Understand ISE Internal Certificate Authority Services

Contents

Introduction

This document describes the CA service and the Enrollment over Secure Transport (EST) service that is present in Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE
- Certificates and Public Key Infrastructure (PKI)
- Simple Certificate Enrollment Protocol (SCEP)
- Online Certificate Status Protocol (OCSP)

Components Used

The information in this document is based on Identity Services Engine 3.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

Certificate Authority (CA) Service

Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). The Cisco ISE Internal Certificate Authority (ISE CA) issues and manages digital certificates for endpoints from a centralized console in order to allow employees to use their personal devices on the network of company. A CA-signed digital certificate is considered an industry standard and more secure. The Primary Policy Administration Node (PAN) is the Root CA. The Policy Service Nodes (PSNs) are subordinate CAs to the Primary PAN.

ISE CA Functionality

The ISE CA offers this functionality:

- Certificate Issuance: Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to the network.
- Key Management: Generates and securely stores keys and certificates on both PAN and PSN nodes.
- Certificate Storage: Stores certificates that are issued to users and devices.
- Online Certificate Status Protocol (OCSP) Support: Provides an OCSP responder to check the validity of certificates.

ISE CA Certificates Provisioned on Administration and Policy Service Nodes

After installation, a Cisco ISE node is provisioned with a Root CA certificate and a Node CA certificate to manage certificates for endpoints.

When a deployment is set up, the node that is designated as the Primary Administration Node (PAN) becomes the Root CA. The PAN has a Root CA certificate and a Node CA certificate that is signed by the Root CA.

When a Secondary Administration Node (SAN) is registered to the PAN, a Node CA certificate is generated

and is signed by the Root CA on the Primary Administration Node.

Any Policy Service Node (PSN) that is registered with the PAN is provisioned an Endpoint CA and an OCSP certificate that is signed by the Node CA of the PAN. The Policy Service Nodes (PSNs) are subordinate CAs to the PAN. When the ISE CA is used, the Endpoint CA on the PSN issues the certificates to the endpoints that access the network.

Note: From ISE 3.1 Patch 2 and ISE 3.2 FCS, OCSP Certificate Hierarchy has been changed.

As per RFC 6960:

â€œA certificate issuer MUST do one of the following:

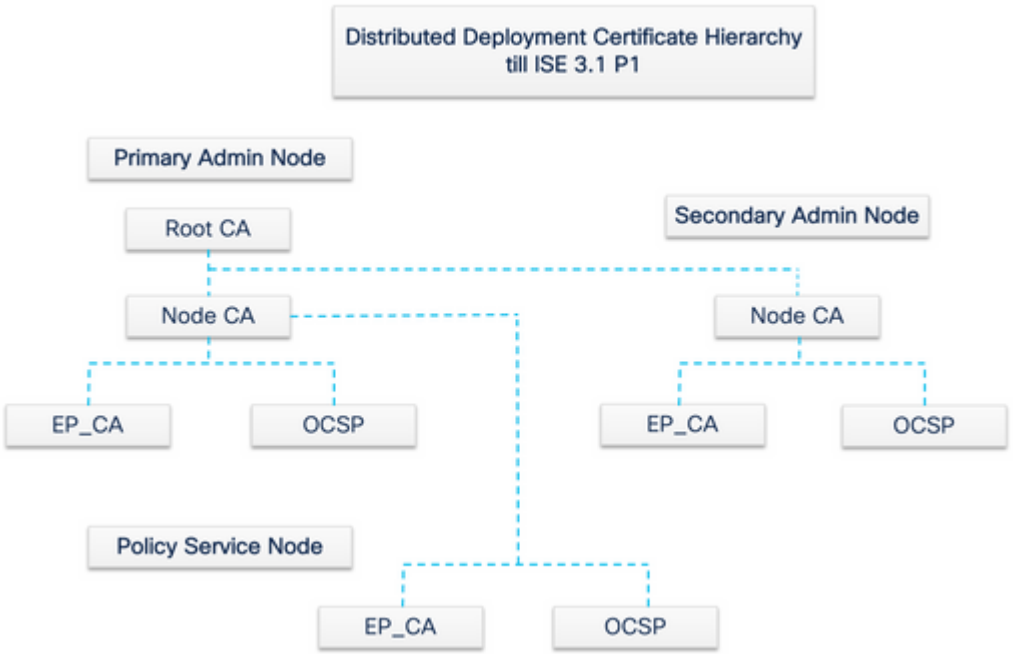
- sign the OCSP responses itself, or

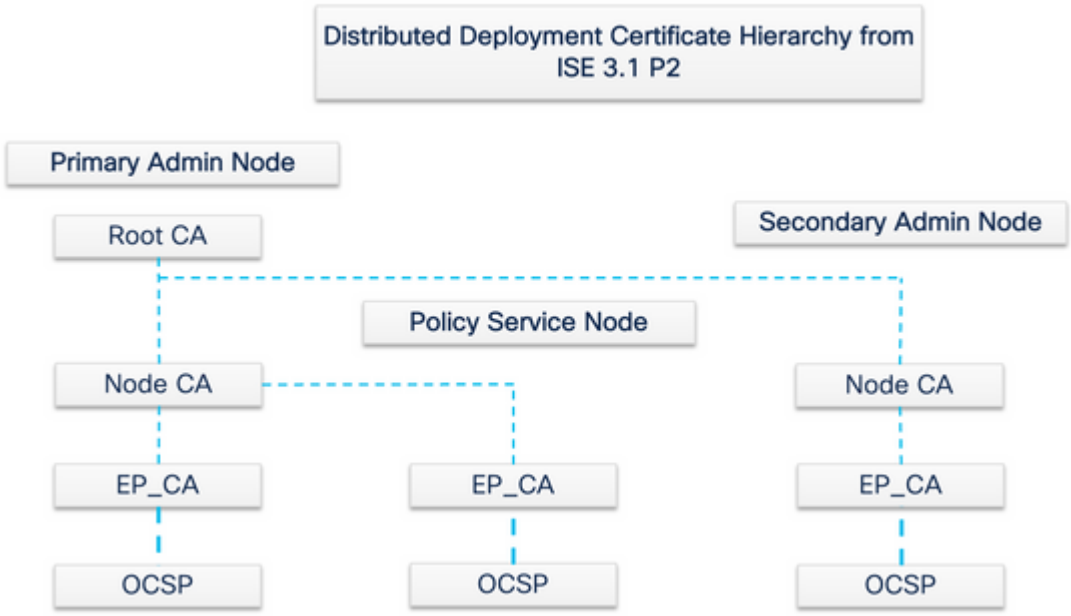
- explicitly designate this authority to another entityâ€

â€œOCSP response signer's certificate MUST be issued directly by the CA that is identified in the request. â€œ

â€œSystem (relies) on OCSP responses MUST recognize a delegation certificate as issued by the CA that issued the certificate in question only if the delegation certificate and the certificate (is) checked for revocation were signed by the same key.â€

In order to be compliant with the previously mentioned RFC Standard, the certificate hierarchy for OCSP Responder Certificate is changed in ISE. OCSP Responder Certificate is now issued by Endpoint Sub CA of the same node instead of Node CA in PAN.





Enrollment over Secure Transport (EST) Service

The concept of public key infrastructure (PKI) has existed for a long time. The PKI authenticates the identity of users and devices by means of signed public key pairs in the form of digital certificates. Enrollment over Secure Transport (EST) is a protocol to provide these certificates. EST service defines how to perform certificate enrollment for clients that use Certificate Management over Cryptographic Message Syntax (CMC) over a secure transport. As per the IETF - â€œEST describes a simple, yet functional, certificate management protocol that targets Public Key Infrastructure (PKI) clients that need to acquire client certificates and associated Certification Authority (CA) certificates. It also supports client-generated public/private key pairs as well as key pairs generated by the CA.â€

EST Use Cases

The EST protocol can be used:

- To enrol Network Devices by means of Secure Unique Device Identity
- For BYOD Solutions

Why EST?

Both EST and SCEP protocols address certificate provisioning. EST is a successor to the Simple Certificate Enrollment Protocol (SCEP). Because of its simplicity, SCEP has been the de facto protocol in certificate provisioning for many years. However, the use of EST over SCEP is recommended for these reasons:

- Use of TLS for secure transport of certificates and messages - In EST, the certificate signing request (CSR) can be tied to a requester that is already trusted and authenticated with TLS. Clients cannot get a certificate for anyone but themselves. In SCEP, the CSR is authenticated by a shared secret between the client and the CA. This introduces security concerns because someone with access to the shared secret can generate certificates for entities other than themselves.
- Support for enrollment of ECC-signed certificates - EST provides cryptographic agility. It supports elliptic curve cryptography (ECC). SCEP does not support ECC and depends on RSA encryption. ECC offers more security and better performance than other cryptographic algorithms like RSA even while it uses a much smaller key size.
- EST is built to support automatic certificate re-enrollment.

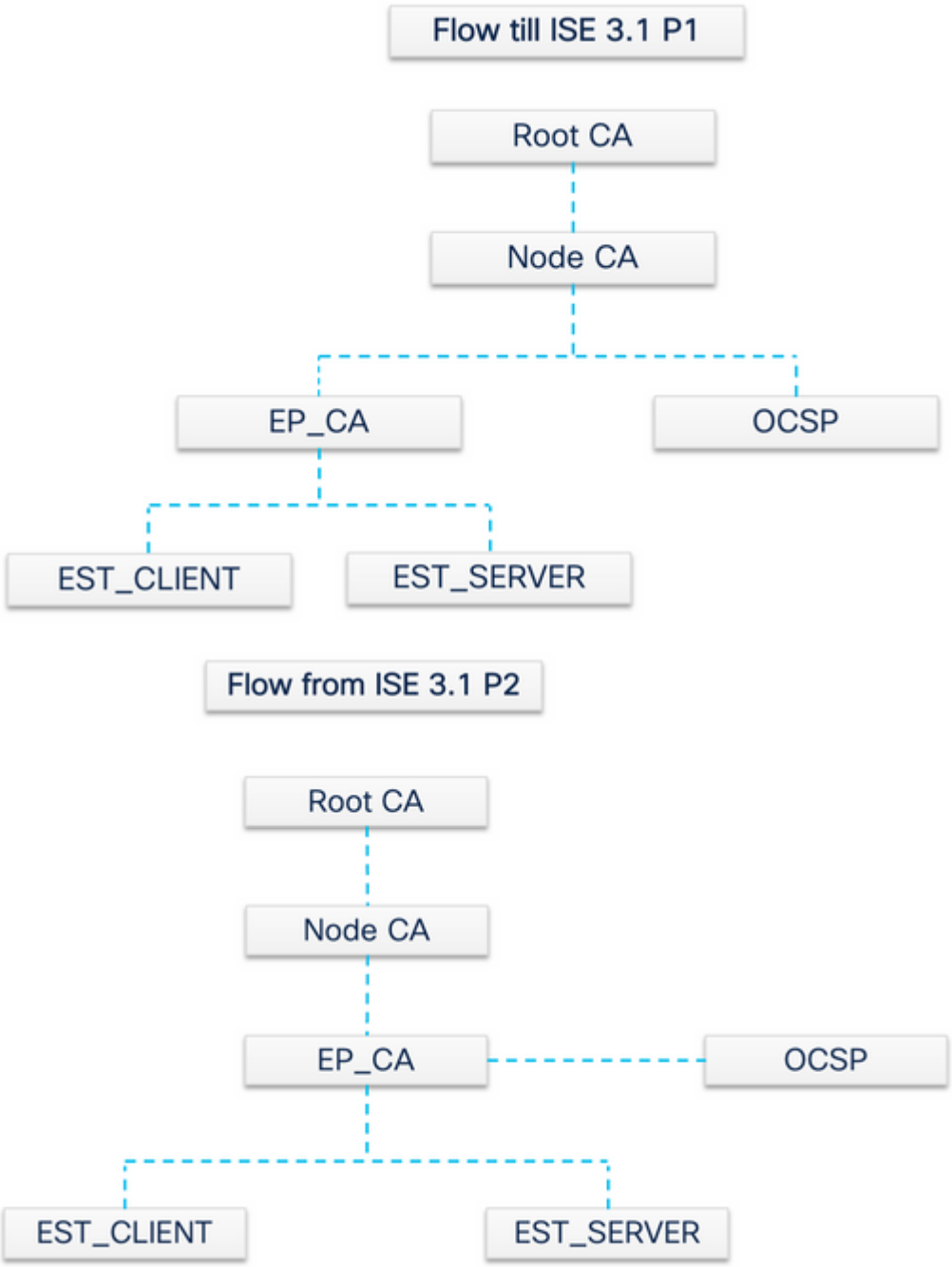
TLS proven security and continuous improvement help ensure that EST transactions are secure in terms of cryptographic protection. SCEP tight integration with RSA to protect data introduces security concerns as technology advances.

EST in ISE

In order to implement this protocol, a client and a server module are needed:

- EST Client - embedded in the regular ISE tomcat.
- EST Server - deployed on an open-source web server called NGINX. This runs as a separate process, and it listens on port 8084.

Certificate-based client and server authentication is supported by EST. The endpoint CA issues the certificate for the EST client and the EST server. The EST Client and Server certificates and their respective keys are stored in ISE CAâ€™s NSS DB.



Types of Requests in ISE EST

Whenever the EST server comes up, it gets the latest copy of all of the CA certificates from the CA server and stores it. Then, the EST client can make a CA certificate request to get the whole chain from this EST server. Before it makes a simple enrollment request, the EST client has to issue the CA certificate request first.

CA Certificates Request (based on RFC 7030)

1. The EST client requests a copy of the current CA certificates.
2. HTTPS GET message with an operation path value of /cacerts.
3. This operation is performed before any other EST requests.
4. A request is made every 5 minutes to get a copy of the most up-to-date CA certificates.
5. The EST server must not require client authentication.

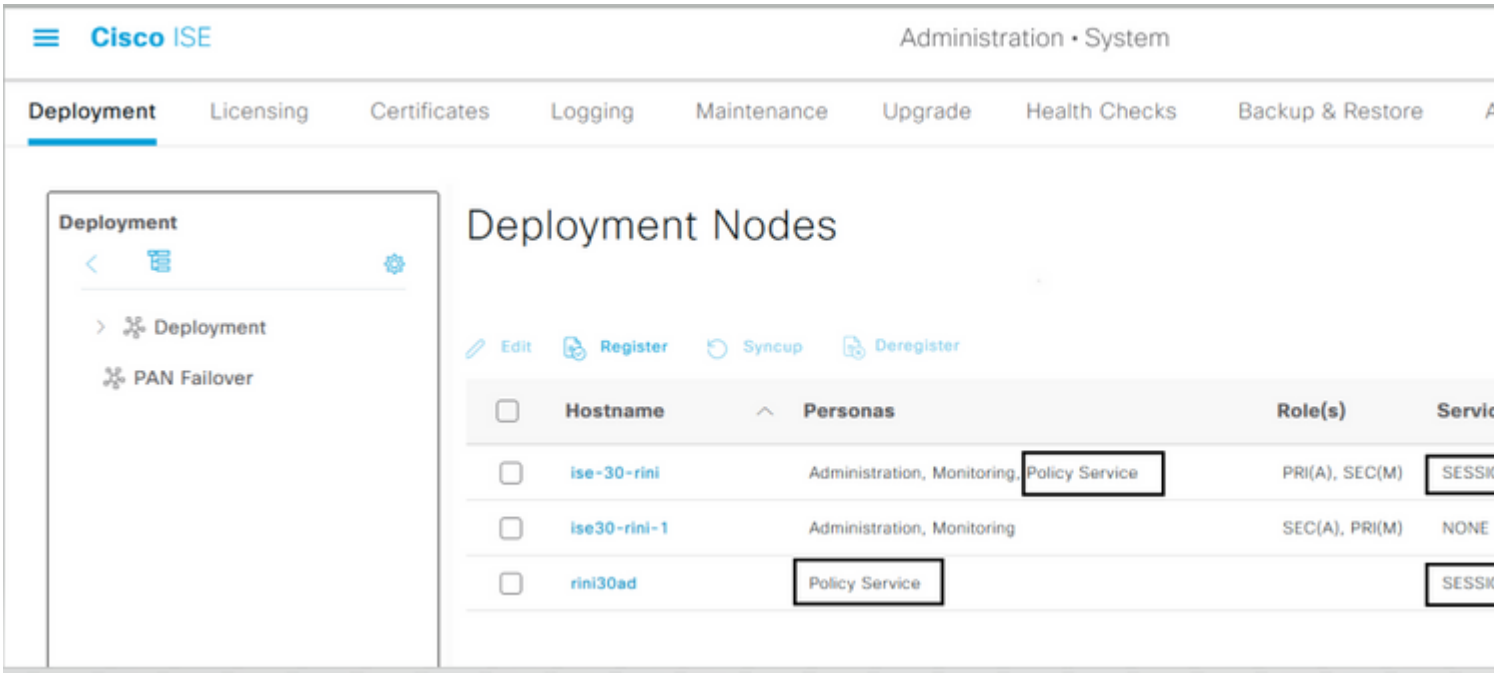
The second request is a simple enrollment request and it needs authentication between the EST client and the EST server. This happens each time an endpoint connects to ISE and makes a certificate request.

Simple Enrollment Request (based on RFC 7030)

1. The EST client requests a certificate from the EST server.
2. HTTPS POST message with the operation path value of /simpleenroll.
3. The EST client embeds the PKCS#10 request within this call which is sent to ISE.
4. The EST server must authenticate the client.

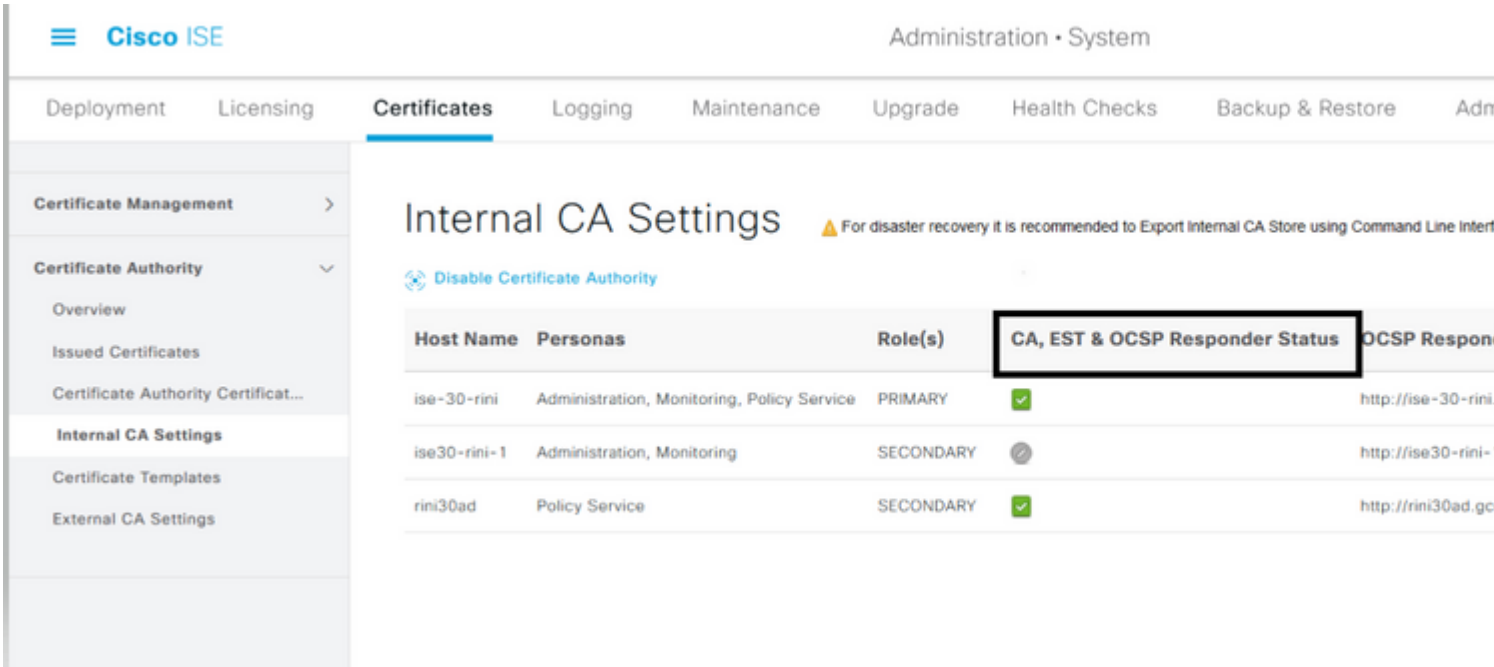
EST and CA Service Status

CA and EST services can only run on a Policy Service node that has session services enabled on it. In order to enable session services on a node, navigate to Administration > System > Deployment . Select the server hostname on which session services need to be enabled and click Edit . Select the **Enable Session Services** check box under Policy Service persona.



Status Shown on GUI

EST service status is tied to the ISE CA service status on ISE. If the CA service is up, then the EST service is up and if the CA service is down, the EST service is also down.



Status Shown on CLI

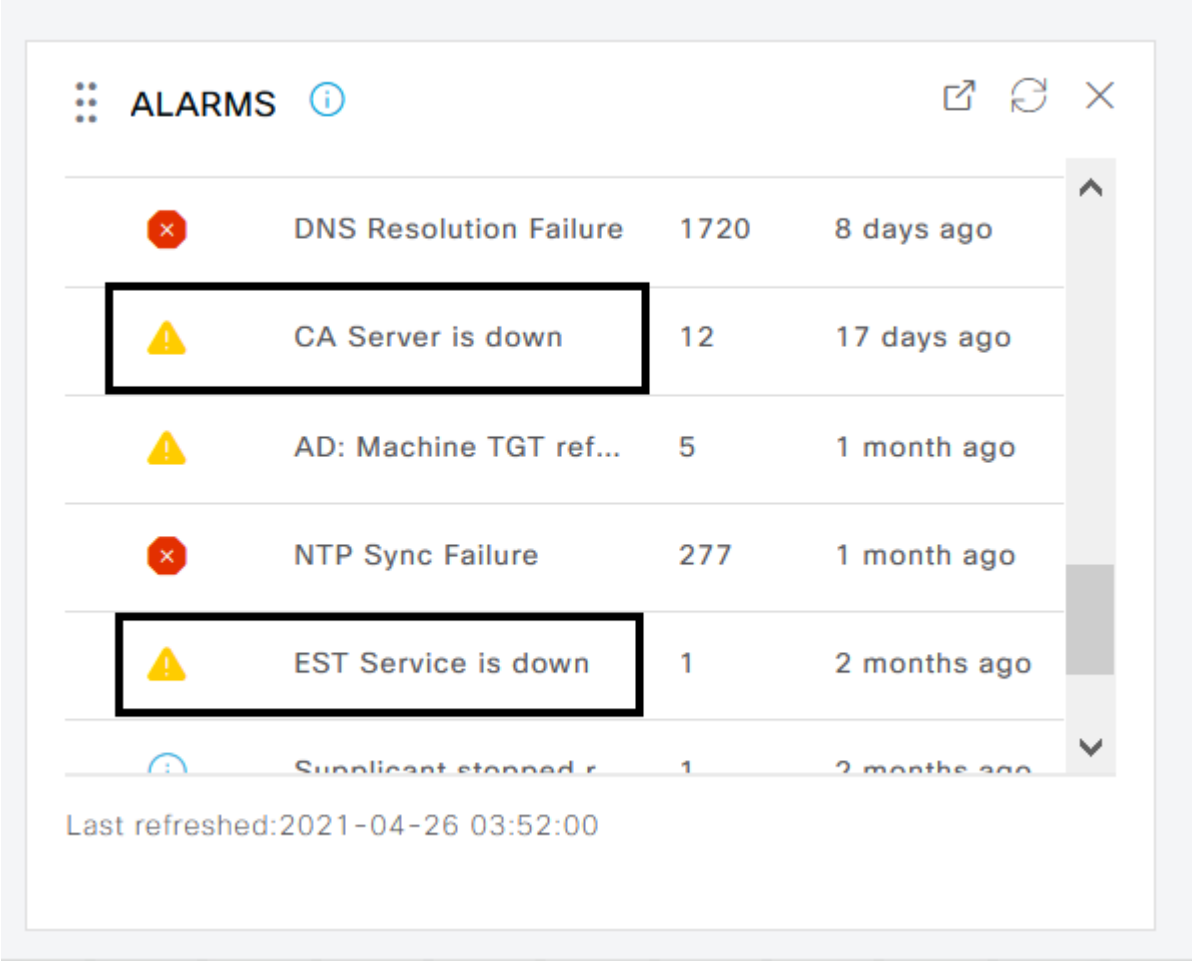
```
ise-30-rini/admin# sh app status ise

ISE PROCESS NAME                          STATE            PROCES
----------------------------------------------------------------
Database Listener                         running          61993
Database Server                           running          159 PR
Application Server                        running          72240
Profiler Database                         running          68224
ISE Indexing Engine                       running          74972
AD Connector                              running          78912
M&T Session Database                      running          68007
M&T Log Processor                         running          70533
Certificate Authority Service             running          63090
EST Service                               running          64492
SXP Engine Service                        disabled
Docker Daemon                             running          64427
TC-NAC Service                            disabled
pxGrid Infrastructure Service             disabled
pxGrid Publisher Subscriber Service       disabled
pxGrid Connection Manager                 disabled
```

```
ise30-rini-1/admin# sh app stat ise

ISE PROCESS NAME                       STATE            PROCES
----------------------------------------------------------------
Database Listener                      running          21387
Database Server                        running          101 PR
Application Server                     running          33099
Profiler Database                      running          29212
ISE Indexing Engine                    running          34969
AD Connector                           running          36017
M&T Session Database                   running          29020
M&T Log Processor                      running          33296
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          24186
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
```

```
rini30ad/admin# sh app status ise

ISE PROCESS NAME                       STATE            PROCES
----------------------------------------------------------------
Database Listener                      running          18903
Database Server                        running          93 PRO
Application Server                     running          35168
Profiler Database                      running          30941
ISE Indexing Engine                    disabled
AD Connector                           running          35800
M&T Session Database                   disabled
M&T Log Processor                      disabled
Certificate Authority Service          running          92557
EST Service                            running          99310
SXP Engine Service                     disabled
Docker Daemon                          running          23637
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
```

Alarms on Dashboard

The alarm is shown on the ISE dashboard if EST and CA services are down.



Impact if CA and EST services are not running

- EST Client /cacerts call failure can happen when EST Server is down. The /cacerts call failure can also happen if the EST CA chain certificate CA chain is incomplete.
- ECC-based endpoint certificate enrollment requests fail.
- BYOD flow breaks if either of the previous two failures occurs.
- Queue Link Error alarms can be generated.

Troubleshoot

If the BYOD flow with EST protocol does not work properly, check these conditions:

- Certificate Services Endpoint Sub CA certificate chain is complete. In order to check whether the certificate chain is complete:
    1. Navigate to Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates .
    2. Select the check box next to the certificate and click **View** in order to check a particular certificate.
- Ensure that the CA and EST services are up and running. If the services are not running, navigate to Administration > System > Certificates > Certificate Authority > Internal CA Settings in order to enable the CA service.
- If an upgrade has been performed, replace the ISE Root CA certificate chain after the upgrade. In order to do this:

1. Choose Administration > System > Certificates > Certificate Management > Certificate Signing Requests .
2. Click Generate Certificate Signing Requests (CSR).
3. Select ISE Root CA in the Certificate(s) will be used for the drop-down list
4. Click Replace ISE Root CA Certificate Chain .

- Useful debug that can be enabled to check the logs include est , provisioning , ca-service , and ca-service-cert . Refer to ise-psc.log , catalina.out , caservice.log , and error.log files.

Related Information

- **Cisco Technical Support & Downloads**