# Certificate Builder Operator's Manual

Software Version 1.0.0

# Table of Contents

# Introduction

This application provides a simple graphical user interface to help you build self-signed or signed X.509 digital certificates for testing purposes. This application can be used to create the following types of X.509 certificates.

1. Self-signed Certificate Authority (CA) certificates
2. Signed Intermediate Certificate Authority (ICA) certificates
3. Signed or self-signed end-entity certificates

This application allows you to build certificates using the RSA signing algorithm or the ECDSA signing algorithm. RSA certificates are created using a fixed key length of 2048 bits and SHA512 for the hash function. ECDSA certificates are created using a fixed key length of 521 bits using the P521 elliptic curve with SHA-512 for the hash algorithm.

Certificates are saved as files using a file name that you can specify in a location that you can specify. The application creates two types of files. The file with a file name extension of “cer” contains only a public key. The file with a file name extension of “pfx” contains both the public key and a private key. The PFX file is password protected. This file can be used by client and server applications that use Transport Layer Security (TLS and/or HTTPS) or have a need to digitally sign digital documents.

This application also allows you to build X.509 certificates for testing NG9-1-1 applications (see Reference 1). The PSAP Credentialing Agency (PCA, see Reference 2) is responsible for issuing certificates to be used by functional elements, services, agencies and agents within a NG9-1-1 emergency services network. Certificates issued by the PCA contain the following information in the otherName sequence of the Subject Alternate Name certificate extension (see Section 4.2.1.6 of RFC 5280 [3] and Section 7.1.2.11 of the PCA Certificate Policy [2]).

1. ID Type (identifies the entity such as: Element, Service, Agent or Agency)
2. ID of the entity
3. Roles assigned to the entity
4. Owner of the certificate assigned to the entity

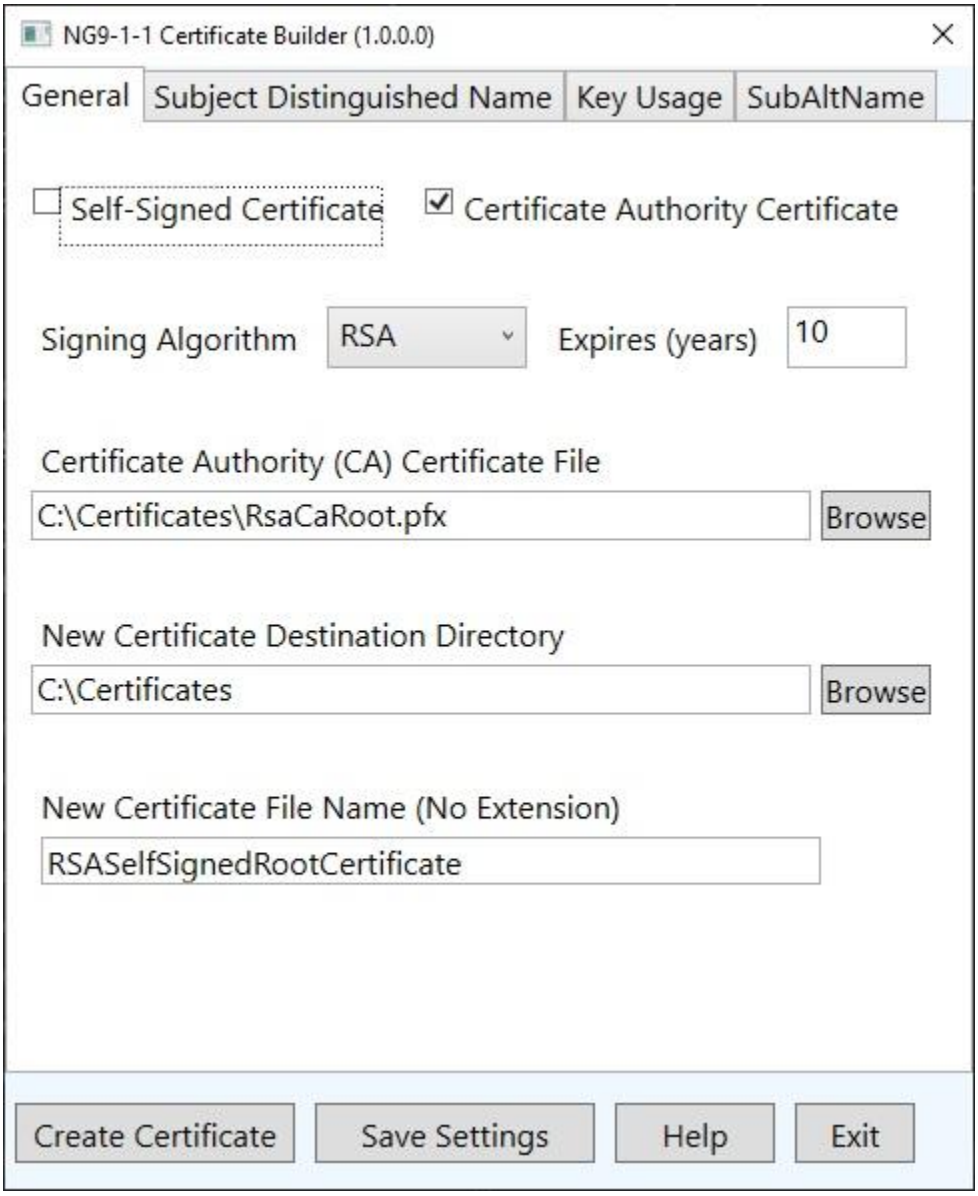
This application allows you to build certificates that include the above information in the otherName sequence of the Subject Alternate Name certificate extension. See the SubAltName Tab.

## References


1. NENA i3 Standard for Next Generation 9-1-1. National Emergency Number Association (NENA) 911 Core Services Committee, i3 Architecture Working Group, NENA-STA-010.3b, October 7, 2021.
2. Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy. NG9-1-1 Interoperability Oversight Commission (NIOC), V1.2, June 26, 2024.
3. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF, RFC 5280, May 2008.

# Settings and Controls

The following figure shows the main window for this application.




To create a new certificate, fill in the information in each of the four tabs and click on the Create Certificate button.

If creating a signed certificate, the application will display a dialog box that prompts you to enter the password for the CA Certificate (signing certificate) file. Then the application will prompt you to enter the password for the PFX file for the new certificate.

If creating a self-signed certificate, the application will display a dialog box that prompts you to enter the password for the PFX file for the new certificate.

The Save Settings button will save the current settings in a file called CertBuilderSettings.json. This file will be saved in the "C:\Users\CurrentUserName\Documents\CertBuilder" folder. When the application starts up, it will check to see if this file exists. If it does, the application will read the last-used settings from this file and load the settings into the appropriate data fields.

The Help button displays this manual using the default PDF file reader that is installed on your computer.

# General Tab Settings

## Self-Signed Certificate

If this checkbox is checked then a self-signed root certificate will be generated. If this checkbox is not checked then a signed certificate will be generated. When generating a signed certificate, the certificate to sign the new certificate with must be specified in the Certificate Authority Certificate text box.

## Certificate Authority Certificate

If this checkbox is checked then the new certificate will be a Certificate Authority (CA) or an Intermediate Certificate Authority (ICA) certificate. CA and ICA certificates may be used to sign other certificates. If this checkbox is not checked then the new certificate will be an end-entity certificate.

This setting determines the basic constraints of the new certificate. If checked, then the basic restraint will be set to "CA".

## Signing Algorithm

This combo box selects the signing algorithm to use for the new certificate. The choices are RSA or ECDSA (Elliptic Curve Digital Signature Algorithm).

The default setting is RSA.

## Expires

This setting specifies the number of years that the new certificate will be valid for. This setting only applies to self-signed certificates.

The minimum setting is 1 year. There is no upper limit for this setting.

## Certificate Authority (CA) Certificate File

This setting specifies the certificate to use to sign the new certificate. The signing certificate file must be in PFX format and it must contain a private key.

Enter the full path to the certificate file or click on the Browse button to open the File Open dialog box so you can navigate to its location.

This setting is required if creating a signed certificate. It is not used when creating a self-signed certificate.

## New Certificate Destination Directory

This setting specifies the directory in which to write the new certificate files. The destination directory must exist before you attempt to create a new certificate. Click on the adjacent Browse button to open the Select Folder dialog box to create (if necessary) and select the destination directory.

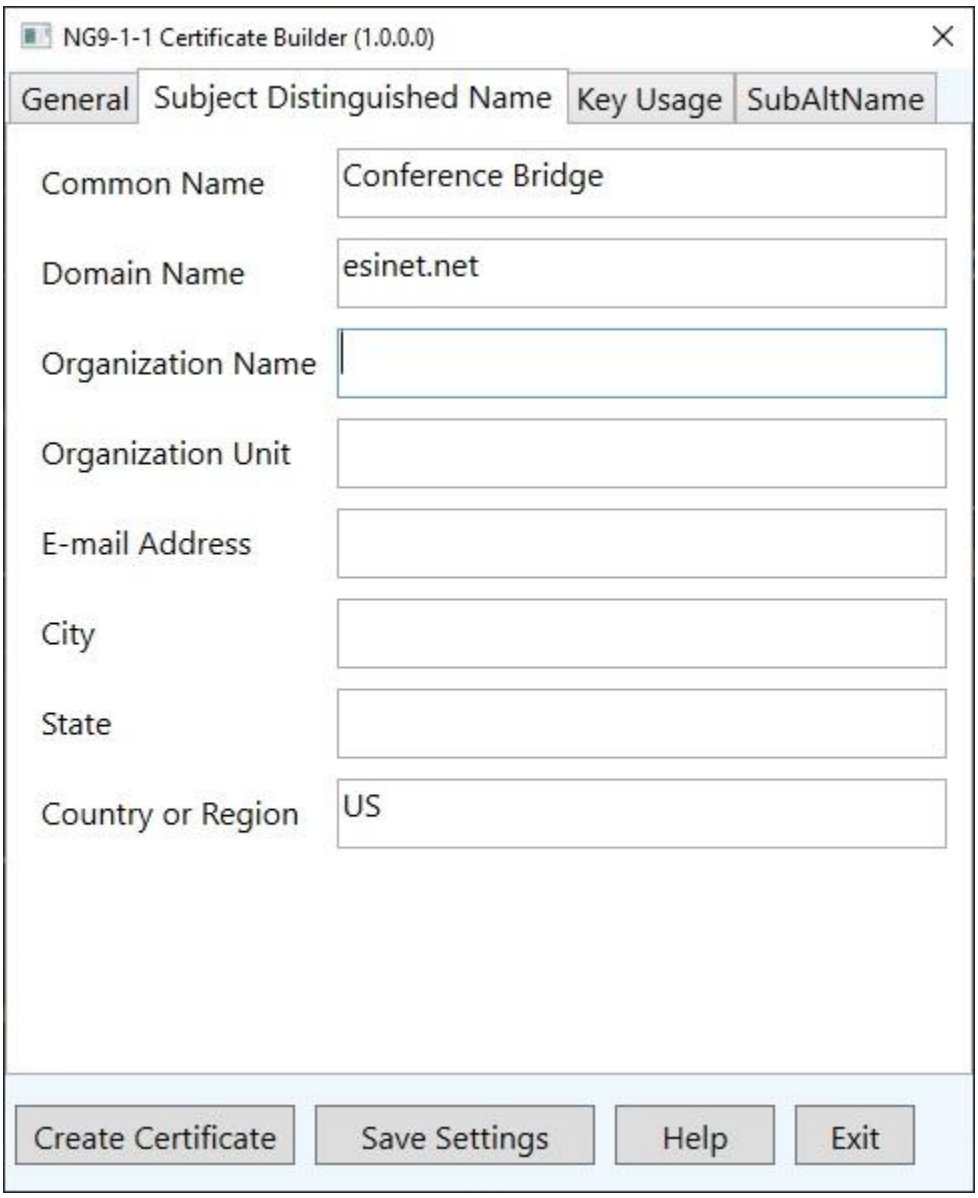
### New Certificate File Name

This text box is for entering the file name the certificate files. Enter a file name without any extension. This application will create two files, one containing the private key (*.pfx) and one without a private key (*.cer).

If the files already exist in the destination directory then they will be overwritten.

## Subject Distinguished Name Tab

The settings in this tab are used to create the distinguished name in the Subject of the new certificate. Each text box corresponds to an attribute of the subject distinguished name.



### Common Name
Specifies the common name (CN) of the certificate. The common name may be any string that can be used to identify the subject of the X.509 certificate.

This field is required.

### Domain Name
Specifies the domain name field of the subject distinguished name.

This field is optional.

### Organization Name
Identifies the organization or agency. This field is optional.

### Organization Unit
Identifies an organizational unit or department within the organization. This field is optional.

### E-Mail Address
Contains the e-mail address of the organization. This field is optional.

### City
Specifies the locality or city of the organization or agency. This corresponds to the “L” field of the distinguished name. This field is optional.

### State
Specifies the state or province of the organization or agency. This field is optional.

### Country or Region
Specifies the country or region of the organization or agency. This field is optional. If specified, this field must contain a two-letter country name.

## Key Usage Tab

The settings in this tab specify values added to the key usage and extended key usage certificate extensions.


The following key usage settings are recommended if creating a Certificate Authority (CA) root certificate, or an Intermedia Certificate Authority (ICA) certificate that will be used to sign other certificates. See Table 8 of the PCA Certificate Policy document.

1. CRL Signing
2. Digital Signature
3. Key Certificate Signing
4. Non-Repudiation

For other types of certificates the following key usage settings are recommended. See Table 9 of the PCA Certificate Policy document.

1. Digital Signature
2. Non-Repudiation
3. Key Encipherment
4. Key Agreement
5. Server Authentication
6. Client Authentication

### CRL Signing
If checked then the certificate can be used for signing Certificate Revocation Lists (CRL). This option should be checked if creating a CA or an ICA certificate. It should not be checked for other types of certificates.

### Data Encipherment
This option indicates that the certificate may be used to encipher (encrypt) data. It may be selected for any type of certificate. The certificate may be used to encrypt data even if this option is not checked.

### Decipher Only
This check box indicates that the public key of the certificate may be used only to decipher data. This option is not normally used.

### Digital Signature
This checkbox should be checked when the public key is used for verifying digital signatures. This checkbox should be checked in most cases.

### Code Signing
This check box should be checked if the certificate will be used to sign executable code modules.

### Encipher Only
This checkbox indicates that the public key of the certificate will be used only to encipher data. This option is not normally used.

### Key Agreement
This checkbox indicates that the public key of the certificate will be used for a key agreement algorithm. It should be checked for non-CA and non-ICA certificates.

### Key Certificate Signing
This checkbox must be checked if the certificate is going to be used to sign other certificates as in the case of CA and ICA certificates.

### Key Encipherment
This checkbox should be checked if the public key of the certificate is going to be used to encipher private or secret keys. It should be checked for non-CA and non-ICA certificates.

### Non-Repudiation

This checkbox should be checked if the subject public key is used to verify digital signatures other than signatures on certificates.

### Server Authentication

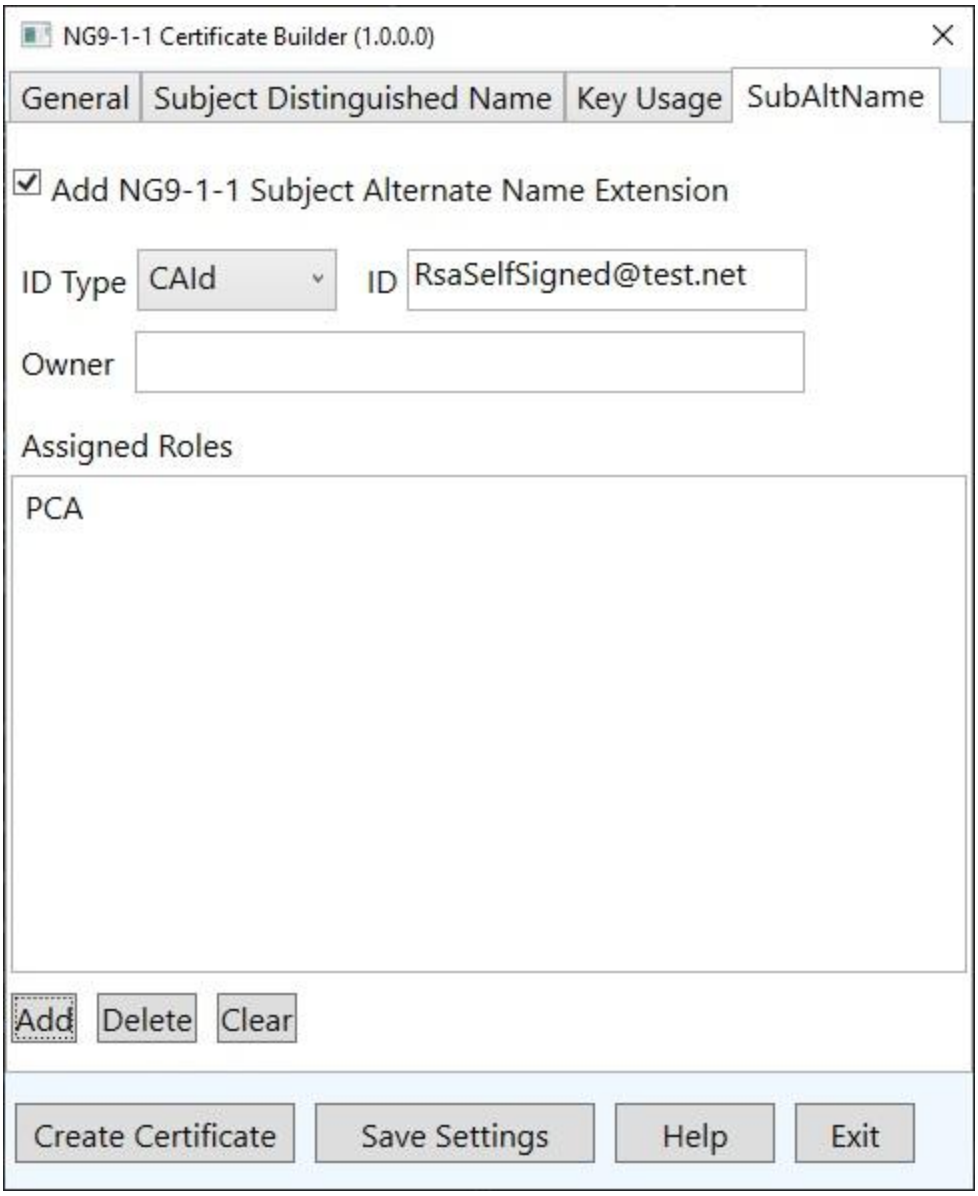
This setting indicates that the certificate will be used by clients to authenticate a server when Transport Layer Security (TLS) is used to establish a network connection. This setting applies to the extended key usage certificate extension.

### Client Authentication

This setting indicates that the certificate will be used by servers to authenticate a client (i.e. mutual authentication) when TLS is used to established a network connection. This setting applies to the extended key usage certificate extension.

## SubAltName Tab

The settings in this tab are for creating certificates used for testing NG9-1-1 applications. These settings apply to the Subject Alternate Name (SubAltName or SAN) certificate extension.




## Add NG9-1-1 Subject Alternate Name

If this checkbox is checked then a NG9-1-1 specific Subject Alternate Name extension containing an otherName sequence will be added to the new certificate. Section 7.1.2.11 of the PCA Certificate Policy document describes the otherName sequence. The otherName sequence for NG9-1-1 is a UTF-8 string that contains four fields: ID Type, ID, Roles and Owner. The following subsections describe the available settings for these fields.

## ID Type

This combo box allows you to specify the type of entity that the certificate is going to be used by. The following table describes the available choices.

| ID Type | Description |
|---|---|

| | |
|---|---|
| ElementId | The certificate is for a functional element within the emergency services network such as a BCF, LNG, Bridge (conference bridge), ECRF, ESRP, etc. |
| ServiceId | The certificate is for a service within the emergency services network. |
| AgencyId | The certificate is for a specific agency within an emergency network. |
| AgentId | The certificate is for an individual agent such as a call taker. |
| CAId | The certificate is for a Certificate Authority or an Intermediate Certificate Authority. |

**Note:** If you change the ID Type selection then you should clear the Assigned Roles list by clicking on the Clear button. Then you can add roles that are appropriate for the new ID Type.

### ID

This text box identifies the entity (element, service, agency, agent or CA) to which the certificate is being issued to. This field is required and should contain the fully qualified domain name of the entity. For example: psap.allegheny.pa.us.

### Owner

The owner field specifies the ID of the issuing agency. For an ICA the Owner field should contain the ID of the CA. For CA certificates, this field may be left empty.

### Assigned Roles

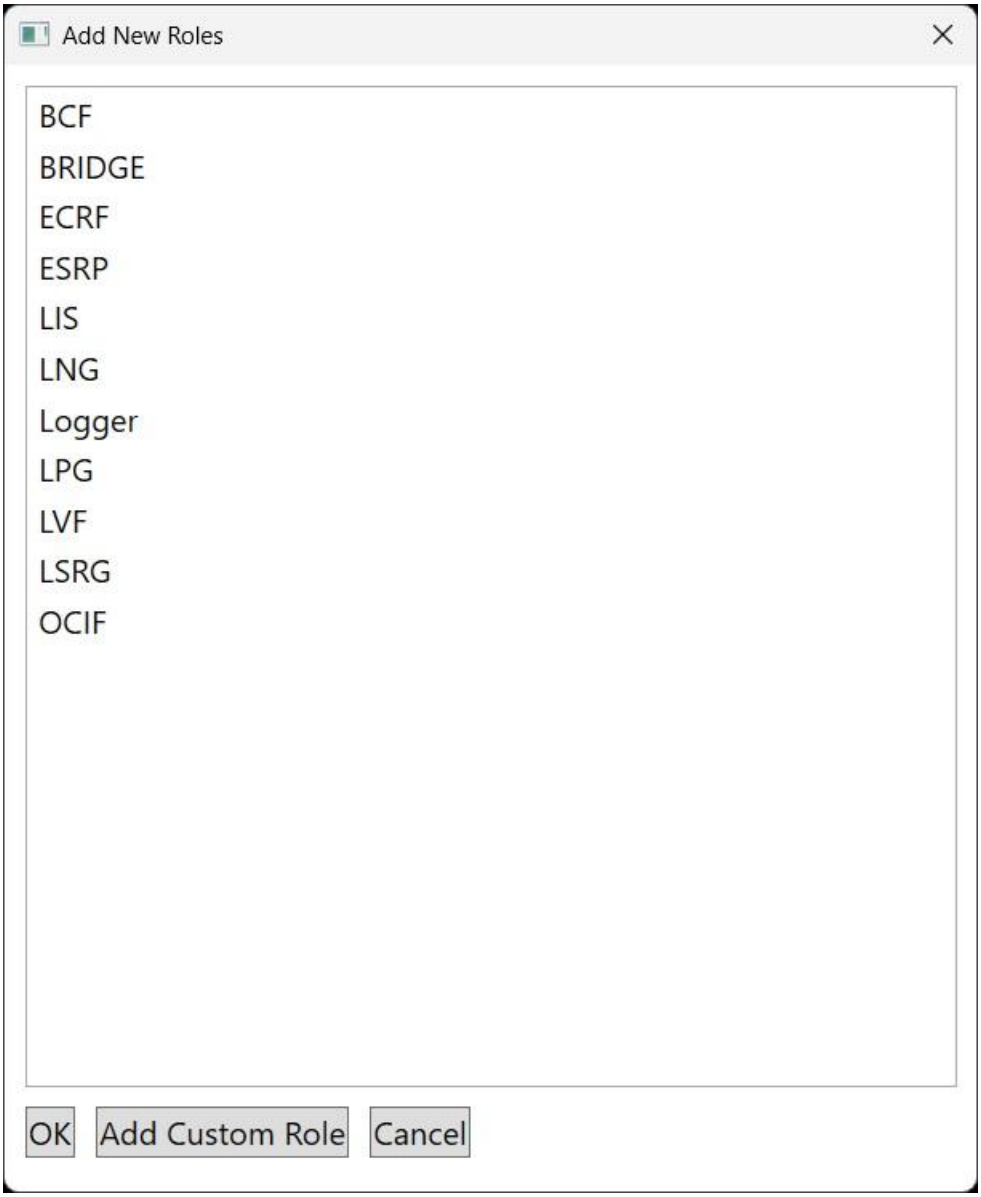
This list box contains the roles to which the subject entity is assigned to. The list may contain multiple roles and it must contain at least one role.

Click on the Add button to select the roles and the following dialog box will appear. Select one or more roles from the list of roles and click on the OK button to add the selections to the list of roles. The contents of the list in the Add New Roles dialog box depends upon the current ID Type selection.

Each ID Type has a different list of allowable roles. This dialog box shown below contains the roles for an agent.

The Delete button deletes the selected roles from the Assigned Roles list box.

The Clear button clears the Assigned Roles list box.




You can add a custom role by clicking on the Add Custom Role button. A dialog box will appear. Type the new custom role in the Custom Role text box and click on the OK button. The custom role will appear in the list of roles shown in the Add New Roles dialog box shown in the above figure. Select the new custom role from the list and click on the OK button.

The software does not remember custom roles that you add so you must repeat the above procedure each time you want to add a custom role.

# Version History

Version 1.0.0 – 9/30/2025

| Change Type | Description |
|---|---|
| NA | Initial version |