Symantec System Recovery 2011: Support for Symantec and Third-Party Encryption Solutions

Symantec™ System Recovery 2011

To sustain your operations, your business, and even your brand, you need to recover from a system failure as quickly as possible. However, manual system recovery processes prolong system downtime – and potential losses.

Symantec System Recovery 2011 offers a superior solution by delivering fast and reliable system recovery that helps minimize downtime and meet recovery time objectives with confidence. In just four simple steps, quickly restore physical and virtual systems to bare metal in minutes, even to dissimilar hardware, virtual environments, or remote locations with Symantec's patented Restore Anyware technology.

Built on 10 years of research and development and with more than 787,000 protected systems, Symantec System Recovery (formerly Backup Exec System Recovery) is one of the most proven, trusted, and reliable system recovery solutions.

Built-in AES Encryption Support

Symantec System Recovery 2011 includes built-in software encryption that enables administrators to ensure the security and integrity of their critical business data when it is protected by Symantec System Recovery and stored to disk in the form of backup files known as recovery points. Backup jobs can be configured to store recovery points in 128-bit, 192-bit, or 256-bit AES encrypted format. A password of sufficient length must be provided (password length depends upon the encryption level selected) to enable this capability.

It is important to note that there is no "back door" mechanism built into the Symantec System Recovery 2011 product to enable access to encrypted recovery points when the user is unable to supply the required password. Without the correct password, the encrypted recovery point will be inaccessible.

In production environments, it is highly recommended that encryption be used when creating recovery points with Symantec System Recovery, even when recovery points are maintained on disk storage within an organizations physical boundary. When recovery points are stored to removable media for offsite transport, or stored to remote network or FTP locations outside of an organizations physical boundary, the need for encryption is even greater.

When using encryption with Symantec System Recovery, a small amount of additional time will be required for backup jobs to complete due to the additional encryption processing load.

Using Symantec System Recovery with Symantec Endpoint Encryption

Symantec Endpoint Encryption provides advanced encryption for desktops, laptops, and removable storage devices. It offers scalable, enterprise-wide security that prevents unauthorized access by using strong access control and powerful encryption.

Using Symantec System Recovery alongside Symantec Endpoint Encryption is fully supported by Symantec. Symantec System Recovery can protect systems also running Symantec Endpoint Encryption and perform bare metal and dissimilar hardware recovery operations of these systems. Please note the following considerations when using Symantec System Recovery to protect systems also running Symantec Endpoint Protection:

Backup Considerations:

- If the system disk (the disk to which Windows is installed) contains multiple volumes, all volumes on that disk should be backed up. When a restore is performed using the Symantec Recovery Disk (SRD), the target disk will be encrypted and unintelligible. As such, when a restore operation from the SRD is performed to that disk, all data on that disk is removed as a part of the restore operation. If only one volume on that disk was backed up, then only one volume will be restored to that disk, potentially resulting in data loss if the disk contained more than one volume originally.
- System and data volumes that are protected with Symantec Endpoint Encryption do not need to be unencrypted before Symantec System Recovery can protect them.
- Symantec System Recovery will see the volumes protected by Symantec Endpoint Encryption in plaintext mode in Windows, and resulting backups are also stored in an unencrypted or plaintext state. For this reason, it is recommended that Symantec System Recovery's own software AES encryption feature be used to encrypt recovery points to ensure data remains securely protected while stored in backup format.
- If recovery points are stored to a direct-attached disk device (such as a USB drive), and that device is also protected by Symantec Endpoint Encryption, Symantec System Recovery will not be able to recover backups using the Symantec Recovery Disk from the direct-attached disk device, as the device will appear as unintelligible due to the encryption.
    - Backups stored to encrypted direct-attached disk devices will have to be temporarily moved to a different location (such as an unencrypted USB device or a network share) in order for recovery to be possible.
    - When using direct-attached disk devices for backup storage, consider leaving the external drive unencrypted and using Symantec System Recovery's built-in software encryption to encrypt the backups stored there. This ensures that the data contained within the backups remains encrypted, and also allows the Symantec Recovery Disk to perform full system recovery tasks directly from the external drive.

Restore Considerations:

- Granular recovery operations that occur within Windows (such as those performed using the Granular Restore Option) are not affected by the presence of Symantec Endpoint Encryption. The Granular Restore Option is a Windows application, and because these restore operations are done within the Windows framework the Symantec Endpoint Encryption solution will be actively running and will be transparent to the granular restore process.
- Cold imaging (creating a backup from the recovery environment) of volumes protected by Symantec Endpoint Encryption is not supported. The encrypted volumes will appear to the Symantec Recovery Disk as encrypted and unintelligible.
- When performing a full system recovery or dissimilar hardware recovery operation using the Symantec Recovery Disk, be sure to select the "Restore master boot record" option.
- After a bare-metal or dissimilar hardware recovery event, disk volumes will need to be re-encrypted.
- LightsOut Restore is not supported on systems running Symantec Endpoint Encryption.

- When performing a data volume recovery operation within Windows, the following error may occur at the end of the restore operation:

  Error EC8F178F: Cannot complete the restore of recovery point: D:\SEE\Data_HotBackup\BESR_XP1_F_Drive001_i004.iv2i. Error EBAB03F1: Access is denied.

  In spite of this error, the volume will have been restored successfully. Initially the drive will not appear in Windows explorer (meaning it has no drive letter assignment). Simply use Disk Management to add a drive letter to the volume and it will be accessible.

- For multi-partition, data disk restore of the first partition of a disk should only be done by disabling encryption of the entire disk.

Physical to Virtual (P2V) Conversion Considerations:

- For P2V operations, the resulting virtual disk files will be stored in unencrypted format (similar to recovery points). In addition, virtual disks created using Symantec System Recovery's P2V capabilities cannot be encrypted with Symantec System Recovery's own software AES encryption feature.
  - Once a virtual machine is launched using the virtual disk files however, the virtual disks can be re-encrypted by Symantec Endpoint Encryption.

Using Symantec System Recovery with Microsoft Bitlocker

Using Symantec System Recovery alongside Microsoft Bitlocker is supported. Symantec System Recovery can protect systems also running Microsoft Bitlocker and perform bare metal and dissimilar hardware recovery operations. The behavior of Symantec System Recovery when used on systems also protected by Microsoft Bitlocker is generally the same as the behavior seen on systems protected by Symantec Endpoint Protection.

Using Symantec System Recovery with Other Third-party Encryption Solutions

Other third-party encryption solutions have not been officially tested with Symantec System Recovery and as such are not officially supported. However, in most cases the behavior of Symantec System Recovery when used alongside other third-party encryption solutions should be similar to the behavior seen with Symantec Endpoint Encryption and the Microsoft Bitlocker solution.

For More Information

Link	Description
www.symantecsystemrecovery.com	Symantec System Recovery Website
http://www.symantec.com/business/support/index?page=home&locale=en_us	Symantec Support Portal
http://entsupport.symantec.com/umi/V-306-38	Symantec System Recovery Software Compatibility List