

Identity for Everything



Quick Start Guide: Certificate Inventory Tool

November 2019



- Introduction
- Logging in
- Dashboard
- Menu
- Discovery/Scanning
 - Groups
 - Agents (Internal Scans)
- Reports
- Other Features

Do you know where you have SSL certificates installed? How about when each certificate is going to expire and which CA you ordered from? What about the hashing algorithm or key lengths used?

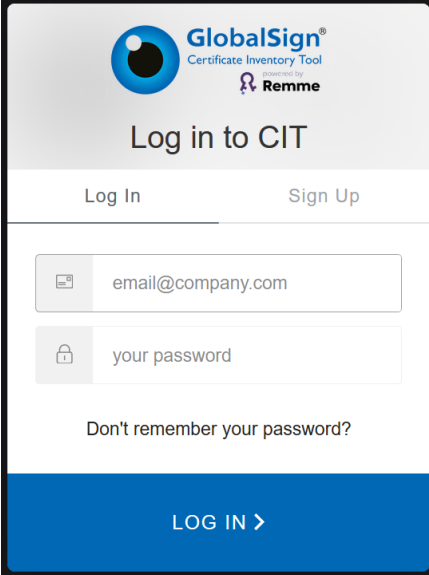
The answers are likely no, or at the very least yes, but it's difficult to compile all the information. We're happy to offer our customers free access to the GlobalSign Certificate Inventory Tool (CIT) to find all SSL certificates on your networks - both internal and public-facing - regardless of the issuing CA.

The resulting inventory is available in an easy-to-use portal, allowing you to run reports on usage, upcoming renewals, configurations, and CA issuance.

This quick start guide is designed to give you the information you need to start using the GlobalSign CIT. Let's get started!

Logging in

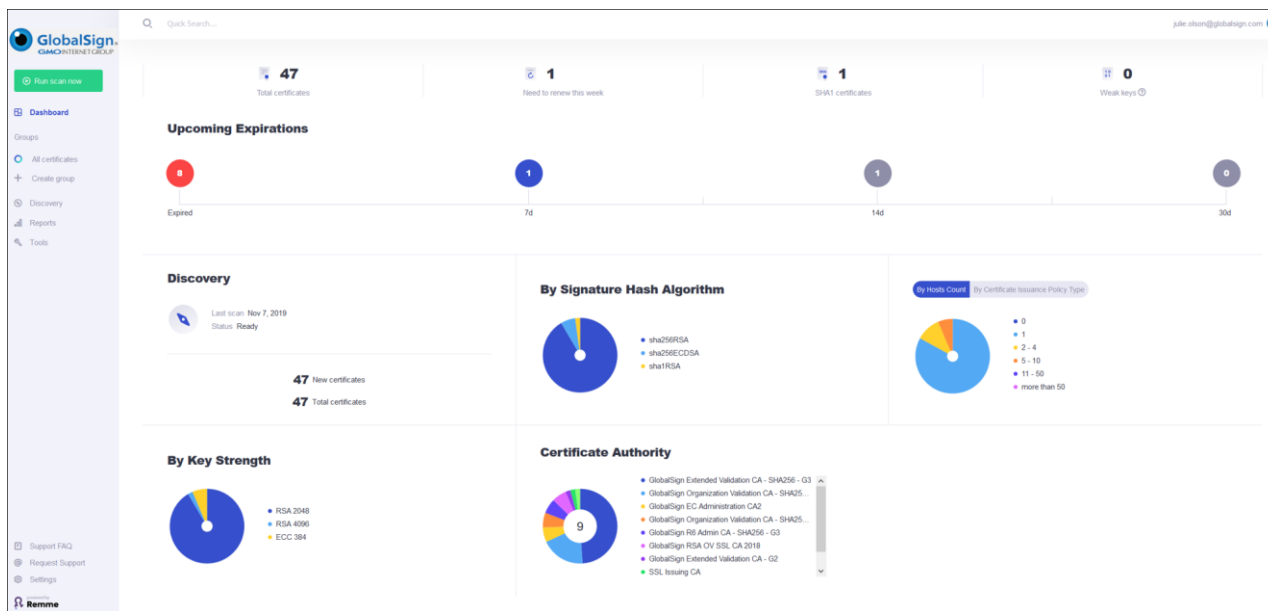
Now that you have a CIT account, go to www.cit.globalsign.com and log in by entering your company email and the password you selected during the sign-up process.



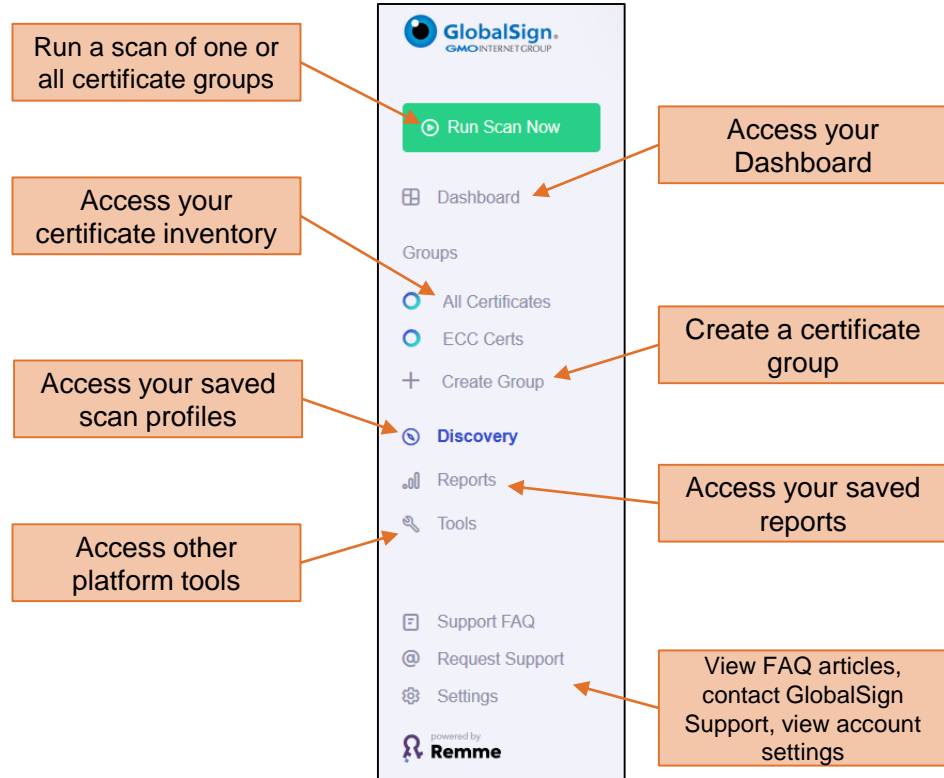
The screenshot shows the login interface for the GlobalSign Certificate Inventory Tool (CIT). At the top, the GlobalSign logo is displayed next to the text "GlobalSign® Certificate Inventory Tool" and "powered by Remme". Below this, the heading "Log in to CIT" is centered. There are two tabs: "Log In" (which is selected) and "Sign Up". The login form consists of two input fields: the first is for the email address, with a placeholder "email@company.com" and an envelope icon; the second is for the password, with a placeholder "your password" and a lock icon. Below the password field is a link that says "Don't remember your password?". At the bottom of the form is a large blue button with the text "LOG IN >".

Note: CIT is a GlobalSign-branded instance of Remme Keyhub. All support questions should be directed to your account manager or support@globalsign.com.

The Dashboard is the main screen where you can view summary pie charts on the certificates in your inventory based on key size, hash, issuing CA, and an expiration timeline. You can run a scan when you are logging into CIT for the first time, or you can do it later.



The left menu is always visible. All main functions can be accessed from this menu.



1. Click **Discovery** in the left menu.
2. Enter the details for your scan profile
 - Domains and sub-domains
 - CT log monitoring
 - Schedule
 - **Note: if you want to run an internal scan, you will have to create an Agent first.**
3. Save the profile, which will run the scan.

The screenshot displays the GlobalSign web interface for creating a scan profile. The left sidebar contains a navigation menu with options: Dashboard, Groups, All Certificates, ECC Certs, Create Group, **Discovery** (selected), Reports, and Tools. A 'Run Scan Now' button is visible at the top of the sidebar. The main content area is titled 'Create Profile' and includes a 'Quick Search...' bar. Below the title, there are tabs for 'All Profiles', 'External Profiles', 'Internal Profiles', and 'Agents'. The 'Create Profile' form has the following sections:

- Create Profile**: A dropdown menu for 'Type of Profile' set to 'External Network'.
- Set Up Profile**: A text input for 'Profile Name' with the placeholder 'My Scan Name'.
- Basic** (selected tab): A text input for 'Profile Target' with the value 'globalsign.com'. Below this are three radio buttons: 'Include Subdomains' (selected), 'Monitor Domain in CT Logs', and 'Monitor Subdomains in CT Logs'.
- Profile Ports**: A text input with the value '443'.
- Schedule**: A section with a 'Schedule Scan' radio button (selected). It includes fields for 'Start Date' (Nov 23, 2019), 'Time' (09:00), and 'Recurring' (Daily). There is also a 'Run Scan Immediately' radio button.

At the bottom of the form are three buttons: 'Save Profile', 'Cancel', and 'Delete'. The footer of the interface shows 'powered by Remme'.

After the scan runs, the results will populate your Inventory.

GlobalSign. GIGAMENTERNET GROUP

Run scan now

Dashboard

Groups

All certificates

Create group

Discovery

Reports

Tools

Support FAQ

Request Support

Settings

Remme

Quick Search...

julie.olson@globalsign.com

Export Upload

Name	Expires on	Days left	Key	Signature	Type	Status
www.globalsign.com	Jun 26, 2020	231	RSA 2048	sha256RSA	EV	Valid
revoked.r3.roots.globalsign.com	Jul 10, 2020	245	RSA 2048	sha256RSA	EV	Valid
adfs.globalsign.com	Oct 19, 2020	346	RSA 2048	sha256RSA	Basic	Valid
revoked.r1.roots.globalsign.com	Jun 20, 2020	225	RSA 2048	sha256RSA	EV	Valid
adfs.globalsign.com	Nov 4, 2018	-309	RSA 2048	sha256RSA	Basic	Expired
cit.globalsign.com	Sep 23, 2020	320	RSA 2048	sha256RSA	EV	Valid
da-psm.globalsign.com	Nov 21, 2020	380	RSA 2048	sha256RSA	Basic	Valid
expired.r1.roots.globalsign.com	Jun 20, 2018	-505	RSA 2048	sha256RSA	EV	Expired
expired.r3.roots.globalsign.com	Jul 10, 2018	-485	RSA 2048	sha256RSA	EV	Expired
iot.globalsign.com	Jun 11, 2021	581	RSA 2048	sha256RSA	EV	Valid

Items per page: 10 1 - 10 of 46

Click on a certificate to expand and view more detailed information about the certificate.

The screenshot displays the GlobalSign dashboard interface. On the left, a table lists certificates with columns for Name, Expires on, Days left, Key, Signature, Type, and Status. The first certificate, 'stolock.globalsign.com', is highlighted with a red 'Expired' status. On the right, a detailed view for 'Dashboard-mspki.globalsign.com' is shown, indicating it is 'Valid' and expires on May 23, 2020. This view includes sections for 'Certificate issuance policy', 'Source where found' (dashboard-mspki.globalsign.com), 'Scan profiles where found' (first test scan), and a 'Certificate chain' showing the hierarchy from GlobalSign Root CA to GlobalSign Organization Validation CA to the specific dashboard certificate. At the bottom, there are fields for 'Subject Alternative Names' and 'CRL Distribution Points'.

Name	Expires on	Days left	Key	Signature	Type	Status
stolock.globalsign.com	Oct 23, 2019	-33	RSA 2048	sha256RSA	Basic	Expired
dashboard-mspki.glob...	May 23, 2020	179	RSA 2048	sha256RSA	Basic	Valid
support.internal.globa...	Mar 13, 2021	474	RSA 2048	sha256RSA	EV	Valid
portal.globalsign.com	Jun 5, 2021	557	RSA 2048	sha256RSA	EV	Valid
stg-gm.globalsign.com	Aug 31, 2020	279	RSA 2048	sha256RSA	Basic	Valid
da-del.globalsign.com	Jun 2, 2021	555	RSA 2048	sha256RSA	Basic	Valid
www.globalsign.com	Mar 5, 2021	466	RSA 2048	sha256RSA	EV	Valid
revoked.r1.roots.globa...	Jul 10, 2020	227	RSA 2048	sha256RSA	EV	Valid
adfs.globalsign.com	Oct 19, 2020	329	RSA 2048	sha256RSA	Basic	Valid
revoked.r1.roots.globa...	Jun 20, 2020	267	RSA 2048	sha256RSA	EV	Valid

Items per page: 10 | 1 - 10 of 47

Dashboard-mspki.globalsign.com Valid | Hide details

Expires on **May 23, 2020** at 04:01
179 days left

Certificate issuance policy: Basic ✓ [Save Pem](#)

Source where found
dashboard-mspki.globalsign.com
[Archive](#) [Delete](#)

Scan profiles where found
first test scan

Certificate chain

- GlobalSign Root CA** Valid
Valid from Sep 1, 1996 to Jan 28, 2028
Issued by GlobalSign Root CA
- GlobalSign Organization Validation CA - SHA256 - G2** Valid
Valid from Feb 20, 2014 to Feb 29, 2024
Issued by GlobalSign Root CA
- dashboard-mspki.globalsign.com** Valid
Valid from May 23, 2018 to May 23, 2020
Issued by GlobalSign Organization Validation CA - SHA256 - G2

Subject Alternative Names
CRL Distribution Points

Discovery/Scanning - Groups

Click **+ Create group** in the left menu to create groups of certificates based on various certificate elements (expiration time, key size, common name etc.). Once saved, you can view certificates that are part of this group, and individually scan groups.

GlobalSign
GSMC/INTERNET/CELEST

Quick Search...

← Groups > Create group

Group name

Group match: All of the following conditions:

Public key type Is ECDSA

Field Select Value

+ Add condition

Save group Cancel

Creating a new group

GlobalSign
GSMC/INTERNET/CELEST

Quick Search...

Export Upload

Name	Expires on	Days left	Key	Signature	Type	Status
valid.r1.roots.globalsign.com	Jun 20, 2020	226	ECC 384	sha256ECDSA	EV	Valid
revoked.r1.roots.globalsign.com	Jun 20, 2020	226	ECC 384	sha256ECDSA	EV	Valid
expired.r1.roots.globalsign.com	Jun 20, 2019	-656	ECC 384	sha256ECDSA	EV	Expired

Items per page: 10 1 - 3 of 3

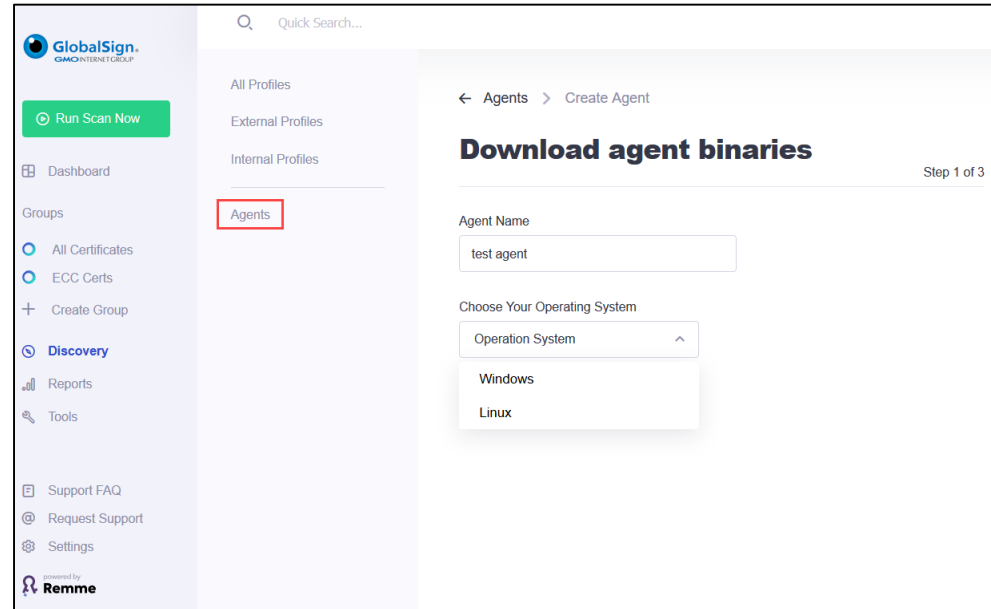
View certificates in the group

Discovery/Scanning - Agent

GlobalSign®

If you want to run a scan of your internal networks, you will need to set up an agent.

1. In the Discovery screen, click **Agents** and then **+ Create**.
2. Name the Agent and choose your operating system.



Discovery/Scanning - Agent

3. Download the Agent to your machine.
4. Activate the Agent.
5. Create an Internal Scan Profile.

← Agents > Create Agent

Download agent binaries

Step 1 of 3

Agent Name
test agent

Choose Your Operating System
Windows

Download agent for your OS:
 [Download Windows agent](#)

or use the following command
[Copy command](#)

[Continue](#) [Cancel](#)

← Agents > Create Agent

Activate the agent to scan your network

Step 2 of 3

The agent should be able to view your internal network perform scans and populate your cloud inventory.

Run the following command to activate your agent:
[Copy Command](#)

[Back](#) [Continue](#) [Cancel](#)

Create Profile

Type of Profile
Internal Network

Set Up Profile

Profile Name
My Scan Name

IP Range
192.168.1.0-192.168.1.2

Profile Ports
443,465,990,995,636,993,3389

Schedule

☒ Schedule Scan

Start Date
Nov 23, 2019

Time
09:00

Recurring
Daily

☒ Run Scan Immediately

[Save Profile](#) [Cancel](#) [Delete](#)

Reports

GlobalSign®

You can create and schedule reports to receive information on one or more of your certificate groups.

The screenshot shows the 'Report Details' form in the GlobalSign interface. The form includes fields for 'Report Name' (set to 'test report'), a description, and a 'Generate common information' checkbox. Under 'Choose settings group', 'All Groups' is selected. The 'Add email address' section has an 'Email address' field and an 'Add' button. The 'Schedule' section shows a start date of 'Nov 8, 2019', a time of '09:00', and a recurring schedule of 'Weekly'. The 'On day of the week' section has radio buttons for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, with 'Mon' selected. At the bottom, there are 'Save report', 'Cancel', and 'Delete' buttons.

Reports will be delivered to your email in a PDF file.



- CSR Decoder – Upload CSR to view more information about the request
 - Paste CSR raw text
 - Upload .pem file

The screenshot displays the GlobalSign CSR Decoder web application. On the left is a sidebar with the GlobalSign logo and navigation links: Dashboard, Groups (All certificates, Ecc certs, Create group), Discovery (Reports), and Tools. The main area has a search bar and three tabs: CSR decoder (active), Certificate decoder, and CSR generator. A blue 'Upload file' button is present. Below the tabs, a text area contains the raw CSR text, which has been decoded into human-readable fields. To the right, the 'CSR details' section shows a table of the decoded information.

CSR details

Common name	testCA1
Key Size	2048
Signature Algorithm	SHA256 with RSA
Country	US
State or province	NH
Locality	Portsmouth
Organization	GlobalSign nv-sa

Subject Alternative Names ^

DNS	testca.com
-----	------------

- Certificate Decoder – Upload public key to view more information about the certificate
 - Paste public key raw text
 - Upload .pem file

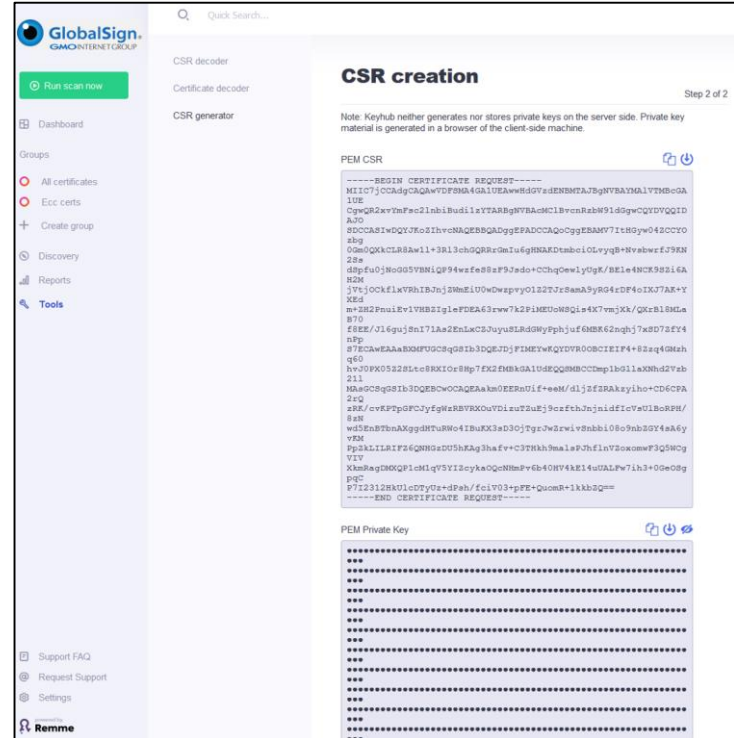
The screenshot shows the GlobalSign Certificate Decoder web application. On the left is a sidebar with navigation links: Dashboard, Groups, All certificates, Ecc certs, Create group, Discovery, Reports, and Tools. The main area has a 'Quick Search...' bar and tabs for 'CSR decoder', 'Certificate decoder', and 'CSR generator'. The 'Certificate decoder' tab is active, showing a text area with a sample certificate in PEM format. Below the text area is a 'Run scan now' button. On the right, the 'Certificate details' section displays the following information:

Certificate details	
Common name	GlobalSign
Issuer	GlobalSign
Key Algorithm	rsa
Key Size	2048
Signature Algorithm	sha256RSA
SHA256 Thumbprint	cbb522d7b71127ad8a0113865bdf1cd4102a7d0759a6f35a7c4720dc983...
SHA1 Thumbprint	D69B561148F01C7C54578C10928DF58B56976AD
Serial	040000000012158530A2
Organization	GlobalSign
Organizational unit	GlobalSign Root CA - R3

Below this, the 'Issuer details' section shows:

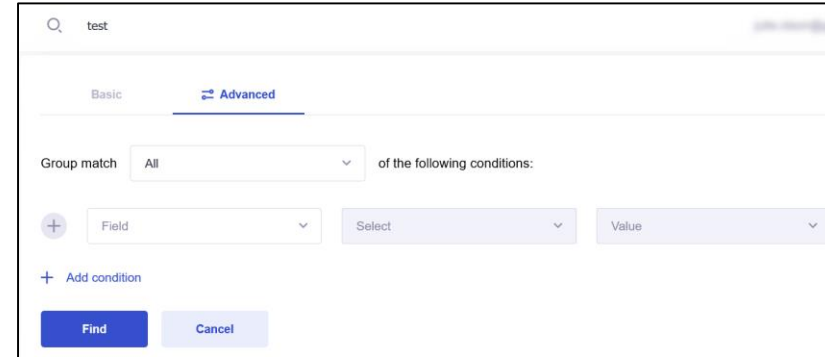
Issuer details	
Common Name	GlobalSign
Organization	GlobalSign
Organizational unit	GlobalSign Root CA - R3

- CSR Generator – Generate a CSR to initiate new certificate issuance (not through CIT)
 - Enter basic information about the certificate and then click **Generate**.
 - Information entered here will not be saved or retrievable elsewhere in the tool.



- Search Bar

- Basic search shows where and how many times your keyword appears in your portal
- Advanced search is similar to Inventory Group creator



- Archive Certificates

- Archiving certificates removes them from your Inventory and mutes expiration notifications
- Archiving certificates removes them from report results
- If the certificate is renewed or added manually to CIT, it will reappear in Inventory and reports, and notifications will resume.

The screenshot displays the GlobalSign dashboard interface. At the top, there are 'Export' and 'Upload' buttons. Below them is a table of certificates with columns: Name, Expires on, Days left, Key, Signature, Type, and Status. The first certificate, 'steflock.globalsign.com', is marked as 'Expired'. The 'Archive' button is highlighted with a red box. To the right of the table, there is a sidebar with sections: 'Certificate issuance policy' (Basic), 'Source where found' (dashboard-mspki.globalsign.com), 'Scan profiles where found' (first test scan), and 'Certificate chain' (showing a hierarchy of certificates from GlobalSign Root CA to dashboard-mspki.globalsign.com). The 'Archive' button is located in the 'Source where found' section.

Name	Expires on	Days left	Key	Signature	Type	Status
steflock.globalsign.com	Oct 23, 2019	-33	RSA 2048	sha256RSA	Basic	Expired
dashboard-mspki.glob...	May 23, 2020	179	RSA 2048	sha256RSA	Basic	Valid
support.internal.globa...	Mar 13, 2021	474	RSA 2048	sha256RSA	EV	Valid
portal.globalsign.com	Jun 5, 2021	557	RSA 2048	sha256RSA	EV	Valid
stp-gm.globalsign.com	Aug 31, 2020	279	RSA 2048	sha256RSA	Basic	Valid
ds-del.globalsign.com	Jun 2, 2021	555	RSA 2048	sha256RSA	Basic	Valid
www.globalsign.com	May 5, 2021	466	RSA 2048	sha256RSA	EV	Valid
revoked.r3.roots.globa...	Jul 10, 2020	227	RSA 2048	sha256RSA	EV	Valid
adfs.globalsign.com	Oct 19, 2020	329	RSA 2048	sha256RSA	Basic	Valid
revoked.r1.roots.globa...	Jun 20, 2020	207	RSA 2048	sha256RSA	EV	Valid

Questions? Problems?

GlobalSign®

- FAQ Articles: <https://faq.cit.globalsign.com/>
- GlobalSign CIT Support Page:
<https://support.globalsign.com/customer/portal/articles/2983266>
- GlobalSign Sales Rep

Thank you

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

