

Use ECS Coins  
for Swag!

# Top 3 win an Atari 2600+

- 1 Get the app
- 2 Visit sessions and sponsors, rate sessions
- 3 Earn ECS Coins
- 4 Spend ECS Coins



[csmmt.eu/app](https://csmmt.eu/app)



run<sub>o</sub>events



# Mastering Microsoft 365 Administration: The checklist

---

## WHOAMI

---



Andreas Krüger

@andikrueger\_de



[linkedin.com/in/andikrueger-de](https://linkedin.com/in/andikrueger-de)









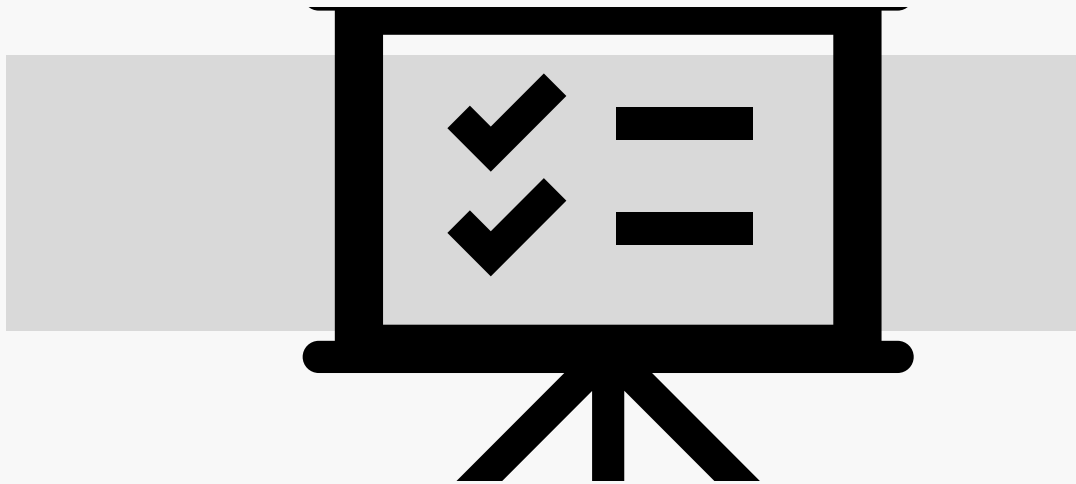


# AGENDA

---

## THE CHECKLIST

Agenda



- ✓ EntraID Settings
- ✓ Apps
- ✓ Organisational Settings
- ✓ Collaboration Settings
  - ✓ SharePoint & OneDrive
  - ✓ Teams
- ✓ Power Platform Settings
- ✓ Tenant Setting Backup



Microsoft Entra admin center

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Home >

Contoso - Main Tenant

+ Add

Manage tenants

What's new

Preview features

Got feedback?

Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Overview

Monitoring

Properties

Recommendations

Tutorials

Search your tenant

EntraID





## EntraID Settings

Identities



- ✓ Admin Accounts
- ✓ User Settings
- ✓ Conditional Access for
  - ✓ Administrative Accounts
  - ✓ User Accounts
  - ✓ Zero Trust
- ✓ Applications
  - ✓ Enterprise Applications
  - ✓ App Registrations

## Global Admin Account

---

- The global administrator is the highest level of administrator.
- The global administrator can manage all aspects of the tenant.
- The global administrator can also assign the services administrator and security administrator roles to other users.
- Use named accounts or at least know who is (single person) using the account

**This global administrative account holds the highest level of access to the tenant - Microsoft 365 and Azure.**

## Break Glass Admin Account

- A break glass admin account is the last resort to get access to a tenant. It is very important to have at least one (1!) of these accounts available!
- Microsoft additionally recommends having separate persona's defined for break glass accounts and for identities that are not part of any persona group. Break glass accounts are excluded from any CA policies and are used in case of emergency where CA may block access for users.





## Account Security

---

- Enable appropriate measures to protect your accounts
- Use privileged administrative workstations (PWA) for administrative access to Microsoft 365
- Enforce MFA for all users
- Validate accounts and service principals frequently
  - At least every 90 days for activity/inactivity
  - Deprovision not used accounts
- Create alerts for usage of high privilege account

## Restrict Access

---

- Restrict the access to your tenant by using conditional access rules based on
  - Account type
  - Persona type
  - Location
  - Device
  - Sign-in frequency
- <https://learn.microsoft.com/en-us/azure/architecture/guide/security/conditional-access-zero-trust>
- <https://github.com/microsoft/ConditionalAccessforZeroTrustResources>

## Personas

### Suggested Personas for Conditional Access



Internals



Guests



Externals



GuestAdmins



Admins



ServiceAccounts



Developer



WorkloadIdentities



## Application Registrations and Enterprise Applications

---

- Establish a proper application governance
  - Do you have all lifecycle events covered with processes? (Create, Read, Update, Delete,...)
  - Are there rules available for any decisions to make?
- Document
  - API permissions with their reasoning –not the Microsoft description of a permission. It needs to be related to the use case of this application.
  - Ownership
  - Responsibility
  - Requestor
  - Risk owner




## Demo Tenant

---

*Let's have a look at some administrative settings.*

Home &gt; Integrated apps

 Enable Dark mode

## Integrated apps

Discover, purchase, acquire, manage, and deploy Microsoft 365 Apps developed by Microsoft partners. You can also deploy and manage Line-of-business add-ins developed within your organization.

For advanced management of these apps go to the respective admin center or page : [Azure Active Directory](#) | [SharePoint](#) | [Teams](#) | [Add-ins](#)

**Deployed apps**

Available apps

Blocked apps

All apps in this list have been installed for tenant users.

Popular apps to be deployed



# Apps





## Apps

App source store



- ✓ Application provisioning
- ✓ Application review

## Apps


---

- Enable only approved apps within the tenant
- Block any other app and any future app
- Review the apps publisher
  - <https://security.microsoft.com/cloudapps/app-catalog>




 Search


Home > Org settings

 Enable Dark mode

# Org settings

Services   Security & privacy   Organization profile

 Search all settings

41 items 

Name ↑

Description

# Org Settings






## Org Settings




The global mighty switches



- ✓ Exchange Calendar Sharing
- ✓ User Owned Apps
- ✓ Bookings
- ✓ Forms
- ✓ Graph Data Connect
- ✓ Microsoft 365 Groups
- ✓ Modern Authentication
- ✓ Microsoft 365 Web
- ✓ Viva Learning
- ✓ Whiteboard

 Contoso Electronics

SharePoint admin center



☰

Home

Sites

Active sites

Deleted sites

Policies

Settings

Content services

Migration

Reports


Contoso - Main Tenant

⚡ What's new?

+ Add cards

Search active sites

Site search

 Search

Go

OneDrive file activity

404 OneDrive files

Last 30 days as of May 12, 2024 (UTC)

SharePoint, OneDrive, Teams

# Collaboration Settings

## Collaboration Settings

SharePoint, OneDrive and Teams



- ✓ Sharing Settings
- ✓ Device Restrictions
- ✓ App Store
- ✓ Policies

## Collaboration Settings

---

- SharePoint and OneDrive
  - Restrict sharing for OneDrive
  - Restrict Sharing for SharePoint
  - Use a lifetime for sharing links
  - Review shared sites
  - Align SharePoint Tenants settings with Conditional Access rules
  - Provision the app catalogue and disable the office store
- Establish a proper user off-boarding for OneDrive and M365 Groups
- Teams
  - Provision selected apps only
  - Restrict access to third party storage providers
  - Restrict guest users





# Power Platform Settings



## Power Platform Settings

With great power,....



- ✓ On-premises Data Gateway
- ✓ Environment Management
- ✓ Self Service Licensing
- ✓ Connectors

## Power Platform Self Service Licensing

---

In Power Platform, there are **three** places to change the self service licensing settings

1. MSCommerce: `Get-MSCommerceProductPolicies -PolicyId AllowSelfServicePurchase`
2. MSOnline: `Get-MsolCompanyInformation | fl AllowAdHocSubscriptions`
3. PowerApps PowerShell: `Get-AllowedConsentPlans`



# Tenant Setting Backup

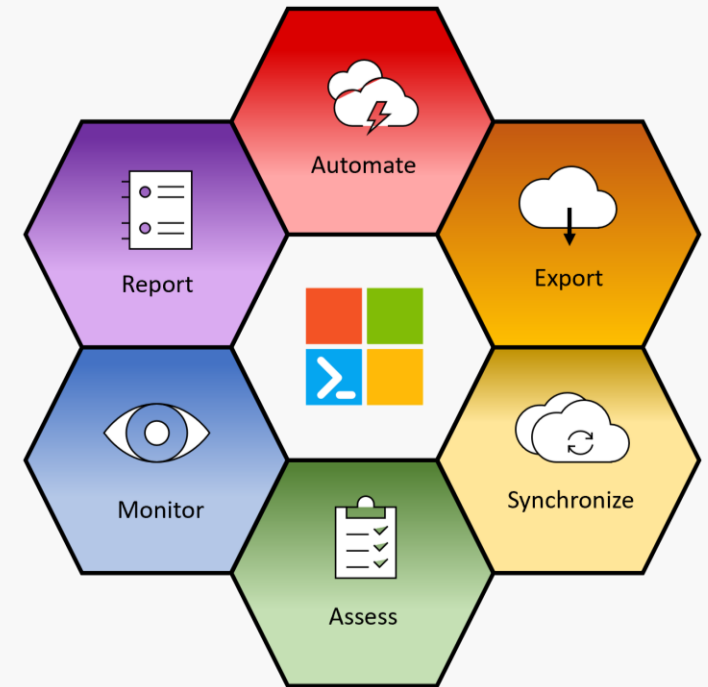


## Tenant Setting Backup – Microsoft 365 DSC

---

Microsoft 365 Desired State Configuration (DSC) is the only tool to export a wide set of M365 settings in a format that can be used to

- Evaluate the settings
- Apply the settings to the same or different tenant
- Create a drift reports for setting changes





## Tenant Setting Backup – Microsoft 365 DSC

---

### Resources:

- User guide:
- <https://microsoft365dsc.com/user-guide/get-started/introduction/>
- Sample Export Script:
- <https://gist.github.com/andikrueger/59946f22ca3a0ab3e87e4ee5fbc383e0>



# Questions



THANK YOU,  
YOU ARE AWESOME ❤️

PLEASE RATE THIS SESSION  
IN THE MOBILE APP.

@andikrueger\_de

<https://de.linkedin.com/in/andikrueger-de>

