GlobalSign PKIaaS connector for Service Now

Admin installation guideline

Version 1.2.1

Table of Contents

Introduction

The Atlas PKIaaS Connector scoped application is a toolbox that allows the customer to communicate with the Atlas API using ServiceNow and Flow Designer. This article provides step-by-step instructions for install and set up GlobalSign PKIaaS connector via Service Now ITSM instance.

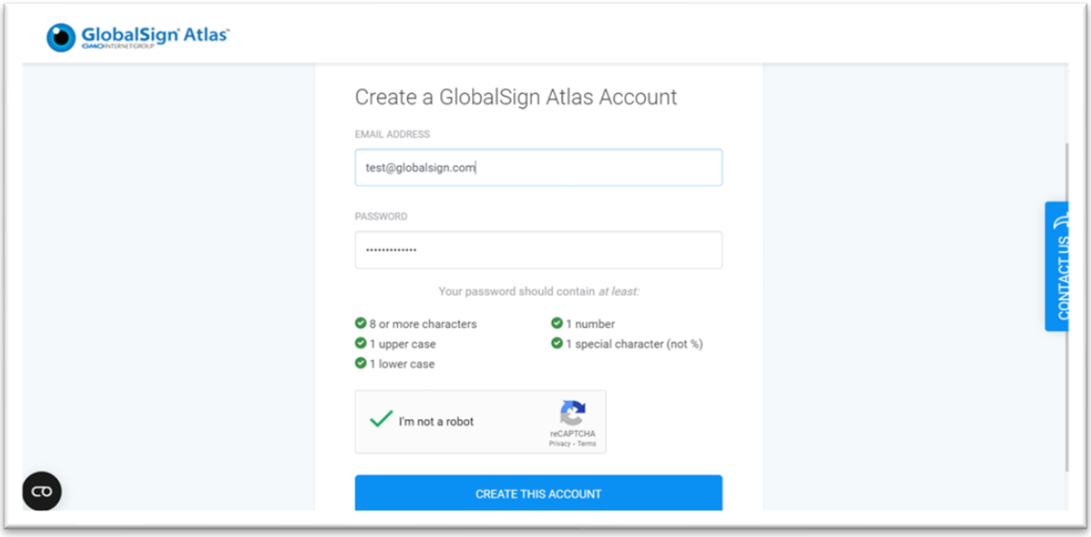
Pre-requisites

To ensure your GlobalSign PKIaaS connector working properly, review and apply the settings below:

- GlobalSign Atlas API credentials, mTLS certificate
- PKCS12 key store certificate
- Service Now ITSM or ITOM service

Registering to GlobalSign Atlas portal

Note: The existing GlobalSign customers (with Atlas portal account or HVCA direct access) can use the existing API credentials and mTLS certificate to set up GlobalSign PKIaaS connector.



Create a GlobalSign Atlas Account

EMAIL ADDRESS: test@globalsign.com

PASSWORD: ••••••••••••••

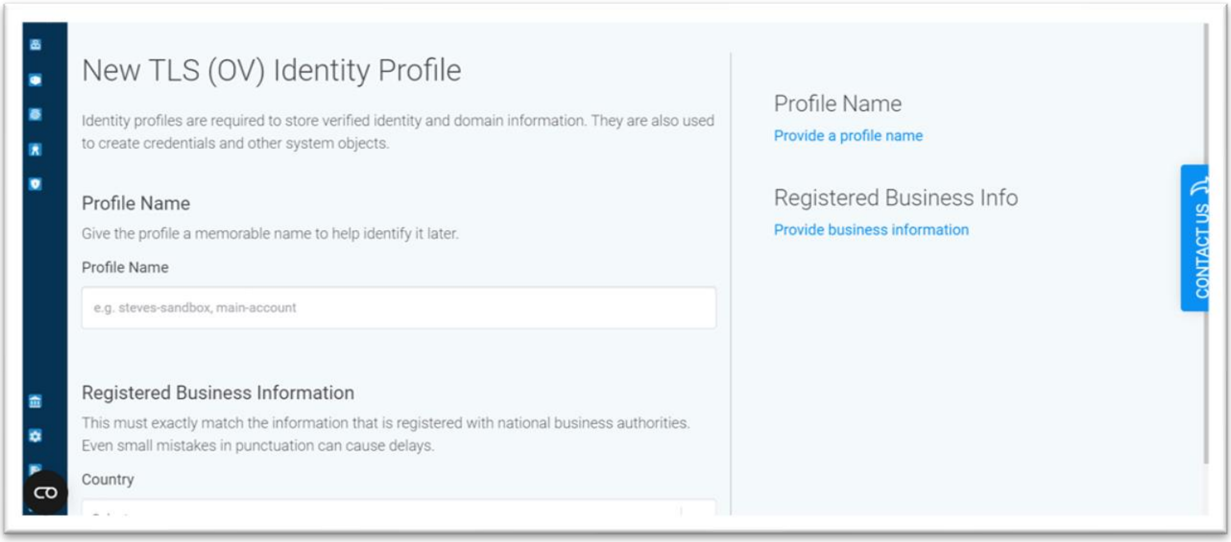
Your password should contain *at least:*

- ✓ 8 or more characters
- ✓ 1 upper case
- ✓ 1 lower case
- ✓ 1 number
- ✓ 1 special character (not %)

1. Go to Atlas website: https://atlas.globalsign.com/signup.
2. Click on Create this Account.
3. Enter in your email address and create a secure password.
4. Click on the link received to verify your account.
5. You can now login to your own Atlas account or use the link https://atlas.globalsign.com/login and click on the sign in button.
6. When you first login you will need to setup your Personal Information in the fields followed by your Company Information.
7. At the next screen, if you are a Direct customer, select your Account Type as "Just My Account". If you're a Service Provider, select "Mine and other organisations"-
8. Next, please read the hosted services agreement referring to Atlas portal usage and click continue.
9. Your Atlas Account is set up, please go to dashboard to start using.

Create identity on GlobalSign Atlas portal

Note: You must complete a purchase (or order a trial service) before you can set up an associated Identity. When you request an Identity for a Trial service or Test Certificates, it will be an auto-vetted, Domain Validated identity and available for use immediately.



New TLS (OV) Identity Profile

Identity profiles are required to store verified identity and domain information. They are also used to create credentials and other system objects.

Profile Name

Give the profile a memorable name to help identify it later.

Profile Name

e.g. steves-sandbox, main-account

Registered Business Information

This must exactly match the information that is registered with national business authorities. Even small mistakes in punctuation can cause delays.

Country

Profile Name

Provide a profile name

Registered Business Info

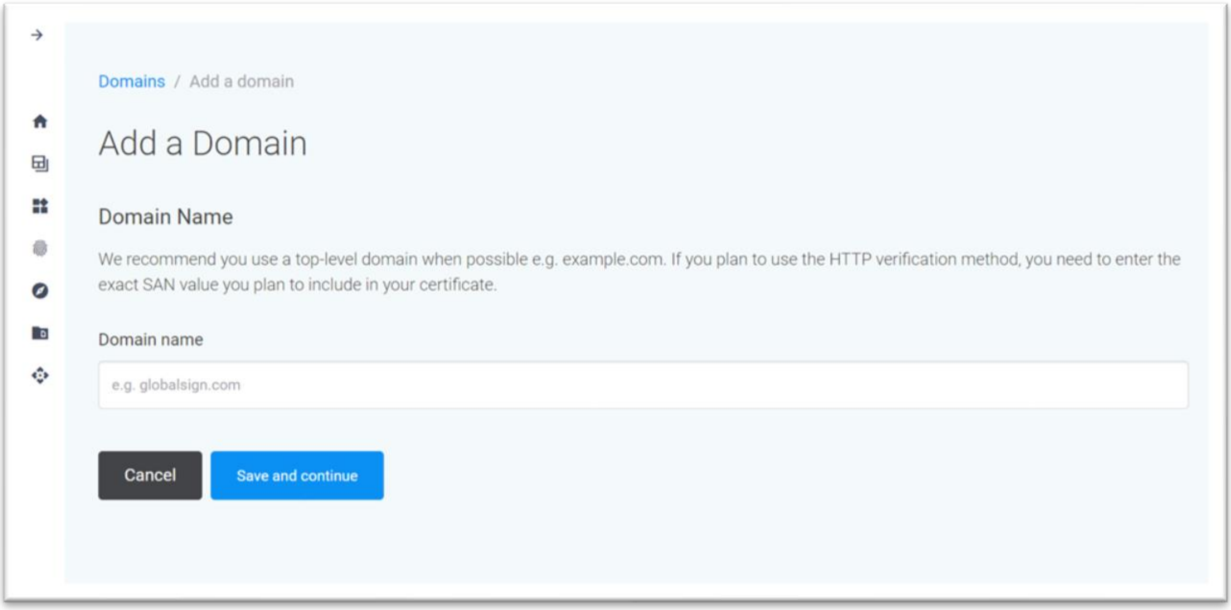
Provide business information

1. After you have purchased a Product Pack, you will be prompted to create an Identity profile. From the Dashboard, click the ‘Request an Identity Profile’ button on the ‘To Do’ action card.
2. Fill out the Identity Profile Screen & click “Request Identity”. The Identity profile screen will vary based on the product you’ve purchased.
3. If the identity belongs to not domain validated or test product packs, such as EV, OV than you need to wait for the vetting process before it will available.

Note: You can navigate to the Identities Menu Item to manage and view the status of your Identities.

Add domain validation

Note: To able to use Service Now platform with your new identity to issue certificates, you need to use validated domain what belong to your identity.



Domains / Add a domain

Add a Domain

Domain Name

We recommend you use a top-level domain when possible e.g. example.com. If you plan to use the HTTP verification method, you need to enter the exact SAN value you plan to include in your certificate.

Domain name

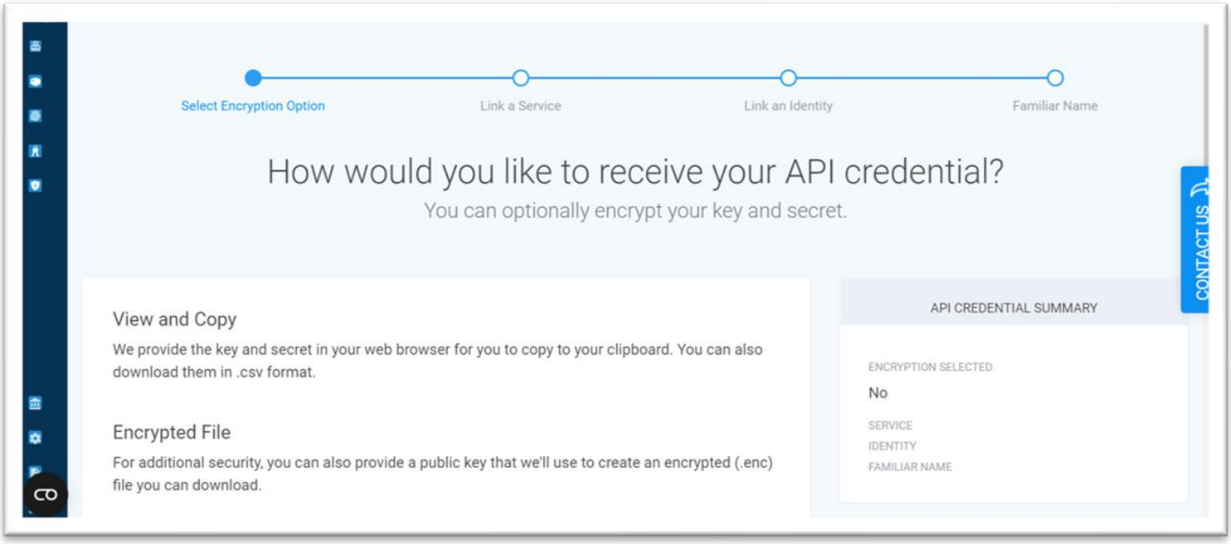
e.g. globalsign.com

To add the validated domain to your identity follow the steps:

1. Login to Atlas portal
2. Click on the left hand side on the “Domains”
3. Select your identity what you created in the previous step.
4. On the right hand side click on “Add a domain” button.
5. Add your domain name. Note: you should access to the DNS record to add the validation text.
6. Click on “Save and continue” button
7. Click on “Verify and View” button
8. On the next screen click on your domain on the left hand side.
9. Click on the “ Verify this domain” button on the right hand side.
10. Scroll down to “Domain Verification Code (DVC)” and click on “copy to clipboard”
11. Add your DVC to your DNS as a DNS TXT record.
12. Scroll down and click on the “Verify via DNS TXT”

Generate API credentials on GlobalSign Atlas portal

Note: To generate API credentials, you must have an automatically or manually vetted identity. For more information see the step above.



How would you like to receive your API credential?

You can optionally encrypt your key and secret.

View and Copy

We provide the key and secret in your web browser for you to copy to your clipboard. You can also download them in .csv format.

Encrypted File

For additional security, you can also provide a public key that we'll use to create an encrypted (.enc) file you can download.

API CREDENTIAL SUMMARY

ENCRYPTION SELECTED

No

SERVICE

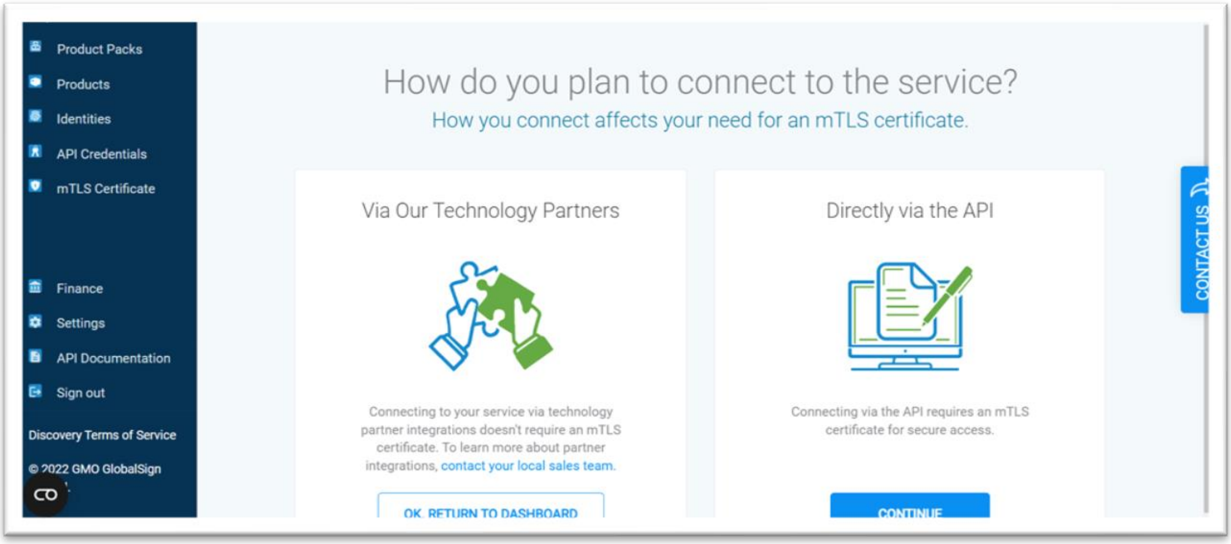
IDENTITY

FAMILIAR NAME

1. Log into Atlas website: https://atlas.globalsign.com/login.
2. Go to dashboard and click on generate API credentials.
3. Select the “View and Copy” method of API key generation: The system would provide you with API key and secret to copy to your clipboard.
4. Select the service
5. Select the identity
6. Add a familiar name
7. You can now copy key and secret to clipboard or/and download them as a .csv file.

Get mTLS (mutual TLS) certificates

Note: To generate a mTLS certificate, you must have API credentials. For more information, please follow the steps above to generate API credentials.



How do you plan to connect to the service?

How you connect affects your need for an mTLS certificate.

Via Our Technology Partners

Connecting to your service via technology partner integrations doesn't require an mTLS certificate. To learn more about partner integrations, contact your local sales team.

Directly via the API

Connecting via the API requires an mTLS certificate for secure access.

1. Log in to your Atlas Account.
2. Click either “mTLS Certificates” from the sidebar, or “Generate An mTLS Certificate” from the dashboard.
3. Select the option “Directly via the API”: Connecting via the API requires an mTLS certificate for secure access, what will direct you to a page showing all API credentials, created under the account.
4. Please then select one or more API credentials to link to the mTLS certificate.
5. Once you have selected an API credential, the details will populate under the “mTLS Certificate Summary” sidebar on the right.
6. You may now click “Continue”
7. The following “Paste a CSR” page will be showing, which is where you need to generate a Certificate Signing Request (CSR) for your mTLS certificate.
8. In order to create a CSR, please follow the guide one step below: “Generate your CSR”
9. Note. The CSR must be at least 2048 RSA key size.
10. Please then paste your CSR in the box and select “Continue”
11. You will now have your mTLS certificate.
12. Please either click “Copy to Clipboard” or simply copy the mTLS certificate, and paste this into a text editor, saving this as a “.cer” file format.
13. Please then click “Download ICA” which is the issuing CA certificate for your mTLS.
14. Your certificate should now be ready to use to authenticate into using the GlobalSign API.

Generate your CSR (Certificate signing request)

Note: For generating mTLS certificate in the step below, you will need to generate CSR. To generate CSR via OpenSSL, you need to download and install first Apache OpenSSL.

To generate the CSR the most easiest way to follow the video via the link below:
https://support.globalsign.com/ssl/ssl-certificates-installation/generate-csr-openssl

You need to use the following command:

```
openssl req -out CSR.csr -new -newkey rsa:2048 -keyout privatekey.key
```

Generate PKCS12 certificate

Note: To generate PKCS12 certificate you need to use Apache OpenSSL.

1. Downloading and installing the right version of OpenSSL for your environment.
2. Open OpenSSL terminal
3. Select the folder in the terminal, where you are storing the previously generated mTLS certificate

Use the command to generate the PKCS12 certificate:

```
Openssl pkcs12 -export -out {your pkcs12 cert name}.pfx -inkey {your private key}.key -in {your mtls cert}.pem
```

Note: You can use for your private key ".key" format also.

4. You need to "Enter pass phrase for *{yout private key}.key* ".
5. Enter Export passwords
6. Revalidate Export password
7. Check the new *{your pkcs12 cert name}.pfx* was created in your actual folder.

Register for Service Now ITSM service

Note: To use GlobalSign PKIaaS service via Service Now ITSM, you need to have Service Now ITSM instance. Please for more information, contact with Service Now: https://www.servicenow.com/products/itsm.html

Install GlobalSign PKIaaS connector from Service Now Store

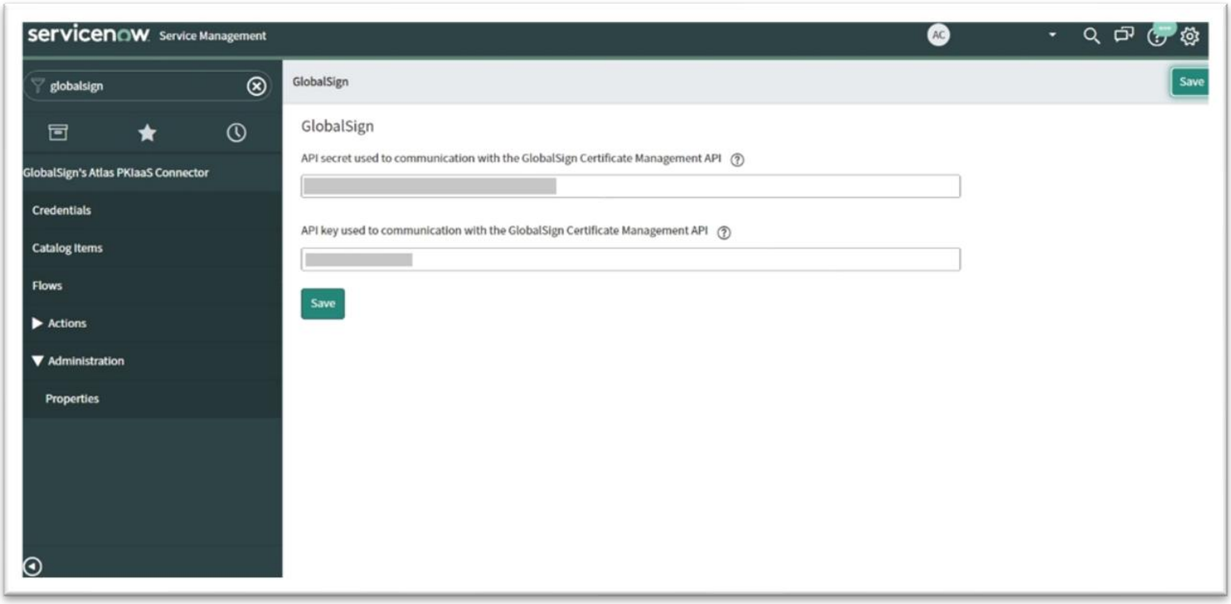
Please follow Service Now official installation guide: https://docs.servicenow.com/bundle/tokyo-application-development/page/build/applications/task/t_InstallApplications.html

Note: If you using different version from Tokyo, please select the right version installation guidelines.

Set up connection of GlobalSign PKIaaS connector

Note: To enable to connect GlobalSign PKIaaS connector and GlobalSign Atlas, you have to have a GlobalSign Atlas portal account, API credentials, mTLS and PKCS12 certificate. For more information follow the "Pre-requisites" section in the guidance.

Set up API credentials via Credential page



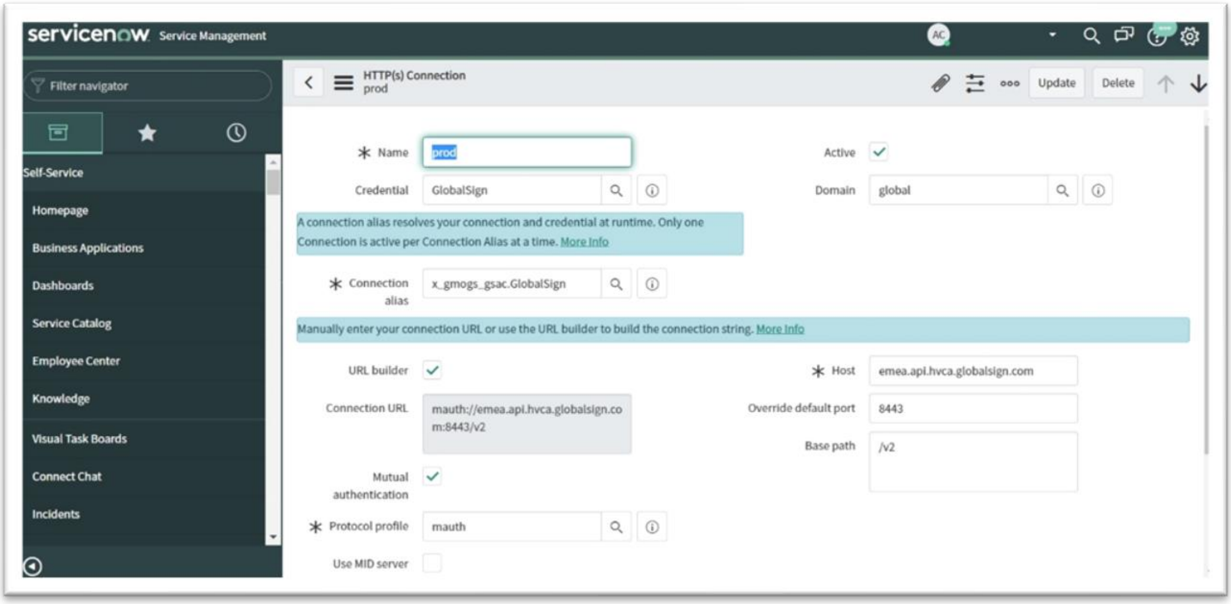
GlobalSign

API secret used to communication with the GlobalSign Certificate Management API

API key used to communication with the GlobalSign Certificate Management API

1. Login into your Service Now instance
2. Type into the search box on the left top: "GlobalSign".
3. You can see now in the list the "GlobalSign PKIaaS connector"
4. Click on the "Credentials" page
5. You can see now the API key and secret fields on the page
6. Add your API key and secret. If you need further information, please follow the steps in the "Pre-requisite -> Generate API credentials on GlobalSign Atlas portal" guidance.
7. Save the settings

Set up connection via Connection page



HTTP(s) Connection
prod

✱ Name	prod	Active	✓
Credential	GlobalSign	Domain	global

A connection alias resolves your connection and credential at runtime. Only one Connection is active per Connection Alias at a time. More Info

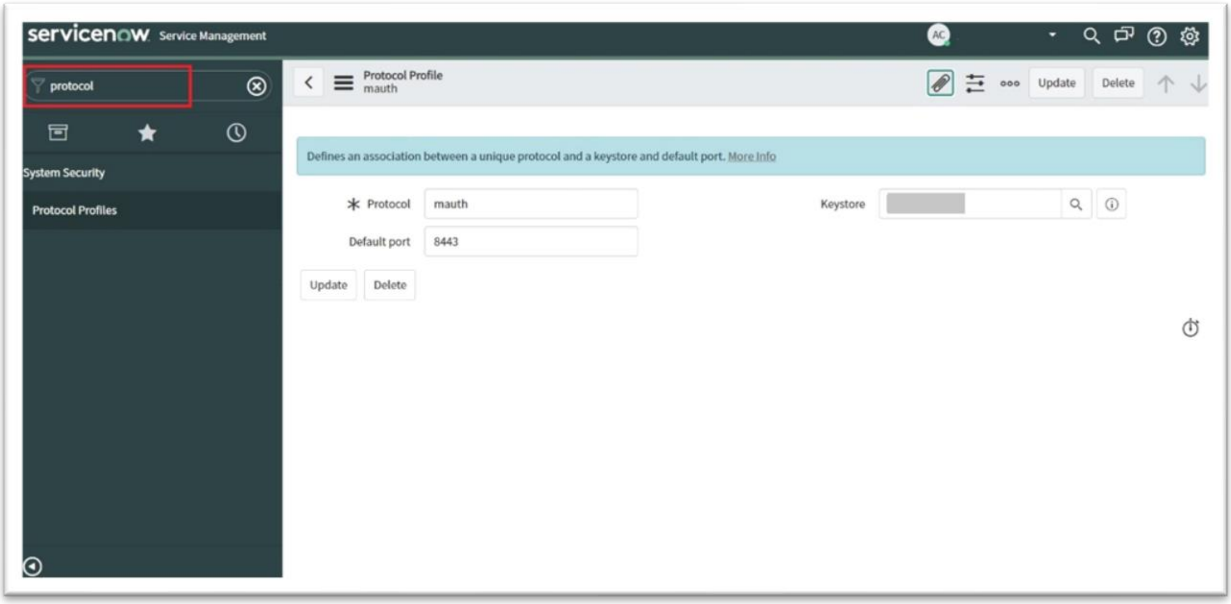
✱ Connection alias: x_gmogs_gsac.GlobalSign

Manually enter your connection URL or use the URL builder to build the connection string. More Info

URL builder	✓	✱ Host	emea.api.hvca.globalsign.com
Connection URL	mauth://emea.api.hvca.globalsign.com:8443/v2	Override default port	8443
		Base path	/v2
Mutual authentication	✓		
✱ Protocol profile	mauth		
Use MID server	□		

1. Login into your Service Now instance
2. Type into the search box on the left top: “GlobalSign”.
3. You can see now in the list the “GlobalSign PKIaaS connector”
4. Click on the “Connections” page
5. In the Connection and Credential table select “GlobalSign”
6. Click on the “GlobalSign” link
7. Scroll to the bottom and click on the “New” in the connection table
8. Provide any recognizable “Name”
9. Click on the magnifier icon beside the “Credential”
10. Select “GlobalSign”
11. You should not change in the “Connection alias”: “x_gmogs_gsac.GlobalSign”
12. You should not change “Domain”: “global”
13. If you would like to use this connection as the active connection, please tick on the checkbox “Active”. Note: Or other connection will be false.
14. Check on the “URL builder” checkbox
15. Add “emea.api.hvca.globalsign.com” to the “Host“
16. Add “8443” to the “Override default port“
17. Add “/v2” to the “Base path” field
18. Turn on the “Mutual authentication”
19. Select “mauth” for “Protocol profile“ To create a new “mauth” profile, follow the steps below “Set up mauth”
20. Leave "Use MID server” empty
21. Leave “Connection timeout” on 0
22. Click on the “Submit” button
23. You can see under the Connections table the new connection with the name what you provided in the “Name” field.

Set up mauth



Defines an association between a unique protocol and a keystore and default port. More Info

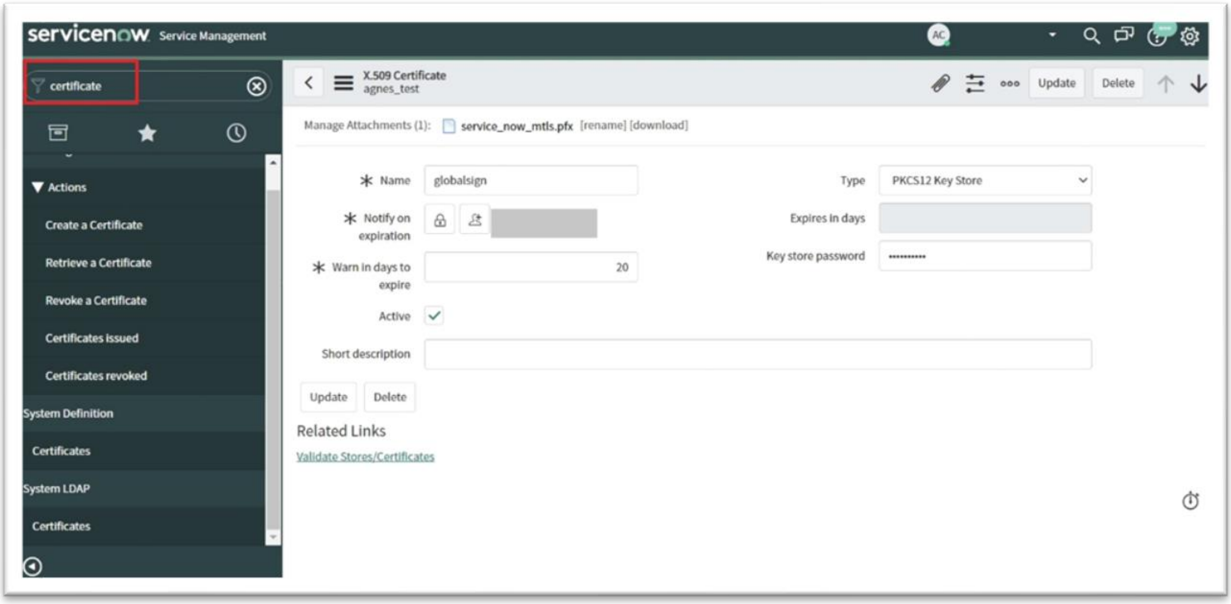
Protocol: mauth

Default port: 8443

Keystore:

1. Login into your Service Now instance
2. Type into the search box on the left top: “protocol”.
3. You can see now in the list the “Protocol Profiles”
4. Click on the “New”
5. Add “mauth” to the “Protocol” field
6. Add “8443” to the “Default port” field
7. Select your keystore. For more information about keystore, follows the steps below in the “Set up keystore” guidance
8. Click on “Submit”

Set up keystore



Manage Attachments (1): service_now_mtls.pfx [rename] [download]

Name: globalsign

Type: PKCS12 Key Store

Notify on expiration:

Expires in days:

Warn in days to expire: 20

Key store password: ••••••••••

Active: ✓

Short description:

1. Login into your Service Now instance
2. Type in the search box on the left top: “globalsign”

3. Click under the “Administration” on the “Key store certificate” menu item.

Other way to reach it:

4. Type into the search box on the left top: “certificate”.
5. You can see now in the list “Certificates” under the “System Definition” category.

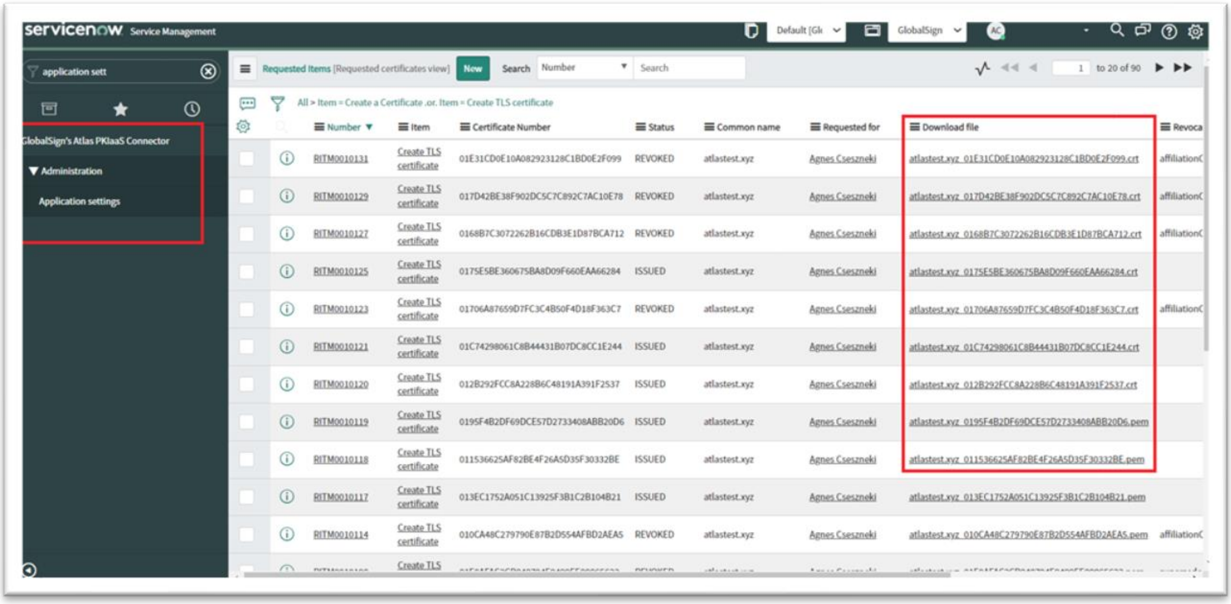
After if you find it:

6. Click on the “New”
7. Add any recognizable name to the “Name” field
8. Select “PKCS12 key store” in the “Type” dropdown
9. Add your password what you used when you generated your PKCS12 certificate. Further information about generating PKCS12 certificate please follow the steps for “Generate PKCS12 certificate” under the “Pre-requisite” section.
10. On the top select the paperclip icon to attach your PKCS12 certificate.
11. Click on “Submit”

Manage GlobalSign PKIaaS connector settings

Downloadable certificate format

The administrator can select 3 different type of the file format (.txt, .pem, .crt) for the downloadable certificate what is visible on the Request item page and on the “Certificate request” module page.


servicenow Service Management
Default [Gl
GlobalSign
AC
application sett
GlobalSign's Atlas PKIaaS Connector
▼ Administration
Application settings
Requested Items [Requested certificates view]
New
Search
Number
Search
1
to 20 of 90

All > Item = Create a Certificate .or. Item = Create TLS certificate

Number ▼	Item	Certificate Number	Status	Common name	Requested for	Download file	Revoca
RITM0010131	Create TLS certificate	01E31CD0E10A082923128C1BD0E2F099	REVOKED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_01E31CD0E10A082923128C1BD0E2F099.crt	affiliationC
RITM0010129	Create TLS certificate	017D42BE38F902DC5C7C892C7AC10E78	REVOKED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_017D42BE38F902DC5C7C892C7AC10E78.crt	affiliationC
RITM0010127	Create TLS certificate	0168B7C3072262B16CDB3E1D87BCA712	REVOKED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_0168B7C3072262B16CDB3E1D87BCA712.crt	affiliationC
RITM0010125	Create TLS certificate	0175E5BE360675BA8D09F660EAA66284	ISSUED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_0175E5BE360675BA8D09F660EAA66284.crt	
RITM0010123	Create TLS certificate	01706A87659D7FC3C4B50F4D18F363C7	REVOKED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_01706A87659D7FC3C4B50F4D18F363C7.crt	affiliationC
RITM0010121	Create TLS certificate	01C74298061C8B44431B07DC8CC1E244	ISSUED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_01C74298061C8B44431B07DC8CC1E244.crt	
RITM0010120	Create TLS certificate	012B292FCC8A228B6C48191A391F2537	ISSUED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_012B292FCC8A228B6C48191A391F2537.crt	
RITM0010119	Create TLS certificate	0195F4B2DF69DCE57D2733408ABB20D6	ISSUED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_0195F4B2DF69DCE57D2733408ABB20D6.pem	
RITM0010118	Create TLS certificate	011536625AF82BE4F26A5D35F30332BE	ISSUED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_011536625AF82BE4F26A5D35F30332BE.pem	
RITM0010117	Create TLS certificate	013EC1752A051C13925F3B1C2B104B21	ISSUED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_013EC1752A051C13925F3B1C2B104B21.pem	
RITM0010114	Create TLS certificate	010CA48C279790E87B2D554AFBD2AEA5	REVOKED	atlastest.xyz	Agnes Csesznekí	atlastest.xyz_010CA48C279790E87B2D554AFBD2AEA5.pem	affiliationC
[illegible]	Create TLS	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

The files are using the following content types:

.txt	text/plain
.pem	application/x-pem-file
.crt	application/x-x509-ca-cert

Managing GlobalSign PKIaaS connector roles

The application currently supporting the following roles:

Admin:

For admin role (x_gmogs_gsac.admin) all the functionality and settings are available.

- Create certificate / Revoke certificate
- All Certificates
- All Requests
- All Application settings
- All development item: actions, flows, catalog items

User_create:

The user (x_gmogs_gsac.user_create) most basic role for this application. The users can see the certificates what was requested for other users, also can not revoke any.

- Only Create certificate
- Only my Certificates
- Only Create certificate requests
- No Application settings
- No development items: actions, flows, catalog items

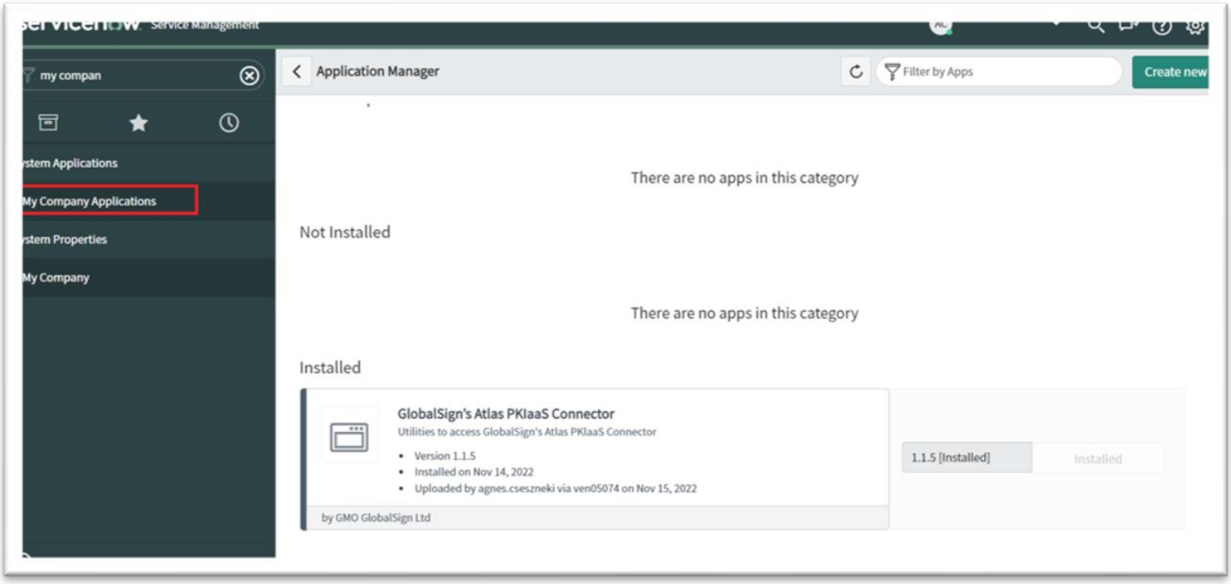
User_revocation:

The revocation user (x_gmogs_gsac.user_revocation) is an extension of the create user role to allow for them not just create but also revoke them certificates. This role can only revoke certificates what was previously requested for this user but can not see the created certificates.

- Only Revoke certificate
- Only my Certificates
- Only Revocation requests
- No Application settings
- No development item: actions, flows, catalog items

Updating GlobalSign PKIaaS connector

Note: Before you updating to the latest version, review the changes in the new version and make sure it not conflicting with any of your custom changes.



There are no apps in this category

Not Installed

There are no apps in this category

Installed

GlobalSign's Atlas PKIaaS Connector
Utilities to access GlobalSign's Atlas PKIaaS Connector

- Version 1.1.5
- Installed on Nov 14, 2022
- Uploaded by agnes.cseszneki via ven05074 on Nov 15, 2022

by GMO GlobalSign Ltd

For updating your GlobalSign PKIaaS connector to the latest version, please follow the steps below:

1. Log in to your Atlas Account.
2. On the left hand side type to the search box: “my company applications”
3. You can see in the menu and click on it.
4. You will see under the “Installed” section “GlobalSign’s Atlas PKIaaS Connector” and the installed version number.
5. If you have new version to install the “Update” button will be active and you can upgrade to the latest version.