



Preface

This document explains how to install Cisco Security Management Suite (Security Manager) in a high availability (HA) or disaster recovery (DR) environment. The Security Manager HA/DR solution is based on Veritas Storage Foundation and High Availability solutions.

For the steps to install Security Manager in a VMware based high availability (HA) or disaster recovery (DR) environment, see [High Availability and Disaster Recovery in Virtual Machines](#).

Audience

The primary audience for this guide is system administrators who are responsible for installing and managing the HA/DR solutions. This guide assumes that you are familiar with the topics in [Table 1](#).

Table 1 **Topics in this Guide**

| Configuration | Topics |
|------------------|--|
| Local Redundancy | <ul style="list-style-type: none">• Cisco Security Management Suite• Microsoft Windows Server 2012, Standard and Datacenter Edition, or Microsoft Windows Server 2012 R2, Standard and Datacenter Edition or Microsoft Windows Sever 2016, Standard and Datacenter Edition• Veritas Storage Foundation HA for Windows 6.0.1, 6.0.2, 6.1, Veritas InfoScale 7.0, Veritas InfoScale 7.2, or Veritas InfoScale 7.4. |

Table 1 *Topics in this Guide (continued)*

| Configuration | Topics |
|--|--|
| Geographic Redundancy | <ul style="list-style-type: none"> • Cisco Security Management Suite • Microsoft Windows Server 2012, Standard and Datacenter Edition, or Microsoft Windows Server 2012 R2, Standard and Datacenter Edition or Microsoft Windows Sever 2016, Standard and Datacenter Edition • Veritas Storage Foundation HA for Windows 6.0.1, 6.0.2, 6.1, Veritas InfoScale 7.0, Veritas InfoScale 7.2, or Veritas InfoScale 7.4. • Veritas Volume Replicator Option |
| Geographic Redundancy without Clustering | <ul style="list-style-type: none"> • Cisco Security Management Suite • Microsoft Windows Server 2012, Standard and Datacenter Edition, or Microsoft Windows Server 2012 R2, Standard and Datacenter Edition or Microsoft Windows Sever 2016, Standard and Datacenter Edition • Veritas Storage Foundation HA for Windows 6.0.1, 6.0.2, 6.1, Veritas InfoScale 7.0, Veritas InfoScale 7.2, or Veritas Infoscale 7.4. • Veritas Volume Replicator Option |

Because the Security Manager HA/DR solution utilizes Veritas Storage Foundation and High Availability Solutions for Windows, we highly recommend the following courses for a local redundancy solution:

- Veritas Storage Foundation for Windows
- Veritas Cluster Server for Windows

For a geographically redundant solution, the following additional courses are highly recommended:

- Veritas Volume Replicator for Windows
- Disaster Recovery Using Veritas Volume Replicator and Global Cluster Option for Windows

Conventions

This document uses the following conventions:

| Item | Convention |
|--|--|
| Commands, keywords, special terminology, and options that should be selected during procedures | boldface font |
| Variables for which you supply values and new or important terminology | <i>italic</i> font |
| Displayed session and system information, paths and file names | <code>screen</code> font |
| Information you enter | boldface screen font |
| Variables you enter | <i>italic screen</i> font |
| Menu items and button names | boldface font |
| Indicates menu items to select, in the order you select them. | Option > Network Preferences |

**Tip**

Identifies information to help you get the most benefit from your product.

**Note**

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Warning**

Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.

Related Documentation

Refer to the following Cisco publications for additional information. These documents are available at <http://www.cisco.com/c/en/us/support/security/security-manager/tsd-products-support-series-home.html>.

- *Installation Guide for Cisco Security Manager 4.21*
- *User Guide for Cisco Security Manager 4.21*
- *Release Notes for Cisco Security Manager 4.21*

Refer to the following publications for additional information concerning Veritas Storage Foundation:

- *Veritas Storage Foundation™ and High Availability Solutions Getting Started Guide*
- *Veritas Storage Foundation™ and High Availability Solutions Release Notes*
- *Veritas Storage Foundation™ and High Availability Solutions Installation and Upgrade Guide*
- *Veritas Storage Foundation™ Administrator's Guide*
- *Veritas™ Cluster Server Release Notes*
- *Veritas™ Cluster Server Installation and Upgrade Guide*
- *Veritas™ Cluster Server Bundled Agents Reference Guide*
- *Veritas™ Cluster Server Administrator's Guide*
- *Veritas™ Volume Replicator Administrator's Guide*
- *Veritas™ Volume Replicator Advisor User's Guide*
- *Hardware Compatibility List (HCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows*
- *Software Compatibility List (SCL) for Veritas Storage Foundation™ and High Availability Solutions for Windows*

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.