SafeNet DataSecure and Key Secure

Release Notes

Version: 6.1.2
Release Notes Issue Date: 09/07/2012
Document part number: 007-012104-001

DataSecure Product Description

The SafeNet DataSecure appliance is fundamental in SafeNet data encryption and control solutions. Using hardware-based encryption, DataSecure appliances cover the broadest variety of data types. They provide a unified platform with data encryption and granular access control capabilities that can be applied to databases, applications, mainframe environments, and individual files. By providing centralized management of keys, policies, and essential functions, DataSecure simplifies administration, helps ensure compliance, and maximizes security.

Key Management

With DataSecure, all cryptographic keys are kept in the centralized, hardened appliance to simplify administration while helping ensure tight security for the broadest array of data types. Key versioning streamlines the time-consuming task of key rotation.

Policy Management

Administrators can set authentication and authorization policies that dictate which application, database, or file servers can be accessed by particular users in the clear. When combined with strong authentication, this policy-driven security provides a vital layer of protection. DataSecure also offers granular access controls to help you comply with the separation of duties required in many security mandates. An administrator can create a policy that prevents certain users from accessing sensitive data without interfering with their day-to-day system administration duties.

Logging, Auditing, and Reporting

When encrypting data within an enterprise, data, keys, and logs are often accessed, encrypted, managed, and generated on multiple devices, in multiple locations. To reduce the cost and complexity of security management, DataSecure provides a single, centralized interface for logging, auditing, and reporting access to data and keys. A centralized mechanism increases security and helps you ensure compliance with industry mandates and government regulations.

KeySecure Product Description

KeySecure offers robust capabilities for managing cryptographic keys across their entire lifecycle, including key generation, key import and export, key rotation, and much more. KeySecure is a KMIP 1.0 standards-based enterprise key management server, so it is ready to integrate with all KMIP compliant encryption devices and software. KeySecure can be integrated through open APIs with database encryption, laptop and device encryption, and file and storage level encryption products.

KeySecure centrally manages keys using a hardened appliance, which maximizes overall security.

Broad Flexibility

KeySecure offers key management capabilities that can be integrated with virtually any commercial encryption product. SafeNet supports a wide range of open cryptographic standard interfaces. KeySecure supports the Key Management Interoperability Protocol (KMIP). Further, customers and partners can take advantage of SafeNet's XML interface to develop their own custom software utilizing the enterprise key management functionality of KeySecure.

High Availability

SafeNet customers can deploy multiple KeySecure appliances in a clustered configuration with real-time replication of keys, policies, and configuration information across multiple appliances - enabling complete disaster recovery and business continuity.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

1. Version Summary

1.1. Release Description

Release 6.1.2

1.2. Supported Platforms

DataSecure software version 6.1.2 is supported on the following platforms:

- i460

KeySecure software version 6.1.2 is supported on the following platform:

- k460

1.3. Scope

All feature descriptions with the exception of data encryption are applicable to KeySecure as well as to DataSecure.

Please see “Advisory Notes” and “Known Issues and Workarounds” for any limitations and restrictions.

1.4. New Features and Enhancements

- **Schedule an Automated Remote Backup.** You can now scheduled automated remote backups. Using a simple extension to the existing remote backup process, this feature enables you to set up a regularly scheduled backup to a remote location. In the final steps of defining normal backup, you specify a Host and Directory Name, and then you can use the new feature to set up a monthly, weekly or daily backup schedule. To perform the familiar, immediate back up process, you’ll use a button labeled “Backup Now”. For details, see the updated instructions for the Create Backup process in the User Guide.
- **Support for Multiple Credentials in Backup operation.** The Administrator can now require multiple Administrators to supply their name and password before the backup operation can proceed. To set up this requirement, navigate to the DataSecure Management Console Device tab>Device Configuration> Administrators>Multiple Credentials. Click Edit to change data in the Multiple Credentials for Key Administration section, and follow the standard procedures as documented. You can enable certain Administrators to supply credentials from remote locations, but only for strictly limited periods of time.

  When the requirement for Multiple Credentials has been set up, for example, a “Confirmation Required” page appears after you click the Back Up Now button. To proceed with the backup, this page requires credentials for the number of Administrators specified by the Multiple Credentials definition. Unless the required number of credentials are provided, it will not be possible to create a backup. [MKS 162480]
- **Delete Multiple Keys (Bulk Key Deletion).** This new feature enables you to delete up to 50 keys at a time. Create a backup first, and be careful, because you clear away a full page of keys with extreme efficiency when using this feature. First you perform a Key Query to populate a Key List with only the keys you want to delete, then you eliminate the entire list of keys on the page, all at one time. The User Guide provides step by step instructions that make it easy — and prevent accidental deletions. For guidance, see Delete Multiple Keys in the updated User Guide.
- **Upgrade to HSM firmware version 6.2.1**. This release includes an upgrade to the latest firmware (version 6.2.1) of HSM on k460 and i460 devices. Devices that have KeySecure or Data Secure 6.1.2 installed at the factory have the latest firmware installed by default. To use this release, Customers with devices already in the field must upgrade them to the latest firmware through the Command Line Interface (CLI) by using the “hsm firmware update” command.

2. Installation Instructions

Install 6.1.2 by using the Command Line Interface (CLI). Detailed step by step instructions are provided in the Command Line Interface Reference Guide for 6.1.2. A summary explanation is provided below.

The KeySecure Quick Start Guide and DataSecure Quick Start Guide provide instructions for installing the appliance, configuring the appliance (including initialization of the HSM), logging in, and related configuration tasks. Always create a complete backup before an installation.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

To upgrade from a patch to a new release, you must first roll back the patch software and then upgrade.

2.1. Supported Upgrade Paths

The following upgrade paths are supported:

- 6.0.1 → 6.1.2.
- 6.1.0 → 6.1.2.

To upgrade to release 6.1.2 from a release previous to 6.0.1, you must first upgrade to release 6.0.1.

Because the 6.1.2 DataSecure and KeySecure release depends on new HSM firmware (version 6.2.1), your upgrade process must include an HSM firmware upgrade, from version 6.2.0 to 6.2.1. This HSM upgrade is explained below.

2.2. Upgrading to Version 6.1.2 using the CLI

To upgrade the software:

1. Log in to the CLI as an administrator with Software Upgrade and System Health Access Control.
2. Enter configuration mode by typing config.
3. Execute the software install command.
4. Select the method you'll use to upload the new software. SafeNet recommends SCP, which works on more platforms, including Windows. Then enter the host, filename, username, and password. If the information is correct, click Confirm to start the upgrade process.
5. Wait while the DataSecure downloads and installs the new software. This will take a few minutes. The CLI will indicate the status of the process. After the software is installed, the DataSecure will reboot. Again, this will take a few minutes. During the reboot you will lose all client connections.
6. Check that the upgrade was successful by logging in to the CLI. Run the show software command to see the current software version.

2.3 Upgrade HSM firmware version to 6.2.1 (for k460/i460 devices)

After upgrading software to version 6.1.2 as mentioned in section 2.1, you must perform these steps

1. Create a full backup, using either the GUI or the CLI. If upgrading the k460, be sure to back up SSKM.
2. Login to CLI as an administrator through ssh or serial console.
3. Logout HSM crypto user through "`hsm logout crypto user`" command.
4. For KeySecure only (SSKM is not implemented for DataSecure): Shut down SSKM (if running), through "`sskm halt`" command.
5. Firmware update requires local PED attendance using the blue key.
6. Executing "`hsm firmware update K6_6.2.1-RC10`" results in a prompt for PED attendance and for an upgrade to the HSM firmware to version 6.2.1.
7. Check firmware version by using the "`hsm show info`" command.
8. Login the Crypto User by using the "`hsm login crypto user`" command.
9. Reboot.
10. When device comes up after reboot:
    a. check that Crypto User is logged-in by using the "`show hsm status`" command
    b. For KeySecure only (because SSKM is not implemented for DataSecure): check that SSKM is running by using the "`show sskm status`" command.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

3. Advisory Notes

Initialization

- **After initializing the Data Secure/KeySecure**, the command line prompt instructs you to press Return to continue. If you do not press Return and end the console connection before seeing the login prompt, you will **not** be able to establish a new console connection until you reboot the DataSecure/KeySecure.

Backup and Restore

- The time required to restore a backup is directly related to the number of keys in the backup file and can take several hours when restoring hundreds of thousands of keys.
- Special characters (including a space) are not allowed in a backup file name. When naming a backup, use only alphanumeric characters in a solid string. Users are not overtly prevented from entering special characters, and the logs do not explicitly warn about the failure of the backup.

Importing Keys and Certificates

- When **importing RSA keys**, the Public key must be imported. If you import the Private Key, then the Private key holds the Public key, so you will not need to import the public key separately. To **import certificates stored in a Netscape database** to a KeySecure, you must convert the individual certificates to a format that the KeySecure can use. PKCS#12 format will work, and can be used to import both the certificate and key in PKCS#12 format. You can find more information and tools for this conversion process at http://www.mozilla.org/projects/security/pki/nss/tools/pk12util.html.

Certificate Authorities

- **Chain revocation is not supported** for Certificate Authority Certificates. If a CA certificate is revoked, the certificates signed by the CA certificate are not automatically revoked. Those certificates must be revoked individually. **Installing a known CA certificate more than once** on a KeySecure can render, under some circumstances, the CRL information unreliable for that CA. In such cases, a certificate that was revoked by that CA actually appears as active. Before installing a known CA, consult the list of CAs on the KeySecure. Do not install duplicates. **CAs issue serial numbers to the certificates they sign** in order to keep track of them. Local CAs use a seed value to determine the serial number. Each time a certificate is signed, the seed value is incremented. **If you back up a local CA, continue to issue certificates with that CA, and then restore the backup**, you might disrupt the CRL operations on that local CA, because the seed value before restoring the backup local CA will be $x + n$, where n is the number of certificates signed by that local CA since the backup was created. When the backup is restored, the seed value for the local CA will revert to x. As such, it is possible that the local CA will issue identical serial numbers to multiple certificates. To avoid this problem, back up local CAs after using them to issue certificates.

Algorithm Support

- **HmacSHA512, HmacSHA384, and HmacSHA256** are not supported by KMIP Create Request; use Register Request instead.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

4. Known Issues and Workarounds

The KeySecure software contains a few known issues that affect functionality. These known issues and workarounds, where they exist, are described below.

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium level priority problems
L	Low	Lowest level priority problems

Issue	Severity	Synopsis
DS-4723	High	**Failure to Sign Request** When the HSM is zeroized, the user cannot use `local ca` to sign certificates. Zeroizing HSM renders all keys, certificates and local CA's unusable. An attempt to use local-ca for signing may show success when the signing did not actually succeed. This misleading error message may incorrectly appear: "Certificate request has been signed." **Workaround:** Create a full backup before HSM zeroization, then delete all keys, certificates and local CAs; and then restore the backup after HSM reinitialization.
DS-4725	High	**On KeySecure, the command `hsm generate certificate` does not correctly update the HSM status** When HSM is reinitialized, using the "hsm generate certificates" command does not result in any failure when SSKM is running, although certificates are not actually generated. **Workaround:** Stop SSKM by using the "sskm halt" command, then run the "hsm generate certificates" command.
DS-4779	High	**When using FireFox to access the HSM page, clicking Save can corrupt the password** If you use Firefox to enter your HSM password on the HSM Configuration page, the initial password data input field does not behave as expected. After you press the Set Password button, this field may contain some ghost characters. Some users have incorrectly assumed that their existing password was in place, but ghosted out. This is not the case: this field is initially blank (empty). If you click the Save button at this point, without clearing the ghost characters and entering the proper password, the empty set will be submitted as the password. **Workaround:** Clear the field of the ghost characters (for example, by using backspace or delete), then continue to enter the established password in the normal manner. This is only needed on Firefox..
DS-3143	Low	**The "zeroize all keys" function may hang.** The "zeroize all keys" function may hang if executed during any other activity on the server. Rebooting the box will solve this problem. Recommendation: Do not run "zeroize all keys" on the CLI when there is activity on the box.
DS-3178	Medium	**SIGN/SIGNV operations don't work for RSA keys using SHA1withRSA algorithm.** When the FIPS security settings are set for "Disable Non-FIPS Algorithms and Key Sizes" even 2, 3 and 4K RSA keys that are FIPS approved are unable to perform SIGN/SIGNV operations using the SHA1withRSA algorithm.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

Issue	Severity	Synopsis
DS-3182	Medium	**When creating a backup using FTP or automated scheduled backup process with FTP, the process of storing the backup file does not work correctly.**
DS-2700	Low	**Incorrect password entered during the first run after the HSM initialization, password rejected.** If you enter an incorrect password during the first run after the HSM has been initialized, the first run does not accept the correct password as valid. Note that you can press <n> (the line break or end-of-line marker), to get out of the password re-entry loop. **Workaround**: Set the HSM password and Crypto User login through commands, as follows: 1. Skip setting the password if it fails. 2. Let the first run complete. 3. Reboot 4. Set hsm password through "hsm set password" command. 5. Do hsm crypto-user login through "hsm login crypto user" 6. Configure SSKM and start it through "sskm interface" and "sskm start" commands…...
DS-3144	Low	**After installing OS on to an i450 server, hsm_mgmt_ca and ssl cert nae_kmip_server set up.** After installing the OS on to an i450 server, both the local CA hsm_mgmt_ca and ssl cert nae_kmip_server were set up. This is not correct. These should be set up only on the k460 platform, not the i450
165946	Medium	**Special characters (including the space) are not allowed in a backup file name** Special characters (including the space) are not allowed in a backup file name, but the user is not overtly prevented from entering special characters. The logs do not list all pieces of potentially useful data related to the failure of the backup.
165936	Medium	**Regarding the Automated Remote Backup feature:** • Currently, you cannot edit a backup for Automated Remote Backup; you can only recreate it. • If you incorrectly enter your credentials at the time you schedule a remote backup via SCP, the error will not be detected during data entry. You will receive an error at the time the backup is scheduled to occur, not at the time you schedule it.
165944	Medium	**A space is not allowed in a log file base name.** Backup (immediate or scheduled) silently fails, despite logged confirmation, when there is a space in the log file base name.
154301	Medium	**Creating multiple large-size Remote Key Foundry (RKF) keys** When creating multiple large-size RKF keys, such as keys 4K in size, or especially 8K, you should pause the operation after the UI returns from the creation phase of each key. This pause is crucial if the UI returns a warning message about KS time-out while communicating with HSM. If you do not voluntarily observe this delay, you should expect errors when you attempt to create the next several RKF keys. We recommend that you delay from 45 seconds to 1 minute after initiating each creation operation to allow for processing. Be aware that the creation of these RKF keys is only enabled when HSM Management is enabled.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

Issue	Severity	Synopsis
128873	Medium	**During an Administrator lockout period, which begins when any Administrator is locked out, attempting to change any Administrator password through the CLI will permanently disallow use of that password** **Summary:** When the Administrator Lockout Period is engaged, attempting to change any administrator password using the CLI will permanently lock that account. For example, if Administrator One failed 5 consecutive login attempts, then a lockout commences. Suppose that, during the resulting lockout period, the CLI is used to change the password of Administrator Two. In this scenario, the password change will fail and Administrator Two will be permanently locked out. **Best Practice:** After failing multiple consecutive login attempts, wait for the Administrator Lockout Period to expire prior to taking any further administrative account action using the CLI. The default lockout time is 5 minutes for the serial console and 30 minutes for the remote access (either the Management Console or the remote CLI using SSH).
122526	Low	**System Cannot Detect Current BIOS Version** **Summary:** After rebooting the device, you may see the following error message in the System Log: localhost System Health: Could not detect current BIOS version. Error 1. This message can be ignored.
121747	Medium	**Networking: Route Table Creation is Not Working Properly When Multiple IPs are Configured for a Single Ethernet Port** **Summary:** Adding multiple IP addresses to a single Ethernet port and then deleting some of those IP addresses can cause the routing table to become out of sync. Modifying the default gateway when the routing table is in this state can cause the system to lose the default gateway settings.
120712	Medium	**String-based Key Queries Time Out on Devices Containing 1 Million Keys** **Summary:** When using a key query to search for key names containing a specific value, if the device holds 1 million keys, the key query will time out after ten minutes.
100536	Medium	**SNMP XML Key statistics Missing Failed Key Import Requests** SMNP statistics do not report KeyImport requests – they are always 0. The statistics reported on the Management Console (Device >> Statistics >> NAE-XML Statistics) and the CLI (`show statistics`) are correct.
85494	Medium	**Cluster: After Removing Node, Cluster Page Still Shows Node Information** **Summary:** If removing a node from a KeySecure cluster takes longer than 30 seconds, the Management Console reports an error even though the node is removed. After clicking Remove from Cluster the node may remain in the cluster list. **Workaround:** Clicking Remove from Cluster a second time will remove it from the Management Console's list.
60022 57596	Low	**Log Signing While the KeySecure is Under a Heavy Load** **Summary:** If the KeySecure is under a heavy load - performing more than 3000 operations per second – enabling the Log Signing feature will slow the log rotation mechanism to the point where the server will not be able to rotate and sign the log files quickly enough. This can potentially disable the logging feature. **Workaround:** Do not enable log signing when the KeySecure is expected to operate under a heavy load.
59942	Low	**Advancing the System Date Can Render the Software Check Invalid** **Summary:** Setting the system date beyond 02/18/2017 causes the KeySecure to fail the software integrity test. **Workaround:** Do not set the system date ahead of this date. New software signing certificates will be issued as needed.

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001

Issue	Severity	Synopsis
59245 57588	Medium	**Log Signing Feature** **Summary:** When enabled, the Log Signing feature uses a large percentage of system memory. **Workaround:** Disable log signing to decrease memory usage by up to 5%. Workaround info may be incorrect: issue 59245 says, “The total memory usage went up to 80% (i426, i416).” And “the memory use went down to 5% after turning log signing off.”
48080	Medium	**Key Generation Requests and Key Permissions** **Summary:** Users cannot see keys that they do not have permission to use. However, when a user tries to create a key using the XML interface, the request will be refused if another key already uses the keyname provided in the key generation request. This is true even if the user does not have permission to view or use the existing key. As such, a user can discover the names of existing keys by making key generation requests with various names until a duplicate name is found. **Workaround:** Do not enable the **Allow Key and Policy Configuration Operations** checkbox for the NAE-XML protocol. This is disabled by default. To check the setting, navigate to Device >> Key Server. Select the NAE-XML protocol and click **Properties.**

Publications

The publications associated with this release are:

- *DataSecure User Guide for Version 6.1.2*
- *KeySecure User Guide for Version 6.1.2*
- *DataSecure Quick Start Guide for Version 6.1.2*
- *KeySecure Quick Start Guide for Version 6.1.2*
- *KMIP Installation Guide for KeySecure, Version 6.1.2*
- *KMIP Installation Guide for DataSecure, Version 6.1.2*
- *KeySecure Command Line Interface (CLI) Guide 6.1.2*
- *DataSecure Command Line Interface (CLI) Guide 6.1.2*

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

007-012104-001 – DS+KS

© 2012 SafeNet, Inc. All rights reserved.

Documentation Part Number: 007-012104-001