

Product Notice #0208

Certificate Renewal Procedure for SIP Phone Support (SPS)

Notice Subject:

This Product Notice describes the procedures for renewing SPS certificates.

Notice Date:

April 3, 2014

Notice Effective Date:

Immediate

Affected Products:

SIP Phone Support (SPS)

Notice Details:

By default, SPS certificates are issued for a period of two years. When the certificate validity period ends, SPS does not handle any calls until a new valid certificate is issued. The procedures below describe how to verify the validity state of the SPS certificate and how to renew SPS certificates.

Verifying the Validity of a Certificate

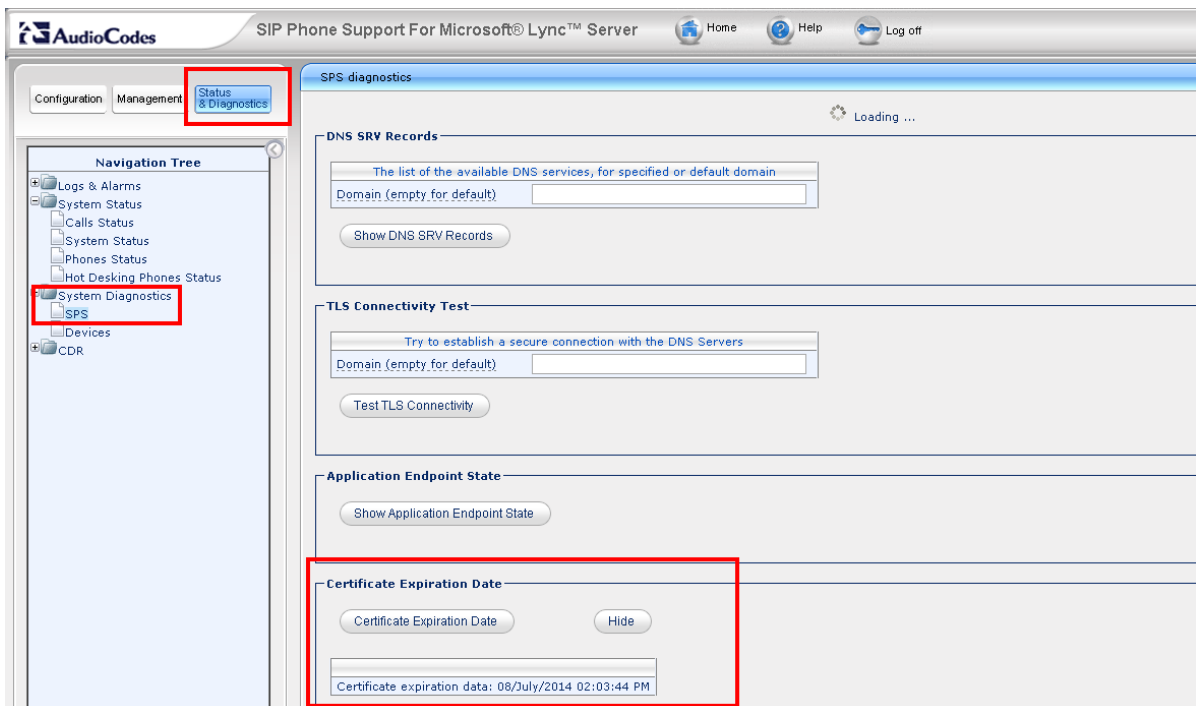
Expired certificates are easily identified because no SPS calls are possible, and the SPS log contains many TLS connection failures.



Note: If the SPS Core service is running after the certificate validity period has ended, it continues to run but **no** calls are possible. If the SPS Core service has been restarted at this point, it will fail.

You can verify the certificate expiration date by navigating to the SPS Diagnosis screen (**SPS Web Admin > Status & Diagnostics > System Diagnostic > SPS**) and clicking the **Certificate Expiration Date** button under the 'Certificate Expiration Group'.

- If the certificate is still valid, the Certificate Expiration Date group displays the certificate's expiration date (see figure below).
- If the certificate has expired, a failed message appears.



The screenshot shows the SPS Web Admin interface for SIP Phone Support For Microsoft Lync Server. The navigation tree on the left is expanded to 'System Diagnostics > SPS'. The main content area shows the 'SPS diagnostics' page with several sections: 'DNS SRV Records', 'TLS Connectivity Test', and 'Application Endpoint State'. The 'Certificate Expiration Date' section is highlighted with a red box and contains a 'Certificate Expiration Date' button and a 'Hide' button. Below these buttons, the text 'Certificate expiration data: 08/July/2014 02:03:44 PM' is displayed.

To confirm that the certificate has expired, open the Windows PowerShell console (**Start > All Programs > Accessories > Window PowerShell**) and run the following:

```
Import-Module lync
Get-CsCertificate
```

If the commands fail, the certificate has expired.



Note: When renewing certificates, make sure to run the procedure as a user with Lync Administrator permissions.

Renewing Expired Certificates

The procedure below describes how to renew a certificate whose validity date has ended (expired).

To renew an expired certificate:

1. Run SPS activation again (**Start > All Programs > AudioCodes > SPS > SPS Core > Activation > Activate SPS**).
2. Restart the SPS core service.

Renewing Unexpired Certificates

The procedure below describes how to renew a certificate whose validity date has not yet ended (unexpired).

Unexpired certificates can be renewed in the following two ways:

- Install the latest SPS core version (spsLync-core-3.0.24.35632-setup) or later. This version has a new menu option called **Renew SPS certificate** under **Start > AudioCodes > SPS > SPS core > Activation**. This re-activates SPS and forces a new certificate, even if the existing certificate has not expired.
- If you cannot install a new SPS core version, do the following:
 1. Copy the appropriate Lync version files from ftp://sps-read:note3d@ftp.audiocodes.com/SPS_Version/Certificate-Renew to a new directory on the SPS server.
 2. Open the Windows PowerShell console (**Start > All Programs > Accessories > Window PowerShell**).
 3. Navigate to the new directory and run the following:

```
.\SpsRenewCert.ps1
```

This runs the same renewal procedure as in the first option above.



Note: Both renewal procedures do NOT require an SPS core restart. You can verify the renewal results by navigating to the SPS Diagnosis page in the SPS Web Admin, as shown above.