
Citrix ADC: Integration Guide

THALES LUNA HSM

Document Information

Document Part Number	007-013602-001
Revision	E
Release Date	11 February 2022

Trademarks, Copyrights, and Third-Party Software

Copyright © 2021 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Overview	4
Certified Platforms	4
Prerequisites	5
Set up Citrix ADC virtual appliance	5
Configure Luna HSM	5
Integrating Citrix ADC with Luna HSM	5
Create NTL	6
Generate a key pair and certificate on Luna HSM	8
Add the key pair and certificate to Citrix ADC	9
Create and test load balancing virtual server	9
Add servers	9
Add services	10
Add virtual servers	11
Contacting Customer Support	14
Customer Support Portal	14
Telephone Support	14
Email Support	14

Overview

Citrix ADC is an application delivery controller and load balancing solution. Thales Luna HSM is used to generate and store the private keys that Citrix ADC uses for SSL communication. The benefits of integrating Citrix ADC with Luna HSM include:

- > Secure generation, storage and protection of the crypto private key on FIPS 140-2 level 3 validated hardware.
- > Full life cycle management of keys.
- > Access to the HSM audit trail.
- > Significant performance improvements by off-loading cryptographic operations from servers.

Certified Platforms

The following platforms are certified for integrating Citrix ADC with Luna HSM:

Third Party Details	Luna HSM Version	Luna Firmware Version
Citrix ADC Virtual Appliance (13.1-12.51_nc)	Appliance Version-7.7.1	7.7.1
Citrix ADC Virtual Appliance (13.0-47.24_nc)	Appliance Version-7.3.0	7.3.3
Citrix ADC Virtual Appliance (13.0-41.20_nc)	Appliance Version-7.3.0	7.3.0
Citrix ADC Virtual Appliance (12.1-51.19_nc)	Appliance Version-6.3.0	6.27.0
Citrix NetScaler Virtual Appliance(11.1-47.14_nc)	Appliance Version-5.4.7	6.10.9

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

NOTE: This integration is tested in both HA and FIPS mode.

Prerequisites

Before you proceed with the integration, complete the following processes:

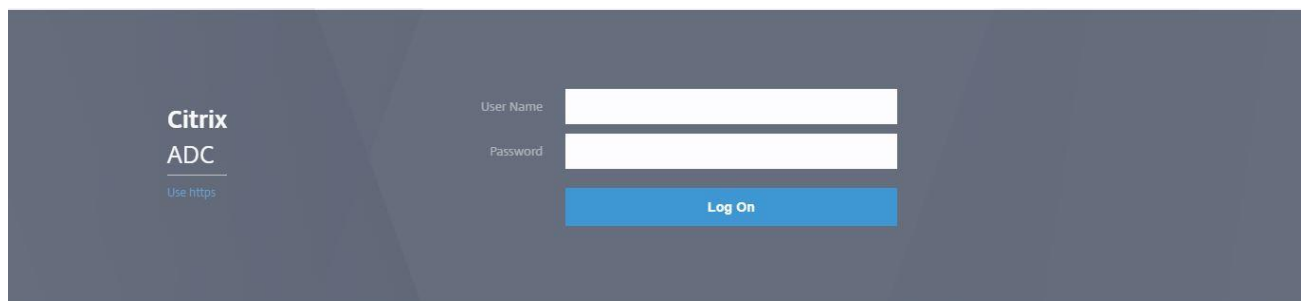
[Set up Citrix ADC virtual appliance](#)

[Configure Luna HSM](#)

Set up Citrix ADC virtual appliance

Use the appropriate virtual image file to deploy the virtual appliance on the VMware. Refer to the [Citrix Product Portal](#) and [Citrix Product Documentation](#) for further information. When your virtual appliance is available on a VMware, access the Citrix ADC Web console through the IP address that was configured during deployment. For example: <http://CitrixADCApplianceIP-Address>.

NOTE: You need a license for Citrix Load Balancing. The Freemium version cannot be used for load balancing.



Configure Luna HSM

Before starting the integration process, ensure that the HSM is configured and a partition is initialized.

NOTE: This integration guide describes steps for creating a Network Trust Link (NTL) between the Citrix ADC host environment and a Luna HSM appliance. Refer to the [Luna HSM documentation](#) for detailed steps on creating HA, initializing the partitions, and initializing various user roles.

Integrating Citrix ADC with Luna HSM

Following are the steps involved in integrating Citrix ADC with Luna HSM that will enable you to generate and store the Citrix ADC SSL communication private keys:

- > [Create NTL](#)
- > [Generate a key pair and certificate on Luna HSM](#)
- > [Add the key pair and certificate to Citrix ADC](#)
- > [Create and test load balancing virtual server](#)

Create NTL

Create a Network Trust Link (NTL) between Luna HSM and Citrix ADC server and configure the Citrix ADC server to access the Luna HSM. To create the NTL:

1. Log in to Citrix Appliance and run **shell** command to get the BSD Shell.

NOTE: For Citrix ADC 13.x.x onwards, skip steps 2 and 3.

2. Copy the required Citrix ADC build containing Luna libraries (for example, build-12.1-51.19_nc_64.tgz) to the **/var** directory on the Citrix ADC Virtual Appliance.

3. Untar the build in the **/var** directory and run the **installns** script.

```
# ./installns
```

4. Navigate to the **/var/safenet** directory and execute the installation script to install the in-built Luna Client available with the appliance version.

```
# ./install_client.sh -v 722
```

Or

```
# ./install_client.sh -v 1030
```

NOTE: 722 and 1030 are the Luna client versions for v7.2.2 and v10.3.0, respectively. You need to change the version number as per the version provided in Citrix ADC Appliance.

NOTE: The Luna Client 6.0.0 provided with the Citrix build does not work in HA mode with Citrix Virtual Appliance.

5. Go to **/var/safenet/config** and run the **safenet_config** file. This script copies the **Chrystoki.conf** file into the **/etc** directory. It also generates a symbolic link **libCryptoki2_64.so** in the **/usr/lib** directory.

```
# cd /var/safenet/config
```

```
# sh safenet_config
```

6. Create an NTL between Citrix ADC and the HSM to communicate securely, as described below:

- a. Change directory to **/var/safenet/safenet/lunaclient/bin** and create a certificate for Citrix ADC.

```
# ./vtl createCert -n <IP address of Citrix ADC>
```

- b. Import the Citrix ADC certificate to Luna HSM.

```
# scp /var/safenet/safenet/lunaclient/cert/client/<IP address of Citrix ADC>.pem <HSM account>@<HSM IP>:
```

- c. Export the Luna HSM certificate to Citrix ADC.

```
# scp <HSM account>@<HSM IP>:server.pem /var/safenet/safenet/lunaclient/cert/server/<HSM IP>.pem
```

- d. Register the Luna HSM certificate on the Citrix ADC appliance.

```
# ./vtl addserver -n <HSM IP> -c /var/safenet/safenet/lunaclient/cert/server/<HSM IP>.pem
```

- e. Log in to Luna Shell and register Citrix ADC as a client on Luna HSM.

```
lunash:> client register -client <client name> -ip <Citrix ADC IP>
```

- f. After registering the client, assign a partition created for Citrix ADC to client.

```
lunash:> client assignPartition -client <Client Name> -partition <Partition Name>
```

- g. On Citrix ADC, verify the NTL connectivity between the Citrix ADC appliance and HSM. At the shell prompt, execute:

```
# ./vtl verify
```

```
root@ns# ./vtl v

The following Luna SA Slots/Partitions were found:

Slot  Serial #          Label
====  =====          =====
    0   1192625854082    citrix
```

7. Exit from shell and log back into ADC CLI and save the configuration.

```
> save ns config
```

```
> save ns config
Done
> |
```

8. Go back to BSD shell and copy the **/etc/Chrystoki.conf** file into the **/var/safenet/config** directory:

```
# cp /etc/Chrystoki.conf /var/safenet/config/
```

This will enable the ADC appliance to start the SafeNet Client processes automatically on reboot

9. Start the SafeNet Gateway client process:

```
# sh /var/safenet/gateway/start_safenet_gw
```

10. Create the **/var/safenet/safenet_is_enrolled** file to signal the ADC appliance to automatically start the SafeNet client processes after reboot:

```
# touch /var/safenet/safenet_is_enrolled
```

11. Reboot the ADC appliance to verify that the processes are started automatically at boot time.

```
# reboot
```

12. After reboot, verify that the SafeNet Gateway client process is running:

```
# ps -aux | grep safenet_gw
```

```
root@ns# ps -aux | grep safenet_gw
root      2226  0.0  0.1 10068  1152  ??  Ss   6:45AM  0:00.00 var/safenet/gateway/safenet_gw
```

Generate a key pair and certificate on Luna HSM

Generate a key pair on Luna HSM using the cmu utility and then create a certificate request using the keys generated. To generate a key pair and certificate:

1. Go to **/var/safenet/safenet/lunaclient/bin** and generate a key pair:

```
# ./cmu generatekeypair -modulusBits=2048 -publicExponent=65537 -sign=T -
verify=T -encrypt=1 -decrypt=1 -wrap=1 -unwrap=1 -label=Citrix_Keys
```

Provide partition password when prompted.

2. Run the cmu utility to list the generated key pair.

```
# ./cmu list
```

Provide partition password when prompted

```
root@ns# ./cmu list
Please enter password for token in slot 0 : *****
handle=188label=Citrix_Keys
handle=182label=Citrix_Keys
```

3. Generate a certificate request.

```
# ./cmu requestcertificate
```

Provide partition password when prompted.

```
root@ns# ./cmu requestcertificate
Please enter password for token in slot 0 : *****
Enter Subject 2-letter Country Code (C) : In N
Enter Subject State or Province Name (S) : UP
Enter Subject Locality Name (L) : Noida
Enter Subject Organization Name (O) : Thales
Enter Subject Organization Unit Name (OU) : HSM
Enter Subject Common Name (CN) : thalesgroup.com
Enter EMAIL Address (E) : abc@def.com
Enter output filename : Citrixcert
```

The certificate request file is saved in **/var/safenet/safenet/lunaclient/bin** directory by default.

4. Get the signed certificate from the trusted CA and copy the certificate to the **/var/safenet/safenet/lunaclient/bin** directory.
5. Import the signed certificate to Luna HSM.

```
# ./cmu import
```

Provide partition password and certificate file when prompted.

```
root@ns# ./cmu import
Please enter password for token in slot 0 : *****
Enter input filename : certnew.cer
```

6. Export the certificate in .pem format from Luna HSM.

```
# ./cmu export
```

Provide partition password and certificate PEM file name when prompted

```
root@ns# ./cmu export
Please enter password for token in slot 0 : *****
Enter output filename : Citrixcert.pem
```

7. Copy the exported certificate to the **/nsconfig/ssl** directory on the ADC.

```
# cp <cert.pem> /nsconfig/ssl/
```


Add the key pair and certificate to Citrix ADC

To add the key and certificate on Citrix ADC:

1. Add the HSM key on Citrix ADC CLI:

```
> add ssl hsmKey <KeyName> -hsmType SAFENET -serialNum <serial number of partition> -password <Partition_password>
```

Note: You can ignore the following error message that you may encounter while adding the key to Citrix: `ERROR: Internal error while adding HSM key.`

2. Verify that the HSM key was added successfully.

```
> show run | grep -i hsm
```

3. Add the HSM certificate-key pair to Citrix ADC.

```
> add ssl certKey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
```

4. Verify that the certificate key-pair was added successfully.

```
> show run | grep -i hsm
```

```
> show run | grep -i hsm
add ssl hsmKey Citrix_Keys -hsmKeyBootTime 100 -hsmType SAFENET -
serialNum 1192625854082 -password
bace4ef2487dc50ba317a95e3b71a91d9c91c20f36e4afb3042a8c713f04e774 -
encrypted -encryptmethod ENCMTHD_3
add ssl certKey Citrixcert -cert "/nsconfig/ssl/Citrixcert.pem" -hsmKey
Citrix_Keys
>
```

Create and test load balancing virtual server

Once you've added the keys and certificate to Citrix ADC, verify that it is working correctly by creating a test load balancing virtual server. For the purpose of this demonstration, Microsoft IIS has been used as the backend server. To create a load balancing virtual server, log on to `<http://CitrixADCWebIP-Address>` and complete the following steps:

- > [Add servers](#)
- > [Add services](#)
- > [Add virtual servers](#)

Add servers

Add a server to configure virtual load balancing. To add a server:

1. Navigate to **Traffic Management->Load Balancing->Servers**.
2. Click **Add** to add the details of the application server.

3. Click **Create** to add a server. The added server appears in the list.

The screenshot shows the 'Create Server' form within the Citrix ADC configuration interface. The top navigation bar includes 'Dashboard', 'Configuration' (selected), 'Reporting', 'Documentation', and 'Downloads'. The form has a title 'Create Server' with a back arrow. It contains the following fields and controls:

- Name***: A text input field containing 'iisserver'.
- IP Address** and **Domain Name**: Radio buttons, with 'IP Address' selected.
- IPAddress***: A text input field containing '10.164.78.157'.
- Traffic Domain**: A dropdown menu with a 'v' icon, and 'Add' and 'Edit' buttons.
- Enable after Creating**: A checked checkbox.
- Comments**: A text input field.
- Create** and **Close** buttons at the bottom.

Add services

Create a service on the server to complete the load balancing operation on failure. To add a service:

1. Navigate to **Traffic Management->Load Balancing->Services**.
2. Click **Add** to add the services.
3. In the server field, add the IP of the machine where your application is already running. Select the protocol and port, as shown in the following image.

The screenshot shows the 'Load Balancing Service' form within the Citrix ADC configuration interface. The top navigation bar is the same as the previous screenshot. The form has a title 'Load Balancing Service' with a back arrow. It contains the following fields and controls:

- Basic Settings**: A section header with a 'Help' button and a right arrow.
- Service Name***: A text input field containing 'iisservice'.
- New Server** and **Existing Server**: Radio buttons, with 'Existing Server' selected.
- Server***: A dropdown menu showing 'iisserver (10.164.78.165)'.
- Protocol***: A dropdown menu showing 'HTTP'.
- Port***: A text input field containing '80'.
- More**: A link to expand the form.
- OK** and **Cancel** buttons at the bottom.

4. Click **OK** to add the service. This will bring up the **Services** page.

5. Verify that the **State** column of the Services Table displays state **UP**. Click **Done**.

The screenshot shows the Citrix ADC Configuration page. The left sidebar has 'Traffic Management' expanded, with 'Load Balancing' and 'Virtual Servers' visible. The main content area is titled 'Services' and shows a table with one service, 'iservice', which is in the 'UP' state. The table has columns for Name, State, IP Address/Domain Name, Port, Protocol, Max Clients, Max Requests, Cache Type, and Traffic Domain.

Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
iservice	UP	10.164.78.165	80	HTTP	0	0	SERVER	0

Add virtual servers

Create and configure a virtual server to act as the load-balancer for the backend server and connect the virtual server to the shared service. To add a virtual server:

1. Navigate to **Traffic Management->Load Balancing->Virtual Servers**.
2. Click **Add**.
3. Enter the Name and IP Address for the Virtual Server. Select the **Protocol** as SSL and then click **OK**.

The screenshot shows the 'Load Balancing Virtual Server' configuration page. The 'Basic Settings' section is active, showing fields for Name, Protocol, IP Address Type, IP Address, and Port. The Name is 'testvs', Protocol is 'SSL', IP Address Type is 'IP Address', IP Address is '10.164.76.40', and Port is '443'. There are 'OK' and 'Cancel' buttons at the bottom.

The **State** column will show as **Down** in the **Basic Settings**. Proceed to bind the service and certificate to bring it **UP**.

4. Click **No Load Balancing Virtual Server Service Binding**. This brings the Service Binding page on to the screen.
5. Click **select service** and then select the service that you've created above. Click the **Bind** button.

6. After service binding, click **Continue**.
7. Click **No Server Certificate**.
8. Select the server certificate exported from Luna HSM and click **Bind**. Click **Continue** and then **Done**.

Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings	
Name	testvs
Protocol	SSL
State	DOWN
IP Address	10.164.76.40
Port	443
Traffic Domain	0

Advanced Settings	
Listen Priority	-
Listen Policy Expression	NONE
Redirection Mode	IP
Range	1
IPset	-
RHI State	PASSIVE
AppFlow Logging	ENABLED
Retain Connections on Cluster	NO
Redirect From Port	-
HTTPS Redirect URL	-

Services and Service Groups	
1 Load Balancing Virtual Server Service Binding	>
No Load Balancing Virtual Server ServiceGroup Binding	>

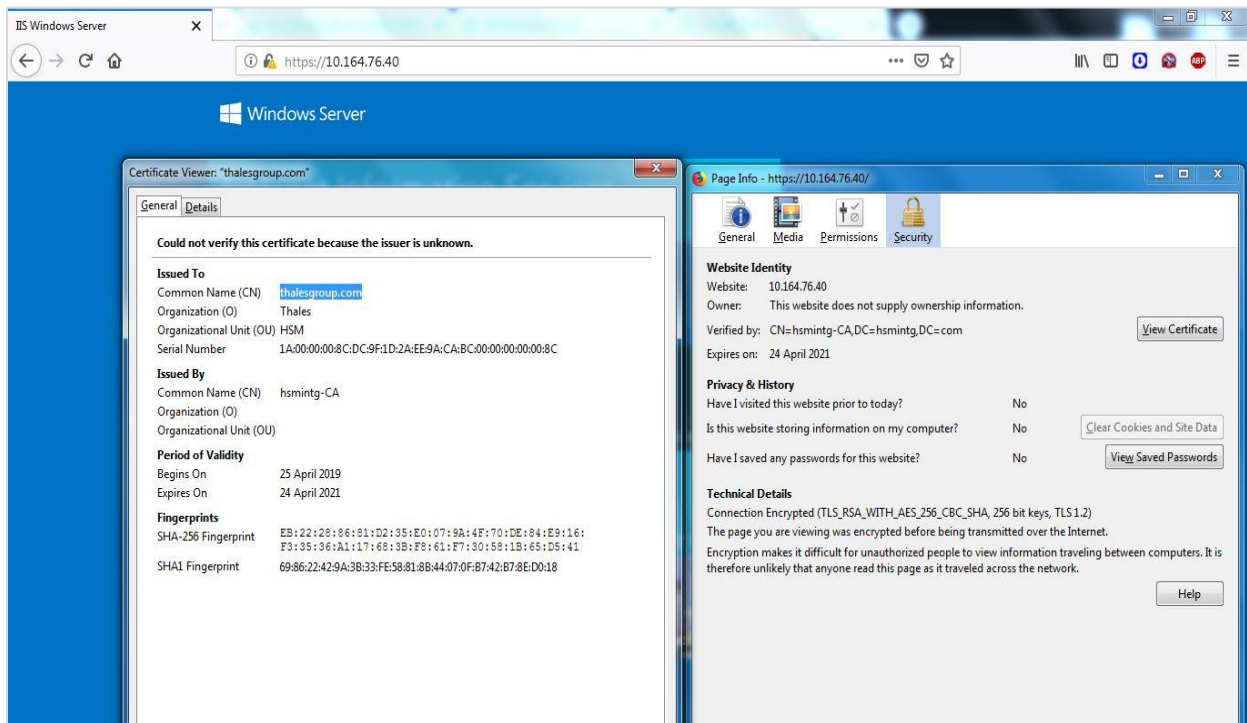
Certificate	
1 Server Certificate	>
No CA Certificate	>

The process of binding the certificate to the service may take a few seconds, after which the **State** and **Effective State** column of the Virtual Server should display **UP**.

Virtual Servers

Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health	Traffic Don
testvs	UP	UP	10.164.76.40	443	SSL	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN	

9. Access the application over HTTPS using the IP of the virtual server on port 443.



Verify the certificate. It should be the same certificate that has been exported from the HSM. This completes the integration of Citrix ADC with Luna HSM.

Contacting Customer Support

If you encounter a problem during this integration, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.