**1. Identify the Certificate Details**

* **Open Certificate Manager (Local Computer):**
  + Press Win + R, type certlm.msc (Local Machine Certificates), and press Enter.
  + Navigate to **Certificates (Local Computer) > Personal > Certificates**.
  + Locate the service account certificate. Check its **Thumbprint**, **Issuer**, and **Expiration Date** to confirm it’s the correct one.

**2. Revoke the Certificate via the Certification Authority (CA)**

* **Access the CA Console** (requires CA admin rights):
  + On the Windows Server hosting the CA, open the **Certification Authority** snap-in (certsrv.msc).
  + Navigate to **Issued Certificates**.
  + Locate the certificate (use the **Serial Number** or **Thumbprint** from Step 1).
  + Right-click the certificate > **All Tasks > Revoke Certificate**.
  + Select a **Reason Code** (e.g., "Key Compromise") and confirm.

**3. Publish the Updated Certificate Revocation List (CRL)**

* **Update the CRL**:
  + In the CA console, right-click **Revoked Certificates** > **All Tasks > Publish**.
  + Choose **New CRL** to update the revocation list.
* **Verify CRL Distribution**:
  + Ensure the CRL is accessible via the **CRL Distribution Points** (CDP) configured in the CA (e.g., HTTP, LDAP).

**4. Remove the Certificate from the Local Machine**

* **Delete the Certificate**:
  + Return to certlm.msc (Local Machine Certificates).
  + Right-click the revoked certificate > **Delete**.
* **Optional**: Export the certificate (as a backup) before deletion if needed for audits.

**5. Update Services Using the Certificate**

* **Reconfigure Services**:
  + Replace the revoked certificate with a new one in the service configuration (e.g., IIS, SQL Server).
  + Restart the service to apply changes.
* **Verify Functionality**:
  + Test the service to ensure it operates with the new certificate.

**6. Verify Revocation Status**

* **Check Revocation via Command Line**:
  + Open Command Prompt as Administrator.
  + Run:

bash

Copy

certutil -verifystore My

* + Look for the certificate’s revocation status.
* **Check via Browser**:
  + Double-click the certificate file (if saved) and check the **Certification Path** for a revocation warning.

**7. Force CRL Check on Client Machines**

* **Update CRL Cache**:
  + On clients validating the certificate, run:

bash

Copy

certutil -urlcache \* delete

* + This clears the local CRL cache, forcing a fresh check against the CA’s CRL.

**Important Notes**

* **Permissions**: You need administrative access to the CA and the local machine.
* **External CAs**: If the certificate was issued by an external CA (e.g., DigiCert), contact their support to revoke it.
* **CRL Validity**: Ensure the CRL’s validity period is appropriate to avoid stale revocation data.

By following these steps, you ensure the certificate is revoked globally (via the CA), removed locally, and services are updated to prevent authentication failures.