Alliance Key Manager Cloud HSM
Frequently Asked Questions

FAQ INDEX

This document contains a collection of the answers to the most common questions people ask about Alliance Key Manager Cloud HSM.

Townsend SECURITY

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

General

Q: What is Alliance Key Manager Cloud HSM

The Townsend Security Alliance Key Manager Cloud HSM provides a complete encryption key management solution to help you meet corporate and regulatory compliance requirements for data security in cloud environments. The Alliance Key Manager solution is a NIST FIPS 140-2 compliant hardware security module (HSM) that manages encryption keys through the key lifecycle, distributes encryption keys to authorized applications and databases, and provides on-device encryption services. The Alliance Key Manager Cloud HSM offering provides a pair (production and high availability failover) of encryption key servers in geographically separate, secure data centers. Cloud users and cloud partners can protect sensitive data with a dedicated HSM that is validated to government standards. Only you have access to the key management HSM - no access is available to your cloud vendor, hosting provider, or Townsend Security.

Q: What is a Hardware Security Module (HSM)?

A Hardware Security Module (HSM) is a dedicated security appliance that provides secure generation, storage, management, and distribution of encryption keys in a tamper-evident device.

Q: Am I locked into my cloud vendor?

No, you can deploy your applications in any cloud or hosting environment, and you can move those applications to other cloud platforms without constraint. Your cloud vendor has no access to the key management HSMs and you can change cloud vendors as needed.

Q: Can Alliance Key Manager protect data in Amazon, Azure, Rackspace and other clouds?

Yes, the Alliance Key Manager Cloud HSM can provide encryption and key management services for any cloud or hosting environment. You can deploy your client-side application data protection in any environment you wish, including international locations (subject to US export regulations).

Q: Can Alliance Key Manager protect data in cloud storage?

Yes, Alliance Key Manager does not restrict your ability to encrypt data in various cloud storage facilities. Your applications have full access to encryption keys and encryption services both inside your IT infrastructure and in your cloud applications. You can easily encrypt data before moving it to cloud storage, and cloud applications have access further encryption or decryption services.

Q: What can I do with Alliance Key Manager?

You can use the Alliance Key Manager HSM to provide encryption keys and encryption services to a wide variety of applications and databases on a number of operating systems and cloud platforms where sensitive data needs to be protected. In addition to key distribution and encryption services, Alliance Key Manager includes no-charge licences to ready-to-use encryption applications including Microsoft SQL Server Transparent Data Encryption (TDE) and Cell Level Encryption in the Extensible Key Management (EKM) architecture, Microsoft SharePoint encryption, support for IBM i FieldProc encryption, and more.

Q: How does Alliance Key Manager work?

When you purchase a perpetual or subscription license (see license options below) for the Alliance Key Manager Cloud HSM service you receive dedicated access to a production and a high availability key server. The key servers are accessible through a secure, authenticated TLS service to your applications and databases. After configuring the key server HSMs you will be able to retrieve encryption keys to your applications and databases and use encryption services on the device.

The key servers are dedicated to you and only you have access to the key servers for configuration, administration and cryptographic functions for industry leading key management.

Townsend Security and the hosting facility monitor the hardware HSM, key management applications, and network environment. You are notified in the event of any outage of primary or high availability failover HSM services, and your HSM services can seamlessly fail over to the high availability key server.

You use Alliance Key Manager applications, shared libraries and DLLs, and sample code to implement security in your client-side applications and databases.

Q: What happens if a key server or network segment fails?

The Alliance Key Manager Cloud HSM option always includes a high availability key server deployed in a geographically separate data center. Key servers are configured to mirror encryption keys and access policies in real time. In the event of a hardware failure of the key server, or the failure of a network segment, your applications and databases can immediately access the failover key server for cryptographic functions.

Q: Does Alliance Key Manager support SQL Server Transparent Data Encryption (TDE)?

Yes, the Alliance Key Manager license includes an unlimited license to use the Townsend Security Key Connection for SQL Server software. Key Connection for SQL Server is an Extensible Key Management (EKM) Provider that installs in your SQL Server environment to support both Transparent Data Encryption and Cell Level Encryption.

For editions of SQL Server that don't include EKM support, such as Standard and Web Editions, Alliance Key Manager includes software libraries to help you encrypt data.

Q: Does Alliance Key Manager support IBM Field Procedures (FIELDPROC)?

Yes, Townsend Security's Alliance AES/400 support for IBM i V7R1/V7R2 supports integration with Alliance Key Manager for FIELDPROC encryption. Alliance AES/400 is a separately licensed and priced software option.

Q: Does Alliance Key Manager support Oracle Database?

Yes, you can encrypt Oracle databases using software libraries and sample code that come with Alliance Key Manager. Examples include PL/SQL, Java, and other languages so that your developers can implement security quickly in Oracle database applications.

Q: Does Alliance Key Manager support MySQL database?

Yes, Alliance Key Manager comes with extensive examples of MySQL database encryption. In addition to working sample applications in Java, you can use a variety of development languages including PHP, Perl, Python, C# and others.

Q: I am a Java (C#, PHP, Perl, Python, etc.) developer. How do I get started?

Alliance Key Manager includes a wide variety of developer resources to help you get started. There is sample code and working sample applications that you can use as a starting point. All major development languages are supported.

Q: How does my application use Alliance Key Manager?

Your application can use the Alliance Key Manager purpose-built encryption applications, shared libraries and DLLs, or you can use the sample source code and applications provided with Alliance Key Manager. You do not need to do extensive research and development on obscure cryptographic APIs to get started. Many Alliance Key Manager customers experience success very quickly upon start of their data protection projects.

Q: Where is Alliance Key Manager available?

Alliance Key Manager Cloud HSM servers are available in Denver, Colorado and in Newark, Delaware. If you would like to deploy Alliance Key Manager in other hosting locations, or in your own data center, please Contact Us for more information.

Q: How do I get started with Alliance Key Manager?

To request an evaluation of Alliance Key Manager or to discuss the key management options available to you, please contact us.

Q: How long does Alliance Key Manager provisioning take?

Alliance Key Manager orders can usually be filled in one to two days. HSMs are pre-deployed in the hosting facility. Orders for larger numbers of key servers may take longer.

Q: Can I try the Alliance Key Manager service with my application before I sign up?

Townsend Security makes it easy for you to evaluate the Alliance Key Manager HSM solution. Our evaluation options give you the ability to fully evaluate the full set of key management and on-device encryption functions and client-side applications. There is no charge for evaluation versions of the key manager.

Reliability and Resilience

Q: Can I ever lose my encrpytion keys?

It is extremely unlikely that you could unintentionally lose your encryption keys if you follow backup and key server guidelines. Alliance Key Manager implements a number of protections to help you prevent the loss of an encryption key. All encryption keys are mirrored to a high availability key server in real time. Additionally, Alliance Key Manager backup and restore services let you make periodic scheduled or on-demand backups of your encryption keys and access policies. It is extremely difficult to lose an encryption key.

Q: How is Alliance Key Manager backed up?

Alliance Key Manager provides both scheduled and on-demand backups of the keys, applications, and access policies. You can backup the keys to a local directory, and download them to your local system. You can also schedule periodic, secure, automatic backups to your FTP server using the Secure Shell sFTP, SSL FTP, or FTP protocols. You can back up your keys to your own servers, or Townsend Security can provide a dedicated backup and log collection server in our hosting data center at an additional charge.

Q: Are the key servers monitored?

Yes, Townsend Security provides hardware and key manager application monitoring in the hosting facility. Both you and the Townsend Security customer support group are notified in the event of a potential or real failure. In most cases hardware failures will not interrupt the availability of the key server, and hardware maintenance will be performed without disruption. In some cases Townsend Security or its hosting partner will need to repair and or replace the key server. You will be notified if this occurs.

Q: What happens in case of failure?

Townsend Security monitors the key servers and optional backup and logging servers. Townsend's hosting partner monitors the network for failures. In the event of a failure Townsend Security will investigate the error and restore operations as soon as possible. If a key server HSM must be replaced, Townsend Security will notify you and will replace the HSM as soon as possible. Your client-side software should seamlessly fail over to the backup key server.

Pricing and Licensing

Q: How is Alliance Key Manager licensed?

There are two ways to license Alliance Key Manager Cloud HSM:

- A one-time perpetual license with annual hardware and software maintenance, and
- A monthly subscription license (see terms below)

In either case you will have a production and a high availability key server HSM dedicated to you. The perpetual license option provides additional ownership options.

Please contact Townsend Security for pricing information.

Q: Do I pay for client-side applications?

No. You never pay for client-side applications, or by the number of systems that connect to the key server, or by the number of keys you generate or use.

Q: How will I be charged and billed for my use of the Alliance Key Manager Cloud HSM service?

The perpetual license option is a one-time license fee and annual maintenance fee. After you complete your evaluation, you will be billed for the one-time license fee and one year of hardware and software maintenance. Payment is due before servers are allocated for your use.

The subscription license is a monthly subscription fee which includes hardware and software maintenance. You must pay the first year's subscription in advance. Subsequent to the first year, you will be billed on a monthly basis. You may terminate your subscription at any time. The first year of subscription is non-refundable. Subsequent pre-paid months will be refunded on a non-prorated basis.

Q: Will I be charged extra for a High Availability Failover key server?

No, the license fees cover two key servers – a production key server in the data center you specify, and a high availability key server in the other data center.

Q: Can I use more than two key servers?

Yes, you can license as many key servers as you wish. Please allow additional time to deliver more than two key servers. You can also purchase Alliance Key Manager for your own data center, or collocate the servers in a hosting provider of your choice. Key servers can be shipped to any location worldwide that is allowed by US export regulations.

Q: How do I terminate Alliance Key Manager service?

You may terminate your perpetual or subscription license at any time by notifying Townsend Security in writing 30 days in advance. It is your responsibility to save or migrate your encryption keys from the HSM, and then destroy the keys – Townsend Security does not have access to your key server HSMs. After terminating your license Townsend Security or its hosting provider will securely destroy the HSM disks containing your keys, or ship the key server HSMs to your location (perpetual license only).

Security and Compliance

Q: Has the data center where the key server is hosted been audited for security?

Hosting.com is committed to meeting the most stringent requirements and having internal controls in place to mitigate risks related to security, availability, and confidentiality for their cloud, dedication and colocation hosting along with their data center operation practices. To achieve this, they have completed both the SOC 2 and SOC 3 audits through the assistance of an independent auditing firm. In fact, they were one of the first managed cloud service providers to complete the SOC 2 and SOC 3 independent audits.

Q: Is the data center where the key server is hosted PCI compliant?

Hosting.com's talent and experience in PCI DSS compliance is far reaching. They helped develop the most recent version of the PCI DSS—specifically the virtualization and cloud components. They are a Level 1 service provider and since 2005, they have provided managed PCI compliance solutions for all types of organizations—from Level 1 service providers to Level 4 merchants. Additionally, their data center has undergone PCI certification as it pertains to physical security.

Q: Is Alliance Key Manager FIPS 140-2 compliant?

Yes, Alliance Key Manager has been validated to FIPS 140-2 Level 1 compliance (certificate 1449). This level of compliance is your assurance that the key management solution meets federal standards for encryption key management, and that it has been independently reviewed and assessed by a NIST chartered security testing laboratory.

Q: Does Townsend Security or anyone else have access to my key server?

No, only you have access to the Alliance Key Manager HSMs. Neither Townsend Security nor the hosting center personnel have any credentials to access your key server HSMs. There are no back-doors or other ways to access the key server. In the event you lose your credentials to access the key server Townsend Security will not be able to help you recover access.

Q: What happens if someone tampers with the HSM appliance?

The Alliance Key Manager HSMs are protected by tamper-evident case hardening. The servers are inspected periodically for damage or evidence of tampering. You will be notified in the event tampering is discovered. Alliance Key Manager Cloud HSMs are hosted in a locked cabinet, in a secure data center monitored around the clock. In the event tampering is detected the key server HSM will be replaced at no charge.

Q: Can Townsend Security recover my keys if I lose my credentials?

No. Townsend Security does not have any credentials to access your key server HSM, and has no way to recover your keys. You may restore your keys to a new key server HSM from a backup you make. The backups are under your control and Townsend Security does not have access to your backups. Restoring to a new key server HSM is the only way to recover from the loss of credentials.

Q: How do I know that I can trust Alliance Key Manager appliances?

The Alliance Key Server solution has been validated to the Federal Information Processing Standard FIPS 140-2 (certificate 1449). FIPS validation means that an encryption key manager can provably meet industry standards and best practices.

Provisioning and Operations

Q: How do I start service with the Alliance Key Manager Cloud HSM option?

Contact Townsend Security to be assigned an account manager and a pre-sales support resource. This team will review your needs to insure that your security goals can be met. After this qualification step you can evaluate the solution with one of our easy evaluation methods. When you are ready to start your service, provide a purchase order and payment to Townsend Security and the key server HSMs will be provisioned for you.

Q: What capacity do I need?

Alliance Key Manager HSMs are not limited by the number of connections, connection speeds, number or type of end points, number of keys, etc. A key server HSM can manage millions of encryption keys and many simultaneous connections. You can also deploy your own load balancing options to use two or more key manager HSMs. If you are concerned about very high levels of key server access, schedule a technical discussion with your account manager.

Q: How do I set up a high availability (HA) configuration?

You can configure bi-directional, real time mirroring of keys and access policies between two or more Alliance Key Manager HSMs. The Townsend Security customer support team will help you with mirroring configuration.

Q: Is there an SLA for the Alliance Key Manager Cloud HSM?

Yes, please contact your account manager for a copy of the SLA, or view online.

Q: How many HSMs can be connected in mirroring group?

There is no limit to the number of Alliance Key Manager HSMs that can be connected for real-time key mirroring. Key and access policy mirroring can be one-directional, or bi-directional in active-active configurations.

Q: Can I move the key server HSM to my own data center or hosting facility?

Yes, if you purchased a perpetual license for Alliance Key Manager Cloud HSM you can move the HSMs to your own data center or other hosting provider. You must provide adequate notice in order to process the move request, and an administrative processing fee will be charged to cover the costs of decommissioning and shipping the servers. You must also plan for continued availability of key management servers during the transition.

Support and Maintenance

Q: How is routine maintenance performed on HSM appliances?

Alliance Key Manager HSMs are designed to operate without the need for periodic maintenance. Hardware servers are replaced every four years (or longer, at your discretion). In the event the hardware servers require hardware updates or bios upgrades, you will be contacted to schedule the service. The Alliance Key Manager Cloud HSM option provides you with two key servers which you configure for mirroring. In the event one key server must be taken off-line for service, you must allow for accessing the other key server during the maintenance period. If operating system or security patches need to be applied, you will be contacted with instructions on how to apply these changes. Townsend Security has no access to your key servers and the application of patches is your responsibility.

Q: I am having a problem with Alliance Key Manager. What do I do?

While it would be a rare occurrence, if you experiencing a problem please contact Townsend Security customer support.

Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

You can contact Townsend Security for an initial consultation at the following locations:

Web: www.townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
International: +1 360 359 4400
Email: info@townsendsecurity.com
Twitter: @townsendsecure