Harmony API Security

Introduction

The Harmony API Manager provides multiple settings to apply the desired level of security for each API (URL). Each setting is independent. Using a combination of independent settings allows the user to create specific levels of security for specific use cases.

Any API Is Anonymous and Publicly Accessible by Default

Any API is anonymous and publicly accessible by default at the time it is created, unless an appropriately configured security profile is assigned.

- At the API level, under Authentication, you can assign a profile to the API that specifies the method type used to authenticate a consumer and allow access to the API. If you do not assign a profile, the API authentication is set to anonymous by default, and anyone can access the API. Note that security profiles do get cached on the gateway, so changes to an already active API could take several minutes to take effect.

Multiple Profiles Assigned to an API

- Multiple Basic profiles within the same environment can be assigned to a single API to accommodate multiple users and credentials.
- To avoid conflicts between different types of authentication methods, do not assign a mix of different authentication types for a specific API or Proxy. These combinations are not allowed:
    - Cannot assign 1 Basic and 1 OAuth profile to a single API
    - Cannot assign 1 Basic and 1 Anonymous profile to a single API
    - Cannot assign 1 OAuth and 1 Anonymous profile to a single API
    - Cannot assign more than 1 OAuth profile per API
    - Cannot assign more than 1 Anonymous profile per API
    - Cannot assign the same profile more than once (no duplicates)
- Create a separate API or Proxy for serving different groups of API Consumers.

Multiple Profiles Available to an Environment

- A profile is only valid in the one environment it was set up in.
- Multiple profiles can be set up within an environment with different methods of authentication and different security options.
- A profile can be assigned to a single API or to multiple APIs that are set up within the same environment.

EXAMPLES:

Assume the classic configuration of one Development environment and one Production environment with 2 APIs.

- API-1 is intended for both the Finance and Accounting department consumers and API-2 is intended ONLY for the Accounting department consumers.
- Create one security profile for Accounting (with the desired security & governance configuration)
- Create another security profile for Finance (with the desired security & governance configuration)
- Assign both the Finance and Accounting profiles to API-1
- Assign ONLY the Accounting security profile to API-2

Once testing is completed in the Development environment, the projects and operations are deployed into the Production environment.

- Each API Security Profile (Finance & Accounting) must be created in the Production environment.
- Each API in the Development environment can be 'Cloned' and published to the Production environment.

NOTE: The name of each API and each profile can be the same as their counterparts in the Development environment for continuity and cross reference (as well as the versioning). However, the URL for each API will reference the Production environment, and will be a distinct and separate URL from the API in the Development environment.

On This Page

Related Articles

- API Logs
- Environments
- Security Profiles
- Configuring OAuth 2.0 with Google
- Configuring OAuth 2.0 with Okta
- Configuring OAuth 2.0 with Salesforce
- Security Profile Creation and Configuration
- Security Profiles

Related Topics

- Jitterbit Security

Last updated: Feb 20, 2020

Profile Authentication

An API security profile governs and secures the consumption of APIs. The security profiles allow for publishing an API or group of APIs to be consumed by a specific API consumer or a group of consumers. You can create and assign security profiles based on the organization's specific security and governance requirements. These are the available method types:

- Anonymous authentication allows access by anyone to consume the API. Additional security options are available under Logging, Rate Limits and Trusted IP Ranges to limit such access.
- Basic authentication provides a username and password within the profile. The same username and password must be entered to access the API at runtime. Additional security options are available under Logging, Rate Limits and Trusted IP Ranges.
    - If you need additional information on how to use HTTP header information or Basic Authentication, please refer to https://en.wikipedia.org/wiki/Basic_access_authentication.
- OAuth 2.0 using Google as the Identity Provider requires the consumer to validate their Google credentials to access the API at runtime.
    - Google requires a Client ID and a Client Secret to be set up within the security profile. The redirect URLs configured within the profile must also be copied into Google. See Configuring OAuth 2.0 with Google for detailed instructions.
- OAuth 2.0 using Salesforce as the Identity Provider requires the consumer to validate their Salesforce credentials to access the API at runtime.
    - Salesforce requires a Consumer Key and a Consumer Secret to be set up within the security profile. The redirect URLs configured within the profile must also be copied into the Connected App within Salesforce. See Configuring OAuth 2.0 with Salesforce for detailed instructions.
- OAuth 2.0 using Okta as the Identity Provider requires the consumer to validate their Okta credentials to access the API at runtime.
    - Okta requires a Client ID and Client Secret to be set up within the security profile. The redirect URLs configured within the profile must also be copied into the Web Application within Okta. See Configuring OAuth 2.0 with Okta for detailed instructions.

Logging/Auditing at Profile Level

- For every hit on the API, the profile used to access the API is recorded in a log. The log is available to view through API Logs.
    - This option records every hit as Anonymous in the log if the profile is set to Anonymous authentication.
    - This option records every hit in the log as the Username required by the profile, if the profile is set to Basic authentication. If the user fails to provide proper credentials, but Anonymous access was also enabled on the API, then Anonymous will be entered into the log.
    - This option records every hit in the log as OAuth2.0 if the profile is set to OAuth 2.0 authentication.
- Custom Request Header: To override the logging behavior above and audit using a value from the request header (i.e. in the case of a single application key being used), you can enter the name of the field the value of which will be recorded in the log.

Rate Limiting at Profile Level

- By default, a profile can access all assigned APIs up to the organization allowance for hits across all APIs within a minute. The organization allowance is stated in the Jitterbit license agreement. If the organization allowance is 10 hits per minute, only 10 hits within a minute will be allowed across all APIs.

EXAMPLES:

- The org allowance is 10 hits per minute. If the org has 10 APIs and each API receives 1 hit within a minute, the limit has been reached and additional hits to any API within the minute will be rejected.
- The org allowance is 10 hits per minute. If the org has 10 APIs and one API receives 10 hits within a minute, the limit has been reached and additional hits to any API within the minute will be rejected.
- The org allowance is 10 hits per minute. The org has 10 APIs. An authentication profile assigned to 1 API limits the number of hits to 5 per minute. If this API is accessed through that profile 5 times within the minute, any additional access to the API through that profile will be rejected. Only 5 hits are available across all of the remaining 9 APIs. If 5 of the remaining APIs receive 1 hit each, all 10 of the hits have been used and additional hits to any of the APIs within the minute will be rejected.
- The org allowance takes precedence over any limit set within a profile. The org allowance is 10 hits per minute. The org has 10 APIs. An authentication profile assigned to 1 API limits the number of hits to 5 per minute. If this API is accessed through that profile 2 times within the minute and 8 of the remaining APIs receive 1 hit each, all 10 of the hits have been used. Any additional hits to any of the APIs within the minute will be rejected.

Rate limiting at the profile level is enabled by checking the box in the Rate Limits section of the profile and selecting a number of hits in the Hits Per Minute field. This limit is per profile, not per organization, environment, or API.

- Rate Limiting enforces a maximum number of hits this particular profile can make against all assigned APIs during a period of one minute.
- When enabled, the system does additional checks on every hit (a request to a valid URL) in order to reject calls over the limit you have set. As such, all calls for this API will sustain additional performance overhead and the consumer may experience an increased number of rejects.
- Once the limit defined in the profile is reached, additional calls via the profile within the minute are rejected. Once the organization's allowance for hits per minute is reached, all calls to any API via any profile within the minute are rejected. Refer to the examples outlined below for additional information.
- If the defined rate per minute limit (at the profile, environment, or organization level) is reached, the API call is rejected by the API gateway and an Error 429 message is returned. The underlying operation is never called.
- Note that attempts against invalid URLs (i.e. Error 404) are not counted against any of the limits and allowances.
- Detailed instructions for setting up API rate limits are available in Security Profile Creation and Configuration and Environments. Review your Jitterbit license agreement for additional information about the organization allowance for hits across all APIs within a minute.

IP Range Restriction at Profile Level

- By default, the API and/or profile do not limit access to any set range of IP addresses.
- Access can be set to only a single IP or a range of IP addresses in the Trusted IP Ranges section of the profile.
  - Select the radio button labeled *"Trust requests only from the following IP ranges".*
  - Enter the Start IP Address and End IP Address in the appropriate boxes.
  - Click the *"+ Add IP Range*" link to add an additional range of IP addresses. Continue until all desired ranges have been set up.
- If a user tries to access your API via a profile that is limited to certain IP ranges, their IP will be checked against the allowed range(s). Access from any IP that is outside of the range(s) set up will be rejected.

Optional SSL Only Mode at the API Level

- By default every API supports both HTTP and HTTPS transfer.
- You can forward HTTP traffic to ensure all communication is encrypted by enabling SSL Only (click the checkbox) in the Settings section of the API.
  - The identity of the HTTPS URL is verified by Symantec Class 3 Secure Server SHA256 SSL CA.
  - The connection to the HTTPS URL is encrypted with modern cryptography (TLS 1.2 encryption, the connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism).