

Communication & Network Security

Network diagram

In order to prepare your organization's network for SalesTim, here is an overview of the the different network flows involved:

This diagram is comprised of three forms of traffic.

Regular Microsoft Teams flows (Purple lines)

The Microsoft Teams client has two main flows, one for authentication against your Azure AD and one for Microsoft API.

The flows are not impacted by SalesTim.

SalesTim's internal flows (Orange lines)

These flows are entirely internal to SalesTim and have no impact on your network infrastructure.

Flows between your organization's network and the SalesTim platform (Green lines)

All the traffic from and to the SalesTim platform uses HTTPS protocol on port 443.

Here is a short description of each flow: 1. *.salestim.io for the main app*, *.salestim.com* for online help contents 2. *.msecnd.net* and *.visualstudio.com* for performance metrics analysis 3. *.windows.net* for blob cache storage 4. *.microsoft.com* for Microsoft Graph API access

Traffic encryption

All the traffic from and to the SalesTim platform is encrypted (and HTTPS protocol enforced), using TLS v1.2, ensuring secure communication between our customers and our platform. To do so, we're using Azure Front Door as the only entry point to the app (web apps and API).

You can review online our latest Certificate Report

::: tip Online SSL Test You can see a detailed report of our SSL certificate using this free online service that performs a deep analysis of the configuration of our SSL:

Launch Qualys SSL Server Test :::

DDoS prevention

While we've prevented rogue traffic from accessing our servers and network, it's still possible for external services to block anyone else from using our service by creating a distributed, denial-of-service attack.

To prevent this, we're using Azure Traffic Manager as a first level of protection.

Learn more about Azure Traffic Manager

Domains whitelisting

We understand that our customers need to be confident that they are communicating with SalesTim in a secure environment. Domains whitelisting is one of the most effective methods of ensuring this and prevents any internet traffic intended for SalesTim from being hijacked or rerouted to a rogue website.

Our complete portfolio of domains are outlined below to help our customers configure their corporate web proxy.

::: tip Note This information is subject to change and we recommend that you check back quarterly for the addition of new domains. :::

SalesTim Web App

- Domains/Hosts: ***.salestim.io**
- Justification/Purpose: SalesTim main web application for Microsoft Teams

SalesTim Help Center

- Domains/Hosts: ***.salestim.com**
- Justification/Purpose: SalesTim Help Center embedded into the Microsoft Teams app

Microsoft Azure Application Insight

- Domains/Hosts:
 - **az416426.vo.msecnd.net**
 - **dc.services.visualstudio.com**
- Justification/Purpose: Azure service used by SalesTim to collect anonymous performance metrics, telemetry and application logs/traces. More infos

Microsoft Azure Blob Storage

- Domains/Hosts: **stappsaprd.blob.core.windows.net**
- Justification/Purpose: Storage used by SalesTim to store templates pictures/icons

Microsoft Graph API

- Domains/Hosts: **graph.microsoft.com**
- Justification/Purpose: API used by SalesTim to interact with Microsoft 365 services

Intercom

- Domains/Hosts:
 - ***.intercom.com**
 - ***.intercom.io**
 - ***.intercomassets.com**
 - ***.intercomcdn.com**
- Justification/Purpose: Used by SalesTim to bring an embedded support system into the app, and connect end-users and administrators with our support team.