

Dynamic Scanner



✅ This feature requires a [Wiz/Gov Advanced license](#). [Learn more.](#)

The Dynamic Scanner can be used to periodically validate the status of ports and IP addresses that were calculated to be potentially exposed based on your cloud network configurations. This provides additional confirmation that resources are accessible from the public internet.

How it works

1. During the regularly scheduled scan of your environment, [Application Endpoints](#) are added to and/or updated on the Security Graph.
2. By default, every day the Dynamic Scanner [attempts to validate the status of ports](#) from an external address.
3. For all [HTTP ports](#), a GET request is sent and any response recorded.
4. For every successful GET request, send an additional GET request for taking a browser screenshot.

⚠️ The Dynamic Scanner does not check all ports on all addresses. It checks only the following:

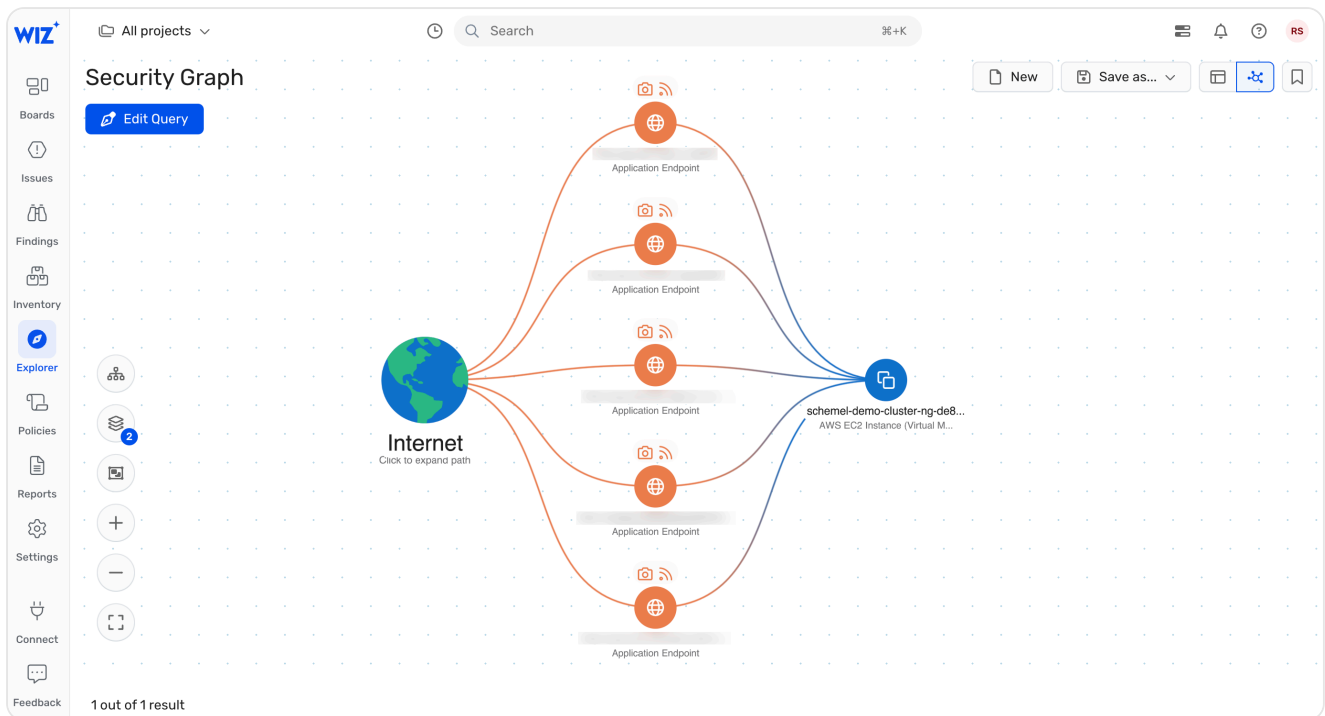
- Ports detected as exposed by the network analyzer.
- Ports from the supported ports list below.

Application Endpoints

After every full scan of your environment, Wiz performs external network exposure analysis on all cloud resources to calculate potential external exposure. [Learn about network exposure.](#)

After calculating which resources are potentially externally exposed and how, Application Endpoints are added to the Security Graph for every identified address/port and attached to every exposed resource.

This VM, for example, has no fewer than five Application Endpoints linked to it on the Security Graph:



Port scan

Using the list of Application Endpoints, the Dynamic Scanner periodically (every seven days, by default) tries to connect to suspected open ports from the outside using the TCP three-way handshake (SYN, SYN-ACK, ACK). After scanning the ports, the result is recorded in the `Port Status` property on the Application Endpoint details drawer.

The possible values and meanings of the `Port Status` property are:

- Open—At least one port is open.
- Closed—All ports are closed.
- Scanner disabled—The Dynamic Scanner is not enabled for the tenant.
- Excluded from scan—The Application Endpoint was not scanned because it is attached to a cloud resource in a Project that is out of the Dynamic Scanner's scope.
- Unsupported port—For an Application Endpoint open on all ports, the Dynamic Scanner checks only supported ports (see [supported ports](#) below).
- Scan failed—The Dynamic Scanner encountered an issue and couldn't scan the port.

The property `Validated Open Ports` lists all open ports.

i You can enable and configure the Dynamic Scanner on the [Settings > Scanners > Dynamic Scanner](#) page.

Validating a result

If you suspect a false positive and that a port is in fact closed:

1. Run the following command from your terminal:

Shell

```
nc -z -v <IP address> <port number>
```

2. If the result is `Connection to <IP Address> port <Port number> [tcp/https] succeeded!`, then the port is in fact open. For any other result, then you were correct and the port is closed.
3. To validate the HTTP status code, run the following command:

Shell

```
curl -i <IP address>
```

We'd very much appreciate you [letting us know](#) about any verified false positives.

HTTP scan

If one of the open ports is defined in Wiz as a [supported HTTP/S port](#), the Dynamic Scanner sends an HTTP GET request to the server. The response is recorded in three properties on the Application Endpoint details drawer:

- **HTTP Status :**
 - HTTP status as it was returned from the server (2xx, 3xx, etc.)
 - "Unsupported HTTP Path" for an invalid path, e.g. `www.example.com/*/foo` or `www.example.com/{path}/foo`
 - "Client error" if the Dynamic Scanner receives an unsuccessful HTTP response, which can occur when the target server is listening for a non-HTTP protocol
- **HTTP Status Code** —Digits only for easy search. Click View Response Body to see the first 1000 characters of the GET response.
- **Web Page Title** —Web page title of the Dynamic Scanner GET request, if applicable.

Supported protocol-specific and HTTP/S ports

The following protocol-specific and HTTP/S ports are scanned:


Protocol	Port(s)
FTP	21

Protocol	Port(s)
SSH	22, 2222
SMTP	25
HTTP/S	80, 443, 591, 1443, 2443, 3443, 4443, 5443, 6443, 7443, 7990, 8000, 8001, 8008, 8080, 8081, 8082, 8088, 8443, 8800, 8808, 8880, 8881, 8882, 8888, 9000, 9090, 10000
SMB	445
IPSec Key Exchange	500
SFTP	990
MSSQL	1433
Grafana	3000
MySQL	3306
Public managed SQL	3342
RDP	3389
UPnP	5000
PostgreSQL	5432
WINRM HTTP	5985
WINRM HTTPS	5986
Redis	6379
Kubernetes API	6443, 10250
Cassandra	7000
Cassandra SSL	7001
Elasticsearch	9200
Kubernetes	10250
Memcached	11211
Istio	15006, 15010, 15012, 15021
MongoDB	27017

Application fingerprinting

For HTTP/S ports, the Dynamic Scanner preserves the raw text of the HTTP GET response, which we use to identify technologies on the application endpoint. Leveraging the [Wappalyzer](#) technology profiler, the Dynamic Scanner runs Wappalyzer templates against the raw text. When a technology is detected, the "Validated in Runtime" signal is added to the hosted technology object on the Wiz Security Graph, and the hosted technology is connected to the application endpoint.


Application fingerprinting can also detect the authentication method and authentication service provider of Application Endpoints. The four types of authentication methods that can be detected are basic, digest, NTLM, and SSO.

-  For SSO, the supported service providers currently are Google Workspace, Microsoft Entra ID (AAD) App, Okta, Ping, and Duo SSO.

[See all supported applications.](#)

Dynamic Application Endpoint severity

Application Endpoint severity is recorded on the Graph object to help you assess the risk that Application Endpoints pose to your environment and more easily prioritize the remediation of related Issues.

-  Application Endpoints have critical severity whenever they were not scanned by the Dynamic Scanner, e.g., if you don't have a Wiz advanced license or narrowed down its scope. This cannot be configured.

The Dynamic Scanner analyzes Application Endpoints based on various factors, such as the identified authentication method, the HTTP status code, and the type of exposed resource. Wiz then calculates the severity of the Application Endpoints based on these factors and one of the following configurable severity policies:

- **Permissive**—A lenient policy, resulting in fewer critical severity Application Endpoints. In particular, the severity will be significantly lower for Application Endpoints returning non-2XX HTTP status codes. This policy helps you focus on addressing the most critical risks and facilitates prioritization in environments with a large number of Issues. Therefore, we do not recommend it for long-term use or for environments with a relatively small number of Issues, where higher sensitivity is required. [See the policy's Rego code.](#)

Below is the full logic of the policy and how it is mapped to different Application Endpoint severities:

▼ **Non-HTTP**

TCP three-way handshake	Severity
Successful	Critical
Unsuccessful	Low

▼ **HTTP**

Status code	Authentication	Severity for directly exposed buckets	Severity for all other scanned resources	Notes
1XX	-	Medium	Medium	1XX status codes informational, indicating that the server has received the request and is processing it. Usually temporary and are replaced with another status code.
101	-	Critical	Critical	101 is a status code for switching protocols.
2XX	Not detected	Critical	Critical	2XX Successful status codes with no authentication detected.
2XX	Digest/NTLM/Basic	High	High	Although an authentication method has been detected, it is not considered secure. - Basic: sends credentials in base64-encoded form, which can be easily decoded; therefore, brute-force attacks can be performed. - Digest: no anti-replay mechanism in place, therefore, susceptible to brute-force attacks.

Status code	Authentication	Severity for directly exposed buckets	Severity for all other scanned resources	Notes
				usually used by M Entra ID (AAD) us once credentials a obtained, it increa chances for latera movement. Also, susceptible to rela and is considered and weak encrypt
2XX	SSO	Medium	Medium	SSO is usually eas implement with M Wiz detects the id providers: Microsc Google, and Ping, which are conside reliable and secur implementation o
3XX	-	Medium	Medium	3xx status codes that further action (redirection) needs performed. At this processing the re cannot determine Application Endpc secure.
4XX	-	Medium	High	4xx status codes an error originatir client's side. It cor related to authent and authorization issues, such as wr request method o timeout.
400	-	Medium	High	400 status code (l request) indicates server cannot or v process the reque

Status code	Authentication	Severity for directly exposed buckets	Severity for all other scanned resources	Notes
401	Digest/NTLM/Basic	Medium	Medium	See above the row status codes with
401	Not detected	Medium	Medium	401 status code (“unauthorized”) indicates that there is an authentication/authorization mechanism in place although it was not detected.
401	SSO	Medium	Medium	See above the row status codes with
404	-	High	High	404 status code indicates that the resource current path was
403	-	Medium	Medium	403 status code indicates that an authorization authentication mechanism is in place.
407	-	Medium	Medium	407 status code requires an authorization authentication mechanism that is in place.
423	-	Medium	Medium	423 status code requires an authorization authentication mechanism that is in place.
498	-	Medium	Medium	498 status code requires an authorization authentication mechanism that is in place.
5XX	-	Medium	Medium	5XX status codes indicate various errors originate from the server side and indicate that the server is not available.

Status code	Authentication	Severity for directly exposed buckets	Severity for all other scanned resources	Notes
500	-	High	High	500 status code is a server error. The server error message might contain sensitive information that could be used by a malicious actor, such as credentials and session tokens.

- Moderate—A more stringent policy, while still taking into account the various factors described above (authentication methods, status codes, etc.). This is the default policy for tenants created after May 9th, 2024. [See the policy's Rego code.](#)

Below is the full logic of the policy and how it is mapped to different Application Endpoint severities:

▼ Non-HTTP	
TCP three-way handshake	Severity
Successful	Critical
Unsuccessful	Low

▼ HTTP				
Status code	Authentication	Severity for directly exposed buckets	Severity for all other resources	Notes
1XX	-	High	High	1XX status codes are informational, indicating that the server has received the request and is processing it. Usually, these are temporary and are replaced with another status code.

Status code	Authentication	Severity for directly exposed buckets	Severity for all other resources	Notes
101	-	Critical	Critical	101 is a status code for switching protocols.
2XX	Not detected	Critical	Critical	2XX Successful status code with no authentication detected.
2XX	Digest/NTLM/Basic	High	High	<p>Although an authentication method has been detected, it is not considered secure.</p> <ul style="list-style-type: none"> - Basic: sends credentials in base64-encoded format which can be easily decoded; therefore, brute-force attacks can be performed. - Digest: no anti-replay mechanism in place, therefore, susceptible to brute-force attack. Usually used by Microsoft Entra ID (AAD) until once credentials are obtained, it increases the chances for lateral movement. Also, it is susceptible to relay attacks and is considered weak encryption.
2XX	SSO (Single sign-on)	Medium	Medium	SSO is usually easily implemented with Microsoft Wiz detects the identity providers: Microsoft, Google, and Ping, which are considered reliable and secure implementations.

Status code	Authentication	Severity for directly exposed buckets	Severity for all other resources	Notes
3XX	-	High	High	3xx status codes that further action (redirection) needs performed. At this processing the request cannot determine Application Endpoints secure.
4XX	-	Medium	High	4xx status codes an error originating client's side. It correlated to authentication and authorization issues, such as wrong request method or timeout.
400	-	High	High	400 status code (Bad request) indicates server cannot or will not process the request.
401	Digest/NTLM/Basic	High	High	See above the rows status codes with authentication methods.
401	Not detected	Critical	Critical	Although a 401 status code ("unauthorized") indicates that there is an authentication/authorization mechanism in place, the authentication was not detected, treated as a 2XX status code with an "unknown" authentication method.
401	SSO	Medium	Medium	See above the rows status codes with authentication methods.

Status code	Authentication	Severity for directly exposed buckets	Severity for all other resources	Notes
404	-	High	High	404 status code indicates that the resource at the current path was not found.
403	-	Medium	High	403 status code indicates that an authorization mechanism is in place.
5XX	-	High	High	5XX status codes indicate various errors originating from the server side and indicate that the service is not available.

- Strict—All Application Endpoints have critical severity, regardless of the factors described above. This is the default policy for tenants created before May 9th, 2024. [See the policy's Rego code.](#)

[Learn how to configure the Application Endpoint severity policy and see the Rego code of each policy.](#)

To understand the difference between the policies, let's assume that a web server is publicly exposed to the Internet with basic authentication:

- For a permissive policy—The severity would be medium since any authentication provides a security boundary.
- For a moderate policy—The severity would be high since basic authentication is considered a weak method susceptible to abuse in man-in-the-middle or brute-force attacks.
- For a strict policy—The severity is always critical.

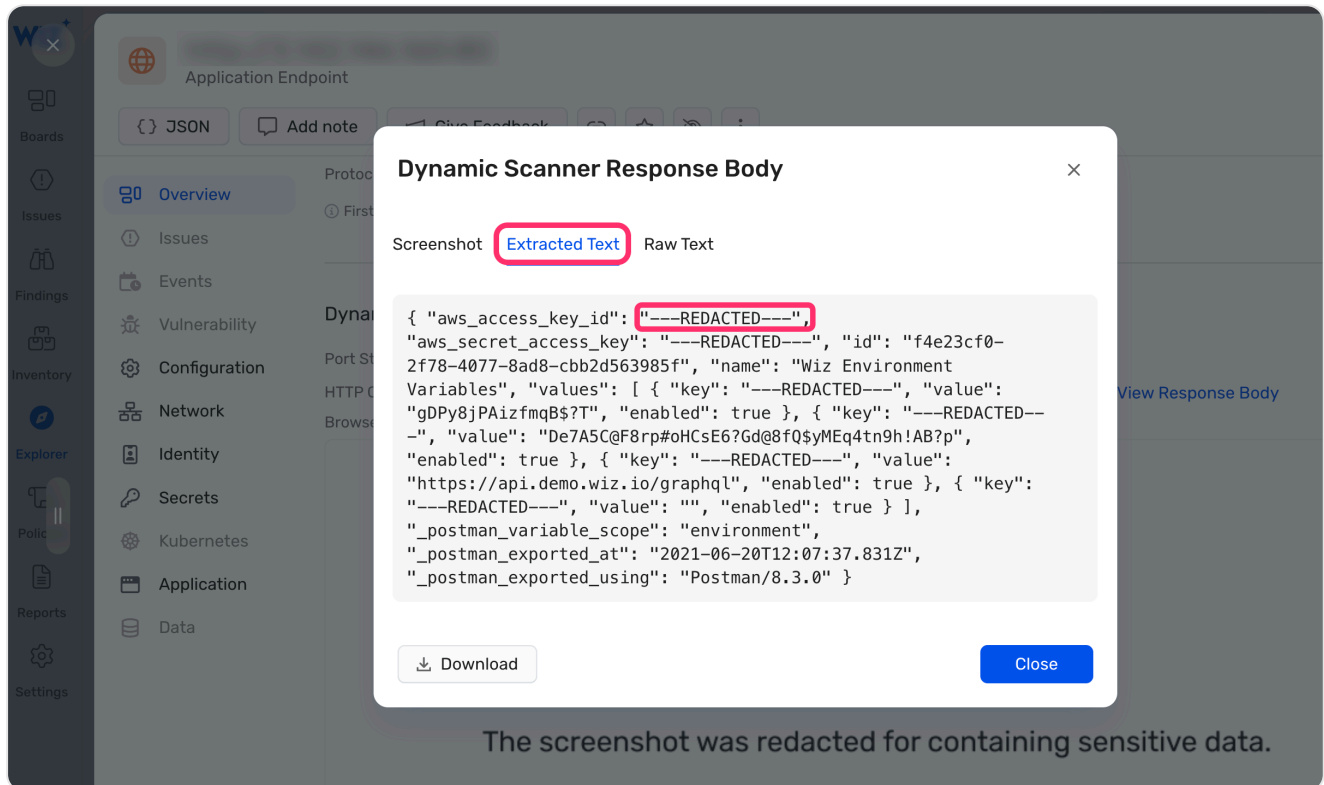
Validation screenshot

If the Dynamic Scanner has managed to successfully connect to an Application Endpoint from an exposed HTTP/S port, it takes a screenshot of the browser and attaches it to the Application Endpoint Graph object. You can browse these screenshots on the Security Graph table view in the dedicated Browser Screenshot column, and hover to enlarge and investigate. Additionally, a camera icon is added to the

Application Endpoint on the Security Graph. Wiz also extracts the raw text from the image.

⚠ Screenshots are supported for HTTP/S ports only.

If sensitive data or secrets are detected in a screenshot, both the screenshot and the sensitive data/secrets are removed from the Wiz backend. If you would like to view their location, you can either access the URL yourself or inspect the extracted text and raw text tabs in the Application Endpoint details drawer.



External data scanning

For HTTP/S ports, the Dynamic Scanner preserves the raw text of the HTTP GET response. This text is subsequently subjected to data scanning and secrets scanning, to identify publicly sensitive data and secrets.

- If sensitive data is detected, a Data Finding object is generated and linked to the Application Endpoint.
- If a secret is identified, a secret instance object is created and linked to the Application Endpoint.

Host Configuration Rules validation

The Dynamic Scanner can check exposed hosted technologies for misconfigurations using Host Configuration Rules. This feature is enabled by default and can be disabled on the [Settings > Scanners > Dynamic Scanner](#) page. [Learn more.](#)

Scan frequency

You can configure the scan frequency on the [⚙️ Settings > Scanners > Dynamic Scanner](#) page.

Scan scope

From the [⚙️ Settings > Scanners > Dynamic Scanner](#) page, you can configure the Dynamic Scanner to validate exposed resources only in specific Projects:

- (Recommended) Specify which Projects should be *excluded*, or
- Select which Projects to scan

Scan impact

The Dynamic Scanner should not impact your environment or network in any way. It implements a throttling mechanism to prevent the same IP address/port from being scanned more than once per second. This protects unusual setups where single endpoints expose a large number of services (e.g. via a load balancer) from being overwhelmed by numerous concurrent requests.

The port scanning makes a simple SYN-ACK request against the suspected open ports only with no payload.

For the HTTP scan, a single read-only request (HTTP GET) is sent to each resource, which should not impact its availability.

FAQ

Questions? Take a look at the [FAQ](#).

 Updated about 1 month ago

← Custom File Detection

Malicious IP and Domain Detection →

Did this page help you?  **Yes**  **No**