

IBM Domino Go 4.6.2.6+

Installing your Web Server Certificate

Your certificate will be sent to you by email. The email message includes the web server certificate that you purchased in the body of the email message. Copy the certificate from the body of the email and paste it into a text editor (such as notepad) to create text files.

Installing the Root Certificates

1. Create 3 text files. The first file should be the Thawte Certificate. Name this file "thawte.txt". The second file should be the GeoTrust True BusinessID certificate. Name this file "True BusinessID.txt". The last file should be Your Web Server Certificate. Name this file "server.txt".
Note: Be sure to include the -----BEGIN CERTIFICATE----- line and the -----END CERTIFICATE----- line.
2. Start the MKKF utility by typing **mkkf**
3. Select "**O**" to Open an existing key ring file. Type the name of the file (usually keyfile.kyr). You will be prompted for the password.
*Note: If you start the "mkkf" utility from the directory that contains your certificates you will not need to include the path.
4. Select "**R**" to receive a certificate into the Key Ring File.
5. You will be prompted for the file name. Enter **thawteroot.txt**
6. Enter **Thawte Server CA** for the label.
7. Press <Enter> to continue.
8. Select "**W**" to work with Keys and Certificates.
9. Select "**L**" to List/Select the key to work with.
10. Find the "**Thawte Server CA**" and select "S" to Select this menu.
11. Select "**T**" to mark this as a Trusted root.
12. Select "**Y**" - Yes - to confirm this request.
13. Press <Enter> to return to the previous menu.
14. Select "**X**" to exit the menu.
15. Repeat steps 4 through 14 using the GeoTrust True BusinessID certificate.
In Step 5, substitute " True BusinessID.txt."
In Step 6, substitute "GeoTrust eBusiness CA."
In Step 10, substitute " GeoTrust eBusiness CA."

Installing your Web Server Certificate

1. From the main menu of the mkkf utility, select "**R**" to Receive a certificate into a Key Ring File
2. Enter the server certificate file name (eg. "server.txt").
3. Select "**W**" to Work with keys and certificates.
4. Select "**L**" to List/Select the key to work with. Select "N" until you find the servername.key file.
5. Select "**S**" to Select this certificate.

6. Select "**F**" to mark this key as the selected deFault key.
7. Select "**X**" to exit this menu.
8. Select "**C**" to Create a "stash file" for the key ring.
Note: This is an important step, which is often overlooked!
9. Select "**X**" to exit the menu.
10. Select "**Y**" - Yes - to save all changes to the key file and confirm the update.
11. Enabling SSL on your Domino Go Web Server
12. Access the web server via your browser. Select "**Configuration and Administration Forms.**"
13. Scroll down to security. Select Security Configuration.
14. Ensure that "Allow SSL connections using port 443" is selected.
15. Ensure that the correct Key Ring file is listed.
16. Apply the changes.

Restarting your Web Server

1. You will need to stop and start your web server with the following commands: **stopsrc -s httpd startsrc -s httpd**

Test your certificate by using a browser to connect to your server. Use the https protocol directive (e.g. <https://your server/>) to indicate you wish to use secure HTTP. The padlock icon on your browser will be displayed in the locked position if your certificates are installed correctly and the server is properly configured for SSL.