Group Calendar

Technical Documentation
OnTime® Group Calendar for Microsoft
ver 1.x revision 1

IntraVision

OnTime® Group Calendar for Microsoft
Version 1.x

Disclamer

This document contains preliminary information about software still under development and is subject to change without further notice.

The content of this document is confidential and may not distributed without explicit permission.

The language in this file is according to en-US culture

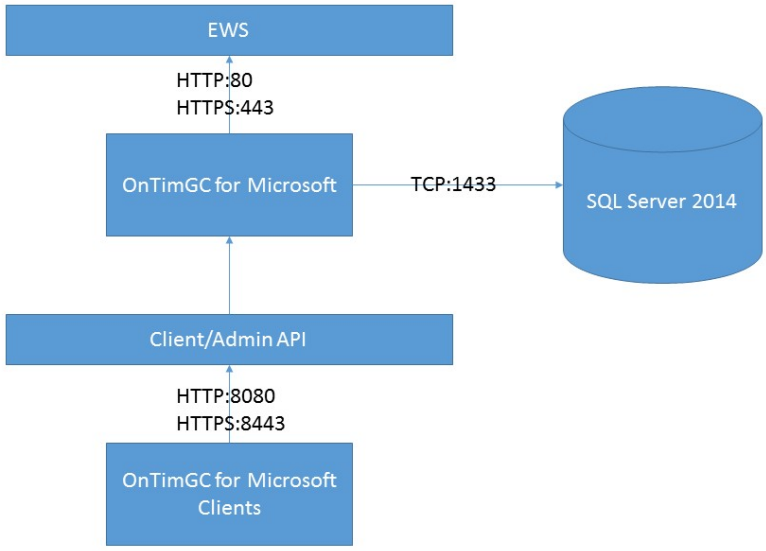
Table of Contents

Overview

Current version

Current version supports a single EWS endpoint – this may On Premise or an Office365 Cloud.

Architecture



The arrows show direction of connection and illustrates that no inbound connections are necessary from the Exchange EWS service.

Components

EWS

OnTimeGC for Microsoft supports Exchange Office 365, Exchange 2013, and Exchange 2010 SP 2 Exchange Web Services.

Prerequisites

Application Impersonation

OnTimeGC for Microsoft requires a Mailbox user designated the Application Impersonation Role exists on the server for operation.

This is due to Exchange requirements that only mailbox users can resolve Exchange addresses needed for OnTimeGC for Microsoft directory synchronization.

A future version using AD/Azure AD as directory source MAY relax on this requirement.

Inclusion Groups

OnTimeGC for Microsoft requires that a number of Distribution Lists which may be nested to any level exist on the Exchange server containing all addresses of users eligible for OnTimeGC for Microsoft inclusion.

This is due to the absence of an Office 365 GAL but will also be required for On Premise solutions.

A future version using AD/Azure AD as directory source MAY relax on this requirement.

Serviceability

NTLM

NTLM is supported for the EWS connection, however invalid credentials will be transformed to a valid set of credentials designating the OnTime Delivery Service user.

The implication of this is that if somehow the OnTime Application user credentials is invalidated on an Exchange Server using NTLM OnTimeGC for Microsoft may fail silently

Java Sockets and Hanging HTTP Requests

While HTTP was originally designed for requests with immediate responses OnTimeGC for Microsoft uses HTTP requests that may not be responded to by EWS for up to 30 minutes.

This is not normally a problem but since Java Sockets do not offer granularity to specify individual TCP keep-alives, QOS must be guaranteed from the Network Provider. A faulty router may cause OnTimeGC to fail silently.

I believe this to be a flaw in the design but until a different technology allowing better granularity is adopted it is up to the Network Provider to ensure QOS.

Vulnerability

Current version stores the Application Impersonation UPN/Password in plain text on the OnTimeGC for Microsoft server file system this MUST and WILL be changed in future versions.

SQL Server

OnTimeGC for Microsoft supports SQL Server 2014. For initial deployment SQL Server 2014 Express Advanced without Reporting Services or Full Text Indexer installed on the OnTimeGC application server is recommended.

Prerequisites

.Net 3.5 SP1

SQL Server requires .Net 3.5 SP1 to be enabled on the server

TCP/IP

Microsoft JDBC driver 4.1 only supports TCP/IP so TCP/IP must be enabled on the SQL Server 2014.

In addition some Instances also requires that SQL Server port are explicitly bound to port 1433

API Login

Both SQL Server login and Microsoft Integrated security are supported. A login must be bound as User on the OnTimeGC for Microsoft Database with the API Role assigned.

Vulnerability

In current version the SQL Server Connection String is stored in plain text on the OnTimeGC for Microsoft Application Server. This MUST and WILL be changed in a future version.

This means that if SQL Server Authentication is selected the username/password can be read from the configuration file. However if the API Login is correctly configured with the API Role the only Stored Procedures in API schema of the OnTimeGC for Microsoft Database could be accessed.

If username/password may not be stored in plain text Integrated security should be chosen as Authentication method.

By requiring that all access to the databases are through the api schema stored procedures the database is effectively shielded from Injection attacks.

OnTimeGC for Microsoft

Prerequisites

OS

OnTimeGC for Microsoft only supports Windows 2012 Server and Windows 2008 R2 Server and only for 64-bit platforms.

Due to security functions needed by Microsoft JDBC/JCIF Driver Itanium architecture microchips are not supported.

OnTime Delivery

The basic platform for OnTimeGC for Microsoft is OnTime delivery that consists of a modified and value-added Java Server runtime and a modified and value-added Tomcat.

The only platforms supported are those that are supplied with OnTime Delivery. The reason for this is that Java is not fully platform independent.

Java Server Runtime

Current version jdk1.8.0_25.

The java runtime supplied with OnTime Delivery is the only runtime that may be used for OnTimeGC for Microsoft.

This version is supplied by IntraVision and can coexist with other versions on the server.

Tomcat

Current version is Tomcat-8.0.14.

This version is supplied by IntraVision and is the only tomcat version supported for OnTimeGC for Microsoft.

Vulnerability

Current version relies on Form based pass-through Authentication against EWS.

This means that username/password is sent as plain text to the OnTimeGC for Microsoft API.

Therefore the OnTime Delivery Tomcat SHOULD have HTTPS enabled and SHOULD have HTTP disabled and the Exchange EWS SHOULD have HTTPS enabled to prevent sniffing of credentials internally.

How to enable HTTPS on Tomcat/IIS is not covered by this document.

Future versions WILL support Windows Integrated Security using an On Premise native Windows HTTP Server API service where credentials are never sent to OnTimeGC for Microsoft. This will both allow SSO and remove the need for HTTPS on the OnTime Delivery Tomcat.