# System Requirements

**Note** There are numerous configurations possible using different hardware setups. Consult the respective Microsoft and Veritas Hardware Compatibility Lists (HCLs).

**Note** Although we make every attempt to ensure the availability of third-party hardware and software platforms specified for Security Manager, we reserve the right to change or modify system requirements due to third-party vendor product availability or changes that are beyond our control.

This chapter describes reference configurations for installing Security Manager in an HA or DR environment. This chapter contains the following sections:



# Hardware Requirements for a Single-Node Site

To install Security Manager in a single-node HA environment, you can configure a fault-tolerant storage array or use internal disks.

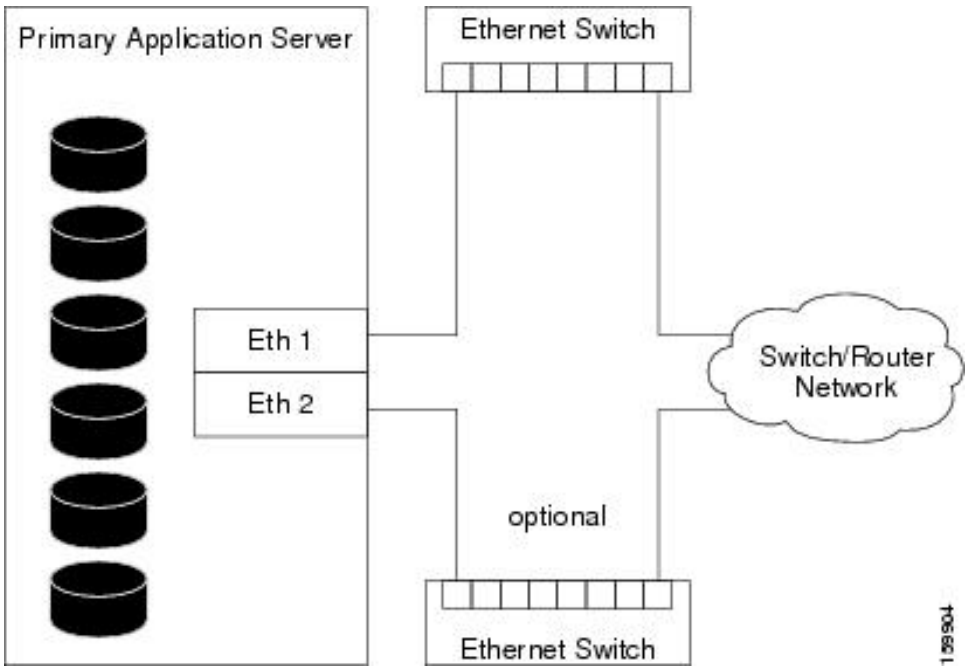
The following are the server hardware specifications for a single-node site:

- Server which meets the basic processor and RAM requirements as described in the *Installation Guide for Cisco Security Manager 4.25*
- Minimum of one Ethernet interface (two recommended)
- Minimum of two physical drives (six recommended)

The Figure 1: Ethernet Connection for a Single-Node Site shows using two Ethernet connections from the server to the switch/router network for redundancy. If an Ethernet port or switch fails, communication to the

server is maintained. If this level of network redundancy is not required, you can use a single connection to the switch/router network (that is, Eth 2 and its associated Ethernet switch are optional).

***Figure 1: Ethernet Connection for a Single-Node Site***




# Hardware Requirements for a Dual-Node Site

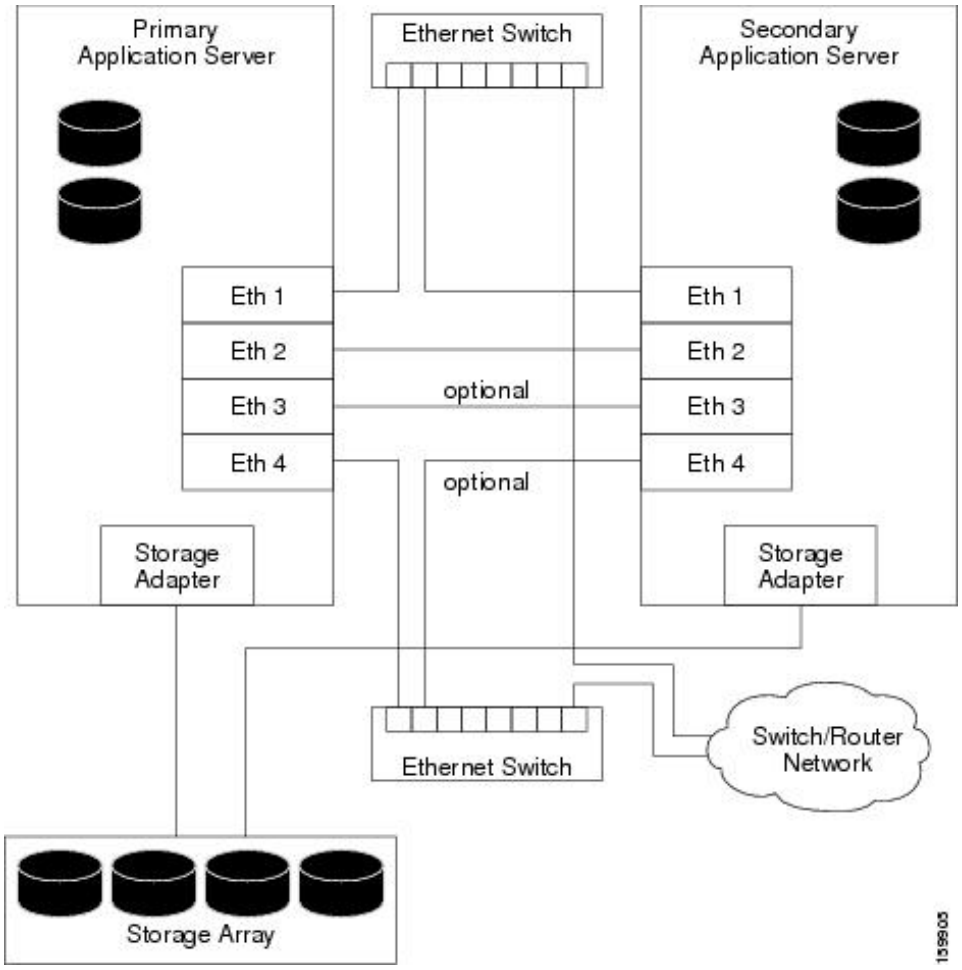
To install Security Manager in a dual-node HA environment, you need two servers that can access a shared storage array.

The following are the server hardware specifications for a dual-node site:

- Servers that meets the basic processor and RAM requirements, as described in the *Installation Guide for Cisco Security Manager 4.25*
- Minimum of two Ethernet interfaces (four recommended)
- Minimum of one internal physical drive (two recommended)
- Minimum of one external drive (two recommended; four recommended if using replication)

Figure 2: Ethernet and Storage Connections for a Dual-Node Site depicts the configuration of a dual-node site showing the Ethernet and external storage connections. Two Ethernet connections are used from the server to the switch/router network for redundancy. If an Ethernet port or switch fails, communications to the server is maintained. If this level of network redundancy is not required, you can use a single connection to the switch/router network (that is, Eth 4 and its associated Ethernet switch are optional). Two direct Ethernet connections are made between the servers for cluster heartbeat communications, although second heartbeat connection (Eth 3) is optional.

*Figure 2: Ethernet and Storage Connections for a Dual-Node Site*




# Software Requirements for a Local Redundancy Configuration

The following software is required to install Security Manager in a local redundancy HA configuration:

- Cisco Security Management Suite 4.25
- Microsoft Windows Server 2019, Standard and Datacenter Edition, Microsoft Windows Server 2016, Standard and Datacenter Edition.

**Note** Starting from version 4.24, Cisco Security Manager supports Microsoft Windows Server 2019

**Note** Starting from version 4.13, Cisco Security Manager supports Microsoft Windows Server 2016

- Veritas Storage Foundation HA for Windows versions 6.0.1 / 6.0.2 / 6.1/Veritas InfoScale 7.0 / 7.2 / 7.4.

**Note** Veritas Infoscale 7.0 does not support Windows Sever 2016. However Veritas Infoscale 7.2 / 7.4 supports Windows Server 2016.

- Dynamic Multipathing Option

A Security Manager license is only required for the active server in a HA/DR configuration. Additional licenses for standby servers are not required.

Veritas Storage Foundation HA for Windows is licensed on a per-node basis. In the same local redundancy configuration example, each server needs to have its own license for running Veritas Storage Foundation HA for Windows.

The Veritas Dynamic Multipathing Option is required only if you plan to use external storage with more than one host bus adapter in a server, which provides multiple paths between the server and storage.

**Note** Beginning with version 4.20, Cisco Security Manager supports Veritas Infoscale 7.4.

# Software Requirements for a Geographic Redundancy (DR) Configuration

The following software is required to install Security Manager in a geographic redundancy (DR) configuration:

- Cisco Security Management Suite 4.25
- Microsoft Windows Server 2019, Standard and Datacenter Edition, Microsoft Windows Server 2016, Standard and Datacenter Edition
- Veritas Storage Foundation HA/DR for Windows 6.0.1 / 6.0.2 / 6.1/Veritas InfoScale 7.0 / 7.2 / 7.4
- Veritas Volume Replicator Option
- Veritas Dynamic Multipathing Option

Security Manager is licensed per active server in an HA/DR configuration. For example, in a geographic redundancy configuration with a single-node cluster at site A and a single-node cluster at Site B, you only need to purchase one copy of Security Manager, since Security Manager is only active on one server at any given time.

Veritas Storage Foundation HA for Windows is licensed on a per-node basis. In the same geographic redundancy configuration example with two servers (one per cluster), each server needs to have its own license for running Veritas Storage Foundation HA for Windows.

The Veritas Volume Replicator Option is licensed on a per-node basis.

The Veritas Dynamic Multipathing Option is required only if you plan to use external storage with more than one host bus adapter in a server, which provides multiple paths between the server and storage.

# Software Requirements for Replication without Clustering

The following software is required to install Security Manager in a geographic redundancy (DR) configuration without clustering:

- Cisco Security Management Suite 4.25
- Microsoft Windows Server 2019, Standard and Datacenter Edition, Microsoft Windows Server 2012, Standard and Datacenter Edition
- Veritas Storage Foundation Basic for Windows 6.0.1 / 6.0.2 / 6.1/Veritas InfoScale 7.0 / 7.2 / 7.4
- Veritas Volume Replicator Option
- Veritas Dynamic Multipathing Option

Security Manager is licensed for each active server in a HA/DR configuration. For example, in a geographic redundancy configuration with replication running between a primary server and a secondary server, you need to purchase only one copy of Security Manager, because Security Manager is active on only one server at any given time.

Veritas Storage Foundation for Windows is licensed on a per-node basis. In the same geographic redundancy configuration example with two servers, each server must have its own license for running Veritas Storage Foundation for Windows.

Veritas Storage Foundation Basic for Windows versions 6.0.1 / 6.0.2 / 6.1 / Veritas InfoScale 7.0 / 7.2 / 7.4 work with up to four volumes and are available for free download.

The Veritas Volume Replicator Option is licensed on a per-node basis.

The Veritas Dynamic Multipathing Option is required only if you plan on using external storage with more than one host bus adapter in a server, which provides multiple paths between the server and storage.

# Preinstallation Worksheets

Use the preinstallation worksheet to plan your installation and to gather the information you will need during configuration. This section contains the following topics:

- Local Redundancy Configuration Worksheet, on page 5
- Geographic Redundancy (DR) Configuration Worksheet, on page 6

## Local Redundancy Configuration Worksheet

Before you install Security Manager in a local redundancy HA configuration, write down the information outlined in the table to assist you in completing the installation.

***Table 1: Preinstallation Worksheet for a Local Redundancy Configuration***

| Information | Primary Site |
|---|---|
| Shared Disk Group Name | datadg |

| Information | Primary Site | |
|---|---|---|
| Shared Volume Name | cscopx | |
| Drive Letter for Security Manager Data | | |
| Shared Disk Group Name for Event Data[1] | datadg_evt | |
| Shared Volume Name for Event Data[2] | cscopx_evt | |
| Drive Letter for Security Manager Event Data[3] | | |
| Cluster Name | CSManager_Primary | |
| Cluster ID | 0[4] | |
| Security Manager Virtual IP Address/Subnet mask | | |
| Cluster Service Virtual IP Address/Subnet mask[5] | | |
| | **Primary Server** | **Secondary Server** |
| Hostname | | |
| Public Network Interface #1 and IP Address/Subnet Mask | | |
| Public Network Interface #2[6] and IP Address/Subnet Mask | | |
| Private Cluster Interconnect #1 | | |
| Private Cluster Interconnect #2 | | |

1 Optional: Use these fields if you want your event data stored separately.
2 Optional: Use these fields if you want your event data stored separately.
3 Optional: Use these fields if you want your event data stored separately.
4 Must be an integer between 0 and 255 and unique for clusters in the same subnet.
5 This is the same value as the Security Manager Virtual IP Address/Subnet mask.
6 Required if a second NIC will be used to access the public network for redundancy.

[7]

# Geographic Redundancy (DR) Configuration Worksheet

If you are installing Security Manager in a geographic redundancy (DR) configuration, write down the information outlined in the table to assist you in completing the installation.

7
1. Optional: Use these fields if you want your event data stored separately.
2. Must be an integer between 0 and 255 and unique for clusters in the same subnet.
3. This is the same value as the Security Manager Virtual IP Address/Subnet Mask.
4. Required if a second NIC will be used to access the public network for redundancy.

*Table 2: Preinstallation Worksheet for a Geographic Redundancy (DR) Configuration*

| Information | Primary Site | | Secondary Site | |
|---|---|---|---|---|
| Disk Group | datadg | | datadg | |
| Data Volume | cscopx | | cscopx | |
| Drive Letter for Security Manager | | | | |
| Disk Group for Event Data[8] | datadg_evt | | datadg_evt | |
| Data Volume for Event Data | cscopx_evt | | cscopx_evt | |
| Drive Letter for Event Data | | | | |
| Storage Replicator Log Volume | data_srl | | data_srl | |
| Replicated Data Set | CSM_RDS | | | |
| Replicated Volume Group | CSM_RVG | | | |
| Cluster Name | CSManager_Primary | | CSManager_Secondary | |
| Cluster ID | 0[9] | | 1[10] | |
| Security Manager Virtual IP Address/Subnet Mask | | | | |
| Replication Virtual IP Address/Subnet Mask | | | | |
| Cluster Service Virtual IP Address/Subnet Mask[11] [12] | | | | |
| | **Primary Server** | **Secondary Server** | **Primary Server** | **Secondary Server** |
| Hostname | | | | |
| Public Network Interface #1 and IP Address/Subnet Mask | | | | |
| Public Network Interface #2 and IP Address/Subnet Mask[13] | | | | |
| Private Cluster Interconnect #1[14] | | | | |
| Private Cluster Interconnect #2[15] | | | | |

8 Optional: Use these fields if you want your event data stored separately.
9 Must be an integer between 0 and 255 and unique for clusters in the same subnet.
10 Must be an integer between 0 and 255 and unique for clusters in the same subnet.
11 Required only for clusters using two servers or multiple adapters to access the public network. For a single server cluster with only one network adapter to access the public network, the fixed IP address of this adapter can be used.
12 This is the same value as the Security Manager Virtual IP Address/Subnet mask.
13 Required if you are using a second NIC to access the public network for redundancy.
14 Required only for clusters using two servers.
15 Required only for clusters using two servers.

16

[16] **1.** Optional: Use these fields if you want your event data stored separately.

**2.** Must be an integer between 0 and 255 and unique for clusters in the same subnet.

**3.** Required only for clusters using two servers or multiple adapters to access the public network. For a single server cluster with only one network adapter to access the public network, the fixed IP address of this adapter can be used.

**4.** This is the same value as the Security Manager Virtual IP Address/Subnet Mask.

**5.** Required if a second NIC will be used to access the public network for redundancy.

**6.** Required only for clusters using two servers.