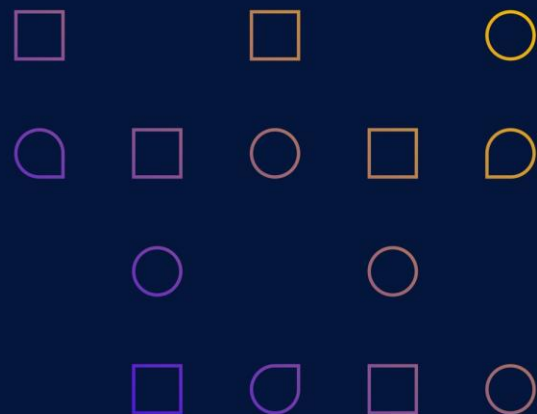


Discovery Center Installation Guide

4.20.0 - Exchange, MIP and Security Updates

November 2025



Introduction	4
System Overview.....	4
Specifications and Prerequisites	5
Choosing Overall Configuration	5
Discovery Center Capacity Planning	6
Hardware Specifications	7
Software Prerequisites.....	9
Network Connections	11
Virtualization.....	11
Pre-Installation Requirements	12
Windows Accounts and Groups.....	12
Internet Information Services	14
.NET Framework.....	15
SQL Server Configuration	16
Installing Discovery Center	19
Discovery Center Post-Installation Functional Checks.....	26
Install Discovery Center Workbench Designer.....	27
Appendix 1: Installation Checklist and Notes	29
Pre-Installation Requirements and Information.....	29
Post Installation Requirements and Information.....	30
Appendix 2: Configuring for SSL and HTTPS.....	31
Preparing a Secure Site	31
Install Discovery Center to an Existing Secure Site	32
Appendix 3: Upgrading an Existing Installation	33
Preparing to Upgrade.....	33
Performing an Upgrade.....	34
Migrating an Existing Installation to HTTPS	36
Post Upgrade Configuration.....	37
Troubleshooting Upgrades.....	38
Appendix 4: Example Installations	40
Local Server Installation	40
Centralized Installation	41
Example Windows Account and SQL Server Logins	42
Appendix 5: Command Line Installation	43
Installer Extended Command Line Properties	43



Example Command Line.....	45
Appendix 6: Configuring Management Reporting Database	46
Creating the Management Reporting Database	46
Configuring the Management Reporting Database for Use	48
Upgrading the Management Reporting Database.....	49
Appendix 7: Additional Configuration for Fully Distributed Configuration	50
Overview	50
System Requirements	51
Information Required for Configuration.....	52
Configuration for Kerberos Delegation.....	53
Additional Information and Troubleshooting	61
Appendix 8: CyberArk Configuration	62
Integration Overview	62
CyberArk Credential Provider Installation	63
CyberArk Safe Configuration.....	66
Appendix 9: SharePoint Online Authentication	69
Registering an Azure Application for a SharePoint Online tenant.....	69
Appendix 10: MIP Sensitivity Label Integration	73
Integration Overview	73
Registering Discovery Center in Azure AD	73
Discovery Center System Setting requirements	77
Appendix 11: Exchange Online ROPC Authentication	79
Resource Owner Password Credentials (ROPC) Authentication.....	79
ActiveNav Exchange Connector Multi-Tenant Application.....	79
Registering an Application for Exchange Connector ROPC Authentication.....	80
Using the Registered Application with Discovery Center	83
Appendix 12: Prerequisites for Preserving NTFS File Owner	84
Appendix 13: Common Problems	85
How to Troubleshoot Installer Problems.....	85
Common Installation Problems.....	85
Using ActiveNav Support	86



Introduction

This document provides a detailed installation guide for the ActiveNav Discovery Center and Discovery Workbench applications. To install other applications and components, refer to their specific documentation.

Key:

Note

Software

Hardware

Roles/Users

Syntax/Config

System Overview

Discovery Center comprises a range of component applications and supporting services provided by Microsoft SQL Server. The main components are Discovery Center, SQL Server Database, SQL Server Analysis (SSAS), and Discovery Center Workbench, outlined in the diagram below:

1. SQL Server Database

The SQL Server Database stores the results of all indexing and analyses, action logs, and configuration settings.

2. SQL Server Analysis (SSAS)

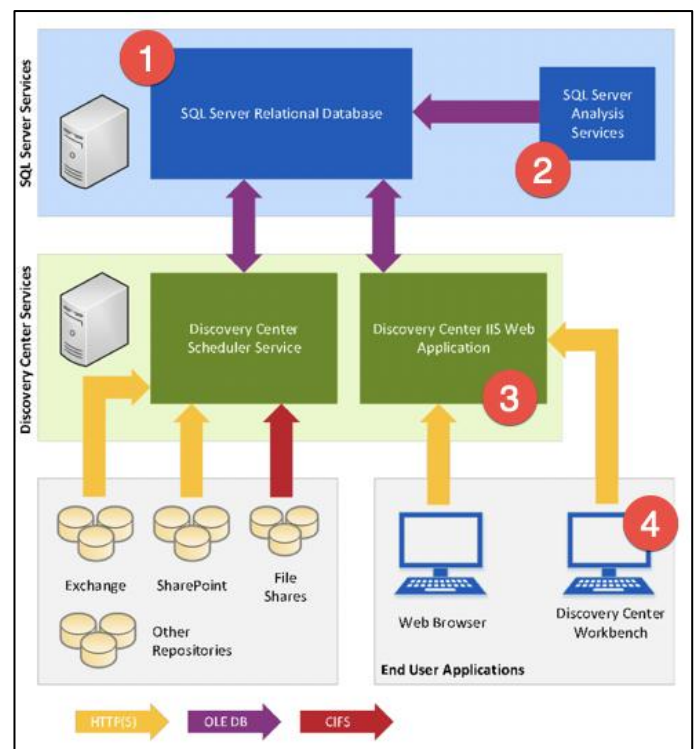
Supports interactive reporting by providing a reporting database.

3. Discovery Center

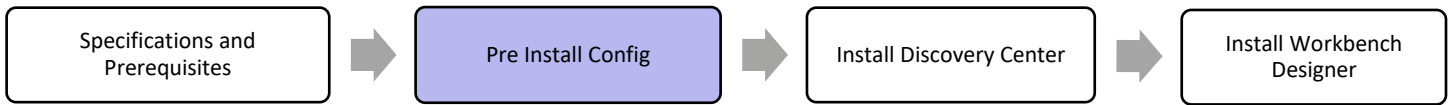
Discovery Center is a web application delivered via Microsoft Internet Information Services (IIS) that manages the indexing and analyses of files in source repositories and delivers reports and actions across index results.

4. Discovery Center Workbench

Design, build, and test classifications for deployment to the Discovery Center, all from the Discovery Center Workbench.



Note: The system must be architected and provisioned according to the project's scale to ensure optimal performance.



Specifications and Prerequisites

Outlined below are the **minimum** hardware specifications and prerequisite software requirements for a Discovery Center deployment:

Note: For large data volumes, working with the minimum specifications may lead to poor performance or a slow responding system.

Choosing Overall Configuration

Depending on your system requirements, you need to choose either a **Local**, **Remote**, or **Fully Distributed** database configuration for Discovery Center and its components.

Local

Installing the SQL Server components and the Discovery Center on the same server offers good performance, reducing the potential for network connectivity issues between Discovery Center and SQL Server but will likely cost more for SQL assets.

Note: The server size must be at least the sum of the sizing for the Discovery Center, and the SQL Server Hosts to accommodate both.

Remote

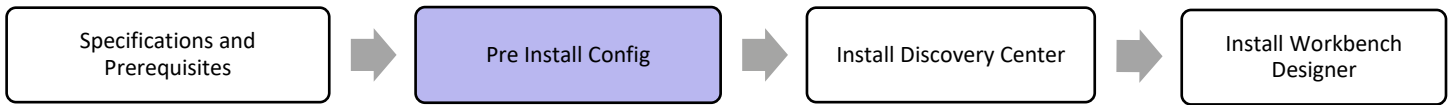
Discovery Center supports a remote SQL Server instance whether deployed on a dedicated server to support the Discovery Center or as part of a shared SQL Server instance. For large deployments, this configuration spreads the database and analysis loads. A well-provisioned SQL Server instance is likely to result in a more responsive deployment for a given investment.

Fully Distributed System

Deploying a system where **Discovery Center**, **SQL Server**, and **SQL Server Analysis Services** are each hosted by a dedicated server will accommodate vast amounts of data. However, additional configuration is required to support authentication between each component.

Note: Review the information in [Appendix 7: Additional Configuration for Fully Distributed Configuration](#) before installation to ensure this configuration's requirements can be met and then follow the steps outlined after installation to enable the system's correct operation.

Pre-Installation Requirements



Discovery Center Capacity Planning

Managing capacity of ActiveNav Discovery Center post-deployment is critical to long-term reliability and manageability. Some questions to consider are:

- Do I need to deploy an additional instance of Discovery Center?
- Do I have enough disk space, cores, and memory allocated on my servers?

The key factor for managing a deployment is the maximum number of Files Under Management (FUM) for each Discovery Center instance. Since most customers cannot determine that number pre-deployment and before the first skim, it is best practice to plan based upon Volume Under Management (VUM) with an assumption that each TB of content consists of roughly 1 million files. For situations where this assumption does not hold, resources provisioned should be increased or decreased proportionately, with due consideration given to adding more Discovery Center instances if required (see below).

SQL Server

Due to the intensity of textual analysis on a SQL Server, dedicated SQL instances are generally recommended. An under-specified SQL Server instance will result in a poorly performing or failing Discovery Center activities:

- **Disk Space** - Disk space allocation is a critical resource due to database size and transaction log growth. Database size is driven by FUM.
- **RAM** - Insufficient RAM for the SQL host will result in an unresponsive database which may cause timeout or processing errors and potentially causing data corruption. Lack of RAM will result in poor reporting performance.
- **Processor Cores** - Too few processor cores will result in an unresponsive database.

Discovery Center Application Hosts

Discovery Centers need to be located close to geographically distributed content or where large volumes of content need to be indexed. Discovery Center hosts can be physical or virtual machines and the following should be considered when planning their specification:

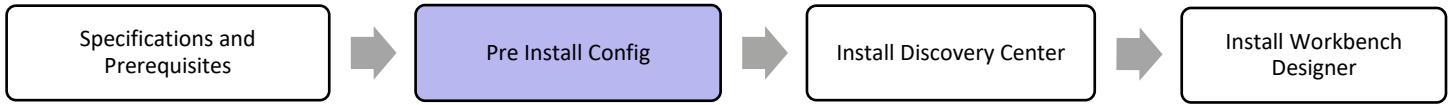
- **Processor Cores** - Too few processor cores will cause poor responsiveness in the web application. Additional cores will allow some index processing to occur in parallel, improving index analysis performance. It is assumed that for deployments with higher file counts, the analysis threads will be increased accordingly.
- **RAM** - Insufficient RAM will cause poor responsiveness in the web application.
- **Disk Space** - Disk space allocation will increase based on the classifications of larger indices, which drives the size of the search data held for indexes, which is required for classification. Disk space will also be needed for application logs and the file cache. Application logs can be deleted based on the system administrator's discretion, and file cache size will be dependent on the analysis thread count setting.

Multiple Discovery Centers

When Discovery Center is deployed in data centers that host large volumes of data to be analyzed, multiple Discovery Center SQL (index) databases can share a SQL server. ActiveNav recommends no more than four (4) index databases per SQL server. Disk space and compute resources should be scaled to support multiple Discovery Center instances.

Databases should follow a naming convention to provide clarity on the different instances that will be hosted on the SQL server. The Discovery Centers application should always be hosted on dedicated servers, even in sites with multiple instances.

Pre-Installation Requirements



Hardware Specifications

The specifications outlined below include minimum **Windows Server OS** requirements, based on the assumption that only Discovery Center applications and services are running on each server.

Note: When deploying Discovery Center and its SQL Server Database on to the same server, add together the CPU cores, Memory, and Hard Disk requirements for each server to provide sufficient capacity.

The table below displays the recommended resources for application and SQL environments based on estimated file counts. Compute resources should be increased as Files Under Management (FUM) grows.

Application Server (each)				DC	SQL/SSAS Server				TempDB (GB)	
Size: Files (m)	Disk (GB)	Cores	RAM	Instances	Databases	Disk (GB)	Cores	RAM	Data	Log
S: up to 25	200	4	8	1	1	250	4	8	25	25
M: 25 - 75	400	4	16	1	1	300	4	8	50	50
L: 75 - 100	600	8	16	1	1	400	8	16	100	100

TempDB sizing estimates if not using autogrow setting.

Under-resourced environments risk reduced performance and/or responsiveness.

Capacity limits of a Discovery Center instance are based on the deployment model being used. Application server cores can be added to support more analysis threads for increased text content analysis performance, and SQL Server cores can be added to improve system responsiveness and performance for reporting.

Although Discovery Center does not have a hard limit on the number of files a single instance can manage, exceeding the upper limit of 100M files is not recommended by ActiveNav as performance will degrade.

Adding Discovery Center Instances

There may be times when additional Discovery Center instances need to be deployed to address capacity issues.

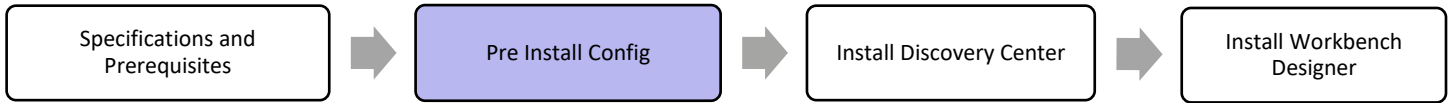
A planned Cap-and-Grow methodology is a recommended best practice where possible. Determining a threshold of when to add additional Discovery Centers can prevent load-balancing index migration exercises.

In over-capacity situations, the need to move indexes from one Discovery Center to another may be required to reduce the capacity of a Discovery Center instance.

Consideration & Recommendations:

- Moving indexes between Discovery Centers:
 - Move high-priority indexes or locations planned to be re-indexed post remediation.
 - Indexes should be removed from the original Discovery Center if they are moved to a different/new Discovery Center to avoid incorrect or double reporting.
 - Server level hosts can be removed from the Discovery Center Network Map which will subsequently remove all indexes from the Discovery Center while retaining Activity History and Actions Audit files. Any metadata manual Markup will have to be reapplied to the re-indexed location.
 - Specific paths can be deleted from the Indexing Overview.
 - If using the Discovery Center Management Reporting Database (MRD), the MRD should be reprocessed on both the original and destination Discovery Centers.

Pre-Installation Requirements



- SQL instances with multiple databases should process the reporting databases sequentially. Processing in parallel can exhaust the transaction log capacity.

Application logs should be deleted periodically to recover disk space on the application server. Retain only what you think you need.

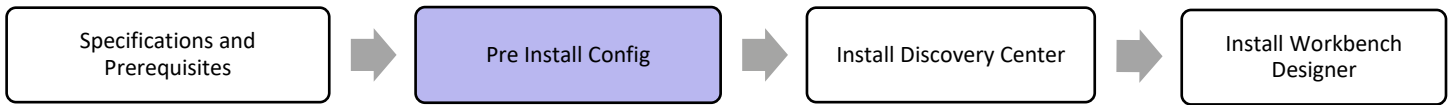
Client Applications

The specifications outlined below include minimum **Windows OS** requirements for workstations used to install and run Discovery Center client applications such as the Workbench and Regex Validator Windows Desktop applications.

Processor	64-bit quad-core
Memory	4GB RAM
Hard Disk	2GB



Pre-Installation Requirements



Software Prerequisites

Discovery Center SQL Server Database Requirements

Microsoft SQL Server 2019 or later, with the latest service packs and installed components and services:

SQL Server Database Engine Services
SQL Server Analysis Services (SSAS)

Configuration for SQL Server

The **SQL Server Analysis Services** Instance **must** use a **multidimensional** model (Tabular and PowerPivot models are not supported).

Discovery Center Server

Windows Server 2016 or later with the latest service packs with the following features and server roles enabled:

Most modern browsers
Microsoft .Net Framework 3.0 or 3.5 Server Feature
Microsoft .Net Framework 4.8 or later
Internet Information Services (IIS)

The **Microsoft Universal CRT package** must be available on the Discovery Center Server; this is a standard component for Windows 10 and Server 2016 onwards.

Note: For earlier versions of Windows, it can be installed via Windows update; see <https://support.microsoft.com/en-gb/help/2999226/update-for-universal-c-runtime-in-windows>.

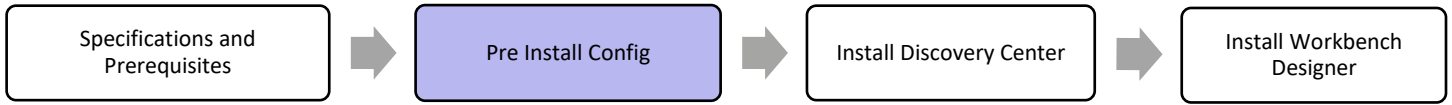
For stable operation of the MIP SDK, the **Microsoft Visual Studio C++ Runtime 14.0** is a pre-requisite for Discovery Center Release 4.20 onwards. The installer will check the registry to determine the version installed and installation or upgrade will not proceed if a valid version is not detected. The latest version can be downloaded at https://aka.ms/vs/17/release/vc_redist.x64.exe

Client Application Workstations

Windows 10 or later
Most modern browsers
Microsoft .Net Framework 4.8 or later



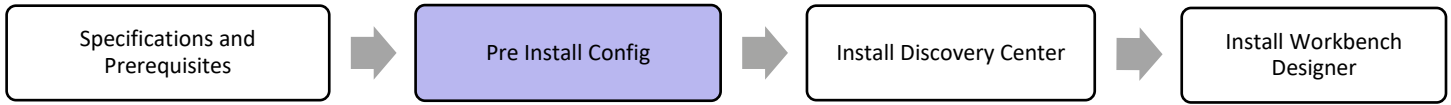
Pre-Installation Requirements



Note: Running the Discovery Center user interface within multiple browser sessions, from a single client workstation, may cause it to become unresponsive. To remediate this, excess instances of the user interface should be closed.



Pre-Installation Requirements



Network Connections

Discovery Center's performance is dependent on the quality of network connections between its components.

Discovery Center <-> SQL Database Server:

Must be on the same Network Switch

High Performance **1GB** Ethernet with **<1ms** Latency

Discovery Center <-> Repository:

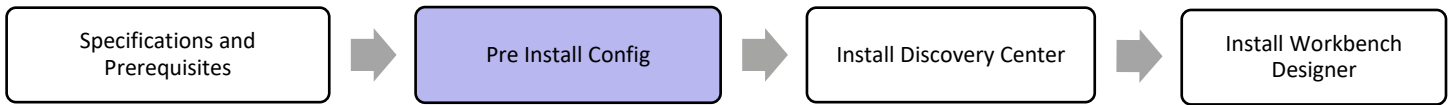
LAN Quality **<50ms** Latency

Discovery Center <-> Client Applications:

LAN Quality **<50ms** Latency

Virtualization

Discovery Center works well in a virtualized environment. SQL Server and its host must be configured per Microsoft and the relevant virtual host recommendations.



Pre-Installation Requirements

The following items and information are required during the installation process and initial configuration of ActiveNav.

Windows Accounts and Groups

Installation User Account

The installing user account must have rights to install software and configure IIS

IIS Administrators rights

SQL Server rights*

SSAS rights*

*See SQL Server Configuration for further information

User Roles

Create the following **groups** on your **Domain Controller** and assign users as necessary.

ActiveNav System Administrator

Discovery Center Network Map and Systems Settings Tabs. After installation, any user account that is a member of the local administrator's group will be assigned to this role.

ActiveNav Administrator

Discovery Center Indexes and Metadata Tabs.

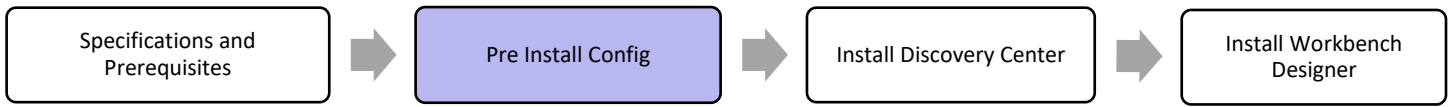
ActiveNav Information Manager

Discovery Center Areas of Interest and Reporting Tabs.

ActiveNav Reviewer

Discovery Center Reporting tab with restricted capabilities.

Pre-Installation Requirements



Service Accounts

Create two or more accounts to control the Discovery Center services.

Scheduler Service

This user (e.g., ANScheduler) can be given read access for the data files to be indexed, OR specific credentials can be provided to Discovery Center. Successful installation and operation of the Discovery Center application requires the following rights:

Logon As A Service for Discovery Center host server

SSAS host login rights

This is normally available by default. In tightly controlled environments, ensure this is checked in advance to ensure that the Process Reporting Database task can access SQL data.

Discovery Center Web Application Service

This account (e.g., ANWebSite) will be used to run the Discovery Center web application and restrict access to the Discovery Center temporary files and database. Successful installation and operation of the Discovery Center application requires the following rights:

Allow log on locally for Discovery Center host server

Choosing Between Local Computer and Domain Accounts

Discovery Center can be configured to use service accounts, either in a Windows domain or as local computer accounts. This choice will affect options for managing user access to the Discovery Center user interface.

Local Computer

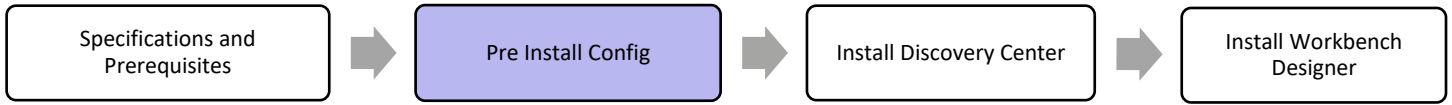
This will prevent groups defined in the local domain from accessing the Discovery Center. These must be configured as local groups on the Discovery Center server. Alternatively, local computer or domain user accounts can be added explicitly to Discovery Center roles via the User Access Tab.

Domain Accounts

The Discovery Center host server must be joined to the appropriate domain to allow users to use existing domain accounts to authenticate with the Discovery Center user interface. This allows the server to successfully validate user credentials when users attempt to log in to the system.

Note: For installations joined to a domain, domain service accounts **must** be used to avoid authentication and authorization problems. Using a database server **separate** from the Discovery Center will require domain accounts to support authentication.

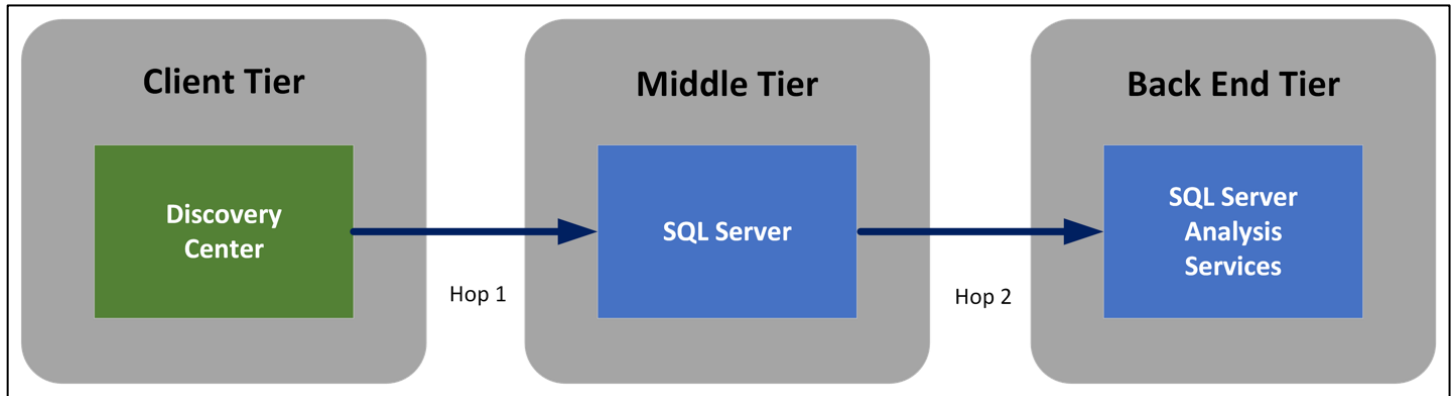
Pre-Installation Requirements



Validate Configuration for a Fully Distributed Deployment

When planning a fully distributed configuration (i.e., Discovery Center, SQL Server, and SQL Server Analysis Services are installed on independent systems), review the requirements in [Appendix 7: Additional Configuration for Fully Distributed Configuration](#) to ensure that this configuration can be supported.

This configuration involves communication between components, as shown in the diagram below. To produce reports, the Discovery Center must be able to access data from **SSAS** via **SQL Server**, creating a situation known as **Double Hop Authentication** requiring SQL Server to present credentials from the Discovery Center service accounts to the Back End Tier.



Internet Information Services

The Discovery Center host server requires the **IIS role**. Using **Windows Server Roles Service Manager**, add the following role services:

Common HTTP Features:

- Default Document
- HTTP Errors
- Static Content
- HTTP Redirection

Health and Diagnostics:

- HTTP Logging

Security:

- Request Filtering
- Windows Authentication

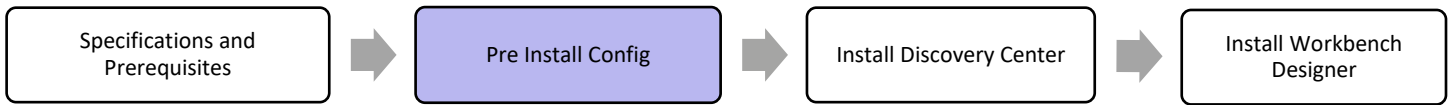
Application Development:

- .NET Extensibility
- ASP .NET
- ISAPI Extensions
- ISAPI Filters

Management Tools:

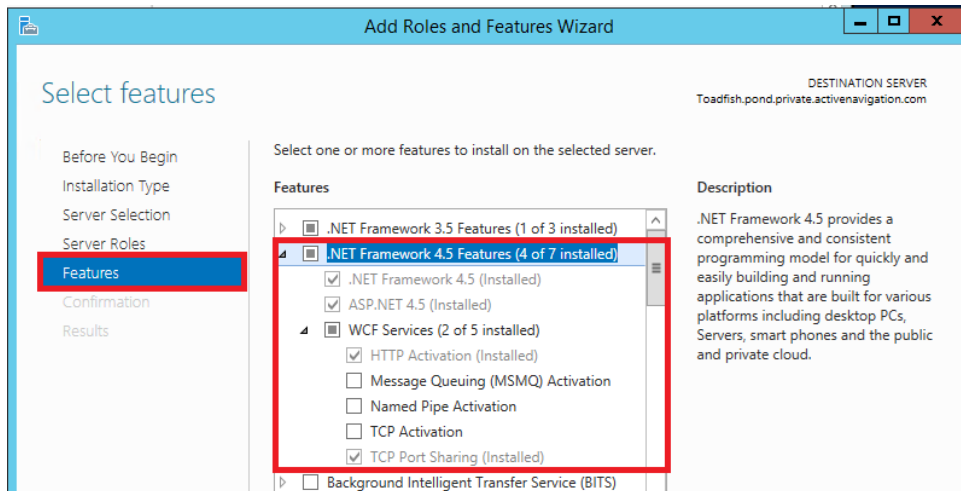
- IIS Management Console
- IIS6 Metabase Compatibility

Pre-Installation Requirements



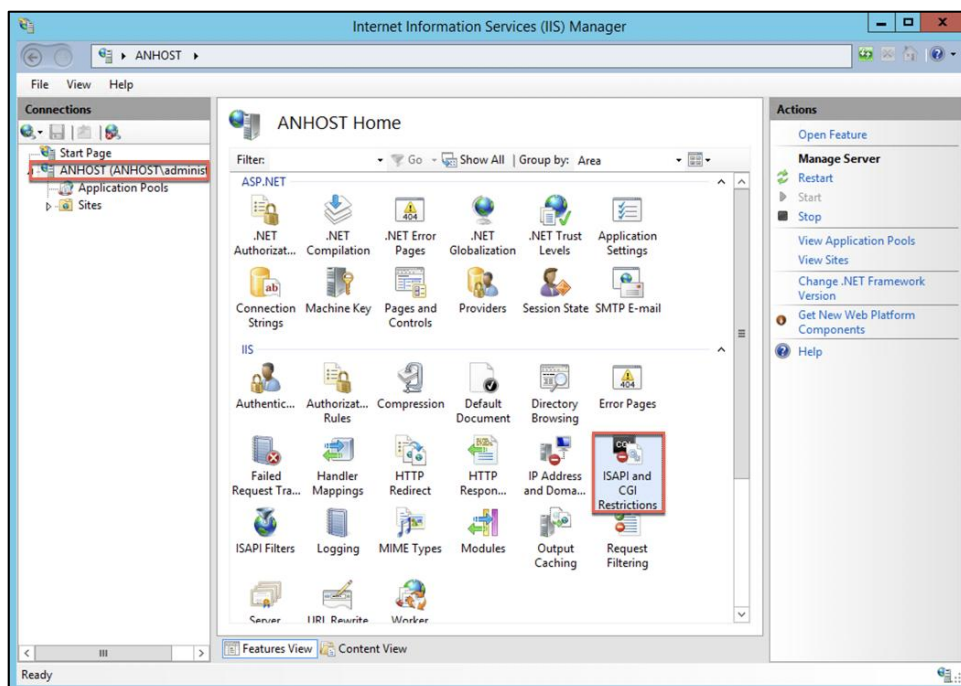
.NET Framework

1. The Discovery Center host server requires **.NET 4.8** or later to be installed, and **.NET Server Features** enabled with Windows Communication Framework as shown below (Windows Server 2012 R2 is shown).

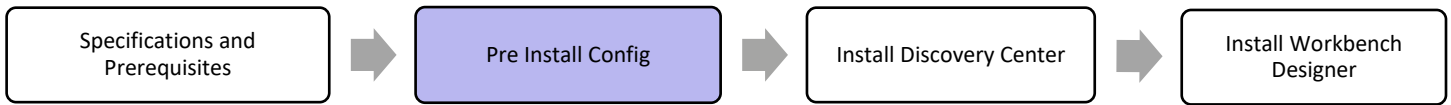


Note: Server feature dialogs will show different versions of **.NET** according to the specific operating system version in use. On **Windows Server 2012**, the options should be set in the **.NET Framework 4** folder.

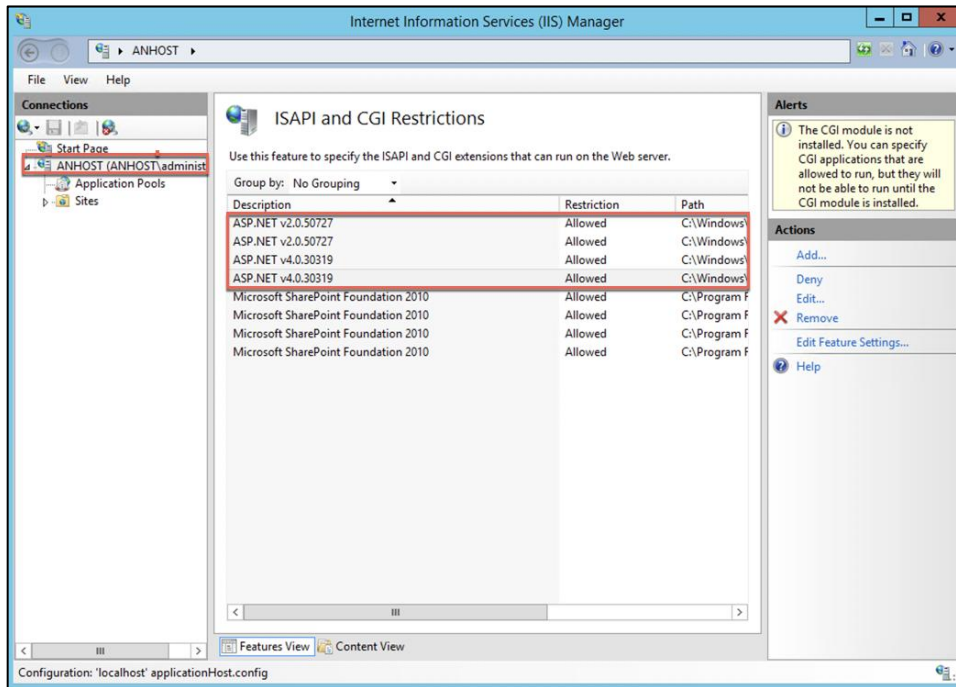
2. Enable (or confirm) that **ASP .NET 4** applications can run. To do this, open **IIS Manager** and edit **ISAPI and CGI Restrictions** for the installation.



Pre-Installation Requirements



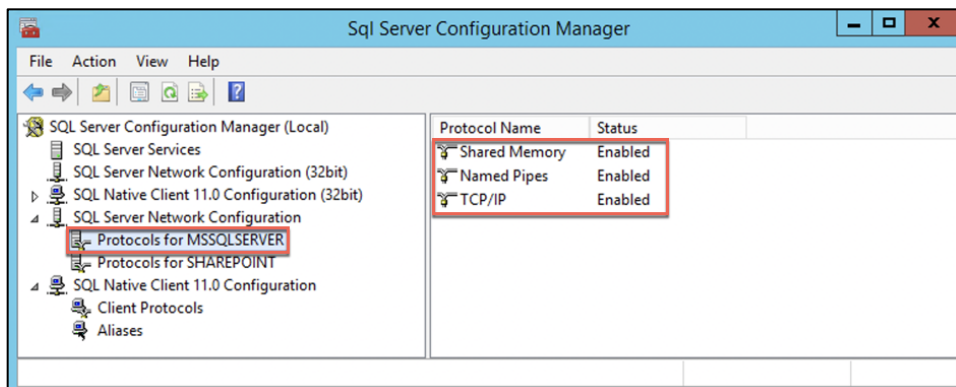
3. Locate the restrictions in place for **.NET 4** and set each to **Allow**, as shown below.



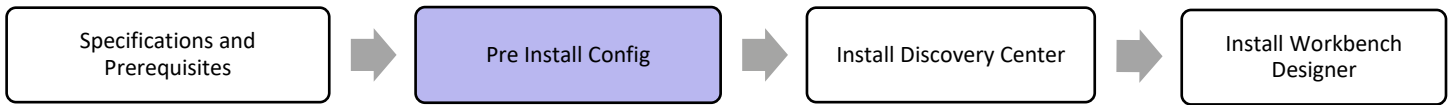
SQL Server Configuration

Verify the Discovery Center SQL Server and SSAS configuration as follows:

1. Confirm that the **SQL Server Configuration Tools** are installed.
2. From **SQL Server Configuration Manager**, note the machine names and instances for SQL Server and SSAS.
3. Note the Windows service account names for **SQL Server** and **SSAS**.
4. Confirm the **SQL Server** instance is configured to provide **Windows Authentication Mode** (also known as Integrated Security).
5. Using **SQL Server Configuration Manager**, confirm that **Shared Memory**, **TCP/IP** and **Named Pipes protocols** are enabled for **SQL Server Network Configuration** (see below).



Pre-Installation Requirements



Assign SQL Server Privileges to Installation Account

The user running the Discovery Center installer should be:

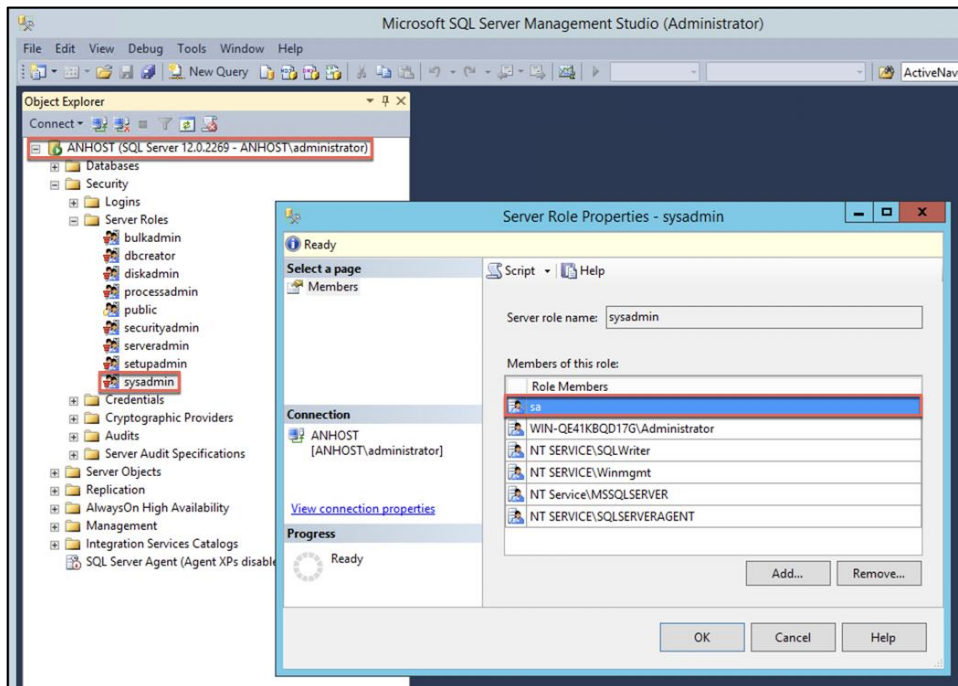
- Assigned the **SQL Server sysadmin role** in SQL Server
- Be a member of the **System Administrators group** for the SSAS instance

*After installation or upgrade, the installing user can have these privileges revoked.

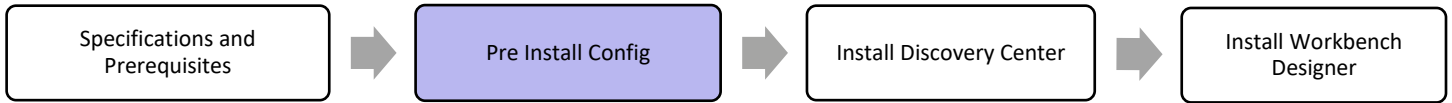
The Discovery Center installer must do the following:

- Create or use a number of logins for the SQL Server.
- Create and configure a SQL database and SSAS cube.
- Makes settings required to support the required SQL CLR assemblies.

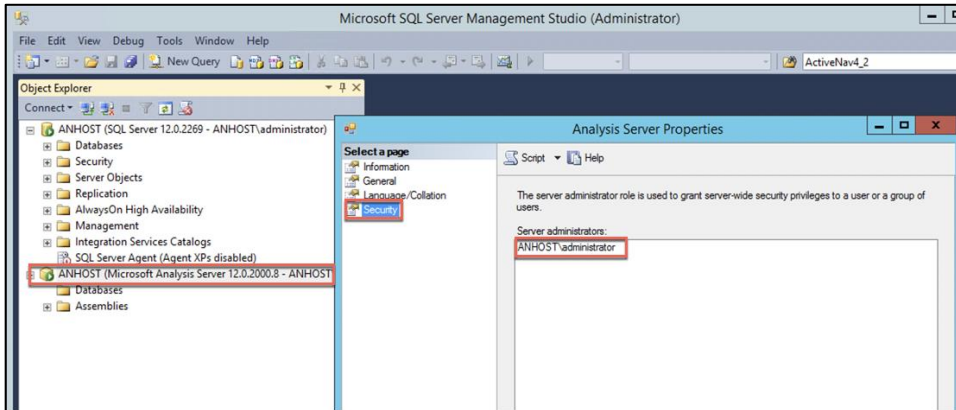
Users with SQL Server administration privileges will be in the **sysadmin role**, shown in **SQL Server Management Studio**:



Pre-Installation Requirements



Users in the **SQL Server SSAS System Administrator** role will appear in **SQL Server Management Studio**, as shown below:

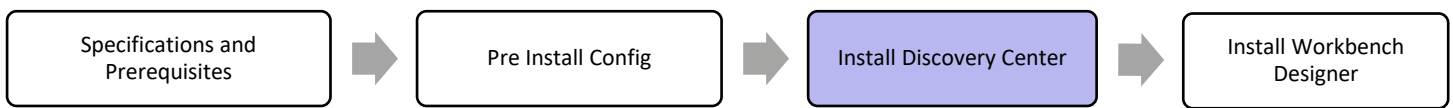


SQL Server Logins

The accounts that run the following services must be able to login to the SQL Server (relational) database to allow Discovery Center to operate.

Discovery Center Scheduler service account
Discovery Center Web Application service account





Installing Discovery Center

Before starting the install, gather the required information and check prerequisites (See [Appendix 1: Installation Checklist and Notes](#)).

Download the installer for **Discovery Center 4.20.0** from the ActiveNav support site <https://support.activenav.com>. Once signed into the support website, click on **Downloads**, then click on **Discovery Center 4.20.0** under **Product Downloads**.

The Discovery Center 4.20.0 zip file contains:

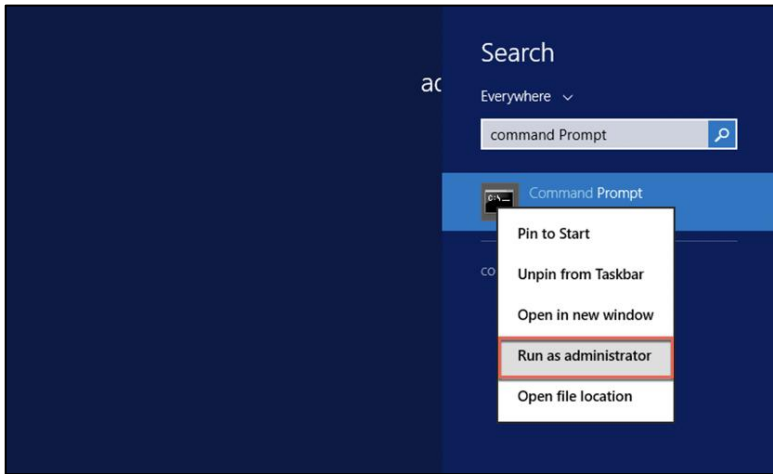
- ActiveNav Discovery Center Software
- ActiveNav Discovery Center Workbench Application
- ActiveNav Regular Expression Validator Application
- ActiveNav Discovery Center Documentation

Run the setup wizard (using the installing user account), follow these steps to start the **ActiveNavigation.Setup.msi** file:

1. Discovery Center host server: Open **Services** and confirm the **IIS Admin Service** is running.

Hyper-V Time Synchronization Service	Synchronizes th...	Running	Manual (Trig...
Hyper-V Virtual Machine Management	Management s...	Running	Automatic
Hyper-V Volume Shadow Copy Requestor	Coordinates the...	Running	Manual (Trig...
IIS Admin Service	Enables this ser...	Running	Automatic
IKE and AuthIP IPsec Keying Modules	The IKEEXT serv...	Running	Automatic (T...
IncrediBuild Agent	Reports Agent s...	Running	Automatic

2. Discovery Center host server: Navigate to **Start**, open a **command prompt** with elevated privileges using the **Run as an administrator** option.

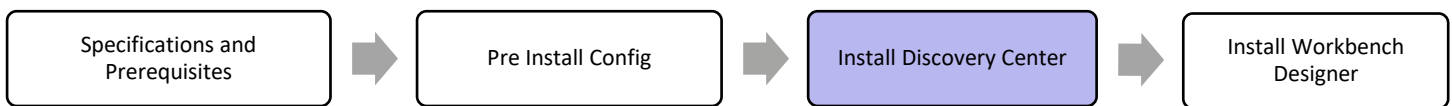


3. Discovery Center host server: Run the following command:

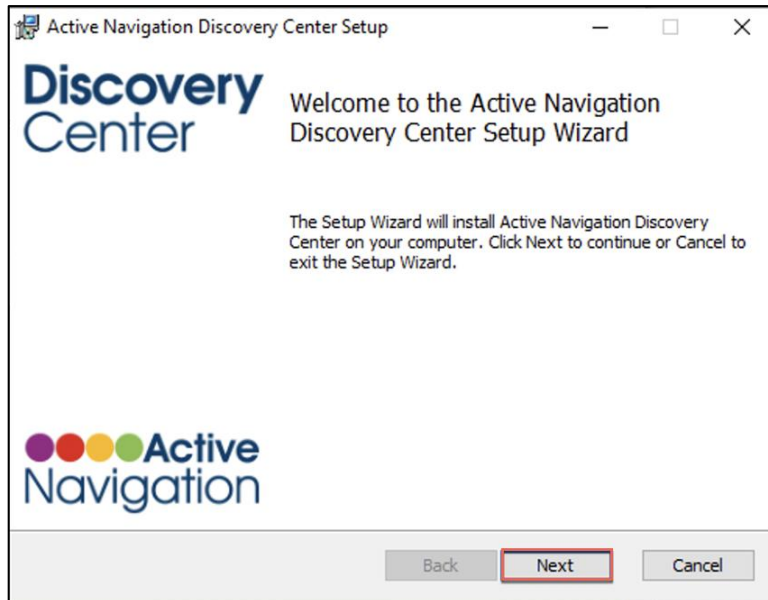
```
msiexec /package <ActiveNavigation.Setup.msi> /!<install.log>
```

Replace **<ActiveNavigation.Setup.msi>** with the name of the downloaded **Discovery Center msi** file and replace **<install.log>** with the name of the log file that will be created.

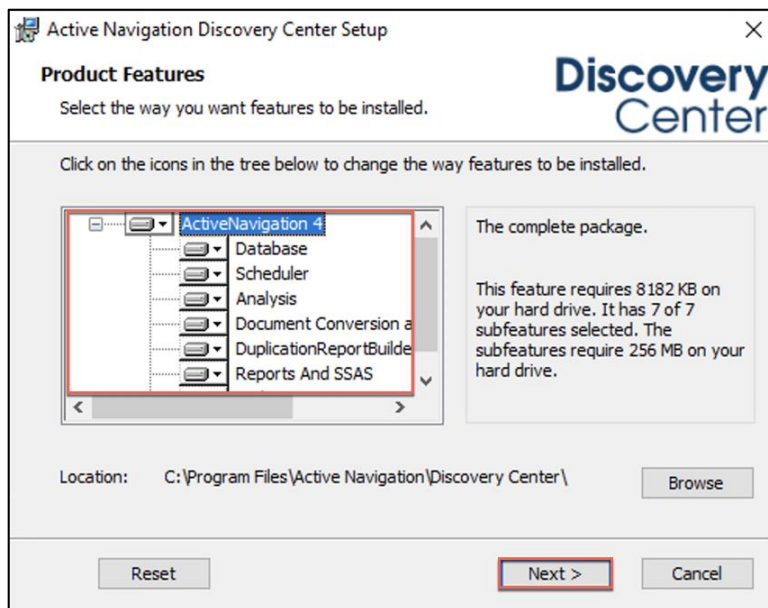




4. Follow the directions provided by the setup wizard. The wizard will check for several prerequisite items and provide an error notification if they cannot be located.



5. Read and accept the License Agreement by checking the box and then clicking **Next** (or cancel as appropriate).
6. **Product Features** allow you to skip specific parts of the installation if they are not needed. Seek advice from ActiveNav Support before electing to omit any part of the installation.





7. Use the **Browse** button to enter any custom locations required for the search data, file cache, or log file locations. By default, these will be created within the Discovery Center directory, as shown in the **Working File Locations** dialog. Provide alternate locations to distribute the working files between disks for performance or storage space reasons.

Active Navigation Discovery Center Setup

Working File Locations
Locations for data and temporary files

Classification data location
C:\Program Files\Active Navigation\Discovery Center\SearchData\ Browse

File cache location
C:\Program Files\Active Navigation\Discovery Center\FileCache\ Browse

Log files location
C:\Program Files\Active Navigation\Discovery Center\Logs\ Browse

Active Navigation Discovery Center creates log files and temporary data on disk during operation. In a default installation these will be in locations within the install folder. You can choose alternative locations here, for example to choose locations with more free space than is available in the install folder. See the installation guide for more information.

< Back Next > Cancel

8. Provide **username** and **password** for the **Windows account** to be used by Discovery Center Scheduler Service.

Note: Ensure that the account has been assigned **Logon as a Service** rights to enable account validation to succeed.

Active Navigation Discovery Center Setup

Scheduler settings
Set scheduler service identity

Enter scheduler service account details

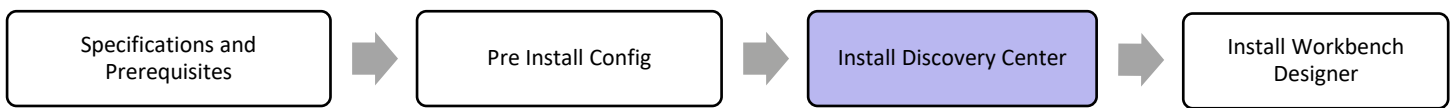
Username must be in form 'DOMAIN\Username' or 'COMPUTERNAME\Username'

Username

Password

It is recommended that you create a service account on your Domain Controller that has permission to read and write to all of the file shares that you expect to work with. Alternatively you can choose an account with lower privileges, but then you will have to specify a user name and password for each index that you create in Active Navigation.

< Back Next > Cancel



9. Enter details for the database instance:

Active Navigation Discovery Center Setup

SQL Server settings
Enter the SQL Server instance and database names

Enter SQL Server instance name

Enter database name

< Back **Next >** Cancel

- Enter the **SQL Server Instance name** in the form of **<database server name\instance name>**.
- Enter a **database name** that Discovery Center will use. If using a non-default, static port, append a comma and the desired port after the instance name.

Note: For multiple Discovery Center instances, ensure that the database names uniquely identify each one (e.g., AN1, AN2, etc.). This name will also be used for each SSAS reporting database.

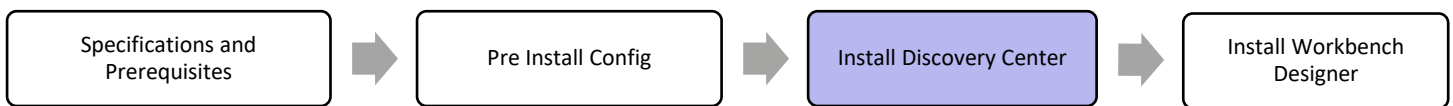
10. Enter the **Analysis Services instance name** in the form of **<server name\instance name>**. If using a non-default, static port, append a comma and the desired port after the instance name.

Active Navigation Discovery Center Setup

SSAS Instance (Reporting Database)
Enter the SQL Server Analysis Services (SSAS) instance name

Enter Analysis Services instance name

< Back **Next >** Cancel



11. Select the **Create new site** option, then click **Next**.

Note: For a deployment to an HTTPS web site see Appendix 2.

Active Navigation Discovery Center Setup

Web site settings

Create new web site or select existing one

☒ Create new site

☐ Select existing site

Back Next Cancel

12. The IIS web site details and application pool details will be populated by default. **Do not change these unless you need to meet specific installation requirements.**
13. Enter your **Username** and **Password** for the Application Pool (the service account to be used by the Discovery Center web application). The website will use this account to access the Discovery Center database.

Active Navigation Discovery Center Setup

Web site settings

Enter new web site settings

Application Pool

Create ASP.NET 4.0 pool with this suffix

ActiveNavigationDiscoveryCenter

Enter account details for Application Pool

Username AN\TestAppPool Password

Site Settings

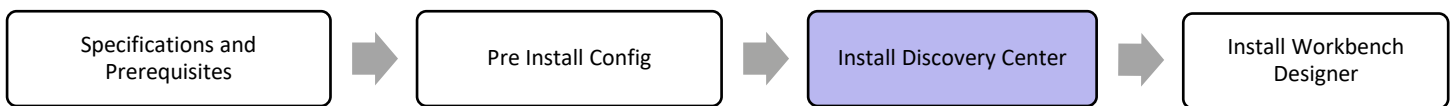
Site name ActiveNavigationDiscoveryCenter

Site port 805

Physical path C:\inetpub\wwwroot\AN40web\

Browse

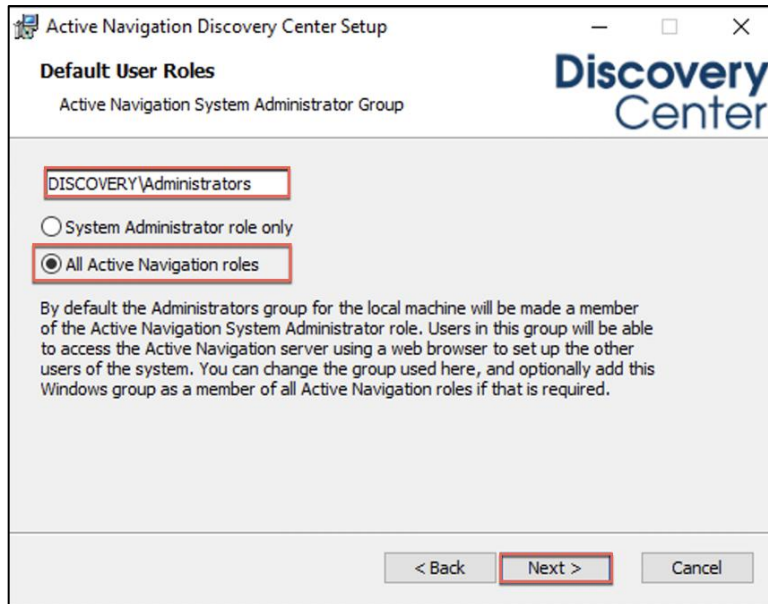
< Back Next > Cancel



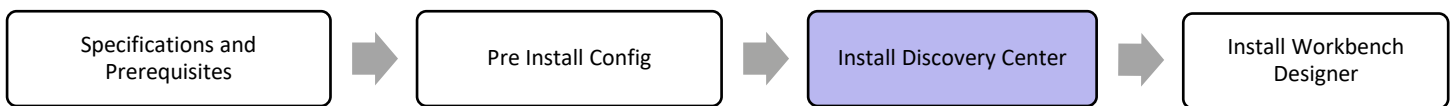
14. The local machine **Administrators** group will be assigned the Discovery Center System Administrator role by default.

Provide a different Windows group if required.

Note: A member of this group of users is responsible for applying the Discovery Center License file after a clean installation and assigning roles to any additional users.



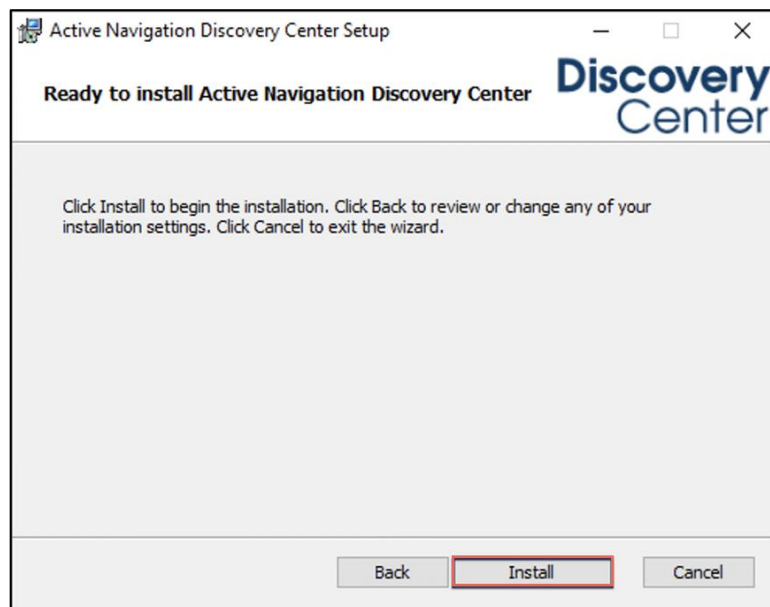
Select the **All Active Navigation roles** option; this will assign the chosen group to **all Discovery Center roles** (If this is not selected, the group will have to delegate these responsibilities to themselves after installation).



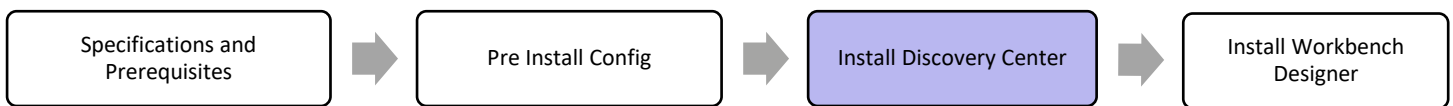
15. Verify all the settings entered before the install takes place, then click **Next**.



16. Click **Install** to setup the Discovery Center, its database, and all other supporting assets.



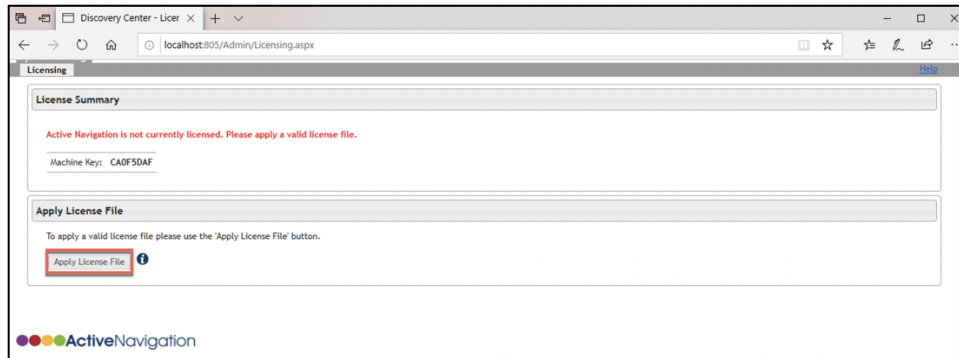
17. Installation progress will be indicated on the installation status bar and summary text. Click **Finish** when complete.



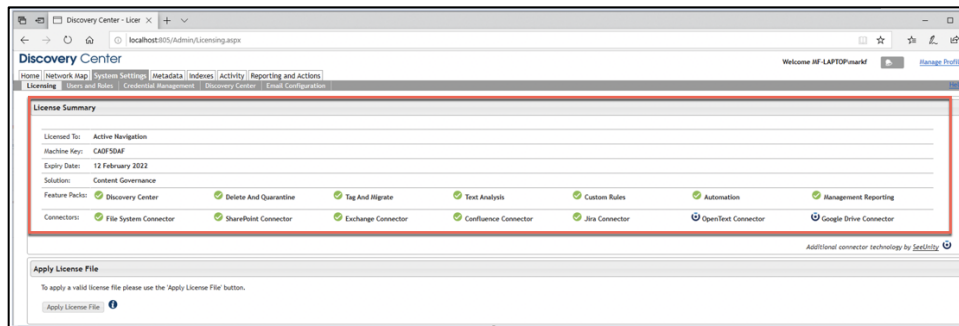
Discovery Center Post-Installation Functional Checks

Run the following tests once the installation is complete to ensure that the installation is configured correctly:

1. Open Discovery Center from your internet browser <http://localhost:805> and enter your credentials if prompted.
Note: You may need to modify your browser security settings and add the Discovery Center to the list of trusted sites.
2. After a successful installation, log on as the user assigned the System Administrator role. When logging into the Discovery Center for the first time, the system will need to be activated. The License Management Page will be displayed; click **Apply License File** and follow the prompts to activate the system.



3. If the License is accepted, a summary of the licensed features will be displayed. If errors are encountered during these steps, check the post-installation requirements provided in [Appendix 1: Installation Checklist and Notes](#).



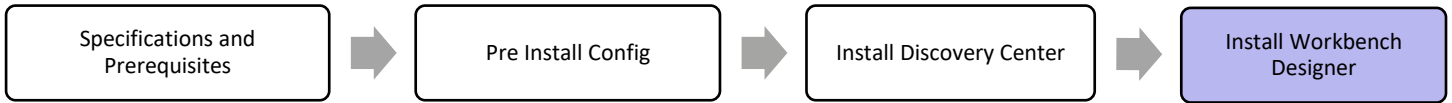
Complete Initial Set Up

If all the following steps have been completed, the installation was a success. For further information, refer to the Discovery Center's documentation by clicking on the **Help** on the right side of the Discovery Center Interface.

1. Note the URL for the Discovery Center; this will be needed when installing client applications.
2. Configure Discovery Center roles.
3. Build a Network Map and schedule Network Discovery.
4. Run a test index.

Generate a test report to validate the configuration

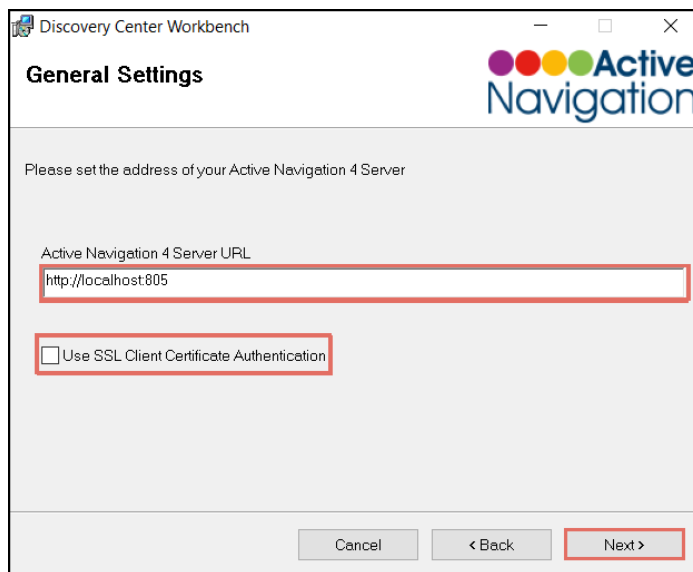
Install Discovery Center Workbench Designer



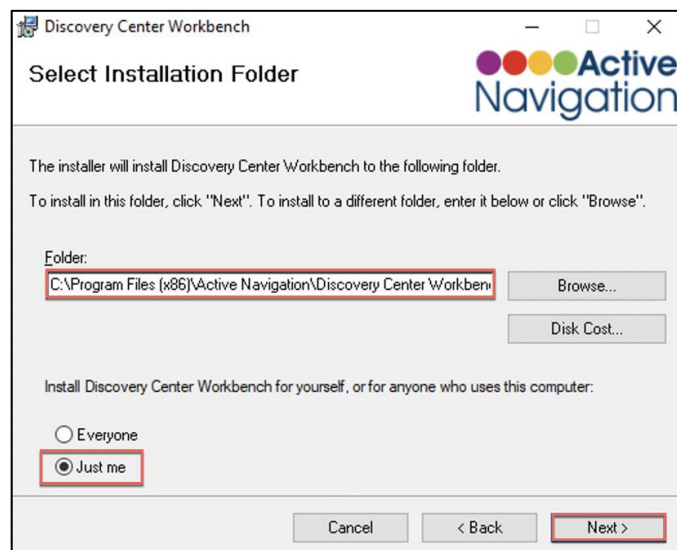
Install Discovery Center Workbench Designer

Discovery Center Workbench is usually installed on a client machine and requires network connectivity to a Discovery Center instance.

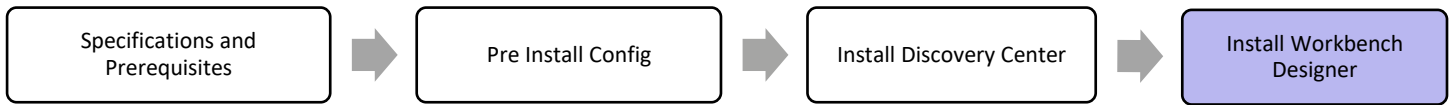
1. Locate and run the **DiscoveryCenterWorkbench.msi** installation file and follow the prompts.
2. In the **General Settings** window, when prompted for the **Active Navigation 4 Server URL**, enter the Discovery Center installation URL using the following format <http://servername:port/>.
3. Select the **"Use SSL Client Certificate Authentication"** checkbox if Workbench should authenticate with Discovery Center using client certificates or smart cards. This requires the certificates to be present in the user's personal certificate store.



4. Unless you wish to change the install location, accept the default install folder, and choose whether to install for all users of this computer or just the current user.



Install Discovery Center Workbench Designer



5. Confirm the install by clicking **Next**, followed by **Close** upon completing the install.

Launch the **Discovery Center Workbench** application and check the results of an index run to test the Discovery Center installation.

Appendix 1: Installation Checklist and Notes

Pre-Installation Requirements and Information

Windows Accounts

- Identify the **installing user account** (the user account will be used to run the installer).
It will require **SQL Server sysadmin, SSAS Server Administrator, IIS Administrator** rights.
- Provide **Windows service account** for **Discovery Center Scheduler Service**. Name as required (or **ANScheduler**) and grant with **Logon as a Service** rights. During installation the account will be granted:
dbo, datareader, and datawriter roles to the **SQL Server database**.
ANProcessor role on the **SQL Server SSAS database**.
- Provide **Windows service account** for **Discovery Center Web Application**. Name as required (or **ANWebApp**). During installation the account will be granted:
Full Control permissions on the **AN40web** folder only.
Datareader and **datawriter** roles to **SQL Server database**.
ANprocessor role on **SQL Server SSAS database**.
- Provide **Windows account or group** for ActiveNav **System Administrator** users.

SQL Server Security

Confirm presence of **SQL Server** logins for the **SSAS service accounts**. Set up these logins if they do not exist.

SQL Server Configuration

Configure **SQL Server** network protocols for use of **Shared Memory, Named Pipes** and **TCP/IP**.

Discovery Center Host Server Configuration

- Enable **Windows Server 4.X.Net Features** including **WCF Activation** (See [.Net Framework](#)).
- Install **.NET 4.8** or later.
- If using **SSL** and **HTTPS**:
Create a valid security certificate.
Create an **IIS website** with **HTTPS binding** and apply the certificate.
- Add the **IIS role** to the **Discovery Center**. Add the following role services to the IIS role:

Common HTTP Features:	Windows Authentication
Default Document	Application Development:
HTTP Errors	.NET Extensibility
Static Content	ASP .NET
HTTP Redirection	ISAPI Extensions
Health and Diagnostics:	ISAPI Filters
HTTP Logging	Management Tools:
Security:	IIS Management Console
Request Filtering	IIS6 Metabase Compatibility
- Ensure the **IIS Admin Service** is running on the **Discovery Center Server**.
- Ensure that **Microsoft Visual Studio Runtime 14.0** is installed at build 35211 or later. Latest version is available at https://aka.ms/vs/17/release/vc_redist.x64.exe



Post Installation Requirements and Information

Windows Accounts

Provide **Windows account** for **other user roles** according to project requirements.

Default Ports Used

Web connection to Discovery Center: 805 TCP, 443 TCP for HTTPS

Remote SQL Server: 1433 TCP

Remote SQL Server Analysis Services: 2383 TCP

Remote SQL Browser Service (required for named instances): 1434 & 2382

Indexing connection to file servers: 445 TCP

NetBIOS name recognition: 137 & 139 TCP 137 & 138 UDP

DNS: 53 TCP, 53 UDP

Indexing connection to SharePoint: 80 TCP, 443 TCP for HTTPS

SQL Server

- Pre-allocate disk space for **SQL database** according to project requirements.
- Validate database recovery model and backup plan according to local database management policies.

<https://msdn.microsoft.com/en-us/library/ms191164.aspx>

<https://msdn.microsoft.com/en-us/library/ms190217.aspx>



Appendix 2: Configuring for SSL and HTTPS

Discovery Center can be configured to provide secure access using an **HTTPS://** URL. This protects against the possibility of data sent to a web browser being intercepted by network monitoring tools.

To create your secure HTTP site, you will need to **configure a secure site in IIS** and then **install the Discovery Center application into this site**.

Preparing a Secure Site

Choice of SSL Certificate

An HTTPS based site requires an **SSL certificate** that enables a browser to validate the site when negotiating a secure connection. There are two options, signed by a trusted root authority or self-signed certificate:

1. Signed by Trusted Root Certificate Authority

Typically for a production deployment, a certificate is prepared for the **specific hostname** and signed by a **trusted root certificate authority**. Follow the procedures set out by your organization to obtain a certificate and complete the configuration of a secure site for use by the Discovery Center installation.

2. Self-Signed Certificate

When setting up a secure site, **IIS will allow a self-signed certificate**, this type of certificate will not include a trusted certificate authority signature. When using a self-signed certificate with Discovery Center, the following factors will affect the use of such a certificate by Discovery Center:

- A self-signed certificate must be added to the **Trusted Root Certification Authorities** folder in the local machine account's certificate store.
- End users will see a security warning when accessing the secure site with a web browser, requiring confirmation that they are prepared to access a site with an untrusted certificate. It is possible to install the certificate as a **trusted** certificate on end user's systems to avoid these warnings, or users may add a security exception in their browser configuration.

Preparing an SSL Certificate

To prepare an SSL certificate for use with IIS:

1. Open **IIS Manager**.
2. Select the **server name** in the hierarchy in the left-hand pane.
3. Locate and open the **Server Certificates** item in the right-hand pane.
4. If using a **trusted certificate** from a 3rd party, choose the **Import** option to add the certificate to IIS.



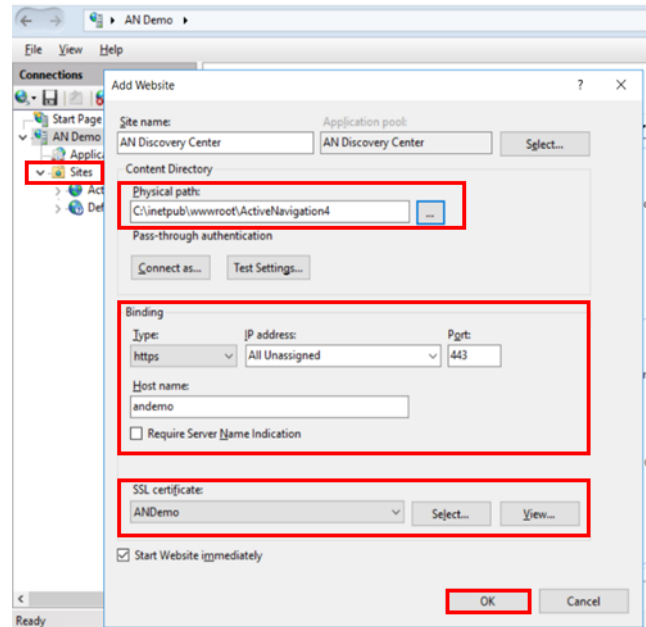
5. If creating a **self-signed certificate**, choose the **Create Self-Signed Certificate** option:

- Enter a **name** for the certificate.
- If offered a choice of certificate store, select **Web Hosting**.

Preparing a Secure Site in IIS

Complete the following steps to configure the secure site to receive the Discover Center installation:

1. **Create a new folder** within the IIS root directory, where the web application files should be installed. The default location for the root directory is 'C:\inetpub\wwwroot\'.
Add Web Site.
2. Open IIS Manager. Right-click the **Sites** node and choose **Add Web Site**.
3. Enter a **name** for the site.
4. Specify the **location** where the web application files should be installed. This should be the folder created in step 1.
5. Select **HTTPS** as the binding type.
6. Specify the **hostname** for the site. This should match the **hostname** used for the **SSL certificate**.
7. From the drop-down list, select the **SSL certificate** configured in the previous stage.
8. Select **OK** to create the website.



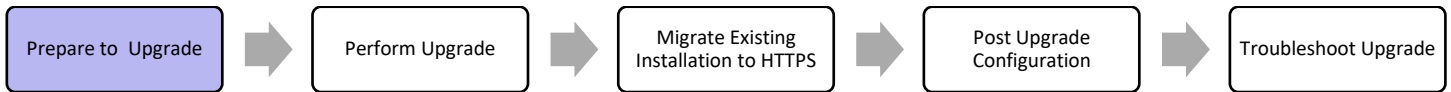
Once created, check access to the empty website. If using a self-signed certificate, a security warning will require a browser exception to be added. If the site creation is successful and the certificate is correctly applied, a warning will be displayed with the message "The Web server is configured to not list the contents of this directory".

Install Discovery Center to an Existing Secure Site

Follow the standard installation steps outlined in [Installing Discovery Center](#) until step 11, Web site settings. At the Web site settings dialog, choose the **Select existing site** option.

On the next page, configure the Web Application service account as in the standard installation, and select the **secure web site** from the **Select web site** drop-down list.

Proceed through the remaining steps for the standard installation. When the install is completed, ensure end-users can successfully access the **Discovery Center** using the **secure website address** and that the **Discovery Center Workbench** can be used to interact with the **Discovery Center web services** without any errors.



Appendix 3: Upgrading an Existing Installation

Discovery Center Release 4.2 SP1 and onwards upgrades are fully supported by the standard installation package. For earlier releases, contact support@activenav.com for assistance with a manual upgrade.

To upgrade client applications such as the Discovery Center Workbench, perform an uninstall, followed by installing the latest version.

Preparing to Upgrade

Review the release notes and this installation guide for the new release to identify any changes in software prerequisites that may affect your installation. Ensure that any new requirements are met before starting your upgrade.

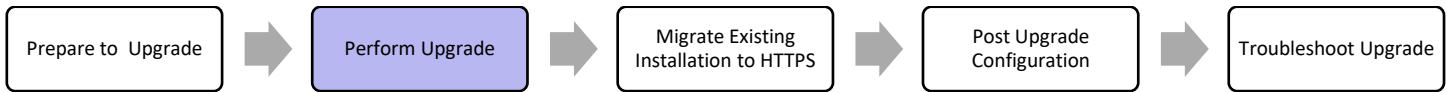
Note: Before upgrading, perform a **database backup** and ensure that the resulting backup file is safely stored. In the event of any error in the automatic upgrade process, it will be necessary to perform a manual upgrade described in the [Troubleshooting Upgrades](#) section.

1. If any standard classification structures, e.g., **File Sizes**, **Filetypes (by Extension)**, or **Filetypes (by Format)**, have been modified, ensure that copies of those structures have been made.
2. Review the release notes to check whether any classification structures have changed, merge the updated structures if appropriate.
3. Review the release notes to check whether there are any existing unsupported indexes.

Close Existing Browsers

Ensure that all users have closed any existing browser sessions accessing Discovery Center; if users see incorrectly displayed elements or unexpected errors, press **Ctrl + F5** to reload the page with a cache refresh to see if this resolves the problem.





Performing an Upgrade

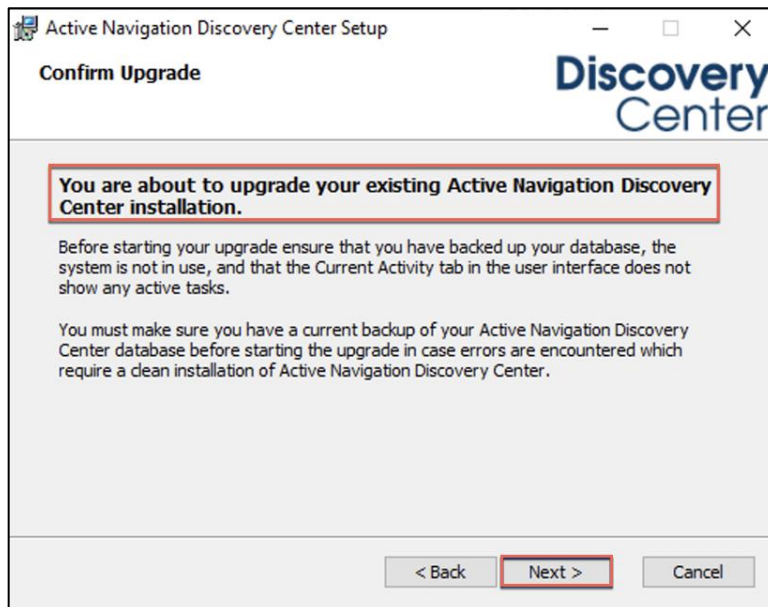


Do not attempt to upgrade Discovery Center while logged in using the Discovery Center Scheduler service account; this may affect the ability of the updater to make required changes and will require additional manual configuration (see [Troubleshooting Upgrades](#)).

1. To perform an upgrade, launch the installation package on the Discovery Center host server (See [Installing Discovery Center](#) for further information).

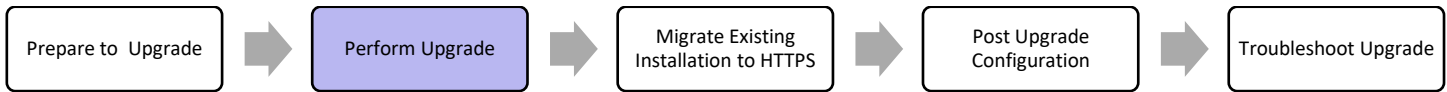
Note: Any changes made to the system configuration since installation may result in the need for additional manual action after the upgrade; take **backups** of the **configuration files** and **account names** to assist in this process **before** proceeding with this process.

2. When the installer is run, it will detect the existing installation and display the following upgrade confirmation dialog. Click **Next**.



3. Proceed with the upgrade installation, following the wizard prompts. The installer will read and use the settings provided during the initial installation.



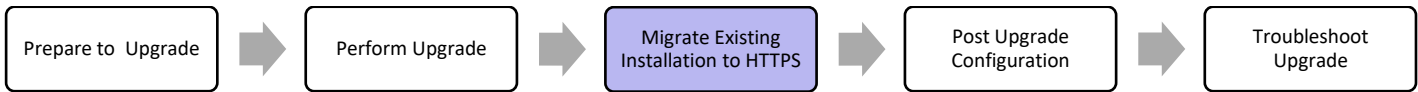


4. The upgrade will require **passwords** for the **Scheduler Service** account and, if applicable, the **Discovery Center Web Application** service account.

5. Upon entering valid passwords, a summary screen is displayed showing the settings that have been detected and used for the upgrade.

Note: It is **not** possible to update settings during an upgrade. If changes are required to any existing settings, **Discovery Center** should be **uninstalled** and a **clean install** performed using the **existing database**.





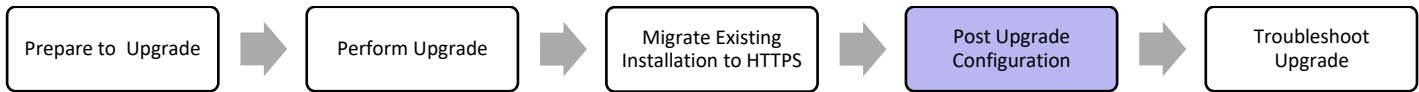
Migrating an Existing Installation to HTTPS

From Release 4.3.9, the Discovery Center installation package supports direct installation to a web application configured for HTTPS. However, this is not possible where a manual configuration has been used to create an HTTPS configuration or for migrating an existing installation to HTTPS. In such cases, you can migrate Discovery Center to HTTPS as follows:

Note: Before upgrading, perform a **database backup** and ensure that the resulting backup file is safely stored. In the event of any error in the automatic upgrade process, it will be necessary to perform a manual upgrade described in the [Troubleshooting Upgrades](#) section.

- From the Discovery Center host server, open **Control Panel > Programs and Features**.
- Locate and right-click the Discovery Center installation entry and select **Change**.
- The Discovery Center installation wizard will run; choose the **Remove** option and ensure that **Remove Database within uninstall** option is **not selected**.
- Complete the uninstall process.
- Perform a new installation specifying the name of the existing database at the appropriate step in the process.
- When configuring the **IIS site** for the new installation, follow the instructions in [Appendix 2: Configuring for SSL and HTTPS](#) to create an installation using HTTPS.





Post Upgrade Configuration

Validate the Upgrade

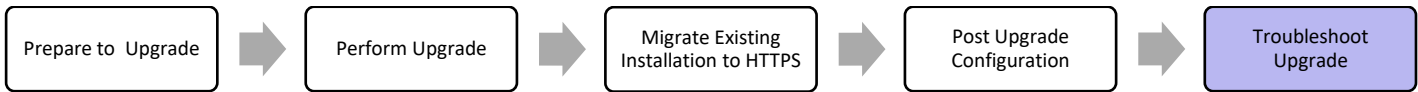
To validate an upgrade of Discovery Center, review the data that is presented in its browser interface.

1. The upgraded database will contain all previous data, which should appear unchanged in the user interface.
2. It is necessary to **process the Discovery Center reporting database**. This can be scheduled for immediate processing from the **Reporting and Actions > Reporting Settings** option in Discovery Center.

Apply any required configuration file changes

The Discovery Center application has a number of settings which are configured based on settings held in various text configuration files within the deployed location on the host server file system. Typically, these settings do not require any changes for the Discovery Center application to function optimally, however in the cases where changes are made any updated values are not persisted following an upgrade and the default settings are reverted to. It is therefore necessary to re-apply any changes that were made to these config files prior to any upgrade again, once an upgrade has completed.

It is strongly recommended that changes to any text configuration file are only made following a recommendation from ActiveNav, refer to support portal knowledge base articles at <https://www.support.activenav.com/> or contact Active Nav Support via email support@activenav.com for further help.



Troubleshooting Upgrades

Failure During Automatic Upgrade

When performing an automatic upgrade in post R4.2 releases, a common error occurs due to the Discovery Center being removed, and the database is retained. Path issues can occur if the Discovery Center is inadvertently installed in a different location. Resolve the errors as they arise as described below; once these errors are resolved, proceed with the install process. The installer will recognize any existing database and upgrade it automatically.

Correcting Connector Path Errors

When Discovery Center is inadvertently installed in a different location, its user interface may exhibit the following behaviors:

- The Network Map tab shows Load Error.
- The Indexes tab does not list indexes.
- The Area of Interest tab reports a server error.

To resolve these problems, the path stored in the **ConnectorDefinition** table of the **Discovery Center database** will need to be corrected for all registered connectors as follows:

1. Open **SQL Server Management Studio**, and for the **Discovery Center database**, create the following query:

```

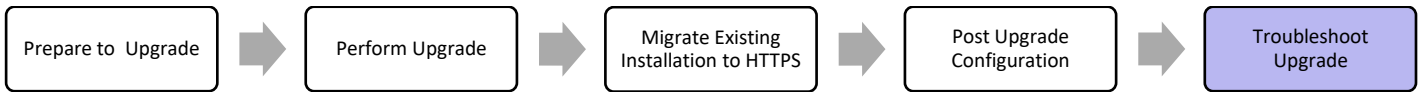
DECLARE @oldInstallLocation NVARCHAR(MAX) = 'C:\Program Files (x86)\Data Discovery Solutions Ltd\'
DECLARE @newInstallLocation NVARCHAR(MAX) = 'C:\Program Files\Active Navigation\'
UPDATE ConnectorDefinition SET path = REPLACE( path, @oldInstallLocation, @newInstallLocation)
SELECT * FROM ConnectorDefinition
  
```

2. Replace the file path with the old installation file path, '**C:\Program Files (x86)\Data Discovery Solutions Ltd**' in the example above.
3. Replace the file path with the new installation file path, '**C:\Program Files\Active Navigation**' in the example above.
4. Run the query and review the results listed to ensure the location(s) specified match the new installations.

Unexpected Behavior in Web Interface

Sometimes browser caching behaviors will cause unexpected errors in the Discovery Center user interface, e.g., unexpected or missing elements in pages or repeated error dialogs. Refresh the browser cache by holding the **SHIFT** key while reloading the browser page.

Appendix 3: Upgrading an Existing Installation



Other Issues

For upgrade issues not covered in this document, refer to support portal knowledge base articles at <https://www.support.activenav.com/> or contact **Active Nav Support** via email support@activenav.com and provide the following information:

1. Full details of the upgrade steps you have performed
2. The version number of the previous release.
3. The version to which you were upgrading.
4. A detailed description of the errors/issues observed during or after the upgrade.
5. A msixexec log file that was generated by running the installation from the command line as documented.



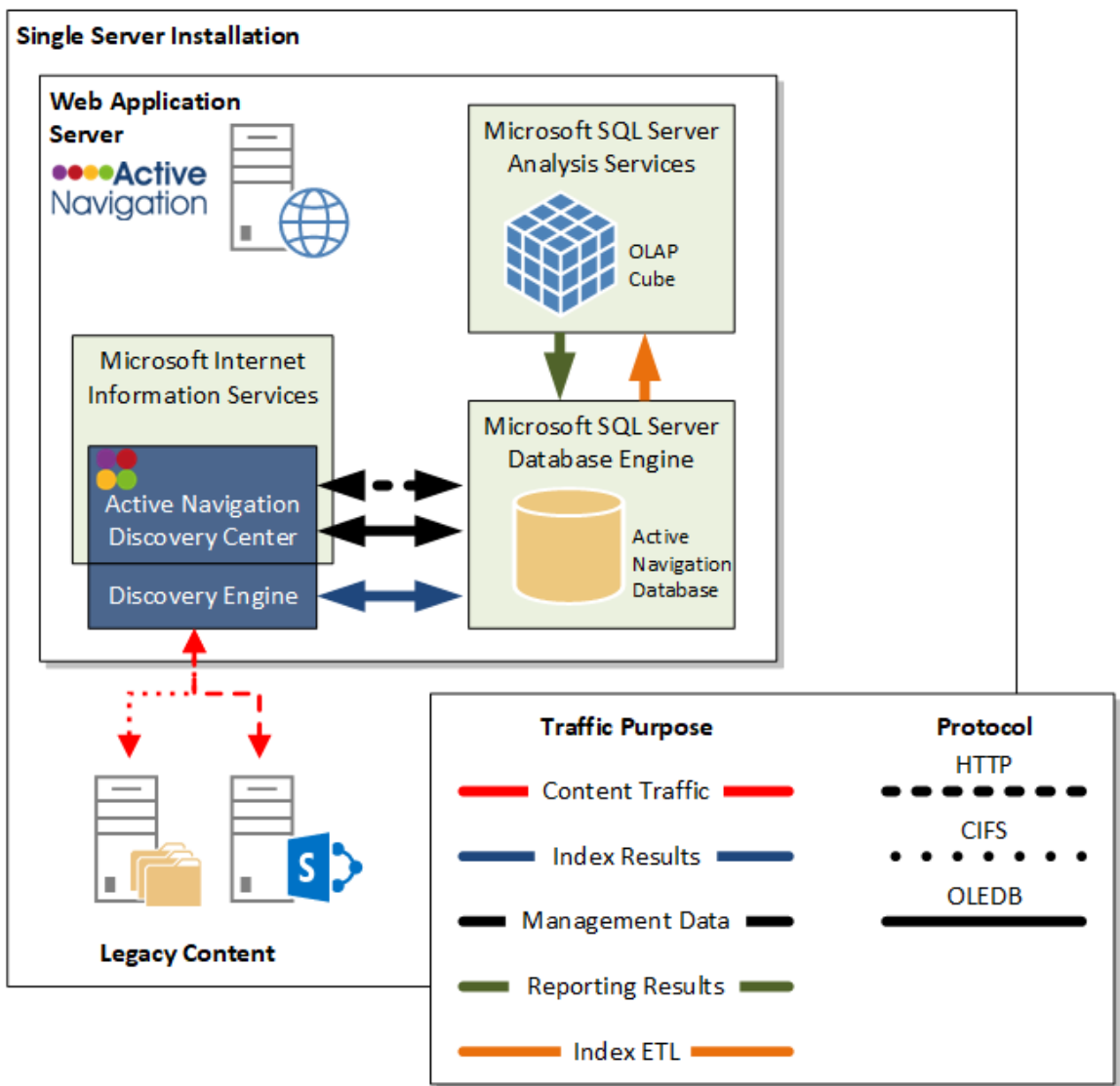
Appendix 4: Example Installations

Local Server Installation

A local server installation places **Discovery Center and all supporting SQL Server components** on a **single-host server**. This installation is simple to implement and can potentially be used for mobile deployments to address locations across a wide geographical area.

The host server must be sufficiently well specified to meet all requirements for **Discovery Center, SQL Server, and SSAS** as described in [Hardware Specifications](#).

Where multiple Discovery Center instances are required, there will be a cost for SQL Server licenses on every machine. Each machine will require additional RAM and disk resources to support SQL Server adequately.

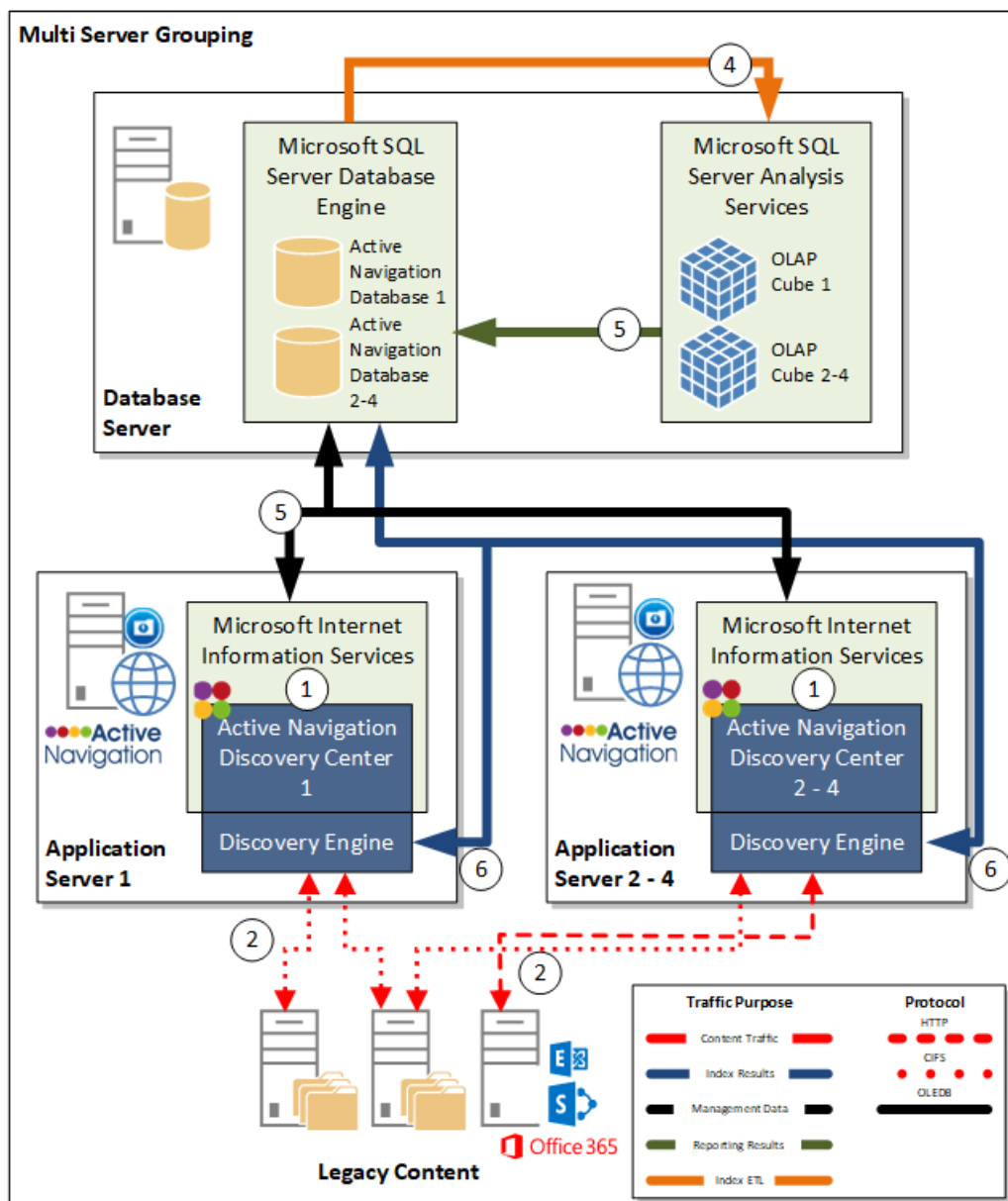


Centralized Installation

Where SQL Server assets (licenses, RAM, disk resource, and administration support) must be centralized for economies of scale, Discovery Centers can be deployed to use a single database farm limited only by SQL Server scale-out capacity. In such circumstances, an Analysis Services system should also be provisioned per Microsoft guidelines.

Note: For this configuration, **insufficiently specified SQL instances may cause degraded performance** or failures due to a lack of SQL system resources. For best performance, this configuration should be implemented with a dedicated and appropriately sized Discovery Center SQL Server instance.

If the centralized SQL Server environment has SQL Server and SQL Server Analysis Services hosted on separate servers, please see [Appendix 7: Additional Configuration for Fully Distributed Configuration](#) for additional steps required to support correct authentication between the elements of the system.



Example Windows Account and SQL Server Logins

In the above examples, the following **Windows account** and **SQL Server login** requirements must be met. Each account or login is shown below against the corresponding traffic in the local server installation diagram above.

Windows Accounts

ID	Description	Example	Rights
1	Discovery Center Web Application Service	Domain\ANWebSite	Windows default user account
2	Discovery Center Scheduler Service	Domain\ANScheduler	Logon as a service
3	Groups for Discovery Center user roles*	Domain\ANSysAdmin Domain\ANAdmin Domain\ANInfoMgr	Standard Windows user groups

*As determined by project requirements. System Administrator role is configured during installation.

SQL Server Logins

ID	Description	Example	Rights
4	SSAS Service login	Domain\SSASService	Windows default user account
5	Discovery Center Web Application login	Domain\ANWebSite	Logon as a service
6	Discovery Center Scheduler Service login	Domain\ANScheduler	Standard Windows user groups

*If SQL Server and SSAS are appropriately configured these logins should exist.



Appendix 5: Command Line Installation

A more advanced configuration of the Discovery Center can be achieved by installation via the windows command line, allowing more detailed control over the install process. Use the **msiexec** command to perform the command line install. Full details of how to use the **Windows Command Line** are provided as part of the Windows built-in help. The basic form of the command uses two options:

/I* <log filename.log> will cause the installer to write a detailed log file.
/package <installer filename.msi> must be provided to specify what to install.

For example: **/package <ActiveNav.Setup.msi> /I*install.log**

Installer Extended Command Line Properties

The Discovery Center supports extended properties shown in the table below. If a specific property is omitted, the installer will use the default value shown.

Note: Note: All values on the command line must be quoted if they contain spaces.

Property Name	Purpose	Default Value
LICENSE_FILE	Optionally specify a Discovery Center license file to be added during installation. (The license file can also be added after the installation by a user in the Active Navigation System Administrator role)	
INSTALLLOCATION	Specify the folder in which to deploy Discovery Center and working files (excluding the web site files, see below)	"C:\Program Files\Active Navigation\Discovery Center"
SEARCHDATADIR	Specify the folder in which to store the classification search index (only needed if the location based on the INSTALLLOCATION is inappropriate)	"C:\Program Files\Active Navigation\Discovery Center\SearchData"
FILECACHEDIR	Specify the folder in which to store the temporary files downloaded during analysis (only needed if the location based on the INSTALLLOCATION is inappropriate)	C:\Program Files\Active Navigation\Discovery Center\FileCache"
LOGDIR	Specify the folder in which to store the application log files (only needed if the location based on the INSTALLLOCATION is inappropriate)	"C:\Program Files\Active Navigation\Discovery Center\Logs"
WEBSITEDIR	Specify the folder into which to deploy the Discovery Center web application and log files	C:\inetpub\wwwroot\AN40Web
WEBSITE_PORT	Any valid port number for IIS	805
APP_POOL_IDENTITY	Specify "other" to allow a custom account to be specified for the IIS application pool (see APP_USER and APP_PASS)	other



Property Name	Purpose	Default Value
APP_USER	Specify a domain account	
APP_PASS	The windows password for the account specified with APP_USER	APP_PASS
APP_POOL_NAME_CUSTOM	A postfix to use for the application pool created by IIS	AN4
APP_NAME	The name (description) of the application created in IIS	ActiveNavigation4
SCHEDULER_IDENTITY	Specify “other” to allow a custom service account to be specified (see SCHED_USER and SCHED_PASS)	Other
SCHED_USER	Specify a domain account with Log on as a Service right	
SCHED_PASS	The Windows password for the account specified with SCHED_USER	
SQL_SERVER_NAME	The server and optional instance to deploy the Active Navigation database in to	localhost
SQL_DATABASE_NAME	This name is used for the SQL Server relational database and SQL Server Analysis Services reporting database that is created and used by Discovery Center	ActiveNav4
SSAS_SERVER_NAME	The server and optional instance to deploy the Discovery Center reporting database in to	Value specified for SQL_SERVER_NAME
DEFAULT_ADMIN_ACC	Specify a Windows group or user to put into the Discovery Center System Administrators role	BUILTIN\Administrators
DEFAULT_ALL_ROLES	Specify 1 to add the administrator group or to be added to all roles in the Discovery Center, or 0 to just add them to the System Administrator role.	0
VALIDATE_APP_POOL_USER	Specify this property with the value 0 to skip the password validity check for the web site application pool user	1
VALIDATE_SCHED_USER	Specify this property with the value 0 to skip the password validity check for the scheduler service account	1
DEBUG_CA	This can be used by developers to interrupt the normal installer operation to allow debugging the installer custom actions	



Example Command Line

```
C:\>msiexec /I* "install-.log" SCHEDULER_IDENTITY=other SCHED_USER=AN\svc-ansched SCHED_PASS=pass  
APP_POOL_IDENTITY=other APP_USER=AN\svc-anweb APP_PASS=pass SQL_DATABASE_NAME=ActiveNav4  
APP_POOL_NAME_CUSTOM=ActiveNav4 APP_NAME=ActiveNav4 WEBSITEDIR=C:\ActiveNavigation\website WEBSITE_PORT=805  
INSTALLLOCATION=C:\ActiveNavigation DEFAULT_ALL_ROLES=1 /package ActiveNavigation.Setup.msi
```





Appendix 6: Configuring Management Reporting Database

If you are using the Management Reporting feature, a **Management Reporting Database** must be created and then configured in the **Discovery Center Report Settings**. The Management Reporting Database will allow you to build a historical record of your information management activities.

Creating the Management Reporting Database

A simple batch file has been provided in the **ManagementReportingDatabase** subfolder of your Discovery Center installation.

Note: For the creation process to be successful, the user running the batch file must have the SQL **sysadmin** role granted in the SQL instance chosen as the Management Reporting Database location. Contact support@activenav.com for more details on these requirements if needed.

To perform the database creation, follow these steps:

1. Open a command prompt window on the server where the Discovery Center application has been installed.
2. Change location in the command window to **the Management Reporting** folder of your Discovery Center installation. If you have installed in the default location, you can use the following command to do this:

```
cd \Program Files\Active Navigation\Discovery Center\ManagementReportingDatabase
```

3. Run the **CreateManagementReportingDatabase.bat** script and enter the details to be used for your database.

Note: For technical reasons, inputs starting with '-' or '--' are not supported. Additionally, if any input contains exclamation marks ('!' characters), then a '!' must be added before each one. For example, 'user!name' would be entered as 'user!!name'.

When prompted, choose whether or not the database should be accessed via service accounts. If a service account is not used, a **named SQL server account** must be used to ensure that the Discovery Center application can access the database.

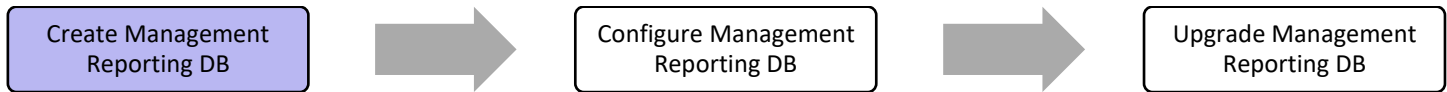
- a. If service account access is used, you will need to enter the name of at least one service account.

Note: If you use the same account for your scheduler and the web application, you only need to enter it once.

```
ManagementReporting>CreateManagementReportingDatabase.bat
Enter Management Reporting Database Instance Name: myserver
Enter Management Reporting Database Name: MRDB
Use Service Accounts For MRDB (y/n)?: y
Enter Discovery Center Scheduler Account Name (domain\username): DOMAIN\SchedulerService
Enter Discovery Center Web Application Account Name (domain\username): DOMAIN\WebAppService
```

- b. If **SQL account access** is used, you will need to enter the account's **username** and **password**; it will be created if it does not already exist.





```
ManagementReportingDatabase>CreateManagementReportingDatabase.bat
Enter Management Reporting Database Instance Name: myserver
Enter Management Reporting Database Name: MRDB
Use Service Accounts For MRDB (y/n)? : n
Enter SQL Account Username To Use For Database: MrdbUser
Enter Password For SQL Account To Use For Database: *****
```

Upon entering the correct details, you will see the progress for creating the database:

```
ManagementReportingDatabase>CreateManagementReportingDatabase.bat
Enter Management Reporting Database Instance Name: myserver
Enter Management Reporting Database Name: MRDB
Use Service Accounts For MRDB (y/n)? : n
Enter SQL Account Username To Use For Database: MrdbUser
Enter Password For SQL Account To Use For Database: *****
Creating database...
Processing directory: Schemas... Done.
Processing directory: Assemblies... Done.
Processing directory: Tables... Done.
Processing directory: Views... Done.
Processing directory: Functions... Done.
Processing directory: ViewsWithFunctions... Done.
Processing directory: StoredProcedures... Done.
Processing directory: Data... Done.
Processing directory: Roles... Done.
Creating SQL login (if required)... Done.
```

Once the process completes, a new **Management Reporting Database** will be available with the name provided on the given SQL instance and permissions granted to allow access and processing from Discovery Center using the specified user accounts.





Configuring the Management Reporting Database for Use

Once the database has been successfully created, you **must** provide the information to the **Discovery Center Web Application** as follows:

1. Open the **Discovery Center Web Interface**.
2. Navigate to the Reporting and **Actions > Reporting Settings** tab.
3. Locate the **Management Reporting Database Processing** section, then choose **Edit** to enable the database **Instance name**, **Database name**, and **various connection credential options** to be entered.

Note: This section of the page is only visible if you have a license that enables **Management Reporting**.

Management Reporting Database Processing

The management reporting database has never been processed. If management reporting is required immediately then use the Process Now button.

Instance name:

Database name:

Credential Type: ☐ Service Account(s) ☒ SQL

Credential:

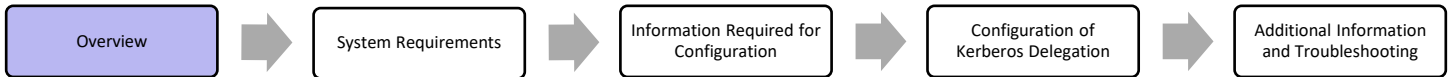
Management Reporting Database Processing Mode

☐ Automatically ☒ Manually

4. There are two options for **Credential Type**, these are:
 - a. **Service Account(s)** – Using Integrated Windows authentication using the service accounts that run the Discovery Center application.
 - b. **SQL** – If the SQL Credential option is selected, a selection list will appear. This list displays all the Credential records that exist in the Discovery Center. These records are defined in the **Credential Management** section of the application located in the **System Settings** tab and allow a username and password combination to be provided. They are used to represent the SQL user and password information.

Note: In either case, the account(s) being used **must** have been **granted the relevant permission** from the **Management Reporting Database**; this can be done either during creation (see [Creating the Management Reporting Database](#)) or manually.

5. Click **Save**; the system will check the connection to the database and the database structure to ensure that the **Management Reporting Database** is accessible with the provided credentials and contains a structure compatible with the current version of Discovery Center. (If the credentials entered are incorrect or the version is incompatible, you will be prompted with a message to correct them).



Upgrading the Management Reporting Database

A simple batch file has been provided to upgrade the **Management Reporting Database**, located in the **ManagementReportingDatabase** subfolder of your Discovery Center installation.

Note: For the upgrade process to be successful, the user running the batch file must have the SQL **sysadmin** role granted in the SQL instance that the Management Reporting Database is installed. Contact support@activenav.com for more details on these requirements if needed.

To perform the upgrade:

1. Open a command prompt window on the server where the Discovery Center application has been installed. You must run the command prompt as a user **with access to SQL** and the **Management Reporting Database**.
2. Change location in the command window to the **Management Reporting** folder of your Discovery Center installation. If you have installed in the default location, use the following command:

```
cd \Program Files\Active Navigation\Discovery Center\ManagementReportingDatabase
```

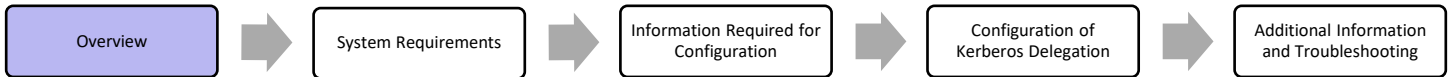
3. Run the **UpdateManagementReportingDatabase.bat** script and enter the details to be used for your database.

```
C:\Program Files\Active Navigation\Discovery Center\ManagementReportingDatabase>UpdateManagementReportingDatabase.bat
Enter Database Instance Name myinstance
Enter Database Name mrdb
```

After entering the correct details, you will see the following message:

```
Database mrdb successfully updated
```



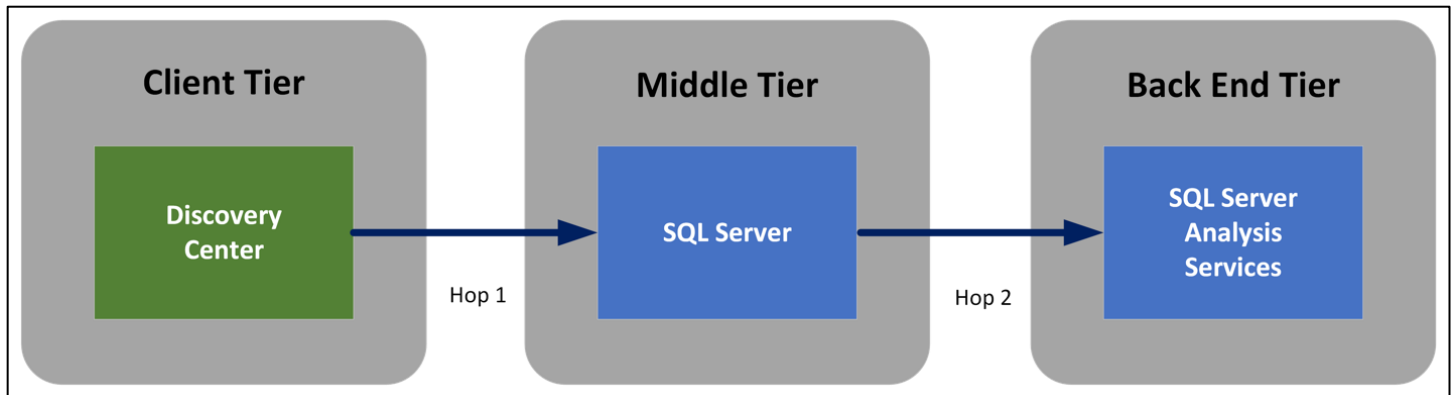


Appendix 7: Additional Configuration for Fully Distributed Configuration

Overview

A fully distributed configuration where **Discovery Center**, **SQL Server**, and **SQL Server Analysis Services** are installed on **separate host servers** requires **extra configuration** to allow authentication between each component.

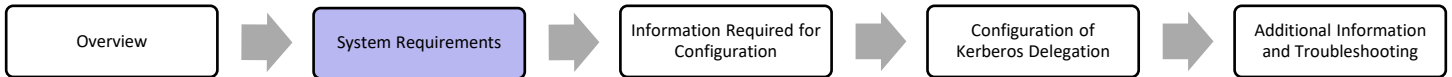
This configuration involves communication between components, as shown in the diagram below. To produce reports, the Discovery Center must be able to access data from **SSAS** via **SQL Server**, creating a situation known as **Double Hop Authentication**. This requires SQL Server to present credentials from the Discovery Center service accounts to the Back End Tier.



Windows provides two built-in authentication mechanisms; these are **NTLM** and **Kerberos**. Under normal circumstances, the underlying environment selects the appropriate authentication mechanism in the background without the user being aware of which is being used. However, **Kerberos must be used** to support **double hop** authentication; this requires certain pre-conditions to be met by the operating environment and specific configuration steps to be taken.

The following sections outline the steps needed to configure a **fully distributed Discovery Center deployment** correctly.

Note: Regarding Azure Cloud deployment - The use of an Azure SQL Database or Azure SQL Managed Instances for the SQL Server host in the Middle Tier above is not supported. This is because Microsoft do not support communication from SQL databases in those environments to SQL Server Analysis Services databases, which is a requirement for the Discovery Center reporting solution. The use of Azure Analysis Services as the SQL Server Analysis Services host in the Back End Tier above is also not supported as Microsoft do not support the use of Multidimensional data models in these environments, which is also a requirement for the Discovery Center reporting solution.



System Requirements

Active Directory

Kerberos authentication provided by **Active Directory** meeting the following requirements:

1. The Windows domain must be operating at a functional level of **Windows Server 2003** or later.
2. The systems that will be used must be time-synchronized.
3. The domain must provide correct name resolution for **DNS** and **NetBios** protocols for short and fully qualified server names.
4. **TCP** and **UDP** traffic must be allowed on **port 88**, where firewalls are present between the installation and the domain controller components.
5. All systems to be used for the deployment must belong to the same Windows domain.
6. Domain administration rights and access to the domain controller must be available to carry out some of the configuration steps described below.

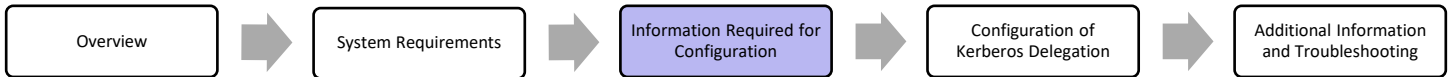
SQL Server

Kerberos authentication depends on the correct configuration of **SPNs** (Service Principal Names) for the components that will be carrying out authentication tasks. The steps to configure SPNs for SQL Server are described in the next section [Information Required for Configuration](#). The SQL Server installation must use either a **domain account** (preferred) or a **built-in** system account such as **Network Service** or **Local System** for the SQL and SSAS services.

Note: Kerberos authentication configuration will not be possible if the SQL Server installation uses local computer accounts for SQL Services.

Record the service accounts used for SQL and SSAS services and the SQL SSAS instance names as these will be required for the configuration of SPNs and delegation properties.



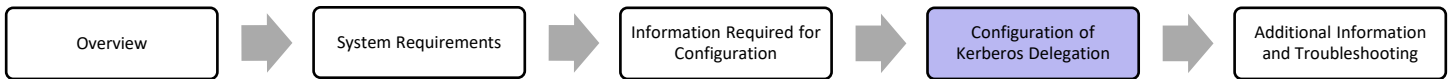


Information Required for Configuration

To complete the Kerberos configuration, you will need to know the following information:

Item	Notes
Local domain controller name	Domain Administrator privileges are required for configuration
SQL Server host name	The fully qualified host name for the SQL Server host server
SQL Server instance name	For SQL Server instance with a non-standard name
SQL Server service account	Must use a domain service account (preferred) or a built-in service account
Local Administrator Credentials to access SQL Server system	To configure Local Security Policies for the SQL Server host server
SQL Server Analysis Services host name	The fully qualified host name for the SQL Server Analysis Services host server
SQL Server Analysis Services instance name	For SQL Server instance with a non-standard name
SQL Server Analysis Services service account	Must use a domain service account (preferred) or a built-in service account





Configuration for Kerberos Delegation

Successful authentication in a double hop scenario requires a **Kerberos delegation** to be configured, which requires careful configuration of **SPN's** for the relevant services and delegation rights for the **middle tier service** account.

There are several ways to configure delegation to support double hop authentication. The steps below outline how to use **constrained delegation** and **protocol transition** to allow the SQL Server service to authenticate with SSAS regardless of whether the client connection to SQL Server was made using **Kerberos**. Additional steps are required but will reduce the risk of authentication failures.

Configure SPNs for SQL and SSAS Using Built-In Service Accounts

If SQL is installed using built-in accounts (e.g., **Network Service** or **Local System**), SPNs are typically set up correctly during installation; however, it is important to ensure this is the case by following these steps, substituting local settings in each example:

Service	Host Name	Instance Name
SQL Server	SQLServer.mydomain.com	default
SSAS Server	SSASServer.mydomain.com	default

Check SPN Settings for SQL Server (Built-In)

For a **non-default SQL** instance, substitute the **instance name** in place of **port number 1433**:

1. Run the following command to list SPN settings for the host SQLServer:

```
Setspn -L SQLServer
```

2. Confirm that the following two **SPN** entries are listed in the results:

```
MSSQLSvc/SQLServer.mydomain.com:1433
```

```
MSSQLSvc/SQLServer:1433
```

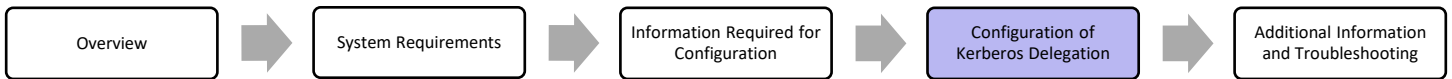
3. If settings are missing, add the relevant entries using commands:

```
Setspn.exe -S MSSQLSvc/SQLServer.mydomain.com:1433 SQLServer
```

```
Setspn.exe -S MSSQLSvc/SQLServer:1433 SQLServer
```

4. If changes were made, repeat the first two steps to confirm the configuration.





Check SPN Settings for SSAS Server (Built-In)

For a **non-default SSAS instance**, add to the SPN a colon and then the instance name (e.g., **MSOLAPSvc.3/SQLServer:myinstance**).

1. Run the following command

```
Setspn -L SSASServer
```

2. Confirm the following two **SPN** entries are listed in the results:

MSOLAPSvc.3/SSASServer.mydomain.com

MSOLAPSvc.3/SSASServer

3. If settings are missing, add the relevant entries using commands:

```
Setspn.exe -S MSOLAPSvc.3/SSASServer.mydomain.com SSASServer
```

```
Setspn.exe -S MSOLAPSvc.3/SSASServer SSASServer
```

4. If changes were made, repeat the first two steps to confirm the correct configuration.

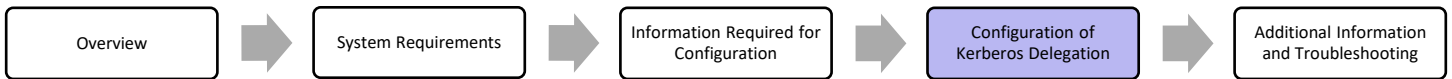
Configure SPNs for SQL and SSAS Using Domain Service Accounts

If SQL is installed using **domain accounts**, the steps are the same as used for built-in accounts, the only difference being the command line species the **service account** instead of the hostname.

Note: If SQL Server uses **domain accounts** for its services, the **setspn** command-line tool can be run from server systems within the domain – **domain administration rights** are required.

When SQL is installed with a **domain account**, an **SPN** is **not** normally configured automatically, and therefore it is normal for the **SPNs** not to be present in this scenario. Substitute the following values for your local settings when running the example command lines below:

Service	Host Name	Instance Name	Service Account
SQL Server	SQLServer.mydomain.com	ANSQL	MYDOMAIN\sqli
SSAS Server	SSASServer.mydomain.com	ANSSAS	MYDOMAIN\ssas



Check SPN Settings for SQL Server (Domain)

For a **default SQL instance**, substitute the **port number 1433** in place of the instance name **ANSQL**:

1. Run the following command to list SPN settings for account **MYDOMAIN\sqli**:

```
Setspn -L MYDOMAIN\sqli
```

2. Confirm that the following two **SPN** entries are listed in the results:

MSSQLSvc/SQLServer.mydomain.com:ANSQL

MSSQLSvc/SQLServer:ANSQL

3. If settings are missing, add the relevant entries using commands:

```
Setspn.exe -S MSSQLSvc/SQLServer.mydomain.com:ANSQL MYDOMAIN\sqli
```

```
Setspn.exe -S MSSQLSvc/SQLServer:ANSQL MYDOMAIN\sqli
```

4. If changes were made, repeat the first two steps to confirm the configuration.

Check SPN Settings for SSAS Server (Domain)

For a **default SSAS instance**, remove the instance name, **ANSSAS** from the **SPN**, e.g., **MSOLAPSvc.3/SSASServer**.

1. Run the following command

```
Setspn -L MYDOMAIN\ssas
```

2. Confirm the following two **SPN** entries are listed in the results:

MSOLAPSvc.3/SSASServer.mydomain.com:ANSSAS

MSOLAPSvc.3/SSASServer:ANSSAS

3. If settings are missing, add the relevant entries using commands:

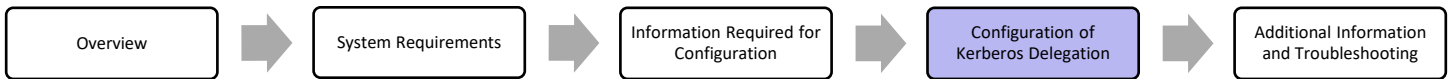
```
Setspn.exe -S MSOLAPSvc.3/SSASServer.mydomain.com:ANSSAS MYDOMAIN\ssas
```

```
Setspn.exe -S MSOLAPSvc.3/SSASServer:ANSSAS SSASServer MYDOMAIN\ssas
```

4. If changes were made, repeat the first two steps to confirm the correct configuration.

Note: If either the SQL or SSAS components are using a named instance, configure an SPN for the SQL Browser service to successfully discover port numbers for the instances. See the link in the [Summary of Common Kerberos Errors](#) for details.





Active Directory Configuration for Service Accounts

The following requires **domain administration rights** and **access to a domain controller**. The steps below are grouped by **Domain Service Account**, **Built-In Service Account**, and **Both** (where the steps are the same for both types of configuration); follow them to ensure your configuration can be used in a **delegation** situation.

Configuration Using Domain Service Account or Built-In Service Account

Domain Service Account

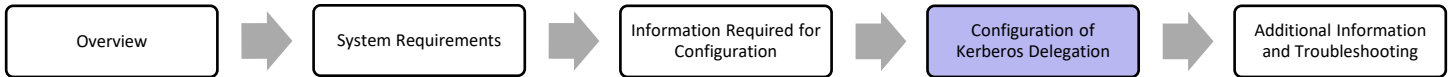
1. On the domain controller, launch the **Active Directory Users and Computers** configuration tool.
2. Locate the service account for the SQL Service and open the properties dialog for the account.

3. Ensure that the account is permitted to participate in **delegation** by ensuring the **Account is sensitive and cannot be delegated** check box is **NOT** checked.
4. If the SPN for the SQL service has been correctly configured to use this account, the user properties dialog will have a tab labeled **Delegation**. If this is not present, check the **SPN** settings.

Built-In Service Account

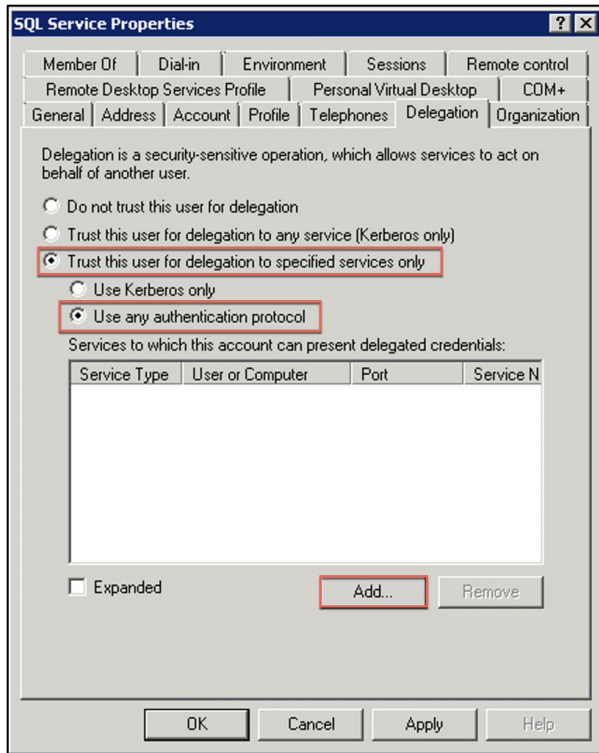
5. If using a built-in service account (e.g., **Network Service**), open the account properties dialog for the **SQL server host** (in our example SQLServer).



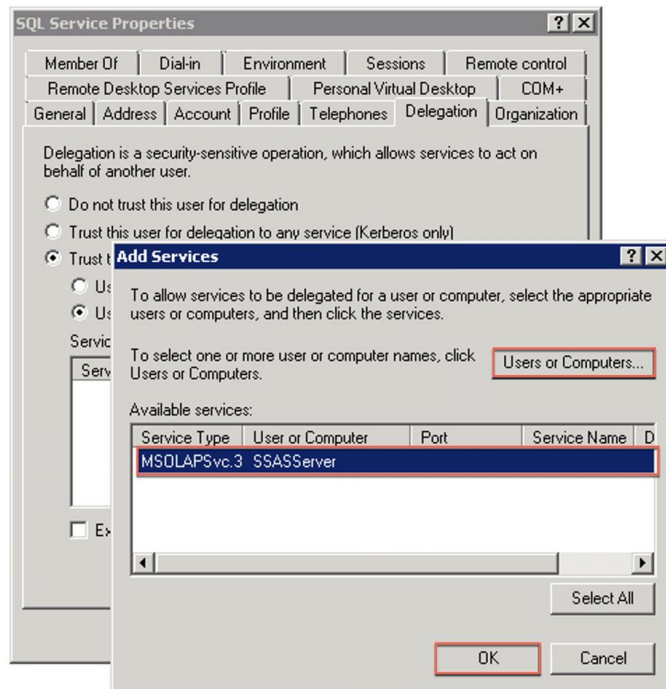


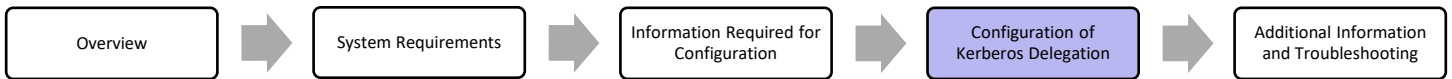
Both

- To allow **constrained delegation**: select the **Delegation** tab, enable the **Trust this user for delegation to specified services only** option, and enable the sub-option **Use any authentication** as shown.



- For security reasons, constrained delegation requires that specific services are identified as valid candidates for delegation. Click the **Add** button in the **Delegation** tab. The **Add Services** dialog will open.
- Click the **Users or Computers** button.





Domain Service Account

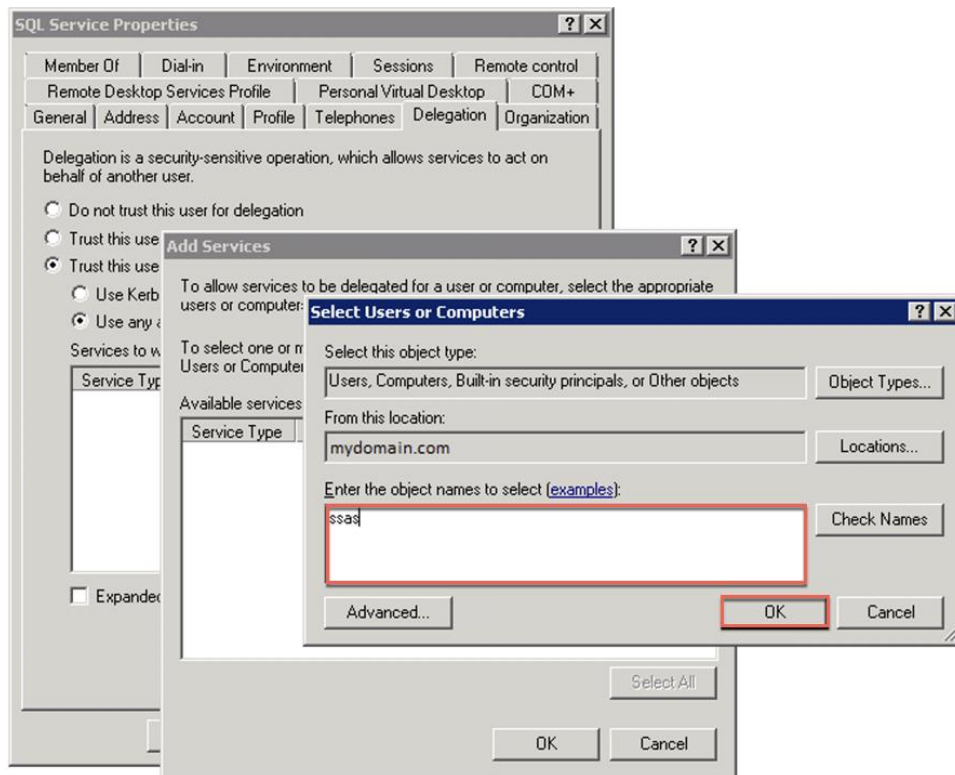
- If the SSAS Service uses a domain service account, enter the name of the account in the **Select Users or Computers** dialog as shown below.

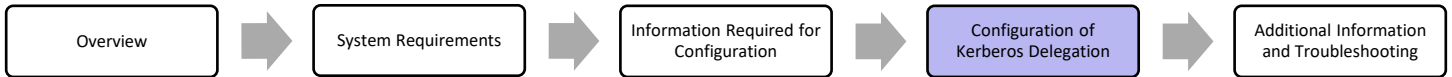
Built-In Service Account

- If the service is using a built-in system account such as a **Network Service**, enter the hostname of the SSAS host system (e.g., **SSASServer**)

Both

- All SPNs registered to the specified account will be added as shown.
- Locate and select the SPN record for service type **MSOLAPSvc.3** on the correct server and select **OK** to dismiss the **Add Services** dialog for the SQL Server service account.
- If the required SPN is **not** listed, review the steps for registering SPNs in the previous section [Configuration for Kerberos Delegation](#).

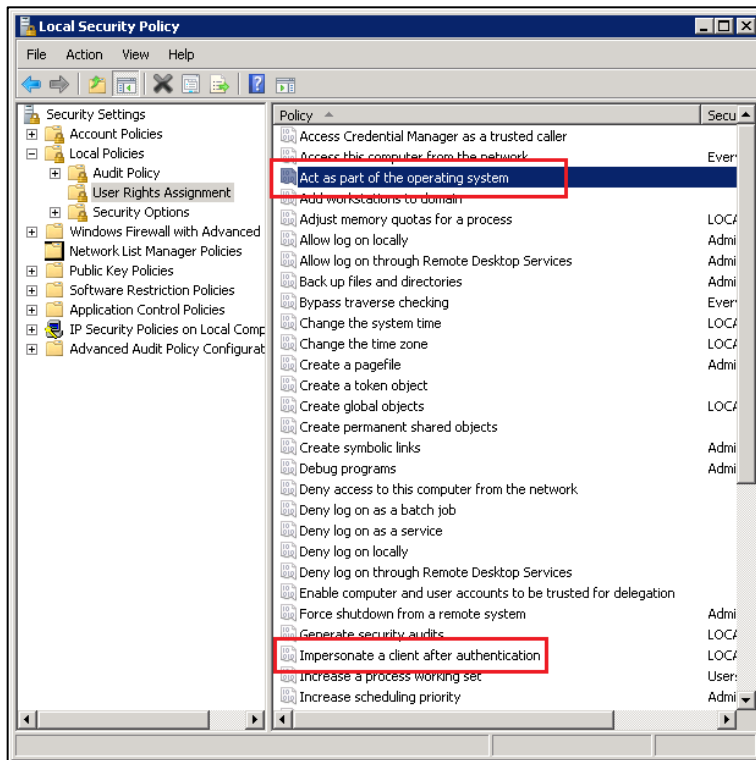




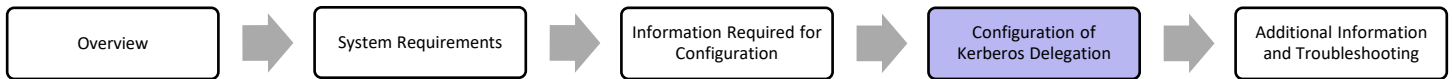
Local Rights on SQL Server (Middle Tier) System

The final requirement for the successful operation of **Kerberos Delegation** is to assign specific user rights to the **SQL Server Service** account on the **SQL Server host system** as follows:

1. Connect to the SQL Server host system.
2. Launch the Local Security Policy application (To run directly, use **secpol.msc**).
3. Select the **Security Settings > Local Policies > User Rights Assignment** node in the directory on the left pane.



4. Right-click **Act as part of the operating system** and click **properties**. Add the **service account used by SQL** to the list of accounts.
5. Right-click **Impersonate a client after authentication** and click **properties**. Add the **service account used by SQL** to the list of accounts.

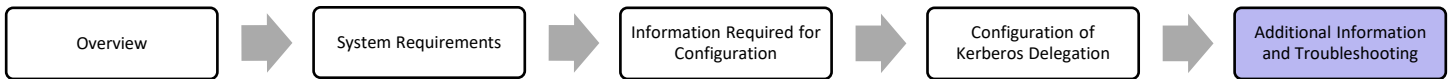


Validating Configuration

Validate your Kerberos configuration to ensure that it allows Discovery Center to function correctly using the following steps:

1. Complete the **ActiveNav Discovery Center Installation**.
2. Perform a **skim index** over a small number of test files.
3. Confirm that the Discovery Center can **generate reports** and **export file details** from the reporting interface.
4. If reports cannot be generated:
 - Review the error log for details of the error(s) encountered.
 - Review the Kerberos configuration steps above; accurate configuration of every step is essential for authentication to succeed.
 - Check the underlying **Active Directory** requirements described above.
 - Review the links in the following section for further information regarding **Kerberos's** correct configuration and troubleshooting configuration issues.





Additional Information and Troubleshooting

Solving problems with Kerberos can be a difficult process; the links below were used in preparing the guidance above and offer additional detail on configuration requirements and troubleshooting.

Configuration of SPN for SQL Server

Summary of configuration for SQL Server:

<https://msdn.microsoft.com/en-us/library/ms191153%28v=sql.105%29.aspx>.

Note: Versions of the page are available for different versions of SQL Server.

Detailed case study of constrained delegation between SQL Server and SQL Server analysis services:

<https://msdn.microsoft.com/en-us/library/ee191523%28SQL.100%29.aspx>

Configuration of SPN for SQL Browser Service

An **SPN** for the **SQL Server Browser** service is required to establish a connection to a named instance of **SQL Server Analysis Services** or **SQL Server**:

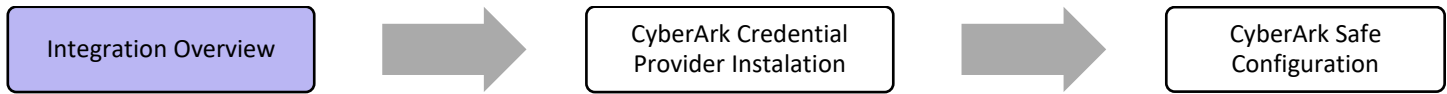
<https://support.microsoft.com/kb/950599>.

Summary of Common Kerberos Errors

Common error messages that can occur when using Kerberos:

<https://msdn.microsoft.com/en-us/library/ms819978.aspx>.





Appendix 8: CyberArk Configuration

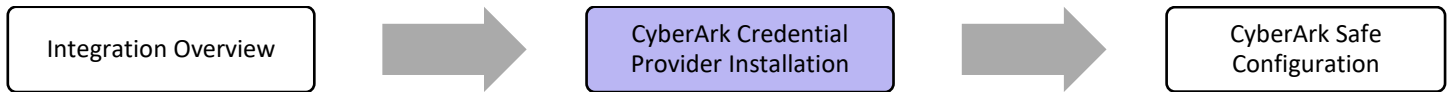
Integration Overview

Discovery Center includes an optional licensed feature that can define **Credentials** using accounts and passwords stored in a **CyberArk vault**.

- Discovery Center integrates with CyberArk using the Application Identity Management (CyberArk AIM) architecture.
- Discovery Center's CyberArk interface uses a collocated CyberArk Credential Provider windows service to communicate with a target **CyberArk vault**.
- For this release, the Discovery Center integrates with **Version 9.95** of the CyberArk Credential Provider **only**.
Discovery Center will be unable to retrieve passwords from the target **vault** if a later version of the Credential Provider is installed.
- Discovery Center's Cyber Ark interface is enabled by installing a license with the **CyberArk AIM** Custom Feature Pack. Once enabled, the Discovery Center application does not require any additional configuration steps.

Note: The **CyberArk Credential Provider Service** must be installed and configured on the **same machine** as the **Discovery Center** application. The **target vault** must also be configured to **accept requests from the Discovery Center**.

For a more detailed description of the CyberArk AIM architecture and the steps required to install and configure the CyberArk AIM facility, refer to the CyberArk document **Credential Provider and Application Server Credential Provider Implementation Guide**.



CyberArk Credential Provider Installation

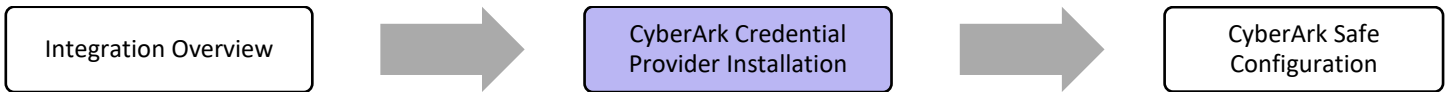
The CyberArk Credential Provider is a windows service that provides a secure, authenticated interface between the client applications and an instance of a Cyber Ark vault.

- A single instance of a Credential Provider windows service acts as the interface point for any CyberArk AIM-enabled application installed on the same machine.
- The Credential Provider does **not** need to be re-installed or reconfigured if it's already present on a machine.
- The Credential Provider **must** be installed on the same machine that hosts the Discovery Center application.
- The **Credential Provider Installer CD Image** is available on the **CyberArk support portal** for registered customers.

Note: Before installing, make a note of the **IP Address** and **Port** of the target **CyberArk vault**. Check that these are not blocked by any firewall or other security settings. The installation will attempt to contact the vault and will fail if the vault is inaccessible.

The following steps describe the simple case for a new Credential Provider Installation where the host machine hasn't been registered with a target CyberArk vault. A standard vault configuration is used. Refer to CyberArk's '**Credential Provider and Application Server Credential Provider Implementation Guide**' for more complex cases such as reinstallation or automated/silent installs.

1. In the **AIM CD Release Image**, navigate to the **Credential Provider > Windows** folder.
2. Run **Setup.exe**, accept the license prompt, and then click **Next**.
3. Enter your **Customer Information** (this doesn't affect the functionality of the Credential Provider).



4. Unless the **target CyberArk vault** has been configured with custom settings, choose the **Typical** option, then click **Next**.

CyberArk Application Identity Manager Setup

Installation type

Select installation type and the folder where setup will install files for Application Password Provider.

☒ Typical
All program features will be installed with the default configuration values.

☐ Custom
Allows you to customize configuration parameters. Recommended when you want to configure the provider to use an existing Vault environment, or when you want to overwrite the default configuration settings.

Destination Folder
C:\Program Files (x86)\CyberArk Browse...

InstallShield

< Back **Next >** Cancel

5. Enter the CyberArk's vault's connection **IP address** and **port**, then click **Next**.

CyberArk Application Identity Manager Setup

Vault's Connection Details

Please enter the Vault's Address and Port number.

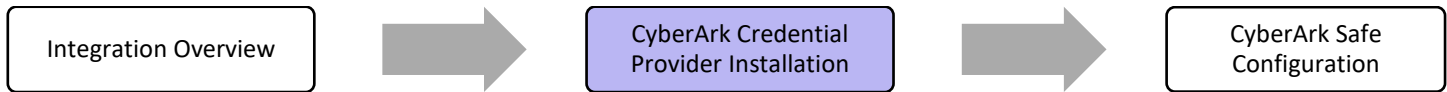
Address:

Port:

InstallShield

< Back **Next >** Cancel

6. If necessary, define an account in the CyberArk vault that can be used by the Credential Provider.

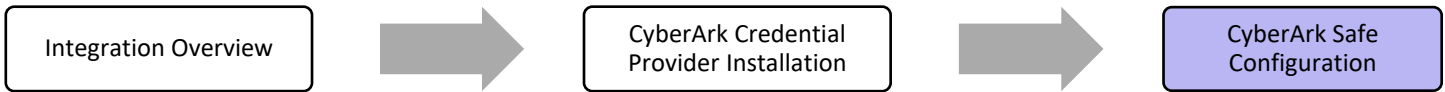


7. Enter the **vault username** and **password**, then click **Next**.

Note: The installation will now attempt to contact the **vault** and register the Credential Provider for the machine. If successful, the installation will start the service. To check this, run the Windows Task Manager select services and confirm that the service **CyberArk Application Password Provider** is visible and has a status of **Running**.

The installation may not complete if:

- The installer cannot contact the **vault** using the given **IP address** and **port**.
- The given **username**, **password**, or **both** are incorrect.
- The target **vault** has the **Credential Provider** for the same machine already registered. This may occur when a Credential Provider has been installed then uninstalled.

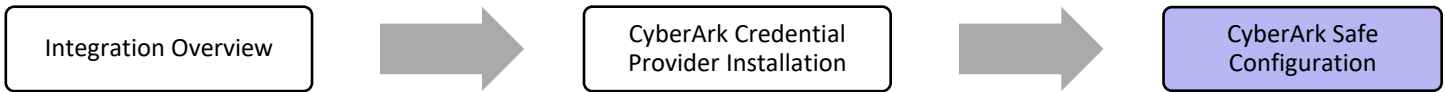


CyberArk Safe Configuration

To allow the **Discovery Center** to access a **safe** on the **target vault**, the safe **must** have both the **Credential Provider** and the **Application** as members. The following describes how the **CyberArk Password Vault Web Access (PVWA)** web application can be used to set a safe's membership and grant access to the Discovery Center's application. For a more complete description of the PVWA, see the CyberArk documents' **Credential Provider and Application Server Credential Provider Implementation Guide**' and **'Privileged Account Security Implementation Guide'**.

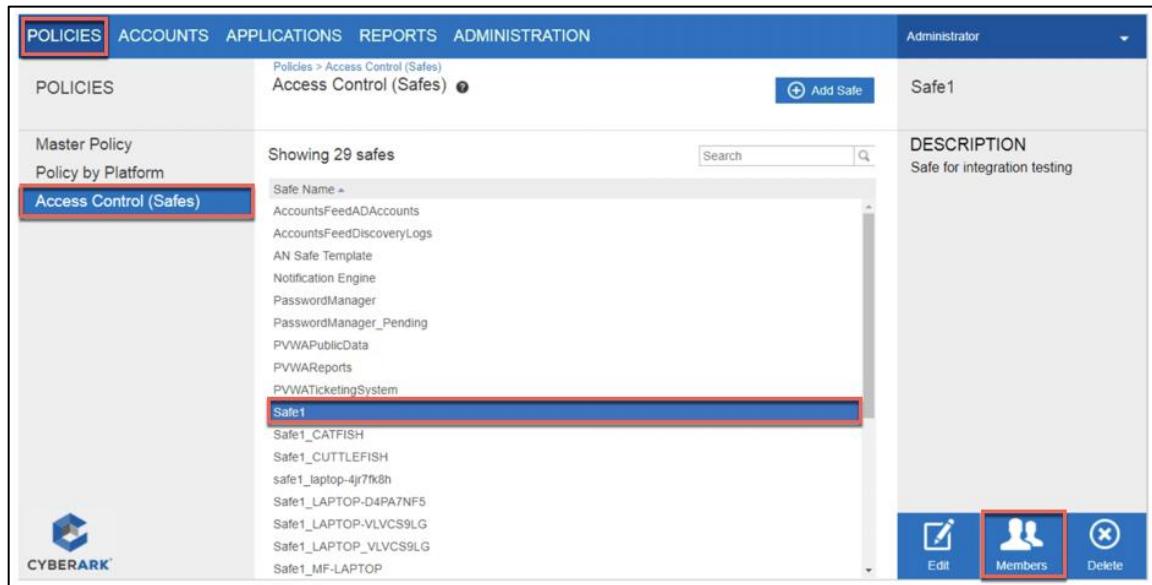
1. In a web browser, enter the **PVWA URL** for the **vault**.
2. Enter the **username** and **password** for the **vault** and select **Sign in**. If successful, the app will show the accounts list.

3. Before configuring a **safe**, a **Discovery Center Application definition** must be created in the **target vault**. In the PVWA app, navigate to the **Applications** tab and click **Add Application**.
4. By default, the Discovery Center identifies itself through the Credential Provider to the vault using the name **Discovery Center**. Enter this into the **Application Name** field along with any relevant **Business Owner** information.
5. Set the **Location** drop-down to **/Applications**, then click **Add**.

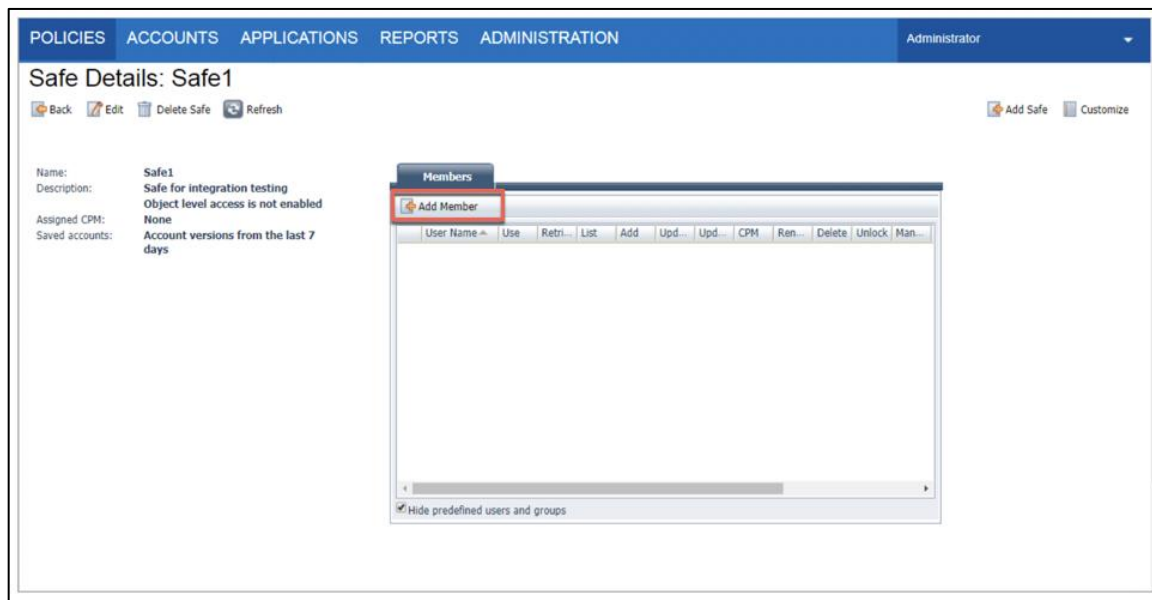


Note: The Applications page also allows you to define additional access restrictions. **Discovery Center CyberArk AIM** integration does not support **hash-based authentication**.

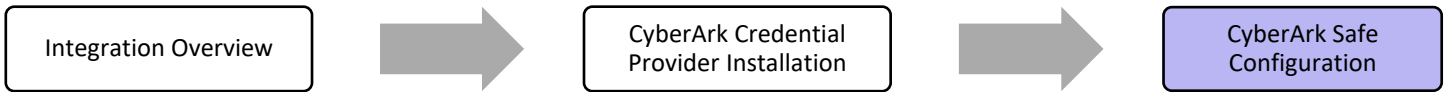
- Navigate to **Policies > Access Control (Safes)** and select the safe that you want to grant access to Discovery Center. The context buttons for **Edit**, **Members**, and **Delete** will appear on the bottom right-hand info panel. Click on the **Members** icon.



- The PVWA will now show the **Safe Details** page. Click on the **Add Member** icon.



- The **Add Safe Member** dialog allows you to specify which **Credential Providers** and **Applications** can access the **safe**. To grant a Discovery Center instance access, both the **Application** and the **Credential Provider** of the **host machine** must be added as **members**.



9. In the **Search** textbox (assuming that the default Credential Provider **Prov_machine_id** naming format has been followed), type **Prov** and click **Search**. The table will show all Credential Provider entities that match the given standard pattern.
10. Select the Credential Provider that matches the name of the machine hosting the Discovery Center. Credential Providers register themselves with the vault during the installation process. Click **Add**.

Add Safe Member

Search: Search In:

Selected Search: Vault Display 4 result(s)

Name	Business Email	Full Name
Prov_LAPTOP-D4PA7NFS		
Prov_LAPTOP-4JR7FK8H		
Prov_LAPTOP-6N5DM0P2		
Prov_LAPTOP-VLVC99LG		

☐ Access

☒ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☒ View Audit log

☒ View Safe Members

☐ Workflow

11. Grant the Discovery Center application access to the safe by entering **Discovery** in the search textbox. The list should show the entry for the Discovery Center.
12. Select the Discovery Center application and click **Add**, then click **Close** to dismiss the dialog.

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
Discovery Center	j.doe@company...	Jane Doe

☐ Access

☒ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☒ View Audit log

☒ View Safe Members

☐ Workflow

13. The Discovery Center and the Provider should now both be shown in the safe member list.

The Discovery Center instance running on the same machine as the registered Credential Provider should now be able to access the accounts stored in the safe.

Appendix 9: SharePoint Online Authentication

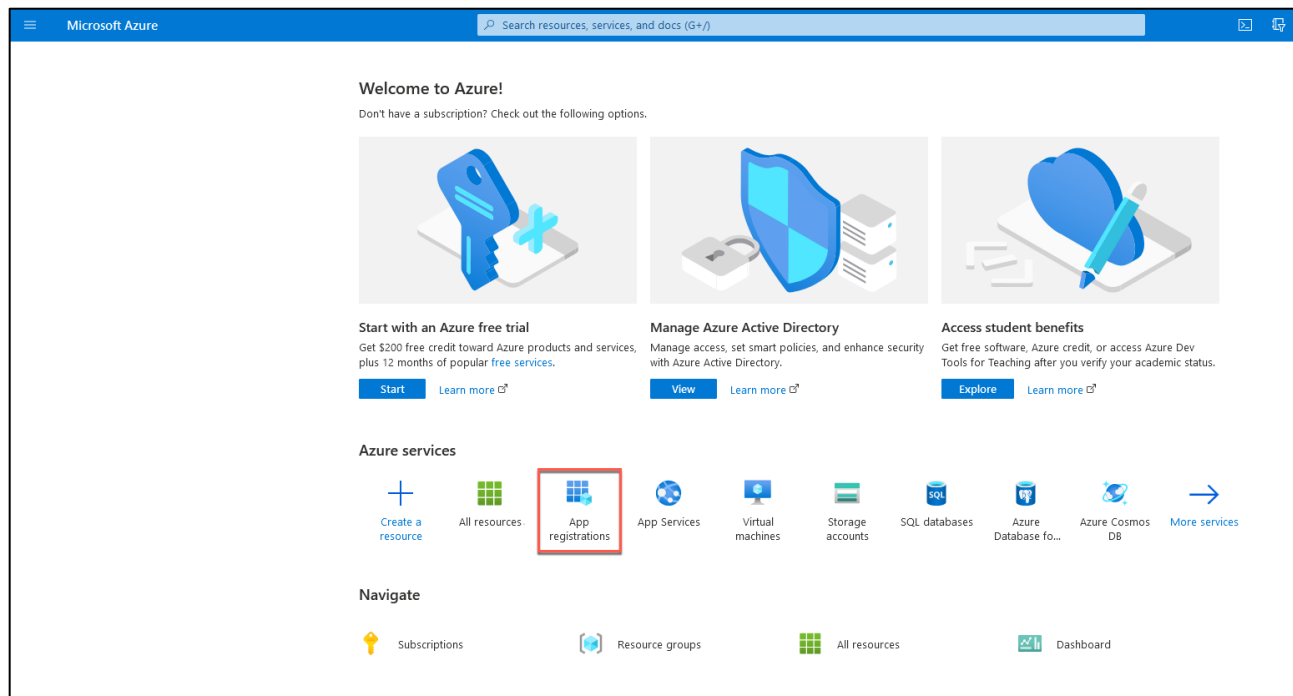
The release of Discovery Center 4.14.3 introduced a new SharePoint connector to provide enhanced performance for operations targeting SharePoint locations. This new connector uses modern APIs when interacting with SharePoint Online to reduce the risk of throttling and to provide other performance improvements. A pre-requisite to the use of these APIs is to authenticate using an Azure AD registered application and certificate. The following provides details on how to set up an application in Azure AD to support this authentication method. Details of how to create and use a credential record in the Discovery Center application to integrate with this application, and ultimately connect to SharePoint Online are included in the Discovery Center User Guide.

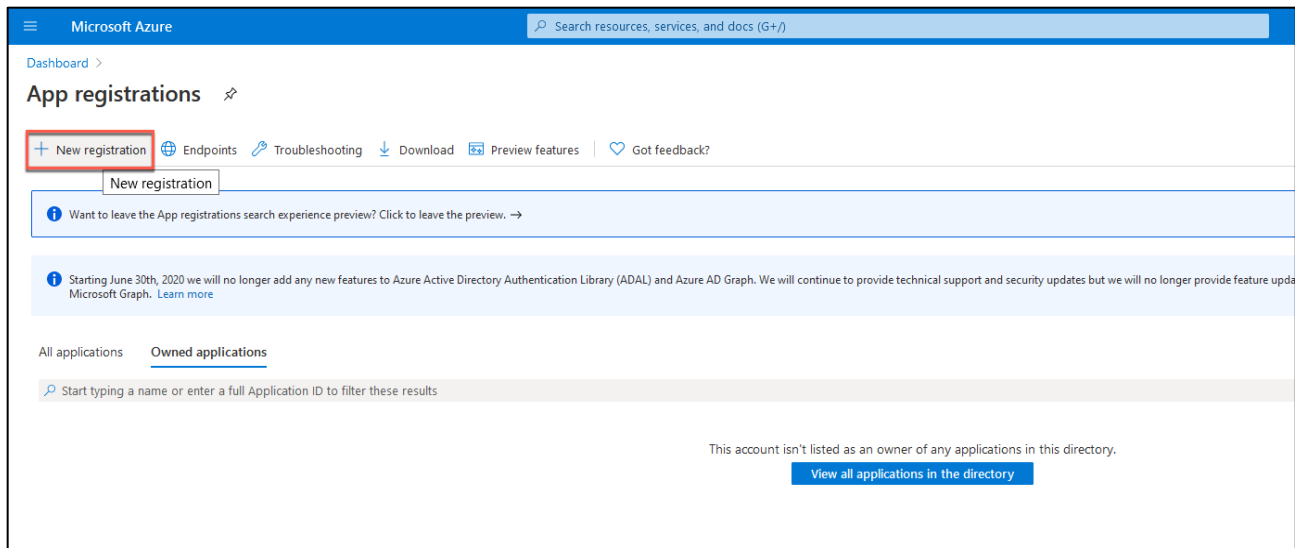
Registering an Azure Application for a SharePoint Online tenant

The following provides steps for registering an application in Azure AD for the SharePoint Online tenant to be accessed with a credential in Discovery Center. The steps include screenshots that were correct at the time of writing, but which may be outdated following any changes to the Azure AD cloud interface. For the latest instructions on how to register applications in Azure AD see <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>.

Note: Discovery Center makes use of a Certificate credential type for authentication with the registered Azure App. As a pre-requisite to this the public key element of a certificate must be uploaded to the Azure app with the private key element being uploaded to the Discovery Center application. The steps below assume a certificate has already been created for this purpose.

1. Log in to Azure AD as user with permissions to add and update App Registrations and navigate to **App Registrations** and choose **New Registration**:





2. Enter the name of the app, choose **Accounts in this organizational directory only** as the Supported account types, leave the **Redirect URL** blank and select **Register**.

Azure Active Directory admin center

Dashboard > All services > andevtest >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

ActiveNav Discovery Center SharePoint Integration ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (andevtest only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register



3. Select **API permissions** and choose **Add a permission**, under **Microsoft APIs** select **SharePoint**. Select **Application permissions** and select the **Sites.FullControl.All** checkbox before selecting **Add Permissions**.

ActiveNav Discovery Center SharePoint Integration | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect what will be used. [Learn more](#)

Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for andevtest

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

< All APIs
SharePoint
<https://microsoft.sharepoint-df.com/> Docs

SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Start typing a permission to filter these results

Permission	Admin consent required
Sites (1)	
<input checked="" type="checkbox"/> Sites.FullControl.All ⓘ Have full control of all site collections	Yes
<input type="checkbox"/> Sites.Manage.All ⓘ Read and write items and lists in all site collections	Yes
<input type="checkbox"/> Sites.Read.All ⓘ Read items in all site collections	Yes
<input type="checkbox"/> Sites.ReadWrite.All ⓘ Read and write items in all site collections	Yes
TermStore	
<input type="checkbox"/> TermStore.Read.All ⓘ Read managed metadata	Yes

Add permissions Discard

4. Select to **Grant admin consent** for the domain for the chosen permissions:

ActiveNav Discovery Center SharePoint Integration | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect what will be used. [Learn more](#)

Configured permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for andevtest

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...
SharePoint (1)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	⚠ Not granted for andevte... ...

To view and manage permissions and user consent, try [Enterprise applications](#).

5. Select **Certificates & secrets** and then **Upload certificate** before browsing to select the public key portion of the certificate to use for authentication with the app (.cer, .pem or .crt file types are accepted).

Dashboard > andevtest > ActiveNav Discovery Center SharePoint Integration

ActiveNav Discovery Center SharePoint Integration | Certificates & secrets

Search (Ctrl+/) < Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators | Preview
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable local scheme. For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Upload certificate	Start date	Expires	Certificate ID
No certificates have been added for this application.				

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Once these steps have been completed credential records can be created in the Discovery Center application to use for authentication to SharePoint Online using this registered app. These credential records should make use of the private key portion of the certificate that has been uploaded to the app, along with the Application ID and Tenant ID shown for the registered app.

Dashboard > andevtest >

ActiveNav Discovery Center SharePoint Integration

Search (Ctrl+/) < Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: ActiveNav Discovery Center SharePoint Integration	Client credentials	: 1 certificate, 0 secret
Application (client) ID	: c612c42f-22ca-490a-a8b5-c7cc801ca596	Redirect URIs	: Add a Redirect URI
Object ID	: 7c90d6f2-cc82-4674-afab-90264bbab8c6	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: ec82da52-3303-4b57-84f0-2a01e3681eb5	Managed application in I...	: ActiveNav Discovery Center SharePoint Integration

Supported account types : My organization only

Full details of how to create and make use of these credentials for interaction with SharePoint Online can be found in the Discovery Center User Guide.

Note: The permissions required for the Azure AD registered app as detailed above are **recommended** requirements of the APIs used to interact with SharePoint Online. **Microsoft has recently introduced the ability to assign Selected Site permissions, but the feature is subject to change.** For more information on the Selected Site permissions, please contact ActiveNav Support Team at support@activenav.com.

Appendix 10: MIP Sensitivity Label Integration

Integration Overview

For Discovery Center to integrate with **MIP Sensitivity Labels** defined for an organization, it must communicate with the organization's **Microsoft Office 365** instance with a given **user account**. This integration allows the Discovery Center application to retrieve the valid set of published MIP Sensitivity Labels for the user account in question.

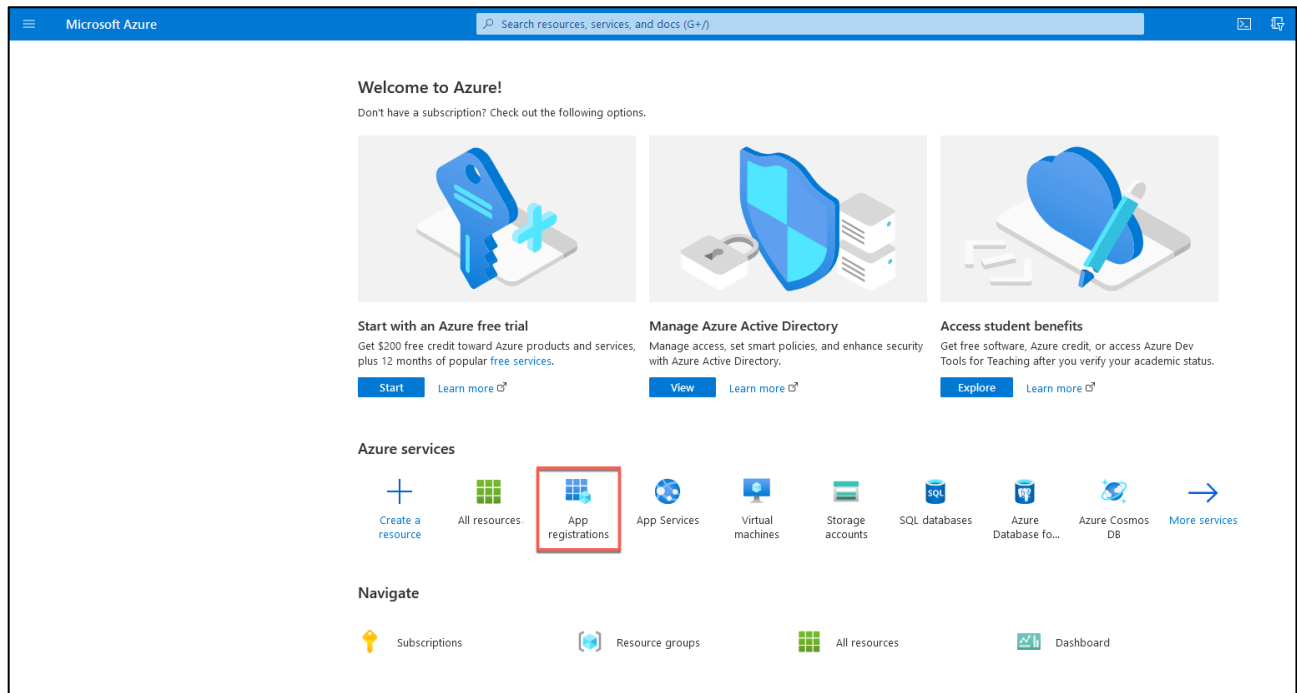
This integration is performed within Discovery Center using the **Microsoft MIP SDK**. This SDK is the only supported means of integration provided by Microsoft for code level integrations and has some pre-requisites.

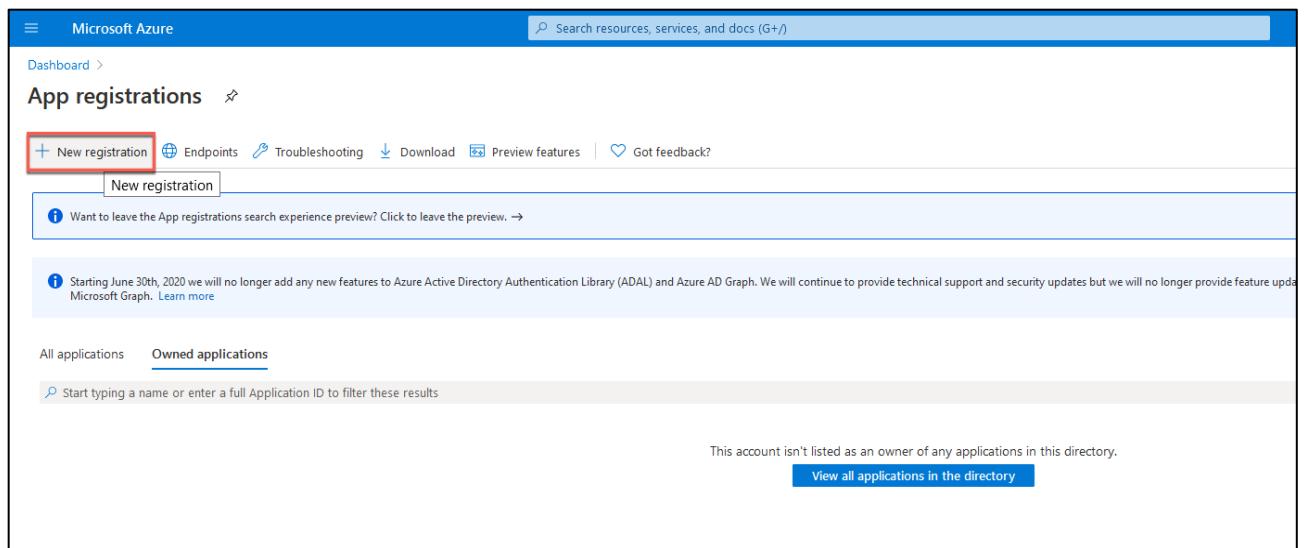
Note: The application making use of the SDK **must** be registered within the **Azure AD** environment of the **Microsoft 365 tenant** where the **MIP Sensitivity Labels** are defined. Details from this registration **must** be provided to the **SDK** from within Discovery Center's configuration, along with the **account of a user** that has **permissions** to **view** and/or **apply** the labels.

Registering Discovery Center in Azure AD

The following details the steps required to register the an application within Azure AD to allow the app registration to then be used by Discovery Center. The steps include screenshots that were correct at the time of writing, but which may be outdated following any changes to the Azure AD cloud interface. For the latest instructions on how to register applications in Azure AD see <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>.

6. Log in to Azure AD as user with permissions to add and update App Registrations and navigate to **App Registrations** and choose **New Registration**:





7. Enter the name of the app, choose **Accounts in this organizational directory only** as the Supported account types, leave the **Redirect URL** blank and select **Register**.

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > App registrations

Register an application

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

*** Name**

The user-facing display name for this application (this can be changed later).

Active Nav Discovery Center

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (anddevtest only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

8. Under **Manage** → **Authentication** and **Advanced Settings** set **Allow public client flows** to **Yes** and **Save**.

Microsoft Azure

Dashboard > App registrations > Active Nav Discovery Center

Active Nav Discovery Center | Authentication

Search (Ctrl+/) Save Discard Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Previ...
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (andevtest only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

☒ Yes ☐ No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

9. Under **Manage** → **API permissions**, select **Add a permission**. Select the **Azure Rights Management Services** option, select **Delegated permissions**, select the **user_impersonation** checkbox before selecting **Add Permissions**.

Microsoft Azure

Dashboard > App registrations > Active Nav Discovery Center

Active Nav Discovery Center | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Previ...
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for andevtest

API / Permissions name	Type	Description	Admin consent req.
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

All APIs

Azure Rights Management Services
<https://aadrm.com/> Docs

What type of permissions does your application require?

☒ Delegated permissions
Your application needs to access the API as the signed-in user.

☐ Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a reply url to filter these results

Permission	Admin consent required
user_impersonation ⓘ Create and access protected content for users	-

Add permissions Discard



10. Select **Add a permission** again, select **APIs my organization uses** and search for and select **Microsoft Information Protection Sync Service**. Select **Delegated permissions** and select the **UnifiedPolicy.User.Read** checkbox before selecting **Add Permissions**.

Microsoft Azure | Search resources, services, and docs (G+)

Dashboard > App registrations > Active Nav Discovery Center

Active Nav Discovery Center | API permissions

Overview | Quickstart | Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for andevtest

API / Permissions name	Type	Description	Admin consent req.
Azure Rights Management Service			
user_impersonation	Delegated	Create and access protected content for users	-
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

← All APIs

Microsoft Information Protection Sync Service
https://psor.a365syncservice.com

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Start typing a reply url to filter these results

Permission	Admin consent required
<input checked="" type="checkbox"/> UnifiedPolicy.User.Read ⓘ Read all unified policies a user has access to.	-

Add permissions Discard

11. Finally, select to **Grant admin consent** for the domain for the chosen permissions:

Azure Active Directory admin center

Dashboard > andevtest > Active Nav Discovery Center

Active Nav Discovery Center | API permissions

Overview | Quickstart | Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

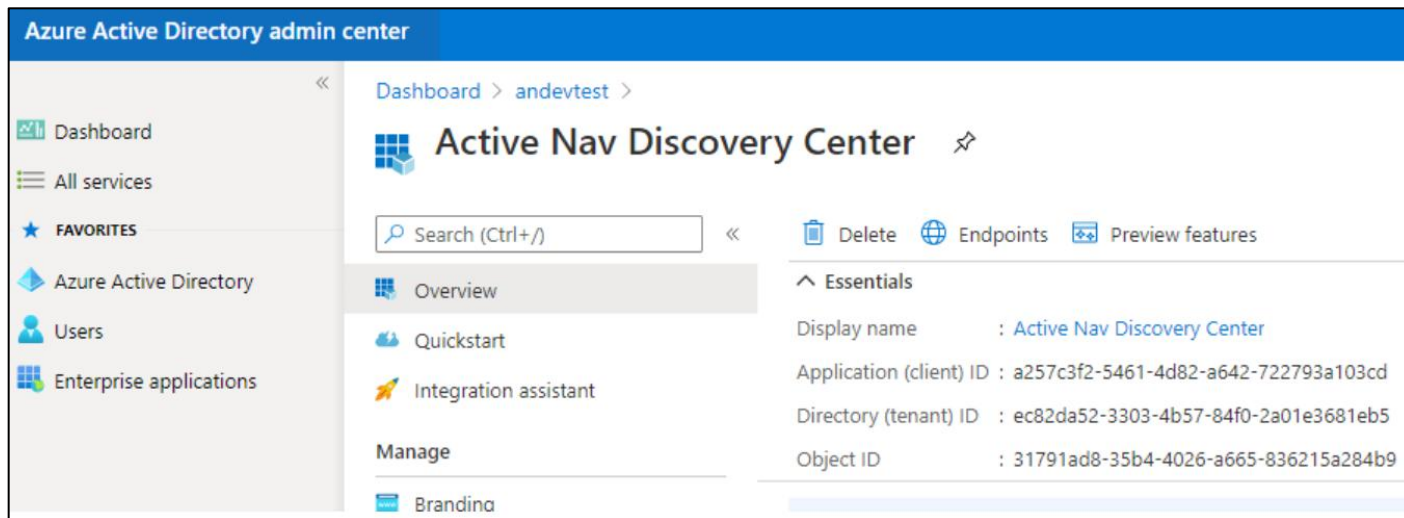
+ Add a permission ☒ Grant admin consent for andevtest

API / Permissions name	Type	Description	Admin consent req.
Azure Rights Management Service			
user_impersonation	Delegated	Create and access protected content for users	-
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-
Microsoft Information Protection			
UnifiedPolicy.User.Read	Delegated	Read all unified policies a user has access to.	-



Discovery Center System Setting requirements

Once Discovery Center has been registered as an app in Azure AD, some of the app registration details need to be applied to the Discovery Center System Settings for the integration to be successful. To find the relevant details in Azure, navigate to the app registration **Overview** page where the values for the **App Name**, **Application ID**, and **Tenant ID** are available and can be copied to the clipboard:



These values can then be applied to the **MIP Settings** section of the **Discovery Center System Settings** page and the credential of a user who has permissions to the MIP Sensitivity Labels published for the Microsoft 365 tenant.

The user account for this integration must have a username and password defined; the MIP SDK does not support the use of an app password for Multi-Factor authentication in the way that other Azure AD apps do.

The account used for this integration must have access to the MIP Sensitivity Labels defined in the Microsoft 365 tenant being used. This permission is dependent on the MIP label policies published in the Microsoft 365 Compliance Center. Essentially, suppose a user account has permissions to read and apply labels to files using other tools, such as directly in MS Office apps or through the Azure Information Protection Unified client. In that case, they will also have permission to do so from Discovery Center via the SDK integration.

Whenever any protection has been applied to a file with an MIP Sensitivity Label, if the user account used for the integration has permission to read the protected file, it will also be able to read and apply MIP Sensitivity Labels. Therefore, it is recommended that the user chosen for the integration is granted permission using an MIP Sensitivity Label policy to read and apply all labels that have been published for an organization. The user should also have permission to access any protected files. Beyond this, no specific MIP-related admin permissions or roles are required for the integration to work successfully.

Scheduling Constraints

Indexing and other network intensive tasks cannot be carried out during the following times.

[Add Schedule Constraint](#)

No schedule constraints have been defined.

Times displayed in (UTC+00:00) Dublin, Edinburgh, Lisbon, London (GMT Summer Time)

Global Settings

Maximum number of skim threads	5	
Maximum number of threads	5	
Maximum number of values for a field	100	
Export location	C:\dev-install\Exports\	
Show Disclaimer	false	
Enable Custom Queries	false	
VUM Warning (Percentage)	90	

Edit

MIP Settings

MIP settings have been successfully validated.

If the MIP settings are updated, the ANScheduler service must be restarted for the changes to be applied.

MIP O365 Tenant ID	5123ad5a-ab71-78f1-82b1-abc6a89e4a0e	
MIP O365 Tenant Locale	en-US	
MIP O365 App ID	12ac34fe-56a7-89ab-dc08-e9f62805g224	
MIP O365 App Name	ActiveNav MIP Labelling PoC	
MIP O365 App Version	1.0.0	
Discovery Center Credential for MIP	MIP User	
MIP O365 Cloud Type	Commercial	

Edit

Appendix 11: Exchange Online ROPC Authentication

Users of the Exchange Connector to process content in Exchange Online should note that Microsoft have confirmed their plans to disable the use of Exchange Web Services (EWS) to access Exchange Online in October 2026. This means that the Exchange Connector in Discovery Center will no longer be compatible with Exchange Online after this date

<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-ews-exchange-online>

Resource Owner Password Credentials (ROPC) Authentication

Discovery Center must authenticate using a secure token obtained from an Azure Active Directory registered application when using the Discovery Center Exchange Connector for indexing and report actions on Exchange Online mailboxes.

The OAuth 2.0 ROPC Grant authentication flow (see <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth-ropc> for details) uses secure tokens. These tokens are provided following authentication to an Azure AD registered application using Discovery Center username and password credentials and are then used for interaction with Exchange Online.

To **enable ROPC in Azure Active Directory**, either use **ActiveNav Exchange Connector multi-tenant application** or **register your application in your Azure Active Directory tenant**.

- If using the provided multi-tenant application, follow the instructions in the section titled [ActiveNav Exchange Connector Multi-Tenant Application](#).
- If registering your application, follow the instructions in the [Registering an Application for Exchange Connector ROPC Authentication](#) and [Using the Registered Application with Discovery Center](#) sections.

Note: This **only** applies to **Exchange Online**. **On-Premises Exchange** instances will use the **username** and **password** credential for **NTLM** authentication.

ActiveNav Exchange Connector Multi-Tenant Application

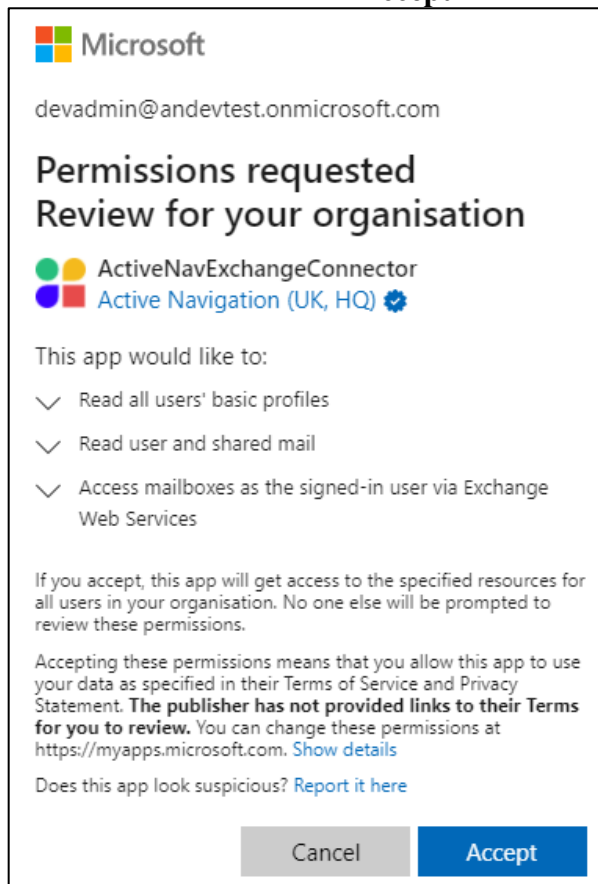
By default, the ActiveNav Exchange Connector uses the ActiveNav Exchange Connector Multi-Tenant Application for authentication. The application must be granted tenant-wide admin consent on the tenant that the connector needs to authenticate against to be successful.

To grant tenant-wide admin consent, take the following steps:

1. Navigate to URL: https://login.microsoftonline.com/common/adminconsent?client_id=182cffc8-d45a-49ad-972f-22675ceeaf2f&redirect_uri=https://activenavcustomerportal.blob.core.windows.net/an-customer-resource/ExchangeConnector.html
2. Sign-in as a user on the Azure Activity Directory tenant who has one of the following roles:
 - Global Administrator**
 - Application Administrator**
 - Cloud Application Administrator.**



A consent prompt will display, detailing the specific permissions the multi-tenant application is requesting. Review the information and select **Accept**.



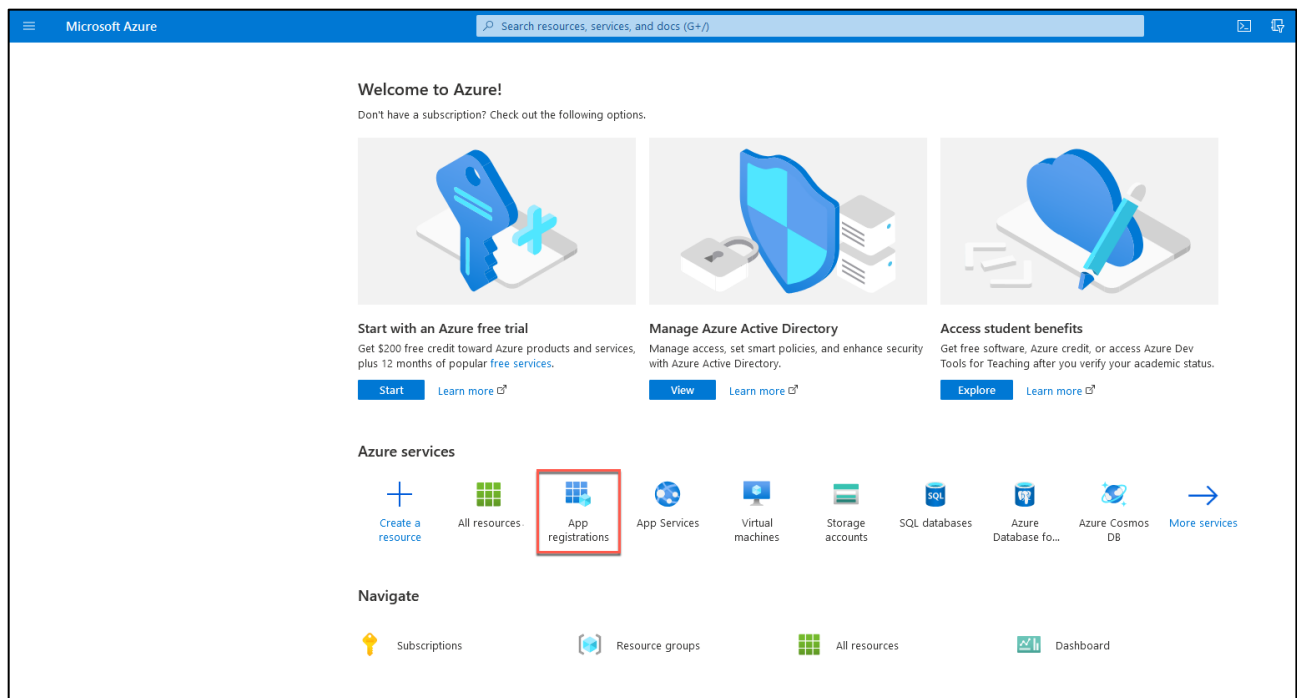
3. This will redirect the user to the URL below, which displays a message confirming that **tenant-wide admin consent** has been **successfully granted** to the application. Note that {TenantId} will be replaced with the identifier for the tenant where consent has been granted.

https://activenavcustomerportal.blob.core.windows.net/an-customer-resource/ExchangeConnector.html?admin_consent=True&tenant={TenantId}

Registering an Application for Exchange Connector ROPC Authentication

The following steps detail what is required to register your own Azure Active Directory application and use this for ROPC authentication when connecting Discovery Center to Exchange Online. The steps include screenshots that were correct at the time of writing, but which may be outdated following any changes to the Azure AD cloud interface. For the latest instructions on how to register applications in Azure AD see <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>.

1. Log in to **Azure AD** as a user with permissions to **add** and **update App Registrations** and navigate to **App Registrations** and choose **New Registration**:



2. Enter the name of the app, choose **Accounts in this organizational directory only** as the Supported account types, leave the Redirect URL **blank**, and select to **Register**.

Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > App registrations >

Register an application

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

*** Name**

The user-facing display name for this application (this can be changed later).

Active Nav Discovery Center

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (anddevtest only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- Under **Manage → Authentication and Advanced Settings** set **Allow public client flows** to **Yes** and **Save**.

Microsoft Azure

Dashboard > App registrations > Active Nav Discovery Center

Active Nav Discovery Center | Authentication

Search (Ctrl+/) Save Discard Got feedback?

Manage

- Overview
- Quickstart
- Integration assistant
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (andevtest only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

Yes No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

- Under **Manage → API permissions** choose to **Add a permission**. The following Delegated permissions will need to be added for the application.

API Name	Permission Name
Microsoft Graph	User.ReadBasic.All
Office 365 Exchange Online	Mail.Read.All
Office 365 Exchange Online	EWS.AccessAsUser.All

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for andevtest

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (1)				
User.ReadBasic.All	Delegated	Read all users' basic profiles	No	
Office 365 Exchange Online (2)				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange ...	No	
Mail.Read.All	Delegated	Read user and shared mail	No	



5. From the same page, **grant admin consent** for the application and selected permissions on the domain by selecting **Grant admin consent for {tenant name}**, where {tenant name} is the name of the tenant where tenant-wide admin consent is being granted.

Using the Registered Application with Discovery Center

This section details the action required to reference your own registered Azure AD Application from Discovery Center for use when performing ROPC authentication Exchange Online.

Navigate to the Overview page for the registered application to obtain the Application (client) ID. This will be used to add the below setting value in the Discovery Center application configuration files, where {ApplicationId} is replaced with the Application (client) ID.

```
<ActiveNavigation.ConnectorsFramework.Exchange.Settings>
  <setting name="AuthClientId" serializeAs="String">
    <value>{ApplicationId}</value>
  </setting>
</ActiveNavigation.ConnectorsFramework.Exchange.Settings>
```

This setting will need to be added to the following Discovery Center configuration files, where {install location} is the installation directory chosen when installing Discovery Center.

- a. {install location}\Analysis\ANAnalysis.exe.config
- b. {install location}\Scheduler\SchedulerTasks.config
- c. {install location}\Scheduler\ActiveNavigation.Scheduler.exe.config
- d. {install location}\Skimmer\ANSkimmer.exe.config

For assistance with locating and updating the Discovery Center configuration files, please contact ActiveNav Support.



Appendix 12: Prerequisites for Preserving NTFS File Owner

The restore of the File Owner to the state prior to labeling will be performed by the Credential applied to target location in Discovery Center. To successfully change the File Owner, this credential must meet the following criteria:

- It must have **Full Control** permission on the target file share;
- It must be assigned **SeRestorePrivilege**. This is most commonly obtained by being a member of the Backup Operators or Administrators group.

Furthermore, if the credential being used to perform the File Owner update is a Local (non-Domain) account, Windows User Account Control (UAC) may prevent the file owner being updated. To circumvent this Microsoft suggest a workaround whereby a registry entry is set to disable UAC for remote connections, detailed here: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/user-account-control-and-remote-restriction> .



Appendix 13: Common Problems

How to Troubleshoot Installer Problems

Most installation problems with the Discovery Center are related to **pre-requisite software**, **user account permissions**, or **both**. Please refer to the installation instructions and check that each step has been followed.

If problems persist, run the installer from the **command window** and generate a **log file** to locate the problem:

1. Open a command window and run the following command where **<ActiveNavigation.Setup.msi>** is the name of your Active Navigation setup file.

```
msiexec /package <ActiveNavigation.Setup.msi> /I* install.log
```

2. Follow the steps in the installer in the usual way until the installer fails.
3. A file named **install.log** will be generated in the same folder as the **setup.msi** script. Open the log file using a text editor and search for **Value 3**; this will highlight where the error lies. If **Value 3** doesn't exist, contact ActiveNav Support.

Common Installation Problems

Below are some common installation problems and their solutions.

Installation fails, and the log indicates that "The library drive or media pool must be empty to perform this operation. Exception from HRESULT 0x800710D3", or the Discovery Center web UI displays "Server Error in '/' Application."

Ensure **ASP.NET v4** has been installed and registered with **IIS** by following the instructions provided in the [.NET Framework](#) section of this guide.

Installation fails with "Scheduler identity validation" message

The installer might display a message with the text **"the user has not been granted the requested logon type at this computer, and user must be given 'Logon as a service right'"**, even though the **Local Policy Manager** application has been used to assign the **Logon as a service** right. To resolve the issue, exit the installer and install using the following **command-line** options:

```
VALIDATE_SCHED_USER=no  
VALIDATE_APP_POOL_USER=no
```

Visiting Discovery Center Shows Only "Page not found" or "404.2 Not Found."

IIS has not been configured to allow **ASP.NET v4 Web Service Extensions**. Enable this using the **IIS Manager** application **ISAPI** and the **CGI Restrictions** configuration option.

Visiting Discovery Center Shows Only "Server Error '/' Application" or "Unknown Error"



Ensure **ASP .NET v4** has been installed and registered with **IIS** by following the instructions in the [.NET Framework](#) section of this guide.

Cannot See All Tabs in the Discovery Center Interface

The Discovery Center tabs are hidden if the **logged-in user** is **not mapped to relevant ActiveNav roles**. Log in as an **ActiveNav System Administrator**, and from the **User Access** tab, map the correct **users** to the necessary **roles**.

Test Index Fails with Error "start location not found."

By default, an index will use the **Scheduler Service account credentials** to access index files. If the **Scheduler** has insufficient rights to the test data set, the text index will fail. Grant the failing index specific credentials or change the Scheduler Service credentials.

Downloaded Connector Files are Blocked from Execution After System Upgrade

A connector package downloaded directly to a server system and copied as part of an upgrade may cause local system policies to mark the zip file and contents as **downloaded from a remote system**, preventing execution.

Installing connector files marked in this way as part of an upgrade will cause errors like this:

System.NotSupportedException: An attempt was made to load an assembly from a network location which would have caused the assembly to be sandboxed in previous versions of the .NET Framework.

Follow these instructions <https://msdn.microsoft.com/en-us/library/ee890038.aspx> to **unblock** the **individual DLLs** installed for the connector.

Using ActiveNav Support

The ActiveNav Support Center allows you to create and track support tickets, review Knowledge Base articles, and access product and documentation downloads. New customers and partners can register on the support site to gain access.

<http://support.activenav.com>



Copyright © 2025 Data Discovery, Limited. All Rights Reserved

ActiveNav is a registered trademark of Data Discovery Solutions Ltd in the United States and other countries. All trademarks used herein are the property of their respective owners.

ActiveNav believes that information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” ActiveNav make no representation or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantable or fitness for a particular purpose.

