Secure your Microsoft Entra identity infrastructure - Microsoft Entra ID

By martincoetzer

Archived: 2026-04-05 15:07:01 UTC

If you're reading this document, you're aware of the significance of security. You likely already carry the responsibility for securing your organization. If you need to convince others of the importance of security, send them to read the latest Microsoft Digital Defense Report.

This document helps you get a more secure posture using the capabilities of Microsoft Entra ID by using a five-step checklist to improve your organization's protection against cyber-attacks.

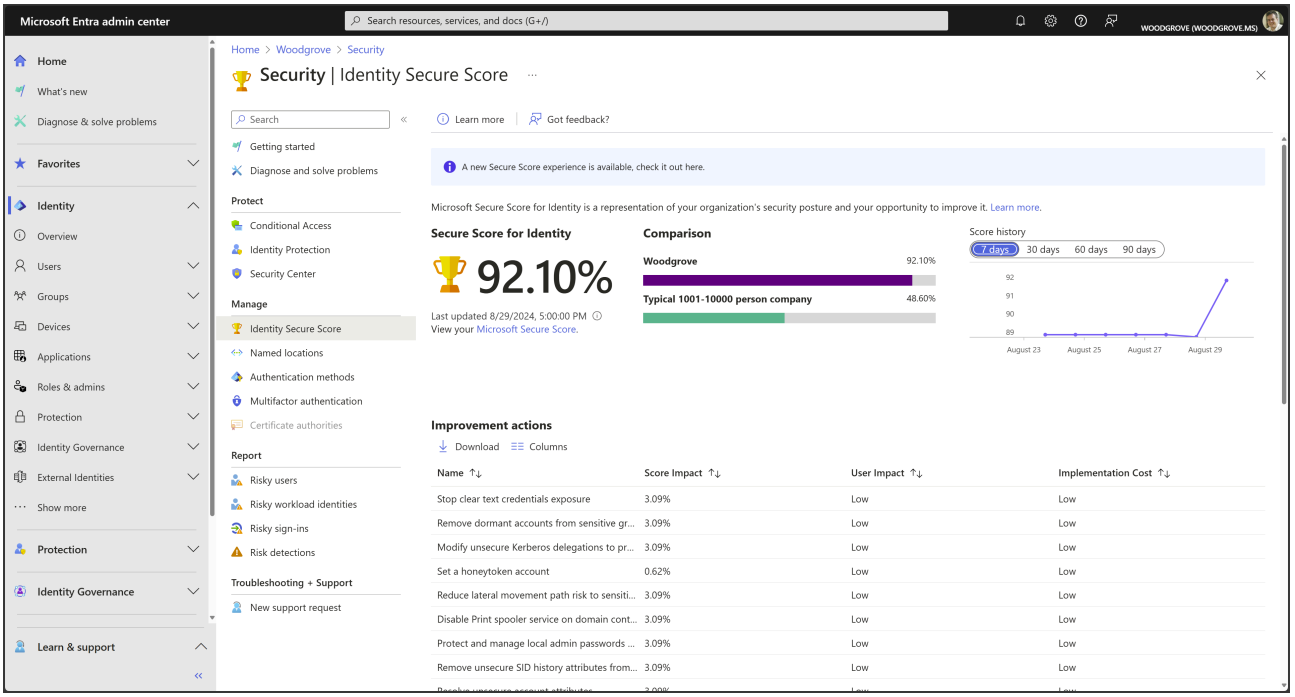
This checklist helps you quickly deploy critical recommended actions to protect your organization immediately by explaining how to:

- Strengthen your credentials
- Reduce your attack surface area
- Automate threat response
- Utilize cloud intelligence
- Enable end-user self-service

Note

Many of the recommendations in this document apply only to applications that are configured to use Microsoft Entra ID as their identity provider. Configuring apps for Single Sign-On assures the benefits of credential policies, threat detection, auditing, logging, and other features add to those applications. Microsoft Entra Application Management is the foundation on which all these recommendations are based.

The recommendations in this document are aligned with the Identity Secure Score, an automated assessment of your Microsoft Entra tenant’s identity security configuration. Organizations can use the Identity Secure Score page in the Microsoft Entra admin center to find gaps in their current security configuration to ensure they follow current Microsoft best practices for security. Implementing each recommendation in the Secure Score page increases your score and allow you to track your progress, plus help you compare your implementation against other similar size organizations.



Before you begin: Protect privileged accounts with MFA

Before you begin this checklist, make sure you don't get compromised while you're reading this checklist. In Microsoft Entra we observe 50 million password attacks daily, yet only a fraction of users and administrators are using strong authentications such as multifactor authentication (MFA). These statistics are based on data as of August 2021. In Microsoft Entra ID, users who have privileged roles, such as administrators, are the root of trust to build and manage the rest of the environment. Implement the following practices to minimize the effects of a compromise.

Attackers who get control of privileged accounts can do tremendous damage, so it's critical to protect these accounts before proceeding. Enable and require Microsoft Entra multifactor authentication (MFA) for all administrators in your organization using Microsoft Entra Security Defaults or Conditional Access. It's critical.

All set? Let's get started on the checklist.

Step 1: Strengthen your credentials

Although other types of attacks are emerging, including consent phishing and attacks on nonhuman identities, password-based attacks on user identities are still the most prevalent vector of identity compromise. Well-established spear phishing and password spray campaigns by adversaries continue to be successful against organizations that don't implement multifactor authentication (MFA) or other protections against this common tactic.

As an organization you need to make sure that your identities are validated and secured with MFA everywhere. In 2020, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) Report identified phishing as the top crime type for victim complaints. The number of reports doubled compared to the previous year. Phishing poses a significant threat to both businesses and individuals, and credential phishing was used in many of

the most damaging attacks last year. Microsoft Entra multifactor authentication (MFA) helps safeguard access to data and applications, providing another layer of security by using a second form of authentication. Organizations can enable multifactor authentication with Conditional Access to make the solution fit their specific needs. Take a look at this deployment guide to see how you how to plan, implement, and roll-out Microsoft Entra multifactor authentication.

Make sure your organization uses strong authentication

To easily enable the basic level of identity security, you can use the one-select enablement with Microsoft Entra security defaults. Security defaults enforce Microsoft Entra multifactor authentication for all users in a tenant and blocks sign-ins from legacy protocols tenant-wide.

If your organization has Microsoft Entra ID P1 or P2 licenses, then you can also use the Conditional Access insights and reporting workbook to help you discover gaps in your configuration and coverage. From these recommendations, you can easily close this gap by creating a policy using the new Conditional Access templates experience. Conditional Access templates are designed to provide an easy method to deploy new policies that align with Microsoft recommended best practices, making it easy to deploy common policies to protect your identities and devices.

Start banning commonly attacked passwords and turn off traditional complexity, and expiration rules.

Many organizations use traditional complexity and password expiration rules. Microsoft's research shows, and National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Identity Guidelines state, that these policies cause users to choose passwords that are easier to guess. We recommend you use Microsoft Entra password protection a dynamic banned password feature using current attacker behavior to prevent users from setting passwords that can easily be guessed. This capability is always on when users are created in the cloud, but is now also available for hybrid organizations when they deploy Microsoft Entra password protection for Windows Server Active Directory. In addition, we recommend you remove expiration policies. Password change offers no containment benefits as cyber criminals almost always use credentials as soon as they compromise them. Refer to the following article to Set the password expiration policy for your organization.

Protect against leaked credentials and add resilience against outages

The simplest and recommended method for enabling cloud authentication for on-premises directory objects in Microsoft Entra ID is to enable password hash synchronization (PHS). If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync for the following two reasons:

- The Users with leaked credentials report in Microsoft Entra ID warns of publicly exposed username and password pairs. An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and tells you,

in this report, if they match credentials in your organization – but only if you enable password hash sync or have cloud-only identities.
- If an on-premises outage happens, like a ransomware attack, you can switch over to using cloud authentication using password hash sync. This backup authentication method allows you to continue accessing apps configured for authentication with Microsoft Entra ID, including Microsoft 365. In this case, IT staff doesn't need to resort to shadow IT or personal email accounts to share data until the on-premises outage is resolved.

Passwords are never stored in clear text or encrypted with a reversible algorithm in Microsoft Entra ID. For more information on the actual process of password hash synchronization, see Detailed description of how password hash synchronization works.

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive. Organizations, which configure applications to authenticate directly to Microsoft Entra ID benefit from Microsoft Entra smart lockout. Federated deployments that use AD FS 2016 and AD FS 2019 can enable similar benefits using AD FS Extranet Lockout and Extranet Smart Lockout.

Step 2: Reduce your attack surface area

Given the pervasiveness of password compromise, minimizing the attack surface in your organization is critical. Disable the use of older, less secure protocols, limit access entry points, moving to cloud authentication, exercise more significant control of administrative access to resources, and embrace Zero Trust security principles.

Use Cloud Authentication

Credentials are a primary attack vector. The practices in this blog can reduce the attack surface by using cloud authentication, deploy MFA, and use passwordless authentication methods. You can deploy passwordless methods such as Windows Hello for Business, Phone Sign-in with the Microsoft Authenticator App or FIDO.

Block legacy authentication

Apps using their own legacy methods to authenticate with Microsoft Entra ID and access company data, pose another risk for organizations. Examples of apps using legacy authentication are POP3, IMAP4, or SMTP clients. Legacy authentication apps authenticate on behalf of the user and prevent Microsoft Entra ID from doing advanced security evaluations. The alternative, modern authentication, reduces your security risk, because it supports multifactor authentication and Conditional Access.

We recommend the following actions:

1. Discover legacy authentication in your organization with Microsoft Entra sign-in logs and Log Analytics workbooks.
2. Setup SharePoint Online and Exchange Online to use modern authentication.

3. If you have Microsoft Entra ID P1 or P2 licenses, use Conditional Access policies to block legacy authentication. For Microsoft Entra ID Free tier, use Microsoft Entra Security Defaults.
4. Block legacy authentication if you use AD FS.
5. Block Legacy Authentication with Exchange Server 2019.
6. Disable legacy authentication in Exchange Online.

For more information, see the article Blocking legacy authentication protocols in Microsoft Entra ID.

Block invalid authentication entry points

Using the *verify explicitly principle*, you should reduce the impact of compromised user credentials when they happen. For each app in your environment, consider the valid use cases: which groups, which networks, which devices and other elements are authorized – then block the rest. With Microsoft Entra Conditional Access, you can control how authorized users access their apps and resources based on specific conditions you define.

For more information on how to use Conditional Access for your Cloud Apps and user actions, see Conditional Access Cloud apps, actions, and authentication context.

Review and govern admin roles

Another Zero Trust pillar is the need to minimize the likelihood a compromised account can operate with a privileged role. This control can be accomplished by assigning the least amount of privilege to an identity. If you're new to Microsoft Entra roles, this article helps you understand Microsoft Entra roles.

Privileged roles in Microsoft Entra ID should be cloud only accounts in order to isolate them from any on-premises environments and don't use on-premises password vaults to store the credentials.

Implement Privilege Access Management

Privileged Identity Management (PIM) provides a time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions to important resources. These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Microsoft Entra Privileged Identity Management (PIM) helps you minimize account privileges by helping you:

- Identify and manage users assigned to administrative roles.
- Understand unused or excessive privilege roles you should remove.
- Establish rules to make sure privileged roles are protected by multifactor authentication.
- Establish rules to make sure privileged roles are granted only long enough to accomplish the privileged task.

Enable Microsoft Entra PIM, then view the users who are assigned administrative roles and remove unnecessary accounts in those roles. For remaining privileged users, move them from permanent to eligible. Finally, establish appropriate policies to make sure when they need to gain access to those privileged roles, they can do so securely, with the necessary change control.

Microsoft Entra built-in and custom roles operate on concepts similar to roles found in the role-based access control system for Azure resources (Azure roles). The difference between these two role-based access control systems is:

- Microsoft Entra roles control access to Microsoft Entra resources such as users, groups, and applications using the Microsoft Graph API
- Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management

Both systems contain similarly used role definitions and role assignments. However, Microsoft Entra role permissions can't be used in Azure custom roles and vice versa. As part of deploying your privileged account process, follow the best practice to create at least two emergency accounts to make sure you still have access to Microsoft Entra ID if you lock yourself out.

For more information, see the article Plan a Privileged Identity Management deployment and securing privileged access.

Restrict user consent operations

It’s important to understand the various Microsoft Entra application consent experiences, the types of permissions and consent, and their implications on your organization’s security posture. While allowing users to consent by themselves does allow users to easily acquire useful applications that integrate with Microsoft 365, Azure, and other services, it can represent a risk if not used and monitored carefully.

Microsoft recommends restricting user consent to allow end-user consent only for apps from verified publishers and only for permissions you select. If end-user consent is restricted, previous consent grants will still be honored but all future consent operations that an administrator must perform. For restricted cases, users can request admin consent through an integrated admin consent request workflow or through your own support processes. Before restricting end-user consent, use our recommendations to plan this change in your organization. For applications you wish to allow all users to access, consider granting consent on behalf of all users, making sure users who didn't yet individually consent can access the app. If you don’t want these applications to be available to all users in all scenarios, use application assignment and Conditional Access to restrict user access to specific apps.

Make sure users can request admin approval for new applications to reduce user friction, minimize support volume, and prevent users from signing up for applications using non-Microsoft Entra credentials. Once you regulate your consent operations, administrators should audit app and consent permissions regularly.

For more information, see the article Microsoft Entra consent framework.

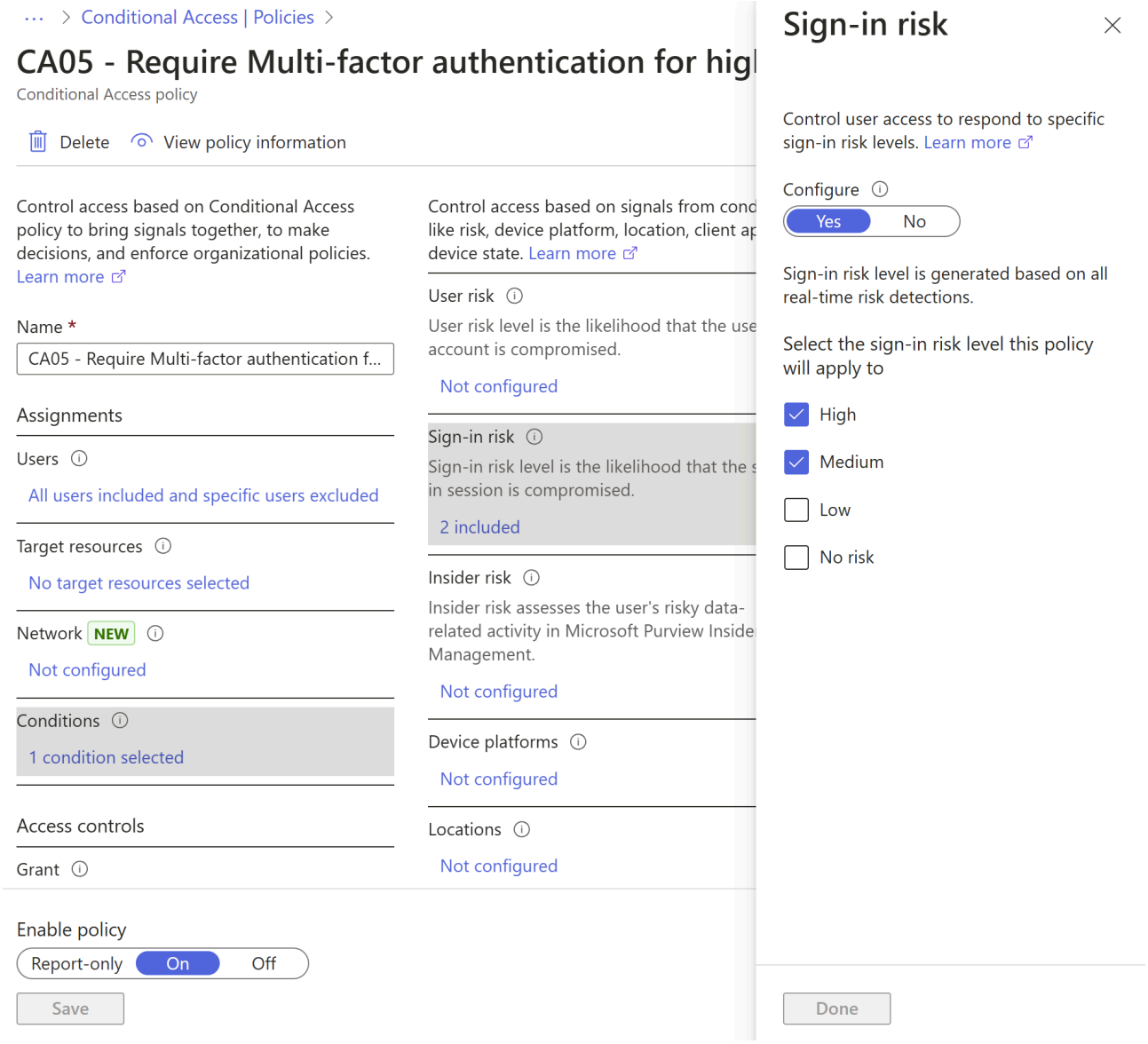
Step 3: Automate threat response

Microsoft Entra ID has many capabilities that automatically intercept attacks, to remove the latency between detection and response. You can reduce the costs and risks, when you reduce the time criminals use to embed themselves into your environment. Here are the concrete steps you can take.

For more information, see the article How To: Configure and enable risk policies.

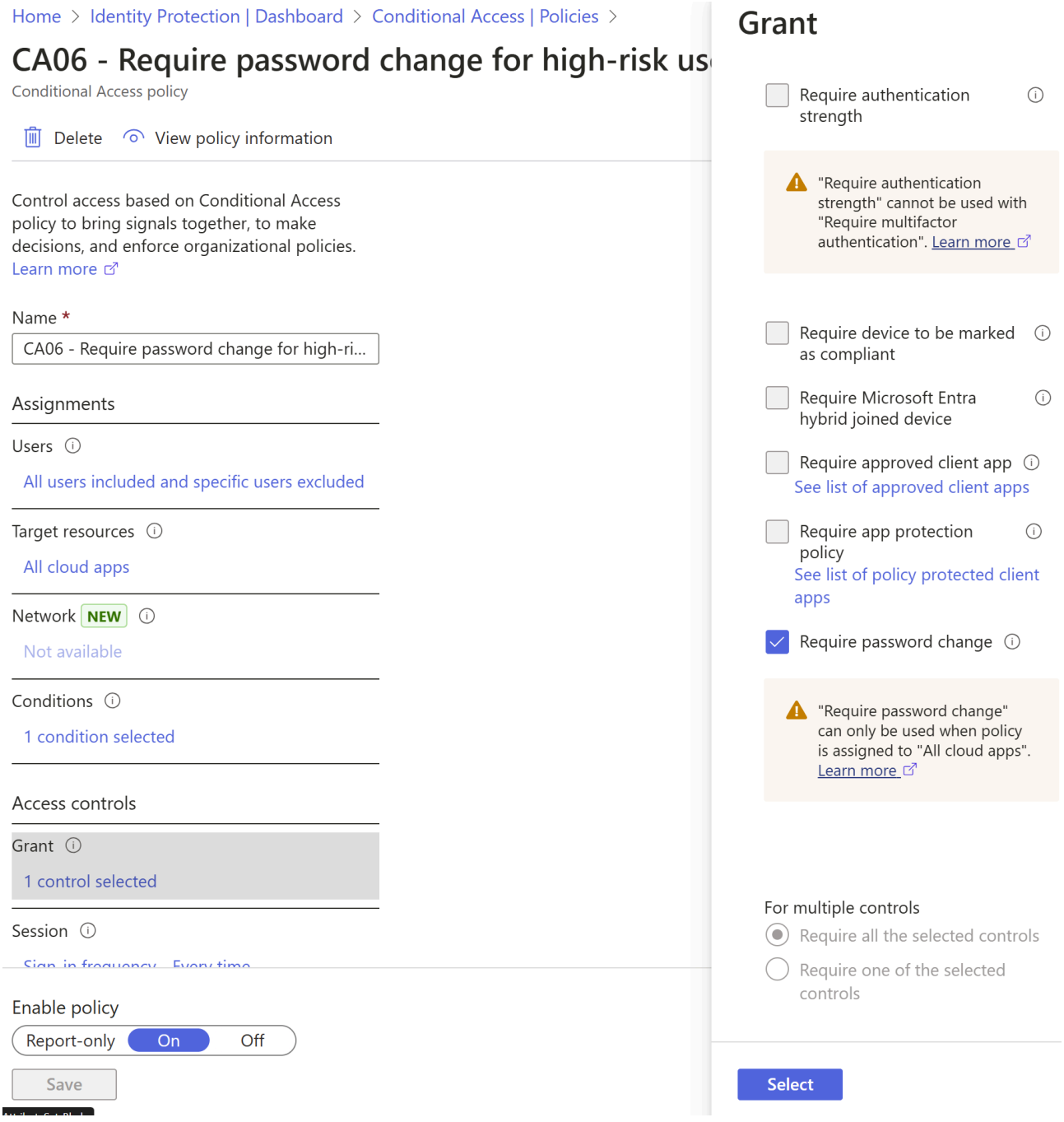
Implement sign-in risk policy

A sign-in risk represents the probability that a given that the identity owner didn't authorize the authentication request. A sign-in risk-based policy can be implemented through adding a sign-in risk condition to your Conditional Access policies that evaluates the risk level to a specific user or group. Based on the risk level (high/medium/low), a policy can be configured to block access or force multifactor authentication. We recommend that you force multifactor authentication on Medium or above risky sign-ins.



Implement user risk security policy

User risk indicates the likelihood of user identity compromise and is calculated based on the user risk detections that are associated with a user's identity. A user risk-based policy can be implemented through adding a user risk condition to your Conditional Access policies that evaluates the risk level to a specific user. Based on Low, Medium, High risk-level, a policy can be configured to block access or require a secure password change using multifactor authentication. Microsoft's recommendation is to require a secure password change for users on high risk.



Included in the user risk detection is a check whether the user's credentials match to credentials leaked by cybercriminals. To function optimally, it’s important to implement password hash synchronization with Microsoft Entra Connect Sync.

Integrate Microsoft Defender XDR with Microsoft Entra ID Protection

For Identity Protection to be able to perform the best risk detection possible, it needs to get as many signals as possible. It’s therefore important to integrate the complete suite of Microsoft Defender XDR services:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Identity

- Microsoft Defender for Cloud Apps

Learn more about Microsoft Threat Protection and the importance of integrating different domains, in the following short video.

Set up monitoring and alerting

Monitoring and auditing your logs is important to detect suspicious behavior. The Azure portal has several ways to integrate Microsoft Entra logs with other tools, like Microsoft Sentinel, Azure Monitor, and other SIEM tools. For more information, see the Microsoft Entra security operations guide.

Step 4: Utilize cloud intelligence

Auditing and logging of security-related events and related alerts are essential components of an efficient protection strategy. Security logs and reports provide you with an electronic record of suspicious activities and help you detect patterns that might indicate attempted or successful external penetration of the network, and internal attacks. You can use auditing to monitor user activity, document regulatory compliance, do forensic analysis, and more. Alerts provide notifications of security events. Make sure you have a log retention policy in place for both your sign-in logs and audit logs for Microsoft Entra ID by exporting into Azure Monitor or a SIEM tool.

Monitor Microsoft Entra ID

Microsoft Azure services and features provide you with configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms and address those gaps to help prevent breaches. You can use Azure Logging and Auditing and use Audit activity reports in the Microsoft Entra admin center. See the Microsoft Entra Security Operations guide for more details on monitoring user accounts, Privileged accounts, apps, and devices.

Monitor Microsoft Entra Connect Health in hybrid environments

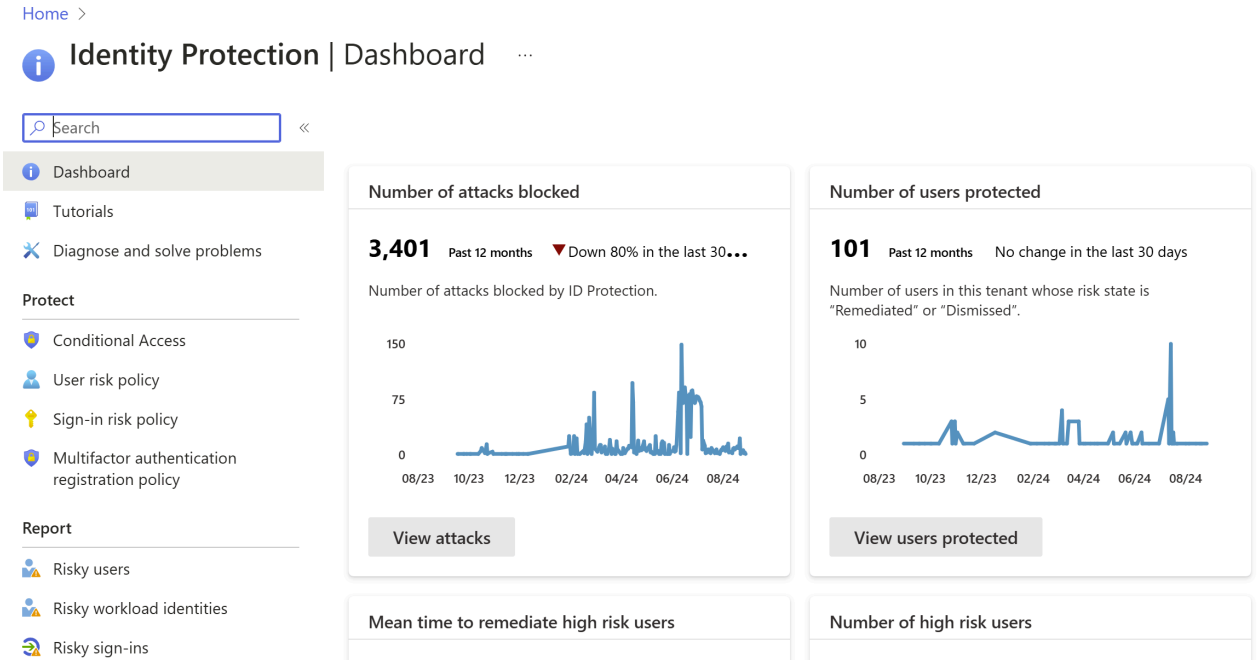
Monitoring AD FS with Microsoft Entra Connect Health provides you with greater insight into potential issues and visibility of attacks on your AD FS infrastructure. You can now view ADFS sign-ins to give greater depth for your monitoring. Microsoft Entra Connect Health delivers alerts with details, resolution steps, and links to related documentation; usage analytics for several metrics related to authentication traffic; performance monitoring and reports. Utilize the Risky IP WorkBook for ADFS that can help identify the norm for your environment and alert when there's a change. All Hybrid Infrastructure should be monitored as a Tier 0 asset. Detailed monitoring guidance for these assets can be found in the Security Operations guide for Infrastructure.

Monitor Microsoft Entra ID Protection events

Microsoft Entra ID Protection provides two important reports you should monitor daily:

1. Risky sign-in reports surface user sign-in activities you should investigate whether the legitimate owner performed the sign-in.

2. Risky user reports surface user accounts that might be compromised, such as leaked credential that was detected or the user signed in from different locations, causing an impossible travel event.



Audit apps and consented permissions

Users can be tricked into navigating to a compromised web site or apps that gain access to their profile information and user data, such as their email. A malicious actor can use the consented permissions it received to encrypt their mailbox content and demand a ransom to regain your mailbox data. Administrators should review and audit the permissions given by users. In addition to auditing the permissions given by users, you can locate risky or unwanted OAuth applications in premium environments.

Step 5: Enable end-user self-service

As much as possible you want to balance security with productivity. Approaching your journey with the mindset that you're setting a foundation for security, you can remove friction from your organization by empowering your users while remaining vigilant and reducing your operational overheads.

Implement self-service password reset

Microsoft Entra ID's self-service password reset (SSPR) offers a simple means for IT administrators to allow users to reset or unlock their passwords or accounts without helpdesk or administrator intervention. The system includes detailed reporting that tracks when users reset their passwords, along with notifications to alert you to misuse or abuse.

Implement self-service group and application access

Microsoft Entra ID can allow nonadministrators to manage access to resources, using security groups, Microsoft 365 groups, application roles, and access package catalogs. Self-service group management enables group owners

to manage their own groups, without needing to be assigned an administrative role. Users can also create and manage Microsoft 365 groups without relying on administrators to handle their requests, and unused groups expire automatically. Microsoft Entra entitlement management further enables delegation and visibility, with comprehensive access request workflows and automatic expiration. You can delegate to nonadministrators the ability to configure their own access packages for groups, Teams, applications, and SharePoint Online sites they own, with custom policies for who is required to approve access, including configuring employee's managers and business partner sponsors as approvers.

Implement Microsoft Entra access reviews

With Microsoft Entra access reviews, you can manage access package and group memberships, access to enterprise applications, and privileged role assignments to make sure you maintain a security standard. Regular oversight by the users themselves, resource owners, and other reviewers ensure that users don't retain access for extended periods of time when they no longer need it.

Implement automatic user provisioning

Provisioning and deprovisioning are the processes that ensure consistency of digital identities across multiple systems. These processes are typically applied as part of identity lifecycle management.

Provisioning is the processes of creating an identity in a target system based on certain conditions. Deprovisioning is the process of removing the identity from the target system, when conditions are no longer met. Synchronization is the process of keeping the provisioned object, up to date, so that the source object and target object are similar.

Microsoft Entra ID currently provides three areas of automated provisioning. They are:

- Provisioning from an external nondirectory authoritative system of record to Microsoft Entra ID, via HR-driven provisioning
- Provisioning from Microsoft Entra ID to applications, via App provisioning
- Provisioning between Microsoft Entra ID and Active Directory Domain Services, via inter-directory provisioning

Find out more here: What is provisioning with Microsoft Entra ID?

Summary

There are many aspects to a secure Identity infrastructure, but this five-step checklist helps you to quickly accomplish a safer and secure identity infrastructure:

- Strengthen your credentials
- Reduce your attack surface area
- Automate threat response
- Utilize cloud intelligence
- Enable end-user self-service

We appreciate how seriously you take security and hope this document is a useful roadmap to a more secure posture for your organization.

Next steps

If you need assistance to plan and deploy the recommendations, refer to the Microsoft Entra ID project deployment plans for help.

If you're confident all these steps are complete, use Microsoft's Identity Secure Score, which keeps you up to date with the latest best practices and security threats.
