



Report Manager

Installation Guide

Version 5.0 SP6

Last Updated: Wednesday, May 1, 2024



Contents

Contents	2
System requirements	4
System Requirements	4
Best Practices	4
Supported software	4
N-able Report Manager server version	4
Operating system	4
Database system	5
Applications	5
Supported browsers	5
Installation Prerequisites	6
Microsoft SQL Server Settings	6
Report Manager Environment	6
Secure export over SSH	7
Install and configure server software	8
Configure Microsoft Windows Server for Report Manager	9
Configuring Windows Server 2012, 2012 R2, 2016	9
Configure Microsoft SQL Server for Report Manager	10
Check the Version of an Existing Microsoft SQL Server	11
Add Content Manager and System User roles to Windows user accounts for Server Reporting Services (SSRS) permissions	12
Install and configure .NET Framework	13
Install, upgrade, or migrate Report Manager	14
Install Report Manager	15
Upgrade Report Manager	20
Upgrade Path	20
Upgrade Instructions	20
Migrate Report Manager to a new server	21
Post-installation - Next Steps	24
Add an N-able Report Manager Data Source	25
Configure an N-able Report Manager data source	25
Configure HTTPS and SSL for Report Manager	27




Configure the Report Manager server to use HTTPS connections	27
Configure Internet Explorer to support Mixed Mode Content	27
Add Report Manager Databases to a maintenance plan	29
Grant Access to Report Manager from N-able Report Manager	30
Access Report Manager	31
Access through the Windows Start menu	31
Access through a supported browser	31
Access through N-able Report Manager	32
Grant Access to Reports	33
Monitor Report Manager as a device through N-able Report Manager	34
Download and Install an Agent	34
Apply the Report Manager Service Template	34
How to Use the Report Manager Customer Purge Utility	35
Best Practices	40
Set up credentials to use Report Builder	41
Assign the account the "N-able Custom Report Author" role	41
Set up File Share or Email for Scheduled Reports	43
Set up a File Share	43
Set up SMTP Server Email	43
Assign browser security zones	44
Configure the Data Retention Time Period	45
Troubleshooting	46
Installation: Requirements Checker Troubleshooting	46
Customer Support	47


System requirements

This section describes hardware and software versions required for Report Manager 5.0 SP6.

System Requirements

Item	Minimum Installation Requirements
CPU	Quad Core
RAM	16+GB (minimum 8GB SQL dedicated)
Hard Disk	200 GB free space on a dedicated data partition is required in order for Report Manager to: <ul style="list-style-type: none"> ■ Import data from an N-able Report Manager server that monitors up to 5000 services ■ Retain data for up to one and a half years
 Systems not meeting these requirements will not be able to upgrade.	

Best Practices

 N-able recommends that you periodically review and evenly increase your system specifications, based upon your database administrator's (DBA) recommendations.

- Set up your hardware to include 15K SAS or SDD hard disks, with battery backup and redundancy.
- Install the SQL Server and Databases on separate physical disks from the Operating System.
- Have dedicated physical hardware (not on a virtual machine).
- Have a LAN connection to N-able Report Manager; data transfers to Report Manager will exceed GBs of data daily.

Supported software

Only English versions of software are supported.

Only 64-bit versions of SQL and the Windows operating system are supported.


N-able Report Manager server version

- N-able Report Manager 12.2 SP1 and later

Operating system

Microsoft Windows Server

- 2019 Standard or Enterprise Edition
- 2016 Standard Edition
- 2012 R2 Standard Edition not supported by Report Manager 2022.5+
- 2012 Standard Edition not supported by Report Manager 2022.5+

 Please be aware that Windows Server 2012 cannot connect to N-central 2022.5 or later. If running, or planning to upgrade to, N-central 2022.5 or later, please install Report Manager on Server 2016.


Database system


Microsoft SQL Server

- 2017 Standard or Enterprise Edition
- 2016 Standard or Enterprise Edition
- 2014 Standard or Enterprise Edition
- 2012 Standard or Enterprise Edition with SP2
- 2012 Standard or Enterprise Edition with SP1
- 2012 Standard or Enterprise Edition

Applications


Microsoft IIS

 Do not change the name of your server after installing IIS.

 Do not remove the default website. The default website is needed to successfully install or upgrade Report Manager.

- IIS 10.0 (Windows Server 2016)
- IIS 8.5 (Windows Server 2012 R2)
- IIS 8.0 (Windows Server 2012)

Microsoft .NET Framework 4.7 and later


 If you are using .NET Framework 4.6 and later, you will need to ensure backwards compatibility to lower versions. In Windows Server Manager, you will need to have the .NET Framework 3.5 feature enabled.

Supported browsers

Browsers


- Microsoft Internet Explorer 11.x
- Mozilla Firefox, versions 85.0 and later
- Google Chrome, versions 88.0 and later

Installation Prerequisites

 This guide does not provide any detailed instructions for installing and configuring Microsoft products. References to those procedures have been provided where ever possible.

N-able recommends that you minimize all windows on your desktop while you install Report Manager. Application windows that are open during installation may hide a dialog that requires your input, making it appear that your installation has stalled.

Microsoft SQL Server Settings

 Microsoft SQL Server settings must be configured properly before installing Report Manager or you will have significant issues with installation and scheduled reporting.

See the Microsoft instructions to upgrade, install, or configure Microsoft SQL Server [2012](#), [2014](#), [2016](#), and [2017](#).

The settings below are critical and must be applied in either a new or existing installation, for Microsoft SQL server to work with Report Manager.

- Install the SQL Server as a default instance.
- Select the NT Authority\System account for SQL Server services.
- Select Mixed Mode for Database Engine Configuration.
- Ensure the following Feature Selections are applied:
 - Database Engine Services
 - Reporting Services
 - Integration Services
 - Management Tools - Complete

Report Manager Environment

Before installing Report Manager, ensure the following items have been reviewed and updated:

1. Report Manager must not be installed on a domain controller. During Report Manager installation, a user account is created that must be added to a local user's account group. A domain controller does not have a Local Users and Groups option available and will halt the installation of Report Manager.
2. Report Manager must not be installed on a computer with other applications or share a host with N-able Report Manager. Report Manager runs without limits to resources to process data and will significantly affect other applications installed on a server. The following are some examples of what should **not** be installed on the same server as Report Manager:
 - CRM
 - Sharepoint
 - Exchange Server
 - PSA and ticketing solutions: HDM, ConnectWise Manage, Autotask
 - WSUS
3. Ensure that there is space in Windows Event log. Report Manager will not start if the Windows Application log is full.
 - Check the Windows Application log properties:
 - For the When maximum event log size is reached setting, select Overwrite events as needed (oldest event first).

4. Ensure HTTP is available as a connection to the SQL Server Reporting Services. Report Manager uses HTTP to access SQL Server Reporting Services. See this [Knowledge Base Article](#) for more information.
5. Set the time zone on the Report Manager server. Report Manager will convert ticketing times to local time zones. If the server is not configured to the local time zones, the data collected will be logged incorrectly.

i The Report Manager server must be in the same time zone as the N-able Report Manager server.

6. Set up the Domain Name System (DNS) Server to resolve addresses automatically. N-able recommends setting up your DNS server to resolve addresses automatically. If this is not done, the installation will not stop, but it will stop you from successfully adding a data source to the system.
7. Fully Qualified Domain Name (FQDN). If you are using a FQDN that does not match the local computer name, Microsoft IIS 5.1 or later has a security feature that helps prevent reflection attacks on your computer. If you will be using the FQDN to access the Report Manager server, see the appropriate Microsoft documentation for more information.
8. Ports. Report Manager does not support custom ports. Use only the following ports:
 - HTTP communication—Port 80
 - HTTPs communication— Port 443
 - Firewalls—80, 443, 1433

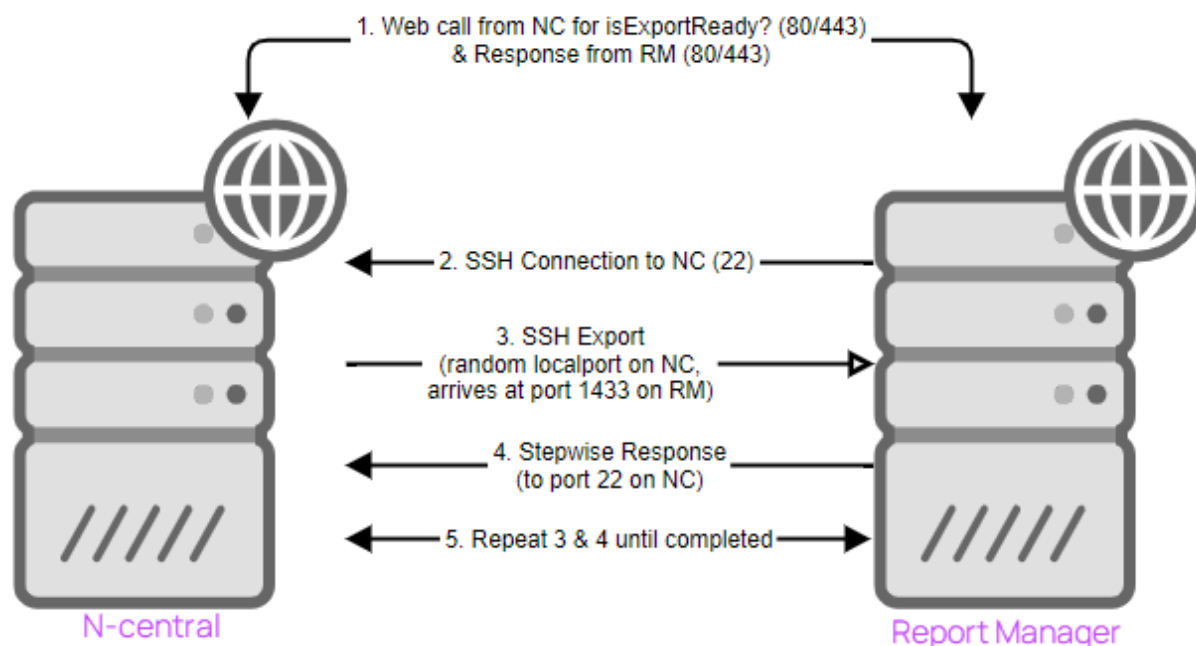
Secure export over SSH

In order to increase security and comply with the California Data Protection Act, N-central 12.2 and higher can Export Data using SSH to Report Manager SP6 and later editions.

⚠ If either N-central or Report Manager is not on a required version, or if port 22 is blocked, the export will continue unencrypted on port 1433.

- Enable port **22** inbound to N-central from Report Manager
- Enable ports **10500-10999** inbound to Report Manager from N-central

The diagram illustrates the connections between N-central (NC) and Report Manager (RM).




Install and configure server software

Windows Server **must** be configured before SQL Server. Typically, you will first configure or update IIS when you set up Windows Server, and then install or configure the .NET Framework.

Links to the Microsoft instructions for installing and configuring Windows Server, SQL Server, IIS, and .NET Framework are provided below.

1. Install and configure Microsoft Windows Server:
 - a. [Review the Windows Server settings](#) that are required for Report Manager, and update those settings if needed.
 - b. Install Windows Server [2012](#) or [2016](#).
 - c. [Install and configure IIS](#).

 Do not remove the default website. The default website is needed to successfully install or upgrade Report Manager.

2. Upgrade, or install and configure Microsoft SQL Server:
 - a. [Review the SQL Server settings](#) that are required for Report Manager, and update those settings if needed.
 - b. If you already have SQL Server, [check that you have the correct version](#).
 - i. See [installing SQL Server 2012](#) for details.
 - ii. See [installing SQL Server 2014](#) for details.
 - iii. See [installing SQL Server 2016](#) for details.
 - iv. See [installing SQL Server 2017](#) for details.
3. [Install and configure the latest .NET Framework](#).


Configure Microsoft Windows Server for Report Manager

Configure Microsoft Windows Server before configuring, installing, or upgrading Microsoft SQL Server.

Before you configure Windows Server, ensure that your version of the Microsoft Windows Server operating system is fully patched and configured to work with Report Manager. Report Manager 5.0 SP6 is compatible with either Windows Server 2012, 2012 R2 or 2016.


The table below provides a complete summary of the Roles, supporting Features or Role Services, and Feature configurations required for Report Manager. See the Microsoft instructions for installing and configuring Windows Server.

Configuring Windows Server 2012, 2012 R2, 2016


Roles	Supporting Features or Role Services	Feature Configuration
Application Server	<ul style="list-style-type: none"> ■ .NET Framework 4.5 ■ COM+ Network Access ■ Web Server (IIS) Support 	<div style="border: 1px solid orange; padding: 5px; margin-bottom: 10px;">  If you are using .NET Framework 4.6 and later, you will need to ensure backwards compatibility to lower versions. In Windows Server Manager, you will need to have the .NET Framework 3.5 feature enabled. </div> <p>.NET Framework 4.5 Features</p> <ul style="list-style-type: none"> ■ .NET Framework 4.5 ■ WCF Services
Web Server (IIS)	<ul style="list-style-type: none"> ■ Management Tools <ul style="list-style-type: none"> ○ IIS Management Console ○ IIS Management Compatibility <ul style="list-style-type: none"> ■ IIS Metabase Compatibility ■ IIS Management Console ■ IIS Scripting Tools ■ IIS WMI Compatibility ○ IIS Management Scripts and Tools ○ Management Service 	

Configure Microsoft SQL Server for Report Manager

Verify the existing version of your [Microsoft SQL Server](#) and review the settings below for Report Manager 5.0 SP6. If required, apply the service packs and upgrade to a new version.

 The Microsoft OLE DB Driver for SQL Server is a mandatory requirement for Report Manager to function. Report Manager will not install without it.


See the Microsoft [download instructions](#), [release notes](#), and [driver announcement](#) for more details.

 The following settings within a SQL server are critical to Report Manager. If these requirements are not met, the installation may not proceed. If installation does proceed, scheduled reporting will not occur.

See the Microsoft instructions to upgrade, install, or configure Microsoft SQL Server [2012](#), [2014](#), [2016](#), and [2017](#).

The settings below are critical and must be applied in either a new or existing installation, for Microsoft SQL server to work with Report Manager.

- Install the SQL Server as a default instance.
- Select the NT Authority\System account for SQL Server services.
- Select Mixed Mode for Database Engine Configuration.
- Ensure the following Feature Selections are applied:
 - Database Engine Services
 - Reporting Services
 - Integration Services
 - Management Tools - Complete

 If you are planning on using the Scheduled Report Trending Report to determine if trends are developing for how long it takes to run scheduled reports, and you want to keep the data for more than 60 days, then adjust the Report Execution Logging setting from the Server Properties page in SQL Server Management Studio.


Check the Version of an Existing Microsoft SQL Server

Verify that your version of Microsoft SQL Server is compatible with Report Manager, and make sure that your [report email settings within Reporting Services are set up appropriately](#).

Follow the [Microsoft instructions to check your SQL server version](#).

Add Content Manager and System User roles to Windows user accounts for Server Reporting Services (SSRS) permissions

During the [installation](#) or [upgrade](#) of Report Manager, you will be asked to provide credentials for a Windows User Account. This is a Windows account with access to SQL Server Reporting Services (SSRS). Report Manager will use this account to generate and schedule reports.

 The password can contain any letters and numbers, and only the following special characters: # \$ % ^ - _ = + !

You will need to add the following user roles to a Windows user account:

- Content Manager
- System

Before adding these roles, make sure that you have reviewed the [system requirements](#) and [installation prerequisites](#), and that the SQL Server is properly [configured](#).

Use SQL Server Reporting Services to add these roles.

See [adding roles using SQL Server Reporting Services 2012](#) for details.


See [adding roles using SQL Server Reporting Services 2014](#) for details.


See [adding roles using SQL Server Reporting Services 2016](#) for details.

See [adding roles using SQL Server Reporting Services 2017](#) for details.

Install and configure .NET Framework

Ensure you have [configured server roles for Microsoft Windows Server](#) before you adjust the IIS and .NET settings.

 If you are using .NET Framework 4.6 and later, you will need to ensure backwards compatibility to lower versions. In Windows Server Manager, you will need to have the .NET Framework 3.5 feature enabled.

 If you installed .NET Framework 4.5 on IIS 8.0, IIS 8.5 or Windows Server 2016, you must manually adjust the settings to Allow for web extensions (ASP.NET).

[Install and configure IIS](#) before [installing Microsoft .NET Framework](#), to ensure that WMI classes are installed properly.

Install, upgrade, or migrate Report Manager

Before you install, upgrade, or migrate Report Manager, complete the following:

1. Verify [System requirements](#).
2. Review and complete [Installation Prerequisites](#).
3. Install Windows Server and SQL Server, and verify proper configuration. See [Install and configure server software](#).
4. Add the following Windows User Account roles with access to SQL Server Reporting Services. (Please refer to the Microsoft instructions for adding user roles to a Windows account.):
 - a. Content Manager
 - b. System User
5. Close all other applications.

Install Report Manager

These instructions are for a new installation of Report Manager, not an [upgrade](#) or [migration](#).

Incomplete Data Export

Do not add a new Report Manager server during an existing export.

If you add a new Report Manager server and begin exporting data to it during an existing export to the old server, the new export will not contain all of the data. N-able recommends the following:


- Let the export to the old server complete first.
- Add, or [migrate to](#), a new Report Manager server.

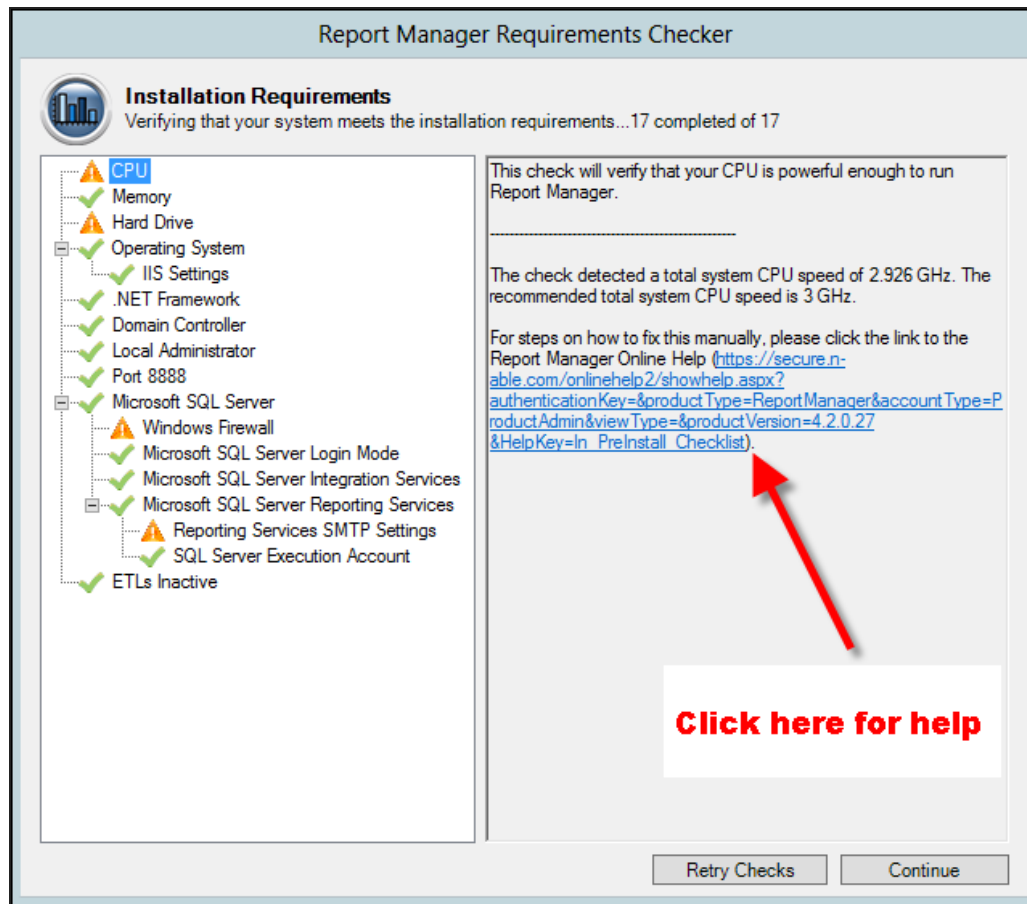
During the installation, Interface, ReportInterface, and Webservice virtual directories are set up within IIS.

The following table shows the significance of these virtual directories.

Directory	What it is
Interface	Used for the Administration Console interface in Report Manager.
ReportInterface	Used for the Reports Console interface in Report Manager.
WebService	Used for communication between Report Manager and the central server.

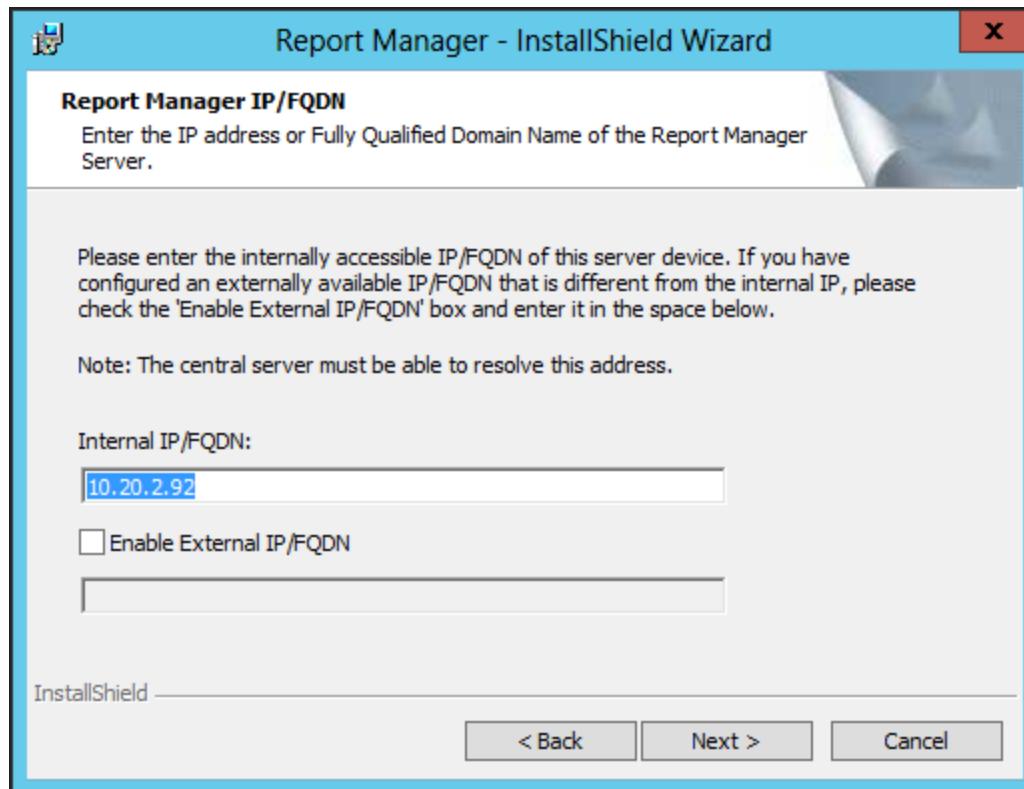
1. Log in as an administrator to the computer upon which Report Manager is being installed.
2. Locate the install file and click Run as Administrator.
3. On the *User Account Control* dialog, click Yes.
 - a. The Requirements Checker will automatically test your system to ensure it meets all requirements.
 - b. When the verification tests are completed, the Installation Requirements window will display all requirements that still need to be met.
4. If necessary, address any issues found by the Requirements Checker, and click Retry Checks to rerun the Requirements Checker.

 If you do not complete the requirements needed, your installation will proceed but your system will respond more slowly. For example, if the minimum requirements for CPU or hard drive are not met. Find help with questions by clicking the link in the Requirements Checker window.



- Click Continue.
- Click through the *Welcome to the InstallShield Wizard for Report Manager* window, and then accept the terms of the license agreement.
- Accept the default folder, or Change to a new folder, and click Next.
- On the *Report Manager IIS IP/FQDN* window, select the option that describes your situation, and click Next.

The default address is the IP address of the Report Manager server. You can use the IP address or a fully qualified domain name (FQDN).



The image shows a Windows-style dialog box titled "Report Manager - InstallShield Wizard". The title bar is blue with a small icon on the left and a red close button on the right. The main content area has a light gray background. At the top, there's a section header "Report Manager IP/FQDN" followed by a description: "Enter the IP address or Fully Qualified Domain Name of the Report Manager Server." Below this, a paragraph of instructions reads: "Please enter the internally accessible IP/FQDN of this server device. If you have configured an externally available IP/FQDN that is different from the internal IP, please check the 'Enable External IP/FQDN' box and enter it in the space below." A note follows: "Note: The central server must be able to resolve this address." There are two input fields. The first is labeled "Internal IP/FQDN:" and contains the text "10.20.2.92". Below it is a checkbox labeled "Enable External IP/FQDN" which is currently unchecked. Under the checkbox is another empty input field. At the bottom left, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Report Manager - InstallShield Wizard

Report Manager IP/FQDN
Enter the IP address or Fully Qualified Domain Name of the Report Manager Server.

Please enter the internally accessible IP/FQDN of this server device. If you have configured an externally available IP/FQDN that is different from the internal IP, please check the 'Enable External IP/FQDN' box and enter it in the space below.

Note: The central server must be able to resolve this address.

Internal IP/FQDN:

☐ Enable External IP/FQDN

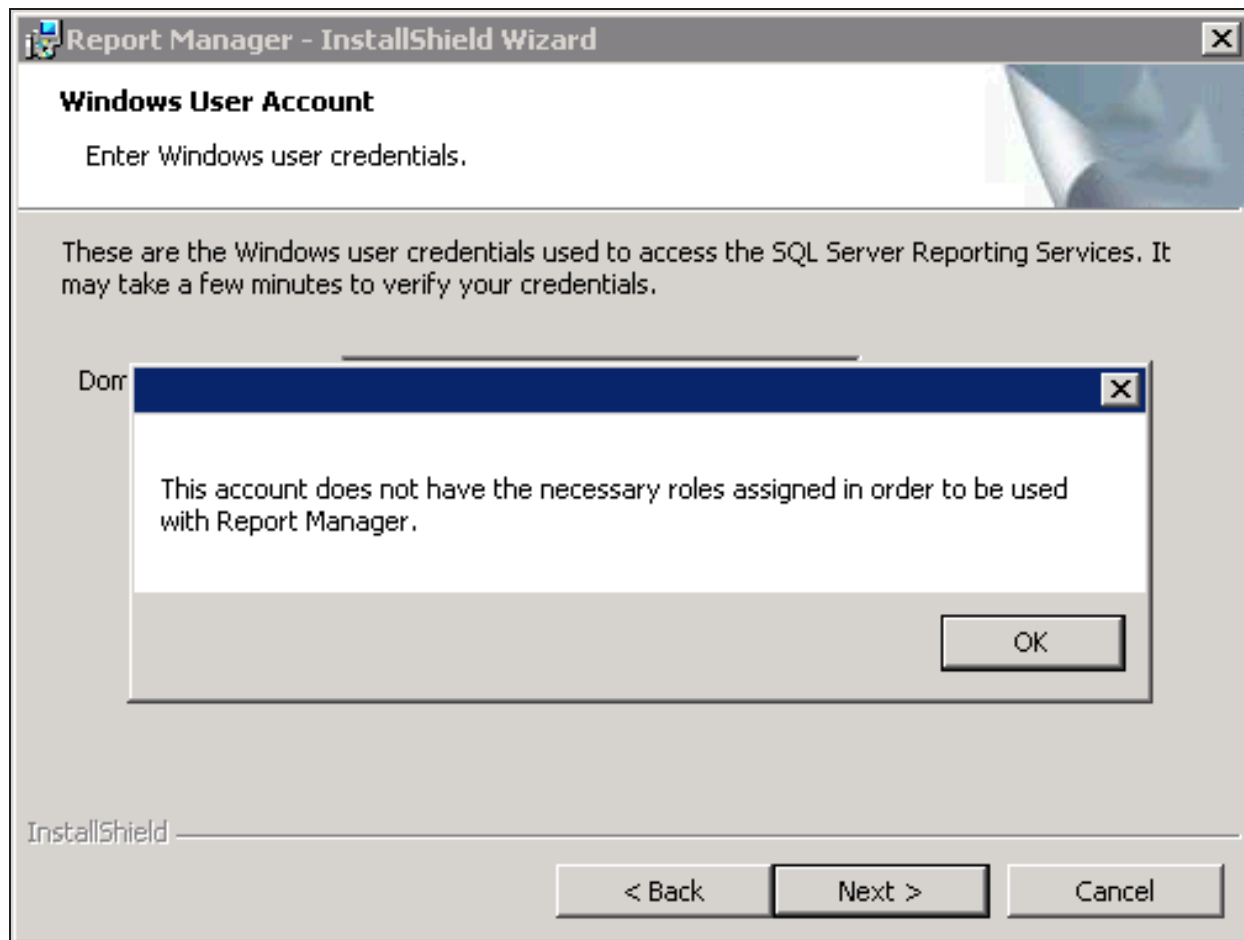
InstallShield

< Back Next > Cancel

9. On the *Windows User Account* window, provide the Windows user credentials, and click Next.

💡 The password can contain any letters and numbers, and only the following special characters: # \$ % ^ - _ = + !

If you receive the *This account does not have the necessary roles* error message, you will need to [set up an account in SSRS](#).




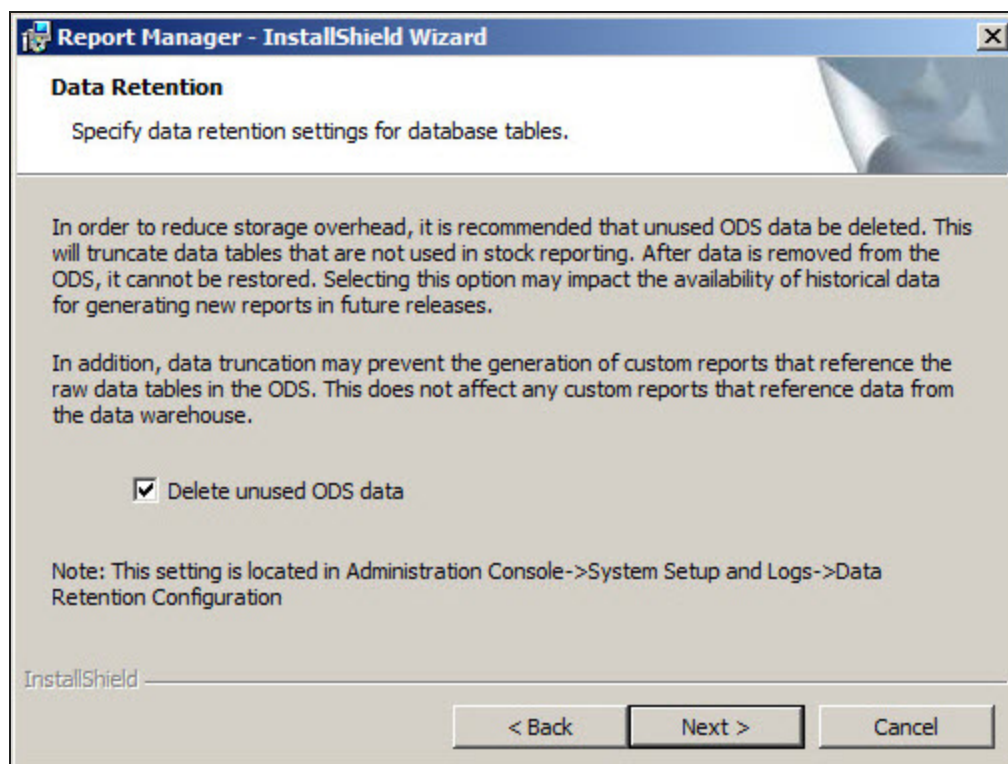
10. On the *Database Folder* window, click Next to accept the default folders, or Change to specify a different folder. Do not use spaces in the folder name.

💡 The drive on which you place a new installation of the Report Manager database and database log files must have a minimum of 100 GB for a dedicated Data Partition. The exception to this is if an existing Operational Data Store (ODS) has been discovered, indicating that this is an upgrade.

11. On the *Report Manager Administrator Sign-in* window, your Username will be reportsadmin@n-able.com.
- If required, provide a new Username for the Report Manager Administrator's account.
 - Provide a Password for the Report Manager Administrator's account and click Next.

12. On the *Data Retention* window, select the Delete unused ODS data option if you want to reduce the size and duration of exports from N-able Report Manager, and click Next.

 This option will impact the availability of historical data for custom reporting if you intend to use the ODS for custom reporting.




13. On the *Ready to Install Report Manager* window, click Install.

When the installation is complete you will be provided with the option to continue with configuring the N-able Report Manager data source. Click Finish

Report Manager opens at the N-able Report Manager Configuration page.

14. Click (?) in the upper right-hand corner of the screen to launch the post-installation instructions.

 If you did not choose to launch Report Manager, you can [access Report Manager](#) through a supported browser or from the Start Menu in Windows.

Upgrade Report Manager

Before upgrading to Report Manager 5.0 SP6 make sure:

1. [All requirements are met.](#)
2. To back up your data so that it is consistent with a date range for both your Report Manager server and your N-able Report Manager Server.

Upgrade Path

You can upgrade to Report Manager 5.0 SP6 from the following versions of Report Manager:

- 5.0 (5.0.0.165+)

Upgrade Instructions

1. Log in to the Report Manager server.
2. Download and run the .exe file from the N-able [Resource Center](#) (also known as the NRC) to install Report Manager 5.0 SP6.
 - a. Log in to the NRC and navigate to the Software Downloads page for Report Manager 5.0 SP6, and click the Report Manager 5.0 SP6 executable.
 - i. If you are using Internet Explorer, click Run.
 - ii. If you are using Firefox, click Save to download the .exe.
 - b. The Report Manager Requirements Checker will verify that all installation requirements are met. If a previous version of Report Manager is detected, the system will perform an upgrade.
 - i. If an earlier, incompatible version is detected, you will receive an error message.
 - ii. After you click Continue in the Requirements Checker, there may be a delay before the first screen of the installer appears.
3. After the upgrade is complete, refresh your browser to see changes.
4. [Grant](#) and [provide access](#) to users.

Migrate Report Manager to a new server

This section lists the steps required for migrating from an old server to a new one.

1. Create folders for migration files.



N-able recommends that you create a folder named ReportManagerBackUpfiles locally on the old server for backed up custom reports and SQL server databases.

- a. Create the folder on the C:\ drive.
 - b. After backing up the custom reports and database files, copy the contents of the ReportManagerBackUpfiles folder on the old server to either a shared folder, or to a folder locally available to the new server.
2. Back up custom reports using SQL Server Reporting Services (SSRS).
 - a. Using Internet Explorer, log in to SQL Server Reporting Services (SSRS) by going to <http://localhost/Reports>.



Firefox does not support SSRS behavior.

- b. Click the Custom Reports folder to view the reports.
 - c. Hover over a custom report name to see the drop-down menu and click Download.
 - d. Save the file to the local ReportManagerBackUpfiles folder that you created in Step 1.
 - e. Repeat steps c and d for each report you want to back up.
3. Stop the following Report Manager Services that are involved with data export and transformation:
 - Report Manager Maintenance
 - Report Manager Maintenance Watchdog
 - World Wide Web Publishing Service
4. Restart SQL Server Integration Services.
5. Using SQL Server Management Studio, back up the following Report Manager databases to the local ReportManagerBackUpfiles folder that you created in Step 1:
 - config
 - ods_*_ds
 - warehouse

See [backing up databases using SQL Server 2012](#) for details.

See [backing up databases using SQL Server 2014](#) for details.

See [backing up databases using SQL Server 2016](#) for details.

See [backing up databases using SQL Server 2017](#) for details.

6. [Transfer the login and password information](#) from the old SQL server to the new server.



Transferring login and password information is necessary because users may not be able to login to databases on the new server.



You will need to use the output script generated by this transfer in Step 11 below.

7. Copy the ReportManagerBackUpfiles folder that you created in Step 1, (which now contains the backed up databases) from the old server and save it to the new server.
8. Install Microsoft SQL Server [2012](#), [2014](#), [2016](#), or [2017](#).

- a. Make sure you are using the [correct version](#).
 - b. For general SQL Server installation, upgrade, and configuration information, refer to [Configuring Microsoft SQL Server](#).
9. After installing Microsoft SQL Server, create two directories that will contain your database and database log files. These will be the directories you will use for the database files, for example: C:\SQLData\ and C:\SQLLog\
10. Using SQL Server Management Studio, restore the following backed up Report Manager databases (that you did in Step 5):
 - config,
 - ods_*_ds
 - warehouse

See [restoring databases using SQL Server 2012](#) for details.

See [restoring databases using SQL Server 2014](#) for details.

See [restoring databases using SQL Server 2016](#) for details.

See [restoring databases using SQL Server 2017](#) for details.

11. [Run the output script](#) that was generated in Step 6 above. This script creates the logins that have the original Security Identifier (SID) and the original password.
12. Install Report Manager, and review the IP addresses.
 - a. Install Report Manager 5.0 SP6.
 - b. If you are migrating a server with a hotfix applied, reapply the hotfix and run the second script, After HF migration.sql. (To run the script, Execute it using SQL Server Reporting Studio.)
 - c. Log in to the Administration Console.
 - d. Review IP addresses in Advanced Settings, and if required, make any necessary changes and Push Settings to All Data Sources.
13. Restore custom reports that you backed up in Step 2.

Repeat the following steps for each custom report that needs to be restored.

- a. Navigate to, or log in to the Report Manager Administration Console.
- b. Click Custom Report Management.
- c. Locate and select the report file to replace, and click Update.
- d. Browse to locate the backup file (from Step 2) on the server.
- e. Select and Open the file.
- f. Click Next.

The screen displays a success page and redirects you to the Custom Report Management screen.

 Make sure that you have [re-enabled SSL to configure HTTPS](#) for Report Manager.

14. Review scheduled reports.

Scheduled reports are automatically restored during the installation process. You will need to [rebuild schedules](#) for the custom reports that have been restored from backup.

 - a. In the Reports Console, navigate to the Scheduled Reports page.

Schedules that need to be recreated for custom reports will be highlighted in the list.
 - b. For each schedule that needs to be rebuilt, select the check box in the far left column and click Rebuild.
15. Restart your server.

Post-installation - Next Steps

After installing Report Manager, perform the following in order:


1. In Report Manager:
 - a. [Add an N-able Report Manager data source](#) for Report Manager.
 - b. [Configure secure communication](#) between Report Manager and N-able Report Manager.
 - c. [Add Report Manager databases to a maintenance plan](#).
 - d. Disable the reportsadmin account for added security (suggested)
2. In N-able Report Manager:
 - a. Enable Report Manager for the Service Organization (not required for N-able Report Manager release 11.0 and later).
 - b. [Grant existing users access](#) to Report Manager.
 - c. [Configure monitoring](#) of your Report Manager server.

Add an N-able Report Manager Data Source

At the end of a new installation, Report Manager launches and opens to the N-able Report Manager Configuration screen, where you can configure data sources for Report Manager.

You can set up one or more data sources. Typically, you will configure N-able Report Manager as a data source for Report Manager. However, you can also add data collection from PSAs you have integrated in N-able Report Manager. Report Manager supports the following PSA Integrations:

- Autotask
- ConnectWise Manage
- Help Desk Manager

 Any time you add an N-able Report Manager data source, consider adding the database to a [database maintenance plan](#) to receive notifications of failure for Report Manager Maintenance.

Best Practice

For the Operational Data Store drive, N-able recommends that you have a minimum of 100 GB free space.


N-able recommends that the Operational Data Store and Operational Data Store logs be stored on separate physical storage drives. These storage locations cannot be changed after the database has been created.

Configure an N-able Report Manager data source

If you are adding a first data source, log in to Report Manager, and open the Administration Console.

If you are adding an additional data source, log in to N-able Report Manager. When complete, navigate to Administration > Report Manager > Administration Console.

1. Click N-central Configuration.
2. Check the Server FQDN/IP field to see if your N-able Report Manager server has already been added.
3. To add a new data source, click Add.
4. Type the Internal FQDN or IP address of the N-able Report Manager server to be added.
5. If required, specify the Operational Data Store Path and Operational Data Store Log Path.
6. Type the Product Administrator user name and password for the N-able Report Manager server.

 The password can contain any letters and numbers, and only the following special characters: # \$ % ^ - _ = + !


7. To add data collection from your PSA connections in N-able Report Manager, select the Automatically collect data from PSA integrations check box.

Report Manager can now connect directly to external PSA servers using the credentials provided by N-able Report Manager. These credentials can only be modified in N-able Report Manager. Report Manager supports the following PSA Integrations:


- Autotask
- ConnectWise Manage
- Help Desk Manager

This option allows for more detailed reporting about PSA tickets generated by notifications in N-able Report Manager.

If you are using a limited integrator account in ConnectWise Manage, you will not be able to connect with N-able Report Manager. You will need to update N-able Report Manager to use any ConnectWise Manage administrator-level account.

 For Report Manager version 5.0 and greater, if you are using a limited integrator account in ConnectWise Manage, you will not be able to connect with N-able Report Manager. You will need to update N-able Report Manager to use any ConnectWise Manage administrator-level account.

8. Click Add.
9. If Autotask information is desired in reports, allow the export to complete. This propagates the Autotask configuration to Report Manager. Observe the dates on the N-able Report Manager Configuration page to confirm this has completed. Carry out the following:
 - a. Click the newly added data source FQDN/IP.
 - b. Click the appropriate System / Service Organization level containing the Autotask Configuration.
 - c. Replace the Autotask API Credentials used by N-able Report Manager with Autotask API Credentials specifically for Report Manager.
Create these credentials in Autotask as follows:

 This procedure to change the Autotask credentials is current as of date of publication. N-able does not guarantee its accuracy or validity.

- i. Navigate to Admin and click Extensions & Integrations.
 - ii. Expand Other Extensions and Tools, then click Integration Center.
 - iii. Under the Integration Vendor Name column, click the ellipsis icon next to Solarwinds MSP - Report Manager.
 - iv. Click Add API User.
 - v. Fill out the required fields.
 - vi. Click Generate Key and then click Generate Secret.
 - vii. Save your changes.
- d. In N-central, click Test Connection if desired.
- e. Click Save.
- f. Allow next Export and ETL to complete, as seen on the N-central Configuration page. Ticketing info should now be available in reports.

Configure HTTPS and SSL for Report Manager

By default, the N-able Report Manager server uses HTTPS for secure and encrypted communication with client computers, while the Report Manager server does not.

You must either configure Report Manager to use HTTPS or configure Internet Explorer to use Mixed Mode content.

Configure the Report Manager server to use HTTPS connections

1. Set up an HTTPS Service in IIS.

Search "How to Set Up an HTTPS Service in IIS" in the Microsoft Knowledge base articles, at <http://support.microsoft.com/kb>.

2. Install an HTTPS certificate in IIS.

Search "How to implement SSL in IIS" in the Microsoft Knowledge base articles at <http://support.microsoft.com/kb>.

3. Enable HTTPS in Reporting Services.

Search "Configuring a Report Server for Secure Sockets Layer (SSL) Connections" in the Microsoft Knowledge base articles at <http://support.microsoft.com/kb>.

4. Enable HTTPS in Report Manager:

- a. After installing Report Manager, log in to the Report Manager Administration Console.
- b. Navigate to the Advanced Settings page, and set the value for Enable HTTPS access? to True.
- c. Click Update to save your changes.

5. Update the Internal and External IP, then update the Export IP:

- a. In the Report Manager Administration Console, navigate to the Server IP Configuration page:
 - i. In the Internal IP Address field, enter the FQDN.
 - ii. In the External IP Address field, enter the FQDN.
 - iii. Check that this resolves correctly on both the N-able Report Manager server and Report Manager server to the desired IP address:
 - This can be done from the Command Prompt on the Report Manager server.
 - For N-able Report Manager, navigate to Administration Console > Test Host Connectivity.
- b. In the Report Manager Administration Console, navigate to ExportIP.
- c. Click Edit in the right hand column.
Update this value to the Internal IP address if N-able Report Manager is on the same local network as Report Manager.
- d. Click Update.
This will Export data from N-able Report Manager straight to Report Manager using your internal network.
- e. Click Push Settings to All Data Sources.


Configure Internet Explorer to support Mixed Mode Content

1. Add the N-able Report Manager and the Report Manager IP Address (or FQDN) to your Trusted sites zone.
2. Clear all cache and cookies.
3. Enable Mixed-mode content:
 - a. Click Tools > Internet Options.
 - b. Select Security.


- c. Click Custom level.
 - d. Scroll down to Miscellaneous, and ensure that Display mixed content is set to Enable.
4. Restart your browser. The browser must be restarted before the changes will take effect.

Add Report Manager Databases to a maintenance plan

N-able recommends that you include all Report Manager ODS and warehouse databases in a Microsoft SQL server database maintenance plan. A maintenance plan will ensure databases are performing optimally.


 For settings not specifically mentioned, you may define them according to your network requirements.

See the [Microsoft instructions](#) for details on using the Maintenance Plan Wizard in SQL Server Management Studio.

1. Set the following in the Maintenance Plan Wizard of Microsoft SQL Server Management Studio:
 - a. Set the plan properties Name to Report Manager.
 - b. Set the Job Schedule properties as follows:
 - i. Select the Recurring schedule type
 - ii. Select Weekly or Daily frequency.
 - iii. Choose your duration settings if you selected a daily frequency.
 2. Select the following maintenance tasks:
 - Check Database Integrity
 - Reorganize Index
 - Update Statistics
 - Back Up Database (Full)
 - Maintenance Cleanup Task
-  N-able does not recommend shrinking your database.
3. For each selected task, define the task, and edit the definitions as required.
 4. For each task:
 - Select all of the ODS databases and the warehouse database.
 - Configure cleanup task settings. The settings for this task do not affect the Report Manager installation.
 5. Select your report option settings.

The Report Manager maintenance plan is created and included under Maintenance Plans.

Grant Access to Report Manager from N-able Report Manager

 Granting access to SOs is not needed when Report Manager is integrated with N-able Report Manager release 11.0 and later. For previous versions of N-able Report Manager, see [KBA45045: Grant Access to Report Manager from MSP N-central](#).

Access Report Manager

Access Report Manager through one of the following methods:

- Windows Start menu
- Supported browser
- N-able Report Manager,

Possible Error when Browsing to Report Manager

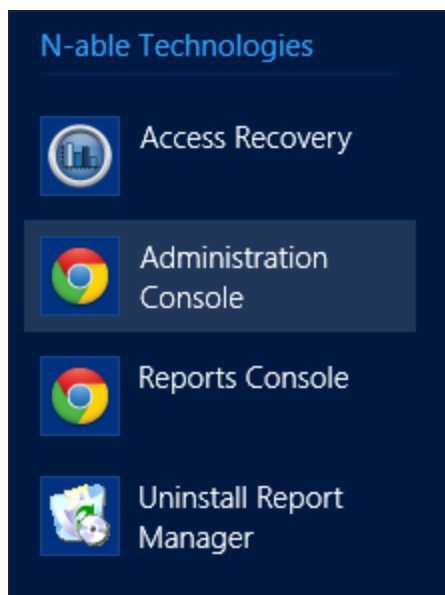
A "Fatal Error" may appear after browsing to Report Manager, and the browser closes. This is because the Microsoft Report Viewer package is missing. Download and re-install the Report Viewer re-distributable package from Microsoft, and re-start your browser to launch Report Manager.

Access through the Windows Start menu

1. On the Report Manager server, access the Start Menu.
2. With the Start Menu open, right click in the background to display All Apps.



3. Click All Apps.
4. Locate the Report Manager application and click Reports Console for Report Manager reports.



5. On the Welcome to Report Manager login screen, enter the Report Manager Username and Password.
6. Click Login.

Access through a supported browser

1. In a [supported browser](#) on the Report Manager server, type the Report Manager Console URL in the address field:

`http://<Report Manager server URI>/ReportInterface/Pages/menu.aspx`

Administration Console URL

2. On the Welcome to Report Manager login screen, enter the Report Manager Username and Password.

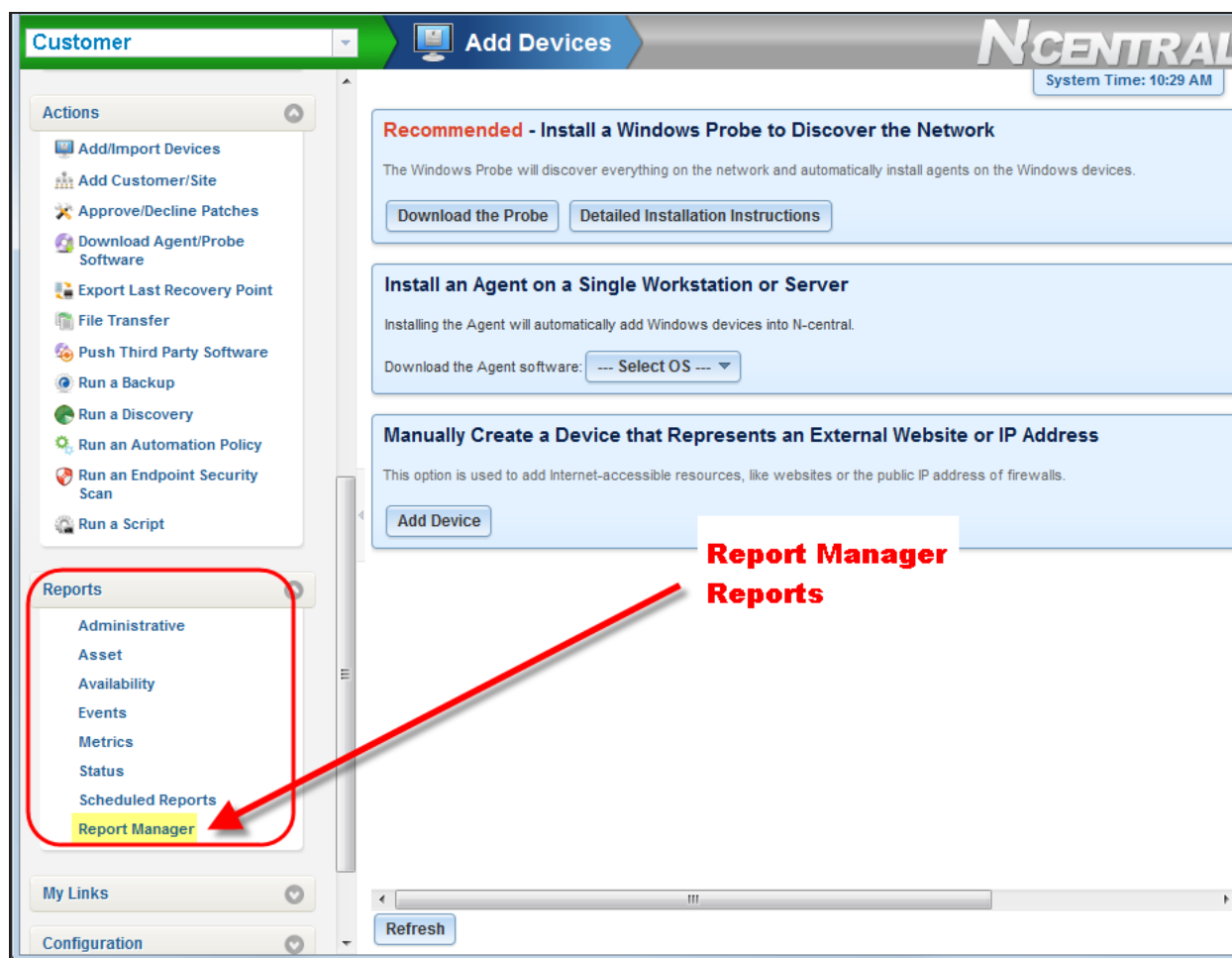
i The default username is **reportsadmin@n-able.com**, and the password is that which you set up during installation.

3. Click Login.

Access through N-able Report Manager

Reports Console

1. Click Report Manager in the Reports pane on the left-side of the screen.



Grant Access to Reports

You will need to set the appropriate permissions in N-able Report Manager for the role to which the user is assigned, for that user to have access to and view reports. For more information about roles and permissions, see the N-able Report Manager online help.

1. In N-able Report Manager, navigate to Administration > User Management > Roles.
2. Scroll to the Reporting section.
3. Under the Report Manager feature, for the Report Manager permission, select Manage from the drop-down list. This will allow the user to view Report Manager reports in N-able Report Manager.
4. Under the Report Manager feature, for the Report Manager Access permission, select Manage from the drop-down list. This will allow the user to view the Report Manager Administration Console.
5. Save your changes.


Monitor Report Manager as a device through N-able Report Manager

Set up Report Manager monitoring to receive failure notifications for the Report Manager Maintenance and Report Manager Maintenance Watchdog services, as well as notification of any ETL process failures. Download and install an agent and apply the Report Manager service template.

Download and Install an Agent

1. Log in to N-able Report Manager and select the customer. Typically, this will be your internal company name.
2. Click Actions > Download Agent/Probe Software.
3. Under Customer/Site Specific Software, select the Windows agent.
4. Install the Windows agent on Report Manager. The Windows agent will register Report Manager with the N-able Report Manager server.

Apply the Report Manager Service Template

 If you have an earlier version of N-able Report Manager, download and install the Report Manager Service Template before applying it to Report Manager.

1. In Views, click All Devices.
2. Select the check box next to the Report Manager device.
3. Click Apply Service Templates.
4. Select the Report Manager service template and click >.
5. Click Apply.


How to Use the Report Manager Customer Purge Utility

The Report Manager Customer Purge utility allows adherence to the General Data Protection Regulation (GDPR) regulations. The utility is an administrator-level tool to completely purge a customer and its related information from the Report Manager System.

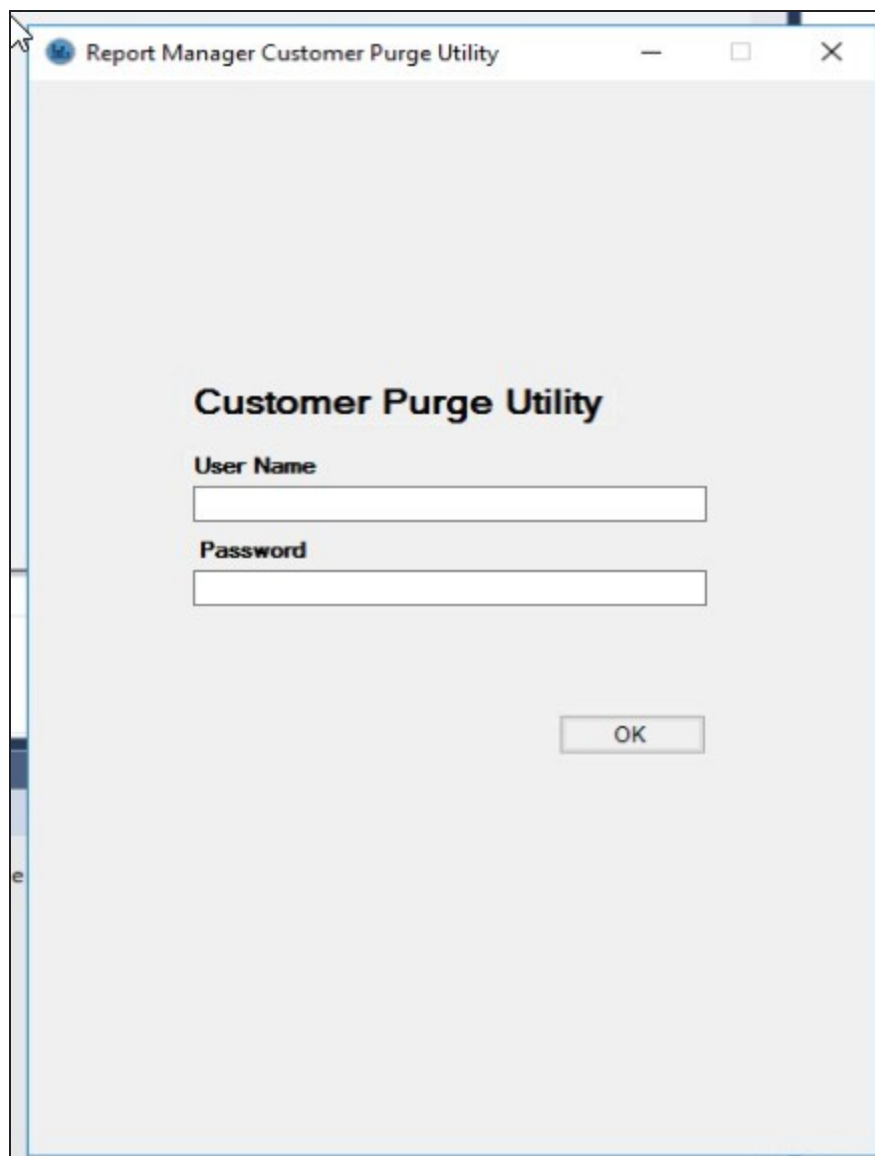
GDPR is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses exporting personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data, and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation was adopted on 27 April 2016, and becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

The Report Manager Customer Purge utility must be placed in the Report Manager BIN directory.

When the purge is complete, you will be able to save the deletion results to a csv file. If there is an error in purge processing, all transactions will be rolled back and the errors will be captured in a log file.

 The purge utility should only be used once the customer has been deleted from N-able Report Manager, and all exports have been completed.

1. Open the utility and log in with the ReportsAdmin account seen in Access Recovery on the Start Menu, which is the `reportsadmin@n-able.com` account and your current password.



The screenshot shows a Windows application window titled "Report Manager Customer Purge Utility". The window has a standard Windows title bar with minimize, maximize, and close buttons. The main content area is light gray and contains the following elements:

- A title "Customer Purge Utility" in bold black text.
- A label "User Name" above a text input field.
- A label "Password" above a text input field.
- An "OK" button located at the bottom right of the input fields.

2. Select the data source from which to delete.
3. Select the Service Organization containing the customer to delete.

4. Select the customer you want to delete.



If there are other copies of the customer in another data source, repeat the process.

Report Manager Customer Purge Utility

Select a Datasource containing the record to purge.

ods_10_ds1

Select the service organization that contains the customer

Temp

Select the customer to purge from the system.

A

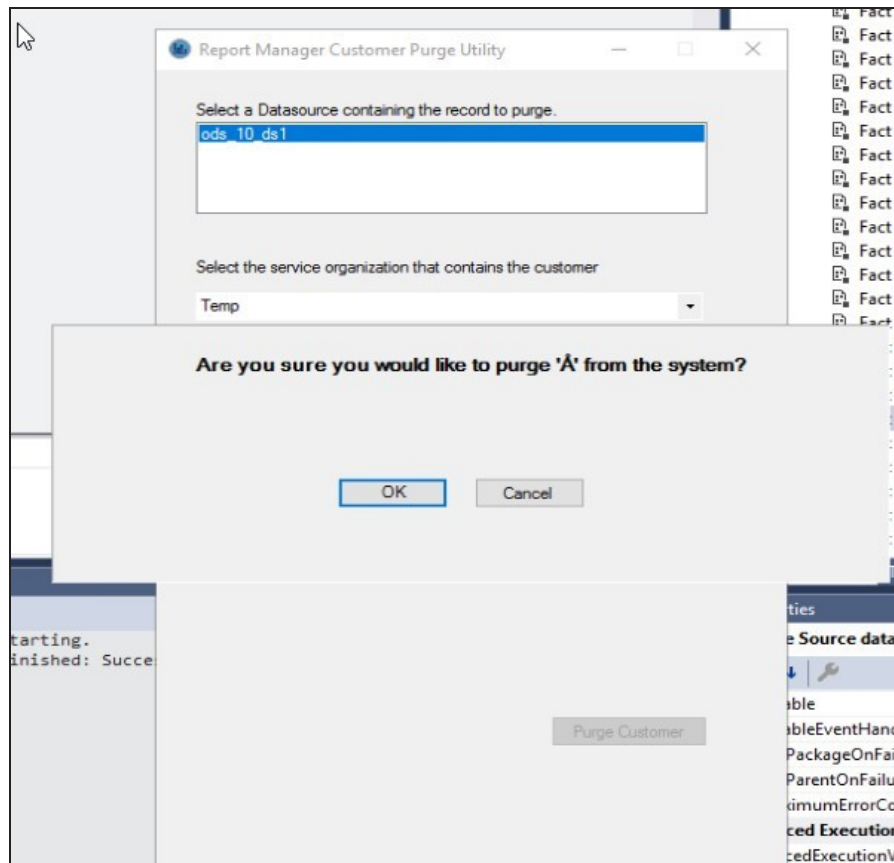
Purge Customer

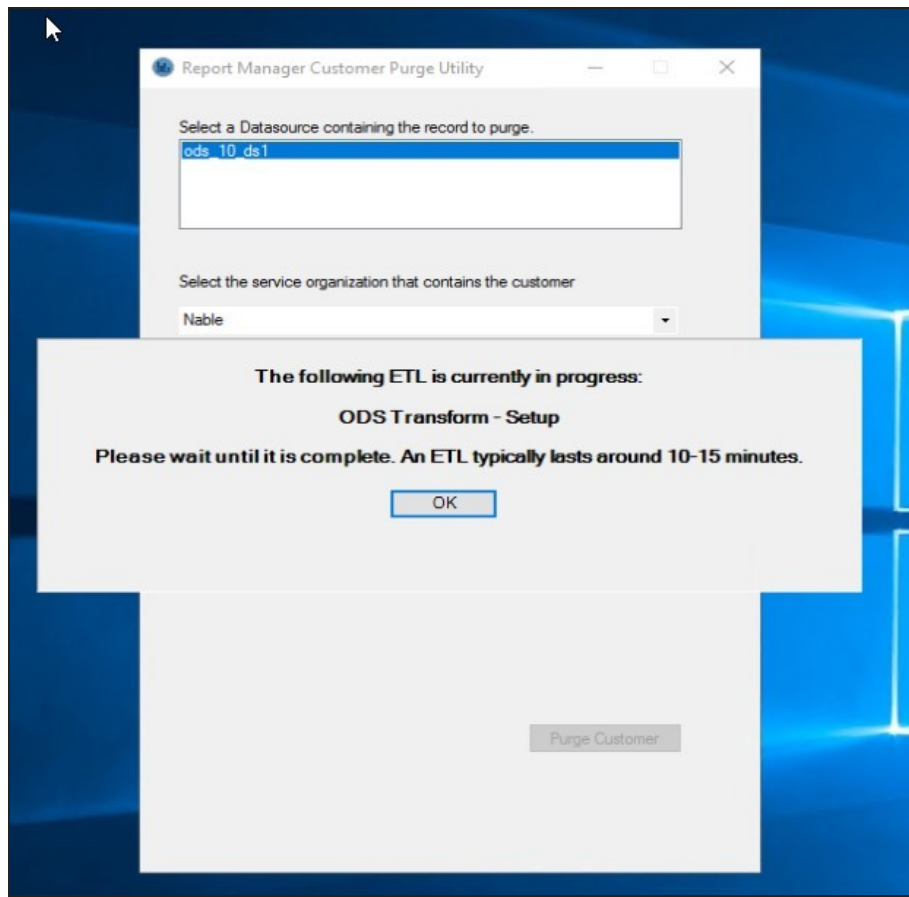
5. Click Purge Customer.

Click OK to confirm the purge.

The customer will be purged from the system.

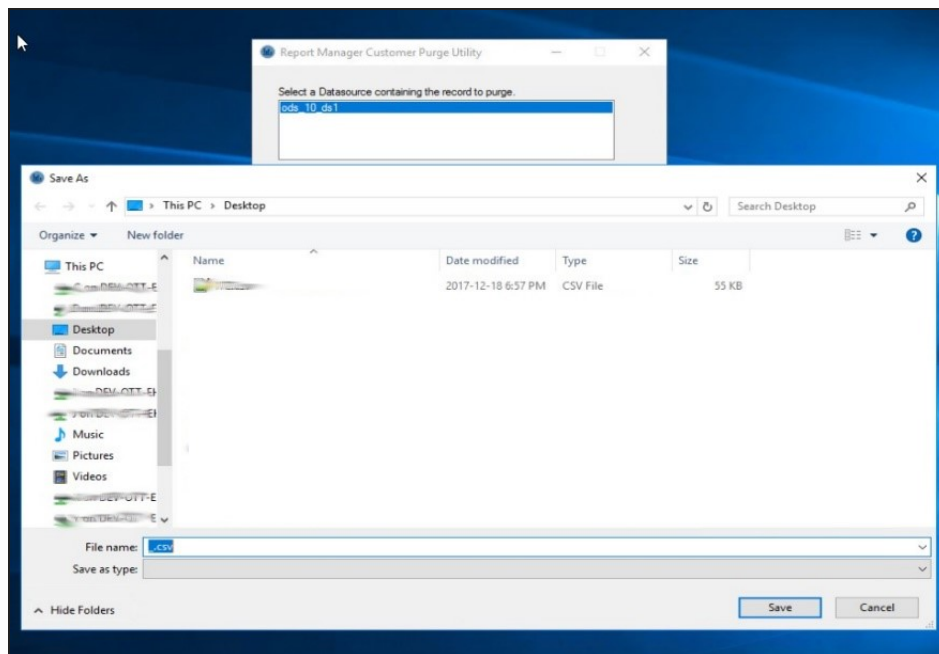
If an ETL or Export is running, you will be asked to try later.





6. When the purge is complete, save the deletion results to a csv file.

If there is an error in purge processing, all transactions will be rolled back and the errors will be captured in a log file.



Best Practices

Optimize Report Manager post-installation by reviewing and implementing best practices. An upgrade, or migration from another server, may have most of these configured.

What	Where	Link to topic
Set up monitoring of Report Manager like a device in N-able Report Manager	In N-able Report Manager, at the Service Organization level or at the Customer level	Monitor Report Manager as a device through N-able Report Manager
Set up access to Report Builder through your desktop	On the Report Manager server, in SQL Server Reporting Services (SSRS)	Set up credentials to use Report Builder
Ensure Report Manager database performance	On the Report Manager server, in SQL Server Management Studio (SSRS)	Add Report Manager Databases to a maintenance plan
Set up a file share for scheduled reports	On the Report Manager server	Set up File Share or Email for Scheduled Reports
Ensure rendering of Report Manager features if you are using IE 8.0 +	On the Report Manager server, in the browser you are using to view Report Manager	Assign browser security zones
Select how long to keep data available for Report Manager	In Report Manager, in the Administration Console	Configure the Data Retention Time Period

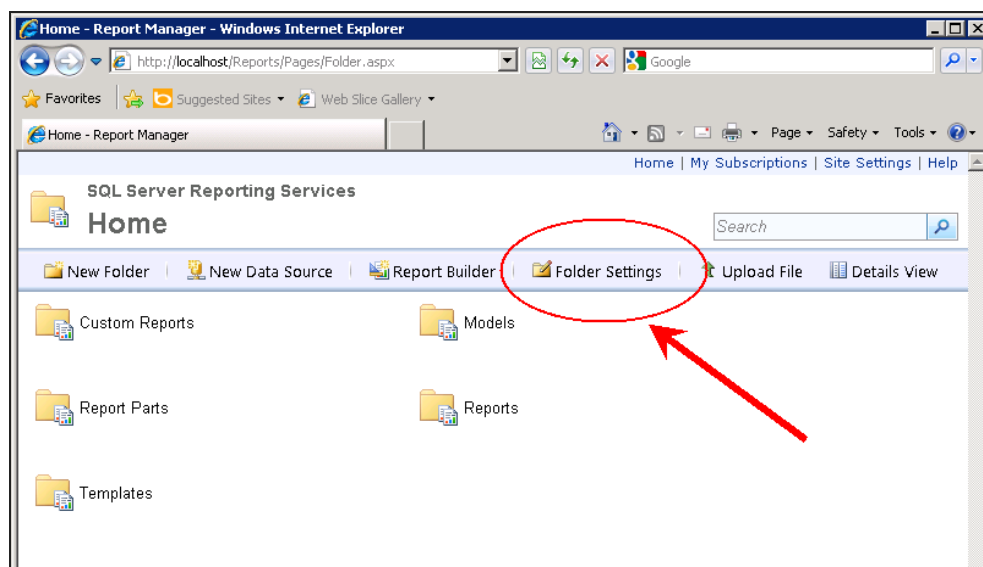
Set up credentials to use Report Builder

To access Report Builder using the Report Manager server, assign to your domain account the appropriate rights to Reporting Services.

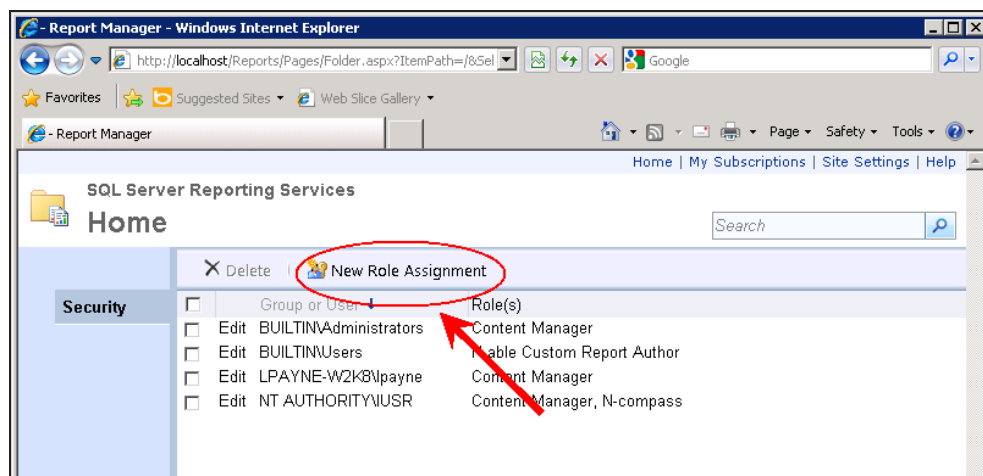
💡 If you have local Administrator rights, no changes are required to your domain account .

Assign the account the "N-able Custom Report Author" role

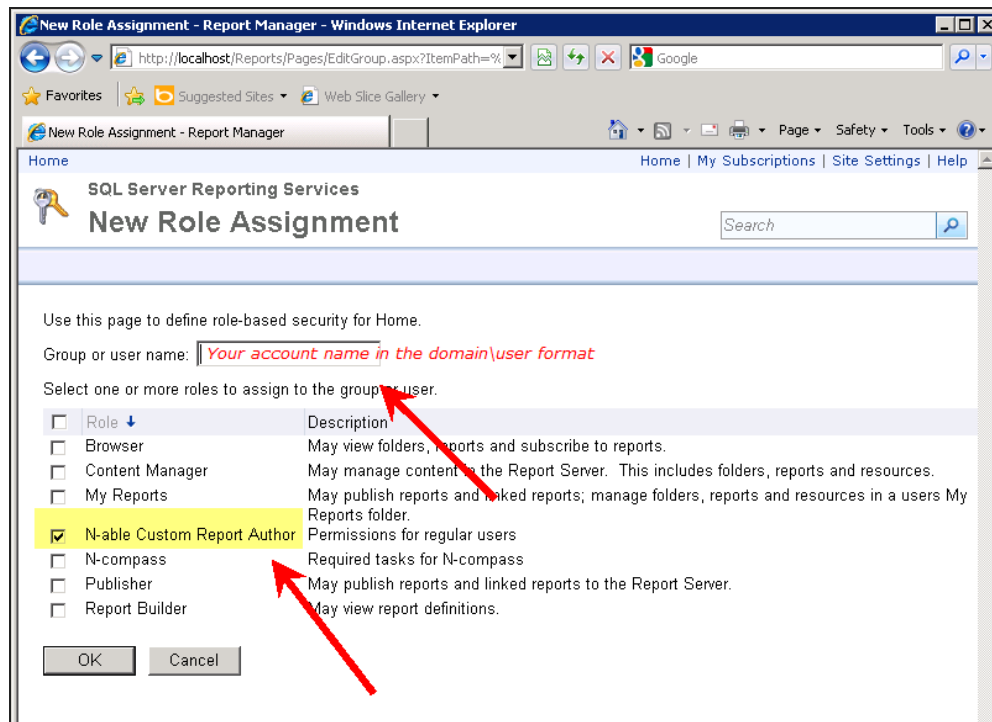
1. Establish a remote desktop connection to the Report Manager server.
2. On the Report Manager server, open a browser.
3. Browse to <http://localhost/Reports>.
4. Click Folder Settings.



5. Click New Role Assignment.



6. In the Group or user name field, specify your account name in the domain or user format.
7. Select the N-able Custom Report Author check box.



8. Click OK.

Set up File Share or Email for Scheduled Reports

Set up necessary sharing permissions in order to use a file share. To send scheduled reports by email, set up the SMTP server. The SMTP server may have been set up during installation. The Requirements Checker will warn you if you have not set up the SMTP server email.

Set up a File Share

1. On the Report Manager server, navigate to the shared folder to which you would like to deliver the reports.
2. Right-click Share. If the folder is already shared, click Change sharing permissions before proceeding.
3. Type `NETWORK SERVICE` in the field at the top of the dialog box.
4. Click Add.
5. Click the Permission Level for the `NETWORK SERVICE` user and select Contributor.
6. Click Share.



If you receive a User Access Control prompt, click Continue.

7. Click Done.

Set up SMTP Server Email

Using Microsoft SQL Server Reporting Services Configuration, configure the email settings to specify the Sender Address and the SMTP Server.

See the Microsoft instructions for configuring email settings for SQL Server [2012](#), [2014](#), and [2016](#).

Assign browser security zones

If you use Internet Explorer 8 or later, assign Report Manager to either Trusted Sites Zone or Local Intranet Zone in order for Report Manager and UI features, such as the Report Scheduling, to render correctly.

For more information on using security zones in Internet Explorer, search the Microsoft knowledge base articles at <http://support.microsoft.com/kb>.

Configure the Data Retention Time Period

⚠ When selecting the retention period, data older than the current date plus the retention period will be purged at the next maintenance operation.

For example, today is April 1st and at 10 a.m. you set the retention period for 3 months. At the next maintenance operation (which will be tonight, April 1st, at midnight), all data older than 3 months (January 1st) will be purged. At the next scheduled maintenance operation (which will be the next night, April 2nd, at midnight), all data older than January 2nd will be purged, and so on.

If you plan to set a retention period, consider to first back up your data. Report Manager does not back up this data prior to it being purged.

⚠ After data is purged it cannot be restored.

1. In Report Manager, click the gear icon in the upper right of the Reports Console window.
In N-able Report Manager, navigate to Administration > Report Manager > Administration Console.
2. Click System Setup and Logs.
3. Click Data Retention Configuration.
4. Choose an ODS retention period.

The Keep All Data default will keep the data in the ODS indefinitely.

The Delete unused ODS data option may have been set during installation. This option reduces the size and duration of exports from N-able Report Manager, reducing traffic on your network. When you select this option, unused tables from the ODS are deleted. In addition, if you are exporting from N-able Report Manager 9.3 or later, this option flags these same unused tables in N-able Report Manager and prevents them from being exported.

⚠ If you use data from the ODS for [custom reporting](#), selecting the Delete unused ODS data option will impact the availability of historical data for generating new custom reports. After unused data is deleted, it cannot be restored. Historical data from the tables not exported will not be accessible in the future. This does not affect custom reports that reference data from the data warehouse, only custom reports referencing data from the ODS.

5. Choose a Data Warehouse retention period.

The Keep All Data default will keep the data in the Data Warehouse indefinitely.

Troubleshooting

The Requirements Checker has integrated online help for all system checks and automatic fixes.

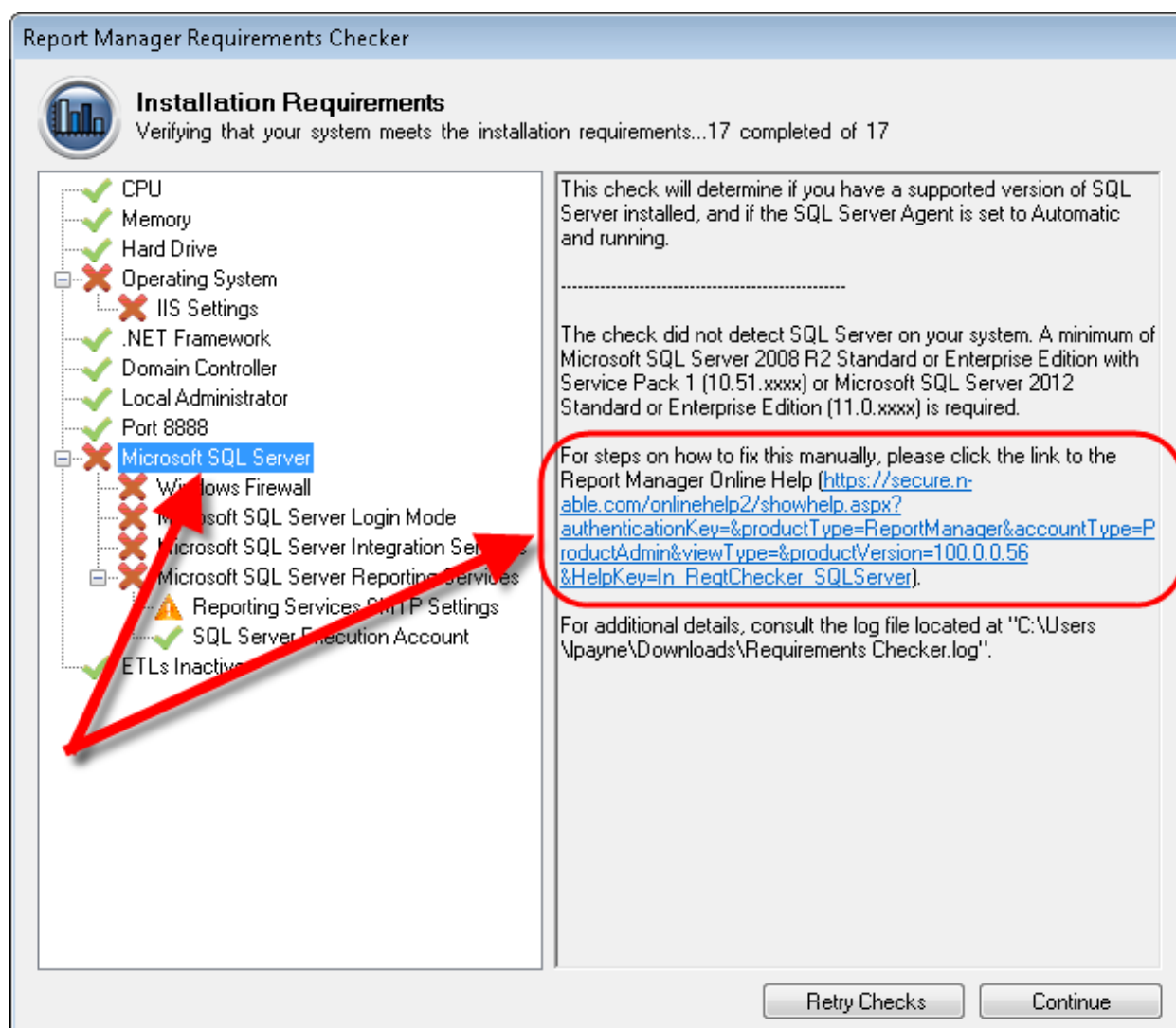
Knowledge base articles have been created using common support issues. N-able encourages you to search the articles to see if your issue has been addressed. The general online help contains a list of Knowledge base articles, and also provides all Report Manager tasks.

i Check with Microsoft for detailed information on installation and configuration of Microsoft products needed for Report Manager. To resolve issues with Microsoft software, see <http://support.microsoft.com/>.

Installation: Requirements Checker Troubleshooting

The Requirements Checker's integrated online help gives immediate feedback for all system checks and automatically fixes failures and provides repair information.

Click the link to open help specific to this issue.





Customer Support

Web Page:	http://www.n-able.com
Technical Support Self-Service Portal:	https://support.n-able.com
Phone:	Toll Free (U.S./CAN): 1-866-302-4689
	International: +800-6225-3000
	Local: (613) 592-6676, select option 2 for support



© 2022 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of N-able. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of N-able, its affiliates, and/or its respective licensors.

N-ABLE DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL N-ABLE, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF N-ABLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale. For more information, visit www.n-able.com.