How Token Protection Enhances Conditional Access Policies - Microsoft Entra ID

By kenwith

Archived: 2026-04-06 01:49:46 UTC

In this article

Token Protection is a Conditional Access session control that attempts to reduce token replay attacks by ensuring only device bound sign-in session tokens, like Primary Refresh Tokens (PRTs), are accepted by Microsoft Entra ID when applications request access to protected resources.

When a user registers a supported device with Microsoft Entra, a PRT is issued and cryptographically bound to that device. This binding ensures that even if a threat actor steals the token, it can't be used from another device. With Token Protection enforced, Microsoft Entra validates that only these bound sign-in session tokens are used by supported applications.

Platform	Status
Windows	Generally Available
iOS / iPadOS	Preview
macOS	Preview

Note

Token Protection currently supports native applications only. Browser-based applications are not supported.

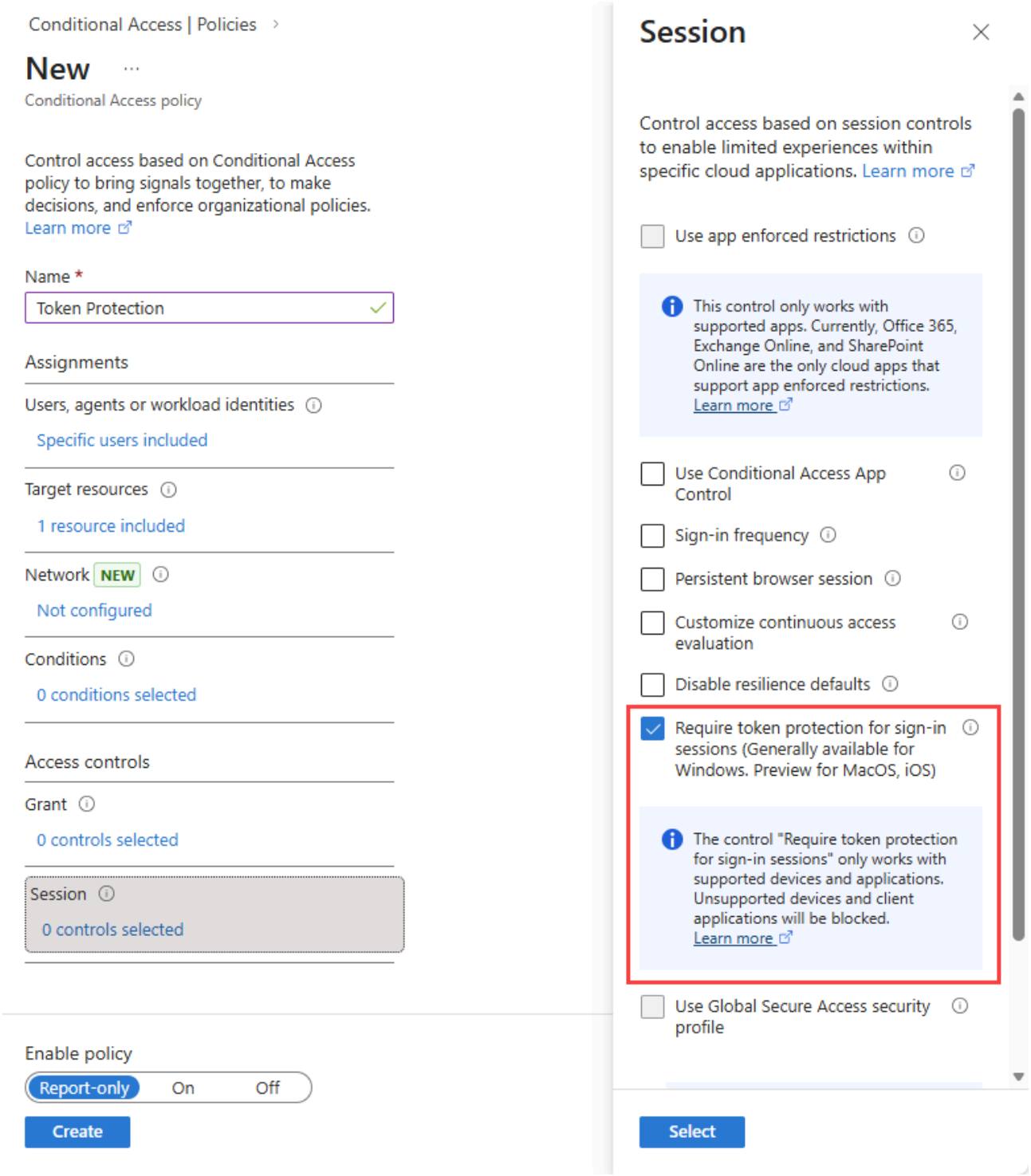
Token Protection policy can be enforced on the following cloud resources:

- Exchange Online
- SharePoint Online
- Microsoft Teams

On Windows, enforcement is also supported for:

- Azure Virtual Desktop

- Windows 365



Windows:

- Windows 10 or newer devices that are Microsoft Entra joined, Microsoft Entra hybrid joined, or Microsoft Entra registered. See the known limitations section in the appropriate deployment guide for unsupported device types.
- Windows Server 2019 or newer that are hybrid Microsoft Entra joined.

- For detailed steps on how to register your device, see Register your personal device on your work or school network.

Apple (Preview):

- macOS 14.0 or later. Requires the Microsoft Enterprise single sign-on (SSO) plug-in. Alternatively, you can also use Platform SSO. Only MDM-managed devices are supported.
- iOS / iPadOS 16.0 or later. Requires the Microsoft Enterprise SSO plug-in. Only MDM-managed devices are supported.
- For detailed steps on how to set up, see Enabling Microsoft Enterprise SSO plug-in and configuring Platform SSO for macOS.

To minimize the likelihood of user disruption due to app or device incompatibility, follow these recommendations:

- Start with a pilot group of users and expand over time.
- Create a Conditional Access policy in report-only mode before enforcing token protection.
- Capture both interactive and non-interactive sign-in logs.
- Analyze these logs long enough to cover normal application use.
- Add known, reliable users to an enforcement policy.

This process helps assess your users' client and app compatibility for token protection enforcement.

Select the guide for your target platform:

- **Windows**: Token Protection deployment guide - Windows
- **iOS, iPadOS, and macOS**: Token Protection deployment guide - Apple

What is a Primary Refresh Token?

Additional resources

Training

- Last updated on 03/24/2026
