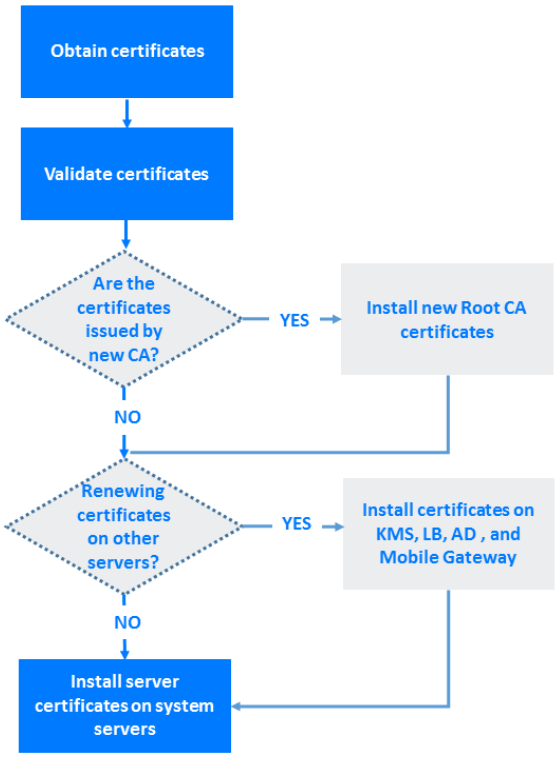
# TLS Certificate Renewal Quick Reference

## TLS certificate renewal workflow

The process used to renew TLS certificates is similar to deploying TLS certificates during the initial HTTPS configuration. Prior to installing the new certificates, determine the maintenance period(s) required for restarting services after the certificates are loaded. It is important to allow enough time to load all certificates prior to their expiration date.




## Certificate requirements

**TLS Server Certificate Requirements**

- P12 file (PKCS12 format), containing server certificate and all CA certificates in the chain
- Pubic key must be an RSA 1024, 2048 or 4096 bit
- Signature hash algorithm must be SHA1 or SHA2*
- Enhanced key usage must contain Server Authentication
- CRL distribution point must be accessible from all system servers and desktops.

**CA Certificate Requirements**

- PEM or CER file (base-64 encoding)
- Pubic key must be an RSA 1024, 2048 or 4096 bit
- Signature hash algorithm must be SHA1 or SHA2*
- CRL distribution point must be accessible from all system servers and desktops.

## Obtain certificates

Acquire new certificates generated according to system requirements.

1. Obtain a new TLS server certificate for each server that requires a renewed server certificate.
2. Get a new Root CA certificate if the Root CA of any of the renewed certificates was not used before in the system.

## Validate certificates

Every new certificate must be validated using the Certificate Validation Tool.

1. Obtain the Certificate Validation Tool: from the VerintConnect home page, go to **Tools & Resources**and select **WFO Tools**.
2. Download the relevant tool from the list, extract the zipped file, and run **Certificate Validation Tool.exe**.
3. Select the relevant Certificate Type and browse to the location of the certificate you are validating.
4. Enter the P12 file Export Password (for server certificates only).
5. Click **Validate Certificate**.
6. The details of the certificate are displayed and are validated. The validation results are as follows:
   - **Green**: indicates the parameter value is valid
   - **Orange**: indicates a warning or a validation issue
   - **Red**: indicates the parameter value is not valid
7. Verify that all parameters are valid.
   - When a **Completed with errors** or **Completed with warnings** result is achieved, review the tool tips of the failed validations, resolve the error, and rerun the tool.
   - When a **Successful Validation** result is achieved, the certificate is valid and is ready to be deployed.

## Install new Root CA certificate (optional)

If the Root CA of any of the renewed certificates is a Root CA which has not used before in the system, install the new root CA certificate on all system servers and workstations.

1. To install the new Root CA certificate on **all** system servers, copy the Root CA certificate to: **<install_dir>\conf\security**.
2. Open a command window as an administrator, and navigate to: **<install_dir>\conf\security**.
3. Enter the following command:

   **installRootCACert.cmd <root_ca_cert_filename>**
4. If more than one new Root CA is used to sign the new server certificates on any system server or on the load balancer, repeat the steps 1-3 for each new root CA certificate.
5. Install the new root CA certificates on all workstations, by loading them to:
   - Windows Trusted Root Certification Authorities store
   - Java Trusted Certificates authorities store (can be added from Java Control Panel)

## Install server certificates on RSA KMS, LB, AD, and MG (optional)

If the TLS server certificate on the RSA Key Management Server needs to be renewed, renew it according to the guidelines in the *RSA Key Manager Server Installation and Configuration Guide* (Renew RSA KMS TLS Certificates).

If the TLS server certificate on the Load Balancer or Active Directory needs to be renewed, replace it according to vendor instructions.

If the TLS server certificate on the Mobile Gateway Server needs to be renewed, renew it according to the guidelines in the *Security Configuration Guide* (Configure Mobile Gateway).

## Install server certificates on system servers

1. Rename the existing TLS server certificate so it can be used later for rollback. The certificate is located under **<install_dir>\conf\security\svr_cert_key.p12**.

   Use the following naming convention: **svr_cert_key.p12.<sequence_number>**, where **<sequence_number>** is incremented sequentially for renaming the existing certificate.
2. Copy the new server certificate to the server to the following location:

   **<install_dir>\conf\security\svr_cert_key.p12**
3. Run the following command:

   **installi360certs.cmd <certificate_password> [keystore_password]** (keystore_password is optional)

   As result, the application services are restarted causing server downtime until the services are up again.
4. Do one of the following:
   - If the Root CA certificate was **not changed** in **any** of the system servers, no further action is required.
   - If the Root CA of **any** of the renewed certificates is a Root CA which has **never been used before** in the system, **reboot all servers** throughout the enterprise once the new TLS server certificates have been loaded to all of the relevant servers.

## Related information

This document is one of many documents which can be used to secure your system.

The following documents provide additional information:

- Technology, Security, and Network Integration Desktop Reference Guide
- Security Configuration Guide
- RSA Key Manager Server Installation and Configuration Guide
- Desktop Application Desktop Reference Guide