Security / Architecture

Permissions Needed on the Windows Machine

The agent can be installed by a standard user. No administrative rights are needed to install the agent. No special firewall or antivirus exceptions are needed.

Credential Security

The agent application does not save, transmit or use the user's Microsoft 365 credential. The agent operates using a delegated permission model and never has access to the user's credential. In most enterprise scenarios, the agent will silently authenticate when the user is logged in. If authentication is required, the user will authenticate directly with either Microsoft, your company's on-premises ADFS server or your 3rd party identity provider.

File Storage on the User's Device

The agent is not designed to store data locally under normal operation. However, it can store temporary files on a user's machine if connectivity to Microsoft Azure is limited. This temporary data does not contain display names, usernames, email addresses, passwords, or any other sensitive information. Regardless of the anonymized nature of this data, it is encrypted at rest. All data gathered by the agent is encrypted from inception until successful transmission to our SaaS platform. This includes in-memory, during transmission, and while at rest.

Network Communications

When testing Microsoft services, the agent is designed to connect to the same endpoints as your user's Microsoft 365 applications. By design, our agent will operate in the same manner as a Microsoft 365 application and communicate with any of the IP ranges and hosts required by Microsoft. Microsoft publishes their up-to-date list here: https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

In addition to the standard endpoints used with Microsoft Apps and services, the agent will also need to access our Microsoft Azure based service. This endpoint can vary depending on the location of your data:

Data Security in Transit

All communications with our API maintain the following standards:

- Communications only take place over SSL/TLS (TLS 1.2) secured connections
- Communications require an authenticated connection from the agent on the client machine
- The payload for all communications is encrypted separately from, or in addition to, the SSL/TLS layer

Data Retention

By default, the data retention is set for 6 months. On request this can be further reduced.

Data Privacy

Please read our Data Privacy here: Data Privacy

Child pages: