Cloud Integration Option Pack

CIOP v2.3.0 Release Notes

8 October 2025

Table of Contents

1. Introduction

These release notes apply to version 2.3.0 of the nShield Cloud Integration Option Pack (CIOP) for Security World Software. They contain information specific to this release such as new features, defect fixes, and known issues.

This document may be updated with issues that have become known after this release has been made available. 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 Entrust nShield Help Center is available to customers under maintenance. 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

1.2. Versions of these Release Notes

Revision	Date	Description
1.0	2025-09-03	Release notes for the nShield Cloud Integration Option Pack v2.3.0

2. Features of nShield Cloud Integration Option Pack v2.3.0

2.1. Asymmetric key support for AWS

CIOP now supports generating and wrapping asymmetric keys for use with AWS.

The following asymmetric keys are now supported:

- `RSA-2048`, `RSA-3072`, `RSA-4096`
- `EC-NISTP256`, `EC-NISTP384`, `EC-NISTP521`, `EC-SECP256K1`

The following wrapping algorithms are now supported:

- `RSAES_OAEP_SHA_256`, `RSAES_OAEP_SHA_1`
- `RSA_AES_KEY_WRAP_SHA_256`, `RSA_AES_KEY_WRAP_SHA_1`

The following wrapping algorithm has been deprecated:

- `RSAES_PKCS1_V1_5`

2.2. Changed install process

Installation is now done by directly via nShield Python `pip` tool instead of `install.bat` or `install.sh`.

The `asn1crypto` wheel is no longer packaged with CIOP, as all supported versions of Security World software include it in their Python installations.

The `cloud_integration_tool` can now be run directly as a script from:

- `"%NFAST_HOME%\python3\Scripts\cloud_integration_tool.exe"` (Windows)
- `/opt/nfast/python3/bin/cloud_integration_tool` (on Linux)

You can add these directories to your `PATH` variable for ease of use.

3. Important information

Consider the following before you deploy CIOP:

- 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 12.80 is required.
- When you are using multiple HSMs, `cloud_integration_tool` defaults to the first usable one. To change this, the `-m` option within `cloud_integration_tool` should be used to specify which one.
- CIOP expects Security World keys to be created with an appropriate set of permissions. Therefore, only Security World keys created by `cloud_integration_tool` can be exported.
- If you are 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 `cloud_integration_tool`):

```
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 5s (Base, Mid, High)
- nShield 5c (Base, Mid, High)
- 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 10 x64
- Microsoft Windows 11 x64
- Microsoft Windows Server 2019 x64
- Microsoft Windows Server 2022 x64
- Microsoft Windows Server 2022 Core x64
- Microsoft Windows Server 2025 x64
- Red Hat Enterprise Linux 8 x64
- Red Hat Enterprise Linux 9 x64
- SUSE Enterprise Linux 12 x64
- SUSE Enterprise Linux 15 x64
- Oracle Enterprise Linux 8 x64
- Oracle Enterprise Linux 9 x64

4.3. Supported Security World versions

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

- Security World v13.6
- Security World v13.4
- Security World v13.3
- Security World v12.80

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

4.5. 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.

4.6. 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.

		Wrapping Algorithm	
		RSAES_OAEP_SHA_*	RSA_AES_KEY_WRAP_SHA_*

		Wrapping Algorithm	
Target Key Type	AES 256	✓	X
	RSA-2048	X	✓
	RSA-3072	X	✓
	RSA-4096	X	✓
	EC-NISTP256	X	✓
	EC-NISTP384	X	✓
	EC-NISTP521	X	✓
	EC-SECP256K1	X	✓
Supported by AWS		✓	✓
Supported in a v3 FIPS 140-2 Level 3 Security World*		✓	✓

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

4.7. 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
Supported in a v3 FIPS 140-2 Level 3 Security World		✓*	✓	x

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

4.8. Google Cloud Key Management

Support for Google Cloud Key Management has been available 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.

4.9. 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	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.

4.10. 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

		Wrapping Algorithm		
Supported in a v3 FIPS 140-2 Level 3 Security World		✓	✓	x

5. Fixed issues from previous release

Reference	Description
NSE-68404	Add support for asymmetric keys for AWS in CIOP
NSE-71817	Remove install.sh/install.bat scripts and declutter archive

6. Known issues

6.1. Known issues in CIOP v2.3.0

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.
NSE-73712	Using RSAES_OAEP_SHA_256 for the wrapping with google-compute-engine is not supported. The cloud_integration_tool will allow the creation of the wrapped key but it does not support the correct encoding to be unwrapped by google-compute-engine. RSAES_OAEP_SHA_1 continues to work.

6.2. Known issues in Security World v12.80+

Some known issues relevant to operating CIOP are listed below. 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.