Official Information: How to connect to eXtollo

ToC:

1. Connect users to eXtollo

When ITx and BUs are new to eXtollo they are facing 2 separate environments. Hence, one environment is the already used Daimler Corporate Network.

The other one is the eXtollo environment which is based on Microsoft Azure.

blocked URL

If ITx and BU users (e.g. Admins, Data Science Users) want to access eXtollo, they need a way to connect through their already used and existing Daimler network to the new eXtollo cloud network. This works with the Hypertext Transfer Protocol Secure better known as (https). By using this protocol Users can access the World Communication Platform (WCP) hosted in Daimler's European Data Center (EDC). Afterwards, WCP connects via the Remote Desktop Protocol (RDP) to the Daimler Hybrid Cloud (DHC) from which users can access their eXtollo Azure region via a Virtual Private Network (VPN) and use the eXtollo Cloud GateWay (CGW) to finally reach their Virtual Data Science Environment. This process was designed to be as easy and user-friendly as possible and to be in line with Daimler global security standards.

blocked URL

A proper VPN connection is crucial in the described connectivity setup to eXtollo. Currently, the VPN setup is carried out by ITI.

2. Steps to VPN setup

blocked URL

Benefits of a VPN connection are:

- Secure way of transferring data between Daimler Data Center and secured Cloud Gateway (CGW) in the Azure cloud
- Convenient and secure access to cloud resources for Data Science and Analytics workers

3. Connect Data to eXtollo

If data sources should be made available in eXtollo, the previous described environments remain the same. Data has to be transferred from the Daimler environment to the eXtollo cloud environment (end-2-end).

blocked URL

Data flows via the Internal Secure Network (ISN) and a set of firewall rules to the Service Zone (SVC) of the Integration Runtimes (IRs) which are in the responsibility of the local ITx unit. Data flow from Data Source to IR depends on the respective data source location and is handled during the data source onboarding. The data is then forwarded to the DHC and enters via the previously described VPN connection the CGW in Azure which will be all defined during the source onboarding process by the eXtollo Data Lake team.

Firewalls and routings are critical to enable user and data access in eXtollo and provide all users of eXtollo Daimler security standards. Here are the most important points:

- Logon permission on IRs (Daimler DC internal) handled via AD-Groups + AD-Users
- Access to Azure infrastructure requires Developer Cloud Accounts
- Logon permission on DSVM handled via local provisioned accounts
- Azure DevOps (VSTS, build pipelines, one-click deployment capabilities, etc.) is highly recommended, but not mandatory
- Users from DCN connecting to WebApps and API gateway

blocked URL