AUTODESK® VAULT SERVER

Advanced Configuration Guide for Autodesk® Vault Server 2013

Autodesk®

Contents

Introduction

The Advanced Configuration Guide contains additional information for setting up the Autodesk® Vault Server 2013. The topics in this guide relate to the Autodesk® Vault Server and can be used for all versions of Vault 2013 unless otherwise noted in the instructions for each configuration. As these topics cover advanced configurations, some familiarity with IT procedures is assumed. For more information, refer to the Autodesk® Vault Server Implementation and Managing Your Data guides.

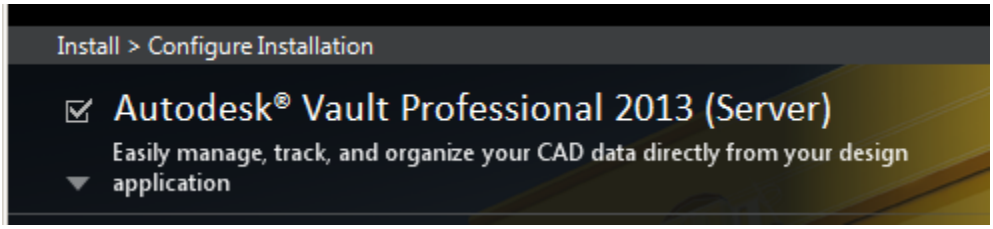
Installing Autodesk Vault Server 2013

For standard installation configurations, consult the Autodesk Vault Server 2013 Implementation guide.

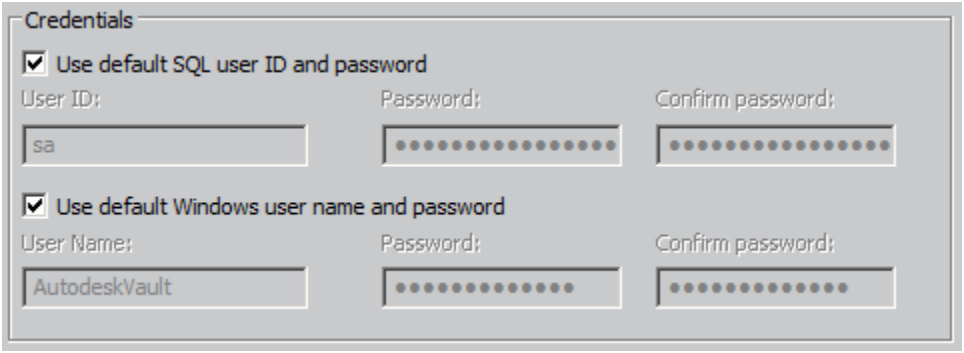
Customizing your Autodesk Vault Server 2013 installation

To customize your installation perform the following:

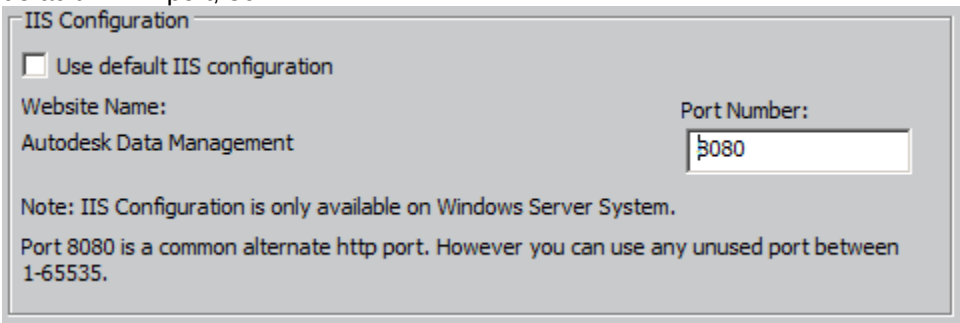
1. From the Install >Configure Installation screen, select the down arrow “Easily manage, track, and organize your CAD data directly from your design application”.



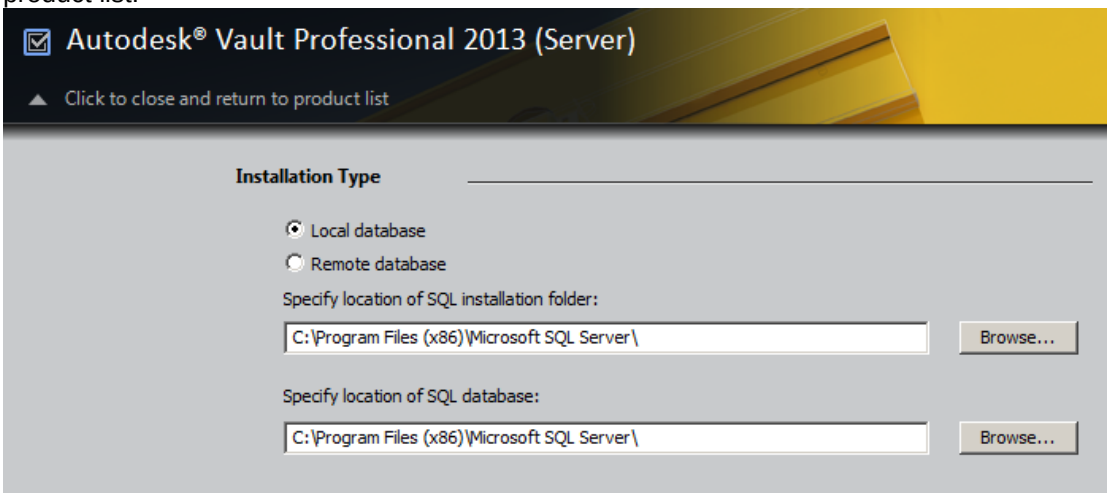
2. Database options will allow you to specify the SQL installation location if SQL has not been installed previously. Also, if a remote SQL location is available this option will be available. You will have the option to set the SQL sa password during installation by checking the box next to Use my SQL credentials.
******This will need to be entered if the AutodeskVault SQL instance was installed prior to the Autodesk Vault Server with a sa password other than the default **AutodeskVault@26200**. Additionally, you can specify the impersonation user account if desired.



3. Vault Server 2013 has the option to automatically configure IIS to a port other than the default HTTP port, 80.



4. Selecting the up arrow at the top of the available options will return you to the installation product list.



IIS

Installing Autodesk Vault Server 2013 on Windows 7, Server 2008, Server 2008 R2

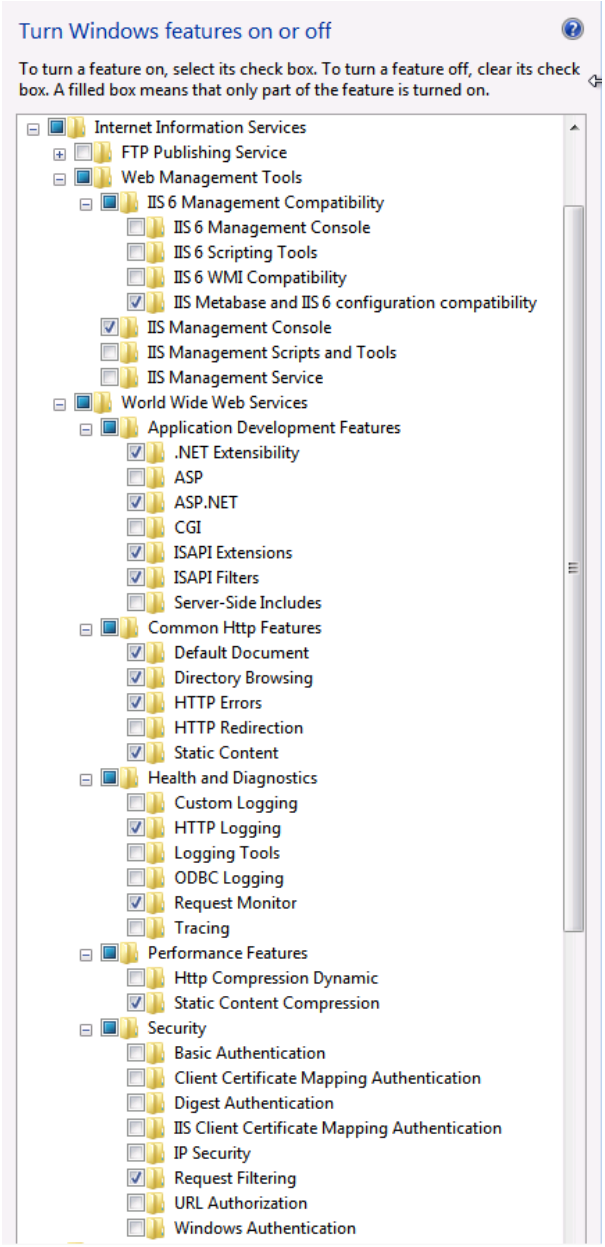
Note: IIS 7.0 has a limit of 10 simultaneous requests on non-server OS editions. When the connection limit is reached, the request is queued until the number of currently processing requests drops below the limit. IIS then will take the first request in the queue and starts to process it. Previous versions of IIS would return an **Error 403.9 Access Forbidden – Too many users are connected**.

Configuring Internet Information Services (IIS) 7.0

If you will be using Microsoft® Internet Information Services (IIS) 7.0 with Autodesk Vault Server, IIS 7.0 may be configured before you install Autodesk Vault Server. IIS 7.0 can be installed by the Autodesk Vault Server 2013 installation process as well. If you are installing IIS 7.0 manually, follow the steps below to configure the system options:

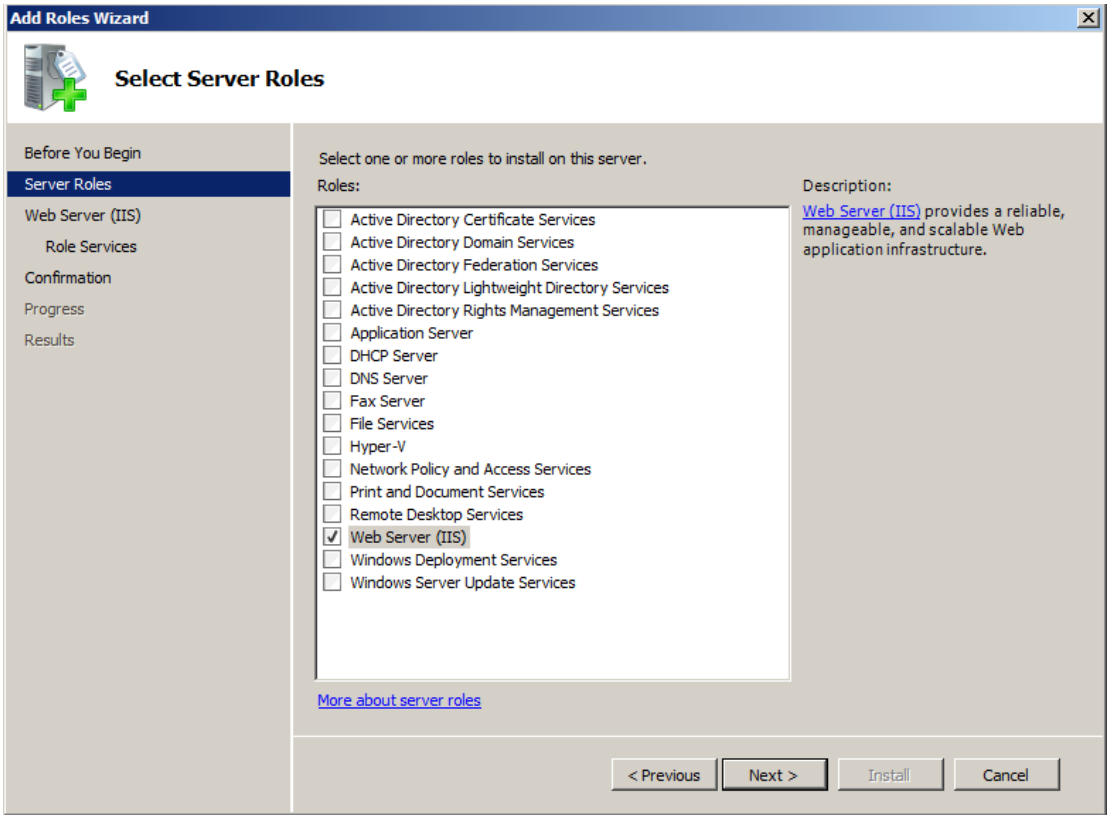
Windows 7

1. From the Windows Start menu select **Settings** > **Control Panel**.
2. In the Control Panel, double-click **Programs and Features**.
3. In the **Programs and Features** group, click **Turn Windows Features On or Off**.
4. If prompted to allow the application to run, click **Continue**.
5. Select the following options underneath **Internet Information Services**:
   IIS Metabase and IIS 6 configuration compatibility; IIS Management Console; .NET Extensibility; ASP.NET; ISAPI Extensions; ISAPI Filters; Default Document; Directory Browsing; HTTP Errors; Static Content; HTTP Logging; Request Monitor; Static Content Compression; Request Filtering.

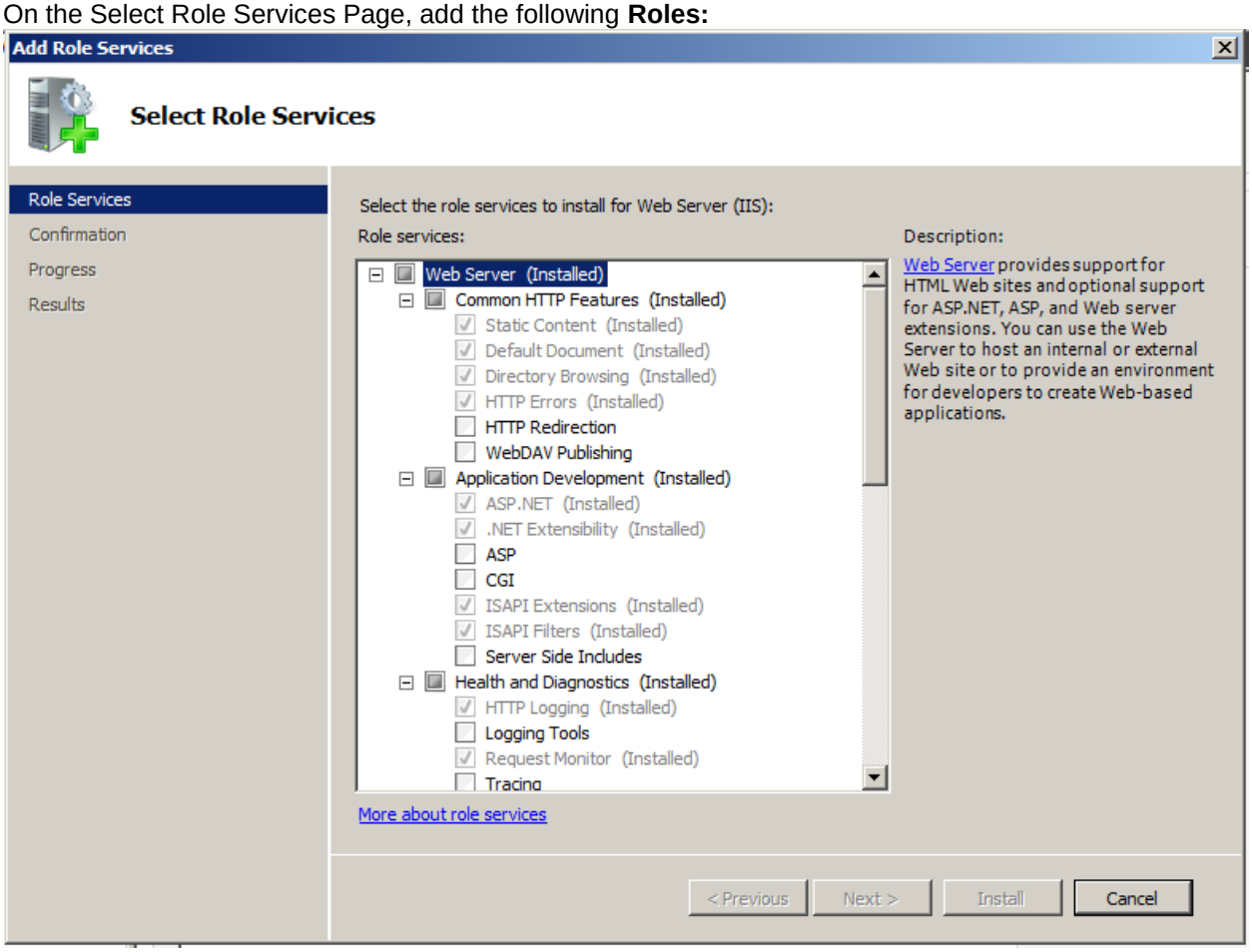


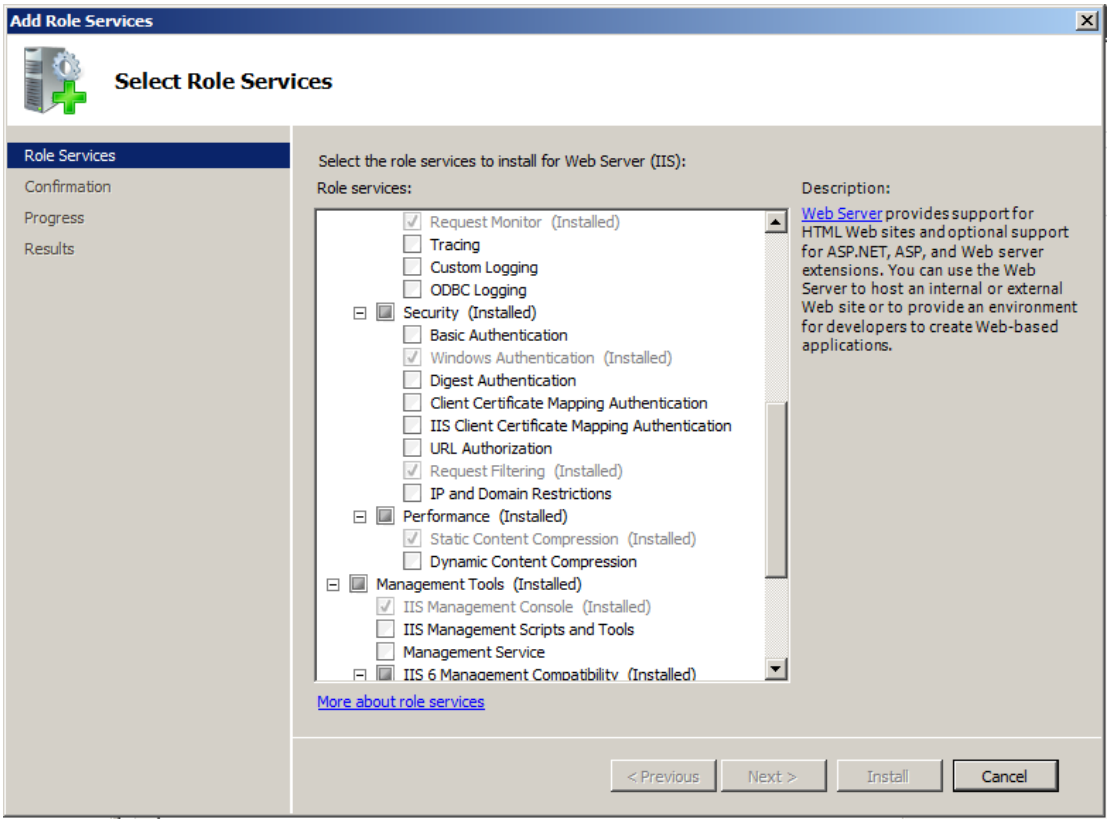
Windows 2008 / 2008 R2

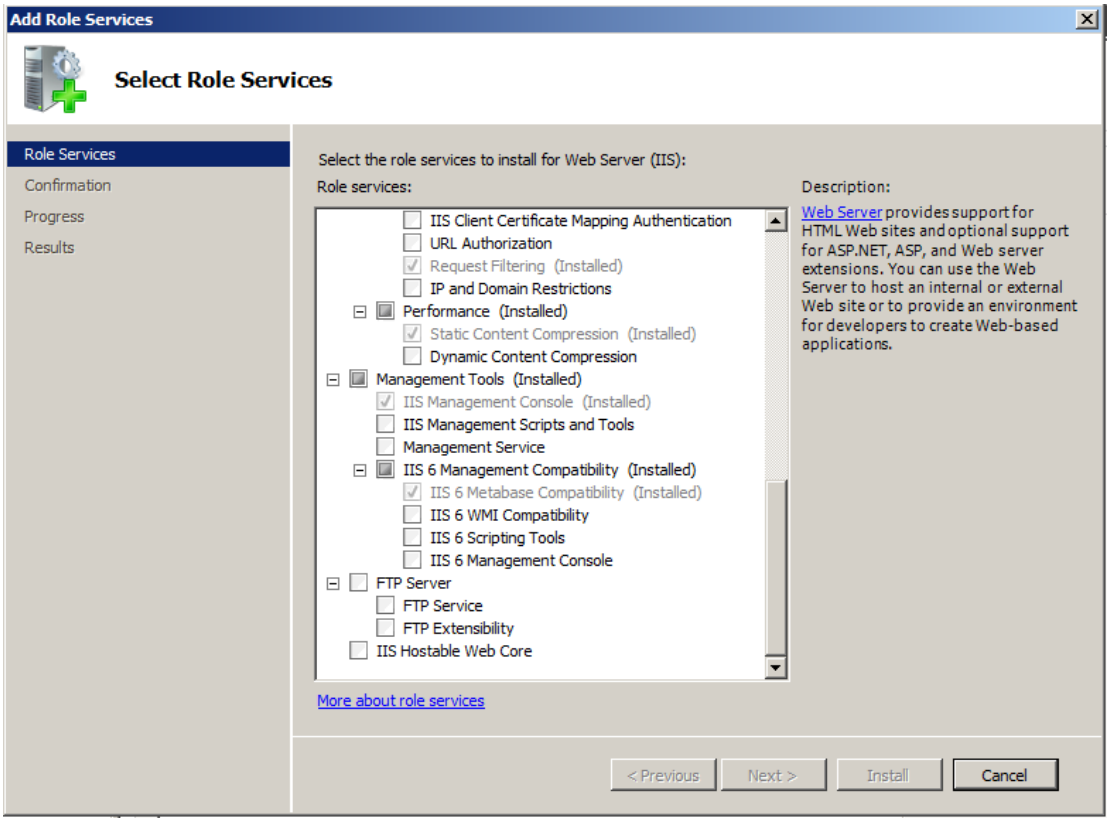
1. From the Windows Start menu select **Server Manager**.
2. Under **Roles Summary** select **Add Role**.
3. On the Select Server Roles Page, select **Web Server (IIS)**



4. On the Select Role Services Page, add the following **Roles:**




Add Role Services
Select Role Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Web Server (IIS):
Role services:
Request Monitor (Installed)
Tracing
Custom Logging
ODBC Logging
Security (Installed)
Basic Authentication
Windows Authentication (Installed)
Digest Authentication
Client Certificate Mapping Authentication
IIS Client Certificate Mapping Authentication
URL Authorization
Request Filtering (Installed)
IP and Domain Restrictions
Performance (Installed)
Static Content Compression (Installed)
Dynamic Content Compression
Management Tools (Installed)
IIS Management Console (Installed)
IIS Management Scripts and Tools
Management Service
IIS 6 Management Compatibility (Installed)
More about role services
Description:
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel


Add Role Services
Select Role Services
Role Services
Confirmation
Progress
Results
Select the role services to install for Web Server (IIS):
Role services:
IIS Client Certificate Mapping Authentication
URL Authorization
Request Filtering (Installed)
IP and Domain Restrictions
Performance (Installed)
Static Content Compression (Installed)
Dynamic Content Compression
Management Tools (Installed)
IIS Management Console (Installed)
IIS Management Scripts and Tools
Management Service
IIS 6 Management Compatibility (Installed)
IIS 6 Metabase Compatibility (Installed)
IIS 6 WMI Compatibility
IIS 6 Scripting Tools
IIS 6 Management Console
FTP Server
FTP Service
FTP Extensibility
IIS Hostable Web Core
More about role services
Description:
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

Role Services: 22 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Not installed
HTTP Errors	Installed
HTTP Redirection	Not installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Not installed
CGI	Not installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Not installed
Health and Diagnostics	Installed
HTTP Logging	Installed
Logging Tools	Not installed
Request Monitor	Installed
Tracing	Not installed
Custom Logging	Not installed
ODBC Logging	Not installed
Security	Installed
Basic Authentication	Not installed
Windows Authentication	Installed
Digest Authentication	Not installed
Client Certificate Mapping Authentication	Not installed
IIS Client Certificate Mapping Authentication	Not installed
URL Authorization	Not installed
Request Filtering	Installed
IP and Domain Restrictions	Not installed
Performance	Installed
Static Content Compression	Installed
Dynamic Content Compression	Not installed
Management Tools	Installed
IIS Management Console	Installed
IIS Management Scripts and Tools	Not installed
Management Service	Not installed
IIS 6 Management Compatibility	Installed
IIS 6 Metabase Compatibility	Installed
IIS 6 WMI Compatibility	Not installed
IIS 6 Scripting Tools	Not installed
IIS 6 Management Console	Not installed

Installing Autodesk Vault Server 2013 with other web applications using a different .NET version

The Autodesk data management software will usually coexist with other web applications in the Default Web Site of IIS. However, there are certain applications that require a different .NET Framework version. This section illustrates how you can configure the Autodesk Vault Server

Virtual directory to run under a different .NET version in the Default Application pool. You cannot run two different versions of .NET Framework in the same application pool with IIS 6.0. To work around this limitation, you will need to create a second application pool, and then configure it to run .NET Framework 4.0. Prior to running the Autodesk Vault Server installation you will have to configure the Default Web Site to use .NET 4.0.

Internet Information Services (IIS) 6

Note: Changing this setting will disable all other virtual folders under the Default Web Site to use .NET 4.0 until you change it back to the required .NET version for that application.

Open the IIS management console.

1. Open each virtual directory and note the .NET version that it is configured to use.
2. Right-click the Default Web Site and select Properties.
3. On the ASP.NET tab, select the **.NET 4.0.30319** from the drop-down list and click OK.
4. Install Autodesk Vault Server 2013.

To create an Application Pool

1. Open **(IIS Manager** in the **Administrative Tools** of the **Control Panel**.
2. Right-click the **Application Pools** folder. Click **New Application Pool**.
3. In the **Application pool ID** field, enter **AutodeskAppPL**.
4. Select the **Use existing application pool** as template radio button and use the **DefaultAppPool** as a template.
5. Click the **OK** button to apply the changes.

To assign the new Application Pool

1. Expand the **Default Web Site** and navigate to the **AutodeskDM\Services** virtual directory.
2. Right-click on the **Services** directory and select **Properties.**
3. In the **Directory** tab, change the **Application Pool** drop-down to the newly created **AutodeskAppPL** Application Pool.
4. **Apply** the changes and close the properties of the Services virtual directory.

To reset the .NET Framework version

1. Open the properties of the **Default Web Site**.
2. In the **ASP.NET** tab, select the original .Net version from the drop-down list. **Note:** If you are changing this from .NET 4.0 to a different version you will have to reconfigure the AutodeskDM\Services virtual directory back to .NET 4.0.
3. Re-check all Virtual directories to make sure the correct .NET version is configured for the application.

Internet Information Services (IIS) 7

To create an Application Pool

1. Open **Internet Information Services (IIS) Manager** in the **Administrative Tools** of the **Control Panel**.
2. Right-click the **Application Pools** folder. Click **Add Application Pool**.
3. In the **Name** field, enter **AutodeskAppPL**.

4. Ensure

   .NET Framework version: is set to **".NET Framework v4.0.30319"**

   Managed pipeline mode: is set to **"Integrated"**

   Start application pool immediately is ticked

5. Click the OK button to apply the changes.

To assign the new Application Pool

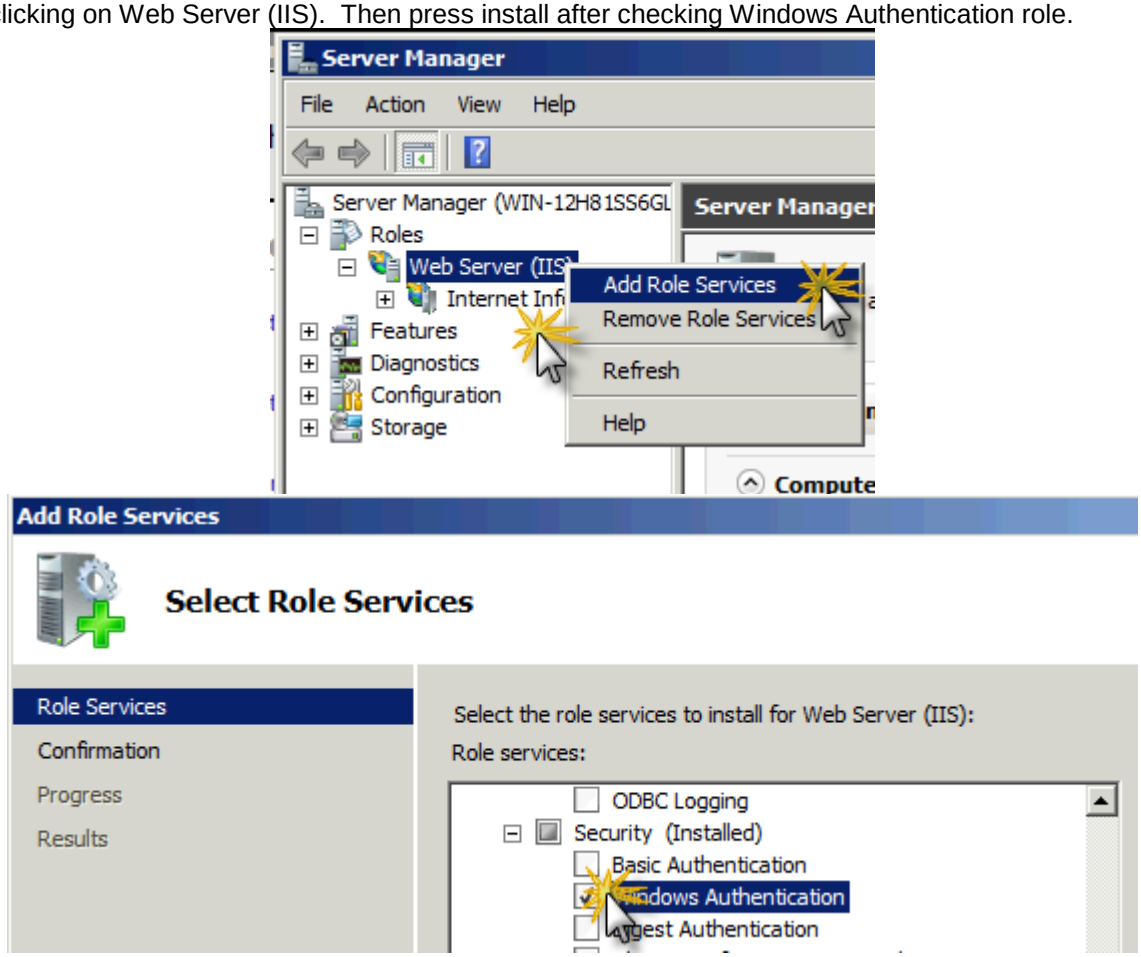
1. Under **Sites**, expand the **Default Web Site** and navigate to the **AutodeskDM\Services** virtual directory.
2. Right-click on the **Services** directory and select **Manage Application -> Advanced Settings.**
3. Under **General**, change the Application Pool to **AutodeskAppPl**
4. Click **OK** to apply the changes and close the properties of the Services virtual directory.

Enabling Windows Authentication on Windows 2008 After Installing Vault Server

With the release of '*TS1110787 – Passing Win Auth Login on Web Client'* users will encounter an issue with enabling their environment properly. The following steps are required to correctly use Windows authentication. Instructions below are for Windows 2008, Windows 2008 R2 and Windows 2003

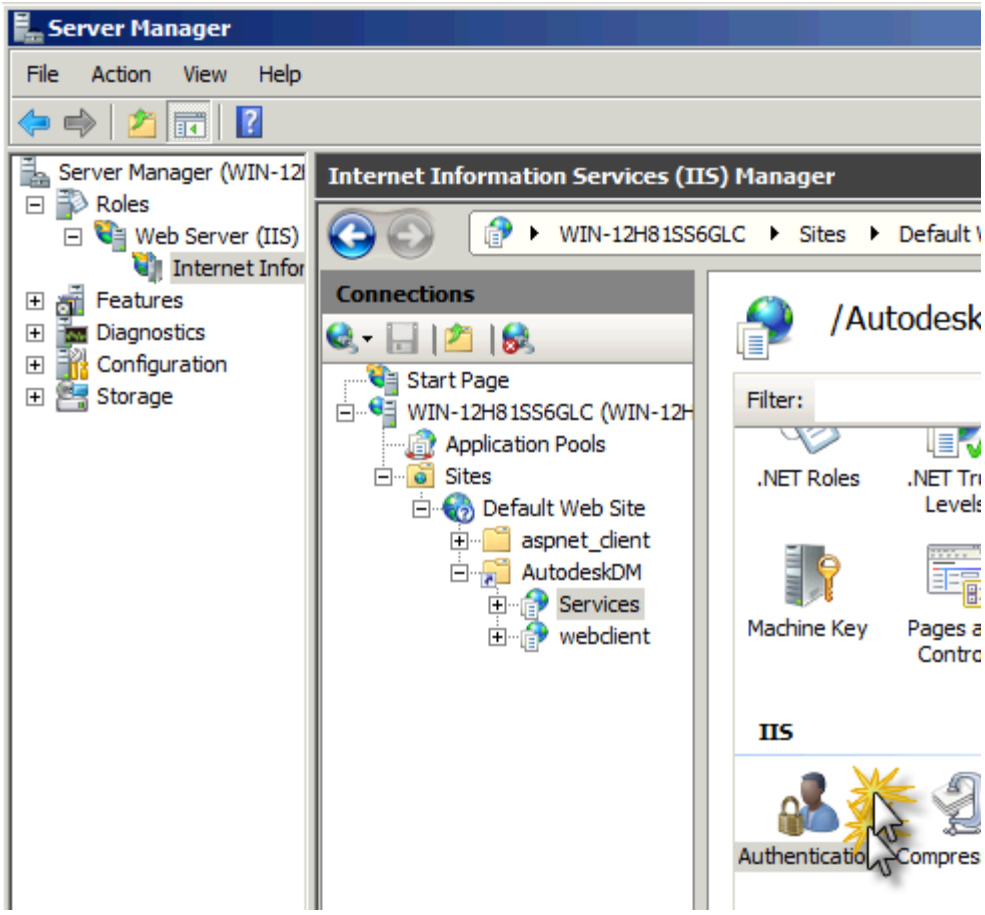
Steps to enable Win Auth in Windows 2008 (IIS7)

1. Open Server Manager in Windows 2008, expand Roles, select Add Role Service upon right-clicking on Web Server (IIS). Then press install after checking Windows Authentication role.

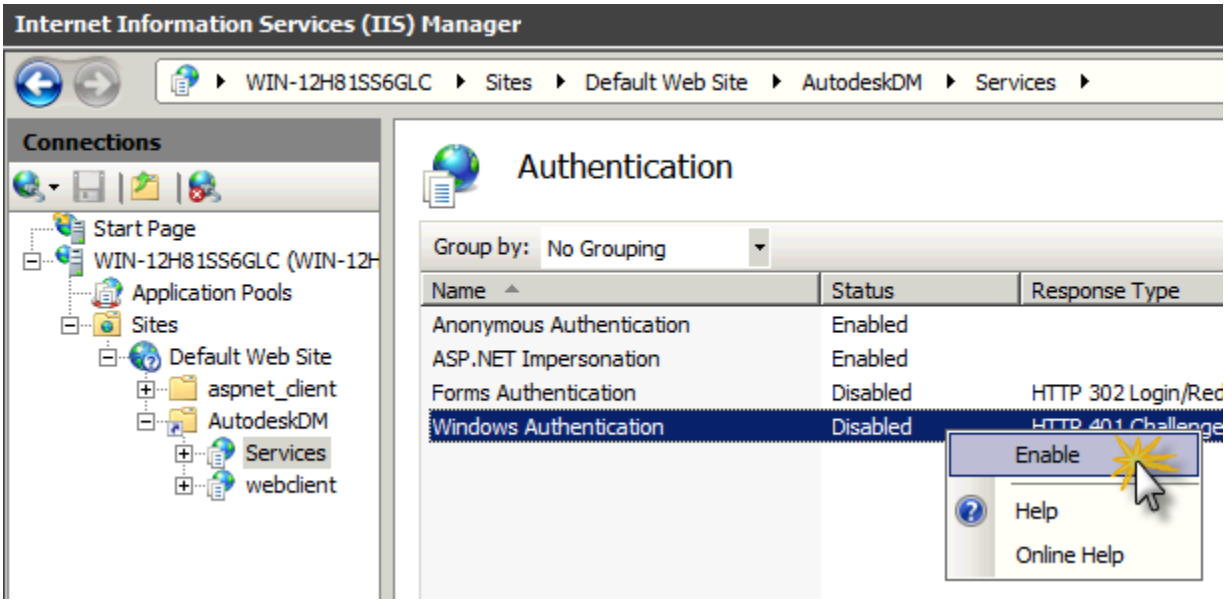


2. While still in Server Manager, expand Web Server (IIS), click on IIS Manager, and navigate through to MachineName>Sites>Default Web Site>AutodeskDM. Select **Services** and Dbl-click on Authentication feature under the IIS section.

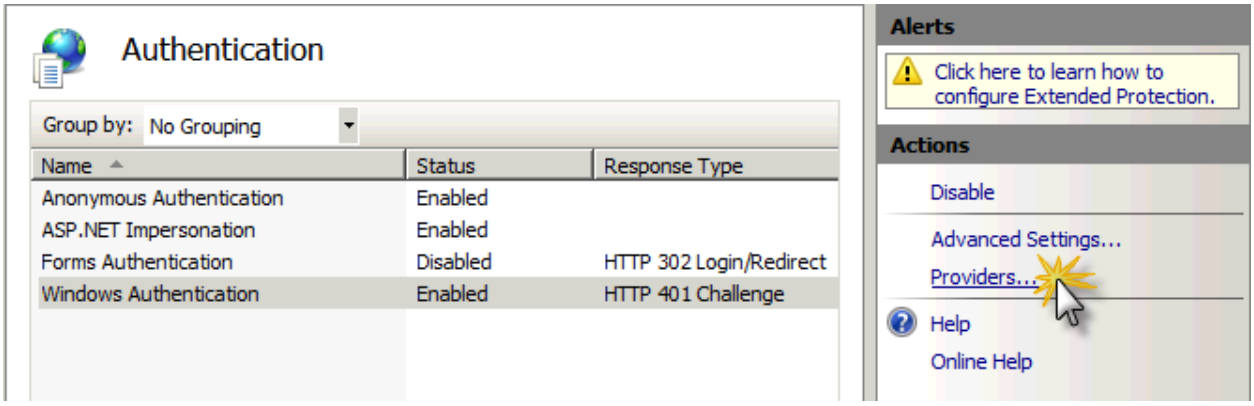
NOTE: *Services is the only tree node that would need Windows Authentication enabled. It is not necessary to enable WinAuth on Default Web Site or AutodeskDM directories.*



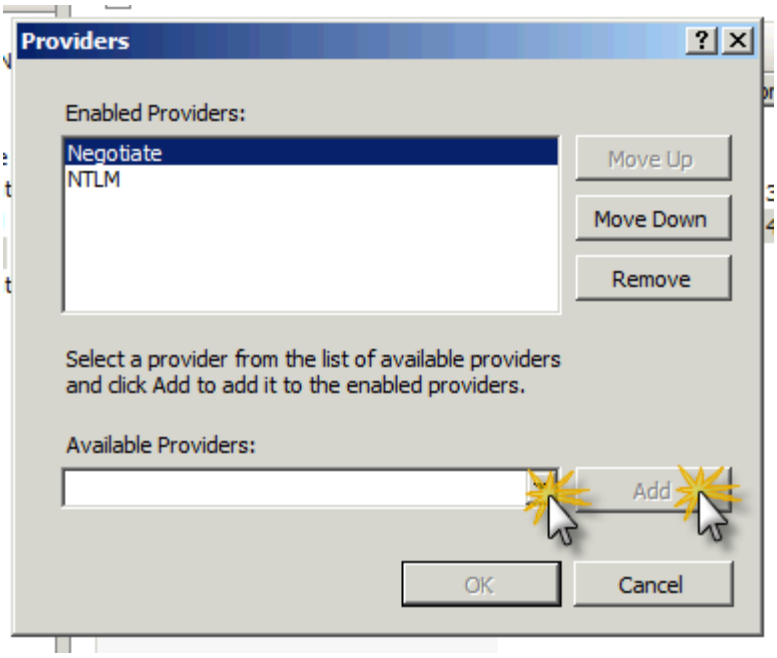
3. Ensure Windows Authentication is Enabled; right-click and select Enable if otherwise.



For Windows 2008 R2, whilst Windows Authentication is still selected select “Providers” and ensure that “Negotiate” and “NTLM” are listed.



If one is missing click “Available Providers” select the provider and click Add



Ensure that they are listed in this Order:-

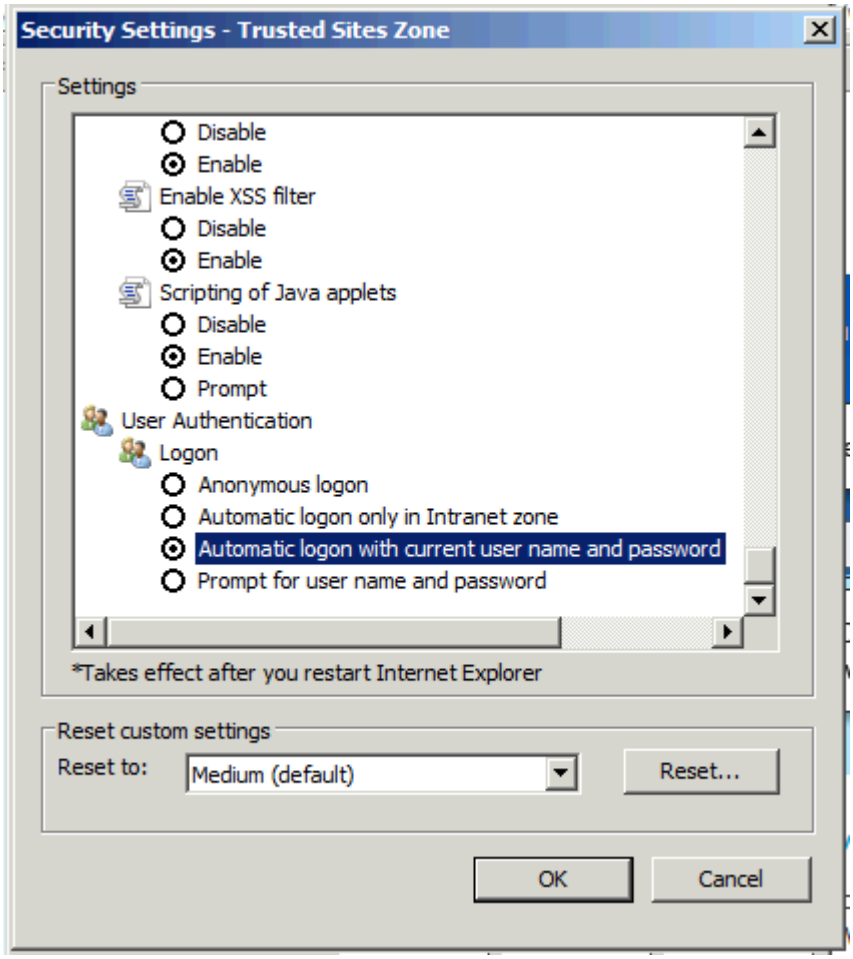
1. Negotiate
2. NTLM

If you have installed the “IIS Management Scripts and Tools” role in IIS, an alternative for setting the UI as shown in the above two screenshots, open a CMD prompt and execute the following commands (no quotes); if your website is other than ‘Default Web Site’, make the substitution prior to running each command:

A) “*C:\Windows\System32\inetsrv\appcmd.exe set config "Default Web Site/AutodeskDM/Services" -section:system.webServer/security/authentication/windowsAuthentication /+"providers.[value='Negotiate']" /commit:apphost*”

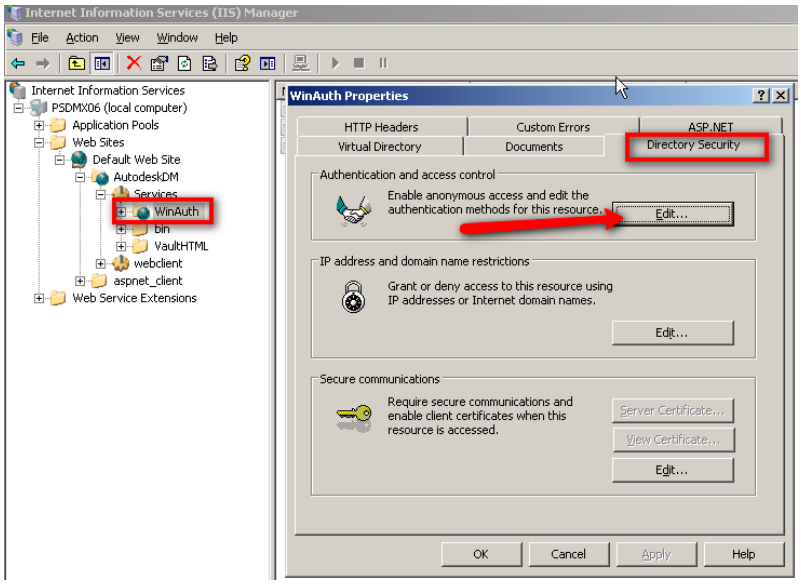
B) "*C:\Windows\System32\inetsrv\appcmd.exe set config "Default Web Site/AutodeskDM/Services" -section:system.webServer/security/authentication/windowsAuthentication /+"providers.[value='NTLM']" /commit:apphost*"

In Internet Explorer, set web browser security settings to automatic logon with current user name and password.

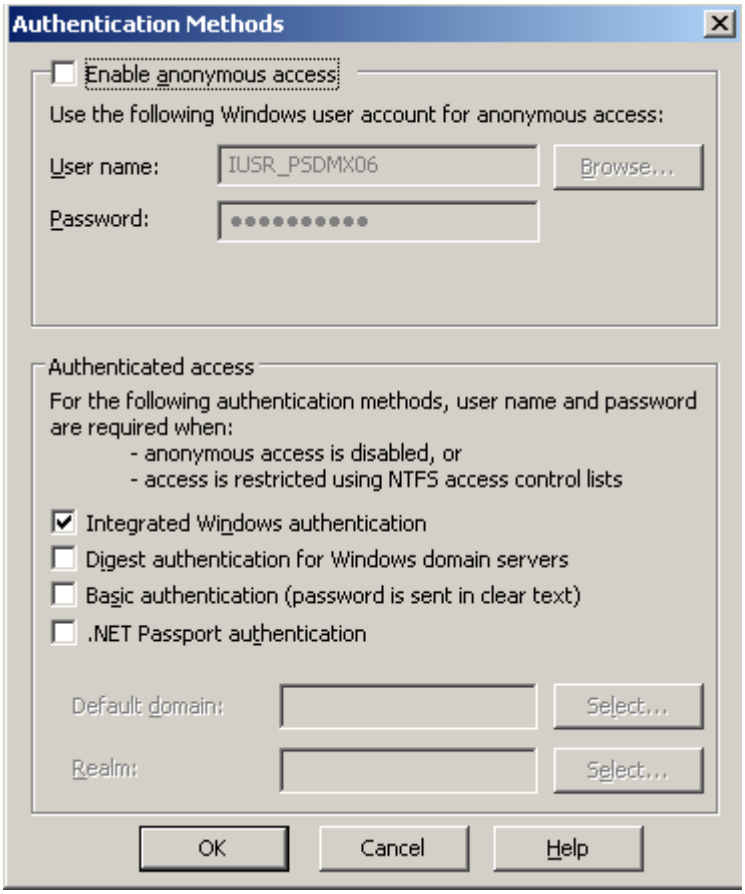


Windows Server 2003 (IIS6)

1. **Right-click** on the **WinAuth** folder under AutodeskDM\Services inside of IIS and select **Properties**. Choose the **Directory Security** tab and click **Edit** under **Authentication and Access Control**.



2. Ensure that only **Integrated Windows Authentication** is enabled.



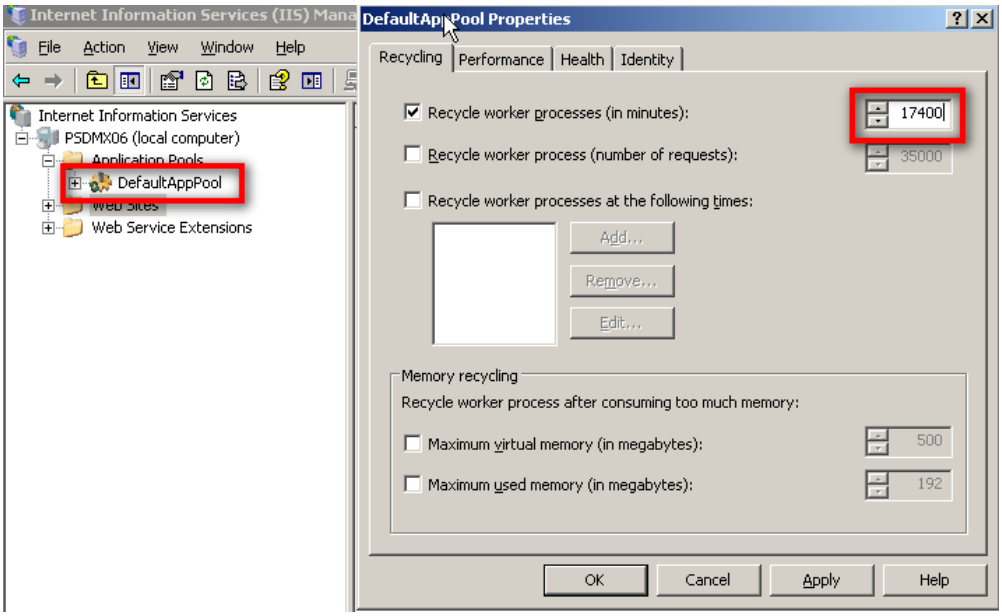
3. Using **Notepad**, **Open** file C:\Program Files\Autodesk\ADMS Professional 2013\Server\Web\Services\WinAuth**web.config**

4. Change <identity impersonate="true"/> to <identity impersonate="false"/>

5. Save the file, then Close notepad.

6. Select the Application pool used by the AutodeskDM website, **Right-Click** and select

Properties.



7. Increase the time the worker process will recycle (Suggested value of 17400).

8. **Stop IIS . [using command iiisreset /stop]**

9. Delete the folder: ***C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\autodeskdm_services***

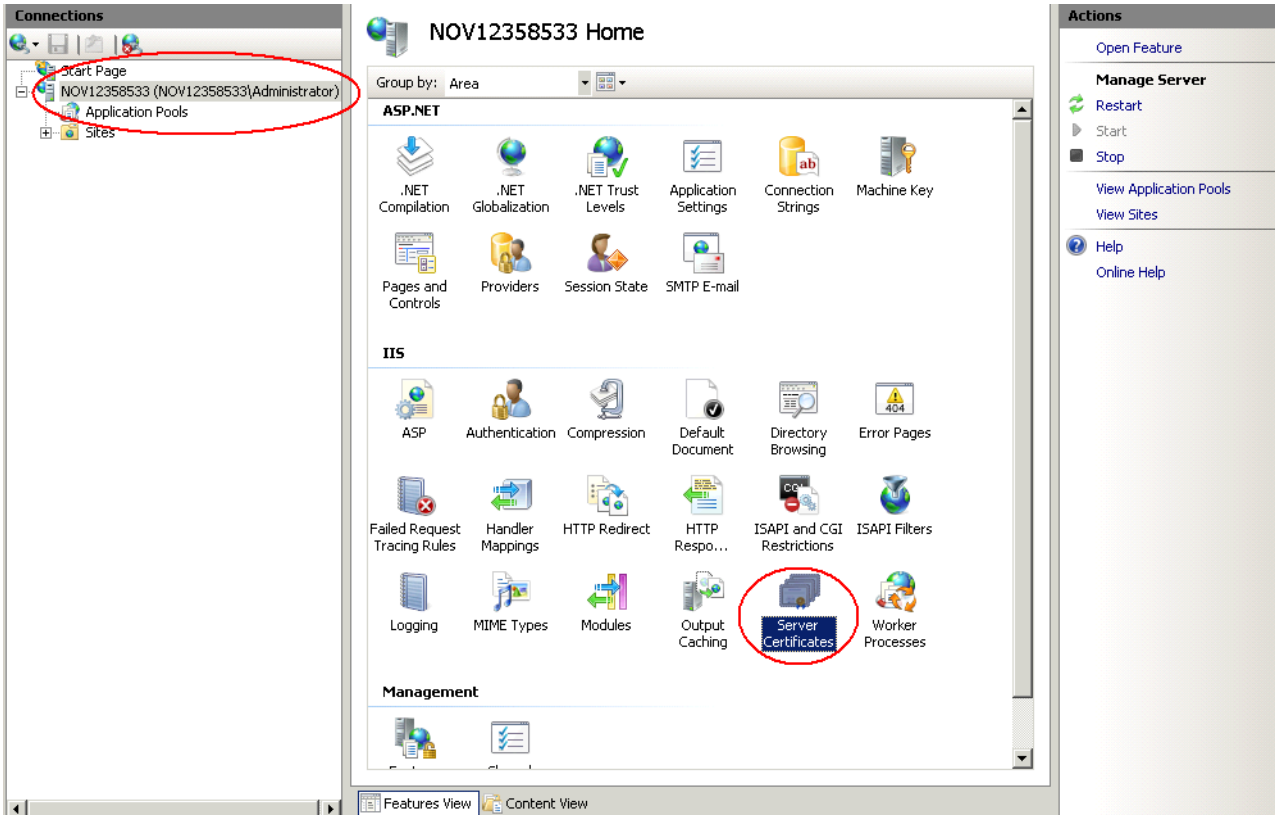
10. **Starts IIS. [using command iiisreset /start]**

Configure IIS 7.0 with an SSL Certificate.

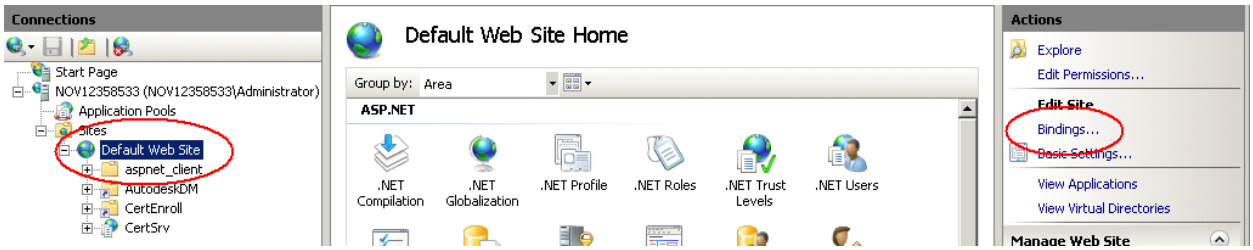
Configure the Server.

NOTE: The following procedure uses the Internet Information Services (IIS) Manager to configure IIS7 to require SSL for access.

1. Log into the computer hosting the Vault Server as a local or domain administrator.
2. From the Start Menu, select **Control Panel**.
3. Double-click the **Administrative Tools**, then double click the **Internet Information Services (IIS) Manager**.
4. Select the IIS server listed on the left hand pane, and then double-click **Server Certificates**.



5.
6. If you already have a certificate from a Certificate Authority, you can **Import** your certificate by using the **Actions** pane on the right hand side of the **Server Certificates** window. You can also create a **Self-Signed Certificate** from the **Actions** pane.
   NOTE: The remainder of this document outlines using a Self-Signed Certificate named **AutodeskDM**.
7. Select **Create Self-Signed Certificate**. Name the certificate **AutodeskDM**, click **OK.**
8. Expand the **Sites** tree and select the website that is hosting the AutodesDM virtual Directory. In the image below, the website is **Default Web Site.** Select **Default Web Site** and click **Bindings** from the **Actions** pane.



9. Click **Add** and change the type to **https** and change the SSL Certificate to **AutodeskDM** (or your imported certificate.) Click **OK**
10. If you wish to restrict all non SSL vault communication, click the **http** binding and select **remove**.
11. Close the **Internet Information Services (IIS) Manager**.

Reconfigure IIS Worker Process and Application Pool

IIS 6

1. Open the Active Directory Users and Computers and select an Organizational Unit (OU) to create the account in.
2. Create an account named **AutodeskID**. Set the password to match your domain password policy
3. Make the **AutodeskID** account a member of the **IIS_WPG** local group on DMMachine.
4. Give AutodeskID account Full Control permissions to the **%SystemRoot%\Temp** directory on DMMachine.
5. Give the AutodeskID account Full Control permissions to the **\\FSMachine\VaultData** remote file store directory.
6. Open Internet Information Services (IIS) Manager and create a new Application Pool named **AutodeskAppPL**.
7. Open the properties of the AutodeskAppPL Application Pool and go to the **Identity** tab.
8. Add the domain account AutodeskID, set the password and apply the changes.
9. Expand the Default Web Site and navigate to the AutodeskDM\Services virtual directory.
10. Right-click on the Services directory and go to the **Directory** tab.
11. Change the Application Pool pull-down to the newly created **AutodeskAppPL** Application Pool.
12. Apply the changes and close the properties of the Default Web site.
13. Close the IIS Manager.
14. Open a Command prompt and type **IISRESET**.
15. Add new files to the vault and verify that the properties are able to be indexed.

IIS 7

1. Open the Active Directory Users and Computers and select an Organizational Unit (OU) to create the account in.
2. Create an account named **AutodeskID**. Set the password to match your domain password policy
3. Make the **AutodeskID** account a member of the **IIS_WPG** local group on DMMachine.
4. Give AutodeskID account Full Control permissions to the **%SystemRoot%\Temp** directory on DMMachine.
5. Give the AutodeskID account Full Control permissions to the **\\FSMachine\VaultData** remote file store directory.
6. Right click on the Application Pools and select Add Application Pool.
7. In the Add Application Pool dialog, name the application pool **AutodeskAppPL** and keep the other options at their default.
8. In the Applications Pool listing, find your newly created application pool and right click on it.
9. Select the Advanced Settings.
10. Under Process Model, Select Identity and change the Identity to use the Domain account (AutodeskID) that you created earlier.
11. Expand the Default Web Site and navigate to the AutodeskDM\Services virtual directory.
12. Right-click on the Services directory and select Manage Application -> Advacned Settings.
16. Change the Application Pool to the newly created **AutodeskAppPL** Application Pool.
17. Apply the changes and close the properties of the Default Web site.

18. Close the IIS Manager.
19. Open a Command prompt and type **IISRESET**.
13. Add new files to the vault and verify that the properties are able to be indexed

SQL

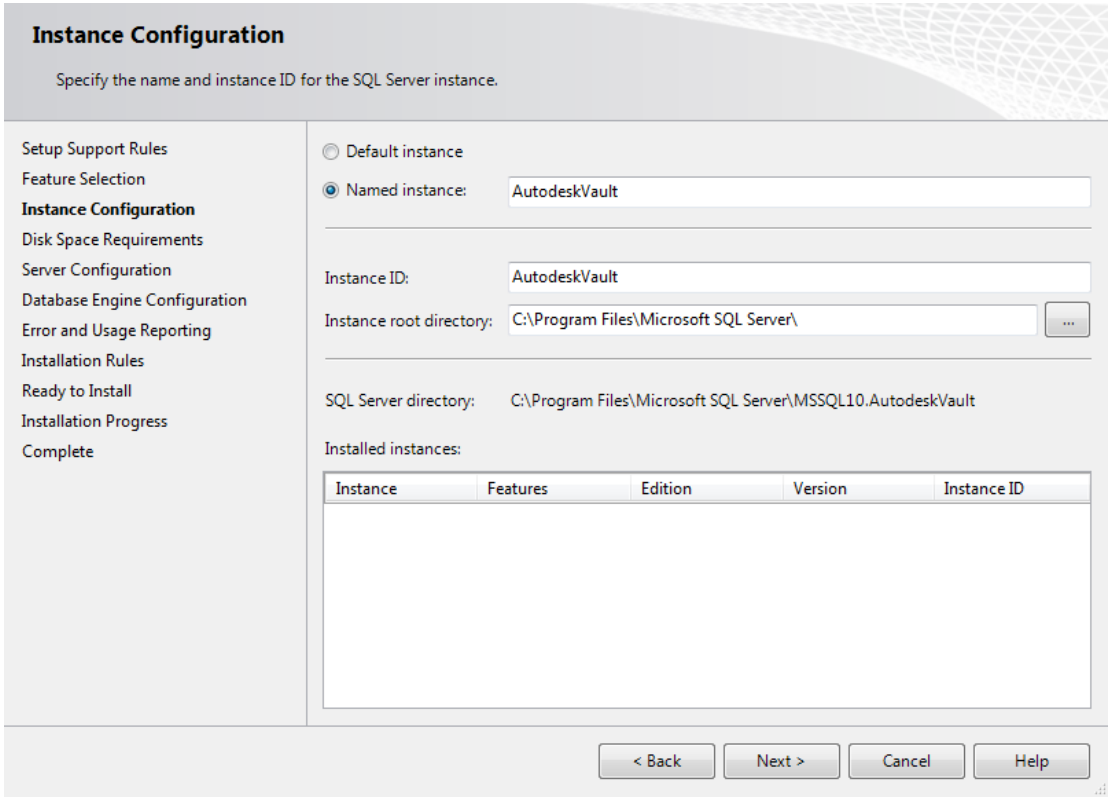
Installing Microsoft SQL Server prior to Autodesk Vault Server 2013

Vault Server 2013 will install Microsoft SQL 2008 SP2 x86 Express Edition (Build Number 10.0.4000.0) if it is unable to find an existing SQL instance named **AUTODESKVAULT**. If you plan on running a full SQL version with Vault Server 2013, it can be installed before or after the installation of Vault Server 2013.

Note: This installation process may require the server to reboot multiple times. Please be sure you are able to perform the necessary reboots. Also, if you use a custom password for the SQL SA account, you will need to specify this password during the installation of the Autodesk Vault Server. Please see the Customizing your Autodesk Vault Server 2013 Installation section in this document.

Microsoft SQL 2008:

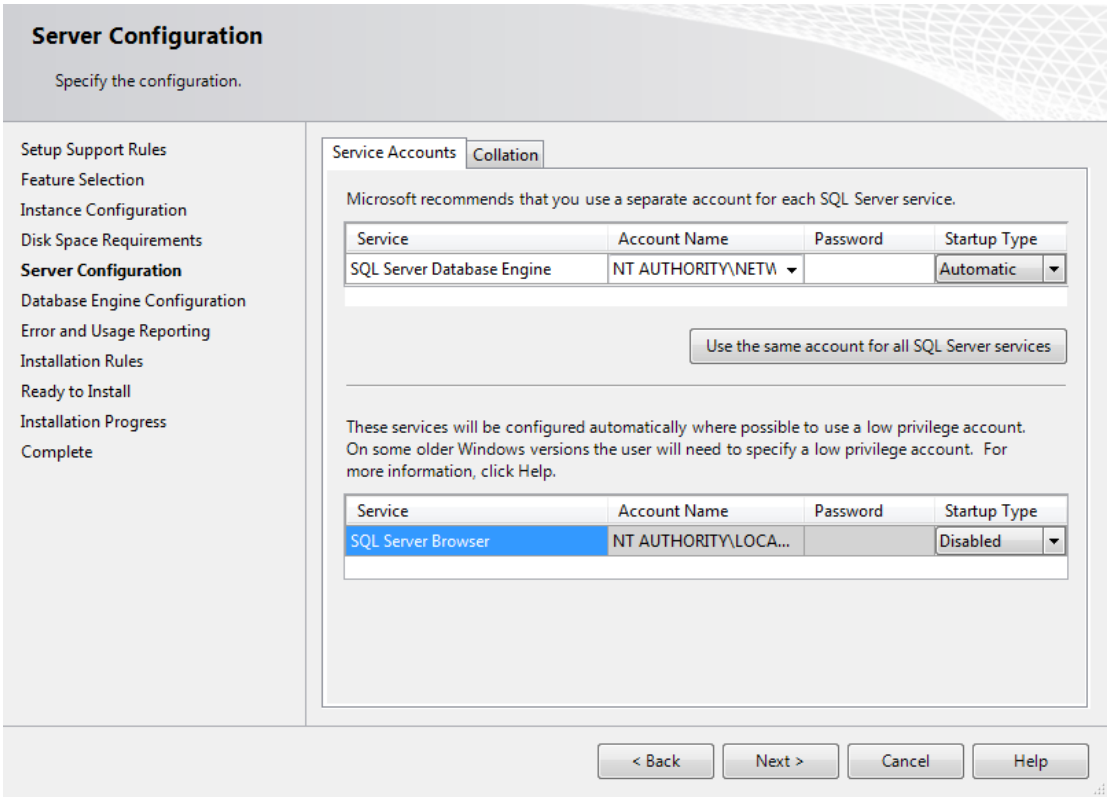
1. Start the installation process for Microsoft SQL 2008 Server by selecting **New SQL Server stand-alone installation or add features to an existing installation** from the installation menu.
2. The installation process installs any necessary prerequisites and begins running the pre-installation checks. Note any errors and take the necessary corrective actions before continuing.
3. In the Feature Selection window, select **Database Engine Services**. You can also specify the installation location at this point.
4. In the Instance Configuration window, select Named instance and enter the name as **AutodeskVault**.



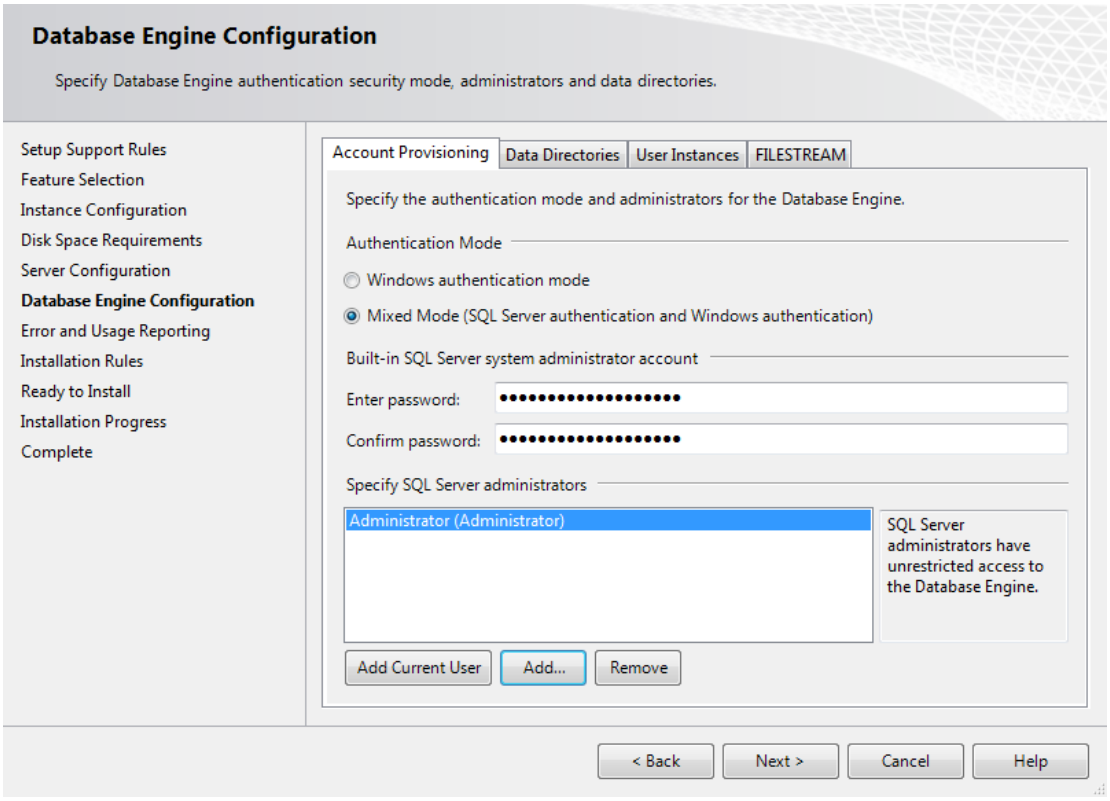
Note: If you install SQL without using this instance name, the Autodesk Vault Server installation will create its own instance of SQL Server called **AutodeskVault** using

Microsoft SQL Express 2008 SP2. It will **NOT** recognize any SQL instance not named **AutodeskVault**.

5. In the Server Configuration window, select the Service Accounts tab.
    a. Specify the **NT AUTHORITY\NETWORK SERVICE** account for the SQL Server Database Engine. The local system account is also acceptable to use. If you plan on performing backups and restores to remote locations specify a Domain User account. Set the Startup Type to Automatic.



6. In the Database Engine Configuration window, select the Account Provisioning tab.
    a. Select **Mixed Mode** authentication and set the SA password. The default password used during a default installation for the SA password is **AutodeskVault@26200**.
    b. Add the local administrator account (or desired account) as a SQL Server administrator. **Only Windows users entered in this dialog will have full rights when logging into the SQL server. All other Windows logins will be treated as a guest account.**



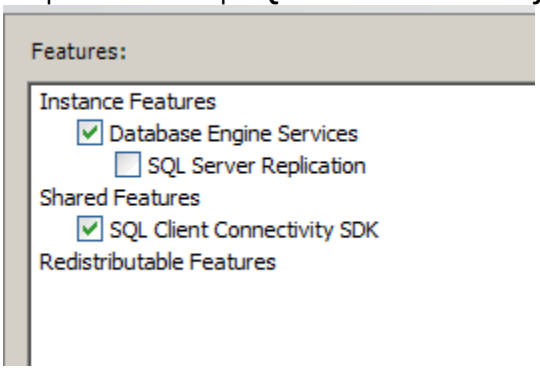
Note: If you use a different SA password, you will need to use the **use my SA Credentials** option in the Customizing your Autodesk Vault Server 2013 Installation section in this document.

7. Verify the installation options chosen and **Install**. Once the installer has finished, it can be closed.
8. Download and install SQL 2008 SP2 and applicable hot fixes from Microsoft's web site if needed. The database engine version will be 10.0.**4**### once SP 2 has been successfully installed. In addition, SQL 2008 SP3 can be applied.

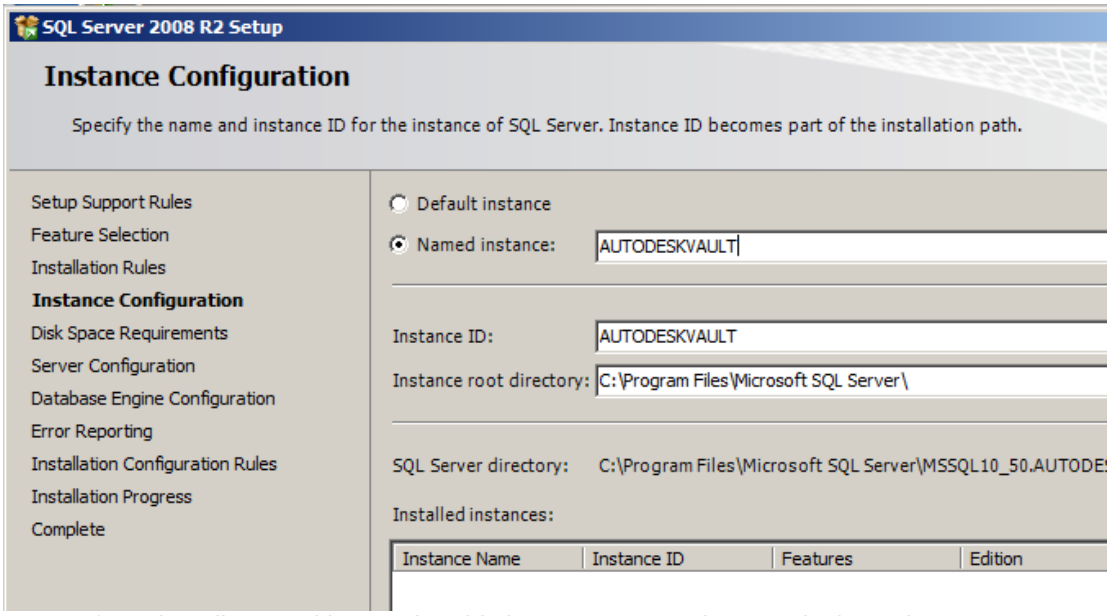
Microsoft SQL 2008 R2 (Express Edition)

1. Start the installation process for Microsoft SQL 2008 R2 Server Express Edition by selecting **New installation or add features to an exisiting installation** from the **Installation** menu.
2. The installation process installs any necessary prerequisites and begins running the pre-installation checks. Note any errors and take the necessary corrective actions before continuing.
3. Select the **Database Engine Services** and any additional roles required by the environment. **SQL Server Replication** is required in a Connected Workgroup environment and not supported with the Express edition of SQL, so it is not necessary to

keep it ticked. Keep **SQL Client Connectivity SDK** ticked**.**

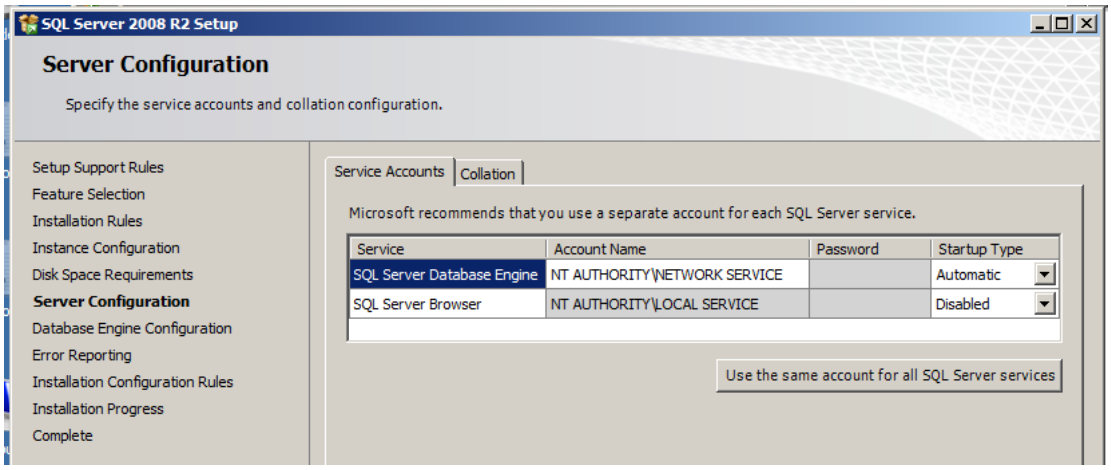


4. In the Instance Configuration window, select Named instance and enter the name as **AUTODESKVAULT**.

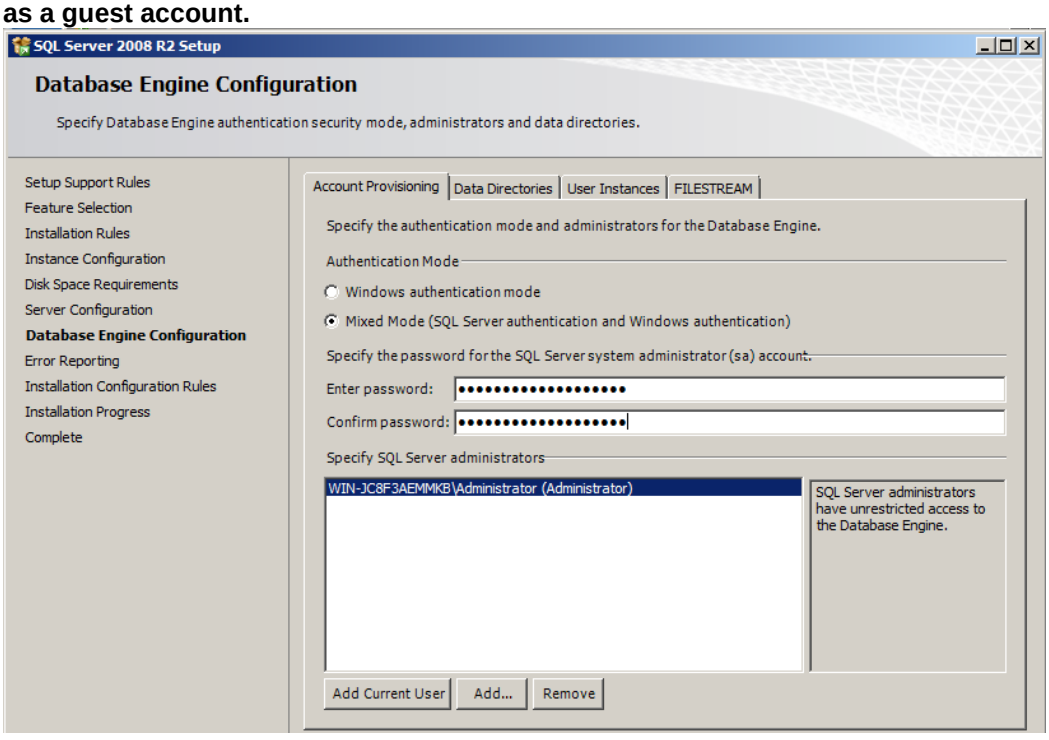


Note: If you install SQL without using this instance name, the Autodesk Vault Server installation will create its own instance of SQL Server called **AUTODESKVAULT** using the 32 bit version of Microsoft SQL Express 2008 SP2. It will **NOT** recognize any other SQL Instance name.

5. In the Server Configuration window, select the Service Accounts tab.
    a. Specify the **NT AUTHORITY\NETWORK SERVICE** account for the SQL Server Database Engine. The local system account is also acceptable to use. If you plan on performing backups and restores to remote locations specify a Domain User account. Set the Startup Type to Automatic.



6. In the Database Engine Configuration window, select the Account Provisioning tab.
    a. Select **Mixed Mode** authentication and set the SA password. The default password used during a default installation for the SA password is **AutodeskVault@26200**.
    b. Add the local administrator account (or desired account) as a SQL Server administrator. **Only Windows users entered in this dialog will have full rights when logging into the SQL server. All other Windows logins will be treated as a guest account.**

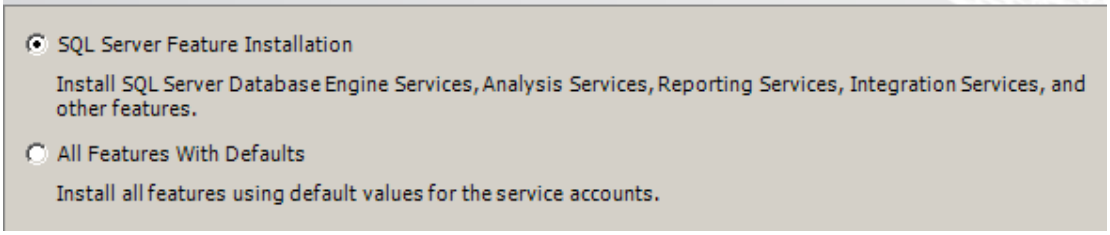


Note: If you use a different SA password, you will need to use the **use my SA Credentials** option in the Customizing your Autodesk Vault Server 2013 Installation section in this document.

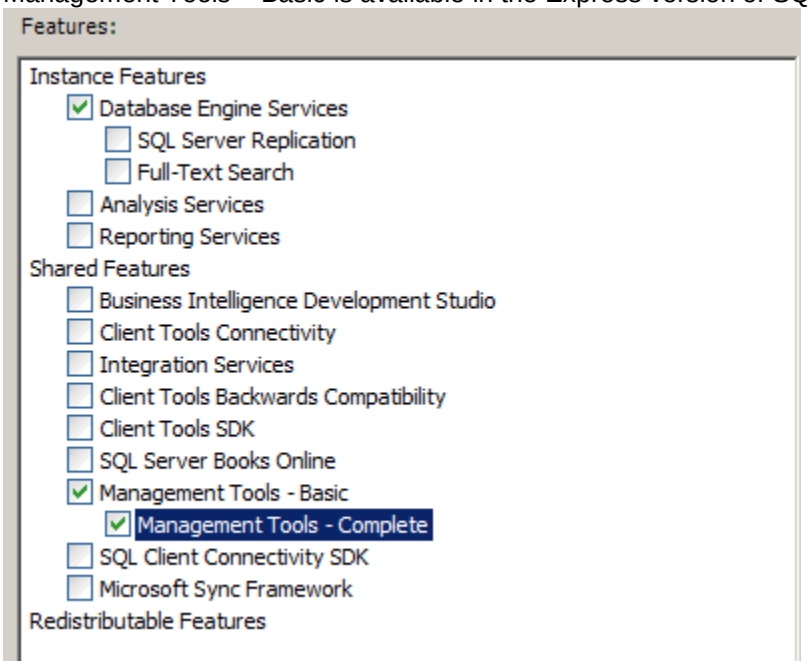
7. Verify the installation options chosen and **Install**. Once the installer has finished, it can be closed.
8. Download and install SQL 2008 R2 SP1 from Microsoft's web site if needed.

Microsoft SQL 2008 R2 (Standard or Enterprise)

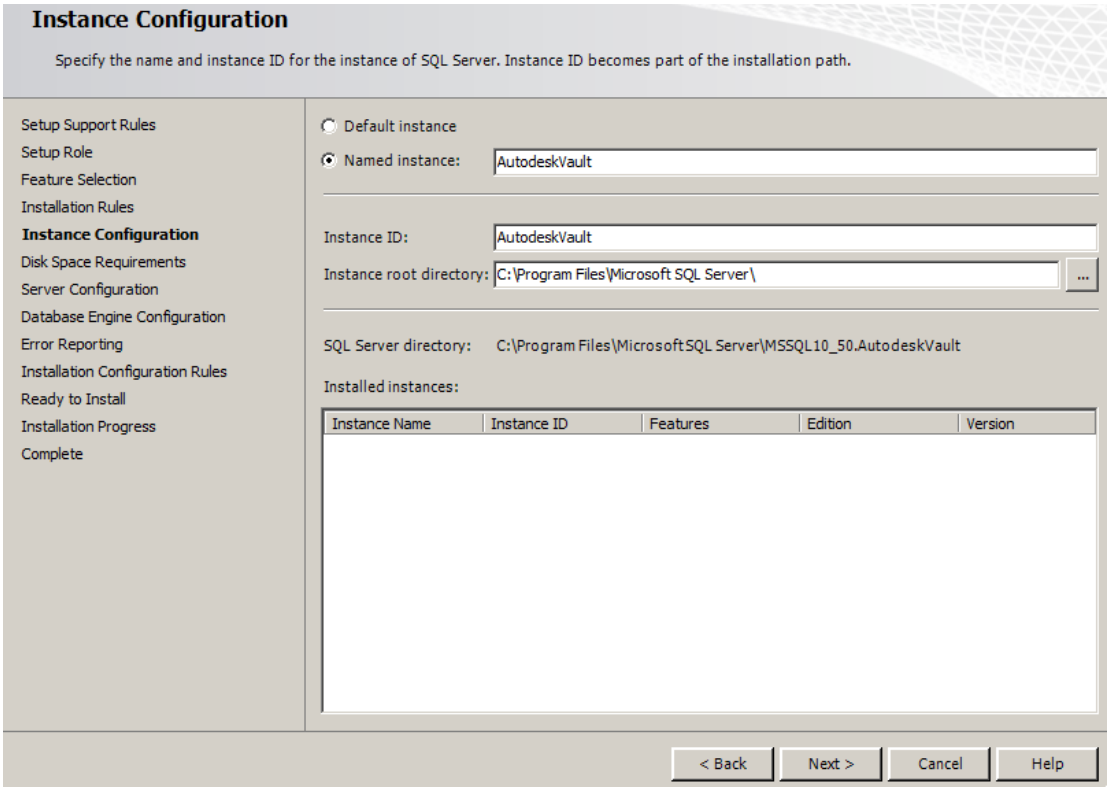
1. Start the installation process for Microsoft SQL 2008 R2 Server by selecting **New SQL Server stand-alone installation or add features to an existing installation** from the installation menu.
2. The installation process installs any necessary prerequisites and begins running the pre-installation checks. Note any errors and take the necessary corrective actions before continuing.
3. During Setup Role, select **SQL Server Feature Installation**



4. Select the **Database Engine Services** and any additional roles required by the environment. **SQL Server Replication** is required in a Connected Workgroup environment and the **Management Tools** is recommended. Please note that only Management Tools – Basic is available in the Express version of SQL.

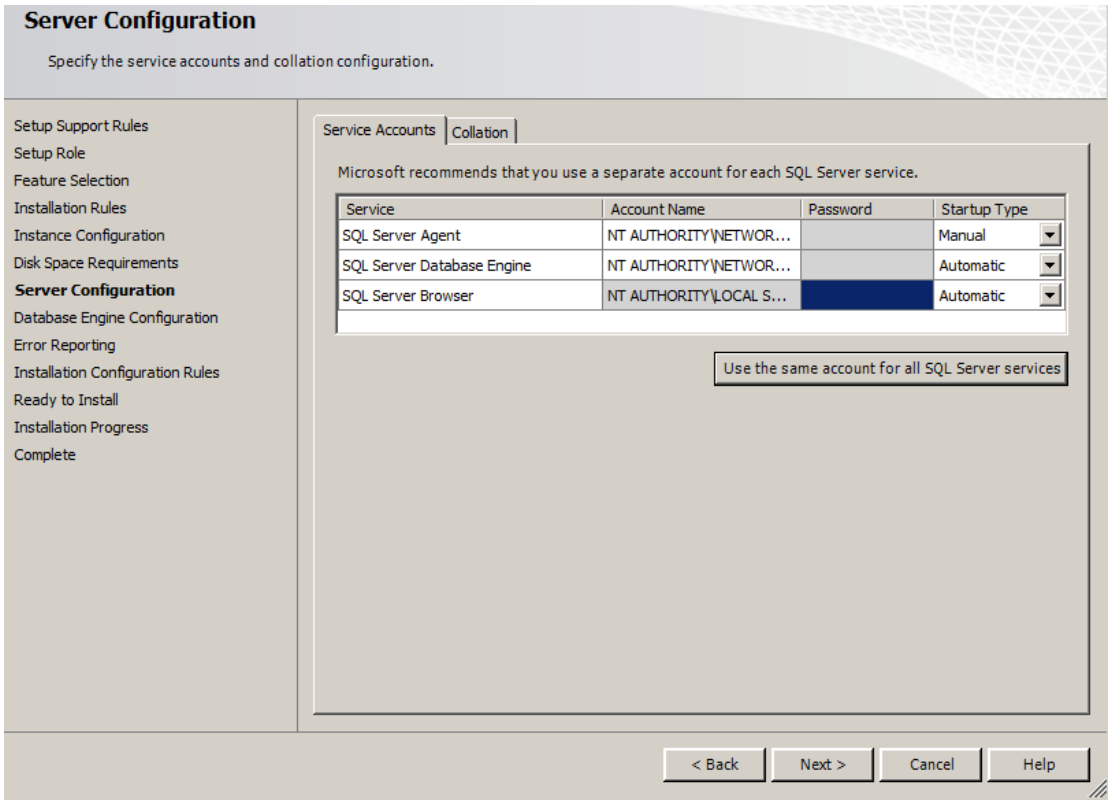


5. In the Instance Configuration window, select Named instance and enter the name as **AUTODESKVAULT**.

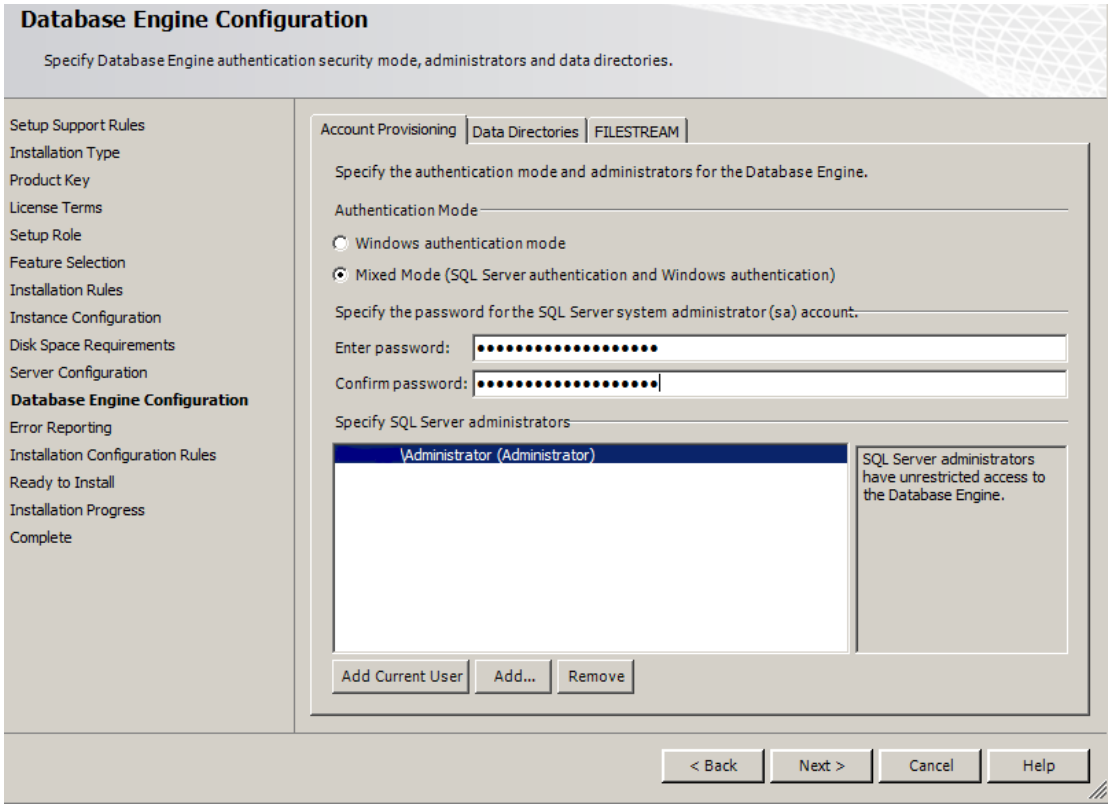


Note: If you install SQL without using this instance name, the Autodesk Vault Server installation will create its own instance of SQL Server called **AUTODESKVAULT** using 32-bit Microsoft SQL Express 2008 SP2. It will **NOT** recognize an SQL instance with a different name.

6. In the Server Configuration window, select the Service Accounts tab.
    a. Specify the **NT AUTHORITY\NETWORK SERVICE** account for the SQL Server Database Engine. The local system account is also acceptable to use. If you plan on performing backups and restores to remote locations specify a Domain User account. Set the Startup Type to Automatic.



7. In the Database Engine Configuration window, select the Account Provisioning tab.
    a. Select **Mixed Mode** authentication and set the SA password. The default password used during a default installation for the SA password is **AutodeskVault@26200**.
    b. Add the local administrator account (or desired account) as a SQL Server administrator. **Only Windows users entered in this dialog will have full rights when logging into the SQL server. All other Windows logins will be treated as a guest account.**



Note: If you use a different SA password, you will need to use the **use my SA Credentials** option in the Customizing your Autodesk Vault Server 2013 Installation section in this document.

8. Verify the installation options chosen and **Install**. Once the installer has finished, it can be closed.
9. Download and install SQL 2008 R2 SP1 from Microsoft's web site if needed.

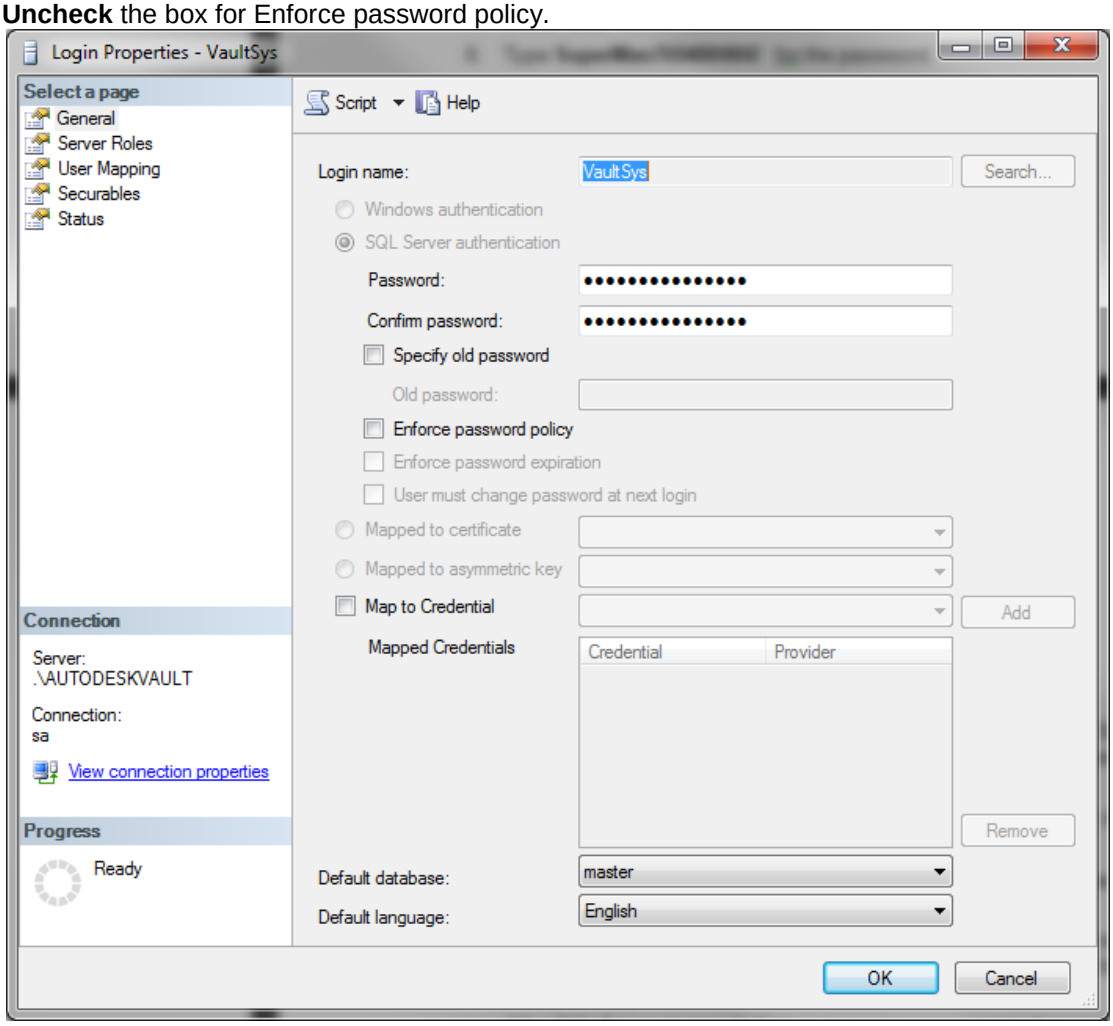
Reconfiguring SQL Logins

If you don't have a domain password policy, you can skip this section. If your domain has a password policy configured, you must use a password that complies with the policy. After the installation is complete, reset the sa password to **AutodeskVault@26200** and uncheck the **Enforce password policy** check box. It is also necessary to create two SQL login accounts named **VaultSys** and **ADMS-<*COMPUTERNAME*>**.

To create the VaultSys account:

1. Open the **Microsoft SQL Server Management Studio**.
2. Expand the **Security -> Logins** folder.
3. Right-click on the Logins folder and select **New Login**.
4. Type **VaultSys** for the login name.
5. Select **SQL Server Authentication**.
6. Type **SuperMan769400006!** as the password.

7. **Uncheck** the box for Enforce password policy.

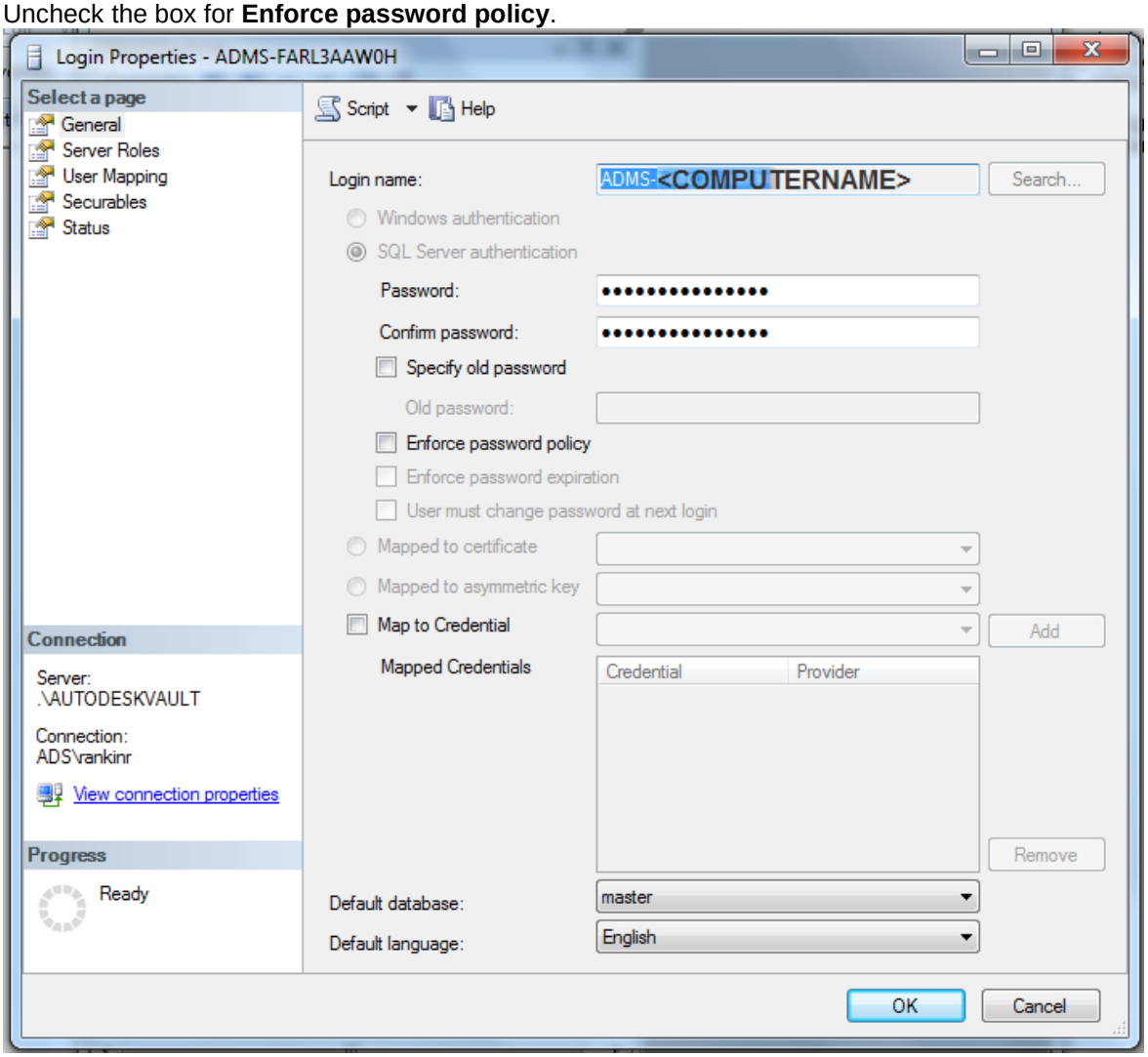


8. Select the **Server Roles** page.
9. Check the boxes next to the following roles:
   - **dbcreator**
   - **processadmin**
   - **setupadmin**
10. Click **OK** to create the account.

To create the ADMS-<COMPUTERNAME> account.

11. Open the **Microsoft SQL Server Management Studio**.
12. Expand the **Security -> Logins** folder.
13. Right-click on the Logins folder and select **New Login**.
14. Type **ADMS-<COMPUTERNAME>** for the login name.(Where **<COMPUTERNAME>** indicates the NT Computer name) Example, if the computer name is MAINSERVER then the login name would = **ADMS-MAINSERVER**.
15. Select **SQL Server Authentication**.
16. Type **WeakerMan769400006!** as the password.

17. Uncheck the box for **Enforce password policy**.



18. Select the **Server Roles** page.
    - Ensure that only **public** is selected.
19. Click **OK** to create the account.

Installing SQL Server on a Domain Controller

Referencing the following Microsoft Article:

http://msdn.microsoft.com/en-us/library/ms143506.aspx:

Installing SQL Server on a Domain Controller

For security reasons, Microsoft recommends that you do not install SQL Server 2008 / 2008 R2 on a domain controller. SQL Server Setup will not block installation on a computer that is a domain controller, but the following limitations apply:

- On Windows Server 2003, SQL Server services can run under a domain account or a local system account.
- You cannot run SQL Server services on a domain controller under a local service account or a network service account.
- After SQL Server is installed on a computer, you cannot change the computer from a domain member to a domain controller. You must uninstall SQL Server before you change the host computer to a domain controller.
- After SQL Server is installed on a computer, you cannot change the computer from a domain controller to a domain member. You must uninstall SQL Server before you change the host computer to a domain member.
- SQL Server failover cluster instances are not supported where cluster nodes are domain controllers.
- SQL Server Setup cannot create security groups or provision SQL Server service accounts on a read-only domain controller. In this scenario, Setup will fail.

Upgrading The AUTODESKVAULT SQL instance.

When upgrading to a higher version of Microsoft SQL Server, it is assumed the appropriate IT and engineering staff required, are available to allow access to the server and client systems, as well as to execute periodic system restarts. It is also recommended that the process be verified in a test environment prior to performing the upgrade on the production environment. Client side systems are needed to verify that the upgrade has been completed successfully.

The server upgrade can be performed at any time after Autodesk Vault Server has been installed.

During the upgrade, the SQL server instance and the Autodesk Vault Server Services are shut down. Anyone logged into the vault at the time is automatically disconnected. Make sure all users are logged out of the Autodesk Vault Server. The upgrade will not affect the state of checked out files, nor will it modify the database structure, state of the files, or parent child relationships.

Before upgrading SQL server, perform a backup from the Autodesk Vault Server Console application. For more information on backing up data, see the Autodesk Vault Server console Help.

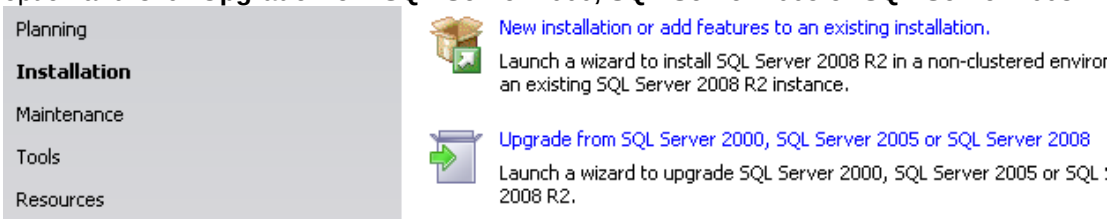
****NOTE** Before performing any of the following steps, first identify the Version, Edition and bitness of the SQL Server Database Engine that is currently installed. See "How to determine the version and edition of SQL Server and its components" (MS Article ID 321185).**

If no AUTODESKVAULT SQL instance is installed, Autodesk Vault Server 2013 will install the 32 bit version of Microsoft SQL Server 2008 (SP2) Express Edition - 10.0.4000.0. This is true for both 32 bit and 64 bit operating systems. If installing on a 64 bit operating system and a 64 bit version of SQL is required, it will need to be installed before installing Vault Server 2013.

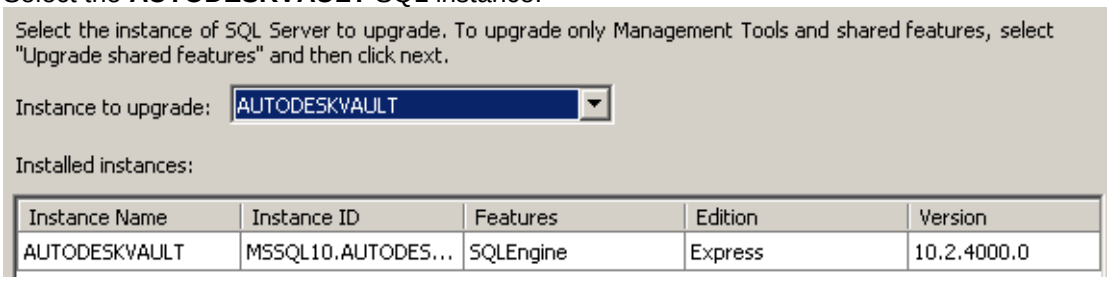
Microsoft does not support cross-platform, in place, upgrades to **or** from 64 bit SQL. See the Microsoft "Version and Edition Upgrades" website for more information.

Upgrading MS SQL Express 2008 SP2 to SQL Express 2008 R2

1. Launch **Setup** from the SQL Express 2008 R2 installation media. Select the **Installation** option and Click **Upgrade from SQL Server 2000, SQL Server 2005 or SQL Server 2008**



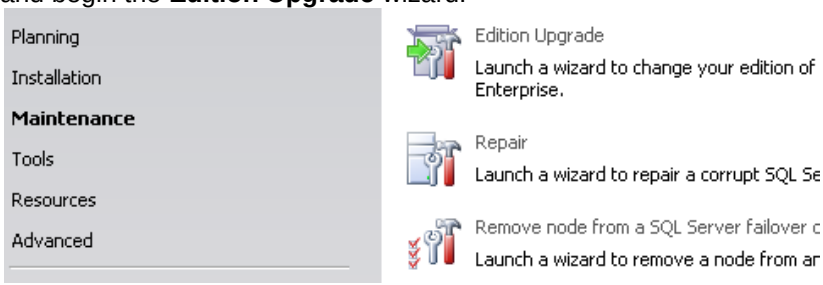
2. Select the **AUTODESKVAULT** SQL instance.



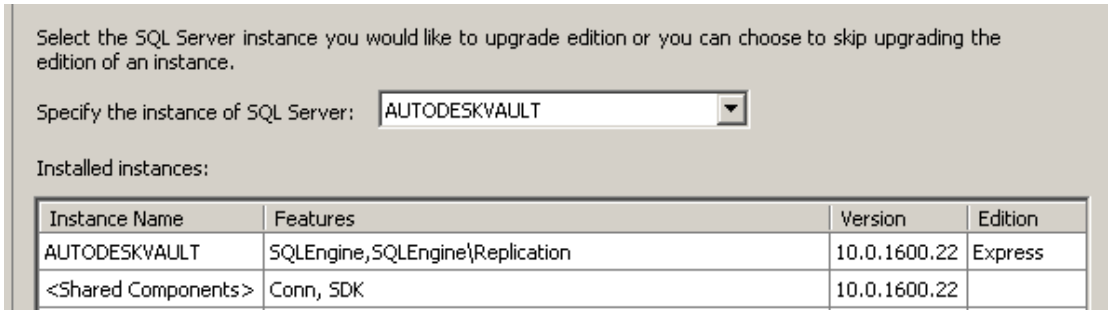
3. Upgrade the instance by completing the wizard.

Upgrading MS SQL Express 2008 SP2 to Full MS SQL 2008

4. Launch **Setup** from the Full SQL 2008 installation media. Select the **Maintenance** option and begin the **Edition Upgrade** wizard.



5. Verify version and or product key for Full SQL 2008 and proceed to the Select Instance window and choose the **AUTODESKVAULT** instance.

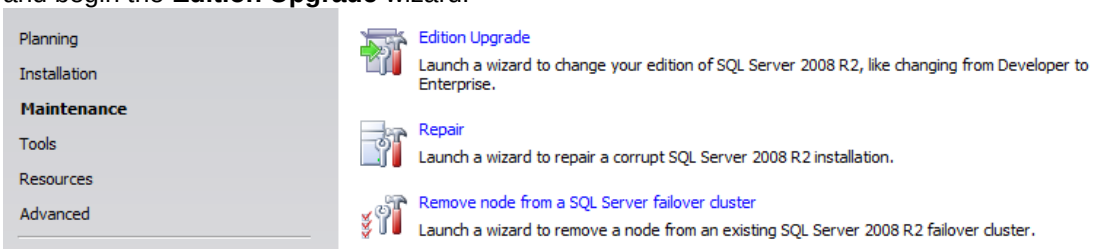


6. Upgrade the Instance. Once the instance has been upgraded, you can install the SQL Management Studio by returning to the "Installation" option and being the **New SQL Server stand-alone installation or add features to an existing installation** wizard.

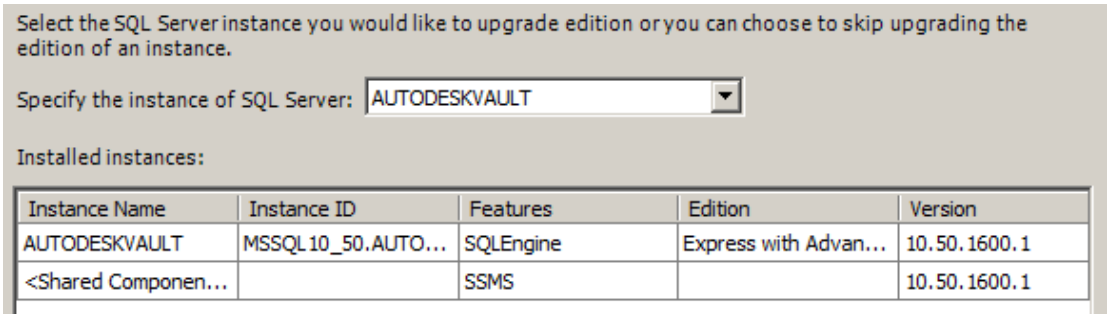
7. Download and apply SQL 2008 SP2 if needed.

Upgrading MS SQL Express 2008 R2 to Full MS SQL 2008 R2

1. Launch **Setup** from the Full SQL 2008 installation media. Select the **Maintenance** option and begin the **Edition Upgrade** wizard.



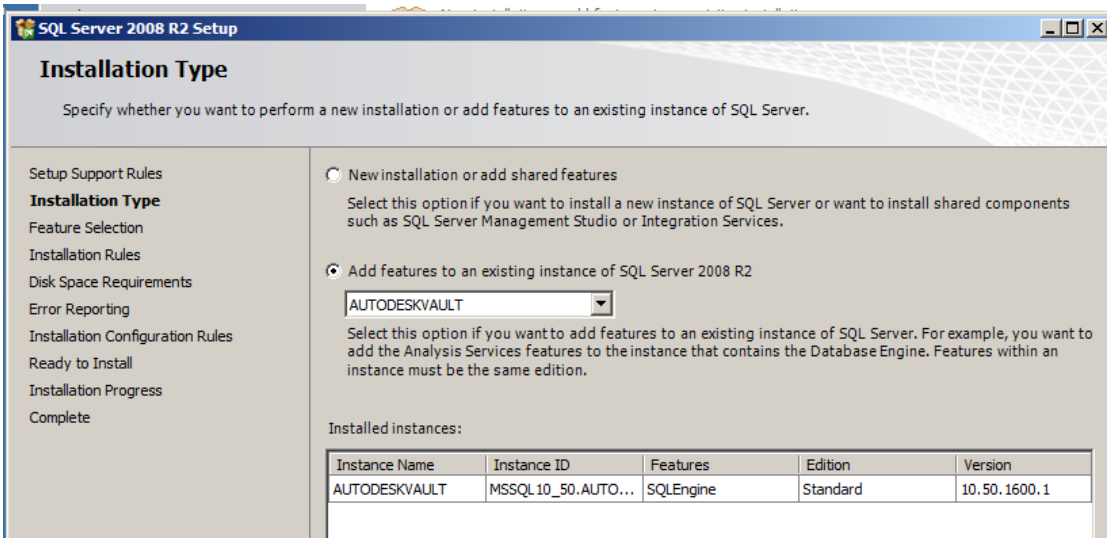
2. Verify version and or product key for Full SQL 2008 and proceed to the Select Instance window and choose the **AUTODESKVAULT** instance.



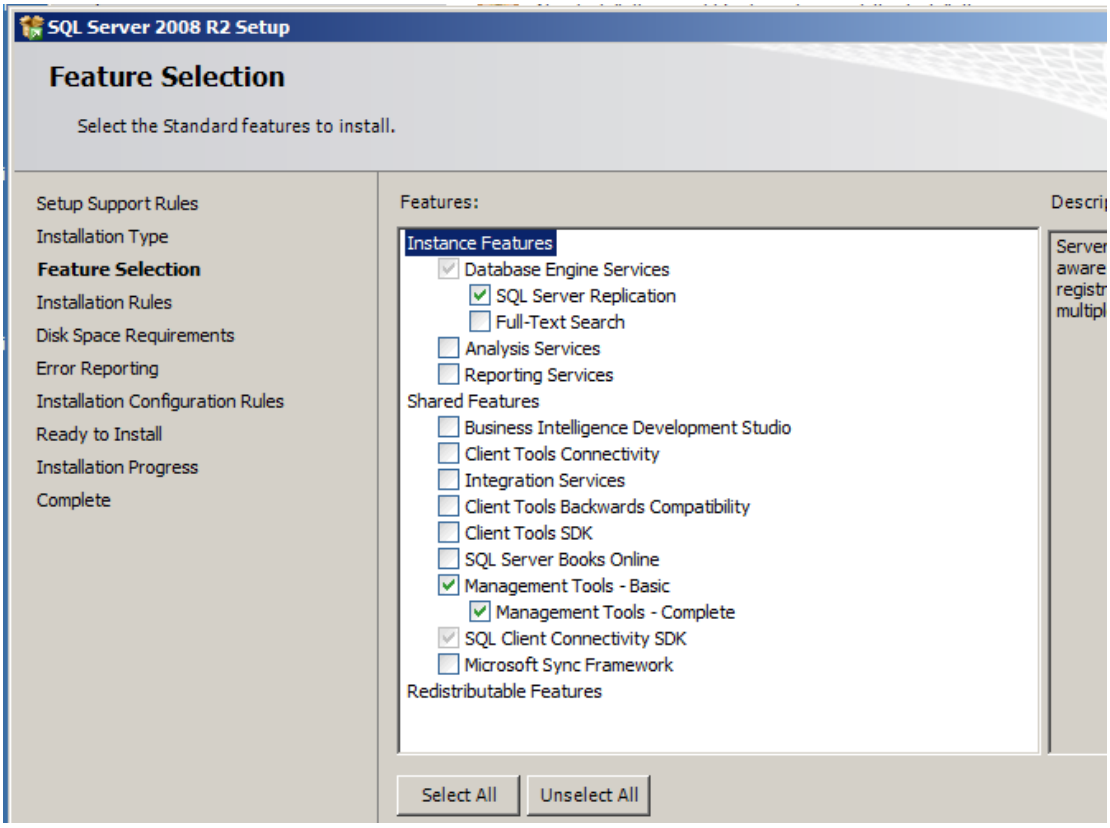
After Upgrading to SQL Standard or Enterprise.

If you intend to implement the more advance features of SQL supported by Autodesk Vault, such as Replication, you will then need to switch to the **Installation** page and click, **New installation or add new features to an existing installation.**

On the **Installation Type** page, ensure that **Add features to an existing instance of SQL Server 2008 R2** and the **AUTODESKVAULT** instance is selected.



On the **Feature Selection** page, ensure the features that you need are ticked.



In the above example, **SQL Server Replication** is needed to implement Connected Workgroups in Vault and **Management Tools – Complete** is recommended.

The SQL Server Agent needs to be set to run automatically on startup. Type **Services.msc** at a **Run** prompt. In the Services Console, locate **SQL Server Agent (AUTODESKVAULT)**, right click and select **Properties**, On the **General** tab, change the **Startup** type to **Automatic**, click **Apply.** Switch to the Log On tab, ensure that Network Service is selected, go back to General tab and click **Start**.

Assigning SQL a custom TCP/IP Port

This section outlines the steps to set SQL to a non-standard TCP/IP port.

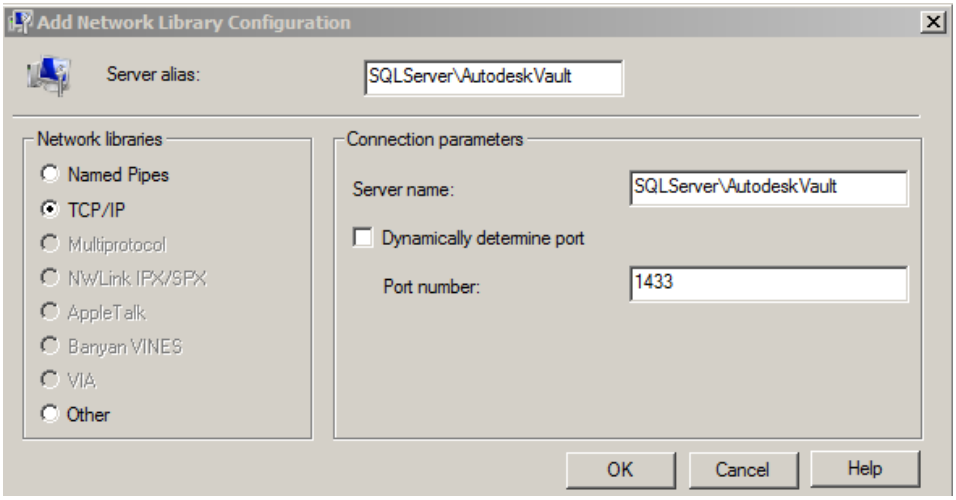
SQL Server 2008 (and R2)

1. Install full SQL Server 2008 as per the Advanced Configuration Guide.
2. On the server where SQL is installed, start the **SQL Server Configuration Manager**.
3. In the SQL Server Configuration Manager dialog, expand the **SQL Server Network Configuration** and select **Protocols for AUTODESKVAULT**.
4. In the right pane double-click on the **TCP\IP** protocol to open its properties.
5. In the TCP\IP Properties dialog, select the **Protocol** tab and change the Enabled property to **Yes**.
6. Select the **IP Addresses** tab.
7. Scroll down to the bottom of the dialog until you get to the **IPAll** section.
8. Change the TCP Port field to the port you desire.
9. Apply your changes and select **OK** to close the TCP\IP Properties dialog.

10. In the SQL Server Configuration Manager dialog, select the **SQL Server Services** section in the left pane.
11. Select **SQL Server (AutodeskVault)** in the right-pane, right-click on it and select **Restart**.

Autodesk Vault Server

1. Run C:\Windows\System32**cliconfig** from and the **SQL Server Client Network Utility**.
2. In the **SQL Server Client Network Utility** dialog, select the **Alias** tab.
3. In the **Alias** tab, select the **Add** button.
4. In the **Edit Network Library Configuration** dialog, select **TCP/IP** under Network Libraries.
5. In the **Server alias** box type the name of the server where SQL is installed along with the instance name.
6. **Uncheck** the **Dynamically** determine port and enter the port number you configured in step 8 above.



7. Click the **OK** button to apply the settings.
8. **Start** your Autodesk Vault Server **installation**.

SQL Maintenance Plans

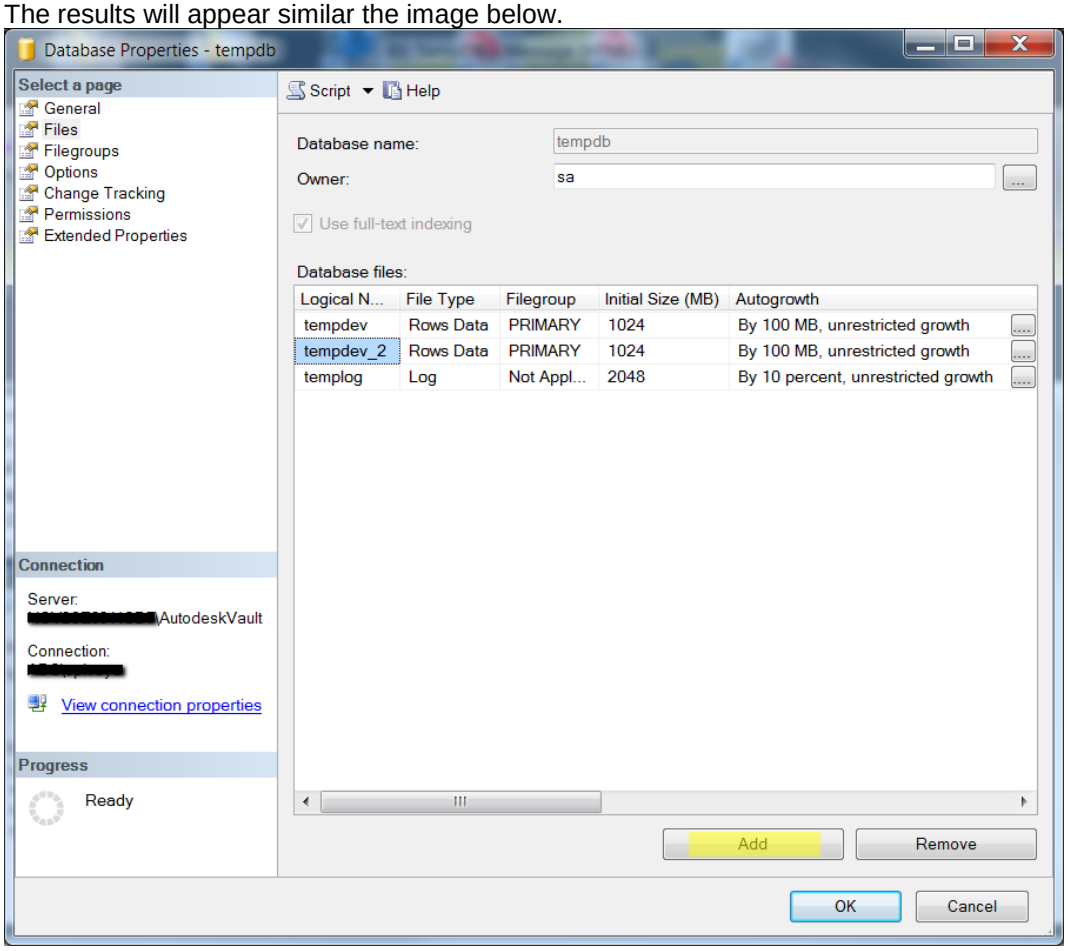
Maintenance plans can be used to schedule tasks required to make sure that the database performs well, such as keeping database and transaction log file sizes small and checking the database for inconsistencies.

The following steps are universal across all versions of SQL in use with Vault 2013 (Express and Full SQL). The complete list of supported database engines is located in the product readme file.

****Please note** that if you are running SQL Express and do not have the SQL Management Studio installed, the following steps can be completed through the command prompt through scripts under the section "Creating a Maintenance Script for Microsoft SQL Express", or you can install the SQL Management Studio for Express, available from Microsoft's web site.

1. Login to the SQL Management Studio.
2. Expand Databases, expand System Databases.
3. Right Click on **tempdb** and select **properties**.
4. Select the **Files** page.
5. If using a multi-core system, additional data files should be configured, using the guidelines below. If using a single-core system, skip to step **d** below.
    a. Data file totals should equal half of the available physical processing cores - up to a maximum of 8 data files. *(example; 8 physical cores would equal 4 total data files, tempdev, tempdev_2, tempdev_3, tempdev_4)*
    b. Click the **Add** button to add additional data files.
    c. Name the new file(s) tempdev_2, tempdev_3, … as needed.
    d. Set initial size of each data file to **1,024** MB. *If using a total of 8 datafiles, an initial size of **512** MB can be used.*
    e. Set Autogrowth to **100** MB, unrestricted growth for each data file.
    f. Set the LDF log file to combined data file total. *(example; if there are 2 data files total, the resulting LDF should be set to an initial size of 2048 MB)*

g. The results will appear similar the image below.



6. Under the **Options** page, set the Recovery model to **Simple** and the Compatibility level to **SQL Server 2008 (100)**.
7. Select **OK**.

Creating a SQL Maintenance Plan for Full SQL

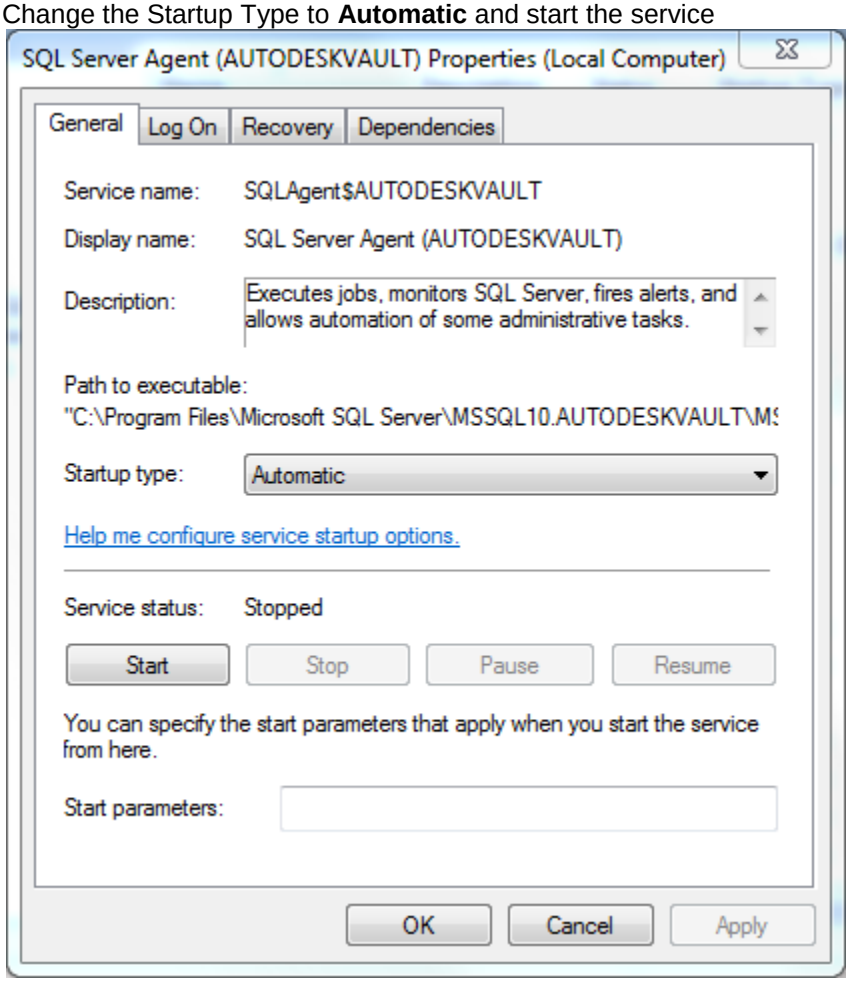
Maintenance plans can be used to schedule tasks required to make sure that the database performs well, such as keeping database and transaction log file size small and checking the database for inconsistencies.

NOTE: These settings are recommended by Autodesk and should be configured automatically for new installations. If migrated from an earlier release of Vault Server, these settings are not enforced as they may have been changed intentionally by the Administrator.

SQL Standard / Enterprise 2008 and 2008 R2

1. Verify that the vaults have been backed up with the Autodesk Vault Server Console before proceeding.
2. Make sure that all users are **logged out** of the vault server.
3. From the Control Panel, double-click Administrative Tools and then double-click the Services icon.
4. Locate the **SQL Server Agent (AUTODESKVAULT)** service.

5. Right-click on the **SQL Server Agent (AUTODESKVAULT)** and select **Properties**.
6. Change the Startup Type to **Automatic** and start the service



7. Open the Microsoft SQL Management Studio and connect to the **AutodeskVault** instance. Use <*ComputerName*>\AUTODESKVAULT as the server name and press **Connect**.
8. Right-click on the Vault database and select properties.
9. On the **Files** page set:-

   the Autogrowth value for all **<Vault>** databases to by 100MB, unrestricted growth

   the Initial Size value of all **<Vault>_log** files to 500MB

   the Autogrowth value for an **<Custom_Library>** files to 25MB

   the Autogrowth values for all **_log** files to **By 10 percent, unrestricted growth**

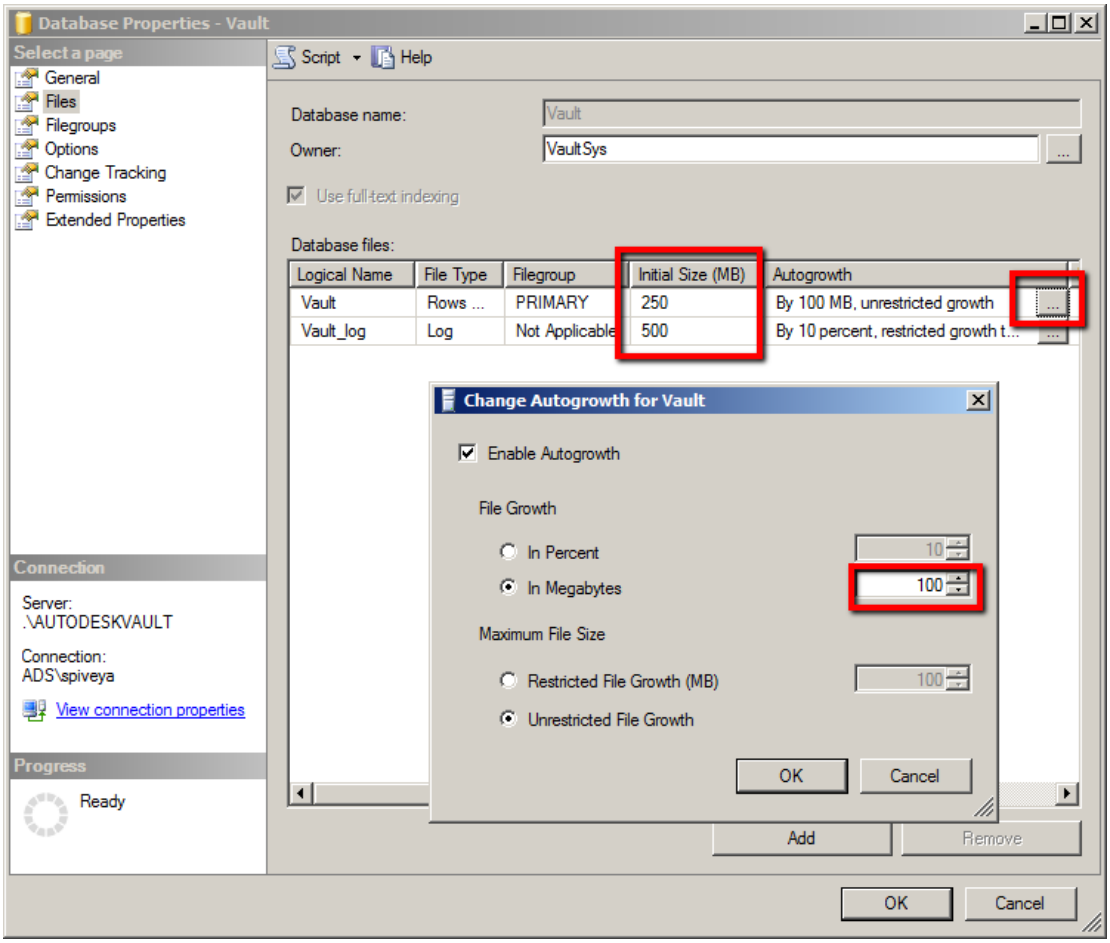
Or, in table form:-

Logical name	**Initial Size (MB)**	**Autogrowth**
KnowledgeVaultMaster		By 10MB, unrestricted growth
KnowledgeVaultMaster_log		By 10 percent, unrestricted growth
<Vault>		By 100MB, unrestricted growth
<Vault>_log	500	By 10 percent, unrestricted growth

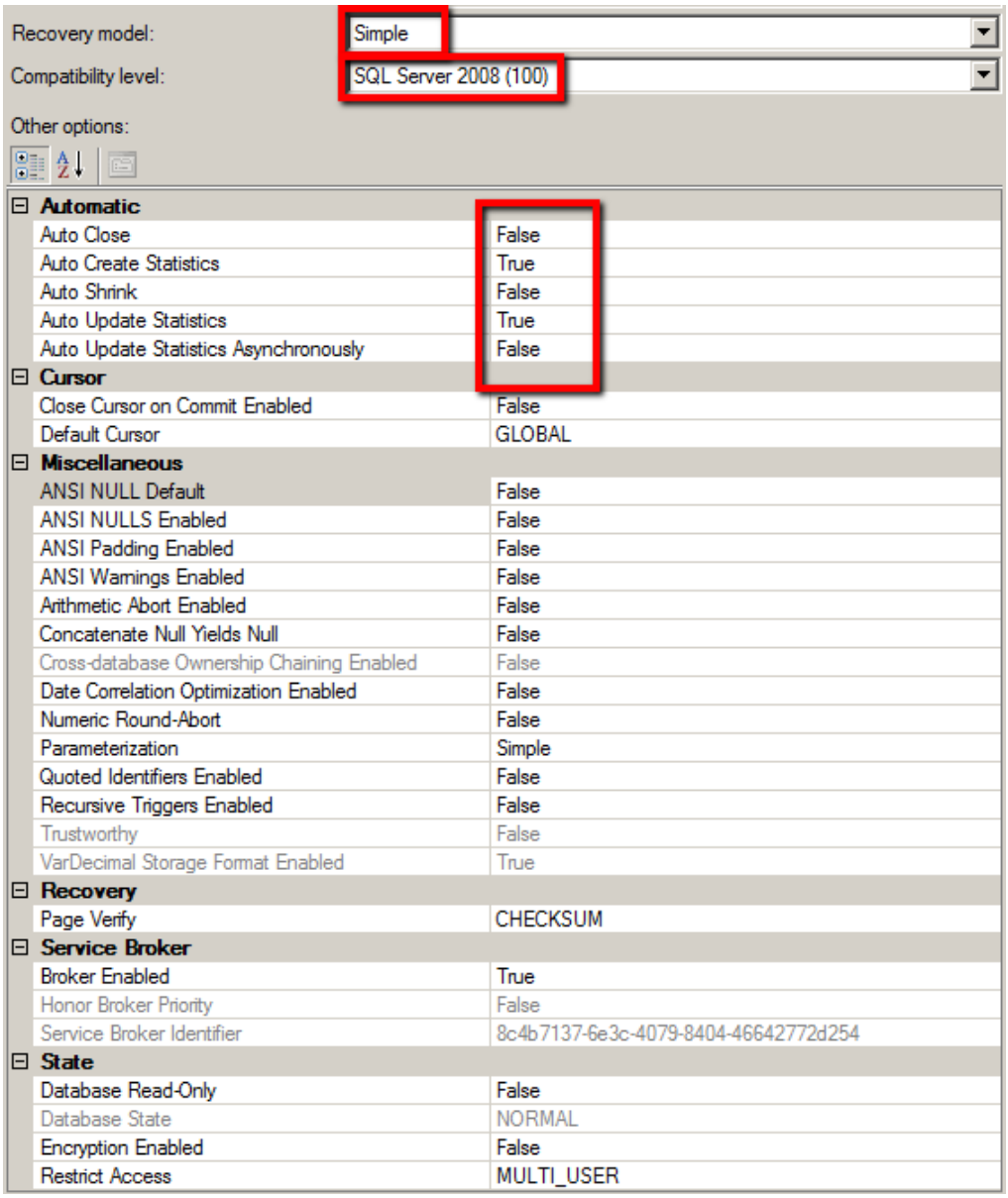
<Custom_Library>		By 25 MB, unrestricted growth
<Custom_Library>_log		By 10 percent, unrestricted growth
<Standard_Library>		By 25 MB, unrestricted growth
<Standard_Library>_log		By 10 percent, unrestricted growth

NOTE: A blank cell in the above table indicates that the default setting should not be changed.

Grey cells, indicate default values and should be set to the above if they are different.

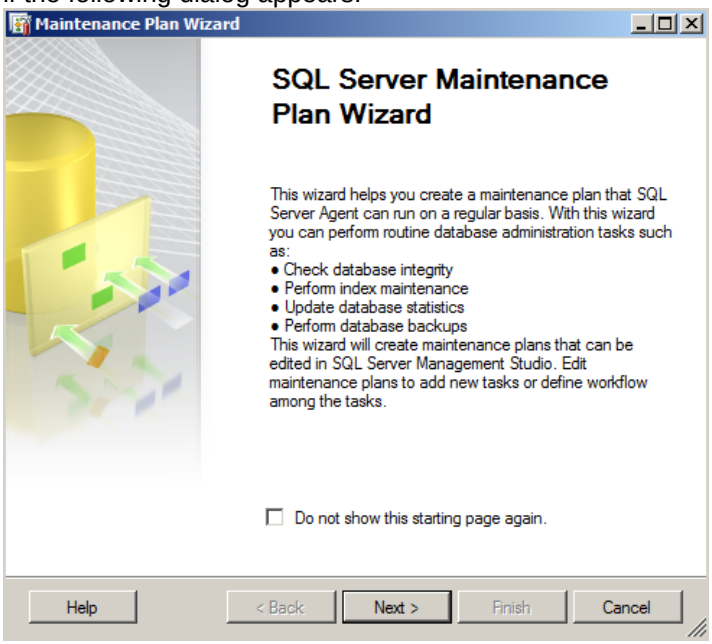


10. On the Options page, change the Recovery Model to **Simple**, Compatibility Level to **SQL Server 2008 (100)** and change the Auto Shrink drop-down list to **False**. All values under the **Automatic** heading should be set as shown below.

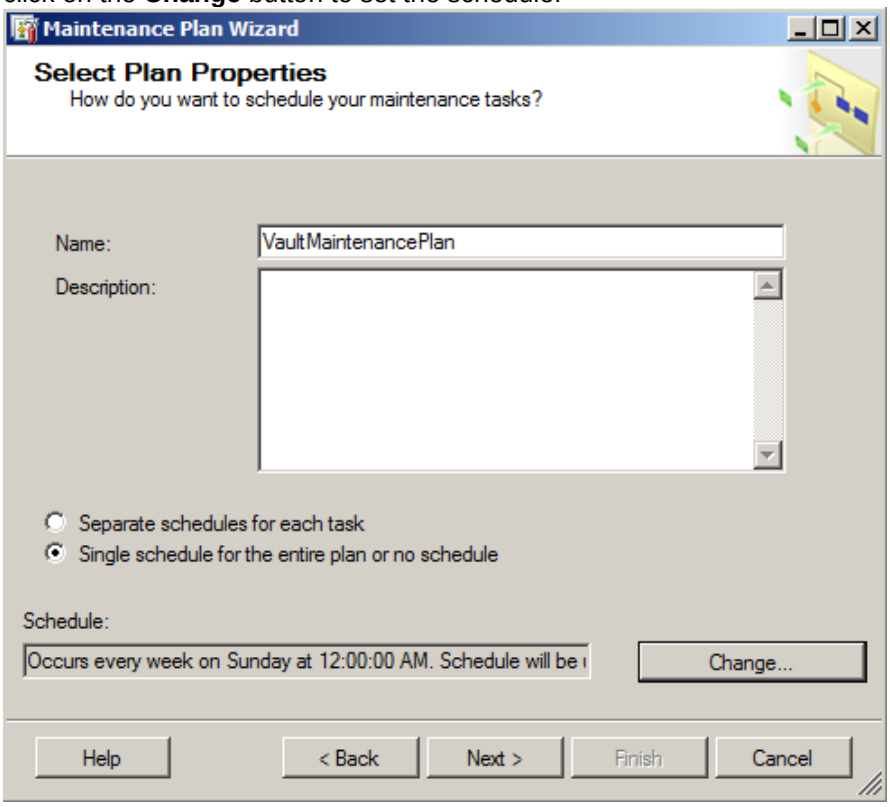


11. Perform these same steps for all of the **Vault** and library databases (steps 8 – 10).
12. Expand the Management folder and select the **Maintenance Plan** folder.

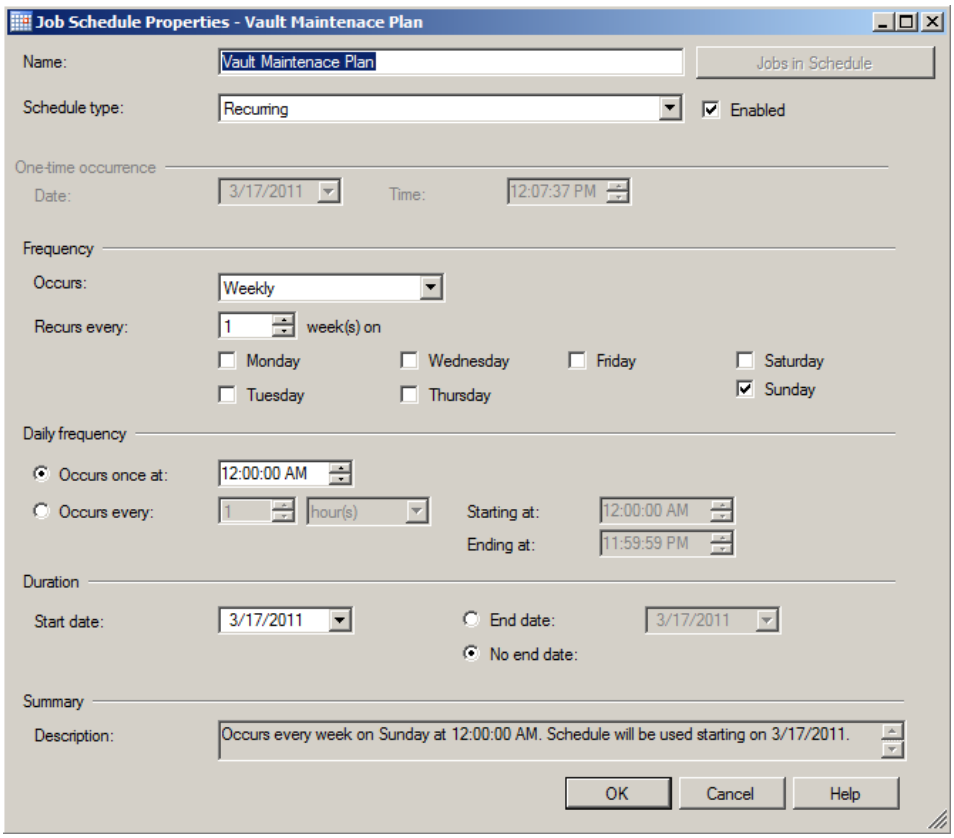
13. Right-click on the Maintenance Plan folder and select **Maintenance Plan Wizard**, hit next if the following dialog appears.



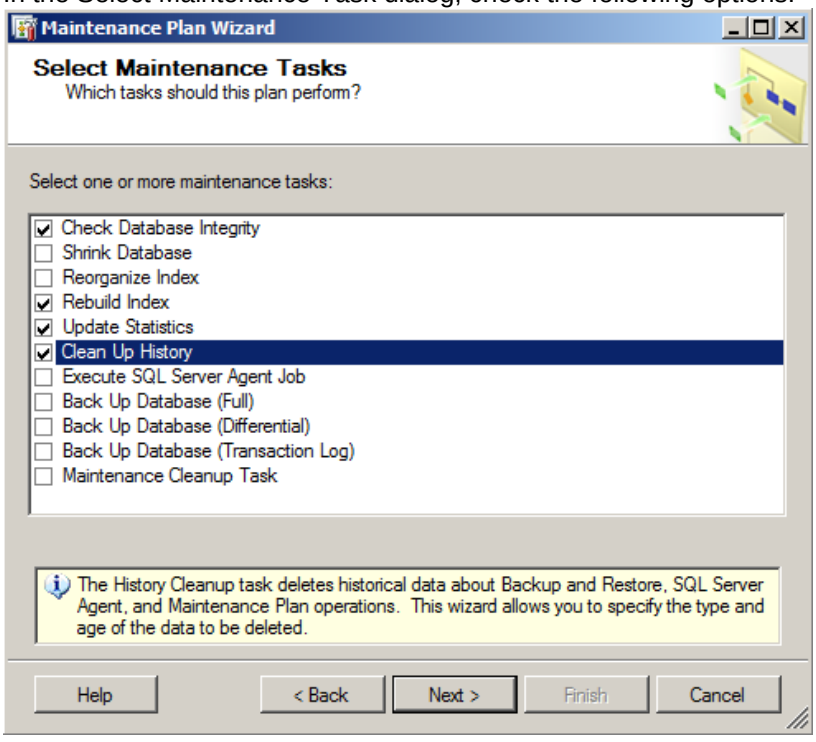
14. In the Select Plan Properties dialog, enter Vault Maintenance Plan for the name and then click on the **Change** button to set the schedule.



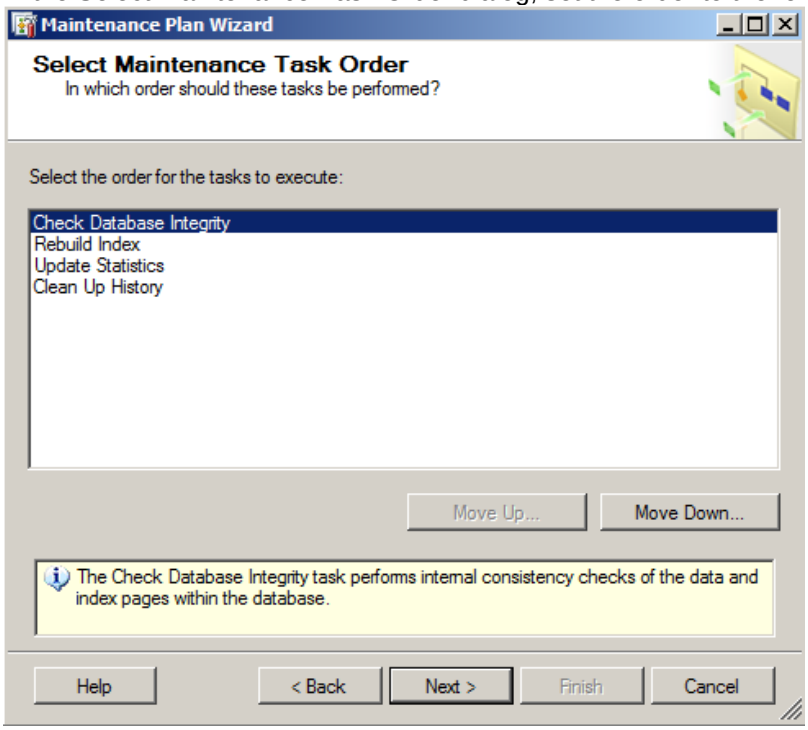
15. In the Job Schedule Properties dialog, set the plan to run after an Autodesk Vault Server Console backup has completed. Depending on the size of your dataset, this schedule may have to be run on a different day and time of the week. You may want to run this task on a Saturday to determine the amount of time it will take to complete and then decide the best day and time to run this job on a regular basis.



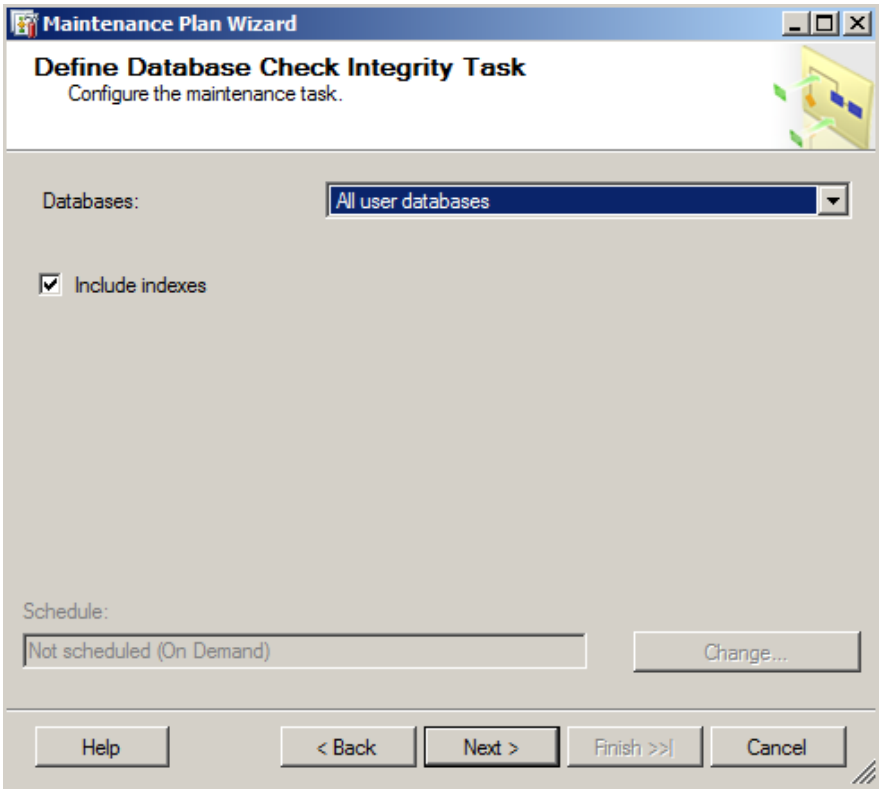
16. In the Select Maintenance Task dialog, check the following options:



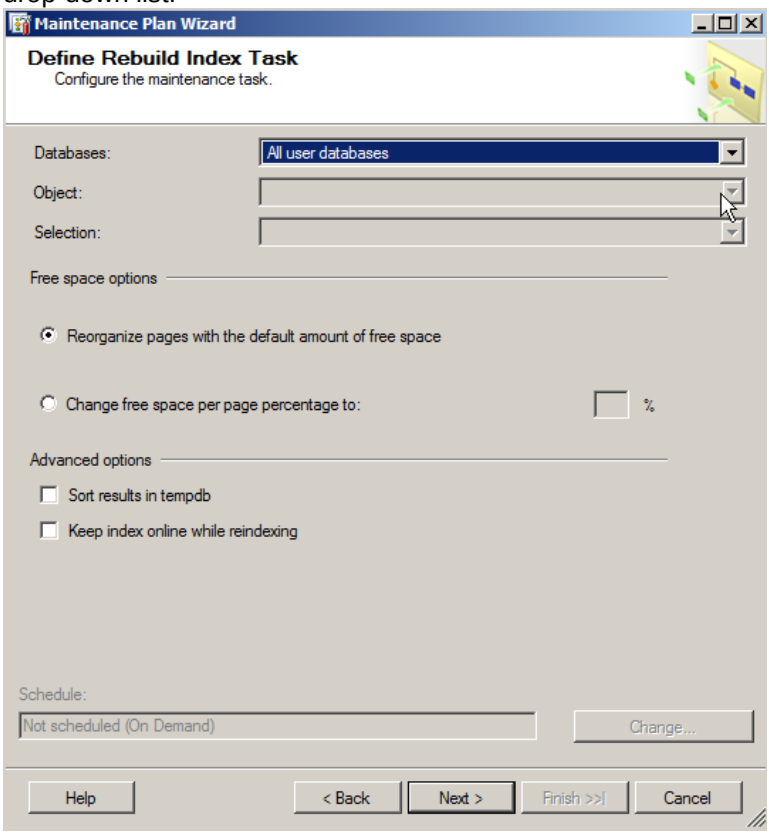
17. In the Select Maintenance Task Order dialog, set the order to the following



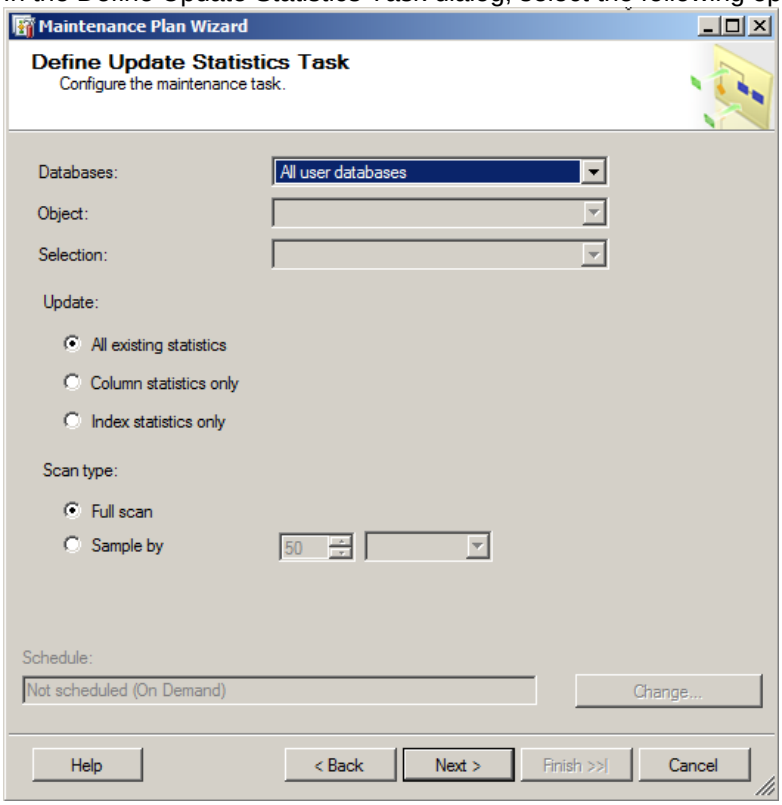
18. In the Define Database Check Integrity Task dialog, select **All user databases** from the databases drop-down list and check the box next to **Include Indexes**.



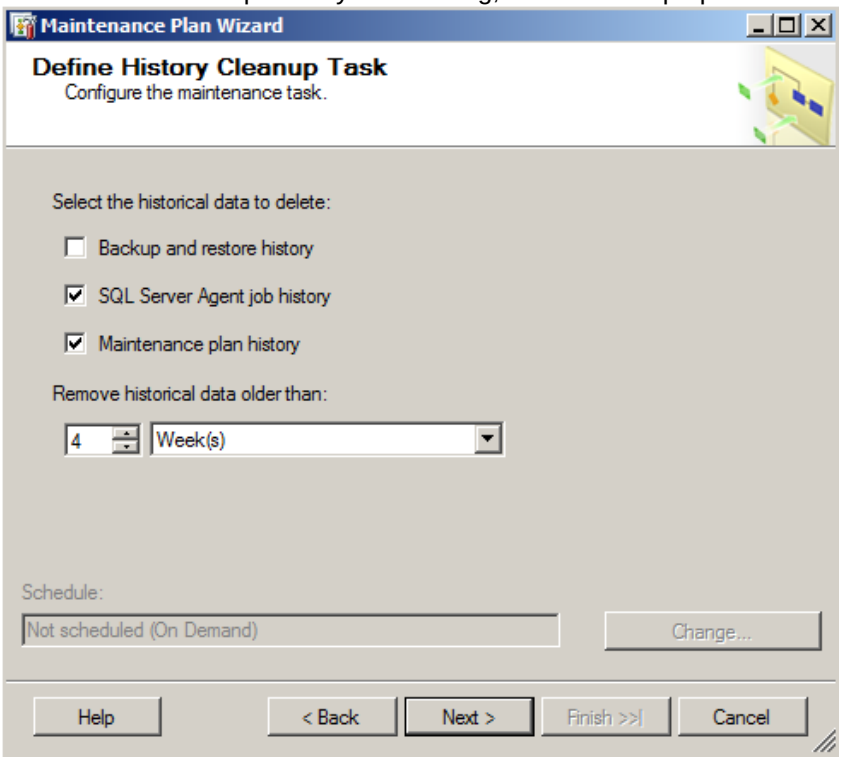
19. In the Define Rebuild Index Task dialog, select **All user databases** from the Databases drop-down list.



20. In the Define Update Statistics Task dialog, select the following options.



21. In the Define Cleanup History Task dialog, select cleanup options as needed.



22. In the Select Report Options dialog, specify the location for the maintenance reports.
23. Click **Next** and then **Finish**.

Creating a Maintenance Script for Microsoft SQL Express

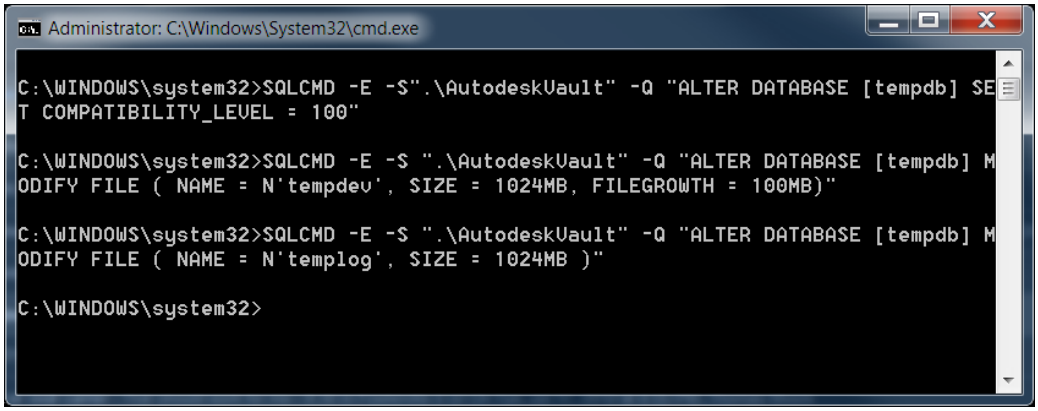
Microsoft SQL Express does not allow you to create a maintenance plan inside of SQL Server Management Studio Express. Additionally SQL 2008 had a security model change from SQL 2005. You will also need to ensure the OS (Windows) user that is running the SQL maintenance plan has the **sysadmin** role inside of SQL.

Tempdb Modifications through the Command Prompt.

As noted earlier in this section, if the SQL Server Management Studio is not installed, the tempdb database changes can be completed through the command prompt by performing the following:

1. Open the **Command Prompt** as **Administrator**.
2. **Copy** and **Paste** each line below into the command prompt and press **Enter**.

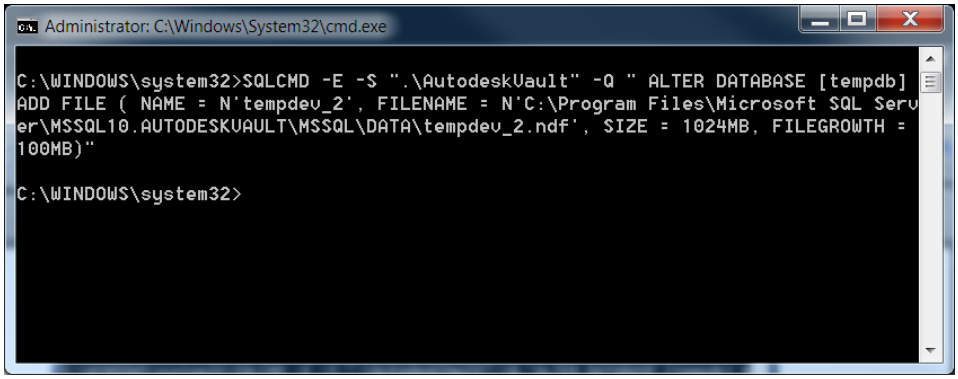
```
SQLCMD -E -S".\AutodeskVault" -Q "ALTER DATABASE [tempdb] SET
COMPATIBILITY_LEVEL = 100"

SQLCMD -E -S ".\AutodeskVault" -Q "ALTER DATABASE [tempdb] MODIFY FILE ( NAME =
N'tempdev', SIZE = 1024MB, FILEGROWTH = 100MB)"

SQLCMD -E -S ".\AutodeskVault" -Q "ALTER DATABASE [tempdb] MODIFY FILE ( NAME =
N'templog', SIZE = 1024MB )"
```



3. If using a multi-core system, additional data files should be configured using the guidelines below. ****Note** The file system path used under **FILENAME =** should be the same location as the SQL data directory. In the example below, it is *N'C:\Program Files\Microsoft SQL Server\MSSQL10.AUTODESKVAULT\MSSQL\DATA.* You will want to modify the script to list your correct path.

    a. Data file totals should equal half of the available physical processing cores - up to a maximum of 8 data files. *If using a total of 8 datafiles, an initial size of **512** MB can be used instead of **1024** MB as shown below. (example; 8 physical cores would equal 4 total data files, tempdev, tempdev_2, tempdev_3, tempdev_4)*

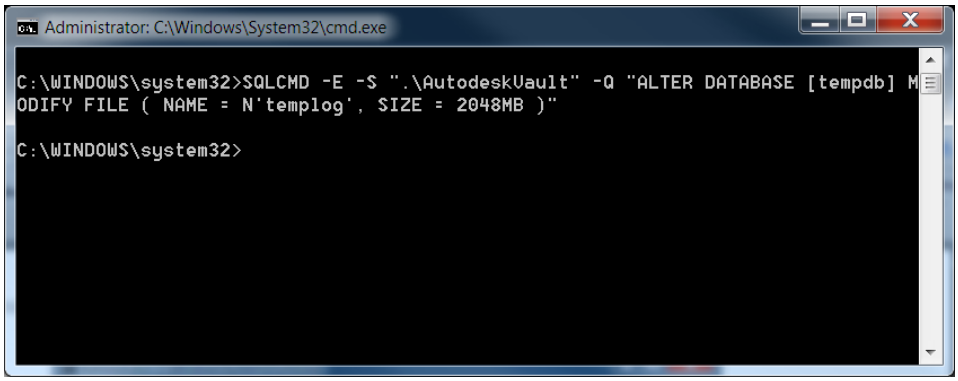
```
SQLCMD -E -S ".\AutodeskVault" -Q " ALTER DATABASE [tempdb] ADD FILE ( NAME =
N'tempdev_2', FILENAME = N'C:\Program Files\Microsoft SQL
Server\MSSQL10.AUTODESKVAULT\MSSQL\DATA\tempdev_2.ndf', SIZE = 1024MB,
FILEGROWTH = 100MB)"
```



b. If additional data files need to be created, simply modify the above example to reflect tempdev_3, etc, for both **NAME** and **FILENAME**.

c. Set the LDF log file to combined data file total. *(example; if there are 2 data files total, the resulting LDF should be set to an initial size of 2048 MB)*

SQLCMD -E -S ".\AutodeskVault" -Q "ALTER DATABASE [tempdb] MODIFY FILE (NAME = N'templog', SIZE = 2048MB)"



Maintenance Plan

Copy the script below and paste it into a new file saved as **VaultMaintenance.bat**.

The following is an **example** of how to run the batch file from the root of **C:** against a database named **Vault** and output the results to a text file.

C:\VaultMaintenance.bat *Vault* > results.txt

Note: A direct copy-paste from this document will **require** the line breaks be repaired. Also note that the user executing the maintenance plan will need to have permissions to do so inside of SQL. This can be accomplished during the installation of SQL or after.

```
REM This begins the maintenance plan.

@echo off

if "%1"=="" goto NOPARAM

set VAULTNAME=[%1]

set VAULTLOG=[%1_log]

@echo Setting %VAULTNAME% database compatibility to 100

sqlcmd -E -S ".\AutodeskVault" -Q "ALTER DATABASE %VAULTNAME% SET
COMPATIBILITY_LEVEL = 100"

@echo Setting %VAULTNAME% database recovery model to simple...
```

```
sqlcmd -E -S ".\AutodeskVault" -Q "ALTER DATABASE %VAULTNAME% SET RECOVERY
SIMPLE"

@echo Setting %VAULTNAME% database Autogrowth value...

sqlcmd -E -S ".\AutodeskVault" -Q "ALTER DATABASE %VAULTNAME%  MODIFY FILE
(NAME=%VAULTNAME%, FILEGROWTH=100MB)"

@echo Setting %VAULTNAME% database Log filesize...

sqlcmd -E -S ".\AutodeskVault" -Q "ALTER DATABASE %VAULTNAME% MODIFY FILE ( NAME =
%VAULTLOG%, SIZE = 512000KB )"

@echo Setting %VAULTNAME% database Autoclose to false...

sqlcmd -E -S ".\AutodeskVault" -Q "ALTER DATABASE %VAULTNAME% SET AUTO_CLOSE OFF
WITH NO_WAIT"

@echo Reindexing %VAULTNAME% database...

sqlcmd -E -S ".\AutodeskVault" -Q "USE %VAULTNAME% DECLARE tableCursor CURSOR FOR
SELECT NAME FROM sysobjects WHERE xtype in('U') DECLARE @tableName nvarchar(128)
OPEN tableCursor FETCH NEXT FROM tableCursor INTO @tableName WHILE
@@FETCH_STATUS = 0 BEGIN DBCC DBREINDEX(@tableName, '') FETCH NEXT FROM
tableCursor INTO @tableName END CLOSE tableCursor DEALLOCATE tableCursor"

@echo Updating Statistics on %VAULTNAME% database...

sqlcmd -E -S ".\AutodeskVault" -Q "USE %VAULTNAME% Exec sp_MSForEachTable 'Update
Statistics ? WITH FULLSCAN'"

goto EXIT

:NOPARAM

echo [FAIL] Please indicate Vault database

pause

:EXIT

REM This ends the maintenance plan.
```

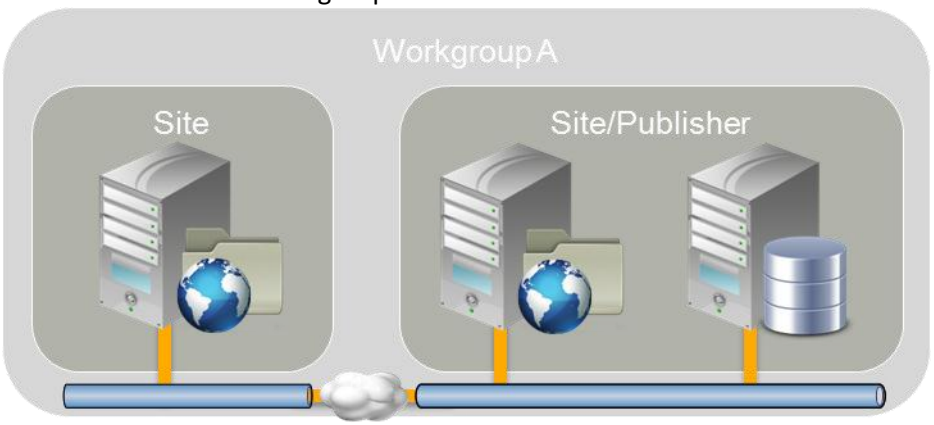
Upgrading a Vault Site Server to a Connected Workgroup Subscriber

To upgrade a Vault Server from being a Site in a Workgroup with no replicated SQL to a Connected Workgroup Subscriber, follow these steps.

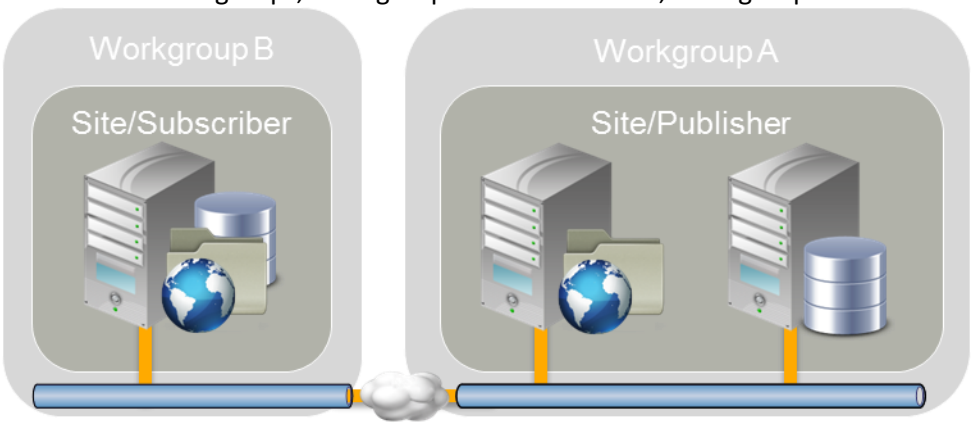
Consider this scenario: This picture shows one Workgroup for simplification purposes. However it could be possible to already have multiple Workgroups configured.

Currently

Current State: Workgroup A consists of a Publisher and two sites.



End State: Two Workgroups, Workgroup A is the Publisher, Workgroup B is a Subscriber



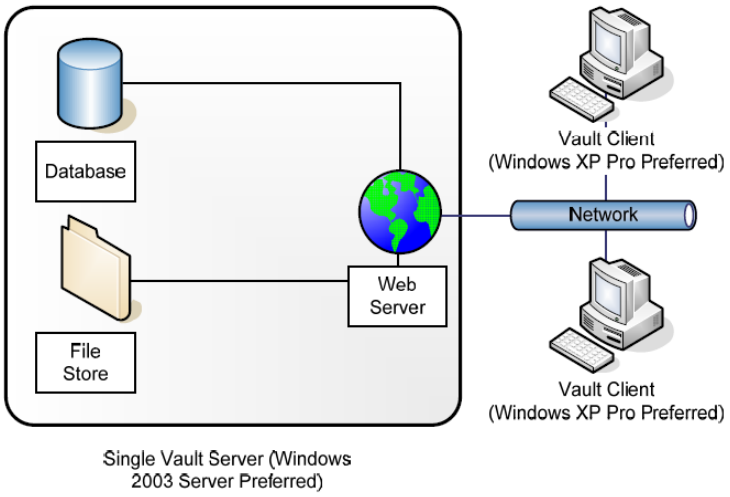
1. On the site that is to be upgraded to be an SQL Subscriber, copy or backup the filestore.
2. On a different site in Workgroup A delete the site in the ADMS Console

3. On the site being upgraded, install SQL Server according to the instructions in the Advanced Configuration Guide.
    a. Note, SQL can be installed on the same machine as Vault Server or on a separate machine.
4. On the Publisher, add a Workgroup pointing to the newly installed SQL Server. (Workgroup B)
5. After Replication has completed, modify the following line in the web.config file on the Vault Server in the new workgroup (Workgroup B).
    a. *<server value="servername\AutodeskVault" />* **- if the SQL Server is on a separate machine**
    b. *<server value=".\AutodeskVault" />* **- if the SQL Server is installed on a the same machine**
6. On the Vault Server in the new workgroup (Workgroup B) Launch the ADMS Console.

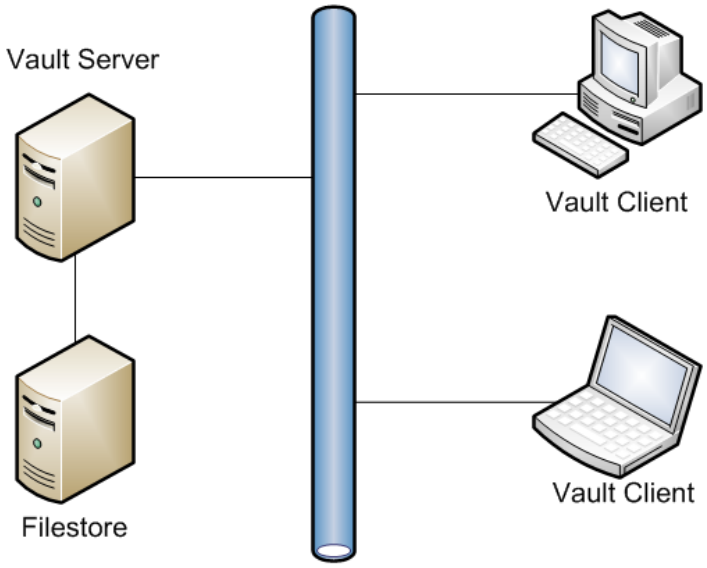
Managing a remote file store

To move the location of your file store to a mapped drive or remote shared location:
The vault supports two basic file store configurations:

1. File store located on the Autodesk Vault Server.



2. File store located on a remote file server that has a shared folder.



A remote file server can be used for hosting the file store and/or backing up and restoring vault data. This section describes the steps required to configure a remote file store.

Moving the file store to a mapped drive or remote share

For simplicity purposes, the computer hosting Autodesk Vault Server is called ***DMMachine*** and the computer hosting the remote file store is called ***FSMachine***. The domain name is ***MyDomain.*** We are also assuming that the server where Autodesk Vault Server is installed is a member server and not a domain controller.

If you have the Autodesk Vault Server installed on a domain control, the AutodeskVault domain account is used and you can go the Moving the File Store section below.

Create a new domain user account.

1. Open the Active Directory Users and Computers and select an Organizational Unit (OU) to create the account in.
2. **Create** an account named **AutodeskRemote**. Set the password to match your domain password policy and set the password to **never** expire.

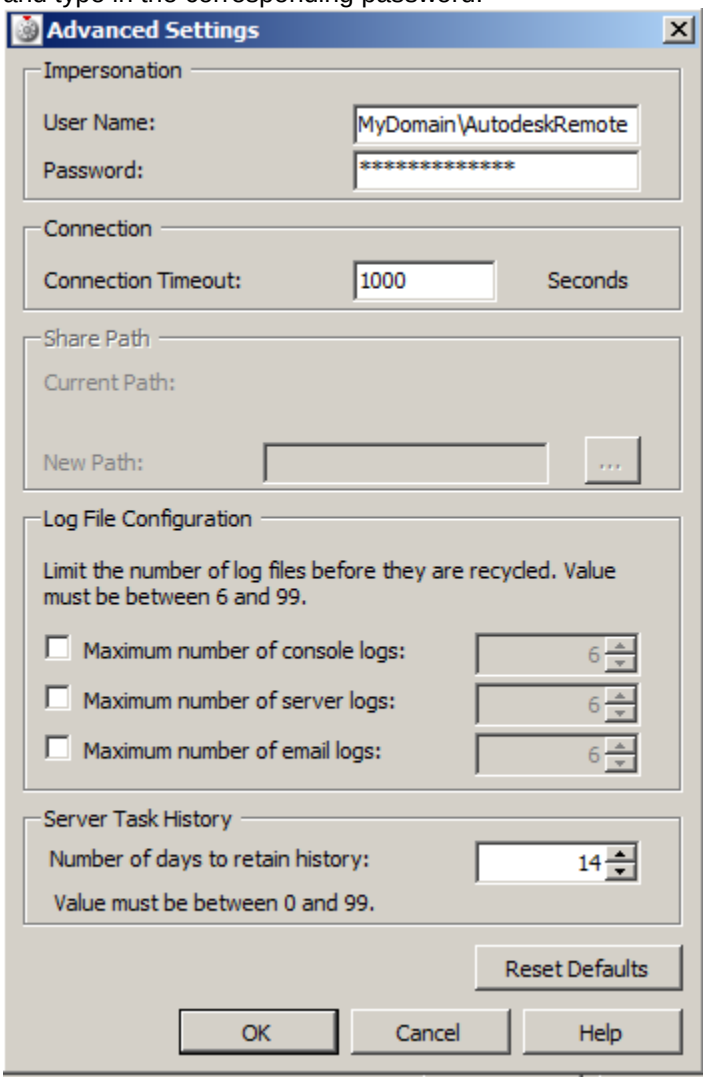
Create a remote share.

1. Open Windows Explorer on the FSMachine and create a directory called **VaultData**.
2. Right-click on the folder and select **Properties**.
3. Go to the **Sharing** tab and create a new share named VaultData.
4. Click Permissions and set the **AutodeskRemote**, **Network Service**, and **System** user to **Full Control**.
5. Click **OK** in the Permissions for Share dialog box.
6. Go to the **Security** tab and add the **AutodeskRemote** account and set it to **Full Control** permission.

Setting the new account in the Autodesk Vault Server Console

1. On the DMMachine, open the Autodesk Vault Server console.
2. Select **Tools** -> **Administration**.
3. In the Advanced Settings tab select the Settings button next to **Advanced Configuration** settings.

4. In the Advanced Settings dialog, change the User Name to **MyDomain\AutodeskRemote** and type in the corresponding password.



5. Apply the changes and then click **OK**.

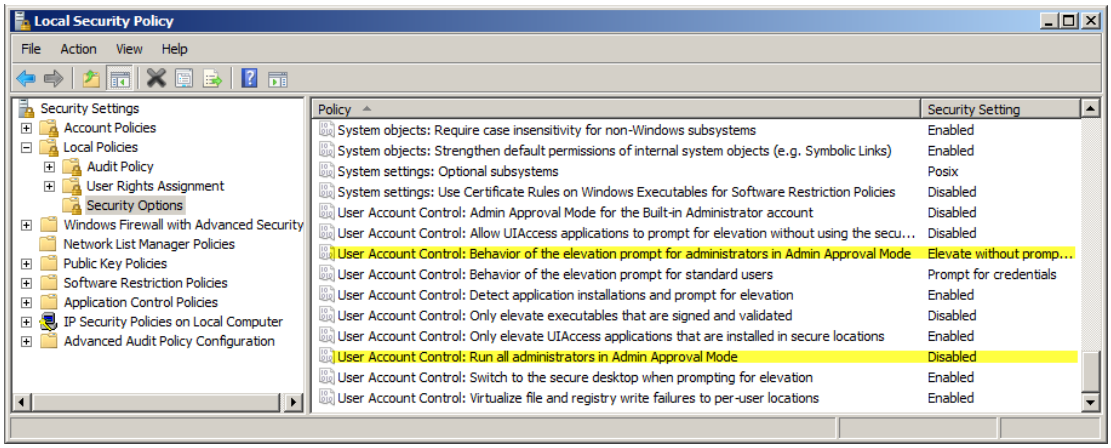
Moving the vault file store

1. Select the vault which you would like to move to a different location.
2. Select Actions -> **Move File Store**.
3. Set the New File Store Location field to \\FSMachine\VaultData.
4. Click **OK**.

User Account Control

If you plan to schedule automatic backups using ADMS Console, the User Account Control settings in Windows 7 \ 2008 \ 2008 R2 must be configured to allow applications to run without prompting for administrator permission. **Note:** Configuring the following settings will affect all of the applications on your computer. All applications will be run without prompting for administrator approval.

1. From the Windows Start menu, type **Run**.
2. In the Run dialog box, enter **secpol.msc**. Click OK.
3. When you are prompted to allow the security policy application to run, click Continue.
4. In the **Local Security Policy** dialog box, expand:-
    a. **Security Settings**
        - **Local Policies**
        - **Security Options**
5. Locate the "**User Account Control: Behavior of the Elevation Prompt for Administrators" (**Windows Server 2008 R2 **= "User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode")** policy and right-click it.
    a. Click **Properties**.
        - Select **Elevate without Prompting**, and then click OK.
6. Locate the **User Account Control: Run all administrators in Admin Approval Mode** policy and right-click it.
    a. Click **Properties**.
7. Select **Disable**, and then click OK



Additionally, portions of the UAC can be disabled through control panel.

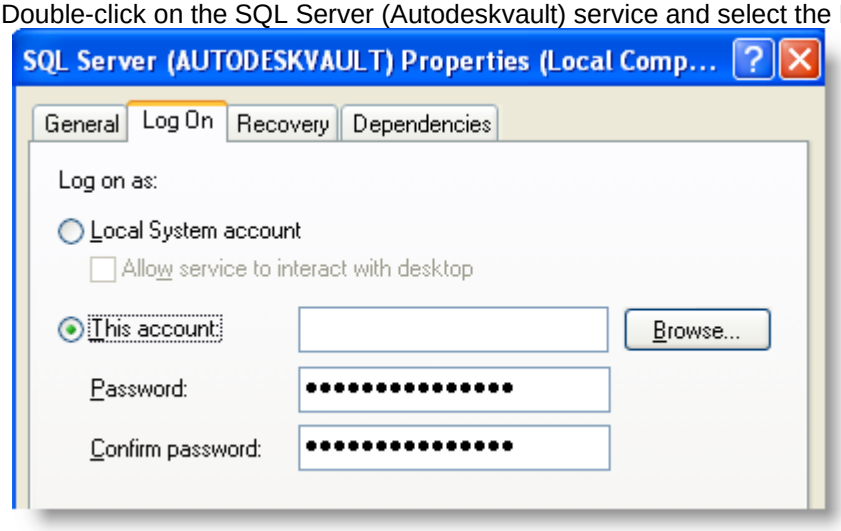
Post-install Configuration Changes

Setting up a remote backup location

If you plan to back up your vault data to a remote share, follow the steps in the Creating a new domain user account, Create a remote share and Setting the new account in the Autodesk Vault Server Console sections in this document. After that is complete, you will have to modify the SQL Service to use a domain account using the following steps:

Note: The new domain account created for these steps needs to be added to the default SQL users group for the AutodeskVault instance. The group created by SQL 2008 is called SQLServer2008MSSQLUser$<*computername*>$AUTODESKVAULT.

1. Double-click the Services icon in the Administrative Tools in the Control Panel
2. Double-click on the SQL Server (Autodeskvault) service and select the Log On tab.



3. Select the This Account radio button and enter a domain account in the form of Domain_Name\Domain_account (with the correct password).

   NOTE: If you change the service's login credentials, you will be prompted to restart the MS SQL Server service. Please do so for changes to take effect. In addition, ensure that clients are not using the Autodesk Vault Server before restarting SQL Server."

4. Verify that the account specified has write access on the share to which you are backing up.

Configuring a remote Vault connection using FQDN

To configure the Vault Server to allow remote connections over the internet using a Fully Qualified Domain Name (FQDN):

1. Create a DNS "A" or host record for your current FQDN with your ISP.
2. Install Autodesk Vault Server on your server and verify that it works properly.
3. On your server, open the Internet Information Services Manager and expand the Websites folder.
4. Right-click on the website that contains the AutodeskDM virtual directory. Click Properties.
5. In the Properties dialog box, click the Website tab.
6. On the Website tab, click Advanced.
7. In the Advanced Website Identification dialog box, under the Multiple identities for the website, click Add.
8. In the Add/Edit Web Site Identification dialog box, select the correct IP address that will interact with the website.
9. Enter the TCP port you want to use. If this is not port 80, then your clients will have to add "**:<port#>**" at the end of the FQDN in order for the connection to work.
10. In the Host Header value, enter the FQDN.
11. Click OK to close each dialog box.

Note: Additional settings may be required for your router or firewall. Check with your IT department for the necessary changes.

How to increase the timeout values on the Autodesk Vault Server

As the vault database increases in size, you may have to modify some timeout values on the server to allow for the server to process more data. Increase the timeout values for client and server functions:

1. Open Windows Explorer and navigate to the **C:\Program Files\Autodesk\ADMS *Product* 2013\Server\Web\Services** directory.
2. Create a backup copy of the **Web.config** file.
3. Open the **Web.config** file with Notepad and look for the following line:

```
190        <timeouts connection="120" defaultCommand="360" longCommand="1800" />
```

   Note: these values may be different, depending on the size of the vault and the speed of the server it is installed on. Higher values may be necessary.

4. **Save** the Web.config file.
5. Open a command prompt and type **IISRESET**.

Note: If you increase the defaultCommand value higher then **1000**, you must increase the **executionTimeout** value to an equal or higher value. This is found on the following line:

```
171    <httpRuntime maxRequestLength="51200" executionTimeout="1000" />
```

Running Autodesk Vault Server with SSL

Setting up the Autodesk Vault Server to use SSL (Secure Socket Layer) is a two step process.

1. On the DM Server machine, install the certificate and setup the website SSL preferences.
2. Verify that the clients can communicate properly with SSL.

Configuring the DM Server machine

It is outside of the scope of this document to instruct you how to setup SSL under IIS. For more information, visit the following web resources. Note that some steps may be different depending upon the version of Windows that you are currently using.

Obtaining and Installing Server Certificates (IIS 6.0)

- http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/9a4ae054-da27-4261-a980-4e7b92091eb7.mspx?mfr=true

Configuring Server Certificates in IIS 7

- http://technet.microsoft.com/en-us/library/cc732230(v=ws.10).aspx

By default, the Autodesk Vault Server installer does not configure the AutodeskDM Virtual Directory to require SSL. After the certificate has been installed on the Default Web Site, users are able to login to the Autodesk Vault Server using both secured and unsecured connections.

Unsecured logins can be accomplished by using localhost, 127.0.0.1, machine name or IP address in the server field of the login dialog.

Secured logins must use the common name to which the certificate was issued.

If Vault Web Client is installed on the server, clients will need to access it from their web browser with https://servername/AutodeskDM/Webclient.

Configure the AutodeskDM Virtual Directory to require SSL Access

NOTE: The following procedure uses the Internet Information Services Manager to configure the AutodeskDM Virtual Directory to require SSL for access.

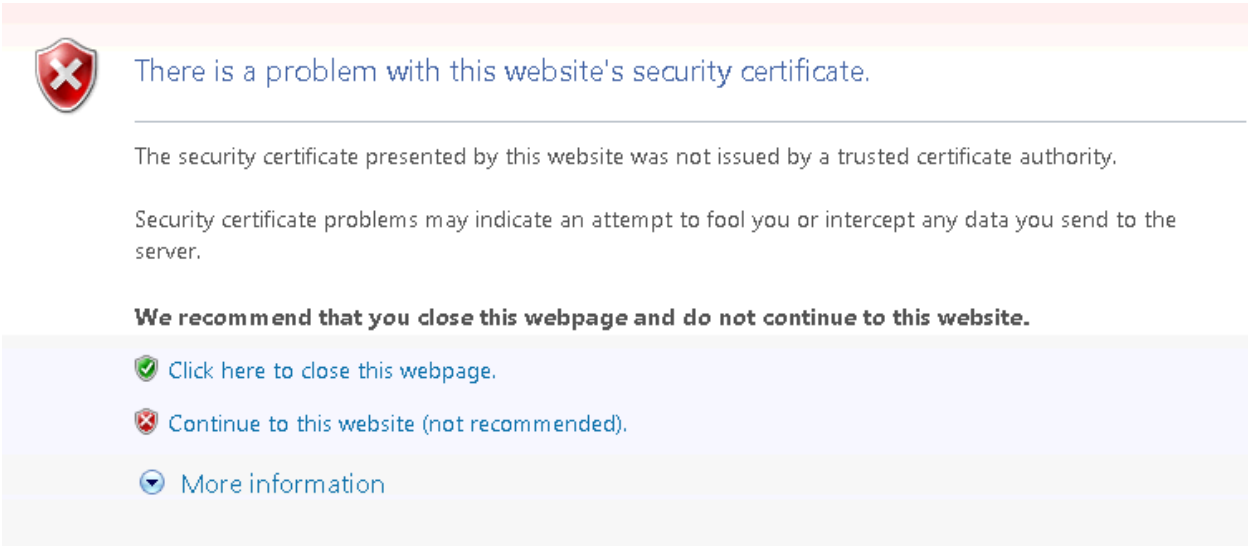
1. Log into the computer hosting the Vault Server as a local or domain administrator.
2. From the Start Menu, select Settings > Control Panel.
3. Double-click Administrative Tools, and then double click Internet Information Services.
4. Click Web Sites under your server name.
5. Select the Default Web Site and expand it. This web site must have the certificate you created installed to it.
6. Right-click the AutodeskDM virtual directory and click Properties.
7. Select the Directory Security tab.
8. Click Edit under Secure Communications.

   NOTE: If the View Certificate button is unavailable, the certificate that you created has not been installed on the AutodeskDM Virtual Directory's parent web site. Install a certificate before continuing with the rest of this process.
9. Click Require secure channel (SSL). Clients browsing to this directory must now use HTTPS.
10. Click OK.
11. Click OK.
12. If the Inheritance Overrides dialog is displayed, click Select All and then click OK. The new security settings are applied to all subdirectories of the AutodeskDM virtual directory.
13. Close the Internet Information Services Console.

Client Configurations

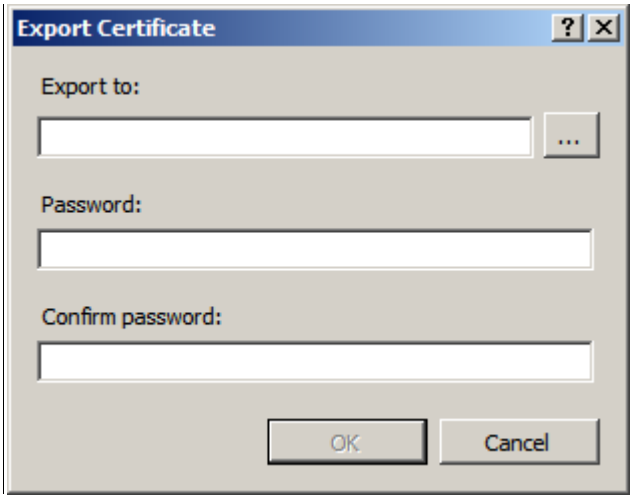
Configuring a Client Computer with Internet Explorer 8

To verify that the SSL client/server communication is properly setup, open Internet Explorer and browse to https://<servername>. If the connection is not working, the Security Alert dialog box is displayed.



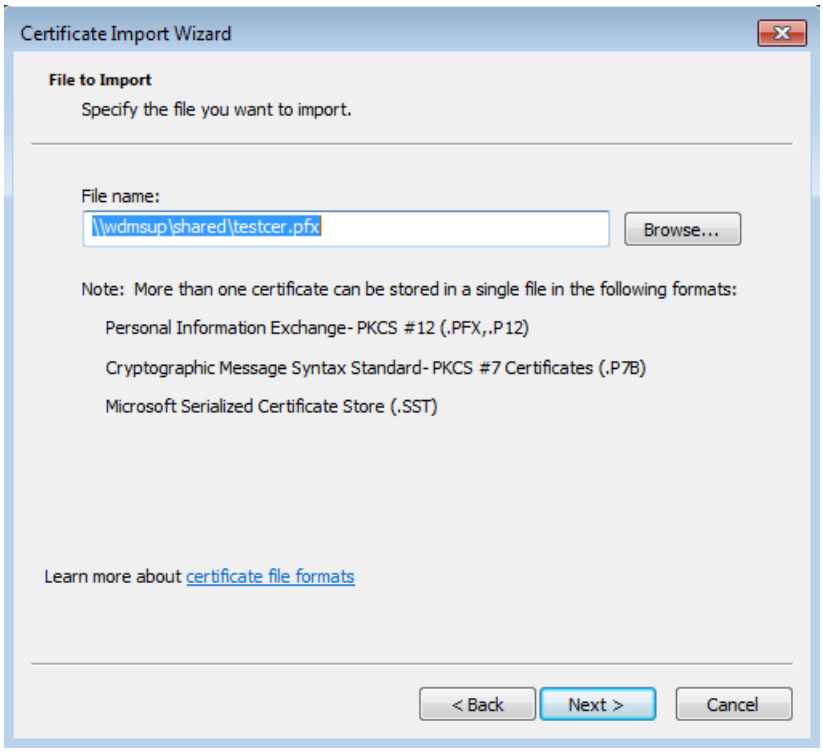
1. Click **Continue to this website (not recommended).**
2. Export the certificate from the server.
    a. Open IIS Manager from Control Panel -> Administrative Tools -> Internet Information Services Manager.
    b. Highlight the computer name.
    c. On the right hand side find the Server Certificates Option and double click.

    d. Find the certificate that you are using in the list and highlight it.
    e. Right click and select Export.
    f. Select a shared location to save the certificate and enter a password for the certificate.

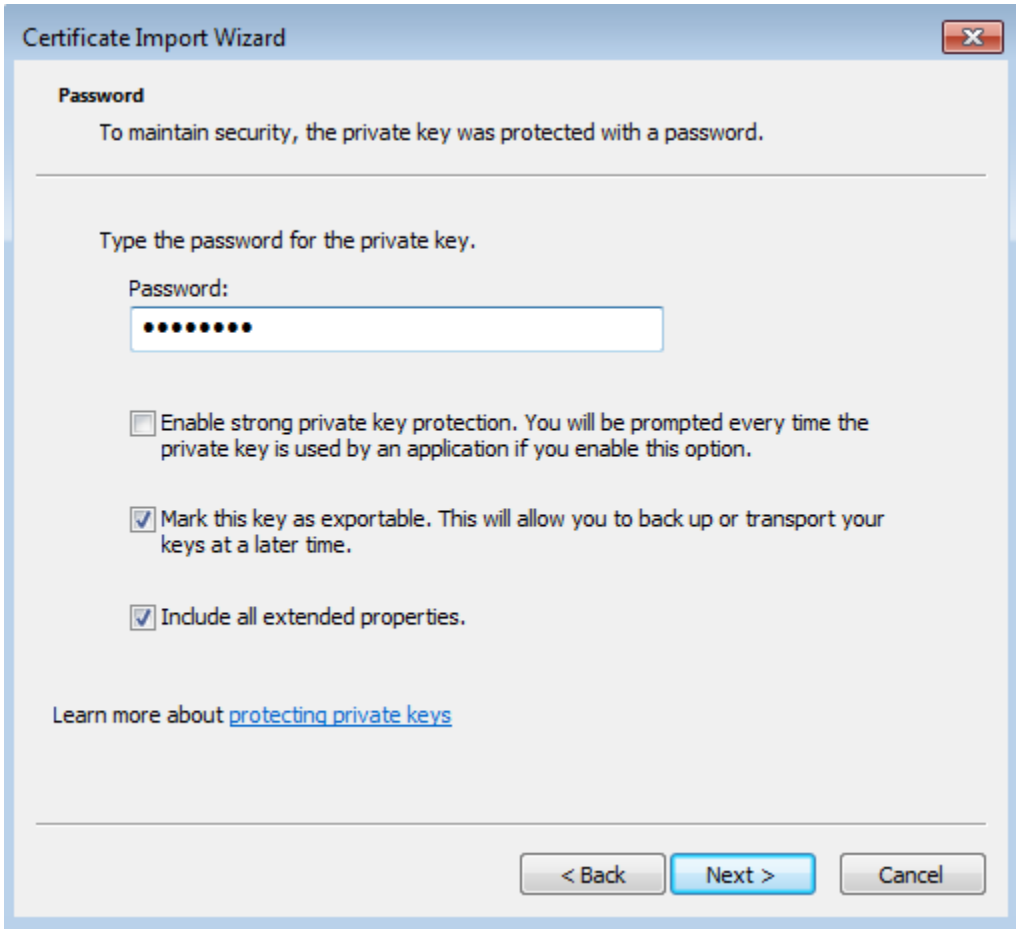


3. Open the share from the client PC and find the newly created certificate.
4. Double click to open the certificate and start the Certificate Import Wizard.

5. Click next on the File to import screen as the file shown should be the certificate you selected earlier.



6. Enter the password you created for the certificate when you exported it from the server.



7. Select Place all Certificates in the following store and select the Trusted Root Certification Authorities.
8. Finish the wizard.

Login from client applications using SSL

1. In the Log in dialog box, enter your user name, password, and the name of the database.

2. For the name of the server, specify the machine name of the server with the prefix: https://. For example:

- If you are using the default SSL port 443: `https://ServerName`
- If you are using a different SSL port: `https://ServerName:XXX` where XXX is the SSL communication port number.

> ***NOTE:*** *The secured login depends on the certificate issued to the server machine. If it is issued for the machine name, then only https://ServerName will work. Otherwise, if the certificate is issued for a dedicated IP, then only https://serverIPAddress will work as a secure vault login.*

Using Vault with a Proxy Server

This section describes setting up a proxy to enable successful Autodesk Client/Server data communication.

If a client machine connects to the web server through a proxy server, then all calls to the Autodesk Vault Server from any Autodesk client will fail. To have a successful Autodesk Client/Server communication, you need to bypass the proxy server.

Change the proxy settings in Internet Explorer 8.x, 9.x

1. Open **Internet Explorer**.
2. From the **Tools** menu, select **Internet Options**.
3. Select the **Connections** tab.
4. Click **LAN Settings**.
5. If **Automatically Detect Settings** is selected, remove the check box.
6. If the **Use a proxy server for your LAN** check box is enabled, turn on the **Bypass proxy server for local addresses** check box.
7. Click the **Advanced** button next to the **Port** field.
8. In the Proxy Setting dialog, add the Vault Server name and IP address into the **Exceptions** field.
9. Click **OK**.
10. Click **OK**.
11. Click **OK** to close Internet Options.

All addresses without a period, for example: http://webserver, will bypass the proxy and be resolved directly.

If Internet Explorer continues to connect to the assigned HTTP proxy server, then the HTTP proxy address may contain a period. If this happens, configure the proxy server to use a host name.

Configure the proxy server to use a host name

1. Follow steps 1-5 above for changing the proxy settings in Internet Explorer.
2. If the “Address” field is http://webserver.domainname.com or http://10.0.0.1, then change it to http://webserver only.
3. Click OK and close Internet Explorer Options.

For more information on advanced proxy bypass configurations:

- Read Microsoft Knowledge Base article 262981: Internet Explorer Uses Proxy Server for Local IP Address Even if the 'Bypass Proxy Server for Local Addresses' Option Is Turned On

- Read the Microsoft document Working with Proxy Servers (http://technet.microsoft.com/en-us/library/cc939852.aspx)

Bypassing a Proxy Server with the Application config file

By default HttpWebRequest's uses the proxy setting specified inside of Internet Explorer. You can change those settings by going to Control Panel -> Internet Options -> Connections Tab -> LAN Settings Button. You can disable auto detection by un-checking the "Automatically Detect Settings" button. In most cases this allows the client application to function properly. However, in some cases you may experience slow connectivity and delayed responses from the application when connected to Autodesk Vault Server. There is an option to disable proxy configuration through your application.exe.config file:

In this example, for Inventor, the config file is located in the following directory. Each client application has a similar config file. Make a backup copy of the file and then edit the file using Notepad.exe ONLY.

"C:\Program Files\Autodesk\Inventor 2013\Bin\Inventor.exe.config"

Add this line of code to the file:

```
<system.net>
  <defaultProxy>
    <proxy autoDetect="False"/>
  </defaultProxy>
</system.net>
```

After you have added the text, save and close the file. The changes will take effect the next time the application is started.

Autodesk Vault Server Log Files

This section shows you where to find the various log files and other files used for troubleshooting potential problems with Autodesk Vault.

For the purposes of this section, we refer to the %temp% folder. This is the temp folder location defined for the Windows user account that is logged in on the computer. By default, this folder is located in the following location for Windows XP and Server 2003

C:\Documents and Settings\ACCOUNTNAME\Local Settings\Temp

And the following location for Windows 7, Server 2008, and Server 2008 R2.

C:\Users\ACCOUNTNAM\AppData\Local\Temp

In this example, ACCOUNTNAME is the name of your user account in Windows.

Vault server log files

There are primarily two different log files to look for in this location. Each of these is described in full detail below.

Folder location and file names:

Microsoft Windows™ XP / Server 2003 - C:\Documents and Settings\All Users\Application Data\Autodesk\VaultServer\FileStore

Microsoft Windows 7 / Server 2008 / Server 2008 R2 - C:\ProgramData\Autodesk\VaultServer\Filestore

Vlog-YYYYMMDD.txt

Any server-side problems relevant to Check-in, Check-out, Get Latest Version, Undo Check-out, Advanced Search and other operations performed from within Vault Explorer or one of the supported product add-ins are written into these log files.

ADMSConsoleLog-YYYYMMDD.txt

Any server-side problems relevant to backup, restore, re-index, purge or other operations performed within Autodesk Vault Server Console are written into these logs.

Emaillog-YYYYMMDD.txt

Email sent from the server.

Autodesk Vault Server 2013 installation log files

During the installation of Autodesk Vault Server there may be errors reported the by the diagnostic tool or during the installation itself. These errors are recorded in log files.

Pre-check log:

%temp%\EDMlog
Prechecks.xml
Prechecks.xsl

Autodesk Vault <Version> 2013 client installation logs:

%temp%
Autodesk Vault <Version> 2013 Install.log
Autodesk Vault <Version> 2013 Setup.log

Autodesk Vault <Version> 2013 server installation logs:

%temp%
Autodesk Vault <Version> 2013 (Server) Install.log
Autodesk Vault <Version> 2013 (Server) Setup.log

Autodesk Server Diagnostic Tool Log files

If you run the Autodesk Server Diagnostic Tool, the log files are located in the %temp%\EDMLog directory.

Autodesk Server Diagnostic Tool:

%temp%\EDMLog
DiagTool.xml
DiagToolLog.xsl

Microsoft SQL Server log files

Folder location and file names:

C:\Program Files\Microsoft SQL Server*%SQL_INSTANCE%*\LOG

Errorlog

Errorlog.1

Errorlog.2

Errorlog.3

The SQL logs are named sequentially with the most recent (current) file being named errorlog followed by errorlog.1 then errorlog.2 and so on.

DWG iFilter Log files

There are log files maintained by the various iFilters used when performing some Vault operations like re-index. These log files can be helpful when troubleshooting problems with block attributes or properties not indexing as expected in Vault Explorer.

Folder location and file names:

Depending on your server setup, your iFilter log files may be contained in a different location.

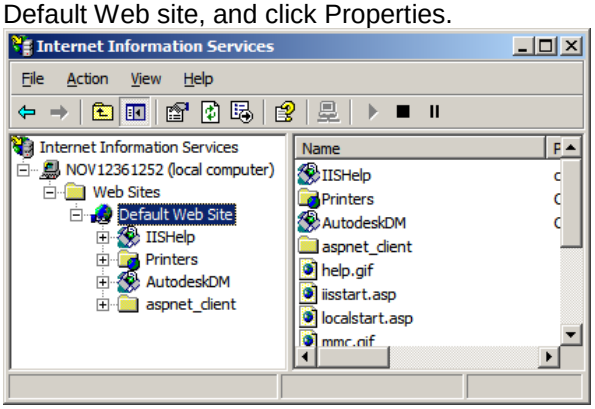
C:\Windows\Temp\ OR %TEMP%

DWGFILT.*.log

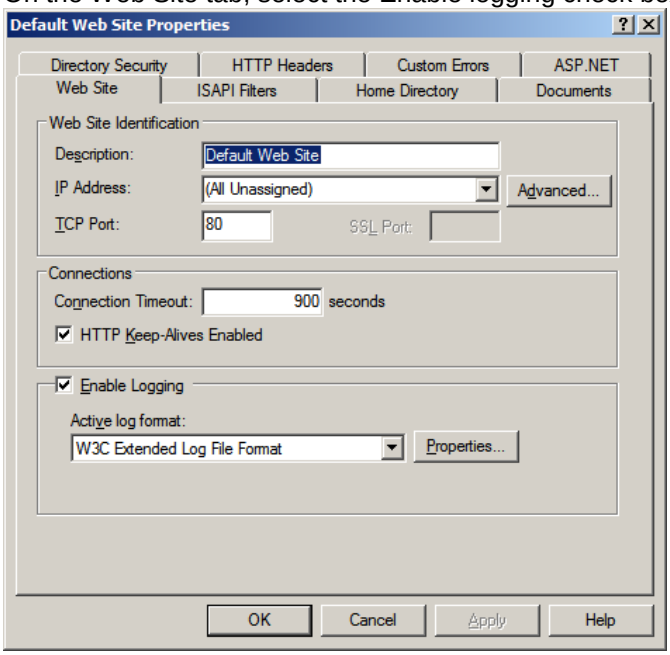
Customize W3C Extended Logging (IIS 6)

The W3C Extended log file format is the default log file format for IIS. It is a customizable ASCII text-based format. You can use IIS Manager to select which fields to include in the log file. [W3C Extended Log File Format]

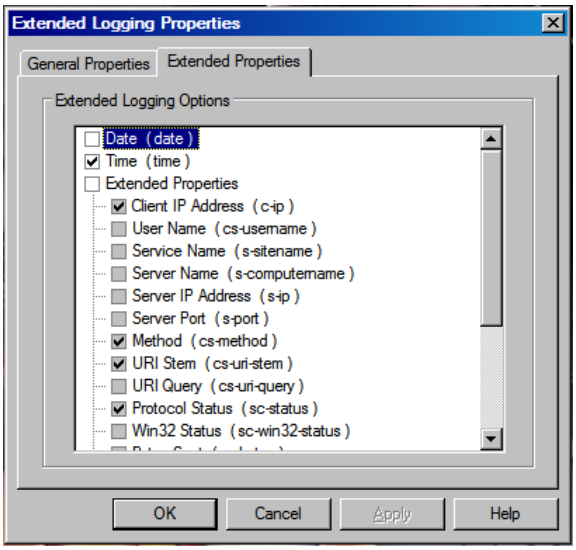
1. From the Windows Start menu, select Control Panel > Administrative Tools > Internet Information Services
2. In IIS Manager, expand the local computer, expand the Web Sites folder, right-click the Default Web site, and click Properties.

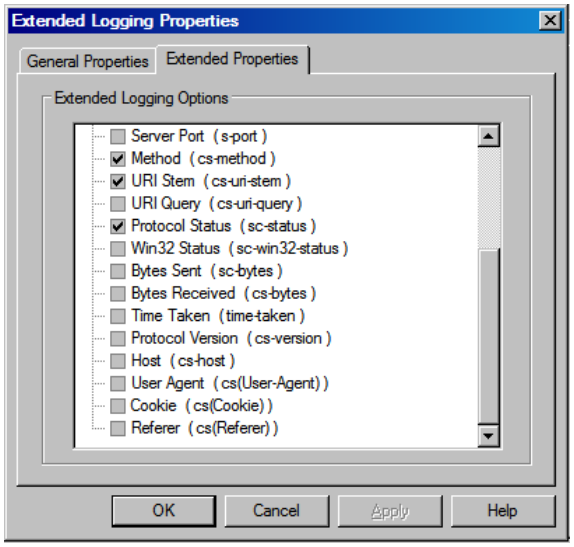


3. On the Web Site tab, select the Enable logging check box (if it is not already selected).



4. In the Active log format drop-down list, select W3C Extended Log File Format and click the Properties button.

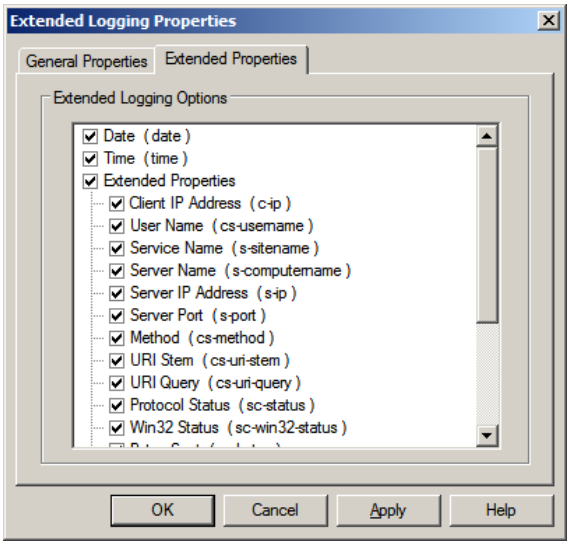


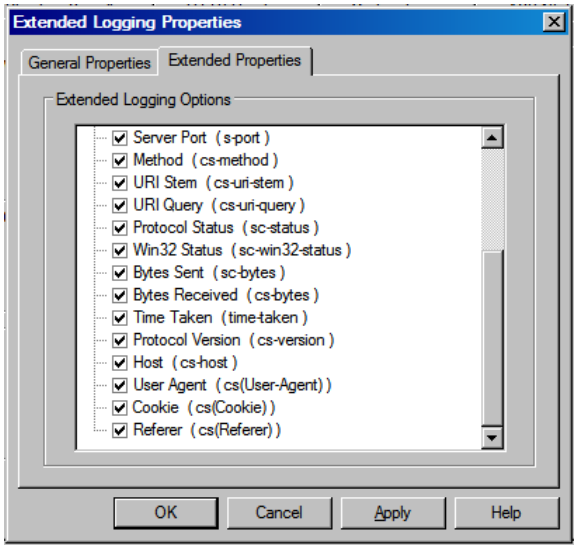


(**BEFORE**)

NOTE: Before changing the extended properties, write down or take snapshots of currently selected W3C properties in case of wanting to go back to the original state in the future.

5. On the Advanced tab (for Windows 2003 server) or Extended Properties tab (for Windows XP), select logging **ALL** properties.

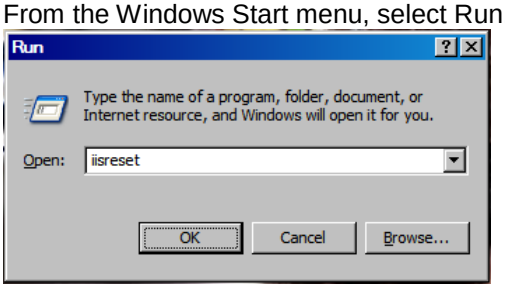




(**AFTER**)

6. Click OK and close IIS Manager.

7. From the Windows Start menu, select Run. Type: **iisreset** and then click OK to restart IIS.



8. IIS logs are located in the following directories:
    a. C:\WINDOWS\system32\LogFiles**W3SVC1** – for the Default Web site communication.
    b. C:\WINDOWS\system32\LogFiles**HTTPERR** – for IIS errors logs.

Enabling Logging in IIS (7.0)

IIS 7.0 (Which comes with Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista) does not automatically install the very valuable Logging Feature by Default.

From a Windows 7 machine you need to make sure that the feature is installed before you can begin viewing the files that it generates.

So in Control Panel>Programs and Features. Click "Turn Windows features on or off". Under.

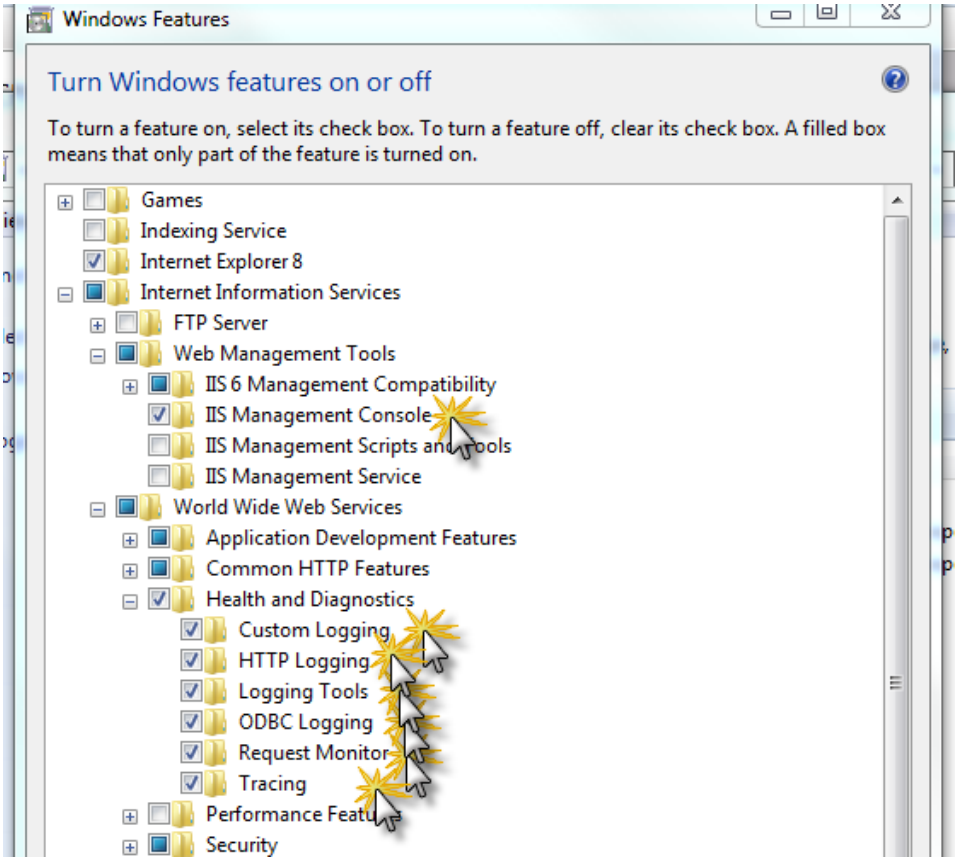
Internet Information Services

Web Management Tools

IIS Management Console, Tick this

World Wide Web Services

Health and Diagnostics, tick all options



Restart the web service (From a command line type IISRESET)

Vault Collaboration and Professional 2013 Multisite Replication

This section addresses topics specifically related to the unique environments associated with replicating data to multiple work sites.

Scalability of Replication

Replication uses a single database for all sites and replicates the file store to each location. This architecture has distinct advantages in ease of implementation, end user experience and the instantaneous nature of the information availability. This architecture is not suited to multiple sites that are distributed over great distances or poor networks. It is recommended that the replication environments are not distributed across multiple continents.

If you are unsure of the appropriateness of Replication in your environment you can easily estimate the performance. The performance can be gauged between two remote sites by browsing a network share between the sites. If the responsiveness of the remote share is deemed acceptable for daily access Replication should also be acceptable. Vault communicates via http which is more efficient than the default windows system which is observed when browsing a remote share.

Content Center in a Replicated Environment

Introduction

Autodesk Inventor Standard Content is delivered in the form of library databases that are hosted by the Autodesk Vault Server. Users access these library databases through Inventor to automatically create selected library components as Inventor part files. Once instanced these components are stored in a folder defined by the Inventor project file. When the assembly is then checked into Vault, the instanced Content components are also checked into Vault.

In a Replicated Autodesk Vault environment we can tune the performance of Content Center by altering the configuration of the Inventor project file.

Assumptions

The following examples assume all software including the Content has been installed. These examples also assume the reader has a functional understanding of how Content is instantiated and referenced. If required please reference the Content Center help files.

The following diagrams show the SQL server as a separate computer for clarity. SQL Server may be on a separate computer or on the Autodesk Vault Server, either case is supported and has no impact on the workflows detailed in this document.

Private Content Center Folder

The default configuration when using Inventor is for each client to have a private Content folder.

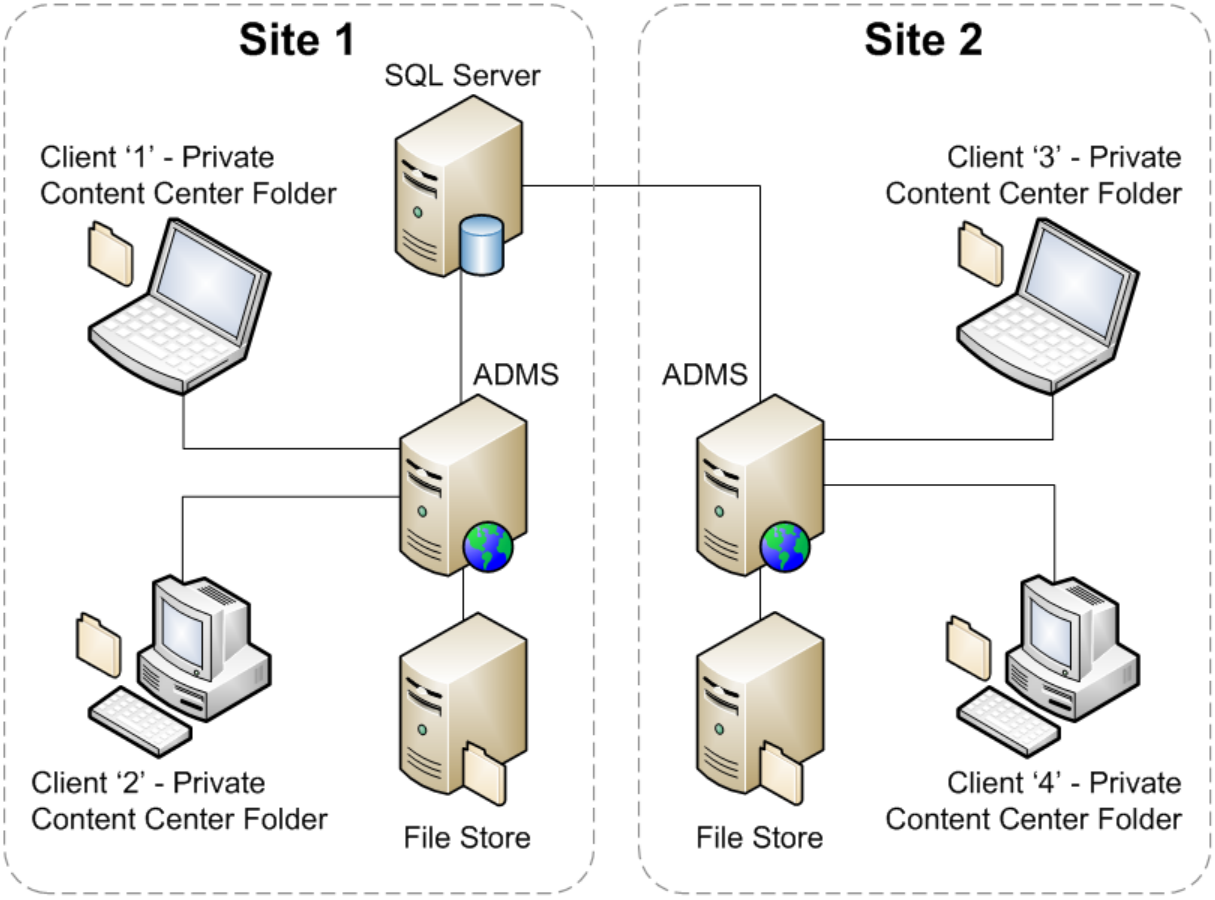
Advantages:

- Suitable for assemblies that have a high volume of Content components by eliminating network traffic for existing local components.
- Allows each user to have only the content they use in their Private Content Folder.

Disadvantages:

- Consumes considerable disk space on the client
- Each client must instantiate each referenced component in their Private Content Folder

Private Content Example

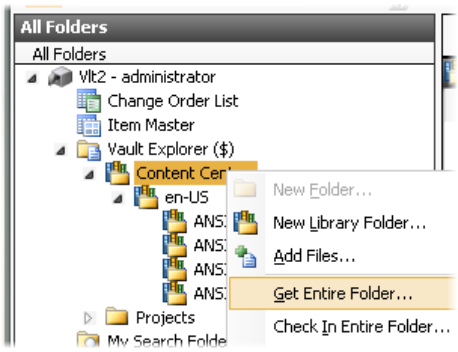


1. Client 1 creates an instance of a component from the Content Center database. The instanced part file is written to the Private Content Center folder located on the client computer.
2. User checks in the instanced component as part of an assembly. The Content part is copied into the Vault file store.

   Note: Keeping the part file in the local folder will remove the delays, for this user, due to instancing the part file or copying it from the file store.
3. Client 2 inserts the same component that Client 1 used. Since the part does not yet exist in the Private Content Center Folder for Client 2 it must be instanced from the database.
4. Once instanced the assembly may be checked into Vault. Vault knows that this component already exists and will resolve the assembly with the existing component in the file store.
5. During the scheduled replication at each Autodesk Vault Server the Content components will be copied to the local file store at each site.
6. Client 3 inserts the same component that Client 1 & 2 have previously used. The component must be instanced from the remote database. This is the same process as Client 2 in step 3 but the instantiation delay may be increased based upon the distance and network latency between the client and the SQL Server.

Seeding the Content Center Folders

The re-instancing of existing components can be avoided by performing a **Get Entire Folder** from the Vault thick client. This will seed the Content Center Folder with all instanced Content that has been checked into the Vault. This applies to both the Private and Shared Content Center Folders. In environments where new content is created frequently it may be advantages to perform this operation on regular basis.



Revision History

Revision	Comments	Date
1.1	Vault Server 2013 uses .NET 4.0, references to .NET 2.0 were removed. Removed references to IE7 Updated links for obtaining and installing SSL Certificates for IIS 6 and IIS 7 Updated SQL Express Maintenance plan	25/4/2012
1.2	Updated SQL Service pack level for SQL 2008 R2. Update SQL Maintenance Plans.	18/7/2012