ICE Private Certificate Stores

Product guide for prerelease

Document version 1841, produced on Friday, September 06, 2024.

main 90adc8bf40040649230176bbdd465f6261a2d8e0

Contents

1 Introduction

This section provides instructions for creating .certstore bundles for use in updating and maintaining certificates. Instant Connect provides for the management of certificate bundles through **certstore,** and **esctools.** Certstore is a proprietary file format employed by Instant Connect to encapsulate certificate bundles. Ecstools is a command line tool for managing certificate bundles.

During installation, ICE installs default versions of all the certificates listed in this section. Those certificates are automatically provisioned throughout the Instant Connect system. Administrators have access to update these certificates according to the policies of their organization.

- **REQUIREMENT** Managing certificates requires **ecstool.** Download ecstool for Linux, macOS, or Windows from the Instant Connect Support Portal.

1.1 Bundle Types:

Instant Connect installs default versions of all the certificates listed below. They are provisioned throughout the system after installation. An administrator can apply a different set of certificates at any time. Instant Connect uses the following three sets of certificates (bundles):

1. A **client certificate bundle,** consisting of the identity certificate that clients will present to a Rallypoint, the private key associated with the certificate, and the CA certificate that will be used to verify the identity certificate presented by the Rallypoint. This certificate bundle is distributed to all ICE Mobile and ICE Desktop clients.
2. A **server certificate bundle,** consisting of the identity certificate that Rallypoints will present to clients, the private key associated with this certificate, and the CA certificate that will be used to verify the identity certificate presented to Rallypoints by ICE clients. This certificate bundle is distributed to all Rallypoints.
3. An **infrastructure certificate bundle,** consisting of all the aforementioned certificates: The client and Rallypoint identity certificates, their private keys and the CA certificates used to verify them. This certificate bundle is distributed to server-side infrastructure (like radio and telephony gateways, and patch servers).

1.1.1 Interoperability Validation Constraints

While certificate bundles are distinct elements, their contents must be inter-related. When supplying a new configuration of certificate bundles, ICE Server validates that all three certificate bundles interoperate by ensuring the following constraints are met:

- Each identity certificate must have a valid private key.
- The CA certificate(s) in the client bundle must be able to verify the identity certificate in the Rallypoint bundle.
- The CA certificate(s) in the Rallypoint bundle must be able to verify the identity certificate in the client bundle.
- The CA certificate(s) in the infrastructure bundle must be able to verify the identity certificates in both the client and Rallypoint bundles.

1.2 Creating keys and certificates

Use the following commands to create keys and certificates as needed. If you already have the necessary keys and certificated, then skip this section and proceed to the **Creating a Private Certstore** section below.

- **To create a private key:** `openssl ecparam -name secp521r1 -genkey -out iceCA.key`
- **To create a Certificate Authority (CA) certificate:** `openssl req -x509 -new -nodes -key iceCA.key -sha256 -days 3650 -out iceCA.pem`
- **To create a key:** `openssl ecparam -name secp521r1 -genkey -out iceClientCert.key`
- **To create a Certificate Signing Request (CSR):** `openssl req -new -key iceClientCert.key -out iceClientCert.csr`
- **To create a certificate from the CSR:** `openssl x509 -req -in iceClientCert.csr -CA iceCA.pem -CAkey iceCA.key -CAcreateserial -out iceClientCert.pem -days 3650 -sha256`

2 Creating a Private Certstore

1. Navigate to the `bin` folder, then execute the following:

   ```
   ./ecstool ice.certstore create
   ```

2. Add `iceDefaultClientCert` and `iceDefaultRpCert` with corresponding tags:

   ```
   ./ecstool ice.certstore --tags:-enginedefault add iceDefaultClientCert iceClientCert.pem iceClientCert.key
   ```

   ```
   ./ecstool ice.certstore --tags:-rpdefault add iceDefaultRpCert iceCA.pem iceCA.key
   ```

3. Add the CA certificate:

   ```
   ./ecstool ice.certstore --tags:-cadefault add iceDefaultCA iceCA.pem
   ```

4. The resulting `ice.certstore` file must be added to Rallypoint and ICE clients to configure them to use the private certstore.

> **Note:** You may *not* substitute the `ecstool` certificate, or key tags and names, e.g., these are required as is: `-enginedefault`, `-rpdefault`, `-cadefault`, `iceDefaultClientCert`, `iceDefaultRpCert`, and `iceDefaultCA`.

3 Configuring Rallypoint to use the Private Certstore

> **Note:** If not done, then loading a certificate via 'ICE Agent' results in the following error: `E/Rallypoint: X509_verify_cert returned 0, errorCode=20, msg=unable to get local issuer certificate - denying access.`

1. On the Rallypoint virtual machine (VM), add the `ice.certstore` file to `/etc/rallypoints`

2. In the same location, open the `rallypointd_conf.json` file to configure the Rallypoint certstore.

3. Update the following line per below to define the path and filename of the certstore:

   ```
   "certStoreFileName":"/etc/rallypointd/ice.certstore",
   ```

4. Update the following code block per below to define the names of the certificate, key, and CA:

```
"certificate":
{
        "certificate":"@certstore://iceDefaultRpCert",
        "key":"@certstore://iceDefaultRpCert"
},

"tls":
{
        "verifyPeers":true,
        "allowSelfSignedCertificates":true,
        "caCertificates":
        [
                "@certstore://iceDefaultCA"
        ]
},
```

5. Save the file.
6. Restart the Rallypoint VM.

4 Configuring ICE Desktop to use the private certstore

4.1 Windows

Add the `ice.certstore` file to the following location:

`C:\Users\<username>\AppData\Roaming\ICE Desktop`

4.1.1 PEM files (Windows)

1. The `iceClientCert.pem` and `iceClientCert.key` files can be used instead of the `ice.certstore` file, if preferred, by adding them to the following location:

   `C:\Users\<username>\AppData\Roaming\ICE Desktop`

2. Restart ICE Desktop.

4.2 macOS

1. Add the `ice.certstore` file to the following location:

   `/Users/<username>/Library/Application\Support/ICE\Desktop`

2. Restart ICE Desktop.

4.2.1 PEM files (macOS)

1. The `iceClientCert.pem` and `iceClientCert.key` files can be used instead of the `ice.certstore` file, if preferred, by adding them to the following location:

   `/Users/<username>/Library/Application\Support/ICE\Desktop`

2. Restart ICE Desktop.

> **Note:** If both the PEM files and the `ice.certstore` file exist in that same location, then the PEM files are used.

5 Configure ICE Mobile to use the private certstore

5.1 Android

1. Add the `ice.certstore` file to the following location:

   `/Android/data/com.dillonkane.ice.flutter/files/directory`

2. Restart the ICE Mobile app.

5.2 iOS

1. Add the `ice.certstore` file to the following location:

   `/ICE Mobile`

2. Restart the ICE Mobile app.