



# MSFT365 Security Control Checklist



**Microsoft 365, as a service, contains many features that focus on security.** Each service uses Azure Active Directory for authentication and authorization to access either the app itself or the content that resides within it. Organization-specific security controls and procedures should augment all out-of-the-box configurations. Remember that security within Microsoft 365 is not just about enabling features and controls; it also involves teaching and guiding end-users to understand the restrictions and knowing how to use them.

Knowing which controls to enable, licenses to purchase, or rules to create is critical to deploying successful security capabilities. All organization types and sizes will benefit from enabling the most common controls regardless of whether the tenant is new or currently being used.

## Common Security Controls

All organizations need to review their current Microsoft 365 Tenants and determine the controls to enable. Organizations should use current written policies and core business requirements for enabling the proper controls. The most common security control categories are:

1. Multi-Factor authentication for end-users and administrators
2. Conditional access policies for controlling access
3. Block legacy authentication protocols to reduce the surface area of attack
4. Deployment of core password controls
5. External sharing restrictions and policies
6. Managing mobile device connections, including corporate and personal devices
7. Controlling the dissemination of data capabilities within email and document storage
8. Classification of content with additional protections

**To help with deployment, organizations can step through this checklist and enable as required.**

Enabled	Control Details
<input type="checkbox"/>	<p><b>Require Multi-factor Authentication for Administrators</b></p> <p>Create a conditional access policy that includes all administrator directory roles. Ensure either all cloud apps or specific apps are selected. Grant access and select <a href="#">Require multi-factor Authentication</a>.</p>
<input type="checkbox"/>	<p><b>Require Multi-factor Authentication for All Users</b></p> <p>Create a conditional access policy that includes all user or a group that contains the chosen users. Ensure either all cloud apps or specific apps are selected. Grant access and select <a href="#">Require multi-factor Authentication</a>.</p>
<input type="checkbox"/>	<p><b>Block Legacy Authentication</b></p> <p>Create a conditional access policy that includes all users and groups. Select all cloud apps, then in the conditions, choose to configure and select Exchange ActiveSync and Other Clients. Within access controls, choose <a href="#">Block access</a>.</p>
<input type="checkbox"/>	<p><b>Enforce Trusted Location for Multi-factor Registration</b></p> <p>Create a conditional access policy that includes all users and groups. Select all cloud apps or actions, and select User actions. Choose the <a href="#">Register Security Information</a>. Within Conditions, choose Locations and include Any Location, then exclude All Trusted Locations. Select Client Apps, and set Configure to <a href="#">Yes</a>. Under Access controls, select <a href="#">Block Access</a>.</p>
<input type="checkbox"/>	<p><b>Block Access to Unapproved Locations</b></p> <p>Create Named Locations within Conditional Access to represent the Blocked Locations, Subnet, or IP Ranges for the organization. Create a conditional access policy that includes all users and groups. Ensure either all cloud apps or specific apps are selected. Under conditions, set the included locations to the blocked locations. Within Access Controls, select <a href="#">Block Access</a>.</p>
<input type="checkbox"/>	<p><b>Sign out Inactive Users</b></p> <p>Navigate to the <a href="#">SharePoint Admin Center</a>, expand <a href="#">Policies</a> and choose <a href="#">Access Control</a>. Click the <a href="#">Idle Session Sign-out</a> option. Toggle the <a href="#">Sign out inactive users automatically</a>, then select when to sign out users and how much warning you want to give them before signing them out.</p>

### Configure Password Expiration

Navigate to the Microsoft 365 Admin Center, click on [Settings](#), then choose [Org Settings](#). Click the [Security & privacy](#) page, then select [Password expiration policy](#). Uncheck the box next to set user passwords to expire after a number of days.

### Configure Banned Password Lists

Navigate to [Azure Active Directory](#), choose [Security](#). Under [Manage](#), select [Authentication Methods](#), then select [Password Protection](#). Set the [Enforce custom list](#) to yes, then add the list of banned passwords. To use within On-premises Active Directory as well, install the agent.

### Set the External Sharing Level

Navigate to the [SharePoint Administration Center](#), click [Policies](#), then [Sharing](#). Set the sharing sliders as required, with a recommendation to [use existing guests](#) as the default. Configure any other specific configuration to control sharing and links to content.

### Set the Account Lockout Threshold

Navigate to [Azure Active Directory](#), then select [Security](#), [Authentication](#) methods followed by [Password protection](#). Set the [Lockout Threshold](#) to the number of failed sign-ins allowed before accounts are locked out. To mitigate a denial-of-service account attack, this should be **0**; the default, however, should be **10**.

### Restrict External Sharing by Domain

Navigate to the [SharePoint Administration Center](#), click [Policies](#), then [Sharing](#). Expand [More external sharing settings](#), then check [Limit external sharing by domain](#). Add the chosen domains allowed for external sharing.

### Restrict External Sharing to specific Security Groups

Navigate to the [SharePoint Administration Center](#), click [Policies](#), then [Sharing](#). Expand [More external sharing settings](#) and then check the [Allow only users in specific security groups to share externally](#) option. Add the chosen security groups allowed for external sharing.

## Block Client Forwarding Rules within Exchange Online

Launch [Windows PowerShell](#), create a new PowerShell session to Exchange Online. Execute [New-TransportRule](#) command with the required property values.

```
New-TransportRule -Name "Block Client Forwarding" `
-Priority 1 `
-SentToScope NotInOrganization `
-FromScope InOrganization `
-MessageTypeMatches AutoForward `
-RejectMessageEnhancedStatusCode 5.7.1 `
-RejectMessageReasonText "Message"
```

## Restrict Un-managed Application Consent

Navigate to [Azure Active Directory](#), click [Enterprise applications](#). Select [Consent and permissions](#), then choose [User consent settings](#).

Under the [User consent for applications](#) option, set to the required control. The recommendation is to use [Users can consent to apps from verified publishers or your organization, but only for permissions, you select](#).

## Enable Sign-in Risk-based Conditional Access

Navigate to [Azure Active Directory](#), then click [Security](#). Click [Conditional Access](#). Create a new [Conditional Access Policy](#). Under assignments, select [Users and Groups](#) and set to [All Users](#). Within [Cloud Apps or Actions](#), select All Cloud Apps or the chosen Apps. Select [Conditions](#), and configure the Sign-in Risk to either [High](#) or [Medium](#).

## Enable User Risk-based Conditional Access

Navigate to [Azure Active Directory](#), then click [Security](#). Click [Conditional Access](#). Create a new [Conditional Access Policy](#). Under assignments, select [Users and Groups](#) and set to [All Users](#). Within [Cloud Apps or Actions](#), select All Cloud Apps or the chosen Apps. Select [Conditions](#), and configure [User Risk](#) to be High. Under [Access Controls](#), choose [Grant](#) and set to [Require Password Change](#).

Checklist completed