bns™

ENTERPRISE SMS SERVER

Deployment guide for AWS

Software version 2.0

3 March 2023

bns

BETTER NETWORK SERVICES GROUP

aws PARTNER Amazon RDS Ready

aws Qualified Software

Deployment guide AWS

Better Network Services Group Pty Ltd (BNS Group) ABN 54 003 868 120

The software described in this Guide is supplied under a license agreement and may only be used in accordance with that agreement.

BNS Enterprise SMS Server ™ is a trademark of Better Network Services Group Pty Limited (BNS Group). Other brands or product names are trademarks or registered trademarks of their respective holders.

Trademark acknowledgements:

- MessageMedia is a registered trademark of Message4U Pty Limited.
- SINCH is a registered trademark of SINCH Limited.
- Microsoft® is a registered trademark of Microsoft Corporation Inc.
- Windows® is a registered trademark of Microsoft Corporation Inc.
- AWS is a trademark of Amazon Web Services Inc

.

Table of Contents

BNS Group would like to thank the following people and organizations for making BNS Enterprise SMS Server a world class product:

- To all our staff and their families for working tirelessly to deliver world class products.
- Messaging and Collaboration team Suncorp Group
- Amazon Web Services ISV partner team for assisting BNS with technical foundation technical reviews and achieving the AWS RDS Service ready designation.

1 Introduction

BNS Enterprise SMS Server was previously known as msXsms Enterprise SMS server. Product rebranding in March 2023 was necessary as BNS re-engineered the software for the cloud. Significant re-engineering effort was focused on recovery with AWS RDS MS SQL Server in multi-AZ.

BNS Enterprise SMS Server is a scalable secure SMS text messaging software solution deployed in your own cloud tenancy or your own datacentre. The SMS Server uses SMS industry standards to send SMS messages to a variety of SMS service providers using industry standard SMPP\TLS encryption over the Internet.

Applications can send SMS using SQL or email as the interface to the SMS Server platform. Users can send SMS messages using internal email from their email client such as Microsoft Outlook.

Microsoft SQL Server is used to store SMS data for: data analytics, controls, compliance and audit.

A powerful Microsoft PowerBi data analytics module is provided to analyse meta-data provided by applications or simply provide insights into the use of SMS within the enterprise.

Receiving SMS messages is supported delivering SMS messages to applications and users via email or a SQL database. Routing of inbound SMS is based on the receiving SMS number at the SMS Server.

High availability is provided at all 3 layers of the solution including:

- Platform layer Azure\AWS (SQL High availability)
- Application layer (SMS server level)
- SMS service provider layer (SMS Delivery)

The solution allows a choice of SMS service providers allowing the best per SMS message rate from a list of tested SMS service providers. Changing providers is possible allowing you to negotiate the best possible rate. Without using a solution like BNS's enterprise SMS server means you would use a proprietary REST API from a single provider making it difficult to change and difficult to negotiate per message rates.

The solution allows for primary and backup SMS service providers allowing redundancy at service provider level. If the SMS server cannot reach the primary SMS service provider the SMS server will automatically failover to the backup SMS service provider for a period of time. Switching back to the primary SMS service provider is also automatic after communication is restored to the primary SMS service provider.

Extensive testing and verification in AWS provides enterprise customers the confidence that the SMS Server software meets cloud high availability, security and design compliance.

The SMS Server software was awarded 2 software badges as part of the AWS ISV accelerate program. AWS Foundation Technical Review (AWS verified software) and AWS RDS service ready badge.

AWS ISV Partner path program is a set of useful tools, insightful resources, advanced technologies, and the best practices that may be used by development companies such as BNS in the process of creating cloud-based software for their customers.

BNS achieved the AWS qualified software badge in 2022 after extensive work with AWS to undertake a foundation technology review which is part of the AWS ISV Partner path program.

February 2023. BNS achieved the much higher technical designation for AWS RDS Service Ready.

The AWS Service Ready Program is designed to validate software products built by AWS Partners that work with specific AWS services. These software products are technically validated by AWS Partner Solution Architects for their sound architecture and adherence to AWS best practices, and market adoption including customer successes.

https://aws.amazon.com/partners/programs/service-ready/

1.1 Terminology

SMPP

SMPP - Short Message Peer-to-Peer Protocol

The SMPP (Short Message Peer-to-Peer) protocol is an open, industry standard protocol designed to provide a flexible data communications interface for the transfer of short message data between the SMS Server software and a Message Centres, hereinafter referred to as a SMS Service provider.

The SMS Server software implements version 3.4 of the SMPP standard and has been tested with a number of SMS Service providers. Not all SMS Service providers implement all options within the standard. It is important that the customer selects a supported SMS Service provider which implements the required options in the standard.

SMPP over TLS is used to encrypt communications of SMS messages between the customer's AWS tenancy and the SMS Service provider over the Internet.

SMSC

SMS Message Centre. Is a SMS Service provider supporting SMPP and which has been tested by BNS.

AWS AZ & Multi-AZ

Amazon Web Services availability zone. Availability Zones are distinct locations within an AWS Region that are engineered to be isolated from failures in other Availability Zones.

AWS RDS

Amazon Web Services Relational Database Services

1.2 Features and use cases

Enterprise customers who are modernising their applications for the cloud can implement a SQL Server based SMS interface for all business processes requiring a secure highly scalable solution from their cloud tenancy.

BNS Enterprise SMS server software is an enterprise-grade SMS solution that consolidates different messaging requirements across multiple companies and departments to a single robust, reliable and scalable messaging platform allowing better cost management, compliance and controls.

Customers like Suncorp Group implemented BNS's SMS software in 2009 as it re-engineered and consolidated multiple brands within the group. Brands such as: Suncorp Insurance, Suncorp Bank, AAMI, GIO, Vero and Shannons use the software because it provides multiple brands the ability to use shared infrastructure with high availability and a rich set of features.

All SMS communications are logged and stored within the customer's cloud tenancy using Microsoft SQL Server.

Applications simply write their SMS requests into a SQL Database (SMS-SQL-API) to send and receive SMS messages to\from mobile phones.

Applications periodically process confirmations of their SMS messages and process any incoming messages at the same time.

Multiple applications are supported using a single interface SQL database with row level security.

The SMS software uses industry standards SMPP protocol to communicate with SMS Service providers supporting industry standard version 3.4

Benefits of using the SMS software include:

- Easily on-board business applications with minimal coding.
- Your business applications use SQL server in cloud or on-premises to send and receive SMS.
- Avoids any future re-programming should the underlying SMS provider change.
- Avoids using proprietary REST APIs unique to a single SMS provider.
- Avoids developing high availability controls to multiple SMS service providers.
- Allows production to DR failover of SMS traffic within a region.
- Allows multiple SMS providers to be supported for high availability at the SMS provider level.

- Primary and backup SMS providers are switched automatically without any application changes if there is a loss of communications to a primary SMS service provider.
- Industry-standard SMPP implementation at the SMS server supports many SMS service providers allowing best possible contract rates to be negotiated.
- Controls such as checking for duplicate messages to the same mobile over a 24 hour period is configurable at a server level.

1.3 AWS deployment options

1.3.1 Single-AZ

Deployment in a single AZ requires a minimum of 1 x SMS Server and 1 x AWS RDS service with either: Microsoft SQL Express or Microsoft SQL Server (Standard or Enterprise).

Multiple SMS Servers can be deployed in a single AZ providing high availability of the SMS server software in a single AZ.

For more information refer to section 4.3

1.3.2 Multi-AZ

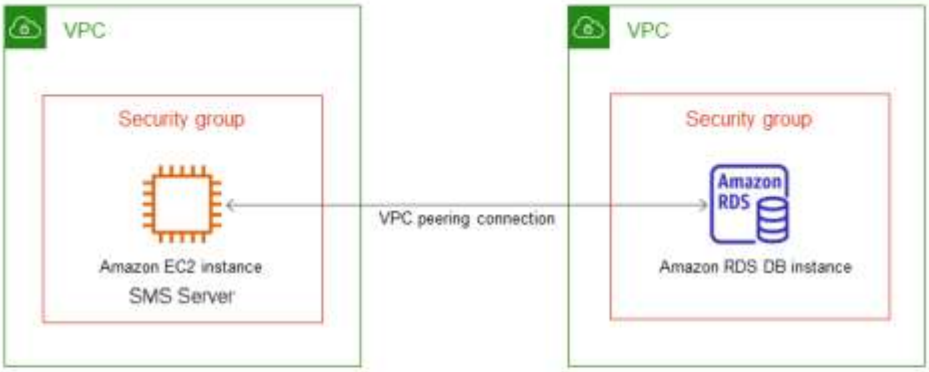
Deployment in multiple AZ requires a minimum of 2 x SMS Server (1 in each AZ) and 1 x AWS RDS service with either: Microsoft SQL Server Enterprise.

For more information refer to section 4.4

1.3.3 Multiple VPC with EC2 instance in one VPC and Database in another VPC

When your DB instances are in a different VPC from the EC2 instance you are using to access it, you can use VPC peering to access the DB instance.

The following diagram shows this scenario.



A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. Resources in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

For more information refer to https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html

1.3.4 Multi-Region

Global delivery of SMS can be performed from one region. The SMS Service provider takes care of global delivery.

If there was a need for multiple regions the design would typically have separate deployments of the platform with regional based SMS Service providers.

Key considerations for using a local SMS Service provider is lower latency for SMPP communications (SMS traffic).

1.4 AWS services used by the software

The following AWS services are required as a minimum:

- EC2 windows server instance(s). OS only no SQL on the Windows Server.
- RDS MS SQL Server or MS SQL Express for a simple installation

AWS Services

Amazon EC2

The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems.

Amazon RDS

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database such as Microsoft SQL Server in the cloud.

Amazon VPC

The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

1.5 Licensing and cost models

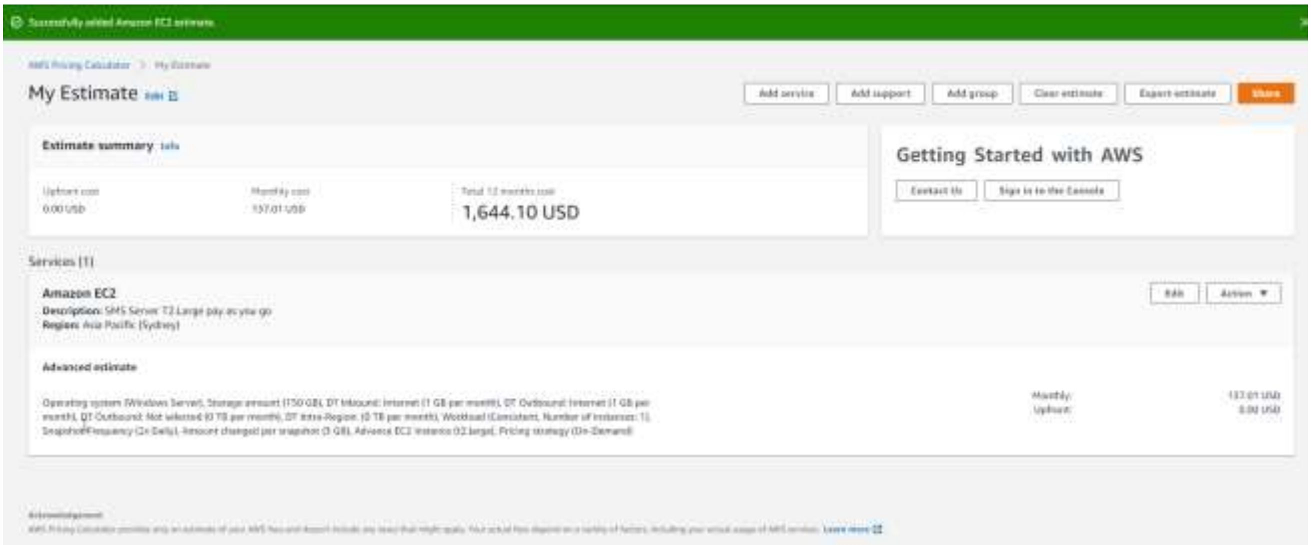
1.5.1 AWS Costs – getting started with a single-AZ

https://aws.amazon.com/ec2/pricing/
https://aws.amazon.com/rds/pricing/

SMS Software hosted on EC2 instance

EC2 instance type t2.large is ideal for a small deployment in a single-AZ to host the SMS software.

Cost per month without any savings plans = estimated without taxes USD137 per month.



Successfully added Amazon EC2 estimate

AWS Pricing Calculator > My Estimate

My Estimate Edit

Estimate summary Info

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	137.01 USD	1,644.10 USD

Getting Started with AWS

Services (1)

Amazon EC2
Description: SMS Server T2 Large pay as you go
Region: Asia Pacific (Sydney)

Advanced estimate

Operating system (Windows Server), Storage amount (150 GB), DT Inbound: Internet (1 GB per month), DT Outbound: Internet (1 GB per month), DT Outbound: Not selected (0 TB per month), DT Intra-Region: (0 TB per month), Workload (Consistent, Number of instances: 1), Snapshot Frequency (2x Daily), Amount changed per snapshot (3 GB), Advance EC2 instance (t2.large), Pricing strategy (On-Demand)

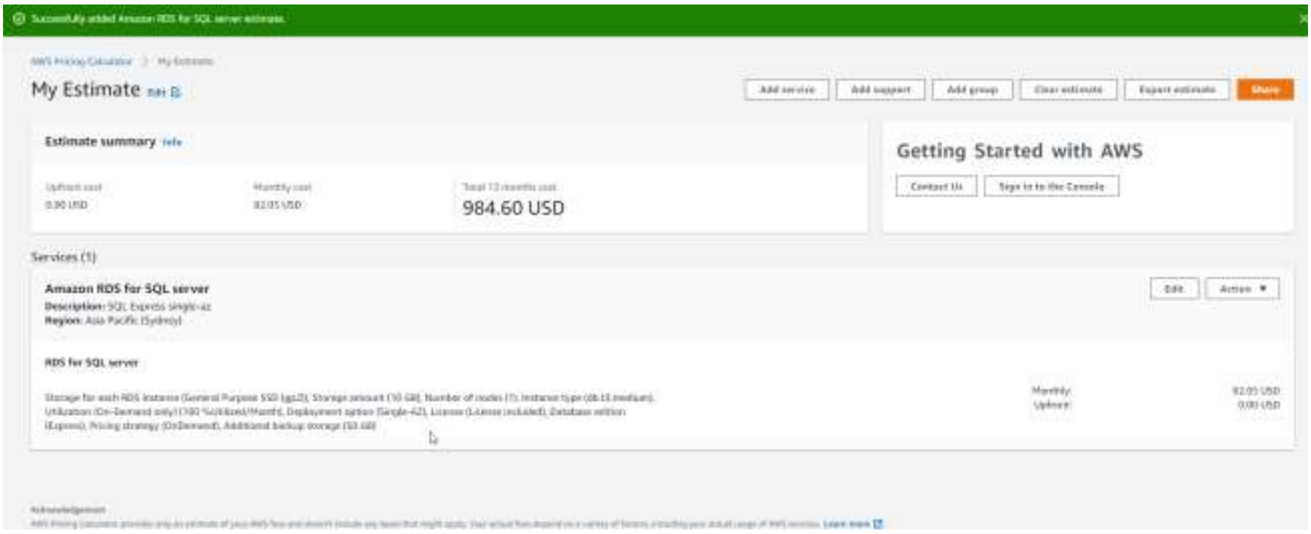
Monthly: 137.01 USD
Upfront: 0.00 USD

Acknowledgement
AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. Learn more

AWS RDS MS SQL Express

SQL Express in most cases will be sufficient for a startup business with a small deployment in a single-AZ.

Cost per month without any savings plans = estimated without taxes USD82 per month.



Successfully added Amazon RDS for SQL server estimate.

AWS Pricing Calculator > My Estimate

My Estimate Edit

Estimate summary Info

Upfront cost
0.00 USD

Monthly cost
82.05 USD

Total 12 months cost
984.60 USD

Getting Started with AWS

Services (1)

Amazon RDS for SQL server
Description: SQL Express single-az
Region: Asia Pacific (Sydney)

RDS for SQL server

Storage for each RDS instance (General Purpose SSD (gp2)), Storage amount (10 GB), Number of nodes (1), Instance type (db.t3.medium), Utilization (On-Demand only) (100 %Utilized/Month), Deployment option (Single-AZ), License (License included), Database edition (Express), Pricing strategy (OnDemand), Additional backup storage (10 GB)

Monthly: 82.05 USD
Upfront: 0.00 USD

Acknowledgement
AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. Learn more

Total of EC2 and RDS for the SMS Solution for a startup \ quick start single-az = USD137 + USD82 = USD219 excluding taxes.

A large customer would provision 2 x T3.2XLarge or equivalent EC2 instances for a production deployment.

1.5.2 SMS server licensing from BNS Group

Enterprise licensing options are available from BNS group (www.bnsgroup.com.au). A usage based model is typically used by enterprise to allow for unlimited scale of the SMS platform and monthly billing.

1.5.3 SMS Service provider costs

Usually this cost is an operational monthly cost based on usage with some fixed costs per month for items such as SMS Numbers for two-way SMS.

1.6 Time to complete deployment

1.6.1 Single-AZ

Software setup can be performed in on a single Windows Server EC2 instance in less than 1 day if all aspects of the project are well organized.

1.6.2 Multi-AZ

Software setup can be performed in a multi-AZ Windows Server EC2 instance in 2 days if all aspects of the project are well organized.

For more information refer to section 5.7

1.7 AWS Regions supported

BNS has tested its software in ap-southeast-2 region.

1.8 Administrator and Developer KB

Refer to the public KB. https://smskb.bnsgroup.com.au/admin-guides

Refer to the public KB. https://smskb.bnsgroup.com.au/sqlinterface

2 Installation checklists

1.9 Upgrading from previous releases

Version upgrades are documented in the SRN for each release.

Refer to https://smskb.bnsgroup.com.au/release-notes

Version history https://smskb.bnsgroup.com.au/version-history **(1.7.33)**

Version history Version History (version 2+) (bnsgroup.com.au) (2.x)

1.10 Worksheet for New Installations

Item	Value / comments
SMS production server name	
SMS production IP address	
Active Directory Domain or workgroup	
SMS service provider SMPP Account login details	
SMS service provider IP Addressing	This is in the boot.ini file firewall rules for outgoing connections.
SMS service provider connection port number	This is in the boot.ini file firewall rules for outgoing connections.
SQL Server connection string including ",port number"	
SQL Port number	
SQL server login (Windows Authentication or Local SQL User)	
Office 365 or equivalent SMTP user credentials for delivery of error messages to administrators.	User email address = If public DNS is not available in your zone the software can be configured to use an IP address of an internal SMTP server.

Email address for alerting IT staff	
Mobile numbers to be used for the in-built health service	
Servers to be used for bid control to the SMS-SQL-API database	Server1= Server2=
Provisioning guides for AWS EC2 and RDS SQL Server	See links below.

https://aws.amazon.com/ec2/getting-started/

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.CreatingConnecting.SQLServer.html

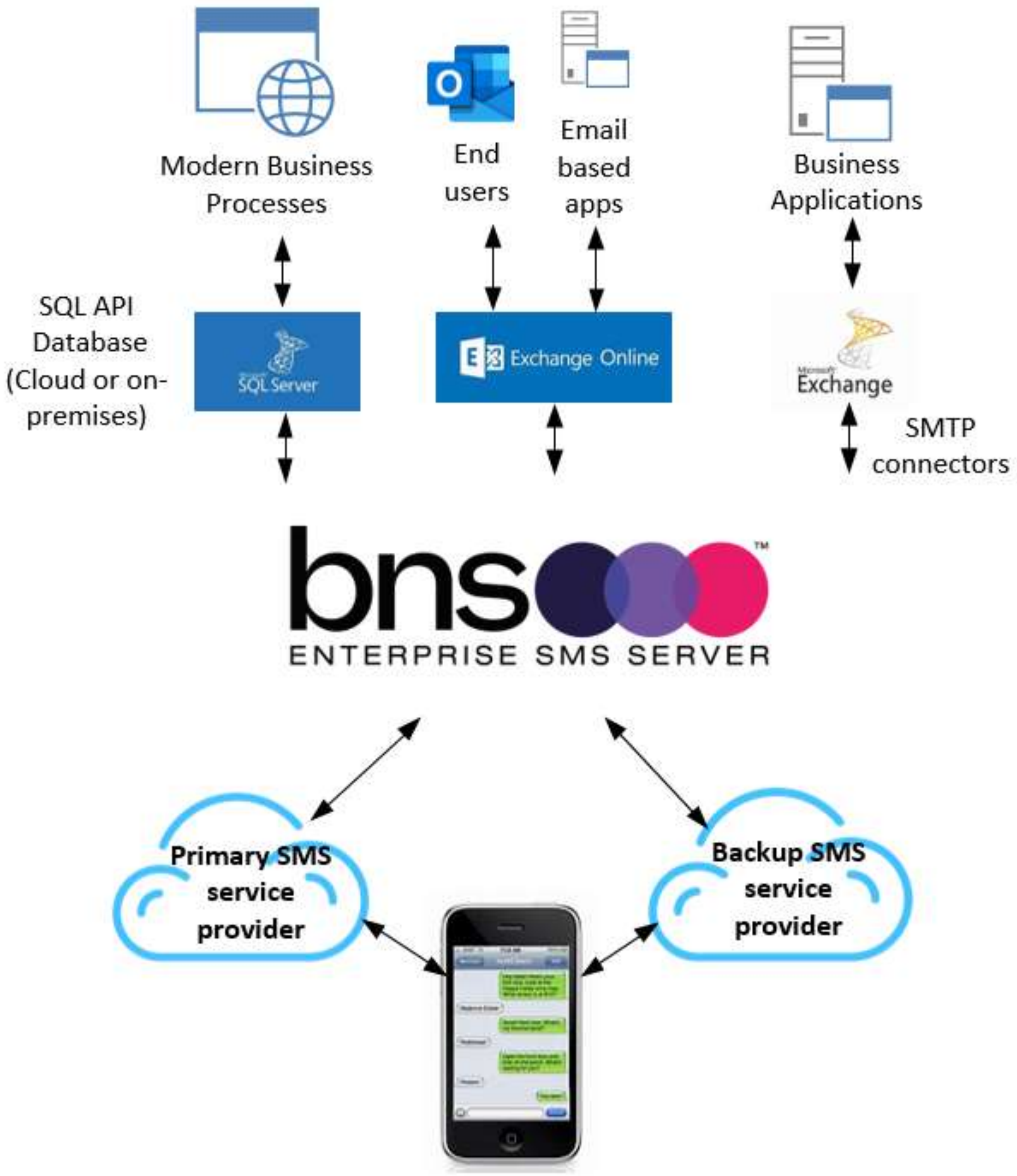
1.11 Checklist for New Installations

This checklist provides you with a list of tasks which must be completed by most customers installing the solution for the first time. Take a copy of this checklist and work your way through this deployment guide.

High level task list	Comments
Infrastructure requirements and firewall rules	
Obtain SMPP credentials from a certified SMS Service provider	
Preparing your SMS server	
Installation Folders	
Setup of SMS Databases in SQL Server	
Install SMS Console	
Installing the SMS Windows Services	
Starting Services	
Test Tool	
Health Service	
Establish your support internal and external support arrangements	
Review Knowledge base https://smskb.bnsgroup.com.au	

SECTION 2 Overall architecture

2.1 Conceptual overview diagram


Modern Business Processes
End users
Email based apps
Business Applications
SQL API Database (Cloud or on-premises)
SQL Server
Exchange Online
Microsoft Exchange
SMTP connectors
bns ENTERPRISE SMS SERVER
Primary SMS service provider
Backup SMS service provider

Refer to the public KB. https://smskb.bnsgroup.com.au/admin-guides

Refer to the public KB. https://smskb.bnsgroup.com.au/sqlinterface

2.2 SMTP Email based applications

BNS Enterprise SMS Server continues to support customers with on-premises Exchange based systems where applications and users send and receive via SMTP Connectors within the Exchange Email system.

As customers migrate their work loads to AWS, they are modernizing their approach to high availability and scalability in the cloud.

BNS recommends that customers using SMTP consider migrating to use the new SQL interface as the API rather than SMTP.

2.3 SQL API

BNS introduced an SQL based API in 2021 allowing customers to use SQL as a method to send and receive SMS messages.

Application developers probably use SQL already. SQL offers organisations a secure and high availability platform for fast processing of SMS content delivery.

SQL allows rich data analytics to be used leveraging meta data held in your database for every SMS transaction.

2.4 End users and Outlook

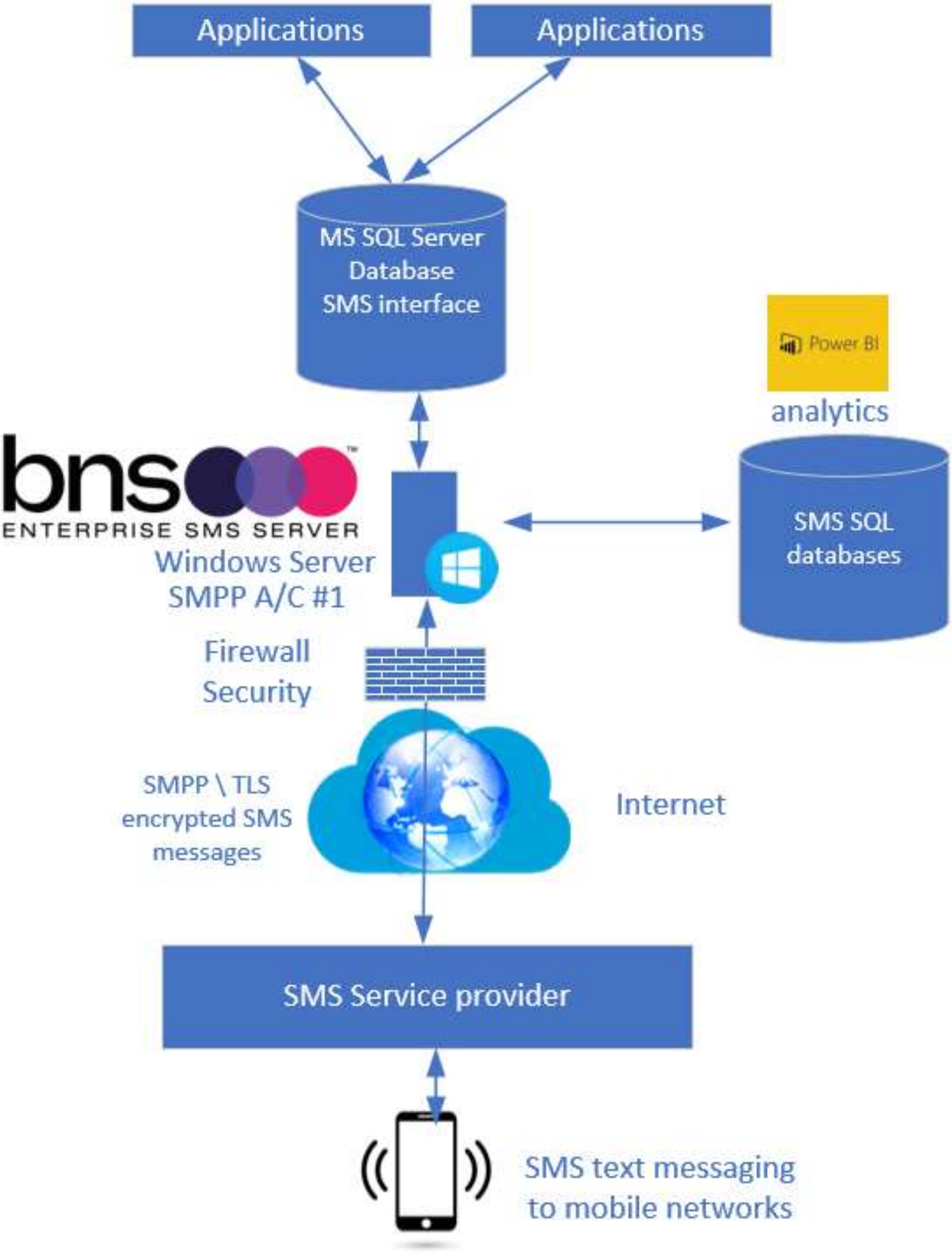
Microsoft Outlook coupled with Office 365 Exchange online is popular for enterprise customers.

BNS Enterprise SMS Server supports Microsoft's recommendations to use the Microsoft Graph API when developing any application working with their cloud based solutions.

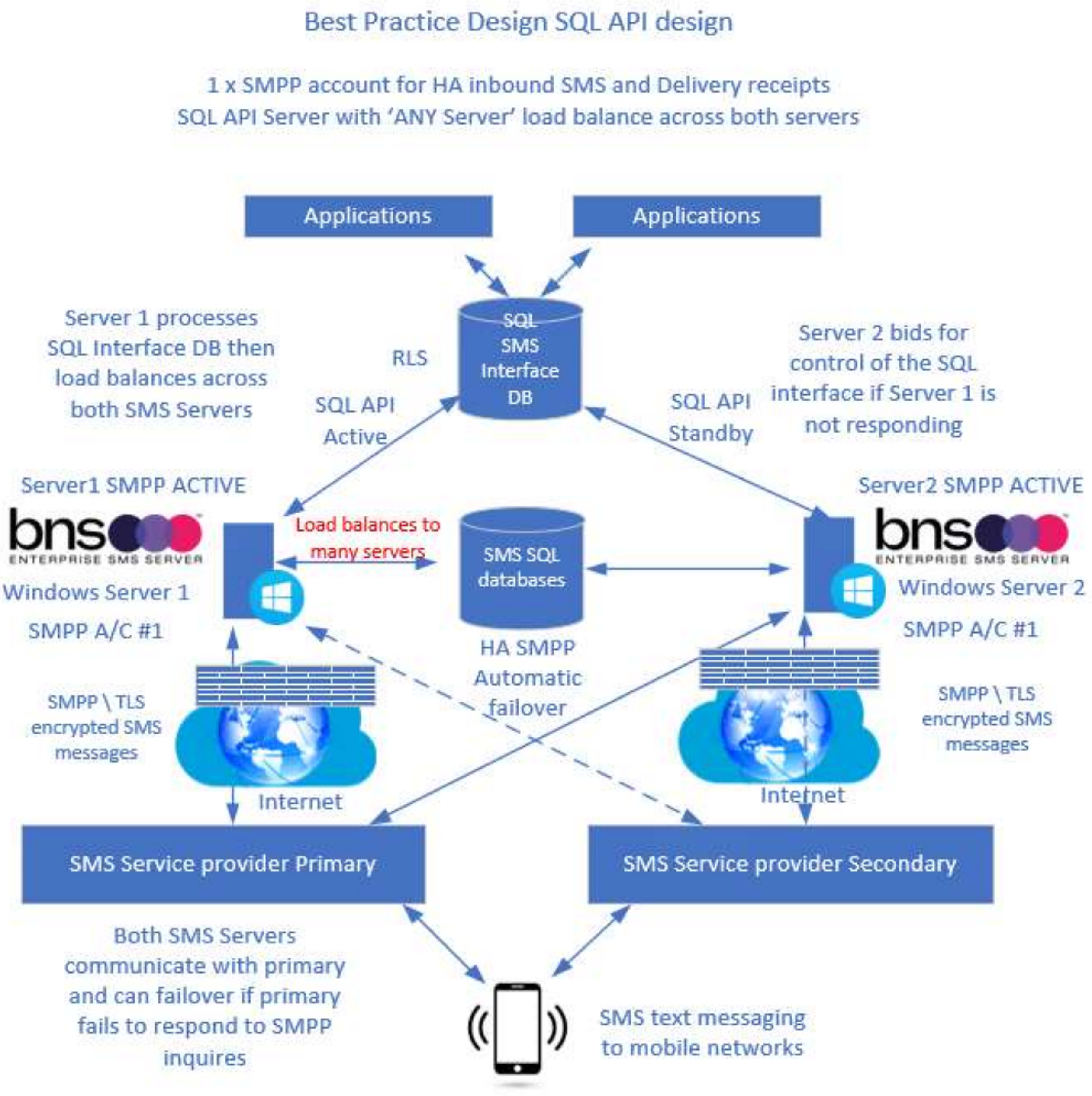
Selected end users or shared mailboxes can be offered one-way or two-way SMS messaging from Office 365.

SECTION 3 SQL API Architecture

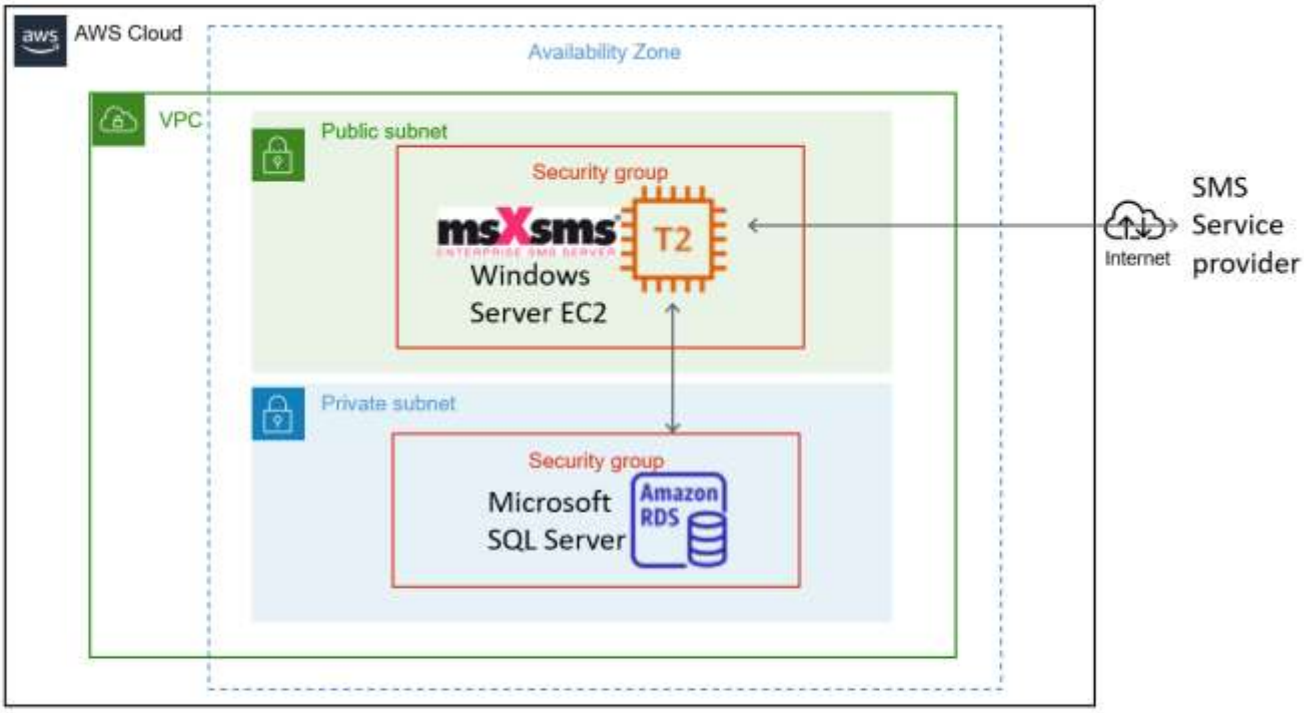
3.1 Simple design



3.2 High availability design


Best Practice Design SQL API design
1 x SMPP account for HA inbound SMS and Delivery receipts
SQL API Server with 'ANY Server' load balance across both servers
Applications
Applications
Server 1 processes SQL Interface DB then load balances across both SMS Servers
RLS
SQL SMS Interface DB
SQL API Active
SQL API Standby
Server 2 bids for control of the SQL interface if Server 1 is not responding
Server1 SMPP ACTIVE
Server2 SMPP ACTIVE
Load balances to many servers
SMS SQL databases
Windows Server 1
SMPP A/C #1
Windows Server 2
SMPP A/C #1
HA SMPP Automatic failover
SMPP \ TLS encrypted SMS messages
SMPP \ TLS encrypted SMS messages
Internet
Internet
SMS Service provider Primary
SMS Service provider Secondary
Both SMS Servers communicate with primary and can failover if primary fails to respond to SMPP inquires
SMS text messaging to mobile networks

3.3 AWS simple implementation architecture



A simple AWS implementation requires the following:

- 1 EC2 windows server instance in a public subnet. Windows server 2016, 2019, 2022 or better
- 1 x elastic fixed public IP is **optional** depending on SMS Service provider and your own security needs.
- 1 x SMPP Account with a SMS Service provider which BNS has tested with.
- 1 x Microsoft SQL Server or SQL Express AWS Relational Database Service
- License and service agreements with BNS Group and SMS Service provider

Refer to section 1.5.1 for sizing of EC2 instance and RDS database

Windows Domain

The Windows server can be in an Active Directory domain or standalone server in a workgroup.

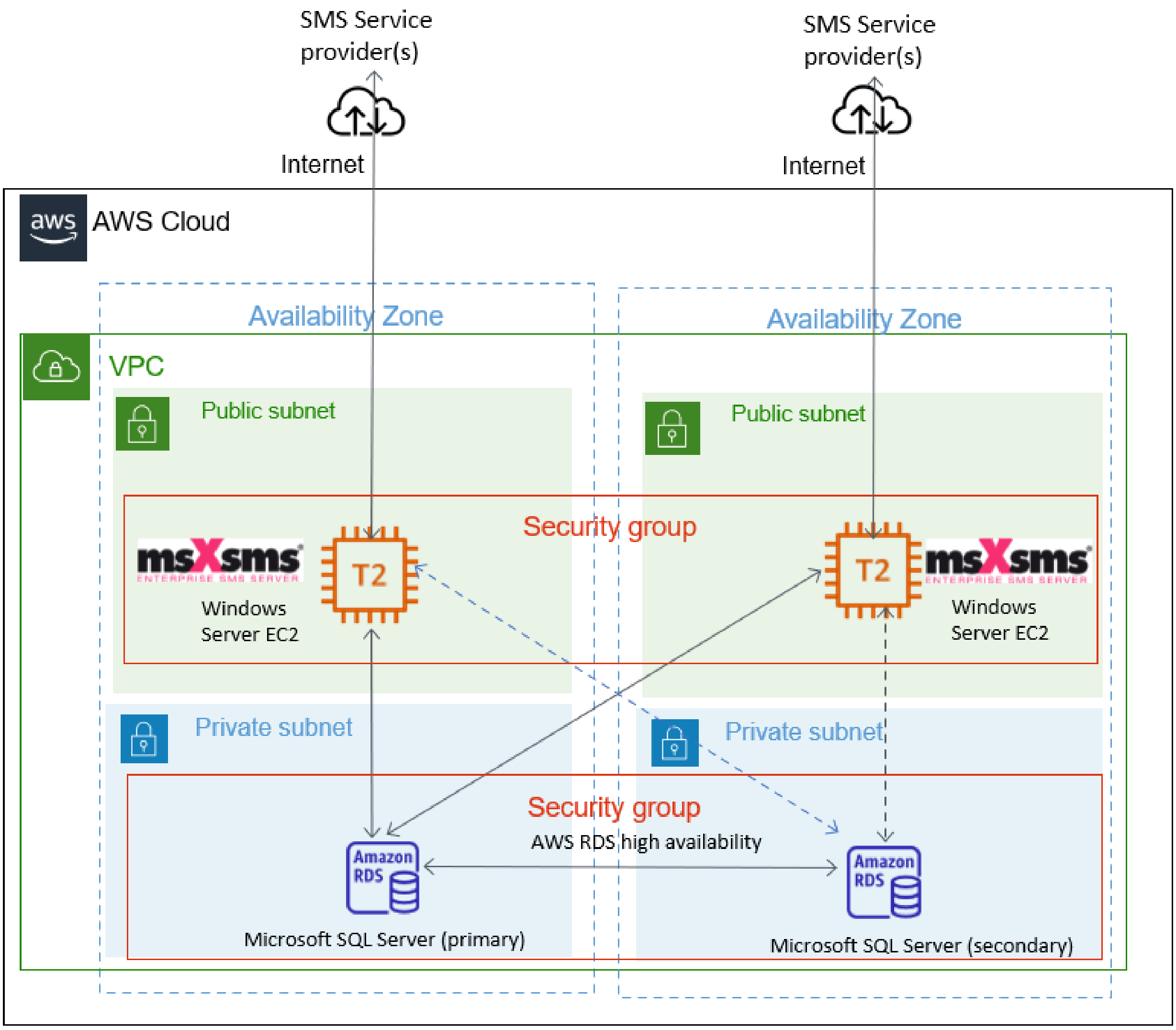
SQL permissions

The SMS Server software can use Windows authentication or SQL Local user authentication to access Microsoft SQL Server.

SMTP sending email

Office 365 secure SMTP\TLS is the default for sending error messages to system administrators. Other SMTP options exist for example sending to an internal SMTP Server.

3.4 AWS High Availability Architecture



High availability requires the following:

- 2 EC2 windows server instance in a public subnet(s). Windows server 2016, 2019, 2022 or better
- 2 x elastic fixed public IP is optional depending on SMS Service provider and your own security needs.
- Minimum of 1 x SMPP Account with 1 x SMS Service provider which BNS has tested with.
- High availability Microsoft SQL Server multi-AZ.
- Minimum of 1 x Microsoft SQL Server Database Service
- License and service agreements with BNS Group and at least 1 SMS Service provider.

The above diagram shows 2 SMS servers in different availability zones accessing Microsoft SQL Server in zone 1. Zone 2 has a secondary SQL server which can be automatically activated by the AWS RDS service within a few minutes.

BNS Enterprise SMS Server software automatically attempts to reconnect to the AWS RDS SQL Server end point connection string allowing the use of a secondary AWS RDS SQL Server in another zone.

Windows Domain

The Windows server can be in an Active Directory domain or standalone.

AWS EC2 instance sizing

Refer to section 4.1.1 for sizing. 2 x EC2 instances T3.2XLarge is recommended for large enterprise.

SQL permissions

BNS Enterprise SMS Server software can use Windows authentication or SQL Local user authentication to access Microsoft SQL Server.

SMTP sending email

Office 365 secure SMTP\TLS is the default for sending error messages to system administrators. Other SMTP options exist for example sending to an internal SMTP Server.

3.4.1 Other options

- Multi-AZ recommended but you could use multiple SMS servers in a single AZ.
- 1 x AWS RDS Service – Microsoft SQL Server configured according to the level of availability required by the customer
- Agreements with BNS Group and at least 1 x SMS Service provider

Notes:

1. Customer can use a single SMS service provider in this design.
2. 2 or more EC2 windows servers provide high availability processing across 1 or more SMS service providers.
3. Business applications are responsible for processing their own SMS data from the SMS-SQL-API Database. Each business application has its own ID to identify which transactions belong to their application.

SECTION 4 Infrastructure

4.1 Infrastructure requirements

4.1.1 Minimum AWS pre-requisites and requirements (Single AZ)

AWS service	Size \ type	Comments
EC2 instance type startup business	T2.Large	8GB RAM with 2 x vcpu
EC2 instance type large enterprise business	T3.2xLarge	32GB RAM with 8 vcpu
AMI type	AWS AMI Windows Server 2016 standard or better	
RDS MS SQL	AWS RDS Microsoft SQL Server	SQL Express can be used for proof of concepts only
Subnets	Public subnet for EC2 instance Private subnet for MS SQL Server	

Description	Requirement	Comments
Operating system	Windows Server 2016, 2019, 2022	
SMPP SMS protocols	SMPP\TLS	TLS 1.2
Directory services	Active Directory (optional)	If not available then a local user service account can be used
SQL Server	Microsoft SQL Server in a single availability zone	AWS RDS SQL Express is supported for proof of concepts
Email & DNS	On-premises Exchange mailbox or Office 365 email account for use by the SMS software for alerting administrators	DNS is required to resolve smtp.office365.com if using Office 365.

Firewall rules	Allow outgoing SMPP protocol on specific ports for bi-directional SMS communications	If outgoing rules are required, the firewall team will be required to allow outgoing SMPP protocol on a port from internal IP addresses to external IP addresses. Contact BNS for further information.

4.2 SQL Server

SQL Server software specifications

Software	Mandatory or optional	AWS RDS Service
Microsoft SQL Server	Mandatory	The SMS Software supports all versions of Microsoft SQL Server. AWS RDS Mult-AZ is supported. For more information about Multi-AZ deployments for AWS RDS for Microsoft SQL Server refer to Multi-AZ deployments for Amazon RDS for Microsoft SQL Server - Amazon Relational Database Service

4.2.1 Minimum AWS RDS MS SQL Server requirement

RDS MS SQL Express is the minimum requirement for a single-AZ deployment ideal for proof of concepts only.

RDS MS SQL Server is required for production deployments in a single-AZ.

4.2.2 AWS RDS Sql Server best practices on how Multi AZ works

- RDS Multi-AZ deployments provide high availability and automatic failover support for DB instances
- Multi-AZ helps improve the durability and availability of a critical system, enhancing availability during planned system maintenance, DB instance failure, and Availability Zone disruption.
- RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different AZ.
- RDS performs an automatic failover to the standby, so that database operations can be resumed as soon as the failover is complete.
- RDS Multi-AZ deployment maintains the same endpoint for the DB Instance after a failover, so the application can resume database operation without the need for manual administrative intervention.
- **Multi-AZ is a High Availability feature and NOT a scaling solution for read-only scenarios; a standby replica can't be used to serve read traffic. To service read-only traffic, use a Read Replica.**
- For more information refer to https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_SQLServerMultiAZ.html

4.2.3 AWS RDS SQL Server version support

The solution supports currently available versions (2016, 2017, 2019) of Amazon RDS Microsoft SQL Server (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html)

BNS has tested Microsoft SQL Server 2022 on Windows Server 2022. As AWS release RDS SQL Server 2022, BNS will test that version of RDS.

Newer versions of RDS Microsoft SQL Server will be tested as soon as possible after released by AWS.

4.2.4 Deploying RDS SQL Server

To deploy RDs SQL Server, the high level steps are –

1. Navigate to RDS console in the AWS Management console and hit Create Database
2. Choose Microsoft SQL Server, Amazon RDS and appropriate SQL Server edition. The software works well with the Express edition.
3. Choose SQL Server version and provide a name in the DB instance identifier.
4. Provide credential information and choose a suitable instance class. Choose storage type and the allocated storage.
5. Software Server supports both single-AZ as well as Multi-AZ RDS instance. Choose the deployment type as per your preference.
6. Keep Public access as 'No' as per security best practice. The RDS instance do not need to be accessible from the Internet.
7. Choose the VPC and the Security groups.
8. Enable Performance Insights to monitor the database load
9. Validate rest of the options and hit Create Database to launch RDS instance.

For step by steps to launch RDS instance, refer to the AWS tutorial - https://aws.amazon.com/getting-started/hands-on/create-microsoft-sql-db/.

For additional details on RDs SQL server, please refer to the AWS public documentation - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html

4.2.5 RDS Connectivity from SMS Servers

BNS Enterprise SMS Server SQL drivers supports both - Single-AZ as well as Multi-AZ RDS SQL Server.

BNS Enterprise SMS Server uses the RDS SQL Server endpoint in the connection string.

BNS Enterprise SMS Server SQL driver doesn't support MultiSubnetFailover for

RDS Multi-AZ but retries the connection during the database failover and re-connects automatically post failover.

4.2.6 AWS RDS SQL Database monitoring

The RDS SQL Server can be monitored using AWS CloudWatch or any other 3rd party tool of your preference. As a best practice, you should monitor and create alarms for the following events –

- Availability – The availability of the RDS SQL server and any event of failover, reboot, deletion or maintenance.
- Configuration Change – Any change in the configuration like instance class change, security group or parameter group change should be monitored
- Low Storage – The storage should be monitored to avoid any disruption
- Performance – The performance must be monitored using Cloudwatch metrics like CPU utilization, Freeable memory, IOPS and latency.

For Database load monitoring, Performance insights should be enabled and monitored.

For details on the monitoring tools & the event notification provided by AWS, please refer to the AWS public documentation - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html

4.2.7 AWS RDS SQL Database troubleshooting

In an unlikely event of disruption to the service both the Database and Application should be checked and troubleshooted. High level steps to troubleshoot the RDS SQL Server instance are –

- Check for RDS events related to availability, reboot or failure
- Try connecting to the RDS instance manually
- Check performance metrics and performance insights to rule out heavy load issue
- Check the events related to security group to make sure that the security groups haven't changed.

Refer to the AWS troubleshooting guide to troubleshoot common scenarios - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Troubleshooting.html

4.2.8 To launch EC2 instance Windows Server

BNS Enterprise SMS Server software will be installed on the Virtual server. Launch 2 x EC2 servers to deploy the solution in high availability configuration. The high level steps to launch EC2 server are - as below –

- Open the Amazon EC2 console in AWS Management console
- In the navigation bar at the top of the screen, the current AWS Region is displayed . Make sure it is displaying the correct region.
- From the Amazon EC2 console dashboard, choose Launch instance.
- Under Name and tags, for Name, enter a descriptive name for your instance.
- Under Application and OS Images (Amazon Machine Image), choose Quick Start, and then choose the windows operating system (OS) for your instance.
- Under Key pair (login), for Key pair name, choose an existing key pair or create a new one.
- In the Summary panel, choose Launch instance.

For further details on launching EC2, please refer to AWS Public documentation - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-instance-wizard.html

4.3 SQL Server Database creation

This is documented in section 8 of this guide. Section 7 installs the software on the SMS Windows server which makes available the SQL DDL scripts required by the SQL admin to create the databases.

4.4 Availability zones

BNS Enterprise SMS Servers can be deployed in a single availability zone or across multiple availability zones (Multi-AZ).

High performance access to SQL Server is required.

Deployment across multiple regions would best be implemented using an instance of the SMS servers and databases within a region. This provides optimal performance for high speed SMS messaging for an enterprise.

4.5 Connectivity to SMS Network Service providers

4.5.1 Encryption of SMS data over the Internet

The software uses SMPP\TLS to encrypt the data.   TLS version 1.2 min is used.

4.6 SMS Service Account

A single SMS Service Account is required for use by ALL SMS Servers.

- Create a user account for the service using Active Directory users and computers or for a non-active directory implementation use a local user using computer management.
- Assign permissions to the service account to enable SMS Windows services to access: AD/DNS, SQL databases.
- This service account must be added to the local administrators group of the SMS server.

4.7 Deployment effort & resources

Depending on the complexity of your design and security determines the amount of time required to deploy a full solution.

A simple deployment with 1 SMS Server in 1 availability zone could be setup within 1 week if SQL admins, security teams, firewall teams etc all work together to implement the required components, firewall rules and other components required for a proof of concept.

AWS links for provisioning https://aws.amazon.com/ec2/getting-started/

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.CreatingConnecting.SQLServer.html

Enterprise designs for production typically take a long time for many reasons.

Skills and Resources required:

- General AWS cloud administration skills
- AWS networking skills

- Amazon EC2 skills
- Amazon RDS database skills
- Windows Server administrator skills
- Windows Active Directory knowledge (if AD is used)
- AWS network security skills

Summary:

- SQL Administrator to setup 3 databases on Microsoft SQL Server. Standard DDL scripts are provided for the SQL admin to execute when the databases have been created.
- Windows server deployment team to deploy 1 or more SMS Servers. For example EC2 instance in AWS using Windows Server 2022 Base AMI.
- Security team – to understand what if any outgoing port rules are required for internal SMS Windows servers to communicate with SMS Service providers.
- Legal – to contract with BNS or its partners for server licensing, support and maintenance.

4.8 Certified SMS Service providers

The SMS software has been fully tested with SINCH and MessageMedia.

www.sinch.com

www.messagemedia.com

Both companies provide global coverage for SMS delivery.

Primary AWS region supported is ap-southeast-2

4.8.1 Other SMPP service providers

SMPP version 3.4 is an industry standard. However, there are many considerations regarding inter-operability and optional implementations within the standard.

BNS has tested with many service providers. For more information contact our support team.

4.9 AWS Security

4.9.1 IAM roles

To deploy an EC2 Windows Server instance will require an IAM role with the least privilege permissions policy. The policy is documented in section 4.9.3 below.

You may already have an IAM role already configured for this purpose. If not create an IAM role called “Deploy EC2 Instance for SMS Server”.

For more information on IAM Roles refer to this link https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

To deploy the associated AWS RDS MS SQL Database will require an IAM role with the least privilege permissions policy. The policy is documented in section 4.9.5 below.

You may already have an IAM role already configured for this purpose. If not create an IAM role called “Deploy RDS MS SQL Server for SMS Server”.

- EC2 Windows administration is performed using Windows local or Active Directory user logins to the Windows Server.
- RDS MS SQL Database administration is managed using Microsoft SQL Management Studio. SQL Server authentication is required.

4.9.2 AWS Managed policies

AWS recommend using policies that grant least privilege, or granting only the permissions required to perform a task. The most secure way to grant least privilege is to write a custom policy with only the permissions needed by your team. You must create a process to allow your team to request more permissions when necessary. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need.

There are two AWS managed policies AdministratorAccess and DatabaseAdministrator which are documented in this link https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html

These two AWS managed policies can be used as a base to create new policies customising them for least privileges for managing EC2 instances and RDS MS SQL databases.

4.9.3 To launch EC2 instance Windows Server

To complete a launch successfully, users must be given permission to use the `ec2:RunInstances` API action, and at least the following API actions:

- `ec2:DescribeImages`: To view and select an AMI.
- `ec2:DescribeInstanceTypes`: To view and select an instance type.
- `ec2:DescribeVpcs`: To view the available network options.
- `ec2:DescribeSubnets`: To view all available subnets for the chosen VPC.
- `ec2:DescribeSecurityGroups` or `ec2:CreateSecurityGroup`: To view and select an existing security group, or to create a new one.
- `ec2:DescribeKeyPairs` or `ec2:CreateKeyPair`: To select an existing key pair, or to create a new one.
- `ec2:AuthorizeSecurityGroupIngress`: To add inbound rules.

For more information refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policies-ec2-console.html#ex-launch-wizard

4.9.4 JSON Policy to launch EC2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*"
    }
  ]
}
```

For more information refer to Example policies for working in the Amazon EC2 console - Amazon Elastic Compute Cloud

4.9.5 Policy to grant permission to create a RDS DB instance and isn't Multi-az

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMSSQLCreate",
      "Effect": "Allow",
      "Action": "rds:CreateDBInstance",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:DatabaseEngine": "mssql"
        },
        "Bool": {
          "rdds:MultiAz": false
        }
      }
    }
  ]
}
```

4.9.6 Other security considerations

The only permissions required are those permissions required to create SQL Databases and EC2 instances.

- SMS Software does not require AWS root privileges for deployment or operation.
- SMS Software requires the permissions described in this document which include SQL Access and access by its windows services to access the Windows Server files and folders.
- No public resources such as S3 buckets
- No keys are required other than the initial EC2 instance for windows which the EC2 customer administrator has and secures.
- RDS SQL local user credentials are required during the installation. These are provided by the RDS SQL administrator to the installation team.
- No specific outgoing network security group rules are required if the default policy allowing ALL outgoing traffic from the public subnet NSG is allowed.
- No specific incoming network security group rules for the public subnet are required for the SMS software to operate.
- Sensitive data is secured within SQL Server databases
- SMS Software encrypts data in transit between AWS and SMS Service providers using SMPP\TLS. TLS version 1.2 and 1.3 is supported.

4.9.7 AWS Encryption EC2 – SMS Windows Server

Amazon EBS encryption as a straight-forward encryption solution for your EBS resources associated with your EC2 instances. With Amazon EBS encryption, you aren't required to build, maintain, and secure your own key management infrastructure. Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots.

For more information refer to AWS documentation at the link below:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

4.9.8 AWS Encryption RDS – SMS Data stored in Microsoft SQL Server

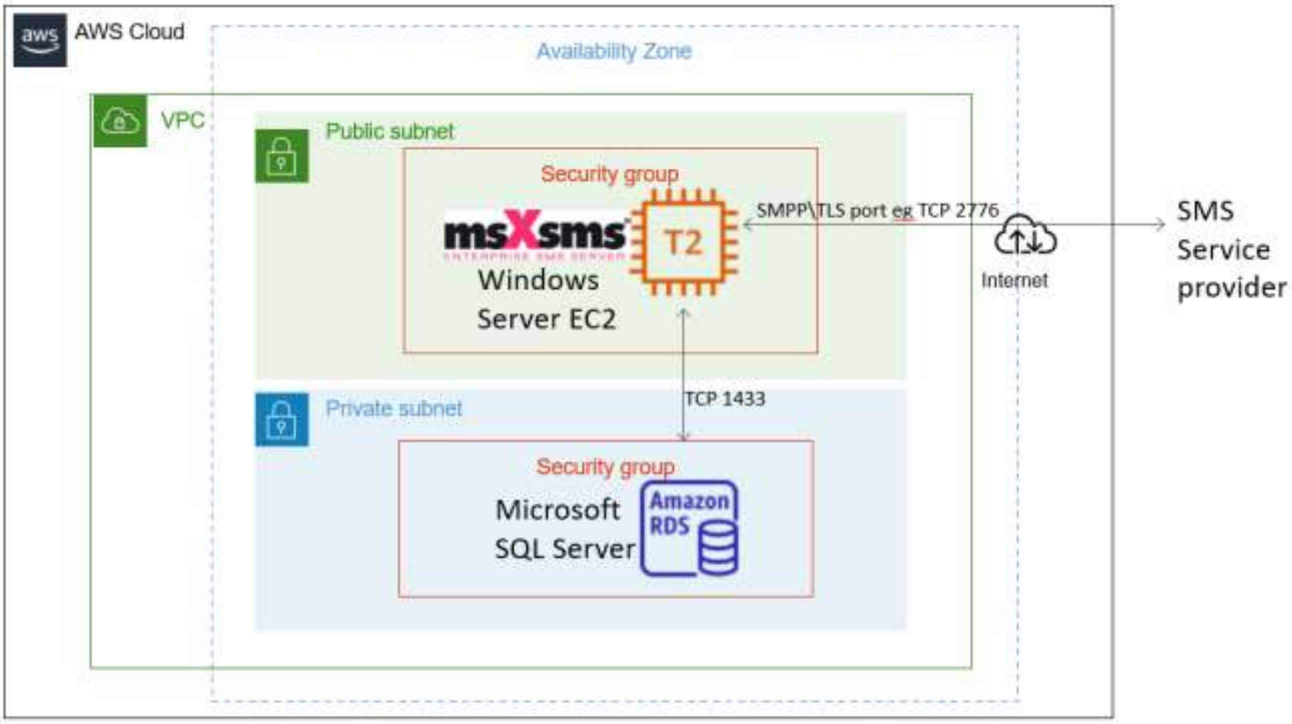
Amazon RDS can encrypt your Amazon RDS DB instances. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots.

Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances. After your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance.

For more information refer to AWS documentation at the link below:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

4.9.9 AWS architecture – Security Groups and Network ACLs



4.9.9.1 Network ACLs

Network ACLs in the public subnet must allow for traffic to flow between the Internet and the public subnet. A VPC public subnet with an Internet gateway is generally configured to allow all traffic to flow in and out of the public subnet.

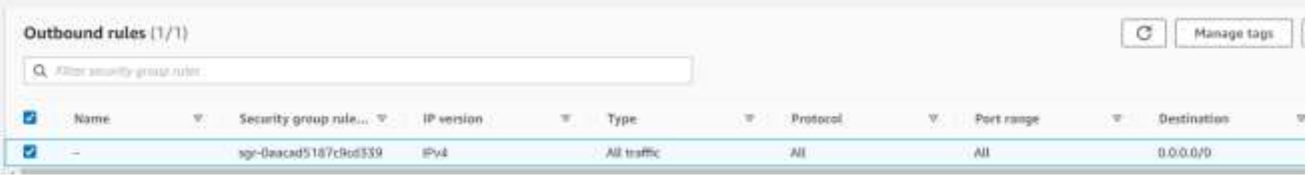
Customers use Security Groups to control access to the EC2 Windows Server hosting the SMS software and the Internet

4.9.9.2 Security Groups

Public Subnet Security Group

A security group is required for the public subnet to control access to\from the Internet.

Below shows an example of an outbound security group for the EC2 Windows SMS server allowing all traffic outbound to the Internet.



Outbound rules (1/1)

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Destination
☑	–	sgr-0aacad5187c9cd339	IPv4	All traffic	All	All	0.0.0.0/0

SMPP\ TLS security

The SMS Server establishes an outbound connection to a SMS Service provider using a port they support for SMPP with TLS encryption.

SMS Service providers do not make any inbound connections to the SMS Server. BNS Enterprise SMS Server uses separate SMPP Transmitter and SMPP Receiver binds. Connection is established from the SMS software to the SMS service provider for both SMPP Transmitter and SMPP Receiver binds.

Inbound security group rules (public subnet)

As mentioned above, no inbound custom rules are required between the SMS Service provider on the Internet and the SMS Server on the VPC public subnet.

RDS DB instance security group rules

The DB instance running on RDS MS SQL Server only needs to be available to the SMS Server, and not to the public Internet, a customer will create a VPC with both public and private subnets. The SMS server is hosted in the public subnet, so that it can reach the public Internet.

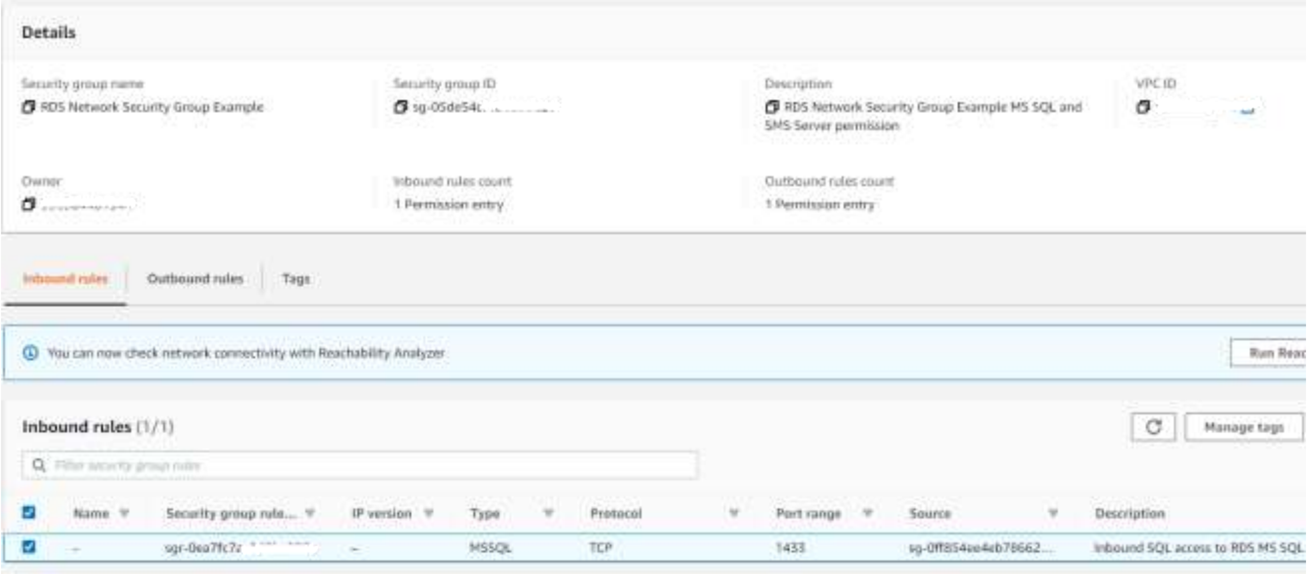
The DB instance is hosted in a private subnet. The SMS Server is able to connect to the DB instance because it is hosted within the same VPC, but the DB instance is not available to the public Internet, providing greater security.

Security group rules need to be set to allow inbound custom rules from the public subnet to the private subnet.

Create the rules between security groups is well documented at https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html

Inbound security group rules to RDS MS SQL Server

An inbound rule must be created to allow access from your EC2 Windows SMS Server.



Details

Security group name
RDS Network Security Group Example

Security group ID
sg-05de54c[redacted]

Description
RDS Network Security Group Example MS SQL and SMS Server permission

VPC ID
[redacted]

Owner
[redacted]

Inbound rules count
1 Permission entry

Outbound rules count
1 Permission entry

You can now check network connectivity with Reachability Analyzer

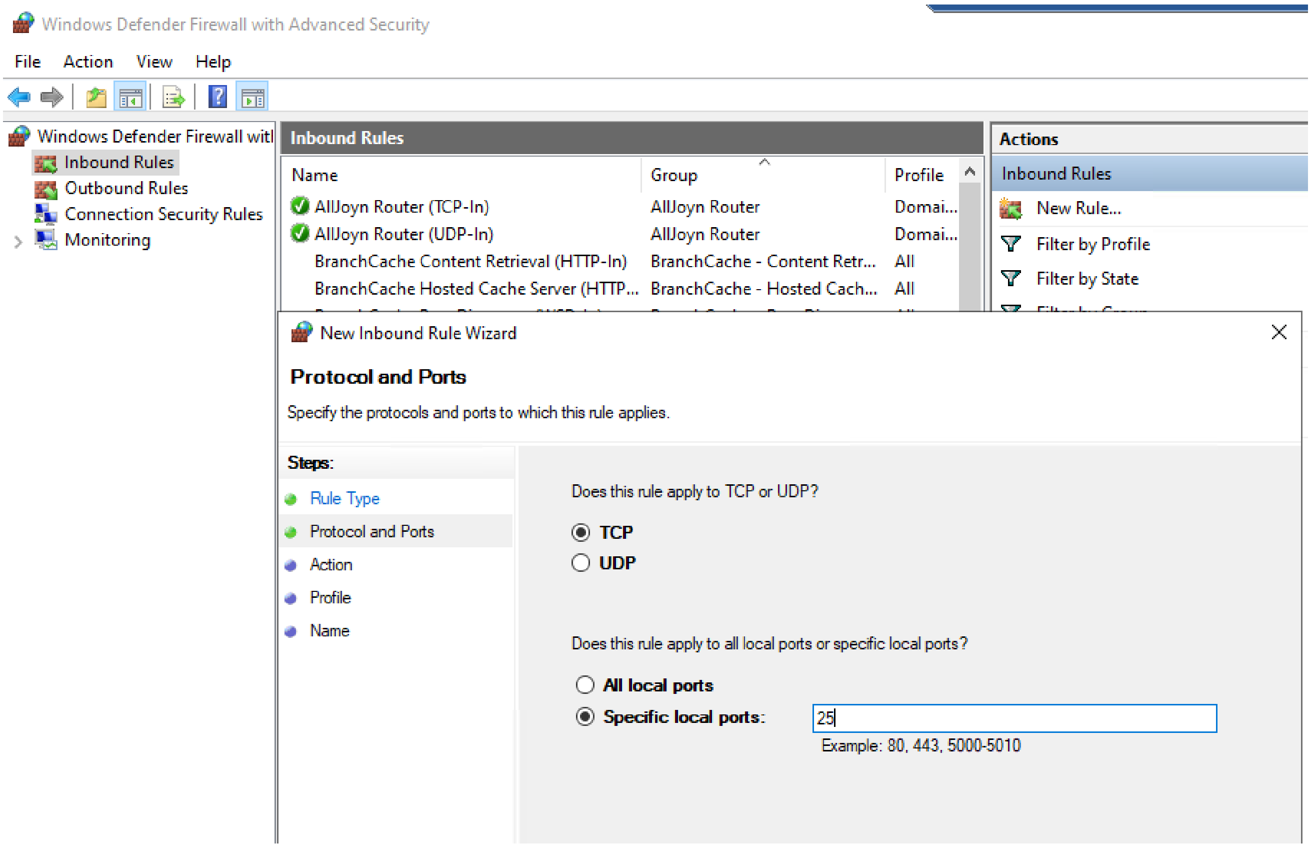
Inbound rules (1/1)

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-0ea7fc7z[redacted]	–	MSSQL	TCP	1433	sg-0ff854ee4eb78662...	Inbound SQL access to RDS MS SQL

SECTION 5 Preparing your SMS server

5.1 Windows Server Operating System

- Perform a typical installation of Windows Server in a domain if you have an Active Directory domain. The software can work without a domain such as in a DMZ.
- If your design has on-premises Exchange then allow port 25 inbound on the SMS Server. There is a whitelist option to allow only connections from specific IP addresses in the smsboot.ini file.



Inbound Rules

Name	Group	Profile
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 25

Example: 80, 443, 5000-5010

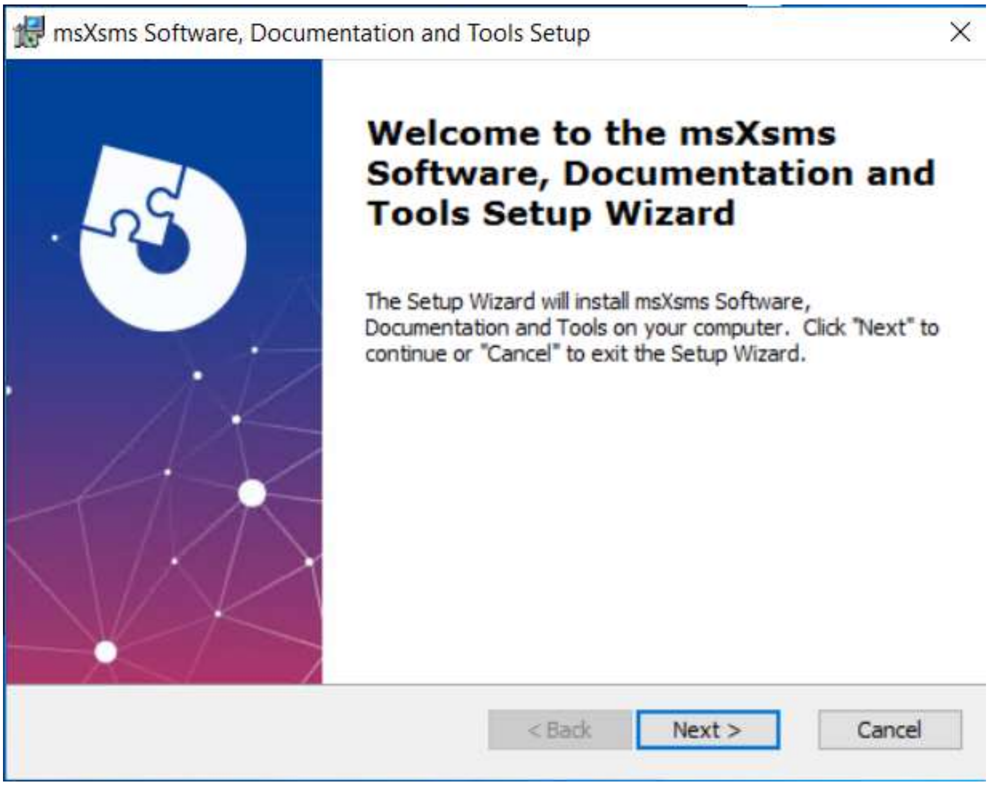
- Example above is Windows Defender firewall allow inbound rule port 25

SECTION 6 Installation folders

6.1 Installing the installation files

Note: **This step is required first because it extracts the SQL scripts available along with other files.**

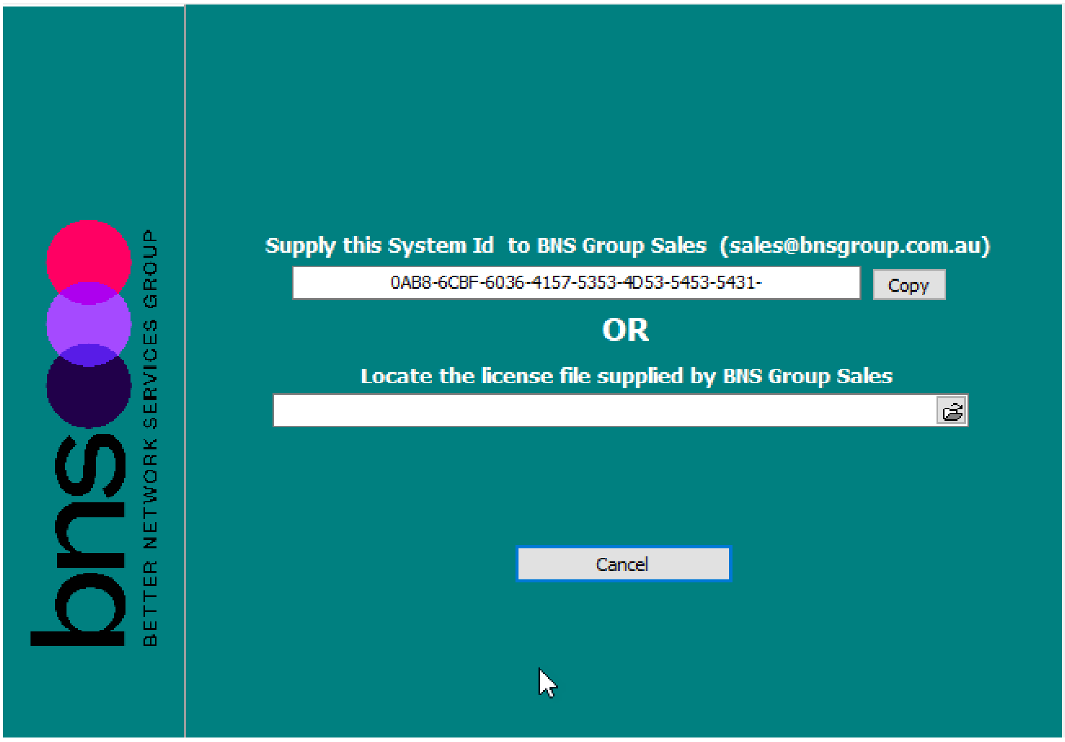
- Download the SMS Software from https://smskb.bnsgroup.com.au/downloadV2
- Extract the files to a location on the Windows Server where you will install the software.
- Run the command prompt elevated (Right click the Start icon and select Command Prompt (Admin)
- From within the command prompt run the MSI Installer install_sms.msi
- Follow the wizard.



msXsms Software, Documentation and Tools Setup

Welcome to the msXsms Software, Documentation and Tools Setup Wizard

The Setup Wizard will install msXsms Software, Documentation and Tools on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

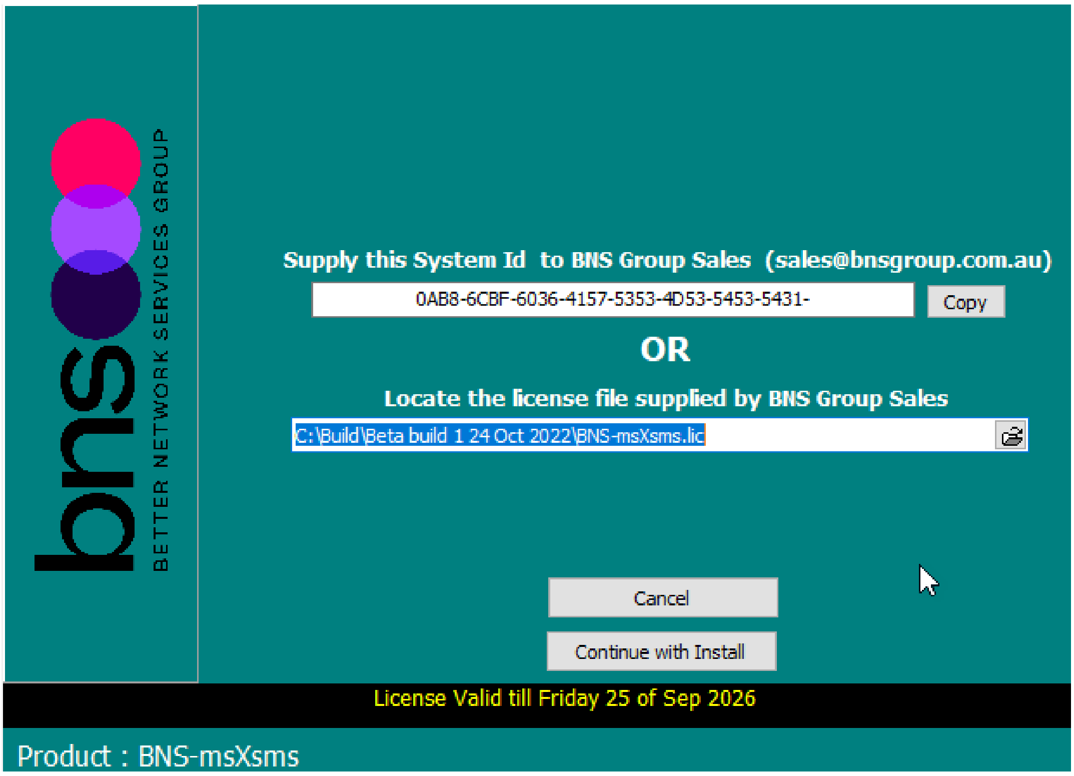


Supply this System Id to BNS Group Sales (sales@bnsgroup.com.au)

0AB8-6CBF-6036-4157-5353-4D53-5453-5431-

Locate the license file supplied by BNS Group Sales

- A license file is required at installation time. Contact your integration partner for a limited trial license or a production license key. The System ID is displayed on the wizard and will be required for a license key to be generated.
- Example shown below.



Supply this System Id to BNS Group Sales (sales@bnsgroup.com.au)

0AB8-6CBF-6036-4157-5353-4D53-5453-5431-

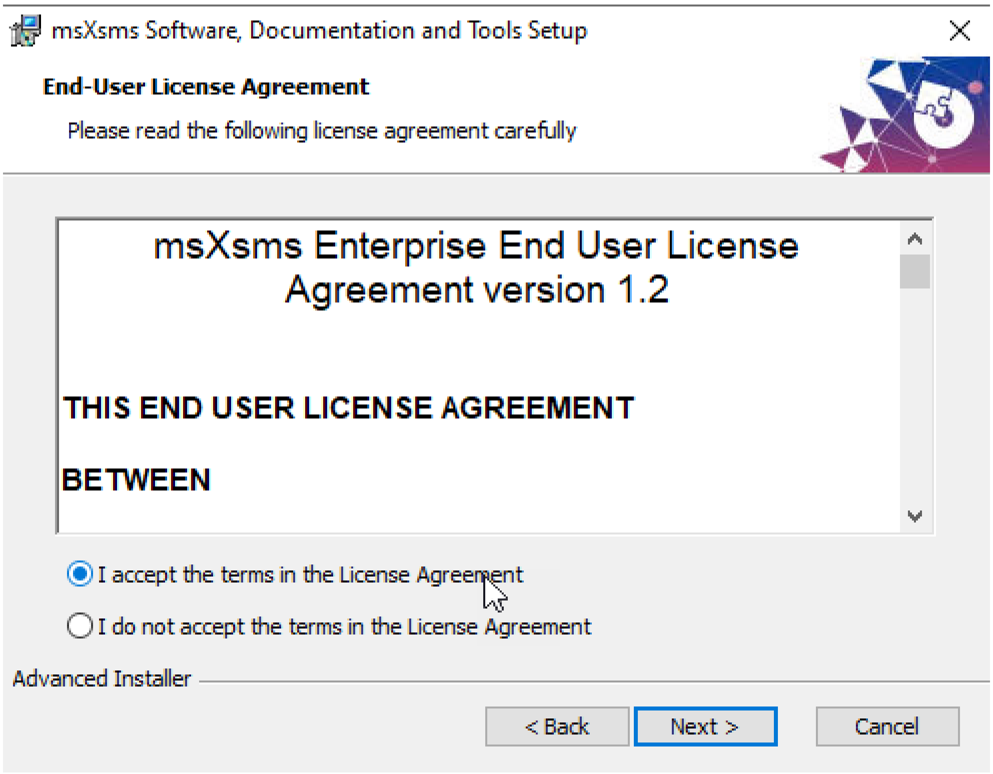
Locate the license file supplied by BNS Group Sales

C:\Build\Beta build 1 24 Oct 2022\BNS-msXsms.lic

License Valid till Friday 25 of Sep 2026

Product : BNS-msXsms

- Press continue



msXsms Software, Documentation and Tools Setup

End-User License Agreement

Please read the following license agreement carefully

msXsms Enterprise End User License Agreement version 1.2

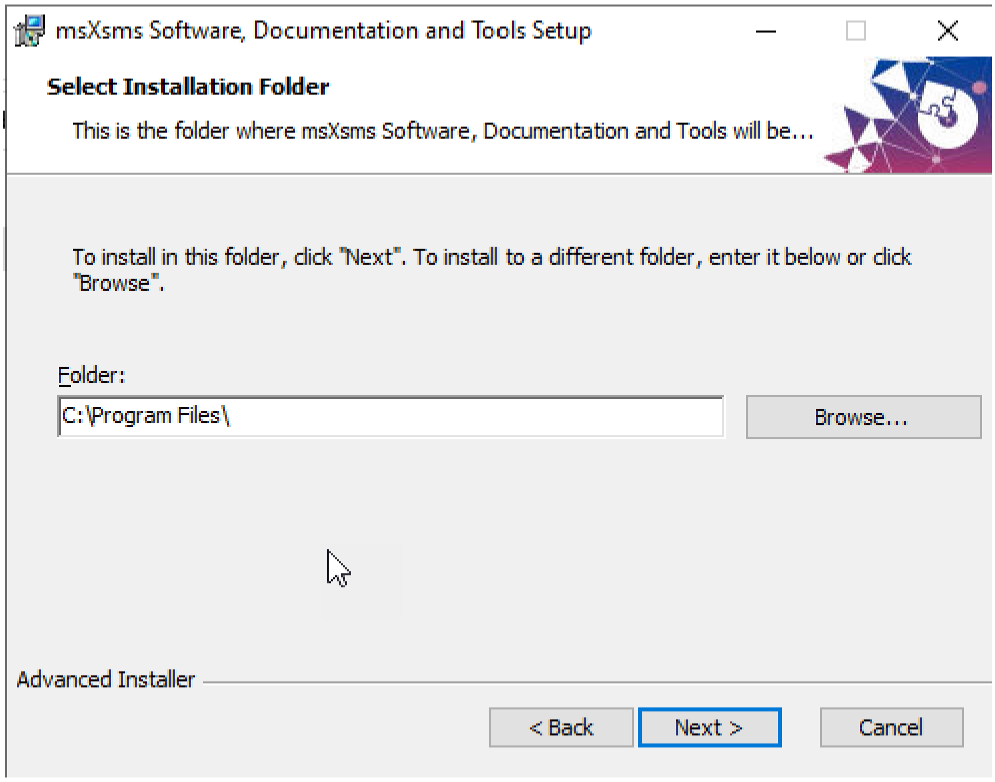
THIS END USER LICENSE AGREEMENT

BETWEEN

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

- Change the driver letter only if you have an application volume.



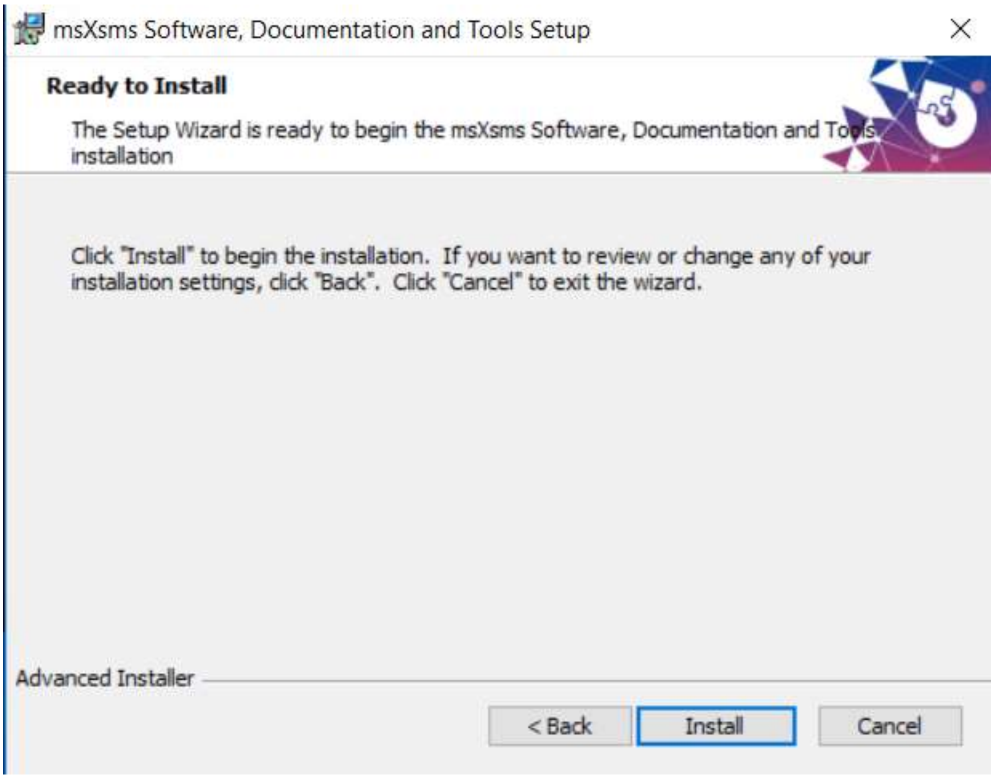
msXsms Software, Documentation and Tools Setup

Select Installation Folder

This is the folder where msXsms Software, Documentation and Tools will be...

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\

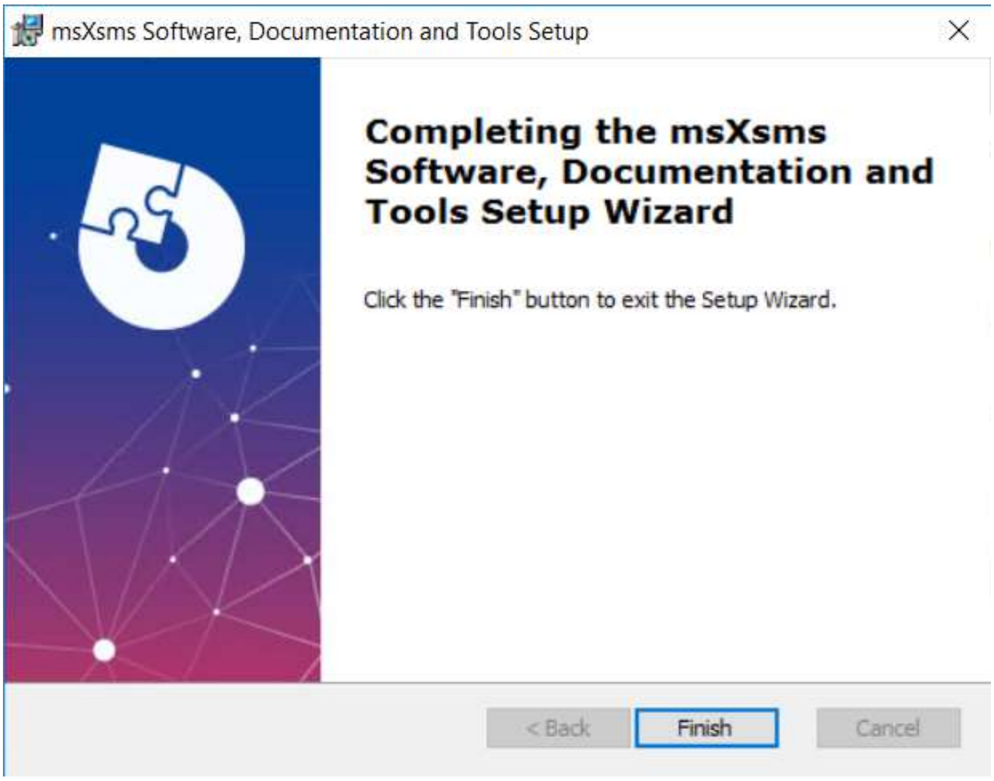


msXsms Software, Documentation and Tools Setup

Ready to Install

The Setup Wizard is ready to begin the msXsms Software, Documentation and Tools installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

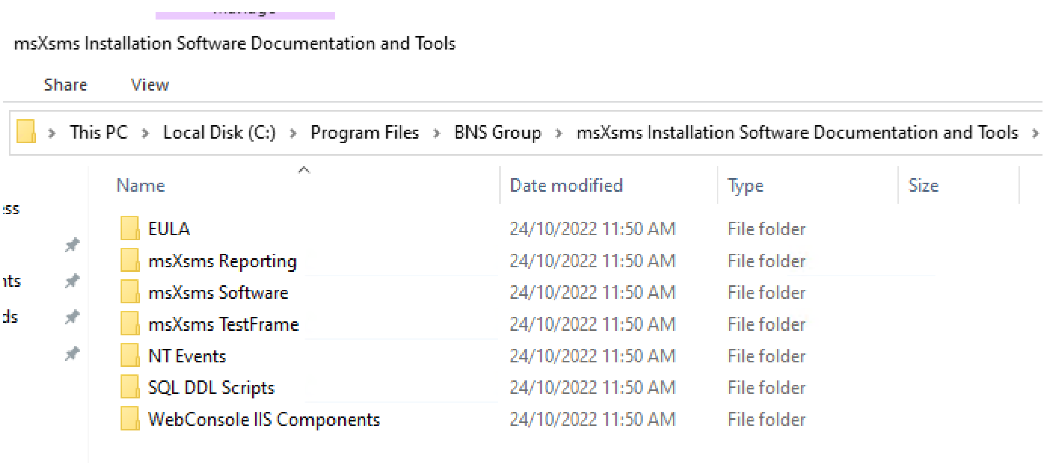


msXsms Software, Documentation and Tools Setup

Completing the msXsms Software, Documentation and Tools Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

- A license key is required at installation time. Contact your integration partner for a limited trial license or a production license key. The System ID is displayed on the wizard and will be required for a license key to be generated.



msXsms Installation Software Documentation and Tools

This PC > Local Disk (C:) > Program Files > BNS Group > msXsms Installation Software Documentation and Tools >

Name	Date modified	Type	Size
EULA	24/10/2022 11:50 AM	File folder	
msXsms Reporting	24/10/2022 11:50 AM	File folder	
msXsms Software	24/10/2022 11:50 AM	File folder	
msXsms TestFrame	24/10/2022 11:50 AM	File folder	
NT Events	24/10/2022 11:50 AM	File folder	
SQL DDL Scripts	24/10/2022 11:50 AM	File folder	
WebConsole IIS Components	24/10/2022 11:50 AM	File folder	

Note: msXsms reporting to be called msXsms Analytics

Web console to be called Cloud Console IIS Components

SECTION 7 Setup databases in AWS RDS Microsoft SQL Server

Most enterprise customers already have a central SQL Server platform which should be used. Microsoft SQL Server and SQL Express are supported in AWS. SQL Express is only to be used for proof of concepts

AWS RDS MS SQL Server endpoint and port information is available in the AWS Console under RDS, Databases.

AWS RDS endpoint connection string must be used. Do not use the Listener endpoint.

If you wish to deploy a new Amazon RDS for SQL Server instance then please follow the AWS guide at - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.CreatingConnecting.SQLServer.html

For high availability, deploy Multi-AZ RDS (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_SQLServerMultiAZ.html)

Security best practice is to not allow public access to your AWS RDS SQL Server.

The high availability configuration is discussed in section 4.4 in detail.

7.1 SQL Server Database creation and sizing

Table 4: SQL Server database capacity planning

Database	Est transaction storage	Size of database	Comments
sms-archive	1 million records	1.3GB Initial sizing depends on expected total number of transactions.	This includes index space.
sms-current	Cleared daily	200MB for small installations 600MB for large installations	This database contains transient data only. Information is moved to the archive early hours the following day.
SMS-SQL-API	Transient, cleared as transactions are processed	400MB initial size	This database contains transient data only. It is cleared by applications and the SMS software. Row level security (RLS) is required when there is more than 1 application accessing this database.

SQL Admins are responsible for creating 3 databases.

The Database names can be named in accordance with your standards.

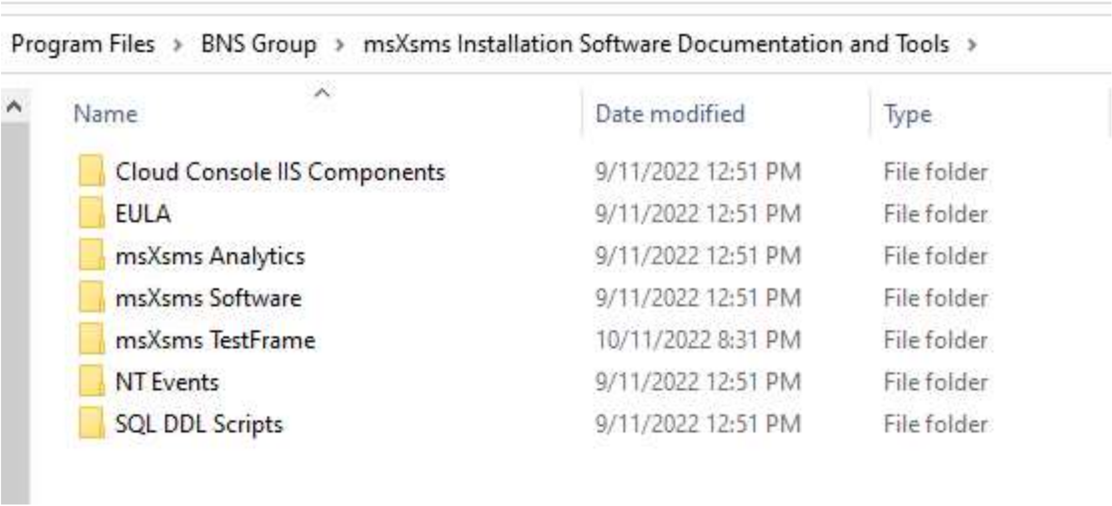
The default database names are:

- sms-current
- sms-archive
- sms-sql-api

■ Create all 3 databases manually in accordance with your standards.

3 DDL scripts are provided to create tables and indexes.

The scripts are located in the SQL DDL scripts folder where the software was initially installed on the SMS Windows Server.



Program Files › BNS Group › msXsms Installation Software Documentation and Tools ›

Name	Date modified	Type
Cloud Console IIS Components	9/11/2022 12:51 PM	File folder
EULA	9/11/2022 12:51 PM	File folder
msXsms Analytics	9/11/2022 12:51 PM	File folder
msXsms Software	9/11/2022 12:51 PM	File folder
msXsms TestFrame	10/11/2022 8:31 PM	File folder
NT Events	9/11/2022 12:51 PM	File folder
SQL DDL Scripts	9/11/2022 12:51 PM	File folder

SQL DBA's can modify and execute the scripts according to their standards and tools they use.

Execute the scripts to create tables in the databases in this order:

- sms-current-virgin-build.sql against the CURRENT DB.
  (note this also creates the SMS-SQL-API DB tables)
- sms-archive virgin-build.sql against the ARCHIVE DB.
- sms-archive-create-indexes.sql against the ARCHIVE DB.

SQL DDL command file	Description
sms-current-virgin-build.sql	Creates the tables in the SQL Database called sms-current. Used for intial creation of tables in the first deployment at your site. You may change the name of the Database to your standards. **Note this script also creates the SMS-SQL-API DB.**
sms-archive-virgin-build.sql	Creates the tables in the SQL Database called sms-archive. Used for intial creation of tables in the first deployment at your site. You may change the name of the Database to your standards.
sms-archive-create-indexes	Provides a series of recommended indexes to create for reporting and inquiry purposes. Modify this to suit your specific needs.

- SQL DBA will execute the SQL statements using SQL Management Studio or other tools against the respective Databases to create the tables.

7.2 Login Permissions sms server service account

- SQL DBA must provide full permissions to all databases to the sms service account.

Service Account functions	Permissions required	Comments
Full access to databases: sms-current sms-archive SMS-SQL-API	Full permissions DataReader and DataWriter	If Active Directory domain is used the service account will be a Windows Authenticated account otherwise the service account will use be a SQL Local user account added to the SQL database.

7.3 Row level security (RLS) for SMS-SQL-API database tables

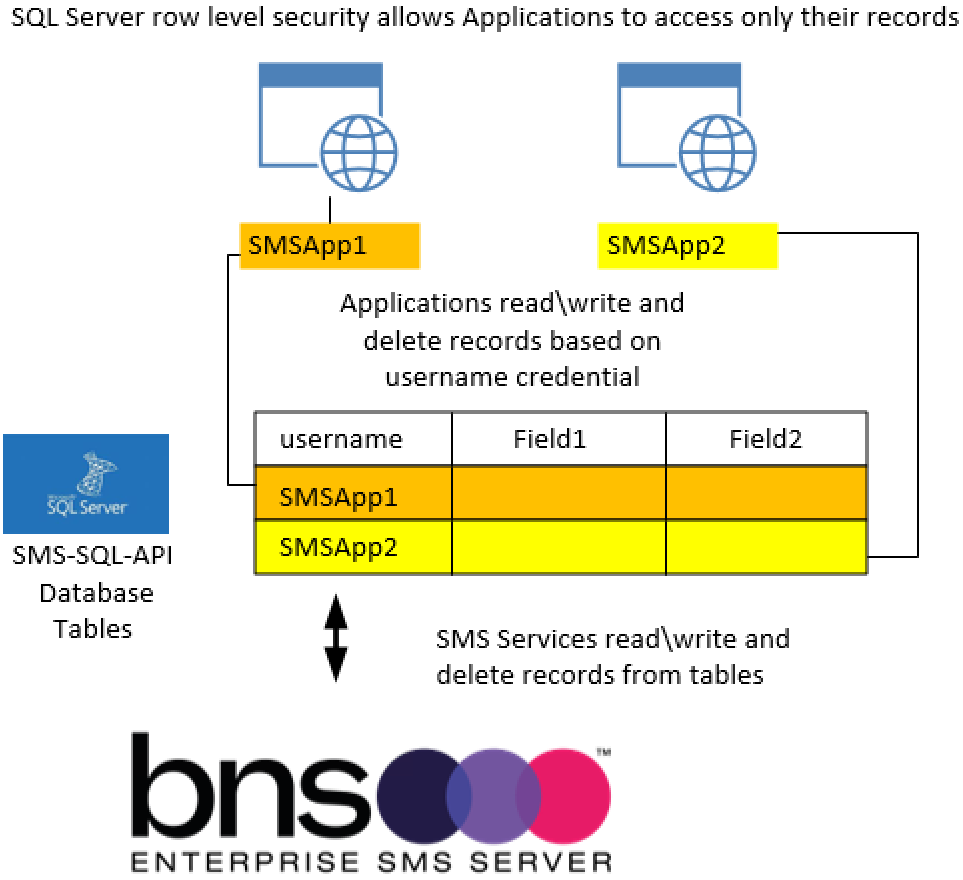
Row-Level Security (RLS) as the name suggests is a security mechanism that restricts the records from a SQL Server table based on the authorization context of the current user that is logged in.

Implementing RLS is mandatory if you have more than 1 application using the SMS-SQL-API database.

Articles on RLS can be found at:

https://www.sqlshack.com/introduction-to-row-level-security-in-sql-server/ and

https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16


SQL Server row level security allows Applications to access only their records
SMSApp1
SMSApp2
Applications read\write and delete records based on username credential
SQL Server
SMS-SQL-API Database Tables
SMS Services read\write and delete records from tables
bns ENTERPRISE SMS SERVER

username	Field1	Field2
SMSApp1		
SMSApp2		

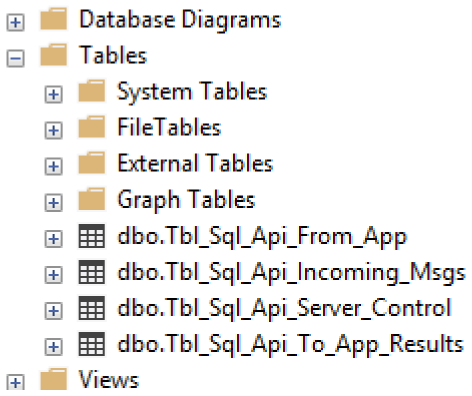
The DDLs provided in the software provides SQL admins the ability to assign RLS based on the application's SQL user login.

7.4 Implementing user login row level security using the scripts provided

Assumptions:

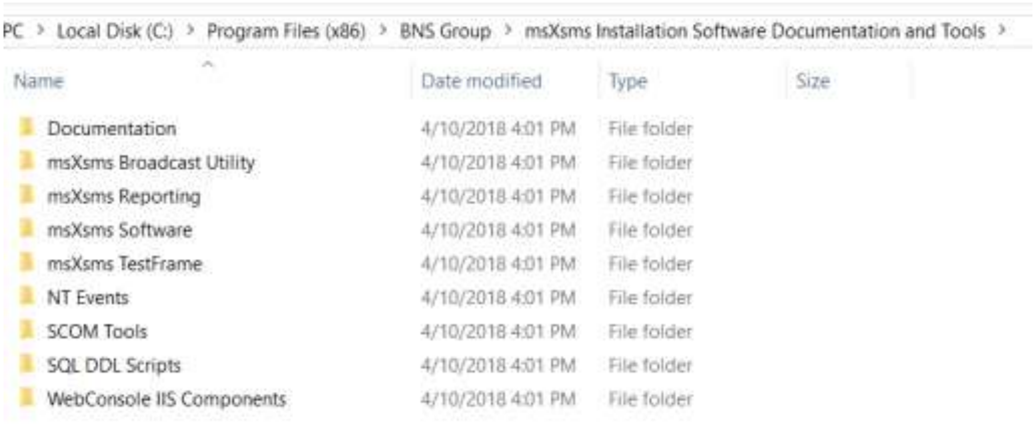
1. You have created a database called SMS-API-SQL database with 4 tables using the DDLs provided.
2. msXsms_sa service account has datareader and datawriter permissions to the SMS-SQL-API database

The tables in the SMS-SQL-API should be as follows:



```
+ Database Diagrams
- Tables
    + System Tables
    + FileTables
    + External Tables
    + Graph Tables
    + dbo.Tbl_Sql_Api_From_App
    + dbo.Tbl_Sql_Api_Incoming_Msgs
    + dbo.Tbl_Sql_Api_Server_Control
    + dbo.Tbl_Sql_Api_To_App_Results
+ Views
```

Locate the SQL Query files in the SQL DDL scripts folder.



PC › Local Disk (C:) › Program Files (x86) › BNS Group › msXsms Installation Software Documentation and Tools ›

Name	Date modified	Type	Size
Documentation	4/10/2018 4:01 PM	File folder	
msXsms Broadcast Utility	4/10/2018 4:01 PM	File folder	
msXsms Reporting	4/10/2018 4:01 PM	File folder	
msXsms Software	4/10/2018 4:01 PM	File folder	
msXsms TestFrame	4/10/2018 4:01 PM	File folder	
NT Events	4/10/2018 4:01 PM	File folder	
SCOM Tools	4/10/2018 4:01 PM	File folder	
SQL DDL Scripts	4/10/2018 4:01 PM	File folder	
WebConsole IIS Components	4/10/2018 4:01 PM	File folder	

Locate the RLS Scripts.

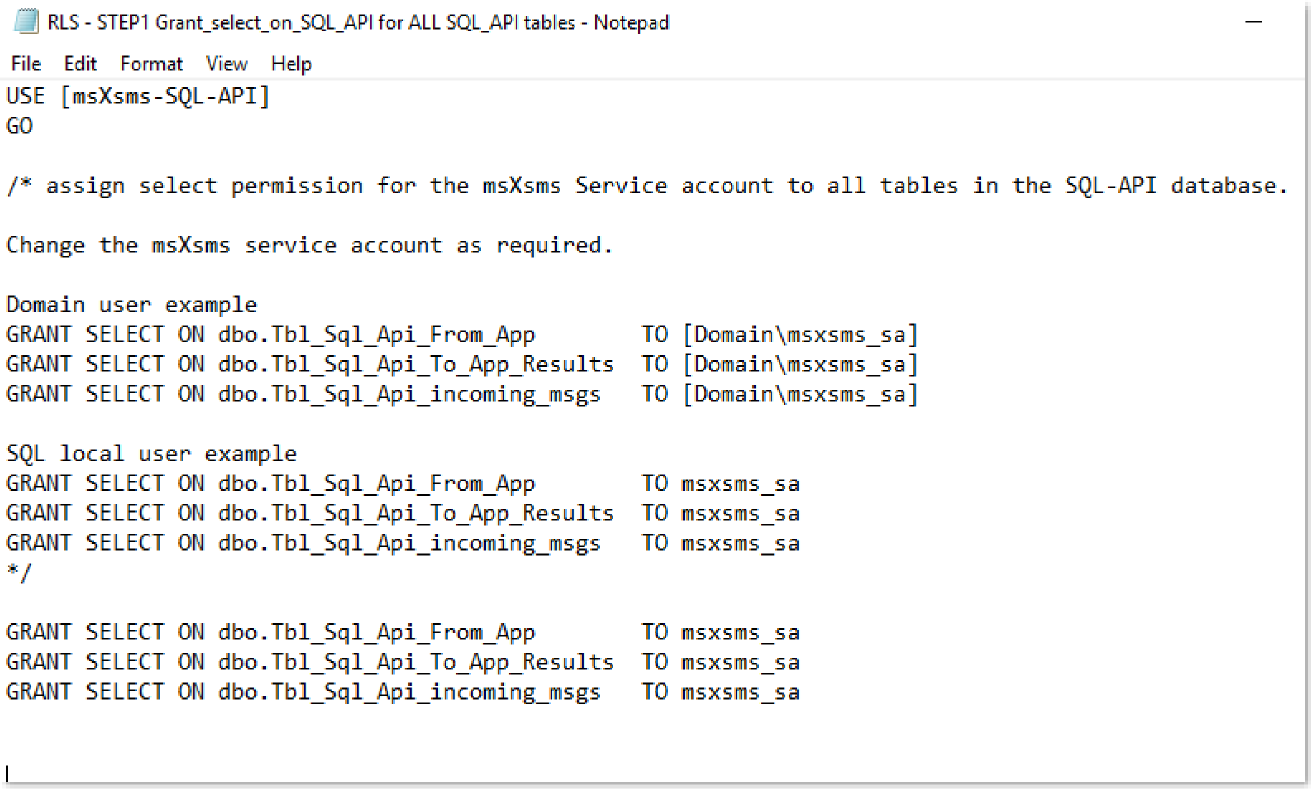
Follow these steps to implement RLS on the SMS-SQL-API database tables.

7.4.1 Step 1 – GRANT Select for all user logins

The SQL query file is called "RLS – STEP1 Grant_slelect_on_SQL_API for ALL SQL_API tables".

- Edit this SQL query to include the service account login (Windows Authenticated domain login or a SQL local user).
- Run the SQL Query on the database tables

  The SQL query will look similar to this example



RLS - STEP1 Grant_select_on_SQL_API for ALL SQL_API tables - Notepad
File Edit Format View Help

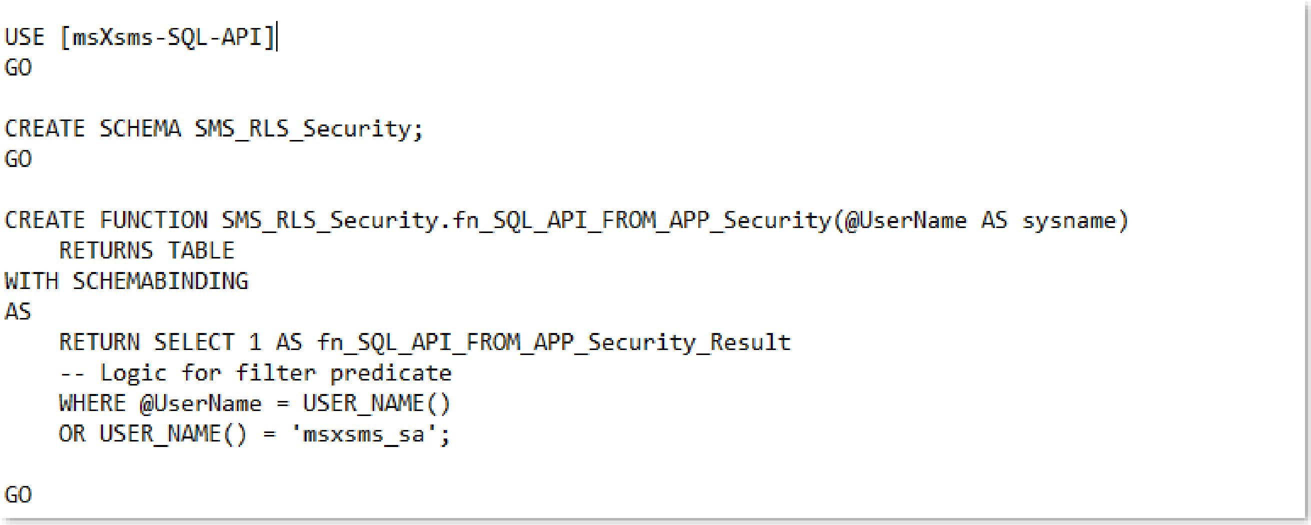
```
USE [msXsms-SQL-API]
GO

/* assign select permission for the msXsms Service account to all tables in the SQL-API database.

Change the msXsms service account as required.

Domain user example
GRANT SELECT ON dbo.Tbl_Sql_Api_From_App        TO [Domain\msxsms_sa]
GRANT SELECT ON dbo.Tbl_Sql_Api_To_App_Results  TO [Domain\msxsms_sa]
GRANT SELECT ON dbo.Tbl_Sql_Api_incoming_msgs   TO [Domain\msxsms_sa]

SQL local user example
GRANT SELECT ON dbo.Tbl_Sql_Api_From_App        TO msxsms_sa
GRANT SELECT ON dbo.Tbl_Sql_Api_To_App_Results  TO msxsms_sa
GRANT SELECT ON dbo.Tbl_Sql_Api_incoming_msgs   TO msxsms_sa
*/

GRANT SELECT ON dbo.Tbl_Sql_Api_From_App        TO msxsms_sa
GRANT SELECT ON dbo.Tbl_Sql_Api_To_App_Results  TO msxsms_sa
GRANT SELECT ON dbo.Tbl_Sql_Api_incoming_msgs   TO msxsms_sa
```

7.4.2 Step 2 – Create Inline Table-valued Function for all tables

The SQL query file is called “RLS – STEP2 Create_inline_tablevalued_Functions for ALL tables”.

Microsoft recommend using a Security schema specifically for RLS objects hence we have a schema called SMS_RLS_Security

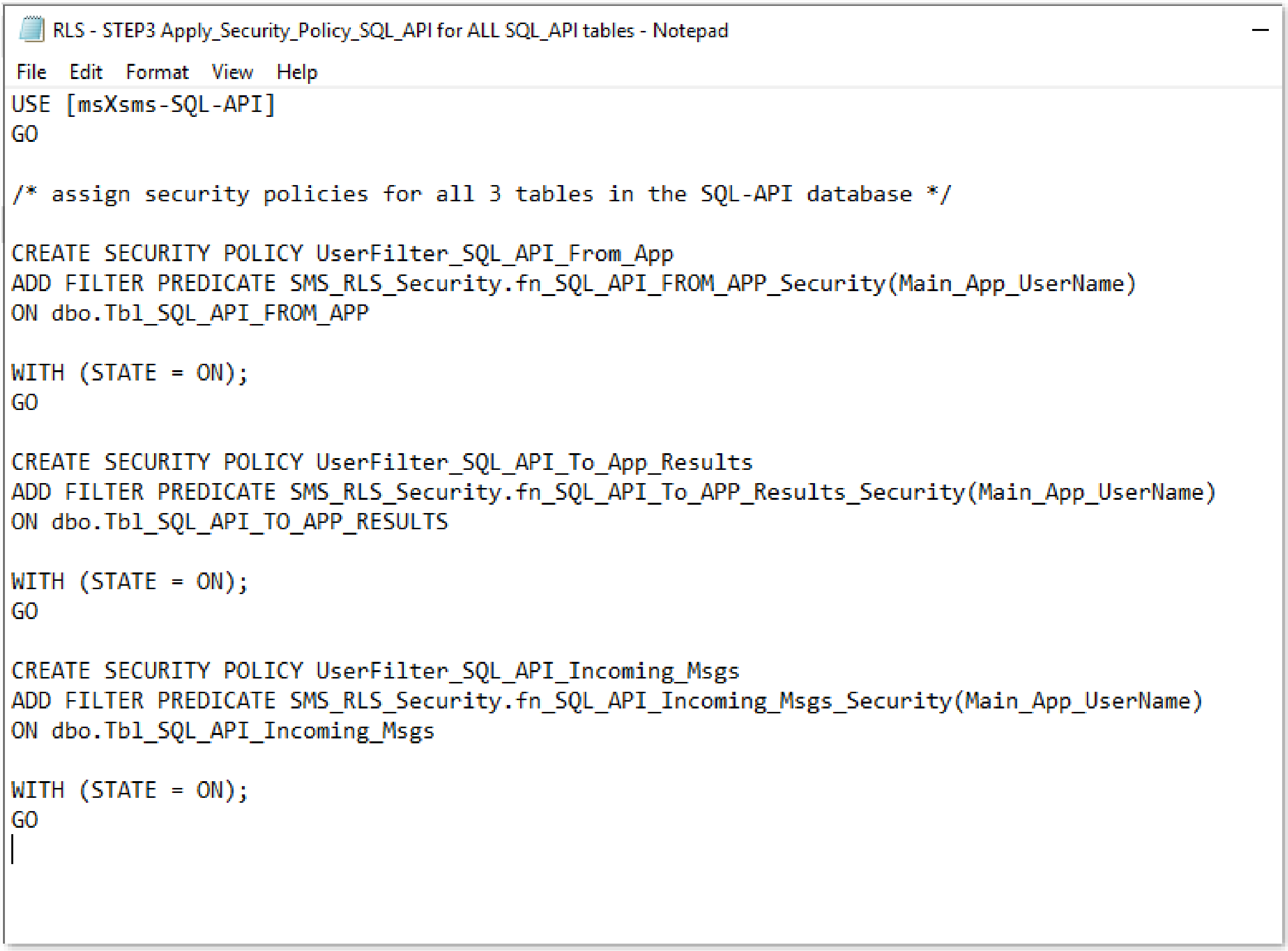
Refer to https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security?view=sql-server-ver16



```
USE [msXsms-SQL-API]
GO

CREATE SCHEMA SMS_RLS_Security;
GO

CREATE FUNCTION SMS_RLS_Security.fn_SQL_API_FROM_APP_Security(@UserName AS sysname)
    RETURNS TABLE
WITH SCHEMABINDING
AS
    RETURN SELECT 1 AS fn_SQL_API_FROM_APP_Security_Result
    -- Logic for filter predicate
    WHERE @UserName = USER_NAME()
    OR USER_NAME() = 'msxsms_sa';

GO
```

7.4.3 Step 3 – Apply RLS Security policy for all tables

The SQL query file is called “RLS – STEP3 Apply_Security_Policy_SQL_API for ALL SQL_API tables”.


RLS - STEP3 Apply_Security_Policy_SQL_API for ALL SQL_API tables - Notepad
File Edit Format View Help

```
USE [msXsms-SQL-API]
GO

/* assign security policies for all 3 tables in the SQL-API database */

CREATE SECURITY POLICY UserFilter_SQL_API_From_App
ADD FILTER PREDICATE SMS_RLS_Security.fn_SQL_API_FROM_APP_Security(Main_App_UserName)
ON dbo.Tbl_SQL_API_FROM_APP

WITH (STATE = ON);
GO

CREATE SECURITY POLICY UserFilter_SQL_API_To_App_Results
ADD FILTER PREDICATE SMS_RLS_Security.fn_SQL_API_To_APP_Results_Security(Main_App_UserName)
ON dbo.Tbl_SQL_API_TO_APP_RESULTS

WITH (STATE = ON);
GO

CREATE SECURITY POLICY UserFilter_SQL_API_Incoming_Msgs
ADD FILTER PREDICATE SMS_RLS_Security.fn_SQL_API_Incoming_Msgs_Security(Main_App_UserName)
ON dbo.Tbl_SQL_API_Incoming_Msgs

WITH (STATE = ON);
GO
```

7.4.4 Confirming that RLS has been setup correctly

Using SQL-API DB Table Tbl_SQL_API_FROM_APP

Right click "Select TOP 1000 records"

Edit the SQL query as follows:

Insert at the top of the query

EXECUTE AS USER = 'msxsms_sa' (or Domain\msxsms_sa if you are using a domain Windows authenticated login)

At the end of the query insert

REVERT;

You should see 1 record.

If you do the same query without setting the EXECUTE AS USER you should not see any data.

7.5 Onboarding applications to use the SQL-API database

Advise developers to read the BNS knowledge base https://smskb.bnsgroup.com.au/sqlinterface

After you have setup credentials for the developer's application advise the developers of those credentials.

Developers will provide their user login username eg: Domain\SMSApp1 in a field called Main_App_Username when they write requests to the SQL-API Table Tbl_SQL_API_FROM_APP.

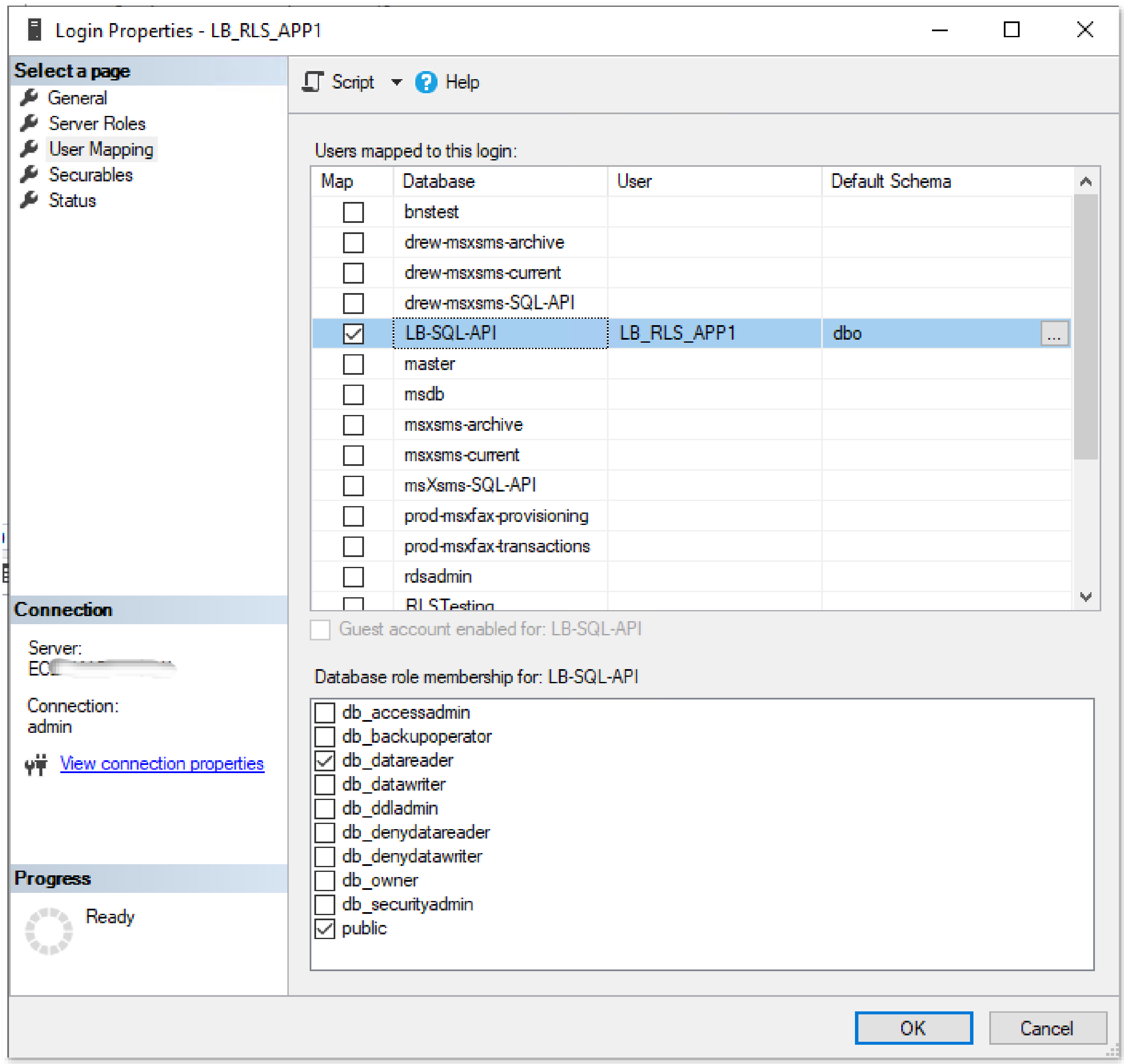
RLS has been applied using the username credential as the mechanism to control access to application's data. This control is a security control introduced by Microsoft in SQL Server 2016 and is supported in AWS RDS.

msXsms services provide the application's login username for transactions it writes back to the application in Tbl_SQL_API_TO_APP and the Tbl_SQL_API_INCOMING_MSGS tables.

Applications are responsible to process their results and any incoming SMS messages, deleting those records after they have processed them.

7.5.1 SQL Administrator actions to onboard new applications

- From SQL Server management studio navigate to SECURITY\LOGINS
- Create a new user login for the application you are on-boarding eg: Domain\SMSApp1 or a SQL Local user depending on your security requirements.
- Right click the user login, select properties
- Select User Mapping
- Select the database SMS-SQL-API
- Assign Datareader to the SMS-SQL-API DB.



Server:
EC[redacted]

Connection:
admin

Ready

Users mapped to this login:

Map	Database	User	Default Schema
□	bnstest		
□	drew-msxsms-archive		
□	drew-msxsms-current		
□	drew-msxsms-SQL-API		
☑	LB-SQL-API	LB_RLS_APP1	dbo
□	master		
□	msdb		
□	msxsms-archive		
□	msxsms-current		
□	msXsms-SQL-API		
□	prod-msxfax-provisioning		
□	prod-msxfax-transactions		
□	rdsadmin		
□	RLSTesting		

□ Guest account enabled for: LB-SQL-API

Database role membership for: LB-SQL-API

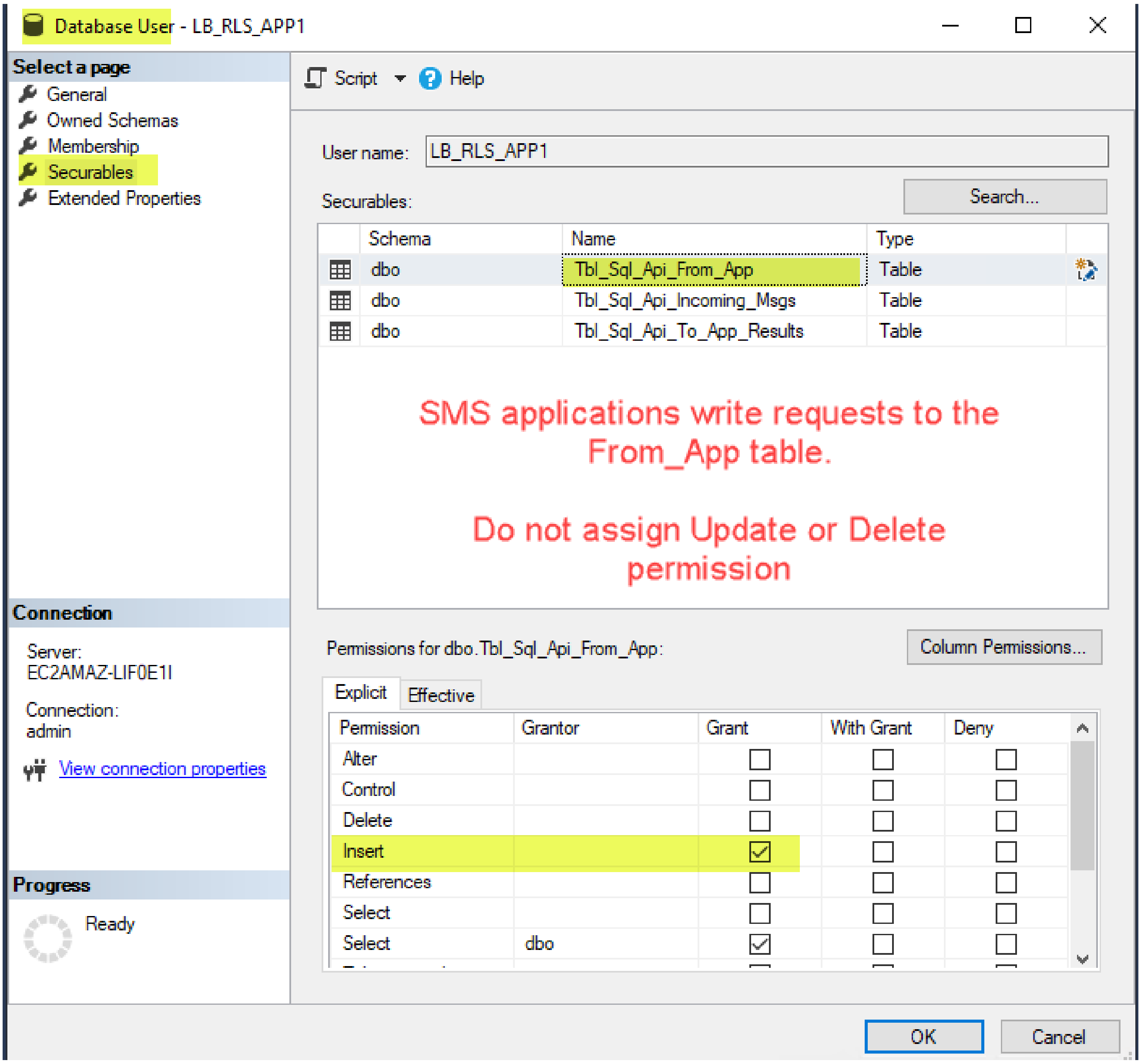
- □ db_accessadmin
- □ db_backupoperator
- ☑ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- □ db_owner
- □ db_securityadmin
- ☑ public

- Open a new query window

The following SQL query is also included in the SQL DDLs folder.

```
USE [SMS-SQL-API]
GO
GRANT SELECT ON dbo.Tbl_Sql_Api_From_App            TO [Domain\xxx]
GRANT SELECT ON dbo.Tbl_Sql_Api_To_App_Results      TO [Domain\ xxx]
GRANT SELECT ON dbo.Tbl_Sql_Api_incoming_msgs       TO [Domain\ xxx]
```

- Execute the query
- **Navigate to Security under the Database itself**.
- Right click the user login
- Select Securables



Server:
EC2AMAZ-LIF0E1I

Connection:
admin

User name: LB_RLS_APP1

Securables:

	Schema	Name	Type
▦	dbo	Tbl_Sql_Api_From_App	Table
▦	dbo	Tbl_Sql_Api_Incoming_Msgs	Table
▦	dbo	Tbl_Sql_Api_To_App_Results	Table

SMS applications write requests to the From_App table.

Do not assign Update or Delete permission

Permissions for dbo.Tbl_Sql_Api_From_App:

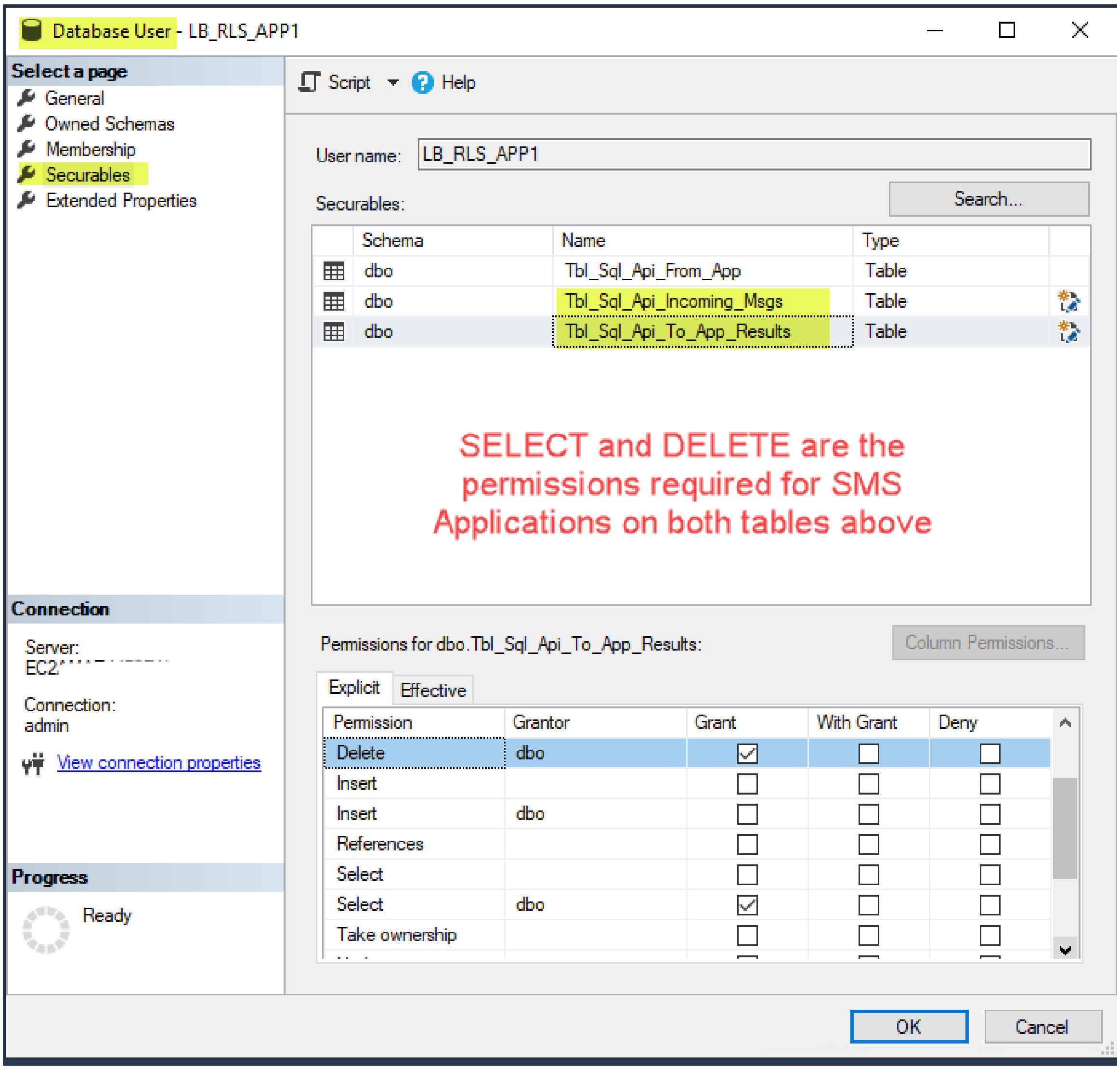
Permission	Grantor	Grant	With Grant	Deny
Alter		☐	☐	☐
Control		☐	☐	☐
Delete		☐	☐	☐
Insert		☑	☐	☐
References		☐	☐	☐
Select		☐	☐	☐
Select	dbo	☑	☐	☐

- Assign the Insert permission to the Table Tbl_Sql_Api_From_App.

SMS Applications write their SMS transmission requests into the above table.

msXsms Services then process those requests and provide results back in another table called Tbl_Sql_Api_To_App_Results.

msXsms Services are responsible for deleting processed records in the Tbl_Sql_Api_From_App table.



Database User - LB_RLS_APP1

Connection

Server:
EC2

Connection:
admin

View connection properties

Progress

Ready

User name: LB_RLS_APP1

Securables:

Schema	Name	Type
dbo	Tbl_Sql_Api_From_App	Table
dbo	Tbl_Sql_Api_Incoming_Msgs	Table
dbo	Tbl_Sql_Api_To_App_Results	Table

SELECT and DELETE are the permissions required for SMS Applications on both tables above

Permissions for dbo.Tbl_Sql_Api_To_App_Results:

Permission	Grantor	Grant	With Grant	Deny
Delete	dbo	☑	☐	☐
Insert		☐	☐	☐
Insert	dbo	☐	☐	☐
References		☐	☐	☐
Select		☐	☐	☐
Select	dbo	☑	☐	☐
Take ownership		☐	☐	☐

SMS Applications read the results for their SMS transmission requests and can process any incoming SMS messages.

SMS Applications are responsible for deleting their records from both tables Tbl_Sql_Api_To_App_Results and Tbl_Sql_Api_Incoming_Msgs.

- Assign Delete permissions for the SMS Application user login to both tables Tbl_Sql_Api_To_App_Results and Tbl_Sql_Api_Incoming_Msgs.

SECTION 8 Install SMS Console

8.1 General

SMS Console is an IIS browser based console which can be installed on the Windows Server where the SMS software is installed. The SMS console should be installed on all servers.

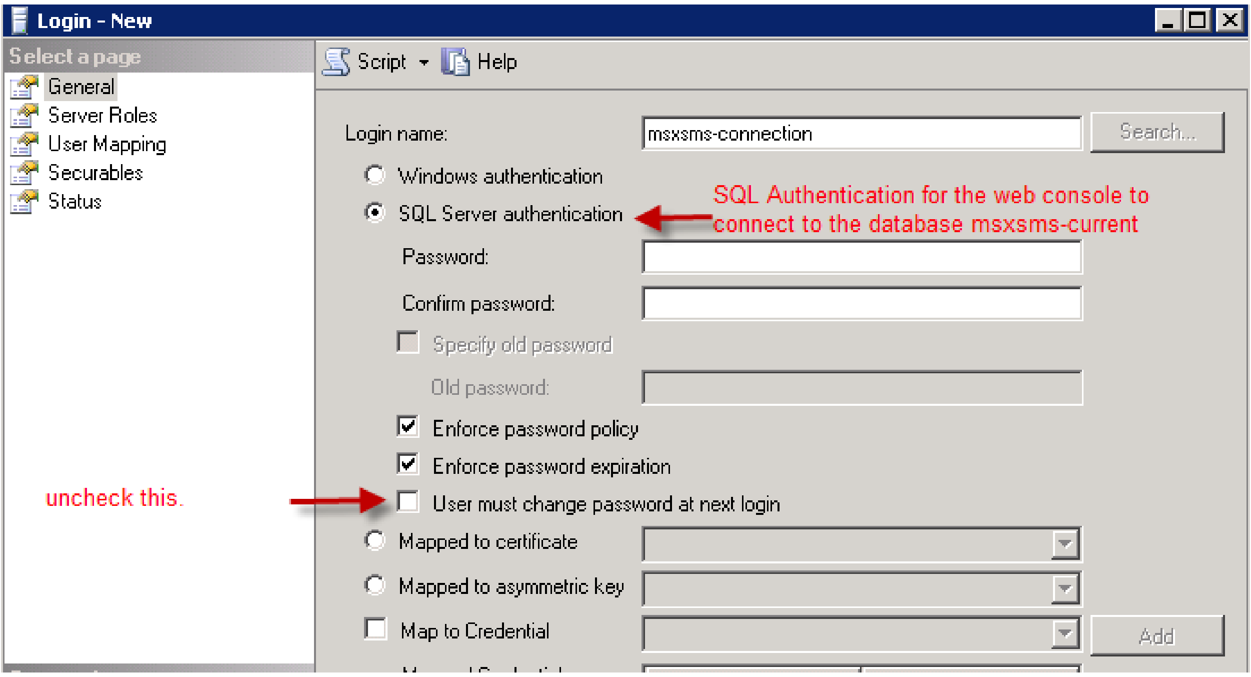
It is compatible with most browsers including: Microsoft Edge.

Console Software Requirements

Software	Version/service packs	Mandatory or optional	Vendor/Manufacturer
.net Framework	Version which comes with the OS	Mandatory	Microsoft Corporation
Internet Information Server	IIS which comes with the OS	Mandatory	Microsoft Corporation

8.1.1 SQL Database Administrator (DBA)

- Your SQL DBA will need create a SQL User account for the Console to connect to the database.
- **sms-console** is the SQL user name used throughout this documentation.



Login - New

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ Help

Login name: msxsms-connection [Search...]

○ Windows authentication

● SQL Server authentication

Password:

Confirm password:

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

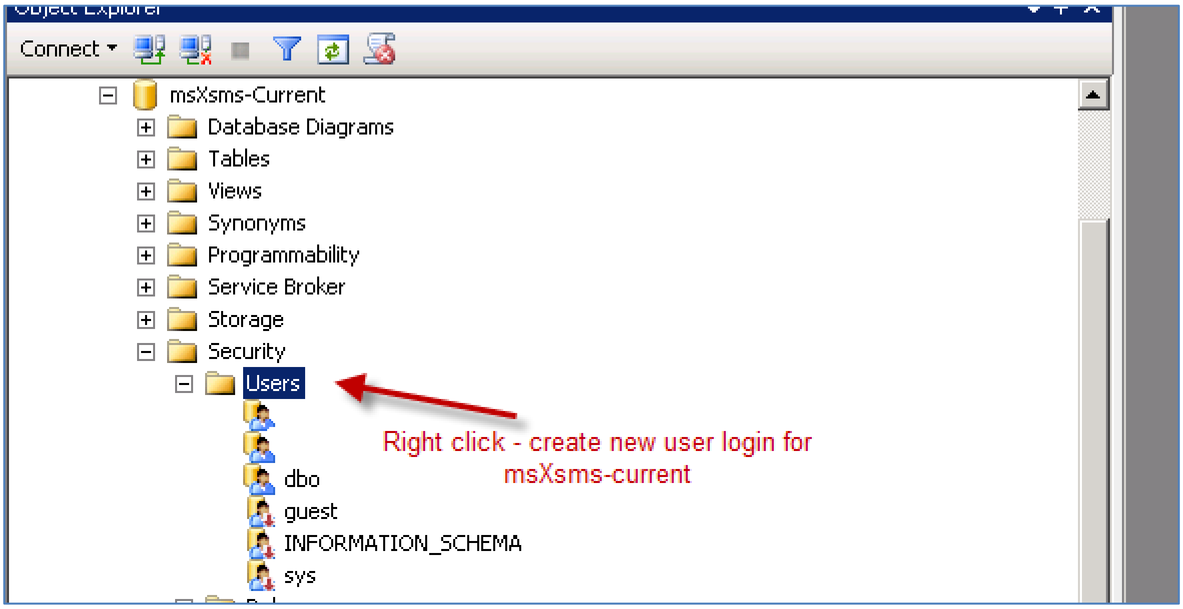
○ Mapped to asymmetric key

□ Map to Credential [Add]

SQL Authentication for the web console to connect to the database msxsms-current

uncheck this.

- Under the sms-current database, create a new user login permission to the database.

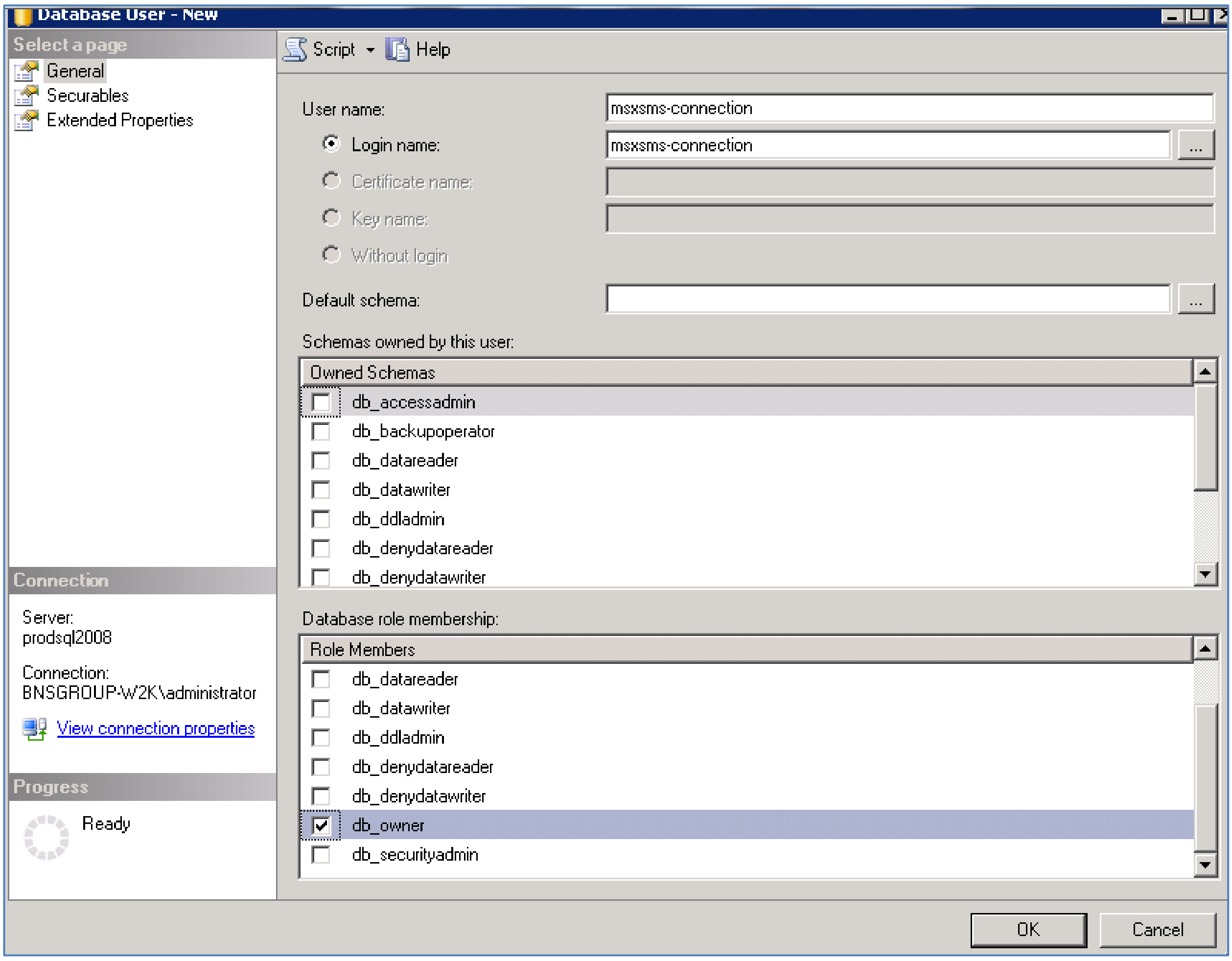


Object Explorer

Connect ▾

- msXsms-Current
  - Database Diagrams
  - Tables
  - Views
  - Synonyms
  - Programmability
  - Service Broker
  - Storage
  - Security
    - Users
      - dbo
      - guest
      - INFORMATION_SCHEMA
      - sys

Right click - create new user login for msXsms-current



User name: msxsms-connection

● Login name: msxsms-connection

○ Certificate name:

○ Key name:

○ Without login

Default schema:

Schemas owned by this user:

Owned Schemas
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter

Database role membership:

Role Members
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin

Connection

Server:
prodsql2008

Connection:
BNSGROUP-W2K\administrator

View connection properties

Progress

Ready

- sms-console will require full permissions to all 3 databases: Datareader\datawriter roles.

8.1.2 SQL API Database permissions for SQL user SMS-Console

- Assign datareader and datawriter for this user to the SMS-SQL-API database.

8.1.3 Active Directory Security Groups

> Customers who deploy msXsms in a workgroup can follow the same principles using local server groups and users.

In this section you will create an AD Security Group for your Configuration/Admin Team to use. We have used the AD Security Group name 'SMS-Admin-Group'.

The SMS console will be expanded to perform other functions such as Operational functions as distinct from Configuration.

Setup another security group such as 'SMS-Operations-Group'. For now it will have no members it is for future use.

- Create an Active Directory Security Group for the infrastructure administrators eg: 'sms-admin-group'.

NOTE: Add your AD domain user account to that group and also the domain account you are currently using to perform the installation of this software.

- Create an Active Directory Security Group for the operations team eg: 'sms-operations-group'. No users required for this group as this is reserved for future use.

8.2 Installation of IIS for the Console

8.2.1 Install Internet Information Server

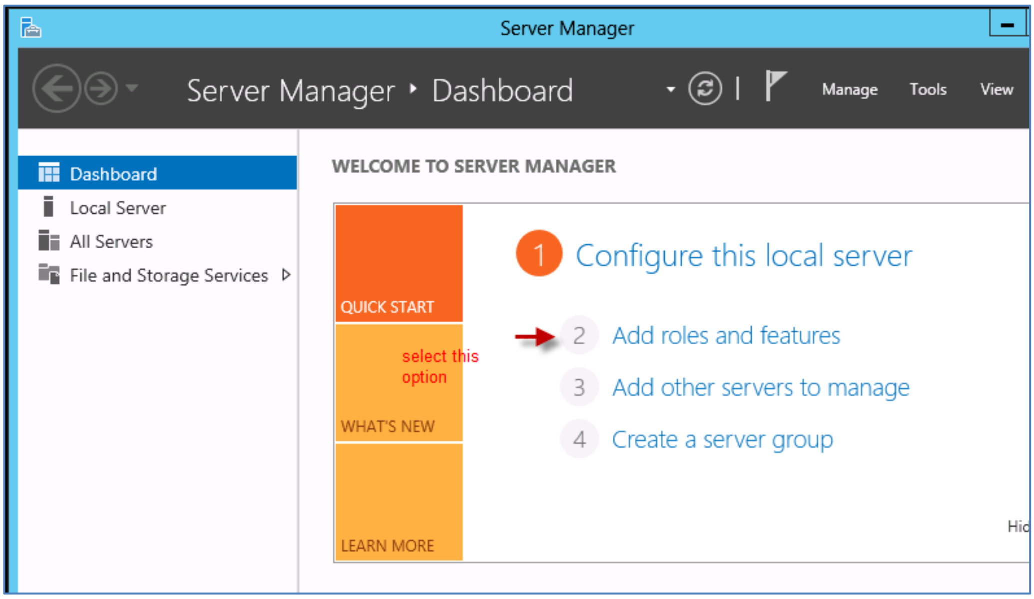
Microsoft's Internet Information Server is required to support SMS console.

This documentation describes the steps required to install IIS.

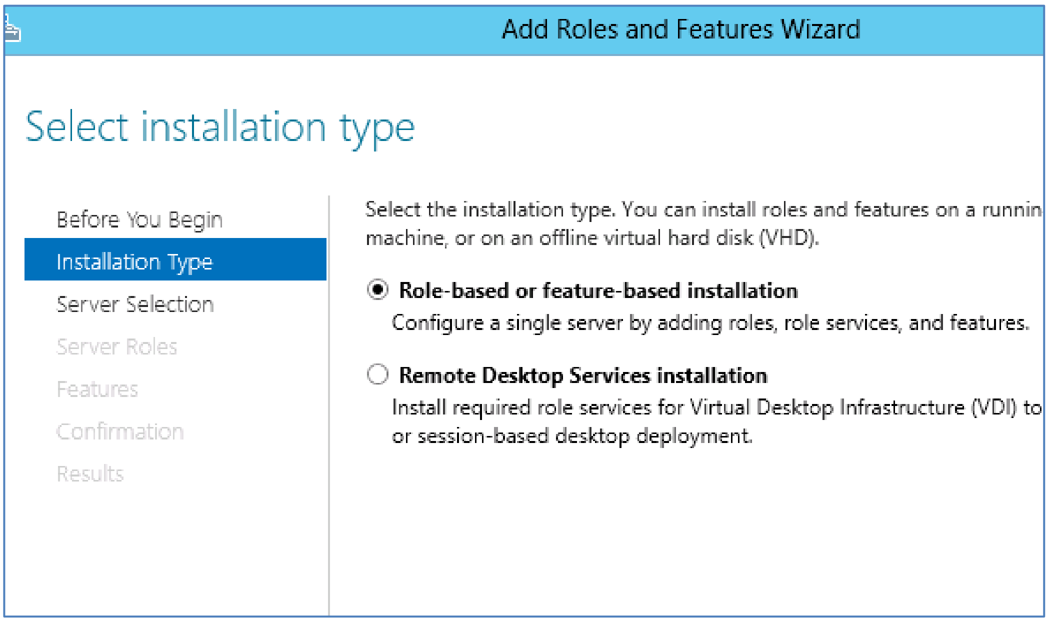
Windows Server 2022 installs ASP.NET version 4.8 which is supported.

8.2.2 Installing IIS on the SMS Server

- Installing IIS



select this option

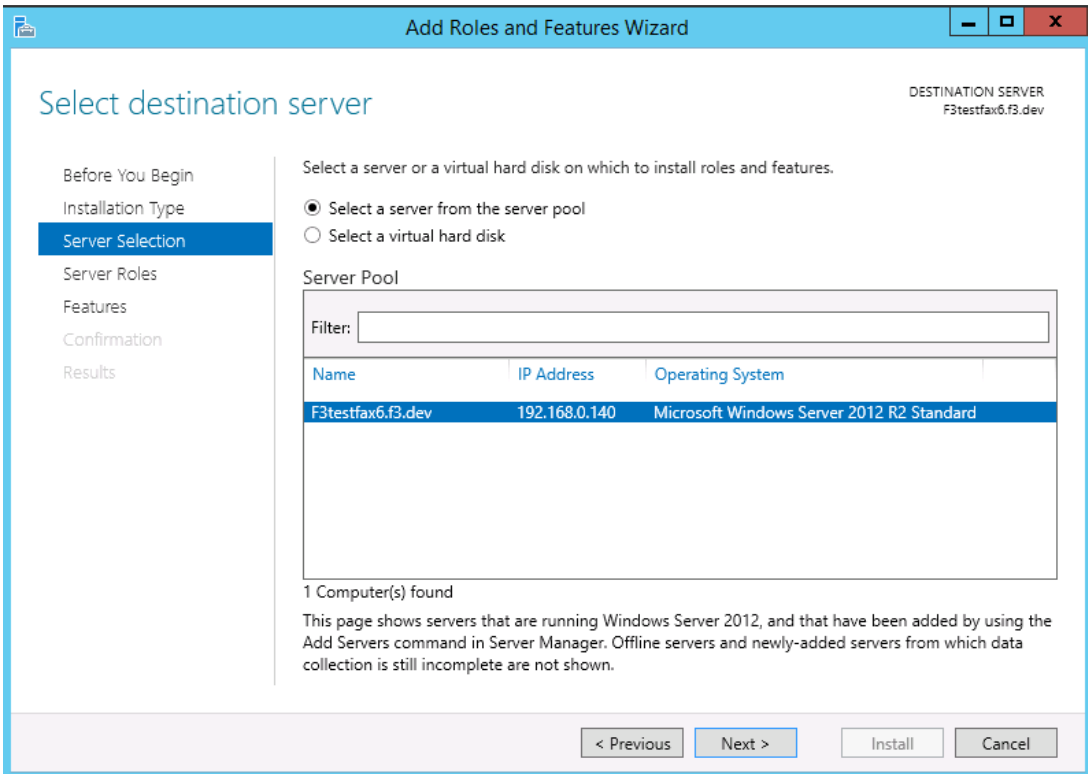


Select installation type

Select the installation type. You can install roles and features on a runnin machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to or session-based desktop deployment.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
F3testfax6.f3.dev

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

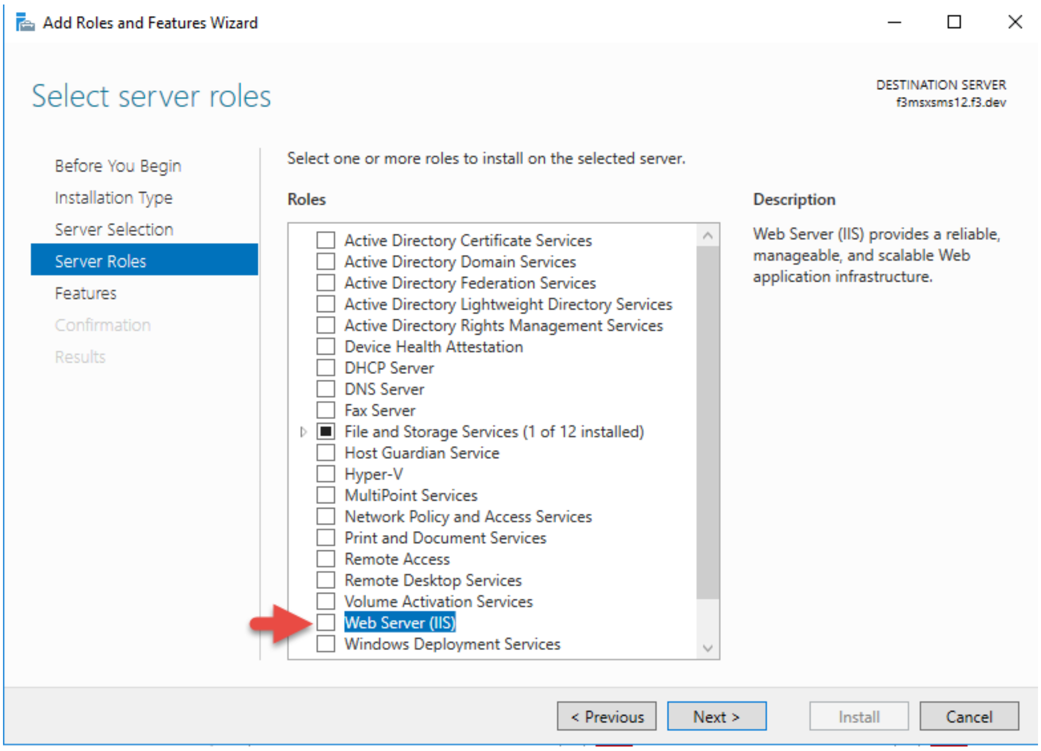
Server Pool

Filter:

Name	IP Address	Operating System
F3testfax6.f3.dev	192.168.0.140	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
f3msxsms12.f3.dev

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

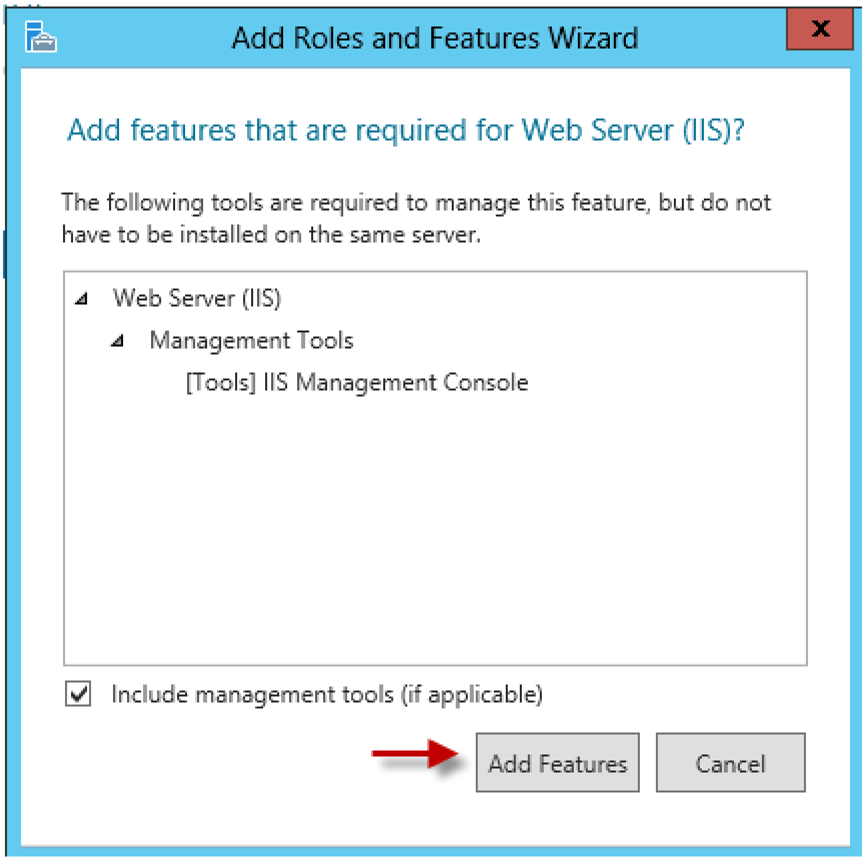
Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.



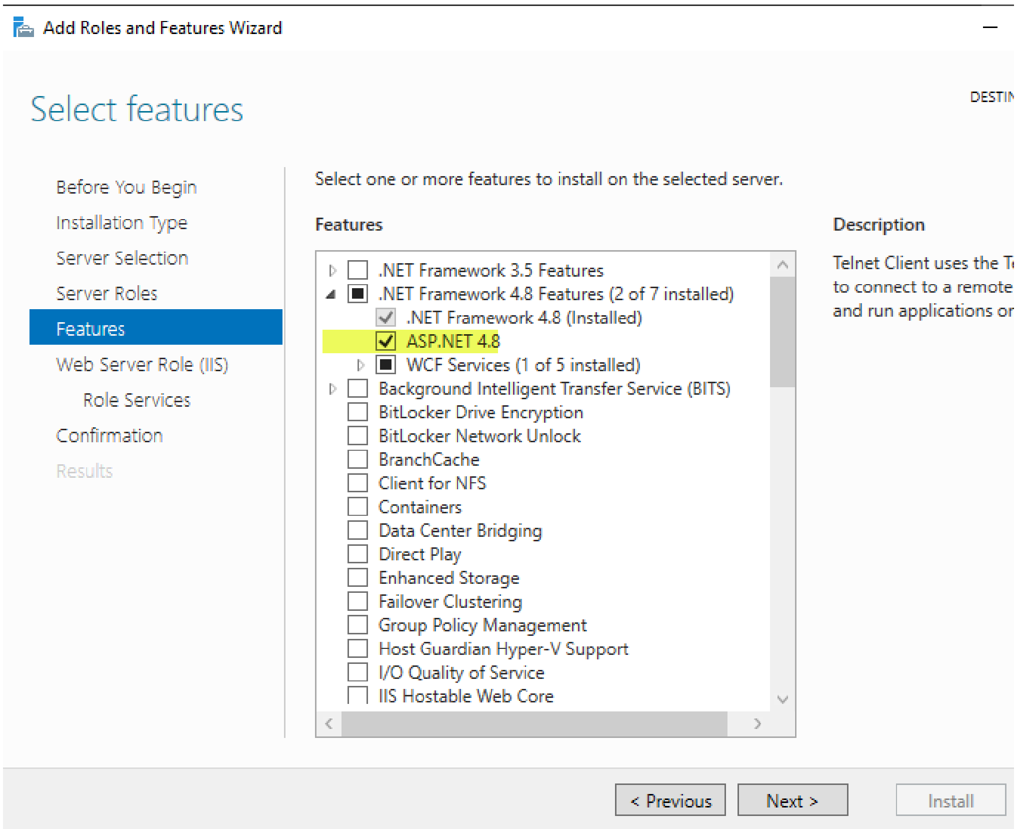
Add Roles and Features Wizard

Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)



Select features

Select one or more features to install on the selected server.

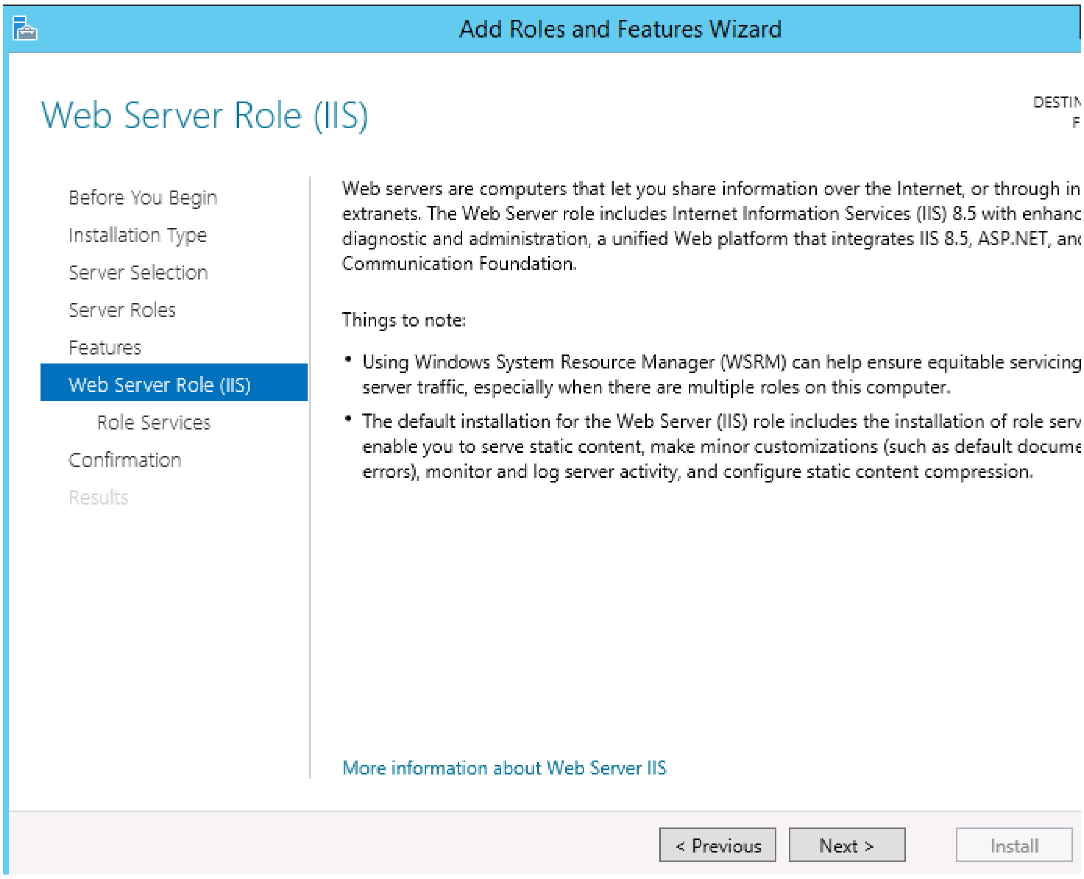
Features

- ☐ .NET Framework 3.5 Features
- ■ .NET Framework 4.8 Features (2 of 7 installed)
  - ☑ .NET Framework 4.8 (Installed)
  - ☑ ASP.NET 4.8
  - ■ WCF Services (1 of 5 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☐ Group Policy Management
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core

Description

Telnet Client uses the T to connect to a remote and run applications or

- Select ASP.NET 4.8 (Windows Server 2022) then press next. This option could be lower depending on the version of Windows server being used.



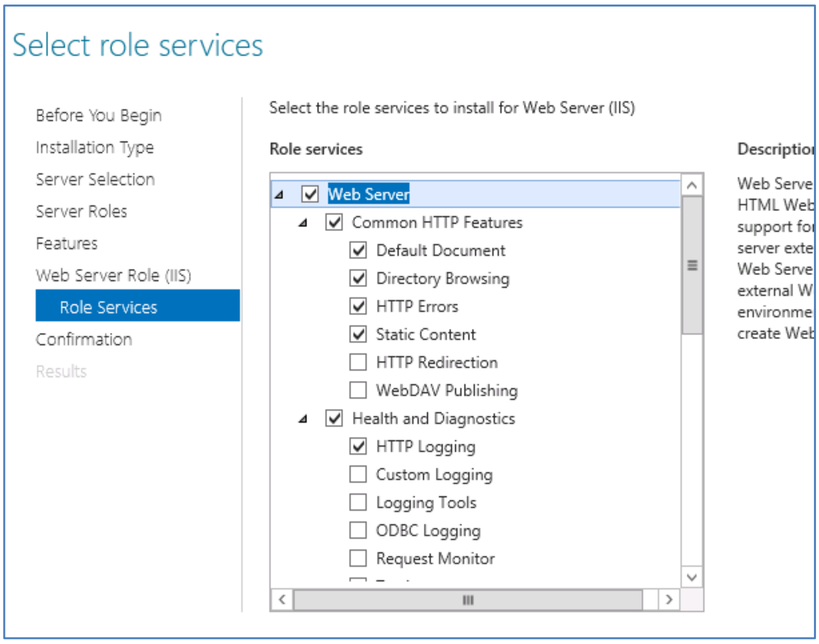
Web Server Role (IIS)

Web servers are computers that let you share information over the Internet, or through in extranets. The Web Server role includes Internet Information Services (IIS) 8.5 with enhanc diagnostic and administration, a unified Web platform that integrates IIS 8.5, ASP.NET, an Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role serv enable you to serve static content, make minor customizations (such as default docume errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS



Select role services

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Web Server Role (IIS)
- Role Services
- Confirmation
- Results

Select the role services to install for Web Server (IIS)

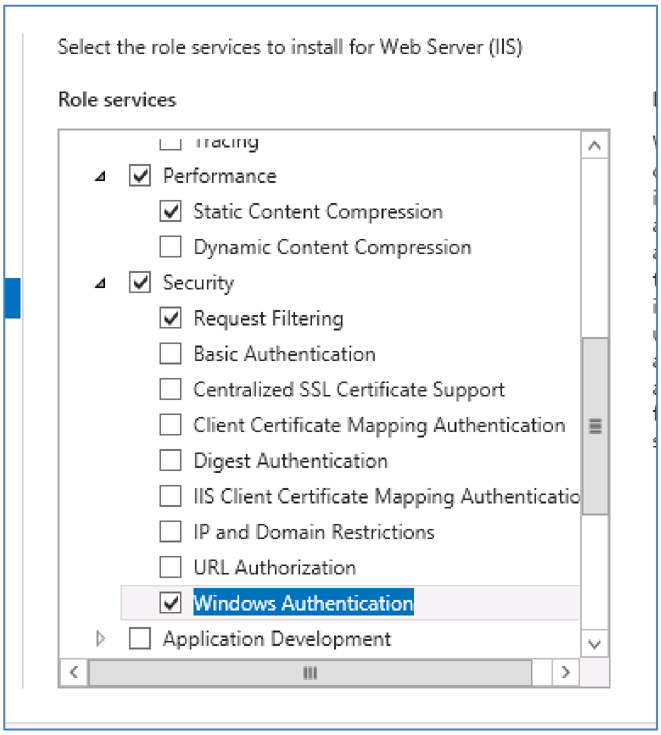
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☐ HTTP Redirection
    - ☐ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - ☐ Custom Logging
    - ☐ Logging Tools
    - ☐ ODBC Logging
    - ☐ Request Monitor

Descriptio

Web Serve
HTML Web
support fo
server exte
Web Serve
external W
environme
create Web

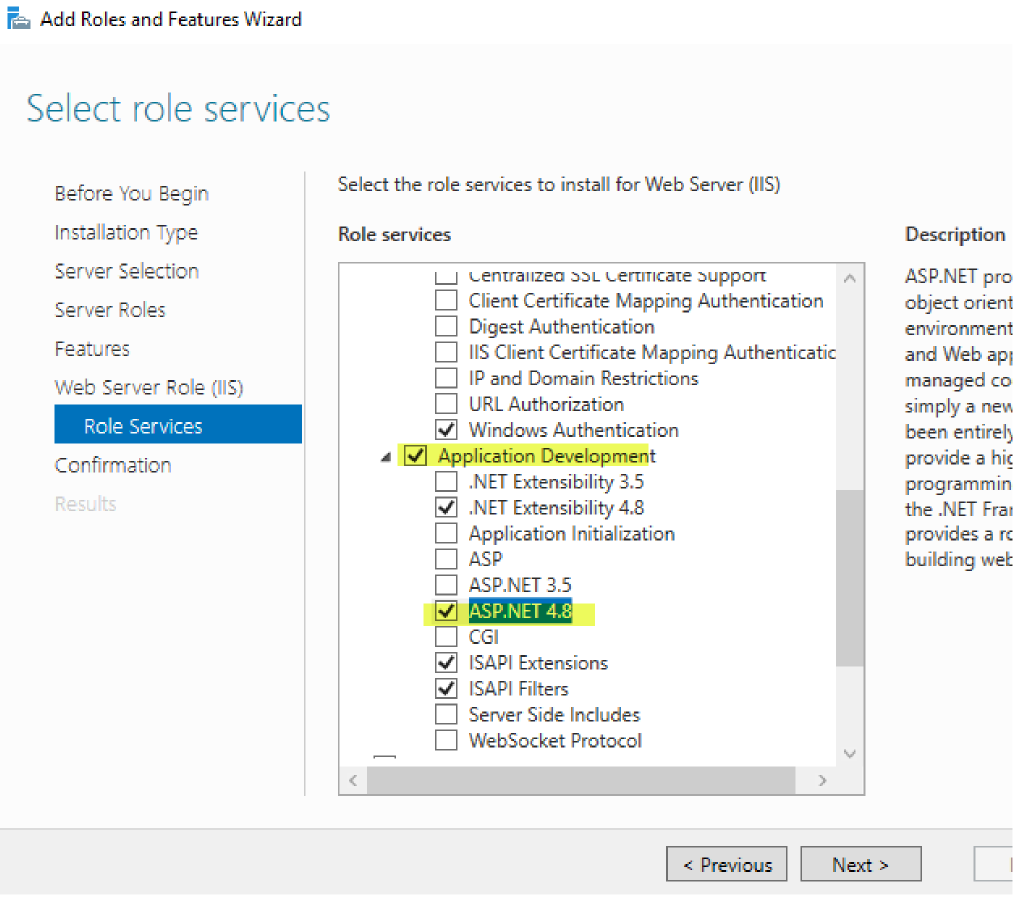
- Scroll down the list of options



Select the role services to install for Web Server (IIS)

Role services

- ☐ Tracing
- ☑ Performance
  - ☑ Static Content Compression
  - ☐ Dynamic Content Compression
- ☑ Security
  - ☑ Request Filtering
  - ☐ Basic Authentication
  - ☐ Centralized SSL Certificate Support
  - ☐ Client Certificate Mapping Authentication
  - ☐ Digest Authentication
  - ☐ IIS Client Certificate Mapping Authenticatio
  - ☐ IP and Domain Restrictions
  - ☐ URL Authorization
  - ☑ Windows Authentication
- ☐ Application Development



Add Roles and Features Wizard

Select role services

Select the role services to install for Web Server (IIS)

Role services

- □ Centralized SSL Certificate Support
- □ Client Certificate Mapping Authentication
- □ Digest Authentication
- □ IIS Client Certificate Mapping Authenticatic
- □ IP and Domain Restrictions
- □ URL Authorization
- ☑ Windows Authentication
- ☑ Application Development
  - □ .NET Extensibility 3.5
  - ☑ .NET Extensibility 4.8
  - □ Application Initialization
  - □ ASP
  - □ ASP.NET 3.5
  - ☑ ASP.NET 4.8
  - □ CGI
  - ☑ ISAPI Extensions
  - ☑ ISAPI Filters
  - □ Server Side Includes
  - □ WebSocket Protocol

Description

ASP.NET pro object orient environment and Web app managed co simply a new been entirely provide a hig programmin the .NET Fran provides a ro building web

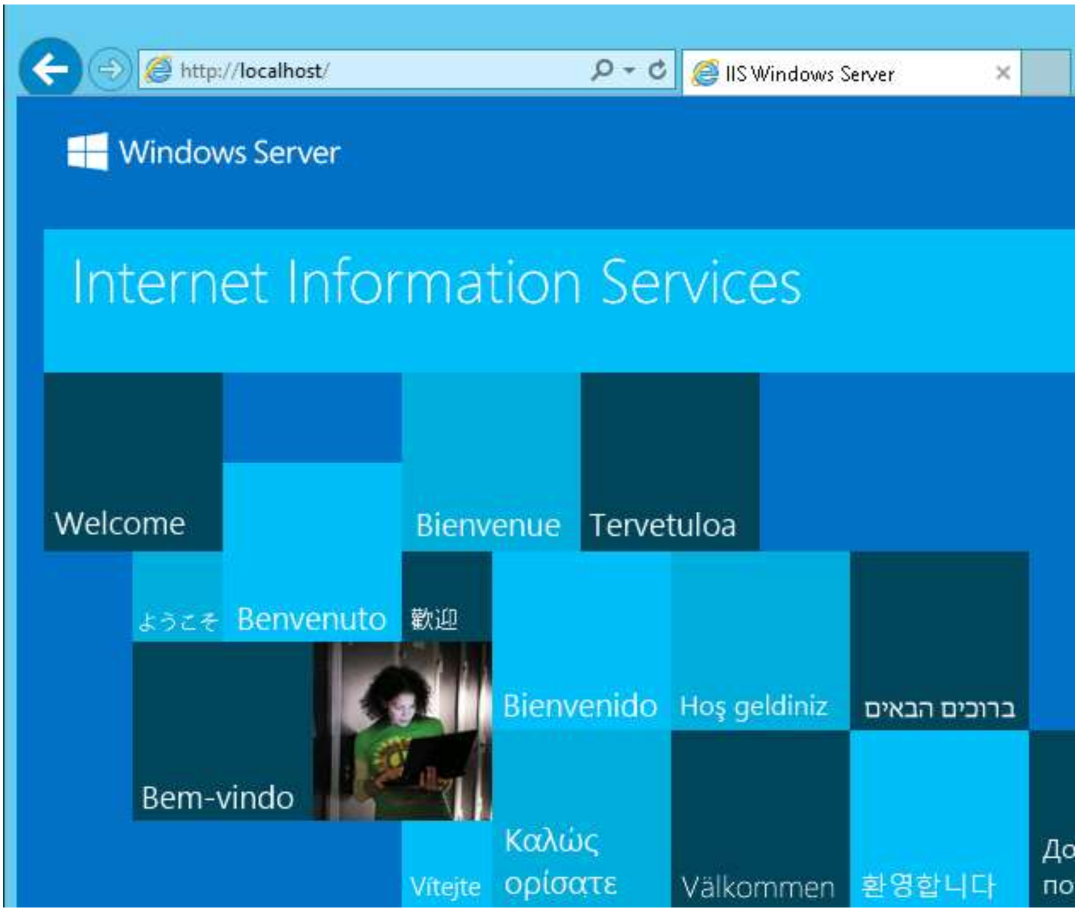
- Select NEXT when you have checked all of the above options

- Select Install

To check that IIS installed correctly open a web browser from your SMS server and proceed to the following address:

- http://localhost

You should see the default IIS webpage for example:


http://localhost/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Bem-vindo
Καλώς ορίσατε
Vítejte
Välkommen
환영합니다
До
по

8.3 Install the Console

8.3.1 Internet Explorer Enhanced Security

Microsoft Edge is supported but we recommend you turn off IE enhanced settings.

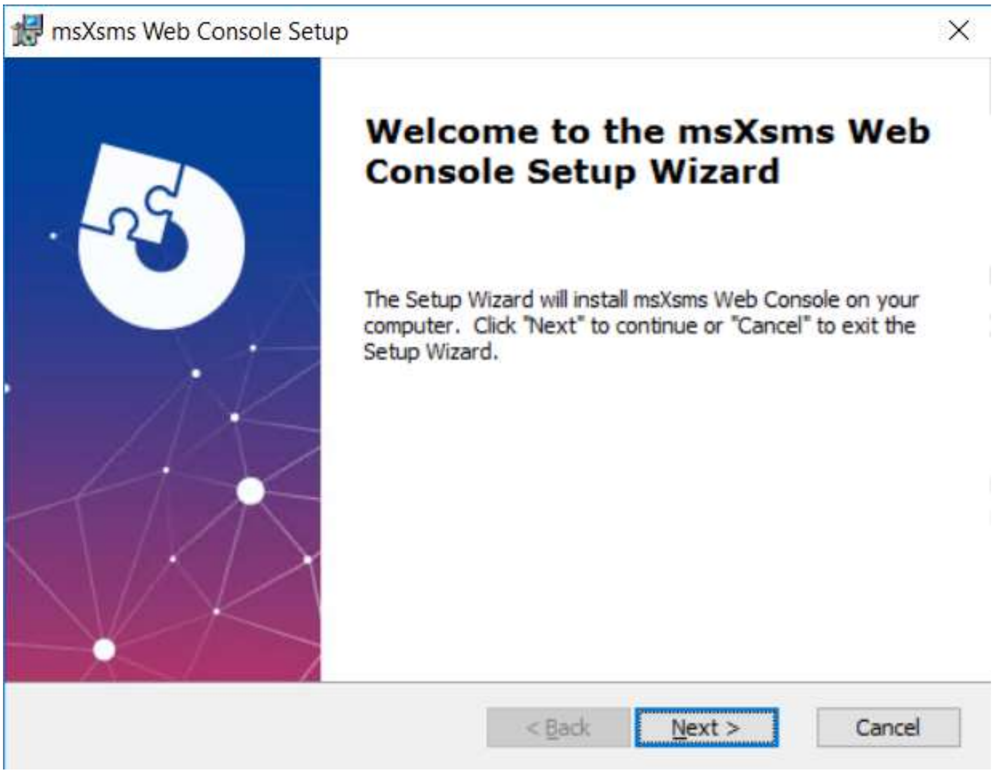
- Run Server Manager
- Turn OFF IE Enhanced Security because this can affect the operation of ASP.NET based applications.

8.3.2 Console installation

The console can be installed on one or more SMS servers.

Navigate to program files\BNS Group\sms Installation Software and Tools.

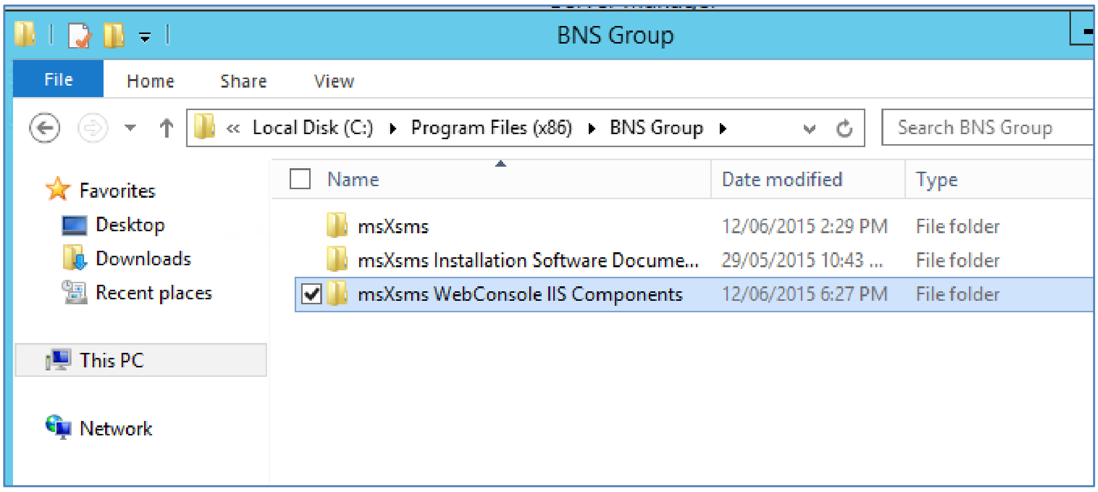
- Open a CMD (Run as Administrator)
- CD to :\Program Files\BNS Group\sms Installation Software Documentation and Tools\Cloud Console IIS Components
- Run Setup_sms_Console.MSI



Welcome to the msXsms Web Console Setup Wizard

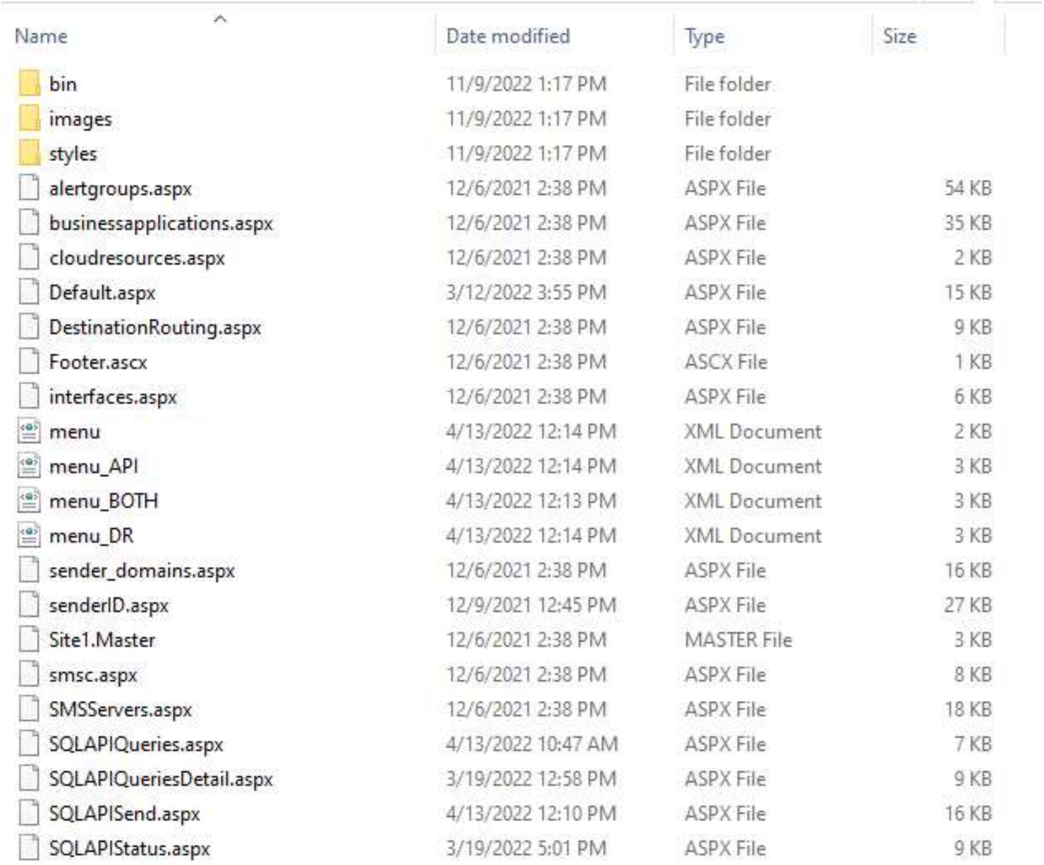
The Setup Wizard will install msXsms Web Console on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

- Install to the volume where all of the software is being installed eg: D: drive.
- Install/Finish



Name	Date modified	Type
msXsms	12/06/2015 2:29 PM	File folder
msXsms Installation Software Docume...	29/05/2015 10:43 ...	File folder
☑ msXsms WebConsole IIS Components	12/06/2015 6:27 PM	File folder

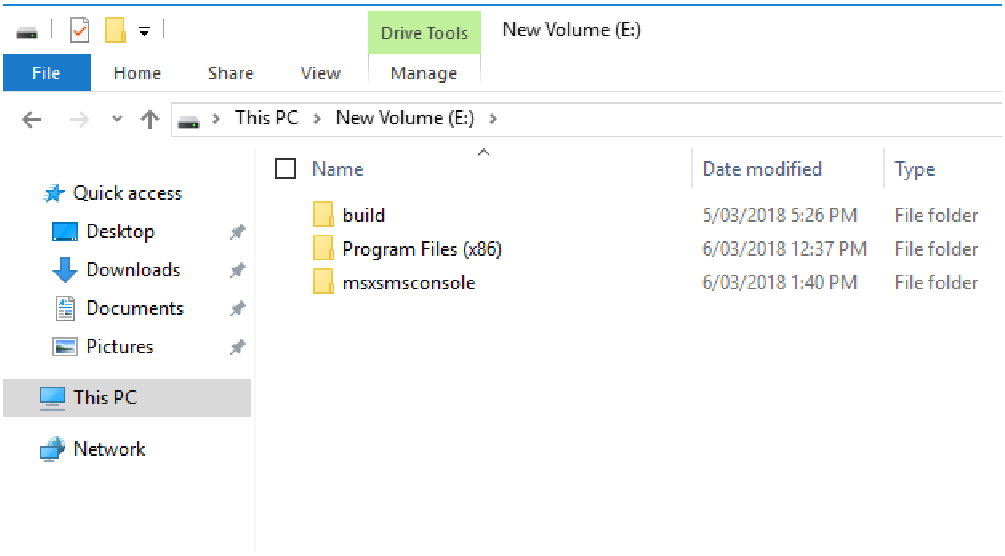
The folder msXsms Console IIS Components contains the files for the web site.



Name	Date modified	Type	Size
bin	11/9/2022 1:17 PM	File folder	
images	11/9/2022 1:17 PM	File folder	
styles	11/9/2022 1:17 PM	File folder	
alertgroups.aspx	12/6/2021 2:38 PM	ASPX File	54 KB
businessapplications.aspx	12/6/2021 2:38 PM	ASPX File	35 KB
cloudresources.aspx	12/6/2021 2:38 PM	ASPX File	2 KB
Default.aspx	3/12/2022 3:55 PM	ASPX File	15 KB
DestinationRouting.aspx	12/6/2021 2:38 PM	ASPX File	9 KB
Footer.ascx	12/6/2021 2:38 PM	ASCX File	1 KB
interfaces.aspx	12/6/2021 2:38 PM	ASPX File	6 KB
menu	4/13/2022 12:14 PM	XML Document	2 KB
menu_API	4/13/2022 12:14 PM	XML Document	3 KB
menu_BOTH	4/13/2022 12:13 PM	XML Document	3 KB
menu_DR	4/13/2022 12:14 PM	XML Document	3 KB
sender_domains.aspx	12/6/2021 2:38 PM	ASPX File	16 KB
senderID.aspx	12/9/2021 12:45 PM	ASPX File	27 KB
Site1.Master	12/6/2021 2:38 PM	MASTER File	3 KB
smsc.aspx	12/6/2021 2:38 PM	ASPX File	8 KB
SMSServers.aspx	12/6/2021 2:38 PM	ASPX File	18 KB
SQLAPIQueries.aspx	4/13/2022 10:47 AM	ASPX File	7 KB
SQLAPIQueriesDetail.aspx	3/19/2022 12:58 PM	ASPX File	9 KB
SQLAPISend.aspx	4/13/2022 12:10 PM	ASPX File	16 KB
SQLAPIStatus.aspx	3/19/2022 5:01 PM	ASPX File	9 KB

8.4 Configure IIS

8.4.1 Create folder for SMS console web site

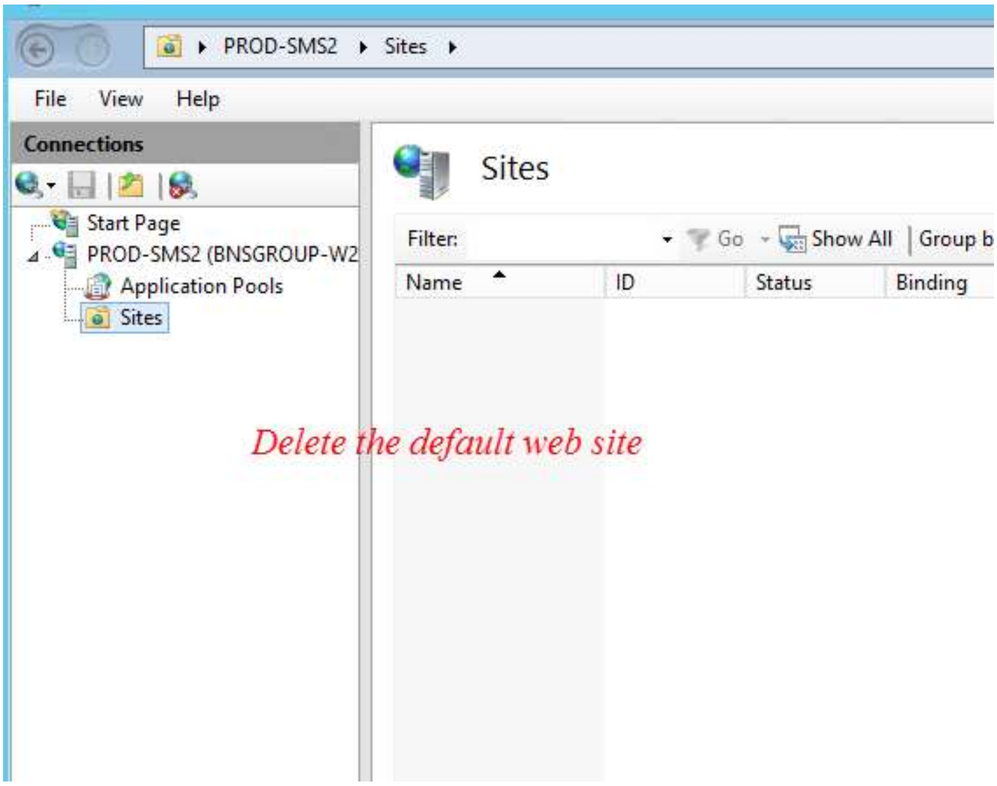


Name	Date modified	Type
build	5/03/2018 5:26 PM	File folder
Program Files (x86)	6/03/2018 12:37 PM	File folder
msxsmsconsole	6/03/2018 1:40 PM	File folder

- Create a folder called smsconsole on any drive letter
- Copy all of the web site files and sub folders from sms Console IIS Components folder into the smsconsole folder.

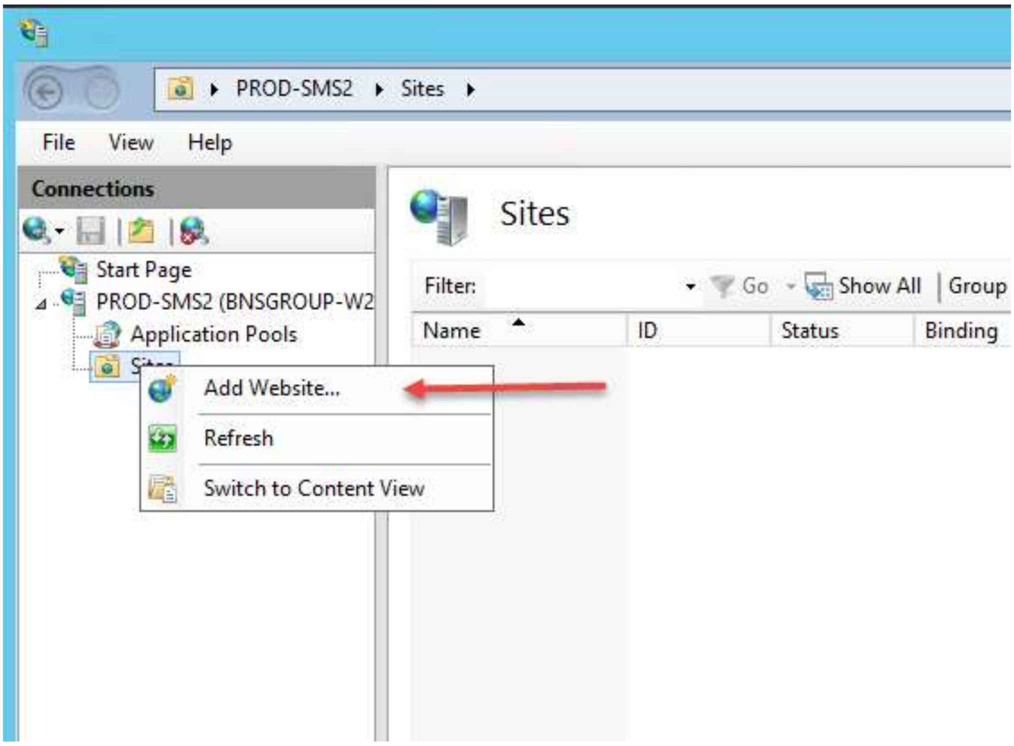
8.4.2 Configure IIS

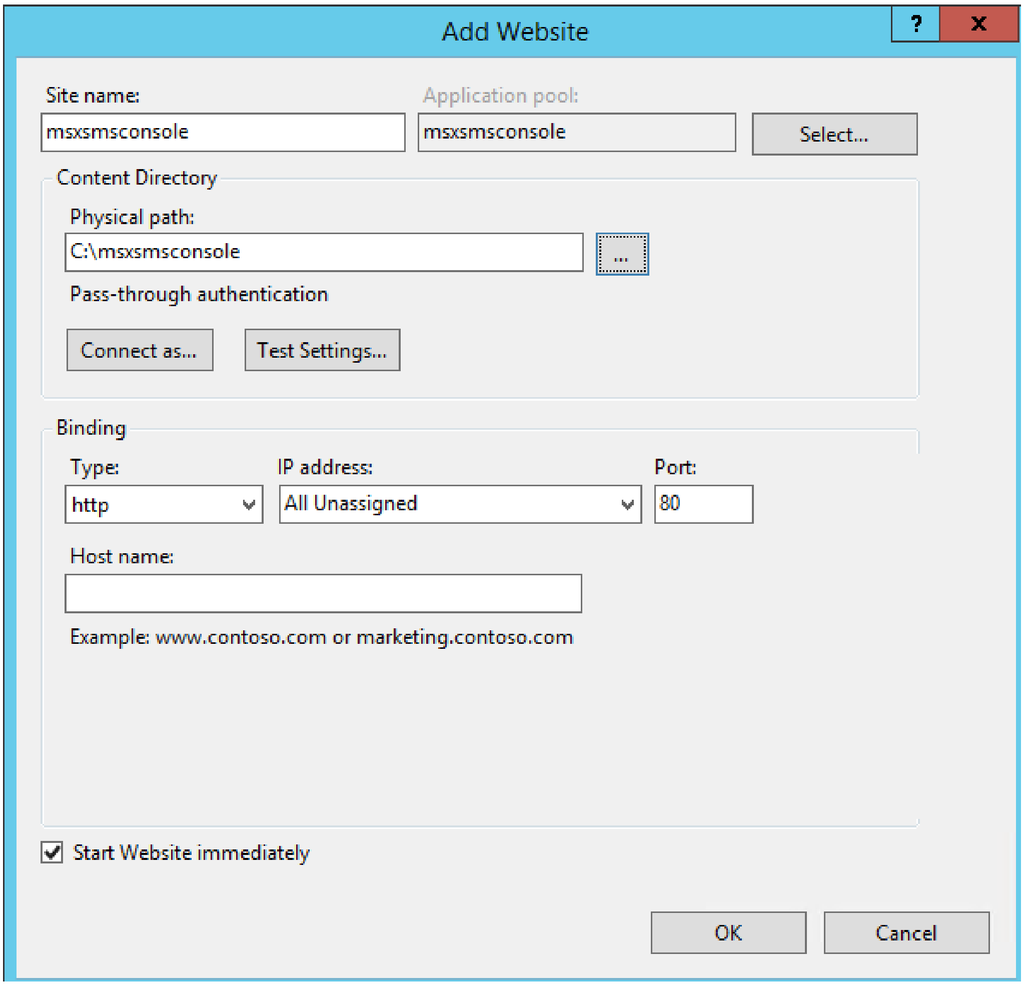
- From the Start screen select Windows Administrative tools
- Run Internet Information Services (IIS) Manager.
- From IIS remove the default web site



Delete the default web site

- From IIS create a web site





Add Website

Site name: msxsmsconsole

Application pool: msxsmsconsole

Content Directory

Physical path: C:\msxsmsconsole

Pass-through authentication

Binding

Type: http

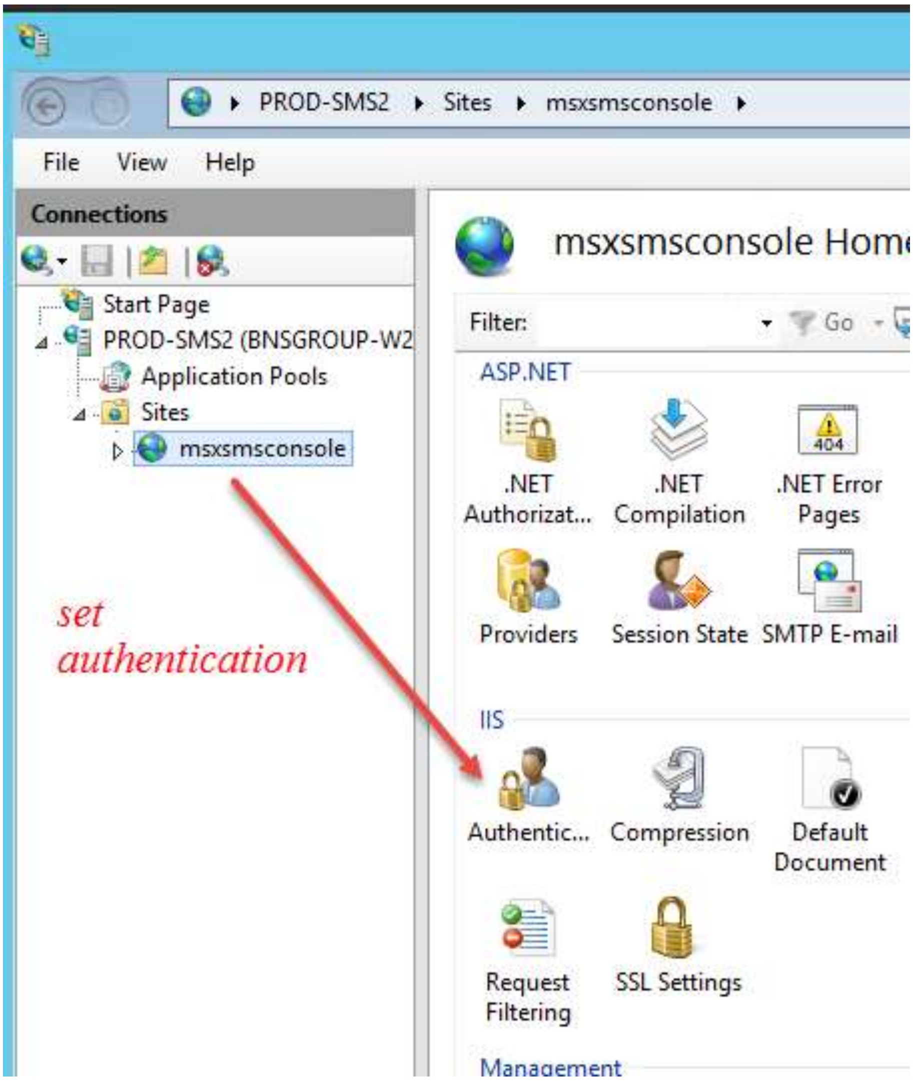
IP address: All Unassigned

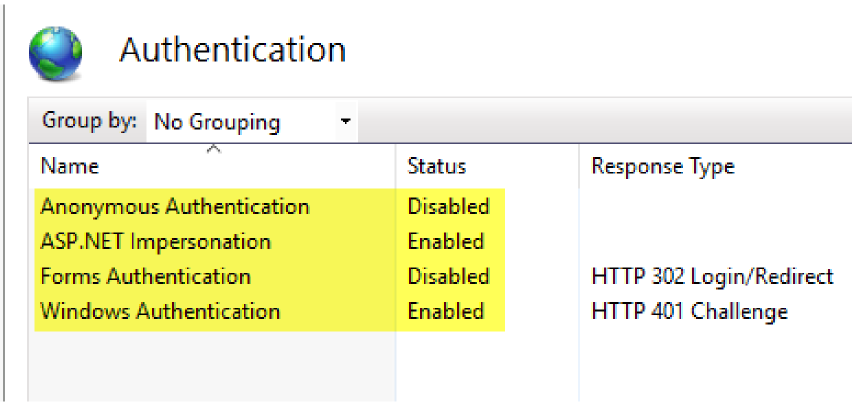
Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

☑ Start Website immediately





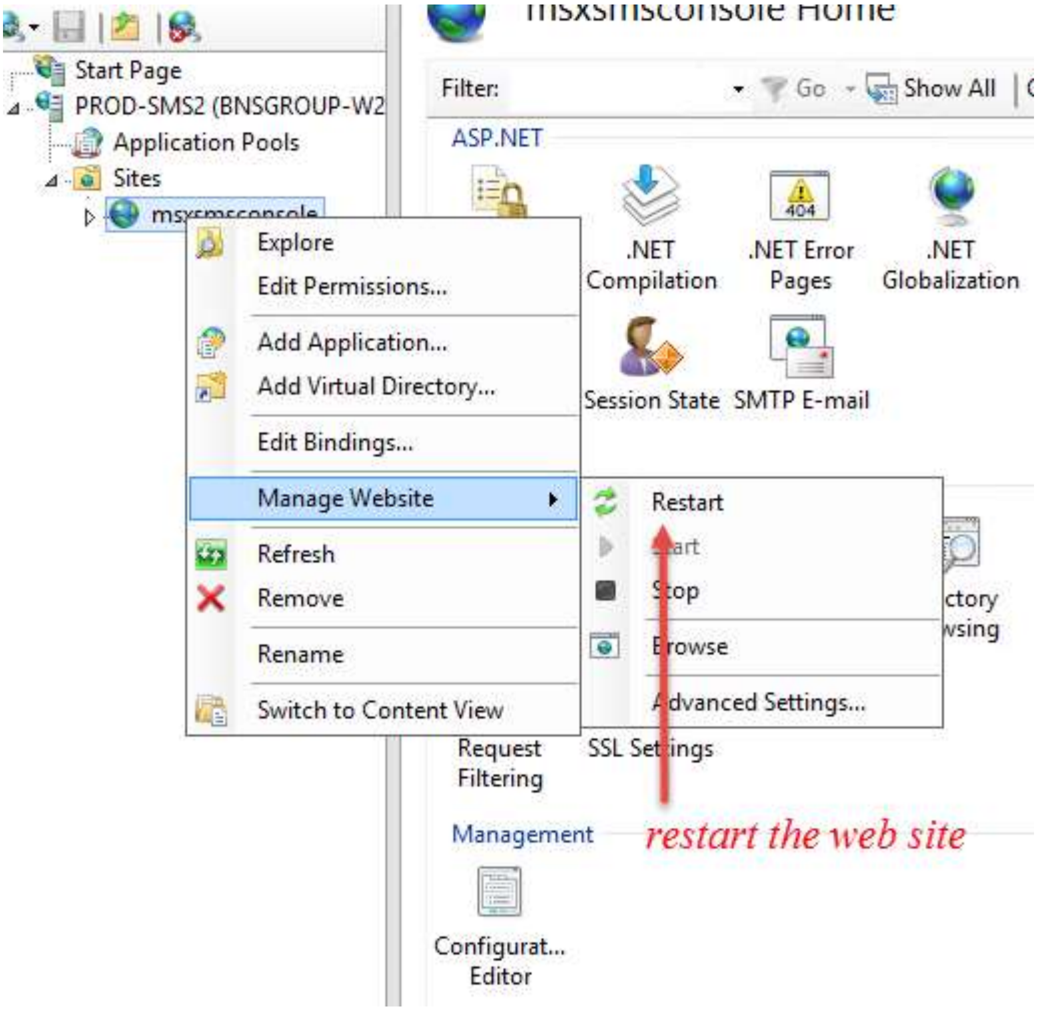
Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Enabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

- Set the above options

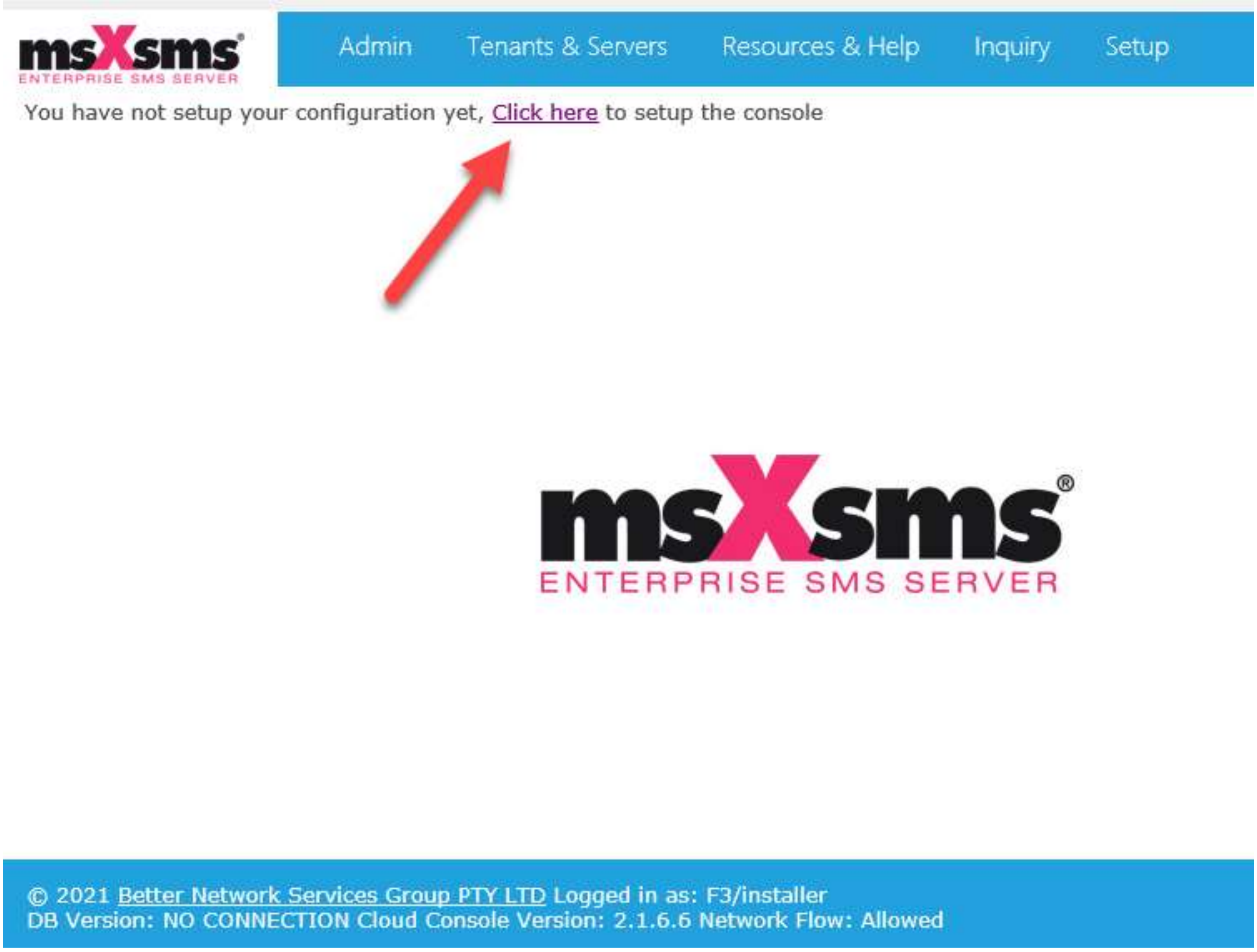
- From IIS, restart the web site



8.5 Configure settings and test console connection

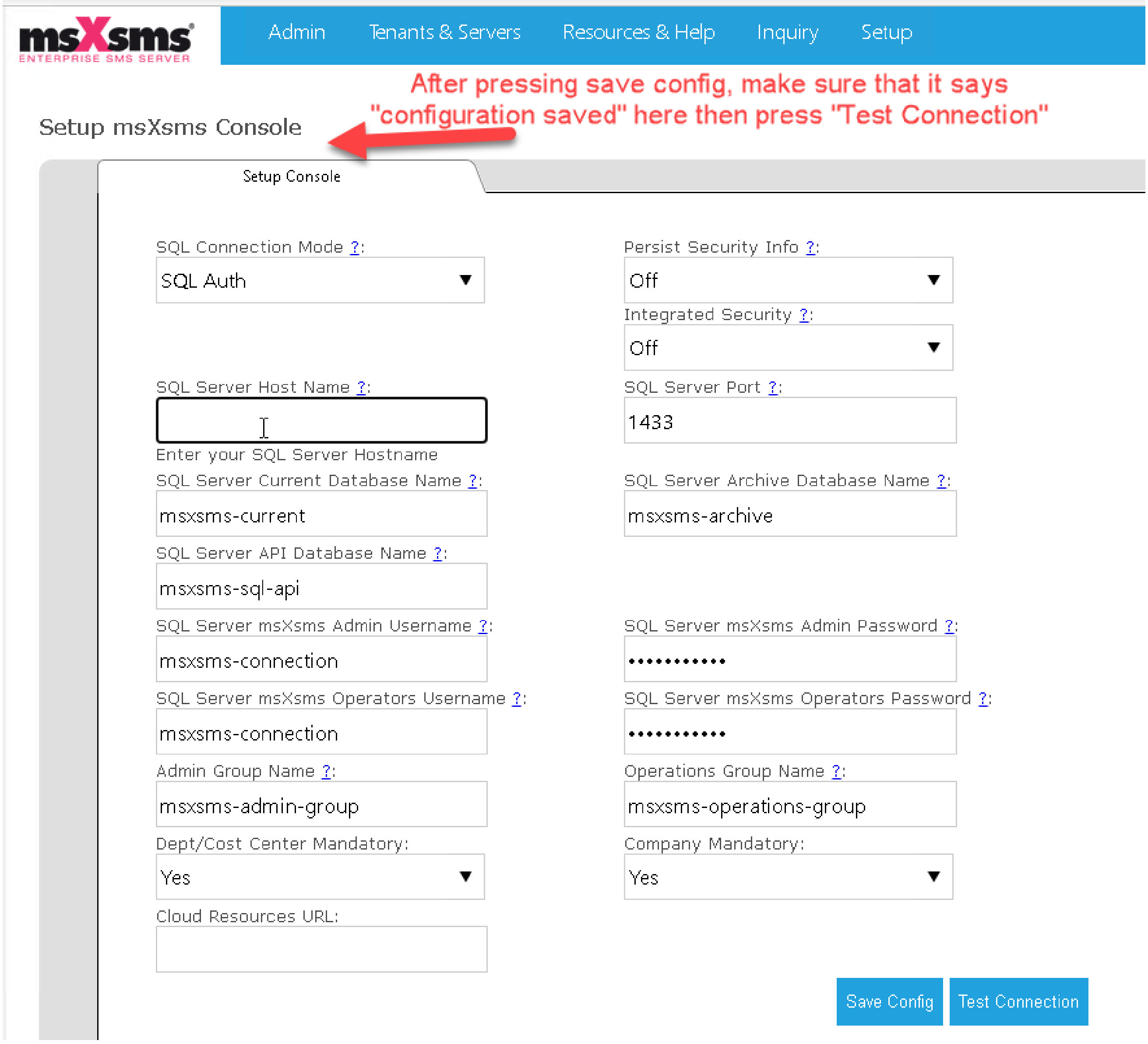
- Run Edge or Internet Explorer from the SMS Server and enter http://localhost

The following web page should be displayed.



You have not setup your configuration yet, Click here to setup the console

© 2021 Better Network Services Group PTY LTD Logged in as: F3/installer
DB Version: NO CONNECTION Cloud Console Version: 2.1.6.6 Network Flow: Allowed



After pressing save config, make sure that it says "configuration saved" here then press "Test Connection"

Setup msXsms Console

SQL Connection Mode ?: SQL Auth

Persist Security Info ?: Off

Integrated Security ?: Off

SQL Server Host Name ?:

Enter your SQL Server Hostname

SQL Server Port ?: 1433

SQL Server Current Database Name ?: msxsms-current

SQL Server Archive Database Name ?: msxsms-archive

SQL Server API Database Name ?: msxsms-sql-api

SQL Server msXsms Admin Username ?: msxsms-connection

SQL Server msXsms Admin Password ?: •••••••••••

SQL Server msXsms Operators Username ?: msxsms-connection

SQL Server msXsms Operators Password ?: •••••••••••

Admin Group Name ?: msxsms-admin-group

Operations Group Name ?: msxsms-operations-group

Dept/Cost Center Mandatory: Yes

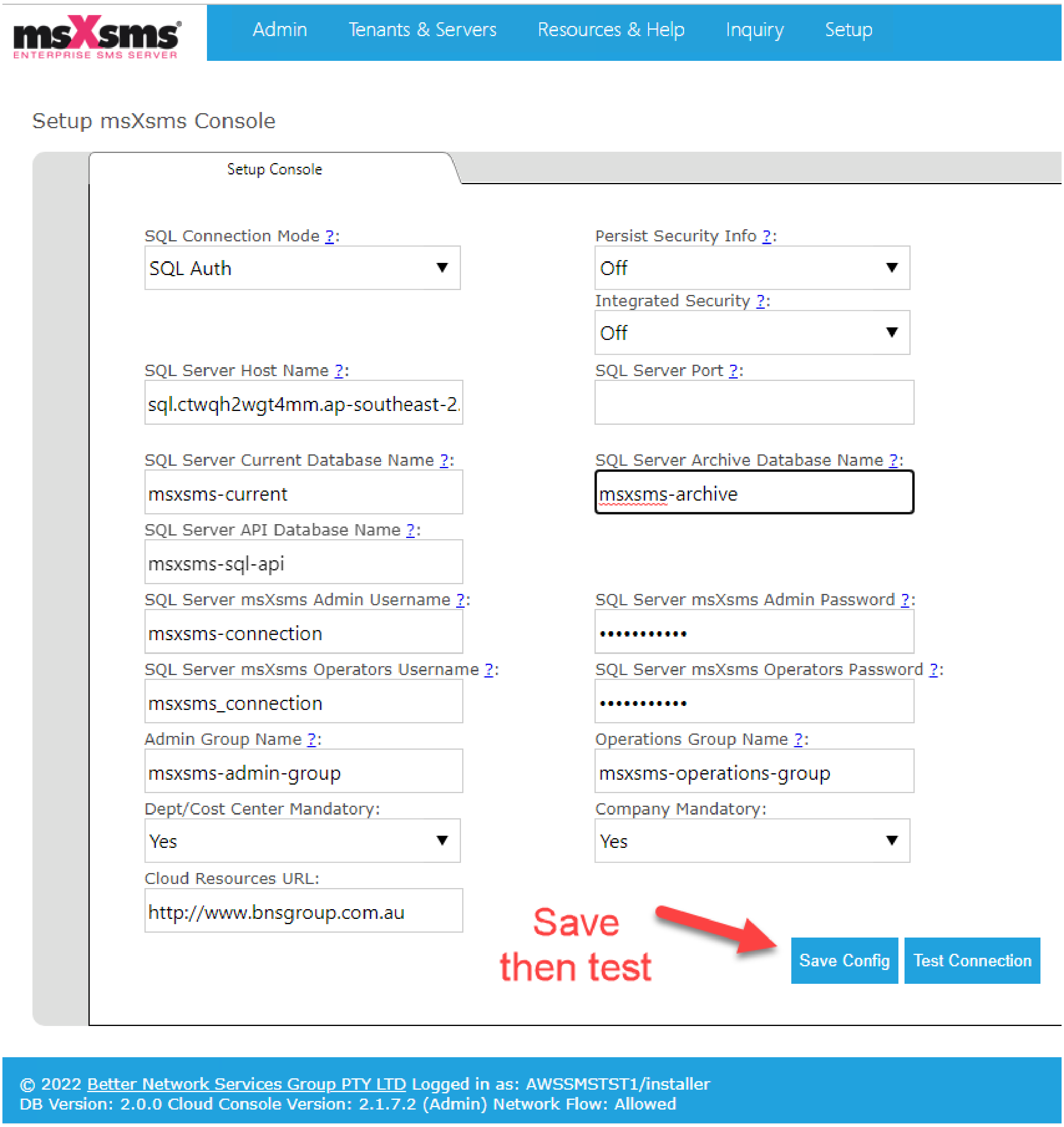
Company Mandatory: Yes

Cloud Resources URL:

- AWS RDS SQL Server Host Name = RDS MS SQL endpoint connection, 1433
- PORT field = blank

- Supply the name of your SQL Server and the names of the current and archive databases.
- If you have SQL Express or an instance then the SQL Server string is Server\Instance
- Supply the SQL Server connection user account. Note this is the same for both Admin and Operations.
- Save the configuration.

8.5.1 Test the connection to the current database

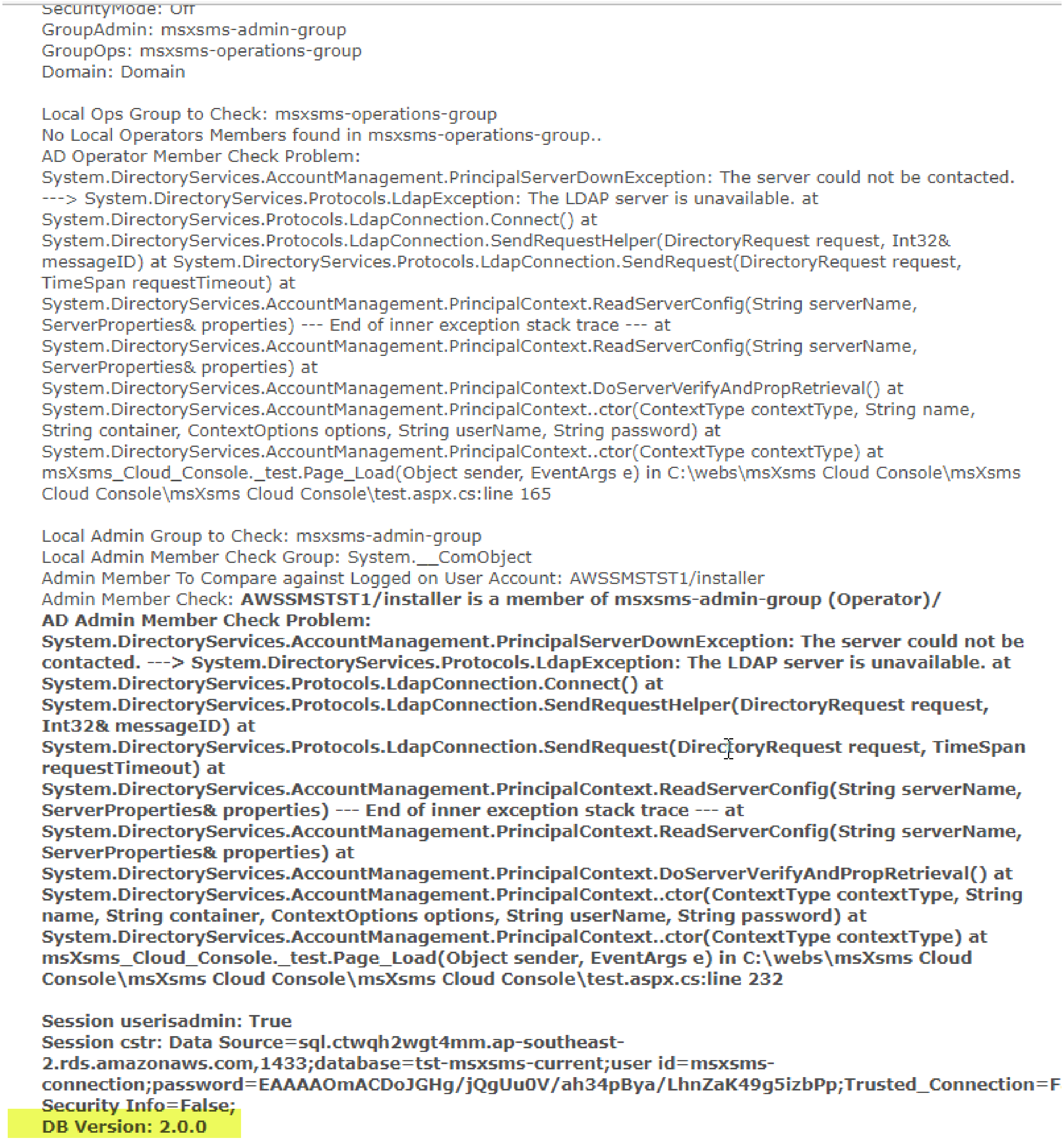


Setup msXsms Console

SQL Connection Mode ?: SQL Auth	Persist Security Info ?: Off
	Integrated Security ?: Off
SQL Server Host Name ?: sql.ctwqh2wgt4mm.ap-southeast-2.	SQL Server Port ?:
SQL Server Current Database Name ?: msxsms-current	SQL Server Archive Database Name ?: msxsms-archive
SQL Server API Database Name ?: msxsms-sql-api	
SQL Server msXsms Admin Username ?: msxsms-connection	SQL Server msXsms Admin Password ?: •••••••••••
SQL Server msXsms Operators Username ?: msxsms_connection	SQL Server msXsms Operators Password ?: •••••••••••
Admin Group Name ?: msxsms-admin-group	Operations Group Name ?: msxsms-operations-group
Dept/Cost Center Mandatory: Yes	Company Mandatory: Yes
Cloud Resources URL: http://www.bnsgroup.com.au	

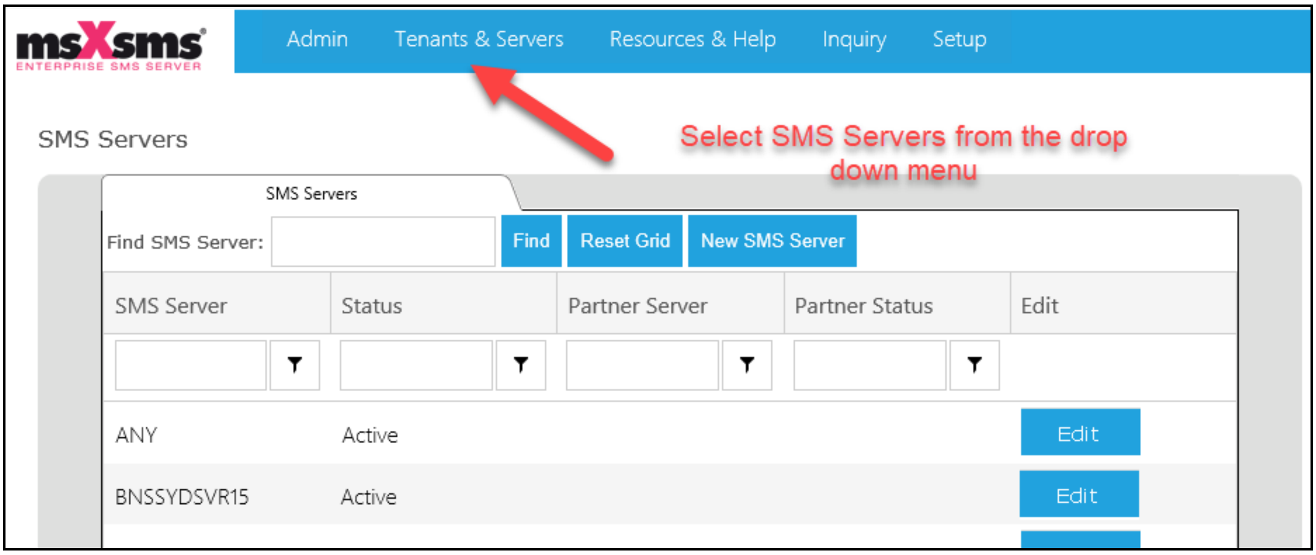
© 2022 Better Network Services Group PTY LTD Logged in as: AWSSMSTST1/installer
DB Version: 2.0.0 Cloud Console Version: 2.1.7.2 (Admin) Network Flow: Allowed

- Select test connection



```
SecurityMode: Off
GroupAdmin: msxsms-admin-group
GroupOps: msxsms-operations-group
Domain: Domain

Local Ops Group to Check: msxsms-operations-group
No Local Operators Members found in msxsms-operations-group..
AD Operator Member Check Problem:
System.DirectoryServices.AccountManagement.PrincipalServerDownException: The server could not be contacted.
---> System.DirectoryServices.Protocols.LdapException: The LDAP server is unavailable. at
System.DirectoryServices.Protocols.LdapConnection.Connect() at
System.DirectoryServices.Protocols.LdapConnection.SendRequestHelper(DirectoryRequest request, Int32&
messageID) at System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRequest request,
TimeSpan requestTimeout) at
System.DirectoryServices.AccountManagement.PrincipalContext.ReadServerConfig(String serverName,
ServerProperties& properties) --- End of inner exception stack trace --- at
System.DirectoryServices.AccountManagement.PrincipalContext.ReadServerConfig(String serverName,
ServerProperties& properties) at
System.DirectoryServices.AccountManagement.PrincipalContext.DoServerVerifyAndPropRetrieval() at
System.DirectoryServices.AccountManagement.PrincipalContext..ctor(ContextType contextType, String name,
String container, ContextOptions options, String userName, String password) at
System.DirectoryServices.AccountManagement.PrincipalContext..ctor(ContextType contextType) at
msXsms_Cloud_Console._test.Page_Load(Object sender, EventArgs e) in C:\webs\msXsms Cloud Console\msXsms
Cloud Console\msXsms Cloud Console\test.aspx.cs:line 165

Local Admin Group to Check: msxsms-admin-group
Local Admin Member Check Group: System.__ComObject
Admin Member To Compare against Logged on User Account: AWSSMSTST1/installer
Admin Member Check: AWSSMSTST1/installer is a member of msxsms-admin-group (Operator)/
AD Admin Member Check Problem:
System.DirectoryServices.AccountManagement.PrincipalServerDownException: The server could not be
contacted. ---> System.DirectoryServices.Protocols.LdapException: The LDAP server is unavailable. at
System.DirectoryServices.Protocols.LdapConnection.Connect() at
System.DirectoryServices.Protocols.LdapConnection.SendRequestHelper(DirectoryRequest request,
Int32& messageID) at
System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRequest request, TimeSpan
requestTimeout) at
System.DirectoryServices.AccountManagement.PrincipalContext.ReadServerConfig(String serverName,
ServerProperties& properties) --- End of inner exception stack trace --- at
System.DirectoryServices.AccountManagement.PrincipalContext.ReadServerConfig(String serverName,
ServerProperties& properties) at
System.DirectoryServices.AccountManagement.PrincipalContext.DoServerVerifyAndPropRetrieval() at
System.DirectoryServices.AccountManagement.PrincipalContext..ctor(ContextType contextType, String
name, String container, ContextOptions options, String userName, String password) at
System.DirectoryServices.AccountManagement.PrincipalContext..ctor(ContextType contextType) at
msXsms_Cloud_Console._test.Page_Load(Object sender, EventArgs e) in C:\webs\msXsms Cloud
Console\msXsms Cloud Console\msXsms Cloud Console\test.aspx.cs:line 232

Session userisadmin: True
Session cstr: Data Source=sql.ctwqh2wgt4mm.ap-southeast-
2.rds.amazonaws.com,1433;database=tst-msxsms-current;user id=msxsms-
connection;password=EAAAAOmACDoJGHg/jQgUu0V/ah34pBya/LhnZaK49g5izbPp;Trusted_Connection=F
Security Info=False;
DB Version: 2.0.0
```

- A successful connection to the database is confirmed if the DB Version: is shown at the bottom of the screen above.



Select SMS Servers from the drop down menu

SMS Servers

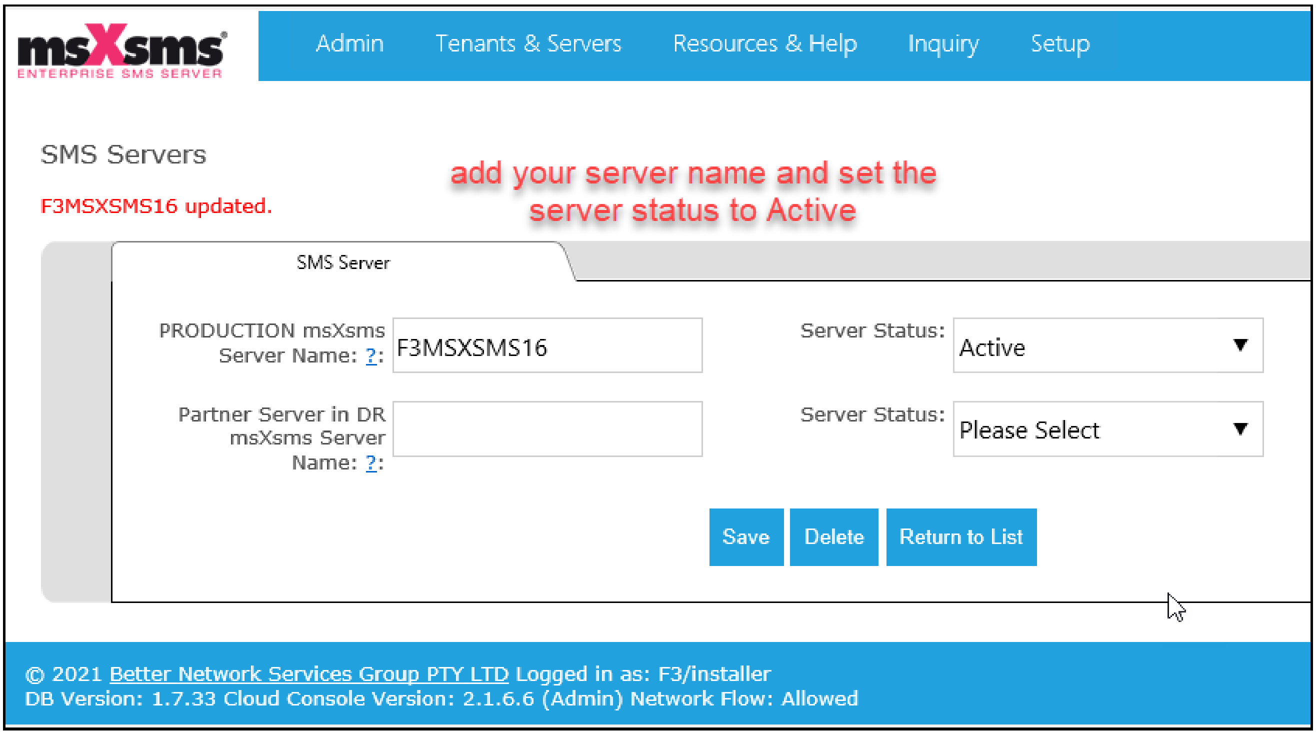
SMS Servers

Find SMS Server:

SMS Server	Status	Partner Server	Partner Status	Edit
ANY	Active			Edit
BNSSYDSVR15	Active			Edit

- Then click on Servers once you have a successful connection.

- Add your new SMS server



add your server name and set the server status to Active

SMS Servers

F3MSXSMS16 updated.

SMS Server

PRODUCTION msXsms Server Name: ?: F3MSXSMS16

Server Status: Active

Partner Server in DR msXsms Server Name: ?:

Server Status: Please Select

© 2021 Better Network Services Group PTY LTD Logged in as: F3/installer
DB Version: 1.7.33 Cloud Console Version: 2.1.6.6 (Admin) Network Flow: Allowed

8.5.2 Display of full message in the inquiry menu option

By default the full message of a SMS will not be displayed in the console. To allow the full message to be displayed to administrators, rename the file NOSHOW.MSG to another value eg: NOSHOWxxxx.MSG

8.5.3 Console administration

Refer to https://smskb.bnsgroup.com.au/console

SECTION 9 Exchange Online Mailbox and Graph API settings

9.1 Exchange online

Note: Exchange online has many limits. Large customers with Exchange Server in their network should consider using SMTP Connectors from\to their Exchange server for SMS traffic which has to be SMTP based.

Customers with Exchange online and knowing the limitations, can use Office 365 mailboxes and transport rules.

Exchange online limits can be found at this URL https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits-1

Create an Office 365 mailbox together with Exchange Online transport rules to allow email based users and applications the ability to send to number@domain.SMS

- Create a mailbox and follow all of the steps to register an application in the Azure portal. This is fully documented with examples at Exchange Online Mailbox SMS (bnsgroup.com.au)
- Record all of the details created in Exchange online and the Azure portal in a password database. The details will be required in the next section as part of the main windows services installation.

SECTION 10 Installing SMS Windows Services

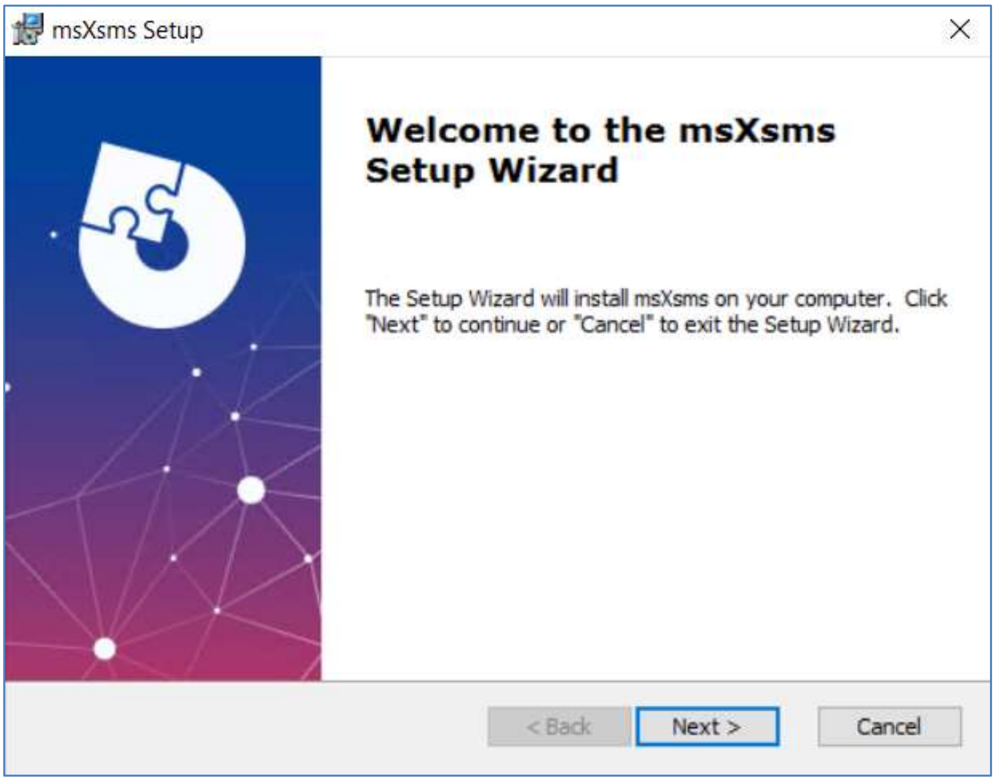
10.1 Before you install the software

- Ensure that you are logged in with full permissions to the server.
- Add the sms service account you set up to the local administrators group.

10.2 Run the Setup program

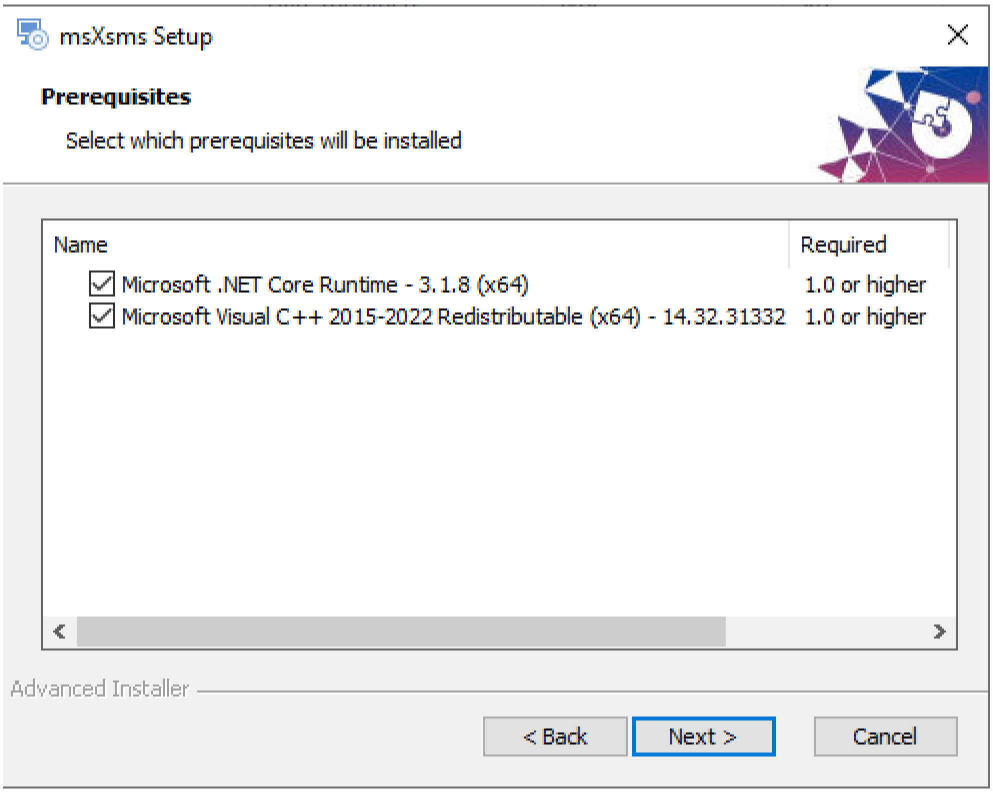
The set up program is located in the directory SMS Software as shown below.

- Run the command prompt elevated.
  - Select Start, All Programs, Accessories then Right click the Command prompt then select 'Run As Administrator'.
- From within the command prompt run the SETUP_SMS.MSI
- Follow the setup wizard.



Welcome to the msXsms Setup Wizard

The Setup Wizard will install msXsms on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

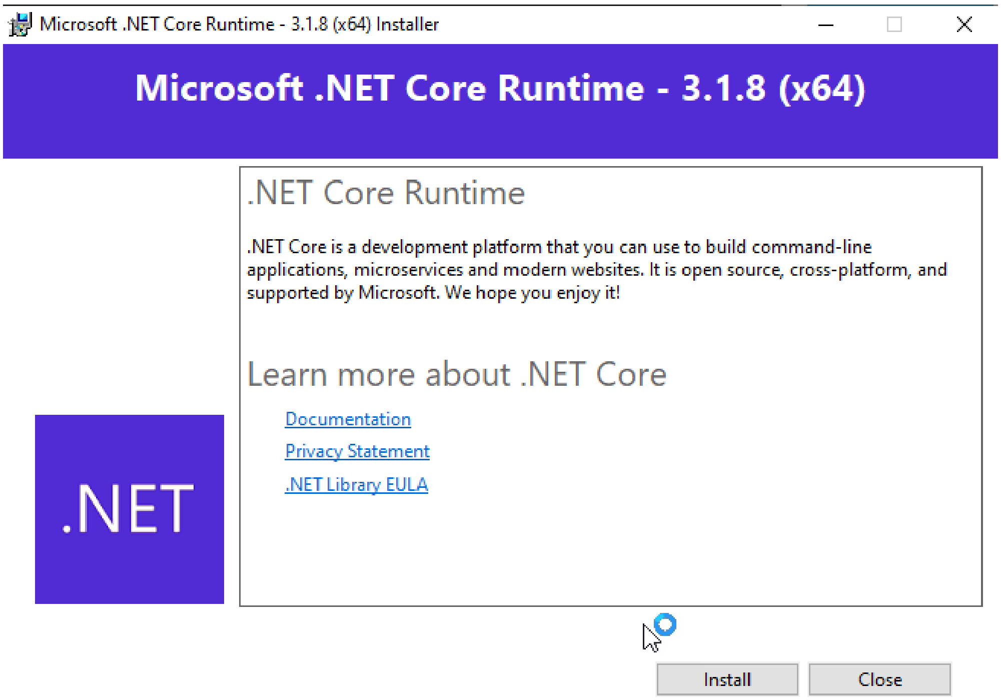


msXsms Setup

Prerequisites

Select which prerequisites will be installed

Name	Required
☑ Microsoft .NET Core Runtime - 3.1.8 (x64)	1.0 or higher
☑ Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332	1.0 or higher



Microsoft .NET Core Runtime - 3.1.8 (x64) Installer

Microsoft .NET Core Runtime - 3.1.8 (x64)

.NET Core Runtime

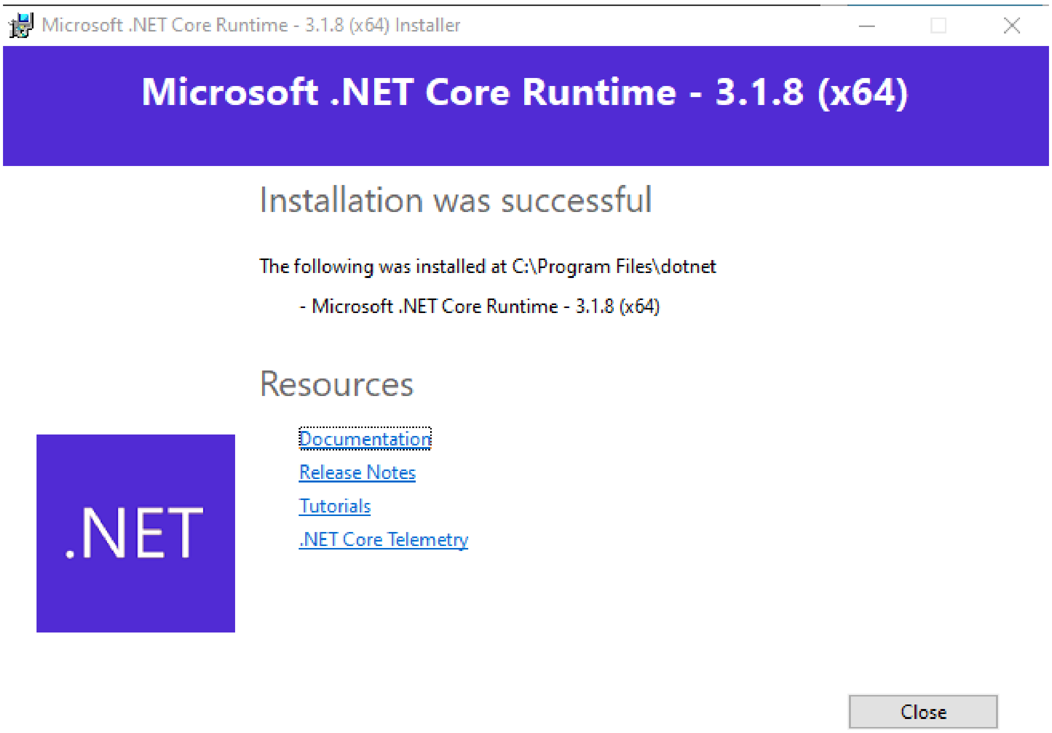
.NET Core is a development platform that you can use to build command-line applications, microservices and modern websites. It is open source, cross-platform, and supported by Microsoft. We hope you enjoy it!

Learn more about .NET Core

Documentation

Privacy Statement

.NET Library EULA



Microsoft .NET Core Runtime - 3.1.8 (x64) Installer

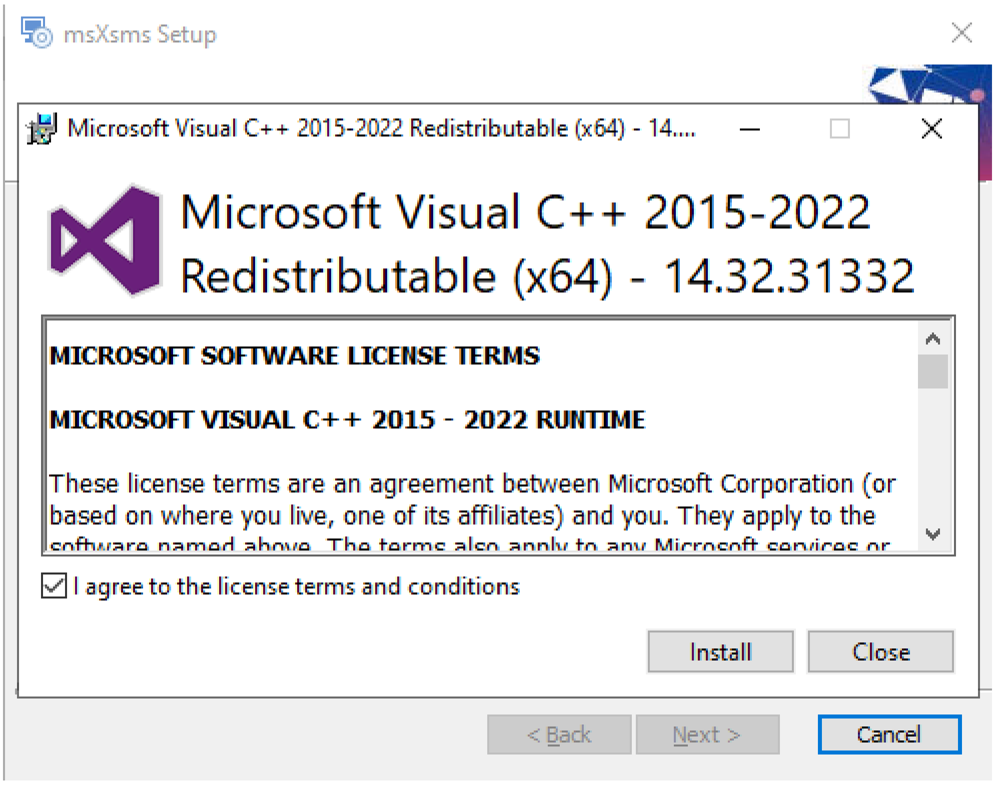
Microsoft .NET Core Runtime - 3.1.8 (x64)

Installation was successful

The following was installed at C:\Program Files\dotnet

- Microsoft .NET Core Runtime - 3.1.8 (x64)

Resources



msXsms Setup

Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14....

Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332

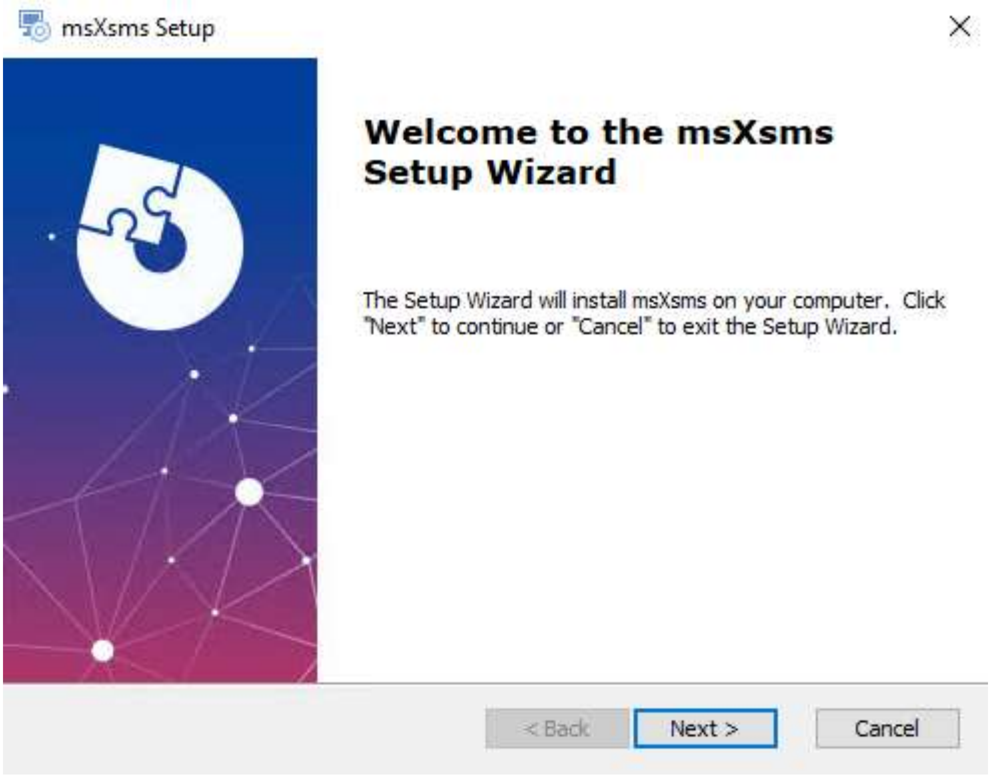
MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT VISUAL C++ 2015 - 2022 RUNTIME

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. They apply to the software named above. The terms also apply to any Microsoft services or

☑ I agree to the license terms and conditions

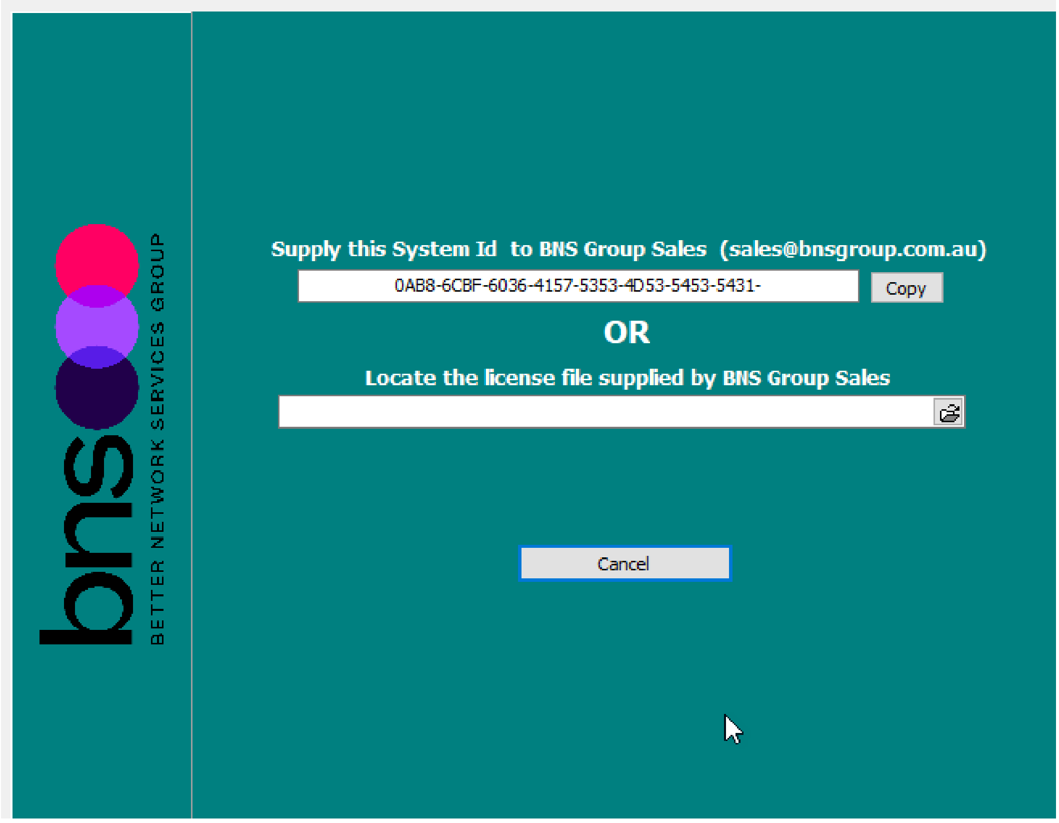
If you see a screen from the installation showing something similar to the following, it is because there is a later version already installed on this server.



msXsms Setup

Welcome to the msXsms Setup Wizard

The Setup Wizard will install msXsms on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.



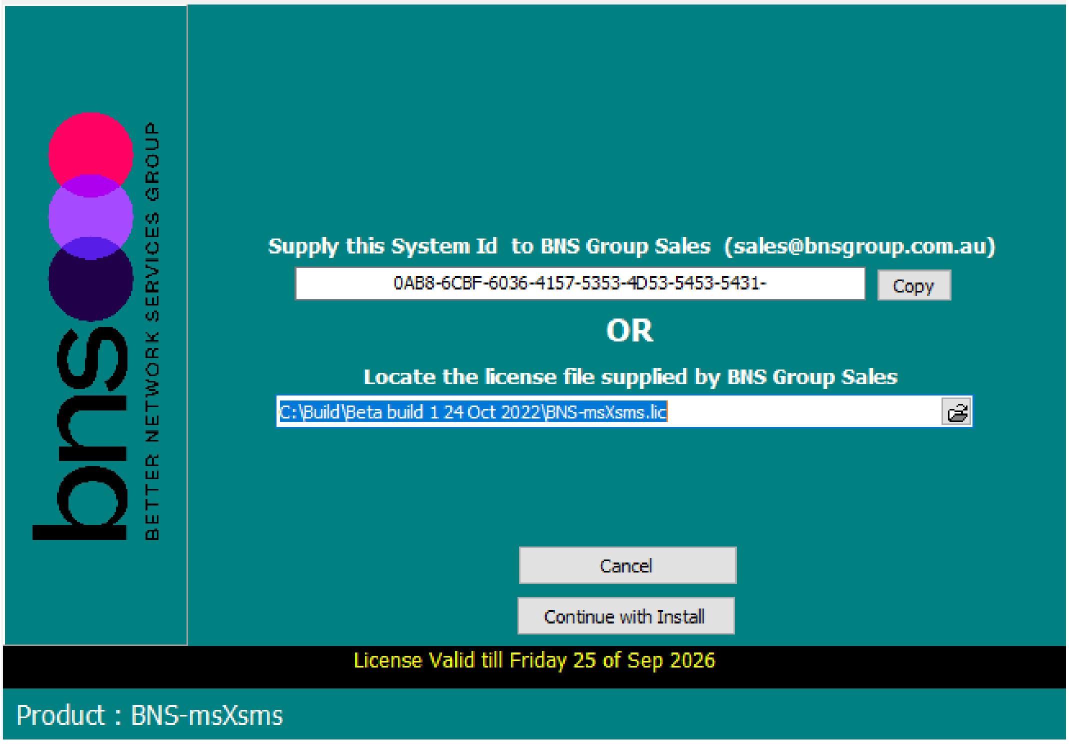
Supply this System Id to BNS Group Sales (sales@bnsgroup.com.au)

0AB8-6CBF-6036-4157-5353-4D53-5453-5431-

OR

Locate the license file supplied by BNS Group Sales

- Locate the license file used earlier.



Supply this System Id to BNS Group Sales (sales@bnsgroup.com.au)

0AB8-6CBF-6036-4157-5353-4D53-5453-5431-

OR

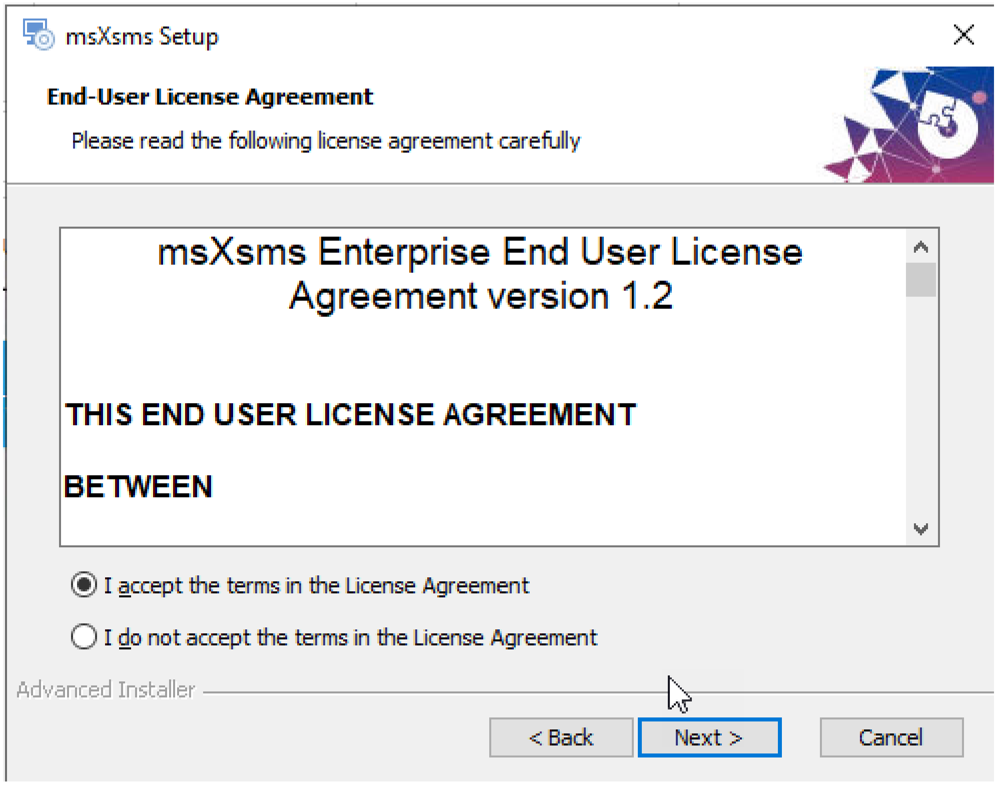
Locate the license file supplied by BNS Group Sales

C:\Build\Beta build 1 24 Oct 2022\BNS-msXsms.lic

License Valid till Friday 25 of Sep 2026

Product : BNS-msXsms

- Press continue with install once you supply a valid license file.



msXsms Setup

End-User License Agreement

Please read the following license agreement carefully

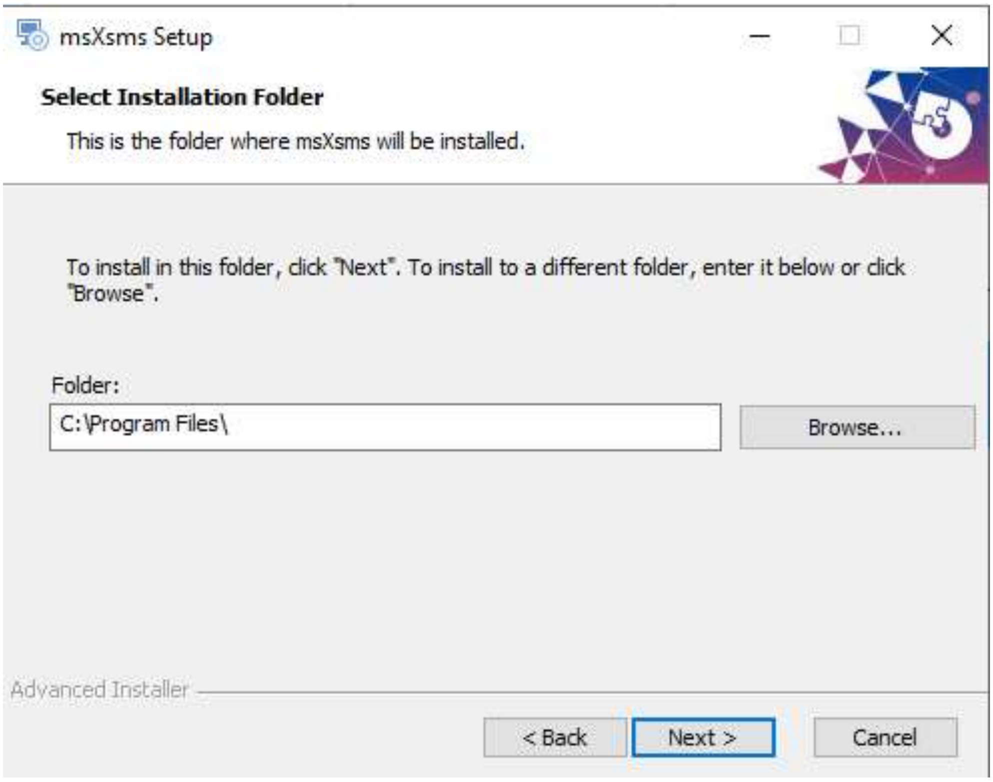
msXsms Enterprise End User License Agreement version 1.2

THIS END USER LICENSE AGREEMENT

BETWEEN

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement



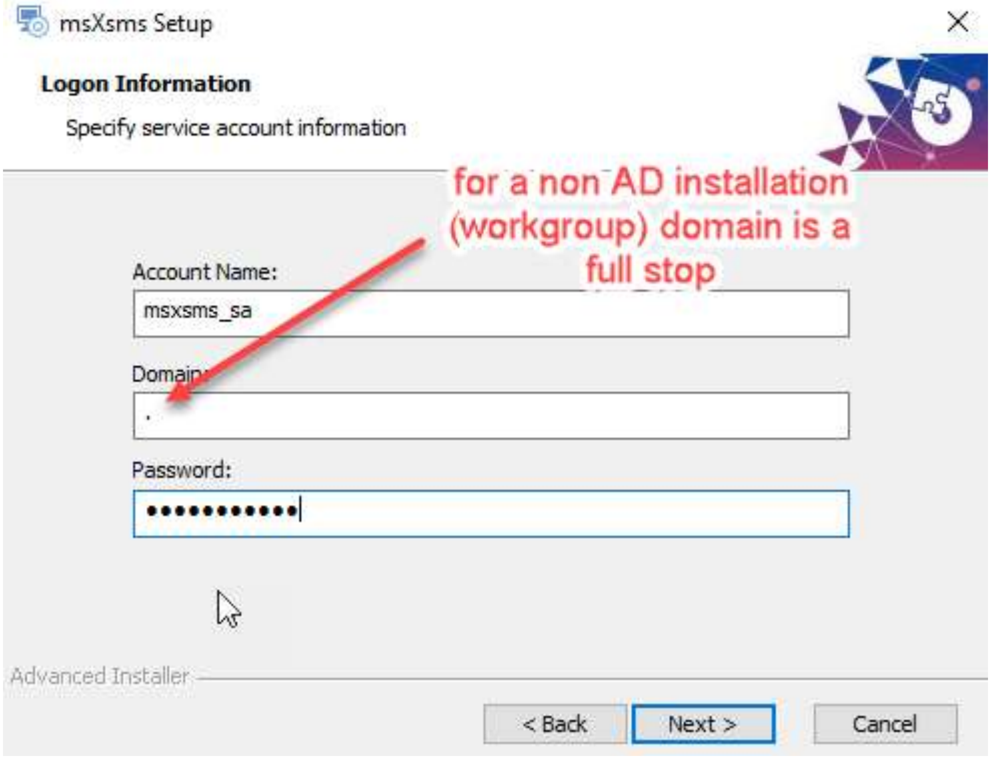
msXsms Setup

Select Installation Folder

This is the folder where msXsms will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\



msXsms Setup

Logon Information

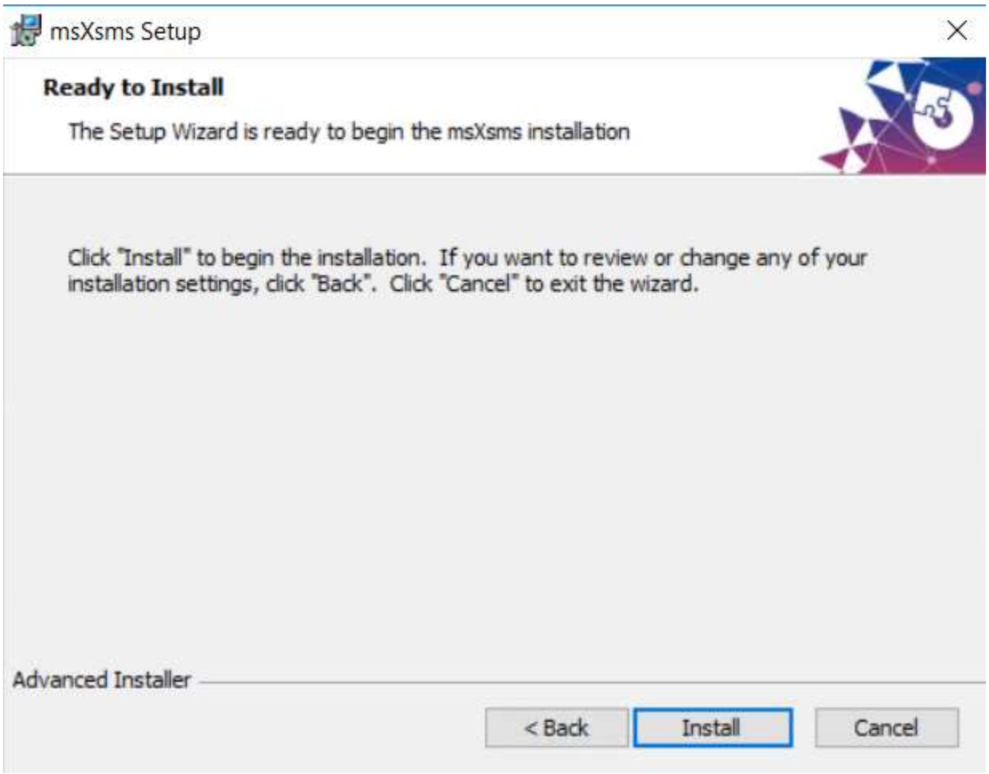
Specify service account information

Account Name: msxsms_sa

Domain: .

Password: ●●●●●●●●●●●●

All SMS Servers can use the same service account.

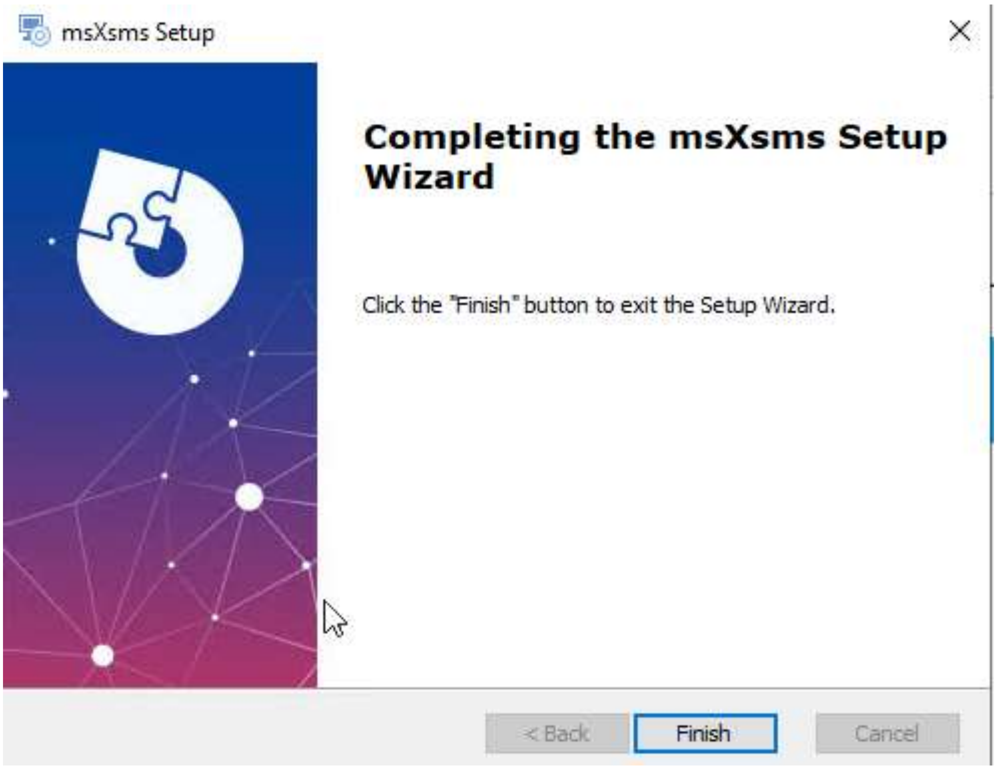


msXsms Setup

Ready to Install

The Setup Wizard is ready to begin the msXsms installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

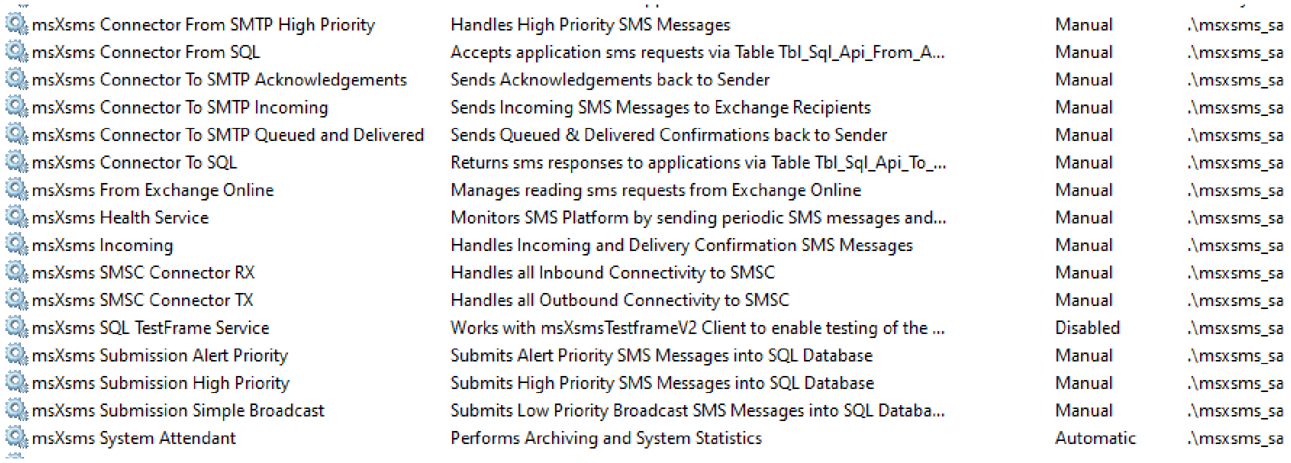


msXsms Setup

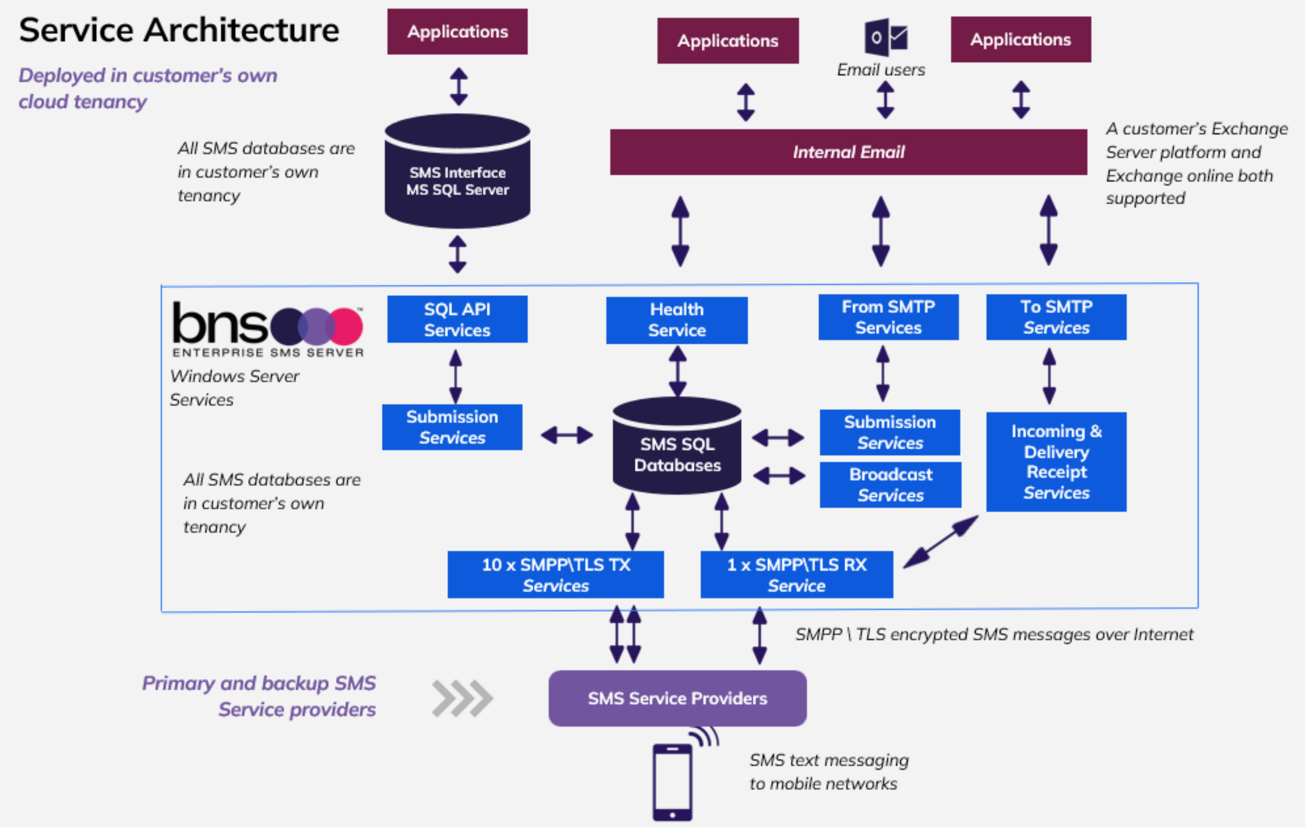
Completing the msXsms Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

10.3 Check the services are installed



msXsms Connector From SMTP High Priority	Handles High Priority SMS Messages	Manual	.\msxsms_sa
msXsms Connector From SQL	Accepts application sms requests via Table Tbl_Sql_Api_From_A...	Manual	.\msxsms_sa
msXsms Connector To SMTP Acknowledgements	Sends Acknowledgements back to Sender	Manual	.\msxsms_sa
msXsms Connector To SMTP Incoming	Sends Incoming SMS Messages to Exchange Recipients	Manual	.\msxsms_sa
msXsms Connector To SMTP Queued and Delivered	Sends Queued & Delivered Confirmations back to Sender	Manual	.\msxsms_sa
msXsms Connector To SQL	Returns sms responses to applications via Table Tbl_Sql_Api_To_...	Manual	.\msxsms_sa
msXsms From Exchange Online	Manages reading sms requests from Exchange Online	Manual	.\msxsms_sa
msXsms Health Service	Monitors SMS Platform by sending periodic SMS messages and...	Manual	.\msxsms_sa
msXsms Incoming	Handles Incoming and Delivery Confirmation SMS Messages	Manual	.\msxsms_sa
msXsms SMSC Connector RX	Handles all Inbound Connectivity to SMSC	Manual	.\msxsms_sa
msXsms SMSC Connector TX	Handles all Outbound Connectivity to SMSC	Manual	.\msxsms_sa
msXsms SQL TestFrame Service	Works with msXsmsTestframeV2 Client to enable testing of the ...	Disabled	.\msxsms_sa
msXsms Submission Alert Priority	Submits Alert Priority SMS Messages into SQL Database	Manual	.\msxsms_sa
msXsms Submission High Priority	Submits High Priority SMS Messages into SQL Database	Manual	.\msxsms_sa
msXsms Submission Simple Broadcast	Submits Low Priority Broadcast SMS Messages into SQL Databa...	Manual	.\msxsms_sa
msXsms System Attendant	Performs Archiving and System Statistics	Automatic	.\msxsms_sa


Service Architecture
Deployed in customer's own cloud tenancy
Applications
Applications
Email users
Applications
All SMS databases are in customer's own tenancy
SMS Interface MS SQL Server
Internal Email
A customer's Exchange Server platform and Exchange online both supported
bns ENTERPRISE SMS SERVER
Windows Server Services
SQL API Services
Health Service
From SMTP Services
To SMTP Services
Submission Services
SMS SQL Databases
Submission Services
Broadcast Services
Incoming & Delivery Receipt Services
All SMS databases are in customer's own tenancy
10 x SMPP\TLS TX Services
1 x SMPP\TLS RX Service
SMPP \ TLS encrypted SMS messages over Internet
Primary and backup SMS Service providers
SMS Service Providers
SMS text messaging to mobile networks

10.4 Add the service account to local administrators group

- Check that this has been completed.

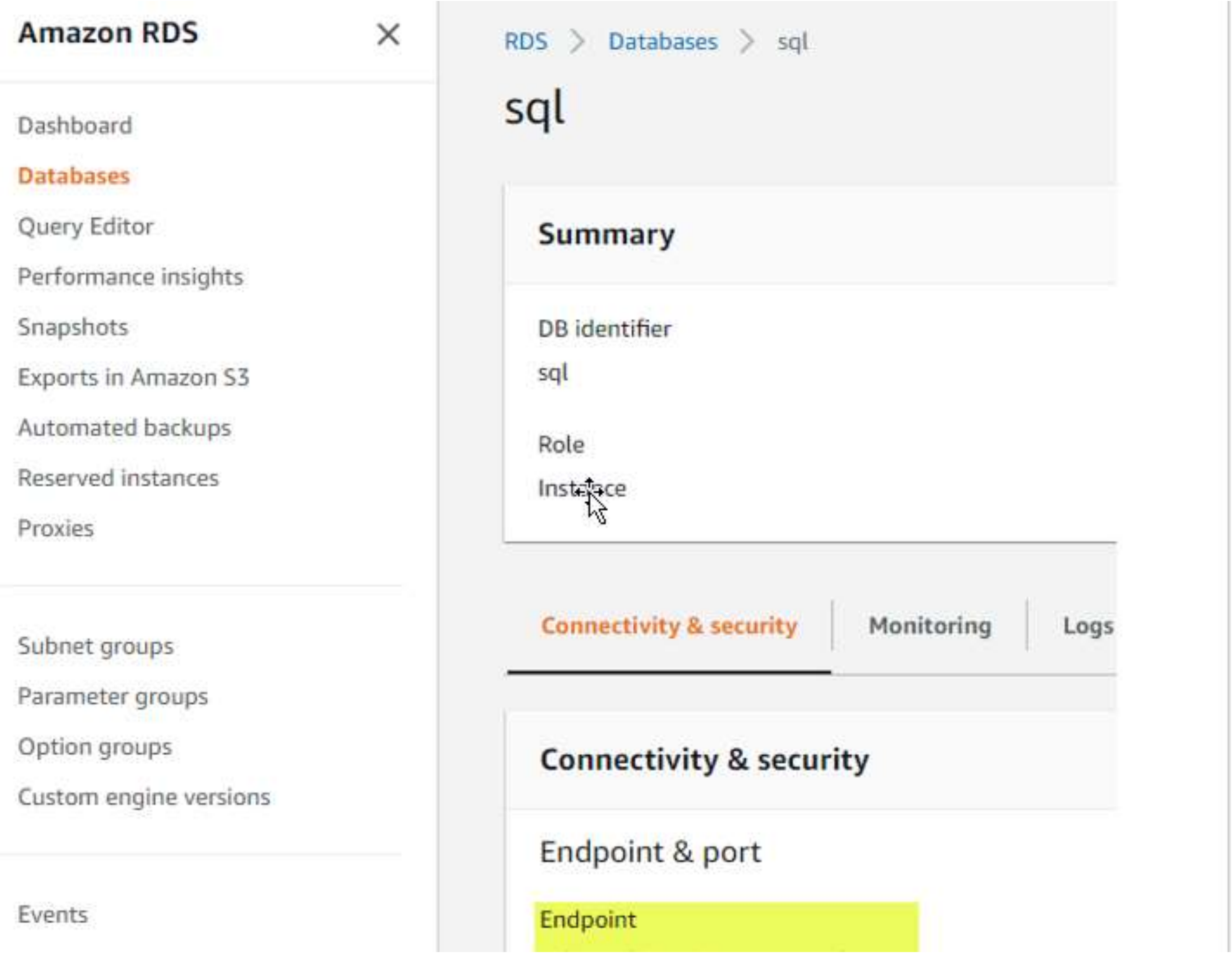
10.5 SMS Configuration smsboot.ini

Edit the settings in the smsboot.ini file as required to connect to:

- SQL server Databases
- SMPP Service provider(s)
- SMTP servers or Office 365 SMTP
- Active Directory if applicable
- The relevant ini file values need to be edited. See below.

```
[From-SMTP-Connector]
From-SMTP-Connector-High-IP-str= nnn.nnn.nnn.nnn
From-SMTP-Connector-High-Port-str=25
From-SMTP-Connector-MaxRecipientsInMsg-int=1000
From-SMTP-Connector-EnableWhiteList-bool=0
From-SMTP-Connector-WhiteList-str=xxx.xxx.xxx.xxx;yyy.yyy.yyy.yyy
From-SMTP-Connector-SystemAlertDomain-str=alert.sms
From-SMTP-Connector-SupportedSmsDomains-str=all.domains
From-SMTP-Connector-SimpleBroadcastDomains-
str=@broadcast(.*)\.sms;@(.*)broadcast\.sms

SMSC-Connector-SMPP-Carriers-
str=SINCH;MessageMedia;Soprano;TIM;OptusProd;OptusDR;Simulator1;Simulator2;Generi
c3.4
SMSC-Connector-SMPP-Production-str=Simulator1  (Enter the SMPP Carrier you are
using from the above certified list)
SMSC-Connector-SMPP-FailOver-str=XXXXX (enter your backup SMPP carrier if you
have a separate contract with another carrier)


SMSC-Connector-XXXXXXX-SMSC-SystemId-str=enter your SMPP account here

SMSC-Connector-XXXXXXX-SMSC-Password-str=enter your password here

SMSC-Connector-XXXXXXX-SMSC-PasswordEncrypted-int=1 (Set this to 1 after you have
supplied the password.  After the services start, the password you entered in
this ini file will be encrypted.  Make sure you close the INI file before
starting services.

To-SMTP-Connector-SenderName-str=SMS Gateway
To-SMTP-Connector-SenderEmail-str= Office 365 SMS Service login email address
To-SMTP-Connector-AdministratorEmail-str=Administrator@domain.com
To-SMTP-Connector-SmtpServerDNSorIP-str=smtp.office365.com
To-SMTP-Connector-SmtpServerPort-int=587
To-SMTP-Connector-SmtpUserName-str=Office 365 SMS Service login email address
To-SMTP-Connector-SmtpPassword-PasswordEncrypted-int=1 (change to 1)
```

```
To-SMTP-Connector-SmtpPassword-str=your password
To-SMTP-Connector-SmtpUseTLSEncryption-int=1
To-SMTP-Connector-MaxAcksToProcess-int=1000
To-SMTP-Connector-MaxConfToProcess-int=1000
To-SMTP-Connector-MaxInboundToProcess-int=1000
To-SMTP-Connector-SubjectPrefix-Ack-str=SMS Conf for:
To-SMTP-Connector-SubjectPrefix-Failed-str=SMS Failed message to:
To-SMTP-Connector-SubjectPrefix-Sent-str=SMS Queued to:
To-SMTP-Connector-SubjectPrefix-Delivered-str=SMS Delivered to:
To-SMTP-Connector-SubjectPrefix-BCast-str=SMS Broadcast request Ref# :
To-SMTP-Connector-SenderName-Inbound-str=[Main_AppCustom1] SMS
To-SMTP-Connector-SenderEmail-Inbound-str=[Main_SMSC_Sender_SMSNo]@outlook.sms
To-SMTP-Connector-SubjectPrefix-Inbound-str=SMS from:



Incoming-Service-DefaultInboundRouteEmail-str=administrator@domain.com
```



DB identifier
sql

Role
Instance

Endpoint

```
[Database]
Database-Prod-SqlServer-str=AWS RDS end point string with ,1433 at the end
Database-Prod-ArchiveSqlServer-str= xxxxxxxxxx
Database-Prod-SqlDB-str=sms-current
Database-Prod-ArchiveDB-str=sms-archive
Database-Prod-AuthType-str=auServer
```

```
Database-Prod-SqlLogin-str=SQL local user for this SMS Server
Database-Prod-PasswordEncrypted-int=1
Database-Prod-SqlPass-str=password for this SQL local user  password will be encrypted when the services start.
Database-Prod-Port-str=1433
```

Email protective marking (refer to BNS technical support).

```
[SQL-API-Database]
SQL-API-Database-SqlServer-str= AWS RDS end point string with ,1433 at the end

SQL-API-Database-SqlDB-str=SMS-SQL-API
SQL-API-Database-AuthType-str=auServer
SQL-API-Database-SqlLogin-str=your service login
SQL-API-Database-PasswordEncrypted-int=1
SQL-API-Database-SqlPass-str=password of the service password will be encrypted when the services start.
SQL-API-Database-Port-str=1433


[From-SQL-LoadBalancer]
SQLI-AnyServer-List-str=SMSServer1:1,SMSServer2:1,SMSServer3:2 (See notes)
SQLI-MyServer-List-str=SMSServer4:1,SMSServer5:1,SMSServer6:1
```

Notes for SQL Load Balancer

1. Keyword ANY Server in the cloud console configuration uses the SQLI-AnyServer-List-str list.
2. Enter your initial server to replace SMSServer1:1 and remove the others in the ANYServer list.
3. Add additional as your deploy them.
4. The :1 in the example above means a weighting for the load balancer. Ie: 1 will be sent to that server, 2 meaning 2 messages will be sent to a server etc in a round robin.
5. This must be set correctly otherwise the server on startup will check the existence of the server

SQLI-MyServer-List-str

1. Administrators can create their own custom server lists to load balance messages to.
2. This applies to SMTP and SQL API.
3. Example: MYServer is like a custom server tag. The tag must be in the format SQLI-TAG-List-str
4. In this example the tag is MYServer.

```
[System-Health]
System-Health-External-AlertTheseEmailAdrsEachCycle-str=address1@domain.com,address2@domain.com
```

- The above email addresses are notified if there is a detected health issue.

```
System-Health-External-SendEmailsOnExceptionOnly-int=1

System-Health-External-AlertTheseMobilesEachCycle-str=611234567890,611234567098
```

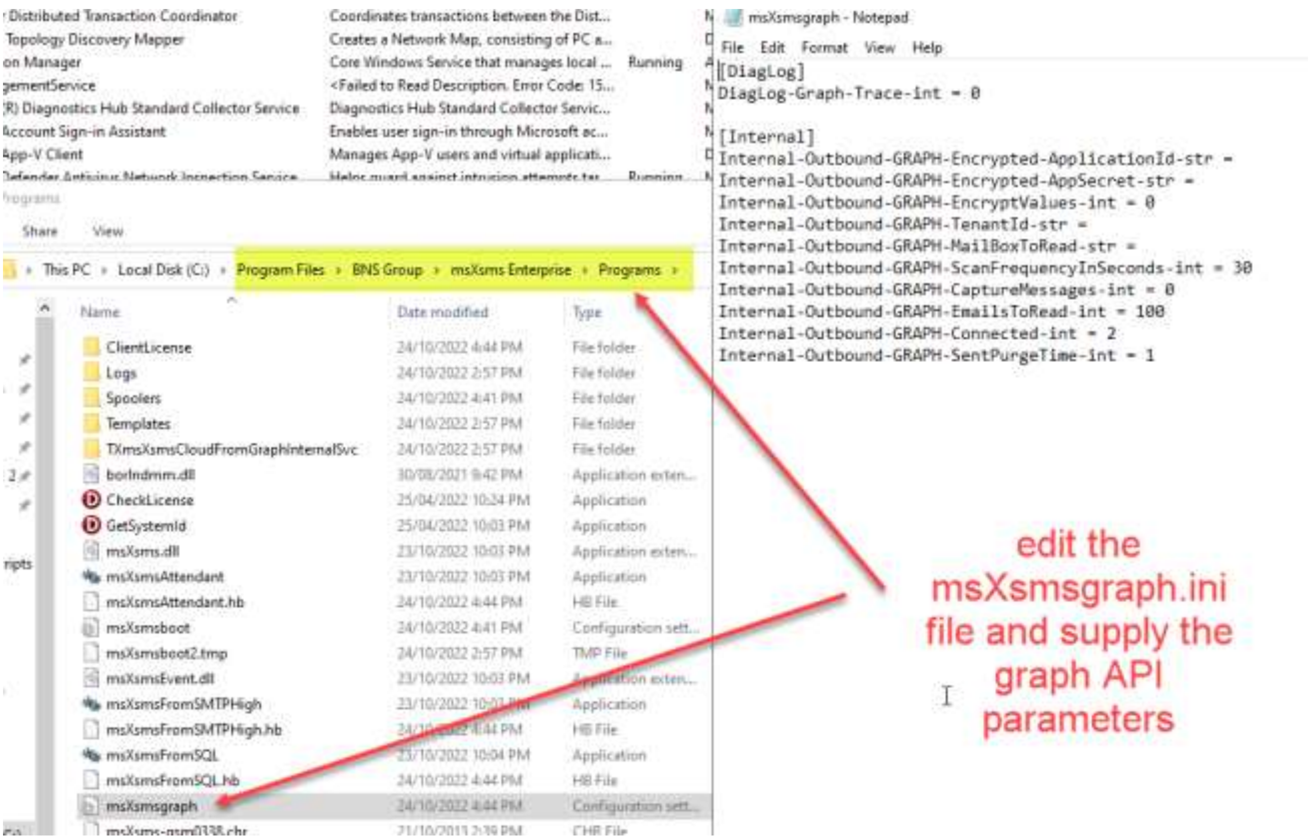
- The above mobile numbers will receive an SMS at a scheduled time.

```
System-Health-MessageMask-str=Health Check from Local Server [Server] at Local Time of [DateTime]
System-Health-ShowLastNCharsInServerName-int=4
System-Health-SendTimes24hr-str=0900,1500,2000
```

- The above times are the defaults for sending a health check SMS

```
System-Health-MaxCycleTimeInMins-int=30
System-Health-Business-Application-SenderEmailAdr-str=HealthCheckerServer1@system.internal
System-Health-SmtpServerDNSorIP-str=smtp.office365.com
System-Health-SmtpServerPort-int=587
System-Health-SmtpUseTLSEncryption-int=1
System-Health-SmtpFromDisplayName-str=msXsms Health Check Service
System-Health-SmtpUserName-str= Office 365 SMS Service login email address
System-Health-SmtpPassword-EncryptPassword-int=1 (Set this to 1)
System-Health-SmtpPassword-str= Office 365 SMS Service password
```

10.6 Graph API Settings



Distributed Transaction Coordinator	Coordinates transactions between the Dist...	
Topology Discovery Mapper	Creates a Network Map, consisting of PC a...	
on Manager	Core Windows Service that manages local ...	Running
gementService	<Failed to Read Description. Error Code: 15...	
(R) Diagnostics Hub Standard Collector Service	Diagnostics Hub Standard Collector Servic...	
Account Sign-in Assistant	Enables user sign-in through Microsoft ac...	
App-V Client	Manages App-V users and virtual applicati...	
Defender Antivirus Network Inspection Service	Helps guard against intrusion attempts tar...	Running

This PC › Local Disk (C:) › Program Files › BNS Group › msXsms Enterprise › Programs ›

Name	Date modified	Type
ClientLicense	24/10/2022 4:44 PM	File folder
Logs	24/10/2022 2:57 PM	File folder
Spoolers	24/10/2022 4:41 PM	File folder
Templates	24/10/2022 2:57 PM	File folder
TXmsXsmsCloudFromGraphInternalSvc	24/10/2022 2:57 PM	File folder
borlndmm.dll	30/08/2021 9:42 PM	Application exten...
CheckLicense	25/04/2022 10:24 PM	Application
GetSystemId	25/04/2022 10:03 PM	Application
msXsms.dll	23/10/2022 10:03 PM	Application exten...
msXsmsAttendant	23/10/2022 10:03 PM	Application
msXsmsAttendant.hb	24/10/2022 4:44 PM	HB File
msXsmsboot	24/10/2022 4:41 PM	Configuration sett...
msXsmsboot2.tmp	24/10/2022 2:57 PM	TMP File
msXsmsEvent.dll	23/10/2022 10:03 PM	Application exten...
msXsmsFromSMTPHigh	23/10/2022 10:03 PM	Application
msXsmsFromSMTPHigh.hb	24/10/2022 4:44 PM	HB File
msXsmsFromSQL	23/10/2022 10:04 PM	Application
msXsmsFromSQL.hb	24/10/2022 4:44 PM	HB File
msXsmsgraph	24/10/2022 4:44 PM	Configuration sett...
msXsms-gsm0338.chr	21/10/2013 2:39 PM	CHR File

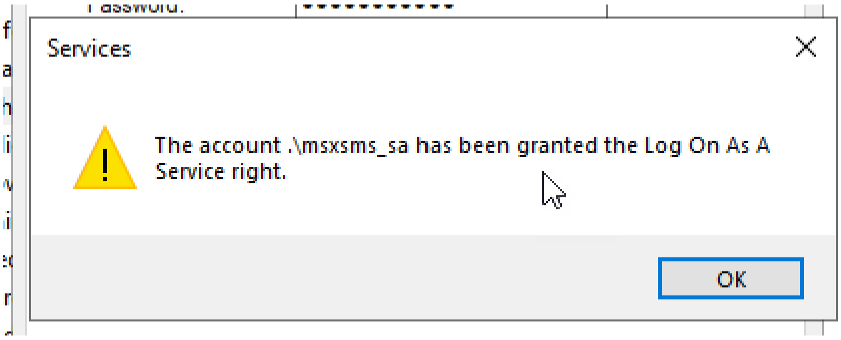
```
[DiagLog]
DiagLog-Graph-Trace-int = 0

[Internal]
Internal-Outbound-GRAPH-Encrypted-ApplicationId-str =
Internal-Outbound-GRAPH-Encrypted-AppSecret-str =
Internal-Outbound-GRAPH-EncryptValues-int = 0
Internal-Outbound-GRAPH-TenantId-str =
Internal-Outbound-GRAPH-MailBoxToRead-str =
Internal-Outbound-GRAPH-ScanFrequencyInSeconds-int = 30
Internal-Outbound-GRAPH-CaptureMessages-int = 0
Internal-Outbound-GRAPH-EmailsToRead-int = 100
Internal-Outbound-GRAPH-Connected-int = 2
Internal-Outbound-GRAPH-SentPurgeTime-int = 1
```

edit the msXsmsgraph.ini file and supply the graph API parameters

- These parameters were created in the previous chapter Exchange Online mailbox.

10.7 Check services

- In service control manager, set the password again to assign logon as service permission for the windows service account

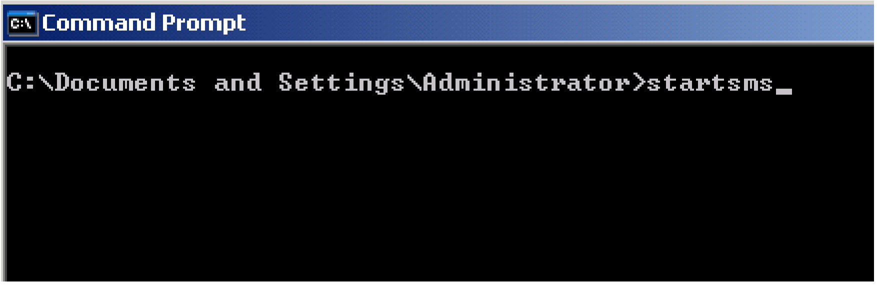


Services

The account .\msxsms_sa has been granted the Log On As A Service right.

ALL services are set to run 'manual' except for the SMS System Attendant Service.

- Some services must be disabled by design, for example:
  - SQL API Services will be disabled on servers which are not eligible in the design to take control over the API databases. Refer to API Control table implementation.
- Other services must be set to MANUAL on production and DR servers except for the msXsms Attendant which is always to be set to Automatic on both production and DR SMS Servers.
- You can start all services by starting just the SMS System Attendant.
- Another method is to Run STARTSMS. This method starts the services quicker.
- STARTSMS can be run from the Windows search option next to the Windows Start button or by launching a CMD window.

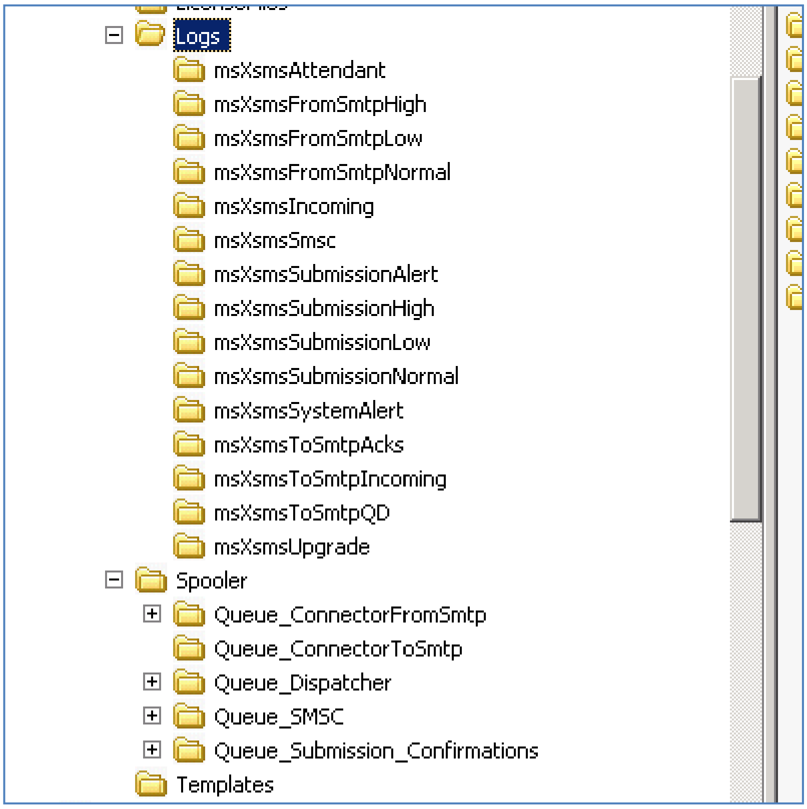


```
C:\Documents and Settings\Administrator>startsms_
```

Stopsms stops all services but for now please make sure all services are running.

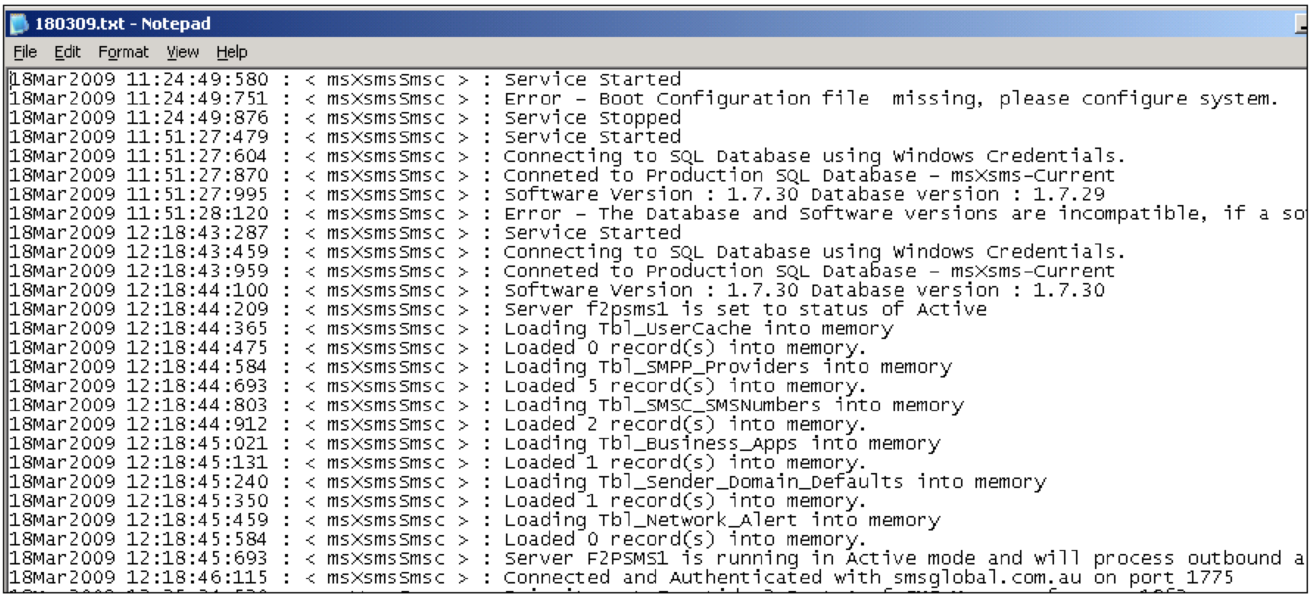
10.8 Check log files for all services

SMS services produces detailed log files which can be found in the following folders.



```
⊟ Logs
    msXsmsAttendant
    msXsmsFromSmtpHigh
    msXsmsFromSmtpLow
    msXsmsFromSmtpNormal
    msXsmsIncoming
    msXsmsSmsc
    msXsmsSubmissionAlert
    msXsmsSubmissionHigh
    msXsmsSubmissionLow
    msXsmsSubmissionNormal
    msXsmsSystemAlert
    msXsmsToSmtpAcks
    msXsmsToSmtpIncoming
    msXsmsToSmtpQD
    msXsmsUpgrade
⊟ Spooler
  ⊞ Queue_ConnectorFromSmtp
    Queue_ConnectorToSmtp
  ⊞ Queue_Dispatcher
  ⊞ Queue_SMSC
  ⊞ Queue_Submission_Confirmations
  Templates
```

Open each log file to see if the services started without any errors and were able to connect to SQL.



```
18Mar2009 11:24:49:580 : < msXsmsSmsc > : Service Started
18Mar2009 11:24:49:751 : < msXsmsSmsc > : Error - Boot Configuration file  missing, please configure system.
18Mar2009 11:24:49:876 : < msXsmsSmsc > : Service Stopped
18Mar2009 11:51:27:479 : < msXsmsSmsc > : Service Started
18Mar2009 11:51:27:604 : < msXsmsSmsc > : Connecting to SQL Database using Windows Credentials.
18Mar2009 11:51:27:870 : < msXsmsSmsc > : Conneted to Production SQL Database - msXsms-Current
18Mar2009 11:51:27:995 : < msXsmsSmsc > : Software Version : 1.7.30 Database version : 1.7.29
18Mar2009 11:51:28:120 : < msXsmsSmsc > : Error - The Database and Software versions are incompatible, if a so
18Mar2009 12:18:43:287 : < msXsmsSmsc > : Service Started
18Mar2009 12:18:43:459 : < msXsmsSmsc > : Connecting to SQL Database using Windows Credentials.
18Mar2009 12:18:43:959 : < msXsmsSmsc > : Conneted to Production SQL Database - msXsms-Current
18Mar2009 12:18:44:100 : < msXsmsSmsc > : Software Version : 1.7.30 Database version : 1.7.30
18Mar2009 12:18:44:209 : < msXsmsSmsc > : Server f2psms1 is set to status of Active
18Mar2009 12:18:44:365 : < msXsmsSmsc > : Loading Tbl_UserCache into memory
18Mar2009 12:18:44:475 : < msXsmsSmsc > : Loaded 0 record(s) into memory.
18Mar2009 12:18:44:584 : < msXsmsSmsc > : Loading Tbl_SMPP_Providers into memory
18Mar2009 12:18:44:693 : < msXsmsSmsc > : Loaded 5 record(s) into memory.
18Mar2009 12:18:44:803 : < msXsmsSmsc > : Loading Tbl_SMSC_SMSNumbers into memory
18Mar2009 12:18:44:912 : < msXsmsSmsc > : Loaded 2 record(s) into memory.
18Mar2009 12:18:45:021 : < msXsmsSmsc > : Loading Tbl_Business_Apps into memory
18Mar2009 12:18:45:131 : < msXsmsSmsc > : Loaded 1 record(s) into memory.
18Mar2009 12:18:45:240 : < msXsmsSmsc > : Loading Tbl_Sender_Domain_Defaults into memory
18Mar2009 12:18:45:350 : < msXsmsSmsc > : Loaded 1 record(s) into memory.
18Mar2009 12:18:45:459 : < msXsmsSmsc > : Loading Tbl_Network_Alert into memory
18Mar2009 12:18:45:584 : < msXsmsSmsc > : Loaded 0 record(s) into memory.
18Mar2009 12:18:45:693 : < msXsmsSmsc > : Server F2PSMS1 is running in Active mode and will process outbound a
18Mar2009 12:18:46:115 : < msXsmsSmsc > : Connected and Authenticated with smsglobal.com.au on port 1775
```

Log file smsSmsc shows the initial startup of the service which created the ini file then stopped.

When the ini file was edited with correct configuration values and the services were subsequently started, connection to SQL failed because version checking of the software versus the database version did not match.

Connection and binding to the SMS Service provider is the final stage of a successful startup in this example log file.

10.8.1 Licensing

To fully license your product, you are required to supply a value called “System ID” to your reseller who in turn obtains a license key for the subscription period eg: 12 months.

The System ID is nothing more than a value generated which is tied to the configuration of your hardware. It does not identify anything about your organization or credentials or any other elements which would breach security. It is only a means of generating a key pair based on your server configuration.

10.9 Anti-virus software

After the software has been installed the following directories must be excluded from being scanned:

Exclude these directories from Real time scanning and scheduled scans

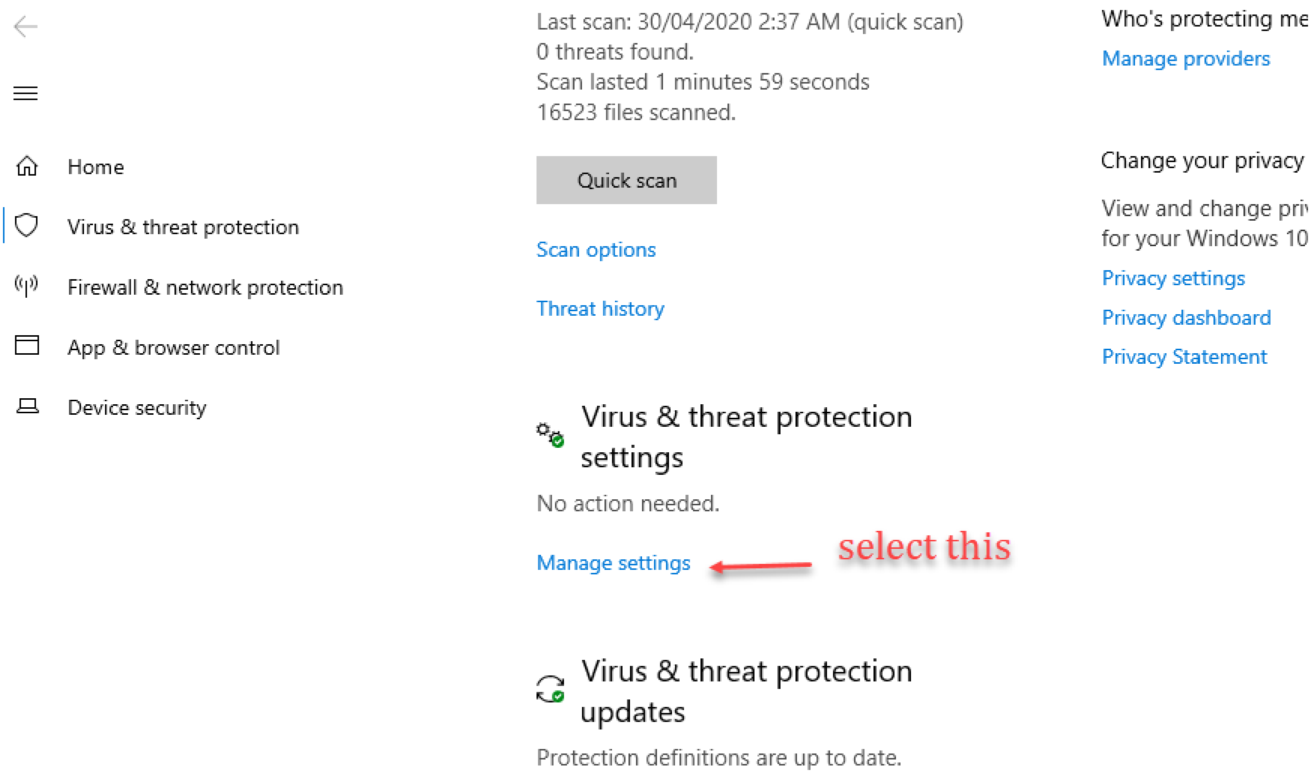
Program files\BNS Group and all sub directories

Program files(x86)\BNS Group and all sub directories

10.9.1 Windows Server Windows Defender

For performance reasons it is recommended to exclude the BNS Group folder from being scanned for threat protection.

- Settings
- Update and Security
- Windows Security
- Virus & threat protection



Last scan: 30/04/2020 2:37 AM (quick scan)
0 threats found.
Scan lasted 1 minutes 59 seconds
16523 files scanned.

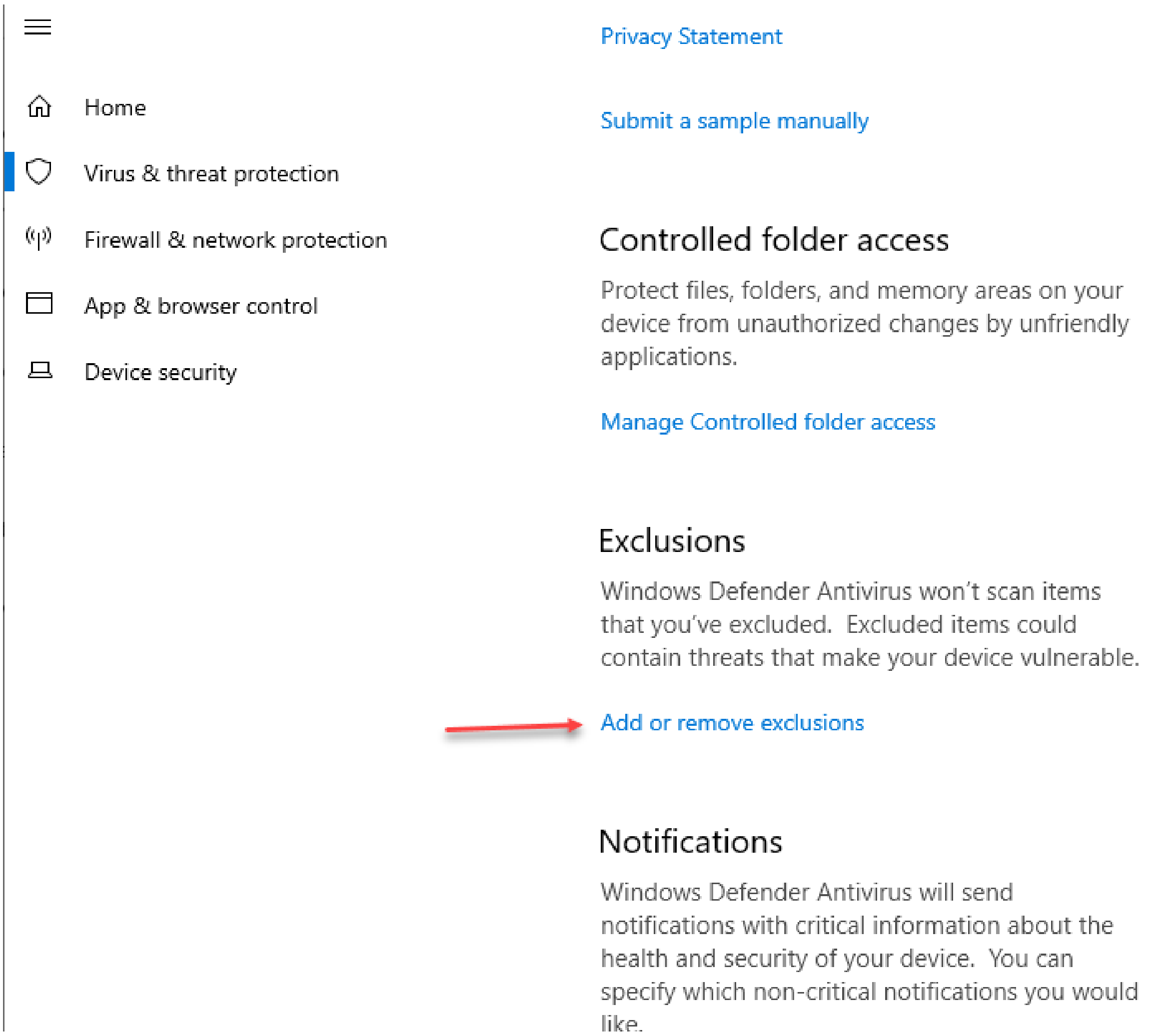
Virus & threat protection settings

No action needed.

Virus & threat protection updates

Protection definitions are up to date.

View and change pri
for your Windows 10



Privacy Statement

Submit a sample manually

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Manage Controlled folder access

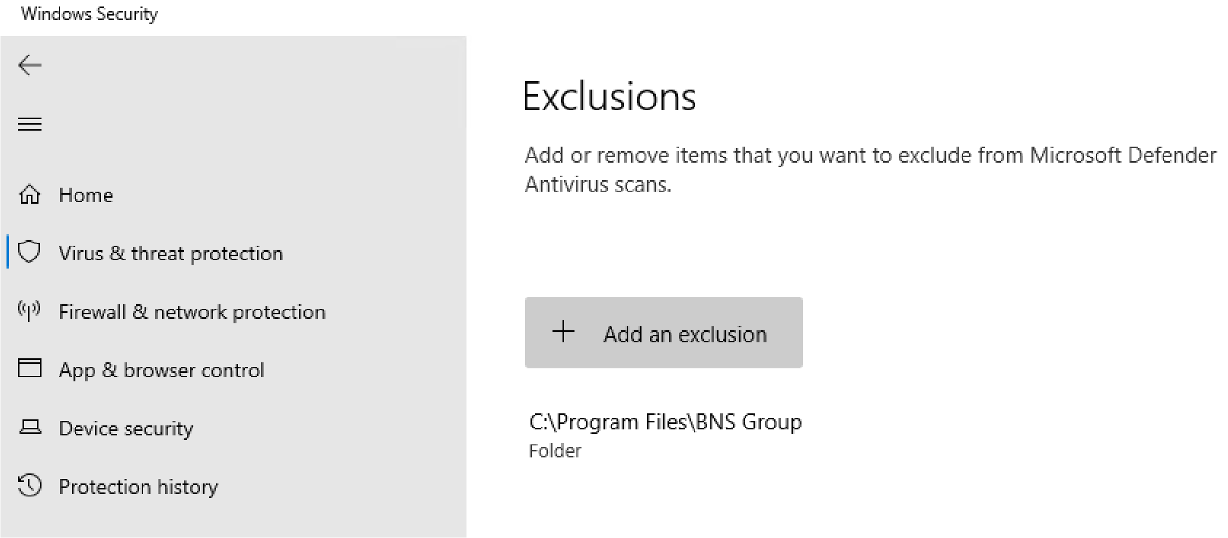
Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

Add or remove exclusions

Notifications

Windows Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.



Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

C:\Program Files\BNS Group
Folder

Adding the BNS Group root folder will exclude sub folders will prevent Defender consuming excessive CPU on a busy system.

SECTION 11 Data Analytics

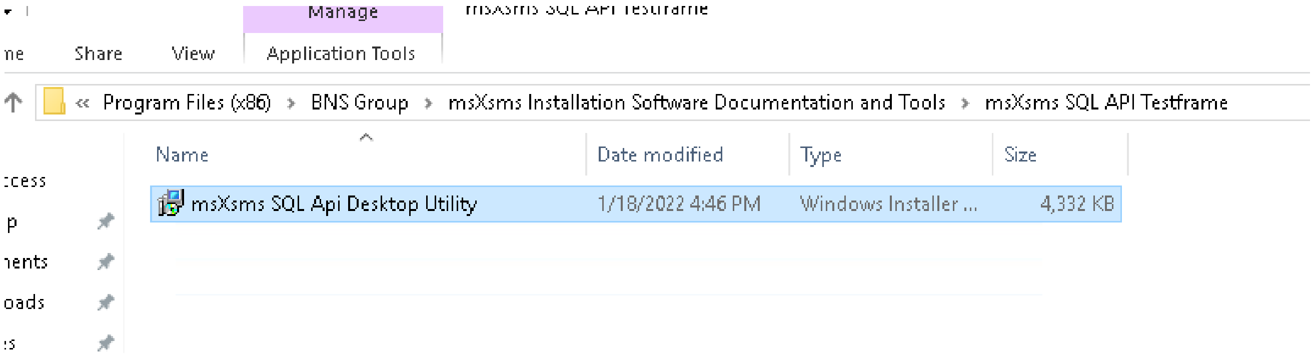
11.1 Available in 2023

To be documented.

SECTION 12 Test tool – SMS SQL API Desktop utility

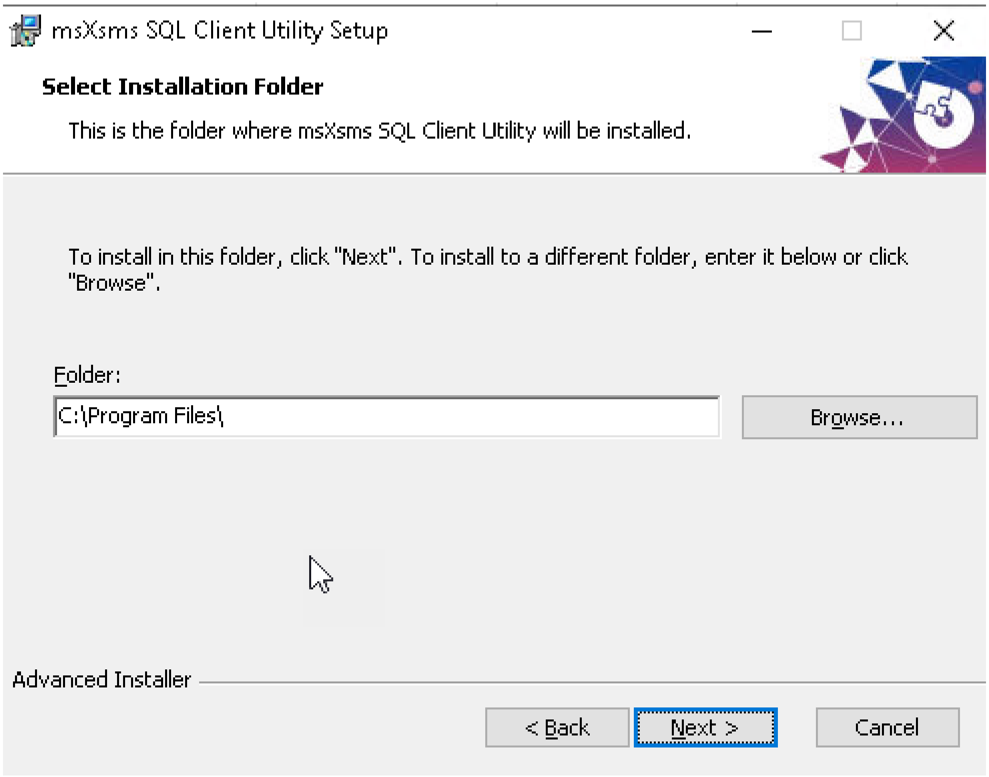
12.1 Installing the test tool

From the installation folders. Run the setup.



Manage
msXsms SQL API Testframe
ne
Share
View
Application Tools
« Program Files (x86) › BNS Group › msXsms Installation Software Documentation and Tools › msXsms SQL API Testframe
ccess
p
nents
oads
s

Name	Date modified	Type	Size
msXsms SQL Api Desktop Utility	1/18/2022 4:46 PM	Windows Installer ...	4,332 KB



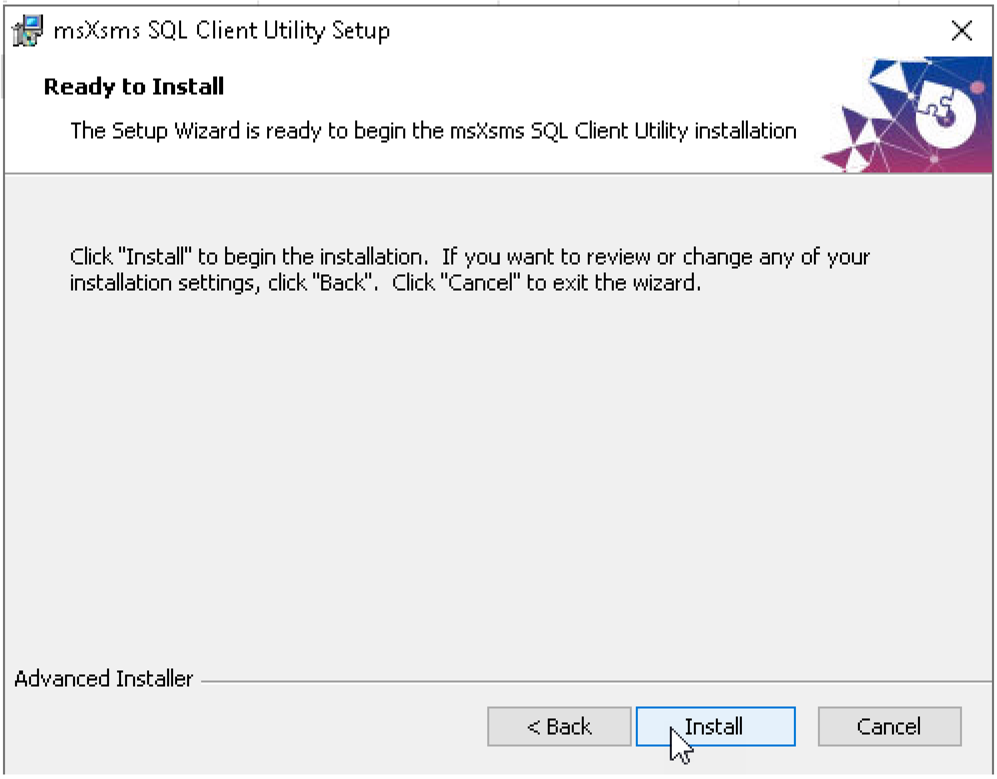
msXsms SQL Client Utility Setup

Select Installation Folder

This is the folder where msXsms SQL Client Utility will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\

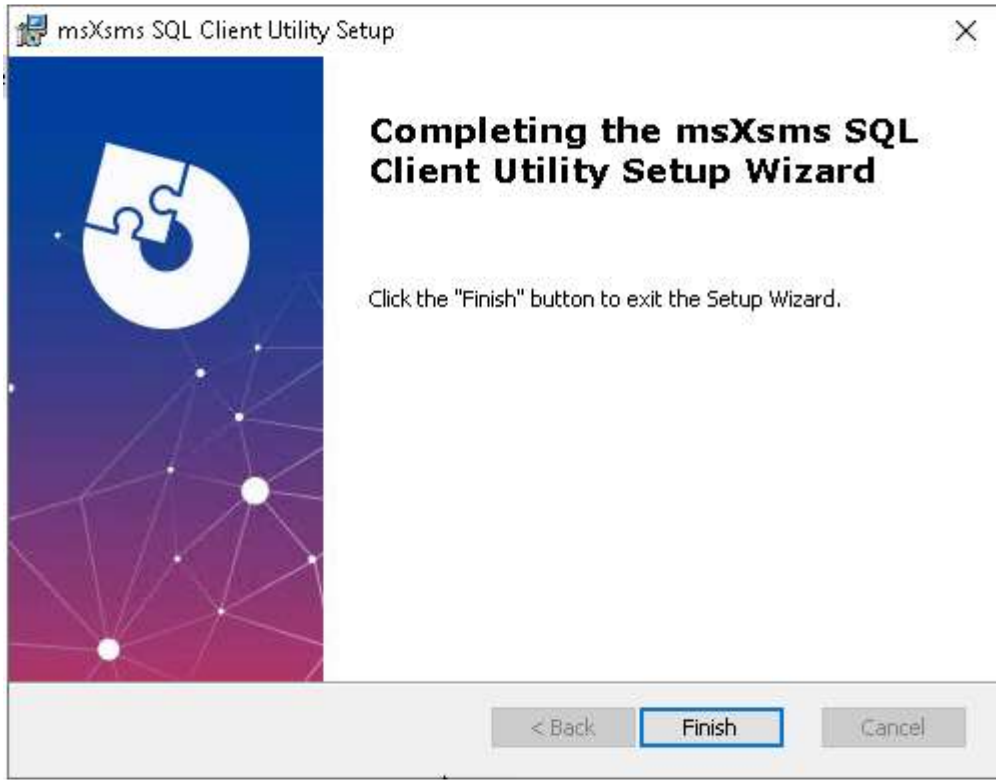


msXsms SQL Client Utility Setup

Ready to Install

The Setup Wizard is ready to begin the msXsms SQL Client Utility installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.



msXsms SQL Client Utility Setup

Completing the msXsms SQL Client Utility Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

12.2 Configuring the test tool

KB article required for test tool >

SECTION 13 Health Service

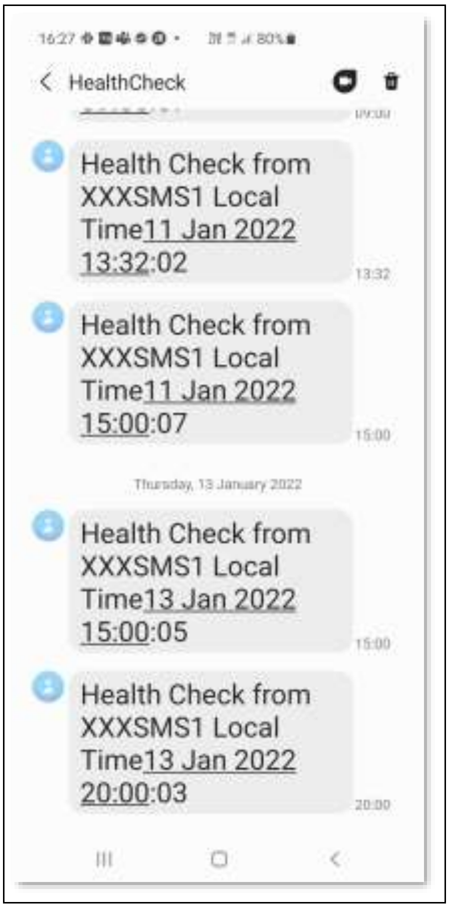
13.1 What is the Health Service?

The health service is a Windows Service running on each SMS Server. The service sends test SMS messages to a configured set of mobile numbers at times defined by the system administrator.

For example, a system engineer and\or platform owner can receive multiple SMS messages from that server during the day to prove that end to end connectivity is fully operational.

A platform owner would expect an SMS from the servers at say 9am in the morning and 3pm in the afternoon. If the SMS messages do not arrive that will be an indication that something is not operational either within the customer's network or the service provider or the mobile telecommunications network.

Example phone SMS messages. Some customers do not allow full server names to be exposed on public networks. **Eg: Federal Government. That is configurable**.



Health Check from XXXSMS1 Local Time11 Jan 2022 13:32:02 13:32

Health Check from XXXSMS1 Local Time11 Jan 2022 15:00:07 15:00

Thursday, 13 January 2022

Health Check from XXXSMS1 Local Time13 Jan 2022 15:00:05 15:00

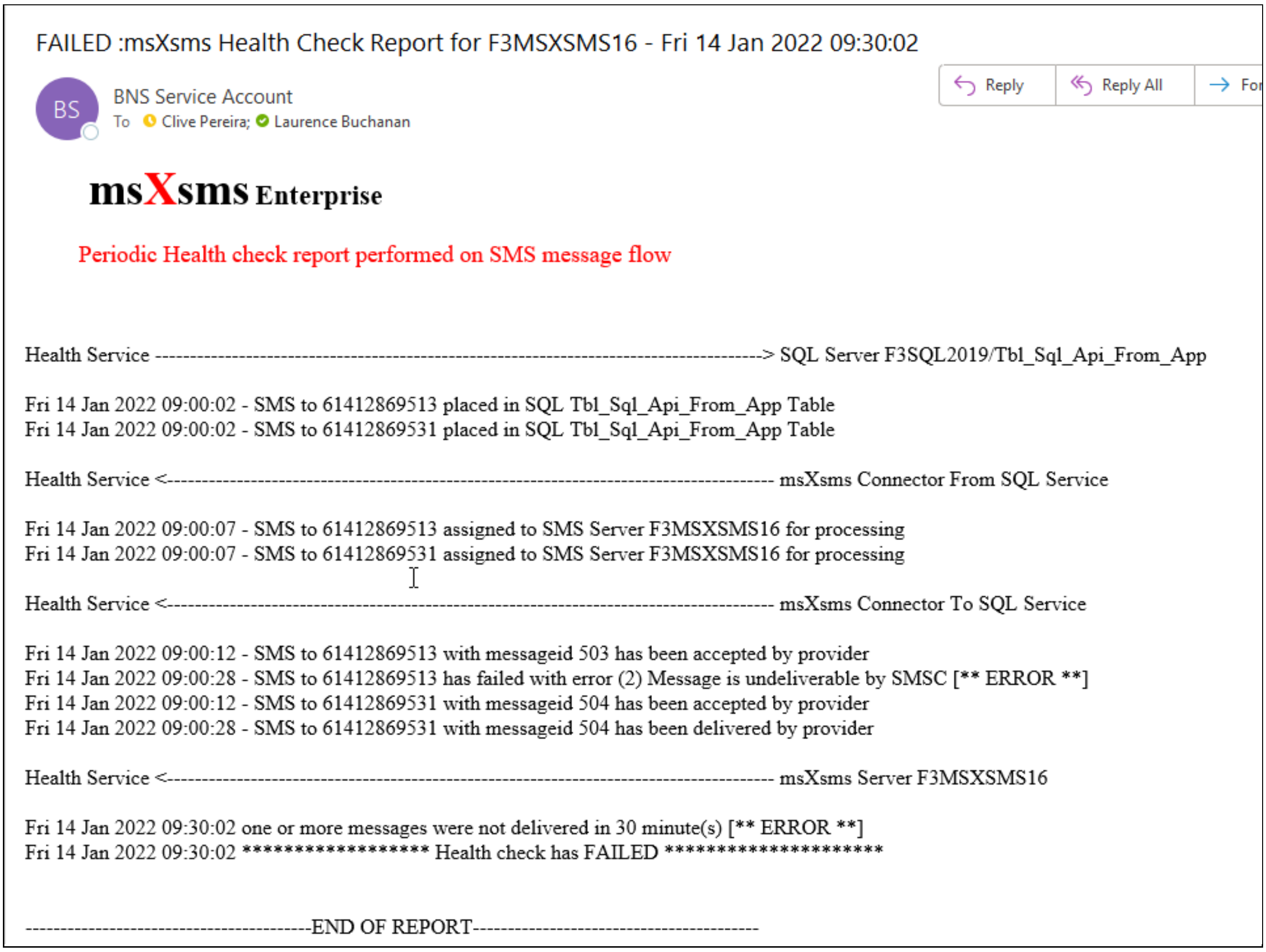
Health Check from XXXSMS1 Local Time13 Jan 2022 20:00:03 20:00

13.2 System alerts

In addition to the health service, the system will send email alerts to a nominated email address if it detects warnings or errors.

The health service can detect a SMS message flow problem and report it via email to the nominated system administrator email address.

Example email message from the Health service to the system administrator showing that SMS message flow issues were detected.



FAILED :msXsms Health Check Report for F3MSXSMS16 - Fri 14 Jan 2022 09:30:02

BS BNS Service Account
To Clive Pereira; Laurence Buchanan

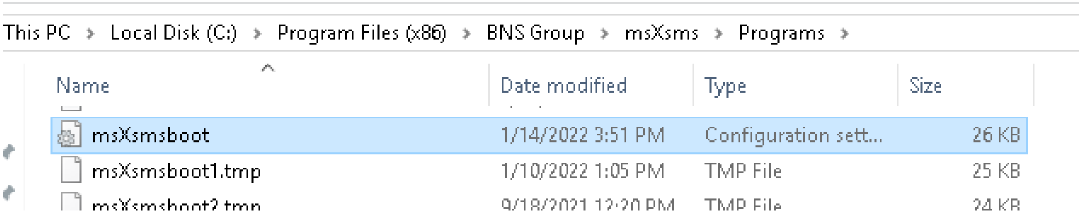
msXsms Enterprise

Periodic Health check report performed on SMS message flow

```
Health Service ------------------------------------------------------------------------------------> SQL Server F3SQL2019/Tbl_Sql_Api_From_App

Fri 14 Jan 2022 09:00:02 - SMS to 61412869513 placed in SQL Tbl_Sql_Api_From_App Table
Fri 14 Jan 2022 09:00:02 - SMS to 61412869531 placed in SQL Tbl_Sql_Api_From_App Table

Health Service <------------------------------------------------------------------------------------ msXsms Connector From SQL Service

Fri 14 Jan 2022 09:00:07 - SMS to 61412869513 assigned to SMS Server F3MSXSMS16 for processing
Fri 14 Jan 2022 09:00:07 - SMS to 61412869531 assigned to SMS Server F3MSXSMS16 for processing

Health Service <------------------------------------------------------------------------------------ msXsms Connector To SQL Service

Fri 14 Jan 2022 09:00:12 - SMS to 61412869513 with messageid 503 has been accepted by provider
Fri 14 Jan 2022 09:00:28 - SMS to 61412869513 has failed with error (2) Message is undeliverable by SMSC [** ERROR **]
Fri 14 Jan 2022 09:00:12 - SMS to 61412869531 with messageid 504 has been accepted by provider
Fri 14 Jan 2022 09:00:28 - SMS to 61412869531 with messageid 504 has been delivered by provider

Health Service <------------------------------------------------------------------------------------ msXsms Server F3MSXSMS16

Fri 14 Jan 2022 09:30:02 one or more messages were not delivered in 30 minute(s) [** ERROR **]
Fri 14 Jan 2022 09:30:02 ****************** Health check has FAILED ********************


-----------------------------------------END OF REPORT-----------------------------------------
```

13.3 Configuring the Health Service

Configuration of the Health service is in the smsboot.ini file in the programs folder.



This PC › Local Disk (C:) › Program Files (x86) › BNS Group › msXsms › Programs ›

Name	Date modified	Type	Size
msXsmsboot	1/14/2022 3:51 PM	Configuration sett...	26 KB
msXsmsboot1.tmp	1/10/2022 1:05 PM	TMP File	25 KB
msXsmsboot2.tmp	9/18/2021 12:20 PM	TMP File	24 KB

The ini file contains the parameters for the Health service to function

```
[System-Health]

System-Health-External-AlertTheseEmailAdrsEachCycle-str=emailaddress1,emailaddress2

System-Health-External-SendEmailsOnExceptionOnly-int=1

System-Health-External-AlertTheseMobilesEachCycle-str=61412nnnnnn,61412nnnnnn

System-Health-MessageMask-str=Health Check from [Server] Local Time[DateTime]

System-Health-ShowLastNCharsInServerName-int=4

System-Health-SendTimes24hr-str=0900,1500,2000

System-Health-MaxCycleTimeInMins-int=30

System-Health-Business-Application-SenderEmailAdr-str=HealthCheckerServer<ServerName>@system.internal

System-Health-SmtpServerDNSorIP-str=smtp.office365.com

System-Health-SmtpServerPort-int=587

System-Health-SmtpUseTLSEncryption-int=1

System-Health-SmtpFromDisplayName-str=msXsms Health Check Service

System-Health-SmtpUserName-str=<customer’s smtp user email address used for the service to send emails. Eg: SMSServiceAccount@xxxxxxxxxxxxxx >

System-Health-SmtpPassword-EncryptPassword-int=0

System-Health-SmtpPassword-str=C2A96FC2B06AC2ADC288C2ABC2906F7BC2A6C29CC28A7B7BC28C7D717E7E

System-Health-SyslogPort-int=514
```

Configure the ini file

- nominate the email addresses to receive error reports in relation to health.
- Nominate the mobile numbers to receive health check SMS messages each day.
- Create a business application entry for the health service for each SMS Server. **HealthCheckerServer<ServerName>@system.internal.** Set the name in the ini file to match the entry you made in the business applications section of the SMS cloud console. All administration functions through the SMS console are documented in https://smskb.bnsgroup.com.au/console
- when setting the initial password for the SMTP email user account used to send emails, set System-Health-SmtpPassword-EncryptPassword-int=1
- Set the value of the password in System-Health-SmtpPassword-str then save and close the ini file. Stop SMS services using an elevated CMD window command STOPSMS
- Then run STARTSMS from the same CMD window. After all services are started, the password in the smsboot.ini file should then be encrypted.
-

SECTION 14 Configuring other services

14.1 Simple broadcast

Simple broadcast is currently restricted to SMTP based submissions using internal email servers sending on port 25.

- Simple broadcast requires the following services to be enabled on the SMS Server:
  - sms from SMTP service
  - sms submission services

Refer to the simple broadcast admin guide - [> Simple Broadcast Admin Guide (bnsgroup.com.au)]

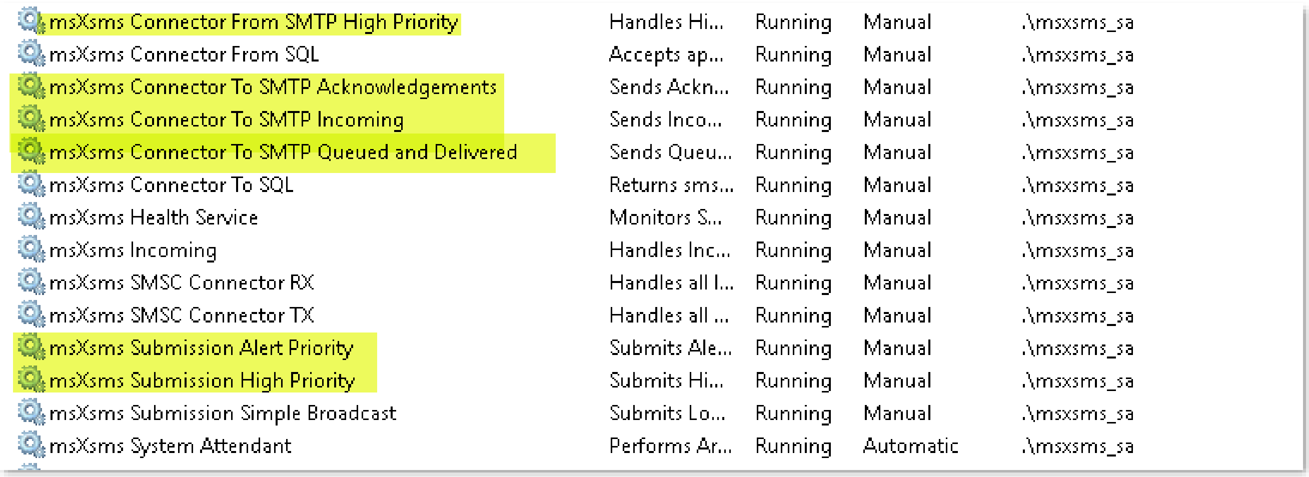
Refer to the simple broadcast end user guide – [> Send Simple SMS Broadcast from Outlook (bnsgroup.com.au)]

14.2 SMS Submissions using SMTP

SMTP to SMS is currently restricted to internal email servers sending on port 25.

By default, some of the services supporting SMTP are set to disabled.

To activate all of the required services to support SMTP ensure that all of the services are set to manual from disabled



msXsms Connector From SMTP High Priority	Handles Hi...	Running	Manual	.\msxsms_sa
msXsms Connector From SQL	Accepts ap...	Running	Manual	.\msxsms_sa
msXsms Connector To SMTP Acknowledgements	Sends Ackn...	Running	Manual	.\msxsms_sa
msXsms Connector To SMTP Incoming	Sends Inco...	Running	Manual	.\msxsms_sa
msXsms Connector To SMTP Queued and Delivered	Sends Queu...	Running	Manual	.\msxsms_sa
msXsms Connector To SQL	Returns sms...	Running	Manual	.\msxsms_sa
msXsms Health Service	Monitors S...	Running	Manual	.\msxsms_sa
msXsms Incoming	Handles Inc...	Running	Manual	.\msxsms_sa
msXsms SMSC Connector RX	Handles all I...	Running	Manual	.\msxsms_sa
msXsms SMSC Connector TX	Handles all ...	Running	Manual	.\msxsms_sa
msXsms Submission Alert Priority	Submits Ale...	Running	Manual	.\msxsms_sa
msXsms Submission High Priority	Submits Hi...	Running	Manual	.\msxsms_sa
msXsms Submission Simple Broadcast	Submits Lo...	Running	Manual	.\msxsms_sa
msXsms System Attendant	Performs Ar...	Running	Automatic	.\msxsms_sa

Previous versions of BNS's SMS Enterprise SMS server software had 3 SMTP priorities: Low Normal and High.

BNS changed this in version 2.0 of the software because SQL interfaces will be used mainly for applications in the future.

In Version 2.0 there are 2 x FROM SMTP services and 2 x Submission Services.

One is designated as HIGH priority and the other as NORMAL priority. SMTP priority allows messages to traverse the Exchange server system as quick as possible for SMTP based applications based on the destination address space eg: number@high.sms and number@normal.sms

All SMS transmission priorities are now controlled in the Applications & Users section of the SMS console.

BNS may implement its GRAPH API support into the platform allowing Exchange online transport rules to route SMS traffic via a mailbox. This is only to be used for low volumes. All high volumes are to use SQL as the main interface.

14.2.1 Exchange on-premises transport role servers

Customers with Exchange on-premises transport role servers can continue to use private domain addressing with the .SMS extension.

Eg: POLICY_RENEWALS.SMS

14.2.1.1 smsboot.ini file listen on port 25

The IP address of this server needs to be defined in the smsboot.ini file and firewall rules on the Windows Server need to allow connections on port 25.

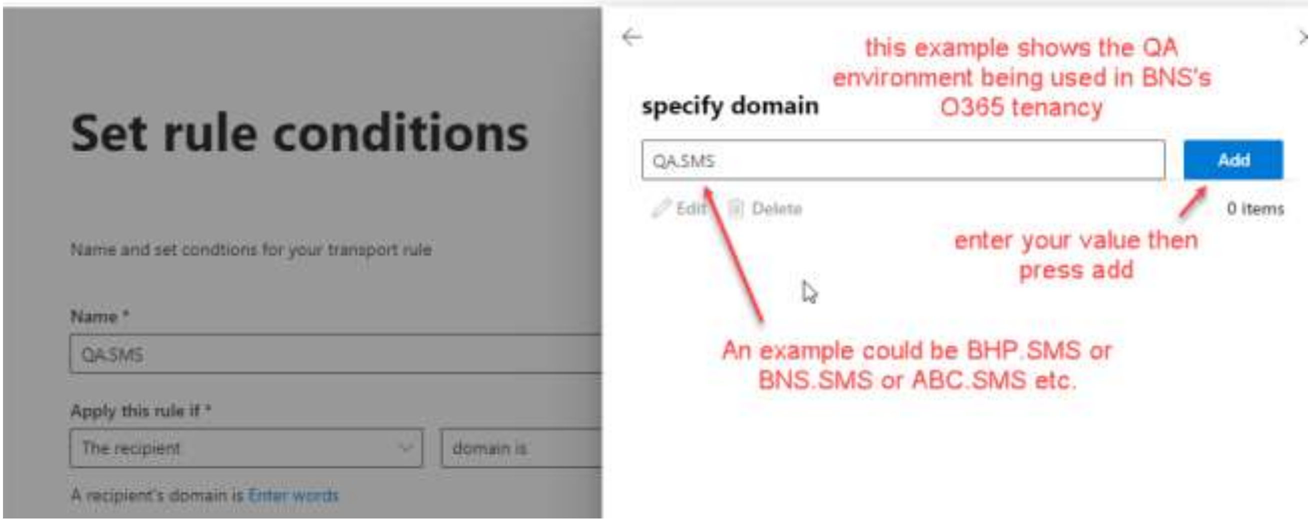
INI File parameters

```
[From-SMTP-Connector]
From-SMTP-Connector-High-IP-str=nnn.nnn.nnn.nnn
From-SMTP-Connector-High-Port-str=25
```

14.2.2 Exchange Online transport rules

Exchange Online transport rules can be used to re-direct outbound SMS requests to a mailbox for processing by the SMS Server.

How to create a new transport rule in Exchange Online



Set rule conditions

Name and set condtions for your transport rule

Name *: QA.SMS

Apply this rule if *: The recipient | domain is

A recipient's domain is Enter words

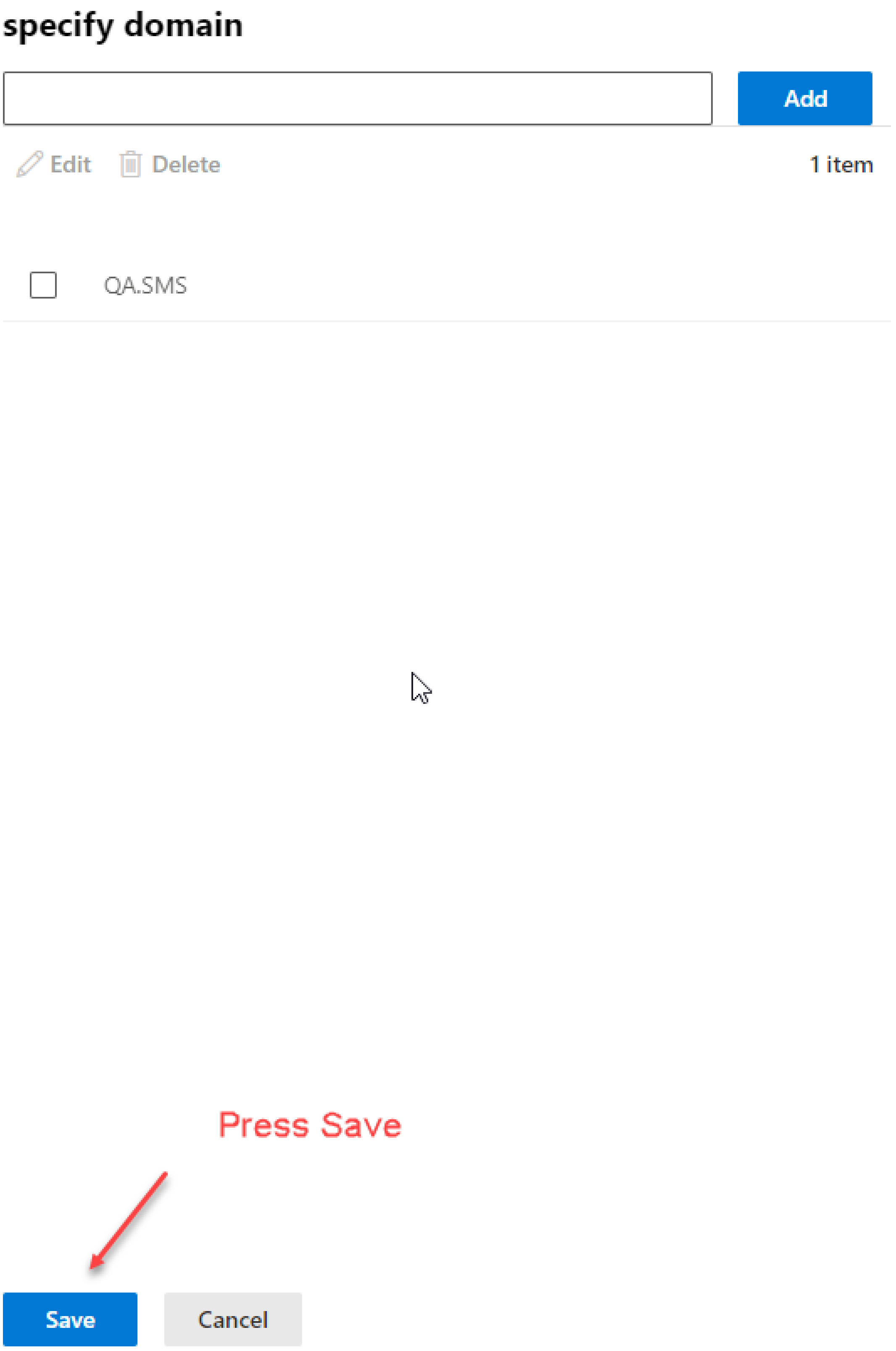
specify domain

QA.SMS

this example shows the QA environment being used in BNS's O365 tenancy

enter your value then press add

An example could be BHP.SMS or BNS.SMS or ABC.SMS etc.

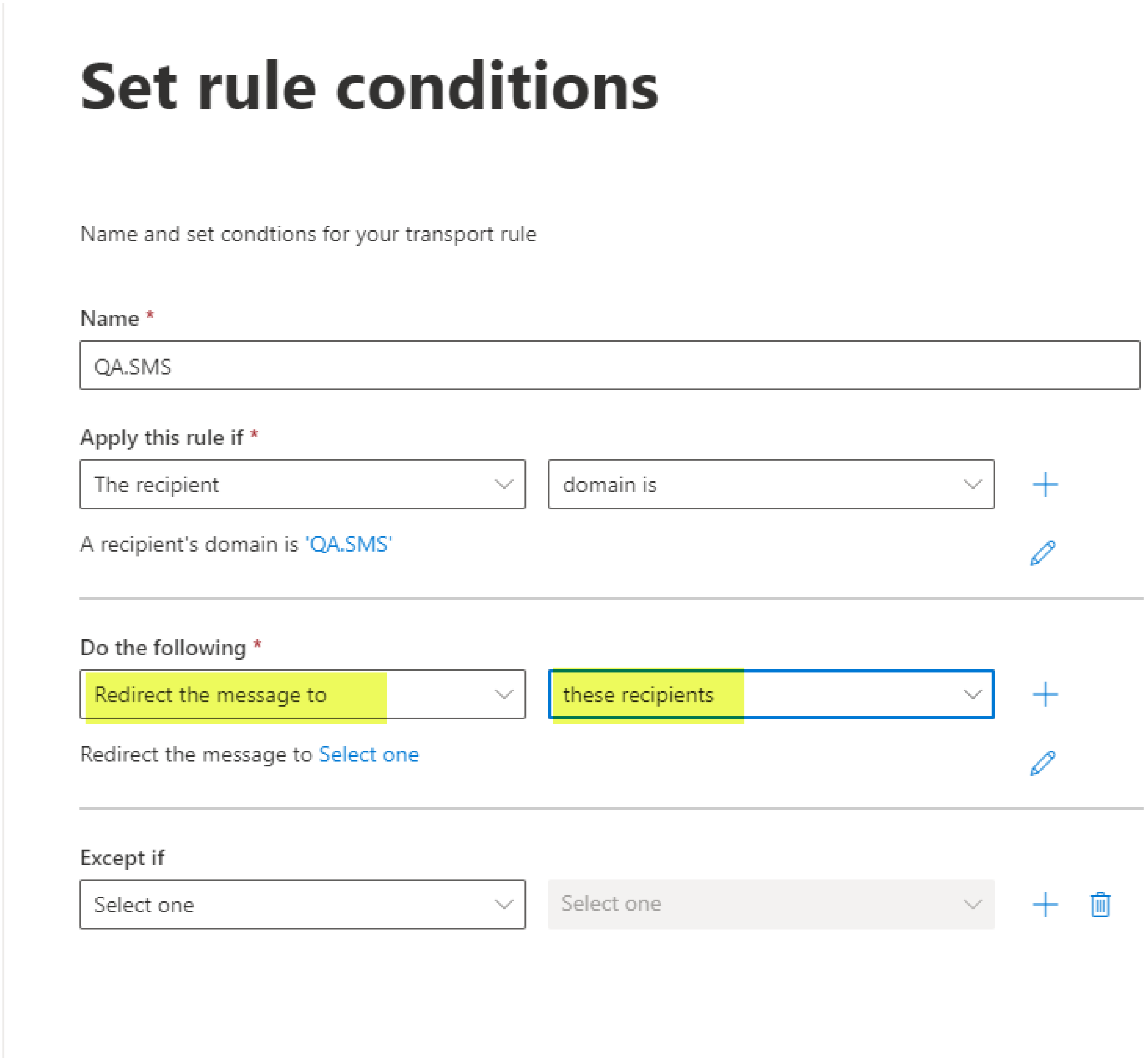


specify domain

☐ QA.SMS

1 item

Press Save



Set rule conditions

Name and set condtions for your transport rule

Name *

QA.SMS

Apply this rule if *

The recipient | domain is

A recipient's domain is 'QA.SMS'

Do the following *

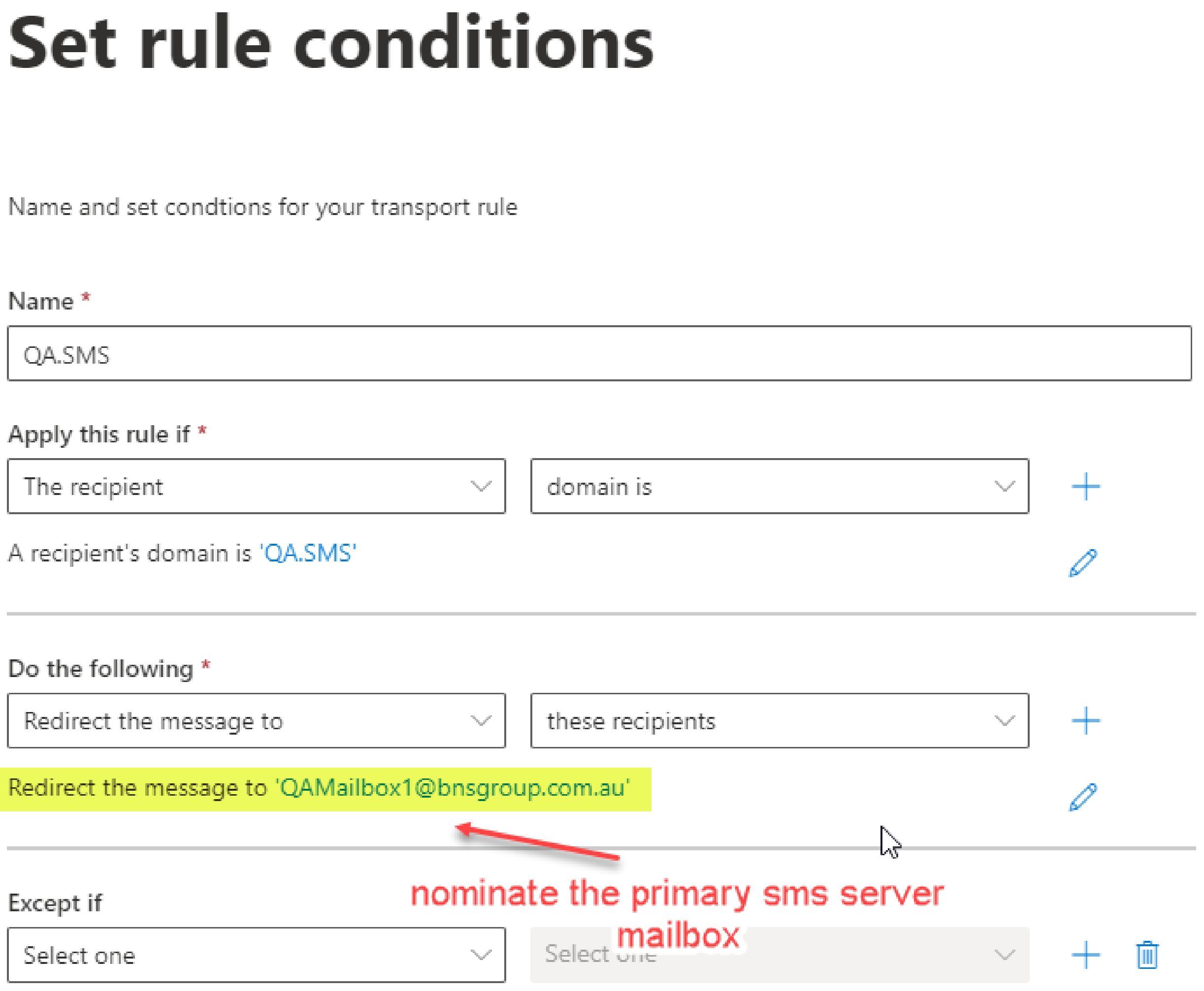
Redirect the message to | these recipients

Redirect the message to Select one

Except if

Select one | Select one

Select the mailbox of the primary active SMS server



Set rule conditions

Name and set condtions for your transport rule

Name *

QA.SMS

Apply this rule if *

The recipient | domain is

A recipient's domain is 'QA.SMS'

Do the following *

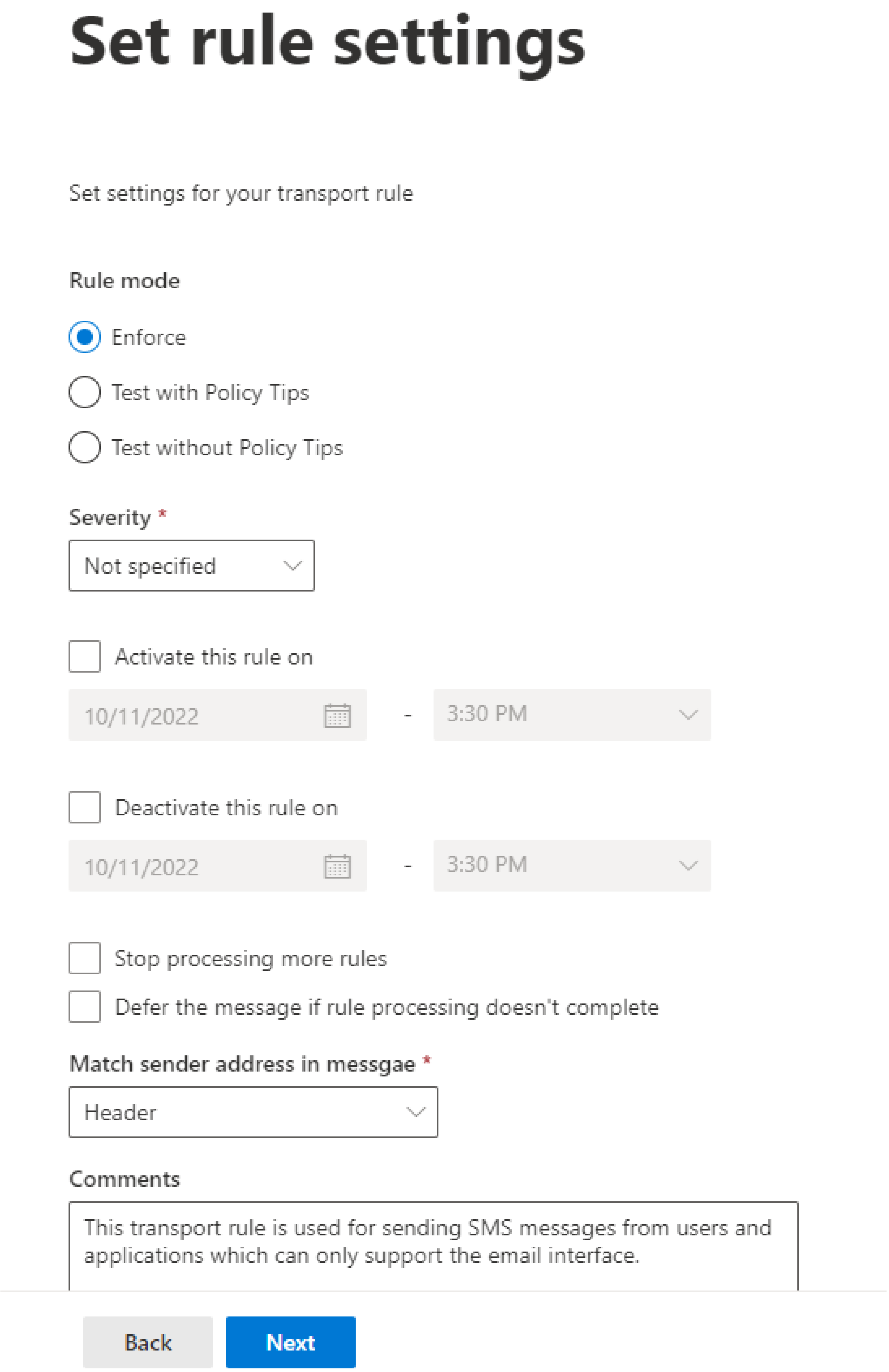
Redirect the message to | these recipients

Redirect the message to 'QAMailbox1@bnsgroup.com.au'

nominate the primary sms server mailbox

Except if

Select one | Select one



Set rule settings

Set settings for your transport rule

Rule mode

● Enforce

○ Test with Policy Tips

○ Test without Policy Tips

Severity *

Not specified

□ Activate this rule on

10/11/2022 - 3:30 PM

□ Deactivate this rule on

10/11/2022 - 3:30 PM

□ Stop processing more rules

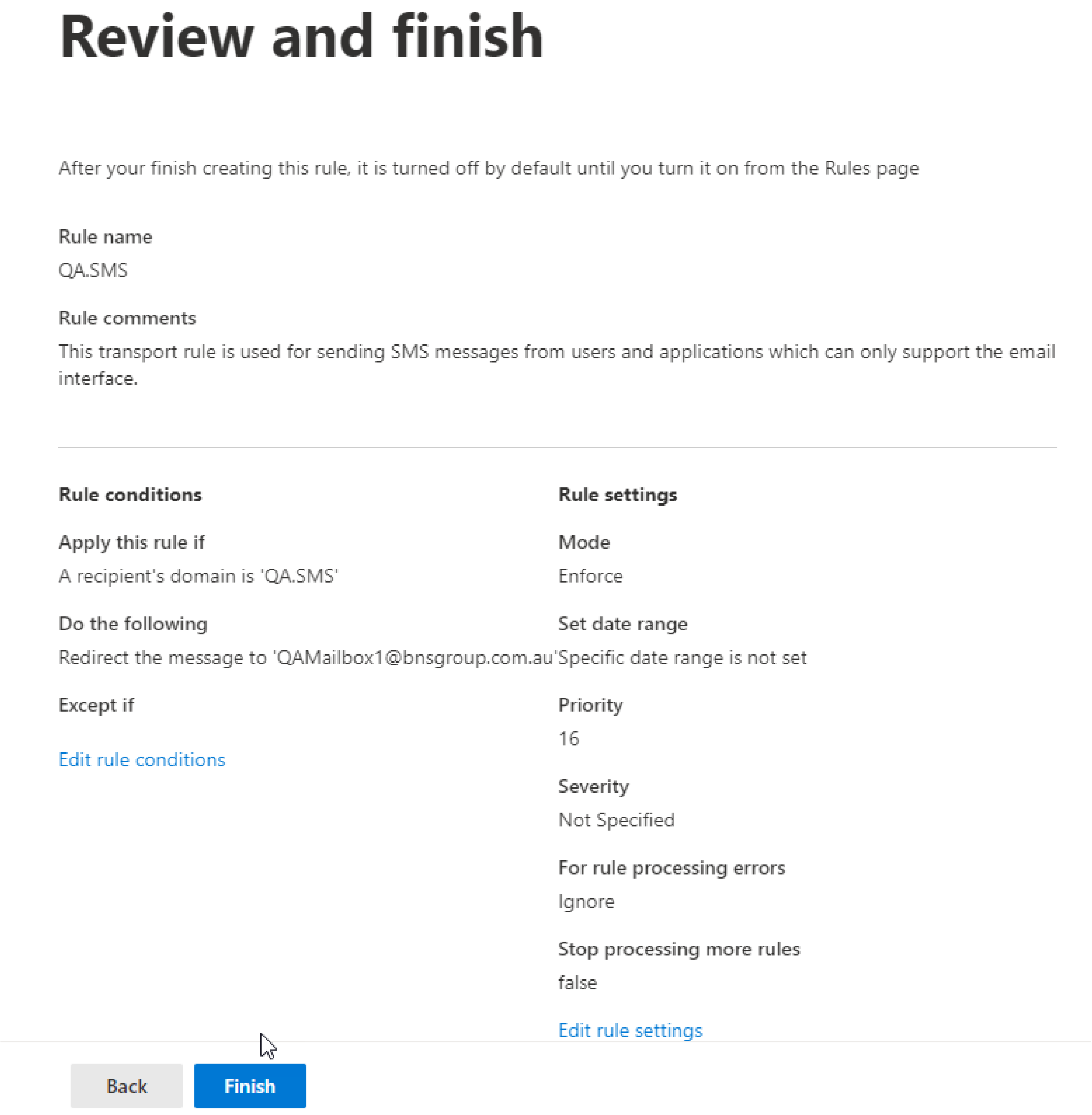
□ Defer the message if rule processing doesn't complete

Match sender address in messgae *

Header

Comments

This transport rule is used for sending SMS messages from users and applications which can only support the email interface.



Review and finish

After your finish creating this rule, it is turned off by default until you turn it on from the Rules page

Rule name

QA.SMS

Rule comments

This transport rule is used for sending SMS messages from users and applications which can only support the email interface.

Rule conditions

Apply this rule if

A recipient's domain is 'QA.SMS'

Do the following

Redirect the message to 'QAMailbox1@bnsgroup.com.au'

Except if

Edit rule conditions

Rule settings

Mode

Enforce

Set date range

Specific date range is not set

Priority

16

Severity

Not Specified

For rule processing errors

Ignore

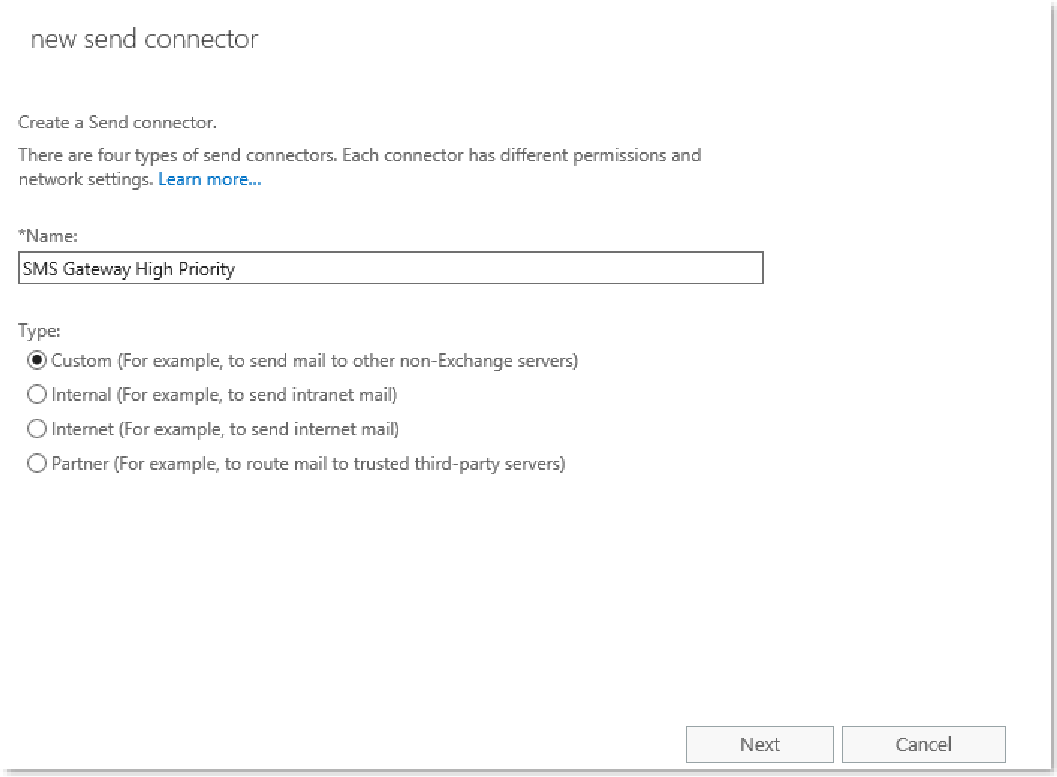
Stop processing more rules

false

Edit rule settings

14.2.3 On-premises Exchange SMTP Connector example

- Open the Exchange Admin Center.
- Navigate to Mail Flow, Send Connectors
- Select New Send Connector



new send connector

Create a Send connector.

There are four types of send connectors. Each connector has different permissions and network settings. Learn more...

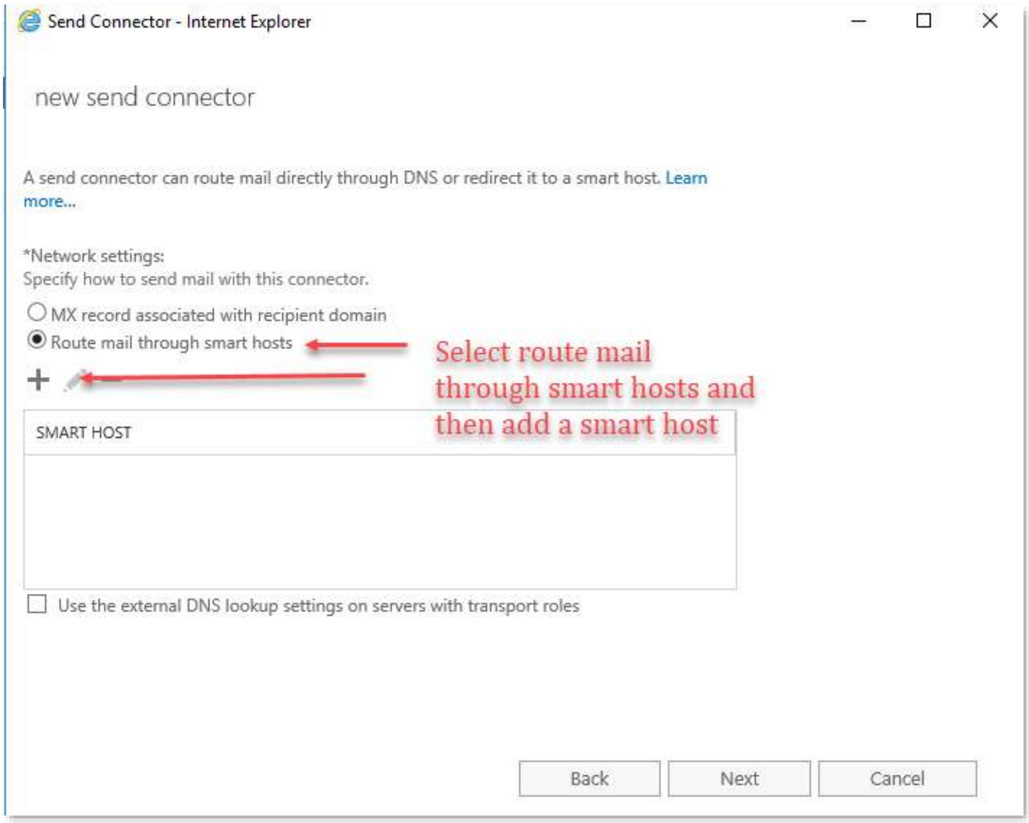
*Name:

SMS Gateway High Priority

Type:

● Custom (For example, to send mail to other non-Exchange servers)
○ Internal (For example, to send intranet mail)
○ Internet (For example, to send internet mail)
○ Partner (For example, to route mail to trusted third-party servers)

- Press Next



new send connector

A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...

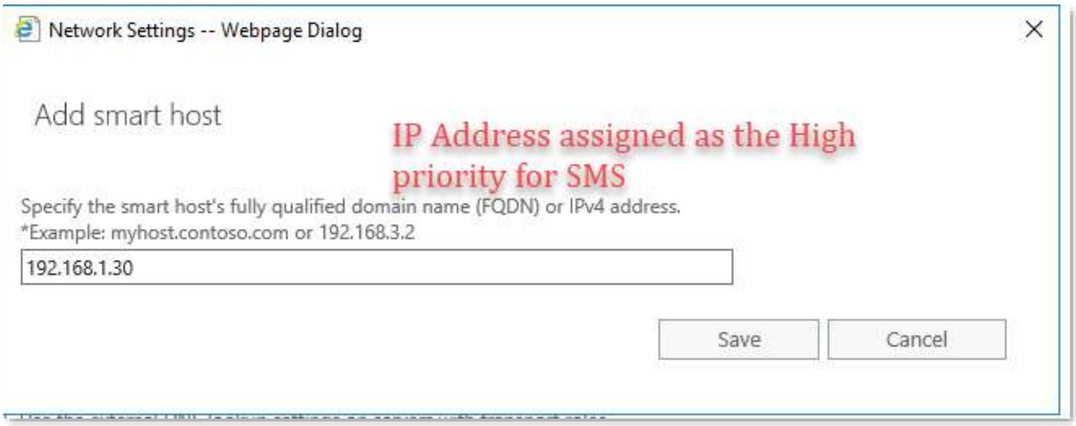
*Network settings:
Specify how to send mail with this connector.

○ MX record associated with recipient domain
● Route mail through smart hosts

Select route mail through smart hosts and then add a smart host

SMART HOST

□ Use the external DNS lookup settings on servers with transport roles

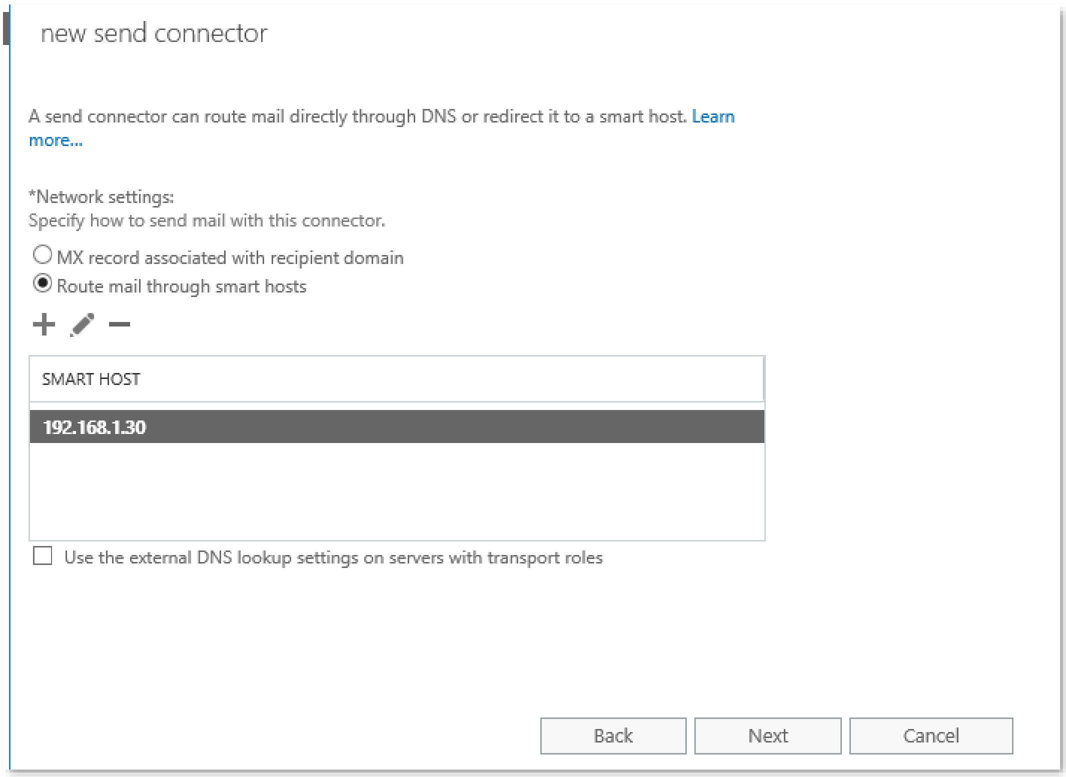


Add smart host

IP Address assigned as the High priority for SMS

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
*Example: myhost.contoso.com or 192.168.3.2

192.168.1.30



new send connector

A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...

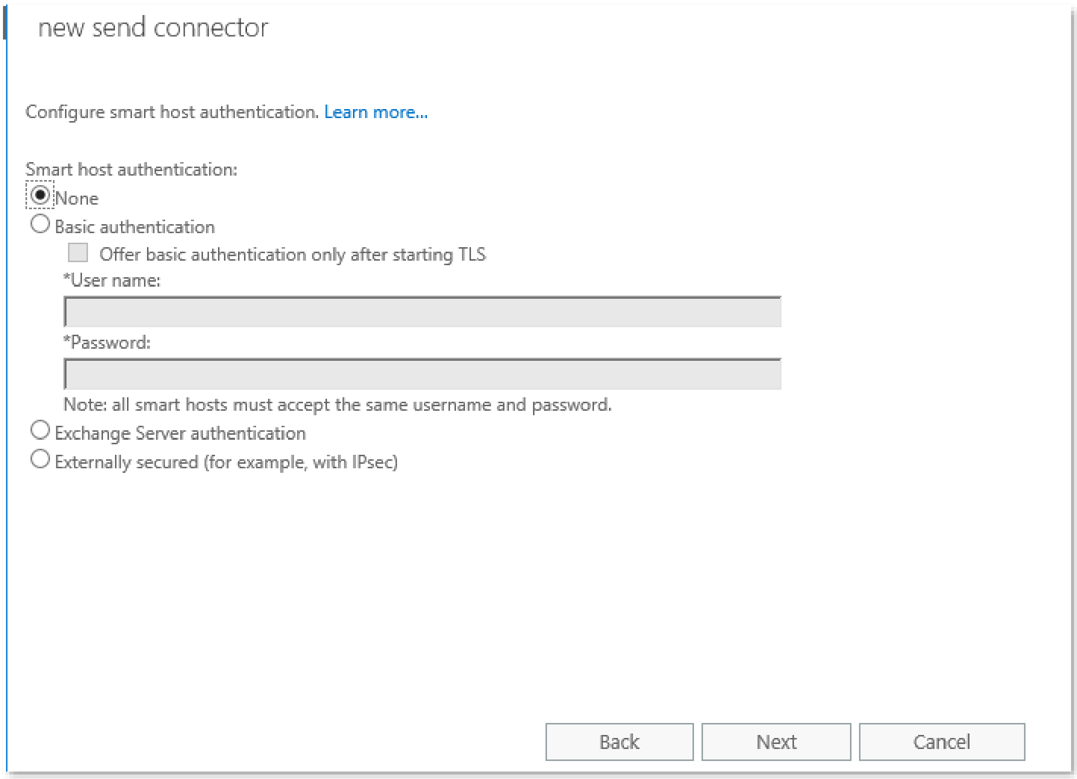
*Network settings:
Specify how to send mail with this connector.

○ MX record associated with recipient domain
● Route mail through smart hosts

SMART HOST
192.168.1.30

□ Use the external DNS lookup settings on servers with transport roles

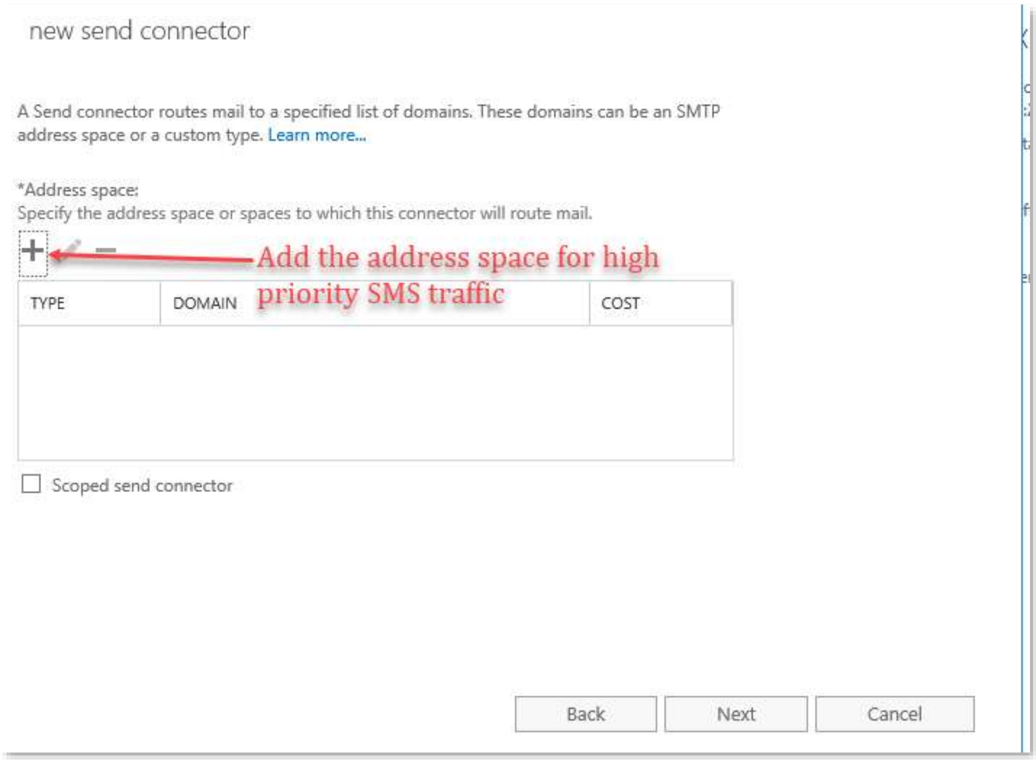
- Multiple SMS Servers can be defined for redundancy



new send connector

Configure smart host authentication. Learn more...

Smart host authentication:
● None
○ Basic authentication
□ Offer basic authentication only after starting TLS
*User name:
*Password:
Note: all smart hosts must accept the same username and password.
○ Exchange Server authentication
○ Externally secured (for example, with IPsec)



new send connector

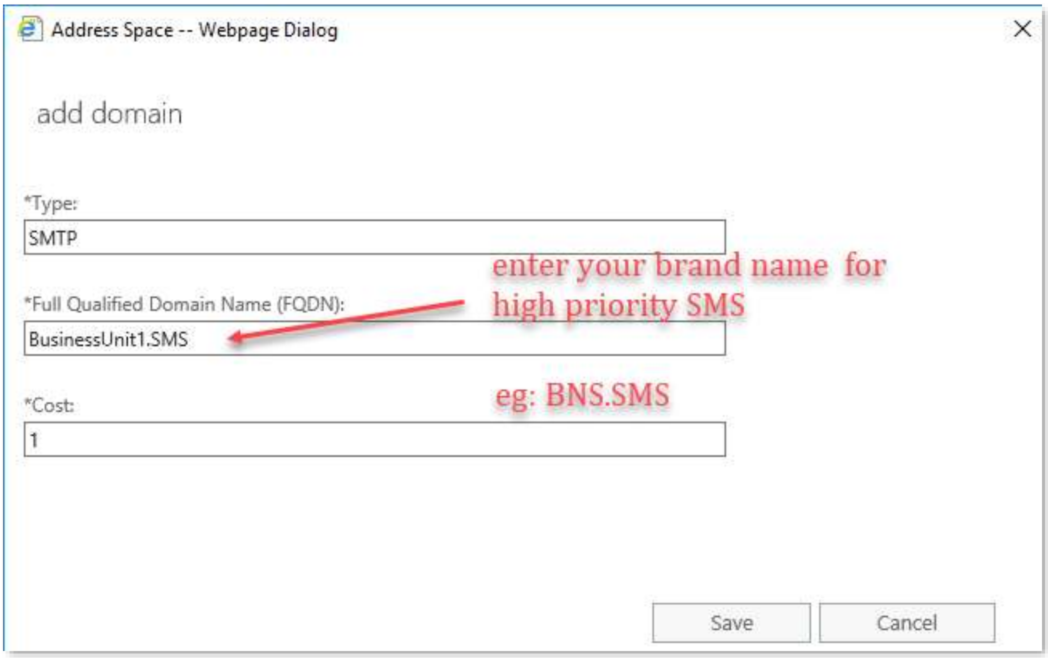
A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. Learn more...

*Address space:
Specify the address space or spaces to which this connector will route mail.

TYPE	DOMAIN	COST

☐ Scoped send connector

- Click on the Add button



Address Space -- Webpage Dialog

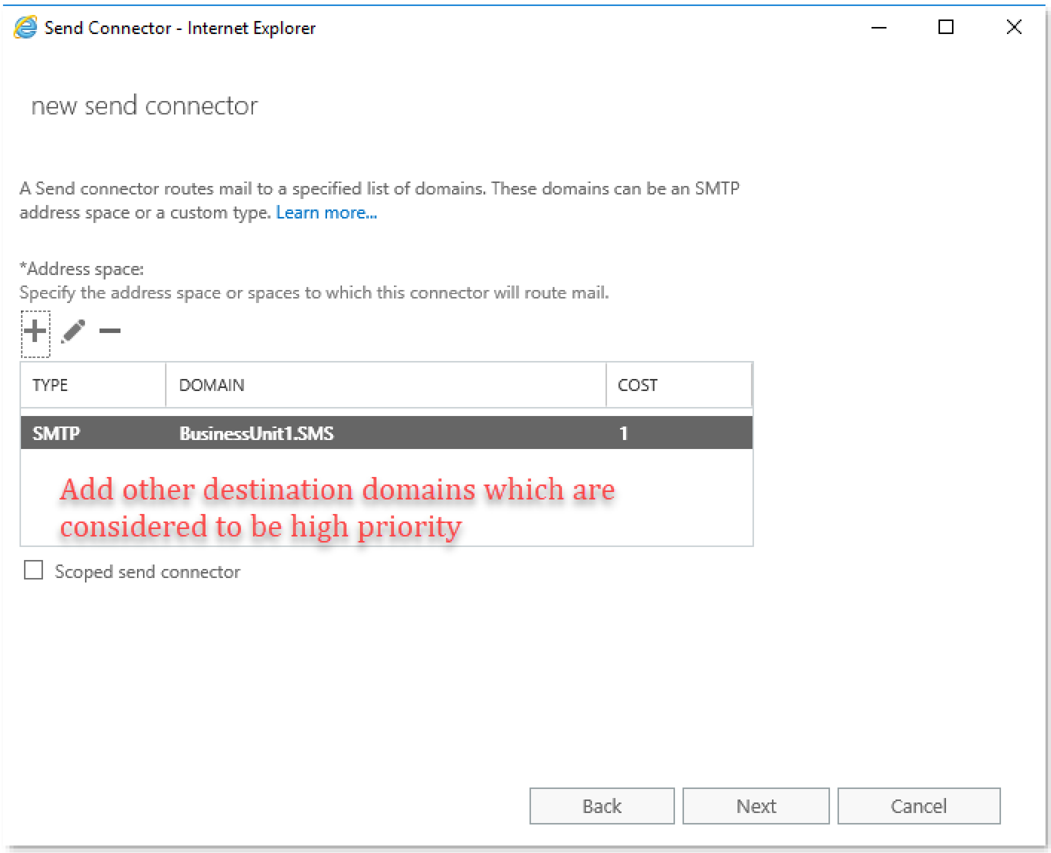
add domain

*Type:
SMTP

*Full Qualified Domain Name (FQDN):
BusinessUnit1.SMS

*Cost:
1

- Customers may decide that they wish to use sub domains so they are better positioned for migration to Exchange Online.
- Ie: use SMS.DomainName addressing as opposed to xxxxxxxx.SMS



Send Connector - Internet Explorer

new send connector

A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. Learn more...

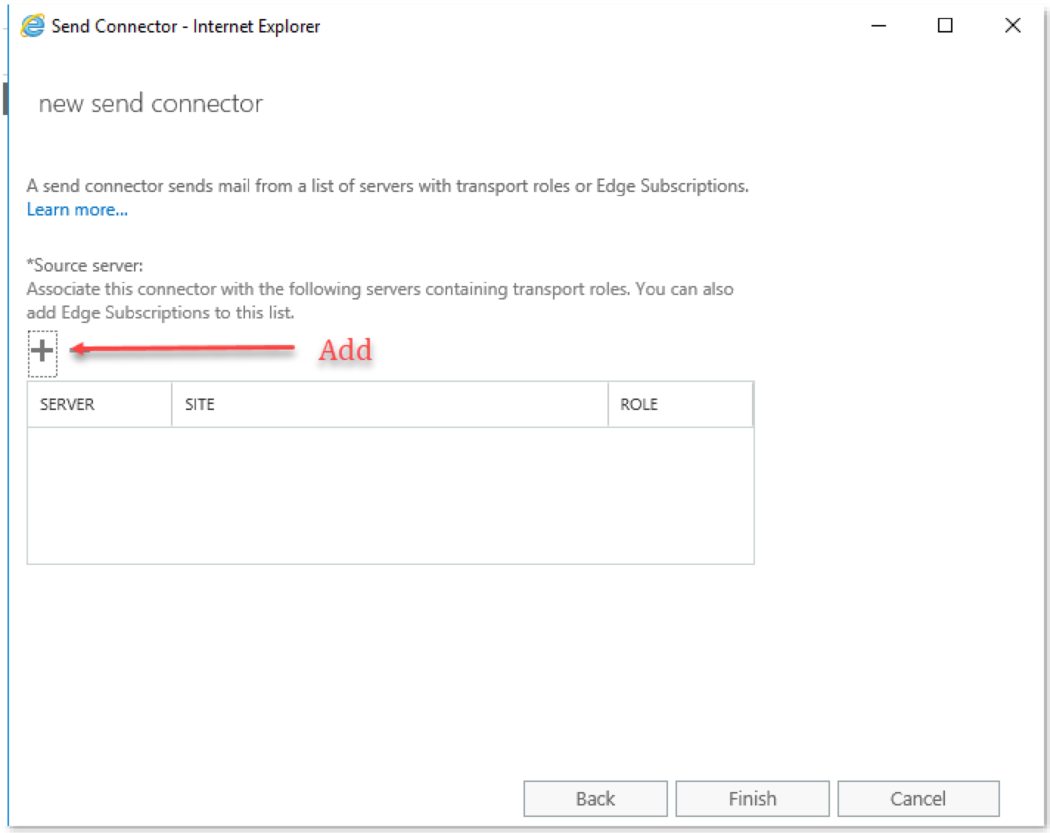
*Address space:
Specify the address space or spaces to which this connector will route mail.

TYPE	DOMAIN	COST
SMTP	BusinessUnit1.SMS	1

Add other destination domains which are considered to be high priority

□ Scoped send connector

- Select Next to add a server which has the transport role.



Send Connector - Internet Explorer

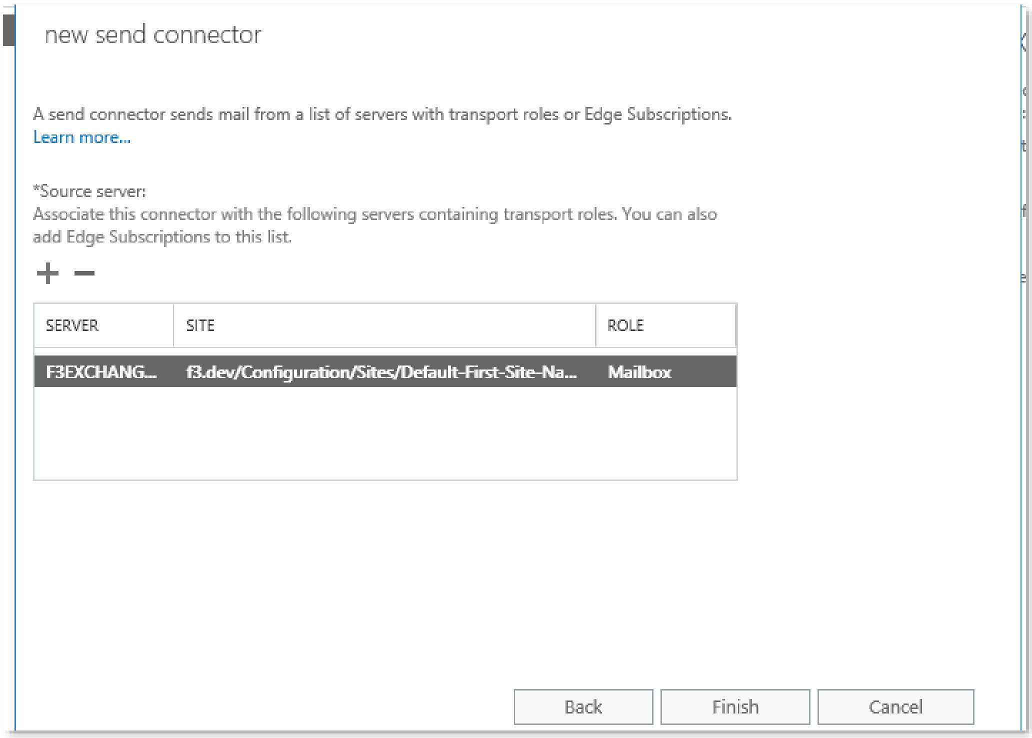
new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions. Learn more...

*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.

Add

SERVER	SITE	ROLE



new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions.
Learn more...

*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.

SERVER	SITE	ROLE
F3EXCHANG...	f3.dev/Configuration/Sites/Default-First-Site-Na...	Mailbox

Muiltple transport role servers can be used.

14.2.4 Testing via SMTP

Outlook can be used to send messages via SMTP connectors to the SMS server.

A test utility called the SMS Test Frame can also be used. For more information refer to https://smskb.bnsgroup.com.au/testframe

SECTION 15 Testing the system

15.1 SMS Console

BNS engineers will help the customer configure the system using the SMS Console in addition to the smsboot.ini file configuration settings.

SMS Console documentation can be found at this link https://smskb.bnsgroup.com.au/console

15.2 Testing from the test frame

This is the best option to use during deployment. It can test SQL and SMTP interfaces are configured correctly.

BNS engineers will help the customer perform initial tests using the test frame software.

15.3 Testing from Email environment

BNS engineers will help the customer perform initial tests using either Exchange online or Exchange Server and Microsoft Outlook.

SECTION 16 Backup and recovery

16.1 Disaster recovery

The architecture allows a proxy Windows SMS server in a DR site to take over from a failed production Windows SMS Server.

This is detailed later in this deployment guide.

16.2 Data storage

All data is stored in SQL Server. Current day data is stored in the sms-current Database. Early hours of the following day, the previous days information is then moved to the sms-archive database.

The SMS-SQL-API database contains only transient information between business applications and the SMS Server core services.

Standard backup and recovery of SQL server should be managed by the customer.

16.3 Configuration files

Configuration files are stored on each Windows SMS Server. They are simple text files which can be edited using notepad.

16.4 AWS EC2 instance backup and recovery

BNS recommends that a weekly backup of the EC2 instance be performed. The design of the SMS software holds all data in SQL server. Therefore, the data on the SMS server is transient and contains mainly log files.

If the SMS Server EC2 instance blue screens for example, a simple restore of the EBS volumes including the root volume should be performed to bring the system back to a working state.

To backup EC2 instances follow the AWS backup documentation in the link below

https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/ec2-backup.html

After a restore, if the Windows server is part of an AD domain, it is advisable to confirm that logins to the AD Domain are operation. Failure to login to the Windows server would be most likely a Kerberos machine account authentication error. For more information refer to Kerberos Authentication Overview | Microsoft Docs

16.5 AWS RDS SQL backup and restore

The SMS Server design has a Current DB and an Archive DB.

The software processes all SMS traffic into the Current DB in a 24 hour period.

A configurable value in the smsboot.ini file controls the time that the previous days transactions are moved from the Current DB to the Archive DB.

System-Attendant-Service-Archive24hrStartTime-str=0030

System-Attendant-Service-Archive24hrStopTime-str=0530

The default recommended time window is between 0030hours and 0530hours (Local Server time).

Therefore, RDS SQL backups should be performed daily after this time window eg: 0630hours (region local time). Both the current and archive DBs should be backed up at the same time.

If the Archive DB needs to be restored it can be restored independent of the current DB because there is no linkage between the two DBs.

If the Current DB needs to be restored from a previous backup the current day transactions will be lost.

To backup AWS RDS follow the AWS documentation in the link below

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_CommonTasks.BackupRestore.html

SECTION 17 Routine maintenance

17.1 Software Windows service credentials

If the customer requires the SMS Services to change passwords from time to time, the service accounts will need to be changed in services control manager for each server which is using that service account.

17.2 SMPP \ TLS

The SMS Software negotiates TLS based on the SMS Service providers TLS cyphers. As such there is no key management required on the SMS Server for TLS encryption.

17.3 Software patches and upgrades

If Software patches to the SMS software are required, BNS will notify all customers.

Upgrades are managed through a software release notice which describes the upgrade process relevant to that release of software.

17.4 License management of the SMS Software

Annual licenses are provided to the customer which are renewed usually as part of an enterprise agreement. BNS will provide updated license files which are deployed by the customer in accordance with instructions provided by email.

17.5 AWS Service limits

AWS maintains service quotas (formerly called service limits) for each account to help guarantee the availability of AWS resources and prevent accidental provisioning of more resources than needed. Some service quotas are raised automatically over time as you use AWS. However, most AWS services require that you request quota increases manually.

If any resource used by the SMS Software is limited in any way, the customer will need to manually request a service increase.

BNS has reviewed both EC2 and RDS quotas listed in the AWS console. BNS is not aware of any limitation which could be exceeded by the software itself.

Refer to service limits at this link
https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

SECTION 18 Emergency Maintenance

18.1 Handling fault conditions

Depending on what the fault is will depend on what action is required by the customer's IT team.

Irrespective of the fault a ticket should be raised with BNS using email support@bnsgroup.com.au

Minimum information required in your email to Support@bnsgroup.com.au

1. A brief description of the problem
2. Your contact details including telephone number
3. The name of your organization
4. Criticality / business impact

On receipt of your email, BNS's automated ticketing systems will provide a case number response back via email. BNS generally contact the customer by telephone.

The following are identifiable possible faults which could occur and the recommended action.

18.1.1 Business processes are unable to access the SMS-SQL-API DB

Recommended actions:

- Check with the SQL Admin for any exceptions in the access control logs in SQL Server.
- Run the test tool provided with the SMS Software (refer section 12).

18.1.2 SMS messages are not being received from the Health Service to nominated handsets

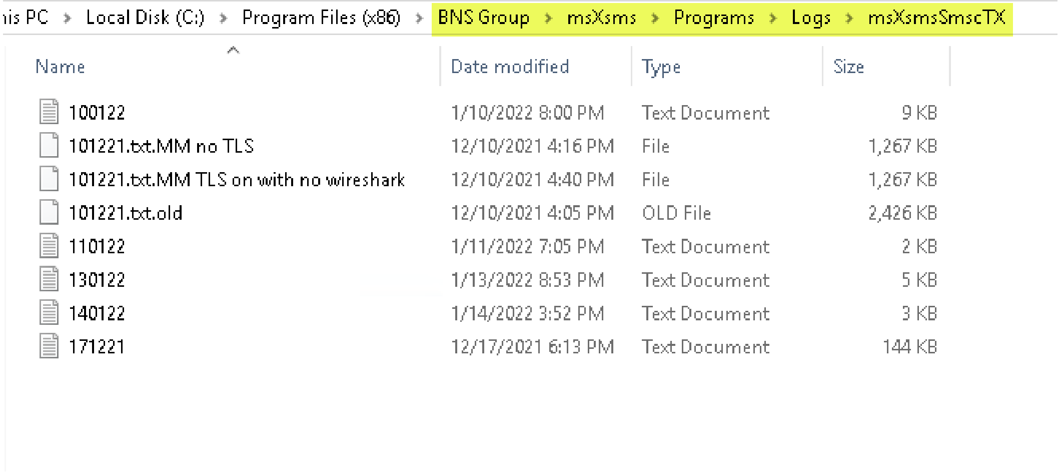
Recommended actions:

- Check the Health Service log files to ensure the service is not reporting any error messages.
- Run the test tool provided with the SMS Software (refer section 12). Confirm what happens with the test tool and report this to BNS on a support ticket.

18.1.3 SMS messages are not being sent to handsets

Recommended actions:

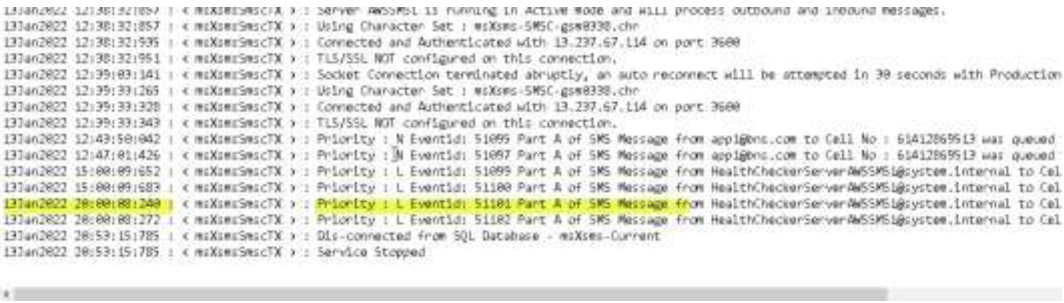
- Run the test tool provided with the SMS Software (refer section 12). Confirm what happens with the test tool and report this to BNS on a support ticket.
- Check the log file for the smscTX service for any reported errors and see if it is actually processing messages.
- Send a copy of this TX log to BNS on the support ticket.



is PC > Local Disk (C:) > Program Files (x86) > BNS Group > msXsms > Programs > Logs > msXsmsSmscTX

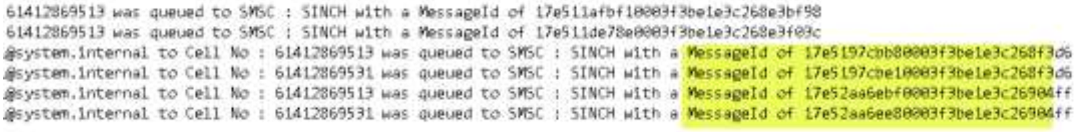
Name	Date modified	Type	Size
100122	1/10/2022 8:00 PM	Text Document	9 KB
101221.txt.MM no TLS	12/10/2021 4:16 PM	File	1,267 KB
101221.txt.MM TLS on with no wireshark	12/10/2021 4:40 PM	File	1,267 KB
101221.txt.old	12/10/2021 4:05 PM	OLD File	2,426 KB
110122	1/11/2022 7:05 PM	Text Document	2 KB
130122	1/13/2022 8:53 PM	Text Document	5 KB
140122	1/14/2022 3:52 PM	Text Document	3 KB
171221	12/17/2021 6:13 PM	Text Document	144 KB

Open the log file to see if messages are being processed. Local server times are used in the log file.



```
13Jan2022 12:38:32:857 | < msXsmsSmscTX > : Server AWSSMS1 is running in Active mode and will process outbound and inbound messages.
13Jan2022 12:38:32:857 | < msXsmsSmscTX > : Using Character Set : msXsms-SMSC-gsm0338.chr
13Jan2022 12:38:32:935 | < msXsmsSmscTX > : Connected and Authenticated with 13.237.67.114 on port 3600
13Jan2022 12:38:32:951 | < msXsmsSmscTX > : TLS/SSL NOT configured on this connection.
13Jan2022 12:39:03:141 | < msXsmsSmscTX > : Socket Connection terminated abruptly, an auto reconnect will be attempted in 30 seconds with Production
13Jan2022 12:39:33:265 | < msXsmsSmscTX > : Using Character Set : msXsms-SMSC-gsm0338.chr
13Jan2022 12:39:33:328 | < msXsmsSmscTX > : Connected and Authenticated with 13.237.67.114 on port 3600
13Jan2022 12:39:33:343 | < msXsmsSmscTX > : TLS/SSL NOT configured on this connection.
13Jan2022 12:43:50:042 | < msXsmsSmscTX > : Priority : N EventId: 51095 Part A of SMS Message from api@bns.com to Cell No : 61412869513 was queued
13Jan2022 12:47:01:426 | < msXsmsSmscTX > : Priority : N EventId: 51097 Part A of SMS Message from api@bns.com to Cell No : 61412869513 was queued
13Jan2022 15:00:09:652 | < msXsmsSmscTX > : Priority : L EventId: 51099 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 15:00:09:683 | < msXsmsSmscTX > : Priority : L EventId: 51100 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 20:00:08:240 | < msXsmsSmscTX > : Priority : L EventId: 51101 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 20:00:08:272 | < msXsmsSmscTX > : Priority : L EventId: 51102 Part A of SMS Message from HealthCheckerServerAWSSMS1@system.internal to Cel
13Jan2022 20:53:15:785 | < msXsmsSmscTX > : Dis-connected from SQL Database - msXsms-Current
13Jan2022 20:53:15:785 | < msXsmsSmscTX > : Service Stopped
```

If you see MessageIds from the service provider in the log as the example below but you are not seeing them on destination handsets then the issue is with the service provider. A manual failover to a secondary service in this instance would be required. This is documented at https://smskb.bnsgroup.com.au/manualfailover don't forget to log the issue with your SMS Service provider and advise the business what has happened. Messages which have been sent to the SMS Service provider cannot be sent again. You will have to wait until their service is restored. However, if their outage is likely to be some time, you can perform a manual failover to a secondary provider to process new SMS requests.



```
61412869513 was queued to SMSC : SINCH with a MessageId of 17e511afbf10003f3be1e3c268e3bf98
61412869513 was queued to SMSC : SINCH with a MessageId of 17e511de78e0003f3be1e3c268e3f03c
@system.internal to Cell No : 61412869513 was queued to SMSC : SINCH with a MessageId of 17e5197cbb80003f3be1e3c268f3d6
@system.internal to Cell No : 61412869531 was queued to SMSC : SINCH with a MessageId of 17e5197cbe10003f3be1e3c268f3d6
@system.internal to Cell No : 61412869513 was queued to SMSC : SINCH with a MessageId of 17e52aa6ebf0003f3be1e3c26904ff
@system.internal to Cell No : 61412869531 was queued to SMSC : SINCH with a MessageId of 17e52aa6ee80003f3be1e3c26904ff
```

SECTION 19 Support

19.1 How to receive support

Primary support is via email by sending a request to support@bnsgroup.com.au

If the customer has a system down condition:

- Log a support via email first support@bnsgroup.com.au then
- Call +61 2 80016653 24 x 7 and leave your details for 'Technical Support'.

19.2 Support Tiers

BNS has 1 main support tier for enterprise customers offering a 4 hour SLA response during business hours 9am to 6pm Monday through Friday Australian Eastern time zone Sydney\Canberra.

Support requests logged via email to support@bnsgroup.com.au is mandatory to receive a 4 hour response.

All support is via: email, telephone and remote assist using Microsoft Teams or the preferred remote tools supported by the customer.

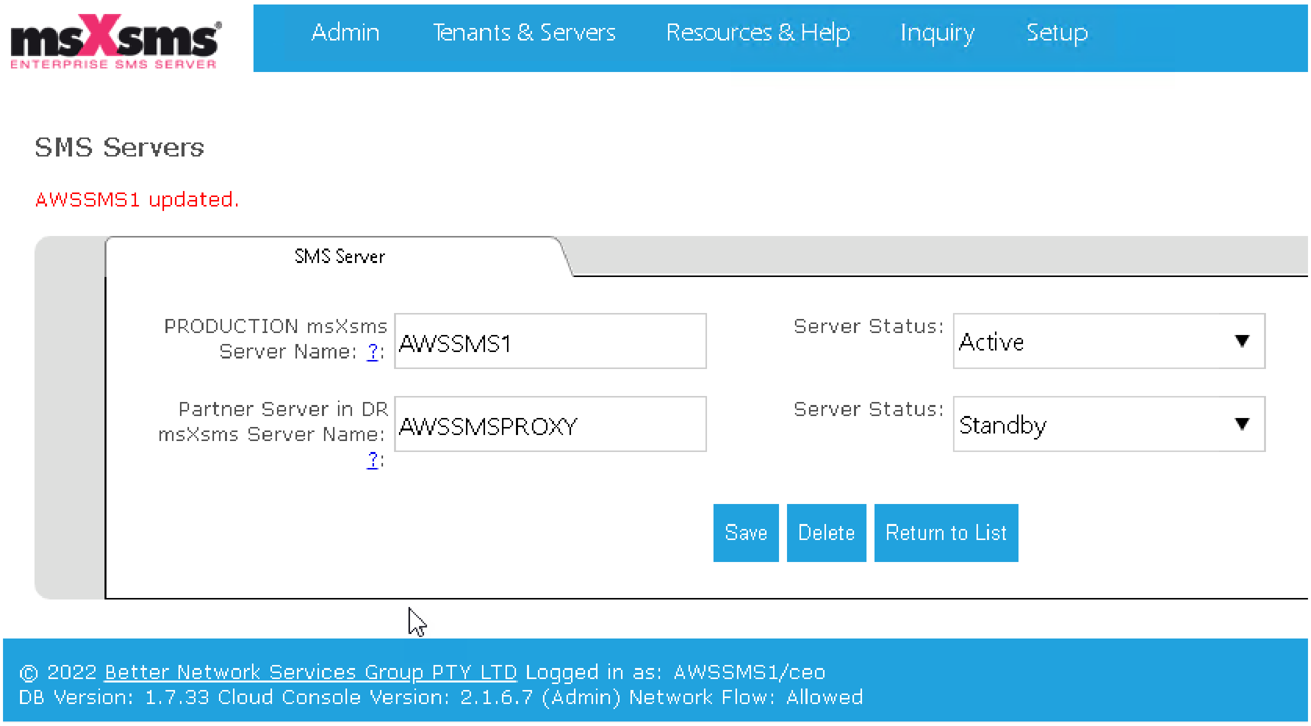
BNS operates a 24 x 7 service for taking support requests after an initial email has been sent to support@bnsgroup.com.au

- For urgent service, call +61 2 80016653 24 x 7 and leave your details for 'Technical Support'. State that your request is urgent.

Customers requiring premium service for 24 x 7 service should contact BNS for more information.

SECTION 20 Disaster Recovery planning

20.1 DR Partner Server



SMS Servers

AWSSMS1 updated.

PRODUCTION msXsms Server Name: ?:	AWSSMS1	Server Status:	Active ▼
Partner Server in DR msXsms Server Name: ?:	AWSSMSPROXY	Server Status:	Standby ▼

© 2022 Better Network Services Group PTY LTD Logged in as: AWSSMS1/ceo
DB Version: 1.7.33 Cloud Console Version: 2.1.6.7 (Admin) Network Flow: Allowed

A high level design with 2 x SMS servers spread across 2 AWS AZ's have sufficient capacity to handle a failure of 1 SMS server in 1 AZ or the loss of an AZ. .

A DR partner server **is not relevant** for new deployments in AWS due to the scale and resilience of AWS.

A DR partner server was relevant pre-cloud designs when a customer had a pair of data centres and wanted a traditional prod\dr architecture.

Cloud based computing allows rapid recovery of virtual machines from snapshots and provides automatic recovery and failover of AWS RDS Database servers.

BNS Enterprise SMS Server software has been re-engineered for cloud for:

- Multi-AZ failover support
- Sufficient capacity to manage without 1 SMS server for a period of time
- Moving of SMS records from a failed server to the other server
- Automatic take-over of SQL API processing responsibility
- Automatic re-deployment of messages across SMPP binds on a server

However, if a customer does need a standby server to be a partner server refer to https://smskb.bnsgroup.com.au/smsdr

SECTION 21 Appendix

21.1 AWS RDS performance testing

The following tests were performed in February 2023 using AWS RDS Microsoft SQL Express. Use of the SQL Express edition is not recommended for a customer deployment except for a proof of concept or dev\test.

Production deployments require AWS RDS Microsoft SQL Server in Single-AZ or Multi-AZ.

Tests conducted by BNS were end to end tests including SMPP\TLS transmission to Messagemedia over the Internet. BNS and MessageMedia are both located in AWS tenancies, therefore SMPP latency is the lowest possible TCP\IP latency.

21.1.1 AWS EC2 instance – SMS Server

EC2 T3.2XLarge was used as this will be the benchmark instance class with multiple SMPP binds. This test was with 1 x SMSCTX SMPP bind and 1 x SMSCRX SMPP bind.

EC2 instance	Details	Comment
EC2 Type	T3.2xLARGE	32 GB RAM 8 x VCPU
Name	AWSSMSTST4	
2 x EBS volumes	Root and Data	Application installed on D drive GP2 Root volume GP3 app volume
Software build	Ver2 12 Feb 2022 Build 3	

21.1.2 AWS RDS MS SQL Express

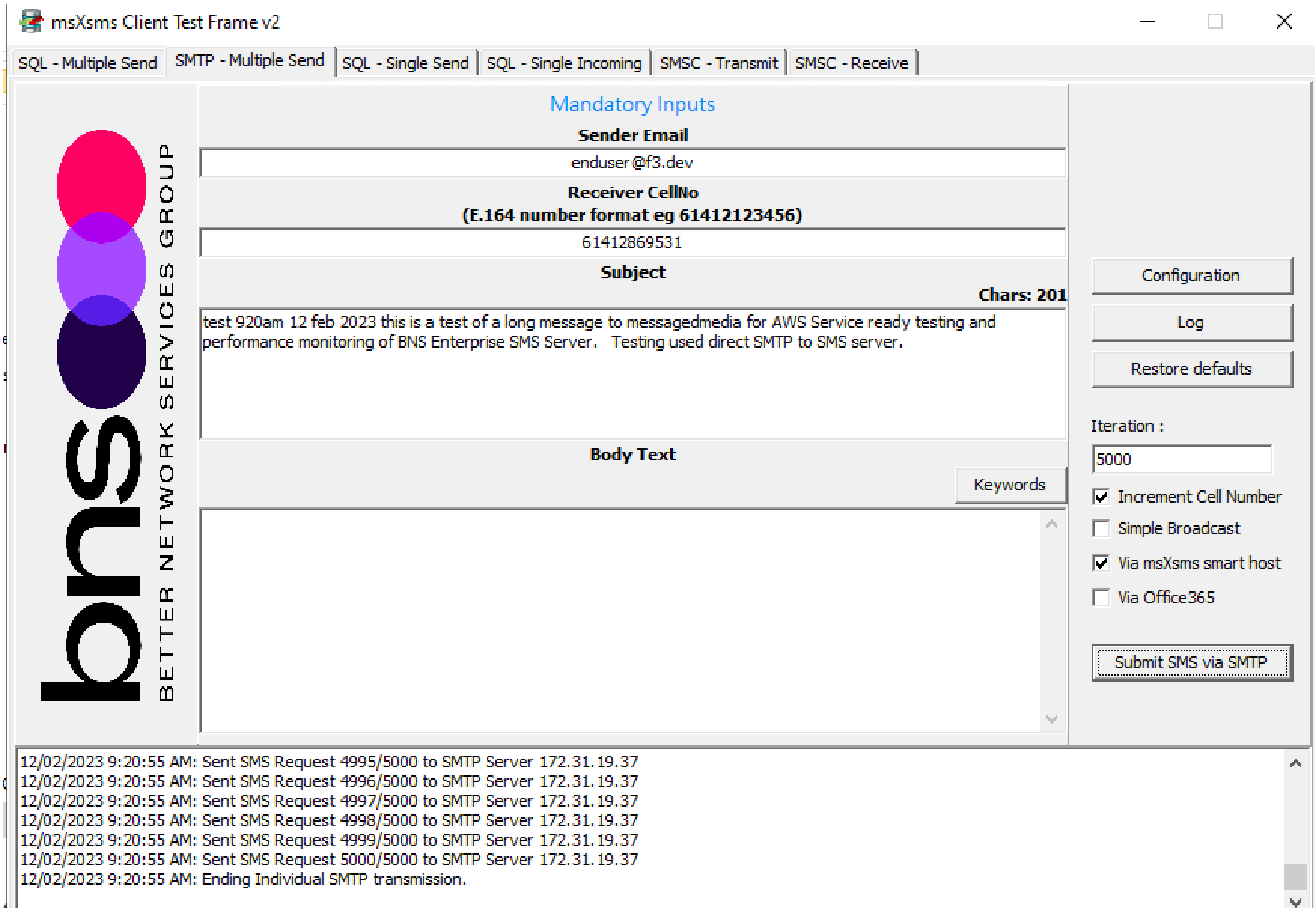
AWS RDS	Details	Comment
DB Id	Sql	
RDS class	Db.t3.medium	2 x vcpu 4GB ram
Engine	SQL Server Express Edition	
Databases	TST-SMS-Current TST-SMS-Archive TST-SMS-SQL-API	
Storage	GP2	
Availability zone	ap-southeast-2c	
Engine version	15.00.4073.23.v1	

Enhanced monitoring is set to 60 seconds.   Default.

21.1.3 MessageMedia

MessageMedia was used with a special account setting to allow a load test without the actual messages being submitted to the mobile network.

21.1.4 SMPP Client tool \ service details from AWSSMSTST4



Mandatory Inputs

Sender Email: enduser@f3.dev

Receiver CellNo (E.164 number format eg 61412123456): 61412869531

Subject — Chars: 201

test 920am 12 feb 2023 this is a test of a long message to messagedmedia for AWS Service ready testing and performance monitoring of BNS Enterprise SMS Server. Testing used direct SMTP to SMS server.

Body Text

Iteration : 5000

☑ Increment Cell Number
☐ Simple Broadcast
☑ Via msXsms smart host
☐ Via Office365

```
12/02/2023 9:20:55 AM: Sent SMS Request 4995/5000 to SMTP Server 172.31.19.37
12/02/2023 9:20:55 AM: Sent SMS Request 4996/5000 to SMTP Server 172.31.19.37
12/02/2023 9:20:55 AM: Sent SMS Request 4997/5000 to SMTP Server 172.31.19.37
12/02/2023 9:20:55 AM: Sent SMS Request 4998/5000 to SMTP Server 172.31.19.37
12/02/2023 9:20:55 AM: Sent SMS Request 4999/5000 to SMTP Server 172.31.19.37
12/02/2023 9:20:55 AM: Sent SMS Request 5000/5000 to SMTP Server 172.31.19.37
12/02/2023 9:20:55 AM: Ending Individual SMTP transmission.
```

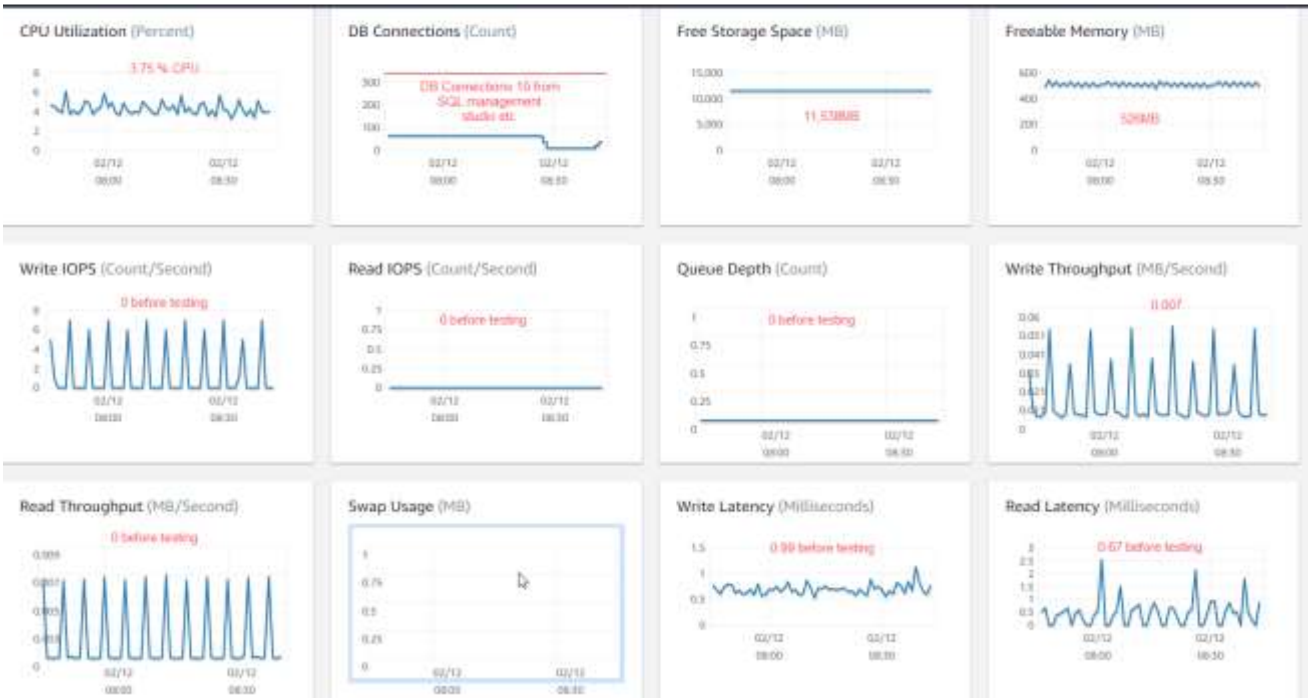
Note: we used enduser@f3.dev as an app with no sending of any confirmations back. SMTPQD service was therefore less loaded than perhaps could have been.

21.1.5 SMPP\TLS transmission from BNS AWS to MessageMedia AWS

Item	Value	Comments
SMPP TX binds	1	
SMPP RX binds	1	
Total number of long SMS messages sent	5000	
Long SMS message size	201 characters	
SMPP messages parts per long SMS message	2	
Total SMPP messages parts	10,000	
Transmission started	12Feb2023 09:20:15:505	
Transmission completed	12Feb2023 09:25:54:867	
Total time	5 mins (300 seconds)	
Per second rate SMPP parts		10,000 SMPP parts \ 300 seconds = **33.33 SMPP parts per second**
Per second rate long SMS message 201 characters from application		5,000 long messages (201 characters) \ 300 seconds = **16.66 long messages per second**

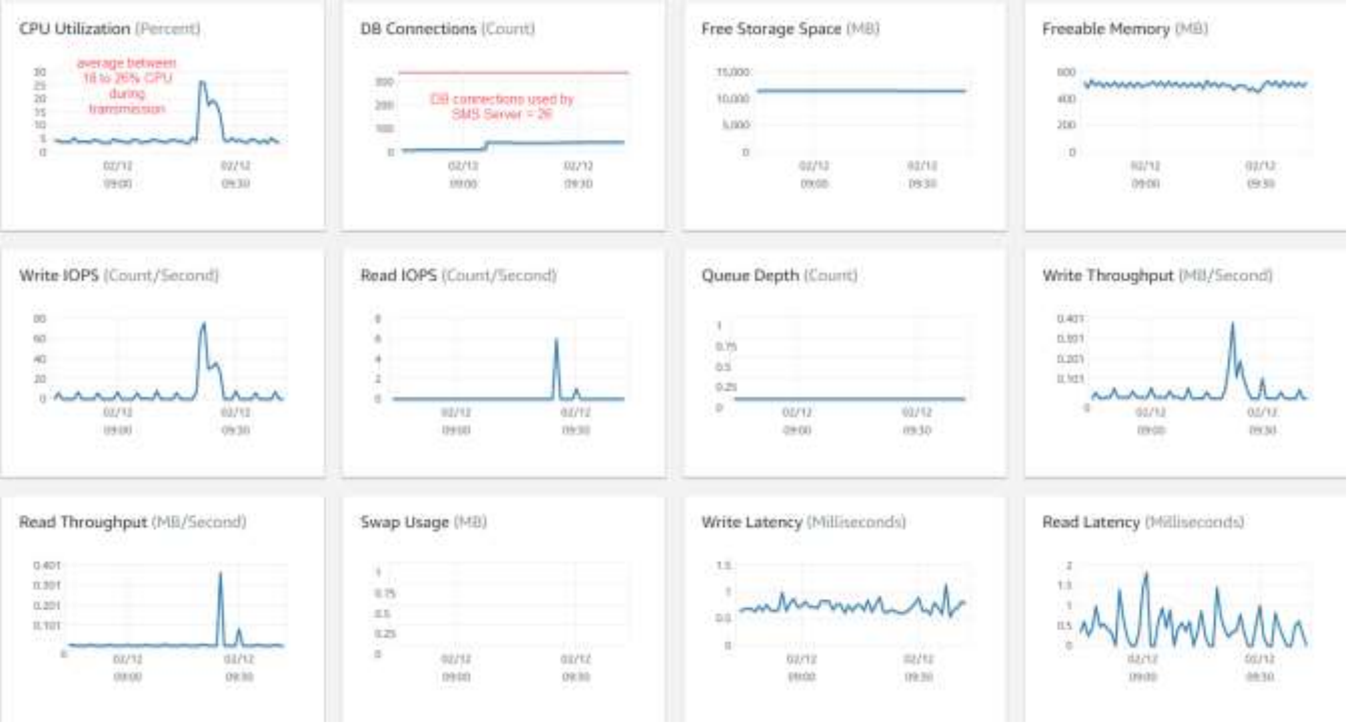
21.2 AWS RDS SQL Express metrics

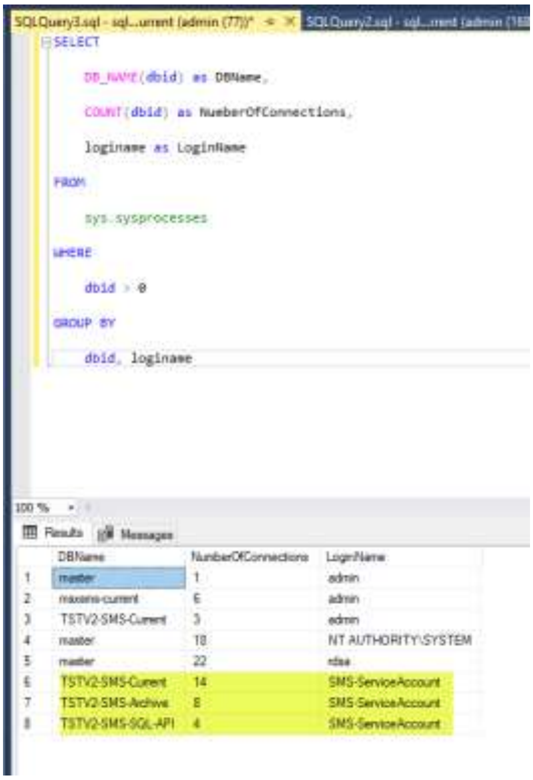
21.2.1 Before testing commenced



SQL Management Studio and other management processes had a total of 11 DB Connections. All applications were closed before the tests.

21.2.2 RDS metric summary after test completed




SQLQuery3.sql - sql...urrent (admin (77))*
SQLQuery2.sql - sql...rrent (admin (16
100 %
Results
Messages

```
SELECT

    DB_NAME(dbid) as DBName,

    COUNT(dbid) as NumberOfConnections,

    loginame as LoginName

FROM

    sys.sysprocesses

WHERE

    dbid > 0

GROUP BY

    dbid, loginame
```

	DBName	NumberOfConnections	LoginName
1	master	1	admin
2	maxsms-current	6	admin
3	TSTV2-SMS-Current	3	admin
4	master	18	NT AUTHORITY\SYSTEM
5	master	22	rdsa
6	TSTV2-SMS-Current	14	SMS-ServiceAccount
7	TSTV2-SMS-Archive	8	SMS-ServiceAccount
8	TSTV2-SMS-SQL-API	4	SMS-ServiceAccount

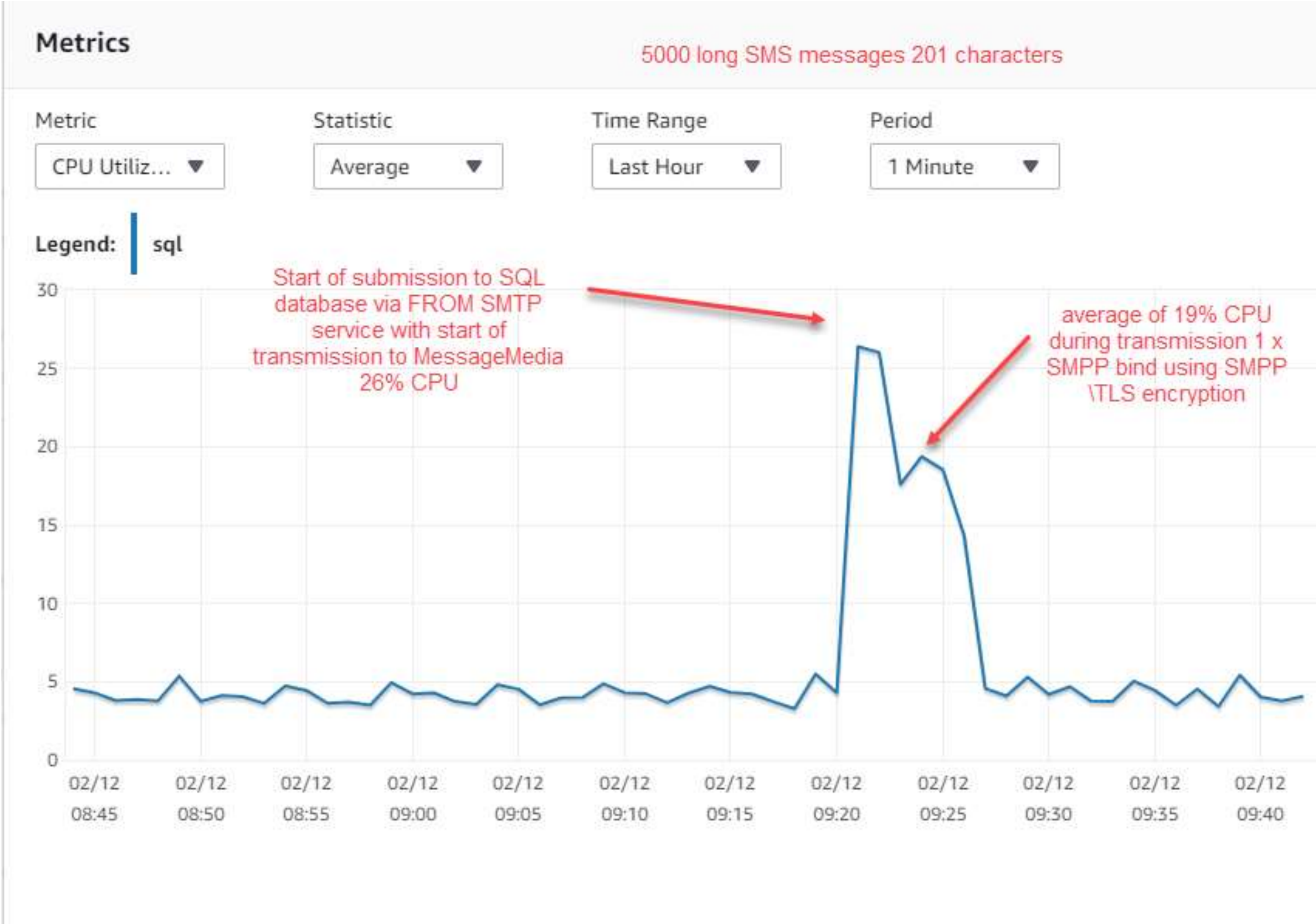
SMS Service account is the total number of connections from Windows Service accounts = 26

CPU utilization of RDS SQL Express during transmission started with submission service reading SMTP submissions processing EML files and submitting to MainStore of Current DB.

SMS Transmission SMPP\ TLS commences transmission as soon the transactions are written to the mainstore.

CPU tapers off as submission service completes writing.

SMS transmission SMPP service continues showing a drop to around 19% CPU of RDS SQL Express utilization.



Metrics

5000 long SMS messages 201 characters

Metric: CPU Utiliz...

Statistic: Average

Time Range: Last Hour

Period: 1 Minute

Legend: sql

Start of submission to SQL database via FROM SMTP service with start of transmission to MessageMedia 26% CPU

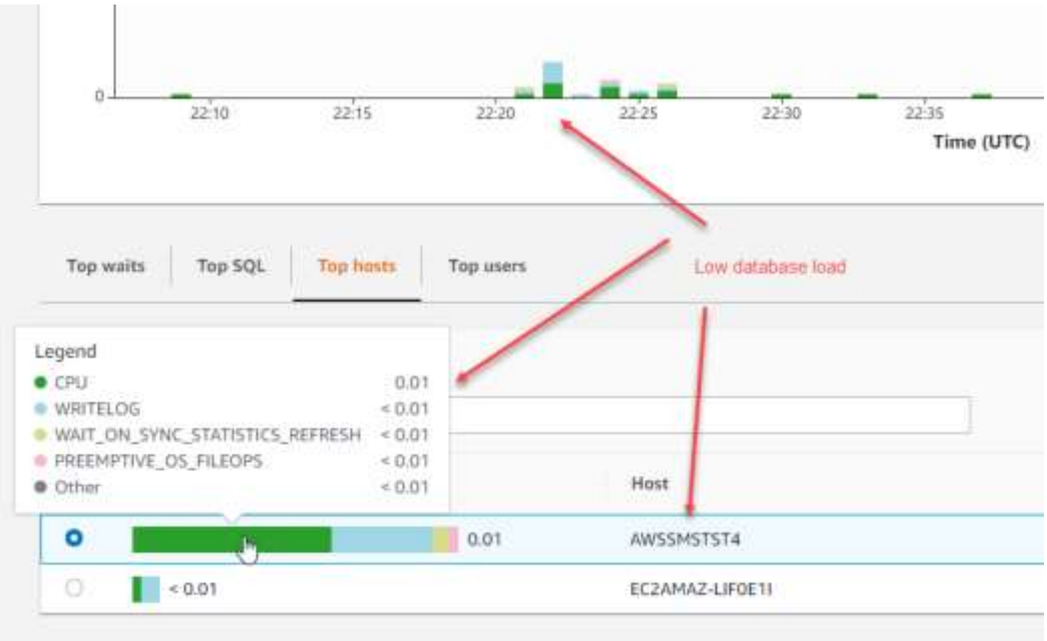
average of 19% CPU during transmission 1 x SMPP bind using SMPP \TLS encryption

21.2.3 AWS RDS metric summary table

Item	Value	Comments
CPU utilisation	19 to 25%	
DB Connections	26	Total used by SMS Server
Freeable memory	450MB	Drop from average 500MB before test.
Write IOPS	Peak 76 Average 36	Estimate based on metric chart
Read IOPS	Peak 6	
Read Latency	0.5ms	Estimate based on metric chart
Write Latency	0.75ms	Estimate based on metric chart

21.2.4 Performance insight for database load

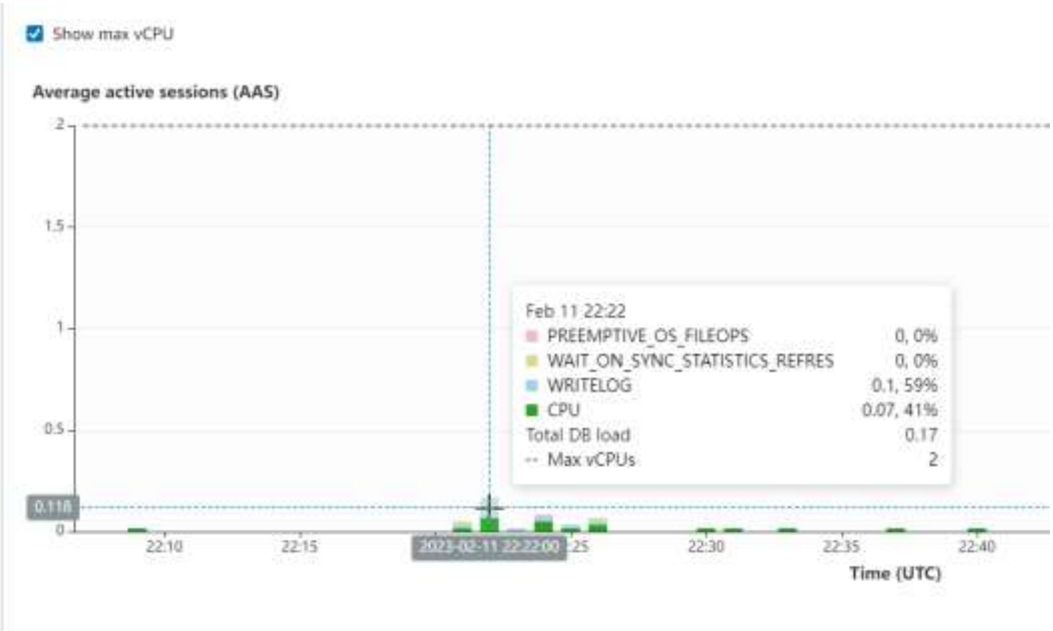
Overall there was low database load.



Legend

● CPU	0.01
● WRITELOG	< 0.01
● WAIT_ON_SYNC_STATISTICS_REFRESH	< 0.01
● PREEMPTIVE_OS_FILEOPS	< 0.01
● Other	< 0.01

		Host
●	0.01	AWSSMSTST4
○	< 0.01	EC2AMAZ-LIFOE1I



☑ Show max vCPU

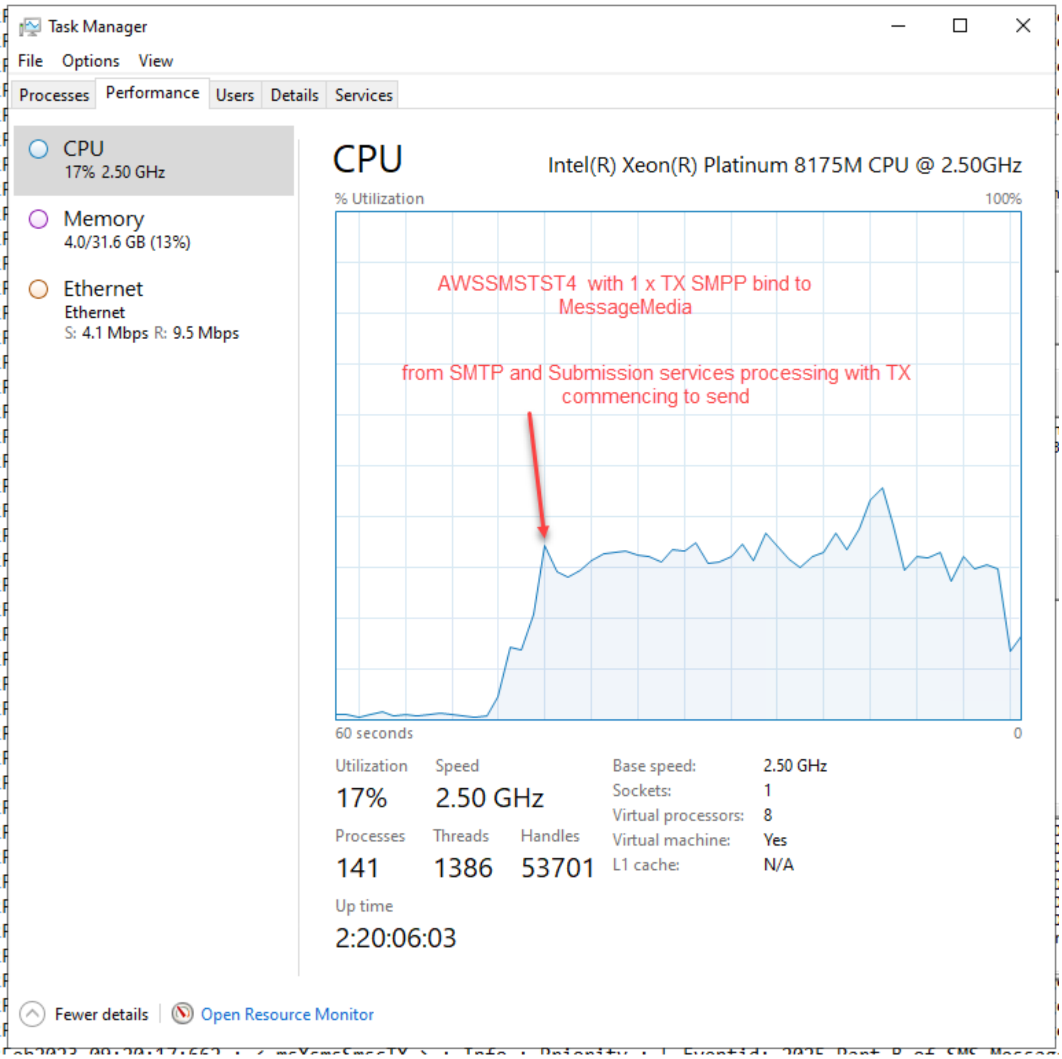
Average active sessions (AAS)

Feb 11 22:22

▨ PREEMPTIVE_OS_FILEOPS	0, 0%
▨ WAIT_ON_SYNC_STATISTICS_REFRES	0, 0%
▨ WRITELOG	0.1, 59%
🟩 CPU	0.07, 41%
Total DB load	0.17
-- Max vCPUs	2

21.3 EC2 instance AWSSMSTST4

Software version 2 build 3 with 1 single TX and RX bind.G



CPU
17% 2.50 GHz

Memory
4.0/31.6 GB (13%)

Ethernet
Ethernet
S: 4.1 Mbps R: 9.5 Mbps

CPU Intel(R) Xeon(R) Platinum 8175M CPU @ 2.50GHz

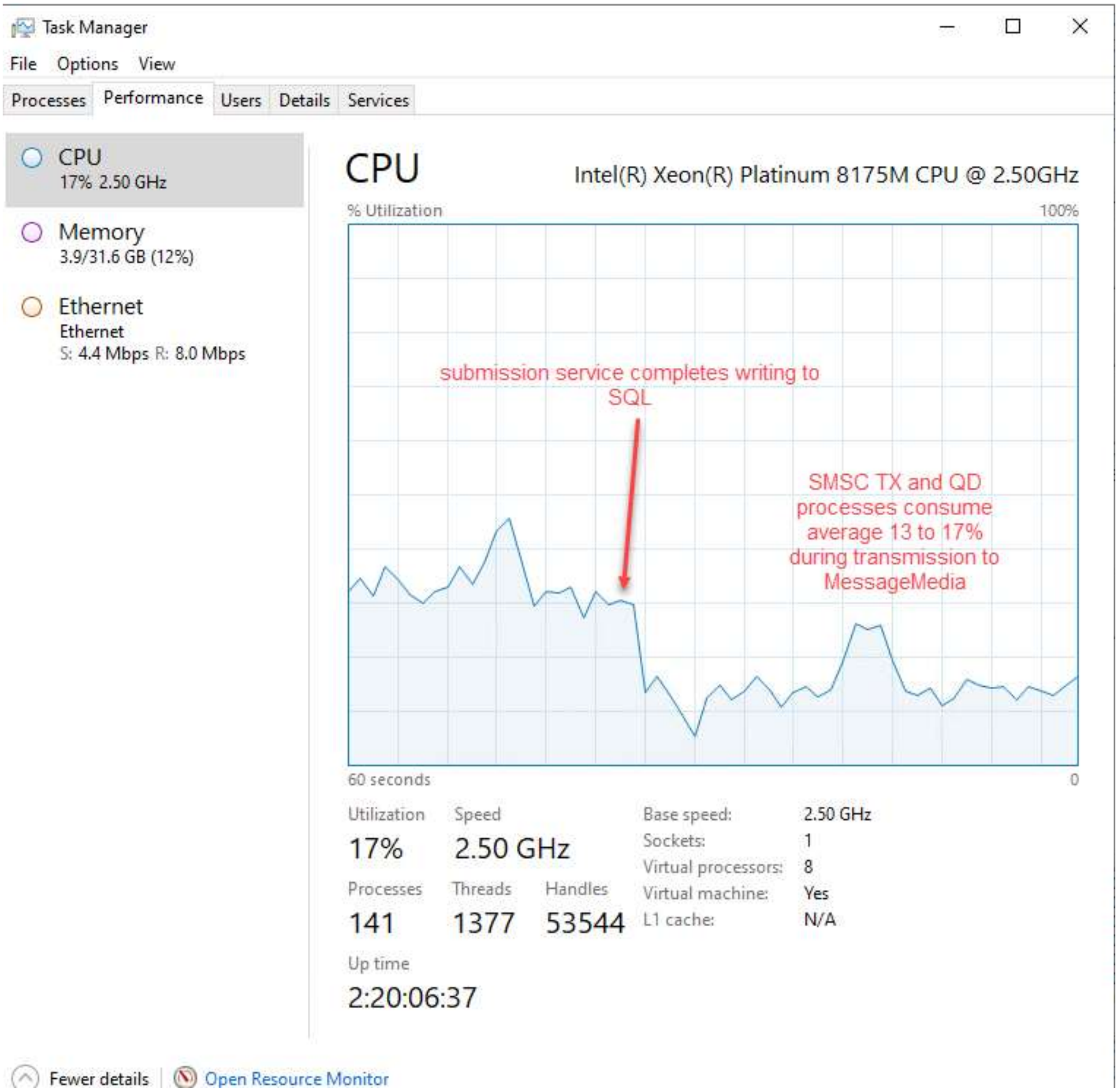
AWSSMSTST4 with 1 x TX SMPP bind to MessageMedia

from SMTP and Submission services processing with TX commencing to send

Utilization 17%
Speed 2.50 GHz
Processes 141
Threads 1386
Handles 53701
Up time 2:20:06:03

Base speed: 2.50 GHz
Sockets: 1
Virtual processors: 8
Virtual machine: Yes
L1 cache: N/A

```
Feb2023 09:20:17:662 : < msXsmsSmscTX > : Info : Priority : 1 Eventid: 2025 Part B of SMS Messag
```



submission service completes writing to SQL

SMSC TX and QD processes consume average 13 to 17% during transmission to MessageMedia

Utilization 17%

Speed 2.50 GHz

Processes 141

Threads 1377

Handles 53544

Up time 2:20:06:37

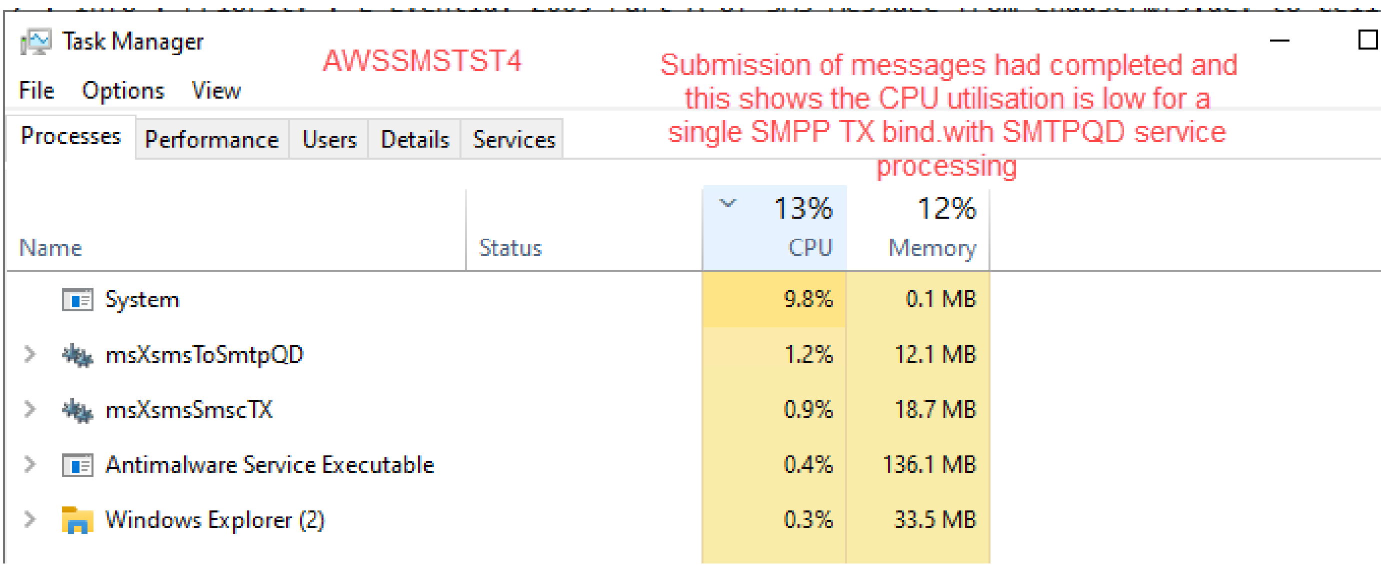
Base speed: 2.50 GHz

Sockets: 1

Virtual processors: 8

Virtual machine: Yes

L1 cache: N/A



AWSSMSTST4

Submission of messages had completed and this shows the CPU utilisation is low for a single SMPP TX bind.with SMTPQD service processing

Name	Status	13% CPU	12% Memory
System		9.8%	0.1 MB
msXsmsToSmtpQD		1.2%	12.1 MB
msXsmsSmscTX		0.9%	18.7 MB
Antimalware Service Executable		0.4%	136.1 MB
Windows Explorer (2)		0.3%	33.5 MB

The operating system was using 13%

Antimalware – BNS excluded the SMS Server folder from Defender.