K2 Installation and Configuration - checklist and guide

October 25

DOCUMENT VERSION | 2.0

Table of Contents

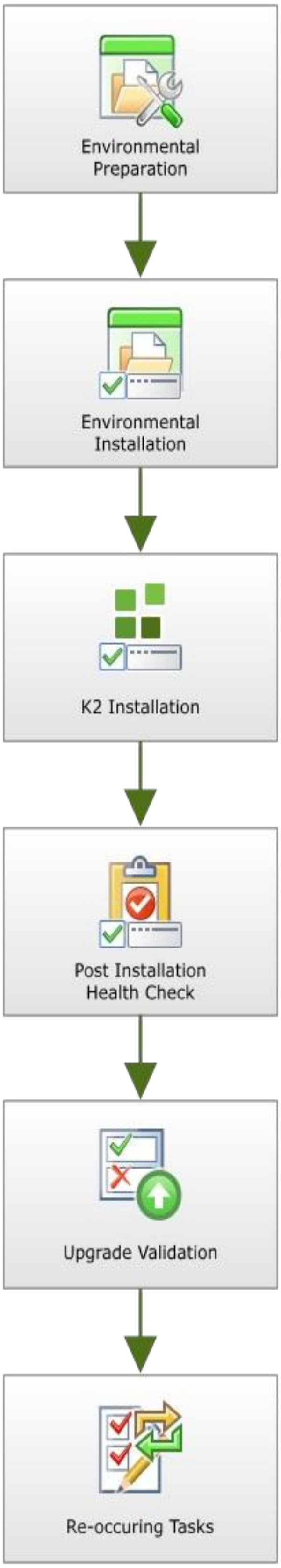
1. Administrators Guide

Introduction

This guide aims to assist K2 Administrators in preparing and installing the environment for a K2 installation, validating the installation on completion, upgrading the installation, and listing a number of routine common admin tasks to ensure a healthy system.

A number of worksheets are provided for the Administrator to enter information describing the environment and system (account details etc.), these worksheets should be filed for later use.

This document will be updated from time to time with new information and common admin tasks.


Environmental Preparation
Environmental Installation
K2 Installation
Post Installation Health Check
Upgrade Validation
Re-occuring Tasks

1. **Environment Preparation**

◊ **Worksheets**

- Contact people
- Active Directory
- Server Details
- Service Accounts
- DNS Host Records
- Kerberos
- SharePoint Configuration guide

◊ Reference

- Supported topologies

2. **Environment Installation**

◊ Environment topology
◊ K2 Technology Prerequisites
◊ DNS
◊ Accounts
◊ Authentication
◊ Installation parameters
◊ IIS Configuration

- K2 Workspace and Web Services
- Web site summary

◊ SQL Reporting Services
◊ Setting NT Authentication providers

3. **K2 Installation** (covered in the Getting Started Guide online)

◊ Standalone install
◊ Distributed install
◊ Client install

4. **K2 Post Installation health check**

5. **Reoccurring administrative tasks**

◊ Clear the SmartActions mailbox

6. **Appendix and troubleshooting**

◊ IIS 7 Kernel Mode Authentication
◊ Tighten K2 Reporting structure for shared SSRS service
◊ Set K2 host server to use private queues
◊ Disable Generate publisher information
◊ Disable loopback checks
◊ Kerberos tweaks

2. K2 Environment Preparation and Worksheets

This topic is a summary of system infrastructure, for use before installation.

Introduction

K2 blackpearl integrates with several Microsoft technologies to provide a rich and flexible environment for building dynamic business process applications. This document is intended to facilitate the K2 installation process by consolidating the most important elements of a K2 installation such as contact people, server names and service accounts into a single document. This document is not intended as an educational source for K2 installation and product functionality, the documents listed below should be seen for that:

Document	K2 blackpearl	K2 blackpoint
Compatibility Matrix	Click here	Click here
Getting Started Guide	Click here	Click here
Developer Reference	Click here	Click here
Product Download	Click here	Click here

Contact People

A K2 installation incorporates many disparate components and as such it is critically important that the proper people be either directly involved in the installation process or be made available when needed.

Provide the contact details for each of the roles below.

Note, it is very common for one person to own more than one role.

Role	Phase	Contact Name	Contact Details
K2 Administrator	Pre- Install, Install, Post-Install		Phone: Mobile: Email:
Domain Administrator	Pre- Install Post- Install		Phone: Mobile: Email:
IIS Administrator	Pre- Install		Phone: Mobile: Email:

DNS Administrator	Pre- Install		Phone: Mobile: Email:
SharePoint Farm Administrator (if applicable)	Pre- Install Post- Install		Phone: Mobile: Email:
SQL Server Administrator	Pre- Install Post- Install		Phone: Mobile: Email:
Developer	Post- Install		Phone: Mobile: Email:

Server Topology

K2 can be configured within many different types of server environments, from all-in-one self-contained servers to highly distributed and highly available farms.

In order to properly plan this upcoming installation, review the typical configurations listed in the Installation and Configuration > Planning Guide > Deployment Scenarios section of the Getting Started Guide and identify which one suites your environment. The worksheet below can be used to record planned installation type.

You may also wish to draw up a diagram of your planned environment for clarity. An example is provided in the Getting Started Guide at the path mentioned above.

Installation Type	Details	Selection & Comments

Active Directory

By default, K2 leverages Active Directory (AD) for authentication and authorization of users. It is important to understand and plan accordingly around the AD domains that are to be incorporated.

Record the Active Directory information in the worksheet below.

Request	Details
List all domains that K2 will need to authenticate against:	
Note the NetBIOS name and FQDN of each domain and which ones are children of others (if more than one domain):	
If more than one domain is to be leveraged, describe what trusts are in places as well as internal policies around AD trusts:	

Server Details

Record the details of the components of the planned K2 installation.

Functional Role	Version & Service Pack	Server Name(s)	Operating System	32 bit / 64 bit	Comments
K2 Host Server/K2 Server Farm					
K2 Workspace Server					
SharePoint Web Front End(s)					
SharePoint Central Administration host					
SharePoint databases					
Load Balancer/Front-End Proxy					
SQL Server Database					
SQL Server Reporting Server					

Firewall and Ports

The following is a list of ports that need to be opened before installation and at runtime:

- Installation:
  - K2Server, SharePoint Server or any server we install components on -> SQL Server: 1433
- Runtime:
  - K2Server -> SQL: 1433
  - K2Server -> SMTP: 25 if default
  - K2Server -> Exchange WebServices
  - SharePoint, any server that will open connection to K2 -> K2Server: 5555, 5252
  - Users -> Workspace port
  - MSDTC ports between K2 and SQL (in cases where MSMTC is clustered, the following information resources are invaluable:

http://www.lewisroberts.com/2009/08/16/msdtc-through-a-firewall-to-an-sql-cluster-with-rpc/

http://support.microsoft.com/kb/306843)

For more information on K2 and Firewalls, please see the KB article KB001318 here: http://help.k2.com/en/KB001318.aspx

Service Accounts

As K2 incorporates a number of disparate technologies, service accounts play a significant role. As such there should be proper planning around this area. For more information around this please refer to K2 blackpearl or K2 blackpoint product documentation on the topic.

Record the details of the service accounts to be used in the planned K2 installation.

Account Type	Account Name	Account Password *(if appropriate to document)*
K2 Server Service Account		
K2 Administration Account		
Workspace Server Application pool Account		
Reporting Services Application pool account		
SharePoint Application pool account		

DNS Host Records

The creation of static DNS HOST (A) records for the K2 Server and K2 Workspace server(s) is advised to allow for simpler failover and horizontal scaling (K2 Server Farm) should that be required. For more information on this please see the documentation on this topic (K2 blackpearl or K2 blackpoint).

Naming convention examples: workspace.contoso.com, ws.contoso.com, k2workspace.contoso.com.

If DNS records have been created, record them here. If more servers are in the architecture, please add their details to the list below.

Server Role	Server Name	HOST (A) records
K2 Host Server/K2 Server Farm		
K2 Workspace		
SharePoint Web Front End		
SQL Reporting Services instance		

Kerberos Preparation

If you have opted to distribute K2 components in a fashion that has pieces of the architecture running on different servers Kerberos will need to be configured in order to delegate credentials, unless K2 Pass Through Authentication (K2PTA) is enabled. To understand the difference between Kerberos and PTA and for information on whether Kerberos is required, see the KB article KB001226: Introduction to K2 Pass-Through Authentication (http://help.k2.com/en/kb001226.aspx) and the K2 Pass-through Authentication whitepaper: http://help.k2.com/files/3533

For more information on Kerberos, please review our documentation:

- K2 Deployment Considerations
  - ◊ K2 blackpearl
  - ◊ K2 blackpoint
- Security and Kerberos White Paper

If Kerberos preparation has been done, record the information here.

Service/ Component	DNS Entry FQDN	Service Account	SPNs that have been Created *(NOTE: examples provide, please replace with actual or state that none have been set)*
K2 Server			K2Server/k2server:5252 K2Server/k2server.domain.com:5252 K2HostServer/k2server:5555 K2HostServer/k2server.domain.com:5555
K2 Workspace			HTTP/k2workspacce.domain.com HTTP/k2workspace
SharePoint Web Application			HTTP/mainapplication HTTP/mainapplication.domain.com
SharePoint Web Application			HTTP/mysite HTTP/mysite.domain.com
SharePoint Central Admin			HTTP/mossadmin HTTP/mossadmin.domain.com

SharePoint Configuration Guidance

K2 environments are often tightly integrated with SharePoint. In order to facilitate the K2 environment setup, it is highly recommended that the document Guidance on setting up a SharePoint environment before installing K2 integration be reviewed.

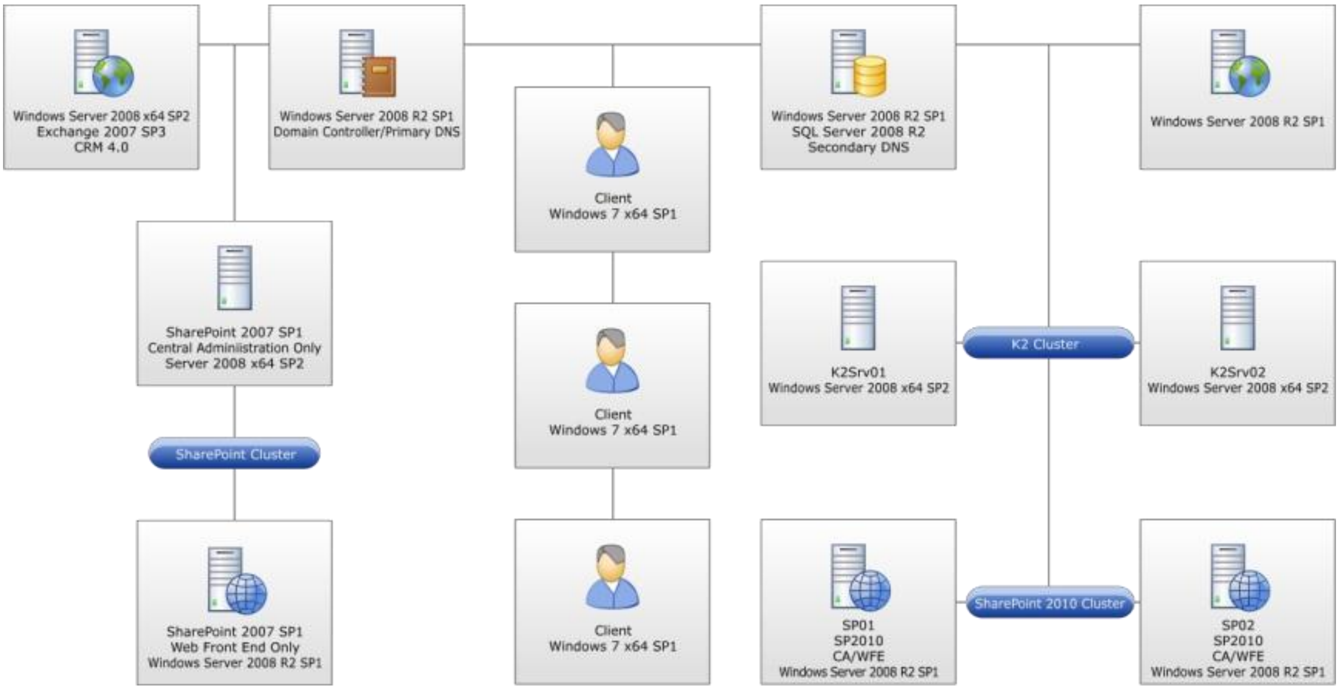
3. Environment Installation

This document outlines the initial installation steps for K2 and should be used as a supplement to the official K2 product installation documentation.

This document can be used as a checklist for an installation as there are a number of tables provided where an installer may enter site-specific date (account details for example).

Example of an Environment Topology Diagram

Although the principle shown in the diagram remains the same, the software versions are continuously upgraded



Specify the domain or domains.

Note: There are multiple domains in use. As this is the case, if an installation account other than one which is a member of the **<DOMAIN>** domain is used, the disable domain check as well as K2 security labels steps must be carried out. These steps are listed as additional sections toward the end of this document.

Label	Role	FQDN
K2 Server	K2 Server	
K2 Web	K2 Workspace	
SharePoint Farm WFE	Microsoft Office SharePoint Server Farm	
SharePoint CA	SharePoint Central Administration	
SharePoint Database	SharePoint Database	

SQL Server	SQL Server host	
SSRS (optional)	SQL Server Reporting Services host	
Mail Server	Exchange Server	

K2 Technologies Prerequisites

For a list of the K2 prerequisites, refer to the **Installation and Configuration > Prerequisites** section of the Getting Started Guide.

The Installation and Configuration account must have local admin rights on each server as well as DB creator and security administrator roles in SQL. For the deployment of K2 for SharePoint components the installation account must have DBO rights on the SharePoint Admin Content database. For further information consult the official K2 documentation at http://help.k2.com and the latest compatibility matrix located at http://help.k2.com/en/blackpearlmatrix.aspx.

DNS Records

Ensure that the following DNS record types have been created. The "DNS Reference" column will be referred to throughout the installation step sections.

Naming convention examples: workspace.contoso.com, ws.contoso.com, k2workspace.contoso.com.

FQDN	Record Type	Purpose	DNS Reference
	HOST (A)	SSRS web service and manager	**[DNS_SSRS]**
	HOST (A)	K2 workspace & web services	**[DNS_WORKSPACE]**
	HOST (A)	K2 Server	**[DNS_K2SRV]**
	HOST (A)	SQL Server	**[DNS_SQLSRV]**
	HOST (A)	SMTP	**[DNS_MAIL]**

Accounts

Ensure the following accounts are created for each component listed in the table below.

Software	Component	Service Account	Account Reference
SSRS	SQL Server Reporting Services		**[ACC_SSRS]**
K2	K2 blackpearl Host Server		**[ACC_BPSERVER]**
K2	K2 blackpearl Web Components		**[ACC_BPWORKSPACE]**
K2.net Admin	Administration Account		**[ACC_K2ADMIN]**

The following table lists the account memberships required on each server.

Server	Account	Group
	[ACC_BPSERVER]	Local Administrators
	[ACC_BPWORKSPACE]	IIS_IUSRS

Rights Assignment	Assigned:
Assign "NT Authority\Authenticated Users" "Browse" rights for SQL Server Reporting Services	
Assign "**[ACC_BPWORKSPACE]**" "Content Manager" rights for SQL Server Reporting Services	

Authentication (Kerberos)

As Kerberos is used the following SPNs are set.

Service	DNS Entry FQDN	Service Account	SPNs
K2 blackpearl Server			
K2 blackpearl Workspace			
SQL Reporting Services			
MS SQL Server			
SharePoint WA			

Note: As Kerberos authenticated connections to the SQL Server Database Engine and SQL Server Reporting Services are required, the relevant SPNs are listed in the above section. These, however, are not a replacement for each component's standard installation & configuration documentation and those relevant documents should also be consulted for further information.

For Kerberos Delegation the following needs to be set on each account listed in the table.

Service Account/Computer	SPNs to Delegate to
	Any service Kerberos only
	Any service Kerberos only
	Any service Kerberos only
	Any service Kerberos only
	Any service Kerberos only

If Kerberos Protocol Transition is required and must be set on the following accounts, the reasons why are listed within the table.

Service Account	Reason

Further installation parameters

Listed are further installation parameters used within the installation, please take note of column "Parameter Reference" as this is referenced in the installation steps.

Item	Value	Parameter Reference
Installation Path		[PARM_InstallPath]
K2 blackpearl Version		[PARM_K2Version]
K2 Server Installation Type		[PARM_K2StandFarm]
Host Server Port		[PARM_HSPort]
Workflow Server Port		[PARM_WkflPort]
Workspace Application Pool Name		[PARM_WKSAppName]
K2 Pass-Through Authentication		[PARM_PassThru]
From Email Address		[PARM_EmailAdd]
Reporting Services		

If additional configuration & troubleshooting steps are required please specify these as per information in Appendix and Troubleshooting.

List of installation items available: use this table in conjunction with the component installation table.

Item	Value
K2 blackpearl Server	A
K2 for Reporting Services	B
K2 Workspace	C
K2 for SharePoint	D
K2 Designer for SharePoint	E
K2 for Visual Studio Core	F
K2 for Visual Studio 2008	G
K2 for Visual Studio 2010	H
K2 Studio	I
K2 Documentation	J

Component installation table: reference values of the installation item from the preceding table.

Server	A	B	C	D	E	F	G	H	I	J
	x		x						x	x
				x	x					
		x								

Installation & Configuration Steps Summary

Listed here is a summary of the configuration steps which will be undertaken during the installation and configuration of the K2 components.

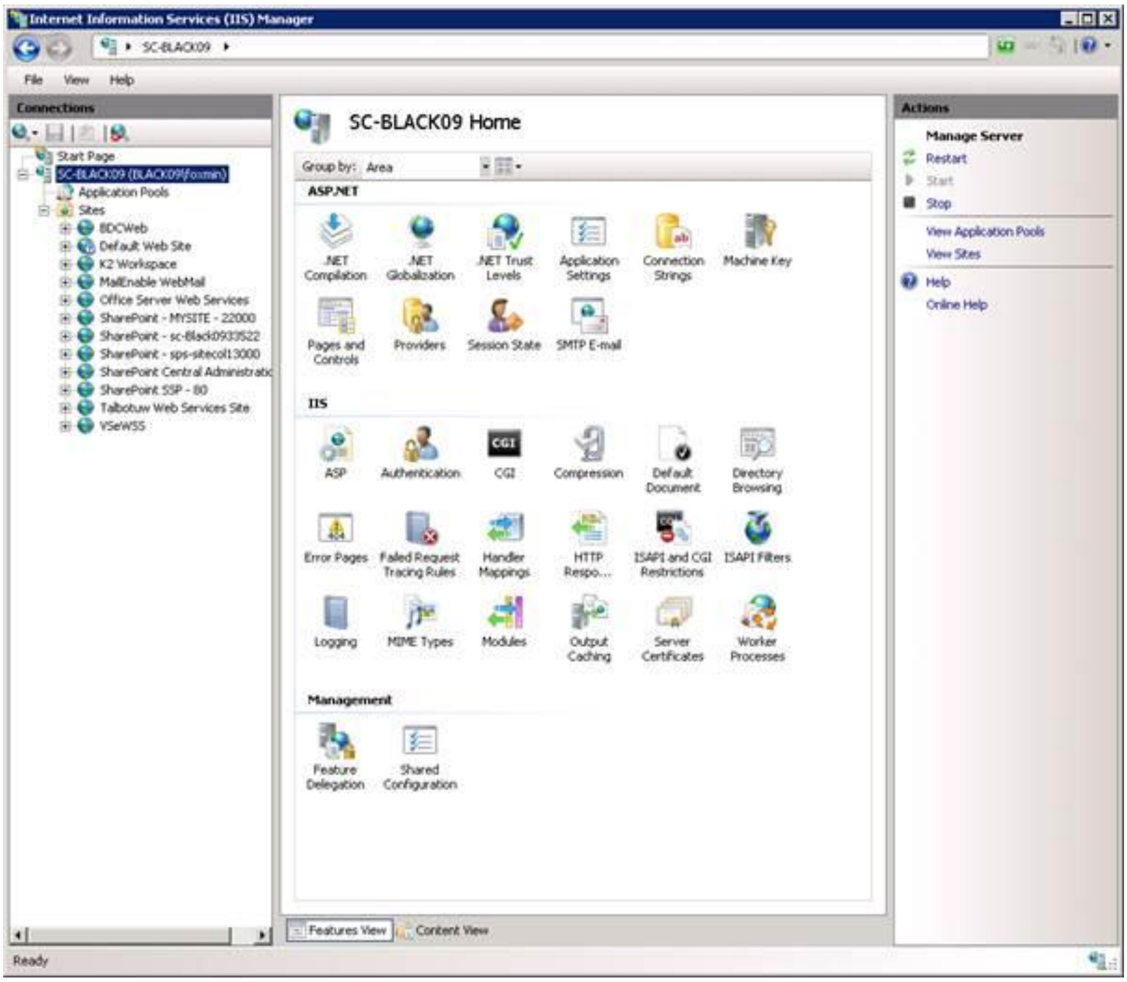
1. Installation to the K2 Host Servers via the K2 Setup Manager
2. Installation to the K2 Web Servers via the K2 Setup Manager
3. Installation to the Reporting Services Servers via the K2 Setup Manager
4. Installation to the SharePoint Servers via the K2 Setup Manager

IIS Configuration

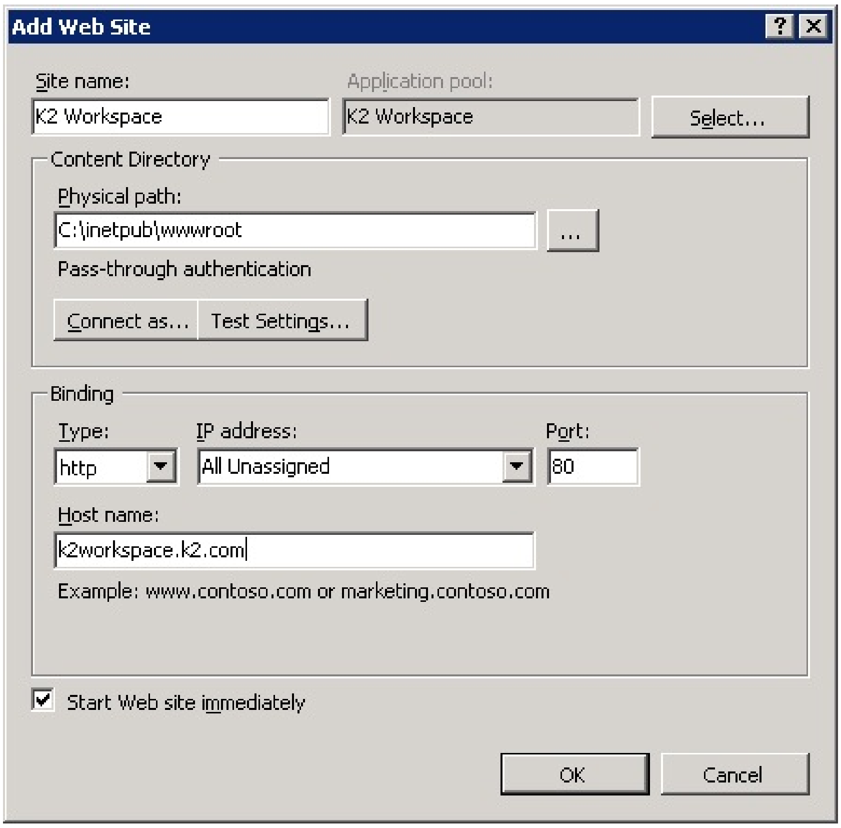
This section outlines the IIS preparation steps to be taken prior to installation.

K2 blackpearl Workspace & Web Services

1. Create an IIS web site on K2 Workspace servers (the K2 Setup Manager will do this during installation).



2. Give the Site Description a meaningful name.
3. If host headers are used assign the “Host name” with **[DNS_WORKSPACE]**.
4. Specify the path for the website; the default value is “C:\Inetpub\wwwroot”.



Add Web Site

Site name: K2 Workspace

Application pool: K2 Workspace

Content Directory

Physical path: C:\inetpub\wwwroot

Pass-through authentication

Binding

Type: http

IP address: All Unassigned

Port: 80

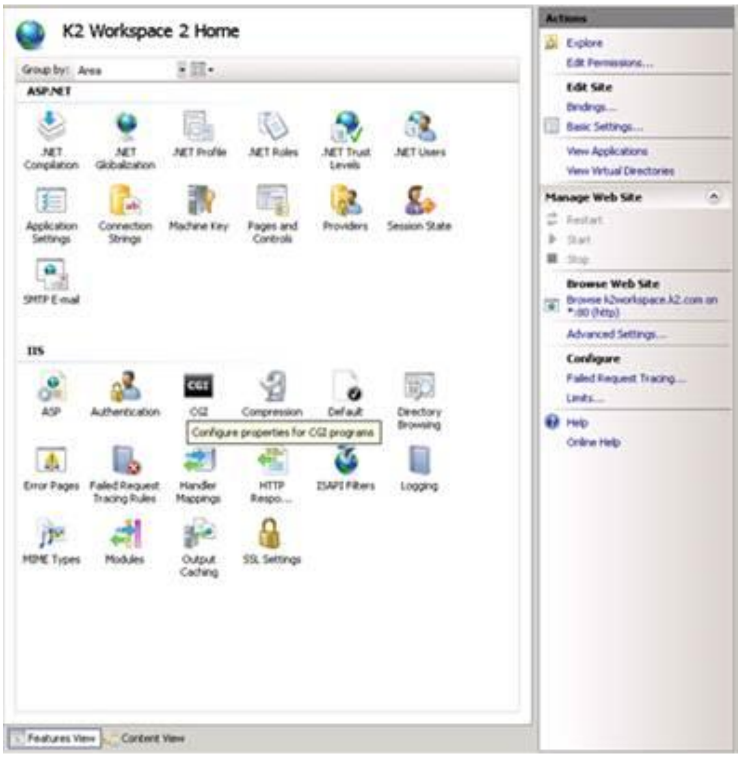
Host name: k2workspace.k2.com

Example: www.contoso.com or marketing.contoso.com

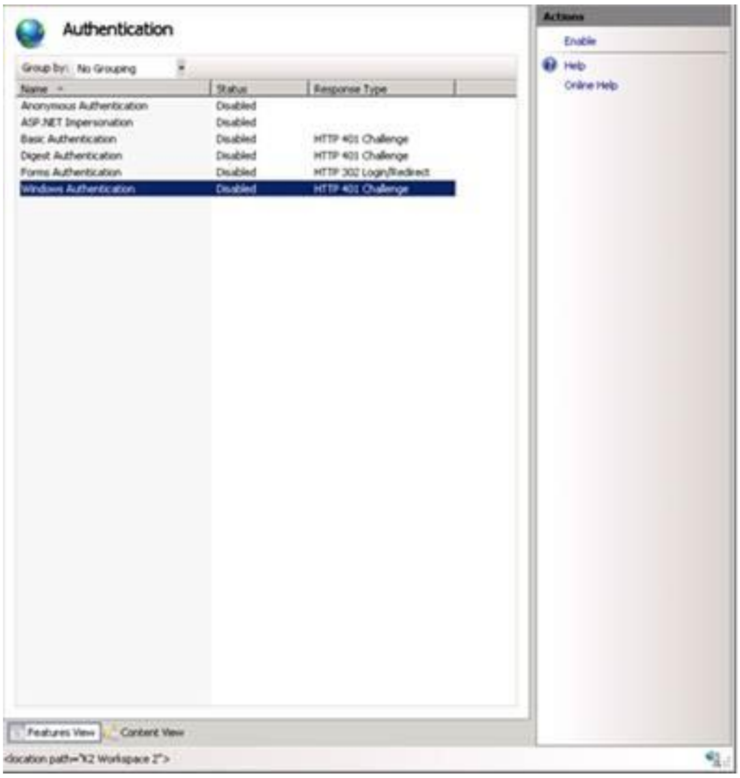
☑ Start Web site immediately

Note: the web site is using the default Application Pool and should be changed to use the blackpearl Application Pool after installing K2 Workspace.

5. Click the newly created web site and in the right hand screen select Authentication.



6. Enable Windows Authentication via right clicking Windows Authentication



Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

<location path="K2 Workspace 2">

Web Site Summary

Web Site	Port	Host Header	Application Pool	Pool ID	Authentication
K2 blackpearl Workspace	80		K2 Workspace		Negotiate,NTLM

SQL Server Reporting Services

Install Microsoft Reporting Services as per Microsoft recommendations. Deployment Guide:

http://technet.microsoft.com/en-gb/sqlserver/bb331776.aspx

Note: Currently K2 integration with SSRS is not being used. K2 blackpearl out of the box reports are executed within the K2 blackpearl Workspace.

Setting up Linked Servers to SQL Server service instances not on the local database instance

Introduction

Occasionally customers need to run distributed queries (queries run against linked servers), certain set up steps need to be performed for this to be possible.

Databases may be set up on different server instances for a number of reasons, amongst others, to improve efficiency in high load environments. Generally speaking the bottleneck is more often than not due to I/O limitation and not CPU or memory issues so splitting databases onto different instances only allows a limited improvement in performance, if any at all, and at a cost of added complexity.

Improving efficiency of I/O transactions in the K2 database(s):
There is little value to putting the databases on different server instances; however, the FILES and FILEGROUPS that those databases live in should be placed on different LUNS (Spindles on a SAN). The K2Server.LOG and K2Server.Data should each be placed on their own LUN in environments where the databases have not been consolidated. Most of the other databases are not as heavy transactionally, so they could be on a common LUN.

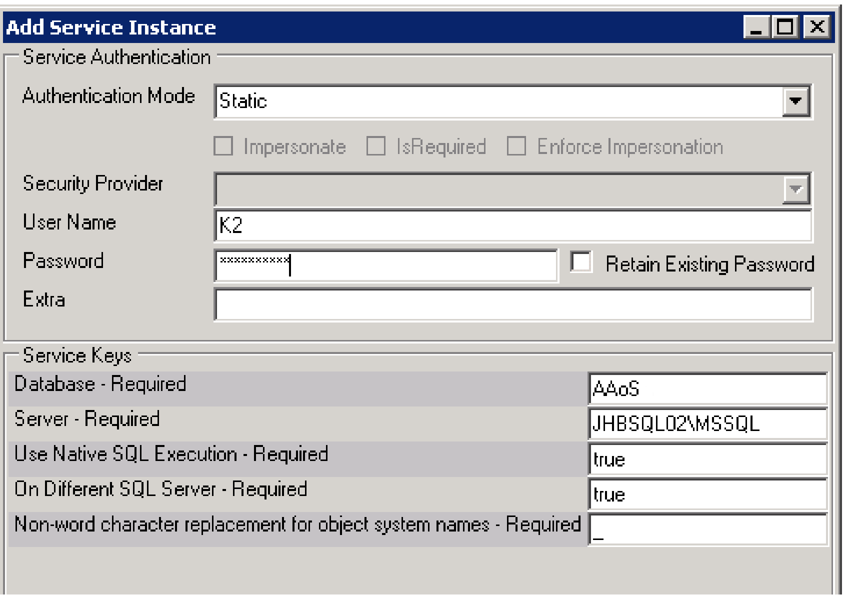
Issues with SQL instances across multiple databases on different servers

The most common issue is the “Login failed for user ’NT AUTHORITY\ANONYMOUS LOGON” error. Also, in the context of linked servers, the GetList method raises the "User does not have permission to perform this action" error.

The "ANONYMOUS LOGON" failure is usually a result of a Kerberos authentication failure between the two SQL Servers. This can be addressed as follows:

1. On the K2 Server, run the SQL Server Configuration Manager tool. Under the SQL Native Client Configuration -> Client Protocols, make sure "TCP/IP" is enabled and change the order so it is at the top of the list (just below Shared Memory).
2. On the primary SQL Server where K2 databases were originally installed, run the SQL Server Configuration Manager tool. Under the SQL Native Client Configuration -> Client Protocols, make sure "TCP/IP" is enabled and change the order so it is at the top of the list (just below Shared Memory).
   Under the SQL Server Network Configuration -> Protocols for MSSQLServer make sure the "TCP/IP" protocol is enabled.
3. On the remote SQL Server where the databases are mirrored for fail-over, run the SQL Server Configuration Manager tool. Under the SQL Server Network Configuration -> Protocols for MSSQLServer make sure the "TCP/IP" protocol is enabled.
4. Make sure that SPNs are set for service accounts used to run the SQL Server service on both servers. They will look something like this:
   MSSQLSvc/<hostname>:1433
5. Make sure the account used to run the primary SQL Server service is trusted for delegation in Active Directory.

6. Restart the SQL Server service on both boxes.
7. Restart the K2 Service and test with a GetList method.



Add Service Instance

Service Authentication

Authentication Mode: Static

☐ Impersonate ☐ IsRequired ☐ Enforce Impersonation

Security Provider:

User Name: K2

Password: ********** ☐ Retain Existing Password

Extra:

Service Keys

Database - Required	AAoS
Server - Required	JHBSQL02\MSSQL
Use Native SQL Execution - Required	true
On Different SQL Server - Required	true
Non-word character replacement for object system names - Required	_

If the **Service Instance Authentication Mode** is set to **Static** when adding the service instance and the error is still generated, the following steps should be followed:

1. Create a linked server on the SQL Server instance that contains the K2 database(s), and name it the same as the **Server** field of the **Service Keys** section of the **Add Service Instance** screen. It must have this exact name.
2. Ensure that the K2 Service Account translates to the ‘K2’ SQL Auth account, in the remote server, when the above linked server object is used (it is defined within the linked server object).

Additional considerations

If the K2 Service account has SysAdmin rights and the SQL service instance **'Native Execution' = FALSE** and **'On Different SQL server' = true**, the linked server is automatically created in SQL when performing a Getlist.

If the SQL service instance uses **'Native Execution' = TRUE** and **'On Different SQL server' = true**, the linked server is automatically created in SQL when performing a Getlist but this fails with error 'Login failed for user ’NT AUTHORITY\ANONYMOUS LOGON' when executing the Getlist.

So the option is to either delete the linked server, set **'Native Execution' = FALSE** and **'On Different SQL server' = true** prior to executing the first Getlist, or to specify a SQL account to be used in the Linked Server (using SQL Management Studio).

Setting the NT Authentication Providers

Windows 2008: http://technet.microsoft.com/en-us/library/cc754628%28WS.10%29.aspx

Windows 2008 R2: This can also be set from the IIS management GUI in step 6 once windows authentication has been enabled the option to set "Providers" is listed on the left hand bar.

Note: The default provider's setting for all websites in IIS 7.5 is Negotiate with NTLM as backup.

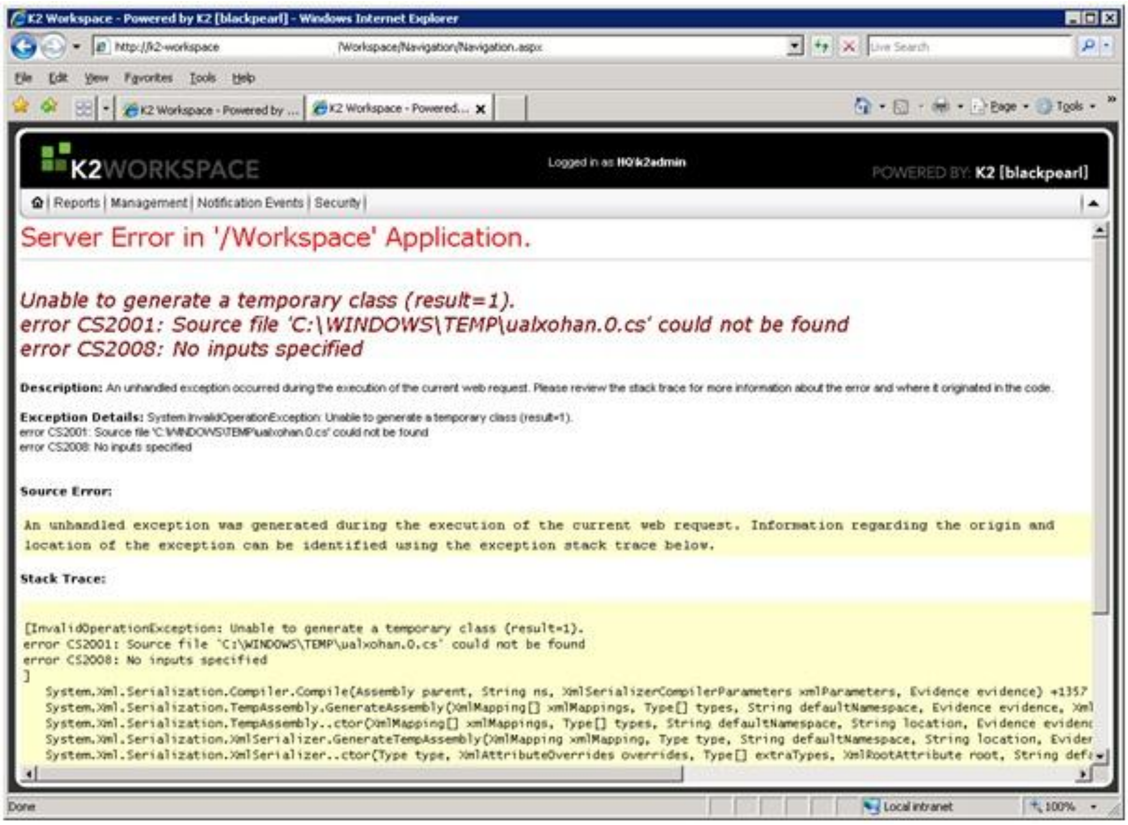
4. Post Installation Steps

K2 Workspace

Apply the following checks and settings on all nodes where the K2 blackpearl Workspace has been installed.

1. Open up the IIS Manager snap in, expand the IIS instance, Application Pools and right click on the application pool "K2 BlackPearl Application Pool", select Properties.
2. Click on the tab identity, insure that the account is correct "**[ACC_BPWORKSPACE]**", and also insert the password to ensure that this is correct.
3. Now stop and restart the application pool.
4. Add the account used "**[ACC_BPWORKSPACE]**" to the local "IIS_WPG" group on each node this can be done using the "Local Users and Groups" snap in.

If you receive an error about access to the "C:\Windows\Temp" Directory when browsing to the workspace, you must grant the workspace application pool account **[ACC_BPWORKSPACE]** "Modify" rights on the directory "C:\Windows\Temp".


K2 Workspace - Powered by K2 [blackpearl] - Windows Internet Explorer
http://k2-workspace /Workspace/Navigation/Navigation.aspx
Live Search
File Edit View Favorites Tools Help
K2 Workspace - Powered by ...
K2 Workspace - Powered...
Page Tools
K2WORKSPACE
Logged in as HQ\k2admin
POWERED BY: K2 [blackpearl]
Reports | Management | Notification Events | Security
Done
Local intranet
100%

Server Error in '/Workspace' Application.

Unable to generate a temporary class (result=1).
error CS2001: Source file 'C:\WINDOWS\TEMP\ualxohan.0.cs' could not be found
error CS2008: No inputs specified

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.InvalidOperationException: Unable to generate a temporary class (result=1).
error CS2001: Source file 'C:\WINDOWS\TEMP\ualxohan.0.cs' could not be found
error CS2008: No inputs specified

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and
location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[InvalidOperationException: Unable to generate a temporary class (result=1).
error CS2001: Source file 'C:\WINDOWS\TEMP\ualxohan.0.cs' could not be found
error CS2008: No inputs specified
]
   System.Xml.Serialization.Compiler.Compile(Assembly parent, String ns, XmlSerializerCompilerParameters xmlParameters, Evidence evidence) +1357
   System.Xml.Serialization.TempAssembly.GenerateAssembly(XmlMapping[] xmlMappings, Type[] types, String defaultNamespace, Evidence evidence, Xml
   System.Xml.Serialization.TempAssembly..ctor(XmlMapping[] xmlMappings, Type[] types, String defaultNamespace, String location, Evidence evidenc
   System.Xml.Serialization.XmlSerializer.GenerateTempAssembly(XmlMapping xmlMapping, Type type, String defaultNamespace, String location, Evider
   System.Xml.Serialization.XmlSerializer..ctor(Type type, XmlAttributeOverrides overrides, Type[] extraTypes, XmlRootAttribute root, String defa
```

K2 Updates

It is advised that the latest updates from K2 be installed.

5. K2 Software Installation

K2 Software Installation

Details concerning the installation of K2 blackpearl and blackpoint can be found online in the K2 blackpearl Getting Started Guide and the K2 blackpoint documentation.

The links below refer directly to the relevant sections of the Getting Started Guide:

- Standalone install Distributed install Client install
- Post installation - refer to the section in the Getting Started Guide (Installation and Configuration > Installation > Post installation common tasks)
  - Workspace
  - Updates

Exchange Runtime Operational Rights

It is important to set up runtime operational rights for Exchange, see this KB article for more information: http://help.k2.com/en/kb001189.aspx

6. K2 Health Check Procedure after Install

This topic covers a procedure for validating the basic health of a K2 environment after installation.

Introduction

This document covers a simple system settings review, build, deploy, and run procedure to confirm the following:

- K2 Workflows can be created, deployed, and executed in the environment.
- K2 SmartObjects can be created, deployed, and executed in the environment. Core K2 dependencies and integrations are functioning:
    - Email integration
    - InfoPath integration
    - SharePoint Workflow integration
    - K2 Worklist Web Part
- Authentication across components is functioning

Testing before going live

Before testing, database backups of the clean, newly installed state should be made, then test workflows deployed and tested, and finally, the clean state should be restored.

Note: This document is not intended as a training vehicle; prior knowledge of K2 is expected and required.

Environment Verification Checklist

Task	Result
Verify K2 Instillation WRT Authentication, DNS, IIS, Kerberos, MSMQ, MSDTC	
Verify port configuration	
Verify Browser Configuration	
Verify all server roles for performance	
Verify all server roles for instillation	
Verify .Net versions and patch levels	
Analyze and investigate logs	
Performance monitor all server roles	
Verify the Client Event e-mail notification (For troubleshooting see K2 connection string editor tool on K2 underground http://www.k2underground.com/groups/k2_connection_string_editor/default.aspx)	

Build, deploy, execute

Build and deploy a K2 InfoPath Workflow

Requirements:

- Create a form template using InfoPath Form Designer with two views – one for process start and one for actioning a task.
- Create K2 InfoPath Workflow
  - If the user (client) intends to use InfoPath Forms Services, web enable the form
  - Document library created for form template in either template or content type mode
  - Upload the template (via the K2 InfoPath Workflow wizard). Add InfoPath Client Event with at least one Finish action
- Connect the Start event to client event with a line rule
  - Destination user can be the process originator or another user
  - Include an email notification
- Add Activity to act as final process step
  - Connect client event to final activity with line rule
  - Include an email notification event used to notify tester of process instance completion.
  - Deploy K2 InfoPath Workflow to K2 and SharePoint Form Library
- If any errors occur during deployment, evaluate and mitigate as appropriate
  - Redeploy the workflow

Result and Comments:

Execute K2 InfoPath workflow

Requirements:

- Grant process start rights to the user being used to start the workflow if necessary.
- Initiate a workflow via the InfoPath form start view by creating a form from the form library
- Verify the email notification for the task is received by the destination user of the client event.
- Verify you can view the task in a the K2 Worklist via K2 Workspace and/or the K2 Worklist web part in SharePoint
- Open the InfoPath Form and execute the Finish action
- Verify the email signifying process completion is received

Result and Comments:

Build and deploy K2 SharePoint Workflow Integration Process

Requirements:

- Create a K2 SharePoint Workflow Integration Process
  - Associate it with a List or Document library
  - Forms: ASP.NET
  - Task list and Workflow History lists can be new or the existing ones in the site
  - Start page is optional.
  - Enable start process when item is created.
- Add a SharePoint Workflow Integration client event with at least one Finish action
  - Destination user can be the process originator or another user
  - Include an email notification
- Add Activity to act as final process step.
  - Connect client event to final activity with line rule
  - Include an email notification event used to notify tester of process instance completion.

Result and Comments:

Execute K2 SharePoint Workflow

- Grant process start rights to the account being used to start the workflow if necessary. Initiate a workflow by adding an item to the SharePoint List or Document Library
- Verify the email notification for task is received by the destination user of the client event
- Verify you can view the task in the K2 worklist via K2 Workspace and/or the K2 Worklist web part in
- SharePoint
- Open the form and execute the Finish action
- Verify you received the email from the final activity.

Result and Comments:

Build and deploy K2 Events Process

Requirements:

- Create a K2 SharePoint Events Process
  - Associate it with a specific List or Document library
  - Enable start process when item is created. Add Activity to act as final process step.
- Connect start event to final activity with line rule
  - Include an email notification event used to notify tester of process instance completion. Deploy the workflow to K2 and the SharePoint list or document library
- If any errors occur during deployment, evaluate and mitigate as appropriate.

Optional:

- Add a client event with at least one Finish action in-between the start event and final activity.
  - The client page does not need to exist
  - You can action the task via the K2 Worklist by using the context menu to execute the finish action.

Result and Comments:

Execute K2 Events Process

- Grant process start rights to the account being used to start the workflow if necessary. Initiate a workflow by adding an item to the SharePoint List or Document Library
- Verify you receive an email from the final activity.

Result and Comments:

Build and deploy K2 SmartObject

Requirements:

- Create a simple SmartObject using the K2 Designer for Visual Studio or the K2 SmartObject Test Tool.
  - Could be a simple SmartBox SmartObject – Employee with a few fields is a common example
  - Could also be a SmartObject that directly wraps a Service Object already available on the K2 Server. Deploy SmartObject to K2 server using K2 Designer for Visual Studio or K2 SmartObject Test Tool (publish). Verify deployment completes successfully

Result and Comments:

Execute SmartObject method

- Execute a SmartObject method

Examples

- Create instance of SmartBox SmartObject
- Execute a List method to return all or a filtered list of items

Result and Comments:

Execute K2 Reports

Requirements:

- Execute the Process Overview Report from K2 Workspace from a remote client machine.
- Create a K2 Process Portal site in your primary SharePoint site, add some workflows to the site, and run a report from a remote client machine.
- Execute the Process Overview or another K2 report from the SQL Reporting services (if the K2 for Reporting Services component was installed) site from a remote client machine.

Results: The reports should run without errors.

Result and Comments:

7. Administration Tasks

Over time, there are a number of tasks an administrator needs to perform to maintain a K2 system. Listed below are common tasks:

- Empty SmartActions mailbox

Administration task: SmartActions fail: mailbox full error

SmartActions Mailbox Maintenance

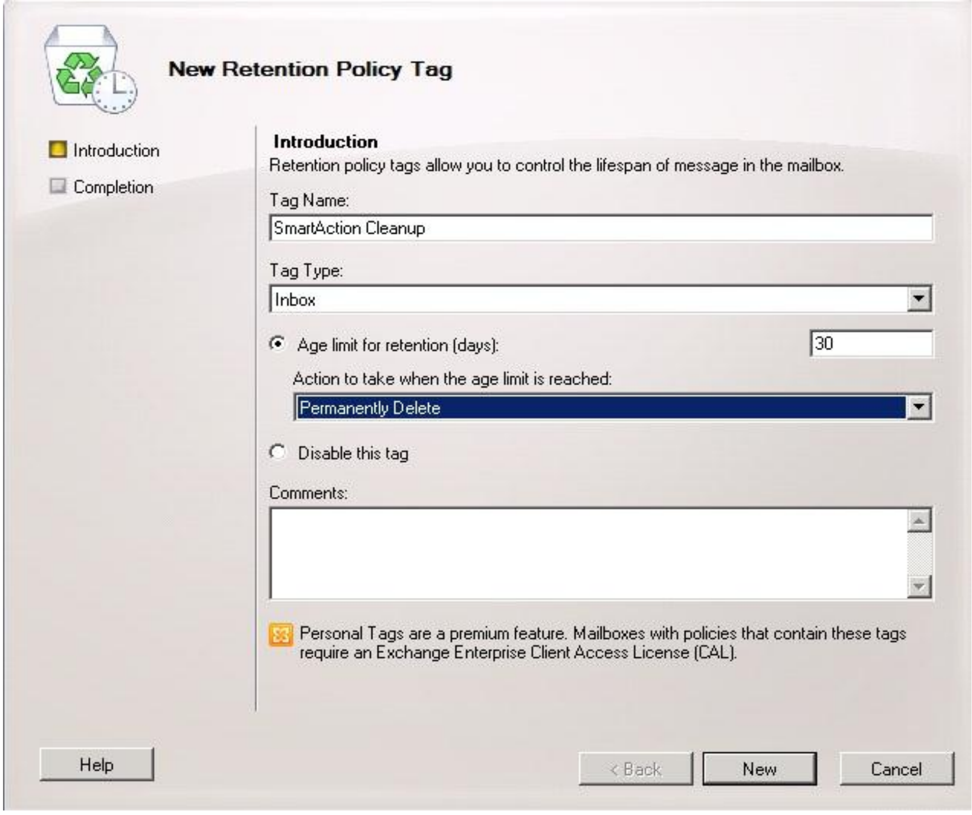
If the mailbox configured for SmartActions becomes full, SmartActions will fail and report an error stating that the mailbox is full. It is therefore important to regularly log into the mailbox as the configured account using OWA (Outlook Web App - previously called Outlook Web Access) and delete or archive SmartAction emails.

It is possible to automate this action using a Retention Policy Tags set up in the Exchange Management console. See http://technet.microsoft.com/en-us/library/dd297955.aspx for more information on Retention Tags and Policies.

⚠ If the K2 server encounters issues processing the mailbox, pending actions could potentially be deleted after the set retention period.

Setting up a Retention Policy Tag

1 In the Exchange Management Console (Organization Configuration > Mailbox). Select the Retention Policy Tags tab and select New Retention Policy Tag in the Actions pane.



New Retention Policy Tag

Introduction
Retention policy tags allow you to control the lifespan of message in the mailbox.

Tag Name: SmartAction Cleanup

Tag Type: Inbox

● Age limit for retention (days): 30

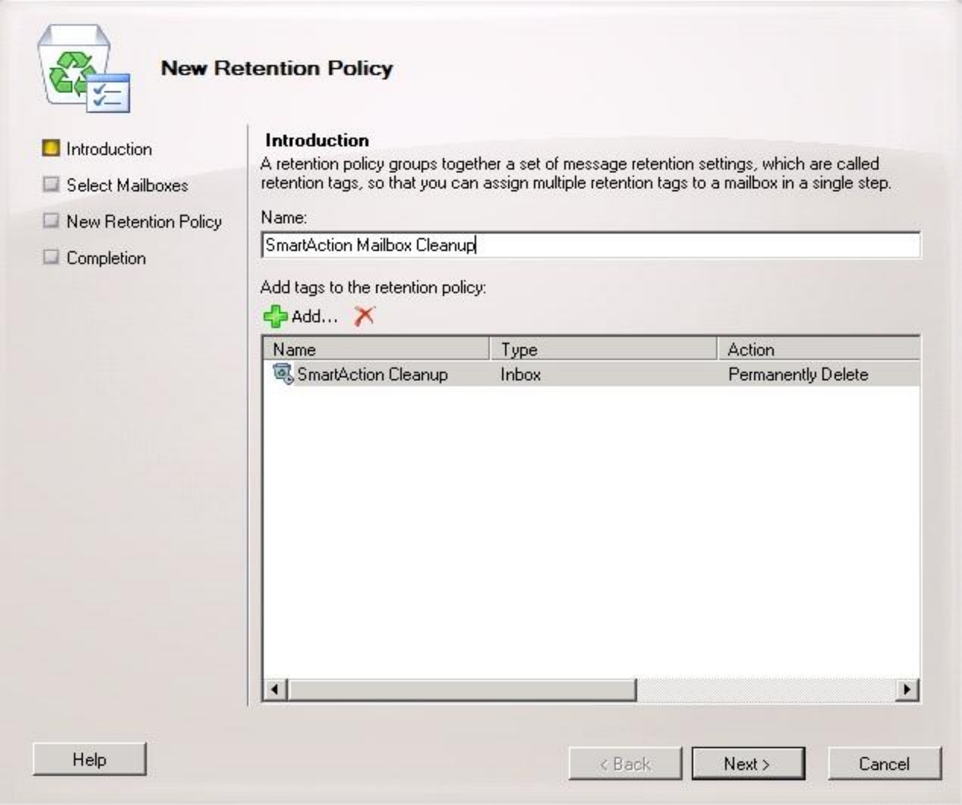
Action to take when the age limit is reached: Permanently Delete

○ Disable this tag

Comments:

Personal Tags are a premium feature. Mailboxes with policies that contain these tags require an Exchange Enterprise Client Access License (CAL).

2 Switch to the Retention Policies tab, select New Retention Policy in the Actions pane. Add the previously created tag.



New Retention Policy

Introduction

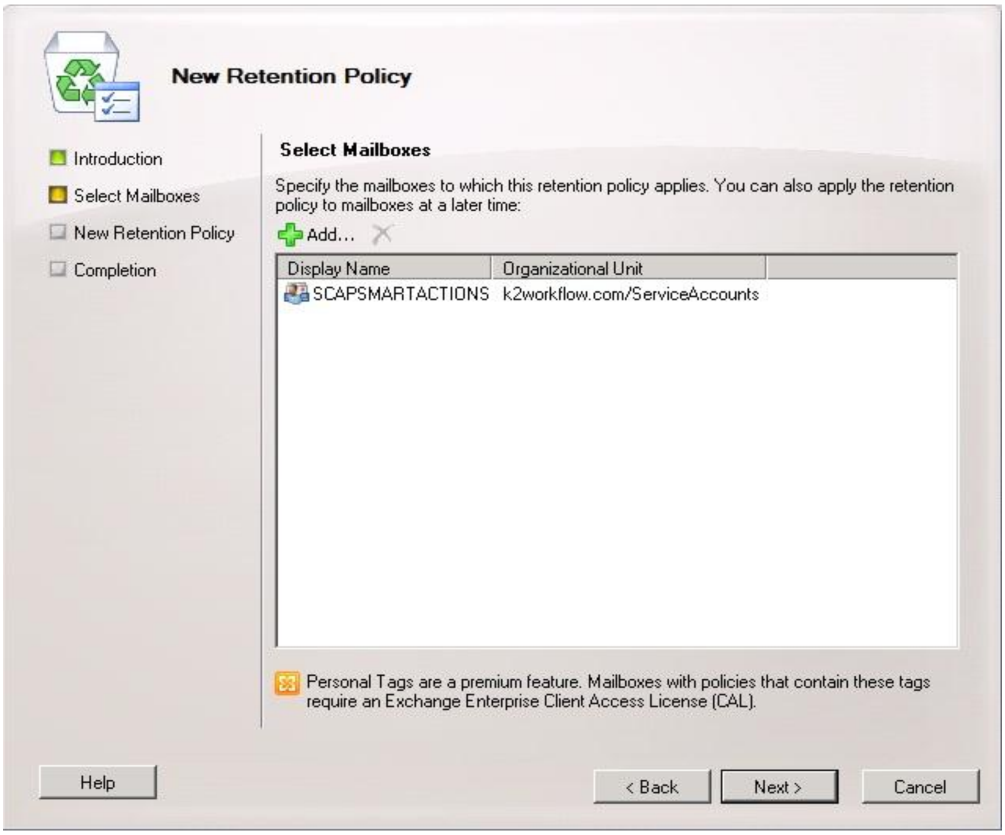
A retention policy groups together a set of message retention settings, which are called retention tags, so that you can assign multiple retention tags to a mailbox in a single step.

Name: SmartAction Mailbox Cleanup

Add tags to the retention policy:

Name	Type	Action
SmartAction Cleanup	Inbox	Permanently Delete

3 Select the SmartAction mailbox to apply to.



New Retention Policy

- Introduction
- Select Mailboxes
- New Retention Policy
- Completion

Select Mailboxes

Specify the mailboxes to which this retention policy applies. You can also apply the retention policy to mailboxes at a later time:

Display Name	Organizational Unit
SCAPSMARTACTIONS	k2workflow.com/ServiceAccounts

Personal Tags are a premium feature. Mailboxes with policies that contain these tags require an Exchange Enterprise Client Access License (CAL).

8. Appendix and Troubleshooting

This section contains troubleshooting steps and additional configuration options.

IIS 7 kernel Mode Authentication

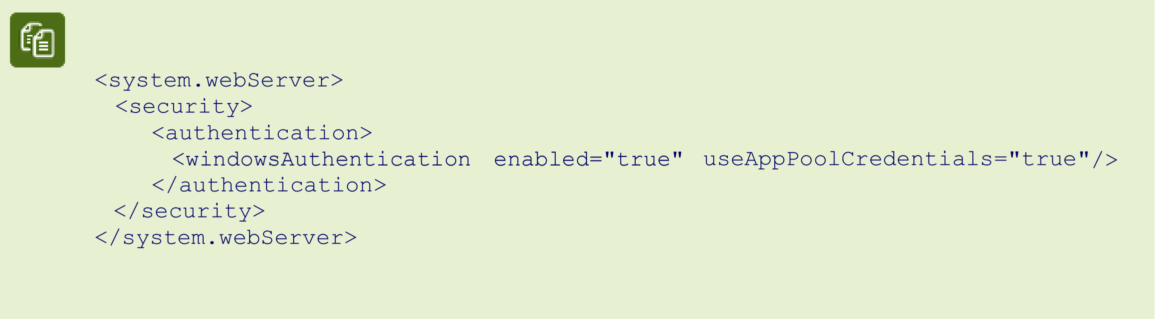
IIS 7.0 introduces Kernel mode authentication which is set as enabled by default, what this means is that the authentication is handled by the machine account by default. When kernel mode authentication is enabled, Kerberos tickets for the requested site need to be encrypted with the machine accounts master key. This means that there needs to be an SPN set on the machine account for the site in question, this by default is automatically handled by IIS 7.0. Such a change allows you to run applications within one web site under one FQDN using multiple application pools with different identities avoiding the duplicate SPN issue. However such a model will cause Kerberos authentication failure for sites deployed as a farm or with a Host Header.

To resolve this issue there are 2 approaches;

1. Enable use of the application pools credentials, (this is the advised approach).
2. Disable kernel authentication for the web site.

1. Enable Use of Application Pool Credentials

- Open the “ApplicationHost.config” file with a text editor, this is located in “%windir%\System32\inetsrv\config\”.
- Locate your website or virtual directory **(for a SharePoint web application you will need to make the setting at the web site level)**.
- Within the “<system.webServer>” section add the following entry in the nested “<authentication>” section, “**useAppPoolCredentials="true"**”. The entry should look something similar to the bellow;



```
<system.webServer>
  <security>
     <authentication>
       <windowsAuthentication  enabled="true"  useAppPoolCredentials="true"/>
     </authentication>
  </security>
</system.webServer>
```

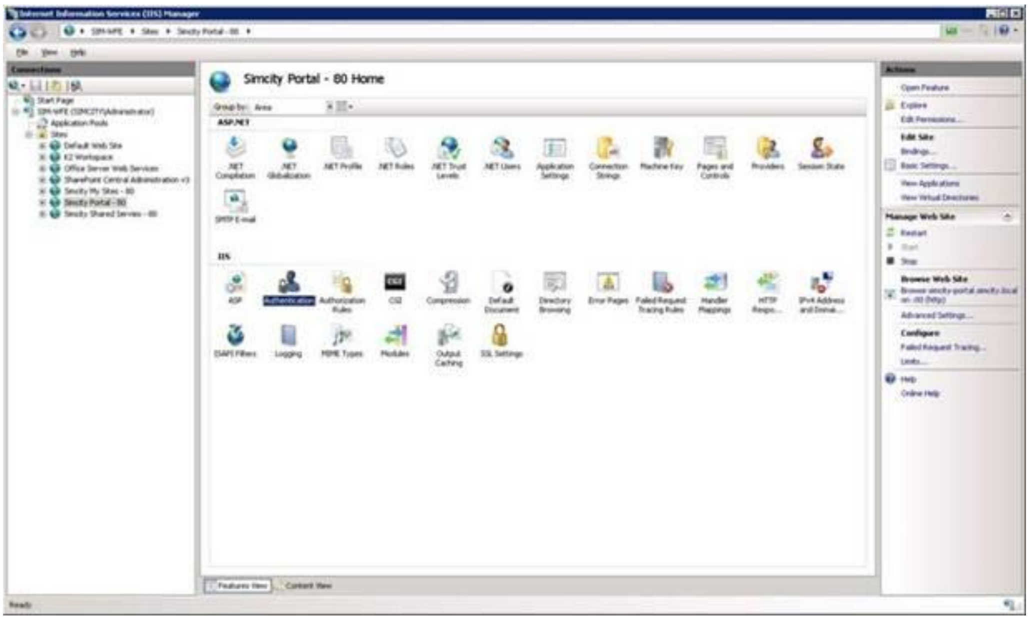
NOTE CONCERNING WINDOWS 2008 R2 & blackpearl 4.5 and above:

There are 3 areas where you must set the “useAppPoolCredentials”;

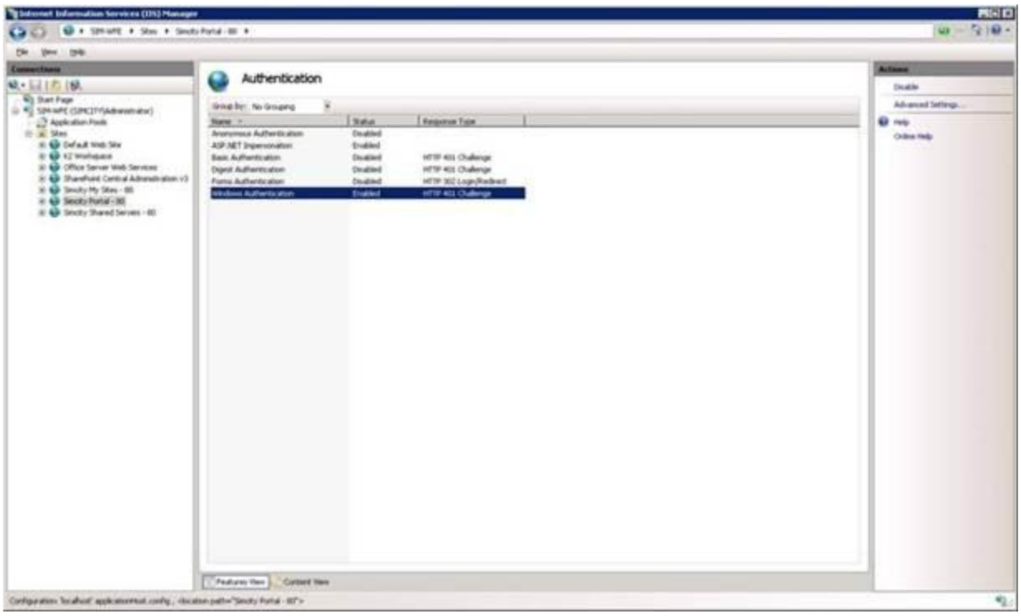
1. **ApplicationHost.config** found at: "*%windir%*\system32\inetsrv\config”
2. **InetPub Web.config** found at: “%InetPubdir%\%WebSiteDir%”
3. **Virtual Dir Web Application web.config** found at: ”%BlackpearlInstallDir%\Workspace\Site”
   and "%BlackpearlInstallDir%\Webservices\RuntimeServices”
   and "%BlackpearlInstallDir%\Webservices\ViewFlow”

2. Disable Kernel Authentication

Using the IIS 7.0 snap-in click on the website you want to disable kernel authentication for. On the right hand side double click on the “Authentication” icon in the left hand side pane as highlighted in the bellow screen shot.

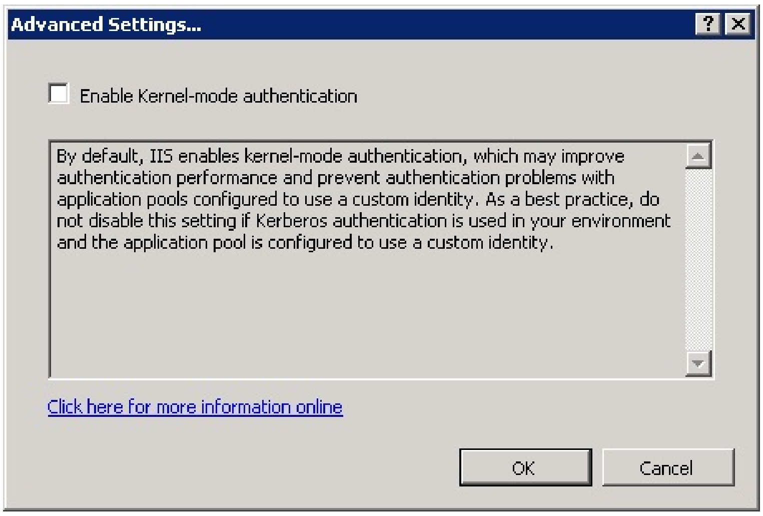


Right click “Windows Authentication” and select “Advanced Settings”



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Uncheck “Enable kernel-mode authentication” and click “OK”.



□ 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.

Tighten K2 Report Structure for Shared SSRS Service

Note that the use of SSRS is optional.

8. The K2 out of the box report RDLs can be moved into the desired folder structure and continue to be executed from the K2 Workspace.
9. The new structure can be configured for reports surfaced in SharePoint via web parts.
10. The K2 report designer from within the K2 Workspace will always publish built reports to the folder “Reporting” on the root level of reporting services. As this is the case the folder should have content manager rights granted to the **[ACC_BPWORKSPACE]** only and the folder set as hidden.
11. If a change to the reporting structure is made the K2 configuration manager will overwrite this upon each execution and the manual steps must be performed, this would be for reconfigurations and updates or K2 SSRS patches.
12. The K2 Workspace **OOBReports.xml** file must also be updated to respect the new structure in SSRS, to do this perform the following steps:
    i. On the K2 Workspace server browse to the %InstallDir%\K2 blackpearl\WorkSpace\Site.
    ii. Open the file “OOBReports.xml”.
    iii. Replace each entry of “ReportPath="/Standard Reports/Hidden” with the new structure.

Set K2 Host Server to use Private queues

Out of the box K2 expects MSMQ to be installed using Active Directory Integration, however this is not the default for MSMQ in Windows 2008 onwards. To use local private queues instead of public AD integrated queues the following configuration changes must be made on each K2 Server.

1. Locate the file **%K2 Install Dir%\K2 Blackpearl\Host Server\Bin\SourceCode.EventBus.Server.config**

- Search for the <msmqpath> and <msmqerrorpath> entries and change them as per below (i.e. replace “**%ServerName%**” with the name of the local server).
  - <msmqpath>**%ServerName%\private$\**EventBus</msmqpath>
  - <msmqerrorpath>**%ServerName%\private$\**EventBus Error</msmqerrorpath>

2. Locate the file **%K2 Install Dir%\K2 Blackpearl\Host Server\Bin\SourceCode.EventBus.ClientRecorder.dll.config**
   - Search for the <msmqpath> entry and make the bellow change.
     - <msmqpath>**%ServerName%\private$\**EventBus</msmqpath>

Disable generate publisher information

For all signed code the .Net Framework will try and contact Microsoft servers to check publisher information, this can result in slow performance of .Net based components when the server has no access to the outside world as a timeout has to occur before this step is passed. To disable this please perform the following steps:

1. Open the .Net 2.0 framework machine.config file for editing, make sure if you are using 64bit to use the copy held in the x64 framework folder.
2. Edit the section “<runtime />” inserting the following;

```
<runtime>
   <generatePublisherEvidence enabled="false"/>
</runtime>
```

This section is contained within the “<configuration>” section.

Disable loopback check

Often the loopback check will cause authentication issues on the server; this is described in the MS support article http://support.microsoft.com/kb/896861.

Method 1: Specify host names (Preferred method if NTLM authentication is desired)

To specify the host names that are mapped to the loopback address and can connect to Web sites on your computer, follow these steps:

1. Set the DisableStrictNameChecking registry entry to 1. For more information about how to do this, click the following article number to view the article in the Microsoft Knowledge Base:
   281308 (http://support.microsoft.com/kb/281308/) Connecting to SMB share on a Windows 2000-based computer or a Windows Server 2003-based computer may not work with an alias name.
2. Click **Start**, click **Run**, type regedit, and then click **OK**.
3. In Registry Editor, locate and then click the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0
4. Right-click **MSV1_0**, point to **New**, and then click **Multi-String Value**.
5. Type BackConnectionHostNames, and then press **ENTER**.

6. Right-click **BackConnectionHostNames**, and then click **Modify**.
7. In the **Value data** box, type the host name or the host names for the sites that are on the local computer, and then click **OK**.
8. Quit Registry Editor, and then restart the IISAdmin service.

Method 2: Disable the loopback check (less-recommended method)

The second method is to disable the loopback check by setting the **DisableLoopbackCheck** registry key.

To set the **DisableLoopbackCheck** registry key, follow these steps:

1. Set the DisableStrictNameChecking registry entry to 1. For more information about how to do this, click the following article number to view the article in the Microsoft Knowledge Base:
   281308 (http://support.microsoft.com/kb/281308/) Connecting to SMB share on a Windows 2000-based computer or a Windows Server 2003-based computer may not work with an alias name.
2. Click **Start**, click **Run**, type regedit, and then click **OK**.
3. In Registry Editor, locate and then click the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
4. Right-click **Lsa**, point to **New**, and then click **DWORD Value**.
5. Type DisableLoopbackCheck, and then press **ENTER**.
6. Right-click **DisableLoopbackCheck**, and then click **Modify**.
7. In the **Value data** box, type 1, and then click **OK**.
8. Quit Registry Editor, and then restart your computer.

Kerberos Tweaks

Following are Kerberos tweaks that should be applied on all servers to force use of TCP and increase token size to deal with large group membership in AD.

1. In Registry Editor, locate and then click the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
2. Create the following **DWORDS**;
   Name: MaxPacketSize
   Value: 1
   Name: MaxTokenSize
   Value: 48k

For more information see http://blogs.technet.com/b/askds/archive/2012/09/12/maxtokensize-and-windows-8-and-windows-server-2012.aspx.