# Deltek Vision® 6.1

# Deltek Vision 6.1 Document Management Installation Guide

March 30, 2010

13880 Dulles Corner Lane
Herndon VA 20171
TEL: 703.734.8606
FAX: 703.734.1146

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published March 2010.

# Contents

# Important Information for Users of Previous Versions of Deltek Vision Document Management

If you are upgrading from an earlier version of Vision, particularly from a 5.x version, note the following important information.

## WSS 2.0 Users

Deltek Vision 5.x and earlier versions supported Windows SharePoint Services 2.0, but Vision 6.x does not support WSS 2.0. If you have not yet upgraded your Windows SharePoint Services installation from WSS 2.0 to WSS 3.0, you must upgrade WSS as your first step. Refer to the *Deltek Vision 5.1 Document Management Upgrade Guide* for the necessary upgrade steps.

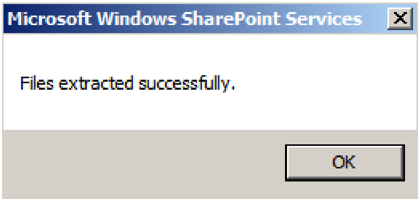
You must upgrade WSS before you implement Deltek Vision 6.1.

## Differences between Vision 5.1 and Vision 6.1 Document Management

The key differences between Vision 5.1 and Vision 6.1 Document Management are the following:

- Unlike Vision 5.1 with Windows SharePoint Services (WSS) 3.0, you cannot install WSS 3.0 to the same Web site as Vision 6.1 when using Windows Server 2008/IIS 7.0.
- During the Vision 6.1 Document Management installation, the WSS 3.0 setup files are extracted automatically.

  When the following dialog box is displayed, click **OK** to continue the Document Management installation.

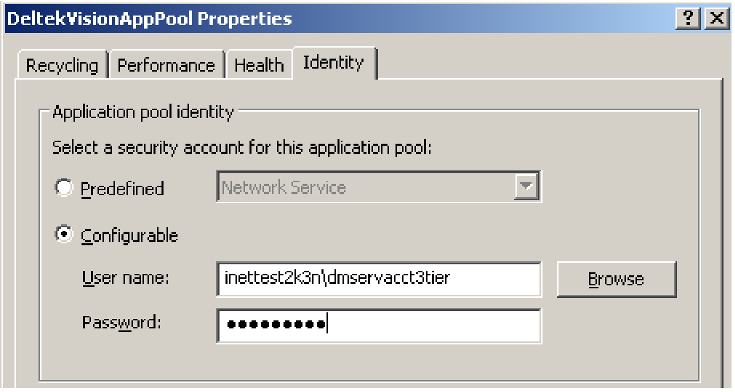
  Microsoft Windows SharePoint Services

  Files extracted successfully.

- With the Vision 5.1 Document Management installation, you had to configure the ASP .NET Impersonation Identity. This installation step is no longer necessary, because the Identity of the Application Pool performs this function in Vision 6.1. The installation of Vision 6.1 creates the DeltekVisionAppPool with the local DeltekVision account as the Identity.

The WSS Service account must be the Application Pool Identity for Vision 6.1 and a domain account, as shown in the following example dialog boxes:

**IIS 6.0 example:**



Application pool identity

Select a security account for this application pool:

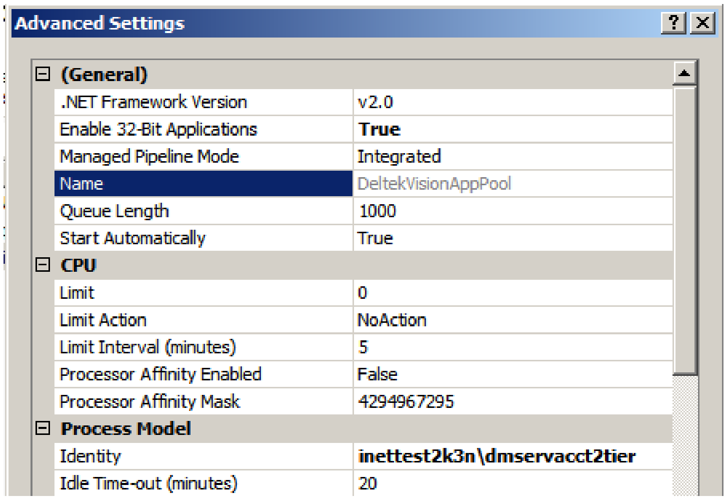
○ Predefined Network Service

● Configurable

User name: inettest2k3n\dmservacct3tier

Password: ●●●●●●●●●

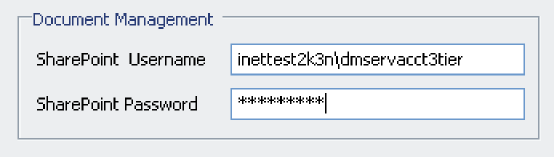
**IIS 7.0 example:**



| | |
|---|---|
| **(General)** | |
| .NET Framework Version | v2.0 |
| Enable 32-Bit Applications | **True** |
| Managed Pipeline Mode | Integrated |
| Name | DeltekVisionAppPool |
| Queue Length | 1000 |
| Start Automatically | True |
| **CPU** | |
| Limit | 0 |
| Limit Action | NoAction |
| Limit Interval (minutes) | 5 |
| Processor Affinity Enabled | False |
| Processor Affinity Mask | 4294967295 |
| **Process Model** | |
| Identity | **inettest2k3n\dmservacct2tier** |
| Idle Time-out (minutes) | 20 |

For this account to be the Application Pool Identity, it must be a member of the IIS_WPG group in IIS 6.0 and the IIS_IUSRS group in IIS7.0, in addition to being a member of the local administrators group for Vision.

- The WSS Service account credentials must be specified in Weblink System Settings, as shown in the following example of the Document Management setup fields.

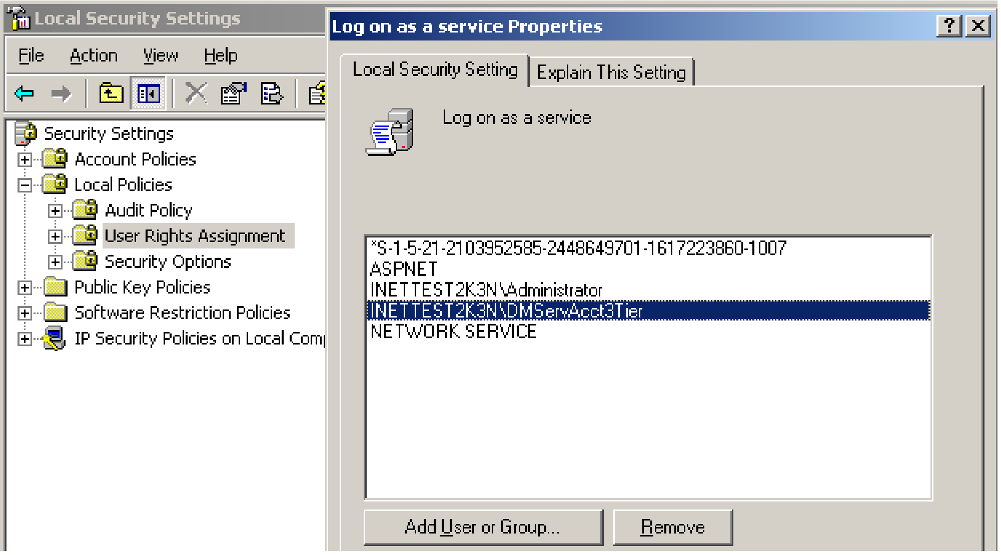


Document Management

SharePoint Username inettest2k3n\dmservacct3tier

SharePoint Password **********

- The WSS Service account must be granted **Logon as a service** rights on the Vision 6.1 Web/Application Server for multi-tier Document Management installations, as shown in the following example of the Local Security Settings setup screens.



*S-1-5-21-2103952585-2448649701-1617223860-1007
ASPNET
INETTEST2K3N\Administrator
INETTEST2K3N\DMServAcct3Tier
NETWORK SERVICE

- The configuration of Service Principal Names and Delegation has changed with Vision 6.1. Specifically, a Service Principal Name (SPN) must be configured for the domain account chosen to be the Vision 6.1 Application Pool Identity / WSS Service account only when deploying a multi-tier deployment of Vision Document Management when using Windows Server 2003/IIS 6.0. When using Windows Server 2008/IIS 7.0, there are three possible authentication configurations, only two of which require you to create an SPN for the Application Pool Identity. Refer to Appendix B for detailed information on the configuration options for Windows Server 2008/IIS 7.0.

  To add the Application Pool Identity as a Service Principal Name, do the following:

  1. Enter the following commands on the domain server where setspn is installed:

     **setspn –A http/<Vision Web/App Server name> <domain app pool identity>**

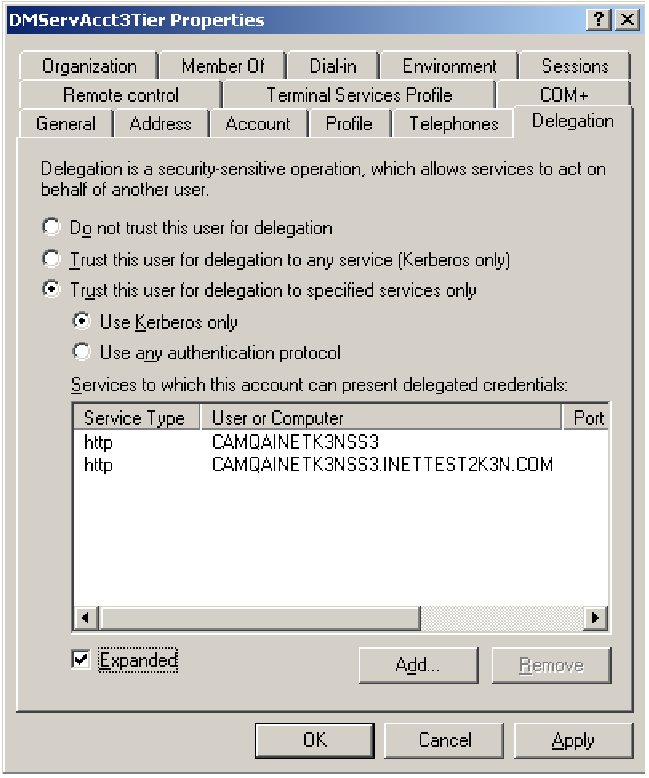
     For example: setspn –A http/camqainetk3nwb5 inettest2k3n\dmservacct3tier

  2. Repeat for the FQDN of the server.

  Refer to the following related Microsoft Knowledge Base article: http://support.microsoft.com/?id=871179

- In a multi-tier installation of Vision Document Management using IIS 7.0 for the Vision Web/Application server, the default configuration of Windows Integrated Authentication (which enables Kernel Mode Authentication) will not work because when you use Kernel Mode Authentication, the Application Pool Identity is effectively ignored. Because Vision requires that this account be used for delegation, you must either disable Kernel Mode Authentication or configure the application pool to explicitly use the Application Pool Identity by modifying the ApplicationHost.config file.

- In multi-tier installations of Vision Document Management, you must configure domain based delegation. This configuration has changed from Vision 5.1. It is now configured for this user account running the Vision 6.1 Application Pool being granted delegation rights to the WSS server. This configuration is shown in the following example of the Delegation tab of the Application Pool Identity Properties dialog box:



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port |
|---|---|---|
| http | CAMQAINETK3NSS3 | |
| http | CAMQAINETK3NSS3.INETTEST2K3N.COM | |

☑ Expanded

## Vision 5.1 to Vision 6.1 Document Management Upgrade

**To upgrade from Vision 5.1 Document Management to Vision 6.1 Document Management, complete these steps:**

1. Uninstall Deltek Vision 5.1 Document Management from Add/Remove Programs on your Deltek Vision Web server and any dedicated Document Management (WSS) servers.
2. Delete the old Deltek.Vision.WSS30.dll from \inetpub\bin or inetpub\virtual directories\wss\<port>\bin.
3. Uninstall the old Deltek.Vision.WSS30.dll from GAC (c:\windows\assembly).
4. Install Vision 6.1 Document Management.

## Vision 6.0 to Vision 6.1 Document Management Upgrade

**To upgrade from Vision 6.0 Document Management to Vision 6.1 Document Management, complete these steps:**

1. Run the Deltek Vision 6.1 installation to upgrade your Vision servers to Deltek Vision 6.1.
2. Run the Deltek Vision 6.1 Document Management installation to upgrade your Document Management server(s) to Deltek Vision 6.1 Document Management.

   **Note**: Run the upgrade on both your Vision and SharePoint servers if they are on different physical machines.

3. Update the Deltek Vision Document Management .NET assembly (Deltek.Vision.WSS30.Server.dll) in your SharePoint site \bin directory with the updated assembly located in <drive>:\Program Files\Deltek\Vision\Support\DM\3.0 folder.

# Important Information Regarding Windows Server 2008, IIS 7.0 and SQL Server 2008

## Windows Server 2008 Specific Information

If you will be installing Vision 6.1 Document Management on Windows Server 2008 / IIS 7.0, refer to Appendix B for detailed configuration information.

## SQL 2008 – Database Rights

If you will use SQL Server 2008 as the database server for your Vision 6.1 Document Management installation, note the following: WSS 3.0 is able to successfully add the domain SharePoint Service Account to the necessary SQL Server fixed server roles in SQL 2005. However, you must perform these grants manually with SQL 2008. The account must be added as a database login and granted securityadmin and dbcreator fixed server roles, as described in the following Technet article:

http://technet.microsoft.com/en-us/library/cc287748.aspx

# Vision Document Management Installation

## Vision Document Management Requirements

The Deltek Vision Document Management installation for Vision 6.1 has the following requirements:

- The Vision Web/Application and Microsoft SharePoint Web server(s) must be running Windows Server 2003 (x86 or x64) or Windows Server 2008 (x86 or x64).

> x64 for the Deltek Vision Web/Application server is only supported with the Deltek Vision 6.1 Sp2 and later versions.

- An Active Directory domain (Server 2003) is required and the domain functional level must be Native. Refer to Appendix A for how to identify and raise your domain functional level.

> Deltek has not as yet had an opportunity to test Windows Server 2008 domains.

- Internet Information Services (IIS) must be configured for Integrated Windows Authentication on both the Vision Web/Application server(s) and the Microsoft SharePoint Web server(s). A standard deployment of Vision supports either Anonymous Access (Vision Security) or Integrated Windows Authentication (Domain security), so this may be a change if you already have Vision deployed. The use of Integrated Security in IIS does not prohibit the use of Vision Security login accounts (for example, you don't have to configure all users in Vision for Integrated Security).

> There are additional Microsoft licensing requirements necessary to support the use of Integrated Windows Authentication with IIS. Specifically, a CAL (Client Access License) is required for each user that will access the IIS server (Vision).

- If you choose to install WSS 3.0 to the same Web site as Vision, (only supported if your Vision Web/Application/SharePoint server is Windows Server 2003/Internet Information Services (IIS) 6.0), the WSS installation will automatically cause all virtual directories in that site to use Integrated Windows Authentication. You must follow the steps below to reconfigure the VisionClient virtual directory to be Anonymous.

**To reconfigure the VisionClient directory, complete the following steps:**

1. Open Internet Information Services.
2. Right click the **VisionClient** virtual directory, and click **Properties** on the shortcut menu.
3. Click the Directory Security tab.
4. Click the **Edit** button under Anonymous Access and Authentication Control.
5. Clear the **Windows Integrated Authentication** option and select **Anonymous Access**.
6. Restart IIS.

# Understanding Infrastructure Configuration Changes

## Delegation and Kerberos Authentication

Delegation is the process of passing the credentials of the logged-in user from one server to another. In the case of Vision Document Management, they would pass from the Vision Web/Application server to the SharePoint server. In Vision 6.1, delegation is configured by modifying the domain user account of the Vision Application Pool Identity to perform delegation.

Kerberos Authentication is a secure key-based authentication protocol necessary for delegation to be performed. Essentially, the Vision Web Server needs to delegate the credentials of the authenticated domain user to the SharePoint server. The Vision Web server requests a key from the Key Distribution Center (KDC—a service which runs on domain controllers). The KDC authenticates the user and provides the key to the Vision Web Server for use in delegating the users' credentials to the SharePoint server.

## Constrained Delegation, Unconstrained Delegation, and Protocol Transition

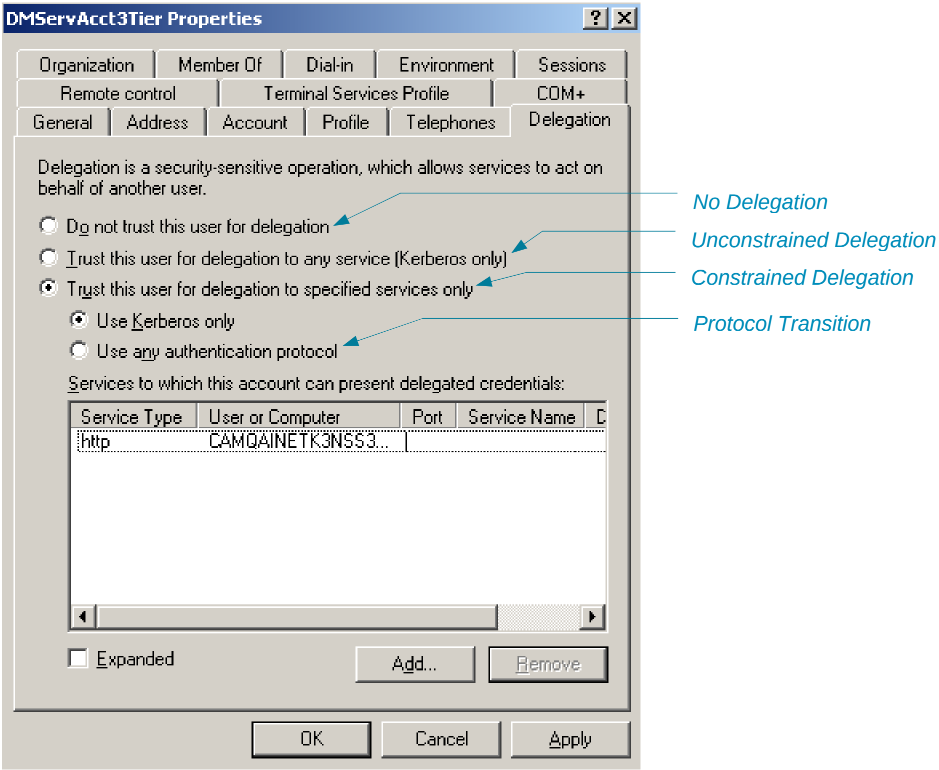
**Unconstrained Delegation** — You are allowing delegation from one computer in the domain to any other User/Computer or Service on the domain with no restrictions. This is the only model available in Windows 2000 and Windows 2003 Mixed domains.

Vision 6.1 with WSS 3.0 does not support Unconstrained Delegation.

**Constrained Delegation —** You are limiting the delegation that can be performed by a computer in the domain to a specific User/Computer or Service. This method of delegation is much more granular and secure and is only available in Server 2003 native domains.

**Protocol Transition** — This option allows you to transition the authentication protocol from the trusted server during the delegation. In the case of Vision Document Management in an Internet deployment, we have the need to transition the protocol from NTLM (as Kerberos is not available through the firewall) on the Vision Web server to Kerberos when communicating to the SharePoint server. This is necessary for Internet deployments because the client must negotiate the Kerberos ticket. This would require that Port 88 be open inbound through the firewall to the domain controller (not an advisable security configuration). The ticket is requested by the Vision Web server on the client's behalf and once granted, it is used to authenticate the user with Kerberos to the WSS server. Again, this option is only available in Server 2003 Native domains.

Windows 2000 Native or Mixed Mode domains have the option on the General tab of the Computer account properties labeled **Trust Computer for Delegation**. The following screen shot is of a computer account in a native Server 2003 functional domain that allows us to show all of the available Delegation and protocol transition configurations.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

- ● Use Kerberos only
- ○ Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | D |
|---|---|---|---|---|
| http | CAMQAINETK3NSS3... | | | |

□ Expanded

*No Delegation*

*Unconstrained Delegation*

*Constrained Delegation*

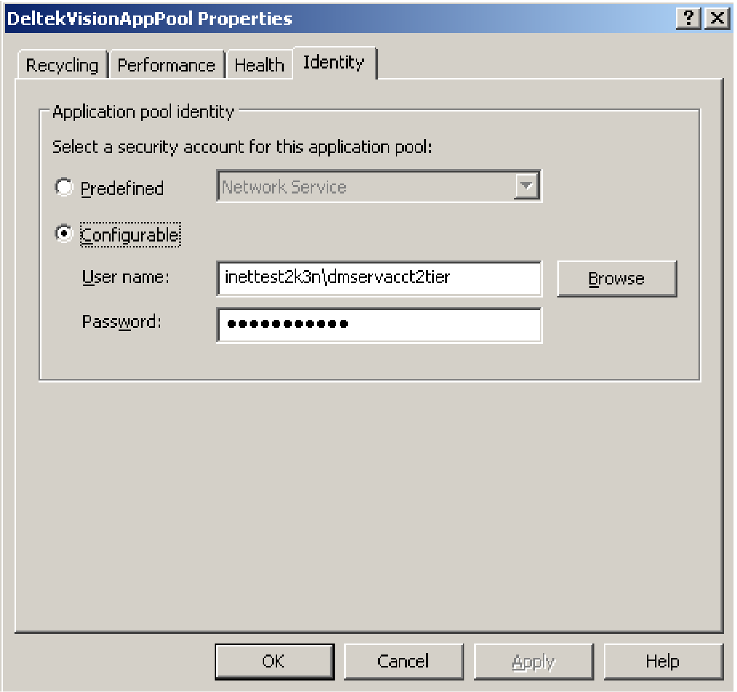
*Protocol Transition*

## Vision Application Pool Identity

With the Vision 5.1 Document Management installation, you had to configure the ASP .NET Impersonation Identity using the Deltek Vision Resource Kit. This installation step is no longer necessary, because the identity of the Application Pool performs this function in Vision 6.1. The installation of Vision 6.1 creates the DeltekVisionAppPool with the local DeltekVision account as the Identity.

The WSS Service account must be the Application Pool Identity for Vision 6.1 and a domain account, as shown in the following example dialog boxes:

**IIS 6.0 example:**



Application pool identity

Select a security account for this application pool:

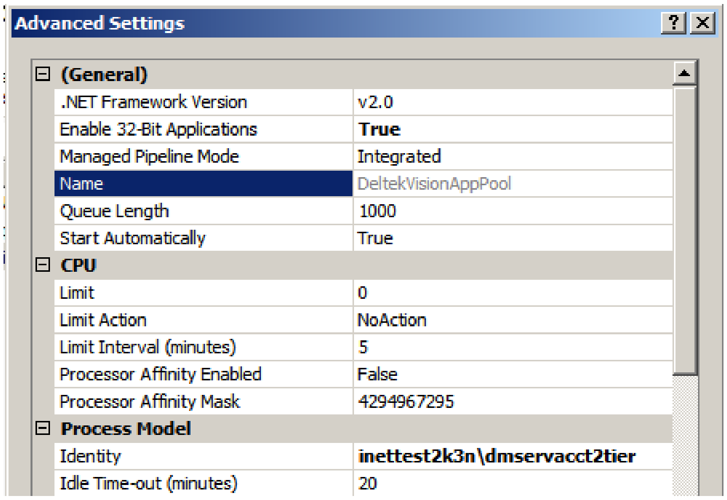
○ Predefined: Network Service

● Configurable

User name: inettest2k3n\dmservacct2tier

Password: ●●●●●●●●●●●●

**IIS 7.0 example:**



| | |
|---|---|
| ⊟ **(General)** | |
| .NET Framework Version | v2.0 |
| Enable 32-Bit Applications | **True** |
| Managed Pipeline Mode | Integrated |
| Name | DeltekVisionAppPool |
| Queue Length | 1000 |
| Start Automatically | True |
| ⊟ **CPU** | |
| Limit | 0 |
| Limit Action | NoAction |
| Limit Interval (minutes) | 5 |
| Processor Affinity Enabled | False |
| Processor Affinity Mask | 4294967295 |
| ⊟ **Process Model** | |
| Identity | **inettest2k3n\dmservacct2tier** |
| Idle Time-out (minutes) | 20 |

For this account to be the Application Pool Identity, it must be a member of the IIS_WPG group in IIS 6.0 and the IIS_IUSRS group in IIS7.0, in addition to being a member of the local administrators group for Vision.

## Service Principal Name (SPN)

In addition to the information provided earlier in this document about the SPN needed for the Vision Application Pool Identity, below are some additional instances where SPNs may need to be configured for your Document Management deployment.

If you are using or will be using a custom Fully Qualified Domain Name (FQDN) as your SharePoint URL (for example, http://sharepoint.company.com, where "sharepoint" is a custom DNS record added to avoid using the actual machine name of the server) and your deployment model requires the configuration of Constrained Delegation, you will need to register the custom FQDN using the Service Principal Name utility (setspn.exe) so that it can be configured for Constrained Delegation or Protocol Transition.

Additionally, when deploying Microsoft Office SharePoint Server (MOSS) 2007, the application pool identity for the SharePoint Web application defaults to a domain account. If your SharePoint Application Pool Identity is a domain account (as opposed to Network Service, which is the default for Windows SharePoint Services 3.0), you will need to create SPNs for this account as identified in the following Microsoft Support article (http://support.microsoft.com/?id=871179).

## Modifications to IIS Metabase

The IIS metabase contains the information on the authentication methods that IIS supports. For Document Management, the options are the following:

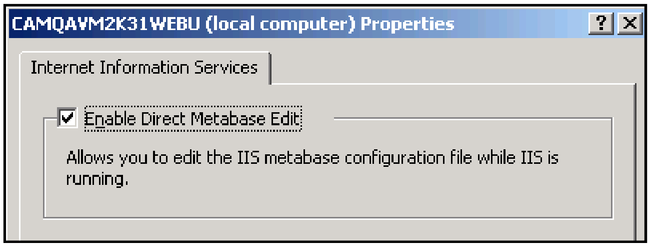
- **Negotiate**, which requires Kerberos
- **NTLM**, which uses NTLM

These options are located in the NTAuthenticationProviders element in the IISWebServer tag as shown in the following example:

```
<IIsWebServer Location="/LM/W3SVC/1"
AppPoolId="DefaultAppPool"
DefaultDoc="Default.htm,Default.asp,index.htm,iisstart.htm,
Default.aspx"
NTAuthenticationProviders="Negotiate,NTLM"
ServerAutoStart="TRUE"
ServerBindings=":80:"
ServerComment="Default Web Site"
ServerSize="1"
>
</IIsWebServer>
```

> The Vision Document Management installation adds the NTAuthenticationProviders element to use both Negotiate and NTLM.

By default, an installation of IIS 6.0 does not include the NTAuthenticationProviders element in the metabase for IIS to use, so all communication defaults to NTLM as the authentication mechanism. In order to edit the metabase.xml file, you need to go into the IIS server properties and select the **Enable Direct Metabase Edit** check box, which allows you to make the change and for it to be dynamic (for example, no need to restart the Web server).


CAMQAVM2K31WEBU (local computer) Properties
Internet Information Services

☑ Enable Direct Metabase Edit

Allows you to edit the IIS metabase configuration file while IIS is running.

Refer to Appendix B for information on the changes needed for the IIS 7.0 configuration file (applicationhost.config) that replaces the IIS 6.0 Metabase.

## Document Management Supported Deployments and Required Infrastructure Configuration Changes

Use the table on the next page to identify necessary infrastructure configuration changes based on your domain and chosen deployment model. The steps necessary to implement those configuration changes are outlined in the "Installation and Configuration" section for your deployment scenario.

| Document Management Supported Deployments and Required Configuration Changes | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Windows SharePoint Services 3.0 (2007) | | | | | | | | |
| Windows Server 2003 Native Domains | | | | Required Configuration Changes | | | Required Delegation | |
| **Deploy-ment Model** | **DM Tier Model** | **Domain Functional Level** | **Deltek Vision URL** | **Set SPN for SharePoint Web Server** | **Use Domain Application Pool Identity (Note 1)** | **IIS Metabase Settings (Note 2)** | **Configure Constrained Delegation (Note 3)** | **Configure Protocol Transition (Note 4)** |
| Intranet | Single | 2003 Native | NETBIOS | No | | Negotiate, NTLM | No | No |
| Intranet | Multi | 2003 Native | NETBIOS | No | Yes | Negotiate, NTLM | Yes | No |
| Intranet | Single | 2003 Native | Servername FQDN | No | Yes | Negotiate, NTLM | No | No |
| Intranet | Multi | 2003 Native | Servername FQDN | No | Yes | Negotiate, NTLM | Yes | No |
| Intranet | Single | 2003 Native | Custom FQDN | Yes | Yes | Negotiate, NTLM | No | No |
| Intranet | Multi | 2003 Native | Custom FQDN | Yes | Yes | Negotiate, NTLM | Yes | No |
| Internet | Single | 2003 Native | Servername FQDN | No | Yes | Negotiate, NTLM | No | No |
| Internet | Multi | 2003 Native | Servername FQDN | No | Yes | Negotiate, NTLM | No | Yes |
| Internet | Single | 2003 Native | Custom FQDN | Yes | Yes | Negotiate, NTLM | No | Yes |
| Internet | Multi | 2003 Native | Custom FQDN | Yes | Yes | Negotiate, NTLM | No | Yes |

**Note 1**: Domain account used for Vision Application Pool Identity must be the SharePoint Services account.

**Note 2**: The Document Management installation is automatically configuring this property.

**Note 3**: Constrained delegation must be configured for **all** multi-tier deployments of Document Management.

**Note 4**: Protocol transition is only required for Internet deployments of Document Management.

# Single Server — New Installation of Document Management 6.1

The following instructions assume that Vision and Windows SharePoint Services 3.0 will exist on the same Web server and assume you are deploying to Windows Server 2003/IIS 6.0. If you will be deploying to Windows Server 2008/IIS 7.0, refer to Appendix B for detailed configuration information.

> Vision and MOSS 2007 are not supported on the same physical server.

If your Windows SharePoint Services server is separate, use the multi-tier installation procedures beginning on page 41.

## Prerequisites

- Install/upgrade to Vision 6.1.
- Change the Application Pool Identity for the DeltekVisionAppPool to be a domain account (the Vision 6.1 installation sets this to be the local DeltekVision account). This account will also be the SharePoint (WSS) Service account. Add this user to the local Administrators and IIS_WPG group on the Vision server.

## Configure Vision Application Pool Identity to be a Domain Account

You must change the Deltek Vision Application Pool Identity to be a domain account. The default is for Vision to use a Local Administrator Account. The DeltekVision user is created during the Vision installation. The reason for this change has to do with the local account's inability to read the SPN configured in Active Directory.

**To change the Vision Application Pool Identity, complete the following steps:**

1. Create a domain user account. No domain Admin rights are needed for this account.
2. Log on to the domain on the Vision Web/Application server using an Administrator account.
3. **Start » All Programs » Administrative Tools » Internet Information Services.**.
4. Expand **Application Pools**.
5. Right-click the **DeltekVisionAppPool** and select **Properties**.
6. Click the Identity tab and change the account from DeltekVision to your Domain\User account created above. Make sure this account is a member of the Local Administrators and IIS_WPG local groups.

## Configure SPN for Vision Application Pool Identity

As mentioned earlier in this document, it is necessary to create a Service Principal Name (SPN) for the domain user running the DeltekVisionAppPool.

**To add the Application Pool Identity as a Service Principal Name, complete the following steps:**

1. Enter the following commands on the domain server where setspn is installed:

   **setspn –A http/<Vision Web/App Server name> <domain app pool identity>**

   For example: **setspn –A http/camqainetk3nwb5 inettest2k3n\dmservacct3tier**

2. Repeat for the FQDN of the server.

Refer to the following related Microsoft Knowledge Base article:

http://support.microsoft.com/?id=871179

> If your Vision Web server is accessed by a DNS / FQDN (Fully Qualified Domain Name) that *does not match* the name of the server (for example, if your Vision Web server is named Server01 and its DNS name is Server01.Company.com, but you have added a custom DNS value Vision.Company.com), you must also add an SPN for this custom DNS name.

## Install and Configure Vision 6.1 Document Management and WSS 3.0

When you install Vision 6.1 Document Management, WSS is automatically installed. (If you are upgrading from Vision 5.1 or already have WSS installed, no changes are made to your WSS installation.) However, the Document Management installation will not automatically configure WSS. The steps to configure SharePoint are outlined in this document.

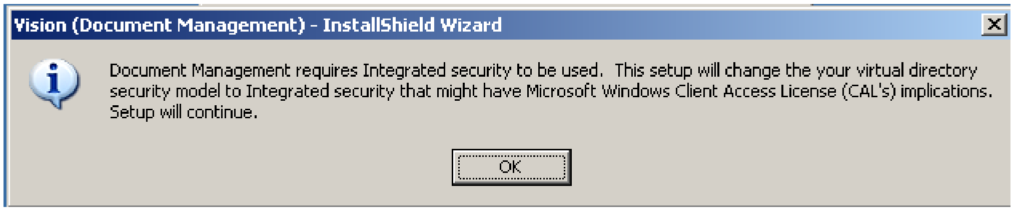
The Document Management installation does the following:

- Installs Web Service Extensions (WSE) 2.0 Sp3.
- Installs WSS 3.0, if it is not already installed.
- Changes the IIS metabase NTAuthenticationProviders element to be “Negotiate,NTLM”.
- Copies Document Management files to the SharePoint ISAPI folder (c:\program files\common files\microsoft shared\web service extensions\12\isapi).
- Copies Document Management files to the Vision Support folder (\program files\deltek\vision\support\DM\30).
- Modifies the SharePoint Web.config file in the ISAPI directory to work with Vision Document Management.
- Installs Deltek.Vision.WSS30.Server dll into the Global Assembly Cache (GAC).

### Install Vision Document Management and WSS

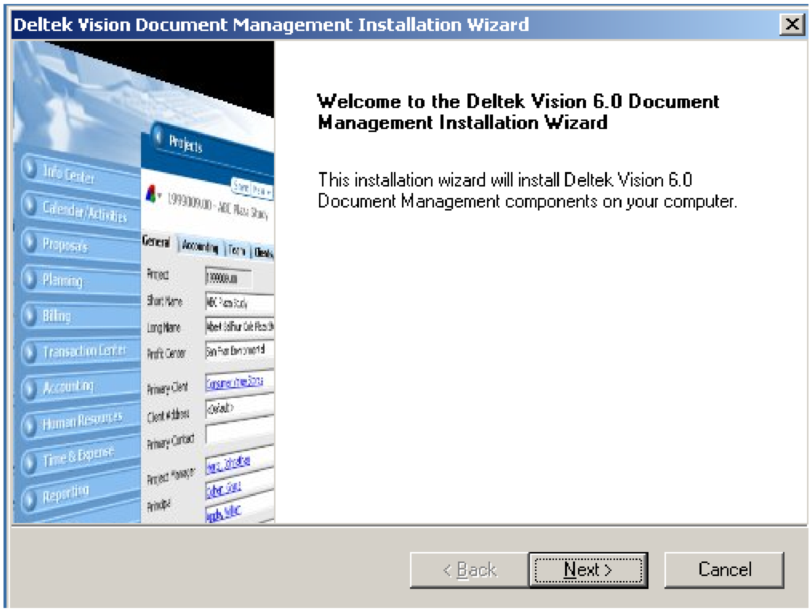
**To install Vision Document Management and WSS, complete the following steps:**

1. If you have previously installed Deltek Vision 5.1 Document Management (or other previous versions), uninstall Deltek Vision Document Management from Add/Remove Programs. (This will not uninstall Windows SharePoint Services 3.0.)
2. Download the DeltekVision61DM.exe file and run the setup on your Vision Web server. The following dialog box displays, indicating the IIS licensing requirements for the use of Windows Integrated Authentication (required to use Vision Document Management):



Document Management requires Integrated security to be used. This setup will change the your virtual directory security model to Integrated security that might have Microsoft Windows Client Access License (CAL's) implications. Setup will continue.

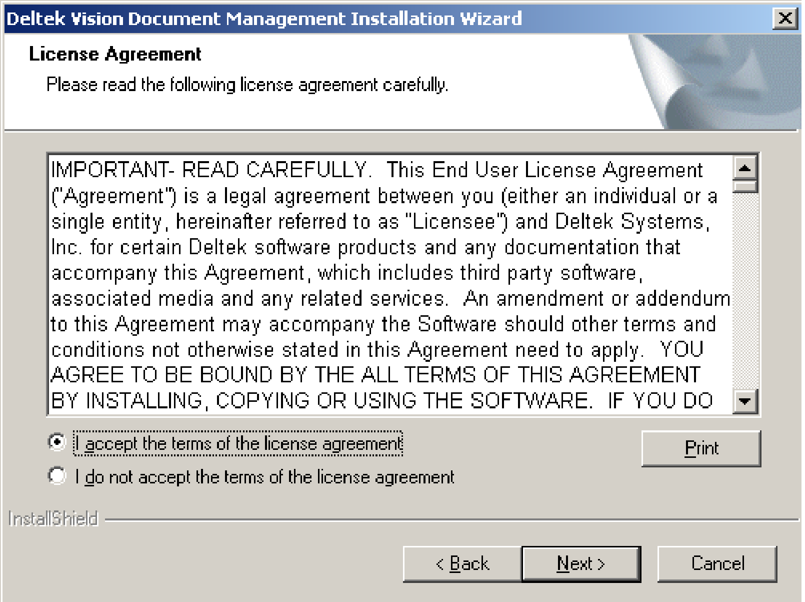
3. Click **OK**. The Document Management Installation Wizard displays.



**Welcome to the Deltek Vision 6.0 Document Management Installation Wizard**

This installation wizard will install Deltek Vision 6.0 Document Management components on your computer.

4. Click **Next**. The License Agreement page displays.



**License Agreement**

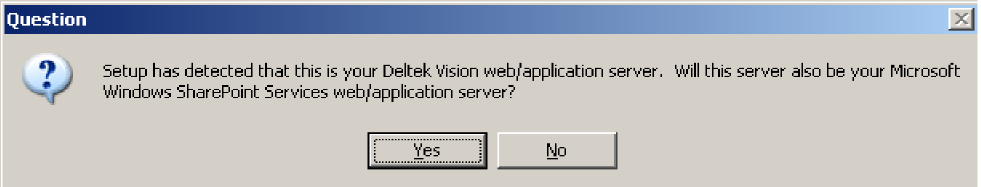
Please read the following license agreement carefully.

IMPORTANT- READ CAREFULLY. This End User License Agreement ("Agreement") is a legal agreement between you (either an individual or a single entity, hereinafter referred to as "Licensee") and Deltek Systems, Inc. for certain Deltek software products and any documentation that accompany this Agreement, which includes third party software, associated media and any related services. An amendment or addendum to this Agreement may accompany the Software should other terms and conditions not otherwise stated in this Agreement need to apply. YOU AGREE TO BE BOUND BY THE ALL TERMS OF THIS AGREEMENT BY INSTALLING, COPYING OR USING THE SOFTWARE. IF YOU DO

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

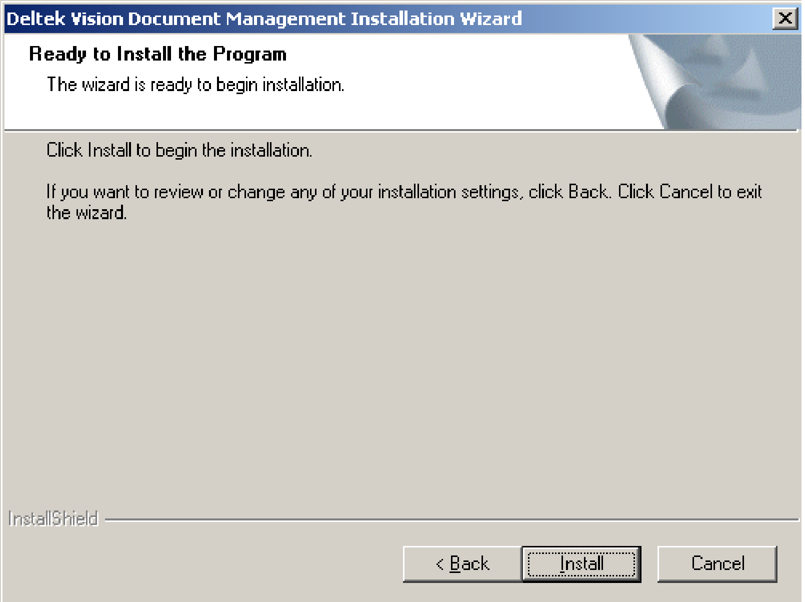
5. Accept the License Agreement and click **Next**. The Web/application server page displays, along with the following confirmation dialog box.



Question

Setup has detected that this is your Deltek Vision web/application server. Will this server also be your Microsoft Windows SharePoint Services web/application server?

6. Click **Yes** since this is a single-tier installation of Vision Document Management and this server will host both Vision and WSS 3.0. The Ready to Install the Program page displays.



Deltek Vision Document Management Installation Wizard

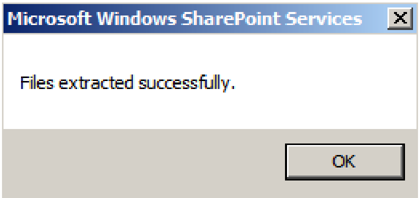
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

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

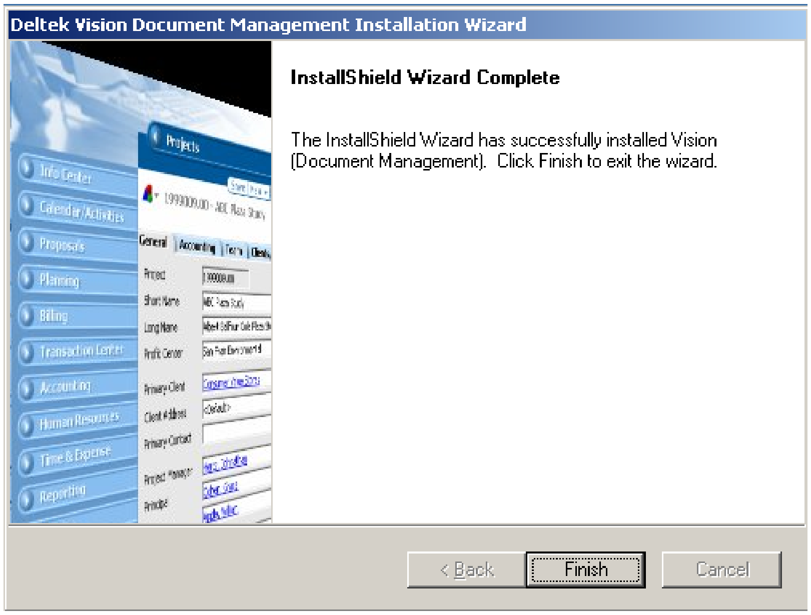
7. Click **Install** to start the installation. The installation automatically downloads the version of Windows SharePoint Services 3.0 specific to your platform (x86 or x64), extracts the WSS 3.0 setup files, and installs Windows SharePoint Services. During the extraction process, you receive the following dialog box. You must click the **OK** button to continue the installation.



Microsoft Windows SharePoint Services

Files extracted successfully.

8. When the installation is complete, the InstallShield Wizard Complete page displays.



Deltek Vision Document Management Installation Wizard

**InstallShield Wizard Complete**

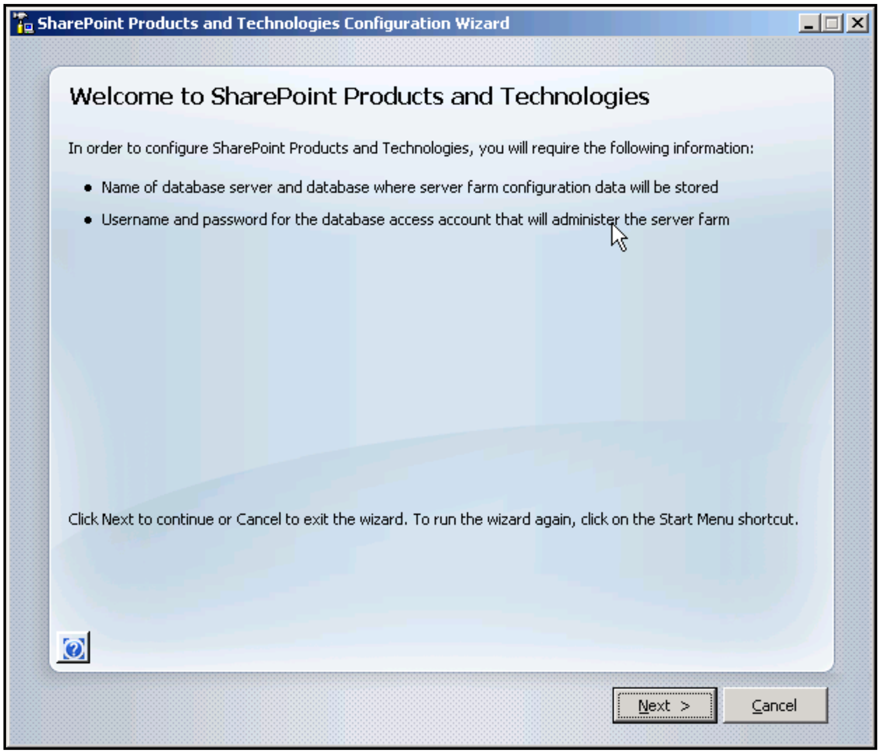
The InstallShield Wizard has successfully installed Vision (Document Management). Click Finish to exit the wizard.

9. Click **Finish**.

## Run the SharePoint Products and Technologies Configuration Wizard

### To run the SharePoint Products and Technologies Configuration wizard, complete the following steps:

1. Click **Start » Administrative Tools » SharePoint Products and Technologies Wizard**. The Welcome page displays.



SharePoint Products and Technologies Configuration Wizard

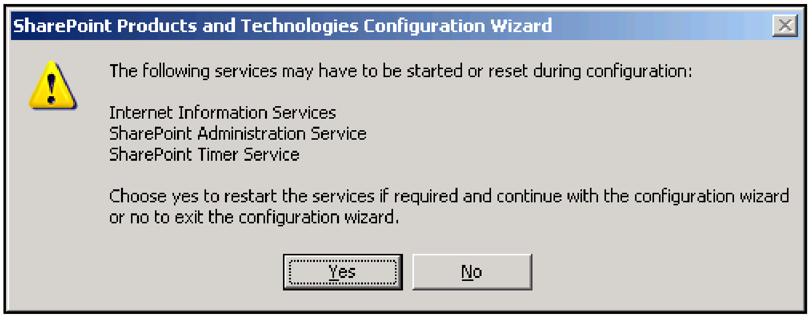
Welcome to SharePoint Products and Technologies

In order to configure SharePoint Products and Technologies, you will require the following information:

- Name of database server and database where server farm configuration data will be stored
- Username and password for the database access account that will administer the server farm

Click Next to continue or Cancel to exit the wizard. To run the wizard again, click on the Start Menu shortcut.

2. Click **Next**. The following dialog box displays.



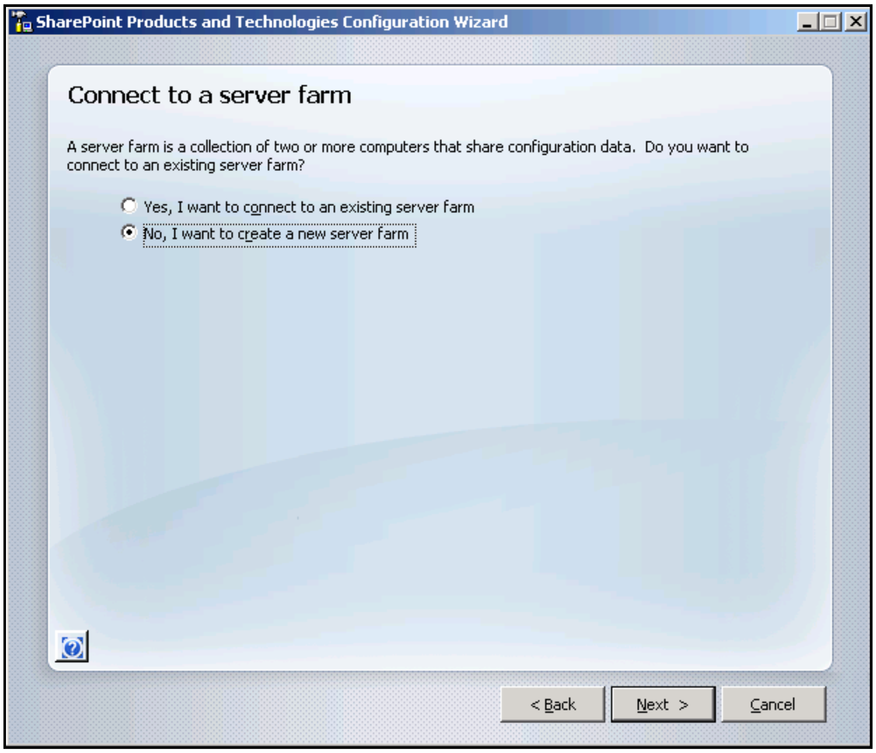
SharePoint Products and Technologies Configuration Wizard

The following services may have to be started or reset during configuration:

Internet Information Services
SharePoint Administration Service
SharePoint Timer Service

Choose yes to restart the services if required and continue with the configuration wizard or no to exit the configuration wizard.

3. Click **Yes**. The Connect to a server farm page displays.



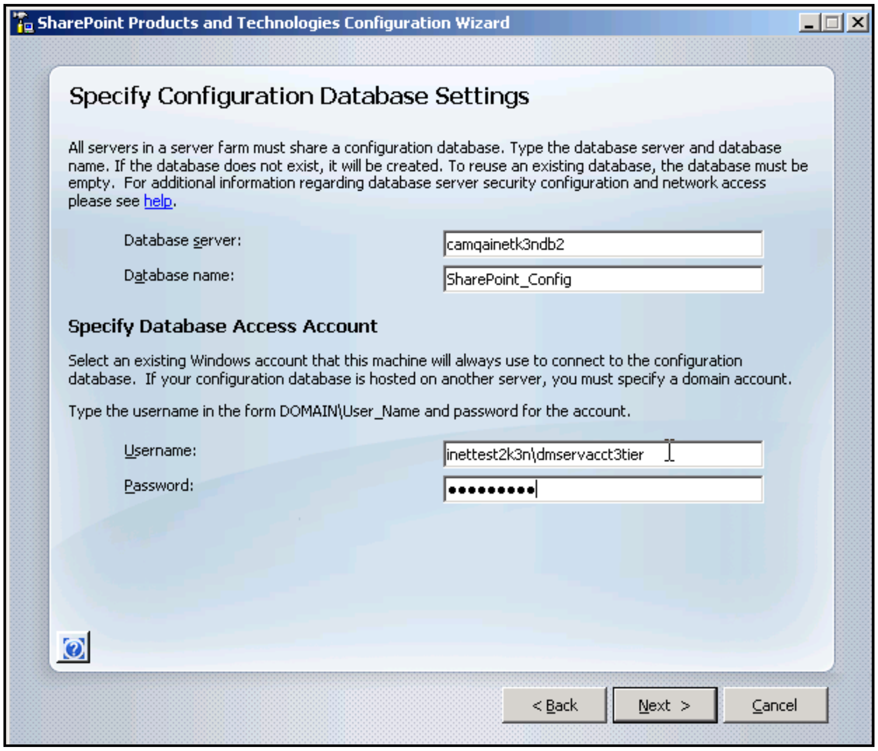
SharePoint Products and Technologies Configuration Wizard

Connect to a server farm

A server farm is a collection of two or more computers that share configuration data. Do you want to connect to an existing server farm?

○ Yes, I want to connect to an existing server farm
● No, I want to create a new server farm

4. Select the **No, I want to create a new server farm** option and click **Next**. The Specify Configuration Database Settings page displays.



Specify Configuration Database Settings

All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must be empty. For additional information regarding database server security configuration and network access please see help.

Database server: camqainetk3ndb2

Database name: SharePoint_Config

Specify Database Access Account

Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account.

Type the username in the form DOMAIN\User_Name and password for the account.

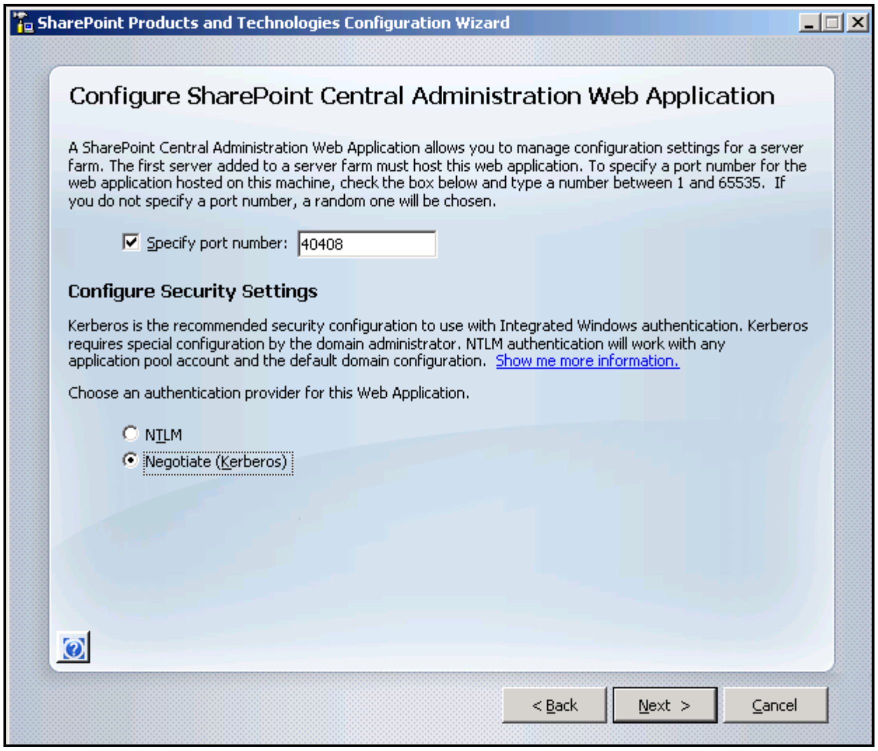
Username: inettest2k3n\dmservacct3tier

Password: ●●●●●●●●●

5. Enter the name of the database server to host the SharePoint configuration database and accept the default database name: SharePoint_Config.

> If you are using SQL Server 2008, refer to Appendix B on page 93 for configuration requirements before proceeding.

6. In **Username**, enter the domain and name of the Vision Application Pool Identity (as configured earlier) as the username for the SharePoint database access account, and enter the user’s password in **Password**.
7. Click **Next**. The Configure SharePoint Central Administration Web Application page displays.



Configure SharePoint Central Administration Web Application

A SharePoint Central Administration Web Application allows you to manage configuration settings for a server farm. The first server added to a server farm must host this web application. To specify a port number for the web application hosted on this machine, check the box below and type a number between 1 and 65535. If you do not specify a port number, a random one will be chosen.

☑ Specify port number: 40408

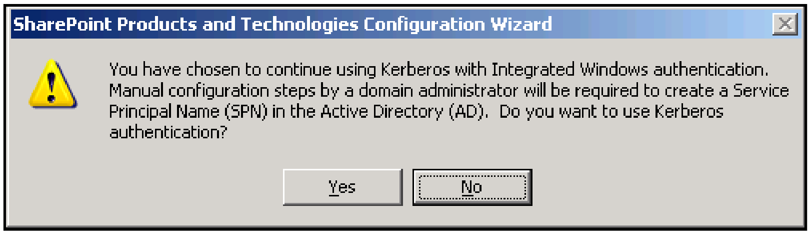
Configure Security Settings

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration. Show me more information.

Choose an authentication provider for this Web Application.

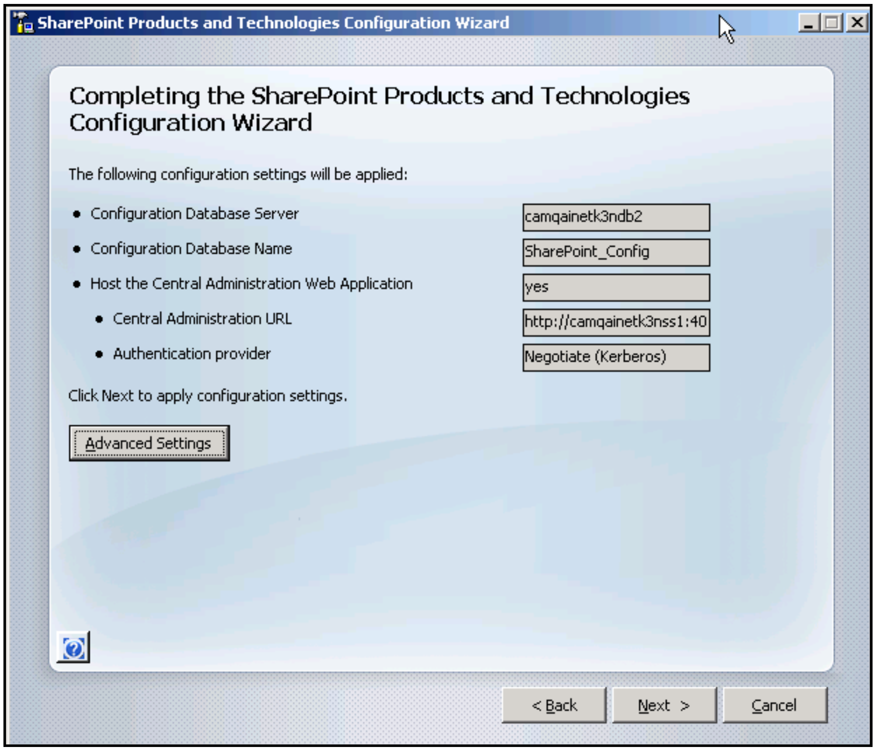
○ NTLM
● Negotiate (Kerberos)

8. Select the **Specify port number** check box and enter the port to be used for the SharePoint Central Administration Web site.
9. Select the **Negotiate (Kerberos)** option for the Authentication provider to use.
10. Click **Next**. The following dialog box displays.



You have chosen to continue using Kerberos with Integrated Windows authentication. Manual configuration steps by a domain administrator will be required to create a Service Principal Name (SPN) in the Active Directory (AD). Do you want to use Kerberos authentication?

11. Click **Yes** to continue using Kerberos with Windows Authentication. The Completing the SharePoint Products and Technologies Configuration Wizard page displays.



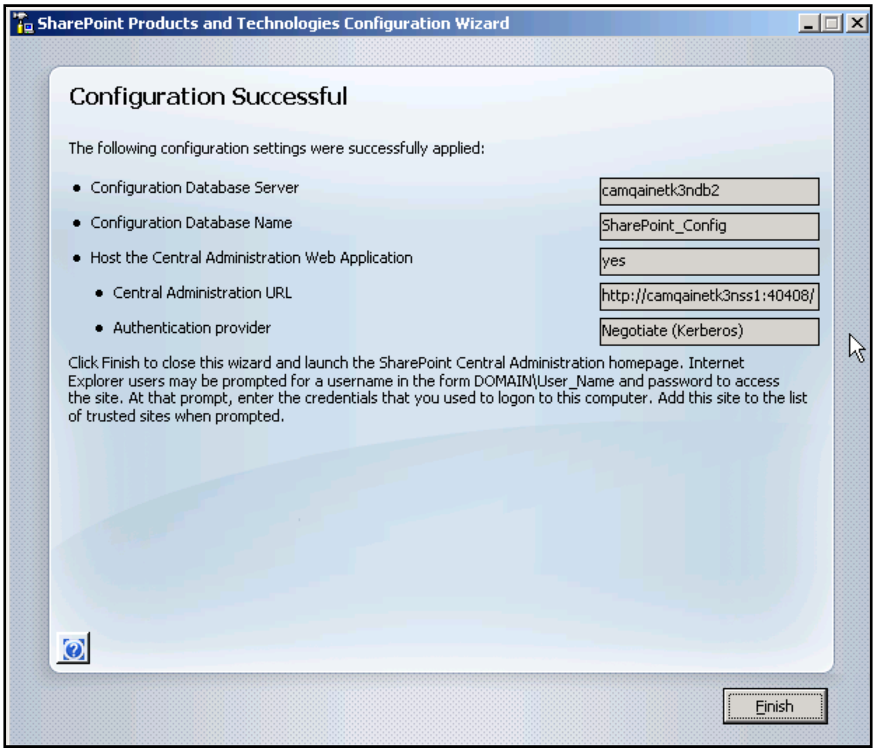
Completing the SharePoint Products and Technologies Configuration Wizard

The following configuration settings will be applied:

- Configuration Database Server: camqainetk3ndb2
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
  - Central Administration URL: http://camqainetk3nss1:40
  - Authentication provider: Negotiate (Kerberos)

Click Next to apply configuration settings.

12. Click **Next** to begin the configuration. This process may take some time to complete. The Configuration Successful page displays when configuration is complete.



Configuration Successful

The following configuration settings were successfully applied:

- Configuration Database Server: camqainetk3ndb2
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
  - Central Administration URL: http://camqainetk3nss1:40408/
  - Authentication provider: Negotiate (Kerberos)

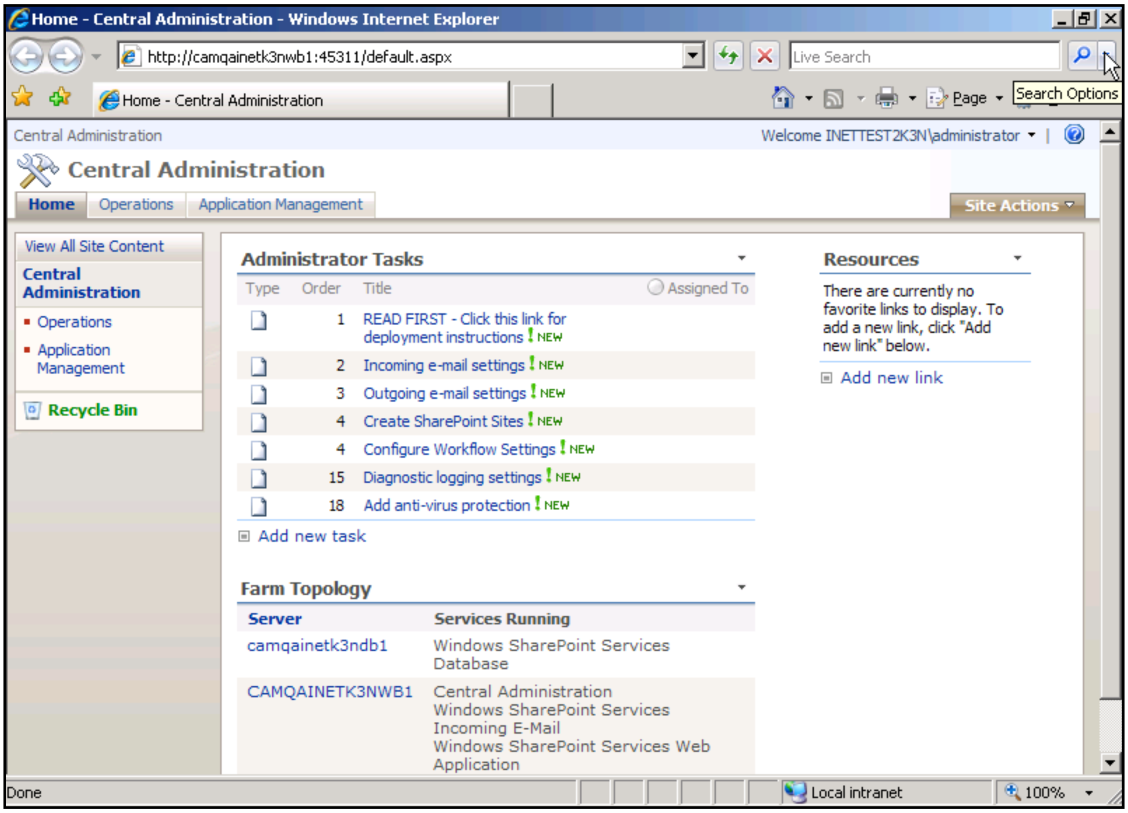
Click Finish to close this wizard and launch the SharePoint Central Administration homepage. Internet Explorer users may be prompted for a username in the form DOMAIN\User_Name and password to access the site. At that prompt, enter the credentials that you used to logon to this computer. Add this site to the list of trusted sites when prompted.

13. Click **Finish** to finish the configuration process. The SharePoint Central Administration page displays.

# Use SharePoint Central Administration to Complete the SharePoint Configuration

**To complete the SharePoint Configuration, complete the following steps:**

1. When you click **Finish** in the preceding procedure, SharePoint Central Administration is launched.



Administrator Tasks

| Type | Order | Title | Assigned To |
|---|---|---|---|
| | 1 | READ FIRST - Click this link for deployment instructions ! NEW | |
| | 2 | Incoming e-mail settings ! NEW | |
| | 3 | Outgoing e-mail settings ! NEW | |
| | 4 | Create SharePoint Sites ! NEW | |
| | 4 | Configure Workflow Settings ! NEW | |
| | 15 | Diagnostic logging settings ! NEW | |
| | 18 | Add anti-virus protection ! NEW | |

Add new task

Farm Topology

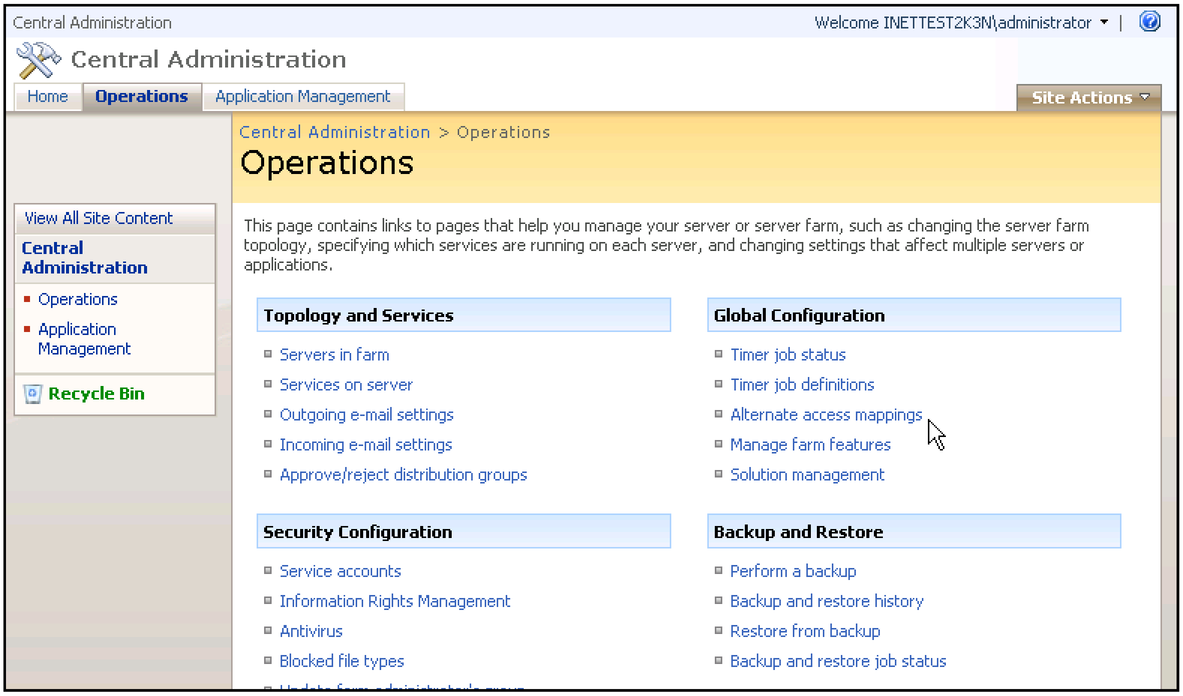
| Server | Services Running |
|---|---|
| camqainetk3ndb1 | Windows SharePoint Services Database |
| CAMQAINETK3NWB1 | Central Administration<br>Windows SharePoint Services Incoming E-Mail<br>Windows SharePoint Services Web Application |

Resources

There are currently no favorite links to display. To add a new link, click "Add new link" below.

Add new link

2. Click **Operations**. The Operations page displays.



Central Administration > Operations

Operations

This page contains links to pages that help you manage your server or server farm, such as changing the server farm topology, specifying which services are running on each server, and changing settings that affect multiple servers or applications.

**Topology and Services**

- Servers in farm
- Services on server
- Outgoing e-mail settings
- Incoming e-mail settings
- Approve/reject distribution groups

**Global Configuration**

- Timer job status
- Timer job definitions
- Alternate access mappings
- Manage farm features
- Solution management

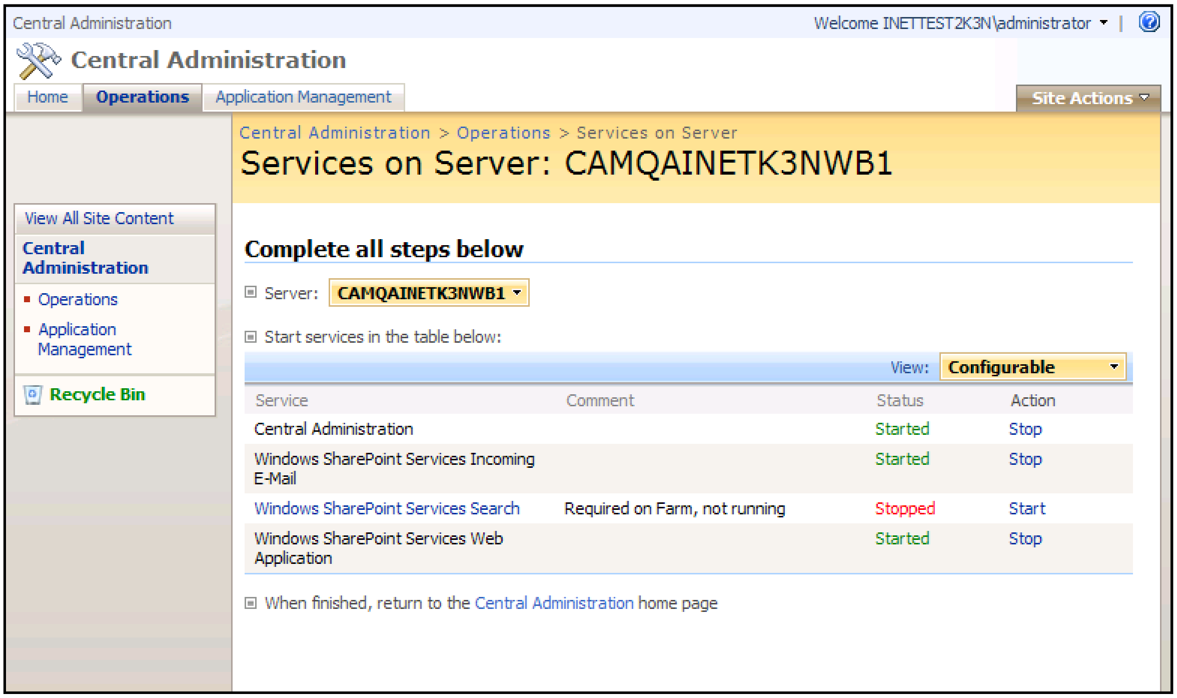
**Security Configuration**

- Service accounts
- Information Rights Management
- Antivirus
- Blocked file types
- Update farm administrator's group

**Backup and Restore**

- Perform a backup
- Backup and restore history
- Restore from backup
- Backup and restore job status

3. Click **Services on Server** under **Topology and Services** to configure the SharePoint Services search.



Central Administration > Operations > Services on Server

Services on Server: CAMQAINETK3NWB1

**Complete all steps below**

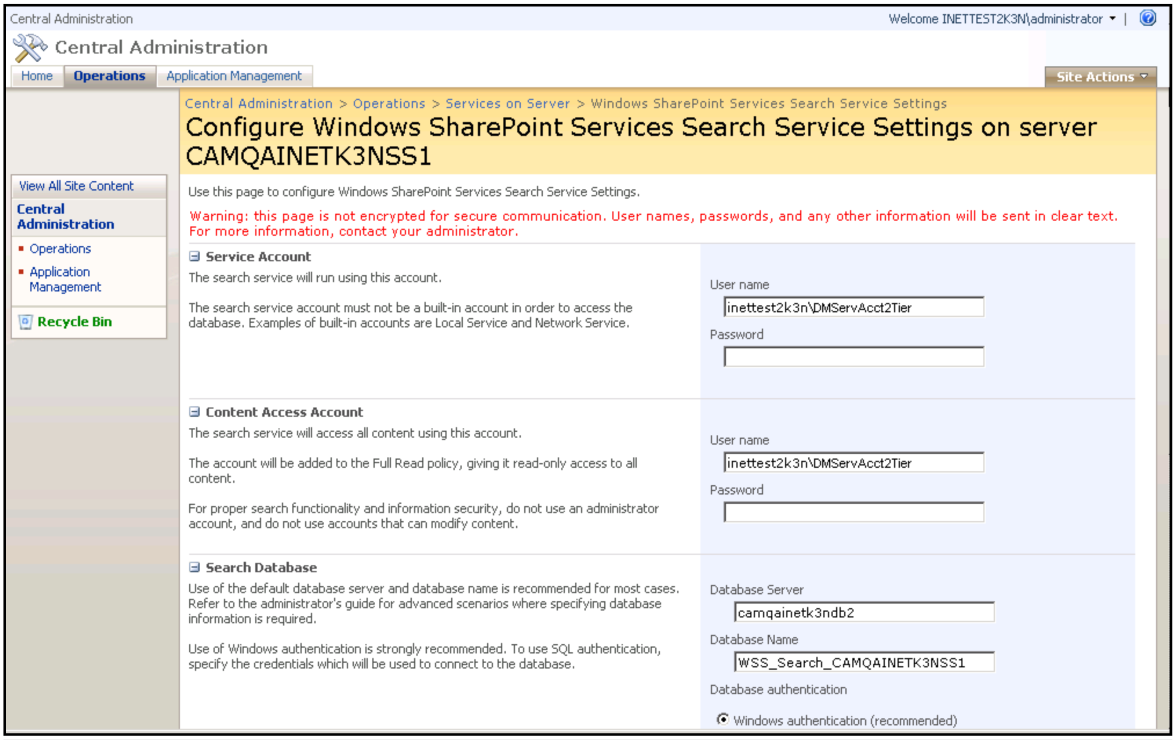
- Server: CAMQAINETK3NWB1
- Start services in the table below:

View: Configurable

| Service | Comment | Status | Action |
|---|---|---|---|
| Central Administration | | Started | Stop |
| Windows SharePoint Services Incoming E-Mail | | Started | Stop |
| Windows SharePoint Services Search | Required on Farm, not running | Stopped | Start |
| Windows SharePoint Services Web Application | | Started | Stop |

- When finished, return to the Central Administration home page

4. Locate the **Windows SharePoint Services Search** option and click **Start**.



Central Administration > Operations > Services on Server > Windows SharePoint Services Search Service Settings

Configure Windows SharePoint Services Search Service Settings on server CAMQAINETK3NSS1

Use this page to configure Windows SharePoint Services Search Service Settings.

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

**Service Account**

The search service will run using this account.

The search service account must not be a built-in account in order to access the database. Examples of built-in accounts are Local Service and Network Service.

User name: inettest2k3n\DMServAcct2Tier

Password:

**Content Access Account**

The search service will access all content using this account.

The account will be added to the Full Read policy, giving it read-only access to all content.

For proper search functionality and information security, do not use an administrator account, and do not use accounts that can modify content.

User name: inettest2k3n\DMServAcct2Tier

Password:

**Search Database**

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

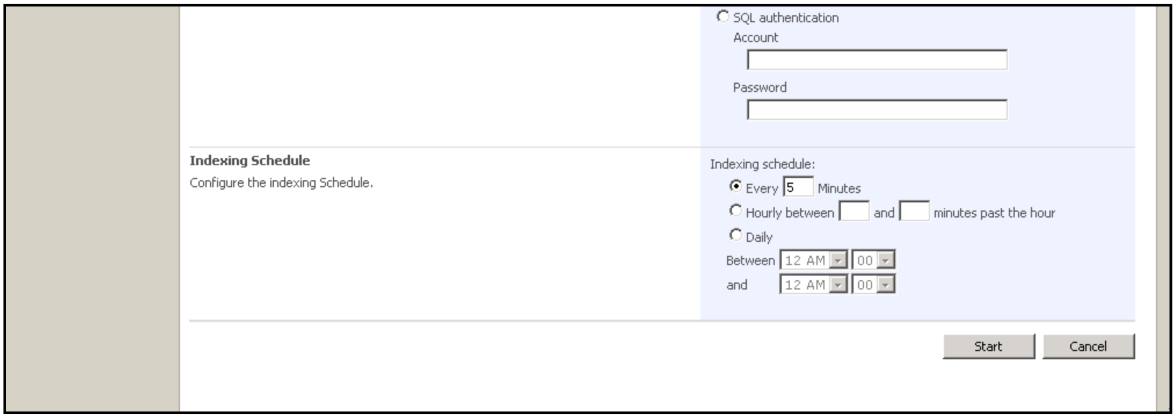
Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: camqainetk3ndb2

Database Name: WSS_Search_CAMQAINETK3NSS1

Database authentication

● Windows authentication (recommended)



○ SQL authentication

Account:

Password:

**Indexing Schedule**

Configure the indexing Schedule.

Indexing schedule:

● Every 5 Minutes

○ Hourly between ___ and ___ minutes past the hour

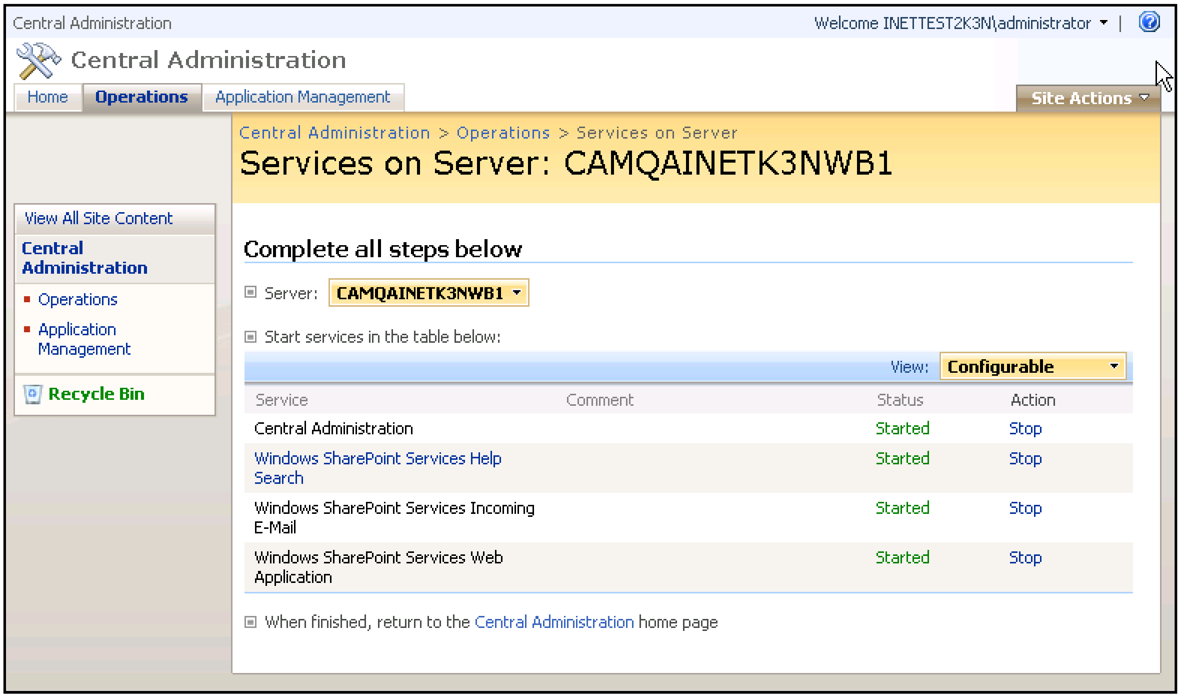
○ Daily

Between 12 AM ▾ 00 ▾

and 12 AM ▾ 00 ▾

5. Configure the search service to include the Service account and Content Access account (use the same account information as your Vision Application Pool Identity).

6. Configure **Search Database** as shown above and click **Start**. After a minute or so, the service's status changes to **Started**.



Central Administration > Operations > Services on Server

Services on Server: CAMQAINETK3NWB1

Complete all steps below

Server: CAMQAINETK3NWB1 ▾

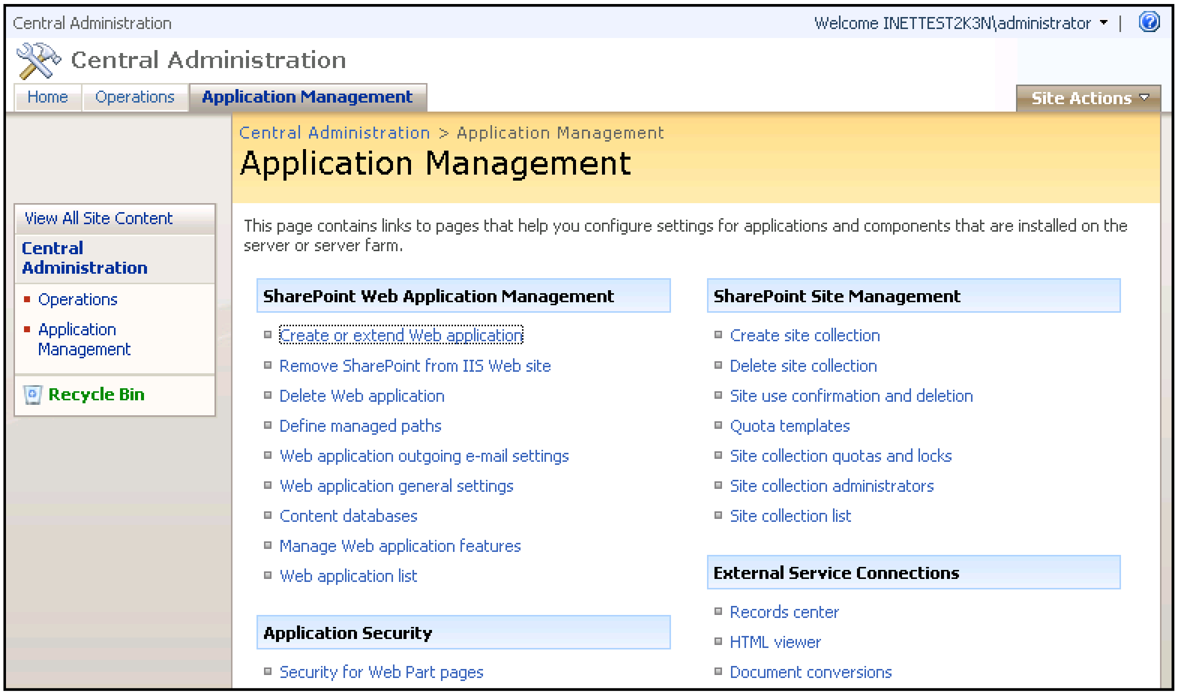
Start services in the table below:

View: Configurable ▾

| Service | Comment | Status | Action |
|---|---|---|---|
| Central Administration | | Started | Stop |
| Windows SharePoint Services Help Search | | Started | Stop |
| Windows SharePoint Services Incoming E-Mail | | Started | Stop |
| Windows SharePoint Services Web Application | | Started | Stop |

When finished, return to the Central Administration home page

7. Click **Application Management** to configure the SharePoint Web Application.



Central Administration > Application Management

Application Management

This page contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

SharePoint Web Application Management

- Create or extend Web application
- Remove SharePoint from IIS Web site
- Delete Web application
- Define managed paths
- Web application outgoing e-mail settings
- Web application general settings
- Content databases
- Manage Web application features
- Web application list

Application Security

- Security for Web Part pages

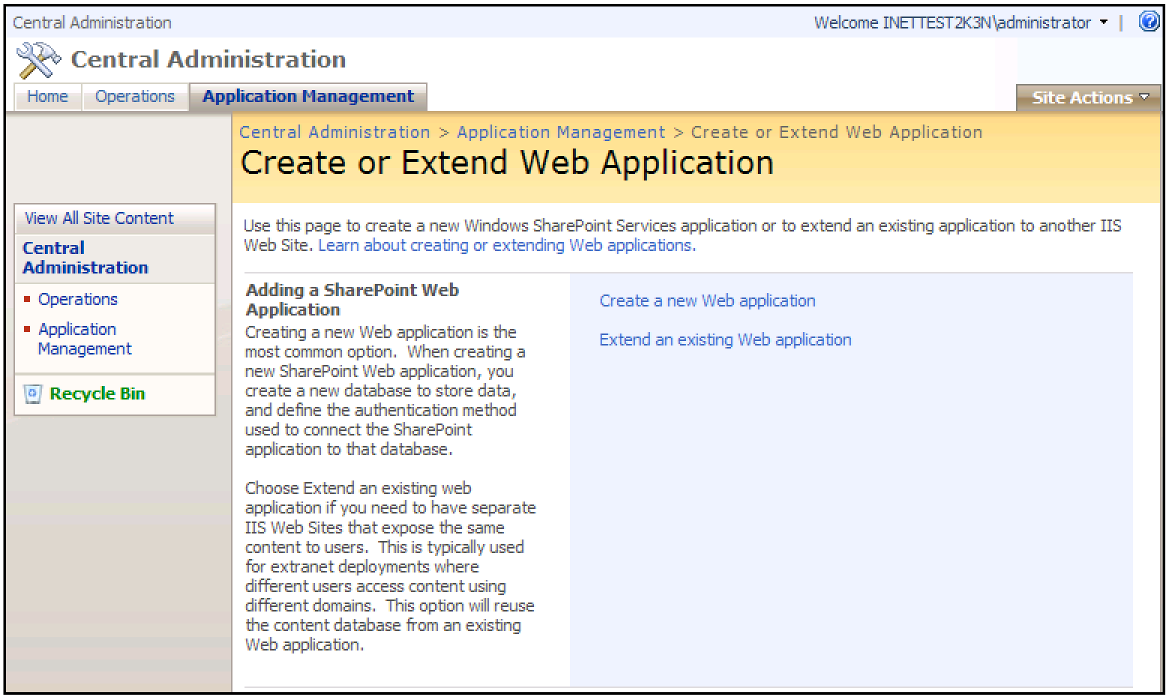
SharePoint Site Management

- Create site collection
- Delete site collection
- Site use confirmation and deletion
- Quota templates
- Site collection quotas and locks
- Site collection administrators
- Site collection list

External Service Connections

- Records center
- HTML viewer
- Document conversions

8. Select the **Create or extend Web application** option. The Create or Extend Web Application page displays.


Central Administration
Welcome INETTEST2K3N\administrator
Central Administration
Home
Operations
Application Management
Site Actions
Central Administration > Application Management > Create or Extend Web Application

Create or Extend Web Application

Use this page to create a new Windows SharePoint Services application or to extend an existing application to another IIS Web Site. Learn about creating or extending Web applications.

Adding a SharePoint Web Application

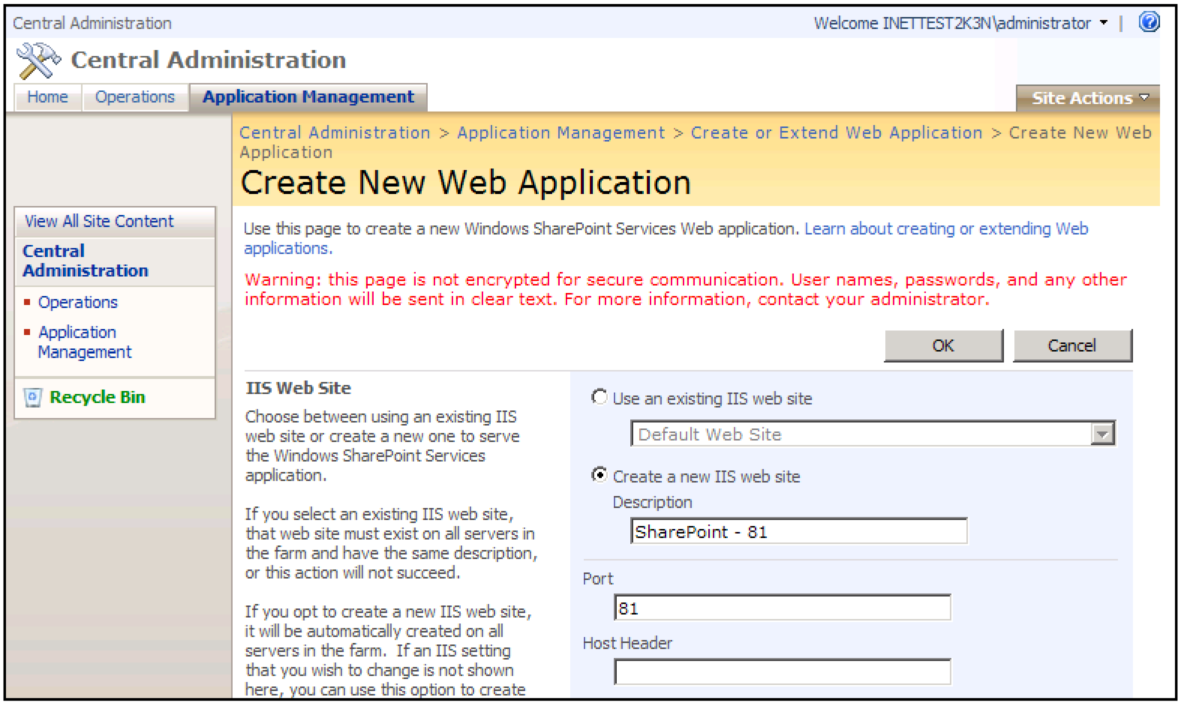
Creating a new Web application is the most common option. When creating a new SharePoint Web application, you create a new database to store data, and define the authentication method used to connect the SharePoint application to that database.

Choose Extend an existing web application if you need to have separate IIS Web Sites that expose the same content to users. This is typically used for extranet deployments where different users access content using different domains. This option will reuse the content database from an existing Web application.

Create a new Web application

Extend an existing Web application

9. Click **Create a new Web application**. The Create a New Web Application page displays.


Central Administration
Welcome INETTEST2K3N\administrator
Central Administration
Home
Operations
Application Management
Site Actions
Central Administration > Application Management > Create or Extend Web Application > Create New Web Application

Create New Web Application

Use this page to create a new Windows SharePoint Services Web application. Learn about creating or extending Web applications.

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

IIS Web Site

Choose between using an existing IIS web site or create a new one to serve the Windows SharePoint Services application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same description, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create

○ Use an existing IIS web site

Default Web Site

● Create a new IIS web site

Description: SharePoint - 81

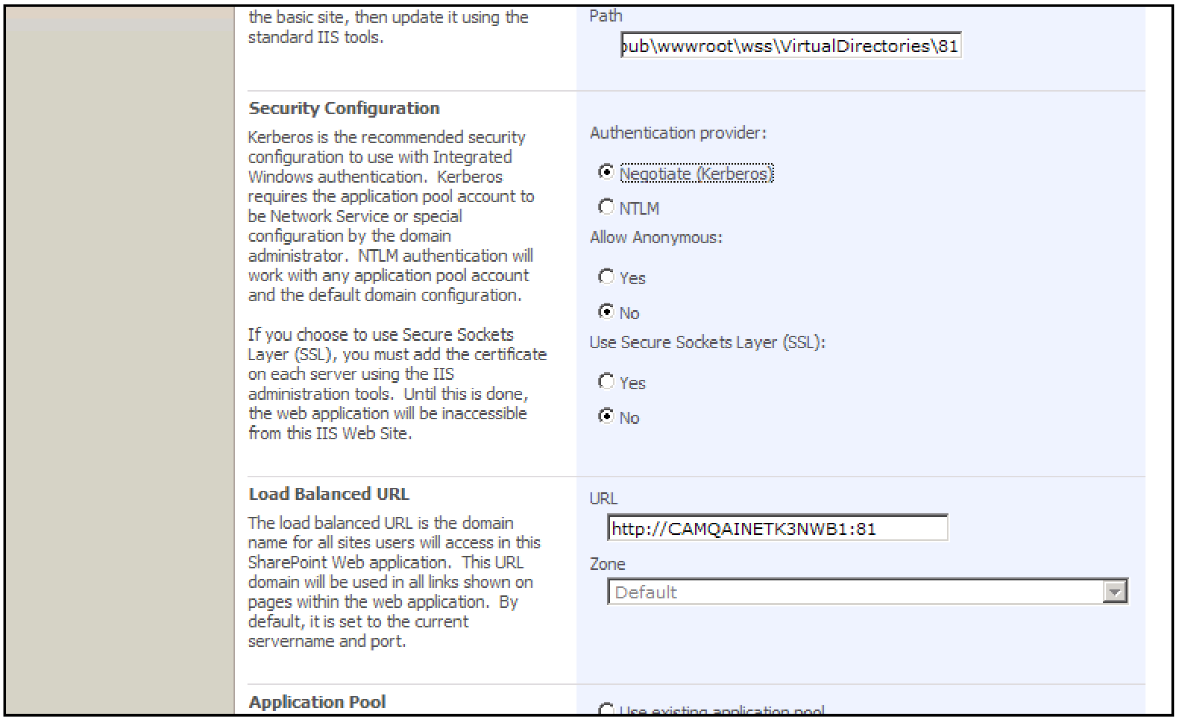
Port: 81

Host Header:

10. Select the **Create a new IIS web site** option. Enter a description for the Web site and specify a port in **Port**.

Vision and SharePoint can be installed to the same Web site if your Vision Web/Application/SharePoint server is Windows Server 2003/Internet Information Services (IIS) 6.0. If you are using Windows Server 2008/Internet Information Services (IIS) 7.0, please install SharePoint to different Web site than Vision.

Alternatively, you can create a new Web site ahead of time using a different IP address and select the option to **Use an existing IIS web site**.



the basic site, then update it using the standard IIS tools.

Path

ub\wwwroot\wss\VirtualDirectories\81

**Security Configuration**

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires the application pool account to be Network Service or special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration.

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS Web Site.

Authentication provider:

● Negotiate (Kerberos)

○ NTLM

Allow Anonymous:

○ Yes

● No

Use Secure Sockets Layer (SSL):

○ Yes

● No

**Load Balanced URL**

The load balanced URL is the domain name for all sites users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port.

URL

http://CAMQAINETK3NWB1:81

Zone

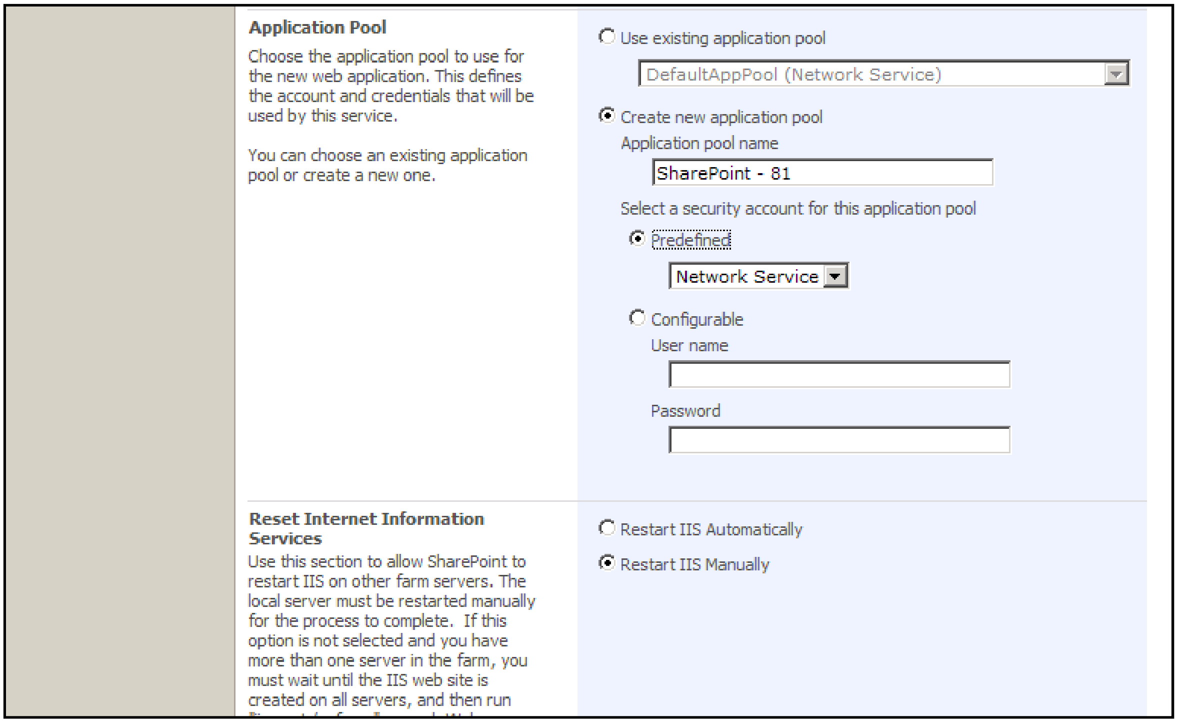
Default

**Application Pool**

○ Use existing application pool

Note the entry in **Path**, which by default is the root of your WSS Web site in a directory named after the port chosen under c:\inetpub\wwwroot\wss\virtualdirectories.

11. Select **Negotiate (Kerberos)** under **Authentication provider**.
12. For the **Allow Anonymous** and **Use Secure Sockets Layer (SSL)** options, accept the default of **No**. If you want to use SSL with SharePoint, you can configure SSL later, but you must not configure SSL to be required.



**Application Pool**

Choose the application pool to use for the new web application. This defines the account and credentials that will be used by this service.

You can choose an existing application pool or create a new one.

○ Use existing application pool

DefaultAppPool (Network Service)

● Create new application pool

Application pool name: SharePoint - 81

Select a security account for this application pool

● Predefined

Network Service

○ Configurable

User name

Password

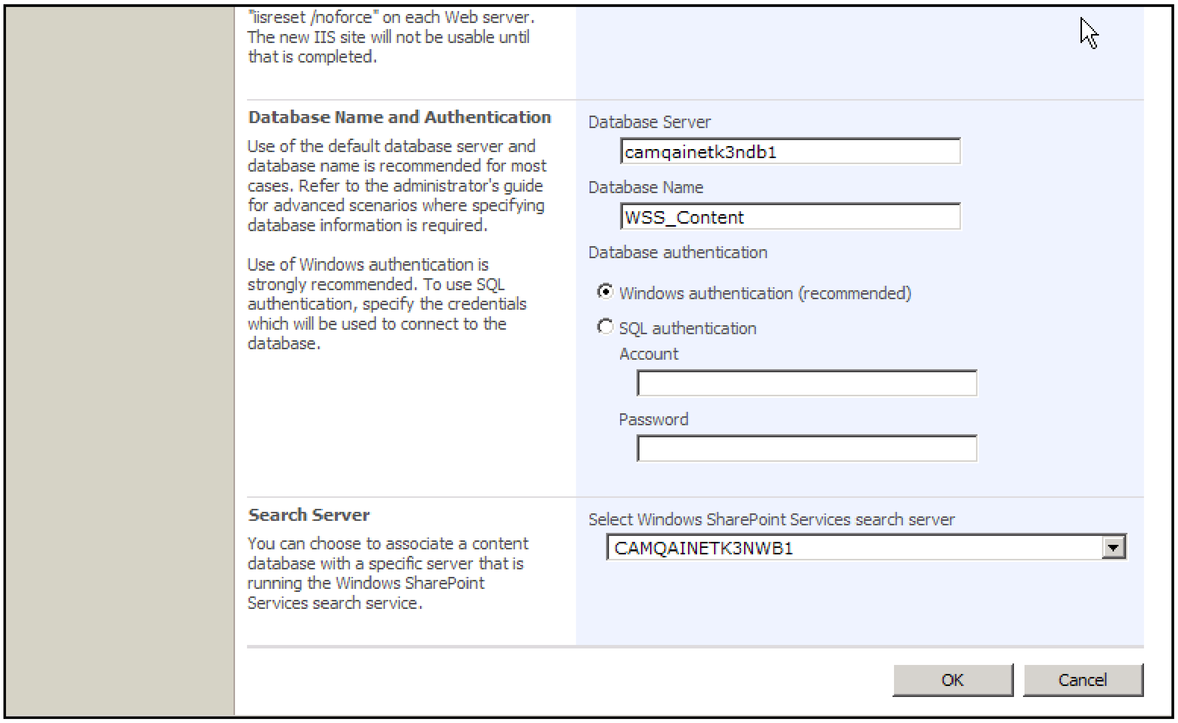
**Reset Internet Information Services**

Use this section to allow SharePoint to restart IIS on other farm servers. The local server must be restarted manually for the process to complete. If this option is not selected and you have more than one server in the farm, you must wait until the IIS web site is created on all servers, and then run

○ Restart IIS Automatically

● Restart IIS Manually

13. Select the **Create new application pool** option and provide a name (Deltek recommends using the same name as the Web site).
14. Select **Predefined** and **Network Service** for the security account to be used for the application pool.
15. Select the **Restart IIS Manually** option for **Reset Internet Information Services**.



"iisreset /noforce" on each Web server. The new IIS site will not be usable until that is completed.

**Database Name and Authentication**

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: camqainetk3ndb1

Database Name: WSS_Content

Database authentication

● Windows authentication (recommended)

○ SQL authentication

Account

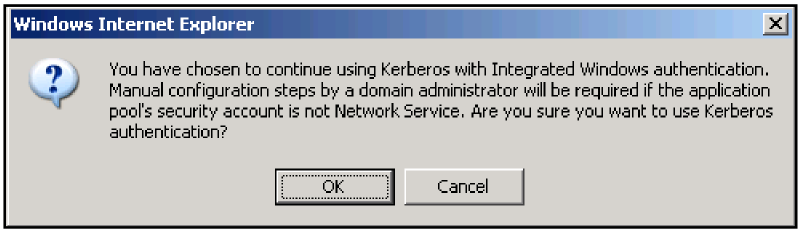
Password

**Search Server**

You can choose to associate a content database with a specific server that is running the Windows SharePoint Services search service.

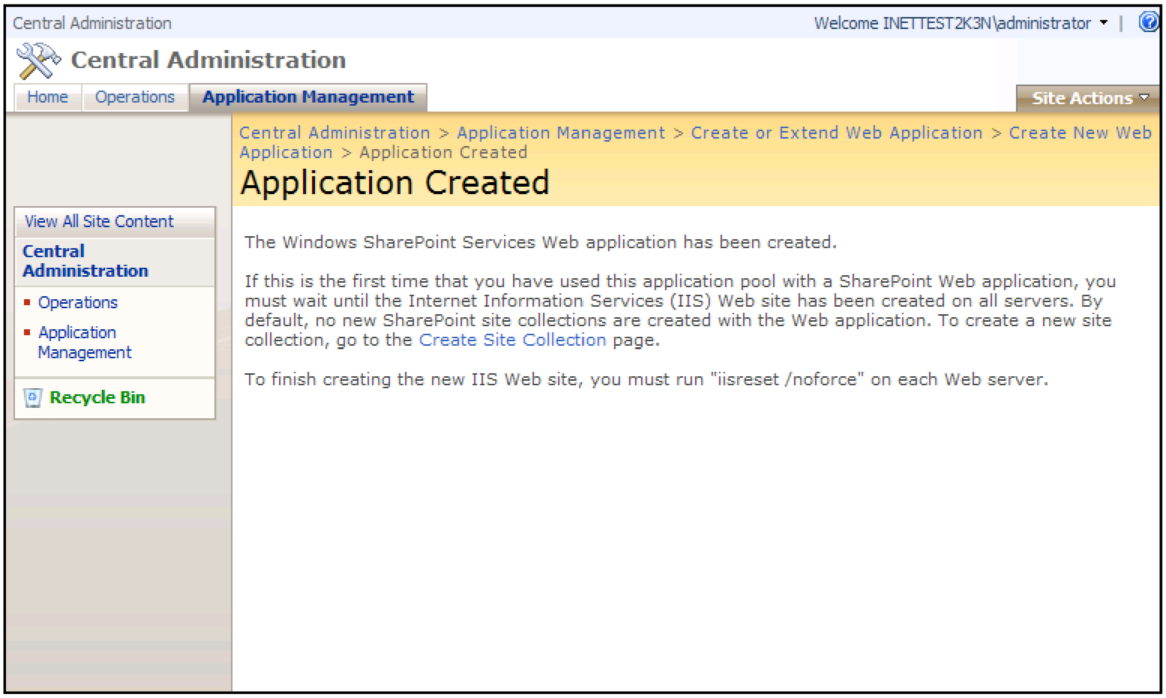
Select Windows SharePoint Services search server: CAMQAINETK3NWB1

16. Verify the name of the server in **Database Server**. (It should be the same as that used for the SharePoint configuration database server.) Accept the default in **Database Name** for the content database.
17. Select **Windows authentication (recommended)** under **Database authentication**. (This will use the SharePoint service account and Vision Application Pool Identity configured previously.)
18. Select the search server in **Select Windows SharePoint Services search server** and click **OK**. The following dialog box displays.



You have chosen to continue using Kerberos with Integrated Windows authentication. Manual configuration steps by a domain administrator will be required if the application pool's security account is not Network Service. Are you sure you want to use Kerberos authentication?

19. Click **OK** to use Kerberos for Windows Authentication. After a few minutes, the Application Created page displays. It indicates the status of the process to create a new Web application.



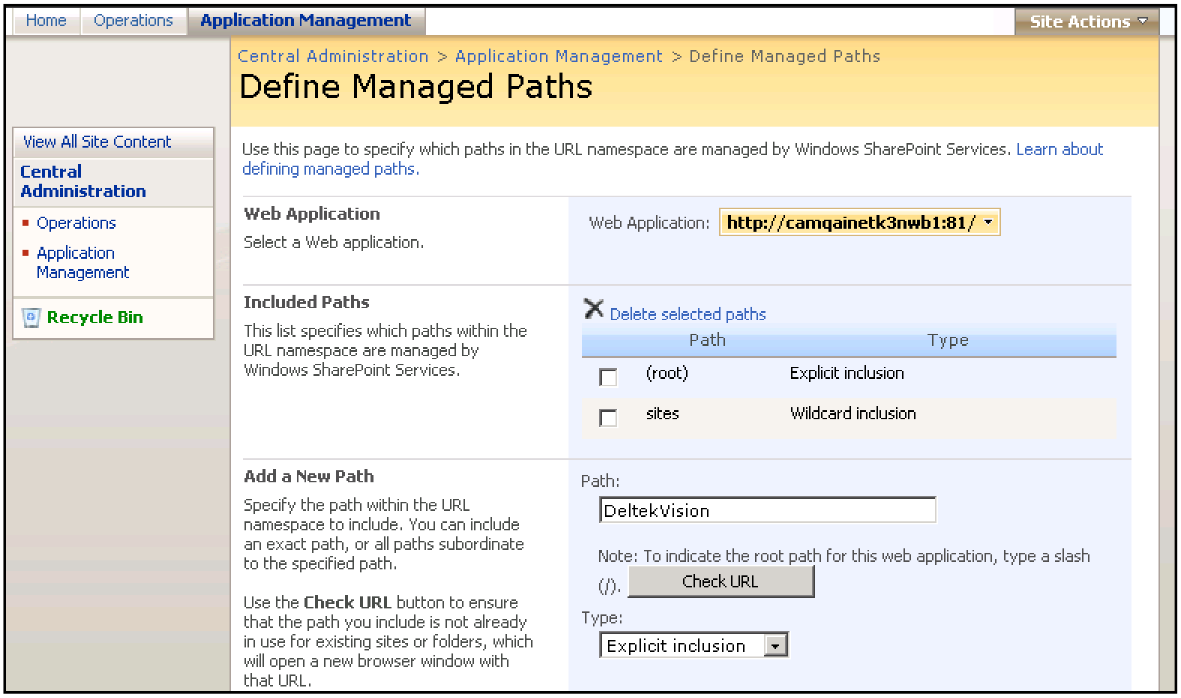
Application Created

The Windows SharePoint Services Web application has been created.

If this is the first time that you have used this application pool with a SharePoint Web application, you must wait until the Internet Information Services (IIS) Web site has been created on all servers. By default, no new SharePoint site collections are created with the Web application. To create a new site collection, go to the Create Site Collection page.

To finish creating the new IIS Web site, you must run "iisreset /noforce" on each Web server.

20. Do not click the **Create Site Collection** link at this time. It is still necessary to add DeltekVision as a managed path with explicit inclusion before you create the site collection.
21. Click **Application Management** and select the **Define Managed Paths** option.



Central Administration > Application Management > Define Managed Paths

Define Managed Paths

Use this page to specify which paths in the URL namespace are managed by Windows SharePoint Services. Learn about defining managed paths.

**Web Application**

Select a Web application.

Web Application: http://camqainetk3nwb1:81/

**Included Paths**

This list specifies which paths within the URL namespace are managed by Windows SharePoint Services.

Delete selected paths

| | Path | Type |
|---|---|---|
| □ | (root) | Explicit inclusion |
| □ | sites | Wildcard inclusion |

**Add a New Path**

Specify the path within the URL namespace to include. You can include an exact path, or all paths subordinate to the specified path.

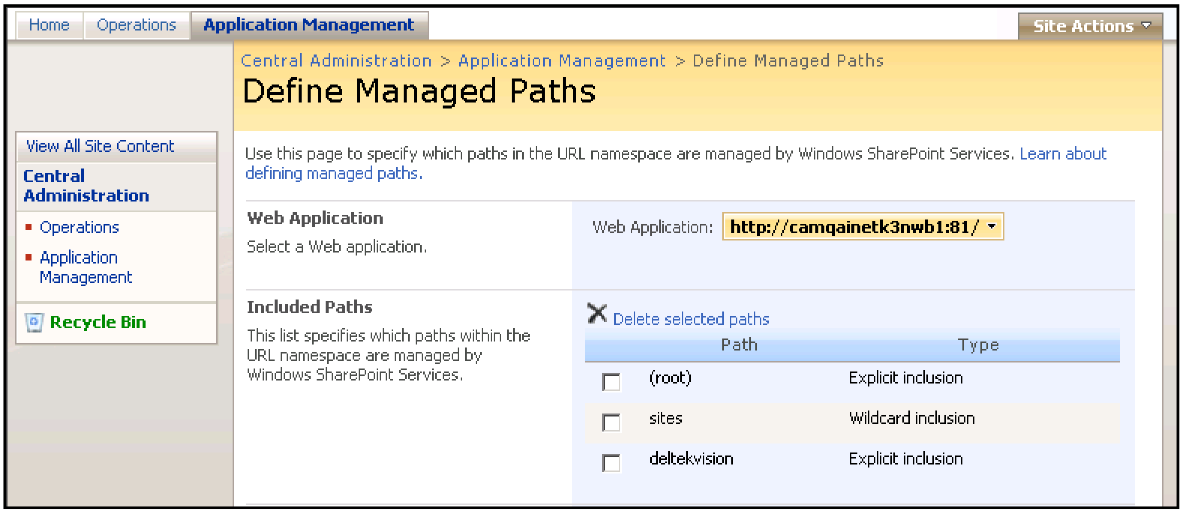
Use the **Check URL** button to ensure that the path you include is not already in use for existing sites or folders, which will open a new browser window with that URL.

Path: DeltekVision

Note: To indicate the root path for this web application, type a slash (/). Check URL

Type: Explicit inclusion

22. Enter **DeltekVision** in **Path** and select **Explicit inclusion** in **Type**.
23. Click **OK**.



Central Administration > Application Management > Define Managed Paths

Define Managed Paths

Use this page to specify which paths in the URL namespace are managed by Windows SharePoint Services. Learn about defining managed paths.

**Web Application**

Select a Web application.

Web Application: http://camqainetk3nwb1:81/

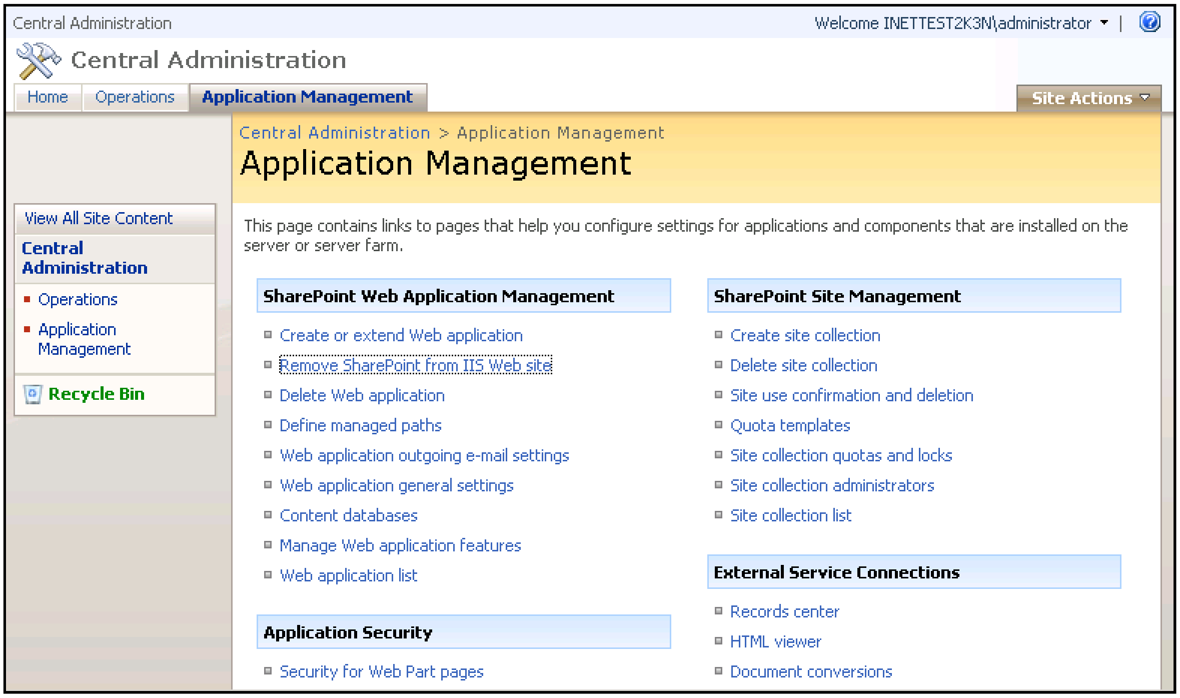
**Included Paths**

This list specifies which paths within the URL namespace are managed by Windows SharePoint Services.

Delete selected paths

| | Path | Type |
|---|---|---|
| □ | (root) | Explicit inclusion |
| □ | sites | Wildcard inclusion |
| □ | deltekvision | Explicit inclusion |

24. Click **Application Management** and select the **Create Site Collection** option under **SharePoint Site Management**.



Central Administration > Application Management

Application Management

This page contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

**SharePoint Web Application Management**

- Create or extend Web application
- Remove SharePoint from IIS Web site
- Delete Web application
- Define managed paths
- Web application outgoing e-mail settings
- Web application general settings
- Content databases
- Manage Web application features
- Web application list

**Application Security**

- Security for Web Part pages

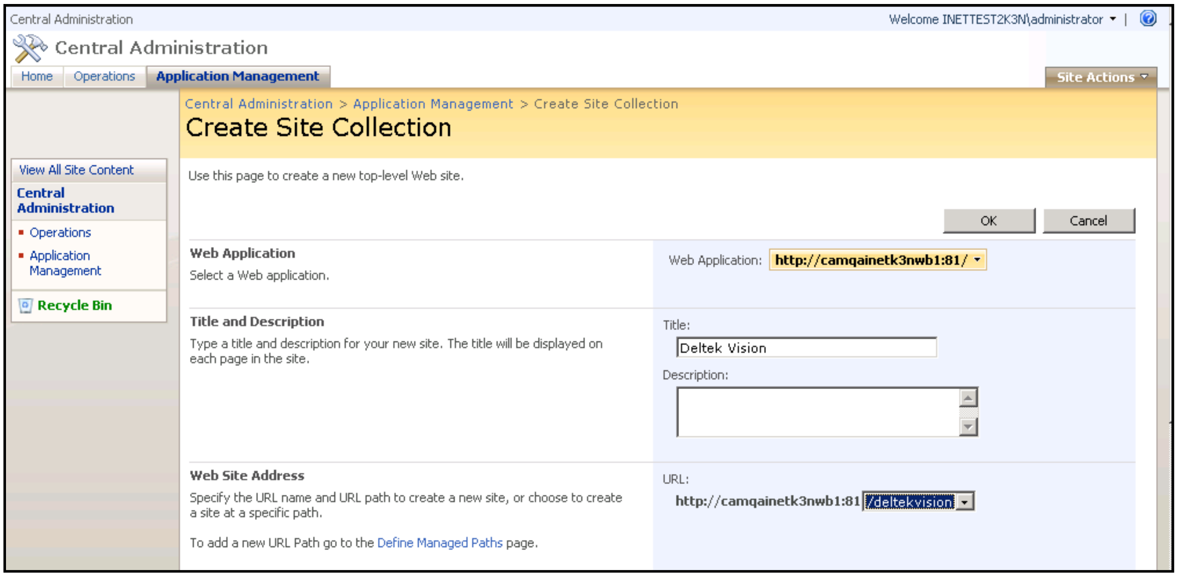
**SharePoint Site Management**

- Create site collection
- Delete site collection
- Site use confirmation and deletion
- Quota templates
- Site collection quotas and locks
- Site collection administrators
- Site collection list

**External Service Connections**

- Records center
- HTML viewer
- Document conversions

The Create Site Collection page displays.



Central Administration > Application Management > Create Site Collection

Create Site Collection

Use this page to create a new top-level Web site.

**Web Application**
Select a Web application.

Web Application: http://camqainetk3nwb1:81/

**Title and Description**
Type a title and description for your new site. The title will be displayed on each page in the site.

Title: Deltek Vision

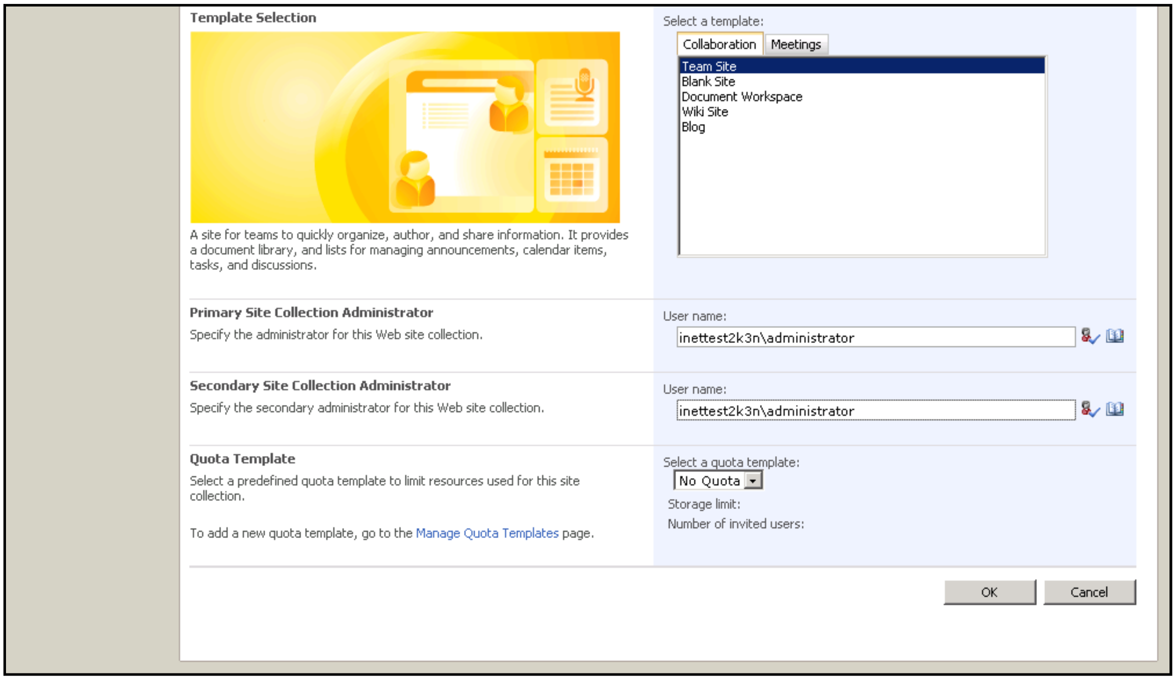
Description:

**Web Site Address**
Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.

To add a new URL Path go to the Define Managed Paths page.

URL:
http://camqainetk3nwb1:81 /deltekvision

25. Enter **Deltek Vision** in **Title** and enter a description, if appropriate.
26. From the **URL** drop-down list, select **/deltekvision**. This will be the top level root for Vision Document Management.



**Template Selection**

A site for teams to quickly organize, author, and share information. It provides a document library, and lists for managing announcements, calendar items, tasks, and discussions.

Select a template:

Team Site
Blank Site
Document Workspace
Wiki Site
Blog

**Primary Site Collection Administrator**

Specify the administrator for this Web site collection.

User name: inettest2k3n\administrator

**Secondary Site Collection Administrator**

Specify the secondary administrator for this Web site collection.

User name: inettest2k3n\administrator

**Quota Template**

Select a predefined quota template to limit resources used for this site collection.

To add a new quota template, go to the Manage Quota Templates page.

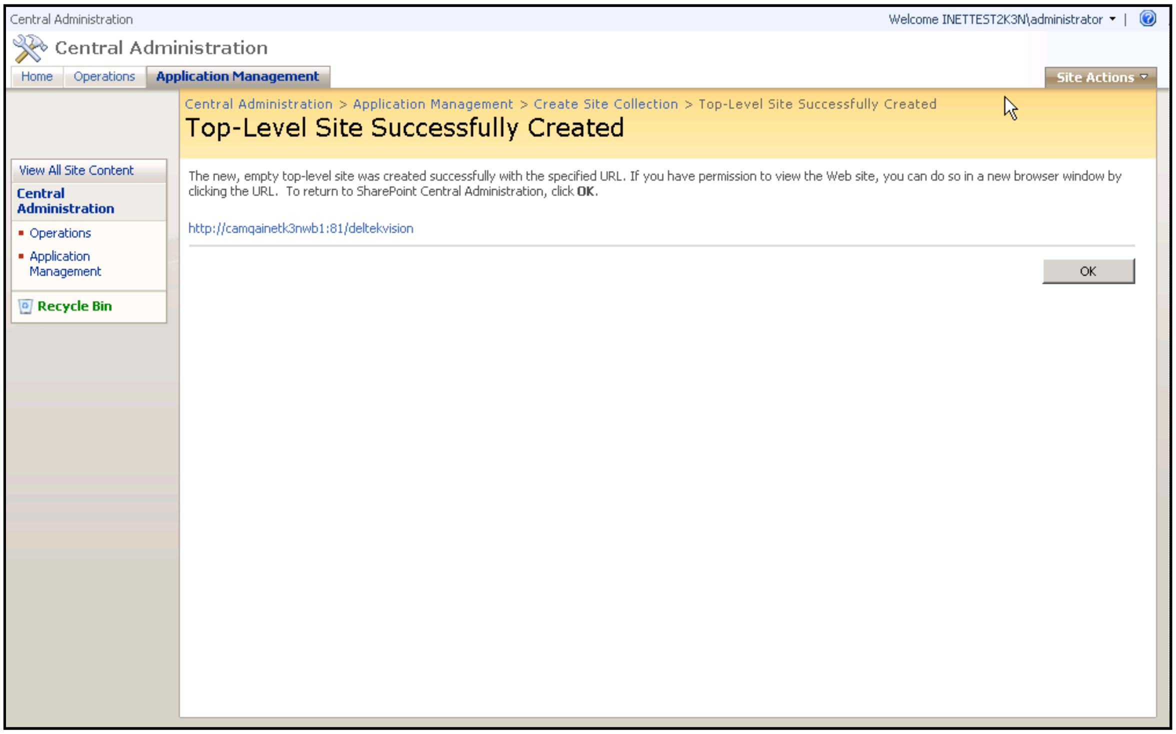
Select a quota template: No Quota

Storage limit:

Number of invited users:

27. Under **Select a template**, accept the default of **Team Site** for the template to be used and enter a username in each of the **User name** fields for the primary and secondary site collection administrators.

28. Select **No Quota** in **Select a quota template** and click **OK**. The Top-Level Site Successfully Created page displays.



Central Administration > Application Management > Create Site Collection > Top-Level Site Successfully Created

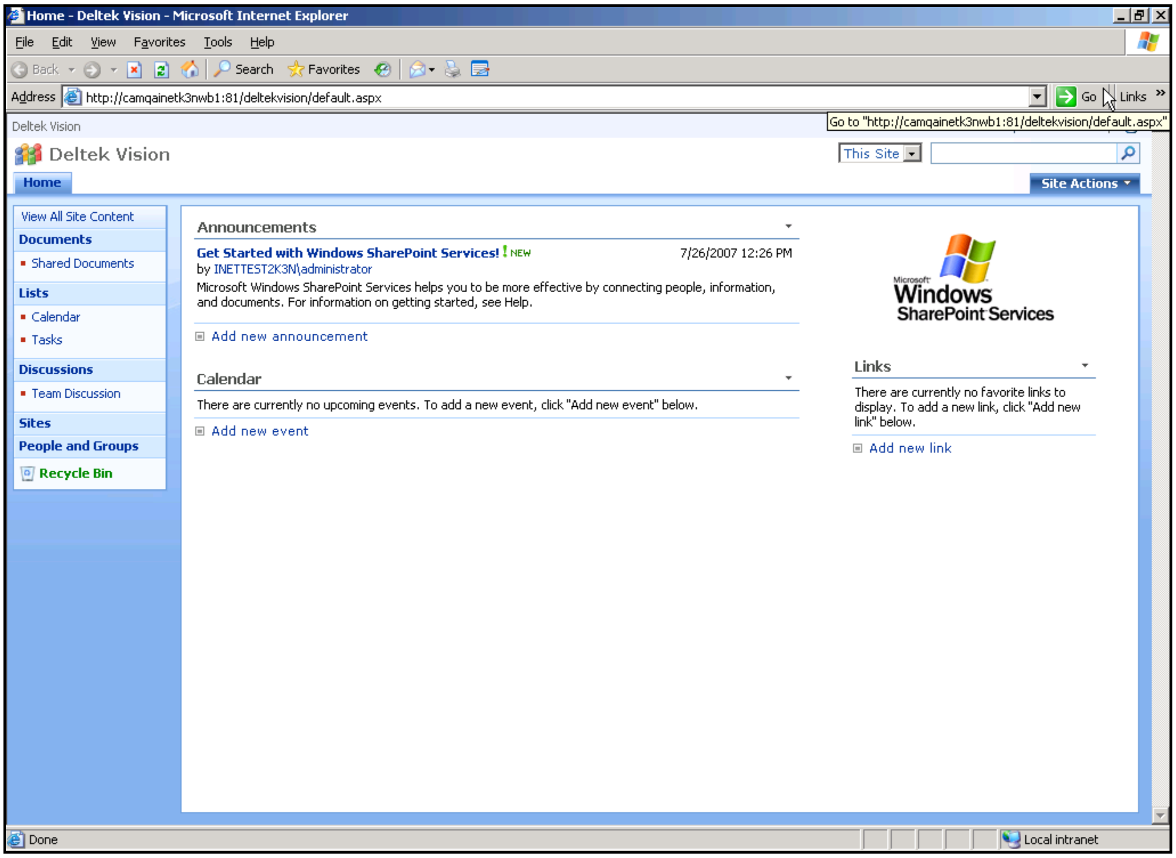
Top-Level Site Successfully Created

The new, empty top-level site was created successfully with the specified URL. If you have permission to view the Web site, you can do so in a new browser window by clicking the URL. To return to SharePoint Central Administration, click **OK**.

http://camqainetk3nwb1:81/deltekvision

29. Click **Start** » **Run**, enter **iisreset /noforce,** and click **Enter**.

30. Click the link for the top level site (in our example it is http://camqainetk3nwb1:81/deltekvision) to display the site.



Get Started with Windows SharePoint Services! NEW 7/26/2007 12:26 PM

by INETTEST2K3N\administrator

Microsoft Windows SharePoint Services helps you to be more effective by connecting people, information, and documents. For information on getting started, see Help.

There are currently no upcoming events. To add a new event, click "Add new event" below.

There are currently no favorite links to display. To add a new link, click "Add new link" below.

31. The SharePoint configuration is complete. Close SharePoint Central Administration.

## Configure SharePoint for a Fully Qualified Domain Name (FQDN) URL (Optional)

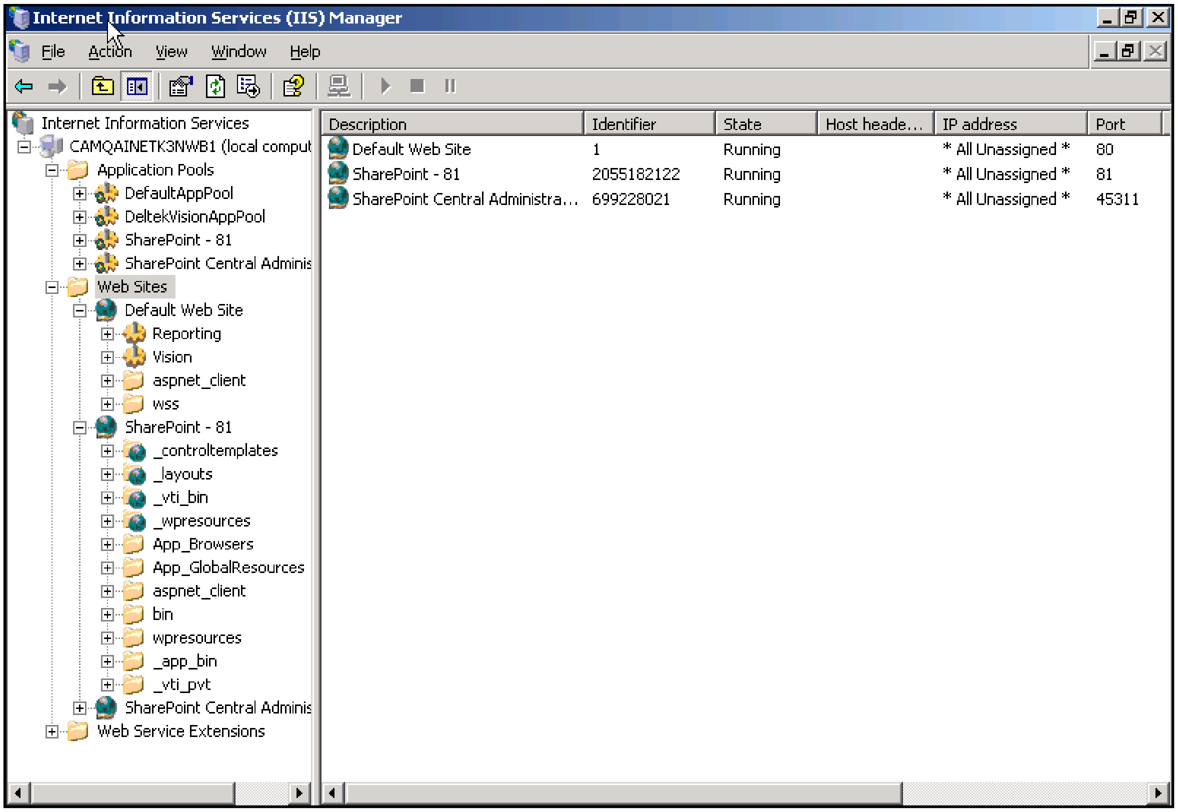
If you will be configuring your SharePoint server to use a custom DNS record for the URL you must create an additional SPN and also create Alternate Access Mappings in SharePoint.

See “Appendix C: SPN Configuration When Using Custom DNS Records” on page 99 for more information.

## Verify IIS Configuration and Configure Deltek Vision Document Management .NET Assembly

### To verify IIS configuration, complete the following steps:

1. Use the directions that follow to open Internet Information Services to view these Web sites:
   - **Default Web Site** — This is your Vision Web Site
   - **SharePoint – 81** — This is your WSS 3.0 Web Site (if installed to a different Web site from Vision
   - **SharePoint Central Administration Web Site**



| Description | Identifier | State | Host heade... | IP address | Port |
|---|---|---|---|---|---|
| Default Web Site | 1 | Running | | * All Unassigned * | 80 |
| SharePoint - 81 | 2055182122 | Running | | * All Unassigned * | 81 |
| SharePoint Central Administra... | 699228021 | Running | | * All Unassigned * | 45311 |

2. Copy the Vision Document Management .NET assembly to SharePoint site directory.
3. Copy Deltek.Vision.WSS30.Server.dll from <Vision Installation Directory>\Support\DM\30 to:

   c:\inetpub\wwwroot\bin (if WSS was installed to the default web site)

   *or to*

   c:\inetput\wwwroot\wss\Virtual Directories\<site>\bin

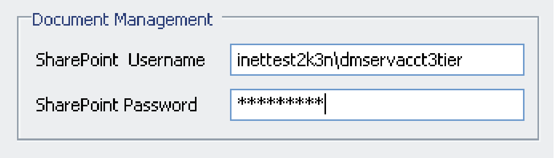
> By default, the <site> directory will reference the port chosen. In our example, the port is 81.

## Configure Document Management Service Account in Weblink

You must configure the Document Management service account (username/password) on the System Settings tab of the Deltek Vision Weblink utility. Follow the instructions below to configure this:

1. On the Vision Web server, launch Weblink from **Start » Programs » Deltek Vision**
2. Enter the Weblink password when prompted.
3. Click the System Settings tab.

   In the **Document Management** group box, enter your SharePoint username and password. This account is your SharePoint Service account/Deltek Vision Application Pool Identity.



Document Management

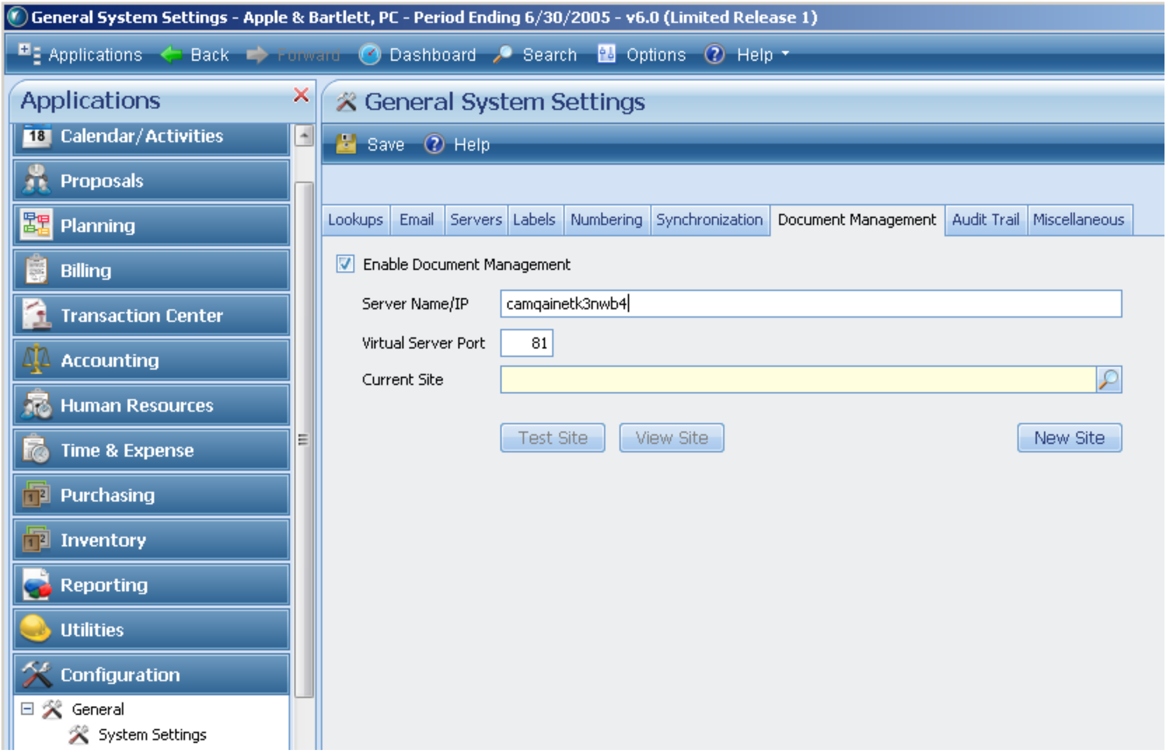
SharePoint Username: inettest2k3n\dmservacct3tier

SharePoint Password: **********

## Configure Vision Document Management

**To configure Vision Document Management, complete the following steps:**

1. Log in to Vision using an account that has access to the Configuration menus.
2. Click **Configuration » General » System Settings** and select the Document Management tab.



General System Settings - Apple & Bartlett, PC - Period Ending 6/30/2005 - v6.0 (Limited Release 1)

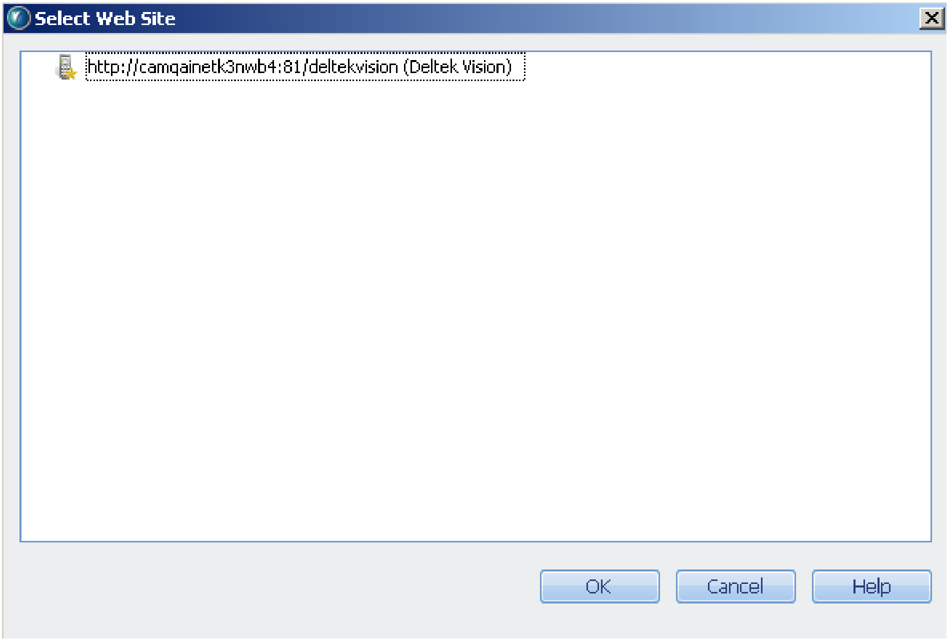
☑ Enable Document Management

Server Name/IP: camqainetk3nwb4

Virtual Server Port: 81

Current Site:

3. Select the **Enable Document Management** check box.
4. Enter the name of the server hosting Document Management. This can be the NetBIOS name, server name FQDN, or custom DNS/FQDN. Enter this value without the protocol prefix (for example, remove the http://). In the illustration above, the value is **camqainetk3nwb4**.
5. Enter the port in **Virtual Server Port**. In our example the port is 81.
6. Click the Lookup icon to select the current site.



http://camqainetk3nwb4:81/deltekvision (Deltek Vision)

7. The Select Web Site dialog box displays the available sites. Select a site and click **OK**.
8. Save your changes.

## Optional: Configure Protocol Transition

If Vision Document Management functionality is required over the Internet and you will be using a custom DNS/FQDN for the SharePoint URL (as in our example, vision1.inettest2k3n.com), then you must configure a form of delegation referred to as Protocol Transition. If Document Management functionality is not required, you can skip this step.

The Kerberos authentication protocol must be used to authenticate from the Vision Web server to the SharePoint server. However, if Vision is deployed in an Internet scenario and there are users outside of the firewall that need to access Document Management features, Kerberos authentication cannot be used to authenticate the client to the Web server. This is because the client needs to have the ability to negotiate a Kerberos ticket with the Key Distribution Center (KDC), which is a service running on a Domain Controller. This requires port 88 to be opened inbound on the firewall to the Domain Controller, which is not an advisable configuration.

To get around this, you must be running a Native Windows Server 2003 functional domain.

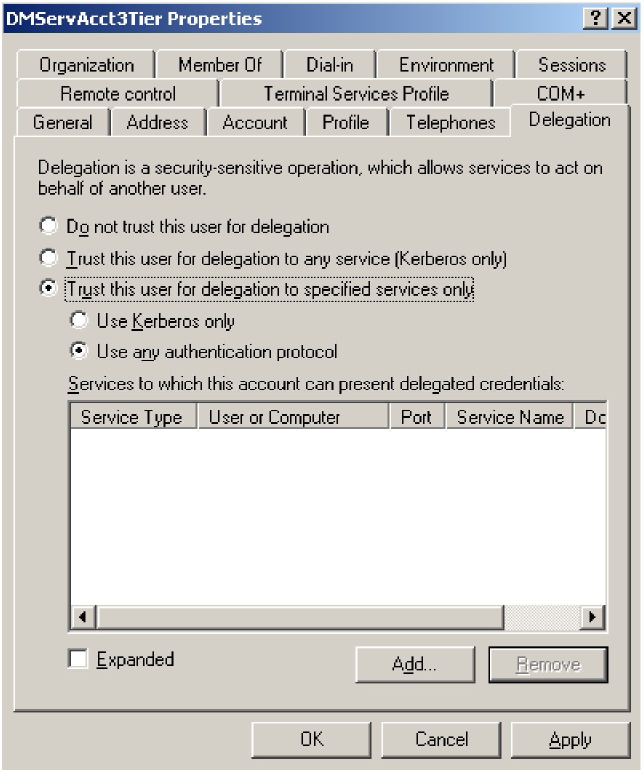
To configure Protocol Transition, select the **Use any authentication protocol** option instead of the **Use Kerberos only** option that is used to configure Constrained Delegation. This allows the client to authenticate to the Vision Web server using NTLM instead of Kerberos, and that authentication is then “transitioned” over to Kerberos for Delegation to the SharePoint server.

**To configure Protocol Transition, complete the following steps:**

1. Open the Active Directory Users and Computers MMC on a Domain Controller.
2. Locate the User account for the Vision Application Pool Identity (WSS Service account).
3. Right-click and select **Properties**.
4. On the Delegation tab, select the **Trust this user for delegation to specified services only** option.

> If you click the second option, you will be configuring Unconstrained Delegation, which would be the equivalent of Delegation in a Windows 2000 or Mixed domain. The Constrained Delegation feature of Windows Server 2003 Native domain is more secure and therefore recommended.

5. Select the **Use any authentication protocol** option.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

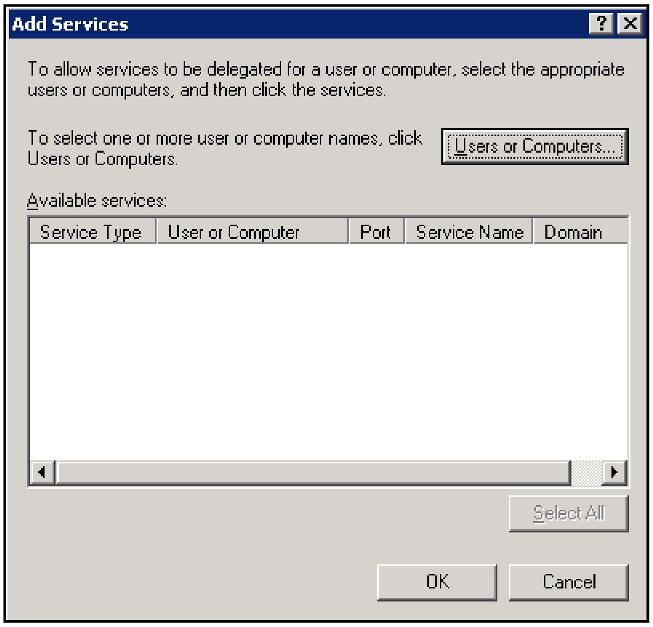
○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

□ Expanded

6. Click the **Add** button. The Add Services dialog box displays.

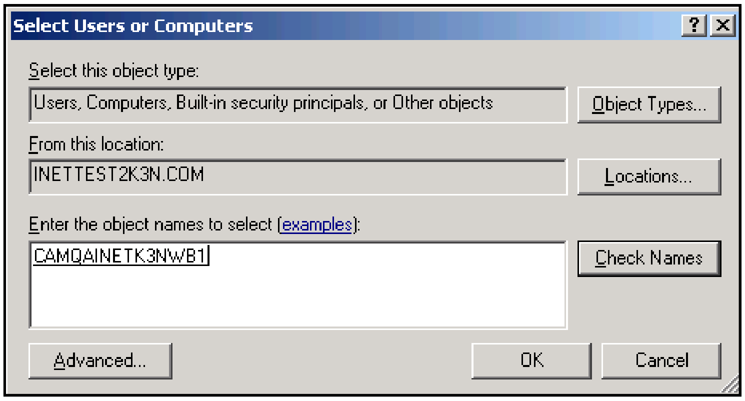


To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

7. Click **Users or Computers**. The Select Users or Computers dialog box displays.



Select Users or Computers

Select this object type:
Users, Computers, Built-in security principals, or Other objects

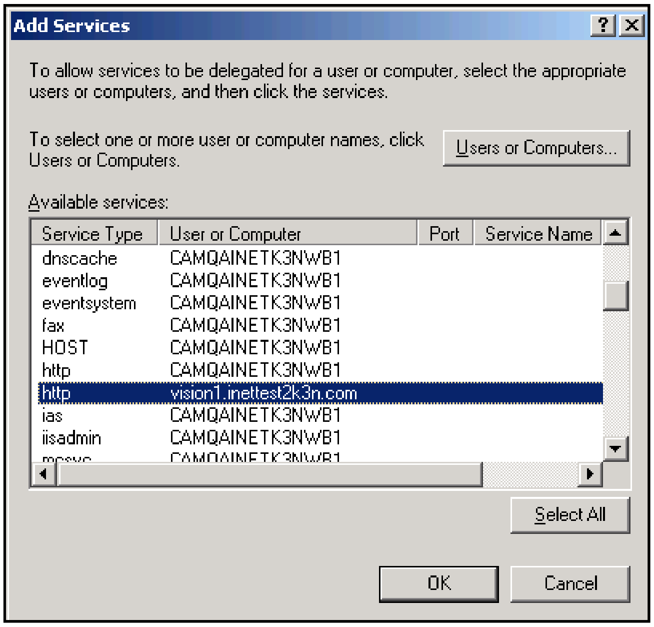
From this location:
INETTEST2K3N.COM

Enter the object names to select (examples):
CAMQAINETK3NWB1

8. Search for the SharePoint server and click **OK**.

9. Locate the http service for the SPN (FQDN) you created earlier (in our example, vision1.inettest2k3n.com), select it, and click **OK**.

   In the following screenshot, there are two http service types listed. Unless you have registered a custom FQDN using the setspn utility, only the server name displays. These service types are known as Service Principal Names (SPNs).



Add Services

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

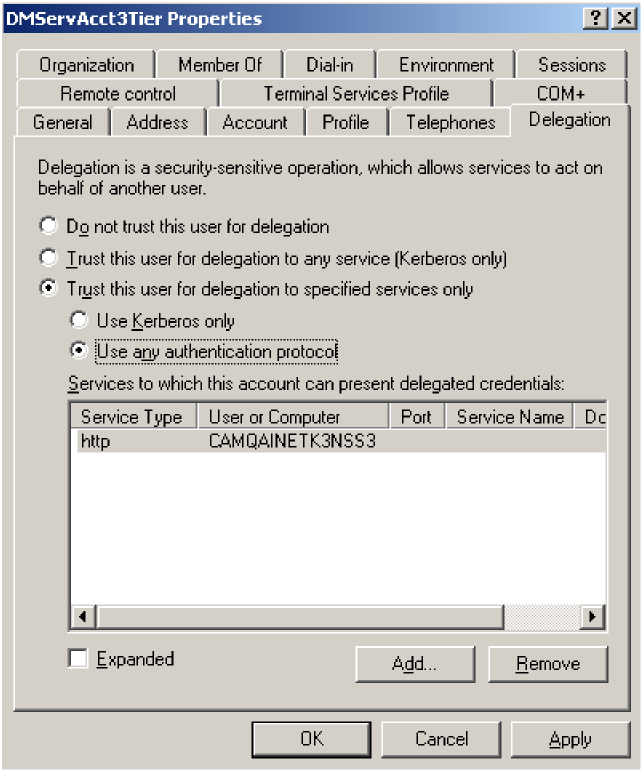
Available services:

| Service Type | User or Computer | Port | Service Name |
|---|---|---|---|
| dnscache | CAMQAINETK3NWB1 | | |
| eventlog | CAMQAINETK3NWB1 | | |
| eventsystem | CAMQAINETK3NWB1 | | |
| fax | CAMQAINETK3NWB1 | | |
| HOST | CAMQAINETK3NWB1 | | |
| http | CAMQAINETK3NWB1 | | |
| http | vision1.inettest2k3n.com | | |
| ias | CAMQAINETK3NWB1 | | |
| iisadmin | CAMQAINETK3NWB1 | | |

The SPN referencing CAMQAINETK3NWB1.inettest2k3n.com was created automatically when the server was added to the domain and the http service (IIS) was installed.

The second SPN referencing vision1.inettest2k3n.com is a new SPN that was created using the setspn utility that allows us to register the custom FQDN of the server, which provides more meaning than the actual machine name.

The Delegation tab options should be as follows:



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|
| http | CAMQAINETK3NSS3 | | | |

☐ Expanded

Because we are explicitly specifying the http service and not all services on the SharePoint server, and because we are using the **Use any authentication protocol option** and not Kerberos, this is known as “Protocol Transition.”

# Multi-Tier—New Installation of Document Management 6.1 with Windows SharePoint Services 3.0

The following instructions assume that Vision and Windows SharePoint Services 3.0 exist on separate servers and assume that you are deploying to Windows Server 2003/IIS 6.0. If you will be deploying to Windows Server 2008/IIS 7.0, refer to Appendix B for detailed configuration information.

## Prerequisites

- Install/upgrade to Vision 6.1.
- Change the Application Pool Identity for the DeltekVisionAppPool to be a domain account. (The Vision 6.1 installation sets this to be the local DeltekVision account.) This account will also be the SharePoint (WSS) Service account. Add this user to the local Administrators and IIS_WPG groups on the Vision server and local Administrators group on the WSS server.

## Configure Vision Application Pool Identity to Be a Domain Account

You must change the Vision Application Pool Identity to be a domain account. (The default is for Vision to use a Local Administrator Account. The DeltekVision user is created during the Vision installation.) The reason for this change is that the local accounts are unable to read the SPN configured in Active Directory.

**To change the Vision Application Pool Identity, complete the following steps:**

1. Create a domain user account. No domain Admin rights are needed for this account.
2. Log on to the domain on the Vision Web/application server using an Administrator account.
3. Click **Start » All Programs » Administrative Tools » Internet Information Services.**
4. Expand **Application Pools**.
5. Right-click **DeltekVisionAppPool** and select **Properties** on the shortcut menu.
6. Click the Identity tab and change the account from DeltekVision to your domain\user account created in step 1. Make sure this account is a member of the Local Administrators and IIS_WPG local groups.

## Configure SPN for Vision Application Pool Identity

As mentioned earlier in this document, it is necessary to create a Service Principal Name (SPN) for the domain user running the DeltekVisionAppPool.

**To add the Application Pool Identity as a Service Principal Name, complete the following steps:**

1. Enter the following commands on the domain server where setspn is installed:

   **setspn –A http/<Vision Web/App Server name> <domain app pool identity>**

   For example: setspn –A http/camqainetk3nwb5 inettest2k3n\dmservacct3tier
2. Repeat for the FQDN of the server.

Refer to the following related Microsoft Knowledge Base article:

http://support.microsoft.com/?id=871179

If your Vision Web server is accessed by a DNS / FQDN (Fully Qualified Domain Name) that *does not match* the name of the server (for example, if your Vision Web server is named Server01 and its DNS name is Server01.Company.com, but you have added a custom DNS value Vision.Company.com), you must also add an SPN for this custom DNS name.

## Install and Configure Vision 6.1 Document Management and WSS 3.0

When you install Vision 6.1 Document Management, WSS is automatically installed. (If you are upgrading from Vision 5.1, no changes are made to your WSS installation.) However, the Document Management installation will not automatically configure WSS. The steps to configure SharePoint are outlined in this document.

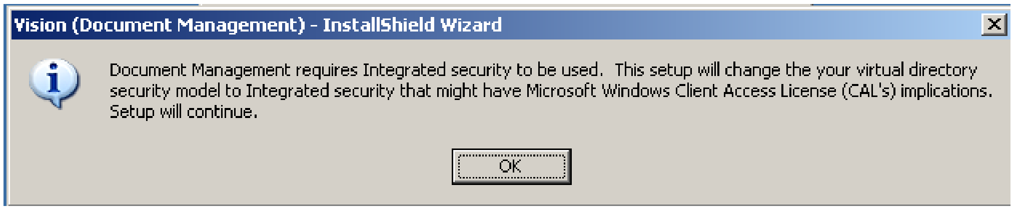
The Document Management installation does the following:

- Installs Web Service Extensions (WSE) 2.0 SP3.
- Installs WSS 3.0. if it is not already installed.
- Changes the IIS metabase NTAuthenticationProviders element to be Negotiate,NTLM.
- Copies Document Management files to the SharePoint ISAPI folder (c:\program files\common files\microsoft shared\web service extensions\12\isapi).
- Copies Document Management files to the Vision Support folder (\program files\deltek\vision\support\DM\30).
- Modifies the SharePoint Web.config file in the ISAPI directory to work with Vision Document Management.
- Installs Deltek.Vision.WSS30.Server.dll into the Global Assembly Cache (GAC).

### Install Vision 6.1 Document Management on the Vision Web Server

**To install Vision 6.1 Document Management on the Vision Web server, complete the following steps:**

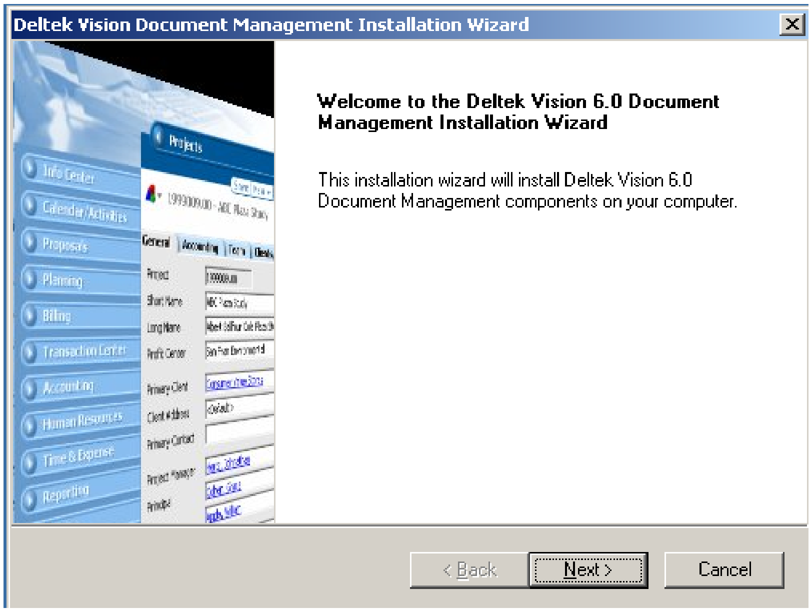
1. Run the setup on your Vision Web server. The following dialog box then indicates the IIS licensing requirements for the use of Windows Integrated Authentication (required to use Vision Document Management):



Vision (Document Management) - InstallShield Wizard

Document Management requires Integrated security to be used.  This setup will change the your virtual directory security model to Integrated security that might have Microsoft Windows Client Access License (CAL's) implications. Setup will continue.

2. Click **OK**. The Welcome page displays.

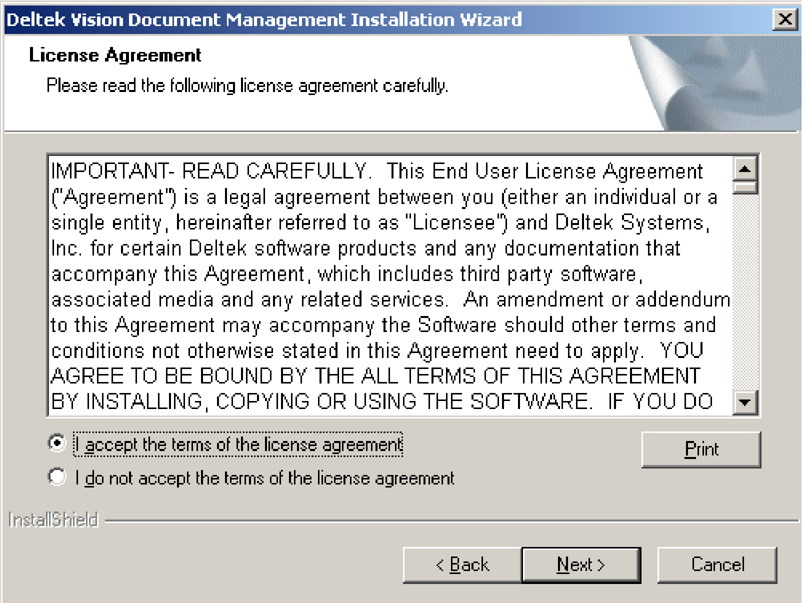


Deltek Vision Document Management Installation Wizard

**Welcome to the Deltek Vision 6.0 Document Management Installation Wizard**

This installation wizard will install Deltek Vision 6.0 Document Management components on your computer.

3. Click **Next.** The License Agreement page displays.



Deltek Vision Document Management Installation Wizard

**License Agreement**

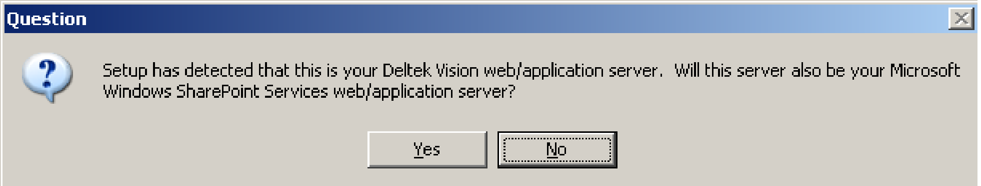
Please read the following license agreement carefully.

IMPORTANT- READ CAREFULLY. This End User License Agreement ("Agreement") is a legal agreement between you (either an individual or a single entity, hereinafter referred to as "Licensee") and Deltek Systems, Inc. for certain Deltek software products and any documentation that accompany this Agreement, which includes third party software, associated media and any related services. An amendment or addendum to this Agreement may accompany the Software should other terms and conditions not otherwise stated in this Agreement need to apply. YOU AGREE TO BE BOUND BY THE ALL TERMS OF THIS AGREEMENT BY INSTALLING, COPYING OR USING THE SOFTWARE. IF YOU DO

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

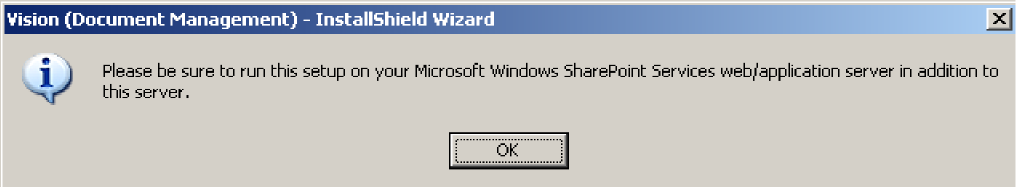
4. Select **I accept the terms of the license agreement** and click **Next**. The following dialog box displays.



Question

Setup has detected that this is your Deltek Vision web/application server. Will this server also be your Microsoft Windows SharePoint Services web/application server?

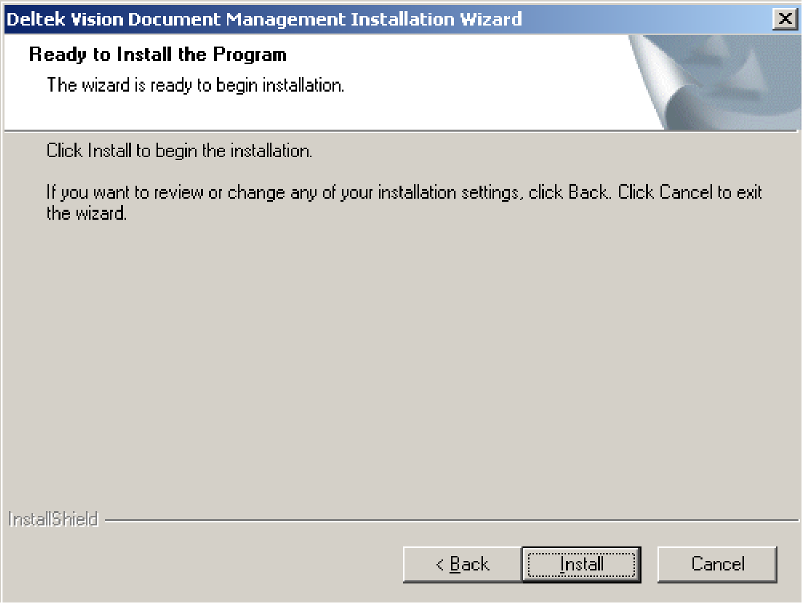
5. Click **No** because this is a multi-tier installation of Vision Document Management and your Vision Web server will not host WSS 3.0. The following dialog box displays to remind you to run the setup on the WSS server.



Vision (Document Management) - InstallShield Wizard

Please be sure to run this setup on your Microsoft Windows SharePoint Services web/application server in addition to this server.

6. Click **OK** to display the Ready to Install the Program page.



Deltek Vision Document Management Installation Wizard

**Ready to Install the Program**

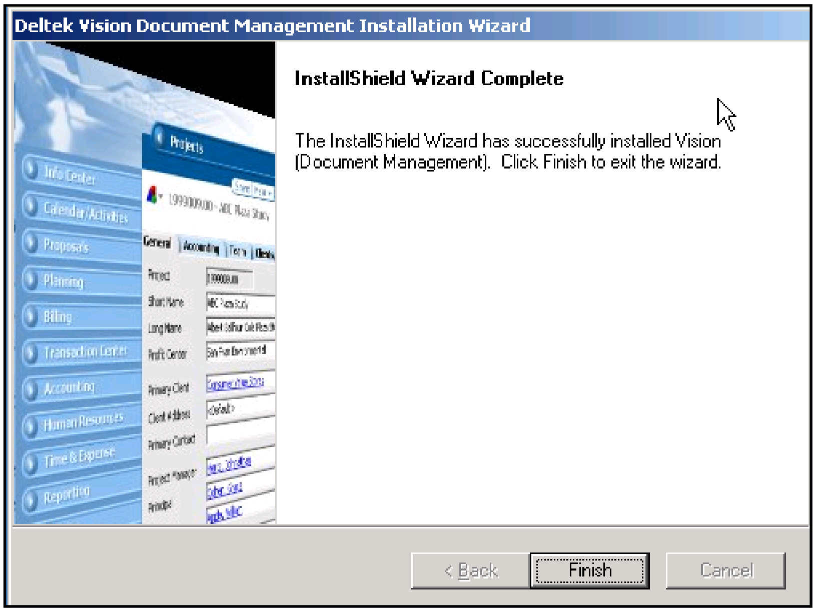
The wizard is ready to begin installation.

Click Install to begin the installation.

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

7. Click **Install** to start the installation.

8. Click **Finish** when the installation is completed.



Deltek Vision Document Management Installation Wizard

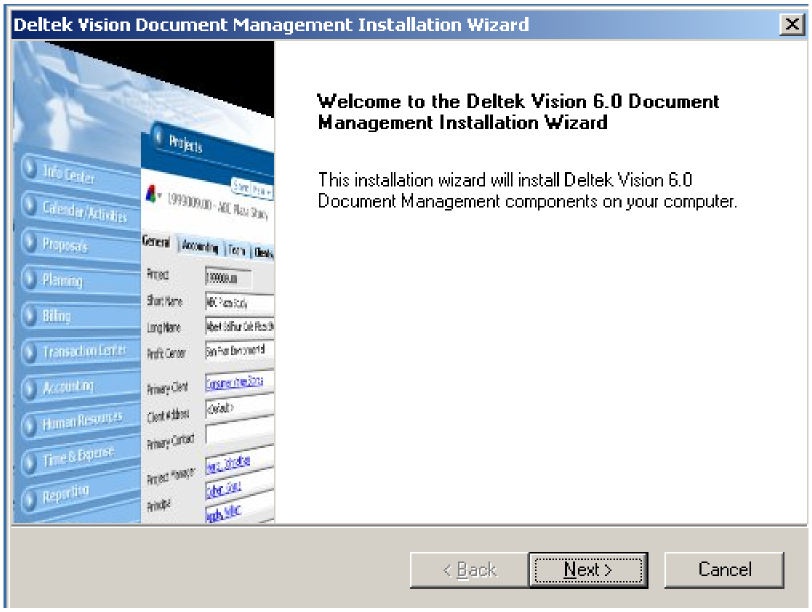
**InstallShield Wizard Complete**

The InstallShield Wizard has successfully installed Vision (Document Management). Click Finish to exit the wizard.

# Install Vision Document Management on the WSS Server

**To install Vision Document Management on the WSS server, complete the following steps:**

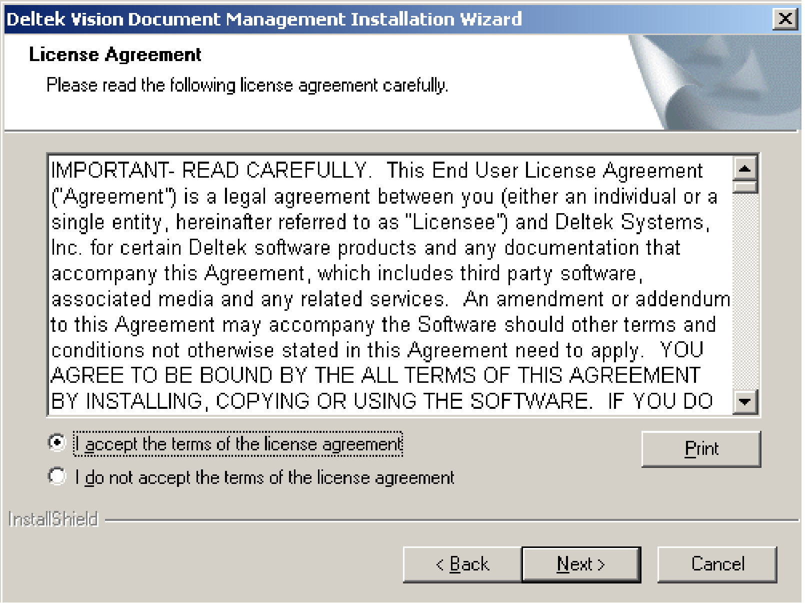
1. If you have previously installed Deltek Vision 5.1 Document Management (or other earlier versions), uninstall Deltek Vision Document Management using Add/Remove Programs. (This will not uninstall Windows SharePoint Services 3.0.)
2. Download DeltekVision61DM.exe and run the setup on your WSS server. The Welcome page displays.



**Welcome to the Deltek Vision 6.0 Document Management Installation Wizard**

This installation wizard will install Deltek Vision 6.0 Document Management components on your computer.

3. Click **Next**. The License Agreement page displays.



**License Agreement**

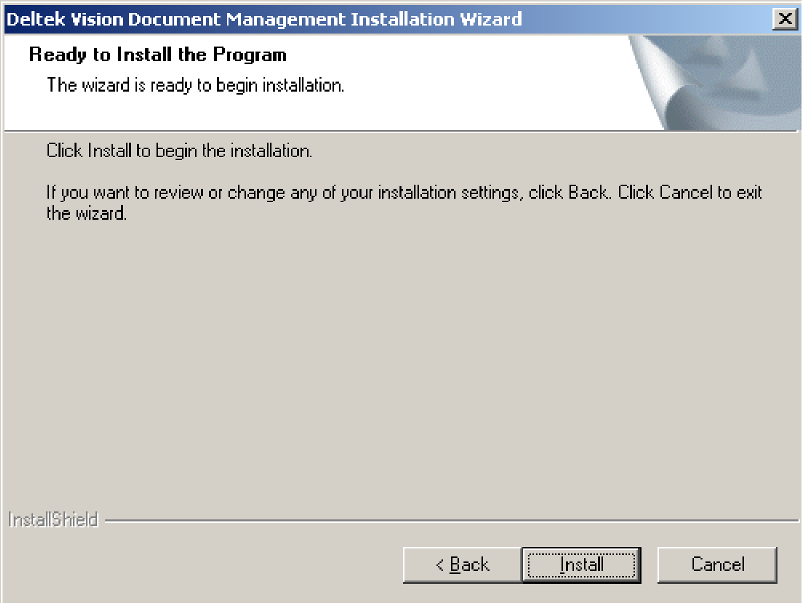
Please read the following license agreement carefully.

IMPORTANT- READ CAREFULLY. This End User License Agreement ("Agreement") is a legal agreement between you (either an individual or a single entity, hereinafter referred to as "Licensee") and Deltek Systems, Inc. for certain Deltek software products and any documentation that accompany this Agreement, which includes third party software, associated media and any related services. An amendment or addendum to this Agreement may accompany the Software should other terms and conditions not otherwise stated in this Agreement need to apply. YOU AGREE TO BE BOUND BY THE ALL TERMS OF THIS AGREEMENT BY INSTALLING, COPYING OR USING THE SOFTWARE. IF YOU DO

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

4. Accept the license agreement and click **Next**. The Ready to Install the Program page displays.



Deltek Vision Document Management Installation Wizard

**Ready to Install the Program**

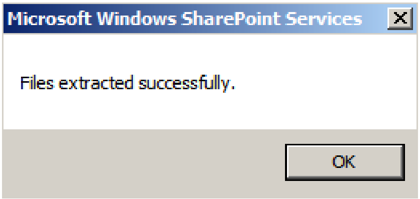
The wizard is ready to begin installation.

Click Install to begin the installation.

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

5. Click **Install** to start the installation. The installation automatically downloads the version of Windows SharePoint Services 3.0 specific to your platform (x86 or x64), extracts the WSS 3.0 setup files, and installs Windows SharePoint Services.

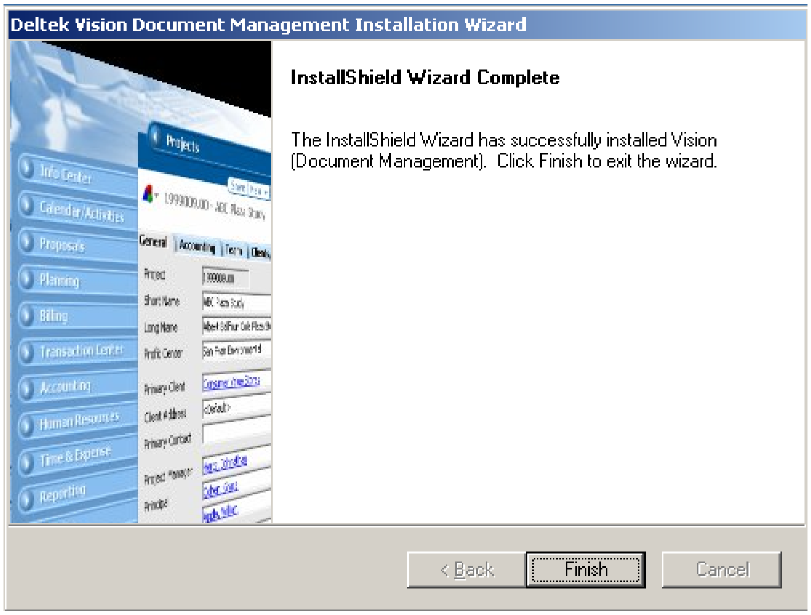
   During the extraction process, the following dialog box displays. You must click **OK** to continue the installation).



Microsoft Windows SharePoint Services

Files extracted successfully.

6. When the installation is complete, the InstallShield Wizard Complete page displays.



Deltek Vision Document Management Installation Wizard

**InstallShield Wizard Complete**

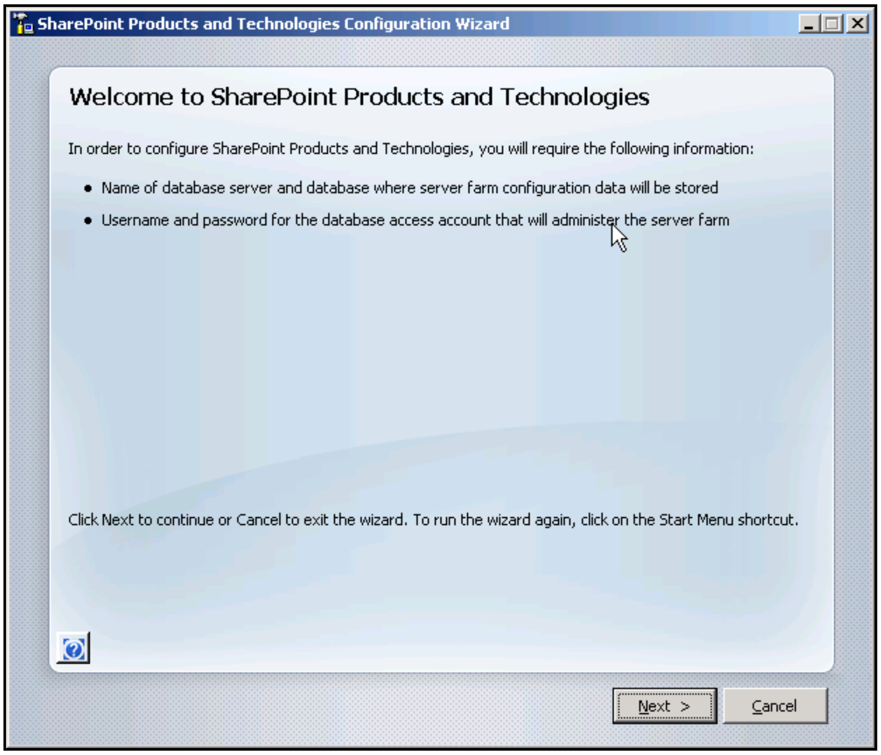
The InstallShield Wizard has successfully installed Vision (Document Management). Click Finish to exit the wizard.

7. Click **Finish**.

## Run the SharePoint Products and Technologies Configuration Wizard

### To run the SharePoint Products and Technologies Configuration wizard, complete the following steps:

1. To run the SharePoint Products & Technologies Configuration Wizard, click **Start » Administrative Tools » SharePoint Products and Technologies Wizard**. The Welcome page displays.



SharePoint Products and Technologies Configuration Wizard

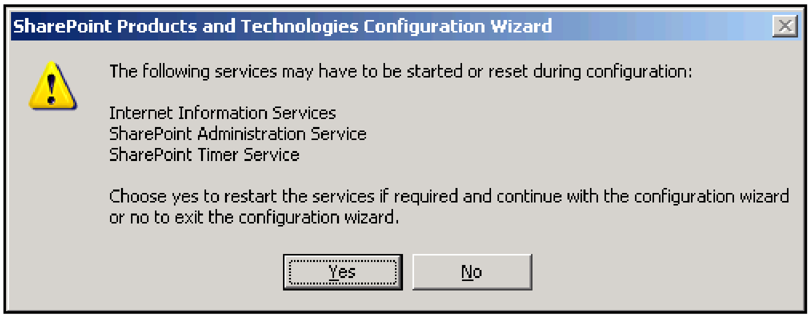
Welcome to SharePoint Products and Technologies

In order to configure SharePoint Products and Technologies, you will require the following information:

- Name of database server and database where server farm configuration data will be stored
- Username and password for the database access account that will administer the server farm

Click Next to continue or Cancel to exit the wizard. To run the wizard again, click on the Start Menu shortcut.

2. Click **Next**. The following dialog box displays.



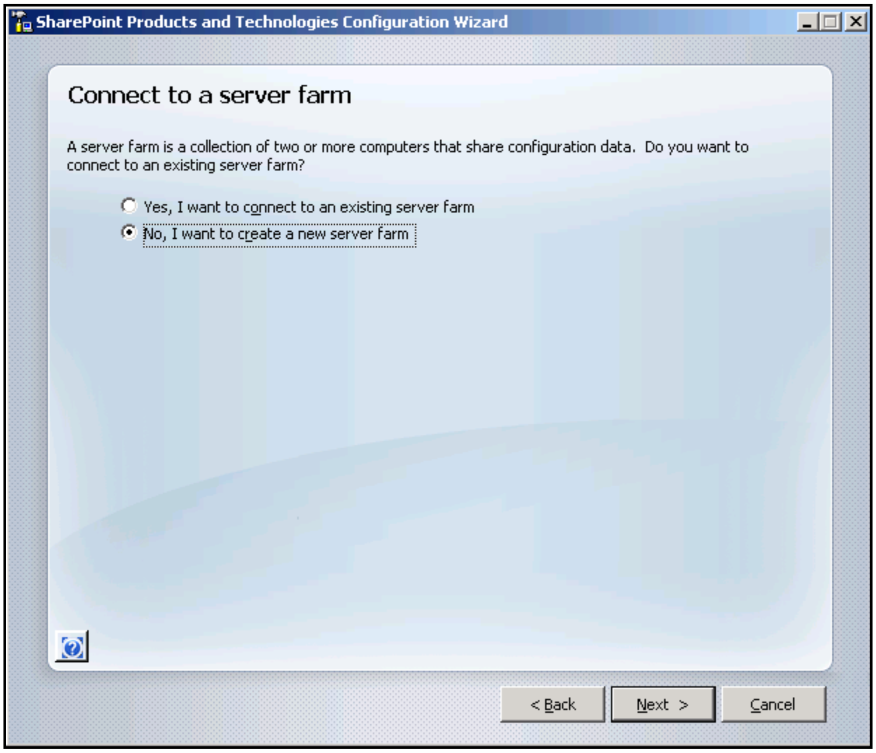
SharePoint Products and Technologies Configuration Wizard

The following services may have to be started or reset during configuration:

Internet Information Services
SharePoint Administration Service
SharePoint Timer Service

Choose yes to restart the services if required and continue with the configuration wizard or no to exit the configuration wizard.

3. Click **Yes**. The Connect to a server farm page displays.

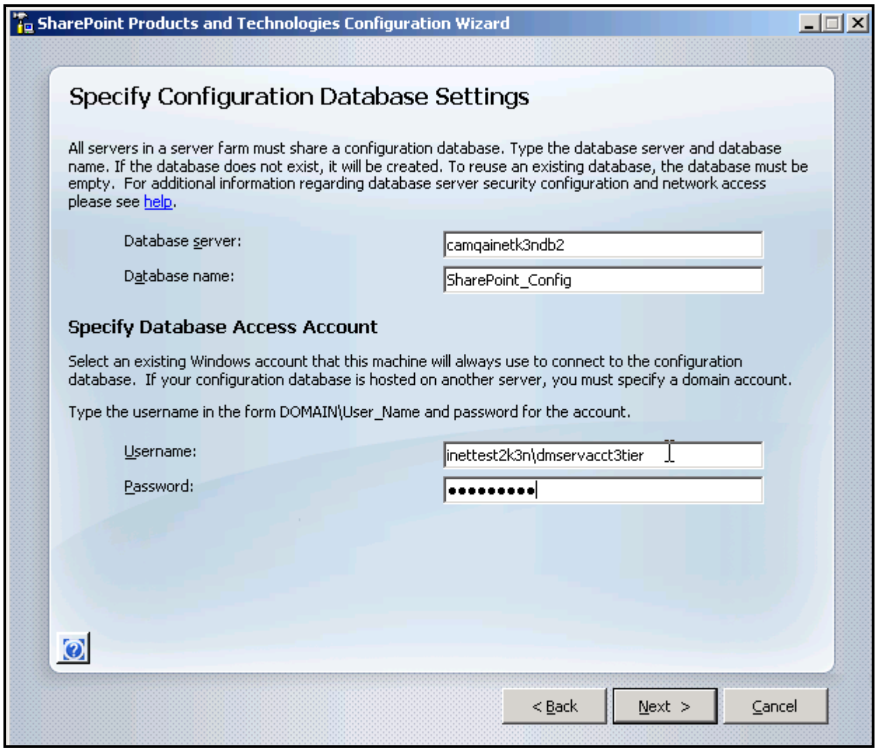


Connect to a server farm

A server farm is a collection of two or more computers that share configuration data. Do you want to connect to an existing server farm?

○ Yes, I want to connect to an existing server farm
● No, I want to create a new server farm

4. Select the **No, I want to create a new server farm** option and click **Next** to display the Specify Configuration Database Settings page.



Specify Configuration Database Settings

All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must be empty. For additional information regarding database server security configuration and network access please see help.

Database server: camqainetk3ndb2

Database name: SharePoint_Config

Specify Database Access Account

Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account.

Type the username in the form DOMAIN\User_Name and password for the account.

Username: inettest2k3n\dmservacct3tier

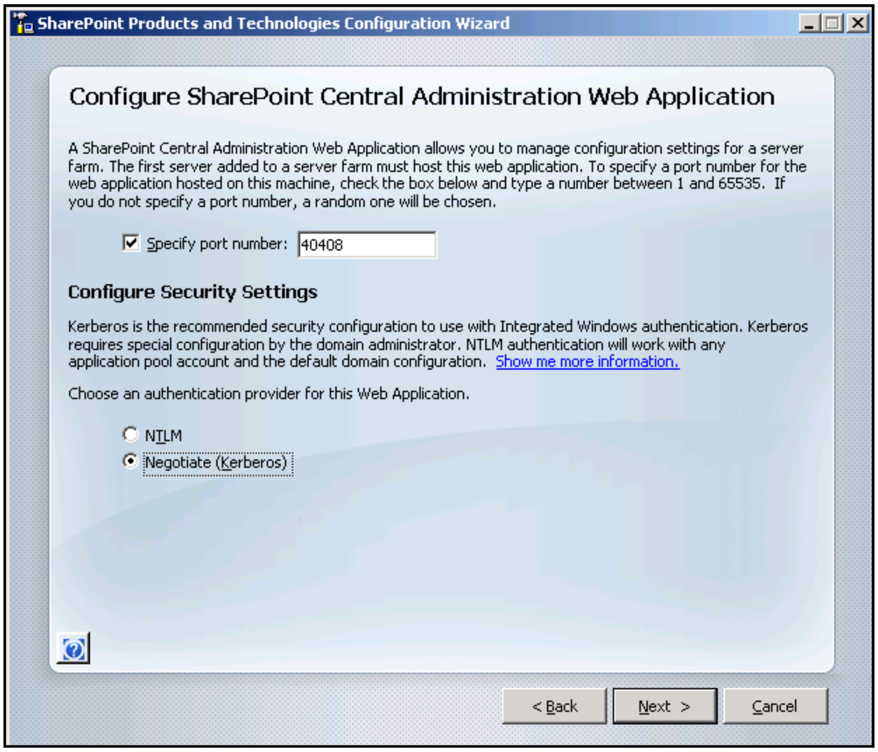
Password: ●●●●●●●●●●

5. Enter the name of the database server to host the SharePoint configuration database and accept the default database name: SharePoint_Config.

If you use SQL Server 2008, refer to Appendix B on page 93 for configuration requirements before proceeding.

6. Enter the domain and name of the Vision Application Pool Identity (configured and added to the local administrator group on the WSS server) as the **Username** for the SharePoint database access account and enter that user's **Password**.

7. Click **Next**. The Configure SharePoint Central Administration Web Application page displays.



Configure SharePoint Central Administration Web Application

A SharePoint Central Administration Web Application allows you to manage configuration settings for a server farm. The first server added to a server farm must host this web application. To specify a port number for the web application hosted on this machine, check the box below and type a number between 1 and 65535. If you do not specify a port number, a random one will be chosen.

☑ Specify port number: 40408

Configure Security Settings

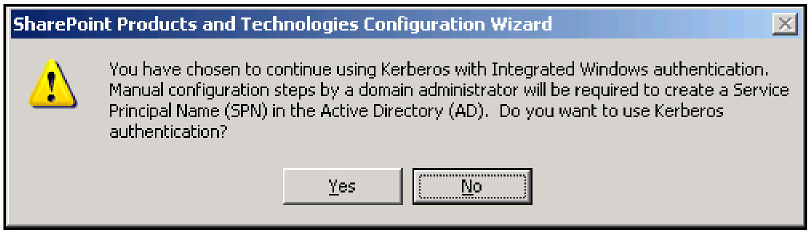
Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration. Show me more information.

Choose an authentication provider for this Web Application.

○ NTLM
● Negotiate (Kerberos)

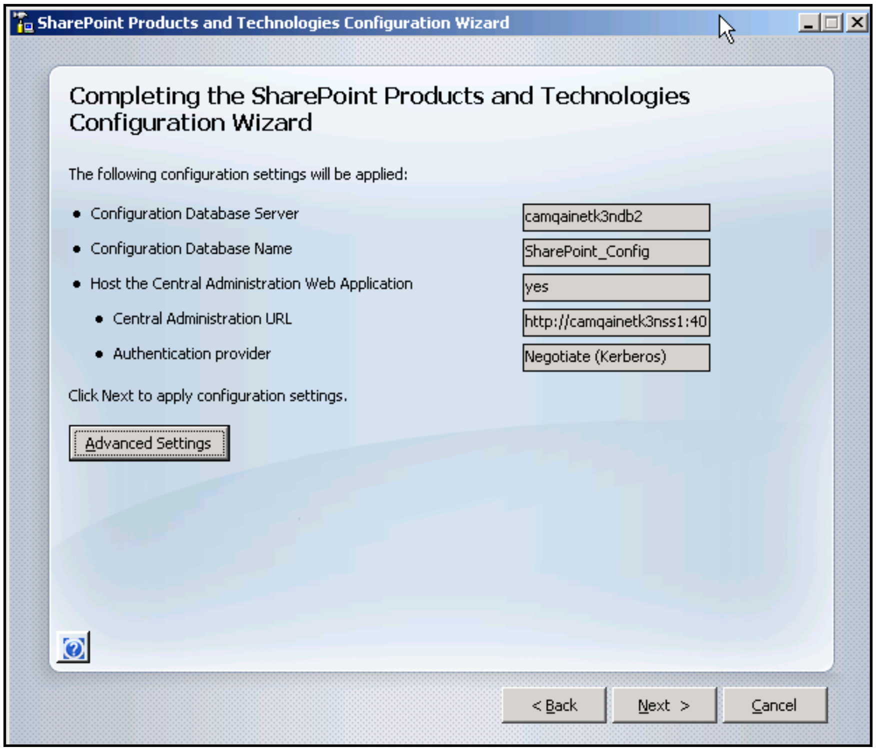
8. Specify the port to be used for the SharePoint Central Administration Web site.

9. Select **Negotiate (Kerberos)** for the authentication provider.



You have chosen to continue using Kerberos with Integrated Windows authentication. Manual configuration steps by a domain administrator will be required to create a Service Principal Name (SPN) in the Active Directory (AD). Do you want to use Kerberos authentication?

10. Click **Yes** to continue using Kerberos with Windows Authentication. The Completing the SharePoint Products and Technologies Configuration Wizard page displays.



SharePoint Products and Technologies Configuration Wizard

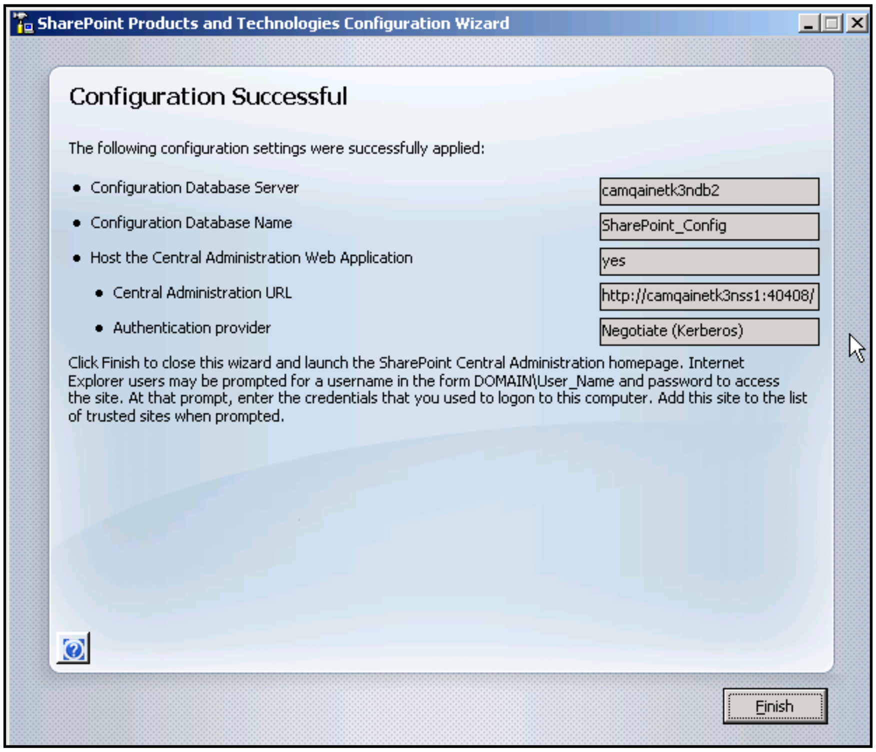
Completing the SharePoint Products and Technologies Configuration Wizard

The following configuration settings will be applied:

- Configuration Database Server: camqainetk3ndb2
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
  - Central Administration URL: http://camqainetk3nss1:40
  - Authentication provider: Negotiate (Kerberos)

Click Next to apply configuration settings.

11. Click **Next** to begin the configuration. This process may take some time to complete. The Configuration Successful page displays when configuration is complete.



SharePoint Products and Technologies Configuration Wizard

Configuration Successful

The following configuration settings were successfully applied:

- Configuration Database Server: camqainetk3ndb2
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
  - Central Administration URL: http://camqainetk3nss1:40408/
  - Authentication provider: Negotiate (Kerberos)

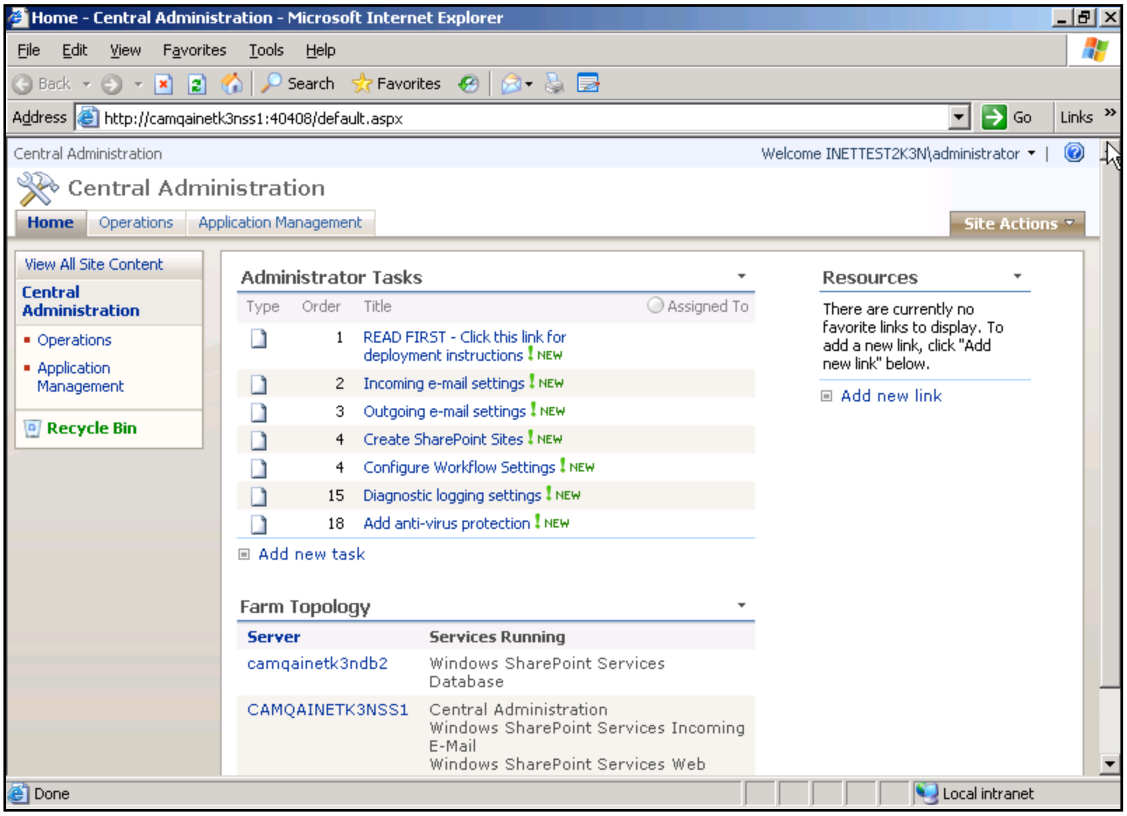
Click Finish to close this wizard and launch the SharePoint Central Administration homepage. Internet Explorer users may be prompted for a username in the form DOMAIN\User_Name and password to access the site. At that prompt, enter the credentials that you used to logon to this computer. Add this site to the list of trusted sites when prompted.

12. Click **Finish** to finish the configuration process. The SharePoint Central Administration page displays.

# Use SharePoint Central Administration to Complete the SharePoint Configuration

### To complete the SharePoint configuration, complete the following steps:

1. When you click **Finish** in the preceding procedure, SharePoint Central Administration is launched.



Address: http://camqainetk3nss1:40408/default.aspx

Administrator Tasks

| Type | Order | Title | Assigned To |
|---|---|---|---|
| | 1 | READ FIRST - Click this link for deployment instructions ! NEW | |
| | 2 | Incoming e-mail settings ! NEW | |
| | 3 | Outgoing e-mail settings ! NEW | |
| | 4 | Create SharePoint Sites ! NEW | |
| | 4 | Configure Workflow Settings ! NEW | |
| | 15 | Diagnostic logging settings ! NEW | |
| | 18 | Add anti-virus protection ! NEW | |

Add new task

Farm Topology

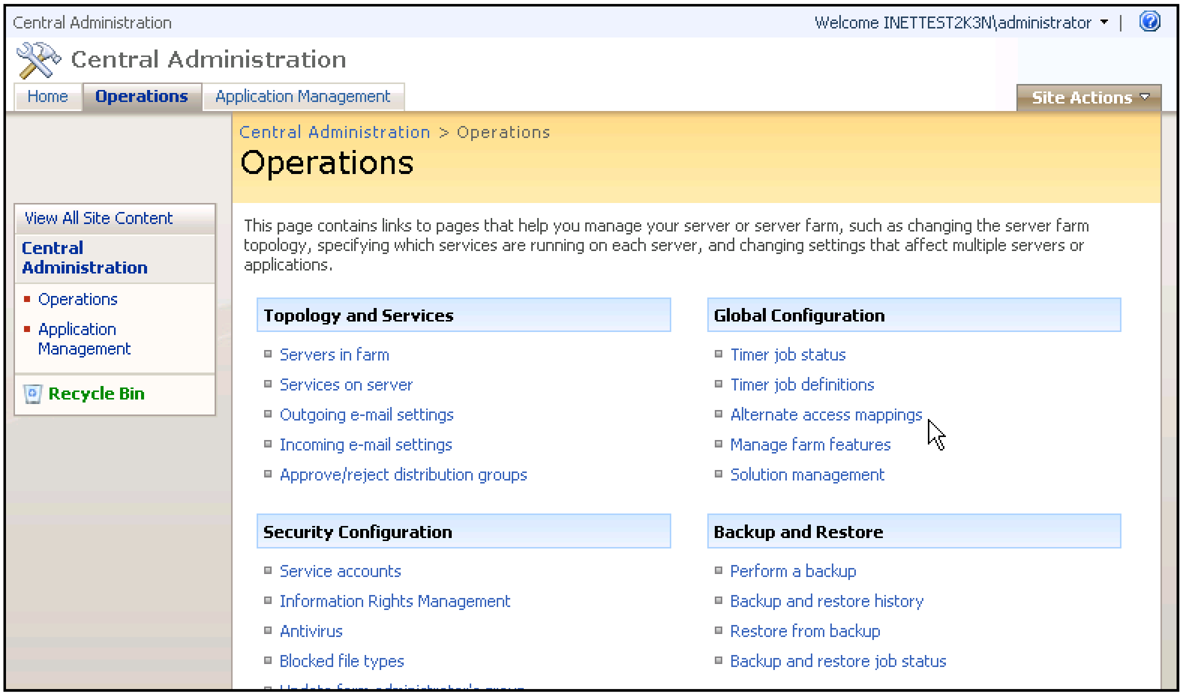
| Server | Services Running |
|---|---|
| camqainetk3ndb2 | Windows SharePoint Services Database |
| CAMQAINETK3NSS1 | Central Administration<br>Windows SharePoint Services Incoming E-Mail<br>Windows SharePoint Services Web |

Resources

There are currently no favorite links to display. To add a new link, click "Add new link" below.

Add new link

2. Click **Operations**. The Operations page displays.



Central Administration — Welcome INETTEST2K3N\administrator

Central Administration

Home | Operations | Application Management — Site Actions

Central Administration > Operations

Operations

This page contains links to pages that help you manage your server or server farm, such as changing the server farm topology, specifying which services are running on each server, and changing settings that affect multiple servers or applications.

**Topology and Services**

- Servers in farm
- Services on server
- Outgoing e-mail settings
- Incoming e-mail settings
- Approve/reject distribution groups

**Global Configuration**

- Timer job status
- Timer job definitions
- Alternate access mappings
- Manage farm features
- Solution management

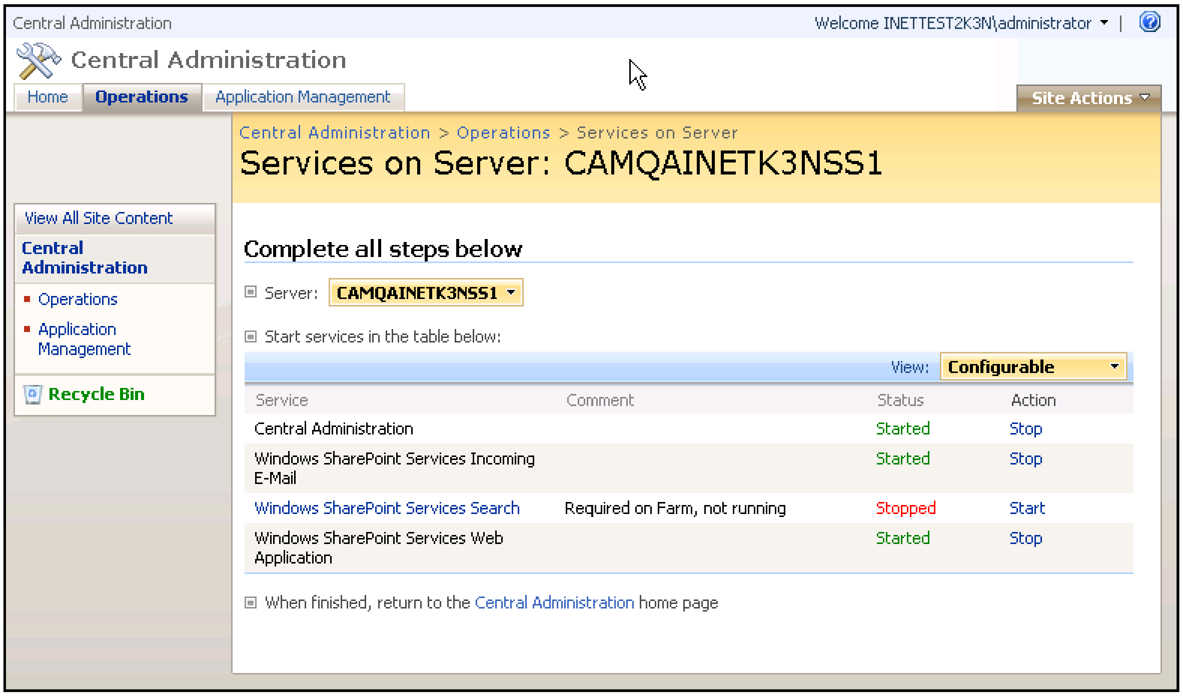
**Security Configuration**

- Service accounts
- Information Rights Management
- Antivirus
- Blocked file types
- Update farm administrator's group

**Backup and Restore**

- Perform a backup
- Backup and restore history
- Restore from backup
- Backup and restore job status

3. Click **Services on Server** under **Topology and Services** to configure the SharePoint Services search.



Central Administration — Welcome INETTEST2K3N\administrator

Central Administration

Home | Operations | Application Management — Site Actions

Central Administration > Operations > Services on Server

Services on Server: CAMQAINETK3NSS1

Complete all steps below

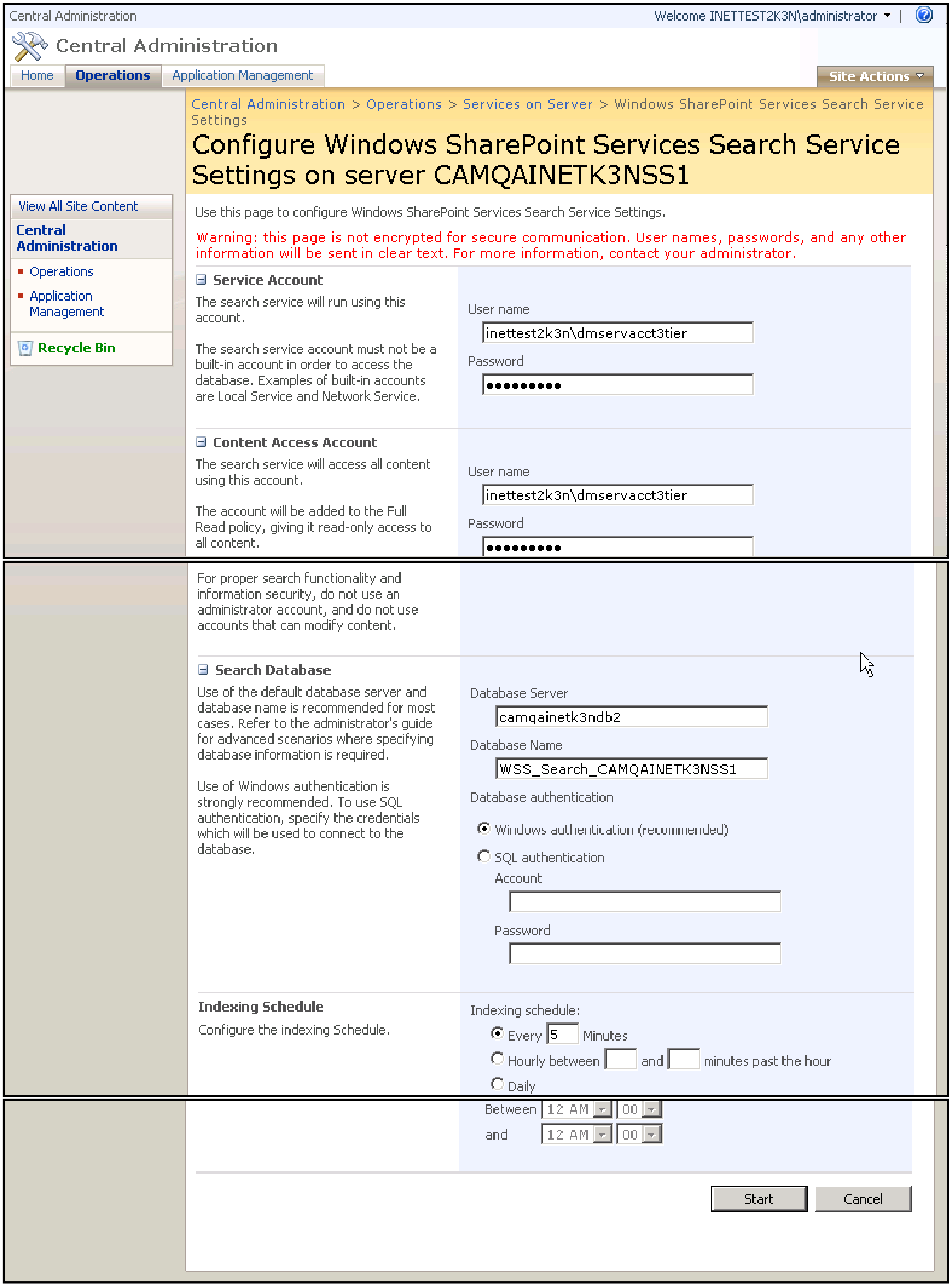
- Server: CAMQAINETK3NSS1
- Start services in the table below:

View: Configurable

| Service | Comment | Status | Action |
|---|---|---|---|
| Central Administration | | Started | Stop |
| Windows SharePoint Services Incoming E-Mail | | Started | Stop |
| Windows SharePoint Services Search | Required on Farm, not running | Stopped | Start |
| Windows SharePoint Services Web Application | | Started | Stop |

- When finished, return to the Central Administration home page

4. Locate the **Windows SharePoint Services Search** option and click **Start**.



Central Administration > Operations > Services on Server > Windows SharePoint Services Search Service Settings

Configure Windows SharePoint Services Search Service Settings on server CAMQAINETK3NSS1

Use this page to configure Windows SharePoint Services Search Service Settings.

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

**Service Account**

The search service will run using this account.

The search service account must not be a built-in account in order to access the database. Examples of built-in accounts are Local Service and Network Service.

User name: inettest2k3n\dmservacct3tier

Password: ●●●●●●●●●

**Content Access Account**

The search service will access all content using this account.

The account will be added to the Full Read policy, giving it read-only access to all content.

For proper search functionality and information security, do not use an administrator account, and do not use accounts that can modify content.

User name: inettest2k3n\dmservacct3tier

Password: ●●●●●●●●●

**Search Database**

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: camqainetk3ndb2

Database Name: WSS_Search_CAMQAINETK3NSS1

Database authentication

● Windows authentication (recommended)

○ SQL authentication

Account:

Password:

**Indexing Schedule**

Configure the indexing Schedule.

Indexing schedule:

● Every 5 Minutes

○ Hourly between ___ and ___ minutes past the hour

○ Daily

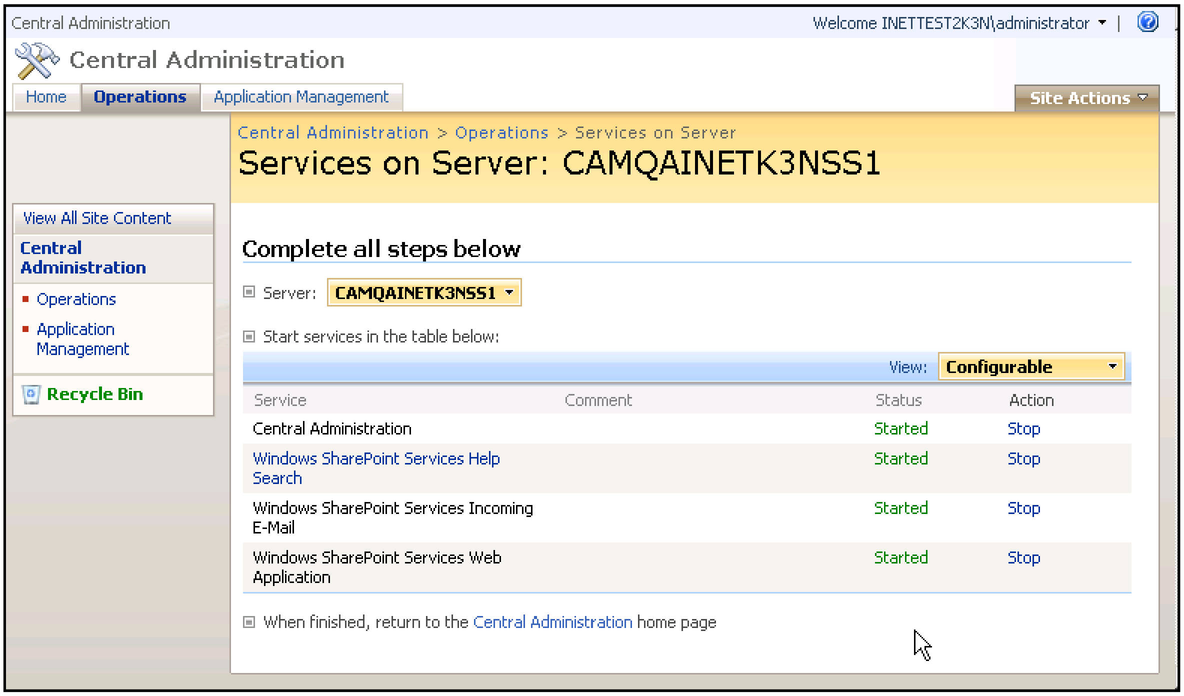
Between 12 AM 00

and 12 AM 00

Start Cancel

5. Configure the search service to include the Service account and Content Access account (use the same account information as your Vision Application Pool Identity).

6. Configure **Search Database** as shown and click **Start**. After a minute or so, the service's status changes to **Started**.



Services on Server: CAMQAINETK3NSS1

Complete all steps below

Server: CAMQAINETK3NSS1

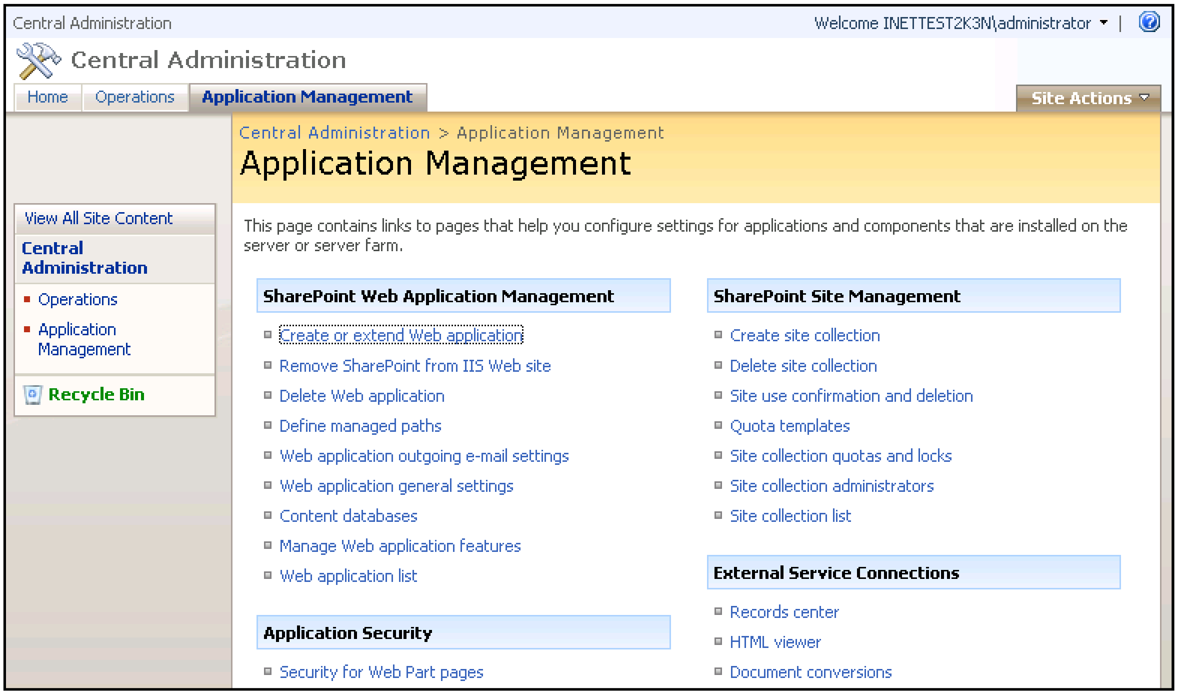
Start services in the table below:

View: Configurable

| Service | Comment | Status | Action |
|---|---|---|---|
| Central Administration | | Started | Stop |
| Windows SharePoint Services Help Search | | Started | Stop |
| Windows SharePoint Services Incoming E-Mail | | Started | Stop |
| Windows SharePoint Services Web Application | | Started | Stop |

When finished, return to the Central Administration home page

7. Click **Application Management** to configure the SharePoint Web Application.



Application Management

This page contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

SharePoint Web Application Management

- Create or extend Web application
- Remove SharePoint from IIS Web site
- Delete Web application
- Define managed paths
- Web application outgoing e-mail settings
- Web application general settings
- Content databases
- Manage Web application features
- Web application list

Application Security

- Security for Web Part pages

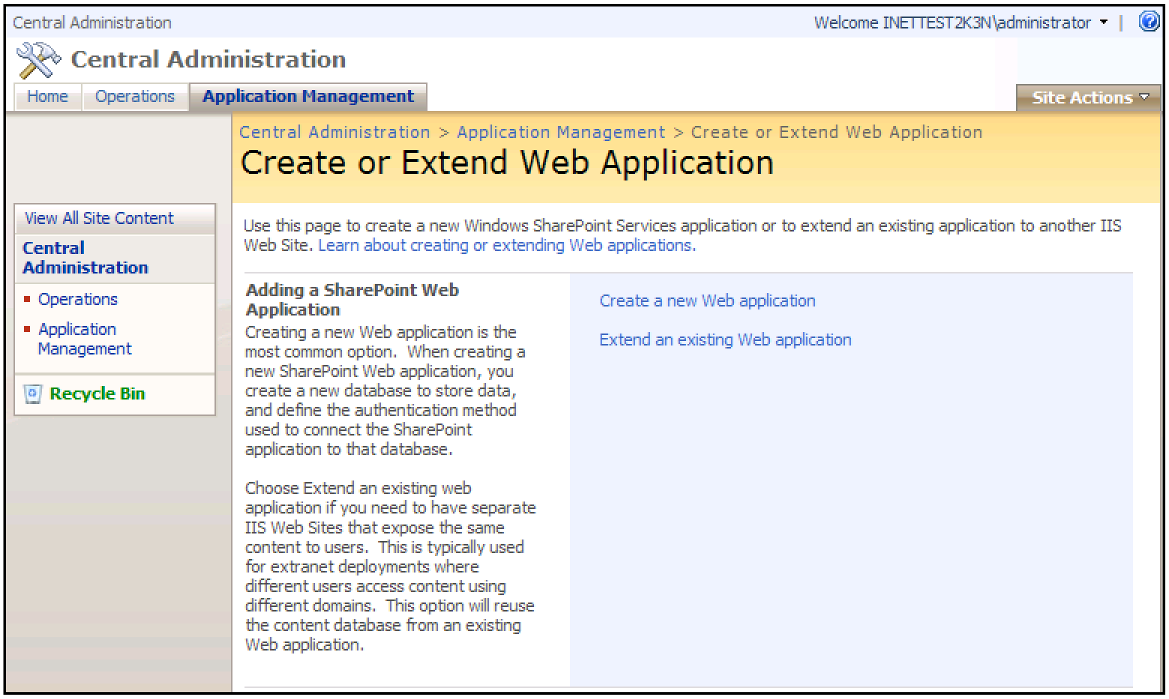
SharePoint Site Management

- Create site collection
- Delete site collection
- Site use confirmation and deletion
- Quota templates
- Site collection quotas and locks
- Site collection administrators
- Site collection list

External Service Connections

- Records center
- HTML viewer
- Document conversions

8. Select the **Create or extend Web application** option. The Create or Extend Web Application page displays.



Central Administration > Application Management > Create or Extend Web Application

Create or Extend Web Application

Use this page to create a new Windows SharePoint Services application or to extend an existing application to another IIS Web Site. Learn about creating or extending Web applications.

**Adding a SharePoint Web Application**

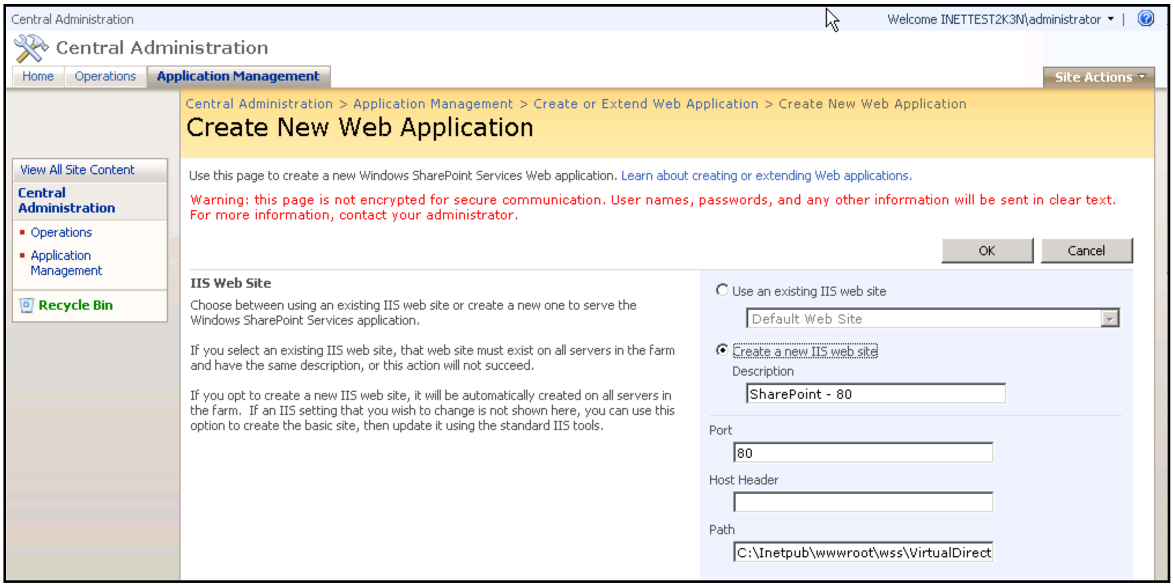
Creating a new Web application is the most common option. When creating a new SharePoint Web application, you create a new database to store data, and define the authentication method used to connect the SharePoint application to that database.

Choose Extend an existing web application if you need to have separate IIS Web Sites that expose the same content to users. This is typically used for extranet deployments where different users access content using different domains. This option will reuse the content database from an existing Web application.

Create a new Web application

Extend an existing Web application

9. Click **Create a new Web application**. The Create a New Web Application page displays.



Central Administration > Application Management > Create or Extend Web Application > Create New Web Application

Create New Web Application

Use this page to create a new Windows SharePoint Services Web application. Learn about creating or extending Web applications.

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

**IIS Web Site**

Choose between using an existing IIS web site or create a new one to serve the Windows SharePoint Services application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same description, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

○ Use an existing IIS web site

Default Web Site

● Create a new IIS web site

Description: SharePoint - 80

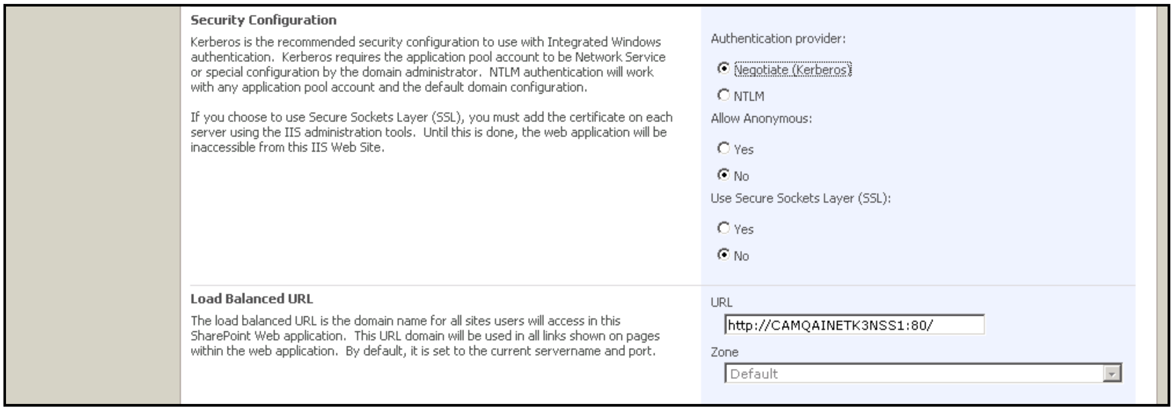
Port: 80

Host Header:

Path: C:\Inetpub\wwwroot\wss\VirtualDirect

10. Select the **Create a new IIS web site** option. Enter a description for the Web site and specify a port in **Port**.

    Because WSS is installed on its own server, it can run on the Default Web Site and Port 80. To accomplish this, select the existing Web site (Default Web Site). Note the entry in **Path**, which by default is the root of your WSS Web site in a directory named after the port chosen under c:\inetpub\wwwroot\wss\virtualdirectories.



**Security Configuration**

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires the application pool account to be Network Service or special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration.

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS Web Site.

Authentication provider:

● Negotiate (Kerberos)

○ NTLM

Allow Anonymous:

○ Yes

● No

Use Secure Sockets Layer (SSL):

○ Yes

● No

**Load Balanced URL**

The load balanced URL is the domain name for all sites users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port.

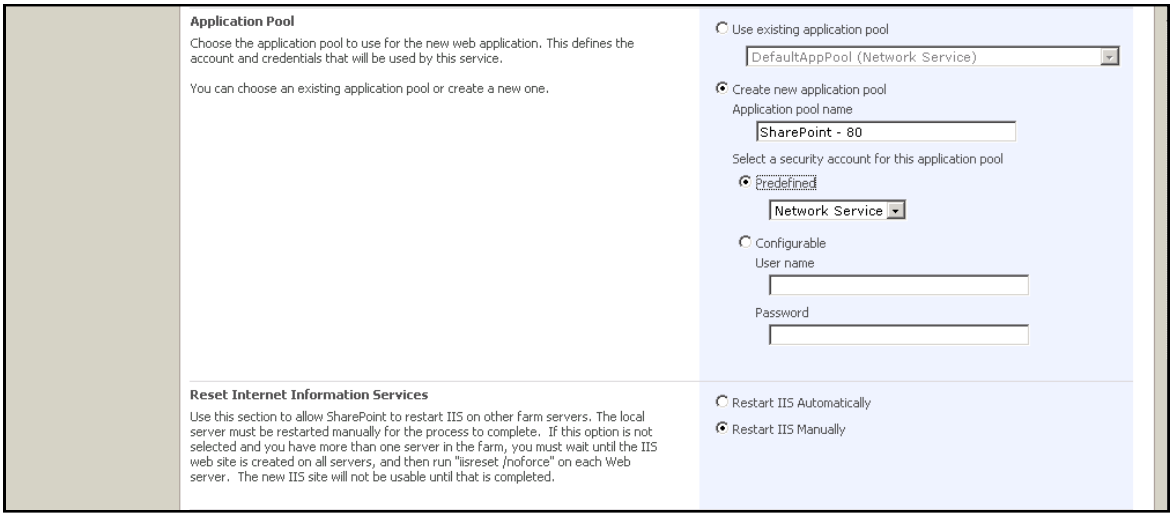
URL

http://CAMQAINETK3NSS1:80/

Zone

Default

11. Select **Negotiate (Kerberos)** under **Authentication provider**.
12. For the **Allow Anonymous** and **Use Secure Sockets Layer (SSL)** options, accept the default of **No**. If you want to use SSL with SharePoint, you can configure SSL later but you must not configure SSL to be required.



**Application Pool**

Choose the application pool to use for the new web application. This defines the account and credentials that will be used by this service.

You can choose an existing application pool or create a new one.

○ Use existing application pool

DefaultAppPool (Network Service)

● Create new application pool

Application pool name

SharePoint - 80

Select a security account for this application pool

● Predefined

Network Service

○ Configurable

User name

Password

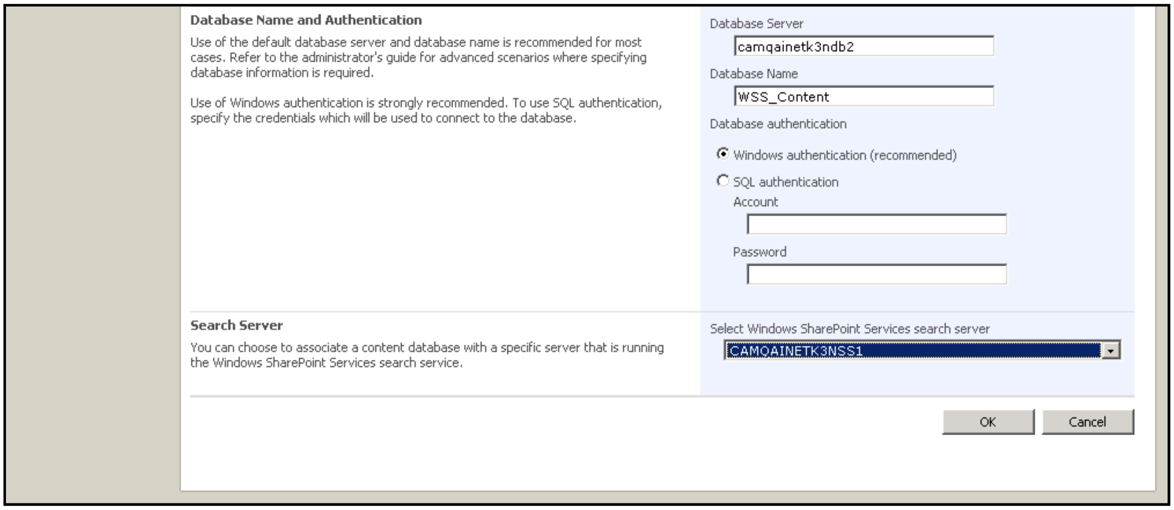
**Reset Internet Information Services**

Use this section to allow SharePoint to restart IIS on other farm servers. The local server must be restarted manually for the process to complete. If this option is not selected and you have more than one server in the farm, you must wait until the IIS web site is created on all servers, and then run "iisreset /noforce" on each Web server. The new IIS site will not be usable until that is completed.

○ Restart IIS Automatically

● Restart IIS Manually

13. Select the **Create a new application pool** option and provide a name (Deltek recommends using the same name as the Web site). Note that if you are installing WSS to the Default Web Site, you can also choose to use the Default App Pool rather than creating a new application pool.
14. Select **Predefined** and **Network Service** for the security account to be used for the application pool.
15. Select the **Restart IIS Manually** option for **Reset Internet Information Services**.



**Database Name and Authentication**

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: camqainetk3ndb2

Database Name: WSS_Content

Database authentication

● Windows authentication (recommended)

○ SQL authentication

Account:

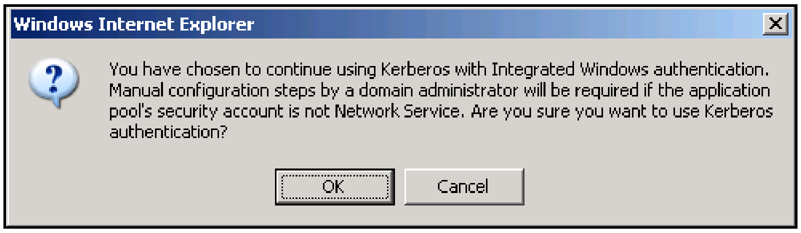
Password:

**Search Server**

You can choose to associate a content database with a specific server that is running the Windows SharePoint Services search service.

Select Windows SharePoint Services search server: CAMQAINETK3NSS1

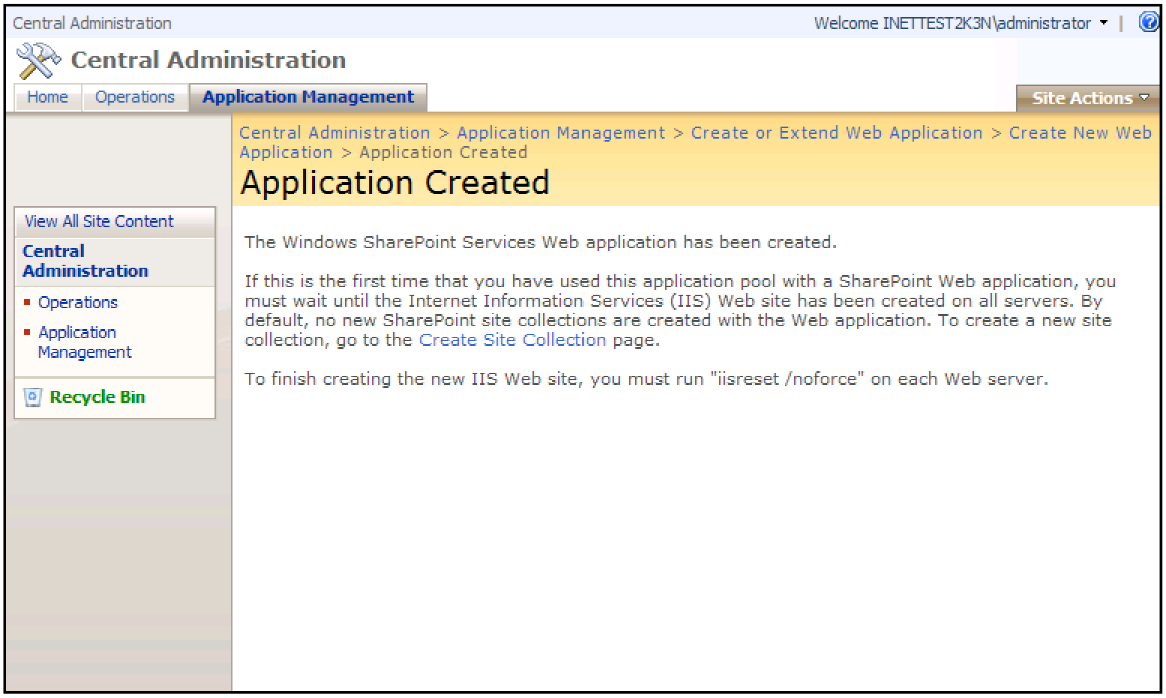
16. Verify the name of the server in **Database Server**. (It should be the same as that used for the SharePoint configuration database server.) Accept the default in **Database Name** for the content database.
17. Select **Windows authentication (recommended)** under **Database authentication**. (This will use the SharePoint service account and Vision Application Pool Identity configured previously.)
18. Select the search server in **Select Windows SharePoint Services search server** and click **OK**. The following dialog box displays.



Windows Internet Explorer

You have chosen to continue using Kerberos with Integrated Windows authentication. Manual configuration steps by a domain administrator will be required if the application pool's security account is not Network Service. Are you sure you want to use Kerberos authentication?

19. Click **OK** to use Kerberos for Windows Authentication. After a few minutes, the Application Created page displays. It indicates the status of the process to create a new Web application.



Central Administration > Application Management > Create or Extend Web Application > Create New Web Application > Application Created

Application Created

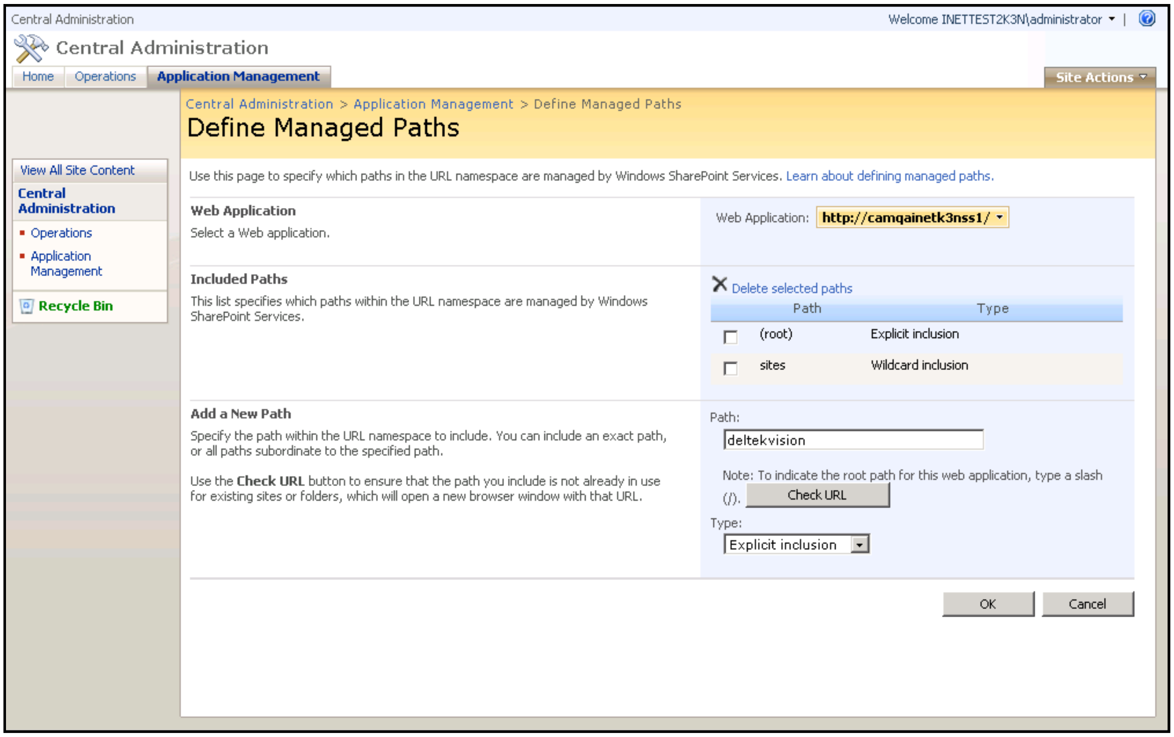
The Windows SharePoint Services Web application has been created.

If this is the first time that you have used this application pool with a SharePoint Web application, you must wait until the Internet Information Services (IIS) Web site has been created on all servers. By default, no new SharePoint site collections are created with the Web application. To create a new site collection, go to the Create Site Collection page.

To finish creating the new IIS Web site, you must run "iisreset /noforce" on each Web server.

20. Do not click the **Create Site Collection** link at this time. It is still necessary to add DeltekVision as a managed path with explicit inclusion before you create the site collection.

21. Click **Application Management** and select the **Define Managed Paths** option.



Central Administration > Application Management > Define Managed Paths

Define Managed Paths

Use this page to specify which paths in the URL namespace are managed by Windows SharePoint Services. Learn about defining managed paths.

**Web Application**
Select a Web application.

Web Application: **http://camqainetk3nss1/**

**Included Paths**
This list specifies which paths within the URL namespace are managed by Windows SharePoint Services.

| | Path | Type |
|---|---|---|
| □ | (root) | Explicit inclusion |
| □ | sites | Wildcard inclusion |

**Add a New Path**
Specify the path within the URL namespace to include. You can include an exact path, or all paths subordinate to the specified path.

Use the **Check URL** button to ensure that the path you include is not already in use for existing sites or folders, which will open a new browser window with that URL.

Path: deltekvision

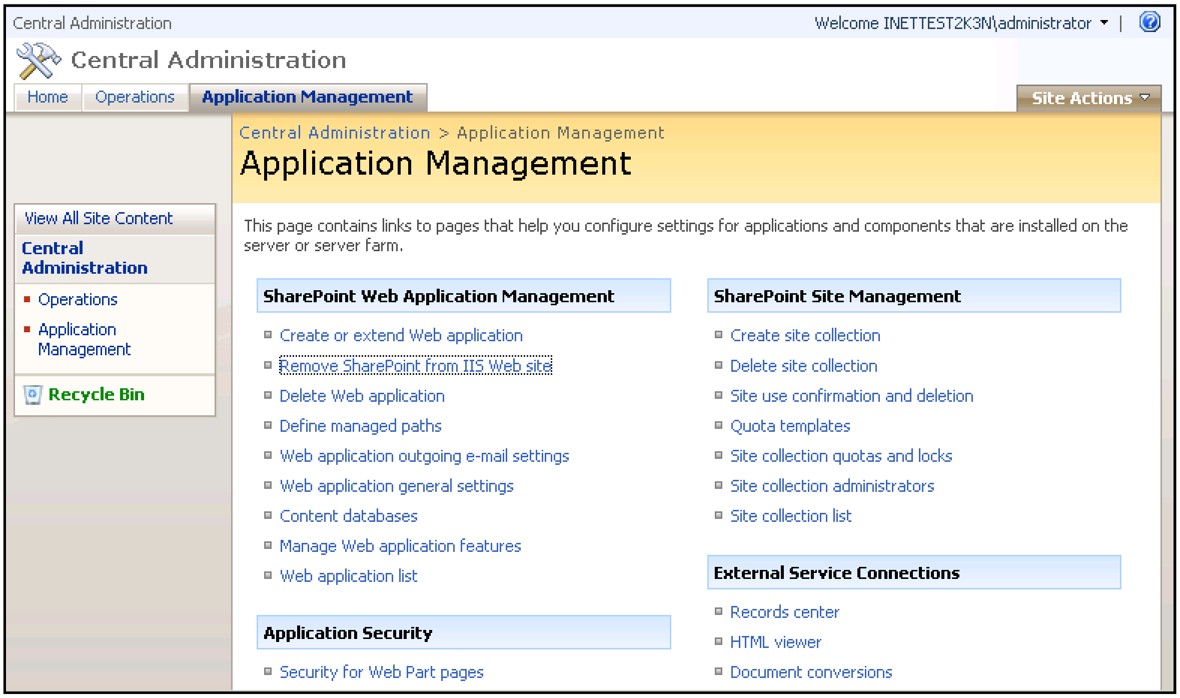
Note: To indicate the root path for this web application, type a slash (/).

Type: Explicit inclusion

22. Enter **DeltekVision** in **Path** and select **Explicit inclusion** in **Type**.

23. Click **OK**.

24. Click **Application Management** and select the **Create site collection** option under **SharePoint Site Management**.



Central Administration | Welcome INETTEST2K3N\administrator ▾ |

Central Administration

Home | Operations | **Application Management** | Site Actions ▾

Central Administration > Application Management

# Application Management

View All Site Content

**Central Administration**

- Operations
- Application Management

**Recycle Bin**

This page contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

**SharePoint Web Application Management**

- Create or extend Web application
- Remove SharePoint from IIS Web site
- Delete Web application
- Define managed paths
- Web application outgoing e-mail settings
- Web application general settings
- Content databases
- Manage Web application features
- Web application list

**Application Security**

- Security for Web Part pages

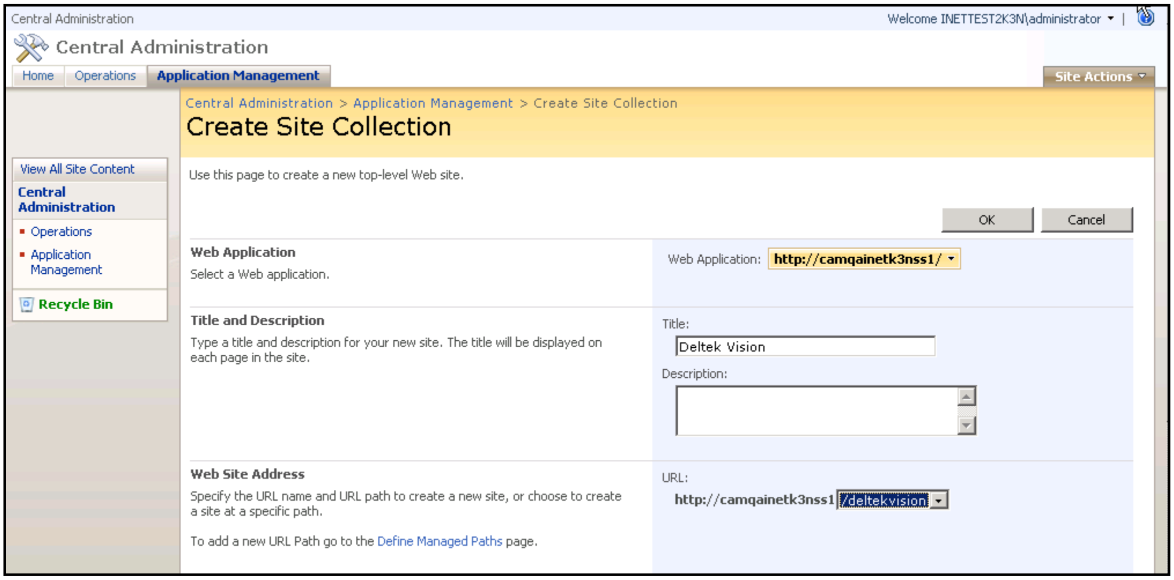
**SharePoint Site Management**

- Create site collection
- Delete site collection
- Site use confirmation and deletion
- Quota templates
- Site collection quotas and locks
- Site collection administrators
- Site collection list

**External Service Connections**

- Records center
- HTML viewer
- Document conversions

The Create Site Collection page displays.



Central Administration | Welcome INETTEST2K3N\administrator ▾ |

Central Administration

Home | Operations | **Application Management** | Site Actions ▾

Central Administration > Application Management > Create Site Collection

# Create Site Collection

View All Site Content

**Central Administration**

- Operations
- Application Management

**Recycle Bin**

Use this page to create a new top-level Web site.

OK | Cancel

**Web Application**

Select a Web application.

Web Application: **http://camqainetk3nss1/** ▾

**Title and Description**

Type a title and description for your new site. The title will be displayed on each page in the site.

Title: Deltek Vision

Description:

**Web Site Address**

Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.

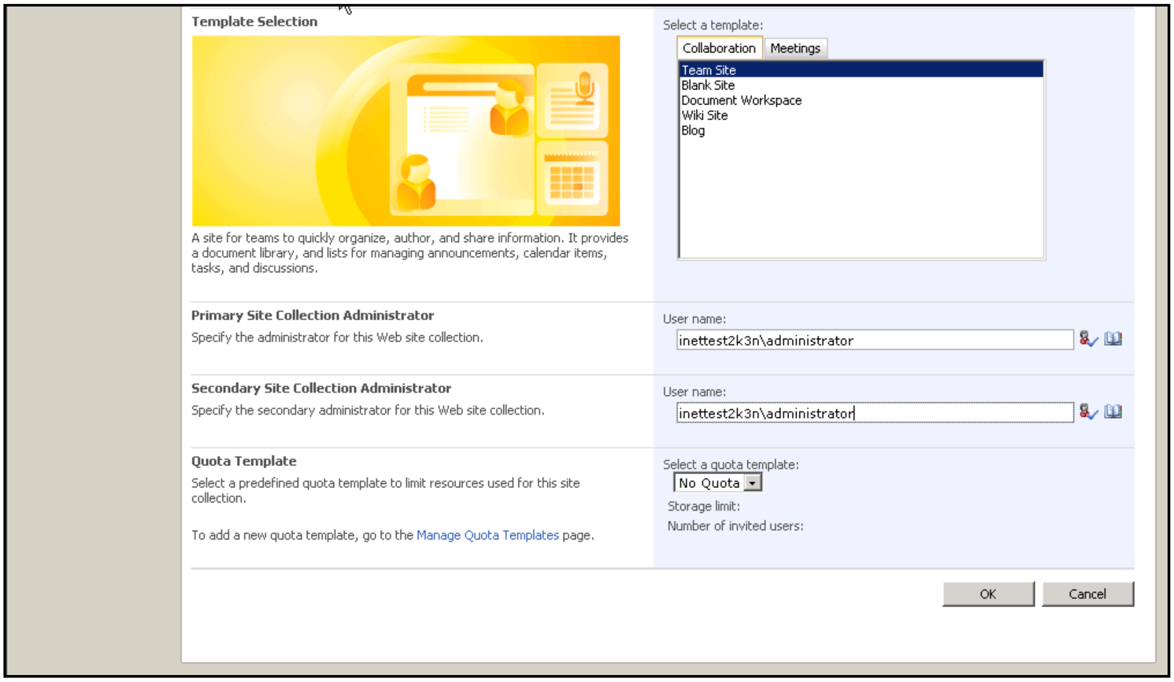
To add a new URL Path go to the Define Managed Paths page.

URL:

http://camqainetk3nss1 /deltekvision ▾

25. Enter **Deltek Vision** in **Title** and enter a description, if appropriate.

26. From the **URL** drop-down list, select **/deltekvision**. This will be the top level root for Vision Document Management.



**Template Selection**

A site for teams to quickly organize, author, and share information. It provides a document library, and lists for managing announcements, calendar items, tasks, and discussions.

Select a template:

**Primary Site Collection Administrator**

Specify the administrator for this Web site collection.

User name: inettest2k3n\administrator

**Secondary Site Collection Administrator**

Specify the secondary administrator for this Web site collection.

User name: inettest2k3n\administrator

**Quota Template**

Select a predefined quota template to limit resources used for this site collection.

To add a new quota template, go to the Manage Quota Templates page.

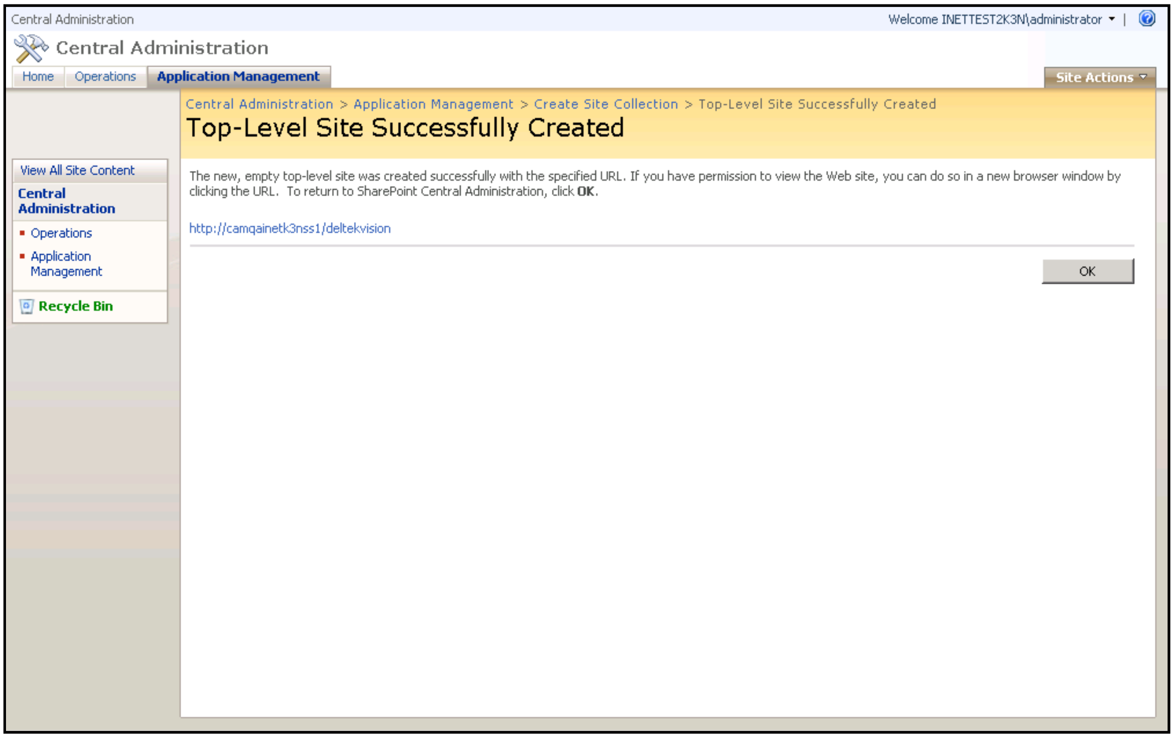
Select a quota template: No Quota

Storage limit:

Number of invited users:

27. Under **Select a template**, accept the default of **Team Site** for the template to be used and enter a username in each of the **User name** fields for the primary and secondary site collection administrators.

28. Select **No Quota** in **Select a quota template** and click **OK**. The Top-Level Site Successfully Created page displays.



Central Administration > Application Management > Create Site Collection > Top-Level Site Successfully Created

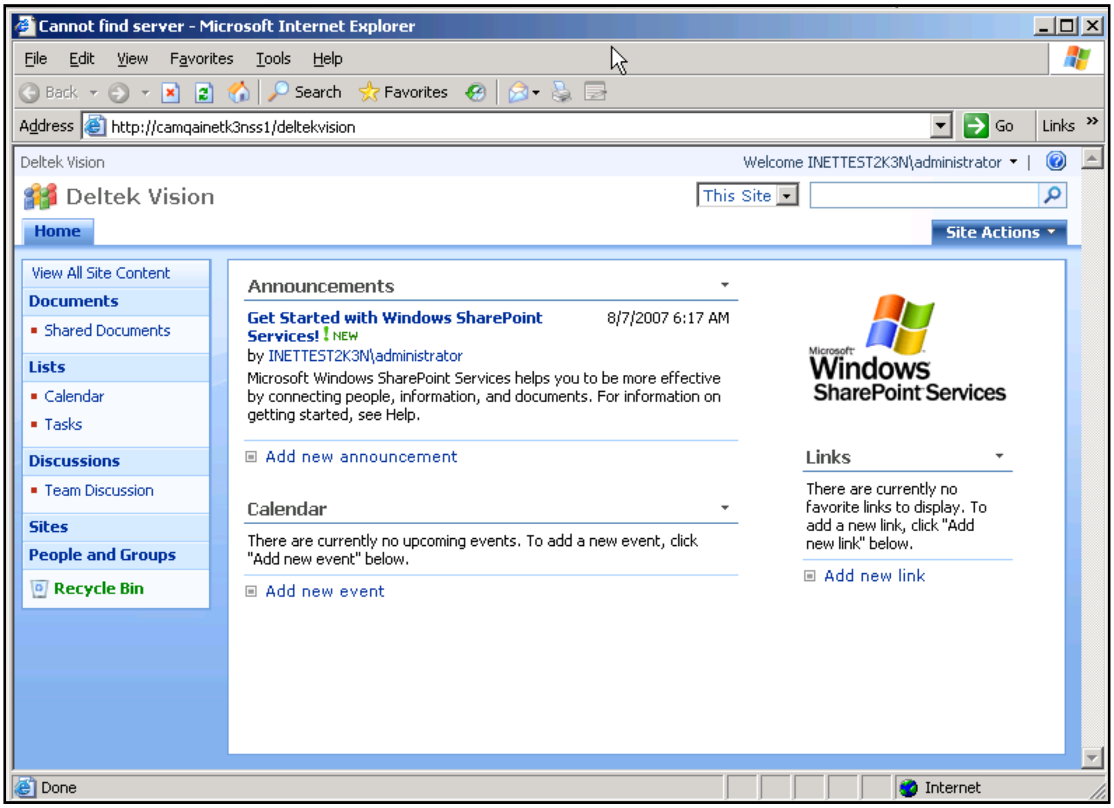
Top-Level Site Successfully Created

The new, empty top-level site was created successfully with the specified URL. If you have permission to view the Web site, you can do so in a new browser window by clicking the URL. To return to SharePoint Central Administration, click **OK**.

http://camqainetk3nss1/deltekvision

29. Click **Start** » **Run**, enter **iisreset /noforce,** and click **Enter**.

30. Click the link for the top level site (in our example it is http://camqainetk3nss1/deltekvision) to display the site.



Get Started with Windows SharePoint Services! NEW 8/7/2007 6:17 AM
by INETTEST2K3N\administrator
Microsoft Windows SharePoint Services helps you to be more effective by connecting people, information, and documents. For information on getting started, see Help.

Add new announcement

Calendar

There are currently no upcoming events. To add a new event, click "Add new event" below.

Add new event

There are currently no favorite links to display. To add a new link, click "Add new link" below.

Add new link

31. The SharePoint configuration is complete. Close SharePoint Central Administration.

## Configure SharePoint for a Fully Qualified Domain Name (FQDN) URL (Optional)

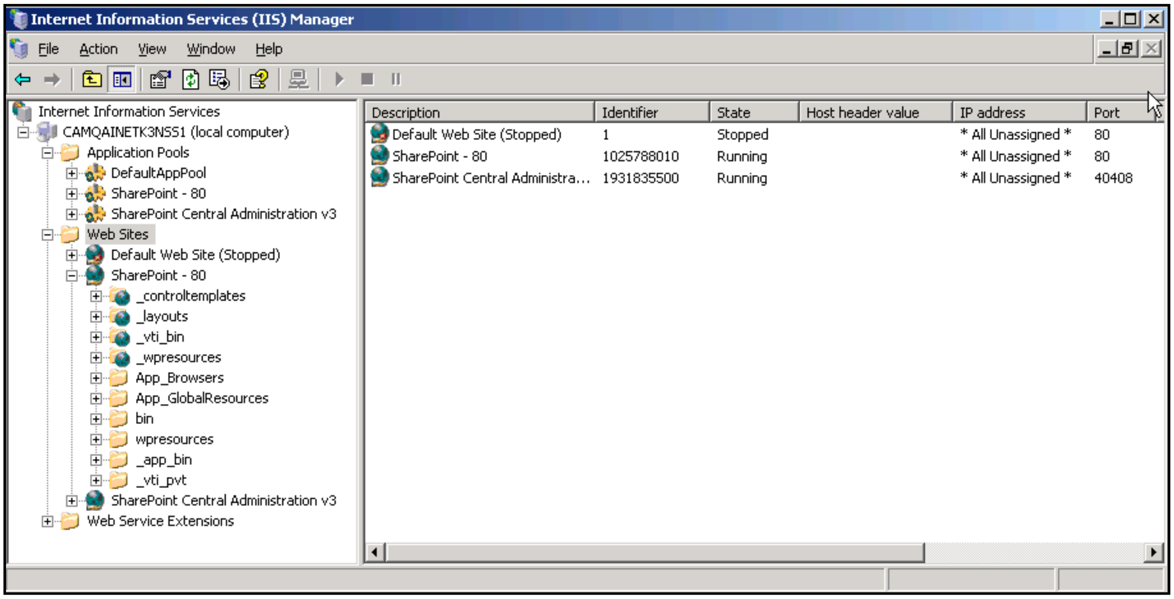
If you will be configuring your SharePoint server to use a custom DNS record for the URL you must create an additional SPN and also to create Alternate Access Mappings in SharePoint.

See “Appendix C: SPN Configuration When Using Custom DNS Records” on page 99 for more information.

## Verify IIS Configuration and Configure Deltek Vision Document Management .NET Assembly

**To verify IIS configuration, complete the following steps:**

1. Use the directions that follow to open Internet Information Services to view these Web sites:
   - **Default Web Site** — Stopped.
   - **SharePoint – 80** — This is your WSS 3.0 Web site.
   - **SharePoint Central Administration Web Site**



| Description | Identifier | State | Host header value | IP address | Port |
|---|---|---|---|---|---|
| Default Web Site (Stopped) | 1 | Stopped | | * All Unassigned * | 80 |
| SharePoint - 80 | 1025788010 | Running | | * All Unassigned * | 80 |
| SharePoint Central Administra... | 1931835500 | Running | | * All Unassigned * | 40408 |

2. Copy the Vision Document Management .NET assembly to SharePoint site directory.
3. Copy Deltek.Vision.WSS30.Server.dll from <Vision Installation Directory>\Support\DM\30 to:

   c:\inetpub\wwwroot\bin (if WSS was installed to the default web site)

   *or to*

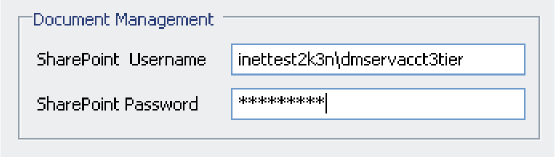
   c:\inetput\wwwroot\wss\Virtual Directories\<site>\bin

> By default, the <site> directory will reference the port chosen. In our example, the port is 80. If you extended WSS to the Default Web Site, the path will be c:\inetput\wwwroot\ bin.

## Configure Document Management Service Account in Weblink

You must configure the Document Management service account (username/password) on the System Settings tab of the Deltek Vision Weblink utility.  Follow the instructions below to configure this:

1. On the Vision Web server, launch Weblink from **Start » Programs » Deltek Vision**.
2. Enter the Weblink password when prompted.
3. Click the System Settings tab.
4. In the **Document Management** group box, enter your SharePoint username and password.  This account is your SharePoint Service account/Deltek Vision Application Pool Identity.



SharePoint Username: inettest2k3n\dmservacct3tier

SharePoint Password: **********

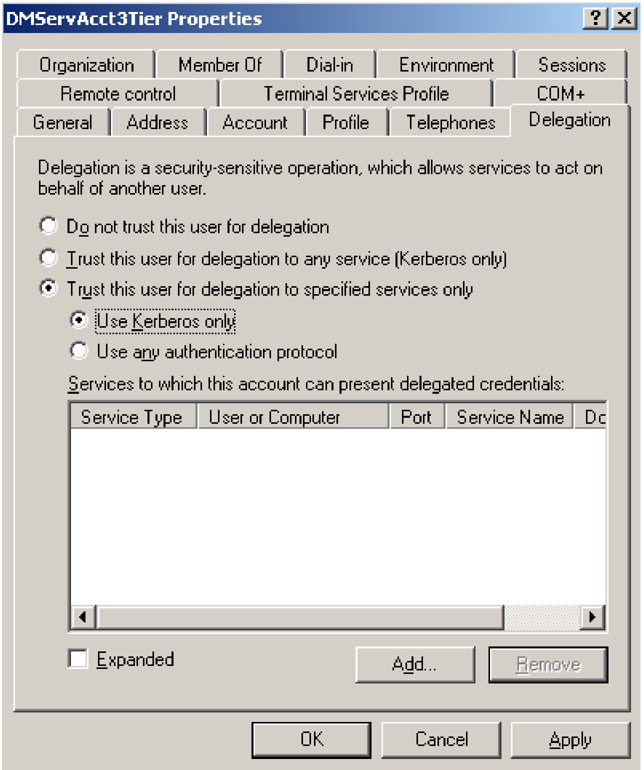
## Configure Constrained Delegation

Because your WSS server is on a separate physical server and because the Vision Web server needs to pass the domain credentials of your Vision Document Management users on to the WSS server, you must configure Constrained Delegation.

> This assumes a non-Internet deployment of Vision Document Management using Kerberos authentication. If you are deploying Vision Document Management so that it is accessible over the Internet, you need to skip ahead to “Configure Protocol Transition” on page 66.

**To configure Constrained Delegation, complete the following steps:**

1. Open the Active Directory Users and Computers MMC on a Domain Controller.
2. Locate the User account for the Vision Application Pool Identity (WSS Service account).
3. Right-click and select **Properties**.
4. On the Delegation tab, select the **Trust this user for delegation to specified services only** option.
5. Select the **Use Kerberos only** option.



DMServAcct3Tier Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

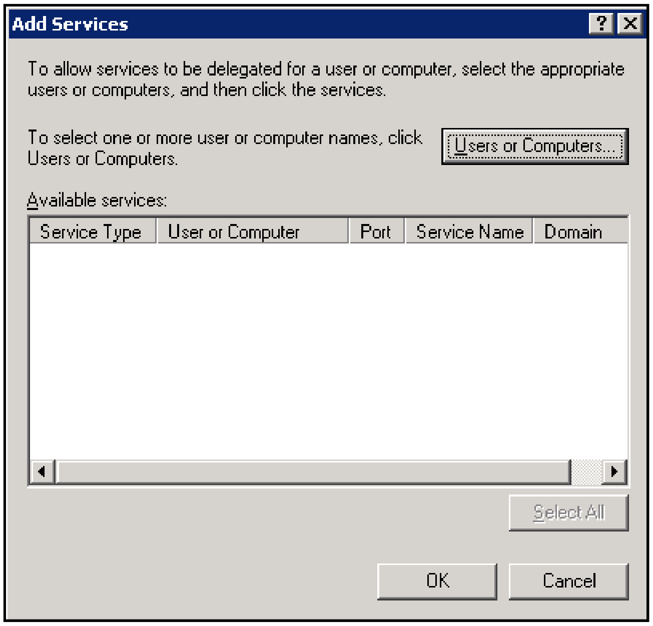
○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
  ● Use Kerberos only
  ○ Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|

□ Expanded

6. Click the **Add** button. The Add Services dialog box displays.

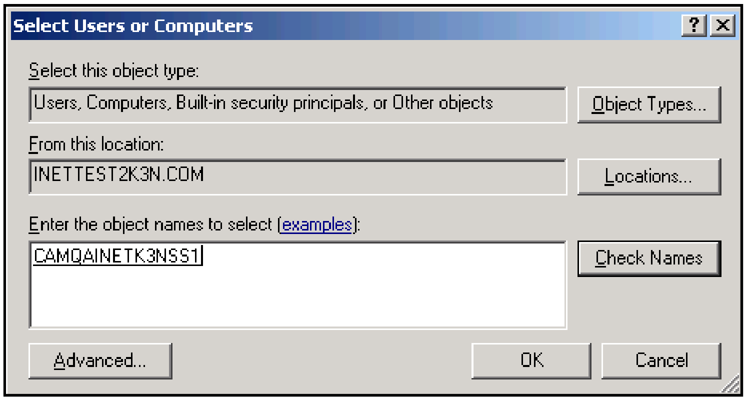


To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

7. Click **Users or Computers**. The Select Users or Computers dialog box displays.

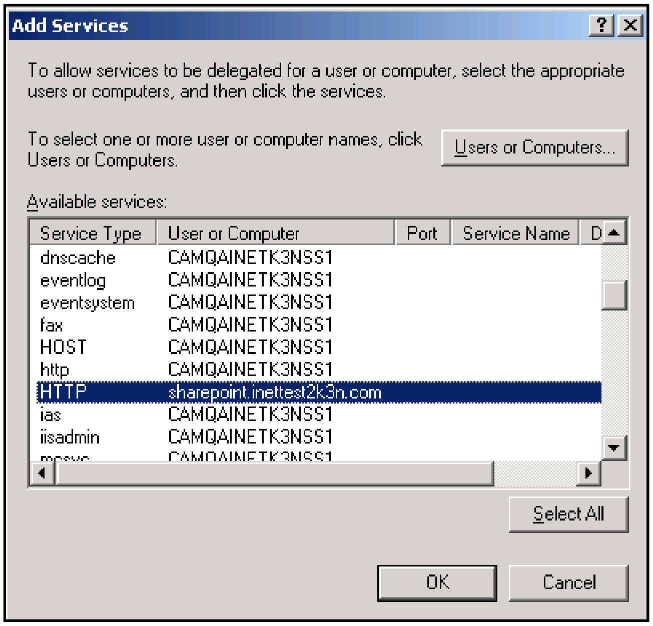


Select this object type:
Users, Computers, Built-in security principals, or Other objects

From this location:
INETTEST2K3N.COM

Enter the object names to select (examples):
CAMQAINETK3NSS1

8. Locate the http service, select it, and click **OK**.



Add Services

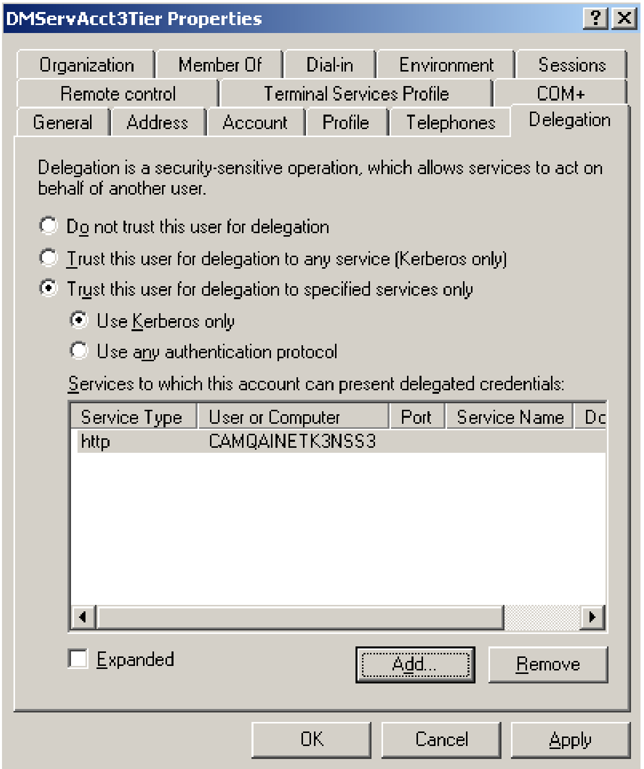
To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

| Service Type | User or Computer | Port | Service Name | D |
|---|---|---|---|---|
| dnscache | CAMQAINETK3NSS1 | | | |
| eventlog | CAMQAINETK3NSS1 | | | |
| eventsystem | CAMQAINETK3NSS1 | | | |
| fax | CAMQAINETK3NSS1 | | | |
| HOST | CAMQAINETK3NSS1 | | | |
| http | CAMQAINETK3NSS1 | | | |
| HTTP | sharepoint.inettest2k3n.com | | | |
| ias | CAMQAINETK3NSS1 | | | |
| iisadmin | CAMQAINETK3NSS1 | | | |
| [illegible] | CAMQAINETK3NSS1 | | | |

The Delegation tab should look like this:



DMServAcct3Tier Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|
| http | CAMQAINETK3NSS3 | | | |

□ Expanded

Because we are explicitly specifying the http service and not all services on the SharePoint server, this is known as Constrained Delegation.

There are two http service types listed. These service types are known as Service Principal Names (SPNs). The SPN referencing CAMQAINETK3NSS1.inettest2k3n.com was created automatically when the server was added to the domain and the http service (IIS) was installed. The second SPN referencing sharepoint.inettest2k3n.com is a new SPN that was created using the setspn utility that allows us to register the custom FQDN of the server, which provides more meaning than the actual machine name.

## Configure Protocol Transition

If Vision Document Management functionality is required over the Internet and you will be using a custom DNS/FQDN for the SharePoint URL (as in our example, vision1.inettest2k3n.com), then you need to configure a form of delegation referred to as Protocol Transition. If Document Management functionality is not required, you can skip this step.

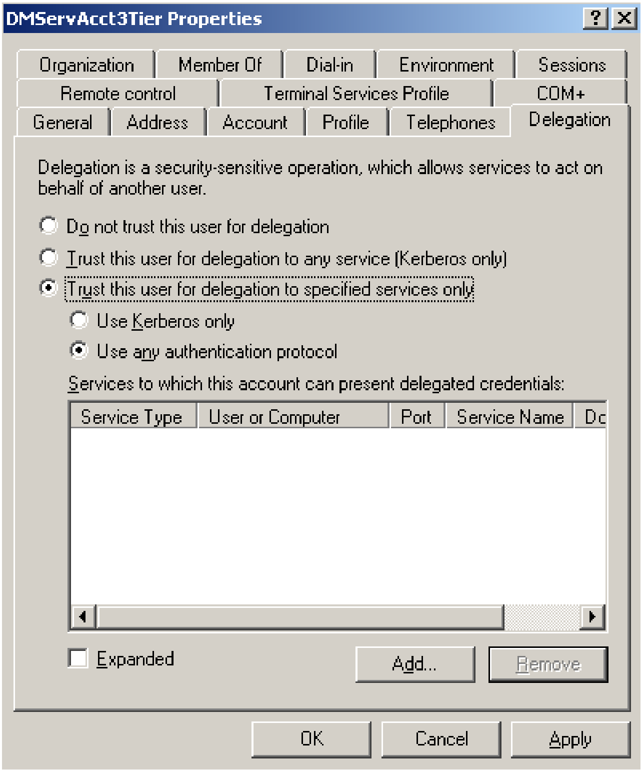
The Kerberos authentication protocol must be used to authenticate from the Vision Web server to the SharePoint server. However, if Vision is deployed in an Internet scenario and there are users outside of the firewall who need to access Document Management features, Kerberos authentication cannot be used to authenticate the client to the Web server. This is because the client needs to have the ability to negotiate a Kerberos ticket with the Key Distribution Center (KDC), which is a service running on a Domain Controller. This requires port 88 to be opened inbound on the firewall to the Domain Controller, which is not an advisable configuration.

To get around this, you must be running a Native Windows Server 2003 functional domain.

Protocol Transition is configured by selecting the **Use any authentication protocol** option instead of the **Use Kerberos only** option, which is used to configure Constrained Delegation. This allows the client to authenticate to the Vision Web server using NTLM instead of Kerberos, and that authentication is then “transitioned” over to Kerberos for Delegation to the SharePoint server.

**To configure Protocol Transition, complete the following steps:**

1. Open the Active Directory Users and Computers MMC on a Domain Controller.
2. Locate the User account for the Vision Application Pool Identity (WSS Service account), which is most likely under the Computers Organizational Unit (OU).
3. Right-click and select **Properties**.
4. On the Delegation tab, select the **Trust this user for delegation to specified services only** option.
5. Select the **Use any authentication protocol** option.



DMServAcct3Tier Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

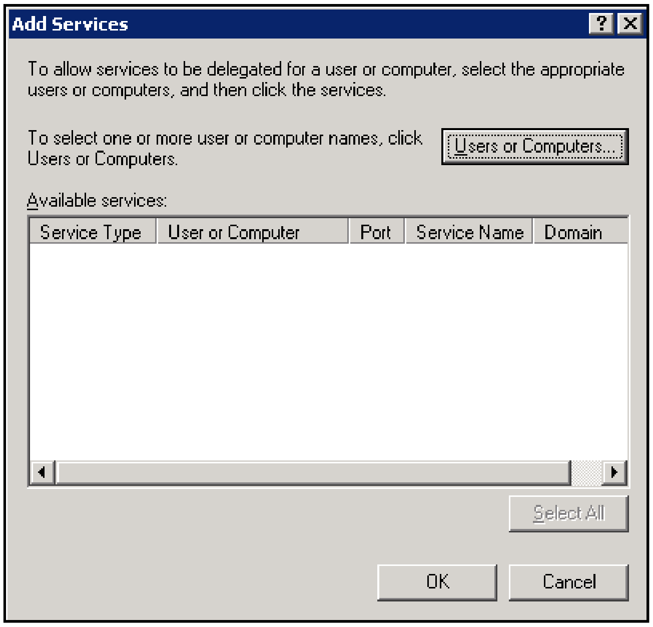
● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|

□ Expanded

6. Click the **Add** button. The Add Services dialog box displays.



Add Services

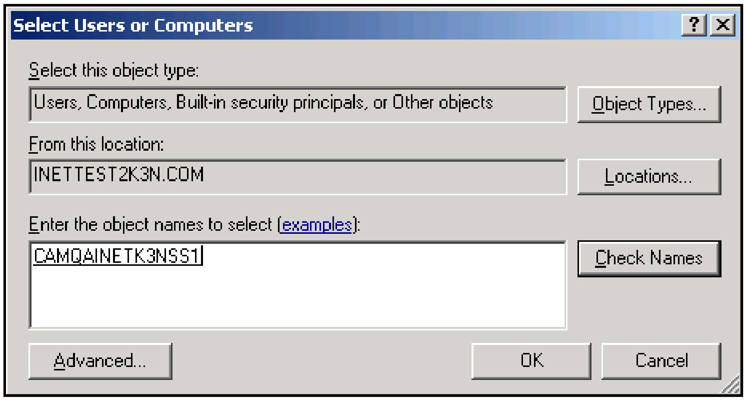
To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

| Service Type | User or Computer | Port | Service Name | Domain |
|---|---|---|---|---|

7. Click **Users or Computers**, search for the SharePoint server, and click **OK**.

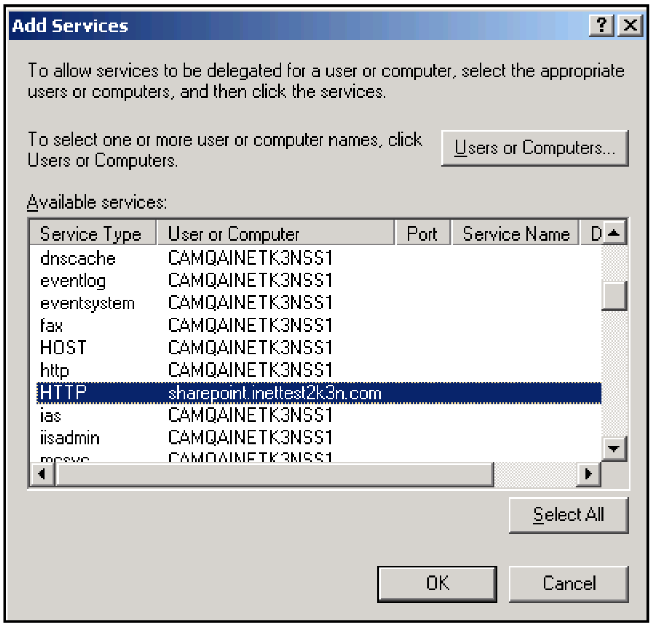

Select Users or Computers

Select this object type: Users, Computers, Built-in security principals, or Other objects

From this location: INETTEST2K3N.COM

Enter the object names to select (examples): CAMQAINETK3NSS1

8. Locate the http service for the SPN (FQDN) you created earlier (in our example, **sharepoint.inettest2k3n.com**), select it, and click **OK**.


Add Services

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

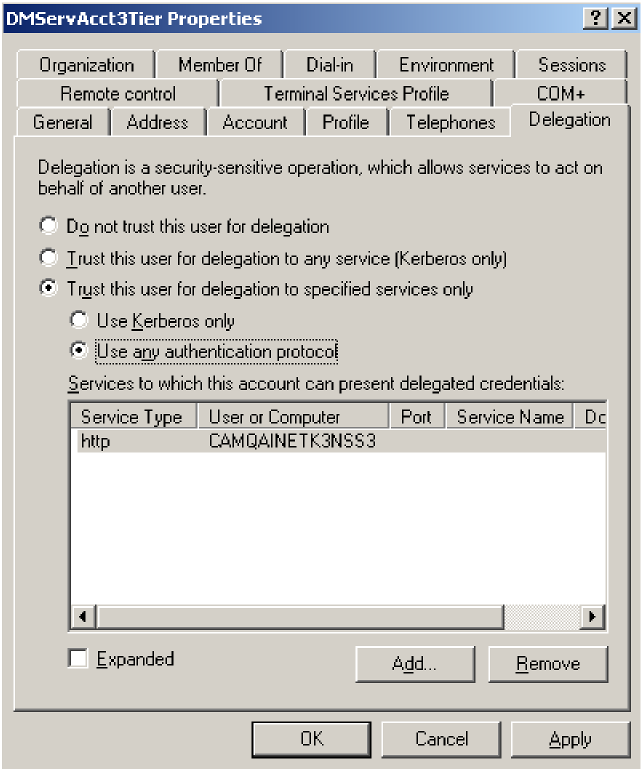
| Service Type | User or Computer | Port | Service Name | D |
|---|---|---|---|---|
| dnscache | CAMQAINETK3NSS1 | | | |
| eventlog | CAMQAINETK3NSS1 | | | |
| eventsystem | CAMQAINETK3NSS1 | | | |
| fax | CAMQAINETK3NSS1 | | | |
| HOST | CAMQAINETK3NSS1 | | | |
| http | CAMQAINETK3NSS1 | | | |
| HTTP | sharepoint.inettest2k3n.com | | | |
| ias | CAMQAINETK3NSS1 | | | |
| iisadmin | CAMQAINETK3NSS1 | | | |
| mcsvc | CAMQAINETK3NSS1 | | | |

This illustration shows two http service types. Unless you have registered a custom FQDN using the setspn utility, only the server name displays. These service types are known as Service Principal Names (SPNs).

The SPN referencing **CAMQAINETK3NSS1.inettest2k3n.com** was created automatically when the server was added to the domain and the http service (IIS) was installed.

The second SPN referencing **sharepoint.inettest2k3n.com** is a new SPN that was created using the setspn utility that allows us to register the custom FQDN of the server, which provides more meaning than the actual machine name.

The Delegation tab should look like this:



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

- ○ Use Kerberos only
- ● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|
| http | CAMQAINETK3NSS3 | | | |

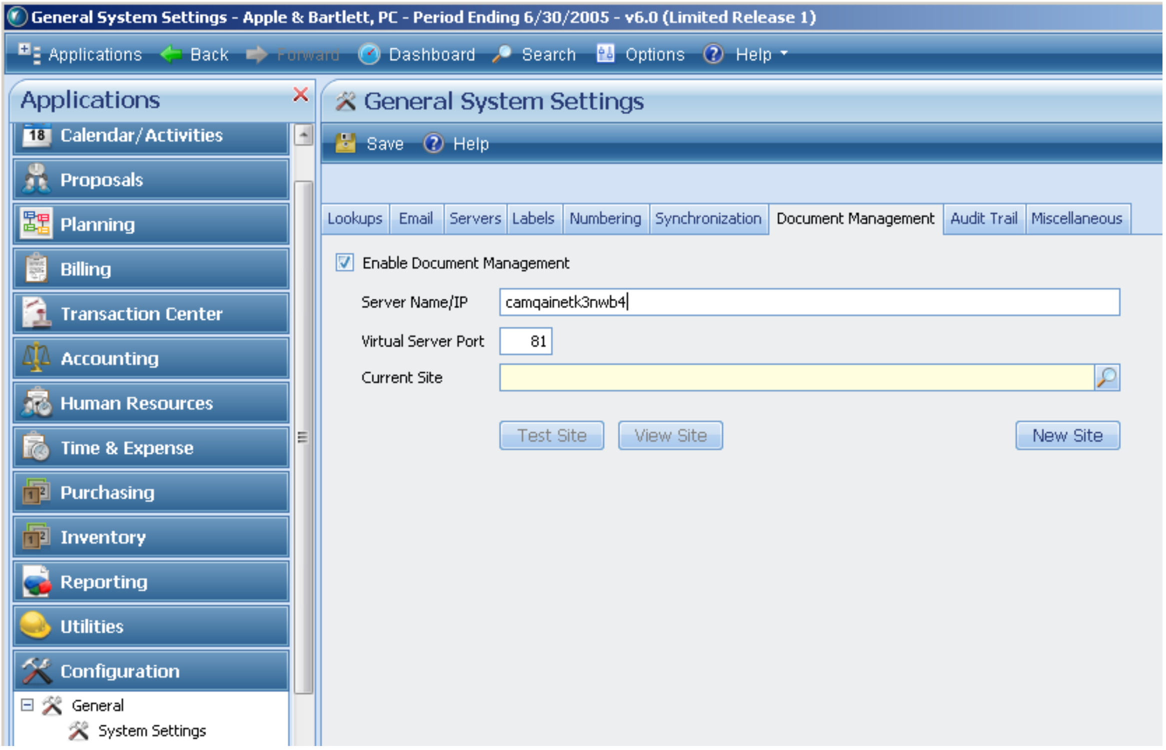
□ Expanded

Because you explicitly specified the http service and not all services on the SharePoint server and because you selected the **Use any authentication protocol** option and not Kerberos, this is known as Protocol Transition.

## Configure Vision Document Management

**To configure Vision Document Management, complete the following steps:**

1. Log in to Vision using an account that has access to the Configuration menus.
2. Click **Configuration » General » System Settings** and select the Document Management tab.



☑ Enable Document Management

Server Name/IP: camqainetk3nwb4

Virtual Server Port: 81

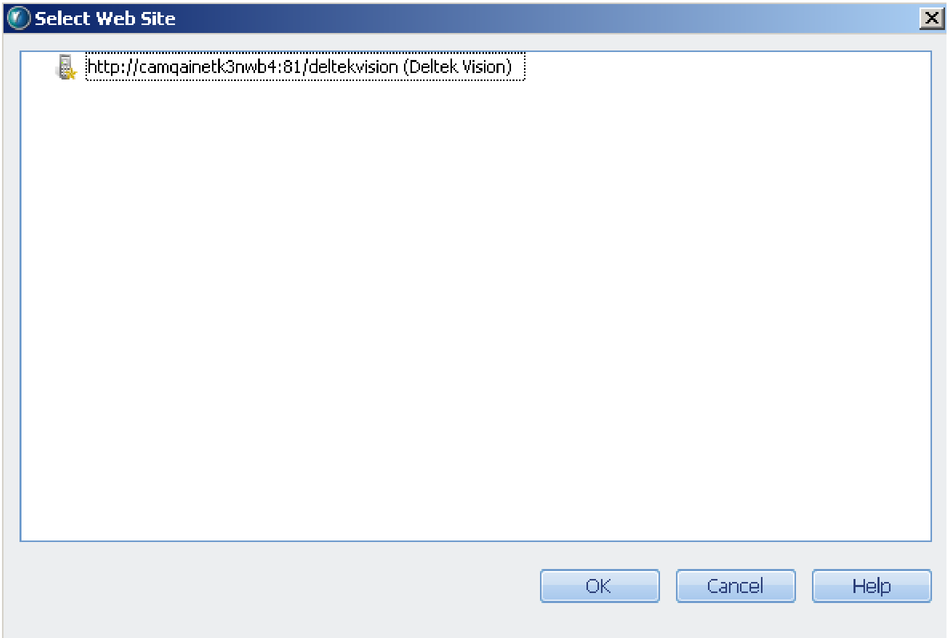
Current Site:

3. Select the **Enable Document Management** check box.

4. Enter the name of the server hosting Document Management. This can be the NetBIOS name, server name FQDN, or custom DNS/FQDN. Enter this value without the protocol prefix (for example, remove the http://). In the illustration above, the value is **camqainetk3nwb4**.

5. Enter the **Virtual Server Port**. In the illustration above, the port is 81.

6. Click the Lookup icon to select the current site.



http://camqainetk3nwb4:81/deltekvision (Deltek Vision)

7. The Select Web Site dialog box displays the available sites. Select a site, and click **OK**.
8. Save your changes.

# Multi-Tier—New Installation of Document Management 6.1 with MOSS 2007

The following instructions assume that Vision and MOSS 2007 exist on separate servers as Vision and MOSS 2007 are not supported on the same physical server. They also assume you are deploying to Windows Server 2003/IIS 6.0. If you will be deploying to Windows Server 2008/IIS 7.0, refer to Appendix B for detailed configuration information

## Prerequisites

- Install and configure MOSS 2007.
- Install/upgrade to Vision 6.1.
- Change the Application Pool Identity for the DeltekVisionAppPool to be a domain account. (The Vision 6.1 installation sets this to be the local DeltekVision account.) This account will also be the SharePoint (WSS) Service account. Add this user to the local Administrators group on the Vision server (and WSS server if running on a separate server).

## Configure Vision Application Pool Identity to Be a Domain Account

You must change the Vision Application Pool Identity to be a domain account. (The default is for Vision to use a Local Administrator Account. The DeltekVision user is created during the Vision installation.) The reason for this change is that the local accounts are unable to read the SPN configured in Active Directory.

**To change the Vision Application Pool Identity, complete the following steps:**

1. Create a domain user account. No domain Admin rights are needed for this account.
2. Log on to the domain on the Vision Web/application server using an Administrator account.
3. Click **Start » All Programs » Administrative Tools » Internet Information Services**.
4. Expand **Application Pools**.
5. Right-click **DeltekVisionAppPool** and select **Properties** on the shortcut menu.
6. Click the Identity tab and change the account from DeltekVision to your domain\user account created in step 1. Make sure this account is a member of the Local Administrators and IIS_WPG local groups.

## Configure SPN for Vision Application Pool Identity

As mentioned earlier in this document, it is necessary to create a Service Principal Name (SPN) for the domain user running the DeltekVisionAppPool.

**To add the Application Pool Identity as a Service Principal Name, complete the following steps:**

1. Enter the following commands on the domain server where setspn is installed:

   **setspn –A http/<Vision Web/App Server name> <domain app pool identity>**

   For example: setspn –A http/camqainetk3nwb5 inettest2k3n\dmservacct3tier
2. Repeat for the FQDN of the server.

Refer to the following related Microsoft Knowledge Base article:

http://support.microsoft.com/?id=871179

If your Vision Web server is accessed by a DNS / FQDN (Fully Qualified Domain Name) that *does not match* the name of the server (for example, if your Vision Web server is named Server01 and its DNS name is Server01.Company.com, but you have added a custom DNS value Vision.Company.com), you must also add an SPN for this custom DNS name.

## Install and Configure Vision 6.1 Document Management and the MOSS 2007 Site Collection

When you install Vision 6.1 Document Management on your MOSS 2007 server, only the necessary components are installed.  Post-installation configuration is necessary. The steps to configure MOSS 2007 are outlined below.

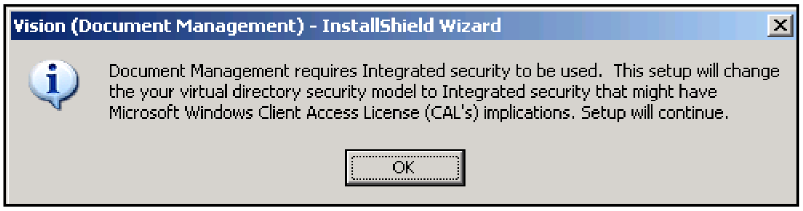
The Document Management installation performs the following:

- Installs Web Service Extensions (WSE) 2.0 Sp3.
- Changes the IIS metabase NTAuthenticationProviders element to be Negotiate,NTLM.
- Copies Document Management files to SharePoint ISAPI folder (c:\program files\common files\microsoft shared\web service extensions\12\isapi).
- Copies Document Management files to the Vision Support folder (\program files\deltek\vision\support\DM\30).
- Modifies the SharePoint Web.config file in the ISAPI directory to work with Vision Document Management.
- Installs Deltek.Vision.WSS30.Server.dll into the Global Assembly Cache (GAC).

### Install Vision 6.1 Document Management on the Vision Web Server

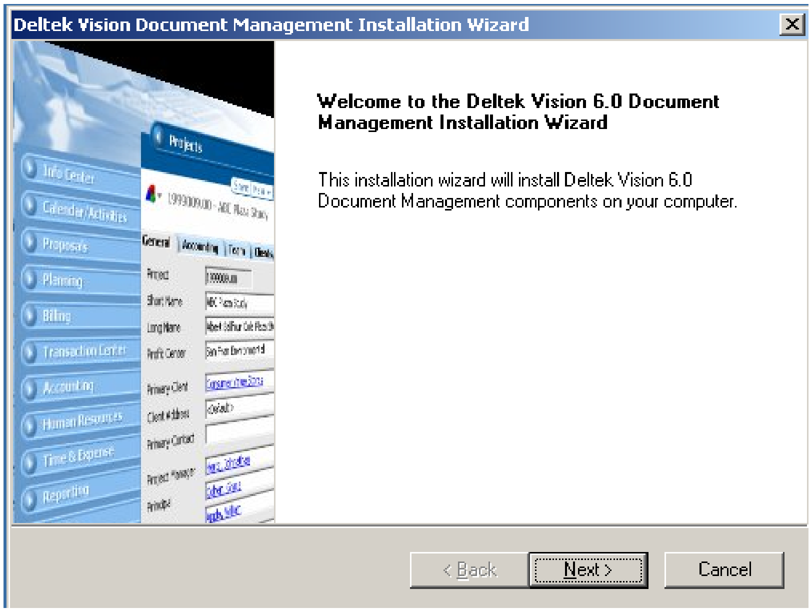
**To install Vision 6.1 Document Management on the Vision Web server, complete the following steps:**

1. Run the setup on your Vision Web server. The following dialog box then indicates the IIS licensing requirements for the use of Windows Integrated Authentication (required to use Vision Document Management):


Vision (Document Management) - InstallShield Wizard

Document Management requires Integrated security to be used.  This setup will change the your virtual directory security model to Integrated security that might have Microsoft Windows Client Access License (CAL's) implications. Setup will continue.

2. Click **OK**. The Welcome page displays.

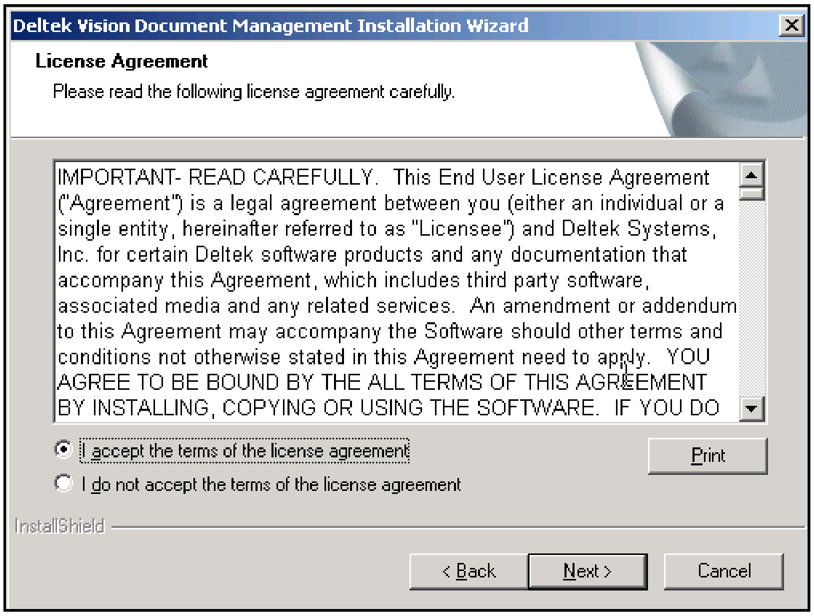


Deltek Vision Document Management Installation Wizard

**Welcome to the Deltek Vision 6.0 Document Management Installation Wizard**

This installation wizard will install Deltek Vision 6.0 Document Management components on your computer.

3. Click **Next**. The License Agreement page displays.



Deltek Vision Document Management Installation Wizard

**License Agreement**

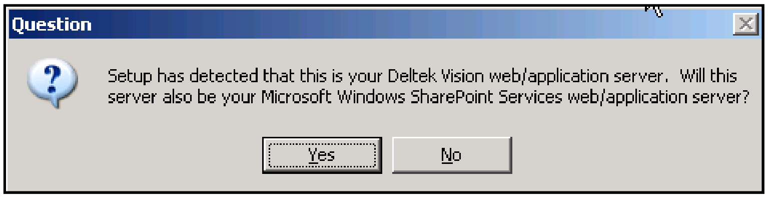
Please read the following license agreement carefully.

IMPORTANT- READ CAREFULLY. This End User License Agreement ("Agreement") is a legal agreement between you (either an individual or a single entity, hereinafter referred to as "Licensee") and Deltek Systems, Inc. for certain Deltek software products and any documentation that accompany this Agreement, which includes third party software, associated media and any related services. An amendment or addendum to this Agreement may accompany the Software should other terms and conditions not otherwise stated in this Agreement need to apply. YOU AGREE TO BE BOUND BY THE ALL TERMS OF THIS AGREEMENT BY INSTALLING, COPYING OR USING THE SOFTWARE. IF YOU DO

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

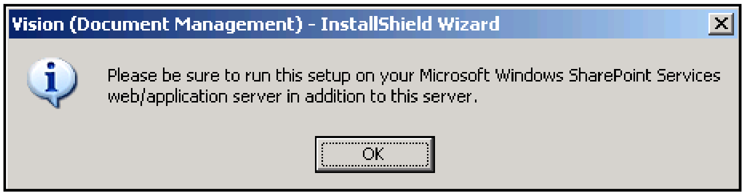
4. Click **I accept the terms of the license agreement** and click **Next**. The following dialog box displays.



Question

Setup has detected that this is your Deltek Vision web/application server. Will this server also be your Microsoft Windows SharePoint Services web/application server?

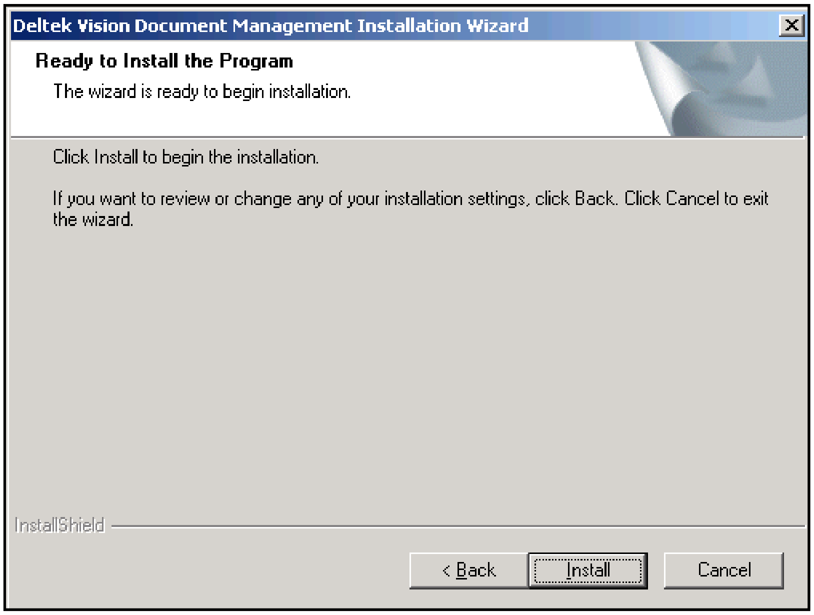
5. Click **No** because this is a multi-tier installation of Vision Document Management and your Vision Web server will not host WSS 3.0. The following dialog box displays to remind you to run the setup on the WSS server.



Vision (Document Management) - InstallShield Wizard

Please be sure to run this setup on your Microsoft Windows SharePoint Services web/application server in addition to this server.

6. Click **OK** to display the Ready to Install the Program page.



Deltek Vision Document Management Installation Wizard

**Ready to Install the Program**

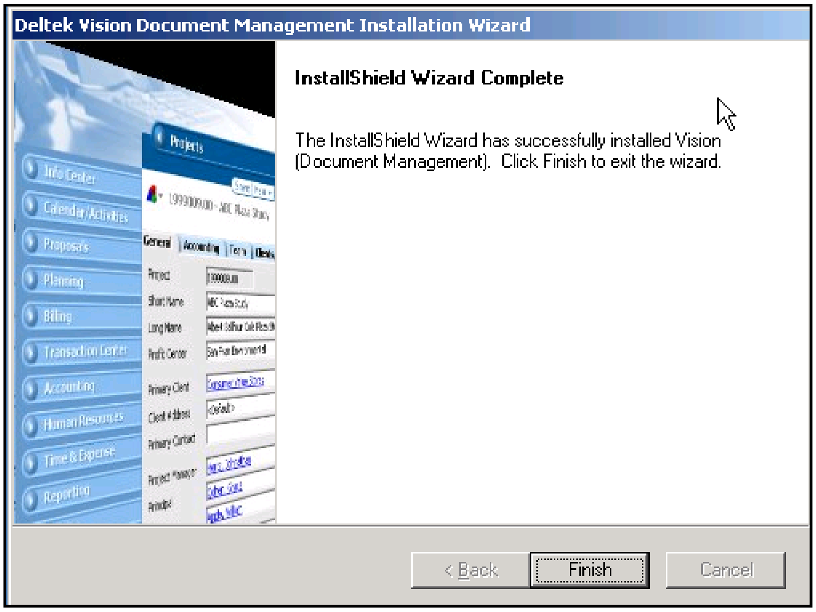
The wizard is ready to begin installation.

Click Install to begin the installation.

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

7. Click **Install** to start the installation.

8. Click **Finish** when the installation is completed.



Deltek Vision Document Management Installation Wizard

**InstallShield Wizard Complete**

The InstallShield Wizard has successfully installed Vision (Document Management). Click Finish to exit the wizard.

# Install Vision Document Management on the MOSS 2007 Server

**To install Vision Documentation Management on the MOSS 2007 server, complete the following steps:**

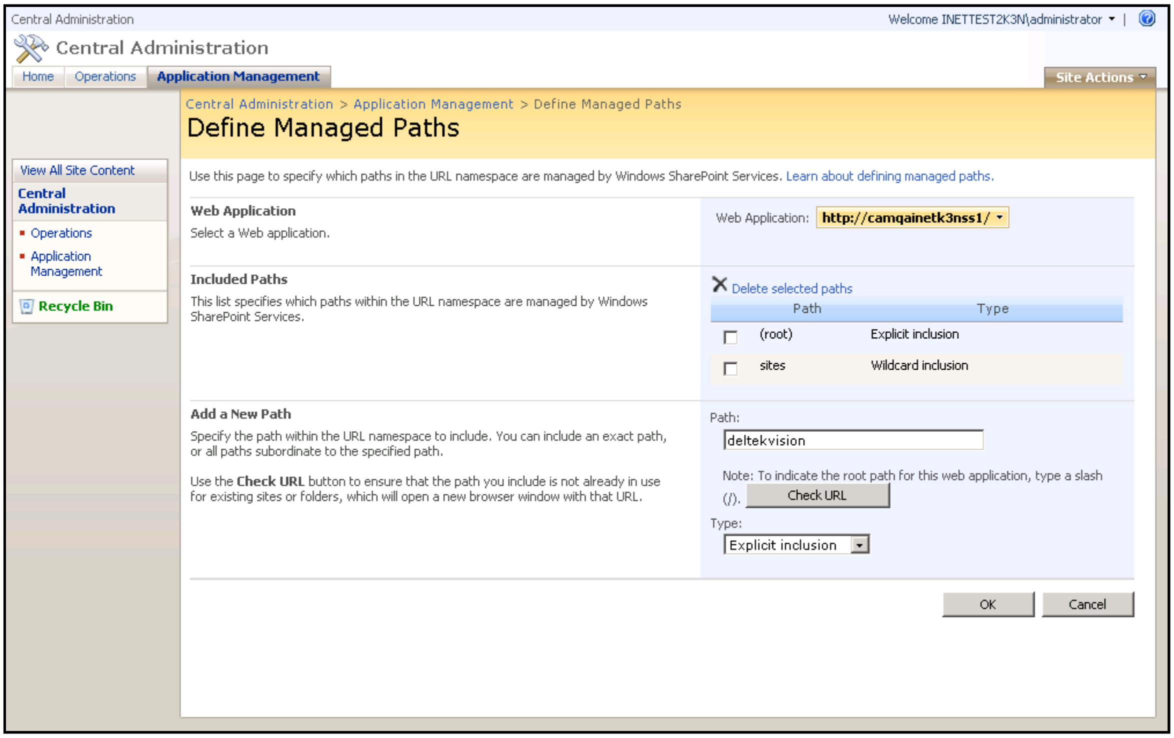
1. Download DeltekVision61DM.exe and run the setup on your MOSS 2007 server. The Welcome page displays.
2. Click **Next**. The License Agreement page displays.
3. Accept the license agreement and click **Next**. The Ready to Install page displays.
4. Click **Install** to start the installation.
5. Click **Finish** when the installation is completed.

# Use SharePoint Central Administration to Complete the SharePoint Configuration

Complete the SharePoint configuration using SharePoint Central Administration. This section assumes that MOSS 2007 has already been installed and configured.

**To complete the SharePoint configuration, complete the following steps:**

1. In SharePoint Central Administration, click **Application Management** and select the **Define Managed Paths** option. This will create a specific URL for your Vision Document Management site collection (for example, http://MOSSServer/DeltekVision).



Define Managed Paths

Use this page to specify which paths in the URL namespace are managed by Windows SharePoint Services. Learn about defining managed paths.

**Web Application**
Select a Web application.

Web Application: **http://camqainetk3nss1/**

**Included Paths**
This list specifies which paths within the URL namespace are managed by Windows SharePoint Services.

| | Path | Type |
|---|---|---|
| □ | (root) | Explicit inclusion |
| □ | sites | Wildcard inclusion |

**Add a New Path**
Specify the path within the URL namespace to include. You can include an exact path, or all paths subordinate to the specified path.

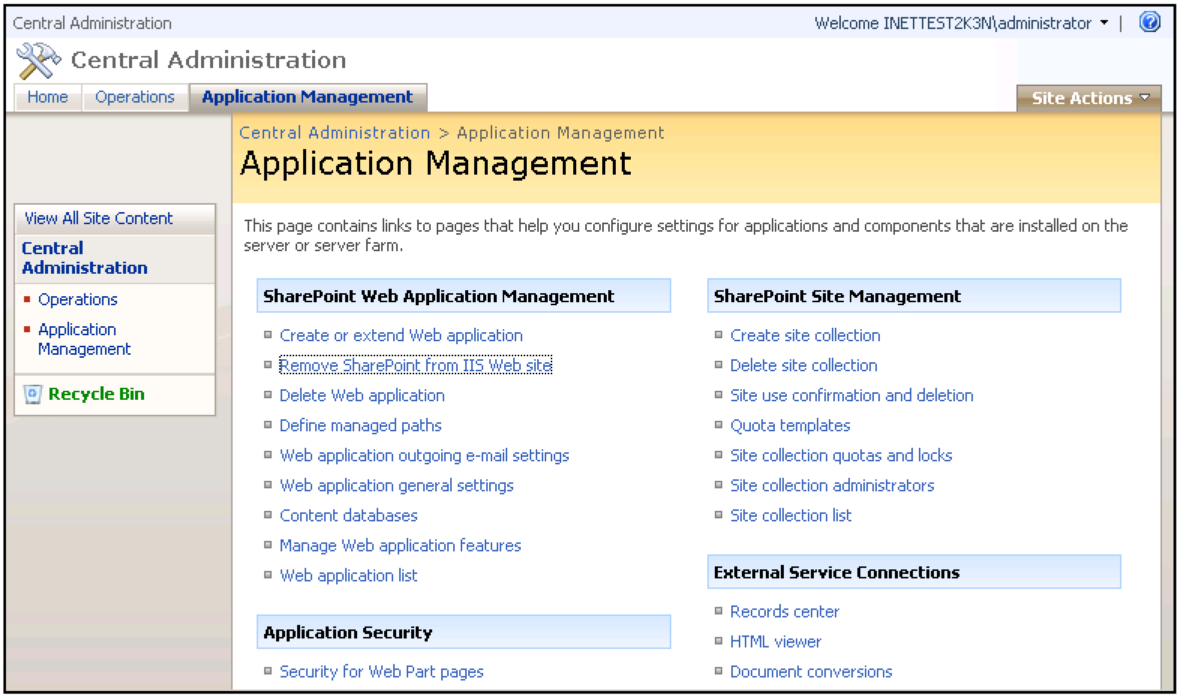
Use the **Check URL** button to ensure that the path you include is not already in use for existing sites or folders, which will open a new browser window with that URL.

Path: deltekvision

Note: To indicate the root path for this web application, type a slash (/).

Type: Explicit inclusion

2. Enter **DeltekVision** in **Path** and select **Explicit inclusion** from the **Type** drop-down list.
3. Click **OK**.
4. Click **Application Management** and select the **Create site collection** option under **SharePoint Site Management**.



Central Administration | Welcome INETTEST2K3N\administrator ▾ |

Central Administration

Home | Operations | Application Management | Site Actions ▾

Central Administration > Application Management

Application Management

View All Site Content

Central Administration

- Operations
- Application Management

Recycle Bin

This page contains links to pages that help you configure settings for applications and components that are installed on the server or server farm.

**SharePoint Web Application Management**

- Create or extend Web application
- Remove SharePoint from IIS Web site
- Delete Web application
- Define managed paths
- Web application outgoing e-mail settings
- Web application general settings
- Content databases
- Manage Web application features
- Web application list

**Application Security**

- Security for Web Part pages

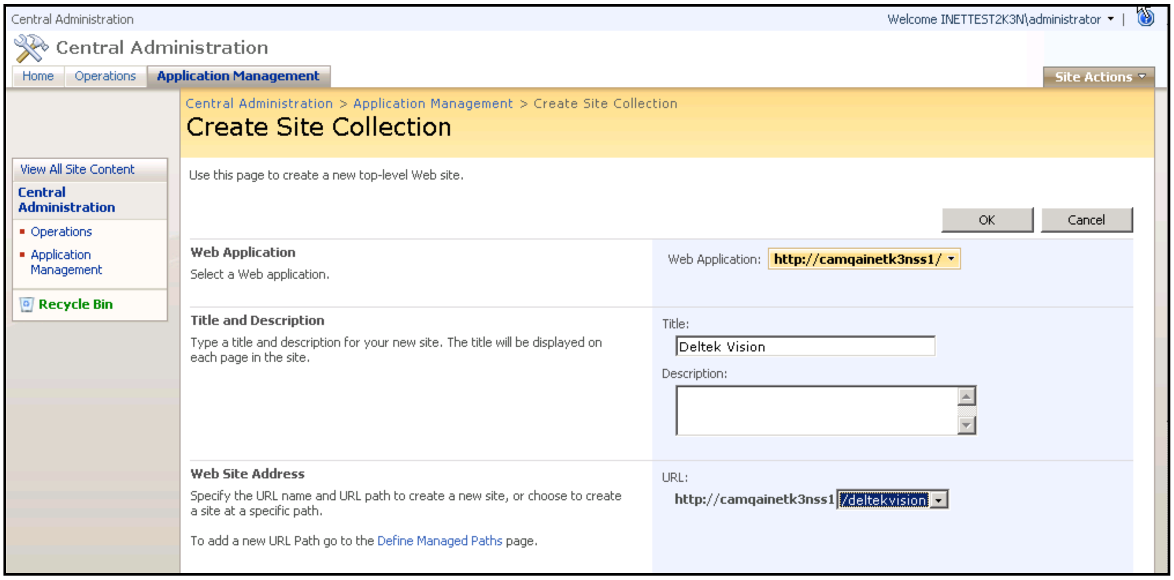
**SharePoint Site Management**

- Create site collection
- Delete site collection
- Site use confirmation and deletion
- Quota templates
- Site collection quotas and locks
- Site collection administrators
- Site collection list

**External Service Connections**

- Records center
- HTML viewer
- Document conversions

The Create Site Collection page displays.



Central Administration | Welcome INETTEST2K3N\administrator ▾ |

Central Administration

Home | Operations | Application Management | Site Actions ▾

Central Administration > Application Management > Create Site Collection

Create Site Collection

View All Site Content

Central Administration

- Operations
- Application Management

Recycle Bin

Use this page to create a new top-level Web site.

OK | Cancel

**Web Application**

Select a Web application.

Web Application: http://camqainetk3nss1/ ▾

**Title and Description**

Type a title and description for your new site. The title will be displayed on each page in the site.

Title: Deltek Vision

Description:

**Web Site Address**

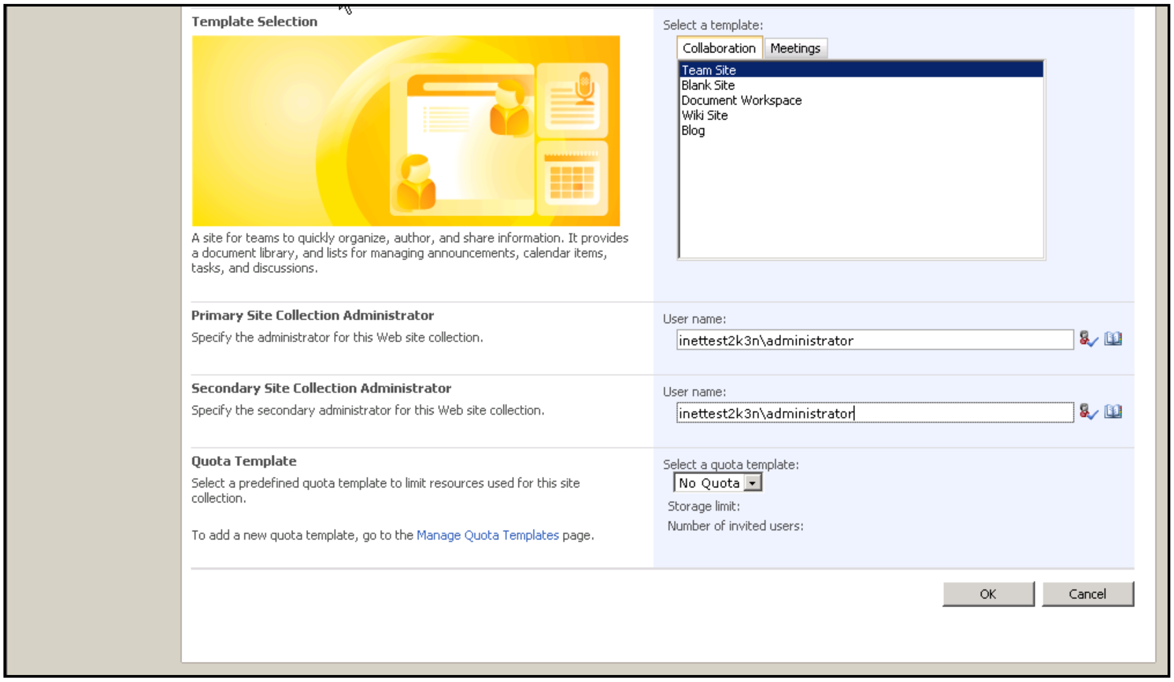
Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.

To add a new URL Path go to the Define Managed Paths page.

URL: http://camqainetk3nss1 /deltekvision ▾

5. Enter **Deltek Vision** in **Title** and enter a description, if appropriate.

6. From the **URL** drop-down list, select **/deltekvision**. This will be the top level root for Vision Document Management.



Template Selection

A site for teams to quickly organize, author, and share information. It provides a document library, and lists for managing announcements, calendar items, tasks, and discussions.

Select a template:

Primary Site Collection Administrator

Specify the administrator for this Web site collection.

User name: inettest2k3n\administrator

Secondary Site Collection Administrator

Specify the secondary administrator for this Web site collection.

User name: inettest2k3n\administrator

Quota Template

Select a predefined quota template to limit resources used for this site collection.

To add a new quota template, go to the Manage Quota Templates page.

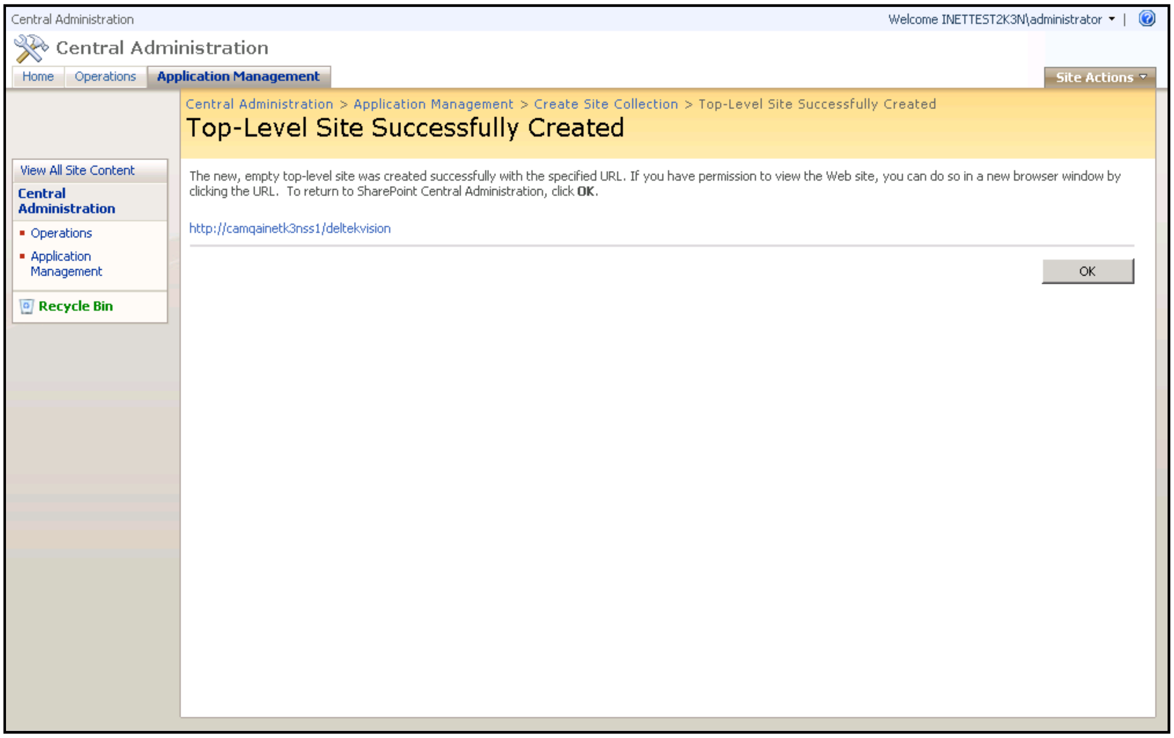
Select a quota template: No Quota

Storage limit:

Number of invited users:

7. Under **Select a template**, accept the default of **Team Site** for the template to be used and enter a username in each of the **User name** fields for the primary and secondary site collection administrators.

8. Select **No Quota** in **Select a quota template** and click **OK**. The Top-Level Site Successfully Created page displays.



Central Administration > Application Management > Create Site Collection > Top-Level Site Successfully Created

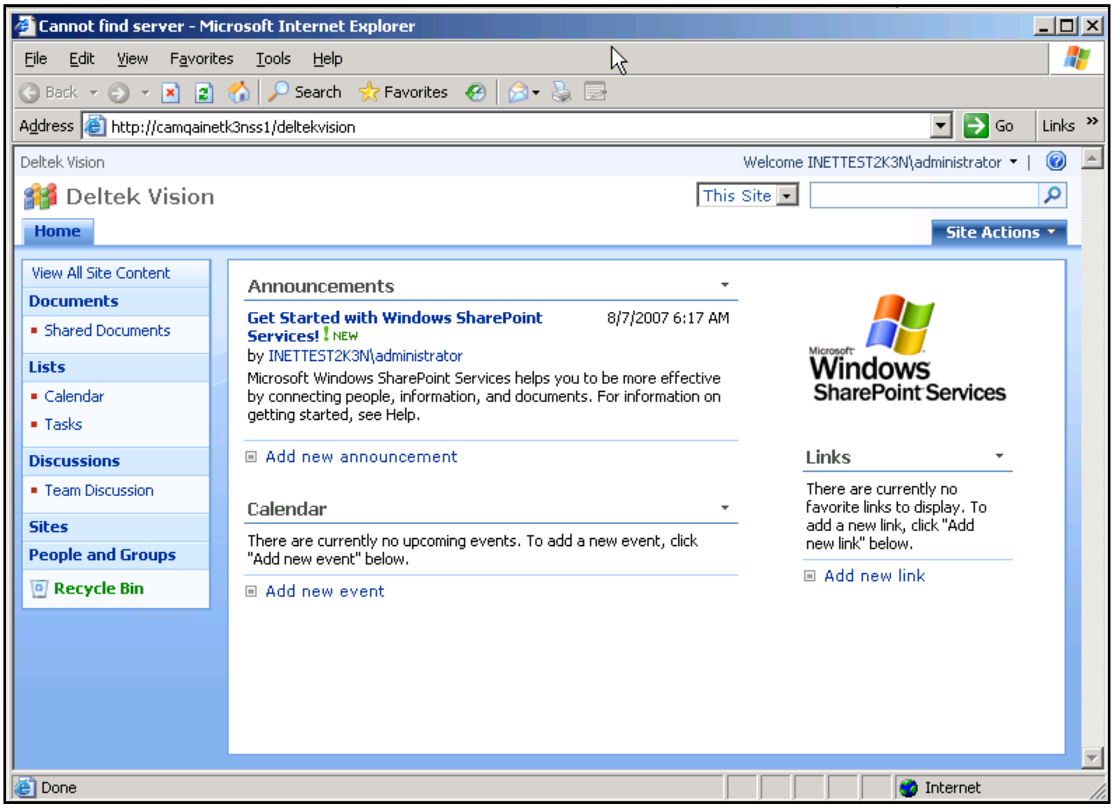
Top-Level Site Successfully Created

The new, empty top-level site was created successfully with the specified URL. If you have permission to view the Web site, you can do so in a new browser window by clicking the URL. To return to SharePoint Central Administration, click **OK**.

http://camqainetk3nss1/deltekvision

9. Click **Start** » **Run**, enter **iisreset /noforce,** and click **Enter**.

10. Click the link for the top level site (in our example it is http://camqainetk3nss1/deltekvision) to display the site.



Get Started with Windows SharePoint Services! NEW 8/7/2007 6:17 AM
by INETTEST2K3N\administrator
Microsoft Windows SharePoint Services helps you to be more effective by connecting people, information, and documents. For information on getting started, see Help.

There are currently no upcoming events. To add a new event, click "Add new event" below.

There are currently no favorite links to display. To add a new link, click "Add new link" below.

11. The SharePoint configuration is complete. Close SharePoint Central Administration.

## Configure SharePoint for a Fully Qualified Domain Name (FQDN) URL (Optional)

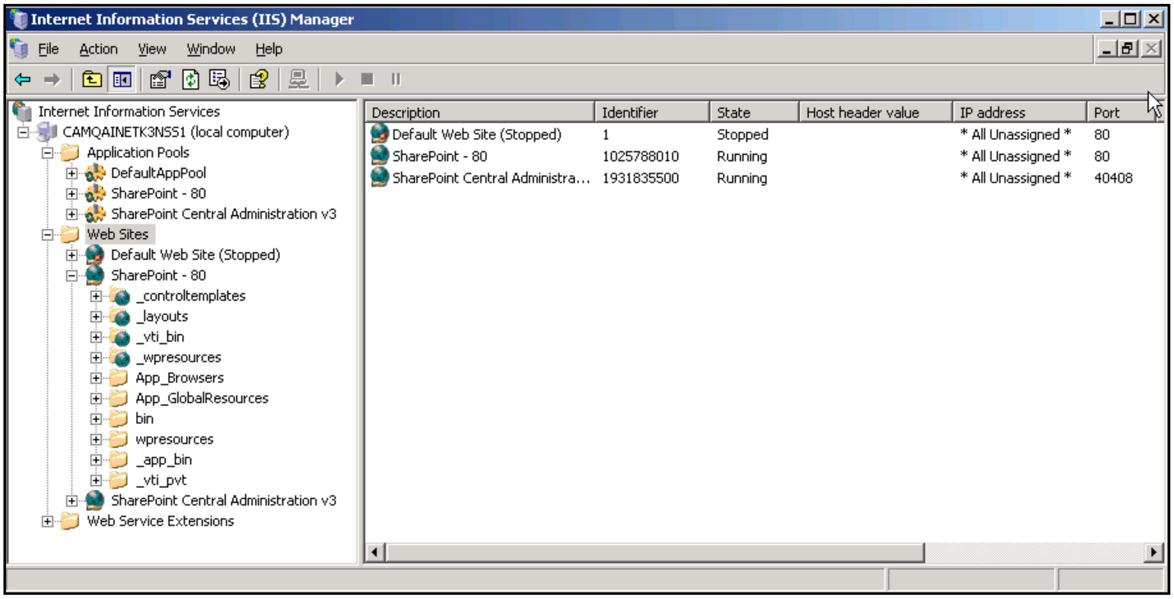
If you will be configuring your SharePoint server to use a custom DNS record for the URL you must create an additional SPN and also to create Alternate Access Mappings in SharePoint.

See "Appendix C: SPN Configuration When Using Custom DNS Records" on page 99 for more information.

## Verify IIS Configuration and Configure Deltek Vision Document Management .NET Assembly

**To verify IIS configuration, complete the following steps:**

1. Use the directions that follow to open Internet Information Services to view these Web sites:
   - **Default Web Site** — Stopped.
   - **SharePoint – 80** — This is your MOSS 2007 Web site.
   - **SharePoint Central Administration Web Site**



| Description | Identifier | State | Host header value | IP address | Port |
|---|---|---|---|---|---|
| Default Web Site (Stopped) | 1 | Stopped | | * All Unassigned * | 80 |
| SharePoint - 80 | 1025788010 | Running | | * All Unassigned * | 80 |
| SharePoint Central Administra... | 1931835500 | Running | | * All Unassigned * | 40408 |

2. Copy Vision Document Management .NET assembly to the SharePoint site directory.
3. Copy Deltek.Vision.WSS30.Server.dll from <Vision Installation Directory>\Support\DM\30 to:

   c:\inetpub\wwwroot\bin (if WSS was installed to the default web site)

   *or to*

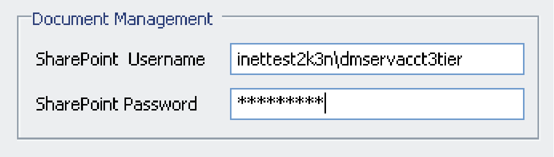
   c:\inetput\wwwroot\wss\Virtual Directories\<site>\bin

> By default, the <site> directory will reference the port chosen. In our example, the port is 80. If you extended WSS to the Default Web Site, the path will be c:\inetput\wwwroot\ bin.

## Configure Document Management Service Account in Weblink

You must configure the Document Management service account (username/password) on the System Settings tab of the Deltek Vision Weblink utility. Follow the instructions below to configure this:

1. On the Vision Web server, launch Weblink from **Start » Programs » Deltek Vision**.
2. Enter the Weblink password when prompted.
3. Click the System Settings tab.
4. In the **Document Management** group box, enter your SharePoint username and password. This account is your SharePoint Service account/Deltek Vision Application Pool Identity.



Document Management

SharePoint Username: inettest2k3n\dmservacct3tier

SharePoint Password: **********

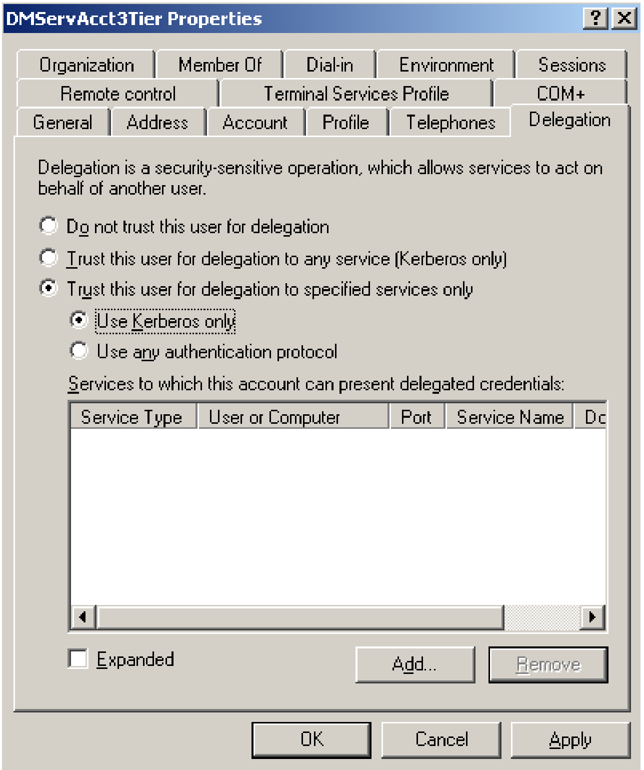
## Configure Constrained Delegation

Because your WSS server is on a separate physical server and because the Vision Web server needs to pass the domain credentials of your Vision Document Management users on to the WSS server, you must configure Constrained Delegation.

> This assumes a non-Internet deployment of Vision Document Management using Kerberos authentication. If you are deploying Vision Document Management so that it is accessible over the Internet, you need to skip ahead to “Configure Protocol Transition” on page 84.

**To configure Constrained Delegation, complete the following steps:**

1. Open the Active Directory Users and Computers MMC on a Domain Controller.
2. Locate the User account for the Vision Application Pool Identity (MOSS Service account), which is most likely under the Computers Organizational Unit (OU).
3. Right-click and select **Properties**.
4. On the Delegation tab, select the **Trust this user for delegation to specified services only** option.
5. Select the **Use Kerberos only** option.



DMServAcct3Tier Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

● Use Kerberos only

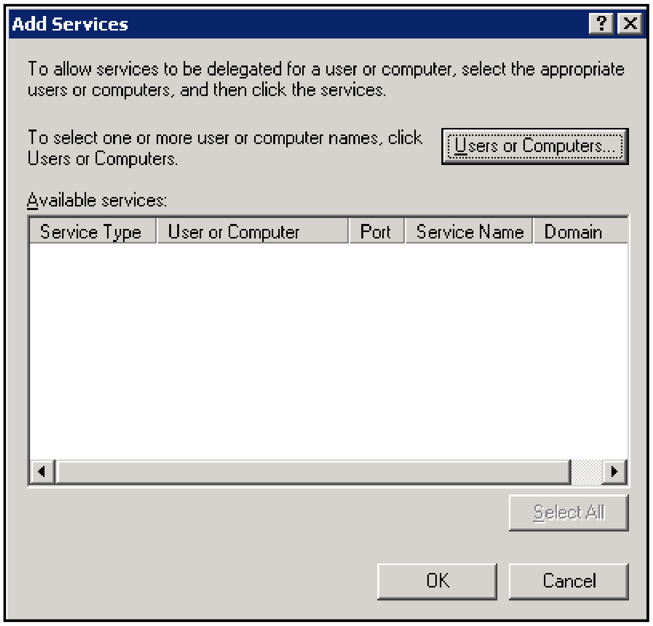
○ Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|

□ Expanded

6. Click the **Add** button. The Add Services dialog box displays.



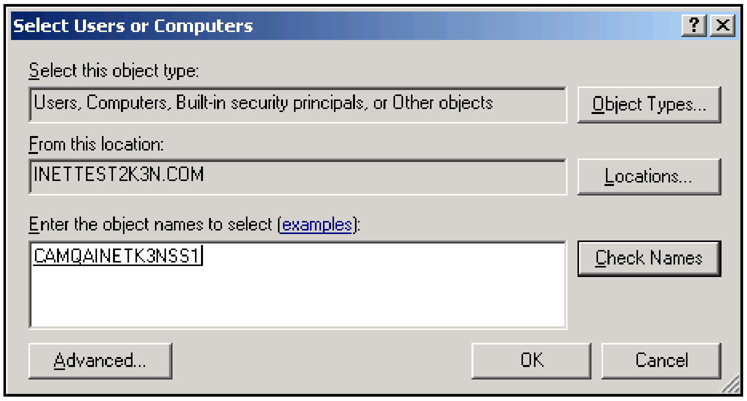
Add Services

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

7. Click **Users or Computers**. The Select Users or Computers dialog box displays.



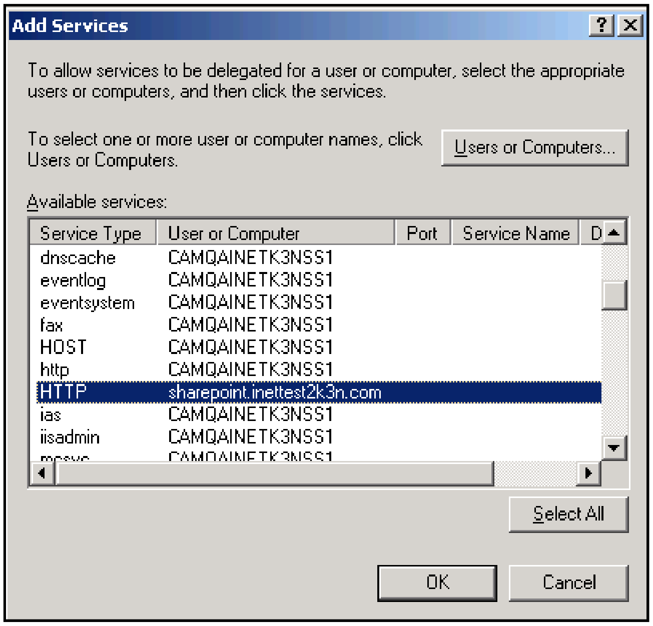
Select Users or Computers

Select this object type:
Users, Computers, Built-in security principals, or Other objects

From this location:
INETTEST2K3N.COM

Enter the object names to select (examples):
CAMQAINETK3NSS1

8. Locate the http service, select it, and click **OK**.



**Add Services**

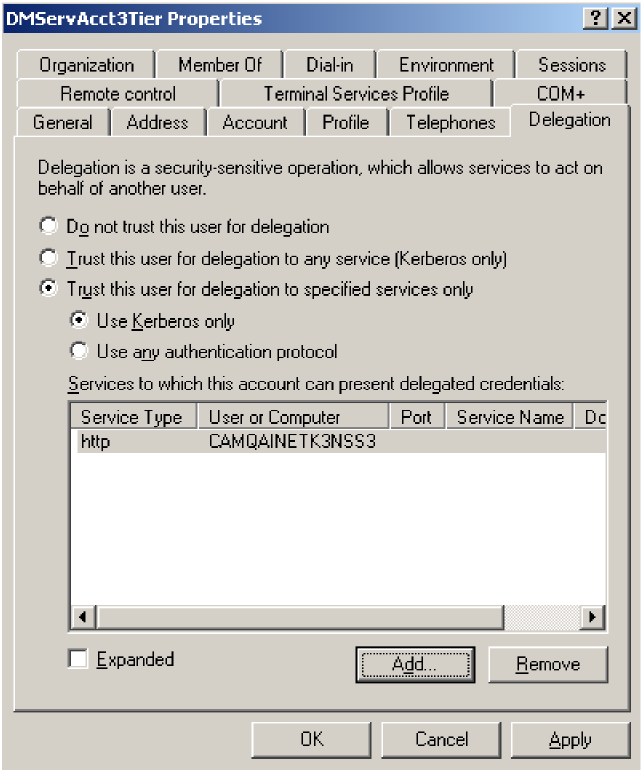
To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

| Service Type | User or Computer | Port | Service Name | D |
|---|---|---|---|---|
| dnscache | CAMQAINETK3NSS1 | | | |
| eventlog | CAMQAINETK3NSS1 | | | |
| eventsystem | CAMQAINETK3NSS1 | | | |
| fax | CAMQAINETK3NSS1 | | | |
| HOST | CAMQAINETK3NSS1 | | | |
| http | CAMQAINETK3NSS1 | | | |
| HTTP | sharepoint.inettest2k3n.com | | | |
| ias | CAMQAINETK3NSS1 | | | |
| iisadmin | CAMQAINETK3NSS1 | | | |

9. The Delegation tab should look like this:



**DMServAcct3Tier Properties**

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|
| http | CAMQAINETK3NSS3 | | | |

□ Expanded

Because we are explicitly specifying the http service and not all services on the SharePoint server, this is known as Constrained Delegation.

There are two http service types listed. These service types are known as Service Principal Names (SPNs). The SPN referencing CAMQAINETK3NSS1.inettest2k3n.com was created automatically when the server was added to the domain and the http service (IIS) was installed. The second SPN referencing sharepoint.inettest2k3n.com is a new SPN that was created using the setspn utility that allows us to register the custom FQDN of the server, which provides more meaning than the actual machine name.

## Configure Protocol Transition

If Vision Document Management functionality is required over the Internet and you will be using a custom DNS/FQDN for the SharePoint URL (as in our example, vision1.inettest2k3n.com), then you need to configure a form of delegation referred to as Protocol Transition. If Document Management functionality is not required, you can skip this step.

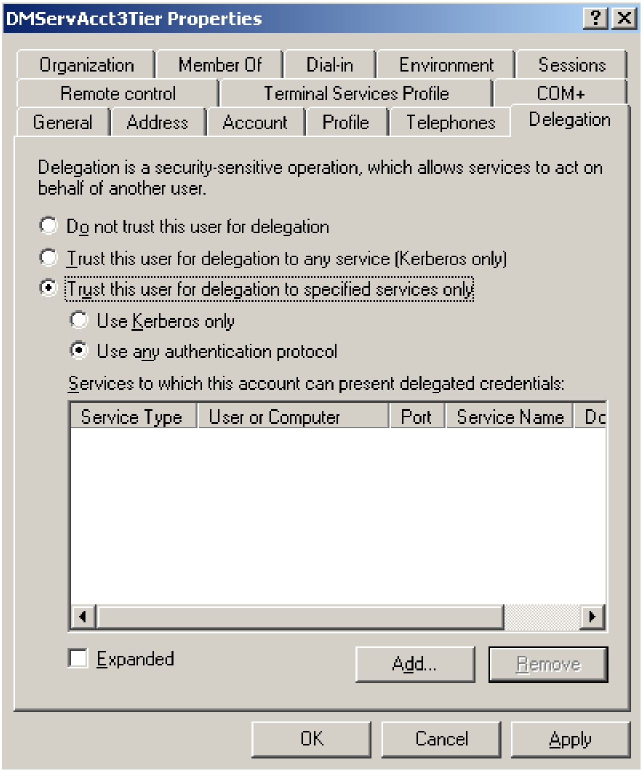
The Kerberos authentication protocol must be used to authenticate from the Vision Web server to the SharePoint server. However, if Vision is deployed in an Internet scenario and there are users outside of the firewall who need to access Document Management features, Kerberos authentication cannot be used to authenticate the client to the Web server. This is because the client needs to have the ability to negotiate a Kerberos ticket with the Key Distribution Center (KDC), which is a service running on a Domain Controller. This requires port 88 to be opened inbound on the firewall to the Domain Controller, which is not an advisable configuration.

To get around this, you must be running a Native Windows Server 2003 functional domain.

Protocol Transition is configured by selecting the **Use any authentication protoco**l option instead of the **Use Kerberos only** option, which is used to configure Constrained Delegation. This allows the client to authenticate to the Vision Web server using NTLM instead of Kerberos, and that authentication is then “transitioned” over to Kerberos for Delegation to the SharePoint server.

**To configure Protocol Transition, complete the following steps:**

1. Open the Active Directory Users and Computers MMC on a Domain Controller.
2. Locate the User account for the Vision Application Pool Identity (MOSS Service account), which is most likely under the Computers Organizational Unit (OU).
3. Right-click and select **Properties**.
4. On the Delegation tab, select the **Trust this user for Delegation to specified services only** option.
5. Select the **Use any authentication protocol** option.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

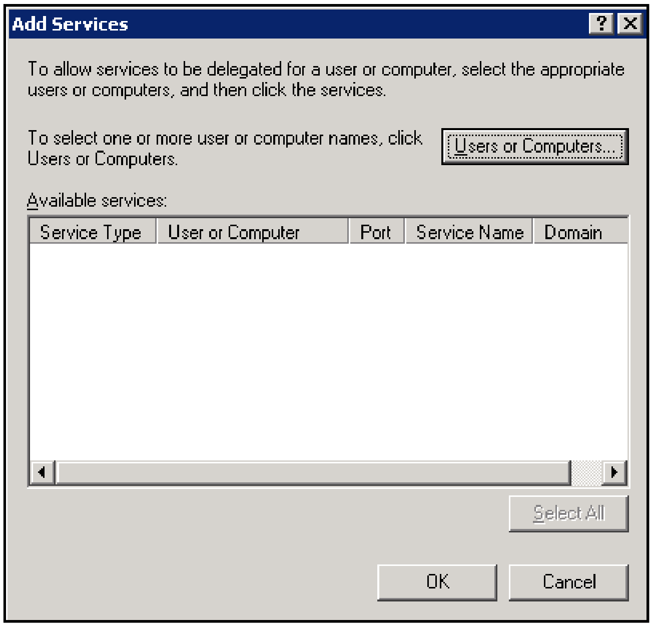
● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Dc |
|---|---|---|---|---|

☐ Expanded

6. Click the **Add** button. The Add Services dialog box displays.



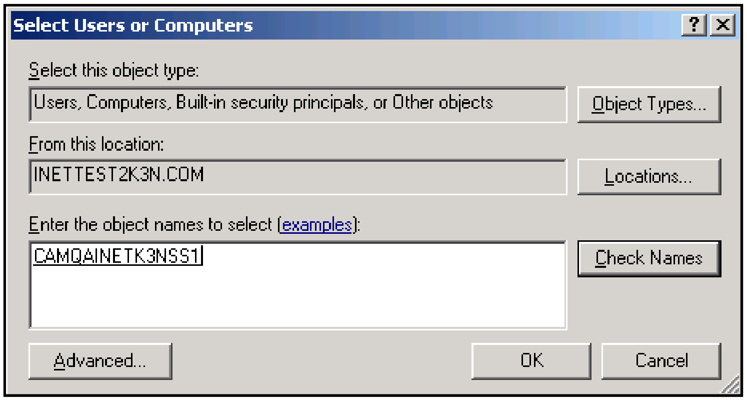
To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

| Service Type | User or Computer | Port | Service Name | Domain |
|---|---|---|---|---|

7. Click **Users or Computers**, search for the SharePoint server, and click **OK**.

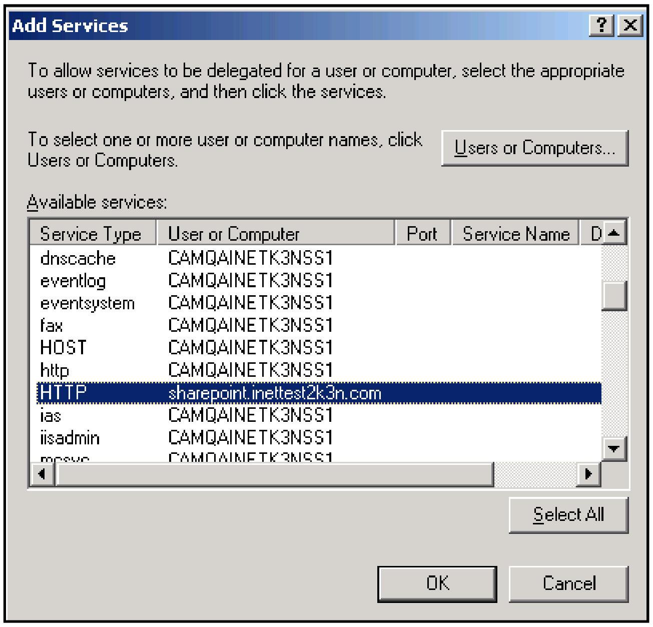


Select this object type:
Users, Computers, Built-in security principals, or Other objects

From this location:
INETTEST2K3N.COM

Enter the object names to select (examples):
CAMQAINETK3NSS1

8. Locate the http service for the SPN (FQDN) you created earlier (in our example, **sharepoint.inettest2k3n.com**) select it, and click **OK**.



To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

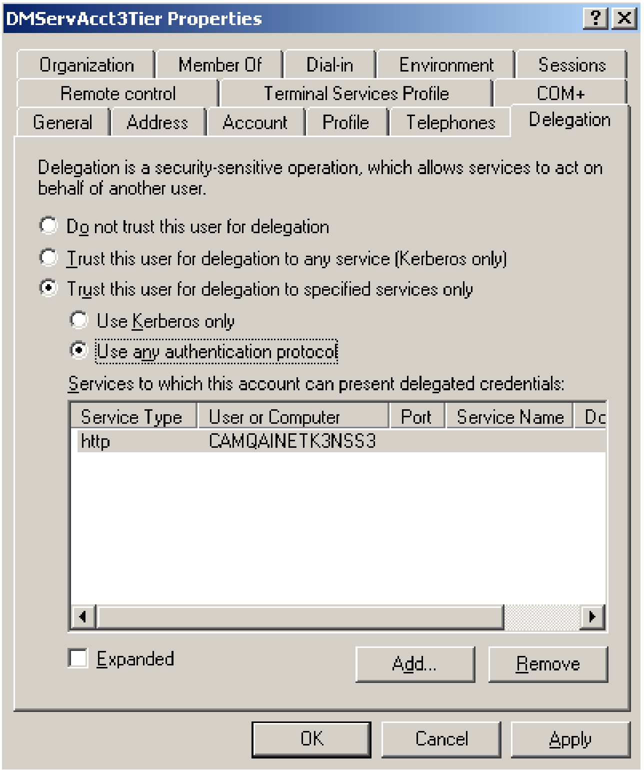
| Service Type | User or Computer | Port | Service Name | D |
|---|---|---|---|---|
| dnscache | CAMQAINETK3NSS1 | | | |
| eventlog | CAMQAINETK3NSS1 | | | |
| eventsystem | CAMQAINETK3NSS1 | | | |
| fax | CAMQAINETK3NSS1 | | | |
| HOST | CAMQAINETK3NSS1 | | | |
| http | CAMQAINETK3NSS1 | | | |
| HTTP | sharepoint.inettest2k3n.com | | | |
| ias | CAMQAINETK3NSS1 | | | |
| iisadmin | CAMQAINETK3NSS1 | | | |

This illustration shows two http service types. Unless you have registered a custom FQDN using the setspn utility, only the server name displays. These service types are known as Service Principal Names (SPNs).

The SPN referencing **CAMQAINETK3NSS1.inettest2k3n.com** was created automatically when the server was added to the domain and the http service (IIS) was installed.

The second SPN referencing **sharepoint.inettest2k3n.com** is a new SPN that was created using the setspn utility that allows us to register the custom FQDN of the server, which provides more meaning than the actual machine name.

The Delegation tab should look like this:



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

- ○ Use Kerberos only
- ● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service Name | Do |
|---|---|---|---|---|
| http | CAMQAINETK3NSS3 | | | |

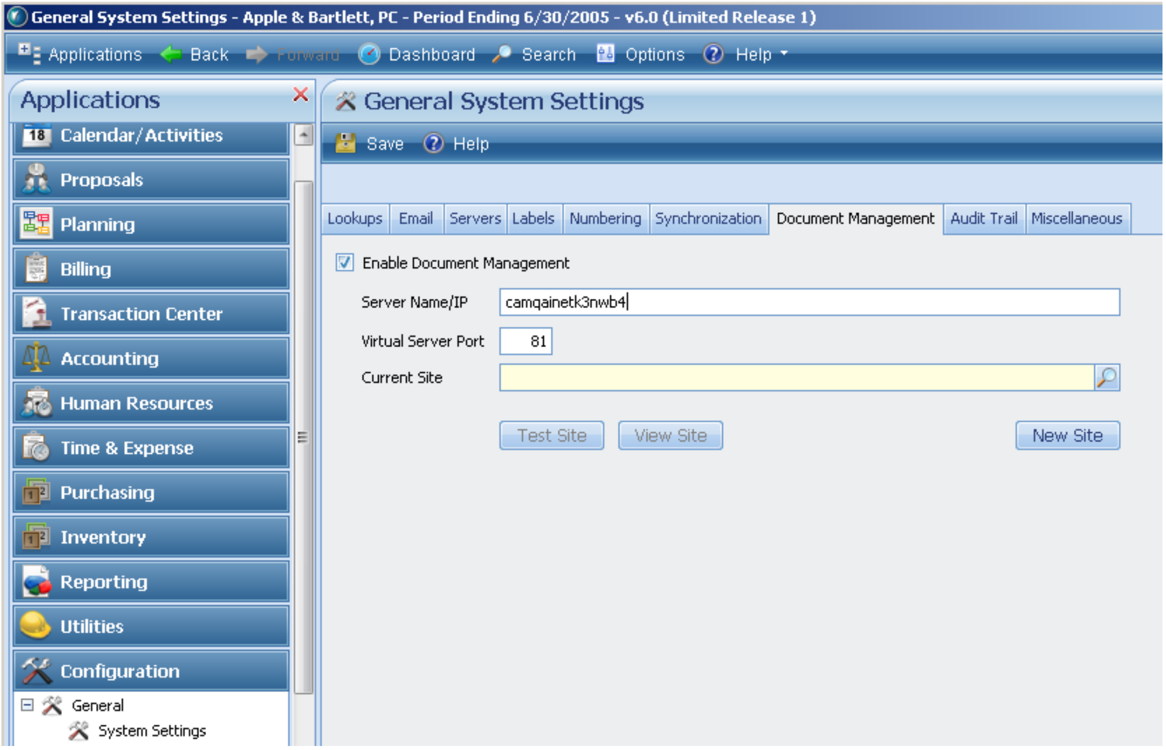
□ Expanded

Because we are explicitly specifying the http service and not all services on the SharePoint server and because we are using the **Use any authentication protocol** option and not Kerberos, this is known as Protocol Transition.

## Configure Vision Document Management

**To configure Vision Document Management, complete the following steps:**

1. Log in to Vision using an account that has access to the Configuration menus.
2. Click **Configuration » General » System Settings** and select the Document Management tab.



General System Settings - Apple & Bartlett, PC - Period Ending 6/30/2005 - v6.0 (Limited Release 1)

☑ Enable Document Management

Server Name/IP: camqainetk3nwb4

Virtual Server Port: 81

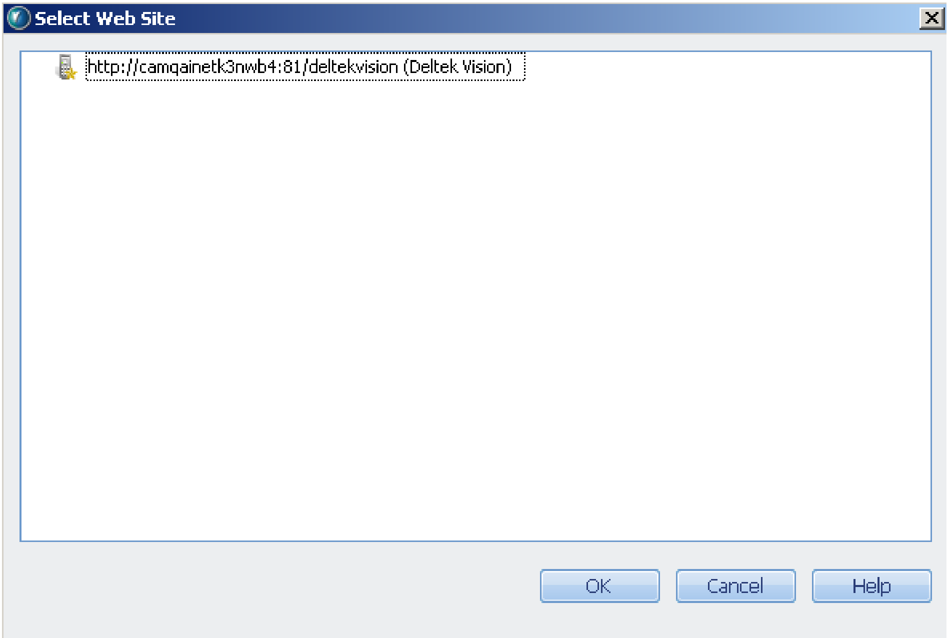
Current Site:

3. Select the **Enable Document Management** option.

4. Enter the name of the server hosting document management. This can be the NetBIOS name, server name FQDN, or custom DNS/FQDN. Enter this value without the protocol prefix (for example, remove the http://). In the illustration above, the value is **camqainetk3nwb4**.

5. Enter the **Virtual Server Port**. In our example the port is 81.

6. Click the Lookup icon to select the current site.



Select Web Site

http://camqainetk3nwb4:81/deltekvision (Deltek Vision)

7. The Select Web Site dialog box displays the available sites. Select a site, and click **OK**.
8. Save your changes.

# Appendix A: Active Directory Domain Functional Level

## Directory Functional Levels

There are three possible active directory functional levels:

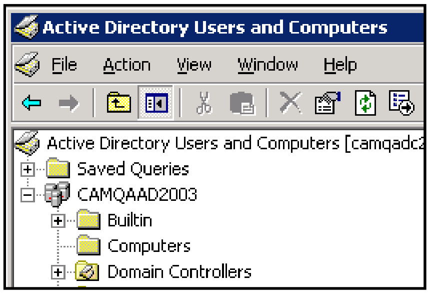
- **Windows 2000 Native** — All domain controllers are Windows 2000
- **Windows 2000 Mixed** — Server 2003 domain with support for Windows 2000 domain controllers
- **Windows Server 2003** — "Native" where all domain controllers are Server 2003

However, only one of these is supported for Vision 6.1 Document Management.

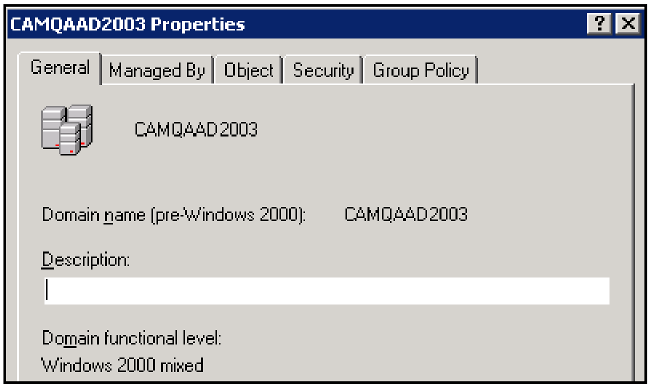
The domain configuration for the first two is effectively the same as far as Document Management is concerned and are not supported for Vision 6.1 Document Management because your only option is to configure what is called Unconstrained Delegation. The third domain can be configured for Unconstrained Delegation; however, Constrained Delegation is much more secure. Another benefit of a native Server 2003 domain is that it supports Protocol Transition, which is necessary to support Internet deployments of Vision where Document Management functionality is required.

## Identify the Domain Functional Level

You can check the functional level of the domain by opening the Active Directory Users and Computers tool on the Domain Controller:


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers [camqadc2
Saved Queries
CAMQAAD2003
Builtin
Computers
Domain Controllers

Right-click the domain, and select **Properties**.



CAMQAAD2003

Domain name (pre-Windows 2000): CAMQAAD2003

Description:

Domain functional level:
Windows 2000 mixed

You may need to raise the domain functional level to that supported by Vision 6.1 Document Management. If so, follow the steps outlined in the next section: “How to Raise the Domain Functional Level.”

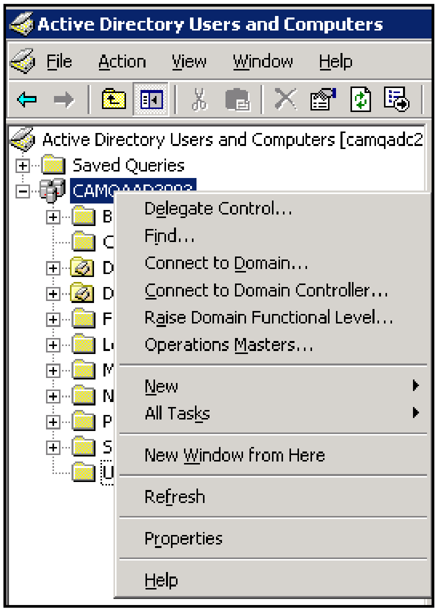
## How to Raise the Domain Functional Level

⚠ This operation cannot be reversed.

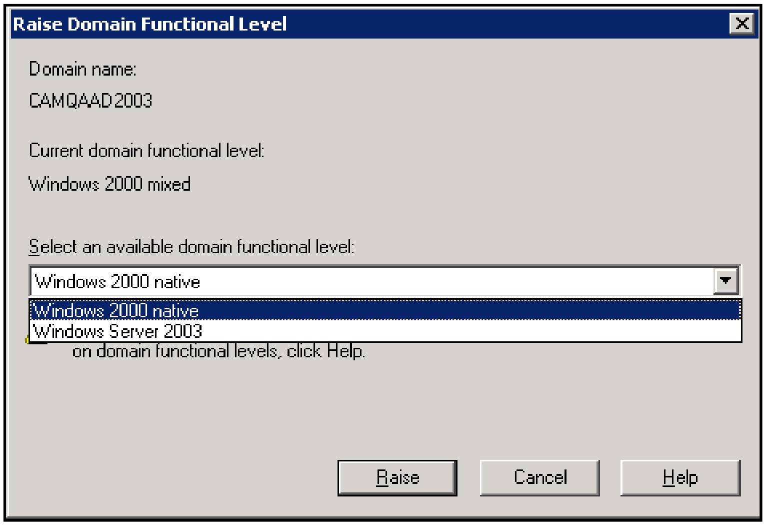
To raise the domain functional level, all Domain Controllers in the domain must be running Windows Server 2003. Also, this action cannot be reversed, so be sure that you want to raise the domain function level before you proceed.

**To raise the domain functional level, complete the following steps:**

1. Open the Active Directory Users and Computers MMC on your Domain Controller.
2. Right-click the domain**,** and select **Raise Domain Functional Level** on the shortcut menu.



3. Select **Windows Server 2003** from the **Select an available domain functional level** drop-down list, and click the **Raise** button.



Raise Domain Functional Level

Domain name:

CAMQAAD2003

Current domain functional level:

Windows 2000 mixed

Select an available domain functional level:

Windows 2000 native

Windows 2000 native

Windows Server 2003

on domain functional levels, click Help.

# Appendix B: Installing Vision 6.1 Document Management on Windows Server 2008/IIS 7.0

The information in this appendix applies only if you are installing Vision 6.1 Document Management in a Windows Server 2008/IIS 7.0 environment.

## Prerequisite Information

If you will install Vision 6.1 Document Management on Windows Server 2008 / IIS 7.0, note the following:

- The IIS role configuration must include the following IIS role service (in addition to those required for Deltek Vision): IIS 6.0 Metabase compatibility
- WSS 3.0 requires .NET 3.0, which is bundled with the operating system and can be installed by choosing .NET Framework 3.0 under **Feature setup** in Server Manager.
- The Managed Pipeline mode for the IIS 7.0 Application Pool for the WSS Web Application must be Classic (not Integrated Pipeline mode) if you choose to create a new Application Pool during the creation of the WSS Web application.
- If you will install WSS 3.0 on the same server as your Vision Web/application server, the WSS Web application must be created in its own Web site. Vision Document Management will not function properly if WSS and Vision exist on the same Web site.
- In a multi-tier installation of Vision Document Management using IIS 7.0 for the Vision Web/application server, the default configuration of Windows Integrated Authentication (which enables Kernel Mode Authentication) will not work because when you use Kernel Mode Authentication the Application Pool Identity is effectively ignored. Because Vision requires that this account be used for delegation, you must either disable Kernel Mode Authentication or configure the application pool to explicitly use the Application Pool Identity by modifying the ApplicationHost.config file. Information on the different configuration options are outlined later in this appendix.

## Configure Vision Application Pool Identity to Be a Domain Account

You must change the Vision Application Pool Identity to be a domain account. The default is for Vision to use a local DeltekVision user created during the Vision installation. This change is necessary because of the local account's inability to read the SPN configured in Active Directory.

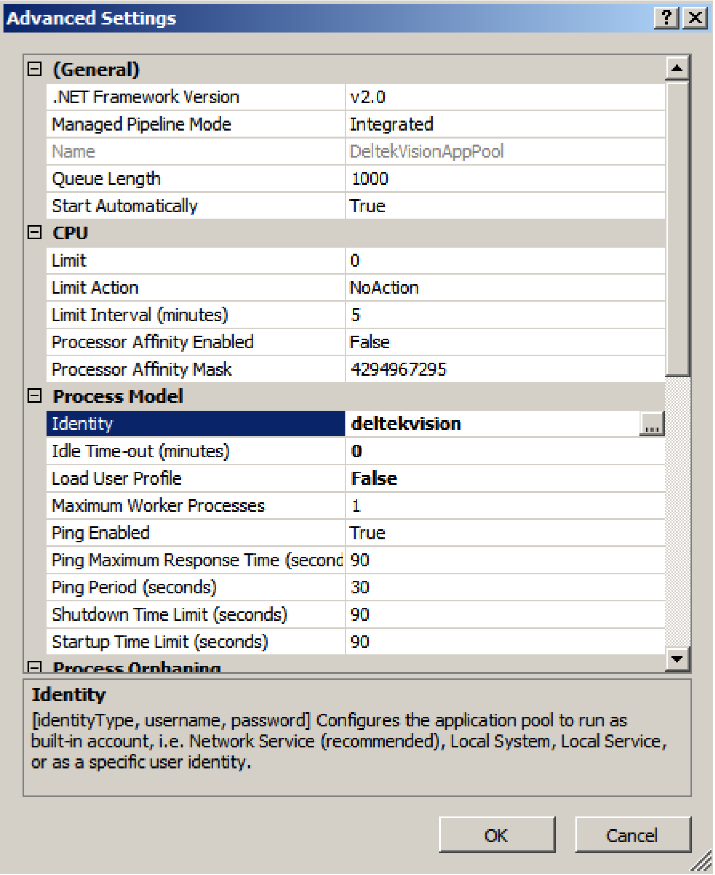
> For this account to be the Application Pool Identity it must be a member of the IIS_IUSRS group in IIS7.0, in addition to being a member of the local administrators group for Vision.

**To change the Vision Application Pool Identity, complete the following steps:**

1. Create a domain user account. This account must also be your WSS 3.0 Service account. No domain Admin rights are needed for this account.
2. Log on to the domain on the Vision Web/application server using an Administrator account.
3. Open Internet Information Services: **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager**.

4. Expand the Server name and then click **Application Pools**.

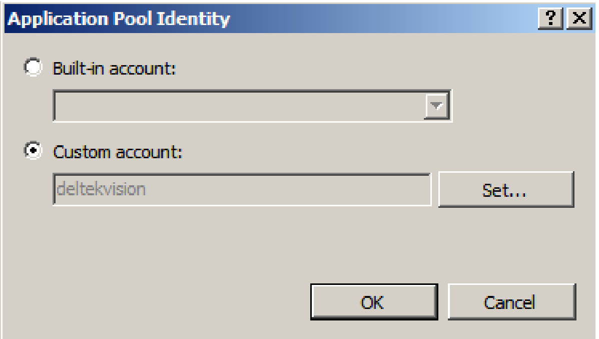
5. Select the **DeltekVisionAppPool** and select **Advanced Settings** from the Action pane on the right hand side. The following displays:



| | |
|---|---|
| **(General)** | |
| .NET Framework Version | v2.0 |
| Managed Pipeline Mode | Integrated |
| Name | DeltekVisionAppPool |
| Queue Length | 1000 |
| Start Automatically | True |
| **CPU** | |
| Limit | 0 |
| Limit Action | NoAction |
| Limit Interval (minutes) | 5 |
| Processor Affinity Enabled | False |
| Processor Affinity Mask | 4294967295 |
| **Process Model** | |
| Identity | **deltekvision** |
| Idle Time-out (minutes) | **0** |
| Load User Profile | **False** |
| Maximum Worker Processes | 1 |
| Ping Enabled | True |
| Ping Maximum Response Time (seconc | 90 |
| Ping Period (seconds) | 30 |
| Shutdown Time Limit (seconds) | 90 |
| Startup Time Limit (seconds) | 90 |
| **Process Orphaning** | |

**Identity**
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Network Service (recommended), Local System, Local Service, or as a specific user identity.

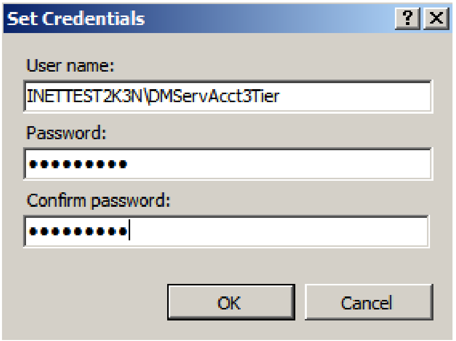
6. Place your cursor in the Identity field and then click the ellipses button to set the identity. The Application Pool Identify dialog box displays:



○ Built-in account:

● Custom account: deltekvision

7. Select the **Custom account** option and click **Set**. The Set Credentials dialog box displays.



User name:
INETTEST2K3N\DMServAcct3Tier
Password:
•••••••••
Confirm password:
•••••••••

8. In **User name**, enter the Application Pool Identity in the form <Domain>\<Username>. In **Password** and **Confirm password**, enter that user's password. Then click **OK** three times to set the identity.

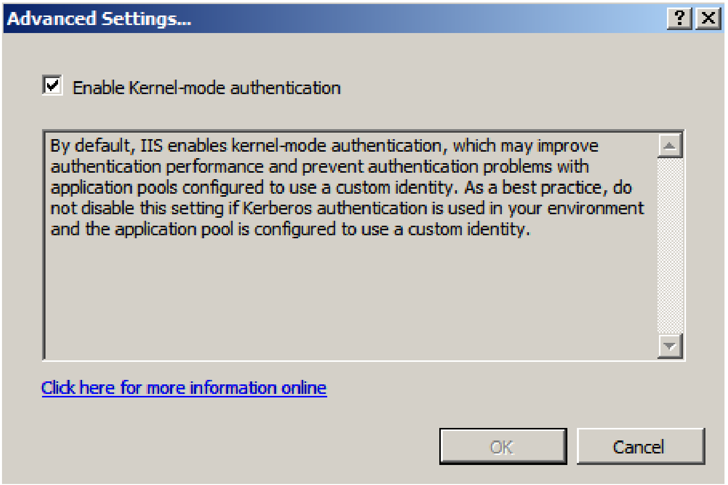
## IIS 7.0 Kernel Mode Authentication

The default configuration of IIS 7.0 when using Windows Integrated Authentication (required for Vision Document Management) is to use Kernel Mode Authentication. Under this configuration, the application pool runs under the Machine account whether or not an identity has been established. Because the Machine account cannot be used for delegation scenarios which are required for multi-tier deployments of Vision Document Management, the additional configuration steps below are necessary.

### Identify if Kernel Mode Authentication Is Enabled

Follow the steps below to identify if Kernel Mode Authentication is enabled. (In a default configuration of IIS 7.0, it will be enabled.)

1. Log on to the domain on the Vision Web/application server using an Administrator account.
2. Open Internet Information Services: **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager**.
3. Expand the server name, expand **Sites**, and expand **Default Web Site** or whichever site Vision is installed to.
4. Select the Vision virtual directory and then double click **Authentication** in the Features view.
5. Select **Windows Authentication** and verify that the status is Enabled (Anonymous Access should be Disabled). If it is not, select **Enable** from the Actions menu.
6. With **Windows Authentication** still selected, click **Advanced settings** on the Action menu. The Advanced Settings dialog box displays:



☑ Enable Kernel-mode authentication

By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.

Click here for more information online

## Kernel Mode Authentication Implementation

As mentioned above, under this default configuration, Vision Document Management will not be able to delegate credentials to a WSS 3.0 server separate from the Vision Web/application server. Two possible configurations allow Document Management to function properly:

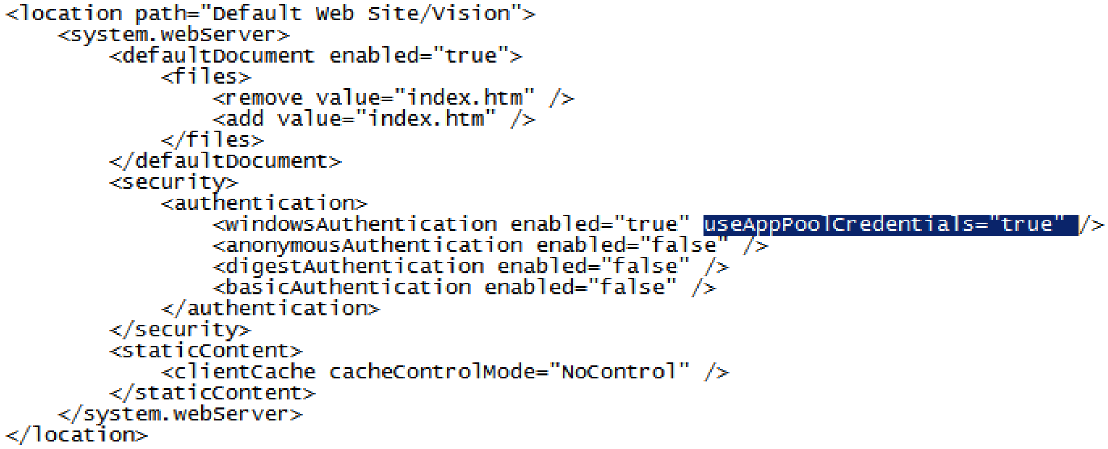
- **Disable Kernel Mode Authentication.** In order to Disable Kernel Mode Authentication, simply uncheck the Enable Kernel Mode Authentication option under the Advanced Settings of the Windows Authentication feature for the Vision virtual directory.
- **Modify the ApplicationHost.config file to force the use of the Application Pool Identity.** In order to continue to use Kernel Mode Authentication but force the Application Pool to run under its Identity rather than the Machine account, it is necessary to modify the ApplicationHost.config file, the steps of which are outlined below:

  1. Click **Start » All Programs » Accessories**.
  2. Right-click **Notepad**, click **Run as**, and select the Administrator account.

     > This is necessary in order to save the changes we need to make to the ApplicationHost.config file, which is protected under UAC (User Account Control) on Windows Server 2008.

  3. Click **Open** on the File menu and locate the ApplicationHost.config file from c:\windows\system32\inetsrv\config.
  4. Click Find on the Edit menu in Notepad and search for the following: <location path=”Default Web Site/Vision”>

5. Locate the windowsAuthentication tag and add **useAppPoolCredentials=”true”** as shown in the following:



```
<location path="Default Web Site/Vision">
    <system.webServer>
        <defaultDocument enabled="true">
            <files>
                <remove value="index.htm" />
                <add value="index.htm" />
            </files>
        </defaultDocument>
        <security>
            <authentication>
                <windowsAuthentication enabled="true" useAppPoolCredentials="true" />
                <anonymousAuthentication enabled="false" />
                <digestAuthentication enabled="false" />
                <basicAuthentication enabled="false" />
            </authentication>
        </security>
        <staticContent>
            <clientCache cacheControlMode="NoControl" />
        </staticContent>
    </system.webServer>
</location>
```

6. Once the edits are complete, save your changes and restart IIS to make the changes effective.

Both of these configuration options require that a Service Principal Name be established for the Application Pool Identity. The following section provides more information on SPNs.

## Service Principal Names

Under the default configuration with Kernel Mode Authentication enabled, it is *not necessary* to create a Service Principal Name for the Application Pool Identity. The default SPNs created will suffice. As a matter of fact, creating an SPN for the Application Pool Identity in this configuration will actually result in a “duplicate SPN” issue, preventing Windows Integrated Security from authenticating anyone to the Web site.

Once one of the above Kernel Mode configuration changes have been established, use the steps outlined below to create a Service Principal Name for the Application Pool Identity of the DeltekVisionAppPool.

> The setspn utility is installed by default on Windows Server 2008. It is not necessary to download and install it separately.

1. Open a command prompt and type the following:

   **setspn –A http/<Vision Web/App Server name> <domain app pool identity>**

   For example: setspn –A http/camqainetk3nwb5 inettest2k3n\dmservacct3tier

2. Repeat for the FQDN of the server.

Refer to the following related Microsoft Knowledge Base article:

http://support.microsoft.com/?id=871179

## Single Server—New Installation of Document Management 6.1

For the most part you will follow the steps outlined earlier in this document for installing Vision and WSS 3.0 on a single server. There are, however, several differences to keep in mind:

- Follow the steps provided earlier in this appendix to configure the Application Pool Identity.
- There is no need to modify the Kernel Mode Authentication settings or configure a Service Principal Name in this configuration, so you can bypass those steps.
- When you get to the point in the procedure where you create the SharePoint Web Application, be sure to either choose a Web site that is different from the one where Vision is installed or create a new Web site during the Create Web Application process.

⚠ **Vision will cease to function** if you install the SharePoint Web Application on the same Web site as Vision**.**

## Multi-Tier—New Installation of Document Management 6.1

For the most part you will follow the steps outlined earlier in this document for installing Vision and WSS 3.0 on separate servers. However, it is important that you follow the specific steps outlined in this appendix when configuring the DeltekVisionAppPool, Kernel Mode Authentication, and Service Principal Names.

# Appendix C: SPN Configuration When Using Custom DNS Records

If you will configure your SharePoint server to use a custom DNS record for the URL you must create an additional SPN and also create Alternate Access Mappings in SharePoint.

## Configure SPN for Custom DNS/FQDN Entry for SharePoint Web Server

Consider the following:

- If the URL you wish to use for your users (and also Vision Document Management) to access SharePoint will be an FQDN (Fully Qualified Domain Name), either based on the server name (for example,  servername.company.com) or based on a custom DNS entry (for example, sharepoint.company.com), you must create a Service Principal Name (SPN).
- If you will use a custom FQDN, you also must configure an Alternate Access Mapping in SharePoint for the FQDN. (Creation of the SPN is not necessary for an FQDN based on the server name.)

> 📖 For more information, refer to the following Microsoft support article: http://support.microsoft.com/?id=871179.

## Add an SPN for a Custom DNS Name

**To add an SPN for a custom DNS name, complete the following steps:**

1. Download **setspn.exe** from the Microsoft Web site: http://support.microsoft.com/kb/927229
2. Install the setspn.exe command line utility on the Vision Web server.
3. Open a command prompt to the c:\program files\resource kit directory and run the following command:

   **Setspn -A HTTP/*CustomDNSName WebServerNetbiosName***

   Where *CustomDNSName* is the fully qualified domain name of the server (for example, Vision.company.com) and *WebServerNetbiosName* is the actual netbios computer name of the server (for example, Server01).
4. **If you are doing a new multi-tier installation of Document Management 6.1 with Windows SharePoint Services 3.0**:  If WSS 3.0 was installed before Deltek Vision Document Management, and the SharePoint Web application pool was created using a domain account, it is necessary to register SPNs for this domain account. Otherwise, you will receive the same authentication errors when you attempt to configure Vision Document Management. See the following Microsoft Support Article for details (http://support.microsoft.com/?id=871179).

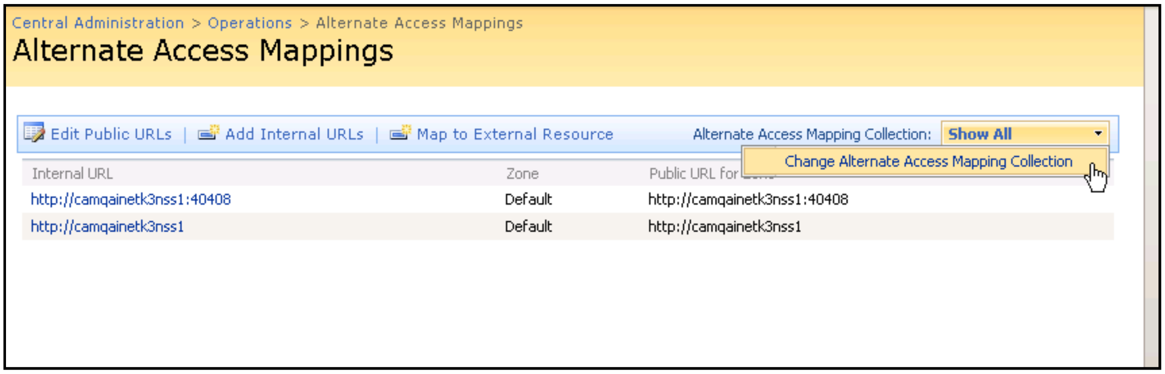
   **If you are doing a new multi-tier installation of Document Management 6.1 with MOSS 2007:** When you install MOSS 2007 and create the Web application, the application pool by default is created using a domain account. Due to this configuration, it is necessary to register SPNs for this domain account. Otherwise, you will receive the same authentication errors when you attempt to configure Vision Document

Management. See the following Microsoft Support Article (http://support.microsoft.com/?id=871179).

## Create or Modify Alternate Access Mappings

**To create or modify alternate access mappings, complete the following steps:**

1. Click **Operations » Alternate Access Mappings**.



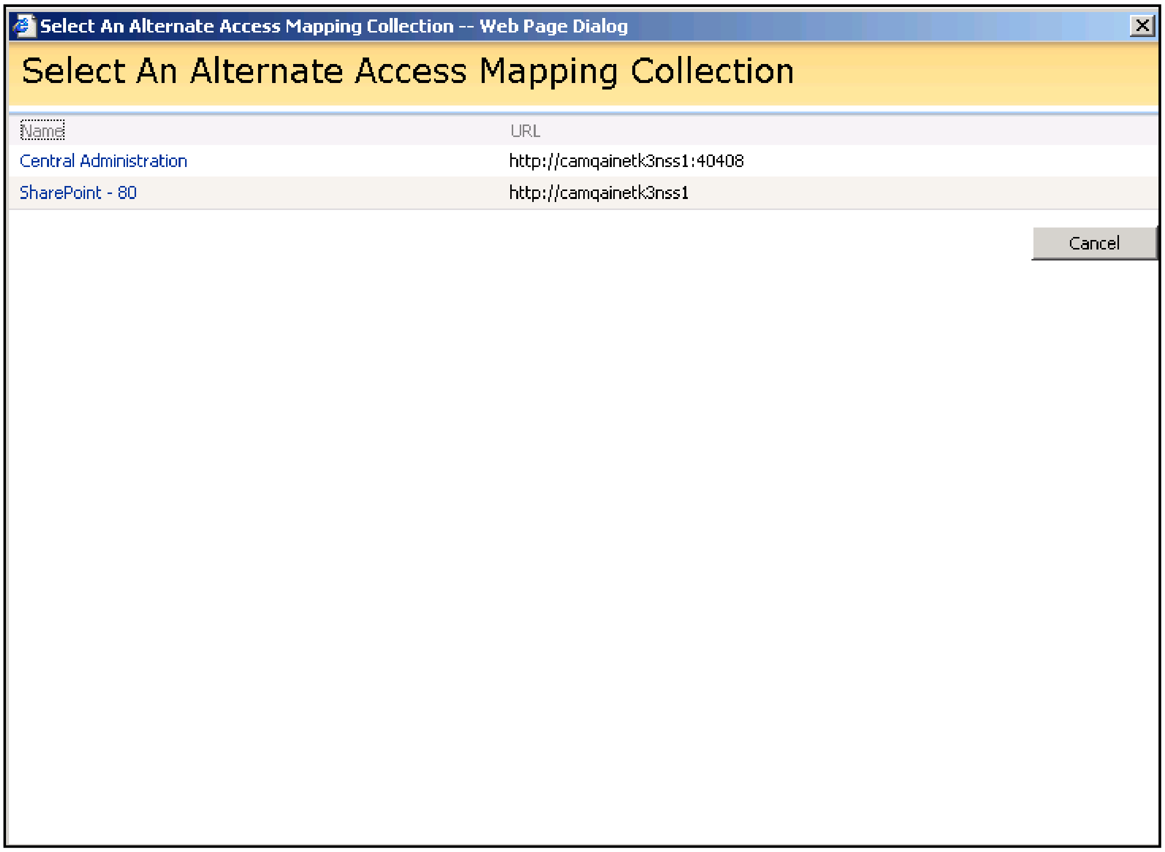
Central Administration > Operations > Alternate Access Mappings

Alternate Access Mappings

Edit Public URLs
Add Internal URLs
Map to External Resource
Alternate Access Mapping Collection:
Show All
Change Alternate Access Mapping Collection

| Internal URL | Zone | Public URL for Zone |
|---|---|---|
| http://camqainetk3nss1:40408 | Default | http://camqainetk3nss1:40408 |
| http://camqainetk3nss1 | Default | http://camqainetk3nss1 |

2. Click **Show All** and select **Change Alternate Access Mapping Collection**. The Select an Alternate Access Mapping Collection page displays.

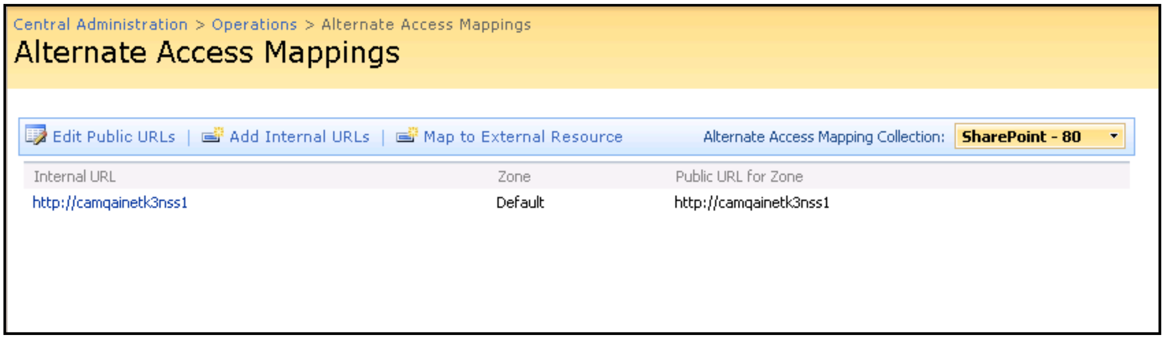


Select An Alternate Access Mapping Collection -- Web Page Dialog

Select An Alternate Access Mapping Collection

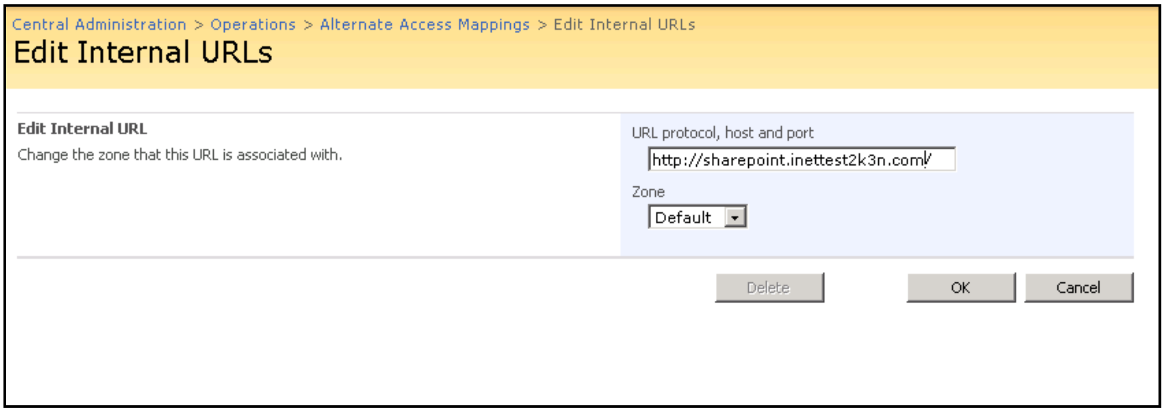
| Name | URL |
|---|---|
| Central Administration | http://camqainetk3nss1:40408 |
| SharePoint - 80 | http://camqainetk3nss1 |

3. Select the link for the new WSS site you created. In the above illustration, it is **SharePoint – 80**. This will filter the list to only show the mappings for this application. The Alternate Access Mapping page displays.


Central Administration > Operations > Alternate Access Mappings
Alternate Access Mappings
Edit Public URLs | Add Internal URLs | Map to External Resource
Alternate Access Mapping Collection: SharePoint - 80

| Internal URL | Zone | Public URL for Zone |
|---|---|---|
| http://camqainetk3nss1 | Default | http://camqainetk3nss1 |

4. Click the link for the Web application you created. The Edit Internal URLs page displays.


Central Administration > Operations > Alternate Access Mappings > Edit Internal URLs
Edit Internal URLs
Delete
OK
Cancel

**Edit Internal URL**

Change the zone that this URL is associated with.

URL protocol, host and port: http://sharepoint.inettest2k3n.com/

Zone: Default

5. Modify the URL to specify the custom FQDN and click **OK**. If a port is specified, do not remove it.

## Configure Delegation When Using a Custom DNS Record and a Domain Account as the Application Pool Identity

**To configure delegation when using a custom DNS record and a domain account as the Application Pool Identity for the SharePoint Web application, complete the following steps:**

1. Open a command prompt to the c:\program files\resource kit directory, and run the following command:

   **Setspn -A HTTP/*CustomDNSName SharePointServerAppPoolID***

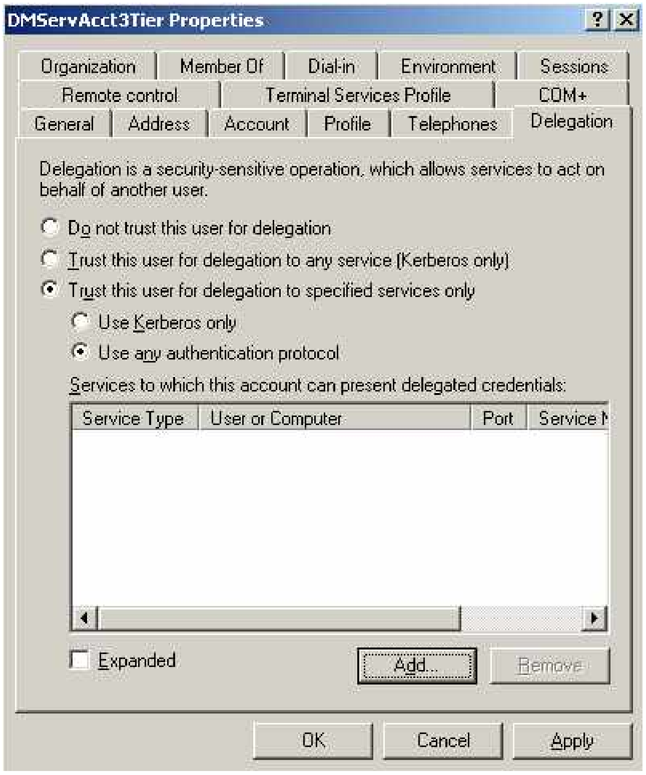
   Example:  setspn –A HTTP/visiondm.domain.com domain\user

   Where *CustomDNSName* is the fully qualified domain name of the server (for example, Vision.company.com) .

   Because the account is the Application Pool Identity for both applications ***and*** SharePoint is using a custom DNS record, the service account (Application Pool Identity) is effectively delegating to itself or, more accurately stated, is delegating to another SPN of which the account is the owner.

2. Open the Active Directory Users and Computers MMC,
3. Locate the service account (Application Pool Identity).
4. Right-click and select **Properties**.

5. Click the Delegation tab:



DMServAcct3Tier Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

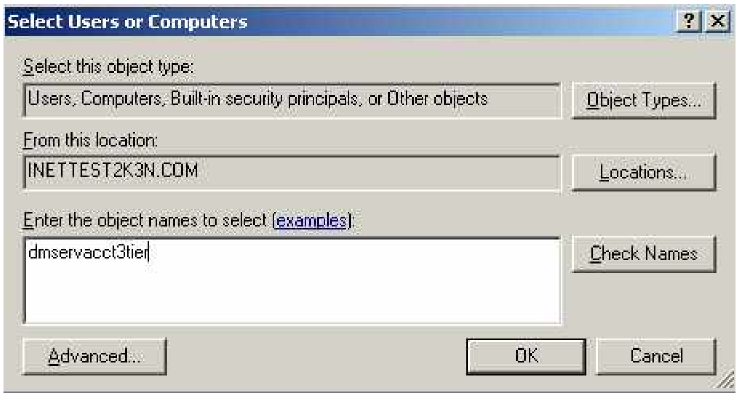
● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port | Service N |
|---|---|---|---|

□ Expanded

6. Click **Add** and enter the service account name (Application Pool Identity). This is the same account for which you are viewing properties. Click **OK**.



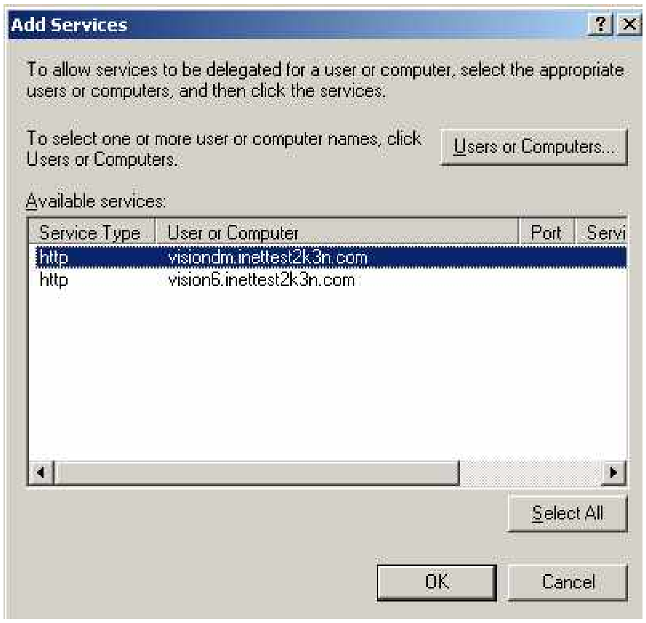
Select Users or Computers

Select this object type:
Users, Computers, Built-in security principals, or Other objects

From this location:
INETTEST2K3N.COM

Enter the object names to select (examples):
dmservacct3tier

7. In the Add Services dialog box, select the SPN for the SharePoint server (**visiondm…**):



To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

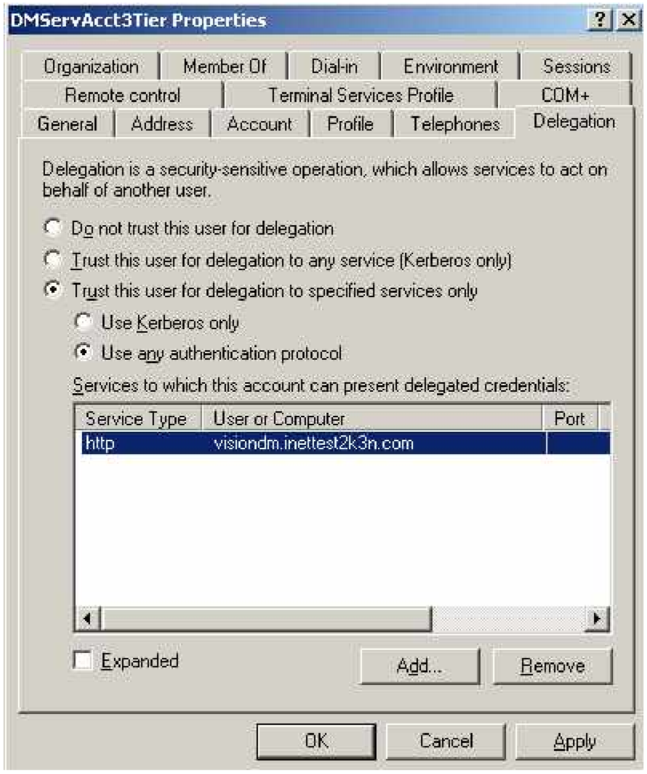
Available services:

| Service Type | User or Computer | Port | Servi |
|---|---|---|---|
| http | visiondm.inettest2k3n.com | | |
| http | vision6.inettest2k3n.com | | |

Note that this account also has an SPN for the Vision server because it is also the Application Pool Identity for the DeltekVisionAppPool.

8. Click **OK**.

   The Delegation tab should look like this when you have completed this procedure:



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

| Service Type | User or Computer | Port |
|---|---|---|
| http | visiondm.inettest2k3n.com | |

□ Expanded