Tintri

TECHNICAL WHITE PAPER

Tintri SecureVM

Encryption of Data at Rest

Revision History

Version	Date	Description	Author
1.0	06/07/2017	Initial Release	Tintri Technical Marketing

Table 1 - Revision history

Contents

Executive Summary

Encryption of data at rest is an essential element in protecting valuable data from unwanted access. This white paper describes the Tintri SecureVM encryption solution, available for use with many Tintri VMstore models. Supported VMstore arrays ship with self-encrypting drives (SEDs) that use the AES-256 (Advanced Encryption Standard) algorithm to encrypt all data written to the drives. Access to each drive is controlled by an authentication key.

Authentication keys can be managed either internally to the VMstore array, or externally using a supported KMIP-compliant external key server. Internal key management protects data when drives are stolen, lost, or returned to the vendor. External key management protects against those threat models, and also protects against the theft or loss of an entire storage system.

This guide explains how SecureVM works and how to enable and use SecureVM with either internal or external key management. It also describes how to change (rotate) authentication keys, and how to backup keys and cryptographically lock an entire storage system when external key management is used.

Consolidated List of Practices

The table below includes the recommended practices in this document. Click the text on any of the recommendations to jump to the section that corresponds to each recommendation for additional information.

DO: Keep in mind that enabling encryption is an irreversible process. You should review all relevant documentation and release notes for the version of Tintri OS you are running prior to enabling encryption. This white paper does not take the place of the VMstore documentation.

DO: Successfully test an external key server configuration prior to enabling encryption.

DO: Engage professional assistance when deploying external key management.

DO: Rotate keys if you suspect authentication keys have been compromised according to your site procedures.

DO: Backup keys and store at least one backup external to the key management server after deployment and anytime you rotate keys or make other changes.

DO: Disable the “Exportable” property of keys and power down a VMstore array you suspect has been compromised following procedures for your site.

Intended Audience

This paper is intended for security administrators, virtualization administrators, and other technology implementation staff. It explains key features of the SecureVM solution including encryption keys and key management. It is intended to help you evaluate the Tintri SecureVM solution and can also help you plan for SecureVM deployment.

Introduction: Tintri SecureVM Overview

Tintri released Tintri SecureVM in 2014 to satisfy the requirement for encryption of data at rest that has become common in sensitive industries such as finance, government, defense and healthcare. SecureVM is designed to satisfy tough policy and regulatory requirements.

Tintri SecureVM encrypts the Tintri VMstore file system and operating system to provide increased data security. It is designed to deliver the security, simplicity, and performance that your IT team needs to be successful.

- **Security.** With SecureVM, data is encrypted inline using the AES 256-bit algorithm. Encryption keys can be rotated on demand if you suspect a key has been compromised for any reason.

- **Simplicity.** SecureVM is easy to activate and manage. Support for replication between encrypted and non-encrypted VMstore arrays makes it easy for your team to address changing data management requirements.

- **Performance.** SecureVM uses self-encrypting devices—self-encrypting Solid State Drives (SSDs) and/or Hard Disk Drives (HDDs) depending on the VMstore model—that perform encryption internal to each device. As a result, VMstore array performance will not decrease when encryption is enabled, and there is no wait time for existing data to be encrypted when the solution is initially enabled. Effective capacity also remains the same when the solution is enabled.

Supported VMstore Series

The SecureVM feature works with the following Tintri VMstore models:

- Hybrid-Flash arrays running Tintri OS 3.1 or later:
    - T600 Series
    - T800 Series
- All-Flash arrays running Tintri OS 4.0 or later:
    - T5000 Series

Self-Encrypting Drives and Encryption Keys

Supported Tintri VMstore array models ship from the factory with self-encrypting drives. These drives use AES-256 encryption to encrypt all data written to the drive. Each self-encrypting drive comes with a built-in 256 bit media encryption key stored within the device. All writes to a drive are encrypted (and all reads are decrypted) using the media encryption key. Encryption at the drive level cannot be disabled.

When you obtain a license and enable SecureVM, each self-encrypting drive enters authenticated access mode. An authentication key is then required to access the media encryption key. The authentication key is a randomly generated 256-bit number. The authentication keys are controlled and managed by enabling encryption, rotating the keys, or disabling the “Exportable” property of the keys (disabling the “Exportable” property of keys is only supported with external key management).

Internal and External Key Management

With SecureVM, authentication keys can be stored and managed either internally or externally.

- **Internal key management.** Authentication keys are stored internally on the VMstore array in segments. The complete set of key segments required to construct the authentication key for a given drive are not stored on the device itself. Without the entire authentication key, the media encryption key cannot be accessed. As a result, encrypted data on the drive cannot be decrypted if the drive is lost, stolen, or if a defective drive is returned.

- **External key management.** Authentication keys are stored on an external key management server using the Key Management Interoperability Protocol (KMIP). External key management requires Tintri OS 4.3 or later.

Rotating Authentication Keys

With both internal and external key management, authentication keys can be changed whenever necessary. The process of changing the keys is commonly referred to as "key rotation".

When you navigate to the Hardware tab of the Tintri management console, you will notice a lock icon to the right of the "Disks" heading. The presence of the lock icon indicates that SecureVM is enabled. (Note that the interface is slightly different on an all-flash VMstore. See the *Tintri VMstore All Flash/Hybrid System Administration Manual* for details.)

Figure 1 - Hardware tab with SecureVM enabled

Hovering the mouse pointer over the lock icon will show you when the key was last rotated.

Figure 2- Hardware tab key rotation dialog

Clicking the lock icon opens a dialog window that shows when the key was last rotated and also provides the option to rotate the key. Rotating the key generates a new authentication key that takes the place of the existing key. Tintri also provides a PowerShell cmdlet to perform key rotation, which is available with the Tintri Automation Toolkit.

Key Management and Threat Models

The choice of internal or external key management is based on the threat models you need to protect against.

With internal key management, data is secure if one or more drives are lost, stolen, or if a defective drive is returned. The data is secure because the entire authentication key for a given drive is not stored on the device itself. Without access to the authentication key, the media encryption key cannot be accessed, and data on the drive is effectively locked.

In addition to the threat models protected against with internal key management, external key management also provides protection against VMstore array theft or loss. The data on the VMstore array is secure because the authentication keys are stored external to the array itself. Without access to authentication keys, media encryption keys cannot be accessed and data on the entire VMstore array is effectively locked.

External key management also includes the ability to cryptographically lock a VMstore array. For instance, you can cryptographically lock a VMstore array while it's in transit or if you believe it has been compromised within the datacenter. (See the section *Managing External Keys* for more information on cryptographic locking.)

Key Management	Drive Theft or Loss	VMstore Theft or Loss	Cryptographic Lock
Internal	✓		
External	✓	✓	✓

Table 2 - Threat model coverage summary

If you choose internal key management, you can convert to external key management later should your requirements change. Note that it is not possible to convert from external key management to internal key management.

The following sections explain more about the use of SecureVM with internal or external key management.

Using Tintri SecureVM with Internal Key Management

When internal key management is enabled, authentication keys are generated and stored in multiple segments distributed across the VMstore. Multiple copies of each authentication key's segments are stored to ensure that the keys can be reconstructed in the unlikely event of one or more component failures.

Enabling Tintri SecureVM with Internal Keys

Enabling SecureVM is simply a matter of providing a license key and enabling encryption with internal keys by means of the Tintri user interface. Note that enabling encryption cannot be reversed, so you should be absolutely certain you are ready to enable encryption before doing so.

If installing a SecureVM license on an existing system, you must add the encryption license first before enabling encryption. If your system has a pre-installed SecureVM license, you only need to enable encryption.

Licenses and encryption settings are configured by accessing the **Settings** option on the application bar of the Tintri management console.

To add an encryption license:

1. In the sidebar of the Settings pane, click **more** and select **Licenses**.

2. Enter the license key in the **Add new license** field. All valid licenses are added automatically. The added license will be displayed in the Installed Licenses section.

To configure internal key management:

1. Select the **Local** option in the pop-up dialog.
2. Click **Encrypt now**.

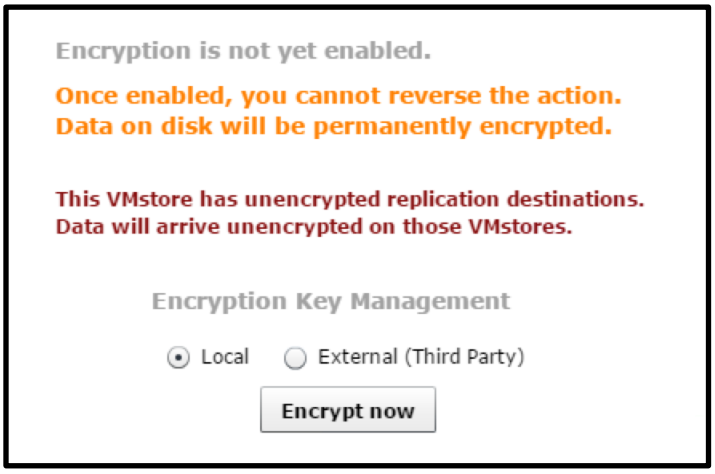

Figure 3 - Configuring internal key management

Because the data on each drive has already been encrypted using the media encryption key, the VMstore array is immediately secured. You don't have to wait hours for the data to be encrypted after SecureVM is enabled. When authentication keys are stored internally, no management is required other than key rotation as described in the earlier section titled *Rotating Authentication Keys*.

DO: *Keep in mind that enabling encryption is an irreversible process. You should review all relevant documentation and release notes for the version of Tintri OS you are running prior to enabling encryption. This white paper does not take the place of the VMstore documentation.*

Using Tintri SecureVM with External Key Management

External key management is supported with Tintri OS 4.3 and later versions. When external key management is used, a secure independent server acts as the key manager. The key management interoperability protocol (KMIP) provides communication between the VMstore array and key server.

Tintri has partnered with Gemalto, maker of SafeNet KeySecure, for external key management. At the initiation of support, KeySecure versions 8.2 and 8.4 are supported, and can be deployed either as a physical or virtual server. Tintri compatibility matrices should be reviewed to confirm that the version being deployed is supported. With either server type, the key server should always be configured so that it is highly available. This is referred to as "clustering" in the SafeNet KeySecure Appliance Administration Guide.

When encryption is enabled on the VMstore array using external key management, signed RSA security certificates are required. These certificates must be exchanged to establish trust before authentication keys are accessible by a given VMstore array. Certificates are supported in PEM (Privacy-Enhanced Electronic Mail) format. The SafeNet KeySecure Appliance Administration Guide provides detailed

information on how to create the certificates needed to configure external key management with the Tintri VMstore array.

The SafeNet KeySecure management interface allows you to perform a variety of functions including creating and managing certificates and certificate authorities, as well as viewing and managing keys and other objects. All Tintri VMstore array authentication keys are prefixed with "tintri-vmstore-*serial number*" making it possible to determine which keys are associated with a given VMstore array.

Enabling Tintri SecureVM with External Keys

Enabling SecureVM is accomplished by providing a license key, if one has not already been installed, and enabling encryption with external keys by means of the Tintri user interface. Note that the encryption process cannot be reversed, so you should be absolutely certain everything is properly configured and you are ready to enable encryption before doing so.

While configuring encryption with external keys is not difficult, there are potentially serious consequences if a mistake is made. Configuration should be performed by a qualified professional.

To configure the VMstore array to use external keys, you must supply the fully qualified domain name(s) of the key server(s) and the port number. The full process is described in detail in the Tintri VMstore All-Flash/Hybrid System Administration Guide for Tintri OS 4.3.

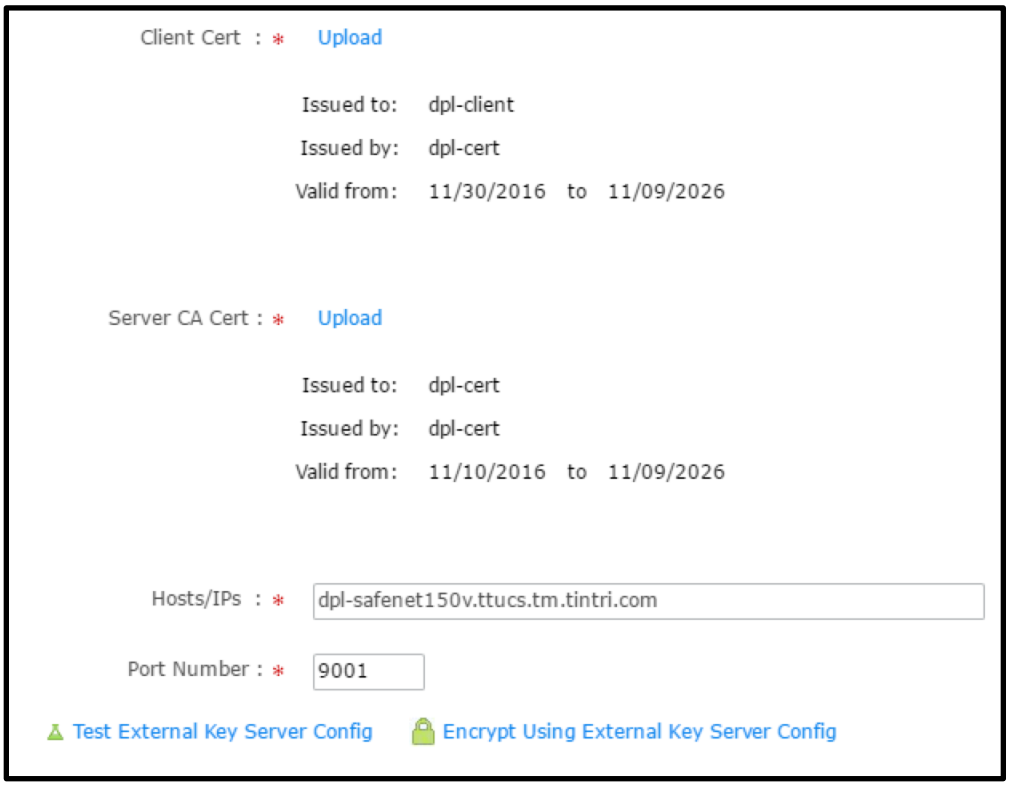

Figure 4 - Configuring SecureVM with external key management

Note that you can test the key server configuration from the settings dialog box before enabling encryption.

DO: *Successfully test an external key server configuration prior to enabling encryption.*

VMstore Array Boot Process with External Key Management

It's important to understand the VMstore boot process that occurs when external key management is in use. The following sequence summarizes the process.

- When a controller is powered on the VMstore array configuration is checked to see if external key management is enabled. If external key management is enabled, the VMstore array will execute a series of steps to retrieve the authentication keys from the external key manager. Note that controller power on occurs when a VMstore array is initially power on, or in the event of a controller replacement.
- When the VMstore array is initially powered on, each of the two controllers will connect to the external key server and independently retrieve the authentication keys.
- When one of the two controllers is already powered on and active, and the other controller is plugged into the chassis, the newly powered on controller will connect to the active controller. The active controller will retrieve the authentication keys and pass them to the newly powered on controller. This process occurs when a standby controller is replaced or re-seated as directed by Tintri Technical Support.
- Successful retrieval of authentication keys from the external key manager allows the controller to unlock all disks, which enables the controller to boot normally. Failure to retrieve authentication keys results in failure to unlock the drives, and the boot process cannot proceed.

Managing External Keys

When authentication keys are managed externally, there are several tasks that can be performed. Key rotation is performed from the Tintri user interface, or by means of the Tintri Automation Toolkit. The remaining tasks are performed from the external key management console.

- **Rotate keys.** If you suspect authentication keys have been compromised, you should rotate the key as described in the earlier section *Rotating Authentication Keys*.
- **Viewing keys.** Keys are easily viewed from the SafeNet KeySecure management console.

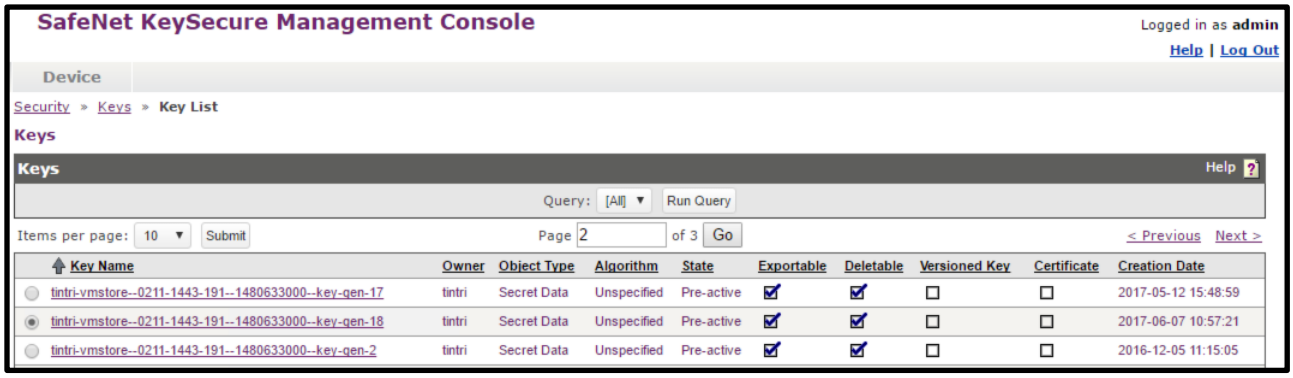

Figure 5 - Authentication keys and properties

- **Backup keys.** It's important to backup the keys and other information stored on the external key manager to protect against catastrophic failure. If keys are lost and can't be recovered, your data becomes inaccessible. This task is performed by selecting "Backup & Restore" from the Maintenance pane of the SafeNet KeySecure management console. This will bring up a dialog that allows you to select the keys and other objects you want to protect and specify where to put the backup. You provide a password that is used to encrypt the backup so that it is secure. Backups can be stored locally on the KeySecure key management server or downloaded to an external system.

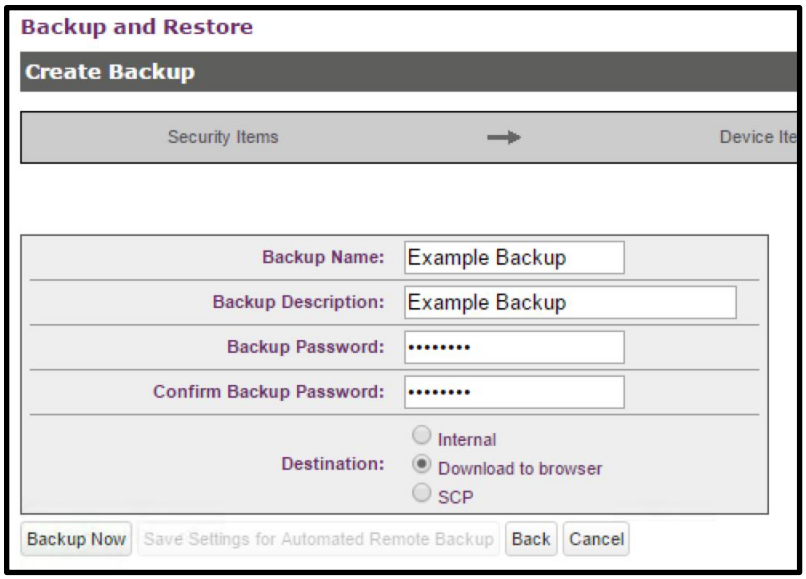

Figure 6 - Create Backup dialog

- **Cryptographic lock.** Situations may arise where you need to cryptographically lock a VMstore array. For example, you suspect a VMstore has been compromised. By disabling the "Exportable" property, the authentication keys can no longer be accessed by the VMstore array controllers. By powering the VMstore array off, you effectively render the data contained in the array inaccessible. If the array is powered on, neither controller will be able to retrieve the authentication keys, the disks will remain locked, and neither controller will be able to successfully complete the boot process. To cryptographically lock a VMstore array:

  1. Navigate to the Security tab in the SafeNet KeySecure management console.
  2. Choose **Keys** from the Managed Objects pane.
  3. Select the key for which you want to disable the "Exportable" property and then click the **Properties** button.
  4. De-select the **Exportable** property.
  5. Save the configuration change.

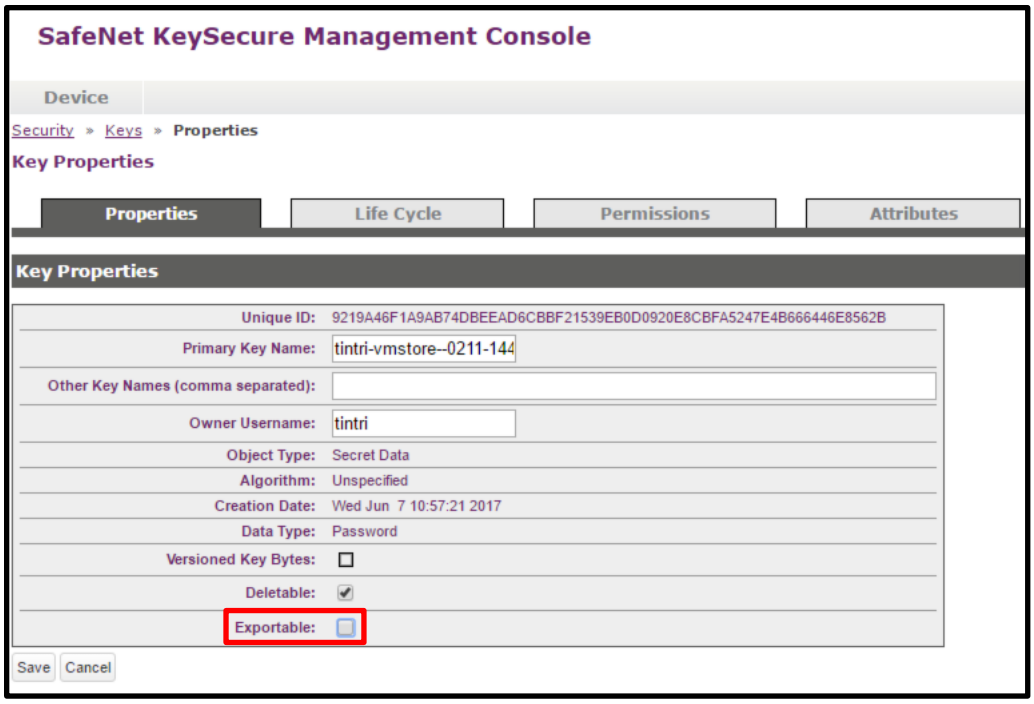

Figure 7 - Exportable property disabled

DO: *Engage professional assistance when deploying external key management.*

DO: *Rotate keys if you suspect authentication keys have been compromised according to your site procedures.*

DO: *Backup keys and store at least one backup external to the key management server after deployment and anytime you rotate keys or make other changes.*

DO: *Disable the "Exportable" property of keys and power down a VMstore array you suspect has been compromised following procedures for your site.*

Conclusion

Tintri SecureVM is a simple to use encryption solution available for use with many Tintri VMstore models. When configuring SecureVM you have the choice of internal key management or external key management. External key management uses a secure key management server to store authentication keys. The option you select depends on the threat models you need to protect against.

For more information on Tintri SecureVM refer to the Tintri System Administration Manual or contact your Tintri sales team.

References

Tintri documentation is available on the Tintri Technical Support portal, support.tintri.com (login required).

- Tintri VMstore All Flash/Hybrid System Administration Manual
- Tintri Automation Toolkit Quick Start Overview Guide

Gemalto SafeNet KeySecure documentation is available through Gemalto.

- SafeNet KeySecure Appliance Administration Guide

303 Ravendale Drive
Mountain View CA 94043
+1 650.810.8200
info@tintri.com