We are excited to announce the ability to configure fine-grained API security for your APIs on the Link API Gateway.

What is changing?

You have more options for securing your endpoints.

API Security

Healthcare APIs frequently face the data authorization challenge of accessing and sharing only the required data. Link API Gateway now supports the following security strategies:

- **Scope Permission** restricts access to your REST endpoint based on a specified scope or REST verb that applies to either a single resource or a collection of resources.
- **Parameter Restrictions** restrict access of a consumer based on static parameter-key value pair.
- **Authority Validation** restricts access to an endpoint based on dynamic simple or complex business rules by creating an API that the Link API Gateway can invoke to validate consumer's request.

Read our **documentation** for more details.

What do I need to do?

No changes are required. Applying additional fine-grained API security is optional. You can configure and enable them when you are ready.

What if I have more questions?

If our **documentation** doesn't answer your questions or you need further assistance, reach out to the Link API Gateway Tier 2 support group via Service-Now.

Visit us anytime at **Link News and Releases** for the most up-to-date information about Link.