



ENTRUST

nShield Security World

nShield Remote Administration Client v12.50.4 User Guide

4 March 2024

Contents

1 Introduction	5
1.1 About this guide	5
1.2 Additional documentation	5
1.2.1 Typographical conventions	5
1.2.2 CLI command conventions	6
2 nShield Remote Administration Client introduction	7
2.1 nShield Remote Administration Client overview	7
2.1.1 Remote Administration Service	8
2.1.2 Cards	8
2.1.3 The nShield Trusted Verification Device	9
2.1.4 nShield HSM administration through your standard remote access solution	9
2.1.5 Communication with an nShield HSM	10
3 Before you install the software	12
3.1 Assumptions	12
3.2 Windows environments	12
3.2.1 Install Microsoft security updates	12
3.3 Unix Environments	12
3.3.1 Install operating environment patches	12
4 Installing the software	13
4.1 Installing the software	13
4.2 Installing the nShield Remote Administration Client software under Windows	14
4.3 Installing the nShield Remote Administration Client software under Linux	15
4.4 Installing the nShield Remote Administration Client software under OS X	16
5 Using the nShield Remote Administration Client GUI	18
5.1 nShield Remote Administration Client GUI	18
5.2 Using the nShield Remote Administration Client GUI	18
5.2.1 Confirming the HSM ESN using the nShield Trusted Verification Device	20

5.2.2 Entering Pass Phrases using your remote access solution	21
5.3 nShield Remote Administration Client command-line utility	21
5.3.1 Using the raccmd command-line utility	21
5.3.2 Options	22
5.3.3 Arguments	22
5.3.4 The associate argument	23
5.3.4.1 Usage	23
5.3.4.2 Options	23
5.3.4.3 Arguments	23
Appendix A Troubleshooting	24
Glossary	25
Authorized Card List	25
Dynamic Slot	25
nShield Remote Administration Card	25
nShield Remote Administration Client	25
nShield Trusted Verification Device	25
Remote access solution	25
Remote Administration	25
Remote Administration Service	26
Standard card reader	26
Standard nShield Cards	26

1 Introduction

This chapter describes the content of this guide, where you can access other documentation, and any typographical conventions about which you should be aware.

1.1 About this guide

This guide includes:

- An introduction to the nShield® Remote Administration Client. See *nShield Remote Administration Client introduction* on page 7.
- Information about what you need to do before installing the software. See *Before you install the software* on page 12.
- Software installation instructions. See *Installing the software* on page 13.
- Details of how to use the software. See *Using the nShield Remote Administration Client GUI* on page 18.
- Troubleshooting steps. See *Troubleshooting* on page 24.

1.2 Additional documentation

We strongly recommend that you read the release notes in the `re1ease` directory of your installation media before you use the software. These notes contain the latest information about your product.

For information about using other nShield software and devices, see the documentation on the installation media that was provided with the product.

For information on integrating nCipher products with third-party enterprise applications, see <https://www.ncipher.com>.

1.2.1 Typographical conventions



This symbol indicates important supplemental information.



This symbol is used to indicate if there is a danger of loss or exposure of key material (or any other security risk).



If there is a danger of damage to the hardware, this is indicated by a caution triangle in the margin. If you see this symbol on the product itself, see the *nShield Solo Installation Guide*.



Si une détérioration du matériel est possible, un triangle d'avertissement l'indique dans la marge. Si ce symbole apparaît sur le produit lui-même, reportez-vous à la partie correspondante du *nShield Solo Installation Guide*.



Besteht die Gefahr eines Hardware-Schadens, wird dies am Rand durch ein Warndreieck angezeigt. Falls Sie dieses Symbol auf dem Produkt selbst bemerken, schlagen Sie im zutreffenden Abschnitt des Installationshandbuchs (*nShield Solo Installation Guide*) nach.

Keyboard keys that you must press are represented like this: `Enter`, `Ctrl-C`.

Examples of onscreen text from graphical user interfaces are represented by **boldface** text. Names of files, command-line utilities, and other system items are represented in **monospace** text. Variable text that you either see onscreen or that you must enter is represented in *italic*.

Examples of onscreen terminal display, both of data returned and of your input, are represented in a form similar to the following:

```
install
```

1.2.2 CLI command conventions

The basic syntax for a CLI command is:

```
command object <object_name> [parameter] [option] [modifier]
```

In this syntax, user-defined values are shown in *italics* and enclosed within the `< >` characters. Optional elements are shown enclosed within the `[]` characters. Mutually exclusive elements are separated by the `|` character.

Many system objects require the inclusion of a user-defined keyword value. For example, the `user` object is executed against a user-supplied *user_name*. Throughout this guide, all user-defined keyword values are shown in *italics*.

Each CLI command that you run performs an operation against the internal configuration of the appliance. The specific type of operation is specified by the first user-defined keyword value in the command string.


2 nShield Remote Administration Client introduction

This chapter describes the nShield Remote Administration Client software and the environment in which it operates.

2.1 nShield Remote Administration Client overview

The nShield Remote Administration Client, which resides on your local Windows, Linux-based or OS X computer, 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:
 - An nShield Trusted Verification Device
nCipher recommends that you only use an nShield Trusted Verification Device.
 - or:
 - 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 remainder of this guide assumes that you are using an nShield Trusted Verification Device. The use of a standard card reader is not covered any further.

The secure connection between a 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
- Select an HSM from a list of all HSMs available through the chosen Remote Administration Service
- Select an nShield Trusted Verification Device

Your local nShield Trusted Verification Device is now associated with the HSM for the duration of the current GUI or command-line session. This means, for example, that:

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

The nShield Remote Administration Client also displays the status of locally attached nShield Trusted Verification Devices.

See:

- [Remote Administration Service on page 8](#) for a description of the Remote Administration Service
- [Cards on page 8](#) for an overview of cards
- [The nShield Trusted Verification Device on page 9](#) for an overview of this device
- [Communication with an nShield HSM on page 10](#) for an example of the communications path
- [nShield HSM administration through your standard remote access solution on page 9](#) for a brief description of managing an nShield HSM in conjunction with the nShield Remote Administration Client.

2.1.1 Remote Administration Service

The Remote Administration Service runs alongside the appropriate hardserver, which is a nCipher-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 nShield Trusted Verification Device 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 upon the hardserver configuration, the Remote Administration Service can associate up to 16 Trusted Verification Devices with each HSM. The default number of devices that can be associated with an HSM is zero.

2.1.2 Cards



The nShield Remote Administration Client only supports nCipher supplied nShield Remote Administration Cards, inserted in an nShield Trusted Verification Device that is connected to the computer where the client is installed. Standard nShield cards are not supported.

nShield Remote Administration Cards are compliant with FIPS140-2 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 the *User Guide* for your HSM for more information about the Authorized Card List.

2.1.3 The nShield Trusted Verification Device

The nCipher nShield Trusted Verification Device 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.

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

Multiple Trusted Verification Devices 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 Trusted Verification Device with a specific HSM. They are configured by the person responsible for setting up your nShield HSM environment.

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

2.1.4 nShield HSM administration through your standard remote access solution

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 their cards are required.



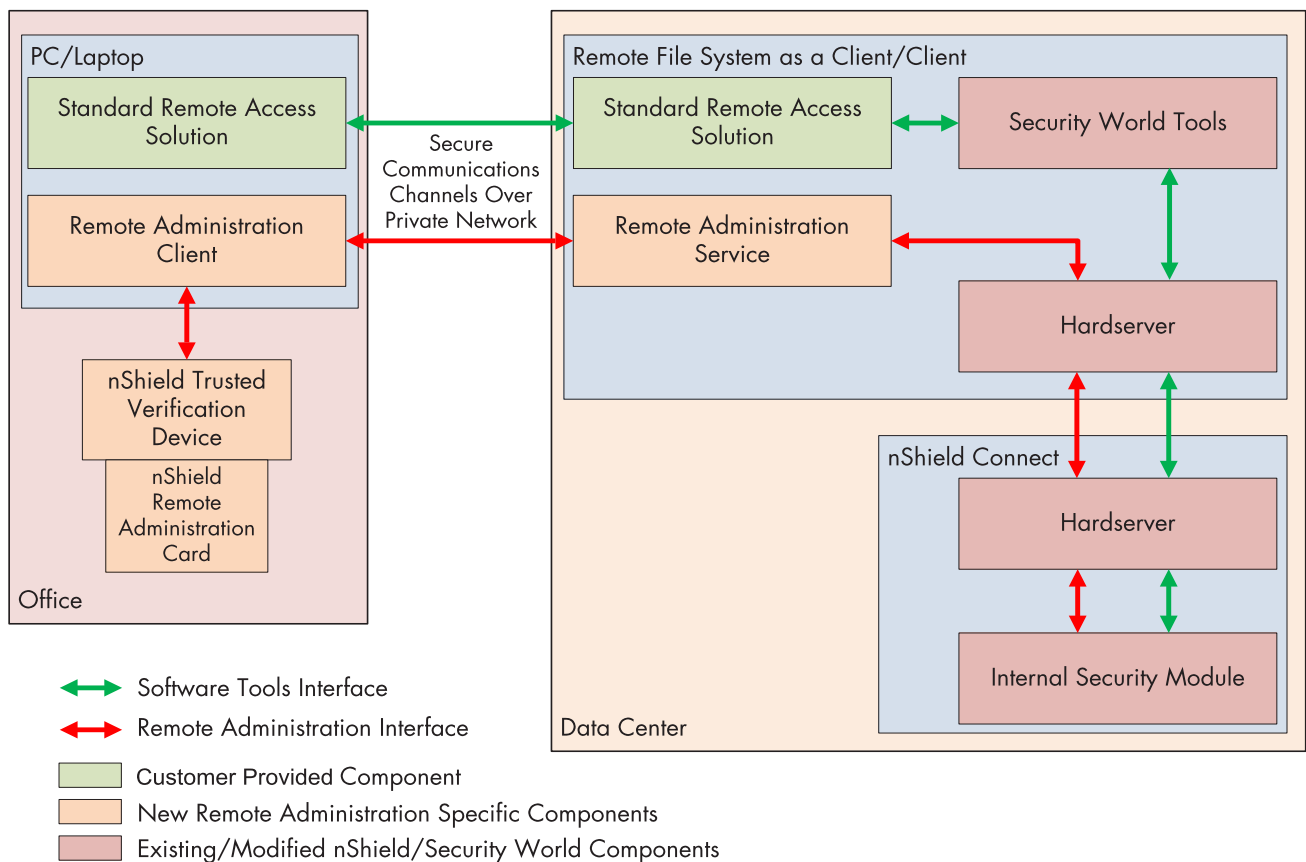
Your remote access solution does not have to be installed on the same computer as the Remote Administration Client software. However, if, for example, you are using your remote access solution in one location, you need to be able to communicate with card holders who are using the Remote Administration Client elsewhere, to tell them when to insert cards in their Trusted Verification Device, verify the ESN of the appropriate HSM, and so on.

Using the remote access solution of your organization means that:

- Pass phrases, for example, are entered using Security World software via your remote access solution.
- An nShield Remote Administration Card is inserted in the appropriate Trusted Verification Device as and when the Security World software instructs you to do so.

2.1.5 Communication with an nShield HSM

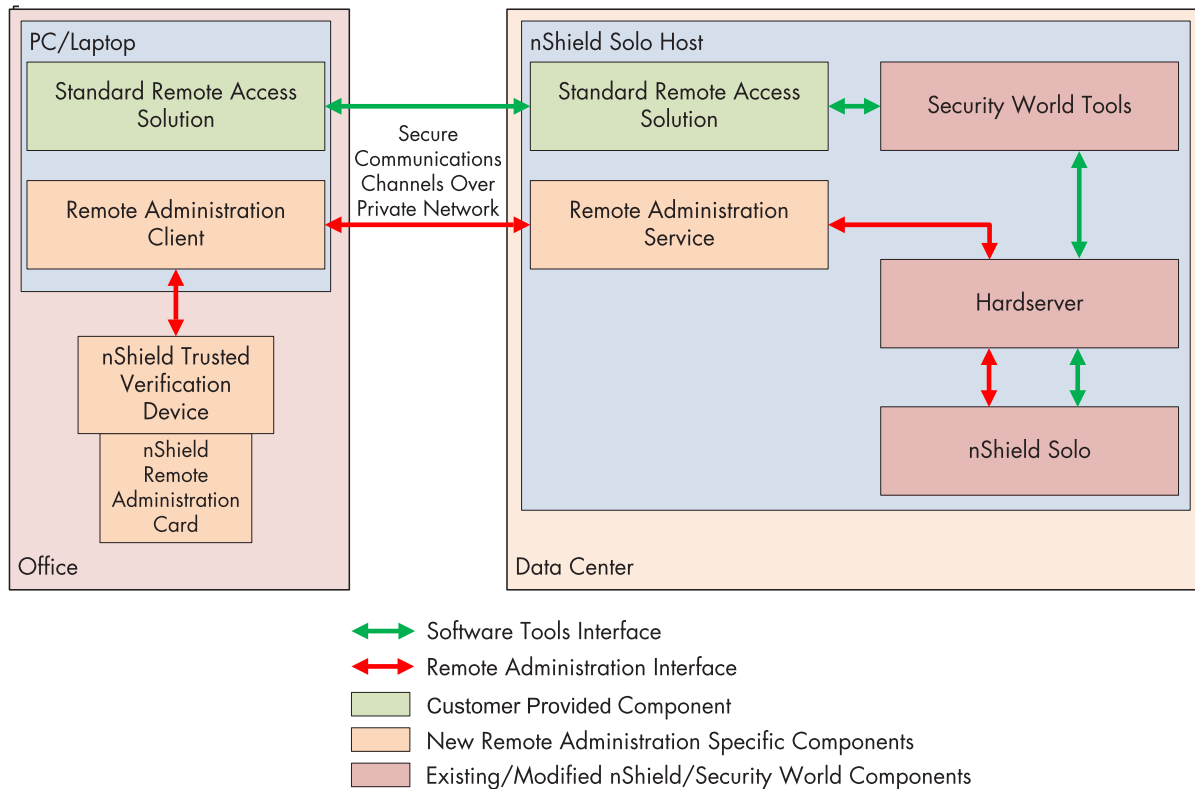
Figure 1. Example of communications between an nShield Remote Administration Card and an nShield Connect



The example in [Figure 1](#) shows an nShield Connect communicating with an nShield Remote Administration Card through the hardserver of the relevant HSM, the hardserver of the client (which may also be the Remote File System), the Remote Administration Service, and the nShield Remote Administration Client.

The remote access solution can reside on different computers to the Remote Administration Client/Service.

Figure 2. Example of communications between an nShield Remote Administration Card and an nShield Solo



The example in [Figure 2](#) shows the nShield Solo communicating with an nShield Remote Administration Card through the hardserver, the Remote Administration Service, and the nShield Remote Administration Client.

3 Before you install the software

This chapter describes the steps you need to take before installing the software.

3.1 Assumptions

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

- The Remote Administration Service has been installed and configured on the appropriate computer/s
- HSM Dynamic Slots have been configured in the relevant hardserver configuration file, see *Configuring Remote Administration* in the *User Guide* for your nShield HSM
- 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 *Firewall settings* in the *Installation Guide* for your nShield HSM.

3.2 Windows environments

3.2.1 Install Microsoft security updates

Ensure that you have installed the latest Microsoft security updates, in accordance with the policies and procedures of your organization. Information about Microsoft security updates is available from <http://www.microsoft.com/security/>.

3.3 Unix Environments

3.3.1 Install operating environment patches

Ensure that you have installed the latest recommended patches. See the documentation supplied with your operating environment for information.

4 Installing the software

This chapter describes the steps you need to take to install the nShield Remote Administration Client software and the nShield Trusted Verification Device.

4.1 Installing the software

The software can be installed under Windows, Linux and OS X. See the *Release Notes* on the installation media for more about supported operating systems.

Once you have completed the pre-installation tasks described in *Before you install the software on page 12*, you are ready to Install the nShield Remote Administration Client software, as described in this chapter.

Follow the instructions in *Installing the nShield Remote Administration Client software under Windows on page 14* or *Installing the nShield Remote Administration Client software under Linux on page 15* or *Installing the nShield Remote Administration Client software under OS X on page 16*, according to your operating system

4.2 Installing the nShield Remote Administration Client software under Windows

Do the following:

1. Log on to Windows as an administrator or as a user with local administrator rights.
2. Place the nShield Remote Administration Client software installation media in your optical disc drive.

The **Remote Administration Client Tools Setup** wizard displays.

If the installation wizard does not start automatically, navigate to **setup.exe** on the installation media and double-click it to manually start the installation.

3. Click **Next >** to display the **License Agreement** page. Read the End User License Agreement (EULA) and, if you accept the terms and conditions, click **Yes** to continue.
Click **Print** if you need a printed copy of the agreement.
4. The **Select Features** page displays, with both Remote Administration Client and Trusted Verification Device driver selected by default.

Click **Browse...** to change the **Destination Folder**, if required.

Click **Disk Space...** to display the **Available Disk Space** window and check the space available on any other drives you may have.

5. Click **Next >** to start the installation.

The **Setup Status** page displays, with a progress bar.

6. When the **Wizard Complete** page displays, click **Finish** to complete the installation.

The Remote Administration Client icon is added to your desktop (*Figure 3. The Windows Remote Administration Client desktop icon on page 14*).

Figure 3. The Windows Remote Administration Client desktop icon



4.3 Installing the nShield Remote Administration Client software under Linux

Do the following:

1. Log in as a user with root privileges.
2. Place **Remote Administration Client Tools** software installation media in your optical disc drive and mount the drive.
3. Open a terminal window, and change to the root directory.
4. Extract the **agg.tar** file to install the software bundle by running the following command:

```
tar xf disc-name/linux/ver/ract/ratls/agg.tar
```

disc-name is the name of the mount point of the installation media.

ver is the version of the operating system:

- **libc6_11**: 32 bit Linux
- **libc6_11/amd64**: 64 bit Linux.

4.4 Installing the nShield Remote Administration Client software under OS X

Do the following:

1. Log onto OS X as a user with Administration rights.
2. Locate the RaInstaller.pkg file on the Remote Administration Client Tools software installation media and double click on this file in the Finder to start the installer.
3. Click **Continue** to proceed to the License Agreement page. Read the End User License Agreement (EULA) and if you accept the terms and conditions, click **Continue** to proceed. A pop-up dialog will appear where you need to click **Agree** to continue with the installation.
4. The **Select Features** page displays, with both Remote Administration Client and Trusted Verification Device (TVD) driver selected by default. Select which components you want to install and click **Continue** to proceed with the installation.
5. The **Installation Type** page displays . You can change the destination of the installation by clicking the **Change Install Location...** button. You can choose to install for all users of the computer (in /Applications), for the current user only (in ~/Applications) or install on a specific disc. You need to select one of the choices before clicking **Continue** to return to the **Installation Type** page. In certain circumstances the **Destination Select** page may appear directly as the user proceeds through the wizard.
6. Click **Install** to start the installation.
7. If you opted to install the TVD driver you will be prompted that the machine will need restarting. Click **Continue Installation**.
8. You will be prompted for your password to install new software. Enter your password and click **Install Software**.
9. The Summary page will appear. If you opted to install the TVD driver click **Restart**, otherwise click **Close**.
10. The Remote Administration client will be available in *Applications* and will show in the Launchpad (*Figure 4. The OS X Remote Administration Client desktop icon on page 17*). It can also be dragged to the Dock for easier access.

Figure 4. The OS X Remote Administration Client desktop icon



5 Using the nShield Remote Administration Client GUI

This chapter describes how to use the nShield Remote Administration Client software.

There are two interface options:

- A wizard-based GUI
- A command-line utility

5.1 nShield Remote Administration Client GUI

The wizard-based GUI consists of a series of dialogs that enable you to:

- Select a Remote Administration Service
- List all available HSMs and select the appropriate one
- Select an nShield Trusted Verification Device

Once you have completed these steps, the selected Trusted Verification Device is associated with the appropriate HSM using one of its Dynamic Slots.

5.2 Using the nShield Remote Administration Client GUI

Do the following:


1. Start the Remote Administration Client by doing one of the following:
 - a. Under Windows, double-click the Remote Administration Client icon.
or:
 - b. Under Linux, navigate to `/opt/nfast/bin/racgui`, or the appropriate installation directory.
 - Make sure the `pcscd` service is running.
 - Navigate to `/opt/nfast/bin/racgui`, or the appropriate installation directory.
 - c. Under OS X, open the Launchpad. Click on the **RemoteAdminClient** icon.

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

2. Enter the IP address or Hostname of the required Remote Administration Service, or select the appropriate entry in the drop-down list, which stores the last 10 connections that have been used.


 If the communication port has been changed from the default (9005), you can also enter the correct number here. For example, *Hostname:Port*.

See your system administrator for more information about IP addresses, Hostnames, and ports.


 Only IPv4 addresses and Hostnames are supported.

3. Click **Connect** to connect with the Remote Administration Service, or **Exit** to close the application.

An error message displays if a connection cannot be established with the IP address or Hostname. If an error occurs, 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.

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

 An HSM that does not support Dynamic Slots because it does not have the appropriate firmware, or does not have any dynamic slots configured, cannot be selected. However, it still displays in the list.

5. Ensure that an nShield Trusted Verification Device is connected to your local computer and, on the **Select Card Reader (step 3 of 3)** wizard page, select it as the reader that you want to associate with the HSM.

If, for example, your computer has its own built-in card reader, this will also be shown on the the **Select Card Reader (step 3 of 3)** wizard page. You should ensure that you select the nShield Trusted Verification Device.

 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.

6. Click **Next** to complete the association of the Trusted Verification Device with the HSM and display the **Use Card Reader** wizard page. The page displays:
- The IP address or Hostname of the Remote Administration Service
 - The ESN of the HSM
 - The assigned HSM slot number



If no slot is available on the HSM, for example, if all configured slots are currently in use, an error message displays and you are returned to the **Select Card Reader (step 3 of 3)** wizard page.

- Whether an nShield Remote Administration Card is inserted in the nShield Trusted Verification Device

When an nShield Remote Administration Card is inserted in an nShield Trusted Verification Device a further window displays.

This explains that you are establishing a secure channel between the smart card and the target HSM, and shows how to use the device buttons. See [Confirming the HSM ESN using the nShield Trusted Verification Device on page 20](#) on page 1 for more information.



If you click **Exit**, or close the window 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 Trusted Verification Device 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.

5.2.1 Confirming the HSM ESN using the nShield Trusted Verification Device

If you have associated a nShield Trusted Verification Device with a Dynamic Slot of an HSM by completing all of the steps described and a nShield Remote Administration Card is inserted:

- The client displays a window stating that you are establishing a secure channel between the smart card and the target HSM, and shows how to use the device buttons.
- The nShield Trusted Verification Device displays the ESN of the HSM.

Do the following:

1. 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.

2. Do one of the following:

- a. If the ESN is correct, press **OK** on the nShield Trusted Verification Device to confirm. The screen of the device displays **Accepted**.

or:

- b. If there is a problem with the ESN, press **C** on the nShield Trusted Verification Device. The screen of the device displays **Abort OK?**.
- c. Press **OK**. The **Card Status** field on the **Use Card Reader** page displays **Unknown card**.
- d. 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. Complete Steps 1 and 2 in this section again.

If you do not confirm the displayed ESN on the nShield Trusted Verification Device within one minute, the device displays **Abort OK?** and you can no longer proceed. Do the following:

1. Click **OK**.

The **Card Status** field on the **Use Card Reader** page displays **Unknown card**.

2. Remove and reinsert the card.
3. Complete Steps 1 and 2 above.

5.2.2 Entering Pass Phrases using your remote access solution

Pass phrases are entered using Security World software via your remote access solution, as and when you are instructed to do so.

5.3 nShield Remote Administration Client command-line utility

The `raccmd` command line utility enables you to:

- List all available HSMs and select the appropriate one
- List all locally available nShield Trusted Verification Devices
- Associate a nShield Trusted Verification Device with an HSM, if a Dynamic Slot is available

5.3.1 Using the `raccmd` command-line utility

Run the following command:

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

On OS X you need to explicitly specify the path to the command-line utility:

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


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

5.3.2 Options

The following options are available:

Option	Description
<code>-h, --help</code>	Show this help message and exit
<code>--address ADDRESS</code>	Address of the Remote Administration Service
<code>--port PORT</code>	Port of the Remote Administration Service
<code>-v, --verbose</code>	Increase the verbosity of the output
<code>--version</code>	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
<code>listhsm</code>	List HSMs attached to a Remote Administration Service.
<code>listreaders</code>	List readers connected to your computer.
<code>associate</code>	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
<code>-h, --help</code>	Show this help message and exit
<code>-i, --interactive</code>	Run with interactive output
<code>-r, --until-removal</code>	Exit on first card removal
<code>-f ASSOC_FILE, --assoc-file ASSOC_FILE</code>	Create this file containing the associated slot, and exit when it is deleted

5.3.4.3 Arguments

Argument	Meaning
<code>ESN</code>	ESN of the HSM to use.
<code>READER</code>	Number of the local reader to use. Use <code>listreaders</code> to display the reader numbers.

Appendix A Troubleshooting

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

i 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.

Glossary

Authorized Card List

Controls the use of Remote Administration cards. If the serial number of a card does not appear in the Authorized Card List, it is not recognized by the system and cannot be used. The list only applies to Remote Administration cards.

Dynamic Slot

Virtual card slots that can be associated with an nShield Trusted Verification Device (or Standard card reader) connected to a remote computer. Dynamic Slots are in addition to the local slot of an HSM and any soft card slot that may be available. HSMs have to be configured to support between zero (default) and 16 Dynamic Slots.

nShield Remote Administration Card

Smart cards that are capable of negotiating cryptographically secure connections with an HSM, using warrants as the root of trust. nShield Remote Administration Cards can also be used in the local slot of an HSM if required. You must use nShield Remote Administration Cards with Remote Administration. If an nShield Remote Administration Card is in a slot, a `slotinfo -s` command will report it to be a *Type3SmartCard*.

nShield Remote Administration Client


A user interface that enables you to select an HSM located elsewhere from a list provided by the Remote Administration Service, and associate an nShield Trusted Verification Device attached to your computer with the HSM. Resides on your local Windows, Linux-based or OS X computer.

nShield Trusted Verification Device

A smart card reader that allows the card holder to securely confirm the Electronic Serial Number (ESN) of the HSM to which they want to connect, using the display of the device. nCipher supplies and the nShield Trusted Verification Device and recommends its use with Remote Administration.

Remote access solution

The remote access solution, such as SSH or a remote desktop application, which is used as standard by your organization. Enables you to carry out Security World administrative tasks from a different location to that of an nShield Connect or nShield Solo.

 nCipher does not provide this software.

Remote Administration

An optional Security World feature that enables Remote Administration card holders to present their cards to an HSM located elsewhere. For example, the card holder may be in an office, while the HSM is in a data center. Remote Administration supports the ACS, as well as persistent and non-persistent OCS cards, and allows most smart card operations to be carried out, apart from loading feature certificates.



You should not use Remote Administration to back-up keys from NVRAM to an nShield Remote Administration Card, as in transit, the keys would not be physically protected from access by the host system.

Remote Administration Service

Enables secure communications between an nShield Remote Administration Card and the hardserver that is connected to the appropriate HSM. Listens for incoming connection requests from nShield Remote Administration Clients. Supplies a list of available HSMs to the nShield Remote Administration Client and maintains an association between the relevant nShield Trusted Verification Device and the HSM.

Standard card reader

A smart card reader for ISO/IEC 7816 compliant smart cards. nCipher recommends that you use an nShield Trusted Verification Device. If standard smart card readers are used, they should only be deployed with the nShield Remote Administration Client command-line utility, not the GUI.

Standard nShield Cards

Smart cards used in the local slot of an HSM. Standard nShield cards are not supported for use with Remote Administration. If an nShield Remote Administration Card is in a slot, a `slotinfo -s` command will report it to be either a *Type1SmartCard* or a *Type2SmartCard*.