Cloud Integration Option Pack

CIOP v2.2.1 Release Notes

09 April 2024

Table of Contents

1. Introduction . . . 1

1.1. Purpose of this release . . . 1

2. Features of nShield Cloud Integration Option Pack v2.2.1 . . . 2

2.1. Support for Google Cloud Key Management . . . 2

3. Important Information . . . 3

4. Compatibility . . . 4

4.1. Supported hardware . . . 4

4.2. Supported operating systems . . . 4

4.3. Supported Security World Versions . . . 4

4.4. Supported Firmware Versions . . . 5

5. Cloud Service Provider Integration . . . 6

5.1. Terminology . . . 6

5.2. Amazon Web Services . . . 6

5.3. Google Compute Engine . . . 7

5.4. Google Cloud Key Management . . . 8

5.5. Microsoft Azure . . . 8

5.6. Salesforce . . . 9

6. Fixed issues from previous release . . . 11

7. Known issues . . . 12

7.1. Known Issues in CIOP v2.2.1 . . . 12

7.2. Known Issues in Security World v12.71 . . . 12

1. Introduction

These release notes apply to version 2.2.1 of the nShield Cloud Integration Option Pack (CIOP) for Security World Software v12.71 release. They contain information specific to this release such as new features, defect fixes, and known issues.

The Release Notes may be updated with issues that have become known after this release has been made available. Please check https://nshieldsupport.entrust.com/hc/en-us/sections/360001115837-Release-Notes for the most up to date version of this document.

Access to the Support Portal is available to customers under maintenance. Please contact Entrust nShield Technical Support at nshield.support@entrust.com to request an account.

1.1. Purpose of this release

CIOP provides users of cloud services the ability to generate keys in their own environment and export them for use in the cloud while having:

- Confidence that their key has been generated securely using a strong entropy source.
- Confidence that the long term storage of their key is protected by a FIPS-certified Hardware Security Module (HSM).

The following cloud services are supported:

- Amazon Web Services (AWS)
- Google Compute Engine
- Google Cloud Key Management (Google KMS)
- Microsoft Azure
- Salesforce

2. Features of nShield Cloud Integration Option Pack v2.2.1

2.1. Support for Google Cloud Key Management

CIOP v2.2.1 provides support for Google Cloud Key Management. The CIOP tool, `cssadmin` now offers `google-cloud-key-management` as an additional provider option. This can be used along with the existing `wrapKey` option to specify the path to a public key generated using Google KMS. `cssadmin` will generate the files required to import keys from an HSM into Google KMS.

> ℹ Please refer to the User Guide for more information on how to use CIOP with Google KMS.

3. Important Information

Before deploying the nShield Cloud Integration Option Pack, the following should be considered:

- That an existing Security World software installation is required before installing the nShield Cloud Integration Option Pack.
- That a usable Security World is required.
- If using the Salesforce provider, that nShield Firmware version 12.70 is required.
- CIOP requires the python module `asn1crypto` to be installed for `nfast python`. This will be carried out by the CIOP installation process. See Fixed issues from previous release.
- When using multiple modules, `cssadmin` defaults to the first usable module. To change this, the `-m` option within `cssadmin` should be used to specify a module.
- The nShield Cloud Integration Option Pack expects Security World keys to be created with an appropriate set of permissions, therefore, only Security World keys created by `cssadmin` can be exported.
- If using `nfkmverify` to verify the generated Security World key the following message may be displayed (where `<key name>` is the name given during execution of `cssadmin`):

  ```
  DISCREPANCY: ACL of application key simple <key name> not of expected form:

  unexpected derivekey mechanism RawEncrypt
  ```

  This is expected behavior and does not indicate a problem with the generated key.

4. Compatibility

4.1. Supported hardware

This release is targeted at deployments with any combination of the following nShield HSMs:

- nShield Solo XC (Base, Mid, High)
- nShield Solo PCI Express (500+, and 6000+)
- nShield Connect (500+, 1500+, and 6000+)
- nShield Connect XC (Base, Mid, High, Serial Console)
- nShield Edge

4.2. Supported operating systems

This release has been tested for compatibility with the following operating systems:

- Microsoft Windows Server 2012 R2 x64
- Microsoft Windows Server 2016 x64
- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2019 Core x64
- Microsoft Windows 10 x64
- Red Hat Enterprise Linux 7 x64
- Red Hat Enterprise Linux AS/ES 6 x86/x64
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 6.10 x64
- Oracle Enterprise Linux 7.6 x64

4.3. Supported Security World Versions

This release can be used with the following nShield Security World Software installations:

- Security World v12.71

4.4. Supported Firmware Versions

This release can be used with the following nShield Firmware versions:

- nShield Firmware v12.60 or higher if using the `aws`, `google-compute-engine`, `microsoft-azure`, or `google-cloud-key-management` providers
- nShield Firmware v12.70 or higher if using the `salesforce` provider

5. Cloud Service Provider Integration

This table shows which Cloud Service Provider is supported in each version of CIOP.

		CIOP v2.0.0	CIOP v2.1.0	CIOP v2.2.1	Minimum Required Security World
Cloud Service Provider	Amazon Web Services	✓	✓	✓	v12.60
	Google Compute Engine	✓	✓	✓	v12.60
	Google Cloud Key Management	x	x	✓	v12.60
	Microsoft Azure	✓	✓	✓	v12.60
	Salesforce	x	✓	✓	v12.70

Note that some of the providers were available in CIOP v1.0 and v1.1 releases but these Release Notes only detail compatibility from CIOP v2.0 onwards. Please refer to the Release Notes for those versions if required.

5.1. Terminology

Target Key
The key to transfer from an nShield HSM to a Cloud hosted HSM.

Wrapping Key
The key obtained from the Cloud Service Provider which is used to protect the target key in transit.

Wrapping Algorithm
The algorithm used to wrap the target key with the wrapping key.

5.2. Amazon Web Services

Support for Amazon Web Services has been available from CIOP v2.0.0. Using this provider requires a minimum of Security World and Firmware v12.60.

The following table shows the supported target and wrapping key combinations supported for AWS.

At time of release, the only wrapping key type supported by AWS is 2048-bit RSA and there is no choice of target key type.

		Wrapping Algorithm		
		RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256	RSAES_PKCS1_V1_5
Target Key Type	AES 256	✓	✓	✓
Supported by AWS		✓	✓	✓
Supported in a v3 FIPS 140-2 Level 3 Security World		✓ (*see note below)	✓	x

* RSAES_OAEP_SHA_1 was made available in FIPS Security Worlds from Security World v12.70, prior to that it was disabled.

5.3. Google Compute Engine

Support for Google Compute Engine has been available from CIOP v2.0.0. Using this provider requires a minimum of Security World and Firmware v12.60.

The following table shows the supported target and wrapping key combinations supported for Google Compute Engine.

At time of release, the only wrapping key supported by Google is the RSA public key certificate maintained by Compute Engine. There is no choice of target key type.

Note that some of the wrapping algorithms that CIOP supports are not currently compatible with Google Compute Engine.

		Wrapping Algorithm		
		RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256	RSAES_PKCS1_V1_5
Target Key Type	AES 256	✓	✓	✓
Supported by Google Compute Engine		✓	x	x

		Wrapping Algorithm		
Supported in a v3 FIPS 140-2 Level 3 Security World		✓ (*see note below)	✓	x

* RSAES_OAEP_SHA_1 was made available in FIPS Security Worlds from Security World v12.70 and prior to that it was disabled.

5.4. Google Cloud Key Management

This is new from CIOP v2.2.1. Using this provider requires a minimum of Security World and Firmware v12.60.

The following table shows the supported target and wrapping key combinations supported for Google Cloud Key Management.

The only supported wrapping algorithm for Google KMS is CKM_RSA_AES_KEY_WRAP.

		Google KMS Wrapping Key (Import Job)		**Supported by Google KMS**	**Supported in a v3 FIPS 140-2 Level 3 Security World ***
		RSA-3072	RSA-4096		
Target Key Type	RSA-2048	✓	✓	✓	✓
	RSA-3072	✓	✓	✓	✓
	RSA-4096	✓	✓	✓	✓
	EC-NISTP256	✓	✓	✓	✓
	EC-NISTP384	✓	✓	✓	✓
	AES-256	✓	✓	✓	✓

* CKM_RSA_AES_KEY_WRAP was made available in FIPS Security Worlds from Security World Version v12.70. If you are using v12.60, this mechanism will be disabled in a FIPS Security World.

5.5. Microsoft Azure

Support for Microsoft Azure has been available from CIOP v2.0.0. Using this provider requires a minimum of Security World and Firmware v12.60.

The following table shows the supported target and wrapping key combinations supported for Microsoft Azure.

The only supported wrapping algorithm for Azure is CKM_RSA_AES_KEY_WRAP.

		Azure Wrapping Key (Key Exchange Key)			**Supported by Azure**	**Supported in a v3 FIPS 140-2 Level 3 Security World ***
		RSA-2048	RSA-3072	RSA-4096		
Target Key Type	RSA-2048	✓	✓	✓	✓	✓
	RSA-3072	✓	✓	✓	✓	✓
	RSA-4096	✓	✓	✓	✓	✓
	EC-NISTP256	✓	✓	✓	✓	✓
	EC-NISTP384	✓	✓	✓	✓	✓
	EC-NISTP521	✓	✓	✓	✓	✓
	EC-SECP256K1	✓	✓	✓	✓	x

* CKM_RSA_AES_KEY_WRAP was made available in FIPS Security Worlds from Security World Version v12.70. If you are using v12.60, this mechanism will be disabled in a FIPS Security World.

5.6. Salesforce

Support for Salesforce has been available from CIOP v2.1.0.

Using this provider requires a minimum of Security World and Firmware v12.70.

The following table shows the supported target and wrapping key combinations supported for Salesforce.

At time of release, the only wrapping key type supported by Salesforce is 4096-bit RSA and there is no choice of target key type.

Note that some of the wrapping algorithms that CIOP supports are not currently compatible with Salesforce.

		Wrapping Algorithm		
		RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256	RSAES_PKCS1_V1_5
Target Key Type	AES 256	✓	✓	✓
Supported by Salesforce		✓	x	x
Supported in a v3 FIPS 140-2 Level 3 Security World		✓	✓	x

6. Fixed issues from previous release

Reference	Description
NSE-33972	An issue requiring that in the case of running cssadmin with multiple modules, only one card could inserted is now resolved. It is now possible to run cssadmin with multiple modules each with a card inserted.
NSE-30881	The requirement to install the asn1crypto python module is no longer present. The dependency is now satisfied from a verified asn1crypto v1.4.0 wheel included in the release. This will now support installing on machines without network access.

7. Known issues

7.1. Known Issues in CIOP v2.2.1

Reference	Description
NSE-41286	If you want to provide FIPS Authorization using an OCS or ACS presented via Remote Administration you will need to remap the relevant Dynamic Slot to Slot 0.

7.2. Known Issues in Security World v12.71

Some known issues relevant to operating CIOP have been listed below. Please refer to the release notes for the Security World version you are using for the full list of known issues.

Reference	Description
	No known issues in Security World software identified at this time.