

# Identity for Everything



Quick Start Guide: Atlas Discovery



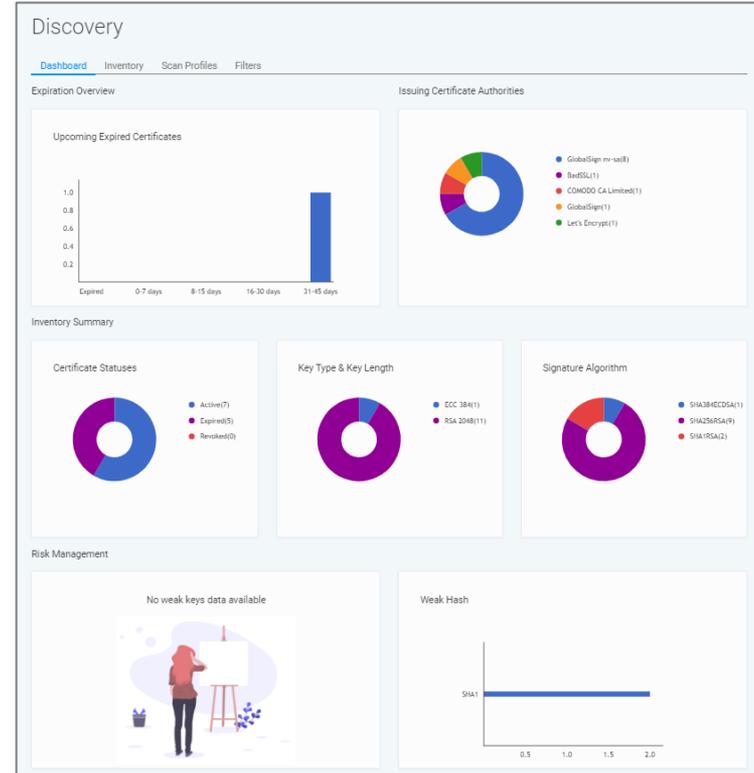
Atlas Discovery is an intuitive, easy to use TLS certificate discovery and reporting tool. It can scan both internal and external domains and networks for certificates, regardless of whether it's self-signed or issued by another CA. It also reports on attributes like key length, algorithm, validity period and expiration dates.

This guide will help you get started using Atlas Discovery to inventory your organization's TLS certificates. We'll take you step-by-step how to unlock all of Discovery's functions so you can get maximum value out of this powerful tool.

To begin, navigate to Discovery on the left nav.

The dashboard is the main screen where you can view a summary of the certificates in your inventory based on key size, hash, issuing CA, and an expiration timeline.

The dashboard links to your inventory. Click on a chart in a widget to go to a filtered view of your inventory.



# Certificate Inventory

The inventory shows all certificates that have been discovered through external & internal scans. Click on a certificate to expand the certificate details.

The screenshot displays the 'Discovery BETA' interface. At the top, there are navigation tabs: 'Dashboard', 'Inventory' (selected), 'Scan Profiles', and 'Filters'. A blue button 'UPLOAD A CERTIFICATE' with a plus icon is in the top right. Below the tabs, the 'Inventory' section features a dropdown menu set to 'Valid Certificate (Default Filter)' and a 'Download as .csv' button. A table lists certificates with columns for 'Common Name', 'Key', 'Signature Algorithm', 'Expiration Date', 'Days Left', and 'Status'. The table contains several entries, including 'GlobalSign Non-Public SHA1 CA - G3', 'GlobalSign ECC EV SSL CA 2018', and 'AlphaSSL CA - SHA256 - G2'. A detailed view of a certificate is shown on the right, titled 'GlobalSign Extended Validation CA - SHA256 - G3'. This view includes buttons for 'Download', 'Archive', and 'Delete', and shows the status as 'VALID'. It also displays the validity period, subject information (Country Name: US, Organization Name: GMO GlobalSign, Inc.), issuer information (Country Name: BE, Organization Name: GlobalSign nv-sa), authority information access (OCSP URL and Issuer Certificate), subject alternate names (34), and certificate properties (Key Size & Type: RSA 2048, Serial Number: 59566ee3a16cb80bc856c9, Signature: sha256WithRSA, SHA1 Thumbprint, SHA256 Thumbprint, and Revocation Status: Not Revoked).

Common Name	Key	Signature Algorithm	Expiration Date ↓	Days Left	Status
GlobalSign Non-Public SHA1 CA - G3	RSA 2048	sha1WithRSA	2029-12-31 18:59:59	2609 days	Active
GlobalSign ECC EV SSL CA 2018	ECC 384	sha384WithECDSA	2028-11-20 19:00:00	2203 days	Active
LLAMA.PE Intermediate CA	RSA 2048	sha1WithRSA	2026-12-07 19:00:00	1489 days	Active
*.gtranslate.net, *.tdn.gtranslate.net	RSA 2048	sha1WithRSA	2026-03-19 12:13:10	1226 days	Active
AlphaSSL CA - SHA256 - G2	RSA 2048	sha256WithRSA	2024-02-20 05:00:00	467 days	Active
AlphaSSL CA - SHA256 - G2	RSA 2048	sha256WithRSA	2024-02-20 05:00:00	467 days	Active

Signature Algorithm	Expiration Date
sha256WithRSA	2022-10-18 13:36:02
sha256WithRSA	2022-10-08 18:59:59
sha256WithRSA	2023-03-25 05:06:07
sha256WithRSA	2023-06-27 01:16:01
sha256WithRSA	2023-05-29 08:35:48
sha256WithRSA	2023-02-17 10:13:58
sha256WithRSA	2023-05-27 22:41:04
atlas.globalsign.com	2023-05-27 04:49:24

**GlobalSign Extended Validation CA - SHA256 - G3**

[Download](#)

[Archive](#)

[Delete](#)

Status: **VALID**

Valid from 2021-09-16 to 2022-10-18

**Subject**

Country Name: US  
Organization Name: GMO GlobalSign, Inc.  
Common Name: www.globalsign.com

**Issuer**

Country Name: BE  
Organization Name: GlobalSign nv-sa  
Common Name: GlobalSign Extended Validation CA - SHA256 - G3

**Authority Information Access**

OCSP URL: <http://secure.globalsign.com/cacert/gsextendvalsha2g3r3.crt>  
Issuer Certificate: <http://ocsp2.globalsign.com/gsextendvalsha2g3r3>

**Subject Alternate Names(34):**

[Click To Expand](#)

**Certificate Properties**

Key Size & Type: RSA 2048  
Serial Number: 59566ee3a16cb80bc856c9  
Signature: sha256WithRSA  
SHA1 Thumbprint: 1a0e8408b5b9238521e1b03742ae47a31dd118d3  
SHA256 Thumbprint: 8209a2053009f06e0abc0524ff37e45d48308c87cd7631e0e20fc03  
Revocation Status: Not Revoked

# Certificate Inventory

You can export your certificate inventory, or manually upload certificates to your inventory.

The screenshot displays the 'Discovery BETA' interface for managing certificates. The main view is the 'Inventory' section, which includes a filter dropdown set to 'Valid Certificate (Default Filter)' and a 'Download as .csv' button. Below this is a table of certificates with columns for Common Name, Key, Signature Algorithm, Expiration Date, Days Left, and Status. An orange arrow points from the 'UPLOAD A CERTIFICATE' button in the top right of the inventory view to a modal window titled 'Upload a Certificate'. This modal window contains a 'Browse for certificate files' button, a 'Certificate Summary' section for 'GlobalSign Non-Public SHA1 CA - G3' (showing it is 'VALID' with expiration details), and 'BACK' and 'UPLOAD' buttons at the bottom.

Common Name	Key	Signature Algorithm	Expiration Date ↓	Days Left	Status
GlobalSign Non-Public SHA1 CA - G3	RSA 2048	sha1WithRSA	2029-12-31 18:59:59	2609 days	Ac
GlobalSign ECC EV SSL CA 2018	ECC 384	sha384WithECDSA	2028-11-20 19:00:00	2203 days	Ac
LLAMA.PE Intermediate CA	RSA 2048	sha1WithRSA	2026-12-07 19:00:00	1489 days	Ac
*.gtranslate.net, *.tdn.gtranslate.net	RSA 2048	sha1WithRSA	2026-03-19 12:13:10	1226 days	Ac
AlphaSSL CA - SHA256 - G2	RSA 2048	sha256WithRSA	2024-02-20 05:00:00	467 days	Ac
AlphaSSL CA - SHA256 - G2	RSA 2048	sha256WithRSA	2024-02-20 05:00:00	467 days	Ac

# Certificate Inventory – Detail Panel

The detail panel provides more information about a certificate, and allows you to download, delete, or archive a certificate from your inventory.

Deleting a certificate permanently deletes it from your inventory, archiving hides the certificate from your inventory - but you can find it again with filters!

The screenshot displays the GlobalSign Discovery interface. On the left, a table lists certificates in the inventory. The selected certificate, 'globalsign.net', is highlighted. On the right, a detailed panel for 'GlobalSign Atlas R3 DV ACME CA 2022 Q2' is shown, including buttons for 'Download', 'Archive', and 'Delete', and a 'VALID' status indicator. The detailed view includes fields for Subject, Issuer, Authority Information Access, Subject Alternate Names, and Certificate Properties.

Common Name	Key	Signature Algorithm	Expiration Date
www.globalsign.com	RSA 2048	sha256WithRSA	2022-10-18 13:36:02
www.globalsign.com	RSA 2048	sha256WithRSA	2022-10-08 18:59:59
radirect.globalsign.com	RSA 2048	sha256WithRSA	2023-03-25 05:06:07
jan.globalsign.com	RSA 2048	sha256WithRSA	2023-06-27 01:16:01
globalsign.net	RSA 2048	sha256WithRSA	2023-05-29 08:35:48
globalsign.net	RSA 2048	sha256WithRSA	2023-02-17 10:13:58
gas.globalsign.com	RSA 2048	sha256WithRSA	2023-05-27 22:41:04
atlas.globalsign.com	RSA 2048	sha256WithRSA	2023-05-27 04:49:24

**GlobalSign Atlas R3 DV ACME CA 2022 Q2**

Download  
Archive  
Delete

Status: **VALID**

Valid from 2022-05-29 to 2023-05-29

**Subject**  
Common Name: globalsign.net

**Issuer**  
Country Name: BE  
Organization Name: GlobalSign nv-sa  
Common Name: GlobalSign Atlas R3 DV ACME CA 2022 Q2

**Authority Information Access**  
OCSP URL: http://ocsp.globalsign.com/ca/gsatlas3dvacmeca2022q2  
Issuer Certificate: http://secure.globalsign.com/cacert/gsatlas3dvacmeca2022q2.crt

**Subject Alternate Names(2):**  
[Click To Expand](#)

**Certificate Properties**  
Key Size & Type: RSA 2048  
Serial Number: 01946a9f0e0be5f73295ee6c223873  
Signature: sha256WithRSA  
SHA1 Thumbprint: 1c0d79f6cc228f6e47ef6c27aef91181a77f1126  
SHA256 Thumbprint: c079e55a0f1c1b9fa85d0e6c35a364bc896a2871452483c347573c07e  
Revocation Status: Not Revoked

## Scan for certificates by making a scan profile

1. Navigate to Scan Profiles > Create a Scan Profile
2. Enter the details for your scan profile
  - External/Agent
  - Target domain/IP address
  - Port
  - Sub-domains
3. Save the profile to run the scan. It will take several minutes for the scan results to populate your inventory. Scans run automatically every 24 hours.

### Create Scan profile

Scan Profile Name

Scan Type

External

Agent

Scan Targets

Provide a valid top-level domain name or IPv4 address or range. You may enter up to 5 targets per scan profile.

   Sub domains

[Add another target](#)

External scans are queued to run immediately upon saving and then again at the same time every 24 hours. You can also run external scans on demand from the Scan Profiles screen.

- Subdomain scans

- Scans the top 200 most used subdomains from public GIT repo
- Bundles subdomain results with top level domain
- It takes Discovery several minutes to collect and post all of the certificates to your inventory.

### Create Scan profile

Scan Profile Name

Scan Type

External

Agent

Scan Targets

Provide a valid top-level domain name or IPv4 address or range. You may enter up to 5 targets per scan profile.

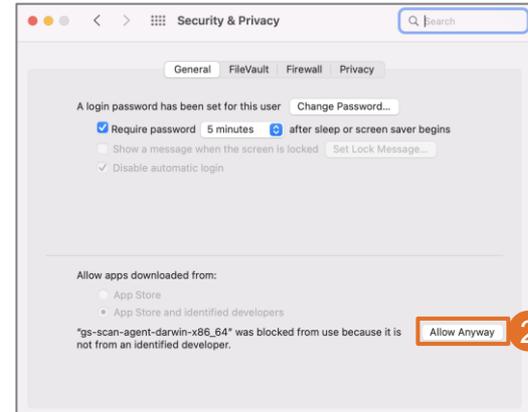
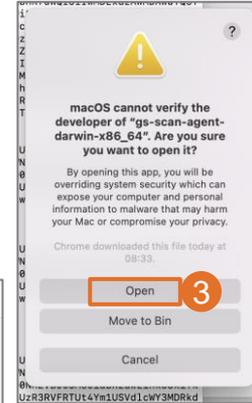
Enter domain, IP address, or IP address range here   Sub domains

[Add another target](#)

External scans are queued to run immediately upon saving and then again at the same time every 24 hours. You can also run external scans on demand from the Scan Profiles screen.



- Internal scanning agent - Darwin & Linux
  - To run the agent, change the agent's executable permissions using command **chmod a+x**.
- Internal scanning agent - Darwin
  - The agent for Darwin is not currently codesigned.
  - On the security pop-up, click **Cancel**.
  - Go to **System Preferences > Security & Privacy > General** tab. Click “Allow Anyway” where it says that the app was blocked.
  - Run the agent again, and on the next pop-up click **Open**.



# Inventory Filters

## Save a custom view of your inventory via Filters

1. Navigate to Filters > Create a Filter
2. Use the rule drop-downs to customize a filtered view of the inventory. Click **Add a rule** for multiple criteria.
3. Save the filter and select it in the drop-down menu on the inventory to view all certificates that match your criteria.

Discovery / Filters / Create a Filter

### Filters for Certificates

Filter Name

Provide a familiar name to identify your filter Name on Certificate Page...

The filter should match; All of the following rules:

1. Show Certificates where the Status is Not Revok
2. Show Certificates where the Public Key Algorithm is RSA

Add a rule

CANCEL

Discovery

Dashboard Inventory Scan Profiles Filters

Certificate Inventory

globalsign all

Common Name	Key	Signature Algorithm	Expiration Date	Days Left	Status
www.globalsign.com	RSA 2048	sha256WithRSA	2022-10-18 13:36:02	83 days	PENDING
www.globalsign.com	RSA 2048	sha256WithRSA	2022-10-08 18:59:59	73 days	ACTIVE
www.doug-beattie.com	RSA 2048	sha256WithRSA	2021-06-24 07:55:57	-988 days	EXPIRED
survey.globalsign.com	RSA 2048	sha256WithRSA	2023-06-13 10:26:18	320 days	ACTIVE
search.globalsign.com	RSA 2048	sha256WithRSA	2023-01-13 20:01:09	170 days	ACTIVE
GlobalSign ECC EV SSL CA...	ECC 384	sha384WithRSA	2028-11-20 19:00:00	2308 days	ACTIVE

Rows per page: 10 1 - 6 of 6

## How many ports can I add to my scan profile?

Currently only one port is allowed per scan target. The default port is 443.

## When I run a scan it shows as not started, why?

If it's an internal scan, most likely you need to download and configure the scanning agent first. If it's an external scan, it's possible the scan job succeeded but it didn't find a certificate at the endpoint. This is a known issue and will be resolved in future releases.

## Why are my scans not running every 24 hours?

Sometimes the scan job gets interrupted and needs to be rebooted. Re-run the scan which will resume automatic scanning.

## What are the limits of domains the tool can check at once?

There is no limit to the number of domains Discovery can check at once, but there is a limit to the number of targets you can add to your scan profile (currently 5).

## Can multiple people use Discovery within an Atlas account?

Yes, you can add other users to your Atlas account so they can view the same detail in Atlas Discovery.

## Does Atlas Discovery monitor CT logs?

No, Atlas Discovery does not currently monitor CT logs. This will be available in a future release.

# Questions? Problems?

- [Atlas Discovery webpage](#)
- [Atlas Discovery datasheet](#)
- Call your 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).

