Oracle Utilities Live Energy Connect Certificate Deployment Procedure for Using Secure ICCP

F48994-07

Last Updated November 03, 2023

ORACLE

Oracle Utilities Live Energy Connect Certificate Deployment Procedure for Using Secure ICCP Guide

F48994-07

Contents

Getting Started

This guide provides instructions on how to deploy the certificates required for using Secure ICCP with Oracle Utilities Live Energy Connect. For more information about Secure ICCP and Secure ICCP best practices, see the Department of Energy report for Secure ICCP Integration Considerations and Recommendations.

See Configuring Live Energy Connect for Secure ICCP for more information about configuring Live Energy Connect for Secure ICCP.

Requirements

The following requirements apply to this deployment procedure.

- Access to a Live Energy Connect installation.
- X.509 certificates are required for using Secure ICCP. You should coordinate with your organization's IT security resources to obtain certificates.
- Obtain a private certificate for the local Live Energy Connect server in PEM format. This must be a private certificate with the RSA key embedded and the RSA password removed.
- Live Energy Connect installed. Refer to the Oracle Utilities Live Energy Connect Installation Guide for instructions on downloading and installing the software.

> **Note**: When installing releases older than 7.1.0.0.0, make sure the Secure ICCP feature is selected in the installer, which will install the Stunnel.

Required Certificates

For a given Oracle Utilities Live Energy Connect server configuration that uses Secure ICCP, the following certificates are required.

SSL/TSL Certificates	ACSE Certificates
■ For each remote Secure ICCP peer, a public SSL/TSL X.509 certificate	■ For each local VCC configured to use Secure ICCP, a private and

SSL/TSL Certificates	ACSE Certificates
and a copy of the CA certificate or chain that was used to sign this public certificate are required.	public ACSE X.509 certificate are required. ■ For each remote Secure ICCP peer VCC, a public ACSE X.509 certificate and a copy of the CA certificate or chain used to sign this public certificate are required.

Note: You can generate your own self-signed X.509 certificates for testing using a tool like openSSL.

Configuring Live Energy Connect for Secure ICCP

To use Secure ICCP with Live Energy Connect you will need to:

- Prepare and deploy the required certificates for the Secure ICCP association(s).
- Enable Secure ICCP in your Live Energy Connect configuration.
- Configure the Stunnel Windows services.

Prepare and Deploy the Required Certificates for the Secure ICCP Association(s)

Secure ICCP is encrypted or authenticated at two levels, the transport layer (SSL/TLS) and the application layer. Therefore, each side of a Secure ICCP association needs to make use of two sets of certificates.

For detailed instructions on how to deploy the certificates used in a Live Energy Connect configuration with Secure ICCP, see Deploying Certificates Used for Secure ICCP.

Enable Secure ICCP in the Live Energy Connect Configuration

If you are creating a new Live Energy Connect server configuration that uses Secure ICCP, or if you are modifying an existing configuration to use Secure ICCP, you will

need to adjust some parameters in the Live Energy Connect Configuration Manager.

The following steps outline how to specify Secure ICCP within the Live Energy Connect Configuration Manager:

1. Open the **Server** tab in the **Properties** panel, change the **Global flags** field from 1 to 3, and click **Apply**.
2. With the appropriate VMD selected, open the **VMD** tab from the **Properties** panel.
3. In the **Flags** field, change the **SECURITY_FLAG** option to **Set**, and click **Apply**.

> **Note**: If a VCC's flags are generated by a setup batch file, then specify that the **SECURITY_FLAG** is set in the setup batch file instead.

4. Repeat steps 2 and 3 for each local VCC using Secure ICCP in your configuration.
5. Open the **LDIB Editor** tab in **Central** panel of the Configuration Manager and click **Refresh**.
6. Enable the **Secure ICCP** option for each local VCC using Secure ICCP in your configuration and click **Apply**.

Configure Stunnel Windows Services

Live Energy Connect creates two Windows services when it is installed, LecClientTunnel and LecServerTunnel. By default, these services are configured to start manually, but in production environments, you will want the service to start automatically.

If your Live Energy Connect configuration accepts inbound Secure ICCP associations, then you must configure the Windows service called **LecServerTunnel** to start automatically by using the Windows Services app. Similarly, if your configuration makes outbound Secure ICCP associations, then you must configure the Windows service, **LecClientTunnel** to start automatically. When the Live Energy Connect server starts, it creates Stunnel configuration files for LecClientTunnel and LedServerTunnel based on your configuration.

After starting a Live Energy Connect configuration with Secure ICCP for the first time, you must start or restart the appropriate Stunnel service to use the new configuration.

> **Note**: If you make any changes to your Live Energy Connect Secure ICCP configuration, you must restart the Stunnel service.

Deploying Certificates Used for Secure ICCP

The following sections outline steps to deploy certificates required to use Secure ICCP with Oracle Utilities Live Energy Connect. You must follow these steps in order.

Deploy the Local Oracle Utilities Live Energy Connect Server's SSL/TSL Certificates

Copy this certificate to the **`\Private\`** folder of the Stunnel installation location and save it as **`Private.pem`**. Typically, the full file path for this directory is: **`C:\ProgramFiles\LiveEnergyConnect\stunnel\config\Private\`**.

> **Note**: The first time you use deploy certificates for Secure ICCP you need to create the **`\Private\`** sub-directory.

Deploy the Remote ICCP Peers' Public SSL/TLS Certificate (s) and Associated CA Certificates

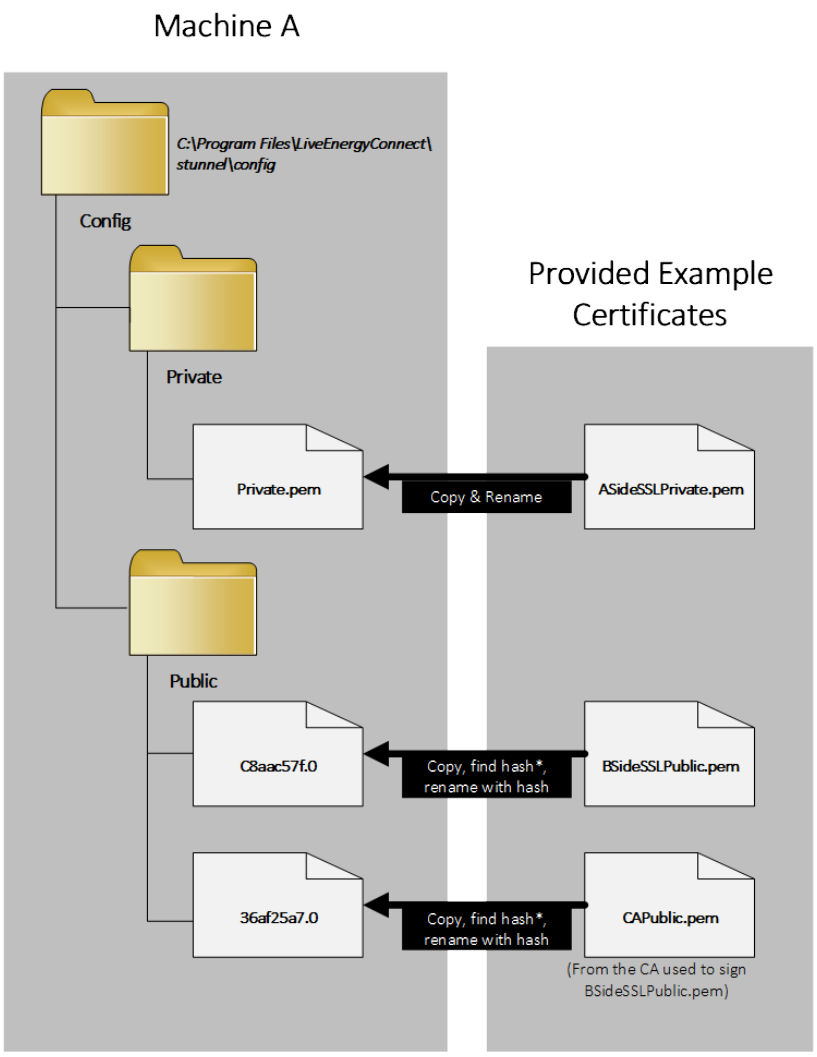
1. Obtain a copy(s) of the public certificate(s) for the remote ICCP peer or peers in PEM format.
2. Use OpenSSL or a similar tool to get the secure hash for each remote server's public certificate. For example, if the remote server's public certificate is called **`BSideSSLPublic.pem`**, use the command: `openssl x509 -inform PEM -in BSideSSLPublic.pem -noout -hash`
3. Using the generated hash value as part of the destination file name, copy each ICCP peer certificate to the **`\Public\`** folder of the Stunnel installation location.
4. Save the certificate in this directory as **`<the returned hash value>.0`**. For example, if the returned hash value from the command above was **`36af25a7`**,

save the copy of the remote server's public certificate as `C:\Program Files\LiveEnergyConnect\stunnel\config\Public\36af25a7.0`.

5. Repeat steps 1-4 for the public CA certificate that is used to sign each remote SSL certificate.

> **Note**: If the same CA is used to sign multiple SSL certificates, then you only need to do this once for that CA certificate.

The following diagram outlines the SSL/TLS certificate deployment procedures:



Deploy the Local VCC(s) ACSE Certificates

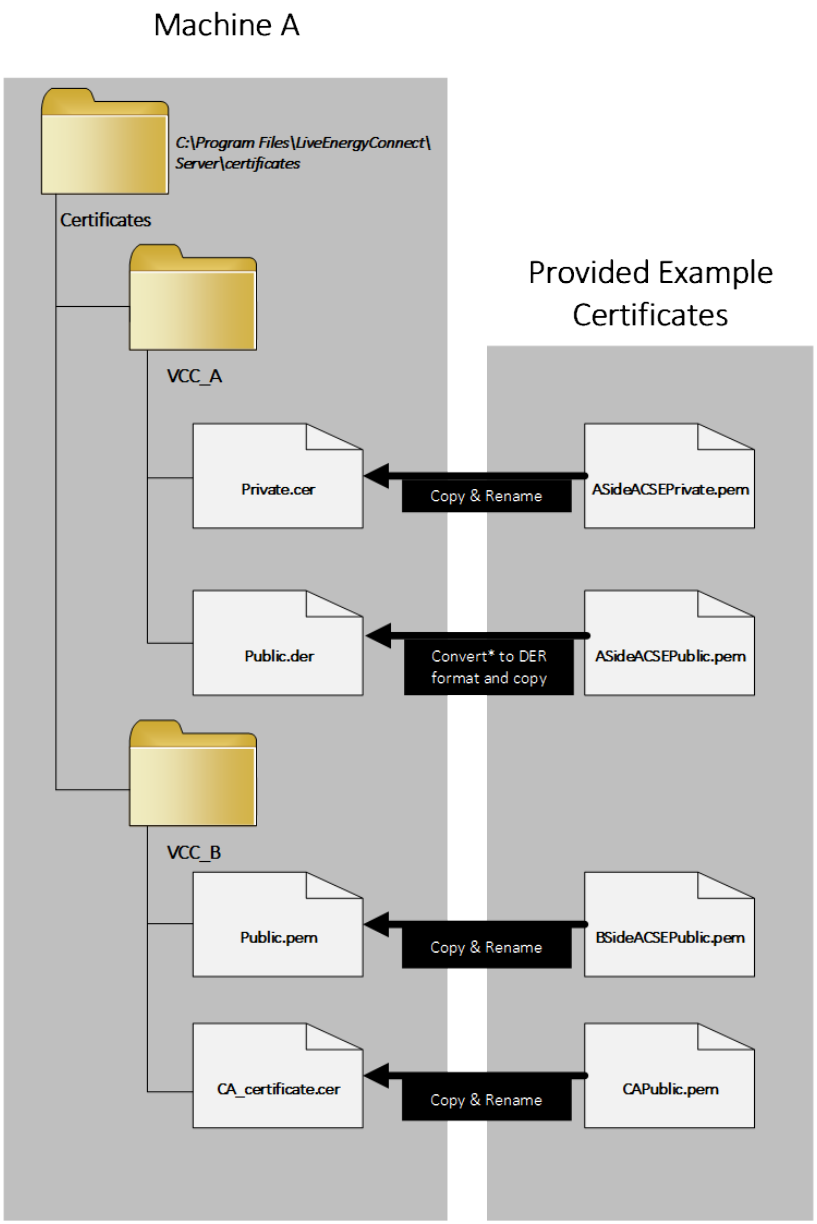
1. Obtain the private ACSE certificate for the local VCC(s) in PEM format. The certificate must be a private certificate with the RSA key embedded, and with RSA password removed.
2. In the installation directory, under the **`Server`** directory, create a **`certificates`** directory. Typically, this folder's path will be *`C:\Program Files\LiveEnergyConnect\Server\certificates`*.
3. For each local VCC, create a folder under *`C:\Program Files\LiveEnergyConnect\Server\certificates`* named for the local VCC. The name of this folder must exactly match the name of the local VCC . For example, if your local VCC was named **VCC_A**, then this folder's path would be: `C:\Program Files\LiveEnergyConnect\Server\certificates\`**`VCC_A`**.
4. Copy the ACSE certificate to the local VCC folder you created in step 3 as **`Private.cer`**.
5. Use OpenSSL or similar procedure to create a public copy of the ACSE certificate in DER format, and copy to the local VCC folder you created in step 3 as **`Public.der`**. For example: `openssl x509 -outform der -in ASideACSEPublic.pem -out Public.der`

Deploy the Remote VCC(s) Public ACSE Certificate(s) and Associated CA Certificate(s)

1. Obtain a copy of the public ACSE certificate(s) for each remote peer VCC, and a copy of the CA certificate(s) used to sign them in PEM format.
2. For each remote VCC, create a folder under the `C:\Program Files\LiveEnergyConnect\Server\certificates` directory named for that remote VCC. The name of this folder must exactly match the name of the remote VCC. For example, if the remote VCC was named **VCC_B** in the server, the folder's path would be: `C:\Program Files\LiveEnergyConnect\Server\certificates\`**`VCC_B`**.
3. Copy the public ACSE certificates for the remote VCC to the folder you created in step 2. In this step, the file name is not important, but the file must have a **`.pem`** or **`.cer`** file extension.

4. Copy the CA certificate used to sign the remotes VCC's public certificate to the folder you created in step 2 as **`CA_certificate.cer`**.

The following diagram summarizes the ACSE certificate deployment procedures:



Refer to Configuring Live Energy Connect for Secure ICCP for more information about using Secure ICCP with Live Energy Connect.

Note: If you have any trouble with the procedures outlined above, contact My Oracle Support.