Workbench User's Guide

Network and Security Considerations

4/13/2025

Contents

Network and Security Considerations

Security Considerations

Login Authentication Requirement

- Workbench uses Genesys Configuration Server authentication.
- To login to Workbench, each user needs a valid Configuration Server User Name and Password with Read and Execute permissions to use the Workbench Client (i.e. "WB9_Client") application.

Network Considerations

Data ingested by Workbench (including Alarm, Changes, Channel Monitoring and Metric events) from the Genesys Engage platform is stored locally in the customer environment; the customer is responsible for protecting this data.

Outbound Network Connectivity Requirements (Remote Alarm Monitoring (RAM) Subscribers)

In some customer environments, outbound network connectivity is restricted. If you subscribe to the Remote Alarm Monitoring (RAM) service from Genesys Care, you will need to enable minimal connectivity for Workbench to send alarms from the Remote Alarm Monitoring service to Genesys for processing. This processing includes routing alarms to Genesys support analysts and displaying alarm notifications in the Genesys Care Mobile App.

The outbound connectivity should allow connectivity from the Workbench host/server to "alarm.genesys.com" (208.79.170.12) on port 443; you may need to engage your networking or security team to enable this connectivity.

> **Important**
>
> - This Remote Alarm Monitoring connectivity requirement only applies if you are using the Remote Alarm Monitoring Service with Workbench.