

2026-03-30



Förebyggande åtgärder för att säkra upp Microsoft 365-miljöer

CERT-SE

2026-03-30

Inledning

Vid uppsättning av en klientorganisation (engelska: tenant) i Microsofts molnmiljö är flexibiliteten hög och nya funktioner läggs till kontinuerligt. CERT-SE uppmanar därför organisationer att regelbundet se över aktiverade, eller inaktiverade, inställningar för att undvika att vanliga användare har möjlighet att utföra åtgärder som de ur säkerhetssynpunkt inte bör kunna göra.

Detta dokument syftar till att ge råd och riktlinjer kring hur organisationer i förebyggande syfte, och med enkla medel, kan höja säkerheten i sina M365-miljöer. CERT-SE uppmanar varje organisation att utvärdera, testa och implementera eventuella lösningar och funktioner utifrån organisationens förutsättningar. CERT-SE har i största möjliga mån försökt begränsa åtgärder och rekommendationer till sådant som är tillgängligt utan licens.

Microsoft erbjuder organisationer möjligheten att automatiserat testa sin klientorganisation mot Zero Trust Framework med verktyget Zero Trust Assessment.

För mer information om Zero Trust Framework och Zero Trust Assessment-verktyget, se följande information:

Microsoft. (27-03-2026). Configure Microsoft Entra for increased security (Preview)

<https://learn.microsoft.com/en-us/entra/fundamentals/configure-security>

Microsoft. (19-03-2026). What is the Zero Trust Assessment?

<https://learn.microsoft.com/en-us/security/zero-trust/assessment/overview>

Microsoft. (16-03-2026). Get started with the Zero Trust Assessment

<https://learn.microsoft.com/en-us/security/zero-trust/assessment/get-started>

Innehållsförteckning

1. Se över användarinställningar.....	4
2. Begränsa vilka applikationer användare kan registrera.....	7
3. Begränsa vilka användare som kan dela filer i SharePoint och till vem.....	9
4. Begränsa vem som kan lägga till enheter i Entra ID.....	10
5. Begränsa vem som ska skapa eller överföra nya Subscriptions i Azure.....	11
6. Security Defaults.....	12

1. Se över användarinställningar

Vid installation av M365-miljö i en klientorganisation har en vanlig användare relativt breda befogenheter. Befogenheterna innebär en möjlighet att registrera applikationer, skapa nya klientorganisationer, samt åtkomst till Microsoft Entra admin center.

CERT-SE:s rekommendation är att begränsa dessa rättigheter, samt att se över gästkontons behörigheter eftersom standardbehörigheten medför säkerhetsrisker.

För att begränsa användarrättigheter, följ instruktionerna nedan.

1. Gå till **Microsoft Entra admin center** (<https://entra.microsoft.com>).
2. Expandera fliken **Users**.
3. Välj **User settings**.
4. Under **Default user role permission**, ändra följande inställningar:
 - **Users can register applications**, ändra till **No**. Inställningen bör kombineras med åtgärder i kommande avsnitt.
 - **Restrict non-admin users from creating tenants**, ändra till **Yes**.
 - **Users can create security groups**, ändra till **No**.
5. Under **Guest user access**, ändra följande inställningar:
 - **Guest user access restrictions**. Ifall gäster inte används inom klientorganisationen så bör inställningen ändras till **Guest user access is restricted to properties and memberships of their own directory objects**. Ifall organisationen använder gästkonton, rekommenderar CERT-SE att ändra inställningen till åtminstone **Guest users have limited access to properties and memberships of directory objects**. Tänk på att justera inställningarna utifrån organisationens behov.
6. Under **Administration center**, ändra följande inställningar:
 - **Restrict access to Microsoft Entra admin center**, ändra till **Yes**.
Viktigt! Inställningen begränsar endast åtkomsten till delar av Entra admin center/Azure-portalen via webbläsaren för vanliga användare och påverkar inte åtkomst till resurser eller objekt med hjälp av Microsoft Graph, PowerShell, Visual Studio med flera samt för administratörer (inklusive egenskapade administrativa

- roller). Användare med roller som medger åtkomst med till exempel Microsoft Graph berörs inte av inställningen. Inställningen innebär även att användare som står som gruppägare inte kommer åt att administrera dessa via webbläsaren, därför behöver detta anpassas utifrån organisationens behov.
7. Under **LinkedIn account connections**, ändra följande inställningar:
 - **Allow users to connect their work or school account with LinkedIn**, ändra till **No**.
Tänk på att justera inställningarna utifrån organisationens behov.
 8. Under **Show keep user signed in**, ändra följande inställningar:
 - **Show keep user signed in**, ändra till **No**.
 - Om inställningen är satt till **Yes**, skapas en långvarig, upp till 90 dagar, **Refresh Token** som riskerar att ge en hotaktör långvarig åtkomst till en session om de lyckas kompromettera ett konto. Genom att sätta värdet till **No** minskar risken för att långvariga webbläsarsessioner bibehålls, upp till 90 dagar med en **Refresh Token**, och kan hjälpa till att begränsa konsekvenserna utifall att ett användarkonto komprometteras.
 9. Under **External users**, välj **Manage external collaboration settings**.
 10. Under **Guest user access**, ändra följande inställningar:
 - Denna inställning definierar vilken åtkomst gäst användare har till de objekt och resurser som existerar i er klientorganisation. Om det inte finns ett specifikt behov i organisationen för gäst användare att komma åt samma information som befintliga medarbetare så bör man begränsa detta till **Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)**.
 11. Under **Guest invite settings**, ändra följande inställningar:
 - Säkerställ att inte vilken användare som helst kan bjuda in gäster. Här kan man specificera om särskilda användare, roller eller endast administratörer ska ha tillåtelse att bjuda in användare. CERT-SE rekommenderar att hellre begränsa för mycket och därefter öppna upp utifrån behov. Om det inte föreligger ett särskilt behov av att kunna bjuda in gäst användare så välj **No one in the organization can invite guest users including admins (most restrictive)** alternativt den mindre restriktiva **Only users assigned to specific admin roles can invite guest users**.
 12. Under **Enable guest self-service sign-up via user flows**, ändra följande inställningar:

- Om organisationen inte aktivt nyttjar gäst-registrering via självservice rekommenderar CERT-SE att ändra inställningen till **No**.

Referenser:

Microsoft. (03-05-25). What are the default user permissions in Microsoft Entra ID?

<https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions>

Microsoft. (12-19-24). Restrict guest access permissions in Microsoft Entra ID.

<https://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissions>

Microsoft. (02-04-26). Manage the 'Stay signed in?' prompt.

<https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-stay-signed-in-prompt>

2. Begränsa vilka applikationer användare kan registrera

Sedan juli 2025 har Microsoft förändrat vem som får lov att registrera applikationer i Entra ID, det är numera inte tillåtet för vilken användare som helst eller vilken applikation som helst. Detta hanteras av Microsoft om man inte gjort ett eget val i sin klientorganisation och även för nya klientorganisationer som registrerats efter juli 2025. Det innebär att Microsoft definierar och kontinuerligt uppdaterar vilka Microsoft Graph- och Office 365 Exchange Online-behörigheter som användare kan godkänna själva, samt vilka mejlklinter som är godkända.

Dessa inställningar gäller endast framtida val av applikationer. Tidigare godkända applikationer bibehåller åtkomst till de behörigheter som redan valts.

Denna åtgärd bör kombineras med åtgärden som beskrivs i föregående avsnitt, under *1. Se över användarinställningar*.

För att begränsa vilka applikationer användare kan registrera, följ instruktionerna nedan.

1. Gå till **Microsoft Entra admin center** (<https://entra.microsoft.com>)
2. Välj **Enterprise apps**.
3. Välj därefter **Consent and permissions** under **Security**.
4. Under **User consent settings**, välj något av de tre alternativen utifrån er organisations behov och kapacitet.
 - **Do not allow user consent** innebär att endast administratörer har rätt att registrera applikationer. Då behöver organisationen även definiera vilka som har behörighet att granska dessa förfrågningar, se punkt fem i detta avsnitt.
 - **Allow user consent for apps from verified publishers, for selected permissions** innebär att endast applikationer från utgivare verifierade av Microsoft tillåts och endast med de definierade behörigheter som man själv väljer i nästa steg, se punkt sex i detta avsnitt.
 - **Let Microsoft manage your consent settings (Recommended)** innebär att Microsoft utgår från deras "best practices" för appbehörigheter, godkända applikationer med mera.

5. Under **Admin consent settings**, välj följande inställningar:
 - Under **Admin consent requests**, ändra till **Yes**.
 - Under **Who can review admin consent requests**, lägg till eventuella administratörer, grupper och/eller roller som ska kunna granska och godkänna dessa förfrågningar. Detta kallas även **Admin Consent Workflow**.
6. Under **Permission classifications**, välj följande inställningar:
 - Under **Low**, **Medium** och **High**, lägg till behörigheter som användare har rätt att ge applikationer åtkomst till. Dessa behöver anpassas utifrån organisationens behov och bör följa principen om lägsta behörighet (least privilege).

Referenser:

Microsoft. (25-03-26). What are the default user permissions in Microsoft Entra ID?

<https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions>

Microsoft. (27-03-26). Configure Microsoft Entra for increased security (Preview)

<https://learn.microsoft.com/en-us/entra/fundamentals/configure-security>

Microsoft. (13-08-24). Publisher verification

<https://learn.microsoft.com/en-us/entra/identity-platform/publisher-verification-overview>

Microsoft. (17-11-24). Delegate app registration permissions in Microsoft Entra ID

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles>

Microsoft. (18-03-25). Overview of user and admin consent

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overview>

Microsoft. (23-01-26). Manage app consent policies

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-app-consent-policies>

Microsoft. (19-01-26). Configure the admin consent workflow

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-admin-consent-workflow>

3. Begränsa vilka användare som kan dela filer i SharePoint och till vem

CERT-SE har observerat att hotaktörer använder sig av SharePoint-tytor för att förmedla skadliga länkar i syfte att lura användare såväl internt inom en organisation som externt utanför organisationen genom nätfiske. Genom att begränsa delning av filer i SharePoint till endast användare inom organisationen går det att minimera risken av att utsättas av nätfiskekampanjer. Tänk på att justera inställningarna utifrån organisationens behov.

För att begränsa vilka användare som kan dela filer i SharePoint och till vem, följ instruktionerna nedan.

1. Gå till **Sharepoint Admin Center**.
2. Expandera fliken **Policies**.
3. Välj **Sharing**.
4. Under **Content can be shared with**, välj lämplig nivå för delning av SharePoint- och OneDrive-relaterat innehåll.

CERT-SE rekommenderar att välja **Only people in your organization**, om det inte finns behov av att dela innehåll externt. Organisationer bör åtminstone begränsa inställningen till **New and existing guests**. Inställningen begränsar åtkomsten till redan befintliga externa gäst användare samt nya som bjuds in i och med den delade länken.

När en ny inbjuden gäst användare accepterar inbjudan skapas ett gästkonto åt användaren i avsändarens domän/klientorganisation. Tänk på att justera inställningarna utifrån organisationens behov.

Referenser:

Microsoft. (22-12-25). *Overview of external sharing in SharePoint and OneDrive in Microsoft 365*. <https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview>

4. Begränsa vem som kan lägga till enheter i Entra ID

Användare har som standard behörighet att själva lägga till enheter i Entra ID. Det medför risker då ett övertaget konto skulle kunna ge en hotaktör behörighet att registrera egna enheter i en klientorganisation. På detta sätt kan de uppnå bibehållen åtkomst/persistens till den berörda klientorganisationen.

För att begränsa vem som kan lägga till enheter i Entra ID, följ instruktionerna nedan. Tänk på att justera inställningarna utifrån organisationens behov.

1. Gå till **Microsoft Entra admin center**.
2. Välj **Devices**.
3. Expandera fliken **Manage**.
4. Välj **Device settings**.
5. Under **Users may join devices to Microsoft Entra**, begränsa vilka som kan lägga till/registrera enheter i Entra ID genom att välja **Selected**, och sedan lägga till specifika användare eller grupper.

Det går även att konfigurera detta via **Intune admin center**. Om användare ska tillåtas att själva lägga till enheter i Entra ID, bör organisationen säkerställa att MFA krävs för att kunna lägga till enheter.

Referenser:

Microsoft. (04-03-25). Understand Intune and Microsoft Entra device limit restrictions.

<https://learn.microsoft.com/en-us/intune/intune-service/enrollment/device-limit-intune-azure>

Microsoft. (27-05-25). Create device limit restrictions in Intune.

<https://learn.microsoft.com/en-us/intune/intune-service/enrollment/create-device-limit-restrictions>

Microsoft. (03-02-26). Manage device identities using the Microsoft Entra admin center.

<https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings>

5. Begränsa vem som ska skapa eller överföra nya Subscriptions i Azure

Det finns observationer på att hotaktörer nyttjar gästkonton för att föra över egna **Subscriptions** till ett offers klientorganisation. Förutom att detta kan resultera i oväntade kostnader för offret, kan det även innebära att en hotaktör får åtkomst till känsliga resurser i miljön. Därför bör organisationer begränsa möjligheterna att både skapa och flytta över **Subscriptions** till sin klientorganisation.

För mer detaljerad information om attackväg och möjliga konsekvenser, se artikel från BeyondTrust under avsnittets referenser.

1. Gå till **Azure Portal**.
2. Välj **Subscriptions**.
3. Välj **Manage Policies** längst upp till vänster.
4. Under **Subscriptions leaving Microsoft Entra tenant**, välj **Permit no one**.
5. Under **Subscriptions entering Microsoft Entra tenant**, välj **Permit no one**.
6. Under **Exempted Users**, välj specifika administratörer som ska ha rättighet att kringgå dessa policys.

Referenser:

BeyondTrust. (28-05-25). Restless Guests: The True Entra B2B Guest Threat Model.

<https://www.beyondtrust.com/blog/entry/restless-guests>

Microsoft. (29-12-25). Manage Azure subscription policies.

<https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy>

6. Security Defaults

Om organisationen inte innehar licenser för att kunna aktivera **Conditional Access Policy** är det möjligt att istället använda det som Microsoft kallar **Security Defaults**. Detta är sedan några år tillbaka standard för de som antingen:

- inte aktiverat Conditional Access Policy,
- inte innehar någon licens, eller
- använder äldre autentiseringsmetoder som inte anses uppfylla moderna säkerhetskrav.

För klientorganisationer som skapats innan oktober 2019 kan inställningarna aktiveras manuellt. Med **Security Defaults** aktiveras ett antal grundläggande säkerhetsinställningar automatiskt inklusive tvingande MFA för samtliga användare i organisationen. Autentiseringsmetoder som Microsoft bedömer som utdaterade, som till exempel Office 2010-klienter, och som inte stödjer MFA, blockeras samt tvingande MFA för att komma åt privilegierade administrativa tjänster. Exempel på privilegierade administrativa tjänster är bland annat Azure Portal, Entra admin center och Azure PowerShell.

Manuell aktivering av **Security Defaults** bör föranledas av noggrann planering och förberedelser eftersom det kan få stora konsekvenser för organisationen.

Referenser:

Microsoft. (21-07-25). Security defaults in Microsoft Entra ID

<https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>