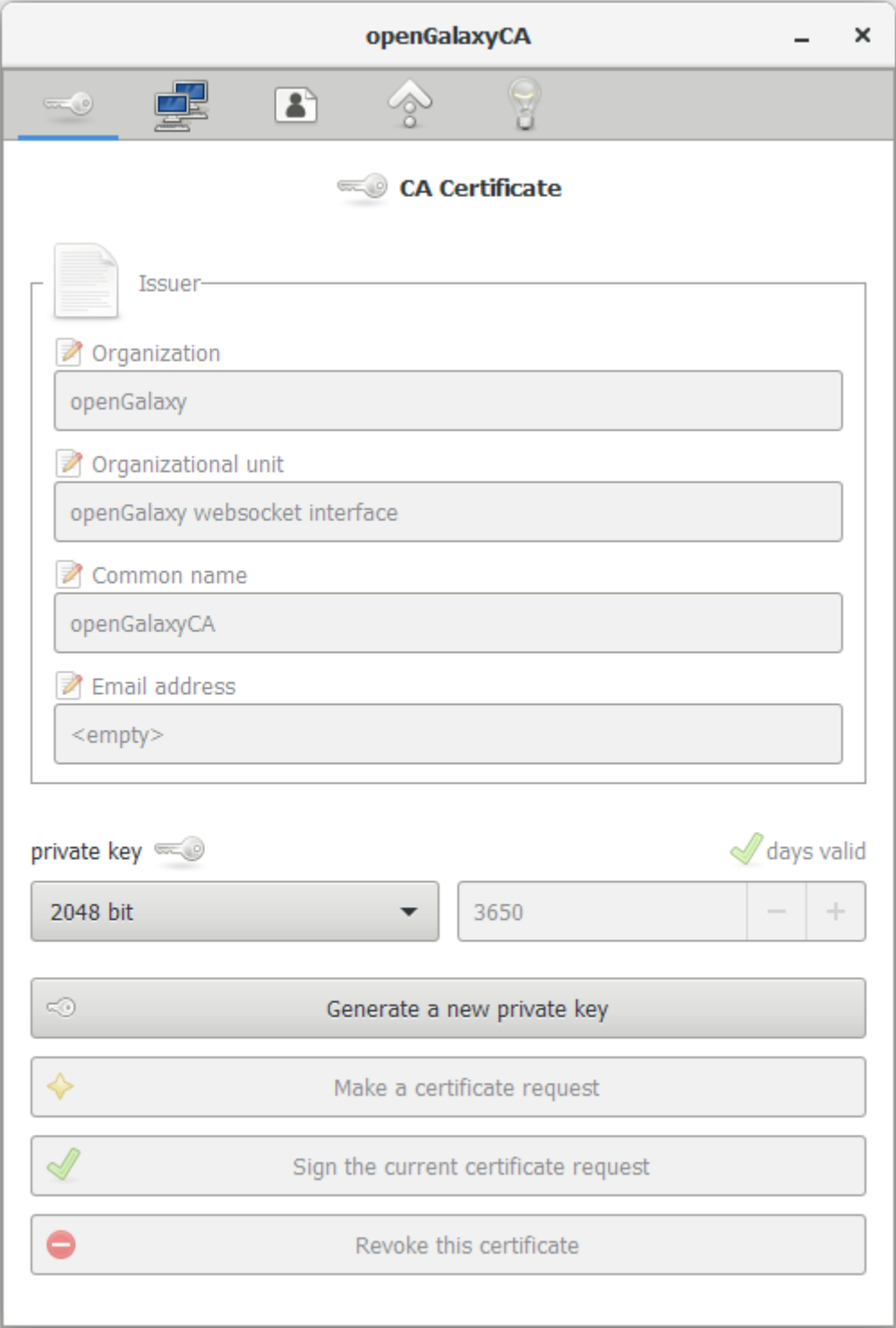


openGalaxy Certificate Manager version 0.14

`opengalaxy-ca` is the application used to create, modify or invalidate all of the *SSL certificates* needed by the openGalaxy server, client and web-interface.

When you run `opengalaxy-ca` you are initially presented with the page to create a *CA certificate*. This certificate is used to 'sign' all other certificates created.



The screenshot shows the 'openGalaxyCA' web application window. The title bar says 'openGalaxyCA' with standard window controls. Below the title bar is a navigation bar with five icons: a key, a computer monitor, a person, an upward arrow, and a lightbulb. The main content area is titled 'CA Certificate' with a key icon. It contains a form for creating a CA certificate with the following fields:

- Issuer**: A document icon and a text input field.
- Organization**: A pencil icon and a text input field containing 'openGalaxy'.
- Organizational unit**: A pencil icon and a text input field containing 'openGalaxy websocket interface'.
- Common name**: A pencil icon and a text input field containing 'openGalaxyCA'.
- Email address**: A pencil icon and a text input field containing '<empty>'.

Below the form, there is a section for the private key:

- private key**: A key icon.
- days valid**: A green checkmark icon.
- 2048 bit**: A dropdown menu.
- 3650**: A text input field.
- Generate a new private key**: A button with a key icon.
- Make a certificate request**: A button with a star icon.
- Sign the current certificate request**: A button with a green checkmark icon.
- Revoke this certificate**: A button with a red minus icon.

Users executing `opengalaxy-ca` need to be a member of group `staff` (GNU/Linux only).

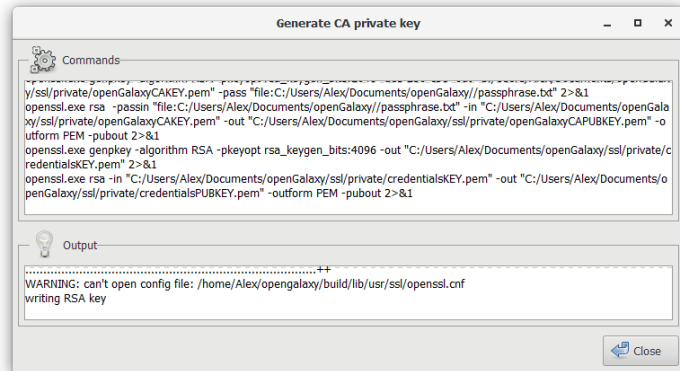
Creating a CA certificate.

To create the CA certificate select a private key size from the drop-down box and press the Generate a new private key button.

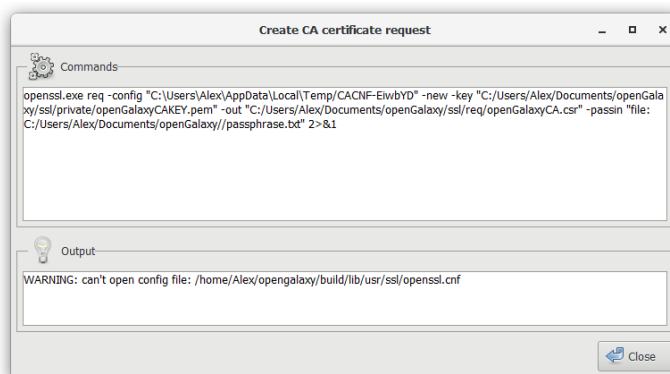
The program will now show you a dialog with the commands (and their output) it is executing.

If there is an error during the process there will be an additional message-box.

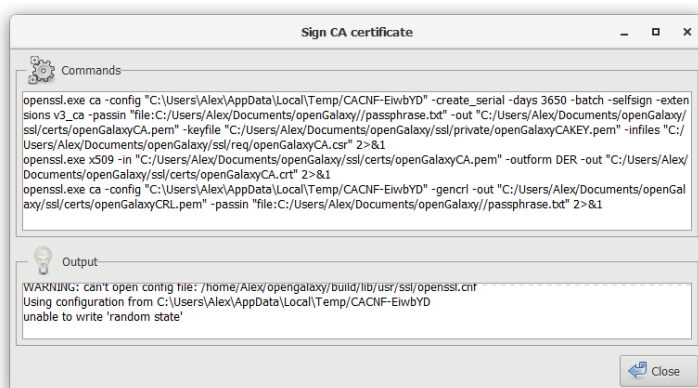
Close the dialog after reviewing the output.



The next step is to create a new certificate request using the Make a certificate request button.



The last step in creating the CA certificate is to sign it (ourselves) by selecting the number of days the certificate should be made valid and then using the Sign the current certificate request button to sign it.



With the CA certificate now available we may proceed to create the SSL certificates used by the openGalaxy server and client applications (and by a web-browser used to access the web-interface).

Creating a server certificate.

The `opengalaxy` server application requires several SSL certificates in order to operate in 'https' mode.

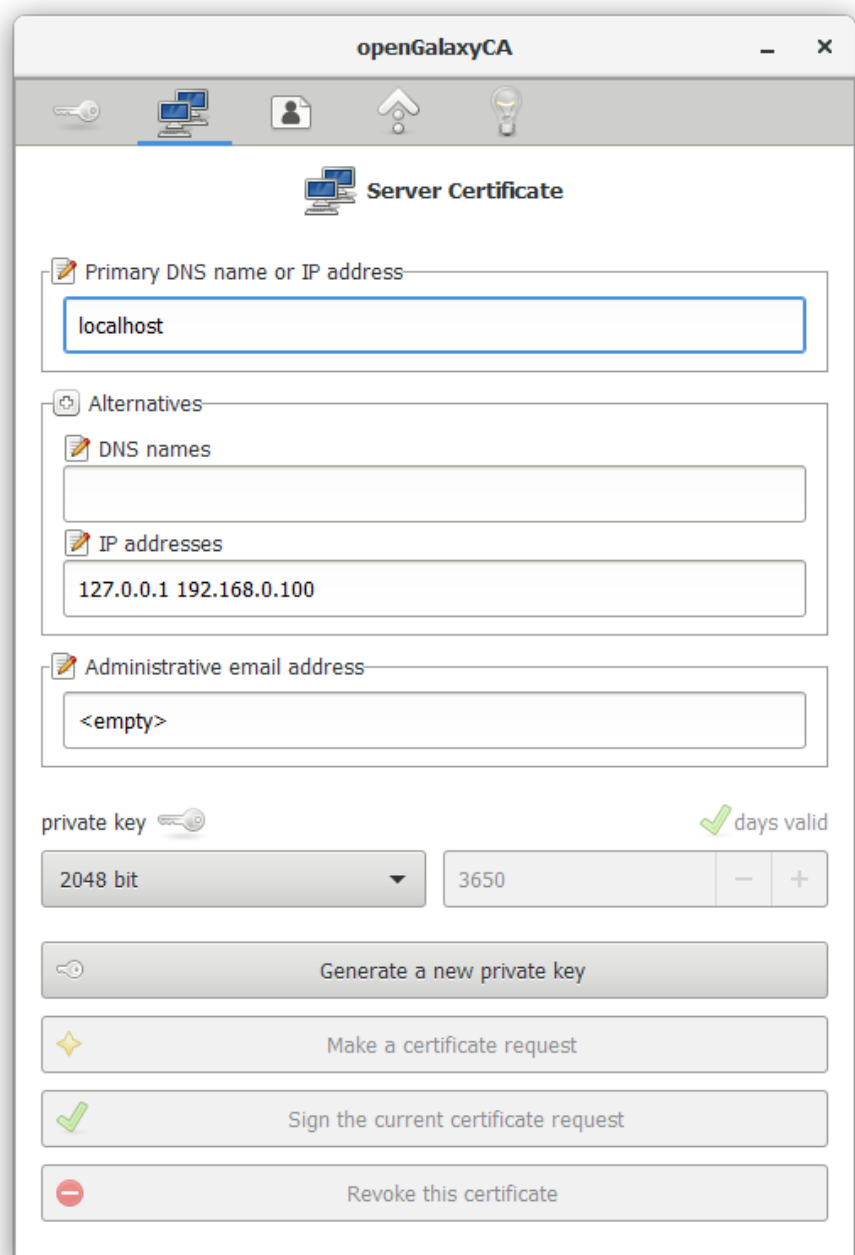
The server needs to be able to present its identity to anyone who makes a connection to it, this is done by means of an SSL server certificate. Additionally the server application needs to determine if that connection is authorized. This is done by requiring the client to prove its identity by means of an SSL client certificate. Finally, all of these certificates need to be 'signed' by our CA certificate in order to prove that they were created by us.

To be able to reject stolen or lost certificates the openGalaxy Certificate Manager maintains a special certificate called the 'Certificate Revocation List'. Instead of needing each individual client certificate the server application uses this CRL certificate to determine if the connection is authorized.

*

The default values presented on this page can only be used if you run both server and client / web-browser on the same computer.

If you want to allow other computers on a network (or the Internet) to be able to access the web-interface you will need to at least change the values for the first three items.



The screenshot shows the 'openGalaxyCA' application window with the 'Server Certificate' tab selected. The interface includes a toolbar with icons for key, server, user, home, and lightbulb. The main form contains the following fields and controls:

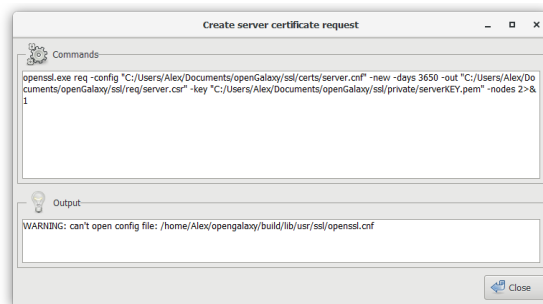
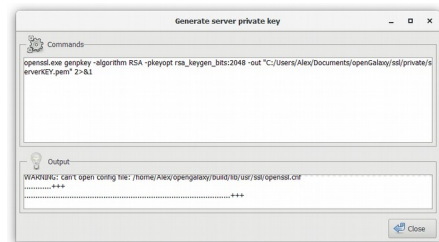
- Primary DNS name or IP address:** A text box containing 'localhost'.
- Alternatives:** A section with two sub-fields:
 - DNS names:** An empty text box.
 - IP addresses:** A text box containing '127.0.0.1 192.168.0.100'.
- Administrative email address:** A text box containing '<empty>'.
- private key:** A dropdown menu showing '2048 bit'.
- days valid:** A text box showing '3650' with minus and plus buttons.
- Buttons:** Four buttons at the bottom: 'Generate a new private key' (with a key icon), 'Make a certificate request' (with a star icon), 'Sign the current certificate request' (with a green checkmark icon), and 'Revoke this certificate' (with a red minus icon).

The Primary DNS name or IP address is the base URL (without https:// in front of it) or IP address of the computer that runs the server application.

The alternative DNS Names and IP addresses may be used to specify any additional url's and IP addresses from which the server may be reachable.

Multiple addresses in these fields must be separated by a space.

When all fields have the correct values continue to create the SSL server certificate in the same way as in the section explaining how to create the CA certificate.



Creating a client certificate.

To be able to connect to an openGalaxy server running in SSL mode at least one SSL client certificate needs to be created.

The screenshot shows the 'openGalaxyCA' application window. The title bar includes the application name and standard window controls. Below the title bar is a navigation bar with icons for a key, a computer, a person, a server, and a lightbulb. The main content area is titled 'Client Certificates' and features a search bar labeled 'List of client certificates'. Below this is a 'Client Information' section with several input fields: 'Name' (containing 'Slim'), 'Surname' (containing 'Shady'), 'Username' (containing 'slim'), 'Password' (masked with dots), and 'Email address' (containing 'none'). A 'New Client' button is located to the right of the email field. Below the input fields, there is a 'private key' section with a dropdown menu set to '2048 bit' and a 'days valid' section with a value of '365' and increment/decrement buttons. At the bottom, there are five action buttons: 'Generate a new private key', 'Make a certificate request', 'Sign the current certificate request', 'Revoke this certificate', and 'Delete this client certificate'.

openGalaxyCA

Client Certificates

Search List of client certificates

Client Information

Name: Slim

Surname: Shady

Username: slim

Password: [masked]

Email address: none

New Client

private key 2048 bit

days valid 365

Generate a new private key

Make a certificate request

Sign the current certificate request

Revoke this certificate

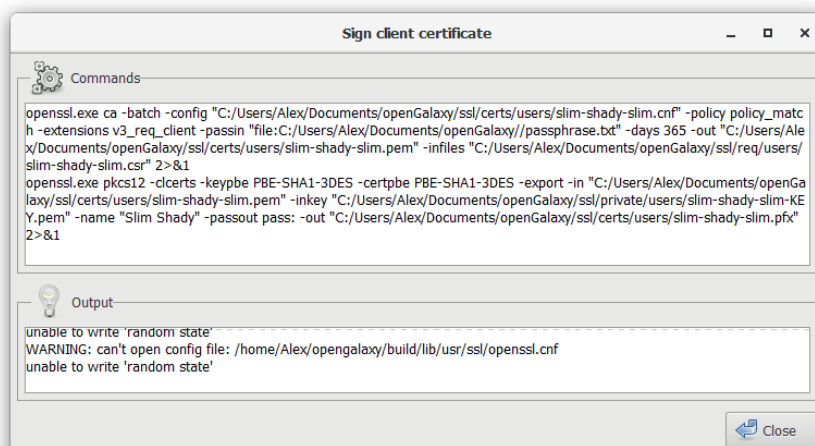
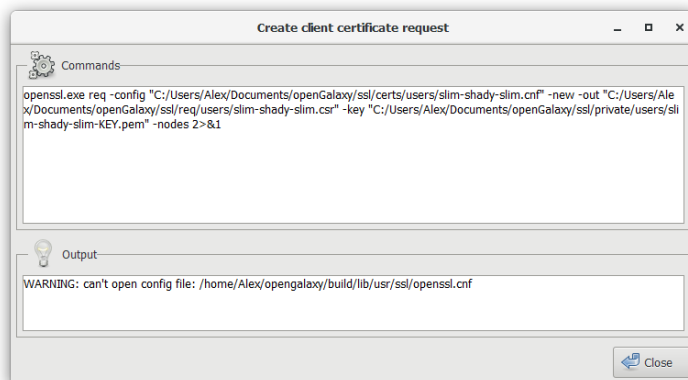
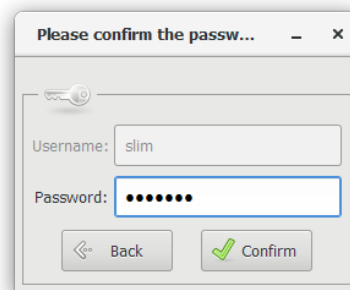
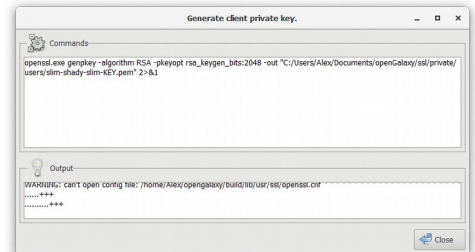
Delete this client certificate

A client certificate should be used by one client only, the server application enforces this by allowing only one session that uses any given client certificate. If multiple connections are made using the same client certificate only the last connection is honored.

To create an SSL client certificate click on the New Client button and place the correct values in the Client Information fields that become available.

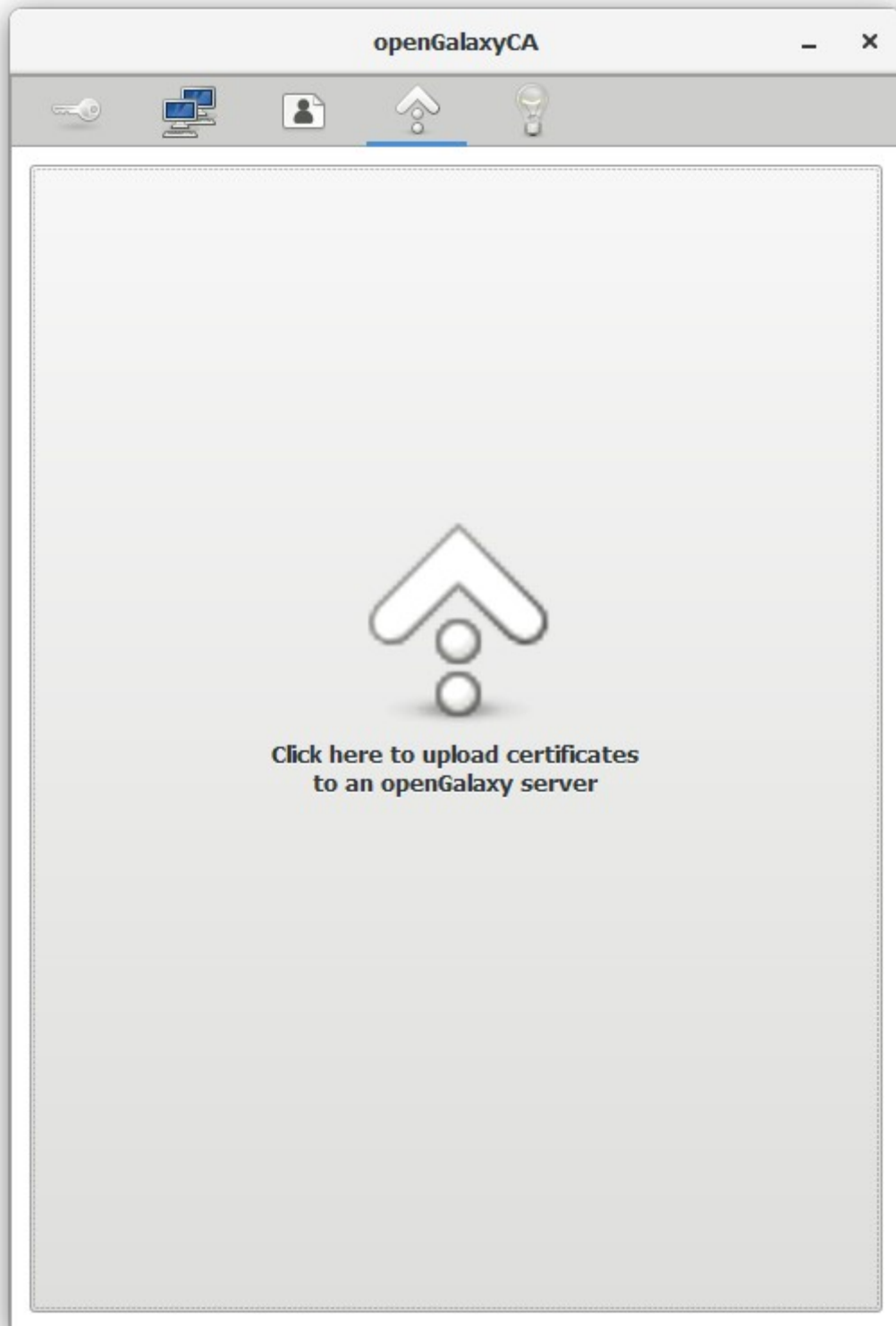
All fields must contain a valid input value in order to create the client certificate.

The procedure to create the certificate is the same as for the CA and server certificates. With the difference that you will be asked to confirm the password when creating a certificate request.



Uploading certificates to a server.

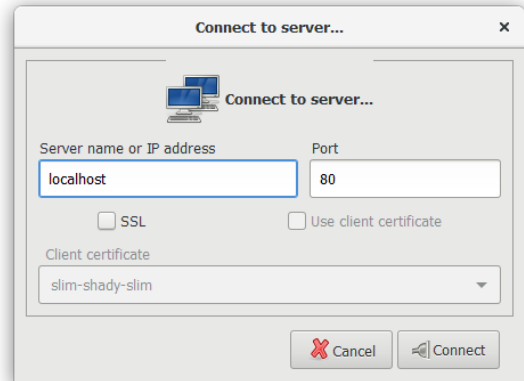
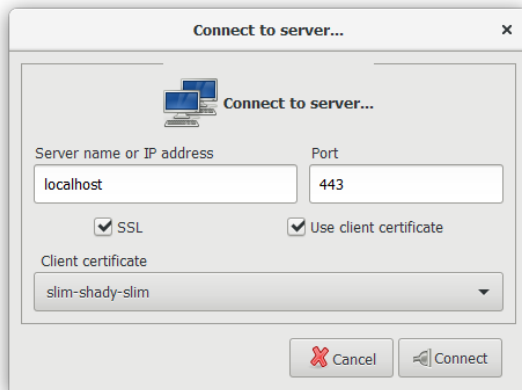
Whenever a certificate has been added, modified or removed these changes need to be pushed to the server application. To apply the changes made to the certificates click on the huge button.



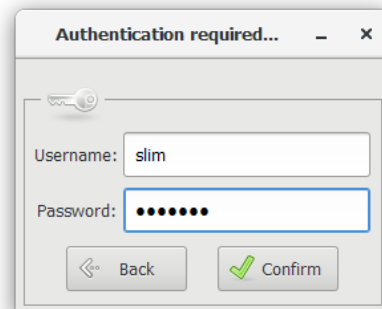
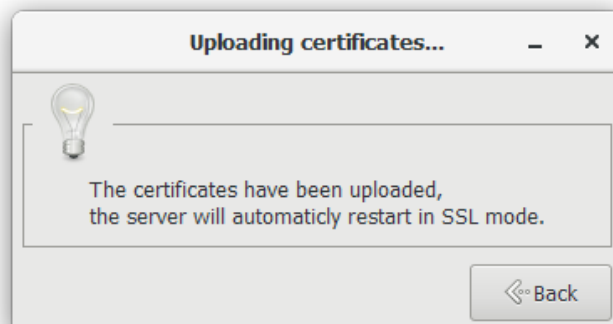
When you run the server application without installing any SSL certificates it will detect they are missing and start in HTTP mode on the network interface and port configured in the server's configuration file (/etc/galaxy/galaxy.conf). If the server was already using SSL certificates and is running in HTTPS mode the port number may differ.

Select the SSL mode, enter the IP address or host-name and the port number then click on the Connect button.

If you have modified the CA certificate you cannot upload the new certificates in HTTPS mode. You will have to (re-)start the server in HTTP mode before the new CA certificate can be uploaded!

A dialog box titled "Connect to server..." with a close button (X) in the top right. It contains a server icon and the title "Connect to server...". Below this, there are two input fields: "Server name or IP address" with the value "localhost" and "Port" with the value "80". There are two checkboxes: "SSL" (unchecked) and "Use client certificate" (unchecked). Below these is a dropdown menu for "Client certificate" with the value "slim-shady-slim". At the bottom right are two buttons: "Cancel" with a red X icon and "Connect" with a speaker icon.A dialog box titled "Connect to server..." with a close button (X) in the top right. It contains a server icon and the title "Connect to server...". Below this, there are two input fields: "Server name or IP address" with the value "localhost" and "Port" with the value "443". There are two checkboxes: "SSL" (checked) and "Use client certificate" (checked). Below these is a dropdown menu for "Client certificate" with the value "slim-shady-slim". At the bottom right are two buttons: "Cancel" with a red X icon and "Connect" with a speaker icon.

If SSL mode was selected the server will ask for the credentials belonging to the certificates used to connect.

A dialog box titled "Authentication required..." with standard window controls (minimize, maximize, close). It contains a key icon. Below this are two input fields: "Username:" with the value "slim" and "Password:" with a masked password (dots). At the bottom are two buttons: "Back" with a left arrow icon and "Confirm" with a green checkmark icon.A dialog box titled "Uploading certificates..." with standard window controls (minimize, maximize, close). It contains a lightbulb icon. Below this is a text box with the message: "The certificates have been uploaded, the server will automaticly restart in SSL mode." At the bottom right is a button: "Back" with a left arrow icon.

When the certificates were successfully processed by the server it will restart after 5 to 10 seconds.

Deleting, revoking or modifying certificates.

Client certificates:

If you want to delete or revoke a client certificate then select the certificate from the drop-down box and click on the [Delete this client certificate](#) or [Revoke this client certificate](#) button. The difference between deleting and revoking is that a revoked certificate can still be restored by signing it again and a deleted certificate is gone forever.

If you wish to modify a client certificate it must first be revoked by clicking the [Revoke this client certificate](#) button. After revoking the certificate a new private key must be generated by clicking on the [Generate a new private key](#) button before the [Client Information](#) fields are made available.

After the fields are modified a new certificate request can be made and then signed by the CA certificate by clicking on the [Make a certificate request](#) button followed by the [Sign the current certificate request](#) button.

If a client certificate is no longer valid because it expired it can be either deleted or renewed by revoking it and resigning the original certificate request.

Server certificate:

To modify the server certificate first click on the [Revoke this certificate](#) button. Then click the [Generate a new private key](#) button to make the other fields available. After modification were made create a new certificate request with the [Make a new certificate request](#) button followed by the [Sign the current certificate request](#) button.

To renew the server certificate if it has expired click on the [Revoke this certificate](#) button followed by the [Sign the current certificate request](#) button.

CA certificate:

An expired or revoked CA certificate also invalidates all client certificates and the server certificate. To renew the CA certificate click on the [Revoke this certificate](#) button followed by the [Sign the current certificate request](#) button to sign the request and to resign any existing client and server certificates.

After all changes have been made the affected client(s) must re-install their certificate and the server needs to be notified of the changes by uploading the new certificates to the server.

Installing client certificates.

The installation of the server certificate is automated, unfortunately the installation of a client certificate cannot be automated and it must be installed manually.

The recommended web-browser to use with openGalaxy is the latest version of Google Chrome (version 50.0.2661.75 at the time of this writing).

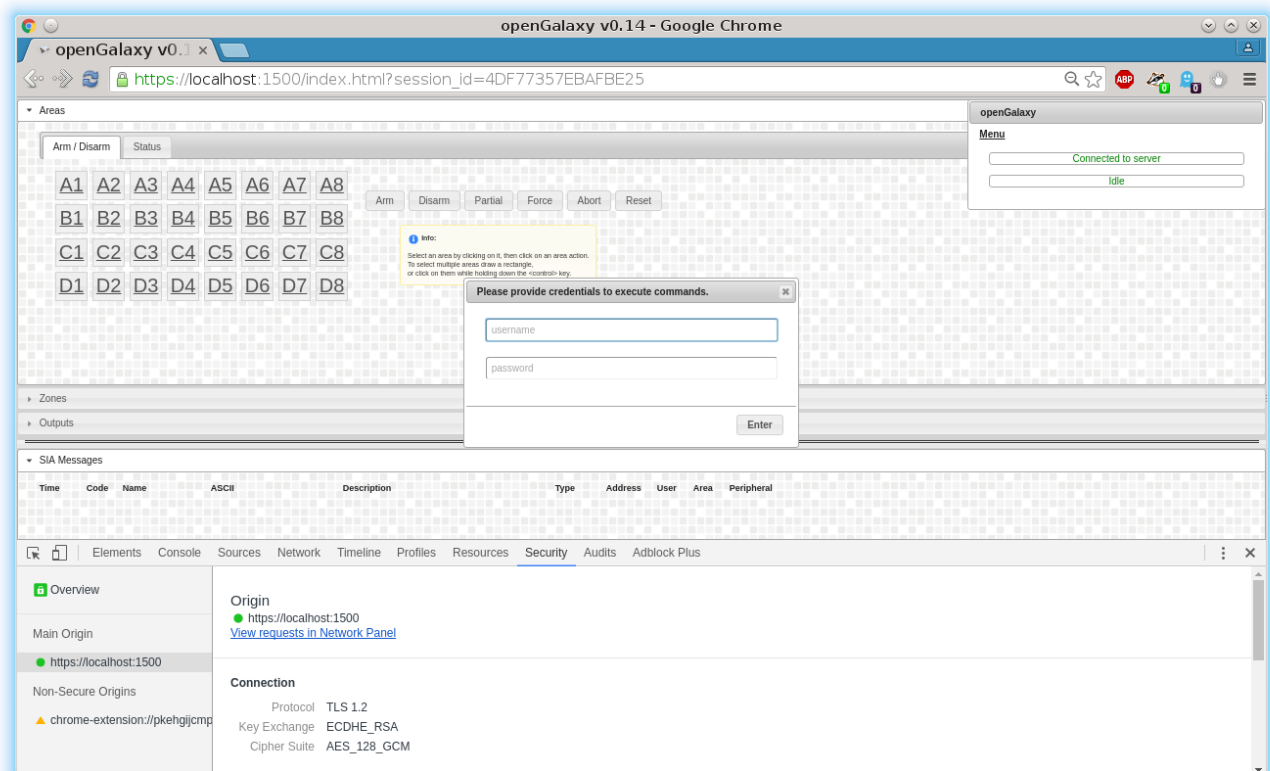
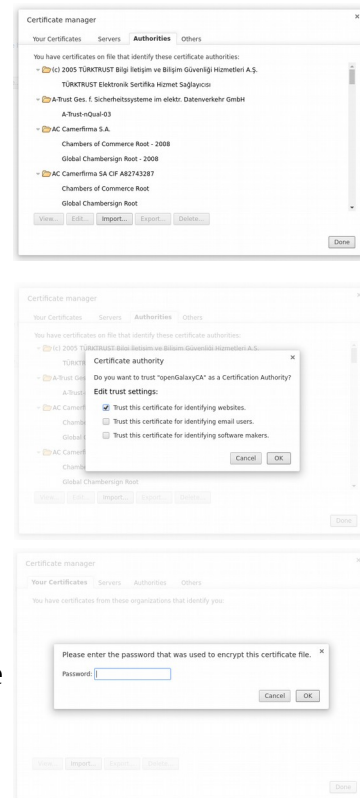
To prepare Chrome for use with openGalaxy open the settings page from the menu or go to the address `chrome://settings/` and click on 'Show advanced settings...'. Then scroll down to the HTTP/SSL section and click on Manage certificates. Go to the Authorities tab and click on Import...

In the dialog that pops up browse to `/usr/share/galaxy/ssl/certs` and select the file `openGalaxyCA.crt`

Now select the Trust this certificate for identifying websites check-box and click on OK.

After installing the CA certificate go to the Your Certificates tab and click on import. In the dialog that pops up browse to `/usr/share/galaxy/ssl/certs/users` and select the `.pfx` file for the client you wish to install. The password is left empty.

When connecting to the server Chrome now asks you what certificate you want to use.



Location and usage of the SSL certificates.

The following certificate files are needed for each application:

opengalaxy :

- openGalaxyCA.pem
- openGalaxyCAPUBKEY.pem
- openGalaxyCRL.pem
- server.pem
- serverKEY.pem
- credentialsKEY.pem

opengalaxy-client :

- openGalaxyCA.pem
- openGalaxyCRL.pem
- [client-certificate].pem
- [client-private-key].pem

Google Chrome :

- openGalaxyCA.crt
- [client-certificate-bundle].pfx

For Windows all references to the locations /usr/share/galaxy and /etc/galaxy should be interpreted as the directory chosen during installation of openGalaxy and defaults to \\MyDocuments\\openGalaxy.

The windows installer for openGalaxy also DOES NOT set any special file permissions for the certificates directory. If the MyDocuments folder is readable to all users, then so are the certificate files and more importantly; the private keys!

The certificates created with opengalaxy-ca are stored in the location /usr/share/galaxy in the subdirectory ssl which has the following structure:

/usr/share/galaxy/ssl/certs[/users]

This is the directory that opengalaxy-ca places the final certificates that are meant to be used by openGalaxy.

/usr/share/galaxy/ssl/newcerts

This directory is used internally by OpenSSL.

/usr/share/galaxy/ssl/private[/users]

The private keys for all certificates are stored here.

/usr/share/galaxy/ssl/req[/user]

Stores all certificate requests made by opengalaxy-ca

The /usr/share/galaxy/ssl directory will never be automatically deleted when re- or uninstalling openGalaxy.

/usr/share/galaxy/passphrase.txt

The text on the first line in this file is the pass phrase used to encrypt the private key of the CA certificate. To access this file you must be root or a member of group staff. Modifying this file implicitly invalidates all certificates so they will need to be recreated from scratch (by deleting the /usr/share/galaxy/ssl directory) !