Veritas Storage Foundation™ and High Availability Solutions Quick Start Guide for Symantec Product Authentication Service

Windows 2000, Windows Server 2003

5.0

11293730

symantec™

Veritas Storage Foundation and HA Solutions Quick Start Guide for Symantec Product Authentication Service

Storage Foundation for Windows HA 5.0

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Storage Foundation for Windows and Storage Foundation HA for Windows are licensed products. See the *Storage Foundation and High Availability Solutions for Windows, Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit http://entsupport.symantec.com and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Chapter 1

Getting Started with Symantec Product Authentication Services

This Getting Started Guide contains the following topics:

About Symantec Product Authentication Services

Symantec Product Authentication Service allows the security adminsitrator to configure authentication to provide a single sign-on service for Symantec applications. In this case, users need log on only once to a single Symantec application, and other applications can then use the credentials acquired through the first logon.

Symantec Product Authentication Service, previously known as Veritas Security Services (VxSS), secures communication between cluster nodes and clients, including the Java console, by using digital certificates for authentication and SSL to encrypt communication over the public network.

Symantec recommends that you configure one root broker in your data center and configure authentication brokers as necessary, including each node in an SFW HA cluster.

- Root broker
  A root broker serves as the main registration and certification authority; it has a self-signed certificate and can authenticate other brokers. The root broker is only used during initial creation of an authentication broker.
- Authentication brokers
  Authentication brokers serve as intermediate registration and certification authorities. Authentication brokers have certificates that are signed by the root. Each node in an SFW HA cluster serves as an authentication broker.

Each authentication broker has a private domain repository that stores the services and users of any Symantec application using the broker for authentication.

You can set up Authentication Service for a cluster using the VCS Cluster Configuration wizard.

For detailed information about the Authentication Service, see the *Symantec Product Authentication Services Administrator's Guide*.

Best Practices

The Symantec Product Authentication Service can be deployed in many different ways. However, using best practices can minimize the ongoing management cost of the security technology.

The guidelines are as follows:

- Minimize the number of root brokers to one.
- Back up the private domain repositories, and keep the backup in a safe place.
- Limit use of private domain repository accounts to Symantec services only.

Minimize the number of root brokers to one

Having a single root broker brings all the Symantec products under the same security domain, instead of creating islands of security. Such consolidation facilitates single sign-on and secure communications among various products.

The root broker owns the trust relationship for all hosts in its trust hierarchy. If you have more than one root broker, you must establish that trust relationship across all root brokers. Maintaining a trust relationship across multiple root brokers can be expensive and time consuming.

Minimizing the number of root brokers is also attractive from a security perspective. Repairing an environment after a root broker has been compromised is more burdensome than if only an authentication broker has been compromised. When a root broker is compromised, the scope of compromise is the entire security domain. With fewer root brokers, the risk of compromising the entire security domain is minimized.

Remember to back up Symantec Product Authentication Service

The private domain repositories for the root broker and the authentication brokers hold essential data. Back up the private domain repositories as frequently as you would back up any essential data. Keep a safe copy off line.

See “Backing up Symantec Product Authentication Services”.

Limit use of private domain repository accounts to Symantec services only

The private domain repository was designed for use when Symantec programs need to authenticate each other. The private domain repository eliminates the need to define and store Symantec programs’ identities in a site’s human user authentication domain (such as: Windows 2000, Active Directory, and so on).

Planning for Symantec Product Authentication Service in an SFW HA environment

Symantec Product Authentication Service is automatically installed with SFW HA. When the cluster is configured using the VCS Configuration Wizard, you can identify and point to a root broker within the cluster or outside of the cluster.

You can install and configure a Symantec Product Authentication Service root broker outside of a cluster by using the executables available from the Product Authentication Service directory included in the SFW HA installation media.

Review the following scenarios and, depending on your environment, take the prescribed actions.

Note: SFW HA 5.0 does not provide support for making a root broker highly available in a clustered environment.

Note: Symantec Product Authentication Service is used only in SFW HA environments, as authentication brokers are not required for standalone SFW systems.

For information on installing SFW HA and configuring a cluster, see the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Scenario 1: one or more clusters with one root broker outside the clusters

Environment: multiple clusters with the root broker established outside those clusters

Description: The root broker is installed on a separate system outside of the clusters and all cluster nodes serve as authentication brokers. This is the recommended setup for Symantec Product Authentication Service.

User Action:

1 From the SFW HA installation media, run the Symantec Product Authentication Service executable to install and configure Symantec Product Authentication Service on the designated system to create the root broker.

See “Installing a root broker on a dedicated system outside the clusters” on page 11.

2 Install SFW HA on all systems that will become nodes in the cluster.

3 Configure the clusters using the VCS Configuration Wizard.(Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Cluster Configuration Wizard). In the Configure Security Service Option panel, specify the root broker you created in step 1. The nodes of the cluster are automatically configured as authentication brokers.

Note: The root broker is only needed when adding a new cluster or a new node to a cluster.

Scenario 2: single cluster with one root broker inside cluster

Environment: a single cluster

Description: Identify a system inside the cluster to be used as the root broker. All systems in the cluster become authentication brokers, including the system used as root, as it becomes a root broker and authentication broker when the cluster is configured.

Note: You do not need to install and configure the root broker separately as mentioned in the first scenario. The VCS Configuration Wizard will automatically configure the root broker and authentication brokers for you.

User Action:

1 Identify the node within the cluster on which the root broker will be installed during cluster configuration.

2 Install SFW HA on all systems that will become nodes in the cluster.

3 Run the VCS Configuration Wizard to configure the root broker. (Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Cluster Configuration Wizard)

In the Configure Security Service panel, specify the root broker you identified in Step 1. The nodes of the cluster are automatically configured as authentication brokers.

Scenario 3: multiple clusters with one root broker inside a cluster

Environment: more than one cluster residing within the same domain

Description: Establish a root broker on a node within one of the clusters. During the configuration process for additional clusters, point to that root broker. The nodes in the additional clusters act as authentication brokers.

User Action:

1. Identify the system on which the root broker will be created during cluster configuration.
2. Install SFW HA on all systems.
3. Run the VCS Configuration Wizard to configure the first cluster. Specify the system hosting the root broker during the configuration process.
4. Run the VCS Configuration Wizard to configure additional clusters, pointing to the root broker on the first cluster. The nodes in the additional clusters act as authentication brokers.

Considerations: The VCS Configuration Wizard can only discover root brokers residing on Windows systems.

Scenario 4: using SFW HA with an existing root broker

Environment: a root broker configured for another Symantec product

Description: configuring SFW HA to use a pre-existing root broker running a Windows operating system.

User Action:

1. Identify the system that is already configured as root broker for another Symantec product.
2. Install SFW HA on the systems that will become the new cluster nodes.
3. Configure the clusters using the VCS Configuration Wizard (Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Cluster Configuration Wizard).
   In the Configure Security Service panel, specify the root broker you identified in Step 1. The nodes of the cluster are automatically configured as authentication brokers.

Scenario 5: multiple clusters with one root broker per cluster

Note: This scenario is NOT RECOMMENDED.

Environment: multiple clusters and multiple root brokers

Description: The root broker is configured during cluster configuration.

User Action:

1. Install SFW HA.

2 Configure a root broker for each cluster during cluster configuration using the VCS Configuration Wizard.

Considerations: Using multiple root brokers increases the footprint of Symantec Product Authentication Service and is not recommended.

Installing a root broker

The following procedure installs a root broker for your configuration.

Installing a root broker on a dedicated system outside the clusters

To install a root broker in a security domain outside of your clusters as described in the first scenario, you need to run the Symantec Product Authentication installation wizard.

However, before installing Symantec Product Authentication Service, you must install the Java Runtime Environment (JRE), version 1.5.02. The JRE package is included as part of the installation media. If you already have JRE 1.5 installed, you do not need to install it again.

To install JRE

1 From the root directory on the installation media, navigate to **Symantec_Product_Authentication_Service**.

2 Double click **VRTSjre.msi**.

3 When the Windows Installer appears, follow the onscreen instructions to install JRE.

To install a root broker from the installation media

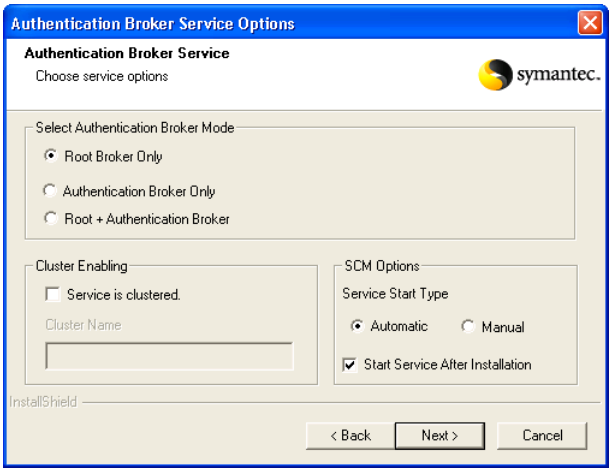
1 From the root directory on the installation media, navigate to **Symantec_Product_Authentication_Service**.

2 Double click **VxSSVRTSatSetup.exe**.

3 Review the Welcome screen and click **Next**.

4 In the Setup Type window, select **Complete** to install both the client and server components. To install the components in a directory other than the default one given, click **Browse**.

5 In the Authentication Broker Service screen, be sure to select the following options:



- Root broker only
- Do not select the **Service is clustered** checkbox, as clustering a root broker is not supported.
- Select **Automatic** for the Service Start Type (manual is selected by default).
- Select the **Start Service After Installation** checkbox.

6 When done, click **Next**.

7 In the Summary screen, verify the settings you have selected and click **Next** to begin installation.

8 The Setup Status screen shows the progress of the installation.

9 Type the root broker password in the text box in the password verification screen and then click **Next**.

Note that the text box for the authentication broker password is not available because you chose to install in Root Broker Only mode.

10 When the InstallShield Wizard Complete screen appears, click **Finish** to close the wizard.

Verify that the service is started

You can verify that the Symantec Product Authentication Service is started by opening the Services window in Windows Administrative Tools as follows:

```
Start > Settings > Control Panel > Administrative Tools >
Services
```

Find **Symantec Product Authentication Service** in the list of services and verify that the status is **Started**.

Upgrading an existing Symantec Product Authentication Service root broker

You can upgrade a lower version of a Symantec Product Authentication Service root broker by using the installation media.

Note: If you have an existing root broker that is using a lower version of Symantec Product Authentication Service, you can continue to use that root broker. Upgrading the root broker is optional.

To upgrade an existing root broker

1. Click Symantec Product Authentication Service on the installation media or double-click **VxSSVRTSatSetup.exe**.
   The progress meter for the Windows Installer displays.
2. You are asked if you want to upgrade Symantec Product Authentication Service. Click **Yes** to continue the upgrade, or **No** to stop the installation process.
3. Review the Welcome screen and click **Next**.
4. Type a new password for the root broker; do not use the old password for the existing root broker. Click **Next** when done.
5. The Setup Status screen shows the progress of the installation.
6. When the InstallShield Wizard Complete screen appears, click **Finish** to close the wizard.

Upgrading a non-secure 4.x SFW HA cluster to a secure 5.0 SFW HA cluster

The product installer upgrades a non-secure 4.x SFW HA cluster to a non-secure 5.0 SFW HA cluster. If you want to configure Symantec Product Authentication Service for secure communication, run the VCS Configuration Wizard. Make sure to select the following options: **Cluster Operations**, **Edit Existing Cluster**, **Reconfigure**, and **Configure Security Services**.

For more information, see the *Veritas Cluster Server 5.0 Administrator's Guide*.

Backing up Symantec Product Authentication Services

The private domain repositories for the root broker and authentication brokers hold essential data. Back up the private domain repositories as frequently as you would back up any essential data, and keep a safe copy off line.

The vssat showbackuplist command

The `vssat showbackuplist` command shows a list of material you should back up so that you can restore the broker later, if necessary.

Caution: The `vssat showbackuplist` command does not itself restore files.

The `vssat showbackuplist` command lists the following:

- Critical broker files that you should back up
- The restore names of the backed-up files, if the name differs from the original
- Registry keys that you should back up

To back up the broker's data on Windows

1. From the command line, locate the `vssat showbackuplist` command which resides in the following Windows directory:
   `C:\program files\veritas\security\authentication\bin`
2. Obtain the actual installation path for Authentication from the Windows registry key:
   `HKLM\Software\Veritas\Security\Authentication\InstallDir`
3. Run the command, using the following syntax, without line breaks:
   `vssat showbackuplist [--filename <file name for list>]`

The `vssat showbackuplist` command is a management tool used to back up and list the critical files. The command does not restore files.

4 Examine the output of `vssat showbackuplist`.
Each directory or file displays on a separate line. If you provide the *`--filename`* argument, output goes to that file. For example, to get the listing in a file named `list.txt`, run the following command:
`vssat showbackuplist --filename list.txt`
If you do not request a file, output is displayed onto the standard output, as follows:

B| FileOrDirToBeBackedup
R| RestoreAboveFileOrDirToFileOrDir
K| RegistryKey

For example, output on Windows appears as follows:

```
C:\Program
Files\Veritas\Security\Authentication\bin>vssat
showbackuplist
B|C:\Program Files\Veritas\Security\Authentication\
systemprofile\VRTSatlocal.conf
B|C:\Program Files\Veritas\Security\Authentication\
systemprofile\certstore
B|C:\Program Files\Veritas\Security\Authentication\
systemprofile\RBAuthSource
B|C:\Program Files\Veritas\Security\Authentication\
systemprofile\ABAuthSource
K|HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\Security\
Authentication
Quiescing ...
Snapshot Directory :C:\Program
Files\Veritas\Security\Authentication\Snapshot
```

5 After backing up the broker's critical data, perform additional backup by running the following command:

```
% reg export
HKLM\SOFTWARE\Veritas\Security\Authentication
<snapshotdir>\AtKey.reg
```

Output is as follows:

```
C:\>reg export
HKLM\SOFTWARE\Veritas\Security\Authentication
"c:\Program
Files\Veritas\Security\Authentication\Snapshot\AtKey.
reg"
```

```
The operation completed successfully.
```

Restoring the backup

The following procedure describes how to restore the broker's data and other important data on Windows.

To restore the backup on Windows

1. From the command line, shut down the broker as follows:
   ```
   net stop vrtsat
   ```
2. Type the following command to return the backup location. The `showbackuplist` command should also return the backup location.
   ```
   % vssregctl -l -q
   -b"Security\Authentication\Authentication Broker"
   -kSnapShotDirectory
   ```
3. Restore the backup files by running the following commands:
   ```
   % reg import <snapshortdir>AtKey.reg
   % "xcopy /E <snapshotdir> <installdir>
   ```
   Sample output of the `reg import` command is as follows:
   ```
   C:\Program
   Files\Veritas\Security\Authentication\Snapshot>reg
   import AtKey.reg
   The operation completed successfully.
   ```
   Sample output of the `xcopy` command is as follows:
   ```
   C:\Program
   Files\Veritas\Security\Authentication>xcopy
   /ESnapshot
   Snapshot\systemprofile\ABAuthSource
   Snapshot\systemprofile\RBAuthSource
   Snapshot\systemprofile\VRTSatlocal.conf
   Snapshot\systemprofile\certstore\28b9d521.0
   Snapshot\systemprofile\certstore\bb7eb69b.0
   Snapshot\systemprofile\certstore\ef12cf8d.0
   Snapshot\systemprofile\certstore\keystore\ABPrivKeyFi
   le.pem
   Snapshot\systemprofile\certstore\keystore\ABPubKeyFil
   e.pem
   Snapshot\systemprofile\certstore\keystore\DummyWebPri
   vKeyFile.pem
   ```

```
Snapshot\systemprofile\certstore\keystore\DummyWebPub
KeyFile.pem
Snapshot\systemprofile\certstore\keystore\PrivKeyFile
.pem
Snapshot\systemprofile\certstore\keystore\PubKeyFile.
pem
Snapshot\systemprofile\certstore\keystore\RBPrivKeyFi
le.pem
Snapshot\systemprofile\certstore\keystore\RBPubKeyFil
e.pem
Snapshot\systemprofile\certstore\trusted\bb7eb69b.0
Snapshot\systemprofile\systruststore\28b9d521.0
16 File(s) copied
```

4 Start the broker by running the following command:

```
net start vrtsat
```

Glossary

The following are concepts necessary for understanding Symantec Product Authentication Service.

Application Host

The machine on which a Symantec application is running.

Authentication

Authentication is the validation of an identity. Clients are asked to identify themselves and to prove their identity. Once they have offered proof and it has been accepted, they are given a certificate, which they then combine it with their private key to make a valid product credential.

Authentication domain

Defines a set of identities for authentication principals. In addition, it can provide authorization information that is related to the principals in the set, such as group membership. An example is names in the Active Directory domain. A special type of authentication domain is the private domain, which is specific to Symantec.

Authentication library

Component that links with a Symantec application client and implements the program calls that request authentication. Conceptually, this library is separate from the part of authentication that is responsible for securing communications. In practice, both components may be part of a single library.

Authentication mechanism

The method by which authentication is conducted for principals in a specific name-space that a domain defines. For example, a Kerberos domain uses Kerberos tickets and password. An authentication mechanism encapsulates all the details of the authentication algorithm, including APIs, protocols, token formats, token contents semantics and database objects formats. Not all the ingredients are relevant in all mechanisms.

Authentication plugin

A component that the authentication broker uses to validate identities within a particular domain type.

Certificate

A certificate is a type of electronic passport or ID card. It vouches for the identity of its holder and binds the principal's name to his or her public key.

A hierarchy of certification authorities sign the certificates that vouch for the authenticity of principals. The root certification authority (on the root broker) is the entity at the top of the hierarchy and is therefore the most trusted certification authority. Its certificate, vouching for itself, is self-signed and is called the root certificate.

The application program environment includes the set of root certificates that the authentication library accepts as valid signers of credentials. This information can be either pre-configured or obtained from the Symantec application service. In principal, this root certificate could be stored as part of the registry configuration. In practice, however, it is traditionally kept in a separate file, or set of files, following one of a small collection of standard formats:

- PKCS#12 as the “standard”
- JKS for Java JSSE use
- PEM in OpenSSL and for S/MIME implementations

Credential

A product credential (or “credential” for short) is an entitlement to be recognized as an authenticated principal. It does include a certificate, but it must also include the principal’s private key. Without both parts, it is not a credential.

A product credential requires both of the following:

- The principal’s private key
- An X.509v3 certificate with special extensions
  The certificate is produced and signed by the authentication broker or root broker to bind the principal’s name to the public key.

The product credential is a single sign-on credential. The product credential is valid for all Symantec applications that are enabled to use Symantec Product Authentication Service and that choose to participate in the Symantec single sign-on session.

Who must have product credentials

Any Symantec resource management application has two components. Both of the following components must be authenticated with valid credentials:

- Symantec application client

A Symantec application client is a program that accesses a Symantec service or function that another program provides.

- Symantec application service
  A Symantec application service is the program that provides the requested services.

Both the client and the service act as clients when seeking authentication. The credential differs, depending upon whether it belongs to an application client or an application service. Generally service credentials have a longer life span than client credentials.

Security policy

A security policy is a well-thought-out set of decisions regarding such things as the following:

- How the product should be used in your environment
- How the product could be misused
- What range of access rules should be enforced by the product.

In order to set the range of allowable policy, think about the following:

- Who/what should use the product at all
- Who/what should be able to perform which tasks using which resources

Secure sockets layer protocol

Secure sockets layer (SSL) is a public key protocol and used for secure communications between clients and servers over the Web. For example, SSL protocol is often used for the transmission of credit cards and other sensitive data over the Internet.

SSL technology provides secured communication among the Symantec application client, authentication broker, and Symantec application service.

During authentication, the client uses the SSL layer for communicating with the authentication broker in order to request a product credential. Once the principal is authenticated, an SSL connection is established between the Symantec application client and the Symantec application service. They send and receive messages as necessary until the client terminates the communication.

Single sign-on authentication through the SSPI plugin

The Security Services Provider Interface (SSPI) from Windows provides a set of authentication and communication security services between applications running on Microsoft platforms.

Symantec Product Authentication Service works with the SSPI plugin to allow for unified login with Microsoft platforms. The user does not have to enter another password.

For example, assume that a user is already logged in to a Windows machine using the account/password of a Windows domain. Symantec Product Authentication Service uses SSPI to acquire a credential. This SSPI connection links the Symantec application client to the authentication broker. The communication from the Symantec application client to the Symantec application service is mutually authenticated over an encrypted channel. Upon authentication by the authentication broker, Symantec Product Authentication Service acquires all the OS groups that the principal belongs to.