

nShield Security World

nShield Security World Software v13.9.9 Installation Guide

09 November 2026

© Entrust Corporation. All rights reserved.

Table of Contents

1. Before you install the software . . . 2
    1.1. Preparatory tasks before installing software . . . 2
        1.1.1. Windows . . . 2
        1.1.2. Linux . . . 3
        1.1.3. All environments . . . 5
    1.2. Firewall settings . . . 7
2. Install the Security World software . . . 9
    2.1. Verify the installation media . . . 9
        2.1.1. Check the release key . . . 9
        2.1.2. The release key . . . 11
        2.1.3. Verify the disc image . . . 12
        2.1.4. Verify the files on the media . . . 12
        2.1.5. Verify without importing the key . . . 13
        2.1.6. Reading the results . . . 14
    2.2. Installing the Security World Software on Windows . . . 15
        2.2.1. Additional steps for nShield 5s . . . 17
    2.3. Install the Security World software on Linux . . . 18
        2.3.1. From tar files . . . 19
        2.3.2. From RPM packages . . . 20
        2.3.3. Additional steps for nShield 5s . . . 23
    2.4. After installing the software . . . 24
3. Using silent installations . . . 26
    3.1. Installing using the silent install functionality . . . 26
    3.2. Uninstalling using the silent install functionality . . . 27
4. Problems during installation and commissioning . . . 29
    4.1. PCIe HSMs . . . 29
5. Uninstalling Security World Software . . . 30
    5.1. Uninstalling the Security World software on Windows . . . 30
        5.1.1. Removal of Security World data . . . 31
    5.2. Uninstalling the Security World software on Linux . . . 31
        5.2.1. Uninstalling the tarballs . . . 31
        5.2.2. Uninstalling the RPMs . . . 31
        5.2.3. Directory Cleanup . . . 34
6. System upgrade . . . 36
    6.1. Software and firmware compatibility . . . 36
    6.2. System upgrade procedure . . . 36
    6.3. Upgrade software . . . 37

6.3.1. Before upgrading software . . . 37
6.3.2. Reinstall Security World software . . . 38
6.3.3. After upgrading software . . . 38
6.4. Upgrade firmware . . . 38
7. Software packages on the installation media . . . 39
7.1. Security World installation media . . . 39

This guide provides installation instructions to help you install the Security World software on the computer, client, or RFS associates with your nShield HSM.

Ensure that you follow the preparation and installation instructions relevant for your HSM.

1. Before you install the software

This guide covers the following HSMs:

- nShield Solo
- nShield Solo XC
- nShield 5s
- nShield Connect
- nShield 5c
- nShield Edge

Before you install the Security World software:

- (**PCIe HSMs only**) Install the module. See Install a PCIe HSM.
- Uninstall any older versions of Security World Software. See Uninstalling Security World Software
- If the nShield Remote Administration Client is installed on the machine, remove it. You will also have to re-install it after you installed the new Security World software version. See Remote Administration v13.9.9 User Guide.
- Complete the preparatory tasks.

1.1. Preparatory tasks before installing software

1.1.1. Windows

1.1.1.1. Turn off sleep mode

Adjust your computer's power saving setting to prevent sleep mode.

1.1.1.2. Install Microsoft security updates

Make sure that you have installed the latest Microsoft security updates. Information about Microsoft security updates is available from http://www.microsoft.com/security/.

1.1.1.3. (**PCIe HSMs only**) Add %NFAST_HOME%\bin\ to the PATH environment variable

The default location for `%NFAST_HOME%\bin\` is `C:\Program Files\nCipher\nfast`. Because of the space in `Program Files`, nShield commands could fail if `NFAST_HOME\bin\` is not in `PATH`.

If you cannot change PATH, you will have to enclose all file names and paths that use variable between double quotation marks (" "). For example:

```
"%NFAST_HOME%\toolkits\pkcs11\cknfast.dll"
```

1.1.2. Linux

1.1.2.1. Install operating environment patches

Make sure that you have installed:

- kernel packages like gcc, kernel-headers, kernel-devel
- the latest recommended patches for your environment in general

See the documentation supplied with your operating environment for information.

1.1.2.2. Users and groups

The installer automatically creates the following group and users if they do not exist. If you wish to create them manually, you should do so before running the installer.

Create the following, as required:

- The nfast user in the nfast group, using /opt/nfast as the home directory.

  

  (**USB HSMs only**) The nfast user must also be a member of the dialout group. dialout grants access to the serial ports, including those that the nShield Edge uses (/dev/ttyUSB*).

  For example, on Linux, run:

  ```
  useradd -a -G dialout nfast
  ```

- If you are installing snmp, the ncsnmpd user in the ncsnmpd group, using /opt/nfast as the home directory.
- If you are installing the Remote Administration Service, the raserv user in the raserv group, using /opt/nfast as the home directory.

1.1.2.3. (nShield 5s only) Network configuration

The nShield 5s appears to the host operating system as a network interface. Communica-

tion with the HSM is performed over this interface using IPv6. The install process automatically configures the nShield 5s and any relevant operating system network settings, with the HSM and host-software using link-local communication.

After the installation process has been completed, the nShield 5s network interfaces should have a link-local IPv6 address. On Windows and Linux, this is assigned automatically. On Linux, the installation process will also detect the following network management services and create appropriate configuration files:

Network management service	Configuration file path
`NetworkManager`	`/etc/network/interfaces.d/nshield`
`systemd.networkd`	`/etc/systemd/network/nshield.network`

These files instruct the network management service not to configure the nShield 5s interfaces. They will be configured by the nShield host software. This covers all of our supported distributions, and more. If your distribution is not using one of these network management services, you will need to configure the interfaces to have a link-local IPv6 address manually.

The following network configuration must be present for the host software and HSM to function:

- The HSM's network interface must be assigned a link-local IPv6 address (https://tools.ietf.org/html/rfc4862).
- Multicast DNS must be possible for the host software to discover the services running on the HSM (https://tools.ietf.org/html/rfc6762).

  This requires inbound UDP packets on port 5353, to receive service advertisement responses from the HSM.

- The following ports must be accessible on the HSM from the host to access management and crypto services.

  Outbound SSH traffic on TCP ports:

  - 2201
  - 2202
  - 2203
  - 2204
  - 2206

1.1.3. All environments

1.1.3.1. Install Java with any necessary patches

The following versions of Java have been tested to work with, and are supported by, your nShield Security World Software:

- Java 8 (or Java 1.8x)
- Java 17
- Java 21
- Java 25

Entrust recommends that you ensure Java is installed before you install the Security World Software. The Java executable must be on your system path.

If you can do so, please use the latest Java version currently supported by Entrust that is compatible with your requirements. Java versions before those shown are no longer supported. If you are maintaining older Java versions for legacy reasons, and need compatibility with current nShield software, please contact Entrust nShield Support, https://nshieldsupport.entrust.com.

To install Java you may need installation packages specific to your operating system, which may depend on other pre-installed packages to be able to work.

Suggested links from which you may download Java software as appropriate for your operating system:

- http://www.oracle.com/technetwork/java/index.html
- http://www.oracle.com/technetwork/java/all-142825.html

1.1.3.2. Identify software components to be installed

Entrust supply standard component bundles that contain many of the necessary components for your installation and, in addition, individual components for use with supported applications. To be sure that all component dependencies are satisfied, you can install either:

- All the software components supplied.
- Only the software components you require.

During the installation process, you are asked to choose which bundles and components to install. Your choice depends on a number of considerations, including:

- The types of application that are to use the module.
- The amount of disc space available for the installation.
- Your company's policy on installing software. For example, although it may be simpler to choose all software components, your company may have a policy of not installing any software that is not required.

Network-attached HSMs

On Windows, the **nShield Hardware Support bundle** and the **nShield Core Tools bundle** are mandatory, and are always installed.

PCIe HSMs

On Windows, the **nShield Hardware Support bundle** and the **nShield Core Tools bundle** are mandatory, and are always installed.

On Windows, the **Windows device drivers** component is installed as part of the **Hardware Support bundle**. On Linux, the **Kernel device drivers** component is installed.

On Linux, you *must* install the `hwsp` component and, for **nShield 5s HSMs** the `nshield5_net` component.

USB HSMs

You *must* install the **Hardware Support bundle**. If the **Hardware Support bundle** is not installed, your module cannot function.

The **Core Tools bundle** contains all the Security World Software command-line utilities, including:

- `generatekey`
- Low level utilities
- Test programs

The Core Tools bundle includes the **Tcl run time** component that installs a run-time Tcl installation within the nCipher directories. This is used by the tools for creating the Security World. This does not affect any other installation of Tcl on your computer.

Network-attached and PCIe HSMs only

You need to install the Remote Administration Service component if you require remote administration functionality. See Preparatory tasks before installing software and Remote Administration v13.9.9 User Guide for more about the Remote Administration Service.

Always install all the nShield components you need in a single installation process to

avoid subsequent issues should you wish to uninstall. You should not, for example, install the Remote Administration Service from the Security World installation media, then later install the Remote Administration Client from the client installation media.

Ensure that you have identified any optional components that you require before you install the Security World Software. See Software packages on the installation media for more about optional components.

1.2. Firewall settings

When setting up your firewall, you should ensure that the port settings are compatible with the HSMs and allow access to the system components you are using.

The following table identifies the ports used by the nShield system components. All listed ports are the default setting. Other ports may be defined during system configuration, according to the requirements of your organization.

Component	Default Port	Protocol	Use
Hardserver	9000	TCP	Internal non-privileged connections from local client applications (local-loopback only)
Hardserver	9001	TCP	Internal privileged connections from local client applications (local-loopback only)
Hardserver	9004	TCP	Incoming nCipher Secure Transport/Impath connections from other hardservers, for example: • From an HSM to the Remote File System (RFS) (**network-attached HSMs**). • From a cooperating client to the RFS it is configured to access (**PCIe HSMs**). • From a non-attended host machine or HSM to an attended host machine when using Remote Operator.
Hardserver in the HSM (**network-attached HSMs only**)	9004	TCP	Incoming impath connections from client machines
Remote Administration Service	9005	TCP	Incoming connections from Remote Administration Clients

Component	Default Port	Protocol	Use
Audit Logging syslog	514	UDP	If you plan to use the Audit Logging facility with remote syslog or SIEM applications, you need to allow outgoing connections to the configured UDP port
mDNS (**nShield 5s only**)	5353	UDP	Send out mDNS Service Discovery requests and receive responses

If you are setting up an RFS or exporting a slot for Remote Operator functionality (**network-attached HSMs**) or using an nShield Edge as a Remote Operator slot for an HSM located elsewhere (**PCIe and USB HSMs**), you need to open port 9004. You may restrict the IP addresses to those you expect to use this port. You can also restrict the IP addresses accepted by the hardserver in the configuration file. See see nShield HSM configuration files for more about configuration files. Similarly, if you are setting up the Remote Administration Service you need to open port 9005.

2. Install the Security World software

This chapter describes how to install the Security World Software on the computer, client, or RFS associated with your nShield HSM.



If you are upgrading an existing installation make sure you have made backup copies of any Security World data files and nShield 5s ssh-keys before you continue.

After you have installed the software, you must complete further Security World creation, configuration and setup tasks before you can use your nShield environment to protect and manage your keys.

2.1. Verify the installation media

The installation media is signed with the Entrust OpenPGP release key. The same key is used to sign the other nShield ISO images, including the CodeSafe, Remote Administration Client (RAC), and firmware images. The procedure in this section applies to all of these images. Verifying the signatures before you install the software confirms that the files came from Entrust and arrived without modification or loss during transit.

There are two signatures, each covering different content:

`<image>.iso.asc` Covers the disc image as a whole. It is a separate file, supplied alongside the `.iso` file, and is not on the media. Use it to verify the `.iso` file, before you mount it.

`SHA256SUMS.asc` Covers `SHA256SUMS`, which lists the SHA-256 digest of every file on the media except `SHA256SUMS` and `SHA256SUMS.asc`. Both files are in the top-level folder of the media, so you do not need to download or relocate them. Use them after mounting the image, when checking physical media or a copy of files from the media, or when `<image>.iso.asc` is unavailable.

Verification needs GnuPG. It is installed by default on most Linux distributions. If GnuPG is not installed, install the `gnupg2` package (`gpg2` on SUSE Linux Enterprise). On Windows, install Gpg4win and run the same commands from a command prompt.

2.1.1. Check the release key

The release public key is in the top-level folder of the media as `pubkey.asc`. To check a

downloaded image before you mount it, use the copy in The release key instead. The copy on the media is there for convenience only. Because the copy travels with the files it authenticates, an attacker who could alter the media could also replace the key, so the copy on the media proves nothing on its own. Trust is established by comparing the key's fingerprint with the fingerprint below, which comes from this guide rather than from the media. The key is also reproduced in The release key, so you can obtain it directly from this guide without needing the media.

Show what the file contains, without adding it to your keyring:

```
gpg --show-keys pubkey.asc
```

The output must list exactly one key with this fingerprint:

```
pub   rsa4096 2023-01-11 [SCEA] [expires: 2030-01-06]
      DC17ECB0C55280DA006B60F6225FC6BC0347CDCF
uid                      Entrust-DPS <devops@ncipher.com>
```

If the output lists more than one key, or the fingerprint differs, stop. Do not install the software. Instead, contact Entrust nShield Support at https://trustedcare.entrust.com/.

A file that contains the genuine key can also contain other keys, and any key can carry the name `Entrust-DPS <devops@ncipher.com>`. The name does not identify the key; only the fingerprint does.

The fingerprint is the permanent identity of the key. It remains the same across releases and does not change when the expiration date shown alongside it is extended. Check the fingerprint, not the expiration date or the contents of `pubkey.asc`.

`gpg --show-keys` needs GnuPG 2.2.8 or later. GnuPG 2.1.23 and later can display the same information without adding the key to your keyring, using the following command:

```
gpg --import --import-options show-only pubkey.asc
```

The `gpg --verify` commands in the following sections check signatures against the keys in your keyring, so import the key after checking it:

```
gpg --import pubkey.asc
```

The output must include `Total number processed: 1`.

If your version of GnuPG is older than 2.1.23, import the key first and then check it:

```
gpg --import pubkey.asc
```

```
gpg --fingerprint devops@ncipher.com
```

The output of `gpg --fingerprint` must list exactly one key, with the fingerprint shown in groups of four characters: `DC17 ECB0 C552 80DA 006B 60F6 225F C6BC 0347 CDCF`. If it lists any other key, stop and do not verify anything with that keyring. Remove the other key with `gpg --delete-keys <fingerprint>` and contact Entrust nShield Support at https://trustedcare.entrust.com/.

Importing keeps the key on your machine for future releases. If you would rather not add it to your keyring, see Verify without importing the key.

2.1.2. The release key

The key is printed here so that you can obtain it from this guide rather than from the files it authenticates. Expand the block below and save it to a file called `pubkey.asc`, then use it in place of the copy on the media. In the web version of this guide, you can instead download the same file: entrust-dps-pubkey.asc. If you download it, save it as `pubkey.asc` so that the commands in this section work unchanged.

If you copy the block from a PDF, preserve the line breaks and the blank line after the first line as shown here. GnuPG rejects the file if the text has been reflowed.

▼ *Armored public key*

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGO++mwBEACqf5upVpOHQ3/VhUZHQkSJOqVGztfnVRonO0ZtOQxZ/1Oa0qHU
IaSia2E449j+EYZOkqPb6/UOf6OWYMh/oMGut1iYEBkJ5/IlK179RkH1WKw3BeDX
1Z++b/T1W3bHPC9hhzVitDw0ZQ38sBvYVL33XYcA3fZDz9oa07BBOXthTcMr4V0Q
COmr0zASIupadjF9WO9MiQhBKnQvN++4YS6MXwBs3X0lqu30zJhtWmYDKnQc9ykI
y6D2OZwtjQIwTu43zevDKPEt2+V8zqGTV+BctUtHQ4HjwyOyQwU918i7xu+On+zD
3dkcX46QCFcxifmegp2/cHm1d+WPZb4cjMV6HmPntKBpGeIh+oXn6JrDRAWR0Kse
v0Pwiq+2C9iC/mixVPZaHIg1pawXyqkNeT/w4EzmN2uaNYm2bgW5vyYW2cTfaZOV
R9w2zUXtxSV/OJMp9mHr2JetuH69h5BpaSG4FpA2+Ulk5tiN1aKivVBdDUZkI4F9
ycZYAh7tb+zhmdwMeM4wzOIM6ThXWOgE4NmjXYQ2IXDgmUXH7iyyDQOcfhMT9v3U
DM/s+6Ig7l5RFCz4VGxb8lAeRZjVkeh9M1Yq+0HYNFiCnSfBFvKGzPy+A78BLQqO
4Ja131uW114ywgs6H+qTAaQIE9U3RCCOfRWXVIIuClIuJnJKK6z8aQSJowARAQAB
tCBFbnRydXN0LURQUyA8ZGV2b3BzQG5jaXBoZXIuY29tPokCVAQTAQoAPgIbLwUL
CQgHAgYVCgkICwIEFgIDAQIeAQIXgBYhBNwX7LDFUoDaAGtg9iJfxrwDR83PBQJn
fQufBQkNJBKzAAoJECJfxrwDR83PDIoP/AlnFqQO1wBEVZXf+39pFfh3SIVF/YgB
afokEAKGUvrhL12KCdWQWBYbXBDLiIaxT6RHEiI9W0bQgcJBAkuB05ykiQa45Var
GdsBgFhSjXq+/lCf6QVaZ6rpV1JlMeMypKCn1EQQcMQQJiIhu/MtTLf/YrbgUaqi
cQBLci82R9K0jxY1GPSRaDJi6IzQFKbjRGoHGT9mvG6H1kAiM6Z/ejNAVEOBmNik
cCPWkGYzeaQDQyCfG+pZ1/IZAA5Xc+DgWRXxA0ChEXfbd0hBINXSwGf+BKGEw2i6
nQB+zjyzGVlPyDiMg6Aeiaq7EVZtodkWxdDs5mibaGphtVaFRhnMZje8601ogJGB
pGdne8euiczR0GVtDNu8VuwzC6Aj2SnNMaC1T5BDTvfs8yeSwIAi0wOIwClZawsI
czr4ntpbuSv+qz/pUFmelLp+tRUtabkZR9uG5P1xVYuC9uZwwEolYyDwPfjy9sQV
dlkOKRznFJcbUd8bgRzJCoIfBYVUmZv7exdiryzFMqdVFgw8Ax80YFR16gVRm+HP
yLlhd1ROPMv5x1H6EPMKVQB18eApQlWnDQ1vCC7IzwDkzZOiUjEsrt7gGgf4S21m
IeaYvVcPbqDWAYthZtBHoZCbYn16jUtAurAbTLhCrt7QIqz50eVr3GRfM31Cmdei
bUX3lVF+1989
=2Wu3
-----END PGP PUBLIC KEY BLOCK-----
```

If GnuPG reports this copy as expired, the expiration date on the key has been extended since this guide was published. Use `pubkey.asc` from the media instead, and check its finger print against the one in Check the release key. Extending the expiration date does not change the fingerprint.

2.1.3. Verify the disc image

Save `<image>.iso.asc` in the same folder as the `.iso` file you downloaded. In that folder, run:

```
gpg --verify <image>.iso.asc <image>.iso
```

Check the output as described in Reading the results.

2.1.4. Verify the files on the media

Check the manifest even after `<image>.iso.asc` has verified the image as a whole. The man ifest lets you verify files after copying them from the media. It also lets you verify the con- tents if you have the image but not its detached signature, for example, if the image was dis tributed within your organization without the signature.

Mount the image, or insert the disc, and change to the top-level folder of the media. This folder contains `SHA256SUMS`, `SHA256SUMS.asc` and `pubkey.asc`. If you are checking a copy of the files, change to the folder that holds the copy of `SHA256SUMS`.

Verify the manifest first. `sha256sum` and its equivalents only confirm that the files match the manifest. This result is meaningful only after you confirm that the manifest is genuine:

```
gpg --verify SHA256SUMS.asc SHA256SUMS
```

Check the output as described in Reading the results.

Then check the files against the manifest. On Linux:

```
sha256sum --check SHA256SUMS
```

Windows has no `sha256sum`, so use PowerShell instead:

```
Get-Content SHA256SUMS | ForEach-Object {
    $digest, $file = $_ -split '\s+', 2
    $actual = (Get-FileHash -Algorithm SHA256 -LiteralPath $file).Hash
    if ($actual -eq $digest) { "OK: $file" } else { "FAILED: $file" }
```

```
}
```

On media with many files, a `FAILED:` line is easy to miss among the `OK:` lines. To show only failures, add `| Where-Object { $_ -notlike 'OK:*' }` on the same line after the final `}`. The check then prints nothing if every file matches.

On Windows, file names on an ISO image are shortened to 64 characters. Some files on the Linux images have longer names, so the check reports them as missing. Check the Linux images on Linux.

You can run these commands against either the disc or a copy of its contents, so the files remain verifiable after you copy them from the media.

These commands check only the files listed in `SHA256SUMS`. They do not report files that are present but not listed. Before you install from a file, check that its path is listed in `SHA256-SUMS`.

2.1.5. Verify without importing the key

`gpgv` checks a signature against a keyring you name on the command line and leaves your own keyring untouched. Use it in place of `gpg --verify` if you do not want to import the release key. It is part of GnuPG on Linux and part of Gpg4win on Windows.

`gpgv` reads keyrings in GnuPG's binary format rather than the armored text in `pubkey.asc`. Check `pubkey.asc` as described in Check the release key, then convert it once, writing the result to a directory you can write to, such as your home directory:

```
gpg --output <dir>/release-key.gpg --dearmor pubkey.asc
```

Then verify against that file. The keyring name must include a directory, for example `./release-key.gpg` if it is in the current directory. With a bare file name, `gpgv` looks for the keyring in your GnuPG home directory instead, and reports `keyblock resource '…': No such file or directory` followed by `Can't check signature: No public key`.

```
gpgv --keyring <dir>/release-key.gpg <image>.iso.asc <image>.iso
gpgv --keyring <dir>/release-key.gpg SHA256SUMS.asc SHA256SUMS
```

`gpgv` reports the full fingerprint of the key that created the signature. Check that it matches the fingerprint in Check the release key:

```
gpgv: Signature made Mon 06 Jul 2026 11:24:03 BST
gpgv:                using RSA key DC17ECB0C55280DA006B60F6225FC6BC0347CDCF
gpgv: Good signature from "Entrust-DPS <devops@ncipher.com>"
```

Older versions of `gpgv`, such as 2.0, show only the key ID `0347CDCF`, so use `gpg --verify` instead.

`gpgv` exits with status 0 for a good signature from any key in the keyring, status 1 for a bad signature, and status 2 when the keyring does not contain the signing key. An exit status of 0 does not by itself show that the release key made the signature; the fingerprint on the `using RSA key` line does. `gpgv` treats every key in the keyring as trusted, so it does not print the trust warning described in Reading the results. It also does not report that a key has been revoked.

2.1.6. Reading the results

A good signature from the release key produces output like this:

```
gpg: Signature made Mon 06 Jul 2026 11:24:03 BST
gpg:                using RSA key DC17ECB0C55280DA006B60F6225FC6BC0347CDCF
gpg: Good signature from "Entrust-DPS <devops@ncipher.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DC17 ECB0 C552 80DA 006B  60F6 225F C6BC 0347 CDCF
```

Check that the fingerprint on the `using RSA key` line, or on the `Primary key fingerprint` line, is the fingerprint in Check the release key. GnuPG 2.5, included in current Gpg4win releases, omits the `Primary key fingerprint` label from that line and prints the fingerprint without spaces: `DC17ECB0C55280DA006B60F6225FC6BC0347CDCF`. Older versions of GnuPG, such as 2.0, show only the key ID `0347CDCF` on the `using RSA key` line, so check the `Primary key fingerprint` line. Do not rely on the name in the `Good signature from` line, because any key can carry that name.

The warning that the key is not certified with a trusted signature is expected and is not a fail ure. It means GnuPG has no independent reason of its own to believe the key belongs to Entrust; the fingerprint check in Check the release key is what establishes that.

Do not install the software if the output contains any of the following:

- `BAD signature`: the file does not match its signature. `gpg` exits with status 1.
- `Can't check signature: No public key`: the key that made the signature is not in your keyring. `gpg` exits with status 2. If you have not imported the release key, import it as described in Check the release key and try again.
- `WARNING: This key has been revoked by its owner!`: the key has been revoked. `gpg` still reports `Good signature` and exits with status 0. Contact Entrust nShield Support at https://trustedcare.entrust.com/.

If the output includes `Note: This key has expired!`, see The release key.

`sha256sum --check` prints `OK` for each file and exits with status 0. The PowerShell equivalent above prints `OK:` followed by each file name, or nothing if you added the filter. A line reporting `FAILED` means the media is damaged or has been altered. For a listed file that is missing, `sha256sum` reports `FAILED open or read`, and PowerShell reports an error followed by `FAILED:` and the file name. `sha256sum --check` then exits with status 1. Do not install from the media.

2.2. Installing the Security World Software on Windows

Before you begin, verify the installation media as described in Verify the installation media.

For information about configuring silent installations and uninstallations on Windows, see Using silent installations.

For a regular installation:



(**nShield 5s only**) Installing Security World software on Windows via Remote Desktop Connection can result in a brief loss of RDP connection. If this happens, it will happen during the **Status:** part of the installation, towards the end. When the session reconnects, the installation carries on until completion.

1. Sign in as an Administrator or as a user with local administrator rights.

   

   If the Found New Hardware Wizard appears and prompts you to install drivers, cancel this notification, and continue to install the Security World Software as normal. Drivers are installed during the installation of the Security World Software.

2. Place the Security World Software installation media in the optical disc drive.
3. Launch `setup.msi` manually when prompted.
4. Follow the onscreen instructions.
5. Accept the license terms and select **Next** to continue.
6. Specify the installation directory and select **Next** to continue.
7. Select all the components required for installation.

   By default, all components are selected. Use the drop-down menu to deselect the components that you do not want to install. **nShield Hardware Support** and **Core Tools** are necessary to install the Security World Software.

   See Software packages on the installation media for more about the component bundles and the additional software supplied on your installation media.

8. Select **Install**.

   The selected components are installed in the installation directory chosen above. The installer creates links to the following nShield Cryptographic Service Provider (CSP) setup wizards as well as remote management tools under **Start** > **Entrust** or **Entrust nShield Security World** (depending on the version of Windows or Windows Server you are running):

   - If **nShield CSPs (CAPI, CNG)** was selected: **32bit CSP install wizard**, which sets up CSPs for 32-bit applications
   - If **nShield CSPs (CAPI, CNG)** was selected: **64bit CSP install wizard**, which sets up CSPs for 64-bit applications
   - If **nShield CSPs (CAPI, CNG)** was selected: **CNG configuration wizard**, which sets up the CNG providers
   - If **nShield Remote Administration Client Tools** was selected: **Remote Administration Client**, which runs the remote administration client

   If selected, the SNMP agent will be installed, but will not be added to the **Services** area in **Control Panel** > **Administrative Tools** of the target Windows machine. If you wish to install the SNMP agent as a service, consult the nShield SNMP Monitor v13.9.9 Install and User guide.

   

   (**PCIe HSMs only**) Do not run any CSP installation wizard before installing the module hardware.

9. Select **Finish** to complete the installation.

   The following global variables are set upon install:

   - `%NFAST_CERTDIR%`
   - `%NFAST_HOME%`
   - `%NFAST_KMDATA%`
   - `%NFAST_LOGDIR%`
   - `%NFAST_SERVICES_HOME%` (**nShield 5s only**)

10. Add `C:\Program Files\nCipher\nfast\bin` to the Windows system path.
11. (**nShield 5s only**) If you are using an nShield 5s, complete the additional steps for nShield 5s.
12. (**PCIe HSMs only**) If you are using a PCIe HSM, you might need to update the power saving settings:
    a. In **Windows Device Manager** > **Security Accelerator** (**nShield Solo**) or **Windows Device Manager** > **Network adapters** (**nShield 5s**), select the appropriate module.

b. Under **Properties > Power Management**, deselect **Allow the computer to turn off this device to save power**.

2.2.1. Additional steps for nShield 5s

1. Stop the nFast Server service.
2. The nShield installer creates and enables an inbound rule called `nShield 5s mDNS` to allow UDP port 5353 for any program. This enables the discovery of nShield 5s modules. If enrollment fails to find any modules in the following step, check that this firewall rule is present and enabled; if it does not exist, create it manually and retry enrollment.
3. Set up the secure communication channels between the host PC and the HSM:

```
"%NFAST_HOME%\bin\hsmadmin" enroll
```



The HSM must be in factory state or else the registered `sshadmin` key must be in place otherwise this command will fail. If you have a backup of your `sshadmin` key, you can restore it using `hsmadmin keys restore`. If this is not a first-time installation of this HSM, and the `sshadmin` key trusted by this HSM is no longer available, enter recovery mode and then retry enrollment.

From firmware versions 13.5 onwards, the secure communication channels between the host PC and the HSM are protected by internally generated certificates. The `hsmadmin enroll` command automatically validates certificates as part of the enrollment process and produces a warning if it fails to find a certificate for any service. This warning is expected if the HSM:

- is in recovery mode
- is running a firmware version prior to 13.5
- has been upgraded to a firmware version of 13.5 or later but has not performed a factory state operation since the upgrade.

If you receive this warning in any other circumstance you should contact Entrust support.

4. Start the nFast Server service.
5. If Remote Administration is installed, also start the nFast Remote Administration service.
6. Entrust recommends that you take a backup of your `sshadmin` key with `hsmadmin keys backup path\to\backup_key` for backups that will be restored to the same machine.

Note that this key will not be usable on another machine or if the OS is re-installed as it has protections tied to the local machine. For backups that may be restored to a different machine or re-installed OS, use `hsmadmin keys backup --passphrase path\to\backup_key` to protect the key with a user-supplied passphrase. Replace `path\to\backup_key` with the actual path to where the backup key should be written in the example commands above.

2.3. Install the Security World software on Linux

Before you begin, verify the installation media as described in Verify the installation media.

1. Sign in and enter a `root` shell.
2. Mount the DVD/ISO image.
3. Extract the required files if you are using `.tar` or install the `rpm` packages.

   The current `rpm` packages are:

rpm package	Description
`nShield-hwsp`	Hardware Support package.
`nShield-ctls`	Management utilities.
`nShield-ctd`	Developer package example programs and libraries.
`nShield-devref`	Reference Documentation for the nCore API.
`nShield-driver-nfp`	nShield Solo XC drivers.
`nShield-driver-nShield5`	nShield 5s drivers.
`nShield-javasp`	Java provider.
`nShield-jd`	Java development software.
`nShield-ncsnmp`	SNMP provider.
`nShield-raserv`	Remote Administration service.

<disc-name> Name of the mount point of the installation media

<ver> Architecture of the operating system, for example, `i386` or `amd64`

<file.tar> Name of the `.tar.gz` file for the component

<file.rpm> Name of the `.rpm` file for the component

2.3.1. From tar files



If you already have an earlier version of the nShield software installed you must run the uninstall script before proceeding with a tar installation:

```
bash /opt/nfast/sbin/install -u
```

1. Change to the directory containing the `tar.gz` packages:

   ```
   cd <disc-name>/linux/ver/
   ```

2. Install the required software components using `tar`:

   ```
   tar -C / -xf <file>.tar.gz
   ```

   

   You must always unpack the `hwsp.tar.gz` archive for new installations.

2.3.1.1. Linux PCI driver installation

If you are using nShield PCI cards you must compile the PCI drivers. To do this you must first install the kernel development tooling and headers for your running kernel.

Check that you have the correct kernel headers:

```
ls -l /lib/modules/$(uname -r)/build
```

The above should print a symlink to your kernel headers. If you see `No such file or directory` you will need to install the correct kernel development packages for your OS.

Compile drivers for nShield Solo+ or SoloXC:

```
cd /opt/nfast/driver
make clean
make
make install
```

Compile drivers for nShield5:

```
cd /opt/nfast/driver-nshield5
make clean
make
make install
```

Finally, You must run the nShield install script:

```
bash /opt/nfast/sbin/install
```

2.3.2. From RPM packages

1. Change to the RPMs folder:

   ```
   cd <disc-name>/linux-rpms/amd64/
   ```

2. Check the Entrust RPM signing public key in `pubkey.asc` in this folder:

   ```
   gpg --show-keys pubkey.asc
   ```

   This is the same key that signs the installation media itself. The output must list exactly one key, with the fingerprint shown in Check the release key. If it does not, stop and contact Entrust nShield Support at https://trustedcare.entrust.com/. `rpm --import` trusts every key in the file, and the check in the following steps accepts packages signed by any key that `rpm` trusts.

3. Import the key into `rpm`:

   ```
   rpm --import pubkey.asc
   ```

4. Verify that each `.rpm` file is signed:

   ```
   rpm --checksig <file>.rpm
   ```

   For a correctly signed package, the output ends with `digests signatures OK`, for exam ple:

   ```
   nShield-hwsp-<version>.x86_64.rpm: digests signatures OK
   ```

   Check for the word `signatures`. For a package that has no signature, `rpm --checksig` prints `digests OK` and exits with status 0. Output containing `NOT OK` means that either the package is signed by a key that `rpm` does not trust or the package has been altered. In either case, `rpm --checksig` exits with status 1.

   `digests signatures OK` means that the package is signed by a key that `rpm` trusts, which includes the keys of your operating system vendor and any other keys imported on the machine. To confirm that the Entrust key made the signature, run:

```
rpm --checksig -v <file>.rpm
```

Every line of the output that reports a signature must end with `key ID 0347cdcf: OK`. `0347cdcf` is the last eight characters of the fingerprint in Check the release key.

Do not install a package unless both checks pass.

2.3.2.1. Using dnf (Red-Hat Enterprise Linux and Oracle Enterprise Linux)

1. Install the required software and driver packages by running `dnf`.

```
dnf install --repofrompath=nc,<location of rpm packages> <package name> <package name>
```

For example:

```
dnf install --repofrompath=nc,/mnt/linux-rpms/amd64/ nShield-ctls nShield-raserv
Added nc repo from /mnt/linux-rpms/amd64/
Last metadata expiration check: 0:04:04 ago on Mon Dec  2 11:08:31 2024.
Dependencies resolved.
================================================================================
 Package            Arch       Version                              Repository  Size
================================================================================
Installing:
 nShield-ctls       x86_64     13.7.3-1.1732201800.6eef148ee17      nc          58 M
 nShield-raserv     x86_64     13.7.3-1.1732201800.6eef148ee17      nc         344 k
Installing dependencies:
 nShield-hwsp       x86_64     13.7.3-1.1732201800.6eef148ee17      nc          71 M
 net-tools          x86_64     2.0-0.52.20160912git.el8             baseos     321 k
 procps-ng          x86_64     3.3.15-14.el8                        baseos     329 k

Transaction Summary
================================================================================
Install  5 Packages

Total size: 130 M
Total download size: 650 k
Installed size: 558 M
Is this ok [y/N]:
```

2.3.2.2. Using zypper (SUSE Enterprise Linux)

1. Add the `nc` repository to zypper.

```
zypper addrepo --gpgcheck-allow-unsigned-repo <location of rpm packages> nc
```

For example:

```
zypper addrepo --gpgcheck-allow-unsigned-repo /mnt/linux-rpms/amd64/ nc
Adding repository 'nc'
.....................................................................................................
```

```
.....................[done]
Repository 'nc' successfully added

URI         : dir:/mnt/linux-rpms/amd64
Enabled     : Yes
GPG Check   : Yes
Autorefresh : No
Priority    : 99 (default priority)

Repository priorities are without effect. All enabled repositories share the same priority.
```

2. Install the required software and driver packages by running `zypper`.

```
zypper install -y --from nc <package name> <package name>
```

For example:

```
zypper install -y --from nc nShield-ctls nShield-raserv
Refreshing service 'Basesystem_Module_15_SP6_x86_64'.
Refreshing service 'Python_3_Module_15_SP6_x86_64'.
Refreshing service 'SUSE_Linux_Enterprise_Server_15_SP6_x86_64'.
Refreshing service 'Server_Applications_Module_15_SP6_x86_64'.
Building repository 'nc' cache
.....................................................................................................
...............[done]
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following 3 NEW packages are going to be installed:
  nShield-ctls nShield-hwsp nShield-raserv

The following 3 packages have no support information from their vendor:
  nShield-ctls nShield-hwsp nShield-raserv

3 new packages to install.

Package download size:   135.0 MiB

Package install size change:
              |     660.5 MiB  required by packages that will be installed
   660.5 MiB  |  -      0 B    released by packages that will be removed

Backend:  classic_rpmtrans
Continue? [y/n/v/...? shows all options] (y): y
Retrieving: nShield-hwsp-13.7.3-1.1743026563.3b0b57a351a.x86_64 (nc)
(1/3),  76.6 MiB
Retrieving: nShield-raserv-13.7.3-1.1743026563.3b0b57a351a.x86_64 (nc)
(2/3), 347.8 KiB
Retrieving: nShield-ctls-13.7.3-1.1743026563.3b0b57a351a.x86_64 (nc)
(3/3),  58.1 MiB

Checking for file conflicts:
.....................................................................................................
.................[done]
(1/3) Installing: nShield-hwsp-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................[done]
(2/3) Installing: nShield-raserv-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................[done]
(3/3) Installing: nShield-ctls-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................[done]
%posttrans(nShield-hwsp-13.7.3-1.1743026563.3b0b57a351a.x86_64) script output:
```

```
...
 ---- Installation complete ----
Running post-transaction scripts
.....................................................................................................
.............[done]
```



If you require them, you can include all the optional RPM packages (such as javasp, raserv or ncsnmp) in the same command line.



If you require PCI drivers to be built and installed you must include the `nShield-driver-nfp` RPM for Solo+/SoloXC modules or the `nShield-driver-nshield5` RPM for nShield5 modules. This will install the required kernel packages and compile the PCI drivers. If however you change your kernel at a later date, you must re-build the drivers manually as explained in Linux PCI driver installation above.

If you are upgrading from an earlier version of nShield you will not need to manually uninstall any RPMs before upgrading.



If you are installing several RPM packages at the same time you may notice the install script is executed multiple times. This is normal and does not indicate a problem.

2.3.3. Additional steps for nShield 5s

The RPMs and install script will automatically run the `/opt/nfast/bin/hsmadmin enroll` command. From firmware versions 13.5 onwards the secure communication channels between the host PC and the HSM are protected by internally generated certificates. The `/opt/nfast/bin/hsmadmin enroll` command automatically validates certificates as part of the enrollment process and produces a warning if it fails to find a certificate for any service. This warning is expected if the HSM:

- is in recovery mode
- is running a firmware version prior to 13.5
- has been upgraded to a firmware version of 13.5 or later but has not performed a factory state operation since the upgrade.

  If you receive this warning in any other circumstance you should contact Entrust support.



(**nShield 5s only**) Entrust recommends that you take a backup of your `sshadmin` key.

For example, you could use `hsmadmin keys backup /root/.ssh/id_n-`

> `shield5_sshadmin` for backups that will be restored to the same machine. If the path `/root/.ssh/id_nshield5_sshadmin` is used, and the `sshadmin` key is missing from the usual installed location under `/opt/nfast`, then that key will be used automatically when running the nShield install script.
>
> Note that this key will not be usable on another machine or if the OS is re-installed as it has protections tied to the local machine. For backups that may be restored to a different machine or re-installed OS, use `hsmadmin keys backup --passphrase /path/to/backup_key` to protect the key with a user-supplied passphrase (replacing `/path/to/back-up_key` with the actual path to where the backup key should be written).

2.4. After installing the software

After you have successfully installed the Security World Software, complete the following steps to finish preparing your HSM for use:

1. Ensure that your public firewall is set up correctly.
   See Before you install the software.
2. **nShield 5s:** If the SSH keys have not been set up, create the communication path between the host machine and the HSM, as described in Set up communication between host and module (nShield 5s HSMs).

   > If you followed all the steps in the installation instructions when installing the software, this should already be set up.

3. **Network-attached HSMs:** Perform the necessary basic HSM-client configuration tasks, as described in Basic HSM and remote file system (RFS) configuration.
4. **PCIe and USB HSMs:** If necessary, perform additional software and HSM configuration tasks, as described in Client software and module configuration: PCIe and USB HSMs:
   - Set up client configuration, as described in Client cooperation
   - Set nShield specific environment variables, as described in Setting environment variables.
   - Configure logging and debugging parameters, as described in Logging and debug-ging
   - Configure Audit Logging, as described in Configuring audit logging
   - Configure the hardserver, as described in Configuring the hardserver

5. Create and configure a Security World, as described in Create a new Security World.
6. Create an OCS, as described in Creating Operator Card Sets (OCSs).
7. **Network-attached HSMs:** Complete additional necessary HSM-client configuration tasks:

    a. To configure the unit so that it works with the client machine, see Configuring the nShield HSM to use the client.

    b. To configure client computers so that they work with the unit, see Configuring client computers to use the nShield HSM.

    

    For this release, you must generate a new client configuration file to take advantage of new functionality. To generate a new client configuration file, back up your existing configuration file and run cfg-mkdefault. This generates a template for the configuration file into which you can copy the settings from your old configuration file.

    c. To enable the TCP sockets for Java applications, run the command:

    ```
    config-serverstartup -sp
    ```

    For more information, see Client configuration utilities.

    When all additional HSM configuration tasks are completed, you can:

    1. Stop and then restart the hardserver, as described in Stopping and restarting the hardserver.
    2. Test the installation and configuration.

3. Using silent installations

This guide describes how to use the command line for software installation and uninstallation for automation.

When you follow the standard installation instructions for Security World Software, the `setup.msi` installer runs automatically when you place the Security World Software installation media in the optical disc drive. You then follow the on-screen instructions from the installer to configure your installation.

However, if you run the `setup.msi` installer from the command line, you have the option to define the components you want to install via the Windows command prompt. This allows your installations to run 'silently', without the need for further interaction with the installer.

3.1. Installing using the silent install functionality

The Windows Installer (MSI) has the ability to install software without user interaction. This is useful for automation purposes.

Before starting, please ensure that:

- Any previously installed Security World Software is uninstalled
- If the directory `C:\Program Files\nCipher` exists, it is deleted
- If the directory `C:\ProgramData\nCipher` exists, it is renamed or deleted

To install the nShield Software using the silent install functionality:

1. Log in as Administrator or as a user with local administrator rights.
2. Place the Security World Software installation media in the optical disc drive. If the installer runs automatically, quit the installer.
3. Open a Command Prompt, and run the `msiexec` command:
    - To perform a full install of the nShield Security World software:

      ```
      msiexec /i <PATH_TO_MSI> /quiet /forcerestart
      ```

      This installs the nShield Security Software to the default installation directory, `%PROGRAMFILES%\nCipher\nfast\`, and restarts the machine.
    - To manually select the packages installed with the nShield Security World software, use the `ADDLOCAL="<options>"` argument and specify the required packages. For example:

```
msiexec /i d:\setup.msi /quiet ADDLOCAL="FeatDrivers,FeatHwsp,FeatCSPs" /forcerestart
```

See the ADDLOCAL options table for a list of available options.



You can generate a verbose install log by adding `/l*v <path-to-file.txt>` to the command after the `/quiet` argument. For example:

```
msiexec /i E:\setup.msi /quiet /l*v C:\users\USER_NAME\installLog.txt>
/forcerestart
```

This creates a log file in the specified directory.

ADDLOCAL options

Option	Description
FeatCSPs	nShield CSP package, includes CAPI and CNG providers and associated tools.
FeatCtd	nShield CipherTools Developer package, includes example programs and libraries.
FeatCtls	nShield Core Tools package, includes diagnostic and performance tools.
FeatDebug	nShield Debug package, includes PDB files.
FeatDocs	nShield Developer Reference, includes documentation of the nCore API.
FeatDrivers	nShield Device Driver package, includes PCIe and USB drivers.
FeatHwsp	nShield Hardware Support package, includes the hardserver.
FeatJava	nShield Java package, includes nShield Java jars.
FeatJavaDev	nShield Java Developer package, includes examples and javadocs.
FeatRACClientTools	nShield Remote Administration Client Tools package, includes nShield Remote Administration Client executables.
FeatRACServer	nShield Remote Administration Server package, includes nShield Remote Administration server.
FeatRnrDrv	nShield Trusted Verification Device drivers.
FeatSnmp	nShield SNMP package, includes SNMP service and tools.

3.2. Uninstalling using the silent install functionality

To uninstall the nShield Security Software using the silent uninstall functionality:

1. Log in as Administrator or as a user with local administrator rights.
2. Place the Security World Software installation media in the optical disc drive. If the

installer runs automatically, quit the installer.

3. Open a Command Prompt, and run the command:

```
msiexec /x <PATH_TO_MSI> /quiet /forcerestart
```

This uninstalls the nShield Security Software packages and restarts the machine.

To generate a verbose uninstall log, add `/l*v <path-to-file.txt>` to the command after the `/quiet` argument. For example:

```
msiexec /x E:\setup.msi /quiet /l*v C:\users\USER_NAME\uninstallLog.txt> /forcerestart
```

This creates a log file in the specified directory.

4. Problems during installation and commissioning

4.1. PCIe HSMs

If problems are encountered when installing or commissioning an nShield HSM which prevent services from starting it will not be possible to use any of the debugging and logging tools described in Checking the installation

In this situation the command `hsmdiagnose` may help identify network and hardware issues that are preventing the system from starting.

This command requires `root` privileges on Linux and the privileges of the built-in local Administrators group on Windows.

```
hsmdiagnose
```

The command takes no parameters:

When the command is executed it will run a series of diagnostics tests and store the results in a file on the client PC. The information in the file is primarily intended for use by Entrust Support but you may be able to use the information to diagnose the issue yourself. If you are unable to do so, contact Entrust Support and send them a copy of the results file.

5. Uninstalling Security World Software

This section describes how to uninstall Security World software.

Entrust recommends that you only uninstall the Security World software in the following cir cumstances:

- You are certain it is no longer required.
- You intend to upgrade it.

In Windows environments, because the `hardserver` is installed as a named service (known as the nFast server), it is only possible to have one Security World software installation on any given computer.

In Linux environments, it is also not possible to have more than one Security World software installation on the same computer.

Entrust therefore recommends that, when you are upgrading, any older versions of soft- ware are uninstalled and deleted.

The automated Security World software installers do not delete user created components, key data, or Security World data. However:

- On Linux, a manual installation using `.tar` files **does** overwrite existing data and directo ries.
- On Windows, if the installer detects an existing Security World Software installation, it asks you if you want to install the new components. These components replace your existing installation.



nShield 5s

Make sure you have completed the steps described in before upgrading software before you uninstall any software.

5.1. Uninstalling the Security World software on Windows

This procedure requires the privileges of the built-in local Administrators group.

1. Open the **Control Panel** and select **Programs and Features**.
2. For the following programs, select **Uninstall** and follow the on-screen instructions:
    - **nShield Software**.
    - **CyberJack Base Components**.

3. If the file `nCipherKM.jar` is present, it is located in the extensions folder of your local Java Virtual Machine. The uninstall process may not delete this file and you have to remove it manually.

5.1.1. Removal of Security World data

The uninstaller removes only those files that were created during the installation.

If you wish to completely uninstall the Security World, including any data created during its operation, including key data, navigate to the installation directory and delete the files in the *%NFAST_KMDATA%* folder.



Do not remove Security World data as part of an upgrade procedure. Only remove Security World data if you wish to do a complete uninstalla tion.

5.2. Uninstalling the Security World software on Linux

This procedure requires `root` privileges.

5.2.1. Uninstalling the tarballs

1. Remove drivers, install fragments, and scripts and to stop services, run the command:

```
/opt/nfast/sbin/install -u
```

2. Refer to Directory Cleanup for follow-on actions post uninstall.

5.2.2. Uninstalling the RPMs

5.2.2.1. Using dnf (Oracle Enterprise Linux and Red-Hat Enterprise Linux)

1. List the installed nShield packages using `dnf`.

```
dnf list installed | grep nShield
```

Example output:

```
dnf list installed | grep nShield
nShield-ctd.x86_64                          13.7.3-1.1731531521.c6069a7d744  @@commandline
```

```
nShield-ctls.x86_64                          13.7.3-1.1731531521.c6069a7d744  @@commandline
nShield-devref.x86_64                        13.7.3-1.1731531521.c6069a7d744  @@commandline
nShield-hwsp.x86_64                          13.7.3-1.1731531521.c6069a7d744  @@commandline
nShield-javasp.x86_64                        13.7.3-1.1731531521.c6069a7d744  @@commandline
nShield-jd.x86_64                            13.7.3-1.1731531521.c6069a7d744  @@commandline
nShield-ncsnmp.x86_64                        13.7.3-1.1731531521.c6069a7d744  @@commandline
nShield-raserv.x86_64                        13.7.3-1.1731531521.c6069a7d744  @@commandline
```

2. Uninstall a single, or set of packages.

```
dnf remove <package name> <package name>
```

Example output:

```
dnf remove nShield-ctls nShield-raserv
Updating Subscription Management repositories.
Dependencies resolved.
================================================================================================================================
================================================
 Package                          Architecture             Version
Repository                       Size
================================================================================================================================
================================================
Removing:
 nShield-ctls                      x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                    247 M
 nShield-raserv                    x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                    1.6 M

Transaction Summary
================================================================================================================================
================================================
Remove  2 Packages

Freed space: 249 M
...
Complete!
```

3. Alternatively, uninstall all installed packages.

```
dnf remove nShield*
```

Example output:

```
dnf remove nShield*
Updating Subscription Management repositories.
Dependencies resolved.
================================================================================================================================
================================================
 Package                          Architecture             Version
Repository                       Size
================================================================================================================================
================================================
Removing:
 nShield-ctd                       x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                    310 M
 nShield-ctls                      x86_64                   13.7.3-1.1731531521.c6069a7d744
```

```
@@commandline                   247 M
 nShield-devref                   x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                    42 M
 nShield-hwsp                     x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                   307 M
 nShield-javasp                   x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                   3.2 M
 nShield-jd                       x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                   8.0 M
 nShield-ncsnmp                   x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                    73 M
 nShield-raserv                   x86_64                   13.7.3-1.1731531521.c6069a7d744
@@commandline                   1.6 M

Transaction Summary
================================================================================================================
================================================
Remove  8 Packages

Freed space: 992
...
Complete!
```

5.2.2.2. Using zypper (SUSE Enterprise Linux)

1. List the installed nShield packages using `zypper`.

```
zypper search --installed-only nShield
```

Example output:

```
zypper search --installed-only nShield
Loading repository data...
Reading installed packages...

S  | Name           | Summary                               | Type
---+----------------+---------------------------------------+--------
i+ | nShield-ctls   | nShield core tools                    | package
i  | nShield-hwsp   | nShield hardware support              | package
i+ | nShield-raserv | nShield remote administration server | package

    Note: For an extended search including not yet activated remote resources please use 'zypper
    search-packages'.
```

2. Uninstall a single, or set of packages.

```
zypper remove -y <package name> <package name>
```

Example output:

```
zypper remove -y nShield-ctls nShield-raserv
Reading installed packages...
Resolving package dependencies...

The following 2 packages are going to be REMOVED:
```

```
  nShield-ctls nShield-raserv

2 packages to remove.

Package install size change:
              |         0 B    required by packages that will be installed
  -250.7 MiB  |  -  250.7 MiB  released by packages that will be removed

Backend:  classic_rpmtrans
Continue? [y/n/v/...? shows all options] (y): y
(1/2) Removing: nShield-ctls-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................................[done]
...
(2/2) Removing: nShield-raserv-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................................[done]
```

3. Alternatively, uninstall all installed packages.

```
zypper remove -y "nShield-*"
```

Example output:

```
zypper remove -y "nShield-*"
Reading installed packages...
Resolving package dependencies...

The following 3 packages are going to be REMOVED:
  nShield-ctls nShield-hwsp nShield-raserv

3 packages to remove.

Package install size change:
              |         0 B    required by packages that will be installed
  -660.5 MiB  |  -  660.5 MiB  released by packages that will be removed

Backend:  classic_rpmtrans
Continue? [y/n/v/...? shows all options] (y): y
(1/3) Removing: nShield-ctls-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................................[done]
...
(2/3) Removing: nShield-raserv-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................................[done]
...
(3/3) Removing: nShield-hwsp-13.7.3-1.1743026563.3b0b57a351a.x86_64
.....................................................................................[done]
```



Files that were created after an `rpm` was installed are not deleted.

Refer to Directory Cleanup for post-uninstall actions.

5.2.3. Directory Cleanup

1. Delete all the files, including those in subdirectories, from `/opt/nfast` and `/dev/nfast/`.



The following commands delete both software and data. If you are

> uninstalling as part of an upgrade ensure that you have performed all the steps in Before upgrading software to ensure that the critical data is backed-up so that it can be restored after the upgrade.

```
rm -rf /opt/nfast
rm -rf /dev/nfast
```

2. If you are not re-installing the product, delete the configuration file `/etc/nfast.conf` if it exists.
3. Unless they are needed for a new installation, remove the user and group `nfast` and, if they exist, the user and group `ncsnmpd`.

```
sudo userdel ncsnmp
sudo userdel nfast
sudo groupdel ncsnmp
sudo groupdel nfast
```

4. If the file `nCipherKM.jar` is present, it is located in the extensions folder of your local Java Virtual Machine. The uninstall process may not delete this file and you may have to remove it manually.

6. System upgrade

Terms used in this topic

software

Security World software running on the PC in which the HSM is installed

firmware

Security World firmware running on the HSM

You can upgrade **software** and **firmware** independently of each other.

6.1. Software and firmware compatibility

In general, Entrust recommends that you use the software and firmware from the same version of Security World. The system is designed to be backwards compatible so that it will still operate with differing versions of software and firmware but some functionality may not be available and you may receive warnings during operation.

This user guide describes the behaviour of v13.5 software interacting with v13.5 firmware. Some areas where functionality differs depending on the version of firmware loaded are also described in this guide but it is not possible to describe all possible combinations of software and firmware.

Release notes and user guides for each Security World release are available from the Entrust website and these together with Entrust Support will help you should you experience any problems when operating with differing versions of software and firmware.

6.2. System upgrade procedure

When upgrading the whole system, Entrust recommends that you always upgrade the host software before upgrading the HSM firmware, however this is not mandatory and you may upgrade the firmware first should you wish to do so.



Always read the release notes accompanying the Security World release before upgrading any part of the system as these may include additional upgrade steps.



If the Version Security Number (VSN) of the firmware has been increased, it may not be possible to roll-back the firmware to the previous version after upgrade. See Version Security Number for more infor-

mation.

6.3. Upgrade software

For Security World software upgrades, you do not need to delete key data or any existing Security World. If you do delete Security World data, it cannot be restored unless you have an up-to-date backup and a quorum of the Administrator Card Set (ACS) available.

6.3.1. Before upgrading software

You must perform these steps if you are planning to re-install the Security World software, for example to re-install it on the same machine after an operating system update, or to install a newer Security World software version as part of an upgrade.

Performing these steps is useful even if you are not planning a re-install because it preserves data that you would otherwise irretrievably lose when you uninstall the Security World software.

1. (**Only if you are using the nShield PKCS #11 library**) Back up the `cknfastrc` file by copying it to external media or to a location not within the Security World installation.
2. (**Linux only**) Back up your Security World and nShield configuration files stored in `/opt/nfast/kmdata/` and `/opt/nfast/hardserver.d` by copying them to external media or to a location not within `/opt/nfast`.

   When you are upgrading the Security World, you will also restore the backup to preserve your PKCS #11 and Soft KNETI authentication settings and any customizations. If you delete the `/opt/nfast` or `$NFAST_HOME` directory without making a copy of it, you will lose these configuration settings. When you are restoring a Security World from a backup, you will need to maintain permissions.

3. (**nShield 5s only**) Back up your SSH keys, see Making a backup of installed SSH keys:

   - If you are planning a clean reinstallation of the Security World software on the **same machine and same operating system**, back up your SSH keys in `/opt/nfast/services` using `hsmadmin keys backup`.
   - If you are planning to re-create the Security World on a **different machine or after re-installing the operating system**, use `hsmadmin keys backup --passphrase`. `hsmadmin keys backup` alone is only suitable for a local backup followed by a local restore on the same machine and same operating system.

     

     If you erase your SSH keys without making a backup you will need

> to use recovery mode, see Recovery mode to restore communication with the HSM. This will return the HSM to factory state, see Factory state.

6.3.2. Reinstall Security World software

Software upgrade is performed by uninstalling the old software as described in Uninstalling Security World Software and then installing the new software as described in Install the Security World software.

6.3.3. After upgrading software

1. Copy back any data that was manually backed-up as part of the procedures in Before upgrading software to the locations from which it was copied.
2. (**nShield 5s only**) Restore communication with the HSM by following the procedures at restoring SSH keys from backup.

6.4. Upgrade firmware

See the following pages for instructions on upgrading the firmware:

- Upgrading the image file and associated firmware: network-attached HSMs
- Upgrade firmware: nShield Solo, Solo XC, and Edge HSMs
- Upgrade firmware: nShield 5s

7. Software packages on the installation media

This guide lists the contents of the component bundles and the additional software supplied on your Security World Software installation media.

Entrust supply the hardserver and associated software as bundles of common components that provide much of the required software for your installation. In addition to the component bundles, provide individual components for use with specific applications and features supported by certain Entrust modules.

To list installed components, use the `ncversions` command-line utility.

7.1. Security World installation media

The following component bundles and additional components are supplied on the Security World installation media.

Linux Package	Windows Feature in the Installer	Content
`hwsp`	nShield Hardware Support	Hardware Support package, including the nShield Server and the most essential setup tools including enquiry, nfkminfo, and the Remote Administration Client command line tool. On Linux this also contains the PCIe HSM device drivers.
`ctls`	nShield Core Tools	Management utilities, including generatekey, diagnostic, OpenSSL, performance tools, the nShield Remote Administration GUI tool, and the PKCS#11 library.
`ctd`	nShield CipherTools	Developer package example programs, and developer libraries for the nCore, SecurityWorld and PKCS#11 APIs for C/C++ and Python.
`devref`	nShield Developer Reference	Reference Documentation for the nCore API.
N/A	nShield CSPs (CAPI, CNG)	CAPI and CNG providers and associated tools.
N/A	nShield Debug	PDB and .map files for nShield libraries and executables.
N/A	nShield Device Drivers	Device drivers for PCI and USB attached nShield devices, included in `hwsp` for Linux.
`javasp`	nShield Java	nCipherKM JCA/JCE Provider, associated classes (including nFast Java generic stub classes).

Linux Package	Windows Feature in the Installer	Content
`jd`	nShield Java Developer	Java developer libraries and documentation for the nCore API and generic stub.
`ncsnmp`	nShield SNMP	nShield SNMP service and tools.
N/A	nShield Trusted Verification Device	Driver for the Trusted Verification Device (TVD), included in `ctls` for Linux.
`raserv`	nShield Remote Administration Server	nShield Remote Administration server for enabling communication between remote clients and their Type3 smartcards and this machine.