Security and Kerberos Authentication with K2 Servers

SECURITY RIGHTS AND STEP-BY-STEP INSTRUCTIONS FOR CONFIGURING KERBEROS FOR K2 [BLACKPEARL]

January 10

Learn about the security rights required by K2 [blackpearl] installation and runtime, and how to configure Kerberos for K2 Servers in a distributed environment. Includes specific examples and a series of checklists for troubleshooting authentication issues.

INTRODUCTION

K2 blackpearl is built upon common security standards for the Windows platform. Use this article to understand what rights are required to install and run K2 blackpearl. This whitepaper also contains detailed information about how to configure K2 blackpearl components to use Kerberos authentication. System administrators must establish Kerberos configuration in a distributed environment where servers are in the same domain and network, and can be hosting server applications such as Microsoft Office SharePoint Server, Internet Information Servers (IIS) Web sites, SQL Server and K2 Servers. Read this paper in its entirety before proceeding further.

CONTENTS

OVERVIEW OF SECURITY

The **System Account Requirements** topic in the K2 [blackpearl] Getting Started guide recommends the K2 Service account be granted "Local Administrator" rights on the server where K2 blackpearl is installed. These rights are necessary for a K2 blackpearl installation to function and are detailed in this KB article. These rights can be individually granted to a non-Administrator account when a security policy requires stricter security on application service accounts.

RUNTIME RIGHTS REQUIRED BY THE K2 ACCOUNTS

The K2 Service and Workspace accounts require access and rights to the following folders and registry keys:

Folder or Registry Key	Account	Rights	Server
%SYSTEMROOT%\temp	K2 Service	Full Control	K2/MOSS
%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12	K2 Service	Write Access	MOSS
%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA	K2 Service	Full Control	K2/MOSS
HKEY_LOCAL_MACHINE\SOFTWARE\SourceCode\Logging	K2 Service	Full Control	K2/MOSS
%SYSTEMROOT%\Microsoft.NET\Framework\v2.0.50727\CONFIG	K2 Service	Modify	K2/MOSS
%PROGRAMFILES%\K2 blackpearl\Host Server\Bin	K2 Service	Modify	K2
%SYSTEMROOT%\Temp	K2 Workspace (Web Application Pool) Account	Modify	K2/MOSS

Granting these rights to the appropriate accounts will allow companies with strict security policies to avoid granting the K2 Service and Workspace accounts full administrative rights to the server.

If installing in a distributed environment, security rights on these folders and the registry key will depend on which components are installed on the server. The only folder listed above that is not directly related to the K2 [blackpearl] Server or Workspace components is the "%COMMONPROGRAMFILES%\Microsoft Shared\web

server extensions\12" folder, which is present only if SharePoint (WSS v3 or MOSS 2007) is installed. If SharePoint is installed on different server, the K2 Service account still requires rights to the folder on that server.

Note: Users deploying K2 Web Designer workflows to SharePoint need 'Contributor' rights on the SharePoint site collection. The MOSS/WSS Web Application Pool account requires Write access to %COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\Layouts\Features and %COMMONPROGRAMFILES%\Microsoft Shared\web server extensions \12\ISAPI and must be a local administrator on the server in order to log K2 [blackpearl] Server errors to the event log.

INSTALLATION RIGHTS

The account under which K2 [blackpearl] is installed requires an account in the local administrators group. This allows the "eventbus" and "eventbus error" message queues to be created as well as the event log source "K2 BlackPearl Server."

The account under which K2 blackpearl is installed also creates the following Performance Counter registry keys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\K2 [blackpearl] Server
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\K2 Server

Once these registry keys are present, the K2 service account will be able to write values to these performance counters without administrative privileges because the K2HostServer.exe application is a trusted application.

Other modifications during installation include the installation of program files, entries in configuration files, such as machine.config, and the creation of the K2 databases. These actions require administrator privileges.

For more information about installing K2 blackpearl, including setting up Kerberos and MSDTC for distributed environments, see the **Getting Started** guide available on the K2 Customer and Partner portal.

RIGHTS REQUIRED BY THE WSS/MOSS APPLICATION POOL ACCOUNT

The WSS or MOSS Web application pool account needs both **db_DataReader** and **db_DataWriter** rights on the WebWorkflow SQL database that is used for the K2 Web Designer in SharePoint sites. The **Execute** right is also need for stored procedures in this database. Without this access the K2 Web Designer will not function.

OVERVIEW OF KERBEROS

Kerberos authentication is a type of Integrated Windows Authentication that allows delegation of users' credentials across multiple servers, allowing a server to pass the credentials of the user to another server or service. In contrast, NTLM, another type of Integrated Windows Authentication, can only pass user credentials to a single server, which is typically between client and server. If those credentials are required by a second server,

the NTLM "double-hop" problem is introduced. In a single server environment where all K2 blackpearl components are installed on one server, NTLM can be used. However, Kerberos authentication is required in a distributed environment where K2 blackpearl components or supporting technologies are installed on different servers on the network.

This information in this section is based on the following assumptions:

1. The administrator or person responsible for configuring Kerberos has read the K2 blackpearl installation documentation included in the Getting Started guide.
2. K2 blackpearl Host Server and other components have been successfully installed.
3. K2 blackpearl configuration manager has been run and completed successfully.
4. K2 blackpearl Host Server can be started up successfully.
5. SQL Server and SQL Reporting Services are running properly.
6. SharePoint Server is running properly (if applicable in the environment).

Note: Kerberos configuration can occur either before or after the installation of K2 blackpearl. The configuration of K2 blackpearl, which occurs directly after installation, allows for the automatic setting of the K2 [blackpearl] Server SPNs.

K2 [BLACKPEARL] INSTALLATION SCENARIOS

K2 supports a variety of installation configurations, including single server, distributed and server farms.

SINGLE SERVER INSTALLATION

All the K2 blackpearl components, dependencies and prerequisites are installed locally on the same physical machine, with the exception of the SQL 2005 Server, which can be installed on a remote or adjacent physical machine.

Kerberos is not required in a single server environment. However it is recommended to use Kerberos authentication if K2 solutions will be migrated and deployed to a distributed system environment such as for testing and production.

DISTRIBUTED INSTALLATION

K2 blackpearl components, dependencies and prerequisites are installed on multiple servers across a network. Kerberos must be configured for a distributed installation to function correctly.

SERVER FARM

A K2 server farm is a clustering environment for multiple K2 Host Servers. There are multiple vendors offering solutions for system clustering and load balancing. Configuration for clustering and/or load balancing systems is beyond the scope of this article.

HOW KERBEROS IS USED IN DISTRIBUTED ENVIRONMENTS

The following server components and web services require Kerberos authentication when K2 blackpearl is installed in a distributed environment. Some specific K2, SQL and SQL Reporting Service, and MOSS rights are discussed as they pertain to successfully using the feature or service. In some cases, Kerberos and K2 Impersonation are required for user authentication and for the server or service to act on the users behalf.

SHAREPOINT AND RUNTIME SERVICES (WEB SERVICES)

SharePointService.asmx: The SharePointService web service is a K2 web service that is used to initiate process instances from SharePoint Events. The web service requires Kerberos authentication in a distributed environment to pass credentials from SharePoint to the SharePointService and then to the K2 blackpearl Server. In a SharePoint Workflow Integration process, K2 impersonation is used to pass credentials from the web service to the K2 blackpearl Server.

SharePoint Wizards (wizards or event templates that allow interaction with SharePoint components, such as documents, search results, list items, records, publishing sites, regular sites and users): The blackpearl server calls the K2 integration components in MOSS/WSS using the blackpearl service account to interact with MOSS/WSS for these events.

InfoPathService.asmx: Delegates the user's credentials to the blackpearl server using Kerberos to create and start the process instance. Note that an InfoPath process does not use K2 Impersonation and requires Kerberos authentication in a distributed environment. When using browser-enabled forms the InfoPathService web service must be installed on the MOSS/WSS server due to an InfoPath Forms Services limitation.

REPORTING

K2 Reports (non-SQL Server Reporting Services (SRSS) reports): Authentication occurs as the end-user via Kerberos. K2 Workspace delegates the user's credentials to the blackpearl server to execute the desired action.

K2 Reports (published to SSRS): SSRS delegates the user's credentials to blackpearl to obtain and return the report data based on the users' View and/or View Participate permissions. When publishing a report from Workspace Report Designer, both the blackpearl server and the SSRS server are accessed as the Workspace Application Pool account.

SRSS Reports (imported into Workspace): User accesses the reports on the Workspace home page or access the Workspace Reports Designer to run a report in SSRS. Authentication occurs as the end-user via Kerberos. Workspace delegates the user's credentials to the SQL Reporting Services web site to run the report. The user must have appropriate permissions (at minimum "Browser") in SSRS to run the report. SSRS delegates the user's

credentials to the blackpearl server to run the report and return the data based on the users' View and/or View Participate permissions. When importing a report from Workspace Reports Designer, both the blackpearl server and the SSRS server are accessed as the Workspace Application Pool account.

OTHER K2 COMPONENTS AND SUPPORTING TECHNOLOGY

Workspace: A user accesses the Workspace Web site from a remote client and must authenticate using Kerberos. Workspace will delegate the user's credentials to the blackpearl server and authenticate using Kerberos.

K2 Web Designer: Process deployment uses the MOSS Application Pool account, which must have Export Server Rights in the K2 Workflow Server. The blackpearl "WebWorkflow" database is also accessed directly using the identity of the MOSS Application Pool account. This account must have at least db_datareader and db_datawriter Roles in the WebWorkflow database.

SQL Server (for blackpearl): The blackpearl server accesses the blackpearl databases using the blackpearl service account or via SQL Authentication as the account specified during the install. SPNs for MSSQLSERVER may or may not be required, depending on the environment. In many cases SQL creates SPNs and in other cases, such as when using a named instance, SPNs must be manually created.

SharePoint SmartObject Service instance: If a security provider/username/password is not configured for the Service Instance and Impersonate is not checked, the Service Instance will run under the context of the blackpearl service account and authenticate in MOSS as such. Note that the Impersonate checkbox should not be used when configuring the service instance as there typically will not be a user to impersonate.

K2 [blackpearl] Worklist Web part: A user accesses a page in SharePoint that is configured with the K2 Worklist web part and must authenticate using Kerberos. The Web part will delegate the user's credentials to the blackpearl server and authenticate using Kerberos to retrieve the worklist, open worklist items, and action worklist items. The Worklist web part does not use K2 Impersonation and requires Kerberos authentication in a distributed environment.

Forms Generation Client Event: When a user opens a Forms Generation Client Event .ASPX web page they are authenticated using Integrated Windows Authentication. The RuntimeServices Application Pool account authenticates against the blackpearl server and impersonates the user to retrieve the worklist item. The same thing occurs when the user actions the workflow using the form, however the actioning also calls the ClientEventServer.asmx web service. This web service is not used if the process is actioned from the context menu in the Workspace worklist.

The identity used for the RunTimeServices Application Pool must have 'Impersonate' Server Rights in the Workflow Server. Since the ClientEventService.asmx Web service uses impersonation when communicating with the blackpearl server, it will not work with Kerberos alone in a distributed environment as they work in conjunction for authentication and authorization.

CONFIGURING ACTIVE DIRECTORY

Active Directory consists of objects such as users, groups and computers. Adding, deleting or updating an object in Active Directory requires replication to every other domain controller that stores the object before the changes can take effect and Kerberos authentication can be tested with those changes.

> **Note:** Active Directory replication can take some time. The replication interval can be set in minutes. There are tools available to force AD replication, such as Repadmin.exe, Replmon.exe, and frsdiag.exe that are part of Windows Server 2003 Service Pack 1 Support Tools which can be downloaded from Microsoft (see URL below). For more details, contact your Domain Administrator.

CREATING SPNS

An important step for setting up Kerberos authentication is to create Service Principal Names (SPNs) for services and to register SPNs under their service accounts in Active Directory. Each service that will use Kerberos authentication needs to have a unique SPN identifier so that a client application can identify the service on the network.

If an SPN was incorrectly set or if there are duplicate SPNs, when a client application attempts to obtain a service ticket from the Key Distribution Center (KDC) for the relevant service, Kerberos authentication will fail.

> **Note:** Kerberos errors can be found in Event Viewer > System if Kerberos logging is enabled. Typical errors include KDC_ERR_PRINCIPAL_UNKNOWN and KDC_ERR_PRINCIPAL_NOT_UNIQUE. For a complete description, refer to the Troubleshooting Kerberos Errors topic on TechNet (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx) .

For details on how to enable Kerberos logging, see the Microsoft knowledgebase article **How to enable Kerberos event logging (http://support.microsoft.com/kb/q262177/).**

Only the domain administrator or a user with domain administration rights can create or add SPNs in Active Directory. To create SPNs, use the Setspn.exe utility with the "-A" option. To display a list of configured SPNs, use the "-L" option. Setspn.exe is part of the **Windows Server 2003 Service Pack 1 32-bit Support Tools** (http://www.microsoft.com/downloads/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en).

To create SPNs for K2 blackpearl components and other relevant services such as SQL Server and SharePoint Server refer to table as shown below for the command format.

> **Notes for the following tables:**
> - SP1 refers to K2 blackpearl SP1 and not other service packs for Windows or the .NET frameworks.
> - The [MachineName] token refers to the name of the computer on which the service is running.
> - The [MachineName.FQDN] refers to the fully-qualified domain name of the computer on which

the service is running.

- Both SPNs are required -- [MachineName] and [MachineName.FQDN]. Do not set only one or the other.
- Specifying the service account is required and should not be ignored.

SPNs needed for	From a command prompt
Host Server (SP1 or higher)	setspn – A K2HostServer/[MachineName]:5555 [DomainName]\[ServiceAccount] setspn – A K2HostServer/[MachineName.FQDN]:5555 [DomainName]\[ServiceAccount]
Host Server (Only prior to SP1)	setspn – A BlackPearlServer/[MachineName]:5555 [DomainName]\[ServiceAccount] setspn – A BlackPearlServer/[MachineName.FQDN]:5555 [DomainName]\[ServiceAccount]
Workflow Server	setspn – A K2Server/[MachineName]:5252 [DomainName]\[ServiceAccount] setspn – A K2Server/[MachineName.FQDN]:5252 [DomainName]\[ServiceAccount]
Workspace Application Pool Identity Account	setspn – A HTTP/[MachineName] [DomainName]\[AppPoolAccount] setspn – A HTTP/[MachineName.FQDN] [DomainName]\[AppPoolAccount] If the web site uses Host Header, create SPNs as the following: setspn – A HTTP/[HostHeaderName] [DomainName]\[AppPoolAccount] setspn – A HTTP/[HostHeaderName.FQDN] [DomainName]\[AppPoolAccount]
SQL Server 2005 Service Account	setspn – A MSSQLSvc/[MachineName]:[Port] [DomainName]\[ServiceAccount] setspn – A MSSQLSvc/[MachineName.FQDN]:[Port][DomainName]\[ServiceAccount]
SQL Reporting Service Application Pool Identity Account	setspn – A HTTP/[MachineName] [DomainName]\[ServiceAccount] setspn – A HTTP/[MachineName.FQDN] [DomainName]\[ServiceAccount]

	If the web site uses Host Header, create SPNs as the following: setspn – A HTTP/[HostHeaderName] [DomainName]\[ServiceAccount] setspn – A HTTP/[HostHeaderName.FQDN] [DomainName]\[ServiceAccount] Or if Local System or Network Service is used as application pool identity account, no SPNs needed. NOTE: See **Section Configure IIS Server for SQL Server Reporting Services** for more details.
SharePoint Server Service Account	setspn – A HTTP/[MachineName] [DomainName]\[ServiceAccount] setspn – A HTTP/[MachineName.FQDN] [DomainName]\[ServiceAccount] If the web site uses Host Header, create SPNs as the following: setspn – A HTTP/[HostHeaderName] [DomainName]\[ServiceAccount] setspn – A HTTP/[HostHeaderName.FQDN] [DomainName]\[ServiceAccount]

The following table lists SPN configurations that are only required for Server Farm installations:

SPNs needed for	From a command prompt
Server Farm Option for K2 Host Server **(SP1 or higher)**	In addition to BlackPearlServer / K2Server SPNs for each farm node, create SPNs for the Farm name as the following: setspn – A K2HostServer/ FarmName]:5555 [DomainName]\[ServiceAccount] setspn – A K2HostServer/ FarmName.FQDN]:5555 [DomainName]\[ServiceAccount]
Server Farm Option for K2 Host Server **(Only prior to SP1)**	In addition to BlackPearlServer / K2Server SPNs for each farm node, create SPNs for the Farm name as the following: setspn – A BlackPearlServer/FarmName]:5555 [DomainName]\[ServiceAccount] setspn – A BlackPearlServer/[FarmName.FQDN]:5555 [DomainName]\[ServiceAccount]

Workflow Server	setspn – A K2Server/[FarmName]:5252 [DomainName]\[ServiceAccount] setspn – A K2Server/[FarmName.FQDN]:5252 [DomainName]\[ServiceAccount]
Server Farm Option for Workspace	setspn – A HTTP/[WorkspaceFarmName] [DomainName]\[ServiceAccount] setspn – A HTTP/[WorkspaceFarmName.FQDN] [DomainName]\[ServiceAccount] NOTE: See **Section Configure IIS Server for K2 Workspace** for more details.

CONFIGURE KERBEROS DELEGATION

Delegation enables a user's credential to be passed from one server to another and for the user's identity to be preserved as services are requested from one computer to another.

Requirements for delegation to work, as an example, for K2 blackpearl Workspace:

- All domain user accounts and service accounts must not have the **Account is sensitive and cannot be delegated** option selected. This option is a Domain security policy setting.
- HTTP SPNs must be created for the application pool identity account running the web site for Workspace.
- The application pool identity account for Workspace must be set to be trusted for delegation in Active Directory.
- SPNs must be created for K2 Host Server and K2 Workflow Server.
- If using constrained delegation, both IIS server for Workspace and K2 Host Server must be in the same domain.
- To use constrained delegation, all domain controllers in the domain must be running Windows Server 2003, and the domain must be operating at the Windows Server 2003 functional level.

Note: To determine which delegation scenario to use, contact your System Administrator and/or Domain Administrator.

Delegation is possible only with Kerberos protocol. All services involved in delegation scenarios must use the Kerberos protocol. There are three delegation scenarios illustrated in this section:

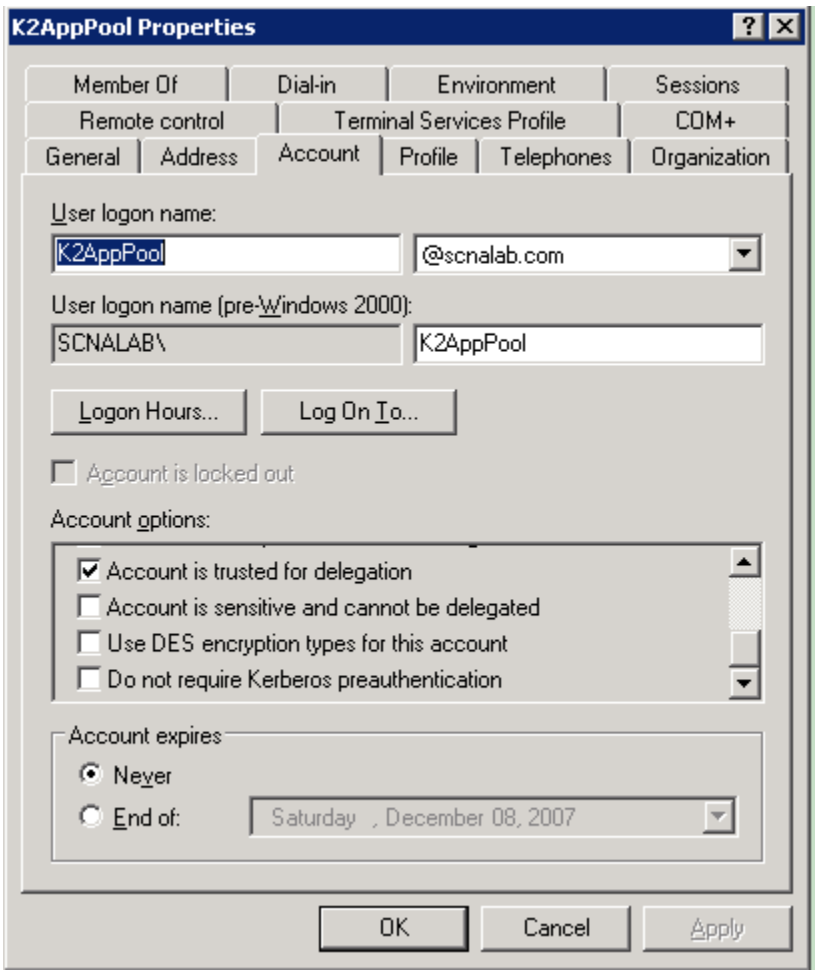
- Non-constrained delegation
- Constrained delegation
- Constrained delegation with protocol transition

NON-CONSTRAINED DELEGATION

To set up Non-Constrained Delegation in domains operating at **Windows Server 2000** functional level, follow these steps:

1. Click Start > All Programs > Administrative Tools > Active Directory Users and Computers.
2. Right-click the service account and select **Properties**
3. Click the **Account** tab
4. Scroll the Account options box and select **Account is trusted for delegation** option.
5. Click **OK**

The properties dialog box should resemble Figure 1.

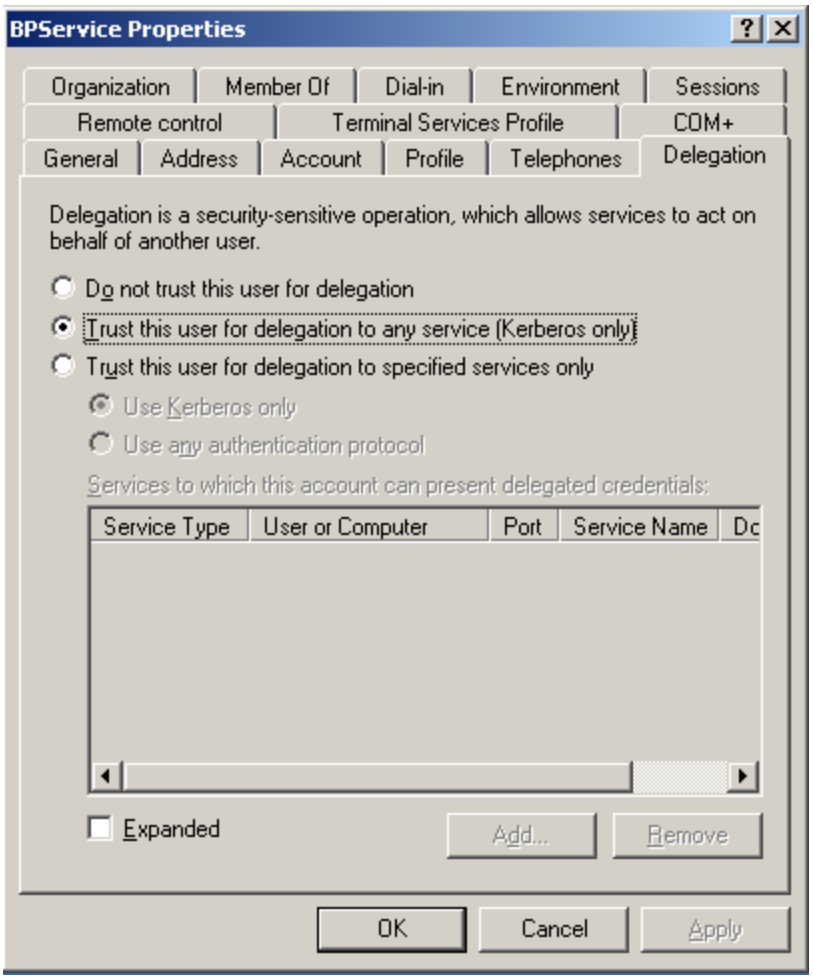


[FIGURE 1: ACCOUNT PROPERTIES FOR WINDOWS 2000 FUNCTIONAL LEVELS]

To set up Non-Constrained Delegation in domains operating at **Windows Server 2003** functional level, follow these steps:

1. Click Start > All Programs > Administrative Tools > Active Directory Users and Computers.
2. Right-click the service account and select **Properties**
3. Click the **Delegation** tab
4. Click **Trust this user for delegation to any service (Kerberos only)**
5. Click **OK**

The properties dialog box should resemble Figure 2.



[FIGURE 2: ACCOUNT PROPERTIES FOR WINDOWS 2003 FUNCTIONAL LEVELS]

Note: If there is no SPN created for the account, the delegation tab (as shown in Figure 2) will not be available.

CONSTRAINED DELEGATION

Constrained delegation gives administrators the ability to specify and enforce application trust boundaries by limiting the scope where application services can act on a user's behalf. This flexibility to constrain service authorization rights helps improve application security design by reducing the opportunities for a network to be compromised by untrusted services.

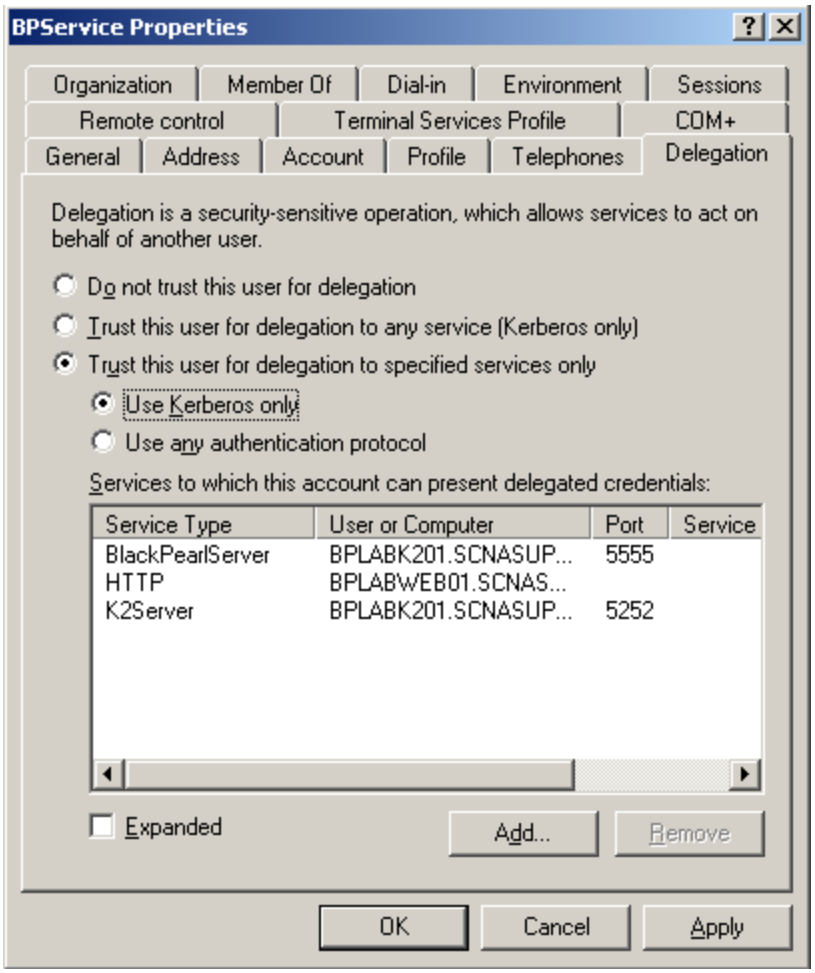
Note: Constrained Delegation is possible only if the domain is Windows Server 2003 functional level.

Constrained delegation cannot be used between services whose accounts are in different domains. All domain controllers in the domain must be running Windows Server 2003, and the domain must be operating at the Windows Server 2003 functional level. The accounts of users accessing the services do not have to be in the same domain as the services.

To set up Constrained Delegation in domains operating at Windows Server 2003 functional level, follow these steps:

1. Click Start > All Programs > Administrative Tools > Active Directory Users and Computers.
2. Right-click the service account and select **Properties**
3. Click the **Delegation** tab
4. Click **Trust this user for delegation to specified services only** and click **Use Kerberos only**
5. Click **Add** to add relevant services

The properties dialog box should resemble Figure 3.



[FIGURE 3: ACCOUNT PROPERTIES CONSTRAINED DELEGATION USING KERBEROS]

CONSTRAINED DELEGATION WITH PROTOCOL TRANSITION

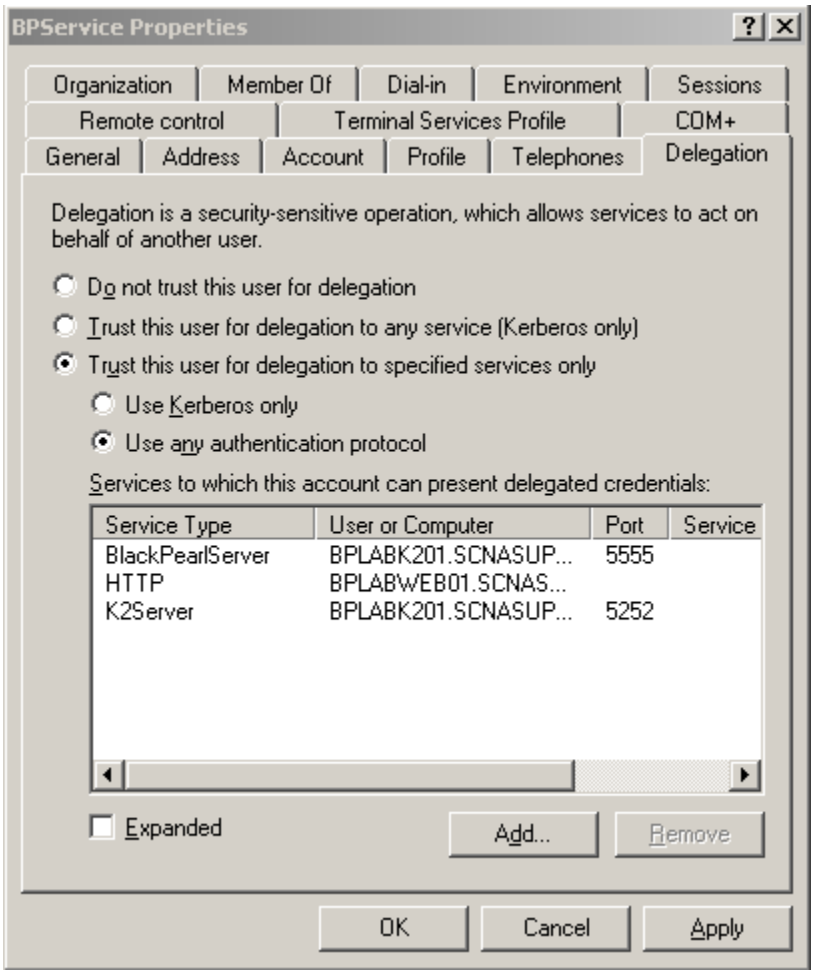
In Windows Server 2003, protocol transition enables delegation to occur even if the authentication process initially uses another authentication protocol instead of Kerberos. For example, it is unrealistic to perform Kerberos authentication over the Internet. Instead, a method such as Secure Socket Layers (SSL) might be used by a front-end IIS server. However, after the front-end server verifies the user's identity, it can perform a protocol transition and subsequently use Kerberos authentication features within the corporate network.

To set up Constrained Delegation with Protocol Transition in domains operating at Windows Server 2003 functional level, follow these steps:

1. Click Start > All Programs > Administrative Tools > Active Directory Users and Computers.
2. Right-click the service account and select **Properties**
3. Click the **Delegation** tab

4. Click **Trust this user for delegation to specified services only** and click **Use any authentication protocol**
5. Click **Add** to add relevant services

The properties dialog box should resemble Figure 4.



[FIGURE 4: ACCOUNT PROPERTIES CONSTRAINED DELEGATION USING ANY PROTOCOL]

CONFIGURE IIS SERVER FOR K2 WORKSPACE

K2 blackpearl Workspace can be hosted under Default Web Site, and the TCP port number is 80 by default. Therefore the URL for Workspace can be written in the format below:

HTTP://[WebserverName]/Workspace/Navigation/Navigation.aspx

Alternatively, a new Web Site can be created for K2 Workspace, with a TCP Port number that is not shared by other Web sites. The URL for Workspace is in this format:

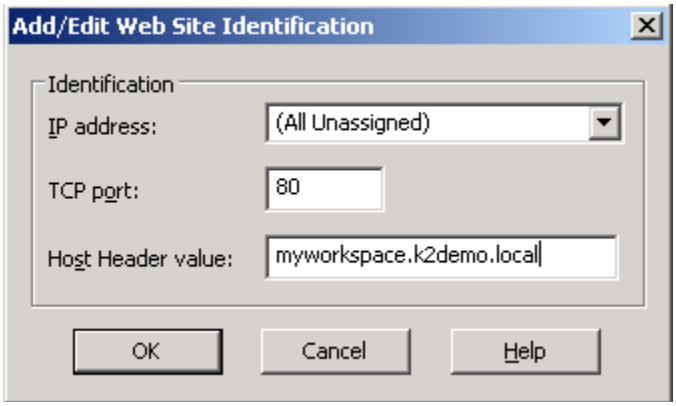
HTTP://[WebserverName]:[TcpPort#]/Workspace/Navigation/Navigation.aspx

The third option is to use host headers. Using this method means there is no need to refer to the actual IIS server name and TCP port number in the URL, for example:

HTTP://[host header]/Workspace/Navigation/Navigation.aspx

To use Host Header for the Web Site for K2 Workspace, follow these steps:

1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. Right-click on the Web site and then click **Properties**.
3. On the **Web Site** tab, click the **Advanced** button, and then click **Add**
4. Enter a TCP port (usually 80) and a value for Host Header, as shown in Figure 5.



[FIGURE 5: CONFIGURING A HOST HEADER]

5. Click OK and then apply the changes
6. Start (or restart) the Web site
7. Register the host header name with the appropriate name resolution (WINS or DNS) system.

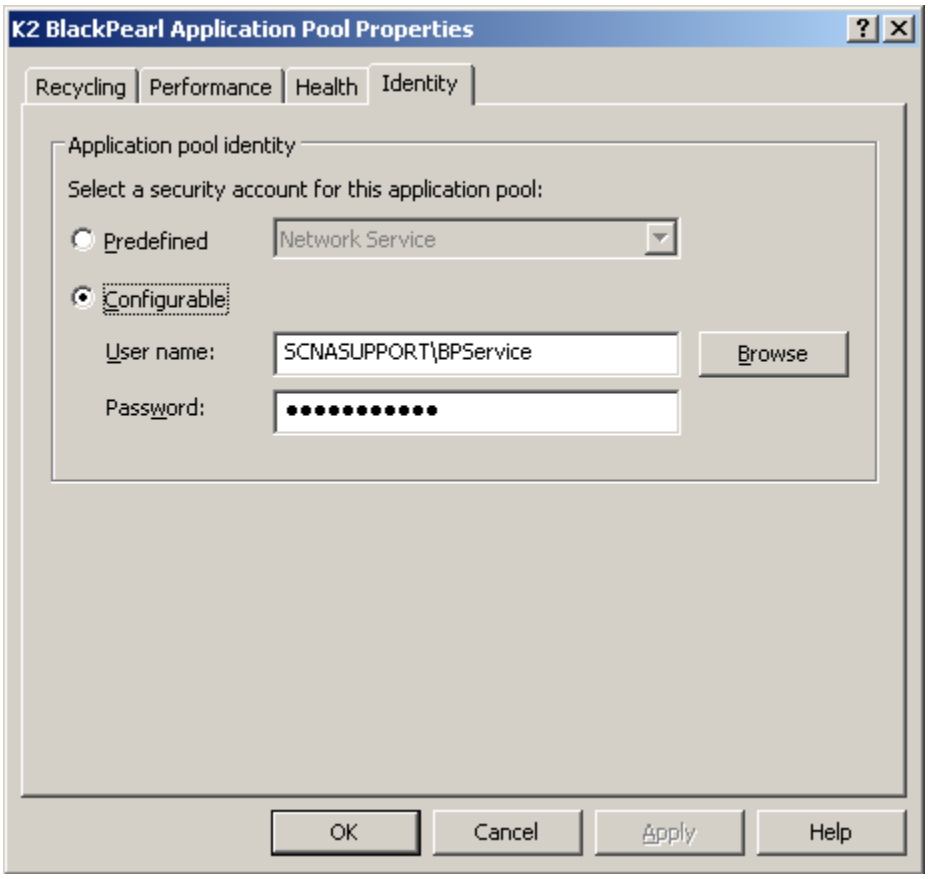
If the computer is on an intranet (a private LAN that uses Internet technology), register it with the intranet's name resolution system, such as the Windows Internet Name Service (WINS). If the computer is on the Internet, register the host header name with the Domain Name System (DNS).

Note: Contact the Domain Administrator for registration of the Host Header name.

APPLICATION POOL AND IDENTITY ACCOUNT

To identify the application pool identity account for K2 blackpearl, follow these steps:

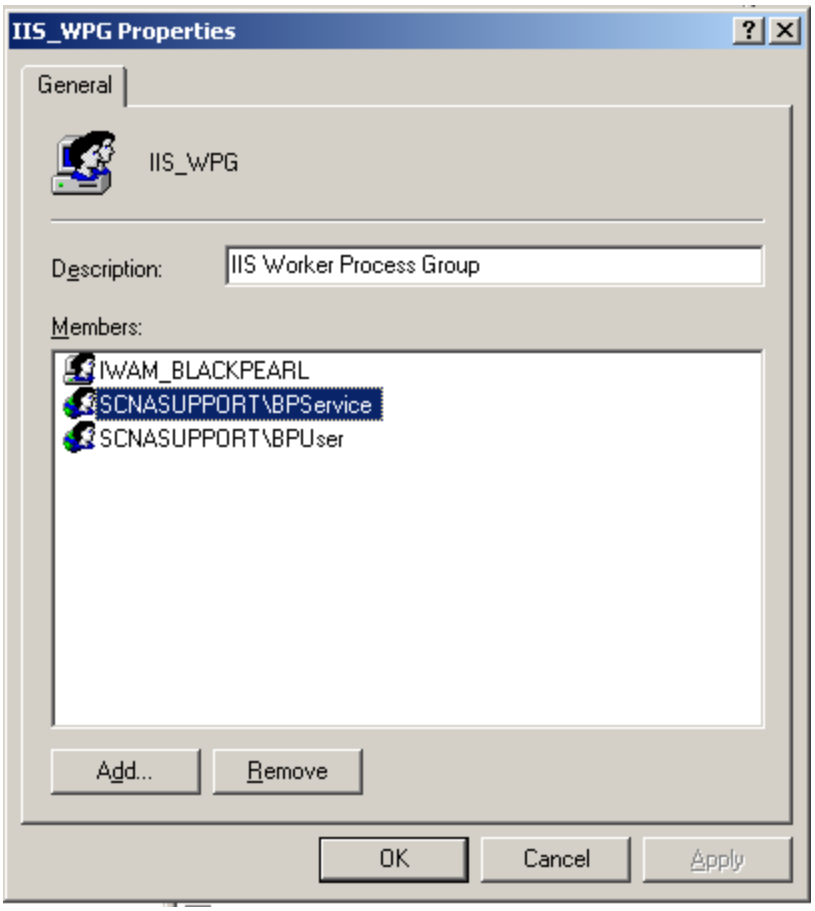
1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager
2. Expand Application Pools, right-click **K2 BlackPearl Application Pool** and select **Properties**
3. Click the **Identity** tab as shown in Figure 6.



[FIGURE 6: DETERMINING THE APPLICATION POOL ACCOUNT]

To add the application pool identity account to IIS_WPG group on IIS server, follow these steps:

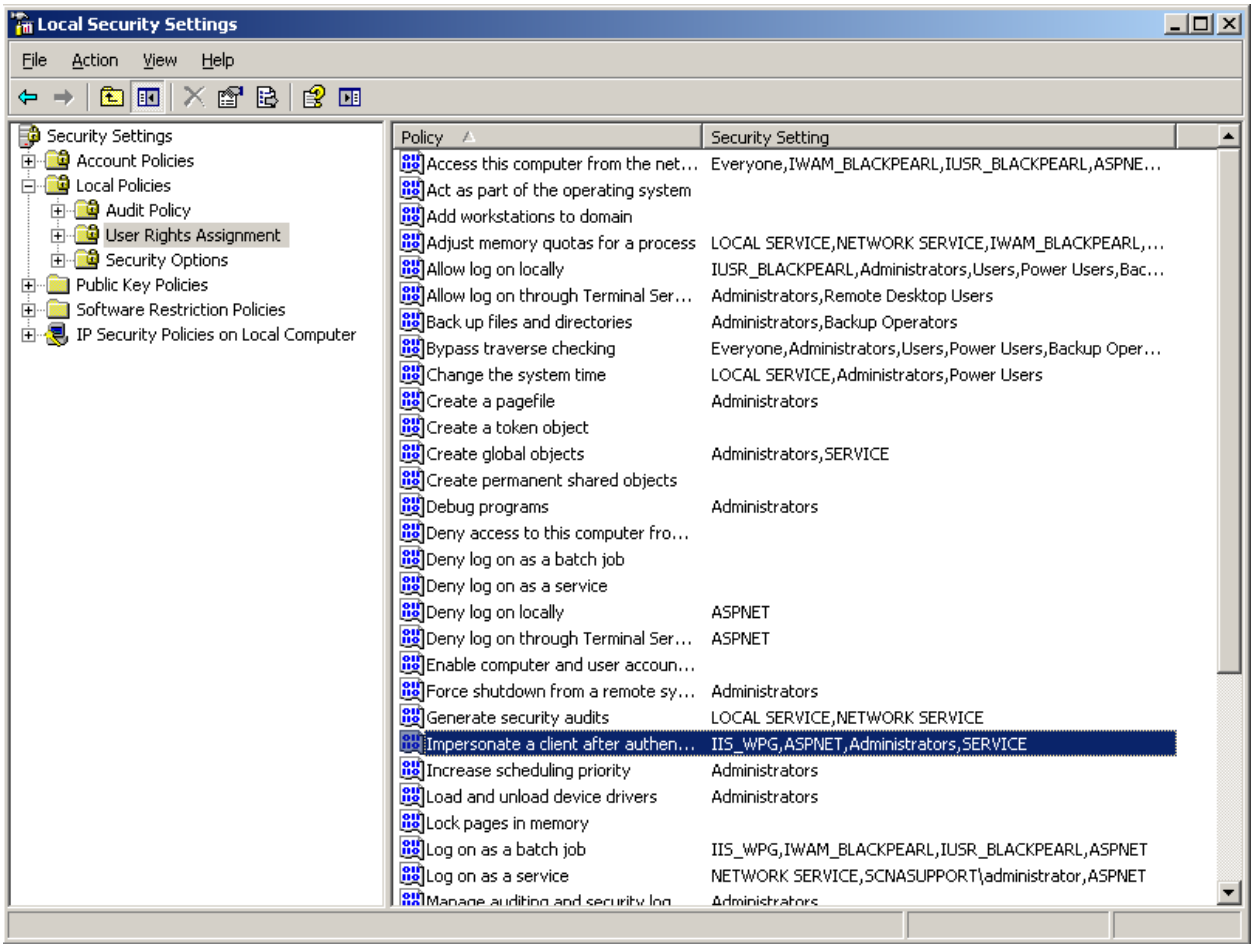
1. Click Start > Administrative Tools > Computer Management > Local Users and Groups > Groups
2. Right-click **IIS_WPG** and select **Properties**
3. Add the identity account to the local IIS_WPG group as shown in Figure 7.



[FIGURE 7: ADDING THE SERVICE ACCOUNT TO THE IIS_WPG GROUP]

To assign the **Impersonate a client after authentication** right to the IIS_WPG group, follow these steps:

1. Click Start > Administrative Tools > Local Security Policy > User Rights Assignment.
2. Right-click **Impersonate a client after authentication** (as shown in Figure 8) and select **Properties**
3. Add the IIS_WPG group
4. Click **OK**

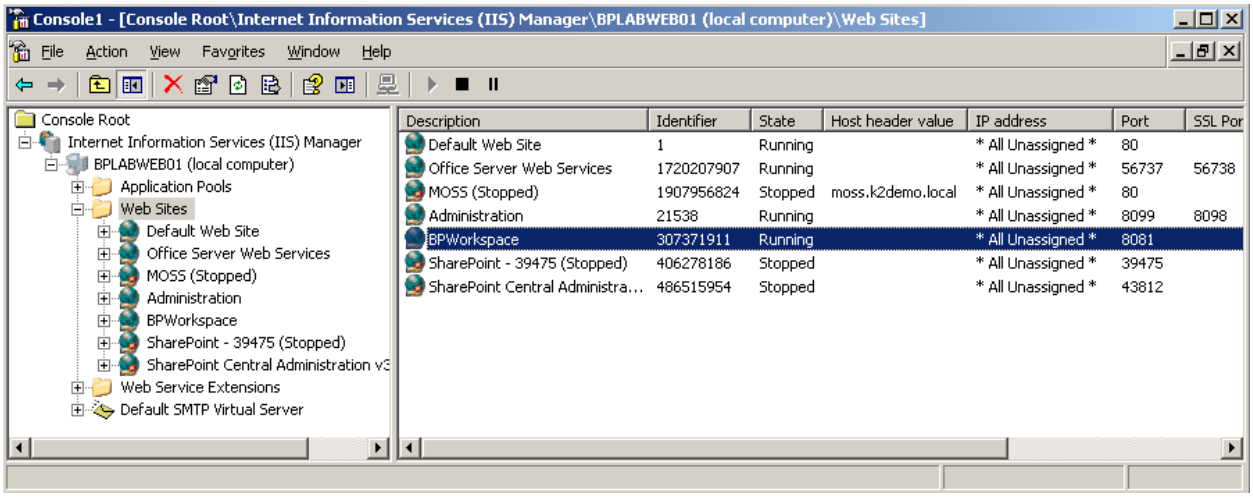


[FIGURE 8: FINDING THE IMPERSONATION RIGHT IN THE POLICY SETTINGS]

CONFIGURE IIS METABASE

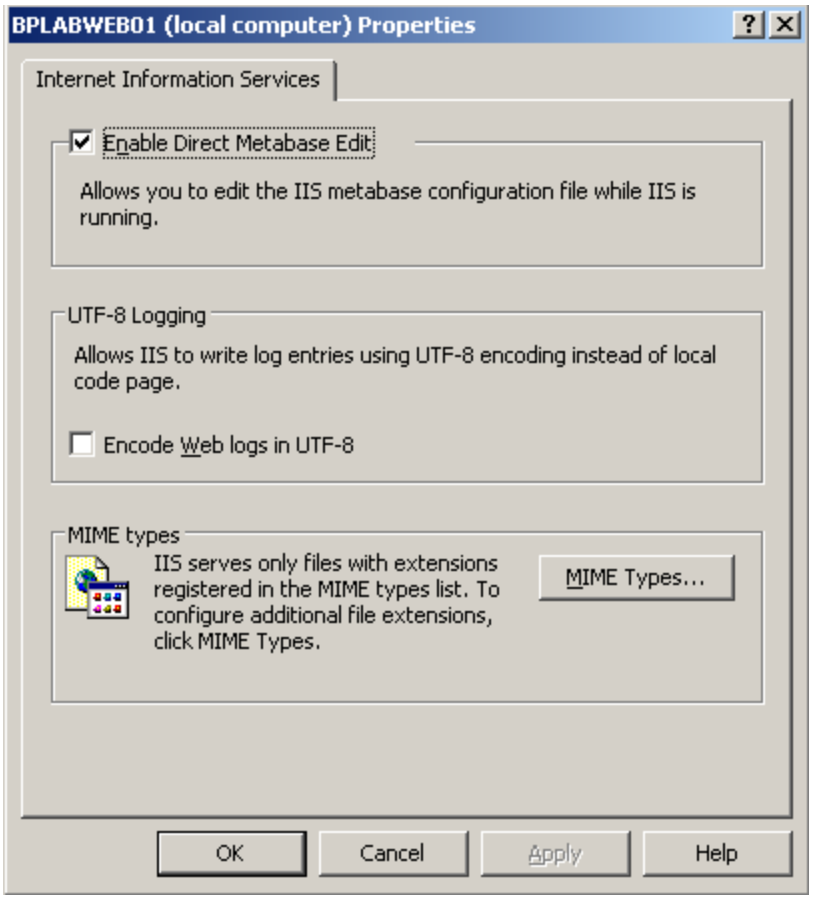
Is it necessary to alter the method in which the web site is authenticating users by updating the IIS metabase. To do this, find the Web site identifier and allow IIS metabase updates on the server by following these steps

1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager.
2. Click on Web Site in the left hand pane and find the identifier of Website for K2 blackpearl Workspace in the right hand pane. In the example in Figure 9 the identifier is the second column. Make a note of this number



[FIGURE 9: FINDING THE IIS WEB SITE IDENTIFIER]

3. Right-click on the server name in IIS manager and select **Properties**
4. Mark the **Enable Direct Metabase Edit** checkbox as shown in Figure 10

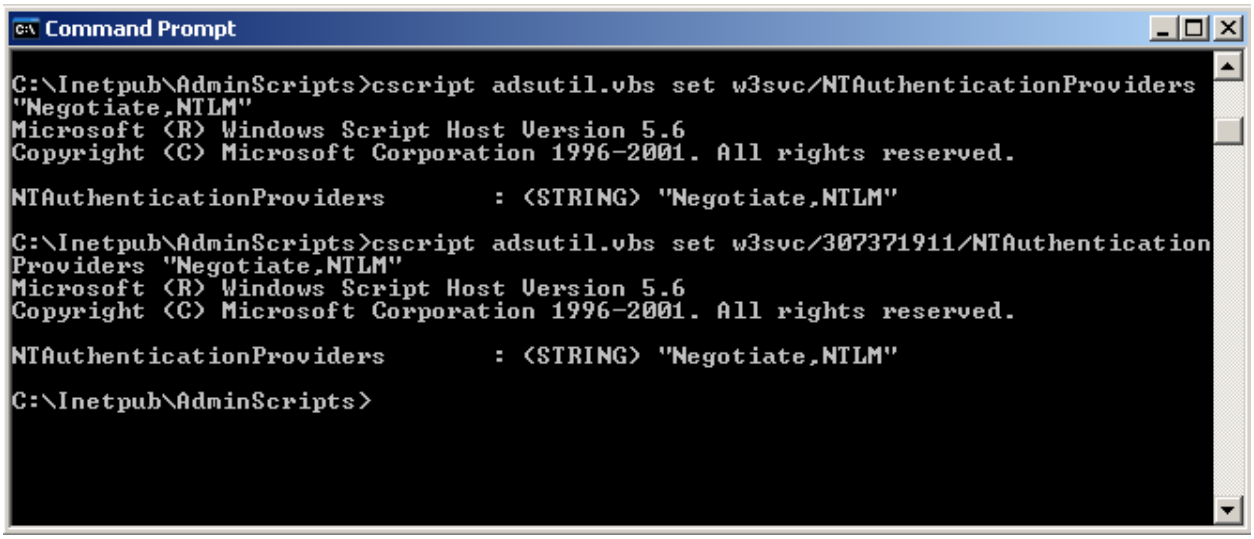


[FIGURE 10: ALLOW IIS METABASE UPDATES]

5. Click **OK**
6. Open a command line window and change directory to C:\Inetpub\Adminscripts.
7. Type the following commands and press ENTER after each. The command window will look similar to Figure 11.

> cscript adsutil.vbs set w3svc/NTAuthenticationProviders "Negotiate,NTLM"
> cscript adsutil.vbs set w3svc/[IISSiteID]/NTAuthenticationProviders "Negotiate,NTLM"

Where [IISSiteID] is the identifier of the web site noted above



[FIGURE 11: SETTING THE AUTHENTICATION PROTOCOL ORDER FOR THE SERVER AND THE SITE]

Important: When entering these commands be careful to use double quotes and not two single quotes. If the resulting screen looks like ""Negotiate,NTLM"" instead of "Negotiate, NTLM" retype the command line using double quotes.

8. Click Start > Run, type "iisreset" and press ENTER. The IIS Reset will proceed automatically and inform the user when it is complete.

FARM OPTIONS FOR K2 WORKSPACE

Similar to a K2 Server Farm, K2 Workspace Farm is Internet Information Server (IIS) configured in a Web cluster with multiple Web servers.

All of the associated Web servers must have K2 blackpearl Workspace installed and to be configured to use the same application pool identity account. HTTP SPNs must be created for the K2 Workspace Farm name under the application pool identity account.

CONFIGURE IIS SERVER FOR SQL SERVER REPORTING SERVICES

When integrating K2 blackpearl with SQL Server Reporting Services (SSRS) in a distributed environment, the SSRS web site must be configured to support Kerberos authentication.

SRSS APPLICATION POOL AND IDENTITY ACCOUNT

The application pool account used for the SSRS web site must be trusted for delegation and the appropriate Service Principal Names must be configured for this account as described in the previous sections.

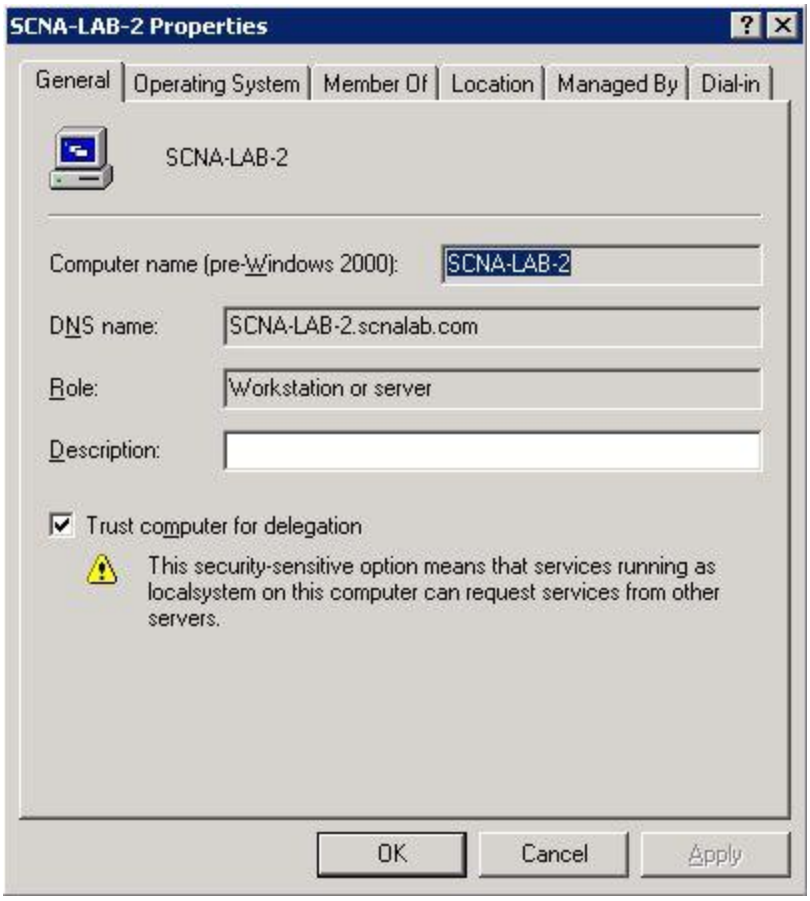
Note: If the Network Service account is being used as the identity for the SSRS web site application pool, it is not necessary to set Service Principal Names, nor does the Network Service account need to be trusted for delegation. However, the computer itself must be trusted for delegation in Active Directory.

To identify the application pool identity account used for the SSRS web site, follow these steps:

1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager
2. Expand **Application Pools**, right-click the application pool used by the SSRS web site and select **Properties**
3. Click the **Identity** tab and make a note of the account

To trust the computer for delegation in Active Directory, follow these steps:

1. Click Start > Administrative Tools > Active Directory Users and Computers
2. Expand the node for the domain where the SSRS computer resides
3. Click the **Computers** container
4. Right-click on the computer that hosts the SSRS web site, and select **Properties**
5. On the **General** tab, make sure the **Trust computer for delegation** checkbox is checked as shown in Figure 12.



[FIGURE 12: TRUSTING THE SRSS COMPUTER FOR DELEGATION]

To add the application pool identity account to the IIS_WPG group on the IIS server, follow these steps:

1. Click Start > Administrative Tools > Computer Management > Local Users and Groups > Groups
2. Right-click **IIS_WPG** and select **Properties**
3. Add the SRSS identity account to the local IIS_WPG group if not already

To assign Impersonate a client after authentication right to IIS_WPG group, follow these steps:

4. Click Start > Administrative Tools > Local Security Policy > User Rights Assignment.
5. Right-click **Impersonate a client after authentication** (as shown in Figure 8) and select **Properties**
6. Add the IIS_WPG group
7. Click **OK**

CONFIGURE THE IIS METABASE

The NTAuthenticationProviders property in the IIS metabase for the SSRS web site must be configured to support Kerberos authentication.

1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager
2. Click on Web Site in left pane and make a note of the identifier of Web site for SQL Server Reporting Services in the right pane
3. Right-click on the server name in IIS manager, and select **Properties**.
4. Mark the **Enable Direct Metabase Edit** checkbox as shown in Figure 10
5. Open a command line window and change directory to C:\Inetpub\Adminscripts.
6. Type the following commands and press ENTER after each. The command window will look similar to Figure 11.

```
> cscript adsutil.vbs set w3svc/NTAuthenticationProviders "Negotiate,NTLM"
> cscript adsutil.vbs set w3svc/[IISSiteID]/NTAuthenticationProviders "Negotiate,NTLM"
```

Where [IISSiteID] is the identifier of the SRSS web site noted above

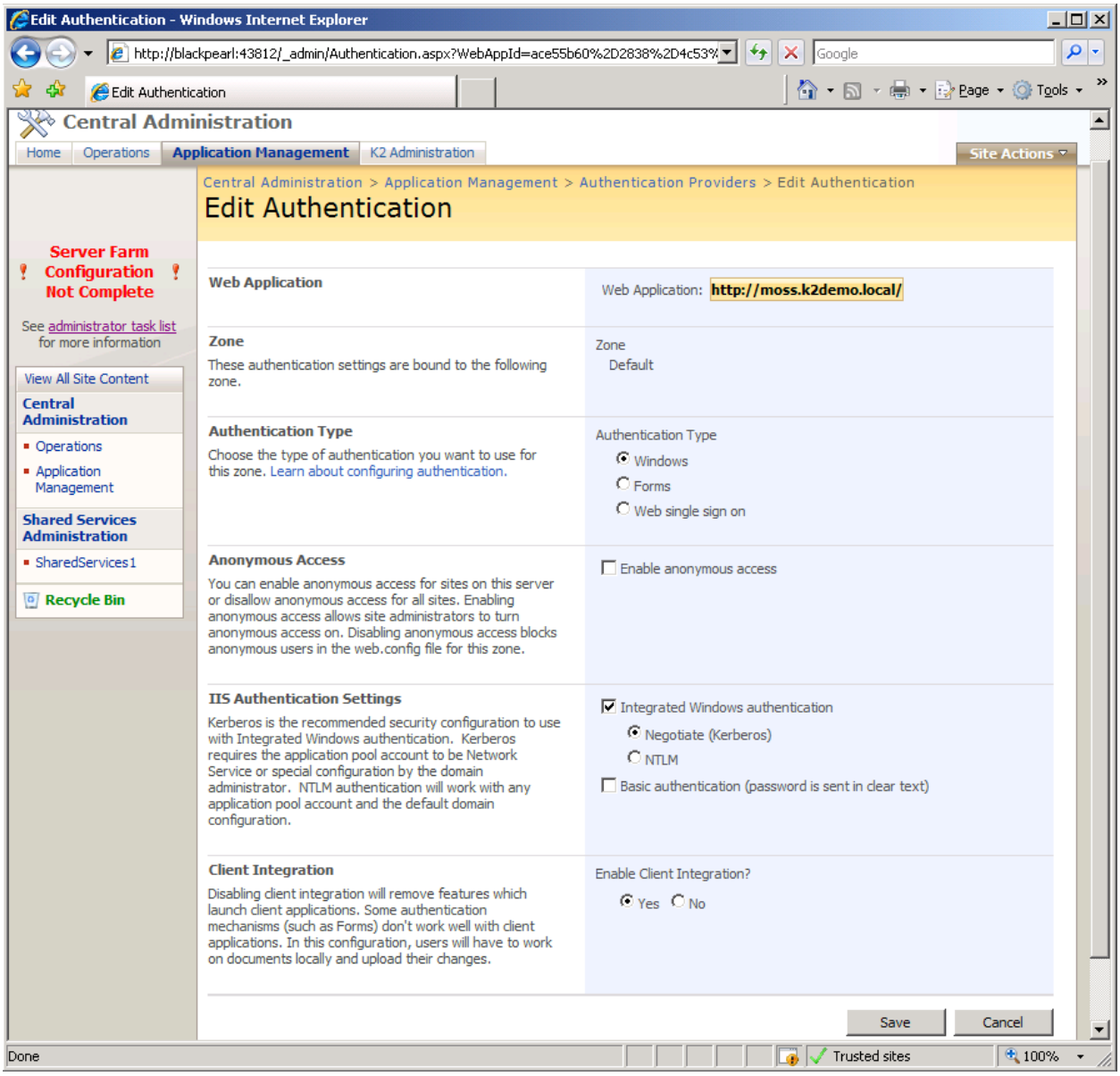
CONFIGURING SHAREPOINT SERVER TO USE KERBEROS AUTHENTICATION

Integration with MOSS or WSS 3.0 is achieved by installing K2 blackpearl MOSS Components or WSS Component, respectively, on a SharePoint Server. SharePoint Server uses NTLM authentication by default but Kerberos is also supported.

Note: Only a SharePoint Administrator can configure IIS authentication settings.

To switch SharePoint from NTLM to Kerberos authentication, follow these steps:

1. Click Start > Administrative Tools > SharePoint 3.0 Central Administration
2. Click **Application Management** tab, and then click **Authentication Providers**
3. Select the **Web Application** from the list
4. Choose a **Zone**
5. On **Edit Authentication** page for IIS Authentication Settings > Integrated Windows authentication, click **Negotiate (Kerberos)** as shown in Figure 13
6. Click **Save**



[FIGURE 13: CONFIGURING SHAREPOINT TO USE KERBEROS]

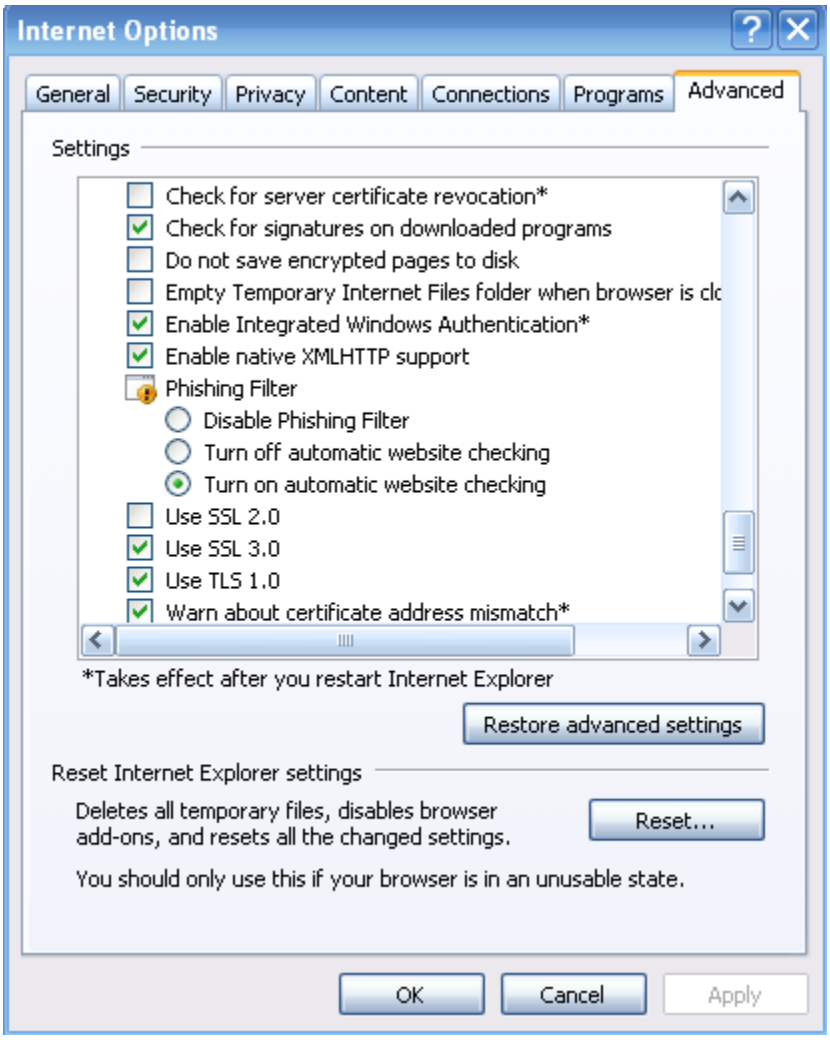
Note: More configuration may be required by SharePoint to use Kerberos. See the blog **Configuring Kerberos for SharePoint 2007: Part 1 - Base Configuration for SharePoint** (http://blogs.msdn.com/martinkearn/archive/2007/04/23/configuring-kerberos-for-sharepoint-2007-part-1-base-configuration-for-sharepoint.aspx) for more information.

CONFIGURING INTERNET EXPLORER (IE)

For an Internet Explorer client to browse to either K2 Workspace or a SharePoint page containing K2 blackpearl components (such as MOSS components or WSS components), IE client settings must be configured as follows:

ENABLE INTEGRATED AUTHENTICATION:

1. In IE, click Tools > Internet Options
2. Select **Advanced** tab, in the **Security** section, mark the **Enable Windows integrated authentication** option as shown in Figure 14
3. Click **OK**

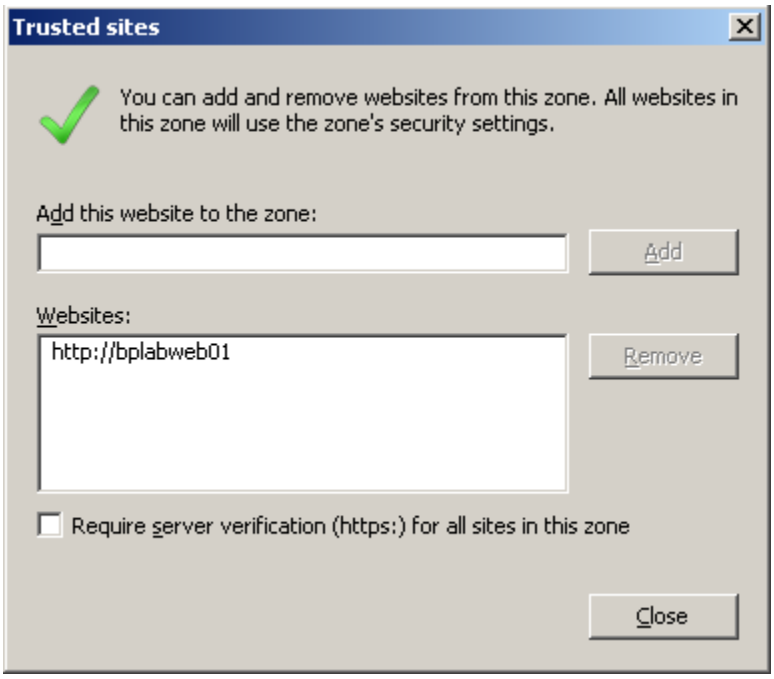


[FIGURE 14: IE INTEGRATED WINDOWS AUTHENTICATION OPTION]

ADD THE WORKSPACE SITE TO THE LIST OF TRUSTED SITES:

1. Click Tools > Internet Options

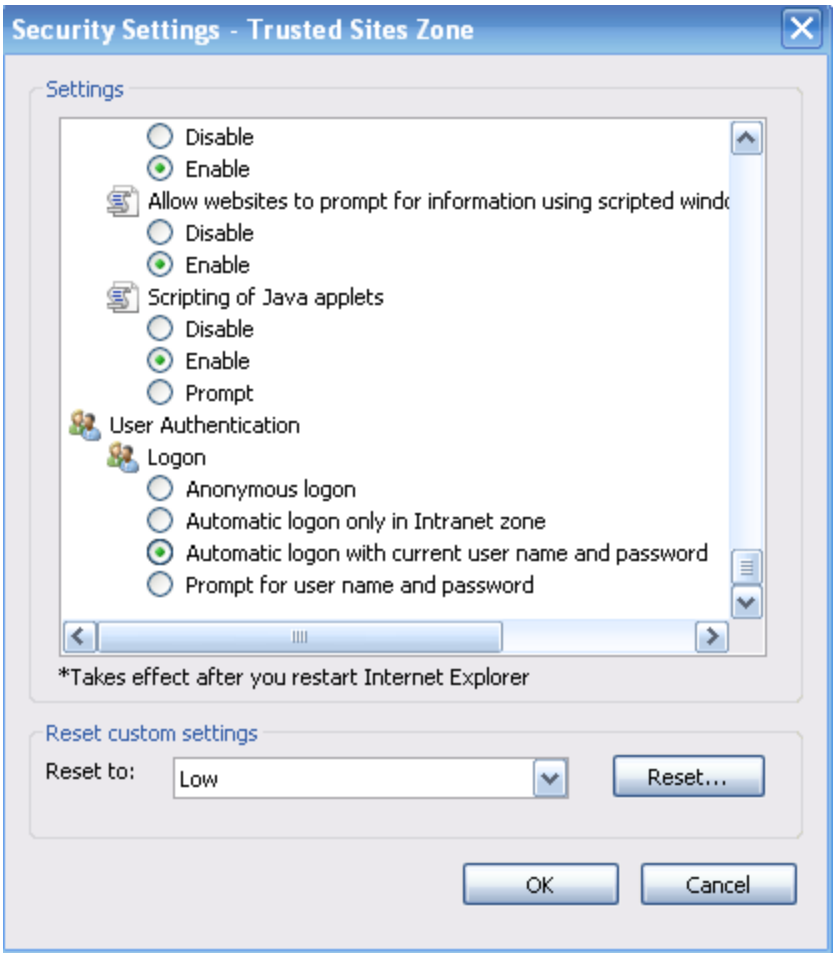
2. On the **Security** tab click the **Trusted Sites** zone
3. Click the Sites button
4. Uncheck **Require server verification (https:) for all sites in this zone**
5. Type the Workspace URL into the text box and click **Add.** The dialog should resemble Figure 15.
6. Click **Close**



[FIGURE 15: CONFIGURING A TRUSTED SITE]

CONFIGURE SECURITY SETTINGS:

1. Click Tools > Internet Options
2. On the **Security** tab click the **Trusted Sites** zone
3. Click **Custom level**
4. Select **Low** from the **Reset custom settings** drop down list as shown in Figure 16
5. Click **Reset**
6. Scroll to the **User Authentication** > **Logon** section and select **Automatic logon with current user name and password**
7. Click **OK**



[FIGURE 16: CONFIGURING SECURITY SETTINGS FOR TRUSTED SITES]

TESTING KERBEROS CONFIGURATION

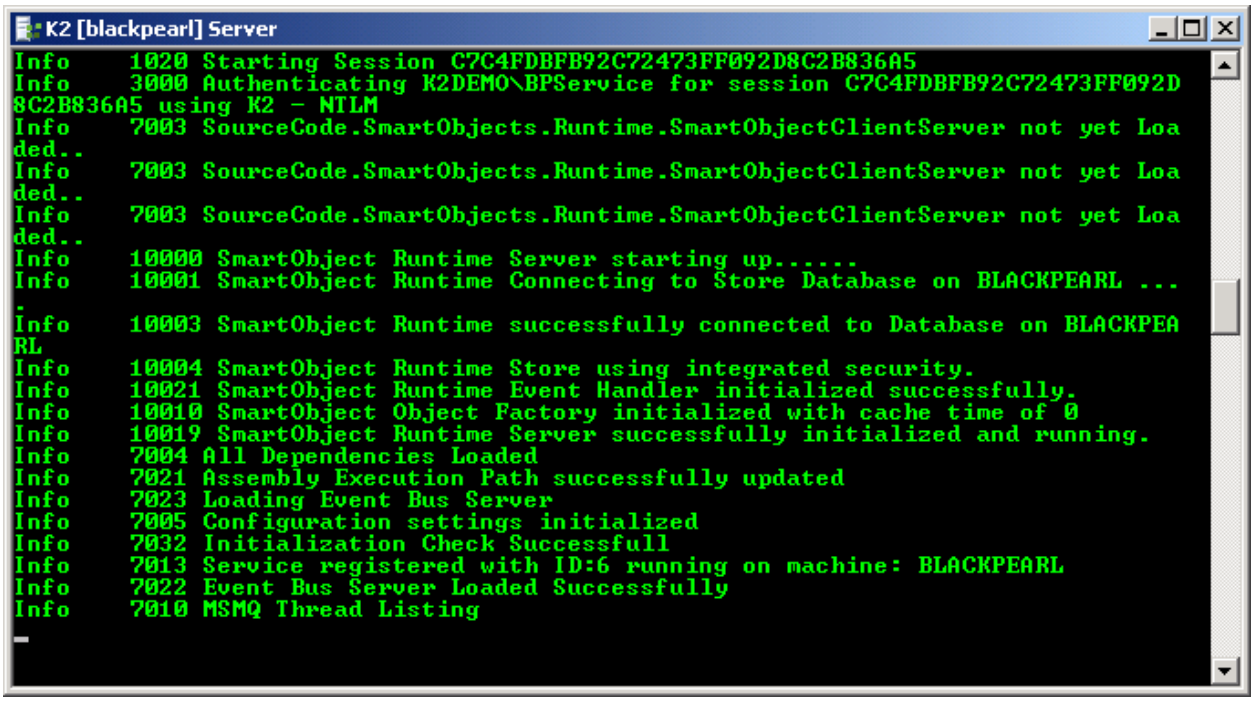
For debugging purpose, running K2 Host Server in console mode can be an effective way to verify if the K2 Host Server has started up successfully, or if it failed to do so. Console mode also reports the reason for the startup failure thus making trouble shooting simpler.

To run K2 Host Server in console mode, follow these steps:

1. Click Start > Administrative Tools > Services
2. Right click **K2 [blackpearl] Server** and select **Stop**
3. Click Start > All Programs > K2 [blackpearl]
4. Right click K2 [blackpearl] Server and select **Run as**
5. Mark **The following user** and enter the username and password for the K2 Service account

6. Click **OK**

The K2 blackpearl Server in console mode should resemble Figure 17.



[FIGURE 17: RUNNING K2 [BLACKPEARL] SERVER IN CONSOLE MODE]

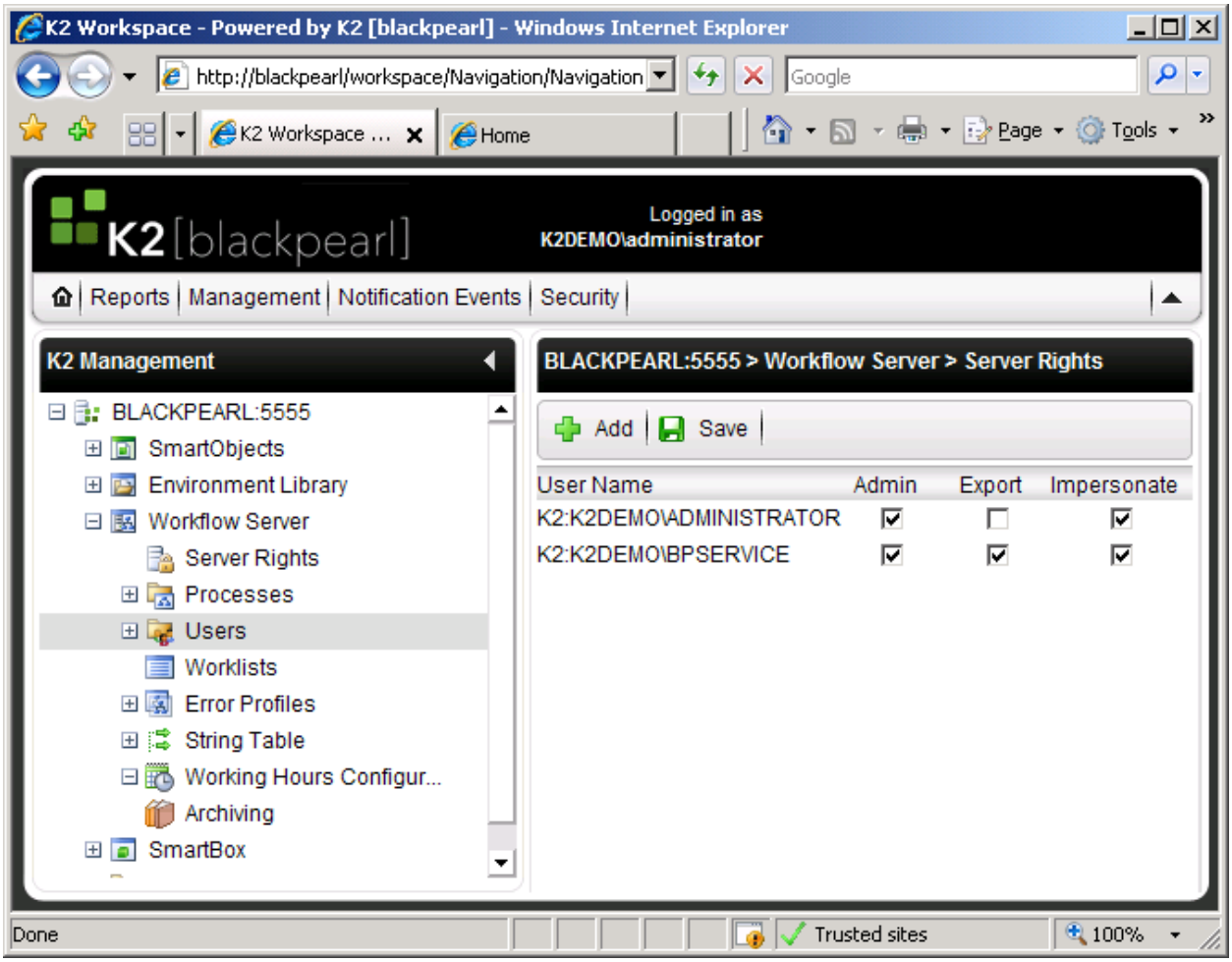
OPEN THE MANAGEMENT CONSOLE

Having verified that K2 blackpearl Server can or has started successfully, the next step is to browse to K2 Workspace from a remote client machine and open Management Console. If the K2 blackpearl Server and K2 Workspace have been installed and configured properly, the logon user's credentials will be authenticated using either NTLM or Kerberos depending on how it was configured and the type of installation.

To browse to K2 Workspace, follow these steps:

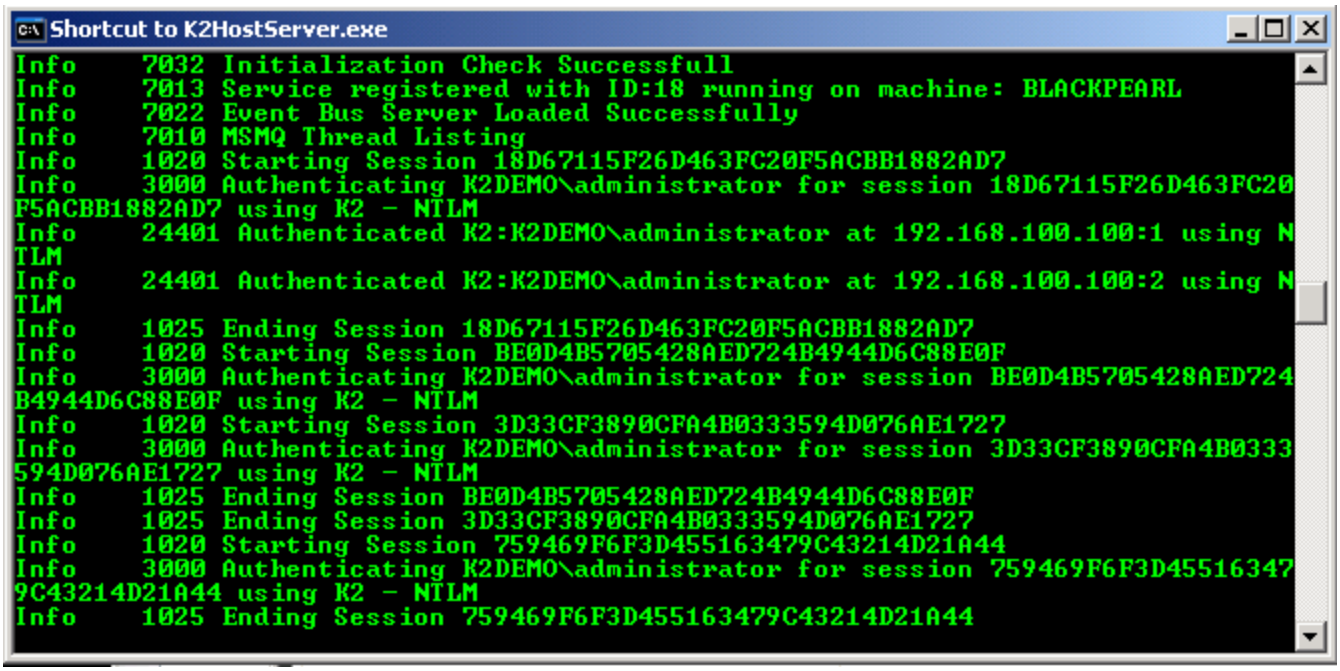
1. Click Start > All Programs > K2 [blackpearl] > K2 [blackpearl] Workspace
2. Click Management > Management Console
3. Expand **Workflow Server**, and click **Server Rights**

The K2 blackpearl Workspace should resemble Figure 18



[FIGURE 18: INSPECTING THE SERVER RIGHTS IN MANAGEMENT CONSOLE]

If authentication with the Workspace web site fails, you may see multiple prompts for user credentials and ultimately an Access Denied error. Or, if fallback to NTLM is successful, launching the K2 blackpearl Server in console mode will show that NTLM configuration is being used by the server, as shown in Figure 19.



[FIGURE 19: K2 BLACKPEARL SERVER RUNNING IN CONSOLE MODE SHOWING NTLM IS USED FOR AUTHENTICATION]

OTHER RESOURCES

For more information on Kerberos authentication, see the following resources.

Basic Overview of Kerberos User Authentication Protocol in Windows 2000 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;217098)

Kerberos Authentication Tools and Settings (http://technet2.microsoft.com/windowsserver/en/library/b36b8071-3cc5-46fa-be13-280aa43f2fd21033.mspx?mfr=true)

Troubleshooting Kerberos Delegation in Windows 2000 and Windows Server 2003 (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerbdel.mspx)

How to configure a Windows SharePoint Services virtual server to use Kerberos authentication and how to switch from Kerberos authentication back to NTLM authentication (http://support.microsoft.com/default.aspx?scid=kb;en-us;832769)

How to enable Kerberos event logging (http://support.microsoft.com/kb/q262177)

Security Model (http://msdn2.microsoft.com/en-us/library/aa292471.aspx)

APPENDIX

APPENDIX A: TROUBLESHOOTING CHECKLIST ON K2 DATABASES

- Is SQL Server 2005 healthy?
- Can you load the SQL Server Management Console?
- Does the account defined for the K2 Service (or used for loading K2 in Console mode) have the necessary database permissions?

APPENDIX B: TROUBLESHOOTING CHECKLIST ON IIS/WORKSPACE/WEB APPLICATION HEALTH

APPPOOL CONFIGURATIONS

- Confirm Identity User account and Password
- Review AppPool consistency (compare/contrast AppPools used across all blackpearl resources, MOSS resources, and web applications)
- Check Permissions of the AppPool identity account
- Confirm web application configurations are set properly

WEB SITES

- Review Ports (check for conflicts, check Ports are accurate)
- Check the Fully Qualified Domain Name (FQDN) being used/defined.
- Check the Host Header being used/defined.
- Determine if a web site can be accessed via different methods (try machine name, FQDN, IP address, or host header)
- Can you load a basic HTML page from the web site? If not, check network policies and perform basic IIS troubleshooting.

CLIENT BROWSER SETTINGS

- What are the differences if a browser loaded from the local IIS/Workspace server or from a remote client machine?
- If errors are displayed, identify where the error is being generated from:
  - Browser? Check browser settings (Trusted Sites, Login settings, Security settings, etc.)
  - IIS? Check AppPool settings, folder permissions, group memberships, and authentication methods. Review log file contents.
  - K2? What is the K2 Console showing? What action is generating the error/conditions?
  - If K2 is not showing any requests from IIS, then the issue probably lies between the client browser and IIS since IIS is blocking the request made by the client.
  - SQL? Check AppPool permissions to the database. Check authentication method (WIA or SQL) and database permissions/ownership settings.

You may need to disable custom errors to get more information on the error.

APPENDIX C: TROUBLESHOOTING CHECKLIST ON NETWORK PERMISSIONS AND SECURITY

ACCOUNT PERMISSIONS

- Confirm K2 Server Service account permissions and membership
- Check IIS AppPool permissions and membership
- Review SQL Server account database permissions/ownership ('dbo')
- Check MOSS account permissions and memberships
- Check User permissions to K2 processes, MOSS sites, and MOSS permissions

KERBEROS AND AUTHENTICATION

- HTTP and Machine SPN's set for proper accounts
- Check for duplicate SPNs
- Confirm there is a pair of SPNs for each account (HTTP and Machine).

APPENDIX D: TROUBLESHOOTING CHECKLIST ON SQL SERVER REPORTING SERVICES (SSRS)

Note: SSRS troubleshooting is very similar to Workspace troubleshooting as they are both web applications.

- Can the SQL Server Management Console load? If SSRS is not healthy, then K2 will likely be impacted.
- Differentiate whether the issue lies within K2 or SSRS or between K2 and SSRS:
  - Can K2 'out of the box' ("OOTB") reports load properly via Workspace? If so, basic K2 reporting is healthy.
  - Can K2 Reports be imported from K2 into SSRS and ran from SSRS? If not, the Workspace AppPool may not be set properly.

APPENDIX E: TROUBLESHOOTING CHECKLIST ON CHECK BASIC PREREQUISITES

FRAMEWORK VERSIONS

- Check for newer (unsupported) Frameworks
- Check for missing Frameworks

CHECK OPERATING SYSTEM VERSIONING

- Check OS Service Packs installed. Make sure existing SPs are supported.
- If "nothing changed", consider when the last Windows Update was run (are they automated?). Can the Updates be uninstalled?

CHECK SERVER PREREQUISITES

- Is the Distributed Transaction Coordinator (DTC) service installed and configured?
- Is Message Queuing (MSMQ) installed?