MICROSOFT TEAMS IŠORINĖS PRIEIGOS KONFIGŪRACIJOS INSTRUKCIJA

MICROSOFT TEAMS Administratoriams

VALSTYBĖS INFORMACINIŲ TECHNOLOGIJŲ PASLAUGŲ DEPARTAMENTAS

2021 m. gegužės 3 d.

Turinys

ĮŽANGA 3
REIKALAVIMAI 4
REKOMENDUOJAMOS SAUGOS NUOSTATOS 6
TEAMS ir O365 ARCHITEKTŪRINAI SĄRYŠIAI 10
REIKALINGOS LICENCIJOS 13
PRISIJUNGIMAS 14
TEAMS ADMIN DASHBOARD 15
EXTERNAL ACCESS 17
DNS ĮRAŠAI IŠORINEI FEDERACIJAI 18
HELPDESK – KONTAKTAI 19

ĮŽANGA

External access (Išorinė prieiga): Šis būdas skirtas išoriniams „Teams“ vartotojams iš viso pasaulio rasti, skambinti, kalbėtis ir nustatyti susitikimus su jūsų domeno vidiniais vartotojais, jūsų „Teams“ tenante. Taip pat galima naudoti šią išorinę prieigą komunikuojant su žmonėmis iš kitų organizacijų, kurios naudoja „Skype for Business“ „Online“, taip pat „On-premises“ bei „Hybrid“ instaliacijas.

Open federation (Atvira federacija): Tai yra standartiškai nustatytas „Teams“ parametras, kai yra įjungiama „External access“ (Išorinė prieiga). Šis nustatymas leidžia jūsų organizacijos žmonėms rasti, skambinti, kalbėtis bei planuoti susitikimus su žmonėmis, nepriklausančiais jūsų organizacijai ir esančiais bet kuriame domene, bet kurioje kitoje organizacijoje.

Tokiu atveju vartotojai gali bendrauti su visais išoriniais domenais, kuriuose veikia „Teams“ arba „Skype for Business“ su taip pat nustatyta atvira federacija, arba jeigu komunikuojamo išorinio domeno administratorius yra įtraukęs jūsų domeną į leidžiamų sąrašą.

Jeigu visgi nuspręsite išjungti „External access“ (Išorinę prieigą), išoriniai vartotojai vis tiek turės galimybę prisijungti prie jūsų susitikimų anonimiškai, jeigu bus pakviesti į juos.

REIKALAVIMAI

„Teams Service Administrator " yra minimalios „Teams“ administratoriaus teisės, reikalingos konfigūruoti „Teams“ „External access“. Šiai grupei priklausiančių teisių bei rolių detalų aprašymą galima rasti paspaudus šią nuorodą:

https://docs.microsoft.com/en-us/microsoftteams/using-admin-roles

Jeigu turite jums suteiktas reikalingas minimalias teises ir **jūsų organizacijoje naudojami tik Microsoft Teams** be papildomu O365 komponentų bei rekomenduojamų saugos nuostatų, tuomet galite pereiti prie skyriaus PRISIJUNGIMAS ir sekti tolimesnius paaiškinimus.

Jeigu jūs turite Microsoft Teams su papildomais O365 komponentais ir su rekomenduojamomis saugos nuostatomis, tuomet:

Konfigūruojant „Teams“ „EXTERNAL ACCESS“, rekomenduojame pritaikyti saugos rekomendacijas[1].

1 - Pagal NACIONALINIO KIBERNETINIO SAUGUMO CENTRO PRIE KRAŠTO APSAUGOS MINISTERIJOS (toliau – NKSC) pateiktas rekomendacijas, įdiekite saugos funkcionalumus pagal žemiau pateiktose nuorodose esančias instrukcijas. (Detalesnė informacija – skyriuje REKOMENDUOJAMOS SAUGOS NUOSTATOS)

Šioje instrukcijoje nenagrinėjami „Teams“ ir „Office 365“ loginiai, konfigūracijos ir architektūros sąryšiai[2].

2 - Plačiau apie „Teams“ ir „O365“ architektūrinius sąryšius (sąveiką) galite pasinagrinėti čia:

https://docs.microsoft.com/en-us/microsoft-365/solutions/productivity-illustrations?view=o365-worldwide (Detalesnė informacija – skyriuje TEAMS ir O365 ARCHITEKTŪRINAI SĄRYŠIAI)

Dauguma diegiamų „Teams“ saugos funkcionalumų reikalingi papildomi O365 komponentai ir licencijos[3].

3 – Rekomenduojamų saugos komponentų bei „Teams“ ir „O365“ architektūros sąryšių reikalingų papildomų komponentų diegimui reikalingas licencijas galite rasti čia:

https://docs.microsoft.com/en-us/microsoft-365/solutions/productivity-illustrations?view=o365-worldwide (Detalesnė informacija – skyriuje REIKALINGOS LICENCIJOS).

Šioje instrukcijoje nenagrinėjami „Teams“ ir „Skype for Bussines“ interoperabilumai[4].

4 - Plačiau apie „Teams“ ir „Skype for Bussines“ interoperabilumą (sąveiką) galite pasinagrinėti čia:

https://docs.microsoft.com/en-us/microsoftteams/teams-and-skypeforbusiness-coexistence-and-interoperability

REKOMENDUOJAMOS SAUGOS NUOSTATOS

1. „Microsoft Teams“ platforma palaiko platformos saugumo konfigūracijos įvertinimo funkcionalumą „Compliance Manager“. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide

2. Jeigu numatyta „Microsoft Teams“ platformoje vykdyti rinkmenų ir tekstinių žinučių perdavimą, rekomenduojama sukonfigūruoti „Data classification“ įrankį, leidžiantį klasifikuoti platformoje saugomus duomenis pagal duomenų jautrumą. Duomenų klasifikavimas įgalina duomenų nutekėjimo prevenciją. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodose žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/archiving-third-party-data?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoftteams/sensitivity-labels

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

3. Platformoje yra galimybė konfigūruoti saugumo paprogramę „Policies“. Ši paprogramė yra atsakinga už turinio kontrolę, duomenų praradimo prevencijos funkciją (angl. DLP) ir turinio saugojimo terminų nustatymo funkciją (angl. Records Management). Tai yra saugumo algoritmai, skirti stebėti sistemos elgseną, nustatyti anomalijas ar veikimo sutrikimus. Manytina, kad tinkamas paprogramės sukonfigūravimas leidžia ženkliai padidinti naudojamos platformos saugumą. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodose žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide

4. Planuojamoje naudoti platformoje veikia perspėjimų apie galimus incidentus paprogramė „Alerts“. Ši paprogramė leidžia „Microsoft Teams“ platformoje veikiantiems saugumo algoritmams nustačius anomalijas ar veikimo sutrikimus pranešimu informuoti administratorių. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

5. Platformoje yra galimybė konfigūruoti audito ataskaitų paprogramę „Reports“. Ši paprogramė leidžia stebėti platformoje veikiančios „DLP“ funkcijos rezultatus, platformoje saugomus failus, saugos auditų ataskaitas, vartotojų prisijungimų ataskaitas, vartotojų veiklos ataskaitas. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodose žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/reports-in-security-and-compliance?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide

6. „Microsoft Teams“ platformoje funkcionuoja teisių nustatymo paprogramė „Permissions“, leidžianti nustatyti vartotojų teises, roles ir leidimus. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

7. Platformoje yra palaikoma platformos įvykių registracijos įrašų saugumo paprogramė „Audit“. Platformos įvykių registravimas ir nuolatinė jų peržiūra leidžia anksčiau nustatyti galimai įvykstančius ar įvykusius incidentus. Detalesnė informacija ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

8. „Microsoft Teams“ platformoje numatytas turinio saugumo įrankis „Insider risk management“, leidžiantis pagal „Alerts“ paprogramės duomenis nustatyti vartotojų veiklos anomalijas. Šis funkcionalumas leidžia apsisaugoti nuo informacijos nutekėjimo. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide

9. „Microsoft Teams“ platformoje numatytas pateiktos informacijos apie platformoje veikiantį duomenų saugojimo taisyklių įrankį „Records management“. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide

Šis įrankis leidžia nustatyti duomenų saugojimo trukmę ir vykdo duomenų prieigos kontrolę.

10. Prie „Microsoft Teams“ platformos jungiantis iš viešųjų tinklų, esančių už įstaigos perimetro rekomenduojama tinkamai sukonfigūruoti saugaus ryšio tunelio (pvz., Virtual Private Network – VPN ar kt.) paslaugą, įgalinančią saugų sujungimą su „Microsoft Teams“ platforma. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodose žemiau.

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/top-security-tasks-for-remote-work?view=o365-worldwide

11. „Microsoft Teams“ platforma palaiko dviejų faktorių autentifikavimo saugumo mechanizmą (angl. Multi-factor authentication, MFA). Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

12. Šiuo metu laikomų saugių ir su „Microsoft Teams“ suderinamų interneto naršyklių sąrašas. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoftteams/get-clients#web-client

13. „Microsoft Teams“ vartotojo tinklo ir sistemos konfigūracija. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoftteams/prepare-network

14. „Microsoft Teams“ tinklo nustatymams rekomenduojama konfigūruoti susitikimų kokybinius nustatymus per politikas. Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoftteams/meeting-policies-in-teams

15. Vartotojo sistemos konfigūracijos, Detalesnė informacija, diegimo, konfigūracijos ir funkcionalumo aprašymai nuorodoje žemiau.

https://docs.microsoft.com/en-us/microsoftteams/devices/usb-devices

TEAMS ir O365 ARCHITEKTŪRINAI SĄRYŠIAI

Dauguma saugumo nuostatų rekomendacijų yra realizuotos Office 365 komponentų pagalba ir nėra tiesioginės „Teams“ funkcijos. Plačiau apie „Teams“ ir „O365“ architektūrinius sąryšius (sąveiką) galite pasinagrinėti nurodytoje nuorodoje:

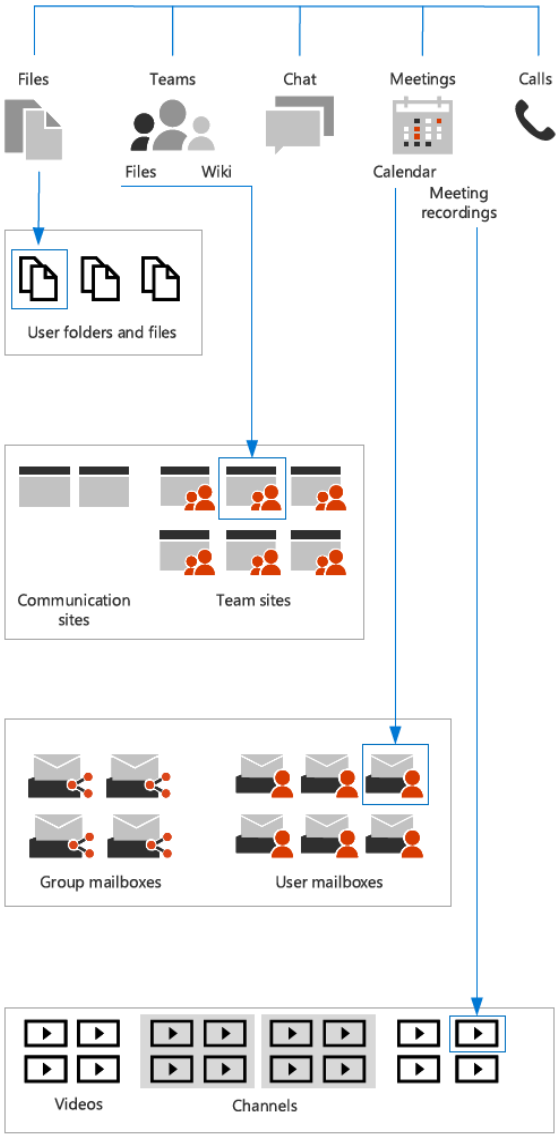
https://docs.microsoft.com/en-us/microsoft-365/solutions/productivity-illustrations?view=o365-worldwide

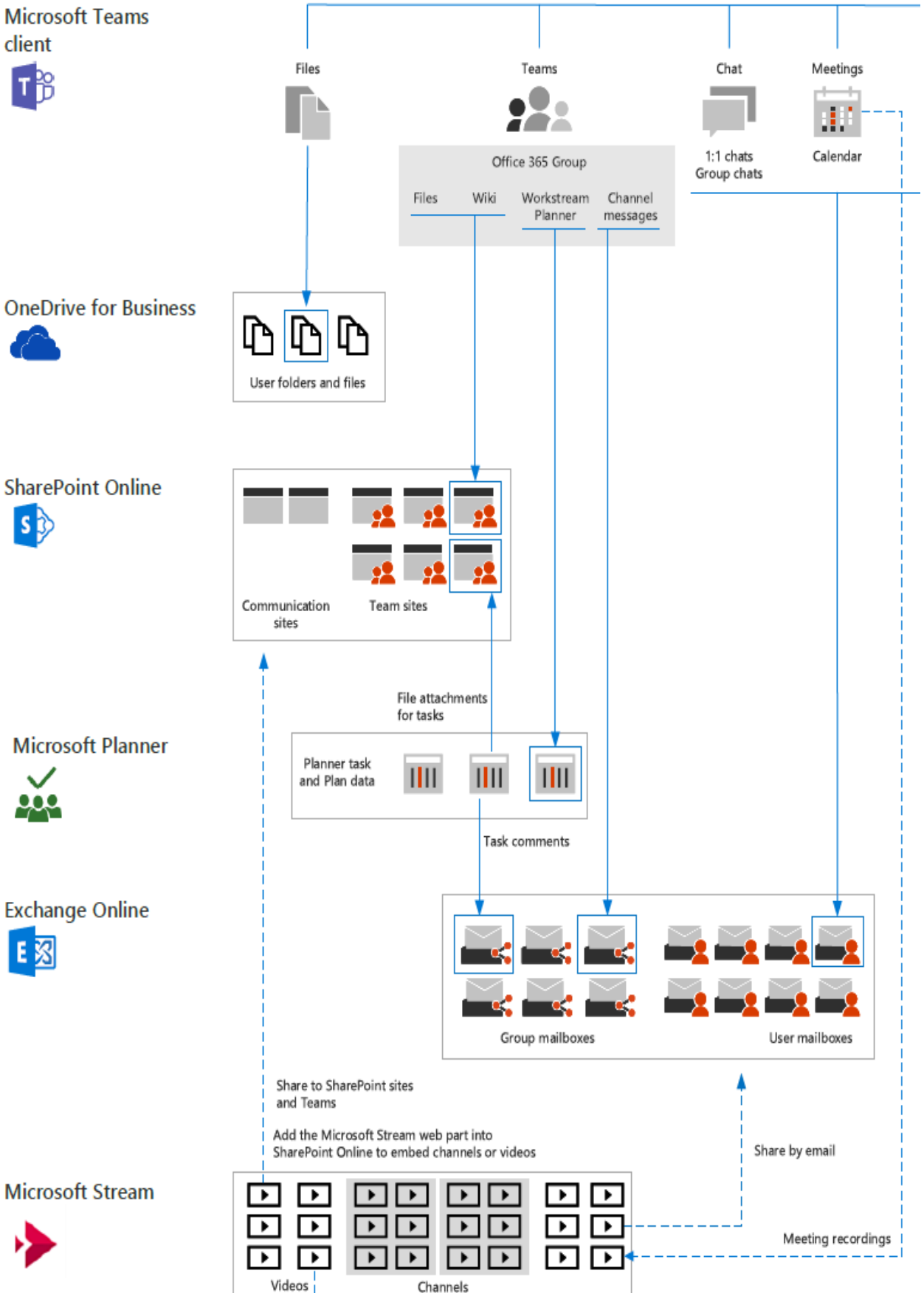
Microsoft Teams and related productivity services

Microsoft 365 provides a suite of productivity services that work together to provide collaboration experiences with data governance, security, and compliance capabilities.

This series of topics provides a view into the logical architecture of productivity services for enterprise architects, leading with Microsoft Teams.

Tool	Great for . . .
Microsoft Teams A client interface on top of other services that provides agile, real-time communication and collaboration for teams. With Microsoft Teams connectors, you can integrate with third-party apps, bots, and add new tabs.	Project-oriented teams to have a conversation, work together in files, call, and meet right where the work is happening. Teams can be public (open to anyone in your organization) or private (managed membership). Use the rich security and compliance capabilities in Microsoft 365 to govern content created through Microsoft Teams.
OneDrive for Business Individual cloud-based file storage. Users can access their OneDrive folders from many locations, including Microsoft Teams.	Storing and syncing files in the cloud and accessing them from anywhere on any device. Ideal for work in progress and sharing with specific individuals. Documents are private until you share them. Share files individually and work on Office documents with others at the same time.
SharePoint Online Create attractive, feature-rich site pages directly in SharePoint Online for teams and communication. Use the same set of security and compliance capabilities across files, whether created through Microsoft Teams or directly in SharePoint sites.	Broad communication using Communication sites and SharePoint News. Storing files in the cloud, making them accessible to a broad audience. Storing sensitive or highly classified files and applying robust permission management, secure access, and compliance capabilities.
Exchange Online & Outlook Email and calendar. Configure security and compliance for email in transit, including data loss prevention policies and classification. Adjust threat protection for spam, malware, phishing, and spoofing. Configure Advanced Threat Protection and threat intelligence capabilities.	Managing time and targeted communications. Schedule and attend meetings either through Outlook or Microsoft Teams. Send protected mail. Take advantage of the most advanced and comprehensive set of protection and compliance capabilities for mail and attachments.
Microsoft Stream The intelligent video service in Office 365.	Create, securely share, and interact with video, whether in a team or across your organization. Host live events.




Microsoft Teams client
Files
Teams
Chat
Meetings
Office 365 Group
Files
Wiki
Workstream Planner
Channel messages
1:1 chats
Group chats
Calendar
OneDrive for Business
User folders and files
SharePoint Online
Communication sites
Team sites
File attachments for tasks
Microsoft Planner
Planner task and Plan data
Task comments
Exchange Online
Group mailboxes
User mailboxes
Share to SharePoint sites and Teams
Add the Microsoft Stream web part into SharePoint Online to embed channels or videos
Share by email
Microsoft Stream
Meeting recordings
Videos
Channels

Microsoft Teams service dependencies

Your organization might want to get started with Microsoft Teams as a first workload, or add it to an existing Office 365 tenant.

What IT architects need to know

Getting started with Teams before other dependent services

You don't need to enable dependent services to get started with Microsoft Teams. These will all 'just work.' However, you do need to be prepared to manage the following:

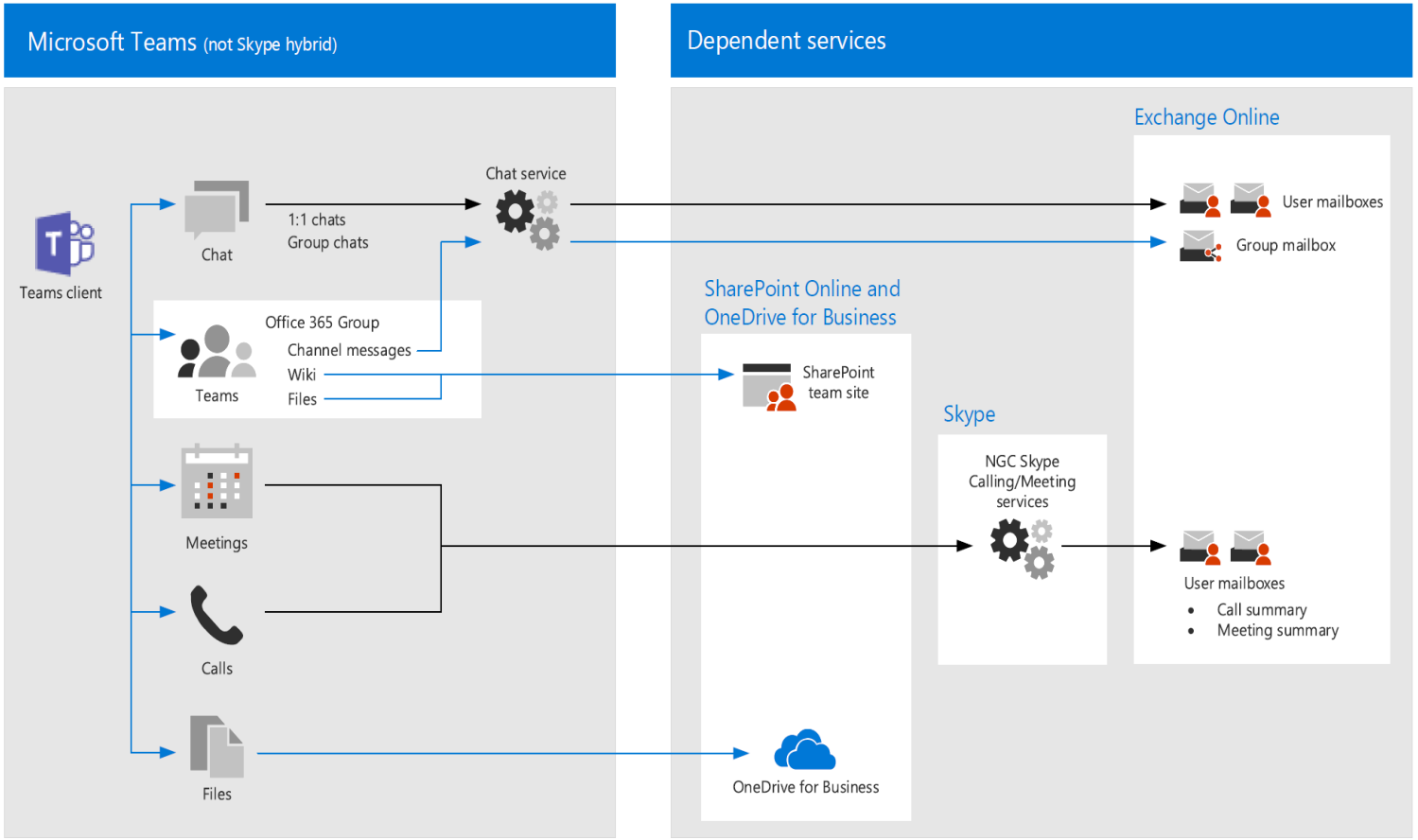
- Office 365 groups
- SharePoint team sites
- OneDrive for Business
- Mailboxes
- Stream videos and Planner plans (if these services are enabled)

Configuring conditional access rules in Azure AD

Be sure to include dependent services in the scope of conditional access rules:

- Microsoft Teams
- SharePoint Online and OneDrive for Business
- Exchange Online
- Skype for Business Online
- Microsoft Stream (meeting recordings)
- Microsoft Planner (Planner tasks and plan data)

For more information, see What are service dependencies in Azure Active Directory conditional access?



REIKALINGOS LICENCIJOS

Rekomenduojamų saugos komponentų, bei „Teams“ ir „O365“ architektūros sąryšiams reikalingų papildomų komponentų diegimui , reikia specialaus licencijavimo:

https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center

https://docs.microsoft.com/en-us/office365/servicedescriptions/downloads/microsoft-365-compliance-licensing-comparison.pdf

Atkreiptinas dėmesys, jog dauguma rekomenduojamų saugos nuostatų, nurodytų skyriuje REKOMENDUOJAMOS SAUGOS NUOSTATOS, įgalintos su *Microsoft 365 E5 | Office 365 E5* Planais. Licenciniai aprašymai yra nuorodoje žemiau.

https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-plan-options

Šioje nuorodoje, 15* Opcijoje, išvardinti reikalingi funkciniai reikalavimai įgyvendinant saugumo reikalavimus:

„Includes Microsoft 365 E5 Compliance, which provides automatic *classification and retention*, Customer Key, Advanced Message Encryption, *Insider Risk Management, Communication Compliance, Information Barriers*, Customer Lockbox, Privileged Access Management, *Advanced Audit, Records Management*, and Advanced eDiscovery capabilities; and *Microsoft 365 E5 Security, which includes Microsoft Defender for Office 365 Plan 2, Microsoft Defender for Endpoint, Azure Active Directory Plan 2, Microsoft Defender for Identity, Microsoft Cloud App Security, and Safe Documents*.“

Galutinis reikalingų licencijų sąrašas, turi būti suderintas su „Microsoft Lietuva“ licencijavimo specialistais ir priklauso nuo diegiamų O365 ir Saugos komponentų derinio.

https://www.microsoft.com/en-us/download/details.aspx?id=102427

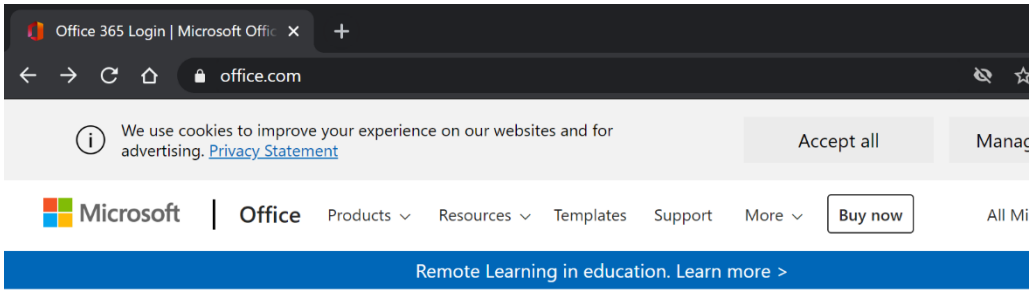
Pageidautina diegiamus komponentus derinti su Duomenų, Saugos, Atitikties ir Vidiniu rizikų valdymo vadybininku – administratoriumi (Microsoft Security Compliance Manager):

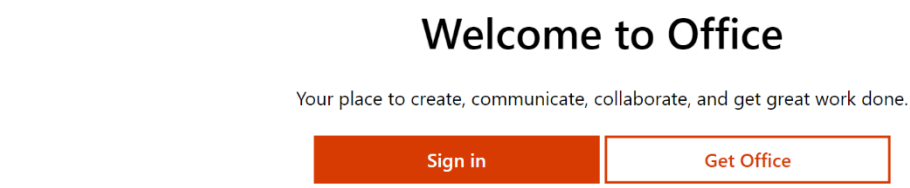
https://docs.microsoft.com/en-us/microsoft-365/compliance/archiving-third-party-data?view=o365-worldwide

*Atkreiptinas dėmesys, jog nuorodoje nurodyti įskiepiai yra 3 šalių. todėl papildomai galbūt reikės pirkti ir į MS 365 diegti įskiepius iš TeleMessage / Globalnet / Veritass.

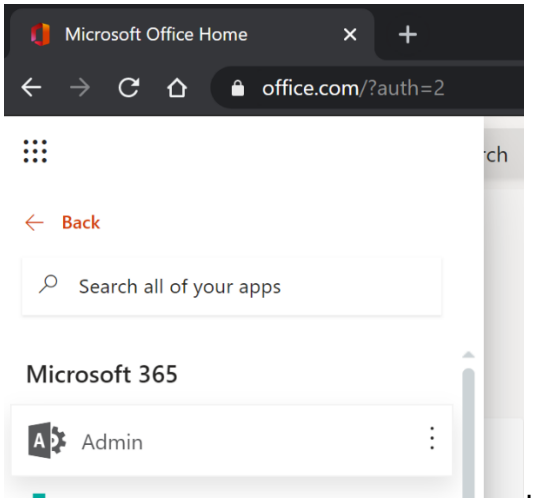
PRISIJUNGIMAS

Vartotojas su skyriuje REIKALAVIMAI nurodytomis teisėmis prisijungia prie O365 portalo: https://office.com/:

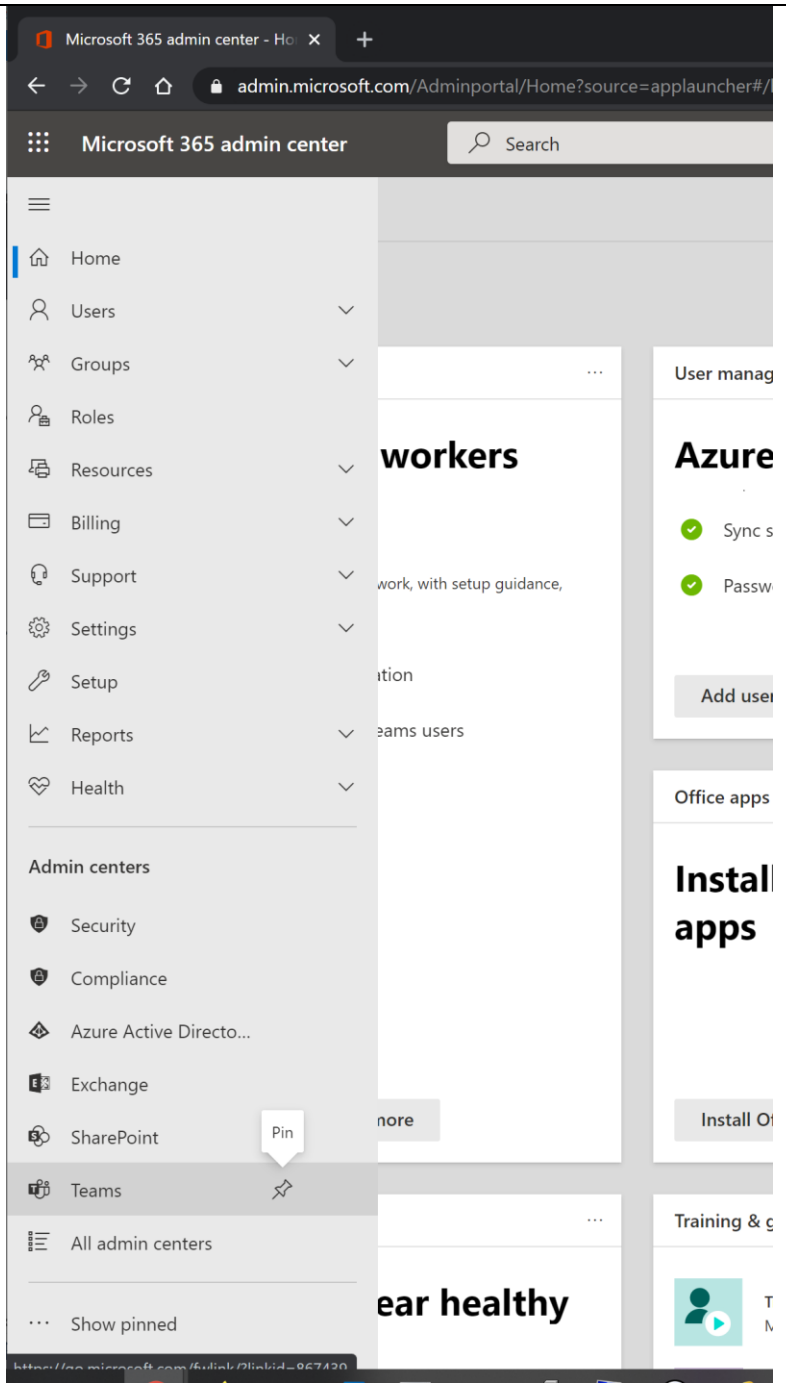


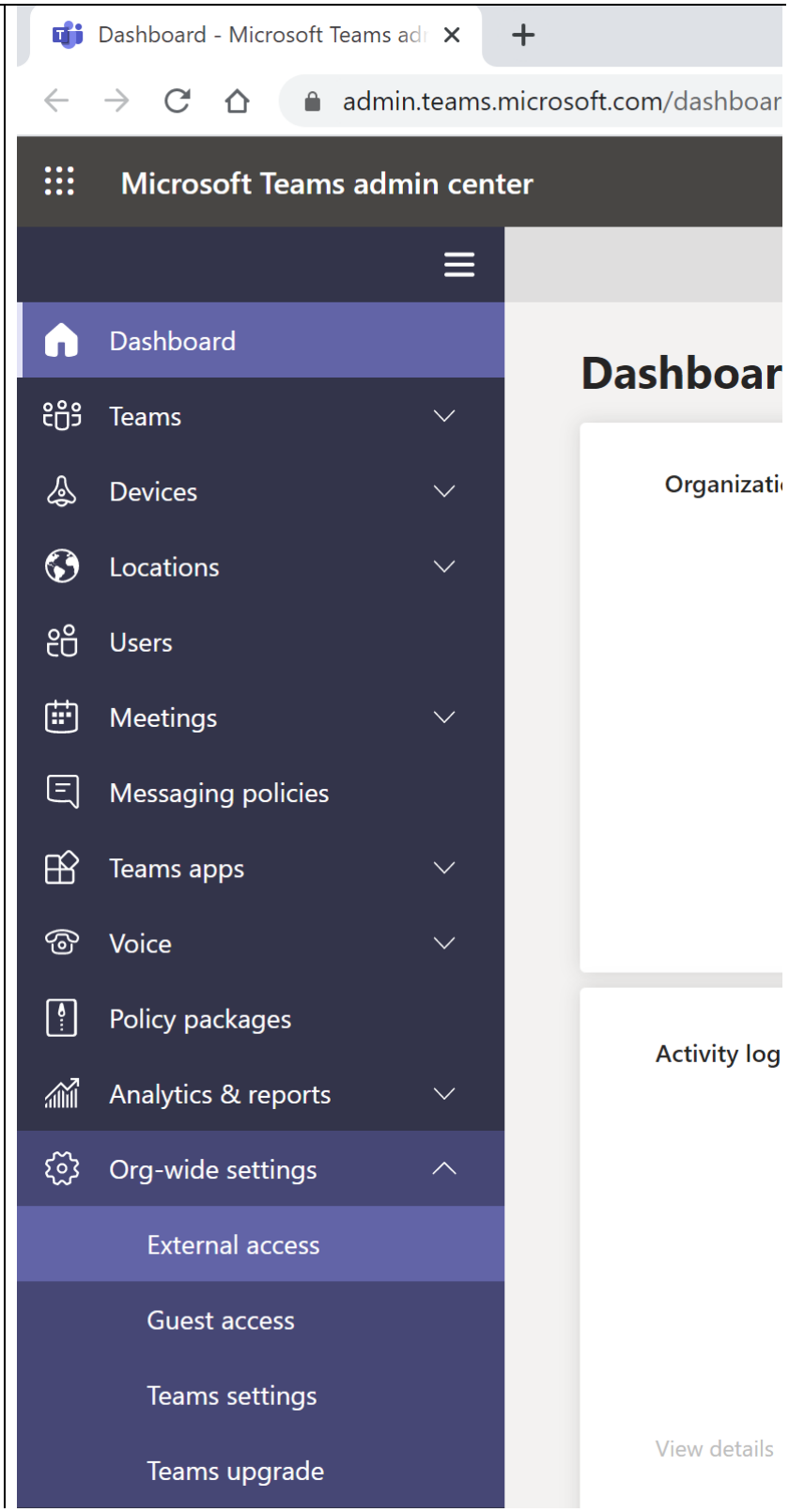


Pasirenkame ADMIN paskyrą:



TEAMS ADMIN DASHBOARD

1	
Pasirenkame „Admins centers“ => Teams arba https://admin.teams.microsoft.com/dashboard	

2	
„Microsoft Teams admin center“ aplinkoje kairiajame meniu pasirenkame **Org-wide settings > External access.** https://admin.teams.microsoft.com/company-wide-settings/external-communications	

EXTERNAL ACCESS

3	
Įjungiame nustatymą **Users can communicate with other Skype for Business and Teams users**.	

Pilnas External access nustatymų aprašymas:

https://docs.microsoft.com/en-us/microsoftteams/manage-external-access

Pakeitimai atlikti „Org-wide settings“ dėl „External access“, įsigalioja 24 val. laikotarpyje.

DNS ĮRAŠAI IŠORINEI FEDERACIJAI

Būtina sąlyga „Microsoft Teams“ External komunikacijai – tvarkingi organizacijos DNS serverių įrašai

Žemiau lentelėje pateikti DNS įrašai tinka „Teams“, taip pat „hibridiniams“ „Teams“ ar „Skype for Business“ scenarijams.

https://docs.microsoft.com/en-us/microsoft-365/enterprise/external-domain-name-system-records?view=o365-worldwide

DNS record	Purpose	Value to use
SRV (Skype for Business Online)	Allows your Office 365 domain to share instant messaging (IM) features with external clients by enabling SIP federation. Read more about Office 365 URLs and IP address ranges.	**Service:** sipfederationtls **Protocol:** TCP **Priority:** 100 **Weight:** 1 **Port:** 5061 **Target:** sipfed.online.lync.com **Note:** If the firewall or proxy server blocks SRV lookups on an external DNS, you should add this record to the internal DNS record.
SRV (Skype for Business Online)	Used by Skype for Business to coordinate the flow of information between Lync clients.	**Service:** sip **Protocol:** TLS **Priority:** 100 **Weight:** 1 **Port:** 443 **Target:** sipdir.online.lync.com
CNAME (Skype for Business Online)	Used by the Lync client to help find the Skype for Business Online service and sign in.	**Alias:** sip **Target:** sipdir.online.lync.com For more information, see Office 365 URLs and IP address ranges.
CNAME (Skype for Business Online)	Used by the Lync mobile client to help find the Skype for Business Online service and sign in.	**Alias:** lyncdiscover **Target:** webdir.online.lync.com

HELPDESK – KONTAKTAI

Jeigu, atlikus skyriuose PRISIJUNGIMAS ir TEAMS ADMIN DASHBOARD išvardintus veiksmus bei praėjus 24 valandų konfigūracijos įsigalėjimo terminui, jūsų valdomo domeno vidiniai vartotojai yra nepasiekiami iš išorinių domenų, prašome kreiptis pagalbos žemiau nurodytais kontaktais.



Valstybės IT paslaugų departamento **HELPDESK**

Tel. Nr. +370 5 2220800

El. p. ITpagalba@vitc.lt

Service desk – IT Pagalba *(paslaugų gavėjams, su kuriais sudarytos sutartys)*
https://servicedesk.vitc.lt/jira/servicedesk