Horizon View
True SSO Enrollment Server Diagnostics Tool 2.2

Table of Contents

Background: 1
Horizon Enrollment Server basic requirement: 1
Windows Certificate Enrollment Settings: 1
NTAuthCertificates: 2
Certificate Templates: 2
Enrollment Servers 2
Enrollment Certificate: 2
es_diag.exe 3
The following arguments can be used with all operations: 4
Select Enrollment Server to execute against: 4
Select authentication method: 4
Controlling the verbosity of the output from the tool: 5
ConnectTest: 5
ESConfig: 5
ListEnvironment: 6
RescanEnvironment: 8
ListConfigs: 8
EnrollmentTest 9
LogonTest 11

Background:

Horizon View True SSO uses Microsoft Enterprise Certificate Servers to issue certificates that is used when the user logs on to the desktop.

The Horizon View Enrollment Server (ES for short) is responsible for sending Certificate Request to certificate servers and for monitoring the PKI configuration settings in the Active Directly.

The tool es_diag.exe that this paper discuss allows you to perform basic validation of the Horizon (Certificate) Enrollment server, the Active Directory PKI settings and Enterprise CA's.

Acronyms/short form names used throughout this document.
CS = Connection Server = Horizon View Connection Server
ES = Enrollment Server = Horizon View Enrollment Server
Cluster = View Cluster = Horizon View Cluster = Horizon View Pod
AD = Active Directory
DC = Domain Controller
CA = Certificate Authority = Certificate Server
Template = Certificate Template

Horizon Enrollment Server basic requirement:

In order for the ES to be able to issue certificates for users in a specific domain these basic requirements must be met:

- The ES must be installed on a system that is a member of the user domain or a domain that has got a two-way trust to the domain where the users are located. It can't be installed on a Domain Controller or the Connection Server, but it may be co-installed with the CA.
- A Certificate Template with Smartcard Logon usage must be configured, and the ES must be given Enroll permission on this Template.
- An enterprise CA must be configured to issue certificates for the wanted Template.
- An Enrollment Certificate generated by an Enterprise CA from the forest where the users are located must be installed into the <system>\<Personal> certificate store of the ES.
- A Horizon View Connection server (pod) must be paired with the ES.

Please refer to the Horizon View Admin Guide and Deployment Guide for detailed information of how to install and configure True SSO.

Windows Certificate Enrollment Settings:

Windows stores the configuration settings used by the Certificate Servers when generating certificates and by Domain Controllers when validating the certificates during the logon in the Active Directory Configuration Container. If there are multiple domains in an active directory forest these settings are shared by all domains in that forest.
The Windows PKI enrollment settings are managed using the <Certification Authority> management console.

You can also view the settings using the <Active Directory Sites and Services> management console. By default these objects are hidden in this console. To show them go to <View> and enable <Show Services Node>. In the tree-view you can then navigate to <Services>, <Public Key Services>.

NOTE: Don't modify these objects from the <Active Directory Sites and Services> console unless you know what you are doing, an invalid setting here may prevent users from logging on.

There are 3 different type of objects that are of interest to the Enrollment Server:

NTAuthCertificates:

This (NTAuth Store) object is stored in the <Public Key Services> container.
The object stores a list of Enterprise CA certificates. A domain controller will only allow a user to perform a Smartcard/Certificate logon if the certificate used for the logon was generated by a CA that has got its root certificate published to this list.

When one installs a Windows Enterprise CA, it will automatically publish its CA certificate to this object.

The Horizon Enrollment server will verify that the configured CA is listed here.

Certificate Templates:

The <Public Key Services\Certificate Templates> container holds templates for the different types of certificates that a Microsoft CA can generate. The template essentially describes the allowed usage of the resulting certificate, and any requirements that needs to be meet in order for the CA to allow a certificate to be used based on the template.

Enrollment Servers:

The <Public Key Services\Enrollment Servers> container holds configuration objects for the Certificate Servers that can issue certificates based on the previously mentioned templates. Essentially these objects are used to list the templates a specific CA can issue.

Enrollment Certificate:

Typically all certificate templates where the usage included <Smartcard Logon> is configured to require two-factor authentication in order to allow a certificate be generated based on it. This is achieved by setting the relevant access control list, and by configuring the template to require the certificate request to be signed by an <Enrollment Certificate>.

The Enrollment Certificate is a very powerful asset since if you are permissioned to use a template, it allows you to generate a smartcard/certificate that can be used to log an arbitrary user to the environment. So you should make sure it never ends up in the wrong hands. The system where an enrollment certificate is installed/used on is often referred to as an "Enrollment Station".

es_diag.exe

This tool allows you to:

- Verify that you can connect to the Horizon View Enrollment Server.
- List the PKI configuration for every domain that the ES domain has got a two way trust with.
- List active configurations that View Connection Servers has sent to the Enrollment Server.
- Test that certificates can be issued for a specific domain/user/template/ca combination.

If you execute the tool with no command line options it will list the available operations:

```
C:\>es_diag.exe

es_diag.exe -- True SSO Enrollment Server Diagnostics Tool 2.2.
               Copyright VMware Inc.

Usage:
es_diag.exe [/ConnectTest | /ESConfig | /ListEnvironment | /RescanEnvironment |
             /ListConfigs | /EnrollmentTest /LogonTest | /Help [args]]
Operations:
/ConnectTest       Connects to the enrollment server.
/ESConfig          Display Enrollment-Server Configuration.
/ListEnvironment   List information about the environment.
/RescanEnvironment Trigger Immediate Re-scan of the environment.
/ListConfigs       List active enrollment configurations.
/EnrollmentTest    Execute a complete enrollment-work flow.
/LogonTest         Perform a test logon using a saved certificate.
/Help              For full description of all or a specific operation.
```

Executing with /Help gives a more comprehensive listing, including all arguments associated with the different tests.

You can also ask for help for a specific operations, e.g:

```
C:\>es_diag.exe /EnrollmentTest /Help
```

The following arguments can be used with all operations:

Select Enrollment Server to execute against:

You can execute the es_diag tool from any Windows system. If you don't specify the name of the Enrollment Server it will try to connect to the ES on the local system, this will obviously fail if it's not installed.

The following optional parameters may be used to specify the name/address of the server to connect to:

```
/ESName:<NetAddress>       - Network Address of ES. default: "localhost".
```

Select authentication method:

By default, the tool will attempt to authenticate to the ES using the credentials of the currently logged on user. You can override this by specifying an alternative user-name and password. The user must either be the built-in administrator account of the ES, or a domain account that is a member of the Administrators group of the Enrollment Server. By default, due to UAC (User Account Control) you cannot use a different local user even if member of the Administrators group.

```
/ESUser:<[domain\\]UserName> - UserAccount used when connecting to the ES.
                               default: current user.
/ESPassword:<password>       - Password used when connecting to the ES.
```

When a View Connection Server is connecting to an Enrollment Server it uses a certificate to authenticate to the service. This certificate must be manually copied from the CS to the ES as part of setting up True SSO. If you execute the tool from a connection server you can use this certificate to authenticate to the ES. This avoids you having to specify a username/password, and it allows you to validate that the CS is paired correctly with the ES. The following parameters is used to specify that certificate authentication should be used:

```
/CertAuth                  - Use a Certificate to Authenticate to the ES.
                             The Horizon View Connection Server uses a
                             certificate to authenticate to the ES, when
                             this option is specified this utility will use
                             this certificate when it connects to the ES.
```

You can also select a different certificate by specifying the friendly name and the name of the certificate store where it's installed.

```
/CertFriendlyName:<name>   - Friendly name of the Certificate.
                             default: "vdm.ec".
/CertStoreName:<name>      - Certificate store for the "vdm.ec" certificate.
                             default: "VMware Horizon View Certificates".
```

Controlling the verbosity of the output from the tool:

You can choose how much information the tool displays when a test is executed using the /Debug and /Trace switches. The tool also logs key-events to the view-log file. If you want to see what's being logged but don't want to open the log-file, you can add the /LogToScreen command line argument. The tool will then write all log-messages directly to the screen, as well as to the log-file.

```
/Debug                      - Displays additional information.
/Trace                      - Displays call information.
/LogToScreen                - Displays log-messages generated by this tool
                              directly to the screen, enables /Trace
```

ConnectTest:

The ***/ConnectTest*** operation verifies that the tool can connect to the Enrollment Server. By default the tool attempts to connect to the local machine as the current user. For more information see section *Select Enrollment Server to execute against* and *Select authentication method.*

Example:

```
C:\>es_diag.exe /connecttest /EsName:plarsson-es1 /certauth /debug
Execute EnrollmentDiags::ConnectTest:
Connect to the Enrollment Service: plarsson-es1
Connected to the Enrollment Service
GetAPIVersion Successful
Open the Enrollment Context
OpenConnection Successful
Successfully connected to the Enrollment Server
CloseConnection Successful
```

ESConfig:

The **/ESConfig** operation displays the Enrollment Server (registry) Configuration.

For description of the displayed settings see the "Enrollment Server Configuration Settings" in the VMWare Horizon Administration Guide.

Note: This operation is supported by Horizon 7.13 and 8.1 and later only.

Example:

```
C:\>es_diag.exe /ESConfig
Execute EnrollmentDiags::DisplayEsConfig:
Connect to the Enrollment Service: localhost
Successfully connected to the Enrollment Server
===============
ES Computer Name    : plarsson-es1.plarsson-dom.int
ES ApiVersion       : 1.0
---------------
Enrollment Server Configuration:
   AllowLoadTest = "1"
   WarnForLonglivedCerts = "true"
   RequestQueueSize = "120"
   MaxSubmitRetryTime = "25000"
   PreferLocalCa = "false"
   LoadBasedRoundRobin = "true"
   MaxSubmitRetryTime = "25000"
   SubmitLatencyWarningTime = "1500"
---------------
```

ListEnvironment:

The ***/ListEnvironment*** operation displays information and status of all Active Directory Domains that the Enrollment Server domain has a two-way trust with. You can optionally limit the tool to display information for a specific domain only.

```
 Args:
/Domain:<EnrollmentDomain> - Restrict the listing to a specific domain.
                             By default all domains seen by the ES is listed.
                             Can't be used with the /DisplayBag - parameter
/DisplayBag                - Display the raw GetEnrollmentStatus result.
```

For additional information, please see section "*The following arguments can be used with all operations"*

Information displayed includes:

- Domains
  - Domain Name, Forest Name,
  - Status describing if the ES can reach a DC in this domain.
- Forests
  - Directory State describing if the ES can read the PKI config from this forest.
  - Enrollment Status – If the ES has got a valid Enrollment Certificate for this forest.
- Certificate Servers
  - Common Name
  - If it listed in the NTAuth Store.
  - Certificate Templates it can issue certificates for.
  - Connection Stat (if the ES got an active connection to the CA).
  - Some runtime statistics liker number issued certificates etc.
- Certificate Templates
  - Name
  - If it meets the requirements for True SSO, if not why not.
  - Minimum-key size.
  - Validity period.

Example:

```
C:\>es_diag.exe /ListEnvironment /EsName:plarsson-es1 /certauth
Execute EnrollmentDiags::ListEnvironment:
Connect to the Enrollment Service: plarsson-es1
Successfully connected to the Enrollment Server
===============
ES Computer Name   : plarsson-es1.plarsson-dom.int
ES ApiVersion      : 1.0
---------------
Domain
Domain Name        : csso-dom.certsso.int
Forest Name        : csso-dom.certsso.int
Domain State       : Ready
---------------
1 Domains
---------------
Forest
Forest Name        : csso-dom.certsso.int
Directory State    : OK
TimeSince Last Sync: 26 sec
```

```
Enroll Cert Status : Valid
  Cert Valid To    : 2020-07-27,14:14:43
---------------
Template           : SmartcardLogon
  Capability       : SmartcardManual
  Capability Notes : Request must be configured to require 1 signature
  Request hash     : SHA1
  Minimum key size : 512
  Validity Period  : 365 days
---------------
Template           : SmartcardUser
  Capability       : SmartcardManual
  Capability Notes : Request must be configured to require 1 signature
  Request hash     :
  Minimum key size : 512
  Validity Period  : 365 days
---------------
Template           : ViewSSO
  Capability       : SsoOptimal
  Capability Notes :
  Request hash     : SHA256
  Minimum key size : 2048
  Validity Period  : 1 day
---------------
3 Templates
---------------
Ca-Server          : csso-dom-CSSO-DS1-CA
  DnsHostName      : csso-ds1.csso-dom.certsso.int
  CertificateStatus: Valid
    Cert Valid To  : 2020-03-03,11:42:18
  ConnectionState  : Disconnected
  CaStatus         : Unknown
  Submit Count:
  Total SubmitCount: 0
  Since Connected  : 0
  Pending Submits  : 0
  Templates        : ViewSSO
---------------
1 Certificate Servers
---------------
1 Forests
---------------
```

Example listing when no Enrollment Certificate has been installed on the ES:

```
C:\>es_diag.exe /ListEnvironment /EsName:plarsson-es1 /certauth
Execute EnrollmentDiags::ListEnvironment:
Connect to the Enrollment Service: plarsson-es1
Successfully connected to the Enrollment Server
===============
ES Computer Name   : plarsson-es1.plarsson-dom.int
ES ApiVersion      : 1.0
---------------
Domain
Domain Name        : csso-dom.certsso.int
Forest Name        : csso-dom.certsso.int
Domain State       : Ready
---------------
1 Domains
---------------
Forest
Forest Name        : csso-dom.certsso.int
Directory State    : OK
TimeSince Last Sync: 74 sec
Enroll Cert Status : NotValid
---------------
```

RescanEnvironment:

The /RescanEnvironment operation triggers Enrollment server to immediate rescan the environment for changes the Active Directory PKI object, and locally installed Enrollment certificates.

Note: This operation is supported by Horizon 7.5 or later only.

Example:

```
C:\>es_diag.exe /RescanEnvironment /EsName:plarsson-es1
Execute EnrollmentDiags::RescanEnvironment:
Connect to the Enrollment Service: plarsson-es1
Successfully connected to the Enrollment Server
```

ListConfigs:

The ***/ListConfigs*** operation displays active Enrollment configurations. In a Horizon View Pod one Connection Server is automatically selected to periodically push the True SSO configuration to the Enrollment Servers used by the pod. All connection servers in the pod will link to this configuration.

This operation lists all current configurations, including the ClusterId, Cluster Name, how many servers is using this configuration and number of seconds since the configuration was refreshed by the 'master' server. The actual configuration will list the Domains and Certificate Servers used for these domains by the pod. Note that the ES will retain the configuration for a few minutes after the last connection server in a pod disconnected. You can optionally specify that the tool should restrict the listing to only include a specific cluster.

For additional information, please see section "*The following arguments can be used with all operations"*

```
 Optional Args:
/ClusterId:<ClusterId>     - Restrict the listing to a specific Cluster id.
                             Can't be used with the /DisplayBag - parameter
/ClusterName:<ClusterName> - Allow you to specify a Horizon View Cluster Name.
                             Can't be used with the /DisplayBag - parameter
/DisplayBag                - Display the raw GetConfigurationStatus result.
```

Example:

```
c:\es_diag.exe /ListConfigs /EsName: plarsson-es1
Execute EnrollmentDiags::ListConfigs:
Connect to the Enrollment Service: plarsson-es1
Successfully connected to the Enrollment Server
===============
Configuration
ClusterId          : da721614-d894-4997-971a-4ebe942e71bb
Cluster Name       : PLARSSON-VW1
Broker Connections : 1
Time since update  : 9 seconds
Domain Name        : plarsson-dom.int
Certificate Servers: plarsson-es1, plarsson-ds1
1 Domains configured
---------------
1 Configuration
---------------
```

EnrollmentTest

The ***/EnrollmentTest*** method executes a complete Certificate Enrollment-work flow. This will allow you to test all the key-components used for the certificate generation. If will test the Enrollment Server, ES to DC connectivity, Certificate Template settings, CA configuration , ES to CA connectivity, CA to DC connectivity and the Enrollment Certificate status.

The tool can either use an existing Enrollment configuration set by a View Connection Server (see *ListEnvironment* for more info) or you can request for a temporary (test) configuration to be created as part of the test.

The tool will connect to the ES, optionally configure the ES, request the Environment Status, build a certificate request based on the properties read from the template, submit the certificate request for a specific user to the Enrollment Server and finally perform basic validation of the resulting Certificate.

The following arguments are mandatory:

```
/Domain:<EnrollmentDomain> - FQDN of the Active Directory Domain.
/Requester:<domain\user>   - Request a certificate for this user.
/Template:<TemplateName>   - Name of Certificate Template.
```

The following arguments are optional:

```
/KeySize:<size>            - Min Key-Size, default 2048. The size specified
                             in the template will be used if greater.
```

If you want to test the CA failover/load balancing functionality, you may want to request multiple certificates. The tool allows you to request multiple certificates for each test-run.

```
/CertCount:<nn>            - Number of Certificates to request. (per thread)
                             1 (default) till 10000.

/ThreadCount:<nn>          - Number of Threads used to dispatch requests.
                             1 (default) max 64.
                             When multiple threads are used, the maximum
                             total requests are limited to 25600.

                             NOTE: Generating 1000's of test certificates
                             using multiple threads may slow down user logons
                             on a production-systems.

                             By default the enrollment server limits the
                             number of test-certificates that can be requested
                             to 500. To allow a larger number of
                             test-certificates to be requested, you need to
                             set the following value on the enrollment server:
```

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
ValueName:  AllowLoadTest
Value Type: REG_SZ
Data:       "TRUE"
```

NOTE: The AllowLoadTest setting is supported by Horizon 7.13 and 8.1 and later only.

Display the Subject name of the certificate as a DN (By default only the CN is displayed).

```
/DisplayAsDn               - Display the SubjectName as a DN.
```

Optionally save the generated certificate (but not the private key) by specifying a file-name.

```
/CertFile:<FileName>       - Write the certificate to the specified file.
```

Optionally perform a S4U logon using the generated certificate.

```
/TestLogon                 - Perform a S4U logon with the issued certificate.
                             See description of 'LogonTest' for more details.
```

If you use an existing enrollment (cluster) configuration set, and execute the ***ListEnvironment*** *before and after executing this command, you can* see from the CA statics which CA was used to generate the request by looking at the ***Submit Count*** values.

One of the following arguments should be specified if you want to use the configuration set from an existing View pod.

```
/ClusterId:<ClusterId>     - Allow you to specify a Horizon View Cluster Id.
/ClusterName:<ClusterName> - Allow you to specify a Horizon View Cluster Name.

                             If a ClusterId or ClusterName is specified the ES
                             will use the runtime configuration (CA-list) of
                             that cluster when requesting the certificate.
                             If none is specified it's necessary to specify a
                             CA to request the certificate from.
```

The following arguments are only used if no ClusterId or ClusterName is specified.
In that instance, you MUST specify at least one CaServer. The tool will then request that the ES creates a new configuration set, wait (default up to 10 sec) for it to be ready and there after use this temporary configuration set when requesting the certificate. This allows you to test a template or CA even if it's not currently used by any Connection Server.

```
/CaServer:<CA>             - Certificate Server(s) to use.
                             Can be specified multiple times.
/WaitForSync:<sec>         - Number of seconds to wait for the ES to connect
                             to and read the active directory. (default 10)
```

For additional information, please see section "*The following arguments can be used with all operations"*

LogonTest

The ***/LogonTest*** method performs a S4U logon using the specified certificate.
This will send a Logon request to a domain controller using a certificate to perform the logon. This will result in basic certificate validation and some aspect of the Domain Controller configuration.

NOTE: for this test to be successful; You MUST be logged on using a domain account to a system that is a member of a domain that has got a two-way trust with the domain that the user-certificate is issued for. The trust requirements are less strict when performing a real True-SSO logon. Not all logon aspects are tested so a success / failure of this test is NOT a guarantee of the same result when performing a genuine True-SSO logon.

The following argument is mandatory:

```
/CertFile:<FileName>    - Read the certificate from the specified file.
                          See description of 'EnrollmentTest' for details of
                          how to generate a test certificate.
```

Display the Subject name of the certificate as a DN (By default only the CN is displayed).

```
/DisplayAsDn              - Display the SubjectName as a DN.
```

Example, using an existing enrollment configuration set; connect to plarsson-es1, request a certificate based on template ViewSSO for user csso-dom\administrator,

```
c:\>es_diag.exe /enrollmenttest /esNAme:plarsson-es1/certauth /domain:csso-dom.certsso.int
/clusterid:6a2eeb21-8868-4a0e-bd6d-619037c6b0a9 /requester:csso-dom\administrator
/template:ViewSSO

Execute EnrollmentDiags::EnrollmentTest:
Connect to the Enrollment Service: plarsson-es1
Use the configuration for ClusterId: 6a2eeb21-8868-4a0e-bd6d-619037c6b0a9
Connect to the Enrollment Service: plarsson-es1
Successfully connected to the Enrollment Server
Successfully requested a Certificate
Subject   : Administrator
UPN:      : administrator@csso-dom.certsso.int
EMAIL:    : administrator@certsso.int
SerialNo  : DE:63:0E:00:00:00:D6:CE:C6:61
UTC Time  : 2016-03-23,17:34:17
Valid From: 2016-03-23,17:24:15
Valid To  : 2016-03-24,17:24:15
Validity  : Certificate is valid
```

Example, using a temporary enrollment configuration set; connect to plarsson-es1, request a certificate based on template ViewSSO for user csso-dom\administrator.

```
C:\>es_diag.exe /enrollmenttest /esNAme:plarsson-es1 /certauth /domain:csso-dom.certsso.int
/caserver:csso-dom-CSSO-DS1-CA /requester:csso-dom\administrator /template:ViewSSO /debug

Execute EnrollmentDiags::EnrollmentTest:
Connect to the Enrollment Service: plarsson-es1
Connected to the Enrollment Service
GetAPIVersion Successful
Open the Enrollment Context
OpenConnection Successful
Successfully connected to the Enrollment Server
Configure the enrollment service for the selected domain
Wait for up to 10 sec for the ES to Sync with the domain
Use CAServer: csso-dom-CSSO-DS1-CA
SetConfiguration Successful
Get Enrollment Propeties
GetEnrollmentStatus Successful
Successfully Retrieved the Enrollment Status
Generate a PKCS10 Certificate Request
Send a Cert-Request to the enrollment service: (1/1)
Successfully requested a Certificate
Successfully requested a certificate: (1/1)
CloseConnection Successful
Subject   : Administrator
UPN:      : administrator@csso-dom.certsso.int
EMAIL:    : administrator@certsso.int
SerialNo  : E0:63:0E:00:00:00:4B:65:C8:61
UTC Time  : 2016-03-23,17:36:01
Valid From: 2016-03-23,17:26:00
Valid To  : 2016-03-24,17:26:00
Validity  : Certificate is valid
```

Example, attempt to request a certificate based on a template that the enrollment server doesn't' have enrollment permission to.

```
C:\>es_diag.exe /enrollmenttest /esNAme:plarsson-es1 /certauth /domain:csso-dom.certsso.int
/clusterid:6a2eeb21-8868-4a0e-bd6d-619037c6b0a9 /requester:csso-dom\administrator
/template:ViewSSO
Execute EnrollmentDiags::EnrollmentTest:
Connect to the Enrollment Service: plarsson-es1
Use the configuration for ClusterId: 6a2eeb21-8868-4a0e-bd6d-619037c6b0a9
Connect to the Enrollment Service: plarsson-es1
Successfully connected to the Enrollment Server
SubmitRequest Failed
Response    ErrorCode = "-2146877422"
   ErrorText = "Denied by Policy Module - 0x0000000080094012 (The permissions on the
certificate template do not allow the current user to enroll for this type of
certificate.)"
   FailureReason = "SubmitFailureMayRetry"
```

Example, executing ListEnvironment AFTER having requested some certificates, note that the Submit count now displays how many certificates that has been issued.

```
Execute EnrollmentDiags::ListEnvironment:
Connect to the Enrollment Service: plarsson-es1
. . .
Successfully Retrieved the Enrollment Status
===============
ES Computer Name   : plarsson-es1.plarsson-dom.int
ES ApiVersion      : 1.0
---------------
Domain
Domain Name        : csso-dom.certsso.int
. . .

---------------
Ca-Server          : csso-dom-CSSO-DS1-CA
  DnsHostName      : csso-ds1.csso-dom.certsso.int
  CertificateStatus: Valid
    Cert Valid To  : 2020-07-27,14:14:43
  ConnectionState  : Connected
  CaStatus         : OK
  Submit Count:
  Total SubmitCount: 4
  Since Connected  : 4
  Pending Submits  : 0
  Templates        : ViewSSO
---------------
1 Certificate Servers
---------------
```