Best Practices for Disaster Recovery with Symantec Endpoint Protection

Question/Issue:

How do I use Disaster Recovery with Symantec Endpoint Protection?

Solution:

This section references information covered in the "Installation Guide" (installation_guide.pdf) provided under the "Documentation" folder on the Symantec Endpoint Protection CD1.

How to prepare for disaster recovery

To perform disaster recovery, you must prepare for disaster recovery. You prepare for disaster recovery by collecting files and information during and after Symantec
Endpoint Protection Manager installation. For example, you must document your encryption password during the installation. You must locate and move your
keystore file to a secure location.

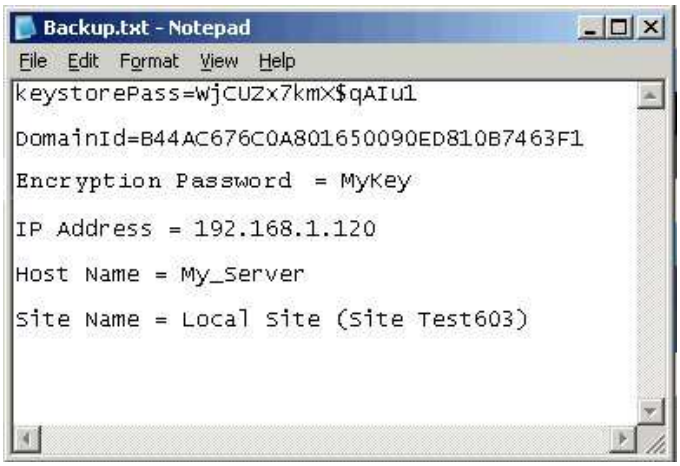
High-level tasks to prepare for disaster recovery:

Task	Additional information
Back up your database on a regular basis, preferably weekly, and store the backups off site.	The database backup directory is located in `\\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup`. The backup file is named <date_timestamp>.zip.
Locate your keystore file and your server.xml file. The keystore file name is keystore_<timestamp>.jks. The keystore contains the private-public key pair and the self-signed certificate. The server.xml file name is server_<timestamp>.xml.	During the installation, these files were backed up to the directory that is named `\\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup`. You can also back up these files from the Admin panel in the Symantec Endpoint Protection Manager Console.
Create and open a text file with a text editor. Name the file Backup.txt, or a similar name. Open server.xml, locate the keystorepass password, and copy and paste it into the text file. Leave the text file open.	The password is used for both storepass and keypass. Storepass protects the JKS file. Keypass protects the private key. You enter these passwords to restore the certificate. The password string looks like the below: keystorePass=`WjCUZx7kmX$qA1u1`
If you have one domain only, find and copy the sylink.xml file from a directory `in \\Program Files\Symantec\ Symantec Endpoint Protection Manager\data \outbox\agent\` . Then, paste it to `\\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup\`. If you have multiple domains, for each domain, locate and copy a sylink.xml file on a client computer. Then paste it into the following location: `\\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup.`	The domain IDs are required if you do not have a backup of the database. This ID is in the sylink.xml file on the clients computers in each domain.

Open each sylink.xml file, locate the DomainId, and copy and paste it into the Backup.txt text file. If the Symantec Endpoint Protection Manager was installed to a Custom Web site and configured to use a custom HTTP port, type the custom port in the Backup.txt text file.	You add this ID to a new domain that you create to contain your existing clients. The string in the sylink.xml file looks like DomainId=B44AC676C08A165009ED819B746F1. If the proper port is not used on restore, communication will not work properly.
In the Backup.txt file, type the encryption password that you used when you installed the first site in the installation instance. **Note**: If the Symantec Endpoint Protection Manager was installed in Simple mode, the password specified for use for the Admin account for the Symantec Endpoint Protection Manager is also the encryption password. If the Admin password is reset post-installation, the encryption password does not change.	You retype this key when you reinstall the Symantec Endpoint Protection Manager. You must retype the identical key if you do not have a backed up database to restore. It is not required if you have a backed up database to restore, but it is a best practice.
In the Backup.txt text file, type the IP address and host name of the computer that runs the Symantec Endpoint Protection Manager.	If you have a catastrophic hardware failure, you must reinstall Symantec Endpoint Protection Manager on a computer that has the same IP address and host name.
In the Backup.txt file, type the site name that identifies Symantec Endpoint Protection Manager. Save and close the Backup.txt file, which now contains the essential information that is required for disaster recovery.	While the site name is not strictly required for reinstallation, it helps to create a consistent restoration.
Copy these files to removable media, and store the media in a secure location, preferably in a safe.	After you secure the files, you should remove these files from the computer that runs the Symantec Endpoint Protection Manager.

C Appendix

The following illustrates a text file that contains the information that is required to perform a successful disaster recovery.



If you create this file, you can copy and paste this information when required during disaster recovery.

About the disaster recovery process

The disaster recovery process requires you to sequentially complete the following procedures:

- Restore the Symantec Endpoint Protection Manager.
- Restore the server certificate.
- Restore client communications.
  Note: How you restore client communications depends on whether or not you have access to a database backup.

Restoring the Symantec Endpoint Protection Manager

If you have a disaster, recover the files that were secured after initial installation. Then open the Backup.txt file that contains the passwords, domain IDs, and so
forth.

About identifying the new or the rebuilt computer
If you had a catastrophic hardware failure, you may need to rebuild the computer. If you rebuild the computer, you must assign it the original IP address and host
name. This information should be in the Backup.txt file.

Reinstalling the Symantec Endpoint Protection Manager
The key task to perform when you reinstall the Symantec Endpoint Protection Manager is to type the same encryption password you specified during installation
of Symantec Endpoint Protection Manager on the server that failed. You should also use the same settings that you used for other options during the previous
installation, such as Web site creation, database type, and password used for the admin user account.

Restoring the server certificate
The server certificate is a Java keystore that contains the public certificate and the private-public key pairs. You must enter the password that is contained in the
Backup.txt file. This password is also in the original server_timestamp.xml file.

To restore the server certificate
1. Log on to the Console, and then click **Admin**.
2. In the Admin pane, under Tasks, click **Servers**.
3. Under View Servers, expand Local Site, and then click the computer name that identifies the local site.
4. Under Tasks, click **Manage Server Certificate**.
5. In the "Welcome" panel, click **Next**.
6. In the Manage Server Certificate panel, check **Update the Server Certificate** and click **Next**.
7. Under "Select the type of certificate to import", check **JKS keystore** and click **Next**.
   Note: If you have implemented one of the other certificate types, select that type.
8. In the "JKS Keystore" panel, click **Browse**, locate and select your backed up as "keystore_<timestamp>.jks" keystore file, and then click **OK**.
9. Open your disaster recovery text file and then select and copy the keystore password.
10. Activate the "JKS Keystore" dialog box and then paste the keystore password into the "Keystore" and "Key" boxes.
    Note: The only supported paste mechanism is Ctrl + V.
11. Click **Next**.
    Note: If you get an error message that says you have an invalid keystore file, it is likely you entered invalid passwords. Retry the password copy and paste process as described above.
12. In the "Complete" panel, click **Finish**.
13. Log off of the Console.
14. Click **Start**> **Settings**> **Control Panel**> **Administrative Tools**> **Services**.
15. In the "Services" window, right-click **Symantec Endpoint Protection Manager** and click **Stop**.
    Note: Do not close the Services window until you are finished with disaster recovery and establish client communications.
16. Right-click **Symantec Endpoint Protection Manager** and click **Start**.
    Note: By stopping and starting Symantec Endpoint Protection Manager, you fully restore the certificate.

Restoring client communications
If you have access to a database backup, you can restore this database and then resume client communications. The advantage to restoring with a database backup
is that your clients reappear in their groups and they are subject to the original policies. If you do not have access to a database backup, you can still recover
communications with your clients, but they appear in the "Temporary group." Then you can recreate your group and your policy structure.

Restoring client communications with a database backup
You cannot restore a database on a computer that runs an active Symantec Endpoint Protection Manager service. You must stop and start it a few times.

To restore client communications with a database backup
1. If you closed the Services window, click **Start**> **Settings**> **Control Panel**> **Administrative Tools**> **Services**.
2. In the Services window, right-click **Symantec Endpoint Protection Manager**, and then click **Stop**.
   Note: Do not close the Services window until you are finished with this procedure.
3. Create the following directory:
   `\\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup`
4. Copy your database backup file to the directory.
   Note: By default, the database backup file is named date_timestamp.zip.
5. Click **Start**> **Programs**> **Symantec Endpoint Protection Manager**> **Database Back Up and Restore**.
6. In the Database Back Up and Restore dialog box, click **Restore**.
7. In the Restore Site dialog box, select the backup file that you copied to the backup directory, and then click **OK**.
   Note: The database restoration time varies and depends on the size of your database.
8. When the Message prompt appears, click **OK**.
9. Click **Exit**.
10. Click **Start**> **Programs**> **Symantec Endpoint Protection Manager**> **Management Server Configuration Wizard**.
11. In the Welcome panel, check **Reconfigure the Management Server**, and then click **Next**.
12. In the Server Information panel, modify input values if necessary to match previous inputs, and then click **Next**.
13. In the Database Server Choice panel, check the database type to match the previous type, and then click **Next**.
14. In the Database Information panel, modify and insert input values to match previous inputs, and then click **Next**.

Note: The configuration takes a few minutes.

15. In the Configuration Completed dialog box, click **Finish**.
16. Log on to the Symantec Endpoint Protection Manager Console.
17. Right-click your groups, and then click **Run Command on Group**> **Update Content**.
    Note: If the clients do not respond after about one half hour, restart the clients.

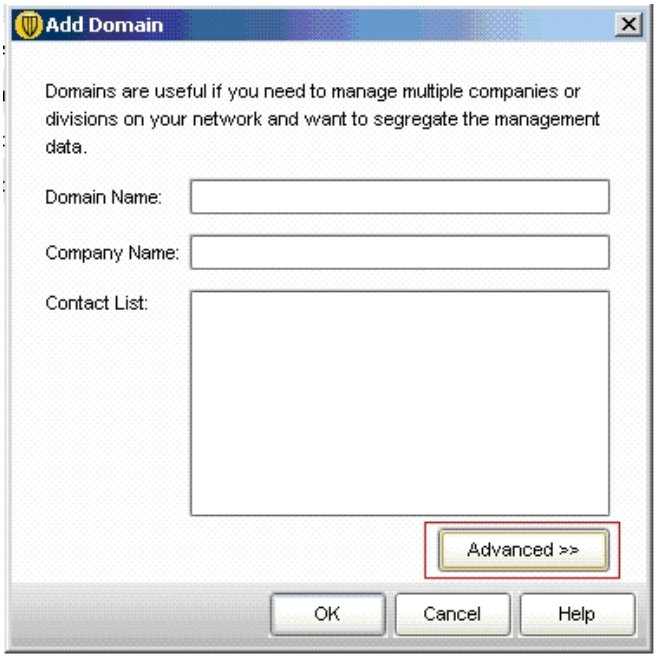
Restoring client communications without a database backup

For each domain that you use, you must create a new domain and insert the same domain ID into the database. These domain IDs are in the disaster recovery
text file if they were typed in to this file. The default domain is the "Default domain."

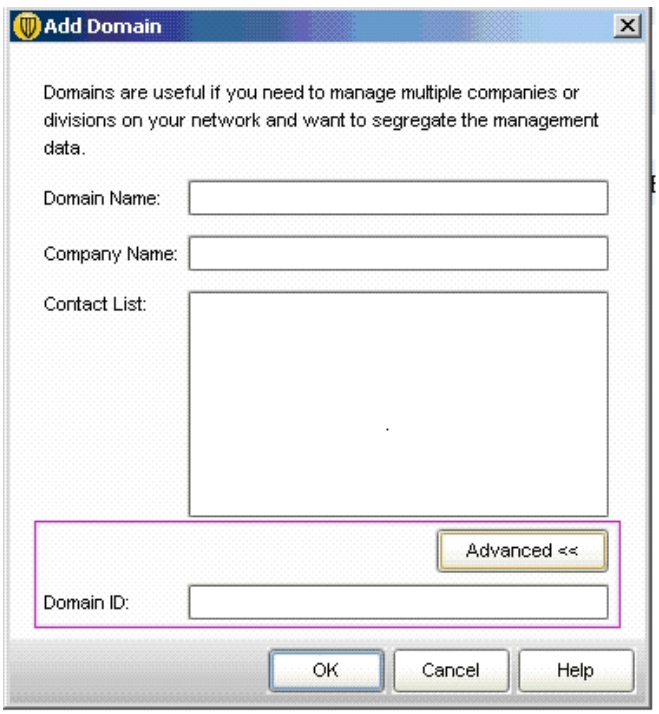
A best practice is to create a domain name that is identical to the previous domain name. To recreate the "Default (default) domain", append some value such as "_2"
(Example: Default_2). After you restore domains, you can delete the old default domain. Then rename the new domain back to "Default."

To restore client communications without a database backup

1. Log on to the Symantec Endpoint Protection Manager Console.
2. Click **Admin**.
3. In the "System Administrator" pane, click **Domains**.
4. Under "Tasks", click **Add Domain**.
5. Click **Advanced**.



6. Open the disaster recovery text file, select and copy the domain ID and then paste the domain ID into the "Domain ID" box.



7. Click **OK**.
8. Repeat this procedure for each domain to recover.
9. Under "Tasks", click **Administer Domain**.
10. Click **Yes** on the "Administer Domain" dialog box.
11. Click **OK**.
12. Restart all of the client computers.
    Note: The computers appear in the Temporary group.
13. If you use one domain only, delete the unused Default domain, and rename the newly created domain to Default.

References:

This document is available in the following languages:

- Brazilian-Portuguese: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/br_docid/20080227100719935
- French: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/fr_docid/20080229140832935
- German: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/de_docid/20080229140856935
- Italian: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/it_docid/20080229140919935
- Spanish: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/es_docid/20080227100747935

Available Translations:

--choose a language---

Other Support Options X

- Need More Help?
  Contact a Support professional through MySupport Online or Phone.
- Customer Care
  For non-technical assistance with product purchases, subscriptions, online services, events, training courses, corporate sales, and more.
- Support Forums
  Pose a question to other users. Discussion Forums about specific Symantec products.

Was this article helpful to you?

Yes No

If any information was unclear, or the information you were seeking was not provided, please let us know. Your feedback will help us improve this service.

(Enter comment here)

(Optional Email Address)

Submit

NOTE: Comments entered here will NOT receive support services. If you need Symantec Enterprise product support, please click here.

Document ID: 2007082112135948
Last Modified: 08/20/2008
Date Created: 08/21/2007
Operating System(s): Windows 2000 Professional, Windows 2000 Server/Advanced Server, Windows XP Professional Edition, Windows Server 2003 Web/Standard/Enterprise/Datacenter Edition
Product(s): Endpoint Protection 11
Release(s): Endpoint Protection 11 [All Releases], Endpoint Protection 11.0