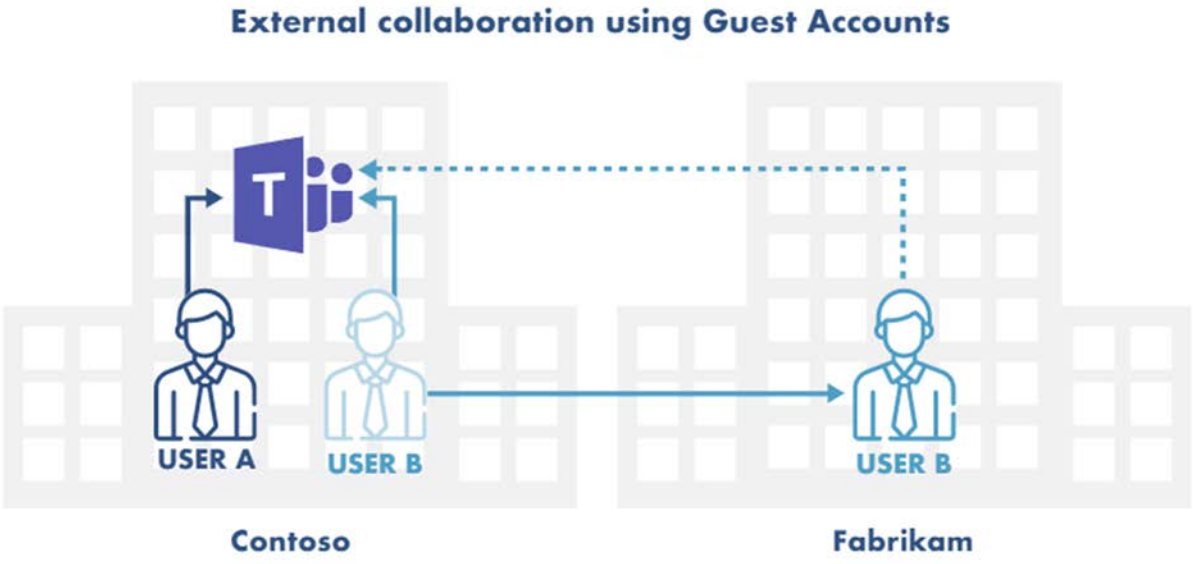
NEXTPLANE

MICROSOFT GUEST ACCESS: EVERYTHING YOU NEED TO KNOW

As an alternative to interoperability, host organizations on Microsoft Teams can invite external members as third-party guests on an as-needed basis. By default, guest access creates the proper levels of separation when working with external parties.

Currently, 44.2% of organizations rely on guest access for third-party collaborations—either to enable external access to their team collaboration platform or to allow their employees to use external team collaboration apps to connect with partner organizations.



Microsoft guest access works seamlessly if both the host organization and the external partners are on Teams. Also, the host and guest organizations want to maintain separate access and data security.

Microsoft Teams also offers an external access federation option for Skype for Business customers that do not want to use guest accounts. However, this option is limited to IM and Presence messages.

In general, the guest access method works well when companies need to add a few external members to a team. However, this capability can quickly become unmanageable when working with a third-party company that requires hundreds or more guest accounts.

There are three critical issues with guest accounts: cost, security, and administrative burden.

First, when it comes to managing external partners that are not on Teams, things become complicated. These organizations must create Azure AD accounts, and their users must learn how to navigate and use Microsoft Teams.

Second, compared to enterprise account password policies, guest accounts' password policy in most cases only requires letters and numbers and does not include Two-Factor Authentication (2FA). Also, it is nearly impossible to control whether guests have robust security measures like password complexity check and password expiration.

Third, administrators have no idea how far away from home their users are playing. Once someone accepts an invitation from another platform, everything they do inside that platform is invisible to the administrator of their home platform. For instance, given the success of Microsoft Teams, a user can end up being a guest in a surprising number of Microsoft Teams tenants.

Fourth, guest accounts are not entirely free. Microsoft Teams only allows five guest accounts per paid Azure AD license. In other words, a company with 1,000 Microsoft licenses can only send out 5,000 guest account invitations.

Finally, Guest accounts require active management. For instance, contractors, clients, interns, or temporary employees come and go out of projects or change jobs or companies. Even with the ability to delete or remove guest accounts, managing guest accounts can result in management hidden costs.

Let us walk through the risks of enabling guest accounts for external federation on your Microsoft Teams.

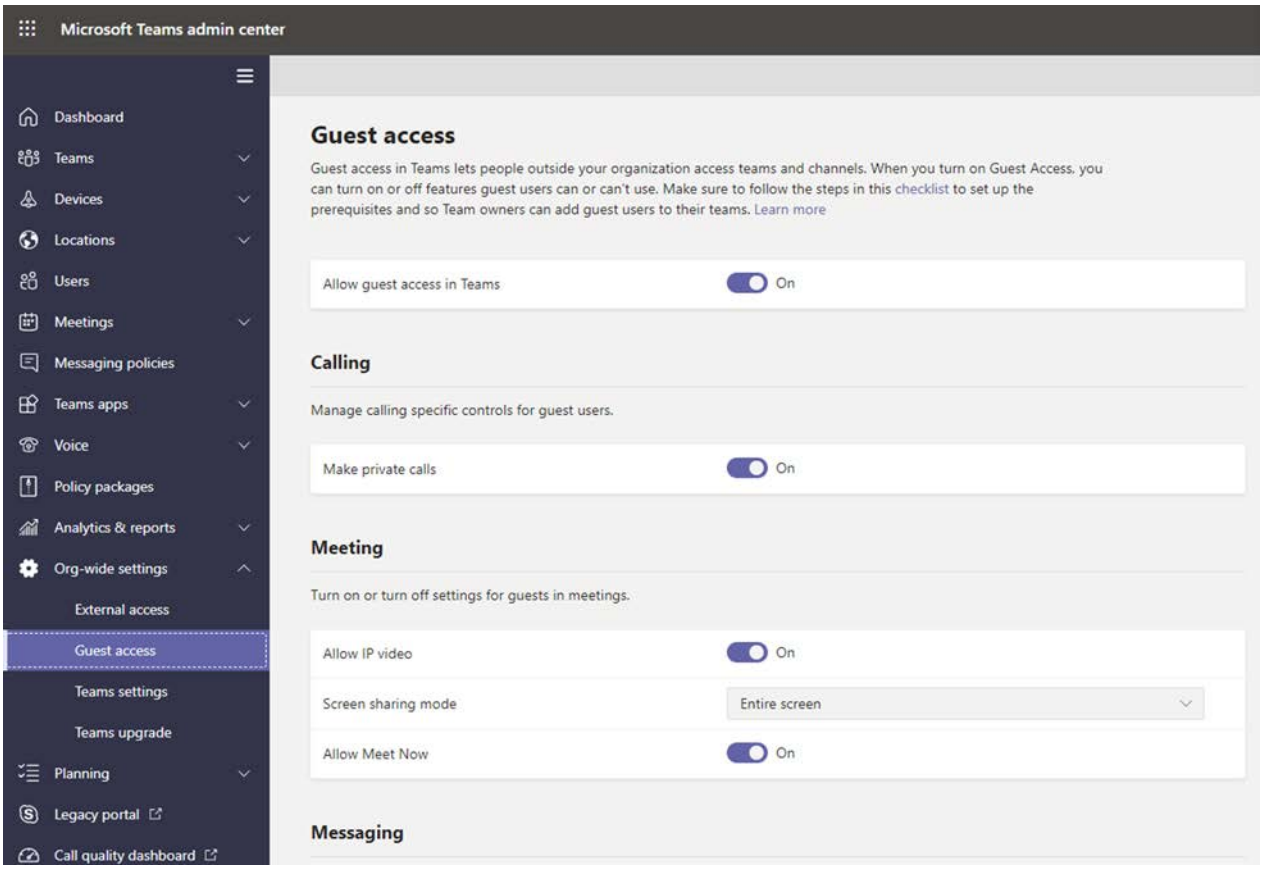
Security and Access Control

Microsoft Guest Access allows Teams users to invite ANY external users with a business or consumer email account, such as Gmail, to participate as a guest in Microsoft Teams tenants with full access to team chats, meetings, and files.

Setting up Microsoft Guest Access can be complicated for organizations that are not on Microsoft Teams. Microsoft Guest Access requires corresponding Azure AD accounts for the guests. This means when users invite their external colleagues to collaborate, using guest accounts, their external colleagues have to create and maintain Azure AD accounts.

Microsoft has decoupled guest accounts' authorization from authentication. As a result, it's nearly impossible to control whether these external Azure AD accounts have strong security measures like password complexity check, password expiration, and Two-Factor Authentication (2FA).

This allows hackers to prey on Guest Access accounts with weak passwords to reach unsuspecting Teams users. Since these compromised guest accounts belong to other companies, you cannot disable them. As a result, they become permanent backdoors to your infrastructure. Most security experts view Microsoft Guest Access as an unmitigated risk to their infrastructure.



Delete/Remove Guest Accounts

Guest accounts require active management. For instance, contractors, clients, interns, or temporary employees come and go out of projects or change jobs or companies. Microsoft provides the ability to delete or remove guest accounts. However, managing guest accounts can become a security and management burden, which can result in hidden costs.

Also, administrators have no idea how far away from home their users are playing. Once someone accepts an invitation from another platform, everything they do inside that platform is invisible to the administrator of their home platform. For instance, given the success of Microsoft Teams, a user can end up being a guest in a surprising number of Microsoft Teams tenants.

Licensing Limitations

The number of guest accounts a company can extend is limited. For instance, Microsoft only allows five guest accounts per paid Azure AD license. In other words, a company with 1,000 Microsoft licenses can only send out 5,000 guest account invitations.

Further complicating the issue is that Microsoft guest accounts invites are not limited to MS Teams, but users can send them for other Microsoft services such as sharing files on One Drive and SharePoint.

There is no limitation or control on how many guest accounts users can send out as long as the company stays within its overall limit. So invitations can begin to pile up. If a company goes beyond its limit, no one can send guest account invites.

End–User Support

End-user support could be more complicated when using guest accounts. For example, if some of the partners decide to block their domains on the Microsoft O365 service, their end users cannot accept and use guest accounts.

In such a scenario, troubleshooting why guest accounts aren't working is impossible. It will create unnecessary support escalations as end-users become frustrated when they can't work with their colleagues.

External Collaboration – NextPlane vs. Microsoft Teams Guest Access

As a general rule, guest accounts are not a viable option for large enterprise companies. Also, external partners may not allow their employees to have guest accounts, or they may be in regulated industries such as healthcare, financial services, where guest accounts can potentially trigger compliance issues.

Also, administrators have no idea how far away from home their users are playing. Once someone accepts an invitation from another platform, everything they do inside that platform is invisible to the administrator of their home platform. People can have accounts on multiple platforms. Given the success of Microsoft Teams, a user on Slack or Cisco WebEx teams can end up being a guest in a surprising number of Teams tenants.

Compliance is the obvious driver for why such oversight might be needed. Companies invest heavily in technologies like communications compliance policies to ensure their company remains within regulatory and legal requirements. Everything works well if collaboration activity remains inside the company. But if someone becomes a guest in another platform and begins communicating there, there's no trace of what they are doing visible to their company, which undermines a carefully built compliance regime.

NEXTPLANE

MICROSOFT GUEST ACCESS: EVERYTHING YOU NEED TO KNOW

NextPlane eliminates the need for external users' need to have access to teams, chats, channels, and files. It also minimizes the IT administrative burdens.

NextPlane intercompany federation allows the host organizations to connect to their external partners securely. As a result, their users can send messages, share their presence status & files, and participate in workspaces & channels, without leaving their respective client applications. Also, external contacts can do the same without leaving their preferred tools.

Unlike Microsoft Guest Access for Teams, NextPlane gives admins user-level control on their companies' external collaboration. It also allows them to track and control their users by federated domains.

To provide Teams admins with user-level control, users must install the NextPlane App on their Teams clients.

NextPlane App takes advantage of the Microsoft Bot Framework to provide a richer collaboration experience for both MS Teams and Non-MS Teams users:

- Add external contacts
- See external contacts' profiles
- Share presence Status
- Send direct messages with rich-text and emoji reactions
- Join and participate in Slack Channels
- Share files

Microsoft Teams users only need the nextplane app, which is available from NextPlane for MS Teams.

The **nextplane** app is not an executable code. It's a registration of NextPlane ConverseCloud within the MS Teams' infrastructure. This registration provides NextPlane ConverseCloud with an access token to call MS Teams API methods and listen to MS Teams events on behalf of NextPlane.

The **nextplane app** passes only chat messages between Microsoft Teams users and the NextPlane ConverseCloud. It treats Microsoft Teams chat inputs as a command and translates them into contact requests, such as SIP invites, and sends them to non-Teams contacts. When the contact request is accepted, it sends Teams users a link to the peer-to-peer chat channel with the invited contact.

Security

NextPlane ConverseCloud only uses the Microsoft Bot Framework to exchange chat messages with the Microsoft Teams users and does not use any other APIs, such as the Microsoft Graph API. By limiting all the internal operations and workflows to the Microsoft Bot Framework, NextPlane does not need or require access to any admin credentials or elevated privileges.

During the installation, the nextplane bot will request the following permissions:

- To receive messages and data
- To send messages and notifications
- To access user profile information

To send and receive messages, NextPlane uses authenticated and encrypted channels. The federated platform may use TLS-enabled SIP, XMPP, or HTTP protocol. The Microsoft Teams users' messages are transferred via the OAuth2-authenticated and TLS-enabled HTTP connection between NextPlane ConverseCloud and the Microsoft Bot Connector.

Privacy

The permissions given to the nextplane app allow NextPlane ConverseCloud to:

- Listen to the Microsoft Teams events, like when users post new messages to their respective Microsoft Teams chat, add emoji, invoke an invite command, modify or delete messages.
- Retrieve and send messages to the Microsoft Teams peer-to-peer chat.

Restricted by the Microsoft Teams Permissions model, NextPlane ConverseCloud can receive events, retrieve, or send messages only to those Microsoft Teams peer-to-peer chats where the NextPlane bots have been added. Otherwise, NextPlane ConverseCloud cannot listen to any events or perform any actions in these chats. Also, NextPlane ConverseCloud has no access to any information (messages or files) shared in the Microsoft Teams channels where users have not added the NextPlane app.

NextPlane ConverseCloud collects different kinds of information, including personally identifiable ones. The following are the types of information NextPlane ConverseCloud collects:

Database

ConverseCloud collects Microsoft Teams users' ID and profile information (name and email) and keeps them in its database. ConverseCloud only uses this information to provide external contacts with their connected Microsoft Teams' users' contact details.

Log Data

The NextPlane servers automatically record a log entry for each message they process. The log entry contains only the metadata without the message content. The metadata consists of the following fields:

- Sender address (e.g., john@acme.com)
- Receiver address (e.g., peter@widget.com)
- Message type (IM, Presence, typing, error)
- Time and date of the message
- Chat session ID

Management

Using NextPlane Management Portal, admins can seamlessly connect different collaboration platforms within a company, or partners such as customers, partners, or suppliers outside the company. The NextPlane management portal provides customers with trailing 12 months of charts and graphs depicting the number of unique users, the number of messages exchanged, as well as detailed usage reports by internal and external federated domains and platforms.

Get More Information

NextPlane can help you with your interoperability and federation needs. Learn how the NextPlane ConverseCloud can help your business by visiting NextPlane, requesting a demo, or by connecting with us at sales@nextplane.net