vmware®

VMware ACE

Virtual Machine Encryption Basics

VMware ACE gives administrators the option of enhancing the security of virtual machines they distribute to end users by encrypting key data and configuration files. This technical note provides an introduction to the encryption used in VMware ACE. It covers the following topics:

- Setting Policies to Control Encryption on page 1
- Understanding When Encryption Is Applied on page 2
- Updating Encryption Policies on page 5

Setting Policies to Control Encryption

Some files in a VMware ACE package are encrypted in all cases, whatever the policy settings may be. Other files are encrypted only if administrators make certain policy settings.

To set policies that control encryption for a virtual machine, open the policy editor and, in the list of policies for that virtual machine, select **Encryption and authentication**. Two settings directly affect encryption.

- **Encrypt data and configuration files when this virtual machine is installed**

  To protect the contents of the virtual machine, you can specify that the package installer encrypts the virtual machine when it is installed. To do so, select **Encrypt data and configuration files when this virtual machine is installed**. Each installation of the virtual machine — for example, on different end users' computers — is encrypted differently.

  You must specify an authentication method under **Authentication** if you want the installer to encrypt the virtual machines.

- **Protect virtual machine configuration files from user tampering**

  If you encrypt the virtual machine, its configuration files are automatically protected against viewing and tampering. Even if you do not encrypt the virtual machine, you may select **Protect virtual machine configuration files from user tampering**.

In addition, the settings under **Authentication** affect the way encryption keys are generated and stored, as described in this technical note.

vmware®

Understanding When Encryption Is Applied

VMware ACE uses the Advanced Encryption Standard (AES) with 128-bit keys.

VMware ACE derives password-based keys from the user's password using an industry-standard algorithm. It generates all other keys using random data provided by the Windows CryptoAPI using industry-standard algorithms.

Administrators who want to specify an existing key for use as a recovery key may import that key using the policy editor.

Encrypted file data is decrypted in memory only and only as it is needed.

The three tables below provide details on which files are encrypted and when encryption is applied.

Encryption in a Package Before Installation

The following table summarizes the various files that make up a package and notes whether and how they are encrypted in transit, before the package is installed on the end user's computer.

File Type	Encryption Notes
Application policy file (`app.vmpl`)	**Encrypted:** Always encrypted when the package is created. **Decrypted:** Not decrypted in transit. The key, called the obfuscation key, is stored in the clear in the installation package metadata.
Application preferences file (`preferences.ini`)	**Encrypted:** Always encrypted when the package is created. **Decrypted:** Not decrypted in transit. The key, called the obfuscation key, is stored in the clear in the installation package metadata.
Application configuration file (`config.ini`)	**Encrypted:** Always encrypted when the package is created. **Decrypted:** Not decrypted in transit. The key, called the obfuscation key, is stored in the clear in the installation package metadata.
Virtual machine configuration file (`.vmx`)	**Encrypted:** Encrypted when the package is created if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Not decrypted in transit. The key, called the obfuscation key, is stored in the clear in the installation package metadata.
Virtual disk files (`.vmdk`)	**Encrypted:** The disk descriptor portion of the virtual disk file or files is encrypted if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. Virtual disk data is not encrypted. **Decrypted:** Not decrypted in transit. The key is a symmetric key stored in the encrypted configuration file.
BIOS settings file (`nvram`)	**Encrypted:** Encrypted only if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Not decrypted in transit. The key, called the auxiliary data key, is stored in the encrypted configuration file.
Virtual machine policy file (`.vmpl`)	**Encrypted:** Always encrypted when the package is created. **Decrypted:** Not decrypted in transit. The key, called the obfuscation key, is stored in the clear in the installation package metadata.

Note: If you need greater security for the package before it is installed on the end user's computer, you may want to use a third-party utility to encrypt the installation package.

Encryption in an Installed Package Before It Is Run for the First Time

The following table summarizes the various files that make up a package and notes whether and how they are encrypted after the package is installed but before the user runs the installed package for the first time.

File Type	Encryption Notes
Application policy file (`app.vmpl`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Not decrypted before the user runs a virtual machine in the package for the first time. The key, called the obfuscation key, is hidden on the end user's computer.
Application preferences file (`preferences.ini`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Not decrypted before the user runs a virtual machine in the package for the first time. The key, called the obfuscation key, is hidden on the end user's computer.
Application configuration file (`config.ini`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Not decrypted before the user runs a virtual machine in the package for the first time. The key, called the obfuscation key, is hidden on the end user's computer.
Virtual machine configuration file (`.vmx`)	**Encrypted:** Remains encrypted if it was encrypted when the package was created — that is, if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Not decrypted before the user runs the virtual machine. The key, called the obfuscation key, is hidden on the end user's computer.
Virtual disk files (`.vmdk`)	**Encrypted:** The disk descriptor portion of the virtual disk file or files is encrypted if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. Both the virtual disk descriptor and virtual disk data are encrypted only if the encryption policy is set to **Encrypt data and configuration files when this virtual machine is installed**. The encryption of virtual disk data takes place at the time the package containing the virtual machine is installed on the end user's computer. **Decrypted:** Not decrypted until the user runs the virtual machine. The key is a symmetric key stored in the encrypted configuration file. The same key is used to encrypt both the disk descriptor and the disk data.
BIOS settings file (`nvram`)	**Encrypted:** Encrypted only if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Not decrypted until the user runs the virtual machine. The key, called the auxiliary data key, is stored in the encrypted configuration file.
Virtual machine policy file (`.vmpl`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Not decrypted before the user runs the package for the first time. The key, called the obfuscation key, is hidden on the end user's computer.

Encryption in an Installed Package After It Is Run for the First Time

The following table summarizes the various files that make up a package and notes whether and how they are encrypted after the user runs the installed package for the first time.

File Type	Encryption Notes
Application policy file (`app.vmpl`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Using a key called the obfuscation key, which is hidden on the end user's computer.

File Type	Encryption Notes
Application preferences file (`preferences.ini`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Using a key called the obfuscation key, which is hidden on the end user's computer.
Application configuration file (`config.ini`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Using a key called the obfuscation key, which is hidden on the end user's computer.
Virtual machine configuration file (`.vmx`)	**Encrypted:** Re-encrypted with an authentication key if an authentication method was specified. **Decrypted:** Depending on the authentication policies set for the virtual machine, the keys may be generated in one of three ways. • For password authentication, the user specifies a password, the key is generated on the basis of the password. • For Active Directory authentication, the key is generated using random data and stored in a per-user-account area of the Active Directory server. • For authentication determined using a script, the script determines how the key is acquired.
Virtual disk files (`.vmdk`)	**Encrypted:** The disk descriptor portion of the virtual disk file or files is encrypted if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. Both the virtual disk descriptor and virtual disk data are encrypted only if the encryption policy is set to **Encrypt data and configuration files when this virtual machine is installed**. **Decrypted:** Using a symmetric key stored in the encrypted configuration file. The same key is used to encrypt both the disk descriptor and the disk data.
BIOS settings file (`nvram`)	**Encrypted:** Encrypted only if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Using a key called the auxiliary data key, which is stored in the encrypted configuration file.
Saved state files (`.vmss`)	**Encrypted:** Encrypted only if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Using a key called the auxiliary data key, which is stored in the encrypted configuration file.
Log files (`.log`)	**Encrypted:** Not encrypted. **Decrypted:** Not decrypted.
Virtual machine policy file (`.vmpl`)	**Encrypted:** Remains encrypted as it was when the package was created. **Decrypted:** Using a key called the obfuscation key, which is hidden on the end user's computer.
Screen shot file (`.png`)	**Encrypted:** Encrypted only if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Using a key called the auxiliary data key, which is hidden on the end user's computer.
Snapshot files (`.vmsn`)	**Encrypted:** If they exist, encrypted only if the encryption policies for the virtual machine include **Protect virtual machine configuration files from user tampering**. **Decrypted:** Using a key called the auxiliary data key, which is stored in the encrypted configuration file.
Lock files (`.lck`)	**Encrypted:** Not encrypted. **Decrypted:** Not decrypted. **Note:** No data is stored in these files.

Updating Encryption Policies

If you want to change any encryption-related policies, you may do so by distributing an update package to your end users. Depending on the file concerned, the change is applied either at the time the update package is installed or the next time the user runs the affected application or virtual machine.

VMware, Inc. 3145 Porter Drive Palo Alto, CA 94304 www.vmware.com
 Revision 20051209 Item: ACE-ENG-Q404-165