Restricting Access to Anonymous Web APIs

Magento 2 allows some web APIs to be accessed by unauthenticated (anonymous) users. Many of these APIs allow a customer to have a robust shopping experience on the website without having to log in.

A subset of these APIs can return information about products, promotions, and storefronts that a merchant might consider proprietary. For example, Catalog module APIs can provide information about an item's pricing and quantity, as well as items that are currently not for sale. The CMS module could reveal information about upcoming promotional landing pages and coupons. The Store module can reveal too much information about individual websites.

For this reason, by default, Magento 2 now prevents anonymous users from accessing the APIs that could reveal sensitive information. When the feature is enabled, the user must have administrator privileges to execute the affected APIs.

The following table lists the APIs that are no longer available to an anonymous user by default:

Product	Module	API	Action
CE	Catalog	/V1/products	GET
CE	Catalog	/V1/products/:sku	GET
CE	Catalog	/V1/products/attributes/:attributeCode	GET
CE	Catalog	/V1/products/types	GET
CE	Catalog	/V1/products/attribute-sets/sets/list	GET
CE	Catalog	/V1/products/attribute-sets/:attributeSetId	GET
CE	Catalog	/V1/products/attribute-sets/:attributeSetId/attributes	GET

CE	Catalog	/V1/products/attribute-sets/groups/list	GET
CE	Catalog	/V1/products/attributes/:attributeCode/options	GET
CE	Catalog	/V1/products/media/types/:attributeSetName	GET
CE	Catalog	/V1/products/:sku/media/:entryId	GET
CE	Catalog	/V1/products/:sku/media	GET
CE	Catalog	/V1/products/:sku/group-prices/:customerGroupId/tiers	GET
CE	Catalog	/V1/categories/:categoryId	GET
CE	Catalog	/V1/categories	GET
CE	Catalog	/V1/products/:sku/options	GET
CE	Catalog	/V1/products/:sku/options/:optionId	GET
CE	Catalog	/V1/products/links/types	GET
CE	Catalog	/V1/products/links/:type/attributes	GET
CE	Catalog	/V1/products/:sku/links/:type	GET
CE	Catalog	/V1/categories/:categoryId/products	GET
CE	CatalogInventory	/V1/stockStatuses/:productSku	GET
CE	Cms	/V1/cmsPage/:pageId	GET
CE	Cms	/V1/cmsBlock/:blockId	GET
CE	ConfigurableProduct	/V1/configurable-products/:sku/children	GET
CE	ConfigurableProduct	/V1/configurable-products/:sku/options/:id	GET

CE	ConfigurableProduct	/V1/configurable-products/:sku/options/all	GET
CE	Store	/V1/store/storeViews	GET
CE	Store	/V1/store/storeGroups	GET
CE	Store	/V1/store/websites	GET
CE	Store	/V1/store/storeConfigs	GET

Important: Preventing anonymous access to these APIs could cause third-party integrations to fail. If a third-party integration calls any of these web APIs, it will receive an authentication error instead of the expected response. In this case, might need to disable this feature.

To disable this feature, log in to the Admin panel and navigate to **System > Configuration > Services > Magento Web API**. Then select **Yes** from the **Allow Anonymous Guest Access** menu.

If the list of APIs that are inaccessible to anonymous users must be updated for a third-party extension, an integrator can add to their extension's `di.xml` file to update or replace the functionality defined in the WebapiSecurity module.

The following APIs remain accessible to anonymous users. Most of these must remain accessible to support the checkout and add-to-cart Ajax functionalities.

Product	Module	API	Action
CE	Checkout	/V1/guest-carts/:cartId/shipping-information	POST
CE	Checkout	/V1/guest-carts/:cartId/totals-information	POST
CE	Checkout	/V1/guest-carts/:cartId/payment-information	POST
CE	Checkout	/V1/guest-carts/:cartId/payment-information	GET
CE	Checkout	/V1/guest-carts/:cartId/set-payment-information	POST
CE	Customer	/V1/customers	POST

CE	Customer	/V1/customers/:customerId/password/resetLinkToken/:resetPasswordLinkToken	GET
CE	Customer	/V1/customers/password	PUT
CE	Customer	/V1/customers/isEmailAvailable	POST
CE	Directory	/V1/directory/currency	GET
CE	Directory	/V1/directory/countries	GET
CE	Directory	/V1/directory/countries/:countryId	GET
CE	GiftMessage	/V1/guest-carts/:cartId/gift-message	GET
CE	GiftMessage	/V1/guest-carts/:cartId/gift-message/:itemId	GET
CE	GiftMessage	/V1/guest-carts/:cartId/gift-message	POST
CE	GiftMessage	/V1/guest-carts/:cartId/gift-message/:itemId	POST
CE	Integration	/V1/integration/admin/token	POST
CE	Integration	/V1/integration/customer/token	POST
CE	Quote	/V1/guest-carts/:cartId	GET
CE	Quote	/V1/guest-carts	POST
CE	Quote	/V1/guest-carts/:cartId	PUT
CE	Quote	/V1/guest-carts/:cartId/order	PUT
CE	Quote	/V1/guest-carts/:cartId/shipping-methods	GET
CE	Quote	/V1/guest-carts/:cartId/estimate-shipping-methods	POST
CE	Quote	/V1/guest-carts/:cartId/items	GET
CE	Quote	/V1/guest-carts/:cartId/items	POST
CE	Quote	/V1/guest-carts/:cartId/items/:itemId	PUT
CE	Quote	/V1/guest-carts/:cartId/items/:itemId	DELETE
CE	Quote	/V1/guest-carts/:cartId/selected-payment-method	GET
CE	Quote	/V1/guest-carts/:cartId/selected-payment-method	PUT

CE	Quote	/V1/guest-carts/:cartId/payment-methods	GET
CE	Quote	/V1/guest-carts/:cartId/billing-address	GET
CE	Quote	/V1/guest-carts/:cartId/billing-address	POST
CE	Quote	/V1/guest-carts/:cartId/coupons	GET
CE	Quote	/V1/guest-carts/:cartId/coupons/:couponCode	PUT
CE	Quote	/V1/guest-carts/:cartId/coupons	DELETE
CE	Quote	/V1/guest-carts/:cartId/collect-totals	PUT
CE	Quote	/V1/guest-carts/:cartId/totals	GET
CE	Search	/V1/search	GET
EE	GiftCardAccount	/V1/carts/guest-carts/:cartId/giftCards/:giftCardCode	DELETE
EE	GiftCardAccount	/V1/carts/guest-carts/:cartId/giftCards	POST
EE	GiftCardAccount	/V1/carts/guest-carts/:cartId/checkGiftCard/:giftCardCode	GET
EE	GiftRegistry	/V1/guest-giftregistry/:cartId/estimate-shipping-methods	POST