nShield Security World

Remote Administration v13.4.5 User Guide

20 March 2024

Table of Contents

1. Remote Administration overview

nShield Remote Administration lets you administer distantly located nShield PCIe and network attached Hardware Security Modules (HSMs). It uses the following components to locally manage remote HSMs:

- Remote Administration Cards — Custom smart cards equipped with a nShield applet.
- Trusted Verification Devices (TVDs) — nShield smart card readers used with Remote Administration Cards to create a secure connection with the target HSM (includes Type A USB connector).
- Remote Administration Client (RAC) software — GUI tool running on client laptop or workstation to configure connection to HSM.
- Remote Administration Service — nShield software that runs on the data center side and enables the connection from Remote Administration Clients to the target HSMs.

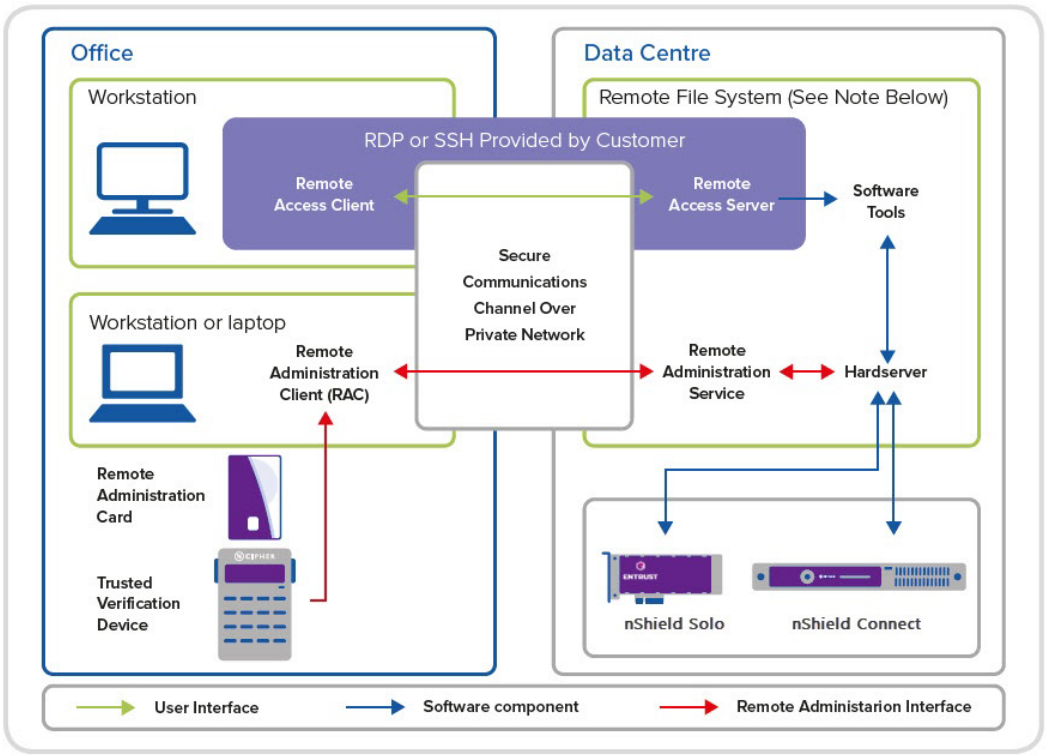


Figure 2.1: Remote Administration architecture

nShield Remote Administration creates a secure connection between your remote HSM and your local Remote Administration Cards and TVD, letting you present your quorum of smartcards and administer your HSMs as if physically present with the device. Communicating over your VPN, you control the HSM from a laptop or

workstation via remote desktop or secure shell session. Whenever a card is required, for example, when creating a card set or authorizing an operation, an nShield Remote Administration Card is inserted in the appropriate card reader as and when the Security World software instructs you to do so.

The full range of administrative tasks can be carried out from a different location to that of an nShield Connect or nShield Solo. Security World software and utilities are used to manage the HSM, communicating through the remote access solution that your organization normally uses, such as SSH or a remote desktop application.

All card holders need to be able to view the same remote session so they know when to insert their cards. As an alternative, the person running the remote session needs to be able to contact all relevant card holders, to tell them when to insert cards in their TVD, and verify the ESN of the appropriate HSM.

Entrust recommends that you only use an nShield Trusted Verification Device or a standard smart card reader for ISO/IEC 7816 compliant smart cards. The remainder of this guide assumes that you are using an nShield TVD.

1.1. Remote Administration Cards

nShield Remote Administration Cards are compliant with FIPS 140 Level 3. They are capable of negotiating cryptographically secure connections with an HSM, using warrants as the root of trust.

nShield Remote Administration Cards store token shares in a similar way to standard nShield cards, but are also capable of establishing and using a secure connection to communicate token shares.

For a card to be recognized by the system, it must be included in the Authorized Card List, which is used to control Remote Administration access. See Edit the Authorized Card List for more information about the Authorized Card List.

1.2. Trusted Verification Devices (TVDs)

The TVD provides additional assurance, by requiring you to verify the Electronic Serial Number (ESN) of the relevant HSM, before it is communicated to the nShield Remote Administration Card and a secure connection is established between the card and the HSM.

Multiple TVDs can be associated with a single HSM, up to the maximum number of

Dynamic Slots allowed in the HSM configuration. Dynamic Slots are virtual card slots that allow you to associate a TVD with a specific HSM. They are configured by the person responsible for setting up your nShield HSM environment.

A nShield Remote Administration Client can connect to one TVD during a session. This can be selected from multiple readers that may be attached to your computer.

A TVD can only be associated with one HSM during a nShield Remote Administration Client session.

1.3. Remote Administration Client (RAC) software

The RAC application resides on your local Windows, Linux-based or macOS computer. This is the RAC icon:

The RAC enables you to:

- Associate a suitable card reader that is attached to your computer with an nShield HSM in a different location
- Present an nShield Remote Administration Card to the appropriate HSM using either:
  - A TVD (recommended).
  - A standard smart card reader for ISO/IEC 7816 compliant smart cards.

    Only use in line with the security policies of your organization. A standard smart card reader provides no protection from security threats such as, for example, malicious software on your computer.

The secure connection between an nShield Remote Administration Card and the target HSM is provided through the Remote Administration Service.

When you start the nShield Remote Administration Client, you:

- Select the appropriate Remote Administration Service. Hostnames are supported.
- Select an HSM from a list of all HSMs available through the chosen Remote

Administration Service.

- Select a TVD.

Your local TVD is now associated with the HSM for the duration of the current GUI or command-line session. This means that:

- A computer equipped with a TVD and the nShield Remote Administration Client can be used to present cards in the data center.
- A quorum of card holders can assemble in a local office to present their cards, rather than traveling to the data center.

The nShield Remote Administration Client also displays whether the TVD is connected and whether a card is inserted.

1.4. Remote Administration Service

The Remote Administration Service runs alongside the appropriate hardserver, which is an nShield-provided software service that controls communication between applications and nShield HSMs.

The hardserver resides on:

- An nShield Solo host.
- A Remote File System (RFS), which is also a client of an nShield Connect.
- A client of an nShield Connect.

The Remote Administration Service:

- Listens by default on port 9005 for incoming connection requests from nShield Remote Administration Clients. The default port can be changed during system configuration.
- Supplies a list of available HSMs to the nShield Remote Administration Client.
- Communicates with the hardserver that is connected to the requested HSM, to establish and maintain an association between the relevant TVD and the HSM.
- Relays encrypted messages between the relevant HSM and the nShield Remote Administration Card in the reader that is attached to your local computer.

Depending on the hardserver configuration, the Remote Administration Service can associate up to 16 TVDs with each HSM. The default number of devices that can be associated with an HSM is zero.

To start or stop the Remote Administration Service, use the following commands in a command window or the Window Control Panel (Windows only):

```
$ systemctl stop nc_raserv
$ systemctl start nc_raserv
```

For more information, refer to the *Client software and module configuration* chapter of your HSM User Guide.

2. Requirements

2.1. Compatibility with nShield firmware and Security World releases

Remote Administration is compatible with all firmware versions of nShield 5s and 5c HSMs.

For nShield Solo, Solo+, Solo XC, and the Connect and Connect XC HSMs:

- Remote Administration is supported from firmware version 2.61.2. For HSM firmware version compatibility, see the release notes at https://nshieldsupport.entrust.com. These notes contain the latest information about your product.
- Remote Administration can be used in conjunction with Remote Operator from 12.81.
- Remote Administration is part of the Security World software from 12.00.
- nShield Solo+/ XC type HSMs must be warranted with a warrant of type KLF2. Some Solo HSMs will require an in-field warrant upgrade from KLF1 to KLF2.

3. Server-side preparation tasks

This chapter outlines the tasks required on the server-side that must be completed before the Remote Administration Client can be installed and used.

For more information on updating the configuration file for your HSM, see the *Hardserver configuration files* (PCIe HSMs) or *HSM and client configuration files* (network-attached HSMs) chapter in the HSM User Guide.

The Remote Administration Client requires that quorum participants use their cards in a TVD associated with the HSM. The steps involved in meeting this requirement are as follows:

1. Remote Administration Service has been enabled.
    - If the HSM and the associated Security World are being installed the first time, install the HSM and, as part of the overall installation process, install the Remote Administration Service bundle (`raserv`). For installation instructions, follow the Installation Guide of the HSM.
    - If the HSM and the associated Security World are already installed but Remote Administration was not installed:
        - You have to re-install the Security World software. See Prepare an existing Security World installation for Remote Administration.
        - If ACS cards are already in use but they are not labeled **Remote Administrator Ready**, then the cards have to be migrated to Java cards before they can be used via a Remote Administration Client.
    - Ensure the Remote Administration Service firewall port (default: 9005) is open for incoming connection requests from nShield Remote Administration clients.
2. Cards have been enabled for use through RAC. See Edit the Authorized Card List.
3. Dynamic slots have been configured so that cards can be presented remotely. See Set up dynamic slots.

In some cases, the steps are covered in more detail in the *User Guide* for your HSM. These are referenced in the appropriate section. We recommend you have the *User Guide* available to you at the same time as reviewing the Remote Administration setup steps.

3.1. Prepare an existing Security World installation for Remote Administration

If you need to enable the Remote Administration Service into an existing system:

1. Ensure the HSM firmware is compatible with Remote Administration.
2. For Solo HSMs only: Ensure the nShield Solo+/ XC HSM is warranted with a KLF2 warrant.
3. For Connect HSMs only: Connect HSM can also accept a configuration from the RFS or a remote computer, see Enable config push on nShield Connect.
4. Re-install the Security World software.

3.2. Ensure the HSM firmware is compatible with Remote Administration

You can confirm current firmware version via the `enquiry` command. In section **Module**, look for **version** and check it against the information in Compatibility with nShield firmware and Security World releases.

If the firmware needs upgrading, follow the instructions relevant to the HSM:

- Upgrade the nShield Connect image file and firmware using the front panel.
- Upgrade the nShield Connect image file and firmware from privileged client.
- Upgrade the nShield Solo firmware.

3.2.1. Upgrade the nShield Connect image file and firmware using the front panel

Important: If you upgrade your nShield Connect firmware you **must** make sure that you have a working quorum of Administrator Cards, as you will need to reload your Security World back onto the HSM once the firmware has been upgraded. If you cannot provide the required quorum from the ACS **do not** perform a firmware upgrade!

1. From the main menu on the nShield Connect front panel, select **System > Upgrade system**.
2. Confirm that you want to upgrade the image file and/or firmware.
3. Verify the image version, HSM (firmware) version, and image VSN that are

displayed, and confirm the upgrade when prompted. If in doubt contact nShield support for assistance in determining the correct version to use.

4. When the image file and/or firmware upgrade is complete, the front panel may be slow to respond. We recommend a full power off and power on to complete the upgrade procedure and to restore optimum front panel responsiveness. This may need to be repeated for a second time if the front panel seems slow to respond.
   a. On the front panel select **System > Shutdown/Reboot > Shutdown**.
   b. Switch the power supplies, at the rear of the nShield Connect, to **0**, then back to **1**.

3.2.2. Upgrade the nShield Connect image file and firmware from privileged client

1. Use the `nethsmadmin` utility to list the nethsm image files on the RFS. Run the command:

   Linux:

   ```
   #/opt/nfast/bin/nethsmadmin --module=MODULE --rfs=RFS_IP --list-images
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>nethsmadmin --module=MODULE --rfs=RFS_IP --list-images
   ```

   In this command:

   - *RFS_IP* specifies the IP address of the RFS.
   - Additionally the `--rfs-hkneti=RFS_HKNETI` and `--rfs-esn=RFS_ESN` options can be set to enable secure authentication of the RFS. There are three possible cases:
     - **Without secure authentication**: The authentication of the RFS will be based on the IP address only if the `--rfs-hkneti` and `--rfs-esn` options are not specified.
     - **Software-based authentication**: The `--rfs-hkneti` option specifies the software KNETI hash of the RFS. The `--rfs-esn` option shall not be specified.

       RFS_HKNETI can be obtained by running `anonkneti -m0 localhost` on the RFS.

- **nToken authentication**: Only if an nToken (or local HSM) is installed in the RFS. The `--rfs-hkneti` and `--rfs-esn` options specify the KNETI hash and ESN of the nToken.

  RFS_HKNETI and *RFS_ESN* can be obtained by running `ntokenenroll -H` on the RFS.

2. If the image file you require is not on the RFS, copy the directory that contains the required image file to the following directory on the RFS:

```
%NFAST_HOME%\nethsm-firmware
```

3. Use the `nethsmadmin` utility to make the nShield Connect use a specific image file from the RFS. Run the command:

```
nethsmadmin --module=MODULE --upgrade-image=image_name
```

In this command:

- *MODULE* specifies the HSM to use, by its ModuleID (default = 1)
- *image_name* specifies the image file to use from the RFS

image_name must be the path to the image file that is displayed when you execute the `nethsmadmin` command with the `--list-images` option. Errors are reported if you use either just the image name, or the full path.

The following is an example of the output:

```
nethsmadmin --upgrade-image=nethsm-firmware/latest-xc-plus-12-60-2-vsn31/nCx3N.nff
Initiating appliance image upgrade using file nethsm-firmware/latest-xc-plus-12-60-2-vsn31/nCx3N.nff
Upgrade operation state changed to: Image Transfer Initiated
Upgrade operation state changed to: Image Transferred
Upgrade operation state changed to: Image Verified
Not able to contact appliance because of reason(23): CrossModule,#1-NetworkError
Upgrade operation final state: Image Verified
Image upgrade completed. Please wait for appliance to reboot.
Please wait for approximately half an hour for the appliance to internally upgrade.
```

The following line is expected as the Connect temporarily severs its network connection whilst it performs certain sensitive activities such as a firmware upgrade. No action is required.

```
Not able to contact appliance because of reason(23): CrossModule,#1-NetworkError
```

If the nShield Connect suffers a loss of power while you are upgrading the image file and/or internal module firmware, you should exit the `nethsmadmin` utility and try to restart the process at Step 1, once power has been restored to the HSM.

4. Run the `enquiry` command-line utility to verify the HSM is in operational state and has the correct firmware version. In Operational mode, the `enquiry` command-line utility shows the version number of the firmware

   Linux:

   ```
   /opt/nfast/bin/enquiry
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>enquiry.exe
   ```

3.2.3. Upgrade the nShield Solo firmware

1. Sign in to the host as an Administrator.
2. Put the HSM in Maintenance mode and reset the HSM.

For information on changing the mode, see the *nShield Edge and nShield Solo User Guide Appendix, Checking and changing the mode on an nShield Solo module*.

3. Run the following command-line utility to check that the HSM is in the pre-maintenance state.

   Linux:

   ```
   /opt/nfast/bin/enquiry
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>enquiry
   ```

If the nShield Solo HSM is still in the operational state, it means that the override switch is on. Refer to the installation instructions in the *nShield Edge and nShield Solo Installation*

> *Guide* for information on accessing the override switch and switching it off.

4. Locate the firmware folder on the installation media in the firmware directory. For example:

   Linux:

   ```
   /tmp/firmware/FW_VERSION
   ```

   Windows:

   ```
   E:\firmware\FW_VERSION
   ```

5. Load the new firmware:

   Linux:

   ```
   /opt/nfast/bin/loadrom –m1 /tmp/firmware/FW_Version/ncx3p-xx.nff
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>loadrom –m1 E:\firmware\FW_VERSION\ncx3p-xx.nff
   ```

   The upgrade may take a while to complete, during which time no activity will be observed. Wait at least five minutes before proceeding unless you are informed the upgrade has completed successfully beforehand.

6. **Solo XC only**:

   Reboot the Solo XC for the firmware upgrade to take effect.

   Linux:

   - Bare metal environments:

     With the module in Maintenance mode, run the following command to reboot the Solo XC.

     ```
     nopclearfail -S -m<module_number>
     ```

     Wait for the Solo XC to reboot, which will take about ten minutes on a host machine running Linux.

The module has completed rebooting when running enquiry no longer shows the module as Offline.

- Virtual environment hosts:

  Reboot the Solo XC by rebooting the system that is hosting the Solo XC.

Windows:

With the module in Maintenance mode, reboot the Solo XC for the firmware upgrade to take effect. To do this, reboot the system that is hosting the Solo XC.

Wait for the Solo XC to reboot. The module has completed rebooting when running enquiry no longer shows the module as Offline.

7. Put the HSM in Initialization mode and reset the HSM:

   Linux:

   ```
   /opt/nfast/bin/initunit
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>initunit
   ```

8. Put the HSM into Operational mode.
9. Run the `enquiry` command-line utility to verify the HSM is in operational state and has the correct firmware version. In Operational mode, the `enquiry` command-line utility shows the version number of the firmware.

3.2.4. Re-install the Security World software

Ensure that you select to install the Remote Administration Service package. The new installation will create the user roles, etc. that are required for Remote Administration. For re-installation instructions, follow the *Installation Guide* of the HSM

3.2.5. Ensure the nShield Solo+/ XC HSM is warranted with a KLF2 warrant

1. Confirm that a warrant is installed and that it is a KLF2 warrant.

```
nfwarrant.exe --check
```

2. If no warrant exists or it is a KLF1 one, generate a certificate signing request:

```
nfwarrant.exe --csr --req=esn_of_module
```

3. Supply the certificate signing request to Entrust nShield Support who will then issue you a warrant for use with the specified HSM.
4. Warrant the HSM, see the *nShield Solo User Guide*.

3.2.6. Enable config push on nShield Connect

You can allow configuration files to be pushed from the RFS and/or any client computer. The RFS config push is preferred unless the config push client is not actually the same machine as the RFS. The RFS config push is recommended at least when securely bootstrapping the configuration of the system from the Connect front panel.

3.2.6.1. Enabling config push from the RFS

On the Connect display, use the right-hand navigation button to select **System > System configuration > Remote File System**, and follow the steps described in the *nShield Connect User Guide*. To enable config push from the RFS, set the push mode to **AUTO** with RFS secure authentication enabled (recommended), or to **ON**.

The RFS config push supports specifying secure authentication from the Connect front panel, whereas the client config push only supports specifying authentication either from the nShield Connect Serial Console `push` command, or from the config file itself.

3.2.6.2. Enabling config push from a client computer

To enable config push from a client computer, on the Connect display, use the right-hand navigation button to select **System > System configuration > Config file options > Client config push > Config push mode**, set **ON** or **OFF**, then select **CONFIRM**. A confirmation message will be displayed.

After enabling config push, specify the IP address of the client to push the

configuration from. On the Connect display, use the right-hand navigation button to select **System > System configuration > Config file options > Client config push > Client address**. Enter the IP address and select **CONFIRM**. A message is displayed confirming your chosen IP address. Select **CONTINUE**.

Any remote computer is allowed to push configuration files if no IP address or the 0.0.0.0 address is specified.

3.2.7. Migrate existing ACS cards to Smartcards

If your existing ACS is of type not explicitly labeled as **Remote Administrator Ready**, it may be necessary to migrate existing ACS to the Smartcards, see *Replacing the Administrator Card Set* in the *nShield Connect User Guide*.

3.3. Change the Remote Administration Service port

To change the port used by Remote Administration Clients to access the Remote Administration Service, set the `port` field in the `remote_administration_service_slot_server_startup` section of the configuration file:

```
[remote_administration_service_startup]
# Start of the remote_administration_service_startup section
# Remote Administration Service communication settings, these are only read at
# Remote Administration Service startup time
# Each entry has the following fields:
#
# The port for the Remote Administration Service to listen on for incoming TCP
# connections from remote administration clients (default=9005)
# port=PORT
```

3.4. Edit the Authorized Card List

You can only use Smartcards with Remote Administration if they belong to the Authorized Card List.

To include a Smartcard in the Authorized Card List:

1. Obtain the serial number for the Smartcard you want to add to the list.

   The serial number is printed on the card or can be displayed by inserting the Smartcard into a slot and running `slotinfo -m1 -s0`, where `1` is the number of the HSM and `0` is the number of the slot.

2. Add the 16-digit serial number of the card to the

`opt/nfast/kmdata/config/cardlist` (Linux) or `C:\ProgramData\nCipher\Key Management data\config\cardlist` (Windows) text file, for example:

```
4286005559064791
4286005559064792
4286005559064793
```

3. Copy the updated `cardlist` file from the RFS to all clients.

   The `cardlist` file must be updated on all clients. Network-attached HSMs use the `cardlist` file on the RFS for front panel operations. Client-initiated card operations use the `cardlist` file on the client computer.

You can allow any Smartcard to be used by adding the wildcard character * to the `cardlist` file instead of individual serial numbers, however Entrust recommends against this. Because authorizing Smartcards in this way allows all Smartcards to be used as Remote Administrator Cards, you should only do it in controlled circumstances.

3.5. Set up dynamic slots

3.5.1. Set up dynamic slots using the nShield Connect HSM front panel

1. Use the nShield Connect front panel controls to navigate to **Security World mgmt > Set up dynamic slots > Dynamic slots** and follow the instructions on the screen.

   OR

   Use the **dynamic_slots** section in the client configuration file to define the number of dynamic slots for each relevant HSM.

2. Clear the HSM for the changes to take effect, run the `nopclearfail` command or press the **Clear** button on the front of the unit. The `-a` option clears all enrolled HSMs.

   Linux:

```
#/opt/nfast/bin/nopclearfail -c -a
```

Windows:

```
C:\Program Files\nCipher\nfast\bin>nopclearfail.exe -c -a
```

The following message is displayed:

```
Module 1, command ClearUnit: OK
Module 2, command ClearUnit: OK
```

3. Check if dynamic slots appear by running the `slotinfo` command:

Linux:

```
#/opt/nfast/bin/slotinfo -m2
```

Windows:

```
C:\Program Files\nCipher\nfast\bin>slotinfo.exe -m2
```

The following message is displayed:

```
Module 2:
Slot    Type            Token       IC  Flags   Details
#0      Smartcard       present     1   A
#1      Software Tkn    -           0
#2      Smartcard       -           0   AD
#3      Smartcard       -           0   AD
```

The dynamic slots are identified with the D flag in the example above, slots 2 and 3.

3.5.2. Set up dynamic slots for nShield Connect remotely via config push option

In the following example the configuration file is pushed from the RFS. For more information, see Enable config push on nShield Connect.

1. Sign in to the RFS machine as a privileged user.
2. Create a copy of the configuration file as `config.new`, from the RFS in the following directory on the remote computer.

Linux:

```
/opt/nfast/kmdata/hsm-ESN/config
```

Windows:

```
C:\Program Data\nCipher\nfast\kmdata\hsm-ESN\config
```

In the example below, following config file copied as `config.new`.

```
/opt/nfast/kmdata/hsm-49D5-C944-F159/config/config.new
```

3. Edit the `config.new` file so that it contains the required configuration for **dynamic_slots** as shown below:

```
[dynamic_slots]
# Start of the dynamic_slots section
# The dynamic smartcard slots that the modules should provide for the use of
# administrators who do not have physical access to the module hardware
# Each entry has the following fields:
#
# ESN of the module to be configured with dynamic slots.
# esn=ESN
#
# Number of dynamic slots the module will support. (default=0)
# slotcount=INT
esn=esn_number
slotcount=2
```

4. Run the `cfg-pushnethsm` utility on the updated configuration file, specifying the updated file and the IP address of the nShield Connect to load the new configuration. To do this, use a command similar to the following:

```
cfg-pushnethsm --address=<module_IP_address> <full_path_to_config_file>
```

In this command, *<module_IP_address>* is that of the nShield Connect on which to load the configuration and *<full_path_to_config_file>* is the path to, and name of the updated configuration file.

For example:

```
/opt/nfast/bin/cfg-pushnethsm –address 192.168.156.30 /opt/nfast/kmdata/hsm-49D5-C944-
F159/config/config.new
```

5. Check that the configuration file on the RFS has been updated with the **dynamic_slots** changes. This can be confirmed using the timestamp on the updated config file.

6. Clear the HSM for the changes to take effect, run the `nopclearfail` command:

```
#/opt/nfast/bin/nopclearfail -c -a
Module 1, command ClearUnit: OK
Module 2, command ClearUnit: OK
```

7. Check if dynamic slots appear by running the `slotinfo` command:

```
#/opt/nfast/bin/slotinfo –m2
Module 2:
Slot    Type            Token       IC  Flags Details
#0      Smartcard       present     1   A
#1      Software Tkn    -           0
#2      Smartcard       -           0   AD
#3      Smartcard       -           0   AD
```

3.5.3. Set up dynamic slots for nShield Solo

1. Sign in into the computer where the nShield Solo HSM is installed, as privileged user.
2. Navigate to the following folder from the terminal.

   Linux:

```
/opt/nfast/kmdata/config/
```

   Windows:

```
C:\Program Data\nCipher\nfast\kmdata\config
```

3. Edit the config file so that it contains the required configuration for dynamic_slots as shown below:

```
[dynamic_slots]
# Start of the dynamic_slots section
# The dynamic smartcard slots that the modules should provide for the use of
# administrators who do not have physical access to the module hardware
# Each entry has the following fields:
#
# ESN of the module to be configured with dynamic slots.
# esn=ESN
#
# Number of dynamic slots the module will support. (default=0)
# slotcount=INT
esn=esn_number
slotcount=2
```

   To add multiple ESN and slot count entries, separate them by four dashes:

```
esn=esn_number_1
slotcount=2
----
esn=esn_number_2
slotcount=2
```

4. Clear the HSM for the changes to take effect, run the `nopclearfail` command:

   Linux:

   ```
   #/opt/nfast/bin/nopclearfail -c -a
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>nopclearfail.exe -c -a
   ```

   The following message will be displayed:

   ```
   Module 1, command ClearUnit: OK
   Module 2, command ClearUnit: OK
   ```

5. Check if dynamic slots appear by running the `slotinfo` command:

   ```
   #/opt/nfast/bin/slotinfo –m1
   Module 1:
   Slot    Type            Token       IC  Flags   Details
   #0      Smartcard       present     1   A
   #1      Software Tkn    -           0
   #2      Smartcard       -           0   AD
   #3      Smartcard       -           0   AD
   ```

3.5.4. Map dynamic slots to slot #0

You must have a working initialized Security World before you can map slots to Slot #0. Some APIs require that all tokens be loaded to Slot #0, for example, PKCS#11.

To map a dynamic slot to slot 0 from the front panel of an nShield Connect:

1. From the menu navigate to **Security World mgmt [3] > Set up dynamic slots [3-9] > Slot mapping** and set the required dynamic slot to exchange for slot 0.
2. Clear the HSM after initiating the change.
3. If you want to set slot mapping using the nShield Connect configuration file, make sure that you have enabled **Allow autopush** for the nShield Connect.

4. Navigate to the nShield Connect configuration file `%NFAST_KMDATA%\HSM-ESN` (for example, `C:\ProgramData\nCipher\Key Management Data\hsm-HSM-ESN\config\config`) and open it using your preferred test editor. Look for:

```
[slot_mapping]
# Start of the slot_mapping section
# Slot remapping configuration.
# Each entry has the following fields:
#
# ESN of the module on which slot 0 will be remapped with another.
# esn=ESN
#
# Slot to exchange with slot 0. Setting this value to 0 means do
# nothing.(default=0)
# slot=INT
```

5. Uncomment the **esn** and **slot** entries and enter the relevant nShield HSM ESN and the number of the slot you want to mark as slot #0 (for example, 2).
6. Save the file as `config.new`.
7. Push the `config.new` file to the nShield HSM using the following command:

```
cfg-pushnethsm.exe -a Connect_IP_address full_path_to_the_config.new_file
```

8. Execute the `nopclearfail -c -mx` command, where *x* is the number of the nShield HSM.

3.5.5. Change the timeout limits for dynamic slots

To change the timeout limit for round trip network delays or card removal, set the `round_trip_time_limit` or `card_remove_detect_time_limit` fields in the `dynamic_slot_timeouts` section of the configuration file:

```
[dynamic_slot_timeouts]
# Start of the dynamic_slot_timeouts section
# Timeout values used to specify expected smartcard responsiveness for all
# modules on the network.
# Each entry has the following fields:
#
# Round trip time limit, in seconds, is how long to wait before giving up due
# to network delays. (default=10)
# round_trip_time_limit=INT
#
# Maximum time, in seconds, that can pass without a response from the
# smartcard before considering it removed and unloading all associated secrets
# (default=30)
# card_remove_detect_time_limit=INT
```

4. Install the Remote Administration Client (RAC) software

If you are installing Security World Software, the RAC software is installed with it on the machine. The instructions in this chapter only apply to installations from the **Remote Administration Client (RAC)** ISO.

4.1. Prerequisites

The following steps should have been completed by the appropriate member of staff in your organization:

In the HSM environment:

- The Remote Administration Service has been installed and configured on the appropriate computer or computers, see Server-side preparation tasks.
- The firewall of the computer where the Remote Administration Service is installed has been configured to allow traffic to and from the nShield Remote Administration Client, see Server-side preparation tasks.
- Dynamic slots have been configured in the relevant hardserver configuration file, see Setting dynamic slots.

On the machine on which RAC will be installed:

- Ensure that you have installed the latest security updates or patches in accordance with the policies and procedures of your organization.
  - Information about Microsoft security updates is available from http://www.microsoft.com/security/.
  - On Linux, ensure that `libpng12` is available. This package is not installed by default on all distributions. For information on Linux in general, see the documentation supplied with your operating environment.
  - For information on macOS, see the documentation supplied with your operating environment.
- If you have another nShield product or an earlier version of the RAC on the computer, you should uninstall it. Failure to do so may result in impaired functionality of the RAC.

4.2. Install RAC on Windows

1. Sign in to Windows as an administrator or as a user with local administrator rights.
2. Mount the ISO.

   If the installation wizard does not start automatically, navigate to `setup.msi` on the installation media and click it to manually start the installation.

3. Click **Next** to display the **License Agreement** page. Read the End User License Agreement (EULA).

   If you accept the terms and conditions, select the check box and click **Next**.

   Click **Print** if you need a printed copy of the agreement.

4. If required, click **Change** to change the **Destination Folder**.

   Click **Next** to display the **Product Features** page, with both Remote Administration Client and Trusted Verification Device driver selected by default.

5. Click **Install** to start the installation.

   The **nShield Remote Administration Client Tools Setup** page displays, with a progress bar.

6. When the installation has completed, click **Finish**.

The program is added to the Windows start menu: **Start > Entrust nShield Security World > Remote Administration Client**.

4.3. Install RAC on Linux

1. Sign in as a user with root privileges.
2. Mount the ISO.
3. Open a terminal window, and change to the root directory.
4. Extract the `rac.tar.gz` file to install the software bundle by running the following command:

   ```
   tar xzvf <disc-name>/lin64/amd64/rac.tar.gz
   ```

   `<disc-name>` is the name of the mount point of the installation media.

5. If you have not used the TVD on your computer previously, you might need to install one of the following drivers from the `<ISO>/tvd/linux` directory on the install media, depending on your distribution:
    - `pcsc-cyberjack-3.99.5final.SP07-1.suse11.4.x86_64.rpm`
    - `pcsc-cyberjack-3.99.5final.SP07-1.suse12.3.x86_64.rpm`
    - `pcsc-cyberjack-3.99.5final.SP09-1.centos6.7.x86_64.rpm`
    - `pcsc-cyberjack-3.99.5final.SP09-1.centos7.1.1503.x86_64.rpm`

4.4. Install RAC on macOS

1. Sign in to macOS as a user with Administration rights.
2. Load the Remote Administration Client software installation media or download the ISO onto your computer.
3. Locate the disk image file `RemoteAdminClient.dmg` and open it in a new window.
4. In the new window, drag the **RemoteAdminClient** icon to the **Applications** folder. Wait for the copy process to finish.
5. If you have not used the TVD on your computer previously, you might need to install the relevant driver from the `<ISO>/tvd/mac` directory on the install media.

The Remote Administration client will be available in **Applications** and will show in the **Launchpad** as a shortcut. It can also be dragged to the Dock for easier access.

5. Use the Remote Administration Client (RAC) software

This chapter describes how the Remote Administration Client can be used to participate in a quorum remotely.

- Example: load a Security World with quorum members presenting their cards via RACs gives an example of the server-side user experience. This is for the user who will connect to the Remote Administration Service and execute the administration task for which the quorum is required. This user needs the RAC client and a TVD on their local machines, but must also be able to connect to the Remote Administration Server via a secure connection.
- Use the RAC GUI to create an association with a dynamic slot and Use the raccmd command-line utility to create an association with a dynamic slot describe how to join a quorum remotely. These options are for the quorum members who are authorizing the task but are not executing it. They only need the RAC client and the TVD.

5.1. Requirements

For all quorum members:

- Remote screen sharing tools such as WebEx, VNC or RDP. Should be able to pass RDP session to each Smartcard holder in turn and make the presenter.
- IPv6 link-local address with the interface, IPv6 address, IPv4 address or hostname to the Remote Administration Service.
- Port number or numbers at which the Remote Administration Service accepts calls from Remote Administration Clients.

For the quorum member who will execute the HSM administration task:

- Tool to connect from the local machine to the Remote Administration Service.

5.2. Use the RAC GUI to create an association with a dynamic slot

The wizard-based GUI consists of a series of dialogs that enable you to associate a TVD with the appropriate HSM using one of its Dynamic Slots.

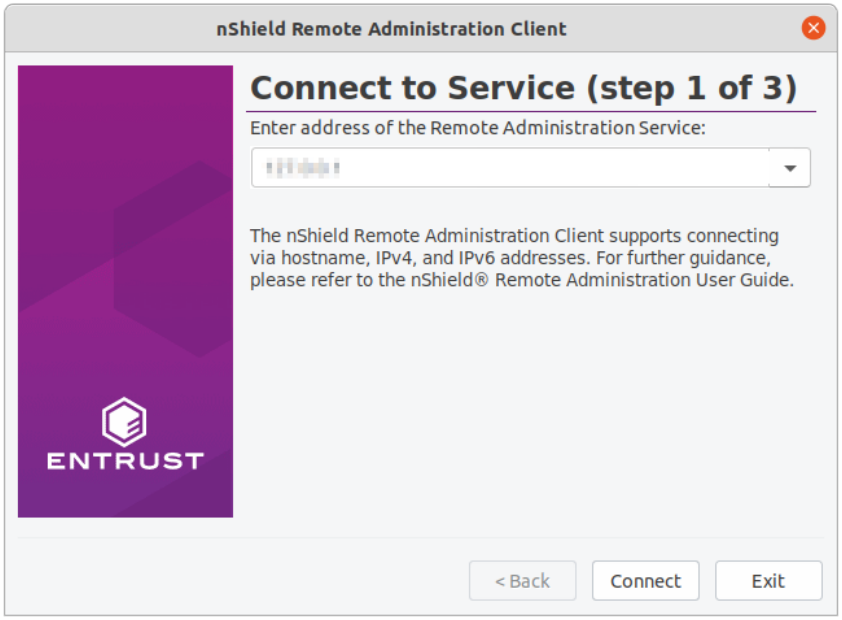
When you are using the GUI, keep in mind the following:

- If you click **Exit**, or close the RAC GUI at any time, you must restart the nShield Remote Administration Client and repeat all steps.
- If you click **Back** on the **Use Card Reader** page, the slot on the HSM will be released for use by another card reader.
- If the network connection is lost, an error message displays.
- If you disconnect the TVD while using the nShield Remote Administration Client, an error message displays and you are returned to the **Select Card Reader (step 3 of 3)** page to select a new reader.
- **Windows 8.1+ only**

  If you disconnect the TVD while you are on the **Use Card Reader** screen, the Windows Smart Card service `SCardSvr` displays an error and terminates.

1. Launch the remote screen sharing tool that will be used between the quorum members.
2. Start the RAC:
   - On **Windows**, double-click the **Remote Administration Client** icon.
   - On **Linux**:
     - Make sure the `pcscd` service is running.
     - Navigate to `/opt/nfast/bin/racgui`, or the appropriate installation directory.
   - On macOS, open the Launchpad and click the **RemoteAdminClient** icon.

   The **Connect to Service (step 1 of 3)** wizard page displays.



3. Enter the IP address or hostname of the required Remote Administration Service, or select the appropriate entry in the drop-down list that stores the last 10 connections that have been used. Examples of supported IP address types are:
    - IPv4 address: *194.3.4.106*
    - IPv6 address: *2001:db8::2:1*
    - Link-local IPv6 address with interface name: *fe80::1%eth0*
    - Link-local IPv6 address with interface number: *fe80::1%2*

    If the communication port has been changed from the default 9005, you can also enter the correct number here, separated by a colon. For example, *Hostname:Port*, *192.0.2.146:9006*.

    Please note you need square brackets to distinguish between IPv6 and its port. For example:

    - IPv6 address: *[2001:db8::2:1]:9006*
    - Link-local IPv6 with interface name: *[fe80::1%eth0]:9006*
    - Link-local IPv6 with interface number: *[fe80::1%2]:9006*

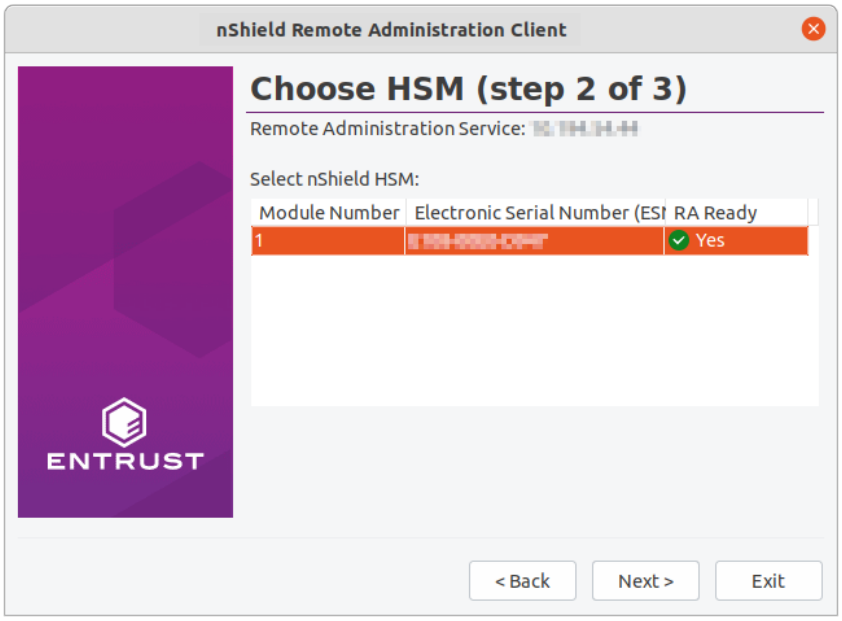
    Square brackets are not required but are permitted for IPv4 addresses and hostnames.

4. Click **Connect** to connect with the Remote Administration Service.

    An error message displays if a connection cannot be established with the IP address or hostname. You can retry or connect to a different Remote Administration Service.

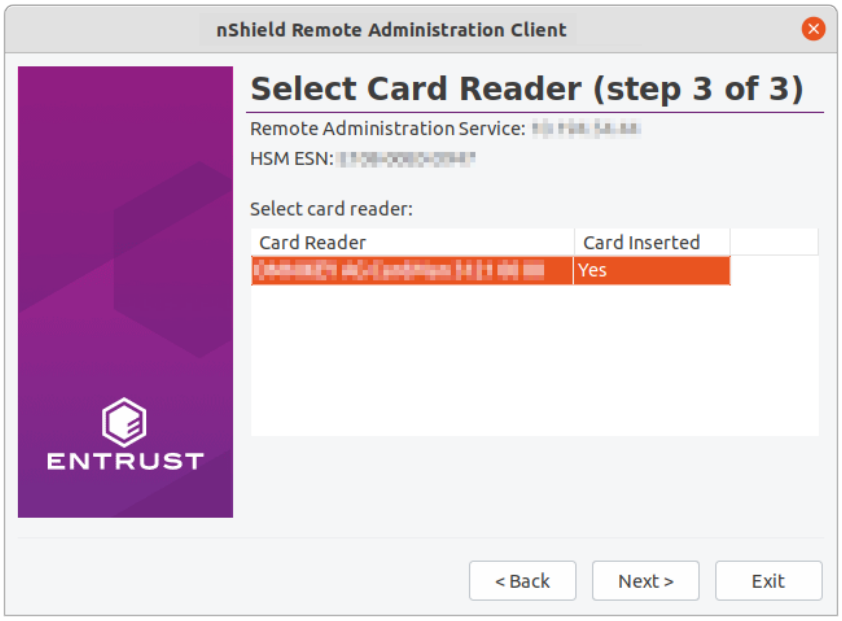
    Depending upon your network environment, there may be a short delay in establishing a connection.

5. On the **Choose HSM (step 2 of 3)** wizard page, select the appropriate HSM from the list, according to its ESN, and click **Next**.



HSMs that do not support Dynamic Slots because they do not have the appropriate firmware, or do not have any dynamic slots configured, cannot be selected. However, they still appear in the list.

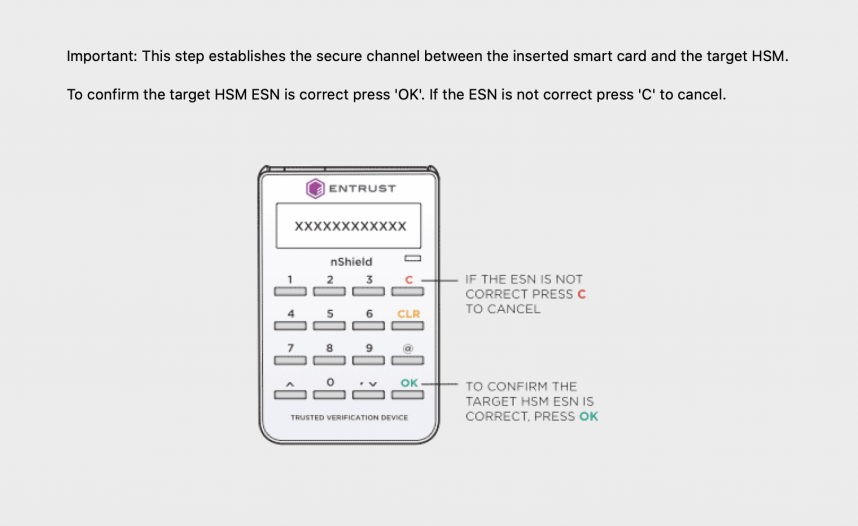
6. Ensure that an nShield Trusted Verification Device is connected to your local computer. The tool shows that no Smartcard have been inserted yet in nShield TVD:



Select the **Card Reader**, insert the Smartcard in the nShield TVD slot, and click **Next**.

You can connect the Trusted Verification Device after the nShield Remote Administration Client has been started. But you must connect it either before you reach the **Select Card Reader (step 3 of 3)** page, or while it is still being displayed, to be able to proceed.

7. Check the displayed ESN against an independent record of the expected ESN.



Do **not** just check the ESN against the one displayed on the last wizard page of the GUI.

- If the ESN is correct, press **OK** on the nShield Trusted Verification Device to confirm. The screen of the device displays **Accepted**.
- If there is a problem with the ESN, press **C** on the nShield Trusted Verification Device. The screen of the device displays **Abort OK?**. Press **OK**. The **Card Status** field on the **Use Card Reader** page displays **Unknown card**.
- If you have selected the wrong HSM, return to the Choose HSM (step 2 of 3) page and select the correct one. Otherwise, proceed according to the security policies of your organization.

If you remove and reinsert the card after you have confirmed the ESN of the HSM, the secure channel connection window re-displays. Select the HSM by its ESN again.

8. The **Use Card Reader** dialog is displayed with information about the Remote Administration:

Remote Administration Service	*<ip-address>* of the Remote Administration server
HSM ESN	*<hsm-esn>*
Slot Number	Number of the dynamic slot used by the card
Card Inserted	**Yes** when the card is inserted in the TVD
Card Serial Number	*<serial-number>* of the Smartcard

The Remote Administration connection is now set up. All remote users will have to enter there passphrases as and when they are instructed to do so.

Do not exit or close the **Use Card Reader** dialog until you want to terminate the session.

5.3. Use the raccmd command-line utility to create an association with a dynamic slot

The `raccmd` command line utility is available on the machine on which the Remote Administration Client was installed. It enables you to:

- List all available HSMs and select the appropriate one
- List all locally available TVDs
- Associate a TVD with an HSM, if a Dynamic Slot is available

You can also script the card presentation process using `raccmd`.

Run the following command:

```
raccmd [-h] [--address ADDRESS] [--port PORT] [-v] [--version] {listhsms,listreaders,associate} ...
```

On macOS, you need to explicitly specify the path to the command-line utility:

```
/Applications/RemoteAdminClient.app/Contents/Resources/raccmd [-h] [--address ADDRESS] [--port PORT] [-v] [--
version]
    {listhsms,listreaders,associate} ...
```

If the Remote Administration Client application has been installed for only the current user, then use **~/Applications/...**.

5.3.1. Example to connect to an HSM using raccmd

1. At the command prompt, execute the `listreaders` and `listhsms` commands to check or confirm the information you will need for parameters of the `raccmd` command.

```
c:\Program Files\nCipher\nfast\bin>raccmd.exe listreaders
1. name_of_TVD
2. name_of_another_card_reader_attached_to_machine
c:\Program Files\nCipher\nfast\bin>raccmd.exe --address Remote_Admin_Service_IP_Address listhsms
1. esn_number
```

   In this example, the TVD is listed as the first reader so the value of TVD_ID will be 1 for the `raccmd` command.

2. Connect to the HSM:

```
c:\Program Files\nCipher\nfast\bin>raccmd.exe --address Remote_Admin_Service_IP_Address associate -
interactive esn_number TVD_ID
Associated with slot 2
Reading...
Confirm HSM ESN on TVD
smartcard_ID
```

5.3.2. Options

The following options are available:

Option	Description
`-h|--help`	Show this help message and exit
`--address ADDRESS`	Address of the Remote Administration Service
`--port PORT`	Port of the Remote Administration Service
`-v|--verbose`	Increase the verbosity of the output
`--version`	Print the version number of the nShield Remote Administration Client utility

5.3.3. Arguments

You should only use one argument at a time.

Argument	Meaning
`listhsms`	List HSMs attached to a Remote Administration Service.

Argument	Meaning
`listreaders`	List readers connected to your computer.
`associate`	Associate an nShield Trusted Verification Device connected to your computer with an HSM, identified by its ESN. One of the Dynamic Slots belonging to the HSM is used for the duration of the session, when the HSM is associated with a device.

5.3.4. The associate argument

When the `associate` argument is used, further command-line options and arguments are available.

5.3.4.1. Usage

```
raccmd associate [-h] [-i] [-r] [-f ASSOC_FILE] ESN READER
```

5.3.4.2. Options

The following options are available:

Option	Description
`-h|--help`	Show this help message and exit
`-i|--interactive`	Run with interactive output
`-r|--until-removal`	Exit on first card removal
`-f ASSOC_FILE|--assoc-file ASSOC_FILE`	Create this file containing the associated slot, and exit when it is deleted

5.3.4.3. Arguments

Argument	Meaning
`ESN`	ESN of the HSM to use.
`READER`	Number of the local reader to use. Use `listreaders` to display the reader numbers.

5.4. Example: load a Security World with quorum members presenting their cards via RACs

1. All quorum members connect through a remote screen sharing tool.
2. One quorum member connects to the Remote Administration Service, for example with ssh.
3. All quorum members who need to present their cards remotely launch their Remote Administration Client and connect to the Remote Administration Service. See:
   - Use the RAC GUI to create an association with a dynamic slot.
   - Use the raccmd command-line utility to create an association with a dynamic slot.
4. The quorum member who is connected via ssh can confirm with the `slotinfo` command that dynamic slots have been configured so that other quorum members can present their cards remotely:

   Linux:

   ```
   #/opt/nfast/bin/slotinfo -m2
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>slotinfo.exe -m2
   ```

   The following example is an output that shows a card present in the physical slot (Slot #0) of the HSM and a card presented via the Remote Administration client in a dynamic slot (here identified as Slot #2 with Flags ADa where D is dynamic).

   ```
   Module 2:
   Slot    Type            Token       IC  Flags   Details
   #0      Smartcard       present     1   A
   #1      Software Tkn    -           0
   #2      Smartcard       present     5   ADa
   #3      Smartcard       -           0   AD
   ```

5. The quorum member who is connected via ssh changes the HSM mode to Initialization remotely using the `nopclearfail` command:

   Linux:

   ```
   #/opt/nfast/bin/nopclearfail --initialization -m2
   Module 2 command ClearUnitEx: OK
   ```

Windows:

```
C:\Program Files\nCipher\nfast\bin>nopclearfail.exe --initialization -m2 Module 2, command ClearUnitEx: OK
```

6. The quorum member who is connected via ssh executes the `new-world` command.

   Linux:

   ```
   #/opt/nfast/bin/new-world -l -m2
   ```

   Windows:

   ```
   C:\Program Files\nCipher\nfast\bin>new-world.exe -l -m2
   ```

7. The following message will be displayed:

   ```
   18:16:43 WARNING: Module #2: preemptively erasing module to see its slots!
   Indoctrinating Module:
   Module 2: 0 cards of 2 read
   Module 2 slot 0: empty
   Module 2 slot 2: empty
   Module 2 slot 3: empty
   Module 2 slot 2: Admin Card #3
   ```

8. Each quorum member is now prompted to present their card. Members who are connected through RAC are prompted to use insert the Smartcard in the nShield TVD when the RAC **Use Card Reader** window appears.
9. The quorum member connected via ssh can monitor the status of the remote cards in the messages:

   ```
   Module 2 slot 2:- passphrase supplied - reading card
   Module 2: 1 card of 2 read
   Module 2 slot 2: Admin Card #3: already read
   Module 2 slot 2: empty
   Module 2 slot 2: Admin Card #4
   Module 2 slot 2:- passphrase supplied - reading card
   Card reading complete.
   security world loaded on 1 module; hknso = 78abcd62770e79eba69f556c4b596b9ed1d59e87
   ```

10. When all cards were read, the HSM can be changed back to **Operational** mode with the `nopclearfail` command:

    Linux:

    ```
    #/opt/nfast/bin/nopclearfail --operational -m2 Module 2 command ClearUnitEx: OK
    ```

Windows:

```
C:\Program Files\nCipher\nfast\bin>nopclearfail.exe --operational -m2 Module 2, command ClearUnitEx: OK
```

11. The mode of the HSM can be confirmed with the `enquiry` command on the ssh prompt:

    Linux:

    ```
    #/opt/nfast/bin/enquiry
    ```

    Windows:

    ```
    C:\Program Files\nCipher\nfast\bin>enquiry
    ```

    The Module#2 part of the configuration file is shown below:

    ```
    Module #2:
    enquiry reply flags none
    enquiry reply level Six
    serial number 49D5-C944-F159
    mode operational
    .....
    ```

12. The remote task has been completed. Remote quorum members can disconnect their Remote Administration Clients and the ssh connection can be closed.

6. Troubleshooting

This appendix describes what you should do if you experience problems with the nShield Remote Administration Client.

If you encounter any errors that are not listed in the following table, contact Support.

Error	Explanation	Action
When attempting to connect with the Remote Administration Service, a **Failed to communicate with the Remote Administration Service**, error message displays.	The IP address or Hostname of the Remote Administration Service is invalid or a firewall between the nShield Remote Administration Client and the Remote Administration Service may be blocking access.	Ask your system administrator to check the firewall and network settings of the computer hosting the Remote Administration Service.
Under Windows, network connections are lost and the nShield Remote Administration Client closes unexpectedly.	The Windows power saving options may have put your computer to sleep.	Disable power saving modes on your computer if you need to present a card for an extended period of time.
The nShield Remote Administration Client GUI or command line utility has difficulty reading a genuine nShield Remote Administration Card.	A smartcard or authentication token process or service, for example associated with your VPN, may be preventing the client from accessing the card.	If it is not essential, stop or disable the conflicting process or service (for example using the Windows Services administrative tool). Contact your system administrator for advice concerning essential processes and services.
A network error message displays.	The network connection has been lost.	Try to connect again, otherwise, contact your system administrator.

7. Uninstall the Remote Administration Client (RAC) software

Uninstall the RAC software before installing other nShield software, for example before installing Security World software or a newer version of RAC.

7.1. Uninstall RAC on Windows

1. Sign in to Windows as a user who has rights to install and uninstall software on the machine.
2. Remove the **Remote Administration Client** and **CyberJack Base Components** via **Control Panel > Programs and Features** (depending on your version of Windows).

The Remote Administration Client program is removed from the Windows **Start Menu**.

7.2. Uninstall RAC on Linux

1. Sign in as a user with root privileges.
2. Ensure that the `/opt/nfast` directory does not contain any files other than those belonging to the nShield Remote Administration Client.
3. Remove the `/opt/nfast` directory.

7.3. Uninstall RAC on macOS

1. Sign in to macOS as a user with Administration rights.
2. Move the executable of the nShield Remote Administration Client into the **Trash/Bin**.

The Remote Administration client will be removed from **Applications** and the **Launchpad**.