MiCC Outbound

Prerequisites

Version 5.0

Mitel®

Powering connections

NOTICE

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

Mitel is a registered trademark of Mitel Networks Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Version Control

Version	Author	Comments	Revision Date
4.5	Craig Butters	Inclusion of SSRS Installation	4th March 2019
4.6	Craig Butters	Update Firewall ports & OS	13th March 2019
4.7	Craig Butters	SIP Rates added	17th April 2020
4.8	Craig Butters	Updated Firewall Diagram	11th June 2020
5.0	Craig Butters	Updated Document to reflect latest prerequisite information.	14th October 2020

TABLE OF CONTENTS

Introduction

This document has been created to guide you through the Prerequisites for the installation of a MiCC Outbound Platform.

This document has been produced to provide a high-level overview of the infrastructure; however, each installation may be slightly different due to server, network, and security considerations. It is recommended that you discuss your platform installation with your Project Manager if you require any further information in relation to this document.

Platform Arrangement

A typical Platform is installed across four, separate distinct roles. These can be defined as follows:

- SQL Database Server
- Application Server
- Web Server
- Call Manager Server (**Note:** A Call Manager server is not always required).

For smaller installations, these roles can be combined into a reduced server footprint.

For larger installations additional Web and Call Manager servers can be added to the platform to ensure enough resources are provisioned for the total number of agents to be supported (see hardware specification guidance for more information).

These servers can be physical devices or virtual machines (VMWare or Hyper-V being the most common virtualisation platforms). For either design, we recommend that careful considerations are made towards disk setup. Considerations should be made to ensure that hypervisors have enough capacity for the Platform servers, along with any other virtualised environments that share the same host.

We do not make specific speed recommendations in regard to the CPU being used within the physical server but do assume a recent a model server grade CPU.

Whilst it is possible to design your own server platform arrangement, we recommend that you discuss your design with your Project Manager.

Server Maintenance

Responsibility for maintaining the server hardware and surrounding infrastructure falls to the customer's IT Support function.

A thorough and regular server maintenance plan should be implemented for all servers that are provisioned to sure system is able to perform at optimal levels. Capacity planning and growth is also the responsibility of the customers IT Support function and where necessary, hardware may be subject to minor changes in line with future software upgrades (both MiCC Outbound software and Microsoft OS and SQL software).

The product is data driven and relies on the performance of the SQL Database to respond adequately, therefore a person with SQL Database Administration skills may be required to help maintain the database server.

MiCC Outbound

Installation Process

The following steps are a high-level outline of a typical installation, which is carried out by a trained MiCC Outbound Engineer.

- A "Preinstallation Form" will be provided by the Noetica Project Manager to capture all the server details, including authentication and remote connection methods. Where necessary, username and password details should be provided separately for security reasons.
- The customer should ensure that servers are installed and configured with all the necessary prerequisites having been met before returning the form.
- The form will be reviewed and verified by Noetica and if complete, the install will be planned.
- Noetica Engineers will download the installation software onto the Platform Servers.
- The installation, configuration and testing will then be completed.
- Instructions on how to connect to the platform and confirmation of file paths, account passwords, etc. will be provided.

Accounts & Authentication

During the installation of the MiCC Outbound Platform, several users are required to be created;

Account	Explaination
.\Synthesys	This is account can be a Microsoft AD account or setup locally on each of the Synthesys™ Platforms servers. It will need full administrative rights over the Platform servers and is used to run the Core Interactive Services. If created locally, this account will need to have the same password on each of the Platform servers. A corresponding account will be created on the SQL Database Server and will require 'Sysadmin' rights on install (this can later be restricted if necessary).
.\Noetica_Setup	This is account can be a Microsoft AD account or setup locally on each of the Synthesys™ Platforms servers. It will need full administrative rights over the Platform servers. If created locally, this account will need to have the same password on each of the Platform servers. This account is used to manage the installation and any upgrades to the Platform servers. A corresponding account will be created on the SQL Database Server and will require 'Sysadmin' rights on install (this can later be restricted if necessary).
.\Synthesys_Admin	This is account can be a Microsoft AD account or setup locally on each of the Synthesys™ Platforms servers. It will need full administrative rights over the Platform servers. If created locally, this account will need to have the same password on each of the Platform servers. This account is used to run the main 'Synthesys.Service' Windows service for the Synthesys™ Core. A corresponding account will be created on the SQL Database Server and will require "dbo.owner" rights to the corresponding Synthesys™ databases.
.\Synthesys_General	This is account can be a Microsoft AD account or setup locally on each of the Synthesys™ Platforms servers. It will need full administrative rights over the Platform servers. If created locally, this account will need to have the same password on each of the Platform servers. This account is used to run the tenant ("Synthesys.General.xx"), Windows services. If you have renamed your tenant to not be "General", then it is recommended that this account is renamed to match. A corresponding account will be created on the SQL Database Server and will require "dbo.owner" rights to the corresponding Synthesys™ databases.

It is recommended that the customer creates these accounts on the MiCC Outbound Platform servers, especially if they are going to be set up within Active Directory. Strong passwords should be used and provided securely as part of the "Preinstallation form".

It is also recommended that any Active Directory Group Policies are reviewed that may prevent the installation of the software or its operation.

Software Specifications

It is assumed that the servers that make up the Platform are "dedicated" and no other applications and/or databases are running. Where servers are "shared" with other applications, it will be the responsibility of the customer to ensure enough resources have been assigned.

We also assume that the latest Microsoft Service Packs and Security Fixes have been applied and these updates are applied in a controlled manner.

Server Specifications

For the App and Web server roles within the MiCC Outbound Platform, the following minimum specifications should be followed:

- Microsoft Server 2016 or above
- Microsoft .Net Framework 3.5 + SP1
- Microsoft .Net Framework 4.8
- Microsoft.NET Core 2.1 Runtime
- Microsoft .Net Core Hosting Bundle for Windows v2.1.5
- Microsoft .Net Core Hosting Bundle for Windows V3.1.8 or above

  MSMQ & MSDTC are required too, however these are included with Microsoft Server and will be installed and configured as part of the installation.

Whilst not required software, we also recommend that SQL Client Tools (Management Studio and Profiler), are installed onto both the Application server and Database Server and match the version of SQL Server.

Additional recommended software:

- Notepad++ on all servers, apart from SQL Server

SQL Server Specifications

For the SQL Database server, we recommend Microsoft SQL 2016 Standard Edition or above.

Within the SQL Server installation, the following items are also required:

- The database must be configured in a 'mixed mode' security mode.
- We require the "Noetica Setup" service to be installed and running on the SQL Server during the installation and upgrade processes.
- We require a user with 'Sysadmin' rights during the installation and upgrade process.
- Where Synthesys™ is installed on a shared SQL Server, it is recommended that Synthesys™ databases are installed onto a designated SQL Instance.
- SQL Server Report Services (SSRS) must be installed and configured on either your SQL Server or onto a dedicated SSRS Reporting server.

Seven databases will be created as part of the MiCC Outbound Platform configuration:

- Phoenix
- Phoneyx
- Synthesys_Admin
- Synthesys_General

- Synthesys_General_Admin
- Synthesys_General_Reporting
- Synthesys_Main

Client Software Specifications

The following minimum client specifications are required:

- Microsoft Windows 8 or above
- Microsoft Internet Explorer 9 or above for legacy app support.
- Google Chrome, Microsoft Edge or Firefox

The Synthesys™ Web Server should be added to the "Trusted Zone" within the browser settings and any pop-up blockers should be disabled.

For "Synthesys™ Management" and "Interaction Studio" users, the following additional items are required:

- Microsoft Silverlight 4
- Microsoft .Net version 3.5 + SP1
- Microsoft .Net version 4.8

Hardware Specifications

The following tables detail our minimum hardware specifications by server role. In some cases, mainly for smaller customers, combination servers can be used, please see Appendix for combined hardware configurations.

Application Server

The Operating System should be installed onto a separate drive, of at least 60GB in size, with the Application provided with a separate drive and partition. For 1-64 users, the web server can run on the application server and so a separate web server is not required.

SYNTHESYS APP SERVER				
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Application (D:)**
1-16	2	4	60	20GB plus 0.5GB per agent
17-32	4	4	60	20GB plus 0.5GB per agent
33-48	4	6	60	20GB plus 0.5GB per agent
49-64	4	8	60	20GB plus 0.5GB per agent
65-128	6	8	60	20GB plus 0.5GB per agent
129-256	8	8	60	20GB plus 0.5GB per agent
257-383	10	12	60	20GB plus 0.5GB per agent
384-512	12	16	60	20GB plus 0.5GB per agent

SQL Server

The Operating System should be installed onto a separate drive, of at least 60GB in size. Separate drives and partitions should be created for SQL Data and Logs, as per Microsoft Best Practices.

Setup and separation of "TempDB" should also be considered where appropriate. Considerations for SQL Backup and Replication drives should also be made. It is recommended that databases are operated in "Full Recovery" mode.

SQL SERVER						
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**SQL Data (D:)**	**SQL Logs (E:)**	**SQL Replication (F:)***
1-16	2	4	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
17-32	2	4	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
33-48	4	6	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
49-64	4	8	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
65-128	4	12	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
129-256	4	16	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
257-383	6	24	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
384-512	8	32	60	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data

Please note that if you are installing SQL with "per-core" licensing model, then 4 cores are the minimum you can license.

Web Server

The Operating System should be installed onto a separate drive, of at least 60GB in size, with the Application provided with a separate drive and partition.

WEB SERVER				
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Web (D:)**
1-16	2	4	60	60GB plus 0.5GB per agent
17-32	2	4	60	60GB plus 0.5GB per agent
33-48	2	4	60	60GB plus 0.5GB per agent
49-64	4	8	60	60GB plus 0.5GB per agent
65-128	6	8	60	60GB plus 0.5GB per agent
129-400	8	12	60	60GB plus 0.5GB per agent

Each web server can host up to 400 agents. The Web Server is an "n+1" design so additional web servers can be deployed for greater capacity.

For 1-64 agents, the web server can run on the application server, negating the need for a separate web server.

SSRS Reporting

For smaller call centres with relatively simple reports, customers can run supported reports directly on the live database server without affecting performance of the Application.

However, for larger or busy call centre, reporting can generate a great deal of data and more complex data mining reports can generate excessive load and create potential database locks, which can lead to degraded Platform performance or even create unexpected outages.

For 100+ agents or when there is evidence that reporting is causing call centre degradation, we recommend setting up a reporting database, using SQL Replication for example, and run all reporting against his database server.

Your Noetica Project Manager can provide further support and details around SQL Replication and reporting scenarios to avoid these issues. Please note that a Reporting Database will require further server resources and additional SQL licensing.

Management of SQL Replication and non-standard reporting will be the responsibility of the customer.

SSRS REPORTING (to be used with Replication)					
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**SQL Data (D:)**	**SQL Logs (E:)**
1-16 agents	2	4	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
17-32 agents	2	4	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
33-48 agents	4	6	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
49-64 agents	4	8	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
65-128 agents	4	12	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
129-256 agents	4	16	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
257-384 agents	6	24	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent
384-512 agents	8	32	60GB	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent

Management of SQL Replication and non-standard reporting will be the responsibility of the customer.

Disk Configuration

Throughout your server design, disk configuration should be carefully considered, and disk drives should, where appropriate, be configured using hardware-based RAID controller cards or using SAN/NAS storage.

It is recommended that the Operating System is installed on its own mirrored (RAID1) partition. For SQL Server, separate disks should be allocated for Data files and Log files.

Server disk speeds should be considered as follows:

15K SAS Storage - Database and core Application modules across the servers

10k SAS Storage – Archive Database

<10k SATA - Aimed only towards archiving and Long-term storage of Log file archives.

Anti-Malware Exclusions

The MiCC Outbound Platform Servers transfer messaging in real-time between many different components within the Platform. Virus scanners can cause delays within this messaging or even deny required detail reaching its intended destination. This can lead to system performance issues or failure within functionality.

Whilst we do not make recommendations on specific Anti-Virus products, it is recommended that exceptions are added to your security products to remove heavy scanning from the following folders across all Platform servers:

- <InstallFolder>\Synthesys*
- <InstallFolder>\Program Files\Noetica\Synthesys.NET*

Active Directory Requirements (Optional)

It is possible to configure the Noetica Platform so that it is integrated with Active Directory for Single Sign On. This is achieved through a windows service installed onto the Application Server (Please see further guidance in the "Domain Membership, Authentication & DNS" section of this document).

This service needs to run under a new Domain User or 'Service Account' with read only access to Active Directory (the password should be set to never expire).

Noetica needs to be supplied with the following information:

- Username and password of the Domain User which the service will run under
- Domain Name of the Active Directory domain
- Active Directory LDAP connection string

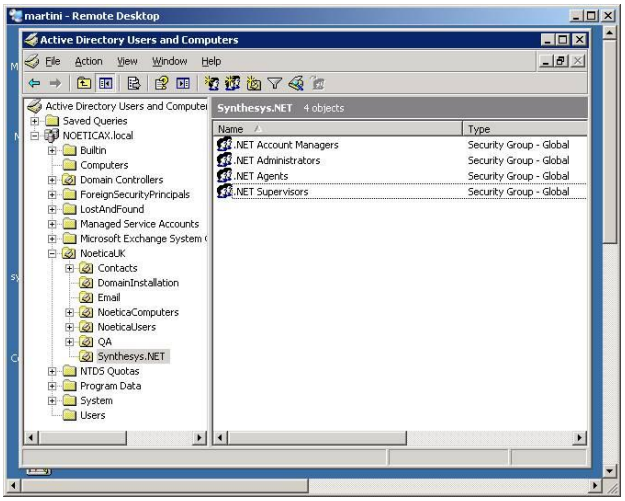
Active Directory Configuration

Platform users have different permissions corresponding to which Role they are assigned.

Global Security Groups need to be created in Active Directory, and these Security Groups will be set to correspond to Synthesys™ Roles in a configuration file (maintained by Noetica). There is no fixed name for each Security Group – they can be named freely.

For example, create Global Security Groups called:

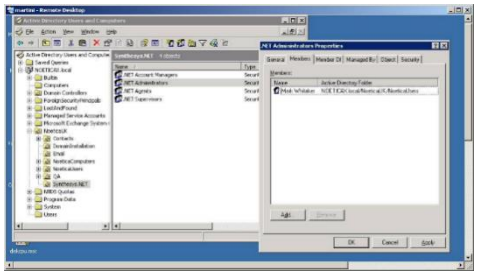
- .NET Account Managers
- .NET Administrators
- .NET Agents
- .NET Supervisors



These can then be set to map to the following Roles in MiCC Outbound:

- Account Manager
- Administrator
- Agent
- Supervisor

MiCC Outbound Users then need to be added to their correct Security Group:



When the Security Groups have been configured, we should be informed the name of each Security Group, and the MiCC Outbound Role it should map to.

We will need an Active Directory Account that has permission to browse the configured Active Directory to run as service on the Application Server. This is to allow us to import users into Synthesys and disable them if they become disabled in Active Directory.

SIP trunk CPS limits

We recommends a minimum of 15 calls per second (CPS) for each 100 concurrent predictive dialler agents. We cannot guarantee dialler performance below that limit.

On a case by case basis, when call connection rates are unusually low (such as poor data or the tail end of a campaign), this limit may not be sufficient, but in the general case this recommendation would ensure good dialler performance. Some SIP carriers insist on a minimum Answer Seizure Ratio (ASR), so you should ask your SIP provider about any such restrictions.

MiCC Call Manager

Installation Process

The following steps are a high-level outline of a typical installation, which is carried out by a trained Engineer.

- A "Preinstallation Form" will be provided by the Project Manager to capture all the server details, including authentication and remote connection methods. Where necessary, username and password details should be provided separately for security reasons.
- The customer should ensure that servers are installed and configured with all the necessary prerequisites having been met before returning the form.
- The form will be reviewed and verified and if complete, the install will be planned.
- Engineers will download the installation software onto the Platform Servers.
- The installation, configuration and testing will then be completed.
- Instructions on how to connect to the platform and confirmation of file paths, account passwords, etc. will be provided.

Accounts & Authentication

During the installation of the Call Manager, services are run by a Windows User or Service Account. This could be one of the same accounts used by MiCC Outbound or it can be a separate user.

It is recommended that the customer creates these accounts on the Noetica Platform servers, especially if they are going to be set up within Active Directory. Strong passwords should be used and provided securely as part of the "Preinstallation form".

It is also recommended that any Active Directory Group Policies are reviewed that may prevent the installation of the software or its operation.

Software Specifications

It is assumed that the Call Manager servers are "dedicated" and no other applications and/or databases are running. We also assume that the latest Microsoft Service Packs and Security Fixes have been applied and these updates are applied in a controlled manner.

Server Specifications

For each of the server roles within the Platform, the following minimum specifications should be followed:

- Microsoft Server 2016 or above
- Microsoft .Net Framework 3.5 + SP1
- Microsoft .Net Framework 4.8

Additional recommended software:

- Wireshark for NVP™/SIP setup and troubleshooting
- Notepad++ on all servers, apart from SQL Server

Hardware Specification

The following tables detail our minimum hardware specifications by server role. In some cases, mainly for smaller customers, combination servers can be used, please see Appendix for combined hardware configurations.

The following can be used a guide for planning your Call Manager environment:

The Operating System should be installed onto a separate drive, of at least 60GB in size, with the Application provided with a separate drive and partition.

NOETICA VOICE PLATFORM (NVP) SERVER					
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Application (D:)**	**Call Recording (E:)****
1-16	4	4	60	20GB plus 0.5GB per agent	2.5GB per agent, per month
17-32	4	4	60	20GB plus 0.5GB per agent	2.5GB per agent, per month
33-48	4	6	60	20GB plus 0.5GB per agent	2.5GB per agent, per month
49-64	4	6	60	20GB plus 0.5GB per agent	2.5GB per agent, per month
65-128	6	6	60	20GB plus 0.5GB per agent	2.5GB per agent, per month
129-256	8	8	60	20GB plus 0.5GB per agent	2.5GB per agent, per month
257-300	8	8	60	20GB plus 0.5GB per agent	2.5GB per agent, per month

For SmartBound™ features such as SnoDrop™, SmartAMD™ and LPD™ are required within your installation or the installation is not connecting to a MiVB, then a Call Manager Server will be required.

If your installation is to connect to a MiVB then further documentation will be supplied that relates to your specific installation by your Project Manager.

Disk Configuration

Throughout your server design, disk configuration should be carefully considered, and disk drives should, where appropriate, be configured using hardware-based RAID controller cards or using SAN/NAS storage.

It is recommended that the Operating System is installed on its own mirrored (RAID1) partition.

Server disk speeds should be considered as follows:

15K SAS Storage - Application modules

10k SAS Storage – Call recordings

<10k SATA - Aimed only towards archiving and Long-term storage of Call Recording and Log file archives.

Anti-Malware Exclusions

The Call Manager Servers transfer messaging in real-time between many different components within the Platform. Virus scanners can cause delays within this messaging or even deny required detail reaching its intended destination. This can lead to system performance issues or failure within functionality.

Whilst we do not make recommendations on specific Anti-Virus products, it is recommended that exceptions are added to your security products to remove heavy scanning from the following folders across all Platform servers:

- <InstallFolder>\VoicePlatform* (where Call Manager is running)

Bandwidth Requirements

Voice bandwidth usage is determined by the codec that is used, for example, a 100Mb/s network can carry voice for over 500 agents using the G.711 codec. For more optimised use of bandwidth the G.729 codec is available, although this can degrade voice quality very slightly.

Firewall or SBC Provision

There are many ways that SIP connectivity can be enabled for your platform, this may include a standard internet-based connection, a leased line or MPLS connection or by some other interconnection.

All the different methods need to be protected by a device and they also need to be able to handle the SIP traffic to be carried. To enable this, it is essential that a SIP compliant firewall is installed or preferably, a Session Border Controller (SBC) that can manage the requirement.

It is very important that the device being used at the perimeter of the network can convert the SIP packets that hold internal network IP addressing across to public IP addressing when being passed to a telco or service that requires this.

We can recommend different levels and types of firewall and SBC dependant on the requirement. Along with this is secure SIP is required then an SBC is a prerequisite within the design.

We can review firewall and network requirements within the scoping and design phase of an implementation.

Call Recording

The Call Manager has built-in call recording features; call recordings are automatically tied to the Synthesys records. Call Recording storage can be on the same disk as the Call Manager software; however, it is recommended that separate disks be used.

Faster disk storage can be used for the initial recording, but cheaper, slower storage can be used for Call Recording archiving. Alternatively, NAS or SAN storage can be setup for the long-term storage of call recordings.

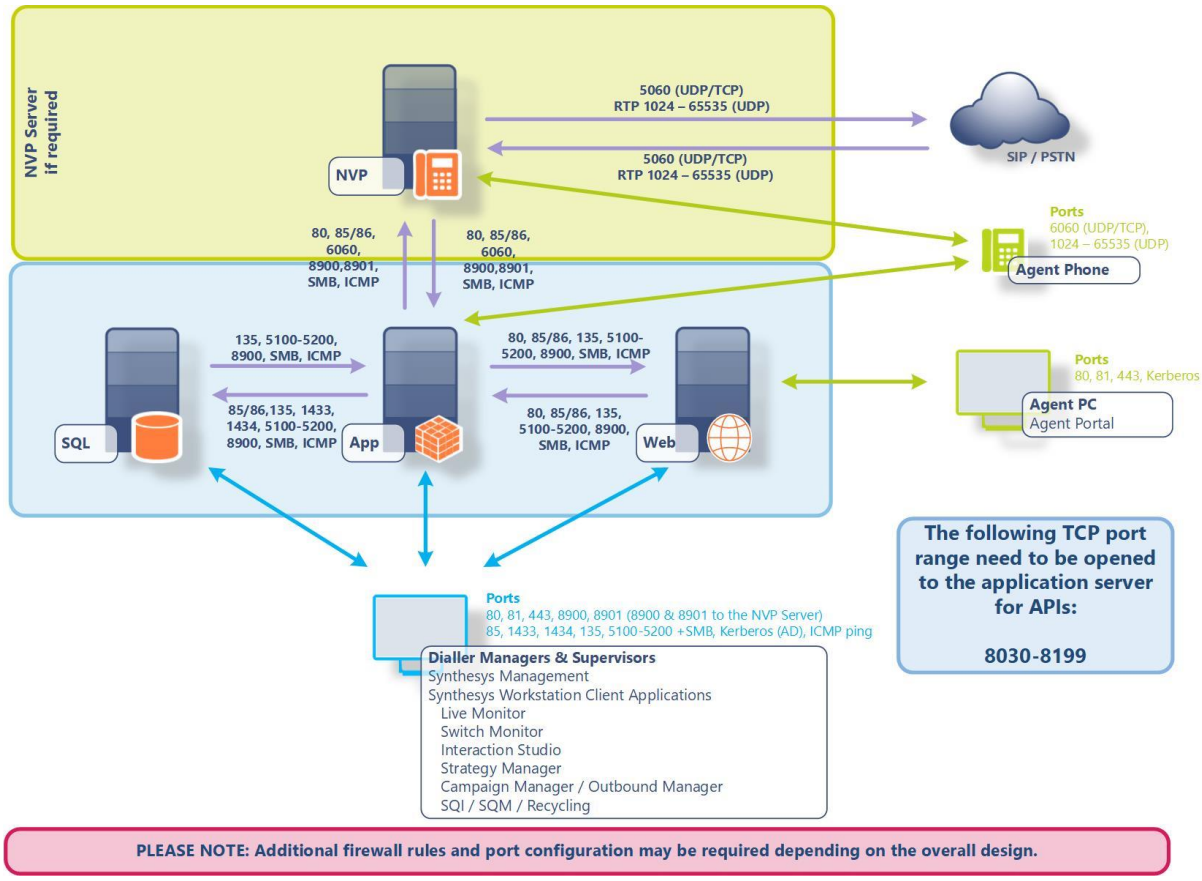
Call Recordings are currently stored in .wav format. See “Hardware specifications” for a guide on how much storage space is required.

Network Specification

All MiCC Outbound Platform servers should be joined to a Microsoft Active Directory domain, where possible. Where Platform servers are not members of the same domain, then additional considerations for allowing authentication will need to be planned; this will be the customers' responsibility, though we can help make recommendations.

Server to Server Communication

We recommend that gigabit switched connections are made between the MiCC Outbound Platform servers and that any firewalls are configured to allow smooth, uninterrupted communication between the servers.



PLEASE NOTE: Additional firewall rules and port configuration may be required depending on the overall design.

The following network ports are used within the solution:

Ports required

Originating Machine	Destinaation Machine	Port / Protocol
App Server	Web Server	Ports 80, 85/86, 135, 5100-5200, 8900, SMB, ICMP
Web Server	App Server	Ports 80, 85/86, 135, 5100-5200, 8900, SMB, ICMP
App Server	SQL Server	Ports 85/86, 1433, 1434, 5100-5200, 8900, SMB, ICMP
SQL Server	App Server	Ports 135, 5100-5200, 8900, SMB, ICMP
Web Server	SQL Server	No connection required
Client Machines	Web Server	Ports 80, 81, 443, Kerberos
Client Machines	App Server	Ports 80, 81, 443, 8901, 85, 1433, 1434, 135, 5100-5200, SMB, Kerberos, ICMP
For NVP if required		
NVP Server	App Server	Ports 80, 85/86, 5060, 6060, 8900, 8901, SMB, ICMP
App Server	NVP Server	Ports 80, 85/86, 5060, 6060, 8900, 8901, SMB, ICMP
Client Phone	NVP Server	Ports 5060/6060, 1024-65535 (UDP)

Explanation of ports

Port	Description
85-86	Used for internal communication by Synthesys; these can be reconfigured.
80	Used for Interaction Studio to communicate with Synthesys Web Server; can be reconfigured, but this requires manual configuration on client machines.
81	Used for web based applications (Portal); can be reconfigured.
135, 5100-5200	Used by MSDTC. The 5100-5200 range can be reconfigured.
1434	This is used by SQL Browser to negotate SQL connections as well as browsing.
1433	Default port used for SQL Server connections; can be reconfigured.
8900/8901	Used for web services communication.
8030-8199	Used for API connectivity.
For NVP if required	
5060/6060	Used for SIP connectivity.
1024-65535	Used for RDP voice.

Web Server to Client Communication

Bandwidth between the agent browser and the Synthesys™ Platform Web Server(s), should be calculated as follows:

Number of Users	Saturated Bandwidth	Recommended Pipe Kbytes/sec	Recommended Pipe Kbits/sec
1	0.2	0.4	64
10	2	4	64
20	4	8	64
50	10	32	256
100	20	64	512
200	40	128	1024
300	60	128	1024
500	100	256	2048

These figures are assuming HTTP traffic on port 80. HTTPS traffic will require approximately 25% more bandwidth.

Domain Membership, Authentication & DNS

It is recommended, where possible, that all servers are joined to an Active Directory domain for servers to communicate with one another effectively. Users of the MiCC Outbound Platform should ideally be joined to the same domain.

Where this is not possible, workaround provisions must be considered for Dialler Managers and Supervisor users to be able to successfully be authenticated to the SMB shares for MiCC Outbound tools that are not web enabled.

Where servers and users are not members of the same domain or are connected via separate networks (or when VPN connectivity is used), it is the customers responsibility to ensure that connectivity to the Noetica Platform servers can be delivered and server names can be resolved within DNS or local Host files are maintained.

If you have any concerns regarding network configuration, DNS, VPN connectivity or authentication, please raise any questions with your Project Manager.

Appendix

Combination Servers

For smaller installations, up to 64 agents, server roles can be combined onto a single server. The following table provides a guideline on how these combine roles can be calculated:

MiCC Outbound App & Web

SYNTHESYS APP & WEB				
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Application (D:) (Synthesys + Web)**
1-16 agents	4	8	60GB	20GB + 60GB plus 1GB per agent
17-32 agents	6	8	60GB	20GB + 60GB plus 1GB per agent
33-48 agents	6	12	60GB	20GB + 60GB plus 1GB per agent
49-64 agents	8	16	60GB	20GB + 60GB plus 1GB per agent

MiCC Outbound App & Web & Call Manager

SYNTHESYS APP & WEB & NVP					
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Application (D:) (Synthesys + Web + NVP)**	**Call Recording (G:)****
1-16 agents	6	12	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	2.5GB per agent, per month
17-32 agents	8	16	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	2.5GB per agent, per month
33-48 agents	8	20	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	2.5GB per agent, per month
49-64 agents	12	24	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	2.5GB per agent, per month

MiCC Outbound App & Web & SQL

SYNTHESYS APP & WEB & SQL							
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Application (D:) (Synthesys + Web)**	**SQL Data (E:)**	**SQL Logs (E:)**	**SQL Replication (F:)***
1-16 agents	6	12	60GB	20GB + 60GB plus 1GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
17-32 agents	8	12	60GB	20GB + 60GB plus 1GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
33-48 agents	10	16	60GB	20GB + 60GB plus 1GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
49-64 agents	12	24	60GB	20GB + 60GB plus 1GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data

MiCC Outbound App & Web & Call Manager & SQL

SYNTHESYS APP & WEB & NVP & SQL							
Agents	**CPU Cores**	**RAM (GB)**	**System OS (C:)**	**Application (D:) (Synthesys + Web + NVP)**	**SQL Data (E:)**	**SQL Logs (E:)**	**SQL Replication (F:)***
1-16 agents	8	16	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
17-32 agents	10	16	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
33-48 agents	10	20	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data
49-64 agents	12	28	60GB	20GB + 60GB + 20GB plus 1.5GB per agent	30GB plus 0.5GB per agent	20GB plus 0.25GB per agent	30% of SQL Data

Remote Connectivity

For us to effectively install and support your installation it is a requirement that we have remote connectivity to the MiCC Outbound Platform Server(s) from the Client Connection Network.

We have listed several proven methods that we support below:

Approved Connection Protocol:

- Microsoft VPN Internet connectivity
- Citrix Internet connectivity
- Direct IP connection (Secured RDP)
- Cisco or Fortigate VPN client software

Approved Connection Software:

- Microsoft Remote Desktop
- LogMeIn.com
- WebEx
- GoToMyPC.com
- UltraVNC
- Windows 10 Quick Assist

Alternative Methods of connection

We would always prefer to use one of the connection methods listed above, however we do understand that there may be circumstances where another connection method is required by a particular client.

Whilst we will endeavour to use alternative software there may be a charge associated with testing and configuring non-approved software on our network as security testing including penetration testing maybe required. There may also be an impact on project lead times as testing will need to be scheduled and carried out. Please contact your Project Manager for further information.

Should a remote connection method be inadequate in allowing us to support you efficiently, we may request an alternative connection method is implemented or a change to SLAs without our standard Software Agreement between parties.

We can support TeamViewer; however, this must be licensed by the customer. Unlicensed versions of TeamViewer will not be supported.