Citrix ADC

INTEGRATION GUIDE

SAFENET LUNA HSM
Trademarks, Copyrights, and Third-Party Software
© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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.

Disclaimer
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.
Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.
## CONTENTS

**PREFACE** .......................................................................................................................... 5  
Scope ........................................................................................................................................ 5  
Document Conventions ............................................................................................................. 5  
Command Syntax and Typeface Conventions ........................................................................ 6  
Support Contacts ..................................................................................................................... 7  
Customer Support Portal ......................................................................................................... 7  
Telephone Support .................................................................................................................. 7  
Email Support .......................................................................................................................... 7  

**CHAPTER 1:  Introduction** ............................................................................................. 8  
Overview ................................................................................................................................ 8  
Third Party Application Details ............................................................................................... 8  
Supported Platforms ............................................................................................................... 8  
Prerequisites ........................................................................................................................... 9  
Setup the Citrix ADC Virtual Appliance ............................................................................... 9  
Configure the SafeNet Luna HSM ......................................................................................... 9  

**CHAPTER 2:  Integrating Citrix ADC with a SafeNet Luna HSM** .................................. 10  
Creating the NTL .................................................................................................................... 10  
Generating a Key Pair and Certificate on SafeNet Luna HSM ............................................... 12  
Adding the Key Pair and Certificate to Citrix ADC ............................................................ 13  
Creating a Test Load Balancing Virtual Server .................................................................... 13  
Adding Servers ...................................................................................................................... 14  
Adding Services ..................................................................................................................... 14  
Adding Virtual Servers ......................................................................................................... 15
PREFACE

This document guides administrators through the steps for integrating Citrix ADC with a SafeNet Luna HSM.

Scope

This document outlines the steps to integrate Citrix ADC (formerly Citrix NetScaler) with a SafeNet Luna HSM. The SafeNet Luna HSM is used to generate and store the private keys that Citrix ADC uses for SSL communication when load balancing.

This integration also provides a sample load balancing configuration for demonstration purposes.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION! Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

**WARNING** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.
## Command Syntax and Typeface Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>The bold attribute is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>&gt; Command-line commands and options (Type <code>dir /p</code>.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Button names (Click <strong>Save As</strong>.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Check box and radio button names (Select the <strong>Print Duplex</strong> check box.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Window titles (On the <strong>Protect Document</strong> window, click <strong>Yes</strong>.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Field names (<strong>User Name</strong>: Enter the name of the user.)</td>
</tr>
<tr>
<td></td>
<td>&gt; Menu names (On the <strong>File</strong> menu, click <strong>Save</strong>.) (Click <strong>Menu &gt; Go To &gt; Folders</strong>.)</td>
</tr>
<tr>
<td></td>
<td>&gt; User input (In the <strong>Date</strong> box, type <strong>April 1</strong>.)</td>
</tr>
<tr>
<td><strong>italic</strong></td>
<td>The italic attribute is used for emphasis or to indicate a related document. (See the Installation Guide for more information.)</td>
</tr>
<tr>
<td>Double quote marks</td>
<td>Double quote marks enclose references to other sections within the document.</td>
</tr>
<tr>
<td><code>&lt;variable&gt;</code></td>
<td>In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.</td>
</tr>
<tr>
<td><code>[ optional ]</code></td>
<td>Square brackets enclose optional keywords or <code>&lt;variables&gt;</code> in a command line description. Optionally enter the keyword or <code>&lt;variable&gt;</code> that is enclosed in square brackets, if it is necessary or desirable to complete the task.</td>
</tr>
<tr>
<td><code>[ &lt;optional&gt; ]</code></td>
<td>Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.</td>
</tr>
<tr>
<td>`{ a</td>
<td>b</td>
</tr>
</tbody>
</table>
Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto 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 Gemalto 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 where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database 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 Gemalto 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@gemalto.com.
CHAPTER 1: Introduction

Overview

Citrix ADC is an application delivery controller and load balancing solution. The SafeNet 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 a SafeNet Luna HSM include:

- Full life cycle management of the keys.
- Access to the HSM audit trail.
- Significant performance improvements by off-loading cryptographic operations from servers.

Third Party Application Details

This integration guide uses the following third party applications:

- Citrix ADC (formerly Citrix NetScaler)

**NOTE:** You require a VPX Citrix License to access the Load Balancing feature.

Supported Platforms

**SafeNet Luna HSM:** SafeNet 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. SafeNet Luna Network HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

<table>
<thead>
<tr>
<th>Third Party Details</th>
<th>SafeNet Appliance version</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ADC Virtual Appliance (13.0-41.20_nc)</td>
<td>Appliance Version- 7.3.0-165</td>
<td>7.3.0-34</td>
</tr>
<tr>
<td>Citrix ADC Virtual Appliance (12.1-51.19_nc)</td>
<td>Appliance Version- 6.3.0-1048</td>
<td>6.27.0</td>
</tr>
</tbody>
</table>
Prerequisites

Before you proceed with the integration, complete the following:

Setup the 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, perform the following steps:

> Access the Citrix ADC Web console through the IP address that was configured during deployment. For example: <http://CitrixADCWebIP-Address>.

Configure the SafeNet Luna HSM

Before you get started ensure that the HSM is configured and has an initialized partition.

NOTE: The integration guide details creating a Network Trust Link (NTL) between the Citrix ADC host environment and the SafeNet Luna HSM appliance.
CHAPTER 2: Integrating Citrix ADC with a SafeNet Luna HSM

To Integrate Citrix ADC with the SafeNet Luna HSM to generate and store the Citrix ADC SSL communication private keys complete the following:

> Creating the NTL
> Generating a Key Pair and Certificate on SafeNet Luna HSM
> Adding the Key Pair and Certificate to Citrix ADC
> Creating a Test Load Balancing Virtual Server

Creating the NTL

Create the Network Trust Link (NTL) between the SafeNet Luna HSM and the Citrix ADC server and configure the Citrix ADC server to access the SafeNet Luna HSM.

To create the NTL

**NOTE:** For Citrix ADC 13.x.x skip step 1 and 2 given below.

1. 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.

2. Untar the build in the var directory and run the installns script.
   
   # ./installns

3. Navigate to the /var/safenet directory and execute the installation script.
   
   # ./install_client.sh -v 722

   **NOTE:** Where 722 is the Luna client version for v7.2.2. Update the label according to your Luna client version. The SafeNet Luna Client 6.0.0 provided with the Citrix build does not work in HA mode with Citrix Virtual Appliance.

4. 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

5. Create an NTL between Citrix ADC and the HSM in order to communicate securely.
   
   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. Copy the certificate to the HSM.
# scp /var/safenet/safenet/lunaclient/cert/client/<IP address of Citrix ADC>.pem <HSM account>@<HSM IP>

c. Copy the certificate and key from the HSM to the ADC.
# scp <HSM account>@<HSM IP>:server.pem /var/safenet/safenet/lunaclient/server_<HSM IP>.pem

d. Register the ADC on the SafeNet HSM.
# client register -client <client name> -ip <Citrix ADC IP>

e. Assign the client a partition from the partition list.
# client assignPartition -client <Client Name> -par <Partition Name>

f. Register the HSM with its certificate on the SafeNet Luna Client.
#. ./vtl addserver -n <HSM IP> -c /var/safenet/safenet/lunaclient/server_<HSM IP>.pem

g. Verify the NTL connectivity between the Client and HSM. At the shell prompt, type:
#. ./vtl verify

h. Exit and log back into ADC CLI and save the configuration.
# save ns config

i. Go back to BSD shell and copy the /etc/Chrystoki.conf file into the /var/safenet/config directory to allow the ADC to start the SafeNet Client processes automatically on reboot:
# cp /etc/Chrystoki.conf /var/safenet/config/

j. Start the SafeNet Gateway client process:
# sh /var/safenet/gateway/start_safenet_gw

k. Create the /var/safenet/safenet_is_enrolled file to signal the ADC to automatically start the SafeNet client processes after reboot:
# touch /var/safenet/safenet_is_enrolled

l. Reboot the ADC to verify that the processes are started automatically at boot time.
# reboot

m. After reboot, verify the SafeNet Gateway client process is running:
# ps -aux | grep safenet_gw
Generating a Key Pair and Certificate on SafeNet Luna HSM

Generate a key pair on the SafeNet 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 gen -modulusBits=2048 -publicExponent=65537 -sign=T -verify=T -
   encrypt=1 -decrypt=1 -wrap=1 -unwrap=1 -label=Citrix_Keys
   ```

2. Run `cmu list` to list the generated key pair.
   
   ```
   # ./cmu list
   ```

3. Generate a certificate request.
   
   ```
   # ./cmu requestcertificate
   ```

Certificate Request file is by default saved in `/var/safenet/safenet/lunaclient/bin`

4. Get the Signed certificate from the trusted CA and copy the certificate to the `/var/safenet/safenet/lunaclient/bin` directory.

5. Import the certificate.
   
   ```
   # ./cmu import
   ```

   
   # ./cmu export
   
   Enter the output file name.

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

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

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

Adding the Key Pair and Certificate to Citrix ADC

Add the newly generated keys and certificates to Citrix ADC.

To add the key and certificate on Citrix ADC

1. Add the HSM key on the Citrix ADC CLI.

   # add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial number of partition> -password <Partition_password>

2. Add the HSM certificate-key pair on the Citrix ADC.

   # add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>

3. Verify the HSM key and certificate key-pair were added successfully.

   # show run | grep -i hsm

   > show run | grep -i hsm
   add ssl hsmKey Citrix_keys -hsmKeyRootTime 100 -hsmType SAFENET -serialNum 1192625854082 -password bace4ef2487dc50ba317e95e3b71e91d9c91c20f36e4afb3042a8c713f04e774 -encrypted -encryptmethod ENCMTHD_3
   add ssl certKey Citrixcert -cert "/nsconfig/ssl/Citrixcert.pem" -hsmKey Citrix_keys

Creating a Test Load Balancing Virtual Server

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

> Adding Servers
> Adding Services
> Adding Virtual Servers
Adding Servers
Add a server to configure virtual load balancing.

To add servers
1. Navigate to Traffic Management -> Load Balancing -> Servers
2. Click Add to add the Details of the application server.
3. Click Create to add the server. The added server displays in the list.

Adding Services
Create a service on the server to complete the load balancing operation on failure.

To add services
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 Screen shot.
Click **OK** to add the service.

The Services page displays.

4. Verify that the **State** column of the Services Table displays state **UP**.

**Adding 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 virtual servers**

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

The Virtual Server generates and the State column in the Basic Settings should display Down.

4. Click No Load Balancing Virtual Server Service Binding.

The Service Binding page displays.

5. Click select service and select the service created above. Click the Bind button.

6. After service binding, click Continue.

7. Click No Server Certificate.

8. Select the recently generated Server Certificate and click Bind. Click Continue and then Done.
9. After Successful Binding of Certificate and service the **State and Effective State** column of the Services Table should display state **UP**.
10. Access the application over HTTPS using the IP of the virtual server on port 443. Verify the Certificate.

This completes the Integration of Citrix ADC with SafeNet Luna HSM.