Syslog Connector
Location	
DeviceLocation	
Comment	This collects logs from Tripwire Log Center

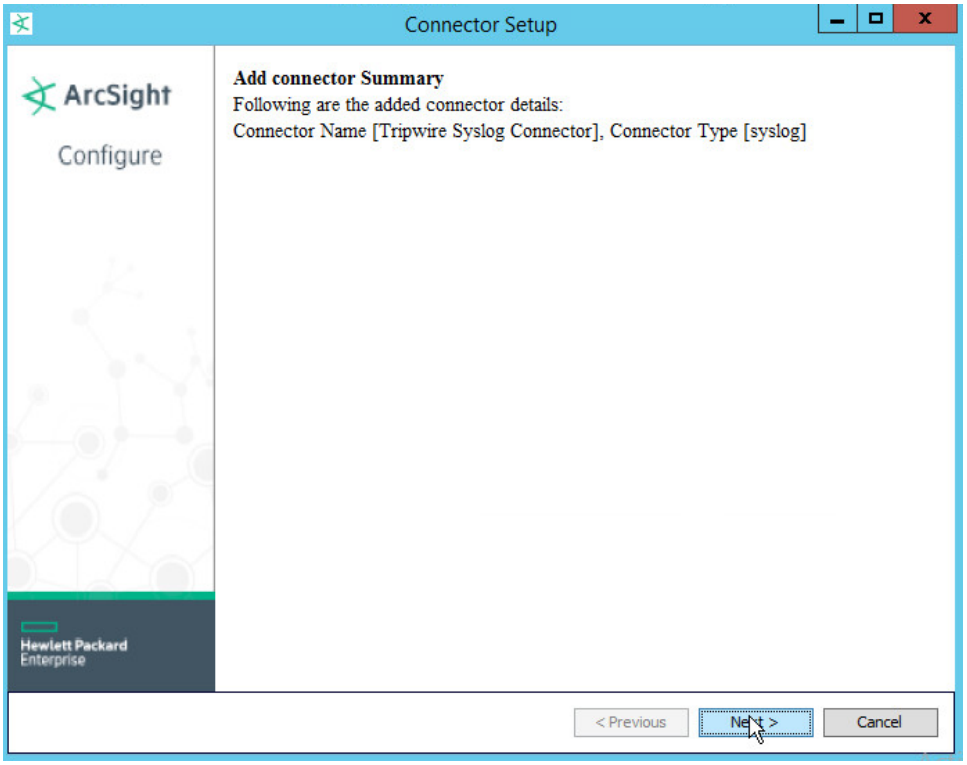
23. Click **Next**.
24. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the VM.



Following certificate will be imported into connector trust store:
Host/port: vm-esm691c_8443
Details: CN=vm-esm691c, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

● Import the certificate to connector from destination
○ Do not import the certificate to connector from destination

25. Click **Next**.

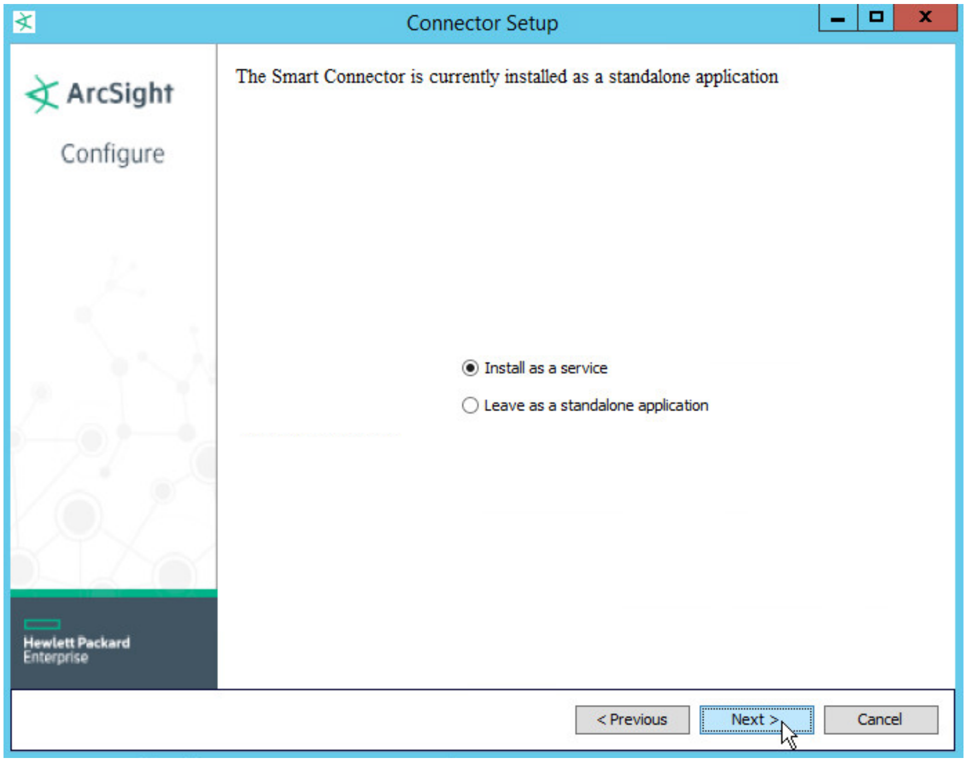


Add connector Summary

Following are the added connector details:

Connector Name [Tripwire Syslog Connector], Connector Type [syslog]

26. Click **Next**.
27. Choose **Install as a service**.

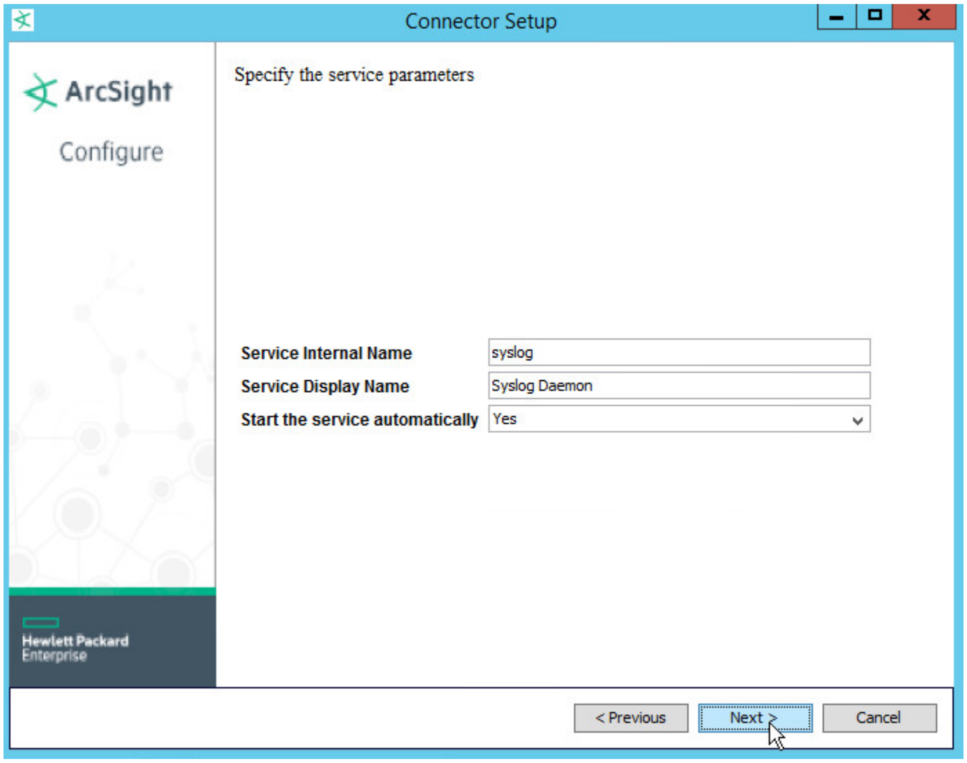


The Smart Connector is currently installed as a standalone application

● Install as a service

○ Leave as a standalone application

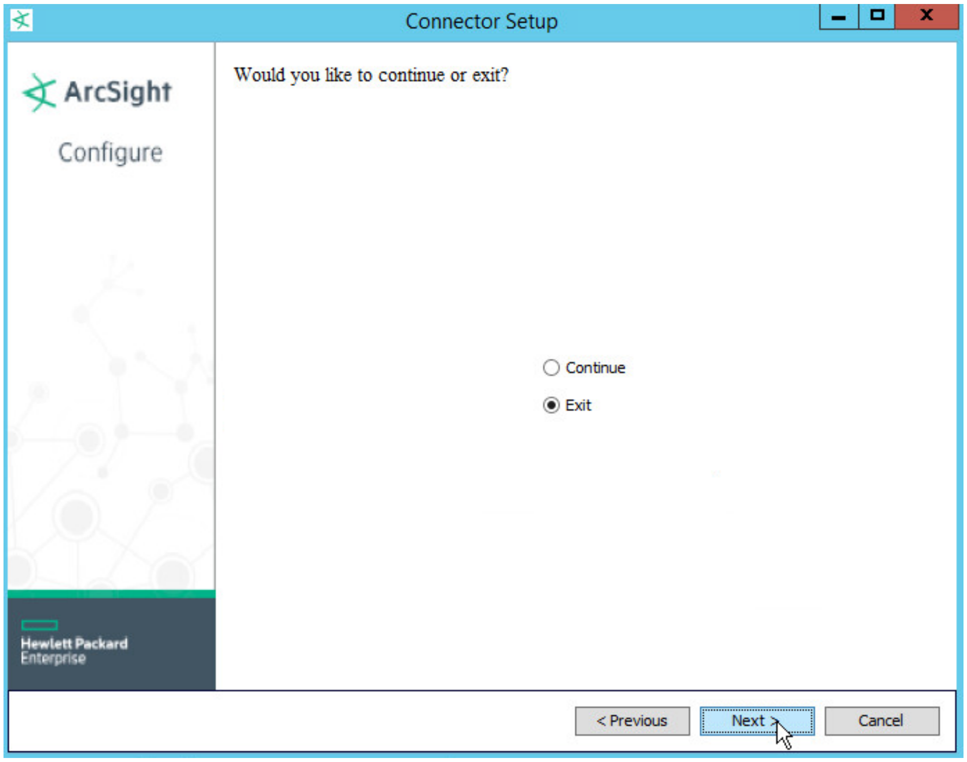
28. Click **Next**.



Specify the service parameters

Service Internal Name	syslog
Service Display Name	Syslog Daemon
Start the service automatically	Yes

29. Click **Next**.
30. Choose **Exit**.

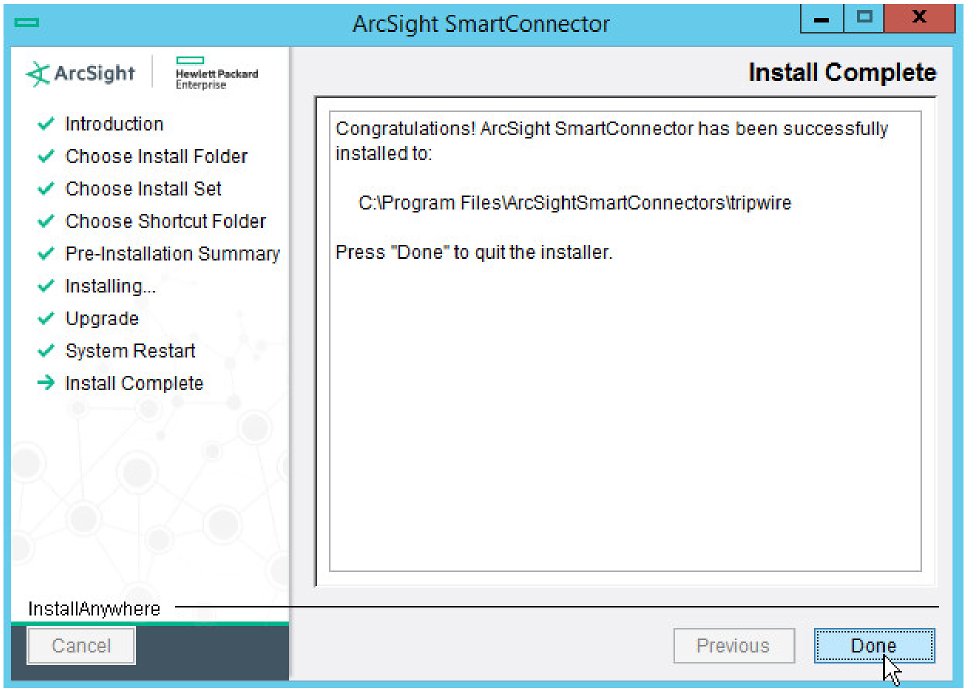


Would you like to continue or exit?

○ Continue

● Exit

31. Click **Next**.



Install Complete

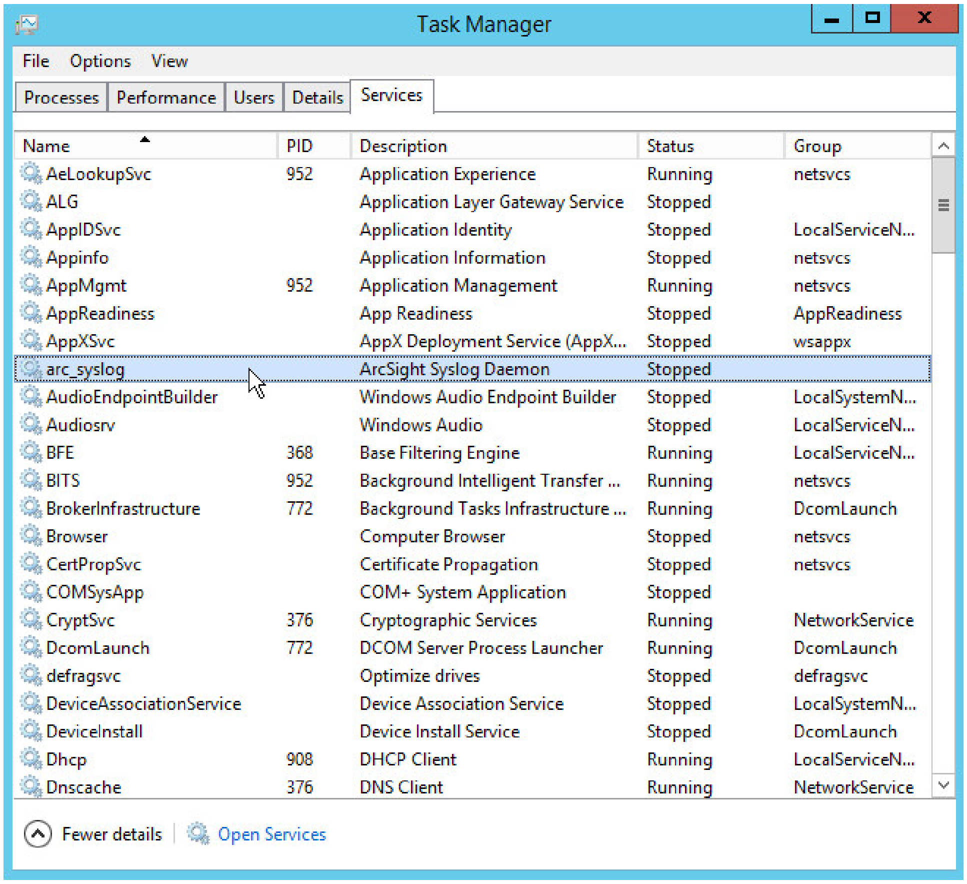
Congratulations! ArcSight SmartConnector has been successfully installed to:

C:\Program Files\ArcSightSmartConnectors\tripwire

Press "Done" to quit the installer.

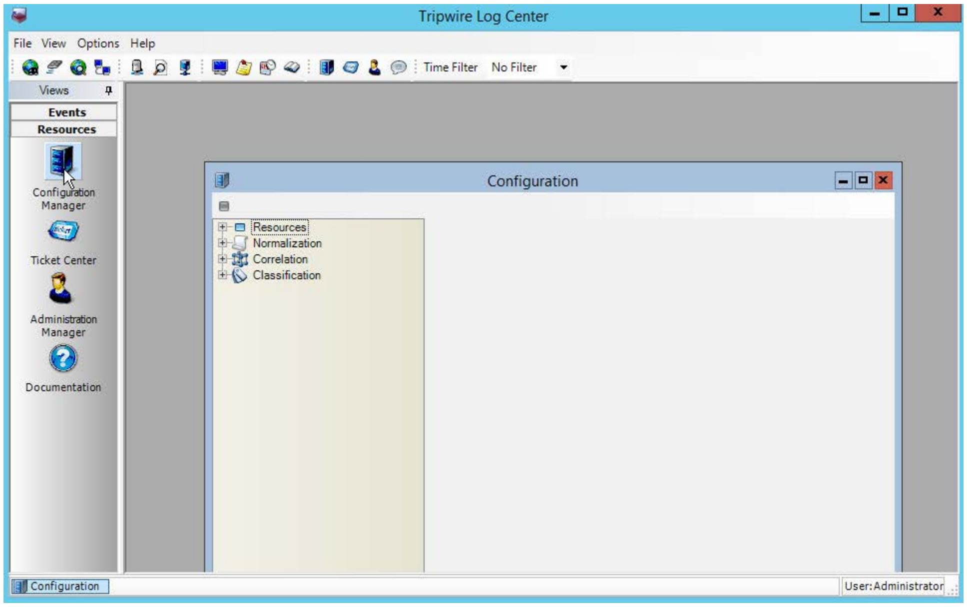
32. Click **Done**.

33. Open **Task Manager**.
34. Click **More Details**.
35. Go to the **Services** tab.
36. Find the service just created for ArcSight and right click it.

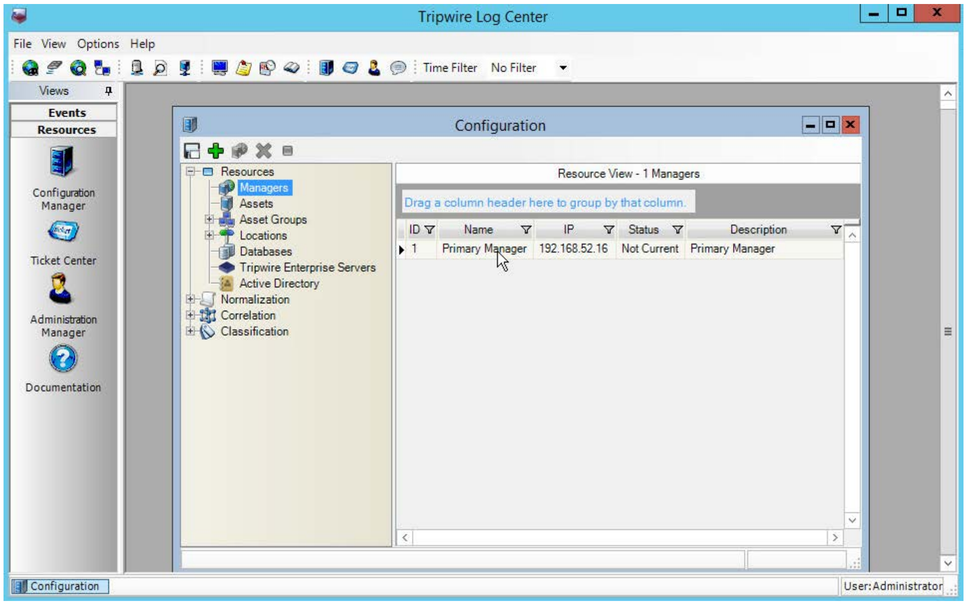


Name	PID	Description	Status	Group
AeLookupSvc	952	Application Experience	Running	netsvcs
ALG		Application Layer Gateway Service	Stopped	
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo		Application Information	Stopped	netsvcs
AppMgmt	952	Application Management	Running	netsvcs
AppReadiness		App Readiness	Stopped	AppReadiness
AppXSvc		AppX Deployment Service (AppX...	Stopped	wsappx
arc_syslog		ArcSight Syslog Daemon	Stopped	
AudioEndpointBuilder		Windows Audio Endpoint Builder	Stopped	LocalSystemN...
Audiosrv		Windows Audio	Stopped	LocalServiceN...
BFE	368	Base Filtering Engine	Running	LocalServiceN...
BITS	952	Background Intelligent Transfer ...	Running	netsvcs
BrokerInfrastructure	772	Background Tasks Infrastructure ...	Running	DcomLaunch
Browser		Computer Browser	Stopped	netsvcs
CertPropSvc		Certificate Propagation	Stopped	netsvcs
COMSysApp		COM+ System Application	Stopped	
CryptSvc	376	Cryptographic Services	Running	NetworkService
DcomLaunch	772	DCOM Server Process Launcher	Running	DcomLaunch
defragsvc		Optimize drives	Stopped	defragsvc
DeviceAssociationService		Device Association Service	Stopped	LocalSystemN...
DeviceInstall		Device Install Service	Stopped	DcomLaunch
Dhcp	908	DHCP Client	Running	LocalServiceN...
Dnscache	376	DNS Client	Running	NetworkService

37. Choose **Start**.
38. Open the **Tripwire Log Center Console**.

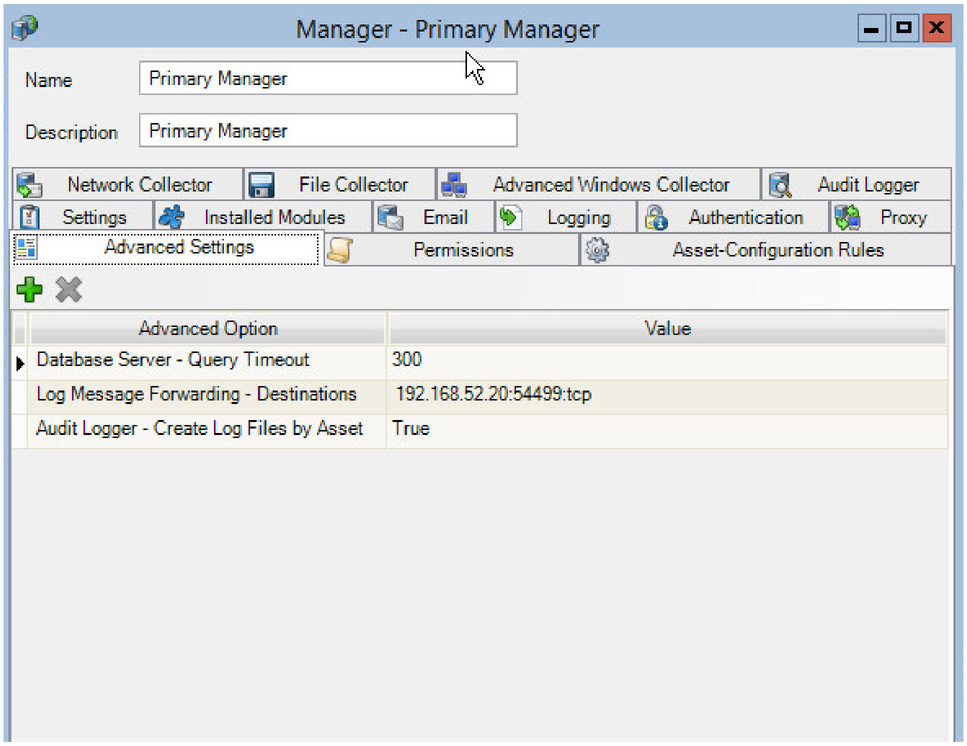


39. Go to the **Configuration Manager**.
40. Select **Resources > Managers**.



ID	Name	IP	Status	Description
1	Primary Manager	192.168.52.16	Not Current	Primary Manager

41. Double click the **Primary Manager** listed.



Name: Primary Manager

Description: Primary Manager

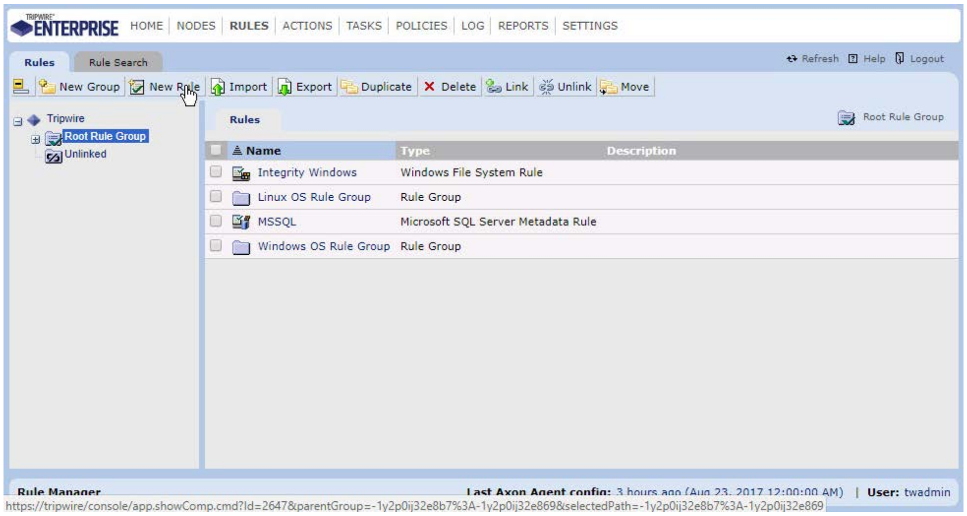
Advanced Option	Value
Database Server - Query Timeout	300
Log Message Forwarding - Destinations	192.168.52.20:54499:tcp
Audit Logger - Create Log Files by Asset	True

42. Click the **Advanced Settings** tab.
43. Click the **+Add** button. This should add a row to the table.
44. In the **Advanced Option** box, select **Log Message Forwarding - Destinations**.
45. In the **Value** box next to it, type **<ip_address>:<port>:tcp**, with the **IP Address** and **port** of the syslog daemon just created.

2.11.2 Configuring Tripwire Enterprise and HPE ArcSight ESM to Detect and Report File Integrity Events

2.11.2.1 Creating a Rule for Which Files to Monitor Across Your Enterprise

1. Log into **Tripwire Enterprise** by going to *https://tripwire* and entering the user name and password.
2. Click the **Rules** link.

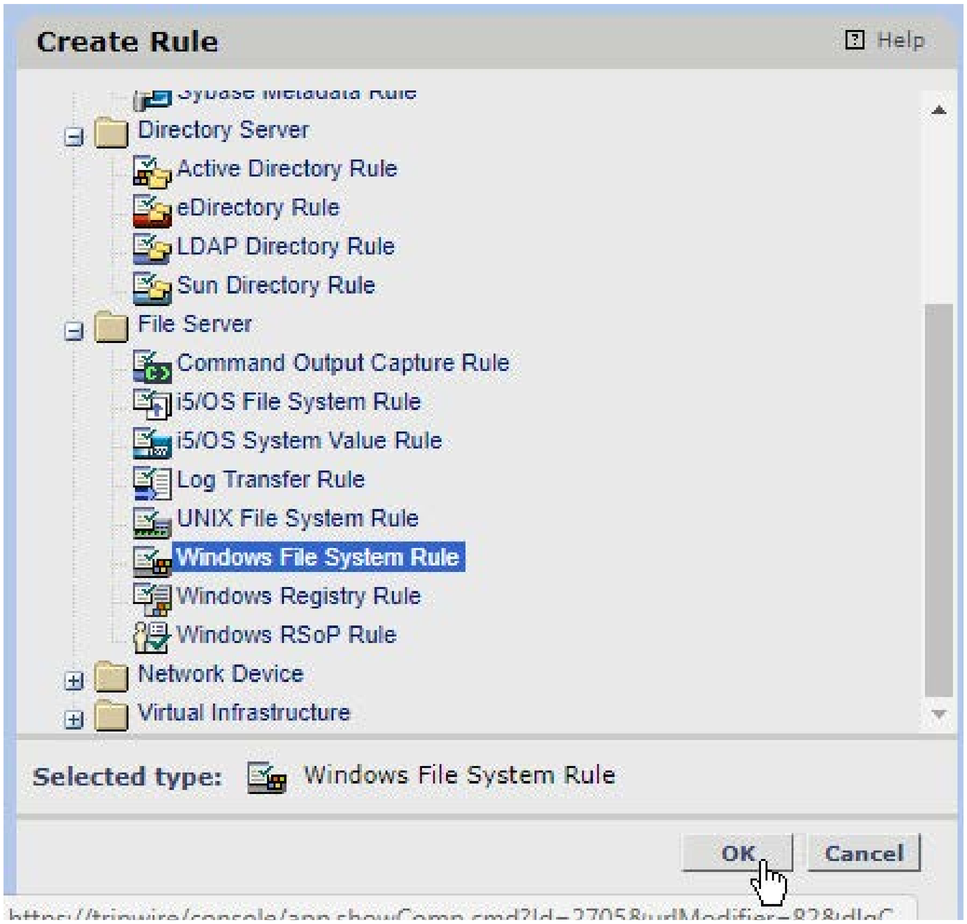


Name	Type	Description
Integrity Windows	Windows File System Rule	
Linux OS Rule Group	Rule Group	
MSSQL	Microsoft SQL Server Metadata Rule	
Windows OS Rule Group	Rule Group	

Rule Manager Last Axon Agent config: 3 hours ago (Aug 23, 2017 12:00:00 AM) | User: twadmin

https://tripwire/console/app.showComp.cmd?Id=2647&parentGroup=-1y2p0ij32e8b7%3A-1y2p0ij32e869&selectedPath=-1y2p0ij32e8b7%3A-1y2p0ij32e869

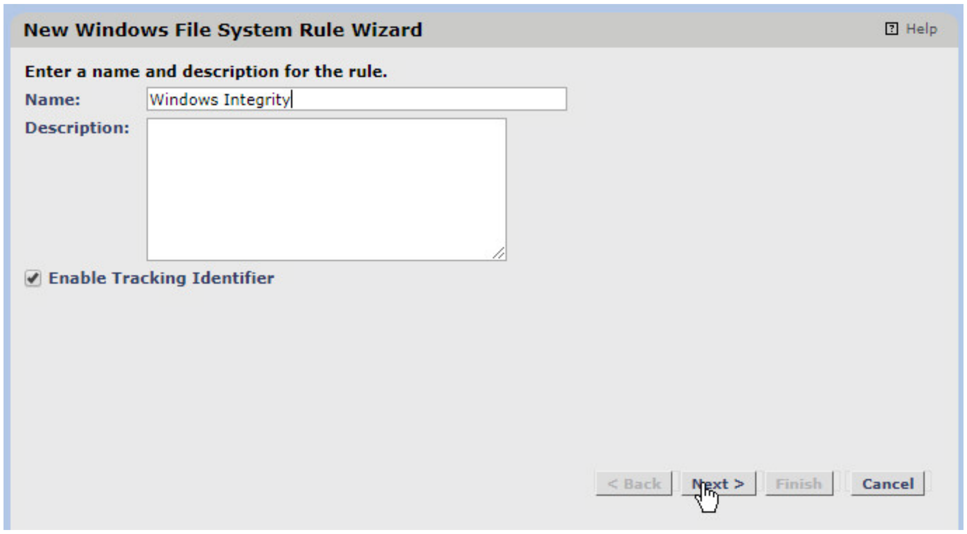
3. Click **New Rule**.
4. Select **Types > File Server > Windows File System Rule**.



Selected type: Windows File System Rule

https://tripwire/console/app.showComp.cmd?Id=2705&urlModifier=82&idIgC

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



New Windows File System Rule Wizard

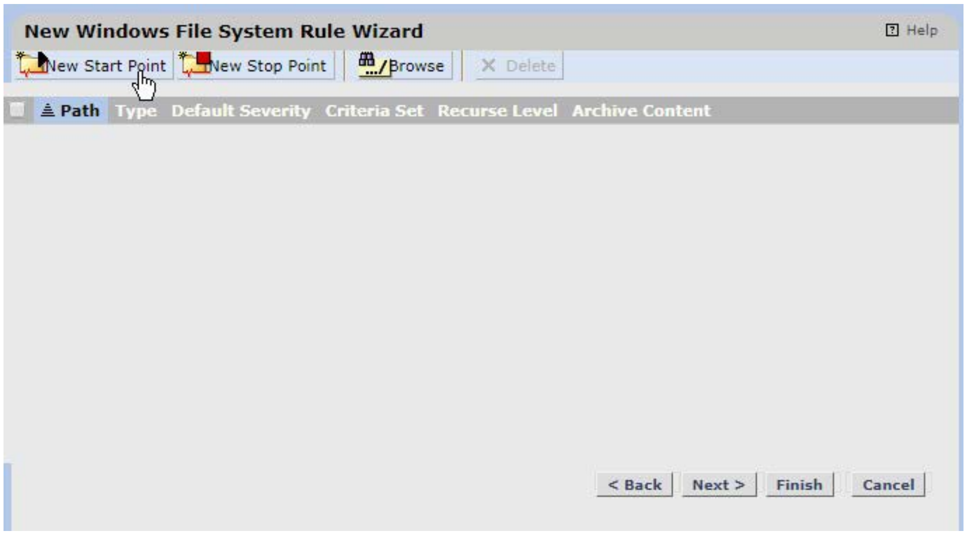
Enter a name and description for the rule.

Name: Windows Integrity

Description:

☑ Enable Tracking Identifier

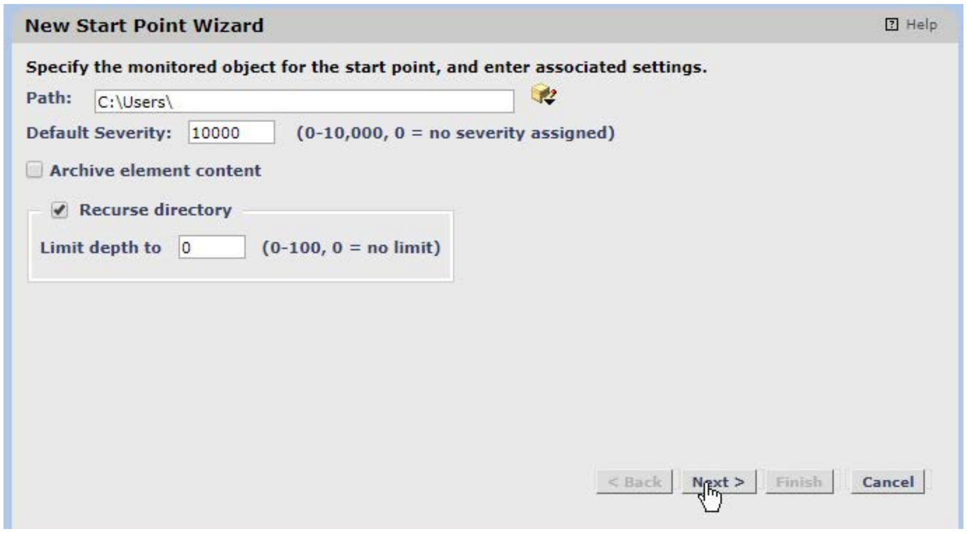
7. Click **Next**.



New Windows File System Rule Wizard

Path	Type	Default Severity	Criteria Set	Recurse Level	Archive Content

8. Click **New Start Point**. This will bring up a **New Start Point Wizard**.
9. Enter the **path** to a folder or file that will be monitored across all Windows Systems. For example, we chose to monitor *C:\Users*.
10. If you selected a directory and want the integrity check to recurse in all sub directories, make sure the box next to **Recurse directory** is checked.


New Start Point Wizard

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

Path: C:\Users\

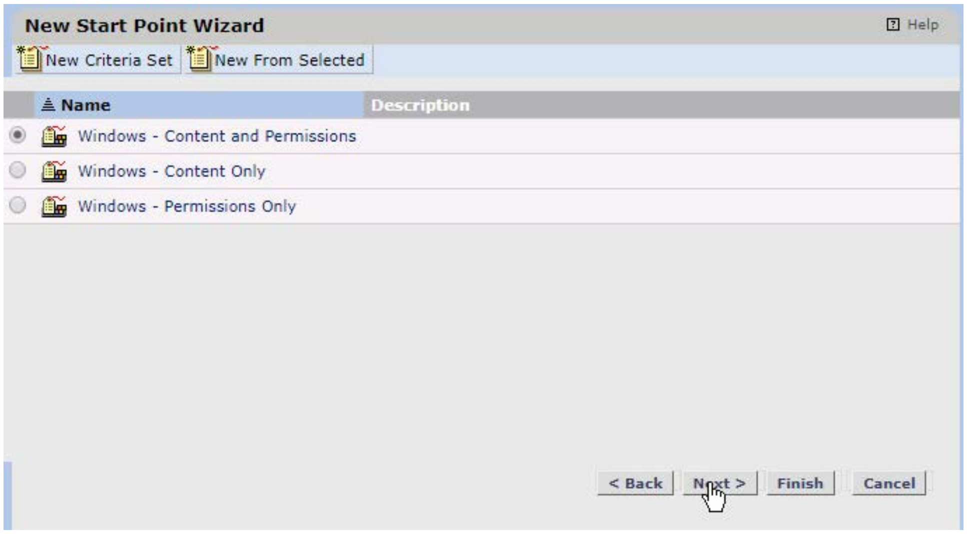
Default Severity: 10000 (0-10,000, 0 = no severity assigned)

□ Archive element content

☑ Recurse directory

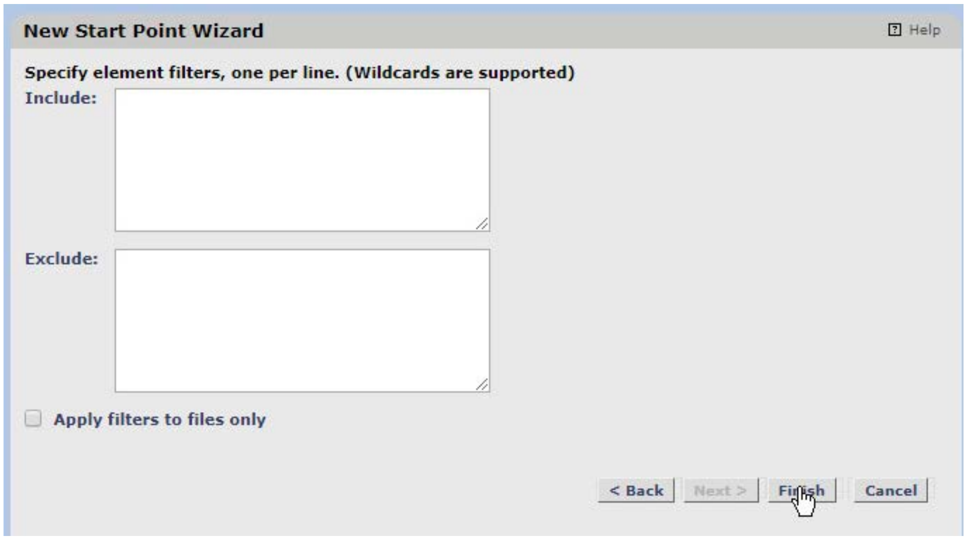
Limit depth to 0 (0-100, 0 = no limit)

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


New Start Point Wizard

	Name	Description
●	Windows - Content and Permissions	
○	Windows - Content Only	
○	Windows - Permissions Only	

13. Click **Next**.


New Start Point Wizard

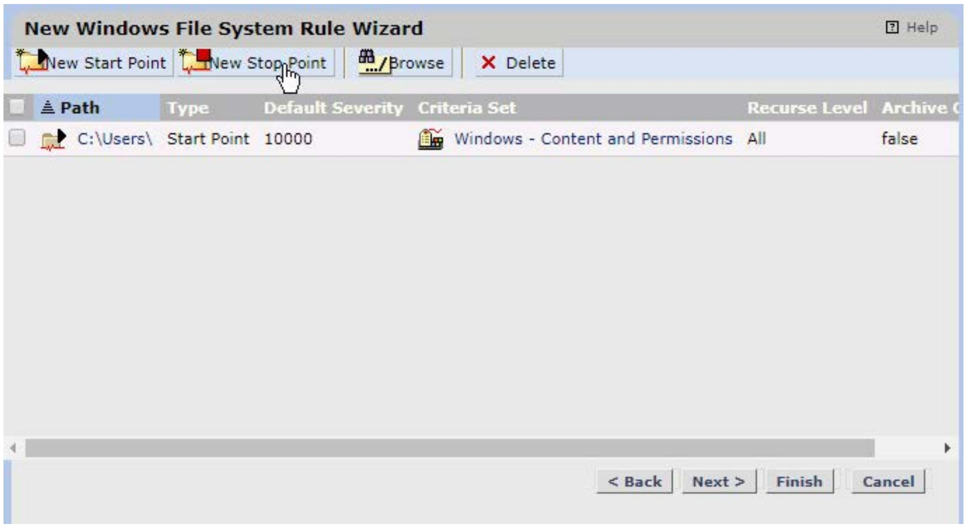
Specify element filters, one per line. (Wildcards are supported)

Include:

Exclude:

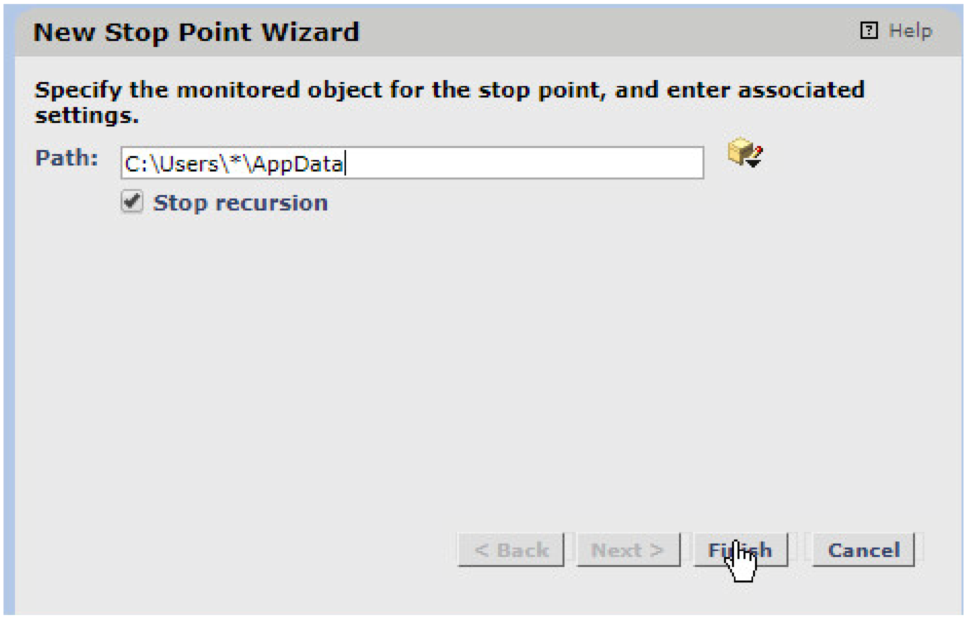
□ Apply filters to files only

14. Click **Finish**.
15. If you wish to exclude directories, click **New Stop Point**.


New Windows File System Rule Wizard

□	Path	Type	Default Severity	Criteria Set	Recurse Level	Archive (
□	C:\Users\	Start Point	10000	Windows - Content and Permissions	All	false

16. Enter the path name of directories you wish to exclude. For example, we chose to exclude *C:\Users\*\AppData* because that provided many false flags of routine application data modification.
17. Check the box next to **Stop Recursion**.



New Stop Point Wizard

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

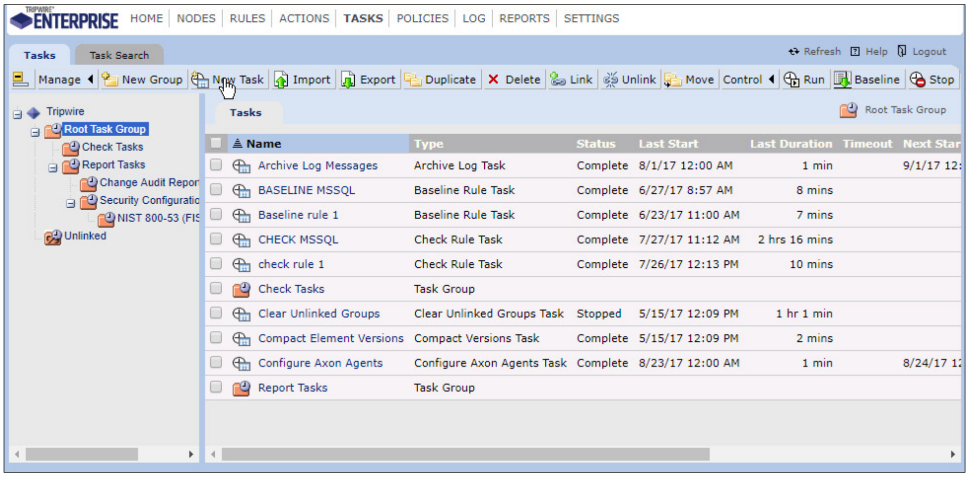
Path: C:\Users\*\AppData

☑ Stop recursion

18. Click **Finish**.
19. The rule created defines a space for the tasks we will create to search through.

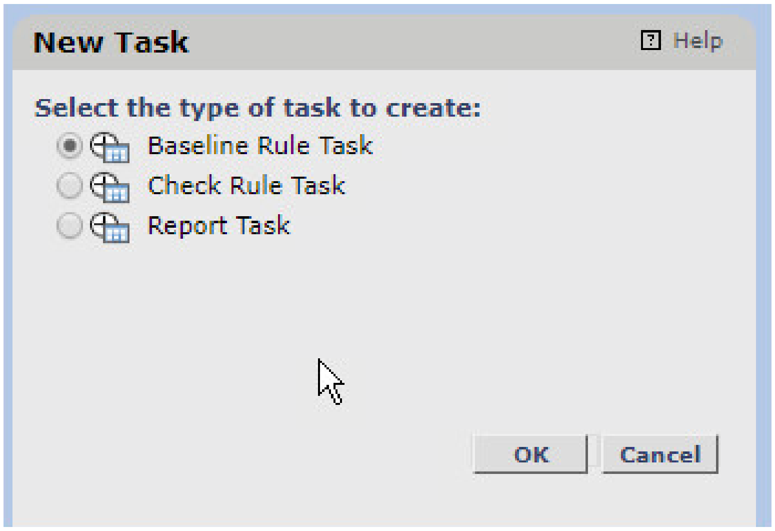
2.11.2.2 *Creating a Baseline Task*

1. Click the **Tasks** link.



Name	Type	Status	Last Start	Last Duration	Timeout	Next Star
Archive Log Messages	Archive Log Task	Complete	8/1/17 12:00 AM	1 min		9/1/17 12:
BASELINE MSSQL	Baseline Rule Task	Complete	6/27/17 8:57 AM	8 mins		
Baseline rule 1	Baseline Rule Task	Complete	6/23/17 11:00 AM	7 mins		
CHECK MSSQL	Check Rule Task	Complete	7/27/17 11:12 AM	2 hrs 16 mins		
check rule 1	Check Rule Task	Complete	7/26/17 12:13 PM	10 mins		
Check Tasks	Task Group					
Clear Unlinked Groups	Clear Unlinked Groups Task	Stopped	5/15/17 12:09 PM	1 hr 1 min		
Compact Element Versions	Compact Versions Task	Complete	5/15/17 12:09 PM	2 mins		
Configure Axon Agents	Configure Axon Agents Task	Complete	8/23/17 12:00 AM	1 min		8/24/17 1:
Report Tasks	Task Group					

2. Click **New Task**.
3. Select **Baseline Rule Task**.

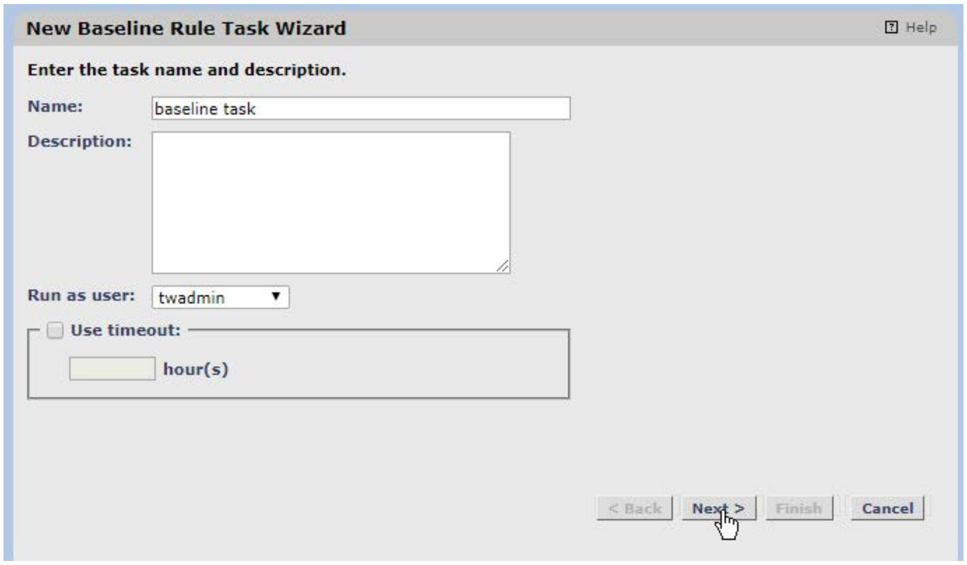


New Task

Select the type of task to create:

- ● Baseline Rule Task
- ○ Check Rule Task
- ○ Report Task

4. Click **OK**.
5. Enter a **name** for the baseline rule task.
6. Select a privileged user in Tripwire Enterprise to run the rule as.



New Baseline Rule Task Wizard

Enter the task name and description.

Name: baseline task

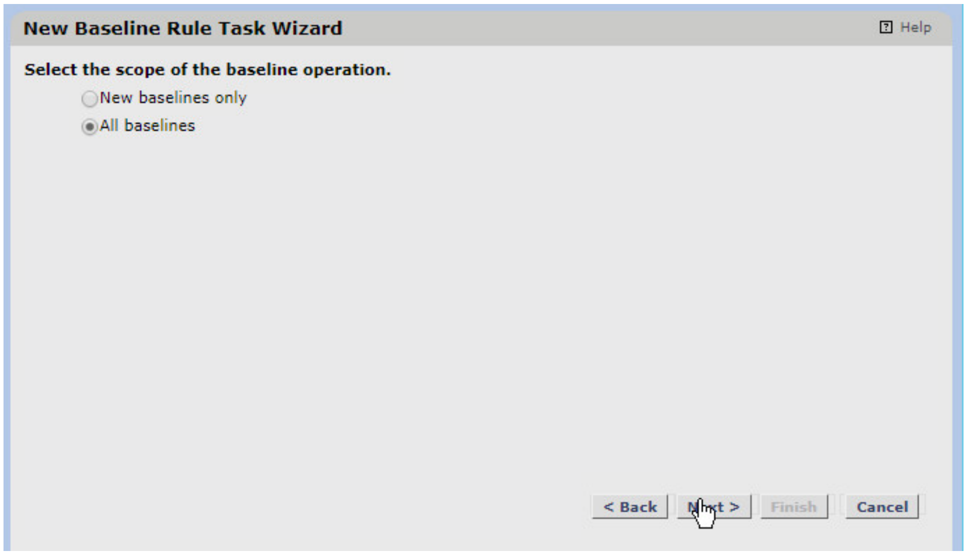
Description:

Run as user: twadmin

□ Use timeout:

hour(s)

7. Click **Next**.
8. Select **All Baselines**.

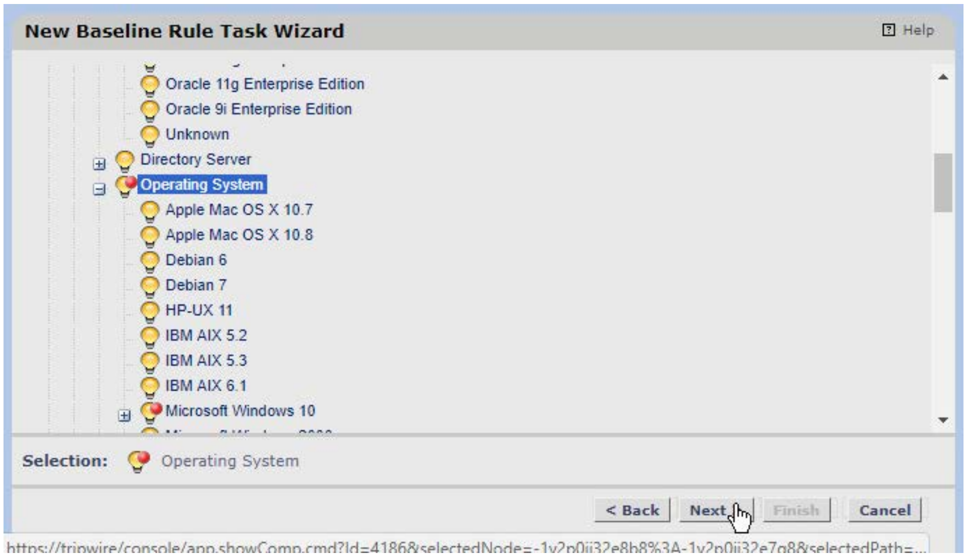


Select the scope of the baseline operation.

○ New baselines only

● All baselines

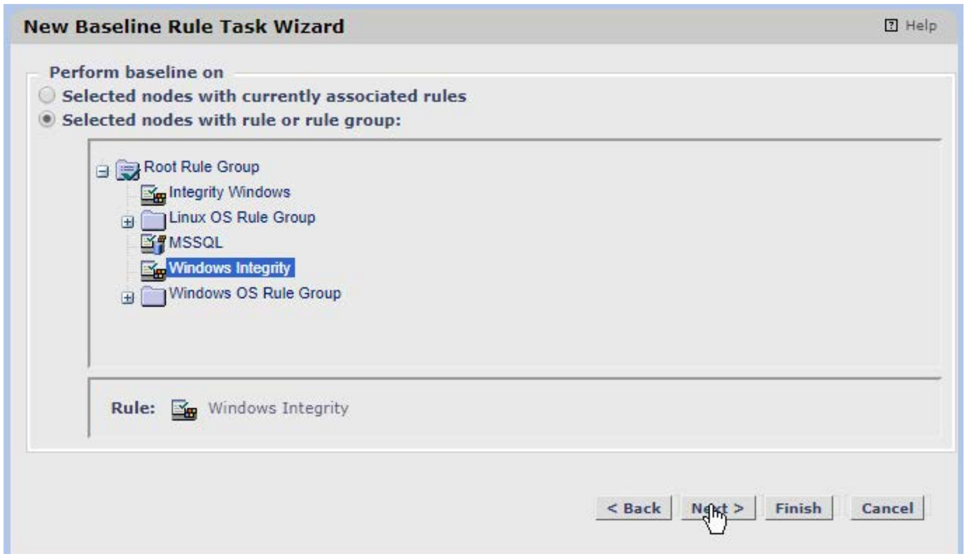
9. Click **Next**.
10. Expand **Root Node Group > Smart Node Groups > System Tag Sets > Operating System**.
11. You can select specific types of operating systems to run the task on or specific machines. We selected **Operating System** to have it run on all applicable Windows machines.



Selection: Operating System

https://tripwire/console/app.showComp.cmd?Id=4186&selectedNode=-1v2p0ij32e8b8%3A-1v2p0ij32e7g8&selectedPath=...

12. Once you have made your selection, click **Next**.
13. Select **Selected nodes with rule or rule group**.
14. Click the rule you created earlier.


New Baseline Rule Task Wizard

Perform baseline on

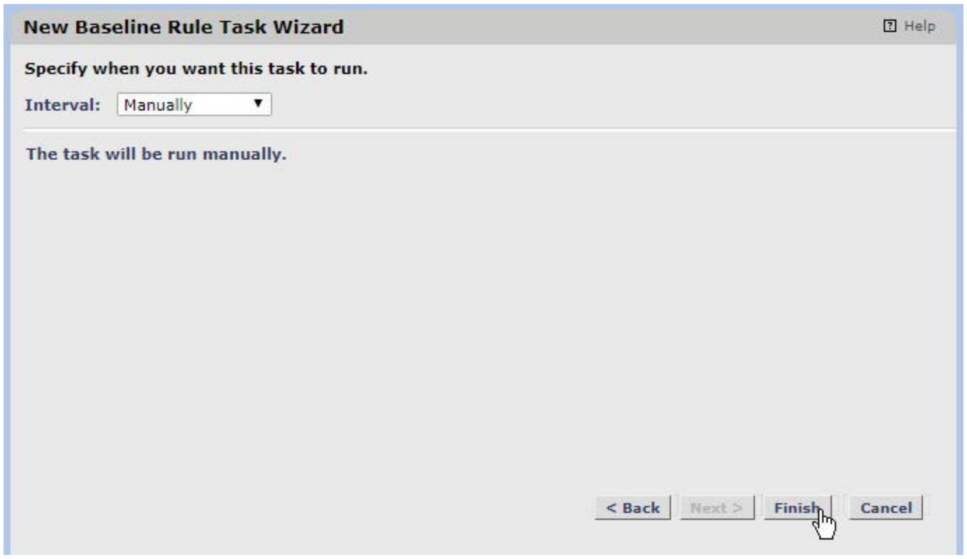
○ Selected nodes with currently associated rules

● Selected nodes with rule or rule group:

- Root Rule Group
  - Integrity Windows
  - Linux OS Rule Group
  - MSSQL
  - Windows Integrity
  - Windows OS Rule Group

Rule: Windows Integrity

15. Click **Next**.
16. Decide how often the baseline task should be run. We set it to **manually** but you can also set a very specific schedule by choosing **periodic**.


New Baseline Rule Task Wizard

Specify when you want this task to run.

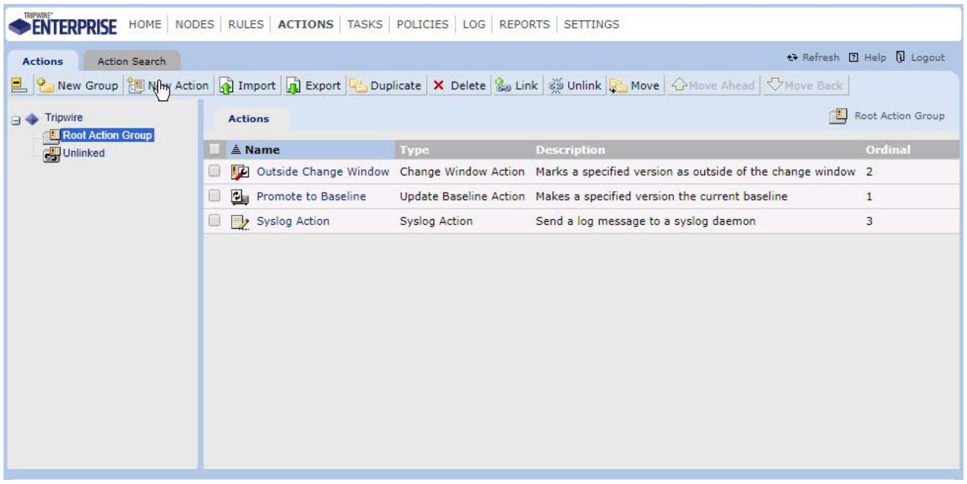
Interval: Manually

The task will be run manually.

17. Click **Finish**.
18. This rule will create baselines of the specified objects. Baselines are essentially versions of the file that check rules will compare against. Baselines should be primarily taken when the integrity of files are known to be good.

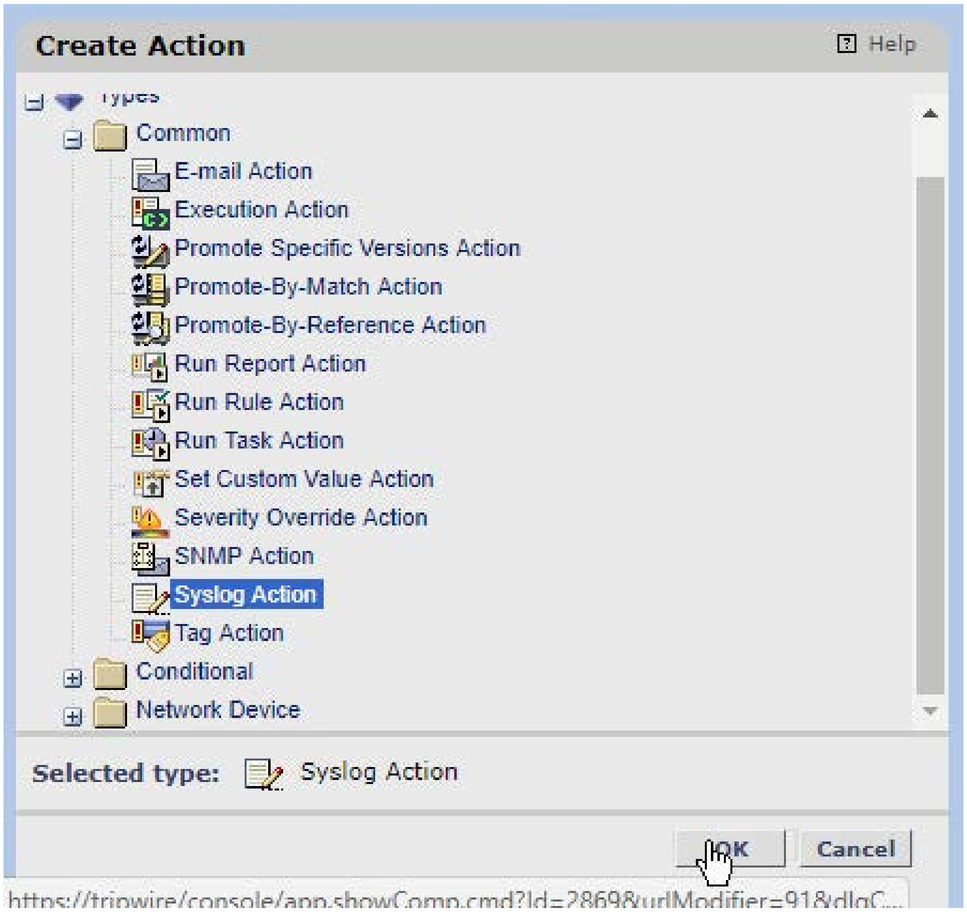
2.11.2.3 Creating a Syslog Action

1. Click the **Actions** link.



Name	Type	Description	Ordinal
Outside Change Window	Change Window Action	Marks a specified version as outside of the change window	2
Promote to Baseline	Update Baseline Action	Makes a specified version the current baseline	1
Syslog Action	Syslog Action	Send a log message to a syslog daemon	3

2. Click **New Action**.
3. Select **Syslog Action**.

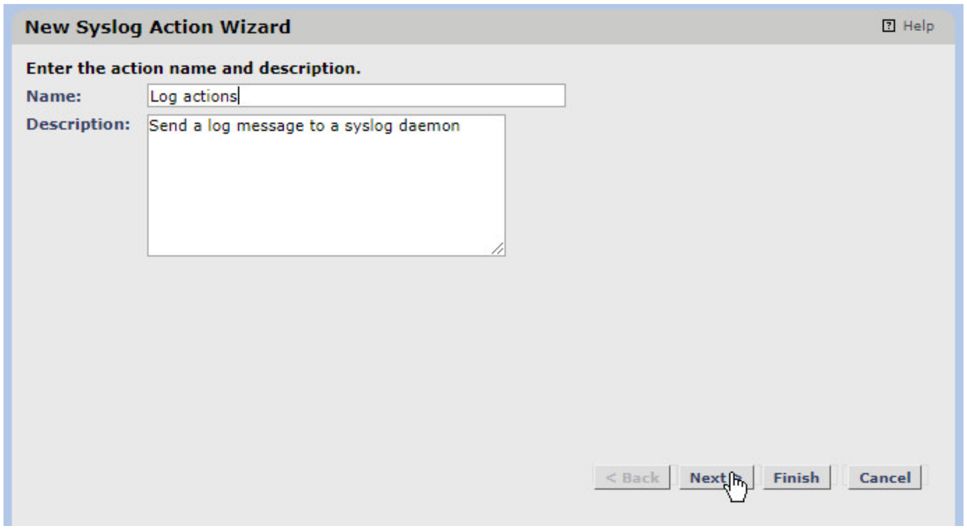


Selected type: Syslog Action

https://tripwire/console/app.showComp.cmd?Id=2869&urlModifier=91&dlgC...

4. Click **OK**.

5. Enter a **name** for the Syslog Action.



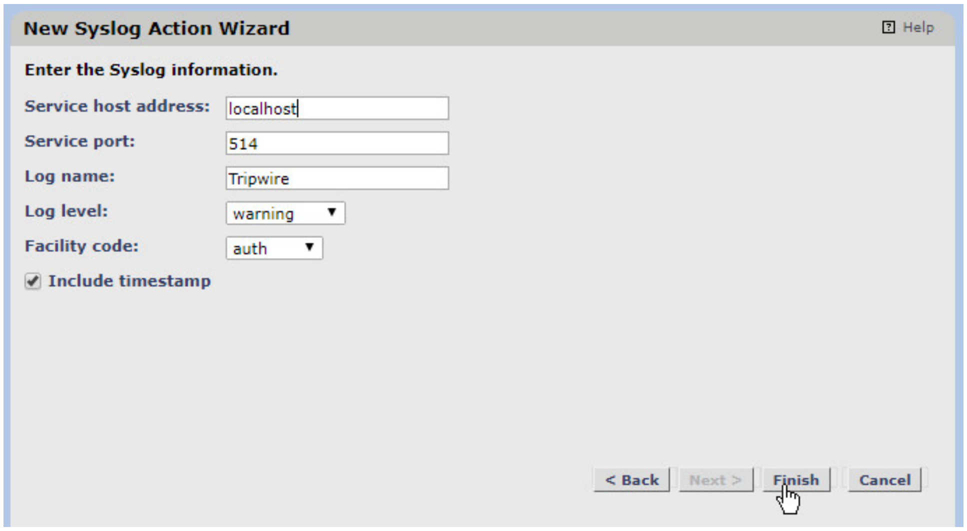
New Syslog Action Wizard

Enter the action name and description.

Name: Log actions

Description: Send a log message to a syslog daemon

6. Click **Next**.
7. Enter the **IP address** of the Tripwire Log Center server.
8. Enter the **port** that Tripwire Log Center receives TCP syslog messages on.
9. Enter a **log name**, a **level**, and a **facility code** per your needs. These will show up in logs, so you can use these to help separate or identify log sources.



New Syslog Action Wizard

Enter the Syslog information.

Service host address: localhost

Service port: 514

Log name: Tripwire

Log level: warning

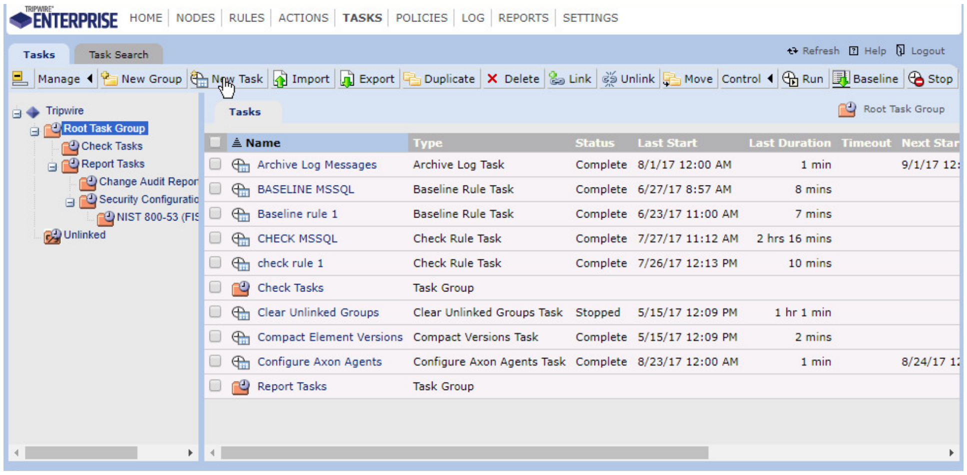
Facility code: auth

☑ Include timestamp

10. Click **Finish**.

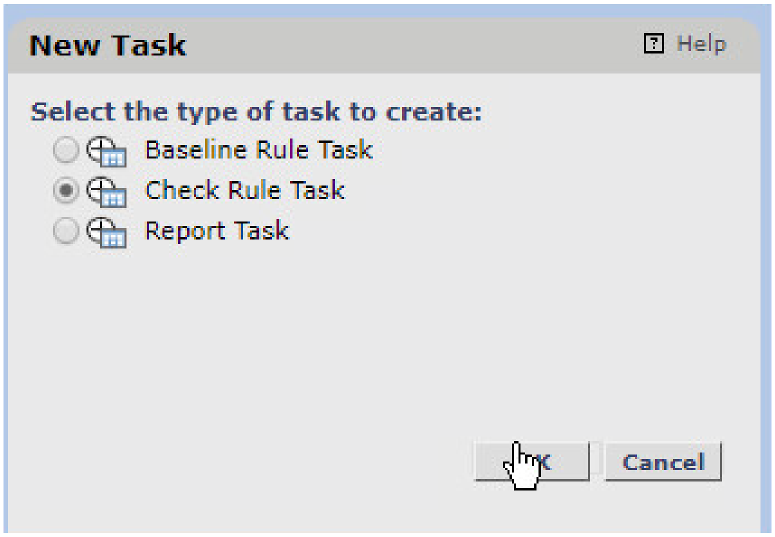
2.11.2.4 Creating a Check Task

1. Click the **Tasks** link.



Name	Type	Status	Last Start	Last Duration	Timeout	Next Star
Archive Log Messages	Archive Log Task	Complete	8/1/17 12:00 AM	1 min		9/1/17 12:
BASELINE MSSQL	Baseline Rule Task	Complete	6/27/17 8:57 AM	8 mins		
Baseline rule 1	Baseline Rule Task	Complete	6/23/17 11:00 AM	7 mins		
CHECK MSSQL	Check Rule Task	Complete	7/27/17 11:12 AM	2 hrs 16 mins		
check rule 1	Check Rule Task	Complete	7/26/17 12:13 PM	10 mins		
Check Tasks	Task Group					
Clear Unlinked Groups	Clear Unlinked Groups Task	Stopped	5/15/17 12:09 PM	1 hr 1 min		
Compact Element Versions	Compact Versions Task	Complete	5/15/17 12:09 PM	2 mins		
Configure Axon Agents	Configure Axon Agents Task	Complete	8/23/17 12:00 AM	1 min		8/24/17 1:
Report Tasks	Task Group					

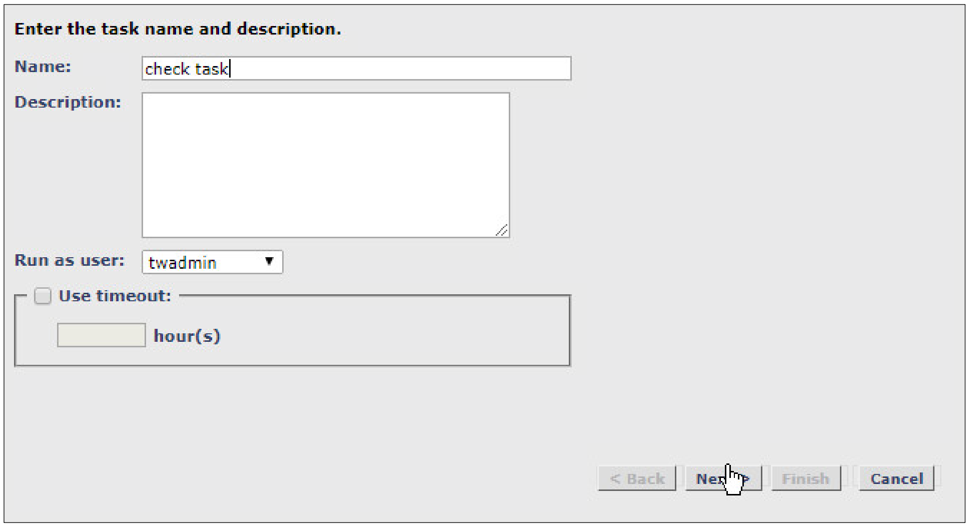
2. Click **New Task**.
3. Select **Check Rule Task**.



Select the type of task to create:

○ Baseline Rule Task
● Check Rule Task
○ Report Task

4. Click **OK**.
5. Enter a **name** for the baseline rule task.
6. Select a privileged user in Tripwire Enterprise to run the rule as.


Enter the task name and description.

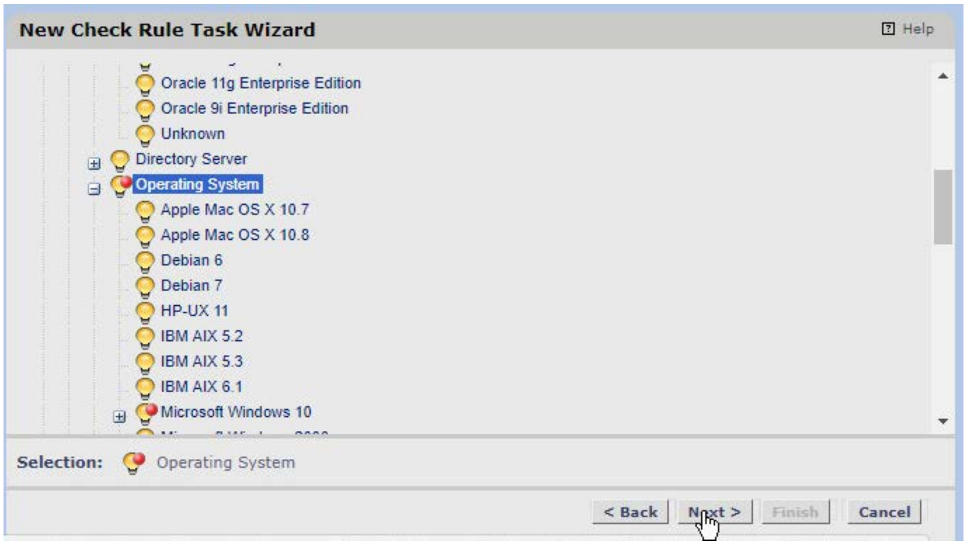
Name: check task

Description:

Run as user: twadmin

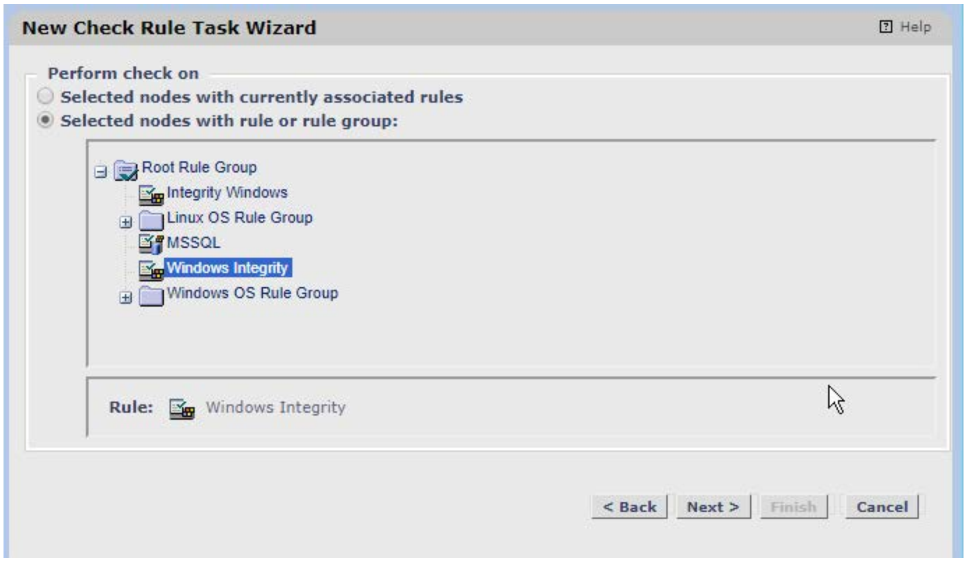
☐ Use timeout: hour(s)

7. Click **Next**.
8. Expand **Root Node Group > Smart Node Groups > System Tag Sets > Operating System**.
9. Here, you can select specific types of operating systems to run the task on or specific machines. We selected **Operating System** to have it run on all applicable Windows machines.


New Check Rule Task Wizard

Selection: Operating System

10. Once you have made your selection, click **Next**.
11. Select **Selected nodes with rule or rule group**.
12. Click the rule you created earlier.


New Check Rule Task Wizard

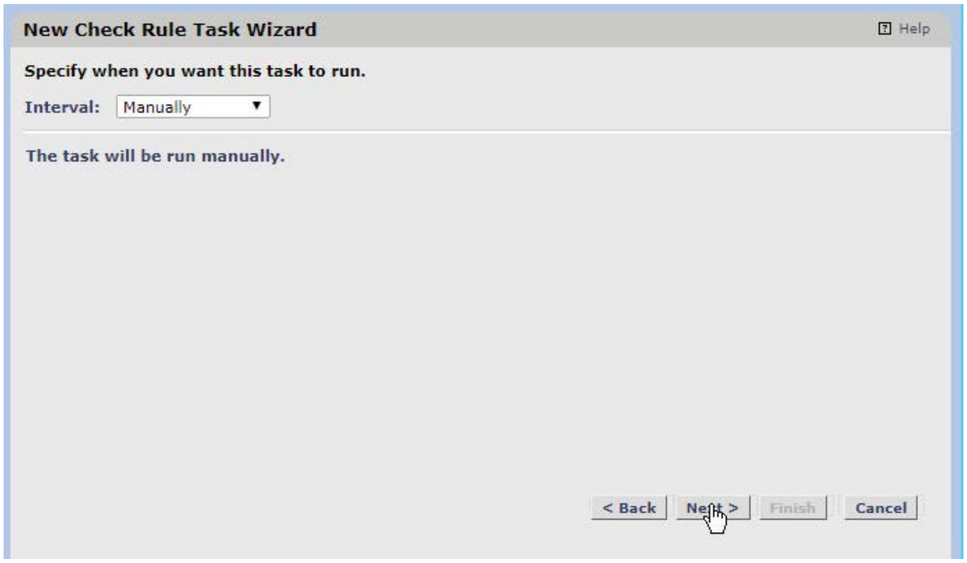
Perform check on

○ Selected nodes with currently associated rules

● Selected nodes with rule or rule group:

Rule: Windows Integrity

13. Click **Next**.
14. Decide how often the check task should be run. We set it to **manually**, but you can also set a very specific schedule by choosing **periodic**.

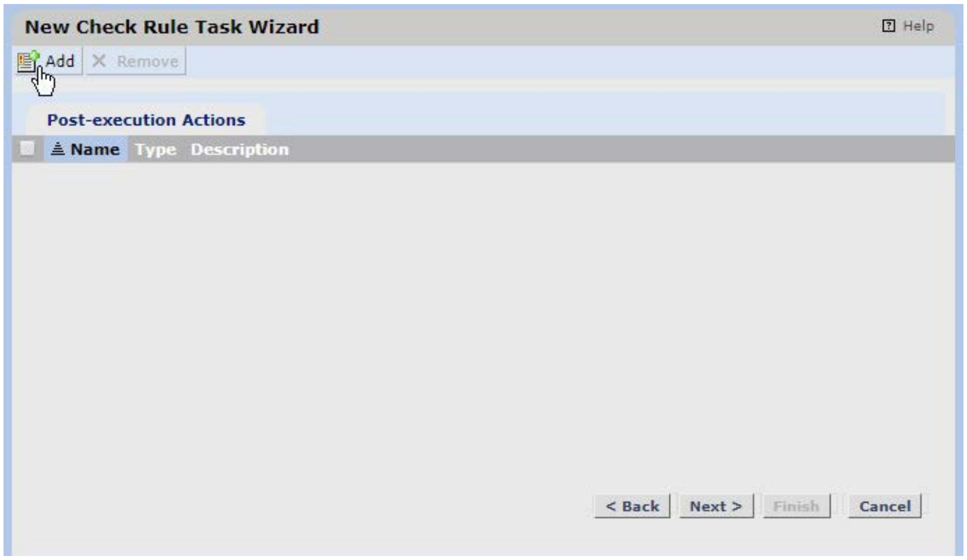

New Check Rule Task Wizard

Specify when you want this task to run.

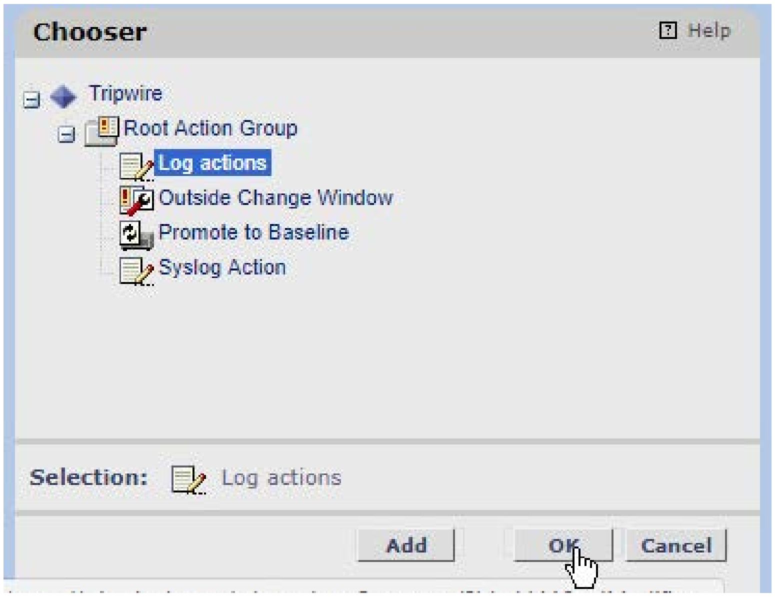
Interval: Manually

The task will be run manually.

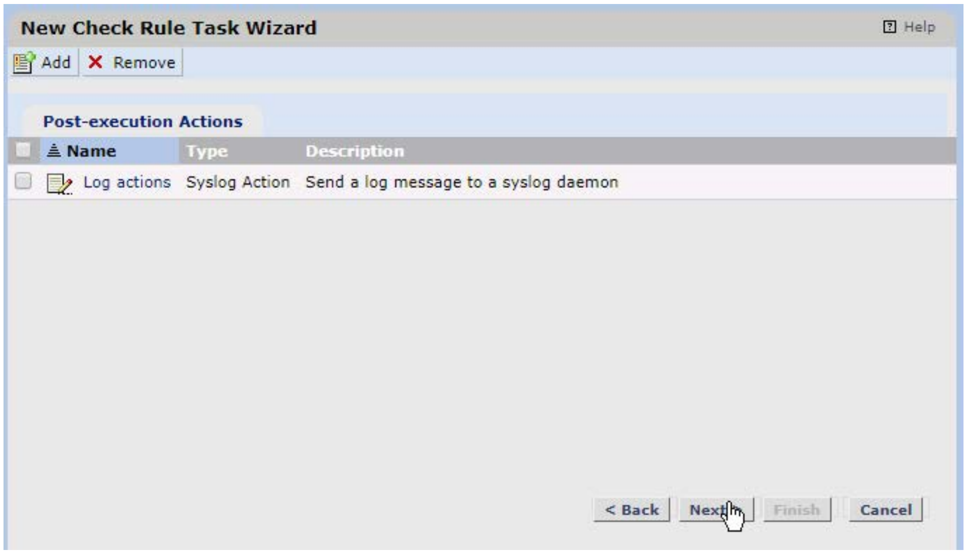
15. Click **Next**.



16. Click **Add**.
17. Select the **Syslog Action** created earlier.



18. Click **OK**.

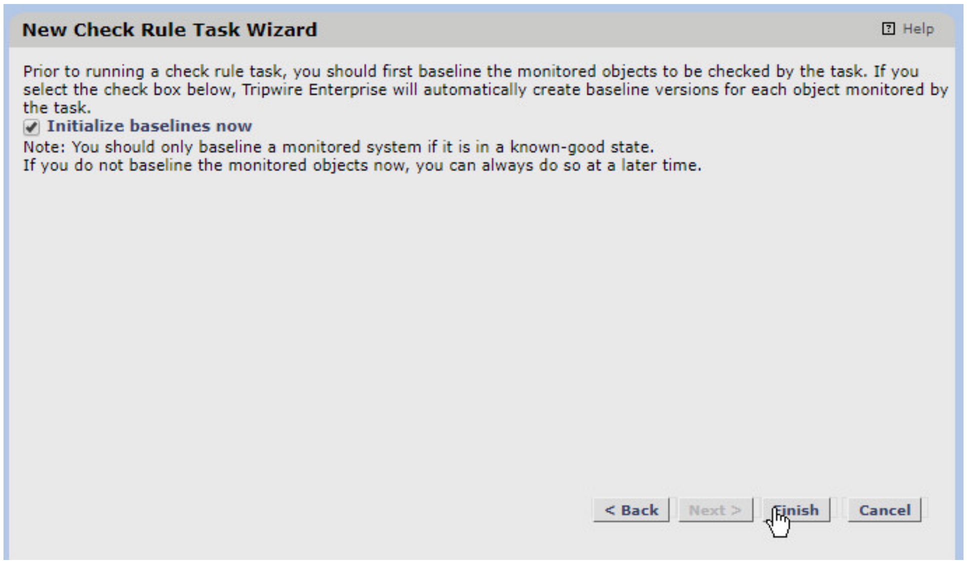


New Check Rule Task Wizard

Post-execution Actions

	Name	Type	Description
□	Log actions	Syslog Action	Send a log message to a syslog daemon

19. Click **Next**.
20. Uncheck the box next to **initialize baselines now** if you do not wish to immediately take a baseline of all systems.



New Check Rule Task Wizard

Prior to running a check rule task, you should first baseline the monitored objects to be checked by the task. If you select the check box below, Tripwire Enterprise will automatically create baseline versions for each object monitored by the task.

☑ Initialize baselines now

Note: You should only baseline a monitored system if it is in a known-good state.
If you do not baseline the monitored objects now, you can always do so at a later time.

21. Click **Finish**.
22. This rule will check the current versions of the selected files against their baselines and log any changes to Tripwire Log Center.

2.11.2.5 Running the Baseline Task

1. Check the box next to the **baseline** task you created earlier.
2. Click **Control > Run** on the taskbar.

3. Wait for the run to finish. You can click the **Log** link to see the progress.
4. When it finishes, it will log a message such as “Task 'Baseline Rule Windows' was completed in 600 seconds.”

2.11.2.6 Make Changes to Monitored Objects

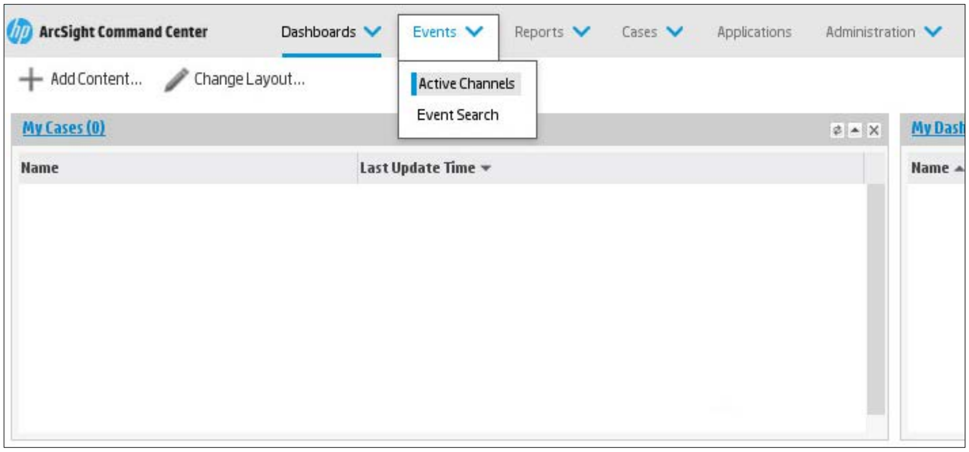
1. Open a machine being monitored by the rule you created.
2. Modify a file or files in the folder that you selected in the rule creation wizard (which are being monitored by Tripwire).

2.11.2.7 Running the Check Task

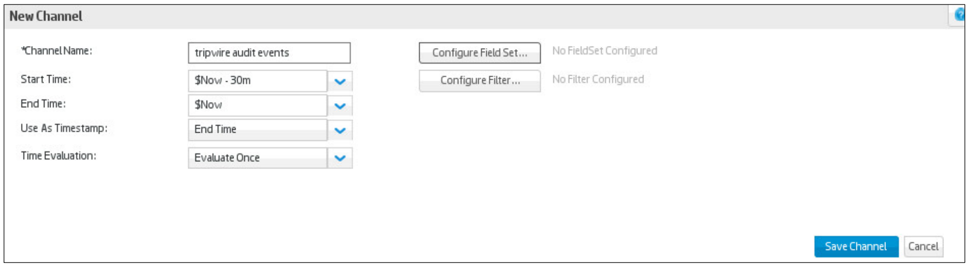
1. Check the box next to the **check** task you created earlier.
2. Click **Control > Run** on the taskbar.
3. Wait for the run to finish. You can click the **Log** link to see the progress.
4. If you made changes to a monitored object, the log message should appear at the time the changes were made even if the change was made prior to the scan.

2.11.2.8 Filtering for Tripwire Enterprise Integrity Events in HPE ArcSight ESM

1. Open the **ArcSight ESM** machine.
2. Log in by going to *https://vm-esm691c:8443* and entering your username/password.



3. Click **Events > Active Channels**.
4. Click **New**.
5. Enter a **name** for the channel. Select a start time to show events, and leave **$NOW** as the end time.



New Channel

*Channel Name: tripwire audit events

Start Time: $Now - 30m

End Time: $Now

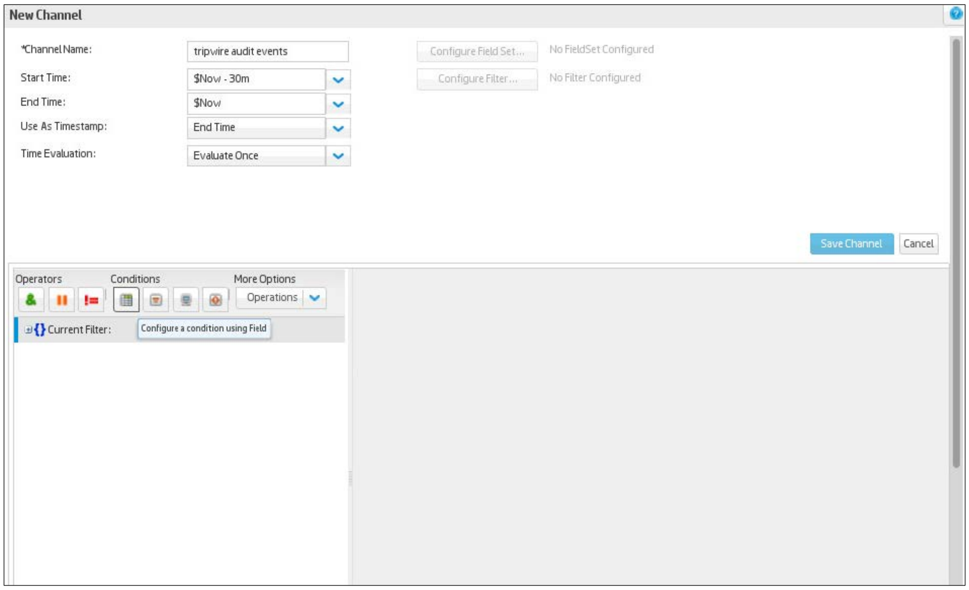
Use As Timestamp: End Time

Time Evaluation: Evaluate Once

No FieldSet Configured

No Filter Configured

6. Click **Configure Filter**.



New Channel

*Channel Name: tripwire audit events

Start Time: $Now - 30m

End Time: $Now

Use As Timestamp: End Time

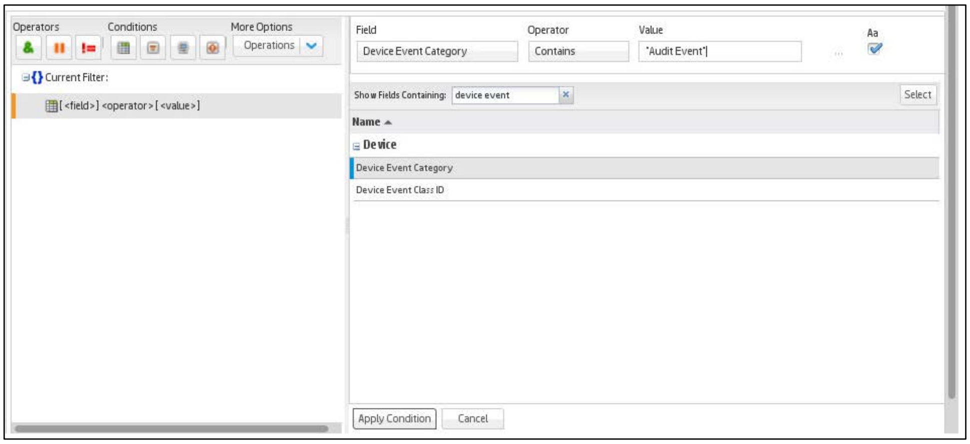
Time Evaluation: Evaluate Once

No FieldSet Configured

No Filter Configured

Current Filter:

7. Click the button that says **Configure a condition using field**.
8. Double click **Device Event Category**.
9. For **Operator**, choose **Contains**.
10. For **Value**, enter **Audit Event**.



Current Filter:

[<field>] <operator> [<value>]

Field: Device Event Category

Operator: Contains

Value: "Audit Event"

Show Fields Containing: device event

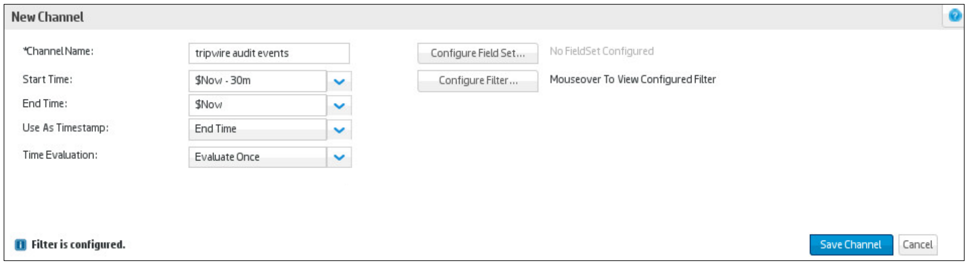
Name

Device

Device Event Category

Device Event Class ID

11. Click **Apply Condition.**
12. Click **Update Filter Configuration** under the list of fields.



New Channel

*Channel Name: tripwire audit events

Start Time: $Now - 30m

End Time: $Now

Use As Timestamp: End Time

Time Evaluation: Evaluate Once

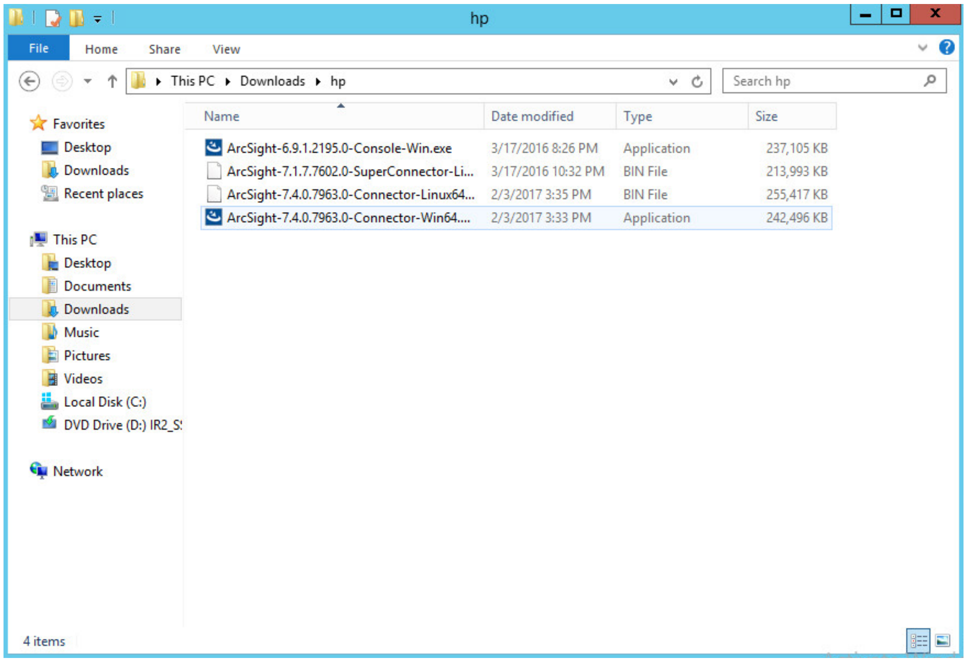
13. Click **Save Channel**.
14. Click the channel you just created. It should show all file changes in the time frame you specified forwarded from Tripwire Enterprise to Tripwire Log Center to ArcSight ESM.

2.12 Integration: HPE ArcSight ESM with Veeam and Hyper-V

This section covers the process for integrating HPE ArcSight ESM with Veeam and Hyper-V. This integration assumes the correct implementation of Veeam and ArcSight as described in earlier sections. The result is the forwarding of logs generated by Veeam and Hyper-V to ArcSight ESM, as well as custom parsers to supplement the information provided by this forwarding process.

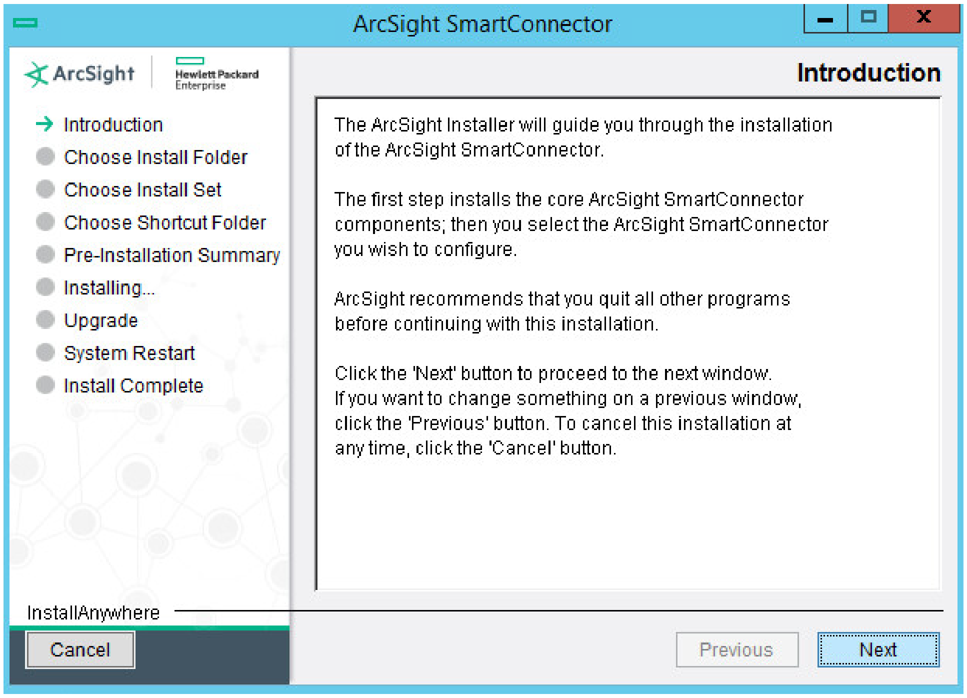
2.12.1 Install ArcSight Connector

1. Run the installation file **ArcSight-7.4.0.7963.0-Connector-Win64** on the Veeam Server.



Name	Date modified	Type	Size
ArcSight-6.9.1.2195.0-Console-Win.exe	3/17/2016 8:26 PM	Application	237,105 KB
ArcSight-7.1.7.7602.0-SuperConnector-Li...	3/17/2016 10:32 PM	BIN File	213,993 KB
ArcSight-7.4.0.7963.0-Connector-Linux64...	2/3/2017 3:35 PM	BIN File	255,417 KB
ArcSight-7.4.0.7963.0-Connector-Win64....	2/3/2017 3:33 PM	Application	242,496 KB

2. Wait for the initial setup to finish.



Introduction

The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector.

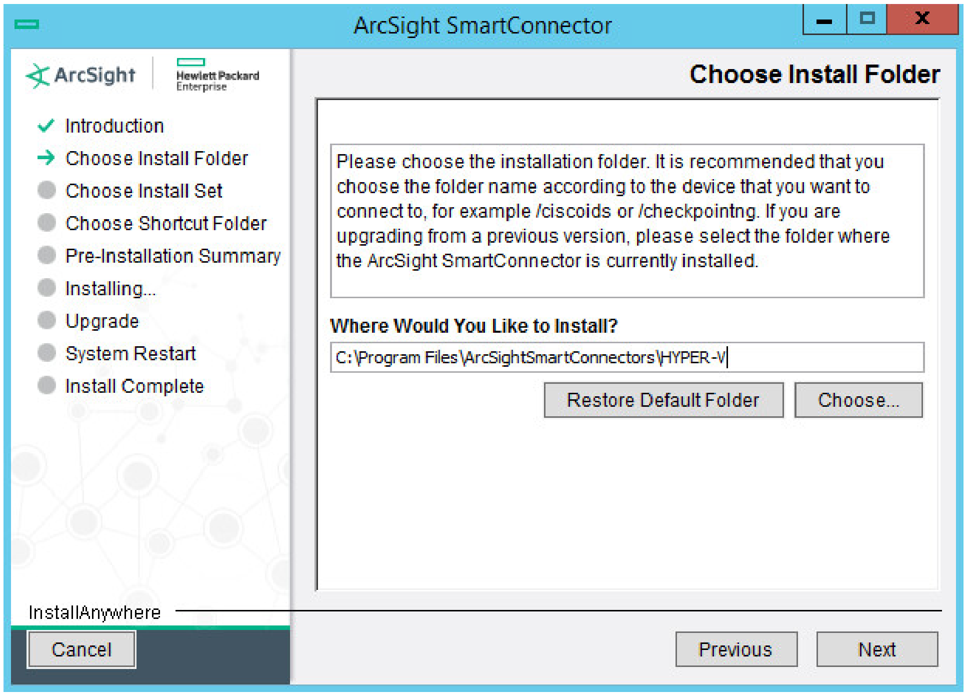
The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.

3. Click **Next**.

4. Choose a destination folder. Note: It is recommended to change the default to `<default>\HYPERV` so that other installed connectors do not overwrite this one.



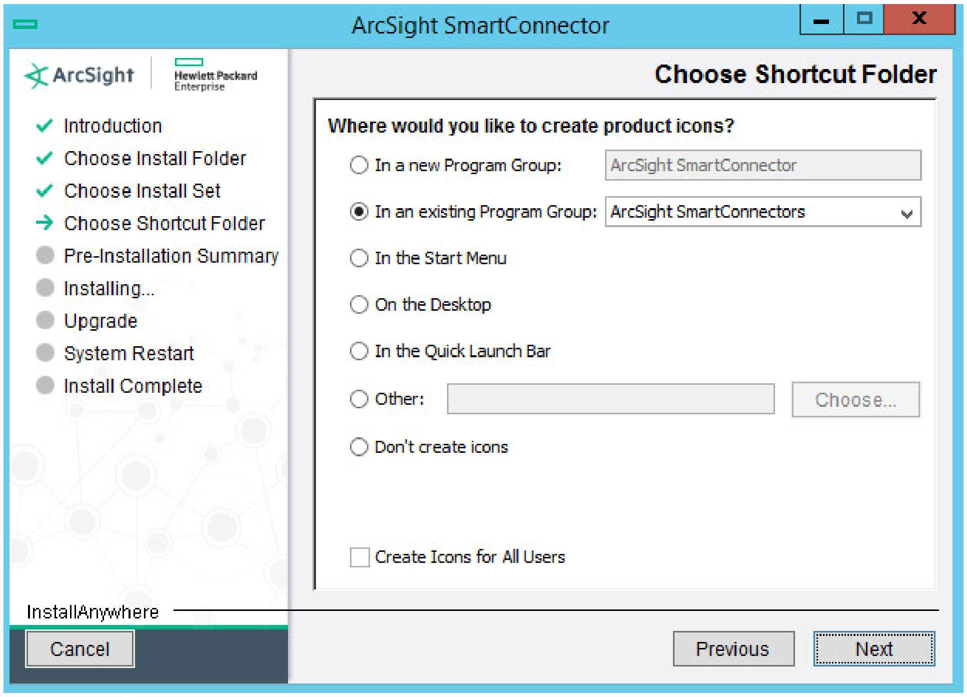
Choose Install Folder

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\HYPER-V

5. Click **Next**.



ArcSight SmartConnector

Choose Shortcut Folder

Where would you like to create product icons?

○ In a new Program Group: ArcSight SmartConnector

● In an existing Program Group: ArcSight SmartConnectors

○ In the Start Menu

○ On the Desktop

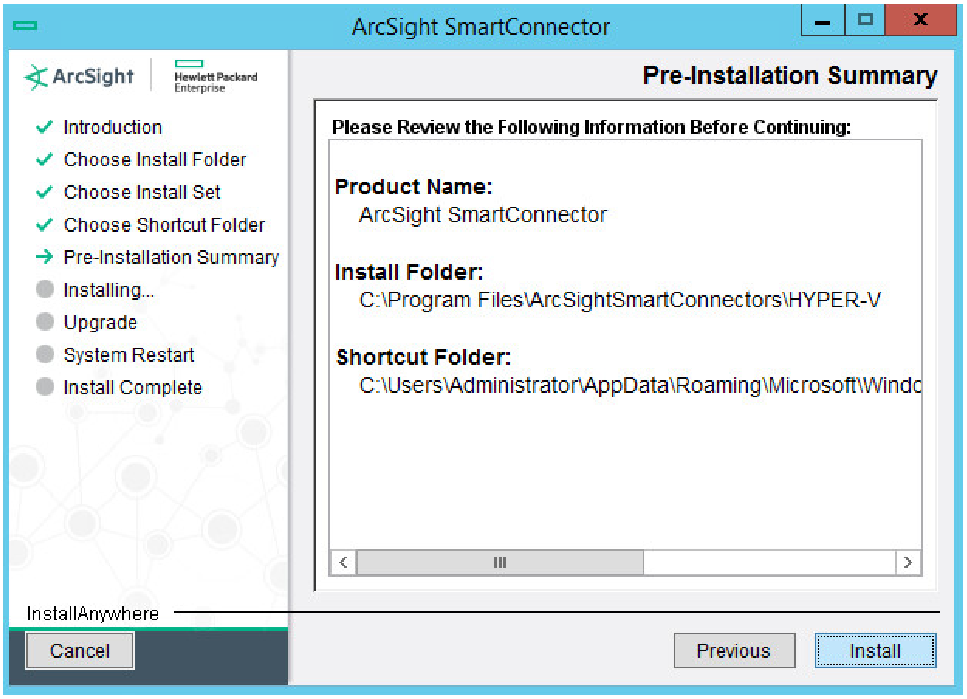
○ In the Quick Launch Bar

○ Other:

○ Don't create icons

□ Create Icons for All Users

6. Click **Next**.



ArcSight SmartConnector

Pre-Installation Summary

Please Review the Following Information Before Continuing:

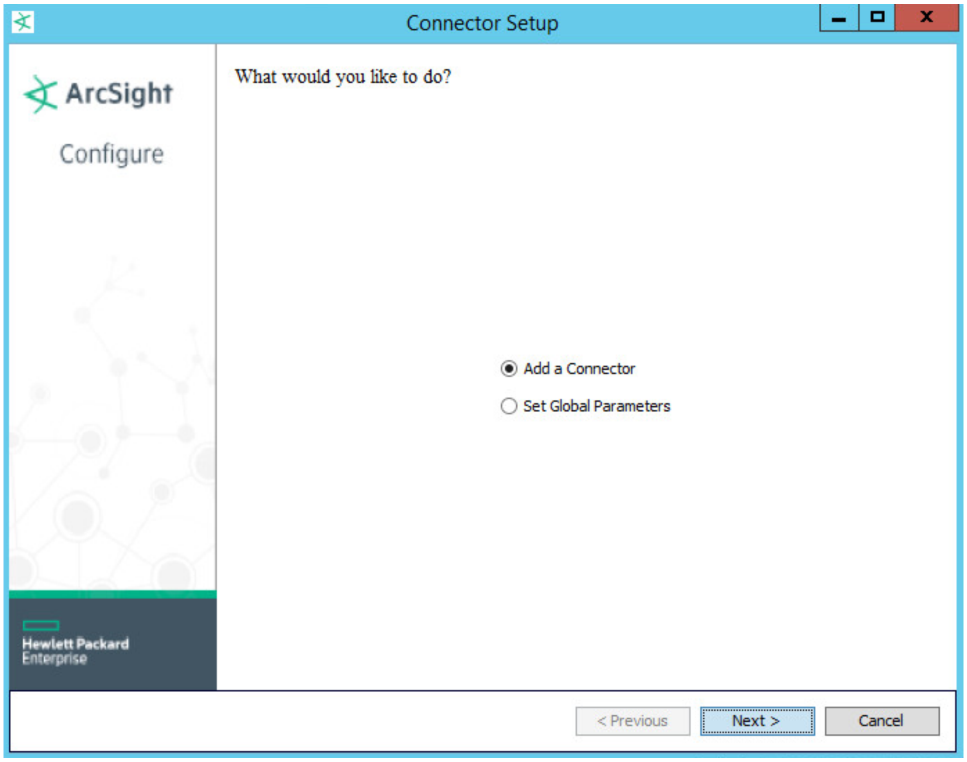
Product Name:
ArcSight SmartConnector

Install Folder:
C:\Program Files\ArcSightSmartConnectors\HYPER-V

Shortcut Folder:
C:\Users\Administrator\AppData\Roaming\Microsoft\Windo

7. Click **Install**.
8. Wait for the installation to finish.

9. Select **Add a Connector**.

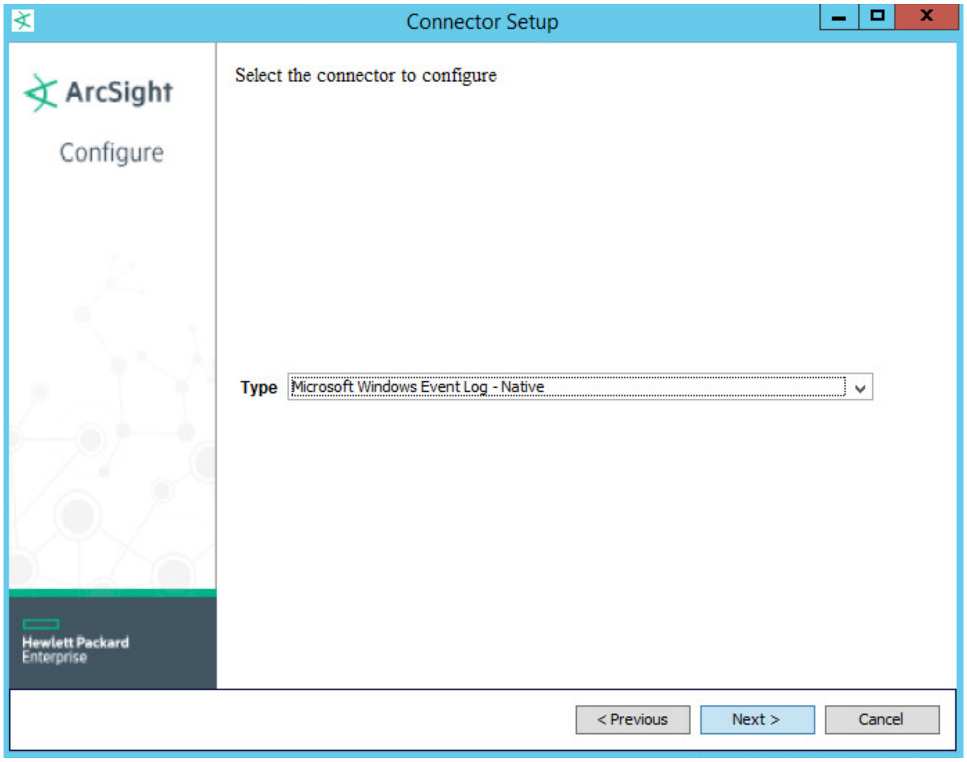


What would you like to do?

● Add a Connector

○ Set Global Parameters

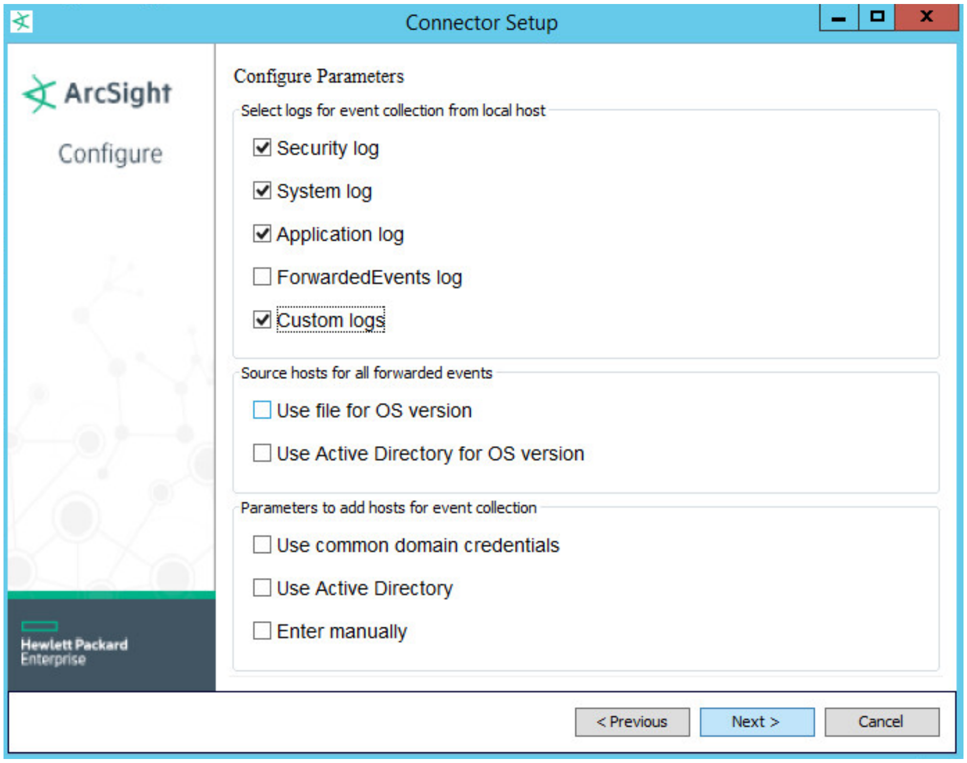
10. Click **Next**.
11. Choose **Microsoft Windows Event Log - Native** from the list.



Select the connector to configure

Type: Microsoft Windows Event Log - Native

12. Click **Next**.
13. Check **Security log**, **System log**, **Application Log**, and **Custom Log**.


Configure Parameters

Select logs for event collection from local host

☑ Security log

☑ System log

☑ Application log

□ ForwardedEvents log

☑ Custom logs

Source hosts for all forwarded events

□ Use file for OS version

□ Use Active Directory for OS version

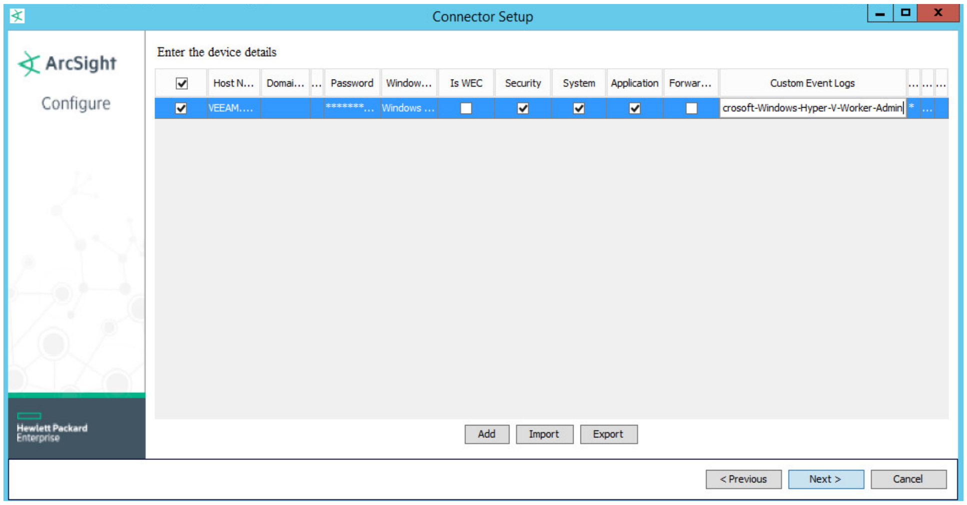
Parameters to add hosts for event collection

□ Use common domain credentials

□ Use Active Directory

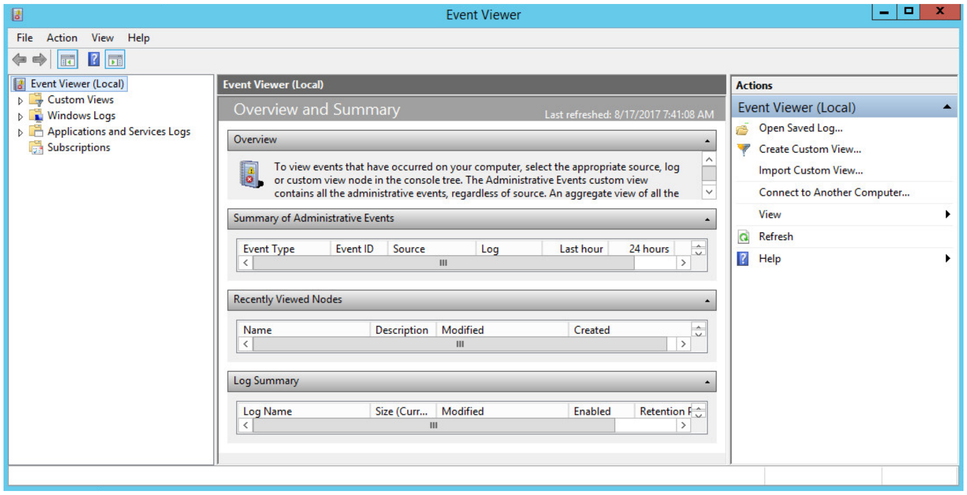
□ Enter manually

14. Click **Next**.
15. Click on the box underneath **Custom Event Logs**.
16. Enter **Veeam Backup, Microsoft-Windows-Hyper-V-VMMS-Admin, Microsoft-Windows-Hyper-V-Integration-Admin, Microsoft-Windows-Hyper-V-SynthNic-Admin, Microsoft-Windows-Hyper-V-Worker-Admin.**


Enter the device details

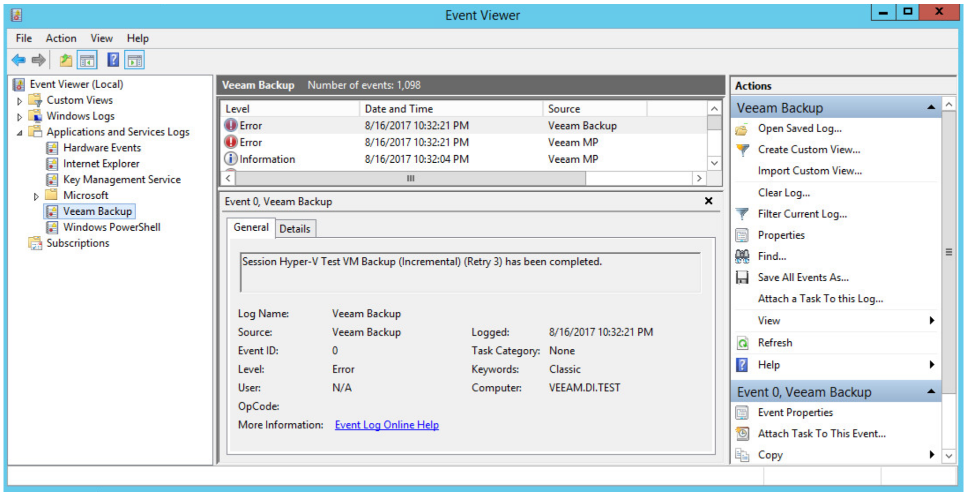
☑	Host N…	Domai…	…	Password	Window…	Is WEC	Security	System	Application	Forwar…	Custom Event Logs	…	…	…
☑	VEEAM.…			*******…	Windows …	□	☑	☑	☑	□	crosoft-Windows-Hyper-V-Worker-Admin	*	…	

17. You can add more application logs through the following process:
    a. Open **Microsoft Event Viewer**.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the

b. Find the log you wish to add.

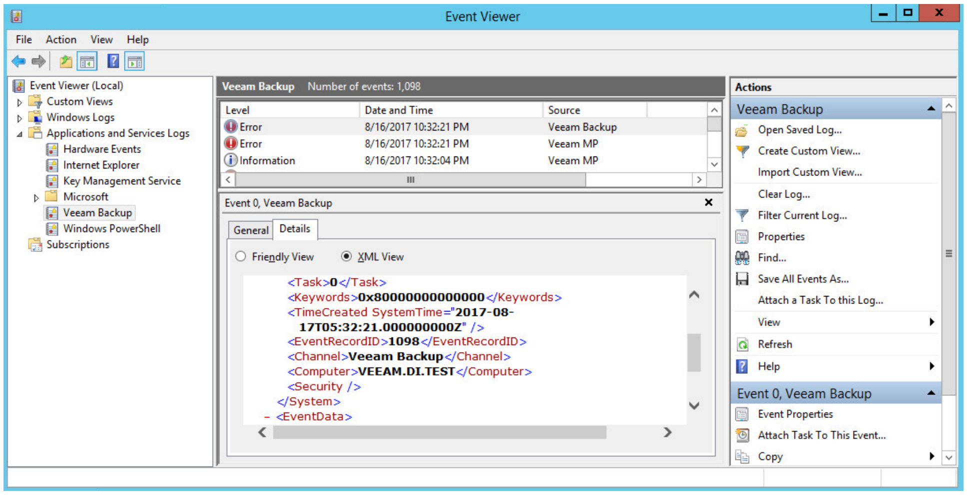


Level	Date and Time	Source
Error	8/16/2017 10:32:21 PM	Veeam Backup
Error	8/16/2017 10:32:21 PM	Veeam MP
Information	8/16/2017 10:32:04 PM	Veeam MP

Session Hyper-V Test VM Backup (Incremental) (Retry 3) has been completed.

Log Name: Veeam Backup
Source: Veeam Backup Logged: 8/16/2017 10:32:21 PM
Event ID: 0 Task Category: None
Level: Error Keywords: Classic
User: N/A Computer: VEEAM.DI.TEST
OpCode:
More Information: Event Log Online Help

c. Open the **Details** pane of a log and find the field **Channel**.



Veeam Backup Number of events: 1,098

Level	Date and Time	Source
Error	8/16/2017 10:32:21 PM	Veeam Backup
Error	8/16/2017 10:32:21 PM	Veeam MP
Information	8/16/2017 10:32:04 PM	Veeam MP

Event 0, Veeam Backup

○ Friendly View ● XML View

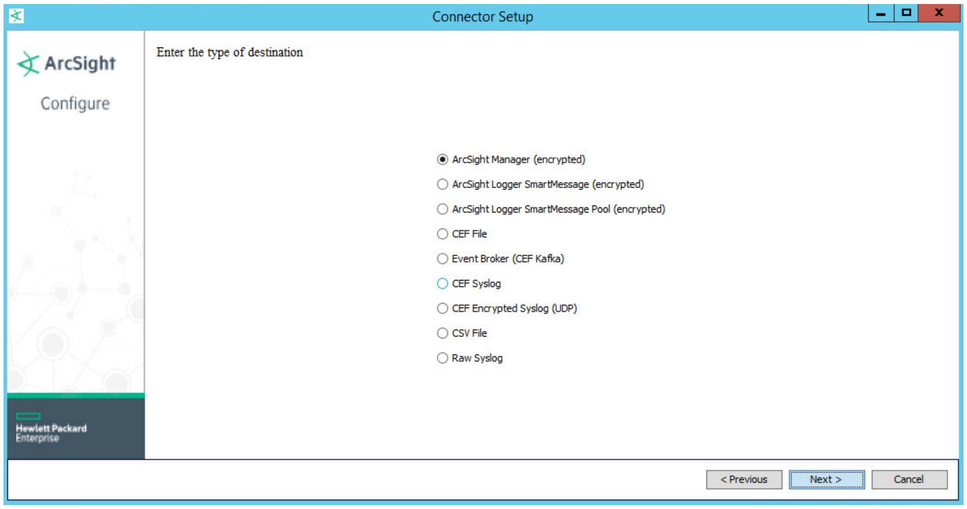
```
      <Task>0</Task>
      <Keywords>0x80000000000000</Keywords>
      <TimeCreated SystemTime="2017-08-
        17T05:32:21.000000000Z" />
      <EventRecordID>1098</EventRecordID>
      <Channel>Veeam Backup</Channel>
      <Computer>VEEAM.DI.TEST</Computer>
      <Security />
    </System>
  - <EventData>
```

d. Note that this may differ from the **Log Name** in the **General** pane. (For example, one of the Hyper-V log's **Log Name** is **Microsoft-Windows-Hyper-V-VMMS/Admin** but the channel name is **Microsoft-Windows-Hyper-V-VMMS-Admin**.)

e. Enter all these channel names separated by commas in the **Custom Event Logs** field.

18. Click **Next**.

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



Enter the type of destination

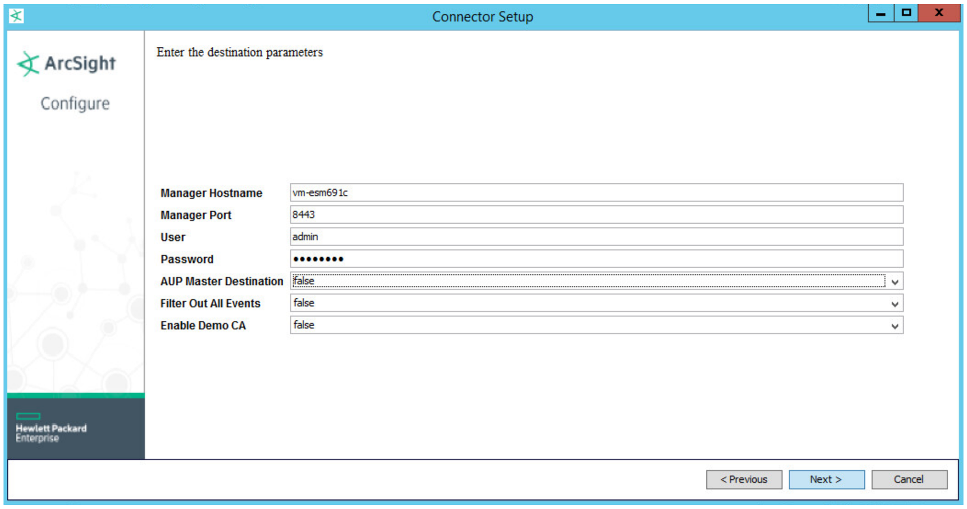
● ArcSight Manager (encrypted)
○ ArcSight Logger SmartMessage (encrypted)
○ ArcSight Logger SmartMessage Pool (encrypted)
○ CEF File
○ Event Broker (CEF Kafka)
○ CEF Syslog
○ CEF Encrypted Syslog (UDP)
○ CSV File
○ Raw Syslog

20. Click **Next**.

21. For **Manager Hostname**, put **vm-esm691c**, or the hostname of your ESM server.

22. For **Manager Port**, put **8443**, or the port that ESM is running on, on the ESM server.

23. Enter the **username** and **password** used for logging into ArcSight Command Center (admin/password).

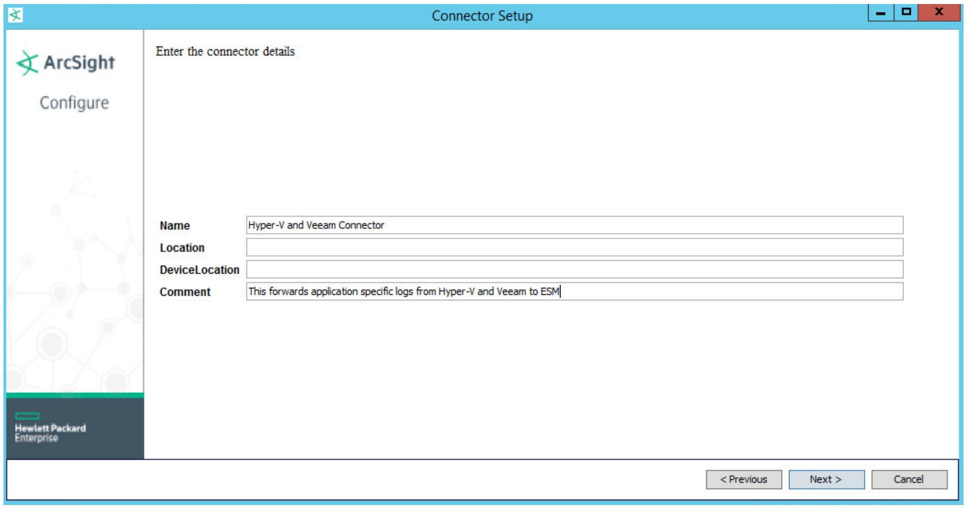


Connector Setup

Enter the destination parameters

Manager Hostname	vm-esm691c
Manager Port	8443
User	admin
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

24. Click **Next**.
25. Set identifying details about the system to help identify the connector (include at least **Name;** the rest is optional).

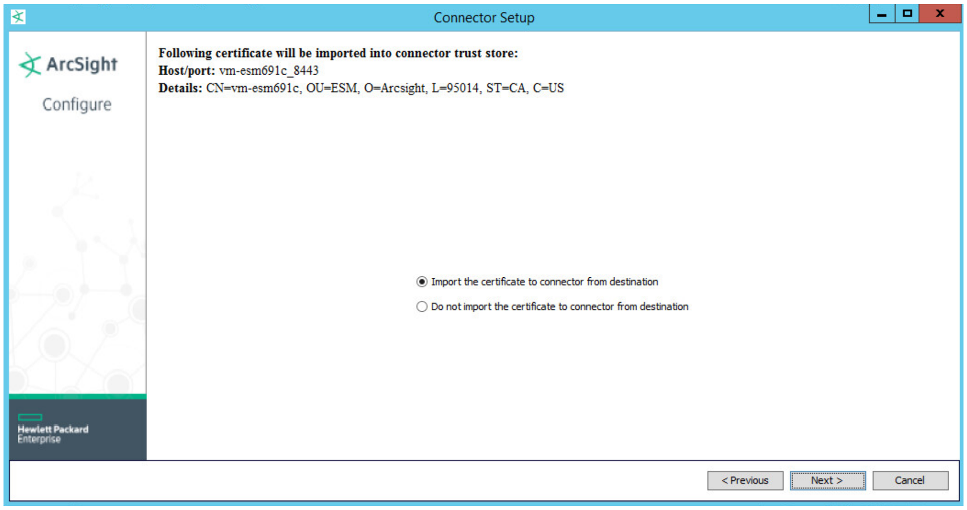


Connector Setup

Enter the connector details

Name	Hyper-V and Veeam Connector
Location	
DeviceLocation	
Comment	This forwards application specific logs from Hyper-V and Veeam to ESM

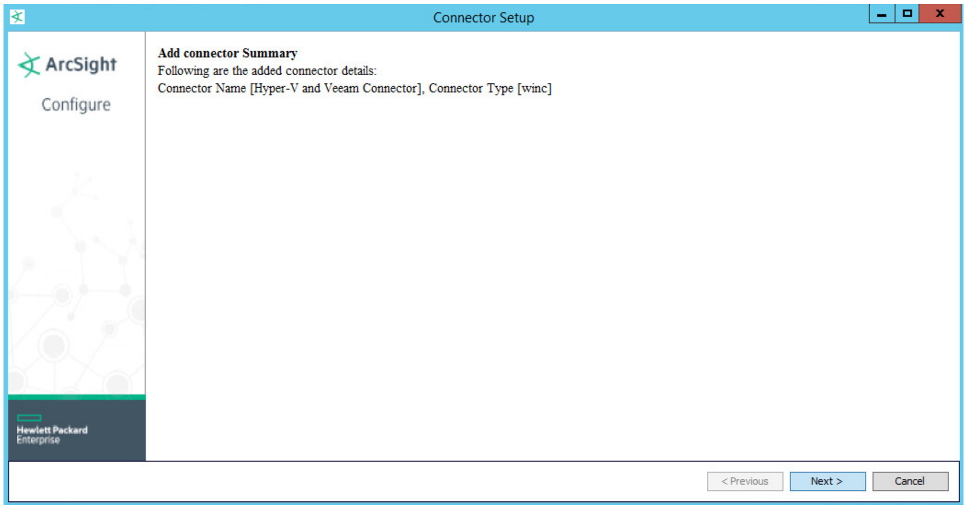
26. Click **Next**.
27. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the VM.



Following certificate will be imported into connector trust store:
Host/port: vm-esm691c_8443
Details: CN=vm-esm691c, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

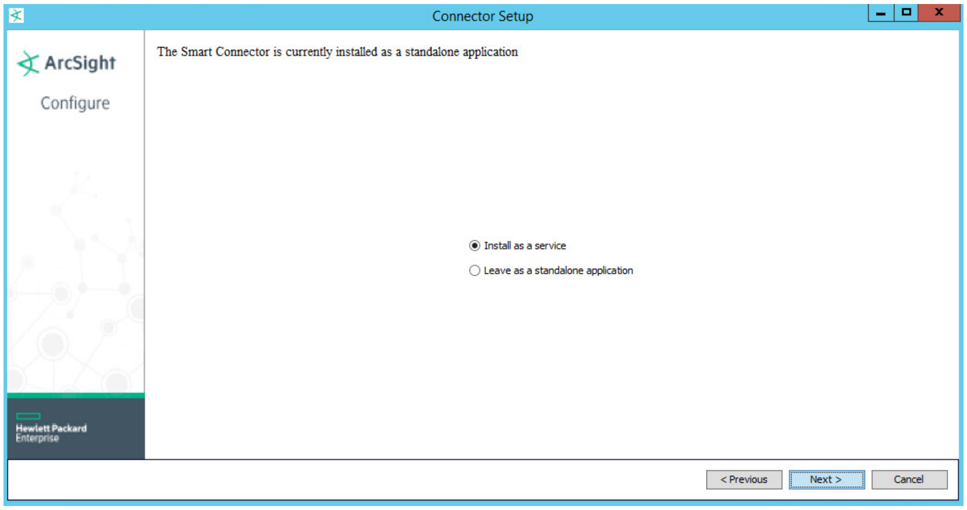
● Import the certificate to connector from destination
○ Do not import the certificate to connector from destination

28. Click **Next**.
29. Wait for the process to complete.



Add connector Summary
Following are the added connector details:
Connector Name [Hyper-V and Veeam Connector], Connector Type [winc]

30. Click **Next**.
31. Choose **Install as a service**.

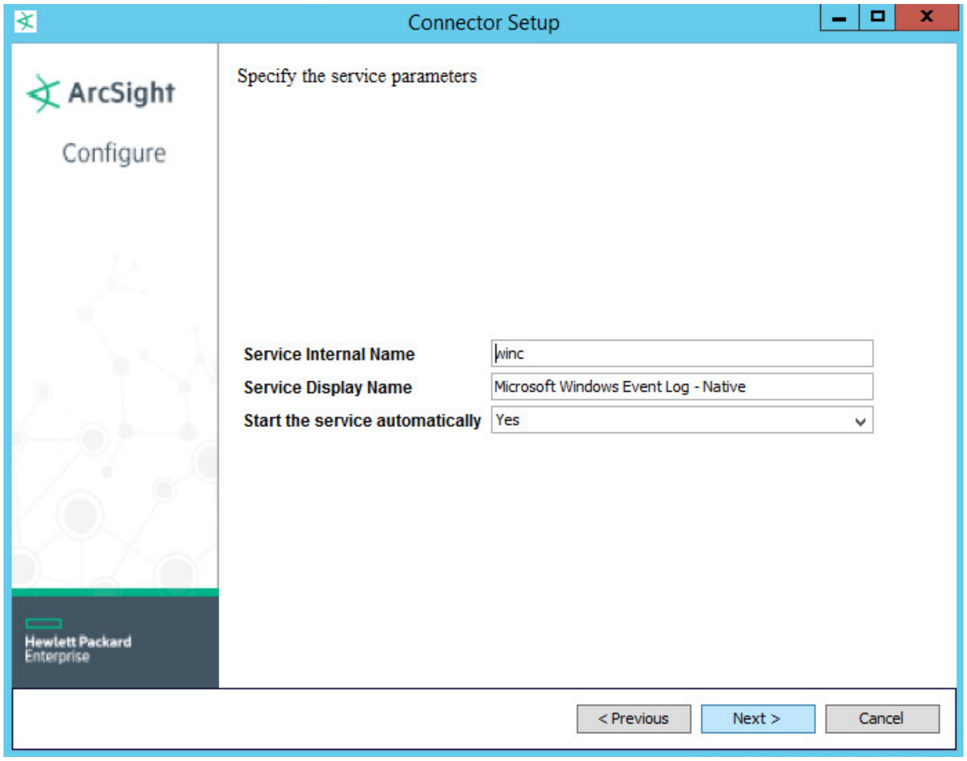


The Smart Connector is currently installed as a standalone application

● Install as a service

○ Leave as a standalone application

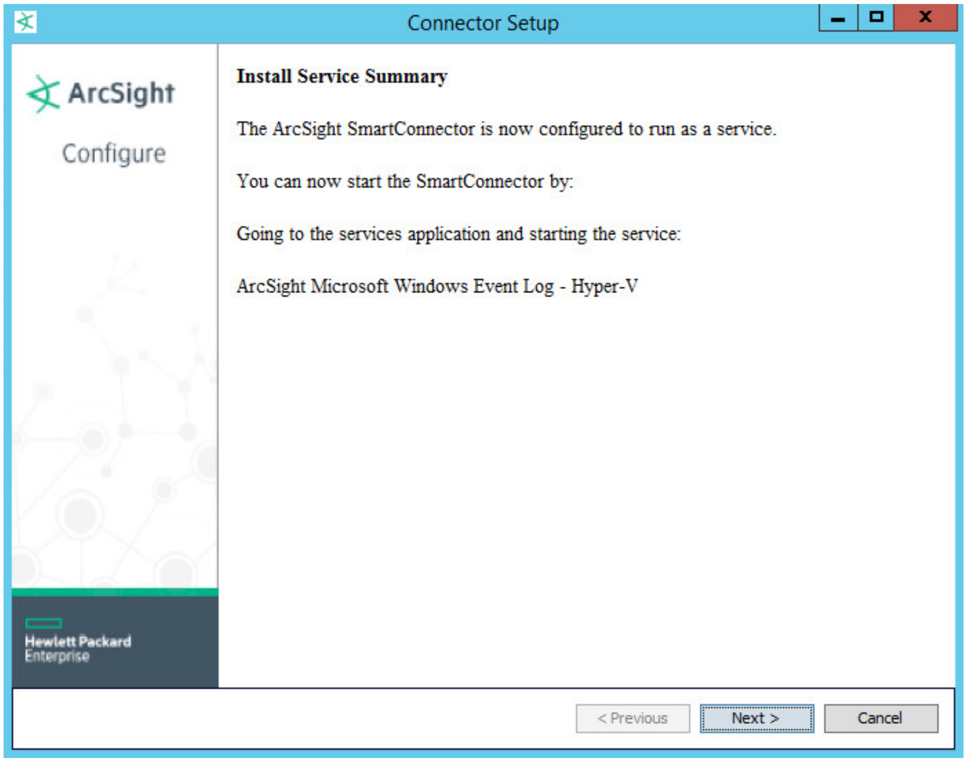
32. Click **Next**.



Specify the service parameters

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

33. Click **Next**.



Install Service Summary

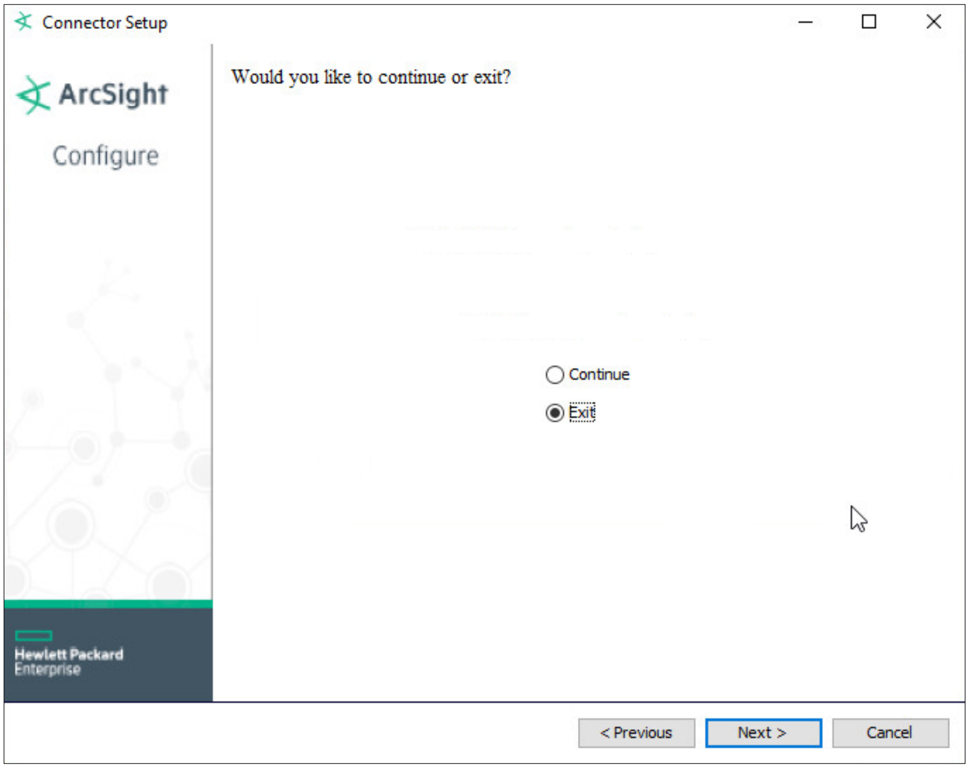
The ArcSight SmartConnector is now configured to run as a service.

You can now start the SmartConnector by:

Going to the services application and starting the service:

ArcSight Microsoft Windows Event Log - Hyper-V

34. Click **Next**.
35. Choose **Exit**.

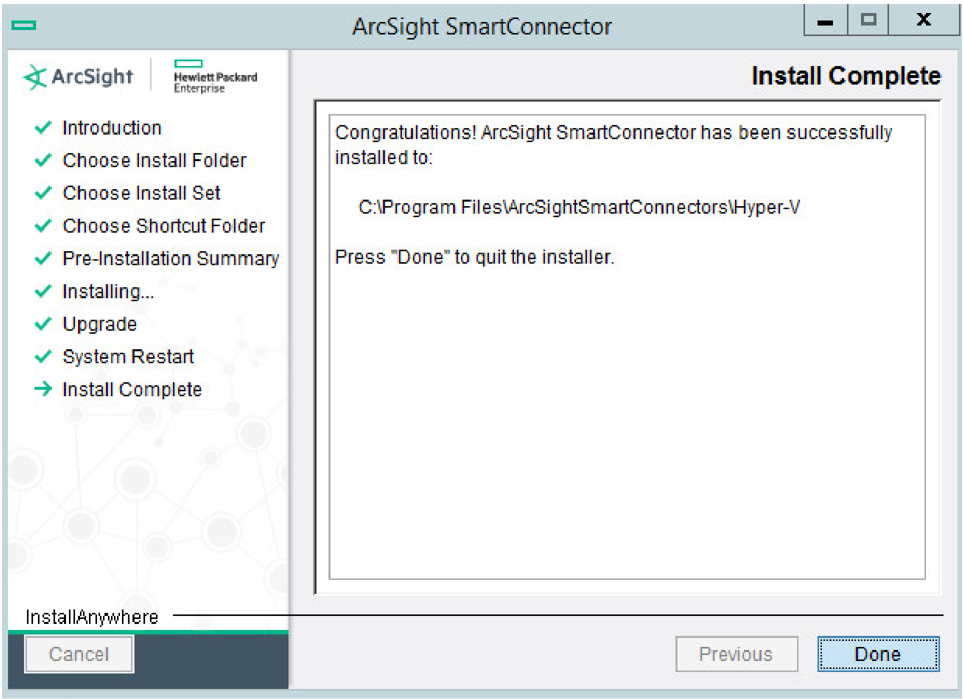


Would you like to continue or exit?

○ Continue

● Exit

36. Click **Next**.



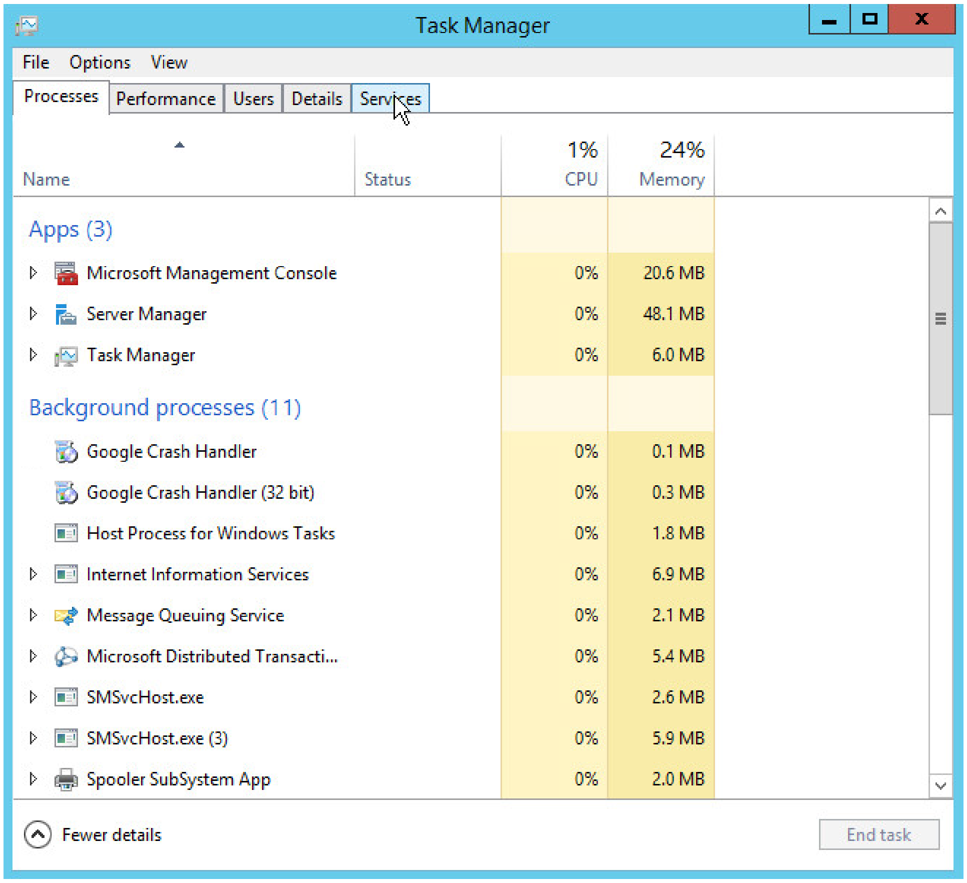
Install Complete

Congratulations! ArcSight SmartConnector has been successfully installed to:

C:\Program Files\ArcSightSmartConnectors\Hyper-V

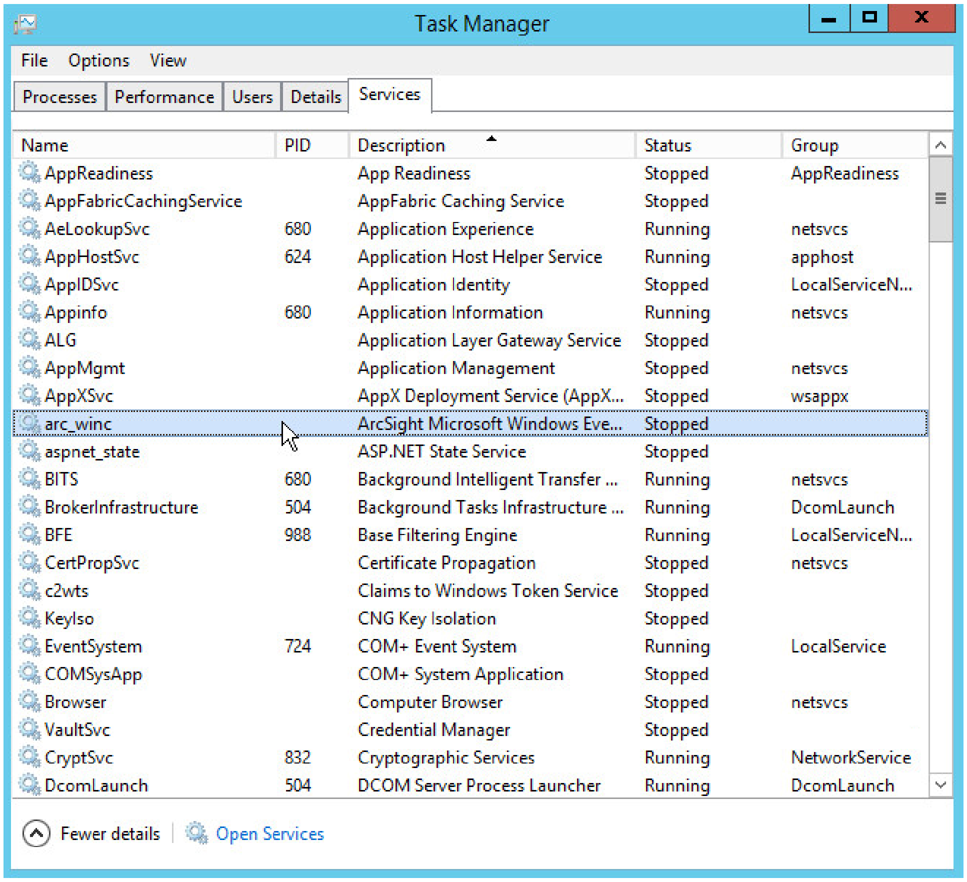
Press "Done" to quit the installer.

37. Click **Done**.
38. Open **Task Manager**.
39. Click **More Details**.



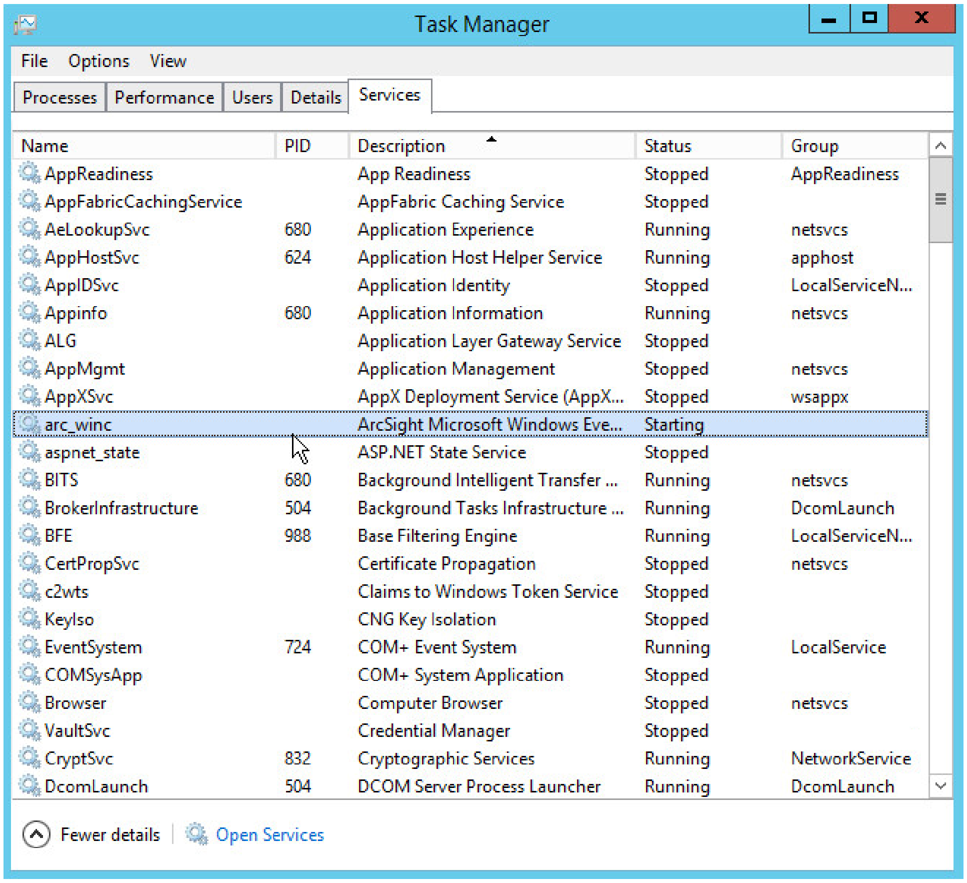
Name	Status	1% CPU	24% Memory
Apps (3)			
Microsoft Management Console		0%	20.6 MB
Server Manager		0%	48.1 MB
Task Manager		0%	6.0 MB
Background processes (11)			
Google Crash Handler		0%	0.1 MB
Google Crash Handler (32 bit)		0%	0.3 MB
Host Process for Windows Tasks		0%	1.8 MB
Internet Information Services		0%	6.9 MB
Message Queuing Service		0%	2.1 MB
Microsoft Distributed Transacti...		0%	5.4 MB
SMSvcHost.exe		0%	2.6 MB
SMSvcHost.exe (3)		0%	5.9 MB
Spooler SubSystem App		0%	2.0 MB

40. Go to the **Services** tab.
41. Find the service just created **arc_winc** for ArcSight, and right click it.



Name	PID	Description	Status	Group
AppReadiness		App Readiness	Stopped	AppReadiness
AppFabricCachingService		AppFabric Caching Service	Stopped	
AeLookupSvc	680	Application Experience	Running	netsvcs
AppHostSvc	624	Application Host Helper Service	Running	apphost
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo	680	Application Information	Running	netsvcs
ALG		Application Layer Gateway Service	Stopped	
AppMgmt		Application Management	Stopped	netsvcs
AppXSvc		AppX Deployment Service (AppX...	Stopped	wsappx
arc_winc		ArcSight Microsoft Windows Eve...	Stopped	
aspnet_state		ASP.NET State Service	Stopped	
BITS	680	Background Intelligent Transfer ...	Running	netsvcs
BrokerInfrastructure	504	Background Tasks Infrastructure ...	Running	DcomLaunch
BFE	988	Base Filtering Engine	Running	LocalServiceN...
CertPropSvc		Certificate Propagation	Stopped	netsvcs
c2wts		Claims to Windows Token Service	Stopped	
KeyIso		CNG Key Isolation	Stopped	
EventSystem	724	COM+ Event System	Running	LocalService
COMSysApp		COM+ System Application	Stopped	
Browser		Computer Browser	Stopped	netsvcs
VaultSvc		Credential Manager	Stopped	
CryptSvc	832	Cryptographic Services	Running	NetworkService
DcomLaunch	504	DCOM Server Process Launcher	Running	DcomLaunch

42. Choose **Start**.



Name	PID	Description	Status	Group
AppReadiness		App Readiness	Stopped	AppReadiness
AppFabricCachingService		AppFabric Caching Service	Stopped	
AeLookupSvc	680	Application Experience	Running	netsvcs
AppHostSvc	624	Application Host Helper Service	Running	apphost
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo	680	Application Information	Running	netsvcs
ALG		Application Layer Gateway Service	Stopped	
AppMgmt		Application Management	Stopped	netsvcs
AppXSvc		AppX Deployment Service (AppX...	Stopped	wsappx
arc_winc		ArcSight Microsoft Windows Eve...	Starting	
aspnet_state		ASP.NET State Service	Stopped	
BITS	680	Background Intelligent Transfer ...	Running	netsvcs
BrokerInfrastructure	504	Background Tasks Infrastructure ...	Running	DcomLaunch
BFE	988	Base Filtering Engine	Running	LocalServiceN...
CertPropSvc		Certificate Propagation	Stopped	netsvcs
c2wts		Claims to Windows Token Service	Stopped	
KeyIso		CNG Key Isolation	Stopped	
EventSystem	724	COM+ Event System	Running	LocalService
COMSysApp		COM+ System Application	Stopped	
Browser		Computer Browser	Stopped	netsvcs
VaultSvc		Credential Manager	Stopped	
CryptSvc	832	Cryptographic Services	Running	NetworkService
DcomLaunch	504	DCOM Server Process Launcher	Running	DcomLaunch

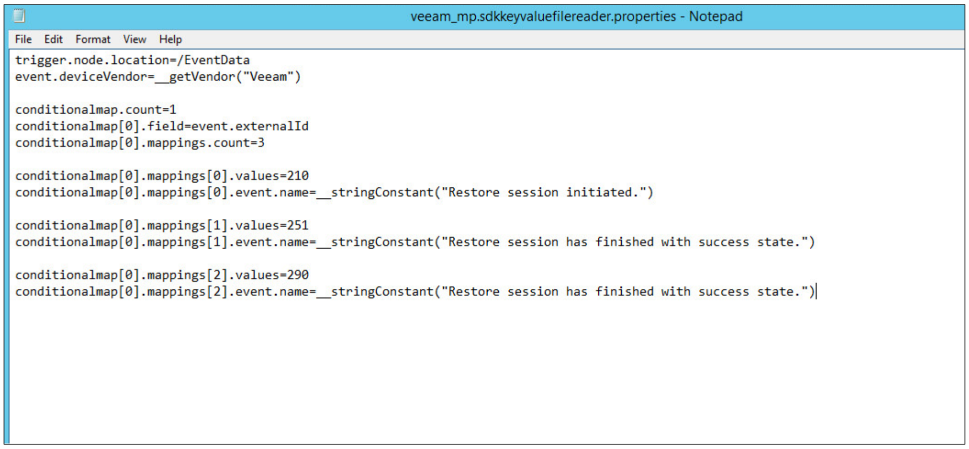
43. The machine will now report its logs to ArcSight ESM.
44. For more fine-grained reporting, such as including more information about the event, you may wish to include custom parsers that are described below.

2.12.2 Create a Parser for Veeam Logs

1. For a Veeam custom parser that handles event numbers **210**, **251**, and **290**, create a configuration file with the following text:

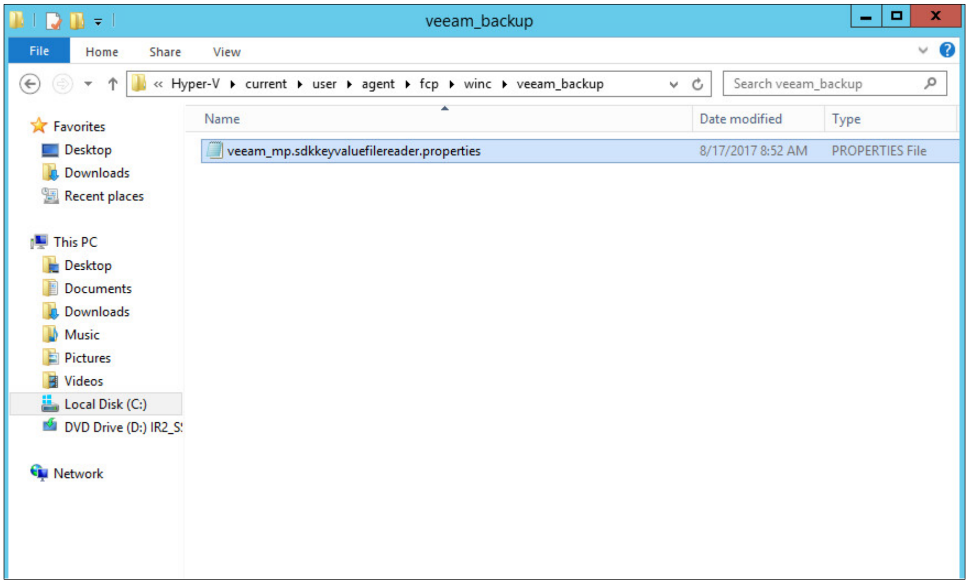
```
trigger.node.location=/EventData

event.deviceVendor=__getVendor("Veeam")

conditionalmap.count=1

conditionalmap[0].field=event.externalId

conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=210
```

```
conditionalmap[0].mappings[0].event.name=__stringConstant("Restore session
initiated.")

conditionalmap[0].mappings[1].values=251

conditionalmap[0].mappings[1].event.name=__stringConstant("Restore session
has finished with success state.")

conditionalmap[0].mappings[2].values=290

conditionalmap[0].mappings[2].event.name=__stringConstant("Restore session
has finished with success state.")
```



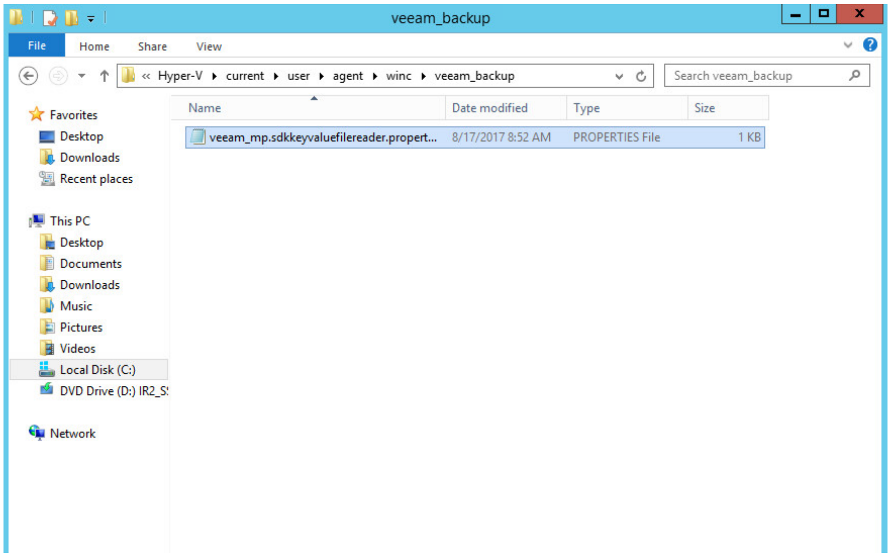
```
trigger.node.location=/EventData
event.deviceVendor=__getVendor("Veeam")

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=210
conditionalmap[0].mappings[0].event.name=__stringConstant("Restore session initiated.")

conditionalmap[0].mappings[1].values=251
conditionalmap[0].mappings[1].event.name=__stringConstant("Restore session has finished with success state.")

conditionalmap[0].mappings[2].values=290
conditionalmap[0].mappings[2].event.name=__stringConstant("Restore session has finished with success state.")
```

2. Save this file as *C:\Program Files\ArcSightSmartConnectors\<name of folder>\current\user\agent\fcp\winc\veeam_backup\veeam_mp.sdkkeyvaluefilereader.properties*



Name	Date modified	Type
veeam_mp.sdkkeyvaluefilereader.properties	8/17/2017 8:52 AM	PROPERTIES File

3. Copy this file to *C:\Program Files\ArcSightSmartConnectors\<name of folder>\current\user\agent\winc\veeam_backup\veeam_mp.sdkkeyvaluefilereader.properties*

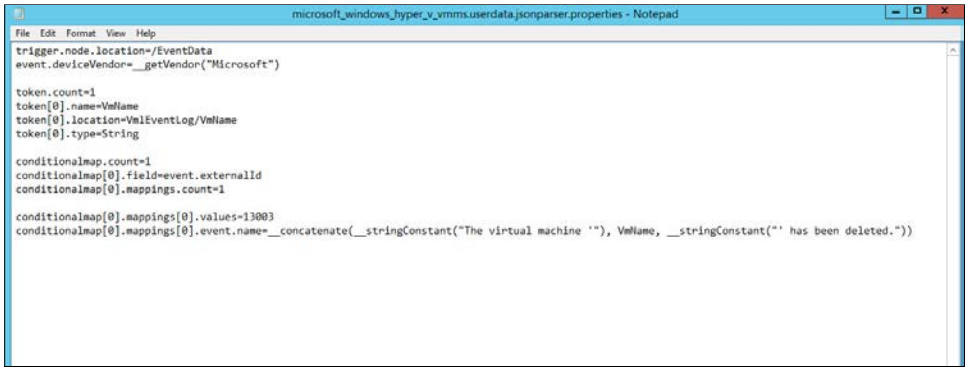


Name	Date modified	Type	Size
veeam_mp.sdkkeyvaluefilereader.propert...	8/17/2017 8:52 AM	PROPERTIES File	1 KB

2.12.3 Create a Parser for Hyper-V Logs

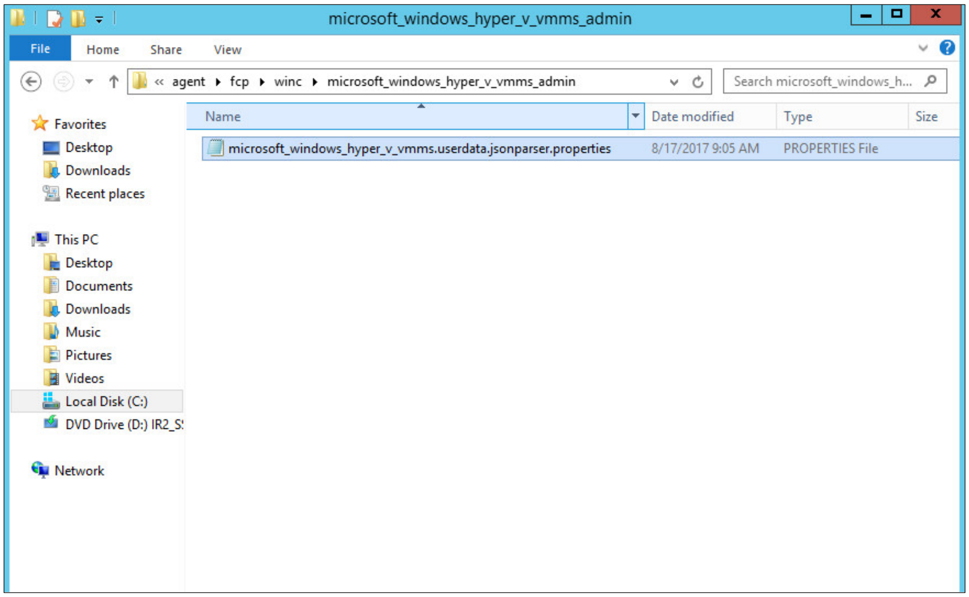
1. For a Hyper-V VMMS custom parser, create a configuration file with the following text:

```
trigger.node.location=/EventData

event.deviceVendor=__getVendor("Microsoft")

token.count=1

token[0].name=VmName

token[0].location=VmlEventLog/VmName

token[0].type=String

conditionalmap.count=1

conditionalmap[0].field=event.externalId

conditionalmap[0].mappings.count=1

conditionalmap[0].mappings[0].values=13003

conditionalmap[0].mappings[0].event.name=__concatenate(__stringConstant("The
virtual machine '"), VmName, __stringConstant("' has been deleted."))
```


microsoft_windows_hyper_v_vmms.userdata.jsonparser.properties - Notepad
File Edit Format View Help

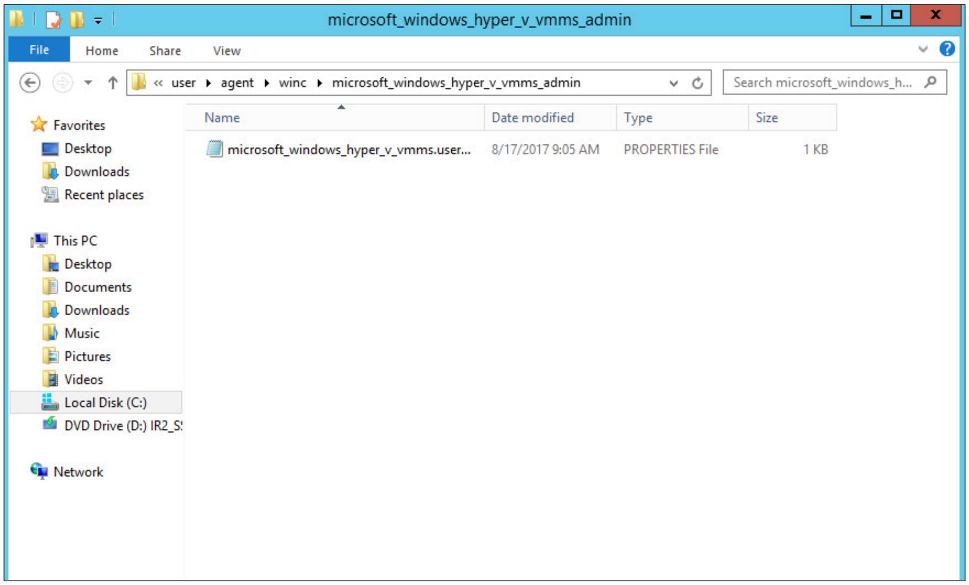
```
trigger.node.location=/EventData
event.deviceVendor=__getVendor("Microsoft")

token.count=1
token[0].name=VmName
token[0].location=VmlEventLog/VmName
token[0].type=String

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=1

conditionalmap[0].mappings[0].values=13003
conditionalmap[0].mappings[0].event.name=__concatenate(__stringConstant("The virtual machine '"), VmName, __stringConstant("' has been deleted."))
```

2. Save this file as *C:\Program Files\ArcSightSmartConnectors\<name of folder>\current\user\agent\fcp\winc\microsoft_windows_hyper_v_vmms_admin\microsoft_windows_hyper_v_vmms.userdata.jsonparser.properties*



Name	Date modified	Type	Size
microsoft_windows_hyper_v_vmms.userdata.jsonparser.properties	8/17/2017 9:05 AM	PROPERTIES File	

3. Copy this file to *C:\Program Files\ArcSightSmartConnectors\<name of folder>\current\user\agent\winc\microsoft_windows_hyper_v_vmms_admin\microsoft_windows_hyper_v_vmms.userdata.jsonparser.properties*



Name	Date modified	Type	Size
microsoft_windows_hyper_v_vmms.user...	8/17/2017 9:05 AM	PROPERTIES File	1 KB

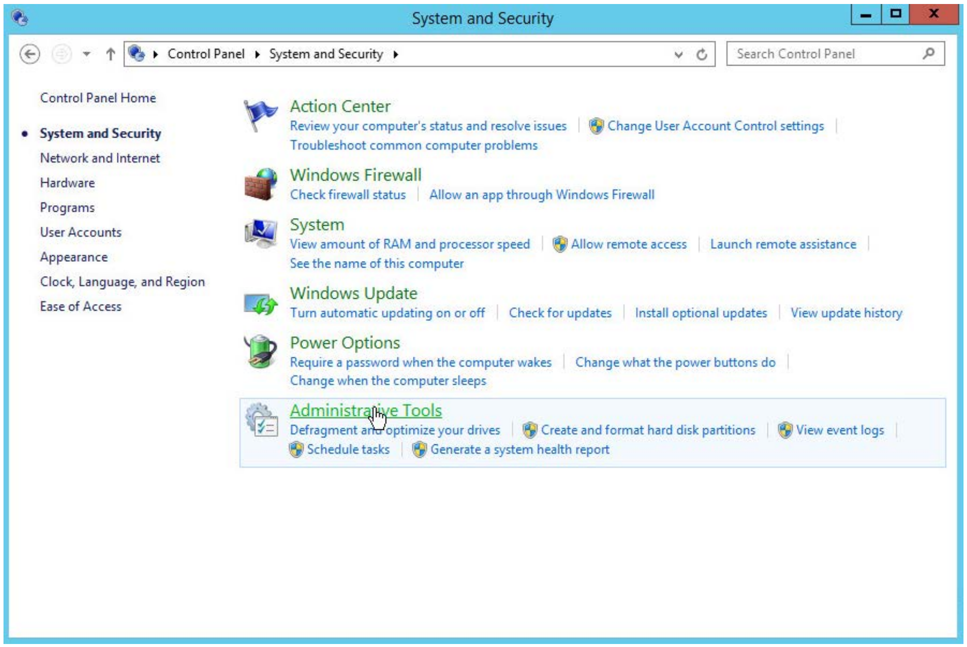
These two parsers will allow for details of VM deletions and VM restores to be shown in ArcSight. Custom parsers are a functionality of ArcSight. For more information on the creation of custom parsers, please see the *ArcSight FlexConnector Developer's Guide*, as well as the *SmartConnector for Microsoft Windows Event Log - Native, Configuration Guide* (for information specific to Windows event logs).

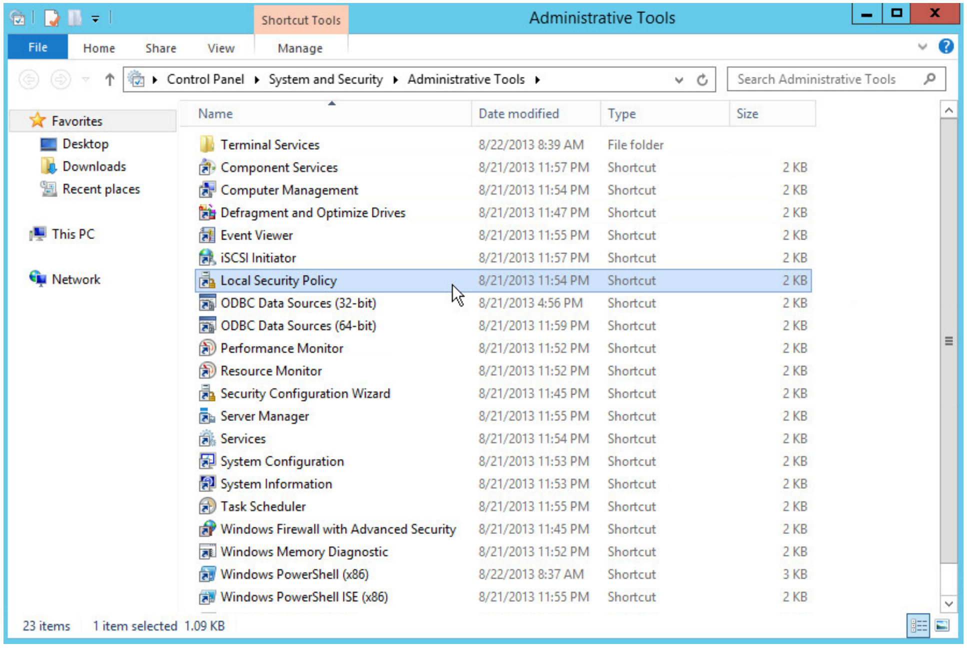
2.13 Integration: GreenTec WORMdisks and IBM Spectrum Protect

This section covers the process for integrating IBM Spectrum Protect and GreenTec WORMdisks. The result is the capability to back up clients directly to WORMdisks in order to preserve data more securely. This integration process does not include instructions related to locking the WORMdisks – that process is found in the *GT_WinStatus User Guide,* that should accompany the installation disk. Scheduling the locking of these disks is left up to the discretion of the adapting organization.

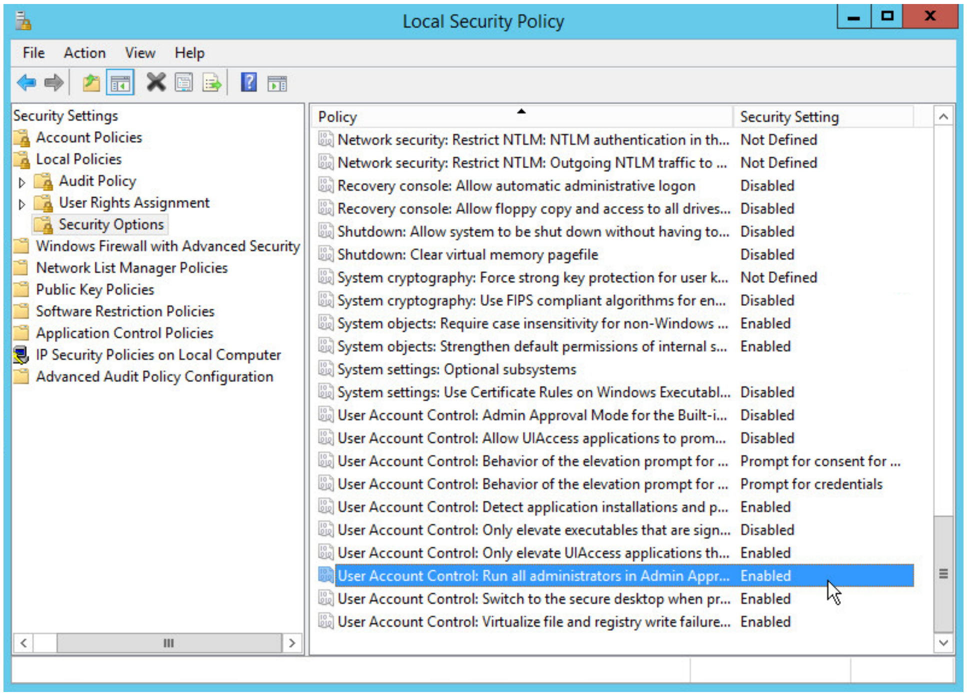
2.13.1 Install IBM Spectrum Protect Server on the GreenTec Server

1. You may need to disable **Run all administrators in Admin Approval Mode**. To do this go to **Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options**. Double click the **User Account Control: Run all administrators in Admin Approval Mode** section. Select **Disable** and click **OK**. Restart the computer.

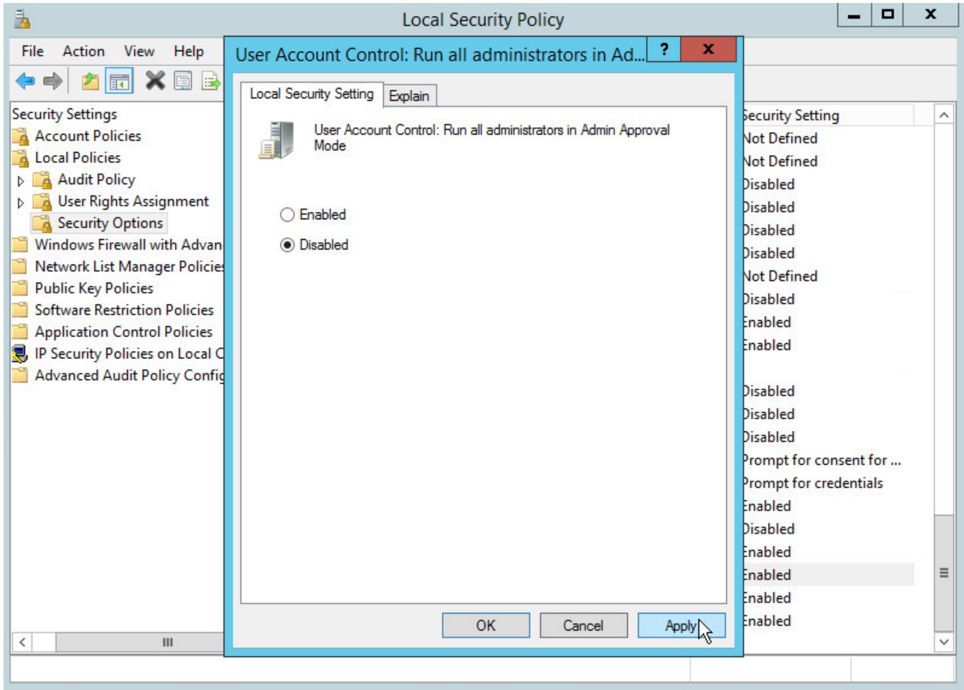

System and Security
Control Panel ▸ System and Security ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems
Windows Firewall
Check firewall status | Allow an app through Windows Firewall
System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer
Windows Update
Turn automatic updating on or off | Check for updates | Install optional updates | View update history
Power Options
Require a password when the computer wakes | Change what the power buttons do | Change when the computer sleeps
Administrative Tools
Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks | Generate a system health report


Shortcut Tools
Administrative Tools
File
Home
Share
View
Manage
Control Panel ▸ System and Security ▸ Administrative Tools ▸
Search Administrative Tools
Favorites
Desktop
Downloads
Recent places
This PC
Network
23 items 1 item selected 1.09 KB

Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Security Configuration Wizard	8/21/2013 11:45 PM	Shortcut	2 KB
Server Manager	8/21/2013 11:55 PM	Shortcut	2 KB
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:53 PM	Shortcut	2 KB
System Information	8/21/2013 11:53 PM	Shortcut	2 KB
Task Scheduler	8/21/2013 11:55 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	8/21/2013 11:45 PM	Shortcut	2 KB
Windows Memory Diagnostic	8/21/2013 11:52 PM	Shortcut	2 KB
Windows PowerShell (x86)	8/22/2013 8:37 AM	Shortcut	3 KB
Windows PowerShell ISE (x86)	8/21/2013 11:55 PM	Shortcut	2 KB


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executabl...	Disabled
User Account Control: Admin Approval Mode for the Built-i...	Disabled
User Account Control: Allow UIAccess applications to prom...	Disabled
User Account Control: Behavior of the elevation prompt for ...	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials
User Account Control: Detect application installations and p...	Enabled
User Account Control: Only elevate executables that are sign...	Disabled
User Account Control: Only elevate UIAccess applications th...	Enabled
User Account Control: Run all administrators in Admin Appr...	Enabled
User Account Control: Switch to the secure desktop when pr...	Enabled
User Account Control: Virtualize file and registry write failure...	Enabled



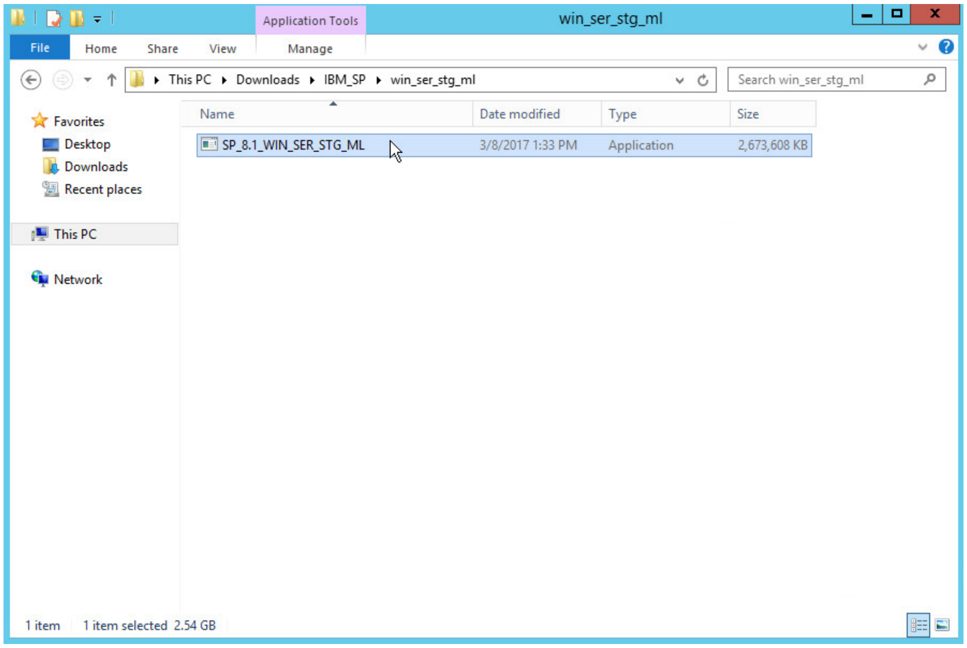
User Account Control: Run all administrators in Ad...

User Account Control: Run all administrators in Admin Approval Mode

○ Enabled

● Disabled

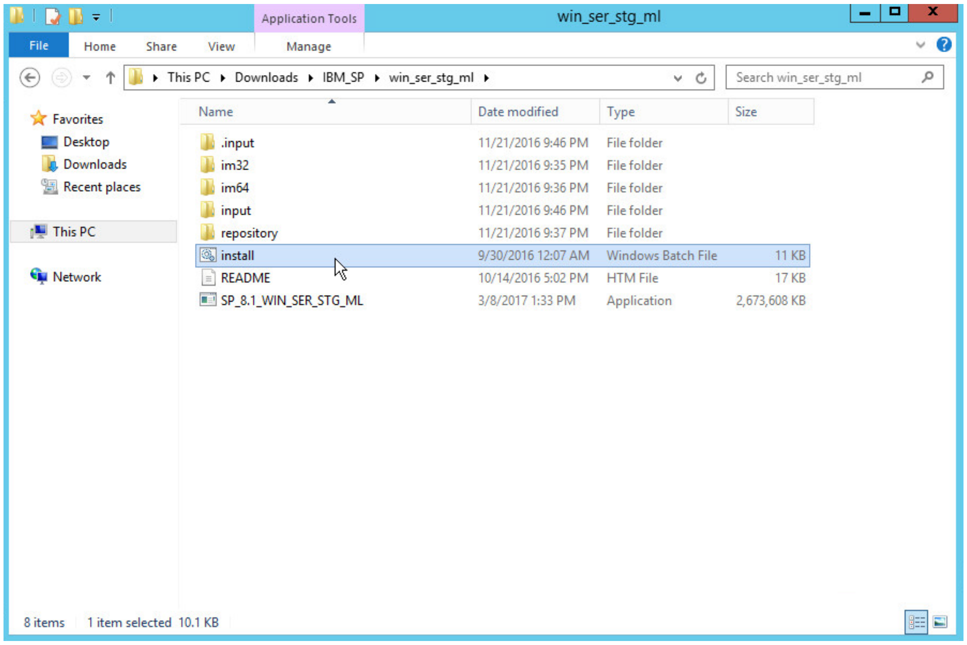
2. Run **WIN_SER_STG_ML** in its own folder to extract the contents.



Name	Date modified	Type	Size
SP_8.1_WIN_SER_STG_ML	3/8/2017 1:33 PM	Application	2,673,608 KB

1 item 1 item selected 2.54 GB

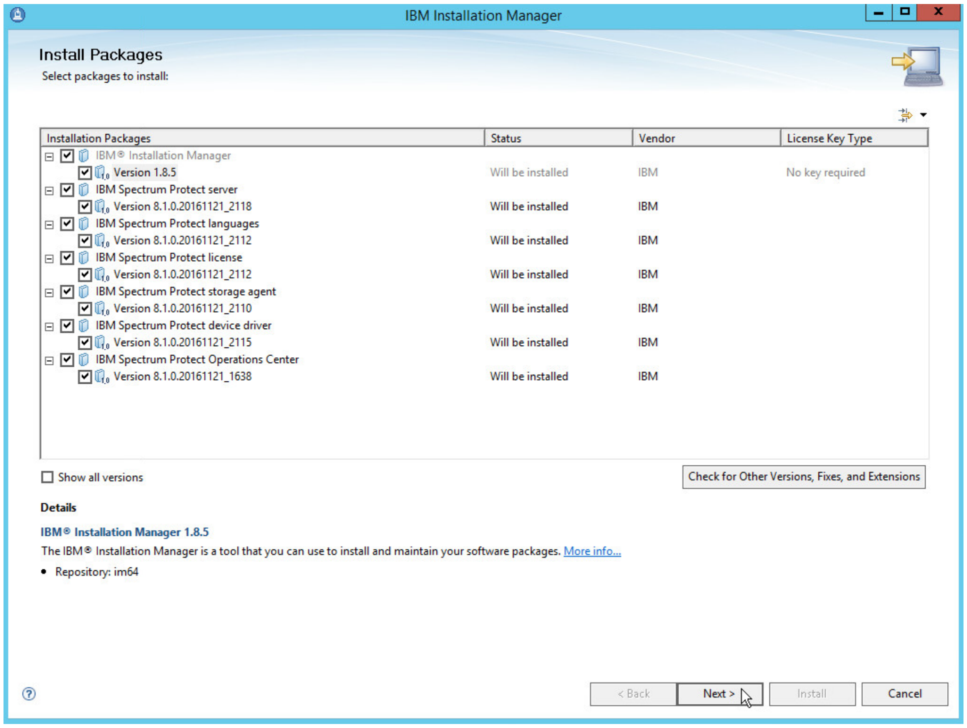
3. Run the **install** script.



Name	Date modified	Type	Size
.input	11/21/2016 9:46 PM	File folder	
im32	11/21/2016 9:35 PM	File folder	
im64	11/21/2016 9:36 PM	File folder	
input	11/21/2016 9:46 PM	File folder	
repository	11/21/2016 9:37 PM	File folder	
install	9/30/2016 12:07 AM	Windows Batch File	11 KB
README	10/14/2016 5:02 PM	HTM File	17 KB
SP_8.1_WIN_SER_STG_ML	3/8/2017 1:33 PM	Application	2,673,608 KB

8 items 1 item selected 10.1 KB

4. Make sure all the boxes are checked.


IBM Installation Manager

Install Packages

Select packages to install:

Installation Packages	Status	Vendor	License Key Type
☑ IBM® Installation Manager			
☑ Version 1.8.5	Will be installed	IBM	No key required
☑ IBM Spectrum Protect server			
☑ Version 8.1.0.20161121_2118	Will be installed	IBM	
☑ IBM Spectrum Protect languages			
☑ Version 8.1.0.20161121_2112	Will be installed	IBM	
☑ IBM Spectrum Protect license			
☑ Version 8.1.0.20161121_2112	Will be installed	IBM	
☑ IBM Spectrum Protect storage agent			
☑ Version 8.1.0.20161121_2110	Will be installed	IBM	
☑ IBM Spectrum Protect device driver			
☑ Version 8.1.0.20161121_2115	Will be installed	IBM	
☑ IBM Spectrum Protect Operations Center			
☑ Version 8.1.0.20161121_1638	Will be installed	IBM	

□ Show all versions

Check for Other Versions, Fixes, and Extensions

Details

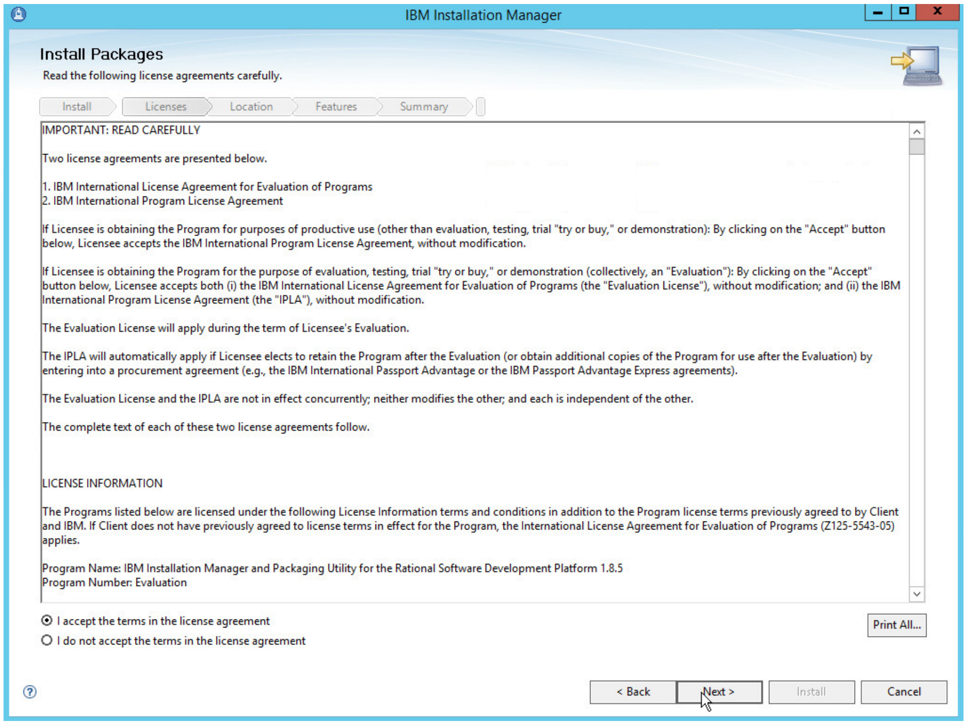
IBM® Installation Manager 1.8.5

The IBM® Installation Manager is a tool that you can use to install and maintain your software packages. More info...

- Repository: im64

< Back | Next > | Install | Cancel

5. Click **Next**.
6. Read and select **I accept the terms in the license agreement**.


IBM Installation Manager

Install Packages

Read the following license agreements carefully.

IMPORTANT: READ CAREFULLY

Two license agreements are presented below.

1. IBM International License Agreement for Evaluation of Programs
2. IBM International Program License Agreement

If Licensee is obtaining the Program for purposes of productive use (other than evaluation, testing, trial "try or buy," or demonstration): By clicking on the "Accept" button below, Licensee accepts the IBM International Program License Agreement, without modification.

If Licensee is obtaining the Program for the purpose of evaluation, testing, trial "try or buy," or demonstration (collectively, an "Evaluation"): By clicking on the "Accept" button below, Licensee accepts both (i) the IBM International License Agreement for Evaluation of Programs (the "Evaluation License"), without modification; and (ii) the IBM International Program License Agreement (the "IPLA"), without modification.

The Evaluation License will apply during the term of Licensee's Evaluation.

The IPLA will automatically apply if Licensee elects to retain the Program after the Evaluation (or obtain additional copies of the Program for use after the Evaluation) by entering into a procurement agreement (e.g., the IBM International Passport Advantage or the IBM Passport Advantage Express agreements).

The Evaluation License and the IPLA are not in effect concurrently; neither modifies the other; and each is independent of the other.

The complete text of each of these two license agreements follow.

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International License Agreement for Evaluation of Programs (Z125-5543-05) applies.

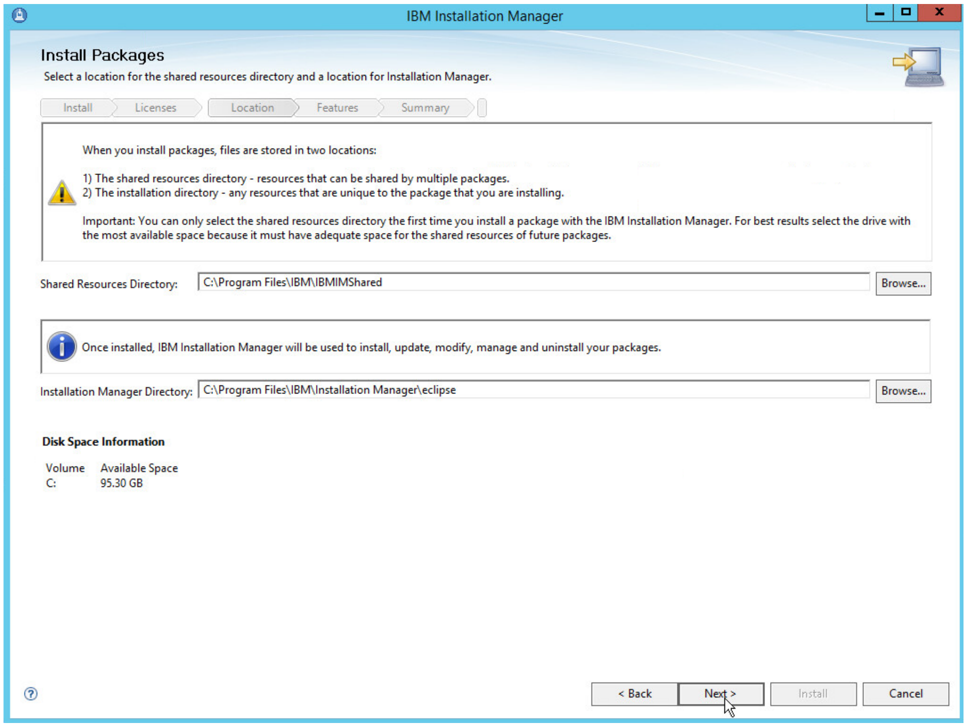
Program Name: IBM Installation Manager and Packaging Utility for the Rational Software Development Platform 1.8.5
Program Number: Evaluation

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

Print All...

< Back | Next > | Install | Cancel

7. Click **Next**.
8. Select the installation location for files.



IBM Installation Manager

Install Packages

Select a location for the shared resources directory and a location for Installation Manager.

When you install packages, files are stored in two locations:

1) The shared resources directory - resources that can be shared by multiple packages.
2) The installation directory - any resources that are unique to the package that you are installing.

Important: You can only select the shared resources directory the first time you install a package with the IBM Installation Manager. For best results select the drive with the most available space because it must have adequate space for the shared resources of future packages.

Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

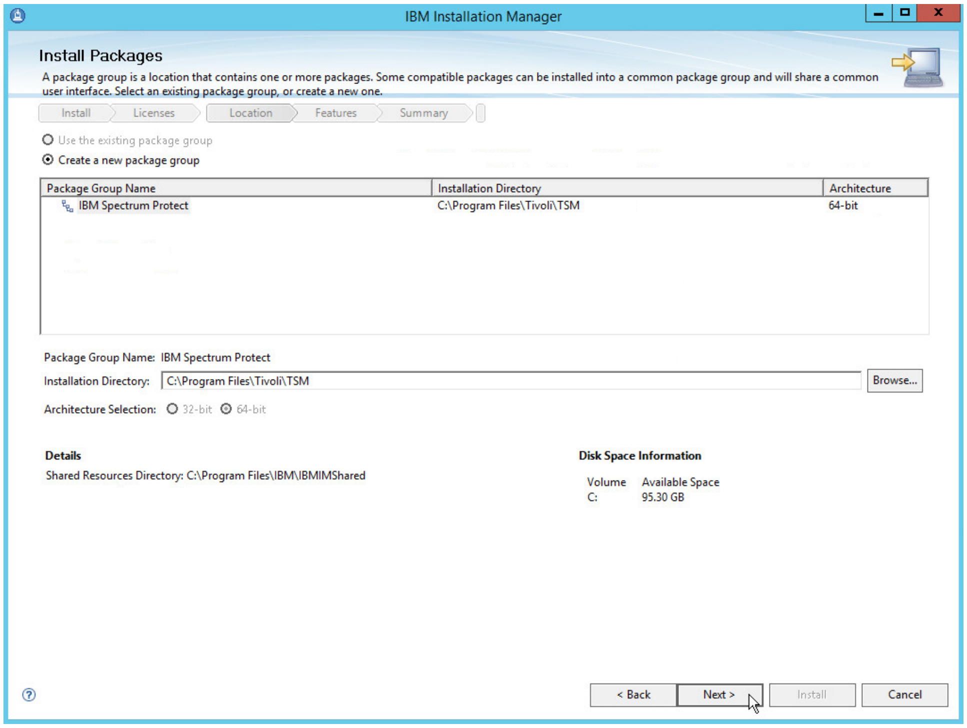
Once installed, IBM Installation Manager will be used to install, update, modify, manage and uninstall your packages.

Installation Manager Directory: C:\Program Files\IBM\Installation Manager\eclipse

Disk Space Information

Volume	Available Space
C:	95.30 GB

9. Click **Next**.


IBM Installation Manager
Install Packages
A package group is a location that contains one or more packages. Some compatible packages can be installed into a common package group and will share a common user interface. Select an existing package group, or create a new one.
Install
Licenses
Location
Features
Summary
○ Use the existing package group
● Create a new package group

Package Group Name	Installation Directory	Architecture
IBM Spectrum Protect	C:\Program Files\Tivoli\TSM	64-bit

Package Group Name: IBM Spectrum Protect

Installation Directory: C:\Program Files\Tivoli\TSM

Architecture Selection: ○ 32-bit ● 64-bit

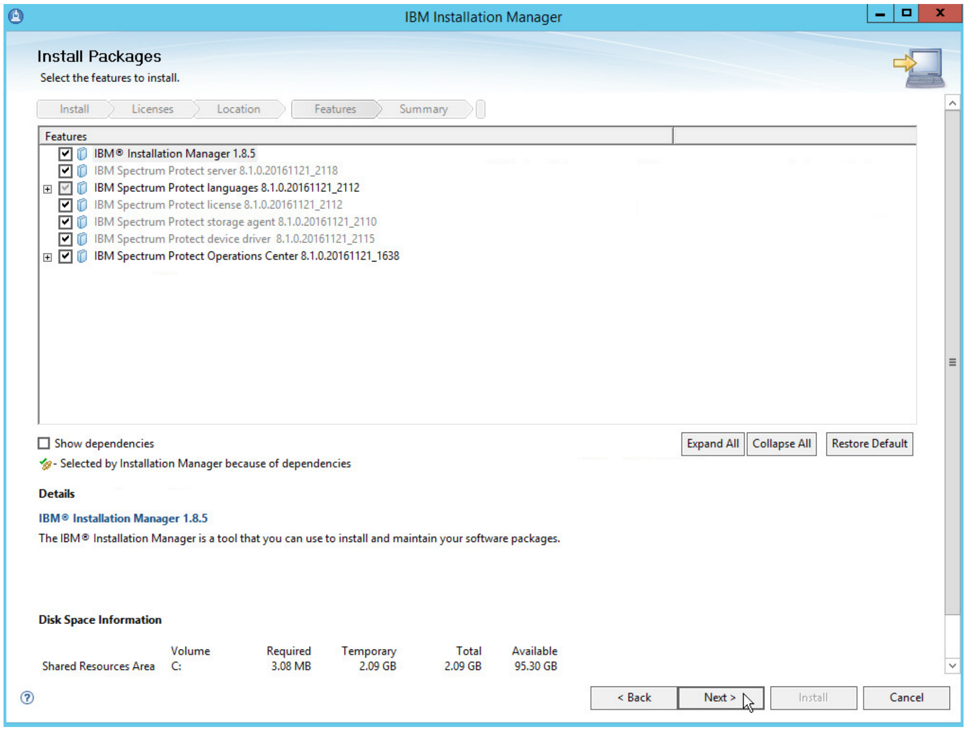
Details

Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

Disk Space Information

Volume	Available Space
C:	95.30 GB

10. Click **Next**.
11. Make sure all the packages are checked.



Features

- ☑ IBM® Installation Manager 1.8.5
- ☑ IBM Spectrum Protect server 8.1.0.20161121_2118
- ☑ IBM Spectrum Protect languages 8.1.0.20161121_2112
- ☑ IBM Spectrum Protect license 8.1.0.20161121_2112
- ☑ IBM Spectrum Protect storage agent 8.1.0.20161121_2110
- ☑ IBM Spectrum Protect device driver 8.1.0.20161121_2115
- ☑ IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

☐ Show dependencies

- Selected by Installation Manager because of dependencies

Details

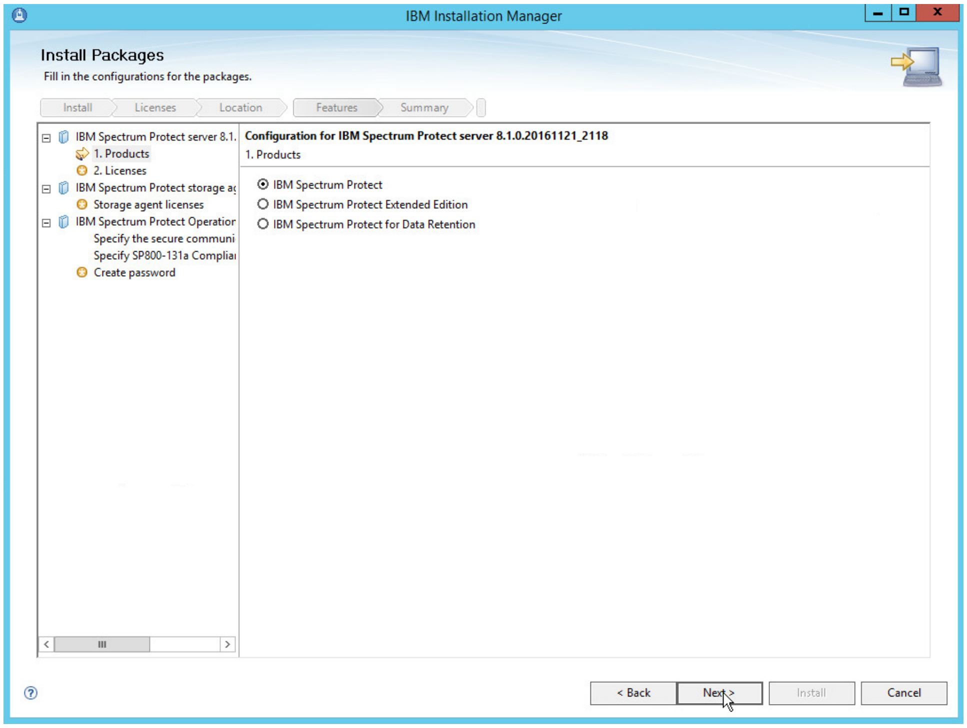
IBM® Installation Manager 1.8.5

The IBM® Installation Manager is a tool that you can use to install and maintain your software packages.

Disk Space Information

	Volume	Required	Temporary	Total	Available
Shared Resources Area	C:	3.08 MB	2.09 GB	2.09 GB	95.30 GB

12. Click **Next**.
13. Select **IBM Spectrum Protect**.

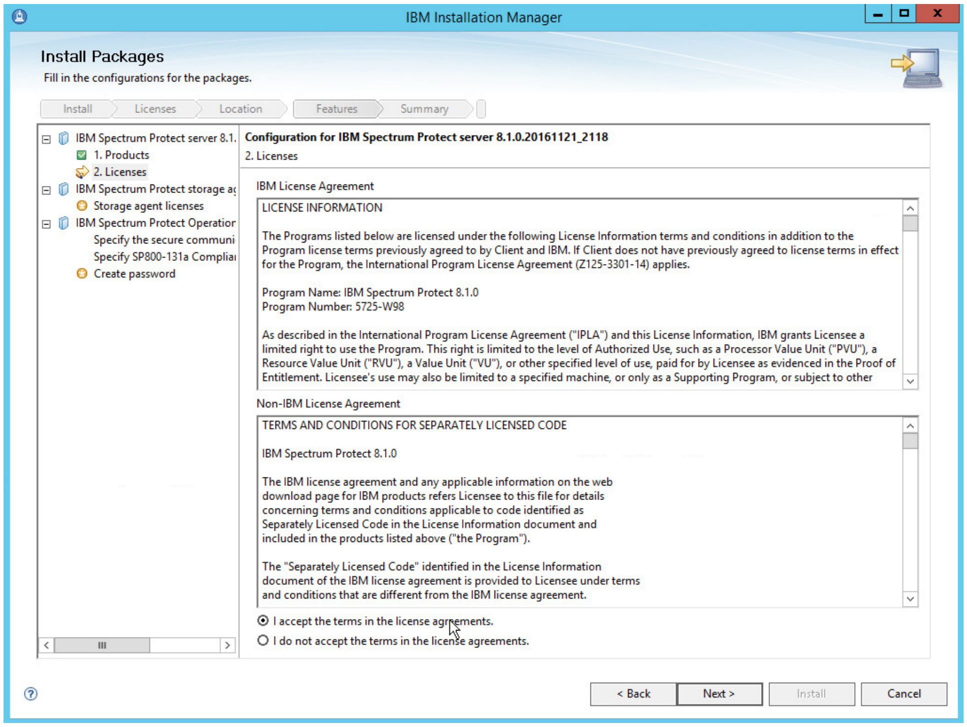

IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage ag
Storage agent licenses
IBM Spectrum Protect Operation
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect server 8.1.0.20161121_2118

1. Products

● IBM Spectrum Protect
○ IBM Spectrum Protect Extended Edition
○ IBM Spectrum Protect for Data Retention

14. Click **Next**.
15. Read and select **I accept the terms in the license agreement**.


IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage ag
Storage agent licenses
IBM Spectrum Protect Operation
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect server 8.1.0.20161121_2118

2. Licenses

IBM License Agreement

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International Program License Agreement (Z125-3301-14) applies.

Program Name: IBM Spectrum Protect 8.1.0
Program Number: 5725-W98

As described in the International Program License Agreement ("IPLA") and this License Information, IBM grants Licensee a limited right to use the Program. This right is limited to the level of Authorized Use, such as a Processor Value Unit ("PVU"), a Resource Value Unit ("RVU"), a Value Unit ("VU"), or other specified level of use, paid for by Licensee as evidenced in the Proof of Entitlement. Licensee's use may also be limited to a specified machine, or only as a Supporting Program, or subject to other

Non-IBM License Agreement

TERMS AND CONDITIONS FOR SEPARATELY LICENSED CODE

IBM Spectrum Protect 8.1.0

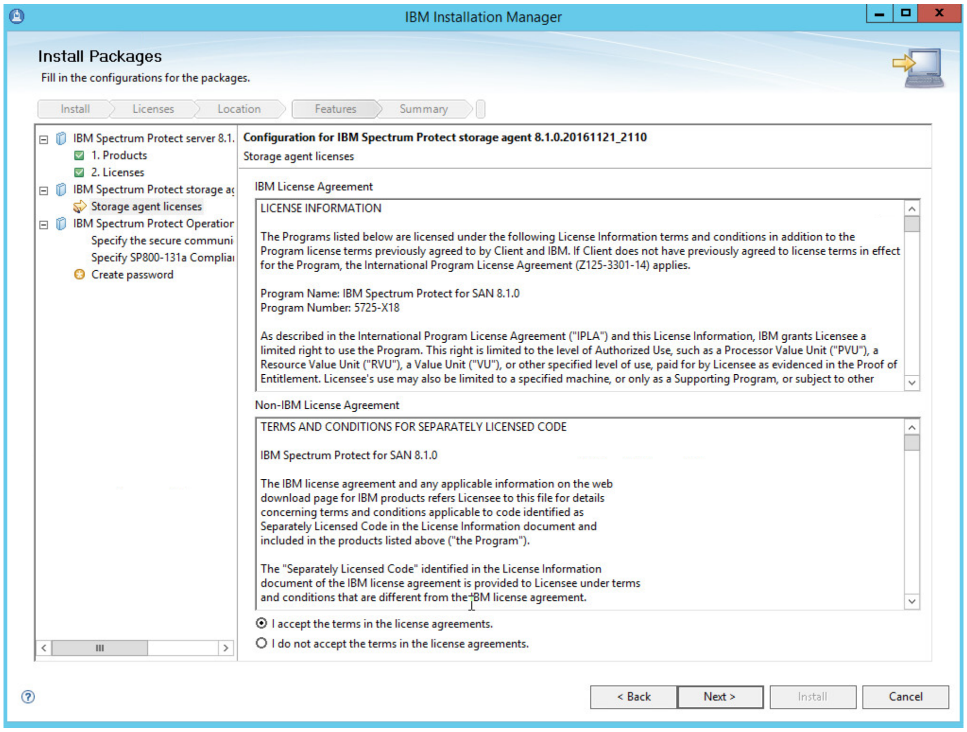
The IBM license agreement and any applicable information on the web download page for IBM products refers Licensee to this file for details concerning terms and conditions applicable to code identified as Separately Licensed Code in the License Information document and included in the products listed above ("the Program").

The "Separately Licensed Code" identified in the License Information document of the IBM license agreement is provided to Licensee under terms and conditions that are different from the IBM license agreement.

● I accept the terms in the license agreements.

○ I do not accept the terms in the license agreements.

16. Click **Next**.
17. Read and select **I accept the terms in the license agreement**.


IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage ag
Storage agent licenses
IBM Spectrum Protect Operation
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect storage agent 8.1.0.20161121_2110

Storage agent licenses

IBM License Agreement

LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions in addition to the Program license terms previously agreed to by Client and IBM. If Client does not have previously agreed to license terms in effect for the Program, the International Program License Agreement (Z125-3301-14) applies.

Program Name: IBM Spectrum Protect for SAN 8.1.0
Program Number: 5725-X18

As described in the International Program License Agreement ("IPLA") and this License Information, IBM grants Licensee a limited right to use the Program. This right is limited to the level of Authorized Use, such as a Processor Value Unit ("PVU"), a Resource Value Unit ("RVU"), a Value Unit ("VU"), or other specified level of use, paid for by Licensee as evidenced in the Proof of Entitlement. Licensee's use may also be limited to a specified machine, or only as a Supporting Program, or subject to other

Non-IBM License Agreement

TERMS AND CONDITIONS FOR SEPARATELY LICENSED CODE

IBM Spectrum Protect for SAN 8.1.0

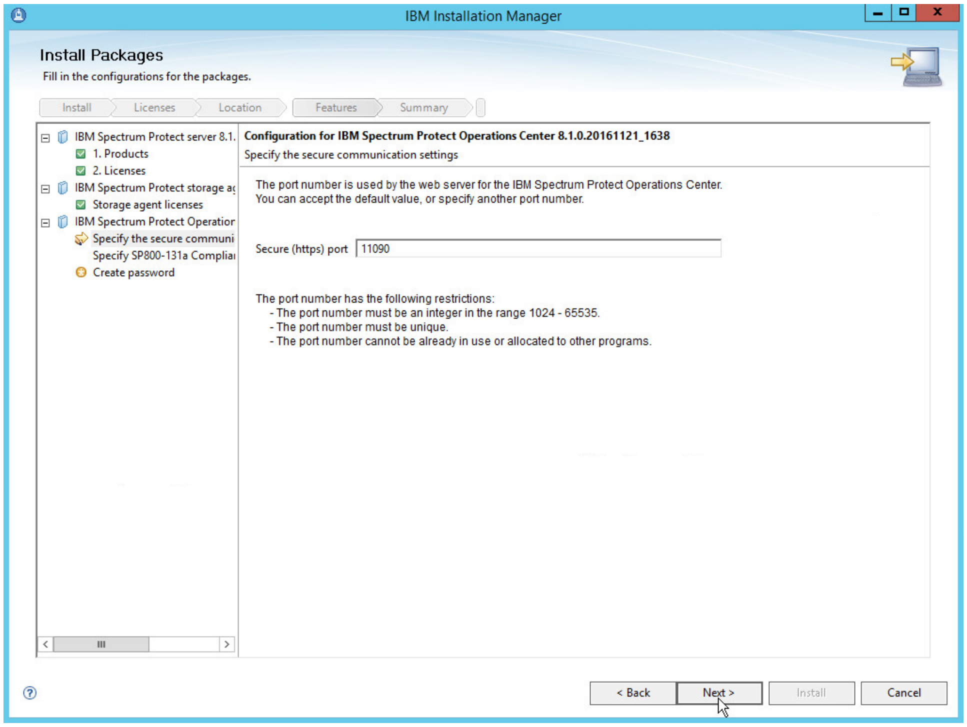
The IBM license agreement and any applicable information on the web download page for IBM products refers Licensee to this file for details concerning terms and conditions applicable to code identified as Separately Licensed Code in the License Information document and included in the products listed above ("the Program").

The "Separately Licensed Code" identified in the License Information document of the IBM license agreement is provided to Licensee under terms and conditions that are different from the IBM license agreement.

● I accept the terms in the license agreements.

○ I do not accept the terms in the license agreements.

18. Click **Next**.
19. Specify **11090** for the port.



IBM Installation Manager
Install Packages
Fill in the configurations for the packages.
Install
Licenses
Location
Features
Summary
IBM Spectrum Protect server 8.1.
1. Products
2. Licenses
IBM Spectrum Protect storage a
Storage agent licenses
IBM Spectrum Protect Operatior
Specify the secure communi
Specify SP800-131a Complia
Create password
< Back
Next >
Install
Cancel

Configuration for IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

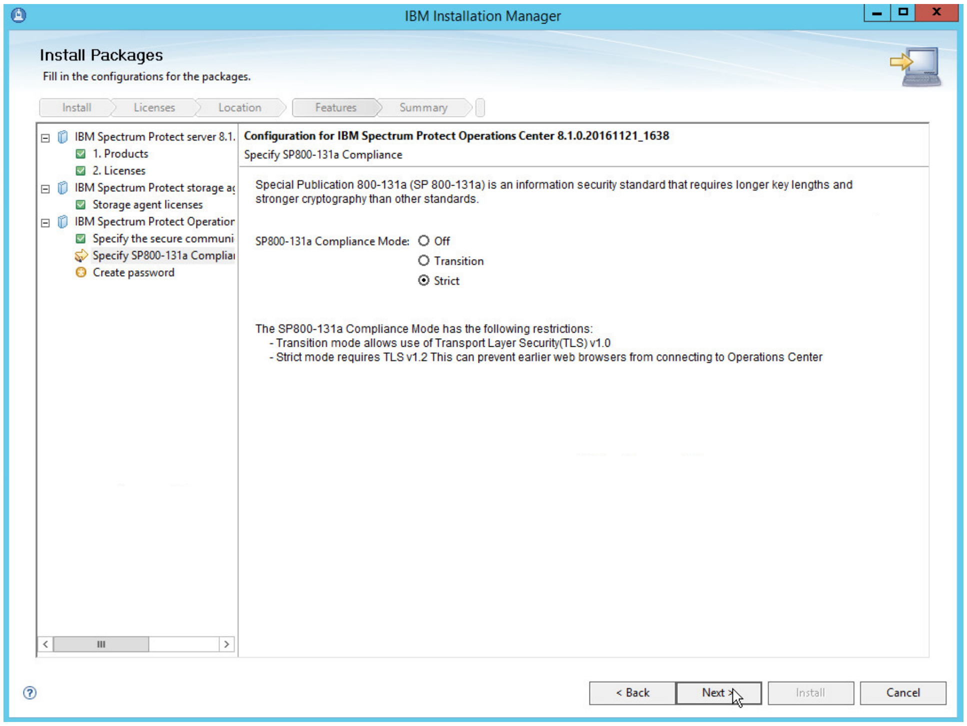
Specify the secure communication settings

The port number is used by the web server for the IBM Spectrum Protect Operations Center.
You can accept the default value, or specify another port number.

Secure (https) port: 11090

The port number has the following restrictions:
- The port number must be an integer in the range 1024 - 65535.
- The port number must be unique.
- The port number cannot be already in use or allocated to other programs.

20. Click **Next**.
21. Select **Strict** for the **SP800-131a Compliance**.



Fill in the configurations for the packages.

Configuration for IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

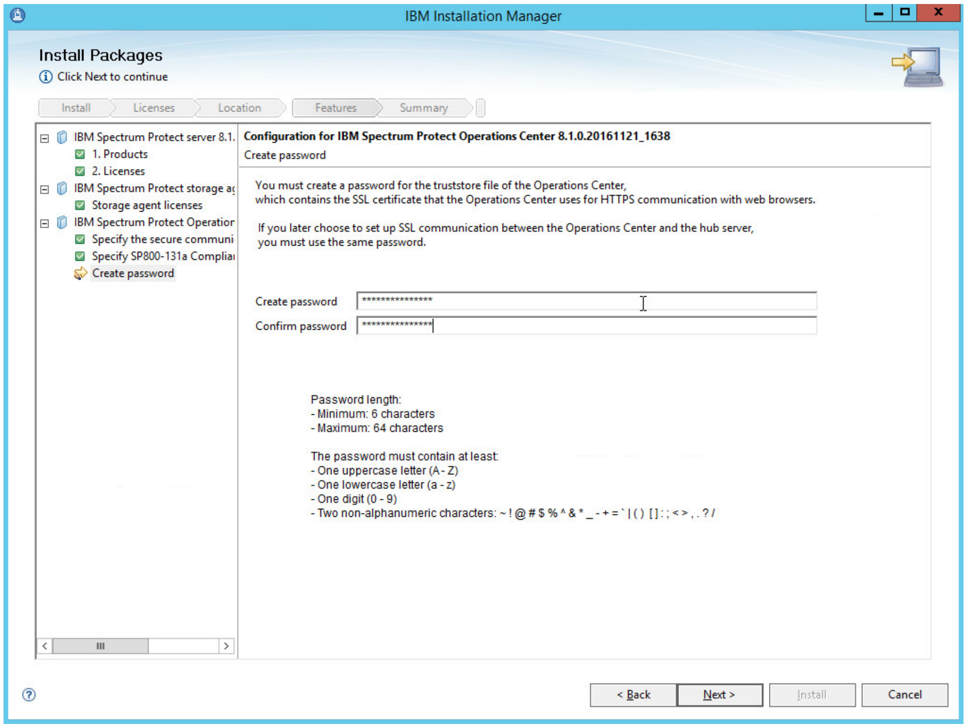
Specify SP800-131a Compliance

Special Publication 800-131a (SP 800-131a) is an information security standard that requires longer key lengths and stronger cryptography than other standards.

SP800-131a Compliance Mode: ○ Off
○ Transition
● Strict

The SP800-131a Compliance Mode has the following restrictions:
- Transition mode allows use of Transport Layer Security(TLS) v1.0
- Strict mode requires TLS v1.2 This can prevent earlier web browsers from connecting to Operations Center

22. Click **Next**.
23. Create a password.



Click Next to continue

Configuration for IBM Spectrum Protect Operations Center 8.1.0.20161121_1638

Create password

You must create a password for the truststore file of the Operations Center,
which contains the SSL certificate that the Operations Center uses for HTTPS communication with web browsers.

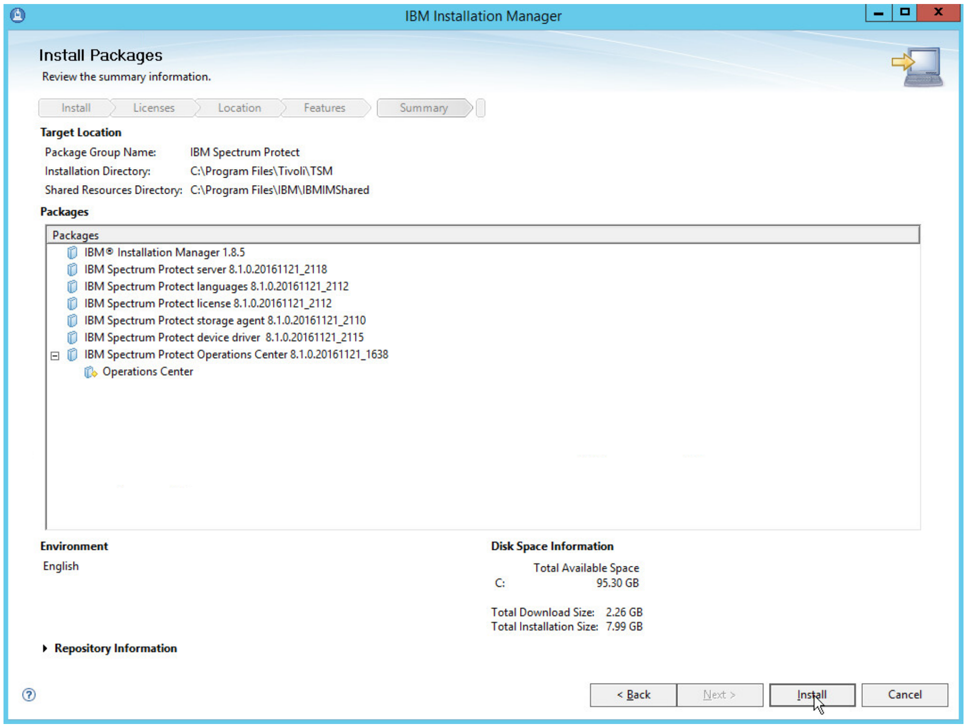
If you later choose to set up SSL communication between the Operations Center and the hub server,
you must use the same password.

Create password ***************
Confirm password ***************

Password length:
- Minimum: 6 characters
- Maximum: 64 characters

The password must contain at least:
- One uppercase letter (A - Z)
- One lowercase letter (a - z)
- One digit (0 - 9)
- Two non-alphanumeric characters: ~ ! @ # $ % ^ & * _ - + = ` | ( ) [ ] : ; < > , . ? /

24. Click **Next**.



Target Location

Package Group Name: IBM Spectrum Protect
Installation Directory: C:\Program Files\Tivoli\TSM
Shared Resources Directory: C:\Program Files\IBM\IBMIMShared

Packages

Packages
- IBM® Installation Manager 1.8.5
- IBM Spectrum Protect server 8.1.0.20161121_2118
- IBM Spectrum Protect languages 8.1.0.20161121_2112
- IBM Spectrum Protect license 8.1.0.20161121_2112
- IBM Spectrum Protect storage agent 8.1.0.20161121_2110
- IBM Spectrum Protect device driver 8.1.0.20161121_2115
- IBM Spectrum Protect Operations Center 8.1.0.20161121_1638
  - Operations Center

Environment

English

Disk Space Information

	Total Available Space
C:	95.30 GB

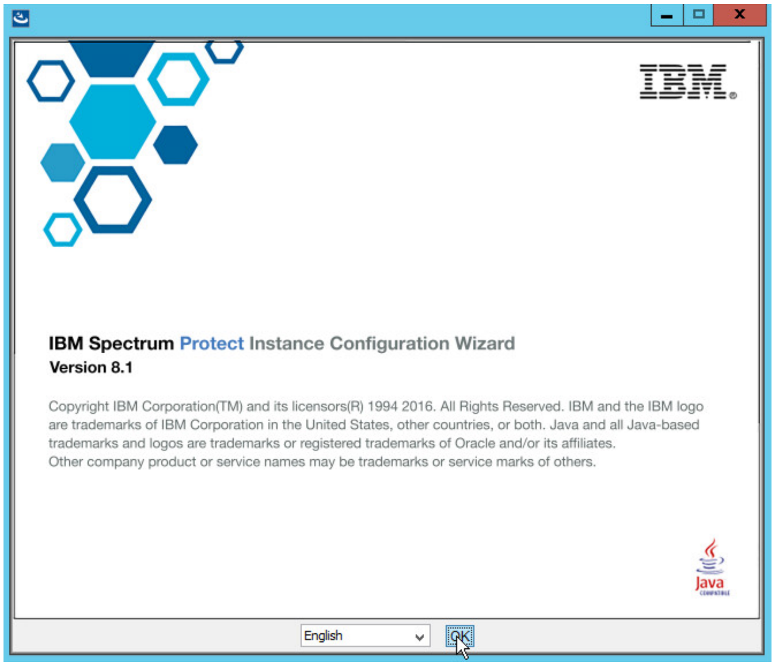
Total Download Size: 2.26 GB
Total Installation Size: 7.99 GB

Repository Information

25. Click **Install**.
26. After the successful installation, click **Finish**.

2.13.2 Configure IBM Spectrum Protect

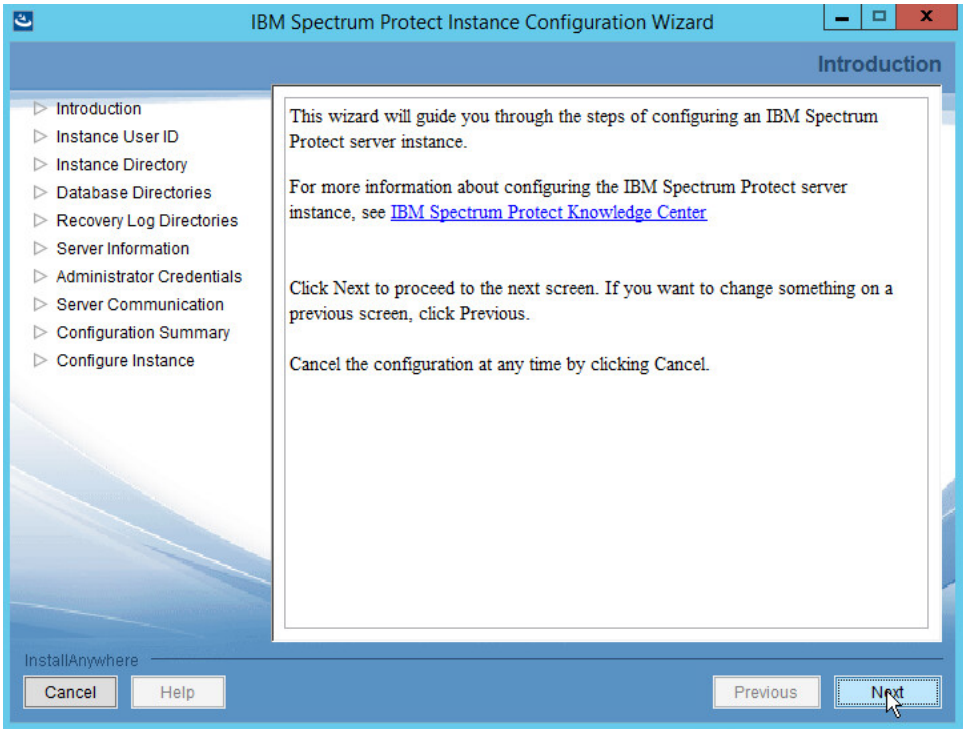
1. Go to **Start > IBM Spectrum Protect Configuration Wizard**.



IBM Spectrum Protect Instance Configuration Wizard
Version 8.1

Copyright IBM Corporation(TM) and its licensors(R) 1994 2016. All Rights Reserved. IBM and the IBM logo are trademarks of IBM Corporation in the United States, other countries, or both. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Other company product or service names may be trademarks or service marks of others.

2. Click **OK**.



IBM Spectrum Protect Instance Configuration Wizard

Introduction

This wizard will guide you through the steps of configuring an IBM Spectrum Protect server instance.

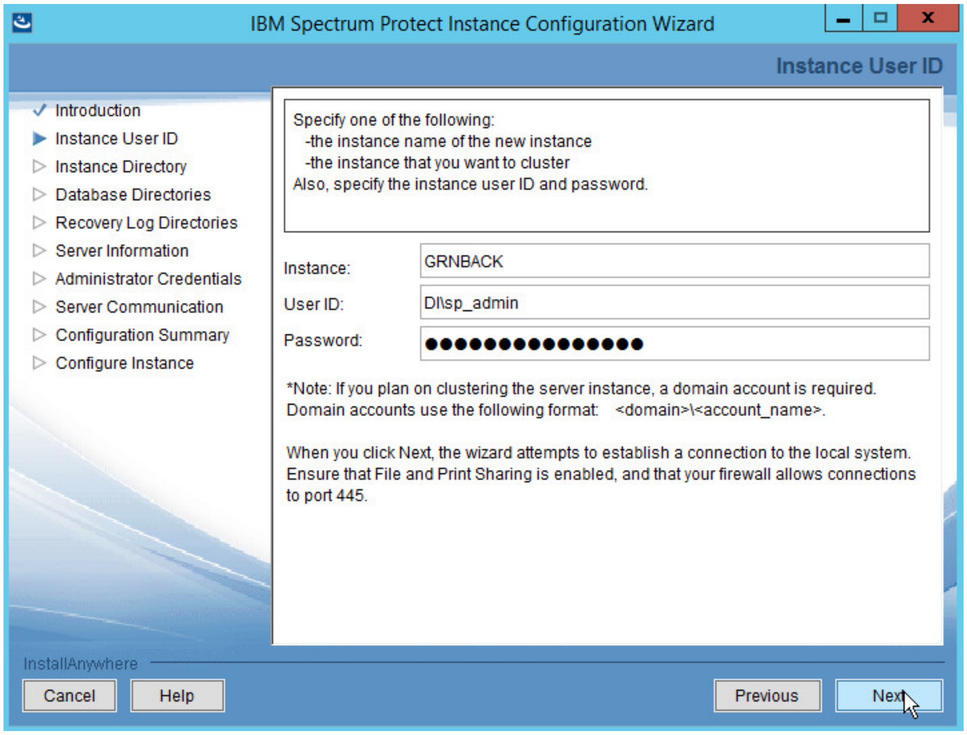
For more information about configuring the IBM Spectrum Protect server instance, see IBM Spectrum Protect Knowledge Center

Click Next to proceed to the next screen. If you want to change something on a previous screen, click Previous.

Cancel the configuration at any time by clicking Cancel.

3. Click **Next**.

4. Specify a name and an account for the IBM server to use. Example: (name: GRNBACK, User ID: DI\sp_admin)



Specify one of the following:
-the instance name of the new instance
-the instance that you want to cluster
Also, specify the instance user ID and password.

Instance: GRNBACK

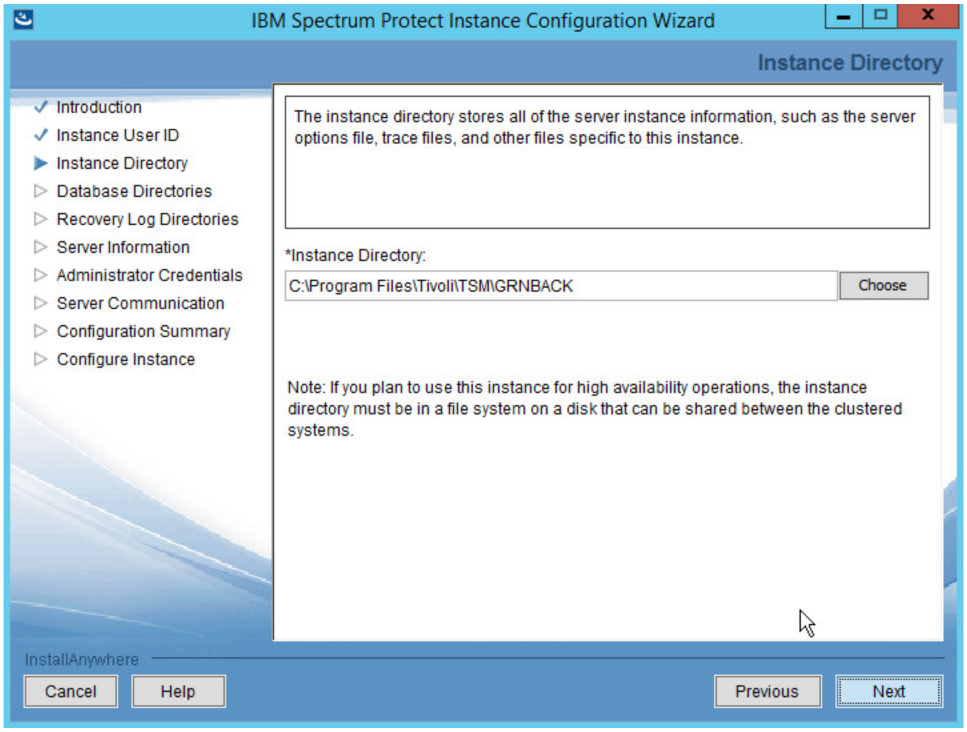
User ID: DI\sp_admin

Password: ●●●●●●●●●●●●●●●

*Note: If you plan on clustering the server instance, a domain account is required. Domain accounts use the following format: <domain>\<account_name>.

When you click Next, the wizard attempts to establish a connection to the local system. Ensure that File and Print Sharing is enabled, and that your firewall allows connections to port 445.

5. Click **Next**.
6. Choose a directory.

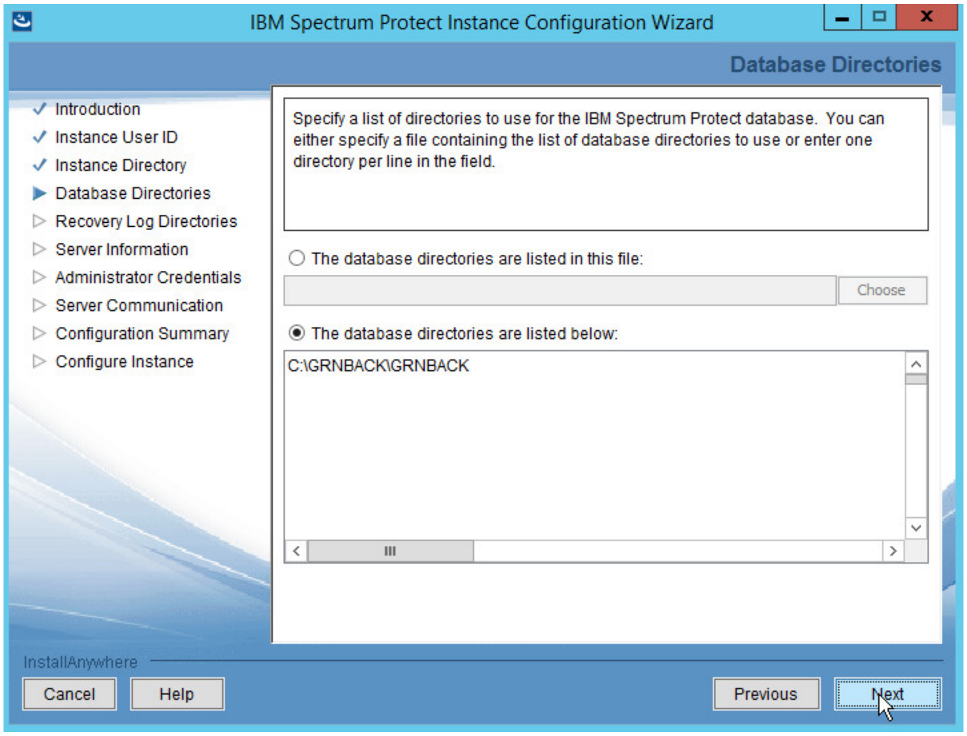


The instance directory stores all of the server instance information, such as the server options file, trace files, and other files specific to this instance.

*Instance Directory: C:\Program Files\Tivoli\TSM\GRNBACK

Note: If you plan to use this instance for high availability operations, the instance directory must be in a file system on a disk that can be shared between the clustered systems.

7. Click **Next**.
8. Click **Yes** if prompted to create the directory.
9. Choose **The database directories are listed below**.
10. Create a directory to contain the database. Example: *C:\BACKSERV\IBMBackupServer*.
11. Enter the directory in the space provided.



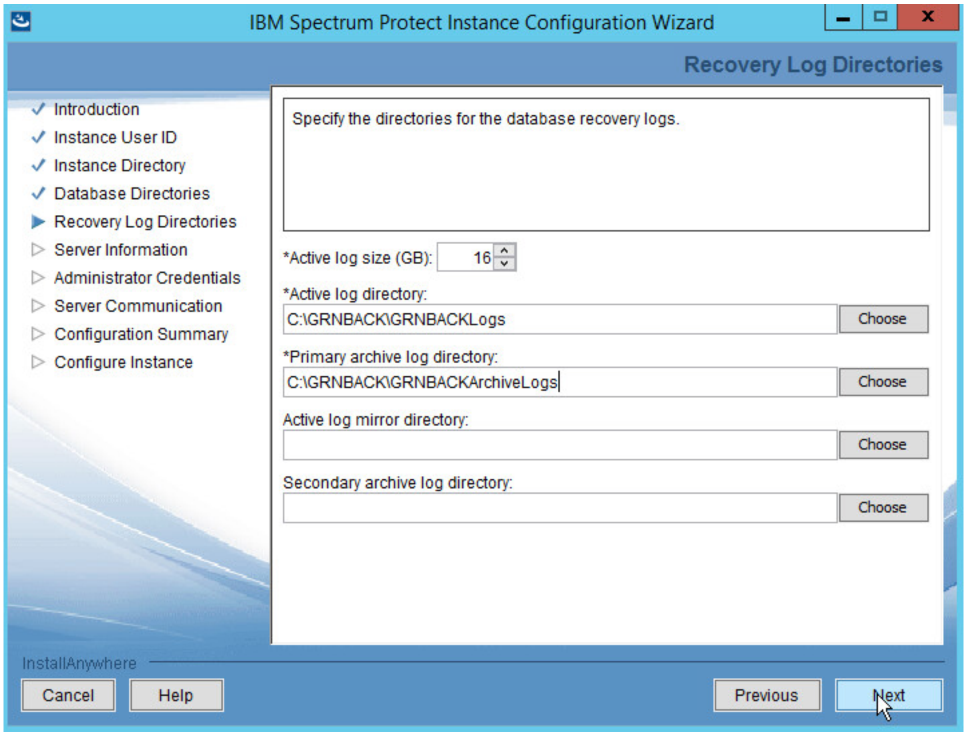
Specify a list of directories to use for the IBM Spectrum Protect database. You can either specify a file containing the list of database directories to use or enter one directory per line in the field.

○ The database directories are listed in this file:

● The database directories are listed below:

C:\GRNBACK\GRNBACK

12. Click **Next**.
13. Create directories for **logs** and **archive logs**. Example: *C:\BACKSERV\IBMBackupServerLogs*, *C:\BACKSERV\IBMBackupServerArchiveLogs*.
14. Enter the directories in their respective fields.



IBM Spectrum Protect Instance Configuration Wizard

Recovery Log Directories

Specify the directories for the database recovery logs.

*Active log size (GB): 16

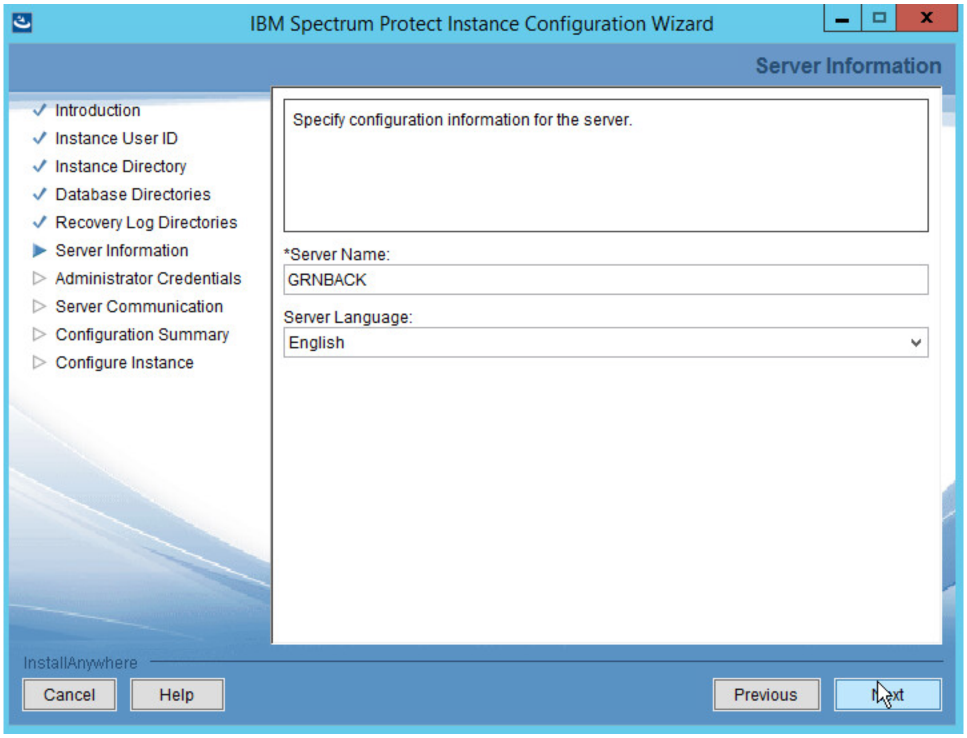
*Active log directory: C:\GRNBACK\GRNBACKLogs

*Primary archive log directory: C:\GRNBACK\GRNBACKArchiveLogs

Active log mirror directory:

Secondary archive log directory:

15. Click **Next**.
16. Specify the **server name**.

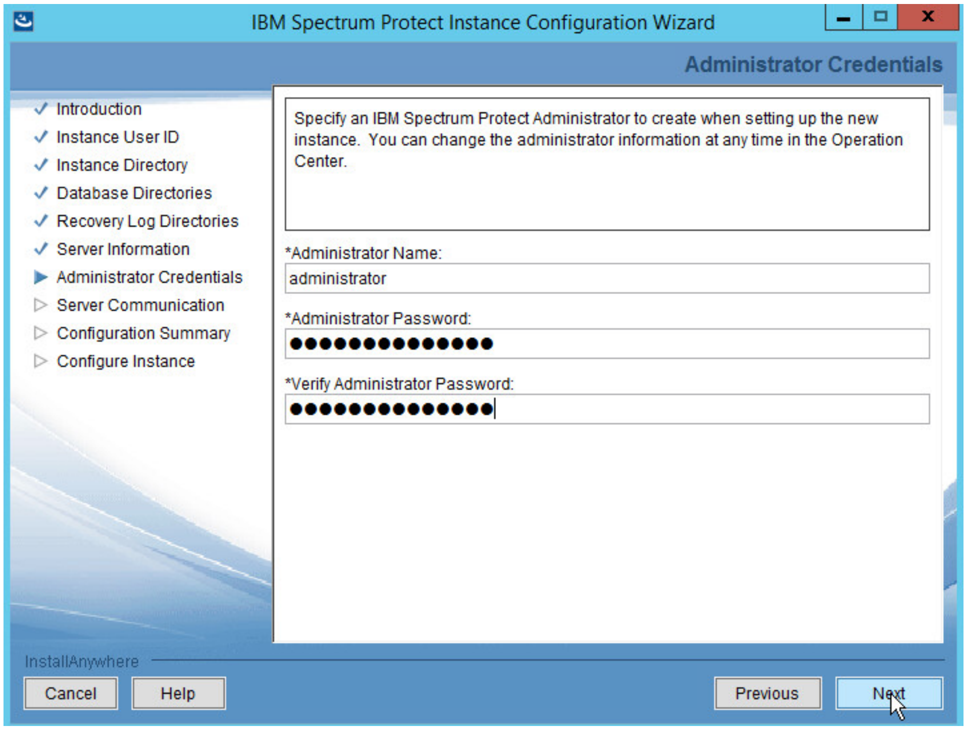


Specify configuration information for the server.

*Server Name: GRNBACK

Server Language: English

17. Click **Next**.
18. Specify an **Administrator account**.



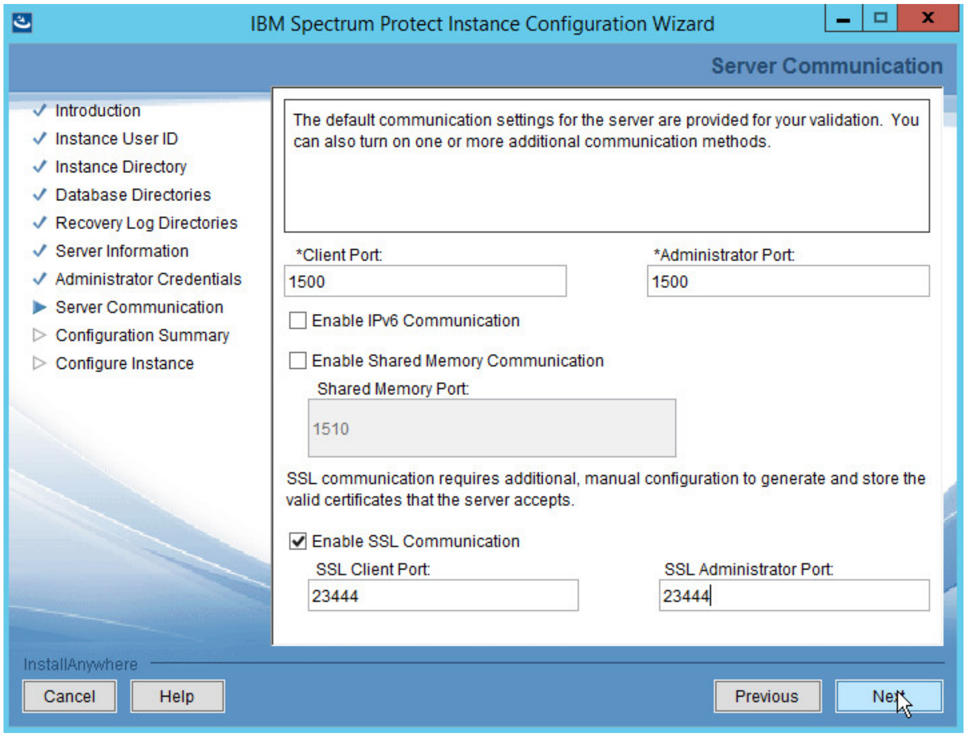
Specify an IBM Spectrum Protect Administrator to create when setting up the new instance. You can change the administrator information at any time in the Operation Center.

*Administrator Name: administrator

*Administrator Password: ●●●●●●●●●●●●●●

*Verify Administrator Password: ●●●●●●●●●●●●●●

19. Click **Next**.
20. Select a **port** (example: 1500).
21. Check the box next to **Enable SSL Communication** and enter a **port** (example: 23444).



The default communication settings for the server are provided for your validation. You can also turn on one or more additional communication methods.

*Client Port: 1500

*Administrator Port: 1500

□ Enable IPv6 Communication

□ Enable Shared Memory Communication

Shared Memory Port: 1510

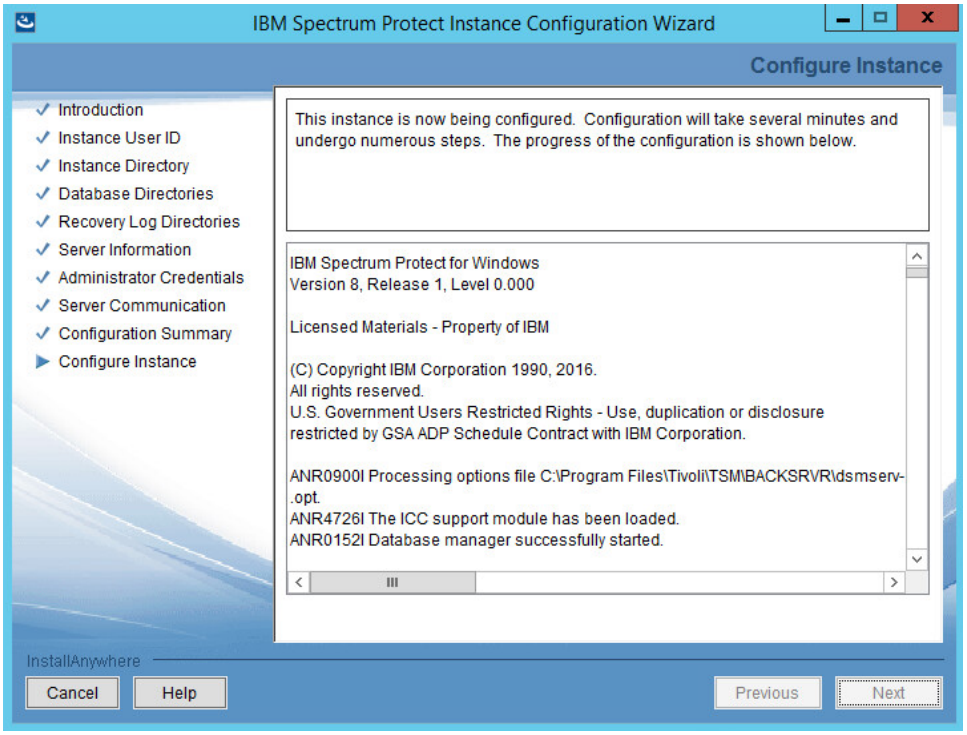
SSL communication requires additional, manual configuration to generate and store the valid certificates that the server accepts.

☑ Enable SSL Communication

SSL Client Port: 23444

SSL Administrator Port: 23444

22. Click **Next**.
23. Click **Next**.
24. Wait for the installation to finish.



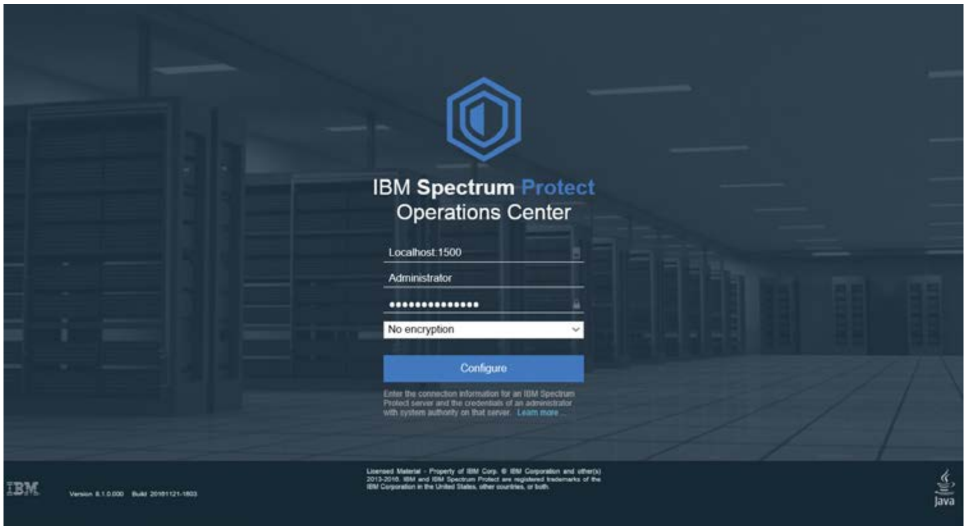
IBM Spectrum Protect Instance Configuration Wizard

Configure Instance

This instance is now being configured. Configuration will take several minutes and undergo numerous steps. The progress of the configuration is shown below.

```
IBM Spectrum Protect for Windows
Version 8, Release 1, Level 0.000

Licensed Materials - Property of IBM

(C) Copyright IBM Corporation 1990, 2016.
All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corporation.

ANR0900I Processing options file C:\Program Files\Tivoli\TSM\BACKSRVR\dsmserv-
.opt.
ANR4726I The ICC support module has been loaded.
ANR0152I Database manager successfully started.
```

25. Click **Next**.
26. Click **Done**.
27. Log in to **Operations Center** by going to *localhost:11090/oc/.*
28. Log in using the credentials provided in the **Configuration Wizard**.



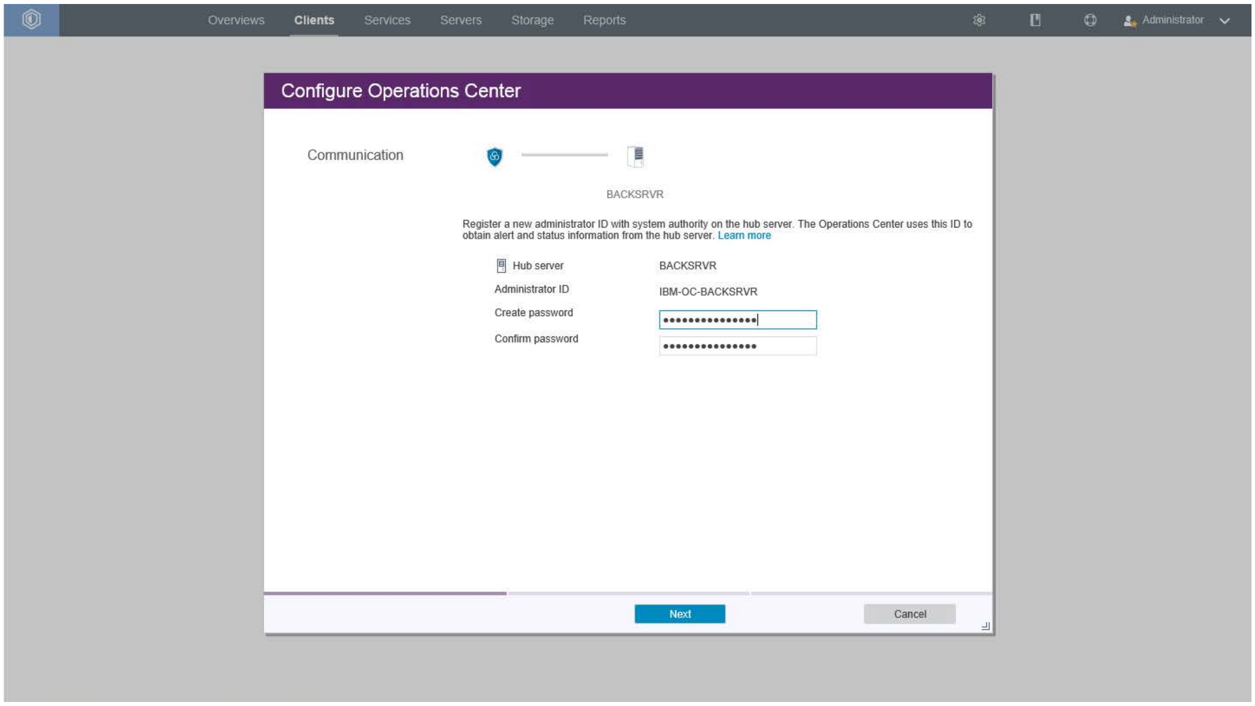
IBM Spectrum Protect
Operations Center

Localhost:1500
Administrator
••••••••••••••
No encryption

Enter the connection information for an IBM Spectrum Protect server and the credentials of an administrator with system authority on that server. Learn more ...

Licensed Material - Property of IBM Corp. © IBM Corporation and other(s) 2013-2016. IBM and IBM Spectrum Protect are registered trademarks of the IBM Corporation in the United States, other countries, or both.

29. Enter the password for a new account to be created on the system.



Configure Operations Center

Communication

BACKSRVR

Register a new administrator ID with system authority on the hub server. The Operations Center uses this ID to obtain alert and status information from the hub server. Learn more

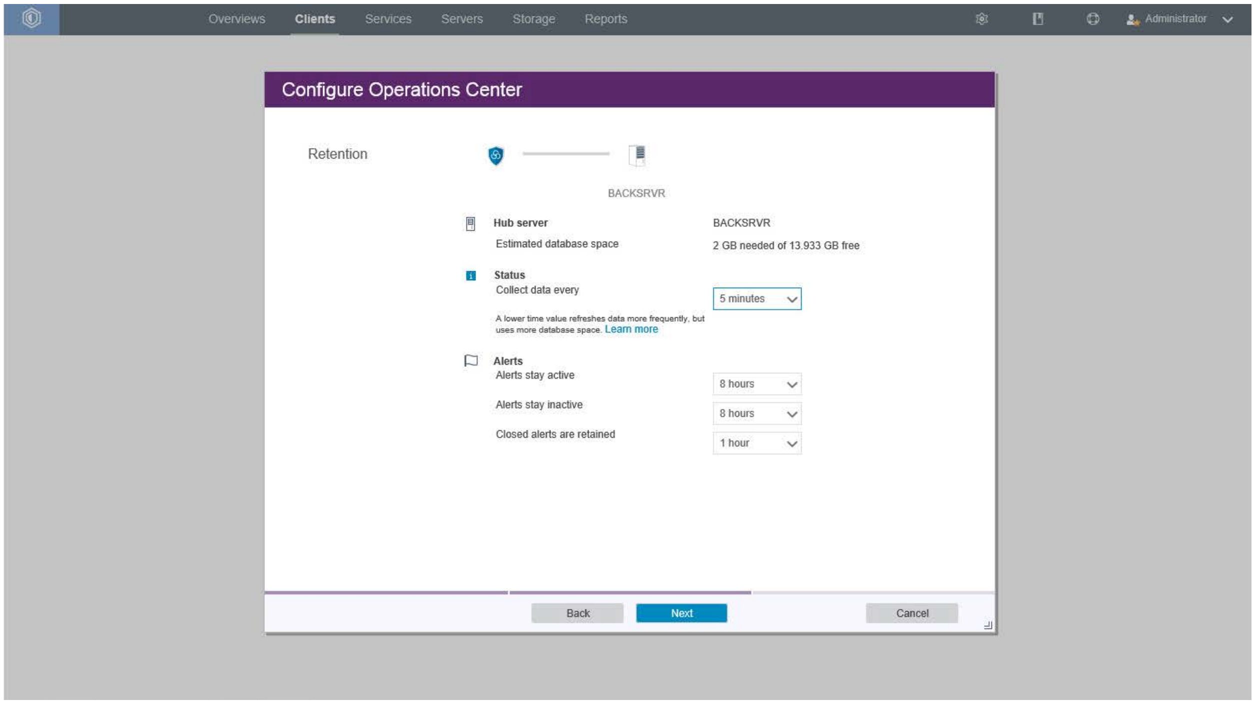
Hub server BACKSRVR

Administrator ID IBM-OC-BACKSRVR

Create password •••••••••••••••

Confirm password •••••••••••••••

30. Click **Next**.
31. Select the time interval for data collection.



Configure Operations Center

Retention

BACKSRVR

Hub server BACKSRVR

Estimated database space 2 GB needed of 13.933 GB free

Status

Collect data every 5 minutes

A lower time value refreshes data more frequently, but uses more database space. Learn more

Alerts

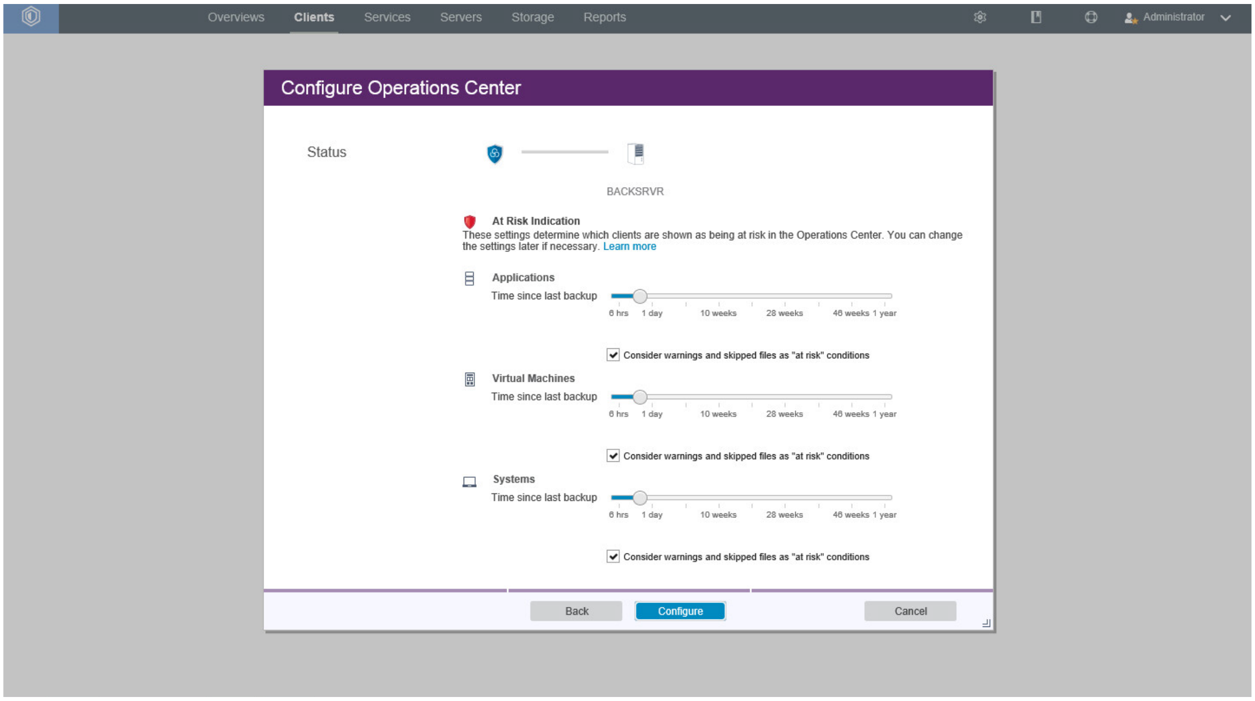
Alerts stay active 8 hours

Alerts stay inactive 8 hours

Closed alerts are retained 1 hour

32. Click **Next**.

33. Select time intervals that suit your organization's needs.



Configure Operations Center

At Risk Indication

These settings determine which clients are shown as being at risk in the Operations Center. You can change the settings later if necessary. Learn more

Applications

Time since last backup

☑ Consider warnings and skipped files as "at risk" conditions

Virtual Machines

Time since last backup

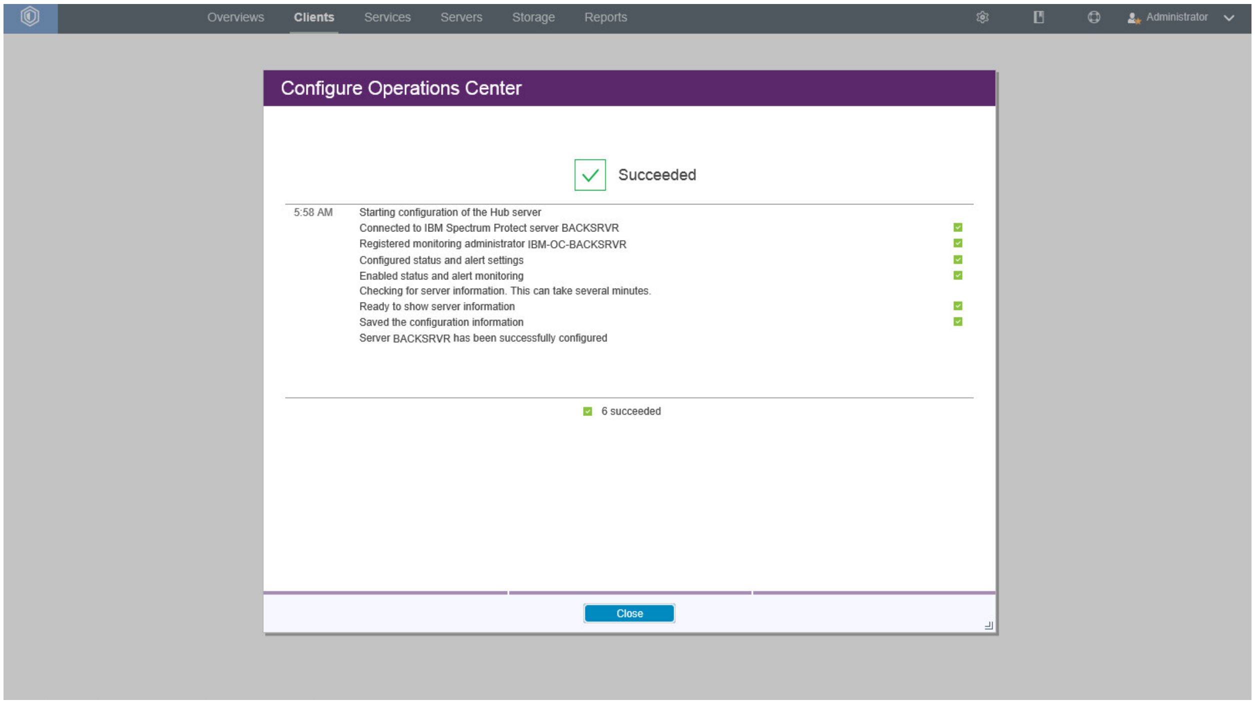
☑ Consider warnings and skipped files as "at risk" conditions

Systems

Time since last backup

☑ Consider warnings and skipped files as "at risk" conditions

34. Click **Configure**.



Configure Operations Center

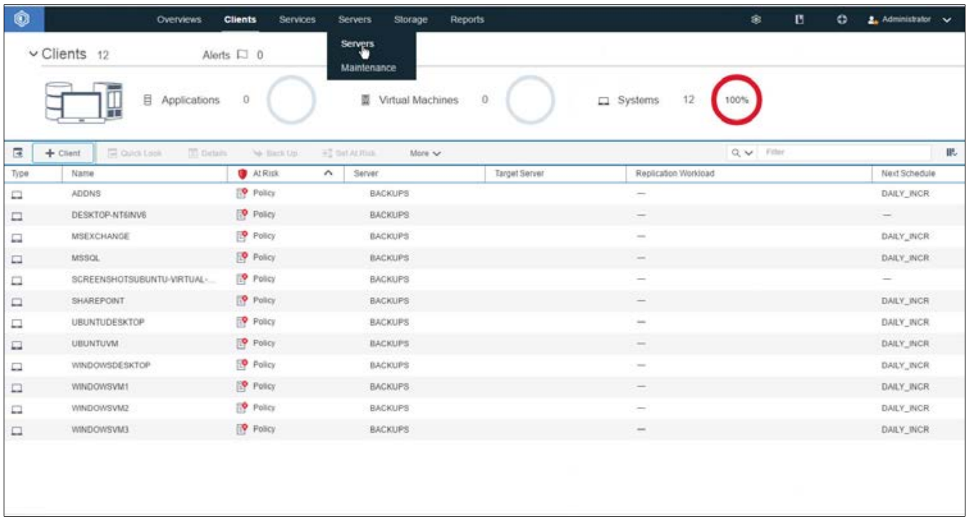
✓ Succeeded

```
5:58 AM   Starting configuration of the Hub server
          Connected to IBM Spectrum Protect server BACKSRVR                    ✓
          Registered monitoring administrator IBM-OC-BACKSRVR                  ✓
          Configured status and alert settings                                 ✓
          Enabled status and alert monitoring                                  ✓
          Checking for server information. This can take several minutes.
          Ready to show server information                                     ✓
          Saved the configuration information                                  ✓
          Server BACKSRVR has been successfully configured
```

✓ 6 succeeded

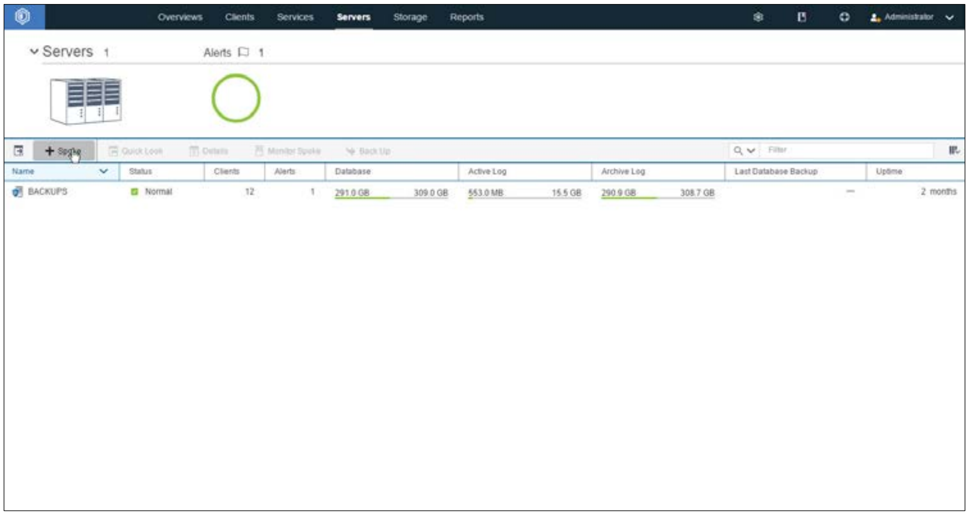
2.13.3 Connect the GreenTec Server to the IBM Spectrum Protect Server

1. Go back to the primary IBM server.



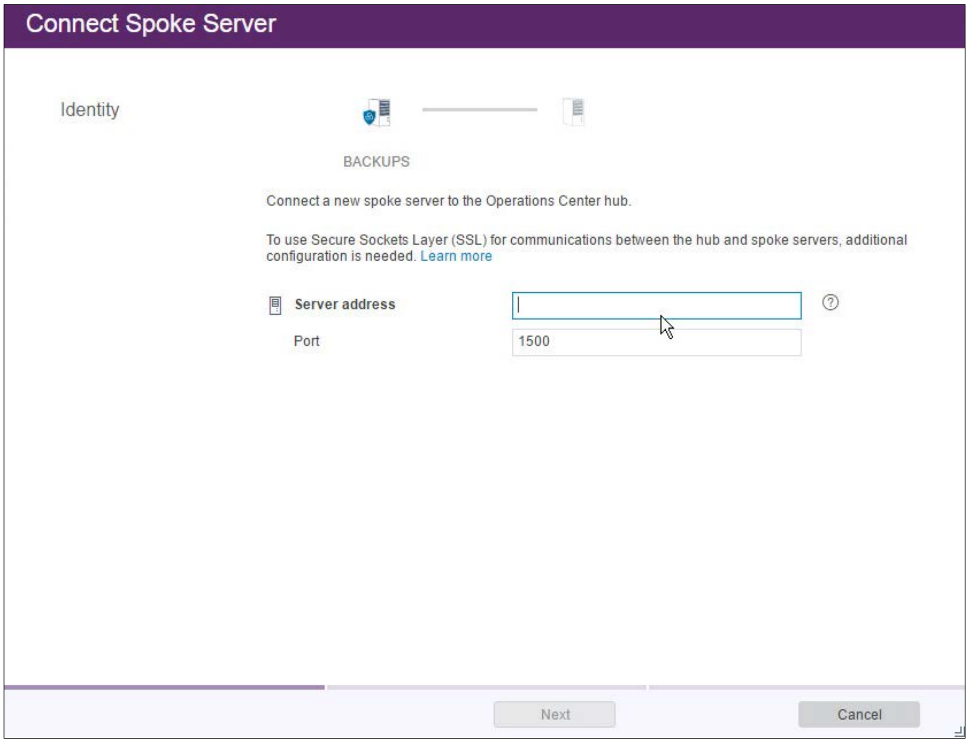
Type	Name	At Risk	Server	Target Server	Replication Workload	Next Schedule
□	ADDNS	Policy	BACKUPS		—	DAILY_INCR
□	DESKTOP-NT6INV6	Policy	BACKUPS		—	—
□	MSEXCHANGE	Policy	BACKUPS		—	DAILY_INCR
□	MSSQL	Policy	BACKUPS		—	DAILY_INCR
□	SCREENSHOTSUBUNTU-VIRTUAL-...	Policy	BACKUPS		—	—
□	SHAREPOINT	Policy	BACKUPS		—	DAILY_INCR
□	UBUNTUDESKTOP	Policy	BACKUPS		—	DAILY_INCR
□	UBUNTUVM	Policy	BACKUPS		—	DAILY_INCR
□	WINDOWSDESKTOP	Policy	BACKUPS		—	DAILY_INCR
□	WINDOWSVM1	Policy	BACKUPS		—	DAILY_INCR
□	WINDOWSVM2	Policy	BACKUPS		—	DAILY_INCR
□	WINDOWSVM3	Policy	BACKUPS		—	DAILY_INCR

2. Click **Servers**.



Name	Status	Clients	Alerts	Database		Active Log		Archive Log		Last Database Backup	Uptime
BACKUPS	🟩 Normal	12	1	291.0 GB	309.0 GB	553.0 MB	15.5 GB	290.9 GB	308.7 GB	—	2 months

3. Click **+Spoke**.



Connect Spoke Server

Identity

BACKUPS

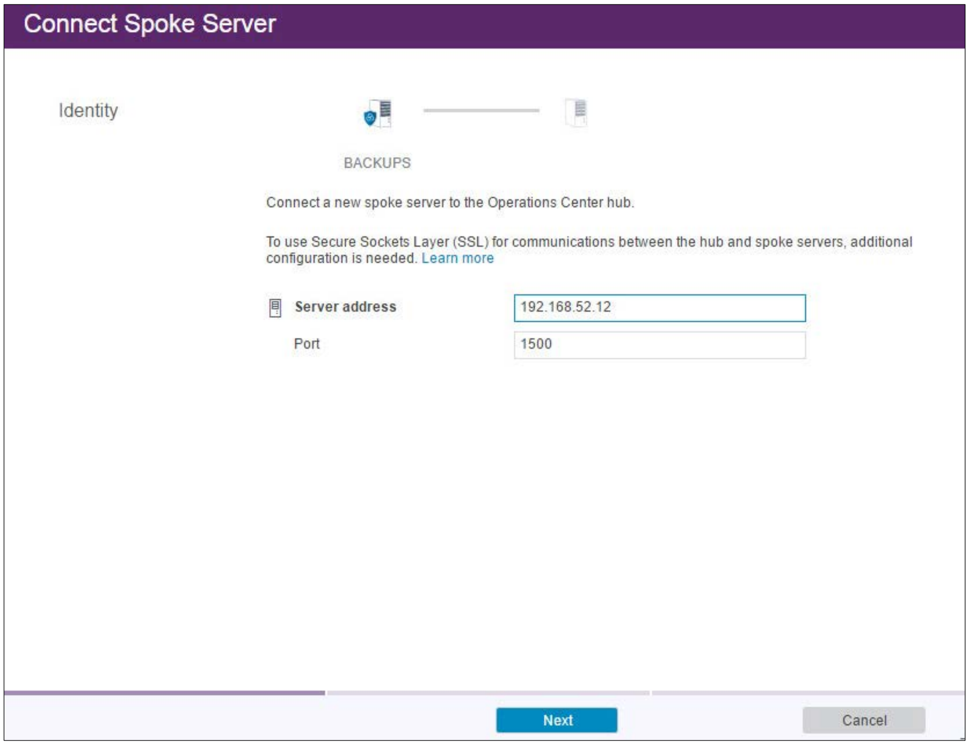
Connect a new spoke server to the Operations Center hub.

To use Secure Sockets Layer (SSL) for communications between the hub and spoke servers, additional configuration is needed. Learn more

Server address

Port 1500

4. Enter the **IP address** of the server with GreenTec disks attached.
5. Enter the **port** that the server is configured to listen for connections on (Example: 1500).



Connect Spoke Server

Identity

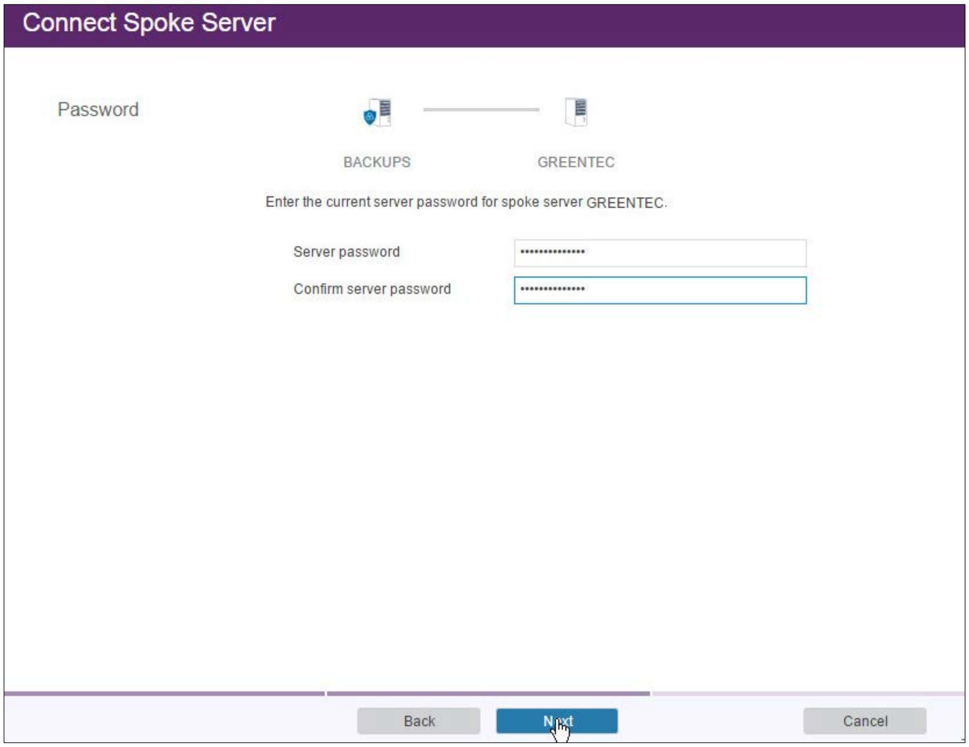
Connect a new spoke server to the Operations Center hub.

To use Secure Sockets Layer (SSL) for communications between the hub and spoke servers, additional configuration is needed. Learn more

Server address: 192.168.52.12

Port: 1500

6. Click **Next**.
7. Enter the password for the new server twice.

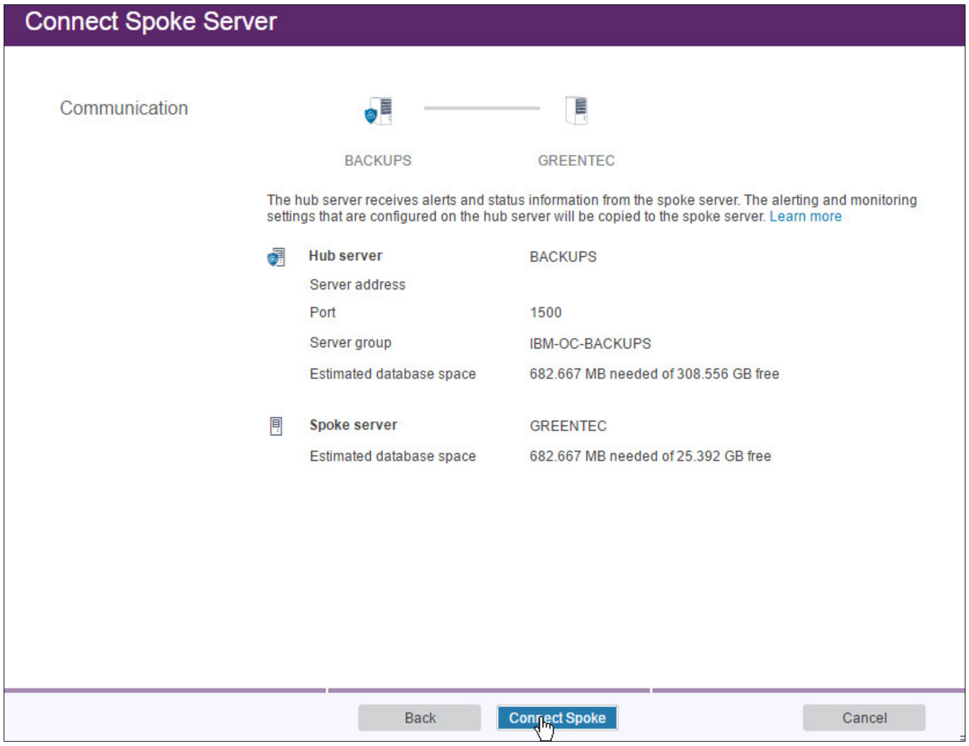


Enter the current server password for spoke server GREENTEC.

Server password: ••••••••••••••

Confirm server password: ••••••••••••••

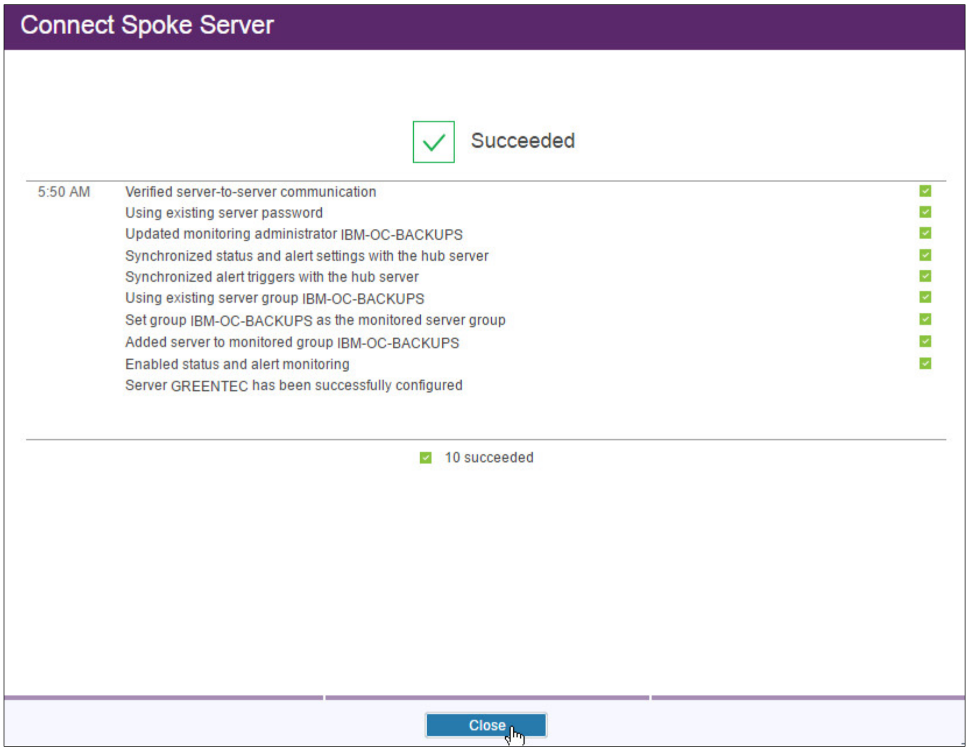
8. Click **Next**.



The hub server receives alerts and status information from the spoke server. The alerting and monitoring settings that are configured on the hub server will be copied to the spoke server. Learn more

Hub server	BACKUPS
Server address	
Port	1500
Server group	IBM-OC-BACKUPS
Estimated database space	682.667 MB needed of 308.556 GB free
Spoke server	GREENTEC
Estimated database space	682.667 MB needed of 25.392 GB free

9. Click **Connect Spoke**.



Connect Spoke Server

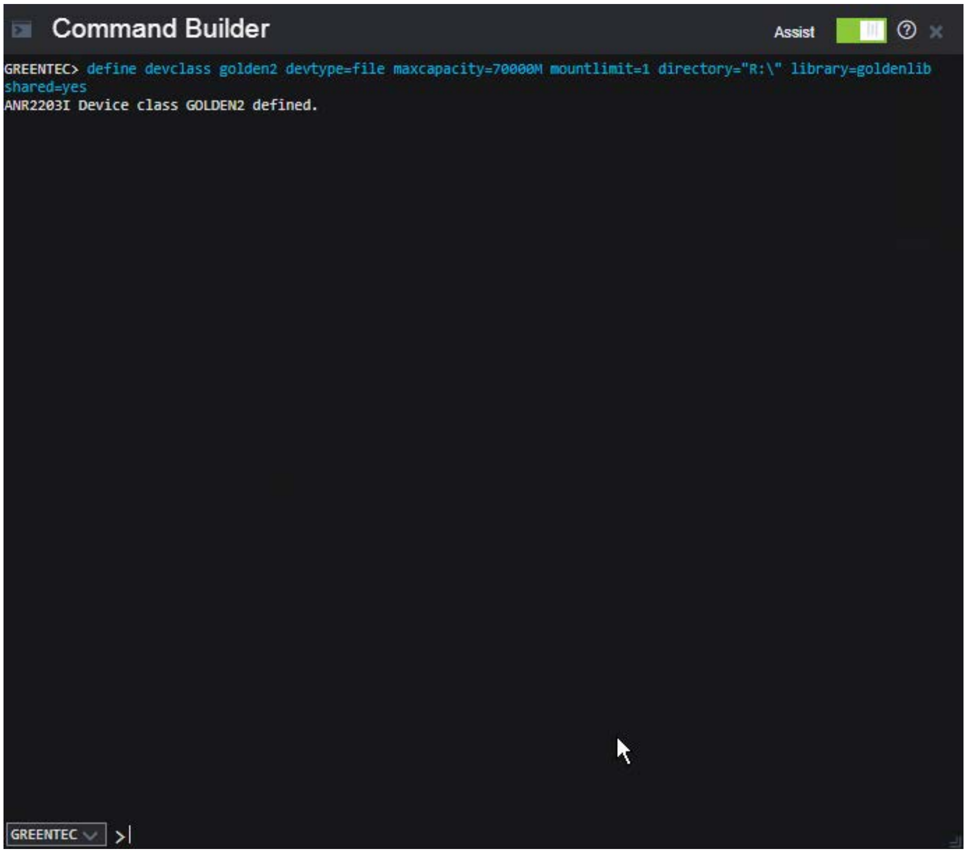
Succeeded

```
5:50 AM    Verified server-to-server communication
           Using existing server password
           Updated monitoring administrator IBM-OC-BACKUPS
           Synchronized status and alert settings with the hub server
           Synchronized alert triggers with the hub server
           Using existing server group IBM-OC-BACKUPS
           Set group IBM-OC-BACKUPS as the monitored server group
           Added server to monitored group IBM-OC-BACKUPS
           Enabled status and alert monitoring
           Server GREENTEC has been successfully configured

10 succeeded
```

10. Click **Close**.

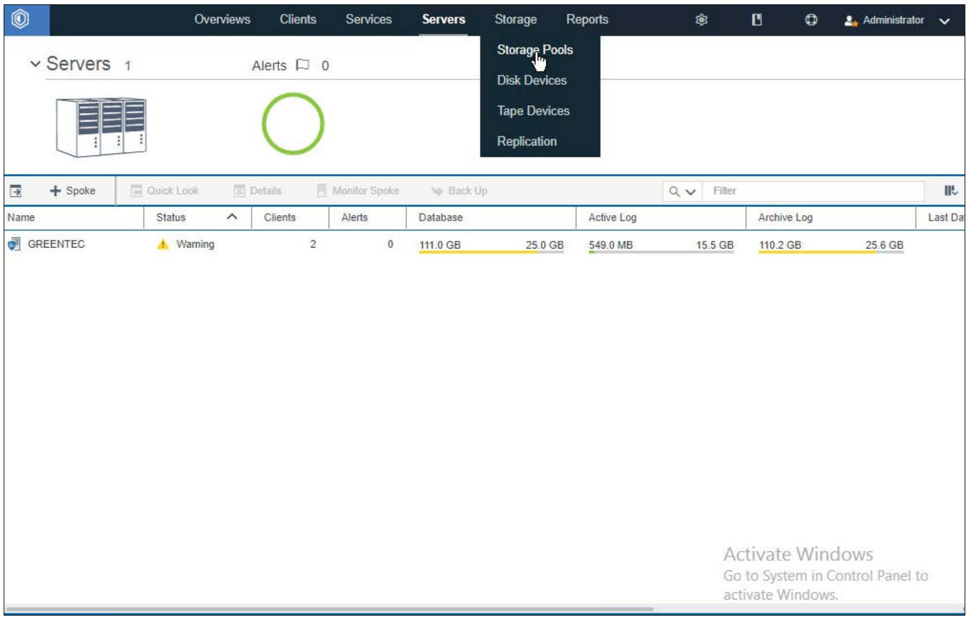
2.13.4 Define a Volume on the GreenTec Server

1. Issue the following command in the Operations Center (on the GreenTec server) command builder to create a device class for the backup disk (replace the name **golden**, max capacity value, and directory value as you see fit).



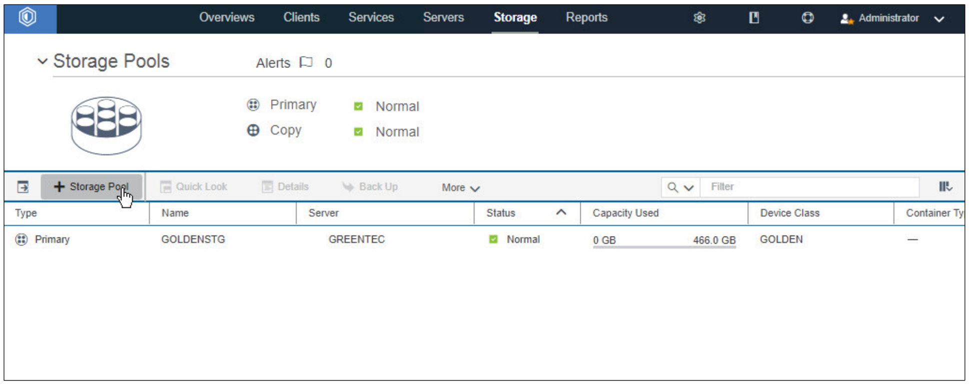
```
GREENTEC> define devclass golden2 devtype=file maxcapacity=70000M mountlimit=1 directory="R:\" library=goldenlib
shared=yes
ANR2203I Device class GOLDEN2 defined.
```

```
> define devclass golden devtype=file maxcapacity=350000M shared=yes
mountlimit=1 directory="E:\" library=backuplib
```



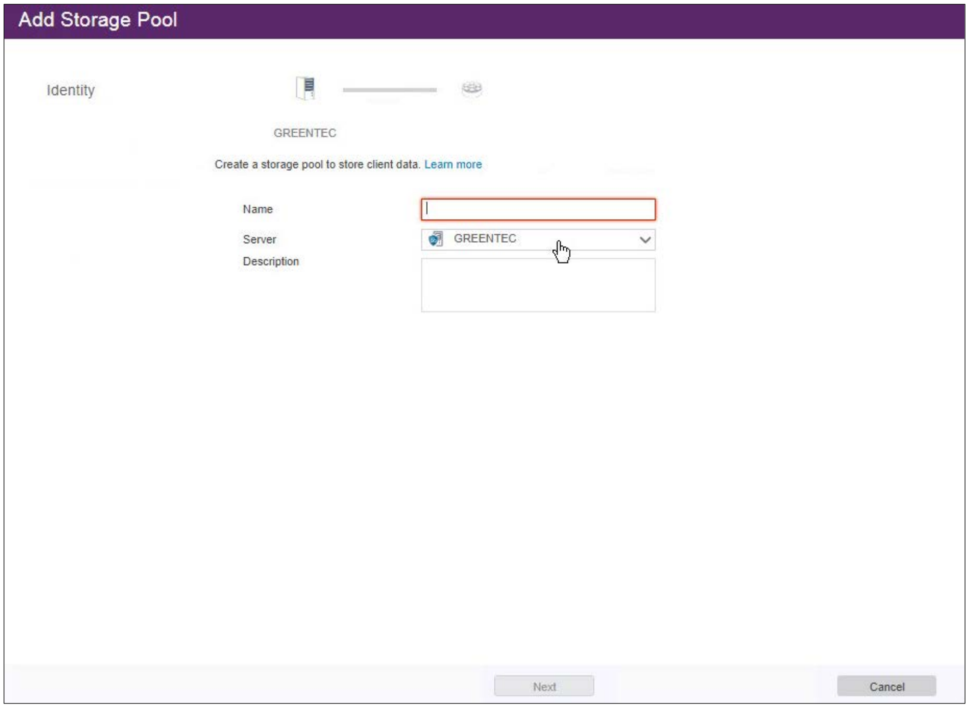
Name	Status	Clients	Alerts	Database	Active Log	Archive Log	Last Da
GREENTEC	Warning	2	0	111.0 GB 25.0 GB	549.0 MB 15.5 GB	110.2 GB 25.6 GB	

2. Go to **Storage > Storage Pools**.



Type	Name	Server	Status	Capacity Used		Device Class	Container Ty
Primary	GOLDENSTG	GREENTEC	Normal	0 GB	466.0 GB	GOLDEN	—

3. Click **+Storage Pool**.
4. Enter a name.



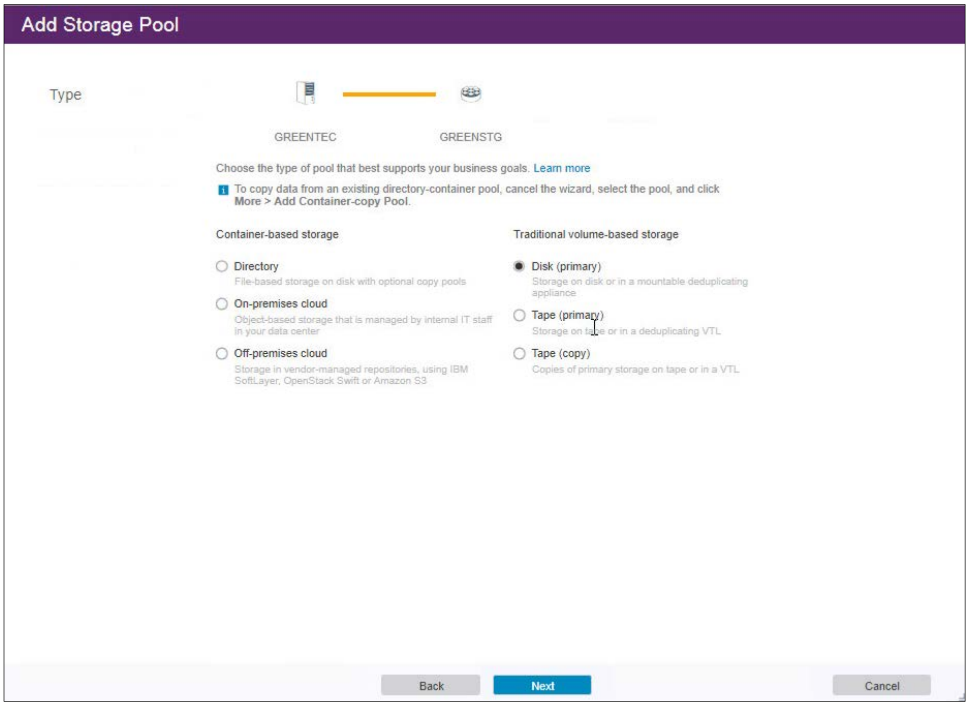
Create a storage pool to store client data. Learn more

Name

Server GREENTEC

Description

5. Click **Next**.
6. Select **Disk (primary).**



Add Storage Pool

Type

GREENTEC GREENSTG

Choose the type of pool that best supports your business goals. Learn more

To copy data from an existing directory-container pool, cancel the wizard, select the pool, and click **More > Add Container-copy Pool**.

Container-based storage

○ Directory
File-based storage on disk with optional copy pools

○ On-premises cloud
Object-based storage that is managed by internal IT staff in your data center

○ Off-premises cloud
Storage in vendor-managed repositories, using IBM SoftLayer, OpenStack Swift or Amazon S3

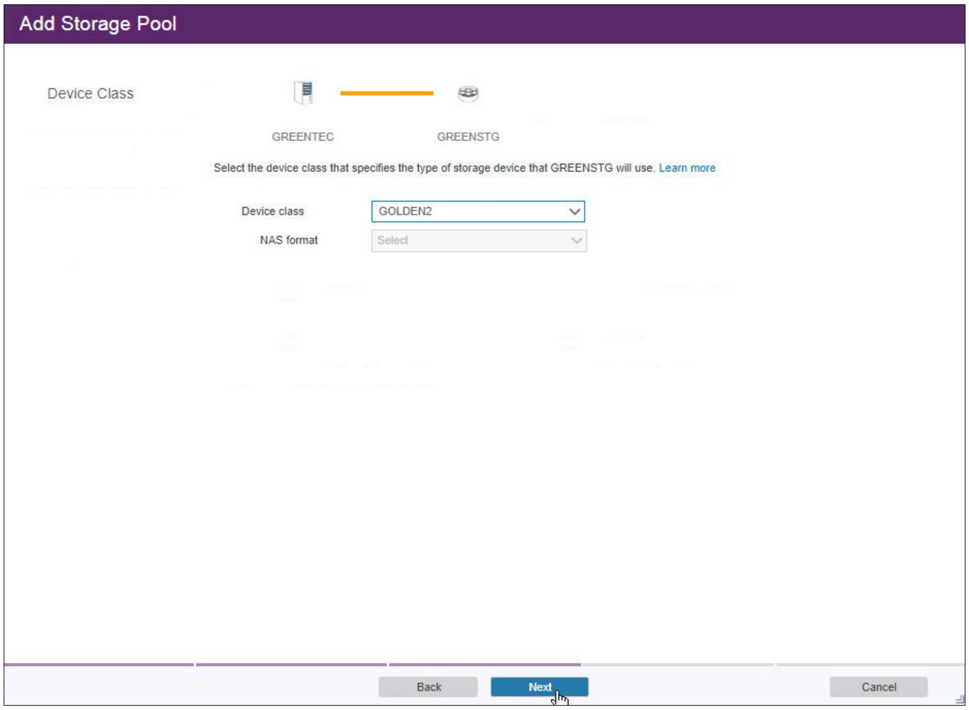
Traditional volume-based storage

● Disk (primary)
Storage on disk or in a mountable deduplicating appliance

○ Tape (primary)
Storage on tape or in a deduplicating VTL

○ Tape (copy)
Copies of primary storage on tape or in a VTL

7. Click **Next**.
8. Select the device class you just created.



Add Storage Pool

Device Class

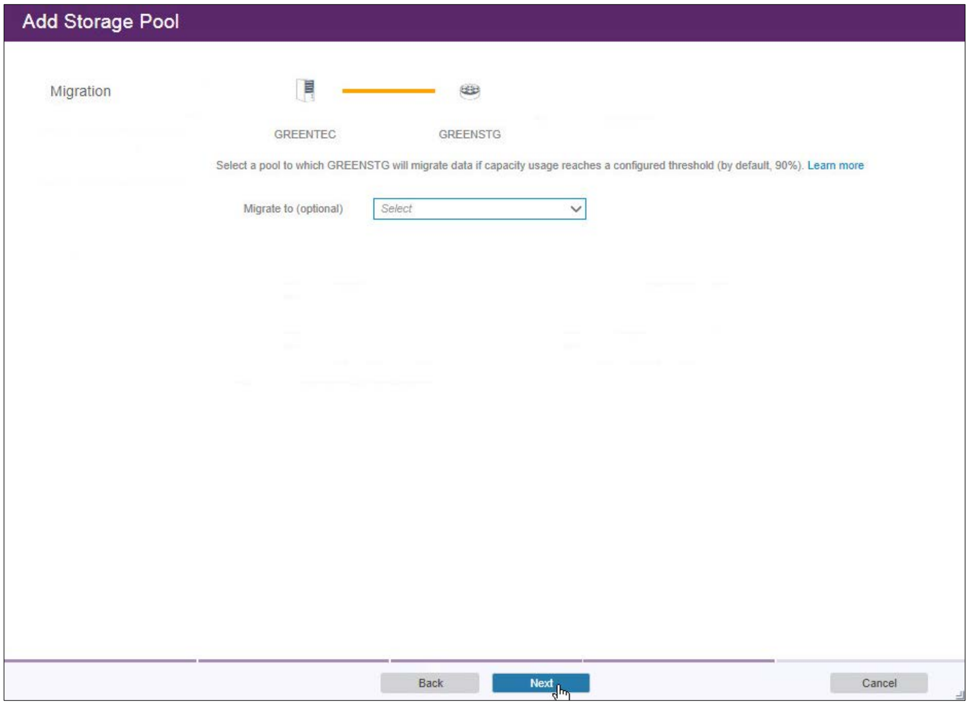
GREENTEC GREENSTG

Select the device class that specifies the type of storage device that GREENSTG will use. Learn more

Device class: GOLDEN2

NAS format: Select

9. Click **Next**.



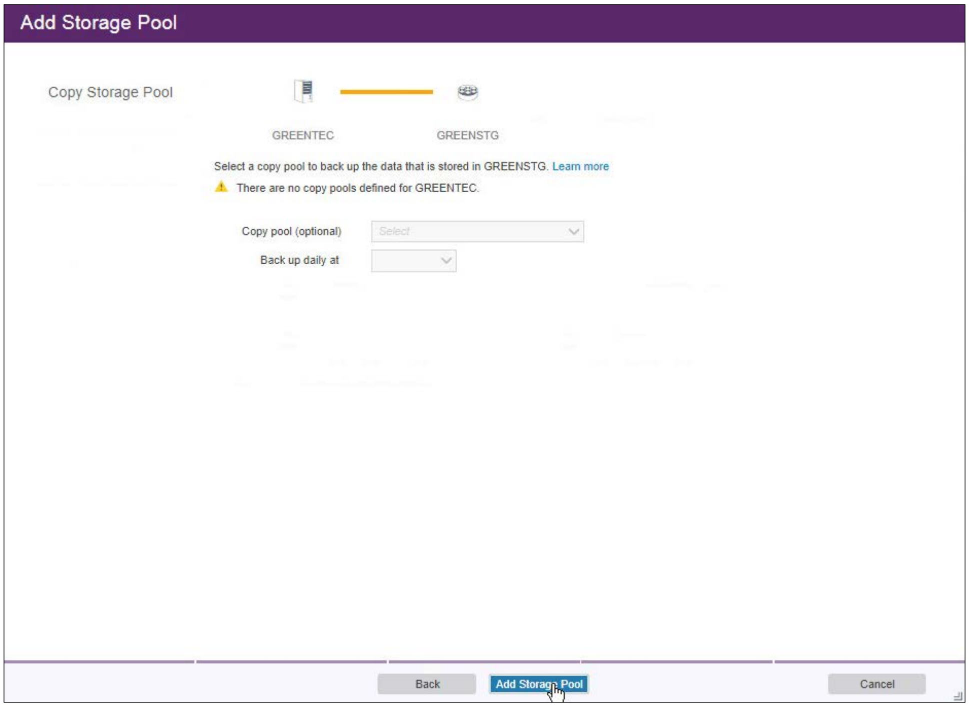
Add Storage Pool

Migration

Select a pool to which GREENSTG will migrate data if capacity usage reaches a configured threshold (by default, 90%). Learn more

Migrate to (optional): Select

10. Click **Next**.



Add Storage Pool

Copy Storage Pool

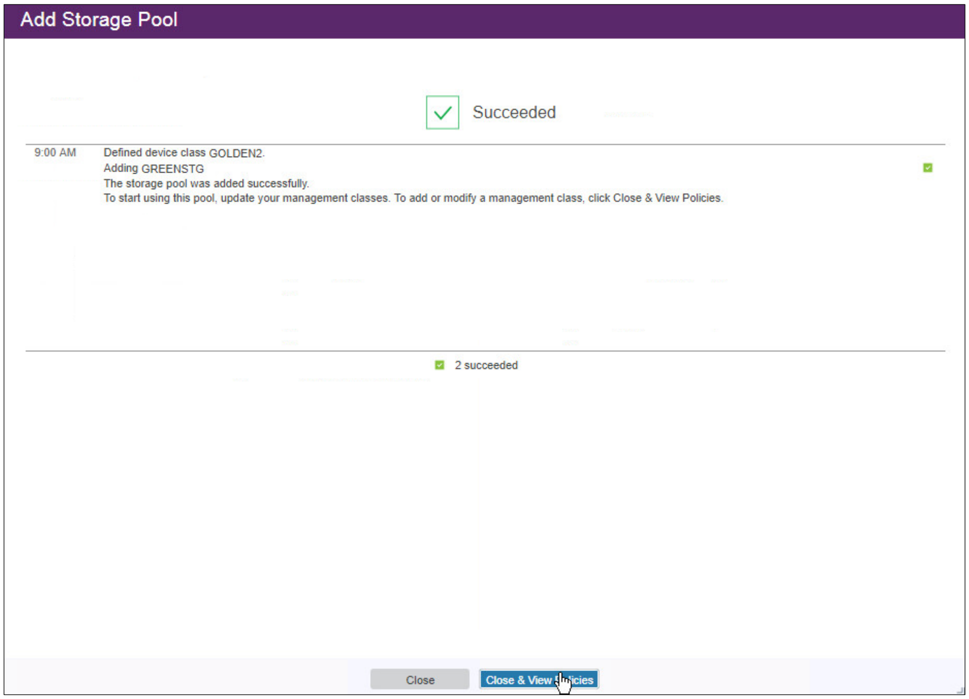
Select a copy pool to back up the data that is stored in GREENSTG. Learn more

There are no copy pools defined for GREENTEC.

Copy pool (optional): Select

Back up daily at

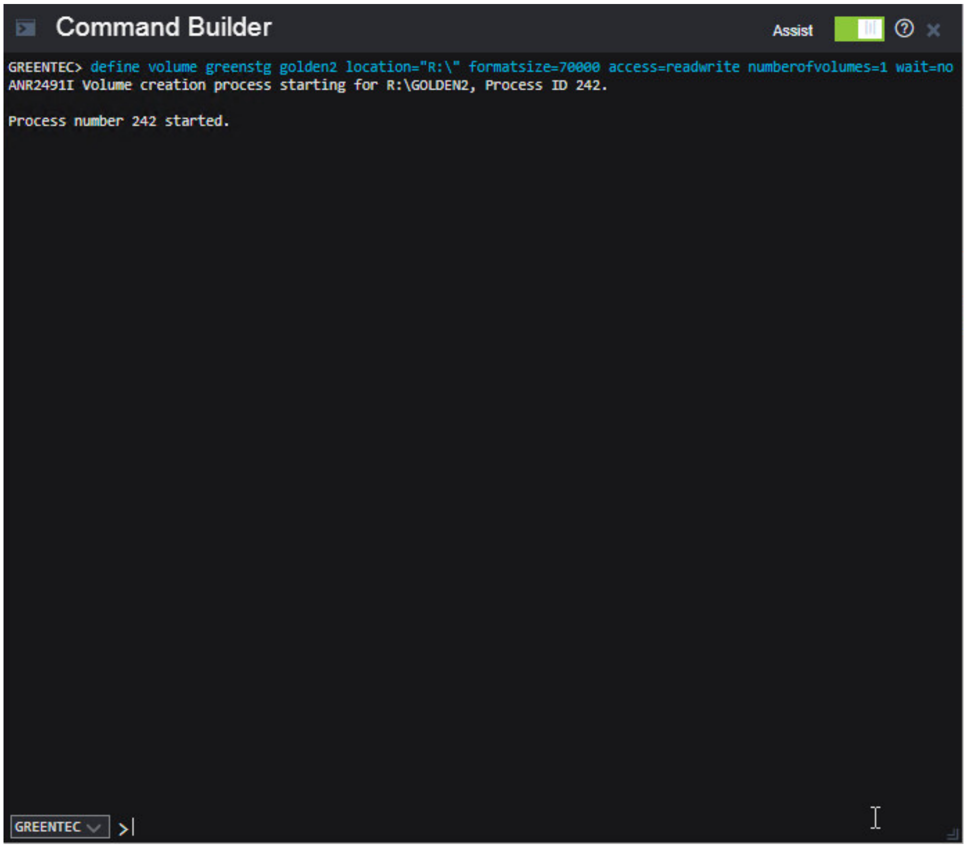
11. Click **Add Storage Pool**.



9:00 AM Defined device class GOLDEN2.
Adding GREENSTG
The storage pool was added successfully.
To start using this pool, update your management classes. To add or modify a management class, click Close & View Policies.

12. Click **Close & View Policies**.
13. Issue the following command in the Operations Center command builder to create a volume on the backup disk.

```
define volume goldenstg golden1 location="E:\" formatsize=350000
access=readwrite numberofvolumes=1 wait=no
```



```
GREENTEC> define volume greenstg golden2 location="R:\" formatsize=70000 access=readwrite numberofvolumes=1 wait=no
ANR2491I Volume creation process starting for R:\GOLDEN2, Process ID 242.

Process number 242 started.
```

14. The storage pool may indicate that there is no capacity, but once you back up something it should correctly show the capacity.

2.13.5 Create a Policy to Back Up to GreenTec disks

1. Issue the following command in the Operations Center (on the GreenTec server) command builder to delete the standard policy domain:

```
delete domain standard
```

2. Issue the following command to create a new domain.

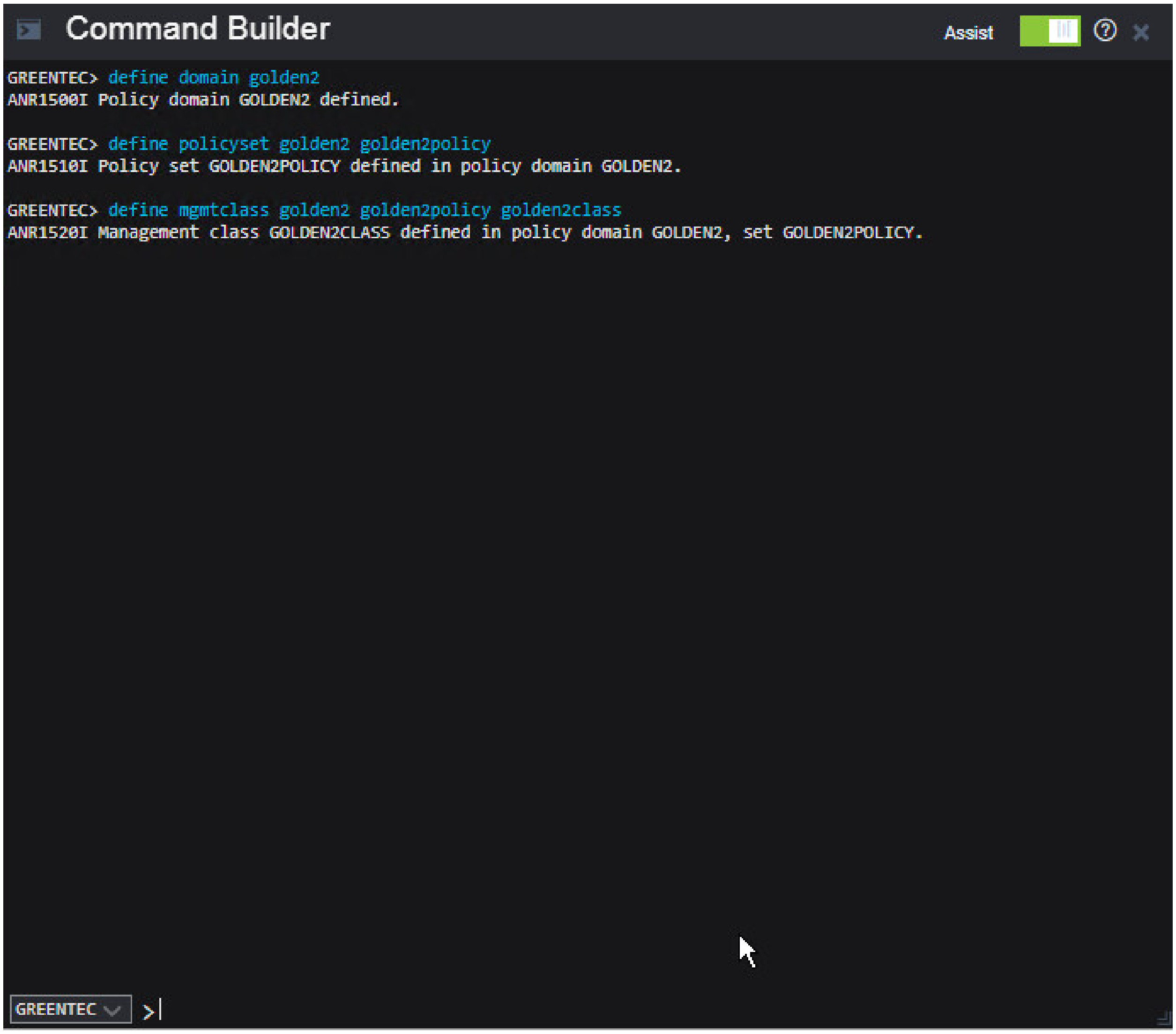
```
define domain golden
```

3. Issue the following command to create a new policy set in this domain.

```
define policyset goldenpolicy
```

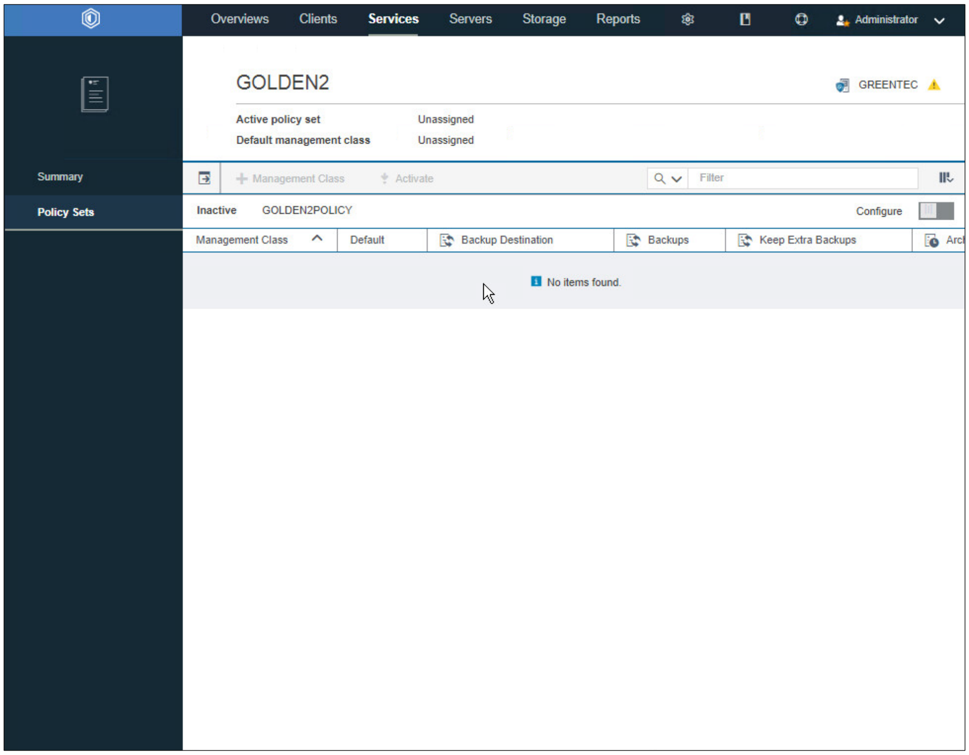
4. Issue the following command to create a management class in this domain.

```
define mgmtclass golden goldenpolicy goldenclass
```



```
GREENTEC> define domain golden2
ANR1500I Policy domain GOLDEN2 defined.

GREENTEC> define policyset golden2 golden2policy
ANR1510I Policy set GOLDEN2POLICY defined in policy domain GOLDEN2.

GREENTEC> define mgmtclass golden2 golden2policy golden2class
ANR1520I Management class GOLDEN2CLASS defined in policy domain GOLDEN2, set GOLDEN2POLICY.
```

5. Click **Services > Policy Sets**.



GOLDEN2

GREENTEC

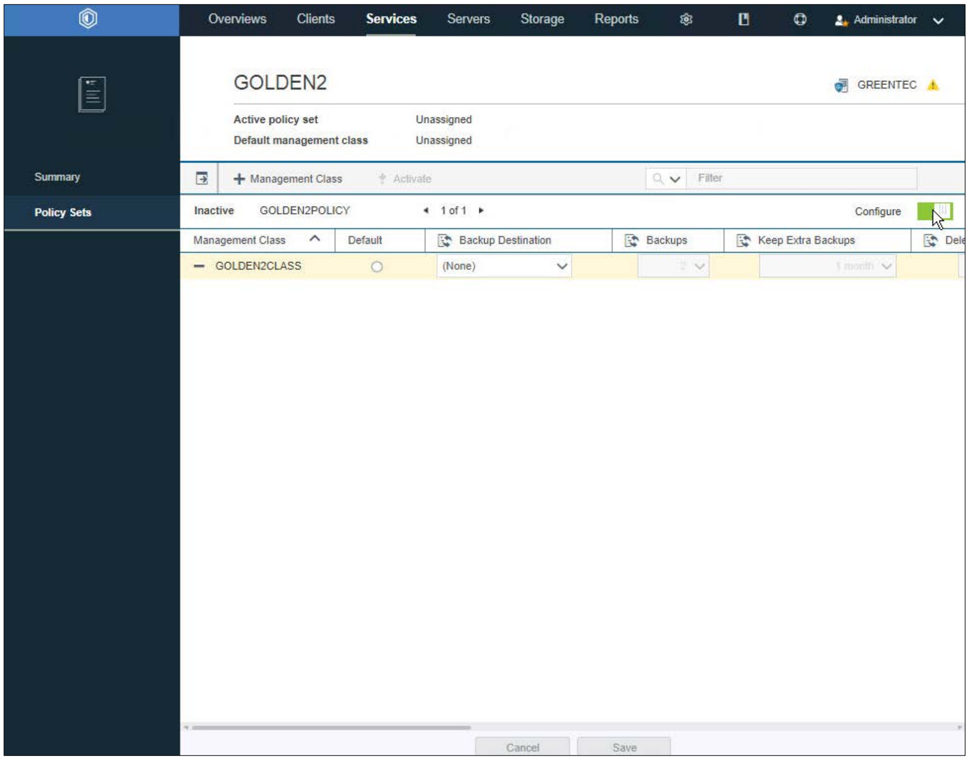
Active policy set Unassigned

Default management class Unassigned

Inactive GOLDEN2POLICY

No items found.

6. Toggle the **Configure** button. This should allow you to edit the settings of the newly created management class.



GOLDEN2

GREENTEC

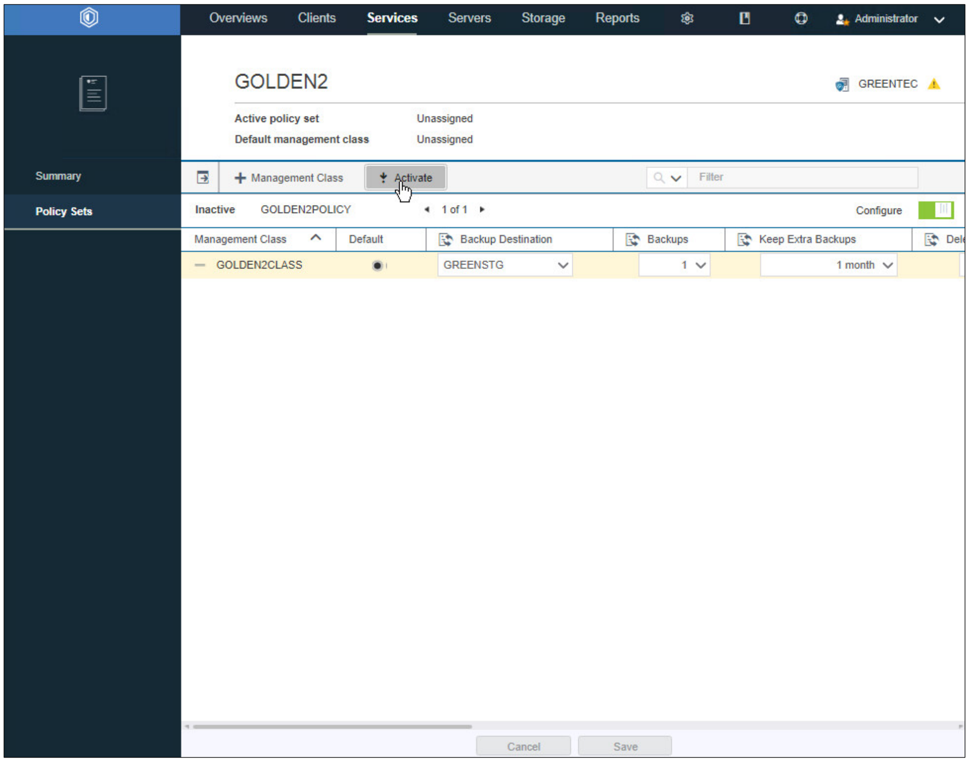
Active policy set Unassigned

Default management class Unassigned

Inactive GOLDEN2POLICY ◂ 1 of 1 ▸

Management Class	Default	Backup Destination	Backups	Keep Extra Backups	Dele
— GOLDEN2CLASS	○	(None)	2	1 month	

7. Select **Default**.
8. For **Backup Destination**, select the storage pool you just created.
9. For **Backups**, select **1**.
10. Select the rest of the settings per your organization's needs.



GOLDEN2 GREENTEC

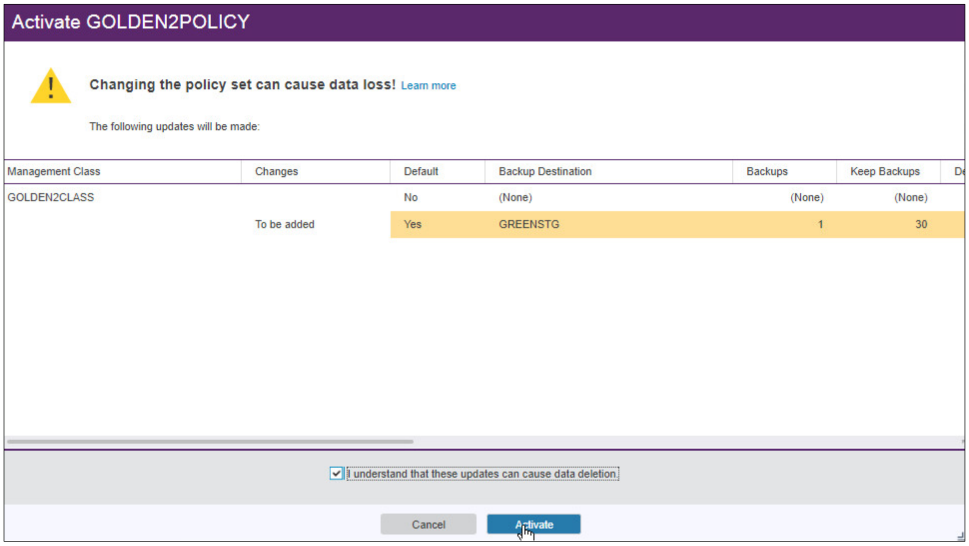
Active policy set Unassigned

Default management class Unassigned

Inactive GOLDEN2POLICY 1 of 1

Management Class	Default	Backup Destination	Backups	Keep Extra Backups	Del
GOLDEN2CLASS	●	GREENSTG	1	1 month	

11. Click the **Activate** button.
12. Check the box next to **I understand that these updates can cause data deletion**.



Activate GOLDEN2POLICY

Changing the policy set can cause data loss!

The following updates will be made:

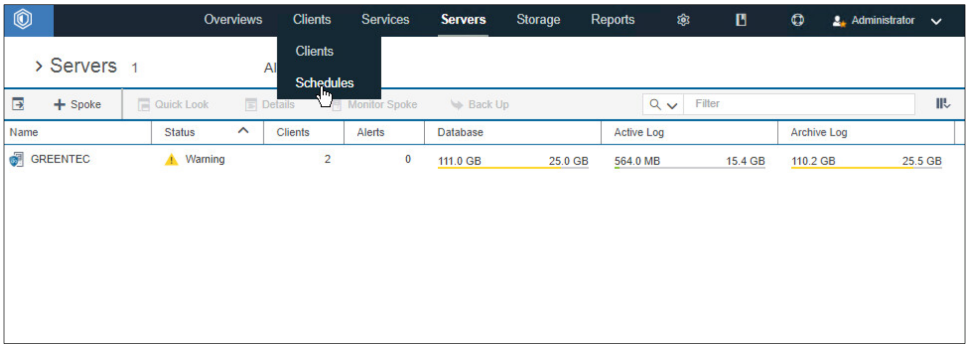
Management Class	Changes	Default	Backup Destination	Backups	Keep Backups	De
GOLDEN2CLASS		No	(None)	(None)	(None)	
	To be added	Yes	GREENSTG	1	30	

☑ I understand that these updates can cause data deletion.

13. Click **Activate**.

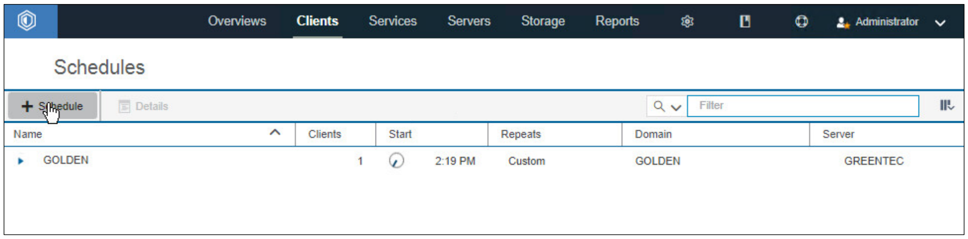
2.13.6 Create a Schedule That Uses the New Policy

1. On the primary IBM Spectrum Protect Server log in to the Operations Center.



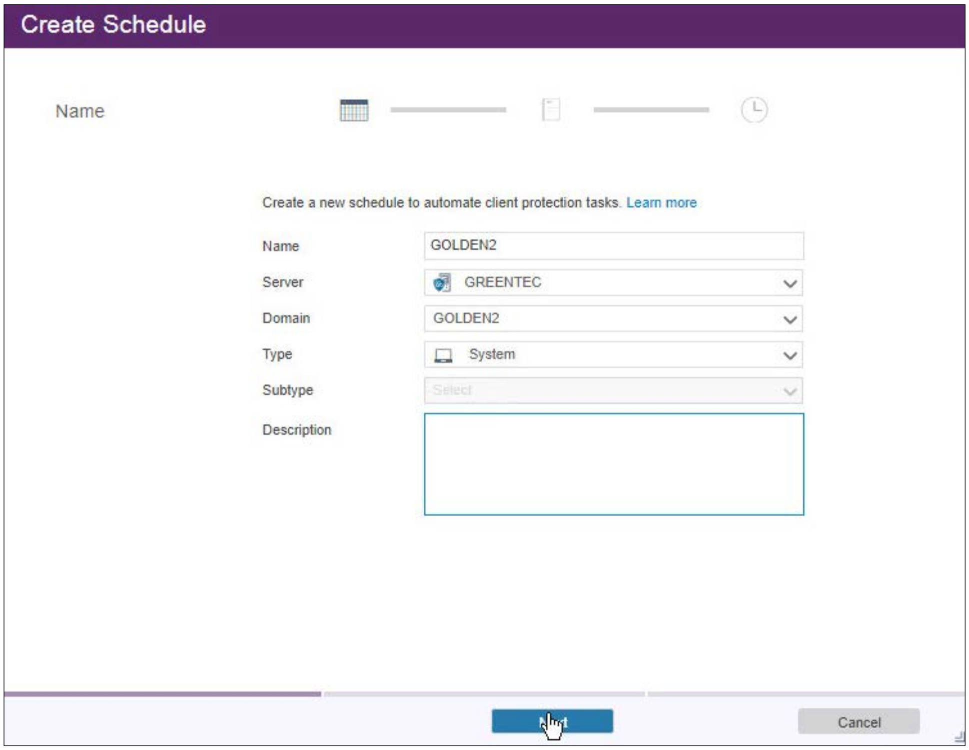
Name	Status	Clients	Alerts	Database	Active Log	Archive Log
GREENTEC	Warning	2	0	111.0 GB 25.0 GB	564.0 MB 15.4 GB	110.2 GB 25.5 GB

2. Go to **Clients > Schedules**.



Name	Clients	Start	Repeats	Domain	Server
GOLDEN	1	2:19 PM	Custom	GOLDEN	GREENTEC

3. Click **+Schedule**.
4. Enter a **name** for the schedule.
5. For **Server**, select the GreenTec server.
6. For **Domain**, select the policy domain you just created.
7. For **Type**, select **System**.



Create Schedule

Name

Create a new schedule to automate client protection tasks. Learn more

Name: GOLDEN2

Server: GREENTEC

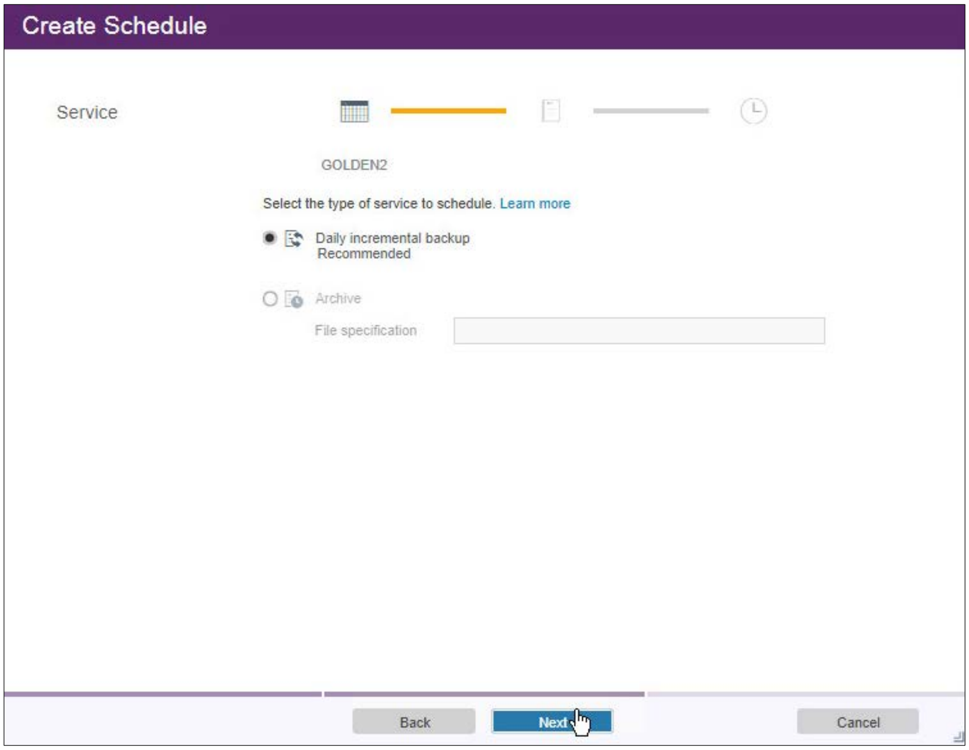
Domain: GOLDEN2

Type: System

Subtype: Select

Description:

8. Click **Next**.
9. Select **Daily incremental backup**.



Create Schedule

Service

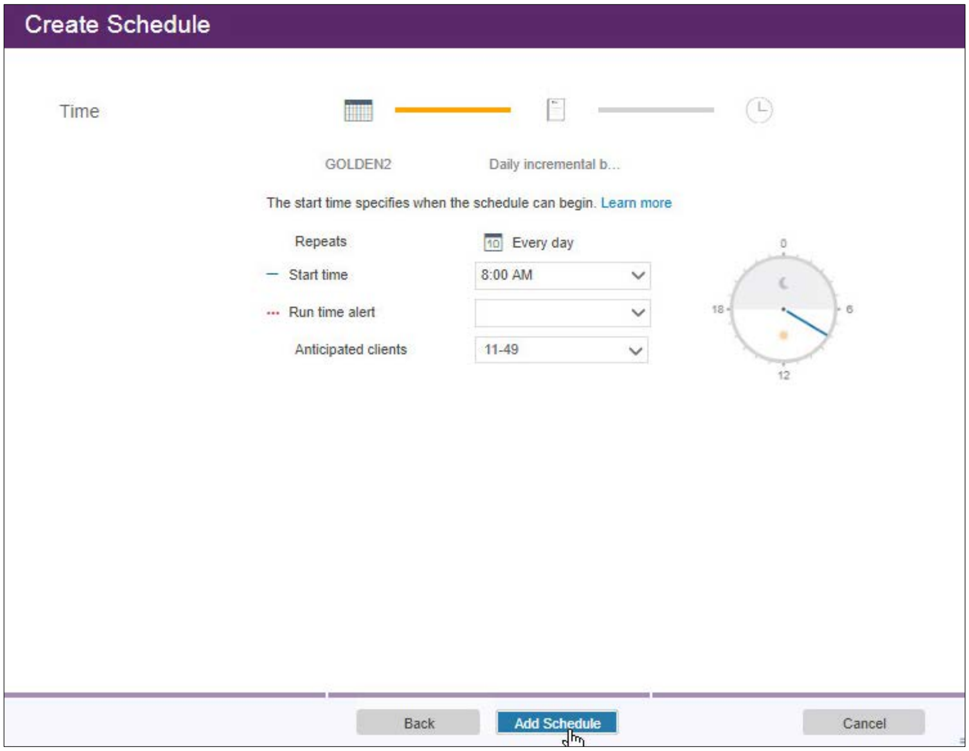
GOLDEN2

Select the type of service to schedule. Learn more

● Daily incremental backup
Recommended

○ Archive
File specification

10. Click **Next**.
11. Configure the schedule settings for your organization's needs. This can be changed later.


Create Schedule

Time

GOLDEN2 Daily incremental b...

The start time specifies when the schedule can begin. Learn more

Repeats: Every day

Start time: 8:00 AM

Run time alert:

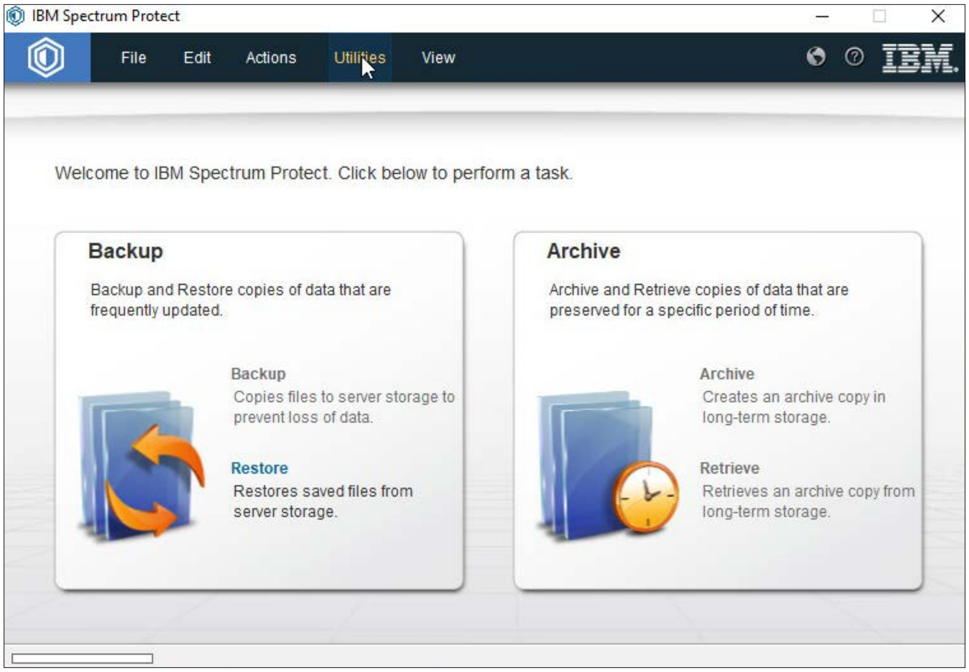
Anticipated clients: 11-49

12. Click **Add Schedule**.
13. From the command builder, run the following command to update the schedule:

```
update schedule golden golden starttime=now action=backup type=client
objects="c:\*" startdate=06/10/2017 perunits=onetime
```

2.13.7 Installing Open File Support on the Client

1. Open the client machine (with the IBM Backup Archive Client installed) to make a golden disk.



Welcome to IBM Spectrum Protect. Click below to perform a task.

Backup

Backup and Restore copies of data that are frequently updated.

Backup
Copies files to server storage to prevent loss of data.

Restore
Restores saved files from server storage.

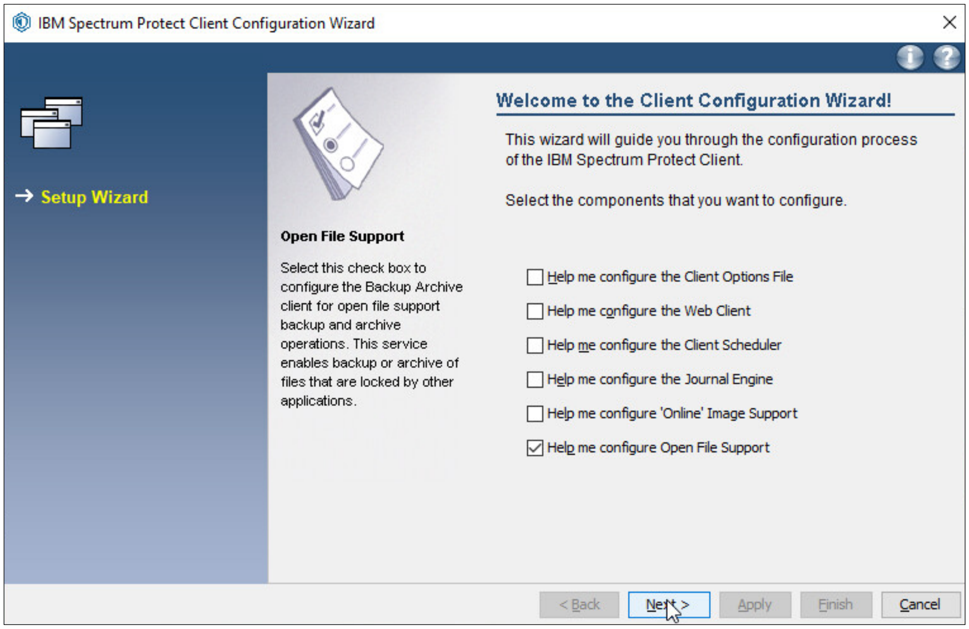
Archive

Archive and Retrieve copies of data that are preserved for a specific period of time.

Archive
Creates an archive copy in long-term storage.

Retrieve
Retrieves an archive copy from long-term storage.

2. Open the **IBM BA Client**.
3. Click **Utilities > Setup Wizard**.
4. Check the box next to **Help me configure Open File Support**.



Welcome to the Client Configuration Wizard!

This wizard will guide you through the configuration process of the IBM Spectrum Protect Client.

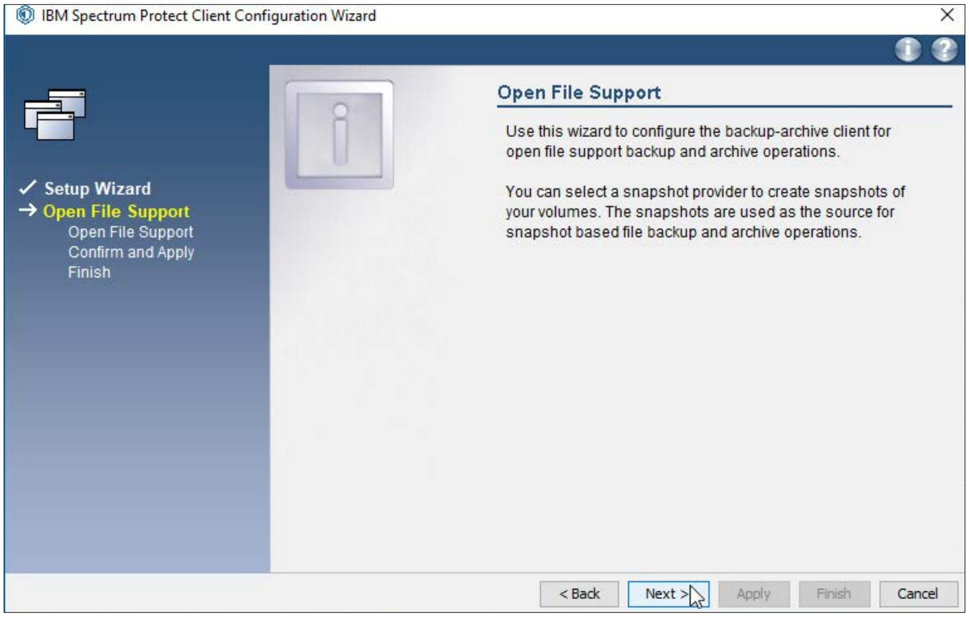
Select the components that you want to configure.

Open File Support

Select this check box to configure the Backup Archive client for open file support backup and archive operations. This service enables backup or archive of files that are locked by other applications.

☐ Help me configure the Client Options File
☐ Help me configure the Web Client
☐ Help me configure the Client Scheduler
☐ Help me configure the Journal Engine
☐ Help me configure 'Online' Image Support
☑ Help me configure Open File Support

5. Click **Next**.



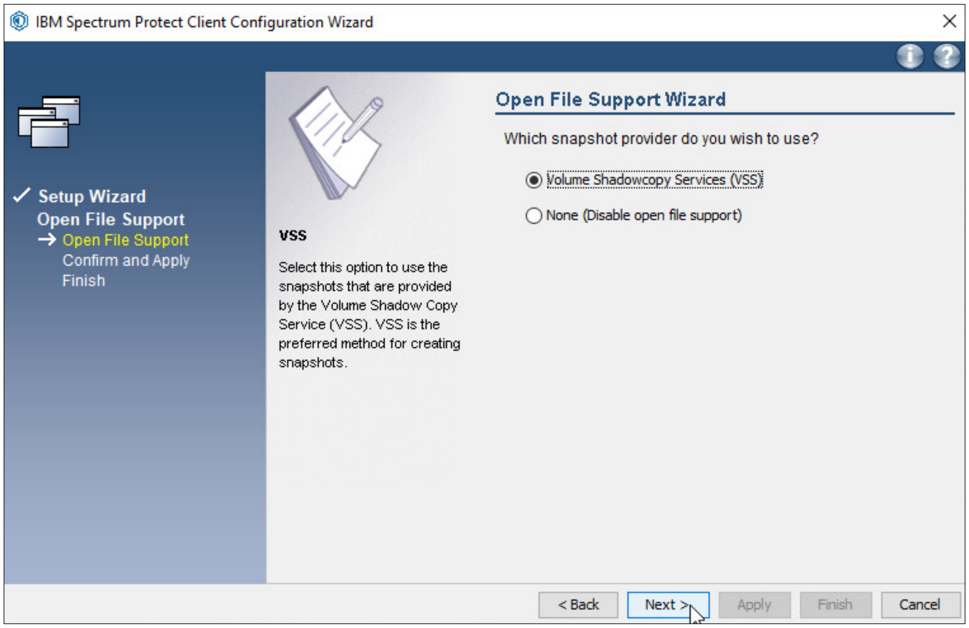
IBM Spectrum Protect Client Configuration Wizard

Open File Support

Use this wizard to configure the backup-archive client for open file support backup and archive operations.

You can select a snapshot provider to create snapshots of your volumes. The snapshots are used as the source for snapshot based file backup and archive operations.

6. Click **Next**.
7. Select **Volume Shadowcopy Services (VSS)**.



IBM Spectrum Protect Client Configuration Wizard

Open File Support Wizard

Which snapshot provider do you wish to use?

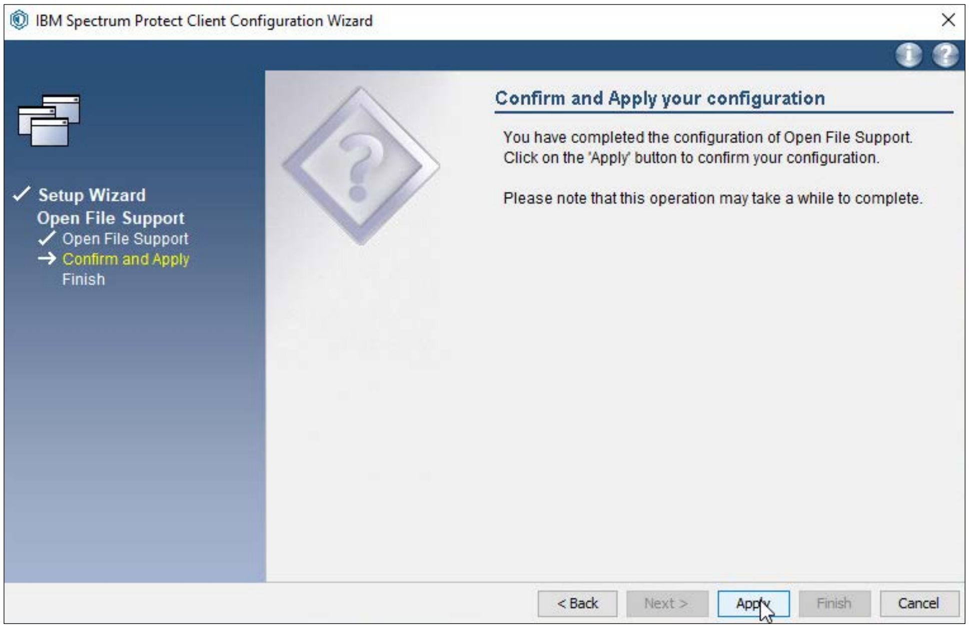
● Volume Shadowcopy Services (VSS)

○ None (Disable open file support)

VSS

Select this option to use the snapshots that are provided by the Volume Shadow Copy Service (VSS). VSS is the preferred method for creating snapshots.

8. Click **Next**.



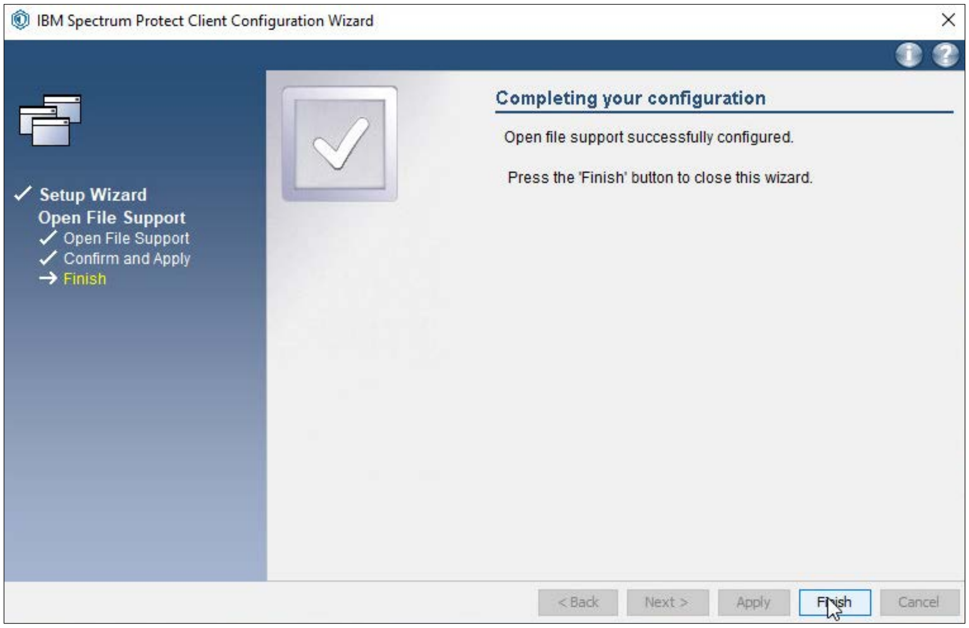
IBM Spectrum Protect Client Configuration Wizard

Confirm and Apply your configuration

You have completed the configuration of Open File Support.
Click on the 'Apply' button to confirm your configuration.

Please note that this operation may take a while to complete.

9. Click **Apply**.



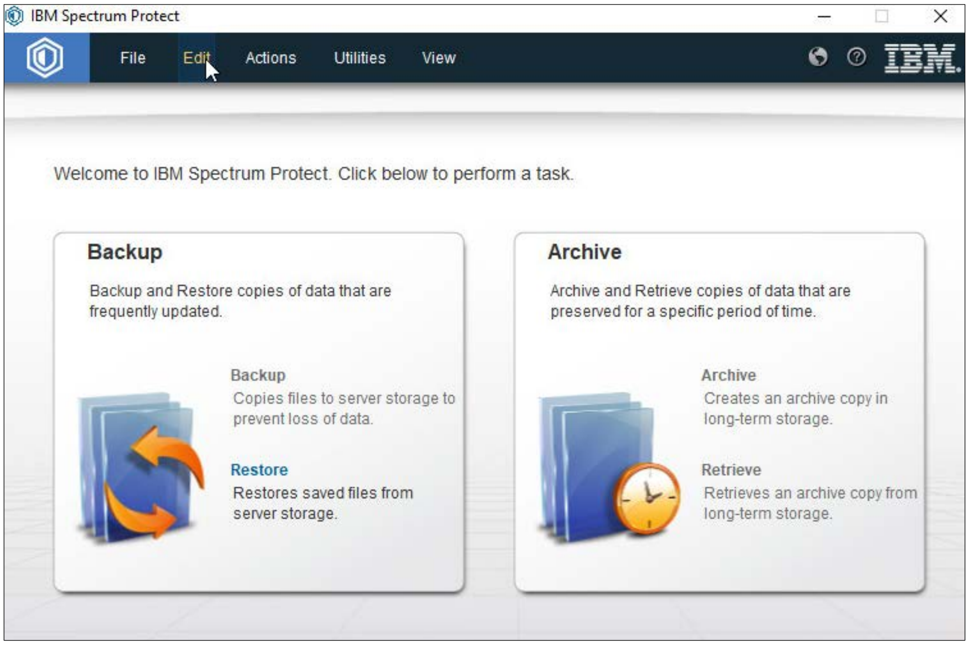
IBM Spectrum Protect Client Configuration Wizard

Completing your configuration

Open file support successfully configured.

Press the 'Finish' button to close this wizard.

10. Click **Finish**.
11. **Restart** the BA Client.



Welcome to IBM Spectrum Protect. Click below to perform a task.

Backup

Backup and Restore copies of data that are frequently updated.

Backup
Copies files to server storage to prevent loss of data.

Restore
Restores saved files from server storage.

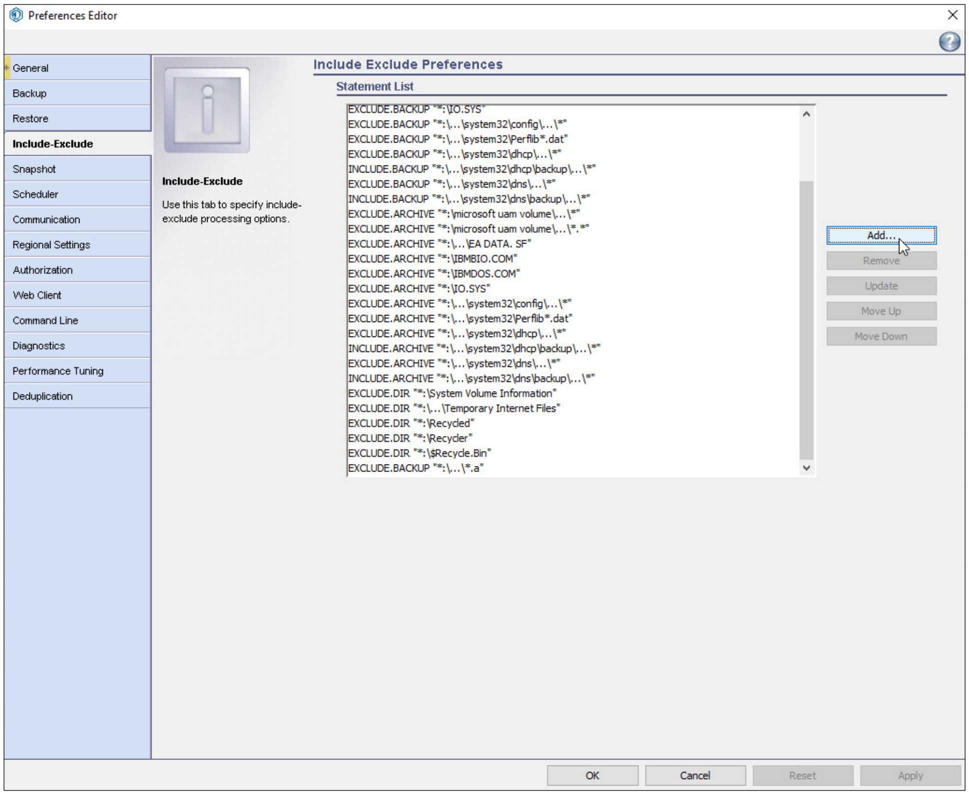
Archive

Archive and Retrieve copies of data that are preserved for a specific period of time.

Archive
Creates an archive copy in long-term storage.

Retrieve
Retrieves an archive copy from long-term storage.

12. Click **Edit > Client Preferences**.
13. Click the **Include-Exclude tab**.



Include-Exclude

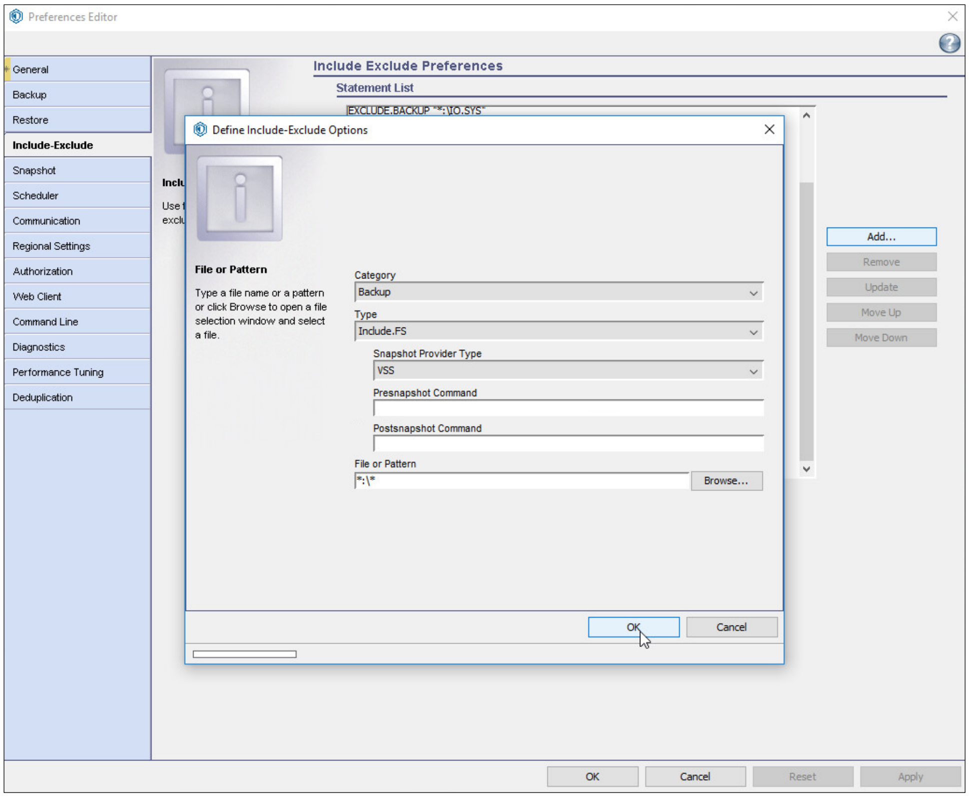
Use this tab to specify include-exclude processing options.

Include Exclude Preferences

Statement List

```
EXCLUDE.BACKUP "*:\IO.SYS"
EXCLUDE.BACKUP "*:\...\system32\config\...\*"
EXCLUDE.BACKUP "*:\...\system32\Perflib*.dat"
EXCLUDE.BACKUP "*:\...\system32\dhcp\...\*"
INCLUDE.BACKUP "*:\...\system32\dhcp\backup\...\*"
EXCLUDE.BACKUP "*:\...\system32\dns\...\*"
INCLUDE.BACKUP "*:\...\system32\dns\backup\...\*"
EXCLUDE.ARCHIVE "*:\microsoft uam volume\...\*"
EXCLUDE.ARCHIVE "*:\microsoft uam volume\...\*.*"
EXCLUDE.ARCHIVE "*:\...\EA DATA. SF"
EXCLUDE.ARCHIVE "*:\IBMBIO.COM"
EXCLUDE.ARCHIVE "*:\IBMDOS.COM"
EXCLUDE.ARCHIVE "*:\IO.SYS"
EXCLUDE.ARCHIVE "*:\...\system32\config\...\*"
EXCLUDE.ARCHIVE "*:\...\system32\Perflib*.dat"
EXCLUDE.ARCHIVE "*:\...\system32\dhcp\...\*"
INCLUDE.ARCHIVE "*:\...\system32\dhcp\backup\...\*"
EXCLUDE.ARCHIVE "*:\...\system32\dns\...\*"
INCLUDE.ARCHIVE "*:\...\system32\dns\backup\...\*"
EXCLUDE.DIR "*:\System Volume Information"
EXCLUDE.DIR "*:\...\Temporary Internet Files"
EXCLUDE.DIR "*:\Recycled"
EXCLUDE.DIR "*:\Recycler"
EXCLUDE.DIR "*:\$Recycle.Bin"
EXCLUDE.BACKUP "*:\...\*.a"
```

14. Click **Add**.
15. For **Category**, select **Backup**.
16. For **Type**, select **Include.FS**.
17. For **Snapshot Provider Type**, choose **VSS**.
18. For **File or Pattern**, enter ***:***.



EXCLUDE.BACKUP "*:\IO.SYS"

File or Pattern

Type a file name or a pattern or click Browse to open a file selection window and select a file.

Category: Backup

Type: Include.FS

Snapshot Provider Type: VSS

Presnapshot Command:

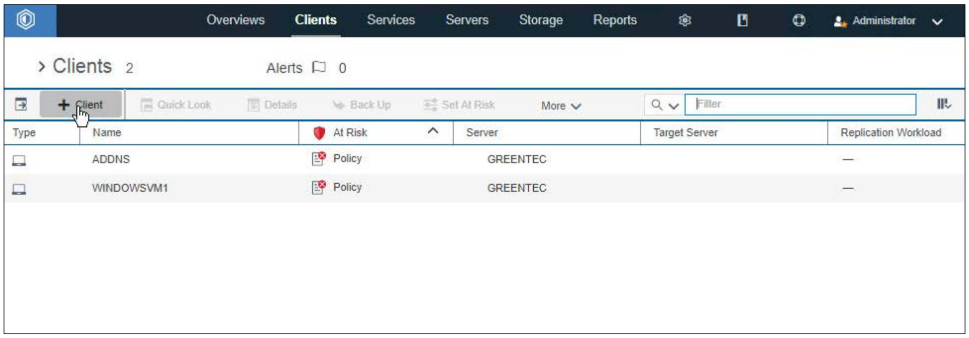
Postsnapshot Command:

File or Pattern: *:*

19. Click **OK**.

2.13.8 Temporarily Add Client to GreenTec IBM Server

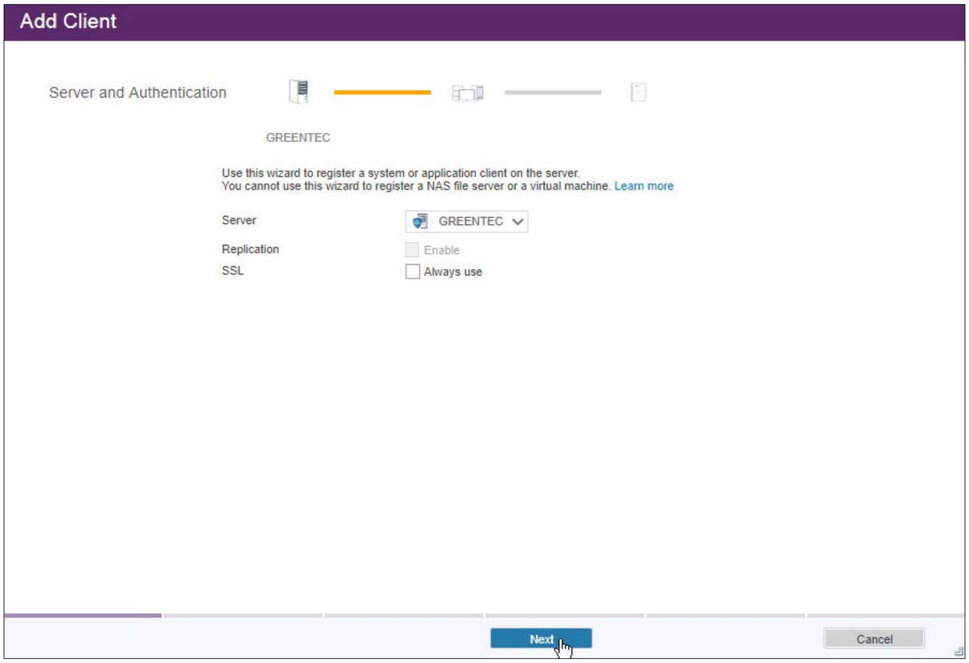
1. Assuming your GreenTec disks are on a separate IBM server, you will need to connect the client you wish to migrate in order to use the created schedule. On the GreenTec server, click **Clients**.



› Clients 2 Alerts 0

Type	Name	At Risk	Server	Target Server	Replication Workload
	ADDNS	Policy	GREENTEC		—
	WINDOWSVM1	Policy	GREENTEC		—

2. Click **+Client**.
3. Select the GreenTec server.



GREENTEC

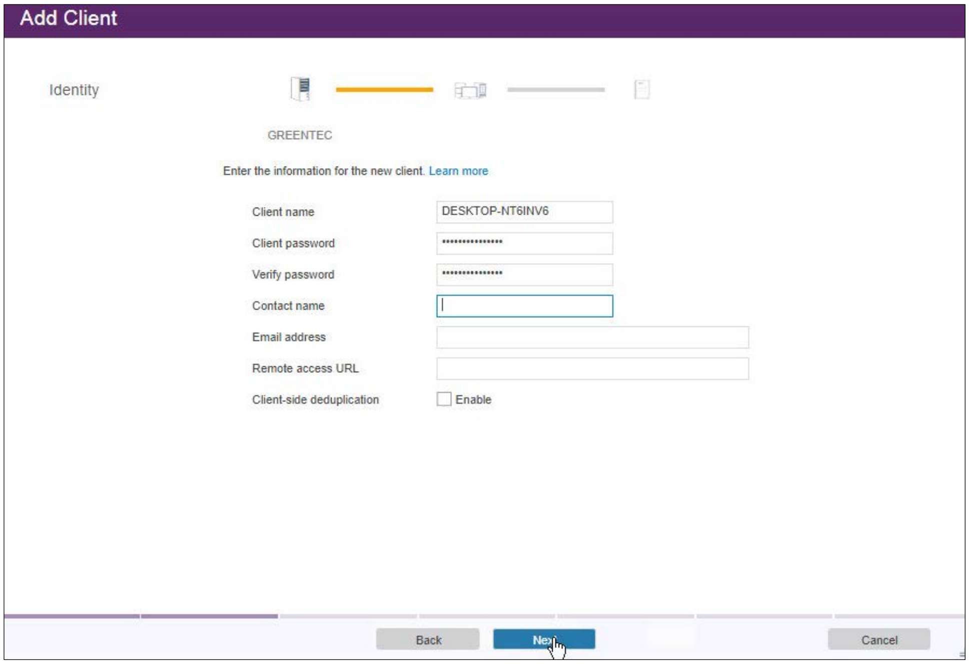
Use this wizard to register a system or application client on the server.
You cannot use this wizard to register a NAS file server or a virtual machine. Learn more

Server: GREENTEC

Replication: ☐ Enable

SSL: ☐ Always use

4. Click **Next**.
5. Enter the information for the client you are migrating to this server.



Add Client

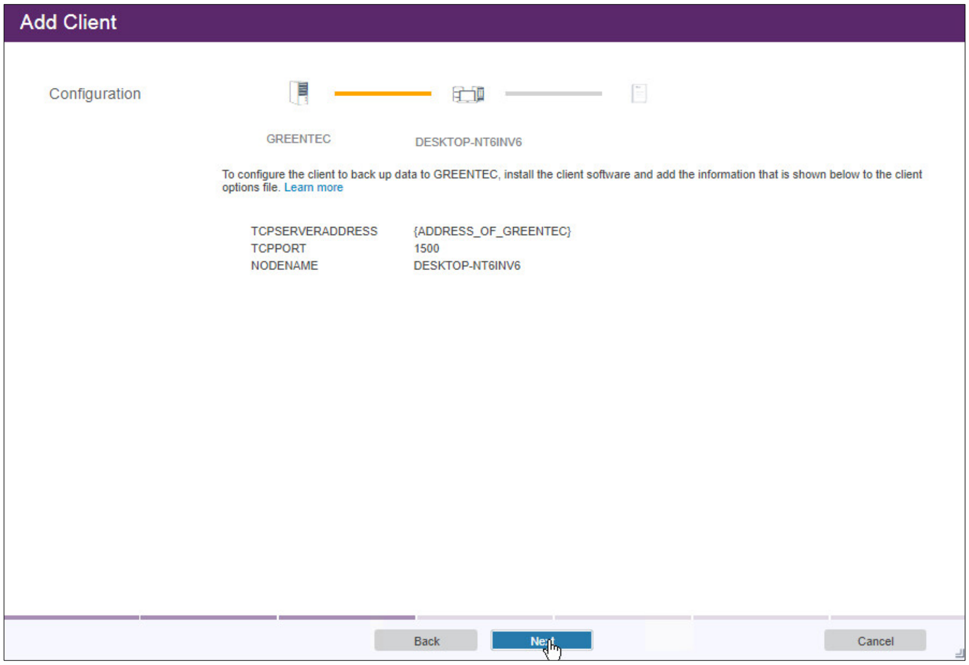
Identity

GREENTEC

Enter the information for the new client. Learn more

Client name	DESKTOP-NT6INV6
Client password	••••••••••••••
Verify password	••••••••••••••
Contact name	
Email address	
Remote access URL	
Client-side deduplication	□ Enable

6. Click **Next**.
7. Take note of the information presented here, namely the **IP** and **port** provided, as you will need it on the client machine to connect to the server.



Add Client

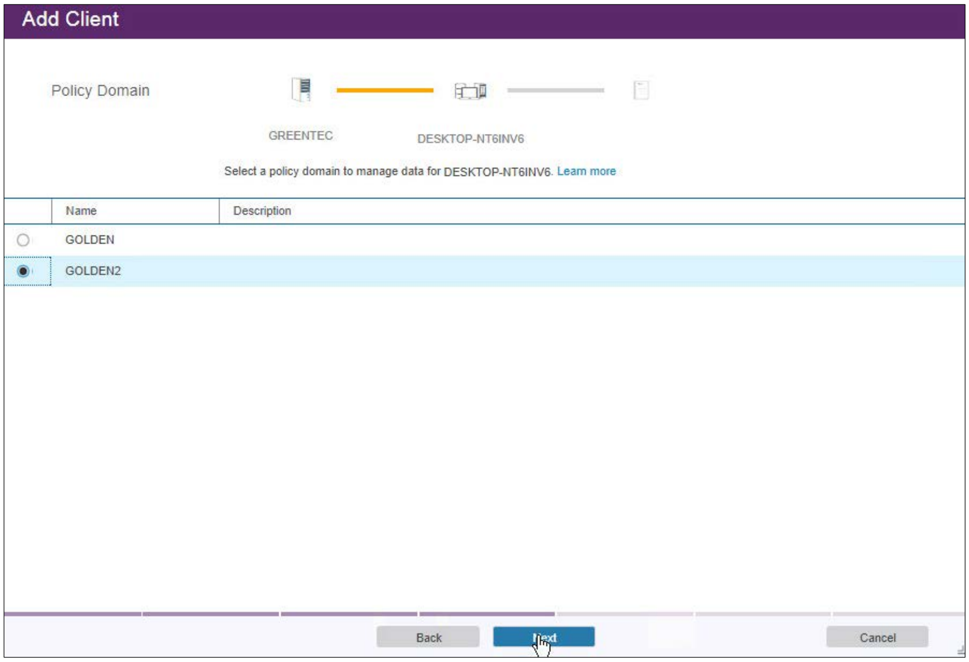
Configuration

GREENTEC DESKTOP-NT6INV6

To configure the client to back up data to GREENTEC, install the client software and add the information that is shown below to the client options file. Learn more

```
TCPSERVERADDRESS     {ADDRESS_OF_GREENTEC}
TCPPORT              1500
NODENAME             DESKTOP-NT6INV6
```

8. Click **Next**.
9. Select the policy domain you created.



Add Client

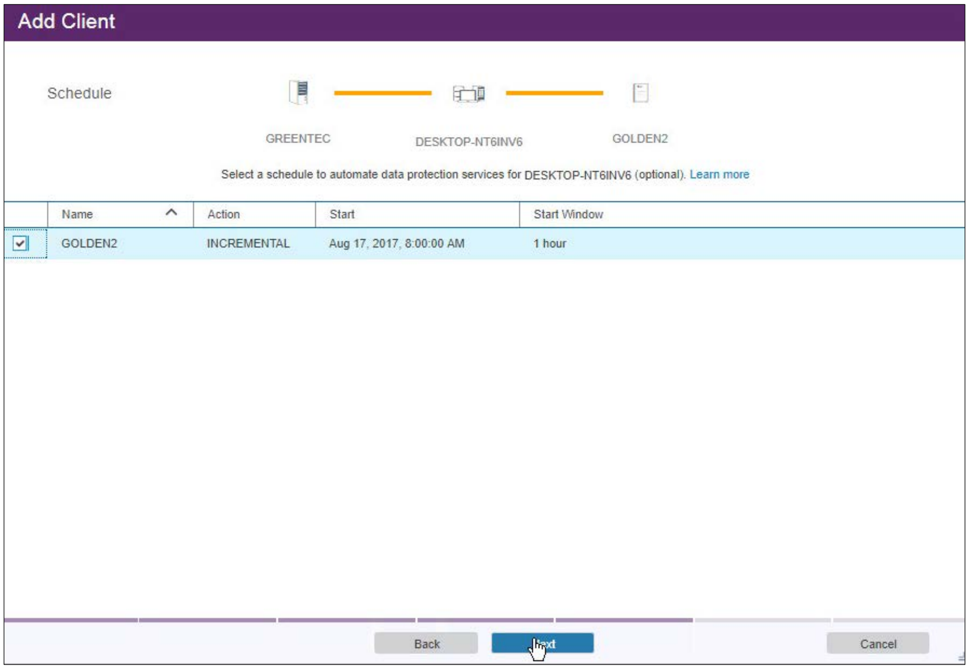
Policy Domain

GREENTEC — DESKTOP-NT6INV6

Select a policy domain to manage data for DESKTOP-NT6INV6. Learn more

	Name	Description
○	GOLDEN	
●	GOLDEN2	

10. Click **Next**.
11. Select the schedule created earlier.



Add Client

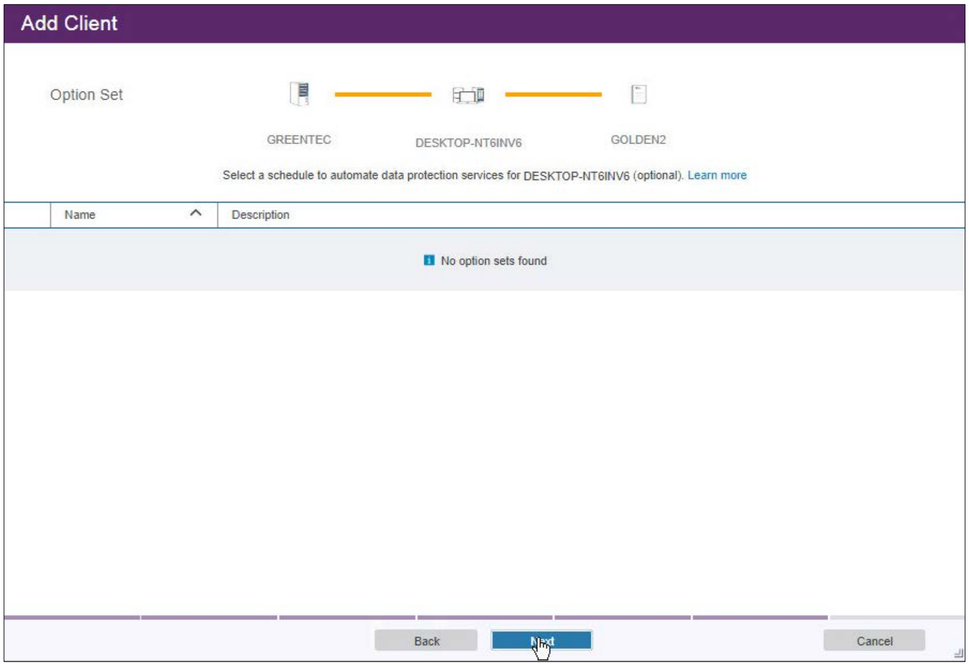
Schedule

GREENTEC — DESKTOP-NT6INV6 — GOLDEN2

Select a schedule to automate data protection services for DESKTOP-NT6INV6 (optional). Learn more

	Name	Action	Start	Start Window
☑	GOLDEN2	INCREMENTAL	Aug 17, 2017, 8:00:00 AM	1 hour

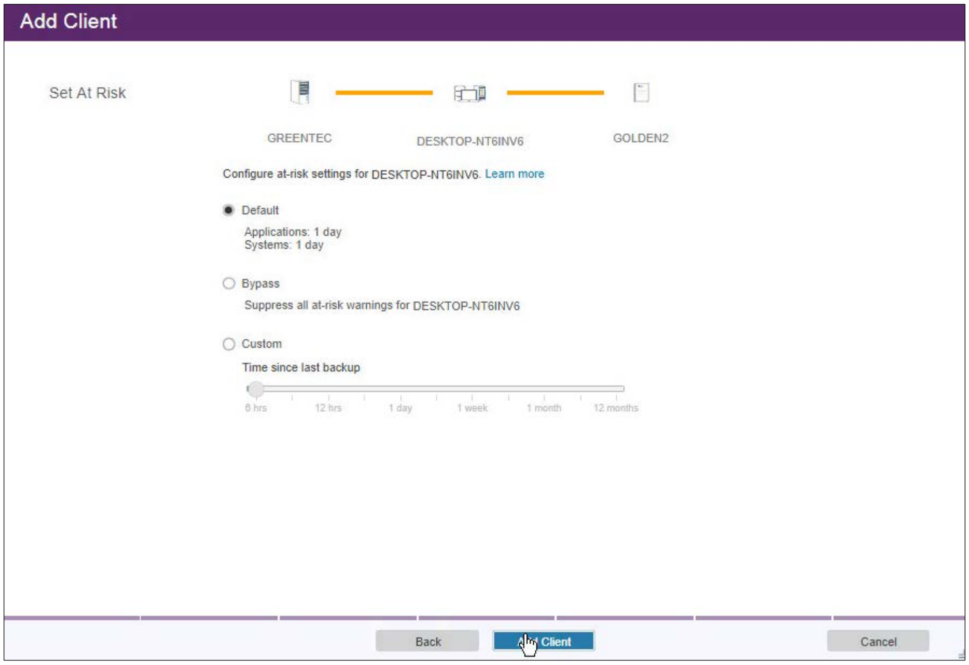
12. Click **Next**.



Select a schedule to automate data protection services for DESKTOP-NT6INV6 (optional). Learn more

No option sets found

13. Click **Next**.
14. Select the at-risk options per your organization's needs.



Configure at-risk settings for DESKTOP-NT6INV6. Learn more

● Default

Applications: 1 day
Systems: 1 day

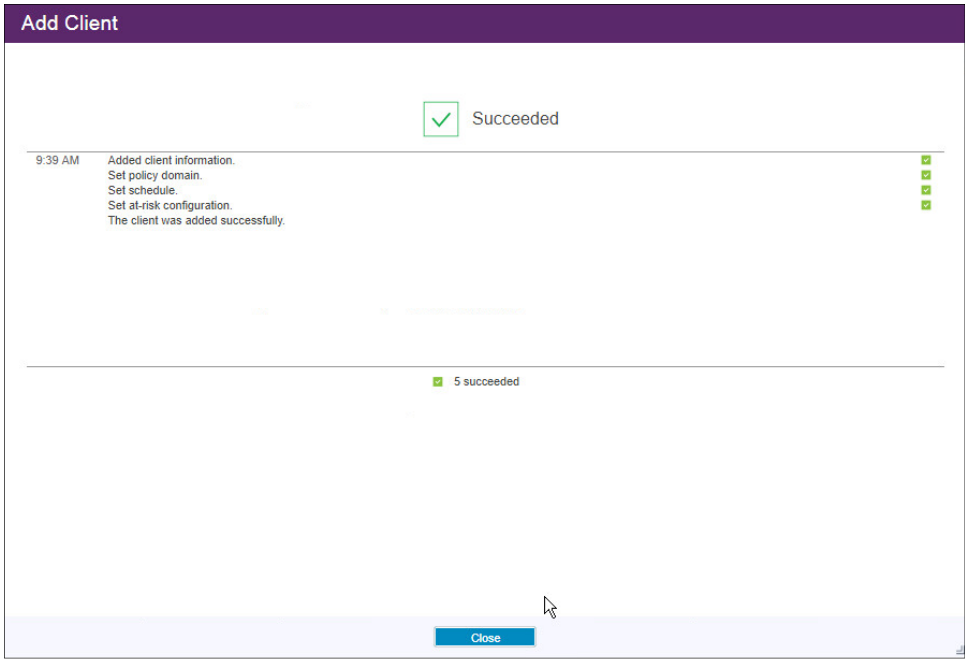
○ Bypass

Suppress all at-risk warnings for DESKTOP-NT6INV6

○ Custom

Time since last backup

15. Click **Add Client**.

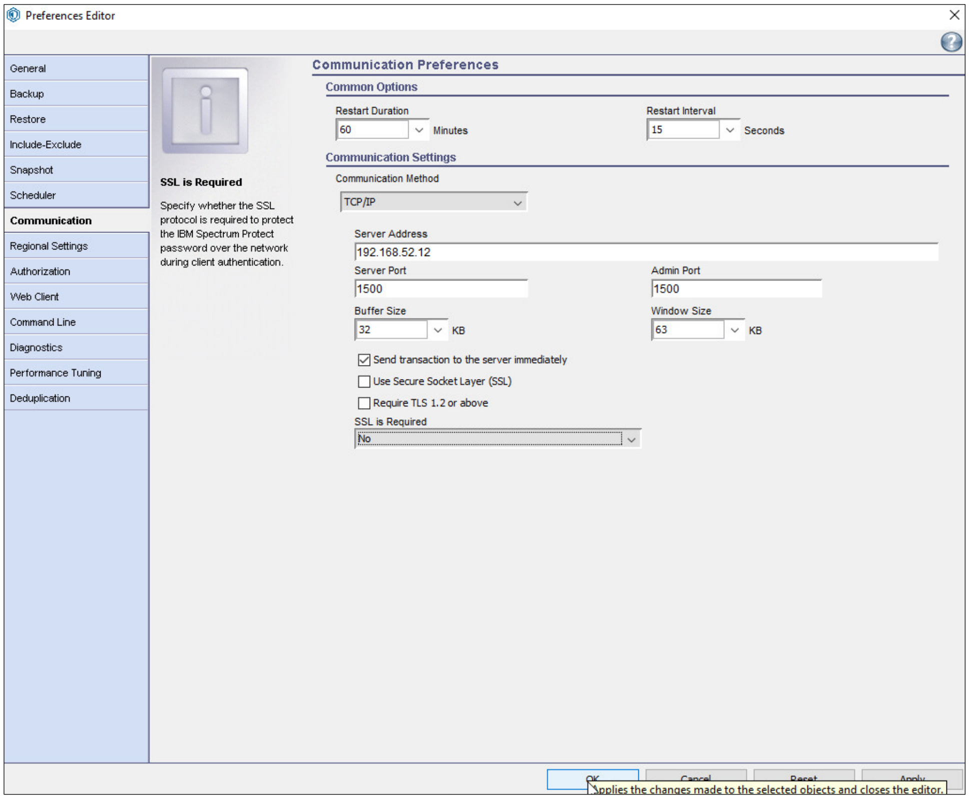

Add Client

Succeeded

9:39 AM Added client information. ✓
Set policy domain. ✓
Set schedule. ✓
Set at-risk configuration. ✓
The client was added successfully.

✓ 5 succeeded

16. Click **Close**.
17. On the client machine, open the BA client.
18. Click **Edit > Client Preferences**.
19. Click the **Communication** tab, and enter the new **server address** and **port**. Only leave **Use SSL** checked if you have set it up for this new server. Similarly, unselect **SSL is required** if you did not setup SSL on this second server.



SSL is Required

Specify whether the SSL protocol is required to protect the IBM Spectrum Protect password over the network during client authentication.

Communication Preferences

Common Options

Restart Duration: 60 Minutes

Restart Interval: 15 Seconds

Communication Settings

Communication Method: TCP/IP

Server Address: 192.168.52.12

Server Port: 1500

Admin Port: 1500

Buffer Size: 32 KB

Window Size: 63 KB

☑ Send transaction to the server immediately

□ Use Secure Socket Layer (SSL)

□ Require TLS 1.2 or above

SSL is Required: No

Applies the changes made to the selected objects and closes the editor.

20. **Restart** the BA client. The client should now connect to the new server.
21. You may be prompted for a password. Enter the password and press **Enter**.
22. To start the schedule, issue the following command in the Operations Center command builder:

```
update schedule golden golden startdate=today starttime=now
```

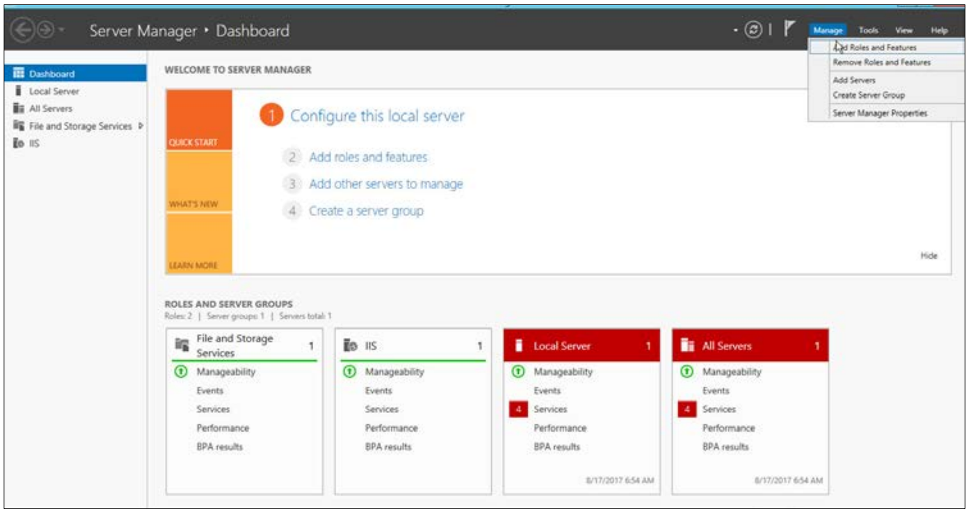
2.14 Integration: Backing Up and Restoring System State with GreenTec

This section covers the process for backing up (and restoring) the Windows System State on a Windows Server with GreenTec as a backup medium. The backup of user information as well as other system state information to a networked GreenTec WORMdisk is intended for the recovery of damage to the Windows system state, such as account permission modification, account creation, account deletion, and various other applicable scenarios.

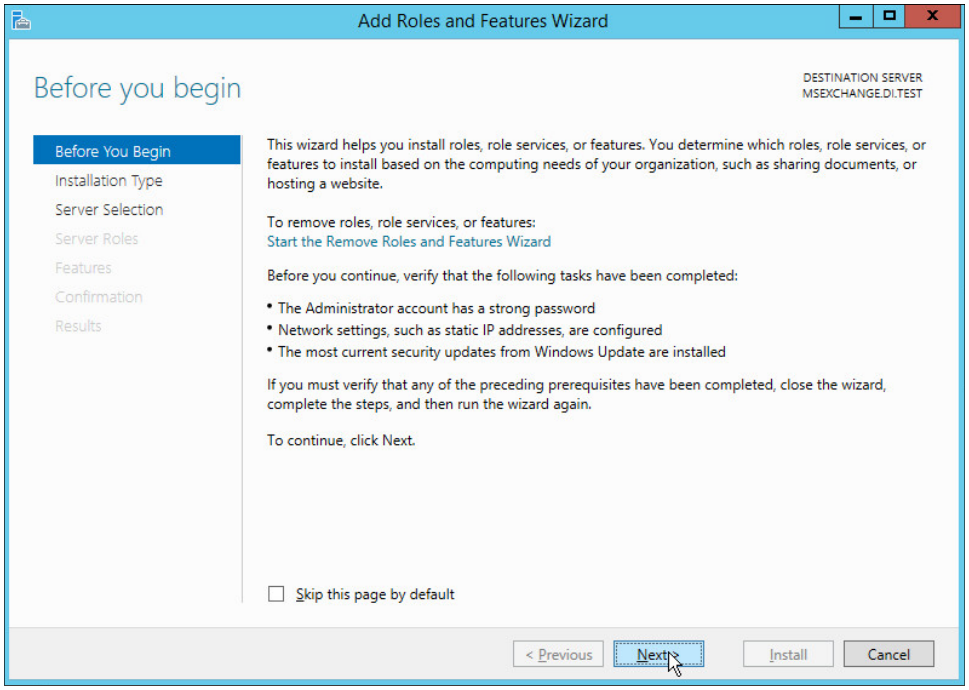
2.14.1 Installing Windows Server Essentials for System State Backup Capability

(NOTE: For older machines, IBM Spectrum Protect's option to back up **SystemState** may be sufficient. However, for newer, more complex versions of Windows, such as Windows Server 2012 and Windows 8+, you should use the following procedure.)

1. Open **Server Manager**.



2. Select **Manage > Add Roles and Features**.



Before you begin

DESTINATION SERVER
MSEXCHANGE.DI.TEST

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

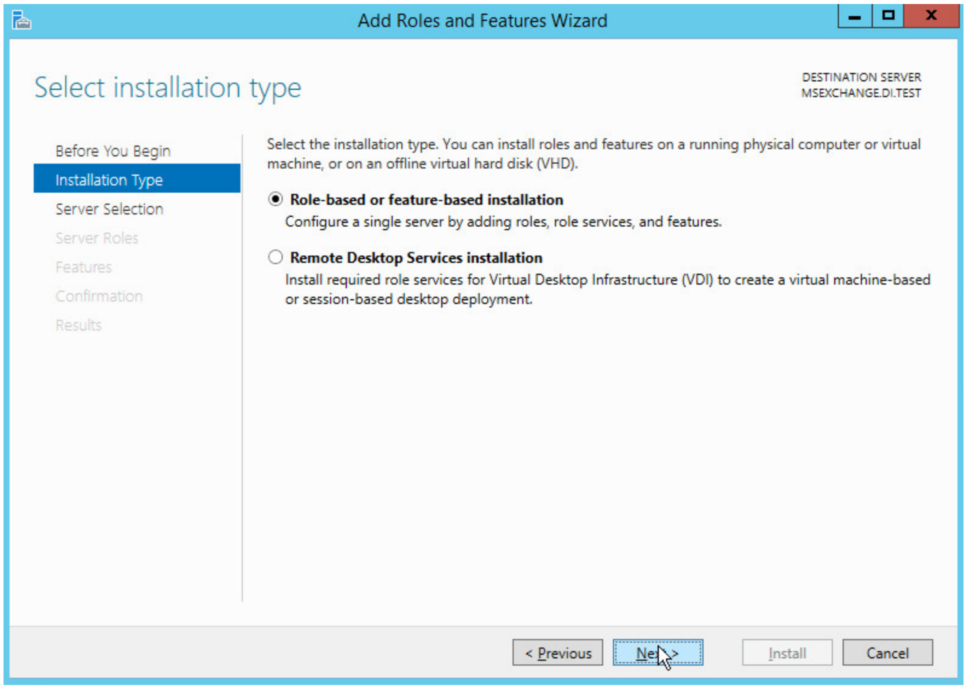
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

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



Add Roles and Features Wizard

Select installation type

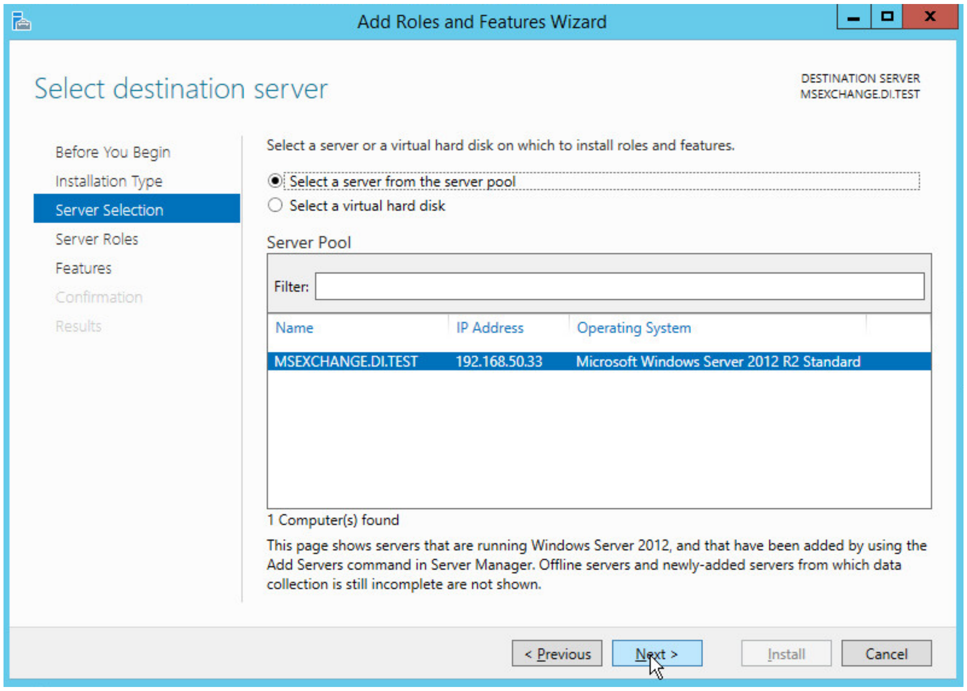
DESTINATION SERVER
MSEXCHANGE.DI.TEST

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

5. Click **Next**.
6. Select the server.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
MSEXCHANGE.DI.TEST

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

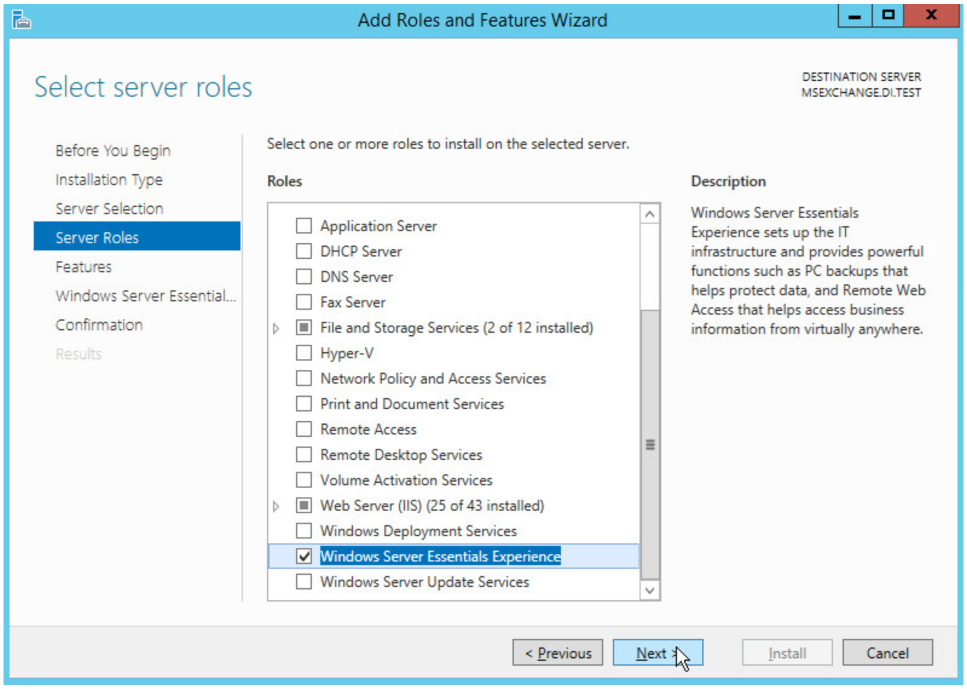
Filter:

Name	IP Address	Operating System
MSEXCHANGE.DI.TEST	192.168.50.33	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.

7. Click **Next**.
8. Select **Windows Server Essentials Experience**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
MSEXCHANGE.DI.TEST

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Windows Server Essential...
- Confirmation
- Results

Select one or more roles to install on the selected server.

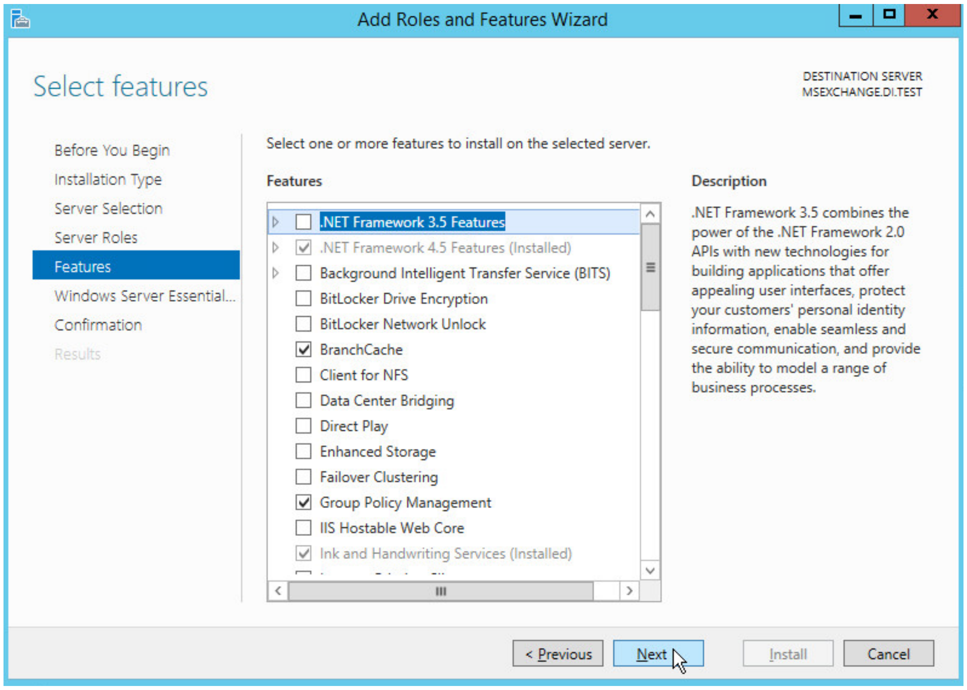
Roles

- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▪ File and Storage Services (2 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ▪ Web Server (IIS) (25 of 43 installed)
- □ Windows Deployment Services
- ☑ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Windows Server Essentials Experience sets up the IT infrastructure and provides powerful functions such as PC backups that helps protect data, and Remote Web Access that helps access business information from virtually anywhere.

9. Click **Next**.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
MSEXCHANGE.DI.TEST

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Windows Server Essential...
- Confirmation
- Results

Select one or more features to install on the selected server.

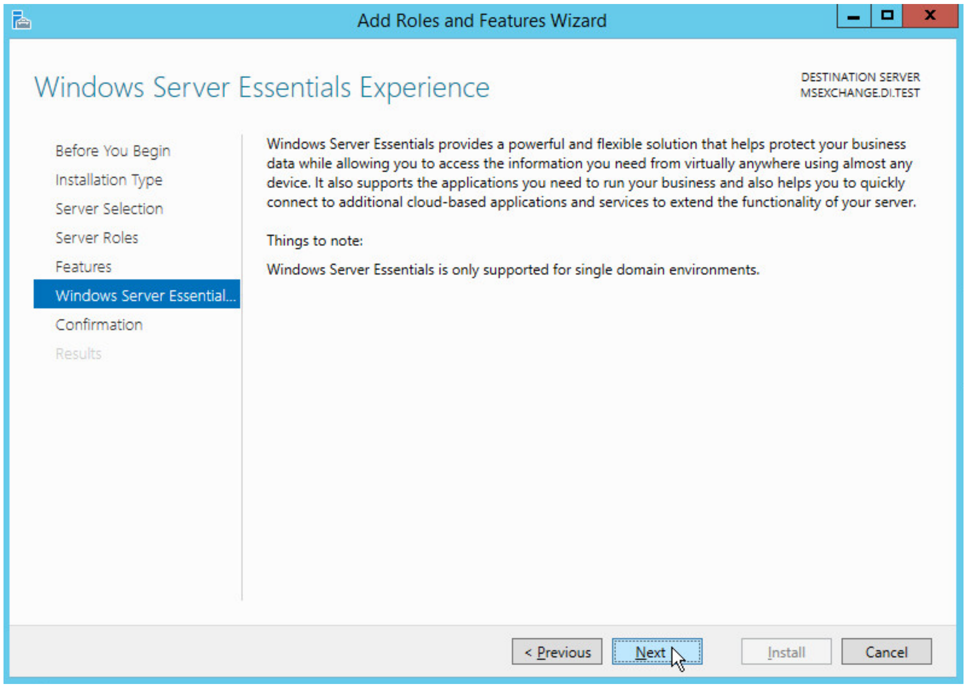
Features

- □ .NET Framework 3.5 Features
- ☑ .NET Framework 4.5 Features (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- ☑ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management
- □ IIS Hostable Web Core
- ☑ Ink and Handwriting Services (Installed)

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

10. Click **Next**.



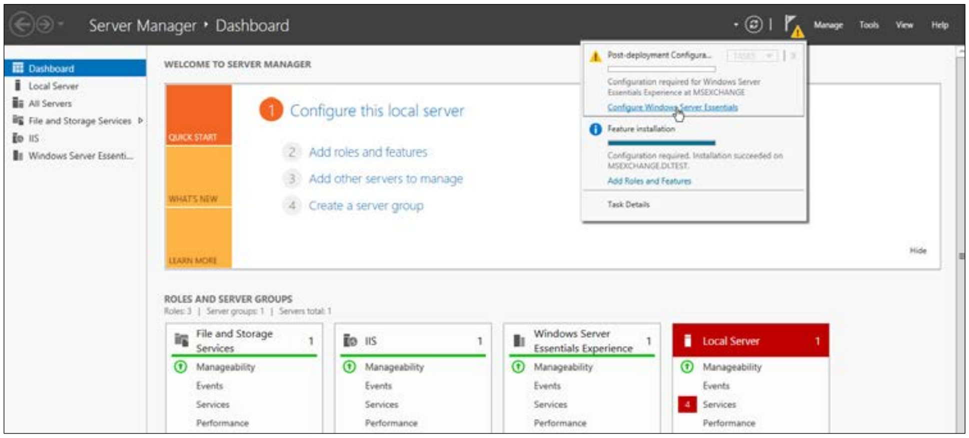
Windows Server Essentials Experience

Windows Server Essentials provides a powerful and flexible solution that helps protect your business data while allowing you to access the information you need from virtually anywhere using almost any device. It also supports the applications you need to run your business and also helps you to quickly connect to additional cloud-based applications and services to extend the functionality of your server.

Things to note:

Windows Server Essentials is only supported for single domain environments.

11. Click **Next**.
12. Click **Install**.


Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Windows Server Essenti...
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Hide
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
File and Storage Services 1
IIS 1
Windows Server Essentials Experience 1
Local Server 1
Manageability
Events
Services
Performance
4

Post-deployment Configura...

Configuration required for Windows Server Essentials Experience at MSEXCHANGE

Configure Windows Server Essentials

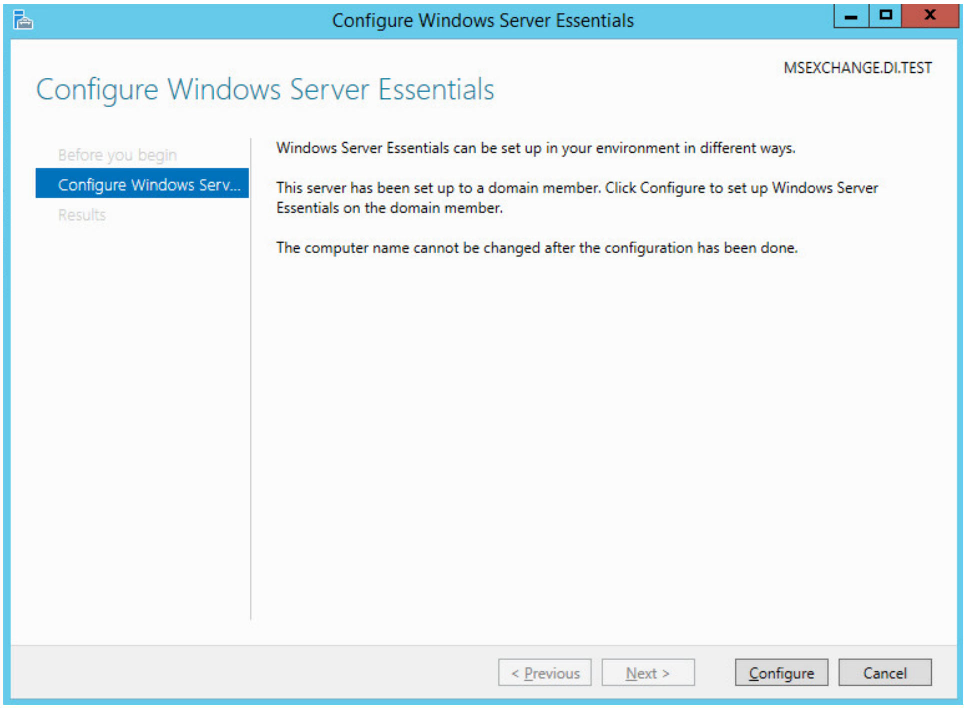
Feature installation

Configuration required. Installation succeeded on MSEXCHANGE.DI.TEST.

Add Roles and Features

Task Details

13. Click **Configure Windows Server Essentials Experience**.


Configure Windows Server Essentials

MSEXCHANGE.DI.TEST

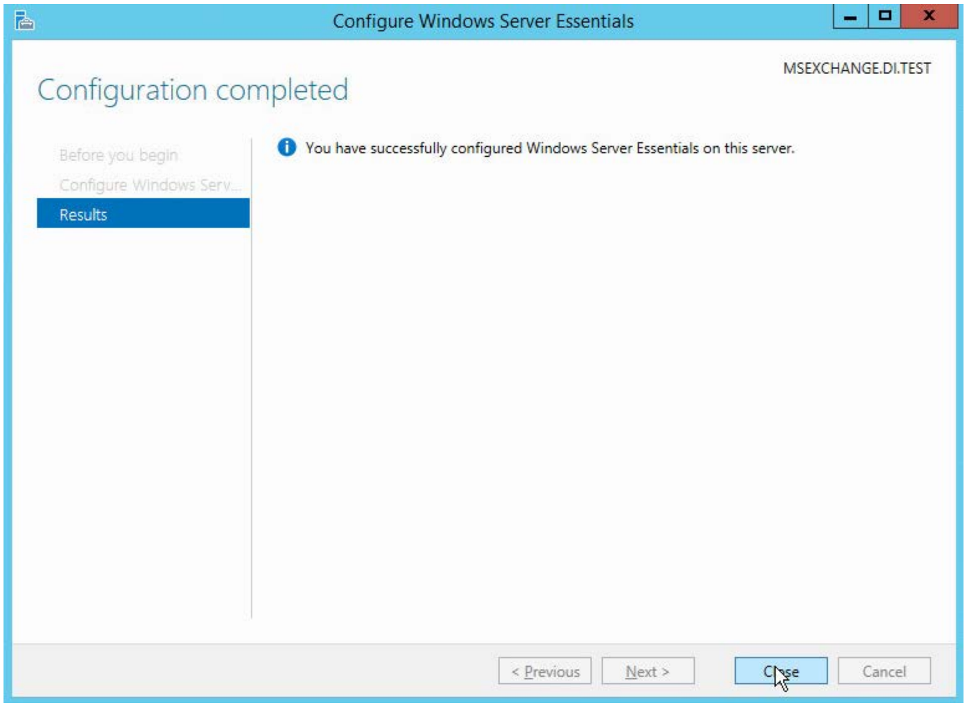
Configure Windows Server Essentials

Windows Server Essentials can be set up in your environment in different ways.

This server has been set up to a domain member. Click Configure to set up Windows Server Essentials on the domain member.

The computer name cannot be changed after the configuration has been done.

14. Click **Configure**.


Configure Windows Server Essentials

MSEXCHANGE.DI.TEST

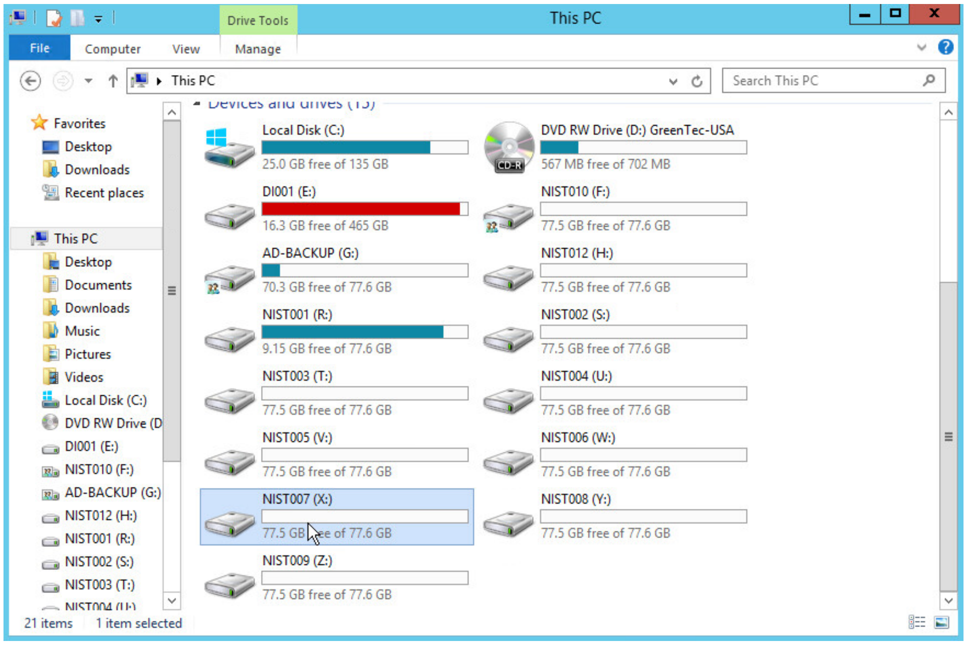
Configuration completed

You have successfully configured Windows Server Essentials on this server.

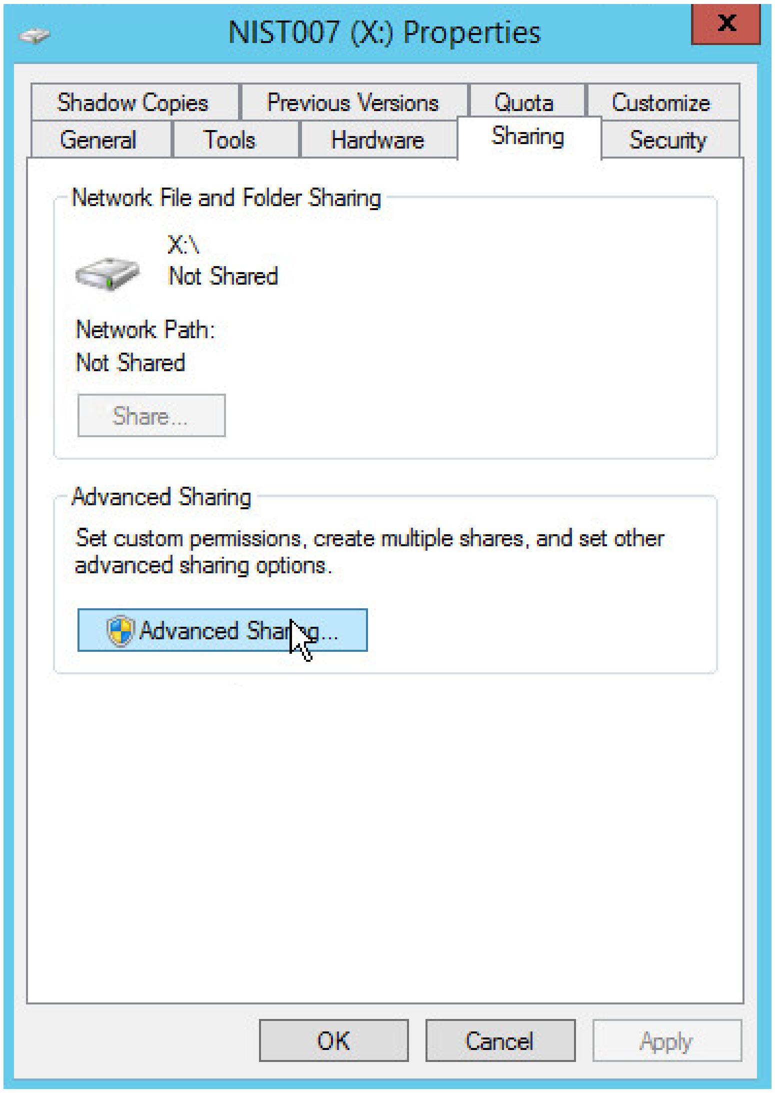
15. Click **Close**.

2.14.2 Configure Network Accessible GreenTec Disk

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



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



NIST007 (X:) Properties

Network File and Folder Sharing

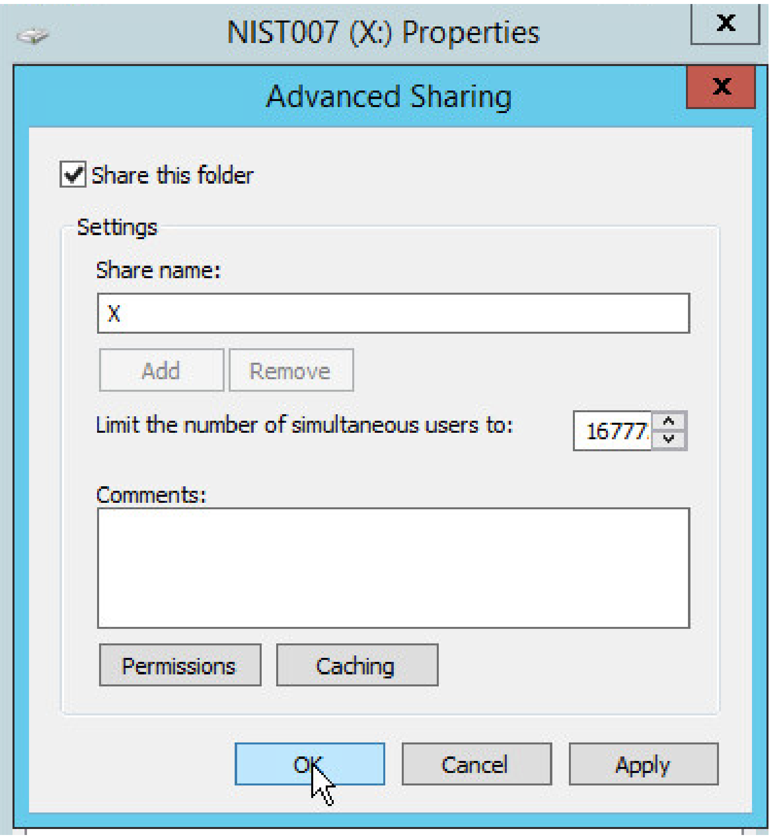
X:\
Not Shared

Network Path:
Not Shared

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

3. Click **Advanced Sharing**.
4. Check the box next to **Share this folder**.

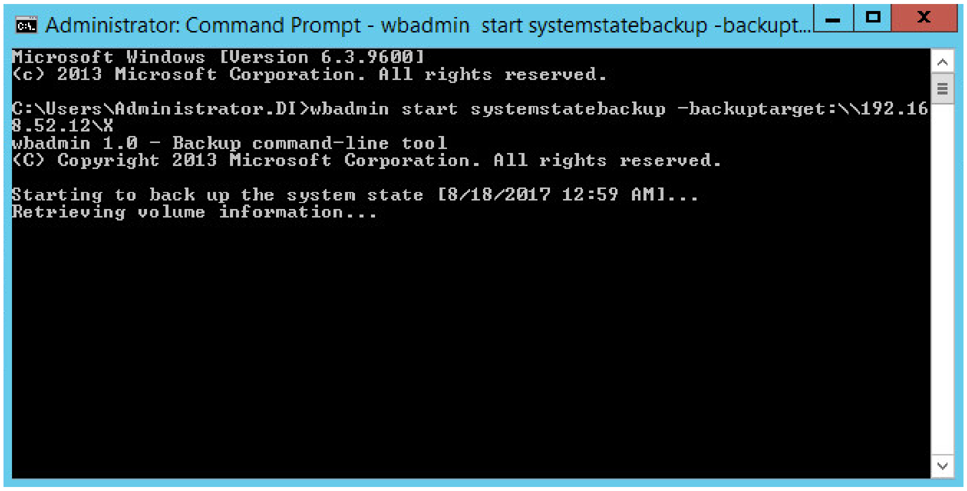


5. Click **OK**.
6. Click **Close**.

2.14.3 Back Up the System State

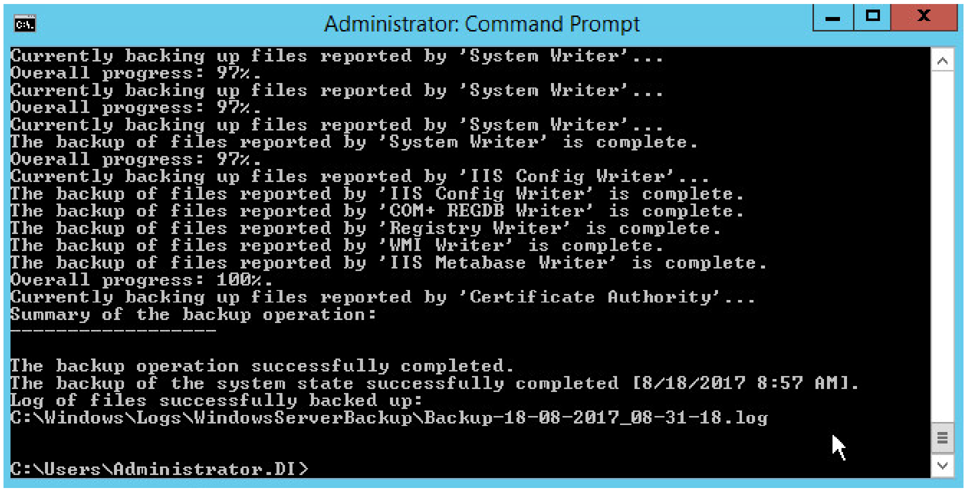
1. Go to command prompt on the Active Directory server and enter the following command:

```
wbadmin start systemstatebackup -backuptarget:z:
```


Administrator: Command Prompt - wbadmin start systemstatebackup -backupt...

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.DI>wbadmin start systemstatebackup -backuptarget:\\192.16
8.52.12\X
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Starting to back up the system state [8/18/2017 12:59 AM]...
Retrieving volume information...
```

(Instead of **z:**, put the location of a disk for the system state backup. You will get an error if you attempt to use the same location as the disc you are trying to back up. Examples of acceptable targets: **C:**, **Z:**, **\\backup-storage\g**)

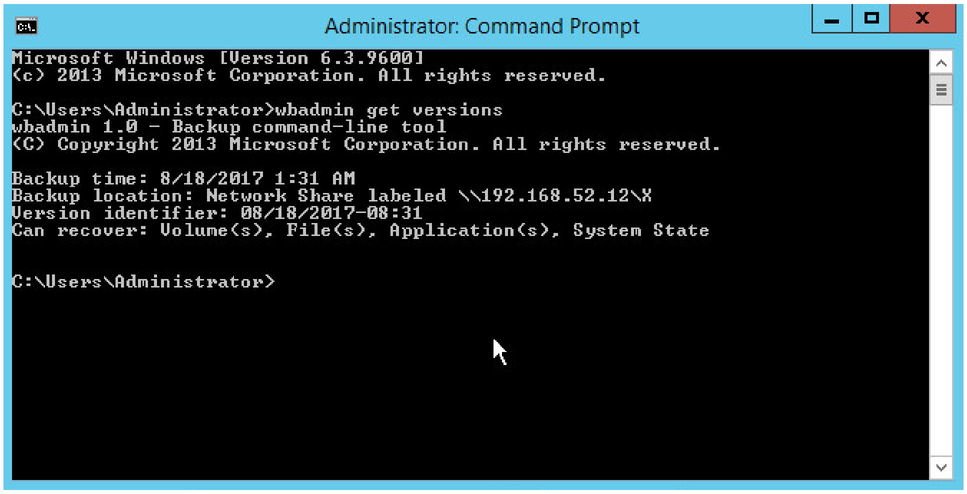


```
Currently backing up files reported by 'System Writer'...
Overall progress: 97%.
Currently backing up files reported by 'System Writer'...
Overall progress: 97%.
Currently backing up files reported by 'System Writer'...
The backup of files reported by 'System Writer' is complete.
Overall progress: 97%.
Currently backing up files reported by 'IIS Config Writer'...
The backup of files reported by 'IIS Config Writer' is complete.
The backup of files reported by 'COM+ REGDB Writer' is complete.
The backup of files reported by 'Registry Writer' is complete.
The backup of files reported by 'WMI Writer' is complete.
The backup of files reported by 'IIS Metabase Writer' is complete.
Overall progress: 100%.
Currently backing up files reported by 'Certificate Authority'...
Summary of the backup operation:
------------------

The backup operation successfully completed.
The backup of the system state successfully completed [8/18/2017 8:57 AM].
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-18-08-2017_08-31-18.log


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

2.14.4 Restoring the System State

1. After determining the point in time of a malicious event, restart the Active Directory Server and press **F2 > F8** to start the **Advanced Boot menu**.
2. Select **Directory Services Repair Mode**.
3. Log in as the machine administrator.
4. Open a command prompt.
5. Enter the following command to see the backup versions available:

```
wbadmin get versions
```

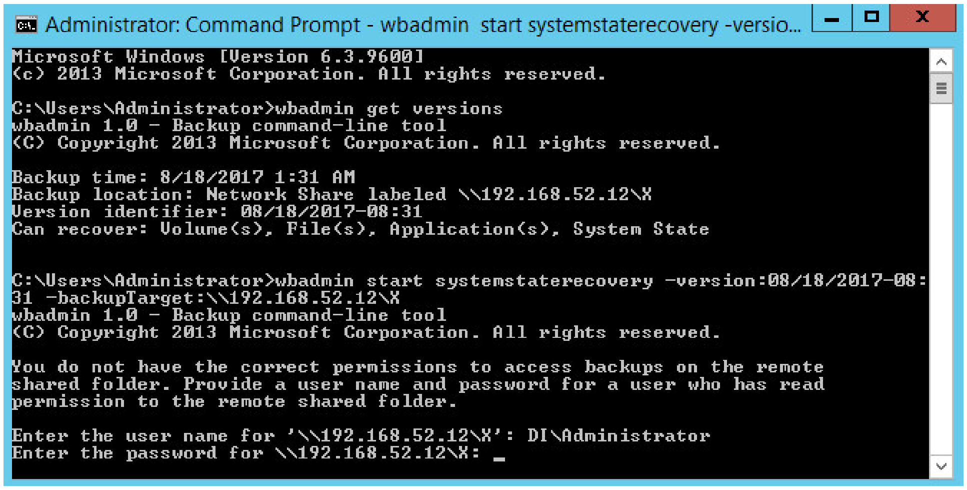


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Backup time: 8/18/2017 1:31 AM
Backup location: Network Share labeled \\192.168.52.12\X
Version identifier: 08/18/2017-08:31
Can recover: Volume(s), File(s), Application(s), System State


C:\Users\Administrator>
```

6. Enter the following command to restore to a specific version (preferably before the malicious event occurred):

```
     wbadmin start systemstaterecovery -version:06/21/2017-15:33 -
    backupTarget:\\192.168.52.12\g
```

   (Replace the **backupTarget** with the location of the backup, and the **version** with the version to restore to.)


Administrator: Command Prompt - wbadmin start systemstaterecovery -versio...

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>wbadmin get versions
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Backup time: 8/18/2017 1:31 AM
Backup location: Network Share labeled \\192.168.52.12\X
Version identifier: 08/18/2017-08:31
Can recover: Volume(s), File(s), Application(s), System State


C:\Users\Administrator>wbadmin start systemstaterecovery -version:08/18/2017-08:
31 -backupTarget:\\192.168.52.12\X
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

You do not have the correct permissions to access backups on the remote
shared folder. Provide a user name and password for a user who has read
permission to the remote shared folder.

Enter the user name for '\\192.168.52.12\X': DI\Administrator
Enter the password for \\192.168.52.12\X: _
```

7. The computer will restart when you finish the restore process.

2.15 Integration: Copying IBM Backup Data to GreenTec WORMdisks

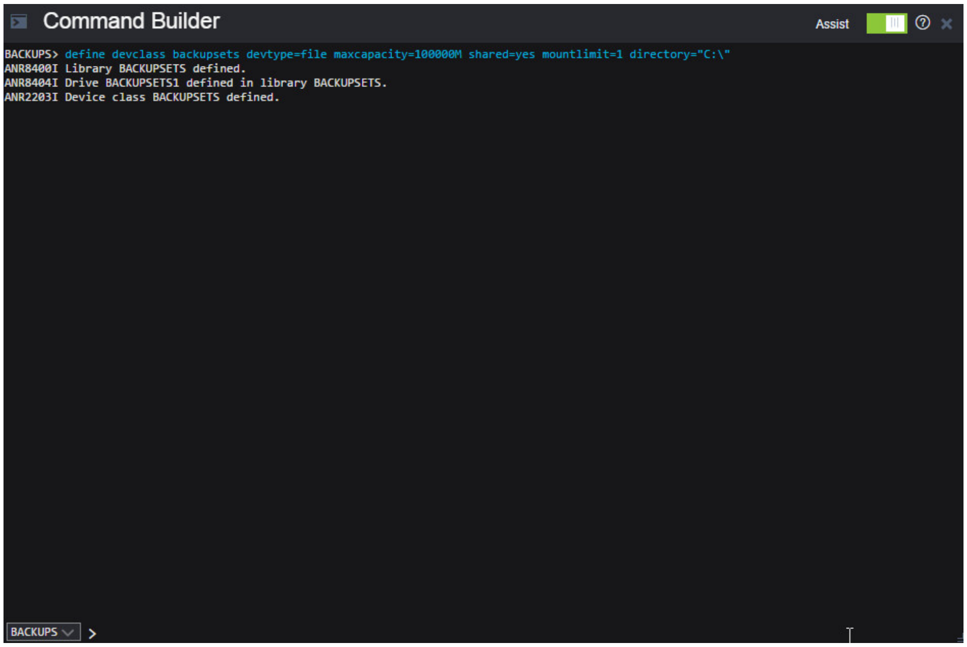
This section covers the process for integrating IBM Spectrum Protect with GreenTec WORMDisks. This integration assumes the correct implementation of IBM Spectrum Protect, as well as the existence of

GreenTec WORMdisks as described in earlier sections. The result of this integration is the capability to store all backup data created by IBM Spectrum Protect for a single client on a secure WORMDisk.

2.15.1 Copying Backups for a Single Machine to a GreenTec WORMDisk

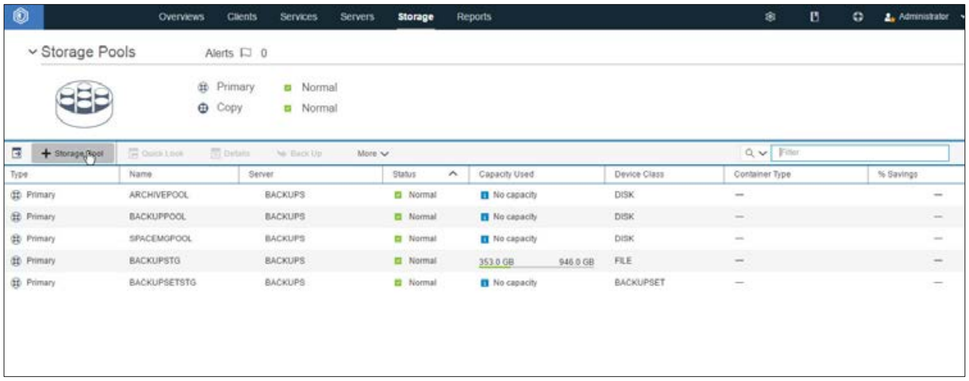
1. On the **IBM Spectrum Protect** server, log on to **IBM Spectrum Protect Operations Center**.
2. Create a new **device class** by running the following command in the Command Builder:

```
define devclass backupset devtype=file maxcapacity=100000M shared=yes
mountlimit=1 directory="C:\"
```



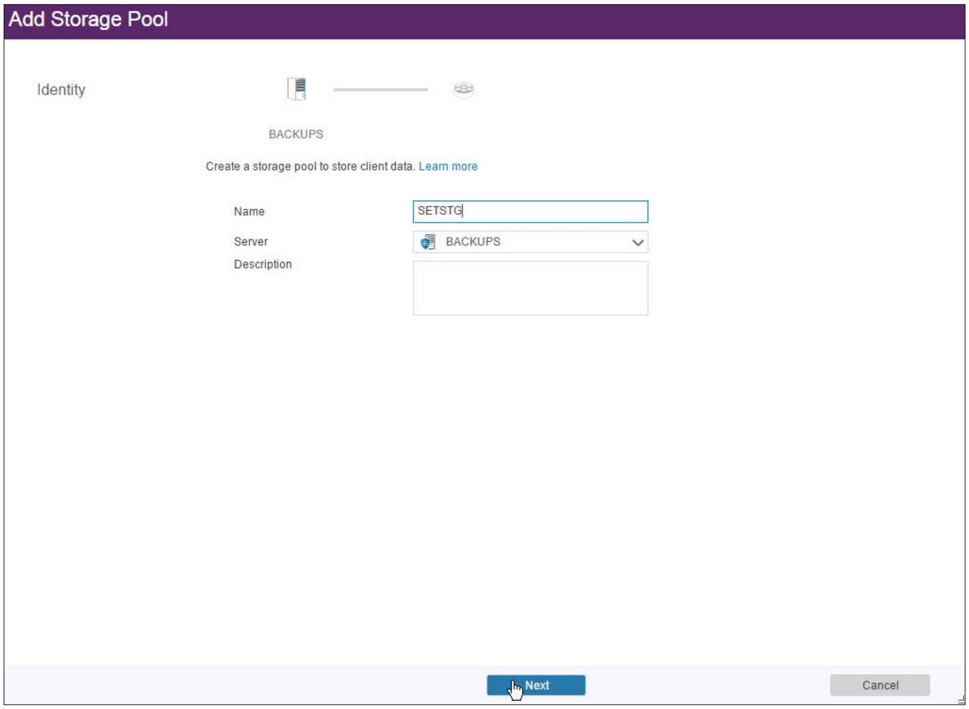
```
BACKUPS> define devclass backupsets devtype=file maxcapacity=100000M shared=yes mountlimit=1 directory="C:\"
ANR8400I Library BACKUPSETS defined.
ANR8404I Drive BACKUPSETS1 defined in library BACKUPSETS.
ANR2203I Device class BACKUPSETS defined.
```

3. Go to **Storage** > **Storage Pools**.



Type	Name	Server	Status	Capacity Used	Device Class	Container Type	% Savings
Primary	ARCHIVEPOOL	BACKUPS	Normal	No capacity	DISK	—	—
Primary	BACKUPPOOL	BACKUPS	Normal	No capacity	DISK	—	—
Primary	SPACEMGPOOL	BACKUPS	Normal	No capacity	DISK	—	—
Primary	BACKUPSTG	BACKUPS	Normal	353.0 GB 946.0 GB	FILE	—	—
Primary	BACKUPSETSTG	BACKUPS	Normal	No capacity	BACKUPSET	—	—

4. Click **+Storage Pool**.
5. Enter a **name**.



Add Storage Pool

Identity

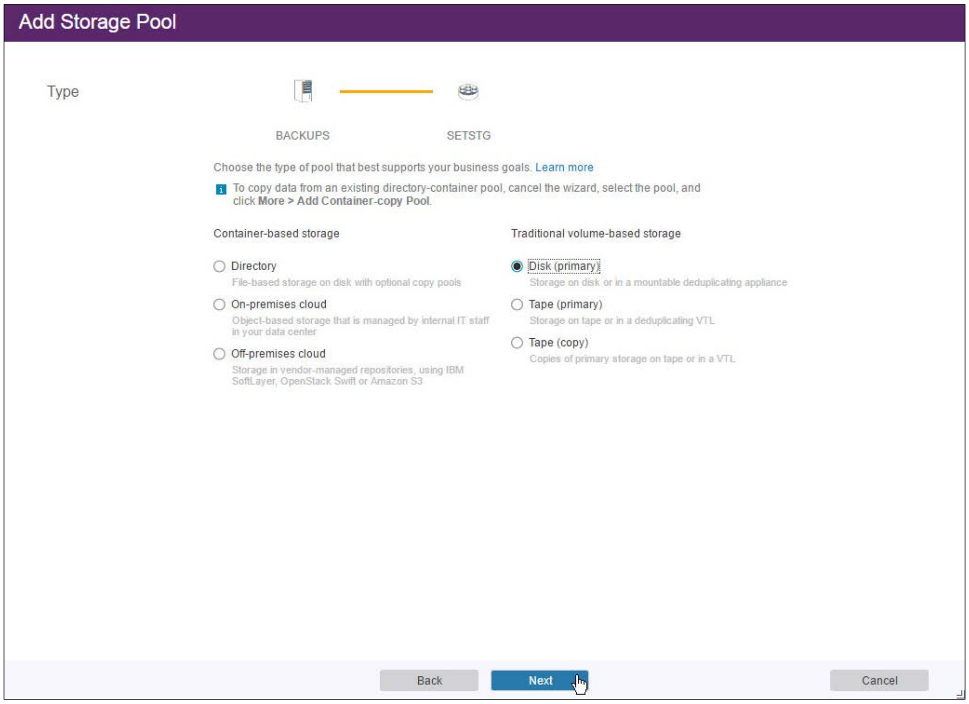
Create a storage pool to store client data. Learn more

Name: SETSTG

Server: BACKUPS

Description:

6. Click **Next**.
7. Select **Disk (primary)**.



Add Storage Pool

Type

Choose the type of pool that best supports your business goals. Learn more

To copy data from an existing directory-container pool, cancel the wizard, select the pool, and click **More > Add Container-copy Pool**.

Container-based storage

○ Directory
File-based storage on disk with optional copy pools

○ On-premises cloud
Object-based storage that is managed by internal IT staff in your data center

○ Off-premises cloud
Storage in vendor-managed repositories, using IBM SoftLayer, OpenStack Swift or Amazon S3

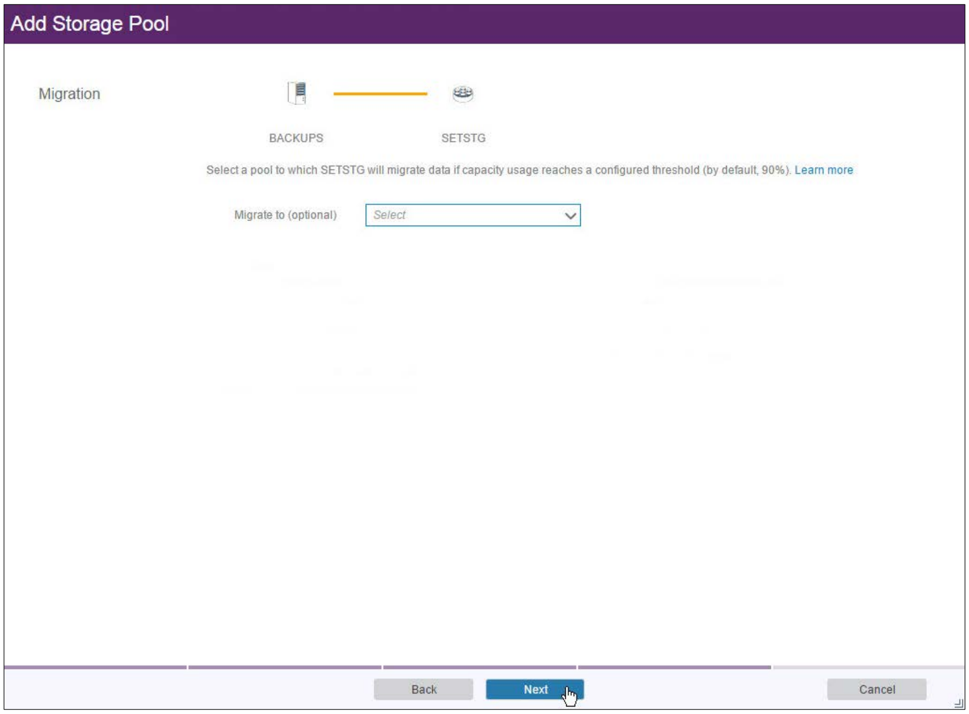
Traditional volume-based storage

● Disk (primary)
Storage on disk or in a mountable deduplicating appliance

○ Tape (primary)
Storage on tape or in a deduplicating VTL

○ Tape (copy)
Copies of primary storage on tape or in a VTL

8. Click **Next**.

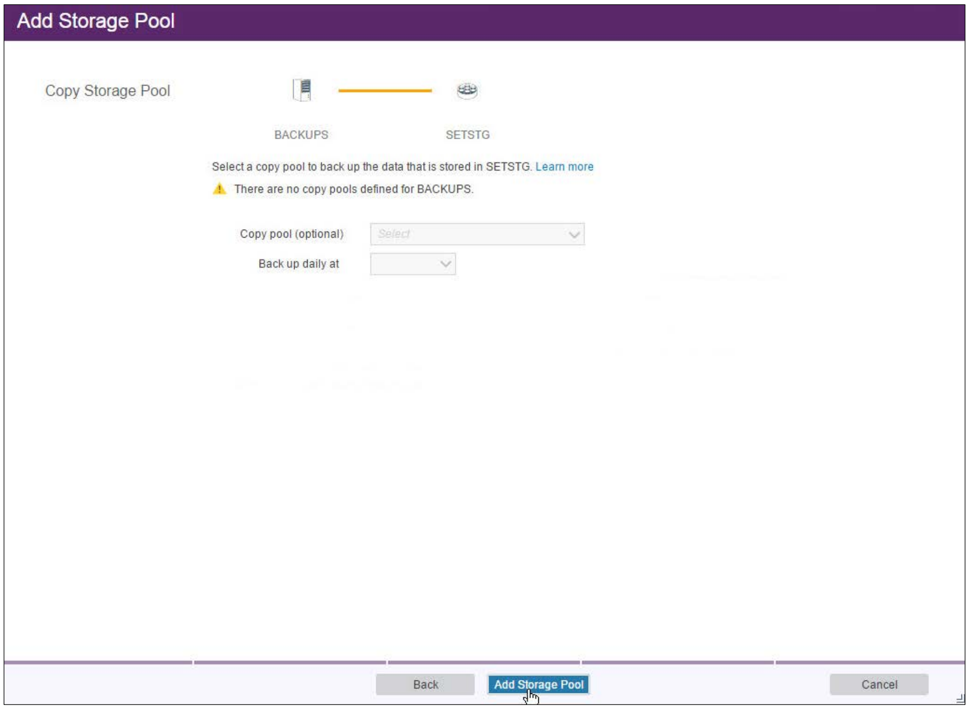

Add Storage Pool

Migration

Select a pool to which SETSTG will migrate data if capacity usage reaches a configured threshold (by default, 90%). Learn more

Migrate to (optional): Select

9. Click **Next**.


Add Storage Pool

Copy Storage Pool

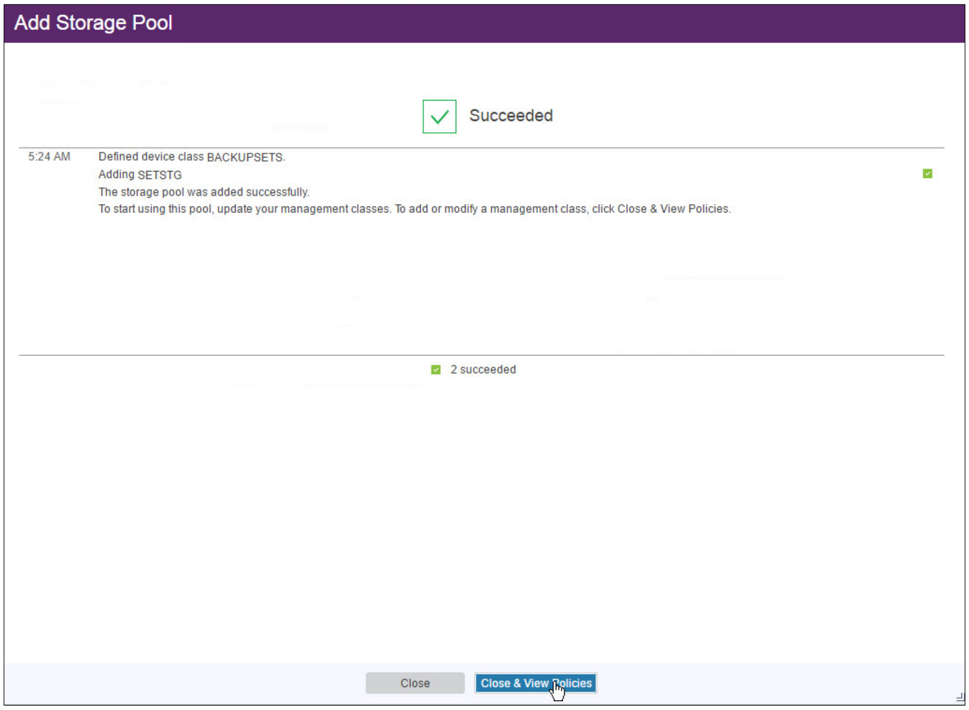
Select a copy pool to back up the data that is stored in SETSTG. Learn more

⚠ There are no copy pools defined for BACKUPS.

Copy pool (optional): Select

Back up daily at

10. Click **Add Storage Pool**.



Add Storage Pool

Succeeded

5:24 AM Defined device class BACKUPSETS.
Adding SETSTG
The storage pool was added successfully.
To start using this pool, update your management classes. To add or modify a management class, click Close & View Policies.

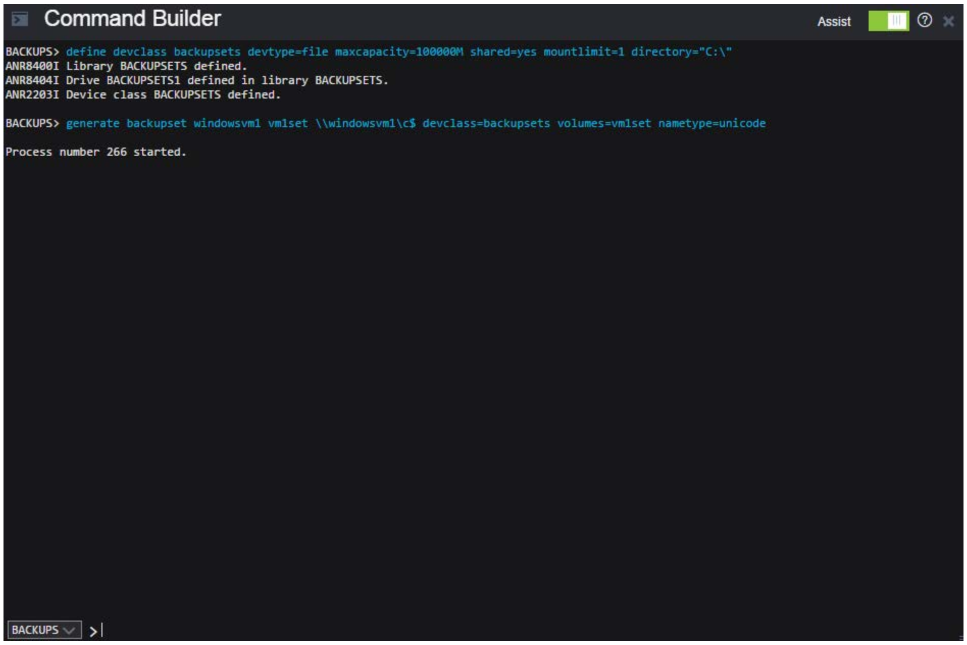
2 succeeded

11. Create a backup set for the client whose data you wish to store securely. Run the following command on Command Builder:

```
generate backupset <name of client> <identifier> \\<name of client>\c$
devclass=file volumes=backupset1 nametype=unicode
```

For example:

```
generate backupset windowsvm1 windowsvm1_backupset \\windowsvm1\c$
devclass=file volumes=backupset1 nametype=Unicode
```



```
BACKUPS> define devclass backupsets devtype=file maxcapacity=100000M shared=yes mountlimit=1 directory="C:\"
ANR8400I Library BACKUPSETS defined.
ANR8404I Drive BACKUPSETS1 defined in library BACKUPSETS.
ANR2203I Device class BACKUPSETS defined.

BACKUPS> generate backupset windowsvm1 vm1set \\windowsvm1\c$ devclass=backupsets volumes=vm1set nametype=unicode

Process number 266 started.
```

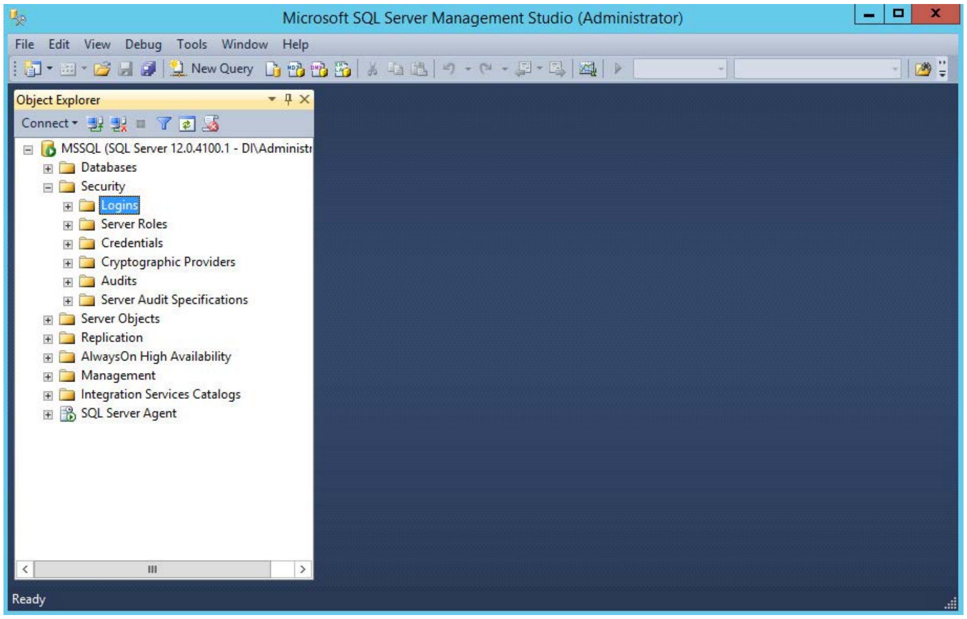
12. This will store all backup data for the client **WINDOWSVM1** in a file called **backupset1**. You can copy this file to a GreenTec disk and store for later use.

2.16 Integration: Tripwire and MS SQL Server

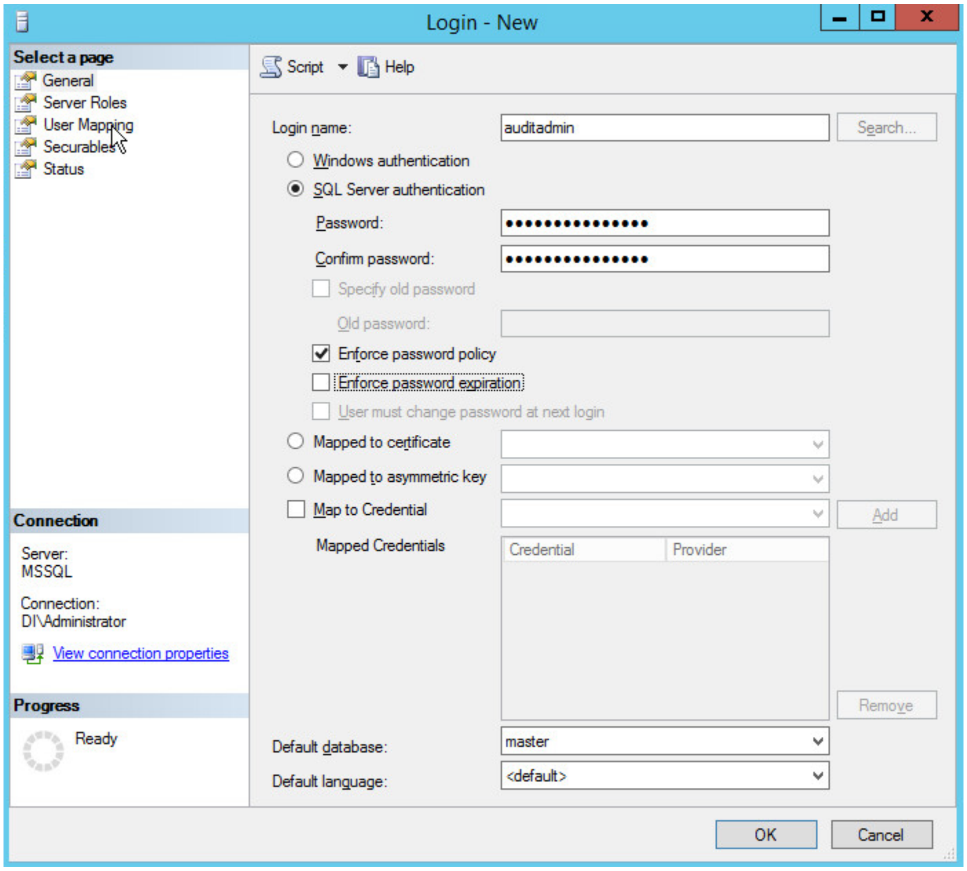
This section covers the process for integrating Tripwire Log Center and Microsoft SQL Server. This integration assumes the correct implementation of Tripwire as described in earlier sections. The result of this integration is the collection of database audit logs in Tripwire, allowing for detection and reporting of events such as specific types of queries, schema modification, and database modification.

2.16.1 Create a New Account on MS SQL Server

1. Open **SQL Server Management Studio.**
2. Hit **Connect** to connect to the database.
3. In the **Object Explorer** window, expand the **Security** folder.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
MSSQL (SQL Server 12.0.4100.1 - DI\Administr
Databases
Security
Logins
Server Roles
Credentials
Cryptographic Providers
Audits
Server Audit Specifications
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent
Ready

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



Login - New

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ Help

Login name: auditadmin [Search...]

○ Windows authentication

● SQL Server authentication

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential [Add]

Mapped Credentials

Credential	Provider

[Remove]

Default database: master

Default language: <default>

Connection

Server:
MSSQL

Connection:
DI\Administrator

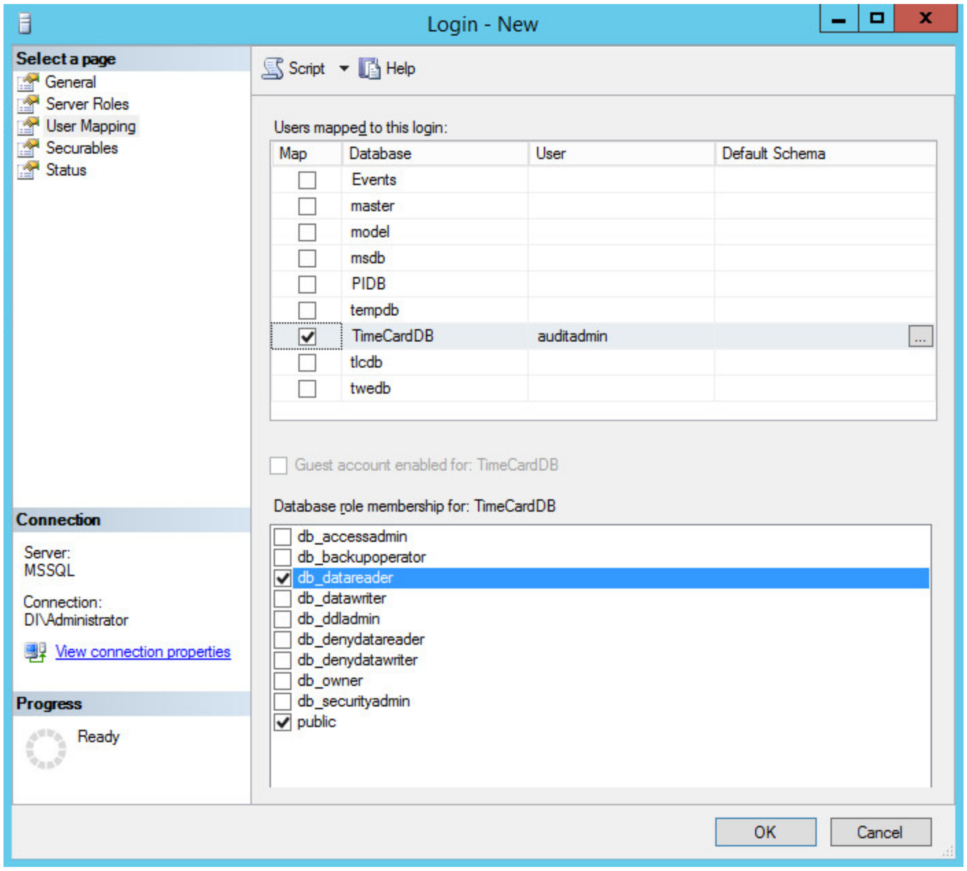
View connection properties

Progress

Ready

[OK] [Cancel]

6. Click **User Mapping.**
7. For each database that Tripwire should monitor, click the database and assign the role **db_datareader**.



Users mapped to this login:

Map	Database	User	Default Schema
□	Events		
□	master		
□	model		
□	msdb		
□	PIDB		
□	tempdb		
☑	TimeCardDB	auditadmin	
□	tlcdb		
□	twedb		

□ Guest account enabled for: TimeCardDB

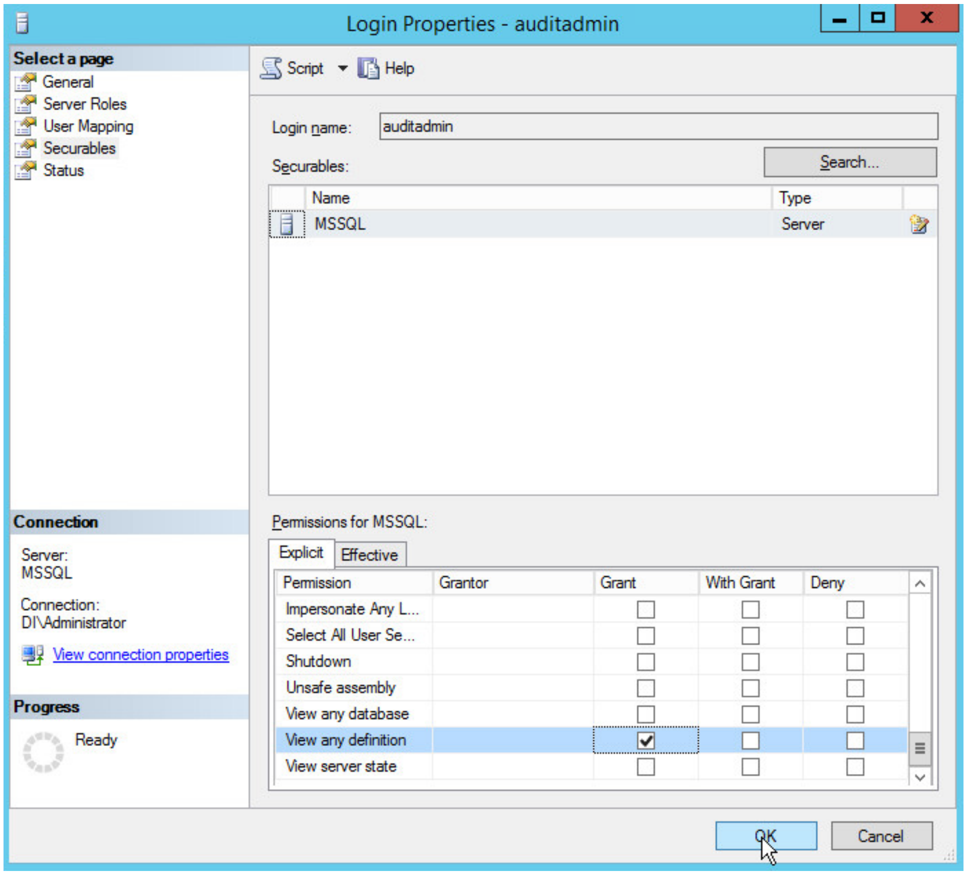
Database role membership for: TimeCardDB

□ db_accessadmin
□ db_backupoperator
☑ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
□ db_owner
□ db_securityadmin
☑ public

Server:
MSSQL

Connection:
DI\Administrator

8. Click **Securables**.
9. Under the **Grant** column, check the boxes next to **Alter trace** and **View any definition** (if this is not available, create the user, then edit properties for that user).



Login name: auditadmin

Securables:

Name	Type
MSSQL	Server

Server: MSSQL

Connection: DI\Administrator

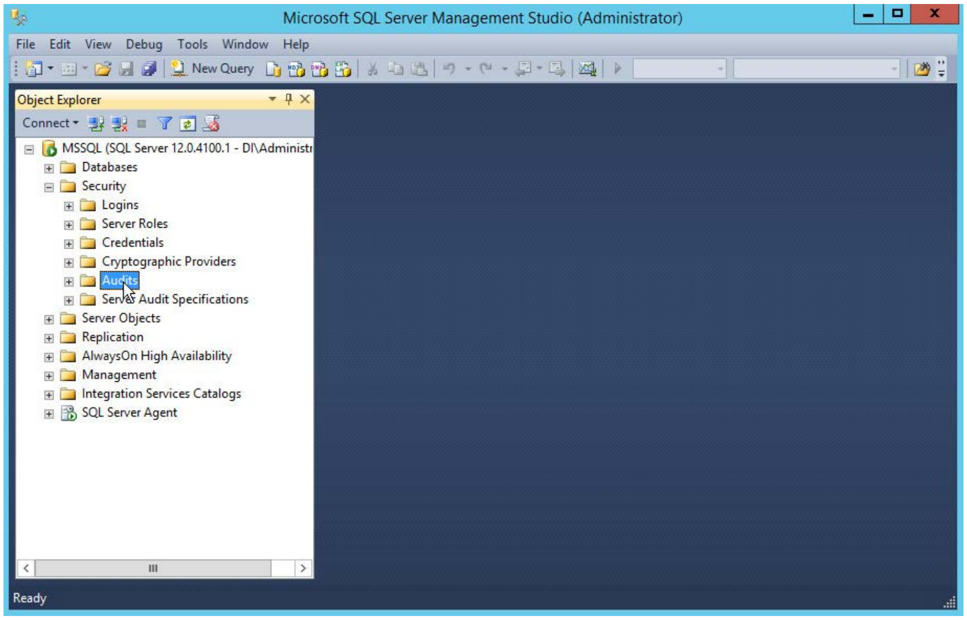
Permissions for MSSQL:

Permission	Grantor	Grant	With Grant	Deny
Impersonate Any L...		□	□	□
Select All User Se...		□	□	□
Shutdown		□	□	□
Unsafe assembly		□	□	□
View any database		□	□	□
View any definition		☑	□	□
View server state		□	□	□

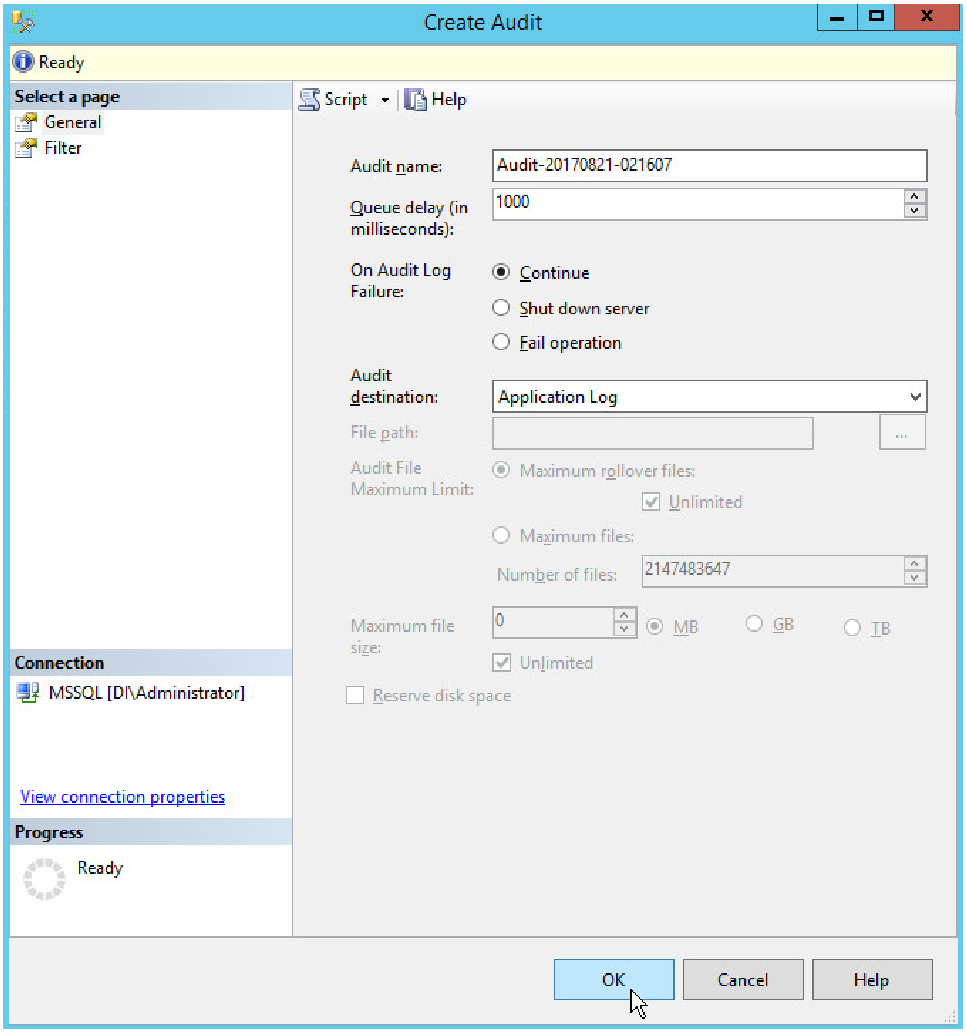
10. Click **OK**.

2.16.2 Create a New Audit on MS SQL Server

1. In the **Object Explorer** window, expand the **Security** folder.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
MSSQL (SQL Server 12.0.4100.1 - DI\Administr
Databases
Security
Logins
Server Roles
Credentials
Cryptographic Providers
Audits
Server Audit Specifications
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent
Ready

2. Right click on the **Audits** folder.
3. Click **New Audit…**.
4. Specify a **filename** or any other settings per your organization's needs. Note: If you specify a filename, you will be able to view any queries you wish to monitor in this **Audit log**, but not in **Tripwire**. However, if you set the **Audit Destination** to **Application Log**, the messages will be forwarded to the **Microsoft Application Log**. This will result in less structured (but still detailed) messages and allows the capability to collect them using **HPE ArcSight ESM.** If your **ArcSight Connector** is configured to collect **Application Logs** from the **MS SQL** server, no further configuration of the connector is required.



Audit name: Audit-20170821-021607

Queue delay (in milliseconds): 1000

On Audit Log Failure: ● Continue ○ Shut down server ○ Fail operation

Audit destination: Application Log

File path:

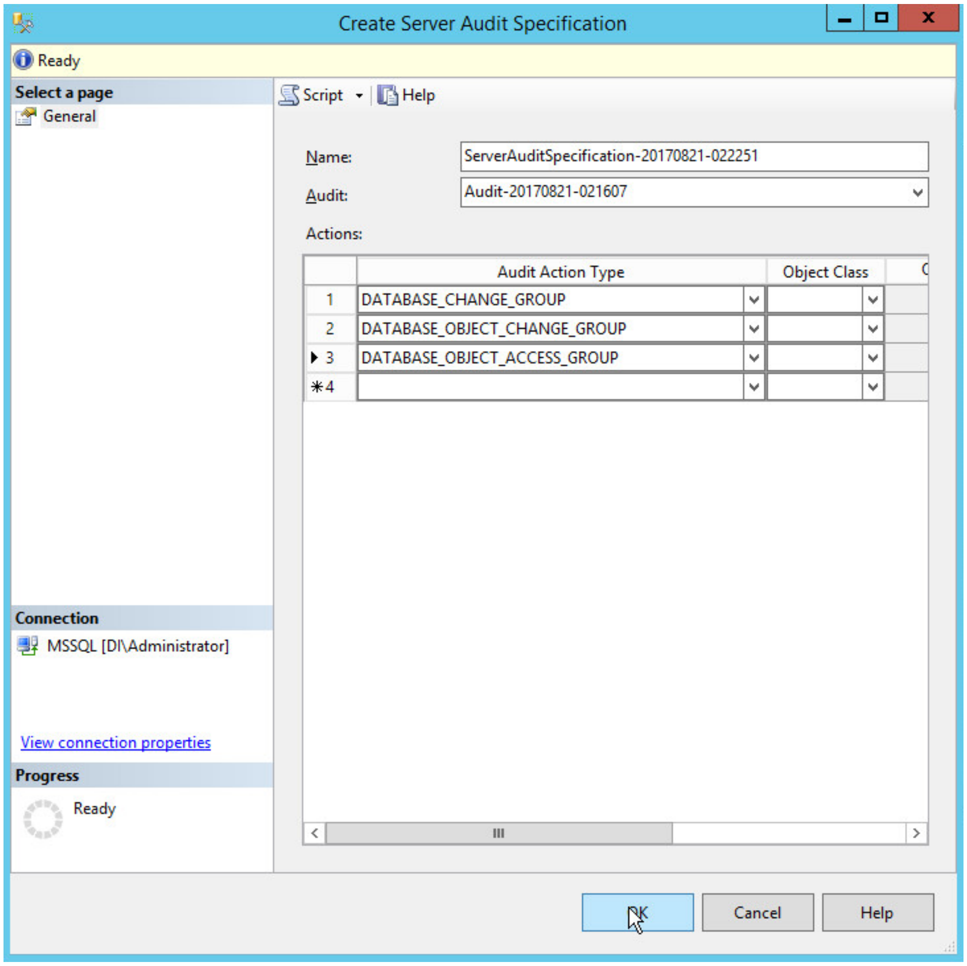
Audit File Maximum Limit: ● Maximum rollover files: ☑ Unlimited ○ Maximum files:

Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB ☑ Unlimited

□ Reserve disk space

5. Click **OK**.
6. Right click **Security** > **Server Audit Specifications**.
7. Click **New Server Audit Specification…**.
8. For **Audit:** select the audit you just created.
9. Specify any **Audit Action Types** that Tripwire should be able to log.



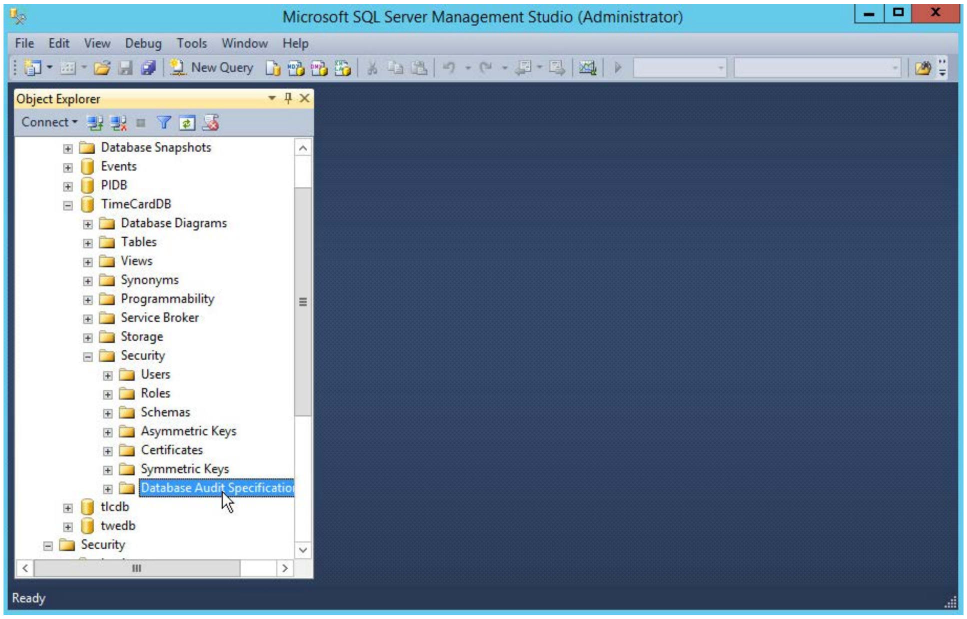
Name: ServerAuditSpecification-20170821-022251

Audit: Audit-20170821-021607

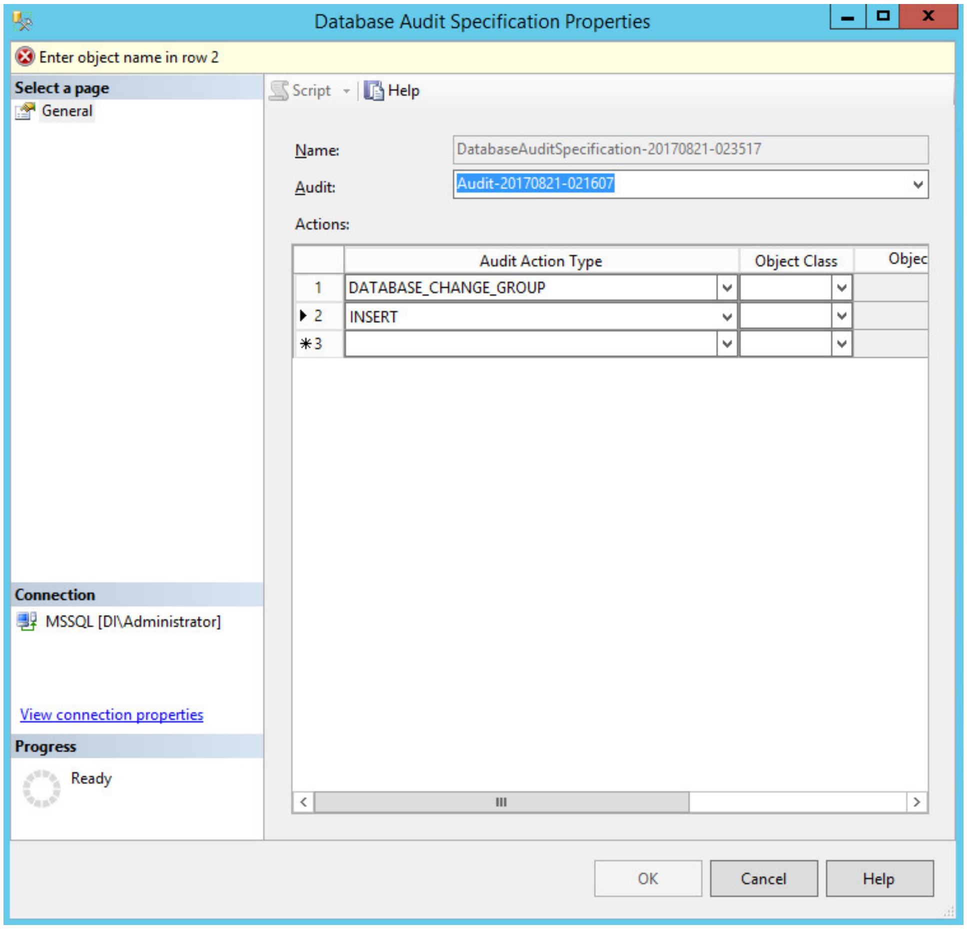
Actions:

	Audit Action Type	Object Class
1	DATABASE_CHANGE_GROUP	
2	DATABASE_OBJECT_CHANGE_GROUP	
▸ 3	DATABASE_OBJECT_ACCESS_GROUP	
✳4		

10. Click **OK.**
11. Open a database that you wish to monitor specific objects in.
12. Right click **Databases** > **<Database name>** > **Security** > **Database Audit Specifications**.



13. Click **New Database Audit Specification…**.
14. Select an **Audit Action Type** to monitor.



Database Audit Specification Properties

Enter object name in row 2

Select a page

General

Script Help

Name: DatabaseAuditSpecification-20170821-023517

Audit: Audit-20170821-021607

Actions:

	Audit Action Type	Object Class	Objec
1	DATABASE_CHANGE_GROUP		
2	INSERT		
3			

Connection

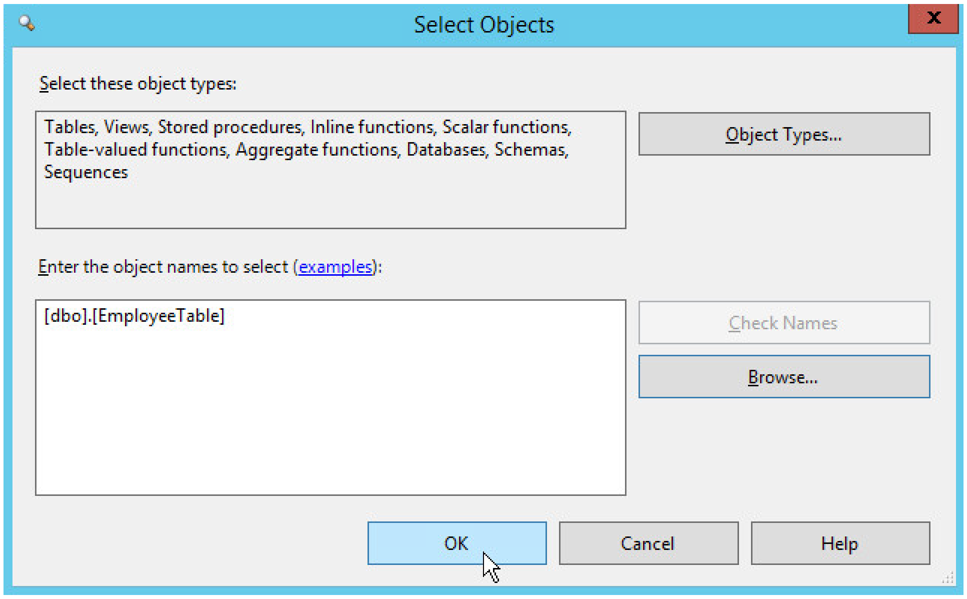
MSSQL [DI\Administrator]

View connection properties

Progress

Ready

15. Select **Object** for the **Object Class**.
16. In the **Object Name** field, use the **Browse** button to find objects that you wish to monitor for the specified **Audit Action Type**.



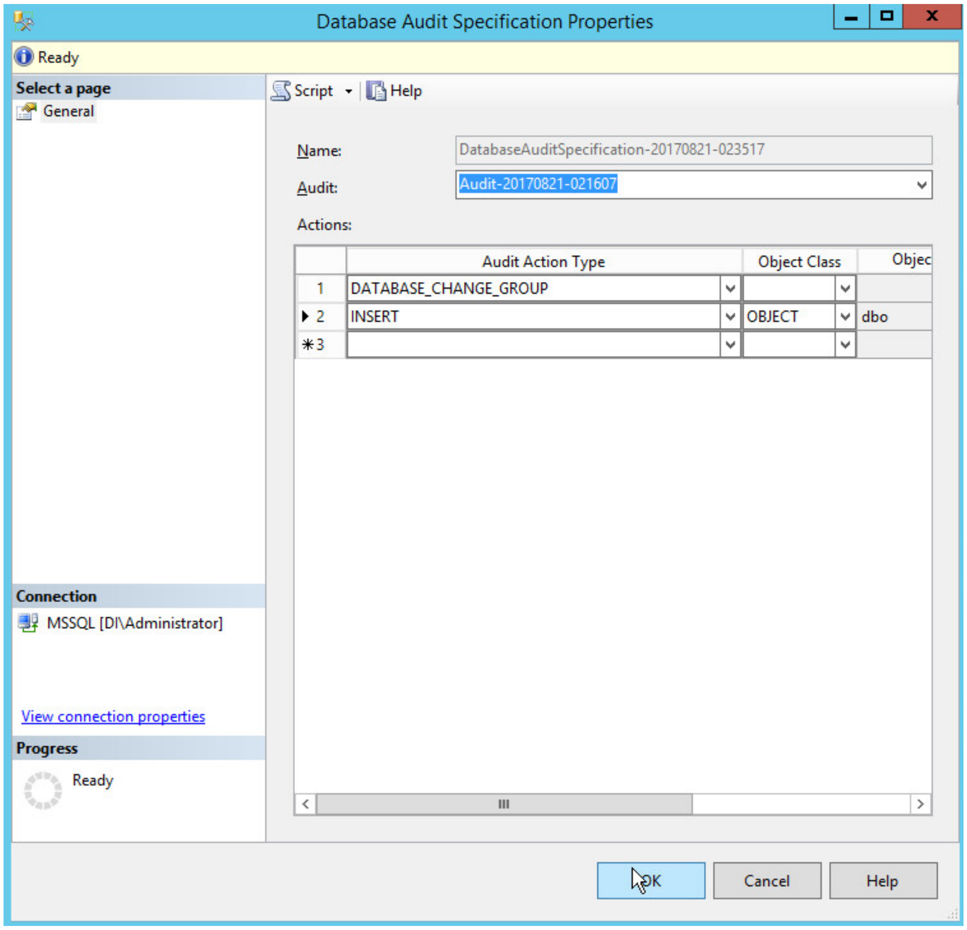
Select these object types:

Tables, Views, Stored procedures, Inline functions, Scalar functions, Table-valued functions, Aggregate functions, Databases, Schemas, Sequences

Enter the object names to select (examples):

[dbo].[EmployeeTable]

17. Create as many types as you wish Tripwire to monitor.



Name: DatabaseAuditSpecification-20170821-023517

Audit: Audit-20170821-021607

Actions:

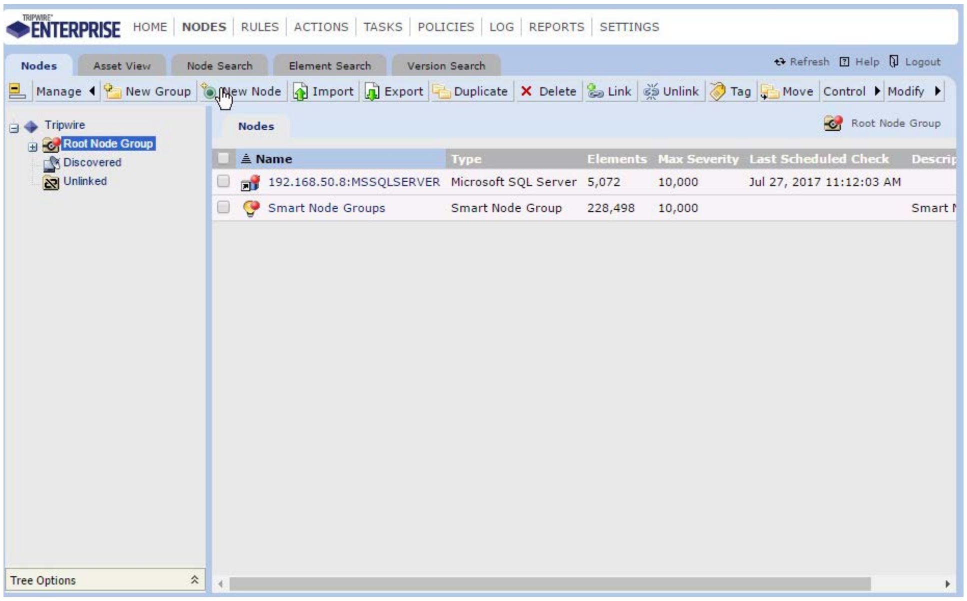
	Audit Action Type	Object Class	Objec
1	DATABASE_CHANGE_GROUP		
▸ 2	INSERT	OBJECT	dbo
✱3			

MSSQL [DI\Administrator]

18. Click **OK**.
19. Find the audits you just created in the **Object Explorer** and right click.
20. Select **Enable ___ Audit Specification** for each one.

2.16.3 Create a New Node for the MS SQL Server on Tripwire Enterprise

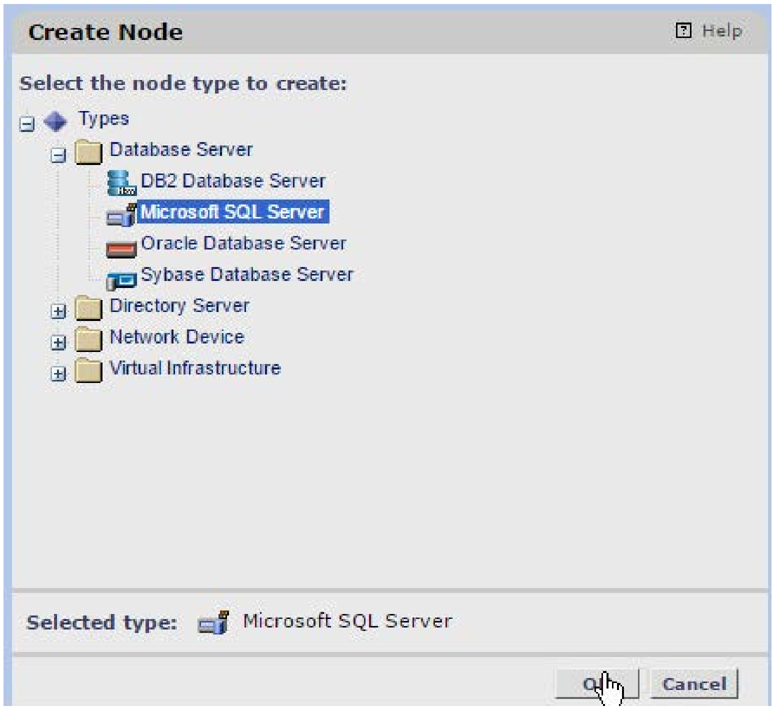
1. Open the Tripwire Enterprise console.
2. Click **Nodes**.



Nodes — Root Node Group

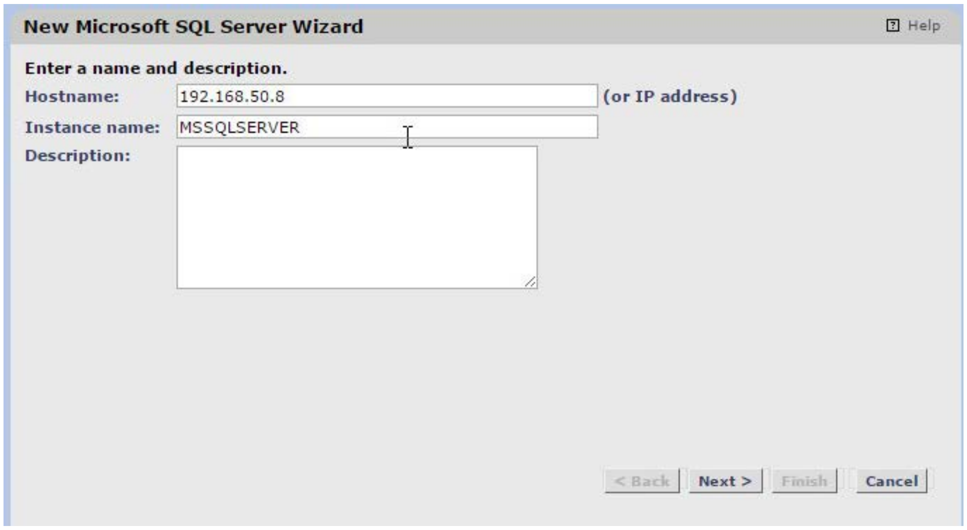
Name	Type	Elements	Max Severity	Last Scheduled Check	Descrip
192.168.50.8:MSSQLSERVER	Microsoft SQL Server	5,072	10,000	Jul 27, 2017 11:12:03 AM	
Smart Node Groups	Smart Node Group	228,498	10,000		Smart N

3. Click **Manage** > **New Node**.



Selected type: Microsoft SQL Server

4. Click **Types** > **Database Server** > **Microsoft SQL Server**.
5. Click **Ok**.
6. Enter the **hostname** or **IP** of the MS SQL Server.
7. Enter the **instance name** of the database.


New Microsoft SQL Server Wizard

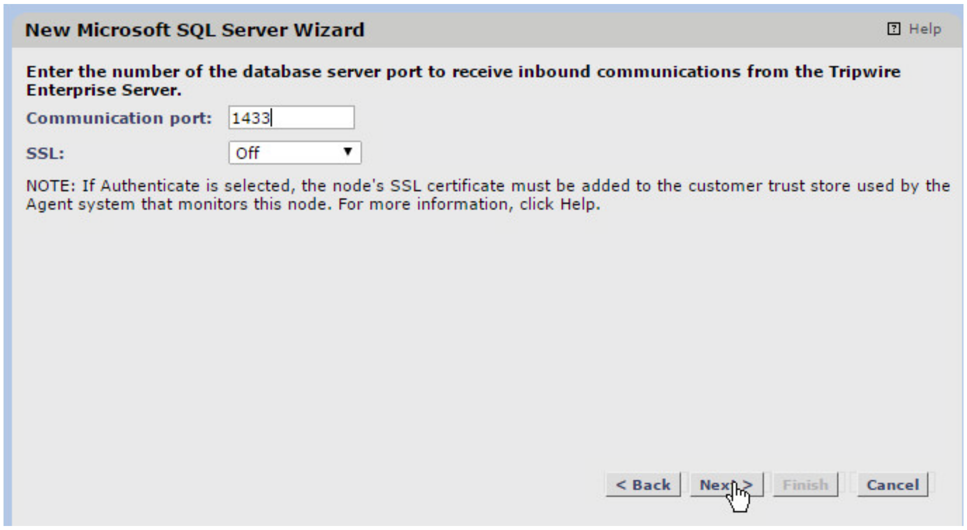
Enter a name and description.

Hostname: 192.168.50.8 (or IP address)

Instance name: MSSQLSERVER

Description:

8. Click **Next**.
9. Enter the **port** the database listens on.


New Microsoft SQL Server Wizard

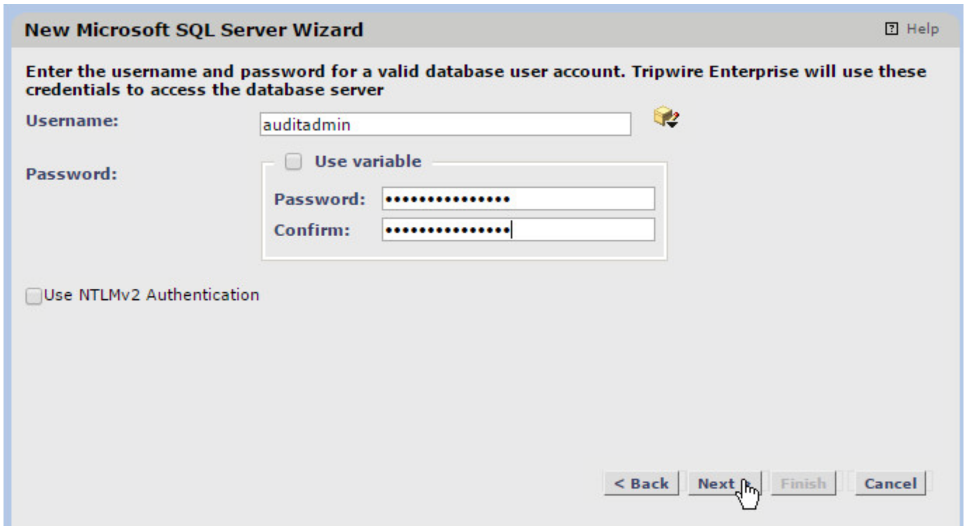
Enter the number of the database server port to receive inbound communications from the Tripwire Enterprise Server.

Communication port: 1433

SSL: Off

NOTE: If Authenticate is selected, the node's SSL certificate must be added to the customer trust store used by the Agent system that monitors this node. For more information, click Help.

10. Click **Next**.
11. Enter the newly created **username** and **password** for the database.


New Microsoft SQL Server Wizard

Enter the username and password for a valid database user account. Tripwire Enterprise will use these credentials to access the database server

Username: auditadmin

Password:

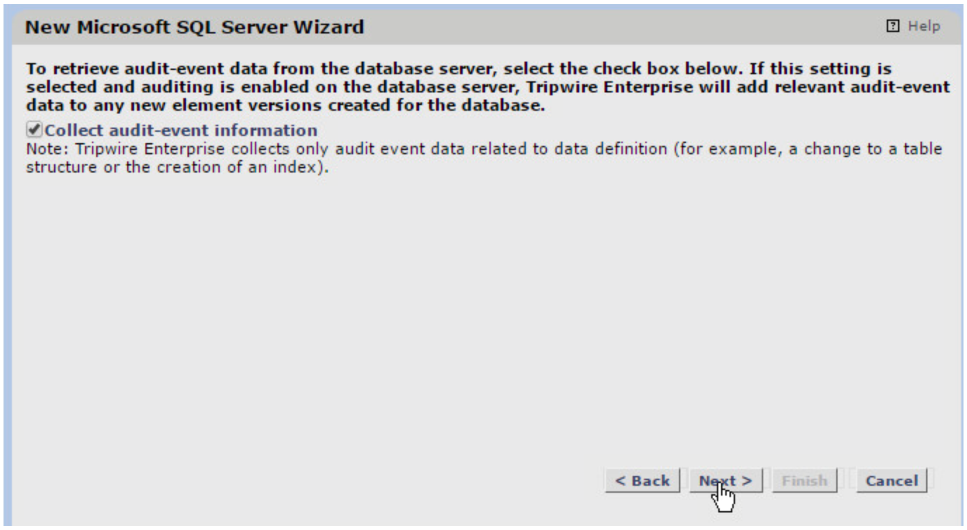
□ Use variable

Password: •••••••••••••••

Confirm: •••••••••••••••

□ Use NTLMv2 Authentication

12. Click **Next**.
13. Check the box next to **Collect audit-event information**.

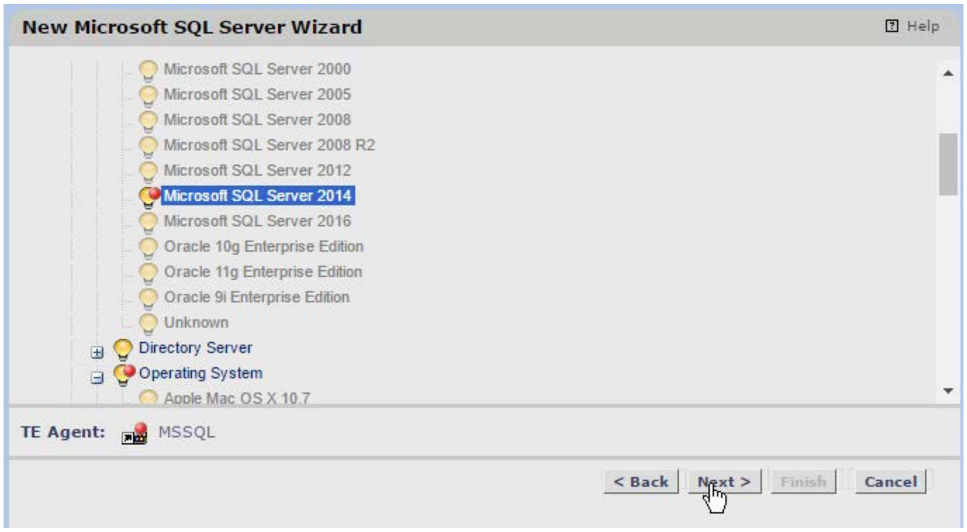

New Microsoft SQL Server Wizard

To retrieve audit-event data from the database server, select the check box below. If this setting is selected and auditing is enabled on the database server, Tripwire Enterprise will add relevant audit-event data to any new element versions created for the database.

☑ Collect audit-event information

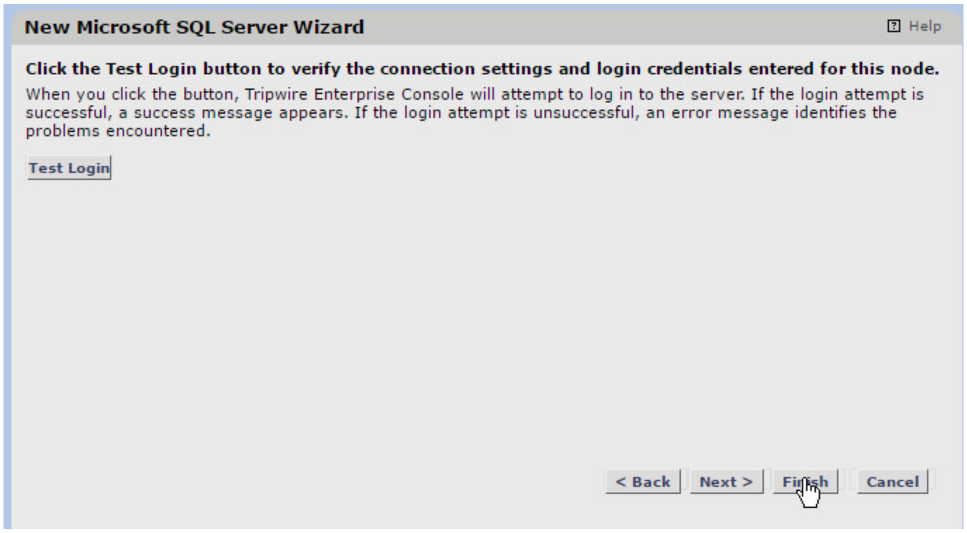
Note: Tripwire Enterprise collects only audit event data related to data definition (for example, a change to a table structure or the creation of an index).

14. Click **Next**.
15. Find the MSSQL Server on the list.


New Microsoft SQL Server Wizard
Help
Microsoft SQL Server 2000
Microsoft SQL Server 2005
Microsoft SQL Server 2008
Microsoft SQL Server 2008 R2
Microsoft SQL Server 2012
Microsoft SQL Server 2014
Microsoft SQL Server 2016
Oracle 10g Enterprise Edition
Oracle 11g Enterprise Edition
Oracle 9i Enterprise Edition
Unknown
Directory Server
Operating System
Apple Mac OS X 10.7
< Back
Next >
Finish
Cancel

TE Agent: MSSQL

16. Click **Next**.
17. **Test Login** to ensure the information you entered was correct.



Click the Test Login button to verify the connection settings and login credentials entered for this node.

When you click the button, Tripwire Enterprise Console will attempt to log in to the server. If the login attempt is successful, a success message appears. If the login attempt is unsuccessful, an error message identifies the problems encountered.

18. Click **Finish.**

Appendix A List of Acronyms

AD	Active Directory
BA	Client Backup-Archive Client
DB	Database
DI	Data Integrity
DNS	Domain Name System
EOF	End of File
ESM	Enterprise Security Manager
HPE	Hewlett Packard Enterprise
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MS SQL	Microsoft Structured Query Language
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
MS	Microsoft
CA	Certificate Authority
DSRM	Directory Services Restore Mode
IIS	Internet Information Services
IP	Internet Protocol
SQL	Structured Query Language
SDK	Software Development Kit
TCP	Transmission Control Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VSS	Volume Shadowcopy Services

VM	Virtual Machines
VnE	Vulnerability and Exposure
WORM	Write Once Read Many