nShield Security World (Multi-Tenancy)

Multi-tenancy on nShield 5s

11 June 2026

Table of Contents

1. Introduction to Multi-tenancy

Multi-tenancy enables multiple users ("tenants") to securely share a single nShield HSM while operating as if each tenant had a dedicated HSM. The HSM owner ("service provider") enables this capability by creating secure instances (VCMs) within the HSM for use by individual tenants. Tenants are fully isolated from one another and, once the initial configuration has been completed, experience functionality and behaviour comparable to that of an exclusive HSM. Once commissioned, a VCM is presented to the tenant as an independent module, equivalent to a physical HSM.

This means that on a single nShield HSM, multiple users are able to load their own Security World with the assurance that all keys are securely separated from, and inaccessible to, all other users.

Multi-tenancy is a licensed feature and is only available when a valid multi-tenant license is installed on the system. For more information, see Multi-tenant licensing.

1.1. Multi-tenancy terms and definitions

VCM

A discrete isolated instance of a multi-tenant nShield HSM that enables a user ("tenant") to access the cryptographic resources of the HSM.

Tenant

An individual or an organization that uses a "VCM" to perform cryptographic operations. With multi-tenancy, multiple tenants can access a single nShield HSM in a fully isolated way.
See Tenants.

Service provider

The individual or organization that owns the physical nShield HSM and is responsible for maintaining it.
See Service providers.

Active VCM

A VCM that has been started and is currently running.

Inactive VCM

A VCM that has been stopped or that has been created but never started.

Enrolled VCM

An active VCM that has established a communication path with a tenant. You cannot enroll an inactive VCM.

2. User Roles

The multi-tenant system defines two user types that are not available in single tenant systems:

- Service provider
- Tenant

2.1. Service provider

The service provider installs, ugrades, and manages the nShield HSM and creates and manages the VCMs for the tenants to use. There is only one service provider per HSM. Service providers cannot access the cryptographic secrets created by tenants on their VCMs.

A service provider can also act in a dual role as service provider and tenant, if they create VCMs for their own use. See Tenant - service provider interactions.

2.2. Tenant

Tenants access the nShield HSM through a VCM, enabling them to perform cryptographic operations.

A tenant may own multiple VCMs; however, only one VCM may be enrolled on an HSM at a time. If a tenant requires multiple concurrently enrolled VCMs, each VCM must be enrolled on a separate multi-tenant nShield HSM. A single nShield HSM can host multiple tenants, each with an independent VCM. Refer to Active and inactive VCMs for additional details. Cryptographic secrets are strictly isolated and tenants cannot access secrets created by other tenants.

2.3. Tenant - service provider interactions

The service provider role and the tenant role could both be held by the same person or organization. In this case, the user must switch between roles to perform the different tasks.

The service provider and tenant need to coordinate with each other when maintaining a VCM. For example, a tenant requests a new VCM from the service provider who then sends a configuration file to the tenant containing the data needed to enroll the new VCM.

The messages are created by the system but the communication method between the ten-

ant and service provider is 'out of band', meaning it is for the two parties to decide on an appropriate method. This could be a secure messaging service, or a shared filesystem.

Similarly if the service provider needs to stop a VCM, they should inform the tenant to whom the VCM belongs, so that they stop using it.

The tenant can optionally specify a validity period on some messages sent to the service provider. If the service provider does not act on the request before the validity period expires, the request will fail and a new request must be generated. It is important that the clock on the tenant's machine is synchronized with the clock on the service provider's machine and that the module clock is synchronized with the service provider host machine.

3. VCMs

The maximum number of active VCMs that a service provider may provision concurrently is determined by the applicable multi-tenancy license. With the exception of licenses issued for base-speed HSMs, all multi-tenancy licenses permit up to 1,000 total VCMs per HSM. For instance a license permitting 15 active VCMs allows for up to 985 inactive VCMs when all active VCMs are in use. Base speed HSMs are limited to a maximum of five VCMs.

VCMs can be created and left inactive, or they can be activated for a period of time and then stopped. The license covers only VCMs that are currently active.

A Security World loaded onto an active VCM will not lose the Security World data when the VCM is stopped. The data is preserved and will be available again when the VCM is restarted. You can only load Security World data onto an active VCM.

Inactive VCMs place no load on the HSM's processor and they consume minimal memory, apart from any Security World data they contain.

While tenants can have multiple inactive VCMs on an HSM, they can only have a single active VCM enrolled on any one HSM at one time. A tenant could have multiple VCMs on the same HSM, but they would need to unenroll the one they were currently using before enrolling a different one.

4. Tenant - VCM relationship

When a tenant requests the creation of a VCM, they send two public keys to the service provider. The tenant must have possession of the corresponding private keys to be able to use the VCM.

Typically, a VCM has a one-to-one relationship with a tenant, meaning that the tenant has exclusive use of the VCM. While it is possible to share keys between tenants to give multiple tenants access to the same VCM, you should consult with Entrust and your organization's security policy before doing this.

A tenant can have a one-to many relationship with VCMs, although as noted previously, they can only have a single enrolled VCM on one HSM at a time. If the organization has multiple multi-tenant nShield HSMs, a tenant could have VCMs enrolled on different HSMs. A containerized solution is also possible, where multiple tenants are hosted on the same physical machine, however conceptually this is the same as having multiple tenants on different machines.

5. Key differences to non multi-tenant systems

5.1. Service and module visibility

When using a multi-tenant system, until you create, start, and enroll a VCM, you will not have access to `ncoreapi` services and the `enquiry` command will not display any modules.

This is because of the difference in user roles between the service provider and the tenant. When you boot a physical nShield HSM into multi-tenant mode, you are booting the physical hardware, which will not appear in the `enquiry` command output, because `enquiry` is looking at the VCMs, not the physical modules.

Until the service provider has created a VCM for a tenant, there are no modules available, so `enquiry` cannot display them. After the VCM has been created, started, and enrolled, the tenant can then access the `ncoreapi` services and can use the `enquiry` command to view the module.

While the same user can be both service provider and tenant, the two roles are distinct, and the user can only use the VCM when acting as the tenant.

5.2. Separation of tenant from physical hardware

In a non-multi-tenant system, commands for management and cryptographic operations were run directly on the machine that contained the nShield 5s module. This direct communication between host and module over the PCIe bus made communication extremely reliable. It also meant that rebooting the host automatically rebooted the HSM.

In a multi-tenant system, the tenant typically does not operate from the same machine that hosts the HSM. In this case, commands that are issued locally by the tenant must be transmitted to the VCM across a network. This means that:

- The network must be correctly configured for the tenant to interact with the VCM.
- Network issues or instability could prevent communication between tenant and VCM.
- The tenant's machine and the HSM that contains the VCM could reboot independently of each other.

This adds complexity to the network configuration and also to the recovery process if a loss of service occurs.

Because the nShield 5s does not support automatic recovery from all

> network outages, some network events will require manual recovery. You should use multi-tenancy on the nShield 5s over reliable networks to minimise outages, for example, a private LAN.

6. Startup overview

The following table contains a brief guide on setting up multi-tenancy. Follow the steps in order, paying attention to the user role required for each one.

You only need to complete the first three steps of the process once. The remaining steps should be completed for each new VCM you set up.

Detailed guidance is available in the folowing user guides:

- nShield v14.1.1 Service Provider User Guide
- nShield v14.1.1 Tenant User Guide

Setup steps

	Service provider	Tenant
1	Purchase and apply the multi-tenant license.	
2	Configure service provider networking.	
3	Configure automatic system log retrieval	
4		Create a tenant request for a VCM.
5		Send the tenant request to the service provider.
6	Create a VCM and allocate an unused address in the subnetwork to it.	
7	Start the VCM.	
8	Send the configuration file to the tenant.	
9		Configure tenant networking.
10		Enroll the VCM.

The total volume of system logs produced will increase with each VCM added. Because of this, Entrust recommends that you use of the nshield audit logging service `nshieldauditd` to automatically fetch system logs from the HSM. If you do not periodically clear logs from the system, the HSM will eventually stop working when its internal disk becomes full.

7. Upgrade to and downgrade from v14.1.1

When upgrading to v14.1.1, first upgrade the host Security World software to v14.1.1, and then upgrade the module firmware to v14.1.1. The firmware upgrade will automatically return the module to a factory state.

When downgrading from the v14.1.1 release, downgrade the module firmware first, and then downgrade the host Security World software. The firmware downgrade will automatically return the module to a factory state.

After the module is returned to a factory state, you must enroll it with the hsmadmin enroll command before performing any other operations.

Use v14.1.1 Security World software only with v14.1.1 firmware.

8. Reinstallation of v14.1.1 host software

If you want to reinstall the v14.1.1 host software on the Service Provider machine, there will be a brief loss of service for all tenants. This is because the scripts used to uninstall the soft ware will remove the device driver and cause the `nshield` interface to be removed from the Service Provider host machine.

After re-installing the host software you must reapply an IP address to the `nshield` inter-face, as described in define the nshield interface.

Once the IP address has been restored, each tenant must restart their hardserver.

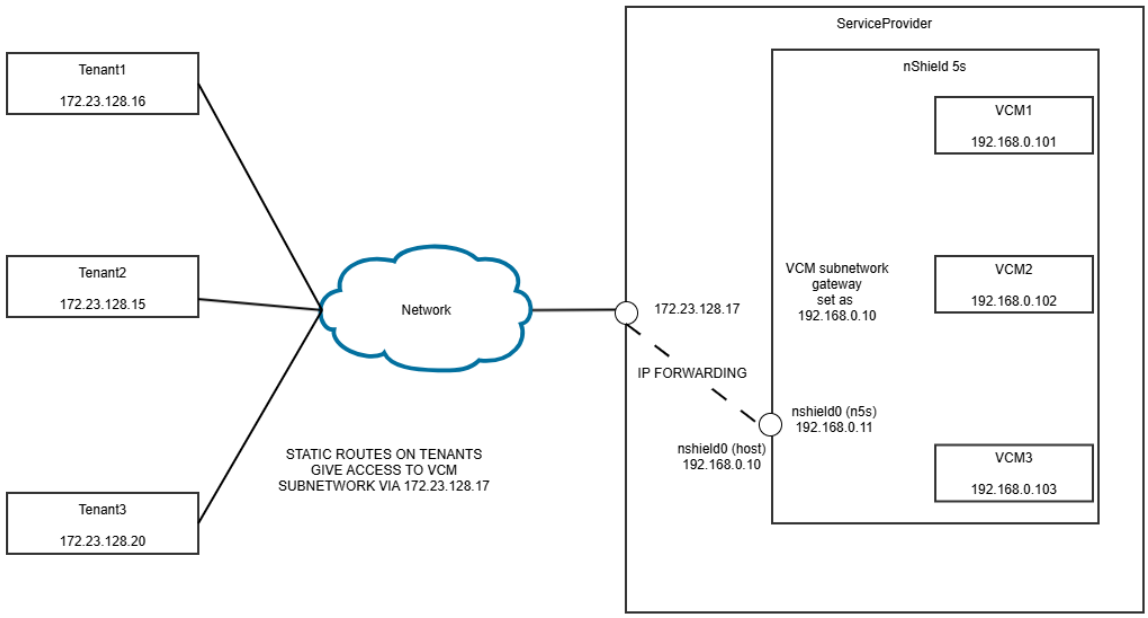
9. Network setup for multi-tenancy on nShield 5s

The exact network setup required depends on:

- Your existing network topology.
- The operating system used by all the machines involved.
- The constraints of your organization's IT and security policies.

It is not possible to give exact instructions for all possible scenarios.

This chapter gives guidance and example commands to set up a network similar to the one in the following diagram on a Linux operating system:



You might need to swap the commands in the examples here if you are using a non-Linux operating system.

The aim is to establish routing between the tenant machines and the VCMs hosted within the Service provider's nShield 5s HSM. This route enables packets to be sent back and forth between a tenant and their allocated VCM.

In this example network there are three tenants and a service provider all using physical machines that have IP addresses in the 172.23.128/24 subnetwork. The service provider defines a 192.168.0/24 subnetwork for the VCMs. In the service provider host machine the nShield 5s appears as device `nshield0`.

If you later uninstall your system, you may need to reverse some of these network changes before you perform a new installation, otherwise you may get some failures in install scripts. Entrust recommends that you keep notes of any network changes that you make for reference when you uninstall and install the system.

9.1. Configure the HSM: service provider

It is the service provider's responsibility to configure the networking of an HSM that will be used for multi-tenancy. This should be done before creating any VCMs.

9.1.1. Define the VCM subnetwork

To define a VCM subnetwork:

1. On the HSM, run `hsmadmin setnetwork` to configure the addressing.
2. On the HSM, run `hsmadmin reset`.

The service provider must define a subnetwork for the VCMs it will host. Each VCM will then be allocated an address within this subnetwork. The options available are:

- IPv4 addressing
- IPv6 addressing
- IPv6 link local addressing

IPv4 and IPv6 define an IP address for the HSM, which is currently unused, and a network mask that determines the number of VCM addresses available. When VCMs are created they can be freely allocated any unused IP address on this subnetwork.

IPv6 link local can be used when the tenants and service provider are hosted on the same physical machine. Because a tenant host machine can only have one active VCM hosted on a given HSM, this solution is only useful for multi-tenant operation if the tenant host machines are containerised by use of Docker containers or a similar technology.

Once the VCM subnetwork has been defined the HSM must be reset using hsmadmin reset so that the settings will be applied to any VCMs that are created.

You cannot change network settings for VCMs that have already been created. If you wish to change your network setup you should first

> delete any existing VCMs, change your network settings, reset the HSM and then create new VCMs.

The following example command defines a VCM subnetwork with 256 addresses, 192.168.0.0 to 192.168.0.255. The address 192.168.0.11 is allocated to the HSM and 192.168.0.255 would be the subnet broadcast address. VCMs can be allocated to any of the other addresses, although one address will be needed for the host interface.

```
sudo /opt/nfast/bin/hsmadmin setnetwork --esn E1CF-F3BB-2811 ipv4static --address 192.168.0.11/24 --gateway
192.168.0.10
```

9.1.2. Define the nshield interface

If you are not using link-local addressing, the `nshield` interface on the host machine in which the HSM is installed, for example `nshield0`, must be assigned an unused IP address on the VCM subnetwork, for example:

```
sudo ip addr add 192.168.0.10/24 dev nshield0
```

> Ensure that the method you use for assigning the address will survive a reboot of the machine.

> If you uninstall the Security World software, the `nshield` interface will be removed when the driver is uninstalled and if you subsequently reinstall the software you must issue this command again.

9.1.3. Enable IP forwarding

IP packets must be forwarded between the externally routable IP address of the machine hosting the HSM and the VCM subnetwork, for example:

```
sudo sysctl net.ipv4.ip_forward=1
sudo sysctl -w net.ipv4.conf.all.forwarding=1
```

> These example commands are very permissive and suitable only for a private network. Your IT or security department might require you to implement something more restrictive depending on the network you are using.

9.1.4. Configure firewall

Your firewall must be configured to allow packets to flow between your tenants and their VCMs. The ports used by services within the VCM can be found in the configuration file, which is automatically generated when the VCM is created. The ports currently used are:

Service	Port
sshadmin	2201
ncoreapi	2203
monitor	2206

An example command to configure the firewall is:

```
sudo iptables -A FORWARD -j ACCEPT
```

Ensure that the method you use for IP forwarding will survive a reboot of the machine.

This example command is very permissive and suitable only for a private network. Your IT or security department might require you to implement something more restrictive depending on the network you are using.

9.2. Create a route from the tenant to the HSM: tenant

The service provider's machine that hosts the HSM acts as the gateway into the VCM sub-network. The tenant should create a static route to the externally routable IP address of the machine that hosts the HSM. This provides the routing entry for the VCM subnetwork.

For example:

```
sudo ip route add 192.168.0.0/24 via 172.23.128.17
```

In the example here, 172.23.128.17 is the IP address of the service provider's machine that hosts the HSM.

Ensure that the method you use for creating the static route will survive a reboot of the machine.

10. Multi-tenant licensing

To use the full set of multi-tenancy features, a valid license must be purchased and applied. Without a license, only a single VCM can be created and started (see Non-multi-tenant operation).

The multi-tenant license must be applied as the first operation after booting the multi-tenant firmware. Refer to Maximum number of concurrently active VCMs feature for how to apply the license.

The multi-tenant license determines the maximum number of active VCMs that can run on the HSM to which the license applies. When you reach the maximum number of active VCMs, you will not be able to start any more VCMs on that HSM. Before you can start another VCM you must stop a VCM that is already running or purchase a new license.

A multi-tenant license enables you to create up to 1,000 inactive VCMs. This means that you can create several inactive VCMs and start only the ones that you want to have currently active, as controlled by your license.

There is an exception for the nShield 5s Base speed HSM which is restricted to only creating 5 VCMs.

10.1. Non-multi-tenant operation

There is no advantage in using multi-tenant firmware for non-multi-tenant operation. Unless you have been advised to use multi-tenant firmware in this way by Entrust it is recommended that you load non-multi-tenant firmware.

If you use multi-tenant firmware without a multi-tenant license, you will be restricted to creating and starting a single VCM. However, you will still need to configure your system as though you were using it for multi-tenancy, including setting up the networking between the tenant and VCM and enrolling the tenant.

To do this, use the hsmadmin vcm single-setup command. This automates the process and configures an `autocreated-vcm` for you.

Use of the command `hsmadmin vcm single-setup` configures a default configuration that is most appropriate for non-multi-tenant operation. It is unlikely to be suitable for multi-tenant operation. If you subsequently purchase a multi-tenant license, you should delete the auto-created VCM and start a fresh installation.

11. Multi-tenancy recovery of a failed VCM

In a multi-tenant system it is possible for the HSM hosting a VCM to reboot independently of the tenant machine or for network outages to prevent communication between the tenant and their VCM. This can result in the `enquiry` command reporting a module as `failed`.

In most cases, the module can be restored to its previous state by a combination of the following:

11.1. Check the network

Ensure that there is network connectivity between the tenant and their VCM. The commands needed to do this will depend on your network and operating system, but you should ideally send ICMP echo requests and ensure that a reply is received, as in the example below where the VCM has an IP address of 192.168.0.107.

```
ping 192.168.0.107
PING 192.168.0.107 (192.168.0.107) 56(84) bytes of data.
64 bytes from 192.168.0.107: icmp_seq=1 ttl=63 time=19.4 ms
64 bytes from 192.168.0.107: icmp_seq=2 ttl=63 time=0.787 ms
64 bytes from 192.168.0.107: icmp_seq=3 ttl=63 time=0.773 ms
```

If you are unable to send and receive packets to and from the VCM, ensure that you have followed all the steps in network configuration and use standard network debugging tools to fix any network issues before continuing.

If any of the network settings you made while following network configuration do not survive reboots, this can be a common cause of failure and you should try to ensure that all settings survive reboot.

11.2. Temporarily reduce load if you are able and your HSM is at high load

If the HSM is running close to its maximum capability, you may experience timeouts in some administrative actions. Testing has shown that on a high-speed HSM this normally only occurs with at least 10 active VCMs all running at their maximum capacity.

As mentioned in the release notes, it is not recommended to run a multi-tenant HSM at such extreme load, but if you do so and experience some failure then it is very helpful to temporarily reduce the load on some VCMs while you attempt to recover. The load can then be restored once the failure is resolved. If you are a tenant, you will need to ask the ser vice provider to do this for you.

11.3. Try recovering with an ncoreapi retry command

A failed VCM can sometimes be recovered using the retry command. In the example below, the failed VCM is shown as module 1 in the `enquiry` command.

```
nopclearfail -m1 -r
```

11.4. Restart the hardserver

If a retry command does not restore the VCM, then try restarting the tenant hardserver. The example below is for a Linux operating system.

```
sudo /opt/nfast/sbin/init.d-ncipher restart
```

On a Windows operating system use the Windows Control Panel to restart the `nfast server` service or use the following commands

```
net stop "nfast server"
net start "nfast server"
```

11.5. Try clearing the module

If none of the procedures above have recovered the VCM, then you may be able to recover it by clearing the VCM with the following sequence of commands. In the example, the failed VCM appears as module 1 in the `enquiry` command.

```
nopclearfail -m1 -M

< WAIT for 30 seconds before issuing the next command >

nopclearfail -m1 -c
```

11.6. Contact support

If none of these methods work then contact Entrust Support.