SIOS

Configuring SIOS LifeKeeper for Milestone XProtect

Introduction

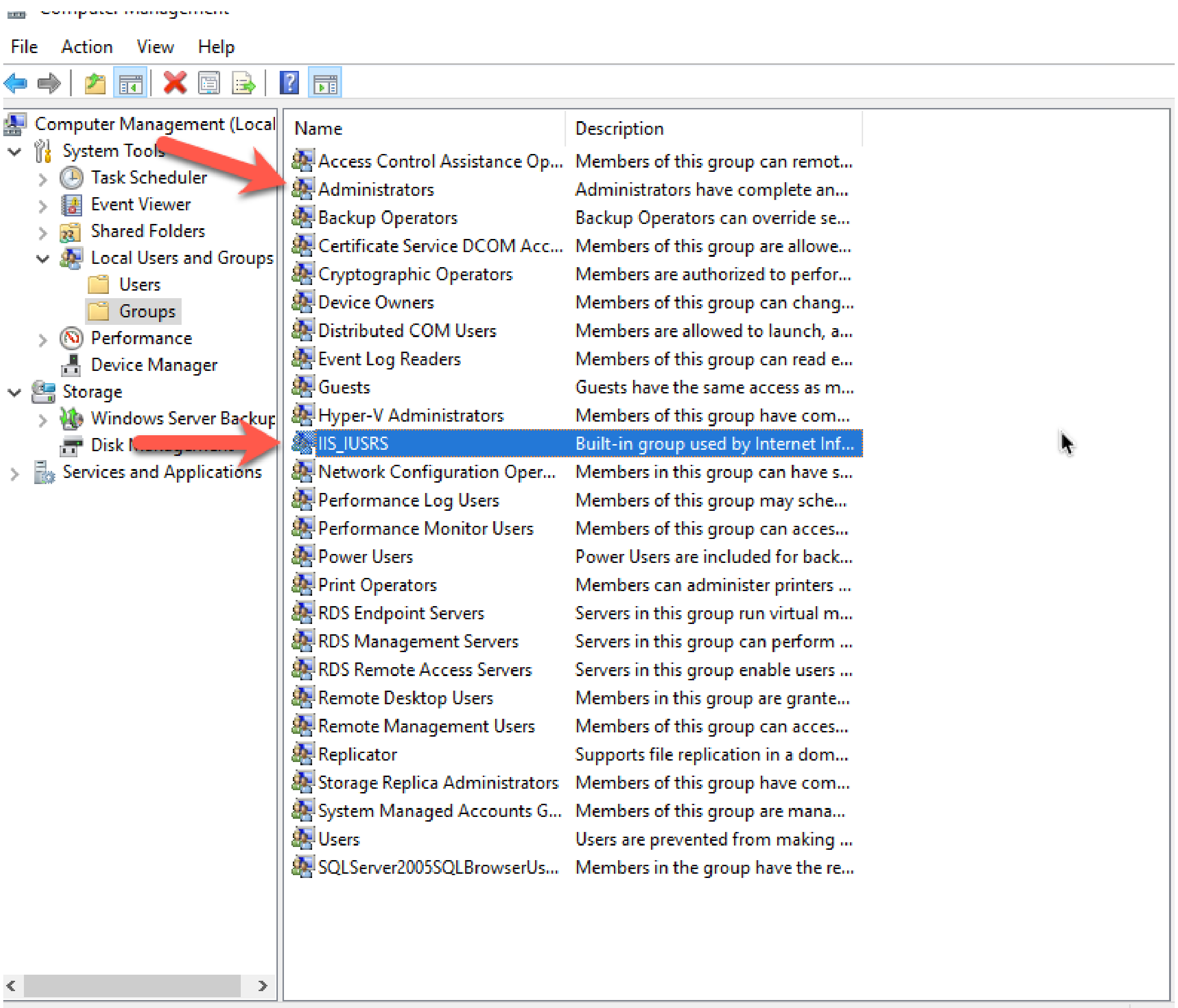
By following the steps below, you will be able to build a two-node Milestone XProtect VMS cluster using the SIOS Protection Suite with Microsoft SQL Server. The steps provided in this document assume that the XProtect Management Server, SQL Server, and all the optional XProtect components are running on the same server. However, you can choose to break out the components across many different cluster pairs if you wish to do that. You should adjust the steps below, installing and clustering just the components you wish to run on each cluster pair.

Pre-Requisites

To create a high availability (HA) cluster, you need at least three servers. Two servers run the XProtect Management Server and all the optional services, and at least one server acts as the XProtect Recording Server. The two XProtect Management Servers will be clustered with SIOS LifeKeeper. The XProtect Recording Server can also be made redundant using the built-in redundancy options. That will not be covered in this guide.

For this guide, we will call these servers XPROTECT1, XPROTECT2 and RECORDING. The following items must be completed.

- When you provision these servers, the names must be in ALL CAPS.
- You must use static IP addresses on these servers.
- XPROTECT1 and XPROTECT2 need host file entries that resolve to one another, even if the DNS is in use.
- These servers can be in a Workgroup or an Active Directory domain.
- If in an AD domain, you must create a domain user account that is added to the local Administrators group and IIS_IUSRS group. This account will be used for both the Milestone XProtect services and the SIOS DataKeeper and LifeKeeper services.
- If in a Workgroup, you need to create a local account on each server and add it to the local Administrators and IIS_IUSRS group. The same account, with **matching passwords**, must be created on each server.
- Make sure the user installing and the account running SQL Server is in the Local Administrators Group and the IIS_IUSRS Group.

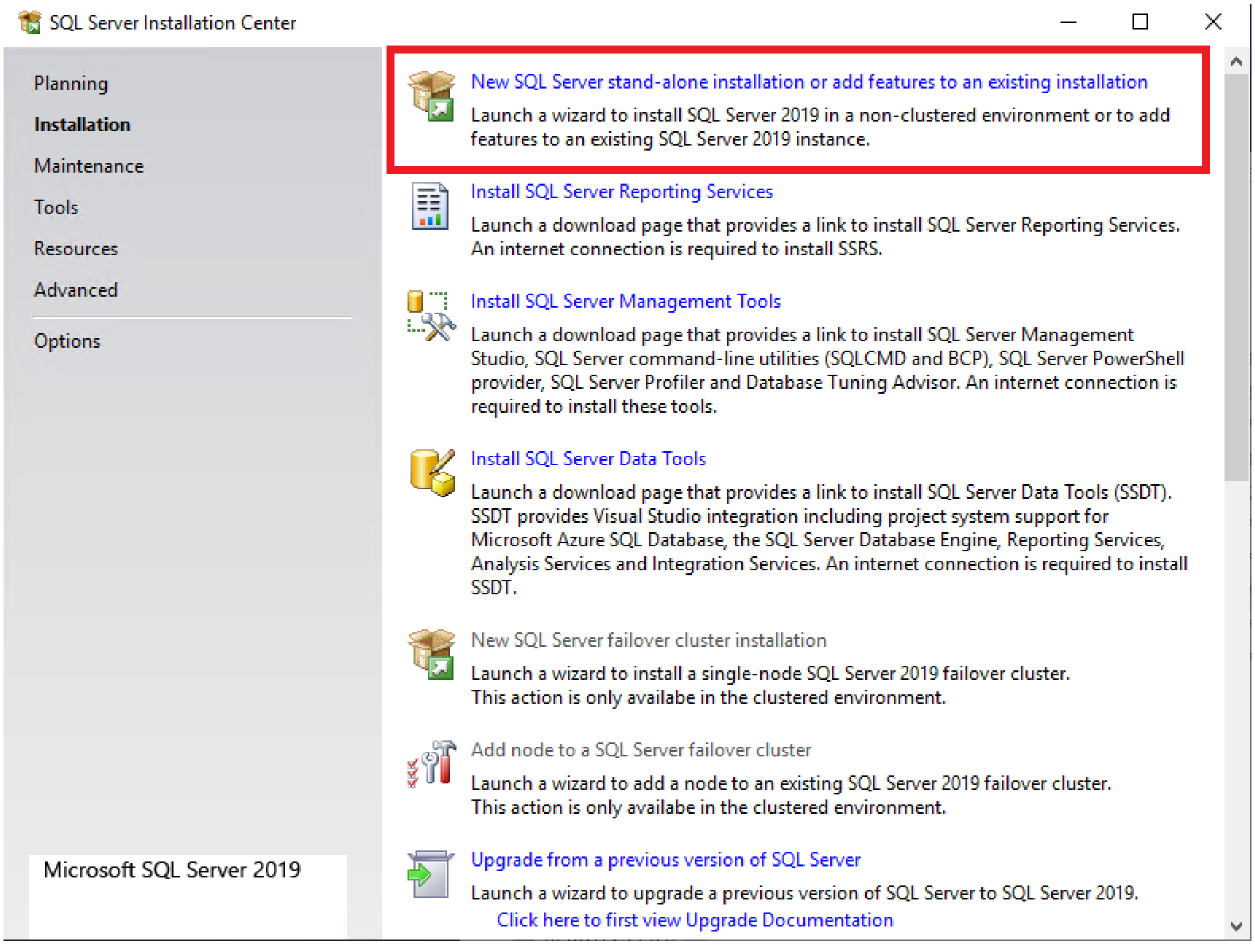


Name	Description
Access Control Assistance Op...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DCOM Acc...	Members of this group are allowe...
Cryptographic Operators	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuration Oper...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor Users	Members of this group can acces...
Power Users	Power Users are included for back...
Print Operators	Members can administer printers ...
RDS Endpoint Servers	Servers in this group run virtual m...
RDS Management Servers	Servers in this group can perform ...
RDS Remote Access Servers	Servers in this group enable users ...
Remote Desktop Users	Members in this group are grante...
Remote Management Users	Members of this group can acces...
Replicator	Supports file replication in a dom...
Storage Replica Administrators	Members of this group have com...
System Managed Accounts G...	Members of this group are mana...
Users	Users are prevented from making ...
SQLServer2005SQLBrowserUs...	Members in the group have the re...

- XPROTECT1 and XPROTECT2 both must have at least one additional partition. The partition drive letters and size must match between the servers.
- Dynamic Pagefile must be disabled; no page file should reside on the extra partition(s) for XPROTECT1 and XPROTECT2.
  - See: https://docs.us.sios.com/dkse/8.6.4/en/topic/disable-automatically-manage-paging-file-size-for-all-drives
- Utilizing two distinct network cards on separate networks is highly recommended (though not mandatory) to optimize network functionality. Establishing a Public network for regular communication purposes, alongside a Private network on a distinct subnet specifically designed for data replication, would be ideal. Both networks should be utilized as communication paths within the cluster.

Step 1 - Install SQL Server

1. Install SQL standalone instance



New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2019 in a non-clustered environment or to add features to an existing SQL Server 2019 instance.

Install SQL Server Reporting Services

Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS.

Install SQL Server Management Tools

Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

Install SQL Server Data Tools

Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

New SQL Server failover cluster installation

Launch a wizard to install a single-node SQL Server 2019 failover cluster. This action is only availabe in the clustered environment.

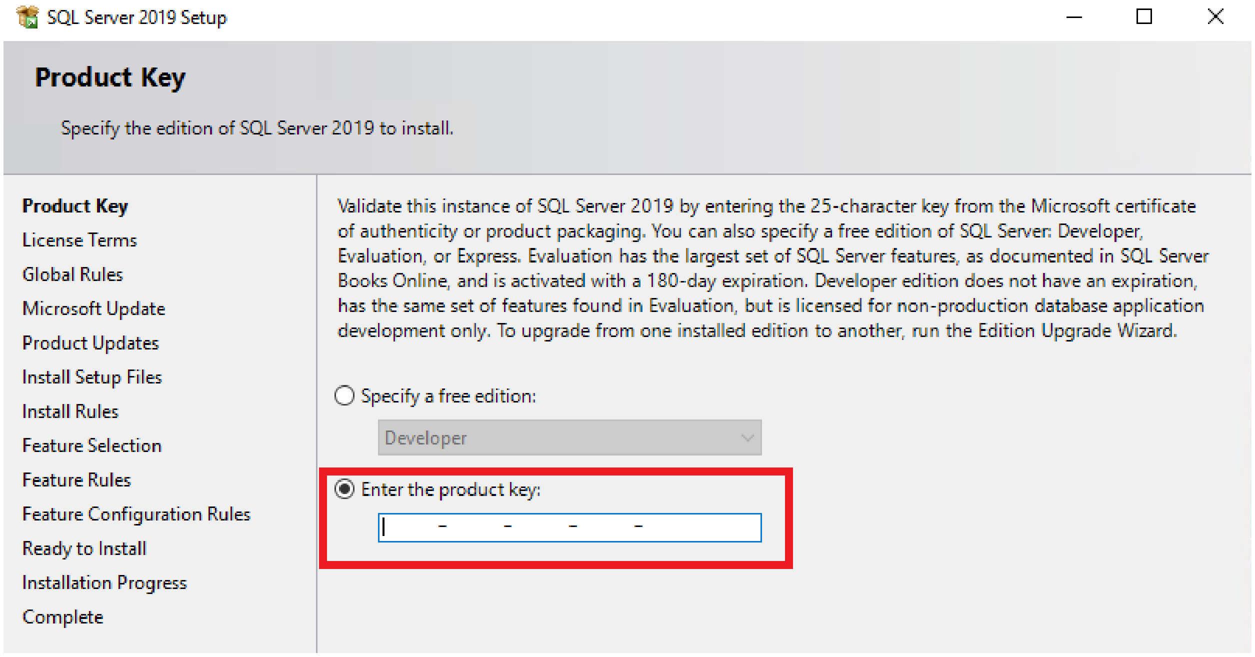
Add node to a SQL Server failover cluster

Launch a wizard to add a node to an existing SQL Server 2019 failover cluster. This action is only availabe in the clustered environment.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2019.
Click here to first view Upgrade Documentation

2. Enter product key



Product Key

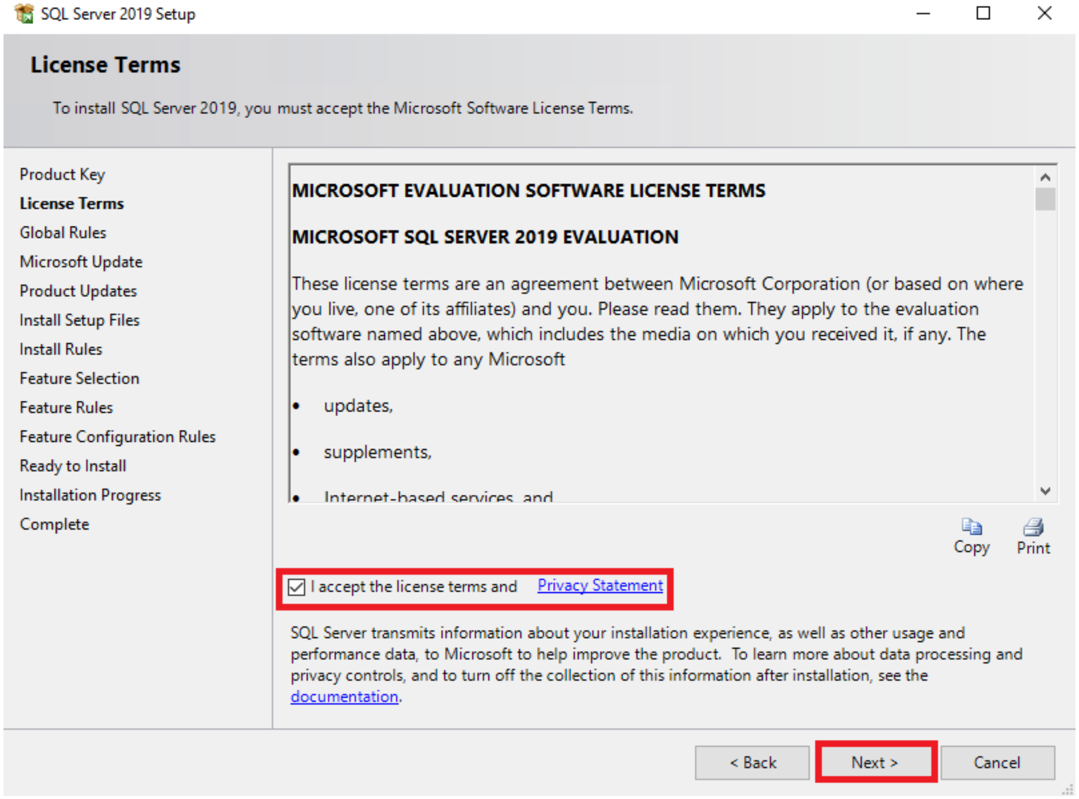
Specify the edition of SQL Server 2019 to install.

Validate this instance of SQL Server 2019 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: Developer, 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. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.

○ Specify a free edition: Developer

● Enter the product key: | - - - -

3. Accept license terms and Privacy Statement



License Terms

To install SQL Server 2019, you must accept the Microsoft Software License Terms.

MICROSOFT EVALUATION SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2019 EVALUATION

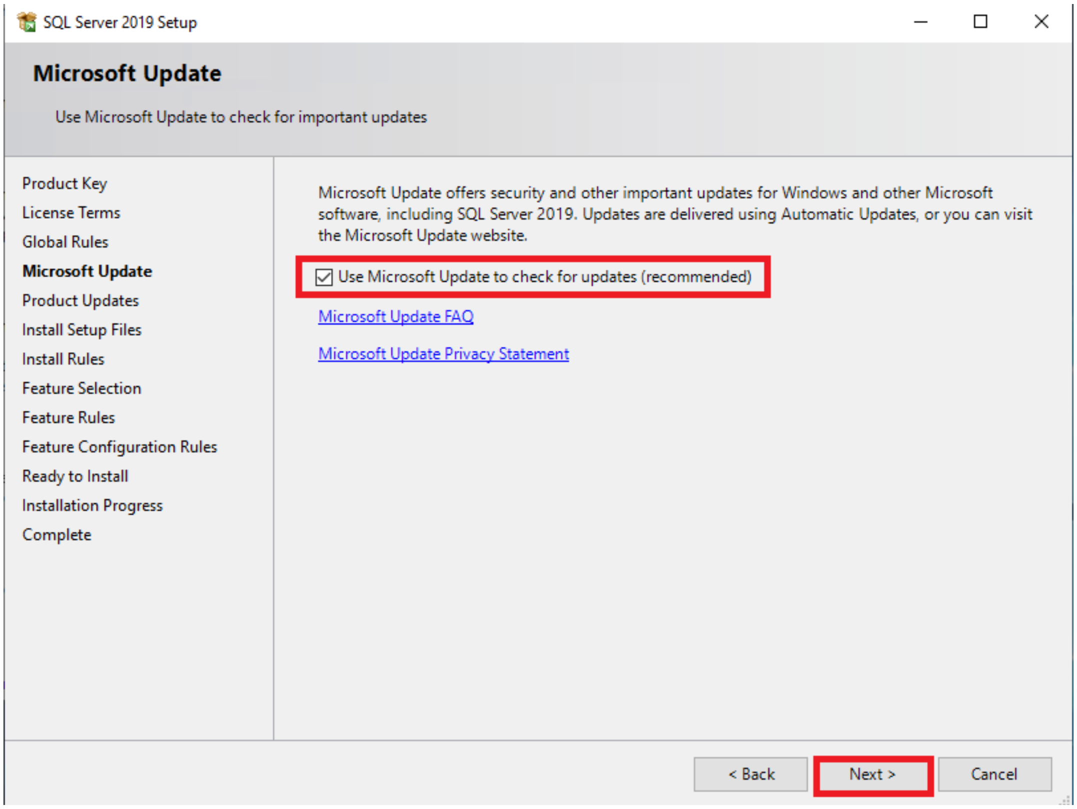
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the evaluation software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

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

☑ I accept the license terms and Privacy Statement

SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.

4. Allow Microsoft Updates by checking the box



SQL Server 2019 Setup

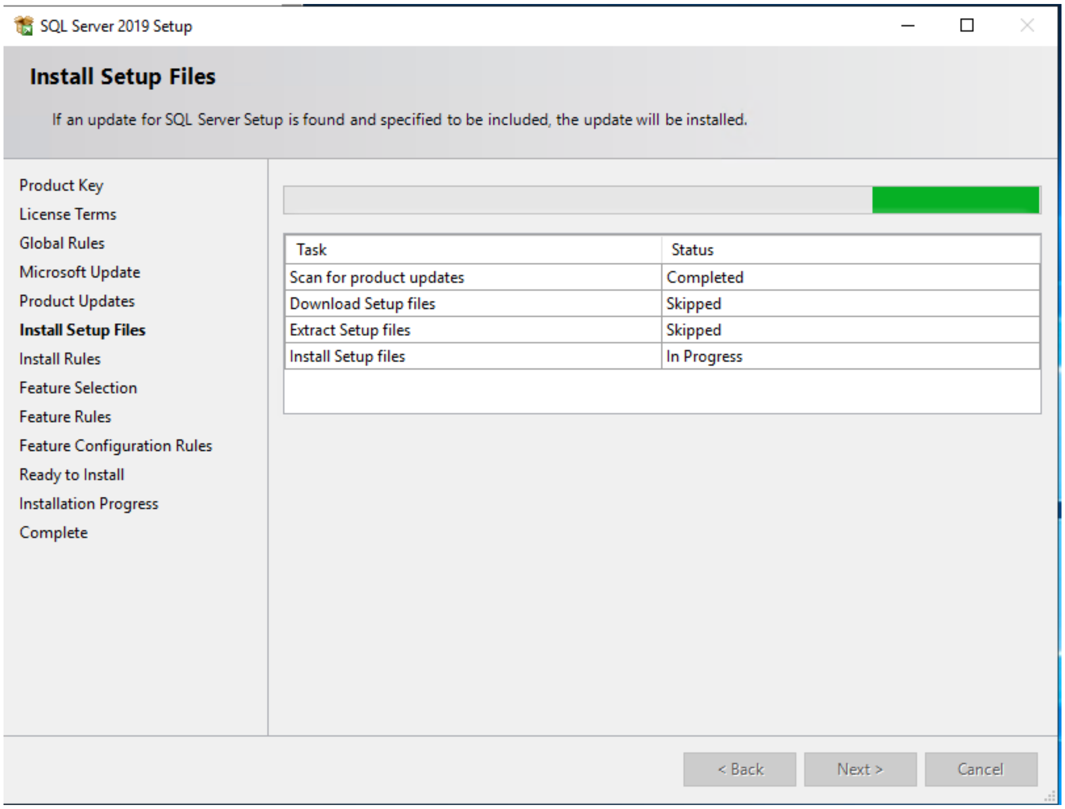
Microsoft Update

Use Microsoft Update to check for important updates

Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2019. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

☑ Use Microsoft Update to check for updates (recommended)

5. Wait for installation of setup files

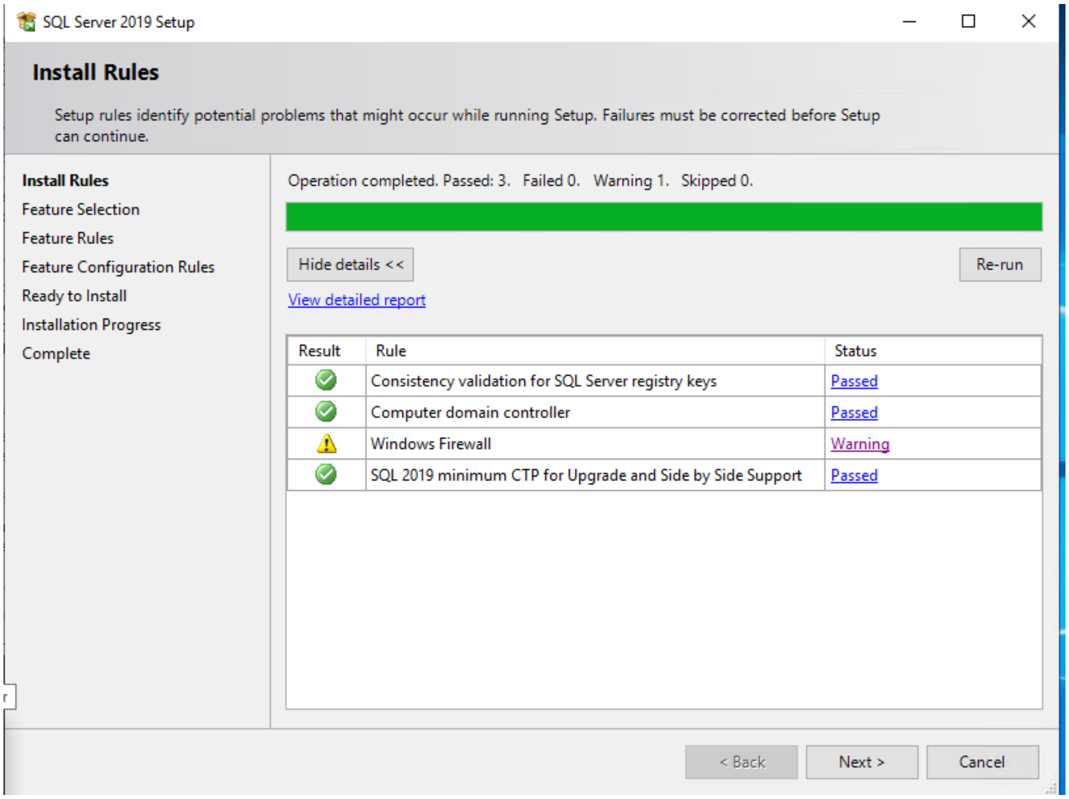


Install Setup Files

If an update for SQL Server Setup is found and specified to be included, the update will be installed.

Task	Status
Scan for product updates	Completed
Download Setup files	Skipped
Extract Setup files	Skipped
Install Setup files	In Progress

6. Verify installations rules passed



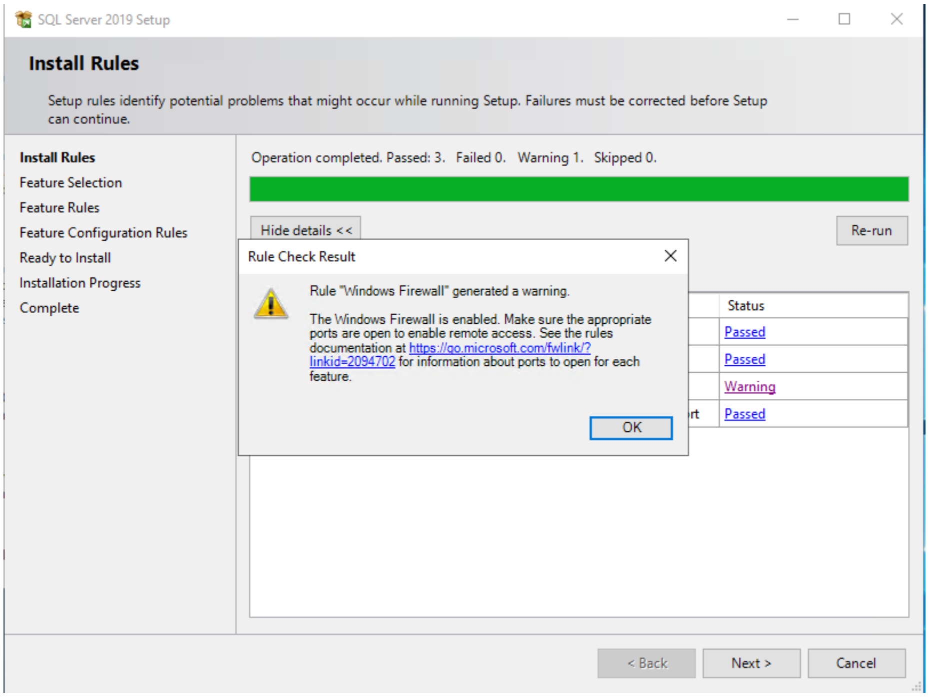
Install Rules

Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.

Operation completed. Passed: 3. Failed 0. Warning 1. Skipped 0.

Result	Rule	Status
✓	Consistency validation for SQL Server registry keys	Passed
✓	Computer domain controller	Passed
⚠	Windows Firewall	Warning
✓	SQL 2019 minimum CTP for Upgrade and Side by Side Support	Passed

a. Check any warnings and correct them as needed.



Install Rules

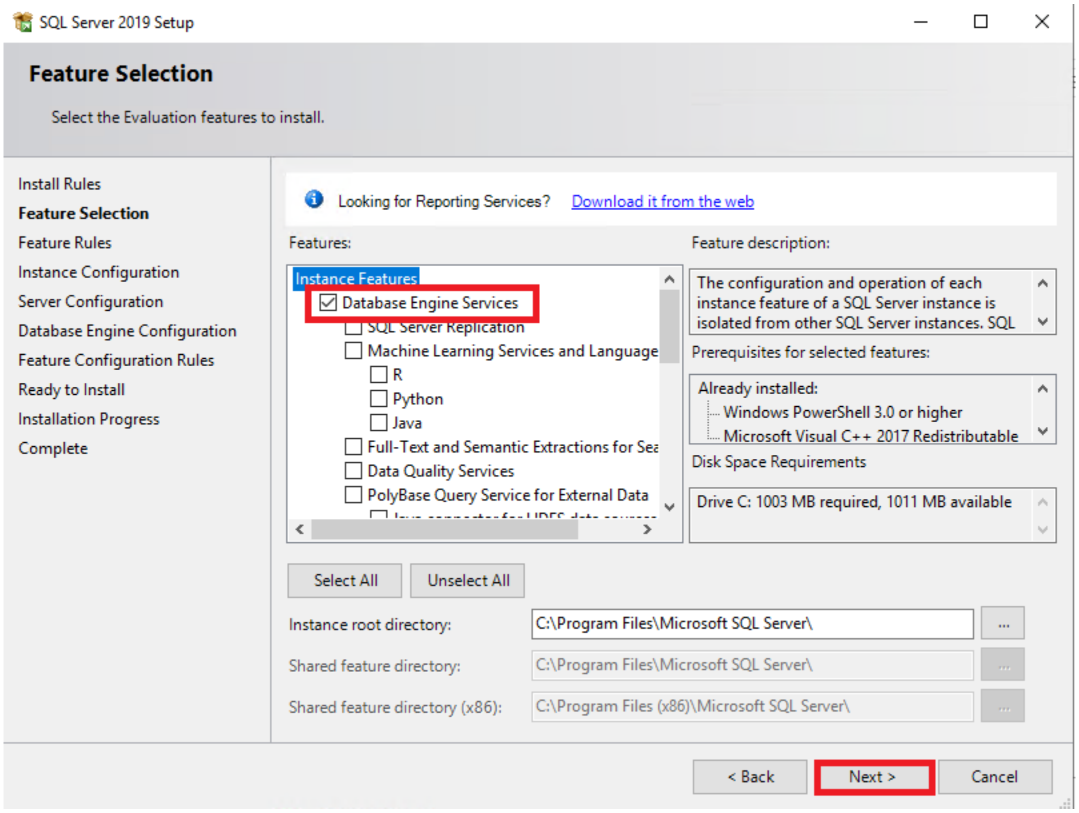
Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.

Operation completed. Passed: 3. Failed 0. Warning 1. Skipped 0.

Rule "Windows Firewall" generated a warning.

The Windows Firewall is enabled. Make sure the appropriate ports are open to enable remote access. See the rules documentation at https://go.microsoft.com/fwlink/?linkid=2094702 for information about ports to open for each feature.

7. Install features and set instance location



SQL Server 2019 Setup

Feature Selection

Select the Evaluation features to install.

Looking for Reporting Services? Download it from the web

Features:

Instance Features
- ☑ Database Engine Services
  - □ SQL Server Replication
  - □ Machine Learning Services and Language
    - □ R
    - □ Python
    - □ Java
  - □ Full-Text and Semantic Extractions for Sea
  - □ Data Quality Services
  - □ PolyBase Query Service for External Data
    - □ Java connector for HDFS data sources

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL

Prerequisites for selected features:

Already installed:
- Windows PowerShell 3.0 or higher
- Microsoft Visual C++ 2017 Redistributable

Disk Space Requirements

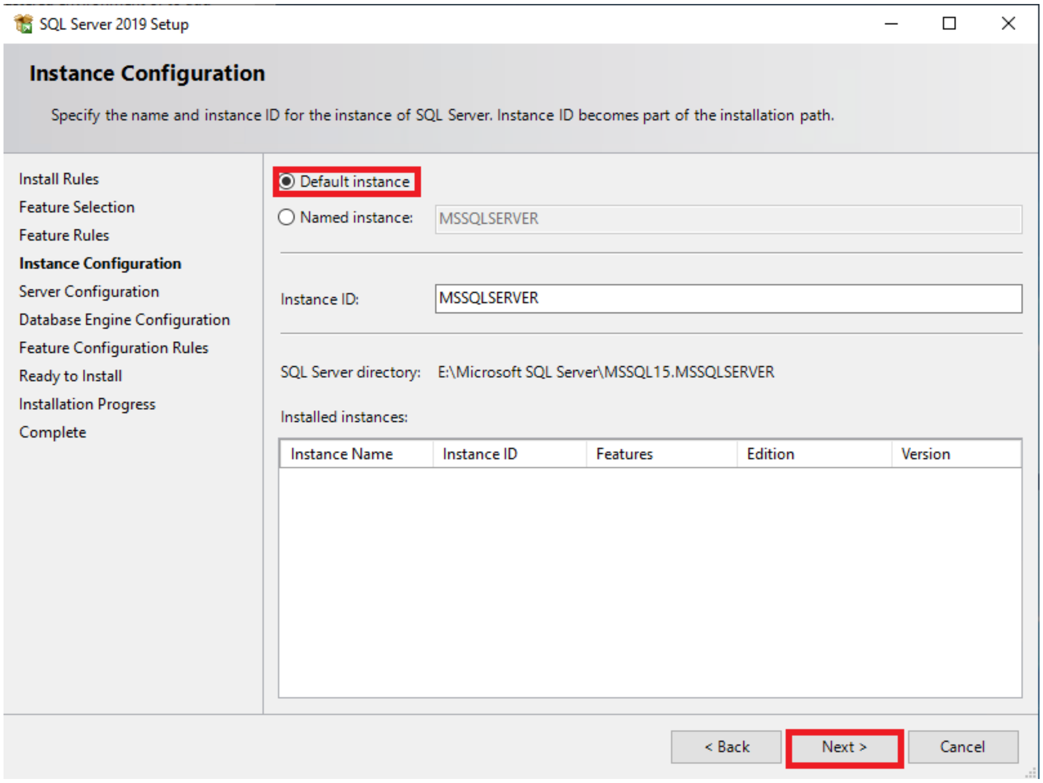
Drive C: 1003 MB required, 1011 MB available

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\

8. Configure Instance with the default instance name



SQL Server 2019 Setup

Instance Configuration

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

● Default instance

○ Named instance: MSSQLSERVER

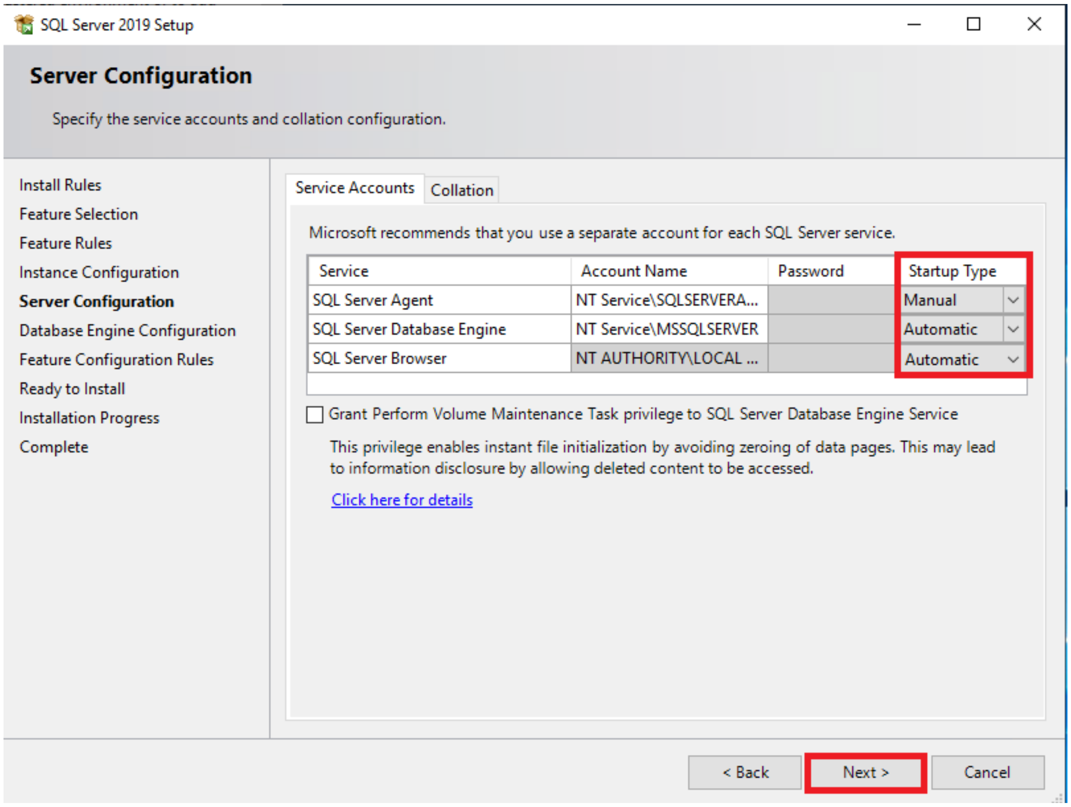
Instance ID: MSSQLSERVER

SQL Server directory: E:\Microsoft SQL Server\MSSQL15.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

9. Configure server with default service accounts



Server Configuration

Specify the service accounts and collation configuration.

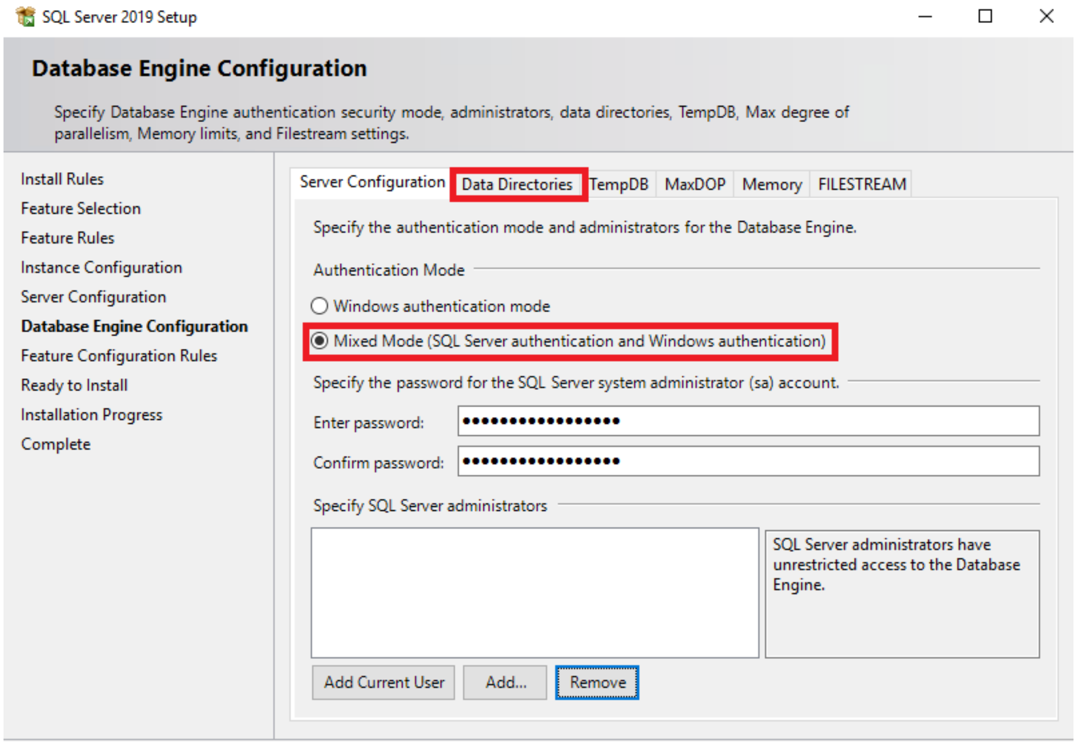
Microsoft recommends that you use a separate account for each SQL Server service.

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 ...		Automatic

□ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

10. Configure Database Engine to have mixed-mode authentication, add necessary users as administrators, and set data directories to use the partition(s) set aside for replication.



Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

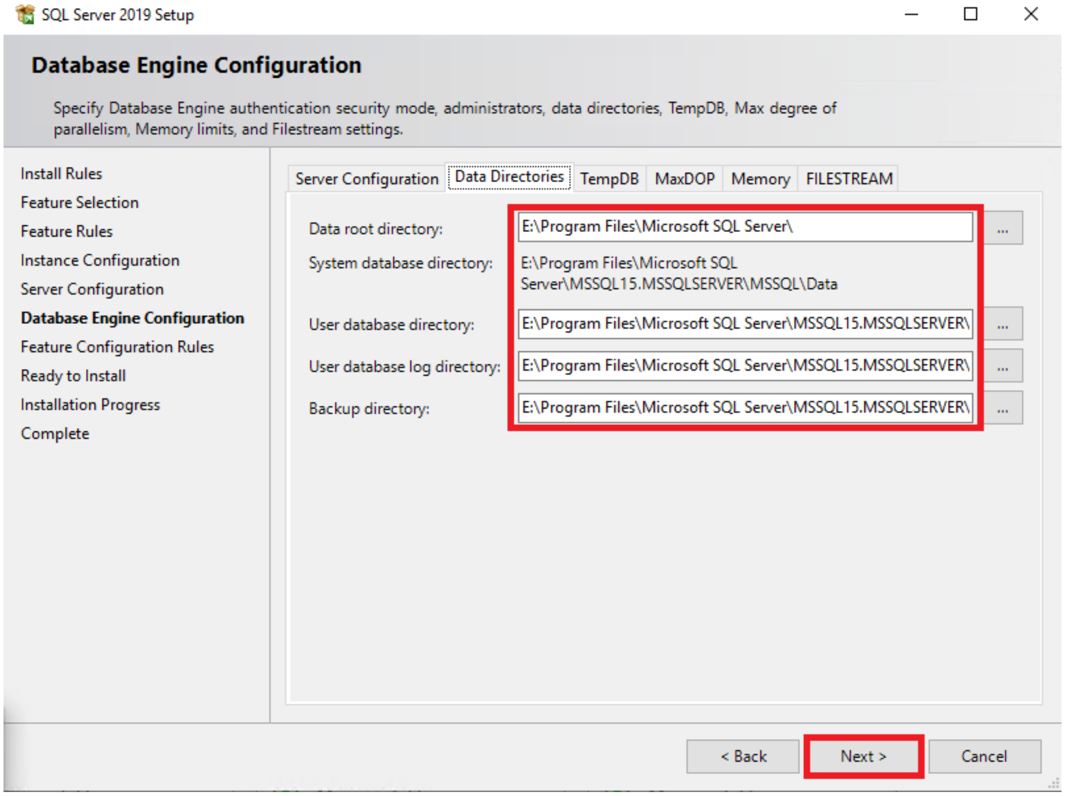
Specify the password for the SQL Server system administrator (sa) account.

Enter password: ●●●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●●●

Specify SQL Server administrators

SQL Server administrators have unrestricted access to the Database Engine.



SQL Server 2019 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories, TempDB, Max degree of parallelism, Memory limits, and Filestream settings.

Data root directory: E:\Program Files\Microsoft SQL Server\

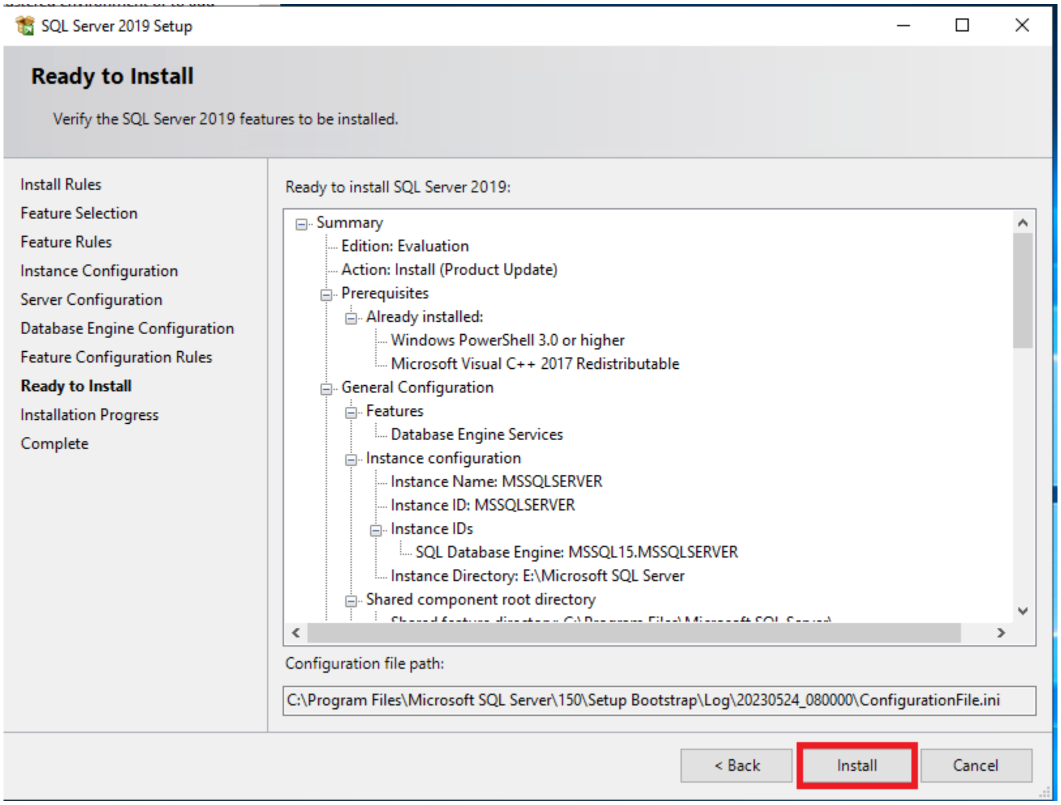
System database directory: E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Data

User database directory: E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\

User database log directory: E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\

Backup directory: E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\

11. Verify Installation Configuration, then install



SQL Server 2019 Setup

Ready to Install

Verify the SQL Server 2019 features to be installed.

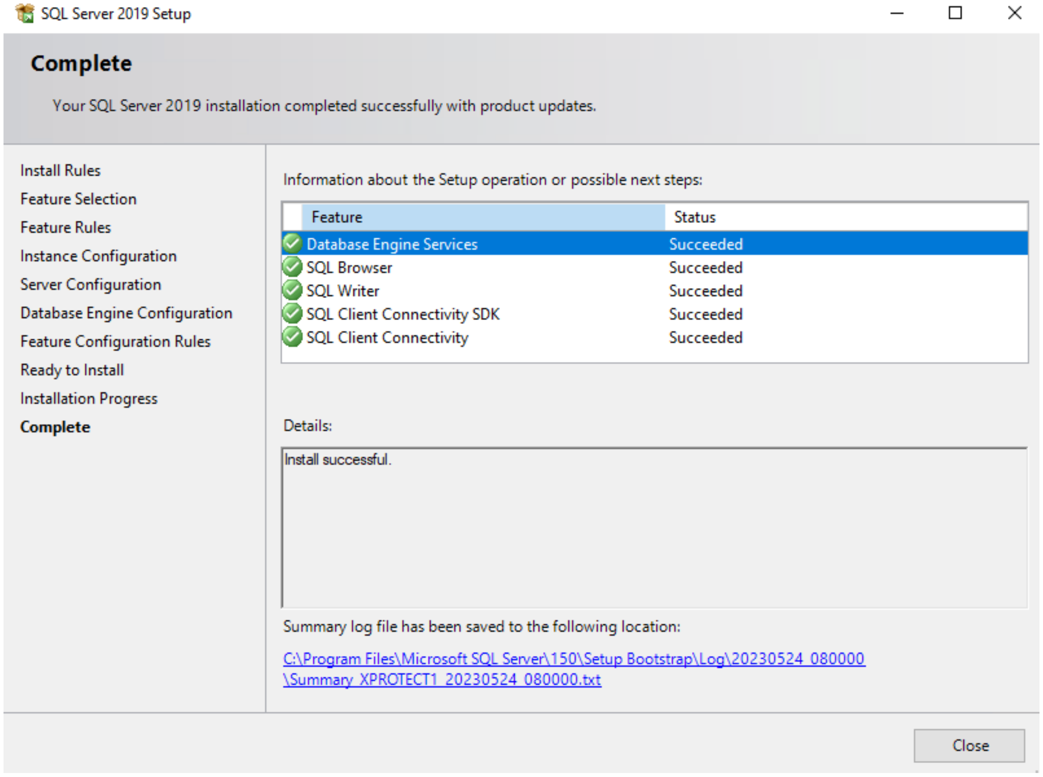
Ready to install SQL Server 2019:

```
Summary
  Edition: Evaluation
  Action: Install (Product Update)
  Prerequisites
    Already installed:
      Windows PowerShell 3.0 or higher
      Microsoft Visual C++ 2017 Redistributable
  General Configuration
    Features
      Database Engine Services
    Instance configuration
      Instance Name: MSSQLSERVER
      Instance ID: MSSQLSERVER
      Instance IDs
        SQL Database Engine: MSSQL15.MSSQLSERVER
      Instance Directory: E:\Microsoft SQL Server
    Shared component root directory
      Shared feature directory: C:\Program Files\Microsoft SQL Server\
```

Configuration file path:

C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20230524_080000\ConfigurationFile.ini

12. Verify installation was successful



SQL Server 2019 Setup

Complete

Your SQL Server 2019 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
✓ Database Engine Services	Succeeded
✓ SQL Browser	Succeeded
✓ SQL Writer	Succeeded
✓ SQL Client Connectivity SDK	Succeeded
✓ SQL Client Connectivity	Succeeded

Details:

Install successful.

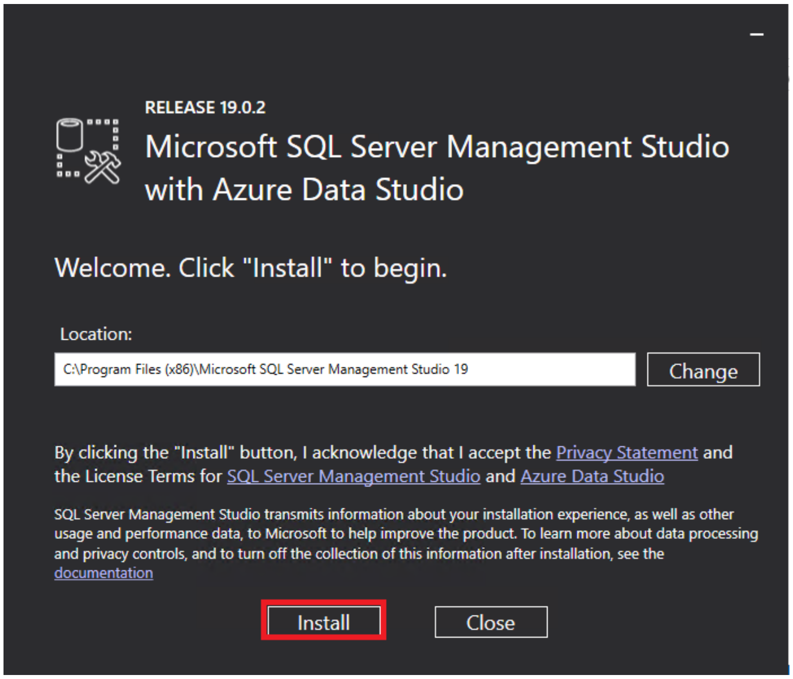
Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\Log\20230524_080000\Summary_XPROTECT1_20230524_080000.txt

13. Repeat steps 1-12 on XPROTECT2

Download and install SQL Server Management Studio on both XPROTECT1 and XPROTECT2
Install SQL Server Management Studio (SSMS):

1. Install



RELEASE 19.0.2

Microsoft SQL Server Management Studio with Azure Data Studio

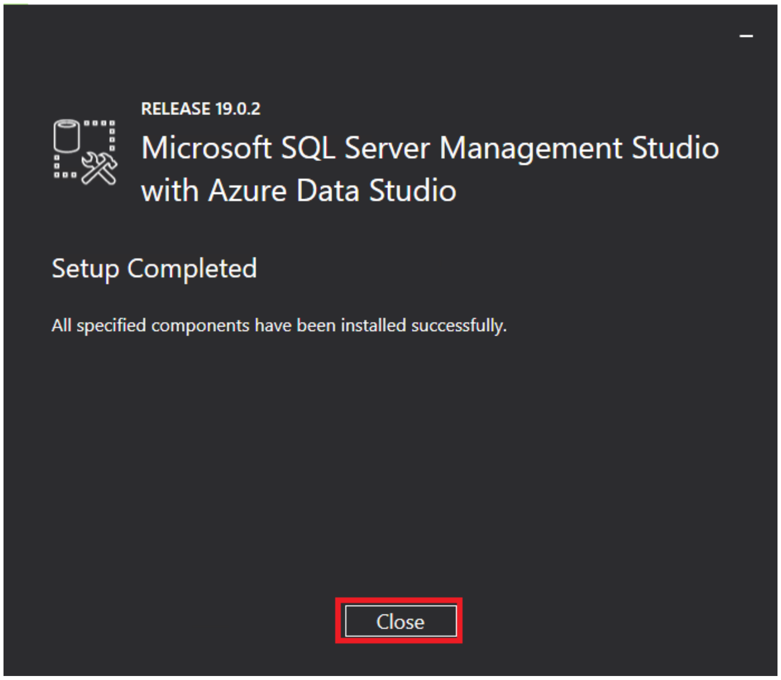
Welcome. Click "Install" to begin.

Location:

C:\Program Files (x86)\Microsoft SQL Server Management Studio 19

By clicking the "Install" button, I acknowledge that I accept the Privacy Statement and the License Terms for SQL Server Management Studio and Azure Data Studio

SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation



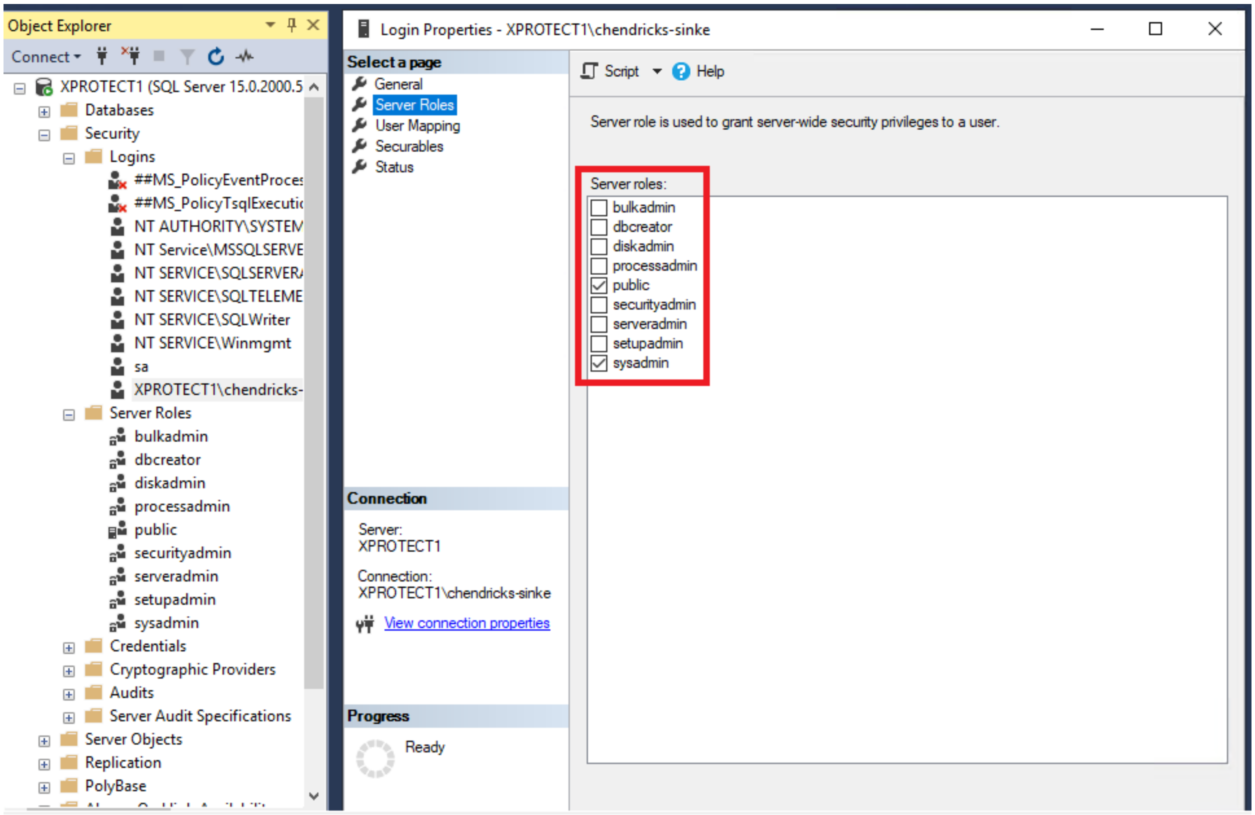
RELEASE 19.0.2

Microsoft SQL Server Management Studio with Azure Data Studio

Setup Completed

All specified components have been installed successfully.

2. Connect to each SQL instance and verify that the user account has ‘sysadmin’ and ‘public’ role



Server role is used to grant server-wide security privileges to a user.

Server roles:

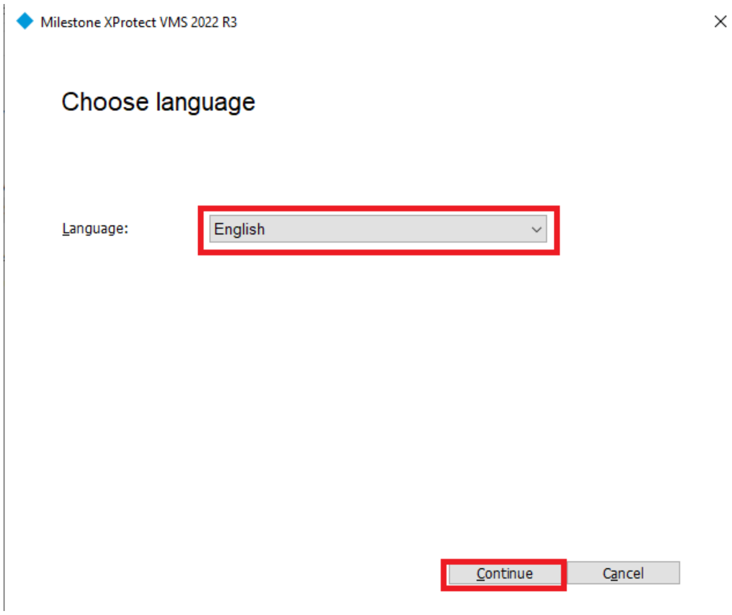
- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

Server:
XPROTECT1

Connection:
XPROTECT1\chendricks-sinke

Step 2 - Install Milestone XProtect

1. Choose language

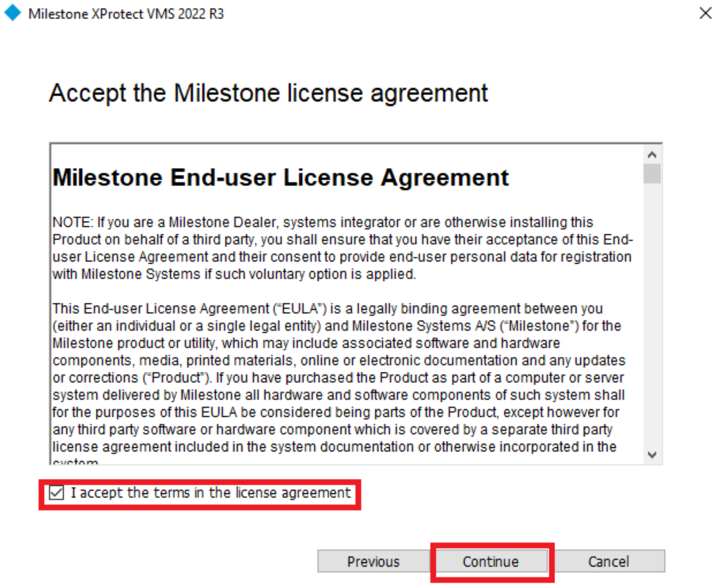


Milestone XProtect VMS 2022 R3

Choose language

Language: English

2. Agree to Terms and Conditions



Milestone XProtect VMS 2022 R3

Accept the Milestone license agreement

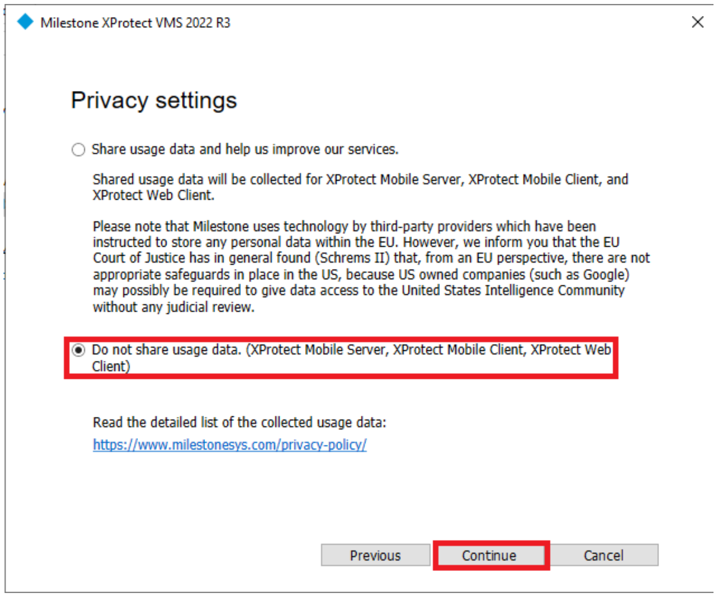
Milestone End-user License Agreement

NOTE: If you are a Milestone Dealer, systems integrator or are otherwise installing this Product on behalf of a third party, you shall ensure that you have their acceptance of this End-user License Agreement and their consent to provide end-user personal data for registration with Milestone Systems if such voluntary option is applied.

This End-user License Agreement ("EULA") is a legally binding agreement between you (either an individual or a single legal entity) and Milestone Systems A/S ("Milestone") for the Milestone product or utility, which may include associated software and hardware components, media, printed materials, online or electronic documentation and any updates or corrections ("Product"). If you have purchased the Product as part of a computer or server system delivered by Milestone all hardware and software components of such system shall for the purposes of this EULA be considered being parts of the Product, except however for any third party software or hardware component which is covered by a separate third party license agreement included in the system documentation or otherwise incorporated in the system

☑ I accept the terms in the license agreement

3. Determine whether you want to share data



Milestone XProtect VMS 2022 R3

Privacy settings

○ Share usage data and help us improve our services.

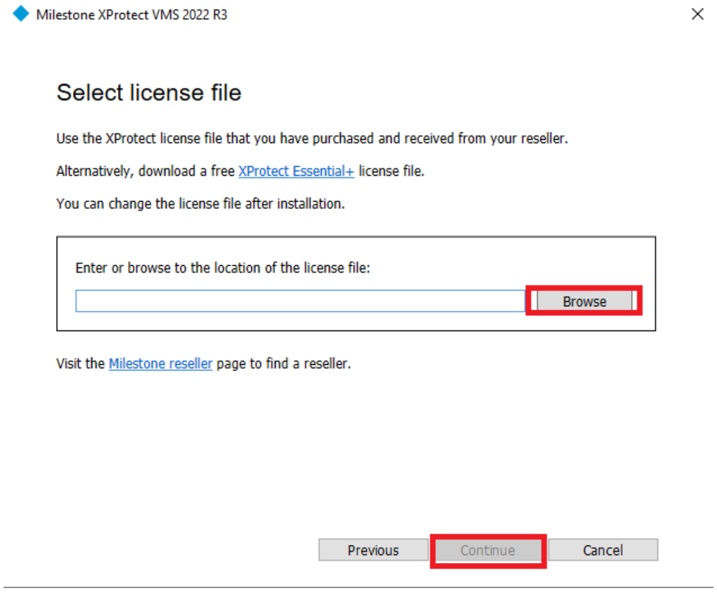
Shared usage data will be collected for XProtect Mobile Server, XProtect Mobile Client, and XProtect Web Client.

Please note that Milestone uses technology by third-party providers which have been instructed to store any personal data within the EU. However, we inform you that the EU Court of Justice has in general found (Schrems II) that, from an EU perspective, there are not appropriate safeguards in place in the US, because US owned companies (such as Google) may possibly be required to give data access to the United States Intelligence Community without any judicial review.

● Do not share usage data. (XProtect Mobile Server, XProtect Mobile Client, XProtect Web Client)

Read the detailed list of the collected usage data:
https://www.milestonesys.com/privacy-policy/

4. Add License



Milestone XProtect VMS 2022 R3

Select license file

Use the XProtect license file that you have purchased and received from your reseller.

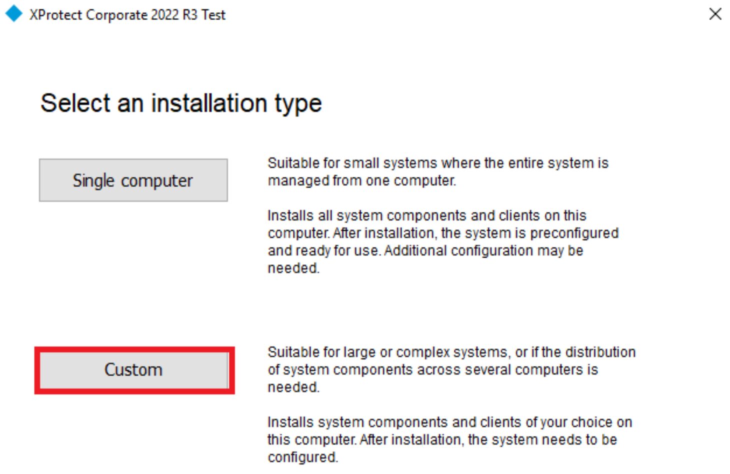
Alternatively, download a free XProtect Essential+ license file.

You can change the license file after installation.

Enter or browse to the location of the license file:

Visit the Milestone reseller page to find a reseller.

5. Choose custom install



XProtect Corporate 2022 R3 Test

Select an installation type

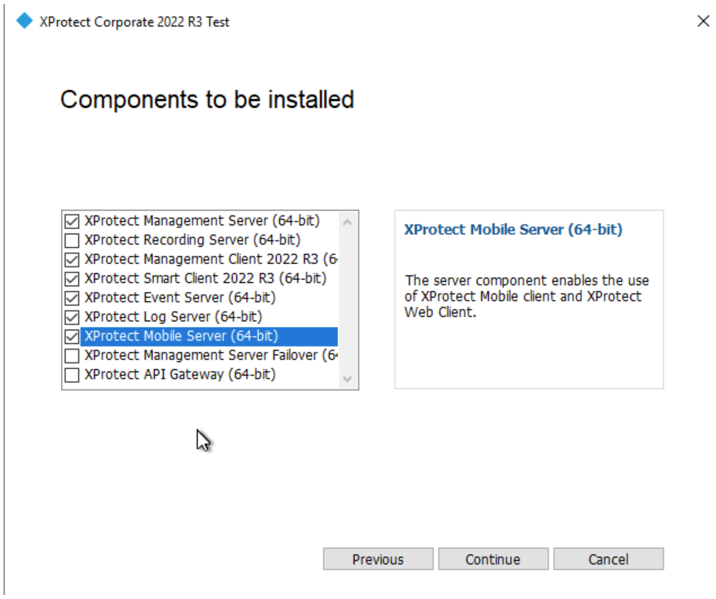
Suitable for small systems where the entire system is managed from one computer.

Installs all system components and clients on this computer. After installation, the system is preconfigured and ready for use. Additional configuration may be needed.

Suitable for large or complex systems, or if the distribution of system components across several computers is needed.

Installs system components and clients of your choice on this computer. After installation, the system needs to be configured.

6. Choose the below components



XProtect Corporate 2022 R3 Test

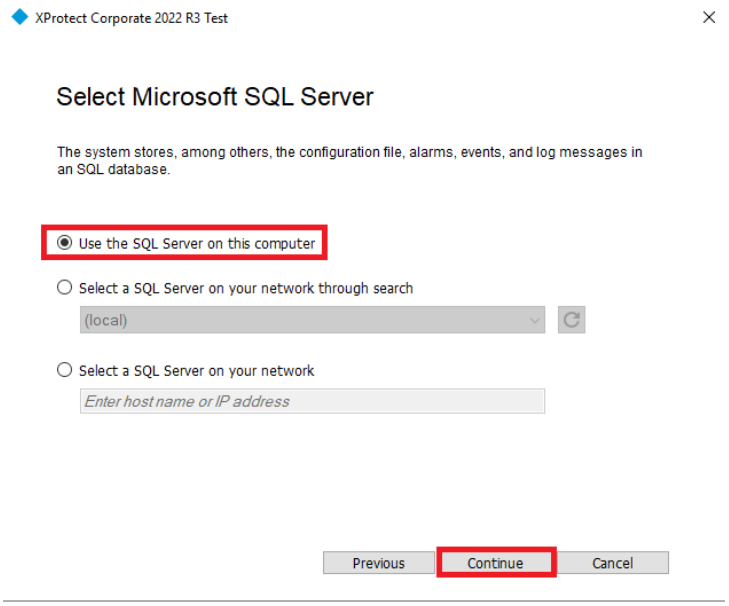
Components to be installed

- ☑ XProtect Management Server (64-bit)
- ☐ XProtect Recording Server (64-bit)
- ☑ XProtect Management Client 2022 R3 (6
- ☑ XProtect Smart Client 2022 R3 (64-bit)
- ☑ XProtect Event Server (64-bit)
- ☑ XProtect Log Server (64-bit)
- ☑ XProtect Mobile Server (64-bit)
- ☐ XProtect Management Server Failover (6
- ☐ XProtect API Gateway (64-bit)

XProtect Mobile Server (64-bit)

The server component enables the use of XProtect Mobile client and XProtect Web Client.

7. Select SQL Server



XProtect Corporate 2022 R3 Test

Select Microsoft SQL Server

The system stores, among others, the configuration file, alarms, events, and log messages in an SQL database.

● Use the SQL Server on this computer

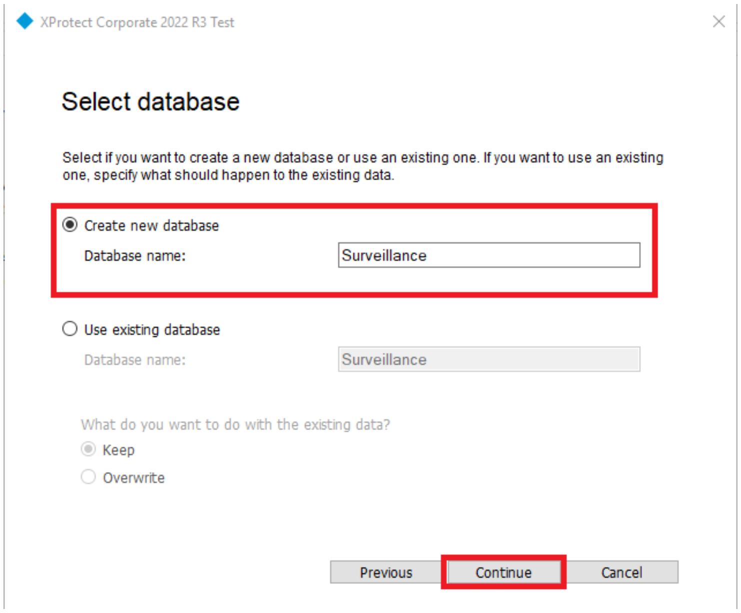
○ Select a SQL Server on your network through search

(local)

○ Select a SQL Server on your network

Enter host name or IP address

8. Create a new database



XProtect Corporate 2022 R3 Test

Select database

Select if you want to create a new database or use an existing one. If you want to use an existing one, specify what should happen to the existing data.

● Create new database

Database name: Surveillance

○ Use existing database

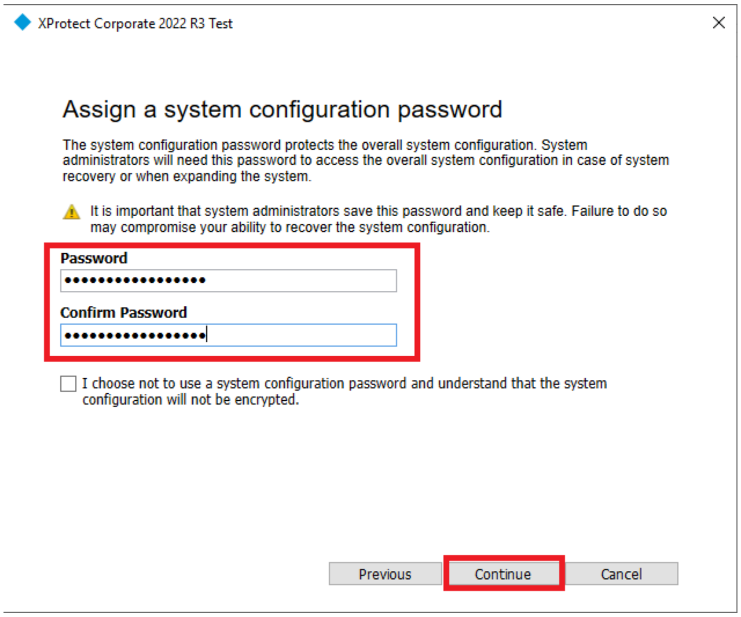
Database name: Surveillance

What do you want to do with the existing data?

● Keep

○ Overwrite

9. Set system configuration password



XProtect Corporate 2022 R3 Test

Assign a system configuration password

The system configuration password protects the overall system configuration. System administrators will need this password to access the overall system configuration in case of system recovery or when expanding the system.

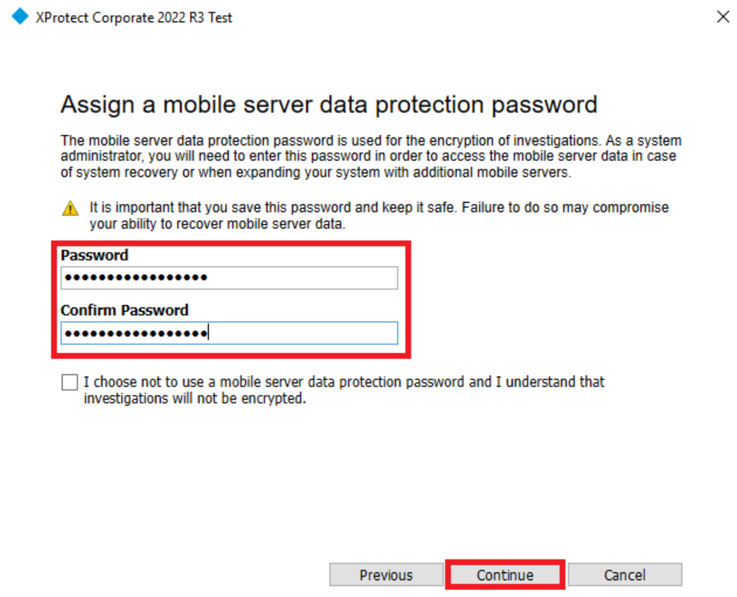
⚠ It is important that system administrators save this password and keep it safe. Failure to do so may compromise your ability to recover the system configuration.

Password: ●●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●●

□ I choose not to use a system configuration password and understand that the system configuration will not be encrypted.

10. Set mobile password



XProtect Corporate 2022 R3 Test

Assign a mobile server data protection password

The mobile server data protection password is used for the encryption of investigations. As a system administrator, you will need to enter this password in order to access the mobile server data in case of system recovery or when expanding your system with additional mobile servers.

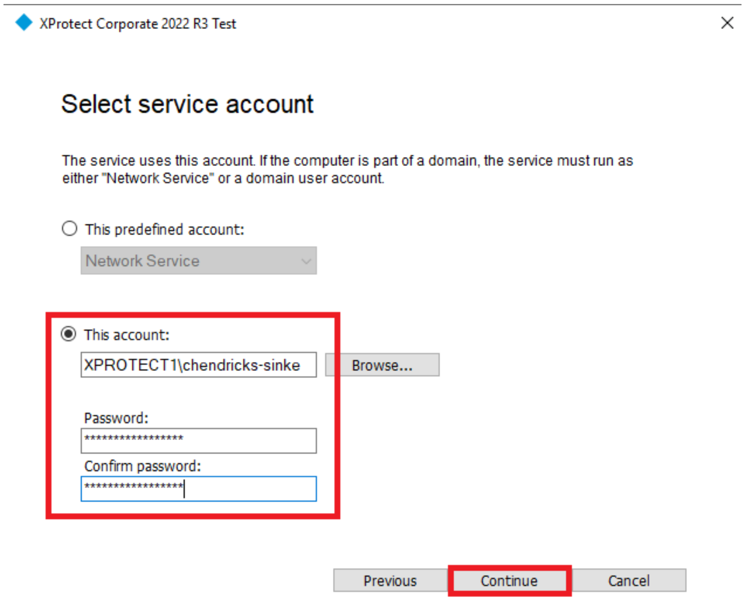
⚠ It is important that you save this password and keep it safe. Failure to do so may compromise your ability to recover mobile server data.

Password: ●●●●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●●●●

□ I choose not to use a mobile server data protection password and I understand that investigations will not be encrypted.

11. Select a service account, using the same account that you set up above that is in the local administrators group on each server and uses the same password across servers.



XProtect Corporate 2022 R3 Test

Select service account

The service uses this account. If the computer is part of a domain, the service must run as either "Network Service" or a domain user account.

○ This predefined account:

Network Service

● This account:

XPROTECT1\chendricks-sinke

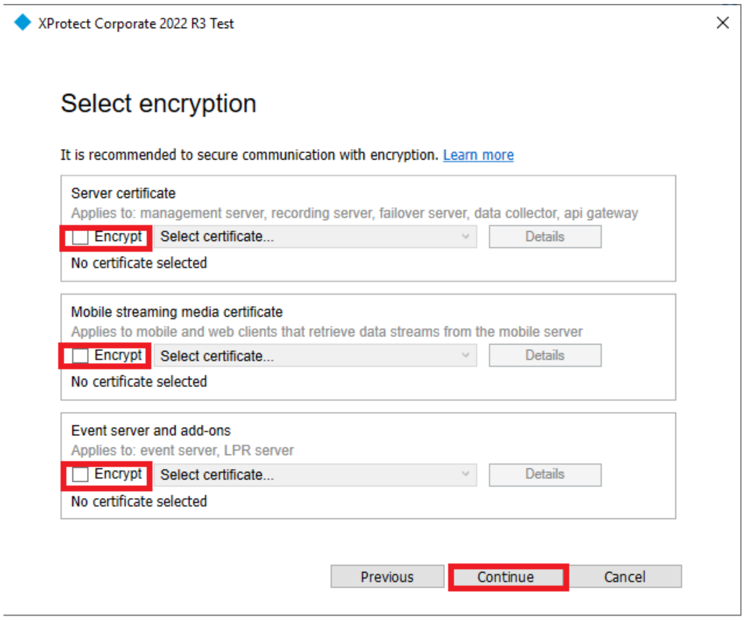
Password:

****

Confirm password:

****

12. Turn off encryption



XProtect Corporate 2022 R3 Test

Select encryption

It is recommended to secure communication with encryption. Learn more

Server certificate

Applies to: management server, recording server, failover server, data collector, api gateway

□ Encrypt Select certificate...

No certificate selected

Mobile streaming media certificate

Applies to mobile and web clients that retrieve data streams from the mobile server

□ Encrypt Select certificate...

No certificate selected

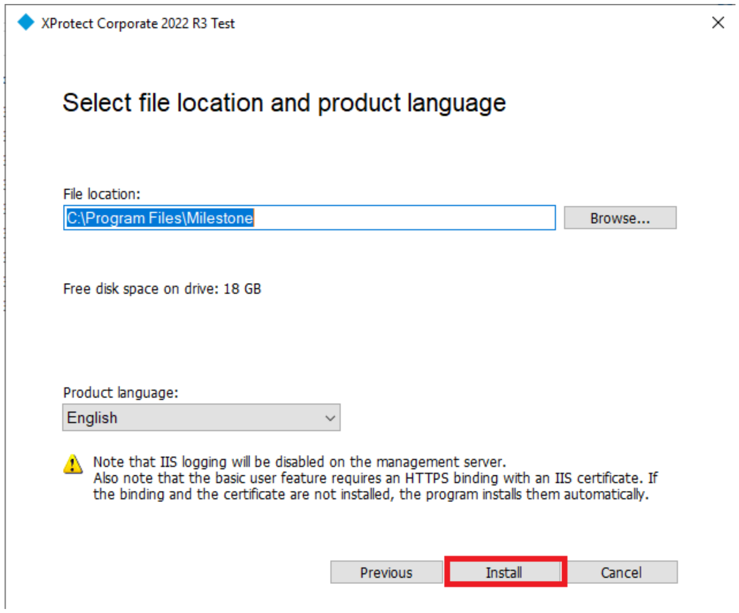
Event server and add-ons

Applies to: event server, LPR server

□ Encrypt Select certificate...

No certificate selected

13. Select Installation location



XProtect Corporate 2022 R3 Test

Select file location and product language

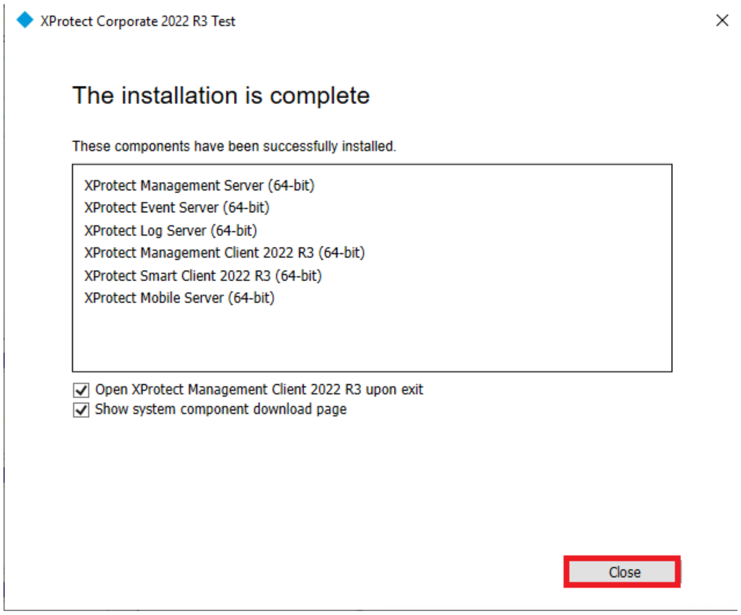
File location: C:\Program Files\Milestone

Free disk space on drive: 18 GB

Product language: English

Note that IIS logging will be disabled on the management server.
Also note that the basic user feature requires an HTTPS binding with an IIS certificate. If the binding and the certificate are not installed, the program installs them automatically.

14. Verify Installation



XProtect Corporate 2022 R3 Test

The installation is complete

These components have been successfully installed.

XProtect Management Server (64-bit)
XProtect Event Server (64-bit)
XProtect Log Server (64-bit)
XProtect Management Client 2022 R3 (64-bit)
XProtect Smart Client 2022 R3 (64-bit)
XProtect Mobile Server (64-bit)

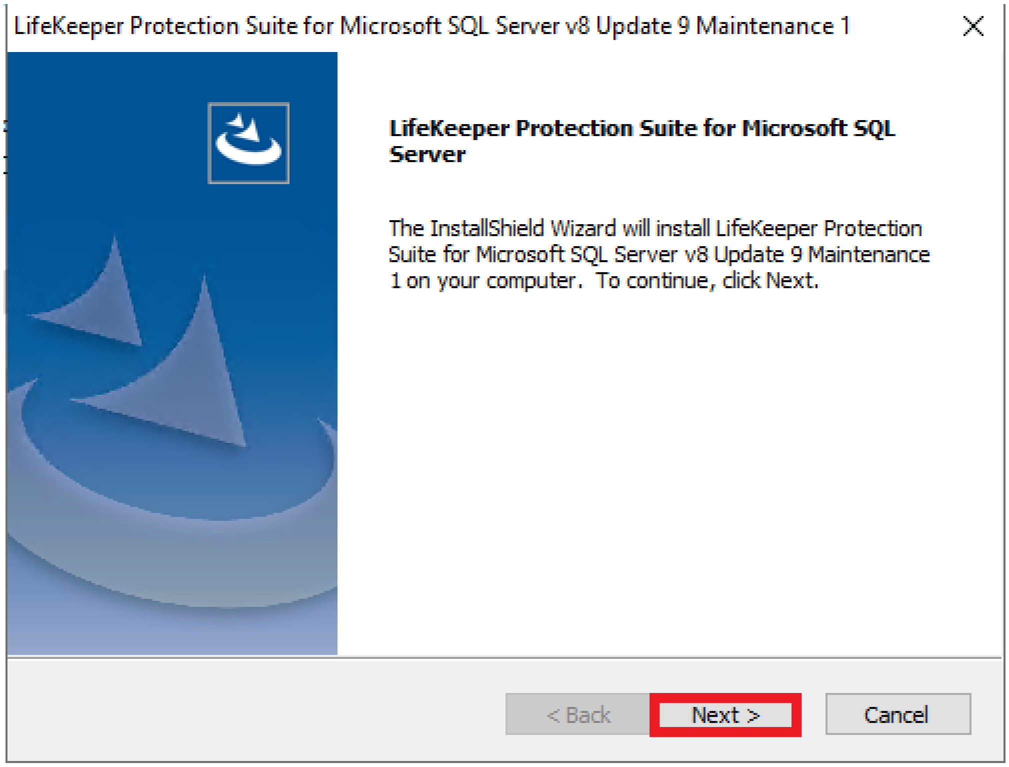
☑ Open XProtect Management Client 2022 R3 upon exit
☑ Show system component download page

15. Repeat steps 1-14 on XPROTECT2

Step 3 - Install SIOS Protection Suite w/SQL Server ARK

Install SPS:

1. Start Install

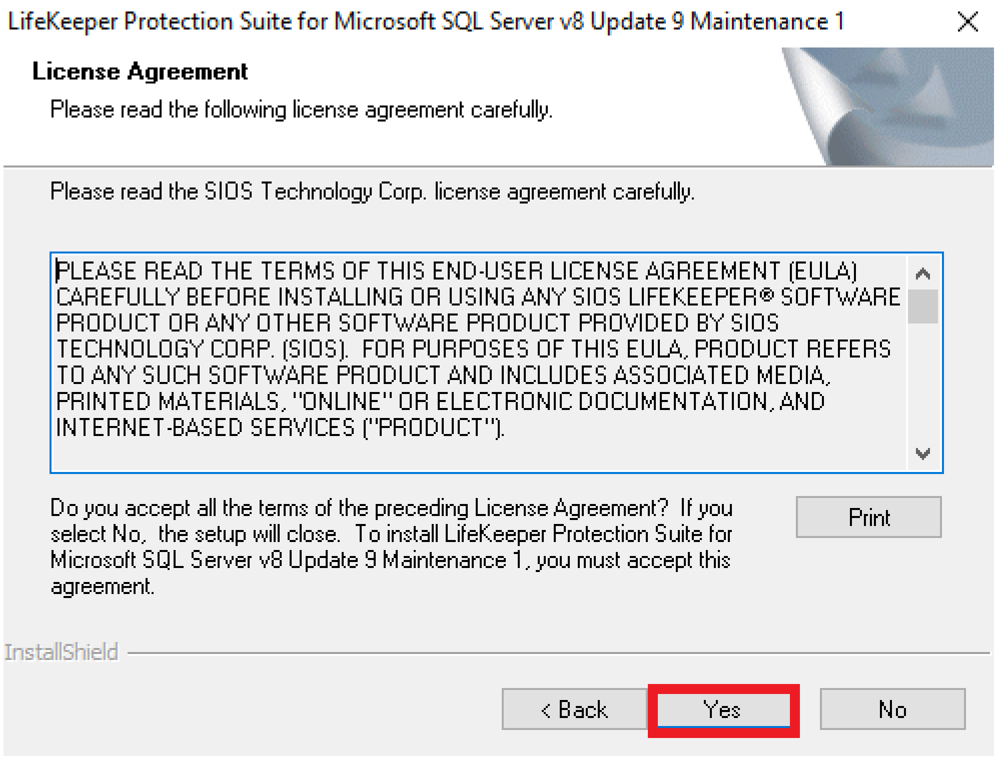


LifeKeeper Protection Suite for Microsoft SQL Server v8 Update 9 Maintenance 1

LifeKeeper Protection Suite for Microsoft SQL Server

The InstallShield Wizard will install LifeKeeper Protection Suite for Microsoft SQL Server v8 Update 9 Maintenance 1 on your computer. To continue, click Next.

2. Accept License Agreement



LifeKeeper Protection Suite for Microsoft SQL Server v8 Update 9 Maintenance 1

License Agreement

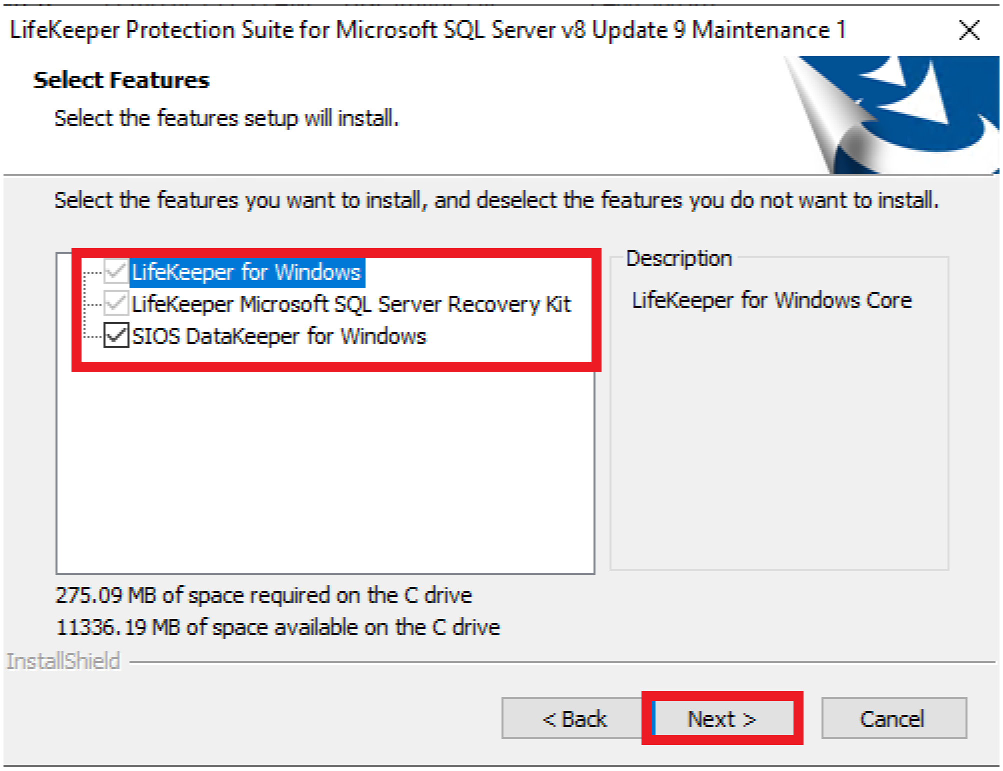
Please read the following license agreement carefully.

Please read the SIOS Technology Corp. license agreement carefully.

PLEASE READ THE TERMS OF THIS END-USER LICENSE AGREEMENT (EULA) CAREFULLY BEFORE INSTALLING OR USING ANY SIOS LIFEKEEPER® SOFTWARE PRODUCT OR ANY OTHER SOFTWARE PRODUCT PROVIDED BY SIOS TECHNOLOGY CORP. (SIOS). FOR PURPOSES OF THIS EULA, PRODUCT REFERS TO ANY SUCH SOFTWARE PRODUCT AND INCLUDES ASSOCIATED MEDIA, PRINTED MATERIALS, "ONLINE" OR ELECTRONIC DOCUMENTATION, AND INTERNET-BASED SERVICES ("PRODUCT").

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install LifeKeeper Protection Suite for Microsoft SQL Server v8 Update 9 Maintenance 1, you must accept this agreement.

3. Select features



LifeKeeper Protection Suite for Microsoft SQL Server v8 Update 9 Maintenance 1

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ☑ LifeKeeper for Windows
- ☑ LifeKeeper Microsoft SQL Server Recovery Kit
- ☑ SIOS DataKeeper for Windows

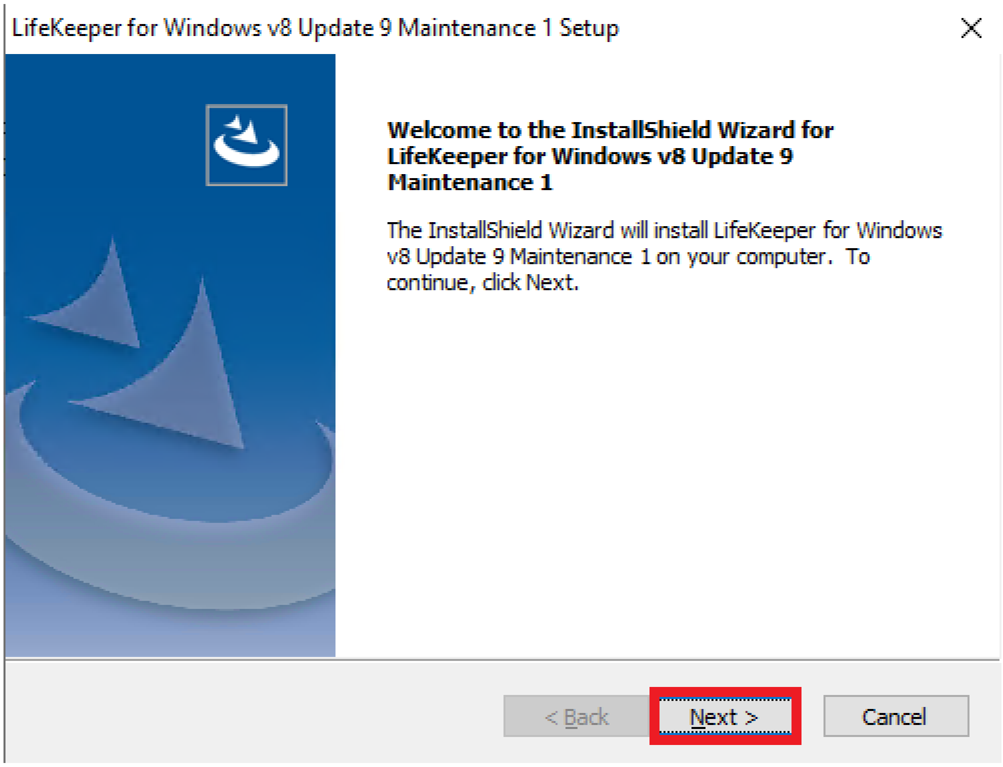
Description

LifeKeeper for Windows Core

275.09 MB of space required on the C drive

11336.19 MB of space available on the C drive

4. Run Update

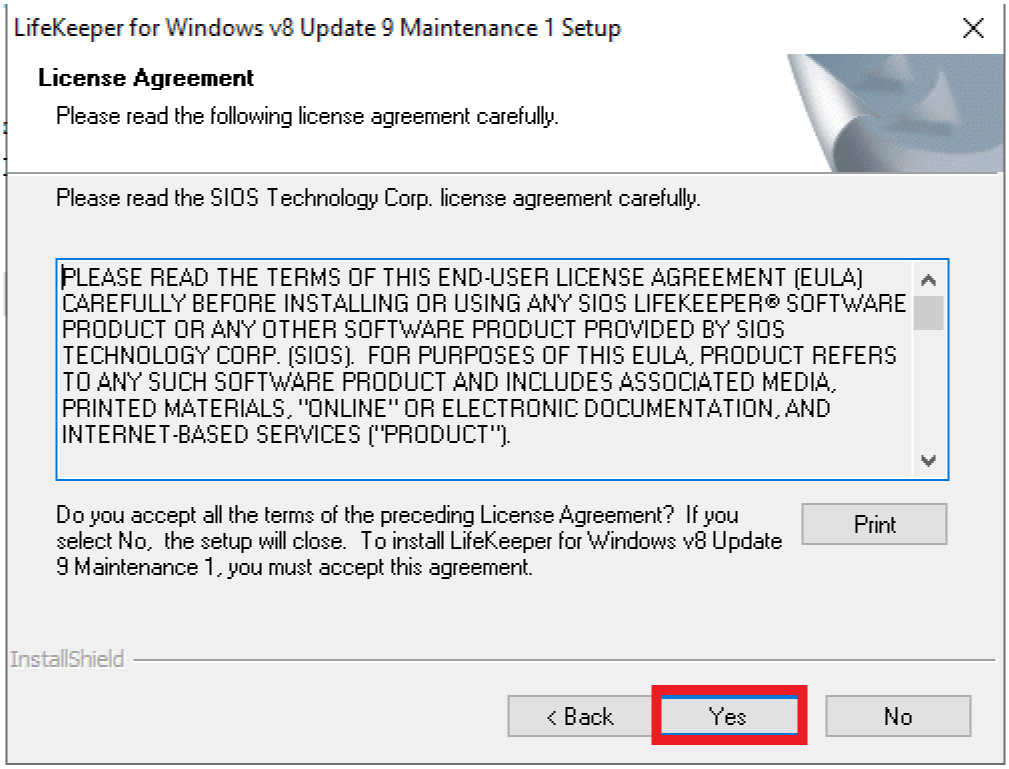


LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup

Welcome to the InstallShield Wizard for LifeKeeper for Windows v8 Update 9 Maintenance 1

The InstallShield Wizard will install LifeKeeper for Windows v8 Update 9 Maintenance 1 on your computer. To continue, click Next.

5. Accept LIcense Agreement (again)



LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup

License Agreement

Please read the following license agreement carefully.

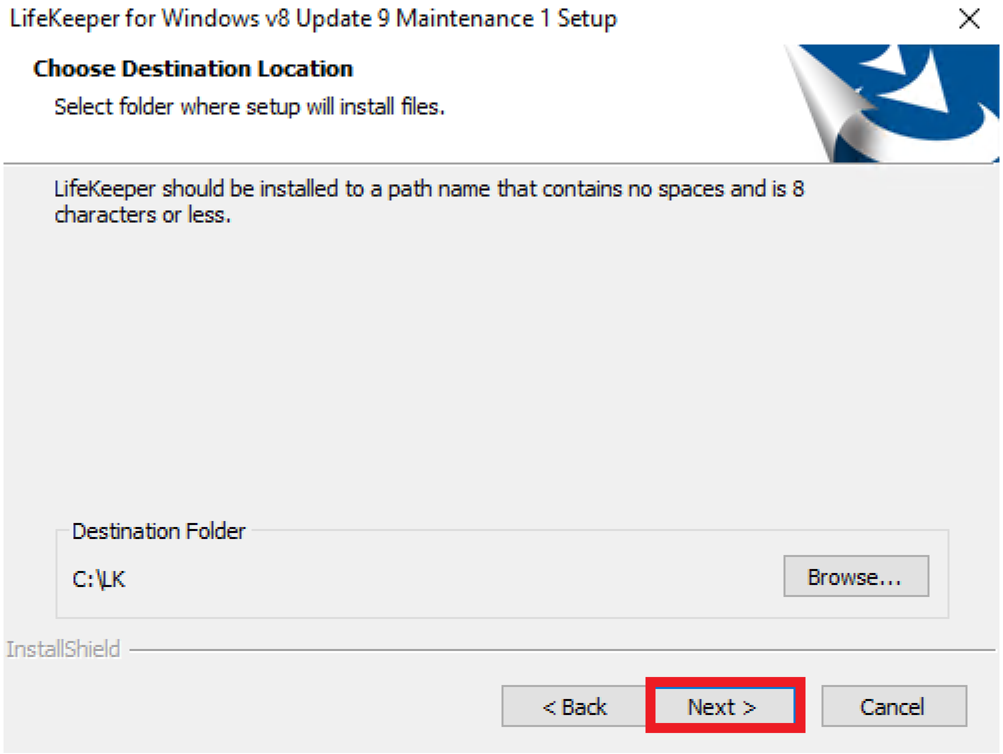
Please read the SIOS Technology Corp. license agreement carefully.

PLEASE READ THE TERMS OF THIS END-USER LICENSE AGREEMENT (EULA) CAREFULLY BEFORE INSTALLING OR USING ANY SIOS LIFEKEEPER® SOFTWARE PRODUCT OR ANY OTHER SOFTWARE PRODUCT PROVIDED BY SIOS TECHNOLOGY CORP. (SIOS). FOR PURPOSES OF THIS EULA, PRODUCT REFERS TO ANY SUCH SOFTWARE PRODUCT AND INCLUDES ASSOCIATED MEDIA, PRINTED MATERIALS, "ONLINE" OR ELECTRONIC DOCUMENTATION, AND INTERNET-BASED SERVICES ("PRODUCT").

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install LifeKeeper for Windows v8 Update 9 Maintenance 1, you must accept this agreement.

6. Choose installation location.
NOTE: Use the default location C:\LK, or minimally don't use a path that has spaces in

the path name.



LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup

Choose Destination Location

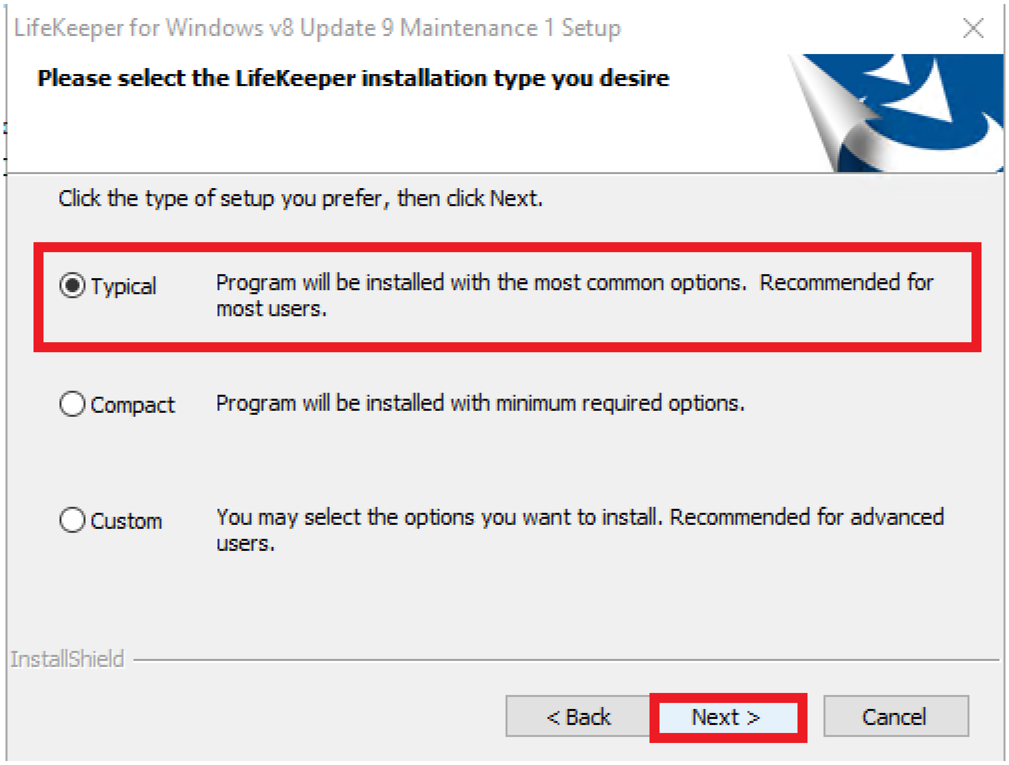
Select folder where setup will install files.

LifeKeeper should be installed to a path name that contains no spaces and is 8 characters or less.

Destination Folder

C:\LK

7. Choose Standard Install (say yes to all recommendations)



LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup

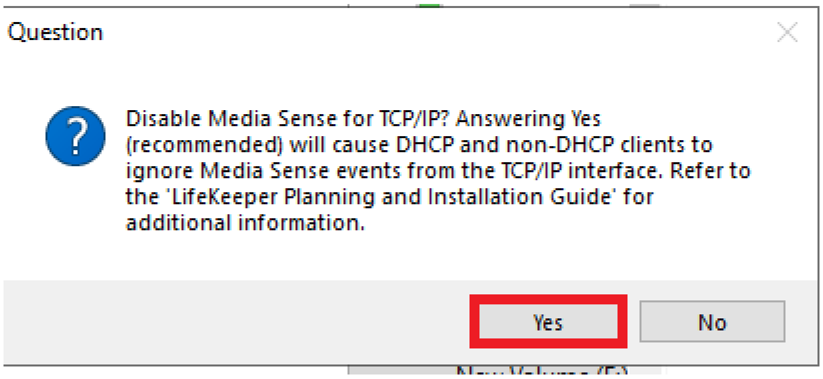
Please select the LifeKeeper installation type you desire

Click the type of setup you prefer, then click Next.

● Typical — Program will be installed with the most common options. Recommended for most users.

○ Compact — Program will be installed with minimum required options.

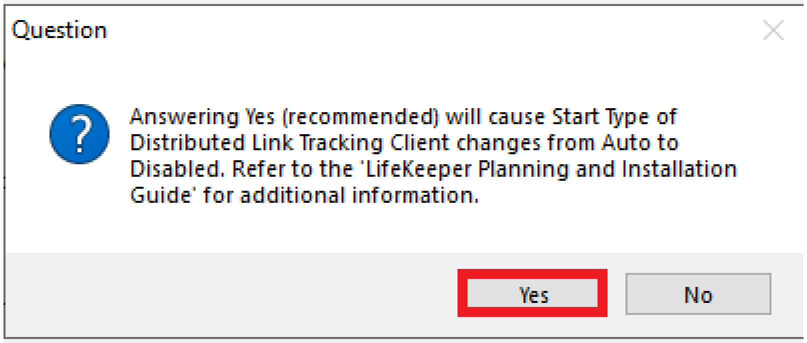
○ Custom — You may select the options you want to install. Recommended for advanced users.



Question

Disable Media Sense for TCP/IP? Answering Yes (recommended) will cause DHCP and non-DHCP clients to ignore Media Sense events from the TCP/IP interface. Refer to the 'LifeKeeper Planning and Installation Guide' for additional information.

a.

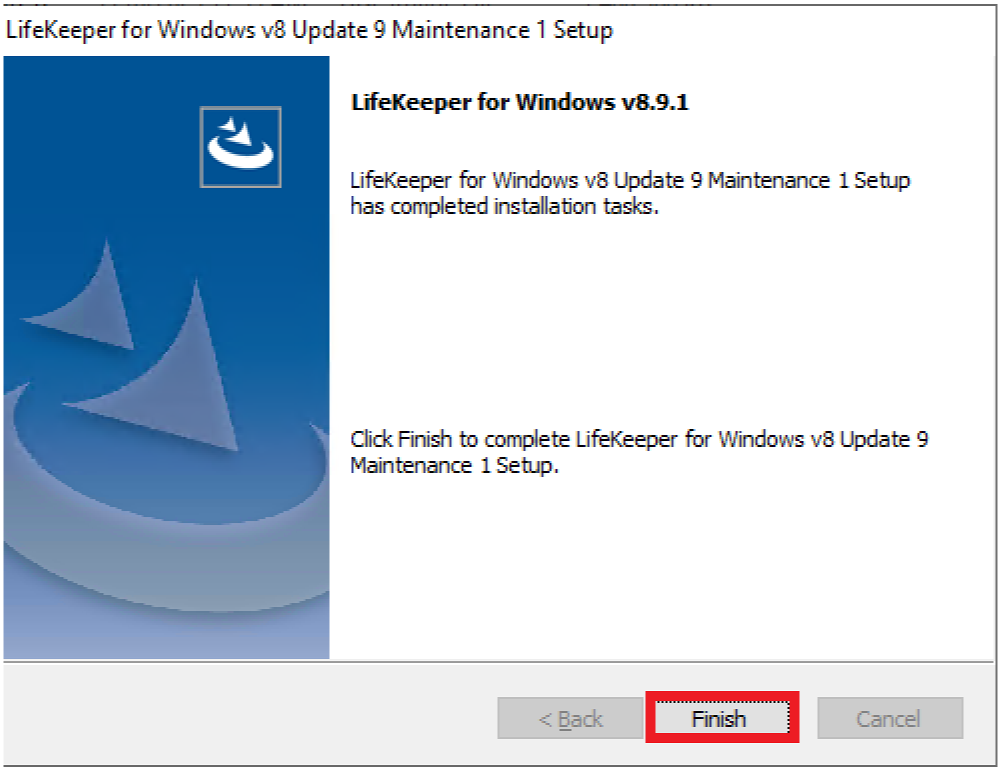


Question

Answering Yes (recommended) will cause Start Type of Distributed Link Tracking Client changes from Auto to Disabled. Refer to the 'LifeKeeper Planning and Installation Guide' for additional information.

b.

8. Finish update



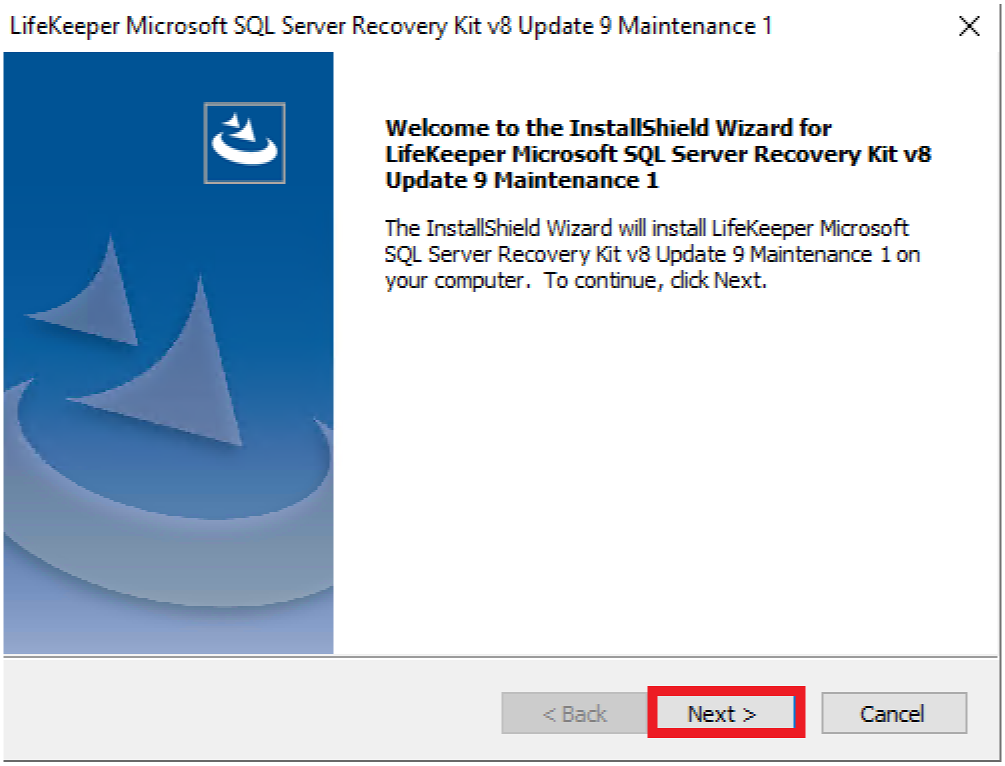
LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup

LifeKeeper for Windows v8.9.1

LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup has completed installation tasks.

Click Finish to complete LifeKeeper for Windows v8 Update 9 Maintenance 1 Setup.

9. Install the Recovery Kit.
   NOTE: This step will begin automatically after LifeKeeper finishes installing.

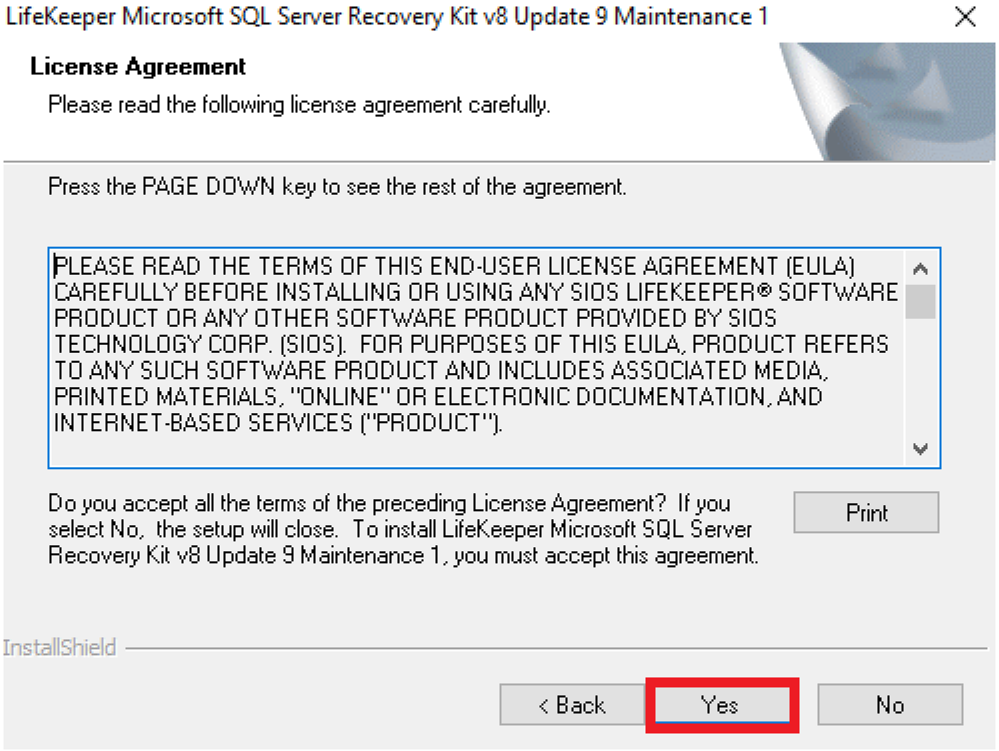


LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1

Welcome to the InstallShield Wizard for LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1

The InstallShield Wizard will install LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1 on your computer. To continue, click Next.

10. Accept License Agreement (again)



LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1

License Agreement

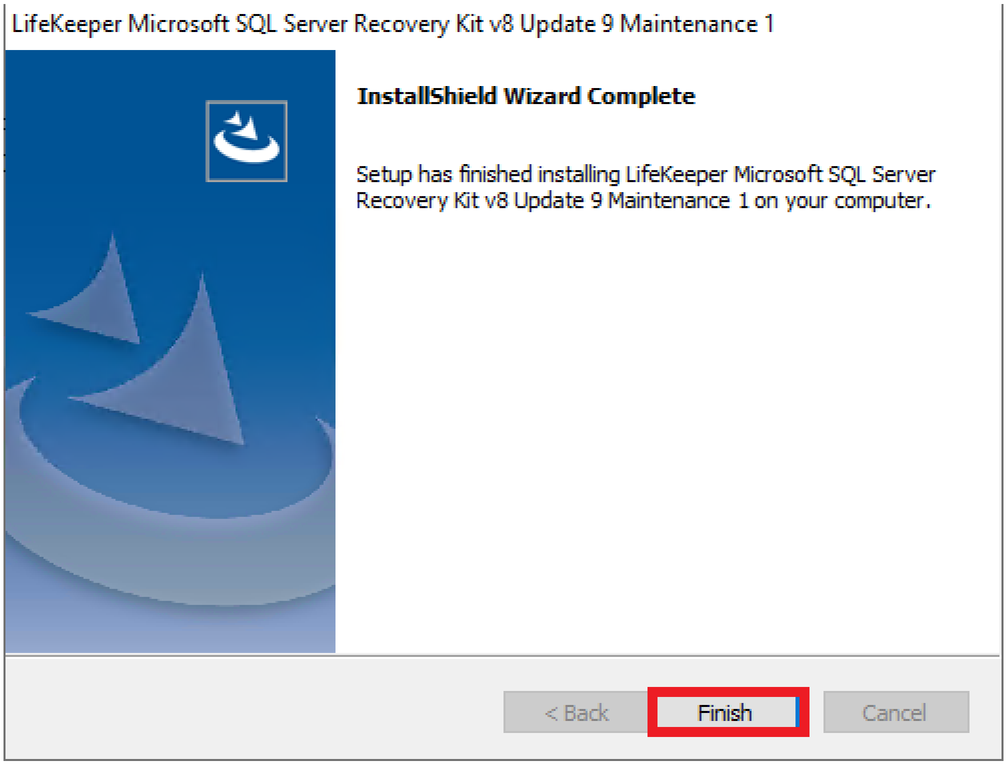
Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

PLEASE READ THE TERMS OF THIS END-USER LICENSE AGREEMENT (EULA) CAREFULLY BEFORE INSTALLING OR USING ANY SIOS LIFEKEEPER® SOFTWARE PRODUCT OR ANY OTHER SOFTWARE PRODUCT PROVIDED BY SIOS TECHNOLOGY CORP. (SIOS). FOR PURPOSES OF THIS EULA, PRODUCT REFERS TO ANY SUCH SOFTWARE PRODUCT AND INCLUDES ASSOCIATED MEDIA, PRINTED MATERIALS, "ONLINE" OR ELECTRONIC DOCUMENTATION, AND INTERNET-BASED SERVICES ("PRODUCT").

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1, you must accept this agreement.

11. Verify Completed Installation of Recovery Kit



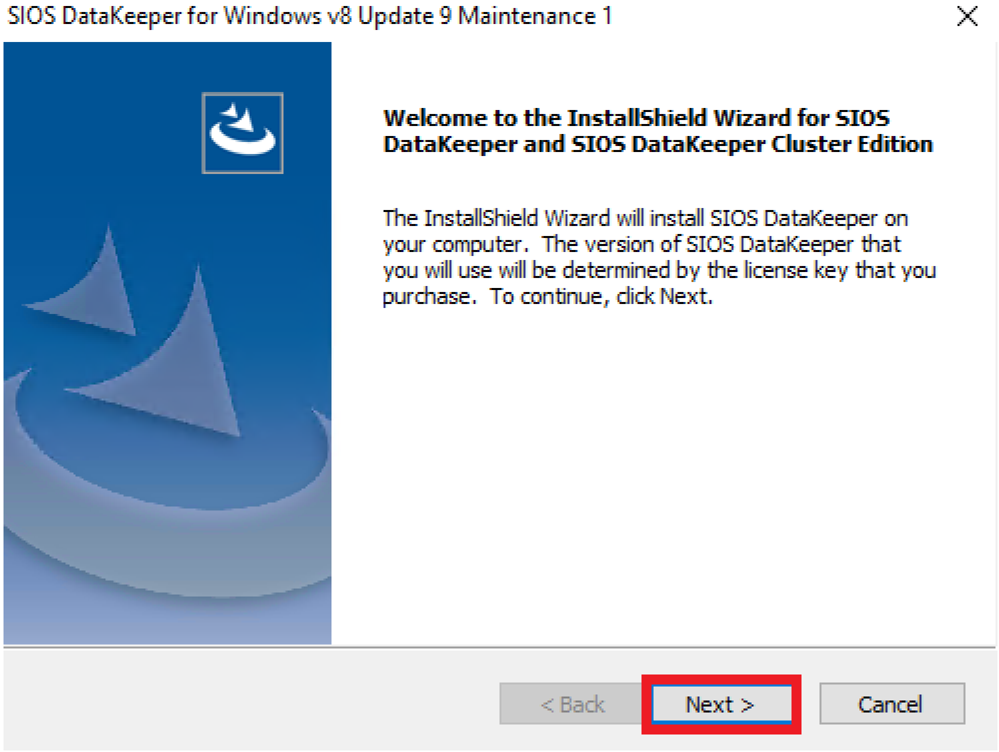
LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1

InstallShield Wizard Complete

Setup has finished installing LifeKeeper Microsoft SQL Server Recovery Kit v8 Update 9 Maintenance 1 on your computer.

12. Install DataKeeper

NOTE: This step will start automatically after the SQL ARK finishes installing.

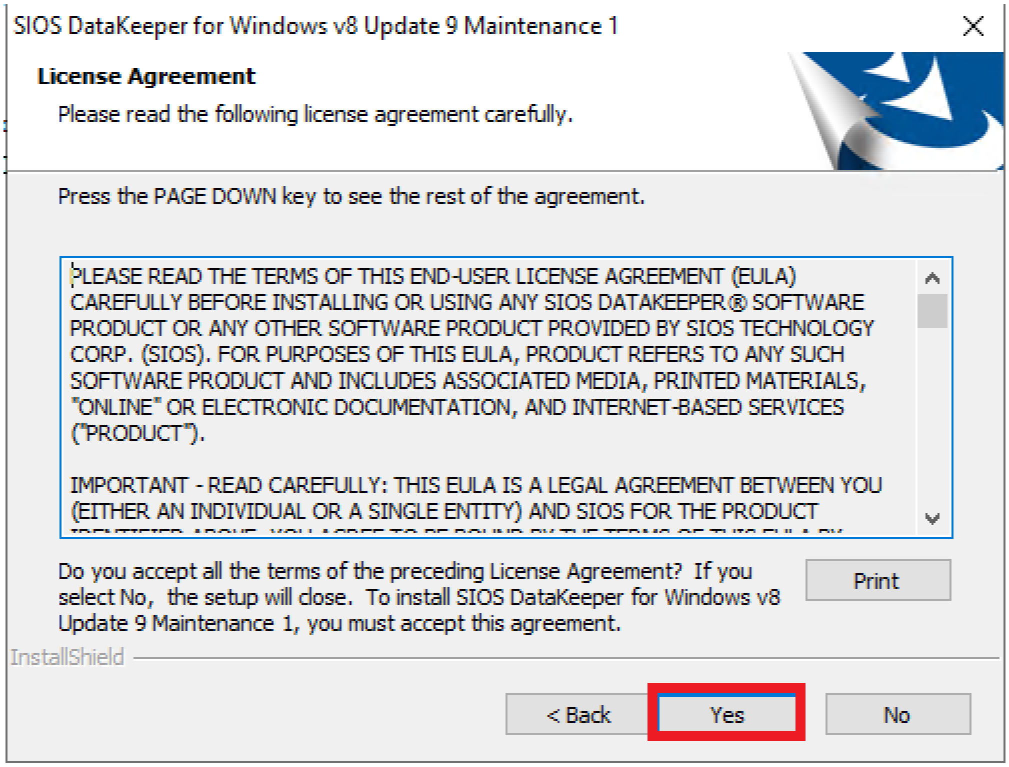


SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

Welcome to the InstallShield Wizard for SIOS DataKeeper and SIOS DataKeeper Cluster Edition

The InstallShield Wizard will install SIOS DataKeeper on your computer. The version of SIOS DataKeeper that you will use will be determined by the license key that you purchase. To continue, click Next.

13. Agree to License Agreement (again)



SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

License Agreement

Please read the following license agreement carefully.

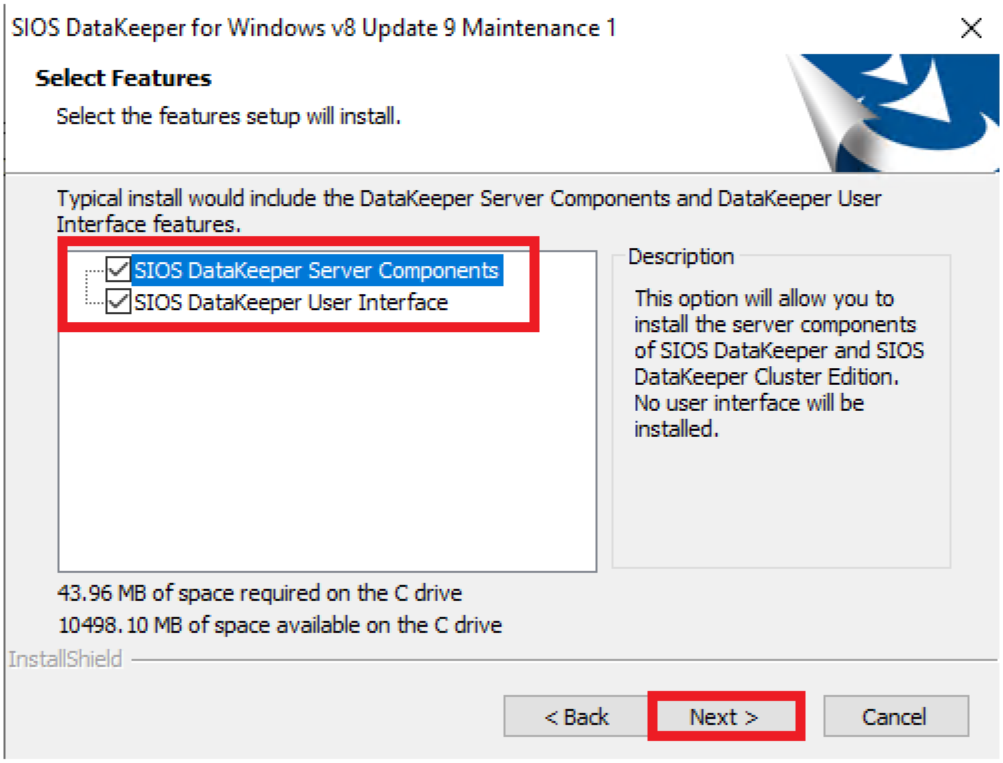
Press the PAGE DOWN key to see the rest of the agreement.

PLEASE READ THE TERMS OF THIS END-USER LICENSE AGREEMENT (EULA) CAREFULLY BEFORE INSTALLING OR USING ANY SIOS DATAKEEPER® SOFTWARE PRODUCT OR ANY OTHER SOFTWARE PRODUCT PROVIDED BY SIOS TECHNOLOGY CORP. (SIOS). FOR PURPOSES OF THIS EULA, PRODUCT REFERS TO ANY SUCH SOFTWARE PRODUCT AND INCLUDES ASSOCIATED MEDIA, PRINTED MATERIALS, "ONLINE" OR ELECTRONIC DOCUMENTATION, AND INTERNET-BASED SERVICES ("PRODUCT").

IMPORTANT - READ CAREFULLY: THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND SIOS FOR THE PRODUCT

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install SIOS DataKeeper for Windows v8 Update 9 Maintenance 1, you must accept this agreement.

14. Select DataKeeper features



SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

Select Features

Select the features setup will install.

Typical install would include the DataKeeper Server Components and DataKeeper User Interface features.

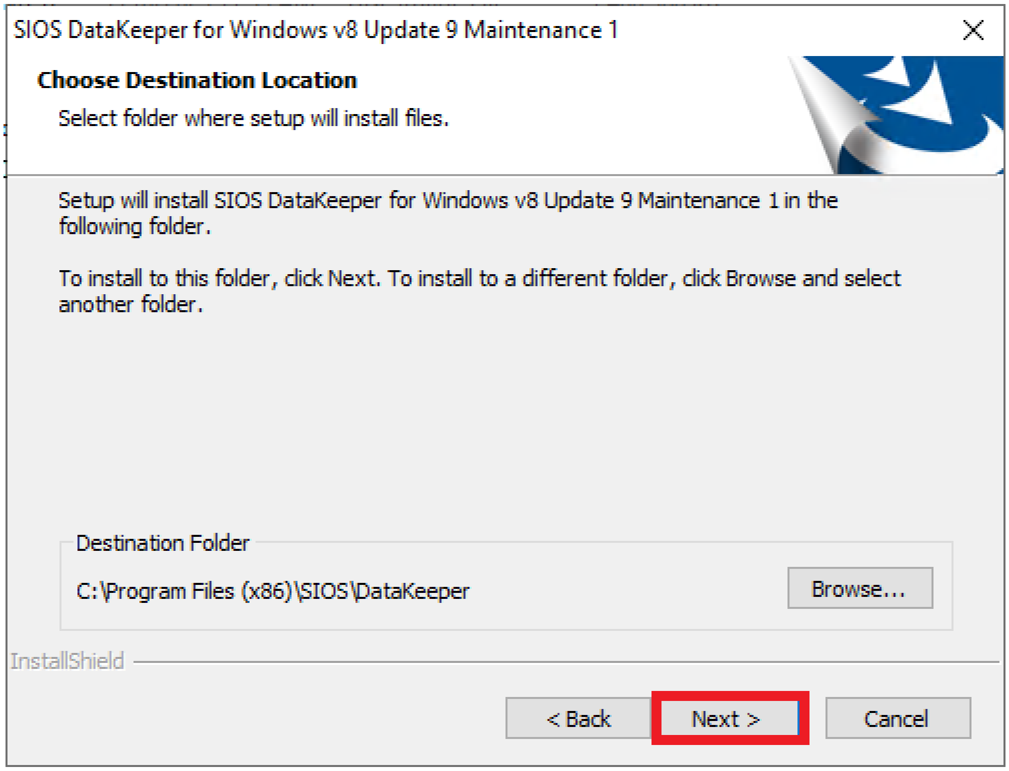
☑ SIOS DataKeeper Server Components
☑ SIOS DataKeeper User Interface

Description

This option will allow you to install the server components of SIOS DataKeeper and SIOS DataKeeper Cluster Edition. No user interface will be installed.

43.96 MB of space required on the C drive
10498.10 MB of space available on the C drive

15. Choose DataKeeper installation location (say yes to all recommendations)



SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

Choose Destination Location

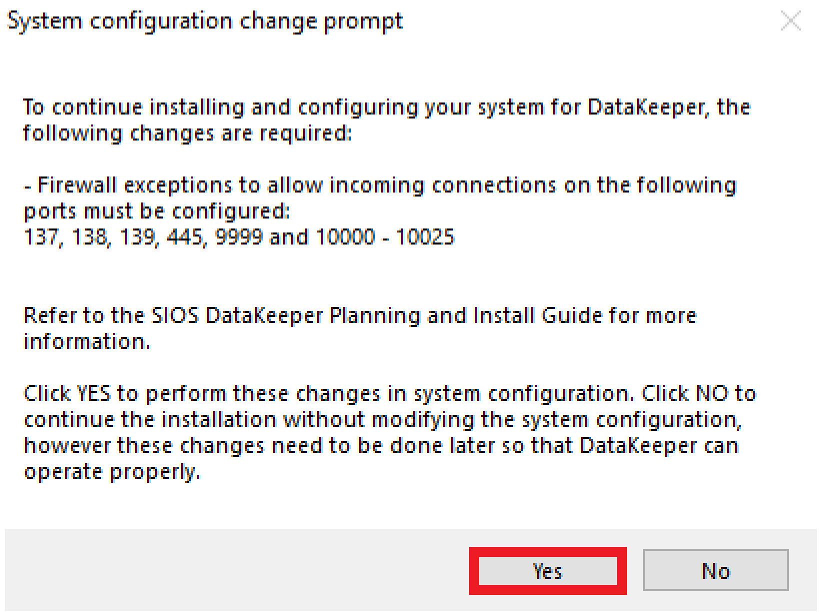
Select folder where setup will install files.

Setup will install SIOS DataKeeper for Windows v8 Update 9 Maintenance 1 in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files (x86)\SIOS\DataKeeper



System configuration change prompt

To continue installing and configuring your system for DataKeeper, the following changes are required:

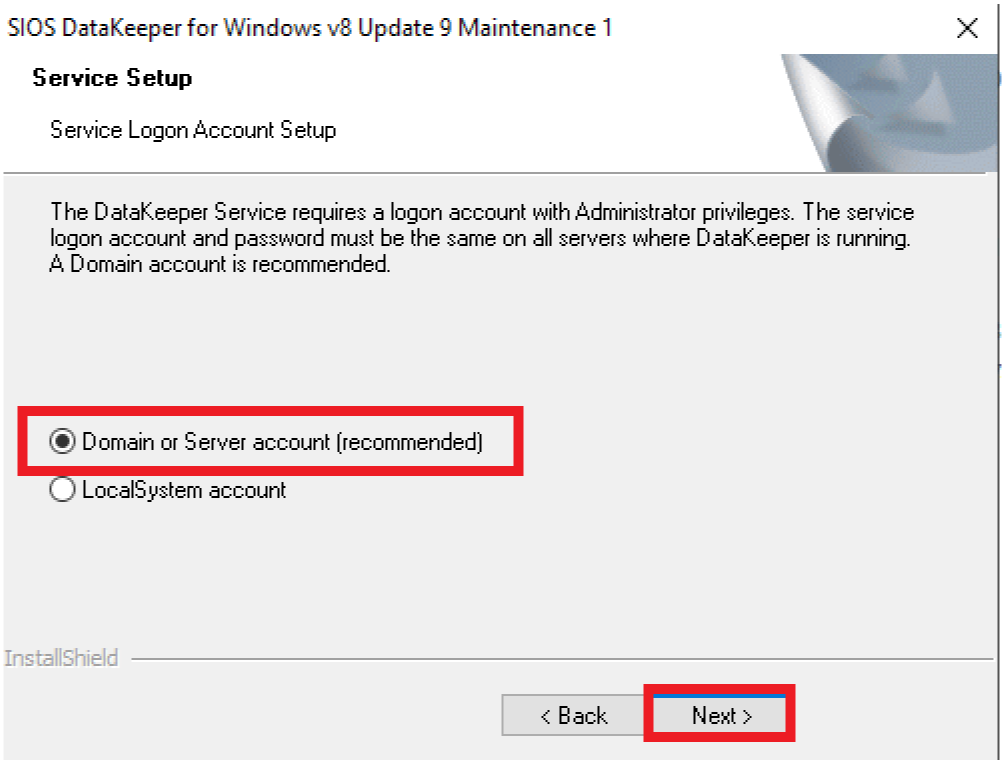
- Firewall exceptions to allow incoming connections on the following ports must be configured:
137, 138, 139, 445, 9999 and 10000 - 10025

Refer to the SIOS DataKeeper Planning and Install Guide for more information.

Click YES to perform these changes in system configuration. Click NO to continue the installation without modifying the system configuration, however these changes need to be done later so that DataKeeper can operate properly.

a.

16. Select Service Account (this should be the one you created earlier that is in the local administrators group on each server)


SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

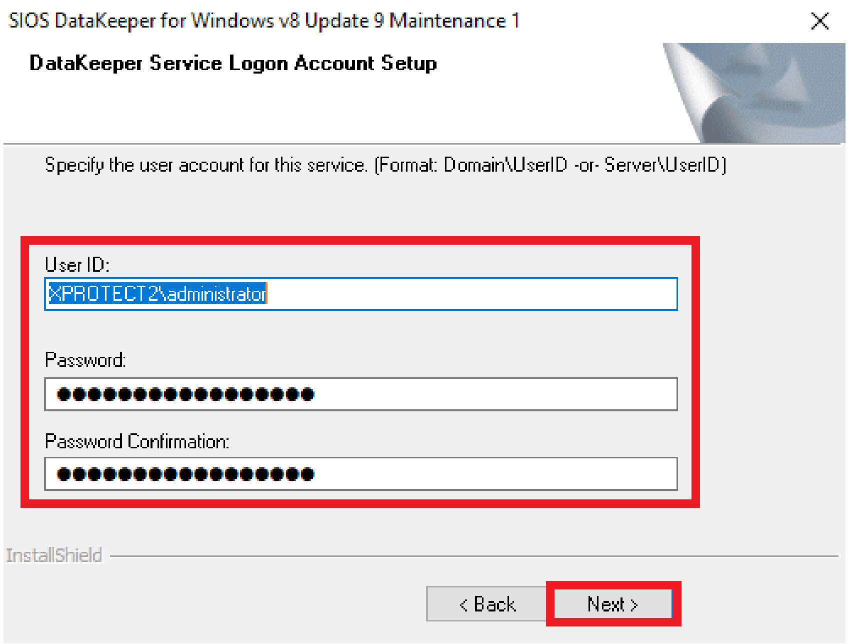
Service Setup

Service Logon Account Setup

The DataKeeper Service requires a logon account with Administrator privileges. The service logon account and password must be the same on all servers where DataKeeper is running. A Domain account is recommended.

● Domain or Server account (recommended)

○ LocalSystem account


SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

DataKeeper Service Logon Account Setup

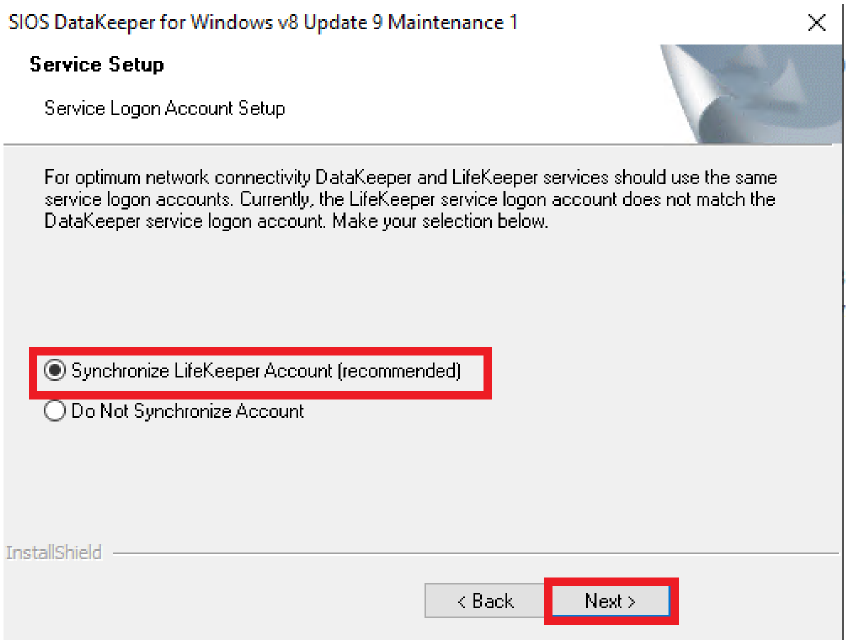
Specify the user account for this service. (Format: Domain\UserID -or- Server\UserID)

User ID: XPROTECT2\administrator

Password: ●●●●●●●●●●●●●●●●●

Password Confirmation: ●●●●●●●●●●●●●●●●●

a.

b. 

SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

Service Setup

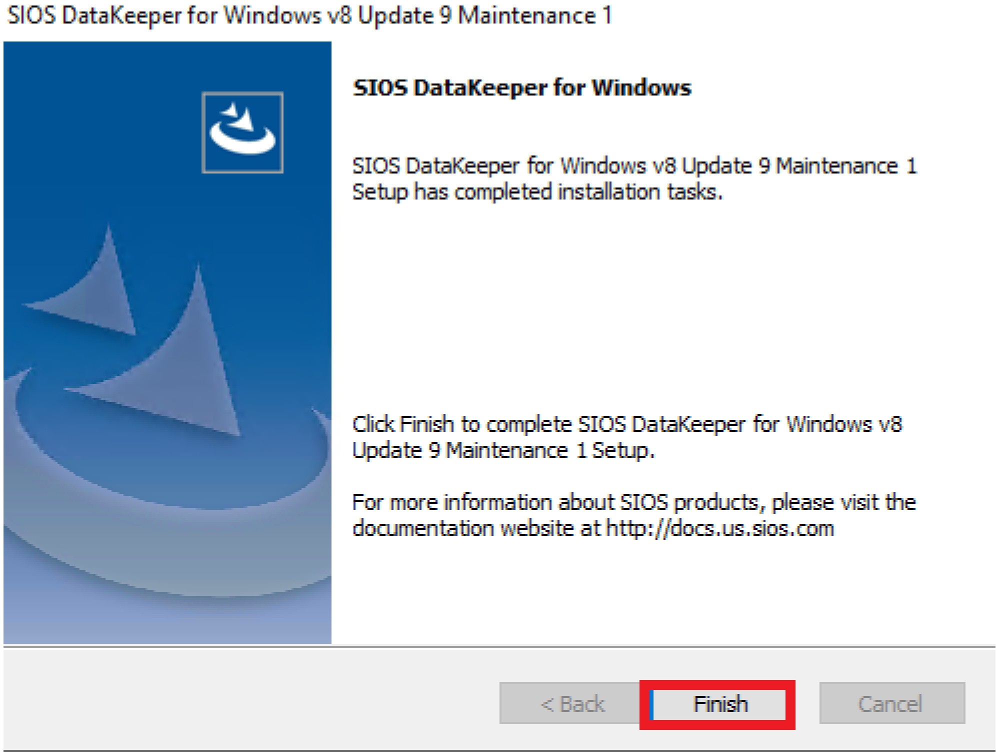
Service Logon Account Setup

For optimum network connectivity DataKeeper and LifeKeeper services should use the same service logon accounts. Currently, the LifeKeeper service logon account does not match the DataKeeper service logon account. Make your selection below.

● Synchronize LifeKeeper Account (recommended)

○ Do Not Synchronize Account

17. Finish Installation



SIOS DataKeeper for Windows v8 Update 9 Maintenance 1

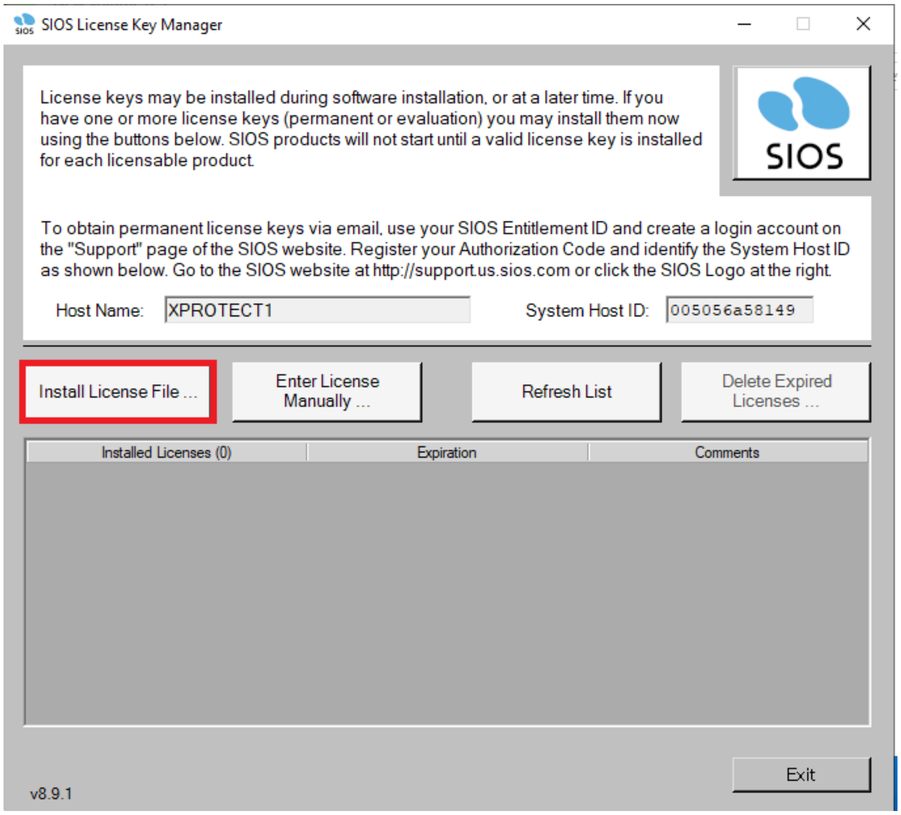
SIOS DataKeeper for Windows

SIOS DataKeeper for Windows v8 Update 9 Maintenance 1 Setup has completed installation tasks.

Click Finish to complete SIOS DataKeeper for Windows v8 Update 9 Maintenance 1 Setup.

For more information about SIOS products, please visit the documentation website at http://docs.us.sios.com

18. Install License file(s)



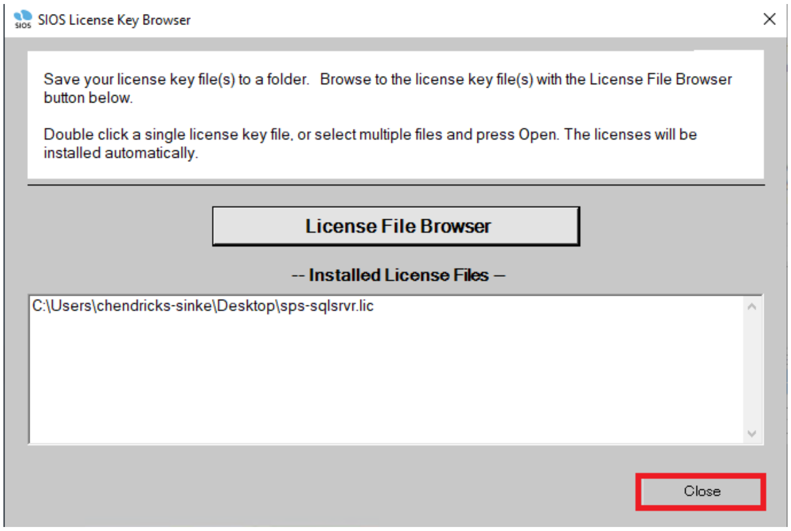
SIOS License Key Manager

License keys may be installed during software installation, or at a later time. If you have one or more license keys (permanent or evaluation) you may install them now using the buttons below. SIOS products will not start until a valid license key is installed for each licensable product.

To obtain permanent license keys via email, use your SIOS Entitlement ID and create a login account on the "Support" page of the SIOS website. Register your Authorization Code and identify the System Host ID as shown below. Go to the SIOS website at http://support.us.sios.com or click the SIOS Logo at the right.

Host Name: XPROTECT1

System Host ID: 005056a58149

a. 

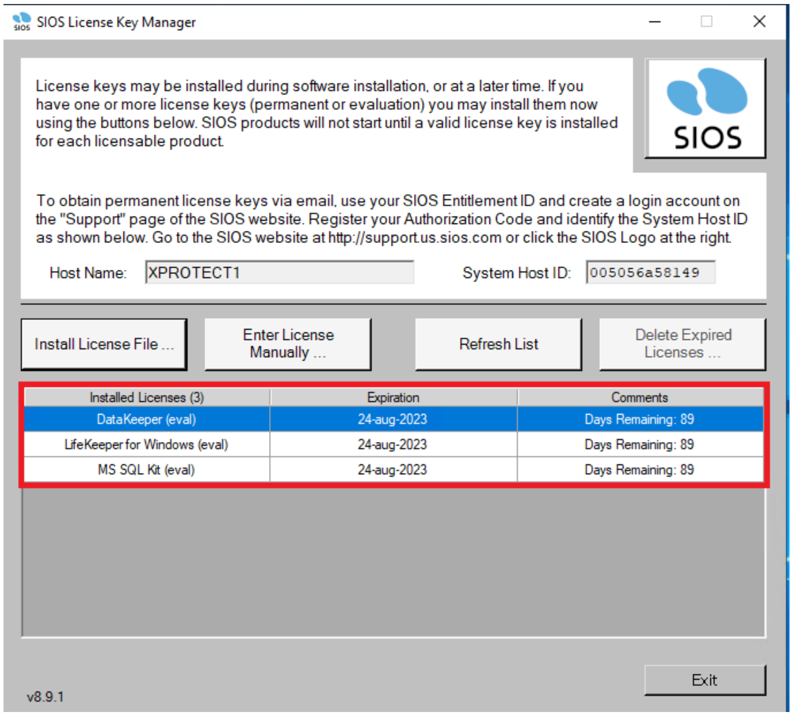
SIOS License Key Browser

Save your license key file(s) to a folder. Browse to the license key file(s) with the License File Browser button below.

Double click a single license key file, or select multiple files and press Open. The licenses will be installed automatically.

-- Installed License Files --

C:\Users\chendricks-sinke\Desktop\sps-sqlsrvr.lic b.



SIOS License Key Manager

License keys may be installed during software installation, or at a later time. If you have one or more license keys (permanent or evaluation) you may install them now using the buttons below. SIOS products will not start until a valid license key is installed for each licensable product.

To obtain permanent license keys via email, use your SIOS Entitlement ID and create a login account on the "Support" page of the SIOS website. Register your Authorization Code and identify the System Host ID as shown below. Go to the SIOS website at http://support.us.sios.com or click the SIOS Logo at the right.

Host Name: XPROTECT1

System Host ID: 005056a58149

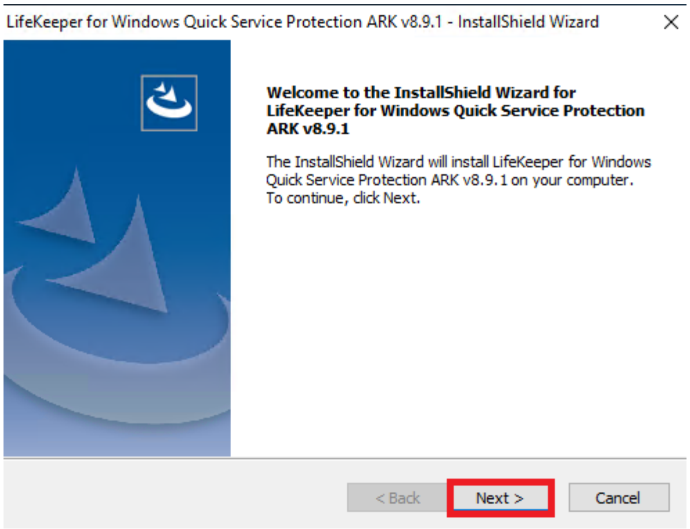
Installed Licenses (3)	Expiration	Comments
DataKeeper (eval)	24-aug-2023	Days Remaining: 89
LifeKeeper for Windows (eval)	24-aug-2023	Days Remaining: 89
MS SQL Kit (eval)	24-aug-2023	Days Remaining: 89

v8.9.1

Install the Quick Service Protection (QSP) Recovery Kit:

NOTE: If you do not have the QSP installer, the installer and relevant documentation for the QSP Recovery Kit can be found **HERE**

1. Run installer

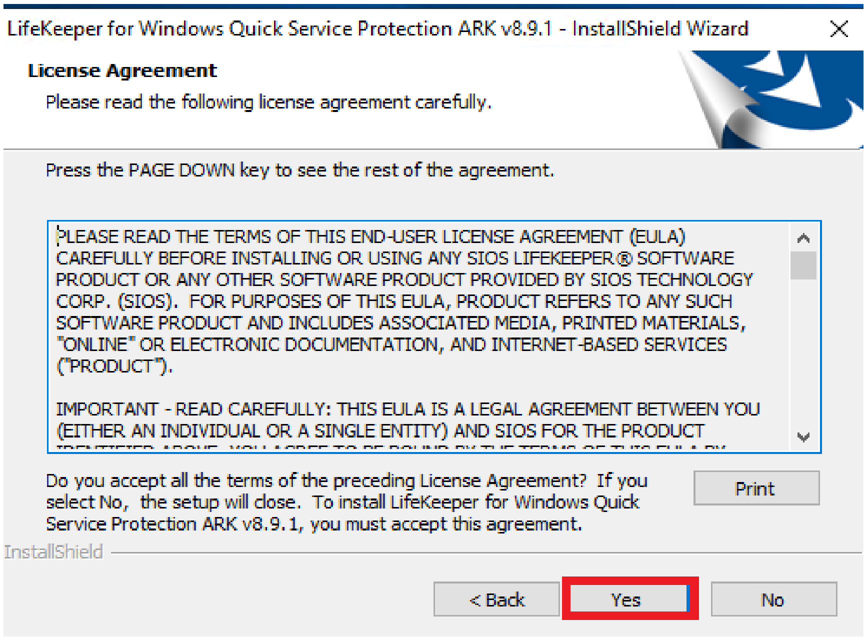


LifeKeeper for Windows Quick Service Protection ARK v8.9.1 - InstallShield Wizard

Welcome to the InstallShield Wizard for LifeKeeper for Windows Quick Service Protection ARK v8.9.1

The InstallShield Wizard will install LifeKeeper for Windows Quick Service Protection ARK v8.9.1 on your computer. To continue, click Next.

2. Agree to License Agreement



LifeKeeper for Windows Quick Service Protection ARK v8.9.1 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

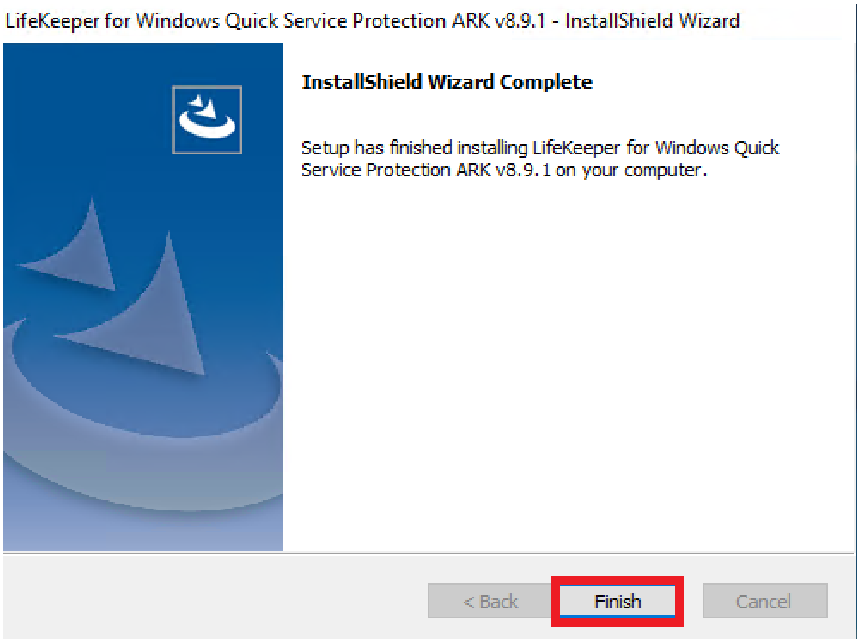
Press the PAGE DOWN key to see the rest of the agreement.

PLEASE READ THE TERMS OF THIS END-USER LICENSE AGREEMENT (EULA) CAREFULLY BEFORE INSTALLING OR USING ANY SIOS LIFEKEEPER® SOFTWARE PRODUCT OR ANY OTHER SOFTWARE PRODUCT PROVIDED BY SIOS TECHNOLOGY CORP. (SIOS). FOR PURPOSES OF THIS EULA, PRODUCT REFERS TO ANY SUCH SOFTWARE PRODUCT AND INCLUDES ASSOCIATED MEDIA, PRINTED MATERIALS, "ONLINE" OR ELECTRONIC DOCUMENTATION, AND INTERNET-BASED SERVICES ("PRODUCT").

IMPORTANT - READ CAREFULLY: THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND SIOS FOR THE PRODUCT

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install LifeKeeper for Windows Quick Service Protection ARK v8.9.1, you must accept this agreement.

3. Verify install and restart LifeKeeper



LifeKeeper for Windows Quick Service Protection ARK v8.9.1 - InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing LifeKeeper for Windows Quick Service Protection ARK v8.9.1 on your computer.

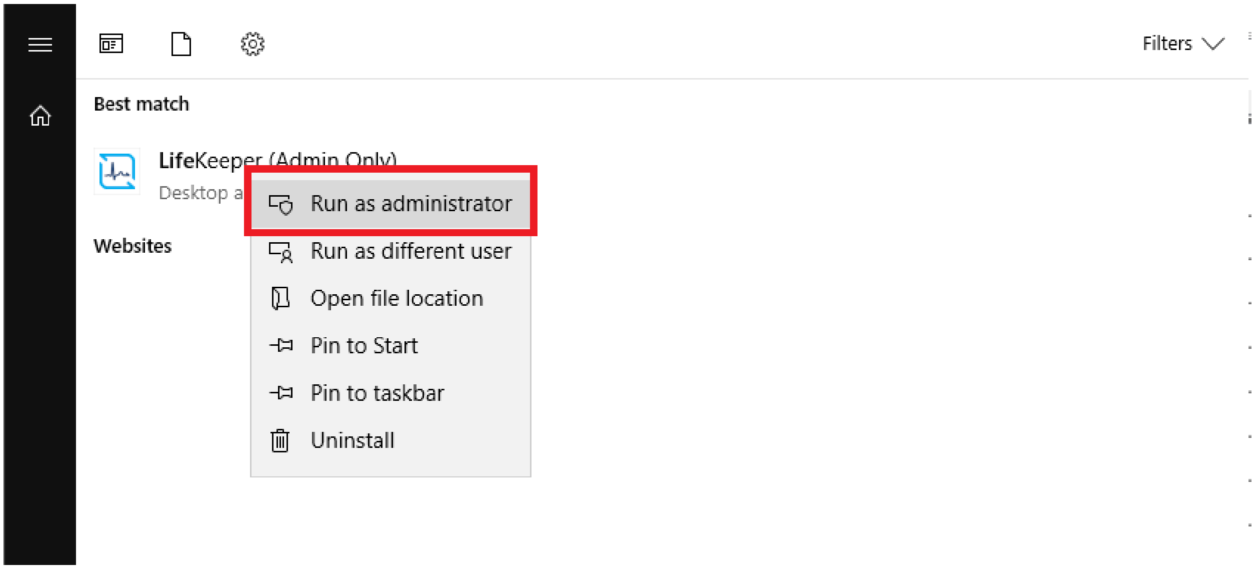
4. Repeats steps 1-3 on XPROTECT2

Step 4 - Create the LifeKeeper Core Cluster Resources

Now that we have installed SIOS software, it's time to configure the resources needed for the cluster via LifeKeeper

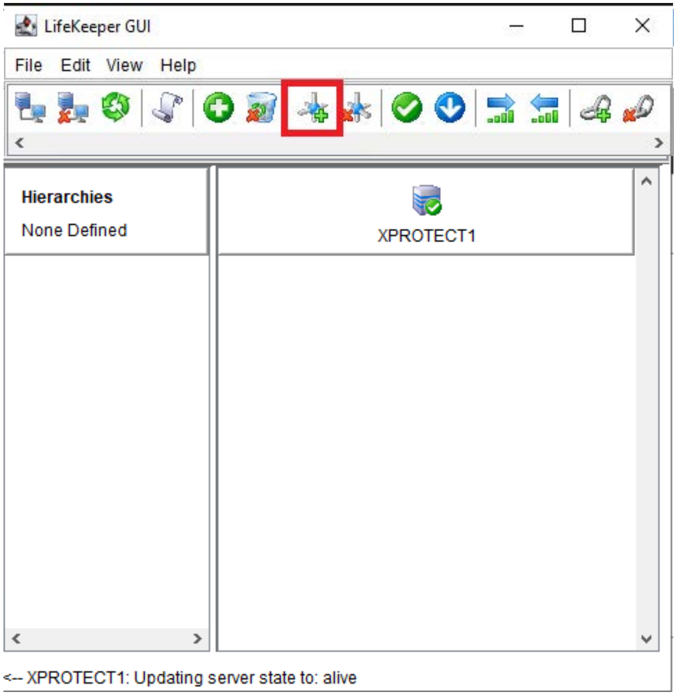
Open LikeKeeper GUI:

1. From the Windows bar search for LifeKeeper, right click and run as administrator



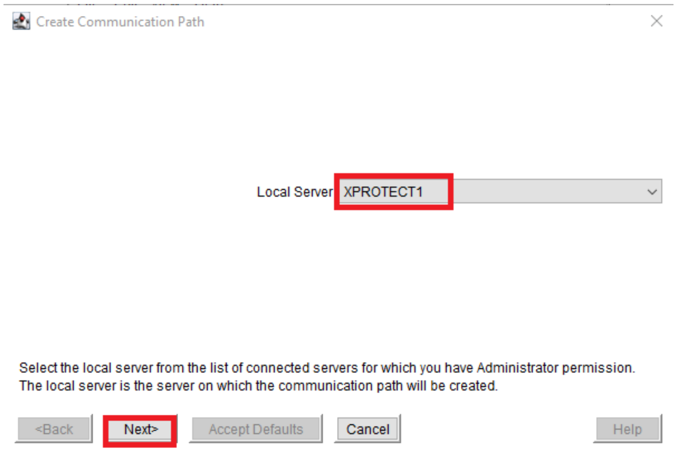
Create Comm Path(s):

1. Click create path button



<-- XPROTECT1: Updating server state to: alive

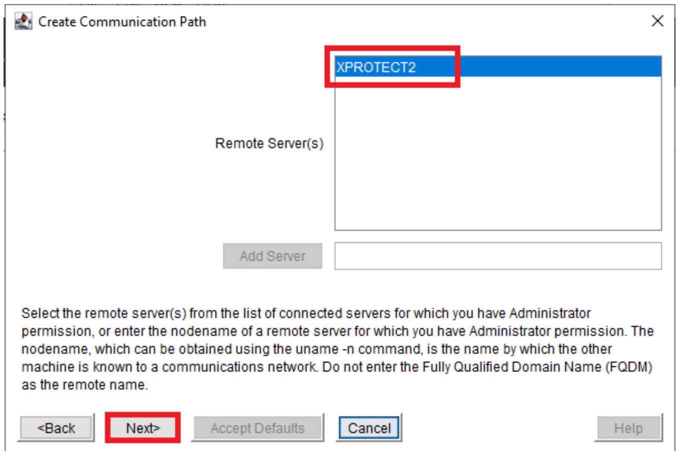
2. Choose local server



Local Server XPROTECT1

Select the local server from the list of connected servers for which you have Administrator permission.
The local server is the server on which the communication path will be created.

3. Choose remote server

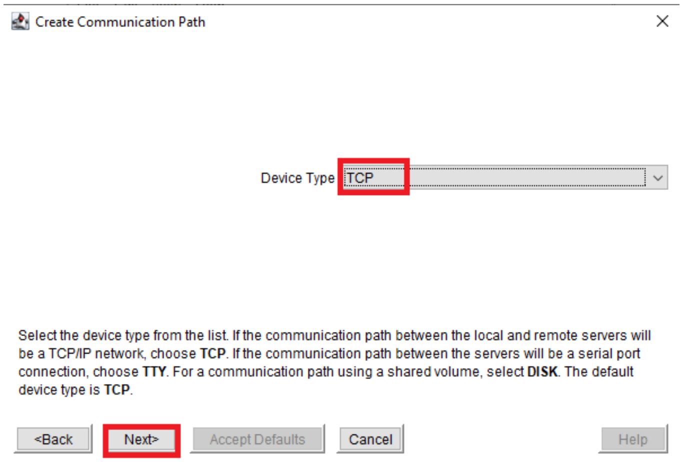


Create Communication Path

Remote Server(s): XPROTECT2

Select the remote server(s) from the list of connected servers for which you have Administrator permission, or enter the nodename of a remote server for which you have Administrator permission. The nodename, which can be obtained using the uname -n command, is the name by which the other machine is known to a communications network. Do not enter the Fully Qualified Domain Name (FQDM) as the remote name.

4. Set device type

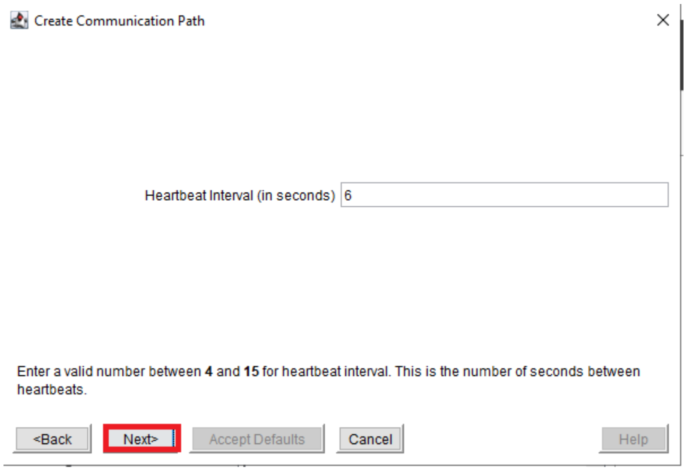


Create Communication Path

Device Type: TCP

Select the device type from the list. If the communication path between the local and remote servers will be a TCP/IP network, choose **TCP**. If the communication path between the servers will be a serial port connection, choose **TTY**. For a communication path using a shared volume, select **DISK**. The default device type is **TCP**.

5. Use default Heartbeat Interval

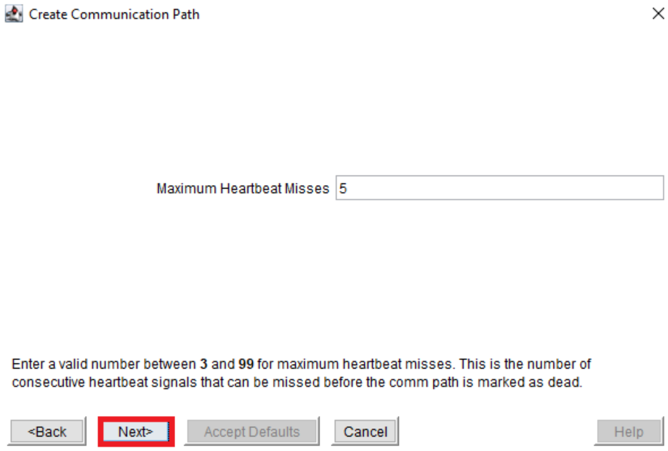


Create Communication Path

Heartbeat Interval (in seconds): 6

Enter a valid number between **4** and **15** for heartbeat interval. This is the number of seconds between heartbeats.

6. Use default Maximum Heartbeat Misses

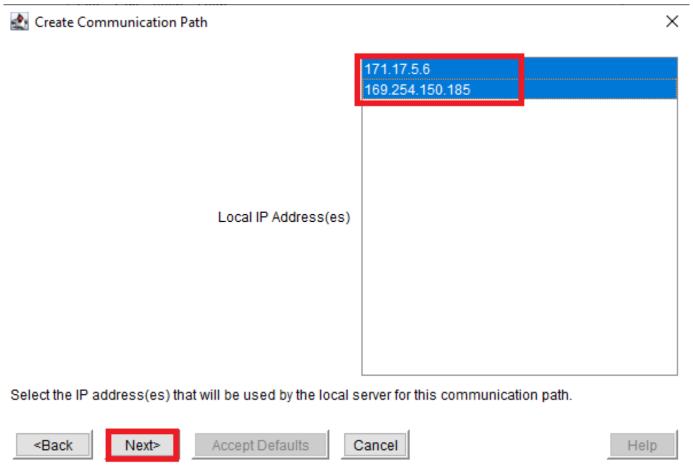


Create Communication Path

Maximum Heartbeat Misses 5

Enter a valid number between **3** and **99** for maximum heartbeat misses. This is the number of consecutive heartbeat signals that can be missed before the comm path is marked as dead.

7. Choose both local IP addresses for redundant comm paths



Create Communication Path

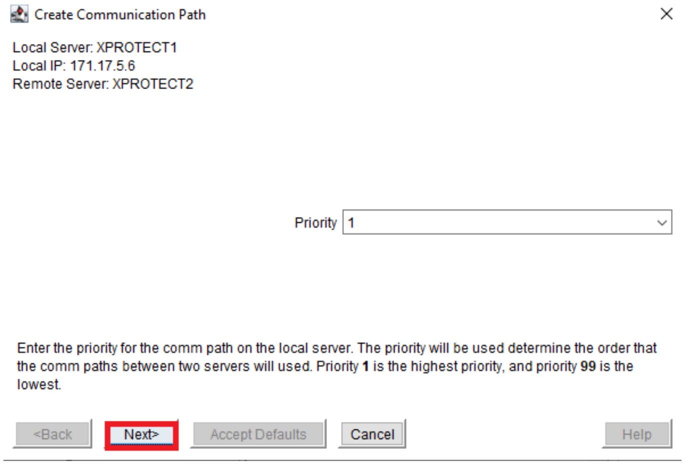
Local IP Address(es)

171.17.5.6

169.254.150.185

Select the IP address(es) that will be used by the local server for this communication path.

8. Choose default priority



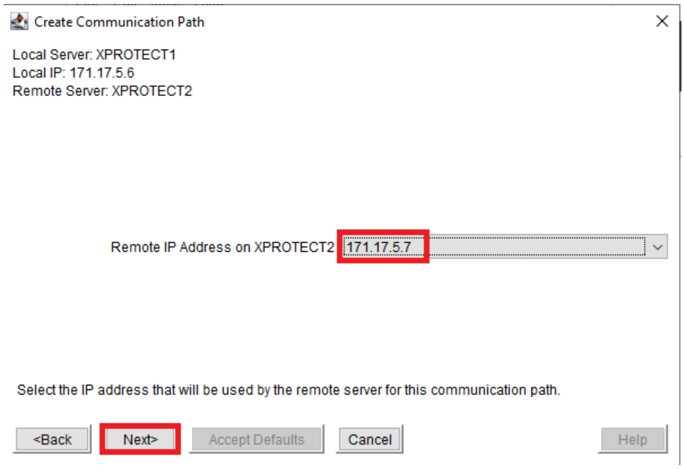
Create Communication Path

Local Server: XPROTECT1
Local IP: 171.17.5.6
Remote Server: XPROTECT2

Priority 1

Enter the priority for the comm path on the local server. The priority will be used determine the order that the comm paths between two servers will used. Priority **1** is the highest priority, and priority **99** is the lowest.

9. Select Remote IP Address for XPROTECT2



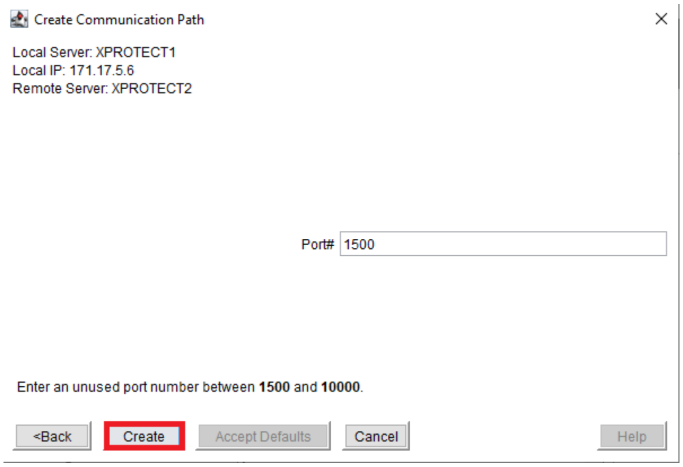
Create Communication Path

Local Server: XPROTECT1
Local IP: 171.17.5.6
Remote Server: XPROTECT2

Remote IP Address on XPROTECT2 171.17.5.7

Select the IP address that will be used by the remote server for this communication path.

10. Choose default port



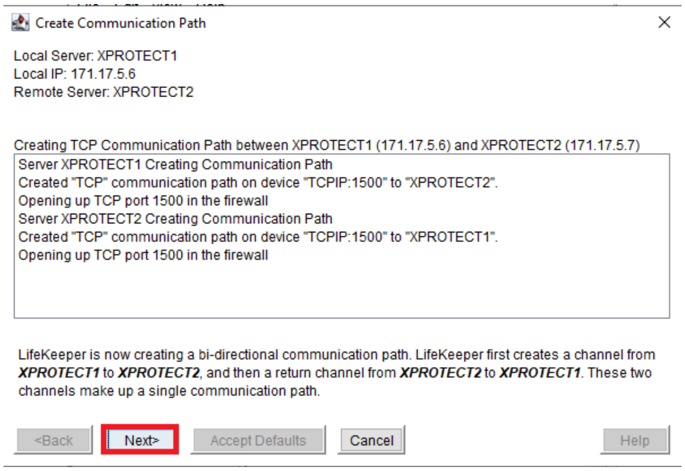
Create Communication Path

Local Server: XPROTECT1
Local IP: 171.17.5.6
Remote Server: XPROTECT2

Port# 1500

Enter an unused port number between **1500** and **10000**.

11. Create communication path



Create Communication Path

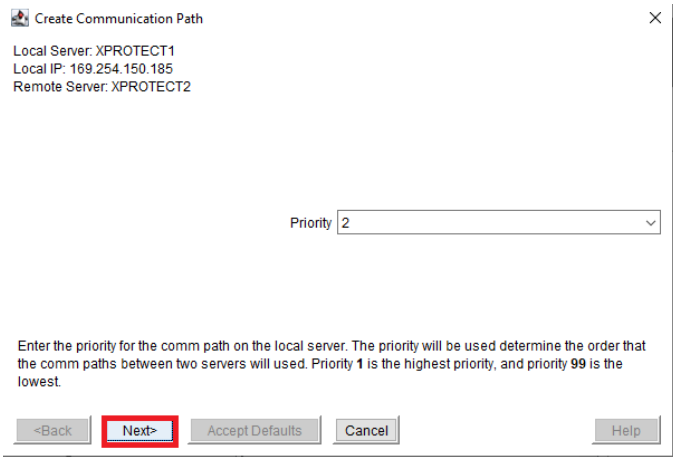
Local Server: XPROTECT1
Local IP: 171.17.5.6
Remote Server: XPROTECT2

Creating TCP Communication Path between XPROTECT1 (171.17.5.6) and XPROTECT2 (171.17.5.7)

```
Server XPROTECT1 Creating Communication Path
Created "TCP" communication path on device "TCPIP:1500" to "XPROTECT2".
Opening up TCP port 1500 in the firewall
Server XPROTECT2 Creating Communication Path
Created "TCP" communication path on device "TCPIP:1500" to "XPROTECT1".
Opening up TCP port 1500 in the firewall
```

LifeKeeper is now creating a bi-directional communication path. LifeKeeper first creates a channel from ***XPROTECT1*** to ***XPROTECT2***, and then a return channel from ***XPROTECT2*** to ***XPROTECT1***. These two channels make up a single communication path.

12. Use default priority



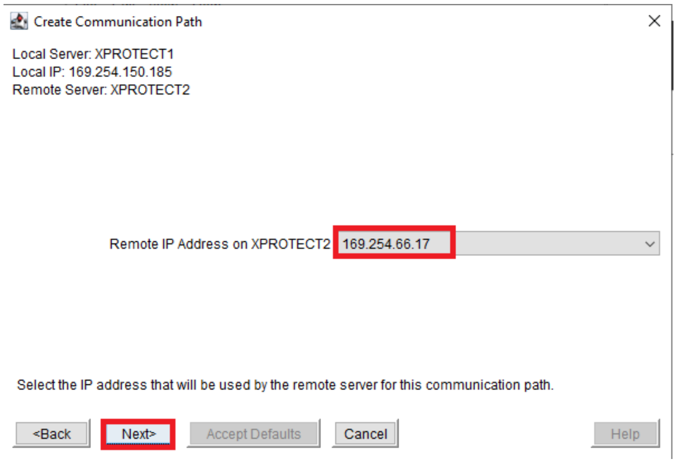
Create Communication Path

Local Server: XPROTECT1
Local IP: 169.254.150.185
Remote Server: XPROTECT2

Priority 2

Enter the priority for the comm path on the local server. The priority will be used determine the order that the comm paths between two servers will used. Priority **1** is the highest priority, and priority **99** is the lowest.

13. Select secondary Remote IP Address for XPROTECT2



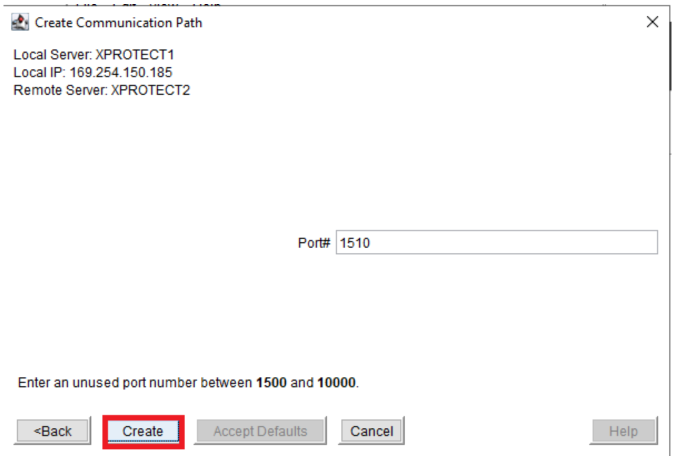
Create Communication Path

Local Server: XPROTECT1
Local IP: 169.254.150.185
Remote Server: XPROTECT2

Remote IP Address on XPROTECT2 169.254.66.17

Select the IP address that will be used by the remote server for this communication path.

14. Use default port for secondary comm path



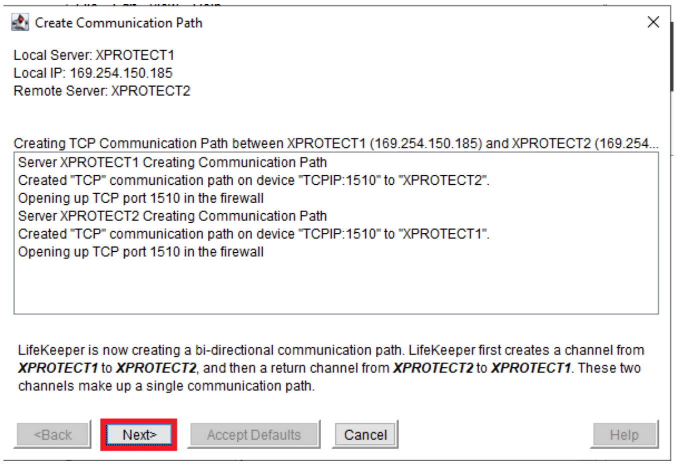
Create Communication Path

Local Server: XPROTECT1
Local IP: 169.254.150.185
Remote Server: XPROTECT2

Port# 1510

Enter an unused port number between **1500** and **10000**.

15. Verify communication path(s) creation was successful



Create Communication Path

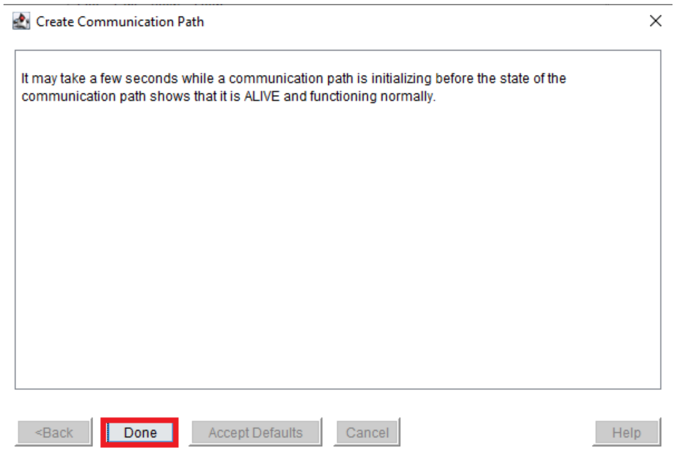
Local Server: XPROTECT1
Local IP: 169.254.150.185
Remote Server: XPROTECT2

Creating TCP Communication Path between XPROTECT1 (169.254.150.185) and XPROTECT2 (169.254...

```
Server XPROTECT1 Creating Communication Path
Created "TCP" communication path on device "TCPIP:1510" to "XPROTECT2".
Opening up TCP port 1510 in the firewall
Server XPROTECT2 Creating Communication Path
Created "TCP" communication path on device "TCPIP:1510" to "XPROTECT1".
Opening up TCP port 1510 in the firewall
```

LifeKeeper is now creating a bi-directional communication path. LifeKeeper first creates a channel from ***XPROTECT1*** to ***XPROTECT2***, and then a return channel from ***XPROTECT2*** to ***XPROTECT1***. These two channels make up a single communication path.

16. Initialize communication path(s)

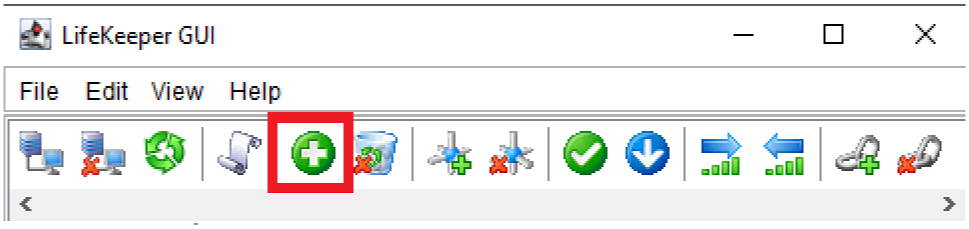


Create Communication Path

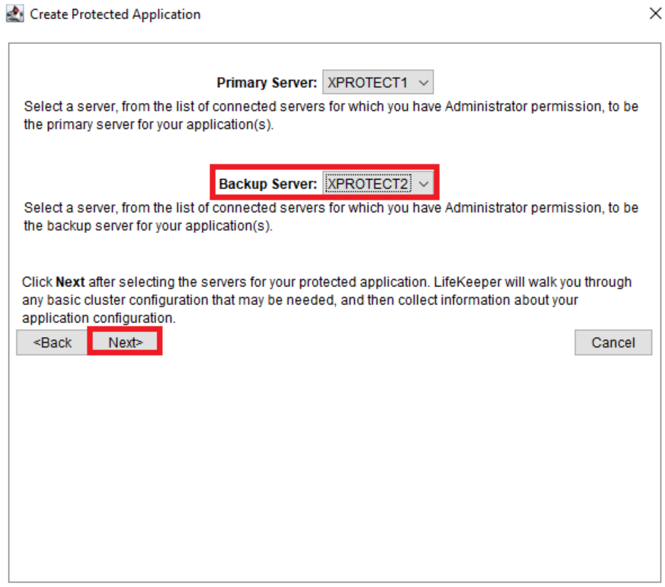
It may take a few seconds while a communication path is initializing before the state of the communication path shows that it is ALIVE and functioning normally.

Create IP Resource:

1. Choose create new resource



2. Choose Primary and Backup Server



Primary Server: XPROTECT1

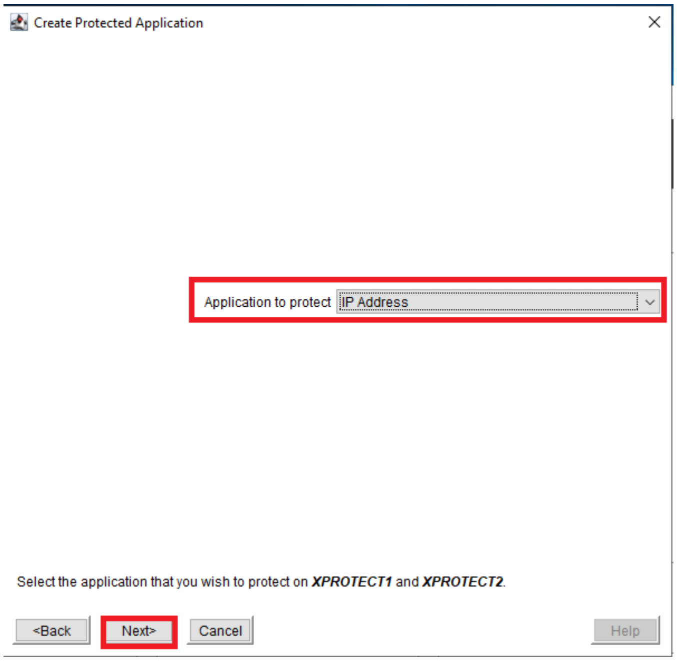
Select a server, from the list of connected servers for which you have Administrator permission, to be the primary server for your application(s).

Backup Server: XPROTECT2

Select a server, from the list of connected servers for which you have Administrator permission, to be the backup server for your application(s).

Click **Next** after selecting the servers for your protected application. LifeKeeper will walk you through any basic cluster configuration that may be needed, and then collect information about your application configuration.

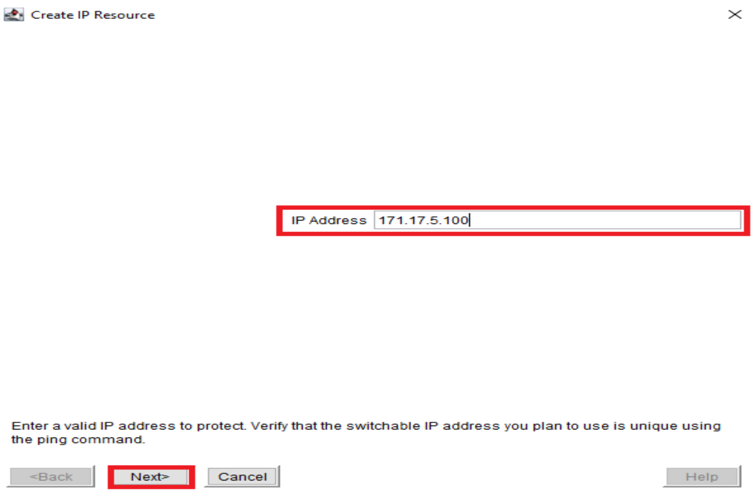
3. Choose IP Address



Application to protect: IP Address

Select the application that you wish to protect on ***XPROTECT1*** and ***XPROTECT2***.

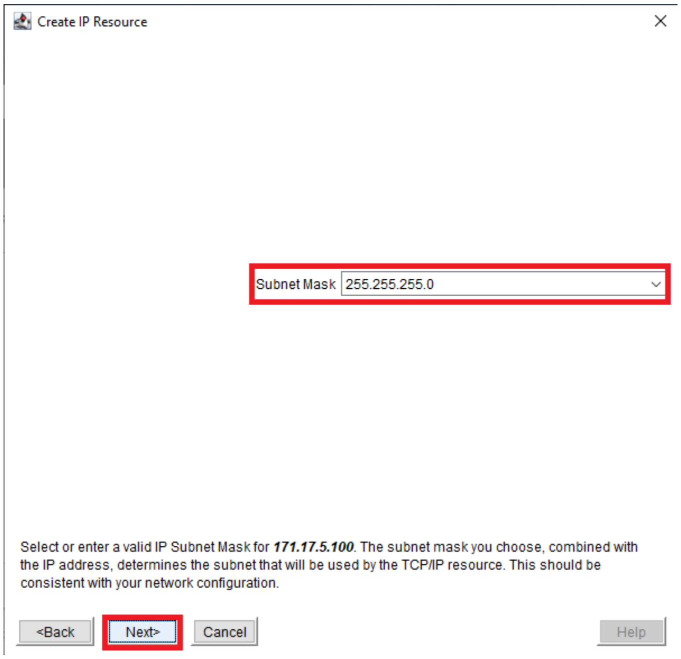
4. Type in the IP you want to use for client connections to the cluster. This is commonly called the virtual IP address.. This address can be any available address on your Public subnet and should not be in use anywhere else.



IP Address 171.17.5.100

Enter a valid IP address to protect. Verify that the switchable IP address you plan to use is unique using the ping command.

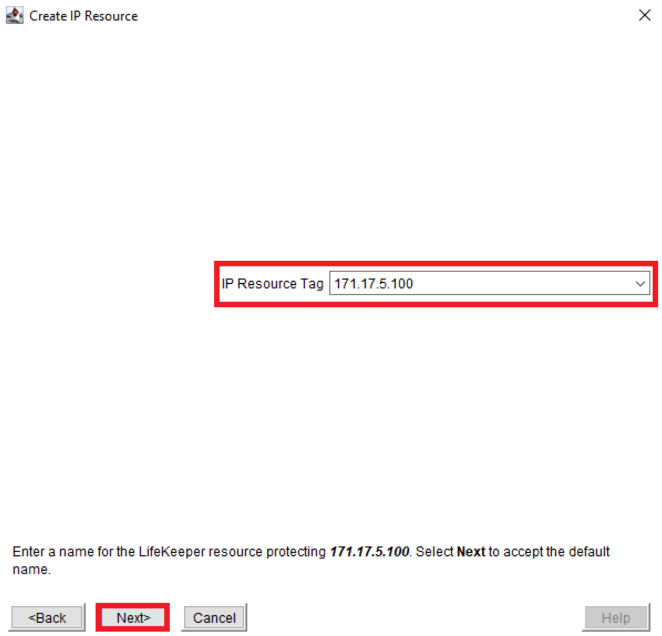
5. Set the Subnet Mask



Subnet Mask 255.255.255.0

Select or enter a valid IP Subnet Mask for ***171.17.5.100***. The subnet mask you choose, combined with the IP address, determines the subnet that will be used by the TCP/IP resource. This should be consistent with your network configuration.

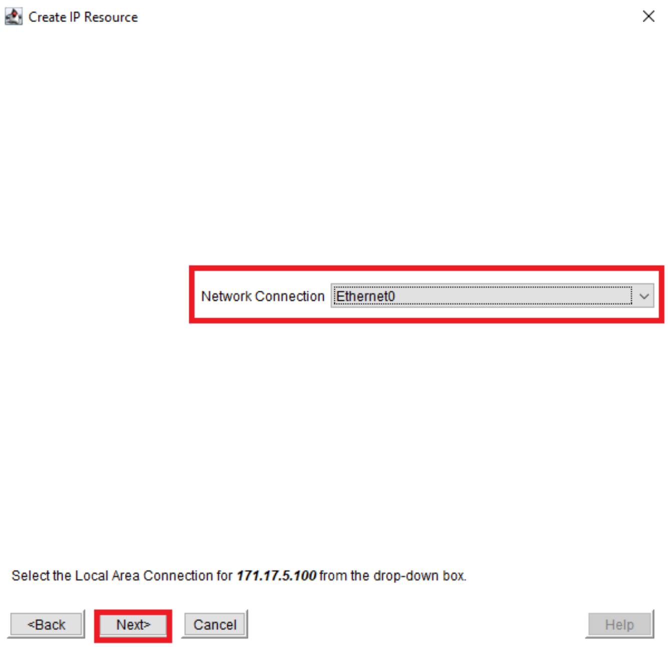
6. Choose a tag for the resource


Create IP Resource

IP Resource Tag 171.17.5.100

Enter a name for the LifeKeeper resource protecting ***171.17.5.100***. Select **Next** to accept the default name.

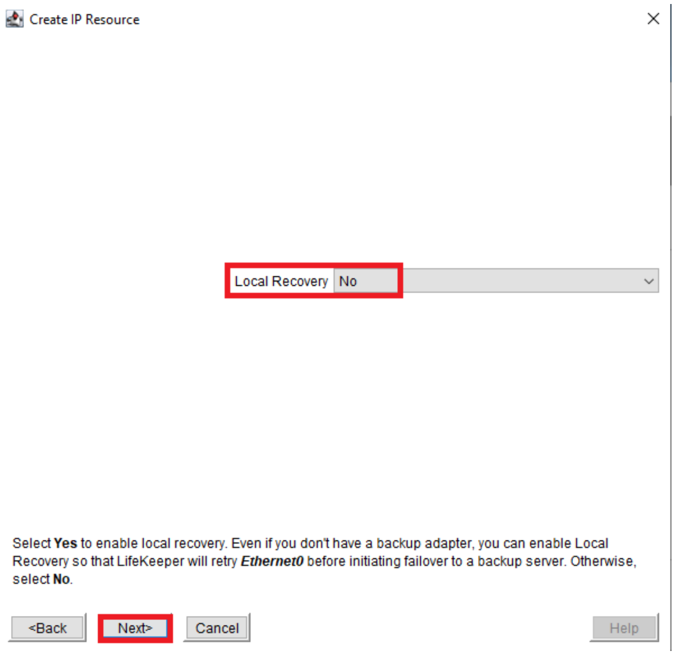
7. Choose the Network Connection


Create IP Resource

Network Connection Ethernet0

Select the Local Area Connection for ***171.17.5.100*** from the drop-down box.

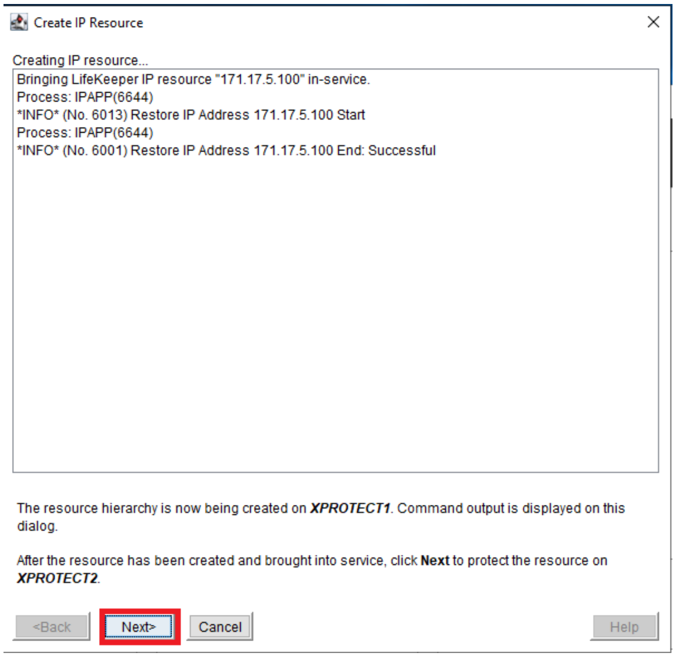
8. Turn off local recovery



Local Recovery: No

Select **Yes** to enable local recovery. Even if you don't have a backup adapter, you can enable Local Recovery so that LifeKeeper will retry ***Ethernet0*** before initiating failover to a backup server. Otherwise, select **No**.

9. Verify the IP resource was created successfully



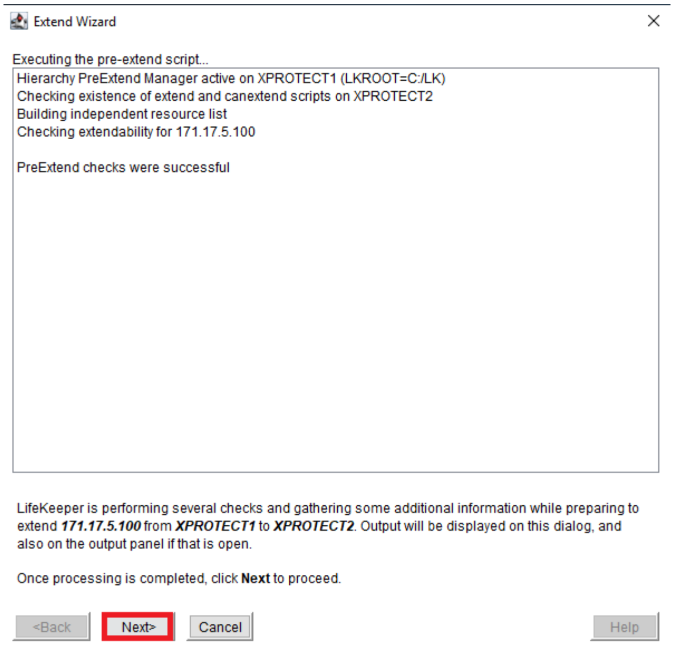
Creating IP resource...

```
Bringing LifeKeeper IP resource "171.17.5.100" in-service.
Process: IPAPP(6644)
*INFO* (No. 6013) Restore IP Address 171.17.5.100 Start
Process: IPAPP(6644)
*INFO* (No. 6001) Restore IP Address 171.17.5.100 End: Successful
```

The resource hierarchy is now being created on ***XPROTECT1***. Command output is displayed on this dialog.

After the resource has been created and brought into service, click **Next** to protect the resource on ***XPROTECT2***.

10. Run the extend checks and verify that they were successful



Extend Wizard

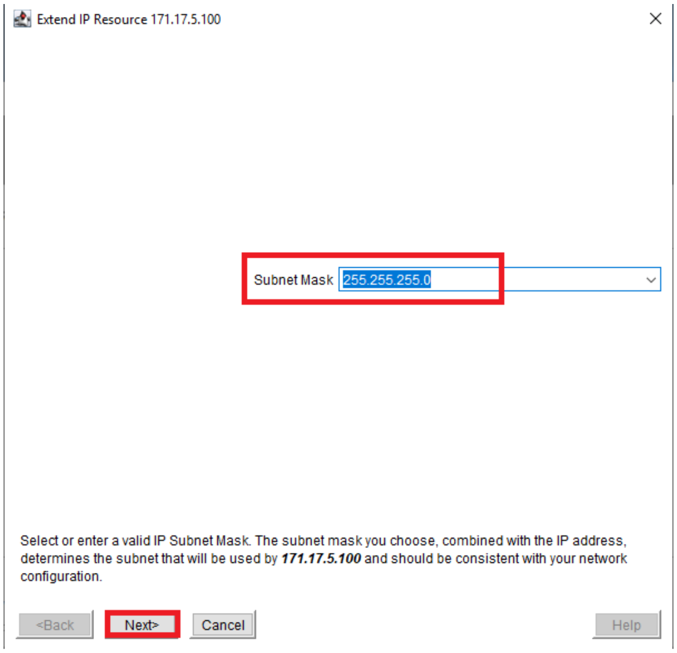
Executing the pre-extend script...

```
Hierarchy PreExtend Manager active on XPROTECT1 (LKROOT=C:/LK)
Checking existence of extend and canextend scripts on XPROTECT2
Building independent resource list
Checking extendability for 171.17.5.100

PreExtend checks were successful
```

LifeKeeper is performing several checks and gathering some additional information while preparing to extend ***171.17.5.100*** from ***XPROTECT1*** to ***XPROTECT2***. Output will be displayed on this dialog, and also on the output panel if that is open.

Once processing is completed, click **Next** to proceed.

11. Choose the Subnet Mask for the extension

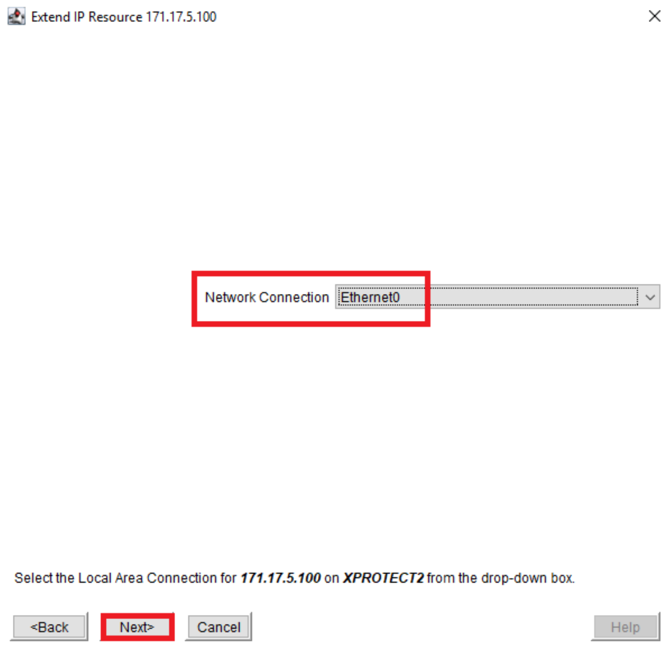


Extend IP Resource 171.17.5.100

Subnet Mask 255.255.255.0

Select or enter a valid IP Subnet Mask. The subnet mask you choose, combined with the IP address, determines the subnet that will be used by ***171.17.5.100*** and should be consistent with your network configuration.

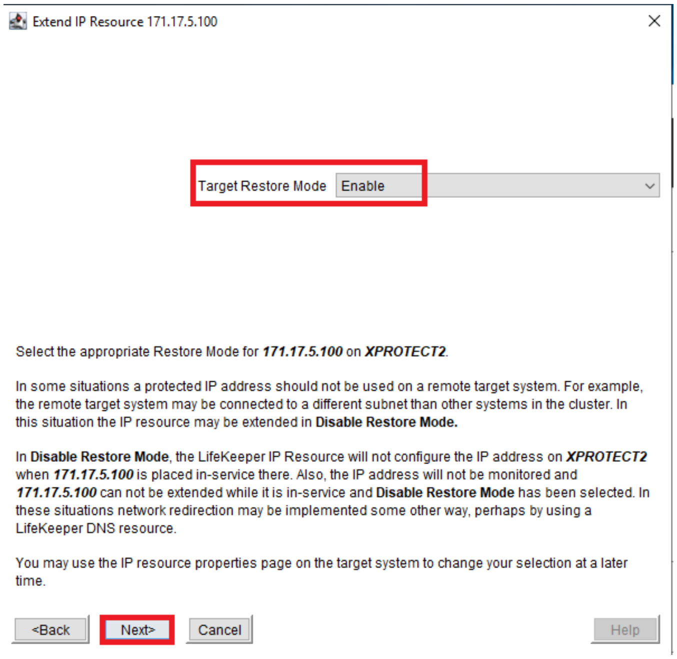
12. Choose the Network Connection for the extend



Network Connection Ethernet0

Select the Local Area Connection for ***171.17.5.100*** on ***XPROTECT2*** from the drop-down box.

13. Enable Target Restore Mode



Target Restore Mode Enable

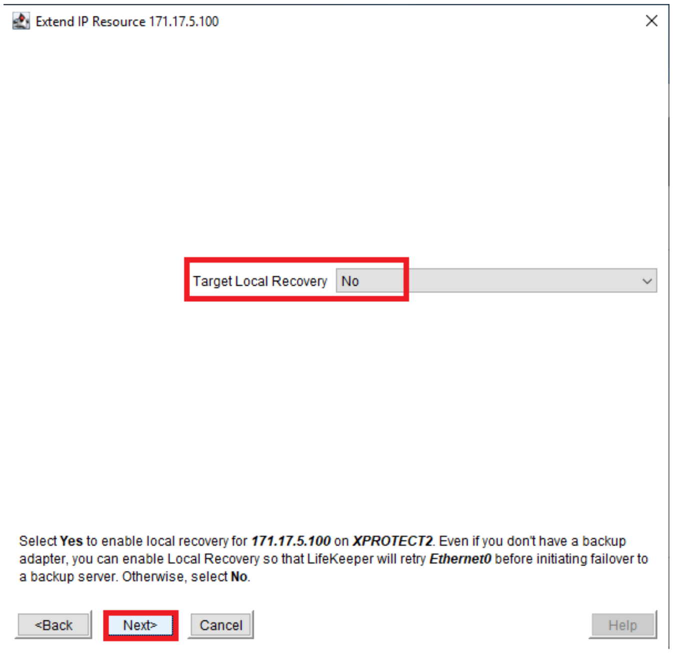
Select the appropriate Restore Mode for ***171.17.5.100*** on ***XPROTECT2***.

In some situations a protected IP address should not be used on a remote target system. For example, the remote target system may be connected to a different subnet than other systems in the cluster. In this situation the IP resource may be extended in **Disable Restore Mode.**

In **Disable Restore Mode**, the LifeKeeper IP Resource will not configure the IP address on ***XPROTECT2*** when ***171.17.5.100*** is placed in-service there. Also, the IP address will not be monitored and ***171.17.5.100*** can not be extended while it is in-service and **Disable Restore Mode** has been selected. In these situations network redirection may be implemented some other way, perhaps by using a LifeKeeper DNS resource.

You may use the IP resource properties page on the target system to change your selection at a later time.

14. Turn off local recovery for the extend

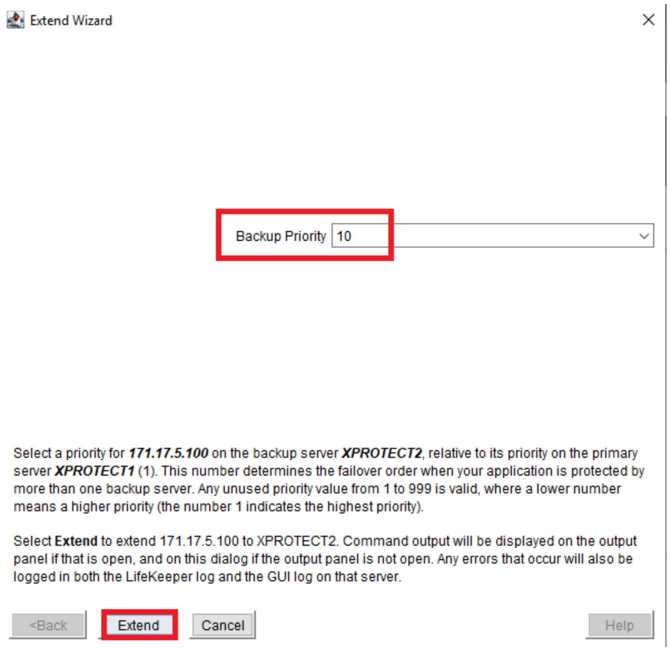


Extend IP Resource 171.17.5.100

Target Local Recovery: No

Select **Yes** to enable local recovery for ***171.17.5.100*** on ***XPROTECT2***. Even if you don't have a backup adapter, you can enable Local Recovery so that LifeKeeper will retry ***Ethernet0*** before initiating failover to a backup server. Otherwise, select **No**.

15. Set backup priority



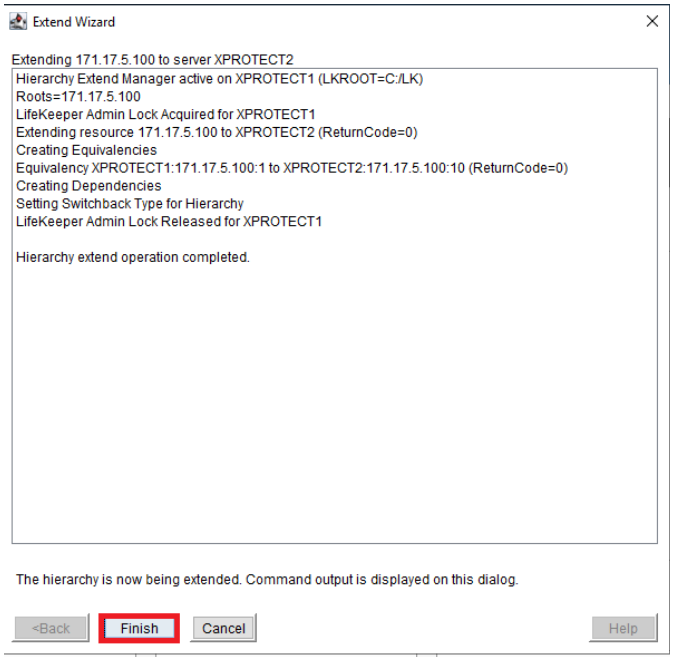
Extend Wizard

Backup Priority: 10

Select a priority for ***171.17.5.100*** on the backup server ***XPROTECT2***, relative to its priority on the primary server ***XPROTECT1*** (1). This number determines the failover order when your application is protected by more than one backup server. Any unused priority value from 1 to 999 is valid, where a lower number means a higher priority (the number 1 indicates the highest priority).

Select **Extend** to extend 171.17.5.100 to XPROTECT2. Command output will be displayed on the output panel if that is open, and on this dialog if the output panel is not open. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on that server.

16. Verify extend was successful

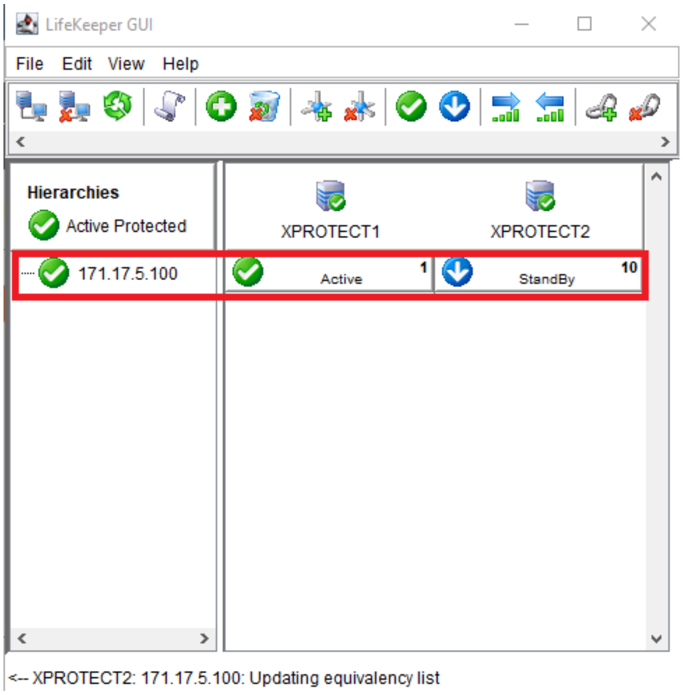


Extending 171.17.5.100 to server XPROTECT2

```
Hierarchy Extend Manager active on XPROTECT1 (LKROOT=C:/LK)
Roots=171.17.5.100
LifeKeeper Admin Lock Acquired for XPROTECT1
Extending resource 171.17.5.100 to XPROTECT2 (ReturnCode=0)
Creating Equivalencies
Equivalency XPROTECT1:171.17.5.100:1 to XPROTECT2:171.17.5.100:10 (ReturnCode=0)
Creating Dependencies
Setting Switchback Type for Hierarchy
LifeKeeper Admin Lock Released for XPROTECT1

Hierarchy extend operation completed.
```

The hierarchy is now being extended. Command output is displayed on this dialog.

17. What LifeKeeper should look like once finished

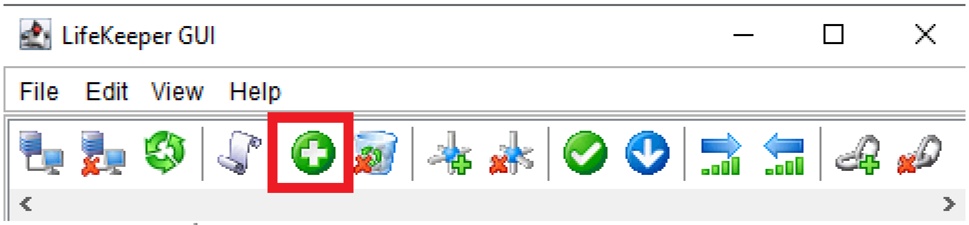


Hierarchies	XPROTECT1	XPROTECT2
✓ Active Protected		
✓ 171.17.5.100	✓ Active 1	StandBy 10

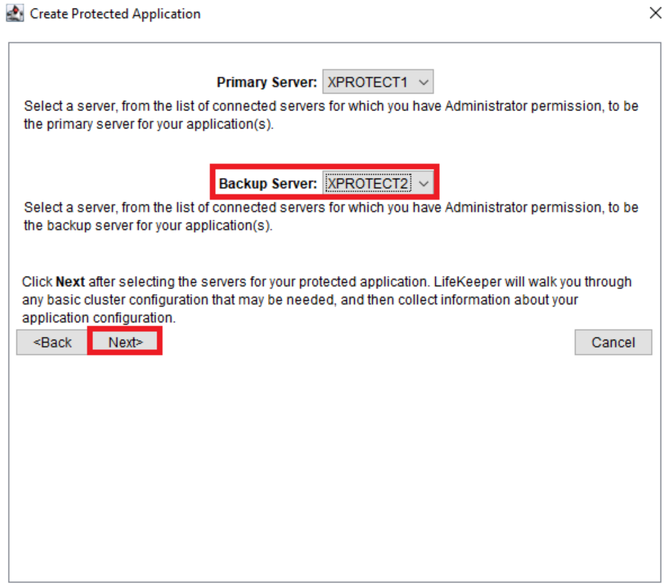
<-- XPROTECT2: 171.17.5.100: Updating equivalency list

Create Volume resource:

1. Choose create new resource



2. Choose Primary and Backup Server



Create Protected Application

Primary Server: XPROTECT1

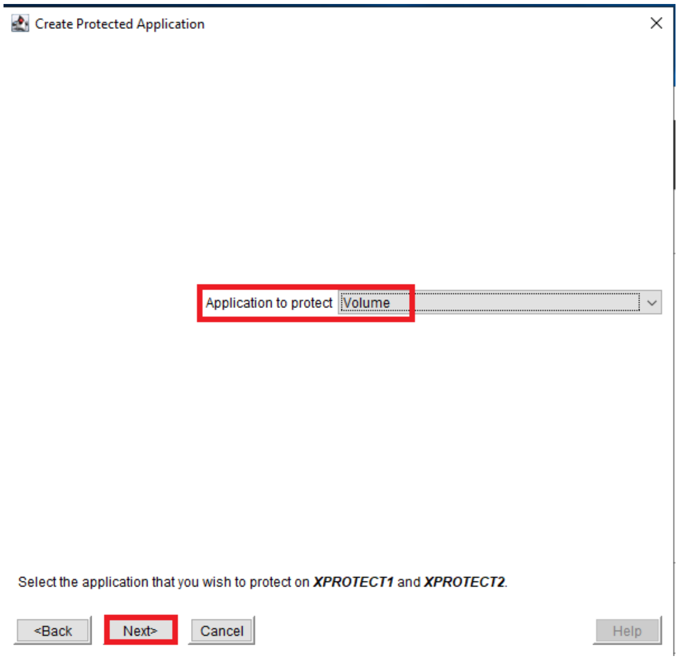
Select a server, from the list of connected servers for which you have Administrator permission, to be the primary server for your application(s).

Backup Server: XPROTECT2

Select a server, from the list of connected servers for which you have Administrator permission, to be the backup server for your application(s).

Click **Next** after selecting the servers for your protected application. LifeKeeper will walk you through any basic cluster configuration that may be needed, and then collect information about your application configuration.

3. Choose Volume resource to protect

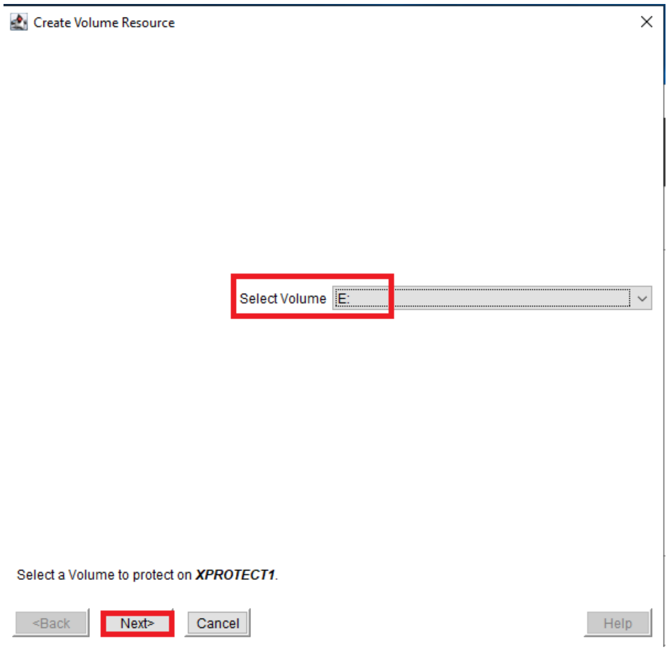


Create Protected Application

Application to protect: Volume

Select the application that you wish to protect on ***XPROTECT1*** and ***XPROTECT2***.

4. Select which volume to protect

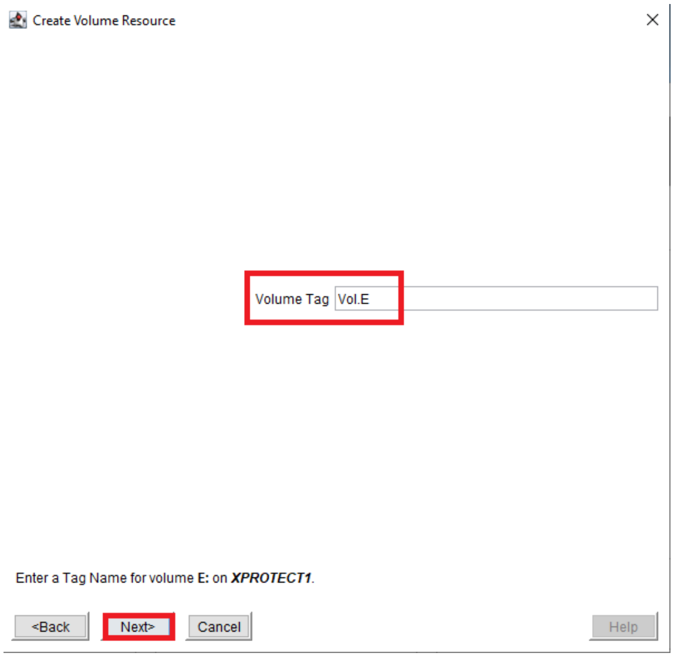


Create Volume Resource

Select Volume E:

Select a Volume to protect on ***XPROTECT1***.

5. Set tag for volume resource

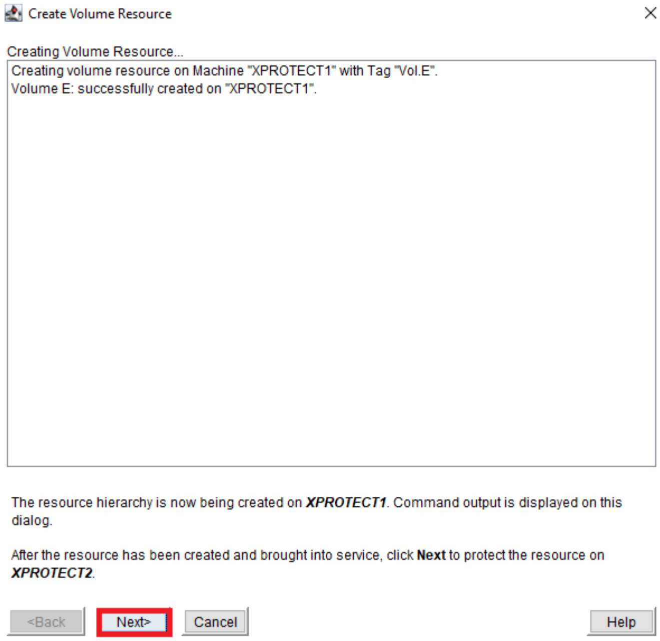


Create Volume Resource

Volume Tag Vol.E

Enter a Tag Name for volume **E:** on ***XPROTECT1***.

6. Verify volume resource creation was successful



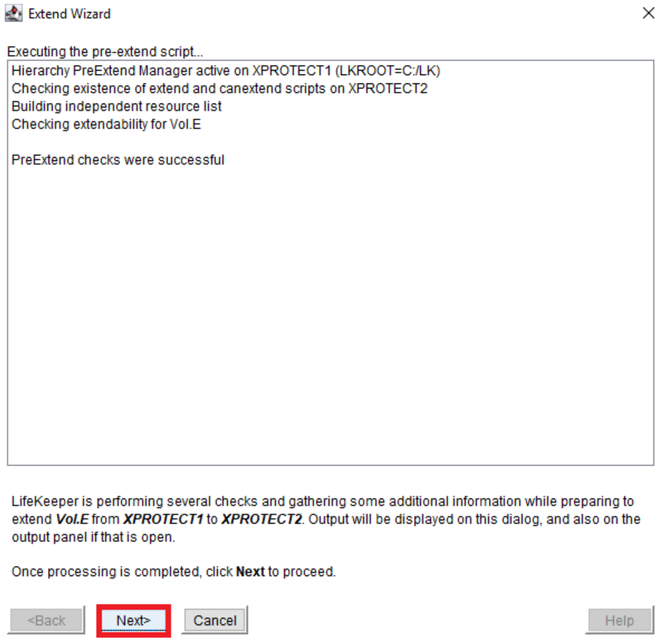
Creating Volume Resource...

```
Creating volume resource on Machine "XPROTECT1" with Tag "Vol.E".
Volume E: successfully created on "XPROTECT1".
```

The resource hierarchy is now being created on ***XPROTECT1***. Command output is displayed on this dialog.

After the resource has been created and brought into service, click **Next** to protect the resource on ***XPROTECT2***.

7. Run extend checks and verify they were successful



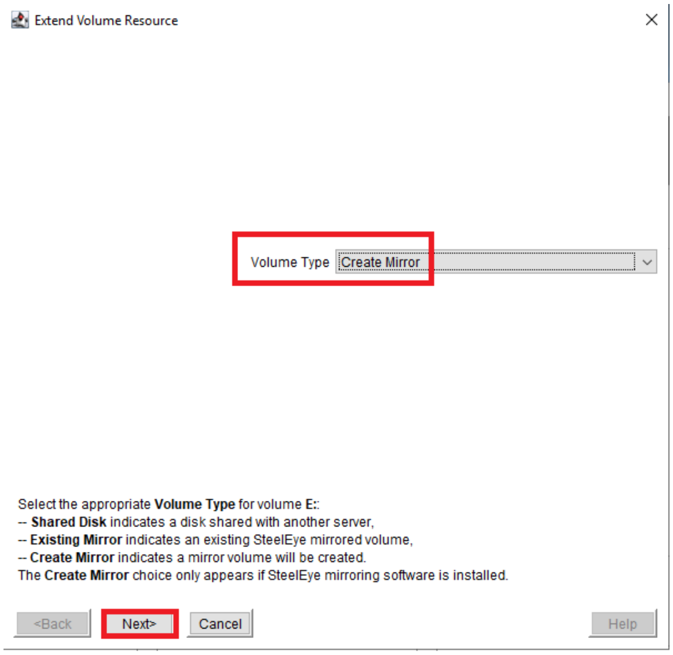
Executing the pre-extend script...

```
Hierarchy PreExtend Manager active on XPROTECT1 (LKROOT=C:/LK)
Checking existence of extend and canextend scripts on XPROTECT2
Building independent resource list
Checking extendability for Vol.E

PreExtend checks were successful
```

LifeKeeper is performing several checks and gathering some additional information while preparing to extend ***Vol.E*** from ***XPROTECT1*** to ***XPROTECT2***. Output will be displayed on this dialog, and also on the output panel if that is open.

Once processing is completed, click **Next** to proceed.

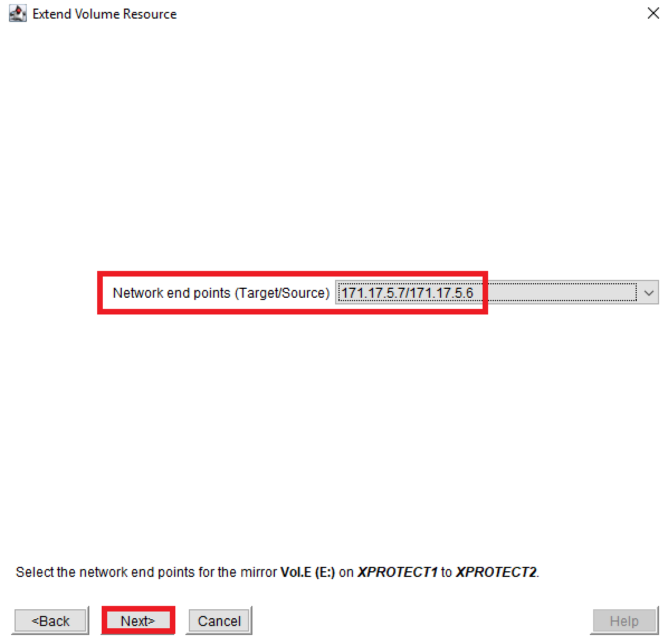
8. Select Create Mirror for Volume Type



Volume Type: Create Mirror

Select the appropriate **Volume Type** for volume **E:**:
-- **Shared Disk** indicates a disk shared with another server,
-- **Existing Mirror** indicates an existing SteelEye mirrored volume,
-- **Create Mirror** indicates a mirror volume will be created.
The **Create Mirror** choice only appears if SteelEye mirroring software is installed.

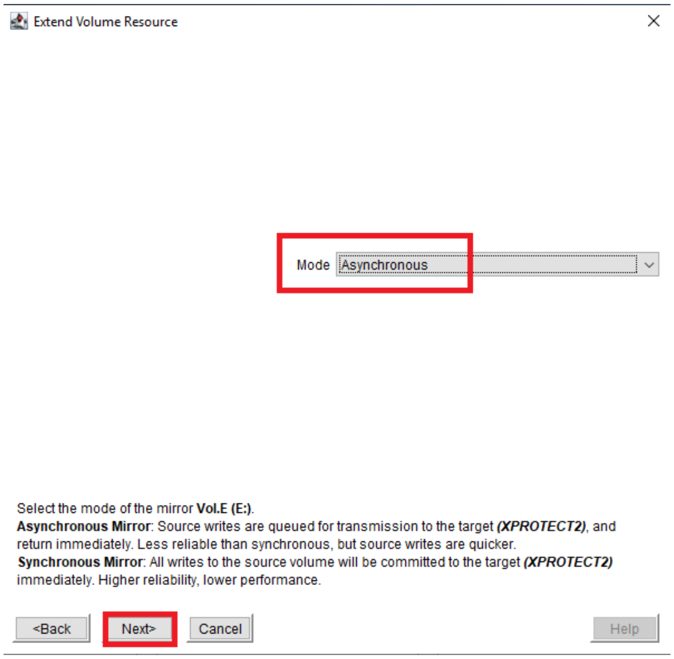
9. Choose end points



Network end points (Target/Source): 171.17.5.7/171.17.5.6

Select the network end points for the mirror **Vol.E (E:)** on ***XPROTECT1*** to ***XPROTECT2***.

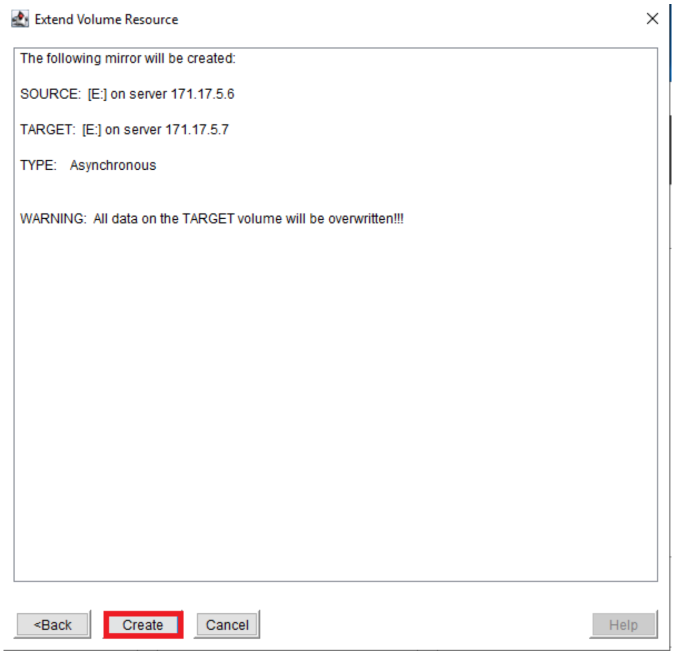
10. Set mode to Asynchronous



Mode: Asynchronous

Select the mode of the mirror **Vol.E (E:)**.
Asynchronous Mirror: Source writes are queued for transmission to the target ***(XPROTECT2)***, and return immediately. Less reliable than synchronous, but source writes are quicker.
Synchronous Mirror: All writes to the source volume will be committed to the target ***(XPROTECT2)*** immediately. Higher reliability, lower performance.

11. Verify mirror info (pay attention to warning about volume being overwritten)



The following mirror will be created:

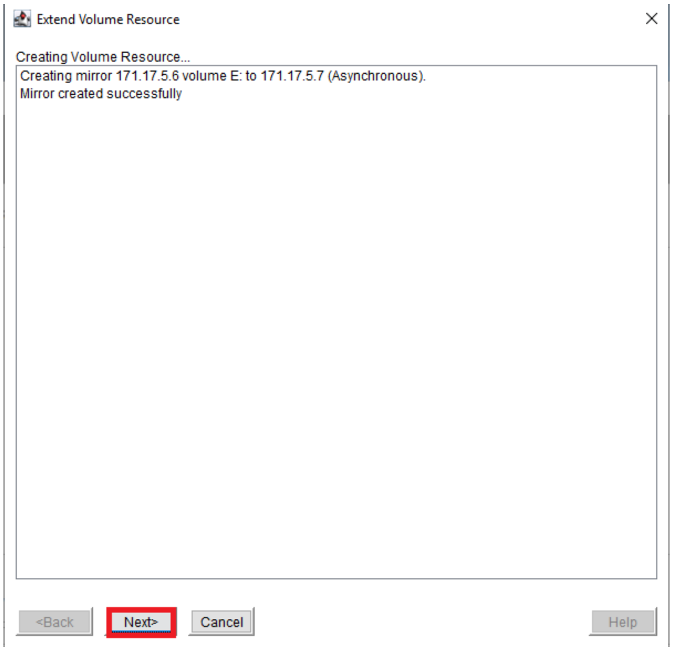
SOURCE: [E:] on server 171.17.5.6

TARGET: [E:] on server 171.17.5.7

TYPE: Asynchronous

WARNING: All data on the TARGET volume will be overwritten!!!

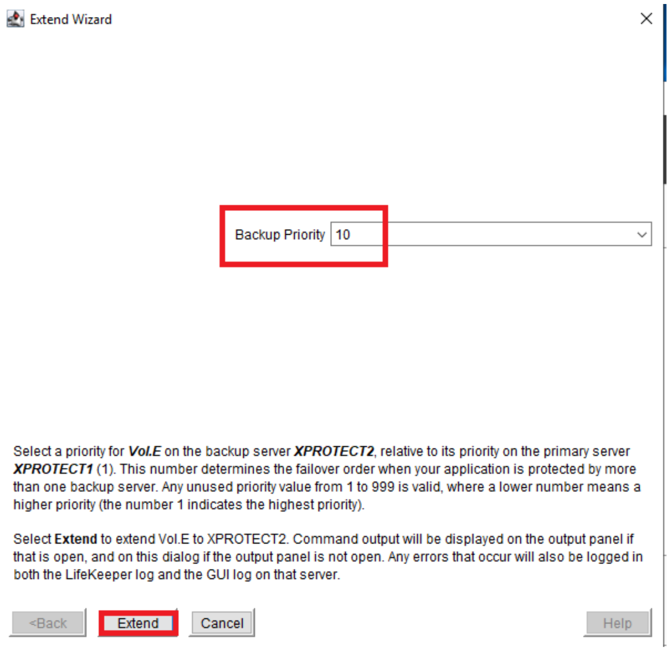
12. Verify mirror was created successfully



Creating Volume Resource...

```
Creating mirror 171.17.5.6 volume E: to 171.17.5.7 (Asynchronous).
Mirror created successfully
```

13. Set Backup Priority

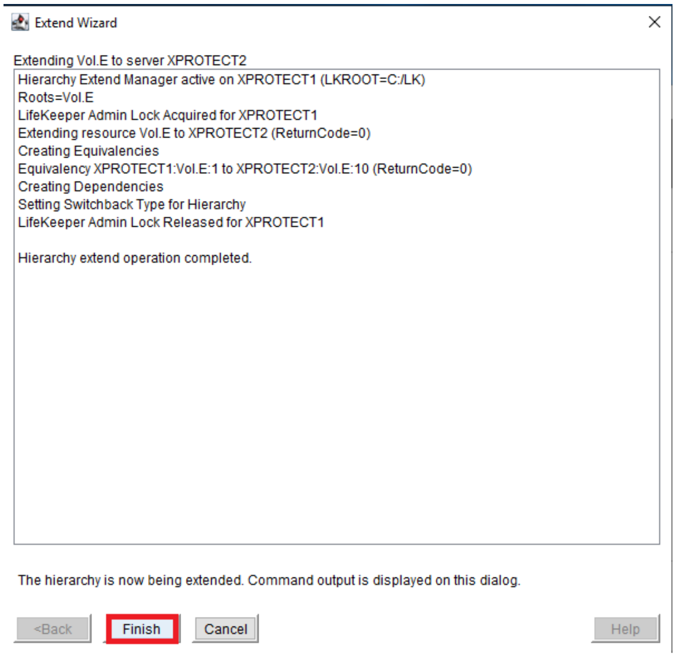


Backup Priority 10

Select a priority for ***Vol.E*** on the backup server ***XPROTECT2***, relative to its priority on the primary server ***XPROTECT1*** (1). This number determines the failover order when your application is protected by more than one backup server. Any unused priority value from 1 to 999 is valid, where a lower number means a higher priority (the number 1 indicates the highest priority).

Select **Extend** to extend Vol.E to XPROTECT2. Command output will be displayed on the output panel if that is open, and on this dialog if the output panel is not open. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on that server.

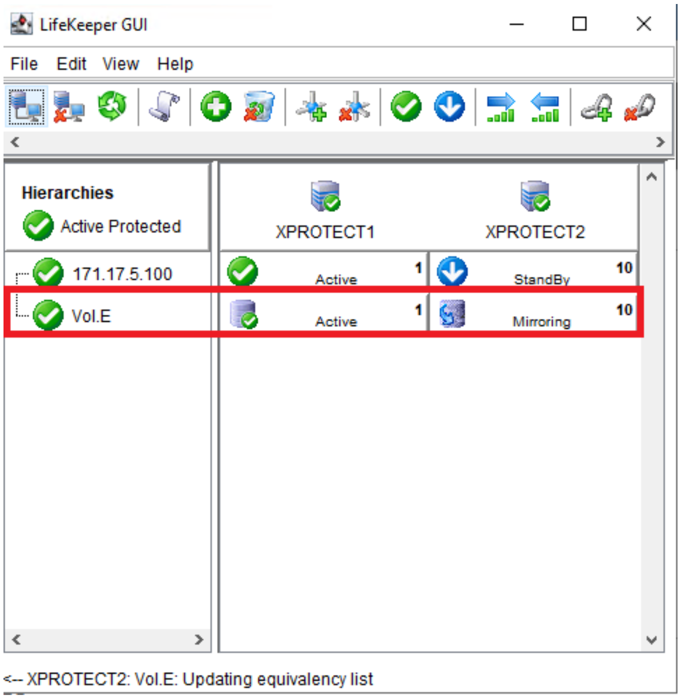
14. Verify volume extend was successful



```
Extending Vol.E to server XPROTECT2
Hierarchy Extend Manager active on XPROTECT1 (LKROOT=C:/LK)
Roots=Vol.E
LifeKeeper Admin Lock Acquired for XPROTECT1
Extending resource Vol.E to XPROTECT2 (ReturnCode=0)
Creating Equivalencies
Equivalency XPROTECT1:Vol.E:1 to XPROTECT2:Vol.E:10 (ReturnCode=0)
Creating Dependencies
Setting Switchback Type for Hierarchy
LifeKeeper Admin Lock Released for XPROTECT1

Hierarchy extend operation completed.
```

The hierarchy is now being extended. Command output is displayed on this dialog.

15. LifeKeeper should look like this when completed



Hierarchies ✓ Active Protected	XPROTECT1		XPROTECT2	
✓ 171.17.5.100	✓ Active	1	StandBy	10
✓ Vol.E	Active	1	Mirroring	10

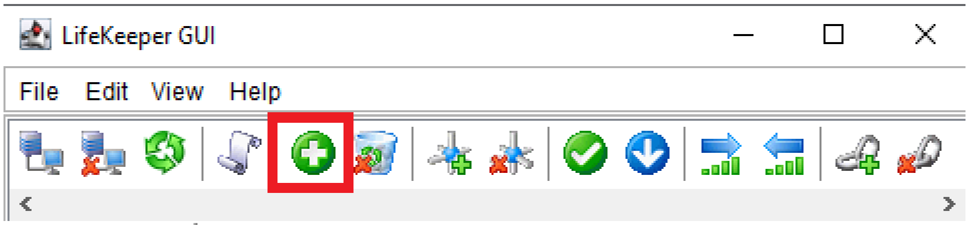
<-- XPROTECT2: Vol.E: Updating equivalency list

Step 5 - Cluster SQL Server with LifeKeeper

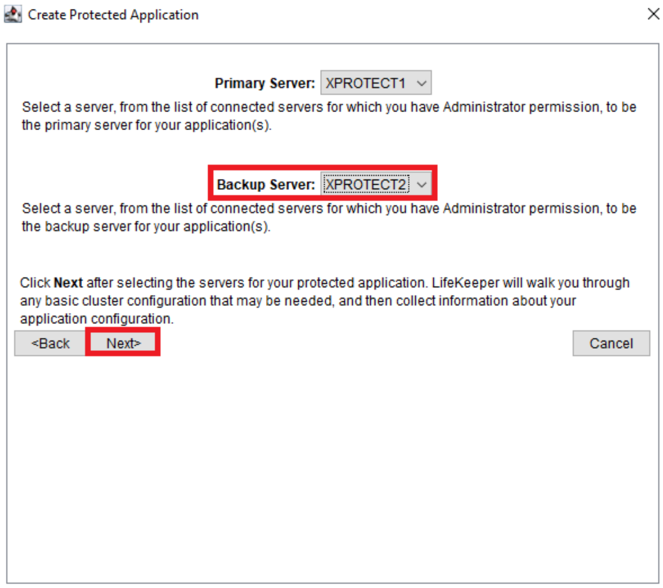
Cluster SQL Server following the SIOS documentation. Create a Virtual IP address first, and then Disk resources. Finally the SQL resource. No NetBIOS name is required. Make sure the SQL Server Service is set to Manual start.

Create SQL resource:

1. Choose create new resource



2. Choose Primary and Backup Server



Primary Server: XPROTECT1

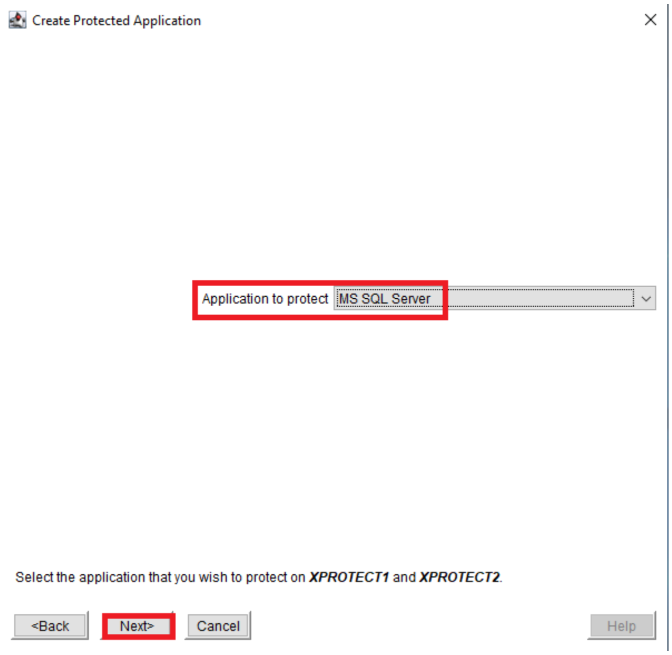
Select a server, from the list of connected servers for which you have Administrator permission, to be the primary server for your application(s).

Backup Server: XPROTECT2

Select a server, from the list of connected servers for which you have Administrator permission, to be the backup server for your application(s).

Click **Next** after selecting the servers for your protected application. LifeKeeper will walk you through any basic cluster configuration that may be needed, and then collect information about your application configuration.

3. Choose MS SQL Server to protect

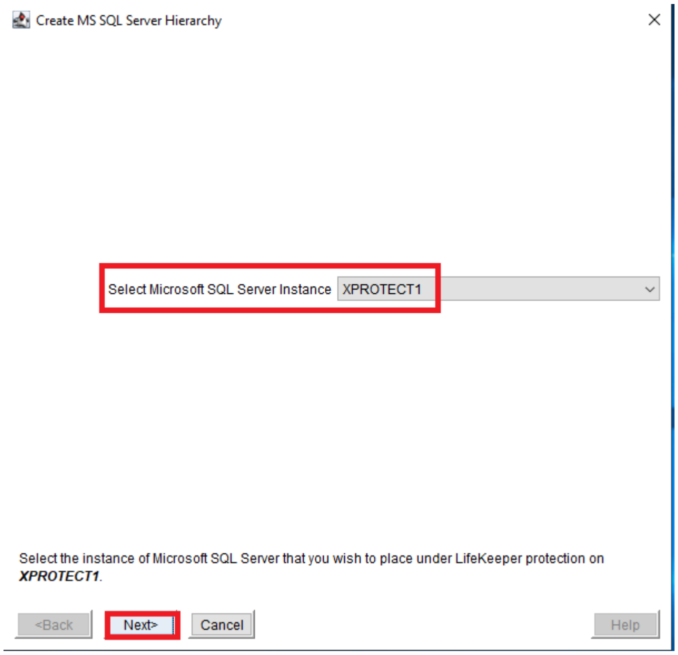


Create Protected Application

Application to protect: MS SQL Server

Select the application that you wish to protect on ***XPROTECT1*** and ***XPROTECT2***.

4. Select what instance to protect

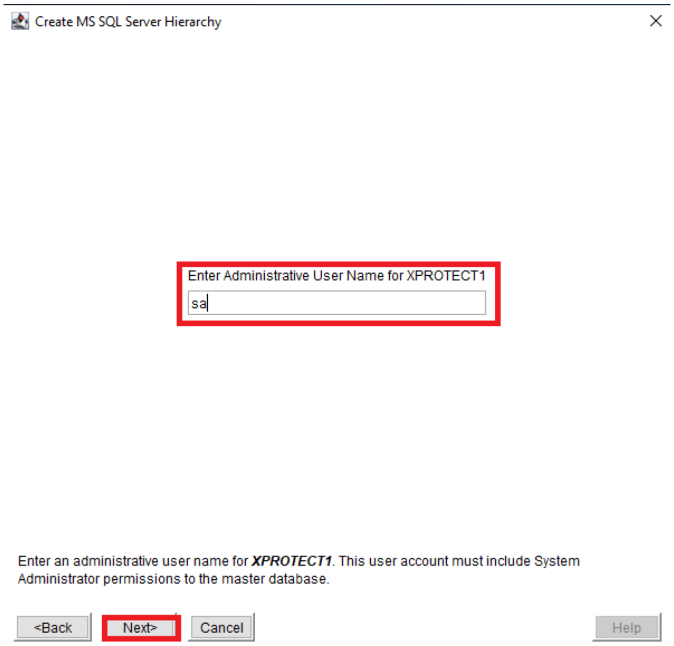


Create MS SQL Server Hierarchy

Select Microsoft SQL Server Instance: XPROTECT1

Select the instance of Microsoft SQL Server that you wish to place under LifeKeeper protection on ***XPROTECT1***.

5. Administrative name should be the one you used when you installed SQL Server. The default account is ‘sa’



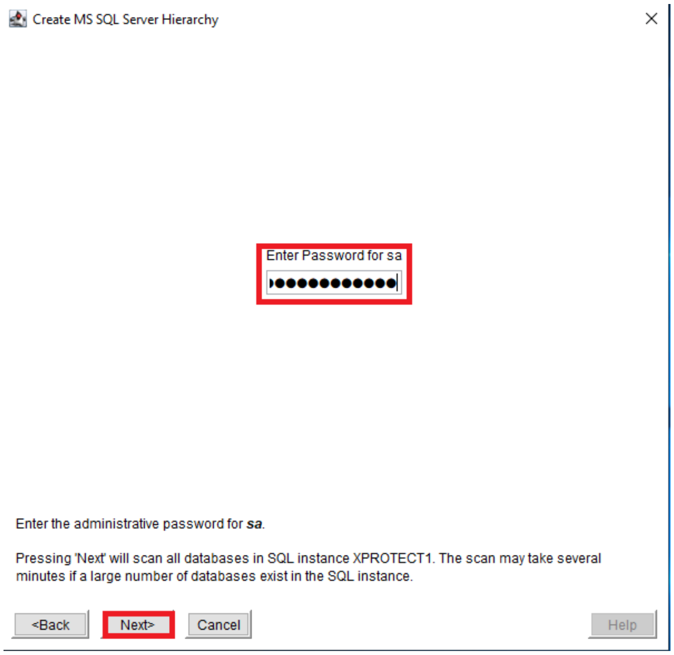
Create MS SQL Server Hierarchy

Enter Administrative User Name for XPROTECT1

sa

Enter an administrative user name for ***XPROTECT1***. This user account must include System Administrator permissions to the master database.

6. Enter the password for the ‘sa’ account.



Create MS SQL Server Hierarchy

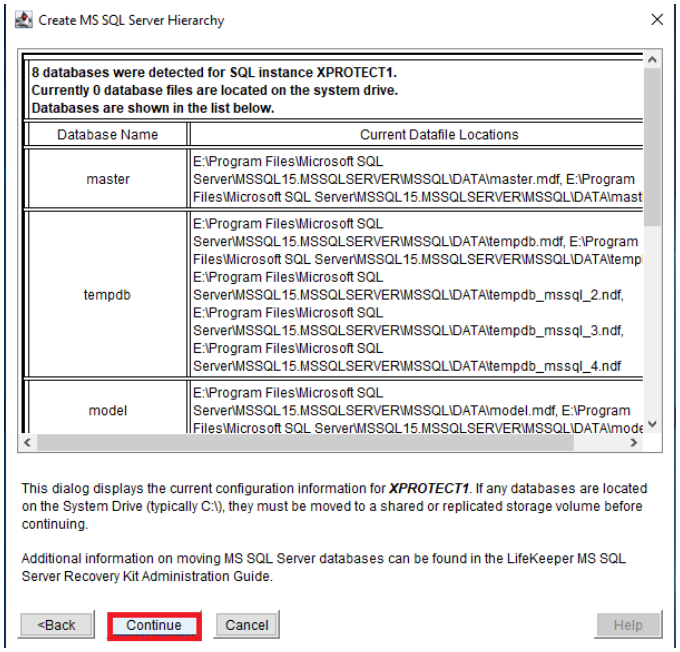
Enter Password for sa

●●●●●●●●●●●●

Enter the administrative password for ***sa***.

Pressing 'Next' will scan all databases in SQL instance XPROTECT1. The scan may take several minutes if a large number of databases exist in the SQL instance.

7. Verify database location(s) looks correct
   Note: If during installation of SQL Server you failed to relocate the system databases to the partition designated for replication, you will be given an option here to allow LifeKeeper to relocate them automatically for you.



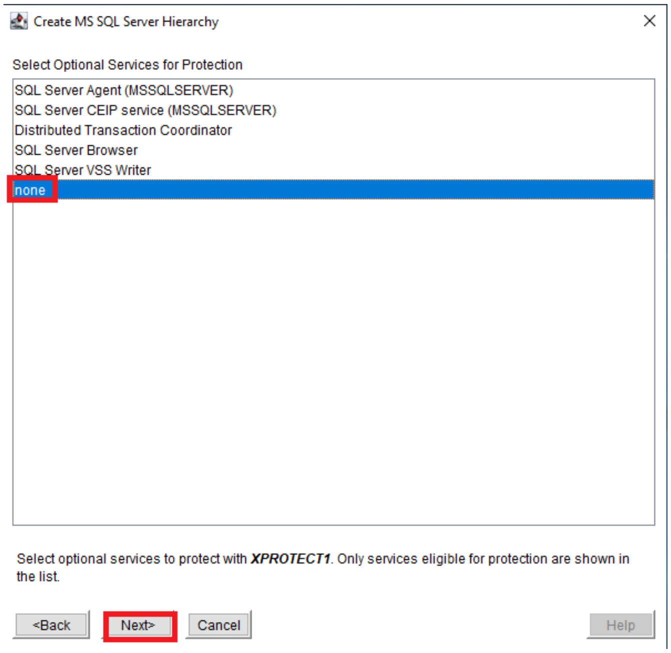
8 databases were detected for SQL instance XPROTECT1.
Currently 0 database files are located on the system drive.
Databases are shown in the list below.

Database Name	Current Datafile Locations
master	E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\master.mdf, E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\mast
tempdb	E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\tempdb.mdf, E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\temp E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\tempdb_mssql_2.ndf, E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\tempdb_mssql_3.ndf, E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\tempdb_mssql_4.ndf
model	E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\model.mdf, E:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\mode

This dialog displays the current configuration information for ***XPROTECT1***. If any databases are located on the System Drive (typically C:\), they must be moved to a shared or replicated storage volume before continuing.

Additional information on moving MS SQL Server databases can be found in the LifeKeeper MS SQL Server Recovery Kit Administration Guide.

8. Protect any additional services you wish to cluster.

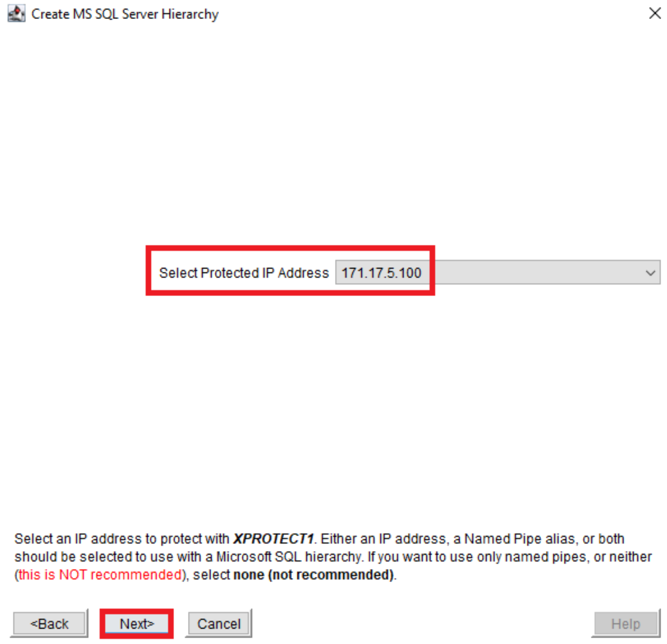


Select Optional Services for Protection

- SQL Server Agent (MSSQLSERVER)
- SQL Server CEIP service (MSSQLSERVER)
- Distributed Transaction Coordinator
- SQL Server Browser
- SQL Server VSS Writer
- none

Select optional services to protect with ***XPROTECT1***. Only services eligible for protection are shown in the list.

9. Select the protected Virtual IP address (the one we created earlier)

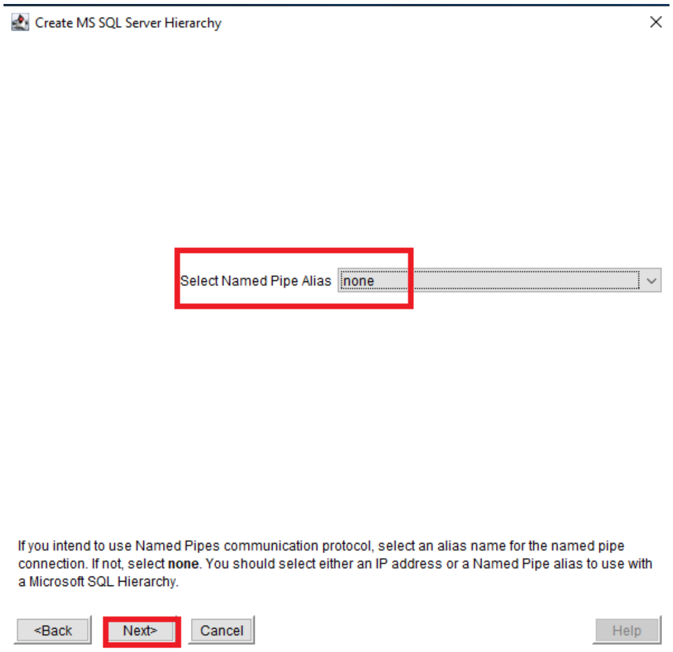


Create MS SQL Server Hierarchy

Select Protected IP Address 171.17.5.100

Select an IP address to protect with ***XPROTECT1***. Either an IP address, a Named Pipe alias, or both should be selected to use with a Microsoft SQL hierarchy. If you want to use only named pipes, or neither (this is NOT recommended), select **none (not recommended)**.

10. Set named pipe alias to none

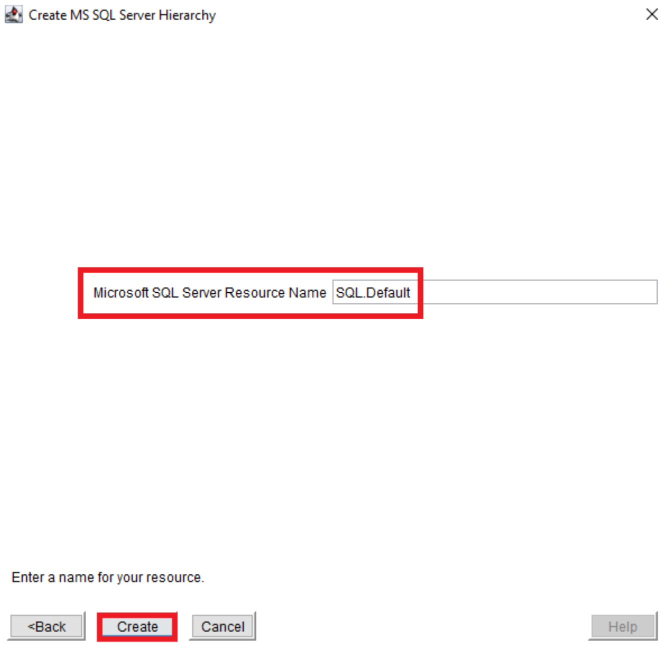


Create MS SQL Server Hierarchy

Select Named Pipe Alias none

If you intend to use Named Pipes communication protocol, select an alias name for the named pipe connection. If not, select **none**. You should select either an IP address or a Named Pipe alias to use with a Microsoft SQL Hierarchy.

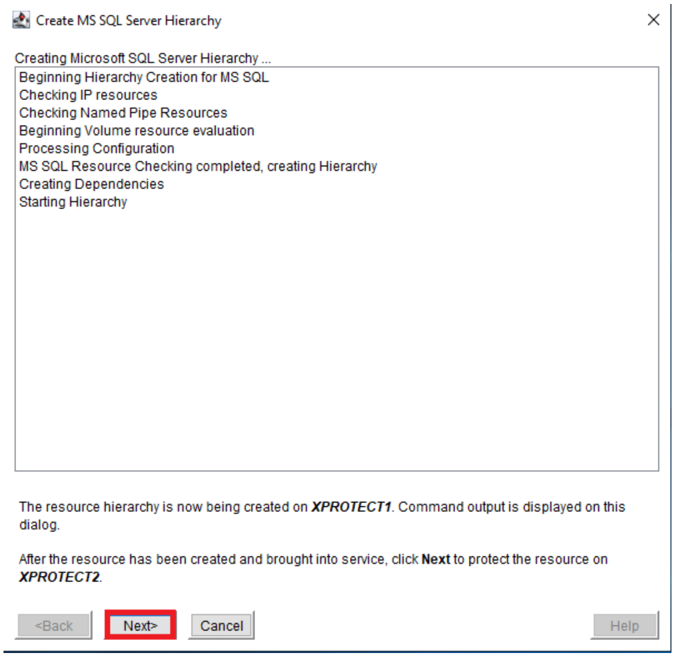
11. Set the resource name



Microsoft SQL Server Resource Name SQL.Default

Enter a name for your resource.

12. Verify resource creation was successful



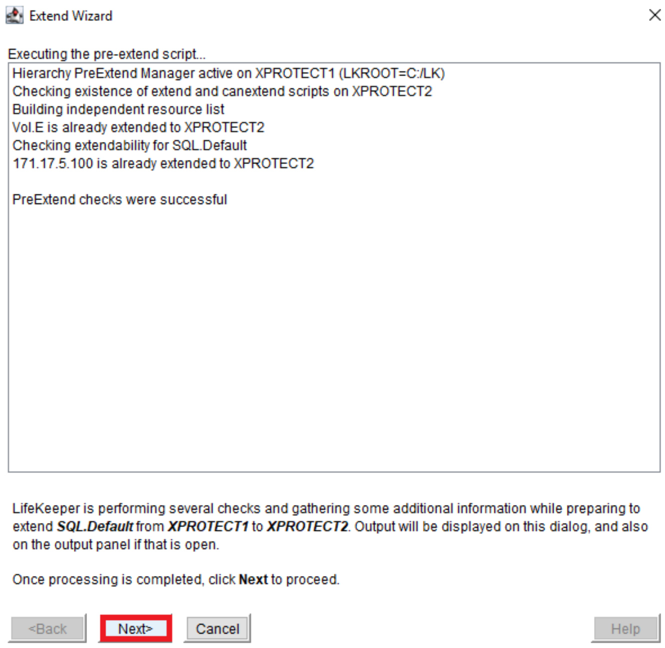
Creating Microsoft SQL Server Hierarchy ...

```
Beginning Hierarchy Creation for MS SQL
Checking IP resources
Checking Named Pipe Resources
Beginning Volume resource evaluation
Processing Configuration
MS SQL Resource Checking completed, creating Hierarchy
Creating Dependencies
Starting Hierarchy
```

The resource hierarchy is now being created on ***XPROTECT1***. Command output is displayed on this dialog.

After the resource has been created and brought into service, click **Next** to protect the resource on ***XPROTECT2***.

13. Verify the extend checks were successful



Extend Wizard

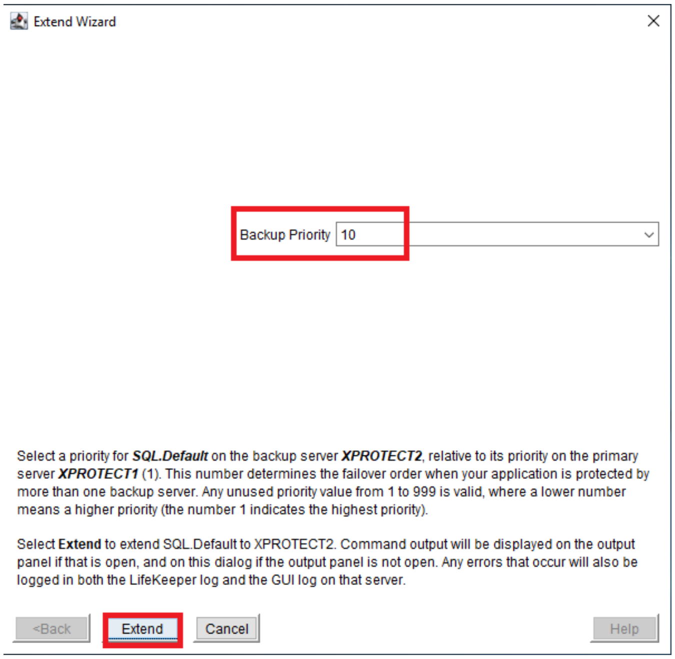
Executing the pre-extend script...

```
Hierarchy PreExtend Manager active on XPROTECT1 (LKROOT=C:/LK)
Checking existence of extend and canextend scripts on XPROTECT2
Building independent resource list
Vol.E is already extended to XPROTECT2
Checking extendability for SQL.Default
171.17.5.100 is already extended to XPROTECT2

PreExtend checks were successful
```

LifeKeeper is performing several checks and gathering some additional information while preparing to extend ***SQL.Default*** from ***XPROTECT1*** to ***XPROTECT2***. Output will be displayed on this dialog, and also on the output panel if that is open.

Once processing is completed, click **Next** to proceed.

14. Set backup priority



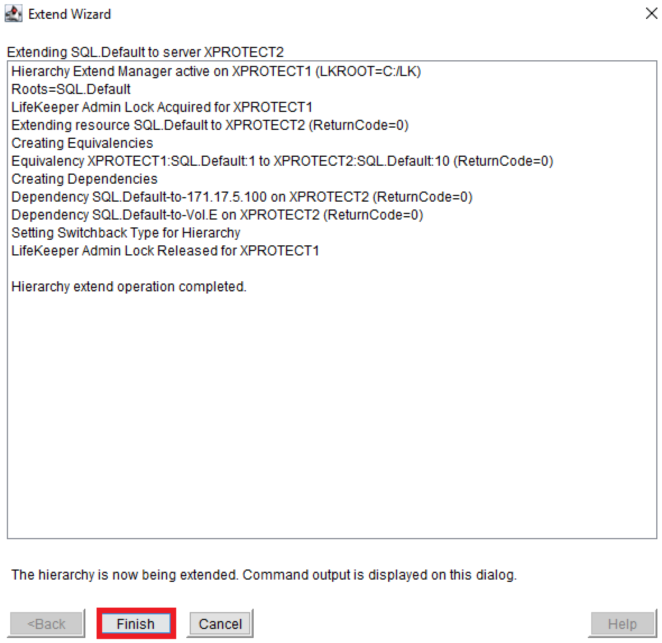
Extend Wizard

Backup Priority 10

Select a priority for ***SQL.Default*** on the backup server ***XPROTECT2***, relative to its priority on the primary server ***XPROTECT1*** (1). This number determines the failover order when your application is protected by more than one backup server. Any unused priority value from 1 to 999 is valid, where a lower number means a higher priority (the number 1 indicates the highest priority).

Select **Extend** to extend SQL.Default to XPROTECT2. Command output will be displayed on the output panel if that is open, and on this dialog if the output panel is not open. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on that server.

15. Verify extend was successful

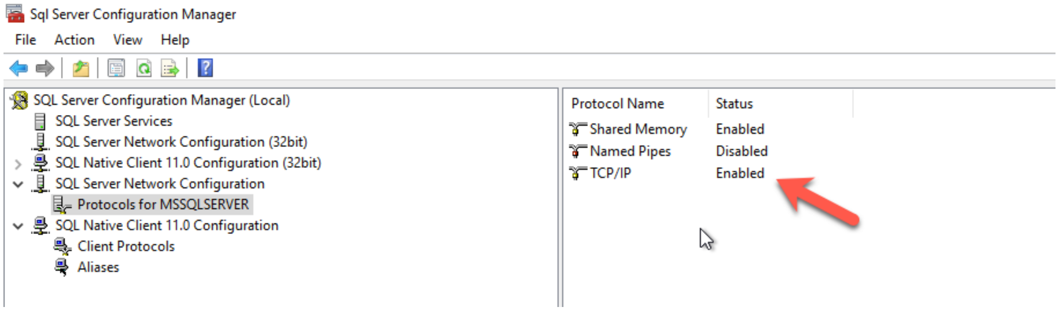


Extending SQL.Default to server XPROTECT2

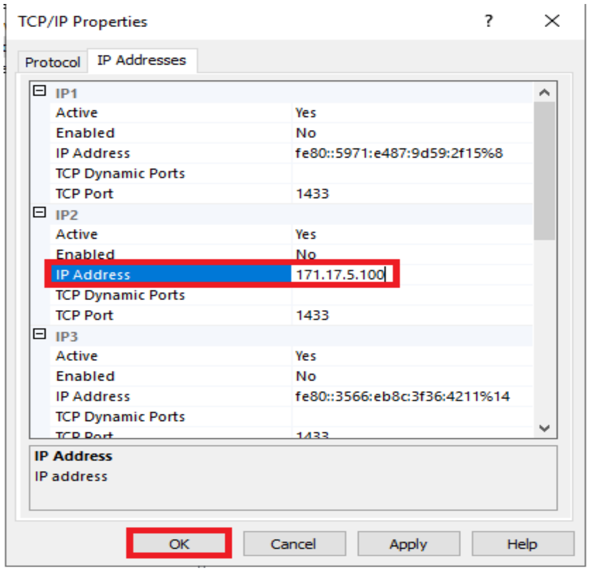
```
Hierarchy Extend Manager active on XPROTECT1 (LKROOT=C:/LK)
Roots=SQL.Default
LifeKeeper Admin Lock Acquired for XPROTECT1
Extending resource SQL.Default to XPROTECT2 (ReturnCode=0)
Creating Equivalencies
Equivalency XPROTECT1:SQL.Default:1 to XPROTECT2:SQL.Default:10 (ReturnCode=0)
Creating Dependencies
Dependency SQL.Default-to-171.17.5.100 on XPROTECT2 (ReturnCode=0)
Dependency SQL.Default-to-Vol.E on XPROTECT2 (ReturnCode=0)
Setting Switchback Type for Hierarchy
LifeKeeper Admin Lock Released for XPROTECT1

Hierarchy extend operation completed.
```

The hierarchy is now being extended. Command output is displayed on this dialog.

16. Enable SQL to listen on TCP and the Virtual IP address. Do this on XPROTECT1 and XPROTECT2


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 11.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for MSSQLSERVER
SQL Native Client 11.0 Configuration
Client Protocols
Aliases

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled

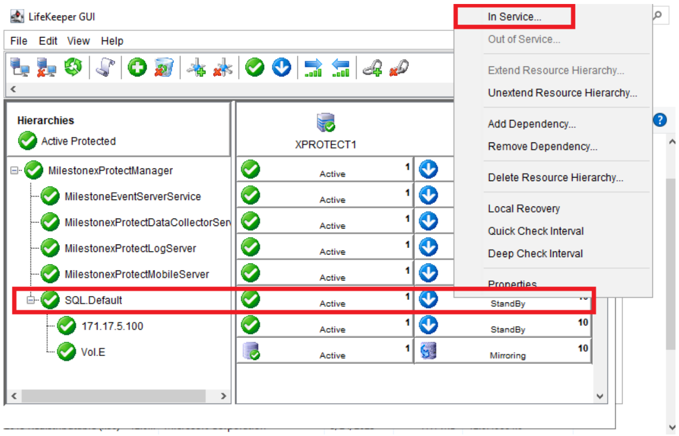


TCP/IP Properties

IP1	
Active	Yes
Enabled	No
IP Address	fe80::5971:e487:9d59:2f15%8
TCP Dynamic Ports	
TCP Port	1433
IP2	
Active	Yes
Enabled	No
IP Address	171.17.5.100
TCP Dynamic Ports	
TCP Port	1433
IP3	
Active	Yes
Enabled	No
IP Address	fe80::3566:eb8c:3f36:4211%14
TCP Dynamic Ports	
TCP Port	1433

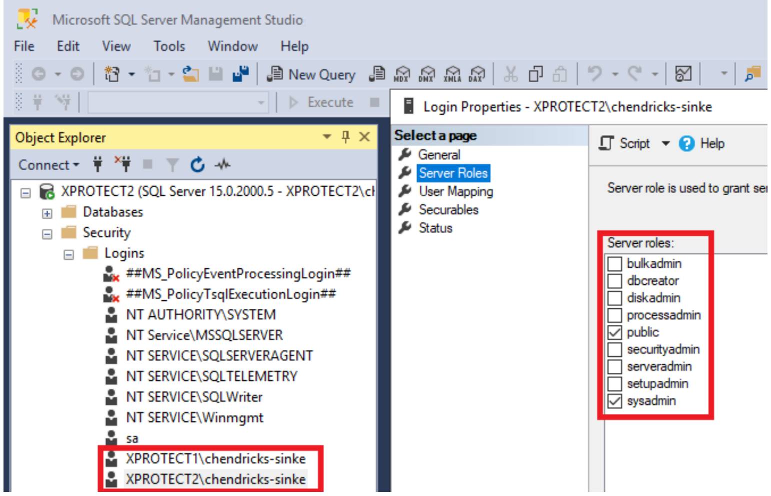
IP Address
IP address

17. Perform a switchover of the SQL Resource using LifeKeeper by right clicking and clicking ‘In Service’ on the secondary (XPROTECT2)



Hierarchies Active Protected	XPROTECT1			
MilestonexProtectManager	Active	1		
MilestoneEventServerService	Active	1		
MilestonexProtectDataCollectorSer	Active	1		
MilestonexProtectLogServer	Active	1		
MilestonexProtectMobileServer	Active	1		
SQL.Default	Active	1	StandBy	10
171.17.5.100	Active	1	StandBy	10
Vol.E	Active	1	Mirroring	10

18. Add the account you created earlier for XPROTECT1 to the sql users while SQL is switched over to XPROTECT2. Make sure to add the appropriate server roles as shown


Microsoft SQL Server Management Studio
File
Edit
View
Tools
Window
Help
New Query
Execute
Login Properties - XPROTECT2\chendricks-sinke
Object Explorer
Connect
XPROTECT2 (SQL Server 15.0.2000.5 - XPROTECT2\cl
Databases
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
NT AUTHORITY\SYSTEM
NT Service\MSSQLSERVER
NT SERVICE\SQLSERVERAGENT
NT SERVICE\SQLTELEMETRY
NT SERVICE\SQLWriter
NT SERVICE\Winmgmt
sa
XPROTECT1\chendricks-sinke
XPROTECT2\chendricks-sinke
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Server role is used to grant se

Server roles:

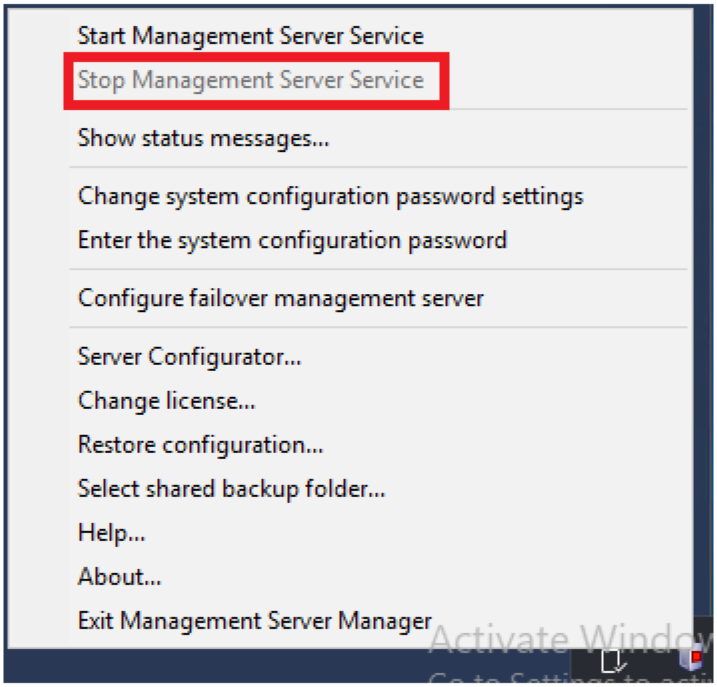
- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

Step 6 - Cluster XProtect with LifeKeeper

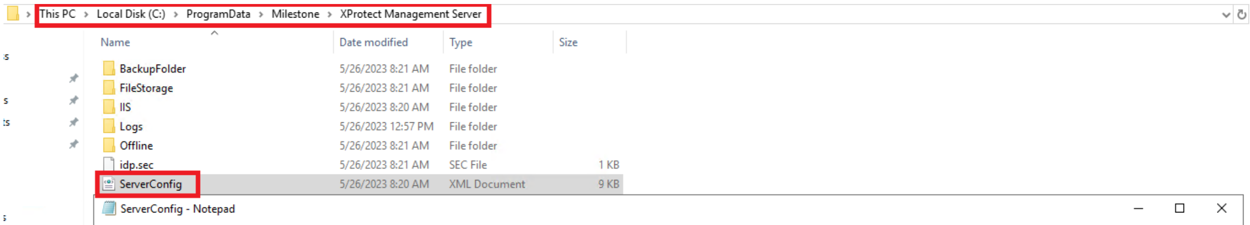
Setup for XProtect:

On XPROTECT1

1. Stop the service by right clicking the system tray icon and clicking 'Stop Management Server Service'


Start Management Server Service
Stop Management Server Service
Show status messages...
Change system configuration password settings
Enter the system configuration password
Configure failover management server
Server Configurator...
Change license...
Restore configuration...
Select shared backup folder...
Help...
About...
Exit Management Server Manager
Activate Window
Go to Settings to acti

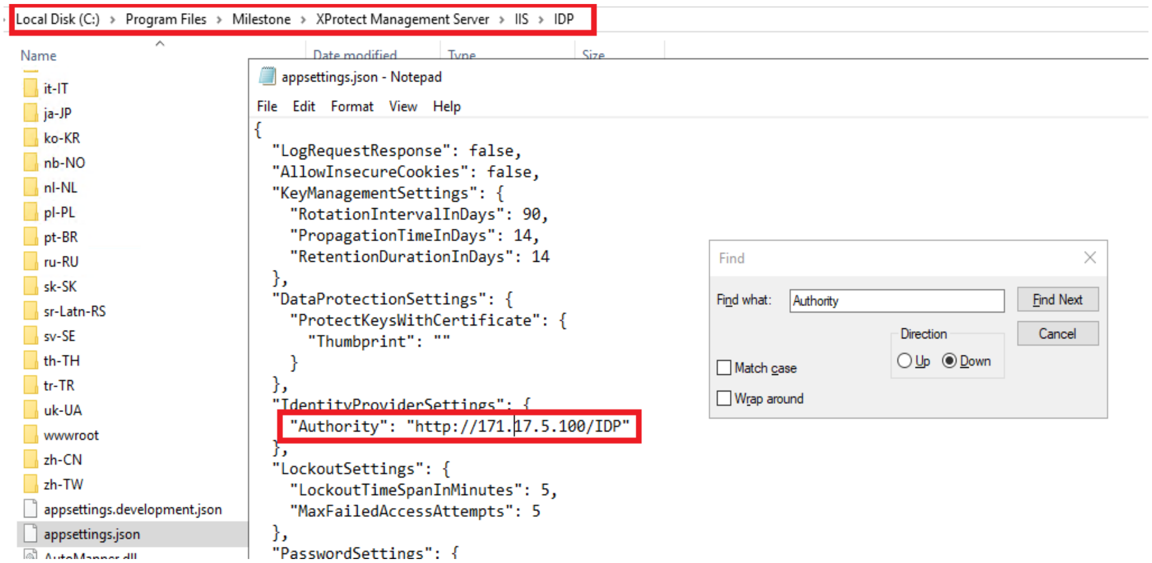
2. Modify the below config files accordingly, using the Virtual IP address address in place of the local computer name in the indicated URLs.
    a. C:/ProgramData/Milestone/xProtect Management Server/ServerConfig


This PC › Local Disk (C:) › ProgramData › Milestone › XProtect Management Server

Name	Date modified	Type	Size
BackupFolder	5/26/2023 8:21 AM	File folder	
FileStorage	5/26/2023 8:21 AM	File folder	
IIS	5/26/2023 8:20 AM	File folder	
Logs	5/26/2023 12:57 PM	File folder	
Offline	5/26/2023 8:21 AM	File folder	
idp.sec	5/26/2023 8:21 AM	SEC File	1 KB
ServerConfig	5/26/2023 8:20 AM	XML Document	9 KB

ServerConfig - Notepad

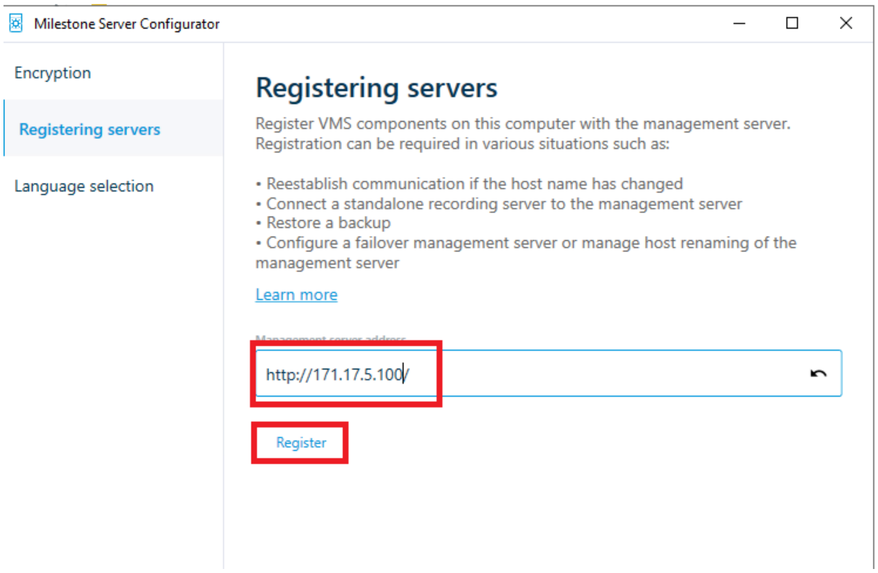
3. C:/Program Files/Milestone/XProtect Management Server/IIS/IDP/appsettings.json



Find what: Authority

```
{
  "LogRequestResponse": false,
  "AllowInsecureCookies": false,
  "KeyManagementSettings": {
    "RotationIntervalInDays": 90,
    "PropagationTimeInDays": 14,
    "RetentionDurationInDays": 14
  },
  "DataProtectionSettings": {
    "ProtectKeysWithCertificate": {
      "Thumbprint": ""
    }
  },
  "IdentityProviderSettings": {
    "Authority": "http://171.17.5.100/IDP"
  },
  "LockoutSettings": {
    "LockoutTimeSpanInMinutes": 5,
    "MaxFailedAccessAttempts": 5
  },
  "PasswordSettings": {
```

4. From the system tray icon right click and choose ‘Server Configurator’ and type in the Virtual IP address.



Registering servers

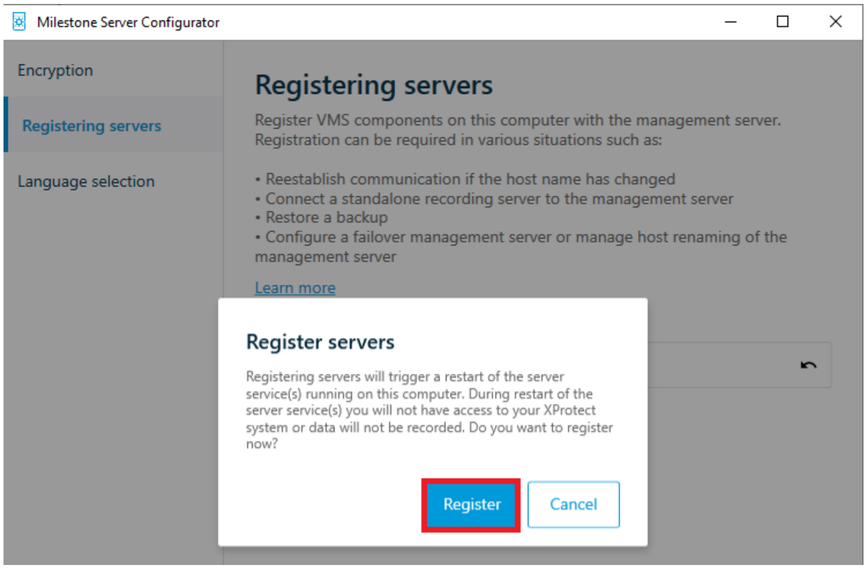
Register VMS components on this computer with the management server. Registration can be required in various situations such as:

- Reestablish communication if the host name has changed
- Connect a standalone recording server to the management server
- Restore a backup
- Configure a failover management server or manage host renaming of the management server

Management server address

http://171.17.5.100/

5. Register the Virtual IP address



Registering servers

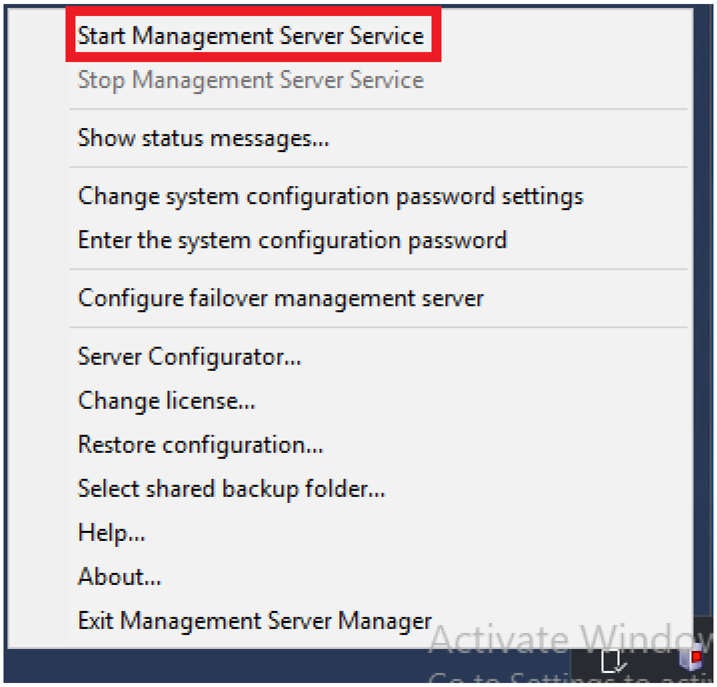
Register VMS components on this computer with the management server. Registration can be required in various situations such as:

- Reestablish communication if the host name has changed
- Connect a standalone recording server to the management server
- Restore a backup
- Configure a failover management server or manage host renaming of the management server

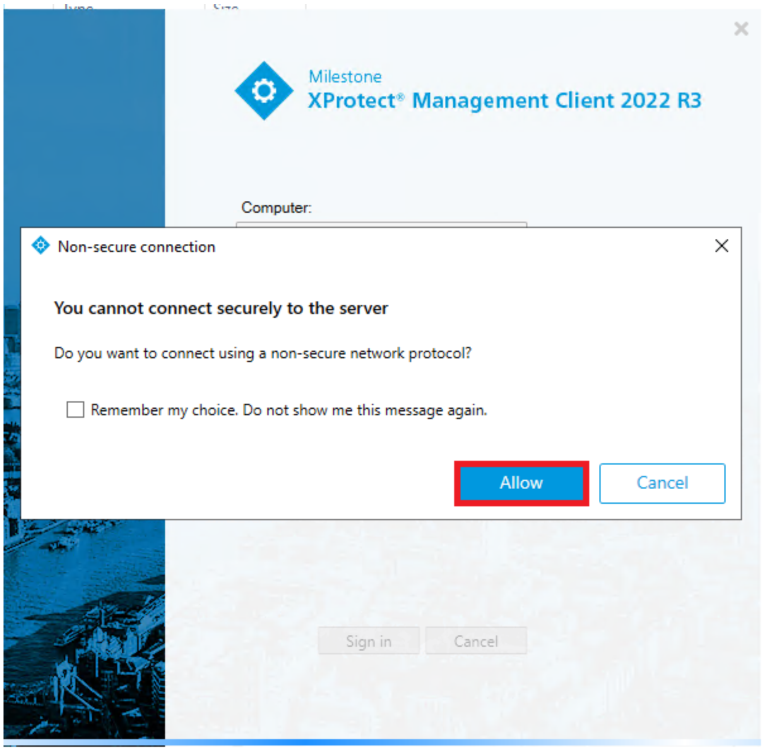
Register servers

Registering servers will trigger a restart of the server service(s) running on this computer. During restart of the server service(s) you will not have access to your XProtect system or data will not be recorded. Do you want to register now?

6. Start the service


Start Management Server Service
Stop Management Server Service
Show status messages...
Change system configuration password settings
Enter the system configuration password
Configure failover management server
Server Configurator...
Change license...
Restore configuration...
Select shared backup folder...
Help...
About...
Exit Management Server Manager
Activate Windo

7. Set the Virtual IP address for the URLs
    a. Open XProtect Management client (click allow for security prompt as shown) and click ‘Add Remove Registered Services’



Milestone
XProtect® Management Client 2022 R3

Computer:

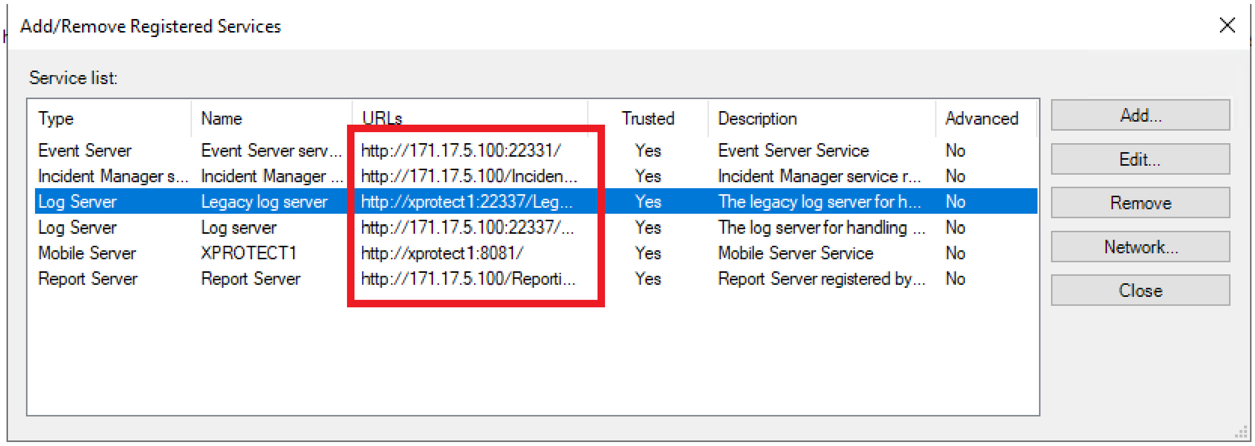
Non-secure connection

You cannot connect securely to the server

Do you want to connect using a non-secure network protocol?

□ Remember my choice. Do not show me this message again.

b. Replace all ‘XPROTECT1’ with the Virtual IP address you created earlier for the URLs highlighted

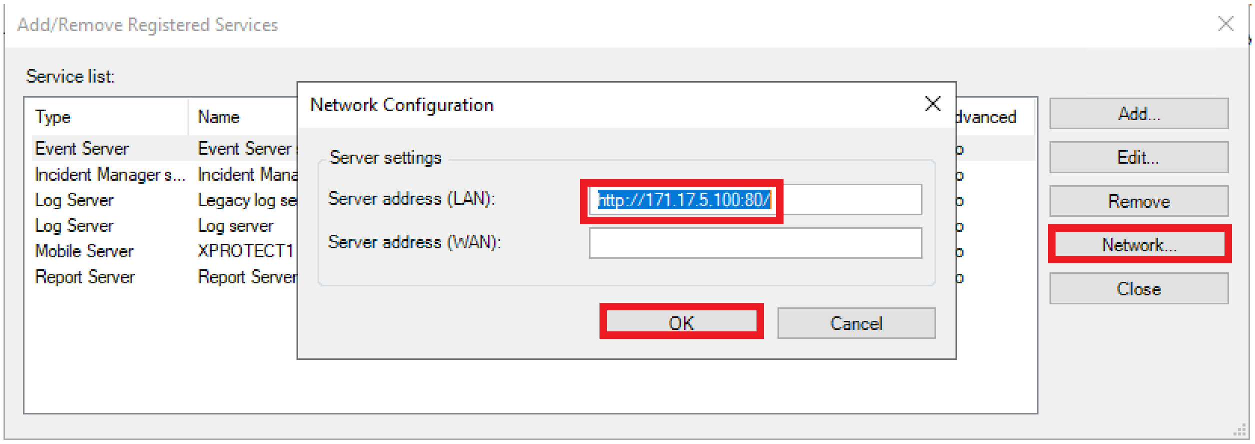


Add/Remove Registered Services

Service list:

Type	Name	URLs	Trusted	Description	Advanced
Event Server	Event Server serv...	http://171.17.5.100:22331/	Yes	Event Server Service	No
Incident Manager s...	Incident Manager ...	http://171.17.5.100/Inciden...	Yes	Incident Manager service r...	No
Log Server	Legacy log server	http://xprotect1:22337/Leg...	Yes	The legacy log server for h...	No
Log Server	Log server	http://171.17.5.100:22337/...	Yes	The log server for handling ...	No
Mobile Server	XPROTECT1	http://xprotect1:8081/	Yes	Mobile Server Service	No
Report Server	Report Server	http://171.17.5.100/Reporti...	Yes	Report Server registered by...	No

c. Click on ‘Network’ and add the Virtual IP address to the Server address (LAN):



Add/Remove Registered Services

Service list:

Type	Name
Event Server	Event Server
Incident Manager s...	Incident Mana
Log Server	Legacy log se
Log Server	Log server
Mobile Server	XPROTECT1
Report Server	Report Server

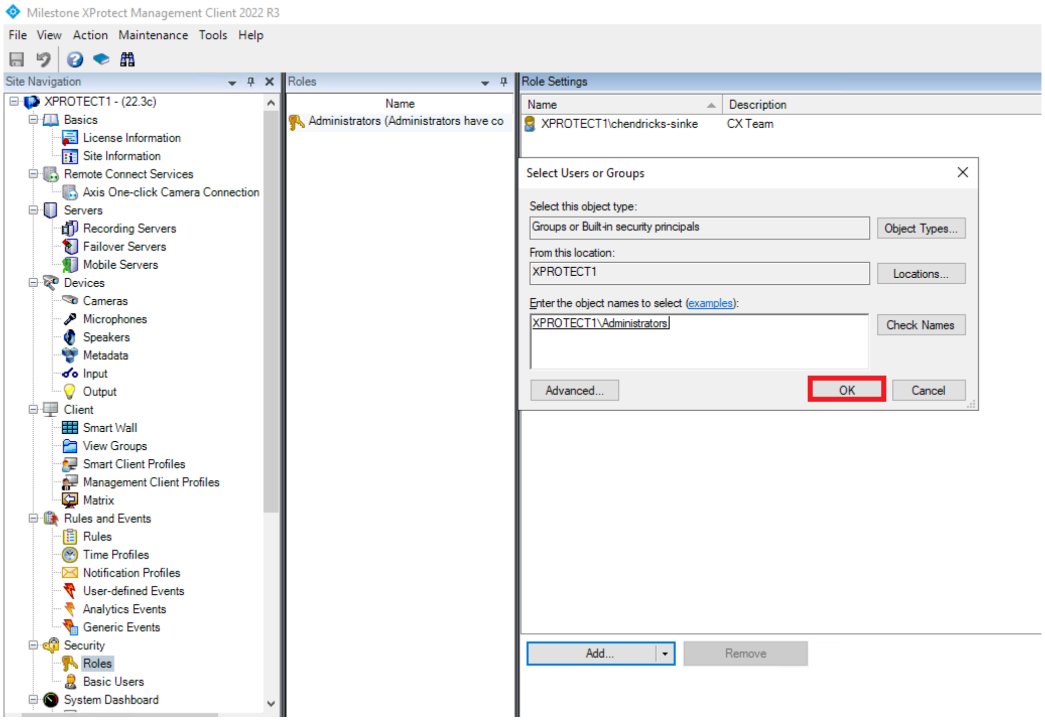
Network Configuration

Server settings

Server address (LAN): http://171.17.5.100:80/

Server address (WAN):

8. Add Administrator roles for failover
    a. Add 'Administrators' group from windows



Milestone XProtect Management Client 2022 R3

Roles

Name
Administrators (Administrators have co

Role Settings

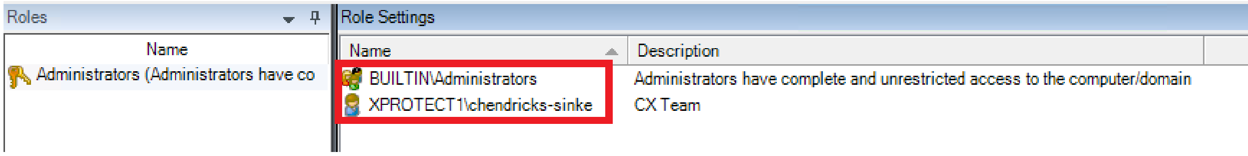
Name	Description
XPROTECT1\chendricks-sinke	CX Team

Select Users or Groups

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

From this location: XPROTECT1

Enter the object names to select (examples): XPROTECT1\Administrators



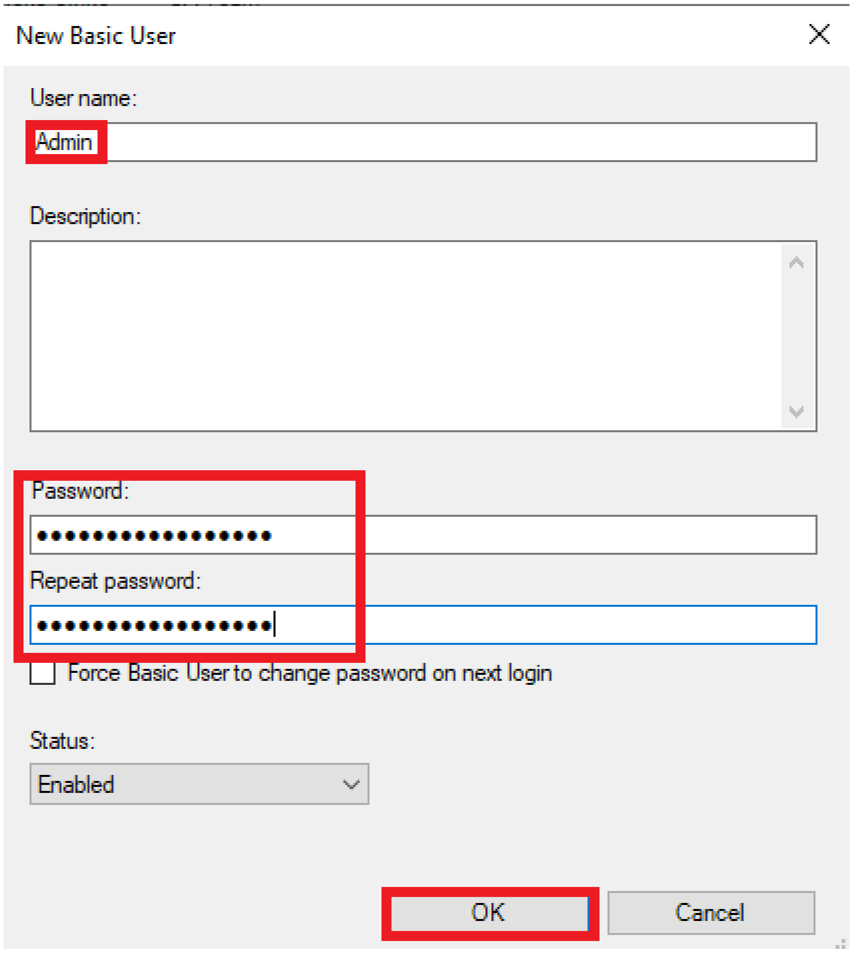
Roles

Name
Administrators (Administrators have co

Role Settings

Name	Description
BUILTIN\Administrators	Administrators have complete and unrestricted access to the computer/domain
XPROTECT1\chendricks-sinke	CX Team

b. Click ‘New Basic User’ and add a local ‘admin’ account



New Basic User

User name: Admin

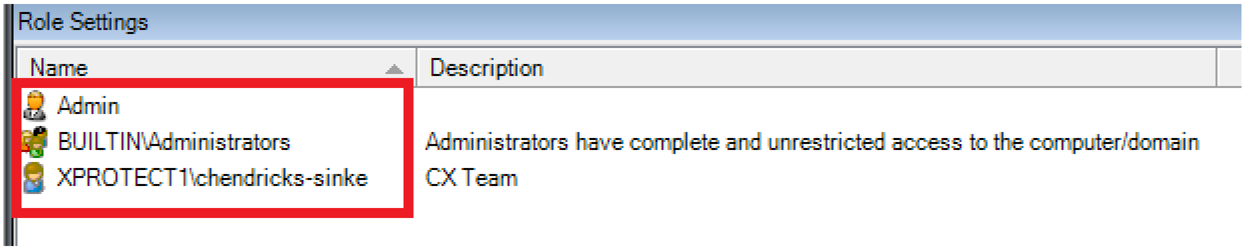
Description:

Password: ••••••••••••••••••

Repeat password: ••••••••••••••••••

□ Force Basic User to change password on next login

Status: Enabled



Role Settings

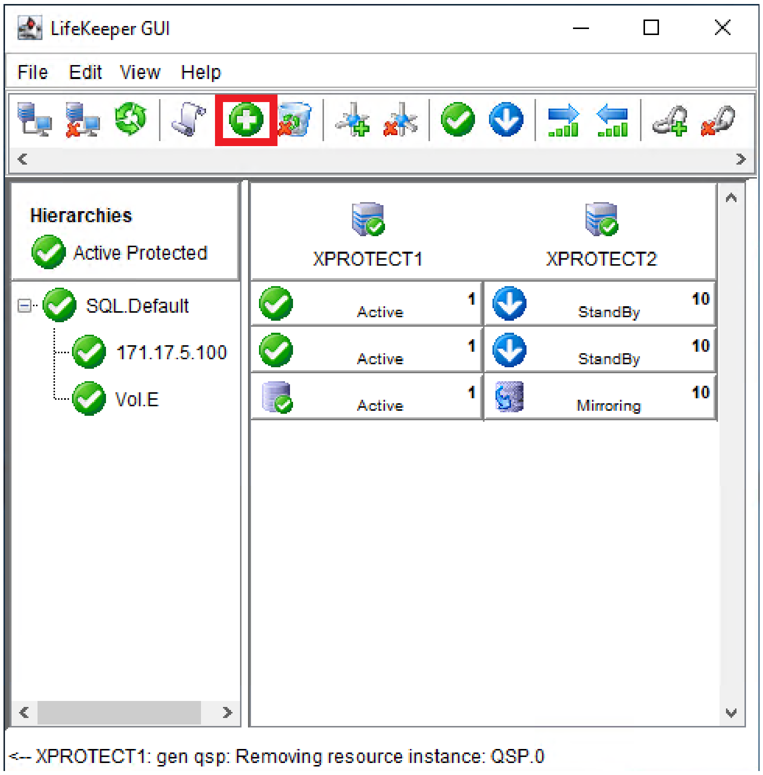
Name	Description
Admin	
BUILTIN\Administrators	Administrators have complete and unrestricted access to the computer/domain
XPROTECT1\chendricks-sinke	CX Team

9. Repeat steps 1-5 on XPROTECT2

Using LifeKeeper to cluster XProtect:

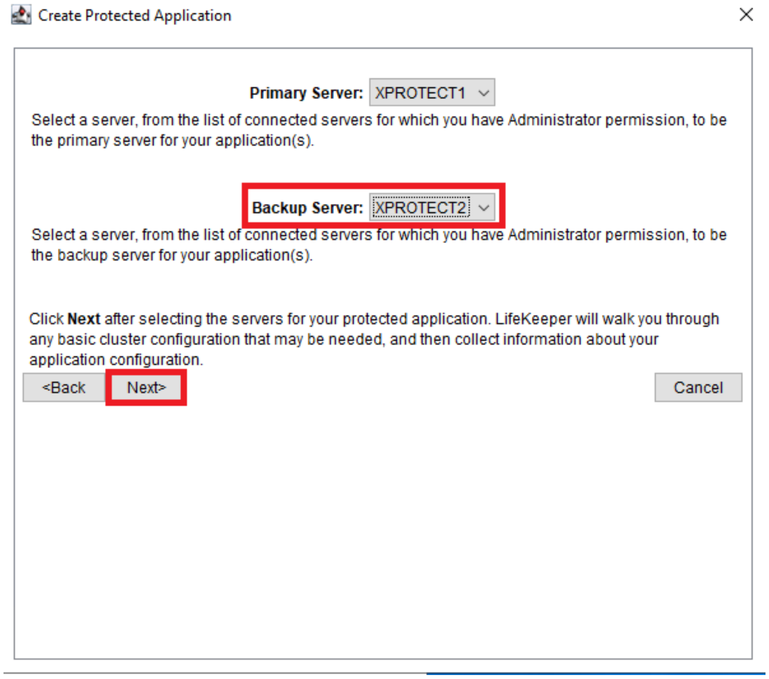
Make sure all XProtect services are running on XPORTECT1 before following the below steps

1. Choose Create New Resource Hierarchy



<-- XPROTECT1: gen qsp: Removing resource instance: QSP.0

2. Choose backup server



Primary Server: XPROTECT1

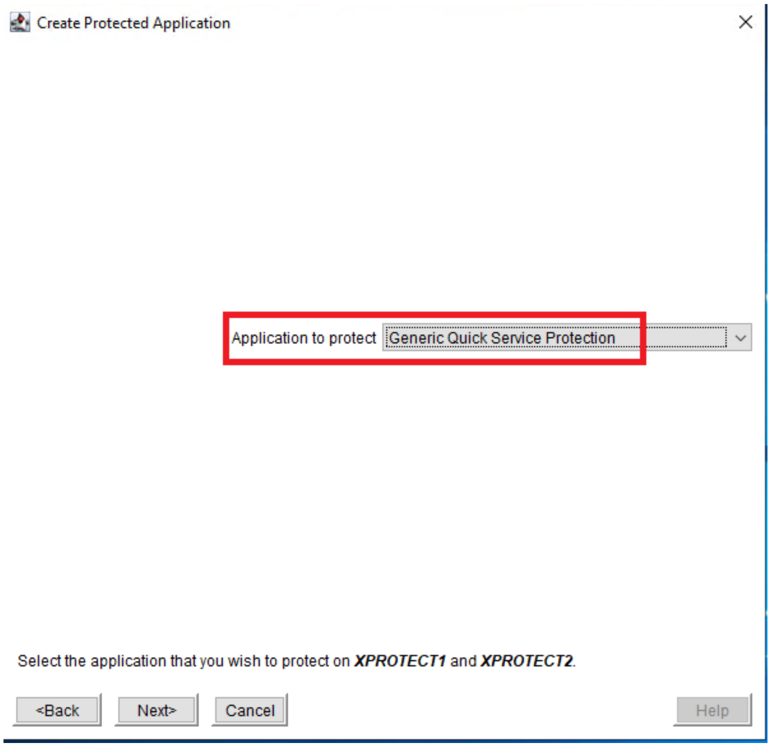
Select a server, from the list of connected servers for which you have Administrator permission, to be the primary server for your application(s).

Backup Server: XPROTECT2

Select a server, from the list of connected servers for which you have Administrator permission, to be the backup server for your application(s).

Click **Next** after selecting the servers for your protected application. LifeKeeper will walk you through any basic cluster configuration that may be needed, and then collect information about your application configuration.

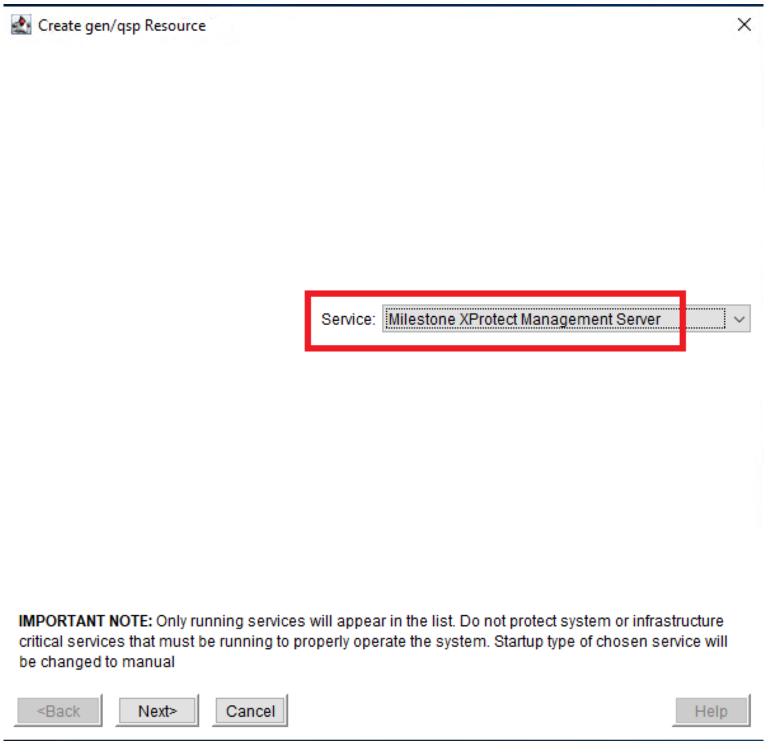
3. Choose Generic Quick Service Protection for application to protect



Application to protect: Generic Quick Service Protection

Select the application that you wish to protect on ***XPROTECT1*** and ***XPROTECT2***.

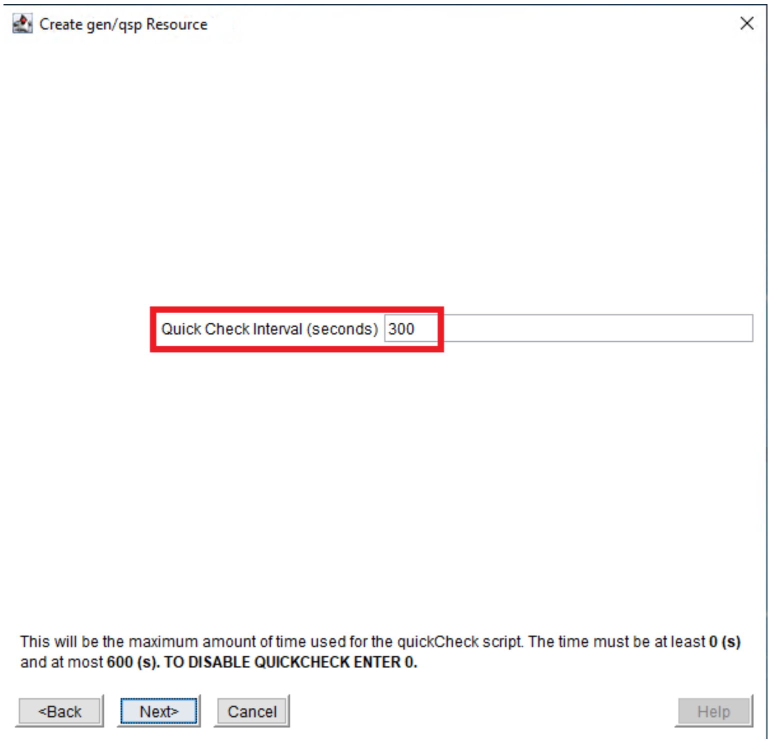
4. Choose service to protect



Service: Milestone XProtect Management Server

IMPORTANT NOTE: Only running services will appear in the list. Do not protect system or infrastructure critical services that must be running to properly operate the system. Startup type of chosen service will be changed to manual

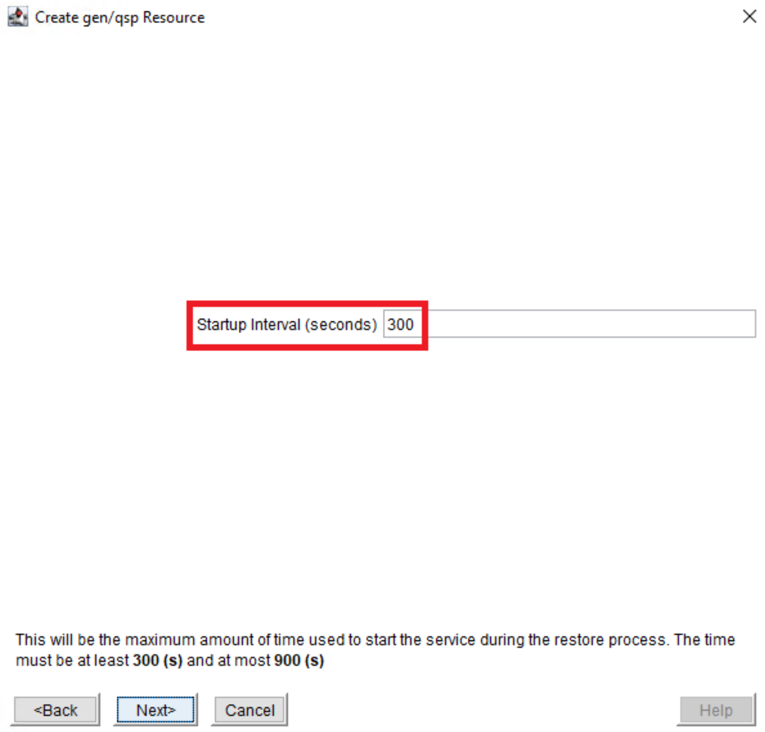
5. Set quick check interval



Quick Check Interval (seconds) 300

This will be the maximum amount of time used for the quickCheck script. The time must be at least **0 (s)** and at most **600 (s). TO DISABLE QUICKCHECK ENTER 0.**

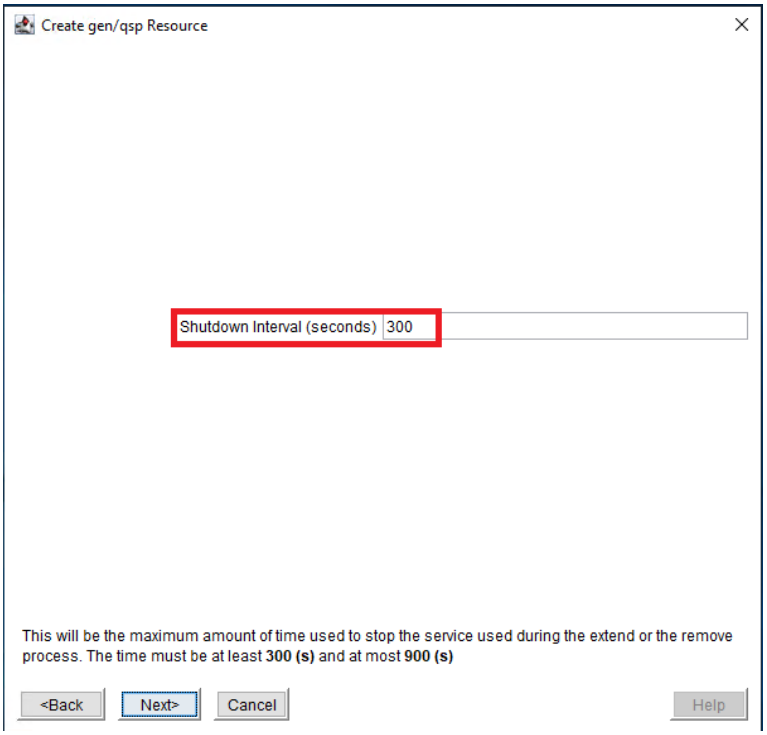
6. Set startup interval



Startup Interval (seconds) 300

This will be the maximum amount of time used to start the service during the restore process. The time must be at least **300 (s)** and at most **900 (s)**

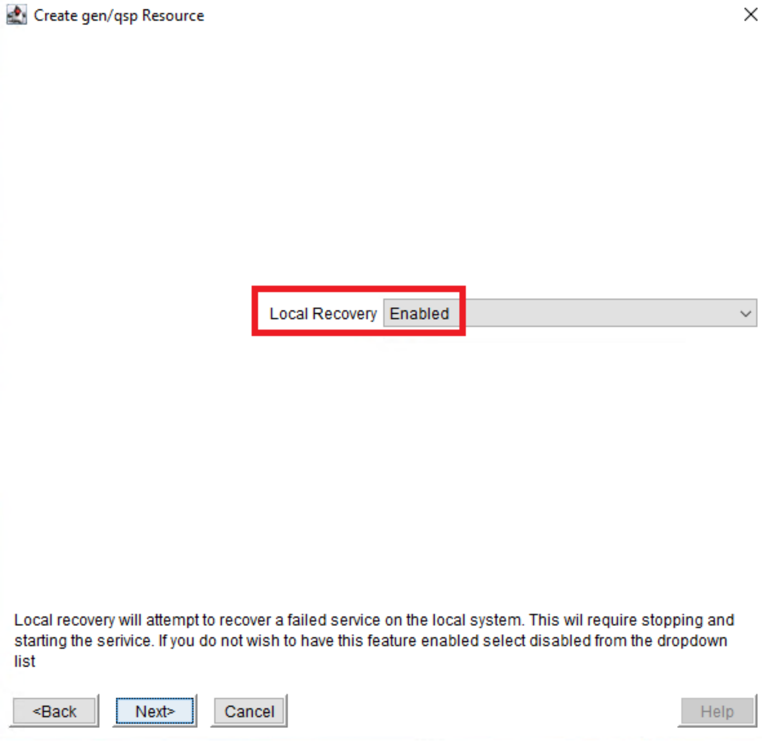
7. Set shutdown interval



Shutdown Interval (seconds) 300

This will be the maximum amount of time used to stop the service used during the extend or the remove process. The time must be at least **300 (s)** and at most **900 (s)**

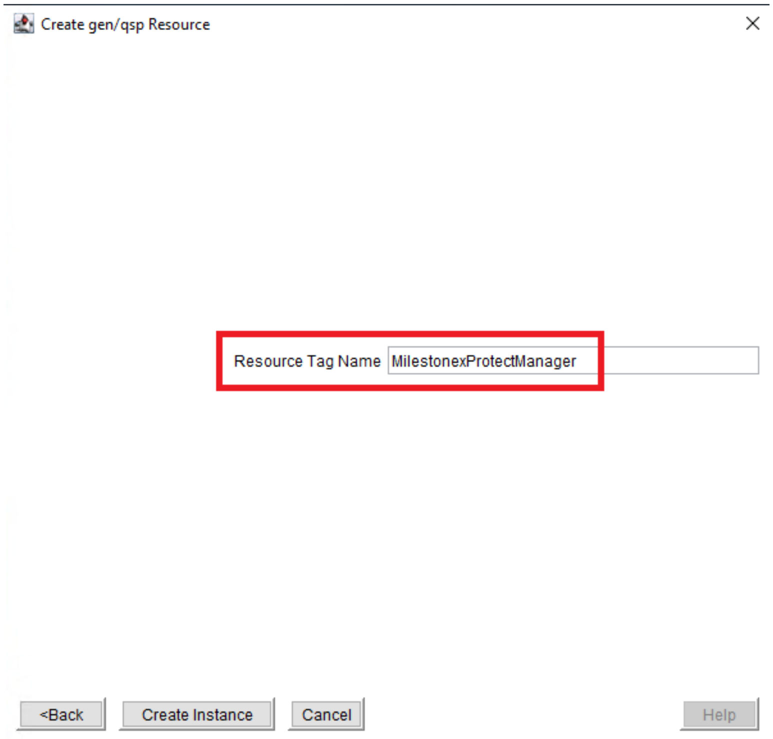
8. Enable local recovery



Local Recovery Enabled

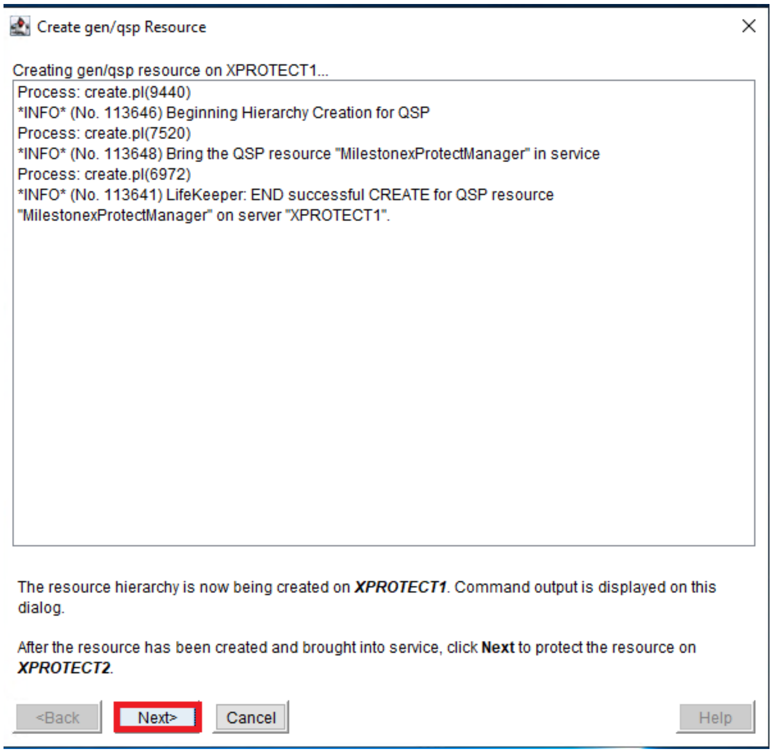
Local recovery will attempt to recover a failed service on the local system. This wil require stopping and starting the serivice. If you do not wish to have this feature enabled select disabled from the dropdown list

9. Choose a tag name



Resource Tag Name MilestonexProtectManager

10. Verify the creation of the resource was successful



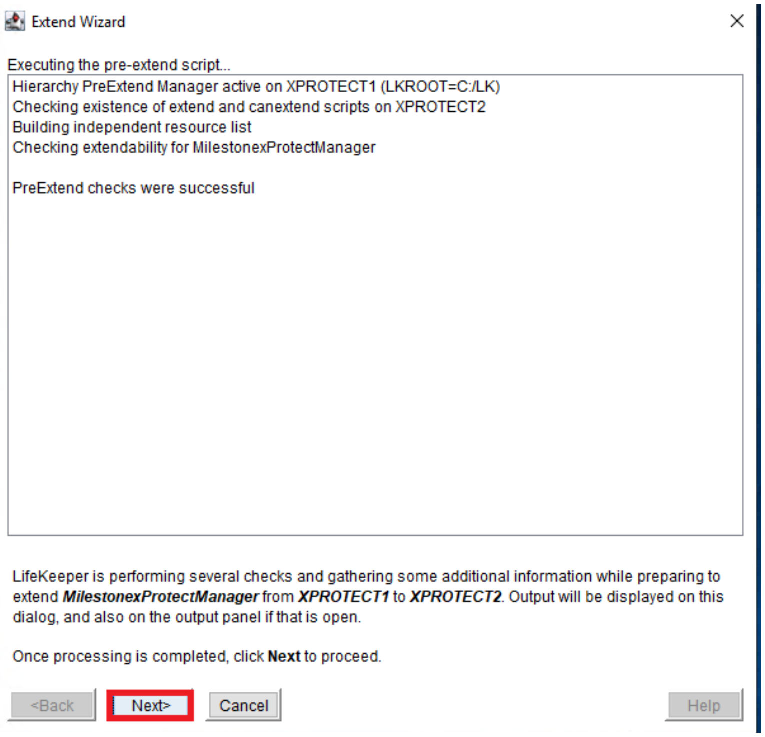
Creating gen/qsp resource on XPROTECT1...

```
Process: create.pl(9440)
*INFO* (No. 113646) Beginning Hierarchy Creation for QSP
Process: create.pl(7520)
*INFO* (No. 113648) Bring the QSP resource "MilestonexProtectManager" in service
Process: create.pl(6972)
*INFO* (No. 113641) LifeKeeper: END successful CREATE for QSP resource
"MilestonexProtectManager" on server "XPROTECT1".
```

The resource hierarchy is now being created on ***XPROTECT1***. Command output is displayed on this dialog.

After the resource has been created and brought into service, click **Next** to protect the resource on ***XPROTECT2***.

11. Run extend checks



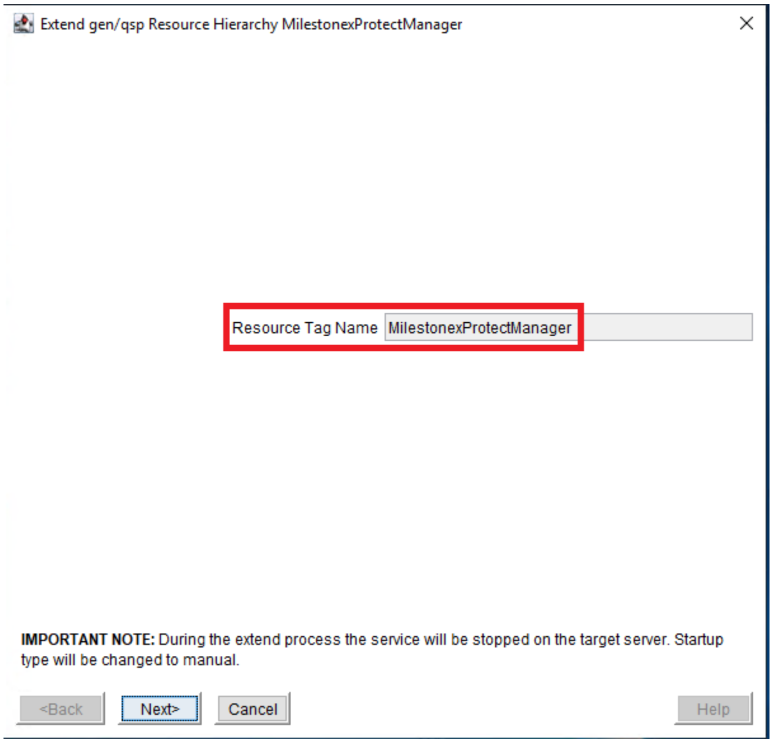
Executing the pre-extend script...

```
Hierarchy PreExtend Manager active on XPROTECT1 (LKROOT=C:/LK)
Checking existence of extend and canextend scripts on XPROTECT2
Building independent resource list
Checking extendability for MilestonexProtectManager

PreExtend checks were successful
```

LifeKeeper is performing several checks and gathering some additional information while preparing to extend ***MilestonexProtectManager*** from ***XPROTECT1*** to ***XPROTECT2***. Output will be displayed on this dialog, and also on the output panel if that is open.

Once processing is completed, click **Next** to proceed.

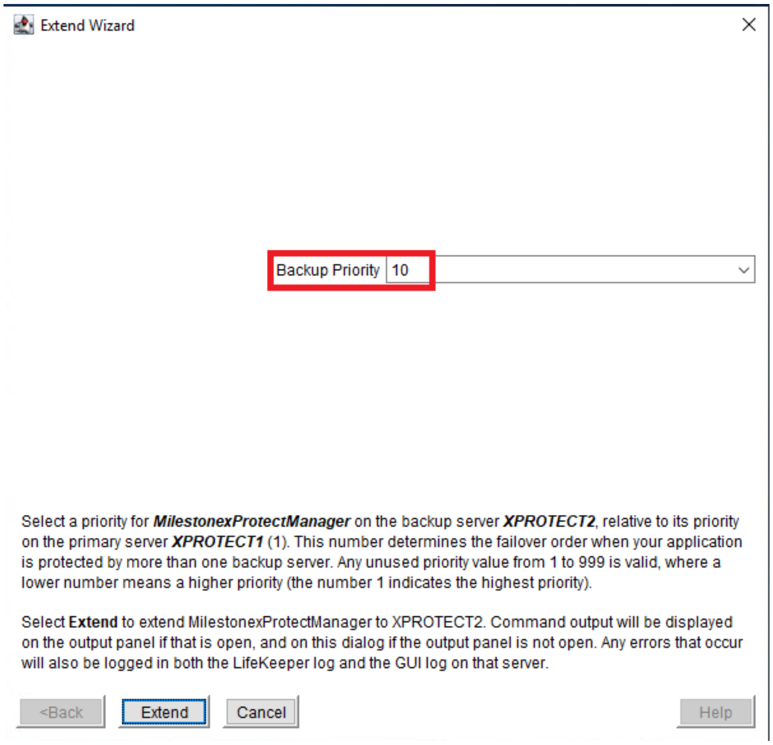
12. Choose extended resource tag name



Resource Tag Name MilestonexProtectManager

IMPORTANT NOTE: During the extend process the service will be stopped on the target server. Startup type will be changed to manual.

13. Set backup priority

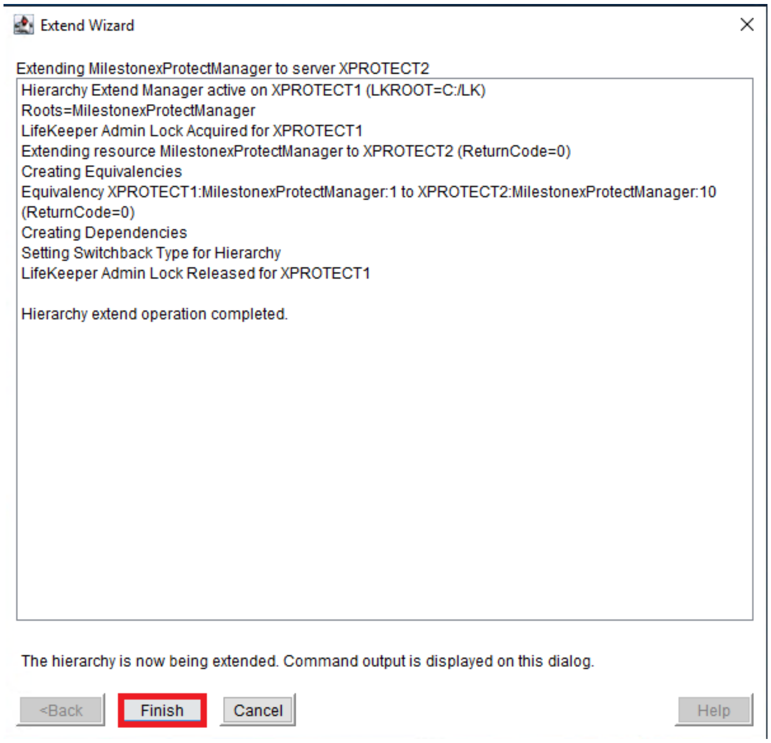


Backup Priority 10

Select a priority for ***MilestonexProtectManager*** on the backup server ***XPROTECT2***, relative to its priority on the primary server ***XPROTECT1*** (1). This number determines the failover order when your application is protected by more than one backup server. Any unused priority value from 1 to 999 is valid, where a lower number means a higher priority (the number 1 indicates the highest priority).

Select **Extend** to extend MilestonexProtectManager to XPROTECT2. Command output will be displayed on the output panel if that is open, and on this dialog if the output panel is not open. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on that server.

14. Verify extend was successful

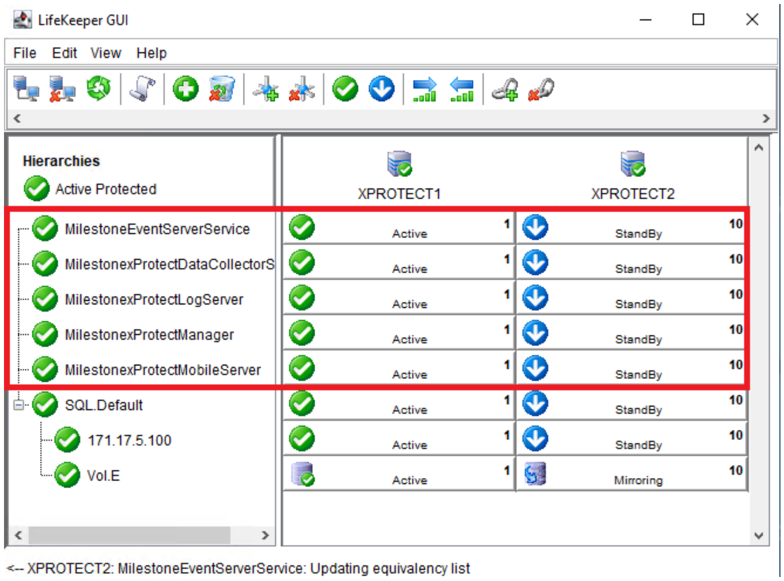


Extending MilestonexProtectManager to server XPROTECT2

```
Hierarchy Extend Manager active on XPROTECT1 (LKROOT=C:/LK)
Roots=MilestonexProtectManager
LifeKeeper Admin Lock Acquired for XPROTECT1
Extending resource MilestonexProtectManager to XPROTECT2 (ReturnCode=0)
Creating Equivalencies
Equivalency XPROTECT1:MilestonexProtectManager:1 to XPROTECT2:MilestonexProtectManager:10
(ReturnCode=0)
Creating Dependencies
Setting Switchback Type for Hierarchy
LifeKeeper Admin Lock Released for XPROTECT1

Hierarchy extend operation completed.
```

The hierarchy is now being extended. Command output is displayed on this dialog.

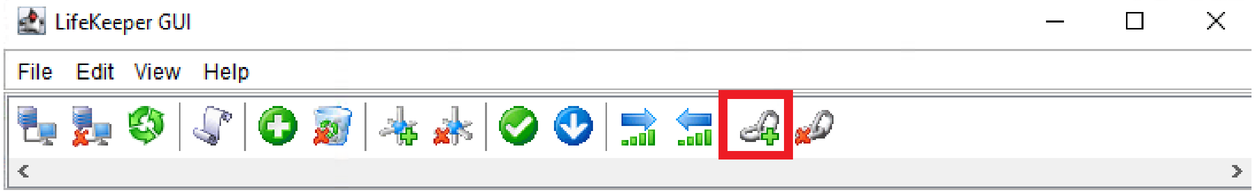
15. Repeat steps 1-14 for each of the Milestone services you wish to protect end result should look similar to this

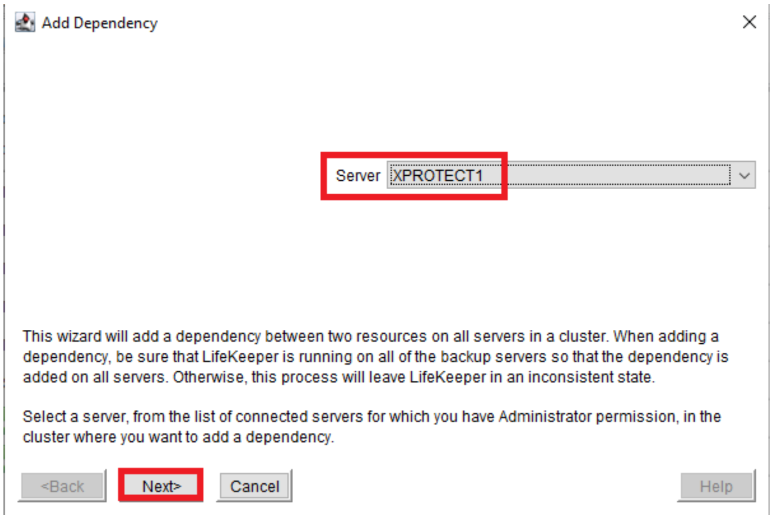


Hierarchies	XPROTECT1		XPROTECT2	
Active Protected				
MilestoneEventServerService	Active	1	StandBy	10
MilestonexProtectDataCollectorS	Active	1	StandBy	10
MilestonexProtectLogServer	Active	1	StandBy	10
MilestonexProtectManager	Active	1	StandBy	10
MilestonexProtectMobileServer	Active	1	StandBy	10
SQL.Default	Active	1	StandBy	10
171.17.5.100	Active	1	StandBy	10
Vol.E	Active	1	Mirroring	10

<-- XPROTECT2: MilestoneEventServerService: Updating equivalency list

16. Make a milestone resource a child of the Milestone XProtect Manager

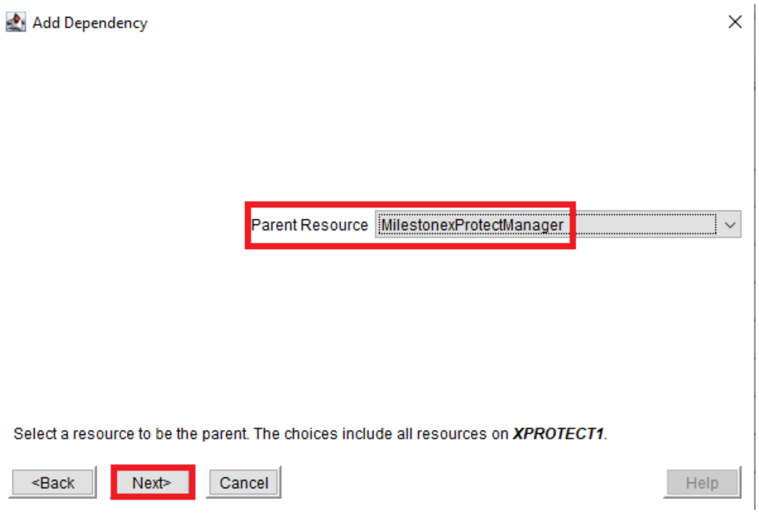




Server XPROTECT1

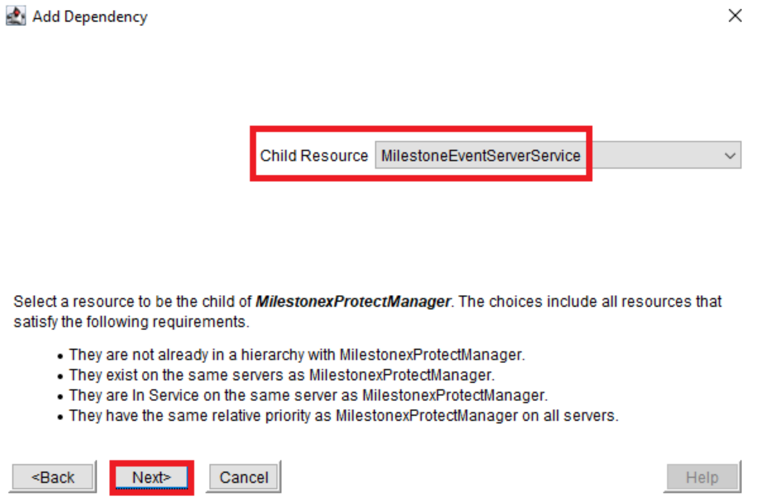
This wizard will add a dependency between two resources on all servers in a cluster. When adding a dependency, be sure that LifeKeeper is running on all of the backup servers so that the dependency is added on all servers. Otherwise, this process will leave LifeKeeper in an inconsistent state.

Select a server, from the list of connected servers for which you have Administrator permission, in the cluster where you want to add a dependency.



Parent Resource: MilestonexProtectManager

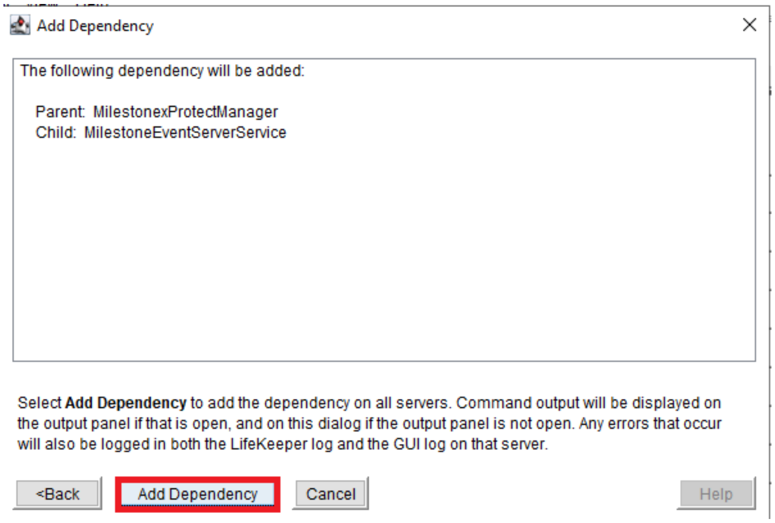
Select a resource to be the parent. The choices include all resources on ***XPROTECT1***.



Child Resource: MilestoneEventServerService

Select a resource to be the child of ***MilestonexProtectManager***. The choices include all resources that satisfy the following requirements.

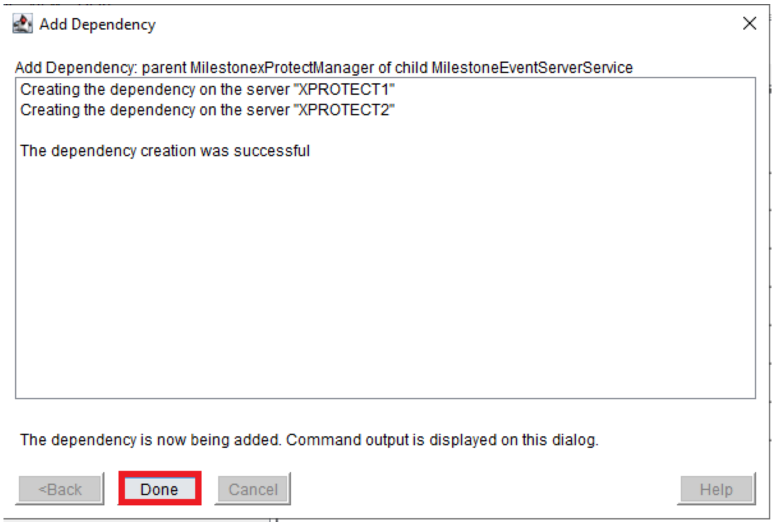
- They are not already in a hierarchy with MilestonexProtectManager.
- They exist on the same servers as MilestonexProtectManager.
- They are In Service on the same server as MilestonexProtectManager.
- They have the same relative priority as MilestonexProtectManager on all servers.



The following dependency will be added:

Parent: MilestonexProtectManager
Child: MilestoneEventServerService

Select **Add Dependency** to add the dependency on all servers. Command output will be displayed on the output panel if that is open, and on this dialog if the output panel is not open. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on that server.

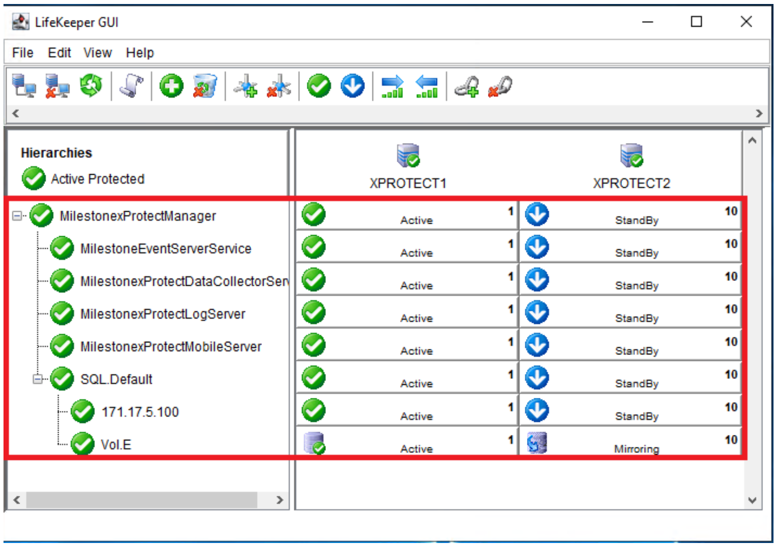


Add Dependency: parent MilestonexProtectManager of child MilestoneEventServerService

```
Creating the dependency on the server "XPROTECT1"
Creating the dependency on the server "XPROTECT2"

The dependency creation was successful
```

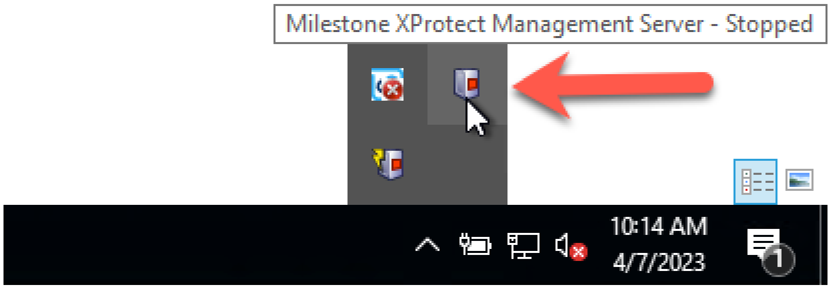
The dependency is now being added. Command output is displayed on this dialog.

17. Repeat this process for every Milestone resource as well as the SQL resource, the end result should look like below



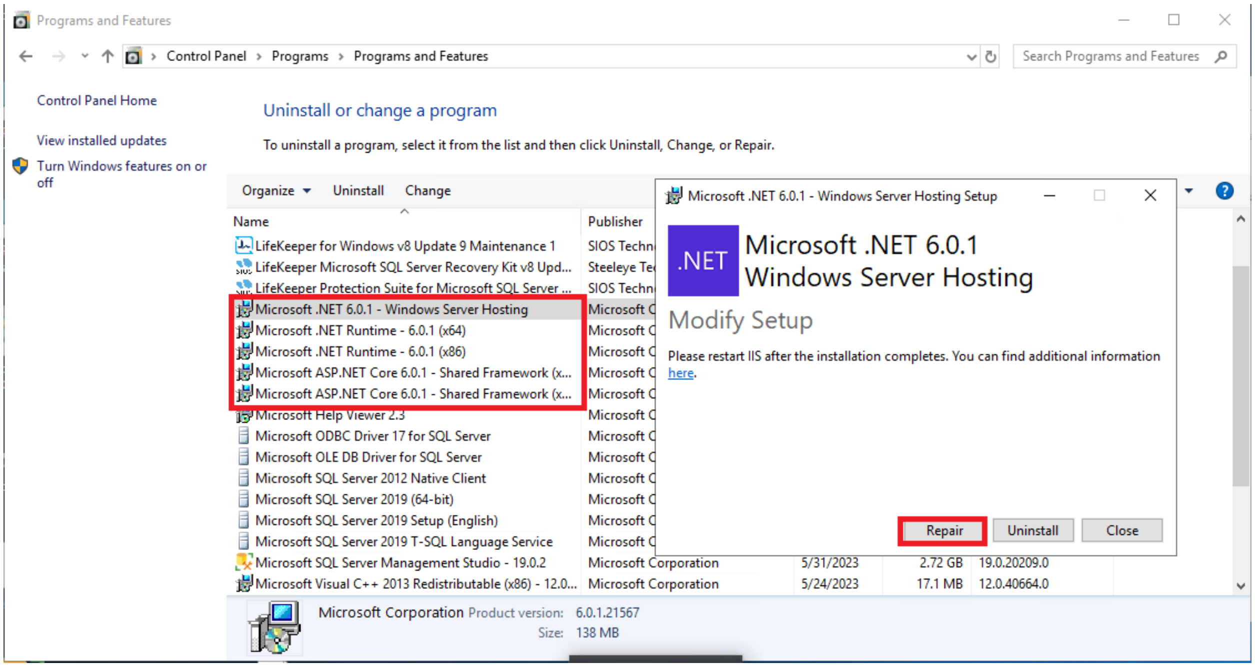
Hierarchies	XPROTECT1		XPROTECT2	
MilestonexProtectManager	Active	1	StandBy	10
MilestoneEventServerService	Active	1	StandBy	10
MilestonexProtectDataCollectorSen	Active	1	StandBy	10
MilestonexProtectLogServer	Active	1	StandBy	10
MilestonexProtectMobileServer	Active	1	StandBy	10
SQL.Default	Active	1	StandBy	10
171.17.5.100	Active	1	StandBy	10
Vol.E	Active	1	Mirroring	10

NOTE: If your first switchover fails with XPROTECT2 being stuck in the 'starting' stage in the system tray icon, please follow the below instructions.



Milestone XProtect Management Server - Stopped

1. Run a repair on each of the Microsoft ASP.Net modules on XPROTECT2 as shown below



Programs and Features

Control Panel › Programs › Programs and Features

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher			
LifeKeeper for Windows v8 Update 9 Maintenance 1	SIOS Techn			
LifeKeeper Microsoft SQL Server Recovery Kit v8 Upd...	Steeleye Te			
LifeKeeper Protection Suite for Microsoft SQL Server ...	SIOS Techn			
Microsoft .NET 6.0.1 - Windows Server Hosting	Microsoft C			
Microsoft .NET Runtime - 6.0.1 (x64)	Microsoft C			
Microsoft .NET Runtime - 6.0.1 (x86)	Microsoft C			
Microsoft ASP.NET Core 6.0.1 - Shared Framework (x...	Microsoft C			
Microsoft ASP.NET Core 6.0.1 - Shared Framework (x...	Microsoft C			
Microsoft Help Viewer 2.3	Microsoft C			
Microsoft ODBC Driver 17 for SQL Server	Microsoft C			
Microsoft OLE DB Driver for SQL Server	Microsoft C			
Microsoft SQL Server 2012 Native Client	Microsoft C			
Microsoft SQL Server 2019 (64-bit)	Microsoft C			
Microsoft SQL Server 2019 Setup (English)	Microsoft C			
Microsoft SQL Server 2019 T-SQL Language Service	Microsoft C			
Microsoft SQL Server Management Studio - 19.0.2	Microsoft Corporation	5/31/2023	2.72 GB	19.0.20209.0
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0...	Microsoft Corporation	5/24/2023	17.1 MB	12.0.40664.0

Microsoft .NET 6.0.1 - Windows Server Hosting Setup

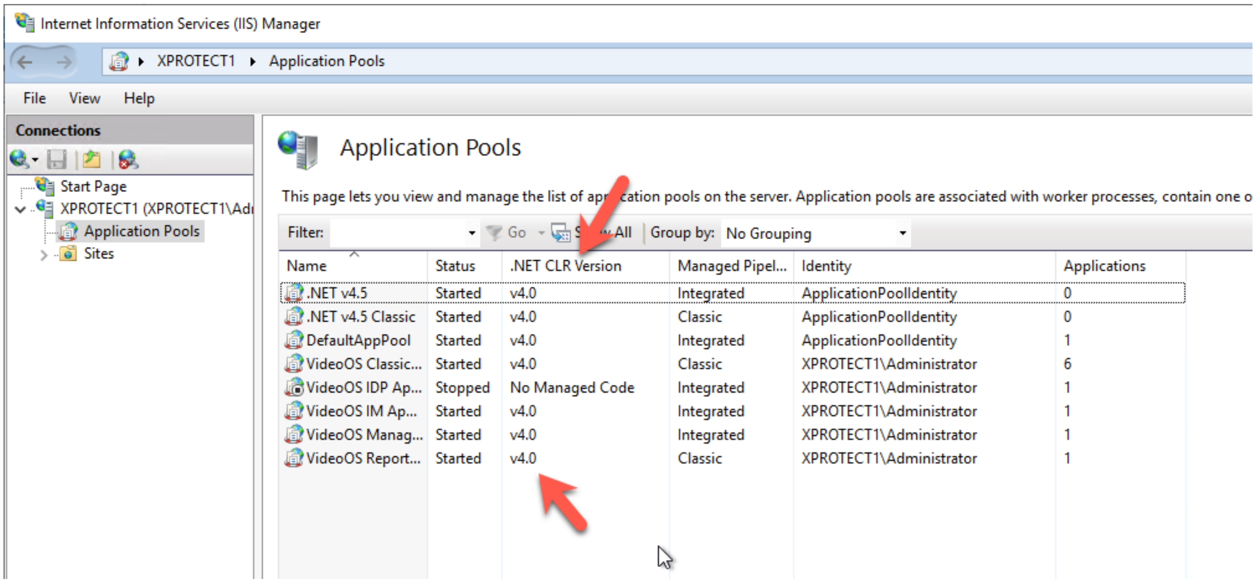
.NET Microsoft .NET 6.0.1 Windows Server Hosting

Modify Setup

Please restart IIS after the installation completes. You can find additional information here.

Microsoft Corporation Product version: 6.0.1.21567
Size: 138 MB

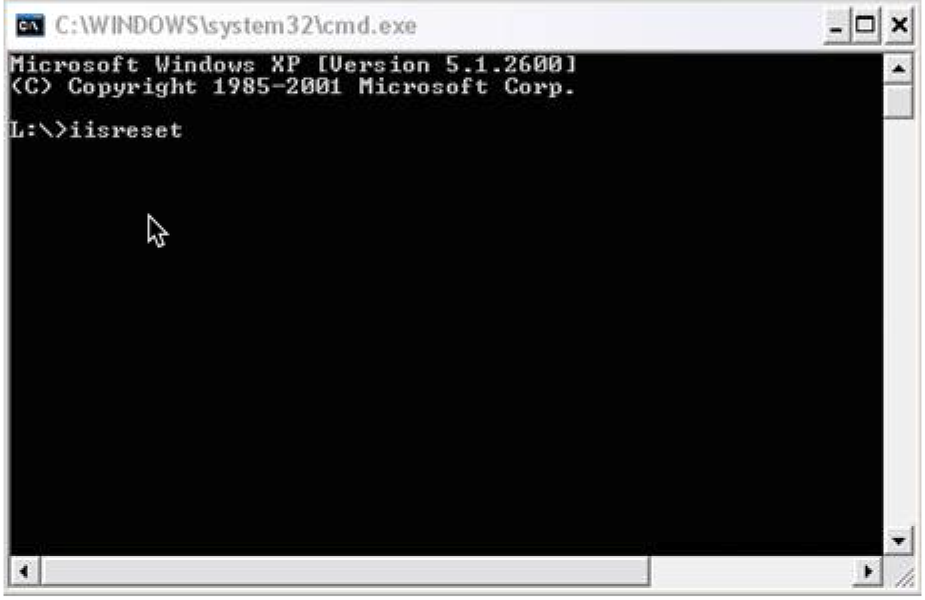
2. You must also ensure all the Application Pools use .Net v4.0, as shown below



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one o

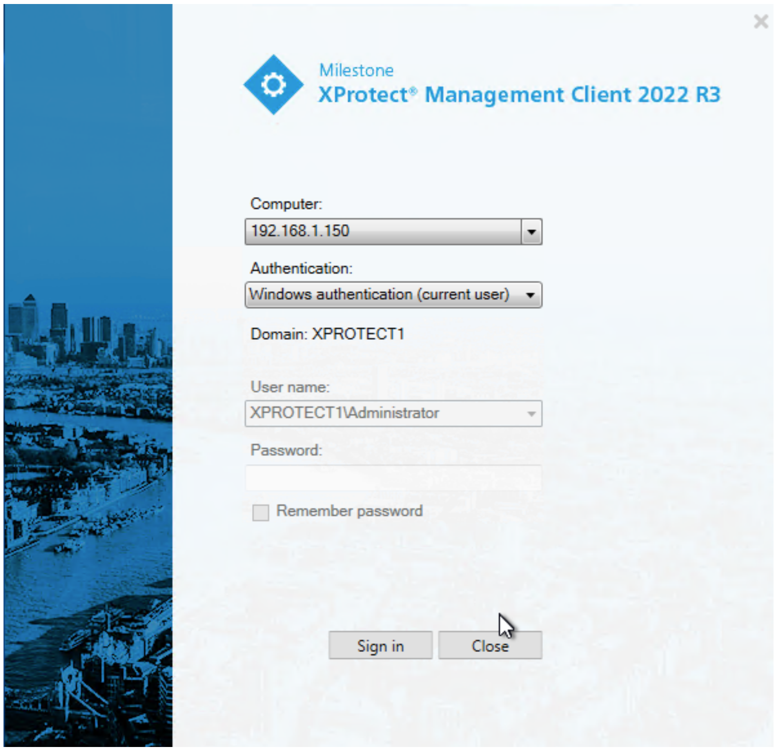
Name	Status	.NET CLR Version	Managed Pipel...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	1
VideoOS Classic...	Started	v4.0	Classic	XPROTECT1\Administrator	6
VideoOS IDP Ap...	Stopped	No Managed Code	Integrated	XPROTECT1\Administrator	1
VideoOS IM Ap...	Started	v4.0	Integrated	XPROTECT1\Administrator	1
VideoOS Manag...	Started	v4.0	Integrated	XPROTECT1\Administrator	1
VideoOS Report...	Started	v4.0	Classic	XPROTECT1\Administrator	1

3. Reset IIS on XPROTECT2



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

L:\>iisreset
```

4. When you open the XProtect Management Client, connect directly to the Virtual IP address.



Milestone
XProtect® Management Client 2022 R3

Computer: 192.168.1.150

Authentication: Windows authentication (current user)

Domain: XPROTECT1

User name: XPROTECT1\Administrator

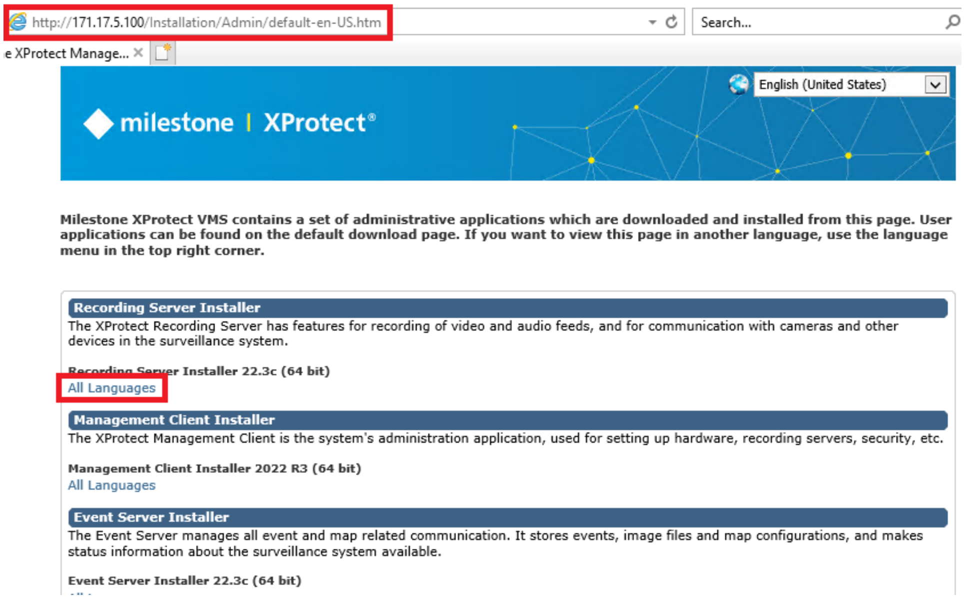
Password:

□ Remember password

Step 7 - Install the Recording Server

Follow the given instructions https://developer.milestonesys.com/s/article/XProtect-Corporate-How-to-install-the-recording-server .

Download Installer software



http://171.17.5.100/Installation/Admin/default-en-US.htm

Milestone XProtect VMS contains a set of administrative applications which are downloaded and installed from this page. User applications can be found on the default download page. If you want to view this page in another language, use the language menu in the top right corner.

Recording Server Installer

The XProtect Recording Server has features for recording of video and audio feeds, and for communication with cameras and other devices in the surveillance system.

Recording Server Installer 22.3c (64 bit)

All Languages

Management Client Installer

The XProtect Management Client is the system's administration application, used for setting up hardware, recording servers, security, etc.

Management Client Installer 2022 R3 (64 bit)

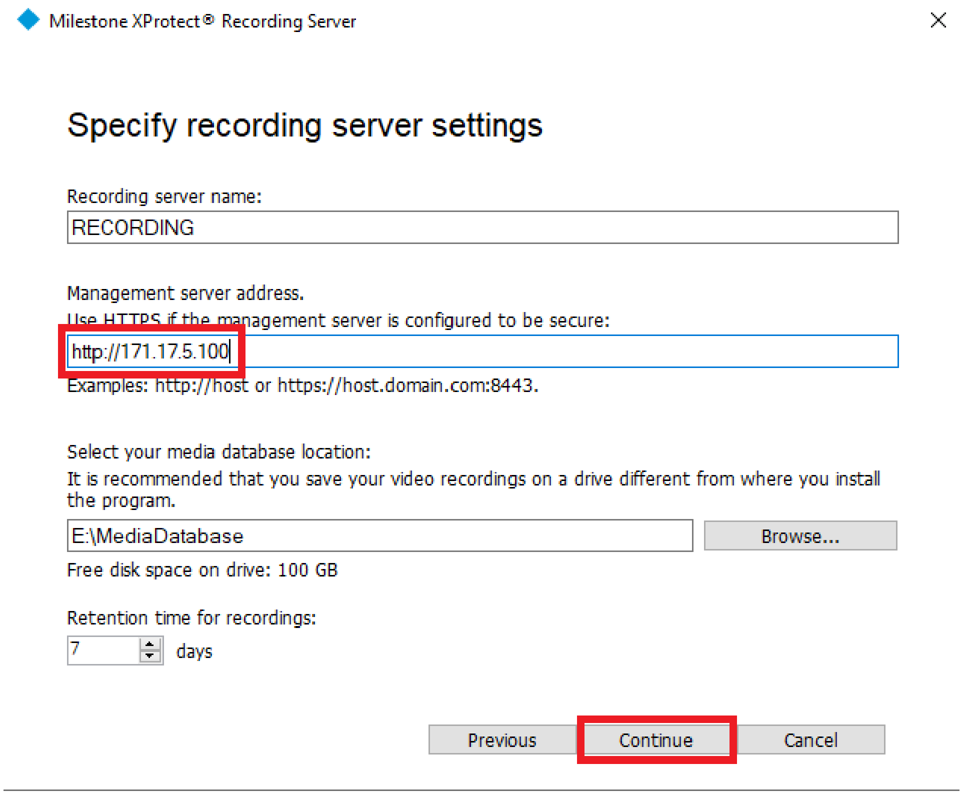
All Languages

Event Server Installer

The Event Server manages all event and map related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.

Event Server Installer 22.3c (64 bit)

Also, install the recording server, specifying the virtual IP address in the installation URL.



Specify recording server settings

Recording server name:

RECORDING

Management server address.

Use HTTPS if the management server is configured to be secure:

http://171.17.5.100

Examples: http://host or https://host.domain.com:8443.

Select your media database location:

It is recommended that you save your video recordings on a drive different from where you install the program.

E:\MediaDatabase

Free disk space on drive: 100 GB

Retention time for recordings:

7 days

Step 8 - Test failover

The minimum requirements for testing the cluster are as follows:

- Perform a manual switchover of the cluster from XPROTECT1 to XPROTECT2, and back to XPROTECT1
- Pull the power cord on the active cluster node. The backup cluster node should recover the protected resources. NOTE: Performing a planned shutdown, or pushing the power button to cause a shutdown, is not the same. The default behavior of a server being shutdown is to NOT failover the resources. This is controlled by the Shutdown Strategy settings of the cluster.
- Manually stop one of the protected Windows services. The default behavior is that LifeKeeper will automatically restart that service.
- Temporarily disable and stop one of the protected Windows services on the active cluster node. LifeKeeper will detect the failure, and with local recovery not being able to successfully restart the service, a failover to the secondary node will be initiated.

In all of the above test, you should be able to open the XProtect Management Client, and connect directly to the Virtual IP address.

About SIOS Technology
SIOS Technology Corp. high availability and disaster recovery solutions ensure availability and eliminate data loss for critical Windows and Linux applications operating across physical, virtual, cloud, and hybrid cloud environments. SIOS clustering software is essential for any IT infrastructure with applications requiring a high degree of resiliency, ensuring uptime without sacrificing performance or data – protecting businesses from local failures and regional outages, planned and unplanned. Founded in 1999, SIOS Technology Corp. (https://us.sios.com) is headquartered in San Mateo, California, with offices worldwide.