Acmetek

A Trusted Advisor of Security Solutions and Services

#TrustedPKIAdvisor

CSR Generation Instructions on Lync 2013

WHITE PAPER

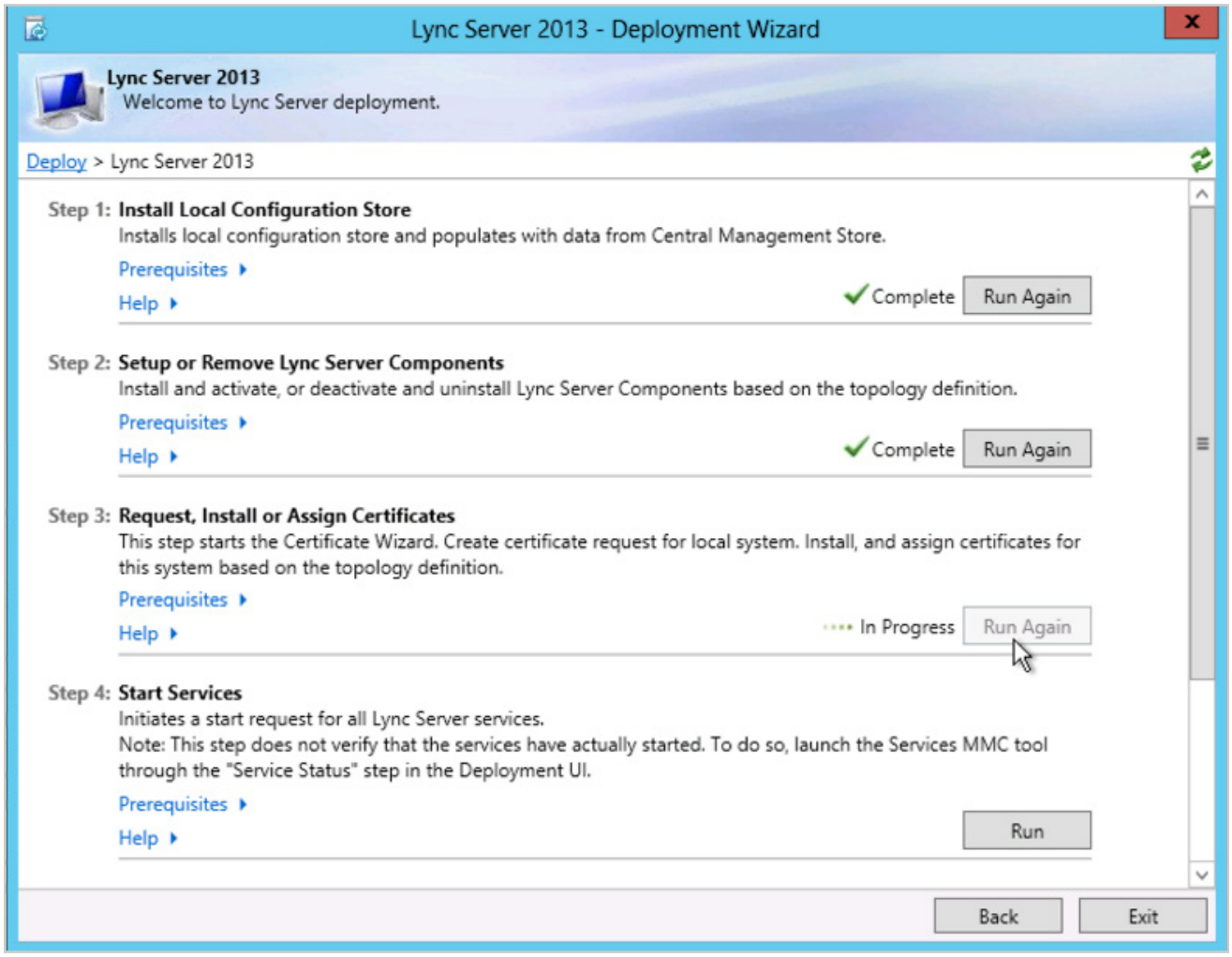
https://www.acmetek.com

Microsoft Lync 2013 combines instant messaging, VoIP calling, live meetings, and videoconferencing, but it's more than the sum of these parts. Although Lync integrates with almost any PBX, it puts the PC at the center of communications so effectively that it could send your current phone system packing.

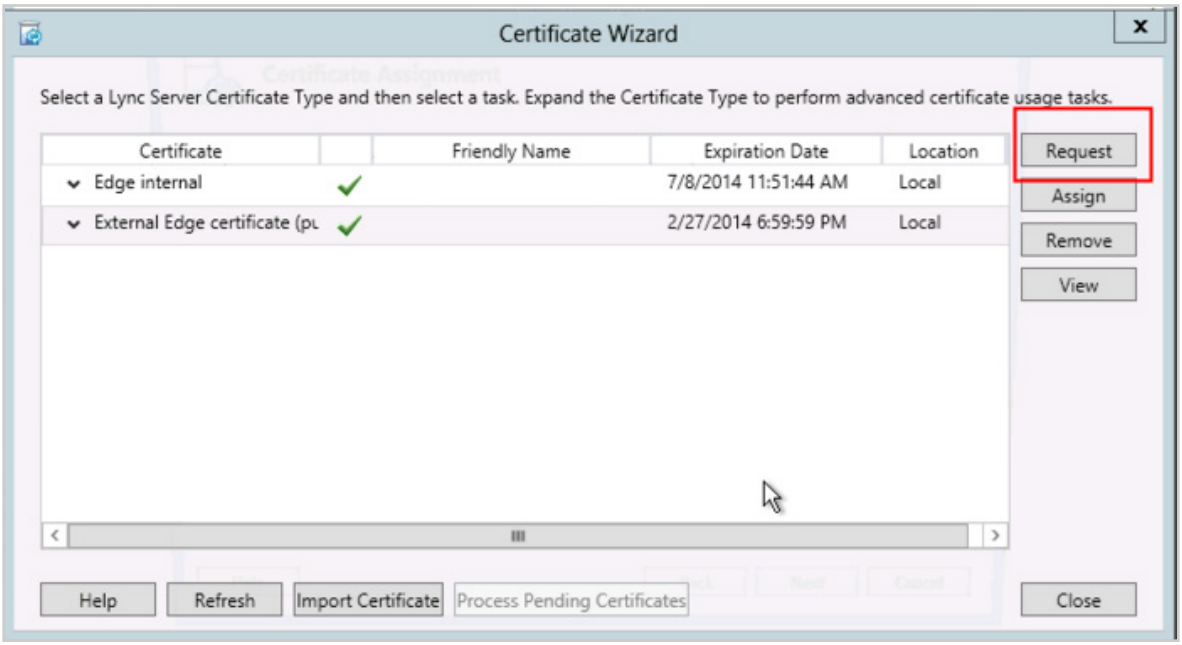
Lync provides clear VoIP calling and crisp videoconferencing without requiring special network accommodations. It integrates with Microsoft Exchange, Microsoft SharePoint, and Microsoft Office, bringing user presence information to Outlook and SharePoint team sites and allowing instant messages and phone calls to be initiated with a click.

Steps for CSR generation:

1. From the Windows start menu click on the **Lync Deployment Wizard** icon.
2. Click on **Install** or **update** Lync Server System.
3. Under the Request, Install, or Assign Certificates section click **Run**.



4. Choose External Edge Certificate and click **Request**.



5. Click **Next**.
6. Choose Prepare the request now, but send it later.
7. Choose the name and destination for the CSR text file. (i.e. C:\Desktop\ExampleCSR.txt).
8. On the Specify Alternate Certificate Template click **Next**.
9. Enter a friendly name for the certificate. Ensure that Bit Length is 2048. Mark the private key as exportable if you have multiple machines in your edge cluster. Click **Next**.
10. Enter your Organization's Name and Unit that the certificate is for. Click **Next**.
11. Enter your Country, State, and City. Click **Next**.
12. The Subject Name and Subject Alternative Names (SAN) will auto-populate. Click **Next**.
13. Check the box on SIP domains. Click **Next**.
14. On the Configure Additional Subject Alternate Names page specify other SANs needed. Click **Next**.
15. On the Summary Page ensure the information is correct, and click **Next**.
16. On the Executing Commands page ensure the Task Status is completed. Click **Next**.
17. On the Certificate Request File page you can click view the certificate to then copy the text and enter it into the DigiCert order form. Click **Finish** to close the Certificate Request File window.

    Congratulations, you have successfully created a CSR on Lync Server 2013!
18. After you receive your SSL Certificate from DigiCert, you can install it.

If you are unable to use these instructions for your server, we recommend that you contact either the vendor of your software or the organization that supports it.

ABOUT ACMETEK

“Acmetek is a Global Distributor and a Trusted Advisor of PKI /IoT & SSL Security Products and Managed Services Company.”

Acmetek Global Solutions, Inc. is a privately held Digital Security Services Company serving USA & APAC clients in website security solutions since 2010. The firm specializes in providing insight and expertise to enterprises, SMBs, governments, and provides a full range of Security Products, SSL, PKI, IoT, Malware Identity Scanning’s, Vulnerability Assessments, and Two-Factor Authentication.

Acmetek is a managed service partner of multi-brand technology solutions like CDW. We manage the Certificate Authority Practices of leading Website Security Brand, DigiCert (formerly known as Symantec). Over a decade of experience in the security industry empowered us to grow as an Authorized Distributor/ Platinum Partner for DigiCert and a leading provider of security solutions and services.

SSL Cert Free Trial | MPKI | Request a Call Back | SSL Support Desk

Our Web Security Solutions

SSL CERTIFICATES

Domain Validation

Activates HTTPS with a padlock. This SSL can issue in minutes.

Organization Validation

Activates HTTPS with a padlock. It validates an organization by providing a trust seal.

Extended Validation

Activates HTTPS with a padlock. It validates the organization by providing the company name before the domain name directly on the browser.

Code Signing Certificates

Protects users from downloading compromised software, prevents tampering, and provides the trusted assurance of authentication.

MPKI SOLUTIONS

Email Certificates

Using an Email certificate for user authentication encrypts transmission and signs the message,delivering comprehensive benefits for the sender and receiver.

Document Signing Certificates

Document signing certificates allow individuals, teams, and organizations to add an electronic, digital signature to a document in a variety of file formats to prove ownership.

Device Certificate

Verify identity, encrypt communications, and secures all home networks for internet connected devices before and after manufacturing.

MDM (Mobile Device Management)

Get a comprehensive look at mobile devices, master mobile email, and application rollout while protecting all data anddevices.

WIFI Certificates

Increases trust in public hotspots and protect user data.