# Internal Certificate Authority

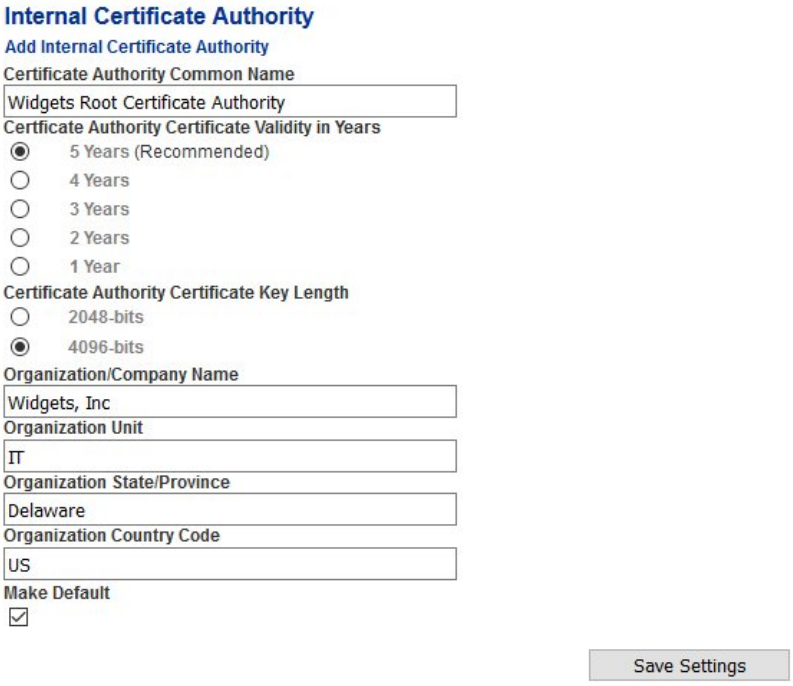
An Internal Certificate Authority can be used to create certificates for internal and external recipients for the purposes of S/MIME encryption and message signing. The certificate generated by the internal CA are not trusted, therefore you must instruct the external recipients of your messages to trust your Internal CA in their clients.

Alternatively, instead of using certificates generated by the internal CA, you can import certificates from a trusted 3rd party Certificate Authority for both internal and external recipients.

## Add Internal Certificate Authority

1. Under the **Certificate Authority Common Name** field, enter the name you wish to assign to the internal CA.
2. Under the **Certificate Authority Certificate Validity in Years** field, select the length of time you wish the Certificate Authority to remain valid. We recommend you leave this setting at the default 5 years.
3. Under the **Certificate Authority Certificate Key Length** select the key length you wish to use. We recommend you leave this setting at the default 4096-bits.
4. Under the **Organization/Company Name** enter the name of your organization.
5. Under the Organization Unit field enter the name of your organization unit.
6. Under the **Organization State/Province** field enter the name of of the organization state/province
7. Under the **Organization Country Code** field enter the two letter code for your organization country. Example, for United States simply enter **US**.
8. Click the checkbox under the **Make Default** field, if you wish to make this Certficate Authority the defalt CA. By default, the first CA that gets created becomes the default CA.
9. Click the **Save Settings** button (**Figure 1**).

**Figure 1**




10. Each Internal Certificate Authority you add shows up in the **Edit/Delete Existing Internal Certificate Authorities** section (**Figure 2**).

**Figure 2**


11. Continue adding Internal Certificate Authorities as needed.

# Set Internal Certificate Authority as Default

1. Under the **Edit/Delete Existing Internal Certificate Authorities** place a checkmark under the Default column of the Internal Certificate Authority you wish to set as default. The system will automatically set the Certificate Authority as the default (**Figure 3**).

**Figure 3**


# Delete Internal Certificate Authority

Default Internal Certificate Authorities or Internal Certificate Authorities that have been used to issue certificates to Internal or External Recipients cannot be deleted. In those cases you must either set another Internal CA as the default and/or you must first remove the Internal Recipients under **Gateway --> Internal Repients** and the External Recipients under **Encryption --> External Recipient Encryption** which will also remove any certificates assigned to those recipients. Please note, you do not have to remove all internal or external recipients, only the recipients that have certificates assigned to them by the Internal Certificate Authority you wish to delete.

> If an internal Certificate Authority cannot be deleted, the Delete column of that entry will contain a icon. Otherwise, if it can be deleted, the Delete column of that entry will contain a icon.

1. Under the **Edit/Delete Existing Internal Certificate Authorities** click the icon of the Internal Certificate Authority you wish to delete.
2. On the confirmation page, click on the **YES** button to delete the Internal CA or click the **NO** button to cancel.

**Figure 4**


3. You will be returned to the **Internal Certificate Authority** Page

---

Revision #1
Created 3 January 2021 13:30:34 by Dino Edwards
Updated 2 December 2021 12:47:24 by Dino Edwards