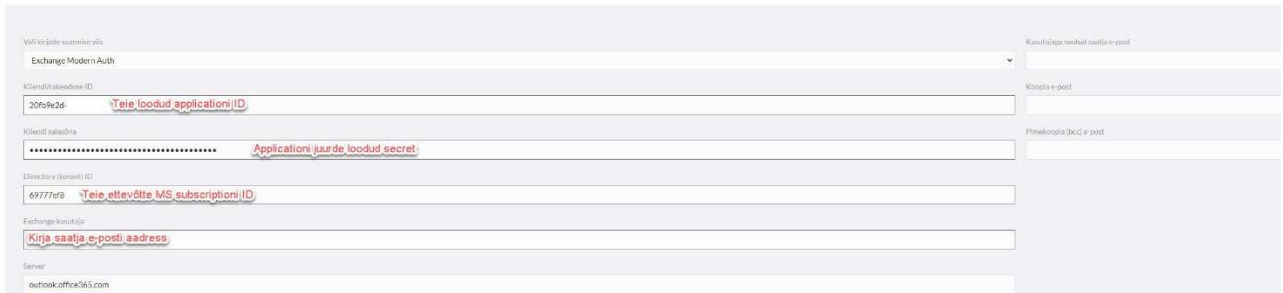


Microsoft Modern Authentication eeldused Merit Aktivas

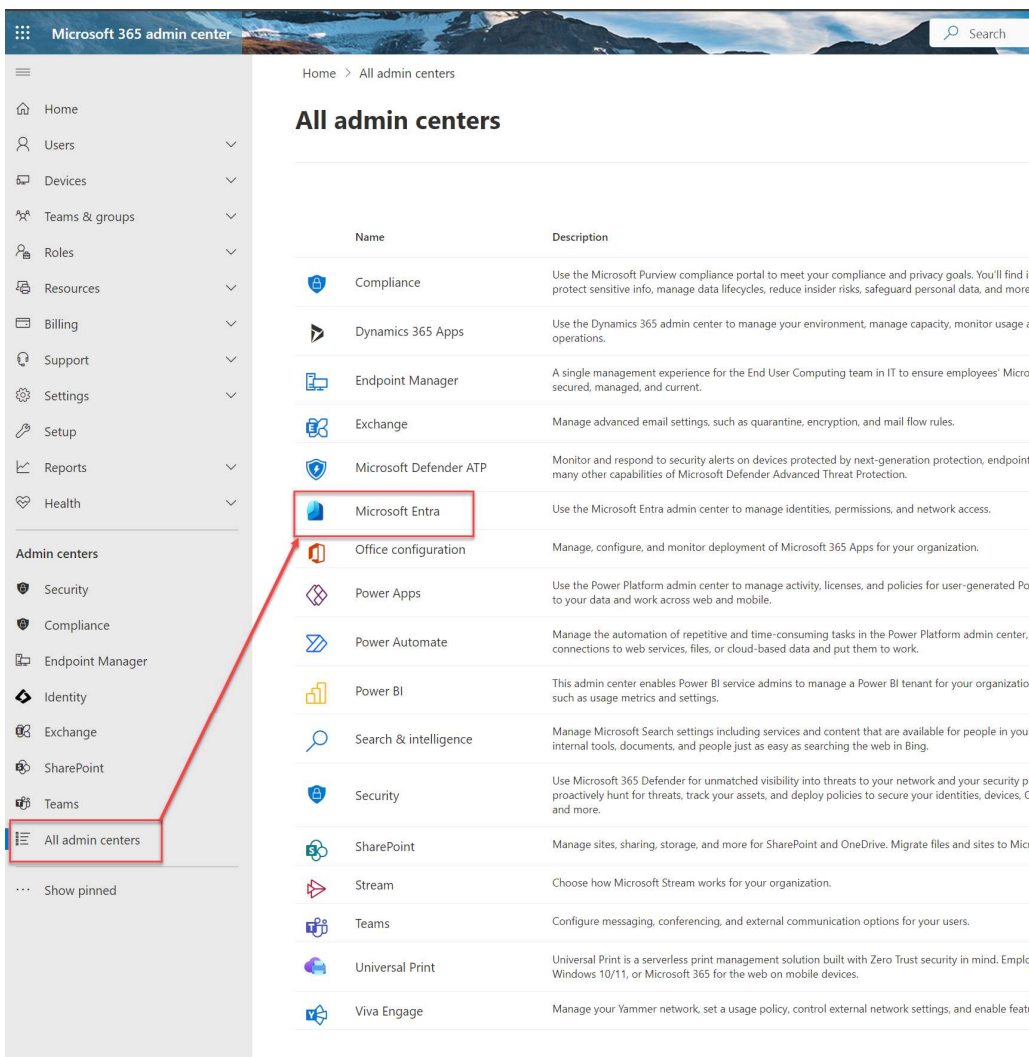
Merit Aktiva E-posti seadistustes, kui saatmisviisiks on valitud Exchange Modern Auth, on näha järgmised read, mis tuleb täita Microsoft Azure Active Directorys loodud Aplikatsiooni andmetega:



The screenshot shows the configuration form for Exchange Modern Auth. The fields are as follows:

- Exchange Modern Auth: [Dropdown menu]
- Client ID (Application ID): 20f9e2d6-Teie loodud application ID
- Client secret: Applicationi juurde loodud secret
- Directory (tenant) ID: 69777d69-Teie ettevõtte MS subscription ID
- Exchange connector: Kirja saatja e-posti address
- Server: outlook.office365.com

Aplikatsiooni enda loomiseks peate oma Office365 keskkonda sisse logima administraatori õigustes kasutajaga ja liikuma „Haldus“->“Kuva kõik“->“Kõik admin keskused“->“Microsoft Entra“



The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar contains a navigation menu with the following items:

- Home
- Users
- Devices
- Teams & groups
- Roles
- Resources
- Billing
- Support
- Settings
- Setup
- Reports
- Health
- Admin centers
 - Security
 - Compliance
 - Endpoint Manager
 - Identity
 - Exchange
 - SharePoint
 - Teams
 - All admin centers

The main content area displays "All admin centers" with a table of services:

Name	Description
Compliance	Use the Microsoft Purview compliance portal to meet your compliance and privacy goals. You'll find in protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more.
Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and operations.
Endpoint Manager	A single management experience for the End User Computing team in IT to ensure employees' Microsoft secured, managed, and current.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Apps	Use the Power Platform admin center to manage activity, licenses, and policies for user-generated Power Apps to your data and work across web and mobile.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, connections to web services, files, or cloud-based data and put them to work.
Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization such as usage metrics and settings.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your internal tools, documents, and people just as easy as searching the web in Bing.
Security	Use Microsoft 365 Defender for unmatched visibility into threats to your network and your security pc proactively hunt for threats, track your assets, and deploy policies to secure your identities, devices, and more.
SharePoint	Manage sites, sharing, storage, and more for SharePoint and OneDrive. Migrate files and sites to Microsoft 365.
Stream	Choose how Microsoft Stream works for your organization.
Teams	Configure messaging, conferencing, and external communication options for your users.
Universal Print	Universal Print is a serverless print management solution built with Zero Trust security in mind. Employ Windows 10/11, or Microsoft 365 for the web on mobile devices.
Viva Engage	Manage your Yammer network, set a usage policy, control external network settings, and enable features.

Kui te olete saanud siseneda oma Entra keskkonda, peaks teile olema koheselt leitav esimene ID, mida teil on tarvis kasutada Aktivas, Directory (tenant) ID:

The screenshot displays the Microsoft Entra admin center interface. On the left, a navigation pane lists various sections, with 'Overview' under the 'Identity' section highlighted by a red box. A red arrow points from this box to the 'Tenant ID' field in the 'Basic information' section of the main content area. The 'Tenant ID' is shown as '69777ef8-'. To the right of the 'Basic information' section, a summary table lists statistics for the tenant.

Basic information	
Name	Users 44
Tenant ID	Groups 8
Primary domain	Applications 2
License	Devices 69

Below the 'Basic information' section, there are three alert boxes:

- Azure AD is now Microsoft Entra ID**: Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
- Upcoming MFA Server deprecation**: Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.
- Migrate legacy**: Please migrate legacy...

Järgmiseks tuleb luua Aplikatsioon, mille kaudu kirjad liikuma hakkavad, sellele Aplikatsioonile tuleb anda õigused ja luua Secret(id):

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane shows the 'Applications' section expanded, with 'App registrations' selected. The main content area is titled 'App registrations' and includes a '+ New registration' button, which is highlighted with a red box. A red arrow points from the 'App registrations' menu item in the sidebar to this button. Below the button, there is a search bar and a table of applications. The table shows two applications: 'PS' and 'YT'.

Display name
PS
YT

Tõenäoliselt loote te Aplikatsiooni ainult oma ettevõttele (ühele domeenile), seega peaks kasutama „Single Tenant“ valikut:

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only only - Single tenant
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

Kui Aplikatsioon on loodud, on teil olemas järgmise välja väärtus Aktivas, Kliendi/Rakenduse ID (number 1), Number 2 tähistab kohta, kus te saate luua omale Aktiva välja „Kliendi salasõna“ ja number 3 tähistab kohta, kus te peate looma omale antud Aplikatsiooni õigused:

Search

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name :
Application (client) ID : 20fb9e2d-
Object ID :
Directory (tenant) ID :
Supported account types : [My organization only](#)

Client credentials : [0 certificate, 2 secret](#)
Redirect URIs : [Add a Redirect URI](#)
Application ID URI : [Add an Application ID URI](#)
Managed application in I... :

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentic solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

API õigused:

Klikka **API Permission** -> **Microsoft Graph** -> **Delegated Permission** -> **User.Read**.

Klikka **API Permission** -> **Microsoft Graph** -> **Application Permission** -> **Mail.Send**.

Klikka **API Permission** -> **Add a permission** -> **APIs in my organization uses** -> **Office 365 Exchange Online** -> **Application Permission** -> **Other permission** -> **full_access_as_app**

Kui kasutaja, millega te loote õiguseis, ei ole kasutaja antud domeenis, ei leia te „Office 365 Exchange Online“ õiguste nimekirjast ja peate selle lisama käsitsi.

The screenshot shows the 'API permissions' page in the Azure AD portal. The left-hand navigation pane has 'API permissions' selected and highlighted with a red box. A red arrow points from this menu item to the '+ Add a permission' button, which is also highlighted with a red box. Below the button, there is a table of configured permissions. The table has columns for 'API / Permissions name', 'Type', 'Description', and 'Admin consent required'. There are two sections: 'Microsoft Graph (3)' and 'Office 365 Exchange Online (1)'. The 'Microsoft Graph' section lists 'Mail.Send' (Delegated, Send mail as a user, No admin consent), 'Mail.Send' (Application, Send mail as any user, Yes admin consent), and 'User.Read' (Delegated, Sign in and read user profile, No admin consent). The 'Office 365 Exchange Online' section lists 'full_access_as_app' (Application, Use Exchange Web Services with full access to all mailboxes, Yes admin consent). Below the table, there is a note: 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.'

Lisaks tuleb teha „grant admin consent“, kuna 2 meie õigustest nõuavad seda:

The screenshot shows the 'API permissions' page with the 'Grant admin consent for' checkbox checked and highlighted with a red box. A red arrow points from this checkbox to the 'Status' column of the table below. The table has columns for 'API / Permissions name', 'Type', 'Description', 'Admin consent required', and 'Status'. There are two sections: 'Microsoft Graph (2)' and 'Office 365 Exchange Online (1)'. The 'Microsoft Graph' section lists 'Mail.Send' (Application, Send mail as any user, Yes admin consent, Status: Granted for i) and 'User.Read' (Delegated, Sign in and read user profile, No admin consent, Status: Granted for v). The 'Office 365 Exchange Online' section lists 'full_access_as_app' (Application, Use Exchange Web Services with full access to all mailboxes, Yes admin consent, Status: Granted for ,).

Search Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (2)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
	4/10/2023	*****	b7b27446-
	10/4/2023	*****	3423cb17-

Secret(id) saate siis luua eelpool näidatud kohas ja Aktivasse on tarvis kopeerida just „Value“ lahtrisse toodud informatsioon. Igale kasutajale võib luua eraldi secreti, kel on tarvis kasutada seda, aga piisab ühestainsast kõigile.

Kui see kõik on tehtud, võiks teie Modern Auth saatisviis ka tööle hakata.

Võimalikud Veateated:

Kui rakenduse ID on vale: „(400) Bad Request“

Kui Tenant ID on vale: „is not avalid for TenantId“

Kui serveri nimi on valesti: „(400) bad Request“

Vale secret: „(401) Unauthorized“

Vale kasutajanimi: „(500) Internal Server Error“