Configurable Token Lifetimes - Microsoft identity platform

By cilwerner

Archived: 2026-04-05 17:56:50 UTC

You can configure the lifetime of access, ID, or Security Assertion Markup Language (SAML) tokens issued by the Microsoft identity platform. Token lifetimes can be set for all apps in your organization, multitenant applications, or specific service principals. Configuring token lifetimes for managed identity service principals isn't supported.

In Microsoft Entra ID, policies define rules applied to individual applications or all applications in an organization. Each policy type has unique properties that determine how it is enforced on the object to which it's assigned.

A policy can be designated as the default for your organization, applying to all applications unless overridden by a higher-priority policy. Policies can also be assigned to specific applications, with priority varying by policy type.

For practical guidance, see examples of how to configure token lifetimes.

Note

Configurable token lifetime policy only applies to mobile and desktop clients that access SharePoint Online and OneDrive for Business resources, and doesn't apply to web browser sessions. To manage the lifetime of web browser sessions for SharePoint Online and OneDrive for Business, use the Conditional Access session lifetime feature. Refer to the SharePoint Online blog to learn more about configuring idle session time-outs.

Note

You might want to increase the token lifetime so that a script runs for more than an hour. Many Microsoft libraries, such as Microsoft Graph PowerShell SDK, extend the token lifetime as needed and you don't need to makes changes to the access token policy.

Note

Configurable token lifetime policy is not supported for applications developed for personal Microsoft accounts (where `signInAudience` is set to `AzureADandPersonalMicrosoftAccount` or `PersonalMicrosoftAccount`).

License requirements

Using this feature requires a Microsoft Entra ID P1 license. To find the right license for your requirements, see Comparing generally available features of the Free and Premium editions.

Customers with Microsoft 365 Business licenses also have access to Conditional Access features.

Token lifetime policies for access, SAML, and ID tokens

You can set token lifetime policies for access tokens, SAML tokens, and ID tokens.

Access tokens

Clients use access tokens to access a protected resource. An access token can be used only for a specific combination of user, client, and resource. Access tokens can't be revoked and are valid until their expiry. A malicious actor that obtains an access token can use it for extent of its lifetime. Adjusting the lifetime of an access token is a trade-off between improving system performance and increasing the amount of time that the client retains access after the user's account is disabled. Improved system performance is achieved by reducing the number of times a client needs to acquire a fresh access token.

The default lifetime of an access token is variable. When issued, an access token's default lifetime is assigned a random value ranging between 60-90 minutes (75 minutes on average). The default lifetime also varies depending on the client application requesting the token or if Conditional Access is enabled in the tenant. For more information, see Access token lifetime.

SAML tokens

SAML tokens are used by many web-based SaaS applications, and are obtained using Microsoft Entra ID's SAML2 protocol endpoint. They're also consumed by applications using WS-Federation. The default lifetime of the token is 1 hour. From an application's perspective, the validity period of the token is specified by the NotOnOrAfter value of the `<conditions ···>` element in the token. After the validity period of the token has ended, the client must initiate a new authentication request, which will often be satisfied without interactive sign in as a result of the Single Sign On (SSO) Session token.

The value of NotOnOrAfter can be changed using the `AccessTokenLifetime` parameter in a `TokenLifetimePolicy`. It will be set to the lifetime configured in the policy if any, plus a clock skew factor of five minutes.

The subject confirmation NotOnOrAfter specified in the `<SubjectConfirmationData>` element is not affected by the Token Lifetime configuration.

ID tokens

ID tokens are passed to websites and native clients. ID tokens contain profile information about a user. An ID token is bound to a specific combination of user and client. ID tokens are considered valid until their expiry. Usually, a web application matches a user's session lifetime in the application to the lifetime of the ID token issued for the user. You can adjust the lifetime of an ID token to control how often the web application expires the application session, and how often it requires the user to be reauthenticated with the Microsoft identity platform (either silently or interactively).

Token lifetime policies for refresh tokens and session tokens

You can't set token lifetime policies for refresh tokens and session tokens. For lifetime, time-out, and revocation information on refresh tokens, see Refresh tokens.

Important

As of January 30, 2021 you can't configure refresh and session token lifetimes. Microsoft Entra no longer honors refresh and session token configuration in existing policies. New tokens issued are set to the default configuration. You can still configure access, SAML, and ID token lifetimes after the refresh and session token configuration retirement.

Existing token's lifetime won't be changed. After they expire, a new token will be issued based on the default value.

If you need to continue to define the time period before a user is asked to sign in again, configure sign-in frequency in Conditional Access. To learn more about Conditional Access, read Configure authentication session management with Conditional Access.

Configurable token lifetime properties

A token lifetime policy is a type of policy object that contains token lifetime rules. This policy controls how long access, SAML, and ID tokens for this resource are considered valid. Token lifetime policies can't be set for refresh and session tokens. If no policy is set, the system enforces the default lifetime value.

Access, ID, and SAML2 token lifetime policy properties

Reducing the Access Token Lifetime property mitigates the risk of an access token or ID token being used by a malicious actor for an extended period of time. (These tokens can't be revoked.) The trade-off is that performance is adversely affected, because the tokens have to be replaced more often.

For an example, see Create a policy for web sign-in.

Access, ID, and SAML2 token configuration are affected by the following properties and their respectively set values:

- **Property**: Access Token Lifetime
- **Policy property string**: AccessTokenLifetime
- **Affects**: Access tokens, ID tokens, SAML2 tokens
- **Default**:
    - Access tokens: varies, depending on the client application requesting the token. For example, continuous access evaluation (CAE) capable clients that negotiate CAE-aware sessions will see a long lived token lifetime (up to 28 hours).
    - ID tokens, SAML2 tokens: One hour
- **Minimum**: 10 minutes
- **Maximum**: One day

Refresh and session token lifetime policy properties

Refresh and session token configuration are affected by the following properties and their respectively set values. After the retirement of refresh and session token configuration on January 30, 2021, Microsoft Entra ID will only honor the default values described below. If you decide not to use Conditional Access to manage sign-in frequency, your refresh and session tokens are set to the default configuration on that date and can't change their lifetimes.

Property	Policy property string	Affects	Default
Refresh Token Max Inactive Time	MaxInactiveTime	Refresh tokens	90 days
Single-Factor Refresh Token Max Age	MaxAgeSingleFactor	Refresh tokens (for any users)	Until-revoked
Multi-Factor Refresh Token Max Age	MaxAgeMultiFactor	Refresh tokens (for any users)	Until-revoked
Single-Factor Session Token Max Age	MaxAgeSessionSingleFactor	Session tokens (persistent and non-persistent)	Until-revoked
Multi-Factor Session Token Max Age	MaxAgeSessionMultiFactor	Session tokens (persistent and non-persistent)	Until-revoked

Non-persistent session tokens have a Max Inactive Time of 24 hours whereas persistent session tokens have a Max Inactive Time of 90 days. Anytime the SSO session token is used within its validity period, the validity period is extended another 24 hours or 90 days. If the SSO session token isn't used within its Max Inactive Time period, it's considered expired and are no longer accepted. Any changes to this default period should be changed using Conditional Access.

You can use PowerShell to find the policies that will be affected by the retirement. Use the PowerShell cmdlets to see the all policies created in your organization, or to find which apps are linked to a specific policy.

Policy evaluation and prioritization

You can create and then assign a token lifetime policy to a specific application and to your organization. Multiple policies might apply to a specific application. The token lifetime policy that takes effect follows these rules:

- If a policy is explicitly assigned to the organization, it's enforced.
- If no policy is explicitly assigned to the organization, the policy assigned to the application is enforced.
- If no policy has been assigned to the organization or the application object, the default values are enforced. (See the table in Configurable token lifetime properties.)

A token's validity is evaluated at the time the token is used. The policy with the highest priority on the application that is being accessed takes effect.

All timespans used here are formatted according to the C# TimeSpan object - D.HH:MM:SS. So 80 days and 30 minutes would be `80.00:30:00`. The leading D can be dropped if zero, so 90 minutes would be `00:90:00`.

REST API reference

You can configure token lifetime policies and assign them to apps using Microsoft Graph. For more information, see the `tokenLifetimePolicy` resource type and its associated methods.

Cmdlet reference

These are the cmdlets in the Microsoft Graph PowerShell SDK.

Manage policies

You can use the following commands to manage policies.

Application policies

You can use the following cmdlets for application policies.

Next steps

To learn more, read examples of how to configure token lifetimes.
