A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

Security Considerations

Release 9.7
Document Version 1.0

January 2024

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

®,™ Trademark of Mitel Networks Corporation

Contents

INTRODUCTION

This document describes how the MiCC Enterprise contact center system can be configured to secure access to the system and how data in transit can be protected via encryption.

SCOPE

MiCC Enterprise is a very open, flexible and highly customizable platform, and is in many instances integrated to Case Management, CRM/ERP and/or recording systems. This document will limit the scope to the MiCC Enterprise system itself.

ACCESS TO THE SYSTEM

MiContact Center Enterprise consists of services and clients that run on the Microsoft Windows platform as well as some Web applications that runs in standard browsers such as Chrome and Firefox.

It is up to the customer's IT department to secure the access to the server using the standard tools and procedures. Documentation in the MiCC Enterprise documentation library specifies the port numbers that need to be opened up in the Windows firewall in order to allow communication to and from these server(s).

ACCESS TO MICC ENTERPRISE APPLICATIONS

There are two different ways to manage user's access to the MiCC Enterprise applications. The MiCC Enterprise system can be integrated with Active Directory, both on prem and Azure hosted) or the system will use its own integrated user and password managent functions

Active Directory based user management

The MiCC Enterprise system can be configured to synchronize users with Active Directory (AD). This is achieved by creating a Group in AD and then when users are added or removed from this Group they are added or removed from being a user in MiCC Enterprise.

For detailed information on how to configure AD synchronization refer to the document "Advanced Configurations" in the user documentation library.

Single Sign On

Single Sign ON (SSO) can be enabled by integrating the MiCC Enterprise system with an eternal Identity Provider (IDP). Typically, this would be enabled when the system is configured to use Azure or on prem AD user management, but any IDP supporting Open ID Connect can be used.

For detailed information on how to configure Single Sign On refer to the document "Advanced Configurations" in the user documentation library.

Integrated User and Password Management

Access to all MiCC Enterprise applications is restricted by a common logon function using the User ID and Password fields. During installation of the main server the installer is asked to provide a password for the Administrator account. This password consists of up to 20 alpha numerical characters.

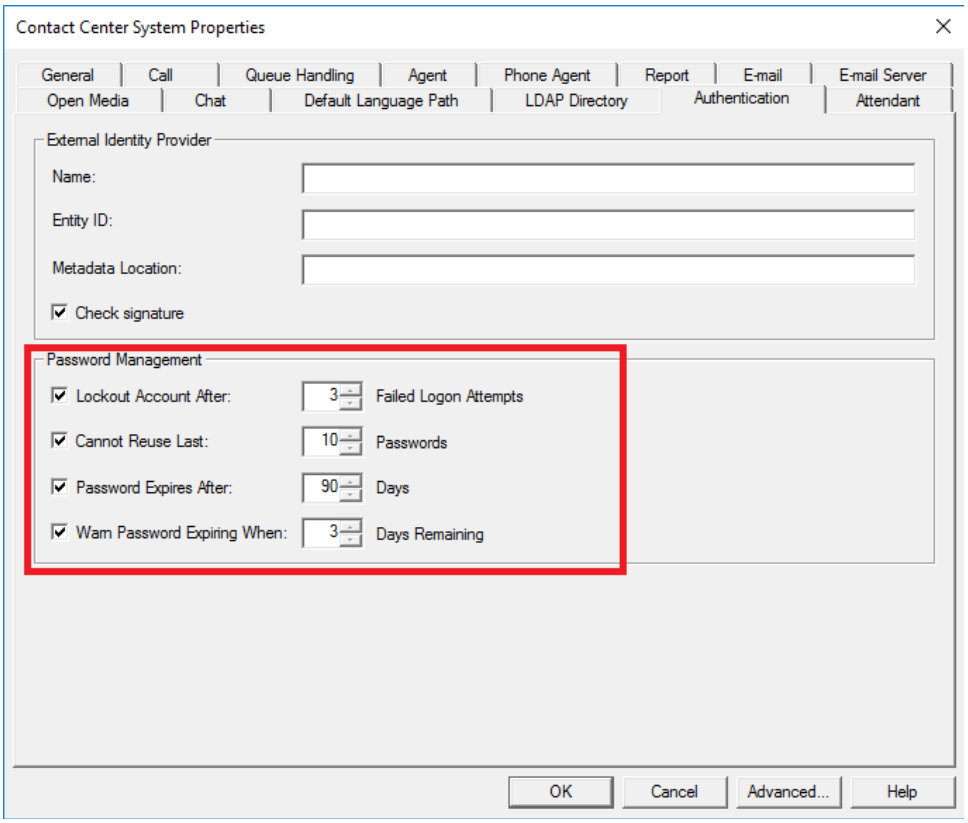
Using this account, other user types can be configured. The user type specifies which applications, and the specific features within these applications, users of this user type are permitted to access.

Users are defined with a User ID and password as well as tagged with a specific User Type restricting access to clients and features.

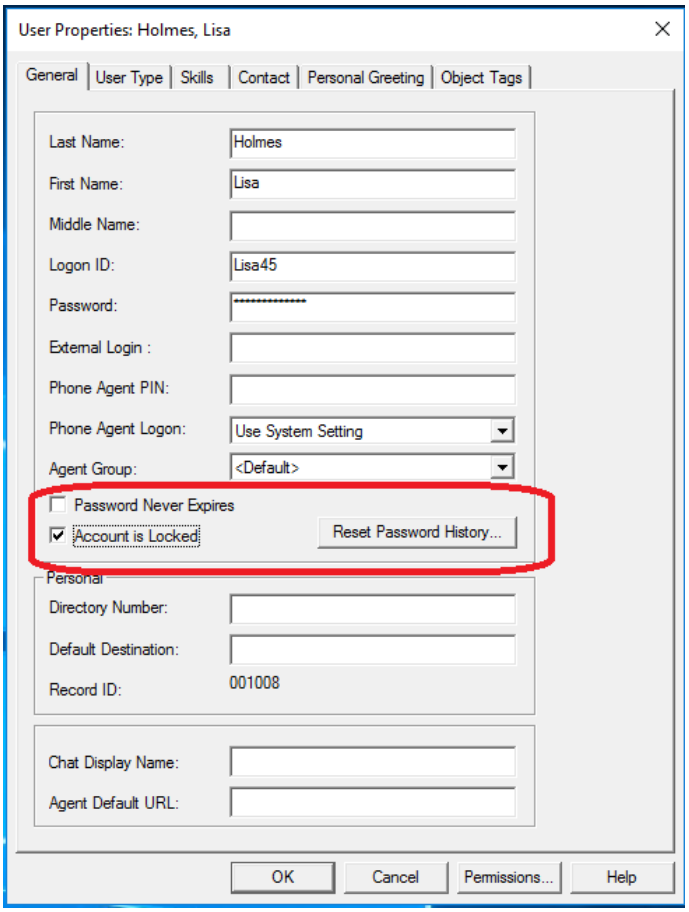
Users can change their password from their logon screen at any time. The system can also be configured to expire passwords after a configurable number of days. It can also be configured to provide a warning message when a configurable number of days remain until the password expires.

To control password updates, the number of previous passwords that cannot be reused can be configured.

It is also possible to configure how many failed logon attempts are permitted before the user is locked out from the system.



If a lock-out occurs, only an administrator can re-open the account again.



PROTECTION OF DATA IN TRANSIT

WEB SERVICES

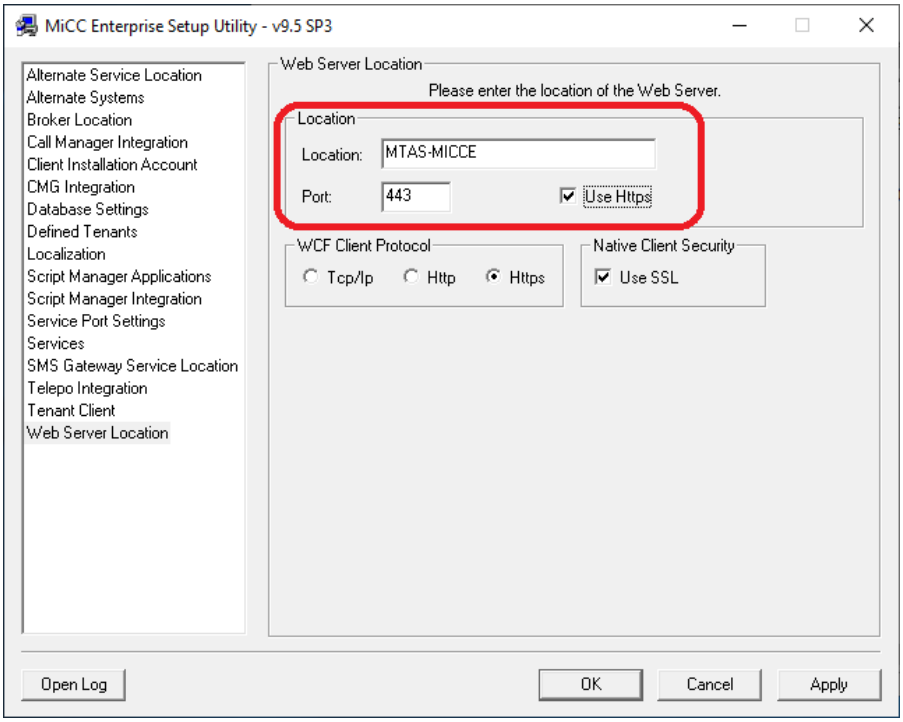
All MiCC Enterprise web services support encryption. HTTPS can be enabled in IIS and all WCF based services can be configured to use HTTPS. This will protect chat, email and open media session information between customers and agents, including all data sent to and from agents using the Web Agent application as well as all communication between the MiCC Enterprise server and agents using the MiCC Agent desktop application. All communication between Information and Report Manager applications and the IIS are also encrypted.

Enable HTTPS in IIS

Here is a description from Microsoft of how to enable HTTPS on IIS and how to generate a Certificate:

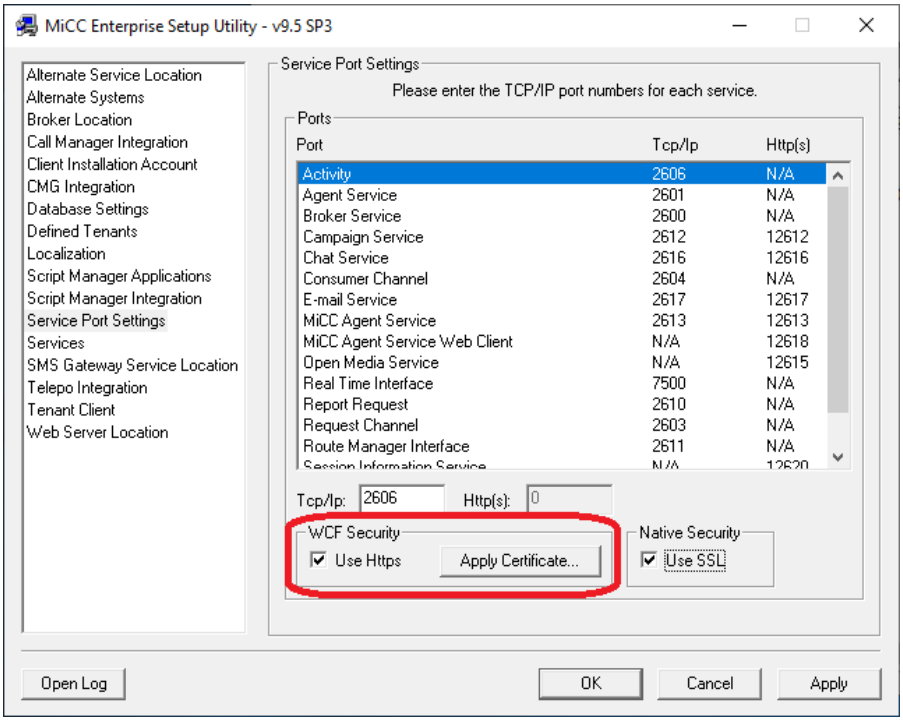
https://support.microsoft.com/en-us/help/324069/how-to-set-up-an-https-service-in-iis

In MiCC Enterprise, HTTPS is enabled using the MiCC Enterprise Setup Utility:

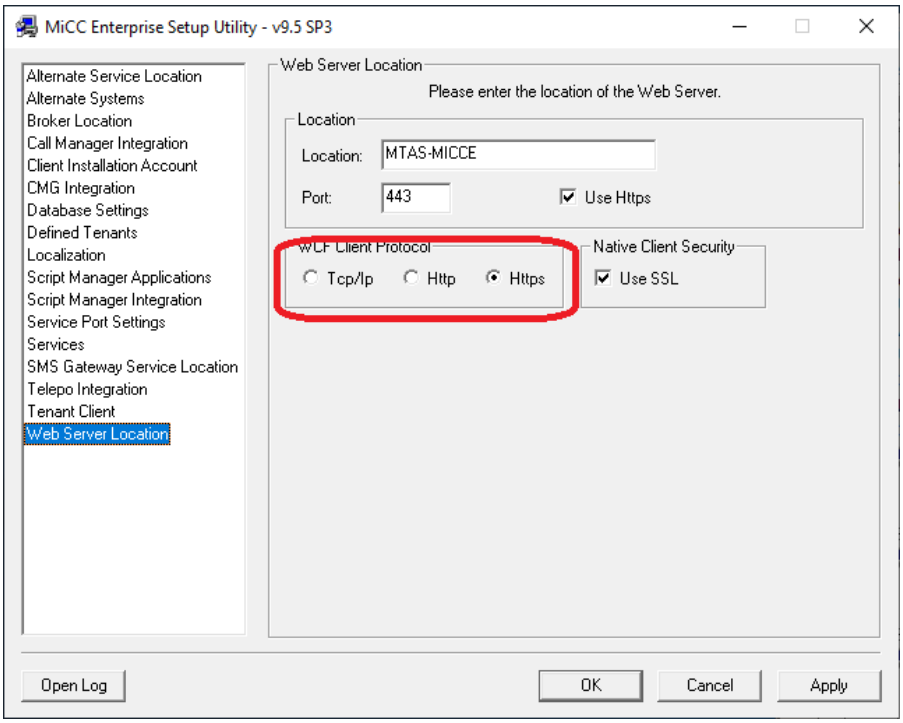

MiCC Enterprise Setup Utility - v9.5 SP3
Alternate Service Location
Alternate Systems
Broker Location
Call Manager Integration
Client Installation Account
CMG Integration
Database Settings
Defined Tenants
Localization
Script Manager Applications
Script Manager Integration
Service Port Settings
Services
SMS Gateway Service Location
Telepo Integration
Tenant Client
Web Server Location
Web Server Location
Please enter the location of the Web Server.
Location
Location:
MTAS-MICCE
Port:
443
Use Https
WCF Client Protocol
Tcp/Ip
Http
Https
Native Client Security
Use SSL
Open Log
OK
Cancel
Apply

Enable HTTPS on WCF Web Services

On the server:



On clients (Agent, Report Manager and Information Manager, or remote server components):



TLS VERSION

MiContact Center Enterprise starts the negotiation with TLS 1.3 and works its way down to what is supported on both sides of the connection. The encryption algorithm is also left up to the settings in Windows OS (the default is AES256).

The following ciphers are supported by MiCCE and TAS:

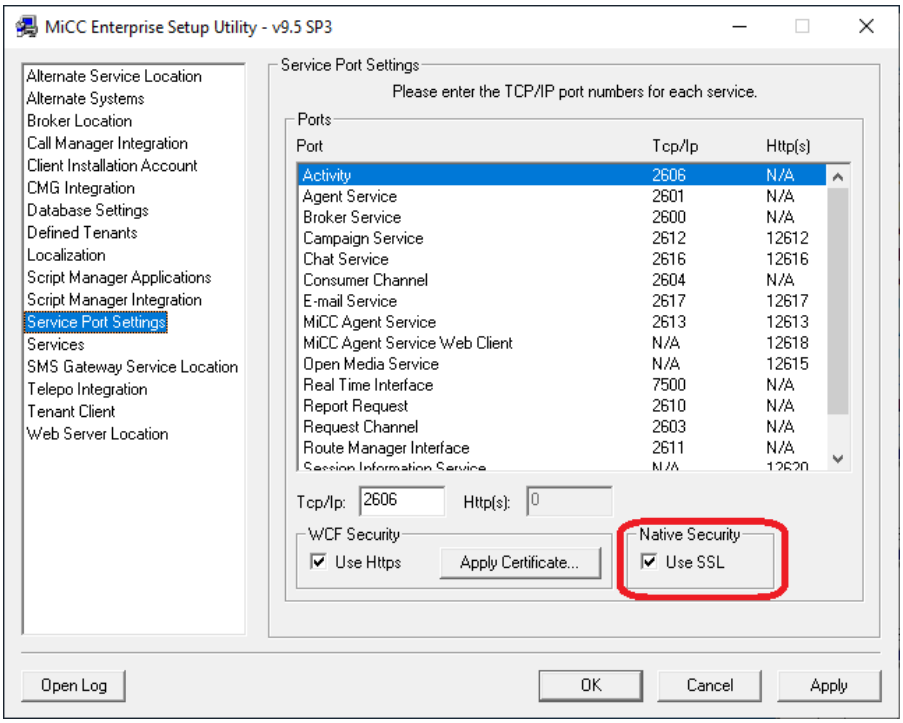
- AES_256_CM_HMAC_SHA1_80
- AES_256_CM_HMAC_SHA1_32
- AES_192_CM_HMAC_SHA1_80
- AES_192_CM_HMAC_SHA1_32
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

For TLS 1.3 to be used the MiCC Enterprise server needs to be running on Windows Server 2022 and connecting clients must be running on Windows 11.

TAS has support for TLS 1.3 as well. When TAS is connected to an MX-ONE 7.5 call manager (or higher) then TLS 1.3 can be configured both for the CSTA connection and the SIP trunk.

CLIENT/SERVER AND SERVER/SERVER COMMUNICATION

Using the MiCC Enterprise Setup program the system administrator can enable SSL on all socket communication between server components as well as Configuration Manager clients and the server.



DATABASE

MiCC Enterprise uses Microsoft SQL to store configuration and historical data. Enabling encryption on the communication to/from the database is described on the following web page:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15

This is all handled internally by SQL so nothing further needs to be configured in the MiCC Enterprise system.

INTERNET INFORMATION SERVICES (IIS)

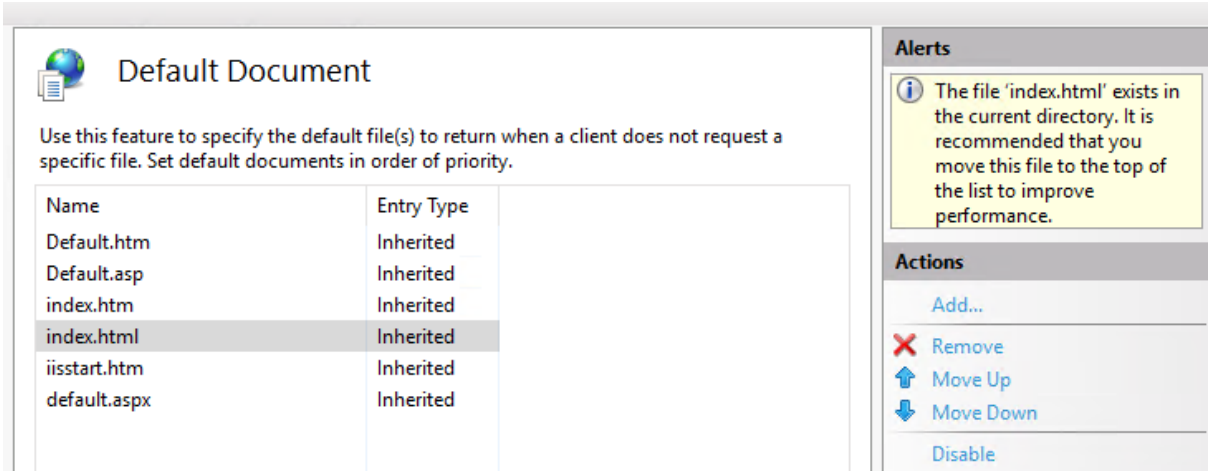
CLICKJACKING

To limit exposure to clickjacking it is recommended that the following procedure is performed on the IIS server hosting the MiCC-E web services:

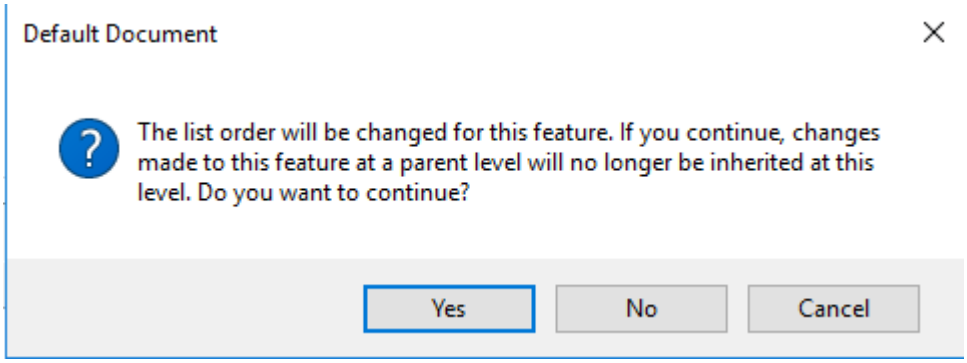
- In Run (Win+R), type “inetmgr”. This will open the IIS Manager.
- Go to Sites | Default Web Site and select Default Document property.

- Double click on Default Document property. This will open Default document pages.
- Right click on Default.htm page and click on disable.
- This setting will be inherited by all the projects. For the WebAgent project we need to enable the index.html page again.
- Click on WebAgent project and open the Default Document Property.
- Right click on index.html of WebAgent and click on enable.

After enabling the following information is seen about performance improvement.



Clicking the 'Move Up' option will result in the following caution.



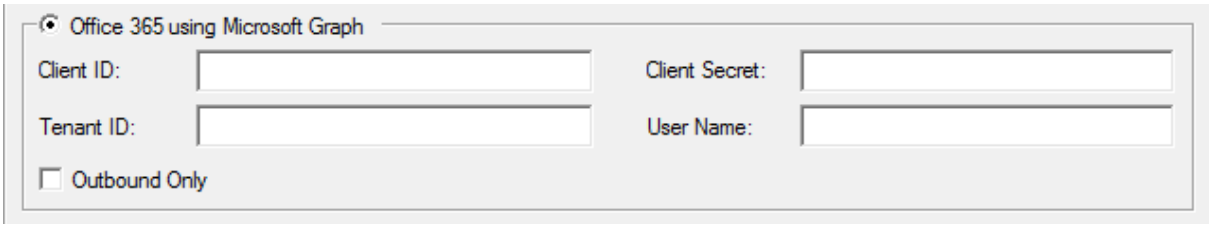
Answer 'Yes' and move to the top of the list.

EMAIL INTEGRATION

OFFICE 365

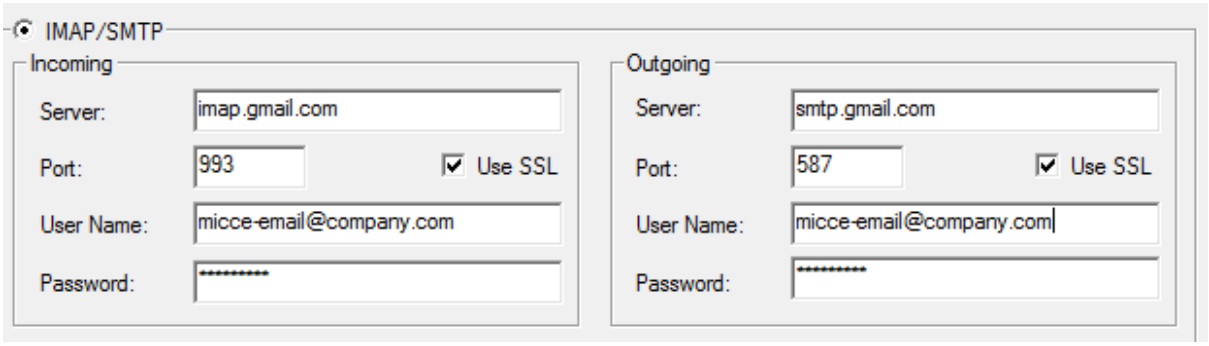
Due to Microsoft deprecating the Basic Authentication option when accessing Exchange Online the email service of MiCC Enterprise is as of release 9.5 Service Pack 3 using the Graph API and OAuth 2.0 when connecting to Office 365.

In order to use Office 365 you must register MiCC Enterprise with Azure Active Directory, receive an access token and configure the settings in MiCC Enterprise System Properties:



IMAP/SMTP

For integration to other Email services then IMAP and SMTP is used. These can be configured to use SSL:



PRODUCT SECURITY INFORMATION

MITEL PRODUCT SECURITY VULNERABILITIES

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:
www.mitel.com/mitel-product-security-policy

MITEL PRODUCT SECURITY PUBLICATIONS

Mitel Product Security Publications are available at:
www.mitel.com/security-advisories

DISCLAIMER

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiCC Enterprise and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.