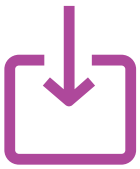
Townsend SECURITY

9 EASY STEPS TO DEPLOY ALLIANCE KEY MANAGER IN

VMware vSphere



1] INSTALL PRODUCTION ALLIANCE KEY MANAGER (AKM) OVA

Alliance Key Manager is a standard VMware virtual machine delivered in OVF or OVA format. Install the production AKM key server. Follow the AKM instructions in the vSphere Quick Start Guide to create two AKM servers - one to be primary and one to act as a failover.

2] CONFIGURE PRODUCTION/FAILOVER AKM

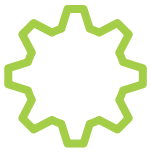
Use SSH to initialize the each AKM server as a primary. This is a one-time step that will create an internal PKI to secure the key manager and generate certificates that will be used by the vSphere KMS Cluster.

3] ACTIVATE MIRRORING

Use SSH to connect to the first AKM and follow the steps to establish mirroring to the second. Follow the AKM instructions in the Server Management Guide. Repeat this process for the second AKM to the first.

4] EXPORT PRODUCTION CERTIFICATES

Use the AKM File Manager to export the client-side certificates and CA certificate that will be used by the vSphere KMS Cluster.



5] CONFIGURE KMS CLUSTER FOR PRODUCTION & FAILOVER

Connect to vSphere and use the KMS Cluster option to define the Production and Failover key servers. The first entry will be the production key server, and the second entry will be the failover key server.

6] ESTABLISH TRUST IN VSPHERE

Use the vSphere option to establish trust between VMware and Alliance Key Manager. You are now ready to start VMware encryption.

7] ENCRYPT VMS

Use vSphere to select VMs to place under encryption control. Encryption keys will be created automatically by VMware and encryption of the VM will start immediately.

8] ENCRYPT VSAN

Use vSphere to select vSAN storage to place under encryption control. Encryption keys will be created automatically by VMware and encryption of vSAN storage will start immediately.

9] IMPLEMENT VTPM

You can implement vTPM with BitLocker and other facilities for OS encryption. vTPM uses the KMS Cluster you configured for key management support. See the VMware documentation for specific vTPM driver installation instructions.

ALLIANCE KEY MANAGER FOR VMWARE

Alliance Key Manager enables VMware customers to use native vSphere and vSAN encryption to protect VMware images and digital assets while deploying a secure, compliant and affordable key manager. VMware customers can deploy multiple, redundant key servers as a part of the KMS Cluster configuration for maximum resilience and high availability.

TOWNSEND SECURITY

Townsend Security creates data privacy solutions to help partners and businesses meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST-validated and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA, GDPR, CCPA, and other regulatory compliance requirements.