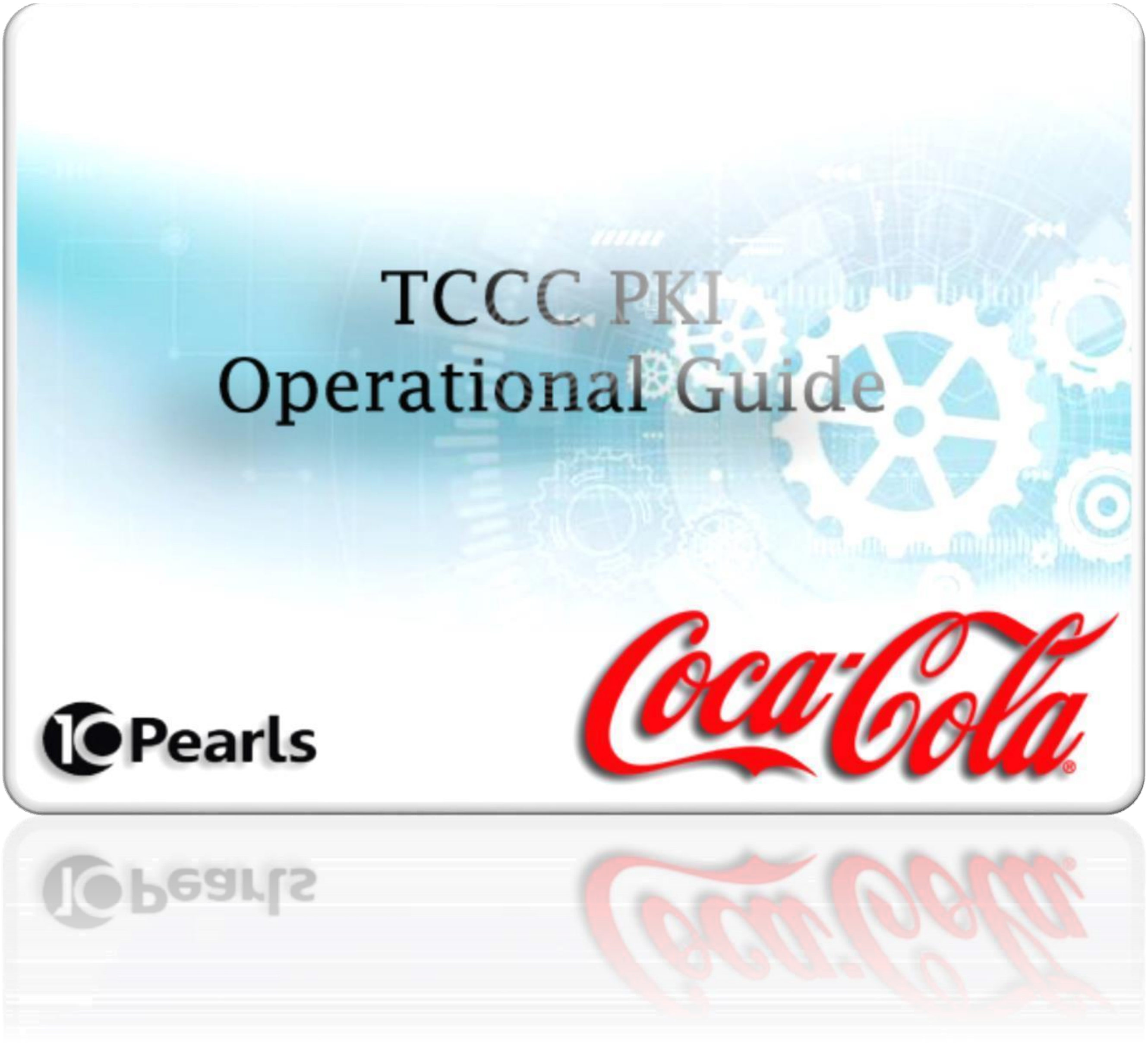
TCCC PKI Operations Guide



Use and Disclosure of Data

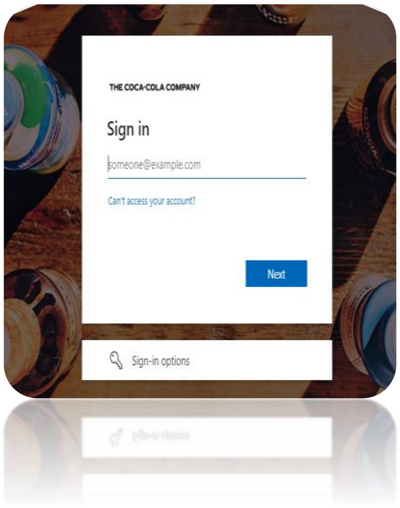
This document is confidential and is not to be disclosed outside of 10Pearls or The Coca-Cola Company.

Setting Up Citrix Workspace

Connecting to Citrix Cloud VDI - Web browser only

Step 1 : In Web browser navigate and login to https://tcccvdi.cloud.com/

{Log in with KO Email & Password } {MFA by SMS or Authenticator App} { Select “Use web browser” }



THE COCA-COLA COMPANY

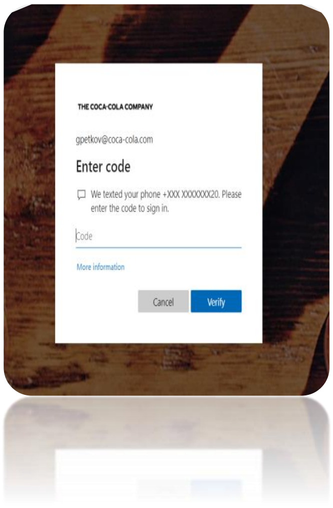
Sign in

someone@example.com

Can't access your account?

Next

Sign-in options



THE COCA-COLA COMPANY

gpetkov@coca-cola.com

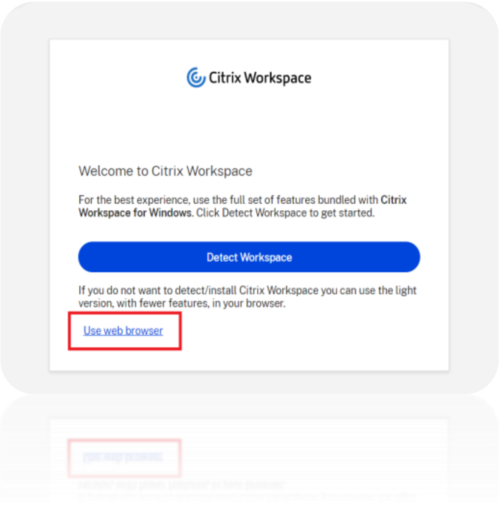
Enter code

We texted your phone +XXX XXXXXXX20. Please enter the code to sign in.

Code

More information

Cancel Verify



Citrix Workspace

Welcome to Citrix Workspace

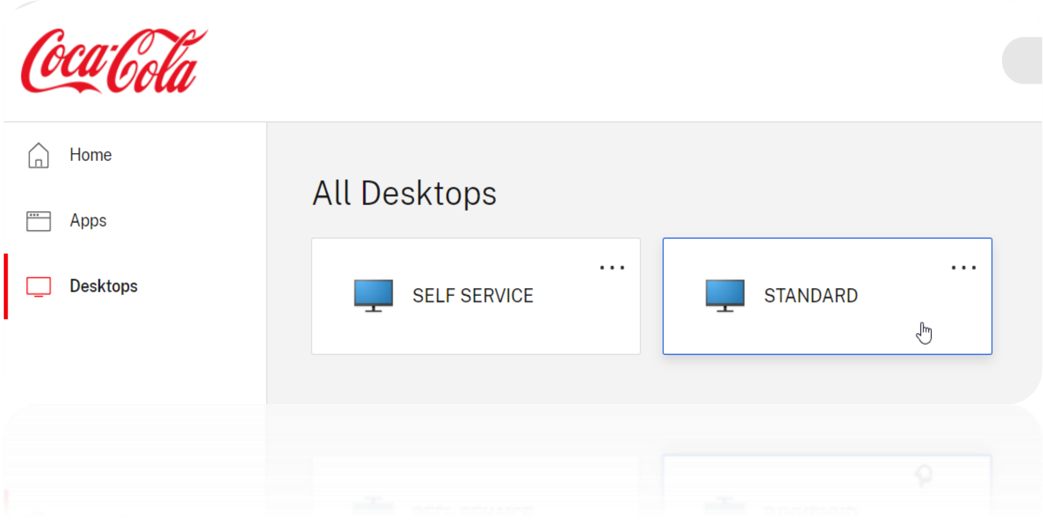
For the best experience, use the full set of features bundled with **Citrix Workspace for Windows.** Click Detect Workspace to get started.

Detect Workspace

If you do not want to detect/install Citrix Workspace you can use the light version, with fewer features, in your browser.

Use web browser

Step 2: Launch your Server and you are good to go!



Home

Apps

Desktops

All Desktops

SELF SERVICE

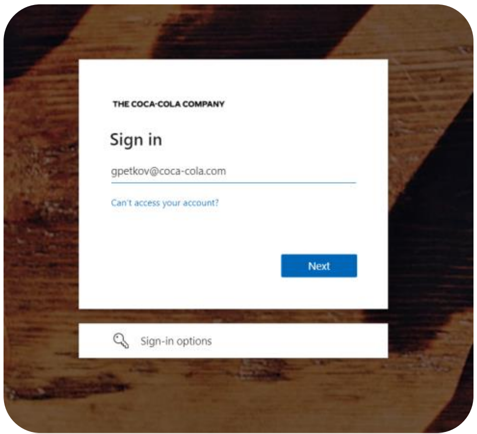
STANDARD

Connecting to Citrix Cloud VDI - Using Citrix Workspace

Step 1: Download and install Citrix Workspace on your device - Citrix Workspace App Downloads - https://www.citrix.com/downloads/workspace-app/

Step 2: In Web browser navigate and login to https://tcccvdi.cloud.com/

Log in with KO Email & Password



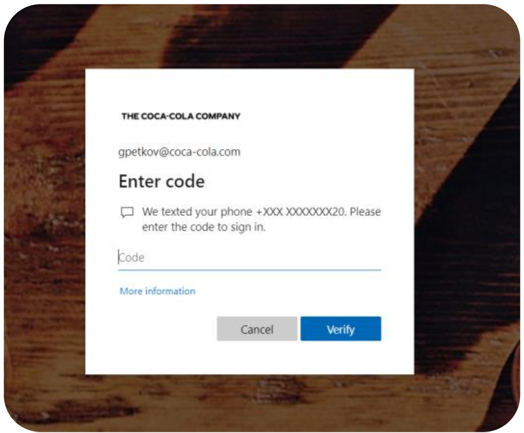
THE COCA-COLA COMPANY

Sign in

gpetkov@coca-cola.com

Can't access your account?

MFA by SMS or Authenticator App



THE COCA-COLA COMPANY

gpetkov@coca-cola.com

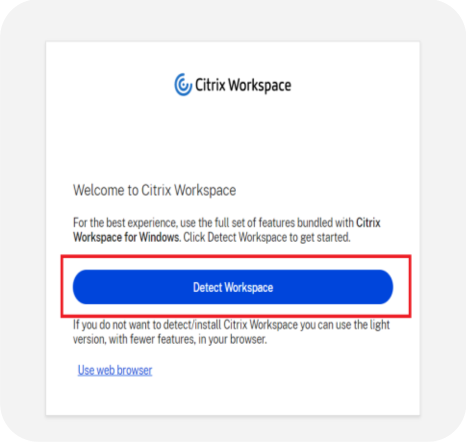
Enter code

We texted your phone +XXX XXXXXXX20. Please enter the code to sign in.

Code

More information

Select "Detect Workspace"



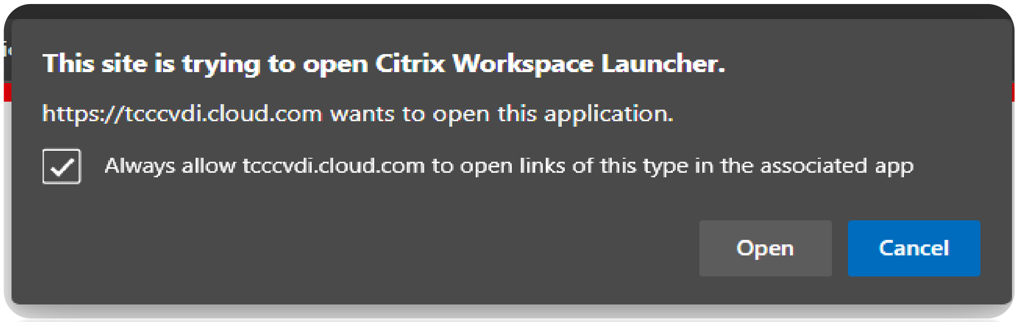
Citrix Workspace

Welcome to Citrix Workspace

For the best experience, use the full set of features bundled with **Citrix Workspace for Windows.** Click Detect Workspace to get started.

If you do not want to detect/install Citrix Workspace you can use the light version, with fewer features, in your browser.

Tick and allow browser to start Citrix Workspace each time

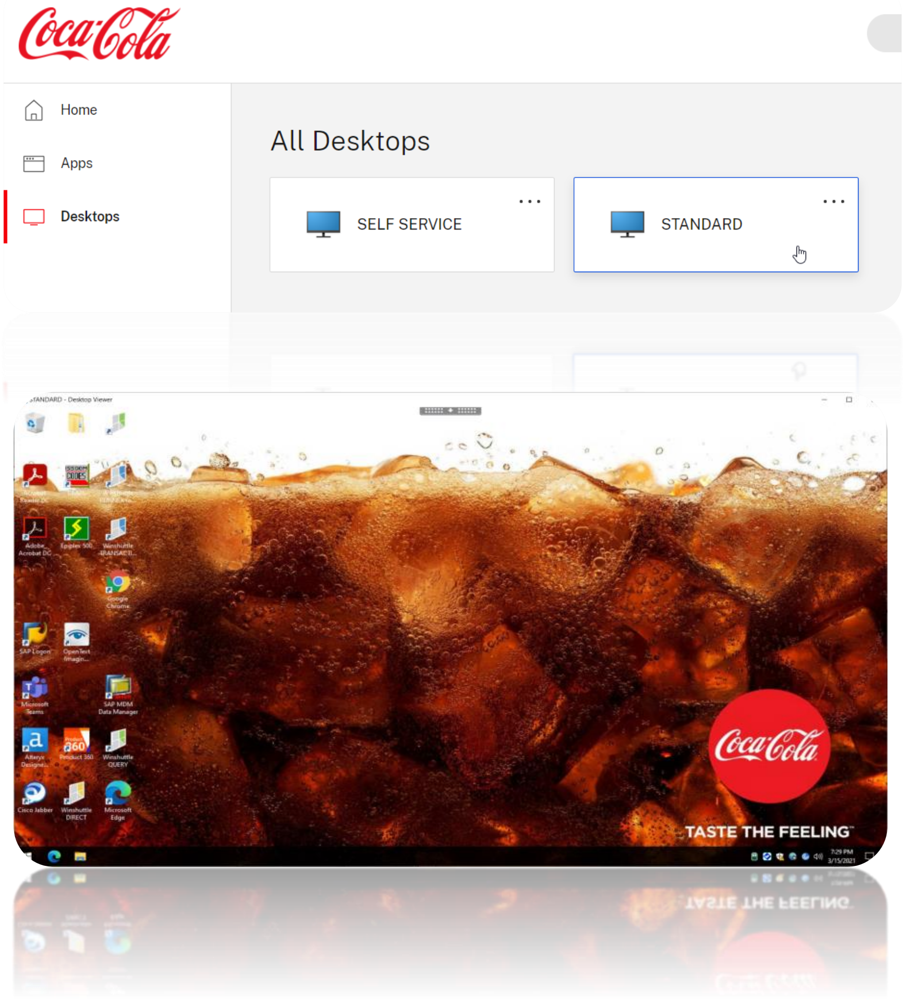


This site is trying to open Citrix Workspace Launcher.

https://tcccvdi.cloud.com wants to open this application.

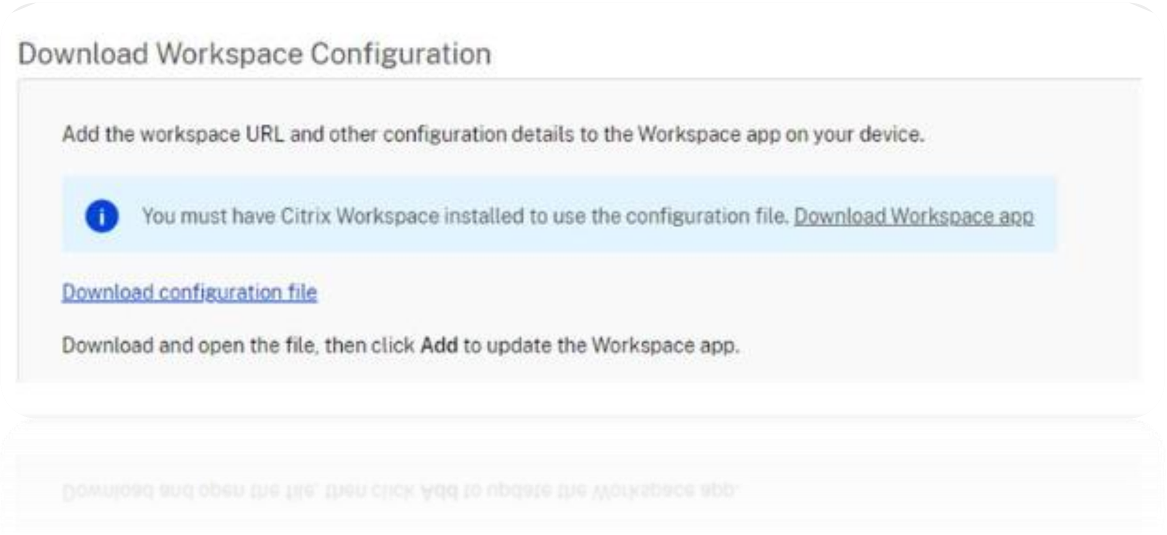
☑ Always allow tcccvdi.cloud.com to open links of this type in the associated app

Step 3: Launch your desktop



Download Workspace configuration file from there and start working with CITRIX Workspace App

https://tcccvdi.cloud.com/Citrix/StoreWeb/#/settings/advanced



Download Workspace Configuration

Add the workspace URL and other configuration details to the Workspace app on your device.

You must have Citrix Workspace installed to use the configuration file. Download Workspace app

Download configuration file

Download and open the file, then click **Add** to update the Workspace app.

--End of the Installations

Coca-Cola Activities:

We performed Coca-Cola activates twice in a day, one at 4am and other at 4pm.

1- We send email to client from Monday to Friday.
2- Saturday and Sunday we only send email internally at devops@10pearls.com.
3- Screenshots of the activities which we performed on daily basis and will only send at devops@10pearls.com for our own records.

To Begin with Activities:

1- We have 2 environments i.e., Prod servers and Pre-Prod Servers.
2- In Both environments the total number of the servers are 37 from Central US and East US respectively.

Manual Checks

While standard server and service monitoring exists for the Coca-Cola Company's PKI environment per the TCCC PKI Design Document (including Microsoft System Center components and SNMP), the following list of regular checks and maintenance items should be performed daily by the PKI Operations Team.

Daily manual tasks consist of connectivity tests, event log checking, CRL checking, and HSM connectivity checking that are performed to ensure that the servers, web interfaces, and certificate services are functional.

If any of these checks do not result in the expected outcome, create and file an incident per the section "Creating Incidents" below. Assign the incident to Peter Hesse (o44419). Additionally, reach out directly to indicate that there is an issue by email (tccc-pki-support@10pearls.com).

Over time this document will be updated to provide additional information about how to diagnose and resolve these issues but at first, establishing these incidents allows us to make changes to the systems to resolve any issues

Start with Production Environment

From Central Location Prod Enrollment Server 1 - zwppkia0001

- **Go to Start Menu bar and type PKIVIEW.MSC –** Once PKIVIEW.MSC opened, check all the certificate are in **OK** status
- If any CA status shown as **ERROR,** then we need to troubleshoot accordingly
- **Type Services in search box –** Services will be opened, check **NFast** and **World Wide Web Services**, both services should be in running state.
- **Type Event Viewer in search box - Event** Viewer will be opened. In Custom we need to check filters for **System** and **Application** **Check filters.**
  - **Logged** – Last 24 hours
  - **Event Level –** Make sure to checked on Critical, Warning and Error
  - **By Source -** CertificateServicesClientAutoEnrollment
  - **Event ID -** 6,13

Go to CMD, Go to this path C:\Program Files (x86) \nCipher\nfast\bin> and run the command nfkminfo and then hit enter and make sure all 2 modules should be OK in status, else we need to troubleshoot accordingly.

Go to RUN and Type CMD go to the path E:\tools\openssl-1.0.2o-x64_86-win64> and run these requests and check all requests status are in OK else we need to troubleshoot and fix. These batch files are for Prod OCSP.

- **TestOCSP1.bat**
- **TestOCSP2.bat**
- **TestOCSP3.bat**
- **TestOCSP4.bat**
- **TestLB1.bat**
- **TestLB2.bat**

NOTE - From the same path you can also check OCSP's Status for Pre-Prod by Running the mentioned below batch files name.

- **TestTestOCSP1.bat**
- **TestTestOCSP2.bat**
- **TestTestOCSP3.bat**
- **TestTestOCSP4.bat**
- **TestTestLB1.bat**
- **TestTestLB2.bat**

Prod Issuing CA 1 - zwppkia0002

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **nFast Server**
- **Type Event Viewer in Search Box and hit enter.**

In Custom we need to check filters for **System** and **Application** **Check filters.**

- **Logged – Last 24 hours**
- **Event Level – Make sure to checked on Critical, Warning and Error**
- **By Source – Certification Authority**
- **Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31,32, 33, 786, 789, 794, 795, 796, 800,801.**

Type CMD in search box and go to this path C:\Program Files (x86) \nCipher\nfast\bin> as need to check some Ip to be responded

Anonkneti 10.114.128.11
Anonkneti 10.114.130.11
Anonkneti 10.114.160.11

Prod Issuing CA 2 - zwppkia0003

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **nFast Server**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**
  - **Logged – Last 24 hours**
  - **Event Level – Make sure to checked on Critical, Warning and Error**
  - **By Source – CertificationAuthority**
  - **Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801**

Prod Issuing CA 3 - zwppkia0004

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **nFast Server**
- **Type Event Viewer in Search Box and hit enter.** In

  Custom we need to check filters for **System** and **Application** **Check filters.**

  - **Logged – Last 24 hours**
  - **Event Level – Make sure to checked on Critical,**
  - **Warning and Error 15- By Source – CertificationAuthority**
  - **16- Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801**

Prod OCSP 1 - zwppkia0005

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **nFast Server**
  - ✓ **W3SVC**
  - ✓ **OcspSvc** ✓
- **Type Event Viewer in Search Box and hit enter.** In

  Custom we need to check filters for **System** and **Application** **Check filters.**

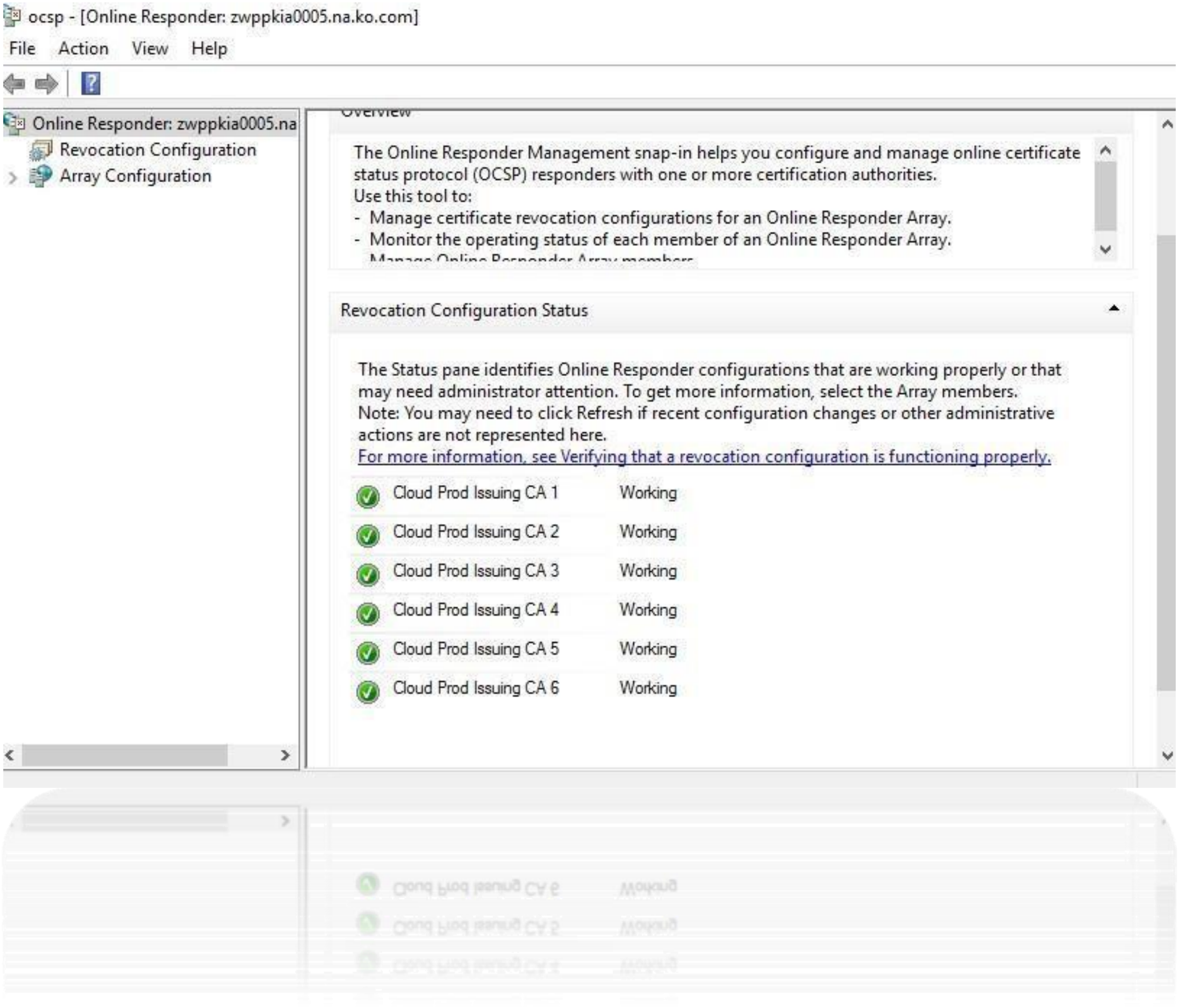
  - **Logged – Last 24 hours**
  - **Event Level – Make sure to checked on Critical, Warning and Error**
  - **By Source - nCipherCSP, nCipherCSP, Online Responder, OnlineResponderRevocationProvider,**

OnlineResponderWebProxy

- **Event ID - 16,17,18,20,21,22,23,25,26,27,29,31,33,34,35**

Type Online Responder in Search Box and hit enter.

Make sure all revocation Configuration status show as GREEN else we need to troubleshoot


ocsp - [Online Responder: zwppkia0005.na.ko.com]
File
Action
View
Help
Online Responder: zwppkia0005.na
Revocation Configuration
Array Configuration
Overview
Revocation Configuration Status

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

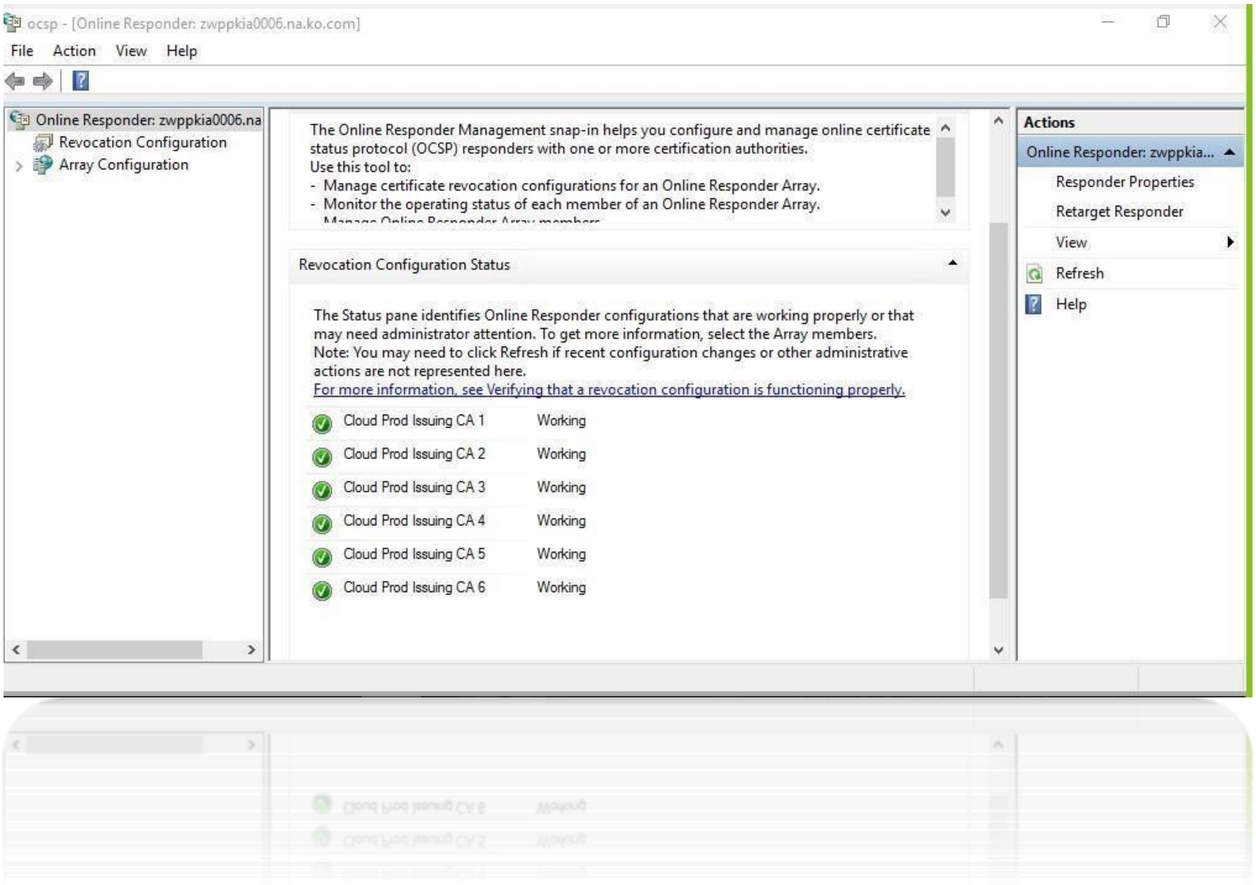
✓	Cloud Prod Issuing CA 1	Working
✓	Cloud Prod Issuing CA 2	Working
✓	Cloud Prod Issuing CA 3	Working
✓	Cloud Prod Issuing CA 4	Working
✓	Cloud Prod Issuing CA 5	Working
✓	Cloud Prod Issuing CA 6	Working

Prod OCSP 2 - zwppkia0006

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **nFast Server**
  - ✓ **W3SVC**
  - ✓ **OcspSvc** ✓
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**
  - **Logged – Last 24 hours**
  - **Event Level – Make sure to checked on Critical, Warning and Error**
  - **By Source – nCipher CSP, nCipherCSP, OnlineResponder,**
  - **OnlineResponderRevocationProvider,**
  - **OnlineResponderWebProxy**
  - **Event ID-**
  - **16,17,18,20,21,22,23,25,26,27,29,31,33,34,35**

Type OnlineResponder in Search Box and hit enter.

Make sure all revocation Configuration status show as GREEN else we need to troubleshoot



The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

✓ Cloud Prod Issuing CA 1	Working
✓ Cloud Prod Issuing CA 2	Working
✓ Cloud Prod Issuing CA 3	Working
✓ Cloud Prod Issuing CA 4	Working
✓ Cloud Prod Issuing CA 5	Working
✓ Cloud Prod Issuing CA 6	Working

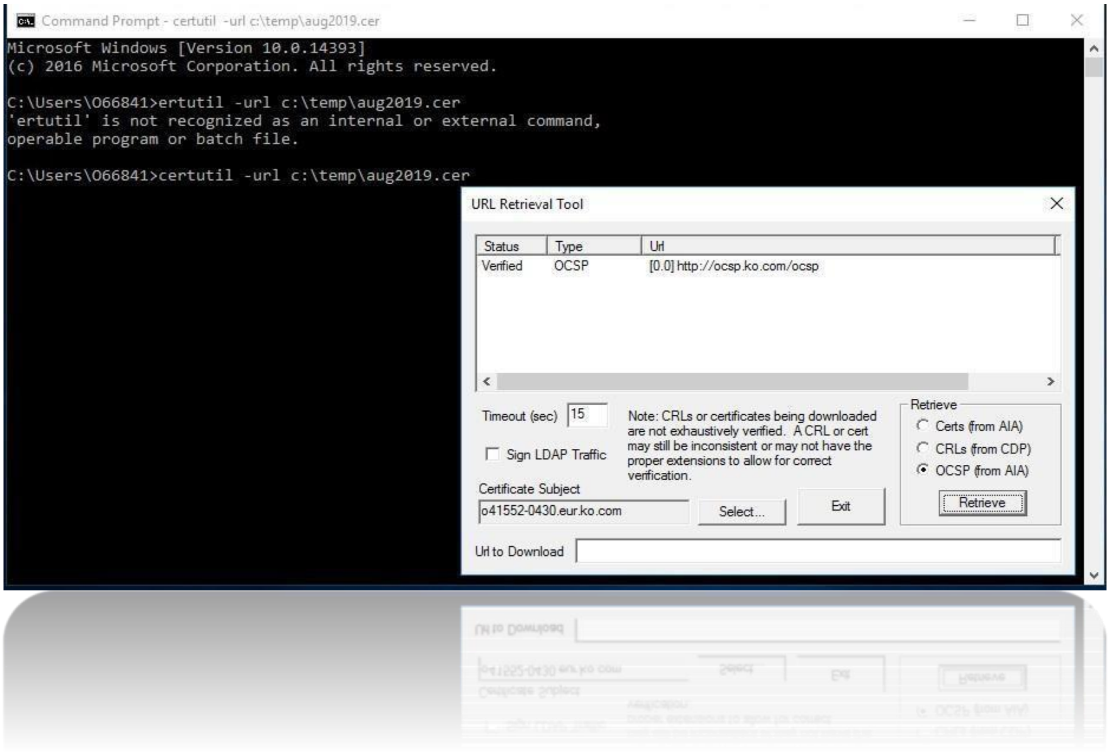
Prod Web Server 1 - zwppkia0007

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **W3SVC**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**
  - **Logged – Last 24 hours**
  - **Event Level – Make sure to checked on Critical, Warning and Error**
  - **By Source – CertificationAuthorityClient-CertCli**

- **Event ID- 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801**

Prod Venafi 1 - zwppkia0015

- Type Services in Search box and hit enter.
- We need to check below services and all services should be in running state
  - ✓ VenafiLogServer
  - ✓ VED
- Type CMD in Search box and hit enter.
- **C:\Users\O51950>**certutil -url c:\temp\aug2019.cer go to this path and hit enter.
- A URL retrieval tool will be opened, and you need to check OCSP from AIA from the retrieval section right below from the box and it will show the verified status.



Command Prompt - certutil -url c:\temp\aug2019.cer

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\O66841>ertutil -url c:\temp\aug2019.cer
'ertutil' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\O66841>certutil -url c:\temp\aug2019.cer
```

URL Retrieval Tool

Status	Type	Url
Verified	OCSP	[0.0] http://ocsp.ko.com/ocsp

Timeout (sec): 15

□ Sign LDAP Traffic

Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

Retrieve
○ Certs (from AIA)
○ CRLs (from CDP)
● OCSP (from AIA)

Certificate Subject: o41552-0430.eur.ko.com

Url to Download:

Prod Venafi 2 - zwppkia0016

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **VenafiLogServer**
  - ✓ **VED**

Prod Venafi DB - zwppkid0017

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **MSSQLSERVER**
  - ✓ **SQLSERVERAGENT**

From Central Location Prod Enrollment Server 2 - zwppkia0008

- **To go Search Box and type PKIVIEW.MSC –** Once PKIVIEW.MSC opened, check all the certificate are in **OK** status
- If any CA status shown as **ERROR,** then we need to troubleshoot accordingly
- **Type Services in search box –** Services will be opened, check **nfast** and **World Wide Web Services**, both services should be in running state.
- **Type Event Viewer in search box - Event Viewer** will be opened. In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours
  Event Level – Make sure to checked on Critical, Warning and Error
  By Source - CertificateServicesClient-AutoEnrollment
  Event ID - 6,13

Prod Issuing CA 4 - zwppkia0009

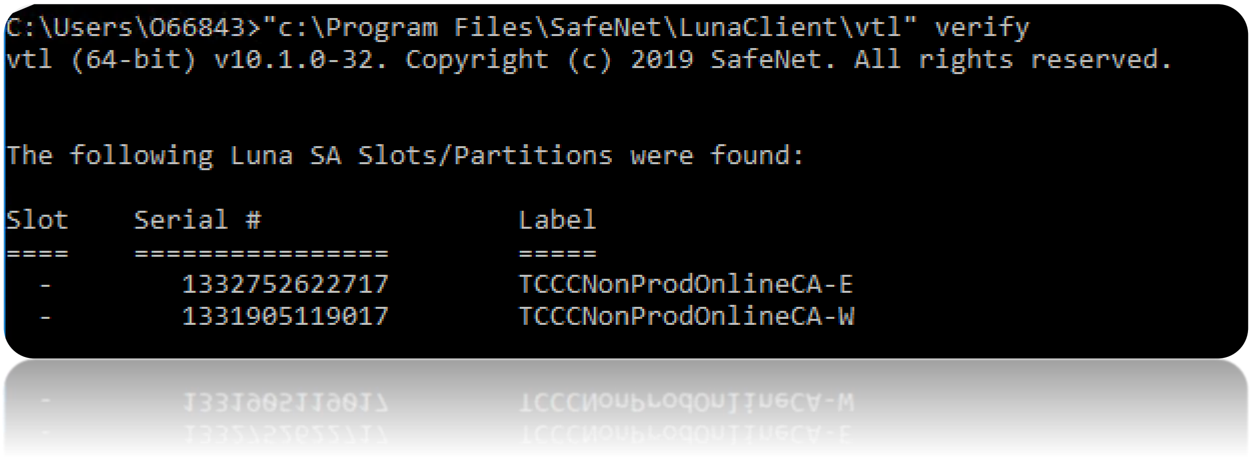
- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours
  Event Level – Make sure to checked on Critical, Warning and Error
  By Source – CertificationAuthority
  Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

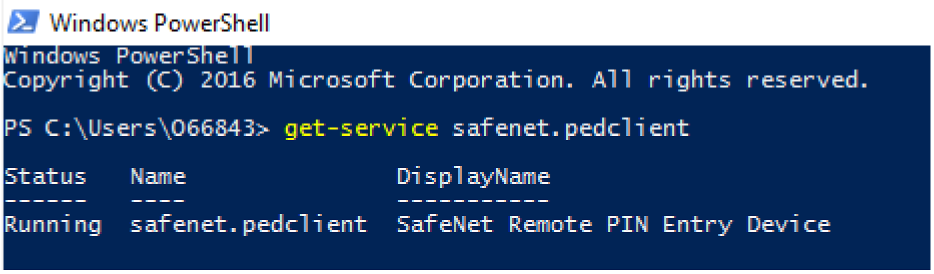
Open CMD and run the below go to the below path and hit enter

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type Get-Service safenet.pedclient and hit enter , your results should be like .



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Prod Issuing CA 5 - zwppkia0010

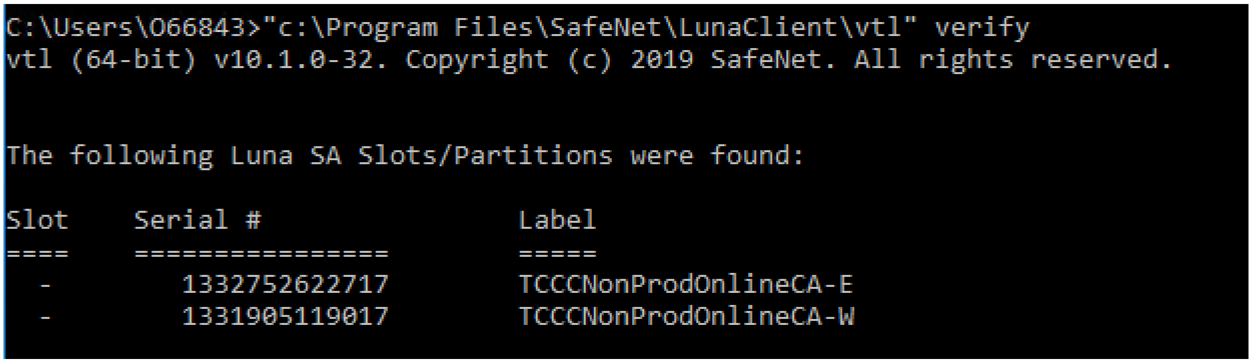
- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours
  Event Level – Make sure to checked on Critical, Warning and Error
  By Source – CertificationAuthority
  Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

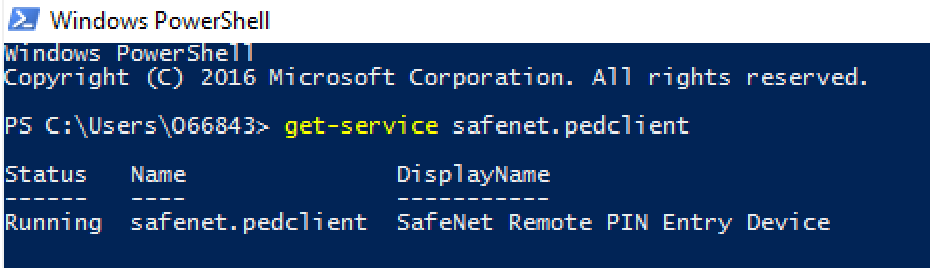
Open CMD and run the below go to the below path and hit enter

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type Get-Service safenet.pedclient and hit enter , your results should be like .



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\O66843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Prod Issuing CA 6 - zwppkia0011

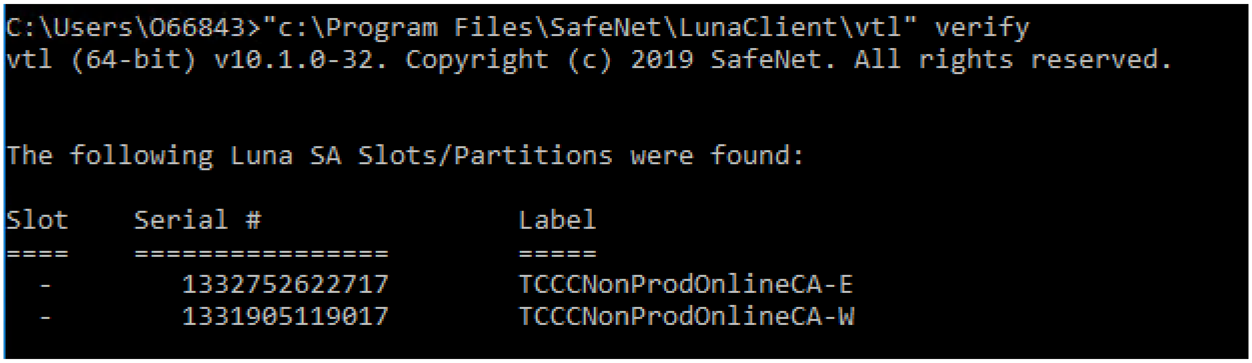
- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical, Warning and Error
By Source – CertificationAuthority
Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

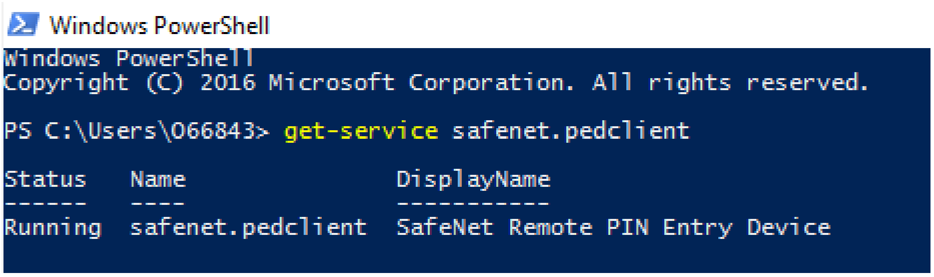
Open CMD and Paste the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot     Serial #                Label
====     ================        =====
  -         1332752622717        TCCCNonProdOnlineCA-E
  -         1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type Get-Service safenet.pedclient and hit enter , your results should be like .



Windows PowerShell

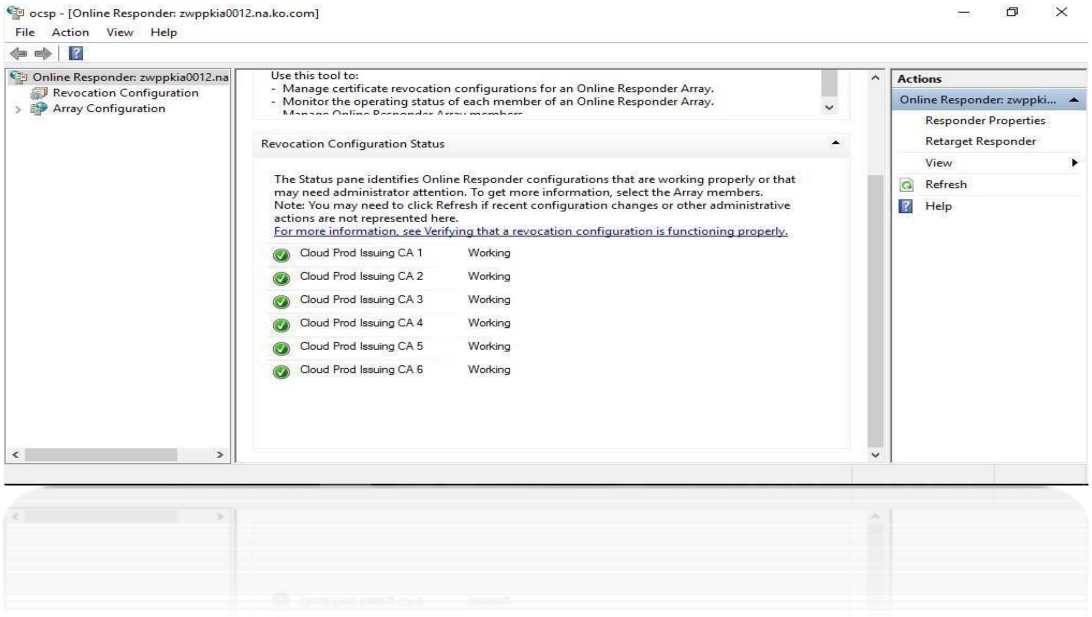
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Prod OCSP 3 - zwppkia0012

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **nFast Server**
  - ✓ **W3SVC**
  - ✓ **OcspSvc** ✓
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours
  Event Level – Make sure to checked on Critical, Warning and Error
  By Source – nCipher CSP, nCipherCSP, OnlineResponder, OnlineResponderRevocationProvider, OnlineResponderWebProxy
  Event ID-16,17,18,20,21,22,23,25,26,27,29,31,33,34,35

Type OnlineResponder in Search Box and hit enter. Make sure all revocation Configuration status show as GREEN **else we need to troubleshoot**



Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

✓ Cloud Prod Issuing CA 1	Working
✓ Cloud Prod Issuing CA 2	Working
✓ Cloud Prod Issuing CA 3	Working
✓ Cloud Prod Issuing CA 4	Working
✓ Cloud Prod Issuing CA 5	Working
✓ Cloud Prod Issuing CA 6	Working

Prod OCSP 4 - zwppkia0013

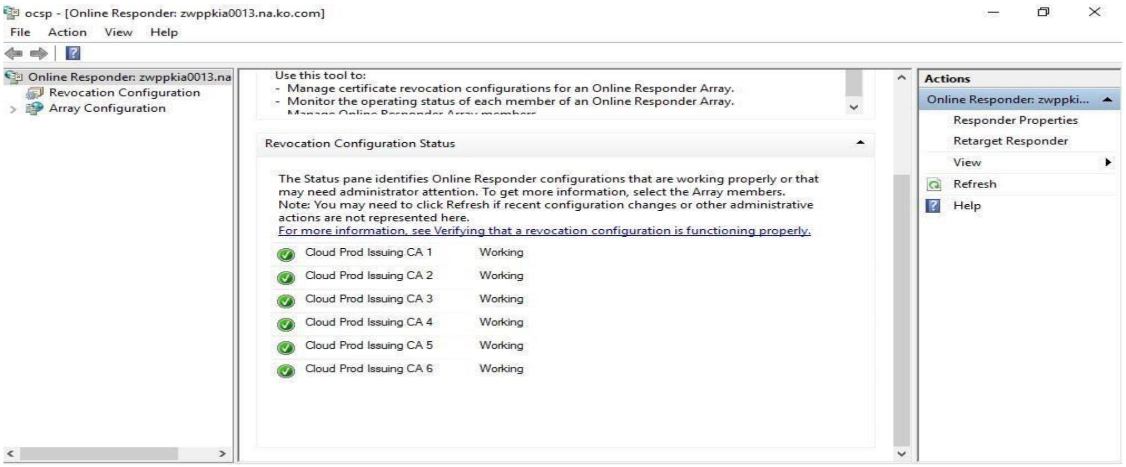
- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **nFast Server**
  - ✓ **W3SVC**
  - ✓ **OcspSvc**
- **Type Event Viewer in Search Box and hit enter.** In

  Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours
  Event Level – Make sure to checked on Critical, Warning and Error
  By Source – nCipher CSP, nCipherCSP, OnlineResponder, OnlineResponderRevocationProvider, OnlineResponderWebProxy
  Event ID-16,17,18,20,21,22,23,25,26,27,29,31,33,34,35

Type OnlineResponder in Search Box and hit enter. Make sure all

revocation Configuration status show as GREEN else we need to troubleshoot



ocsp - [Online Responder: zwppkia0013.na.ko.com]
File
Action
View
Help
Online Responder: zwppkia0013.na
Revocation Configuration
Array Configuration
Revocation Configuration Status
Actions
Online Responder: zwppki...
Responder Properties
Retarget Responder
View
Refresh
Help

Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

✓	Cloud Prod Issuing CA 1	Working
✓	Cloud Prod Issuing CA 2	Working
✓	Cloud Prod Issuing CA 3	Working
✓	Cloud Prod Issuing CA 4	Working
✓	Cloud Prod Issuing CA 5	Working
✓	Cloud Prod Issuing CA 6	Working

Prod Web Server-2 Zwwpkia0014

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**

  ✓ **W3SVC**

- **Type Event Viewer in Search Box and hit enter.** In

  Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours

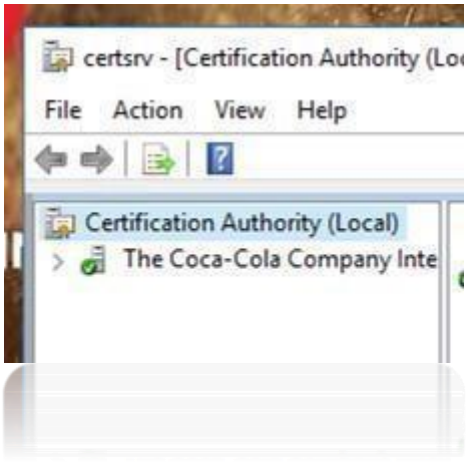
  Event Level – Make sure to checked on Critical, Warning and Error

  By Source – CertificationAuthorityClient-CertCli

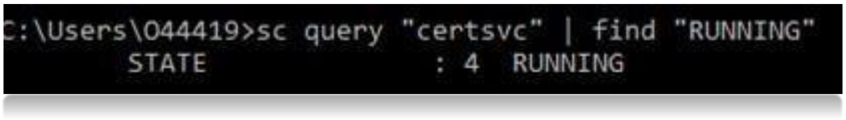
  Event ID- 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Important Checks

We need to ensure that the certsrv service is running on every CA [Ca1 to ca6] when we do our daily checks. Manually looking for the green checkmark


certsrv - [Certification Authority (Lo
File
Action
View
Help
Certification Authority (Local)
The Coca-Cola Company Inte

Check thi command over TestCA1 – TestCA6 [Total 6 servers]
Type : sc query “certsvc” |find “RUNNING”



```
C:\Users\O44419>sc query "certsvc" | find "RUNNING"
        STATE              : 4  RUNNING
```

(If you don’t see the “STATE: 4 RUNNING” it means it isn’t.)

Start with Pre- Production Environment

From East Location

Dev Enrollment Server 1 - zwdpkia0001

To go Search Box and type PKIVIEW.MSC – Once PKIVIEW.MSC opened, check all the certificate are in **OK** status

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ➢ **World Wide Web Services**
  - ➢ **SafeNet Remote Pin Entry Device**

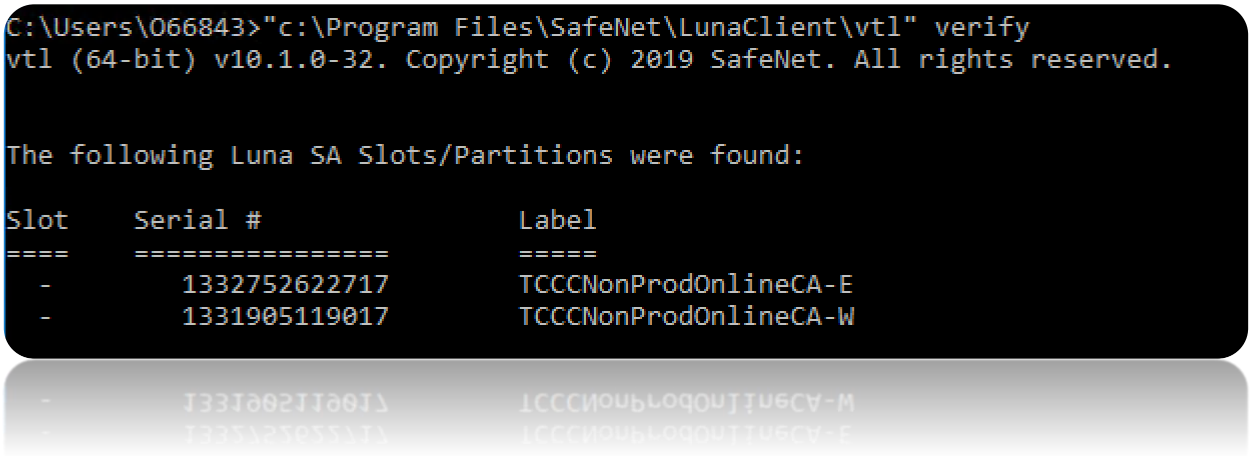
Type Event Viewer in seachbox - EventViewer will be opened . In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical , Warning and Error
By Source - CertificateServicesClient-AutoEnrollment
Event ID - 6,13

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

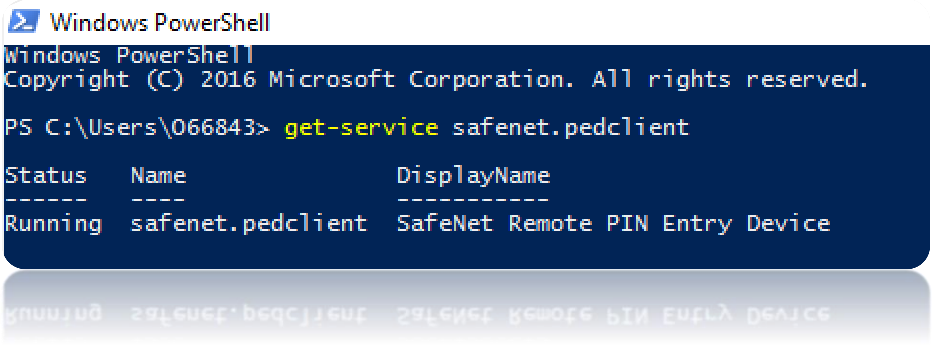
Open CMD and check the below mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\066843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services over the same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test Enrollment Server 1 - zwtpkia0001

To go Search Box and type PKIVIEW.MSC – Once PKIVIEW.MSC opened, check all the certificate are in **OK** status

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**

- **World Wide Web Services**
- **SafeNet Remote Pin Entry Device**

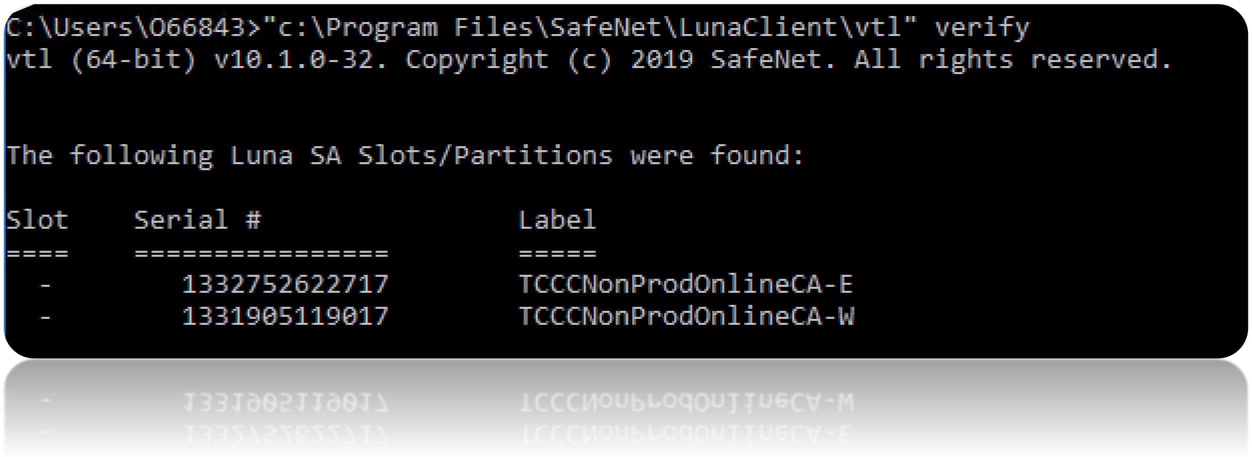
Type Event Viewer in Search box - Event Viewer will be opened. In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical, Warning and Error
By Source - CertificateServicesClient-AutoEnrollment.
Event ID - 6,13

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

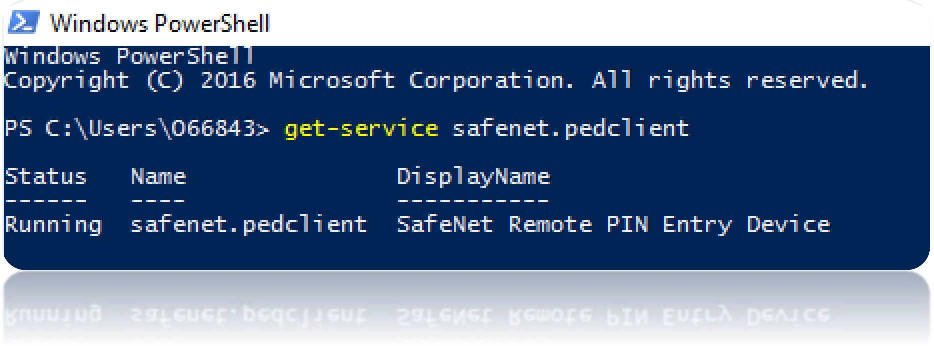
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Dev Issuing CA 1 - zwdpkia0002

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - **CertSVC**
  - **SafeNet Remote Pin Entry Device**

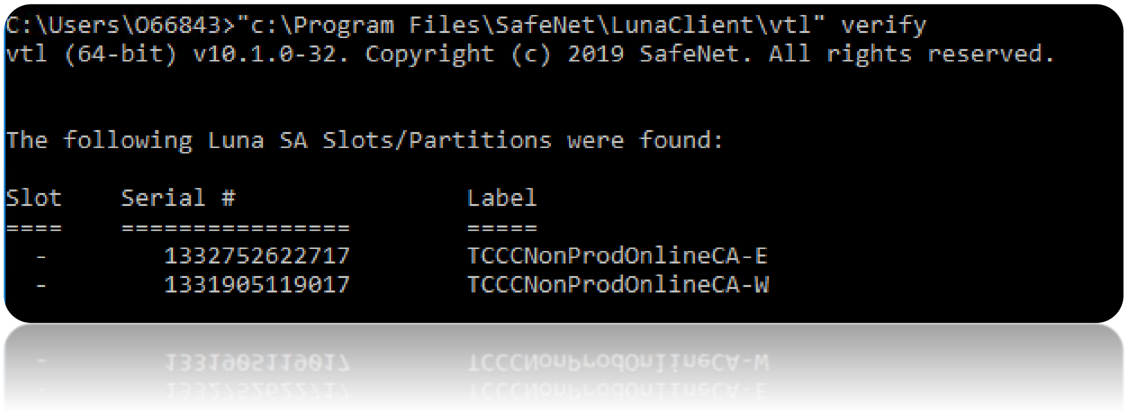
Type Event Viewer in Search box - Event Viewer will be opened. In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical, Warning and Error
By Source - Certification Authority
Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800, 801
Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800, 801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

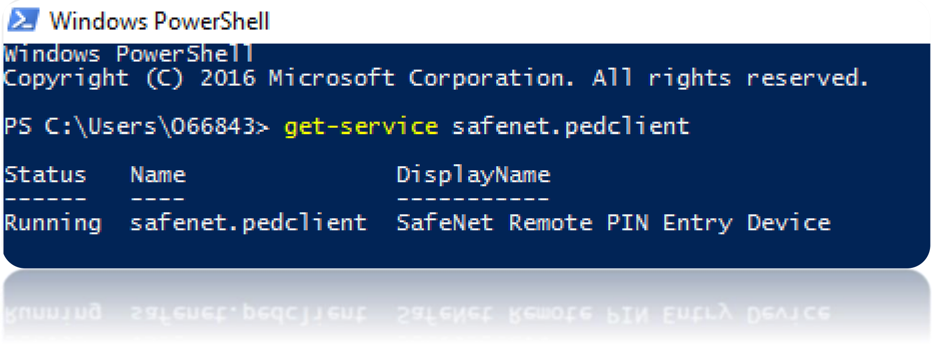
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
 -         1332752622717        TCCCNonProdOnlineCA-E
 -         1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\O66843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Dev Issuing CA 2 - zwdpkia0003

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - **CertSVC**
  - **SafeNet Remote Pin Entry Device**

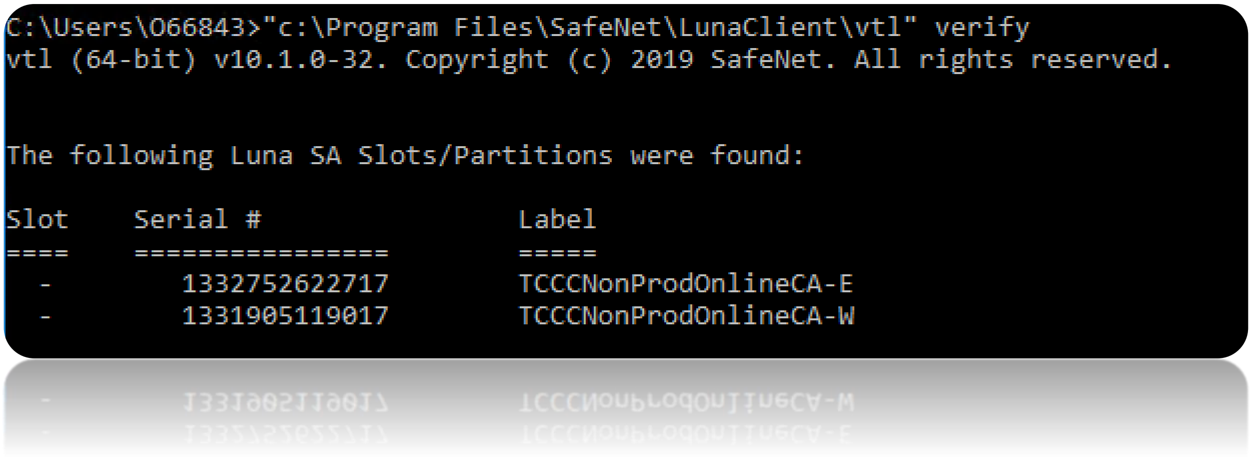
Type Event Viewer in search box - Event Viewer will be opened . In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical , Warning and Error
By Source - Certification Authority
Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800, 801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

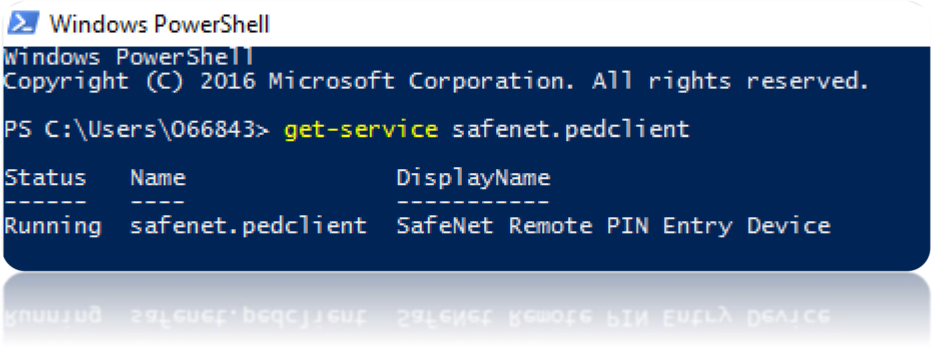
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Dev Issuing CA 3 - zwdpkia0004

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - **CertSVC**
  - **SafeNet Remote Pin Entry Device**

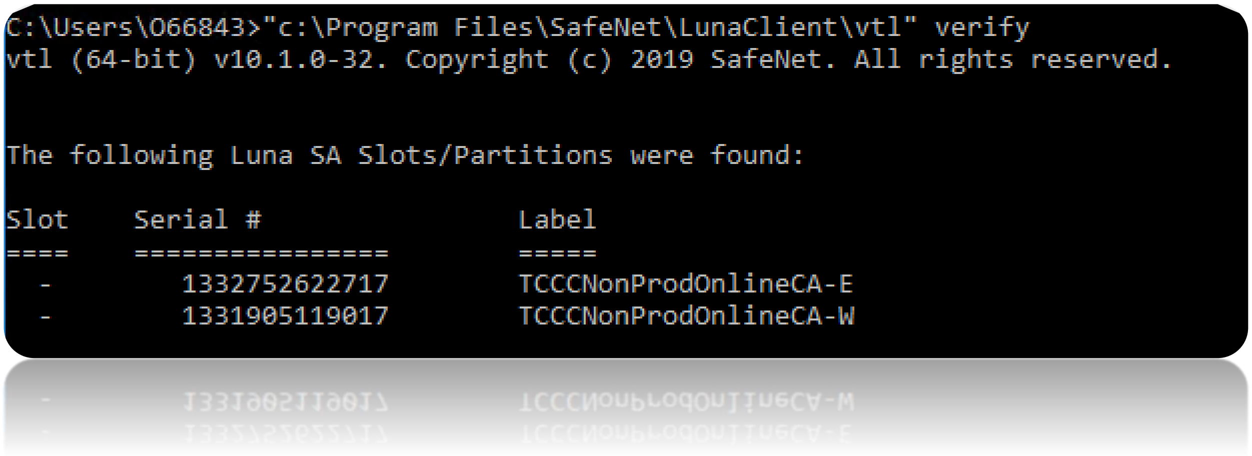
Type Event Viewer in search box - Event Viewer will be opened. In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical, Warning and Error
By Source - Certification Authority
Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800, 801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

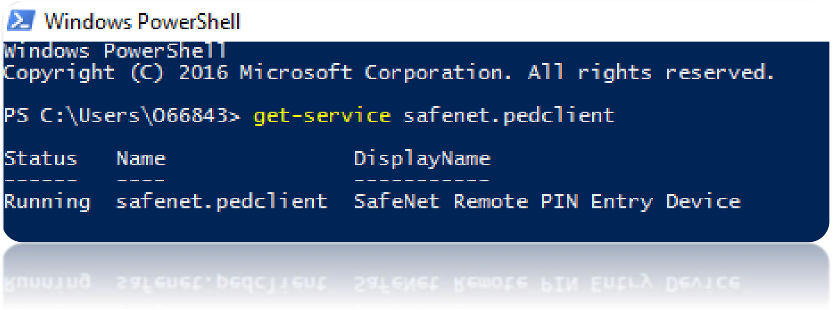
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\066843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Dev Issuing CA 3 - zwdpkia0004

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - **CertSVC**
  - **SafeNet Remote Pin Entry Device**

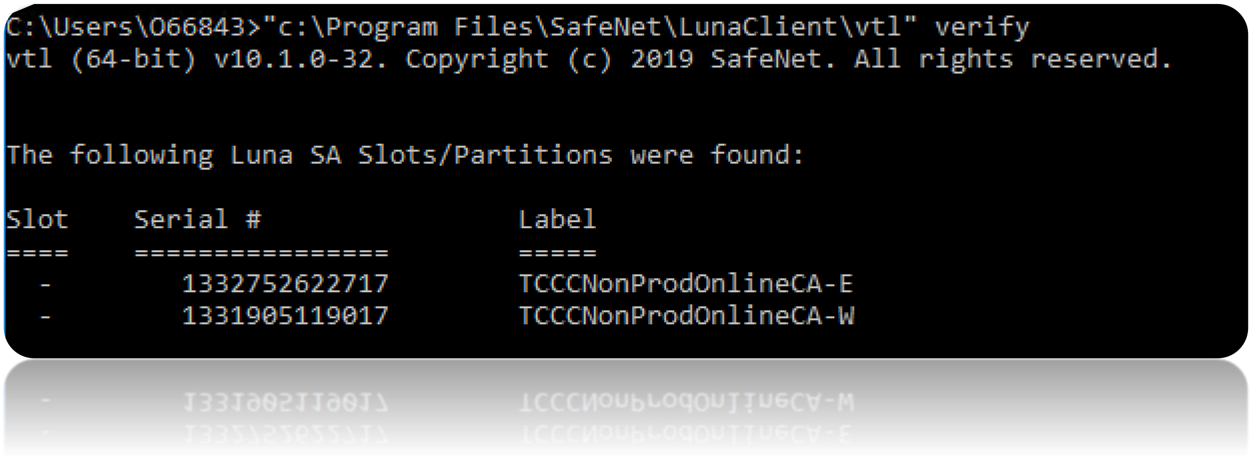
Type Event Viewer in search box - Event Viewer will be opened . In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical, Warning and Error
By Source - Certification Authority
Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800, 801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

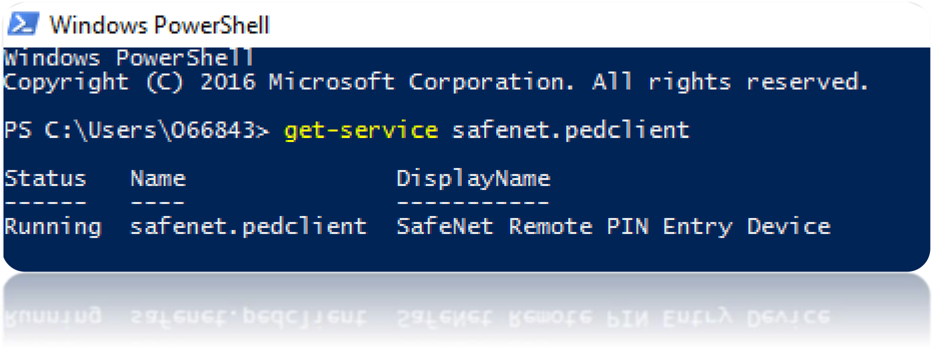
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and grab the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test Issuing CA 1 - zwtpkia0002

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

33- **Logged –** Last 24 hours

34- **Event Level –** Make sure to checked on Critical, Warning and Error

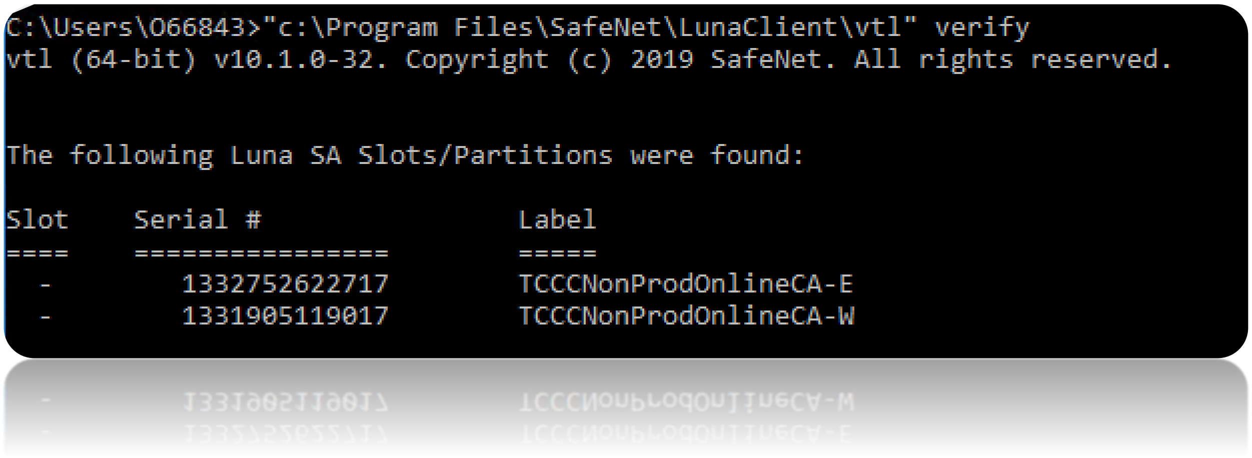
35- **By Source –** Certification Authority

36- **Event ID -** 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

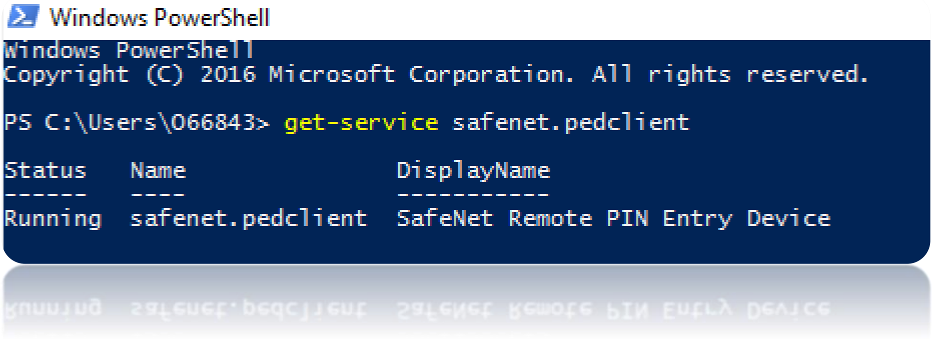
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\066843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test Issuing CA 2 - zwtpkia0003

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application Check filters.**

37- Logged – Last 24 hours

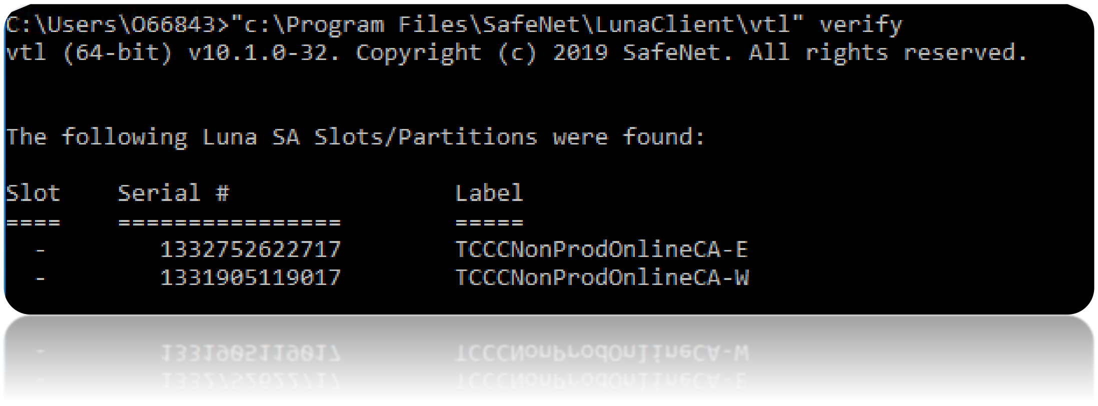
38- Event Level – Make sure to checked on Critical, Warning and Error **39- By Source –** Certification Authority

40- Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

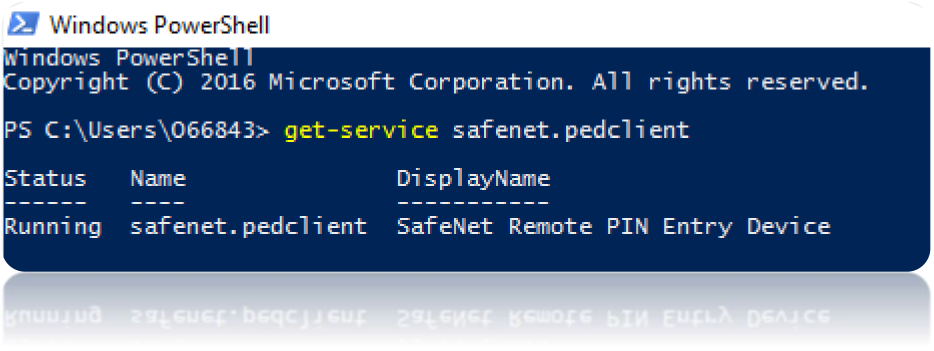
Open CMD and type the mentioned command.

```
"c:\Program Files\SafeNet\LunaClient\vtl" verify
```



```
C:\Users\066843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
 -         1332752622717        TCCCNonProdOnlineCA-E
 -         1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test Issuing CA 3 - zwtpkia0004

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In
  Custom we need to check filters for **System** and
  Application Check filters.

41- **Logged –** Last 24 hours

42- **Event Level –** Make sure to checked on Critical, Warning and Error

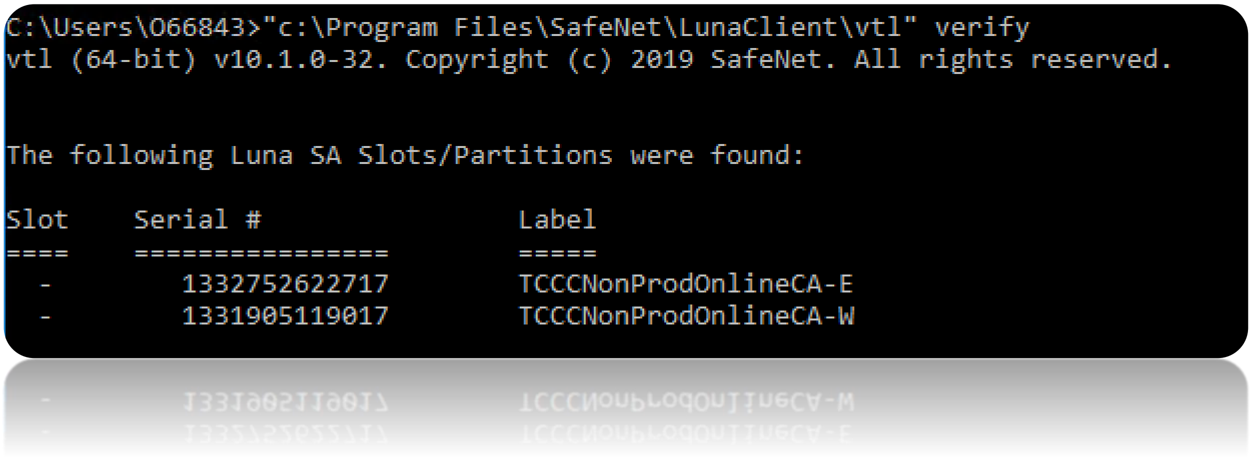
43- **By Source –** Certification Authority

44- **Event ID -** 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

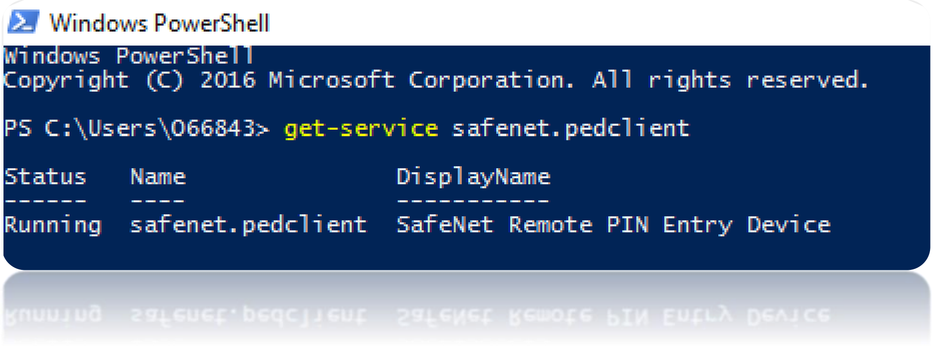
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\O66843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test OCSP 1 - zwtpkia0005

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **SafeNet Remote Pin Entry Device**
  - ✓ **W3SVC**
  - ✓ **OcspSvc**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

45- **Logged –** Last 24 hours

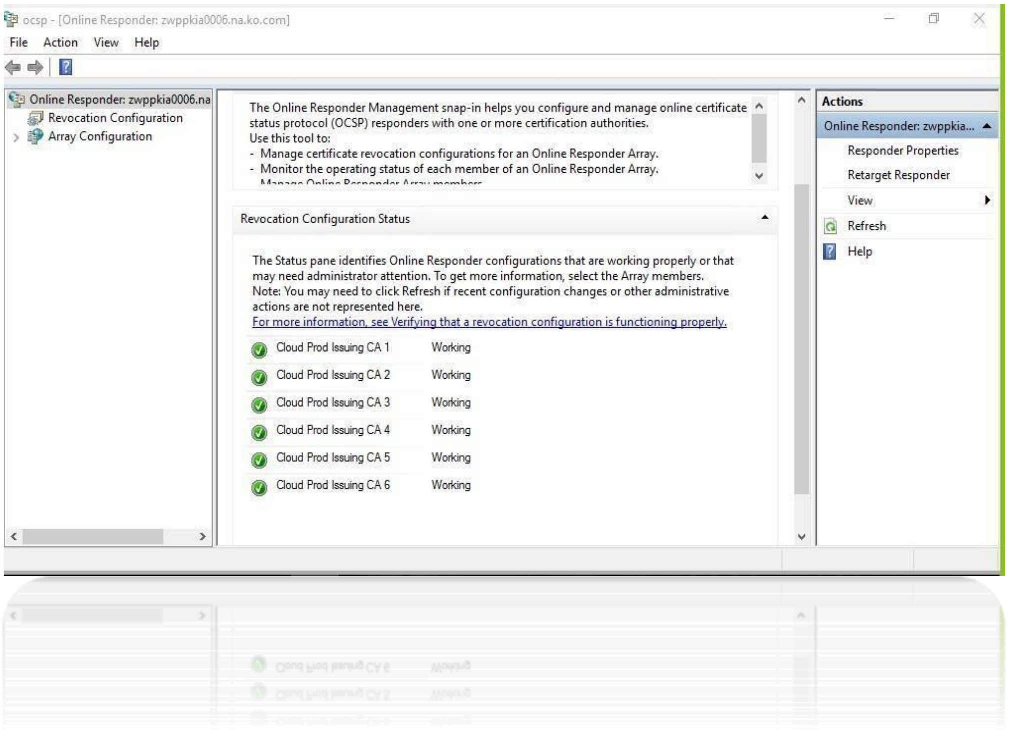
46- **Event Level –** Make sure to checked on Critical, Warning and Error

47- **By Source –** nCipher CSP, nCipherCSP, OnlineResponder, OnlineResponderRevocationProvider, OnlineResponderWebProxy

48- Event ID- 16,17,18,20,21,22,23,25,26,27,29,31,33,34,35 □

Type Online Responder in Search Box and hit enter.

Make sure all revocation Configuration status show as GREEN **else we need to troubleshoot.**



ocsp - [Online Responder: zwppkia0006.na.ko.com]

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

Cloud Prod Issuing CA 1	Working
Cloud Prod Issuing CA 2	Working
Cloud Prod Issuing CA 3	Working
Cloud Prod Issuing CA 4	Working
Cloud Prod Issuing CA 5	Working
Cloud Prod Issuing CA 6	Working

Test OCSP 2 - zwtpkia0006

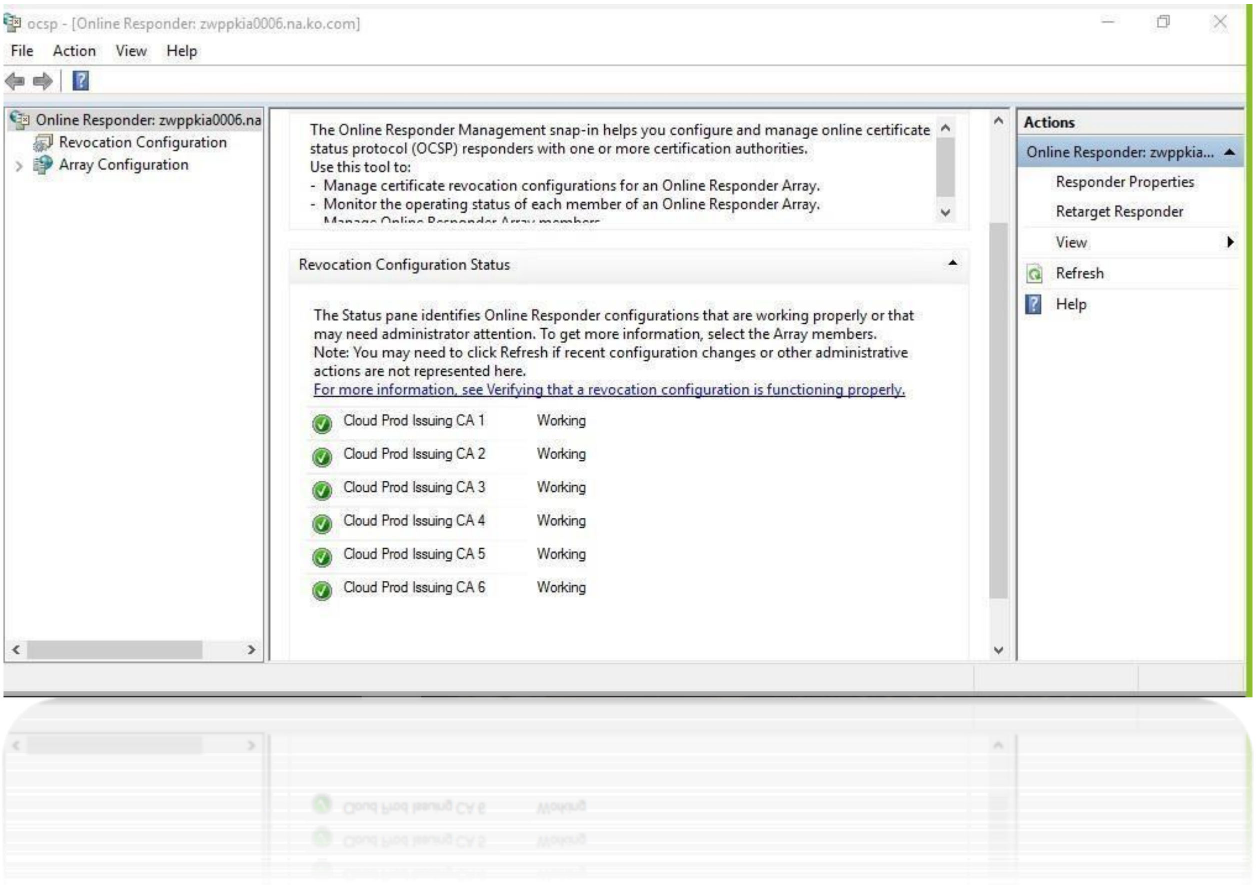
- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **nFast Server**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

49- **Logged –** Last 24 hours

50- **Event Level –** Make sure to checked on Critical, Warning and Error

51- **By Source –** Certification Authority

52- **Event ID -** 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801



The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

✓ Cloud Prod Issuing CA 1	Working
✓ Cloud Prod Issuing CA 2	Working
✓ Cloud Prod Issuing CA 3	Working
✓ Cloud Prod Issuing CA 4	Working
✓ Cloud Prod Issuing CA 5	Working
✓ Cloud Prod Issuing CA 6	Working

Test Web Server 1 - zwtpkia0007

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**

  - ✓ **W3SVC**

- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application Check filters.**

Logged – Last 24 hours
Event Level – Make sure to checked on Critical, Warning and Error
By Source – CertificationAuthorityClient - CertCli
Event ID- 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Test Enrollment Server 2 - zwtpkia0008

To go Search Box and type PKIVIEW.MSC – Once PKIVIEW.MSC opened, check all the certificate are in **OK** status

- **Type Services in search box –** Services will be opened, check **nfast** and **World Wide Web Services**, both services should be in running state.
- **Type Event Viewer in searchbox -** EventViewer will be opened . In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours
  Event Level – Make sure to checked on Critical,Warning and Error
  By Source - CertificateServicesClient-AutoEnrollment
  Event ID - 6,13

Test Issuing CA 4 - zwtpkia0009

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours

Event Level – Make sure to checked on Critical,
Warning and Error

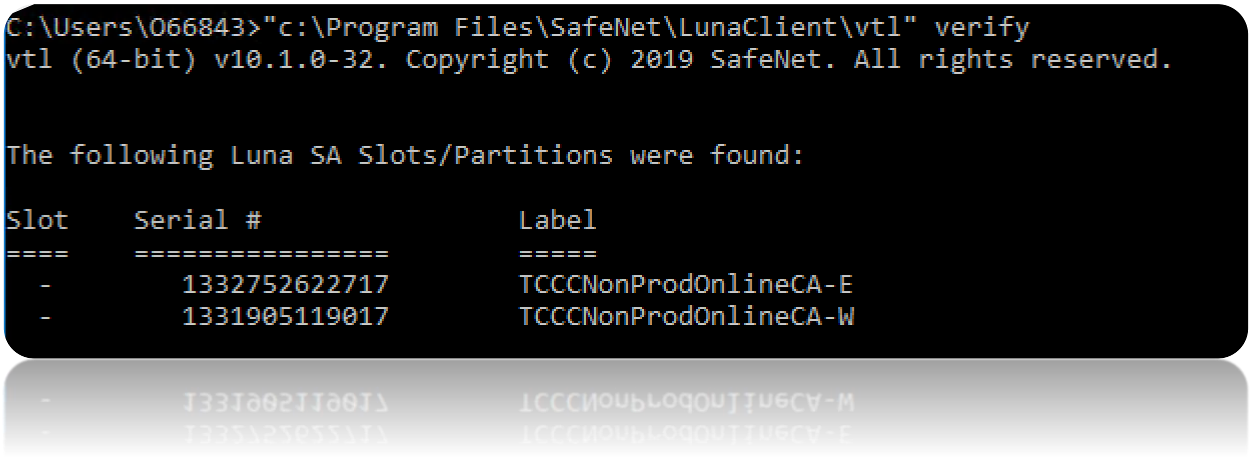
By Source – CertificationAuthority

Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

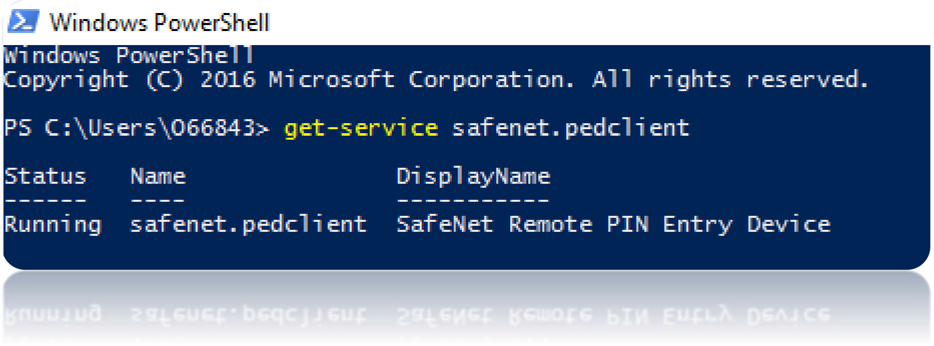
Open CMD and type the mentioned command.

"c:\Program Files\SafeNet\LunaClient\vtl" verify



```
C:\Users\O66843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot    Serial #                Label
====    ================        =====
  -        1332752622717        TCCCNonProdOnlineCA-E
  -        1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\O66843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test Issuing CA 5 - zwtpkia0010

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours

  Event Level – Make sure to checked on Critical, Warning and Error

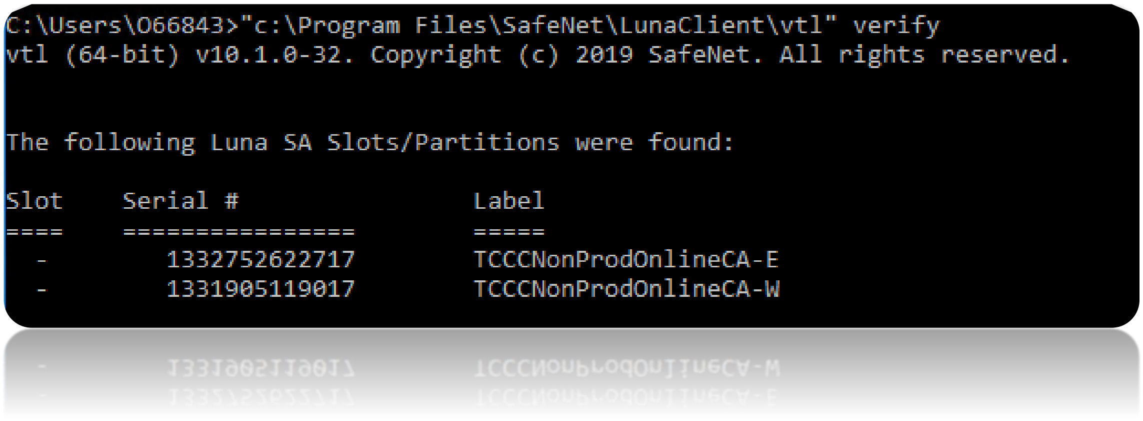
  By Source – Certification Authority

  Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Ensure the HSM Connectivity of the Server for that follow the mentioned below steps.

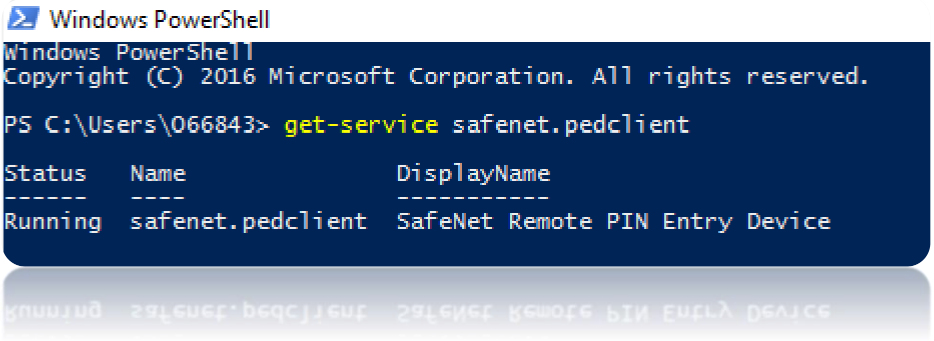
Open CMD and Paste the mentioned command.

```
"c:\Program Files\SafeNet\LunaClient\vtl" verify
```



```
C:\Users\066843>"c:\Program Files\SafeNet\LunaClient\vtl" verify
vtl (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.


The following Luna SA Slots/Partitions were found:

Slot     Serial #                Label
====     ================        =====
  -         1332752622717        TCCCNonProdOnlineCA-E
  -         1331905119017        TCCCNonProdOnlineCA-W
```

Open PowerShell and type the mentioned services on same server



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\066843> get-service safenet.pedclient

Status   Name               DisplayName
------   ----               -----------
Running  safenet.pedclient  SafeNet Remote PIN Entry Device
```

Test Issuing CA 6 - zwtpkia0011

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **CertSvc**
  - ✓ **SafeNet Remote Pin Entry Device**
- **Type Event Viewer in Search Box and hit enter.** In

  Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours

Event Level – Make sure to checked on Critical, Warning and Error

By Source – Certification Authority

Event ID - 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Test OCSP 3 - zwtpkia0012

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **SafeNet Remote Pin Entry Device**
  - ✓ **W3SVC**
  - ✓ **OcspSvc**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

Logged – Last 24 hours

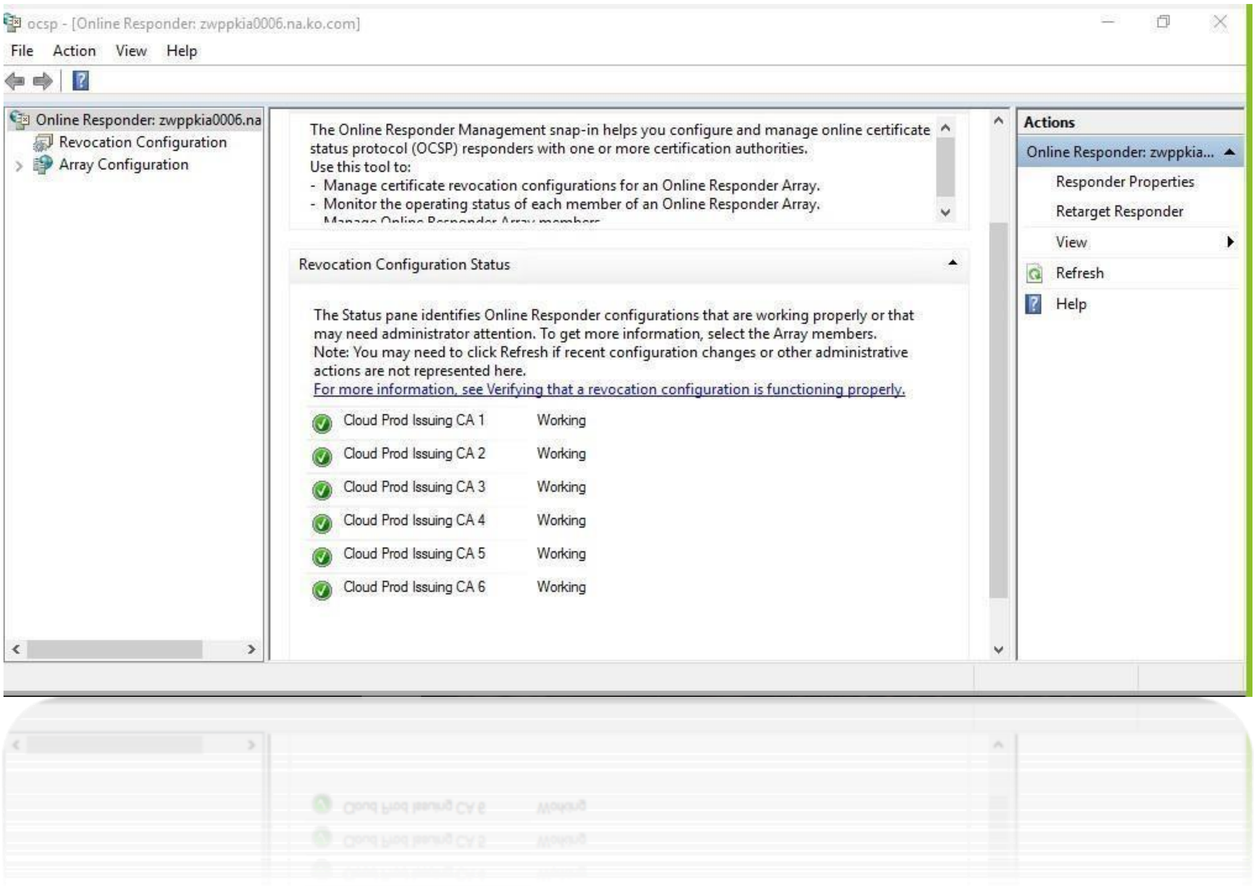
Event Level – Make sure to checked on Critical, Warning and Error

By Source – nCipher CSP, nCipherCSP, Online Responder, OnlineResponderRevocationProvider, OnlineResponderWebProxy

Event ID- 16,17,18,20,21,22,23,25,26,27,29,31,33,34,35

Type Online Responder in Search Box and hit enter.

Make sure all revocation Configuration status show as GREEN else we need to troubleshoot



The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

✓ Cloud Prod Issuing CA 1	Working
✓ Cloud Prod Issuing CA 2	Working
✓ Cloud Prod Issuing CA 3	Working
✓ Cloud Prod Issuing CA 4	Working
✓ Cloud Prod Issuing CA 5	Working
✓ Cloud Prod Issuing CA 6	Working

Test OCSP 4 - zwtpkia0013

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **SafeNet Remote Pin Entry Device**
  - ✓ **W3SVC**
  - ✓ **OcspSvc**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application Check filters.**

Logged – Last 24 hours

Event Level – Make sure to checked on Critical, Warning and Error

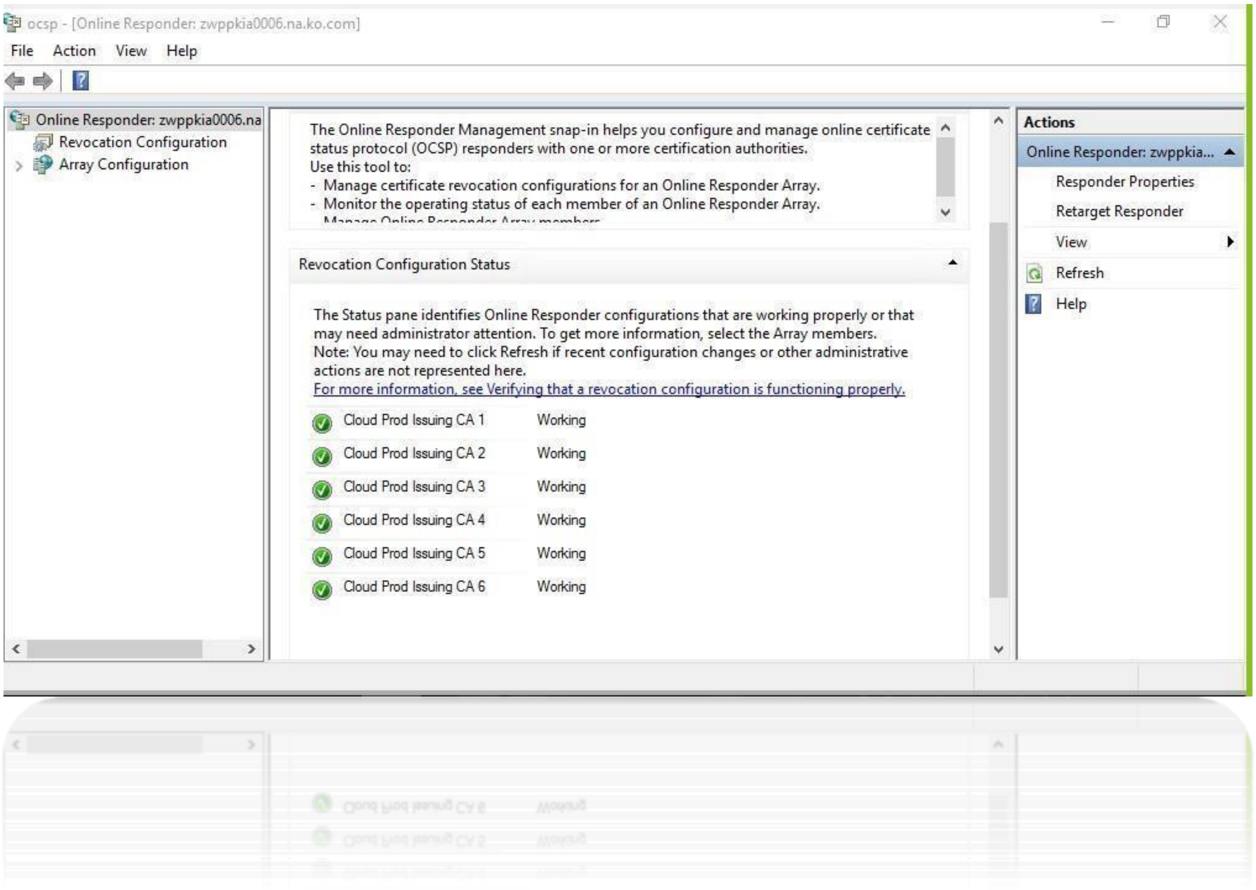
By Source – nCipherCSP, nCipherCSP, Online Responder, OnlineResponderRevocationProvider,

OnlineResponderWebProxy

Event ID- 16,17,18,20,21,22,23,25,26,27,29,31,33,34,35

Type Online Responder in Search Box and hit enter.

Make sure all revocation Configuration status show as GREEN else we need to troubleshoot


ocsp - [Online Responder: zwppkia0006.na.ko.com]
File
Action
View
Help
Online Responder: zwppkia0006.na
Revocation Configuration
Array Configuration
Actions
Online Responder: zwppkia...
Responder Properties
Retarget Responder
View
Refresh
Help
Revocation Configuration Status

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.
Use this tool to:
- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.
Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.
For more information, see Verifying that a revocation configuration is functioning properly.

✓	Cloud Prod Issuing CA 1	Working
✓	Cloud Prod Issuing CA 2	Working
✓	Cloud Prod Issuing CA 3	Working
✓	Cloud Prod Issuing CA 4	Working
✓	Cloud Prod Issuing CA 5	Working
✓	Cloud Prod Issuing CA 6	Working

Test Web Server 2 - zwtpkia0016

- **Type Services in Search box and hit enter.**
- **We need to check below services and all services should be in running state**
  - ✓ **W3SVC**
- **Type Event Viewer in Search Box and hit enter.** In Custom we need to check filters for **System** and **Application** **Check filters.**

  Logged – Last 24 hours

  Event Level – Make sure to checked on Critical, Warning and Error

  By Source – CertificationAuthorityClient-CertCli

  Event ID- 1, 2, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 786, 789, 794, 795, 796, 800,801

Server IP's

Note : If any of the server is not reachable through the DNS , for troubleshoot please check the server through server IP , categorized by region and environment.

Online CAs

The following Online CAs are hosted in Azure East US 2 region:

- Dev
  - ○ The Coca-Cola Company Dev Internal Issuing CA 1
    - ▪ DNS Name: zwdpkia0002.devko.com
    - ▪ IP Address: 10.115.42.135
    - ▪ CCSN CI: TCCC Dev Internal Issuing Certification

  Authority 1 ○ The Coca-Cola Company Dev Internal Issuing CA 2
    - ▪ DNS Name: zwdpkia0003.devko.com
    - ▪ IP Address: 10.115.42.136
    - ▪ CCSN CI: TCCC Dev Internal Issuing Certification

  Authority 2 ○ The Coca-Cola Company Dev Internal Issuing CA 3
    - ▪ DNS Name: zwdpkia0004.devko.com

    - IP Address: 10.115.42.137
    - CCSN CI: TCCC Dev Internal Issuing Certification
    Authority 3
- Test ○ The Coca-Cola Company Test Internal Issuing CA 1
    - DNS Name: zwtpkia0002.testko.com
    - IP Address: 10.115.42.140
    - CCSN CI: TCCC Test Internal Issuing Certification
    Authority 1 ○ The Coca-Cola Company Test Internal Issuing CA 2
    - DNS Name: zwtpkia0003.testko.com
    - IP Address: 10.115.42.141
    - CCSN CI: TCCC Test Internal Issuing Certification
    Authority 2 ○ The Coca-Cola Company Test Internal Issuing CA 3
    - DNS Name: zwtpkia0004.testko.com
    - IP Address: 10.115.42.142
    - CCSN CI: TCCC Test Internal Issuing Certification
    Authority 3
- Prod
    - ○ The Coca-Cola Company Internal Issuing CA 1
        - DNS Name: zwppkia0002.ko.com
        - IP Address: 10.115.25.133
        - CCSN CI: TCCC Internal Issuing Certification Authority 1
    - ○ The Coca-Cola Company Internal Issuing CA 2
        - DNS Name: zwppkia0003.ko.com
        - IP Address: 10.115.25.136
        - CCSN CI: TCCC Internal Issuing Certification Authority
        2 ○ The Coca-Cola Company Internal Issuing CA 3
        - DNS Name: zwppkia0004.ko.com
        - IP Address: 10.115.25.137
        - CCSN CI: TCCC Internal Issuing Certification Authority
        3

Web Servers

- Test ○ The Coca-Cola Company Test Web Server 1
    - DNS Name: zwtpkia0007.na.testko.com
    - IP Address: 10.115.42.143
    - CCSN CI: TCCC Test Internal PKI Web Server 1
- Prod ○ The Coca-Cola Company Prod Web Server 1
    - DNS Name: zwppkia0007.na.ko.com
    - IP Address: 10.115.25.138
    - CCSN CI: TCCC Internal PKI Web Server 1

OCSP Servers

- Test ○ The Coca-Cola Company Test Online Responder 1
    - DNS Name: zwtpkia0005.na.testko.com
    - IP Address: 10.115.42.132
    - CCSN CI: TCCC Test Internal OCSP Server 1 ○ The Coca-Cola Company Test Online Responder 2
    - DNS Name: zwtpkia0006.na.testko.com
    - IP Address: 10.115.42.133
    - CCSN CI: TCCC Test Internal OCSP Server 2
- Prod ○ The Coca-Cola Company Online Responder 1
    - DNS Name: zwppkia0005.na.ko.com
    - IP Address: 10.115.25.134
    - CCSN CI: TCCC Internal OCSP Server 1 ○ The Coca-Cola Company Online Responder 2
    - DNS Name: zwppkia0006.na.ko.com
    - IP Address: 10.115.25.135
    - CCSN CI: TCCC Internal OCSP Server 2

Enrollment Servers

- Test ○ The Coca-Cola Company Test Enrollment Server 1
    - DNS Name: zwtpkia0001.testko.com
    - IP Address: 10.115.42.139
    - CCSN CI: No CI Assigned
- Prod ○ The Coca-Cola Company Prod Enrollment Server 1
    - DNS Name: zwppkia0001.ko.com
    - IP Address: 10.115.25.132
    - CCSN CI: No CI Assigned

Venafi Components

- Test ○ Venafi Test Application Server 1
    - DNS Name: zwtpkia0014.na.testko.com
    - IP Address: 10.115.42.144
    - CCSN CI: Venafi Trust Protection Platform - testko.com ○ Venafi Test Application Server 2
    - DNS Name: zwtpkia0015.na.testko.com
    - IP Address: 10.115.42.145
    - CCSN CI: Venafi Trust Protection Platform - testko.com ○ Venafi Test Database Server
    - DNS Name: zwtpkid0017.na.testko.com
    - IP Address: 10.115.42.146

        - CCSN CI: Venafi Trust Protection Platform - testko.com

- Prod
    - ○ Venafi Prod Application Server 1
        - DNS Name: zwppkia0015.na.ko.com
        - IP Address: 10.115.25.139
        - CCSN CI: Venafi Trust Protection Platform o Venafi Prod Application Server 2
        - DNS Name: zwppkia0016.na.ko.com
        - IP Address: 10.115.25.140
        - CCSN CI: Venafi Trust Protection Platform ○ Venafi Prod Database Server
        - DNS Name: zwppkid0017.na.ko.com
        - IP Address: 10.115.25.141
        - CCSN CI: Venafi Trust Protection Platform

Azure Central US

The infrastructure currently consists of virtual machines in a few categories:

Online CAs

The following Online CAs are hosted in Azure East US 2 region:

- Test ○ The Coca-Cola Company Test Internal Issuing CA 4
        - DNS Name: zwtpkia0009.testko.com
        - IP Address: 10.115.76.7
        - CCSN CI: TCCC Test Internal Issuing Certification Authority 4 ○ The Coca-Cola Company Test Internal Issuing CA 5
        - DNS Name: zwtpkia0010.testko.com
        - IP Address: 10.115.76.8
        - CCSN CI: TCCC Test Internal Issuing Certification Authority 5 ○ The Coca-Cola Company Test Internal Issuing CA 6
        - DNS Name: zwtpkia0011.testko.com
        - IP Address: 10.115.76.9
        - CCSN CI: TCCC Test Internal Issuing Certification Authority 6
- Prod
    - The Coca-Cola Company Internal Issuing CA 4
        - DNS Name: zwppkia0009.ko.com
        - IP Address: 10.115.78.7
        - CCSN CI: TCCC Internal Issuing Certification Authority 4 ○ The Coca-Cola Company Internal Issuing CA 5
        - DNS Name: zwppkia0010.ko.com

- IP Address: 10.115.78.8
- CCSN CI: TCCC Internal Issuing Certification Authority

5 ○ The Coca-Cola Company Internal Issuing CA 6

- DNS Name: zwppkia0011.ko.com
- IP Address: 10.115.78.9
- CCSN CI: TCCC Internal Issuing Certification Authority

6

Web Servers

- Test ○ The Coca-Cola Company Test Web Server 2
  - DNS Name: zwtpkia0016.na.testko.com
  - IP Address: 10.115.76.10
  - CCSN CI: TCCC Test Internal PKI Web Server 2
- Prod ○ The Coca-Cola Company Prod Web Server 2
  - DNS Name: zwppkia0014.na.ko.com
  - IP Address: 10.115.78.10
  - CCSN CI: TCCC Internal PKI Web Server 2

OCSP Servers

- Test ○ The Coca-Cola Company Test Online Responder 3
  - DNS Name: zwtpkia0012.na.testko.com
  - IP Address: 10.115.76.4
  - CCSN CI: TCCC Test Internal OCSP Server 3 ○ The Coca-Cola Company Test Online Responder 4
  - DNS Name: zwtpkia0013.na.testko.com
  - IP Address: 10.115.76.5
  - CCSN CI: TCCC Test Internal OCSP Server 4
- Prod ○ The Coca-Cola Company Online Responder 3
  - DNS Name: zwppkia0012.na.ko.com
  - IP Address: 10.115.78.4
  - CCSN CI: TCCC Internal OCSP Server 3
  - ○ The Coca-Cola Company Online Responder 4
    - DNS Name: zwppkia0013.na.ko.com
    - IP Address: 10.115.78.5
    - CCSN CI: TCCC Internal OCSP Server 4

Enrollment Servers

- Test ○ The Coca-Cola Company Test Enrollment Server 2
  - DNS Name: zwtpkia0008.testko.com
  - IP Address: 10.115.76.6
  - CCSN CI: No CI Assigned
- Prod ○ The Coca-Cola Company Prod Enrollment Server 2

- DNS Name: zwppkia0008.ko.com
- IP Address: 10.115.78.6

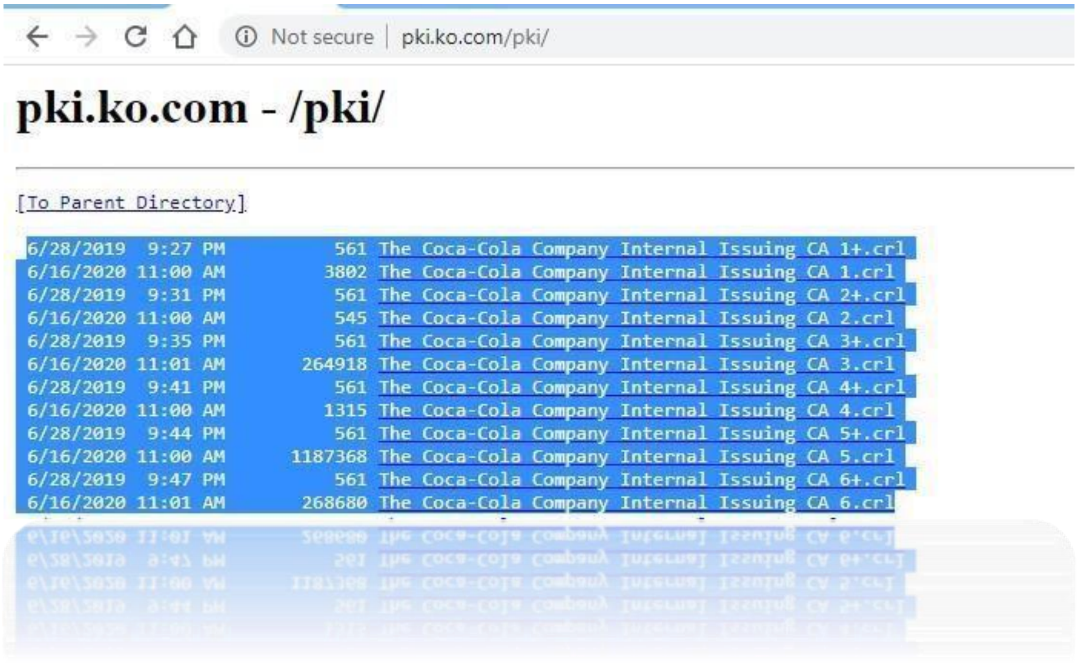
CCSN CI: No CI Assigned

WEBSITE AVAILABILITY

There are Ten (5) sites from both production and non-production environment that should be checked daily to ensure they are reachable and that all CRLs and Delta CRLs are valid.

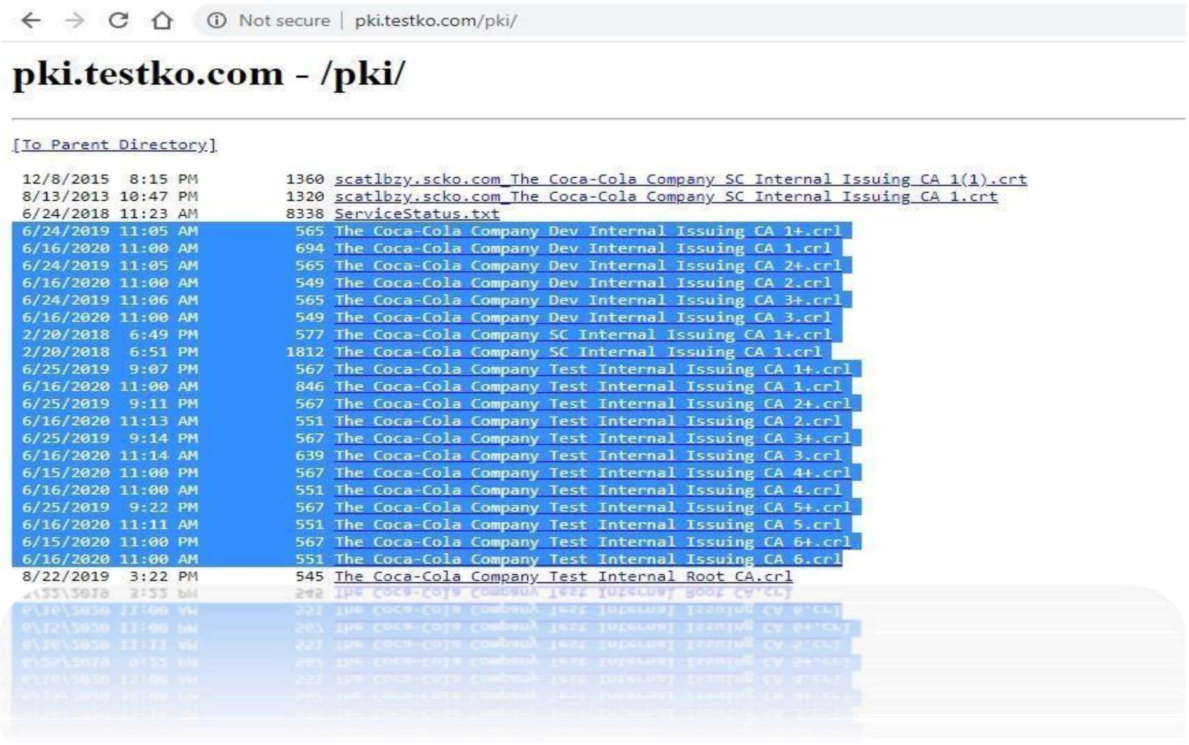
NON-PRODUCTION: http://pki.testko.com/pki/
PRODUCTION : http://pki.ko.com/pki/

Important Instruction for Both Production and Pre-Production CRLs: If we are checking these URL in our **4PM** checks, we will focus and make sure CRLS for **AM** should update similar if we are checking CRLs in our **4AM** checks, we must make sure the CRLS for PM should update accordingly. This site should be checked to ensure it is reachable both within the Coca-Cola network. The following entries should be no more than 24 hours old, typically updated at 11 am every day.



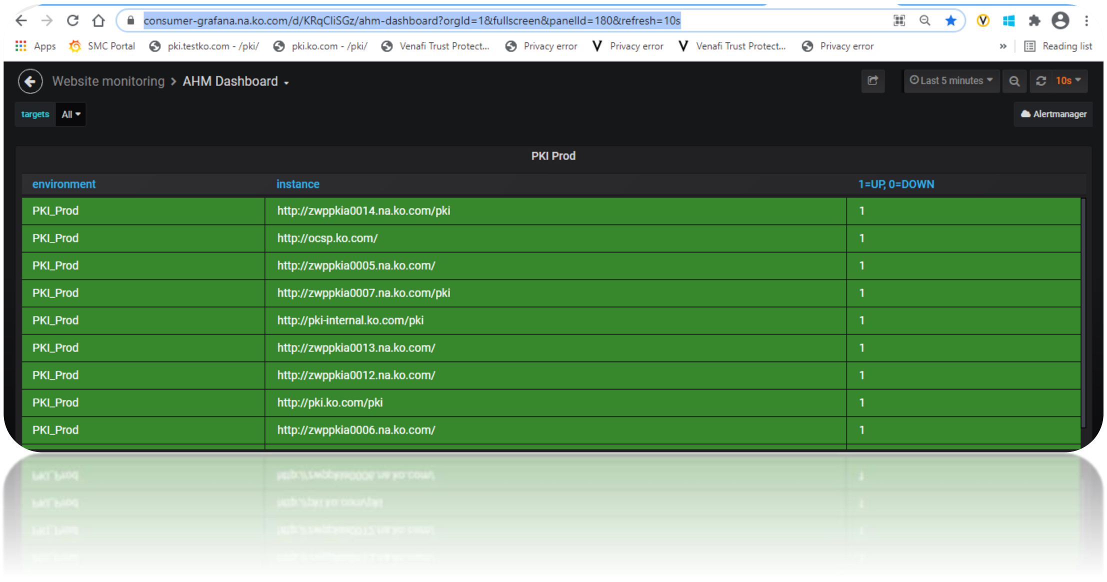
pki.ko.com - /pki/

```
[To Parent Directory]

6/28/2019  9:27 PM         561 The Coca-Cola Company Internal Issuing CA 1+.crl
6/16/2020 11:00 AM        3802 The Coca-Cola Company Internal Issuing CA 1.crl
6/28/2019  9:31 PM         561 The Coca-Cola Company Internal Issuing CA 2+.crl
6/16/2020 11:00 AM         545 The Coca-Cola Company Internal Issuing CA 2.crl
6/28/2019  9:35 PM         561 The Coca-Cola Company Internal Issuing CA 3+.crl
6/16/2020 11:01 AM      264918 The Coca-Cola Company Internal Issuing CA 3.crl
6/28/2019  9:41 PM         561 The Coca-Cola Company Internal Issuing CA 4+.crl
6/16/2020 11:00 AM        1315 The Coca-Cola Company Internal Issuing CA 4.crl
6/28/2019  9:44 PM         561 The Coca-Cola Company Internal Issuing CA 5+.crl
6/16/2020 11:00 AM     1187368 The Coca-Cola Company Internal Issuing CA 5.crl
6/28/2019  9:47 PM         561 The Coca-Cola Company Internal Issuing CA 6+.crl
6/16/2020 11:01 AM      268680 The Coca-Cola Company Internal Issuing CA 6.crl
```



```
pki.testko.com - /pki/

[To Parent Directory]

 12/8/2015  8:15 PM         1360 scatlbzy.scko.com_The Coca-Cola Company SC Internal Issuing CA 1(1).crt
 8/13/2013 10:47 PM         1320 scatlbzy.scko.com_The Coca-Cola Company SC Internal Issuing CA 1.crt
 6/24/2018 11:23 AM         8338 ServiceStatus.txt
 6/24/2019 11:05 AM          565 The Coca-Cola Company Dev Internal Issuing CA 1+.crl
 6/16/2020 11:00 AM          694 The Coca-Cola Company Dev Internal Issuing CA 1.crl
 6/24/2019 11:05 AM          565 The Coca-Cola Company Dev Internal Issuing CA 2+.crl
 6/16/2020 11:00 AM          549 The Coca-Cola Company Dev Internal Issuing CA 2.crl
 6/24/2019 11:06 AM          565 The Coca-Cola Company Dev Internal Issuing CA 3+.crl
 6/16/2020 11:00 AM          549 The Coca-Cola Company Dev Internal Issuing CA 3.crl
 2/20/2018  6:49 PM          577 The Coca-Cola Company SC Internal Issuing CA 1+.crl
 2/20/2018  6:51 PM         1812 The Coca-Cola Company SC Internal Issuing CA 1.crl
 6/25/2019  9:07 PM          567 The Coca-Cola Company Test Internal Issuing CA 1+.crl
 6/16/2020 11:00 AM          846 The Coca-Cola Company Test Internal Issuing CA 1.crl
 6/25/2019  9:11 PM          567 The Coca-Cola Company Test Internal Issuing CA 2+.crl
 6/16/2020 11:13 AM          551 The Coca-Cola Company Test Internal Issuing CA 2.crl
 6/25/2019  9:14 PM          567 The Coca-Cola Company Test Internal Issuing CA 3+.crl
 6/16/2020 11:14 AM          639 The Coca-Cola Company Test Internal Issuing CA 3.crl
 6/15/2020 11:00 PM          567 The Coca-Cola Company Test Internal Issuing CA 4+.crl
 6/16/2020 11:00 AM          551 The Coca-Cola Company Test Internal Issuing CA 4.crl
 6/25/2019  9:22 PM          567 The Coca-Cola Company Test Internal Issuing CA 5+.crl
 6/16/2020 11:11 AM          551 The Coca-Cola Company Test Internal Issuing CA 5.crl
 6/15/2020 11:00 PM          567 The Coca-Cola Company Test Internal Issuing CA 6+.crl
 6/16/2020 11:00 AM          551 The Coca-Cola Company Test Internal Issuing CA 6.crl
 8/22/2019  3:22 PM          545 The Coca-Cola Company Test Internal Root CA.crl
```

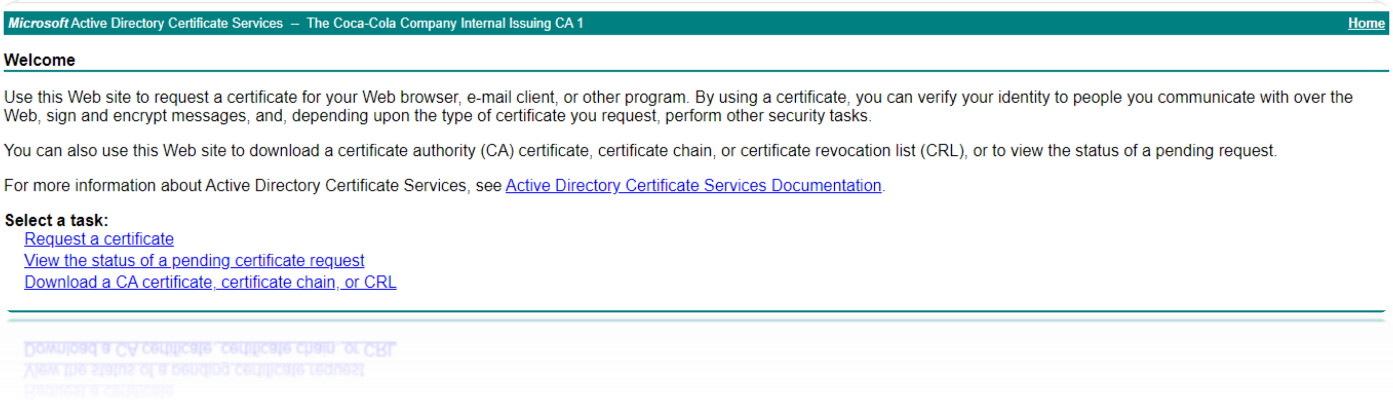
https://consumer-grafana.na.ko.com/d/KRqCIiSGz/ahm-dashboard?orgId=1&fullscreen&panelId=180&refresh=10s



PKI Prod

environment	instance	1=UP, 0=DOWN
PKI_Prod	http://zwppkia0014.na.ko.com/pki	1
PKI_Prod	http://ocsp.ko.com/	1
PKI_Prod	http://zwppkia0005.na.ko.com/	1
PKI_Prod	http://zwppkia0007.na.ko.com/pki	1
PKI_Prod	http://pki-internal.ko.com/pki	1
PKI_Prod	http://zwppkia0013.na.ko.com/	1
PKI_Prod	http://zwppkia0012.na.ko.com/	1
PKI_Prod	http://pki.ko.com/pki	1
PKI_Prod	http://zwppkia0006.na.ko.com/	1

https://zwppkia0001.ko.com/certsrv



Microsoft Active Directory Certificate Services -- The Coca-Cola Company Internal Issuing CA 1 Home

Welcome

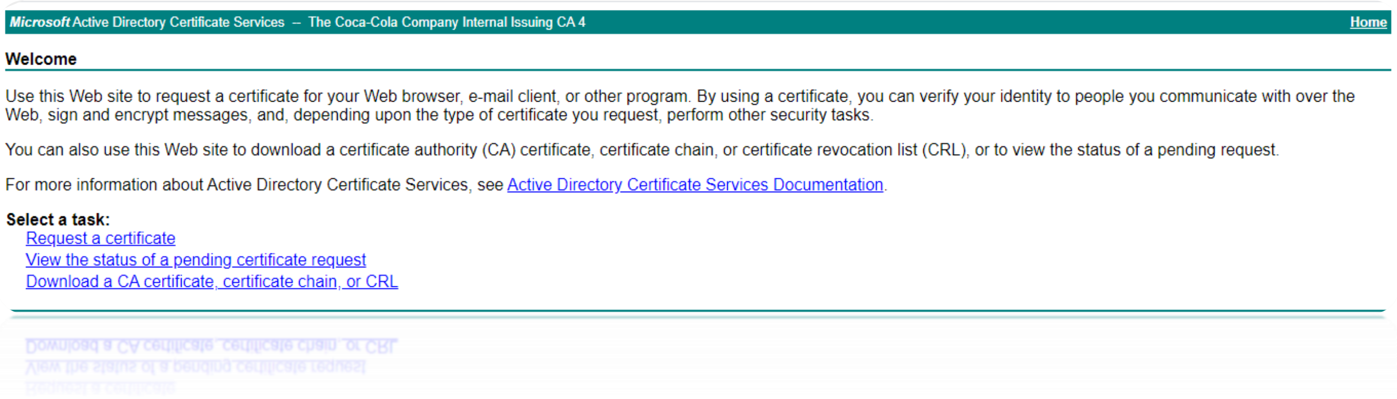
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

https://zwppkia0008.ko.com/certsrv



Microsoft Active Directory Certificate Services -- The Coca-Cola Company Internal Issuing CA 4 Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

You need to check above mentioned URL from your VDI to make sure all are reachable. Open the link in google chrome which is already installed in your VDI and logged in through your VDI username and password. Once you enter make sure you need to click on Load Data to confirm the specific URL is accessible and working fine.

As we have mentioned above in this document that we need to send the email to our client from Monday to Friday. One at 4PM and other at 4AM to following people and group and on Weekend i.e. Saturday and Sunday to **devops@tenpearls.com**. Below is the content that we need to follow:

We have to send to the following group and people and content of the email should be FOLLOWED as mentioned.

TO : phesse@coca-cola.com
CC : tccc-pki-support@10pearls.com , ssalsbury@coca-cola.com , jeffcochran@coca-cola.com Subject: **PKI Health Checks 16th June 2020**

16th June 2020 updates (06:00 AM OR PM EST)

CRLs have been checked which are up to date and the services are running

Thanks and best regards,

-- Your VDI name here