Lotus Domino – Guide to Installing Root Certificates, Generating CSR and Installing SSL Certificate

Trustis Limited

Building 273 New Greenham Park Greenham Common Thatcham RG19 6HN

E: info@trustis.com W: www.trustis.com

Registered in England No: 03613613

Table of Contents

1 Introduction

This document specifies instructions for Installing the Root and Intermediate certificates, generating your CSR, and Installing your certificate.

2 Install Root and Intermediate (AND Server) Certificates

The Root CA certificate and the Issuing CA certificate must be downloaded:

- PEM format Root CA certificate – found at http://www.trustis.com/pki/healthcare/ops/fpsroot-pem.crt
- PEM format Healthcare TT Issuing Authority certificate – found at http://www.trustis.com/pki/healthcare/ops/healthcarett-pem.crt

Installing the certificates on Lotus Domino Server requires both CA certificates and the SSL Server certificate to be merged into the Key Ring file.

NOW Proceed with Sections 3 and 4 of this guide before continuing.

Once you have your SSL Server Certificate, continue with the process below.

This process must be completed for all three certificates.

1. In Notes, from the administration panel, click System Databases and choose Open Domino Server Certificate Administration (CERTSRV.NSF) on the local machine.
2. Click Install Certificate into Key Ring.
3. Enter the file name for the Key Ring that will store this certificate. The Key Ring file was created when you created the server Certificate Signing Request.
4. Detach the file from the email to your hard drive and unzip it.
5. Select File in the "Certificate Source" field. Enter the file name in the file name field.
6. Click "Merge Certificate into Key Ring".
7. Enter the password for the server key ring file and click OK to approve the merge.

For additional information, refer to your server documentation.

3 Certificate Signing Request (CSR) Generation

3.1 For version 4.6x:

1. From the administration panel, click System Databases and choose Open Domino Server Certificate Administration (certsrv.nsf) on the local machine. Click *Create Key Ring*.
2. Enter a name for the key ring file in the "Key Ring File Name" field.
3. Enter a password for the server key ring file in the "Key Ring Password" field.
   Note: Password is an alphanumeric set of characters that protects the key ring from unauthorised use. The password is case sensitive. You should specify at least 12 alphanumeric characters for the password.
4. Select a key size. This is the size Domino uses when creating the public and private key pairs. Select 2048 bit ONLY
   Note: If you are using the international version of Domino, only the 512 bit key size will work for you unless you have Release R5.04. Upgrade to a later version which supports 2048 bit. Sizes LESS than 2048 bit will not be accepted.
5. Specify the components of your server's distinguished name.
6. Click Create Key Ring. Click OK.
7. Click Create Certificate Request.

Note: You must select all the text in the second dialog box, including Begin Certificate and End Certificate when the CSR is requested.

3.2 For R5.0x:

1. Launch the Domino Administration client.
2. Select File-Open Server and select the Domino server you wish to administer, Click the file tab, double click on Server Certificate Administration database (certsrv.nsf)
3. From the administration panel, click System Databases and choose Open Domino Server Certificate Administration (certsrv.nsf) on the local machine.
4. Click Create Key Ring.
5. Enter a name for the key ring file in the "Key Ring File Name" field.
6. Enter a password for the server key ring file in the "Key Ring Password" field.
   Note: Password is an alphanumeric set of characters that protects the key ring from unauthorised use. The password is case sensitive. You should specify at least 12 alphanumeric characters for the password.
7. Select a key size. This is the size Domino uses when creating the public and private key pairs. Select 2048 bit ONLY.
   Note: If you are using the international version of Domino, only the 512 bit key size will work for you unless you have Release R5.04. Upgrade to a later version which supports 2048 bit.
8. Specify the components of your server's distinguished name.
9. Click Create Key Ring. Click OK.
10. Click Create Certificate Request.

Note: You must select all the text in the second dialog box, including Begin Certificate and End Certificate when the CSR is requested.

4 Installing your SSL Server Certificate

You will receive an email from the Registration Authority when your certificate request has been approved that contains a link to a location where your certificate may be obtained. Clicking on this link will bring up a browser window that contains the details of your issued certificate and includes a section that looks something like the following:

-----BEGIN CERTIFICATE-----
MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCAmowggHXA
hAF
UbM77e50M63v1Z2A/5O5MA0GCSqGSIb3DQEOBAUAMF8xCzAJBgNVBAYTAIVTMS
Aw
(.....)
E+cFEpf0WForA+eRP6XraWw8rTN8102zGrcJgg4P6XVS4l39+l5aCEGGbauLP5W6
K99c42ku3QrlX2+KeDi+xBG2cEIsdSiXeQS/16S36ITclu4AADEAAAAAAAAA
-----END CERTIFICATE-----

Copy everything you see **between and including** the lines that look like
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----

and paste it into an appropriately named text file e.g. myserver.pem

Now go back to Section 2 and complete the installation including the CA Root and Intermediate certificates.