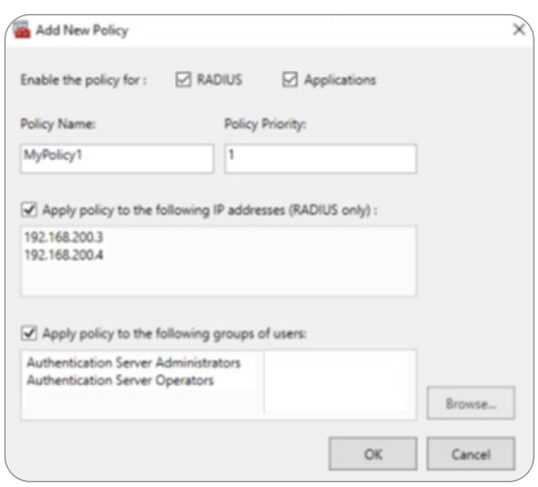
intercede

MyID MFA PSM

What's new in MyID MFA & PSM v5.2

Access Control Policies:

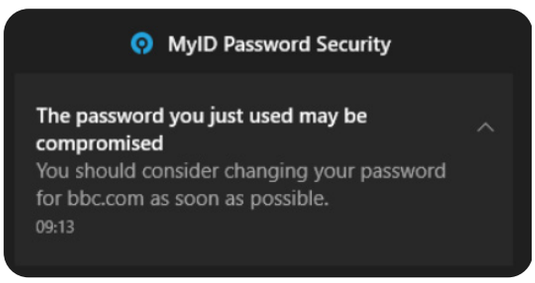
You can now apply access control policies at an application level via the new Access Control tab. This enables you to configure your applications with different authentication options, including RADIUS, for different policies. This gives administrators greater granular control over how your users access your applications.



Breach Password Detection for Browser-Based Applications:

The MyID Windows Desktop Agent now has an optional Edge or Chrome browser extension that allows you to check the security of external passwords. It detects when you use a password in your browser and performs a known breached password check against the password.

If you use a known breached password in your browser, the extension triggers a Windows notification on your client PC, advising you to change your password, and an event log on the authentication server.



Administrators can use charts on the Password Security dashboard and a new report to track the use of breached passwords, making sure that you are aware of any security concerns; you can also configure domain whitelists to streamline your reporting.

This extends the power of the Password Breach database beyond the Active Directory password to protect a wide range of passwords used within an organisation.

New MyID Authenticator App

With MyID MFA 5.2, we have launched a new version of the MyID Authenticator App featuring a modern UI redesign, making the app easier and more intuitive to use. This version also includes German and Arabic language support, extending the audience for the app by allowing your users to work in their native language.

Access Token Lifetimes

You now have greater control over how long your users can stay authenticated before having to carry out authentication again. You can also manually revoke authentication for one or more users (for example, if you believe that they have not logged out of their session on an insecure machine), forcing them to authenticate again without waiting for their authentication to expire.

intercede

MyID MFA PSM

YubiKey Enhancements

You can now add YubiKey devices to a user's account from the user's Properties dialog box. The YubiKey Wizard walks you through the process, making it quick and easy to add a YubiKey device for a user.

Auditor Role

You can grant users read-only access to the Web Management Portal with the new Auditors role. This allows auditors to view dashboards, reports, and individual users' settings, but does not allow them to change user settings.

Windows Server 2025

You can now install the MyID Authentication Server on Microsoft Windows Server 2025.

Server Logging

The logging for the MyID Authentication Server has been streamlined to remove unnecessary duplication, reducing the frequency of log entries and the size of log files to make the logs easier to interpret. As part of this improvement, logging is now enabled by default for the MyID Authentication Server.

Claims Mapping

You can now set up claims mapping for OpenID Connect applications between attributes and either User or LDAP attributes, extending the integration functionality with external applications.

MFA OTP Improvements

You can now select multiple multi-factor authentication token delivery methods at the same time. Users can always get their multi-factor authentication tokens from the MyID Authenticator app and can also get tokens through emails and text messages, depending on the available technologies.

Web Management Portal

The Web Management Portal has been enhanced to allow you to edit device names, and to disable the ability for administrators and operators to change user passwords, making the Web Management Portal more convenient to use, and more secure.

Grid Pattern Improvements

The default policies for both grid patterns and account lockout policies have been improved to increase security. The default grid pattern policy is now for a complex grid, and the minimum length has been increased. The account lockout policies for lockout duration, lockout threshold, and lockout reset have all been made more secure by default.

Group Policy Improvements

The group policies have been updated to provide information about license-dependent features to make it clear which policies apply to MFA and which to PSM, making it easy to see which policies apply to your system.

General Improvements

The Reset Password link is now shown whenever a Password textbox is displayed, regardless of the Passwordless GPO setting.