Confidentiality and Data Protection in Microsoft Teams

Microsoft Teams is the hub for teamwork in Microsoft 365. It enables instant messaging, online meetings with audio and video calling support and offers extensive web conferencing capabilities. In addition, Teams provides file and data collaboration and on-line storage. For core productivity scenarios Microsoft Teams relies heavily on online services like SharePoint and Exchange Online. Data shared via Teams is stored in SharePoint and can be accessed from virtually any device and from anywhere. Stored in the cloud, it is exposed to greater risks and therefore needs extra protection. Client-side encryption is a viable means of ensuring protection of data stored in hosted environments such as Microsoft Teams and SharePoint Online.

How can you protect data with conpal LAN Crypt?

conpal LAN Crypt is a client-side encryption solution that provides file-level encryption. Its powerful key and policy management functionality supports encryption of data using different keys for business, personal and shared data. Encryption and decryption take place on the endpoint. Hence, data is protected on the local machine, when it leaves the client, and in transit. No software hosted on Microsoft cloud servers nor anyone else has access to the plaintext data or to the key used for encryption. conpal LAN Crypt helps organizations keep their data secure and confidential even in cloud-hosted environments.

Admin

Define Rule(s) for encryption of 'Microsoft Teams' folder

A single rule applied the root of the local sync-folder is sufficient. If necessary, rules with different keys can be defined for individual Teams channels or even sub-sections of a channel.

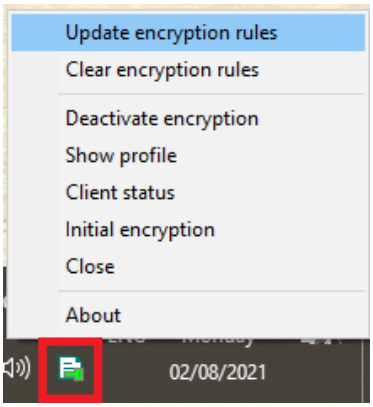
Client

Please follow the steps below to enable conpal LAN Crypt encryption support for Microsoft Teams on the local workstation.

conpal LAN Crypt Client

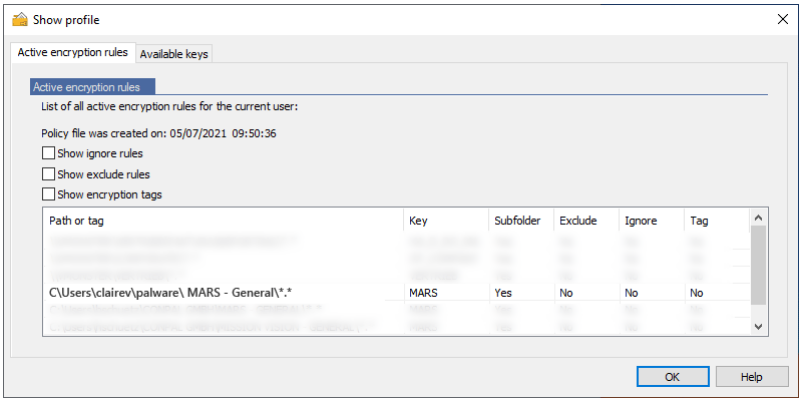
Refresh policy

Right-click on the conpal LAN Crypt icon in the System Tray and select 'Update encryption rules'.



Verify policy (optional)

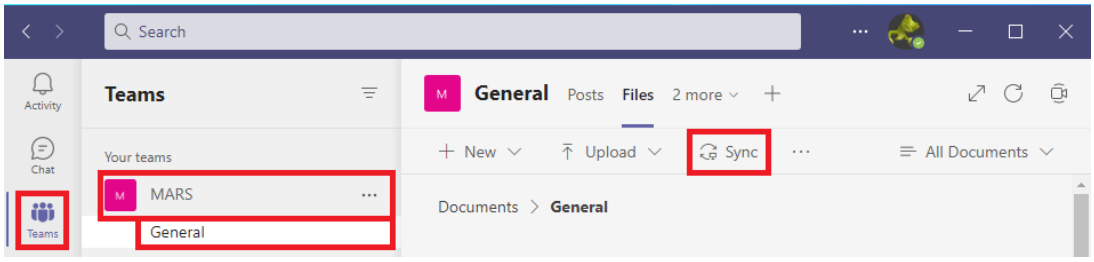
Double-Click on the conpal LAN Crypt icon in the System Tray, or Right-click on the icon to select 'Show Profile'.
Verify that the profile contains at least one encryption rule for the local sync folder.



Microsoft Teams

Local Sync has to be enabled for each Teams channel that you want to use encryption for.
To activate encryption for a specific channel, take the following steps in your Teams app:

1) navigate to the **Navigation Bar**
2) select the '**Teams**' space
3) navigate to the **Site** and select the **Channel** you want to encrypt
   (in our example below, we want to enable encryption for the 'General' channel of the 'MARS' team)
4) Press the '**Sync**' button to start synchronization to your local machine for this channel

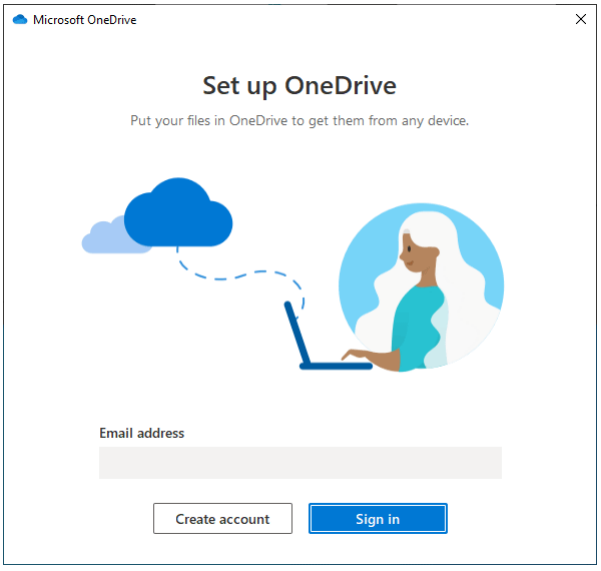


Please repeat this step for every channel you want to have encrypted.

Important:
Your site has to be set up to sync with the OneDrive sync app. If you're the IT admin for your organization, see "Let users sync SharePoint files with the new OneDrive sync app". If you're not the IT admin, and your screens don't look like the ones in this article, see "Sync SharePoint files with the OneDrive sync app (Groove.exe)", or else contact your IT department.
For further details please check the Microsoft documentation "Sync SharePoint and Teams files with your computer" (microsoft.com)

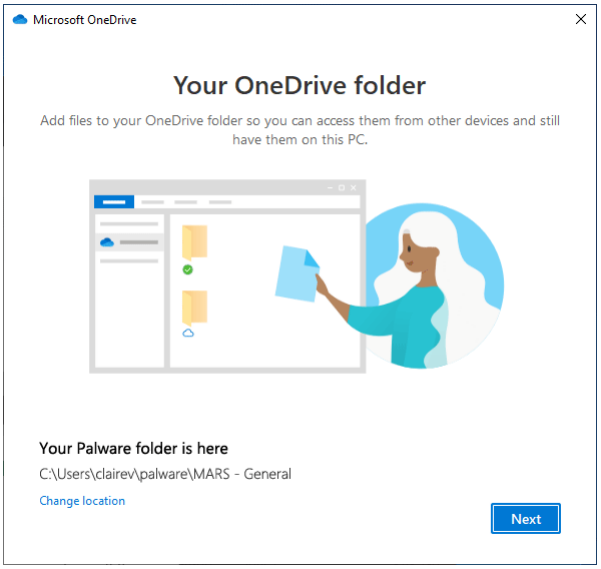
Microsoft OneDrive

Microsoft Teams uses Microsoft OneDrive to synchronize data between the cloud and the local machine. If you have not yet set up OneDrive on your machine, you will have to do so. Please follow the steps prompted by the software.
Once OneDrive is installed, specify the account you want to use to connect to OneDrive. Use the same account you use in Teams.

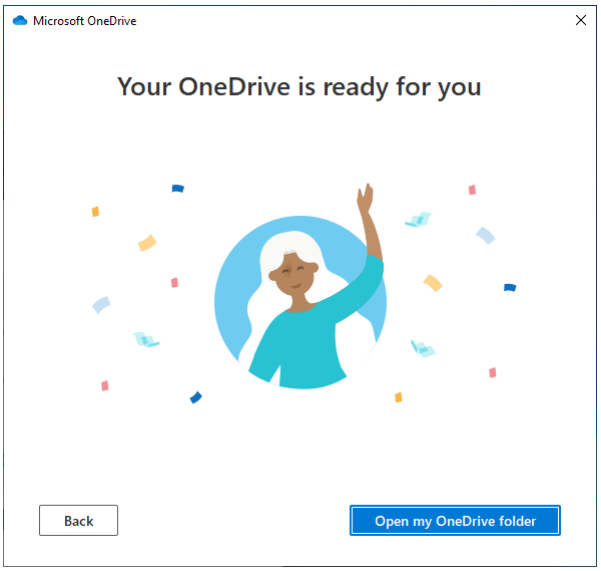


Note: This dialog is only shown if OneDrive has not been set up and configured on your machine yet.

Next, specify the location of the local sync folder. Please make sure that you use the same folder as specified by our Admin in your conpal LAN Crypt profile.

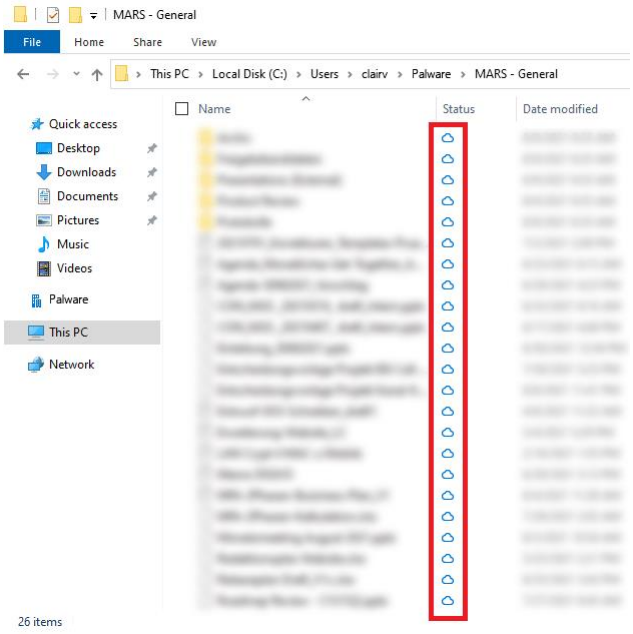


Follow the wizard and you'll soon be ready to go.



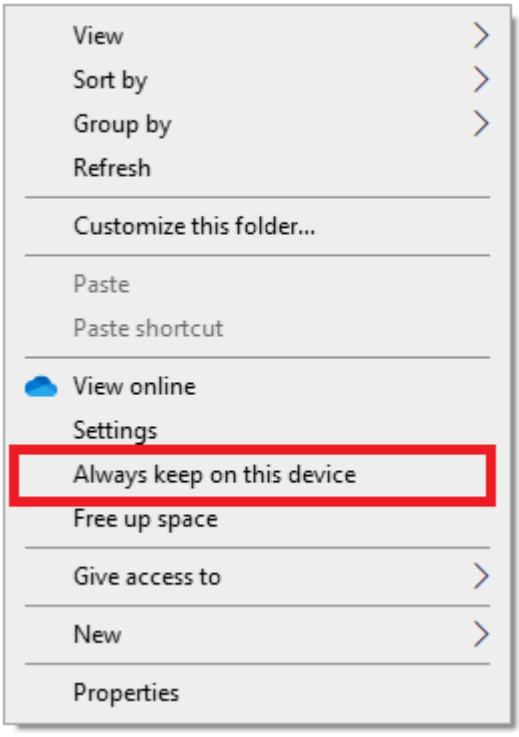
File Explorer sync status

Almost there! Teams is now connected to OneDrive and OneDrive has a connection to your local sync folder. You should now check whether your files have been synced. To do so, navigate to the sync folder in File Explorer. The 'Cloud' symbol next to a file entry indicates that the file is only available in the cloud, and thus isn't synchronized.

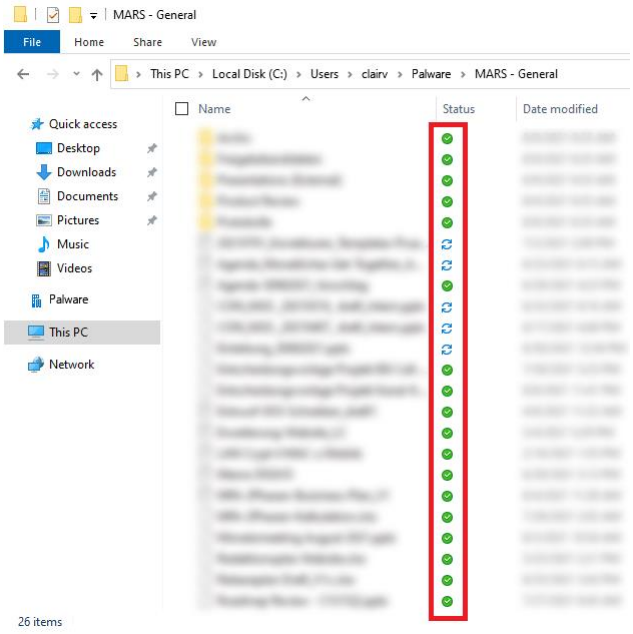


Trigger Sync / Always keep on this device

You need to trigger the synchronization to get the files downloaded to your local machine.
In Windows Explorer, select the top-level folder you work with, open its context menu by right-clicking on it, and select '**Always keep on this device**.'



This triggers the initial synchronization. A green checkmark next to a file indicates that the synchronization is complete and the file has been downloaded to your machine.



Done!

Congratulations! You have just enabled file encryption for Microsoft Teams. It wasn't that hard, was it?

You can now open and edit documents locally using your favorite productivity apps. As for any files protected by conpal LAN Crypt, any changes you make on your local device are automatically encrypted and stored.

Known Limitations

Some limitations apply to conpal LAN Crypt's functionality within Microsoft Teams.

Local App support only

Encrypted files can only be opened with the registered productivity app (e.g. Word, Excel, PowerPoint...) running on your local workstation. Opening of encrypted files from within Teams or the browser is not supported.
We recommend: Open all files within the local productivity app.

Default: Global 'Open in Local App' not supported

Teams allows to specify the default action for opening a file. By default, files will be opened within Teams, but this option can be changed to 'Open in Local App'. If so configured, a double-click on a file would automatically launch the local productivity app and have the file opened in this app. This allows for working with encrypted apps directly from within Teams.

Latest versions of Teams seem to ignore this setting and always open the document in Teams itself. We have no information whether this is a bug or a desired change in the product.

Although not the most convenient option, one can still open encrypted documents right from within Teams using the 'Open in App' Option in the context menu/menu bar.

We recommend: Manually open all files within the local productivity app.