MS teams

Tips and tricks for successful administration

Michael Lappenbusch
IT-SPECIALIST APPLICATION DEVELOPMENT

Table of contents

1.Introduction to MS Teams

What is MS Teams?

Microsoft Teams is a communication and collaboration platform developed by Microsoft. It allows users to communicate with each other through instant messaging, audio and video calls, and online meetings. It also includes features such as the ability to collaboratively edit and share files, create and manage tasks, and create a collaborative virtual workspace.

Teams is integrated with Office 365 and can be used by anyone with an Office 365 subscription. It allows users to collaborate in real time, whether they are in a physical location or working remotely. It also offers built-in third-party apps like Trello, Asana, and others that allow users to organize and manage their work even more effectively.

Teams also has special features for businesses and organizations, such as the ability to create and manage virtual meeting rooms, and the ability to create secure and private channels within Teams to grant access only to specific members or teams.

Overall, Microsoft Teams provides a comprehensive platform for communication and collaboration that empowers users to get their work done more efficiently and effectively, whether they're working in a physical location or working remotely.

MS Teams architecture

Microsoft Teams architecture is a complex and scalable system made up of multiple components. These components work together to ensure Teams performance and availability.

The basic architecture of Teams consists of the following components:

Clients: These are the applications that users use on their devices to access Teams. There are clients for Windows, Mac, iOS and Android.

Services: These are the services that run in the background to provide the various features of Teams. This includes services such as authentication, managing user accounts, managing meetings and calls, managing chat and team conversations.

Databases: Teams uses multiple databases to support its various features. These databases store information such as user accounts, chat histories, calendar information, and file contents.

Network and security components: Teams uses a variety of network and security components to keep communications between users and the service secure. This includes firewalls, load balancers, and Secure Sockets Layer (SSL) certificates.

Cloud infrastructure: Teams runs on Microsoft's Azure cloud platform. This enables teams to scale quickly and maintain high availability.

Integrated Services: Teams also offers integrated third-party services that allow users to organize and manage their work even more effectively. This includes services like Trello, Asana, and others.

Overall, Microsoft Teams architecture is designed to be highly scalable and flexible to ensure it can meet the needs of any size business and organization. It leverages Azure cloud infrastructure and integrated third-party services to ensure high availability and performance.

Supported Platforms

Microsoft Teams supports a variety of platforms to give users the ability to access the application from any device. This includes:

Windows: Teams is available for Windows PCs and tablets. Users can use the application as both desktop and UWP (Universal Windows Platform) app.

Mac: Teams is also available for Mac computers. Users can download and install the application directly from Microsoft website.

iOS and Android: Teams is also available for mobile devices such as iPhones and iPads as well as Android smartphones and tablets. Users can download and install the application from App Store or Google Play Store.

Web: Teams is also available via a web browser. Users can open and use the application through a browser such as Chrome, Firefox, Safari or Edge.

Surface Hub: Teams is also available for Surface Hub. This allows users to conduct meetings and calls from large touch screens.

HoloLens: Teams is also available for HoloLens, Microsoft's augmented reality headset. Users can conduct meetings and calls from this device, and also use other functions.

Xbox: Teams is also available for Xbox, allows users to hold meetings and calls from their Xbox and use other features.

Overall, Microsoft Teams offers broad support across different platforms to ensure users can access the application from any device and get their work done from anywhere.

2.Planning and preparation

Hardware and software requirements

Microsoft Teams has specific hardware and software requirements for the application to function properly.

Hardware requirements:

Processor: An x86 or x64 processor with at least 1 GHz and SSE2 support.

Memory (RAM): At least 4 GB for using Teams on a Windows PC or Mac.

Free disk space: At least 1 GB free disk space.

Screen resolution: At least 1280 x 720 pixels.

Camera and Microphone: Required for video and voice calls.

Internet connection: At least 1.5 Mbps (download) and 512 Kbps (upload) for Teams use.

Software Requirements:

Operating system: Windows 10, MacOS, iOS, Android, or web browser.

Office 365 subscription: A valid Office 365 subscription is required to access Teams.

Web Browser: A supported browser such as Chrome, Firefox, Safari, or Edge.

.NET Framework: .NET Framework 4.5 or later is required to install Teams on a Windows PC.

DirectX: DirectX 9.0c or later is required to support Teams video functionality.

It is important to note that the above requirements are the minimum requirements and higher hardware and software requirements may be required depending on the number of features used simultaneously and the number of users accessing the application.

Planning of user and team accounts

Planning the user and team accounts in Microsoft Teams is an important step to ensure the application can be used effectively and securely. Some important aspects to consider when planning user and team accounts are:

Access Rights: Ensure each user has the correct access rights to the application to ensure they can access the required features and data.

Roles and Permissions: Set the roles and permissions for each user to ensure they can only access the features and data they need.

Security: Ensure the application and the data processed through it are secure by setting up security features such as two-factor authentication and data encryption.

Scalability: Plan user and team accounts so that the application can easily scale as the number of users increases.

Manageability: Plan user and team accounts to be easily managed to ensure the application is working properly.

Integration: Integrate the application with other tools and applications used in the company to increase collaboration and productivity.

Governance: Implement governance processes to ensure application usage is consistent with company policies and regulations.

It is important that user and team account planning is regularly reviewed and adjusted to ensure the application meets the needs of the business and the security of the data is maintained.

MS Teams organization design

MS Teams organization design refers to the structure and organization of teams within the application. A well-thought-out design of the MS Teams organization can help increase collaboration, productivity and make the application easier to manage. Some important aspects to consider when designing MS Teams organization are:

Team Structure: Determine the team structure that works best for your organization. There are several ways to organize teams, such as by department, project, or geographic location.

Team Members: Determine who should be a member of a team and what roles and permissions they should have.

Team Channels: Create team channels to facilitate communication and collaboration within the team. Each channel should be dedicated to a specific topic or project.

File Storage: Create a file storage for each team so that members can access the documents and files they need.

Integration possibilities: Integrate MS Teams with other tools and applications used in the company to increase collaboration and productivity.

Governance: Implement governance processes to ensure application usage is consistent with company policies and regulations.

Scalability: Plan the team structure so that the application can easily scale as the number of teams or members increases.

It is important to regularly review and adjust the MS Teams organization design to ensure it meets the needs of the business and keeps the data safe.

3. Creation and management of MS Teams

Creating MS Teams

The creation of MS Teams takes place in several steps:

Signing up for MS Teams: You need a Microsoft account to use MS Teams. If you don't already have an account, you can create one by visiting Microsoft's website and clicking Sign Up.

Open MS Teams: After logging in, open MS Teams by selecting the "Teams" button in the top left corner of the screen.

Create a new team: Click on the plus sign in the upper left corner of the screen and select "Create team". You can create a team based on a template or create an empty team.

Give the team a name: Give the team a name and add a description (optional). When you create a private team, you can choose the members to join the team. If you create a public team, anyone who receives the invitation can join the team.

Add Team Members: Click the Add Members button to add more members to a team. You can add members in a variety of ways, such as by email address, username, or group.

Create team channels: On the Channels tab, click the Add Channel button to create a new channel. Each channel should be dedicated to a specific topic or project.

Add Tab Apps: On the Channels tab, click the Add Tab button to add tab apps such as document libraries, polls, calendars, and other tools.

Configure security settings: Click the Manage Team button to configure the team's permissions and security settings.

It is important to regularly review and adjust the MS Teams organization design to ensure it meets users' needs and is organized effectively. This may include deleting unused channels, adding new channels to reflect projects that have evolved, and regularly reviewing permissions and security settings to ensure only authorized individuals have access to specific information. Good planning and organization of MS Teams can help improve collaboration and communication within a company.

Manage MS Teams

Managing MS Teams involves various aspects to ensure that the team environment is running smoothly and the needs of the users are being met. Some of the most important aspects of managing MS Teams are:

Creating and managing teams: It is important to create the right teams for the right purposes. This may include deleting unused teams and creating new teams to reflect projects that have evolved. It's also important to regularly review permissions and security settings to ensure only authorized individuals can access specific information.

Manage user and team accounts: It is important to ensure that all user and team accounts are up to date and that only authorized individuals have access to the team environment. This may include deleting user accounts for people who have left the company and creating new accounts for new employees.

Managing Channels and Content: It is important to manage the channels and content in MS Teams to ensure the information is relevant and up-to-date. This may include deleting unused channels and creating new channels to reflect projects that have developed.

Manage security and compliance: MS Teams includes many security and compliance features that enable admins to ensure data security and compliance. These include the ability to encrypt data, implement access controls, and create audit logs.

Manage Devices and Applications: It is important to manage the devices and applications used by the users to access MS Teams. This may include installing the latest updates to increase security and fix issues, as well as supporting and training users to ensure they are able to take full advantage of MS Teams features and resolve issues resolve that may occur. It is also important to ensure that the devices and applications used by the users are compliant with MS Teams requirements and compatible to ensure the team environment runs smoothly.

Manage MS Teams permissions

Managing permissions in MS Teams is an important part of running a successful team environment. It allows admins to have control over who can and cannot access specific content and features.

There are different types of permissions that can be managed in MS Teams, such as access permissions for specific channels, managing memberships in teams, and delegating tasks and responsibilities to other users.

Admins can manage permissions at the team and channel level by opening the settings for each team or channel and setting the desired permissions for the members. There is also the ability to assign roles to users who have specific permissions and responsibilities within the team, such as owners, members and guests.

It's important to ensure permissions are properly managed to ensure the security and integrity of team content and to ensure only authorized users can access specific content and features. It's also important to regularly review and update who has access to specific content to ensure permissions are always correct.

Delegated Access Rights

Delegated access rights allow administrators to give specific users the ability to perform specific tasks on behalf of other users. This can be very useful when it comes to simplifying MS Teams administration and increasing efficiency.

There are several types of delegated access rights available in MS Teams, such as the ability to create or edit calendar events on behalf of other users, the ability to send emails on behalf of other users, and the ability to manage contacts in the manage names of other users.

To grant delegated access rights, administrators must open the settings for each user and set the desired permissions. It is important to ensure that only trusted users are granted delegated access rights and that permissions are regularly reviewed and updated to ensure they are always correct.

It is also important to note that delegated access rights can also pose risks, such as the risk of abuse of privileges, and therefore should be used with caution, and use auditing and monitoring technologies to ensure delegated access rights used correctly and safely.

Access policies for MS Teams

Access Policies for MS Teams are rules that determine who can access specific content or features within the platform. These policies can be applied at different levels, such as organizational level, team level, or at the level of individual channels within a team.

There are different types of access policies available in MS Teams such as the ability to restrict access to specific content or features for specific user groups or roles, the ability to limit access to specific content or features for specific devices or locations and the ability to restrict access to certain content or features based on certain rules or conditions.

To create and apply access policies in MS Teams, administrators must first create and configure the required user roles and groups. They can then create the access policies and apply them to the desired level. It is important to ensure that policies are reviewed and updated regularly to ensure they are always accurate and in line with current requirements.

It is also important to note that access policies not only help to increase the security of MS Teams, but also help increase the efficiency of the platform by ensuring that only authorized users can access the required content and features .

4.Content Management

Manage documents and libraries

Managing documents and libraries in MS Teams is an important part of managing the platform. MS Teams offers various ways to create, organize and manage documents and libraries.

One way to manage documents in MS Teams is using SharePoint document libraries. These libraries allow users to store, organize, and share documents. Administrators can set permissions for each library to ensure only authorized users can access documents.

Another way to manage documents in MS Teams is to use OneDrive for Business. This feature allows users to store their personal documents in the cloud and access them from anywhere. Admins can also set permissions on OneDrive documents to ensure only authorized users can access the documents.

Another way to manage documents in MS Teams is to use cloud storage services like Dropbox or Google Drive. These services allow users to store documents in the cloud and access them from anywhere. Administrators can also set permissions on these documents to ensure only authorized users can access the documents.

It is important that admins regularly review and clean up the documents and libraries in MS Teams to ensure they are up-to-date, relevant and not taking up unnecessary space in the cloud. It's also important to regularly review and update permissions on documents and libraries to ensure only authorized users can access the documents.

Manage lists and tables

Managing lists and spreadsheets in MS Teams is an important part of managing the platform. MS Teams offers various ways to create, organize and manage lists and tables.

One way to manage lists and spreadsheets in MS Teams is using SharePoint lists. These lists allow users to store, organize, and share data. Administrators can set permissions for each list to ensure only authorized users can access the data. It is also possible to create forms to insert or edit data and create automated workflows to perform actions based on specific events.

Another way to manage lists and tables in MS Teams is to use Microsoft Excel. This feature allows users to create and manage complex tables and lists. Admins can also set permissions on Excel spreadsheets to ensure only authorized users can access the spreadsheets.

Another way to manage lists and spreadsheets in MS Teams is to use cloud-based spreadsheet tools like Airtable or Google Sheets. These tools allow users to create and manage spreadsheets in the cloud and access them from anywhere. Administrators can also set permissions on these tables to ensure only authorized users can access the tables.

It is important that admins regularly review and clean up the lists and spreadsheets in MS Teams to ensure they are up to date, relevant and not taking up unnecessary space in the cloud. It's also important to regularly review and update permissions on lists and tables to ensure only authorized users can access the data.

Manage web parts

MS Teams offers the possibility to insert web parts into a channel to extend the functionality of the team. Web parts are small applications that run in a MS Teams conversation and offer the possibility to provide additional information and functionality. There are different types of web parts, such as document libraries, spreadsheets, polls, calendars, and more.

To manage web parts in MS Teams, you must first select the channel where you want to put the web parts. Then click the "Add web part" button and select the desired web part from the list. Once the web part has been added, you can edit and customize it by clicking the "Edit" button.

It is also possible to manage permissions for web parts to ensure that only authorized users can access specific web parts. This can be done through the team's settings by setting permissions for individual users or groups.

It's important to regularly review and update the web parts to ensure they are working properly and contain the most up-to-date data. It's also important to remove redundant web parts to improve team performance.

Manage Content Policies

Content policies are rules used to control and manage the content in MS Teams. They can be used to block certain types of content to ensure only desired content is shared across teams. They may also be used to automatically categorize or tag content to make searching and finding content easier.

Content policies in MS Teams are managed through the Microsoft 365 Security & Compliance Center. Administrators can create, edit and delete policies there. There are different types of content policies, such as file type blocking rules, content auto-flag rules, and content monitoring rules.

When creating a content policy, admins can determine which users or teams the policy applies to and what actions to take when the policy is violated. For example, a policy can specify that certain types of files should be blocked when shared in a team and a notification should be sent to the admin.

It is important to regularly review and update the content policy to ensure it is current and appropriate. It's also important to monitor the impact of the policies on users and make adjustments as needed to improve the user experience.

5. Management of Communications

Configure chat and calling options

MS Teams offers a variety of chat and calling options that can be configured to improve communication in an organization.

Chat Options:

Chat notifications can be configured to receive notifications of new messages, @mentions, and reactions. These notifications can be on desktop, mobile, or via email.

Chat windows can be customized to control the view of messages, the display of emoji, and the use of markdown.

Chat history can be configured to include the number of days to keep messages.

Call options:

Call settings can be configured to automatically answer or reject calls, block or delegate calls, and control call notification display.

Calls can be made directly through MS Teams and there is also the option for calls to be forwarded to external phone numbers.

Calls can be recorded and there is an option to view or download the recordings later.

It is possible for calls to be made via external devices such as a headset or USB telephone.

It is important to note that some of these options may not be available to all users or organizations and there may be limitations when using calling and chat features depending on which MS Teams subscription is used. It's also important to set the right access rights and security configurations to ensure only authorized people have access to the chat and calling options.

Configure meeting options

Microsoft Teams offers a variety of options for configuring meetings. This includes the ability to prepare meetings by setting agenda items and sharing documents, as well as the ability to conduct meetings by using audio and video capabilities and managing attendees.

A key option is the ability to record meetings and later play back or share those recordings. You can also adjust the meeting settings, for example to disable chatting during the meeting or to enable the use of virtual backgrounds.

Another important option is the ability to schedule and organize meetings. This can be done for both regular meetings and ad-hoc meetings and includes the ability to send invitations to attendees, manage the attendee list and send reminders to attendees.

There is also the ability to configure security-related settings for meetings, such as the ability to restrict access to specific meetings or to enforce the use of meeting passwords.

Overall, Microsoft Teams offers a variety of meeting configuration options that allow meetings to be conducted and managed effectively and securely.

Configure video and screen sharing options

Microsoft Teams offers a variety of options for configuring video and screen sharing options, making it possible to conduct and manage meetings effectively and securely. Some of these options are:

Video Features: Microsoft Teams lets you customize video features like camera and microphone controls, screen size, and video resolution. There is also an option to add virtual backgrounds to protect privacy or to look more professional.

Screen sharing: Microsoft Teams makes it possible to share the entire screen or just a specific window while in a meeting. There is also the option to control sharing by turning sharing on or off or passing sharing to another participant.

Video recording: It is possible to start and stop the video recording of the meetings, this allows the meetings to be viewed and shared later.

Access Control: There is also the ability to configure access control for video and screen sharing options by allowing or blocking specific users or groups of users.

Overall, Microsoft Teams offers a variety of options for configuring video and screen sharing options that allow meetings to be conducted and managed effectively and securely, as well as protecting the privacy and professionalism of participants.

Manage communication policies

Microsoft Teams provides the ability to create and manage communication policies to control usage of features such as chat, calling, and meetings. These policies can be used to disable or restrict certain features for specific user groups or teams.

Communication policies are managed through the Office 365 portal or the PowerShell management shell. Before creating a policy, you must ensure that you have the necessary permissions.

There are different types of communication policies that can be created, such as chat policies, calling policies, meetings policies, and video and screen sharing policies.

Chat policies can be used to control the use of certain chat features such as emoticons, gifs, voice messages, and external chat participants. Calling policies can be used to control the use of calling features such as dialing numbers and the use of call recordings. Meetings policies can be used to control the use of meeting features such as the use of live closed captions and the use of recordings.

Video and screen sharing policies can be used to control the use of video and screen sharing features such as the use of live captions and the use of recordings.

Once a policy is created, it can be assigned to control specific user groups or teams. It is also possible to change or remove the policy later if necessary.

It is important that the right communication policies are created and maintained to ensure Microsoft Teams capabilities are being used properly and that company policies are being followed.

6.Security and Compliance Management

Configure security policies

MS Teams offers extensive options to ensure the security of the platform and the data stored on it. This includes, among other things, the configuration of security guidelines.

An important aspect is the ability to manage access rights for users and teams. Administrators can block or unblock certain functions or areas of the platform for certain user groups. They can also determine which users or teams can make changes to specific content.

Another important aspect is the ability to protect documents and content through encryption and access restrictions. Administrators can control who has access to what content and who can edit it. The option of two-factor authentication and the use of Azure Active Directory for identity management can also help increase security.

There is also the option of built-in security and compliance features, such as monitoring of chat and call logs, content archiving, and support for eDiscovery requests.

It is important that security policies are regularly reviewed and updated to ensure they are up to date and that the platform and its content are adequately protected.

Manage security alerts and events

MS Teams offers various ways to manage security alerts and events. One of the most important features is the ability to set up security notifications that are triggered by certain events, such as unauthorized access or changes to important settings. These notifications can be sent via email or SMS and contain information about exactly what happened and how to fix the problem.

Another important tool for managing security alerts and events is the Security and Compliance Report. This report provides detailed information about all security incidents that occurred in MS Teams, such as unauthorized access or suspicious activity. The report also contains recommendations for fixing problems and improving security.

There is also the ability to create and apply custom security policies that govern specific user actions or behavior. For example, a policy can specify that users are not allowed to share passwords in instant messages, or that all files containing a certain type of data must be automatically scanned.

There is also the option to monitor and record user activities in MS Teams. This can be useful to identify unwanted behavior or to understand user activities in case of an investigation.

In conclusion, managing security alerts and events in MS Teams is an important task to ensure users' data and communications are safe. There are many different tools and features that can be used to detect and fix security issues, as well as improve security.

Configure compliance policies

Microsoft Teams offers a variety of options for configuring compliance policies to ensure use of the service meets legal requirements and company policies. This includes the ability to enable or disable meeting and call recording to ensure compliance requirements are met.

Another option is to configure retention policies for chat messages and file attachments, which determine how long this data should be stored before it is automatically deleted. These policies can be applied to user groups or individual users.

It's also possible to perform eDiscovery searches to find and export specific content within Teams that may be relevant to compliance or legal issues.

There is also the option to configure auditing settings that determine which actions by users in Teams should be logged. These logs can be used to monitor policy compliance and monitor potential security breaches.

It is important to note that configuring compliance policies in Microsoft Teams requires a thorough knowledge of legal requirements and company policies and should be done in collaboration with legal and compliance professionals.

Manage compliance alerts and events

MS Teams offers a variety of ways to manage and monitor your organization's compliance policies. One of the most important features is the ability to create and manage compliance alerts and events.

Compliance alerts can be created to monitor specific activities or content related to MS Teams. This includes, for example, certain words or phrases contained in chat messages or emails, or files that are of certain types or sizes. Once such activity or content is detected, an alert is created and sent to the appropriate administrator.

Compliance events can be used to log and track specific activities or events related to MS Teams. This includes, for example, creating or deleting teams or channels, changing permissions for users or teams, or sharing files or content with external users.

To use these features, you must create and configure appropriate compliance policies. This can be done through the Microsoft 365 admin console or through PowerShell. It's important to ensure that the right users have access to the appropriate features to ensure your organization's compliance policies are applied correctly.

7. Management of integration and application options

Configure integration options (e.g. Office 365, OneDrive, etc.)

MS Teams offers the possibility to integrate various Office 365 services such as OneDrive, SharePoint and Exchange. To configure these integration options, the corresponding services must first be activated in Office 365. Subsequently, these services can be integrated into MS Teams via the settings menu.

OneDrive, for example, can be integrated with MS Teams to make files and folders accessible for a team or conversation. In order to integrate OneDrive with MS Teams, one has to go into the settings of MS Teams and select the "Integrations" option. Here you can select OneDrive and start the integration.

SharePoint can also be integrated with MS Teams to make team websites and document libraries accessible. In order to integrate SharePoint with MS Teams, one has to go into MS Teams settings and select the "Integrations" option. Here you can select SharePoint and start the integration.

Exchange Online can be integrated with MS Teams to make calendar, contacts and email accessible. In order to integrate Exchange Online with MS Teams, one has to go into MS Teams settings and select the "Integrations" option. Here you can select Exchange Online and start the integration.

There are also ways to integrate third-party tools like Trello, Asana, and many others. These integration options can be found through the Microsoft Teams app center.

It is important to note that the configuration of integration options should typically be done by an administrator to ensure that the integration options meet desired requirements and security policies.

Configure application options (e.g. PowerApps, Power Automate, etc.)

MS Teams offers the possibility to integrate third-party applications such as PowerApps and Power Automate. PowerApps enables users to create and manage their own applications based on data from Teams, SharePoint and other Office 365 services. Power Automate allows users to create and run automated workflows that synchronize data and actions between various Office 365 services and other applications.

To configure the application options in MS Teams, you must first ensure that you have the necessary permissions to add and manage applications. This typically includes the Team Admin role or a similar role with appropriate permissions.

After that, you can go to the application options in the MS Teams settings and add and configure the desired applications. This typically involves providing the required credentials and configuring permissions for users to use the applications. It is also possible to deploy applications to specific teams or channels and to restrict the use of applications by specific users or groups.

It is important to regularly review and manage application options to ensure applications are functioning properly and security and compliance requirements are met. It is also important to keep the applications up to date and ensure they are compatible with the latest versions of MS Teams and other Office 365 services.

Manage app permissions

MS Teams offers the possibility to integrate external applications and services to extend the functionality of the team. These applications can be added in the form of chatbots, add-ins or tab apps. To ensure security and control, permissions for these applications must be managed.

As an administrator, you can manage permissions for applications at the team and user level. You can control which apps are available to specific users or teams, and what permissions those apps have. For example, you can specify that a specific application has read-only access to specific data, or that an application may only be used by specific users.

There's also the ability to create something called "app management policies," which you can use to set rules that apply to all applications within your organization. For example, this can prevent the use of third-party applications or the use of certain applications in certain areas of your organization.

It is important to carefully manage permissions for applications to ensure data security and compliance requirements are met. It's a good idea to periodically review and update permissions to ensure only authorized applications are being used and that those applications only have the required permissions.

8.Monitoring and Troubleshooting

Configure monitoring options

Microsoft Teams offers a range of monitoring options that allow admins to monitor and analyze usage of the platform. Some of these options include:

Activity Reports: This feature allows admins to generate detailed reports on how Teams is used in their organization, including details on chat and call activity, meetings, file associations, and more.

User activity: Admins can get detailed information about individual user activity in Teams, such as when a user logged in, how many chats they started, and how many files they uploaded.

Compliance Monitoring: This feature allows admins to monitor whether the content in Teams meets their organization's compliance requirements.

Event logs: Admins can search event logs to get details about specific actions in Teams, such as file associations, instant messages, calls, and meetings.

Notifications: Admins can receive notifications when certain events take place in Teams, such as when a user sends an inappropriate chat or when a user uploads a file that violates compliance guidelines.

To configure these monitoring options, admins must first access the Teams admin console and then make the appropriate settings for the desired monitoring options. It may also be necessary to configure special roles and permissions for users to ensure only authorized individuals can access the monitoring data.

Manage logs and reports

MS Teams offers a variety of options for managing logs and reports. One way is to use the "Teams and Chats Log" which provides a record of all activity in a team or chat. This includes messages, calls, meetings, file shares and much more. It can be filtered by specific time periods, users or activities to find relevant information faster.

Another option is to use the "Activity Report" which provides information on MS Teams usage in an organization. This includes the number of active users, the number of meetings and calls, use of chat and file shares, and much more. These reports can also be exported for use in other applications or for further analysis.

There is also the ability to create custom reports that combine data from MS Teams with other data sources in Office 365 for a better understanding of MS Teams usage and impact on the organization.

It is important that the maintenance of logs and reports is monitored and reviewed regularly to ensure all required information is available and to quickly identify and resolve potential problems.

Troubleshoot problems

Troubleshooting MS Teams issues can be a complex task depending on the type of issue. One of the first steps in troubleshooting should be to accurately describe and replicate the problem. This will help determine the cause of the problem and find the right solution.

A common problem that can appear in MS Teams is poor performance or connection issues. This can be caused by poor internet connection or network issues. To troubleshoot this issue, it may help to check the network settings and make sure the correct ports are open.

Another common problem that can occur in MS Teams is a login issue. This can be caused by credential issues or authentication issues. To troubleshoot this issue, it may help to check the login details and make sure they are correct. It can also be helpful to check the authentication settings and make sure they are correct.

Another common problem that can appear in MS Teams is a collaboration issue. This can be caused by document sharing issues or real-time collaboration issues. To fix this problem, it may help to check the sharing settings and make sure they are correct. It can also be helpful to review the real-time collaboration settings and make sure they are correct.

There are many more issues that can occur in MS Teams and troubleshooting can vary depending on the issue. It's important to accurately describe the problem and follow the correct troubleshooting steps to resolve the issue. It is also important to review Microsoft documentation and, if necessary, seek support from Microsoft or a qualified IT service provider to resolve issues quickly and effectively. It can also be helpful to use the user feedback feature in MS Teams to report problems and find solutions. It is important to regularly backup and update the system to avoid potential problems.

9.Upgrades and Migrations

Upgrade to newer versions of MS Teams

Upgrading to a newer version of MS Teams is an important part of managing and maintaining the system. It offers new features and improved security features that make it possible to improve productivity and collaboration. There are several ways how to update MS Teams. One way is to use Microsoft's Update Assistant. This wizard guides the user through the update process and ensures that all required steps are completed. Another option is to use PowerShell commands. This allows the IT team to run the upgrade automatically and integrate it with the existing management solution. It is important to have a test environment ready before upgrading to the production environment. This allows the IT team to test the impact of the upgrade on users and business processes before implementing it in production. It is also important to review Microsoft's documentation and, if applicable, follow the upgrade instructions to ensure the upgrade is successful.

Migrate from older versions of MS Teams

Migrating from older versions of MS Teams can be a complex process that requires careful planning and execution. An important step in migration is identifying the existing configurations and settings to ensure they can be carried over to the new version.

It is important to check the compatibility of the plug-ins and add-ons used as they may not be supported in the new version. Likewise, it's a good idea to review UI customizations and user profiles to make sure they work in the new version.

Another important step in migration is conducting tests to ensure that all features and processes are working as expected. This can be done through the use of test user accounts and test data. It's also important to check Microsoft's documentation and instructions to ensure all steps are performed correctly.

When the migration is successfully completed, it is important to train users on the new version of MS Teams and ensure they are familiar with the new features and settings. It's also important to monitor performance and user adoption to ensure the migration was successful.

Migrating from other team-based platforms to MS Teams

If you're looking to migrate to Microsoft Teams from another team-based platform like Slack or Zoom, there are a few steps you need to take to ensure a successful migration.

Planning: Before you start the migration, you should create a detailed plan that includes the steps you need to take to migrate the data from the legacy platform to Microsoft Teams. This plan should also include the migration schedule.

Data conversion: You need to ensure that the data you want to migrate from the old platform is converted to a format supported by Microsoft Teams. This can be done using tools like the Slack to Microsoft Teams migration app.

User accounts and permissions: Before you migrate the data, you should ensure that all user accounts are set up in Microsoft Teams and have the correct permissions.

Data migration: Once the data has been converted and the user accounts have been set up, you can start the actual migration. This can be done using tools like the Microsoft Teams Migration Center.

After the migration: Once the migration is complete, you should review the data and user accounts in Microsoft Teams to make sure everything migrated successfully. It is also important to inform users about the changes and help them get used to the new platform.

It is important that you follow the steps carefully and in the correct order to ensure that the migration is successful and user productivity is not impacted. It can also be helpful to hire a Microsoft certified partner to ensure the migration is completed successfully.

10.Advanced Configurations

Configure MS Teams-Federated Sharing

MS Teams Federated Sharing allows users to share their team and channel content with other companies or organizations also using MS Teams. To configure MS Teams Federated Sharing, you must first ensure that the correct prerequisites are met. This includes using Azure Active Directory (Azure AD) and using MS Teams in the same Office 365 tenant.

Next you need to configure the right permissions for the users who want to share content. Typically, these users must have the Team Member or Owner role to share content. It's also important that users have the necessary permissions for the libraries and documents they want to share.

Once permissions are configured, users can share content with other companies or organizations by generating a link to their team or channel content. This link can then be sent to the external users who have MS Teams account and permissions to view the content.

It is important to note that MS Teams Federated Sharing is an advanced feature and there are certain limitations and requirements that must be met in order to use it successfully. It is therefore recommended that you read the Microsoft documentation carefully and seek help from a qualified IT professional if necessary.

Configure MS Teams hybrid scenarios

MS Teams hybrid scenarios enable companies to combine the benefits of MS Teams cloud-based communication and collaboration tools with their existing on-premises infrastructure. To configure a hybrid scenario, some preparations must first be made.

First, it must be ensured that the company has an up-to-date version of MS Teams and a supported version of Exchange, Skype for Business and/or SharePoint. Second, the necessary network and security configurations must be made to establish a secure connection between the cloud and the on-premises environment.

After the preparations are complete, the actual configuration of the hybrid scenario can begin. This includes setting up connectors between MS Teams and the on-premises systems, configuring policies for data sharing and identity synchronization, and setting up security features such as two-factor authentication and encryption.

It is important that the configuration of MS Teams hybrid scenarios is performed by experienced IT professionals as it is a complex process that involves taking many different factors into account. It is also important to conduct regular monitoring and testing to ensure configuration is correct and that security and compliance requirements are being met.

Configure MS Teams archive mailboxes

MS Teams archive mailboxes allow admins to remove old or unused Teams conversations and content from the user's primary mailbox and move them to a separate location. Here are the steps required to configure MS Teams archive mailboxes:

Make sure you have the correct permissions to configure archive mailboxes. This typically requires assignment of the Exchange Administrator role or a similar role with appropriate permissions.

Navigate to the Microsoft 365 admin center and select the "Users" option.

Select the user for whom you want to configure an archive mailbox and click the "Edit" button.

In the user profile, scroll to the "Email Options" section and check the "Enable Archive Mailbox" option.

Specify the location for the archive mailbox. This can either be an existing Mailbox container or a new container that you create.

Select the desired options for the archive mailbox, such as retention policies or the ability to search the archive mailbox from Outlook.

Click "Save" to apply the changes.

Verify that the archive mailbox was successfully configured for the user by logging into the user's mailbox and ensuring that an archive folder exists.

It is important to read Microsoft's documentation carefully and, if necessary, to contact the support team if problems arise. It's also important to regularly monitor archive mailboxes to ensure they are functioning properly and that data is being stored securely and in accordance with compliance requirements.

Configure MS Teams compliance options

MS Teams offers a variety of compliance options that enable administrators to ensure that communications and content within the platform comply with applicable legal and corporate requirements. Some of the key features and settings that can be configured by admins to ensure MS Teams compliance include:

Retention Policies: Administrators can create retention policies to regulate the retention of content and messages for a specific period of time. This allows critical information to meet compliance requirements to be retained while unnecessary content is automatically deleted.

In-Place eDiscovery & Legal Hold: Administrators can use In-Place eDiscovery and Legal Hold to identify and secure specific content and messages relevant to compliance or legal needs. This allows that content not to be deleted even when retention policies are applied.

Auditing: Administrators can configure auditing settings to record and monitor activity within the platform. This enables potential compliance violations to be identified and prosecuted.

Data Loss Prevention (DLP): Administrators can configure DLP settings to prevent sensitive information from being inadvertently shared. This can be done, for example, by creating DLP policies that block certain types of content or file attachments being sent in chats or meetings.

Azure Information Protection: Administrators can use Azure Information Protection (AIP) to automatically classify and protect content within MS Teams. This can be done, for example, through the use of AIP policies that automatically encrypt or watermark certain types of information.

It is important to note that the specific configuration of MS Teams compliance options depends on the specific compliance needs of the company and the industry. Administrators should therefore take sufficient time to understand the specific requirements of their company and make the appropriate settings in MS Teams. This includes things like configuring retention policies for chat and call logs, setting compliance tags for specific types of data, setting up notifications of compliance violations, and the ability to export data from MS Teams to use for compliance audits to provide.

It is also important to regularly monitor compliance guidelines and make adjustments where necessary. Working closely with the company's compliance team and using tools to monitor and analyze user activity can help ensure MS Teams is configured and managed in accordance with the company's compliance needs.

imprint

Author: Michael Lappenbusch

E-mail: admin@perplex.click

Homepage: https://www.perplex.click

Release year: 2023