



INTELLICENE
SECURITY // EVOLVED

Symphia NowForce

Three Servers Installation Guide

For version 6.2.2

October 11, 2023

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent Intellicene Inc. is strictly prohibited. By providing this document, Intellicene Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Contact your Intellicene representative for current product features and specifications. All marks referenced herein with the ® or TM symbol are registered trademark or trademarks of Intellicene Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

© 2023 Intellicene Inc. All Rights Reserved Worldwide.

Contents

Contents	2
Summary of Changes	4
Version 6.2.2 - October 2023	4
Version 6.1 - January 2023	4
Overview	5
Components in a Symphia NowForce Three Server Deployment	6
Prerequisites	7
Step 1: Extract the Installation Files	9
Step 2: Confirm and Configure Disk Bytes Per Cluster	10
Step 3: Open Ports	12
Step 4: Add Domain Name to Hosts	12
3rd Party Installation Prerequisites	14
Step 1: Install .NET Framework 4.8	14
Step 2: Install Microsoft SQL Server 2019 Standard	14
Step 3: Download and Install the Latest Cumulative Pack	20
Step 4: Install SQL Server Management Studio	21
Step 5: Download and Install the DB Installation Tool	21
Step 6: Deploy Microsoft IIS Web Server	24
Step 7: Install Rabbit MQ on Windows IIS Server	24
Step 8: Install Node.js Chat Server	26
Step 9: Install Environment Prerequisites	26
Installing the NowForce Application	27
Step 1: Create an SQL User for API Access	27
Step 2: Configure Web Settings	31
Step 3: Configure an SQL Server Backup Maintenance Task	32

Step 4: Configure an SQL Server Differential Backup Maintenance Task	36
Step 5: Install MongoDB Using Percona	41
Step 6: Install a Schema for the Mongo Database on the Ubuntu Server	42
Step 7: Configure SQL Transparent Data Encryption (TDE)	43
Step 8: Configure Node.js Chat Server	44
Step 9: Install the Apple Push Certificate	45
Step 10: Install IIS Website	46
Step 11: Install Windows Services	46
Step 12: Synchronize the MongoDB and SQL Server Databases	47
Step 13: Obtain Licenses	47
Unlocking Files	48
Testing Connections to the Web Server	49
Test connection to Mongo DB Server	49
Test Connection to RabbitMQ	49
Test Connection to SQL Server	50
System Sanity Testing and General Troubleshooting	51
Additional Troubleshooting	52
Monitoring Servers in the NowForce Three Servers Solution	54
All Servers	54
Web Server	54
SQL Server	54
Port Usage in NowForce	55
Ports in NowForce Server	56
Ports in NowForce Dispatcher	57
Required Hosts in NowForce Server and Dispatcher	58

Summary of Changes

Version 6.2.2 - October 2023

- Added the requirement to obtain installation zip file in "Prerequisites" (page 7).
- Added the requirement to download .NET 6.0 in "Prerequisites" (page 7).
- Clarified the NTFS formatting in "Prerequisites" (page 7).
- Added a step for the C:/NowForce folder in "Step 1: Extract the Installation Files" (page 9).
- Updated the steps in the section "Step 2: Confirm and Configure Disk Bytes Per Cluster" (page 10).

Version 6.1 - January 2023

- Added a link to the Symphia NowForce Google Map License Model Application Note in "Prerequisites" (page 7).
- Document rebranded to new company Intellicene.

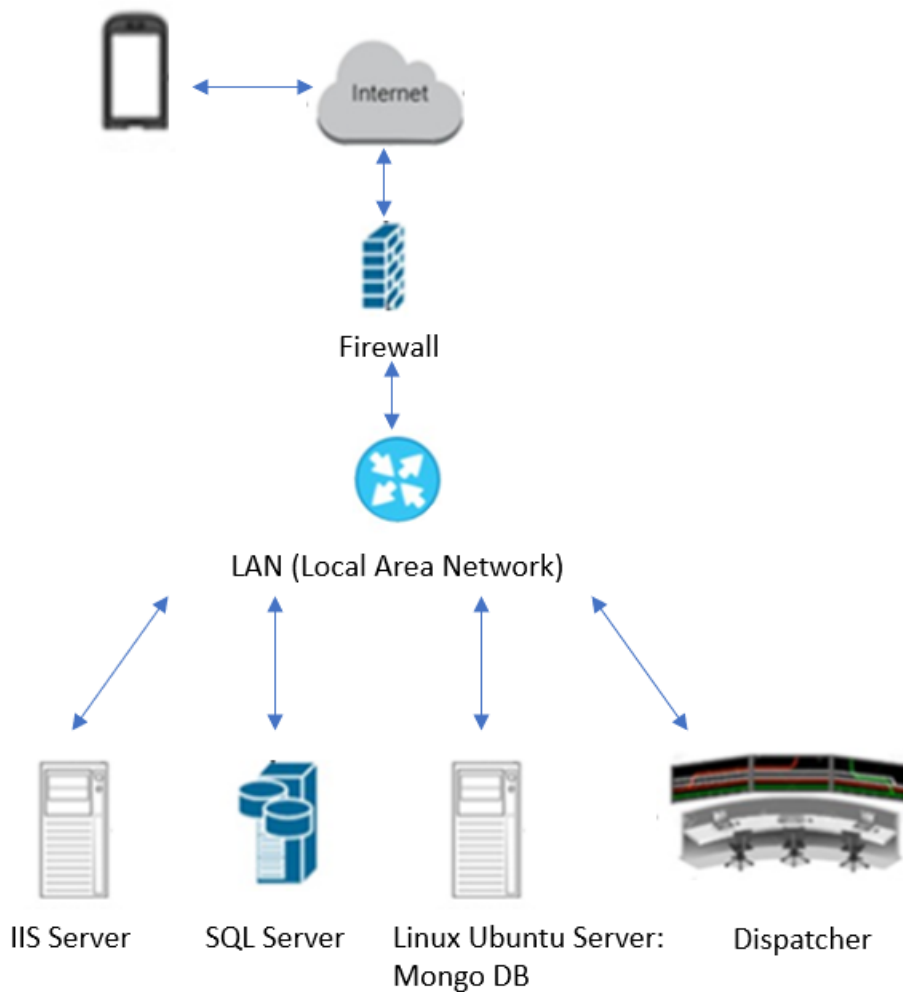
Overview

This guide provides guidelines on how to prepare for and install a Symphia NowForce environment on 3 machines. It explains what the components are, the required order to perform the installation steps, and other related tasks. You must complete all steps for a successful installation.

It is very important that the machines used in the deployment meet the minimum requirements that are listed in the [Symphia NowForce Customer-Furnished Equipment Guide](#).

Components in a Symphia NowForce Three Server Deployment

The following graphic displays the components in the three server environment.



Prerequisites

The following table contains the prerequisites to successfully deploy Symphia NowForce.

Prerequisite	Description
Installation zip file	Obtain the most recent Nowforce installation zip file from your Symphia NowForce contact. For more information, see "Step 1: Extract the Installation Files" (page 9).
Microsoft Windows Server 2019 standard edition (or higher) that will host Microsoft SQL Server 2019 Standard or higher .	<ul style="list-style-type: none"> • Server volumes should be formatted to NTFS 65536 Bytes Per Cluster. For more information, see "Step 2: Confirm and Configure Disk Bytes Per Cluster" (page 10). • The disks and partition sizes required are: <ul style="list-style-type: none"> • C - 100GB for the operating system • D - 500GB for database data • E - 300GB for database logs • F - 100GB for Temp database • G - 700GB for database backups • H - 100 GB for system database • Microsoft SQL Server License. For more information, see the SQL Server Standard per Core License section of the Symphia NowForce Customer-Furnished Equipment Guide.
Microsoft Windows Server 2019 standard edition (or higher) that will host Microsoft IIS Web Server.	<ul style="list-style-type: none"> • .NET 6.0 Hosting Bundle must be installed and can be downloaded from .NET 6.0 • .NET framework 4.8 must be installed and can be downloaded from .NET Framework 4.8. • The disk and partition size required is: <ul style="list-style-type: none"> • C - 100 GB for the operating system • D - 100 GB for the application
A single server running Ubuntu 20.04 or higher	<ul style="list-style-type: none"> • Hosts MongoDB (primary), Node.js, Grafana, and RabbitMQ. • Ubuntu server should contain two volumes: <ul style="list-style-type: none"> • 100GB for the operating system • 300GB for applications and data
Relevant ports should be	For more information, see "Port Usage in NowForce" (page 55).

Prerequisites

Prerequisite	Description
open on the firewall and/or the servers	
Google Maps account	A Google Maps account and a Google Maps Key. See the Symphia NowForce Google Map License Model Application Note for details on purchasing and applying a Google Maps account and Key.
An NServiceBus license (for the Webserver)	This is included in the Installation zip file. After the completion of "Step 1: Extract the Installation Files" (page 9), the license can be found at the file path, C:\NowForce\Installer\Prerequisites\NServiceBus . If you cannot locate the license, contact the NowForce Support team.
Certificates for the website	<ul style="list-style-type: none">• SSL certificates for the website.• A push certificate for Apple (part of IIS installation). <div style="background-color: #e0f2f7; padding: 5px;"><p>Note If this is not a white label deployment, certificates should be requested from the NowForce Support team.</p></div>
OpenTok key	This should be requested from the NowForce Support team.
At least two valid external facing IP addresses	Server hosting Node.js chat.
Domain Name Service (DNS) records	Domain Name Service (DNS) records for: <ul style="list-style-type: none">• Dispatcher• Chat/TCP service• Grafana
Domain names	Domain names should be created for the Internet Web server and the Node.js Chat server. This should be requested from the NowForce Support team.
An SMTP account	If you do not intend on sending email messages from the NowForce account, you should create an SMTP account.

Prerequisite	Description
Configure timezone on all servers	<p>Caution</p> <p>Ensure that the time zone on all NowForce servers is set to (UTC) Coordinated Universal Time.</p> <p>On the Ubuntu server, run the following command to set the time zone to UTC:</p> <pre>sudo timedatectl set-timezone UTC</pre>

For more detailed information on supported hardware and operating system specifications, see the [Symphia NowForce Customer-Furnished Equipment \(CFE\) Guide](#).

Step 1: Extract the Installation Files

The installation requires the use of templates and script files which are packaged in an **Installer.zip** file. These files should be copied to a folder that can be accessed by both the IIS and SQL servers.

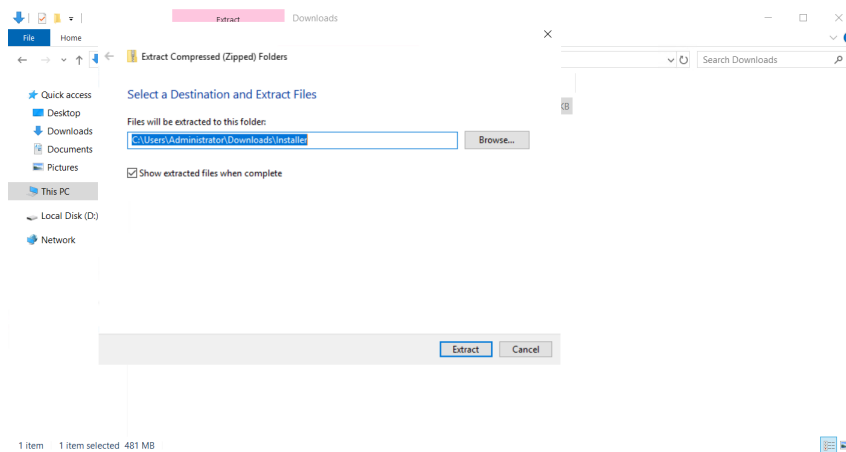
Caution

It is important that you retain the structure of the extracted zip files, so that the scripts will recognize the relative parts and run properly.

▼ To prepare the installation templates and scripts

1. Create the **C:\NowForce** folder if it does not yet exist.
2. Extract all files to the IIS server retaining the directory structure as follows:
 - a. In the Downloads folder, right-click the **Installer.zip** file, and click **Properties**.
 - b. In the General tab, in the Security field, select the **Unblock** checkbox and click **OK**.
 - c. Right-click the **Installer.zip** file, and click **Extract All**.
 - d. Click **Browse...**, select **C:\NowForce** as the folder location to save the extracted files,

click **Select Folder**, and click **Extract**.



3. Open PowerShell ISE as the administrator, as described in "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)
4. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **UnzipFiles.ps1** script to the Powershell ISE window.
5. Press **F5** to run the command.
6. In the PowerShell ISE window, at the Insert installation path prompt, type the folder path that contains the extracted **Installer** folder (for example, **C:\NowForce**). The file path must contain all the folders above the level of the **Installer** folder, but not the **Installer** folder itself.
7. Press **ENTER**.
8. Verify in the Powershell ISE console that the script ran successfully.

Step 2: Confirm and Configure Disk Bytes Per Cluster

To improve SQL Server performance, it is important that all disks or partitions on the SQL server are configured with 65536 Bytes per cluster.

The steps below describe how to ensure that the disk partitions are correctly configured.

Note

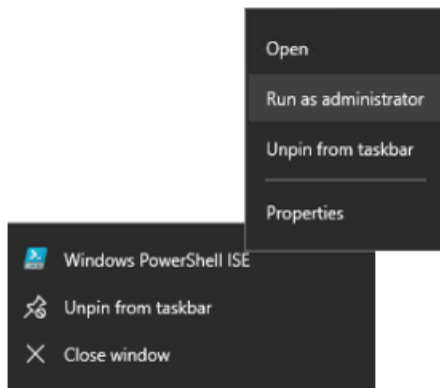
Data disks should be formatted with the NTFS file system.

- ▼ To verify and configure bytes per cluster on the SQL server

Caution

Data that exists on the drive will be deleted.

1. On the SQL Server, in the Windows taskbar, type **Powershell**, and right-click **Windows PowerShell**.



2. Click **Run as administrator**.
3. For every drive that is used for SQL, paste the following command:

```
Format-Volume -DriveLetter D -AllocationUnitSize 65536 -FileSystem NTFS
```

Note

Before running the command for each drive, replace the **D** with the relevant drive.

4. Press **F5** to run each command.
5. To confirm that the disk drives were formatted correctly, paste the following command:

```
Get-CimInstance -ClassName Win32_Volume | Select-Object Name, FileSystem, Label, BlockSize | Sort-Object Name | Format-Table -AutoSize
```

6. Press **F5** to run the command.
7. Confirm that the results display NTFS 65536 for each SQL drive.

Name	FileSystem	Label	BlockSize
C:\	NTFS		4096
D:\	NTFS		65536
E:\	NTFS		65536
F:\	NTFS		65536
G:\	NTFS		65536
H:\	NTFS		65536
I:\	NTFS	Reserved by the System	4096

Step 3: Open Ports

Open the following ports on the SQL server and on the IIS server firewall, and on any external firewall:

▼ To open ports on the IIS server

1. Open PowerShell ISE as the administrator, as described in "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)
2. From the C:\NowForce\Installer\InstallationScripts folder, drag the **OpenPorts.ps1** script to the Powershell ISE.
3. Press **F5** to run the command.
4. Verify in the Powershell ISE console that the script ran successfully.

▼ To open ports on the SQL server

1. From the IIS Server, C:\NowForce\Installer\InstallationScripts folder, copy the **OpenPorts.ps1** script and paste the script in a designated folder or on the desktop of the SQL server
2. Open PowerShell ISE as the administrator, as described in "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)
3. On the SQL server, from the designated folder or desktop , drag the **OpenPorts.ps1** script to the Powershell ISE window.
4. Press **F5** to run the command.
5. Verify in the Powershell ISE console that the script ran successfully.

Step 4: Add Domain Name to Hosts

Caution

A domain name must be used. Do not use localhost, as this will cause the installation to fail.

1. On the IIS server, open PowerShell ISE as the administrator.
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **AddDNSToHosts.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.

4. In the PowerShell ISE window, at the prompt, **Enter a new local DNS for the hosts file**, type the domain name of the application (for example `Example.Nowforce.com`) and press **ENTER**.
5. Verify in the Powershell ISE console that the script ran successfully.

3rd Party Installation Prerequisites

This section provides the steps to install 3rd party software for the Symphia NowForce deployment.

Step 1: Install .NET Framework 4.8

▼ To download and install the Developer pack framework 4.8

1. On the IIS server, download .NET Framework 4.8 from <https://dotnet.microsoft.com/en-us/download/dotnet-framework/thank-you/net48-developer-pack-offline-installer>.
2. Run the **ndp48-devpack-enu.exe** file.
3. On the License terms screen, accept the license terms and click **Install**.
4. When the installation is complete, restart your computer.

Step 2: Install Microsoft SQL Server 2019 Standard

As a prerequisite to installing Symphia NowForce and its related components, you must prepare:

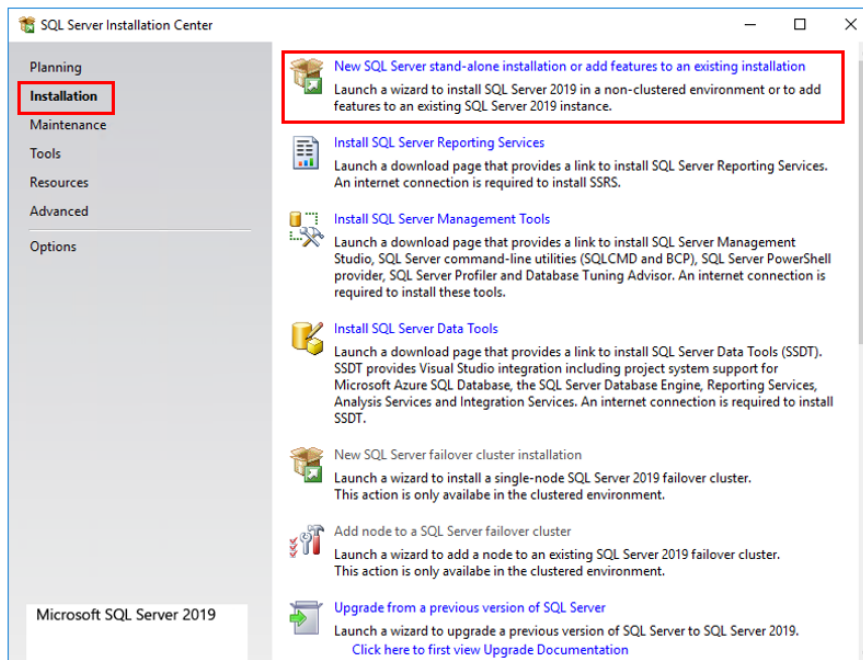
- A Microsoft® SQL Server® 2019 Standard or higher with the latest cumulative patch installed.
- Partitions/Volumes should be NTFS and formatted to 65536 Bytes Per Cluster. For more information see, "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)

Note

- For better performance and order, it is recommended that you create an MSSQL*<DATATYPE>* folder on different partitions/ volumes and store different types of data on different volumes. Name each folder according to the type of data that it stores. For example SQL Data might be stored in D:\MSSQL\DATA, Logs might be stored in E:\MSSQL\LOGS and so on.
- For more information on hardware and software requirements and Microsoft SQL licensing details, see the [Symphia NowForce Customer-Furnished Equipment Guide](#).

▼ To download and install SQL Server 2019 Standard Edition

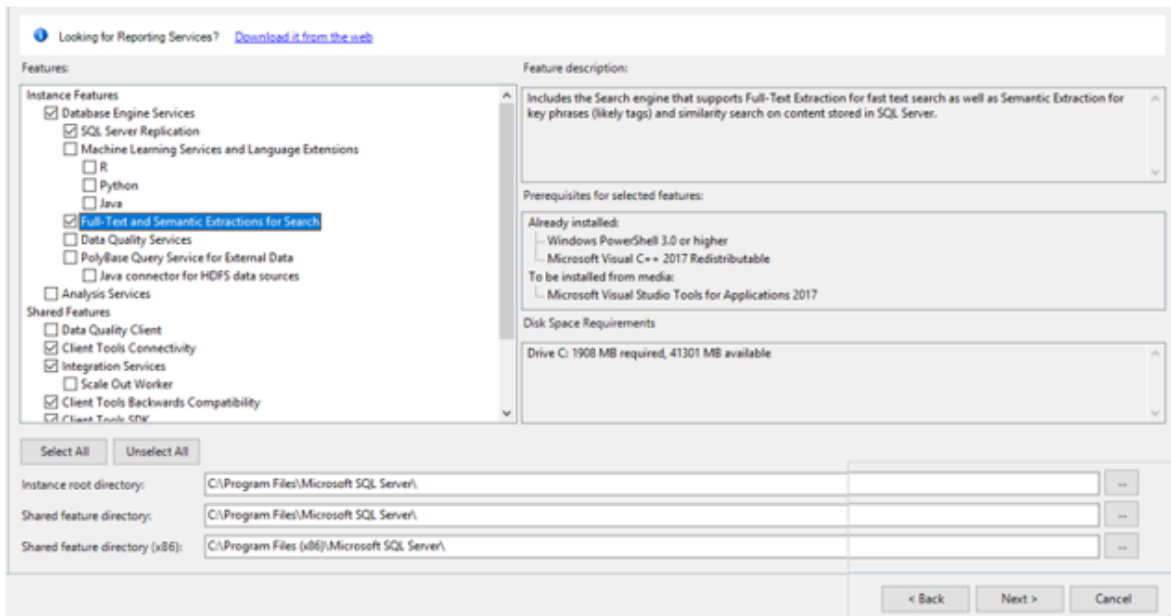
1. Log in to the SQL server computer as an administrator.
2. Navigate to the folder/ mounted drive containing the SQL Server 2019 Standard Edition installation files, right-click **setup** and select **run as administrator**. If necessary, in the User Account Control dialog box that opens, click **Yes** to allow the program access to your machine.
3. On the Select an installation type screen, click **Custom**.
4. On the Specify SQL Server media download target location screen, select a location and click **Install**.
5. On the SQL Server Installation Center screen, click **Installation**, and then select **New SQL Server stand-alone installation or add features to an existing installation**.



6. On the Installation Type screen, click **Next**.

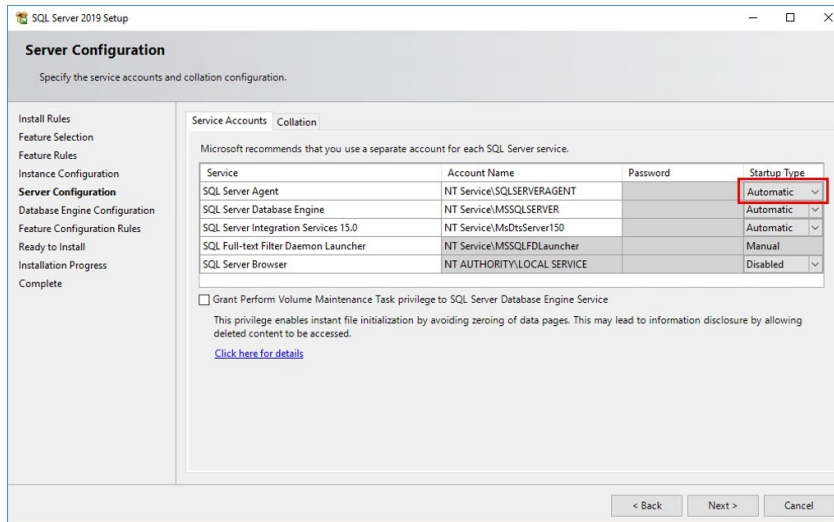
Step 2: Install Microsoft SQL Server 2019 Standard

- On the Product key screen, enter your product key and click **Next**.
- On the License terms screen, accept the license terms and click **Next**.
- On the Microsoft Update screen, if required, select **Use Microsoft Update** checkbox to ensure that the latest Microsoft Windows updates are included , and click **Next**.
- On the Feature Selection screen, select the following features, clear the others, and click **Next**:

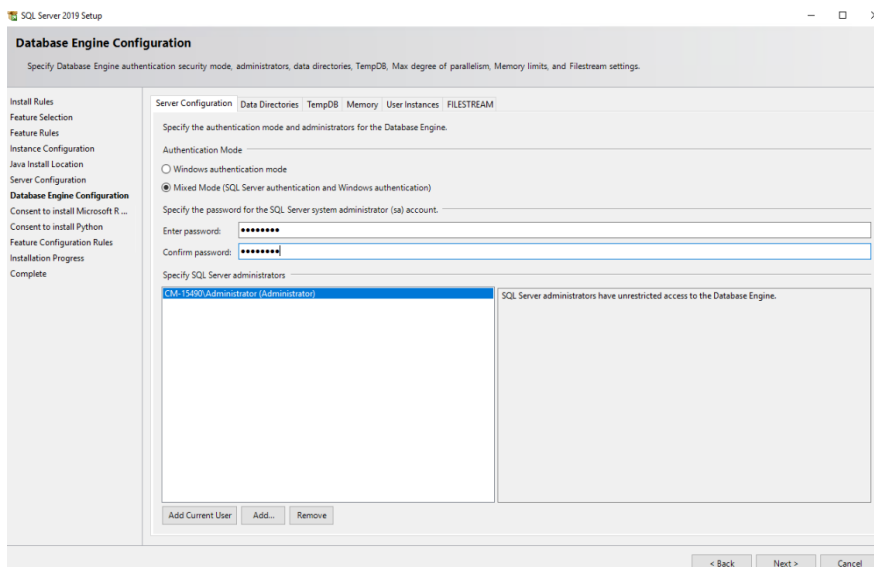


- Database Engine Services.
 - SQL Server Replication.
 - Full-Text and Semantic Extractions for Search.
 - Client Tools connectivity.
 - Integration Services.
 - Client tools Backwards Compatibility.
 - Client Tools SDK.
- On the Feature Rules screen, click **Next**.
 - On the Instance Configuration screen, in the Named instance box, type **SQLExpress_NF** and click **Next**.

13. On the Server Configuration screen:
- In the Service Accounts tab, change the **Startup Type** for **SQL Server Agent** to **Automatic**.



- In the Collation tab, leave the selected collation as **SQL_Latin1_General_CP1255_CI_AS**.
 - Click **Next**.
14. On the Database Engine Configuration screen, in the Server Configuration tab:



- Select **Mixed Mode (SQL Server authentication and Windows authentication)** as the Authentication Mode.

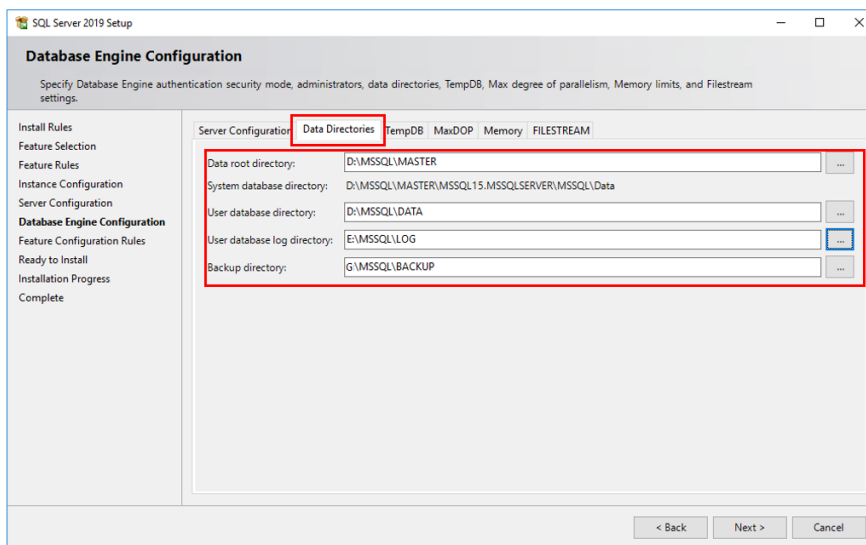
Step 2: Install Microsoft SQL Server 2019 Standard

- b. In the **Password** box, type a strong password for the SQL Server system administrator (SA) account.
- c. Re-enter the password to confirm it.
- d. Click **Add Current User** to add the new admin user.

Tip

Take note of the user name and password, as you may need to enter this information in further installations.

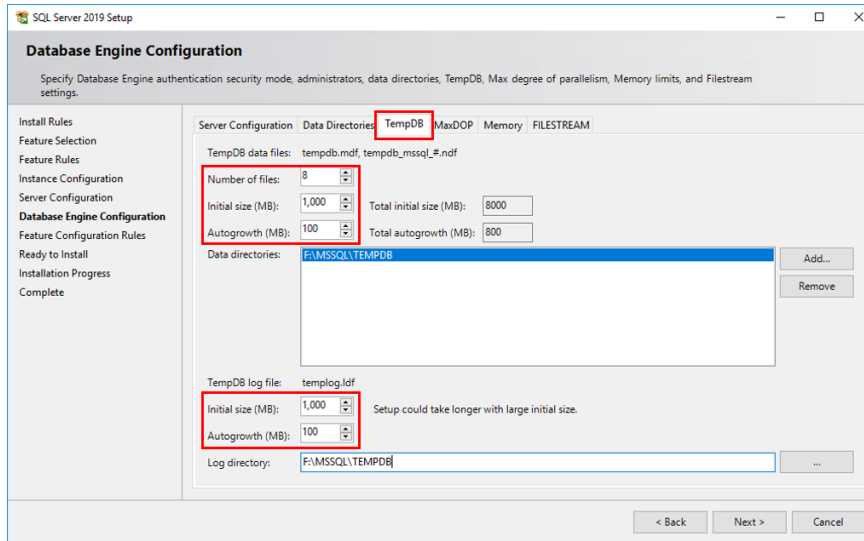
15. On the Database Engine Configuration screen, click the **Data Directories** tab and define the Data and Log directories:



Note

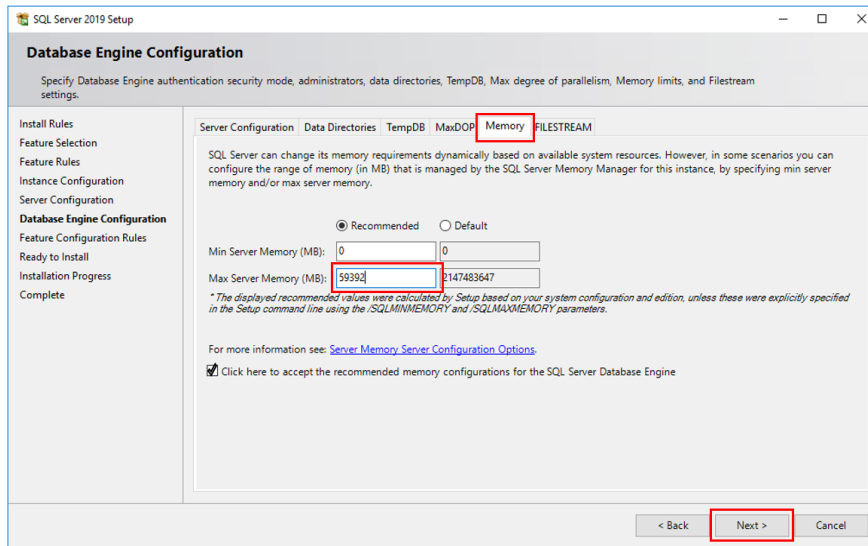
Create the folder paths if not previously created.

- In the **Data root directory** box, select **D:\MSSQL\MASTER**
 - In the **User database directory** box, type **D:\MSSQL\DATA**
 - In the **User database log directory** box, type **E:\MSSQL\LOG**
 - In the **Backup directory** box, type **G:\MSSQL\BACKUP**
16. On the Database Engine Configuration screen, click the **TempDB** tab, and define the TempDB file location as follows:



- a. In the **TempDB data files** area, change the:
 - **Number of files** to 8. (servers having less than 8 CPU cores use the number of cores minus 1)
 - **Initial size (MB)** to 1000.
 - **Autogrowth** to 100.
 - b. In the **Data directories** box:
 - i. Click **Remove** to remove the current location.
 - ii. Click **Add** and change the mapping to **F:\MSSQL\TempDb**.
 - c. In the **TempDB log file** area, change the:
 - **Initial size (MB)** to 1000.
 - **Autogrowth** to 100.
17. On the Database Engine Configuration screen, click the **Memory** tab:

Step 3: Download and Install the Latest Cumulative Pack



- a. Select **Recommended**.
 - b. In the **Max Server Memory** box, assign the value of 4GB less than the amount of memory in the machine.

For example in a machine with 64 GB of memory, assign 60 GB for SQL.
 - c. Select the **Click here to accept the recommended memory...** checkbox.
 - d. Click **Next**.
18. On the Consent screens, accept and click **Next**.
 19. On the **Ready to Install** screen, click **Install**.
 20. When the installation completes successfully, click **Close**.

Step 3: Download and Install the Latest Cumulative Pack

To install the latest updates for the SQL server 2019, download and install the cumulative pack.

▼ To download and install the cumulative pack

1. On the SQL server, download the latest cumulative pack from <https://www.microsoft.com/en-us/download/confirmation.aspx?id=100809>.
2. Run the **SQLServer2019-KB5007182-x64.exe** file. The KB number in the file name varies per release.
3. On the License Terms screen, accept the license terms and click **Next**.

4. On the Select Features screens, click **Next**.
5. On the Consent screens, accept and click **Next**.
6. On the Check Files In Use screen, wait for the check to complete, and click **Next**.
7. On the Ready to update screen, click **Update**.
8. When the update completes, click **Close**.

Step 4: Install SQL Server Management Studio

Download and Install SQL Server Management Studio (SSMS) from the SQL Server Installation Center. SSMS is used to query, design and manage databases and data warehouses.

▼ To download and install the SQL Server Management Studio

1. On the SQL server, in your browser, go to <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>.
2. In the Download SSMS area, click **Free Download for SQL Server Management Studio SSMS**.
3. Run the **SSMS-Setup-ENU.exe** file and click **Install**.
4. If prompted, restart the server.

Step 5: Download and Install the DB Installation Tool

You must use the DB Installation Tool to install the NowForce database on the SQL server.

▼ To download and install the prerequisites for the DB Installation Tool

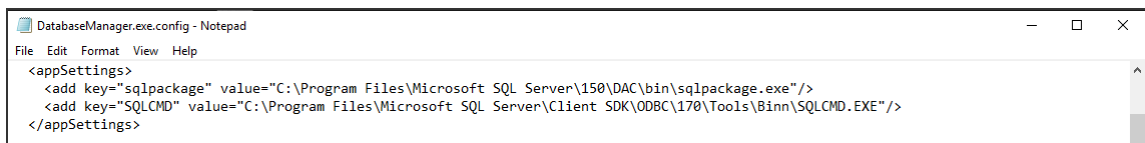
1. On the SQL server, download Microsoft Command Line Utilities 15 for SQL Server Utility from the link, <https://docs.microsoft.com/en-us/sql/tools/sqlcmd-utility?view=sql-server-ver15> and do the following:
 - a. Scroll to the **Download and install sqlcmd** heading, and click **Download Microsoft Command Line Utilities 15 for SQL Server (x64)** to start the download.
 - b. Run the **MsSqlCmdLnUtils.msi** file.

Step 5: Download and Install the DB Installation Tool

- c. On the Welcome screen, click **Next**.
 - d. On the License Agreement screen, accept the terms and click **Next**.
 - e. On the Ready to Install the Program screen, click **Install**.
 - f. When the installation is complete, click **Finish**.
2. On the SQL server, download the Dac Framework SQL Package from the link, <https://docs.microsoft.com/en-us/sql/tools/sqlpackage/sqlpackage-download?view=sql-server-ver15> and do the following:
 - a. In the **Download and install SqlPackage** table, click the **MSI Installer** link to download the **DacFramework.msi** for Windows.
 - b. Run the **DacFramework.msi** file.
 - c. On the Welcome screen, click **Next**.
 - d. On the License Agreement screen, accept the terms and click **Next**.
 - e. On the Ready to Install Microsoft SQL Server Data-Tier Application Framework screen, click **Install**.
 - f. When the installation is complete, click **Finish**.

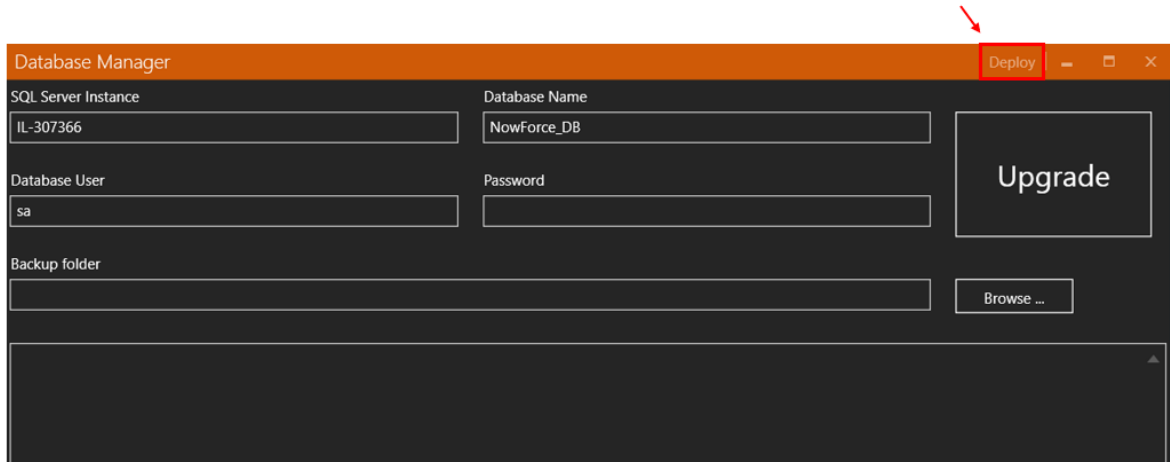
▼ To download and install the DB Installation Tool

1. From the IIS server, copy the **C:\NowForce\Installer\Database** folder and paste the **Database** folder on the desktop of the SQL server.
2. In the **DatabaseManager.exe.config** file, verify the values of folder locations and update if required, as follows:
 - a. From the **Desktop\Database** folder, open the **DatabaseManager.exe.config** file.
 - b. In the appSettings area, the first "add key" value must be **"sqlpackage"**
value="C:\Program Files\Microsoft SQL Server\150\DAC\bin\sqlpackage.exe"/>



```
DatabaseManager.exe.config - Notepad
File Edit Format View Help
<appSettings>
  <add key="sqlpackage" value="C:\Program Files\Microsoft SQL Server\150\DAC\bin\sqlpackage.exe"/>
  <add key="SQLCMD" value="C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\SQLCMD.EXE"/>
</appSettings>
```

- c. In the appSettings area, the second "add key" value must be **"SQLCMD"**
value="C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\SQLCMD.EXE"/>
3. From the **Desktop\Database** folder, run the **DatabaseManager.exe** file.
 4. In the Database Manager window, click **Deploy** to open the DEPLOY DAC PACKAGE window.



5. In the DEPLOY DAC PACKAGE window:

a. In the relevant boxes, type the:

- SQL Server Instance name

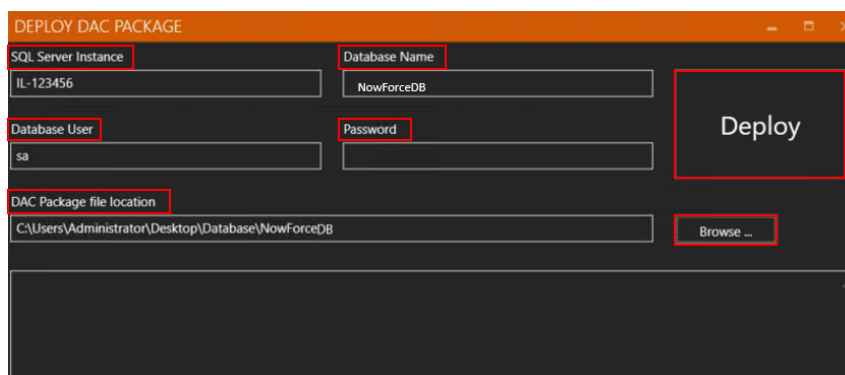
Note

To identify the SQL Server Instance name, launch **SSMS** and in the Server name box, the instance name displays.

- Database Name - Name the database, for example, **NowForceDB**.
- Database User
- Password

Note

The (sa) user and password created in "Step 2: Install Microsoft SQL Server 2019 Standard" (page 14).



b. In the DAC Package file location field, click **Browse...**

- c. In the File Explorer, navigate to the **Desktop\Database** folder and click **NowForceDB.dacpac**
- d. Click **Open**.
6. Click **Deploy**.

A message indicates that the deployment completed successfully. In case of error, check the logs in the **Database\logs** folder.

Step 6: Deploy Microsoft IIS Web Server

In the Symphia NowForce Three Servers installation, deploy and configure a Microsoft IIS Web Server.

▼ To deploy Microsoft IIS Web Server on the IIS server

1. Open PowerShell ISE as the administrator, as described in "Step 2: Confirm and Configure Disk Bytes Per Cluster" (page 10)
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **SetupIISFeatures.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. Verify in the Powershell ISE console that the script ran successfully.

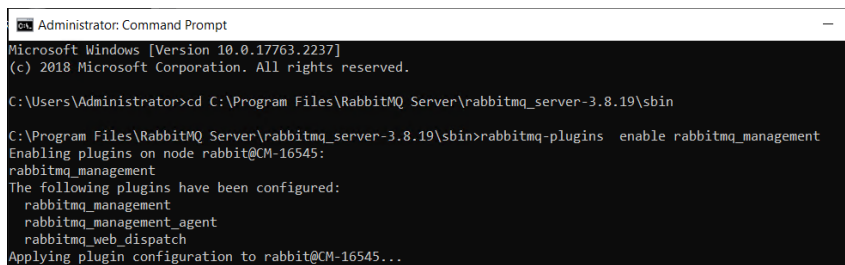
Step 7: Install Rabbit MQ on Windows IIS Server

RabbitMQ is open source message broker software. It accepts messages from producers and delivers them to consumers, acting like a middleman. RabbitMQ is used to reduce loads and delivery times taken by web application servers.

▼ To download and install RabbitMQ

1. On the IIS server, download the latest erlang dependency from https://erlang.org/download/otp_win64_24.0.exe.
2. Run the **otp_win64_24.0.exe** file.
3. On the Choose Components screen, click **Next**.
4. On the Choose Install Location screen, click **Next**.
5. On the Choose Start Menu Folder screen, click **Install**.

6. When the installation is complete, click **Close**.
7. Download RabbitMQ from <https://github.com/rabbitmq/rabbitmq-server/releases/download/v3.8.19/rabbitmq-server-3.8.19.exe>.
8. Run the **rabbitmq-server-3.8.19.exe** file.
9. On the Choose Components screen, click **Next**.
10. On the Choose Install Location screen, click **Install**.
11. When the installation is complete, click **Next**.
12. On the Completing RabbitMQ Server 3.8.19 Setup screen, click **Finish**.
13. Enable the RabbitMQ Management UI:
 - a. Open the Command Prompt and type `cd` followed by the RabbitMQ installation folder path: `C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.19\sbin` and press **ENTER**.



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2237]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.19\sbin

C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.19\sbin>rabbitmq-plugins enable rabbitmq_management
Enabling plugins on node rabbit@CM-16545:
rabbitmq_management
The following plugins have been configured:
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch
Applying plugin configuration to rabbit@CM-16545...
  
```

Note

Verify that the RabbitMQ server version in the file path matches the installed version of RabbitMQ.

- b. At the Command Prompt, type `rabbitmq-plugins enable rabbitmq_management` and press **ENTER**.
14. Add an Administrative user for RabbitMQ:
 - a. Open a new PowerShell ISE window as the administrator. You must open a new Powershell ISE window, and not use a window that is open from previous steps.
 - b. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **AdministrativeRabbitMQ.ps1** script to the Powershell ISE window.
 - c. Press **F5** to run the command.

The script creates the username: **APIUser** and the password: **Verint1!**
15. In your browser, go to **http://<ISServerIPAddress>:15672/** and log in to Rabbit MQ using the above credentials.

Step 8: Install Node.js Chat Server

Node.js manages the Symphia NowForce chat application.

▼ To download and install node.js

1. On the IIS server, in your browser, go to <https://nodejs.org/en/download/>.
2. From the LTS tab, click **Windows installer**.
3. Run the **node-v16.13.1-x64.msi** file and click **Next**.
4. On the License terms screen, accept the license terms and click **Next**.
5. On the Destination Folder screen, click **Next**.
6. On the Custom Setup screen, click **Next**.
7. On the Tools for Native Modules screen, click **Next**.
8. On the Ready to install Node.js screen, click **Install**.
9. When the installation completes, click **Finish**.

Step 9: Install Environment Prerequisites

The Dynamic Compression feature enables the IIS web server to save bandwidth. The following task adds Dynamic Compression to the IIS configuration.

▼ To add dynamic compression

1. On the IIS server, open PowerShell ISE as the administrator.
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **PostIISInstall.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. At the Insert Installation Path prompt, type the folder path for the **Installer** folder (C:\NowForce) and press **ENTER**.
5. Verify in the Powershell ISE console that the script ran successfully.

Installing the NowForce Application

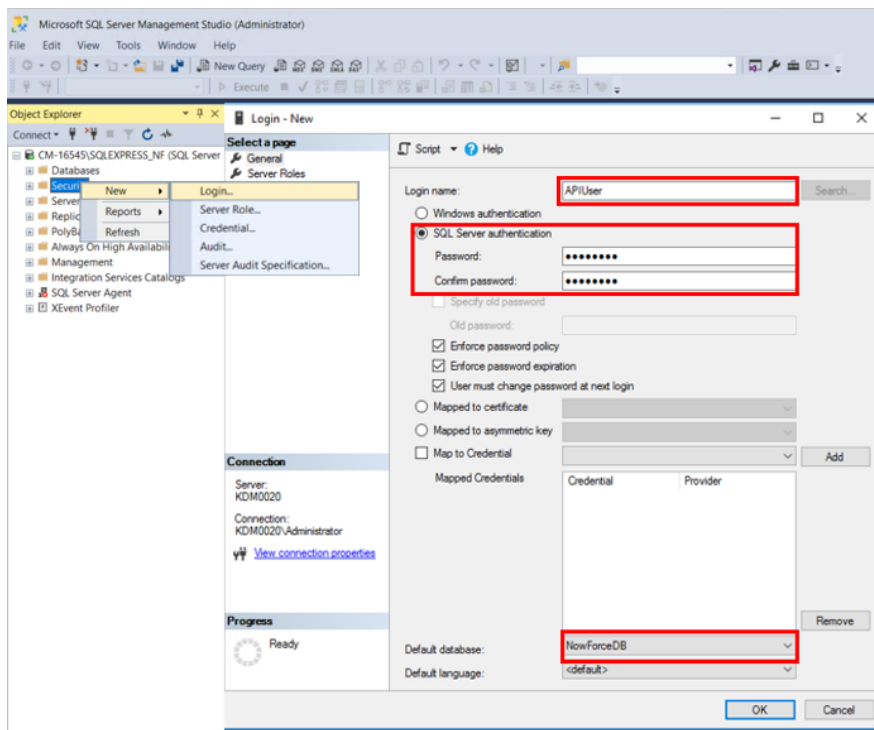
This section describes the steps to install the Symphia NowForce application.

Step 1: Create an SQL User for API Access

You must create an SQL user for API access to the NowForce database.

▼ To create the API user

1. On the SQL server, in the Windows taskbar, type **SSMS**, and then click **Microsoft SQL Server Management Studio 18**.
2. Right click **Security**, click **New** and click **Login....**
3. In the **Login - New** screen:



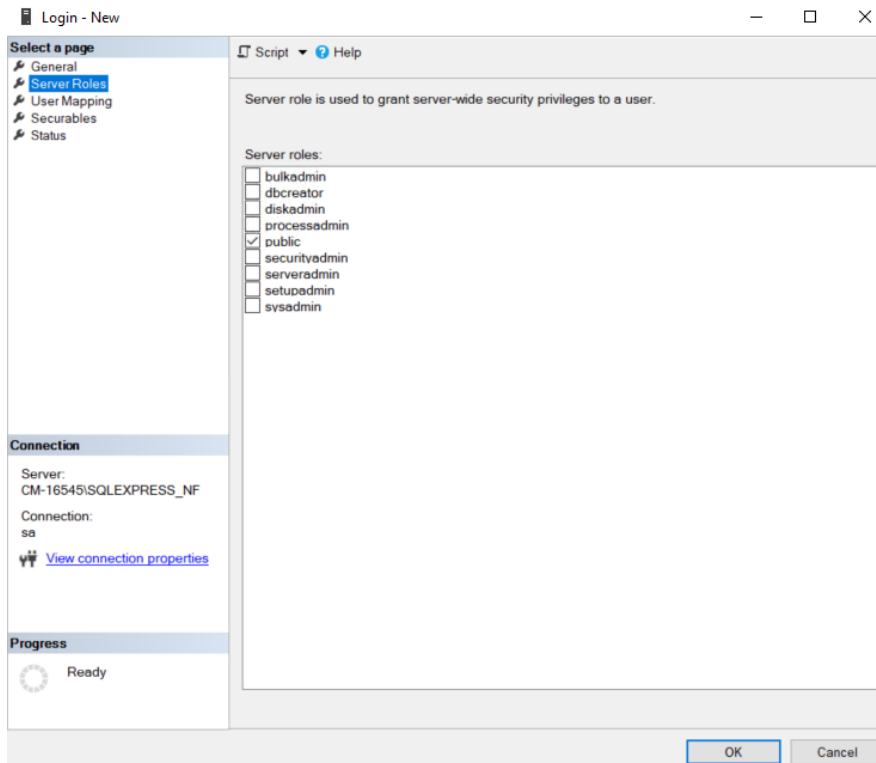
Step 1: Create an SQL User for API Access

- a. Enter the Login name: **APIUser**.
- b. Select **SQL Server authentication**.
- c. Enter and confirm a secure password and save it for use in application configurations.

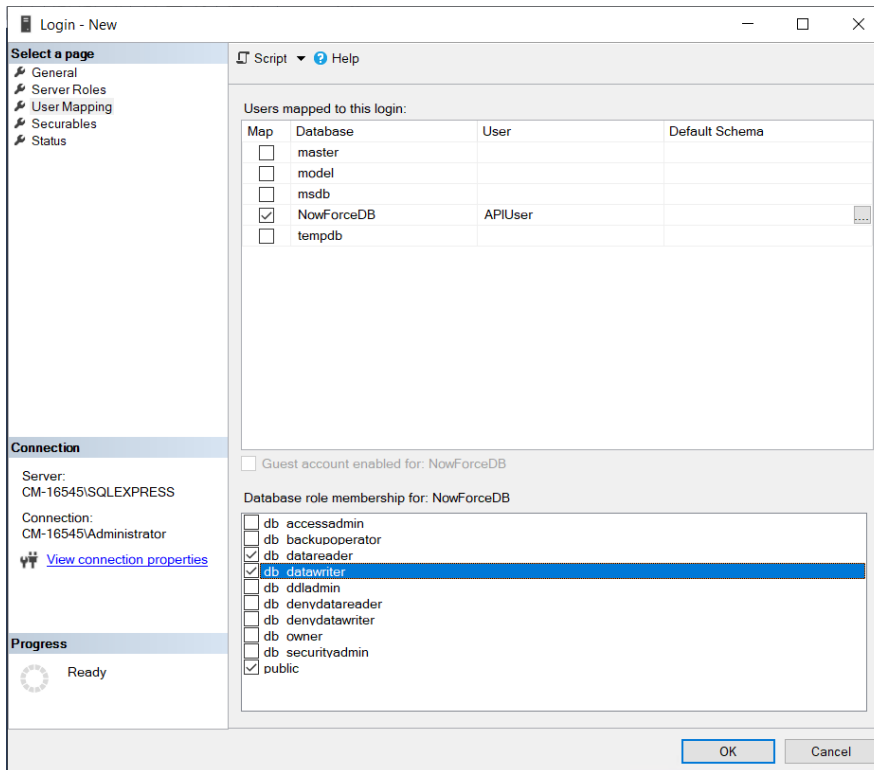
Note

If configured so, you might be required to change your password on your first sign-in.

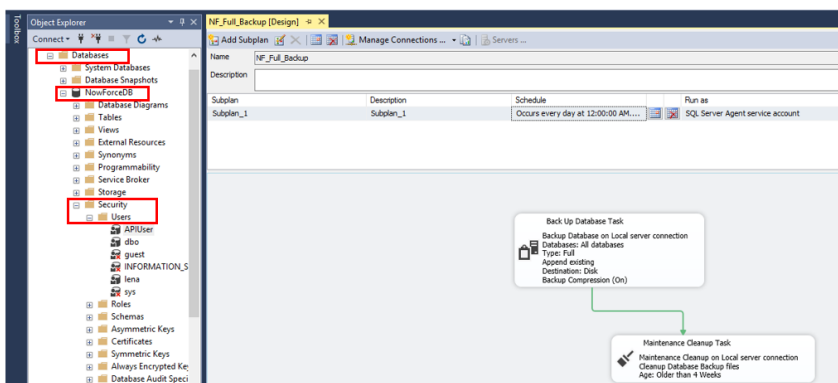
- d. In the Default database box, select **NowForceDB**.
4. In the Server Roles page, select **Public** if not already selected.



5. In the User Mapping page:

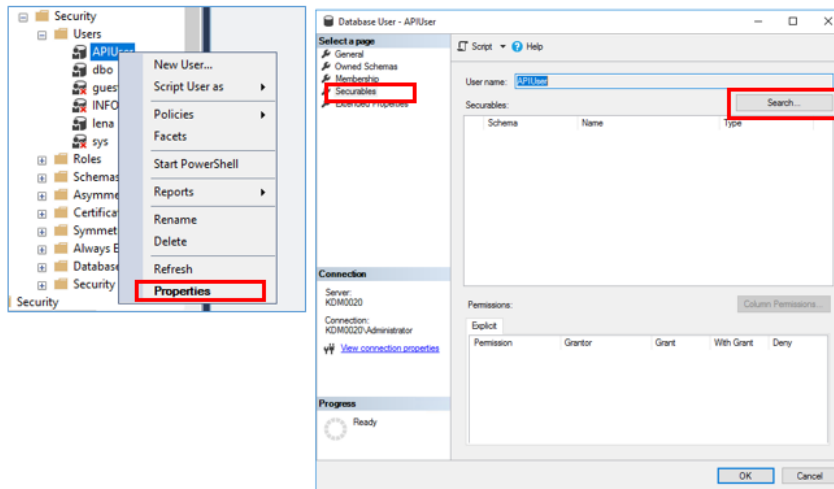


- a. In the Users mapped to this login area, select the **NowForceDB** checkbox.
 - b. In the Database role membership for: NowForceDB area, select the **db_datareader**, **db_datawriter**, and **public** checkboxes.
 - c. Click **OK**.
6. Add Select, Insert, Update, Delete, and Execute permissions for the dbo schema as follows:
- a. In the SSMS Object Explorer, expand **Databases > NowForceDB > Security > Users**.

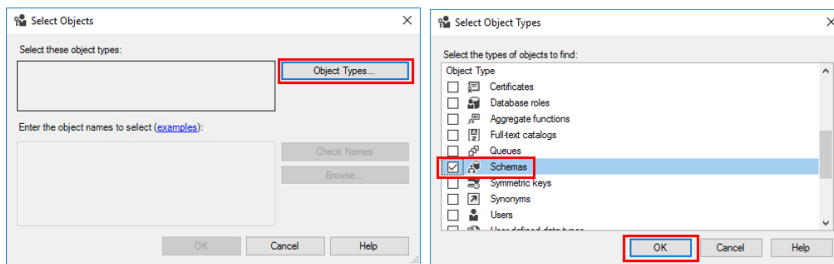


Step 1: Create an SQL User for API Access

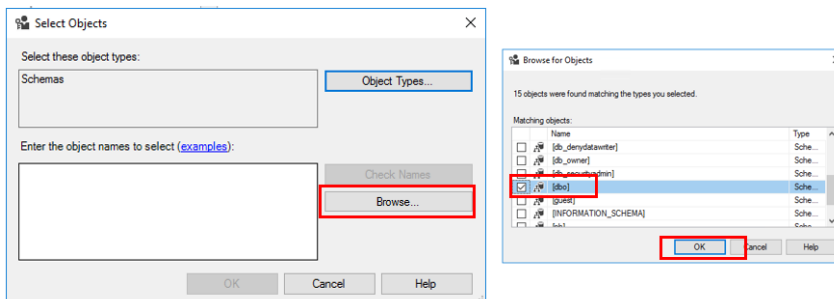
- b. Right-click **APIUser** and click **Properties**.



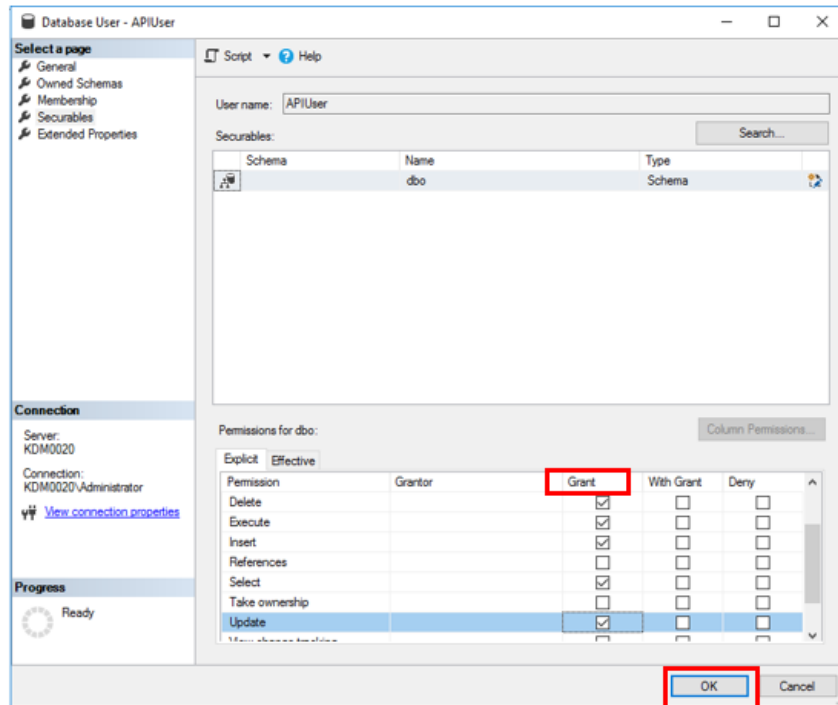
- c. Select the **Securables** page, and click **Search**.
d. In the Add Objects screen, select **Specific Objects**, and click **OK**.
e. In the Select Objects screen, click **Object Types...**, select the **Schemas** checkbox, and click **OK**.



- f. In the Select Objects screen, click **Browse**.



- g. Select the **dbo** checkbox and click **OK** twice.
h. In the Permissions for **dbo** area, in the Grant column, select the **Delete**, **Execute**, **Insert**, **Select** and **Update** checkboxes, and click **OK**.



7. Connect to the Microsoft SQL server with the new user to confirm the user has access to the NowForceDB.
 - a. In the Windows taskbar, type **SSMS**, and then click **Microsoft SQL Server Management Studio 18** to open SSMS
 - b. In the Authentication box, select **SQL Server Authentication**.
 - c. In the Login box, type **APIUser**, and type the password.
 - d. Click **Connect**.
 - e. If the system prompts you to change your password , complete the password change to log in.

NowForceDB is visible in the Databases tree.

Step 2: Configure Web Settings

Configure the web settings with the parameters of the machine.

▼ To configure web settings

1. Open PowerShell ISE as the administrator, as described in "Step 2: Confirm and Configure Disk Bytes Per Cluster" (page 10)

Step 3: Configure an SQL Server Backup Maintenance Task

2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **AddDNSToAppConfig.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. At the command line, enter the following

At the prompt	Type and press ENTER
Enter a new DNS name for the hosts file	The new URL created in " Step 4: Add Domain Name to Hosts " (page 12)
Insert installation path	The folder path containing the Installer folder (C:\NowForce)
Insert Database	The name of the database (NowForceDB)
Insert API User password	The API User password that you configured in the SQL
Insert database instance name	The SQL instance name (SQLEXPRESS_NF)
Insert IIS app IP address	The IP address of the workstation running IIS
Insert MongoDB IP address	The IP address of the workstation running MongoDB (This should be the same IP address as the previous.)

5. Verify in the Powershell ISE console that the script ran successfully.

Step 3: Configure an SQL Server Backup Maintenance Task

It is extremely important that you take regular backups of your databases. Adding a scheduled backup task ensures that backups will be taken at regular intervals.

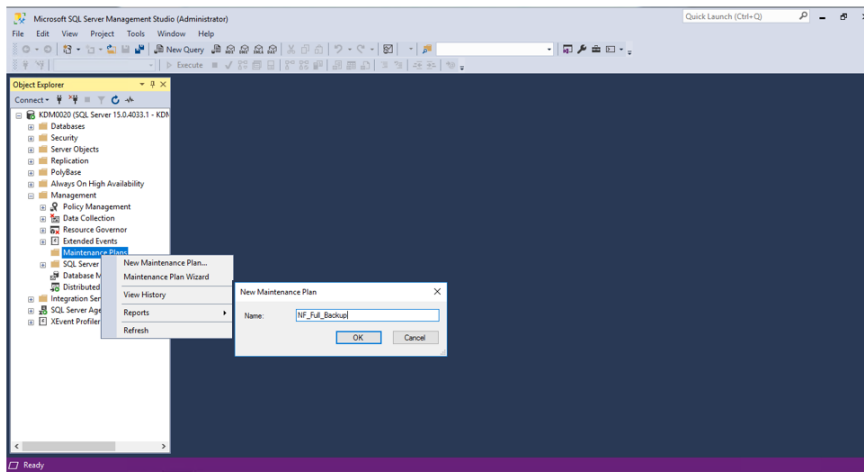
Note

Even with a scheduled backup task, it is important to verify that backup tasks were successful.

▼ To create and configure a backup task

1. On the SQL server, in the Windows taskbar, type **SSMS**, and then click **Microsoft SQL Server Management Studio 18**.
2. Authenticate with the system administrator (SA) credentials created during SQL installation "[Step 2: Install Microsoft SQL Server 2019 Standard](#)" ([page 14](#)), and click **Connect**.

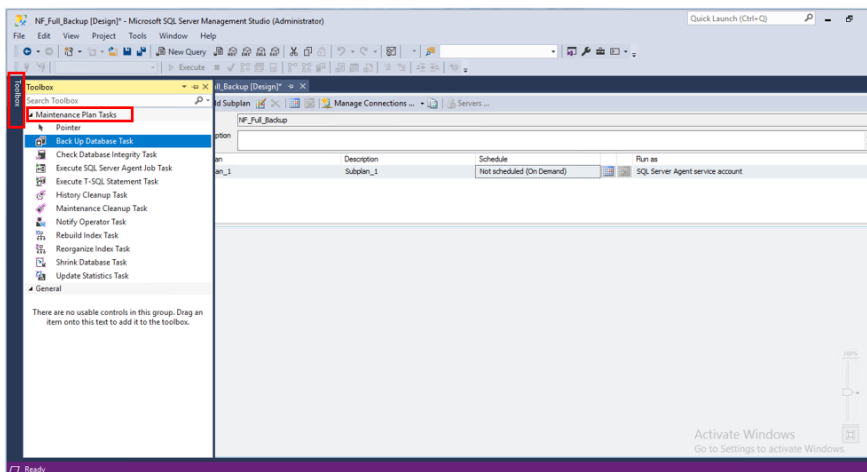
- In the Object Explorer tree, expand **Management**, and then right-click **Maintenance Plans**.
- Select **New Maintenance Plan**, name the plan, such as **NF_Full_Backup** and click **OK**.



- When the design screen appears, click **Toolbox** to the left of Object Explorer, and expand **Maintenance Plan Tasks** when it appears.

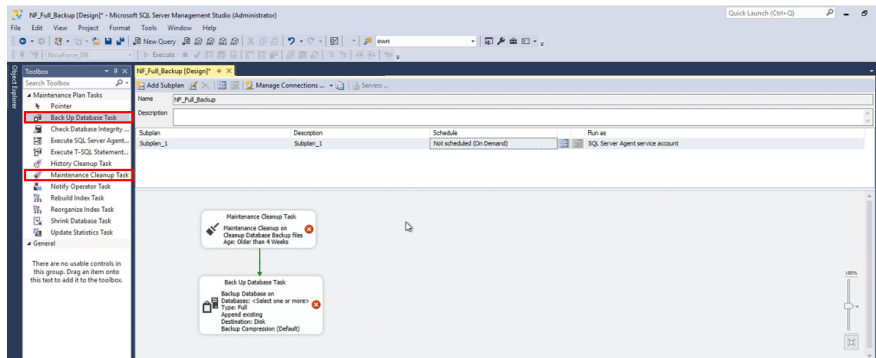
Note

It might take a few seconds to appear.

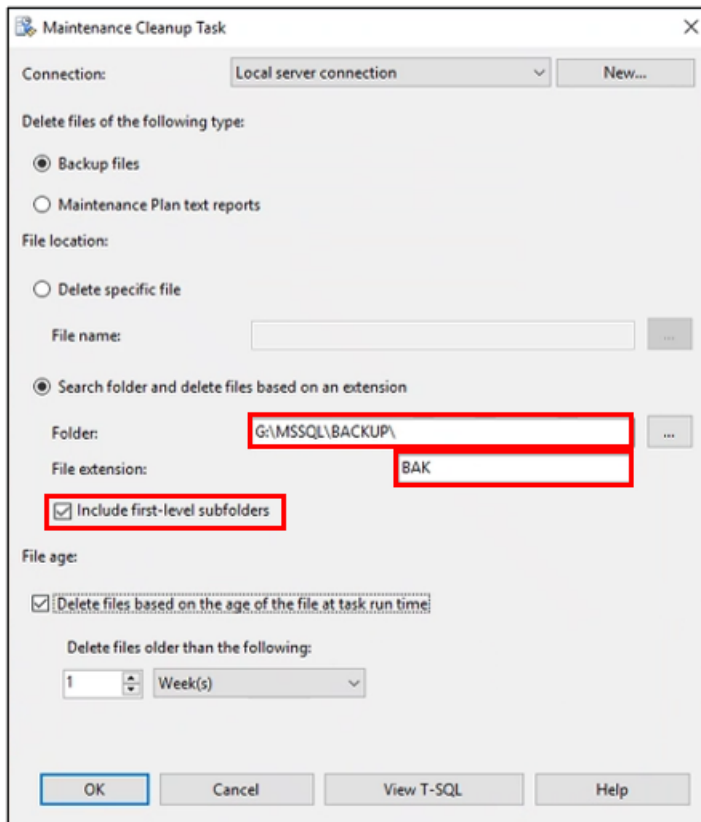



- Select and drag **Maintenance Cleanup Task** to the workspace below the Subplan table.
- Click **Toolbox** again and then select and drag the **Back-Up Database Task** to the workspace below the Subplan table.
- Select the **Maintenance Cleanup Task** rectangle and drag the line to the **Back-Up Database Task**.

Step 3: Configure an SQL Server Backup Maintenance Task



9. Double-click the **Maintenance Cleanup Task** rectangle.
10. In the Maintenance Cleanup Task window, in the **Search folder and delete files based on an extension** area:
 - a. In the **Folder** box, navigate to the backup folder and type a \ (backslash) at the end of the folder path.
 - b. In the **File extension** box, type **BAK**.
 - c. Select the **Include first-level subfolders** checkbox.
11. In the **File age** area, select the **Delete files based on the age of the file at task run time** checkbox.
12. In the **Delete files older than the following** boxes, select **1 Week**.




13. Click **OK**.
14. Double-click the **Back Up Database Task** rectangle.
15. In the Back Up Database Task window, in the General tab:
 - a. The Backup type should be set to **Full**.
 - b. From the Database(s) dropdown menu, select **All databases**, and click **OK**.
 - c. In the **Back up to** box, select **Disk**.
16. In the Back Up Database Task window, in the **Destination** tab:
 - a. Select **Create a backup file for every database**.
 - b. Select the **Create a sub-directory for each database** checkbox.
 - c. In the Folder box, type or select the path for the SQL backup folder.
 - d. In the Backup file extension box, type **BAK**.
17. In the **Options** tab, in the Set backup compression area, select **Compress backup**.
18. Click **OK**.
19. In the Subplan table click the  **Subplan Schedule** icon.

20. In the New Job Schedule window, select the following:
 - a. In the Frequency area, in the **Occurs** box, select **Daily**.
 - b. In the Daily Frequency area, in the **Occurs once at** box, select an off peak time at the site where the server is hosted, for example at night.

The screenshot shows the 'New Job Schedule' dialog box with the following configuration:

- Name:** NF_Full_Backup
- Schedule type:** Recurring
- Enabled:**
- One-time occurrence:** Date: 12/30/2021, Time: 1:43:26 PM
- Frequency:** Occurs: Daily, Recurs every: 1 day(s)
- Daily frequency:** Occurs once at: 12:00:00 AM, Occurs every: 1 hour(s)
- Starting at:** 12:00:00 AM, **Ending at:** 11:59:59 PM
- Duration:** Start date: 12/30/2021, End date: 12/30/2021, No end date
- Summary:** Description: Occurs every day at 12:00:00 AM. Schedule will be used starting on 12/30/2021.

21. Click **OK**.
22. On the main SSMS Toolbar, click the  **Save Selected Items** icon.
23. In the Object explorer Tree, expand **SQL Server Agent** and then expand **Jobs**.
24. Right-click the **NF_Full_Backup** job (or the name you gave to the job), click **Start Job at Step...** and the job runs.
25. Click **Close** to close the job status window.

Step 4: Configure an SQL Server Differential Backup Maintenance Task

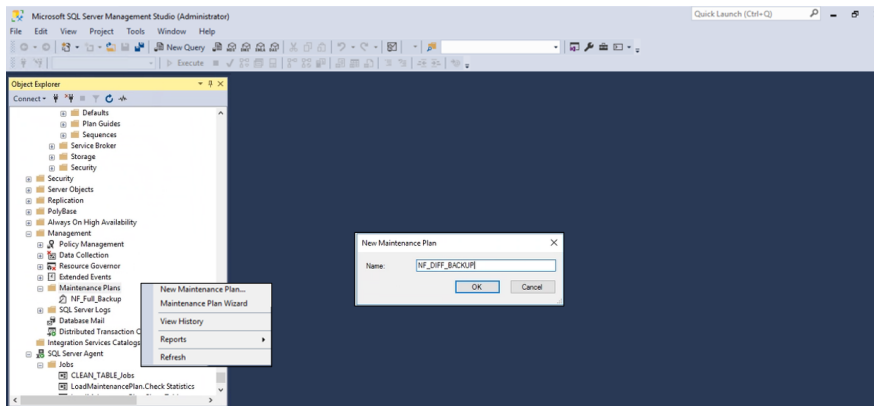
It is important to configure a differential backup maintenance task every hour. The differential backup prevents gaps in storing database data between daily full database backups.

Caution

The configuration for the Differential Backup Maintenance Task appears similar to the configuration of the Full Backup Maintenance Task. It is important to note that the configurations require different selections.

▼ To create and configure a differential backup task

1. On the SQL server, in the Windows taskbar, type **SSMS**, and then click **Microsoft SQL Server Management Studio 18**.
2. Authenticate with the system administrator (SA) credentials created during SQL installation "Step 2: Install Microsoft SQL Server 2019 Standard" (page 14), and click **Connect**.
3. In the folder location **G:\MSSQL**, create the folder **DIFF_BACKUP**.
4. In the Object Explorer tree, expand **Management**, and then right-click **Maintenance Plans**.
5. Select **New Maintenance Plan**, name the plan **NF_DIFF_Backup** and click **OK**.

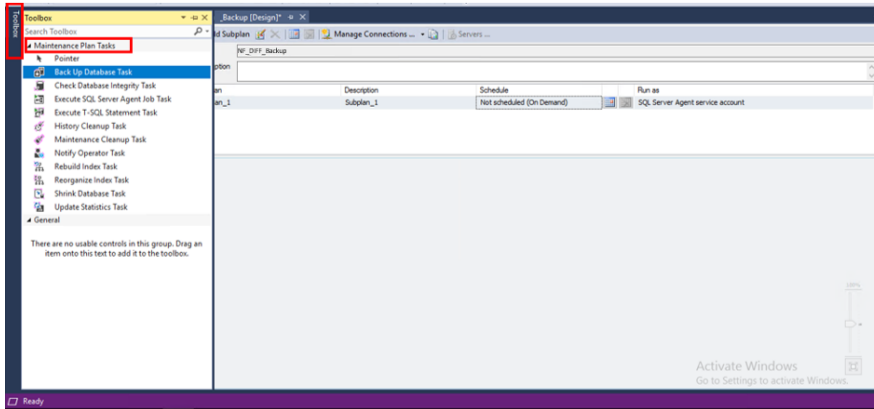


6. When the design screen appears, click **Toolbox** to the left of Object Explorer, and expand **Maintenance Plan Tasks** when it appears.

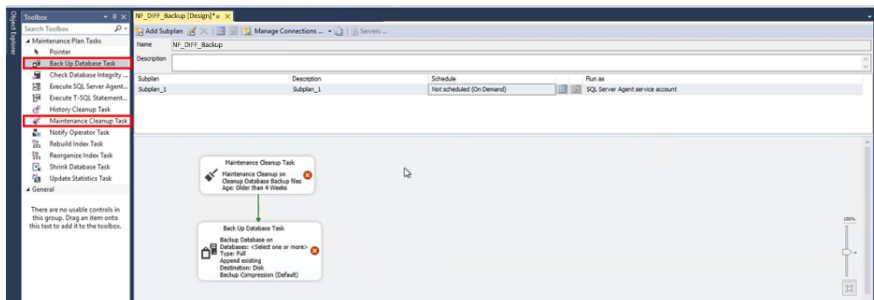
Note

It might take a few seconds to appear.

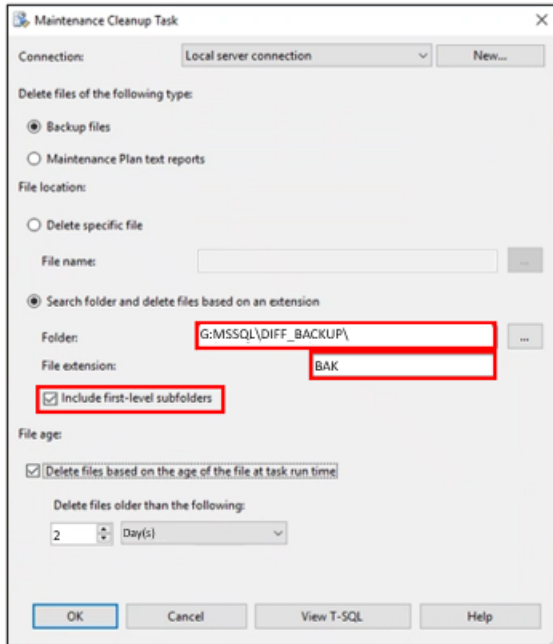
Step 4: Configure an SQL Server Differential Backup Maintenance Task



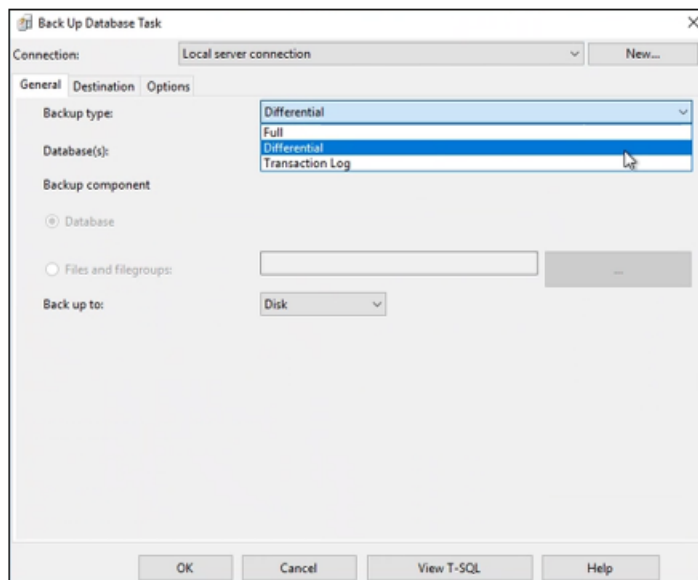
7. Select and drag **Maintenance Cleanup Task** to the workspace below the Subplan table.
8. Click **Toolbox** again and then select and drag the **Back-Up Database Task** to the workspace below the Subplan table.
9. Select the **Maintenance Cleanup Task** rectangle and drag the line to the **Back-Up Database Task**.



10. Double-click the **Maintenance Cleanup Task** rectangle.
11. In the Maintenance Cleanup Task window, in the **Search folder and delete files based on an extension** area:
 - a. In the **Folder** box, navigate to the **DIFF_BACKUP** folder and type **** (backslash) at the end of the folder path.
 - b. In the **File extension** box, type **BAK**.
 - c. Select the **Include first-level subfolders** checkbox.
12. In the **File age** area, select the **Delete files based on the age of the file at task run time** checkbox.
13. In the **Delete files older than the following** box, select **2 Days**.




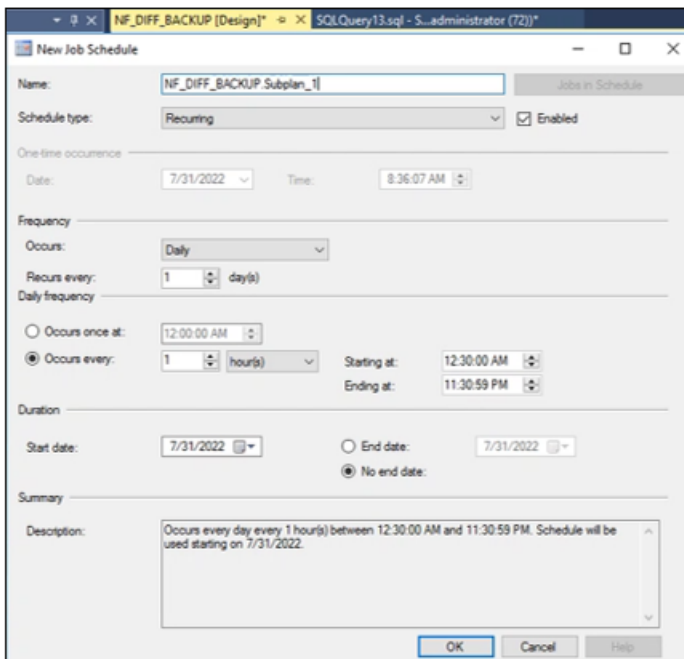
14. Click **OK**.
15. Double-click the **Back Up Database Task** rectangle.
16. In the Back Up Database Task window, in the General tab:
 - a. In the Backup type dropdown menu, select **Differential**.




- b. From the Database(s) dropdown menu, select **All databases**, and click **OK**.
 - c. In the **Back up to** box, select **Disk**.

Step 4: Configure an SQL Server Differential Backup Maintenance Task

17. In the Back Up Database Task window, in the **Destination** tab:
 - a. Select **Create a backup file for every database**.
 - b. Select the **Create a sub-directory for each database** checkbox.
 - c. In the Folder box, type or select the path for the **DIFF_BACKUP** folder.
 - d. In the Backup file extension box, type **BAK**.
18. In the **Options** tab, in the Set backup compression area, select **Compress backup**.
19. Click **OK**.
20. In the Subplan table click the  **Subplan Schedule** icon.
21. In the New Job Schedule window, select the following:
 - a. In the Frequency area, in the **Occurs** box, select **Daily**.
 - b. In the Daily Frequency area, in the **Occurs every** box, select **1 hour(s)**.
 - c. Set the **Starting at** time for an off peak time at the site where the server is hosted, for example at night. Ensure that you select a different time than the previous Job Schedule, for example 12:30.



22. Click **OK**.
23. On the main SSMS Toolbar, click the  **Save Selected Items** icon.
24. In the Object explorer Tree, expand **SQL Server Agent** and then expand **Jobs**.

25. Right-click the **NF_DIFF_Backup** job (or the name you gave to the job), click **Start Job at Step...** and the job runs.
26. Click **Close** to close the job status window.

Step 5: Install MongoDB Using Percona

Percona is a 3rd party tool used for encrypting MongoDB data.

Before installing MongoDB on the Ubuntu server, you must download and install a SSH (Secure Shell Protocol) client application to access the Ubuntu server.

▼ To install MongoDB on the Ubuntu server

Note

In this section, copy each command, paste at the command line, and then press **ENTER** after each command.

For any commands that continue beyond one line of text:

1. Copy and paste the command to a notepad.
2. Fix the command so that it appears on one line.
3. Paste the command into the command prompt.

1. On the Ubuntu server, open the SSH console as an administrator.
2. Run updates on the machine:

```
sudo apt-get update
```

3. Download Percona release packages:

```
$ wget https://repo.percona.com/apt/percona-release_latest.${lsb_release -sc}_all.deb
```

4. Install Percona release packages:

```
$ sudo dpkg -i percona-release_latest.${lsb_release -sc}_all.deb
```

5. Check that the Percona repositories are available:

In the **/etc/apt/sources.list.d/percona-release.list** file check for the Percona repositories.

6. Enable the repository:

```
$ sudo percona-release enable psmdb-50 release
```

7. Update the local cache:

```
$ sudo apt update
```

8. Install the latest version of Percona Server for MongoDB:

```
$ sudo apt install percona-server-mongodb
```

9. Add the encryption:

- a. Open the config file: `$ nano /etc/mongod.conf`
- b. In the **mongod.conf** file, under **security:**, at **enableEncryption:**, type **true**.
- c. At **encryptionKeyFile:**, type **/data/key/mongodb.key**.

```
security:
enableEncryption: true
encryptionKeyFile: /data/key/mongodb.key
```

10. Create the encryption key:

```
$ mkdir /data/key
```

```
$ openssl rand -base64 32 > /data/key/mongodb.key
```

```
$ chmod 600 /data/key/mongodb.key
```

11. Copy the encryption key to a separate server and save a backup at Intellicene.

12. Restart the service:

```
$ sudo systemctl restart mongod
```

13. Set MongoDB to start automatically:

```
$ systemctl enable mongod.service
```

14. Confirm that the service is running:

```
$ sudo systemctl status mongod
```

Step 6: Install a Schema for the Mongo Database on the Ubuntu Server

The following task describes how to install a schema for the MongoDB on the Ubuntu Server.

Before installing the schema for MongoDB on the Ubuntu server, you must download and install a client application to interact with the MongoDB database and run scripts. [NoSQLBooster](#) and

[MongoDB Compass](#), among other MongoDB client tools are available for download on the Internet.

1. On the Ubuntu server, open the command line interface using the preferred MongoDB client application.
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **ClientSupportedVersions** script to the command line interface.
3. Run the command.
4. Verify that the script ran successfully.
5. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **Schemes** script to the command line interface.
6. Run the command.
7. Verify that the script ran successfully.
8. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **UserPermissionApiMapping** script to to the command line interface.
9. Run the command.
10. Verify that the script ran successfully.

Step 7: Configure SQL Transparent Data Encryption (TDE)

Configure SQL TDE to protect data and encrypt the files.

▼ To configure the SQL TDE

Note

Before you begin:

- In this section, copy each command, paste at the command line, and then press **ENTER** after each command.
- For any commands that continue beyond one line of text:
 1. Copy and paste the command to a notepad.
 2. Fix the command so that it appears on one line.
 3. Paste the command into the command prompt.

1. Backup the existing SQL database on the SQL server.
2. On the SQL server, open the Command Prompt as an administrator.
3. Create a Master key:
 - a. `USE Master`
 - b. `GO`
 - c. At `CREATE MASTER KEY [ENCRYPTION BY PASSWORD = 'password']`, replace **'password'** with a strong password containing 12 characters, including letters, numbers, and special characters.
 - d. `GO`
4. Create the TDE certificate:
 - a. `CREATE CERTIFICATE TDECertificate WITH SUBJECT = 'TDECertificate', START_DATE = '4/12/2018', EXPIRY_DATE='4/12/2025'`
 - b. `GO`
5. Backup the TDE certificate:
 - a. `BACKUP CERTIFICATE TDECertificate TO FILE = 'G:\SQLSERVER\CURR\TDECert' WITH PRIVATE KEY (FILE = 'G:\SQLSERVER\CURR\TDECertPrivateKey', ENCRYPTION BY PASSWORD = the password you created above)`
 - b. `GO`
6. Create the database encryption key:
 - a. `USE NowForceDB GO CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256 ENCRYPTION BY SERVER CERTIFICATE TDECertificate`
 - b. `GO`
7. Activate the TDE encryption:
 - a. `ALTER DATABASE NowForceDB SET ENCRYPTION ON`
 - b. `GO`
8. Use the SQL Server Management Studio (SSMS) to backup the database and the transaction log backup.
9. Copy the encryption keys and password to a safe place on another server and save a backup at Intellicene.

Step 8: Configure Node.js Chat Server

Node.js manages the Verint NowForce chat application.

▼ To configure Node.js

1. On the IIS server, in the Windows Explorer, type **cmd**, and select run as administrator to open the Command Prompt as administrator.
 - a. At the command line, type `cd C:\NowForce\Installer\NodeJsServices\Chat` and press **ENTER**.
 - b. At the command line, type `npm install` and press **ENTER**.
 - c. At the command line, type `node server.js` and press **ENTER**.
2. Manually install NSSM.
 - a. In your browser, go to <https://nssm.cc/release/nssm-2.24.zip>.
 - b. In the Downloads folder, right-click the **nssm-2.24.zip** file and click **Extract All**.
 - c. Click **Browse...**
 - d. Select **C:\NowForce** as the folder location to save the extracted files and click **Select Folder**.
 - e. Click **Extract**.
3. Add the Chat application to NSSM.
 - a. Open the Command Prompt.
 - b. Copy and paste the following at the command line: `C:\NowForce\nssm-2.24\win64\nssm.exe install NowForce.Chat "C:\Program Files\nodejs\node.exe" server.js && C:\NowForce\nssm-2.24\win64\nssm.exe set NowForce.Chat AppDirectory "C:\NowForce\Installer\NodeJsServices\Chat`

Caution

In the command line, the `nssm.exe` file path must match the exact file path of `nssm.exe` on your workstation.

- c. Press **ENTER**.

Step 9: Install the Apple Push Certificate

In the case of a White Label, the customer provides the certificate. In other cases, ask Symphia NowForce Support for a certificate.

▼ To install the certificate

1. On the IIS server, open PowerShell ISE as the administrator.
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **InstallCertificates_NowForce.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. At the prompt, type the folder path for the Installer folder (`C:\NowForce`) and press **ENTER**.
5. Verify in the Powershell ISE console that the script ran successfully.

Step 10: Install IIS Website

▼ To install the IIS Services

1. Open PowerShell ISE as the administrator, as described in "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **InstallIISSetup_NowForce.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. At the prompt, type the folder path for the Installer folder (`C:\NowForce`).
5. Verify in the Powershell ISE console that the script ran successfully.
6. In the config file, manually edit the MongoDB value:
 - a. In the File Explorer, navigate to **C:\NowForce\Installer\Web\API\ Web.config**, right-click, and click **Edit with Notepad**.
 - b. Find and update the key "MongoServer" to **mongodb://<MongoDBServerIPAddress>:27017**.
 - c. Find and update the key "MongoDbName" to **NowForceDB**.

Step 11: Install Windows Services

1. On the IIS server, open PowerShell ISE as the administrator, as described in "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **InstallServices.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. At the prompt, type the folder path for the Installer folder (`C:\NowForce`) and press **ENTER**.
5. Verify in the Powershell ISE console that the script ran successfully.

Step 12: Synchronize the MongoDB and SQL Server Databases

After successful completion of the previous steps, synchronize the MongoDB and SQL databases on a web server.

▼ To synchronize the MongoDB and SQL databases

1. On the IIS server, open PowerShell ISE as the administrator, as described in "Step 2: Confirm and Configure Disk Bytes Per Cluster" (page 10).
2. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **Synchronize the MongoDB and SQL Server Databases.ps1** script to the Powershell ISE window.
3. Press **F5** to run the command.
4. Verify in the Powershell ISE console that the script ran successfully.

Step 13: Obtain Licenses

After completing installation steps, obtain NowForce licenses.

1. Contact Verint Systems Inc. support at support@nowforce.com to obtain licenses.
2. Once licenses have been applied by Verint Systems Inc. support, verify that the licenses are correct.
 - a. Log in to NowForce using the default administrative user account, NF_30.
 - b. From the Main screen, click **Settings** and then click **Users**.
 - c. Click **Licenses**.
 - d. Verify that the listed licenses are correct. If licenses are not as expected, contact support@nowforce.com.

Note

You can complete the validation tests using the default administrative user account, NF_30, before obtaining user licenses.

Unlocking Files

If you forgot to unblock the installation files at the start of the installation process, as described in "[Step 1: Extract the Installation Files](#)" (page 9), follow the below procedure to unblock the installation files. After completing the below procedure, you can continue with the installation process without repeating any previous steps.

▼ **To retroactively unblock installation files**

1. Open PowerShell ISE as the administrator, as described in "[Step 2: Confirm and Configure Disk Bytes Per Cluster](#)" (page 10)
1. From the **C:\NowForce\Installer\InstallationScripts** folder, drag the **UnblockFiles.ps1** script to the Powershell ISE window.
2. Press **F5** to run the command.
3. In the PowerShell ISE window, at the Insert installation path prompt, type the folder path that contains the extracted **Installer** folder (for example, `C:\NowForce`). The file path must contain all the folders above the level of the **Installer** folder, but not the **Installer** folder itself.
4. Press **ENTER**.
5. Verify in the Powershell ISE console that the script ran successfully.

Testing Connections to the Web Server

This topic describes how to verify connectivity between the Web Server and the other server components.

Test connection to Mongo DB Server

Install NoSQLBooster on the Web Server and test connections to the Web Server.

▼ To install NoSQLBooster and check connectivity to the MongoDB server

1. Download NoSQLBooster from <https://nosqlbooster.com/>.
2. In the Connections screen, click **Create** to create a connection to the MongoDB server's IP with the port.
3. Click **Test Connection**, and ensure that the Status is **OK**.
4. Click **Save and Connect**.

Troubleshooting

- Verify that the correct port is specified and that the port to the MongoDB server is open.
- Verify that Mongo service is running.

Test Connection to RabbitMQ

▼ To test connectivity to the RabbitMQ Server

1. Install a Telnet client on Web Server (if not installed yet).
2. In the Windows Explorer, type **cmd**, and select run as administrator to open the Command Prompt as administrator.
3. Type `dism /online /Enable-Feature /FeatureName:TelnetClient` and press **ENTER**.
4. Type `telnet <RabbitMQ server IP> 5672` and press **ENTER**.

Note

Ensure that Telnet connects to the RabbitMQ server.

5. Ensure that RabbitMQ management UI opens.
 - a. In your browser, go to **http://<IISServerIPAddress>:15672/**.
 - b. Login with the RabbitMQ credentials, created during RabbitMQ installation.

Troubleshooting

- Verify you specified the correct port and that the port to the RabbitMQ server is open.
- Verify that RabbitMQ service is running.

Test Connection to SQL Server

▼ To test connectivity to the SQL Server

1. Create a file with a .udl extension.
 - a. Right-click the desktop and navigate to **New > Text Document**.
A new file Text Document.txt is created.
 - b. In the Windows Explorer, search for and open **File Explorer Options**.
 - c. In the View tab, clear the **Hide extensions for known file types** checkbox and click **OK**.
 - d. Right-click the new text document and click **Rename**.
 - e. Change the file extension to **.udl**.
 - f. In the warning message, click **OK**.
2. Double-click the .udl file.
A Data Link Properties box opens.
3. Complete the connection details.
4. Click **Test Connection**.
5. In the Test connection succeeded box, click **OK**.

Troubleshooting

- Check the firewall and ensure all relevant ports are open.
- Ensure that the user has permission to connect to the specified database.

System Sanity Testing and General Troubleshooting

This topic describes some basic sanity procedures that will confirm the NowForce system is up and running correctly.

▼ To perform sanity verification in a NowForce environment

1. Browse to **https://<web domain>/api/en-US/m/GetStatus/xml/30/30**.
 - Verify that valid xml is displayed in the browser. If an error appears:
 - Check that the IIS server can connect to the SQL Server and Mongo databases.
 - Check that the API user used to connect to SQL has permissions to access NowForceDB.
2. Browse to **https://<web domain>/ld**, and verify that the login page opens.
3. Enter the default credentials:
 - a. Username – NF_30
 - b. Password – password

Note


If the login does not work even after a refresh, check the errors table in the SQL NowForceDB for more information.

4. Once logged in to Dispatcher (LD):
 - a. Verify that all the panels open without errors.
 - b. Verify that the map is visible in the Map panel.

Note

If the map is not visible, check with support that the customer domain was added to the Google Maps account.

- c. Open the Settings screen and open panels individually to verify that they load.

- d. Create a user in the Users panel:
 - i. On the top right of the screen, click the  icon.
 - ii. Complete the user details.
 - iii. Click **Save**.
5. Login with the user to the Android Symphia NowForce app:
 - a. Activate SOS.
 - b. Verify that an SOS incident is created in the Dispatcher (LD).
 - c. Verify that video is recorded by mobile and displayed in Incident Management (IM) in **Dispatcher (LD)**.
 - d. Write a message in Chat on the mobile and ensure that the Chat message appears in IM.
 - e. Write a chat message in IM in SOS incident and ensure that the message appears in Mobile.
 - f. Close the SOS incident.
6. Create a new incident in Dispatcher (LD):
 - a. Lock the phone while the mobile user is logged in to the SymphiaNowForce app.
 - b. Dispatch an incident to the mobile user.
 - c. Verify that the incident arrives to the mobile without unlocking the mobile.
 - d. Respond to the incident, such as EnRoute etc.
 - e. Verify that statuses are updated in the Dispatcher (LD) without refreshing the browser.
 - f. Close the incident.
7. Create a new message in Dispatcher (LD):
 - a. Lock the phone while the mobile user is logged in to SymphiaNowForce app.
 - b. Send a message to the mobile user.
 - c. Verify that the message arrives to the mobile without unlocking the mobile.
8. Repeat steps 5 – 7 for iOS SymphiaNowForce app.

Additional Troubleshooting

1. If Incident dispatch or Messages work for Android, but not for iOS.
 - a. Check that the Apple Push certificate is installed on the IIS server.
 - b. In the NowForceDB in MSSQL, in the Organizations Configurations table, check that the value of the ConfigurationId = 21 and the OrganizationId = 30.

- c. Check that the Certificate Friendly name value is accurate.
 - i. In the Windows Explorer, search **Certificates**.
 - ii. Navigate to the Apple Push certificate and double-click to open.
 - iii. In the Details tab, browse to the Friendly name to view the value.
2. If maps are not loading:
 - Verify that the customer domain was added to Google maps account.

Monitoring Servers in the NowForce Three Servers Solution

To ensure that the servers in this solution are working as expected, you should monitor the following items and send alerts when the limits are breached.

All Servers

- CPU – Alert if > 80% for more than 5 minutes.
- RAM – Alert if > 80% for more than 15 minutes. (Except for SQL Server).
- Disk space - Alert if > 80% for more than 30 minutes.

Web Server

- **Rabbitmq– # of messages in queues** – Alert if more than 20 messages.
- **Windows services**
 - **Monitor all “NowForce ... ” services** – Alert if a service is stopped.
- **IIS** – Check application pools are running.
- **IIS** – Check website is running.
- **HTTP** – Keep alive HTTP request every 30 seconds – Alert if no response or HTTP response > 2xx.

SQL Server

- SQL Server services are running.

Port Usage in NowForce

For NowForce system components to function behind a firewall, you must open designated ports on the Windows server firewall and on any external firewall. Consider which applications are used on each workstation, and open the relevant ports.

Note

The network and communication between internal servers must be open on all ports.

Ports in NowForce Server	56
Ports in NowForce Dispatcher	57
Required Hosts in NowForce Server and Dispatcher	58

Ports in NowForce Server

Required and optional ports used on the SymphiaNowForce server are listed in the following table.

Port	Protocol	Source	Destination	Use
443	HTTPS, TCP, and WebSockets	NowForce Web Server IP address and Dispatcher workstation	apiv3.voicelayer.io *.opentok.com *.tokbox.com *.googleapis.com	(Required) Enables outbound communication for use of PTT, video streaming, and location updates.
443	HTTPS, TCP, and WebSockets	All IP addresses Set the IP range to 0.0.0.0/0.	NowForce Web Server IP address	(Required) Enables inbound communication for app users, dispatchers, and integration systems secure access to the NowForce API.
5228, 5229, and 5230	TCP	NowForce Web Server IP address	fcm.googleapis.com *.firebaseio.com	(Optional best practice) Enables outbound communication for sending push notifications to NowForce app users, using Firebase, a Google Push Notification Service. If this port is not used, there is a fallback that is used.
4200	HTTPS, TCP, and WebSockets	All IP addresses Set the IP range to 0.0.0.0/0.	NowForce Web Server IP address and Dispatcher workstation	(Required) Enables inbound secure connection for chat between the mobile app and the dispatcher. Note The port number is defined in the API configuration and can be changed.
4200	HTTPS, TCP, and WebSockets	NowForce Web Server IP address	All IP addresses Set the IP range to 0.0.0.0/0.	(Required) Enables outbound secure connection for chat between the mobile app and

Port	Protocol	Source	Destination	Use
		and Dispatcher workstation		the dispatcher. Note The port number is defined in the API configuration and can be changed.

Ports in NowForce Dispatcher

Required and recommended ports used for Dispatcher are listed in the following table.

Port	Protocol	Source	Destination	Use
443	HTTPS, TCP, and WebSockets	NowForce Web Server IP address and Dispatcher workstation	apiv3.voicelayer.io *.opentok.com *.tokbox.com *.googleapis.com	(Required) Enables outbound communication for use of PTT, video streaming, and location updates.
4200	HTTPS, TCP, and WebSockets	All IP addresses Set the IP range to 0.0.0.0/0.	NowForce Web Server IP address and Dispatcher workstation	(Required) Enables inbound secure connection for chat between the mobile app and the dispatcher. Note The port number is defined in the API configuration and can be changed.
4200	HTTPS, TCP, and WebSockets	NowForce Web Server IP address and Dispatcher workstation	All IP addresses Set the IP range to 0.0.0.0/0.	(Required) Enables outbound secure connection for chat between the mobile app and the dispatcher. Note The port number is defined in the API configuration and can be changed.
3478	UDP	*.opentok.com *.tokbox.com	NowForce Web Server IP address	(Recommended) Enables inbound communication so the

Port	Protocol	Source	Destination	Use
				client can accept incoming video streaming. Using this port enhances video streaming.

Required Hosts in NowForce Server and Dispatcher

In the event that your company security policy does not allow opening ports to all hosts, enable traffic on port 443 for all of the following hosts.

Host	Protocol	Inbound/Outbound	Use
*.nowforce.com	TCP + WebSockets	Inbound / Outbound	Connection to the server's web application for Dispatchers and Mobile App
maxcdn.bootstrapcdn.com	TCP	Inbound	Required resources
*.opentok.com	TCP	Inbound	Video Streaming
*.tokbox.com	TCP	Inbound	Video Streaming
*.gstatic.com	TCP	Inbound	Google Maps GIS service
*.googleapis.com	TCP	Inbound	Google Maps GIS service
*.intercom.io	TCP	Outbound	NowForce Customer Support Widget
*.intercomcdn.com	TCP	Outbound	NowForce Customer Support Widget
*.voicelayer.io	TCP	Inbound and Outbound	The Push To Talk VOIP provider used by the NowForce app
*.widebridgecloud.com	TCP	Inbound and Outbound	The Push To Talk VOIP provider used by the NowForce app from versions 6.2 and later