Symantec Data Insight Installation Guide

Microsoft Windows

2.5

Symantec Data Insight Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 2.5.0

Legal Notice

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support 4

Chapter 1 Introducing Symantec Data Insight 9

About Symantec Data Insight 9
About the Management Server 10
About the Collector worker node 10
    About the Scanner 11
    About the Collector 12
About the Indexer worker node 12
About Communication Service 12
About Symantec Data Insight installation tiers 13
    About three-tier installation 13
    About two-tier installation 13
    About single-tier installation 13

Chapter 2 Preinstallation 15

Preinstallation steps 15
Operating system requirements 16
System requirements for Symantec Data Insight components 17
List of ports 17
Web server version 18

Chapter 3 Installing Symantec Data Insight 19

About installing Symantec Data Insight 19
Performing a single-tier installation 19
Performing a two-tier installation 20
Performing a three-tier installation 21
Installing the Management Server 21
Installing the worker node 24

Chapter 4 Upgrading Symantec Data Insight 27

Upgrading Data Insight to 2.5 27

Chapter 5 Post-installation configuration 31

Post-installation configuration 31
Registering the worker node 31
About post-installation security configuration for Management Server 32
About SSL client/server certificates 33
Generating Management Console certificate 33
Configuring your corporate firewall 38

Chapter 6 Installing Windows File Server agent 39

About Windows File Server agent 39
Installing Windows File Server agent manually 40
Configuring the Windows File Server using ConfigureWindowsFileServer.exe 42

Chapter 7 Getting started with Data Insight 45

About the Data Insight Management Console 45
Logging in to the Data Insight Management Console 45
Logging out of the Data Insight Management Console 46
Displaying online help 46

Chapter 8 Uninstalling Symantec Data Insight 47

Uninstalling Symantec Data Insight 47

Index 49

Chapter 1

Introducing Symantec Data Insight

This chapter includes the following topics:

- About Symantec Data Insight
- About the Management Server
- About the Collector worker node
- About the Indexer worker node
- About Communication Service
- About Symantec Data Insight installation tiers

About Symantec Data Insight

Symantec Data Insight is a solution for unstructured data access management. It monitors file system activity and helps answer questions such as who is using the data, who owns the data and who has access to the data. Data Insight gives you full visibility into data access, which helps drive security remediation and compliance efforts.

Based on a distributed client-server architecture, a typical Data Insight deployment consists of the following:

- Management Server
  See "About the Management Server" on page 10.
- Collector worker nodes
  See "About the Collector worker node" on page 10.
- Indexer worker nodes

See “About the Indexer worker node” on page 12.

The way you deploy Symantec Data Insight depends on the size of your organization, the geographical distribution of your datacenters , and the number of filers and shares that you want Data Insight to monitor.

See “About Symantec Data Insight installation tiers” on page 13.

About the Management Server

The Management Server is the main component of a Data Insight deployment and hosts the product's web interface. You can also configure the Management Server to connect to multiple storage devices to extract access events and store the extracted data locally to answer queries. Your deployment can only have one Management Server.

The Data Insight Management Server performs the following functions:

- Hosts the Web-based graphical user interface (GUI).
- Scans Active Directory to obtain information about users in the organization and correlates this information with the access events.
- Ensures that the configuration data on the worker nodes is synchronized with the Management Server's configuration data.
- Authenticates the Data Insight users.

Users interact with Data Insight primarily through the Data Insight management console . In this interaction, the user connects to the Web server through a Web browser. By default, the Web server runs on HTTPS port 443.

About the Collector worker node

The Collector worker node is a host machine that scans file system and SharePoint site collection hierarchies in your environment and collects access events from Network Attached Storage (NAS) devices. Data Insight uses this information to perform advanced reporting on the business owners of data and the access history of data. By scanning for file metadata and security descriptors, it reports on the loopholes of permissions on files and folders. The details that are captured by the Collector node also help you find stale and orphan files in the scanned data repositories.

You can have multiple Collector worker nodes attached to the Management Server for load balancing. You can configure each collector node to connect to a subset of storage devices to extract file system metadata and extract access events from these devices. Each filer or Web application can have exactly one Collector node associated with it.

Note: Symantec recommends that the Collector worker nodes share a fast network with the storage devices.

A Collector worker node consists of the following components:

- Scanner
- Collector

About the Scanner

The Scanner is a Data Insight process that scans enterprise data repositories by mounting CIFS network shares or accessing SharePoint servers using the Data Insight Web Service. The Scanner captures the file or folder hierarchy of a share or site collection and helps you collect in-depth information about files and folders.

Note that the Scanner is a scheduled process. Schedule of the scan can be controlled at the worker node level, filer/Web application level, or the share/site collection level. For detailed information on administration topics (including how to schedule scanning) see the *Symantec Data Insight Administrator's Guide*.

Depending on how the scans are scheduled, the Scanner stores the collected data in separate database files, with the appropriate timestamp. For each subsequent scan, Scanner only scans the files that are added or modified since the last full scan. These files are eventually uploaded to the Indexer node using the Communication Service.

See “About the Indexer worker node” on page 12.

The Scanner captures information about the following attributes for each file or directory:

- The size of a file.
- The access time.
- The creation time.
- The modification time.
- The Security ID of the file owner (SID).
- The Access Control Lists (ACLs)

The details the Scanner captures helps in the computation of metadata-based data ownership.

About the Collector

The Collector is a Data Insight process that enables you to collect and parse access events from various storage repositories. The Collector examines the access events available on these storage systems to parse the events that report the read, write, create, delete, and rename activity on files or folders. The access events are processed in batches that consist of several thousand events. Each batch of events that are collected in a cycle is stored in a separate file with appropriate timestamp that indicate the ending time of the last entry in that batch. This data is pruned based on events that are not from the configured shares or site collections and is then segregated on a per-share basis. These files are periodically shipped to the appropriate Indexer node.

Data Insight collects information about access events from various storage repositories through exposed vendor APIs.

For detailed instructions on enabling audit service, see the *Symantec Data Insight Administrator's Guide*.

About the Indexer worker node

The access events that are collected from the storage repositories are periodically uploaded to the Indexer node. You can choose to have multiple indexers for load balancing purposes. Each storage repository can have exactly one Indexer node associated with it. The indexer performs the following functions:

- Uses the data from the collector process and scanner to create index files, also known as segment files.
- Uses the segment files to service queries from the management console.

Each segment file contains information about the file system events that occur between a certain date range. Once a segment file is created and saved on the disk, it is never modified. The indexer process reads these segment files multiple times to service queries.

About Communication Service

Each node in a Data Insight deployment runs a process called Communication Service. This service is responsible for all inter-node communication. Communication Service uses Secure Sockets Layer (SSL) to secure communication between the Data Insight nodes. The SSL keys are generated during installation.

By default, Communication Service connects through sever port 8383. This port must be visible to bi-directional HTTPS traffic between all Data Insight nodes. The service is also responsible for scheduling various tasks on a Data Insight node, which include, scheduling file system scans and uploading files to the Indexer worker node.

About Symantec Data Insight installation tiers

Symantec Data Insight supports three different installation types: three-tier, two-tier, and single tier. Your installation type depends on the total number of storage devices that you want Data Insight to scan and their geographical distribution. Single-tier installations are used for Proof of Concept (POC) deployments or smaller setups .

The type and scope of deployment should be determined with the help of Symantec.

About three-tier installation

To implement the three tier installation, you must install the Management server, the Collector worker node, and the Indexer worker node on separate computers. Depending on the size of your organization, you can choose to have multiple Collector and Indexer worker nodes. When your storage repositories span datacenters that are geographically apart, you need multiple Collector worker nodes. When you have a very large number of storage repositories, you need multiple Indexer worker nodes. However, it is recommended that the Management Server and Indexer worker nodes must be co-located on the same network.

About two-tier installation

To implement the two-tier installation, you must install the Management Server and the Collector worker nodes on separate computers. When your storage repositories span datacenters that are geographically apart, you need multiple Collector worker nodes. In this mode, the Management Server also functions as the Indexer.

About single-tier installation

To implement the single-tier installation, you must install only the Management Server. In this mode, the Management Server functions as the Collector as well as the Indexer. Use single-tier installation only for POC deployments or smaller setups.

Note: You can start out with a single-tier deployment and gradually add worker nodes to transition your system to a two-tier or a three-tier setup as the number of sites and storage repositories increase.

Preinstallation

This chapter includes the following topics:

- Preinstallation steps
- Operating system requirements
- System requirements for Symantec Data Insight components
- List of ports
- Web server version

Preinstallation steps

Before you install the Symantec Data Insight servers, verify the following installation prerequisites:

- Verify the server system requirements.
  See "System requirements for Symantec Data Insight components" on page 17.
- Gather the required materials.
- The Data Insight host has a minimum of 10 GB of available disk space.
- The Management Server node can connect to the domain controller of each Active Directory domain that needs to be scanned.
- The Data Insight server that hosts the Collector worker node can connect to the filers that it is supposed to monitor.
- The Collector worker node must be in the same Active Directory domain as the filer.
- A bi-directional network connection on port 8383 exists between the Management Server and the worker node(s), and between the worker node(s).
- The firewall is configured to allow `https` access to the required ports.

- The keystore file (commd.keystore) that enables secure communication between the worker node and the Management Server is copied to the worker node from the Management Server.
  See "Registering the worker node" on page 31.
- You have obtained the credentials required during software installation. These credentials are required to log into the Data Insight Console after the installation.

  Note: Additional credentials are required when you configure storage repositories and Active Directory, and for scanning of shares or site collections. For a list of these credentials, see the *Symantec Data Insight Administrator's Guide*.

- Prepare for SMTP Alerting. When installing the Management Server, ensure that you have the details of your SMTP server and authentication details, if any, available.
- Prepare for Exclude Rules. Gather a list of users and IP addresses used by other scanners, like the virus scanner, that you want Data Insight to ignore. For more details, see the *Symantec Data Insight Administrator's Guide*.

Operating system requirements

Table 2-1 provides an overview of Symantec Data Insight operating system requirements:

Table 2-1 Symantec Data Insight operating system requirements

Operating system supported	Notes
Windows Server 2003	Windows Server 2003 (32-bit and 64-bit) Standard Edition and Enterprise Edition Windows Server 2003 R2 (32-bit and 64-bit) Standard Edition and Enterprise Edition
Windows Server 2008	Windows Server 2008 (32-bit and 64-bit) Standard Edition and Enterprise Edition Windows Server 2008 R2 (32-bit and 64-bit) Standard Edition and Enterprise Edition
VMware	32 bit and 64 bit on Windows 2003
VMware	32 bit and 64 bit on Windows 2008

Note: You must ensure that VMware Tools is installed for Windows 2003 and Windows 2008 on VMware.

System requirements for Symantec Data Insight components

Table 2-1 lists the minimum system requirements for Symantec Data Insight components.

Table 2-1 System requirements for Symantec Data Insight components

Component	System requirements
Management Server	■ Windows Server 2003 or 2008. The operating system can either be 32 bits or 64 bits. ■ 4 GB RAM ■ 2 CPUs
Indexer worker node	■ Windows Server 2003 or 2008. The operating system can either be 32 bits or 64 bits. ■ 8 GB RAM ■ 2 CPUs
Collector worker node	■ Windows Server 2003 or 2008. The operating system can either be 32 bits or 64 bits. ■ 4 GB RAM ■ 2 CPUs
Windows File Server agent node	■ Windows Server 2003 or 2008. The operating system can either be 32 bits or 64 bits. ■ 4 GB RAM ■ 2 CPUs
SharePoint Web Service	Microsoft SharePoint 2007 or SharePoint 2010

Note: The type and scope of deployment should be determined with the help of Symantec.

List of ports

This section lists the default ports that must be open before you begin installation.

Table 2-3 List of default ports

Component	Default Port
Management Server	Management console HTTPS port 443 Communication Service port 8383 Standard RPC ports 139 and 445
Collector worker node	Communication Service port 8383 Standard RPC ports 139 and 445
File Server	For Net App filers - HTTP port 80 (optional) and standard RPC ports 139 and 445 On EMC Control Station - HTTP port 80 and HTTPS port 443 On Windows File Servers managed without an agent - Standard RPC ports 139 and 445
Windows File Server agent node	Communication Service port 8383 Standard RPC ports 139 and 445
SharePoint Web Service	SharePoint Web Service is accessed over the same port as the configured Web Applications. This port on the SharePoint Web Servers should be accessible from the Collector node.

Note: The default ports for Data Insight components are configurable at the time of installation.

Web server version

Symantec Data Insight uses Apache Tomcat 6.0.32.

Installing Symantec Data Insight

This chapter includes the following topics:

- About installing Symantec Data Insight
- Performing a single-tier installation
- Performing a two-tier installation
- Performing a three-tier installation
- Installing the Management Server
- Installing the worker node

About installing Symantec Data Insight

You can perform a three-tier, two-tier, or single-tier installation of Symantec Data Insight.

Performing a single-tier installation

The computer on which you install Symantec Data Insight must contain only the software that is required to run the product. Symantec does not support installing Symantec Data Insight on a computer with non-essential applications.

To perform a single-tier installation

1. Perform the preinstallation steps.

   See “Preinstallation steps” on page 15.

2. Install the Management Server.

   See “Installing the Management Server” on page 21.

3. Perform other post-installation configuration.

   See “Post-installation configuration” on page 31.

Performing a two-tier installation

To perform a two-tier installation

1. Perform the preinstallation steps.

   See “Preinstallation steps” on page 15.

2. Install the Management Server.

   See “Installing the Management Server” on page 21.

3. Install one or more Collector worker nodes.

   See “Installing the worker node” on page 24.

4. Register the worker nodes with the Management Server.

   See “Registering the worker node” on page 31.

5. Perform other post-installation configuration.

   See “Post-installation configuration” on page 31.

Note: Choose the two-tier installation mode when your filers are distributed across geographically remote locations that are far away from the Management Server. Install one Collector for each remote location. For example, the main datacenter of your organization is in New York, with additional filers in Singapore and Australia. In this case, the Management Server must be located in New York and there must be one Collector each in Singapore and Australia.

Performing a three-tier installation

To perform a three-tier installation

1. Perform the preinstallation steps.

   See "Preinstallation steps" on page 15.

2. Install the Management Server.

   See "Installing the Management Server" on page 21.

3. Install one or more Collector worker nodes.

   See "Installing the worker node" on page 24.

4. Install one or more Indexer worker nodes.

   See "Installing the worker node" on page 24.

5. Register the worker nodes with the Management Server.

   See "Registering the worker node" on page 31.

6. Perform other post-installation configuration.

   See "Post-installation configuration" on page 31.

Note: Typically, you do not opt for a three-tier installation directly. Symantec recommends that you start with a single-tier or two-tier installation, and add additional indexer nodes later, as required.

Installing the Management Server

Symantec recommends that you disable any antivirus, pop-up blocker, and registry protection software before you begin the Symantec Data Insight installation process.

Throughout the installation process, the setup wizard displays installation information and options. Use the following options to navigate through the installation process:

- Click **Next** to display the next screen.
- Click **Back** to return to the previous screen.
- Click **Cancel** to end the installation.

To install the Management Server

1. Log on (or remote logon) as Administrator to the computer that is intended for the Management Server.
2. To launch the installer, double-click `Symantec_Data_Insight_2.5_N_xPP.exe`,

   where,

   - `N` is the build number, and
   - `PP` is the architecture - x86:32 bit, x64:64 bit.
3. On the **Welcome to the Symantec Data Insight** Setup Wizard window, click **Next**.
4. Symantec recommends that you let the installation process complete once you start it. You can uninstall the software after the installation is complete.
5. In the License Agreement window, select **I accept the agreement**, and click **Next**.
6. In the Select Destination Directory window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is C:/Program Files/Symantec/DataInsight.
7. In the Configure Type of Install window, select **Install Everything** installation option, and click **Next**.
8. In the Configure Data Directory window, select the location where you want to store the product data. Click **Next**.

   Select a location with enough free space and high-performance disks. If you are not sure, choose the default location; you can relocate the data directory to a different location later.

9 In the Management Server Properties window, enter the following details:

Management Server Address	The Fully Qualified host name (FQHN) of the current host. The remote worker nodes use this address to communicate with the Management Server
Web Server port	The secure (HTTPS) Web server port on which you can access the Web interface of the Management Server.

Select the **Scan current Active Directory Domain** checkbox, if you want the Management Server to automatically start scanning the Active Directory domain which the Management Server is a part of. If the Management Server is not part of any Active Directory domain, this option is disabled.

Click **Next**.

For information on customizing the Active Directory domains to be scanned, see the *Symantec Data Insight Administrator's Guide*.

The installer validates whether the appropriate ports are free to accept connections.

10 In the Configure Networking window, enter the following information, and click **Next**:

Communication Service Port	See “About Communication Service” on page 12.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data stored on the local system. This service port does not need to be accessible outside the host machine.

11 In the Configure a Product Administrator window, enter the following information , and click **Next**:

- Name of the user who can log in to Symantec Data Insight with Product Administrator privileges
- Name of the domain to which the user belongs

Note: The product administrator must be a local user or must belong to the same domain as the Management Server.

12 To disable crash reporting, in the Configure Crash Reporting window, uncheck the **Enable Dr.Watson for Windows** checkbox.

By default the checkbox is selected.

13 In the Select Start Menu Folder, select the folder where you want the installer to place the program shortcuts.

The option, **Create shortcuts for all users**, is selected by default.

14 In the Additional Tasks window, select the tasks, as appropriate.

15 To start the installation process, click **Next**.

16 The Installing window appears and displays a progress bar.

17 The Completing the Symantec Data Insight setup wizard window provides you an option to start Data Insight Services (recommended).

The next screen provides you an option to launch the Management Server on exit. Select this option to launch the Console and complete setting up the Management Server. .

18 To exit setup, click **Finish**.

Note: Once you install the Management Server, log on to the Management Server to configure the SMTP settings and other product users, as necessary.

Installing the worker node

Throughout the installation process, the setup wizard displays installation information and options. Use the following options to navigate through the installation process:

- Click **Next** to display the next screen.
- Click **Back** to return to the previous screen.
- Click **Cancel** to end the installation.

Installing the worker node

1 Log on (or remote logon) as Administrator to the computer that is intended for the worker node.

2 Double-click `Symantec_Data_Insight_2.5_architecture.exe` to launch the installer..

3 The Welcome to the Symantec Data Insight Setup Wizard window appears. Click **Next**.

4 In the License Agreement window, select **I accept the agreement**, and click **Next**.

5 In the Select Destination Directory window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is C:\Program Files\Symantec\Data Insight.

Note: You cannot install the worker node on the same machine as the Management Server.

---

6 Depending on your deployment scenario, in the Configure Type of Install window, select **Install Indexer and Collector** or **Install Collector only** as the installation option.

7 Click **Next**.

8 In the Configure Data Directory window, browse to the location where you want to store the product data.

Select a location with enough free space and high-performance disks. If you are not sure, choose the default location; you can relocate the data directory to a different location later.

9 In the Worker Node Properties window, enter the Fully Qualified Host Name (FQHN) of the host. This name must be resolvable from the Management Server and the other worker nodes.

10 In the Configure Networking window, enter the following information:

Communication Service Port	See "About Communication Service" on page 12.
Configuration Service Port	Configuration service is a process that provides interface to configuration and other product data stored on the local system. This service port does not need to be accessible outside the host machine.

Note: The installer validates whether the appropriate ports are free to accept connections.

---

11 To disable crash reporting, in the Configure Crash Reporting window, uncheck the **Enable Dr.Watson for Windows** checkbox.

By default the checkbox is selected.

12 In the Select Start Menu Folder, select the folder where you want the installer to place the program shortcuts. The option, **Create shortcuts for all users**, is selected by default. To start the installation process, click **Next**.

13 To register the worker node with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** checkbox.

See "Registering the worker node" on page 31.

14 To exit setup, click **Finish**.

Chapter 4

Upgrading Symantec Data Insight

This chapter includes the following topics:

- Upgrading Data Insight to 2.5

Upgrading Data Insight to 2.5

You can upgrade an existing Data Insight Server with Symantec Data Insight 2.0 or later versions to 2.5. Data Insight does not support upgrading a version prior to 2.0 directly to 2.5. If the server is installed with a version prior to 2.0, you must upgrade to version 2.0 before you can upgrade to 2.5.

Before you begin the upgrade to Symantec Data Insight 2.5, note the following:

- As a best-practice measure, Symantec recommends that you take a backup of the server's `Data` folder.
- In case of a multi-node setup, the upgrade setup must be run first on the Management Server, then on the Indexer nodes, followed by the Collector nodes. You can upgrade the Windows File Server agent only after upgrading the Collector nodes.
- Data Insight does not support the upgrade of policies. Policies are deleted from Data Insight during the upgrade to 2.5. The old policy configuration is saved to a text file located at $data\conf\policy.db_upgrade.<*version*>, where, <*version*> is the version you are upgrading from. You must manually recreate all the policies after the upgrade is complete.

To upgrade theData Insight to 2.5:

1. Log on as Administrator to the server that you want to upgrade.
2. To launch the Symantec Data Insight 2.5 installer, double-click `Symantec_Data_Insight_2.5_N_xPP.exe,`
3. where,
   - `N` is the build number, and
   - `PP` is the architecture - x86:32 bit, x64:64 bit.
4. When the setup prompts you to upgrade from current version to 2.5, click **Yes**.
5. On the Welcome to the Symantec Data Insight Setup Wizard window, click **Begin Upgrade**.

   The setup wizard runs through the upgrade automatically.
6. You must upgrade the product data before you start Data Insight services. On the **Completing the Symantec Data Insight 2.5 Upgrade Wizard** window, select the **Launch the Upgrade Data Wizard** check box.
7. Click **Finish** to exit the setup.

To upgrade the product data using Upgrade Data Wizard:

1. Launch the Upgrade Data wizard.
2. On the Upgrade Product Data window, select the **Make temporary backup of data before upgrading** check box.

   Symantec recommends that you take a backup of the product data before starting the data upgrade. This ensures that the original data can be restored from backup if the upgrade fails. Data Insight deletes the backup after completing the upgrade successfully.
3. Create the backup of the product data. To select a backup location, browse to the location where you want the backup data to be stored.

   Before you begin the upgrade, ensure that there is enough free space available in the target location to take a backup. Data Insight requires that your system must have free space to accomodate your `data` directory and an additional 100 MB of data for the upgrade to succeed. If enough free space is not available, the upgrade wizard fails. If this happens, relaunch the upgrade wizard by executing the command `INSTALL_DIR\bin\UpgradeData.exe`.
4. Click **Upgrade Now** to start the data upgrade process.

5 The Data Upgrade window appears and displays a progress bar while upgrading the product data.The time taken in the upgrade process depends upon the size of the data.

6 On successful completion of the data upgrade, click **OK**.

7 On the Start Data Insight Services window, select **Start Data Insight Services now**. Click **Next**.

8 Click **Finish** to exit the wizard.

Note: You can also upgrade the Windows File Server agent using the Management Console. For more details, see the *Symantec Data Insight Administration Guide*.

Chapter 5

Post-installation configuration

This chapter includes the following topics:

- Post-installation configuration
- Registering the worker node
- About post-installation security configuration for Management Server
- Configuring your corporate firewall

Post-installation configuration

You must complete the following configuration after you finish installing Symantec Data Insight:

- Register the worker node with the Management Server.
  See "Registering the worker node" on page 31.
- Configure post-installation security settings.
  See "About post-installation security configuration for Management Server" on page 32.
- Configure your corporate firewall.
  See "Configuring your corporate firewall" on page 38.

Registering the worker node

You must register the worker node with the Management Server to enable communication between them.

You do not need to perform these steps if you have upgraded a worker node.

To register the worker node with the Management Server

1. Do one of the following:
   - To launch the Worker Node Registration Wizard immediately after completing the Worker Node installation wizard, select the **Launch Worker Node Registration Wizard after exit** checkbox.
   - To register the worker node at a later time, execute `RegisterWorkerNode.exe` located in the Data Insight installation bin directory.
2. In the Register Worker Node with Management Server window, enter the following information:
   - Fully Qualified Host Name (FQHN) of the Management Server host
   - Location of the Communication Service keystore file
     The keystore file, `commd.keystore`, enables secure communication between worker nodes and the Management Server. It is present in the `keys` subfolder of the Management Server's data directory. You must manually copy the keystore file from the Management Server machine to a temporary location on the worker node. By default the data directory is located on the Management Server at `C:\DataInsight\data`. It might be different for your setup. You can locate the data directory by reading the file `C:\Program Files\Symantec\DataInsight\datadir.conf` on the Management Server.
3. Click **Register Now**.
4. After the successful registration of the worker node, delete the `commd.keystore` file from the temporary location.

About post-installation security configuration for Management Server

Symantec Data Insight secures communications between all Data Insight servers. This task is accomplished by encrypting the transmitted data and requiring servers to authenticate with each other.

The following sections describe the Symantec Data Insight security configuration and how to change the default security configuration.

About SSL client/server certificates

Symantec Data Insight secures all data flowing between the Management Server and the Worker nodes using the Secure Socket Layer/Transport Layer Security (SSL/TLS) protocol. The SSL/TLS protocol not only encrypts the data that is transmitted, Symantec Data Insight also uses it for mutual authentication between servers.

Data Insight implements authentication with the mandatory use of client and server-side certificates or keys. Connections between the Data Insight servers use a single, self-signed certificate. The Management Server generates the certificate at install time and is unique to your deployment. It is present on the Management Server node in the `keys` folder under the `data` folder. The file is called `commd.keystore`. When you configure Worker Nodes, this file must be manually copied over to the new Worker node before installation.

Generating Management Console certificate

The Management Server provides a Web interface (administration console) for reporting and administration purposes. You access this interface with a Web browser. The Management Server and browser communicate through an SSL connection.

To ensure confidentiality, all communication between the Management Server and the browser is encrypted using a symmetric key. To initiate a connection, the Management Server and browser negotiate the encryption algorithm (algorithm, key size, and encoding) and encryption key to use.

By default, connections between the Management Server and the browser use a single, self-signed certificate. The certificate is generated by Management Server at install time and is unique to your deployment. It's present on the Management Server node in a folder called *keys* under the data folder. The file is called `webserver.keystore`. While this certificate is secure, you will get a warning message in the browser when accessing the Web Interface because it's a self signed certificate. To avoid getting this warning, Symantec recommends that you generate a unique certificate for your organization's installation. This new certificate replaces the default certificate.

To generate a unique Management Console certificate

1. Collect the following information to generate a certificate request:

   - Common name
     The fully qualified DNS name of the Management Server. This name must be the actual name of the server that is accessible by all the clients. For example: https://*server_name*.

- Organization name
  For example, Symantec, Inc.
- Organizational unit (optional)
- City
  For example, San Francisco
- State
  For example, CA
- Country
  For example, US
- Expiration
  Expiration time in days (90)

2 Use `keytool.exe` to create the self-signed certificate (keystore file), which you need to generate the Certificate Signing Request (CSR). `keytool.exe` is a utility for managing keys and certificates. These items are used in self-authentication or data integrity and authentication services, using digital signatures. Certificates also enable users to cache the public keys of their communicating peers.

To create this file, go to the root directory of the Symantec Data Insight installation and perform the following steps in this order:

- From a command window, go to the `installdir\DataInsight\jre\bin` directory, where `installdir` is the directory into which you installed the Management Server.
- Run the following command with the information collected in 1:

```
keytool -genkey -alias tomcat -keyalg RSA -validity 730 -keysize 1024
-keypass changeit -keystore webserver.keystore -storepass changeit
-storetype JKS -dname cn=common_name,o=organization_name,
ou=organization_unit,l=city,s=state,c=US
```

The `-storepass changeit` command sets the password to **changeit**. Enter this password if you are prompted for a password after running the command. This command creates the self-signed certificate (webserver.keystore) in the `installdir\DataInsight\jre\bin` directory.

Note: At this time, Data Insight does not support setting the password to anything other than **changeit**.

3 Generate the certificate signing request (CSR) file. The CSR file is the request that you submit to the Signature Authority to obtain a signed certificate.

From the `installdir\DataInsight\jre\bin` directory and run the following command:

```
keytool -certreq -alias tomcat -keyalg RSA -keystore webserver.keystore
-storetype JKS -storepass changeit -file "DataInsight.csr"
```

If you are prompted for a password, press **Enter**. This command creates a file called `DataInsight.csr`. You submit this file to the Signature Authority.

4 To generate a certificate you send the .CSR file to a Certified Signature Authority (your own or a third party, such as VeriSign).

To obtain a signed certificate from your internal Signature Authority, contact your system administrator for instructions.

For the VeriSign Signature Authority, perform one of the following actions:

- Current Customers
  If you are a current VeriSign customer, go to the following page and buy an additional certificate:
  http://www.VeriSign.com/products-services/security-services/ssl/current-ssl-customers/index.html.
  You need your Common Name, Order Number, or Serial Number to begin the transaction, as well as the CSR.

- New customers
  If you are not a current customer and want to purchase the signed certificate from VeriSign, go to the following page:
  http://www.VeriSign.com/products-services/security-services/ssl/buy-ssl-certificates/index.html.
  To purchase the signed certificate, you will need the following information, in addition to the CSR:

  - The length of time for the certificate (one year or two years).
  - The number of servers that host a single domain (up to five servers).
  - The server platform.
  - The organization, organizational unit, country, state, or locality (all spelled without abbreviations).
  - Payment information and a billing contact.
  - The common name. This name is the host name and domain name, such as www.company.com or company.com.
  - An email where VeriSign can reach you to validate the information.

- Documentation to demonstrate that your organization is legitimate.

To obtain signed certificates from other Signature Authorities, go to their Web sites and follow the instructions to enroll and obtain a signed certificate. This process is similar to the VeriSign process. However, check with the organization to identify any additional environment information that may be needed for the certificate.

The certified Signature Authority sends you the signed certificate (this process might take 3-5 days). Internal Signature Authorities must return the root certificate along with the signed certificate.

5 Place the signed certificate into the directory (`installdir\datainsight\jre\bin`) with the webserver.keystore file. To email the certificate, paste it into a text document exactly as it appears on the screen. Include the top line and bottom line (-----*Begin Certificate*----- *and* -----*End Certificate*-----). Make sure that no extra lines, spaces, trailing carriage returns, or characters have been inadvertently added. Save this file in the same directory where the`webserver.keystore` file is located. If the signed certificate is provided as an attachment to an email, copy this file into the same directory where the `webserver.keystore` file is located.

6 Keep a copy of both the webserver.keystore file and the signed certificate file in a separate, secure location.

7 Confirm the signed certificate is correct. Open a command prompt and run the following command to view the certificate's fingerprint(s)

```
keytool -printer -file signed_certificate_filename
```

The following is an example output:

```
Owner: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll

Issuer: CN=ll, OU=ll, O=ll, L=ll, S=ll, C=ll

Serial Number: 59092b34

Valid from: Thu Sep 25 18:01:13 PDT 1997 until: Wed Dec 24 17:01:13

PST 1997

Certificate Fingerprints:

MD5: 11:81:AD:92:C8:E5:0E:A2:01:2E:D4:7A:D7:5F:07:6F SHA1:
20:B6:17:FA:EF:E5:55:8A:D0:71:1F:E8:D6:9D:C0:37 37:13:0E:5E:FE
```

8. Call or email the person who sent the certificate and compare the fingerprint(s) you see with the fingerprint(s) they sent you. If the fingerprint(s) are not exactly equivalent, the certificate may have been replaced in transit by an attacker's certificate.

   If you used an Internal Signing Authority, also view the fingerprint(s) of the root certificate using the same `-printer` command.

   ```
   keytool -printer -file
   ```

   name_of_root_certificate_provided_by_internal_signature_authority

   Compare the displayed fingerprint with the well-known fingerprint (obtained from a newspaper or the root CA's Web page). Contact the certificate's issuer if you have questions.

   When you execute the command, the `-import` command prints out the certificate information and prompts you to verify it.

9. Return to the `installdir\DataInsight\jre\bin` directory and update the local`webserver.keystore` file with the signed certificate as follows:

   - Internal signature authority
     Use the following command to update the `webserver.keystore` file with the root certificate:

     ```
     keytool -import -file root_certificate_filename -keystore
     webserver.keystore -storepass changeit
     ```

     Use the following command to update the .keystore file with the signed certificate:

     ```
     keytool -import -alias tomcat -keystore webserver.keystore
     -trustcacerts -file signed_certificate_filename
     ```

   - VeriSign or third-party signature authority
     Use the following command to update the local .keystore file with the signed certificate:

     ```
     keytool -import -alias tomcat -keystore webserver.keystore
     -trustcacerts -file signed_certificate_filename
     ```

10 Copy the updated `webserver.keystore` file into the `$datadir\keys` directory. By default, `$datadir` is located at `C:\DataInsight\data`. Note that this operation overwrites an existing file of the same name in that location. Rename the existing file if you want to keep it.

11 Restart the Data Insight Web service by performing the following steps in this order:

- net stop DataInsightWeb.
- net start DataInsightWeb.

Configuring your corporate firewall

The instructions in this section assume that the Management Server and Worker nodes are installed inside your corporate LAN behind a firewall. If this is the case, update your corporate firewall settings as follows:

- Allow 2-way connections between the Management Server and the Worker Nodes and between Worker Nodes. Configure your firewall to accept connections on the port you entered for the Communication Service when installing the Management Server and Worker Nodes. By default, the Communication Service communicates over port 8383. You can configure the servers to use any other port. Traffic on this port is HTTPS.
- Allow Windows Remote Desktop Client connections (TCP port 3389). This feature can be useful for setup purposes.
- The Web Interface of the Management Server runs on port 443 (configurable at the time of installation). This port must be opened at the Management Server to allow HTTPS communication between browsers and the Web server.

Chapter 6

Installing Windows File Server agent

This chapter includes the following topics:

- About Windows File Server agent
- Installing Windows File Server agent manually
- Configuring the Windows File Server using ConfigureWindowsFileServer.exe

About Windows File Server agent

Symantec Data Insight requires an agent to be installed on a Windows File Server machine if you want to monitor access events on the file server. Data Insight can automatically install the agent on the Windows File Server when adding the file server using the Console.

For detailed information about automatically installing the agent on the Windows File Server, see the *Symantec Data Insight Administrator's Guide*.

Optionally, you can choose to install the agent manually on the file server.

To configure a Windows File Server manually

1. Install the Windows File Server agent on the file server machine.

   See "Installing Windows File Server agent manually" on page 40.

2. Register the agent with the Management Server using the `RegisterWorkerNode.exe` utility. During registration, you can specify the address of the worker node that is intended to be the Collector node of this file server . Registration takes place through the Collector worker node. Registering the agent ensures that the file server can communicate with the Collector worker node.

   See "Registering the worker node" on page 31.

3. Add the file server to the Management Server using the `ConfigureWindowsFileServer.exe` utility.

   See "Configuring the Windows File Server using ConfigureWindowsFileServer.exe" on page 42.

4. If the file server is clustered using MSCS, do the following:.

   - Install the agent on each node of the cluster.
   - Register each node with the Management Server using its physical host address.
   - Run `ConfigureWindowsFileServer.exe` from each cluster node after registering the node.

Installing Windows File Server agent manually

To install the Windows File Server agent manually

1. Locate the agent installer binary from the agent bundle that ships with the product. The agent bundle is a compressed file that contains the agent installer along with some installation templates. It is called `Symantec_DataInsight_windows_winnas_2.5_X_arch.zip`.

2. Select the proper bundle based on the architecture of your file server and unzip it in a temporary location to get the installer binary. The binary is called `Symantec_DataInsight_windows_winnas_2.5_X_arch.exe`.

3. Log on (or remote logon) as Administrator to the Windows file server, where you intend to install the agent.

4. Double-click the agent installer to launch it.

5. The Welcome to the Symantec Data Insight Setup Wizard window appears. Click **Next**.

6 In the License Agreement window, select **I accept the agreement**, and click **Next**.

7 In the Select Destination Directory window, browse to the directory in which you want Data Insight to be installed. By default, the destination directory is `C:/Program Files/Symantec/Data Insight`.

8 In the Configure Data Directory window, browse to the location where you want to store the product data. Select a location with enough free space. If you are not sure, choose the default location; you can relocate the data directory to a different location later.

9 In the Configure Networking window, enter the following information:

- Communication Service Port
  See "About Communication Service" on page 12.
- Configuration Service port
  Configuration service is a process that provides interface to configuration and other product data that is stored on the local system. This service port does not need to be accessible outside the host machine. Configuration Service Port Note: The installer validates whether the appropriate ports are free to accept connections.

Note: The installer validates whether the appropriate ports are free to accept connections.

10 To disable crash reporting, in the Configure Crash Reporting window, clear the **Enable Dr.Watson for Windows** checkbox. By default the checkbox is selected.

11 In the Select Start Menu Folder, select the folder where you want the installer to place the program shortcuts. The option, **Create shortcuts for all users**, is selected by default.

12 To start the installation process, click **Next**.

13 To register the worker node with the Management Server after you exit setup, select the **Launch Worker Node Registration Wizard after exit** checkbox.

See "Registering the worker node" on page 31.

14 To exit setup, click **Finish**.

Configuring the Windows File Server using ConfigureWindowsFileServer.exe

Run the `ConfigureWindowsFileServer.exe` utility to configure the file server from the file server machine. You must run this utility after you have registered the agent node with the Management Server to add the file server to the Management Server configuration. Data Insight starts monitoring this file server after you have completed this step.

To configure the Windows File Server from the file server machine

1 Double-click `ConfigureWindowsFileServer.exe` located in the `bin` folder of the installation.

The File Server Configuration Wizard appears.

2 Select **This File Server is a part of MSCS cluster** check box if this node is a part of an MSCS cluster. If you select this option, specify name of this cluster in the Cluster Name text box. You must enter the exact same name in this field when you run this utility on all nodes of this cluster.

3 Select the Collector worker node for this file server using the Collector Node drop-down. All communication with this file server happens through. the associated Collector node.

4 Select **Automatically discover shares on this filer** check box if you want Data Insight to automatically discover shares on this filer and add them to the configuration.

Note: If this filer is a Clustered file server, you need to log into the Console later and specify credentials of an Administrative user on this cluster before discovery can happen.

You can optionally specify shares that need to be ignored during discovery by specifying matching patterns in the adjoining text box.

5 Select **Scan new shares immediately** check box to add newly added shares to the scan queue immediately without waiting for the normal full scan schedule. However, scanning will still take place only during the times scanning is permitted on the node.

6 Click **Configure Now** button to finish the configuration. The utility will contact the Management Server through the selected Collector node and add the file server to the Management Server. If this is a clustered file server and the filer has already been added through the first node, this step associates this additional cluster node with the existing filer configuration.

Alternately, you can choose to not run this utility post-registration, and configure the agent from the Management Console.

To configure the agent from the Management console

1. Register the agent with the Management Server.
2. Log on to the Management Console.
3. From the **Settings** > **Filers** page, select **Add Windows File Server**.

   On the Add new filer page, clear the **Let Data Insight install the agent automatically** check box.
4. Select this node from the list view control to associate this node with the file server.

Chapter 7

Getting started with Data Insight

This chapter includes the following topics:

- About the Data Insight Management Console
- Logging in to the Data Insight Management Console
- Logging out of the Data Insight Management Console
- Displaying online help

About the Data Insight Management Console

Users interact with Data Insight primarily through the Data Insight Management Console. The Data Insight Console is a graphical user interface that provides a central point to view storage resources that Data Insight monitors, schedule processes, and view reports, among other features. The Console is automatically installed with the Management Server. You access the Console through a Web browser that has a network connection to the Management Server. By default, the Management Server runs on HTTPS port 443.

Logging in to the Data Insight Management Console

To log on to the console from the Management Server or a worker node

1 Do one of the following:

- Click the shortcut created on the Desktop during installation.

- Click **Start** > **Programs** > **Symantec** > **Symantec Data Insight** > Data Insight Console.

2 On the Login screen, enter the credentials of a user with privileges to log in to the Management Server.

3 Enter the name of the domain to which the user belongs.

4 Click **Submit**.

The Management Console appears.

To log on to the console from a machine other than the Management Server or the worker nodes

1 Open a Web browser and enter https://*ms_host*:*ms_port*. For example, https://datainsight.company.com:443.

2 On the Login screen, enter the credentials of a user with privileges to log in to the Management Server.

3 Enter the name of the domain to which the user belongs.

4 Click **Submit**.

The Management Console appears.

Logging out of the Data Insight Management Console

To log out

1 Click logout at the top right of the screen. The management console prompts you to confirm the logout.

2 Click **OK** to go back to the login screen.

Displaying online help

To access online help, click the **Help** button in the upper-right corner of any screen in the Management Console. Symantec Data Insight displays the help in a separate window. The online help shows the table of contents in the left pane and context-sensitive help in the right pane.

Chapter 8

Uninstalling Symantec Data Insight

This chapter includes the following topics:

- Uninstalling Symantec Data Insight

Uninstalling Symantec Data Insight

To uninstall Data Insight

1 If you created shortcuts during the installation, select **Start > All Programs > Symantec Data Insight > Symantec Data Insight** Uninstaller.

If no shortcuts exist, open the **Add or Remove Programs** control from the **Windows Control Panel**, and select the Symantec Data Insight entry. Then click **Change/Remove**.

Optionally, you can uninstall Symantec Data Insight using the uninstall.exe file. This file is located in the Data Insight installation folder (for example, `C:\Program Files\Symantec\DataInsight`).

2 In the Delete Data window, select the **Delete all product data** checkbox to remove all configuration as well as audit log data collected and stored by the product. Do not select this option, if you are attempting to repair the installation by uninstalling and reinstalling the software.

3 Click **Next** to uninstall.

The uninstaller removes all Symantec Data Insight components.

4 Click **Finish** to complete the uninstall process.

5 If you uninstall a worker node, log in to the management console, click the **Settings** tab.

6 Navigate to the page for the worker node, and click **Delete**.

Index

C

Collector process
    about 12
Collector worker node
    Collector 12
    overview 10
    Scanner 11
Communication Service 12
corporate firewall
    configuring 38

I

Indexer worker node
    overview 12
installation
    overview 19
    post-installation configuration 31
installation tiers 13
    single-tier installation 13
    three-tier installation 13
    two-tier installation 13

M

Management Console
    generating certificate 33
    logging in 45
    logging out 46
    overview 45
Management Server
    installing 21
    overview 10
    security configuration 32

O

online help 46

P

post-installation configuration 31
    security configuration 32
preinstallation steps 15

S

Scanner process
    about 11
single-tier installation
    overview 13
    performing 19
SSL client/server certificates 33
Symantec Data Insight
    installation 19
    installation tiers 13
    operating system requirements 16
    overview 9
    ports 17
    system requirements for components 17
    uninstalling 47
system requirements 17
    web server version 18

T

three-tier installation
    overview 13
    performing 21
two-tier installation
    overview 13
    performing 20

U

uninstalling 47

W

Windows File Server
    configuring
        silently 43
        using configureWindowsFileServer.exe 42
Windows File Server agent
    installation overview 39
    installing
        manual 40
worker node
    installing 24

worker node *(continued)*
    registering 31