ExtremeCloud IQ - Site Engine and ExtremeControl Secure Communication

ExtremeCloud IQ - Site Engine and ExtremeControl use server certificates to provide secure communication for application web pages and for internal communication between server components. While these certificates provide secure communication, there can be cases where you want to update a server certificate to a custom certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which ExtremeCloud IQ - Site Engine and/or ExtremeControl must communicate. Additionally, you can use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access application web pages.

NOTE: ExtremeCloud IQ - Site Engine automatically generates alarms as the ExtremeControl Engine Internal Communications Server Certificate, the Captive Server Portal Server Certificate, the RADIUS Server Certificate, the AAA Configuration Truststore, and the ExtremeControl Appliance Truststore approach their expiration date. ExtremeCloud IQ - Site Engine generates a Notification alarm 30 days before expiring, a Warning alarm 7 days before expiring, and a Critical alarm when the certificate expires.

This document describes the process for updating the different ExtremeCloud IQ - Site Engine and ExtremeControl server certificates, providing a general workflow along with links to detailed instructions. Use the following table to determine what sections of this document might be useful for your ExtremeCloud IQ - Site Engine deployment.

Deployment Model	Refer to the Following Sections
ExtremeCloud IQ - Site Engine Only	Updating the ExtremeCloud IQ - Site Engine Server Certificate
ExtremeCloud IQ - Site Engine with ExtremeControl	Updating the ExtremeCloud IQ - Site Engine Server Certificate Updating the Captive Portal Server Certificate Updating the ExtremeControl Engine Internal Communications Server Certificate

Deployment Model	Refer to the Following Sections
ExtremeCloud IQ - Site Engine with ExtremeControl with Agent-Based Assessment	Updating the ExtremeCloud IQ - Site Engine Server Certificate Updating the Captive Portal Server Certificate Updating the ExtremeControl Engine Internal Communications Server Certificate Updating the Certificate Configuration for ExtremeControl Agent-Based Assessment

In addition, this document provides information about options for configuring advanced security settings, as well as reference information and a glossary of certificate management terminology.

Updating the ExtremeCloud IQ - Site Engine Server Certificate

The ExtremeCloud IQ - Site Engine server uses a private key and server certificate to provide secure communication for administrative web pages, ExtremeControl, and for internal communication between servers.

During installation, ExtremeCloud IQ - Site Engine generates a new, unique private server key and server certificate for the ExtremeCloud IQ - Site Engine server. While these provide secure communication, there can be cases where you want to update to a certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which ExtremeCloud IQ - Site Engine must communicate. Additionally, you can use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access web pages.

NOTE: If you are using the advanced security options, be sure the client certificate trust mode and server certificate trust mode are configured appropriately before updating the ExtremeCloud IQ - Site Engine server certificate.

You need a server private key and server certificate to perform the certificate replacement. If you do not have these, you need to generate them.

Here is the general workflow for updating the server certificate. For complete instructions, see Update the ExtremeCloud IQ - Site Engine Server Certificate.

1. If necessary, generate a server private key and server certificate:
    a. Generate a server private key.
    b. Create a Certificate Signing Request.
    c. Submit the request to a Certificate Authority or generate a self-signed certificate.
    d. Verify the contents of the server certificate.
2. Verify that you have met the certificate requirements.
3. Replace the existing certificate with the new certificate.
4. Enforce the appliance to deploy the new private key and server certificate.
5. Verify the certificate.

NOTE: When you change the ExtremeCloud IQ - Site Engine server certificate, the NAC Request Tool can no longer connect to the ExtremeCloud IQ - Site Engine server and you need to Update the NAC Request Tool Truststore.

Updating the ExtremeControl Captive Portal Server Certificate

The ExtremeControl engine uses a private key and server certificate to provide secure communication for ExtremeCloud IQ - Site Engine captive portal web pages.

During installation, ExtremeCloud IQ - Site Engine generates a unique private server key and server certificate for the captive portal server. While these provide secure communication, you can update to a "browser-friendly" certificate in order to eliminate the browser warnings that might appear when end users access captive portal web pages for registration or remediation, and when administrators and sponsors access the ExtremeControl registration administration and sponsor administration web pages.

You need a server private key and server certificate to perform the certificate replacement. If you do not have these, you need to generate them.

Here is the general workflow for updating the server certificate.

1. If necessary, generate a server private key and server certificate:
    a. Generate a server private key.
    b. Create a Certificate Signing Request.
    c. Submit the request to a Certificate Authority or generate a self-signed certificate.
    d. Verify the contents of the server certificate.
2. Verify that you have met the certificate requirements.
3. Replace the existing certificate with the new certificate.
4. Enforce the appliance to deploy the new private key and server certificate.
5. Verify the certificate.

Updating the ExtremeControl Engine Internal Communications Server Certificate

The ExtremeControl engine Internal Communications server uses a private key and server certificate to provide secure communication between the engine and the ExtremeCloud IQ - Site Engine server, other ExtremeControl engines, and ExtremeControl assessment servers. It also provides secure communication for the ExtremeControl administrative web pages and with the assessment agent.

During installation, ExtremeCloud IQ - Site Engine generates a unique private server key and server certificate for the Internal Communications server. While these provide secure communication, there can be cases where you want to update the Internal Communications server certificate to a custom certificate provided from an external certificate authority, or add certificates in order to meet the requirements of external components with which ExtremeControl must communicate. Additionally, you can use a "browser-friendly" certificate so that users don't see browser certificate warnings when they access administrative web pages.

You need a server private key and server certificate to perform the certificate replacement. If you do not have these, you need to generate them.

NOTE: If you are using the advanced security options, be sure the client certificate trust mode and server certificate trust mode are configured appropriately before updating the Internal Communications server certificate.

The general workflow for updating the server certificate:

1. If necessary, generate a server private key and server certificate:
   a. Generate a server private key.
   b. Create a Certificate Signing Request.
   c. Submit the request to a Certificate Authority or generate a self-signed certificate.
   d. Verify the contents of the server certificate.
2. Verify that you have met the certificate requirements.
3. Replace the existing certificate with the new certificate.
4. Enforce the appliance to deploy the new private key and server certificate.
5. Verify the certificate.

NOTE: If you are using the advanced security options, be sure the client certificate trust mode and server certificate trust mode are configured appropriately before updating the assessment server certificate.

Advanced Security Options

Trust mode settings let you specify how ExtremeCloud IQ - Site Engine clients and server components handle the server certificates used to provide secure network communications. These settings can be set to a strict mode as a way to provide even greater network security, if desired. You can access client certificate trust mode and server certificate trust mode settings on the Administration > **Certificates** tab.

Client Certificate Trust Mode

The client certificate trust mode specifies how ExtremeCloud IQ - Site Engine clients handle a server certificate they receive. You can set the trust mode in the Update Client Certificate Trust Mode window.

By default, the trust mode is set to "Prompt" so that if a client encounters a new certificate that is does not trust, the user is prompted to either accept or reject the new certificate. If the server certificate has been replaced and the user expects to see the new certificate,

then they can accept the certificate if it is correct. If the server certificate has not been replaced and the client has inadvertently connected to a server that is not trusted, then the user can reject the certificate.

For the highest level of security, change the trust mode to the "Strict" setting where if a client encounters a new certificate that is does not trust, the certificate is rejected and the client connection fails. While this option is the most secure, if the server certificate is replaced, the new certificate will be rejected. Therefore, if you are replacing a server certificate, you should revert back to the "Prompt" trust mode until all client users have accepted the new certificate.

Server Certificate Trust Mode

The server certificate trust mode specifies how servers will handle the certificates they receive from other servers. You can set the trust mode in the Update Server Certificate Trust Mode window.

Depending on your deployment, there can be potentially many servers in ExtremeCloud IQ - Site Engine and ExtremeControl. For example, there is the ExtremeCloud IQ - Site Engine server, the ExtremeControl appliance servers, and ExtremeControl assessment servers. In addition, there might be external servers such as LDAP servers that both ExtremeCloud IQ - Site Engine and ExtremeControl can communicate with. As these different servers communicate, they use server certificates to determine whether or not they will trust each other.

By default, the server certificate trust mode is set to "Trust All" certificates. This mode is primarily used while setting up an ExtremeCloud IQ - Site Engine/ExtremeControl deployment. Following this initial phase, you can change the trust mode to "Trust and Record." In this mode, all certificates from other servers continue to be accepted without a trust check, but each server also records the certificate that it receives and associates that certificate with the sending server. In this way, each server builds their own set of recorded certificates, creating a list of certificates that they trust. It is important to give this phase enough time so that connections between the various servers can take place and all certificates are recorded. When you are confident that all certificates have been exchanged and recorded, you can change the trust mode to "Locked," providing the highest level of security.

In the "Locked" trust mode, any certificate from another server must match the certificate that was recorded for that server during the "Trust and Record" phase. If the server certificate does not match, then the server is not trusted. The "Locked" mode provides an extra level of security intended to detect and prevent someone from spoofing a server. If an IP address or hostname is hijacked and connections are routed to another server, that server is not trusted.
While the "Locked" mode is the most secure, if any server certificate is replaced, the new

certificate is rejected. Therefore, if you are replacing a server certificate, you should revert back to the "Trust and Record" mode until the new certificate has been recorded.

When the trust mode is changed, the ExtremeCloud IQ - Site Engine server is immediately changed to use the new mode. ExtremeControl appliances begin using the new trust mode when they are enforced.

Reference Information

Updating the NAC Request Tool Truststore

If you change the ExtremeCloud IQ - Site Engine server certificate, the NAC Request Tool can no longer connect to the ExtremeCloud IQ - Site Engine server and you see an error message such as:

```
14:11:02,070 ERROR NacRequest:1625 - The security certificate
presented is not trusted from NacWebService at IP: 120.110.92.12
14:11:02,072 DEBUG NacRequest:1696 - Exiting with code: REMOTE(6)
```

To configure the NAC Request Tool to trust the ExtremeCloud IQ - Site Engine server's certificate, use the `acceptcert` operation:

```
    NacRequest -server <server IP> -username <username> -
password <password> -oper acceptcert
```

This command modifies data in the directory where the NAC Request Tool is stored, and allows you to continue to use the NAC Request Tool.

How to Add OpenSSL to Your Path

Some certificate management operations (such as generating and verifying server certificates) use OpenSSL software to perform certain tasks. OpenSSL is available on the ExtremeCloud IQ - Site Engine server, the ExtremeControl engine, or can be downloaded from http://www.openssl.org. After downloading and installing OpenSSL, add the OpenSSL tool to your path using the following commands:

For bash shell: `export PATH=$PATH:<OpenSSL install dir>/bin`

For tsch or csh shell: `set PATH = ($PATH <OpenSSL install dir>/bin)`

Glossary

Certificate
A document that identifies a server or a client (user), containing a public key and signed by a certificate authority.

Certificate Authority (CA)
A trusted third-party that generates and signs certificates. A CA can be a commercial concern, such as Go Daddy or GeoTrust. A CA can also be an in-house server for certificates used within an enterprise.

CA Certificate
A certificate identifying a certificate authority. A CA certificate can be used to verify that a certificate issued by the certificate authority is legitimate.

Certificate Chain
An ordered set of certificates which can be used to verify the identity of a server or client. It begins with a client or server certificate, and ends with a certificate that is trusted.

Certificate Issuer
The certificate authority that generated the certificate.

Certificate Signing Request (CSR)
A document containing identifiers, options, and a public key, that is sent to a certificate authority in order to generate a certificate.

Certificate Subject
The server or client identified by the certificate.

Client Certificate
A certificate identifying a client (user). A client certificate can be used in conjunction with, or in lieu of, a username and password to authenticate a client.

Intermediate Certificate
A certificate in the middle of a certificate chain, that bridges the trust relationship between the server certificate and the trusted certificate.

Legacy Certificate
The certificates that shipped with NetSight and NAC 4.0.0 and earlier.

PKCS #8
(Public-Key Cryptography Standard #8) One of several standard formats which can be used to store a private key in a file. It can optionally be encrypted with a password.

Server Certificate

A certificate identifying a server. When a client connects to the server, the server sends its certificate to the client and the client validates the certificate to trust the server.

Spoofing

Hijacking a server's IP address or hostname so that requests to the server are redirected to another server. Certificate validation is used to detect and prevent this.

Truststore

A repository containing trusted certificates, used to validate an incoming certificate. A truststore usually contains CA certificates, which represent certificate authorities that are trusted to sign certificates, and can also contain copies of server or client certificates that are to be trusted when seen.

10/2021
PN:9037217-00