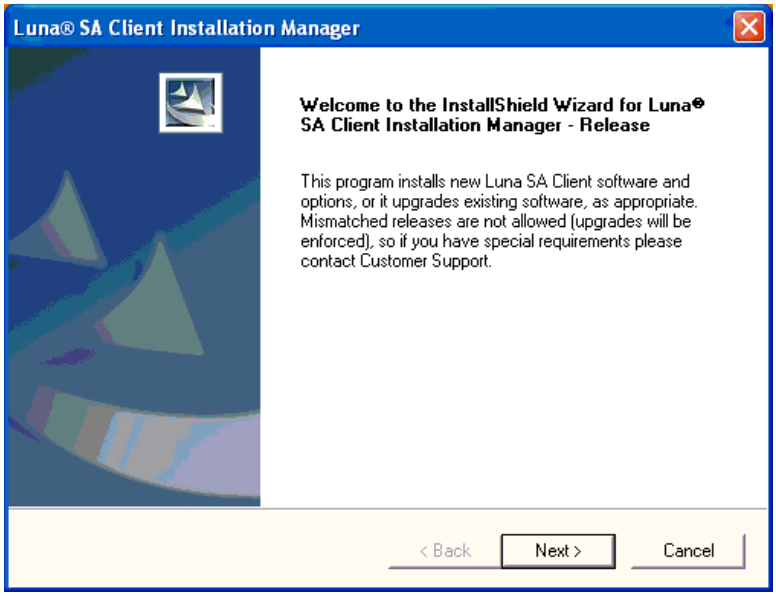
SafeNet Luna SA Client Software Installation

The Luna Appliance comes with software that must be installed on any client machine that requires connectivity to the HSM Partitions. Protegrity DPS software requires that the Hub Controller has this connectivity to the HSM appliance if HSM functionality is desired for the configuration.

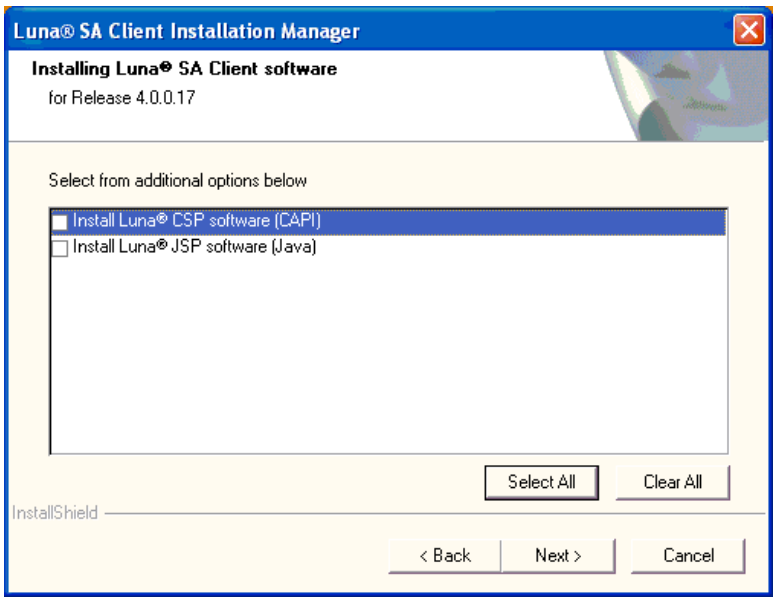
Although the Luna SA client software is simple and straightforward, the screenshots below illustrate the step by step progression of the Luna SA Client software installation process:

Note: The software process below is created from the **Windows** setup from the Luna SA software CD Release 4.0.

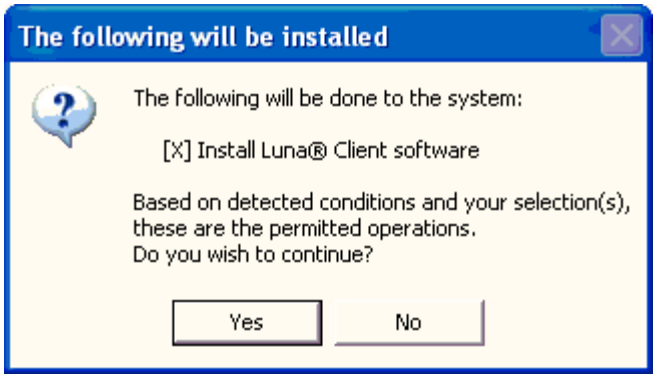
Insert the CD into the client box to start the installation.



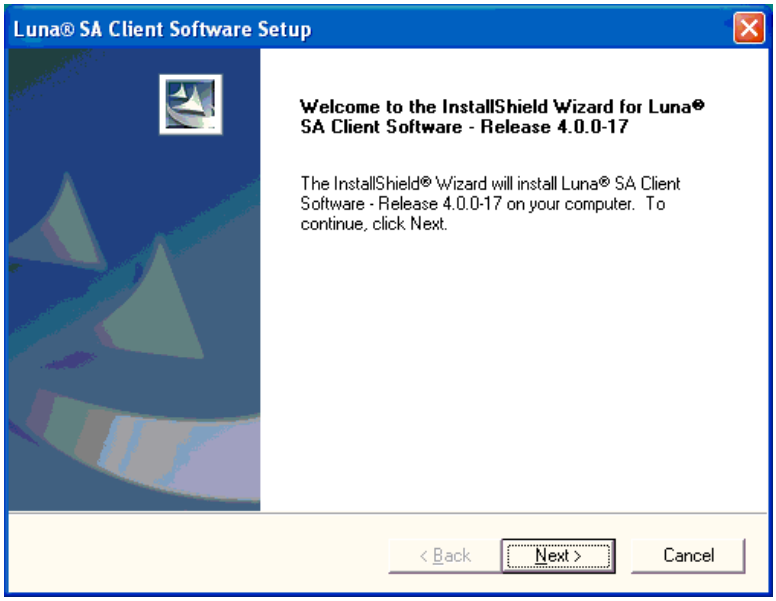
Click Next >>



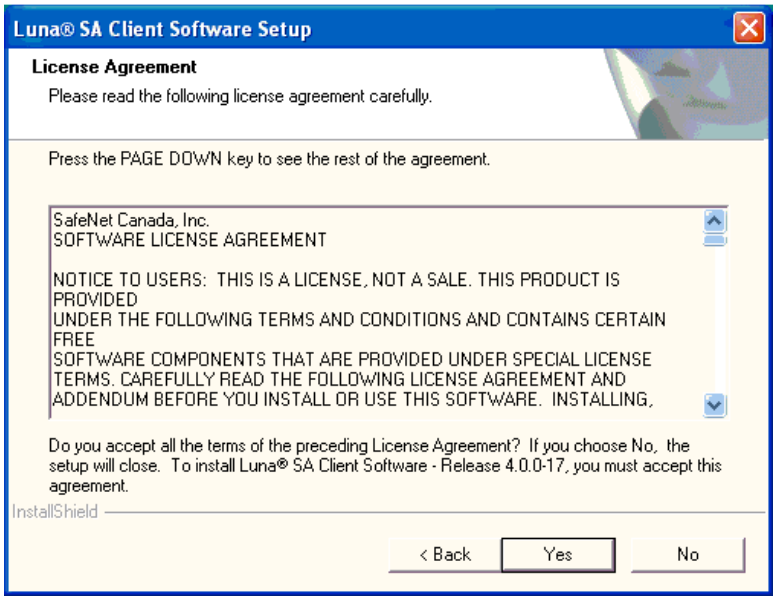
You do not need to check off any additional items. Click Next >>



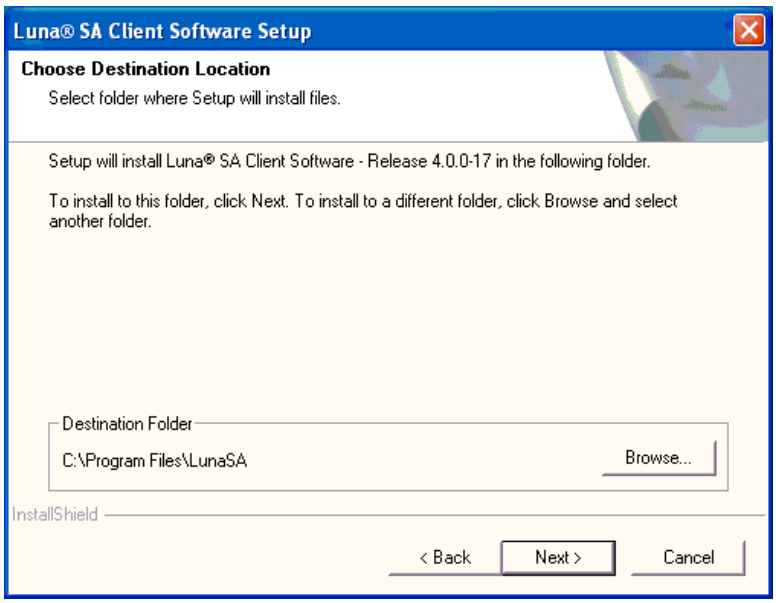
Click Yes



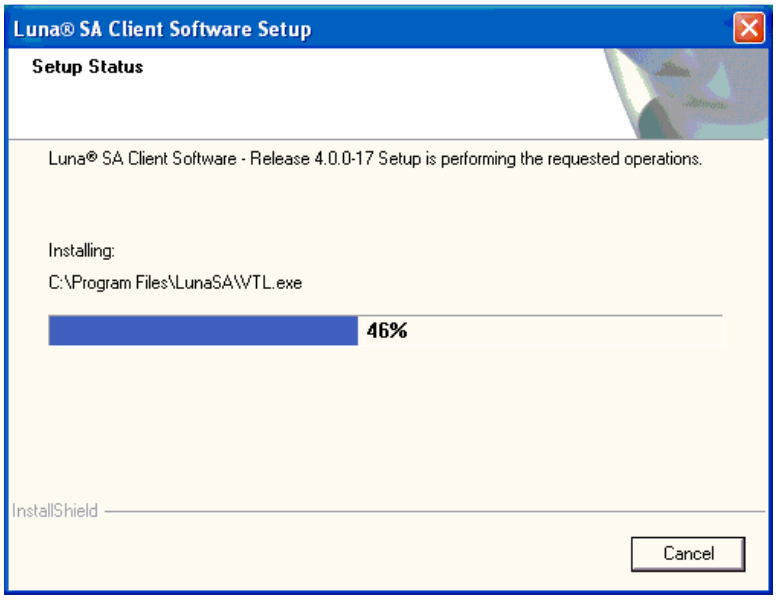
You will then be taken to another screen to start the install of the client software. Click Next >>



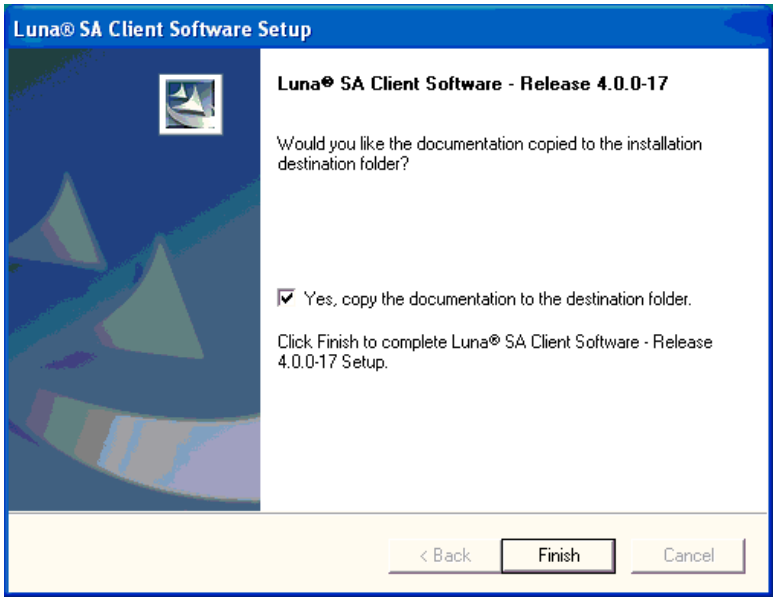
Click Next >>



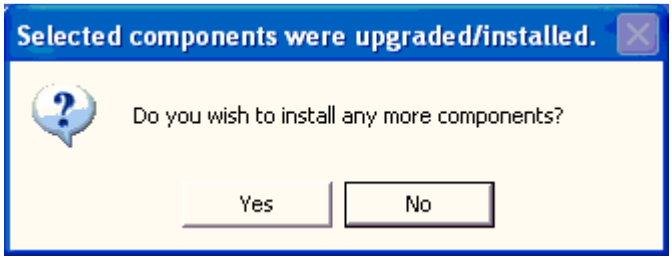
Choose a Destination Folder and Click Next >>



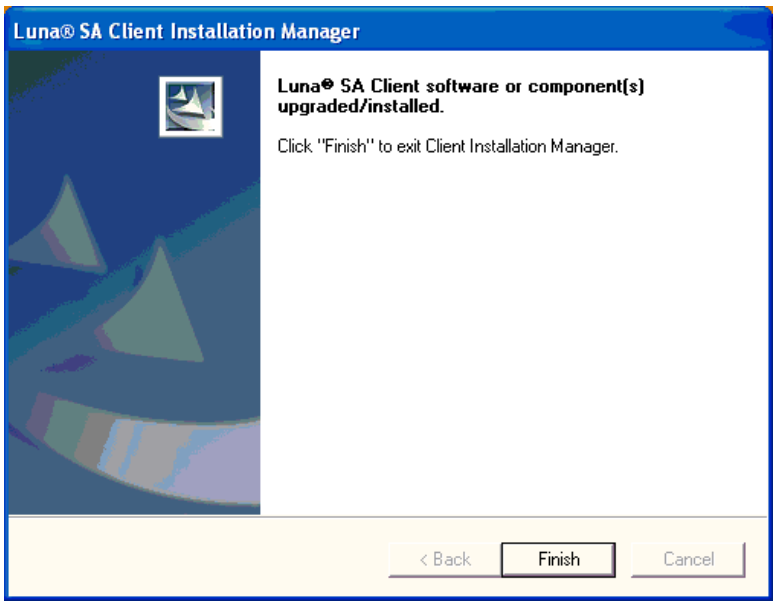
The installation will proceed



Click Finish



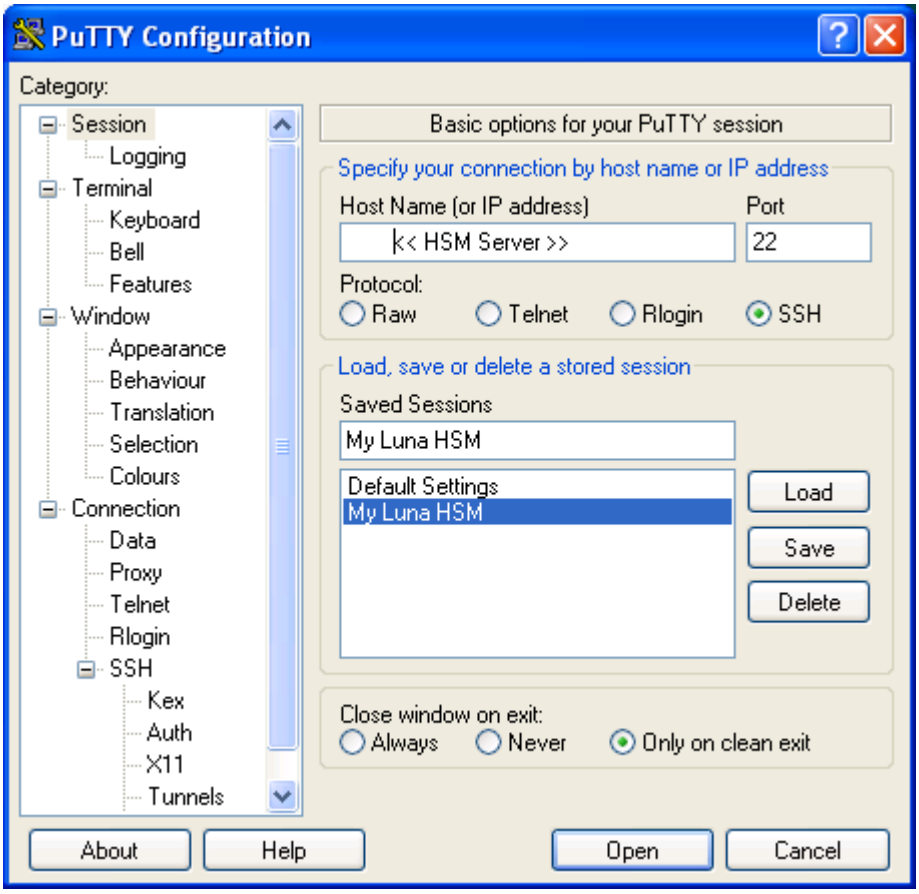
You may check No. There are no other components needed



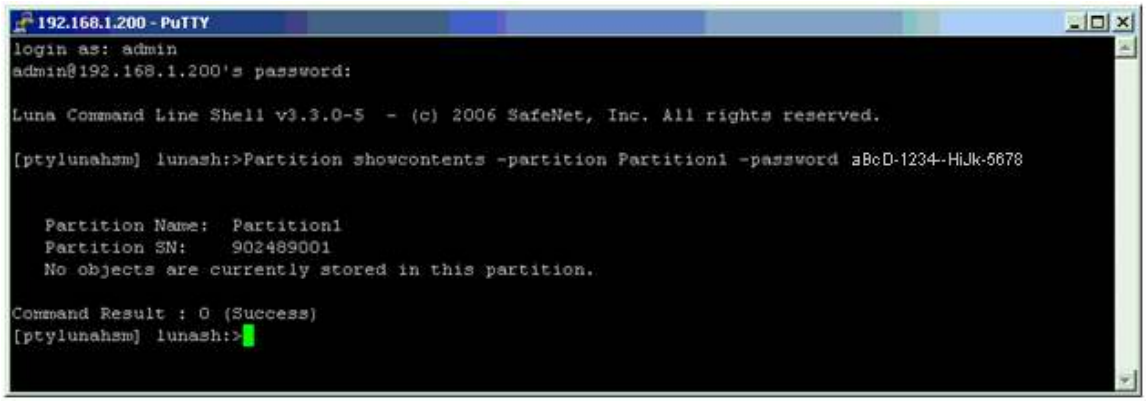
Click Finish and the installation is complete.

Communication with HSM Appliance

Connection to the HSM is done using the command line tool **PuTTY.exe** found in the root of the Luna SA install folder. This will only connect after the HSM has been configured and connected into the network and is also reachable by the client machine (i.e. PING)



Double click on the Putty.exe and you will see the screen above. Put in the IP address or server name like the above example. You may save the configuration to be retrieved later.



You will be brought to a command line style connection where you will need to login to the HSM appliance.

It is here that you will need the HSM Login and Password to perform administrator functions like connect and register clients to allow access to partitions.

Network Trust Link for Client Connection

With the assistance of your local network administrator, you should already have prepared the ***Client system*** for network connection. This means:

- Configure all the necessary IP settings (hostname, IP address, DNS, gateway, etc.) as appropriate to your network, and as applicable to your Client's operating system.
- Install an ssh client (the ctp copy utility should already have been installed during the Luna software installation).
- Start network services on your Client machine and verify that you have achieved a proper, working network configuration (by means of "ping" and other network utilities).

In order to connect a Client to an HSM Partition on the Luna appliance, you must first create a Network Trust Link (NTL) between them. An NTL consists of:

- the Network Trust Link Agent (NTLA), a software library that resides on the Client
- the Network Trust Link Server (NTLS), the server software that manages Network Trust Links on the Luna appliance and,
- the NTL itself, an encrypted, secure communications channel between the Client's NTLA and the Luna appliance's NTLS.

Network Trust Links use digital certificates to verify the identities of connecting clients. During the initial Luna system configuration (earlier in this chapter), the Administrator generated a unique certificate that identifies the Luna appliance. Similarly, each Client must generate its own certificate that identifies it uniquely (next section). Both the Client and the Luna appliance use these certificates to verify the other's identity before an NTL is created between them.

To create an NTL, the Client and Luna appliance must first exchange certificates. Once the certificates have been exchanged, the Client registers the Luna SA's certificate in a trust list, and the Luna appliance, in turn, registers the Client's certificate in its list of clients.

When the certificates have been exchanged and registered at each end, the NTL is ready to use. This is described in upcoming pages of this section.

The client software was installed for your operating system during the general installation (refer to the *Luna QuickStart Guide*).

You will perform the actions in this section:

- the first time you commission a Luna appliance, and you require a client to exchange certificates with the HSM and to be assigned to an HSM Partition, and
- whenever you have a new client that needs access to an HSM Partition

Create a Client Certificate (Windows)

Begin by creating a certificate and private key for the client, using the vtl command-line interface.

Before you run the `vtl createCert` command, run `hostname` to view the hostname of your client computer. Then, when you run the `vtl createCert -n <clientHostname>` command (example below), be sure to input the hostname *exactly* as reported (uppercase/lowercase). If you create a certificate using a hostname parameter that is not an exact case-match for the client's hostname, you may be unable to create an NTLS link.

```
c:\Program Files\LunaSASP\ >vtl createCert -n <clientHostname>
```

Example

```
c:\Program Files\LunaSASP > vtl createCert -n myClient1

c:\Program Files\LunaSASP\cert\client > dir
vtl
myClient1.pem
myClient1Key.pem
multitoken2
```

After the createCert command, vtl gives the full pathname to the key and cert files that were generated.

"-n" (name) is the only mandatory item, and must be the client hostname. Additional optional parameters can be added. Refer to the Reference section of this Help for full command syntax and description.

If you are working without DNS, then supply the client IP numerically, instead:

```
c:\Program Files\LunaSASP\>vtl createCert  -n <clientIPaddress>
```

In the `createCert` command, provide only the unqualified hostname, rather than the fully qualified hostname.

Import Luna Appliance Server Cert onto Client (Windows)

1. Open a command prompt window on the Client, and change directory to `c:\Program Files\LunaSA\`.
2. Securely transfer the `server.pem` file from the Luna SA, using the supplied Chrysalis Transfer Program (ctp) utility.

   ```
   c:\Program Files\LunaSA\ > ctp admin@myLuna3:server.pem .
   admin@myLuna3's password:
   server.pem           100%
   |*****************************************************|   928
   00:00
   ```

   Note the dot (.) at the end of the command, denoting "place the resulting file in the current directory".
3. Verify that the Server Certificate has arrived on the Client:

   ```
   c:\Program Files\LunaSA\cert\server > dir
   server.pem
   ```

Example (*No DNS*)

Any time the IP or hostname of the Luna appliance has changed (such as moving from a pre-production environment), the client(s) that have previously connected via SSH will detect a mismatch in the Luna appliance's server certification information and warn you of potential security breach. In this case you will need to remove that server's certificate information from the client's known host file found in:

`/<user home dir>/.ssh/known_hosts2`

If this is happening in a production environment, this could potentially be a security breach needing investigation.

Similarly, when you first open a ctp or ssh link, you must accept the certificate.
You can check the fingerprint of the certificate with:

```
lunash:> sysconf -fingerprint -ssh
```

Export a Client Cert to a Luna Appliance (Windows)

Send the client certificate (that you created on the previous page) to the Luna appliance, as follows.

The command is:

```
C:\Program Files\LunaSA\ > ctp cert\client\<clientCert>.pem admin@<serverhostname-or-IP>:/
```

You are prompted for the Luna appliance admin password.

Example

```
c:\> cd \Program Files\LunaSA\cert\client

c:\ Program Files\LunaSA\cert\client: dir

myClient1Key.pem  myClient1.pem

c:\ Program Files\LunaSA\> ctp "c:\Program Files\LunaSA\cert\client\myClient1.pem"
     admin@myLuna3:
```

 You must ctp to the admin account on the Luna appliance, or the client certificate will not register correctly.

For networks without DNS, use the Luna appliance's IP address, instead of the hostname.

Note the ":" after the destination. This is required. Without the colon, ctp does not recognize the supplied destination as a remote server.

The file arriving at the HSM is automatically placed in the appropriate directory. Do not specify a directory for destination.

Register the HSM Server Cert with the Client (Windows)

Use vtl, the supplied client-side tool for managing Luna client/server setup. The vtl command is not interactive. It is called from the command line or a shell prompt, it completes its current task, and it exits back to the shell.

Invoke the `vtl addServer` command so that the client can create a secure connection with the HSM (the server).

The vtl executable is located at `c:\Program Files\LunaSA\` unless you have changed the default installation.

```
C:\Program Files\LunaSA > vtl addServer -n <LunaSAhostname-or-IPaddress> -c
<serverCert-file>
```

Example

```
c:\Program Files\LunaSA > vtl addServer -n myLuna3 -c server.pem
```

If you are working without DNS, then give the server IP number, rather than its name, as in:

```
c:\Program Files\LunaSA\>vtl createCert -n <clientIPaddress> -c server.pem
```

Register the Client Cert to an HSM Partition

The client certificate, which has been securely transferred (ctp'd) from the client to the HSM Server, in previous sections, must be registered by the HSM Server.

You must be connected to the HSM Server (the Luna SA) and logged in as "admin".

The command is:

```
lunash:> client -register -client <client's-name> -hostname <client's-hostname>
```

The <client's-name>, above can be any string that allows you to easily identify this client - many people use the hostname, but the <client's-name> can be any string that you find convenient.

The command is expecting to find (on the Luna appliance) a client certificate filename that matches the client's hostname, as you provide it here. In other words, this is a check that you are registering the client whose .pem file you created in the previous steps and ctp'd to the appliance.

Example – lunash client registerClient Command

```
lunash:> client -register -client MyClient -hostname MyClient

Client registration successful.

lunash:> client -list

registered client 1: MyClient

lunash:>
```

If you are working without DNS, then register the client by its IP address, rather than its hostname.

lunash:> client -register -client <client's-name> -ip <clientIPaddress>

The Client is now registered with the Luna SA HSM.

You can verify on the Luna SA, with the 'client -list' command.
Refer to the Reference section of this Help for command syntax and descriptions.

De-Register (registration not complete)
If you have multiple Luna appliances connected and registered with a client and you de-register that client from one of the Luna appliances, then you must also de-register that Luna appliance on the client side.
Failure to do so will result in a "Broken pipe" error, which indicates an incomplete registration.

Re-Register
If you wish to de-register a client and then re-register with a new certificate, on the same Luna appliance, then you must stop and re-start the ntls service. Before such a restart, any attempts to connect will fail, and "Error on SSL accept" is logged.

Administration commands may take a few seconds to be noted by the NTLS. If you have added or deleted a client, we suggest that you wait a few seconds before connecting.

Assign a Client to a Luna HSM Partition

At this point, you should already have

- initialized the HSM and created one-or-more HSM Partitions,
- exchanged certificates between the Luna SA and the Client,
- registered the certificates of Client and Luna SA with each other,

to create a Network Trust Link (ntl) between Client and Luna SA.
The final Configuration step, before your Client can begin using the Luna SA, is to assign the Client to a specific Partition.

You will perform the actions in this section:

- Whenever you have a new client that needs access to an HSM Partition.

You must be connected to the HSM Server and logged in as "admin".

Assign a Client to a Partition

Now, assign the registered client to the HSM Partition.

The command is:

```
lunash:> client assignPartition -client <clientname> -partition <partition name>
```

Example – lunash client - assignPartition Command

```
lunash:> client assignPartition -client myClient1 -partition myPartition1
partition assign successful.
```

The parameter <partition name> is the name of the HSM Partition that was created earlier, following configuration of the HSM.

To verify, look at the HSM Partition assigned to the client.

```
lunash:> client -show -client <clientname>
```

Refer to the Reference section of this Help for command syntax and descriptions.

Verify Your Setup

Before beginning to use a Client application with your newly configured Luna SA, you can verify that the foregoing setup has been properly performed.

1. On your Client computer, open a command-line console.
2. Go to the Luna directory (`c:\Program Files\LunaSA` for Windows, or `/usr/LunaSA` for Linux, Solaris or AIX, or `/opt/LunaSA` for HP-UX), and type vtl verify.
3. The response should be similar to:

```
Slot     Serial #      Label
====     ========      =====
1        2279315       Partition1
```

   If you get an error message, then some part of the configuration has not been properly completed. Retrace the procedure.

At this point, the client and HSM are configured and registered with each other. You can now begin to use the Luna HSM with your application.

You can use the "`partition list`" command for a list of HSM Partitions on the HSM, and the "`client list`" command for a list of the clients assigned to an HSM Partition.

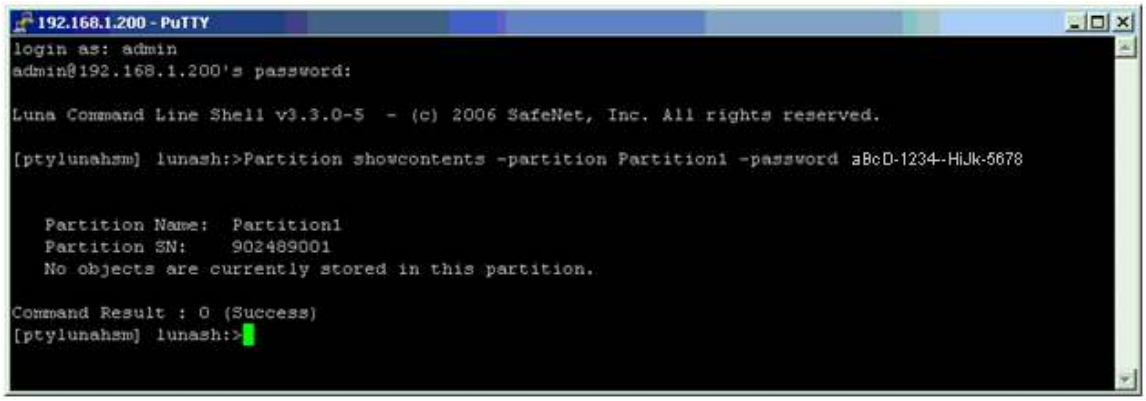
Hub Controller Configuration for HSM

Note: At this point the following should all have been completed:

1) *HSM Appliance is configured and connected to the network*
2) *Partitions have been created in the HSM appliance*
3) *Client Computer has client software installed*
4) *Network Trust Link established*
5) *Hub Controller is installed and keys created (See DPS Installation Guide for HUB Controller)*

For this configuration example, the HSM appliance has already been configured with a partition named ***Partition1*** *where the Protegrity keys will be stored.*

Connection to the HSM server is done using the command line tool **Putty.exe** found in the root of the Luna SA install folder.



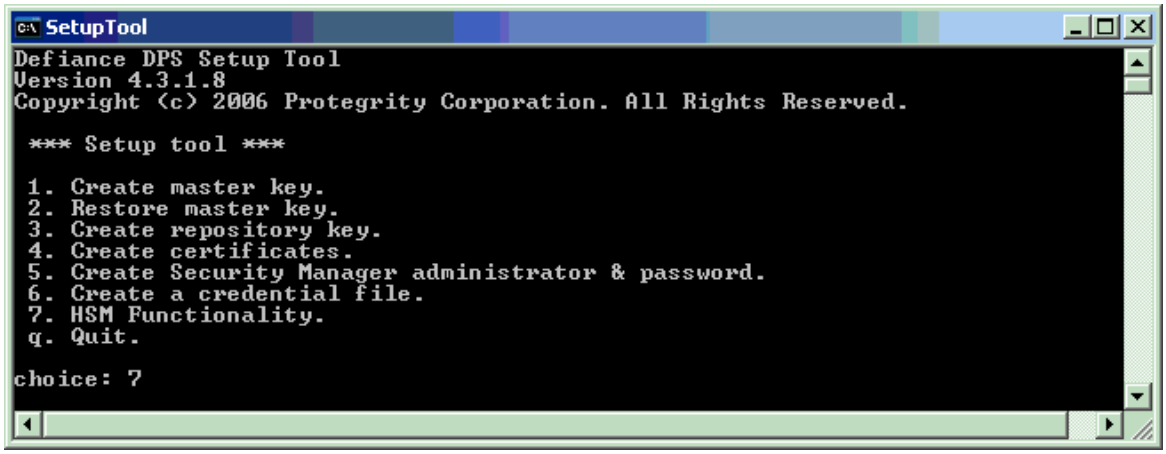
You will be brought to a command line style connection where you will need to login to the HSM appliance.

It is in the above illustration the command line:

lunash:> Partition showcontents -partition Partition1 –password aBcD-1234-HiJk-5678

has been executed and shows that there are no objects currently stored in Partition1. To run this command for another configuration, replace “Partition1” and the partition password with the relevant information from your configuration.

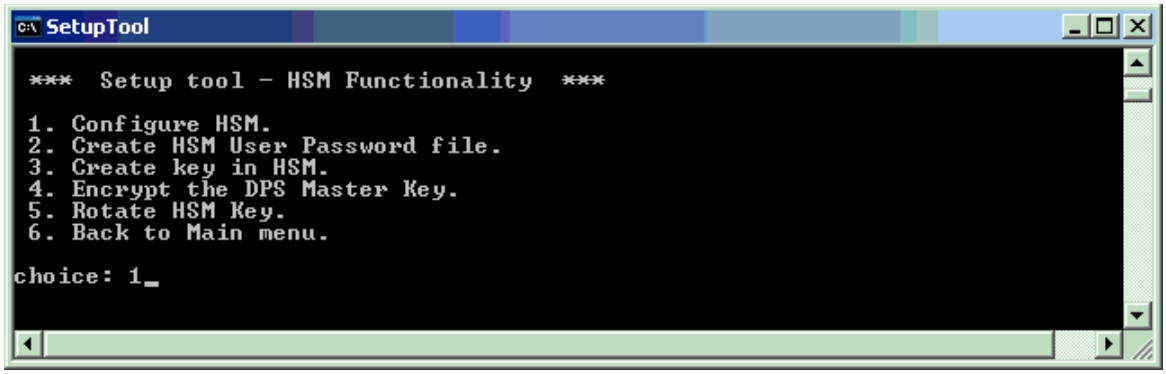
Run the Defiance Setup Tool



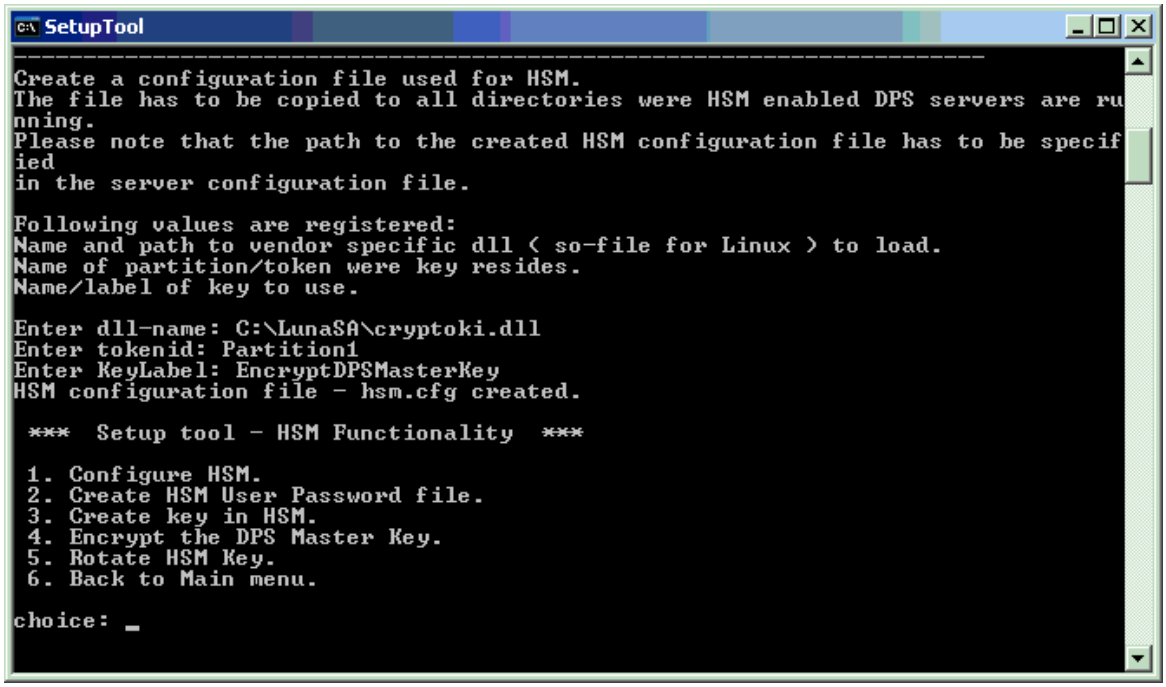
Run the Defiance Setup Tool to get to the menu. Use option 7 to configure HSM Functionality. Run through the menu in numerical order. Choose 1

Choice 1: HSM Configuration

This operation creates a configuration file for the HSM. The file created is named **hsm.cfg**.



1. Select option 1 from the menu.



2. Enter the path and filename.
   The location of the dll depends on the HSM that is installed and the way it is installed, e.g. "C:\LunaSA\cryptoki.dll".

3. Enter the token identifier, name of the partition/token, where the DPS keys will reside.

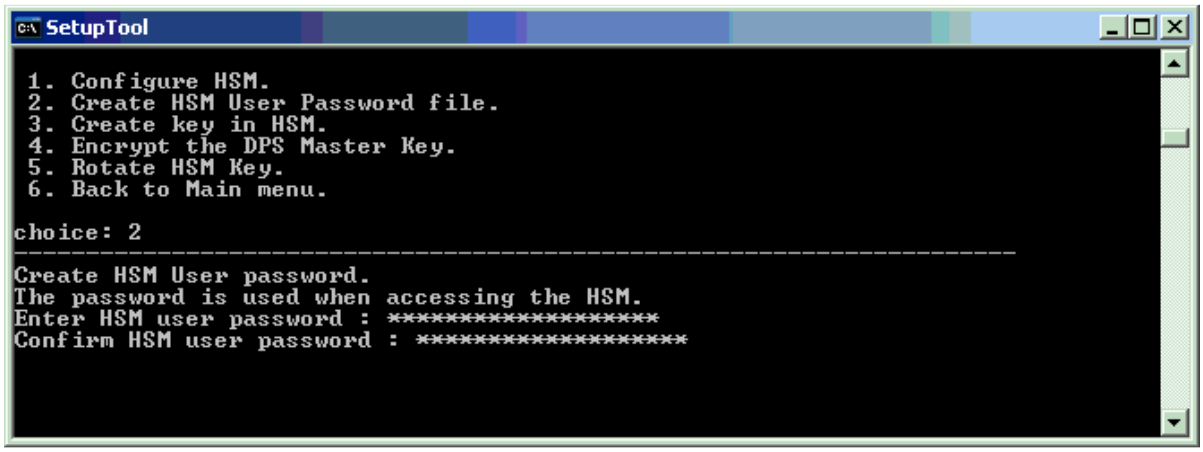
4. Enter the key label (this is the name of the key used for encryption and decryption of the DPS Master Key).
   When these values are entered, the Setup Tool will create a configuration file. The file will be named "hsm.cfg". This file has to be copied to all DPS servers that are using the HSM protected Master key.

NOTES

If the file already exists you will be asked if you want to replace current values with the new values. Please review the configuration file to make sure that the path is correct. The path to the HSM User password file is set to the directory where Setup Tool is run, by default

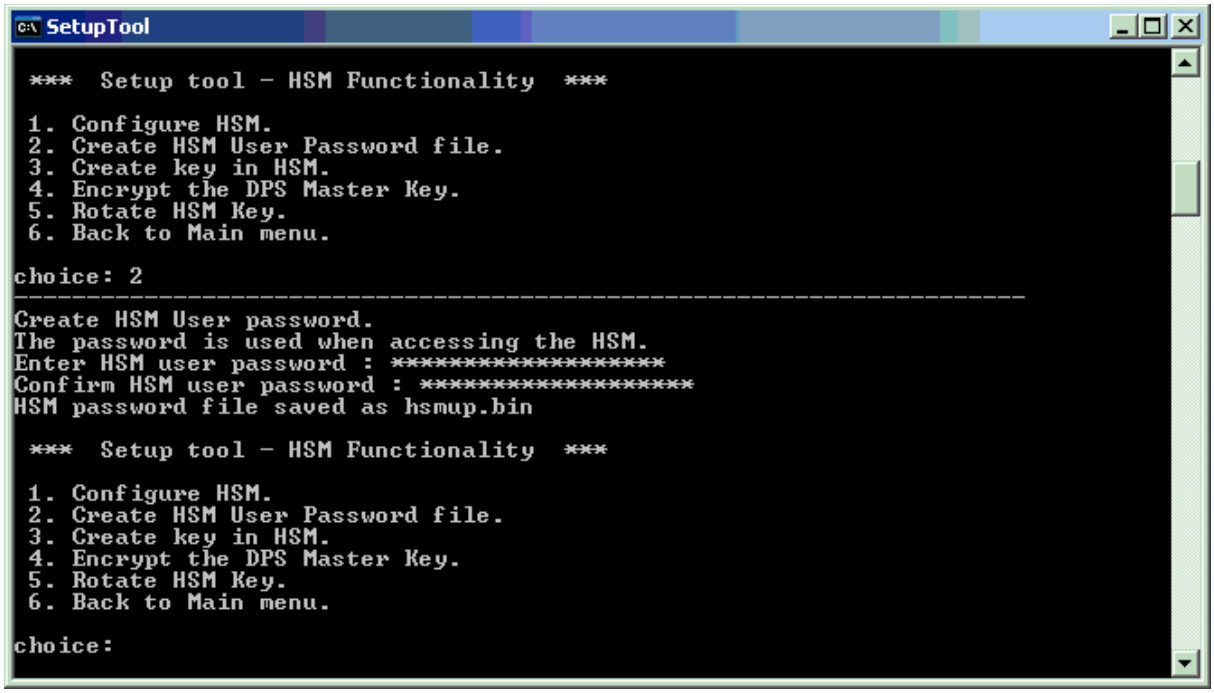
Choice 2: Create HSM User Password File

This operation is used to create the HSM user password file that is used by DPS to log on to the HSM.



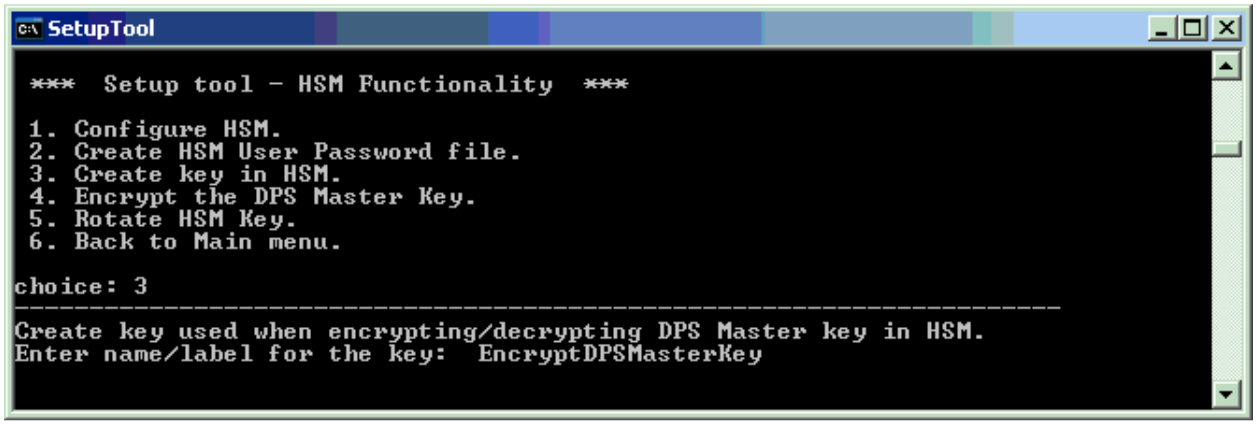
Select option 2 from the menu.

2. Enter the HSM user password. This is the password used to log on to the HSM. The password has to match the user password created in the HSM. The registered password is scrambled and saved in a file named "hsmup.bin". All DPS servers that are using the same HSM user can use the same password file. Make sure that the configuration file, hsm.cfg, points to a valid file.

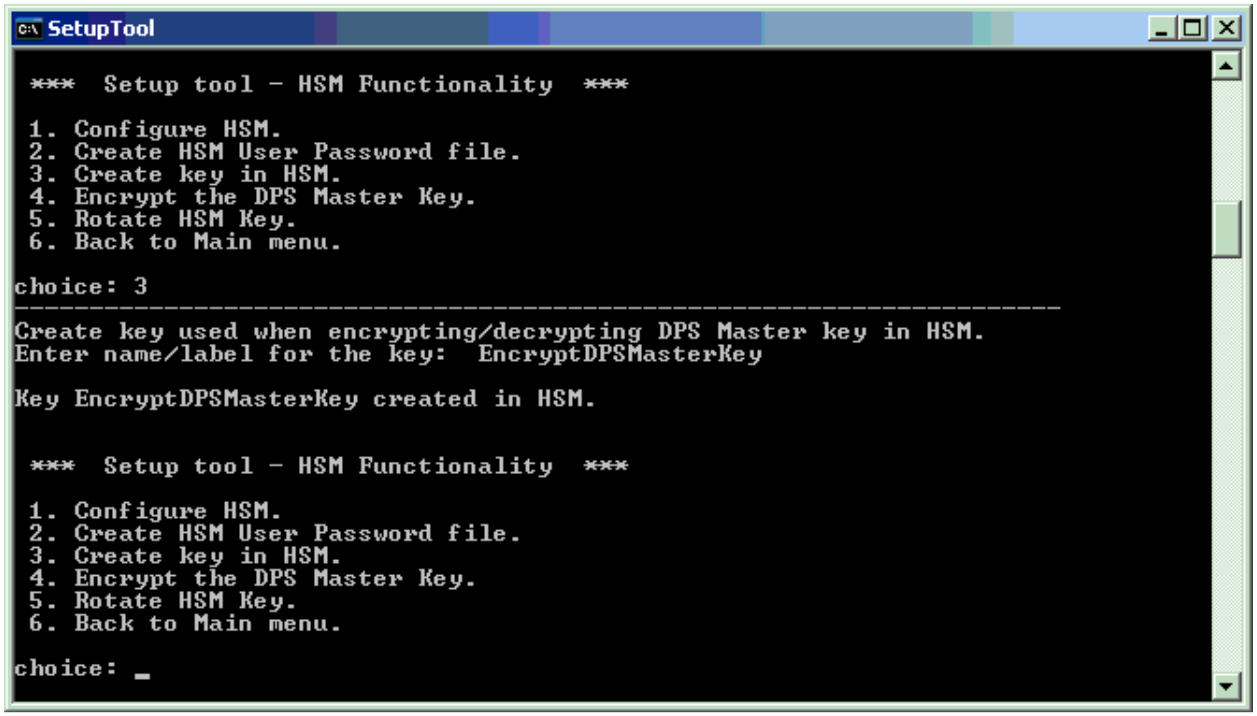


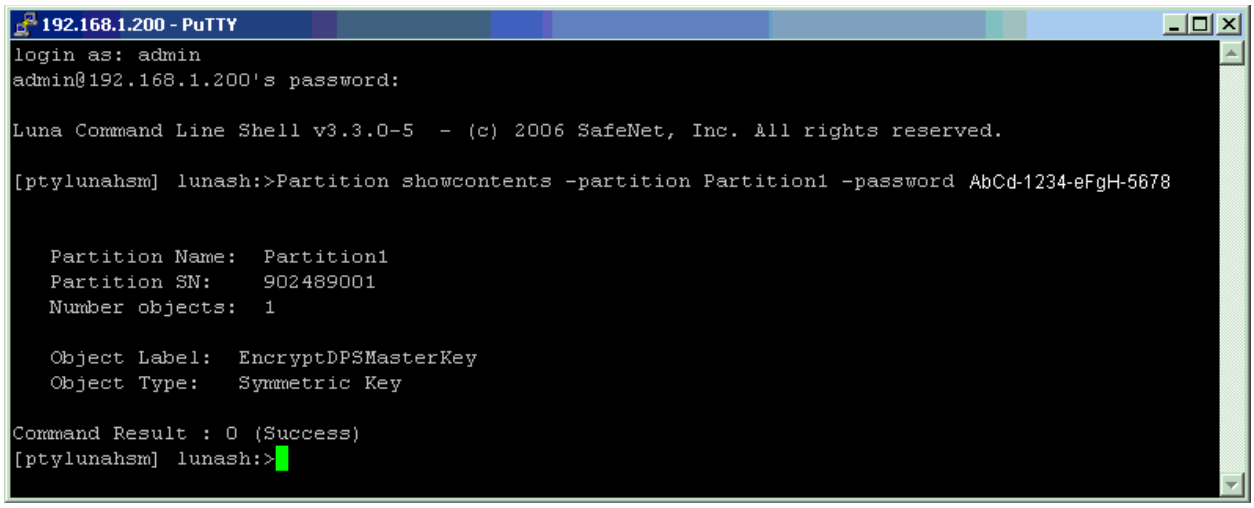
Choice 3: Create Key in HSM

This operation creates a key in the HSM. The key is an AES256 key that will be used to encrypt/decrypt the DPS Master Key.



Select option 3 from the menu and Enter the Key name





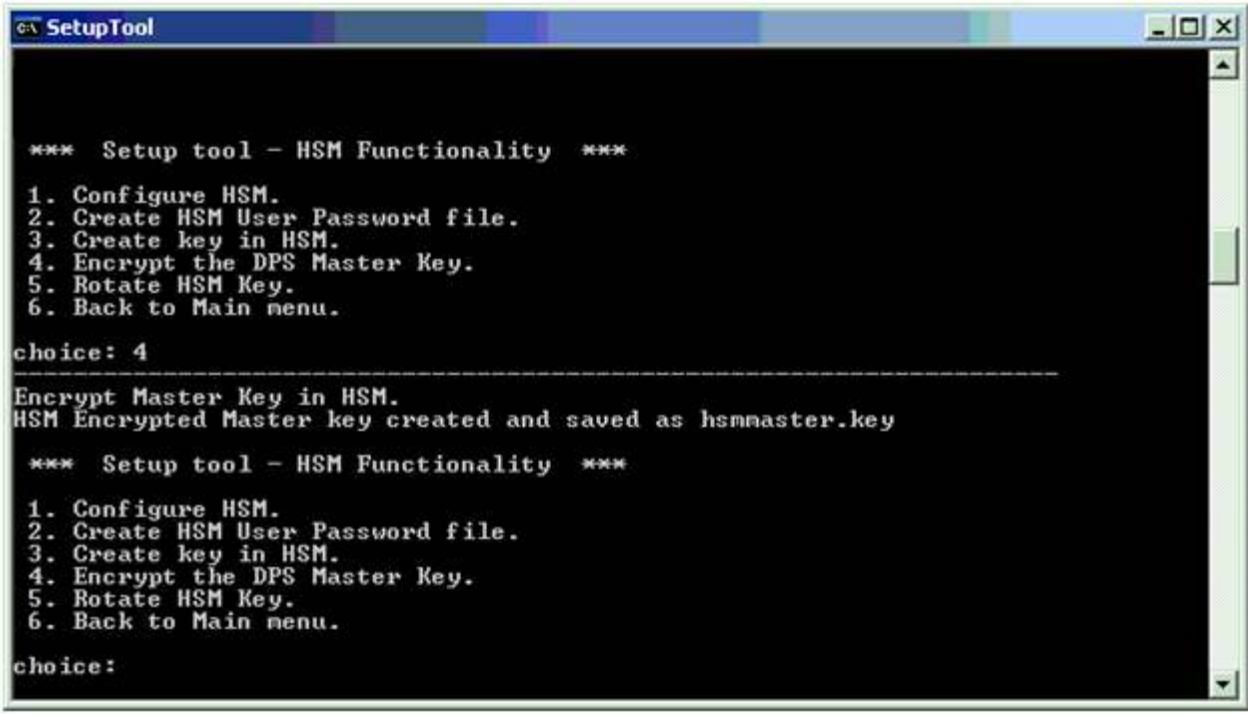
At this point, you may verify the creation of the new key in the HSM by rerunning the Partition showcontents command through the Putty tool.

Run the command:

lunash:> Partition showcontents -partition ***<<PARTITION NAME >>>*** *–password* ***<<Partition PWD>>>***

Choice 4: Encrypt the DPS Master Key

This option is used to encrypt the Defiance DPS Master Key in the HSM. To perform HSM encryption of the Master Key, the Master Key has to have been created, and the master.key file has to exist.



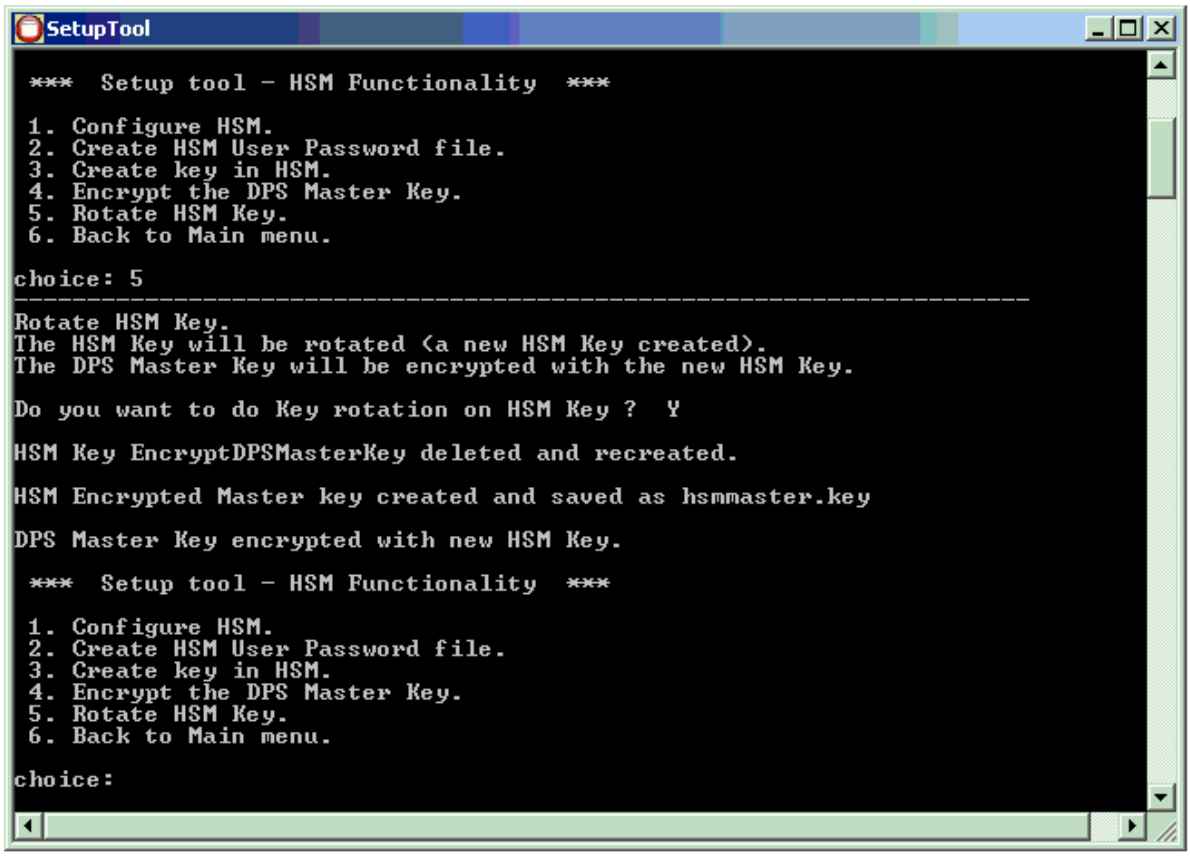
Select option 4 from the menu.

The key file is created automatically. The key file is created in the \data directory.

Choice 5: Rotate HSM Key

The Setup Tool provides the functionality to rotate the HSM key without affecting the other DPS keys. This is added as a separate menu-item in the submenu for HSM and appears as option 5, *Rotate HSM Key*.

When a rotation of the HSM key is wanted select the menu item and follow the instructions. Then the old HSM key is deleted and new one created. This new HSM key will be used to encrypt/decrypt the master key that will be stored in a new HSM master key file used for DPS in general. The file hsmmaster.key now contains the DPS Master key encrypted with the new rotated HSM key.



Select option 5 from the menu. What happens is:

1. hsmmaster.key is decrypted with the key from HSM. Now we got our original Master key.
2. Key in HSM is deleted.
3. New key in HSM is created with same name.
4. The Master Key is encrypted with the new key from within the HSM

.. And now the same Master Key is encrypted with a new HSM based key.

Activate HSM through CFG Files

Once the key is on the HSM appliance, you will still need to adjust the configuration files to allow HSM to interact with the Security Manager.

In Defiance DPS 4.3, the configuration settings have all been turned off with the Octothorpe (#) and starts with default settings. To activate and\or change any of the default settings, remove the # from the start of any of the configuration lines and adjust the parameters.

To evoke the HSM functionality in DPS, you will need to adjust the configuration files installed with the DPS installation AFTER running the Setup Tool option for HSM Functionality.

In the Adminiserver.cfg under the Key Management Configuration section, the parameter ***defaultkeyhandler =*** determines if the HSM is used for Key Management. The default setting is "internal".

The Hsm.cfg file is created by running the Setup Tool. The parameter **hsm=** controls if the HSM will be used for encryption of the Master Key.

Of the following examples with their default settings, the first is an excerpt of the *Adminiserver.cfg - Key Management Configuration* section. The second is the complete *Hsm.cfg* file. The last is the excerpts of the *Key Management* section that can be found in each of the *Logserver.cfg, Membersourceserver.cfg, Pepserver.cfg* files.

The highlighted areas are what need to be adjusted for HSM Functionality depending on desired configuration:

Adminserver.cfg

```
# ----------------------------
# Key Management configuration
# ----------------------------
[keymanagement]

# Default key hanndler.
# Use: 'defaultkeyhandler = internal' keys stored in keystore.db
# Use: 'defaultkeyhandler = hsm' keys stored in hsm.
#
#defaultkeyhandler = internal

#hsmconfigfile = <full path>/<file name>
```

HSM.cfg *- created by Setup Tool*

```
# ------------------------
# HSM configuration
# ------------------------
[hsm]
# HSM YES / NO.
hsm = YES

# path to the vendor specific dll to load.
dll = C:\LunaSA\cryptoki.dll

# path to the HSM Encrypted Master key.
masterkeyfile = hsmmaster.key

# tokenid, name of token were key resides
tokenid = <<<Name of HSM Partition to store keys>>>

# HSM key identifier / key label security
keylabel = <<<<Name of Key Label used in configuration setup>>>

# path to the HSM User password file.
userpassword = hsmup.bin
```

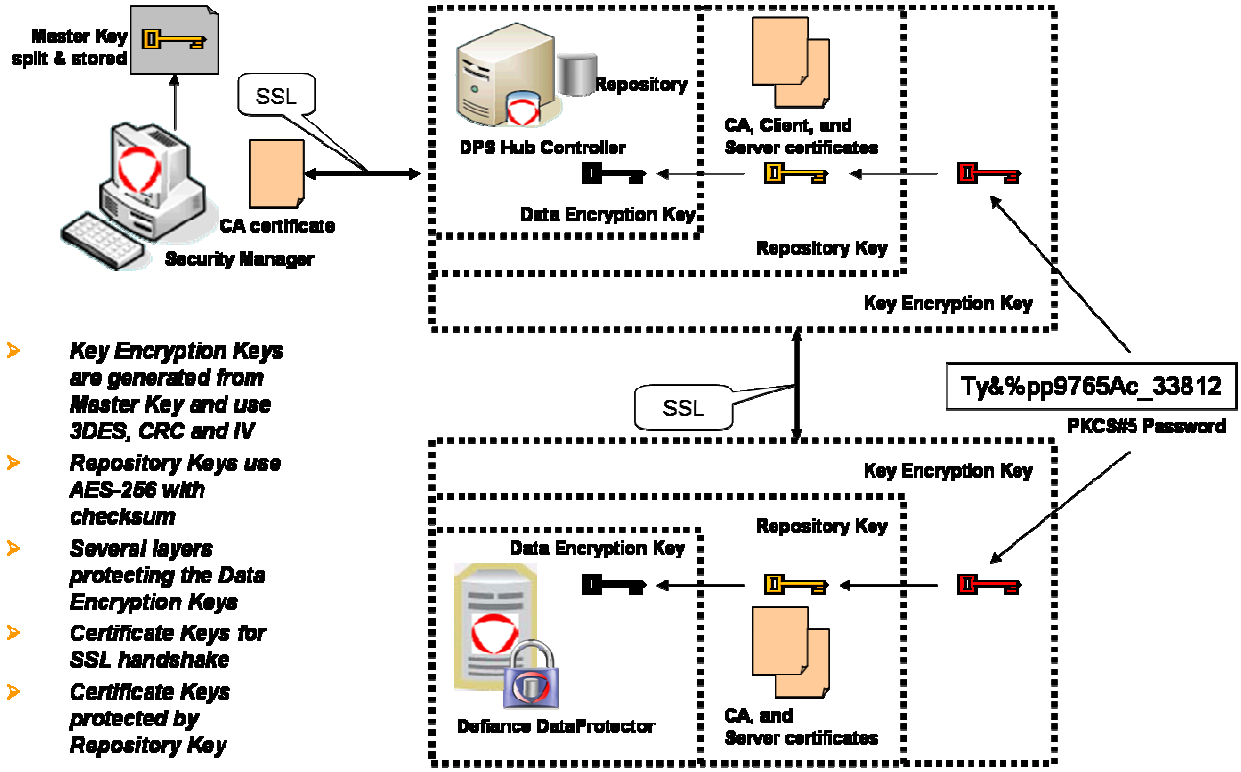
Each of the other configuration files for the Member Server, Pep Server and the Log Server just need to point to the HSM.cfg file:

Logserver.cfg, Membersourceserver.cfg, Pepserver.cfg:

```
# ----------------------------
# Key Management configuration
# ----------------------------
[keymanagement]

hsmconfigfile = <full path>/<file name>
```

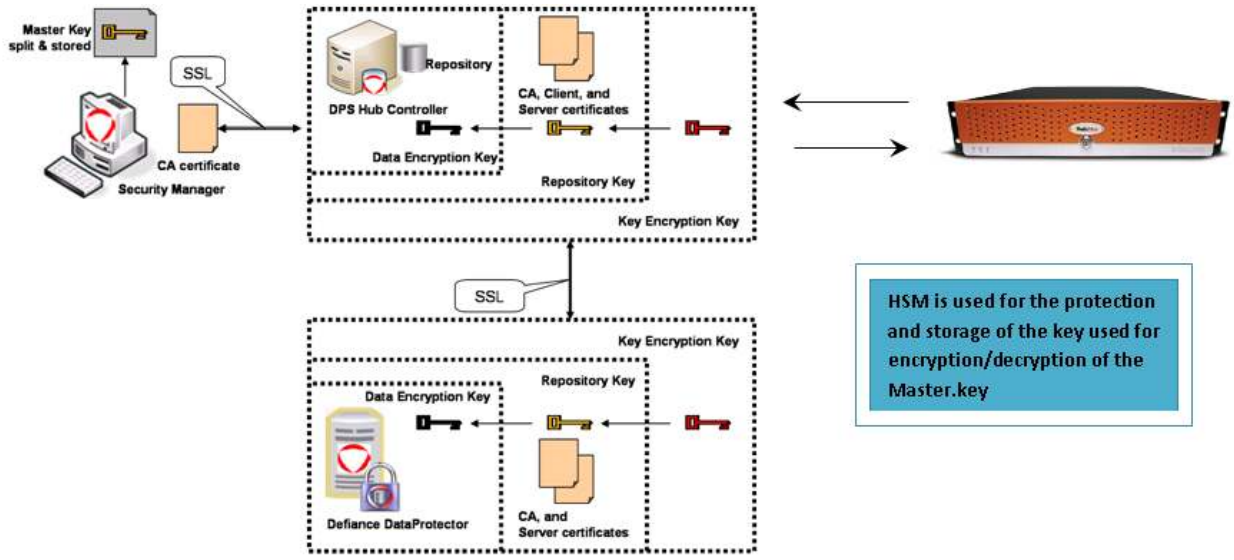
HSM Protection: None



- *Key Encryption Keys are generated from Master Key and use 3DES, CRC and IV*
- *Repository Keys use AES-256 with checksum*
- *Several layers protecting the Data Encryption Keys*
- *Certificate Keys for SSL handshake*
- *Certificate Keys protected by Repository Key*

The standard installation will have the Master Key password encrypted and residing on the Hub Controller. There is no need to run the Setup Tool for the HSM Functionality

HSM Protection: Master Key Encryption



Running the HSM Functionality option from the Setup Tool on the Hub Controller will add the following changes to the DPS setup:

1) A new file will be created in the DPS \data folder: **HSM.cfg**
2) The encryption\decryption key for the Master Key will be created on the HSM.
3) A new key will be created in the DPS \data folder: **hsmmaster.key**

HSM.cfg

In the *HSM configuration* section, set the **hsm=** parameter to *YES*

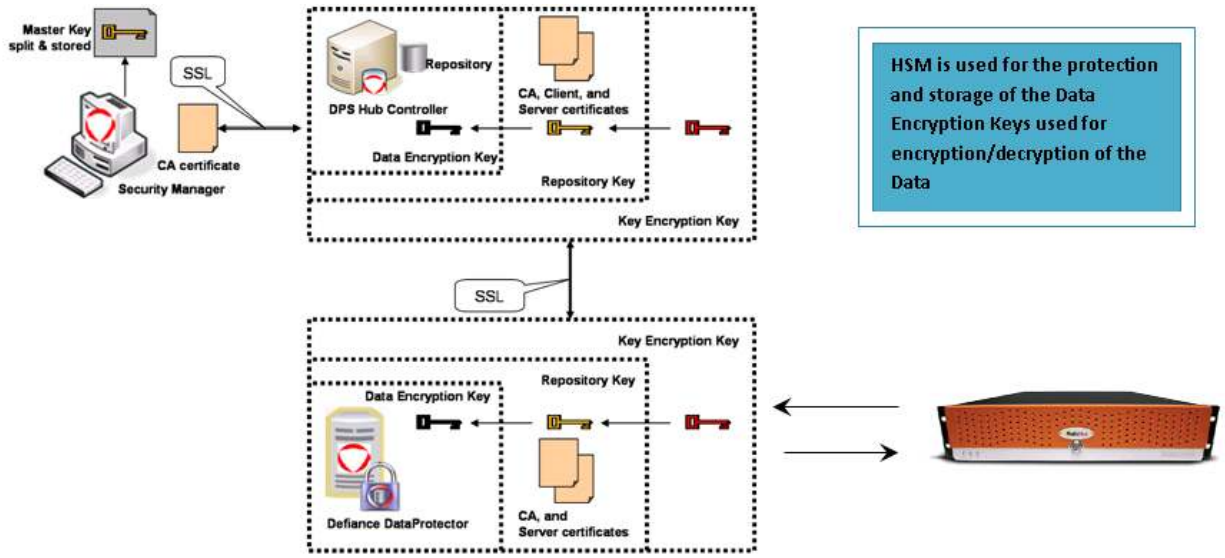
Adminserver.cfg

In the *Key Management configuration* section, you can leave the default setup disabled with the # or if you choose to activate, set the parameter defaultkeyhandler to "internal":

#defaultkeyhandler = internal -Disabled

defaultkeyhandler = internal -Activated

HSM Protection: Data Encryption Keys



HSM.cfg

In the *HSM configuration* section, set the **hsm=** parameter to *NO*

Adminserver.cfg

In the *Key Management configuration* section, set the parameter defaultkeyhandler to "HSM":

defaultkeyhandler = HSM

You will need to configure the *hsmconfigfile p*arameter also in the *Key Management configuration* section with the path to the HSM.cfg file:

*hsmconfigfile = C:/Program Files/Protegrity/Data/hsm.cfg**

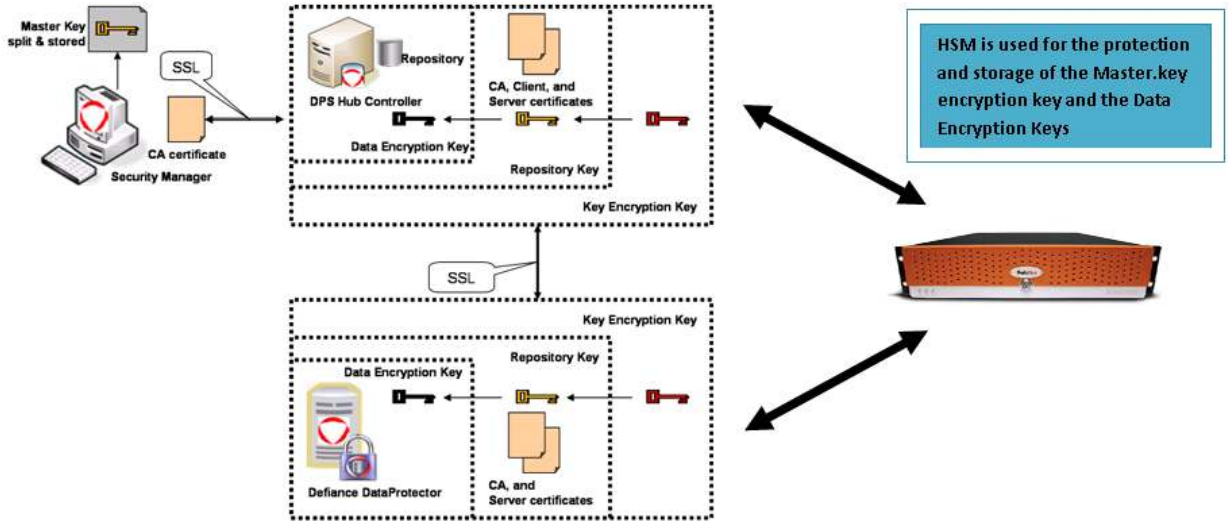
Logserver.cfg, Membersourceserver.cfg, Pepserver.cfg

You will need to configure the *hsmconfigfile p*arameter also in the *Key Management configuration* section with the path to the HSM.cfg file. The HSM.cfg file will need to be copied to each server and then the path filled in on the *hsmconfigfile = parameter*::

*hsmconfigfile = C:/Program Files/Protegrity/Data/hsm.cfg**

***Note:** Paths to hsm.cfg may differ depending on installation

HSM Protection: Master Key and Data Encryption Keys



HSM.cfg

In the *HSM configuration* section, set the **hsm=** parameter to *YES*

Adminserver.cfg

In the *Key Management configuration* section, set the parameter defaultkeyhandler to "HSM":

defaultkeyhandler = HSM

You will need to configure the *hsmconfigfile p*arameter also in the *Key Management configuration* section with the path to the HSM.cfg file:

*hsmconfigfile = C:/Program Files/Protegrity/Data/hsm.cfg**

Logserver.cfg, Membersourceserver.cfg, Pepserver.cfg

You will need to configure the *hsmconfigfile p*arameter also in the *Key Management configuration* section with the path to the HSM.cfg file. The HSM.cfg file will need to be copied to each server and then the path filled in on the *hsmconfigfile = parameter*:

*hsmconfigfile = C:/Program Files/Protegrity/Data/hsm.cfg**

***Note:** Paths to hsm.cfg may differ depending on installation