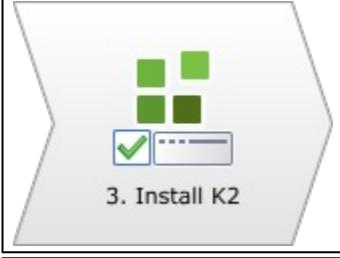
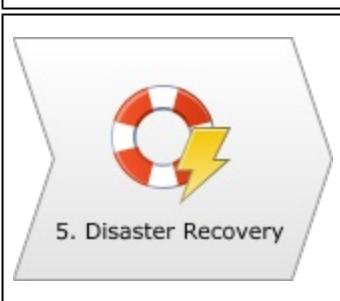


Getting Started

The table below shows the steps that need to be taken for a first-time installation in the first column, the step's description in the second column and individual parts of the step in the third column. It is highly recommended that first-times installers scan through all the material (at least at a high level) to get an overview of the installation and configuration of K2 blackpearl.

Index keywords have been extensively updated since K2 blackpearl 4.5 and using the index system will allow a user to find relevant information much faster than scrolling through the Table of Contents tree view.

 1. Planning K2 Installation	<p>In order to plan an effective, efficient and scalable environment, a K2 blackpearl installation needs to be planned out considering the following four tiers: K2 server tier; web tier; database tier; and client tier.</p>	<ul style="list-style-type: none"> ▪ Architecture ▪ Component Overview ▪ Supported Topologies ▪ Additional Planning Considerations
 2. Prerequisites	<p>Certain requirements need to be met before an install can be initiated. This section details all the requirements needed during a full installation.</p>	<ul style="list-style-type: none"> ▪ Hardware ▪ Software ▪ Permissions ▪ Environment Configuration
 3. Install K2	<p>Each of the various installation types, from single server standalone machine to a installation over a distributed environment are described in this section.</p>	<ul style="list-style-type: none"> ▪ Standalone install ▪ Client Tools Only install ▪ Custom standalone install ▪ Distributed environment ▪ Unattended installation ▪ Integration configuration
 4. Maintenance	<p>Once you have K2 blackpearl up and running in your environment, there may be times when you need to modify components or change configuration settings. This can be accomplished by re-running the Setup Manager.</p>	<ul style="list-style-type: none"> ▪ Adding Components ▪ Updating the K2 License Key ▪ Repair ▪ Remove Components ▪ Upgrading
 5. Disaster Recovery	<p>Disaster recovery is described as the process, policies and procedures put in place to deal with potential natural or human-induced disasters. A disaster is an event that creates chaos and could prevent the continuation of normal functions.</p>	<ul style="list-style-type: none"> ▪ Introduction with Scenarios

 6. Troubleshooting	If errors occur, this section (and the Troubleshooting Index entries) will help a user find a solution.	▪ Start Troubleshooting
---	---	-------------------------



When using the Getting Started Guide as a reference, be sure to use the **Index** tab functionality to find the specific information needed.
Also please use the **Community Comment** link at the foot of every help page to send the K2 documentation team comments.

What's new?

- See What is new in this release

Suggested Links

- For in-depth technical information, visit the [Online K2 Help System](#)

1.1 Introduction



K2 blackpearl helps people build process-driven applications – fast.

Process-driven applications span employees, departments, organizations and line-of-business systems. They can be set up to automate and manage business processes — such as document approval, vacation requests and inventory tracking — or pull together business processes, people, services, information and systems into a single application that improves business efficiency.

Then, what's been built can be used like building blocks to assemble new applications.

K2 blackpearl was created to be simple, so that non-technical people can contribute to and participate in the application-building process; and flexible, because business needs constantly shift; and fast, because time is money.

K2 blackpearl helps people create or amend process-driven applications through wizards and other graphical tools; and in most cases, no code is required. This simplicity and familiarity allows non-technical users to actually design, build and change these applications, rather than just trying to convey their needs to IT.

Because the actual definitions behind an application are not tied to the canvas or tool that created it, IT and others in the organization can work together on the same process, using skill-appropriate tools.

Envision it today. Build it today. Release it today. Change it when you need to. That's the vision behind K2 blackpearl and process-driven applications.

Process-driven applications are flexible. Visual tools for process design, rules, forms and reports allow stakeholders to easily change or adapt the applications themselves.

Process-driven applications aggregate. They pull together business processes, people, services, information and systems simply — without unnecessary complexity.

Process-driven applications can be specific to a need. But they are not necessarily independent of each other. They can share portions of process flows, rules and policies, business entities (customers, products, invoices, etc.) forms, reports, services, infrastructure, and line-of-business information.

A process-driven application can be a business process management (BPM) solution. It can be used to collaboratively model, build, deploy and manage business processes. It can be used to automate an expense claim or provision new customer accounts.

A process-driven application can be a composite application. It can be an application that brings together information, rules and policies and functional capabilities from various line-of-business systems into a single application. It can be used to build a CRM solution, manage inventory or track customer activity. A process-driven application can combine elements of a BPM solution and composite applications - allowing people to build applications that are supported by an automated process or set of processes. A process-driven application can be built to take orders and manage fulfilment or manage an HR department with processes for requesting reviews, tracking performance and managing employee information.

K2 blackpearl is about empowering those who know the business's needs best; it is about reducing the load on IT resources; and it is about ending up with on-the-mark applications that allow people to complete their work in less time with fewer mistakes.

Documentation Revision Information	
Document Title	K2 blackpearl Getting Started Guide
Product Version	4.6.6 (4.12060.1560.0)

1.2 How to use this Getting Started Guide

How to use this Guide

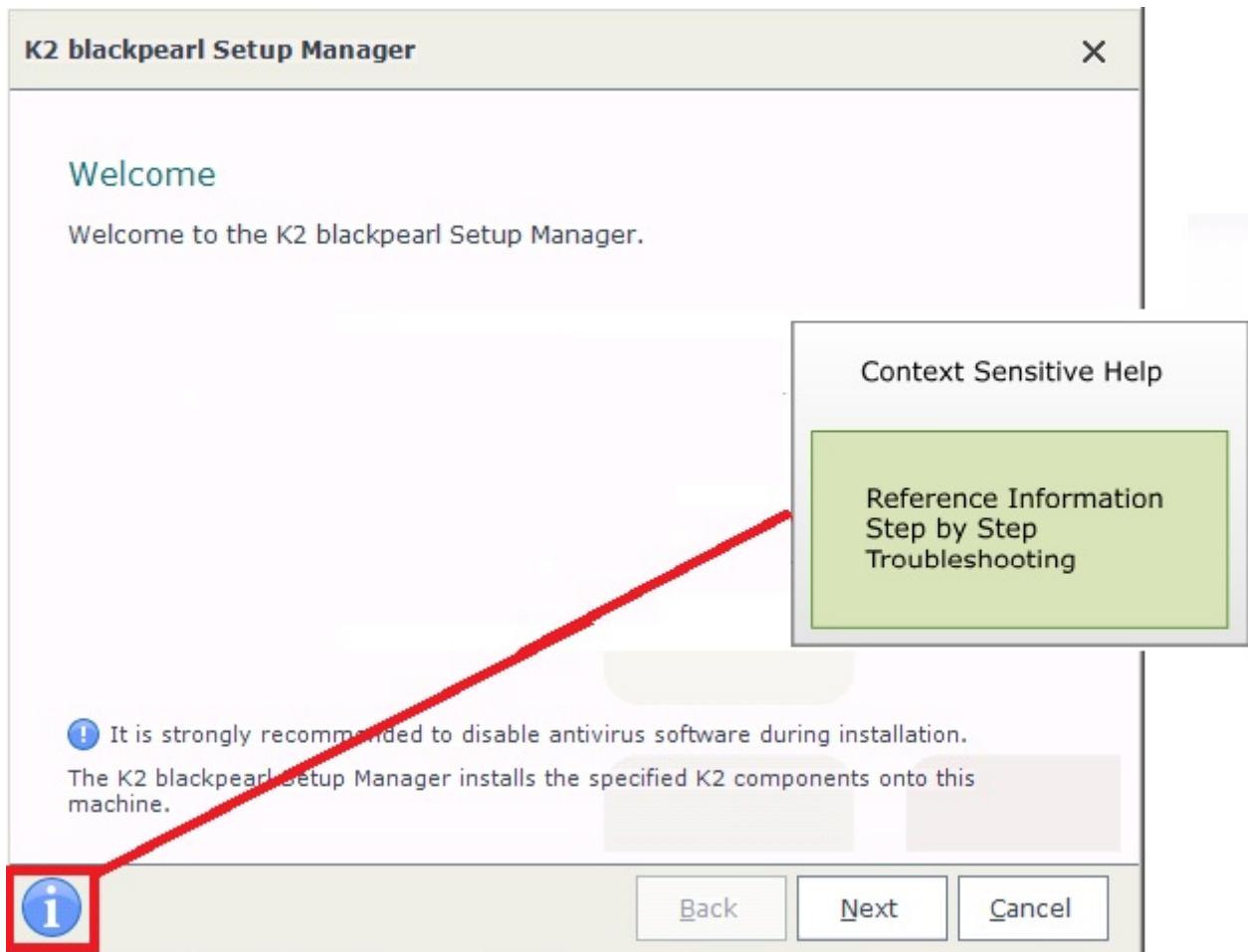
This guide is designed to provide assistance in planning and installing K2 blackpearl for the [installer](#). The Setup Manager offers context sensitive help to this guide. K2 blackpearl reference and architectural information have been provided as well to assist the installer with planning and installing K2 blackpearl.

This help file includes the following types of topics to assist the installer with details that they require:

Topic Types	
Planning	Architecture and component information to assist in the planning of the K2 blackpearl environment.
Installation and Configuration	Detailed information on installing and configuring K2 blackpearl, including prerequisites and step by step guides
Reference Topics	Reference and troubleshooting information for the K2 Setup Manager

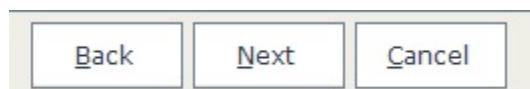
K2 I button

The I (Information) button is located on the lower left hand corner of the Setup Manager and the Configuration Manager. Clicking on the button will locate the relevant topic in the help file and launch the help for the installer to view and read.



Navigating the User Interface

The controls shown below are common controls displayed on the Setup and Configuration manager:



Installation and Configuration Manager Controls

Back Indexes to a previous screen

Next	Indexes to the next screen
Finish	This control completes the wizard when configuration details have been captured initiating either the install or configuration process
Cancel	Cancels the wizard



Depending on the context, the controls described above may be either enabled or disabled. The information in this guide will help you navigate through the Setup and Configuration manager screens.

1.3 What is new in this release

What is new in this release

New Features

Refer to the What's new in this release topic in the K2 blackpearl User guide for information on new features for this release of K2 blackpearl.

Enhancements

Refer to the What's new in this release topic in the K2 blackpearl User guide for information on any enhancement included in this release.

Bug Fixes

1. A number of bug fixes have been made to K2 components for more information read [KB001559 - High Priority Fixes for K2 4.6.6](#).

1.4 Planning the Environment

Planning the K2 Environment

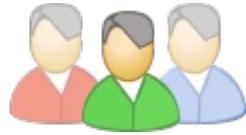
K2 provides the platform that enables developers and business users to assemble dynamic business applications from reusable items. To meet the needs of multiple industries and situations, K2 is built on the Microsoft platform and gives customers and partners the ability to work together and build applications in a familiar environment.

This section describes the various deployment scenarios of the K2 blackpearl software and discusses how to choose the scenario that best fits an organization's needs. This information will help the IT Administrator to identify the various K2 components and to familiarize themselves with installation and architectural requirements of K2 blackpearl. Along with understanding the various K2 components, it is important that the person performing the installation knows the organization's existing network and architecture.

K2 blackpearl allows for a flexible installation configuration based on an organization's needs. This section introduces eleven installation configurations. Scaling from a single server up to a large server farm, K2 blackpearl can be tuned for any architecture requirement. Because this flexibility introduces complexity, the architect of a K2 blackpearl solution should understand some basic concepts, such as Kerberos, NLB, IIS, Domain Configuration and SQL Server best practices.

Planning the Tiers

In order to plan your K2 environment, there are several tiers that need to be designed. In order to plan an effective environment with room for growth, the following sections will help you determine your needs per tier:

K2 blackpearl Tiers	
	K2 Server Tier The K2 Server can be scaled out onto multiple servers to allow for redundancy and high availability.
	Web Tier The K2 Workspace can be scaled out onto multiple servers to allow for redundancy and high availability.
	Database Tier Scaling out the K2 databases onto multiple clustered servers, or scaling out specific K2 databases onto different servers can increase performance.
	Client Tier Understanding the client tools and how to best share data and processes is part of planning the client tier.
	Development, Testing, Staging, and Production Environments Best practice in application design dictates more than one environment to be used for development and testing.

Internationalization / Worldwide English

K2 blackpearl provides full support for Worldwide English, and was also tested for Traditional Chinese, Simplified Chinese, German and French. This allows K2 blackpearl to run in English on non-English platforms. Support for non-English platforms includes the following components:



For all items listed below, clarify versioning using the [prerequisites](#) section and the compatibility matrix.

Microsoft Technology	English (Worldwide)	Chinese (Traditional & Simplified)	German	French
Windows Server 2008 R2	yes	yes	yes	yes
SQL Server 2008	yes	yes	yes	yes
SharePoint 2010 (WSS/Foundation)	yes	yes	yes	yes

Visual Studio 2010	yes	yes	yes	yes
Internet Explorer 8	yes	yes	yes	yes
Internet Explorer 9	yes	yes	yes	yes

Localization

K2 currently ships the K2 products in English (United States) and does not support localization.

There is one K2 component namely the worklist web part that is open source and the UI can be translated if required. The code is available on blackmarket on K2 Underground.



Note: Once modified, the Web Part becomes custom code and is no longer supported.

K2 Requirements

There are several hardware and software requirements regardless of the deployment scenario you choose. These are detailed in the following sections under the Prerequisites topic:

- [Hardware Requirements](#)
- [Software Requirements](#)
 - Licensing
 - Integration
 - By Component
 - By Server Role
- [Permissions for K2 Components](#)
- [Environment Configuration](#)



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.1 K2 blackpearl Components Overview

K2 blackpearl Components Overview

The K2 blackpearl components are divided into two categories, namely server components and client components. In addition to the server components, all data is stored in the K2 databases on a SQL Server instance.

- A server component is installed on a server either sharing the resources or functioning independently.
- A client component refers to the designer tools installed on a client machine, such as K2 Designer for Visual Studio and K2 Studio.
- Databases are installed on a SQL Server either locally or remotely.

The component name implies the role the component plays, but the install location may differ depending on the type of installation. For example, in the Single Server Install scenario, all of the components are installed on a single server. When installing in a distributed configuration the components are installed according to the resources they require to function.

K2 blackpearl Components Summary: Client	
K2 for Visual Studio	Design environment for developing K2 applications
K2 Studio	Design environment for developing K2 applications
K2 Designer for SharePoint	Browser based design environment for developing K2 applications
K2 blackpearl Components Summary: Server	
Server Components	Server-side components for management and operational requirements of the K2 blackpearl environment
Workspace Components	Web components supporting the Web client applications (e.g. Workspace)
K2 for SharePoint (MOSS)	Components enabling Microsoft Office SharePoint Server (MOSS) integration
K2 for SharePoint (WSS)	Components enabling Microsoft Windows SharePoint Services (WSS) integration
K2 for Reporting Services	Installed on the Reporting Services server, allows connectivity for reports
K2 blackpearl Components Summary: Shared	
K2 Documentation	Documentation resources for the K2 blackpearl product
Configuration Manager	Environment configuration application; requirement for all installation scenarios

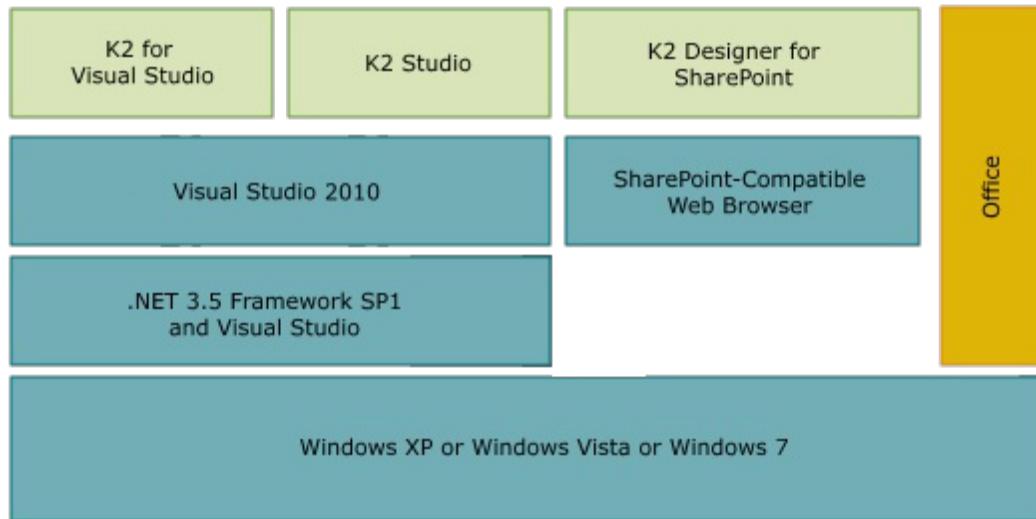


Depending on SharePoint product installed, either the K2 for SharePoint (MOSS) or K2 for SharePoint (WSS) components will be displayed for installation.

1.4.1.1 Client Components

Client

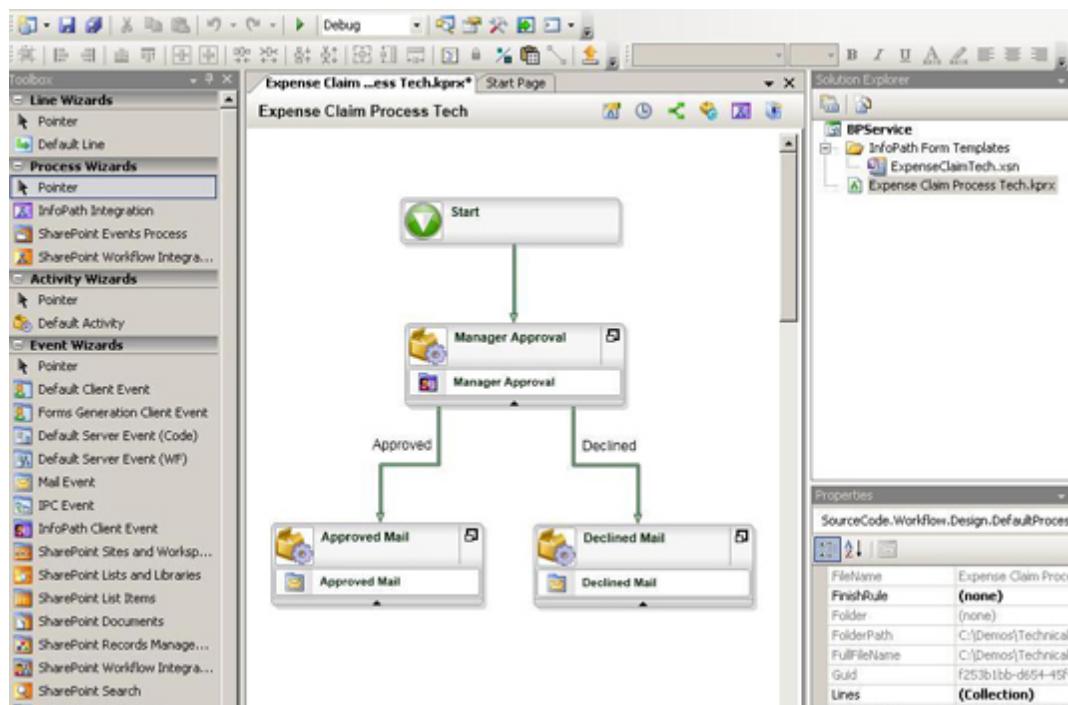
The K2 client components consist of the process designers that are installed on a client machine. The K2 designers include environments for Visual Studio 2010 and K2 designer for SharePoint. Each of these environments provide a connection to the server environment to expose information for use in building applications, such as connection variables and business entity information. In addition, the designers provide the ability to deploy new applications directly to the server environment. Multiple environments can be setup to handle the development lifecycle.



1.4.1.1.1 K2 for Visual Studio

K2 for Visual Studio

The K2 Designer for Visual Studio is a design environment for creating blackpearl applications. The K2 Designer is built on top of Visual Studio 2010 and is the workflow design tool for developers. The workflows created within the K2 Designer for Visual Studio enables integration with Microsoft Office, Microsoft InfoPath and Microsoft SharePoint, along with a number of other third-party software packages.



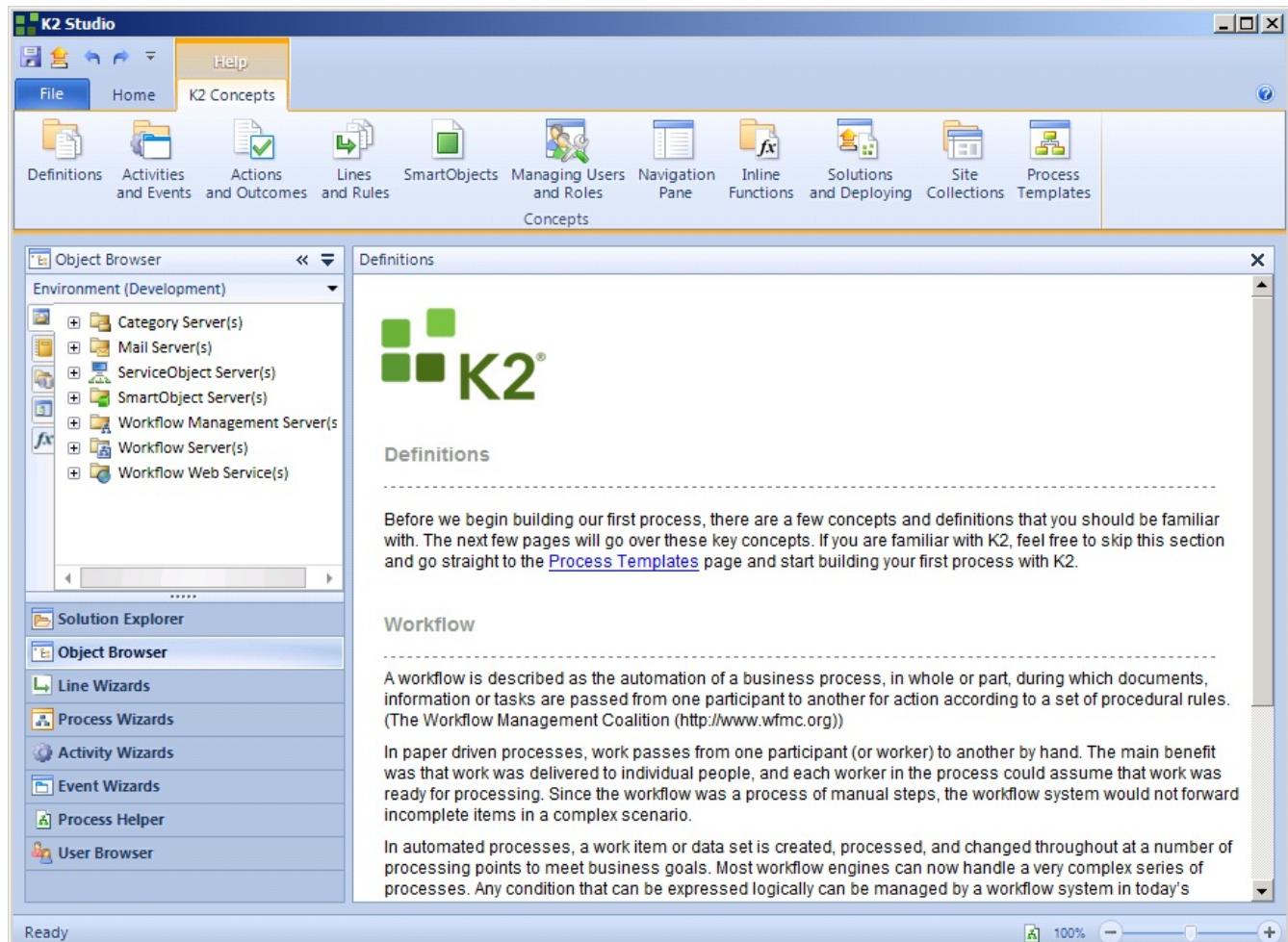
With the K2 Designer for Visual Studio, developers simply drag and drop components onto the process-design canvas. Windows Presentation Foundation-based wizards — including wizards for integrating with technologies like SharePoint, sending e-mail and displaying ASP.NET or Microsoft Office InfoPath 2007 forms — guide the developer through configuration and automatically generate the underlying definitions, Workflow Foundation schedules files, rules and activities. Developers may use a K2-provided SDK to develop their own custom wizards. Processes built in K2 are extensible. K2 leverages the .NET framework — including Windows Workflow Foundation (WF), Windows Communication Foundation (WCF) and Windows Presentation Foundation (WPF) — so developers can open and extend processes within the WF design canvas or directly through custom C# or Visual Basic code. Process debugging is available, allowing developers to access executing processes.

The K2 for Visual Studio component can be installed alone on a client machine without installing other K2 components; however, Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) with or without Sp1 is required.

1.4.1.1.2 K2 Studio

K2 Studio

K2 Studio is a "codeless" design environment for creating blackpearl applications. The K2 Designer presents similar tooling to the K2 Designer for Visual Studio environment in a familiar format utilizing a context relevant ribbon. Any projects created in this environment can be opened in K2 Designer for SharePoint or K2 Designer for Visual Studio. The workflows created within the K2 Studio enables integration with Microsoft Office, Microsoft InfoPath and Microsoft SharePoint, along with a number of other third-party software packages.



With the K2 Studio, developers simply drag and drop components onto the process-design canvas. Windows Presentation Foundation-based wizards — including wizards for integrating with technologies like SharePoint, sending e-mail and displaying ASP.NET or Microsoft Office InfoPath 2007 forms — guide the developer through configuration and automatically generate the underlying definitions, Workflow Foundation schedules files, rules and activities. Developers may use a K2-provided SDK to develop their own custom wizards. Processes built in K2 are extensible.

Process debugging is available, allowing developers to access executing processes.

1.4.1.1.3 K2 Designer for SharePoint

K2 Designer for SharePoint

K2 Designer for SharePoint is surfaced in Microsoft Office SharePoint Server (MOSS) 2007 and Microsoft SharePoint 2010 and provides the tools to build, modify and share processes in document, list and form libraries. The K2 Designer for SharePoint is hosted inside a browser. Everything that happens inside the browser for a particular process is maintained in the same project structure as a project designed in K2 Studio.

The major advantage to hosting the process designer within the browser is a broad reach to users in an organization. This allows users who do not want or need K2 Studio to participate in K2 process design. However, the browser experience is not the same as a traditional Windows-based development environment. There are many differences between the process environments, but the core features are supported in all environments.



The K2 Designer for SharePoint is only available from within a SharePoint Library, List or Form. To take advantage of this functionality, the user (or a SharePoint administrator) must activate this and the supporting features by using the K2 Administration page in SharePoint Central Administration.

1.4.1.1.4 K2 blackpearl Documentation

K2 Documentation

The documentation for K2 blackpearl includes resources for the K2 platform. This includes:

- K2 blackpearl Getting Started Guide
- K2 blackpearl User Guide
- K2 blackpearl Developer Reference

Documentation refreshes are done periodically with updates posted to the Customer and Partner portal.

1.4.1.1.5 Setup Manager

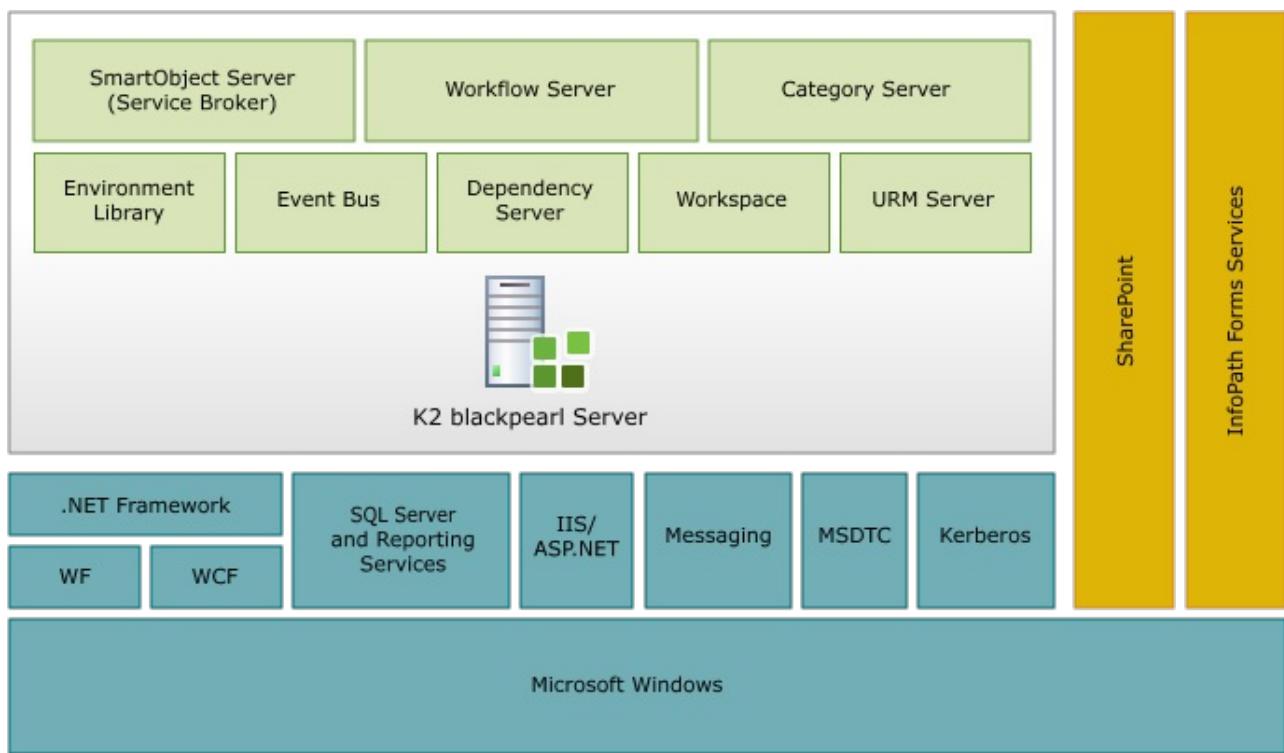
Setup Manager

The K2 Setup Manager is run by default after the K2 Setup Manager installs the selected components. The K2 Setup Manager's role is to configure the components installed on the local machine and it ensures that where connection to an external resource or service is required, the connection has been established and communication takes place. From an environmental perspective, the role of the K2 Setup Manager is to ensure that all K2 components are configured and communicate correctly so that the environment functions as required.

1.4.1.2 Server Components

Server

The K2 server components consist of the K2 Server and the other server based components that allow for integration with the various server products, such as SharePoint or Reporting Services.



1.4.1.2.1 Server Components

K2 Server

The base framework for the K2 server components is a hostable runtime environment that provides common infrastructure, such as communication, security, single sign-on, session management, logging, high availability and server component federation.

There are several server modules built into the host server that provide different pieces of functionality. Each of these modules can make use of any of the common infrastructure components and are pluggable, allowing for the separation of modules onto different machines to maximize performance. The host environment also allows developers to build their own services that can be hosted within the framework. The server modules included with the platform are:

- SmartObject Server
- Workflow Server
- Category Server
- Environment Library
- Event Bus
- Dependency Server
- User Rights Management Server

These server-side components are used for managing the operations of the K2 blackpearl environment. K2 Server is one of the principle components responsible for running the processes that are exported to it from the designers. The K2 Server requires access to its databases for the successful completion of the process instances and the successful running of the K2 Server.

1.4.1.2.2 Web Components

K2 Workspace

K2 Web components support the Web applications (e.g., Workspace). Report Design, Server Management, Workspace Security and Notification Event tasks can be accomplished in the K2 Workspace, including:

- Worklist
- Management Console (SmartObject Services, Environment Library, Workflow Server, SmartBox, Roles)
- Report Designer
- Notification Event Designer

In addition to the administrative tasks, the K2 Workspace includes the Worklist for users to see what items require their attention. This enables the client to display current and completed Worklist items and reports.

1.4.1.2.3 K2 for SharePoint

K2 for SharePoint

K2 provides several optional components that can be used with a SharePoint environment. Components are available for Windows SharePoint Services 3.0 (WSS), Microsoft Office SharePoint Server 2007 (MOSS), SharePoint 2010 Foundation and SharePoint Server 2010. The K2 for SharePoint components provide a Web-based designer that is hosted within the SharePoint environment and a K2 Worklist Web part. SharePoint wizards allow documents, lists, users and sites to be used or created based on a process. The K2 for SharePoint components also provide integration with MOSS-specific functionality, such as Records management, Publishing, Business Data Catalogue, Search and InfoPath Forms Services.

The SharePoint Components are split into two separate versions.



Only one of the following components can be installed per server. The Setup Manager will look at the dependencies and will display the correct component.

MOSS Components: Components enabling SharePoint integration with Microsoft Office SharePoint Server 2007 (Enterprise or Standard Edition), Microsoft Office Forms Server 2007

WSS Components: Components enabling Microsoft Windows SharePoint Services 3.0 integration

SharePoint 2010: Components enabling Microsoft SharePoint 2010 integration

SharePoint 2010 Foundation: Components enabling Microsoft SharePoint 2010 Foundation integration

Installed on the SharePoint machine, the K2 for SharePoint components enable interaction and communication between the K2 Server and functions found in SharePoint including Microsoft InfoPath processes. The following integration features require Microsoft Office SharePoint Server 2007 or SharePoint 2010:

- SmartObject and process data search
- Business Data Catalogue* (MOSS) or Business Connectivity Service (SharePoint 2010)
- InfoPath Forms Services*
- Publishing sites and pages
- Records management



The starred (*) features are only available in the Enterprise edition of MOSS 2007. InfoPath Forms Services integration, which provides browser-enabled InfoPath forms for user interaction, requires Microsoft Office Forms Server 2007 or the Enterprise edition of MOSS 2007.

In SharePoint 2010, forms based on browser-compatible form templates (.xsn) can be opened in a Web browser from computers that do not have InfoPath 2010 installed, but will open in InfoPath 2010 when it is installed.

The remaining integration features are available on any edition of SharePoint, including Windows SharePoint Server v3:

- K2 Designer for SharePoint
- Workflow integration
- Site management
- User management
- List and library management
- Events
- Document manipulation

1.4.1.2.4 K2 for Reporting Services

K2 for Reporting Services



Contextualized Assistance: Reporting Services Service scenario

K2 reporting tools give anyone the power to create and execute reports that meet individual needs and preferences and are based on corporate information and appropriate level of security. Common business entities are surfaced to report builders so they can access all necessary data without the need to recall where it is stored. Users can build reports for personal use or to share with others in the organization. K2 reports leverage the Microsoft Windows SQL Server 2008 or later Reporting Services platform for storing and rendering reports. This allows any Reporting Services-compatible tool, such as Business Intelligence Studio, to create and access the Report Definition Language (RDL) generated reports.

Reports can be created and rendered locally using the K2 Report Designer without SQL Reporting Services. However, it is highly recommended that SQL Reporting Services is utilized for maximum reporting capabilities, including access to out-of-the-box reports and sharing custom reports.

The K2 for Reporting Services component can be installed on an existing Reporting Services environment, but does require Microsoft SQL Server 2008 or greater.

1.4.1.2.5 K2 blackpearl Documentation

K2 Documentation

The documentation for K2 blackpearl includes resources for the K2 platform. This includes:

- K2 blackpearl Getting Started Guide
- K2 blackpearl User Guide
- K2 blackpearl Developer Reference

Documentation refreshes are done periodically with updates posted to the Customer and Partner portal.

1.4.1.2.6 Setup Manager

Setup Manager

The K2 Setup Manager is run by default after the K2 Setup Manager installs the selected components. The K2 Setup Manager's role is to configure the components installed on the local machine and it ensures that where connection to an external resource or service is required, the connection has been established and communication takes place. From an environmental perspective, the role of the K2 Setup Manager is to ensure that all K2 components are configured and communicate correctly so that the environment functions as required.

1.4.1.3 Technology Requirements

Technology Requirements



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>

Understanding the required and support technologies

The main and supporting technologies of the K2 platform. The K2 Server can be installed on Microsoft Windows 2008 Server, using .NET 3.5 SP1 and SQL Server 2008 SP1, and integrated with Visual Studio 2010, and the 2007 and 2010 Microsoft Office Systems (including Microsoft SharePoint).

Functional Roles

Microsoft Windows Server

Microsoft SQL server 2008 SP1 and Reporting Services

Microsoft Windows Vista SP1, or Microsoft Windows 7 (or later)

.NET 3.5 Technologies

Messaging

Internet Explorer 8 or 9 or 10

Microsoft Visual Studio 2010

Microsoft Office technologies

1.4.1.3.1 Functional Roles

Functional Roles



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>

There are three main K2 blackpearl functional roles that are used in this article to outline the environmental requirements.

Operators

Operators install, run and monitor the health and performance of K2 blackpearl servers.

Required for Operators

- Microsoft Windows Server 2008 R2 or newer
- Microsoft SQL Server 2008 R2 and Reporting Services
- .NET 3.5 SP1 or later
- IIS / ASP.NET
- Kerberos
- Microsoft Distributed Transaction Coordinator
- Messaging
- Microsoft Internet Explorer 8, 9 or 10

Optional for Operators

- Microsoft SharePoint Server 2010
- InfoPath Forms Services

Designers

Designers design, build and deploy dynamic business applications to K2 blackpearl servers.

Required for Designers

- Microsoft Windows Vista or later
- .NET 3.5 SP1 or later
- Microsoft Internet Explorer 8, 9 or 10

Recommended for Designers

- Microsoft Visual Studio 2010

Optional for Designers

- Microsoft Office Word, Excel and PowerPoint 2007 or later
- Microsoft Office InfoPath 2007

Users

Users leverage dynamic business applications on K2 blackpearl server

Required for Users

- Microsoft Windows Vista or later
- .NET 3.5 SP1 or later
- Microsoft Internet Explorer 8, 9 or 10

Optional for Users

- Microsoft Office Word, Excel and PowerPoint 2007 or later
- Microsoft Office InfoPath 2007

1.4.1.3.1.1 K2 blackpearl 4.5 Support for Microsoft 2008 Technologies

K2 blackpearl 4.5 Support for Microsoft 2008 Technologies

Microsoft has updated their product stack in their operating system, data storage and software development tools with the 2008 offerings. The focus of this document is to address the support that K2 offers with regards to these Microsoft product offerings and how to configure them to work with K2. Before you begin ensure that you have read this document in full before attempting your K2 installation on Windows Server 2008. Many of the configuration steps MUST be performed prior to installing K2 blackpearl.

These new releases affect the K2 blackpearl Functional Roles in the following areas.

Operators

Operators install, run and monitor the health and performance of K2 blackpearl servers.

Required for operators

- Microsoft Windows Server 2008 R2
- Microsoft SQL Server 2008 SP3
- .NET 3.5 SP1 or later
- IIS / ASP.NET
- Kerberos
- Microsoft Distributed Transaction Coordinator
- Messaging
- Internet Explorer 8 or 9 (IE 8 can be run in compatibility mode for non ie 8 compliant sites)

Designers

Designers design, build and deploy dynamic business applications to K2 blackpearl servers.

Required for Designers

- Microsoft Windows Vista SP1 or SP2 or later
- .NET 3.5 SP1 or later
- Internet Explorer 8 or 9

Recommended for Designers

- Microsoft Visual Studio 2010

1.4.1.3.1.2 Microsoft 2008 Technologies Support

Microsoft has updated their product stack in their operating system, data storage and software development tools with the 2008 offerings. The K2 Getting Started Guide has been updated with information relating to the support and configuration of certain of these Microsoft product offerings.

Ensure that you have read the updated documentation in full before attempting your K2 installation on Windows Server 2008. Many of the configuration steps MUST be performed prior to installing K2 blackpearl.

MOSS

If you are running Windows SharePoint Services (WSS) or Microsoft Office SharePoint Server (MOSS) 2007 on Windows Server 2003, and you wish to upgrade to Windows Server 2008, you must install the Office System Service Pack 1 before upgrading the operating system. If performing a clean installation of WSS or MOSS, you must install the Service Pack 1 of the installation source for WSS or MOSS.

For more information, see [Windows Server 2008 Resource Center for SharePoint Products and Technologies on TechNet](#).

WINDOWS SERVER 2008

Windows Server 2008 delivers valuable new functionality and powerful improvements to the core Windows Server operating system to help organizations of all sizes increase control, availability, and flexibility for their changing business needs. New Web tools, virtualization technologies, security enhancements, and management utilities help save time, reduce costs, and provide a solid foundation for your information technology (IT) infrastructure.

SQL 2008

Microsoft SQL Server 2008 provides a trusted, productive, and intelligent data platform that enables you to run your most demanding mission-critical applications, reduce time and cost of development and management of applications, and deliver actionable insight to your entire organization.

If more information is required refer to the following Microsoft site links for information on the respective products.
 Windows Server 2008: <http://www.microsoft.com/windowsserver2008/en/us/default.aspx>
 Microsoft SQL Server 2008: <http://www.microsoft.com/sqlserver/2008/en/us/default.aspx>

Upgrade Considerations

When upgrading from K2 blackpearl 0807 (4.8210.2.450) to K2 blackpearl 4.5 (4.10060.1.0) consider the following:

Target Microsoft Product	No K2 Product Installed	K2 blackpearl 4.5 (4.10060.1.0) Upgrade Supported K2 Product Installed
Windows Server 2003 Standard, Enterprise SP2	Clean Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions	Upgrade Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.
Windows Server 2003 R2 Standard, Enterprise SP2	Clean Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.	Upgrade Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.
Windows Server 2008 Standard, Enterprise	Clean Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.	Custom Upgrade Install – follow steps below. <ol style="list-style-type: none"> 1. Uninstall existing K2 products from all machines 2. Upgrade Windows Server 2003 to Windows Server 2008 per Microsoft upgrade instructions 3. Clean Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions and utilize existing databases.
SQL Server 2005 Express, Standard, Enterprise SP3	Clean Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.	Upgrade Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.
SQL Server 2008 Express, Standard, Enterprise RTM or SP1	Clean Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.	Custom Upgrade Install – follow steps below. <ol style="list-style-type: none"> 1. Upgrade Install – follow K2 blackpearl 4.5 (4.10060.1.0) installation instructions.

-
2. Upgrade SQL Server 2005 to SQL Server 2008 per Microsoft upgrade instructions



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.1.3.2 Microsoft Windows Server

Microsoft Windows Server 2008

Required for Operators

The K2 blackpearl Host Server and other server components require Windows Server 2008 R2, or later.

IIS / ASP.NET

Required for Operators

The K2 blackpearl Web services and Workspace Web site run from a standard, dedicated Internet Information Services (IIS) Web site. Furthermore, the extension of SharePoint is accomplished through the SharePoint central administration site, including integration with the Business Data Catalog (BDC) and the activation of the K2 Designer for SharePoint.

Kerberos

Required for Operators

The K2 blackpearl Host Server environment requires Kerberos authentication and authorization for a federated network topology where multiple pieces of the K2 blackpearl Server system are installed on different servers. Kerberos is also required if system headers route network traffic to different sites on one or more servers.

Microsoft Distributed Transaction Coordinator

Required for Operators

K2 blackpearl is a modular application that can be distributed into independent components. Transactions allow modular execution of component operations to provide failover and fault handling between K2 components. The failure of one component does not corrupt the operation of other components. To support distributed transaction management between the K2 Host Server and the SQL databases, for instance, Microsoft Data Transaction Coordinator (MSDTC) must be enabled. When working in an environment where the K2 Host Server is located on a different server than the K2 databases, Network DTC must also be enabled on both servers.

For more information on activating network DTC in Windows Server 2008 with SP2, see [Enable Network DTC access](#) or [Configuring MSDTC in a K2 Windows Server 2008 environment](#)

For more information on how to configure MSDTC in a clustered environment, see [How to configure Microsoft Distributed Transaction Coordinator on a Windows Server 2008 cluster](#).



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.1.3.3 Microsoft SQL Server & Reporting Services

Microsoft SQL Server & Reporting Services

Required for Operators

K2 blackpearl installs the operational database and builds upon the Reporting Services of Microsoft SQL Server.

SQL and Reporting Services Operational Requirements

Case sensitive databases are NOT supported.

The following collation setting is required: Latin1_General_CI_AS



The above collation setting is required for all K2 Databases.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.1.3.4 Microsoft Windows Vista or later

Microsoft Windows Vista SP1/SP2 or greater

Required for Designers and users

The K2 for Visual Studio component can be installed on Windows Vista SP1 or SP2, or later.



Note: The design tools and their associated requirements can be installed on Windows Server 2008, though installing these on a server running K2 blackpearl should only be done for development and testing purposes.

1.4.1.3.5 .NET Technologies

.NET Framework

K2 blackpearl requires both .NET 3.5 and .NET 4 and supports .NET 4.5.

The Setup Manager and K2 Workspace require .NET 3.5 to execute while K2 Studio, K2 Server and K2 for Visual Studio require .NET 4 (but also support .NET 4.5. Note that Visual Studio 2010 does not support .NET 4.5).

Note the migration issues between .NET 3.5 and .NET 4 as discussed by Microsoft here:

[http://msdn.microsoft.com/en-us/library/ee941656\(v=vs.100\).aspx](http://msdn.microsoft.com/en-us/library/ee941656(v=vs.100).aspx) and those between .NET 4 and .NET 4.5 here: [http://msdn.microsoft.com/en-us/library/hh367887\(v=VS.110\).aspx](http://msdn.microsoft.com/en-us/library/hh367887(v=VS.110).aspx) also, .NET 4.5 does not support Microsoft Windows XP.

.NET 3.5 Technologies

Required for Operators, Designers

The .NET Framework 3.5 includes a set of managed-code application programming interfaces (APIs) that is an integral part of Windows Vista SP1 or SP2 and Windows Server 2008 operating systems. The .NET Framework 3.5 includes version 3.0 of the common language runtime, so it is not necessary to install .NET Framework 3.0 before installing .NET Framework 3.5, which consists of three major components:

- Windows Presentation Foundation (WPF) is a user interface subsystem and API based on XML and vector graphics, which uses 3D graphics hardware and Direct3D technologies for an enhanced user interface.
- Windows Communication Foundation (WCF) is a service-oriented messaging system which allows programs to interoperate locally or remotely, similar to Web services.
- Windows Workflow Foundation (WF) allows for building of task automation and integrated transactions using workflows.

Windows Presentation Foundation

Windows Presentation Foundation (WPF) offers technologies that allow K2 blackpearl to solve many of the challenging technical hurdles and provide multiple design canvases, specifically the construction of visual design canvases, better use of the available on-screen real estate, and the ability to use highly visual artifacts to contextualize process-related objects for the non-developer community. For K2 blackpearl developers, an improved development experience is accomplished through a rich set of wizards and full integration with Visual Studio 2010.

Windows Workflow Foundation

Windows Workflow Foundation (WF) is not a server or an application. It is the framework used to build an application or a server with workflow capabilities. Windows WF is an in-process engine that runs inside a host process. The host process is responsible for providing a set of services to WF. A wide variety of host processes are available on the Windows platform including console applications, Windows applications, Web applications, Web services applications, SharePoint Server and NT Service applications. Effectively, any executable process can host Windows WF. K2 blackpearl makes extensive use of the WF API and is capable of hosting both managed (.NET-based) components as well as WF schedules. Out-of-the-box K2 blackpearl events generate WF schedules and provide the ability to communicate with WF schedules generated from other server products such as Microsoft Office SharePoint Server 2007 and Microsoft SharePoint Server 2010. Adherence to this common infrastructure and platform technology brings many benefits to the K2 blackpearl platform including support for pre-built WF activities and better management of underlying workflow logic. K2 blackpearl provides the tooling that allows business users to create WF-based workflows, extending its usefulness beyond the professional developer.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.1.3.6 Messaging

Messaging

Required for Operators

SMTP services are used by K2 blackpearl to send e-mail notifications. Any compatible mail server is supported, such as Windows SMTP, Exchange Server, or third-party SMTP servers that can be installed on Windows Server 2008 or later. A message queuing service is required for the K2 blackpearl Event Bus Server (K2 blackpearl supports Microsoft Message queuing out of the box). The Event Bus Server is used to watch events and send notifications on certain conditions and thresholds, providing a mechanism for reporting business activity and gathering key performance indicators (KPIs) based on current conditions in the business environment.

1.4.1.3.7 Internet Explorer

Internet Explorer

Required for Operators, Designers, Users

Internet Explorer for Windows with the latest updates and service packs, if applicable, is required for designing and running reports, browsing the task list in K2 Workspace or SharePoint, configuring events and notifications, and managing K2 blackpearl servers.

1.4.1.3.8 Microsoft Visual Studio 2010

Microsoft Visual Studio 2010 (Professional / Premium / Ultimate)

Recommended for Designers

The K2 for Visual Studio component is a licensed extension of the Microsoft Visual Studio 2010 environment. Integrated project management and debugging, multiple design views, a full-featured toolbox, and the K2 Object Browser are some of the main elements of the K2 Designer for Visual Studio hosted inside the industry-standard development environment.

1.4.1.3.8.1 Version Support and Backwards Compatibility 2010



The version of K2 Studio cited here is the version installed with K2 blackpearl.

Version Support and Backwards Compatibility

The following versions of K2 Designer client tools are supported.

- K2 Studio
- K2 Designer for Visual Studio:
 - Visual Studio 2010

The level of compatibility available depends on the starting point (i.e., the K2 Designer Client tool used to create the project originally) of the K2 Project.

Starting Designer	Target Designer	Compatibility Level
K2 Studio*	VS 2010*	Two Way

* The starting designer and the target designer are interchangeable, with the same compatibility level of support available

1.4.1.3.9 Microsoft Office technologies

Microsoft Office Technologies

The Office servers and clients that are listed here are optional components with which K2 blackpearl can integrate. Specific components of the 2007 Office system are optional for different roles, as described in the following sections.

Microsoft Office SharePoint Server 2007 & Windows SharePoint Services v3

Optional for Operators

Integration with MOSS 2007 and WSS v3 provides site and user management, content management, and data reporting from within the familiar SharePoint user interface. K2 blackpearl provides custom wizards and templates for different types of sites, such as Publishing sites and Records Centers. Document management is not limited to a single site. Documents can be moved to entirely different sites on different servers, if the process requires it. The K2 blackpearl SharePoint integration also includes security and rights management, SmartObject-data viewing through the Business Data Catalog (BDC), and the rendering of K2 blackpearl InfoPath forms in a browser by InfoPath Forms Services. The following integration features require Microsoft Office SharePoint Server 2007:

- SmartObject and process data search
- Business Data Catalog*
- InfoPath Forms Services*
- Publishing sites and pages
- Records Management



The starred (*) features are only available in the Enterprise edition of MOSS 2007. InfoPath Forms Services integration, which provides Browser-enabled InfoPath forms for user interaction, requires Microsoft Office Forms Server 2007 or the Enterprise edition of MOSS 2007. The remaining integration features will work with any edition of SharePoint, including Windows SharePoint Server v3:

- K2 Designer for SharePoint
- Workflow integration
- Site management
- User management
- List and library management
- Events
- Document manipulation

Microsoft SharePoint Server 2010

K2 for SharePoint 2010 makes use of the new functionalities provided in SharePoint 2010 to perform the same functionality available in the K2 for SharePoint 2007. However, there are new functionalities or some technologies previously used and supported in K2 for SharePoint 2007 that are no longer supported in K2 for SharePoint 2010. For more details, see [K2 for SharePoint 2010 Introduction](#).

InfoPath Forms Services

Optional for Operators

InfoPath Forms Services (IPFS), included as part of Microsoft Office SharePoint Server 2007 Enterprise edition or Microsoft Office Forms Server 2007, is required to render InfoPath forms in the browser. IPFS is also required to display custom InfoPath-based workflow forms in Office applications.

Note: A corresponding version of Office 2007 is also required to enable this functionality. The Pro Plus, Enterprise and Ultimate versions include the ability to show custom InfoPath-based workflow forms, the Message Bar, and the Workflows menu item in Word, Excel, PowerPoint and InfoPath.

Microsoft Office Word, Excel & PowerPoint 2007

Optional for designers, Users

The applications of the 2007 Microsoft Office System, Word, Excel, PowerPoint and InfoPath, are capable of displaying workflow notifications in the Message Bar. This allows a user to open a document that is part of a workflow and perform actions within the application. Furthermore, if the workflow forms are based on InfoPath, these applications can display the form above the current document. If the workflow uses ASP.NET forms, users are taken to the site or the form is displayed in a workflow dialog box.

1.4.2 K2 Architecture

K2 Architecture

The overall K2 architecture includes Microsoft components and K2 blackpearl-hosted server components. Depending on the role a server plays in the deployment, all or some of these components will be installed. At a high level, the K2 blackpearl Server uses common Microsoft components, such as the .NET 3.5 Framework with SP1, which includes Windows Workflow Foundations (WF) and Windows Presentation Foundation (WPF). These components are shown logically in Figure 1 for server components and in Figure 2 for client components. The K2 blackpearl components are discussed in further detail in the following two topics.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

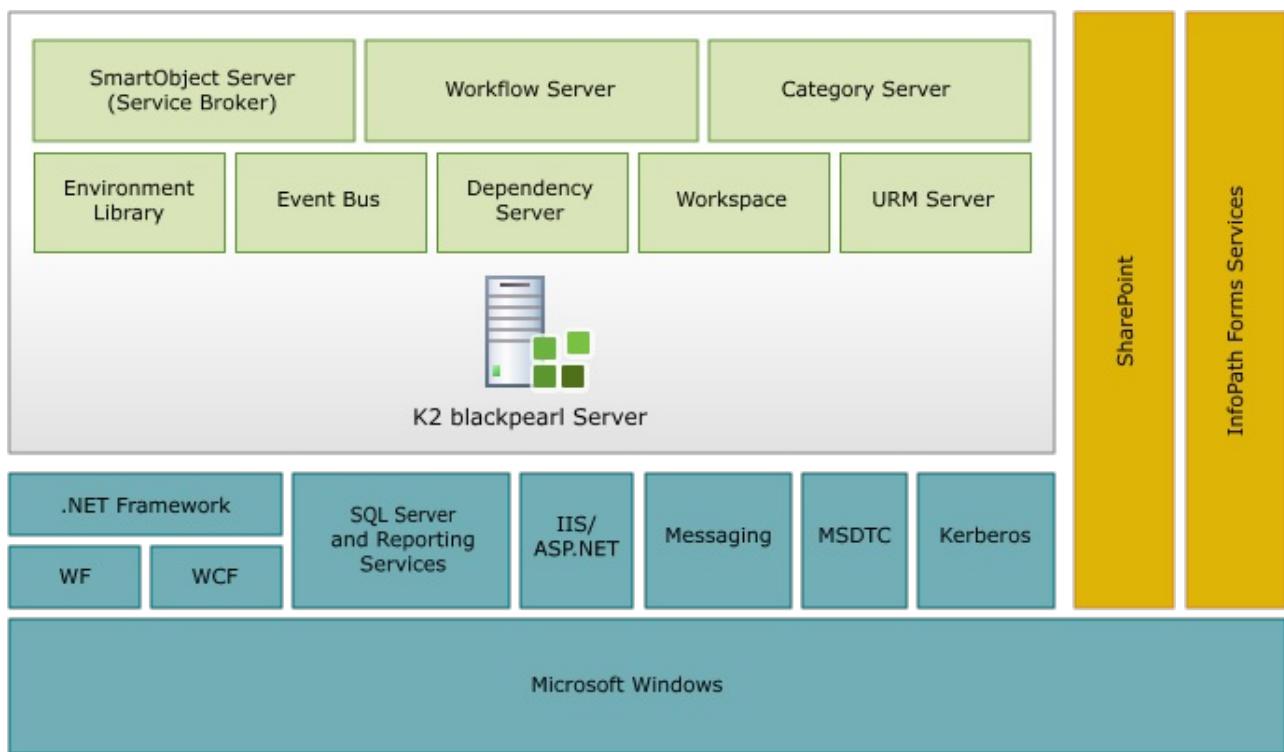
1.4.2.1 K2 Architecture: Server

K2 Architecture: Server

The K2 Server is a sophisticated yet flexible platform which leverages Microsoft Components for its operation. The K2 Server can be configured for Standalone, Distributed (Single Server) and Distributed (NLB or K2PTA).

As can be seen from the diagram below, the K2 Server leverages a number of Microsoft based technologies to facilitate framework support and integration, data storage and retrieval, web based content and services, messaging and user authentication. The K2 Server's flexibility is further extended to the end user writing custom components which can be integrated with the system for example custom user managers.

The K2 SmartObject Server; which forms the basis the data layer between K2 Server and 3rd party products enables the K2 Server to interact real time with external systems for example SAP.



Server architectural components, Microsoft server components (blue), the K2 hosted servers (green, horizontal) and optional server components for integration (yellow, vertical)

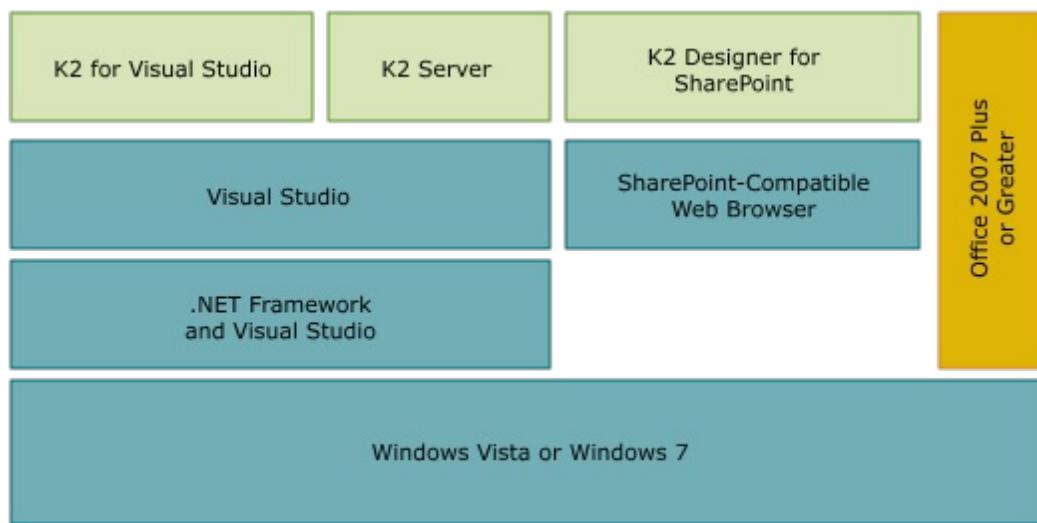
1.4.2.2 K2 Architecture: Client

K2 Architecture: Client

The K2 Client Architecture utilizes Microsoft Client based technologies to interact with users to 1) author processes 2) enables Information Workers to interact with the K2 Server to complete their assigned tasks.

K2 Process Designers will use any one of the K2 Designers which are sophisticated and flexible design environments (the K2 Designers on offer include two standard local run desktop options and a web based, light client offering as well). The K2 Designers enable the authoring of processes which enable human to system or system to system orientated interaction.

Information workers can be notified by e-mail or use their tasklist to keep up to date with their latest task list items. Actioning a task list item can be accomplished using the out of the box workspace or a worklist hosted in SharePoint. An e-mail approval system is also available enabling Information Workers to interact with the K2 Server directly via e-mail to action a tasklist item.



Client architectural components, Microsoft client components (blue), the K2 blackpearl design environments (green, horizontal), and the optional components (yellow, vertical)

1.4.3 Deployment Scenarios

K2 Supported Topologies

The preceding sections have enabled the installer to identify various K2 components and to familiarize themselves with installation and architectural requirements. The following section assists the installer with deciding which scenario to pursue with regards to installing K2 blackpearl. K2 is a robust n-tiered enterprise application which can be configured by the installer to integrate with their existing environment.

This deployment planning guide offers guidance for determining the type of installation best suited to specific environments.

To decide which scenario will work for an organization, the person installing K2 blackpearl must be familiar with the network and requirements. It is important that once reviewed, the installer uses the content within this document to determine which scenario is the most suitable and how it will impact the network. A decision chart follows this section, use the chart as a guide to make the appropriate decision.

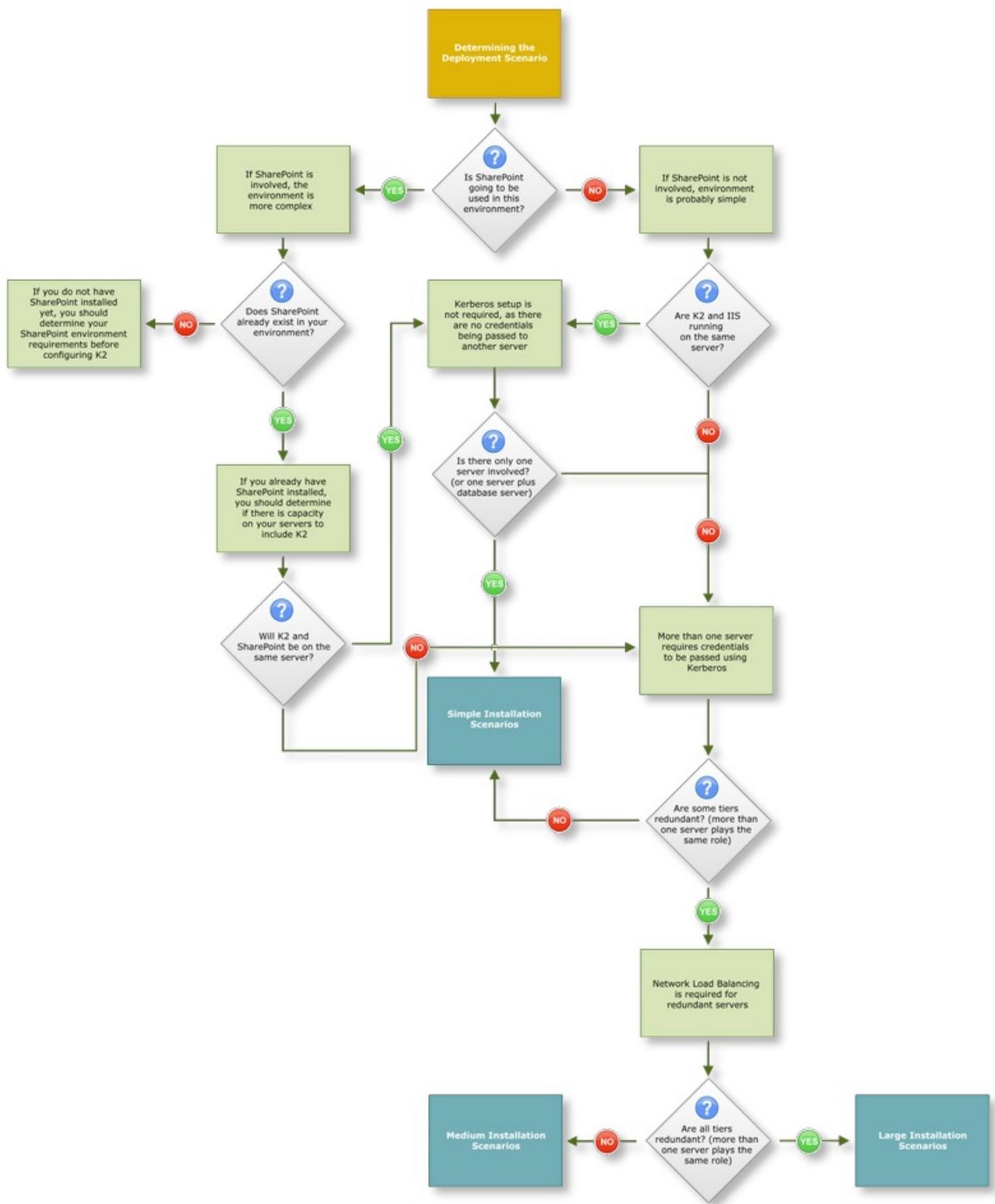
These scenarios are for production environments. It is important to note that many larger organizations will also have development and staging environments to test new systems and processes. It is strongly advised that the test environment (and ideally the development environment as well) are configured identically to the production environment.

This flowchart should help in deciding which of the following types of installation is appropriate:

- **Simple Installation Scenarios:** Small scale installations, with little or no redundancy
 - [Standalone Install](#)
 - [Small Scale Install](#)
 - [Scaling for Data Availability](#)
 - [Scaling for Better Performance](#)
- **Medium Installation Scenarios:** Medium scale installations, with some redundancy
 - [Scaling for Page Rendering](#)
 - [Scaling for Data and Performance](#)
 - [Medium Scale Install](#)
 - [Maximum Redundancy on Six Servers](#)
- **Large Installation Scenarios:** Fully redundant installations
 - [Large Scale Install](#)
 - Segmentation by Site Collections
 - Multiple SharePoint and K2 farms



The following diagram assumes that SharePoint is already installed and configured in the environment. The initial installation of K2 blackpearl can be performed without SharePoint components. After SharePoint is introduced to the environment, the SharePoint components (either MOSS or WSS) can be installed on those servers. However, this document assumes that SharePoint is already configured and used by the organization.



1.4.3.1 Standalone Install

Standalone Install

Standalone installations are better suited for low-load environments such as a development or proof of concept environment. Since all components are installed on the same physical server as the K2 Server, there are no credentials passed between servers.

Standalone Install	
Server A	K2 blackpearl (all components)* Internet Information Server (IIS) SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation) SQL Server 2008

 Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

The **Standalone Installation** configuration for K2 blackpearl is shown below. All K2 components, IIS, SharePoint, and the database instance are installed on the same physical platform.



Considerations for the Standalone Install

When all K2 components are installed on a single, standalone server there are performance related issues that need to be considered. Although all components on a single machine will mitigate security requirements, there will be an impact on the processing capabilities of the physical machine.

If this installation scenario is used for a development or proof of concept environment, it is recommended that additional RAM or a faster processor is used in order to maintain an acceptable level of performance.

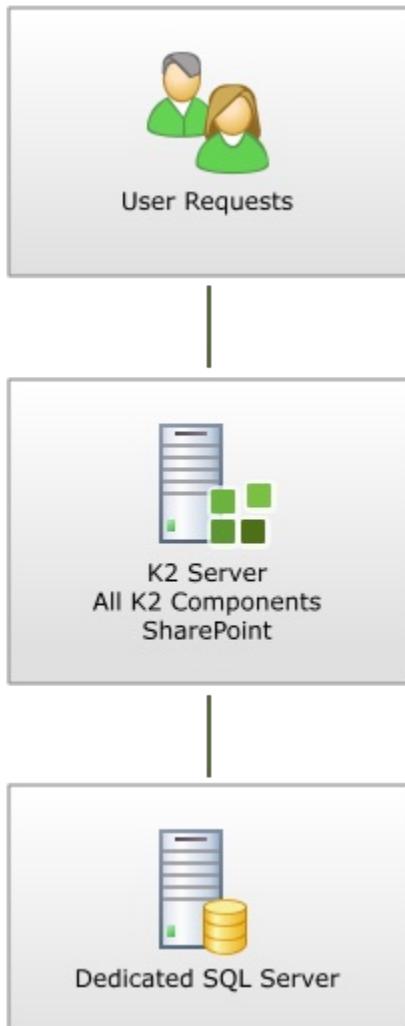
1.4.3.2 Small Scale Install

Small Scale Install

In many cases K2 blackpearl is installed into an existing infrastructure; therefore, the database components can be easily installed on an existing SQL server. This is true even when all K2 components are installed on an existing server which is likely running WSS. This is suitable for small usage, such as a test or training environment.

Small Scale Install	
Server A	K2 blackpearl (all components)* Internet Information Server (IIS) SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation) or later
Server B	SQL Server
 Note: Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.	

The **Small Scale Install** configuration for K2 blackpearl is shown below. All K2 components, IIS, SQL Reporting Services, and SharePoint are installed on one server, and the databases are located on a separate server.



Considerations for the Small Scale Install

For small scale installations, hardware and SQL Server considerations must be taken into account.

Hardware

If this installation scenario is used, it performs best as a development or proof of concept environment. It is

recommended that additional RAM or a faster processor is used in order to maintain acceptable levels of performance.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources or be located on an independent platform, such as this small scale install. Considering that in most cases K2 is being introduced into an existing environment, the K2 Databases would be installed on an independent server that runs SQL Server.

1.4.3.3 Scaling for Data Availability

Scaling for Data Availability

Since many business critical processes may be automated using K2 blackpearl, it may be important to have a redundant system for data availability. This scenario is the same as the Small Scale install, but with a SQL cluster as the database back-end rather than a single server.

Scaling for Data Availability Install	
Server A	K2 blackpearl (all components)* Internet Information Server (IIS) SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation)
Server B, C	SQL Server (Clustered)



Note: Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

The **Scaling for Data Availability** scenario is shown below. All of the IIS, K2, SQL Reporting Services, and SharePoint components are installed on one server, with a clustered SQL server instance for data redundancy.



Considerations for the Scaling for Data Availability Install

For this installation topology, the SQL Server configuration needs to be evaluated.

SQL Server

The SQL Server can share physical resources or be located on an independent platform, such as in this install, or it can be clustered. For more information regarding SQL Server clustering, refer to the SQL planning and architecture documentation (<http://technet.microsoft.com/en-us/sqlserver/bb331768.aspx>).

Considering that in most cases K2 is being introduced into an existing environment, the K2 Databases would be installed on an existing SQL Server cluster. It is important that the **DTC component is configured properly** in order for communications between the K2 Server and the SQL Server can function properly.

If SQL Server Reporting Services is installed on a separate server, then Kerberos will need to be configured for communications between the K2 Server and Reporting Services.

1.4.3.4 Scaling for Better Performance

Scaling for Better Performance

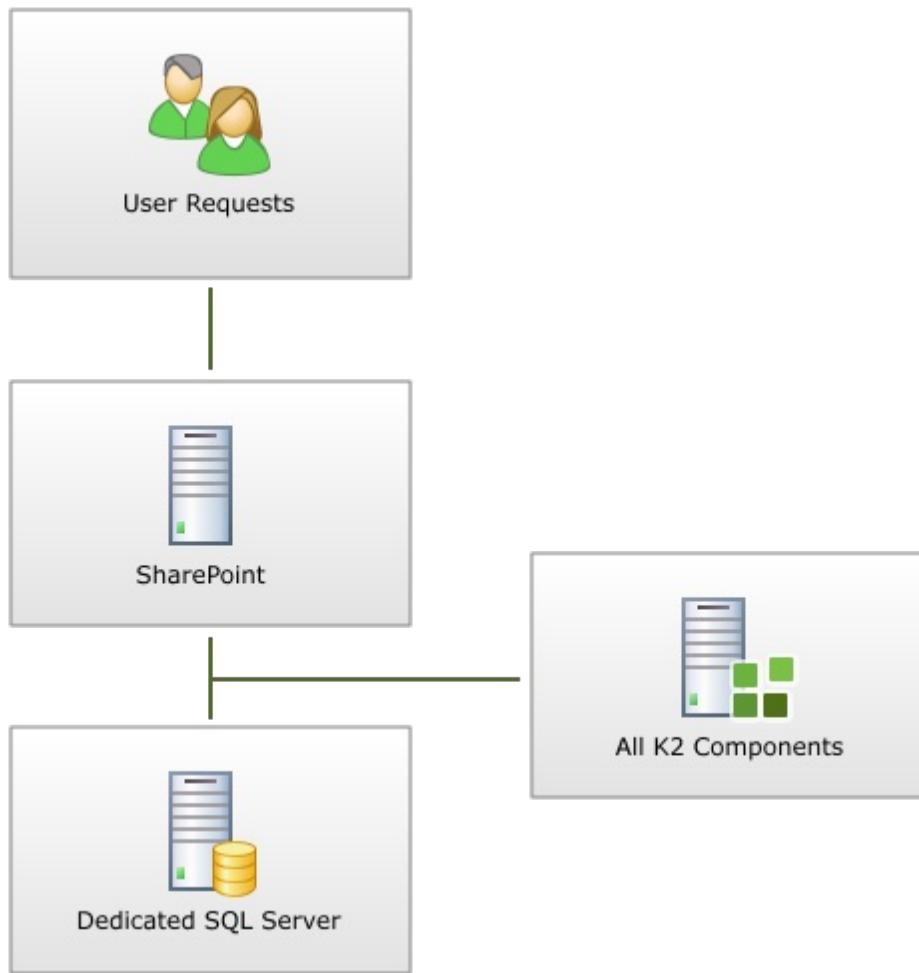
This scenario is better suited for small organizations that do not require any redundancy. Although able to support an increasing load on the K2 infrastructure, the K2 Server is separated from the SharePoint server for scalability.

Scaling for Better Performance Install	
Server A	SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation)
Server B	K2 blackpearl (all components)* Internet Information Server (IIS)
Server C	SQL Server



Note: Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

The **Scaling for Better Performance** scenario is shown below. All of the K2 components are separated out from the SharePoint components, with a separate SQL server.



Considerations for the Scaling for Better Performance Install

Since this scenario deploys the various components onto multiple servers, there are some considerations around Kerberos and location of the components that should be addressed.

Kerberos



The default method for user authentication for new distributed installations is K2 Pass-Through Authentication: [Introduction](#) Kerberos is still supported.

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. Whenever credentials must pass more than one “hop” between servers, Kerberos must be configured. This is known as the “double-hop issue.”

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources or be located on an independent platform, such as in this install. Considering that in most cases K2 is being introduced into an existing environment, the K2 Databases would be installed on an independent server that runs SQL Server 2008. Since this is a common occurrence, the installation documentation takes this into consideration.

K2 Workspace

Clients access Workspace via the IIS Server operating from the K2 Server. If the user environment expands so that the performance of the K2 Server is affected by the number of users logging onto K2 Workspace, it is advised that the IIS components be relocated to a different server.

1.4.3.5 Scaling for Page Rendering

Scaling for Page Rendering

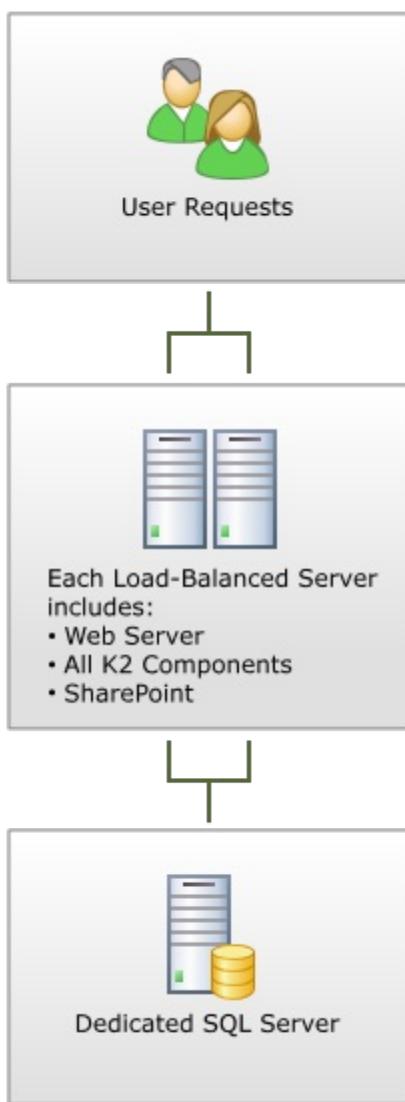
Since many business-critical processes may be automated using K2 blackpearl, it may be important to have a redundant system to ensure processes are not interrupted. This scenario is the same as the Small Scale install, but with adding a Network Load Balanced (NLB) cluster to ensure failover via load balancing.

Scaling for Page Rendering	
Server A, B	NLB SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation) and IIS NLB K2 blackpearl (all components)
Server C	SQL Server 2008



Note: Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

The **Scaling for Page Rendering** scenario is shown below. All of the K2, IIS, and SharePoint components are installed on two nodes in an NLB cluster for better page rendering performance and fail over via load balancing.



Considerations for the Scaling for Page Rendering Install

This scenario introduces a NLB cluster into the installation topology; therefore, it is important to understand NLB before installing this scenario.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources or be located on an independent platform, such as in this install. Considering that in most cases K2 is being introduced into an existing environment, the K2 Databases would be installed on an independent server that runs SQL Server 2008. Since this is a common occurrence, the installation documentation takes this into consideration.

1.4.3.6 Scaling for Data and Performance

Scaling for Data and Performance

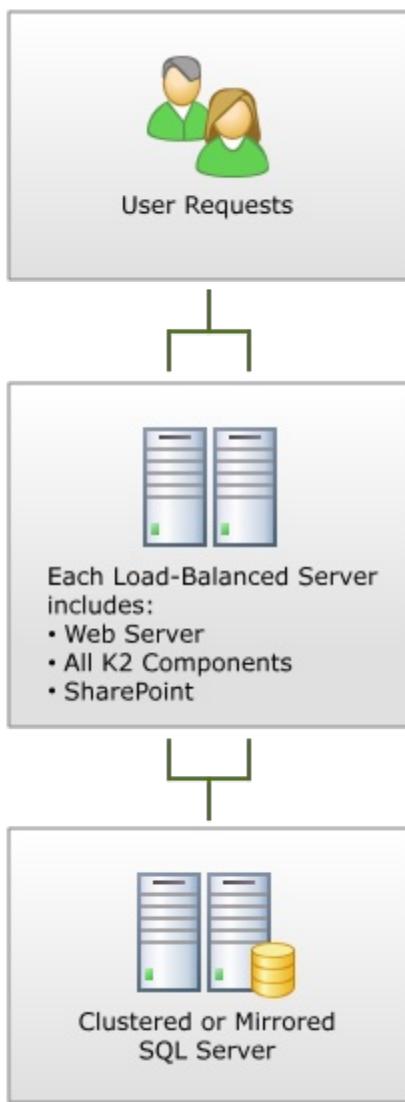
Both the Scaling for Page Rendering and Scaling for Data Availability scenarios start to address redundancy into the system. This scenario addresses both the data availability, by adding a SQL cluster into the infrastructure, as well as failover via load balancing on the other components.

Scaling for Data and Performance	
Server A, B	NLB SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation) and IIS NLB K2 blackpearl (all components)
Server C, D	Clustered SQL Server



Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

In the figure below, the **Scaling for Data and Performance** scenario is shown. There is a SQL cluster, and all IIS, SharePoint, SQL Reporting Services, and K2 components are on an NLB cluster.



Considerations for the Scaling for Data and Performance Install

This scenario introduces a NLB cluster into the installation topology; therefore, it is important to understand NLB before installing this scenario.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it also can be clustered. For more information regarding SQL Server clustering, refer to the SQL Server Failover Clustering documentation (<http://msdn.microsoft.com/en-us/library/ms189134.aspx>)

In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

1.4.3.7 Medium Scale Install

Medium Scale Install

K2 blackpearl is a scalable platform, wherein the K2 Server can be separated from the SharePoint and IIS components. This allows for a Web farm to be set up for better rendering performance, and it lessens the impact of client requests through IIS on the K2 Server.

Medium Scale Install.

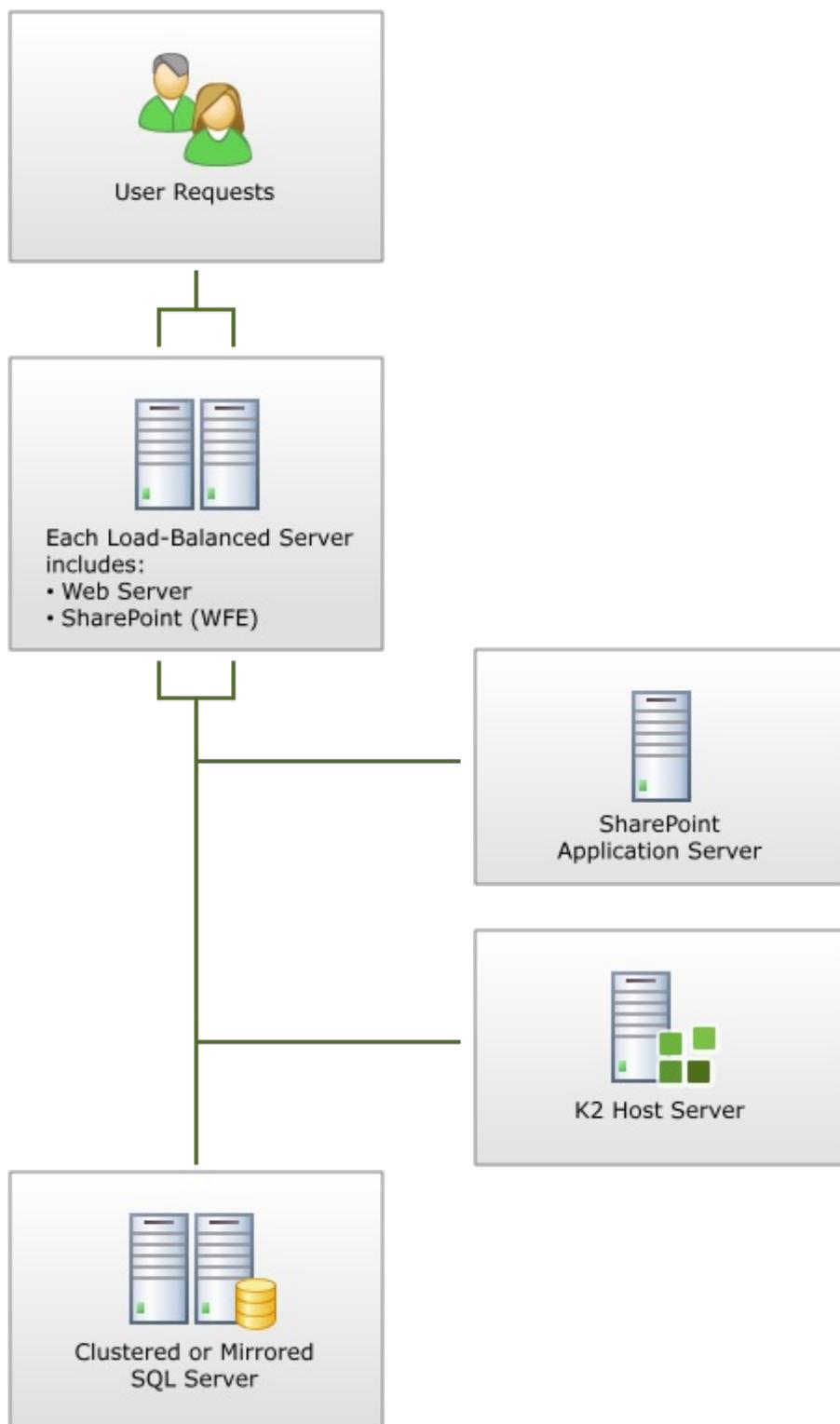
Scaling for Medium Scale Install	
Server A	NLB SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation)
Server B	NLB K2 blackpearl (all components)
Server C	MOSS Application Servers
Server D	Clustered SQL Server



Note: Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

Also depending on your SharePoint environment, the application servers such as Excel Services, InfoPath Server, and Indexing can be split off onto a separate server. Refer to the SharePoint installation guidance for installation options. This server will not be needed if only WSS is installed.

The figure below shows the **Medium Scale Install** scenario. K2 has its own dedicated server separating it from an NLB cluster set up for SharePoint and IIS. A SQL cluster is also introduced for data redundancy.



Considerations for the Medium Scale Install

By scaling out this install, there are several considerations such as Kerberos and NLB that should be addressed.

Kerberos



The default method for user authentication for new distributed installations is K2 Pass-Through Authentication (see the [Introduction to Kerberos here](#)) Kerberos is still supported.

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. As discussed earlier, whenever credentials must pass more than one "hop" between servers, Kerberos must be

configured. This is known as the “double-hop issue.”

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, the SharePoint and Web components are on NLB servers, therefore, these components need to be installed on each NLB server.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it also can be clustered. For more information regarding SQL Server clustering, refer to the SQL planning and architecture documentation (<http://technet.microsoft.com/en-us/library/ms157293.aspx>).

In most cases K2 databases are installed on an established SQL Server 2008 cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

K2 Workspace

Clients access Workspace via the IIS Server operating from the K2 Server. If the performance of the physical server is affected by the number of users logged into K2 Workspace, it is advised that the IIS be relocated to an independent hardware platform.

1.4.3.8 Maximum Redundancy on Six Servers

Maximum Redundancy on Six Servers

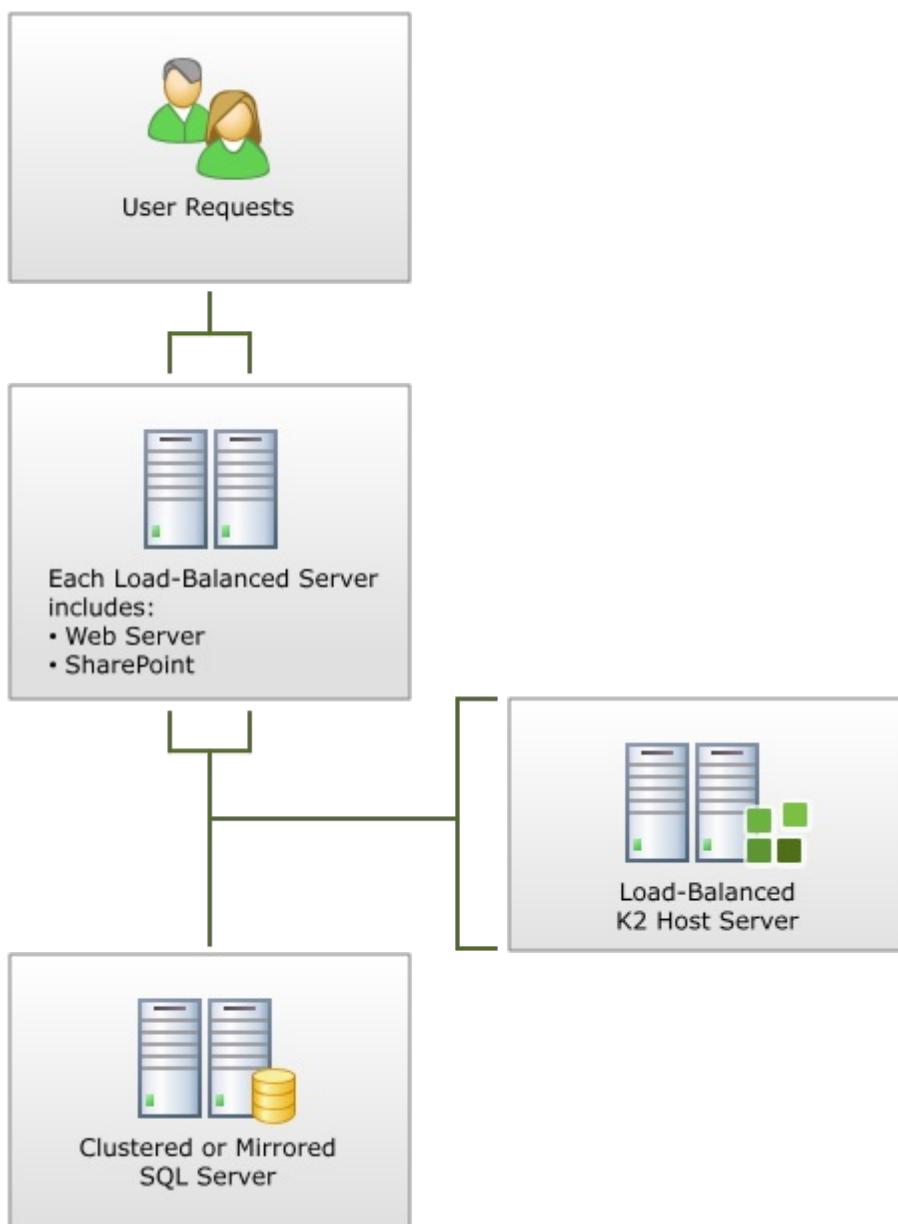
This topology adds maximum availability on the fewest number of servers. This scenario is intended for organizations that require redundancy of all application server roles. Having an NLB cluster for the K2 Server and a separate NLB cluster for the Web tier maximizes its availability and performance. A SQL cluster also allows for data redundancy.

Maximum Redundancy on Six Servers Install	
Server A, B	NLB SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation) and IIS
Server C, D	NLB K2 blackpearl (all components)
Server E, F	Clustered SQL Server



Note: Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation...

The **Maximum Redundancy on Six Servers** install scenario is shown below.



Considerations for the Maximum Redundancy on Six Servers Install

This installation brings the complexity of Kerberos and NLB to the scenario.

Kerberos



The default method for user authentication for new distributed installations is K2 Pass-Through Authentication (see the [Introduction to Kerberos here](#)) Kerberos is still supported.

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. As discussed earlier, whenever credentials must pass more than one “hop” between servers, Kerberos must be configured. This is known as the “double-hop issue.”

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be accomplished before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, the SharePoint and Web components are on NLB servers, therefore, these components need to be installed on each NLB server. Additionally, the K2 Server resides on NLB servers, therefore each NLB server needs the K2 Server installation.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it can be clustered. For more information regarding SQL Server clustering, refer to the SQL Server Failover Clustering documentation (<http://msdn.microsoft.com/en-us/library/ms189134.aspx>)

In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a likely occurrence and the installation documentation takes this into consideration.

1.4.3.9 Large Scale Install

Large Scale Install

The Large Scale Install scenario is specifically suitable for high work load environments, with components scaled to three tiers. Each component is load balanced, and multiple dedicated databases allow for maximum growth and availability. Multiple databases are dedicated to individual load-balanced components to allow for maximum growth and availability. Kerberos is mandatory for this configuration option. Both NLB and Kerberos must be configured correctly and must be able to communicate before K2 blackpearl is installed.

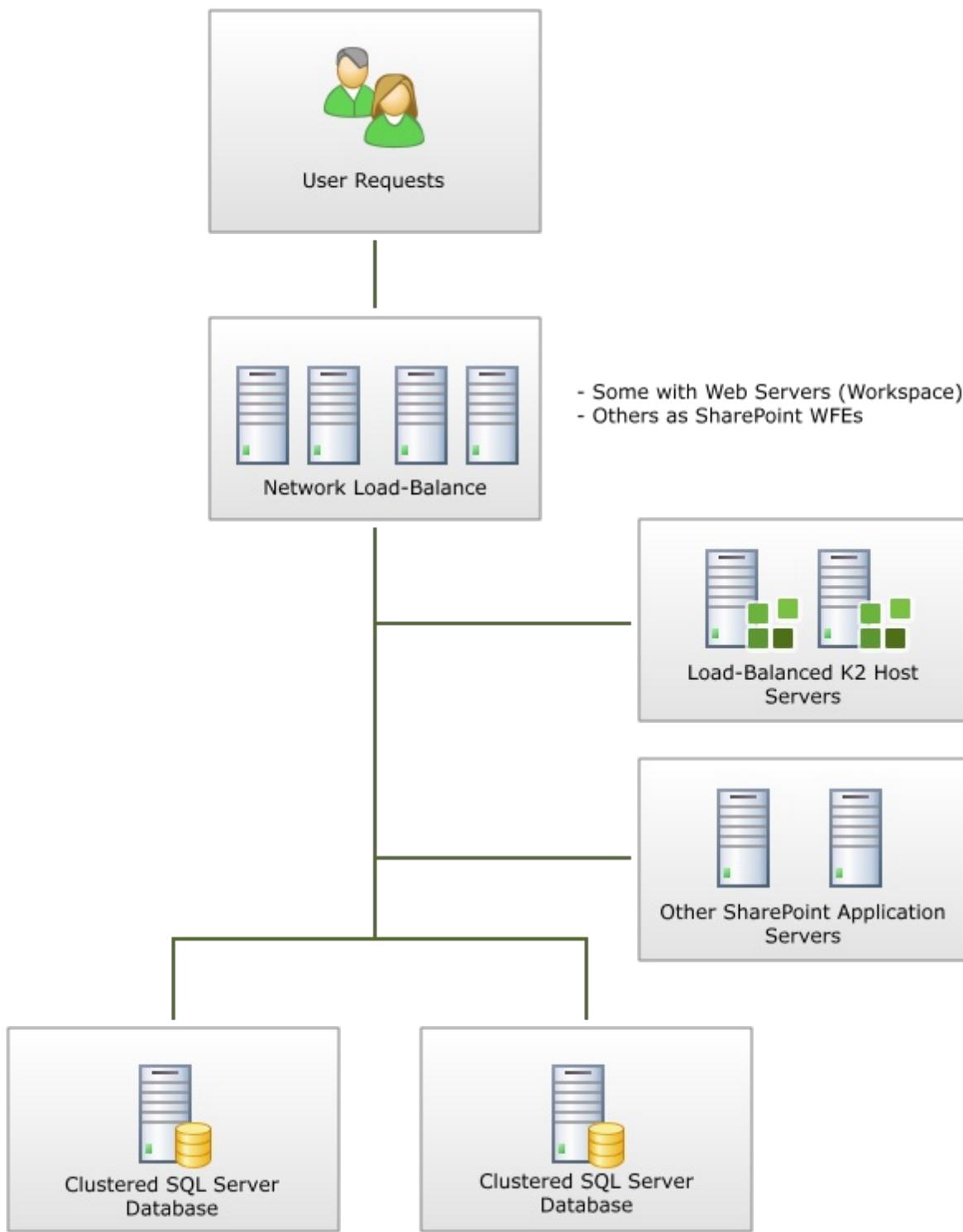
Large Scale Install	
Server A, B	NLB SharePoint 2007 (MOSS or WSS), SharePoint 2010 (Server or Foundation) NLB IIS with K2 Workspace components
Server C, D	NLB K2 blackpearl Servers
Server E, F	MOSS Application Servers
Server G, H	Clustered SQL Server



Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

Also depending on your MOSS environment, the application servers such as Excel Services, InfoPath Server, and Indexing can be split off onto a separate server. Refer to the SharePoint installation guidance for installation options. These servers will not be needed if only WSS is installed.

The **Large Scale Install** scenario is shown below. Not all of the SharePoint features are shown here. Refer to the SharePoint documentation for installation guides and options.



Considerations for the Large Scale Install

While the diagram shows one topology, each tier can be scaled out depending on needs. However, Kerberos and NLB will factor into this scenario.

Kerberos



The default method for user authentication for new distributed installations is K2 Pass-Through Authentication (see the [Introduction to Kerberos here](#)) Kerberos is still supported.

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. As discussed earlier, whenever more than two hops are required, Kerberos must be configured.

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on [Kerberos](#) later in this help file.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, each load-balanced component should have the full install on each NLB node.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the [DTC component is configured properly](#) in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it can be clustered. For more information regarding SQL Server clustering, refer to the SQL Server Failover Clustering documentation (<http://msdn.microsoft.com/en-us/library/ms189134.aspx>)

In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

1.4.3.10 Segmentation by Site Collection

Segmentation by Site Collection

Building on previous topology descriptions, this install scenario can be used where there is natural segmentation by Site Collection within a SharePoint farm. The expected volumes would be similar to a single farm installation, however as there are multiple farms scaled independently, there is near limitless ability to scale.

Similar to the Large Scale Install scenario, this scenario is specifically suitable for high work load environments. Each component is load balanced, and multiple dedicated databases allow for maximum growth and availability. Multiple databases are dedicated to individual load-balanced components to allow for maximum growth and availability.

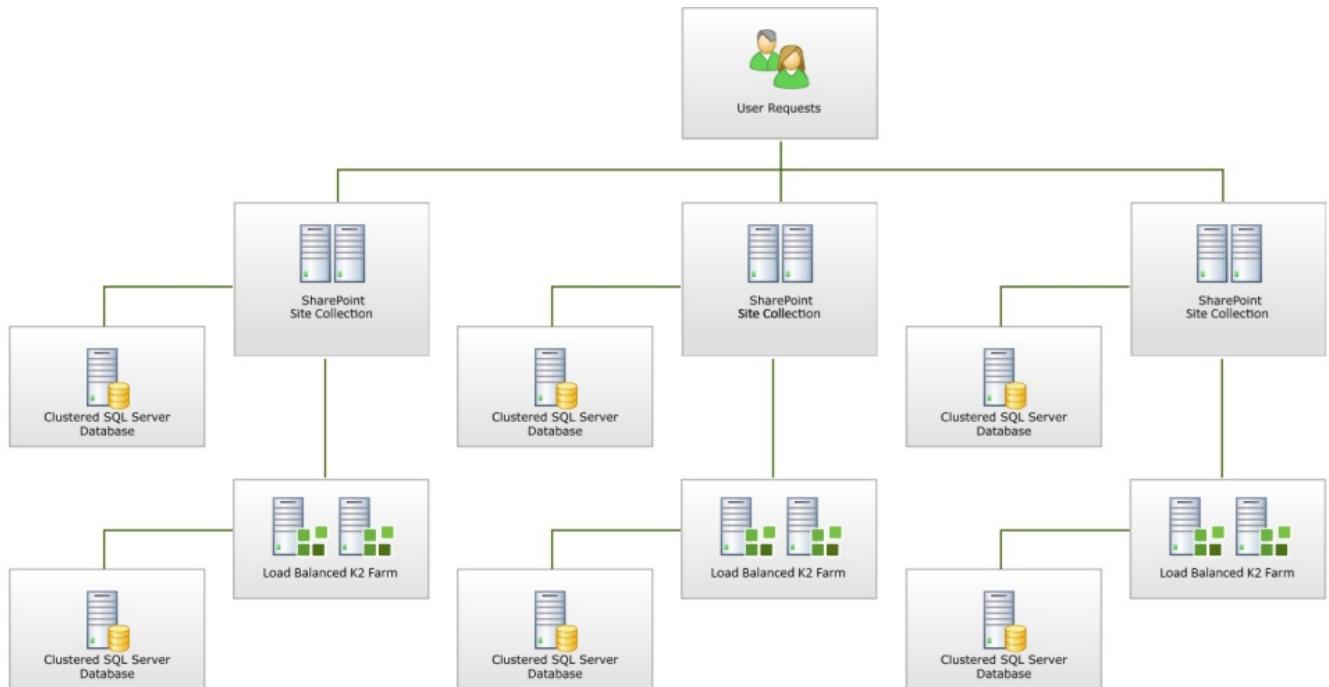
Kerberos is mandatory for this configuration option. Both NLB and Kerberos must be configured correctly and must be able to communicate before K2 blackpearl is installed.



Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

Also depending on your MOSS environment, the application servers such as Excel Services, InfoPath Server, and Indexing can be split off onto a separate server. Refer to the SharePoint installation guidance for installation options. These servers will not be needed if only WSS is installed.

The **Segmentation by Site Collection Install** scenario is shown below. Not all of the SharePoint features are shown here. Refer to the SharePoint documentation for installation guides and options.



Considerations for the Segmentation by Site Collection Install

- Each site collection can only work with a single K2 farm.
- This model works very well if there are different project loads across site collections and/or geographic issues as the underlying K2 architecture can be scaled separately.
A custom K2 worklist and reporting needed if there is a desire to aggregate data across K2 farms in a single view.
- While the diagram shows one topology, each tier can be scaled out depending on needs. However, Kerberos and NLB will factor into this scenario.

Kerberos



The default method for user authentication for new distributed installations is K2 Pass-Through Authentication (see the [Introduction to Kerberos here](#)). Kerberos is still supported.

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. As discussed earlier, whenever more than two hops are required, Kerberos must be configured.

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, each load-balanced component should have the full install on each NLB node.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it can be clustered. For more information regarding SQL Server 2008 clustering, refer to the Getting Started with SQL Server 2008 Failover Clustering documentation (<http://msdn.microsoft.com/en-us/library/ms189134.aspx>)

In most cases K2 databases are installed on an established SQL Server 2008 cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

1.4.3.11 Multiple SharePoint and K2 Farms

Multiple SharePoint and K2 Farms

Building on previous topology descriptions, this install scenario can be leveraged in multi SharePoint farm environments to allow completely independent K2 farms per SharePoint farm. The expected volumes would be similar to a single farm installation, however as there are multiple farms scaled independently, there is near limitless ability to scale.

Similar to the Large Scale Install scenario, this scenario is specifically suitable for high work load environments. Each component is load balanced, and multiple dedicated databases allow for maximum growth and availability. Multiple databases are dedicated to individual load-balanced components to allow for maximum growth and availability.

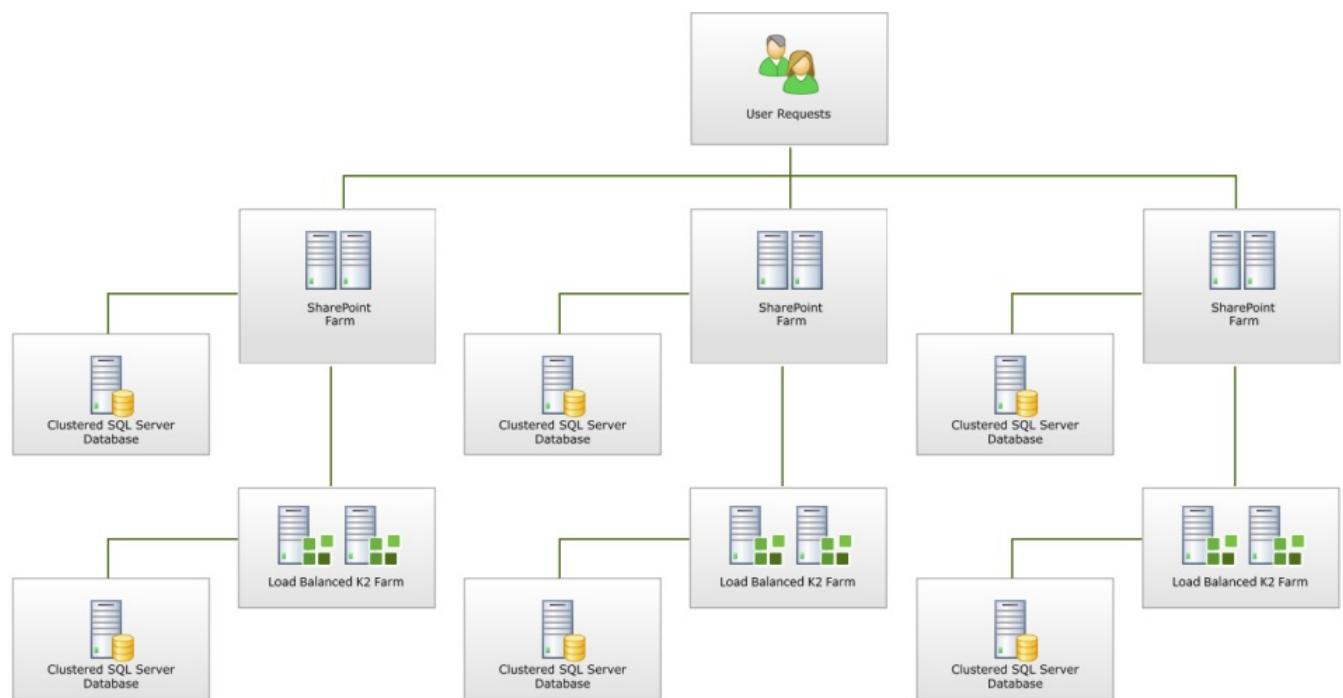
Kerberos is mandatory for this configuration option. Both NLB and Kerberos must be configured correctly and must be able to communicate before K2 blackpearl is installed.



Depending on the SharePoint product installed, either the MOSS, WSS, SharePoint 2010 Server or SharePoint 2010 Foundation components will be displayed for installation.

Also depending on your MOSS environment, the application servers such as Excel Services, InfoPath Server, and Indexing can be split off onto a separate server. Refer to the SharePoint installation guidance for installation options. These servers will not be needed if only WSS is installed.

The **Multiple SharePoint and K2 farms Install** scenario is shown below. Not all of the SharePoint features are shown here. Refer to the SharePoint documentation for installation guides and options.



Considerations for the Multiple SharePoint and K2 Farms Install

Useful to segment due to:

- Load
- Language
- Geography
- Legal requirements
- Operational ownership/support

Kerberos



The default method for user authentication for new distributed installations is K2 Pass-Through Authentication (see the [Introduction to Kerberos here](#)). Kerberos is still supported.

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. As discussed earlier, whenever more than two hops are required, Kerberos must be configured.

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

Network Load Balancing

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.

When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, each load-balanced component should have the full install on each NLB node.

SQL Server

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it can be clustered. For more information regarding SQL Server clustering, refer to the Getting Started with SQL Server Failover Clustering documentation (<http://msdn.microsoft.com/en-us/library/ms189134.aspx>)

In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

1.4.4 Additional Planning Considerations

Additional Planning Considerations

When deploying K2 blackpearl, there are several decisions for the infrastructure that should be made before installing K2:

- Network Load Balancing
- Pass-through authentication
- Kerberos
- IIS
- Domain configuration
- Database sizing

Work through the infrastructure appraisal phase methodically to ensure nothing is overlooked and all factors are considered. The hardware and software pre-requisites as detailed earlier in this paper are places to start with the appraisals.

The K2 components can be installed on one server or in a distributed server configuration. When the work load requirements necessitate that the components be installed on independent machines, the components are distributed on the network. Security is a consideration when components are distributed onto different servers. Where there would be more than one hop between servers, Kerberos authentication must be configured.

Implementing K2 on an existing network may require that changes be made to the existing infrastructure.

The following sections will describe these considerations in more detail. Additional references can be found on Microsoft's Web site, and they have been included as links where appropriate.

1.4.4.1 Network Load Balancing Setup and Configuration



The machines residing in the individual Network Load Balancing (NLB) configurations must be configured prior to K2 installation. The following deployment consideration sections discuss NLB setup.

Network Load Balancing vs Clustering

NLB clusters dynamically distribute the flow of incoming TCP and UDP traffic among the cluster nodes according to a set of traffic-handling rules. NLB clusters provide a highly available and scalable platform for applications such as IIS. NLB is used for stateless applications; i.e. those that do not rely on any state as a result of a request.

NLB and server clusters complement each other in complex architectures: NLB is used for load balancing requests between front-end Web servers while server clusters provide high availability for backend database access.

A server cluster is a collection of servers that together provides a single, highly available platform for hosting applications. Applications can be failed-over to ensure high availability in the event of planned downtime due to maintenance or unplanned downtime due to hardware, Operating System or application failures. Server clusters provide a highly available platform for applications such as SQL Servers. Server clusters are used for stateful applications that rely on some state context from one request to the next.

Server clusters provide high availability and disaster tolerance for mission-critical database management, file sharing, intranet data sharing, messaging, and general business applications. With Windows Server 2008 R2 with SP1, failover clustering allows flexibility for adding and removing hardware in a geographically dispersed cluster environment, as well as providing improved scaling options for applications. Windows Server 2008 R2 also allows server clusters to be deployed in a variety of different configurations, in particular:

- Single cluster configurations with dedicated storage.
- Multiple clusters on a storage area network (SAN), potentially with other Windows servers or operating systems.



The K2 Server is not supported in the Windows server cluster environment. The K2 Server is only supported on NLB clusters.

Physical Network Environment

Since a large installation typically uses more than one Web server in a load-balanced configuration, setting up the local network infrastructure can be more complex than setting up a normal Web application system. This is because the Windows NLB technology causes multiple Web servers to appear as a single server. As a result, the network infrastructure must support the creation of multiple broadcast domains (virtual local area network, or VLAN) to segment incoming Web requests from the main production network.

NLB broadcasts incoming traffic destined for the servers in an NLB group to all ports within their network collision domain (in this case, VLAN). In normal Web server deployment scenarios, the incoming traffic typically consists of a small number of HTTP GET requests and this may not be an issue. However, K2 blackpearl and SharePoint network traffic may consist of large documents moving between servers.

As a result, it is imperative that the NLB adapters for the Web servers are not connected to the normal server network. A separate logical or physical network, such as a VLAN, must be created so the larger amount of incoming traffic is not flooded to the network ports of other servers, thereby causing performance degradation on all servers within the network, not just the Web servers.

Furthermore, traffic to and from a SharePoint site or the K2 Workspace involves a considerable amount of communication from the Web servers to the back-end servers running SQL Server; good connectivity between them is required. It is therefore recommended that Web servers be dual-homed:

- One network adapter handling the incoming Web requests by using NLB
- One network adapter acting as a normal server adapter to communicate to the server running SQL Server along with the other servers within the infrastructure, such as domain controllers for authentication purposes

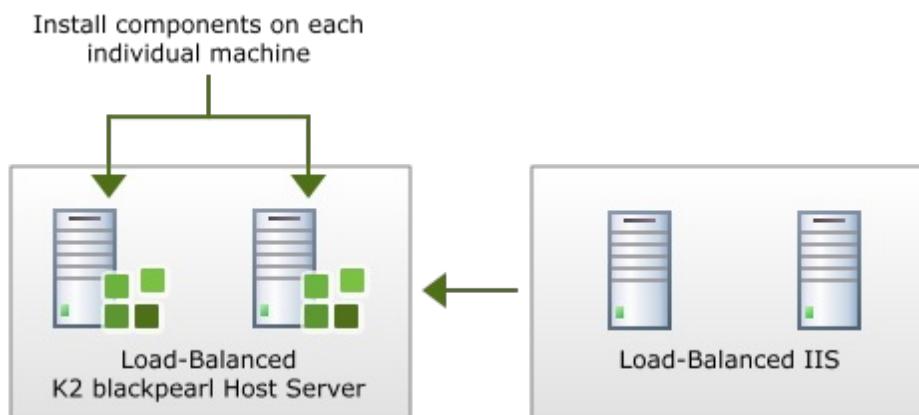
Installing Components in a Redundant Environment

When installing for load balancing, the installation must be performed on each machine independently. If for example the K2 Server is being installed in a NLB cluster similar to the example below, the server components must be installed on each individual machine.

The NLB cluster is configured using the operating system and should be configured prior to installing and configuring the K2 environment.

As illustrated below, when installing the components for load balancing, the components need to be pointed to the K2

Server NLB cluster. For example, the component is pointed at the NLB name and not the individual machines within the NLB cluster.



Additional Resources for NLB

NLB FAQ:

[http://technet.microsoft.com/en-us/library/cc725691\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc725691(v=WS.10).aspx)



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.4.2 K2 Pass-Through Authentication

K2 Pass-Through Authentication

When components are installed on separate servers, credentials must be passed between the services. This can be accomplished by setting up K2 Pass-Through Authentication, which is configured as part of the installation and configuration process of K2. Any time where two or more hops are required for user authentication, K2 Pass-Through Authentication must be configured.

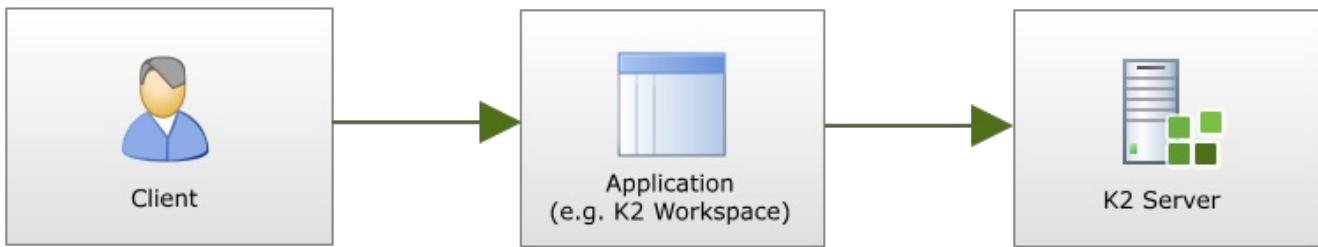


K2 Pass-Through authentication is the default option when installing distributed configurations. Kerberos is a supported alternative.

What is K2 Pass-Through Authentication

K2 Pass-Through Authentication is a K2 proprietary authentication methodology specifically for authenticating users whose credentials need to be passed between machines that interact with the K2 APIs. This authentication model can be used as an alternative to Kerberos, but is not in any way intended to be a replacement for Kerberos.

K2 Pass-Through Authentication enables the removal of Kerberos dependencies and still allow a user's credentials to be passed between machines in such a way that the user can be authenticated in a secure manner without compromising the integrity of the K2 Server Transactions and data.



Why use K2 Pass Through Authentication

K2 Pass-Through Authentication is intended as an out of the box means for K2 blackpoint and K2 blackpearl installations to be able to authenticate user requests. The K2 Pass-Through Authentication is available as a native feature of K2 blackpearl and K2 blackpoint; support for this feature will install with the KB001290 update. K2 Pass-Through can be implemented by various organizations depending on their requirements or internal skills availability. The list below is some of the reasons why an organization would use K2 Pass-Through Authentication.

- Limited Internal Organization Skills
- No access to Active Directory to make the required changes
- Business requirements that don't warrant the need for a Kerberos implementation



K2 Pass-Through Authentication is not a Kerberos replacement, it is a Kerberos alternative which can be implemented for specific delegation requirements when an anonymous connection is made which results in Kerberos failure.

1.4.4.3 Kerberos Setup and Configuration

Kerberos

When components are installed on separate servers, credentials must be passed between the services. This can be accomplished by setting up Kerberos, which should be configured prior to installing K2. Any time where two or more hops are required for user authentication, Kerberos must be configured.

What is Kerberos?

The authentication model implementation is dependent on whether user credentials must be passed from one system to another. When they are passed, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.

The rule of thumb for when Kerberos configuration is required falls to one question: Does a system need to impersonate a user? If the answer to that question is yes, then Kerberos is required. An alternative approach to the need to configure Kerberos would be to assess whether two or more hops between servers are required. In such a case, Kerberos is required. This is commonly known as the "double-hop issue."

How can I tell if Kerberos is not configured properly?



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

The need for Kerberos configuration may only become evident once the following errors are detected. These errors will appear as soon as one of the servers attempts to pass credentials.

- "NT AUTHORITY/ANONYMOUS LOGON"
- "401 - Access Denied"



Kerberos is configured as part of the installation, some configuration happens once the components are installed. See the installation documentation for additional information.

Neither Microsoft nor K2 developed the Kerberos standard. The MIT standard has been implemented in the platform and K2 relies on the implementation to successfully pass credentials between servers.

A detailed guide on Security and Kerberos Authentication with K2 Servers can be found on the K2 Underground: (http://k2underground.com/files/folders/technical_product_documents/entry21001.aspx)

Additional Resources for Kerberos

Kerberos Protocol Transition and Constrained Delegation:

<http://technet2.microsoft.com/windowsserver/en/library/c312ba01-318f-46ca-990e-a597f3c294eb1033.mspx?mfr=true>

Knowledge Base Articles on Kerberos:

http://help.k2.com/en/search.aspx?q=Kerberos&languages=lang_en

Information on the Double-Hop Issue:

<http://support.microsoft.com/kb/329986>

Windows 2000 Kerberos Authentication:

<http://technet.microsoft.com/en-us/library/Bb742431.aspx>



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.4.4 Internet Information Service (IIS)

Internet Information Service (IIS)

IIS requires good planning and an understanding of system and user accounts, Web sites, application pools, and permissions to folders and other environment resources. Involve the IIS administrator in planning the K2 installation, configuration, and Web application design.

Host Headers and Ports

Understand how to use host headers and ports and how to reference them properly when setting SPNs for Kerberos implementations.

MetaBase.xml

The settings contained in the MetaBase.xml file must be accurate when implementing Kerberos. Refer to the installation documentation for setting SPNs for Kerberos and editing the Metabase.xml for more information.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.4.5 Domain Configuration

Domain Configuration

Many variables in a network can affect how K2 blackpearl, IIS, Active Directory, Visual Studio, Exchange, Office (including Outlook), and SharePoint are installed and function. Proxy servers, multiple domain controllers, firewalls, and network policies may also affect the manner in which these applications or servers function within their environment.

Incorrect or incomplete DNS settings often cause one or more features of a K2 Server to fail, such as user authentication or Active Directory lookup. It is very important that DNS is setup and functioning correctly and reliably. DNS issues usually result in the K2 Server being unable to resolve users and/or user e-mail addresses against Active Directory.

Delegation (full or constrained): Delegation is required on Windows Servers to impersonate other servers/users/services.

K2 can be installed in single or multiple domain configurations. A domain in a tree configuration may have another tree domain along side with perhaps the added complexity of an external domain. K2 will support these configurations when Kerberos is configured correctly.

Domain Policies

The following domain group policy and/or local security settings configurations are required:

System	Item to Configure	Description
IIS Server	IIS_WPG Group	<ul style="list-style-type: none"> The K2 Workspace Service Account must be added to this group The K2 Workspace must run under Windows Integrated Authentication mode
K2 Server	Login Account	<ul style="list-style-type: none"> The K2 Server Service Account must have Log on as a Service permissions
Client Machines	Internet Access	<ul style="list-style-type: none"> User must have Internet Explorer Internet Explorer must be configured properly



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.4.4.5.1 DNS Basics

What is DNS

DNS stands for Domain Name System. Think of it as a filing system or database for all the domain names on the internet. What is a domain name? When you browse to a web address, such as k2.com, you instruct your computer to visit a particular "domain" - a human friendly representation of a particular location on the Internet. These names are sometimes referred to as host names. Host names are not case sensitive and can contain alphabetic or numeric letters or the hyphen. A host name is also the name provided within a local network to each individual computer. We most often use host names with reference to servers. Each organization that maintains a computer network will have at least one server handling DNS queries. That server, called a name server, will hold a list of all the IP addresses within its network, plus a cache of IP addresses for recently accessed computers outside the network. Each computer on each network needs to know the location of only one name server.

Computer networks don't communicate in terms of "names," but rather numbers. Each server that serves content, be it web sites, e-mail, file server, etc., has a special number assigned to it, called an IP address (IP stands for Internet Protocol). A computer network has no idea what k2.com is or how to find it, but if we used the IP address of the site, it would understand what the connection should be. Therefore, there needed to be a way to translate the domain (a human understandable name like k2.com), into terms that the computer network would understand, one based on IP numbers. This is what DNS does. DNS is a system whereby we can keep a registry of human friendly names mapped to network friendly numbers.

When visiting a website like k2.com, an Internet browser checks to see if it has been there recently, in which case the IP address might be cached or stored locally on the computer. If the IP address cache is not found, the computer looks outside to DNS servers provided by the corporate network or Internet Service Provider (ISP). If those servers can't provide the information they in turn look to a server farther upstream on the Internet. These searches are forwarded up the line until they find the address or determine that it doesn't exist. If the address is available, it is then passed back to your browser. If not, a message telling the browser that the host name or domain is not available is sent.

How DNS works

So, how does the process work? How does a domain name, something humans understand, get translated into a IP number, something that computer networks will understand? As mentioned in the previous section, each domain has to have something called a name server. This is a server that is designated as authoritative for answering queries regarding the domain, communicating what number goes to what domain.

Where does the process start? Technically, ".com" is a domain. Every "." in the domain name is a separator representing a different level. Thus, when an Internet browser asks for the number assigned to k2.com, the computer network first has to go to the name server for the ".com" domain and request the name server for the "k2" domain under it. Theoretically there can be an infinite number of levels. We could ask for anthony.tom.bob.k2.com, and the computer would start from the right side of the domain name, ".com," and ask for the name server authoritative for each level. There does not need to be that many name servers in the search, for if the k2.com name server knew the IP address of anthony.tom.bob.k2.com, it could just send that information through the network and the process would stop. But, if it didn't have all the information, it would tell my computer where the next link in the chain was. If at any time the process hits a name server that is supposed to be authoritative for its level and that name server does not know where to direct the search, it will return an error. If there is no such domain as anthony.tom.bob.k2.com, then when the internet browser attempts to view the site, an error will be returned at whatever link of the chain the name servers have no information. Whenever a computer connects to the internet, your ISP gives that computer the IP addresses of special servers designed to answer enquires from that computer about domains. These designated servers in turn get their information from ICANN.

ICANN and the Top Level Domains

ICANN stands for the *Internet Corporation for Assigned Names and Numbers*. All the concepts discussed above can be found in the ICANN's name, and thus we can infer that they manage the whole DNS process. ICANN sets up, manages and maintains all the authoritative name servers for the very top level domain, the domain that is to the farthest right of any address. These servers are always on and their addresses never change. Their only purpose is to start the whole search and convert procedure. These ICANN servers have a list of other servers, managed by different companies, which ICANN has authorized to be authoritative for the next step in the process, the "Top Level Domains" or TLDs. They would be the ".com", ".net", ".org", ".ac", etc. These servers are also referred to as 'root servers'. ICANN is the organization at the very top of the tree, and they manage and delegate the whole name server process for everyone else.

For more information about the DNS system see - [DNS Beyond the Basics](#)

1.4.4.5.2 DNS Beyond the Basics

Beyond the Basics of DNS

Forward and Reverse Lookup

Forward Lookup refers to the process of 'looking forward' from a hostname or domain name to lookup the IP address for it.

Reverse Lookup refers to the opposite process, finding the domain or hostname that relates to a known IP address

DNS servers maintain forward and reverse lookup zones, with directories which facilitate this process.

A forward lookup is used in the standard DNS queries described above. A reverse lookup is often used by e-mail servers to combat spam. When a message comes in, a server may also do a reverse lookup on the IP address the mail came from. If it doesn't match the domain name the e-mail claims to be coming from, the server may discard the message.

Caching

Once the computer or the DNS servers it has referred to have an IP for a domain or host name, it will 'cache' it, or hold the information for a period of time. This time will vary from system to system, but it is typically a fairly short time. The principal reason for the short time period is that IP addresses can change.

Fully Qualified Domain Name

A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the host name and the domain name. For example, an FQDN for a hypothetical mail server might be mymail.k2.com. The host name is mymail, and the host is located within the domain k2.com.

Understanding more about DNS Mapping

Domain name syntax

A domain name consists of one or more parts, technically called labels, that delimited by dots, such as example.com. The following list provides the basic outline of DNS name syntax:

- The right-most label conveys the top-level domain; for example, the domain name [www.example.com](#) belongs to the top-level domain com.
- The hierarchy of domains descends from right to left – with each label to the left indicating a further subdivision, or subdomain of the domain to the right. For example: the label example specifies a subdomain of the com domain. The tree of subdivisions may have up to 127 levels.
- Each label may contain up to 63 characters. The full domain name may not exceed a total length of 253 characters in its external dotted-label specification.
- DNS names may technically consist of any character representable in an octet. However, the allowed formulation of domain names in the DNS root zone, and most other sub domains, uses a preferred format and character set. The characters allowed in a label are a subset of the ASCII character set, and includes the characters a through z, A through Z, digits 0 through 9, and the hyphen. This rule is known as the LDH rule (letters, digits, hyphen).
- A host name is a domain name that has at least one IP address associated. For example, the domain names [www.example.com](#) and example.com are also host names, whereas the com domain is not.

DNS Resolvers

The client-side of the DNS is called a DNS resolver. It is responsible for initiating and sequencing the queries that ultimately lead to a full translation of the resource sought, e.g., the translation of a domain name into an IP address.

A DNS query may be either a non-recursive query or a recursive query:

- A non-recursive query is one in which the DNS server provides a record for a domain for which it is authoritative itself, or it provides a partial result without querying other servers.
- A recursive query is one for which the DNS server will fully answer the query (or give an error) by querying other name servers as needed. DNS servers are not required to support recursive queries.

The resolver, or another DNS server acting recursively on behalf of the resolver, negotiates use of recursive service using bits in the query headers. Resolving usually entails searching in sequence through several name servers to find the needed information. However, some resolvers function more simply by communicating only with a single name server. These simple resolvers (called "stub resolvers") rely on a recursive name server to perform the work of finding information for them.

A DNS Example Record

A Resource Record (RR) is the basic data element in the domain name system. Each record has a type (A, MX, etc.), an expiration time limit, a class, and some type-specific data. Resource records of the same type define a resource

record set. An example DNS configuration (with the most commonly used resource record types) is shown in the table below, with explanations of each of the record types in the following paragraphs:

A Records

example.com 69.90.142.25 (a primary server)

help.example.com 69.90.142.26

CNAME Records

vpn.example.com Cr758341-a.ourisp.com

files.example.com example.com

www.example.com example.com

MX Records

example.com example.com (see below for more information)

A Records / Host Records

The bread and butter behind the DNS system is the A Record. The A record (address record, or host record) maps a domain name to an IP address on the local network or on the Internet.

In this example, the network system is hosting example.com. Using a dynamic DNS tool, we could set our domain to be example.com and the IP address (69.90.142.25) will be automatically updated via dynamic DNS. For our vpn, we need to create a static A record with the IP address (69.90.142.26) associated with vpn.example.com.

So, we have two names mapped to IP addresses (A Records):

- example.com - 69.90.142.25
- help.example.com - 69.90.142.26

CNAME Records / Alias Records

CNAME Records (Canonical Name records) act as aliases for host names. Instead of mapping a domain name to an IP address (an A record) you can map a domain name to another domain name. In the example, you have:

files.example.com - example.com

www.example.com - example.com

vpn.example.com - Cr758341-a.ourisp.com

What are the advantages of CNAMEs? Multiple domain names can be mapped to one - sometimes dynamic - IP address. In our example, files.example.com and www.example.com will now be associated with example.com's IP address (a Dynamic DNS A record). In the case of the vpn, CNAMES gives the options of changing a not-so-easy-to-remember-super-long domain name into something better.

MX Records / Mail Records

MX Records (Mail eXchanger record) tells mail systems how to handle mail that is addressed to a particular domain. Like CNAME records, the MX record maps a domain name to another domain name.

In the example, we use our primary machine as a server for mail to xyx@example.com. Every MX record is tagged with a priority number. The MX record with the lowest number is the primary mail server. If the primary server is unavailable, the backup mail server (also called a "secondary mail server") will queue the mail.

For a list of all the resource record types used in DNS lookups, see the Wikipedia article
http://en.wikipedia.org/wiki/List_of_DNS_record_types

1.4.4.6 Database

Manage Database Size

The size of the K2 Database can grow to be much larger to improve database management. The K2 Archive Utility enables the administrator to export the completed processes to a K2 Archive Database.

Database Access

Access to the databases is secure and two options are available when installing K2. During installation, the Database Settings dialog will prompt the installer to select either Windows Authentication or SQL Authentication.

Provided the User Account accessing SQL has the appropriate login credentials, either one of the two methods can be used. If SQL Authentication is selected, a connection string is stored in a configuration file which makes access to a database containing secure information vulnerable if the folder where the configuration file is located unsecured. Windows Integrated Authentication is more secure, as the login credentials are managed via Active Directory and user names and passwords are not exposed in plain text in a configuration file.

Installing the Database

The database can be installed either locally or remotely. To install the database remotely, the K2 Service Account must have been allocated access rights on the remote SQL Server. Refer to the [Installation Account permissions](#) for further details.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5 Prerequisites

K2 Installation Prerequisites

There are several hardware and software requirements regardless of the deployment scenario you choose. These are detailed in the following sections:

- Hardware Requirements
- Software Requirements
 - Licensing
 - Integration
 - By Component
 - By Server Role
- Permissions for K2 Components
- Environment Configuration



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.1 Hardware Prerequisites

Hardware Prerequisites

The following guidelines should be followed for hardware selection when installing from an installation media such as a DVD:

Component	Requirement
Computer and Processor	<p>Minimum: Server with processor speed of 2.5 gigahertz (GHz) or higher</p> <p>Recommendations:</p> <ul style="list-style-type: none"> • 64 bit wherever possible • Multiple AMD64 or Intel x86_64 multi-core CPUs <p>*32-bit and 64-bit support</p>
Memory	<p>K2 Server</p> <ul style="list-style-type: none"> • 4 GB min • 8 GB recommended (especially if 64 bit servers are used) <p>SQL Server</p> <ul style="list-style-type: none"> • Recommend at least twice the amount of K2 server as a starting point
Hard Disk	<p>K2 Server</p> <ul style="list-style-type: none"> • 350mb + 1Gig for Documentation <p>K2 workspace</p> <ul style="list-style-type: none"> • 350mb + 1 Gig for Documentation <p>SharePoint</p> <ul style="list-style-type: none"> • 500mb + 1 Gig for Documentation <p>SQL Server</p> <ul style="list-style-type: none"> • Minimum 5 GB • Recommend 10 GB to start <p>Workstation</p> <ul style="list-style-type: none"> • 450 mb + 1 Gig for Documentation
Display	1024x768 or higher resolution monitor
Connection	<p>100 megabits per second (Mbps) connection speed required for farm deployment</p> <p>56 kilobits per second (Kbps) required for client to server connection</p>
E-mail Notifications	<p>Internet Simple Mail Transfer Protocol/Post Office Protocol 3 (SMTP/POP3)</p> <p>or</p> <p>Internet Message Access Protocol 4 (IMAP4)</p>
Additional space will be required if a downloaded version of the installation is to be copied onto the servers and workstations.	
Full K2 blackpearl Installation	1.5 GB (x2 for extraction)
K2 blackpearl Update Only	1 GB (x2 for extraction)



If you are installing a single server environment, it is recommended that you have more RAM and a larger processor in order to have acceptable performance. If you are separating out the components onto multiple tiers, those tiers should be sized appropriately based on usage and performance requirements.



- IA 64 – Itanium 64 is NOT supported
- While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.1.1 32-bit and 64-bit

32-bit and 64-bit



32-bit/64-bit Compatibility

As of K2 blackpearl 4.6, the following components and platforms are supported:

- Server Components (64-bit support only): K2 Server, K2 Databases, K2 for SharePoint, K2 Runtime Web Services, K2 Workspace, K2 for Reporting Services
- Client Components (32-bit and 64-bit support): K2 Studio, K2 for Visual Studio, K2 Documentation

K2 runs in full 64-bit mode, meaning that it is a true 64-bit application and therefore does not have the 2 GB restriction that 32-bit applications have when running the 64-bit version.

95% of the code is compiled in a MSIL and will run in 32-bit and 64-bit depending on the environment hosting K2. The other 5% gets compiled to target a specific instruction set (x86 or x64) and is mostly the unmanaged components like the host server core and services. With installation, the installer detects if the environment is 64-bit or 32-bit and will install the correct components. When installing on a 64-bit environment, the 32-bit components will be installed as well. It is clearly visible in the Global Assembly Cache. These components are required by applications like "Microsoft Visual Studio" that is 32-bit application only and will execute under the WOW (Windows on Windows) emulated process. These applications cannot make use of the 64-bit components and therefore the 32-bit components are required.



The platform (e.g., 32-bit or 64-bit) must be identical for all servers that are Network Load Balanced participating in a K2 blackpearl Role.

The K2 installer will install the appropriate 32-bit components when K2 Designer for Visual Studio are installed.

The K2 blackpearl 64-bit installer can be deployed in a number of scenarios. As an overview, 32-bit and 64-bit components can be configured in an environment and function as a whole to provide a fully deployed system.

The table below describes the various supported communication topologies between 32-bit and 64-bit components:

\ TO FROM	64-bit K2 Server	64-bit K2 Workspace	64-bit K2 for SharePoint	64-bit K2 for Reporting Services	64-bit K2 Databases	64-bit K2 for Visual Studio
32-bit K2 Server	Not Supported	Supported	Supported	Supported	Supported	Supported
32-bit K2 Workspace	Supported	Not Supported	Supported	Supported	Supported	Supported
32-bit K2 for SharePoint	Supported	Supported	Not Supported	Supported	Supported	Supported
32-bit K2 for Reporting Services	Supported	Supported	Supported	Not Supported	Supported	Supported
32-bit K2 Databases	Supported	Supported	Supported	Supported	Not Supported	Supported
32-bit K2 for Visual Studio	Supported	Supported	Supported	Supported	Supported	N/A

1.5.2 Software Prerequisites

Software Prerequisites

The information below describes all the software requirements for a K2 installation.

- K2 blackpearl licensing
- Integration with designers' wizards
- By component
- By server role



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

Server Component	Operating system
K2 Server K2 Databases K2 Reporting Services K2 for SharePoint K2 Workspace	<ul style="list-style-type: none"> ● * ** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
K2 for Visual Studio K2 Studio These two components may be installed on ANY of the operating systems listed.	<ul style="list-style-type: none"> ● * ** Windows Vista SP1 or SP2 or Windows 7 RTM or SP1 or Microsoft Windows 8 (Windows 8 / Pro / Enterprise)
<p>*Latest security patches *32-bit and 64-bit support</p>	
Server Component	Windows Components
K2 Server	<ul style="list-style-type: none"> ● Microsoft Message Queuing (MSMQ) Services <ul style="list-style-type: none"> ● Message Queuing Server ● Directory Service Integration ● A User Manager: The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 Reporting Services K2 for SharePoint K2 Workspace	<ul style="list-style-type: none"> ● IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured) ● ASP.NET ● Windows Authentication Role Services
K2 Database	<ul style="list-style-type: none"> ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 for Visual Studio K2 Studio	<ul style="list-style-type: none"> ● No Windows components
Server Component	Additional Software
K2 Server	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5 <p>For more information on .NET framework and K2, please see the topic: .NET Technologies</p> ● Windows Support Tools (see Install Windows Support Tools for more information: for 32-bit see http://go.microsoft.com/fwlink/?LinkId=62270.

	<p>Note: Windows Support Tools is a prerequisite if the installer is to automatically set the SPNs during the installation of K2 blackpearl. Otherwise, the Windows Support Tool is regarded as optional software.</p> <ul style="list-style-type: none"> Windows Identity Foundation Redistributable (for more information, see http://support.microsoft.com/kb/974405). Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). If CRM is used: Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server, the server must have .NET 4 enabled.) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en
K2 Database	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Note: .NET Framework 4.0 is supported but not a prerequisite Microsoft SQL Server 2012 Express, Standard, BI, Enterprise or Microsoft SQL Server 2008 Express, Standard, Enterprise SP3 or Microsoft SQL Server 2008 R2 SP1
K2 Workspace	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Microsoft Report Viewer Redistributable 2005 SP1 <ul style="list-style-type: none"> Full installation: http://www.microsoft.com/downloads/details.aspx?FamilyID=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=en Upgrade installation: http://www.microsoft.com/downloads/details.aspx?FamilyId=35F23B3C-3B3F-4377-9AE1-26321F99FDF0&displaylang=en Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en <p>NOTE: K2 Reports Runtime – requires Microsoft Report Viewer Redistributable 2008 SP1 K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2005 SP1</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Silverlight 4 or 5: (required for View Flow) http://www.silverlight.net/getting-started
* IISReset or reboot is recommended after installation	
K2 Studio	<ul style="list-style-type: none"> Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5
 For more information on .NET framework and K2, please see the topic: .NET Technologies Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. Microsoft Exchange Server 2007 SP3 (required for Exchange Wizard) or Microsoft Exchange Server 2007 Management Tools SP3 or Microsoft Exchange 2010 SP1 or Microsoft Exchange 2010 SP2 Windows Powershell Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server)

	<p>http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en</p> <ul style="list-style-type: none"> ● OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx ● Microsoft Office SharePoint Server (MOSS) 2007 SP3 <ul style="list-style-type: none"> ● Excel Web and Calculation Services ● Trusted file locations for Excel spreadsheets ● Microsoft SharePoint Server 2010 RTM or SP1 ● Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets ● Either Visual Studio 2012 or Visual Studio 2010 Web Deployment Projects is required to deploy projects in K2 Studio (http://www.microsoft.com/en-us/download/details.aspx?id=25163) <p>Windows SDK v7.0A is required when the 'Generate ASP Pages' option is used. This is installed and configured when Visual Studio 2010 or 2012 is installed.</p>
K2 for SharePoint	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 http://www.microsoft.com/downloads/details.aspx?FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7&displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 ● Microsoft Windows SharePoint Services 3.0 (WSS) SP2 or Microsoft Office SharePoint Server 2007 (MOSS) Standard, Enterprise SP3 or SharePoint 2010 Foundation or SharePoint 2010 Foundation SP1 or SharePoint Server 2010 or SP1 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode) ● SharePoint Foundation 2010 Client Side Object Model Redistributable (required for CSOM Service Broker and is installed on the K2 Server) ● Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en ● Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en ● Visual Studio 2010 Web Deployment Projects (required for Forms Technology): http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24509
K2 for Visual Studio	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 (.NET Framework 4.5 is supported but not required): <ul style="list-style-type: none"> For more information on .NET framework and K2, please see the topic: .NET Technologies ● Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) with or without Sp1 ● A User Manager: <ul style="list-style-type: none"> Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. ● Windows Powershell ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en ● OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx ● Excel Web and Calculation Services <ul style="list-style-type: none"> with Trusted file locations for Excel spreadsheets or Microsoft SharePoint Server 2010 and Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS

	<p>2007) with Trusted file locations for Excel spreadsheets</p>
K2 for Reporting Services	<ul style="list-style-type: none"> ● Microsoft SQL Server 2012 Reporting Services or Microsoft SQL Server 2008 Reporting Services ● Microsoft Report Viewer Redistributable 2008 <p style="margin-left: 20px;">http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en</p> <p style="margin-left: 20px;">or</p> <p style="margin-left: 20px;">Microsoft Report Viewer Redistributable 2008 SP1</p> <p style="margin-left: 20px;">http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en</p> <p>NOTE: K2 Reports Runtime and K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2008 SP1</p> <ul style="list-style-type: none"> ● Microsoft .NET Framework 3.5 SP1 Redistributable Package and Microsoft .Net Framework 4 http://www.microsoft.com/downloads/details.aspx?FamilyID=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en ● Microsoft Internet Explorer 8 or 9 or 10 (Plug-in support is only available in Internet explorer 10 on the desktop, and this version of Internet Explorer 10 must be used for items built on Silverlight, such as the K2 designer for SharePoint). ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server)

1.5.2.1 K2 Platform Licensing

K2 Licensing

The K2 blackpearl product requires a license to install. Unless a License Key has been obtained, the product installation will be unable to complete and you will be unable to use K2 blackpearl. The License Key provided will depend on the product option that has been purchased by the organization.

System Key

The System Key is obtained during the configuration step of the K2 Server. The System Key is required to obtain a License Key, regardless of the mechanism used to obtain the License Key.

License Key

License Keys can be obtained via E-mail, Telephone, or directly through the [K2 Customer and Support Portal](#). For more information regarding licensing options, please contact your K2 Sales Representative.



The System Key and the License Key are unique to the machine where K2 blackpearl is being installed and configured.

Developer License details

The following are important considerations that applies to the Developer license:

- Each K2 blackpearl Production Server License allows for unlimited installations of K2 blackpearl Development Servers for non-production use only.
- K2 blackpearl Development Servers may not run as a Windows Service and can only be operated in console mode.
- K2 blackpearl Development Servers are limited to Single Server installations.
- Development Server licenses can be requested on the K2 Customer Portal
<https://portal.k2.com/licensekey/Default.aspx>

Console Mode has the following limitations and performance implications for all Development Servers:

- Requires Local Login
- Single-threaded Execution only
- Single CPU only (multiple processor use is disabled)

1.5.2.2 Integration

Software - Integration

There are certain wizards and Inline Functions in the K2 designers that have their own specific prerequisites if they are to be used in K2 processes. Listed below are the wizards and the respective prerequisite.

Wizard/Inline Function	Prerequisite	Installed on
Active Directory	Active Directory Server (Windows 2000 Functional Level or greater)	K2 Server
LDAP	LDAP-compatible systems with protocol version 3 or higher.	LDAP Server
Exchange For more details on Exchange see: Exchange Server Configuration	Microsoft Exchange Server 2007 and Microsoft Exchange 2007 Management Tools SP2 or SP3 or Microsoft Exchange 2010 and Windows Powershell 2 and WinRM (Windows Remote Management) or Microsoft Exchange Server 2013 (On premise or online)	K2 Server
CRM Entity	Microsoft Dynamics CRM 4.0 SDK must be installed as per the Software Prerequisites topic If CRM 2011 is going to be used, Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable must be installed on the K2 Server with .NET Framework 4. The redistributable will be automatically installed during setup or reconfiguration of the system. Note: Microsoft Dynamics CRM 4.0 Workgroup, Professional (Pro) Server or Enterprise Server needs to be present on the users network	K2 Server and is required by: K2 Studio K2 for SharePoint K2 for Visual Studio K2 for Reporting Services
Oracle Service Instance (Optional software, only necessary if Oracle is being used)	64-bit Oracle Data Access Components (ODAC) (can be downloaded from the Oracle site, here .) Oracle version 9 and up is supported. Note: If the ODAC is not installed prior to registering a new service instance, an error is generated saying the assembly can not be loaded	K2 Server

	because it is either not present or one of its dependencies is missing.	
Get Content Control	OpenXML SDK 2.0 Redistributable http://msdn.microsoft.com/en-us/office/bb265236.aspx	K2 Server and Client
Get Cell Get Cell with Input Get Range Get Range with Input	Microsoft Office SharePoint Server (MOSS) 2007 and Excel Web and Calculation Services -with- Trusted file locations for Excel spreadsheets or Microsoft SharePoint Server 2010 and Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets	K2 Server and SharePoint Web Front Ends
K2 Services	.NET Framework 3.5 SP1 or .NET 4 Framework (for K2 Server)	K2 Server and Client
Create Folder in List	Windows SharePoint Services (WSS) 3.0 or MOSS 2007 or SharePoint 2010 Foundation or SharePoint Server 2010 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode)	SharePoint Web Front Ends
Convert Document	SharePoint 2010 Foundation or SharePoint Server 2010 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode)	SharePoint Web Front Ends
Create Document	Windows SharePoint Services (WSS) 3.0 or MOSS 2007 or SharePoint 2010 Foundation or SharePoint Server 2010 and OpenXML SDK 2.0 Redistributable http://msdn.microsoft.com/en-us/office/bb265236.aspx or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode)	K2 Server and SharePoint Web Front Ends
Insert into Document	OpenXML SDK 2.0 Redistributable http://msdn.microsoft.com/en-us/office/bb265236.aspx	K2 Server and SharePoint Web Front Ends

| us/office/bb265236.aspx |

InfoPath 2013

If InfoPath 2013 forms are going to be used, the forms must be set to InfoPath 2010 compatibility mode in the forms options. Further, Microsoft Office 2013 installations need to be licensed as unlicensed installations cause forms publishing issues.

1.5.2.3 Prerequisites by Component

Prerequisites by Component

K2 blackpearl has many components that can be installed. In a distributed environment, these components can be installed on independent servers or combined. It is important to know what the components require and their function so that you can decide which server should be the home for which component.

The K2 Installer will validate that the prerequisites for the component are installed before allowing you to proceed with the installation. The K2 Installer will determine which platform version is being used and will install K2 blackpearl components accordingly. For all intents and purposes, the requirements for installing a 64-bit installation are identical to its 32-bit counterpart.

The following sections will describe the prerequisites for each server role listed below:

K2 blackpearl Components	
	K2 for Visual Studio The K2 Designer for Visual Studio is a design surface that allows developers to use a tool they are familiar with (Visual Studio) to develop, design, and deploy K2 applications
	K2 Studio The K2 Studio is a design surface to allow business users to design and deploy K2 applications
	K2 for SharePoint Installs the K2 features for SharePoint, including the K2 Worklist Web Part, K2 Designer for SharePoint, and integration components Two options, either Microsoft SharePoint Portal Server 2007 or Windows SharePoint Services 3.0
	K2 for Reporting Services K2 Reports are rendered using Microsoft SQL Server Reporting Services
	K2 Server Runs the K2 Host Server, which is the application server that runs all K2 applications and components
	K2 Workspace Web based interface to interact with and manage K2 processes and the K2 environment
	K2 Databases While not a component you select to install, when configuring the K2 Server component the installer will create the K2 Databases

1.5.2.3.1 Prerequisites for the K2 Server role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 Server

The K2 Server role is defined to be the server on which the K2 Host Server runs. The K2 Server component, configuration manager will be installed on this server.



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Server	
Operating System	* *** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
Windows Components	<ul style="list-style-type: none"> ● Microsoft Message Queuing (MSMQ) Services <ul style="list-style-type: none"> ● Message Queuing Server ● Directory Service Integration ● A User Manager: The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured)
Additional Software	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5 For more information on .NET framework and K2, please see the topic: .NET Technologies ● Windows Support Tools (see Install Windows Support Tools for more information: for 32-bit see http://go.microsoft.com/fwlink/?LinkId=62270. Note: Windows Support Tools is a prerequisite if the installer is to automatically set the SPNs during the installation of K2 blackpearl. Otherwise, the Windows Support Tool is regarded as optional software. ● Windows Identity Foundation Redistributable (for more information, see http://support.microsoft.com/kb/974405). ● Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). ● If CRM is used: Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server, the server must have .NET 4 enabled.) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9df&displaylang=en
Optional Software: Oracle	<p>64-bit Oracle Data Access Components (ODAC) (can be downloaded from the Oracle site, here.)</p> <p>Oracle version 9 and up is supported.</p> <p>Note: If the ODAC is not installed prior to registering a new service instance, an error is generated saying the assembly can not be loaded because it is either not present or one of its dependencies is missing.</p>
<p>*Latest security patches</p> <p>*32-bit and 64-bit support</p>	



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.2.3.2 Prerequisites for the K2 Database component



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 Databases



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 Database, while not a component that you select to install, will be installed during the configuration of the K2 Server. The K2 Database require the following prerequisites:

K2 blackpearl Prerequisites for the K2 Databases	
Operating System * & **	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
Windows Components	<ul style="list-style-type: none"> Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured)
Additional Software **	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Note: .NET Framework 4.0 is supported but not a prerequisite Microsoft SQL Server 2012 Express, Standard, BI, Enterprise or Microsoft SQL Server 2008 Express, Standard, Enterprise SP3 or Microsoft SQL Server 2008 R2 SP1
<small>* Latest security patches</small>	
<small>** 32-bit and 64-bit support</small>	

1.5.2.3.3 Prereqs K2 Designer for SharePoint



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 Designer for SharePoint

The K2 Designer for SharePoint is installed on a Microsoft Office SharePoint Server 2007, Windows SharePoint Services 3.0 Server, SharePoint 2010 Foundation or SharePoint Server 2010. The K2 for SharePoint component, configuration manager, and K2 documentation will also be installed on this server.



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 Designer for SharePoint role requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Designer for SharePoint	
Operating System * & **	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
*Latest security patches *32-bit and 64-bit support	
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 Component	<ul style="list-style-type: none"> K2 for SharePoint <p>The K2 Designer for SharePoint can only be installed with or where the K2 for SharePoint component is installed.</p>
Additional Software *	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 Redistributable Package (.Net Framework 4 is supported but not required): http://www.microsoft.com/downloads/details.aspx?FamilyID=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en SharePoint 2010 Foundation RTM / SP1(or later) or SharePoint Server 2007 Standard or Enterprise SP2 Microsoft Report Viewer Redistributable 2005 with SP1 <ul style="list-style-type: none"> Full installation: http://www.microsoft.com/downloads/details.aspx?FamilyID=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=en Upgrade installation: http://www.microsoft.com/downloads/details.aspx?FamilyId=35F23B3C-3B3F-4377-9AE1-26321F99FDF0&displaylang=en or Microsoft Report Viewer Redistributable 2008 <ul style="list-style-type: none"> http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 <ul style="list-style-type: none"> http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Silverlight 4 or 5: (required for K2 Designer for SharePoint and View Flow. Minimum required version for Silverlight is 4.0.50917.0) <ul style="list-style-type: none"> http://www.silverlight.net/getting-started Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may

be configured for use with K2 blackpearl.

- Microsoft Exchange Server 2007 SP3 (required for the Exchange Wizard)
 - Microsoft Exchange 2007 Management Tools SP2 or SP3

or

- Microsoft Exchange Server 2010 or Microsoft Exchange Server 2010 SP1
- Windows Powershell

or

- Microsoft Exchange Server 2013 (On premise or online)
- Microsoft Dynamics CRM 4.0 Workgroup, Professional (Pro) Server or Enterprise Server (required for CRM Wizard and CRM SmartObjects)
- Microsoft Dynamics CRM 4.0 SDK

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en>

- OpenXML SDK 2.0 Redistributable (required for Inline Functions)
<http://msdn.microsoft.com/en-us/office/bb265236.aspx>

- Microsoft Office SharePoint Server (MOSS) 2007 SP3
Excel Web and Calculation Services
with
Trusted file locations for Excel spreadsheets

or

Microsoft SharePoint Server 2010 RTM or SP1

and

Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007)

with

Trusted file locations for Excel spreadsheets

* IISReset or reboot is recommended after installation



The minimum requirement is Microsoft .NET Framework 3.5 SP1

1.5.2.3.4 Prerequisites for the K2 for Reporting Services component



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 for Reporting Services



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The Microsoft SQL Server 2008 Reporting Services component is now optional for all K2 blackpearl installations and can only be installed during a custom K2 blackpearl installation. The K2 for Reporting Services component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 for Reporting Services component	
Operating System* **	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
<i>*32-bit and 64-bit support</i>	
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software	<ul style="list-style-type: none"> Microsoft SQL Server 2012 Reporting Services or Microsoft SQL Server 2008 Reporting Services Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en <p>NOTE: K2 Reports Runtime and K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2008 SP1</p> <ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 Redistributable Package and Microsoft .Net Framework 4 http://www.microsoft.com/downloads/details.aspx?FamilyID=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en Microsoft Internet Explorer 8 or 9 or 10 (Plug-in support is only available in Internet explorer 10 on the desktop, and this version of Internet Explorer 10 must be used for items built on Silverlight, such as the K2 designer for SharePoint). Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server)



It is recommended that you run SQL Reporting Services in Native mode, however K2 blackpearl supports SharePoint Integrated mode. For more information see **KB article How K2 Reporting has changed since K2 4.5** (<http://help.k2.com/en/kb001195.aspx>)

The minimum requirement is Microsoft .NET Framework 3.5 SP1

1.5.2.3.5 Prerequisites for the K2 for Visual Studio component



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 for Visual Studio



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 for Visual Studio component installs the K2 Designer for Visual Studio. This designer allows developers to use a tool they are familiar with (Visual Studio) to develop, design, and deploy K2 applications. The K2 for Visual Studio component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 for Visual Studio component	
Operating System * * *	<ul style="list-style-type: none"> Windows Vista SP1 or SP2 or Windows 7 with or without SP1 or Microsoft Windows 8 (Windows 8 / Pro / Enterprise) Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
<p>*Latest security patches *32-bit and 64-bit support</p>	
Additional Software	<ul style="list-style-type: none"> Microsoft .NET Framework 4 (.NET Framework 4.5 is supported but not required): For more information on .NET framework and K2, please see the topic: .NET Technologies Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) with or without Sp1 A User Manager: Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. Windows Powershell Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx Excel Web and Calculation Services with Trusted file locations for Excel spreadsheets or Microsoft SharePoint Server 2010 and Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets

You can validate that you have the appropriate extensions installed by going into Visual Studio and selecting Help > About. You should see the following extensions listed:

- Extensions for Windows WF

1.5.2.3.6 Prerequisites for the K2 for SharePoint component



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 for SharePoint



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 for SharePoint Server component installs the necessary features and integration with either Microsoft Office SharePoint Server 2007, Windows SharePoint Services 3.0, SharePoint 2010 Foundation or SharePoint Server 2010. This includes the K2 Worklist Web Part, K2 Designer for SharePoint, and integration components. The K2 for SharePoint component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 for SharePoint component	
Operating System ***	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
*Latest security patches *32-bit and 64-bit support	
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software *	
	<ul style="list-style-type: none"> Microsoft .NET Framework 4 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Microsoft Windows SharePoint Services 3.0 (WSS) SP2 or Microsoft Office SharePoint Server 2007 (MOSS) Standard, Enterprise SP3 or SharePoint 2010 Foundation or SharePoint 2010 Foundation SP1 or SharePoint Server 2010 or SP1 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode) SharePoint Foundation 2010 Client Side Object Model Redistributable (required for CSOM Service Broker and is installed on the K2 Server) Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en Visual Studio 2010 Web Deployment Projects (required for Forms Technology): http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24509
* IISReset or reboot is recommended after installation	



- The following article can be helpful when experiencing conflicts between Microsoft SharePoint and Microsoft Report Viewer:
<http://help.k2.com/en/KB001205.aspx>
- The minimum requirement is Microsoft .NET Framework 3.5 SP1

1.5.2.3.7 K2 Studio



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 Studio



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 for Studio component installs the K2 Designer for Studio. The K2 for Studio component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 for Studio component	
Operating System * * *	Microsoft Windows Server 2008 Standard, Enterprise, R2, SP1, SP2 or Microsoft Windows Vista with SP1 or SP2 (Business or Ultimate) or Windows 7 with or without SP1 or Microsoft Windows 8 (windows 8 / Pro / Enterprise)
<p>*Latest security patches *32-bit and 64-bit support</p>	
Additional Software	<ul style="list-style-type: none"> Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5< br /> For more information on .NET framework and K2, please see the topic: .NET Technologies Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. Microsoft Exchange Server 2007 SP3 (required for Exchange Wizard) or Microsoft Exchange Server 2007 Management Tools SP3 or Microsoft Exchange 2010 SP1 or Microsoft Exchange 2010 SP2 Windows Powershell Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx Microsoft Office SharePoint Server (MOSS) 2007 SP3 <ul style="list-style-type: none"> Excel Web and Calculation Services Trusted file locations for Excel spreadsheets Microsoft SharePoint Server 2010 RTM or SP1 Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets Either Visual Studio 2012 or Visual Studio 2010 Web Deployment Projects is required to deploy projects in K2 Studio (http://www.microsoft.com/en-us/download/details.aspx?id=25163) <p>Windows SDK v7.0A is required when the 'Generate ASP Pages' option is used. This is installed and configured when Visual Studio 2010 or 2012 is installed.</p>

1.5.2.3.8 Prerequisites for the K2 Workspace



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 Workspace



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 Workspace is a web based application used to manage processes and the K2 environment. The K2 Workspace requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Workspace	
Operating System * * *	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows Server 2008 R2, SP1 or Windows Server 2012
*Latest security patches *32-bit and 64-bit support	
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software	
	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Microsoft Report Viewer Redistributable 2005 SP1 <ul style="list-style-type: none"> Full installation: http://www.microsoft.com/downloads/details.aspx?FamilyID=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=en Upgrade installation: http://www.microsoft.com/downloads/details.aspx?FamilyId=35F23B3C-3B3F-4377-9AE1-26321F99FDF0&displaylang=en and Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en
NOTE: K2 Reports Runtime – requires Microsoft Report Viewer Redistributable 2008 SP1 K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2005 SP1	
	<ul style="list-style-type: none"> Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Silverlight 4 or 5: (required for View Flow) http://www.silverlight.net/getting-started
* IISReset or reboot is recommended after installation	

1.5.2.4 Prerequisites by Role

Prerequisites by Role

There are several roles that servers play in a K2 Environment. One server may play multiple roles, or many servers may be clustered together to perform a single role. The K2 Installer will determine which platform version is being used and will install K2 blackpearl components accordingly. For all intents and purposes, the requirements for installing a 64-bit installation are identical to its 32-bit counterpart.

The following sections will describe the prerequisites for each role listed below:

K2 blackpearl Roles	
	K2 Server Runs the K2 Host Server
	Web Server Runs the K2 Workspace on top of Microsoft Internet Information Services (IIS)
	SharePoint Server Runs the K2 for SharePoint components on top of either Microsoft Office SharePoint Server 2007 or Windows SharePoint Services 3.0
	Reporting Services Server Runs the K2 for Reporting Services component on top of Microsoft SQL Server Reporting Services
	Database Server Houses the K2 Databases on top of Microsoft SQL Server 2008 or SQL Server 2012
	Client Machine Runs the client based K2 Designers

For more information see the online [K2 blackpearl Compatibility Matrix](#)

1.5.2.4.1 Prerequisites for the K2 Server role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



K2 Server

The K2 Server role is defined to be the server on which the K2 Host Server runs. The K2 Server component, configuration manager will be installed on this server.



Please note that Setup Manager needs .NET Framework 3.5 SP1 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

The K2 Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Server	
Operating System	* *** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
Windows Components	<ul style="list-style-type: none"> ● Microsoft Message Queuing (MSMQ) Services <ul style="list-style-type: none"> ● Message Queuing Server ● Directory Service Integration ● A User Manager: The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured)
Additional Software	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5 <p style="margin-left: 20px;">For more information on .NET framework and K2, please see the topic: .NET Technologies</p> ● Windows Support Tools (see Install Windows Support Tools for more information: for 32-bit see http://go.microsoft.com/fwlink/?LinkId=62270. Note: Windows Support Tools is a prerequisite if the installer is to automatically set the SPNs during the installation of K2 blackpearl. Otherwise, the Windows Support Tool is regarded as optional software. ● Windows Identity Foundation Redistributable (for more information, see http://support.microsoft.com/kb/974405). ● Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). ● If CRM is used: Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server, the server must have .NET 4 enabled.) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9df&displaylang=en
Optional Software: Oracle	<p>64-bit Oracle Data Access Components (ODAC) (can be downloaded from the Oracle site, here.)</p> <p>Oracle version 9 and up is supported.</p> <p>Note: If the ODAC is not installed prior to registering a new service instance, an error is generated saying the assembly can not be loaded because it is either not present or one of its dependencies is missing.</p>
<p>*Latest security patches</p> <p>*32-bit and 64-bit support</p>	



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.2.4.2 Prerequisites for the Web Server role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



Web Server

The Web Server role is defined to be the server on which the K2 Workspace runs. The K2 Workspace component, configuration manager, and K2 documentation will be installed on this server.

The Web Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the Web Server	
Operating System * **	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
*Latest security patches *32-bit and 64-bit support	
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software *	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Microsoft Report Viewer Redistributable 2005 SP1 <ul style="list-style-type: none"> Full installation: http://www.microsoft.com/downloads/details.aspx?FamilyID=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=en Upgrade installation: http://www.microsoft.com/downloads/details.aspx?FamilyId=35F23B3C-3B3F-4377-9AE1-26321F99FDF0&displaylang=en and Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en <p>NOTE: K2 Reports Runtime – requires Microsoft Report Viewer Redistributable 2008 SP1 K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2005 SP1 </p> <ul style="list-style-type: none"> Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Silverlight 4 or 5: (required for View Flow) http://www.silverlight.net/getting-started <p>* IISReset or reboot is recommended after installation</p>



- The minimum requirement is Microsoft .NET Framework 3.5 SP1



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.2.4.3 Prerequisites for the SharePoint Server role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



SharePoint Server

The SharePoint Server role is defined to be the server on which the K2 for SharePoint component will be installed, and is already running either Microsoft Office SharePoint Server 2007, Windows SharePoint Services 3.0, SharePoint 2010 Foundation or SharePoint Server 2010. The K2 for SharePoint component, configuration manager, and K2 documentation will be installed on this server.

The SharePoint Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the SharePoint Server	
Operating System	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
*Latest security patches *32-bit and 64-bit support	
Windows Components <ul style="list-style-type: none"> ● IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured) ● ASP.NET ● Windows Authentication Role Services 	
Additional Software *	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 ● Microsoft Windows SharePoint Services 3.0 (WSS) SP2 or Microsoft Office SharePoint Server 2007 (MOSS) Standard, Enterprise SP3 or SharePoint 2010 Foundation or SharePoint 2010 Foundation SP1 or SharePoint Server 2010 or SP1 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode) ● SharePoint Foundation 2010 Client Side Object Model Redistributable (required for CSOM Service Broker and is installed on the K2 Server) ● Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en ● Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en ● Visual Studio 2010 Web Deployment Projects (required for Forms Technology): http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24509
* IISReset or reboot is recommended after installation	



The minimum requirement is Microsoft .NET Framework 3.5 SP1



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.2.4.4 Prerequisites for the Reporting Services Server role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



Reporting Services Server

The Reporting Services Server role is defined to be the server on which the K2 Reports will be stored, and is already running Microsoft SQL Server Reporting Services. This may or may not be installed on the SQL Server itself, depending on your environment. The K2 for Reporting Services component, configuration manager, and K2 documentation will be installed on this server.

The Reporting Services Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the Reporting Services Server	
Operating System	<ul style="list-style-type: none"> Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
*Latest security patches	
*32-bit and 64-bit support	
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software	<ul style="list-style-type: none"> Microsoft SQL Server 2012 Reporting Services or Microsoft SQL Server 2008 Reporting Services Microsoft Report Viewer Redistributable 2008 <p>http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en</p> <p>or</p> <p>Microsoft Report Viewer Redistributable 2008 SP1</p> <p>http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en</p> <p>NOTE: K2 Reports Runtime and K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2008 SP1</p> <ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 Redistributable Package and Microsoft .Net Framework 4 http://www.microsoft.com/downloads/details.aspx?FamilyID=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en Microsoft Internet Explorer 8 or 9 or 10 (Plug-in support is only available in Internet explorer 10 on the desktop, and this version of Internet Explorer 10 must be used for items built on Silverlight, such as the K2 designer for SharePoint). Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server)



Important: You must be running Reporting Services in Native mode. K2 blackpearl does not currently support SharePoint Integrated mode.



The minimum requirement is Microsoft .NET Framework 3.5 SP1

Microsoft SQL Server 2008

In K2 blackpearl 4.5 and later the K2 Workspace Report Designer does not use the SSRS server.

SSRS integration is still supported for customers:

- Who wish to use the SSRS server to expose reports in other contexts other than K2 Workspace or K2 Process Portals
- Who wish to use other design tools and then import reports into K2 Workspace Report Designer

K2 blackpearl leverages the services available in SQL Server 2008, which provides the following features:

"Microsoft SQL Server 2008 Reporting Services (SSRS) provides a full range of ready-to-use tools and services to help you create, deploy, and manage reports for your organization, as well as programming features that enable you to extend and customize your reporting functionality." (<http://msdn.microsoft.com/en-us/library/ms159106.aspx>)

For further details on deployment options: <http://msdn.microsoft.com/en-us/library/bb522791.aspx>

For further details on security: <http://msdn.microsoft.com/en-us/library/bb522728.aspx>



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.2.4.5 Prerequisites for the Database Server role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



Database Server

The Database Server role is defined to be the server on which the K2 Database will be housed, and is already running Microsoft SQL Server. The K2 Database is created and configured during the installation of the K2 Server component. The K2 Server component is not normally installed on the SQL server.

The Database Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the Database Server	
Operating System ***	Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
* Latest security patches **32-bit and 64-bit support	
Windows Components	<ul style="list-style-type: none"> Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured)
Additional Software	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Note: .NET Framework 4.0 is supported but not a prerequisite Microsoft SQL Server 2012 Express, Standard, BI, Enterprise or Microsoft SQL Server 2008 Express, Standard, Enterprise SP3 or Microsoft SQL Server 2008 R2 SP1

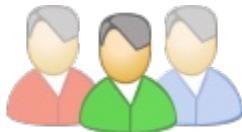


While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.2.4.6 Prerequisites for the Client Machine role



For the latest information concerning K2 blackpearl software compatibility, please see the article **K2 blackpearl Compatibility Matrix** on <http://help.k2.com/en/blackpearlmatrix.aspx>



Client Machine

The Client Machine role is defined to be the desktop or laptop on which the client based K2 designers will be installed, for example the K2 Designer for Visual Studio. The appropriate K2 designer component, configuration manager, and K2 documentation will be installed on this machine.

The Client Machine role requires the following prerequisites:

K2 blackpearl Prerequisites for the Client Machine	
Operating System	<ul style="list-style-type: none"> Microsoft Windows Vista with SP1 or SP2 (Business or Ultimate) or Windows 7 with or without SP1 or Microsoft Windows 8 (Windows 8 / Pro / Enterprise)
<small>* Latest security patches **32-bit and 64-bit support</small>	
Additional Software and Settings	
	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 or .NET 4 http://www.microsoft.com/downloads/details.aspx?familyid=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 Designer for Visual Studio	<ul style="list-style-type: none"> Microsoft .NET Framework 4 Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) with or without SP1 or Microsoft Visual Studio 2012 (Professional / Premium / Ultimate)
K2 Studio	<ul style="list-style-type: none"> Microsoft .NET Framework 4 Either Visual Studio 2012 or Visual Studio 2010 Web Deployment Projects is required to deploy projects in K2 Studio (http://www.microsoft.com/en-us/download/details.aspx?id=25163) Windows SDK v7.0A is required when the 'Generate ASP Pages' option is used. This is installed and configured when Visual Studio 2010 or 2012 is installed.
K2 Designer for SharePoint	<ul style="list-style-type: none"> Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Silverlight 4 or 5: http://www.silverlight.net/getting-started
K2 Workspace - View Flow (optional)	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 Microsoft Silverlight 4 or 5: http://www.silverlight.net/getting-started <p>See KB001183 - How to: Remove the option to install Silverlight when accessing the View Flow for the first time</p>
K2 Documentation	<ul style="list-style-type: none"> Adobe Flash Player* http://www.adobe.com/go/EN_US-H-GET-FLASH Windows Media Player*



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Windows SDK v7.0A

Any project that uses the Generate ASP Page option requires that the Windows SDK v7.0A is installed. The SDK is installed and set up with Visual Studio 2010 or with Visual Studio 2008 Web Deployment Projects.

1.5.3 Before you begin



This section covers important information for installation. The user installing the K2 system should read through these sections before commencing the install.

Before you install K2 blackpearl, there are several configuration steps that you need to complete:

Windows Server 2008

- Set up DNS
- Set up Service Accounts
- Set up Permissions
- Set up NLB
- Set up MSMQ
- Set up DTC
- Set up IIS 7

Windows Server 2012

- Set up DNS
- Set up Service Accounts
- Set up Permissions
- Set up NLB
- Set up MSMQ
- Set up DTC
- Set up IIS 8

1.5.3.1 Service Account Requirements and Permissions

Set up Service Accounts

There are several service accounts that should be set up prior to installing K2 blackpearl. These service accounts are as follows:

Account	Used For
K2 Service Account	This account is used for the identity in which the K2 Server operates. This account will need permissions on the K2 Server and SharePoint Server.
K2 Installation account	The Installation Account is the account which the person installing and configuring K2 logs on to the servers with. This account must be a domain account.
K2 Administration Account	This account is used for basic administration of the K2 Server, such as setting security for the environment and managing services. This account may be the same as the K2 Service Account, but it is recommended that the accounts are different.
K2 Workspace Service Account	This account is used by the application pool that runs the K2 Workspace. This account will need permissions on the Web Server, and rights within Reporting Services.
SharePoint Service Account	This account is used by the application pool that runs SharePoint. Note: This account probably already exists in your environment.
Reporting Services Service Account	This account is used by SQL Server Reporting Services to run the application pool for the web services and reports home page. Note: This account probably already exists in your environment.

1.5.3.1.1 Installation Account

The Installation Account is the account which the person installing and configuring K2 logs on to the servers with. This account must be a domain account.

The below permissions are required during installation and configuration of K2 blackpearl. After the installation is complete, you can revoke these permissions. However, you may need to add these permissions back when reconfiguring your environment.



It is recommended to install all K2 components using the K2 Service Account. Log on to the server as the K2 Service Account before installing.



It is strongly recommended that the Installation Account be in the same domain as the service accounts, and if possible, your user accounts. This will configure this domain as the default K2 User Manager label. To add additional domains, please see the [Adding Multiple Active Directory Domains](#) topic.

The Installation Account will need the following permissions during installation and configuration:

All Servers with K2 Components	
Permission	Used For
Local Administrator	In order to successfully install and configure K2 blackpearl components, the Installation User account must be a local administrator on all the servers that will have K2 components installed.

SQL Server	
Permission	Used For
dbcreator on the SQL Server	For the K2 components to be installed properly, the Setup User account needs dbcreator on the SQL server.
securityadmin on the SQL Server	For the K2 components to be installed properly, the Setup User account needs securityadmin on the SQL server.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.1.2 Set up the K2 Service Account

The K2 Service Account is the account under which the K2 service runs.

The rest of this guide will use domain\K2 Service Account as a placeholder for the K2 Service account name. When installing K2 in your environment, replace this placeholder with your actual account name.

The K2 Service Account will need the following permissions:

K2 Server	
Permission	Used For
Log on as a Service	In order to run the K2 blackpearl Service, the Service Account will need this permission. To see how to set this permission, click here .
Rights	Folder or Registry Key
Full Control	%SYSTEMROOT%\temp
Full Control	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA
Full Control	HKEY_LOCAL_MACHINE\SOFTWARE\SourceCode\Logging (* Note)
Modify	%PROGRAMFILES%\K2 blackpearl\Host Server\Bin (* Note)
* Note	The following step is done post installation

SharePoint Server	
Permission	Used For
Site Collection Administrator	In order for the K2 Service to create sites, assign permissions, work with the SharePoint Workflow Integration features, and for the Identity Service to be able to resolve and cache SharePoint groups, the service account needs to be a Site Collection Administrator on all sites where K2 features are to be used.
Local Administrator	If your security policies do not allow for local administration rights on servers, please see the below table for the specific permissions required.
Rights	Folder or Registry Key
Full Control	%SYSTEMROOT%\temp
Full Control	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA
Full Control	HKEY_LOCAL_MACHINE\SOFTWARE\SourceCode\Logging (* Note)
Write Access	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12 (Applicable to Microsoft Office SharePoint Server 2007)
Write Access	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\14 (Applicable to Microsoft SharePoint Server 2010)
* Note	The following step is done post installation

Authenticated Users	
Rights	Folder or Registry Key
Modify	C:\Users and all folders below. (Applicable to Windows 2008 Servers). Apply this to all SharePoint Web Front Ends



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.1.3 Set up the K2 Workspace Service Account

The K2 Workspace Service Account is the account that the K2 Workspace application pool will run under.

The rest of this guide will use domain\K2 Workspace Service Account as a placeholder for the K2 Workspace Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

The K2 Workspace Service Account will need the following permissions:

Web Server	
Permission	Used For
IIS_WPG Local Group	In order to function properly as an application pool within IIS, the K2 Workspace Service Account needs to be a member of this group if Windows Server 2003 is used.
IIS_IUSRS	In order to function properly as an application pool within IIS, the K2 Workspace Service Account needs to be a member of this group if Windows Server 2008 is used
Rights	Folder or Registry Key
Modify	%SYSTEMROOT%\temp

In K2 blackpearl 4.5 the K2 Workspace Report Designer does not use the SSRS server.

SSRS integration is still supported for customers:

- Who wish to use the SSRS server to expose reports in other contexts other than K2 Workspace or K2 Process Portals
- Who wish to use other design tools and then import reports into K2 Workspace Report Designer

Reporting Services Server	
Permission	Used For
Content Manager	The K2 Workspace Application pool Account (i.e. the Service Account) must be added in the Content Manager role on the SQL Server Machine, where the SSRS Server has been installed and configured.

Application Pool Rights

The K2 Workspace Service Account will require elevated permissions to run the application pool. We will use the aspnet_regiis command to configure this. This tool ships with the .NET Framework, and takes the pain out of configuring all the required NTFS permissions, IIS_WPG group membership, security policy user rights assignments, and IIS metabase access rights. For more information, see the MSDN article on setting security rights for .NET Applications, at <http://msdn2.microsoft.com/en-us/library/ms998297.aspx>.

To use the aspnet_regiis command, perform the following steps:

1. Open a command prompt (Start > Run > cmd)
2. Change directories to the .NET Framework folder (C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727)
3. Type aspnet_regiis -ga domain\K2 Workspace Service Account and hit Enter
4. After the command completes, type **iisreset** and hit Enter



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.1.3.1 IIS Group Membership

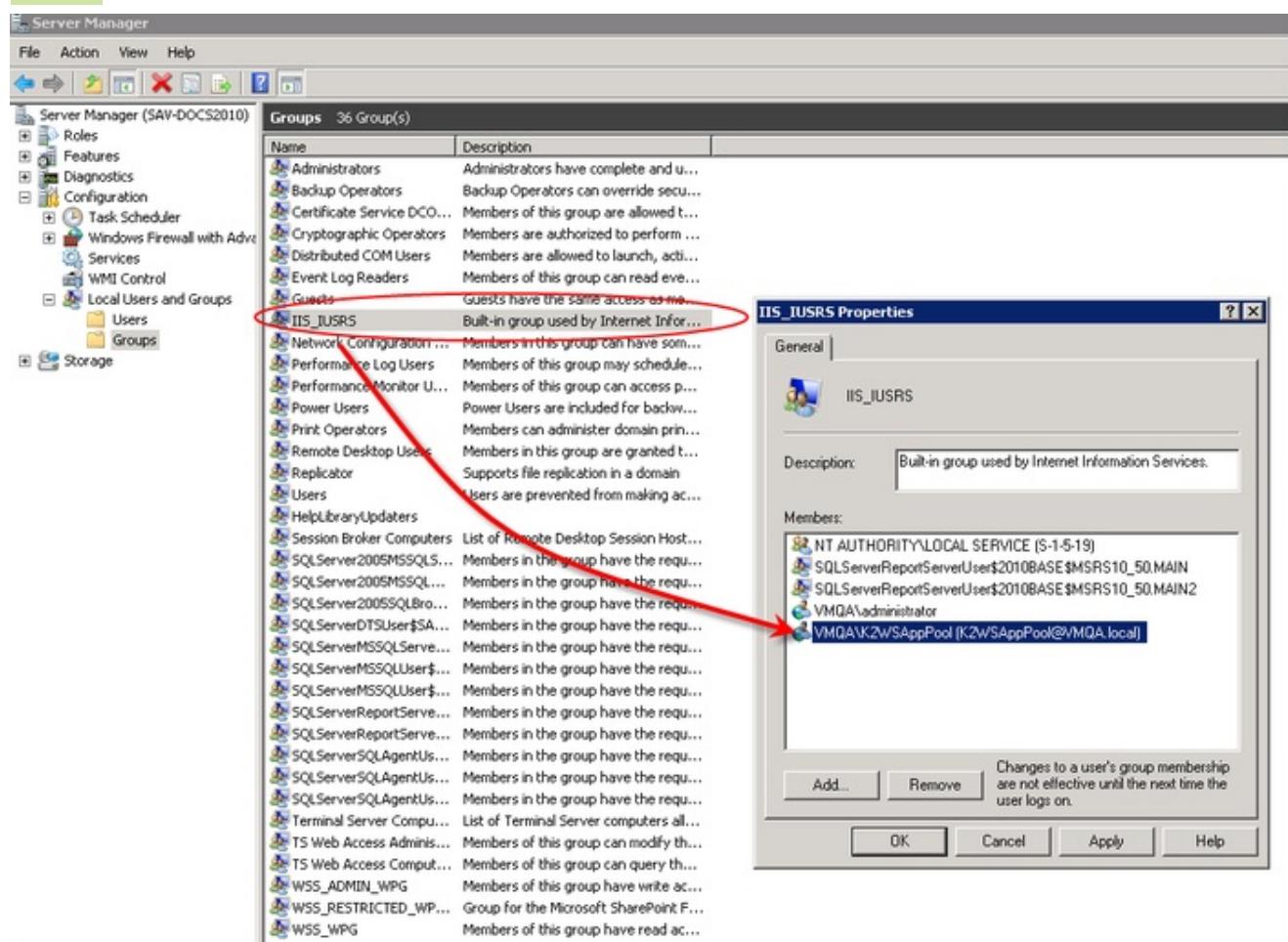
Formerly in Windows Server 2003, the group used by IIS was called "IIS_WPG", this group is no longer available under Windows Server 2008 and has been renamed to "IIS_IUSRS". The new group for IIS can be located by following these steps:



The following steps cannot be performed from an Active Directory machine

- 1
- 2
- 3
- 4
- 5

- Click Start to open the **Windows Start** menu
- Highlight **Computer** and right click, select **Manage**
- When the **Server Manager** opens, open the following nodes: **Configuration > Local Users and Groups > Groups**
- Under groups the IIS_IUSRS group can be located as shown below
- The account for the Workspace Application Pool must be added to this group, which is demonstrated in the image, or to Add a new User Account:
 1. Click **Add**
 2. Enter the name of the User account in part or whole into the Add User field
 3. Click **Check Names**, to confirm the name or make a selection if there are more than one with similar naming
 4. Click **OK**
 5. Click **OK** when complete





While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.1.4 Set up the SharePoint Service Account

The SharePoint Service Account is the account that the SharePoint application pool will run under. This account probably already exists in your environment, but there are some permissions that should be validated to ensure that the K2 integration with SharePoint functions properly.

The rest of this guide will use domain\SharePoint Service Account as a placeholder for the SharePoint Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

The SharePoint Service Account will need the following permissions:

SharePoint Server	
Permission	Used For
Local Administrator	In order to log K2 blackpearl Server messages to the Event log, the SharePoint Service Account must be a local administrator on the SharePoint server.
Rights	Folder or Registry Key
Modify	%SYSTEMROOT%\temp
Write	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\Layouts\Features
Write	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\ISAPI



Note that the \12\ in the folders mentioned above will be \14\ on a Microsoft SharePoint Server 2010 system.

SQL Server	
Permission	Used For
db_DataReader on the database	For the K2 Designer for SharePoint to function properly, the SharePoint Service Account needs read permission on the database. This is automatically set up by the Setup Manager during install. For upgrade scenarios where multiple k2 databases still exists, the database rights required for webdesigner, will still be applied on the the webdesigner database. For new installations where a single K2 database exists, the database rights for webdesigner will be applied on the webdesigner schema instead.
db_DataWriter on the database	For the K2 Designer for SharePoint to function properly, the SharePoint Service Account needs write permission on the database. This is automatically set up by the Setup Manager during install.
Execute on Stored Procedures in the database	For the K2 Designer for SharePoint to function properly, the SharePoint Service Account needs to be able to execute the Stored Procedures on the database. This is automatically set up by the Setup Manager during install.

Authenticated Users	
Rights	Folder or Registry Key
Modify	C:\Users and all folders below. (Applicable to Windows 2008 Servers). Apply this to all SharePoint Web Front Ends



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.1.5 Set up the Reporting Services Service Account

The Reporting Services Service Account is the account that the Reporting Services application pool (called ReportServer) will run under. This account probably already exists in your environment, but there are some permissions that should be validated to ensure that the K2 integration with Reporting Services functions properly.

The rest of this guide will use domain\Reporting Services Service Account as a placeholder for the Reporting Services Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

Application Pool Rights

The SQL Reporting Services Service Account will require elevated permissions to run the application pool. We will use the aspnet_regiis command to configure this. This tool ships with the .NET Framework, and takes the pain out of configuring all the required NTFS permissions, IIS_WPG group membership, security policy user rights assignments, and IIS metabase access rights. For more information, see the MSDN article on setting security rights for .NET Applications, at <http://msdn2.microsoft.com/en-us/library/ms998297.aspx>.

To use the aspnet_regiis command, perform the following steps:

- 1
- 2
- 3
- 4

- Open a command prompt (Start > Run > cmd)
- Change directories to the .NET Framework folder (C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727)
- Type aspnet_regiis -ga domain\Reporting Services Service Account and hit Enter
- After the command completes, type **iisreset** and hit Enter

Reporting Services Permissions

The SQL Reporting Services Service Account will also require permissions on the SQL Reporting Services databases. To set these permissions, perform the following steps:

- 1
- 2
- 3
- 4
- 5
- 6
- 7

- Open **Reporting Service Configuration** (Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration)
- Connect** to the appropriate Instance
- On the Web Service Identity tab, confirm that Reporting Services picked up the new service account and listed it in the **ASP.NET Service Account** text box
- Make sure the SQLRS Service Account is selected, and click **Apply**
- The Task Status will update, and the icon next to the Web Service Identity will change to Configured (a green check mark)
- Close the Reporting Services Configuration Manager window
- Open a command prompt and perform an **IIS Reset** again (type iisreset and hit Enter)

Additional Configuration.

In order for users to browse the reports on the server, the following permissions must be configured:

Server Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role System User
 Home Folder Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role Browser



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2 Microsoft 2008 Support and Configuration Requirements

Introduction

Microsoft has updated their product stack in their operating system, data storage and software development tools with the 2008 offerings. The focus of this document is to address the support that K2 offers with regards to these Microsoft product offerings and how to configure them to work with K2.

The Microsoft products that previous K2 blackpearl installations operate with were systems that utilize Windows Server 2003 as the base operating system, SQL 2005 for data storage, and Visual Studio 2005 or 2008 as the process design tool. Currently Windows Server 2008 is the base operating system with SQL Server 2008 SP1 or later for data storage and Visual Studio 2010 or later as one of the process design tools (the other tools being K2 studio, K2 Designer for SharePoint and K2 Forms).

Before you begin ensure that you have read this document in full before attempting your K2 installation on Windows Server 2008. Many of the configuration steps **MUST** be performed prior to installing K2 blackpearl.

MOSS

If you are running Microsoft Office SharePoint Server (MOSS) 2007 on Windows Server 2003, and you wish to upgrade to Windows Server 2008, you must install the Office System Service Pack 1 before upgrading the operating system. If performing a clean installation of MOSS, you must use the Service Pack 1 of the installation source for MOSS.

For more information, see [Windows Server 2008 Resource Center for SharePoint Products and Technologies](#) on TechNet.

If more information is required then refer to the following Microsoft site links for information on the respective products:

- Windows Server 2008 R2: <http://www.microsoft.com/en-us/server-cloud/windows-server/default.aspx>
- SQL Server 2008 SP1: <http://www.microsoft.com/sqlserver/en/us/default.aspx>
- Microsoft Visual Studio 2010: <http://msdn.microsoft.com/en-us/vstudio/default.aspx>

Windows Server 2008

Windows Server 2008 delivers valuable new functionality and powerful improvements to the core Windows Server operating system to help organizations of all sizes increase control, availability, and flexibility for their changing business needs. New Web tools, virtualization technologies, security enhancements, and management utilities help save time, reduce costs, and provide a solid foundation for your information technology (IT) infrastructure.

Windows Server 2008 supersedes Windows Server 2003 as the server-based operating system. Windows Server 2008 is strongly recommended for new machines, new system infrastructure as Microsoft will be shortly discontinuing the availability of licenses for Windows Server 2003. Windows Server 2008 also introduces IIS7 to the production environments; IE8 is also fully supported.

Before you install K2 blackpearl, there are several configuration steps that you need to complete:

- Set up DNS
- Set up Service Accounts
- Set up Permissions
- Set up NLB
- Set up MSMQ
- Set up DTC
- Set up IIS 7

1.5.3.2.1 Adding DNS Entries

Setting up DNS

It is important to have the DNS lookup zones configured before installing K2 blackpearl. During the configuration of the K2 components, connections will be made to the various server roles to ensure that the components can talk to each other appropriately. If the DNS settings are incorrect, your K2 environment will not function correctly.



DNS entries must be added by a domain administrator who has rights to add DNS host entries.

To set up the DNS, follow the below steps:



On the Domain Controller, open the **DNS Management Console** (Start > All Programs > Administrative Tools > DNS, or run dnsmgmt.msc)



Expand the Forward Lookup Zones node, and add a **New Host (A or AAAA)** to your domain



In the **New Host** window, enter in the appropriate name and IP Address, make sure the Create associated pointer (PTR) record check box is checked, and click Add Host



If you are using a cluster, be sure to use the virtual IP address of the cluster.

Repeat the above steps for as many servers as you have in your K2 environment.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.2 Set SPN



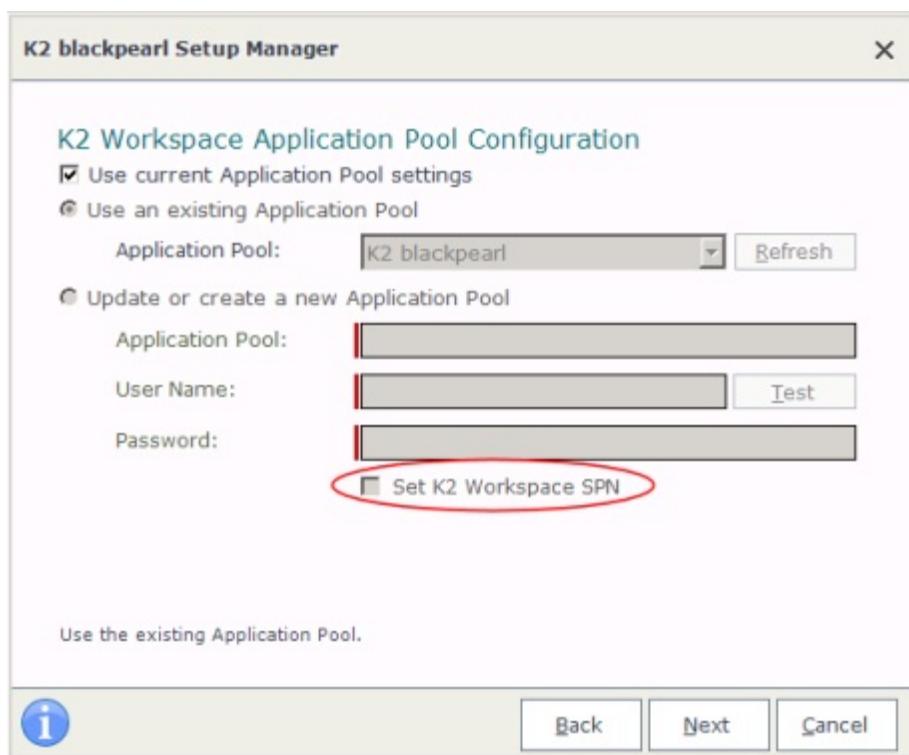
This section applies to preparing for installing distributed environments where Kerberos will be implemented. SetSPN.exe is a tool supplied along with the Windows Server 2008 operating system.

Set SPN



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

During the installation of K2 blackpearl, on a number of user page locations the Setup Manager will prompt the user to set an SPN. If this option is enabled, then the SPN for the Service instance will be created automatically during the installation process. Shown below is an example user page, where the user is prompted to enable "Set K2 Workspace SPN".



When the K2 Setup Manager has been enabled by the user to set SPNs, the setup manager proceeds to set SPNs regardless of whether SPNs are already active. This may result in the creation of duplicate SPNs. The user can check if SPNs are already active by using the SetSPN.exe tool provided with Windows Server 2008. If an SPN already exists for the service instance, there would be no need to enable the option to automatically set SPNs. The K2 Analysis tool can also be used to detect errors such as duplicate SPN's but this can only take place once K2 blackpearl is installed. By using the SetSPN tool before, duplicate SPNs can be detected beforehand. Example usage of the SetSPN commands:

Switch	Usage
- X	Search for duplicate SPNs
- X - F	Search tree wide for duplicate SPNs



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.2.1 Set SPNs for the K2 Service Account

K2 Service Account

In a distributed environment where components are installed on more than one server, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

There are two sets of SPNs that need to be set up for the K2 Service Account:

- K2Server
- K2HostServer

The following placeholders are used in the commands:

- domain\K2 Service Account - The K2 Service Account that runs the K2 Service
- MachineName - The name of the computer on which the K2 Service is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the K2 Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly. The SPNs listed below are for K2 blackpearl.



If you have a K2 Server farm running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A K2Server/MachineName:5252 domain\K2 Service Account
- setspn -A K2Server/MachineName.FQDN:5252 domain\K2 Service Account
- setspn -A K2HostServer/MachineName:5555 domain\K2 Service Account
- setspn -A K2HostServer/MachineName.FQDN:5555 domain\K2 Service Account



If you are installing K2 blackpearl on an **NLB environment**, the MachineName will change to the the LBHostName

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\K2 Service Account



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.2.2 Set SPNs for the Reporting Services Service Account

Reporting Services Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order to access the K2 Reports from the K2 Workspace, you need to set the SPNs for the Reporting Services Service Account.

The following placeholders are used in the commands:

- domain\Reporting Services Service Account - The Reporting Services Service Account that runs the Reporting Services application pool
- MachineName - The name of the computer on which Reporting Services is running
- MachineName.FQDN - The fully qualified domain name of the computer on which Reporting Services is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you are using **Host Headers** to access your Reporting Services Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\Reporting Services Service Account
- setspn -A HTTP/MachineName.FQDN domain\Reporting Services Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\Reporting Services Service Account

Configure Delegation for Reporting Services Service Account

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.



Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)



Find the domain\Reporting Services Service Account and view its properties



On the Delegation tab, select the **Trust this user for delegation to specified services only** option

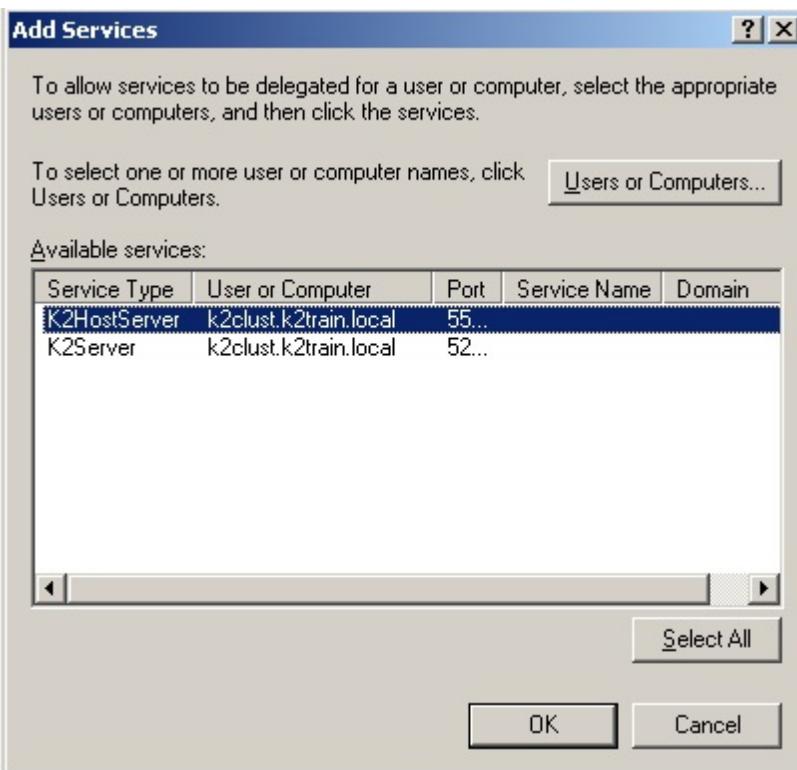


Select the **Use Kerberos only** option, and click on **Add**

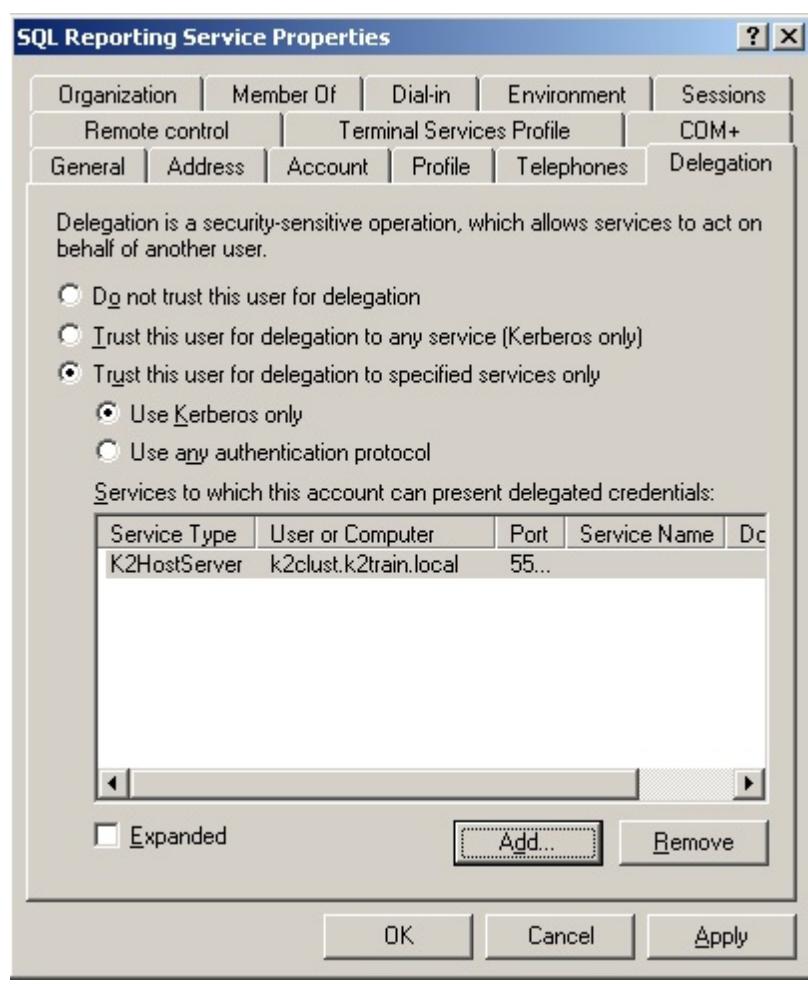


Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account

In the Available Services section, select the **K2HostServer** item listed:



Click **OK**. Your properties should resemble the following:





Click **OK**

Configure Delegation for the K2 Service Account

In order to use the SQL Server Reporting Services Service Object to schedule Reporting Services reports and include SmartObject data, you will need to configure the K2 Service Account with delegation.



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a **Trust this user for delegation check box**.

- 1** Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)
- 2** Find the domain\K2 Service Account and view its properties
- 3** On the Delegation tab, select the **Trust this user for delegation to specified services only** option
- 4** Select the **Use Kerberos only** option, and click on **Add**
- 5** Click on **Users or Computers** and select the domain\Reporting Services Service Account you created as the SQL Server Reporting Services Service Account
- 6** In the Available Services section, select the **HTTP** item listed
- 7** Click **OK** twice to exit the dialog windows



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.2.3 Set SPNs for the K2 Workspace Service Account

K2 Workspace Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order to access the K2 Workspace from another machine, you need to set the SPNs for the K2 Workspace Service Account.

The following placeholders are used in the commands:

- domain\K2 Workspace Service Account - The K2 Workspace Service Account that runs the K2 blackpearl application pool
- MachineName - The name of the computer on which the K2 Workspace is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the K2 Workspace is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have the K2 Workspace running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.



If you are using **Host Headers** to access your K2 Workspace, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\K2 Workspace Service Account
- setspn -A HTTP/MachineName.FQDN domain\K2 Workspace Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\K2 Workspace Service Account

Configure for Delegation

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a **Trust this user for delegation** check box.

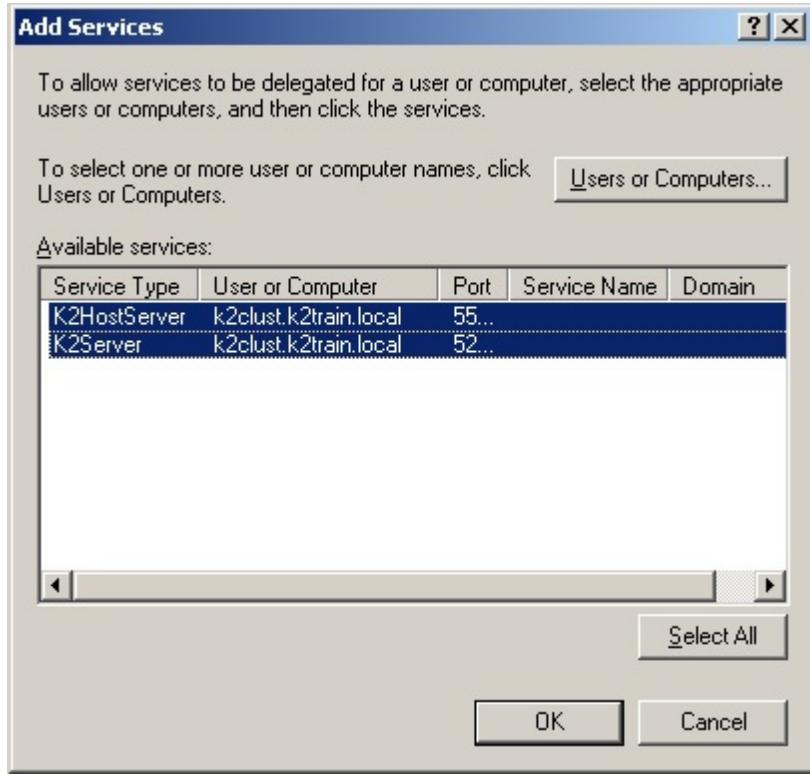
- 1 Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)
- 2 Find the domain\K2 Workspace Service Account and view its properties
- 3 On the Delegation tab, select the **Trust this user for delegation to specified services only** option
- 4 Select the **Use Kerberos only** option, and click on **Add**

(5)

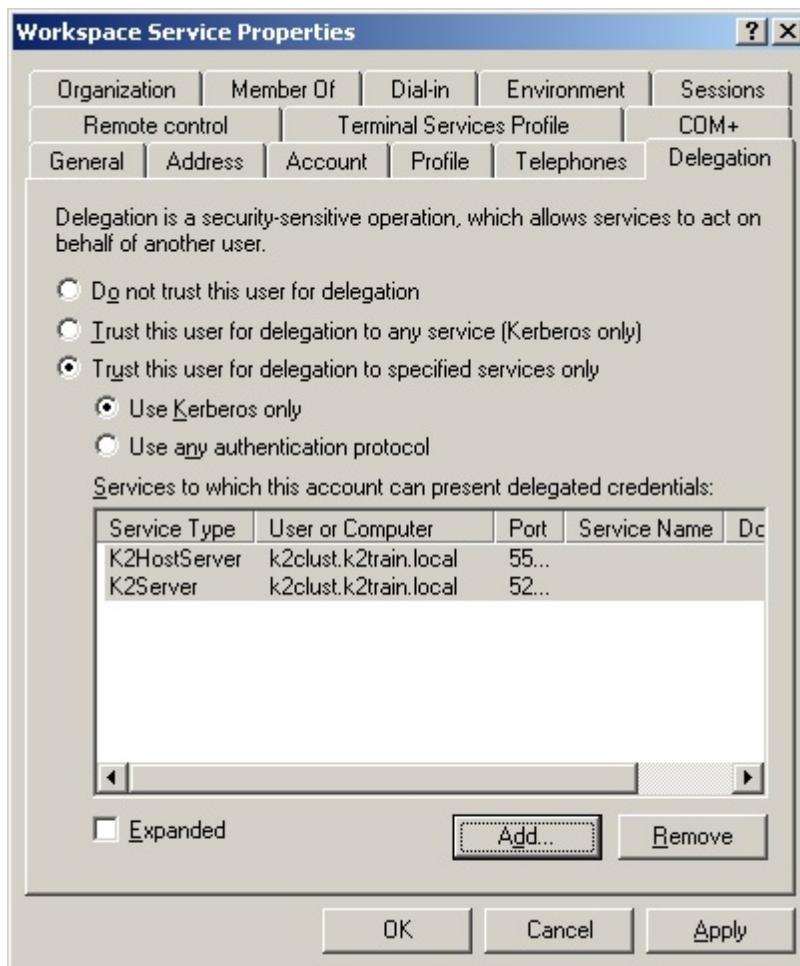
Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account

(6)

In the Available Services section, select both the **K2HostServer** and **K2Server** items listed:



Click **OK**. Your properties should resemble the following:



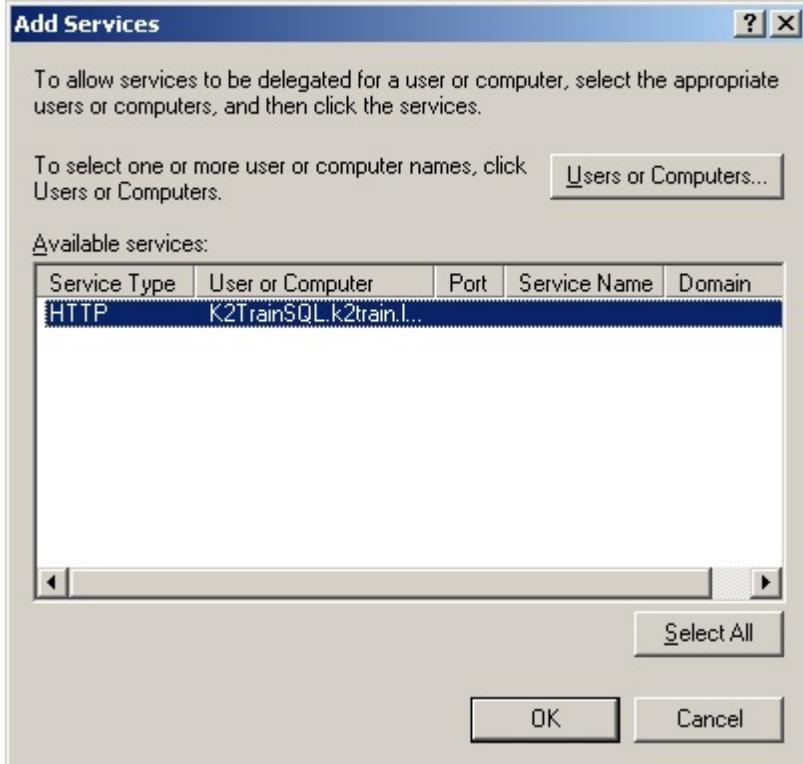
8 Click **OK**. This will allow the K2 Workspace Service Account to delegate to the K2 Server Service Account.

Also, since the SQL Reporting Services reports will also be rendered in the K2 Workspace, the K2 Workspace Service Account should also be allowed to delegate to the SQLRS Account.

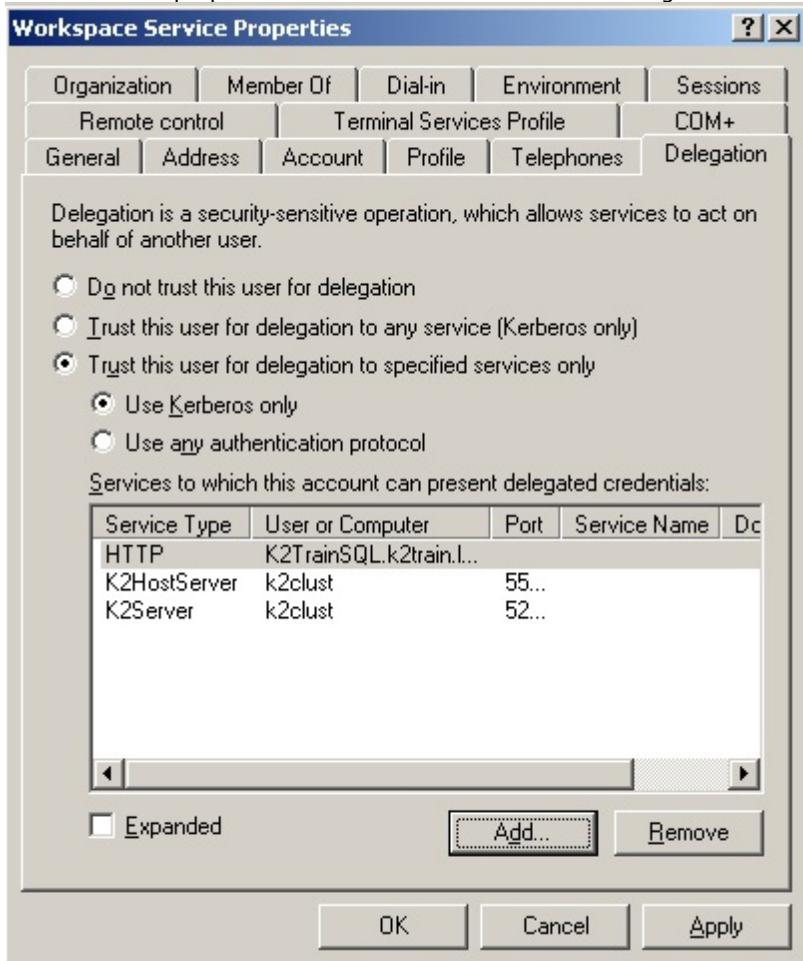
9 Click **Add** again

10 Click on **Users or Computers** and select the domain\Reporting Services Service Account you created as the SQL Reporting Services Service Account

In the Available Services section, select the HTTP item listed:



Click **OK**. Your properties should now resemble the following:



If you are using SharePoint Integrated process, K2 Workspace Service Account should also be allowed to delegate to the MOSS Account



- 14 Click **Add** again
- 15 Click on **Users or Computers** and select the domain\MOSS Account you created as the MOSS Server Account
- 16 In the Available Services section, select the HTTP item listed
- 17 Click **OK**



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.2.4 Set SPNs for the SharePoint Service Account

SharePoint Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order for the K2 Worklist Web Part and K2 Designer for SharePoint to function properly from another machine, you need to set the SPNs for the SharePoint Service Account.

The following placeholders are used in the commands:

- domain\SharePoint Service Account - The SharePoint Service Account that runs the SharePoint application pool
- MachineName - The name of the computer on which SharePoint Service is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the SharePoint Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have SharePoint running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.



If you are using **Host Headers** to access your SharePoint Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\SharePoint Service Account
- setspn -A HTTP/MachineName.FQDN domain\SharePoint Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\SharePoint Service Account

Configure for Delegation

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.

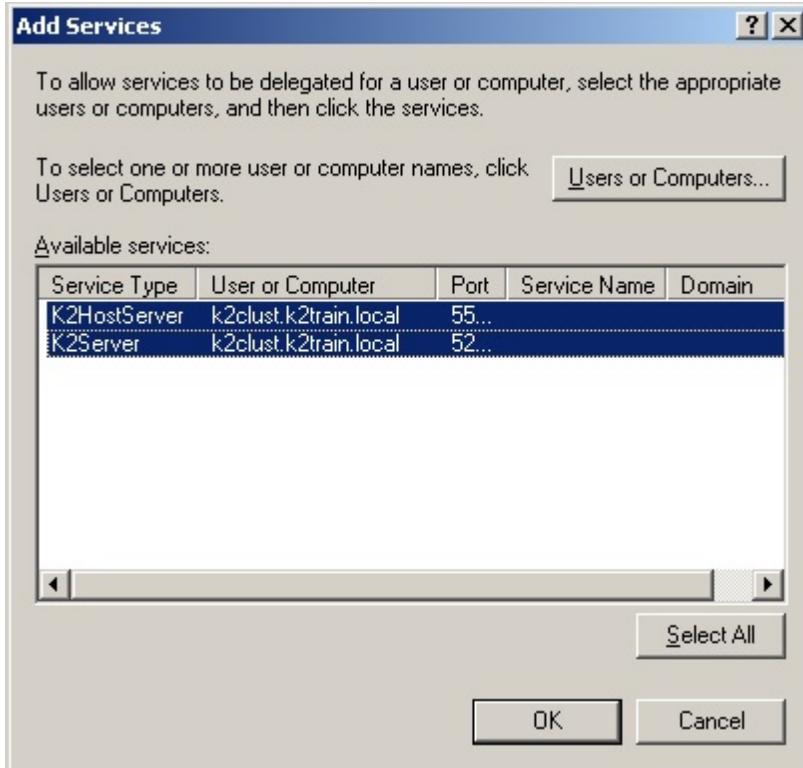
- 1 Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)
- 2 Find the domain\SharePoint Service Account and view its properties
- 3 On the Delegation tab, select the **Trust this user for delegation to specified services only** option
- 4 Select the **Use Kerberos only** option, and click on **Add**

(5)

Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account

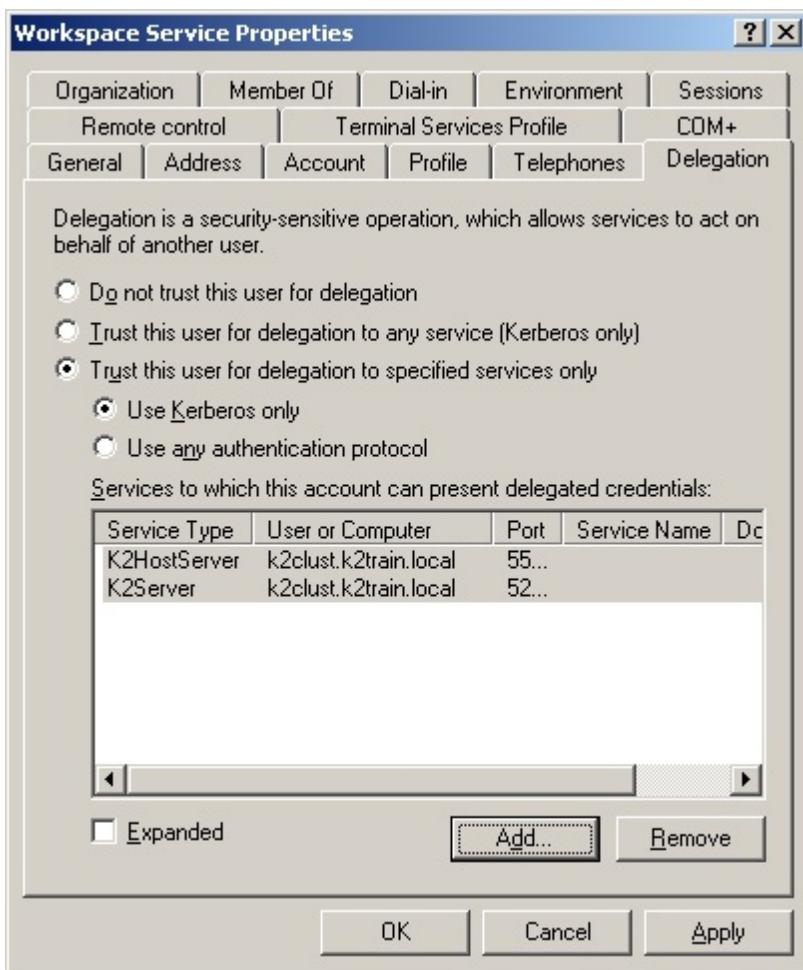
(6)

In the Available Services section, select both the **K2HostServer** and **K2Server** items listed:



(7)

Click **OK**. Your properties should resemble the following:





Click **Add** again



Click on **Users or Computers** and select the domain\K2 Workspace Account you created as the K2 RuntimeServices Account



In the Available Services section, select the HTTP item listed



Click **OK**. This will allow the SharePoint Service Account to delegate to the K2 Workspace Account.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.2.5 Set SPNs for the SQL Server Service Account

SQL Server Service Account

In a distributed environment where components are installed on more than one server, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

When the SQL service does not run under a local system account, the following SPNs apply for the SQL Server Service Account:

- MSSQLSvc

The following placeholders are used in the commands:

- domain\SQL Server Account - The Account that runs the SQL Server Service
- MachineName - The name of the computer on which the SQL Server is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the SQL Server is running
- port - The port that SQL Server is running under



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly. The SPNs listed below are for K2 blackpearl.



If you have a K2 Server SQL farm running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A MSSQLSvc/MachineName:port domain\SQL Server Account
- setspn -A MSSQLSvc/MachineName.FQDN:port domain\SQL Server Account



If you are installing K2 blackpearl on an **NLB environment**, the MachineName will change to the the LBHostServerName

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\SQL Server Account

You can also test the configuration by executing the following SQL Script on your SQL Server:

- select c.session_id, c.net_transport, c.auth_scheme, s.login_name from sys.dm_exec_connections c join sys.dm_exec_sessions s on c.session_id = s.session_id where s.login_name = '[domain]\[accountname]'

Where '[domain]\[accountname]' is the domain and username for the K2 service account. If Kerberos is being used, then it will display "KERBEROS".



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.3 Set up Permissions

Permissions and Authentication for Windows Server 2008

In addition to the Service Accounts already discussed, LDAP over SSL (LDAPS) will need to be configured for some environments in order to use the Active Directory Event Wizard. See [Using the AD wizard on Windows 2008](#) and the [LDAP requirement](#) in the troubleshooting section.

Other permissions that need to be set up as part of the installation process:

Server Role	Permission
K2 Server	The K2 Service Account will need permission to Log on as a Service.
Reporting Services Server	In order to access the temporary directory during runtime, some permissions are required for all authenticated users.
IIS Server	In order to access the temporary directory during runtime, some permissions are required for all authenticated users.
SharePoint Server	In order for K2 workflow processes to be able to be deployed, some permissions are required on the SharePoint directory.

1.5.3.2.4 Set up NLB

Setting up NLB

It is important to set up the Network Load Balancing (NLB) clusters before installing K2 blackpearl. It is also important to test that the cluster is performing correctly prior to installing K2 blackpearl. An incorrectly configured cluster can cause issues when using K2 blackpearl, and it adds a layer of complexity to troubleshooting.

The Network Load Balancing supported by K2 is:

- Windows Network Load Balancing Manager

The following sections will describe how to configure the two supported types as recommended by K2.

Windows Network Load Balancing Manager



Configuring Network Load Balancing is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

The 64-bit version of Network Load Balancing Manager (nlbmgr.exe) must be used for 64-bit Windows operating systems. For more information and to get the 64-bit version of the Network Load Balancing Manager tool, please refer to the following Microsoft KB Article: <http://support.microsoft.com/kb/892782>

When configuring a cluster, follow the below steps:



1 Open **Network Load Balancing Manager (nlbmgr.exe)** (Start > All Programs > Administrative Tools > Network Load Balancing Manager, or Start > Run > nlbmgr.exe)



2 Add a **New Cluster** (right-click on Network Load Balancing Clusters and select New Cluster)



3 On the **Connect** screen, connect to the first host in the cluster and select the appropriate connection as the interface. If the server has multiple network adapters, many interfaces may be displayed. Be sure to select the appropriate network adapter from the list, and click next



4 On the **Host Parameters** screen, select the host priority, add the host IP address and subnet mask, select the initial host start then click next



5 On the **Cluster IP Addresses** screen, add in any additional IP addresses that the cluster can be accessed from, and click next



6 In the **Cluster Parameters** window, enter the appropriate IP address, subnet mask, full internet name, and cluster operation mode, and click next



7 On the **Port Rules** screen, edit the existing rule to use the appropriate affinity. See the notes below for recommendations based on the cluster type. Click next to continue



8 To add a second node to the cluster, right-click on the newly created cluster and select **Add Host to Cluster**



9 Connect to the second host, and make sure to select the appropriate interface



For a K2 Host Server cluster, use a Unicast operation mode and set the affinity to **None**. Since the K2 Host Server is a stateless machine, no affinity is necessary per session.



For a K2 Workspace Server cluster, use a Unicast operation mode and set the affinity to **Single**. You will want to ensure that the web pages retain an affinity to the web server during the session.



For a K2 for SharePoint Server cluster, use a Unicast operation mode and set the affinity to **Single**. You will want to ensure that the web pages retain an affinity to the web server during the session.

The same is true for all server clusters that host web based components (such as Process Portals, web services, web parts).



In some cases, the Network Load Balancing Manager console will time out before the second node is configured. If that happens, just right-click on the cluster and select Refresh. You should see all the nodes in a Converged state. Make sure that your cluster is configured correctly before starting the installation.

As mentioned in the [Network Load Balancing Setup and Configuration](#) topic, at least two network adaptors are required when the

Unicast operation mode is selected.

Set up the NLB configuration to allow traffic through on the **K2 Workflow** (default of 5252) and **K2 Hostserver** (default of 5555) ports.

Hardware based load balancing

Follow the hardware manufacturer's guidelines for configuring a load balanced host. Use the above notes for specifics on a K2 Host Server Cluster or a K2 Workspace Server Cluster.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.5 MSMQ

MSMQ

MSMQ (Microsoft Message Queuing) is a messaging protocol that enables applications running on independent, physical servers to communicate in a failsafe manner. The method used to enable MSMQ for a K2 installation is dependent on how AD (Active Directory) has been configured for the domain. MSMQ Directory Service Integration is required for K2 blackpearl installations.



Note for Windows Server 2012: setting the appropriate permissions as mentioned in step 6 below (for Windows Server 2008). In Windows Server 2012, the permissions should be granted to the Root Object and not the Computer Object as in Windows Server 2008.

To install MSMQ in Windows Server 2008, follow the steps below:



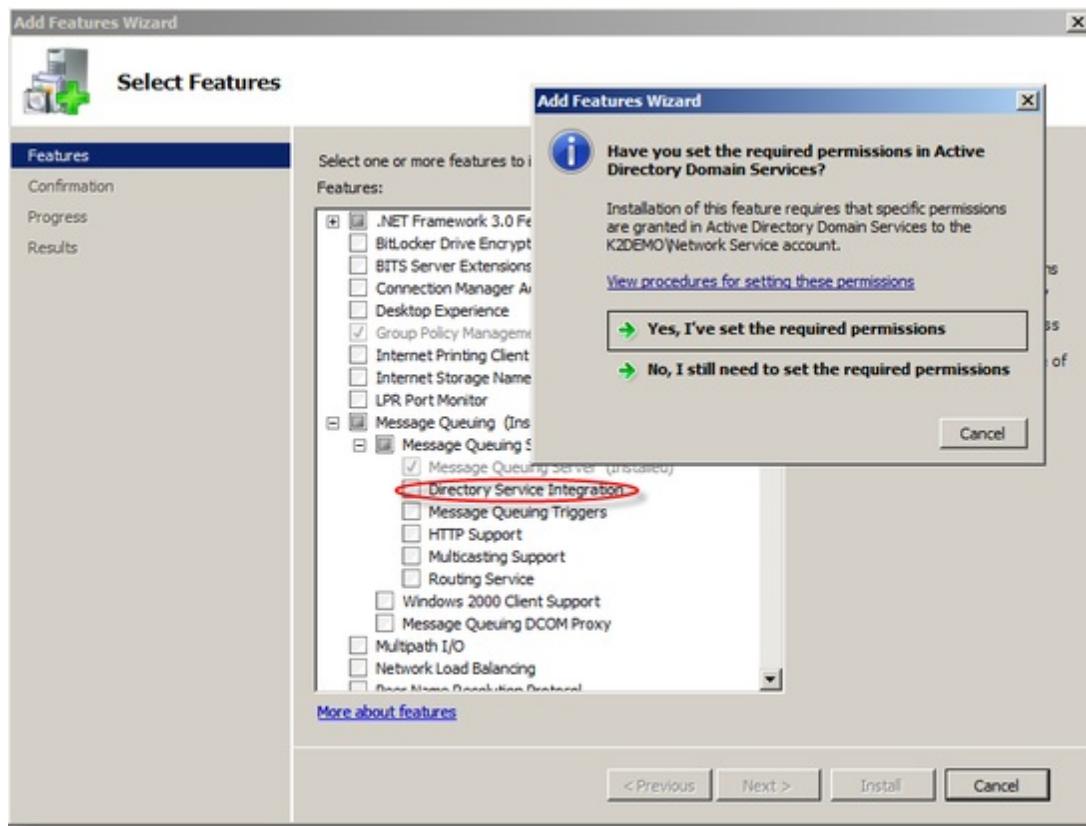
Open the **Programs and Features** window (Start > Control Panel > Programs and Features)



Click on the **Turn Windows features on or off** link



Then click on the **Add Features** button



Expand the **Message Queuing** node



Select **Message Queuing Services** and sub-nodes **Message Queuing Server** and **Directory Services Integration**



Choose the appropriate permissions settings response (please read the **Install Message Queuing** topic in the Windows Server 2008 Help file and take note of the two different methods for configuring permissions depending on whether the Windows Server 2008 computer is a domain controller or not)

Install Message Queuing

and appropriate permissions in Active Directory Domain Services before installing these features.

► To grant permissions for a computer object to the Servers object in Active Directory Domain Services before installing the Routing Service feature on a computer that is not a domain controller

1. Click Start, point to Programs, point to **Administrative Tools**, and then click **Active Directory Sites and Services** to open **Active Directory Sites and Services**.
2. Click to expand Active Directory Sites and Services, click to expand Sites, and then click to expand the site which this computer will be a member of.
3. Right-click **Servers** and select **Properties** to display the **Servers Properties** dialog box.
4. Click the **Security** tab of the **Servers Properties** dialog box.
5. Click the **Add** button to display the **Select Users, Computer, or Groups** dialog box.
6. Click the **Object Types** button to display the **Object Types** dialog box, click to enable **Computers**, and then click **OK**.
7. Enter the name of the computer for which the Routing Service or Directory Service Integration feature will be installed, click **Check Names**, and then click **OK**.
8. Enable the following permissions for this computer object:
 - Allow Read
 - Allow Write
 - Allow Create all child objects
9. After enabling these permissions, click **Advanced** to display the **Advanced Security Settings for Servers** dialog box.
10. Select the computer object from the list of permission entries and click the **Edit** button.
11. Select **This object and all descendant objects** from the **Apply to:** dropdown list and click **OK**.
12. Click **OK** to close the **Advanced Security Settings for Servers** dialog box.
13. Click **OK** to close the **Server Properties** dialog box.

► To grant the Network Service account the Create MSMQ Configuration Objects permission to the computer object in Active Directory Domain Services before installing the Directory Services Integration feature on a computer that is a domain controller

1. Click Start, point to Programs, point to **Administrative Tools**, and then click **Active Directory Users and Computers** to open **Active Directory Users and Computers**.
2. Click the **View** menu and click to enable the options for **Users, Groups, and Computers as containers** and

Click **Next**, then click **Install**

Once the installation has completed, click on **Close** and reboot the server

Post Installation Checks

Perform the following post installation steps to verify that MSMQ is configured correctly:

1

Verify that the Workgroup registry key located under HKLM\Software\Microsoft\MSMQ\Parameters\ is set to 0

2

Restart MSMQ

3

Verify that MSMQ is running in Domain mode after this procedure

4

In Computer Management confirm that Message Queuing has a node called Public Queues and that the K2Server Service account has rights to this folder

For further information regarding MSMQ and Windows Server 2008 integration view [http://technet.microsoft.com/en-us/library/cc749102\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc749102(WS.10).aspx)

1.5.3.2.6 Enable and Configure the DTC Components

The K2 Host Server makes use of Microsoft's Distributed Transaction Coordinator (DTC) to ensure data integrity between the K2 Server and the databases.



For the DTC to function correctly, the DTC Components need to be enabled and configured on all servers where K2 server components are installed, including the SQL Server, IIS Servers (including K2 Workspace, SharePoint, and Reporting Services Servers), and K2 Server.

Setting DTC to start automatically

The DTC is a service that coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

The DTC is provided as a standard service with the Windows Server 2008 operating system, but does not start up automatically as a service.

To configure the Service to startup automatically, do the following:

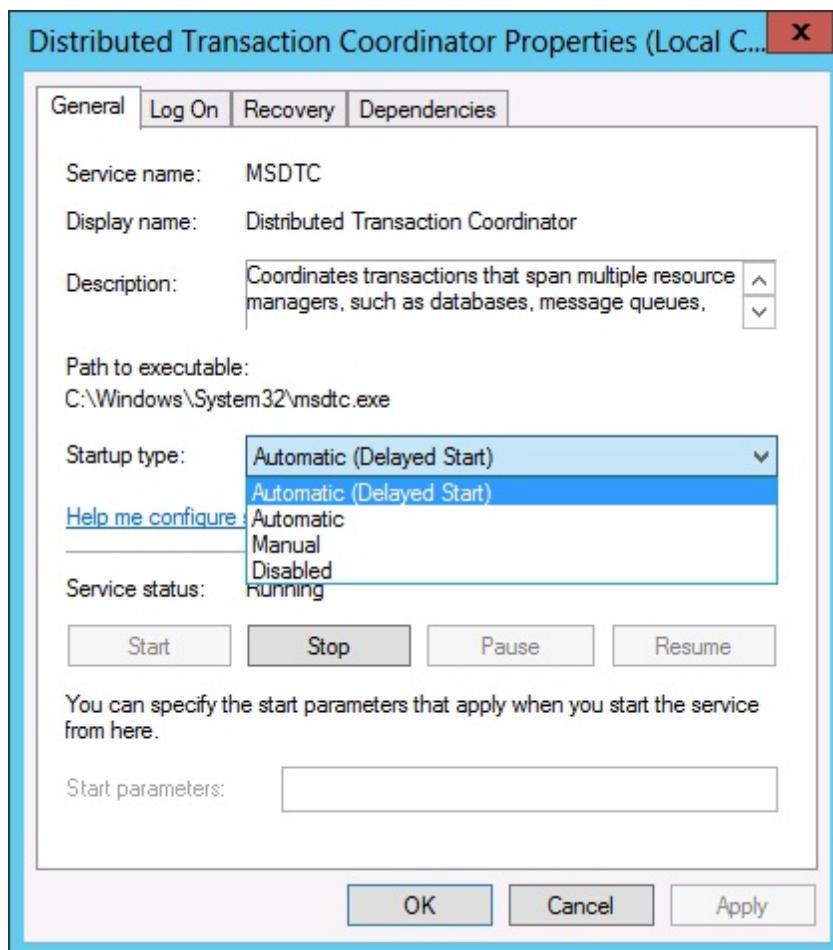
- 1
- 2
- 3

Open the **Services Manager** (Start > All Programs > Administrative Tools > Services)

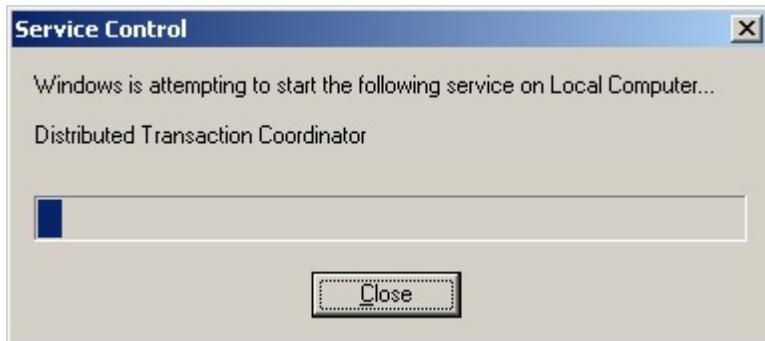
Locate the **Distributed Transaction Coordinator** Service in the list of services

To configure the service to start automatically, right click on the Distributed Transaction Coordinator Service and select **Properties**

In the dialog that appears, located the drop down menu for Startup type, and select the Automatic option, and click **OK**



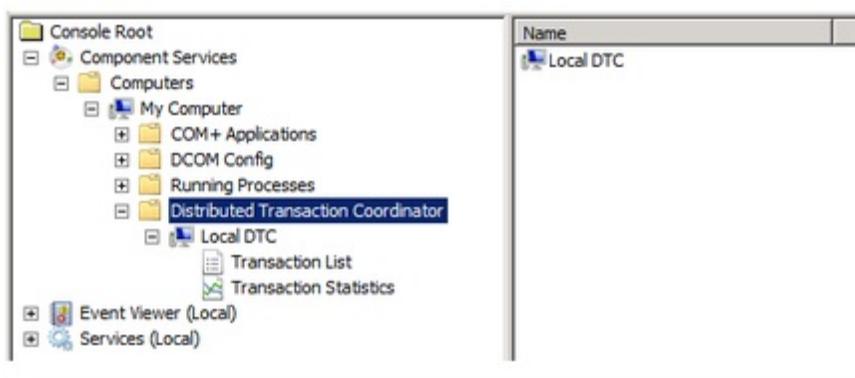
4 If the service is not started, click on the start button. The following dialog appears and displays the system's progress in starting the service. If the action is successful, the dialog disappears and the service's status is set to **Started**.



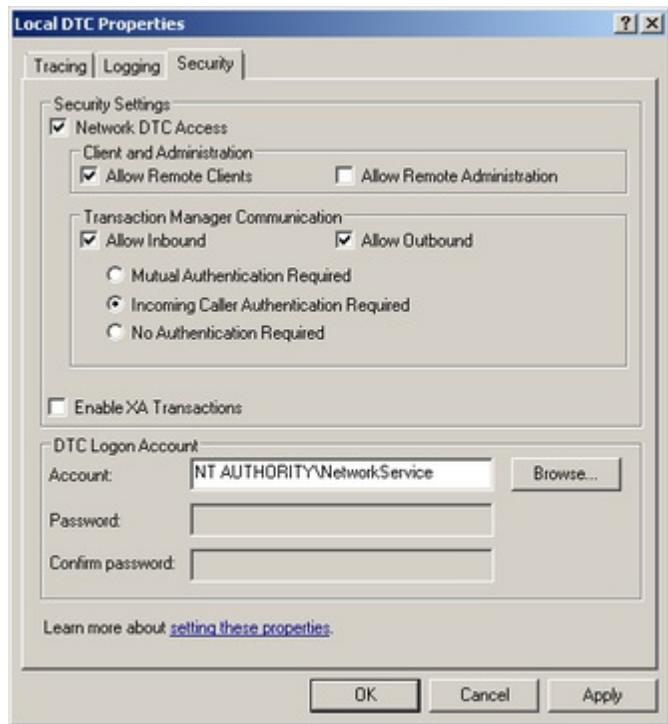
Configuring DTC

To configure DTC, follow the below steps:

- 1** Open Component Services
- 2** From the Console Node expand the following nodes Component Services > Computers > My Computer
- 3** From the My Computer node, locate the new node Distributed Transaction Coordinator
- 4** Expand the node to view the Local DTC
- 5** Right Click on Local DTC and select properties



- 6** On the Local DTC Properties tab, click the **Security** tab, and configure the properties as follows:
 - **Network DTC Access:** Checked
 - **Allow Remote Clients:** Checked
 - **Allow Inbound:** Checked
 - **Allow Outbound:** Checked
 - **Incoming Caller Authentication Required:** Selected



 Click **OK**, and in the warning dialog that appears, click **Yes**

 When the MS DTC service has been restarted, you can click **OK** on all the dialogs and close Component Management

 This setting is for clustered installations. For non-clustered environments, you can leave the Mutual Authentication Required option selected, as it is the most secure option. The MSDTC transaction mode must be set to either **No Authentication Required** or **Incoming Caller Authentication Required** to function correctly on a Windows Server 2008-based failover cluster.

Taken from: [http://msdn.microsoft.com/en-us/library/dd897479\(v=BTS.10\).aspx](http://msdn.microsoft.com/en-us/library/dd897479(v=BTS.10).aspx)

You must use the **Incoming Caller Authentication Required** transaction mode between Windows Server 2003-based computers in a clustered environment.

You must use the **No Authentication Required** transaction mode where one or more of the following conditions are true:

- The network access is between computers that are running Microsoft Windows 2000.
- The network access is between two domains that do not have a mutual trust configured.
- The network access is between computers that are members of a workgroup.

Even for the Incoming Caller Authentication Required setting to work in the cluster environment you need to have the environment configured correctly for the Kerberos authentication. And again this might break if there is a Windows 2000 server coming into picture as it would only work if you have set No Authentication Required throughout on all the Windows 2003 server machines.

Based on the explanation above, we recommend having "No Authentication Required" setting on the cluster and the other standalone server interacting with the cluster to avoid running into any compatibility issues with older operating systems and authentication failures.

Taken from: <http://support.microsoft.com/?id=899191>

DTC Configuration when a Firewall is Active

The following configuration is performed using the **dcomcnfg.exe** application located in the **Windows\System32** folder.

Firewall Configuration

Configure firewall to allow MSDTC access with the following command:

```
netsh advfirewall firewall add rule name="MSDTC" dir=in action=allow
program="%windir%\system32\msdtc.exe" enable=yes
```

Configure firewall to allow SQL Server access with the following command:

```
netsh advfirewall firewall add rule name="MSSQLSERVER" dir=in action=allow program="C:\Program
Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\Sqlservr.exe" enable=yes
```

These firewall settings must be activated on SQL server in order for MSDTC to work:

- Distributed Transaction Coordinator (RPC)
- Distributed Transaction Coordinator (RPC-EPMAP)
- Distributed Transaction Coordinator (TCP-In)

For information please see the Knowledge base article [KB001318 - K2 and Firewalls](#)

And this MSDN blog: <http://blogs.msdn.com/b/chrisforster/archive/2009/05/29/windows-2008-sql-server-cluster-with-msdtc-when-using-windows-firewall-with-advanced-security.aspx>



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.2.7 IIS 7 Configuration

IIS7 Configuration

K2 Workspace will be affected if IIS 7 is not configured correctly. Configure the IIS 7 application pool Managed Pipeline mode setting to **Classic** and ensure that

- Windows Authentication is **enabled**
- Anonymous authentication is **disabled**

To configure IIS7, the configuration takes place on the server machine where K2 Workspace is installed. If SharePoint is planned for the same physical machine, ensure that during the installation a new Web site is created for K2 Workspace. This will ensure port numbers between K2 Workspace and SharePoint do not conflict. Once K2 Workspace has been installed, two additional steps may be required to configure the K2 Workspace Web site and the runtime Web services.

Configure the Run Time Web Services



- 1 Open Internet Information Services (IIS) Manager
- 2 Locate the [Machine Name] > Sites > [K2 Workspace Site Name]
- 3 Click on Advanced Settings
- 4 From General > Application Pool, ensure that the Website has been assigned the correct application pool
- 5 If not, click in Application Pool and click on the ellipse
- 6 From the Select Application Pool Dialog, click on the Application Pool drop down and select the correct Application Pool
- 7 Click Ok to save the changes
- 8 Click Application Pools
- 9 Select the correct application pool from the list
- 10 Click the Advanced Settings link
- 11 Under the Advanced Settings > General section, locate the Managed Pipeline Mode entry
- 12 If the Managed Pipeline Mode is NOT set to Classic, click on the drop down as shown below and select classic as the mode
- 13 Click Ok



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3 Windows Server 2012 Configuration Requirements

Introduction

Microsoft has updated their product stack in their operating system, data storage and software development tools with the 2012 offerings. The focus of this document is to address the support that K2 offers with regards to these Microsoft product offerings and how to configure them to work with K2.

The Microsoft products that previous K2 blackpearl installations operate with were systems that utilize Windows Server 2008 as the base operating system, SQL 2008 for data storage, and Visual Studio 2008 as the process design tool. Currently Windows Server 2008 or 2012 is the base operating system with SQL Server 2008 SP1 or later for data storage and Visual Studio 2010 or later as one of the process design tools (the other tools being K2 studio, K2 Designer for SharePoint and K2 Forms).

Before you begin ensure that you have read this document in full before attempting your K2 installation on Windows Server 2012. Many of the configuration steps **MUST** be performed prior to installing K2 blackpearl.

If more information is required then refer to the following Microsoft site links for information on the respective products:

- For more information on Windows Server 2012, as well as on server roles and technologies, see the TechNet page: [Windows Server 2012](#)
- SQL Server 2012: <http://www.microsoft.com/sqlserver/en/us/default.aspx>
- Microsoft Visual Studio 2012: <http://www.microsoft.com/visualstudio/eng>

Windows Server 2012

Windows Server 2012 delivers valuable new functionality and powerful improvements to the core Windows Server operating system to help organizations of all sizes increase control, availability, and flexibility for their changing business needs. New Web tools, virtualization technologies, security enhancements, and management utilities help save time, reduce costs, and provide a solid foundation for your information technology (IT) infrastructure. The latest version of the Windows Server operating system offers businesses and hosting providers a scalable, dynamic, and multi tenant-aware infrastructure that is optimized for the cloud.

Windows Server 2012 supersedes Windows Server 2008 as the server-based operating system. Windows Server 2012 is strongly recommended for new machines and new system infrastructure. Windows Server 2012 also introduces IIS 8 to the production environments; IE 10 is also fully supported.

Before you install K2 blackpearl, there are several configuration steps that you need to complete:

- Set up DNS
- Set up Service Accounts
- Set up Permissions
- Set up NLB
- Set up MSMQ
- Set up DTC
- Set up IIS 7

Running K2HostServer in console mode

When running the K2HostServer in console mode on a Windows Server 2012 machine, the K2 Service Account user must be a local administrator on that machine AND the K2HostServer console application needs to be run using the "Run As Administrator" option.

1.5.3.3.1 Adding DNS Entries

Setting up DNS

It is important to have the DNS lookup zones configured before installing K2 blackpearl. During the configuration of the K2 components, connections will be made to the various server roles to ensure that the components can talk to each other appropriately. If the DNS settings are incorrect, your K2 environment will not function correctly.



DNS entries must be added by a domain administrator who has rights to add DNS host entries.

To set up the DNS, follow the below steps:



On the Domain Controller, open the **DNS Management Console** (Administrative Tools > DNS, or run dnsmgmt.msc, or find DNS in the Server Manager)



Expand the Forward Lookup Zones node, and add a **New Host (A or AAAA)** to your domain



In the **New Host** window, enter in the appropriate name and IP Address, make sure the Create associated pointer (PTR) record check box is checked, and click Add Host



If you are using a cluster, be sure to use the virtual IP address of the cluster.

Repeat the above steps for as many servers as you have in your K2 environment.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.2 Set up SPNs



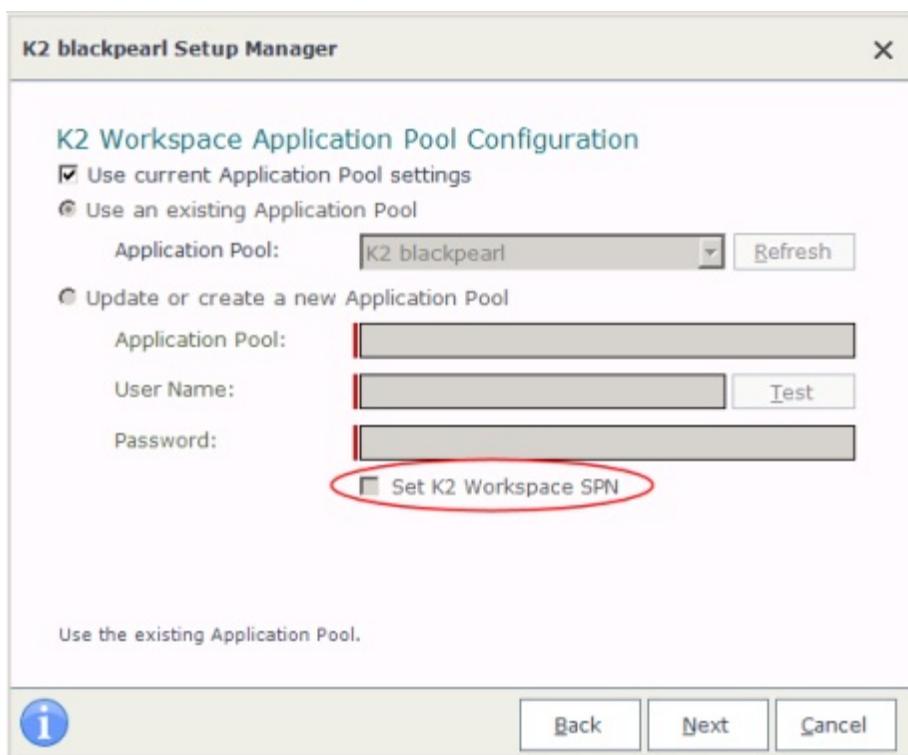
This section applies to preparing for installing distributed environments where Kerberos will be implemented. SetSPN.exe is a tool supplied along with the Windows Server operating system.

Set SPN



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

During the installation of K2 blackpearl, on a number of user page locations the Setup Manager will prompt the user to set an SPN. If this option is enabled the SPN for the Service instance will be created automatically during the installation process. Shown below is an example user page, where the user is prompted to enable "Set K2 Workspace SPN".



When the K2 Setup Manager has been enabled by the user to set SPNs, the setup manager proceeds to set SPNs regardless of whether they are already active. This may result in the creation of duplicate SPNs. The user can check if SPNs are already active by using the SetSPN.exe tool provided with Windows Server. If an SPN already exists for the service instance, there would be no need to enable the option to automatically set SPNs. The K2 Analysis tool can also be used to detect errors such as duplicate SPN's but this can only take place once K2 blackpearl is installed. By using the SetSPN tool before, duplicate SPNs can be detected beforehand. Example usage of the SetSPN commands:

Switch	Usage
- X	Search for duplicate SPNs
- X - F	Search tree wide for duplicate SPNs



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.2.1 K2 Service Account

K2 Service Account

In a distributed environment where components are installed on more than one server, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

There are two sets of SPNs that need to be set up for the K2 Service Account:

- K2Server
- K2HostServer

The following placeholders are used in the commands:

- **domain\K2 Service Account** - The K2 Service Account that runs the K2 Service
- **MachineName** - The name of the computer on which the K2 Service is running
- **MachineName.FQDN** - The fully qualified domain name of the computer on which the K2 Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly. The SPNs listed below are for K2 blackpearl.



If you have a K2 Server farm running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A K2Server/MachineName:5252 domain\K2 Service Account
- setspn -A K2Server/MachineName.FQDN:5252 domain\K2 Service Account
- setspn -A K2HostServer/MachineName:5555 domain\K2 Service Account
- setspn -A K2HostServer/MachineName.FQDN:5555 domain\K2 Service Account



If you are installing K2 blackpearl on an **NLB environment**, the MachineName will change to the the LBHostName

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\K2 Service Account



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.2.2 Reporting Services Service Account

Reporting Services Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order to access the K2 Reports from the K2 Workspace, you need to set the SPNs for the Reporting Services Service Account.

The following placeholders are used in the commands:

- domain\Reporting Services Service Account - The Reporting Services Service Account that runs the Reporting Services application pool
- MachineName - The name of the computer on which Reporting Services is running
- MachineName.FQDN - The fully qualified domain name of the computer on which Reporting Services is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you are using **Host Headers** to access your Reporting Services Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\Reporting Services Service Account
- setspn -A HTTP/MachineName.FQDN domain\Reporting Services Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\Reporting Services Service Account

Configure Delegation for Reporting Services Service Account

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.

- 1 Open **Active Directory Users and Computers** (Administrative Tools > Active Directory Users and Computers)
- 2 Find the domain\Reporting Services Service Account and view its properties
- 3 On the Delegation tab, select the **Trust this user for delegation to specified services only** option
- 4 Select the **Use Kerberos only** option, and click on **Add**
- 5 Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account



In the Available Services section, select the **K2HostServer** item.

Click **OK**. The "Trust this user for delegation to specified service only" and "Use Kerberos only" options should be selected.

Click **OK**

Configure Delegation for the K2 Service Account

In order to use the SQL Server Reporting Services Service Object to schedule Reporting Services reports and include SmartObject data, you will need to configure the K2 Service Account with delegation.



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.



Open **Active Directory Users and Computers** (Administrative Tools > Active Directory Users and Computers)

Find the domain\K2 Service Account and view its properties

On the Delegation tab, select the **Trust this user for delegation to specified services only** option

Select the **Use Kerberos only** option, and click on **Add**

Click on **Users or Computers** and select the domain\Reporting Services Service Account you created as the SQL Server Reporting Services Service Account

In the Available Services section, select the **HTTP** item listed

Click **OK** twice to exit the dialog windows



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.2.3 K2 Workspace Service Account

K2 Workspace Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order to access the K2 Workspace from another machine, you need to set the SPNs for the K2 Workspace Service Account.

The following placeholders are used in the commands:

- domain\K2 Workspace Service Account - The K2 Workspace Service Account that runs the K2 blackpearl application pool
- MachineName - The name of the computer on which the K2 Workspace is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the K2 Workspace is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have the K2 Workspace running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.

If you are using **Host Headers** to access your K2 Workspace, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\K2 Workspace Service Account
- setspn -A HTTP/MachineName.FQDN domain\K2 Workspace Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\K2 Workspace Service Account

Configure for Delegation

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.



Open **Active Directory Users and Computers** (Administrative Tools > Active Directory Users and Computers).



Find the domain\K2 Workspace Service Account and view its properties.



On the Delegation tab, select the **Trust this user for delegation to specified services only** option.



Select the **Use Kerberos only** option, and click on **Add**.

- 5 Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account.
- 6 In the Available Services section, select both the **K2HostServer** and **K2Server** items.
- 7 Click **OK**. "Trust this user for delegation to specified service only" and "Use Kerberos only" should be selected.
- 8 Click **OK**. This will allow the K2 Workspace Service Account to delegate to the K2 Server Service Account.
- Also, since the SQL Reporting Services reports will also be rendered in the K2 Workspace, the K2 Workspace Service Account should also be allowed to delegate to the SQLRS Account.
- 9 Click **Add** again.
- 10 Click on **Users or Computers** and select the domain\Reporting Services Service Account you created as the SQL Reporting Services Service Account.
- 11 In the Available Services section, select the HTTP item.
- 12 Click **OK**. "Trust this user for delegation to specified service only" and "Use Kerberos only" should be selected.
- 13 If you are using SharePoint Integrated process, K2 Workspace Service Account should also be allowed to delegate to the MOSS Account.
- 14 Click **Add** again.
- 15 Click on **Users or Computers** and select the domain\MOSS Account you created as the MOSS Server Account.
- 16 In the Available Services section, select the HTTP item listed.
- 17 Click **OK**.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.2.4 SharePoint Service Account

SharePoint Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order for the K2 Worklist Web Part and K2 Designer for SharePoint to function properly from another machine, you need to set the SPNs for the SharePoint Service Account.

The following placeholders are used in the commands:

- domain\SharePoint Service Account - The SharePoint Service Account that runs the SharePoint application pool
- MachineName - The name of the computer on which SharePoint Service is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the SharePoint Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have SharePoint running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.



If you are using **Host Headers** to access your SharePoint Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\SharePoint Service Account
- setspn -A HTTP/MachineName.FQDN domain\SharePoint Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\SharePoint Service Account

Configure for Delegation

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.

- 1 Open **Active Directory Users and Computers** (Administrative Tools > Active Directory Users and Computers).
- 2 Find the domain\SharePoint Service Account and view its properties.
- 3 On the Delegation tab, select the **Trust this user for delegation to specified services only** option.
- 4 Select the **Use Kerberos only** option, and click on **Add**.



Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account.

In the Available Services section, select both the **K2HostServer** and **K2Server** items.

Click **OK**. The "Trust this user for delegation to specified service only" and "Use Kerberos only" options should be selected.

Click **Add** again.

Click on **Users or Computers** and select the domain\K2 Workspace Account you created as the K2 RuntimeServices Account.

In the Available Services section, select the HTTP item listed.

Click **OK**. This will allow the SharePoint Service Account to delegate to the K2 Workspace Account.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.2.5 SQL Server Service Account

SQL Server Service Account

In a distributed environment where components are installed on more than one server, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

When the SQL service does not run under a local system account, the following SPNs apply for the SQL Server Service Account:

- MSSQLSvc

The following placeholders are used in the commands:

- domain\SQL Server Account - The Account that runs the SQL Server Service
- MachineName - The name of the computer on which the SQL Server is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the SQL Server is running
- port - The port that SQL Server is running under



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly. The SPNs listed below are for K2 blackpearl.



If you have a K2 Server SQL farm running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A MSSQLSvc/MachineName:port domain\SQL Server Account
- setspn -A MSSQLSvc/MachineName.FQDN:port domain\SQL Server Account



If you are installing K2 blackpearl on an **NLB environment**, the MachineName will change to the the LBHostServerName

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\SQL Server Account

You can also test the configuration by executing the following SQL Script on your SQL Server:

- select c.session_id, c.net_transport, c.auth_scheme, s.login_name from sys.dm_exec_connections c join sys.dm_exec_sessions s on c.session_id = s.session_id where s.login_name = '[domain]\[accountname]'

Where '[domain]\[accountname]' is the domain and username for the K2 service account. If Kerberos is being used, then it will display "KERBEROS".



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.3 Set up Permissions

Permissions and Authentication for Windows Server 2012

In addition to the Service Accounts already discussed, LDAP over SSL (LDAPS) will need to be configured for some environments in order to use the Active Directory Event Wizard. See [Using the AD wizard on Windows](#) and the [LDAP requirement](#) in the troubleshooting section.

Other permissions that need to be set up as part of the installation process:

Server Role	Permission
K2 Server	The K2 Service Account will need permission to Log on as a Service.
Reporting Services Server	In order to access the temporary directory during runtime, some permissions are required for all authenticated users.
IIS Server	In order to access the temporary directory during runtime, some permissions are required for all authenticated users.
SharePoint Server	In order for K2 workflow processes to be able to be deployed, some permissions are required on the SharePoint directory.

1.5.3.3.4 Set up NLB

Setting up NLB

It is important to set up the Network Load Balancing (NLB) clusters before installing K2 blackpearl. It is also important to test that the cluster is performing correctly prior to installing K2 blackpearl. An incorrectly configured cluster can cause issues when using K2 blackpearl, and it adds a layer of complexity to troubleshooting.

The Network Load Balancing supported by K2 is:

- Windows Network Load Balancing Manager

The following sections will describe how to configure the two supported types as recommended by K2.

Windows Network Load Balancing Manager



Configuring Network Load Balancing is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

The 64-bit version of Network Load Balancing Manager (nlbmgr.exe) must be used for 64-bit Windows operating systems. For more information and to get the 64-bit version of the Network Load Balancing Manager tool, please refer to the following Microsoft KB Article: <http://support.microsoft.com/kb/892782>

When configuring a cluster, follow the below steps:



1 Open **Network Load Balancing Manager (nlbmgr.exe)** (Administrative Tools > Network Load Balancing Manager, or Run > nlbmgr.exe)

If the feature has not been added to the Windows Server 2012, use the Add Roles and Features wizard on the Server Manager > Dashboard.



2 Add a **New Cluster** (right-click on Network Load Balancing Clusters and select New Cluster)



3 On the **Connect** screen, connect to the first host in the cluster and select the appropriate connection as the interface. If the server has multiple network adapters, many interfaces may be displayed. Be sure to select the appropriate network adapter from the list, and click next



4 On the **Host Parameters** screen, select the host priority, add the host IP address and subnet mask, select the initial host start then click next



5 On the **Cluster IP Addresses** screen, add in any additional IP addresses that the cluster can be accessed from, and click next



6 In the **Cluster Parameters** window, enter the appropriate IP address, subnet mask, full internet name, and cluster operation mode, and click next



7 On the **Port Rules** screen, edit the existing rule to use the appropriate affinity. See the notes below for recommendations based on the cluster type. Click next to continue



8 To add a second node to the cluster, right-click on the newly created cluster and select **Add Host to Cluster**



9 Connect to the second host, and make sure to select the appropriate interface



For a K2 Host Server cluster, use a Unicast operation mode and set the affinity to **None**. Since the K2 Host Server is a stateless machine, no affinity is necessary per session.



For a K2 Workspace Server cluster, use a Unicast operation mode and set the affinity to **Single**. You will want to ensure that the web pages retain an affinity to the web server during the session.



For a K2 for SharePoint Server cluster, use a Unicast operation mode and set the affinity to **Single**. You will want to ensure that the web pages retain an affinity to the web server during the session.

The same is true for all server clusters that host web based components (such as Process Portals, web services, web parts).



In some cases, the Network Load Balancing Manager console will time out before the second node is configured. If that happens, just right-click on the cluster and select Refresh. You should see all the nodes in a Converged state. Make sure that your cluster is configured correctly before starting the installation.

As mentioned in the Network Load Balancing Setup and Configuration topic, at least two network adaptors are required when the Unicast operation mode is selected.

Set up the NLB configuration to allow traffic through on the **K2 Workflow** (default of 5252) and **K2 Hostserver** (default of 5555) ports.

Hardware based load balancing

Follow the hardware manufacturer's guidelines for configuring a load balanced host. Use the above notes for specifics on a K2 Host Server Cluster or a K2 Workspace Server Cluster.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.5 MSMQ Settings

MSMQ

MSMQ (Microsoft Message Queuing) is a messaging protocol that enables applications running on independent, physical servers to communicate in a failsafe manner. The method used to enable MSMQ for a K2 installation is dependent on how AD (Active Directory) has been configured for the domain. MSMQ Directory Service Integration is required for K2 blackpearl installations.

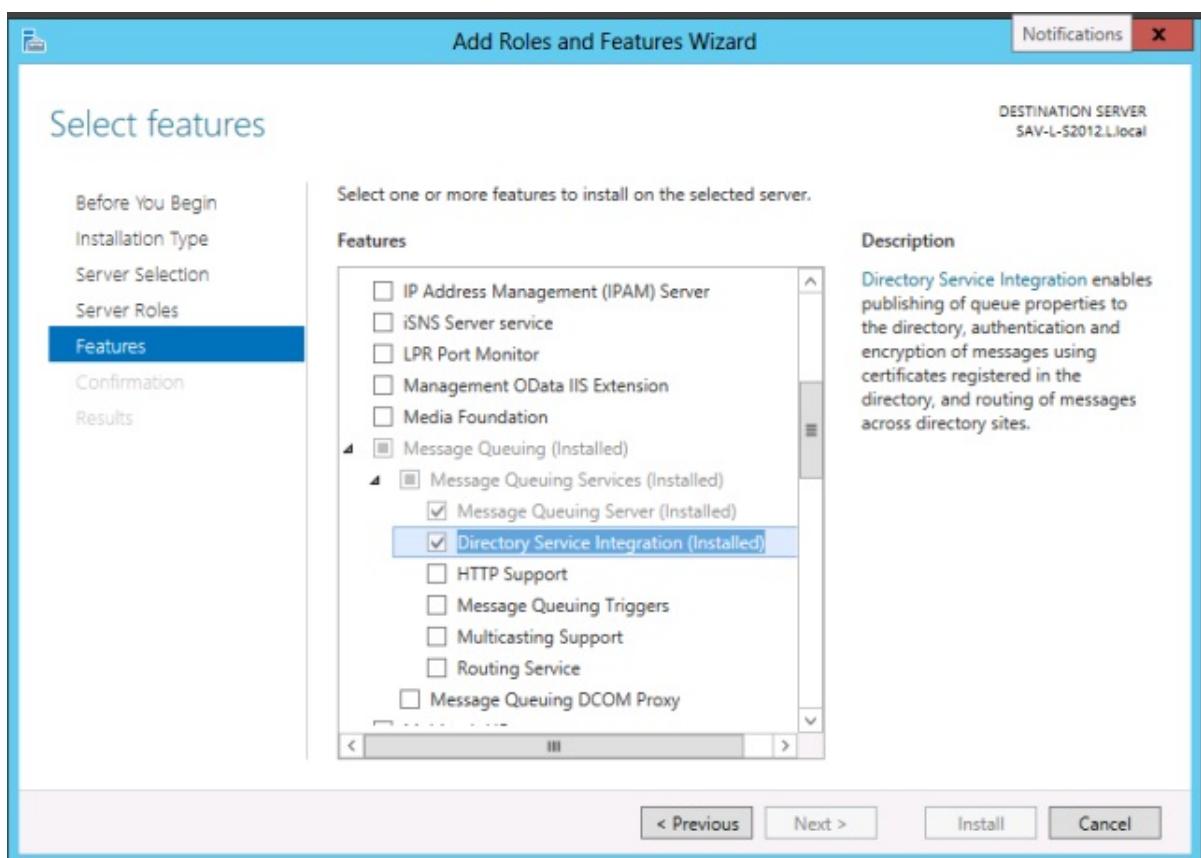
To install MSMQ in Windows Server 2008, follow the steps below:

- 1
- 2
- 3

Open the **Programs and Features** window (Control Panel > Programs and Features)

Click on the **Turn Windows features on or off** link

Select the Destination Server from the **Server Selection** link, then click on the **Add Features** link



- 4
- 5
- 6
- 7
- 8

Expand the **Message Queuing** node

Select **Message Queuing Services** and sub-nodes **Message Queuing Server** and **Directory Services Integration**

Choose the appropriate permissions settings response (please read the **Install Message Queuing** topic in the Windows Server 2012 Help and take note of the two different methods for configuring permissions depending on whether the Windows Server computer is a domain controller or not)

In Windows Server 2012, the permissions should be granted to the Root Object and not the Computer Object as in Windows Server 2008.

Click **Next**, then click **Install**

Once the installation has completed, click on **Close** and restart the server

Post Installation Checks

Perform the following post installation steps to verify that MSMQ is configured correctly:



- 1 Verify that the Workgroup registry key located under HKLM\Software\Microsoft\MSMQ\Parameters\ is set to 0
- 2 Restart MSMQ
- 3 Verify that MSMQ is running in Domain mode after this procedure
- 4 In Computer Management confirm that Message Queuing has a node called Public Queues and that the K2Server Service account has rights to this folder

For further information regarding MSMQ and Windows Server integration view [http://technet.microsoft.com/en-us/library/cc749102\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc749102(WS.10).aspx)

1.5.3.3.6 Enable and Configure DTC Components

The K2 Host Server makes use of Microsoft's Distributed Transaction Coordinator (DTC) to ensure data integrity between the K2 Server and the databases.



For the DTC to function correctly, the DTC Components need to be enabled and configured on all servers where K2 server components are installed, including the SQL Server, IIS Servers (including K2 Workspace, SharePoint, and Reporting Services Servers), and K2 Server.

Setting DTC to start automatically

The DTC is a service that coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

The DTC is provided as a standard service with the Windows Server operating system, but does not start up automatically as a service.

To configure the Service to startup automatically, do the following:

①

Open the **Services Manager** (Administrative Tools > Services)

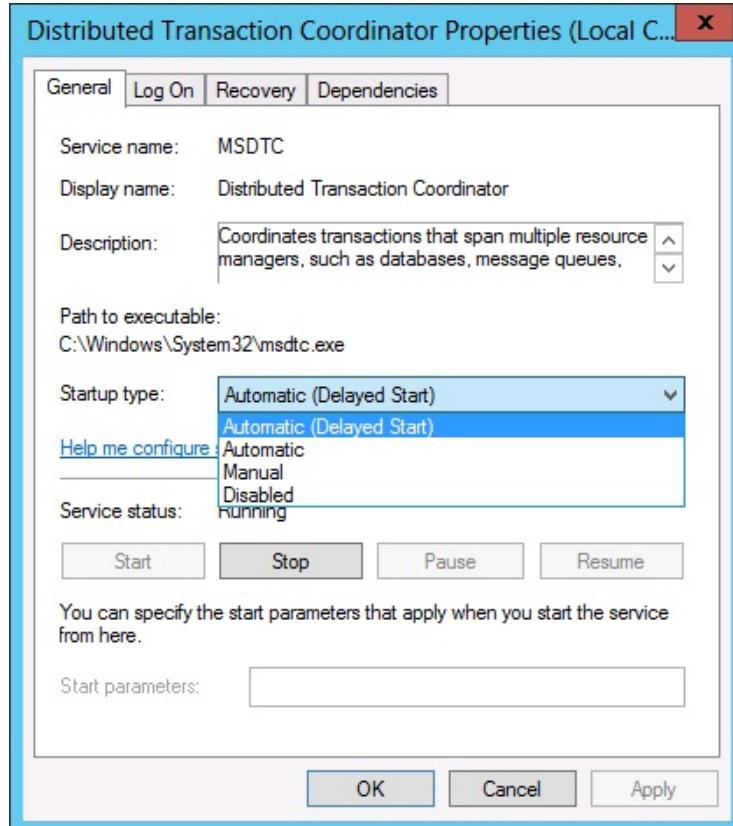
②

Locate the **Distributed Transaction Coordinator** Service in the list of services

③

To configure the service to start automatically, right click on the Distributed Transaction Coordinator Service and select **Properties**

In the dialog that appears, located the drop down menu for Startup type, and select the Automatic option, and click **OK**



④

If the service is not started, click on the start button. If the action is successful, the service's status is set to **Started**.

Configuring DTC

To configure DTC, follow the below steps:

①

Open Component Services (Administrative Tools > Component Services)

②

From the Console Node expand the following nodes Component Services > Computers > My Computer

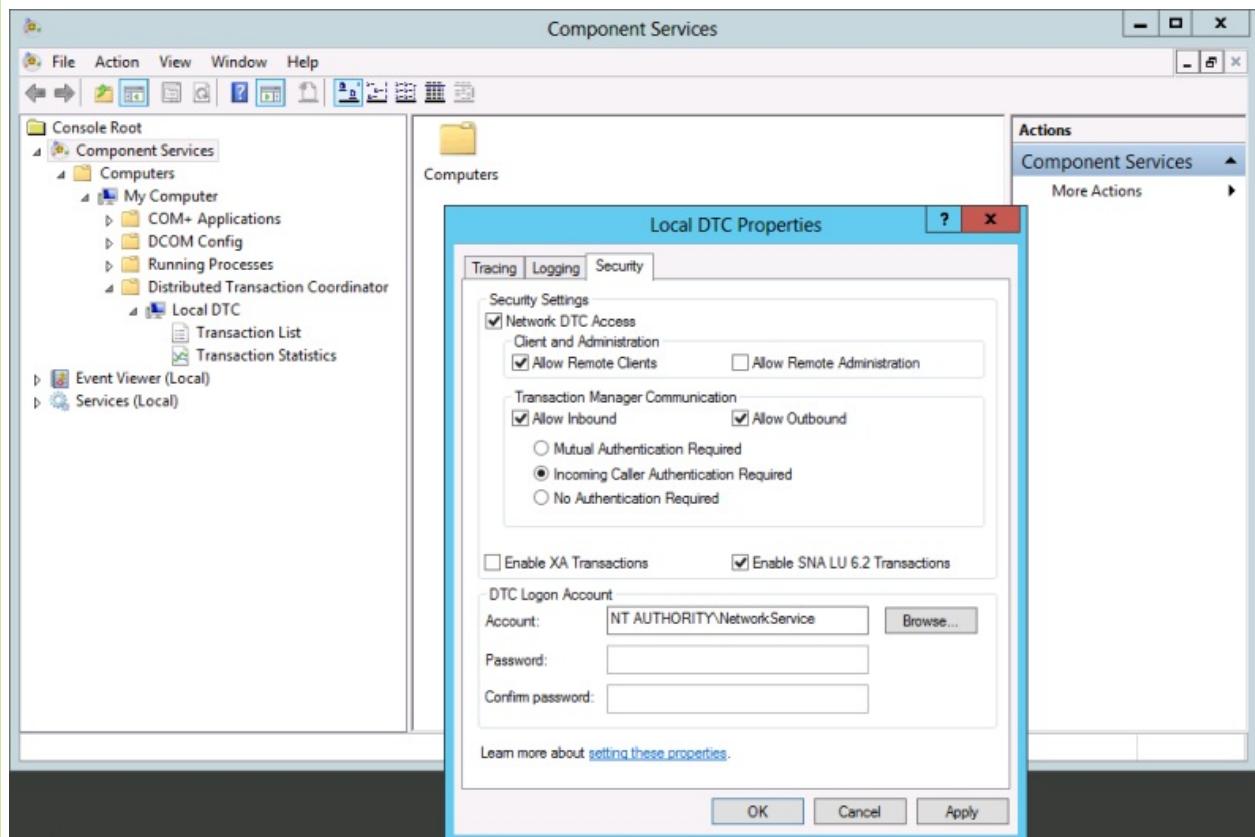
From the My Computer node, locate the new node Distributed Transaction Coordinator

Expand the node to view the Local DTC

Right Click on Local DTC and select properties

On the Local DTC Properties tab, click the **Security** tab, and configure the properties as follows:

- **Network DTC Access:** Checked
- **Allow Remote Clients:** Checked
- **Allow Inbound:** Checked
- **Allow Outbound:** Checked
- **Incoming Caller Authentication Required:** Selected



Click **OK**, and in the warning dialog that appears, click **Yes**

When the MS DTC service has been restarted, you can click **OK** on all the dialogs and close Component Management



This setting is for clustered installations. For non-clustered environments, you can leave the Mutual Authentication Required option selected, as it is the most secure option. The MSDTC transaction mode must be set to either **No Authentication Required** or **Incoming Caller Authentication Required** to function correctly on a Windows Server 2008-based failover cluster.

Taken from: [http://msdn.microsoft.com/en-us/library/dd897479\(v=BTS.10\).aspx](http://msdn.microsoft.com/en-us/library/dd897479(v=BTS.10).aspx)

*You must use the **Incoming Caller Authentication Required** transaction mode between Windows Server 2003-based computers in a clustered environment.*

*You must use the **No Authentication Required** transaction mode where one or more of the following conditions are true:*

- The network access is between computers that are running Microsoft Windows 2000.
- The network access is between two domains that do not have a mutual trust configured.
- The network access is between computers that are members of a workgroup.

Even for the Incoming Caller Authentication Required setting to work in the cluster environment you need to have the environment configured correctly for the Kerberos authentication. And again this might break if there is a Windows 2000 server coming into picture as it would only work if you have set No Authentication Required throughout on all the Windows 2003 server machines.

Based on the explanation above, we recommend having "No Authentication Required" setting on the cluster and the other standalone server interacting with the cluster to avoid running into any compatibility issues with older operating systems and authentication failures.

Taken from: <http://support.microsoft.com/?id=899191>

DTC Configuration when a Firewall is Active

The following configuration is performed using the **dcomcnfg.exe** application located in the **Windows\System32** folder.

Firewall Configuration

Configure firewall to allow MSDTC access with the following command:

```
netsh advfirewall firewall add rule name="MSDTC" dir=in action=allow program="%windir%\system32\msdtc.exe"
enable=yes
```

Configure firewall to allow SQL Server access with the following command:

```
netsh advfirewall firewall add rule name="MSSQLSERVER" dir=in action=allow program="C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Binn\Sqlservr.exe" enable=yes
```

These firewall settings must be activated on SQL server in order for MSDTC to work:

- Distributed Transaction Coordinator (RPC)
- Distributed Transaction Coordinator (RPC-EPMAP)
- Distributed Transaction Coordinator (TCP-In)

For information please see the Knowledge base article [KB001318 - K2 and Firewalls](#)

And this MSDN blog: <http://blogs.msdn.com/b/chrisforster/archive/2009/05/29/windows-2008-sql-server-cluster-with-msdtc-when-using-windows-firewall-with-advanced-security.aspx>



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.3.7 IIS 8 Configuration

IIS 8 Configuration

K2 Workspace will be affected if IIS 8 is not configured correctly. Configure the IIS 8 application pool Managed Pipeline mode setting to **Classic** and ensure that:

- Windows Authentication is **enabled**
- Anonymous authentication is **disabled**

To configure IIS 8, the configuration takes place on the server machine where K2 Workspace is installed. If SharePoint is planned for the same physical machine, ensure that during the installation a new Web site is created for K2 Workspace. This will ensure port numbers between K2 Workspace and SharePoint do not conflict. Once K2 Workspace has been installed, two additional steps may be required to configure the K2 Workspace Web site and the runtime Web services.

Configure the Run Time Web Services

- 1 Open Internet Information Services (IIS) Manager
- 2 Locate the [Machine Name] > Sites > [K2 Workspace Site Name]
- 3 Click on Advanced Settings on the Action panel under Manage Website
- 4 From General > Application Pool, ensure that the Website has been assigned the correct application pool
- 5 If not, click in Application Pool and click on the ellipse
- 6 From the Select Application Pool Dialog, click on the Application Pool drop down and select the correct Application Pool
- 7 Click Ok to save the changes
- 8 Click Application Pools under the Connections panel
- 9 Select the correct application pool from the list
- 10 Click the Advanced Settings link on the Actions panel under Edit Application Pool
- 11 Under the Advanced Settings > General section, locate the Managed Pipeline Mode entry
- 12 If the Managed Pipeline Mode is NOT set to Classic, click on the drop down as shown below and select classic as the mode
- 13 Click Ok



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.4 SQL Server 2008 SP1

1.5.3.4.1 K2 Workspace Permissions Requirements

K2 Workspace Permissions Requirements

The K2 Workspace Application pool Account (i.e. the Service Account) must be added in the Content Manager role on the machine where the SSRS Server has been installed and configured.

In K2 blackpearl 4.5 the K2 Workspace Report Designer does not use the SSRS server.

SSRS integration is still supported for customers:

- Who wish to use the SSRS server to expose reports in other contexts other than K2 Workspace or K2 Process Portals
- Who wish to use other design tools and then import reports into K2 Workspace Report Designer

1.5.3.4.2 Database Renaming During Installation

Database Renaming During Installation



The following applies for when the “default” names of the K2 Databases are renamed

When installing the K2 databases and at the same time implementing a database name change, intermittent authentication issues may arise during the installation. To avoid receiving the error messages, the following configuration steps are required:

- 1 From the SQL Server Configuration Manager
- 2 Expand the SQL Server Network Configuration
- 3 Select the node Protocols for MSSQLSERVER, a list of protocol names and their current status will be displayed in the right hand pane
- 4 Enable Named Pipes
- 5 Restart the SQL Server, and once the SQL Server restarts and is up and running the authentication issues should be resolved



The Named Pipes status is set to Disabled by default, and must be enabled manually



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.4.3 SQL Reporting Services

SQL Reporting Services

In K2 blackpearl 4.5 the K2 Workspace Report Designer does not use the SSRS server.

SSRS integration is still supported for customers:

- Who wish to use the SSRS server to expose reports in other contexts other than K2 Workspace or K2 Process Portals
- Who wish to use other design tools and then import reports into K2 Workspace Report Designer

K2 blackpearl leverages the services available in SQL Server 2008, which provides the following features:

"Microsoft SQL Server 2008 Reporting Services (SSRS) provides a full range of ready-to-use tools and services to help you create, deploy, and manage reports for your organization, as well as programming features that enable you to extend and customize your reporting functionality." (<http://msdn.microsoft.com/en-us/library/ms159106.aspx>)

For further details on deployment options: <http://msdn.microsoft.com/en-us/library/bb522791.aspx>

For further details on security: <http://msdn.microsoft.com/en-us/library/bb522728.aspx>

K2 for SQL Server 2008 Reporting Services

This component is now optional for all K2 blackpearl installations and can only be installed during a Custom K2 blackpearl installation, and will not install as part of the default installation configuration. K2 for SSRS (SQL Server Reporting Services) is selected from the components listing and is installed on the local machine.

When a user wants to direct the local machine to the SSRS server, this is done from the K2 Workspace Management Console.

Additional Configuration.

- A Reporting Service binding of 'All assigned' is recommended when installing K2.
- In order for users to browse the reports on the server, the following permissions must be configured:
 - Server Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role System User
 - Home Folder Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role Browser
- In SQL Server 2008, SSRS uses Http.sys to host the Reporting virtual directories. Read the following article for a brief explanation of this: <http://blogs.devhorizon.com/reza/?p=748>



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5 User Authentication and Security

1.5.3.5.1 Introduction to User Managers

Introduction to User Managers

Use this topic to familiarize yourself with user authentication, authorization and labels in K2.

Definitions

The following key terms are used throughout this section.

User Manager: All configurations necessary to associate K2 with an identity store, such as the security provider, security label, authentication provider and role provider.

Security Label: Also called K2 Label, User Label and simply Label, it is the token string that is pre-pended to the user's identity, for example the 'K2' label is used for Active Directory users by default, which appear in the K2 context as K2:[Domain\Username]. The context for the label does not extend beyond the K2 platform. The Security Label identifies specific instances of Authentication Providers and/or Role Providers.

Security Provider: The implementation of an authentication mechanism represented by a set of interfaces for interacting with an identity store and authenticating users located in that store.

Authentication Provider: The mechanism to confirm the identity of a user when they login or interact with services and data sources. User authentication is performed by passing a set of user credentials. Authentication can be integrated or require the use of a prompt or a web-based form.

Role Provider: The mechanism by which users and groups are resolved in K2 from the identity store.

Fully Qualified Name (FQN): The FQN is the user or role value in [Security Label]:[User/Role Name] format used by K2 for authorization such as assigning tasks, interacting with tasks or assigning permissions.



K2 will prepend the security label for the default user manager when an authentication request occurs without a security label.

Available User Managers

Active Directory (Default): requires access to Active Directory domain functional level Windows 2003 or higher to provide authentication and roles. Active Directory (AD) must be installed and available at the time of installation to configure the AD user manager.

SQL: requires access to the SQL user manager database, K2SQLUM by default, to provide authentication and roles. SQL user manager can be configured as a non-default user manager or as the default user manager either during or post installation.

LDAP: requires access to a LDAP-compatible system with protocol version 3 or higher to provide authentication and roles. LDAP user manager can be configured as a non-default user manager.

Custom: requires access to the custom identity store to provide authentication and roles. Custom user manager can be configured as a non-default user manager or as the default user manager post installation.

User Managers				
	Active Directory	SQL	LDAP	Custom
Security Label – Default Value	K2	K2SQL	K2LDAP	{Custom}
Can be configured as default during installation?	Yes	Yes	No	No
Can be configured as default post installation?	No	Yes*	No	Yes*
Can be configured as non-default post installation?	No	Yes	Yes	Yes
Can be configured with multiple security labels?	No	Yes	Yes ⁺	Yes ⁺

* For more information, please refer to Changing the Default User Manager.
 +The LDAP User Manager implements two IHostableSecurityProviders .NET types -
 SourceCode.Security.Providers.LdapProvider.Forms.Ldap and
 SourceCode.Security.Providers.LdapProvider.Trusted.Ldap - each can only be configured for a single security label. Each Custom User Manager .NET type that implements IHostableSecurityProvider can only be configured for a single security label.

Installing K2

The following default user manager installation scenarios are available out of the box:

- Active Directory
- SQL

Additional user managers can be added post-installation:

- SQL
- LDAP
- Custom



The installation procedure requires that a User Manager is available during the course of the installation; prompts for user credentials form part of the process and must be validated before the installation can be completed.



Only one security label can be registered for each User Manager .NET type that implements `IHostableSecurityProvider`. See the User Managers table above for more information.

Refresh the User Manager Cache

Any change in the configuration of user managers will require an update of the existing user cache. Download and execute the SQL command against the K2HostServer database.



```
UPDATE [K2HostServer].[Identity].[Identity]
SET [ExpireOn] = GETDATE()
, [Resolved] = 0
, [ContainersResolved] = 0
, [ContainersExpireOn] = GETDATE()
, [MembersResolved] = 0
, [MembersExpireOn] = GETDATE()
```

GO

Additional Considerations

The K2 Event Bus utilizes MSMQ and Active Directory. Because of this the K2 Event Bus will be unable to function if SQL or a custom user manager is used in place of AD unless a custom Event Recorder is introduced as well. For more information, see [How to add a 3rd-party event recorder to the K2 blackpearl Server](#).

K2 configuration for non-AD users and SharePoint 2010 requires a claims based SharePoint web application. For more information see [Claims - based Authentication](#).

K2 configuration for non-AD users and SharePoint 2007 is not supported.

All Users

K2 does not support a concept of "All Users" for assigning tasks, interacting with tasks or assigning permissions. Built-in or configured groups for the appropriate K2 user manager, for example Domain Users for Active Directory, should be used instead.

The following "All Users" containers are not supported by K2.

Active Directory, SharePoint 2007 and SharePoint 2010 classic-mode

- NT Authority\Authenticated Users

SharePoint 2010 claims-mode

- All Authenticated Users
- All Users (*{WindowsProvider}*), aka NT AUTHORITY\Authenticated Users
- All Users (*{FormsProvider}*)
- All Users (*{TrustedProvider}*)

1.5.3.5.2 Service Accounts

Service Accounts

When using non - administrative accounts with K2 and asymmetric encryption is involved for example SSL (Certificate Based Encryption), permissions need to be set on the private key.

The following resource is available to view the steps required for configuration purposes.

<http://blogs.technet.com/askds/archive/2008/04/28/askds.aspx>



When assigning permissions ensure that ONLY "Read" permissions are assigned to the Service accounts.

1.5.3.5.3 Kerberos for Windows Server 2008

Kerberos for Windows Server 2008

A number of resources have been made available to setup and configure Kerberos on a K2 blackpearl environment. With the introduction of Windows Server 2008, some enhancements are available with regards to Kerberos system dependencies.



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

1.5.3.5.3.1 SQL Server Reporting Services

SSRS : SQL Server Reporting Services

SSRS 2008 is no longer resource dependant on IIS. When a dependency on IIS was the case, SSRS had to be installed on a machine that had an instance of IIS active and available. SSRS for 2008 now uses HTTP.SYS for its URL reservations.

Resource Description	Link
For further information on this topic specific to this Microsoft product's architecture and operation, see the following link	http://msdn.microsoft.com/en-us/library/bb630409.aspx
Setup SSRS with Kerberos for a Domain User	Setting up SSRS with a Domain user as an application pool account

In K2 blackpearl 4.5 the K2 Workspace Report Designer does not use the SSRS server.

SSRS integration is still supported for customers:

- Who wish to use the SSRS server to expose reports in other contexts other than K2 Workspace or K2 Process Portals
- Who wish to use other design tools and then import reports into K2 Workspace Report Designer

1.5.3.5.3.2 Setting up SSRS with a Domain user as an application pool account

Setting up SSRS with a Domain user as an application pool account



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Perform the steps below to configure SSRS for a Domain user application pool account:

1

Create a HTTP SPN for the NetBIOS and FQDN under the Application pool account name (Use either SetSPN or ADSI Edit)

2

Secondly update the following node in the C:\Program Files\Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting Services\ReportServer\rsreportserver.config:



Copy Existing Code

```
<AuthenticationTypes>
    <RSWindowsNegotiate />
</AuthenticationTypes>
```

The changes to the code are below:



Copy Changes Required

```
<AuthenticationTypes>
    <RSWindowsNegotiate />
    <RSWindowsKerberos />
    <RSWindowsNTLM />
</AuthenticationTypes>
```

3

Verify that the following have been set in the following location:

C:\Program Files\Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting Services\ReportServer\web.config



Copy Changes Required

```
<configuration>
    <system.web>
        <authentication mode="Windows" />
        <identity impersonate="true" />
```

Additional Resources

For additional information see the following resource: [How to: Configure Windows Authentication in Reporting Services](#)



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.3.3 Setup Kerberos delegation for IIS 7.0

Setup Kerberos delegation for IIS 7.0



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

When using Kerberos delegation with websites hosted in IIS 7.0 there are a few things to consider:

1. Using machine name and port OR using CNAME host headers as URL vs. using Host or A type DNS records for host headers
2. Using Kernel mode authentication or not (<http://blogs.msdn.com/sudeepg/archive/2009/02/08/iis-7-kernel-mode-authentication.aspx>)

Kernel mode authentication

Kernel mode allows multiple sub level applications for one IIS site under different application pool identities without having duplicate SPNs

Benefits

Kernel Mode Authentication allows authentication persistence when switching the request from one application pool to another application pool. It re-authenticates only once for the first time when the request is made to that application. For rest all requests Kernel mode authentication (KA) session is maintained, which is a huge performance gain!

Easier Kerberos delegation configuration

When using CNAME DNS records for sites you don't need to create any SPNs under the Application pool identity (the fully qualified domain name (FQDN) or host headers that you are using for the site resolves to the FQDN of the web server's NETBIOS name.) In IIS 7.0, they use the web server computer's active directory account (ComputerName\$) to decrypt the service ticket. In other words, by default, we no longer use the application pool identity to decrypt the service ticket.

Caveats:

It is not possible to use a CNAME DNS record when pointing to a farm as your load balancer cannot guarantee that it will forward the request always to the same host.

When using "Host" or "A" type DNS records (using a FQDN/host header that does not resolve to the web server's fully qualified NETBIOS name), an SPN must be added when using an FQDN/host header that does not resolve to the web server's fully qualified NETBIOS name OR if you are using application pool identity.

Create SPNs

This step is only necessary in the following circumstances:

1. Create a web farm
2. The Host Header used do not resolve to a specific Server's FQDN
3. If delegation is to be forced to run under the specific application pool identity (decryption of service tickets are performed by the application pool identity rather than the system account). Use SETSPN.exe tool or ADSI edit mmc to add SPNs



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.3.4 Activate Delegation for the Application Pool Account

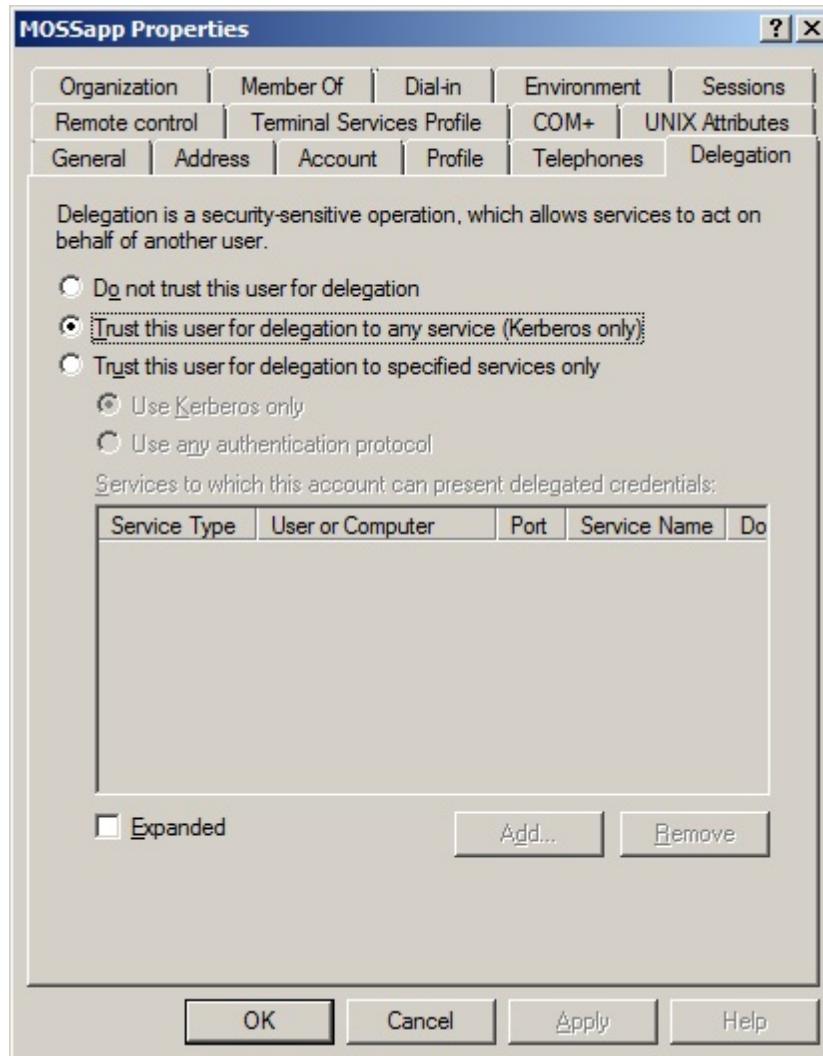
Activate Delegation for the K2 Workspace/Runtime Application Pool Account



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Activating delegation permissions in Active directory for the application pool account is only required under the following circumstances

- A web farm is currently being established / setup•
- The host headers used do not resolve to a specific server FQDN
- You want to force delegation to run under the specific application pool identity (decryption of service tickets are performed by the application pool identity rather than the system account)



[figure 1: Trust this delegation]



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.3.5 Activate delegation settings for IIS 7.0 web application

How to Activate delegation settings for IIS 7.0 web application



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.



Folder paths provided are the default paths used during installation. If they have been changed, then they must be amended accordingly

Two options are available when activating delegation for a web application. The difference between the two is the level of security that is provided. Option 1 is the most secure because delegation activation is specific to each individual application.

Option 1 - High Security

This option only activates Kerberos delegation for this specific application pool account. This method is more secure, but requires more administration to implement, especially if multiple application pool accounts are active that require Kerberos delegation.



Locate the applicationhost.config, configuration file in the following location :
C:\Windows\System32\inetsrv\config\applicationHost.config:



Open the configuration file using a text editor:



Copy Expected, current config file

```
<location path="[YOUR WEB APPLICATION]">
<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
enabled="true" userName="IUSR" />
        <basicAuthentication
enabled="false" />

        <clientCertificateMappingAuthentication
enabled="false" />
        <digestAuthentication
enabled="false" />

        <iisClientCertificateMappingAuthentication
enabled="false">

            </iisClientCertificateMappingAuthentication>
            <windowsAuthentication
enabled="false">
                <providers>
                    <add
value="Negotiate" />
                    <add value="NTLM" />
                </providers>
            </windowsAuthentication>
        </iisClientCertificateMappingAuthentication>
    </authentication>
</security>
</system.webServer>
</location>
```



change to the following:

--

**Copy**

Implemented changes...

```

<location path="[YOUR WEB APPLICATION]">
<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
enabled="false" userName="IUSR" />
        <basicAuthentication
enabled="false" />

        <clientCertificateMappingAuthentication
enabled="false" />
        <digestAuthentication
enabled="false" />

        <iisClientCertificateMappingAuthentication
enabled="false">

            </iisClientCertificateMappingAuthentication>
<windowsAuthentication enabled="true"
useKernelMode="true"
useAppPoolCredentials="true">
            <providers>
                <add
value="Negotiate" />
                <add value="NTLM" />
            </providers>
        </windowsAuthentication>
    </authentication>
</security>
</system.webServer>
</location>

```

Option 2 - Medium to Low Security

The second option sets authentication at the root for all IIS 7.0 applications, rather than at the application level. The cautionary point here is that setting this at root level will affect ALL sites that are under the designated application pool account.



Locate the applicationhost.config, configuration file in the following location :
C:\Windows\System32\inetsrv\config\applicationHost.config:



Open the configuration file using a text editor:

**Copy Expected, current config file**

```

<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
enabled="true" userName="IUSR" />
        <basicAuthentication
enabled="false" />

        <clientCertificateMappingAuthentication
enabled="false" />
        <digestAuthentication
enabled="false" />

        <iisClientCertificateMappingAuthentication
enabled="false">
    </authentication>
</security>
</system.webServer>

```

```

        enabled="false">

        </iisClientCertificateMappingAuthentication>
            <windowsAuthentication
        enabled="false">
                <providers>
                    <add value="Negotiate"
    />
                    <add value="NTLM" />
                </providers>
            </windowsAuthentication>

```

Make the following changes:

 Copy

```

<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
    enabled="false" userName="IUSR" />
        <basicAuthentication
    enabled="false" />

        <clientCertificateMappingAuthentication
    enabled="false" />
        <digestAuthentication
    enabled="false" />

        <iisClientCertificateMappingAuthentication
    enabled="false">

        </iisClientCertificateMappingAuthentication>
<windowsAuthentication enabled="true"
useKernelMode="true"
useAppPoolCredentials="true">
    <providers>
        <add value="Negotiate"
    />
        <add value="NTLM" />
    </providers>
</windowsAuthentication>

```



If you are not using kernel mode, then you will just need to enable windows authentication.

Option 3: Utilizing the AdminPack for IIS7.0 enables the user to configure system settings from a user interface, rather than editing configuration files manually.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.3.5.1 Option 3: Utilizing the AdminPack for IIS7.0

Option 3: Utilizing the AdminPack for IIS7.0



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Administration Pack for IIS 7.0 is a collection of tools and UI Extensions to help you administer your IIS 7.0 server

This collection of tools and UI Extensions assist the WEB Administrator in the follow areas

- Request Filtering UI - This UI exposes the configuration of the IIS runtime feature called Request Filtering. Configuration
- Editor UI - This UI provides an advanced generic configuration editor entirely driven by our configuration schema. It includes things like Script Generation, Search functionality, advanced information such as locking and much more Database
- Manager UI - This UI allows you to manage SQL Server databases from within IIS Manager, including the ability to create tables, execute queries, add indexes, primary keys, query data, insert rows, delete rows, and much more.
- IIS Reports UI - This extensible platform exposes a set of reports including some log parser based reports, displaying things like Top URL's, Hits per User, Page Performance, and many more.
- FastCGI UI - This UI exposes the configuration for the FastCGI runtime feature. ASP.NET Authorization UI - This UI allows you to configure the ASP.NET authorization settings.
- ASP.NET Custom Errors UI - This UI allows you to configure the Custom errors functionality of ASP.NET

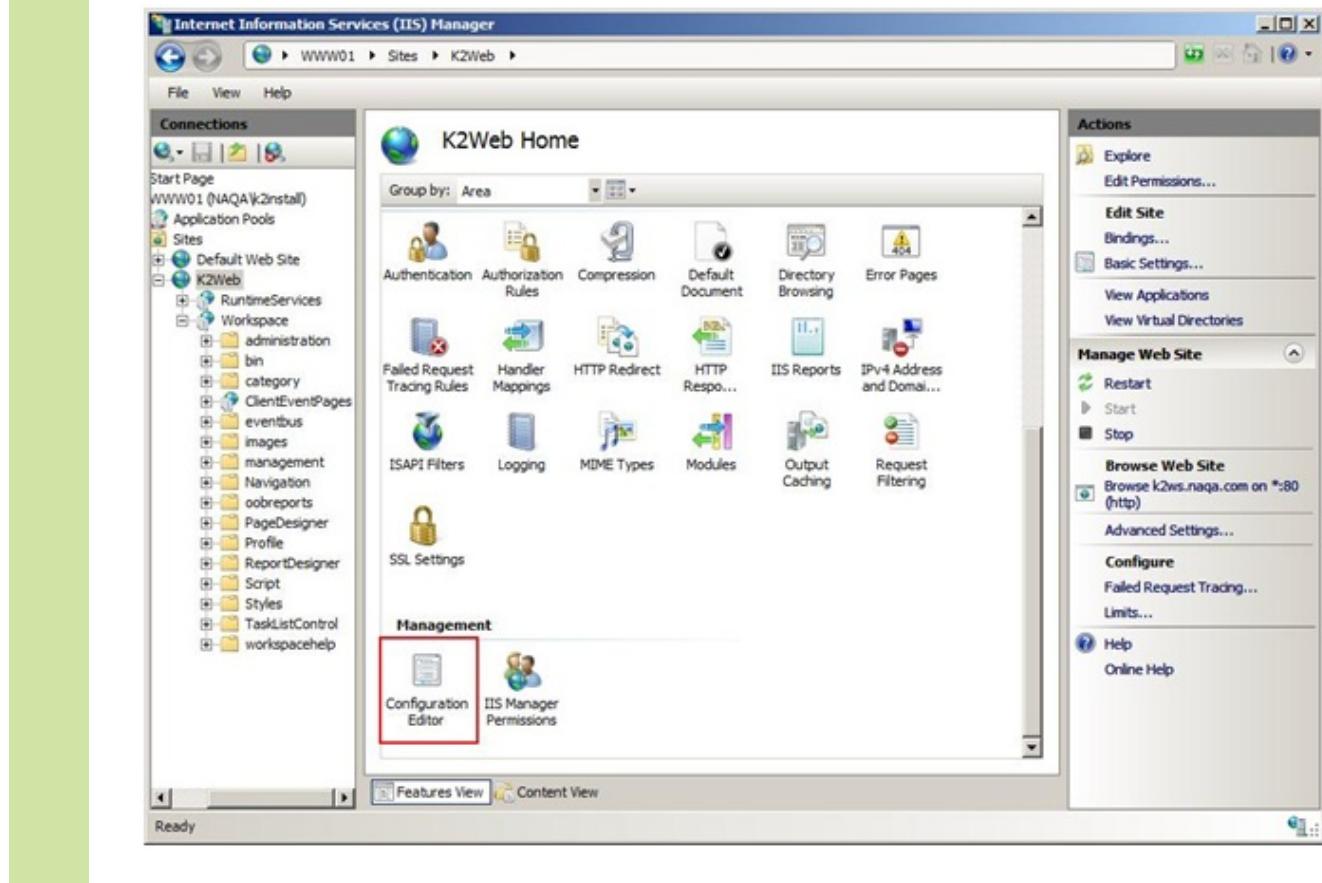
The IIS Manager can be obtained from the following location: [Administration Pack for IIS 7.0 \(x86\)](#)

Option 3 - Using the Administration Pack for IIS 7.0

For Option 3, the Administrator will use the Configuration Editor.

Once the Administration Pack has been installed, do the following:

- 1 Open IIS Manager
- 2 From the Connections Browser, locate the **Sites** node
- 3 Expand the node and locate the [K2 Site]

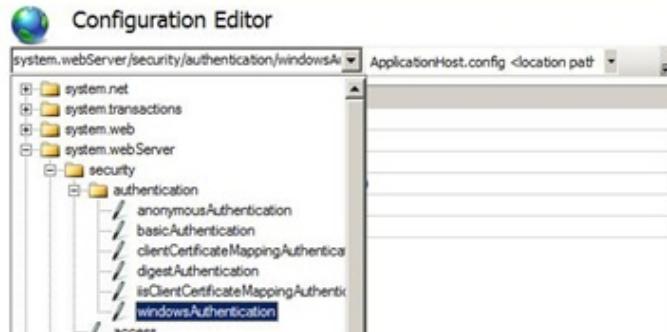


(4)

Under Management click the **Configuration Editor**

(5)

Locate the following node system.web.Server > Security > authentication > windowsAuthentication



(6)

from the ...windowsAuthentication/providers

Collection Editor - system.webServer/security/authentication/windowsAuthentication/providers/	
Items:	
value	Entry Path
NTLM	MACHINE/WEBROOT/APPHOST
Negotiate	MACHINE/WEBROOT/APPHOST

(7)

Click on Providers, to view the two values



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.3.6 Farm configuration for Kerberos delegation

Farm configuration for Kerberos delegation



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

This topic deals with Farm configuration for Kerberos delegation and also applies to "Host" or "A" type DNS records.



Create a "Host" or "A" type DNS records



Add SPNs to the Application pool identity or Service account (depending on if this is a web application or NT service)

Activate delegation on the service account/ application pool identity. (this is done through Active directory users and groups)



For Web servers only : force Kernel mode and Application pool identity use for delegation on the site.



(see section "IIS 7.0 – activate settings for the application pool" below for more detail)



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.4 Kerberos Delegation For SharePoint

1.5.3.5.4.1 Site authentication to Kerberos for SharePoint site

Site Authentication to Kerberos for SharePoint site



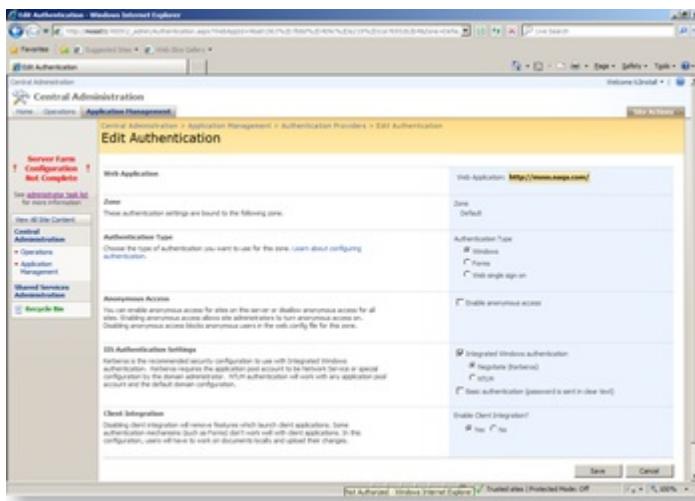
Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.



SPNs should be created for SharePoint web application pool identity Application pool account. Use either SETSPN.exe command line utility or ADSI edit MMC

Edit Authentication Settings for Web Applications

This can be performed via SharePoint Central Administration web application, as shown in the image below.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.4.2 Activate Delegation Settings for SharePoint Account

How to Activate delegation settings for IIS 7.0 SharePoint Web Application



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.



Folder paths provided are the default paths used during installation. If they have been changed, then they must be amended accordingly

Two options are available when activating delegation for a web application. The difference between the two is the level of security that is provided. Option 1 is the most secure because delegation activation is specific to each individual application.

Option 1 - High Security

This option only activates Kerberos delegation for this specific application pool account. This method is more secure, but requires more administration to implement, especially if multiple application pool accounts are active that require Kerberos delegation.



Locate the applicationhost.config, configuration file in the following location :
C:\Windows\System32\inetsrv\config\applicationHost.config:



Open the configuration file using a text editor and make the following changes:



Copy Expected, current config file

```
<location path="[YOUR SHAREPOINT WEB APPLICATION]">
<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication enabled="true" userName="IUSR" />
        <basicAuthentication enabled="false" />

        <clientCertificateMappingAuthentication enabled="false" />
        <digestAuthentication enabled="false" />

        <iisClientCertificateMappingAuthentication enabled="false">

            </iisClientCertificateMappingAuthentication>
            <windowsAuthentication enabled="false">
                <providers>
                    <add
                        value="Negotiate" />
                    <add value="NTLM" />
                </providers>
            </windowsAuthentication>
        
```

change to the following...,

**Copy**

Implemented changes...

```

<location path="[YOUR SHAREPOINT WEB
APPLICATION]">
<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
enabled="false" userName="IUSR" />
        <basicAuthentication
enabled="false" />

        <clientCertificateMappingAuthentication
enabled="false" />
        <digestAuthentication
enabled="false" />

        <iisClientCertificateMappingAuthentication
enabled="false">

        </iisClientCertificateMappingAuthentication>
<windowsAuthentication enabled="true"
useKernelMode="true"
useAppPoolCredentials="true">
    <providers>
        <add
value="Negotiate" />
        <add value="NTLM" />
    </providers>
</windowsAuthentication>

```

Option 2 - Medium to Low Security

The second option sets authentication at the root for all IIS 7.0 applications, rather than at the application level. The cautionary point here is that setting this at root level will affect ALL sites that are under the designated application pool account.

1

Locate the applicationhost.config, configuration file in the following location :
C:\Windows\System32\inetsrv\config\applicationHost.config:

2

Open the configuration file using a text editor and make the following changes

**Copy Expected, current config file**

```

<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
enabled="true" userName="IUSR" />
        <basicAuthentication
enabled="false" />

        <clientCertificateMappingAuthentication
enabled="false" />
        <digestAuthentication
enabled="false" />

```

```

<iisClientCertificateMappingAuthentication
enabled="false">

</iisClientCertificateMappingAuthentication>
    <windowsAuthentication
enabled="false">
        <providers>
            <add value="Negotiate"
/>
            <add value="NTLM" />
        </providers>
    </windowsAuthentication>

```

Change to the following,

Copy

```

<system.webServer>
<security>
    <authentication>
        <anonymousAuthentication
enabled="false" userName="IUSR" />
        <basicAuthentication
enabled="false" />

        <clientCertificateMappingAuthentication
enabled="false" />
        <digestAuthentication
enabled="false" />

        <iisClientCertificateMappingAuthentication
enabled="false">

        </iisClientCertificateMappingAuthentication>
    <windowsAuthentication enabled="true"
useKernelMode="true"
useAppPoolCredentials="true">
        <providers>
            <add value="Negotiate"
/>
            <add value="NTLM" />
        </providers>
    </windowsAuthentication>

```



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.5.3.5.5 Troubleshooting and Resources

Troubleshooting Tools

The following tools will be helpful when preparing to configure Kerberos and for troubleshooting any possible errors.

Tool	Description
netstat -a -n -p tcp	Used to locate available TCP ports. From the command prompt, type the following command to return a list of TCP ports that are being used
ADSI Edit	Create your own query to look for instances of duplicate SPNs Note: SETSPN has a few new query options that will help you troubleshoot duplicate spns
Delegconfig	Delegation test web application. It can be downloaded here: http://www.iis.net/downloads/default.aspx?tabid=34&g=6&i=1434

Reference material



The references below direct the reader to online blogs or articles that may be of use.

SharePoint + Kerberos on Windows Server 2008 (IIS 7) : <http://sharepointspot.blogspot.com/2008/12/sharepoint-kerberos-on-windows-2008.html>

IIS 7 and Kernel mode authentication : <http://blogs.msdn.com/sudeepg/archive/2009/02/08/iis-7-kernel-mode-authentication.aspx>

Changes Between IIS 6.0 and IIS 7.0 Security :<http://learn.iis.net/page.aspx/110/changes-between-iis6-and-iis7-security/>

IIS 7.0: Configuring Authentication in IIS 7.0 :[http://technet.microsoft.com/en-us/library/cc733010\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc733010(WS.10).aspx)

1.5.3.5.6 Introduction

Introduction: K2 Pass-Through Authentication



Contextualized Assistance: K2 Pass-Through Authentication scenario

K2 Pass-Through Authentication is a K2 proprietary authentication methodology specifically for authenticating users whose credentials need to be passed between machines that interact with the K2 APIs. This authentication model can be used as an alternative to Kerberos, but is not in any way intended to be a replacement for Kerberos.

K2 Pass-Through Authentication enables the removal of Kerberos dependencies and still allow a user's credentials to be passed between machines in such a way that the user can be authenticated in a secure manner without compromising the integrity of the K2 Server Transactions and data.



Why use K2 Pass Through Authentication

K2 Pass-Through Authentication is intended as an out of the box means for K2 blackpearl installations to be able to authenticate user requests. The K2 Pass-Through Authentication is available as a native feature of K2 blackpearl and K2 blackpoint; support for this feature will install with the KB001290 update. K2 Pass-Through can be implemented by various organizations depending on their requirements or internal skills availability. The list below is some of the reasons why an organization would use K2 Pass-Through Authentication.

- Limited Internal Organization Skills
- No access to Active Directory to make the required changes
- Business requirements that don't warrant the need for a Kerberos implementation



K2 Pass-Through Authentication is not a Kerberos replacement, it is a Kerberos alternative which can be implemented for specific delegation requirements when an anonymous connection is made which results in Kerberos failure.

1.5.3.5.6.1 Installation and Configuration Settings

Installation

The local group policy for each K2 Server Machine must be updated as per the following topic: Local Security Policy

SharePoint Requirements

If the Client User's service call requires access to a specific database where K2 Pass Through Authentication would be used, then the following user must be added to the database NT AUTHORITY\ANONYMOUS LOGON .

Configuration Settings

The required updates to K2 blackpearl to support K2 Pass-Through Authentication will install with K2 blackpearl 1290 for all distributed installations. The updates are intended for distributed installations and this is assumed by the installer when the Custom Option is selected. If a simple full installation is chosen, K2 Pass Through is not needed so the User configuration page will not display.



The K2 Pass-Through Authentication installation screen is only visible when installing K2 Server in a distributed configuration.

Along with the UI based configuration that is made while installing the system, settings are also located within the K2HostServer.Config file using the DelegationContext node. The selection implemented using these settings will determine how the system responds and handles authentication errors.



Once these settings have been implemented they are global for the K2 components. especially when K2 Servers for example are load balanced. All nodes MUST have the same configuration to avoid inconsistent behavior.

The manner in which K2 Pass-Through Authentication works can be configured using the DelegationContext node in the AppSettings section of K2HostServer.Config. This setting is global for all server connections, regardless of the source. If a network load balancer (NLB) is in place, all K2 Server nodes should have the same setting to prevent inconsistent behavior.

ClientKerberos

Client Kerberos is the default setting and the system will assume such if no change is made. With this option set, the K2 Server will behave as per normal before K2 Pass-Through Authentication was introduced. This means that normal delegation will take place using NTLM and assume that Kerberos has been configured.

If Kerberos was not configured, the error message will be logged in the K2 Server Log. When a connection is made that requested K2 Pass-Through Authentication, and delegation failed an error message will be logged in the K2 Log Files to identify the problem. When Kerberos Delegation or NTLM authentication takes place, the assumption is that the system is working as expected and no error messages will be recorded since there is no need.

Client Kerberos is the recommended option for enabling maximum security which implies that the system administrator has decided not to use K2 Pass Through Authentication. This is the recommended option owing to the benefits of using Kerberos, however this does introduce the requirement for good planning and a higher degree of expertise to install. Resources are available from the K2 Customer portal to assist in configuring Kerberos, and it is strongly recommended that these be used.

ClientWindows

ClientWindows constrains K2 Pass-Through Authentication to only occur if the client credentials are of WindowsIdentity type i.e. a valid windows token. This implementation will prevent less secure User Clients such as Forms and Claims identities from passing credentials. If Kerberos (or NTLM) is working, it uses those credentials. This is the recommended option for environments containing only Windows users and who need to maximize functionality and security, and this does not require Kerberos to be configured.



Recommendation: When the K2 Server is run in console mode make sure to be logged in as the correct user and make use of the "Run as Administrator" option to ensure that the correct elevated privileges are utilized.

1.5.3.5.6.2 How K2 Pass-Through Works

How K2 Pass-Through Authentication works

For K2 Pass-Through Authentication to function as securely as possible follows a protocol which is used to ensure that regardless of the manner in which the K2 Client APIs are used each valid authentication attempt is successful.

1. A client which may be a thick or lite client e.g. K2 Workspace makes a normal connection to the relevant K2 client API.



This initial connection is secure even for custom applications as it's all conducted internally

2. The K2 client API will analyze the current configuration (e.g. user context and threads) to ascertain who is the intended end user of the application
3. The user token is interrogated to ensure that it is a properly authenticated Windows token (e.g. against Active Directory).

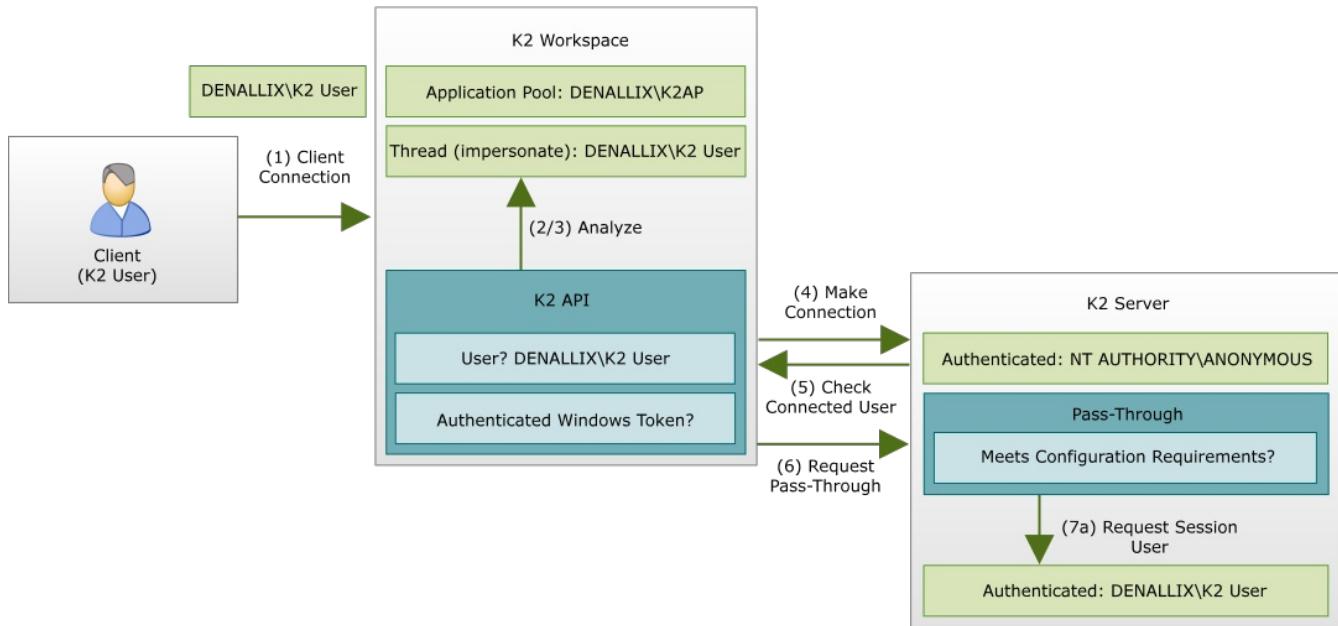


This process is to verify the ClientWindows configuration option

4. To initiate the process a connection is made to the K2 Server, just prior to K2 Pass-Through Authentication being performed
5. The relevant K2 client API will ask the K2 Server which client was authenticated, to determine if it's different to the user calculated in step (2)
6. If there is a difference, then the K2 Client API will request K2 Pass-Through Authentication, and then send the K2 Server the user's name, as well as passing in the result of (3)
7. From the K2 Server's side and depending on the requirements of the configuration option (e.g. ClientWindows):
 - a. If step (6) is successful, the K2 Server will switch its security context from the current user (e.g. the anonymous user) to the K2 Pass-Through Authentication user
 - b. If unsuccessful, an error will be logged due to the fact that there is a configuration issue on the client (by the fact that K2 Pass-Through Authentication failed). Any further functionality will continue as the user (e.g. anonymous) as connected in step (4), including any connections to back-end systems.



When configurable levels of trust are required for each server on an individual basis in a distributed environment, Kerberos should be considered as this feature is beyond the Scope of K2 Pass-Through Authentication.



1.5.3.5.6.3 Connecting to the K2 Server

Establishing a Connection with the K2 Server

A client connection can be made with the K2 Server from many different sources, these include both K2 and non K2 Clients. Some examples of client connection sources are:

- K2 Workspace
- ASP.NET Forms
- InfoPath
- SharePoint
- Custom thick or thin client

When the client connection is attempted, it may be a direct connection or the connection may have been delegated via another machine.

Kerberos Vs K2 Pass-Through

If Kerberos has not been configured, the possibility will always be present that the client credentials will be lost as they are delegated through the application layers especially when the number of physical machines in question increases. The primary reason for this is that the various application layers do not have valid credentials from Active Directory. The most obvious evidence of this is when an Anonymous User Error is generated when a client application on one machine has attempted a connection with an adjacent machine and the connection was refused.

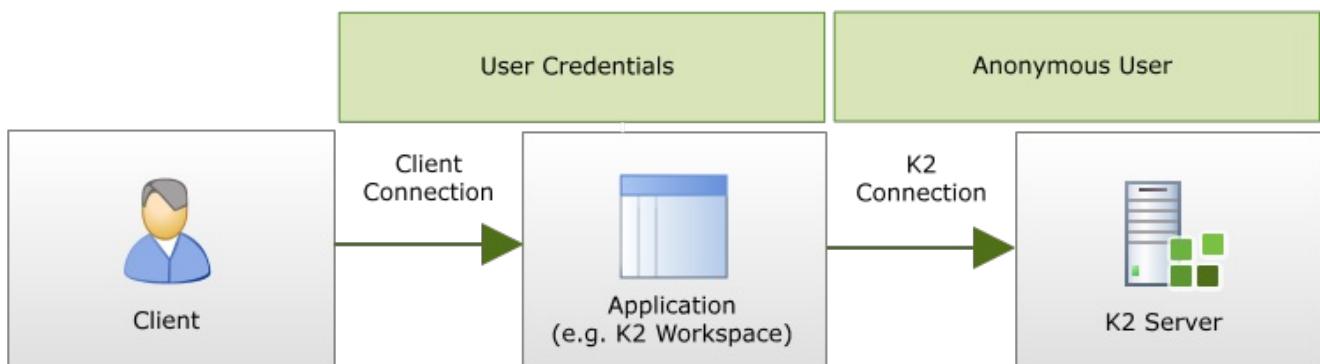
Since the credentials would normally only be lost on the second hop (ie second machine to machine delegation, K2 Pass-Through can be requested)

Connection Pass Through

As described above, the credentials would normally loose context on the second hop i.e. the IIS Server attempts to place a call to the K2 Server, but the logon comes through as anonymous and no valid windows token can be passed.

K2 Pass-Through is only available on the second hop and this is when the K2 Client APIs contact the K2 Server. When this takes place, there is one of two possible outcomes:

1. When the connection is made VIA the APIs, they gather valid information relevant to the user. If these credentials are the same as the user on the K2 Server, then the APIs will pass credentials in the same manner as Kerberos or NTLM enabling a logon to take place successfully.
2. If however, the information that has been gathered about the user is not the same and this could be owing to an Anonymous error or a Service of some kind this means that delegation has failed. For this scenario, the details of the original user are passed to the K2 Server and they are used instead.



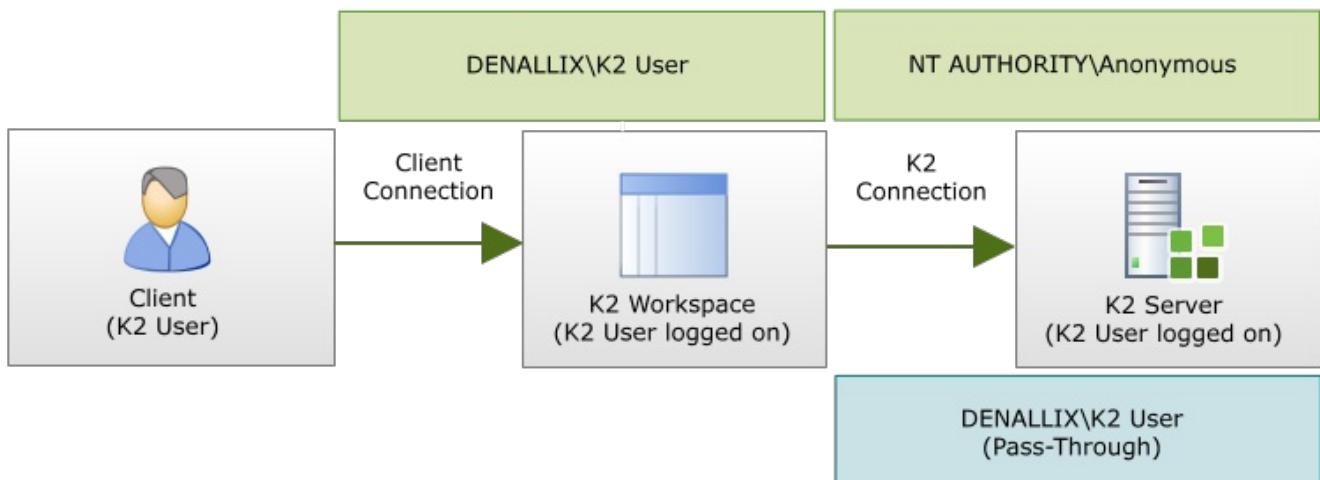
Double Hop

A hop, refers to when credentials are passed from one machine to the next. In most cases the first hop takes place between the Client and service or server of some kind.

In the diagram below this is a single hop, but this only applies to non-distributed installations where passing of credentials is not a problem. In the diagram below NTLM is used and this enabled the credentials to be authenticated

In the second diagram, the credentials are passed twice, from client to the IIS Server and then onto the K2 Server. This is a double hop, and is typical of a scenario where K2 Pass-Through Authentication is useful.

In the first step, NTLM is again used to authenticate between the client and the IIS Server. This could be the K2 Workspace Machine for example. However, when the IIS Server needs to place a request to the K2 Server, this now crosses the physical machine boundary, and the IIS Service does not have the authority to pass these credentials. This would typically result in an Authentication Anonymous error that Kerberos would negotiate. It is also the scenario for which K2 Pass-Through is useful.



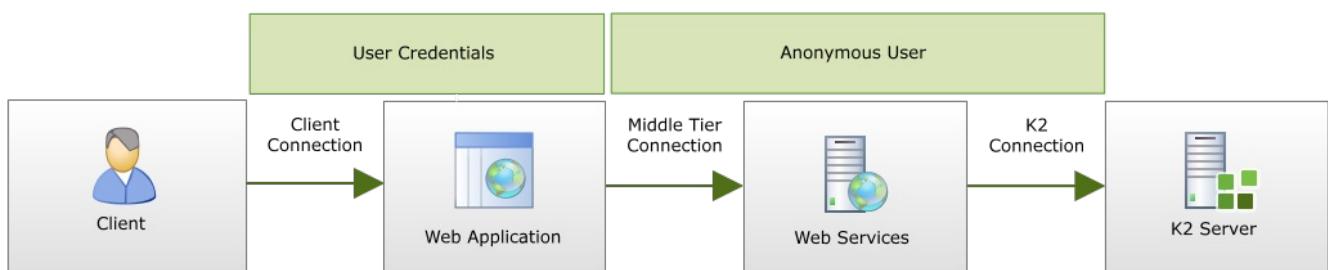
Trip Hop

Caution: A virtual machine is still considered as a physical machine since it introduces the logical machine boundary barrier. The triple hop limitation comes into effect when there are too many machines located either before or after the K2 Server in the sequence of credential passing. If the K2 Server is the third machine in line or web service, SQL Database is the third machine away from the K2 Server this will cause a delegation failure and credentials will not be passed. Also, this is now beyond the scope of K2 Pass-Through Authentication and the need now arises for Kerberos to be installed.

In the above scenario, the hop between the custom Web service and the K2 Server now means that the context of the User has been completely lost and in this instance K2 Pass-Through Authentication cannot be used. This is because the identity of the User and their credentials were lost long before they reached the K2 Server and the K2 Server cannot recover them in this scenario.

The situation below presents a similar situation, where the K2 Server is first in line but now too far away. Credentials can be passed to the Custom Web Service successfully using NTLM, however once the Custom Web Service needs to pass those same credentials onto a 3 part system, for example SQL Server a delegation error takes place.

K2 Pass-Through Authentication will only and always come into effect in relation to the K2 Server and K2 components. The 3 hop limitation is not a limitation of K2 Pass-Through Authentication, but is rather a extent to which K2 Pass-Through can be leveraged to ensure that credentials are passed from machine to machine. Once the 3 hop limitation has been reached, then the requirement is that Kerberos must be configured.



1.5.3.5.6.4 Credentials Delegation

Credentials Delegation

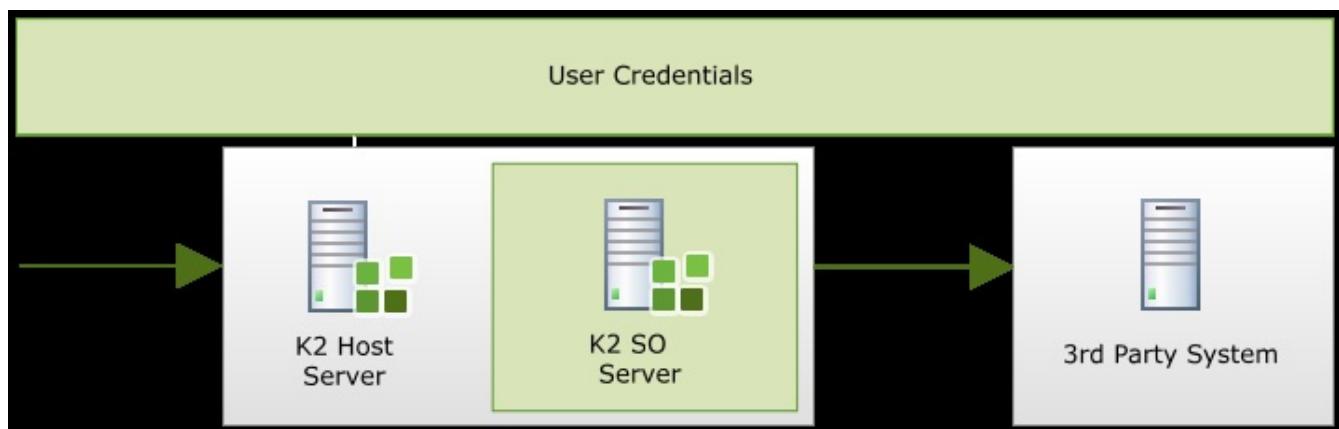
K2 Pass-Through Authentication offers a number of methods for delegating or storing securely a set of user credentials and then delegating them. These options enable K2 Pass-Through to be as intuitive as possible yet there may be additional setup and configuration required along with prerequisites and potential limitations.

The options that are available for Delegation are:

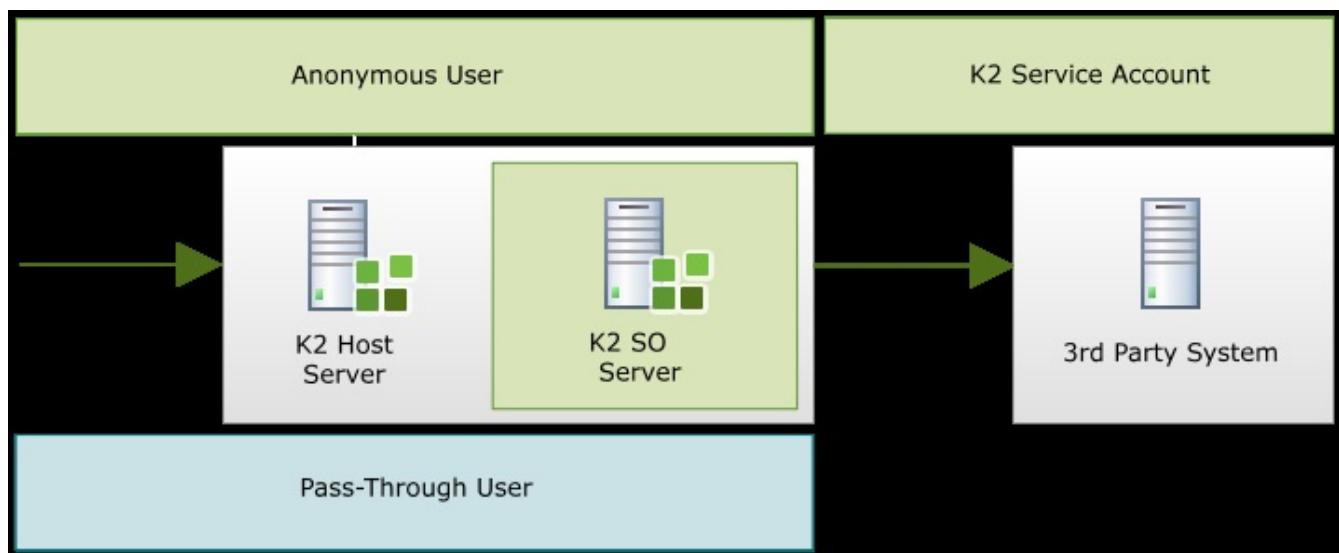
- Single Sign On
- Enforce Impersonation
- SharePoint Impersonation
- Dynamic SQL Service Impersonation

K2 Delegation Overview

The K2 Server which is a Hosted Service (including the K2 SmartObject Server) may at times be required to pass the Client's credentials to a 3rd party system. The K2 Workflow Server, which is one of the hosted services, does not independently perform delegation of the Client's credentials. Since the K2 Workflow Server is a hosted service it only calls 3rd party systems asynchronously (not in real time), such as within a workflow's Server Event. The physical limitation with this is that there will never be any client credentials to delegate by the hosted service.



When K2 Pass-Through Authentication is necessary for the connection from InfoPath to the K2 Host Server, only the K2 Server has the K2 Pass-Through Authentication user. This identity is only recognized by the K2 Server and not any 3rd party system. This prevents the K2 Server from passing any credentials to SharePoint for example, and the K2 Service Account is used as if there is no pass-through because this is a delegation scenario. If Kerberos were configured, the Client's credentials would be passed through the chain all the way to SharePoint (InfoPath to K2 Host Server to K2 SmartObject Server to SharePoint).



1.5.3.5.6.4.1 Single Sign On

Single Sign On



The Active Directory credentials that are cached are stored securely in the K2 Databases using an encrypted password



Single Sign on is a feature that has been primarily used in conjunction with 3rd party systems where a secondary set of credentials were cached against a security label and this would create a single sign in identity. This feature was originally made available so that K2 blackpearl was capable of authenticating a client user for systems for example K2 Connect for SAP and SalesForce.

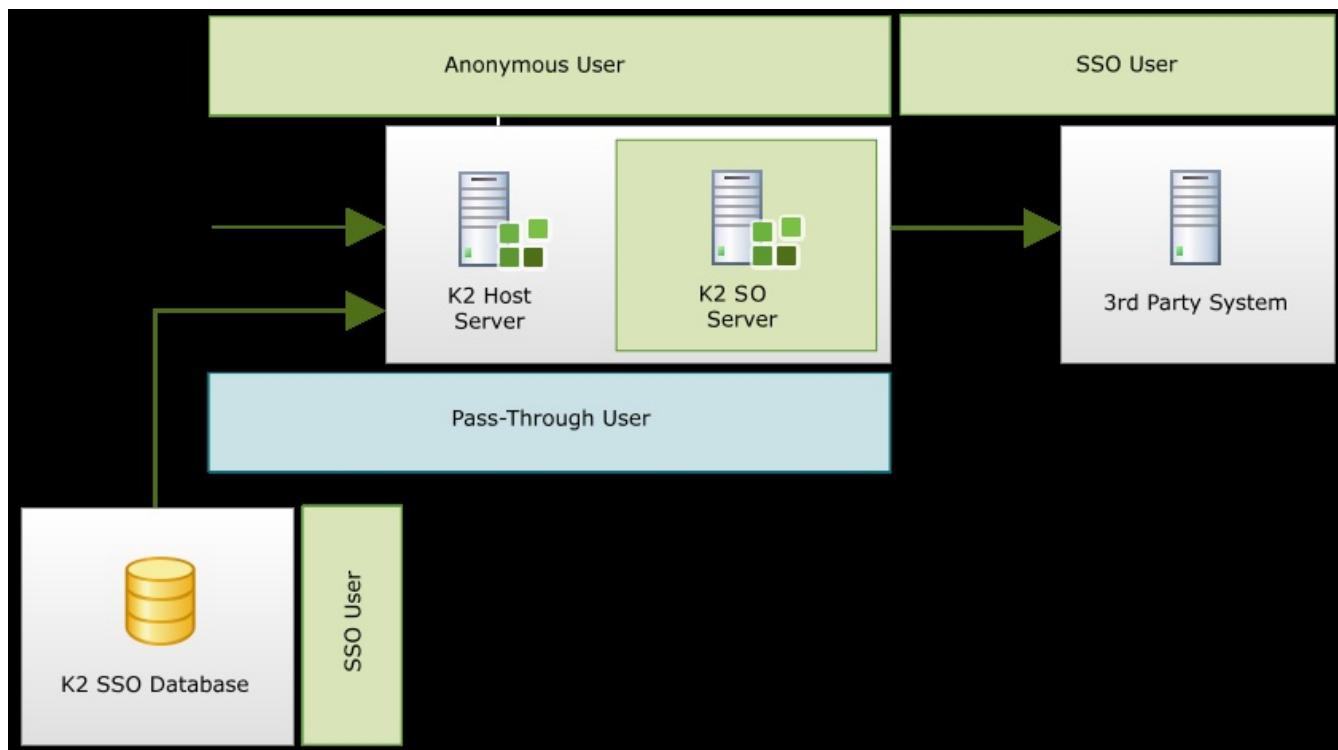


Single Sign On will only come into affect if first K2 Pass-Through were called. Therefore, if the K2 Server using K2 Pass-Through does not receive a pass through call or does not determine that a Pass-Through requirement exists then SSO would not be called in affect either.

Single Sign On has been enhanced to work in conjunction with K2 Pass-Through Authentication so that Active Directory credentials can also be cached in a similar way. This feature enhancement enables the system to check for cached credentials when calling an external system for the current K2 Pass-Through Authentication user. All Active Directory passwords are stored securely within the K2 Databases using K2 symmetric key. This method is therefore by no means a security threat or risk.

Once credentials have been cached and they are available K2 can then logon and impersonate the user when calling the 3rd party system. This method is equivalent to if Kerberos were used to do the same.

There are a number of steps that K2 Host Server follows when utilizing Single Sign On with K2 Pass-Through Authentication:



1.5.3.5.6.4.2 Enforce Impersonation

Enforce Impersonation



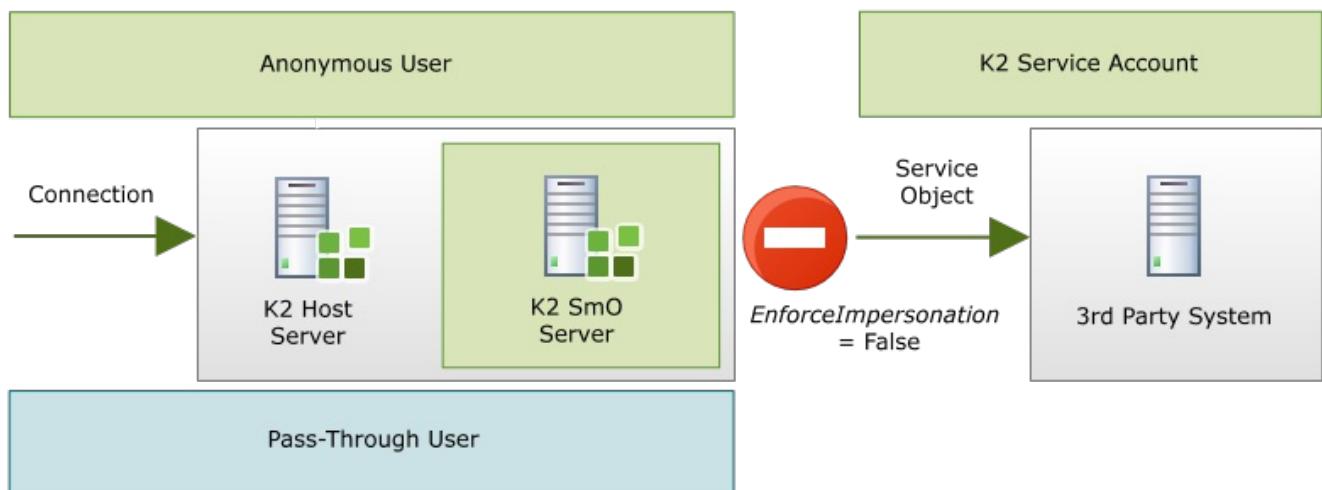
In scenarios where SharePoint Impersonation or Dynamic SQL Service Impersonation are being used; if the Enforce Impersonation flag is set to **True** the native impersonation functionality of the SharePoint Server and the SQL Server Respectively will reject the connection attempt. See the relevant topics for further information. Links are provided in this Caution Box.

If K2 Pass-Through had been called by a service instance and there were no cached credentials for Single Sign On to be used then there would be no user credentials available. In certain instances, it would be acceptable that the K2 Service Account be used to impersonate the Pass-Through user. There are scenarios where setting this flag to true to enforce the impersonation would be unacceptable ie Auditing Processes where the User Credentials should be used to record user access and not the service account.

To provide security an additional, user configurable flag has been added called `EnforceImpersonation`. This setting is configured using the K2 Workspace Service instance tooling.



By default this flag is set to **FALSE**



If Kerberos were configured and functioning or Pass-Through had taken place, this setting would be redundant as the K2 Server would be executing as the Client User and there is no reason to prevent the connection.

1.5.3.5.6.4.3 SharePoint Impersonation

SharePoint Impersonation

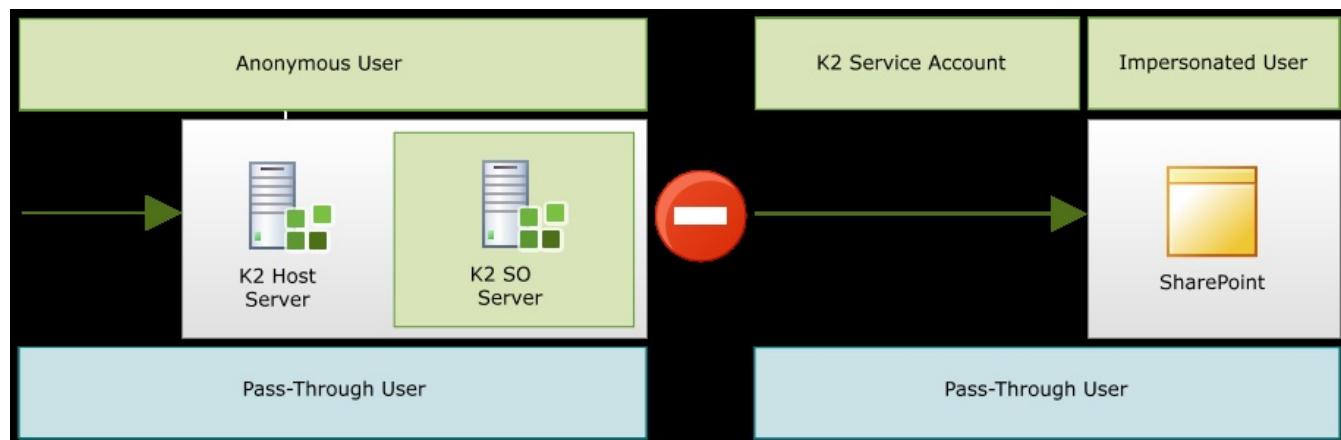
Microsoft SharePoint includes native impersonation capabilities, which can be leveraged when Kerberos has not been configured and credentials need to be passed between machines. One particular scenario where the SharePoint Impersonation can be useful is when SSO capabilities are not available and SharePoint based Service Instances must be executed as the service account.

Service Instance Configuration

From within K2 Workspace, the service instances are configured and the enforce impersonation flag for the relevant service must be set to false. In spite of SharePoint impersonating the Client, the K2 SmartObject Server is unaware of this so if the impersonation flag is set to true, the authentication attempt will be blocked.

How it Works

The K2 SmartObject Server passes the details of the K2 Pass-Through Authentication user to K2's SharePoint-based web service. From this point SharePoint's native impersonation features are used to impersonate the K2 Pass -Through Client user. This methodology is fully supported by Microsoft's SharePoint, and the Client has been successfully impersonated all activity with SharePoint will be logged as being performed by the client, using the client's credentials in the same manner that they would have had Kerberos been configured, for example, if a new list item was created the audit will reflect that the Client user created the List Item and this is supported in all versions of SharePoint namely SharePoint 2007 to SharePoint 2010 from WSS to Enterprise.



1.5.3.5.6.4.4 Dynamic SQL Service Impersonation

Dynamic SQL Server ServiceObject Impersonation

SQL Server includes native impersonation capabilities which can be leveraged when Kerberos has not been configured and credentials need to be passed between machines to authenticate the K2 Pass-Through User.

Service Instance Configuration

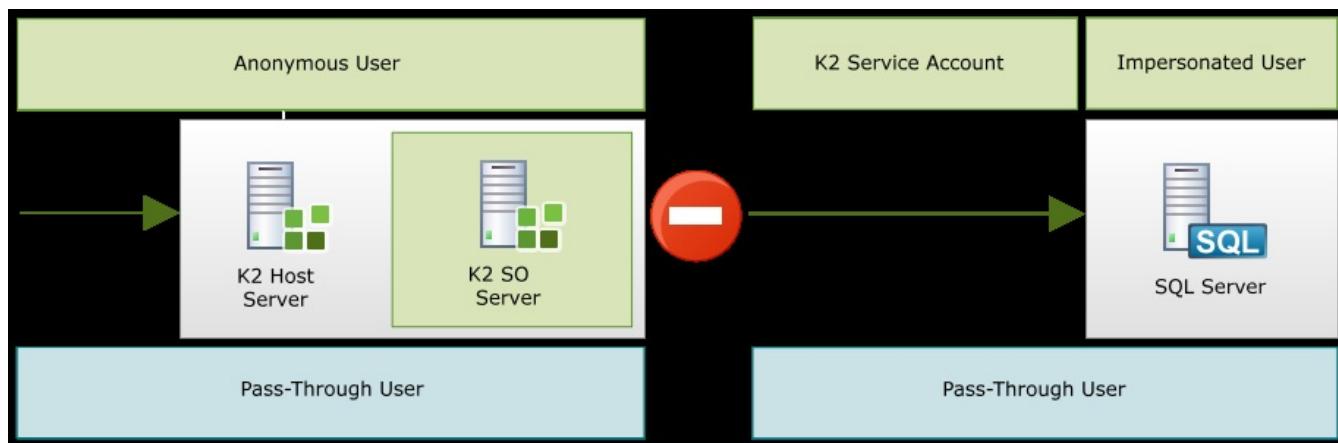
From within K2 Workspace, the service instances are configured and the enforce impersonation flag for the relevant service must be set to false. In spite of SQL Server impersonating the Client, the K2 SmartObject Server is unaware of this so if the impersonation flag is set to true, the authentication attempt will be blocked.



If the Enforce Impersonation flag is set to true, this will result in an Anonymous User error and authentication will fail. The event will be logged in the K2 Logs. See the section on Log Messages.

How it Works

K2 Pass-Through utilizes the K2 Dynamic SQL Server Service Object to impersonate the Pass-Through User. This then allows the K2 Server via the K2 SQL Server Service Object to impersonate the end user to access secure data sources authentically and without creating a security risk and this in spite of only having the K2 Service Account where no Kerberos has been configured or SSO credentials are available.



Authenticating Against the SQL Server Impersonation Functionality

The Dynamic SQL Server Service is able to negotiate the credentials passing of the Pass-Through User by using SQL Server's User Impersonation capability. SQL Server has an "EXECUTE AS LOGON" connection string property. Since this method is available as a SQL Server Product feature, it has the support of the product vendor.

1.5.3.5.6.4.4.1 Dynamic SQL Server Configuration Requirements

Setup Requirements

The following configuration prerequisites are required

1. The K2 Server must run under an account [Domain Name]/K2Service account
2. Within Active Directory there is an user group called 'Domain/SqlUsers' which must contain the names of the users who want access to the specific database(s)
3. The Active Directory user 'Domain/SqlUser1' which makes the delegated call

SQL Server Instance Configuration



These scripts need to be run once per SQL Server instance.

Map Login

For each SQL Server Instance, the following mappings need to be created:

- The SqlServer LOGIN needs to be mapped to [Domain\SqlUsers]
- The LOGIN needs to be mapped to the K2 Host Server Service Account

The above configuration enables the SQL Server to resolve the AD group or user by associating the Windows SID to a SQL SID.



Both AD Groups and AD Users can be added that you can set up a whole AD Group as a LOGIN, it needn't just be an AD User:

Associate Windows SID to SQL SID

```
USE [master];
--Represent caller SID within SQL
CREATE LOGIN [Domain\SqlUsers] FROM WINDOWS;
--Represent service account SID within SQL
CREATE LOGIN [Domain\K2Service] FROM WINDOWS;
GO
```

Grant Impersonation Rights

The Grant IMPERSONATION rights on the K2 Host Server service account script enables the following actions:

- This allows the service account to impersonate as the specific LOGIN
- This is unnecessary if the service account LOGIN has high enough privileges (e.g. sysadmin)

Grant Impersonation Rights

```
USE [master];
--Allow one SID to impersonate as the other
GRANT IMPERSONATE ON LOGIN::[Domain\SqlUsers] TO [Domain\K2Service];
GO
```

Map Server Login to the Local DataBase Principle

The Impersonation rights granted above must be mapped to a database user:

- In the specific database (eg SalesDB), make sure the LOGIN above is mapped to a database USER
- Since LOGINS operate at the SQL Server level, you need a USER principle in each database that is tied to the LOGIN
- Either use an existing USER (such as dbo) or create a brand new database USER as per below

Map Server Login to the Local Database Principle

```
USE [SalesDB];
--Map server LOGIN to a local database principle, in this case using
--the same name for convenience (can also use a different USER name)
CREATE USER [Domain\SqlUsers] FOR LOGIN [Domain\SqlUsers];
GO
```

Grant User Rights



Running this script would not normally be required, but if it is required then only once per SQL Server Instance

- Ensure that the USER specified above has rights to execute/read/write/delete all appropriate objects
- If the LOGIN was mapped to dbo or assigned dbowner (or similar) permissions to the USER then nothing further is required.
- If not, then the following script must be run for the specific database

Grant User Rights

```
USE [SalesDB];
GRANT EXECUTE ON [dbo].[MyProcOrTable] TO [Domain\SqlUsers];
GO
```

1.5.3.5.6.5 Information and Error Messages

Troubleshooting the Log Messages

The list of error messages below are some of the error messages that may occur if or when Kerberos failure takes place. This topic is not intended to cover all aspects but is intended solely to indicate the most likely errors. The types of error messages that will be encountered are divided into two categories namely Information Messages and Error Messages.



See the following topic for more information on the K2 Logging framework : [K2 Auditing and Logging](#)

Information Log Messages

`Switching Security Context from <anonymous user> to <pass-through user> for Session <id>.`

This message displays when a successful K2 Pass-Through Authentication event has occurred. Namely, the client API requested K2 Pass-Through Authentication and the K2 Server confirmed that it meets the requirements of the configuration settings.

`No delegated or cached credentials are available to impersonate [pass-through user] for Session [session id]. External calls will be made in the context of the Service Account.`

If the K2 Host Server needs to contact another hosted server (e.g. the SmartObject Server) and K2 Pass-Through Authentication occurred successfully on the original client connection, K2 Host Server will attempt to use SSO credentials so that the K2 Service Account isn't used. If the current K2 Pass-Through Authentication user has no cached credentials, you'll see this message.

Error Log Messages

`K2 Pass-Through Authentication failed. Current Host Server configuration prevents pass-through to non-Windows identities.`

The message above displays if K2 Pass-Through Authentication is attempted, you have the configuration setting of ClientWindows and the K2 Client API either found a non-Windows token (e.g. Forms) or it wasn't able to verify that the Windows token is authenticated.

`Windows (Kerberos/NTLM) Identity Required. The end-user's identity is not being passed correctly between your client and server, perhaps due to incorrect Kerberos configuration. Either correctly configure Kerberos or utilize K2 Pass-Through Authentication by setting the DelegationContext in K2HostServer.Config to ClientAny or ClientWindows mode instead of <current setting>.`

This message will display if you have ClientKerberos configured (or no setting) and K2 Pass-Through Authentication was attempted, meaning that your Kerberos configuration isn't working. K2 Pass-Through Authentication would fail in this circumstance, so this is a warning that someone should resolve this by either enabling K2 Pass-Through Authentication or fixing Kerberos.

Mismatch Error

The following error: "A mismatch between the end user and the connection credentials has been detected. This may be intentional and will only require action if specific problems are currently being encountered. Refer to Kerberos and K2 Pass-Through Authentication settings..." occurs whenever a client (SourceCode.Workflow.Client) wants to use pass-through, but it is not allowed. This occurs when a user is logged in with the same account as the Workspace AppPool account, PTA-ClientWindows is enabled, and a connection needs to be made to another server such as a domain controller. It should not occur for Kerberos failures. However, there could be a non-related Kerberos failure at the same time depending on the connection being made.

1.5.3.5.6.6 Scenario Walkthrough

Real Time Scenario Explanation

K2 Pass-Through Authentication is of great value in a variety of scenarios for both runtime and the management of K2 components for example K2 Worklist Webpart, K2 Workspace, K2 Process Portal, Custom Task Pages and so on.

The scenario described in this section is designed to illustrate how K2 Pass-Through Authentication can be implemented for an environment where Kerberos has not been configured correctly.

1. SharePoint, with a Site containing an Announcements List
2. K2 Server
3. K2 Workspace
4. Thick-client InfoPath Form we'll use as our client

Run Time Scenario

In this scenario, the InfoPath form will be used to connect in real time to the SharePoint list via a K2 SmartObject. Without K2 Pass-Through Authentication and in an environment where Kerberos is configured incorrectly, this scenario wouldn't be possible and would result in refused connections and Kerberos failure. At each stage a description will be provided as to how K2 Pass-Through Authentication is being used to resolve the Kerberos issues.

SmartObject Creation

From within SharePoint, use K2 SmartObject Configuration to add a SmartObject to the Announcements list – ensuring that you check the integrated check box.

Potential Kerberos-Related Problems	How K2 Pass-Through Authentication Will Help
Under pre K2 Pass-Through Authentication circumstances, the user would not be able to connect K2 SharePoint to create the SmartObject as this is a double hop ie Kerberos delegation failure	Connection will be made

K2 Pass-Through Authentication provides the following functionality

1. K2's SharePoint components use SourceCode.HostClientAPI to contact the K2 Server

 If Kerberos is not configured for this step, this will come through as anonymous
2. K2 Pass-Through Authentication the logon attempt is successful as the user creating the SmartObject
3. K2 Host Server will then call the K2 SmartObject Server
4. The K2 SmartObject Server verifies that the K2 Pass-Through User has rights to create SmartObjects and ServiceInstances
5. The K2 SmartObject Server will execute the relevant methods of K2's SharePoint ServiceObject
6. K2 Server will then contact SharePoint to retrieve the metadata for the Announcement List. This facilitates the creation of the correct SmartObject structure. This is performed as the K2 Service Account context (SharePoint already validated the end-user's permissions so there's no need to do it twice), meaning no other K2 Pass-Through Authentication functionality is used here
7. The SmartObject and related ServiceInstance are created, using the structure retrieved from SharePoint.

InfoPath Form Configuration

This step configures the InfoPath form and integrates it with the SmartObject created in the previous step.

1. Right click the InfoPath form template and choose "Integrate with SmartObject"
2. Select the SmartObject previously created for the Announcements list and choose to link the "Create" method with your form.
3. Add the metadata for the "Create" method to your form and then link this SmartObject method to a button so that you can create an Announcement from the InfoPath form.
4. Publish this InfoPath form so that you can execute it.

Potential Kerberos-Related Problems	How K2 Pass-Through Authentication Will Help
Unable to connect to K2 via the K2	Will allow connection to be made.

Runtime Services (on the K2 Workspace or SharePoint server) as this is a double hop

What happens here with K2 Pass-Through Authentication is as follows:

1. The K2 Runtime services (which may be hosted on the K2 Workspace or SharePoint server) will be contacted by the wizard on the client used to add the SmartObject.
2. These will in turn call K2 via SourceCode.HostClientAPI, performing K2 Pass-Through Authentication in order to log in to K2 as the end-user (if the end user credentials were lost on the hop via the K2 Runtime Services).
3. K2 Host Server will then contact the K2 SmartObject Server in order to retrieve the SmartObject details, via the K2 SharePoint ServiceObject. No connection to SharePoint is required here, so no further K2 Pass-Through Authentication functionality is used.

Executing the InfoPath form – using SharePoint Impersonation

Open the InfoPath form and add an announcement. Once this is complete, verify in SharePoint that the creator of the announcement list item was the end-user and not the K2 Service Account. This has been achieved without any delegation, using K2 Pass-Through Authentication's SharePoint impersonation feature.

Potential Kerberos-Related Problems	How K2 Pass-Through Authentication Will Help
Can't connect to K2 via the K2 Runtime Services (on the K2 Workspace or SharePoint server) as this is a double hop	Will allow connection to be made.
Don't have user credentials to call SharePoint, only the K2 Service Account	Will use SharePoint impersonation in order to make the updates in SharePoint as the end user.

Events taking place using K2 Pass-Through Authentication are as follows:

1. The K2 Runtime services (which may be hosted on the K2 Workspace or SharePoint server) will be contacted by the InfoPath form (running on the client)
2. The K2 Runtime Services will in turn call K2 via SourceCode.HostClientAPI, performing K2 Pass-Through Authentication in order to log in to K2 as the Client-user (if the Client user credentials were lost on the hop via the K2 Runtime Services)
3. K2 Host Server will then contact the K2 SmartObject Server - this will be done as the K2 Service Account
4. The request will be passed to the K2 SharePoint ServiceObject in order to execute the relevant method
5. The K2 SharePoint ServiceObject will pass the K2 Pass-Through user identity to the K2 SharePoint web services (connecting in the K2 Service Account's context) on the SharePoint server. These will perform an impersonation on SharePoint prior to performing the desired functionality – in this case adding the Announcement

Executing the InfoPath form – Enforce Impersonation

Although the option to Enforce Impersonation is redundant with regards to SharePoint (we can use SharePoint impersonation so there is no security issue) we can illustrate how this option functions in this scenario because K2 will contact SharePoint as the K2 Service Account prior to impersonation being performed.

For this step, before opening the InfoPath form and adding the Announcement, do the following:

1. Use the K2 SmartObject Service Tester to locate the ServiceInstance for the Announcements list
2. Set the property to **True**, ensuring that impersonate is also still true. This creation of the Announcement should now fail as the SmartObject Server was contacted as the K2 Service Account instead of the end-user – which was blocked by this property.

Potential Kerberos-Related Problems	How K2 Pass-Through Authentication Will Help
Can't connect to K2 via the K2 Runtime Services (on the K2 Workspace or SharePoint server) as this is a double hop.	Will allow connection to be made.
Don't have user credentials to call SharePoint, only the K2 Service Account.	Will block the Service Account from utilizing a SmartObject marked as integrated.

Events that take place with K2 Pass-Through Authentication are as follows:

1. The K2 Runtime services (which may be hosted on the K2 Workspace or SharePoint server) will be contacted by the InfoPath form (running on the client)
2. These will in turn call K2 via SourceCode.HostClientAPI, performing K2 Pass-Through Authentication in order to log in to K2 as the end-user (if the end user credentials were lost on the hop via the K2 Runtime Services)
3. K2 Host Server will then contact the K2 SmartObject Server. This will be done as the K2 Service Account
4. The K2 SmartObject Server identifies that the EnforceImpersonation property and the Impersonate property

are both true. It then checks the current user in the K2 Host Server as well as the current user executing the code, as they are different (showing we're executing as the service account) an exception is thrown and execution of the SmartObject method stops

Executing the InfoPath form – using Single Sign On

In this instance Single Sign On is used to contact SharePoint as the correct user instead of using the native impersonation functionality available in the K2 SharePoint ServiceObject. Since the system is running as the actual Client user, this will even succeed if the EnforceImpersonation property is true.

To add SSO credentials for the end user, either use the K2 Workspace to cache the credentials, or just connect to the K2 Host Server via any API (e.g. via the Workflow Management API) with a connection string that resembles the following:

```
Integrated=False; IsPrimaryLogin=True; SecurityLabelName=K2; UserID=[user\domain];
Password=[password]; Host=[k2 server]; Port=[port]
```

Once this is done, open the InfoPath form and create an Announcement. Again, it should be created as the end user and not the K2 Service Account.

Potential Kerberos-Related Problems	How K2 Pass-Through Authentication Will Help
Can't connect to K2 via the K2 Runtime Services (on the K2 Workspace or SharePoint server) as this is a double hop.	Will allow connection to be made.
Don't have user credentials to call SharePoint, only the K2 Service Account.	Use SSO to store and retrieve credentials. Logging on as and impersonating that user so that the credentials are used to call SharePoint, just as if Kerberos was working.

What happens here with K2 Pass-Through Authentication is as follows:

1. The K2 Runtime services (which may be hosted on the K2 Workspace or SharePoint server) will be contacted by the InfoPath form (running on the client)
2. These will in turn call K2 via SourceCode.HostClientAPI, performing K2 Pass-Through Authentication in order to log in to K2 as the end-user (if the end user credentials were lost on the hop via the K2 Runtime Services)..
3. K2 Host Server will note that it needs to call a hosted server (the K2 SmartObject Server) and that it is doing K2 Pass-Through Authentication. It will then retrieve the SSO credentials for that user which are now present.
4. The K2 Host Server will logon and impersonate the end-user by using the SSO credentials, before calling the K2 SmartObject Server as the impersonated SSO user (end user).
5. The request running under the SSO credentials will be passed to the K2 SharePoint ServiceObject in order to execute the relevant method to add the Announcement
6. Once this is complete, the K2 Host Server will revert to the Service Account.

1.6 K2 blackpearl Installation Guide

Installation Overview

When installing K2 blackpearl, the Setup Manager will walk you through selecting the components based on the prerequisites or dependencies being available prior to install. The Setup Manager will install the selected components and configure them.



Please note that Setup Manager needs .NET Framework 3.5 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

Installing K2 blackpearl can be done in a number of ways:

1. **Standalone System.** All K2 components (with the possible exception of the K2 Database) are installed on a single server
2. **Distributed Environment.** K2 components are separated onto various servers
3. **Client Tools Only:** Installs the Development tools. These tools enable the K2 Process Developers to build processes collateral for the K2 Environment

If there are errors with the installation and environment configuration, the K2 Configuration Analysis tool will be run automatically once the Setup Manager is complete to identify the errors and assist the person installing the K2 components to resolve them.

The next sections will walk you through either scenario and help you configure your environment.



While not required, it is strongly recommended to close all other open applications, including anti-virus software and other disk-intensive applications, before installing K2 blackpearl. While K2 will install successfully, the performance of the installer may be hindered by the applications.



- Do not run Windows Updates while installing
- Where errors or issues are encountered during the course of the installation process, it is strongly recommended that they be addressed before proceeding with the installation. Be sure that you completed installing all of the prerequisites and did the set up steps in the **Before you begin** section prior to installing K2 blackpearl.

K2 blackpearl Installation Guide

The K2 blackpearl Installation Guide is intended to provide adequate guidelines on:

1. Assessing the target environment
2. Planning the environment and performing pre - installation tasks
3. Performing the installation
4. Performing post installation tasks.

The above four steps should be performed as listed to ensure a successful installation.



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.



Since all environments are not the same but are diverse in nature, it is not possible to provide information that suits every prospective environment exactly. Owing to this, the information below is provided as a guideline to the process of creating a K2 blackpearl environment.

Installation Checklist

Prerequisites		
Item		
Reference Topic		
<input type="checkbox"/>	Hardware	Hardware Prerequisites
<input type="checkbox"/>	Software	Software by Component Software by Server Role
Before you begin		
Item		
<input type="checkbox"/>	Adding DNS Entries	Adding DNS Entries

<input type="checkbox"/>	Set up Service Accounts	Setting up Service Accounts
<input type="checkbox"/>	Set up Permissions	Set up Permissions
<input type="checkbox"/>	Set up NLB	Setting up NLB
<input type="checkbox"/>	Set up SPNs and Delegation	Set SPNs for the K2 Service Account Set SPNs for the Reporting Services Service Account Set SPNs for the K2 Workspace Service Account Set SPNs for the SharePoint Service Account
<input type="checkbox"/>	Set up MSMQ	Setting up MSMQ
<input type="checkbox"/>	Set up DTC	Setting up DTC
Installing K2 blackpearl		
Item	Reference Topic	
<input type="checkbox"/>	Installing a standalone system	Installing the Components
<input type="checkbox"/>	Installing a distributed environment*	
	<input type="checkbox"/> Install and configure the K2 Host Server	Install K2 blackpearl on the K2 Server
	<input type="checkbox"/> Install and configure the K2 Reports	Install the K2 for Reporting Services component
	<input type="checkbox"/> Install and configure the K2 Workspace	Install K2 Workspace on the IIS Server
	<input type="checkbox"/> Install and configure the K2 for SharePoint component	Install the K2 for SharePoint component on the SharePoint Server
	<input type="checkbox"/> Installing the Client Components	Installing K2 for Visual Studio
<input type="checkbox"/>	Post installation common tasks	K2 Environment Security Adding Multiple Active Directory Domains
<input type="checkbox"/>	Installing additional nodes	Adding another K2 Server to the farm Configuring Additional K2 Workspace Nodes
Troubleshooting		
Item	Reference Topic	
<input type="checkbox"/>	Troubleshooting common issues	See the Troubleshooting section of the help file
<input type="checkbox"/>	Environment Validation	Checklist: Environment Validation

* Kerberos is only setup if K2 Pass Through Authentication will not be used.

1.6.1 Optional installation logging for troubleshooting

Trace Logging

The trace logging feature is available only for the K2 Setup Manager and is intended to provide event logging for the installation process. The intended user base for this feature are K2 Support or Customer Infrastructure Administrators and Installers who would need to troubleshoot any errors that they may encounter when installing a distributed environment. The Trace Logging feature is not part of the K2 Logging framework which is operational at run time, this feature is only operational during the installation process and only logs events relevant to the installation.

Operational Considerations

The feature is enabled by default and can be disabled manually before the K2 Setup Manager is run.

How this works

During the course of the installation, multiple threads are active and this results in a large volume of potential information being generated by the logging service. Owing to this, the trace logging service will only log event items which are deemed necessary or which may be useful for debugging.



The items or elements deemed useful for debugging are predetermined and there are no additional settings that can be configured.

How to Enable or Disable Trace logging

Trace Logging is disabled manually by amending the Product.config file and setting a flag as shown below.

To make the changes, browse to the folder where the K2 blackpearl installer unpacked to and edit the Product.config file to make the changes.

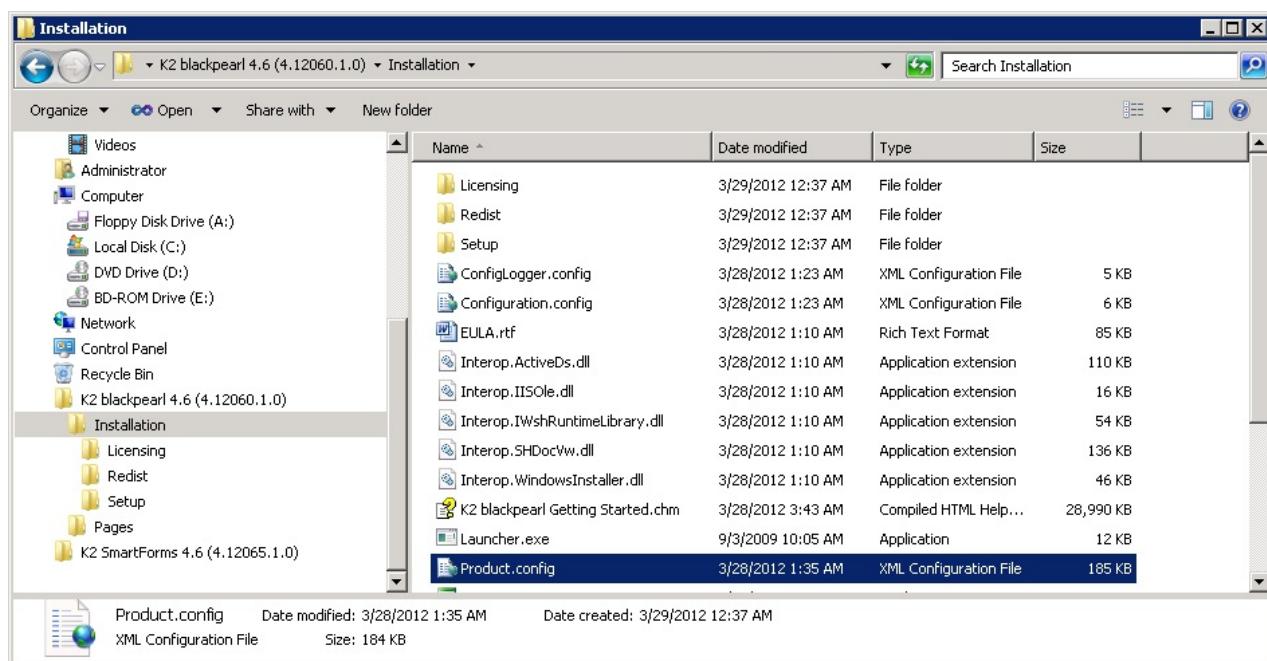
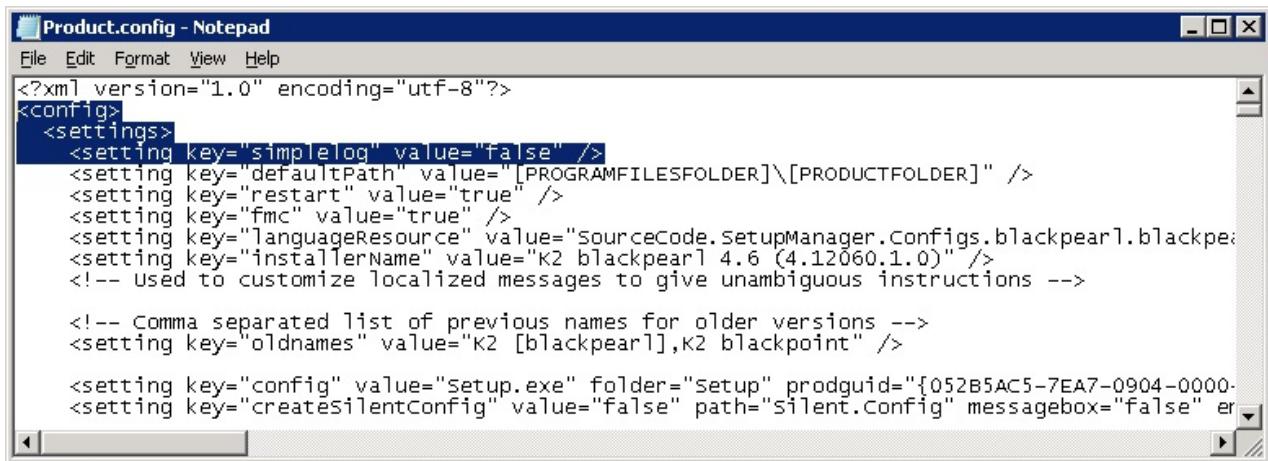


Figure 1: Example of extraction folder. Note the Product.config file is in the Installation folder.

1. Open the Product.config
2. Set the following key to **true or false** to enable or disable trace logging respectively, then save the file



```

<?xml version="1.0" encoding="utf-8"?>
<config>
  <settings>
    <setting key="simplelog" value="false" />
    <setting key="defaultPath" value="[PROGRAMFILESFOLDER]\[PRODUCTFOLDER]" />
    <setting key="restart" value="true" />
    <setting key="fmc" value="true" />
    <setting key="languageResource" value="SourceCode.SetupManager.Configs.blackpearl.blackpearl" />
    <setting key="installerName" value="K2 blackpearl 4.6 (4.12060.1.0)" />
    <!-- Used to customize localized messages to give unambiguous instructions -->
    <!-- Comma separated list of previous names for older versions -->
    <setting key="oldnames" value="K2 [blackpearl],K2 blackpoint" />
    <setting key="config" value="setup.exe" folder="Setup" prodguid="{052B5AC5-7EA7-0904-0000-000000000000}" />
    <setting key="createsilentconfig" value="false" path="silent.Config" messagebox="false" error="true" />
  </settings>
</config>

```

3. Start the Installer (Setup.exe)



The changes to the Product.config file must be made before the K2 Installer is started.

Setting	Description
Simple Log = "false"	No trace logging is run during the installation process.
Simple Log = "true"	When set to true, trace logging is enabled. This is the default setting.

Accessing the Installer Trace Logs

Once the installation is complete, the Installer Trace log is available at "%temp%\k2 setup log" and named "**InstallerTrace[date_iteration].log**". If there are issues with the installation, the K2 Configuration Analysis tool would indicate that there are / may be issues that require resolving.

1.6.2 Installing a standalone K2 blackpearl system

A standalone system install

A standalone system install is one where all components of the K2 blackpearl system are hosted on the same server. These components are described in the image below:



Please note that Setup Manager needs .NET Framework 3.5 to execute while the K2 Server, K2 Studio and K2 for Visual Studio components require .NET Framework 4.

Server Component	Operating system
K2 Server K2 Databases K2 Reporting Services K2 for SharePoint K2 Workspace	<ul style="list-style-type: none"> * *** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012
K2 for Visual Studio K2 Studio These two components may be installed on ANY of the operating systems listed.	<ul style="list-style-type: none"> Microsoft Windows Vista with SP1 or SP2 (Business or Ultimate) or Windows 7 with or without SP1 or Microsoft Windows 8 (windows 8 / Pro / Enterprise)
<p>*Latest security patches *32-bit and 64-bit support</p>	
Server Component	Windows Components
K2 Server	<ul style="list-style-type: none"> Microsoft Message Queuing (MSMQ) Services <ul style="list-style-type: none"> Message Queuing Server Directory Service Integration A User Manager: The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 Reporting Services K2 for SharePoint K2 Workspace	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
K2 Database	<ul style="list-style-type: none"> Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 for Visual Studio K2 Studio	<ul style="list-style-type: none"> No Windows components
Server Component	Additional Software
K2 Server	<ul style="list-style-type: none"> Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5 <p>For more information on .NET framework and K2, please see the topic: .NET Technologies</p> Windows Support Tools (see Install Windows Support Tools for more information: for 32-bit see http://go.microsoft.com/fwlink/?LinkId=62270). <p>Note: Windows Support Tools is a prerequisite if the installer is to automatically set the SPNs during the installation of K2 blackpearl. Otherwise, the Windows Support Tool is regarded as optional software.</p> <ul style="list-style-type: none"> Windows Identity Foundation Redistributable (for more information, see

	<p>http://support.microsoft.com/kb/974405).</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). • If CRM is used: Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server, the server must have .NET 4 enabled.) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en
K2 Database	<ul style="list-style-type: none"> • Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Note: .NET Framework 4.0 is supported but not a prerequisite • Microsoft SQL Server 2012 Express, Standard, BI, Enterprise or Microsoft SQL Server 2008 Express, Standard, Enterprise SP3 or Microsoft SQL Server 2008 R2 SP1
K2 Workspace	<ul style="list-style-type: none"> • Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 • Microsoft Report Viewer Redistributable 2005 SP1 <ul style="list-style-type: none"> • Full installation: http://www.microsoft.com/downloads/details.aspx?FamilyID=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=en • Upgrade installation: http://www.microsoft.com/downloads/details.aspx?FamilyId=35F23B3C-3B3F-4377-9AE1-26321F99FDF0&displaylang=en <p style="text-align: center;">and</p> <p style="text-align: center;">Microsoft Report Viewer Redistributable 2008</p> <p style="text-align: center;">http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en</p> <p style="text-align: center;">or</p> <p style="text-align: center;">Microsoft Report Viewer Redistributable 2008 SP1</p> <p style="text-align: center;">http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en</p> <p>NOTE: K2 Reports Runtime – requires Microsoft Report Viewer Redistributable 2008 SP1 K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2005 SP1</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). • Microsoft Silverlight 4 or 5: (required for View Flow) http://www.silverlight.net/getting-started
* IISReset or reboot is recommended after installation	
K2 Studio	<ul style="list-style-type: none"> • Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5
 For more information on .NET framework and K2, please see the topic: .NET Technologies • Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. • Microsoft Exchange Server 2007 SP3 (required for Exchange Wizard) or Microsoft Exchange Server 2007 Management Tools SP3 or Microsoft Exchange 2010 SP1 or Microsoft Exchange 2010 SP2 • Windows Powershell • Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en • OpenXML SDK 2.0 Redistributable (required for Inline Functions)

	<p>http://msdn.microsoft.com/en-us/office/bb265236.aspx</p> <ul style="list-style-type: none"> ● Microsoft Office SharePoint Server (MOSS) 2007 SP3 <ul style="list-style-type: none"> ● Excel Web and Calculation Services ● Trusted file locations for Excel spreadsheets ● Microsoft SharePoint Server 2010 RTM or SP1 ● Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets ● Either Visual Studio 2012 or Visual Studio 2010 Web Deployment Projects is required to deploy projects in K2 Studio (http://www.microsoft.com/en-us/download/details.aspx?id=25163) <p>Windows SDK v7.0A is required when the 'Generate ASP Pages' option is used. This is installed and configured when Visual Studio 2010 or 2012 is installed.</p>
K2 for SharePoint	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 ● Microsoft Windows SharePoint Services 3.0 (WSS) SP2 or Microsoft Office SharePoint Server 2007 (MOSS) Standard, Enterprise SP3 or SharePoint 2010 Foundation or SharePoint 2010 Foundation SP1 or SharePoint Server 2010 or SP1 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode) ● SharePoint Foundation 2010 Client Side Object Model Redistributable (required for CSOM Service Broker and is installed on the K2 Server) ● Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en ● Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en ● Visual Studio 2010 Web Deployment Projects (required for Forms Technology): http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24509
K2 for Visual Studio	<ul style="list-style-type: none"> ● Microsoft .NET Framework 4 (.NET Framework 4.5 is supported but not required): <p style="margin-left: 20px;">For more information on .NET framework and K2, please see the topic: .NET Technologies</p> ● Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) with or without Sp1 ● A User Manager: <p style="margin-left: 20px;">Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl.</p> ● Windows Powershell ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en ● OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx ● Excel Web and Calculation Services <p style="margin-left: 20px;">with Trusted file locations for Excel spreadsheets or Microsoft SharePoint Server 2010 and Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets</p>

K2 for Reporting Services	<ul style="list-style-type: none"> ● Microsoft SQL Server 2012 Reporting Services or Microsoft SQL Server 2008 Reporting Services ● Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en <p>NOTE: K2 Reports Runtime and K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2008 SP1</p> <ul style="list-style-type: none"> ● Microsoft .NET Framework 3.5 SP1 Redistributable Package and Microsoft .Net Framework 4 http://www.microsoft.com/downloads/details.aspx?FamilyID=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en ● Microsoft Internet Explorer 8 or 9 or 10 (Plug-in support is only available in Internet explorer 10 on the desktop, and this version of Internet Explorer 10 must be used for items built on Silverlight, such as the K2 designer for SharePoint). ● Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server)
---------------------------	--

Before starting the installation there are prerequisites that need to be met. Details can be found at these links:

- [Hardware](#)
- Software prerequisites for a standalone installation are listed in the table below
- [Permissions for K2 components](#)
- [Pre configure environment](#)

Software prerequisites for a standalone installation

Server Component	Operating system
K2 Server	● Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 * **
K2 Databases	
K2 Reporting Services	
K2 for SharePoint	
K2 Workspace	
K2 for Visual Studio	● Windows Vista SP1 or SP2 or Windows 7 RTM or SP1
K2 Studio	
These two components may be installed on ANY of the operating systems listed.	

*Latest security patches

*32-bit and 64-bit support

Server Component	Windows Components
K2 Server	<ul style="list-style-type: none"> ● Microsoft Message Queuing (MSMQ) ● A User Manager: The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 Reporting Services	<ul style="list-style-type: none"> ● IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager ● Distributed Transaction Coordinator (DTC) ● IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 for SharePoint	
K2 Workspace	

K2 Database	<ul style="list-style-type: none"> Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured)
K2 for Visual Studio K2 Studio	<ul style="list-style-type: none"> No Windows components
Server Component	Additional Software
Common software to all Server Components	<ul style="list-style-type: none"> Microsoft .NET Framework 4 <p>For more information on .NET framework and K2, please see the topic: .NET Technologies</p>
K2 Server	<ul style="list-style-type: none"> Windows Support Tools (see Install Windows Support Tools for more information: for 32-bit see http://go.microsoft.com/fwlink/?LinkId=62270). <p>Note: Windows Support Tools is a prerequisite if the installer is to automatically set the SPNs during the installation of K2 blackpearl. Otherwise, the Windows Support Tool is regarded as optional software.</p> <ul style="list-style-type: none"> Windows Identity Foundation Redistributable (for more information, see http://support.microsoft.com/kb/974405). Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). <p>Note: .NET Framework 4.5 is supported but not a prerequisite</p>
K2 Database	Microsoft SQL Server 2012 Express, Standard, BI, Enterprise or Microsoft SQL Server 2008 Express, Standard, Enterprise SP3 or Microsoft SQL Server 2008 R2 SP1
K2 Workspace	<ul style="list-style-type: none"> Microsoft Report Viewer Redistributable 2008 SP1* <p>http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 8 or 9 Microsoft Silverlight 4 or 5: (required for View Flow) <p>http://www.silverlight.net/getting-started</p>
* IISReset or reboot is recommended after installation	
K2 Studio	<ul style="list-style-type: none"> Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. Microsoft Exchange Server 2007 SP3 (required for Exchange Wizard) or Microsoft Exchange Server 2007 Management Tools SP3 or Microsoft Exchange 2010 SP1 or Microsoft Exchange 2010 SP2 or Microsoft Exchange 2013 Windows Powershell Microsoft Dynamics CRM 4.0 Workgroup, Professional (Pro) Server or Enterprise Server or Microsoft Dynamics CRM 2011 (required for CRM Wizard and CRM SmartObject) Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 SDK <p>http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en</p> <ul style="list-style-type: none"> OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx Microsoft Office SharePoint Server (MOSS) 2007 SP3 <ul style="list-style-type: none"> Excel Web and Calculation Services Trusted file locations for Excel spreadsheets Microsoft SharePoint Server 2010 RTM or SP1 Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets
K2 for SharePoint	<ul style="list-style-type: none"> Microsoft .NET Framework 4 Microsoft Windows SharePoint Services 3.0 (WSS) SP2 or Microsoft Office SharePoint Server 2007 (MOSS) Standard, Enterprise SP3 or SharePoint 2010

	<p>Foundation or SharePoint 2010 Foundation SP1 or SharePoint Server 2010 or SharePoint Server 2010 SP1</p> <ul style="list-style-type: none"> Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en Microsoft Internet Explorer 8 or 9 Microsoft Dynamics CRM 4.0 Workgroup, Professional (Pro) Server or Enterprise Server or Microsoft Dynamics CRM 2011 (required for CRM Wizard and CRM SmartObject) Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 SDK http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en
K2 for Visual Studio	<ul style="list-style-type: none"> Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) or with SP1 A User Manager: Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl Microsoft Exchange Server 2007 SP3 (required for Exchange Wizard) or Microsoft Exchange Server 2007 Management Tools SP3 or Microsoft Exchange 2010 SP1 or Microsoft Exchange 2010 SP2 or Microsoft Exchange 2013 Windows Powershell Microsoft Dynamics CRM 4.0 Workgroup, Professional (Pro) Server or Enterprise Server (required for CRM Wizard and CRM SmartObjects) Microsoft Dynamics CRM 4.0 SDK http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx Microsoft Office SharePoint Server (MOSS) 2007 SP3 <ul style="list-style-type: none"> Excel Web and Calculation Services Trusted file locations for Excel spreadsheets Microsoft SharePoint Server 2010 or Microsoft SharePoint Server 2010 SP1 Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets <p>Note: .NET Framework 4.5 is supported but not a prerequisite</p>
K2 for Reporting Services	<ul style="list-style-type: none"> Microsoft SQL Server 2012 Reporting Services or Microsoft SQL Server 2008 Reporting Services Microsoft Internet Explorer 8 or 9 Microsoft Dynamics CRM 4.0 Workgroup, Professional (Pro) Server or Enterprise Server Microsoft Dynamics CRM 4.0 SDK



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Installation steps

Click on this link to see a flow diagram of the install steps.

Before the installation is started, the user must decide if the trace logging feature should be enabled. See the topic [Optional installation logging for troubleshooting](#) for more information.

When the installation is started, the Setup Manager will run through the following steps:

- 1 On the **Welcome** screen, click **Next**
- 2 The Setup Manager will check for the **latest version** of K2 blackpearl.

On the **Welcome** screen, click **Next**

The Setup Manager will check for the **latest version** of K2 blackpearl.

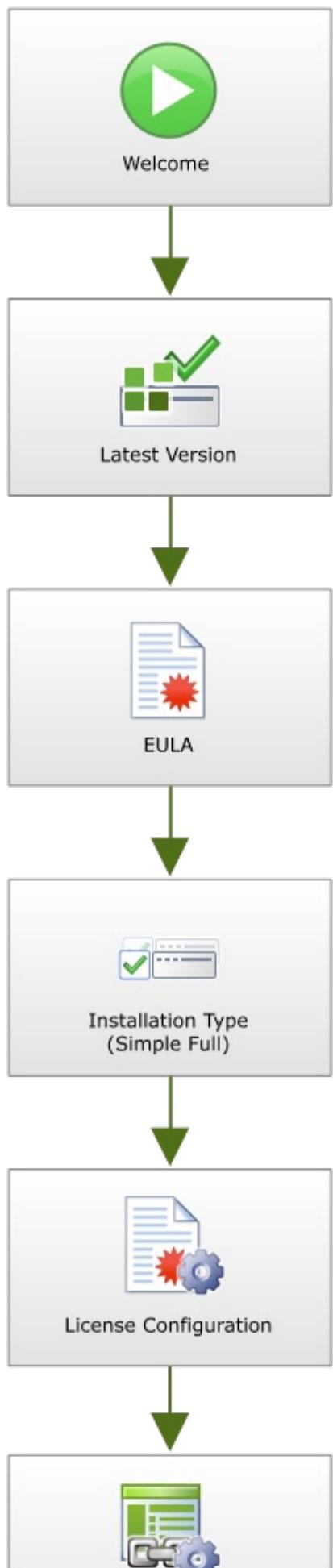
-  The **End User License Agreement** needs to be agreed to before continuing.
-  The **Installation Type** screen allows the user to select either a Simple install or a Custom install. The Simple install allows for a Full install (follow the steps below) or **Client Tools only install**.
-  On the **License Configuration** screen, the user must enter the license corresponding to the system key displayed.
-  Once the license has been entered, the **K2 Workspace web site** must be configured.
-  The next step is to configure the optional **CRM** server details.
-  If an Exchange Server is being used in the environment K2 is being installed to, it will be configured on the **Exchange Server Configuration screen**.
-  As with the previous step, if Exchange is being used, the **Exchange Integration screen** needs to be configured.
-  SmartActions are enabled by default and set up on the **SmartActions Configuration** screen.

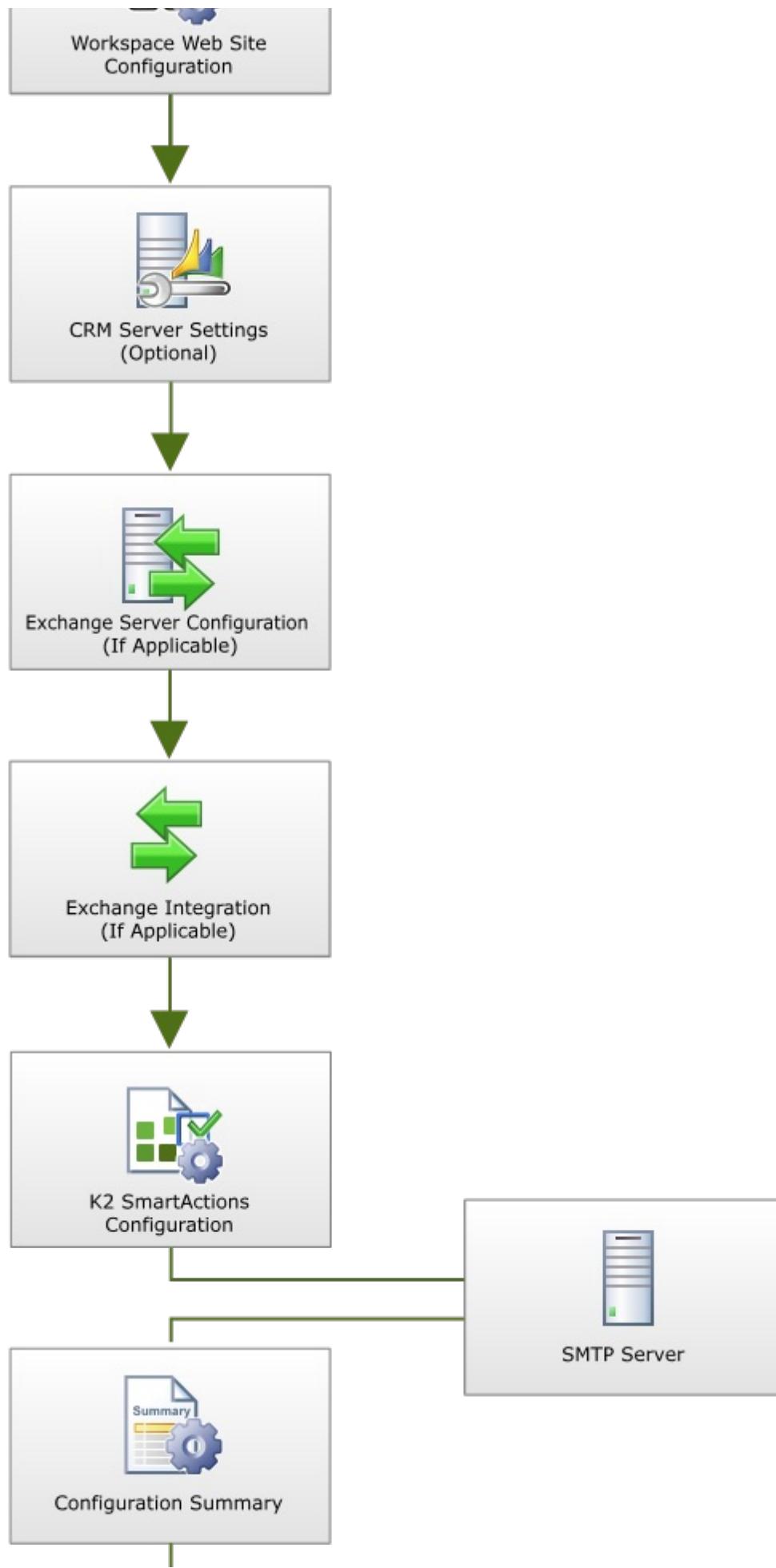
Note: The **SMTP Settings** screen is displayed after step 10 (SmartActions setup) only if the **Use Exchange for mail integration** option has been selected on the **Exchange Server Configuration** screen.

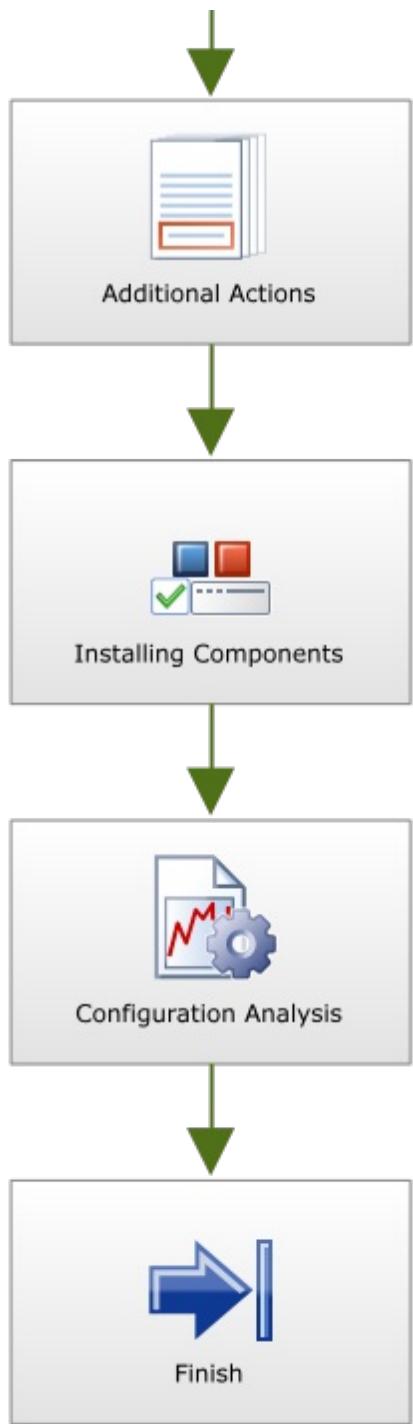
-  Finally, the **Configuration Summary** screen will be shown where the installation can be reviewed.
-  Before the install begins, the **Additional Actions** screen is displayed if there are any actions that need to be performed.
-  The **Installing Components** screen displays the status of the installation and then displays the Configuration Status screen.
-  Once the components are installed and configured, the **Configuration Analysis** tool runs to verify settings.
-  This **Finished** page appears when the K2 Setup Manager is complete.

The Finished page of the Setup Manager provides the option of starting the SharePoint Configuration, see the topic **SharePoint Configuration** in the installation Post common tasks section of this help file.

1.6.2.1 Standalone Install Flow Diagram







1.6.2.2 Welcome Screen

Welcome Screen

After you have installed all the [prerequisites](#), created the [service accounts](#), enabled DTC and installed MSMQ, you are now ready to install the K2 blackpearl Server.

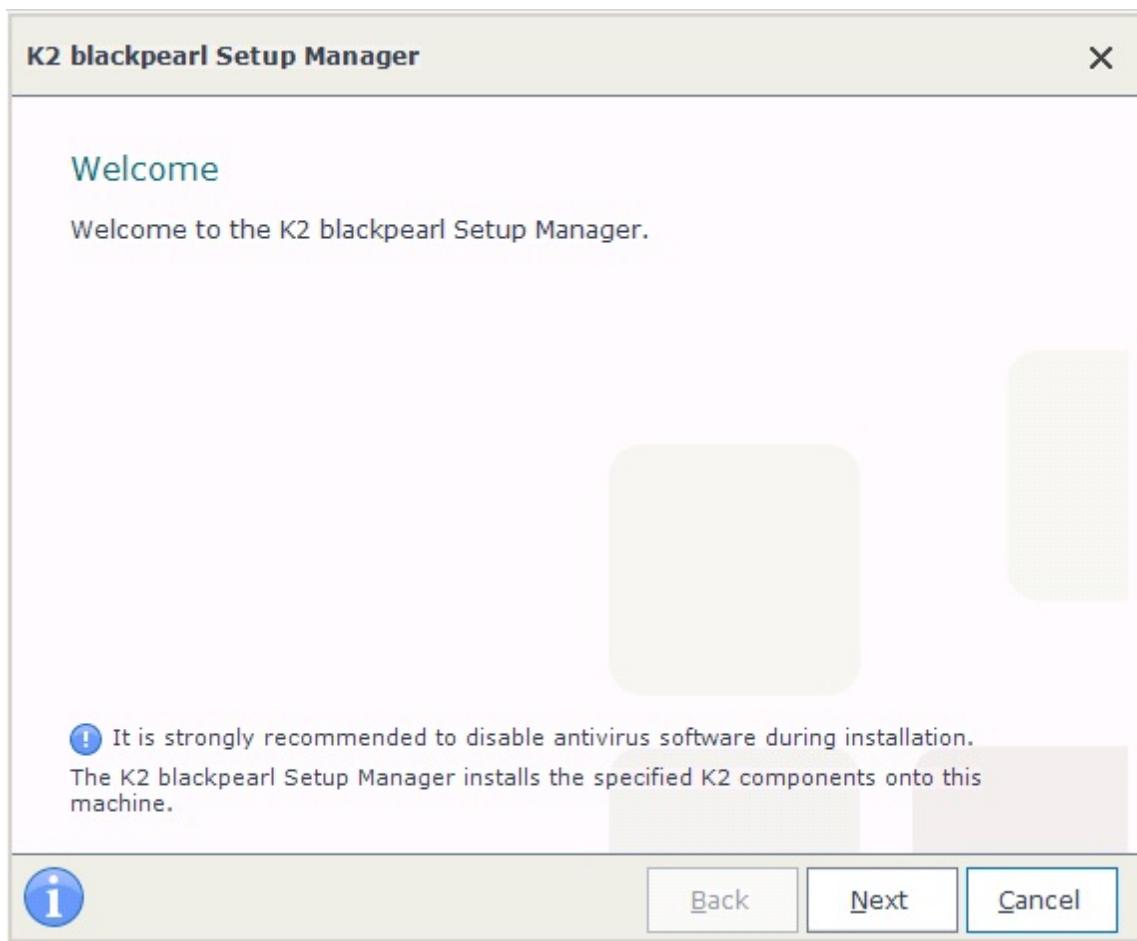


All user names, domain names and URLs displayed in the setup manager pages in this guide are examples. Be sure to replace the values with your actual user names and URLs in your environment.



It is recommended to install all K2 components using the K2 Service Account. Log on to the server as the K2 Service Account before installing.

The **Welcome** screen displays when you start the Setup Manager.



What to do on this page

The steps below offer details on how to complete the page:



Click **Next** to proceed

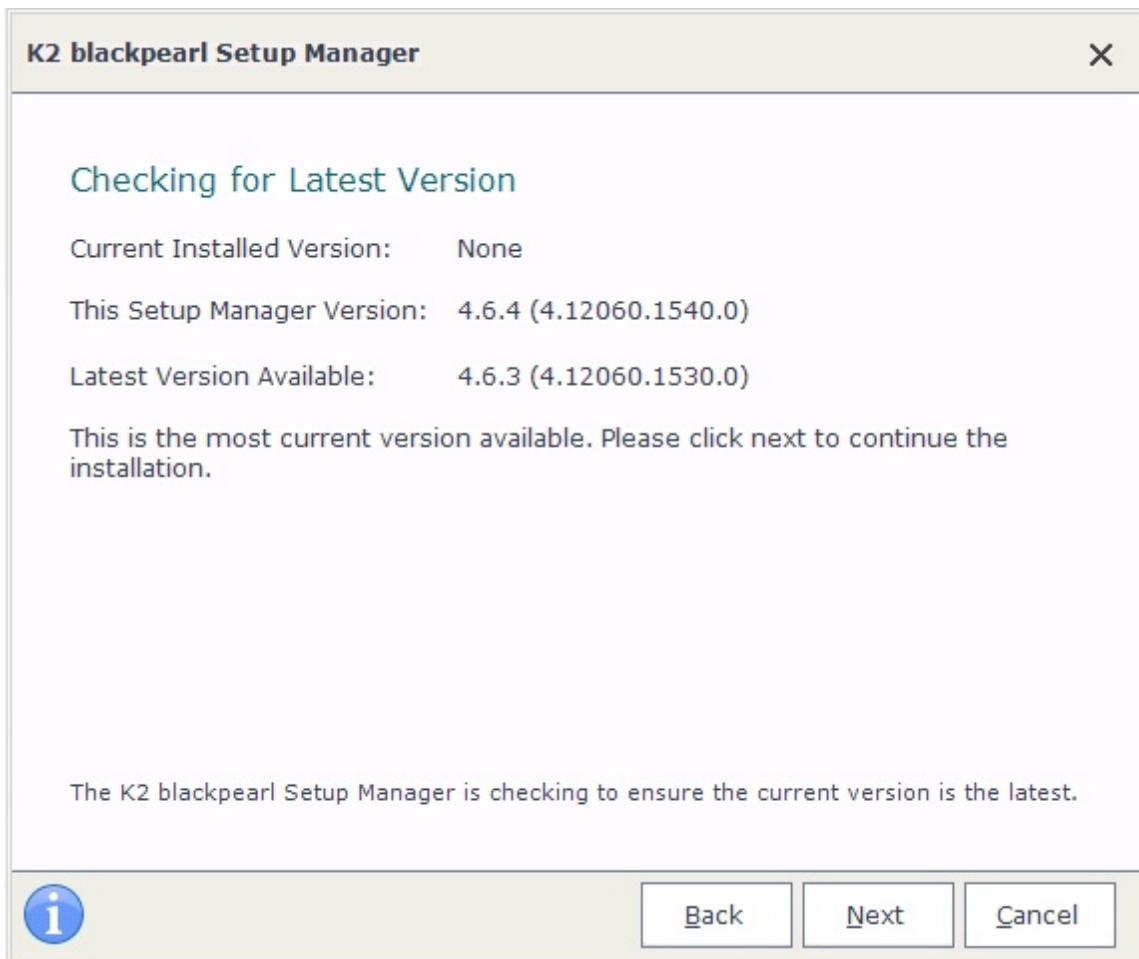
1.6.2.3 Latest Version Validation

Latest Version Validation



An internet connection is required for this feature to be able to report accurately on the version that is currently being installed.

The K2 Installer, once the welcome screen has been displayed, will verify online whether the version being installed is the latest version. Although the latest major version may be the version being installed, there may be an update which includes enhancements or fixes.



The version validation feature will provide assistance in three ways:

1. The version in use is correct with no further updates required
2. The version in use has an update available which must be downloaded
3. The utility is unable to determine if there is an update

Checking for Latest Version	
Current Version	The version of the installer currently being used to install K2 blackpearl
Latest Version*	The version of the installer which is available from the K2 Portal
* The latest version can only be determined with the aid of an internet connection.	

What to do on this page

The steps below provide details on how to complete this page:



- 1 Wait for the page to report on the versioning



Take the necessary action as reported by the user page

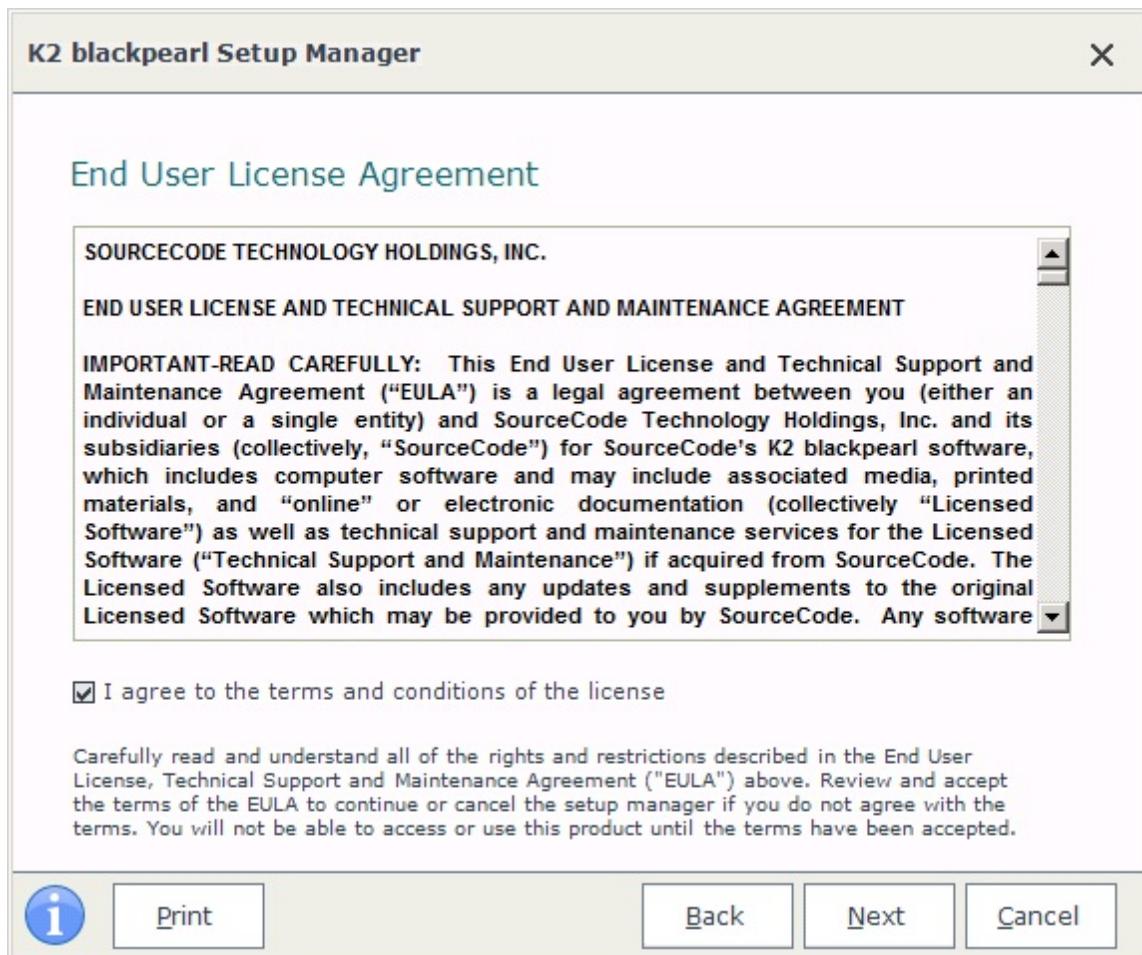


Click **Next** to proceed

1.6.2.4 End User License Agreement

End User License Agreement

The EULA describes the terms and conditions under which the K2 Platform (in whole or in part) can be installed. The software can only be installed when the person installing the software agrees to the terms and conditions as outlined in the EULA.



End User License Agreement	
I agree to the terms and conditions of the license	The installer has the option to agree or not agree with the EULA. The product can only be installed if the installer selects this checkbox.
 Important: Selecting the I agree checkbox and clicking Next is indicative of full agreement with the terms and conditions of the EULA. Selecting the option I agree therefore binds the organization to comply with all terms and conditions as stated by the agreement.	

What to do on this page

The steps below provide details on how to complete this page:

- 1 Read and become familiar with the contents of the EULA
- 2 Select the **I agree to the terms and conditions of the license** checkbox (Selecting this option legally binds the organization to terms and conditions)
- 3 Click **Next** to proceed
- Optional Click **Cancel**, and the installation is discontinued and the Setup Manager will exit.

Step
Optional Step Click the **Print** button to print out a hardcopy of the EULA.

1.6.2.5 Installation Type

Installation Type

On the **Installation Type** screen, select the type of installation and browse to the location where you want to install the K2 components.

The choice of installation may have an effect on the order in which user pages are displayed.

K2 blackpearl Setup Manager

Installation Type

(Simple Installation)
 Full Installation
 Client Tools Only
 Custom Installation

Installation Folder

Installation Folder:

Select the installation type and the folder where the application will be installed. To install to a different folder, click the 'Browse' button and select another folder.

i

Installation Type

On the **Installation Type** section, the **Simple Installation** allows a user to either do a full installation or only install the client tools:

- **Full Installation:** This option performs an installation of the entire K2 blackpearl on a Single machine based on the prerequisites installed. This install does not allow a user to select specific components to be installed it simply installs all the components.

This option does not prompt the individual installing K2 to select components, but installs K2 components based on the prerequisites available.

- **Client Tools Only:** This option only installs the client tools on the local machine.
- **Custom Installation:** The **Custom Installation** option can do either a standalone installation, or a **distributed installation** (depending on what the user specifies). This install allows a user to select specific components to be installed.

Installation Folder

On the **Installation Folder** section, browse to the location where you want to install the K2 blackpearl components.

Installation Folder	
Installation Folder	<ul style="list-style-type: none"> • The default installation location is C:\Program Files (x86)\K2 blackpearl • This location can be changed by typing in a folder location manually • You can also click on the browse button to navigate to a folder



Important: When selecting a location, ensure that the location exists on the **LOCAL** system. Do not install a component on a network drive, K2 blackpearl will not function properly.

What to do on this page

The steps below provide details on how to complete this page:



Select an installation type.



Select an installation location. The default is recommended, however any local location is suitable. You can use the browse button to navigate to a folder location. Network drive locations are not recommended.



Click **Next** to proceed.

If the default selection was chosen, the installer will bypass the component selection screens and proceed to the license screen here: **License Configuration**

If the Client Tools only installation was selected, the **Client Components** screen shows.

Choose one of these options to continue.

1.6.2.6 License Configuration

License Configuration

The License Configuration page displays only when the K2 Server is being installed. To proceed with the installation from this page a License key must be obtained for the regional support centre. See below for greater detail.



A Trial license cannot be used on a distributed installation, and is only valid for standalone installations.

K2 blackpearl Setup Manager

License Configuration

System Key:

License Key:

Key Request: <https://portal.k2.com/licensekey/Default.aspx>

Enter a valid license key to activate your installation. Navigate to <https://portal.k2.com/licensekey/Default.aspx> to request a key if one is not yet available to you.

i

System Key	The system key is generated at the time of installation and must be paired with a valid license key for the installation to be successful.
License Key	The License key is obtained directly from K2 Support. The URL provided on screen will enable the installer to request a license key.

The configuration cannot proceed unless a license key is available.

What to do on this page:

To obtain a license:

- Copy the System Key first
- Click on the URL provided on the License page (see above, below the License Key field). This will direct you to the K2 blackpearl site to request your license key

To license your copy of the K2 blackpearl platform:



If a license key is available, enter the license key



Click **Next**



If the license key is valid, the installation will proceed

If the license key is *invalid*, or a license key is *not available* the wizard will prevent the installation from proceeding

Developer License details

The following are important considerations that applies to the Developer license:

- Each K2 blackpearl Production Server License allows for unlimited installations of K2 blackpearl Development Servers for non-production use only.
- K2 blackpearl Development Servers may not run as a Windows Service and can only be operated in console mode.
- K2 blackpearl Development Servers are limited to Single Server installations.
- Development Server licenses can be requested on the K2 Customer Portal (<https://portal.k2.com/downloads/bp/default.aspx>)



K2 blackpearl Development Servers may not run as a Windows Service and can only be operated in console mode.

Console Mode has the following limitations and performance implications for all Development Servers:

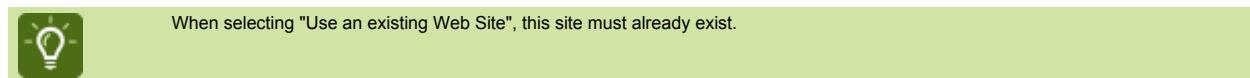
- Requires Local Login
- Single-threaded Execution only
- Single CPU only (multiple processor use is disabled)

1.6.2.7 K2 Workspace Web Site Configuration

K2 Workspace Web Site Configuration for a custom installation

The K2 Workspace Web Site Configuration screen enables:

1. The selection of a web site cluster if applicable
2. The creation of the K2 Workspace Site
3. The ability to select an existing site if one exists
4. If multiple IIS bindings are used, the installer will allow the user to select one



K2 blackpearl Setup Manager

K2 Workspace Web Site Configuration

Create a new Web site

Web site name:

Use an existing Web site

Web site name:

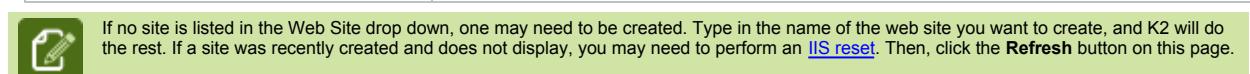
User Name:

Password:

Specify the settings of the Web site used for K2 Workspace. Enter the credentials that K2 should use for the K2 Workspace Application Pool, K2 Administrator Account and the K2 Service Account.

This Setup Manager screen will only show during custom installs and installs over a distributed network. During a Simple Full install, the option of entering a Web site Cluster will not appear.

Feature	Description
Create a New Web Site	If the user wants to create a new site, type the name in the Web Site Name field, and K2 will create it automatically.
Use an Existing Web Site Name	The name of the site that was created under IIS . Note: The site can be created without closing the K2 Setup Manager. Click Refresh to reload the list of available web site options.
Test the User Account credentials	To test the username / password combination, click the Test button.



What to do on this page

1. If the Workspace web site is going to be installed over a load balanced environment, enter load balanced URL here.

To configure the K2 Workspace Web Site:

Option 1- Create a new web site:



- 1 Enter the name for the New web site
- 2 Click **Next** to proceed
- 3 The Setup Manager will create the new Web site

Option 2 - Use an existing Web site



- 1 Select the web site to use from the Web Site drop down menu
- 2 Click **Next** to proceed

1.6.2.8 CRM Configuration

CRM Configuration

The CRM Configuration screen allows a user to add the details of the CRM Server and the Organizations name. The CRM server details entered on this screen are used to create the Environment Library entry that can be used within the K2 wizards. This screen is optional and the installation will complete without any information being entered on the screen.

Ensure that the Microsoft CRM Server is started before adding the information to this screen. CRM integration in K2 such as the CRM Entity Wizard is dependent on the information entered on this screen.



- The CRM Service Instance needs to be created manually using the CRM Server Connections Settings page available in Central Administration under K2 for SharePoint > Data Management.
- If the CRM Service Settings screen is left blank during installation it can be configured at a later time by running the Reconfigure option in the K2 Setup Manager.

As of K2 4.6.2 support has been added for CRM 2011. During installation or upgrade if the CRM configuration is enabled and CRM 2011 is selected the installer will switch the K2 Server to run on the .NET 4 Framework. If CRM 4 is selected then the K2 Server will continue to run on .NET 3.5 SP1. In an environment that is running a Farm it will be necessary to check that all the servers can be switched to run on the .NET 4 Framework.

K2 blackpearl Setup Manager

CRM Configuration

Enable CRM Integration

CRM Version:

Server URL:

Organization:

Enable CRM Integration to interact with CRM entities in K2 projects. Specify the CRM server URL and Organization.

What to do on this page

To configure the CRM Server:

- 1
- 2
- 3

Select which version of CRM server to use with the drop-down box. Either CRM4 or CRM 2011.

Type the CRM Server URL that can be obtained from the main page of the Microsoft CRM Service.

Add your organizations name as it appears in the CRM Service.



Use the **Test** button to check the entered data.



Click **Next** to continue.

1.6.2.9 Exchange Server Configuration

Exchange Server Configuration

The installer uses Exchange Autodiscover to pre-populate the required Exchange server settings. If Autodiscover is not enabled on the Exchange server, you must manually configure the settings. It is recommended that Autodiscover be available in your environment prior to installation. Autodiscover is used before making a call to Exchange. This allows one of the Exchange server nodes in the farm to switch dynamically and K2 features dependent on Exchange will continue to work. The K2 Service Account's email address is always used for the discovery process. Using the Autodiscover service to find the most appropriate URL for the specified user's mailbox instead of using a hard-coded EWS URL means that your workflow always uses the correct EWS URL for that particular mailbox. Autodiscover determines the best endpoint for a particular user (the endpoint that is closest to the user's Mailbox server).

Online: Exchange Online always has Autodiscover available, see <http://msdn.microsoft.com/en-us/library/exchange/gg194011%28v=exchg.140%29.aspx> for further information. During the setup you are asked for an email address and password of one of the online accounts. This account is used for the discovery process and to reply to SmartActions. **Recommendation:** Use the K2 Service email account in Active Directory as the Online account. Note that the Exchange Online integration only uses Static credentials for all interaction with Exchange. RunAs does not apply when configuring for Exchange Online. For Exchange Online, the static account that is configured during the installation needs to be part of the "Organizational Management" role group in Exchange for the analysis to be performed.

For Exchange Services (Meetings, Tasks, Mailboxes) for Online Integration the following rights are required:

- K2HostServer (Service) Account needs "ApplicationImpersonation" rights on Exchange Online.
- For Enable/Disable mailbox the static account used to install with needs to be part of the "Organizational Management" or "Recipient Management" role group; or create the account as a "Global Administrator" in Exchange Online.



The following Exchange Metadata Service methods are not supported for Exchange Online: Get Available Exchange Servers, Get Available Storage Groups, and Get Available Mailbox Databases

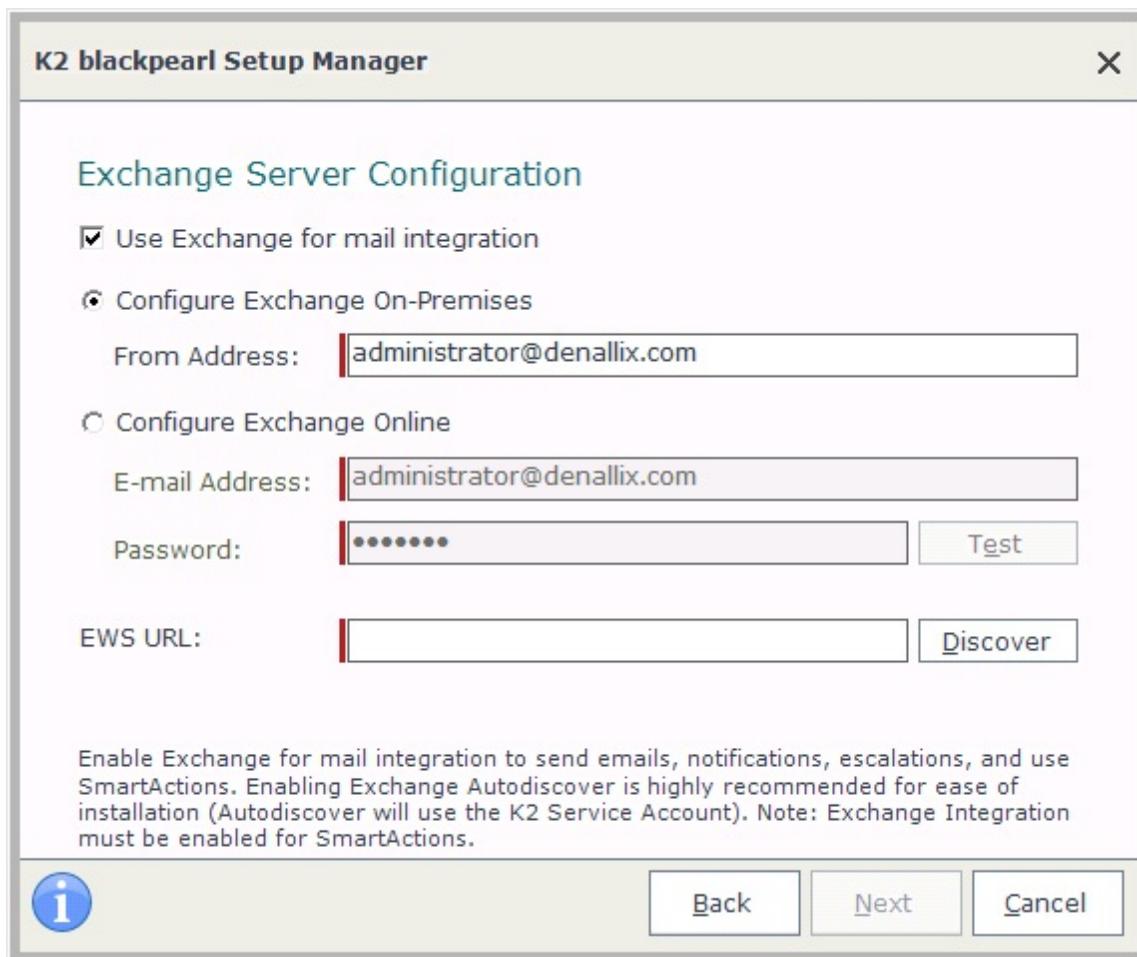
Autodiscover provides the following values required by the K2 Setup Manager:

- EWS URL
- TLS encryption setting
- SMTP Server
- Port

This page configures the Microsoft Exchange Server to be used in K2 workflows. In this screen, select whether or not your environment requires Exchange Integration. Selecting the Use Exchange for mail integration will configure the following functionality:

- K2 SmartActions
- Exchange wizards in all the K2 designers
- Registering the Exchange Service Instance
- Creation of Exchange SmartObjects

The EWS URL is a required field that can be discovered by clicking the Discover button or the URL can be typed in the text field and subsequently verified by clicking the Test button.



K2 blackpearl Setup Manager

Exchange Server Configuration

Use Exchange for mail integration

Configure Exchange On-Premises

From Address:

Configure Exchange Online

E-mail Address:

Password:

EWS URL:

Enable Exchange for mail integration to send emails, notifications, escalations, and use SmartActions. Enabling Exchange Autodiscover is highly recommended for ease of installation (Autodiscover will use the K2 Service Account). Note: Exchange Integration must be enabled for SmartActions.



Feature	Description
Use Exchange for mail integration	Enables the use of an Exchange server within the K2 environment - for K2 SmartActions, the Exchange wizards in all the K2 designers, as well as the associated Exchange SmartObject Service Instances and SmartObjects.
Configure Exchange On-premises	Configures the K2 environment to use a local Exchange On-premises server.
From Address	A unique e-mail address and mailbox dedicated for use by the K2 Server only
Configure Exchange Online	Configures the K2 environment to use the internet based Exchange Online server.
Email Address	The email address to be used to access the Exchange server.
Password	The password of the email address to be used to access the Exchange server.
Test	Use the Test Button to test the connection to the Exchange server.
EWS URL	The default Exchange Web Service URL for the selected Exchange server. Click the Discover button to automatically discover the URL or type the URL in the text field and verify it by clicking the Test button.

What to do on this page

To configure the Exchange Server details:



Enable the Use Exchange for mail integration check box or click **Next** to continue.



2 Select to either use Exchange On-premises (a Microsoft Exchange Server on your local server or network), or to use Exchange online.

3 Enter the Email Address and Password of the account to be used for Exchange integration with K2.

4 Click the Discover button next to EWS URL to automatically discover the URL or type the URL in the text field and verify it by clicking the Test button.

5 Click **Next** to proceed

1.6.2.10 Exchange Integration

Exchange Integration

This screen is reliant on the “Use Exchange for mail integration” checkbox being selected on the first Exchange panel in the Setup Manager. If Autodiscover is enabled it is used to discover the required settings.

Exchange Server prerequisites

K2 requires that Microsoft Exchange 2007 Management Tools SP2 or SP3 be installed if a Microsoft Exchange 2007 server is being used.

If Microsoft Exchange 2010 or Microsoft Exchange 2013 is being used, Windows Powershell 2 and WinRM (Windows Remote Management) are required by K2.

The reason for these software prerequisites is to allow the K2 server to examine the users Exchange server for database and other details. The Exchange Server Configuration panel in the K2 Setup Manager is populated with the user's Exchange server details if Exchange integration is enabled.

The K2 Setup Manager automatically detects the Exchange server settings using the Microsoft Exchange Management Tools (Exchange server 2007) or Windows Remote Management (Exchange Server 2010 or Microsoft Exchange Server 2013) and pre-populates the integration screen for new installations. If the prerequisite software is not detected or the installation is an upgrade, the screen is not displayed.

The Exchange Server Configuration separates common Exchange activities, such as creating calendar items and meeting requests, from administrative tasks. Different Exchange permissions are required for each, however the installation account must have the following rights if one or both options are chosen so it can browse for Exchange servers, storage groups and mailbox databases:

- For Exchange 2010, the installation account must be a member of the View-Only Organization Management group in AD.
- For Exchange 2007, the installation account must be part of the View-Only Administrator role in Exchange.

Standard Exchange Integration

If the standard integration is chosen, the Exchange Management service instance is the service that performs the common Exchange functions and requires impersonation capabilities in Exchange. When used in a wizard, this service executes using the credentials as configured in the Run As dialog for the event, or as the K2 Server Service Account if no credentials are configured. When used directly in a SmartObject call, the context is the current user's credentials. In conjunction with the Exchange Management service instance, the Exchange Meta Data service instance is used by the SmartObjects and the K2 Designer for SharePoint. This service executes under the identity of the K2 Server Service account. The authentication method can be changed in the K2 Management Console and, if changed, may require some additional Exchange and/or Kerberos configuration.

- For Exchange 2010, the user performing these actions must be part of the ApplicationImpersonation Exchange role.
- For Exchange 2007, the user performing these actions must have Exchange Impersonation rights. Important: In Exchange 2007, you cannot specify the same account for standard and administrative tasks.

For Exchange Services (Meetings, Tasks, Mailboxes) for Online Integration the following rights are required:

- K2HostServer (Service) Account needs “ApplicationImpersonation” rights
- For Enable/Disable mailbox the static account used to install with needs to be part of the “Organizational Management” or “Recipient Management” role group; or create the account as a “Global Administrator” in Exchange Online.

Administrative Exchange Integration

If the administrative integration is chosen, the Exchange Administration service instance is the service that performs the mailbox functions, specifically enabling and disabling mailboxes. The identity used for this service requires additional permissions in Exchange.

- For Exchange 2010, the user needs to be a member of the Recipient Management or Organization Management group in AD and have Execute rights on Microsoft.PowerShell.
- For Exchange 2007, the user needs to be a member of the Exchange Organization Administrators role in Exchange. Important: In Exchange 2007, you cannot specify the same account for standard and administrative tasks.

Depending on what you've chosen on this screen, the appropriate service instances will be created with the information specified. An environment library field for the Exchange server will also be configured.



Ensure that the Microsoft Exchange Server Service is running for the automatic detection of the information on this screen. Exchange integration in K2 is dependent on the information specified on this screen.
If the Exchange integration is not enabled, it can be configured at a later time by running the Reconfigure option in the K2 Setup Manager.

This screen is optional and does not need to be completed for the installation to complete. The following logic applies

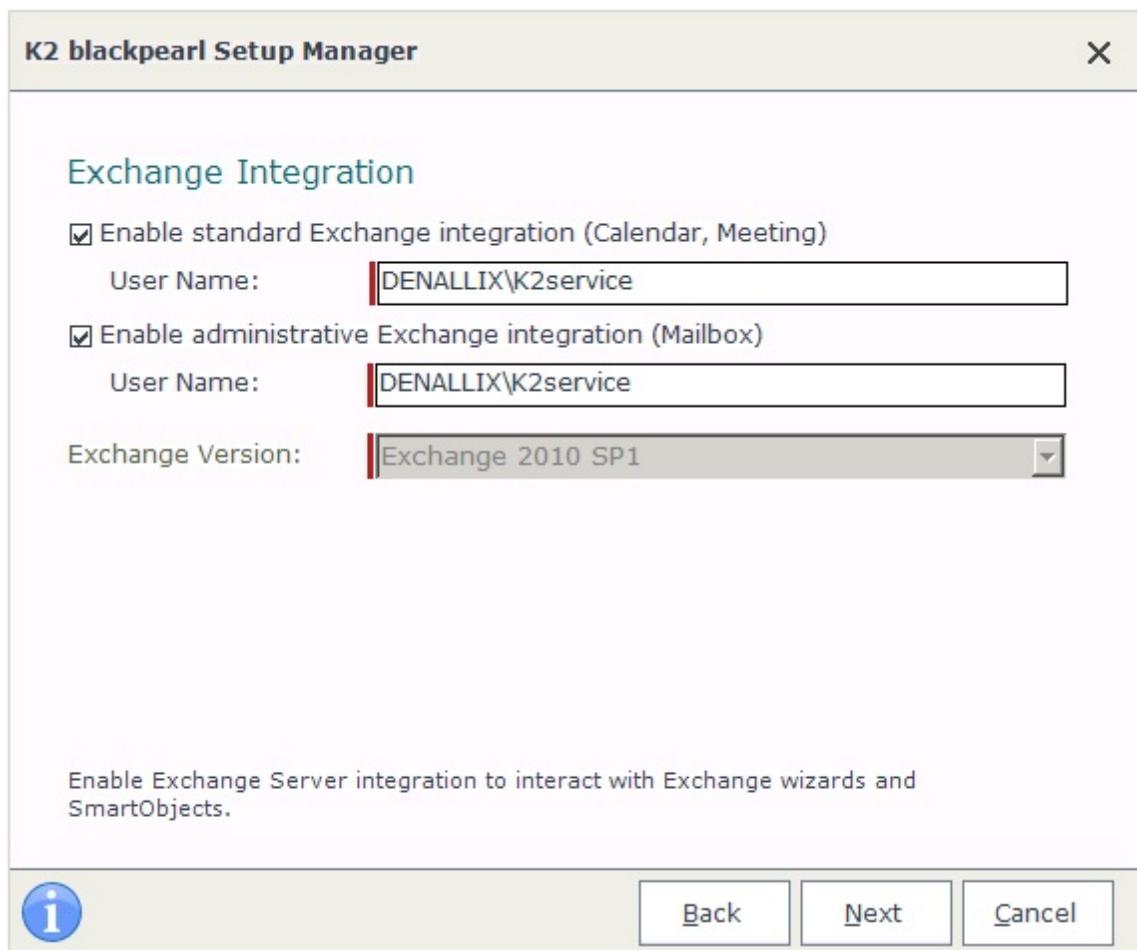
when selecting *Configure Exchange On-premises* or *Configure Exchange Online* on the Exchange Server Configuration screen:

If On-premises

- Selecting the *Enable administrative Exchange Integration (Mailbox)* option will create or enable the mailbox
- Deselecting the *Enable administrative Exchange Integration (Mailbox)* option will disable the mailbox

If Online

- Selecting the *Enable administrative Exchange Integration (Mailbox)* option will remove or restore access to a mailbox
- Deselecting the *Enable administrative Exchange Integration (Mailbox)* option will not allow the Exchange wizard to remove or restore access to a mailbox



Feature	Description
Enable standard Exchange Integration (Calendar, Meeting)	Used to enable Microsoft Exchange integration to interact with Appointments, Meetings and Tasks. This allows K2 to send calendar appointments and meeting requests under the specified credentials.
Enable administrative Exchange integration (Mailbox)	Used to enable Microsoft Exchange integration to enable and disable mailboxes. This allows K2 to create a mailbox under the specified credentials.
Exchange Version	Displays the Microsoft Exchange Servers discovered by autodiscovery and/or the DNS MX record.
Storage Group	(Exchange 2007 only) The first storage group available on the selected Microsoft Exchange server. This can be changed if required.

What to do on this page

To configure the Exchange Server Settings:



- 1 Tick either of the checkboxes **Enable Standard** or **Administrative Exchange Integration**. Otherwise click **Next** to skip this step.
- 2 Select the Microsoft Exchange Server name from the drop down list.
- 3 Ensure that the Storage Group name is correctly populated. (Exchange 2007 only)
- 4 Click the **Next** button to continue.

1.6.2.11 K2 SmartActions Installation

SmartActions incoming e-mail configuration



Incoming e-mails to the SmartActions mailbox are defined as those sent by a user to action a task or get help.

The SmartActions incoming e-mail configuration panel is enabled by default but configured as an optional component if the SmartActions feature is not required. For SmartActions to function the main consideration is the availability of a dedicated e-mail account and for the mailbox to be accessible by the K2 Server. It is recommended that the person performing the install see the topic **K2 SmartAction Pre-installation**.

To complete this step in the installation the following items are required.

- **Exchange Server:** Microsoft Exchange Server with Autodiscover and Exchange Web Services (EWS)
- **Unique E-mail Account:** The account details of a separate account to be used instead of the K2 Service Account

If the Exchange Server has Autodiscovery enabled, then selecting the Enable SmartActions for Exchange check box will populate the required fields using the Autodiscover service. If the Exchange Server does not have Autodiscovery enabled then these fields must be entered manually.



The account specified should fulfil the following requirements

1. The account must **NOT** be a personal e-mail account
2. Should only be an administrative account and dedicated for use by K2 SmartActions

K2 blackpearl Setup Manager

SmartActions Configuration

Enable SmartActions for Exchange

Use K2 Service account (DENALLIX\Administrator)

Use specified account

User Name:

Password:

E-mail address:

It is required that the e-mail address used to send and receive SmartAction messages is a dedicated address used only for SmartActions.

Enable SmartActions to action tasks via e-mail. Use the service account or specify a different account. For Exchange Online a different account cannot be specified.



If SmartActions for Exchange is enabled, once the details have been entered and the Next button is clicked, the following warning panel is shown:

Warning

The selected Exchange server and e-mail address will update the Outgoing SMTP Server and E-mail From Address. Would you like to continue?

Yes**No**

During a fresh (first time) installation, clicking the Yes button here will overwrite the SMTP and e-mail From Address details entered at the Outgoing E-mail screen. If **upgrading** K2 blackpearl, the details entered on the SmartActions Configuration page will not overwrite the SMTP and e-mail From Address details entered at the Outgoing E-mail screen.



Please contact K2 Support if the install is a first-time installation and different SMTP and E-mail From Address is needed for SmartActions.

Incoming E-mail Configuration**Enable SmartActions For Exchange**

Disabled by default. K2 SmartActions requires a dedicated e-mail address for incoming messages. This panel uses Autodiscover to find one or more Exchange servers, and also uses Autodiscover to find the (EWS) URL for retrieving the e-mail address and mailbox details for the specified user.



If the **Exchange Server** field is empty but the user knows there is an Exchange 2010 server, either Powershell 2 or WinRM are missing and should be installed first (as mentioned in the Software Integration section).

Use K2 Service account

Utilizing this option will extract the K2 Service Account details from Active Directory including the e-mail address. Note: if no mail box has been setup and configured for the K2 Service Account one must be created.

Use specified account

The specified account is a separate account that the K2 Server will use to access the mail box and process incoming e-mails.

User name / password

The user name and password for the specified account. The account credentials can be tested with the **Test** button.

E-mail Address

The e-mail address associated with the account specified. This is the account that will send and receive SmartAction messages.

What to do on this page

To configure the SmartActions email:

- 1
- 2
- 3
- 4
- 5

Tick the checkbox Enable SmartActions for Exchange. Otherwise click **Next** to skip this step.

If Autodiscovery has been enabled, then all the required fields will be populated.

If your environment will not be using the K2 Service account then select the Use specified account and enter the user name and password combination.

Select the email address from the drop-down list pre-populated by the Autodiscover function.

Click the **Next** button to continue.



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.

1.6.2.12 SMTP Settings (outgoing mail)

SMTP Settings (outgoing mail)

This page configures the E-mail SMTP server to be used to send K2 related E-mail notifications. This screen will not be displayed when the *Use Exchange for mail integration* option has been selected on the Exchange Server Configuration screen.

K2 blackpearl Setup Manager

SMTP Settings (outgoing mail)

SMTP Server:

Port:

Use TLS encryption for connection

From Address:

Specify the outgoing e-mail SMTP server and from address.

i Back Next Cancel



For backwards compatibility considerations for future versions, the **From Address** specified above must be a unique e-mail address and mailbox dedicated for use by the K2 Server only!

Feature	Description
SMTP Server	The name of the physical server to send K2 related E-mails
Test	Use the Test Button to test the connection to the SMTP Server
Port	The TCP Port of the SMTP Server
Use TLS encryption for connection	Enables the use of Transport Layer Security (TLS) to encrypt communications with the SMTP Server
From Address	A unique e-mail address and mailbox dedicated for use by the K2 Server only

What to do on this page

To configure the SMTP E-Mail Server details:

- (1)
- (2)

Enter the physical machine name of the SMTP Server

Enter the address for the K2 Server e-mail account

Note: For backwards compatibility considerations for future versions, the **From Address**

specified here must be a unique e-mail address and mailbox dedicated for use by the K2 Server only!

Click **Next** to proceed



1.6.2.13 Configuration Summary



Once the Setup Manager starts the installation, the process CANNOT be stopped!

Configuration Summary

The Configuration Summary screen displays the details captured in the Setup Manager Wizard. Information contained in this summary should be scrutinized for accuracy.

K2 blackpearl Setup Manager

Configuration Summary

Item	Setting
Selected Components	
K2 Core	Install
K2 blackpearl Server	Install
K2 for Visual Studio Core	Install
K2 for Visual Studio 2010	Install
K2 Studio	Install
K2 Workspace	Install
K2 for SharePoint 2010	Install
K2 Designer for SharePoint 2010	Install
K2 blackpearl Setup Manager	Install
License Configuration	

Review the configuration settings to ensure they are correct. Click 'Next' to have the settings applied or 'Back' to make changes.

i Print Copy Back Next Cancel

Feature	Description
Print	Allows you to print your configuration settings. This can be a useful record of the configuration details.
Back	Navigate in reverse order through the wizard user pages to make changes
Install	Click Install to proceed with the installation. Once this option is selected the installation cannot be stopped.
Cancel	Cancel the current installation session

What to do on this page

To make changes:

- 1 Click **Back** to navigate in reverse order through the Setup Wizard pages to locate the page that requires an update.
- 2 Make the change.
- 3 Click the **Next** button until the Configuration Summary page is displayed again.

Click **Back** to navigate in reverse order through the Setup Wizard pages to locate the page that requires an update.

Make the change.

Click the **Next** button until the Configuration Summary page is displayed again.



Click **Next** to proceed.

To Install:



Review the summary details to make sure the captured information is accurate.



Click **Next** to start the installation process

1.6.2.14 Additional Actions

Additional Actions

The Additional Actions screen displays the additional, required actions that needs to be performed, by clicking **Next** these actions will be performed by the K2 blackpearl Setup Manager before starting the installation process.

-  If there are any Updates that ship with the product the Update details will be displayed in the Actions window.
-  If the user clicks 'Next' then all listed actions will be done by the Setup Manager. Alternatively the user may elect to perform some of these actions at this point, and then click on 'Refresh' in which case the list will be refreshed to only contain the actions that are still required.

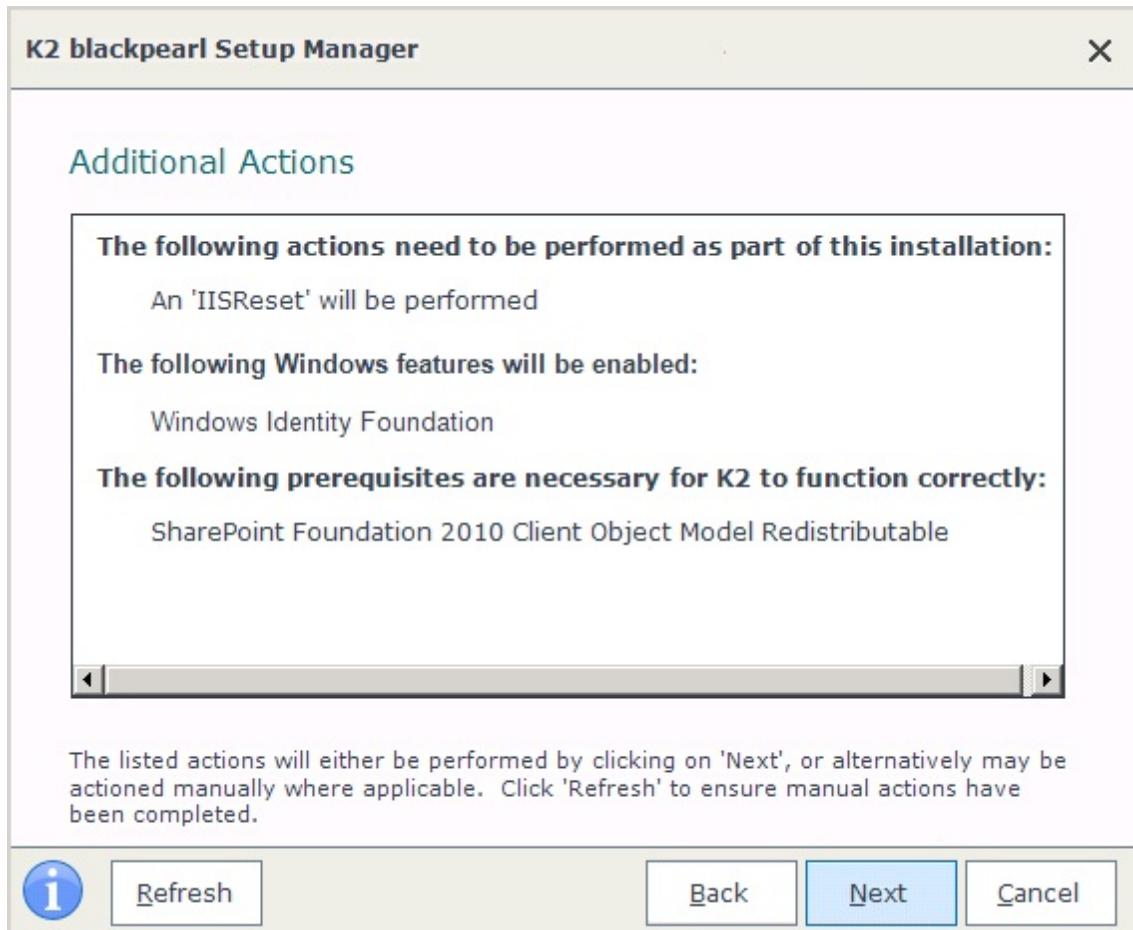
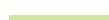


Figure 1: Simple Additional Actions Screen

Feature	Description
Refresh	Click 'Refresh' to ensure manual actions have been completed.
Back	Navigate in reverse order through the wizard user pages to make changes
Next	Click 'Next' to proceed with the installation. Once this option is selected all the listed actions will be performed by the Setup Manager. Note: The installation cannot be stopped after this button is clicked.
Cancel	Cancel the current installation session

What to do on this page

To make changes:





- Click **Back** to navigate in reverse order through the Setup Wizard pages to locate the page that requires an update
- Make the change
- Click the **Next** button until the Additional Actions page is displayed again

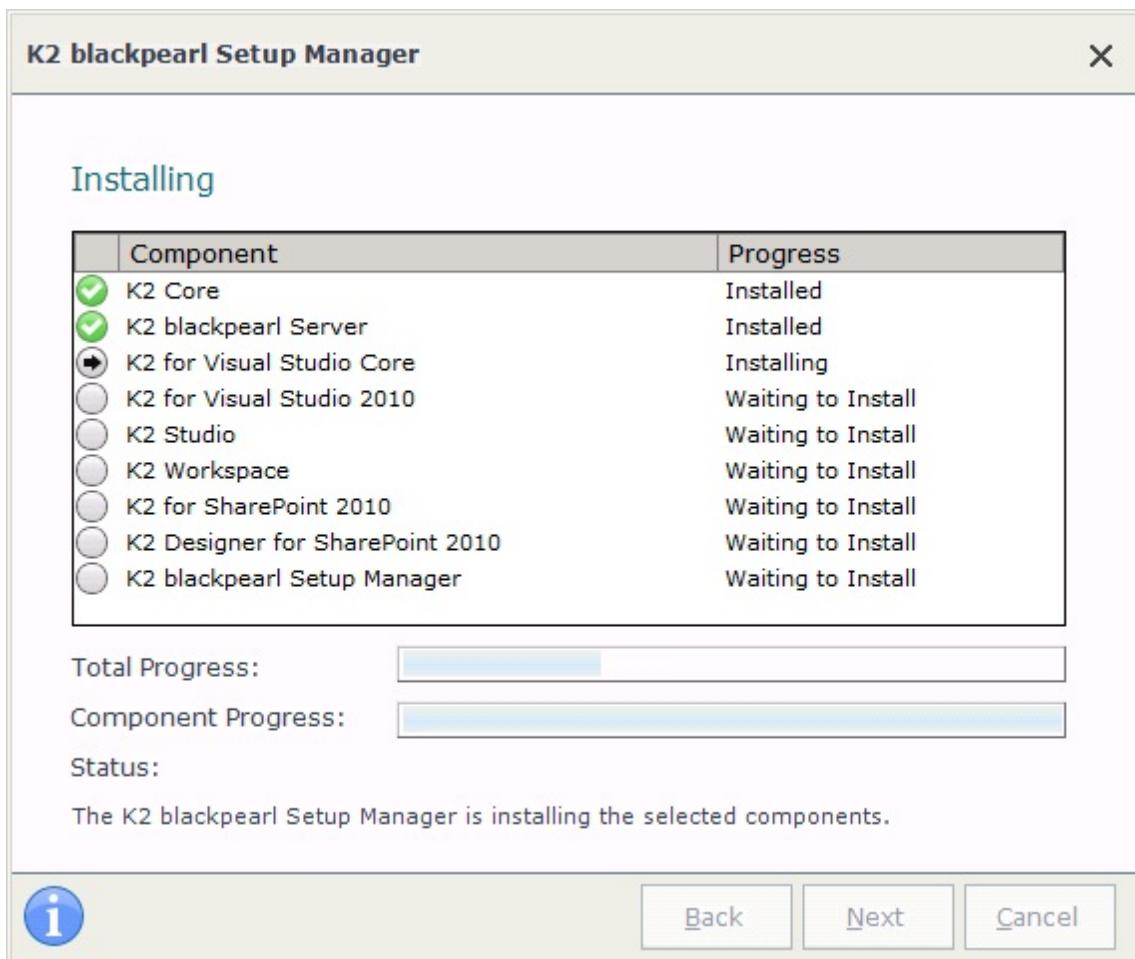
To Install:

- Review the **Additional Actions** details list
- Click **Next** to start the installation process. **Note:** All listed actions will be done by the Setup Manager after clicking on the 'Next' button

1.6.2.15 Installing Components

Installing Components

The Installing Components screen displays the status of the installation, with a progress bar for each component as well as an overall progress bar. The component progress bar indicates the progress of the individual component, whereas the Total Progress Indicator reports on the installation progress as a whole. Once the installation, ie the manual file copying process is complete the Setup Manager automatically proceeds with the configuration process.



What to do on this page

There is nothing to do on this page but to wait for the installation to complete.



Important: It is strongly advised that the installation is not interrupted for any reason. Interrupting the installation will cause file corruption and unpredictable results in your environment.

The Setup Manager will automatically start the Configuration process.

Installation Troubleshooting

Between the install progress and configure progress screens a warning pop-up message will display in case something failed during the install. This will prevent the application from continuing to the configuration process automatically. The user will be notified with a message similar to the following:

"At least one component failed to install properly. Click Yes if you wish to continue to configure the rest of the components, or No to inspect the install state for each component."

When clicking **Yes**, the Setup Manager will automatically continue configuring just those components that have been installed properly.

Clicking on **No** will let the user stay on the install progress screen. This way a user can look at all the components

and inspect which ones failed to install properly. The **Next / Configure** button will now be enabled so that the user can still proceed to configure components.

Configuration Status

The Configuration Status screen displays a progress bar for you to see which components have successfully been configured or are still being configured.

The screenshot shows the 'K2 blackpearl Setup Manager' window with the title 'Configuration Summary'. It contains a table with two columns: 'Item' and 'Setting'. The table lists 'Selected Components' and 'License Configuration'.

Item	Setting
Selected Components	
K2 Core	Install
K2 blackpearl Server	Install
K2 for Visual Studio Core	Install
K2 for Visual Studio 2010	Install
K2 Studio	Install
K2 Workspace	Install
K2 for SharePoint 2010	Install
K2 Designer for SharePoint 2010	Install
K2 blackpearl Setup Manager	Install
License Configuration	

Review the configuration settings to ensure they are correct. Click 'Next' to have the settings applied or 'Back' to make changes.

Buttons at the bottom: Print, Copy, Back, Next, Cancel.

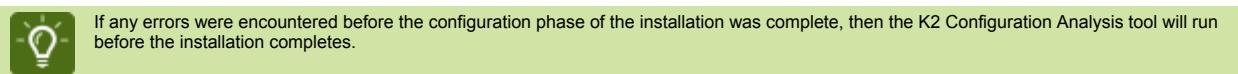
What to do on this page

There is nothing to do on this page but to wait for the configuration to complete.



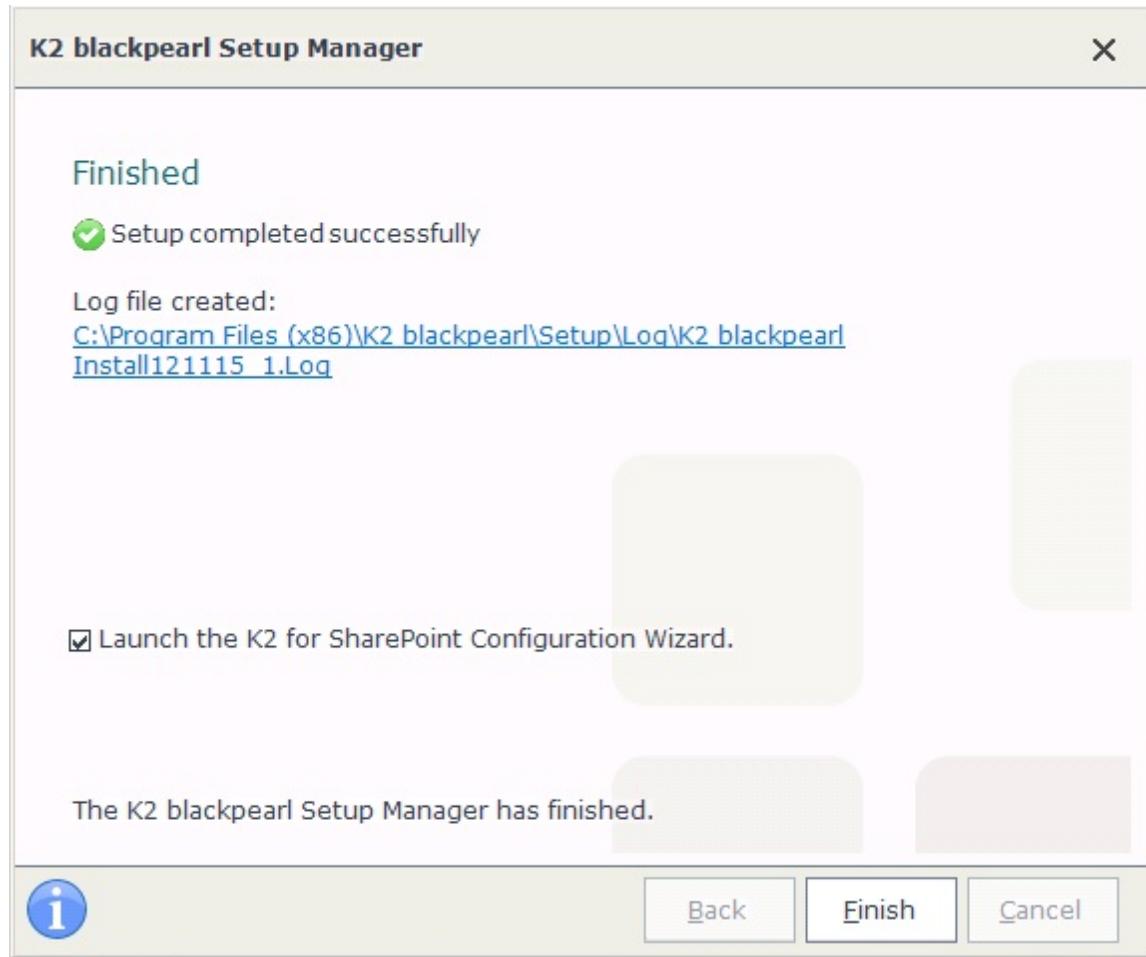
Important: It is strongly advised that the configuration is not interrupted for any reason. Interrupting the configuration will cause file corruption and unpredictable results in your environment.

1.6.2.16 Setup Manager Finished



Setup Manager Finished

This Finished page appears when the K2 Setup Manager is complete. There will be a link to the log file that was created. This log file can be helpful when troubleshooting issues in the K2 Environment. The next part of the installation is configuring SharePoint to use K2. The **K2 for SharePoint configuration Wizard** can be opened automatically by the Setup Manager provided the check box is selected. If the check box is not selected the K2 for SharePoint Configuration wizard must be initiated manually from the icon on the desktop in order to complete the installation.



What to do on this page

- 1
- 2

The user can select the checkbox to launch the **K2 for SharePoint Configuration Wizard** or deselect it and start the wizard at a later stage from SharePoint Central Administration.

Clicking the **Finish** button will finalize the installation process.



Tip: Once the installation is complete, it may be necessary to clear the Internet cache on the client machines for the new K2 components to be visible.

1.6.2.17 Client Tools Only install

A standalone system Client Tools Only install

The Client Tools Only option will only install the client tools on the local machine. The user can either select the **Simple Install (Client Tools Only)** option or the **Custom Install** option can be selected and then only select the *Client Components node* from the Select Components screen.

Before starting the installation there are prerequisites that need to be met. Details can be found at these links:

- Hardware
- Software
- Permissions for K2 components
- Pre configure environment



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

During Client Tools Only install:

- When choosing the Manually Configured Environment option, as long as all the settings are known beforehand, no special user rights are needed.
- If an Existing Environment is chosen, the user will need access to the database for the settings. See the [Installation Account](#) topic for details.
- During an upgrade, the same rules as stated above apply.

Installation steps

When the installation is started, the Setup Manager will run through the following steps:



On the **Welcome** screen, click **Next**

The Setup Manager will check for the **latest version** of K2 blackpearl.

The **End User License Agreement** needs to be agreed to before continuing.

The **Installation Type** screen allows the user to select either a Simple install or a Custom install. The Simple install allows for a Full install or Client Tools only install.

Selecting Client tools Only install and clicking next presents the **Client Components** screen where a choice concerning the installation environment needs to be made. Click the **Next** button to continue.

Existing environment

Configure the connection to the server hosting the K2 **database on this screen**.

Finally, review the **Configuration Summary** and click the Next button to install the Client Tools.

Manually configured environment

Enter all data necessary to configure the **K2 Server** on this screen then click the **Next** button to continue.

Note: No SQL connection is required.

Finally, review the **Configuration Summary** and click the Next button to install the Client Tools.

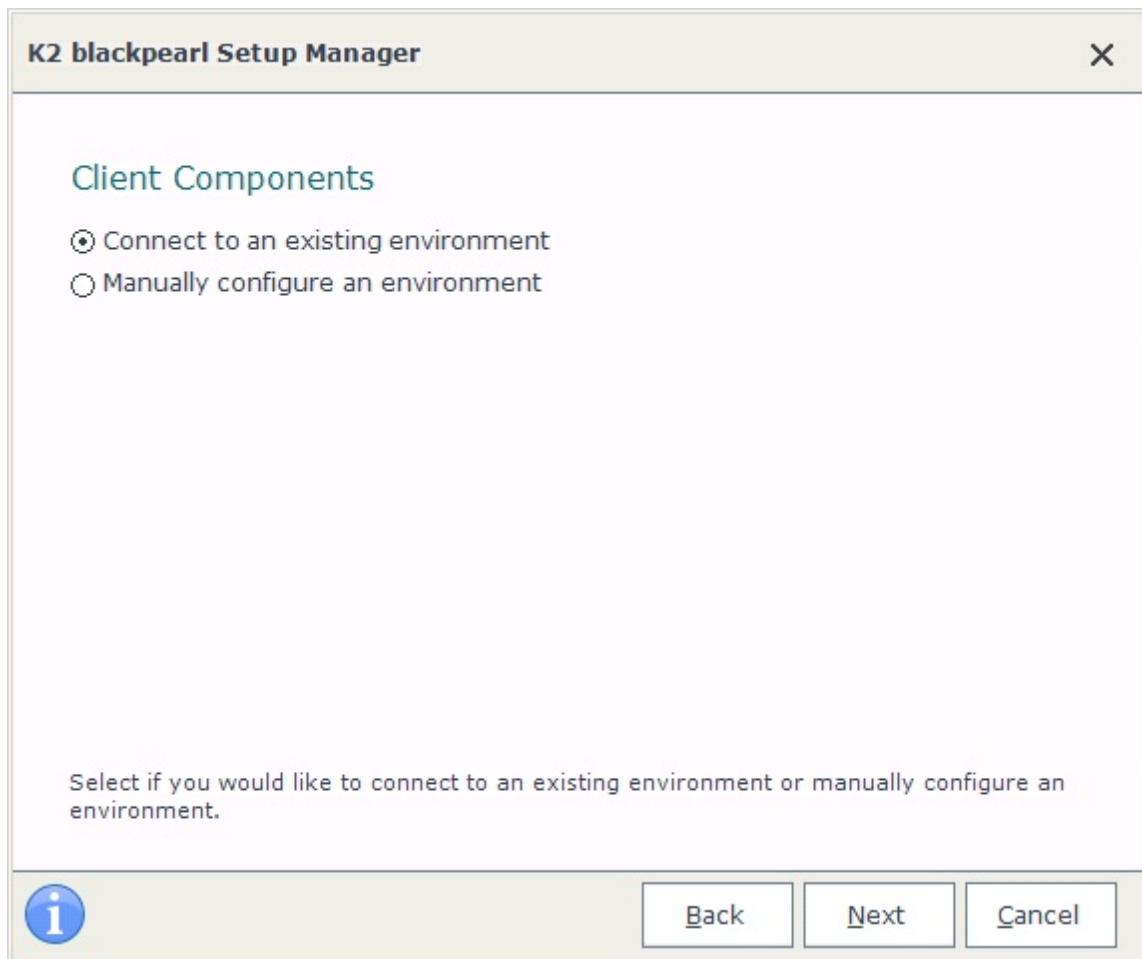
1.6.2.18 Client Components

Client Components

On the **Client Components** screen, the user is installing the K2 blackpearl Client Components only. Client Components are the various K2 blackpearl process designer technologies, for example K2 Designer for Studio. Since a designer does consume resources based on the target environment, the setup manager requires that it configures the designer for the current environment. Alternatively, the user installing the software can configure the designers integration with the current environment.



The environment refers to an Environment Library, which is used for storing all information about your various environments (such as server names, URLs, SharePoint Servers and sites) external to the process. This allows users to easily build the same process for any of the available environments configured without needing to rework the process by changing these common variables.



1. **Connect to an existing environment.** This allows the user installing the K2 Client Tools to select an existing HostServer Database to connect to. After clicking the **Next** button, the user will see the HostServer Database screen, where a connection to a database can be set up so its configuration information can be used. The server connection can be tested with the Test button. See the **HostServer Database** topic for detailed information.
2. **Manually configure an environment.** This allows the user to type in the K2 Server name to connect to. After clicking the **Next** button, the user will see the K2 Server Configuration screen, where you can type in a Server Name and the ports. See the **K2 Server Configuration** topic for details.

1.6.2.19 Host Server Database

Host Server Database Configuration

On the HostServer Database screen, type in the name of the SQL Server where the K2 databases are stored. This points the K2 for SharePoint component to the HostServer database set up by the K2 Server, to share configuration information. If you changed the Host Server database name, update it here and click **Next**.

K2 blackpearl Setup Manager

K2 Database

SQL Server: Server\Instance,Port

Database Name:

Windows Authentication
 SQL Authentication

User Name:

Password:

Enter the K2 database name and the SQL server where it resides.

i

Feature	Description
SQL Server	Populate the name of the SQL Server where the K2 Databases will be installed. Note: When a named instance has been used, provide that named instance here i.e. Sqlserver\Instance
Database Name	The default name of the HostServer Database is pre-populated here and can be altered. Note: The default names are recommended for ease of identification.

- ① The name of the Database server must populate the field labelled SQL Server (or named instance if a named instance has been used i.e. Sqlserver\Instace)

- The DataBase Name example **Host Server** will be populated automatically

Authentication:

The user page offers a choice in Authentication either Windows or SQL Authentication.

- If Windows Authentication is selected the credentials of the K2 Service Account will be used to authenticate the connection to the SQL Server.
- If SQL Authentication is selected, a connection string must be established to connect to the SQL Server

**For SQL Authentication Only:**

1. Enter the User Name and Password
2. Click Test to verify the connection to the database
3. If the test passes, proceed to **Step 4**
4. If not, the User Name and Password must be correct before the Setup Manager will allow the installation to proceed



Click **Next** to continue



If you make use of the SQL Server 2012 AlwaysOn solution, be sure to point to the correct SQL Server Always on Listener/Instance. For more information on this new comprehensive high availability and disaster recovery solution for SQL Server 2012, see the TechNet article [AlwaysOn FAQ for SQL Server 2012](http://technet.microsoft.com/en-us/sqlserver/gg508768.aspx) (<http://technet.microsoft.com/en-us/sqlserver/gg508768.aspx>)

1.6.2.20 K2 Server Configuration

K2 Server Configuration

The **K2 Server Configuration** screen allows the user to set ports, names and addresses of the server.

K2 blackpearl Setup Manager

K2 Server Configuration

Host Service Port:

Workflow Service Port:

Discovery Service Port:

Set K2 Host Server SPN
 Start the K2 blackpearl Service

SMTP Server:

From Address:

Specify the ports for Host Server and Workflow services, SPN and start options, and the outgoing e-mail SMTP server and from address.

i

Feature	Description
Host Service Port	Enter the Host Service Port Number (the default port is 5555)
Workflow Service Port	Enter the Workflow Service Port Number (the default port is 5252)
Set K2 Host Service SPN	Select this if you want the Installer to set the K2 Host Server SPN
Set K2 blackpearl Service	Select this if you want the K2 blackpearl Service to be automatically started
SMTP Server	Enter the SMTP Server to be used for e-mail deliveries
Test	Use the Test Button to test the connection to the SMTP Server

What to do on this page

To configure the K2 Server:



Select the appropriate K2 Server option for your installation scenario



Click **Next** to proceed



Recommendation: When the K2 Server is run in console mode make sure to be logged in as the correct user and make use of the "Run as Administrator" option to ensure that the correct elevated privileges are utilized.

1.6.2.21 Custom Install

Performing a Custom Install on a standalone system

The **Custom Installation** option can do either a standalone installation, or a distributed installation (depending on what the user specifies). This install allows a user to select specific components to be installed. Continue on this page for the standalone custom installation or see topic **Install a distributed environment** for details on performing a custom install on a distributed environment.



Please bear in mind that the list of steps below is based on all components being selected for installation. The user installing the system should ignore steps not related to their install.

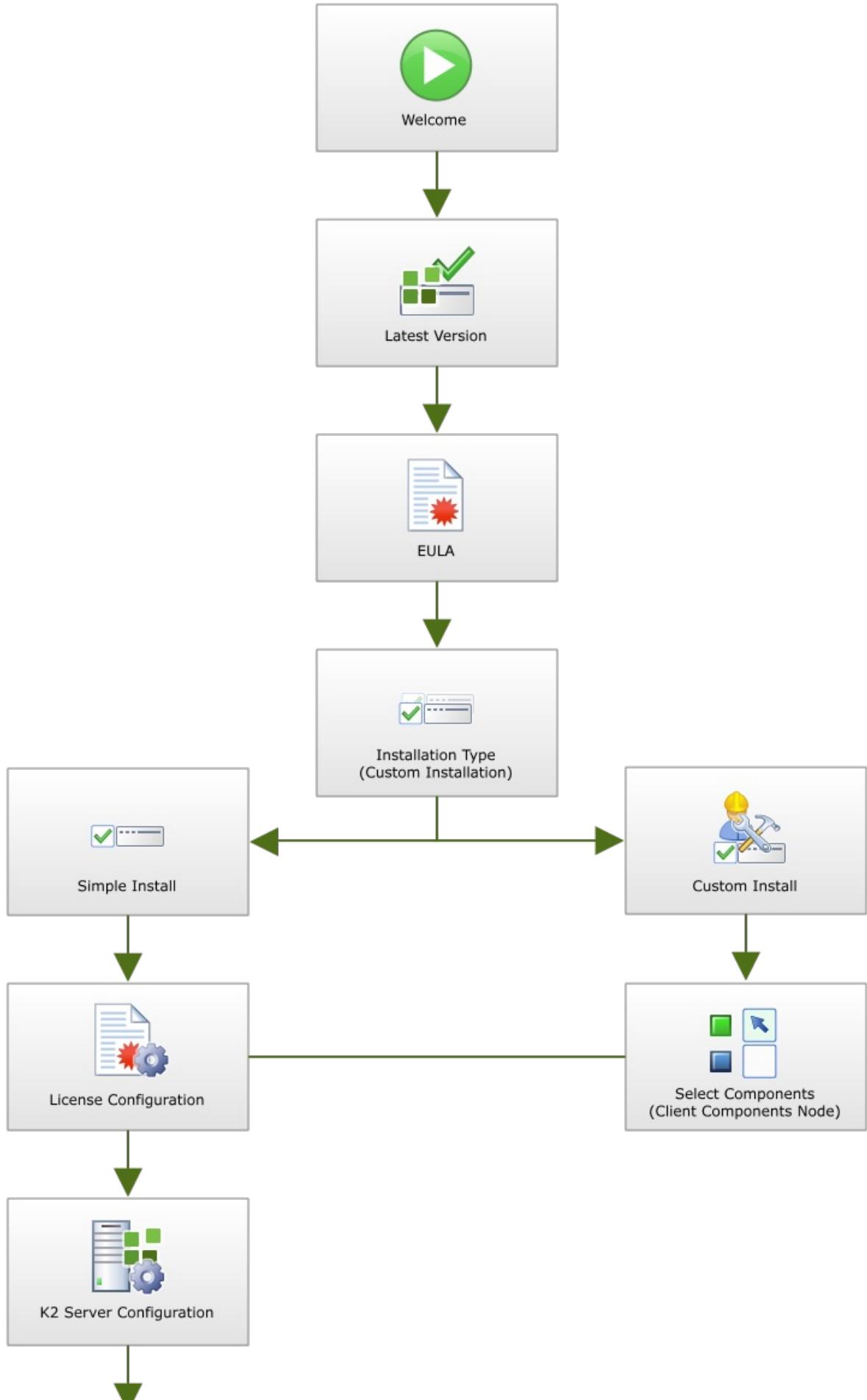
- 1 On the **Welcome** screen, click **Next**
- 2 The Setup Manager will check for the **latest version** of K2 blackpearl.
- 3 The **End User License Agreement** needs to be agreed to before continuing.
- 4 The **Installation Type** screen allows the user to select either a Simple install or a Custom install.
- 5 The **Select Components** screen enables the selection of either all or some of the components available in the K2 Platform.
- 6 On the **License Configuration** screen, the user must enter the license corresponding to the system key displayed.
- 7 Select the standalone option on the **K2 server configuration** screen and click the **Next** button. The K2 Server Farm option relates to installing on a distributed environment.
- 8 This step allows the user to set the **K2 Pass-through Authentication** for the K2 Server.
- 9 On the **K2 blackpearl Server Configuration** screen, take note of the ports that are used for communication.
- 10 This page also allows for the configuration of the E-mail server to be used to send K2 related E-mail notifications.
- 11 At this step the **K2 Workspace web site** must be configured.
- 12 Once the Workspace web site has been created or selected, the **Workspace application pool** must be configured.
- 13 Configure the **SQL Reporting Services** on this screen.
- 14 The next step is to configure the optional **CRM** server details.
- 15 Customize **K2 blackpearl database configurations** at this step if necessary.
- 16 On this screen, configure the **administrator and service accounts**.
- 17 If an Exchange Server is being used in the environment K2 is being installed to, it will be configured on the **Exchange Server Configuration screen**.
- 18 As with the previous step, if Exchange is being used, the **Exchange Integration screen** needs to be configured.
- 19 SmartActions are enabled by default and set up on the **SmartActions Configuration** screen.

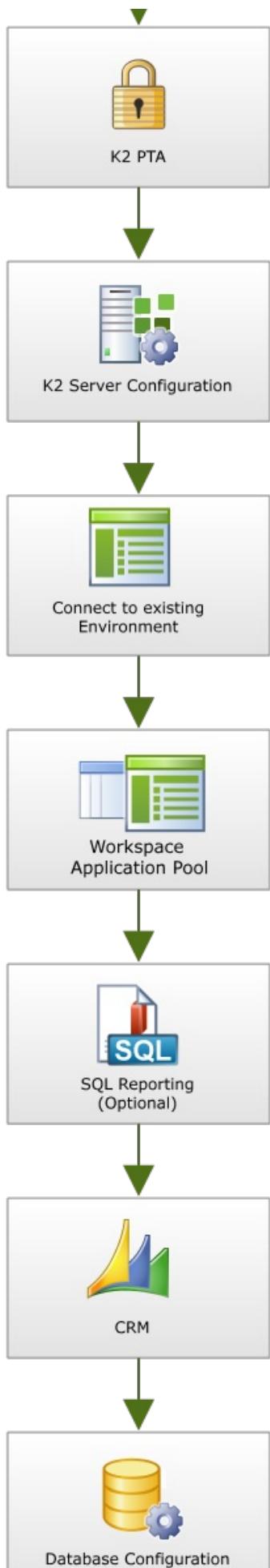
Note: The **SMTP Settings** screen is displayed after step 18 (SmartActions setup) only if the **Use Exchange for mail integration** option has been selected on the **Exchange Server Configuration** screen.

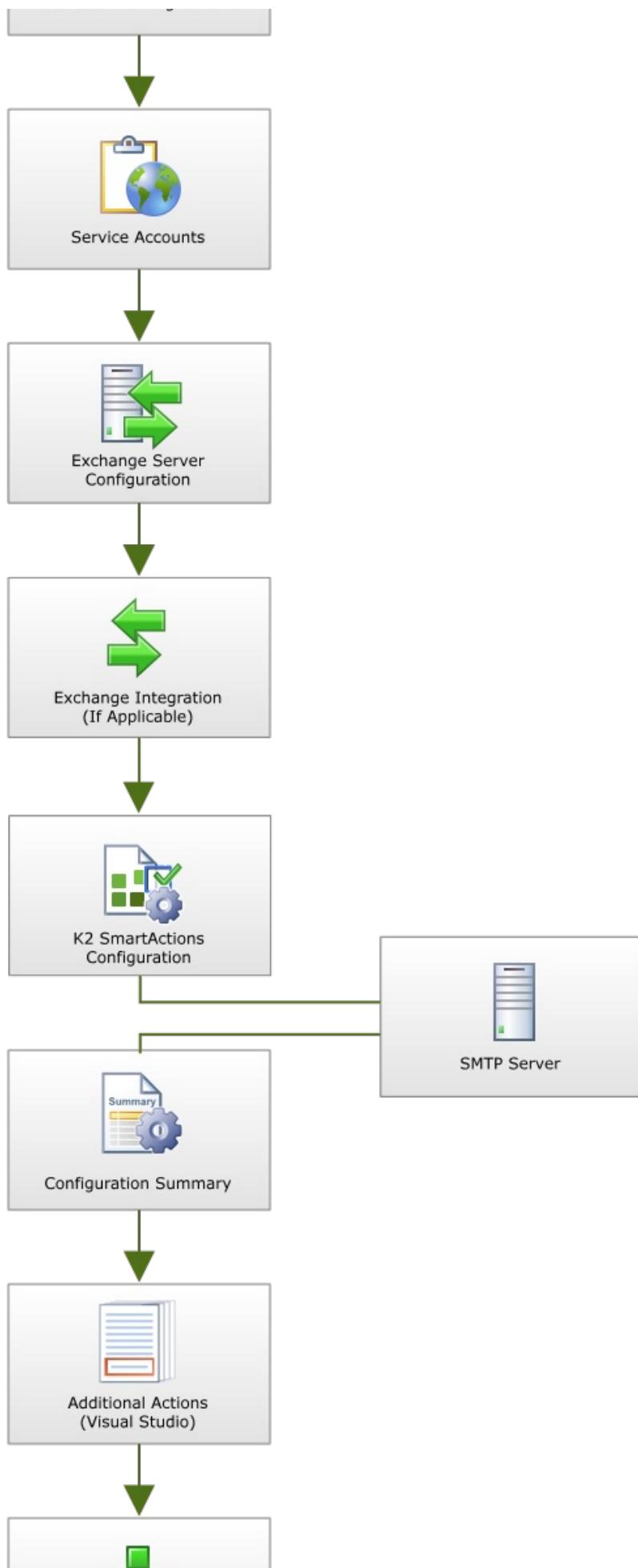


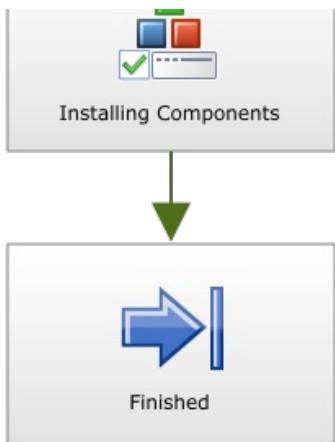
- Finally, the **Configuration Summary** screen will be shown where the installation can be reviewed.
- Before the install begins, the **Additional Actions** screen is displayed if there are any actions that need to be performed.
- The **Installing Components** screen displays the status of the installation and then displayed the Configuration Status screen.
- This **Finished** page appears when the K2 Setup Manager is complete.

1.6.2.21.1 Custom Installation Flow Diagram









1.6.2.21.2 K2 Database Configuration

Database Configuration

On the Database Configuration screen, type in the name of the SQL Server where you wish to install the K2 Databases. You may test the connection, configure Authentication, and then click on **Next** to continue.

K2 blackpearl Setup Manager

Database Configuration

Server Name:

Server\Instance,Port

Windows Authentication
 SQL Authentication

User Name:

Password:

The Local SQL server database configuration failed, enter the details of the SQL Server that will host the K2 database.



SQL Server Connection Details	
Server Name	Type in the name of the SQL Server where wish to install the K2 Databases (if a named instance is to be used, please provide that named instance here i.e. Sqlserver\Instance)
Test	Use the Test Button to test the connection to the SQL Server
Authentication	
Windows Authentication	Select this option if using Windows Authentication for connections to the SQL Server
SQL Authentication	Select this option if using SQL Authentication for connections to the SQL Server
User Name	Enter the required User Name if using SQL Authentication for connections to the SQL Server
Password	Enter the required Password if using SQL Authentication for connections to the SQL Server



If you make use of the SQL Server 2012 AlwaysOn solution, be sure to point to the correct SQL Server Always on Listener/Instance.
For more information on this new comprehensive high availability and disaster recovery solution for SQL Server 2012, see the TechNet article AlwaysOn FAQ for SQL Server 2012 (<http://technet.microsoft.com/en-us/sqlserver/gg508768.aspx>)

1.6.2.22 Select Components

Select Components



For a **Simple Installation** type, the Select components user page will only display if one or more of the required prerequisites are not met.

The Select Components screen enables the selection of either all or specific components available in the K2 Platform. Components that are not required can be disabled by removing the green check mark next to the component. Since each component plays a vital role in the K2 environment, disabling components for a standalone installation will reduce functionality. However, when installing a distributed installation installing components on independent machines enhances performance.

This page includes items that are required by default and cannot be removed from the [components](#) list. For example, the K2 blackpearl Setup Manager is required to be installed with all K2 components. Depending on the version of the software installed, components related to that version will be listed as can be seen in the image below.

K2 blackpearl Setup Manager

Select Components

Select the components that will be installed and configured on this computer.

i

Back **Next** **Cancel**

Select Components	
Check box	<ul style="list-style-type: none"> • Checking the check box next to a component enables the item to be installed • Removing the check mark from the box marks the component to not be installed and displays the red X



An item cannot be installed unless all the dependencies are already installed. You can click on the [Check Dependencies](#) link to see what other prerequisites are required before you can install the component. If you want to install a component that is missing some dependencies, cancel the installer and fix the dependencies. Then, restart the K2 blackpearl setup manager.

What to do on this page

The steps below provide details on how to complete this page:



Select the desired components to install. For a standalone installation, all of the components should be selected. The distributed installation guide will walk you through which components to install on which server role.



Click **Next** to proceed.

Note: You may be prompted to reset IIS before installing web components. Click **Yes** to continue with the installation.

- Check Dependencies

1.6.2.23 K2 Server Configuration

K2 Server Configuration

The **K2 Server Configuration** screen allows the user to set ports, names and addresses of the server.

K2 blackpearl Setup Manager

K2 Server Configuration

Host Service Port:

Workflow Service Port:

Discovery Service Port:

Set K2 Host Server SPN
 Start the K2 blackpearl Service

SMTP Server:

From Address:

Specify the ports for Host Server and Workflow services, SPN and start options, and the outgoing e-mail SMTP server and from address.



Feature	Description
Host Service Port	Enter the Host Service Port Number (the default port is 5555)
Workflow Service Port	Enter the Workflow Service Port Number (the default port is 5252)
Set K2 Host Service SPN	Select this if you want the Installer to set the K2 Host Server SPN
Set K2 blackpearl Service	Select this if you want the K2 blackpearl Service to be automatically started
SMTP Server	Enter the SMTP Server to be used for e-mail deliveries
Test	Use the Test Button to test the connection to the SMTP Server

What to do on this page

To configure the K2 Server:



Select the appropriate K2 Server option for your installation scenario



Click **Next** to proceed



Recommendation: When the K2 Server is run in console mode make sure to be logged in as the correct user and make use of the "Run as Administrator" option to ensure that the correct elevated privileges are utilized.

1.6.2.24 K2 Pass-Through Authentication

K2 Pass Through Authentication



The following user page will only appear when a K2 Server standalone installation is being performed. It appears between the two K2 Server Configuration User Pages.

K2 Pass-Through Authentication is configured during the installation of K2 blackpearl Server. The user page appears between the two K2 Server Configuration pages when installing the K2 Server. The default setting is Client Windows and this is intended for new installations where Kerberos has not yet been configured. If Kerberos has already been configured or will be configured then Client Kerberos should be selected.



Owing to the technical requirements of both installing either for Client Windows ie K2 Pass Through Authentication or Client Kerberos, it is strongly advised that the section on [K2 Pass-Through Authentication](#) be reviewed before a selection is made!



The Unattended installer panel functions in the opposite manner to the UI based installer as shown below. This is by design and further details can be found here:[K2 Pass-Through settings for Unattended Installer: Additional Notes](#)

K2 blackpearl Setup Manager

K2 Pass-Through Authentication

Windows: Reverts to Windows user tokens when Kerberos is not configured.
 Kerberos: Enforces the use of Kerberos/NTLM user tokens for authentication with K2 Server.

K2 Pass-Through Authentication options allow you to determine how user tokens are handled by the K2 Server. See the K2 Help for more information about these options.

 [Back](#) [Next](#) [Cancel](#)

Feature	Description
Windows	Also referred to as Client Windows ; this is the default installer option which facilitates the installation and configuration of the K2 Server to utilize K2 Pass-Through Authentication.
Kerberos	Also referred to as Client Kerberos ; this is the alternative option to Client Windows for installations that require the use of Kerberos

What to do on this page

To configure K2 Pass-Through Authentication:



Select the appropriate K2 Pass-Through Authentication option for your installation of K2 Server



Click **Next** to proceed

1.6.2.25 Workspace Application Pool Configuration

Workspace Application Pool Configuration

The **K2 Workspace Application Pool Configuration** screen enables the user to create a new Application Pool for the K2 Workspace web service. If an Application Pool does not already exist or a custom one is required, a new application pool can be created from the screen as shown below.

K2 blackpearl Setup Manager

K2 Workspace Application Pool Configuration

Use current Application Pool settings
 Use an existing Application Pool
 Update or create a new Application Pool

Application Pool:

Application Pool:

User Name:

Password:

Set K2 Workspace SPN

Use the existing Application Pool.



Feature	Description
Use an existing Application Pool	The name of the site that was created under IIS .
Update or Create a new Application Pool	If you want to create a new application pool, type the name in the Application Pool Name field, and K2 will create it automatically for you.
Application Pool	Enter the name of the Application Pool; a custom name can be entered or use the existing, DefaultAppPool
User	The fully qualified domain user account under which the Application Pool hosting the site is run.
Password	The password for the Service Account. Use the Test button to check the credentials.



If no application pool is listed in the Application Pool drop down, one may need to be created. Type in the name of the application pool you want to create, and K2 will do the rest. If an account was recently created and does not display, you may need to perform an [IIS reset](#). Then, click the **Refresh** button on this page.

What to do on this page

To configure the K2 Workspace Application Pool:

-  Select to use an existing Application Pool, or to create a new one
-  If the Existing Application Pool option was selected, click **Next** to continue or if you selected to create a new Application Pool proceed, to the next step
 1. Enter a name for the new application pool, or use the default
 2. Provide a User account that is preferable the same user account at the K2 Server service account
 3. Enter the password for the User Account provided
-  Enable or disable the Option to set the K2 Workspace Machine SPN
-  When prompted with the warning:
The Set K2 Workspace SPN option will reconfigure the SPN for this application pool if one has already been created. Do you wish to continue?
-  click **Yes**

Validate the K2 Workspace Application Pool

After installing and configuring the K2 Workspace Application Pool, you can check a few things to ensure that the Runtime Web Services was set up properly:

-  Open **IIS**
-  Expand the **Web sites** section
-  Expand the **Web site** that will be used to host the K2 Runtime Web Services
-  Right click on the RuntimeServices virtual directory and select **Properties**
-  Select the **Virtual Directory** tab
-  Confirm that the Local Path points to [INSTALLDIR]\Webservices\Runtimeservices (For Example: C:\K2 blackpearl\Webservices\Runtimeservices)

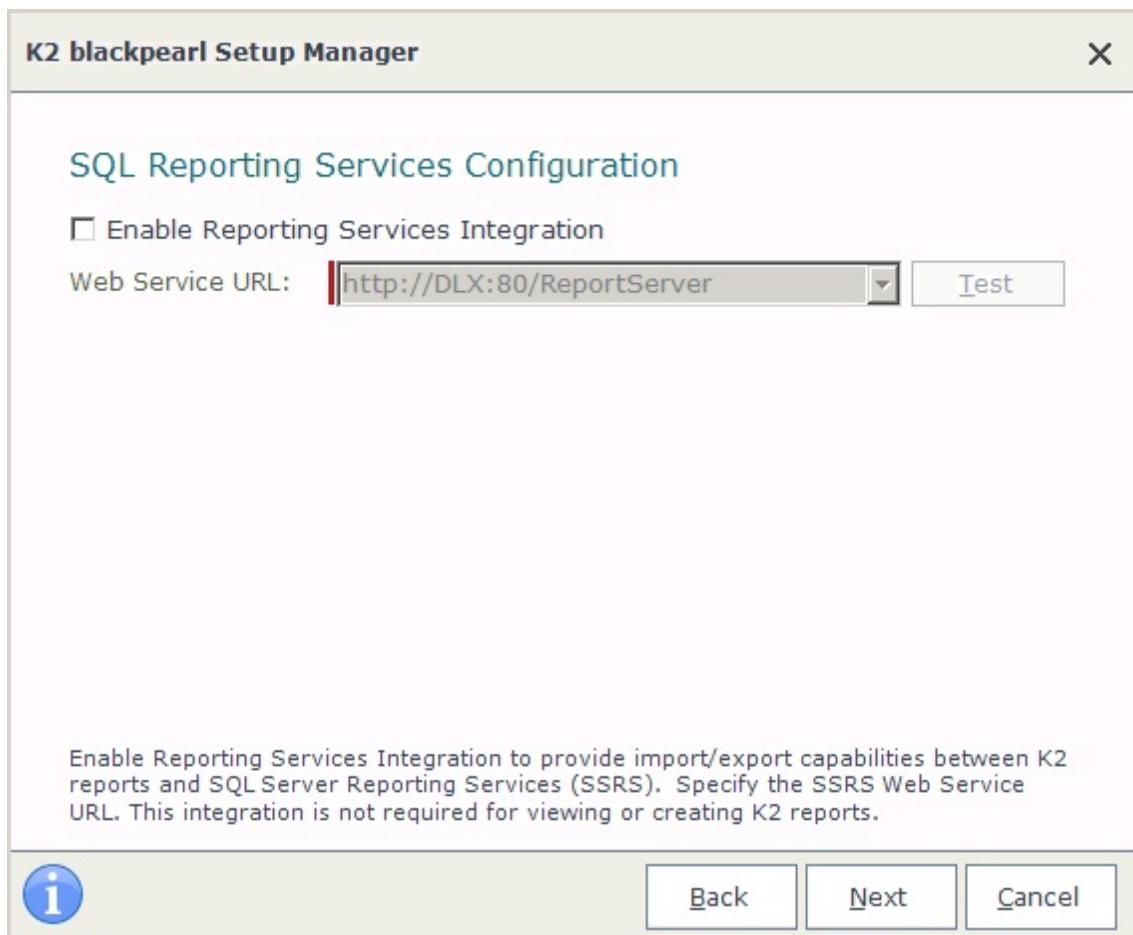


It is advised to test the K2 Runtime Web Services on a client machine as well. If InfoPath is used on a client machine, it is further advised to use NTLM authentication instead of Negotiate authentication when using IIS7.

1.6.2.26 SQL Reporting Services

SQL Reporting Services

The SQL Reporting Services Configuration screen sets up the environment for the K2 for Reporting Services component.



Feature	Description
Enable Reporting Services Integration	Enable Reporting Services Integration to provide import/export capabilities between K2 reports and SQL Server Reporting Services (SSRS). This integration is not required for viewing or creating K2 reports
Web Service URL	Add the Reporting Services web service URL
Test	Use the Test Button to test the connection to the SQL Server Reporting Services Web Server



Note: The K2 installer will try to connect to the SQL Reporting services web service URL provided during installation, if it cannot, the out-of-the-box reports will not be installed and the K2 Datasource will not be configured. However, the K2 Report Designer in K2 Workspace will still function for new custom reports.

What to do on this page

To configure the SQL Reporting Services details:

- 1 Add the Web Site URL
- 2 Click **Next** to proceed

In case of Connection Fail

If the message:

SQL Reporting Service Site

Connection Failed: This reporting service is running in SharePoint Integrated mode.

This is currently not supported for K2

Reporting components.

is displayed, please see the topic concerning the **Reporting Services Server** in the software by role prerequisites section.

1.6.2.27 Database Configurations

Database Configurations

The Database Configurations page lists all the K2 Databases and where they will be configured. At this point, the databases have not been created yet by the Setup manager. The connection details can be changed by clicking on the **Change** link in the connection column per database (which also allows you to rename the database), or by clicking the **Change All** button to make changes to all databases at once.

Database Name	SQL Server	Status	Connection
K2	DLX	Up to date	Change

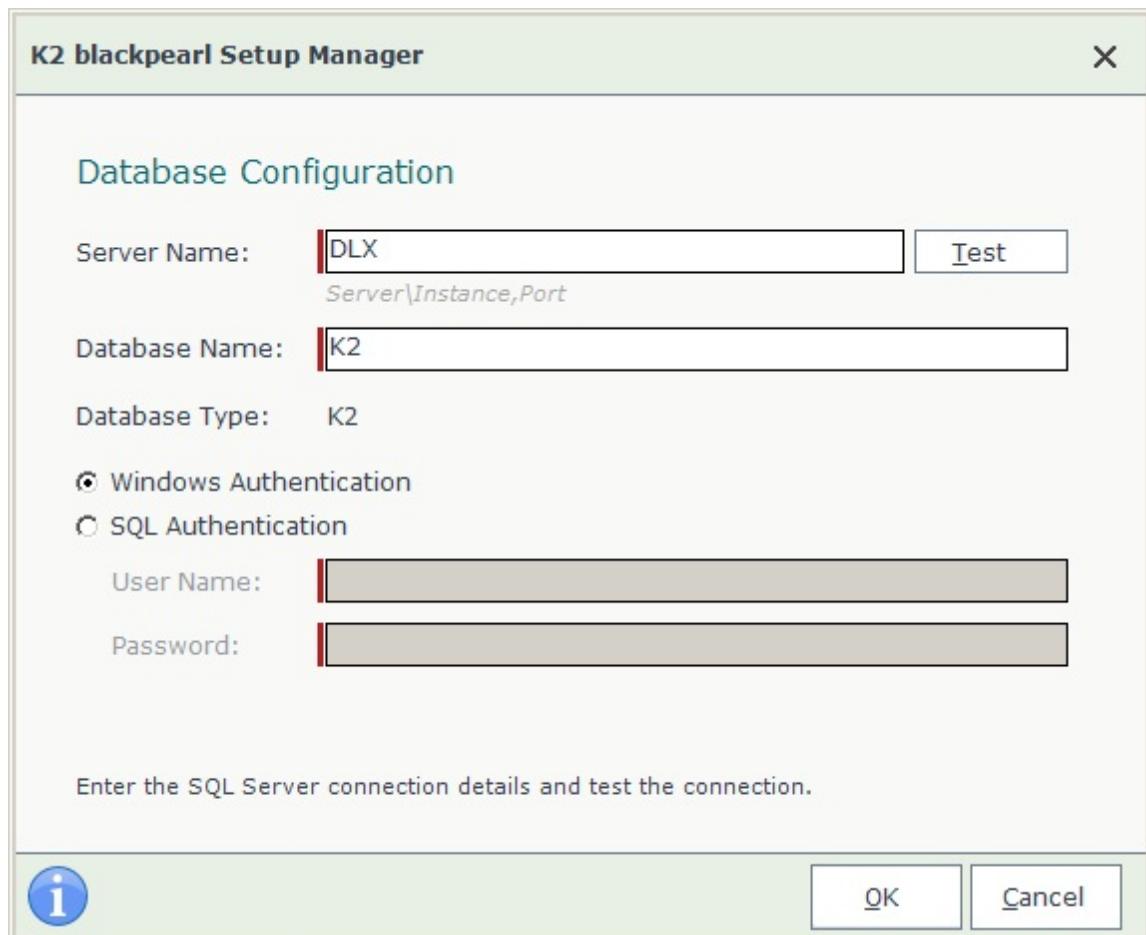
[Change All](#)

Click a "Change" link to customize a specific K2 blackpearl database connection. Click the "Change All" button to change all K2 blackpearl databases to use the same connection.

[Back](#) [Next](#) [Cancel](#)

Feature	Description
Database Name	The name of the K2 blackpearl database. These are system databases and therefore are pre-named. However, you can click the Change link and rename the database if desired.
SQL Server	The name of the SQL Server
Status	The database has been flagged for creation on the named server
Connection	The connection details can be changed by clicking on the Change link
Change All	Enables the changes made to be applied to all the databases listed

The SQL Server Connection Details screen allows you to change the SQL server on which to install the K2 Databases. If you selected to change a single database, you can change the name of the database to be created on this screen:



You can also specify either Windows Authentication or SQL Authentication .

Feature	Description
Server Name	This identifies the Machine name of the SQL Server
Windows Authentication	User rights to the [Server].[Database] are authenticated against Active Directory
Feature	Description
Server Name	This identifies the Machine name of the SQL Server
SQL Authentication	User rights to the [Server].[Database] are authenticated using SQL Authentication
User Name	Enter the name for the SQL Account that has been granted access to the K2 blackpearl databases.
Password	Enter the password for the SQL Account that has access to the databases for verification.

What to do on this page

To configure the Database Connections:

- 1 Click on the **Change** link or the **Change All** button
- 2 To change the SQL Server to install the K2 Databases to, enter the name of the SQL Server
 - To change a database name, enter the name for the database
 - To configure SQL Authentication, select the SQL Authentication option and enter the Account Name and Password
- 3 Click the **Test Database connection** button

Click on the **Change** link or the **Change All** button

- To change the SQL Server to install the K2 Databases to, enter the name of the SQL Server
 - To change a database name, enter the name for the database
 - To configure SQL Authentication, select the SQL Authentication option and enter the Account Name and Password

Click the **Test Database connection** button



If all details are correct, click **Next** to proceed

1.6.2.28 Service Accounts Configuration



The Accounts specified on this page must be given the correct permissions, or startup and operational errors related to permissions will be encountered. Set up Permissions

Service Accounts Configuration

The Service Accounts Configuration screen configures two accounts; the Administrator Account and K2 Service Account. These accounts are the Domain User accounts used by the Administrator and the K2 Server.

K2 blackpearl Setup Manager

Service Accounts Configuration

K2 Administrator Account

Use Existing Credentials

User Name:

Password:

K2 Service Account

Use Existing Credentials

User Name:

Password:

Specify the user names and passwords for the K2 Administrator and Service accounts.

Service Accounts	Description
K2 Administrator Account	This account will be given Administrative rights to the K2 Server for the Administrator to perform administrative functions. domain\K2 Administrator Account
K2 Service Account	This account is the dedicated account for the K2 Service domain\K2 Service Account
Test	Checks to verify that the credentials specified are valid. Note: Test will only verify that the account exists and will not test if the permissions available to the account are correct or sufficient for the K2 Service to run.

What to do on this page

To configure the Administrative Account:



Disable the option, **Use Existing Credentials** or click **Next** to continue



- (2) Enter the name of the User account as a fully qualified domain account (domain\K2 Administrator Account)
- (3) Enter the password
- (4) Click **Test** to validate the user name and password

To configure the Service Account:



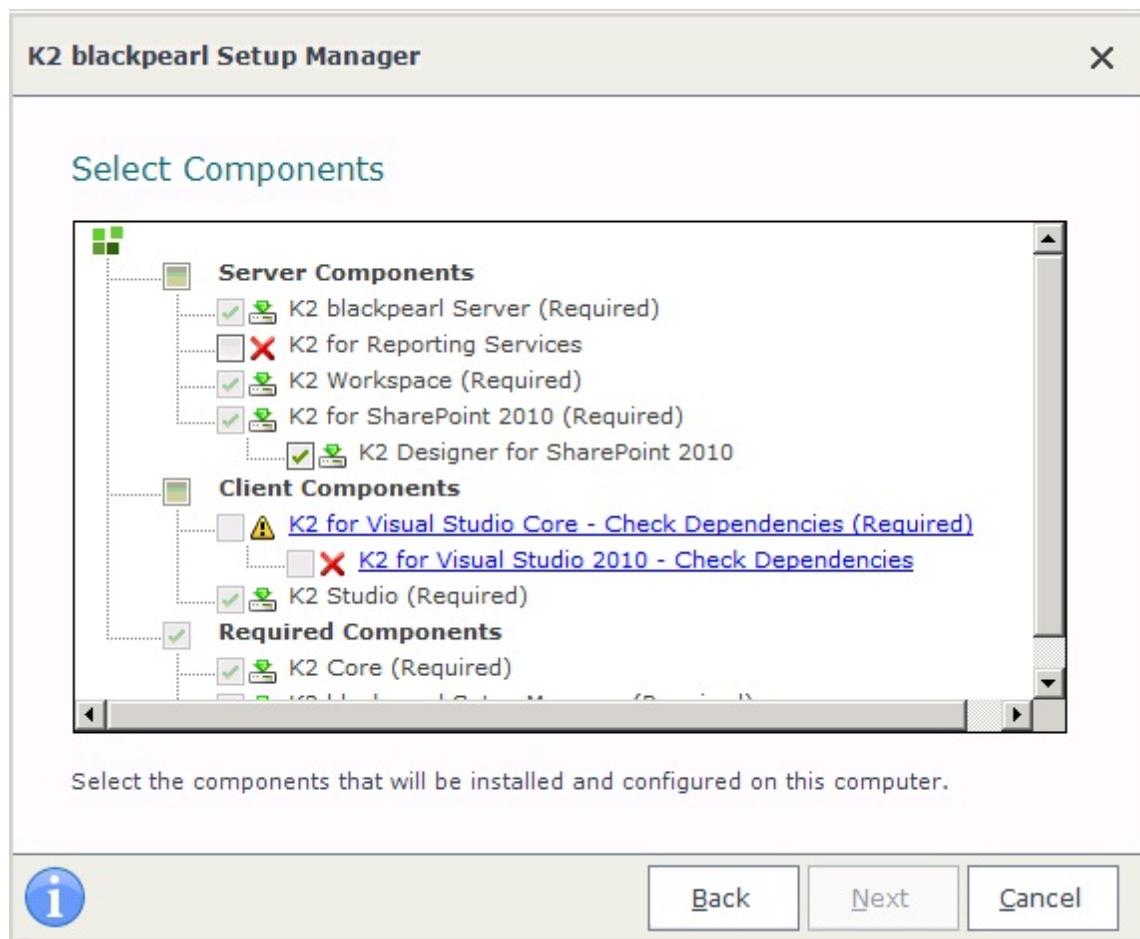
- (1) Enter the name of the User account as a fully qualified domain account (domain\K2 Service Account)
- (2) Enter the password
- (3) Click **Test** to validate the user name and password

1.6.2.29 Check Dependencies

K2 Setup Manager - Check Dependencies

An item cannot be installed unless all the dependencies are already installed to support it. You can click on the Check Dependencies link to see what other prerequisites are required before you can install the component. If you want to install a component that is missing some dependencies, cancel the installer and fix the dependencies. Then, restart the K2 blackpearl Setup Manager.

The Check Dependencies screen enables the installer to view and print the missing dependencies, clicking **Ok** will take the installer back to the selection screen, cancel the installation and fix the dependencies. Then, restart the K2 blackpearl Setup Manager.



If the **Simple Installation > Full Installation** option is selected, the installer will only install the options in accordance with the existing prerequisites that have been installed. The user must manually verify before installing that all required prerequisites are installed if all components are required.

1.6.2.30 User Manager Settings

Setup Manager - User Manager

If Active Directory is not detected ie the AD Service is not found on the K2 Server host machine, the User Manager Settings configuration screen will present the option to install the K2 SQL user manager. For the installation of custom user managers the installation must be completed with the K2 SQLUM installed, and then the steps in KB000577 must be followed. For more information on the K2 SQLUM please see [User Managers](#).



If you use SQL Connections to connect to the SQL Server, the K2 Service account must be a SQL User account on the SQL Server.

If you use Windows Authentication to connect to the SQL Server, the K2 Service account must be both a SQL User account and a Windows User account on the SQL Server.

K2 blackpearl Setup Manager

User Manager Settings

User Manager:

Installation Folder

Installation Folder:

Select the user manager and the folder where the application will be installed. To install to a different folder, click the 'Browse' button and select another folder.

i

What it is	Description
User Manager	The custom User Manager drop down
Installation Folder	The local directory that the custom User Manager will be installed to

- 1 Select the required User Manager
- 2 Confirm the location that the User Manager will be installed to
- 3 Click **Next** to continue

If the SQL User Manager is selected for installation, use the following settings as additional configuration guidelines:

SQL Databases

Make sure that the SQL Database and SQL Server names are unique and reflect their function. For example:
K2-SQL (database)

K2-MAIN (Server)

K2 Workspace Application Pool

In SQL, create a new Windows Login using a K2-SQL user

During the installation, specify this account for the Application Pool account

K2 Server Service Account

Create a Windows User (i.e. K2-MAIN\K2Service)

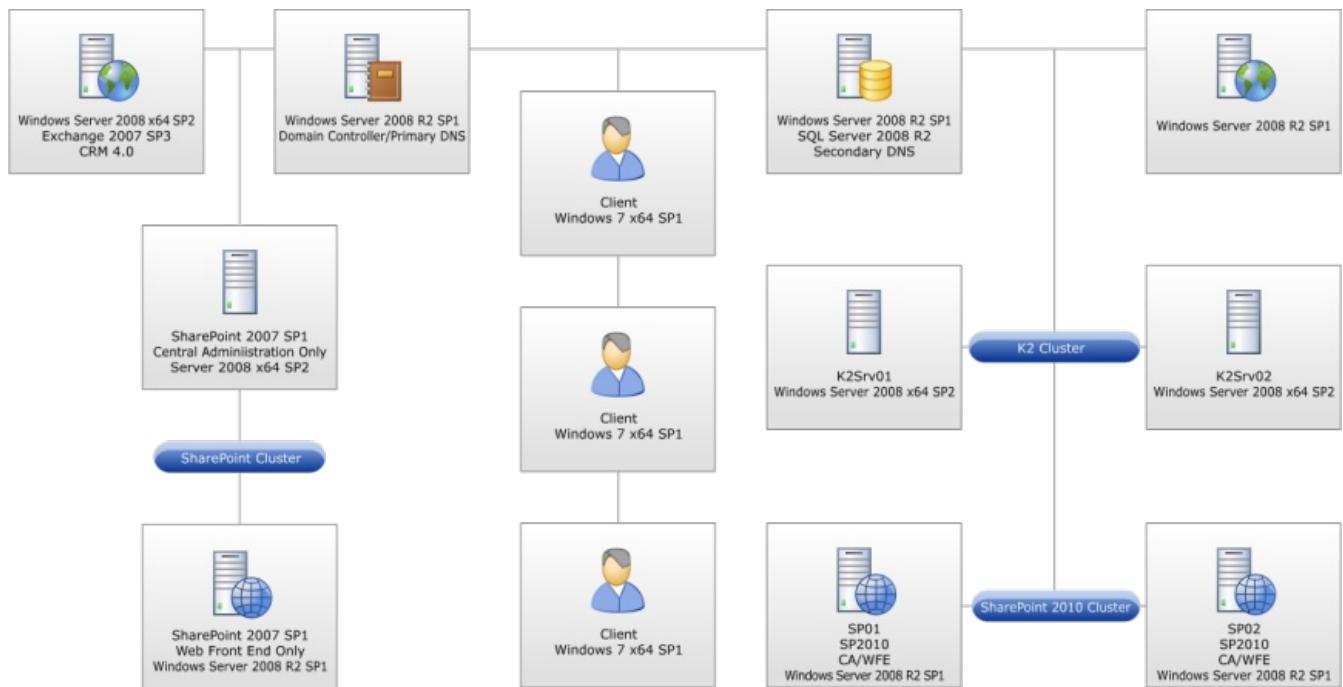
Configure this user as a SQL user (i.e. user K2Service)

During the installation use the K2Service user for the K2 Server Service Account

1.6.3 Installing a distributed K2 blackpearl system

Installing a distributed K2 blackpearl system

Due to the scalability of the K2 blackpearl system, an install in a distributed environment can become quite complex, especially when network load bearing clusters come into the picture. Below is an example of a distributed installation.



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Before the installation is started, the user must decide if the trace logging feature should be enabled. See the topic [Optional installation logging for troubleshooting](#) for more information.

The order of the components listed below should be followed in a distributed installation.

See these topics for details concerning the installation of a distributed K2 system:

1. Install and configure the K2 Host Server
2. Install and configure the K2 Reports
3. Install and configure the K2 Workspace
4. Install and configure the K2 for SharePoint components
5. Install the Client components: K2 for Visual Studio
6. Install the Client components: K2 Studio
7. Distributed install of the K2 View Flow via Group Policy



The same version of K2 blackpearl must be installed on all K2 servers in the distributed environment.



Be sure to see the section on Post installation common tasks once done with the install.

1.6.3.1 Install K2 blackpearl Host Server

Install and configure a K2 Host Server



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Prerequisites



The K2 Server role is defined to be the server on which the K2 Host Server runs. The K2 Server component, configuration manager, and K2 documentation will be installed on this server.



The same version of K2 blackpearl must be installed on all K2 servers in the distributed environment.

The K2 Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Server	
Operating System	<ul style="list-style-type: none"> • * ** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 • *Latest security patches • **32-bit and 64-bit support
Windows Components	<ul style="list-style-type: none"> • Microsoft Message Queuing (MSMQ) Services <ul style="list-style-type: none"> • Message Queuing Server • Directory Service Integration • A User Manager: The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl • Distributed Transaction Coordinator (DTC) • IPv4 (IPv6 can exist, but IPv4 must also be configured)
Additional Software	<ul style="list-style-type: none"> • Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5 <ul style="list-style-type: none"> For more information on .NET framework and K2, please see the topic: .NET Technologies • Windows Support Tools (see Install Windows Support Tools for more information: for 32-bit see http://go.microsoft.com/fwlink/?LinkId=62270. <ul style="list-style-type: none"> Note: Windows Support Tools is a prerequisite if the installer is to automatically set the SPNs during the installation of K2 blackpearl. Otherwise, the Windows Support Tool is regarded as optional software. • Windows Identity Foundation Redistributable (for more information, see http://support.microsoft.com/kb/974405). • Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). • If CRM is used: Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server, the server must have .NET 4 enabled.) <ul style="list-style-type: none"> http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9df&displaylang=en



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Rights and Permissions

The K2 Service Account is the account under which the K2 service runs.

The rest of this guide will use domain\K2 Service Account as a placeholder for the K2 Service account name. When installing K2 in your environment, replace this placeholder with your actual account name.

The K2 Service Account will need the following permissions:

K2 Server	
Permission	Used For
Log on as a Service	In order to run the K2 blackpearl Service, the Service Account will need this permission. To see how to set this permission, click here .
Rights	Folder or Registry Key
Full Control	%SYSTEMROOT%\temp
Full Control	%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA
Full Control	HKEY_LOCAL_MACHINE\SOFTWARE\SourceCode\Logging (* Note)
Modify	%PROGRAMFILES%\K2 blackpearl\Host Server\Bin (* Note)
* Note	The following step is done post installation

The Installation Account will need the following permissions during installation and configuration:

All Servers with K2 Components	
Permission	Used For
Local Administrator	In order to successfully install and configure K2 blackpearl components, the Installation User account must be a local administrator on all the servers that will have K2 components installed.

Kerberos / Pass Through Authentication

When components are installed on separate servers, credentials must be passed between the services. This can be accomplished by setting up **Kerberos**, which should be configured prior to installing K2. Any time where two or more hops are required for user authentication, Kerberos must be configured.

Pass Through Authentication is a K2 proprietary authentication methodology specifically for authenticating users whose credentials need to be passed between machines that interact with the K2 APIs. This authentication model can be used as an alternative to Kerberos, but is not in any way intended to be a replacement for Kerberos within the overall infrastructure.

Install Steps

After you have installed all the [prerequisites](#), created the [service accounts](#), enabled DTC and [installed MSMQ](#), you are now ready to install the K2 blackpearl Server.

Once the installation is done, the **Configuration Analysis tool** will be available to help troubleshoot any errors detected during the installation.



It is recommended to install all K2 components using the K2 Service Account. Log on to the server as the K2 Service Account before installing.

Click on this link to see a flow diagram of the install steps.

To install the K2 Server component, follow the below steps:

- 1 From the local installation folder, double-click on the **Setup.exe** file
- 2 On the **Welcome** screen, click Next
- 3 On the **Checking for Latest Version screen**, the installation will verify the version
- 4 On the **End User License Agreement** screen, read through the EULA. You must select the **I agree** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next
- 5 On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder, and click Next

(6)

On the **Select Components** screen, you should see that the only components for which the prerequisites are met are:

- K2 blackpearl Server
- K2 blackpearl Setup Manager

You will also see a link to Check Dependencies for the other components.



If you want to install one of the components on this server that have a Check Dependencies action, cancel the installation and fix the dependency. Then, restart the installation and you should be able to select that component.

(7)

On the **License Configuration** screen type in the License Key.



If you do not have a license key, you can request one by opening Internet Explorer and going to <https://portal.k2.com/licensekey/Default.aspx>. You will need an internet connection, and you will also need a Customer and Partner portal account. Enter in the appropriate information, and the license key will be generated automatically for you.

(8)

On the **K2 Server Configuration screen**, select the appropriate option:

K2 blackpearl Setup Manager

K2 Server Configuration

Standalone K2 Server
 K2 Server Farm
 Add K2 Server to existing Farm
 Configure K2 Server Farm

K2 Server Farm Name (FQDN):

Add a server to the denallix.com farm

i

Back **Next** **Cancel**

- **Standalone K2 Server.** Single K2 Server in your environment. This does not mean that all K2 components are installed on the same server, it means that there is only one server with the K2 blackpearl Server component installed.

- **K2 Server Farm.** Multiple K2 Servers in your environment.

If you selected the K2 Server Farm option, additional radio buttons are now enabled for you to choose from:

- **Add K2 Server to existing Farm.** Select this option if a K2 Server Farm already exists, and you are connecting an additional server to the farm.
- **Configure K2 Server Farm.** Select this option if this is the first K2 Server you are configuring.

If you are installing K2 Server in a distributed environment but there is only a single server playing the K2 Server Role, select **Standalone K2 Server**

If you are installing K2 Server for the first time in a distributed environment with multiple K2 Servers, select **K2 Server Farm** and **Configure K2 Server Farm**

If you are installing a second node to your K2 Server farm, select **K2 Server Farm** and **Add K2 Server to existing Farm**

Click Next to continue the Configuration Manager

 On the **K2 Pass-Through Authentication** screen, if Kerberos is installed select **Kerberos** and if not then select **Windows**

 On the **K2 Server Configuration** screen, take note of the ports that are used for communication. It is strongly recommended to leave the default ports as is.

 It is strongly recommended to leave the default ports. It is also important to verify that those ports are not blocked in your environment to ensure that K2 runs successfully.

The ports are as follows:

- **Host Service Port.** By default, port 5555 is used to communicate with the K2 Host Server.
- **Workflow Service Port.** By default, port 5252 is used to communicate with the workflow service. For backwards compatibility, be sure to leave this at port 5252.
- **Discovery Service Port.** This should be a unique port that gets assigned to each server cluster you have in the environment. It is used by the K2 management tools to identify your clustered K2 servers in your environment. This port is only displayed if you are installing a K2 Server Farm. By default, port 49599 is used on non NLB environments, and port 49600 is used for NLB environments.

Also on this screen, there is a **Set K2 Host Server SPN** check box:

- This check box is enabled by default, and will therefore automatically configure the SPN settings for the K2 Host Server. When you click Next, you will be warned that you will be reconfiguring the current SPN configuration. If you click Yes, the check box will remain checked and the SPNs will be configured automatically. If you click No, the check box will be unchecked and you will have to manually configure the SPNs.
- If you uncheck this check box, you will have to manually configure the SPNs for the K2 Server.
- If the check box is disabled by the system, verify that the Microsoft Windows Support Tools (in particular, SetSPN.exe) is installed on the machine.
- On the **SMTP Server Configuration** section, enter the name of the SMTP Server that will send K2 related E-mail, and click Next

For more information on which SPNs are required, refer to the [SPNs for K2 Service Account](#) topic. Once you have decided whether or not to allow the system to set the SPNs for you, click Next



If the account you are logged in as while installing the K2 Server does not have domain administrator rights to configure the SPNs, you will need to configure the SPNs manually after installing K2. If you do not configure the SPNs properly in a distributed environment, the K2 Server will not function properly.

 On the **Workspace Web Site Configuration** screen, type in the URL to the K2 Workspace Web Site, and click Next



Even though we have not configured the K2 Workspace yet, enter the URL which you will use to access the Workspace. If this is a clustered workspace, be sure to enter the URL used to access the cluster.

It is preferred to use the fully qualified URL to your workspace web site.

 On the **Exchange Server Settings** screen, enter details as required. See the topics [Exchange Server Configuration](#) and [Exchange Integration](#) for important information.

Note: The **SMTP Settings** screen is displayed after the SmartActions setup step only if the **Use Exchange for mail integration** option has been selected on the **Exchange Server Configuration** screen.

 On the **CRM Server Settings** screen, the details of the CRM Server and the Organizations name can be added. The CRM server details entered on this screen are used to create the Environment Library entry that can be used within the K2 wizards. This screen is optional and the installation will complete without any information being entered on the screen. Ensure that the Microsoft CRM Server is started before adding the information to this screen. CRM integration in K2 such as the CRM Entity Wizard is dependent on the information entered on this screen.

 On the **Database Configurations** screen, you will see the list of K2 Databases that will be created as well as the SQL Server they will be created on. You can change the installation location for the databases by clicking on each database's change link, or the **Change All** button. You can select whether you want to use Windows or SQL Authentication by changing the database configuration. You can also change the Database Name by clicking on the change link and editing the Database Name field. When you have completed your database configuration, click Next to continue.



On the **Service Accounts Configuration** screen, enter in the following user accounts:

- **K2 Administrator Account.** This account will be given Administrative rights to the K2 Server for the Administrator to perform administrative functions. domain\K2 Administrator Account
- **K2 Service Account.** This account is the dedicated account for the K2 Service. domain\K2 Service Account

You can test that the user name and passwords are valid by clicking on the Test button. When you finished entering in the accounts, click Next to continue.



On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Install.



The Setup Manager will update and show you the progress of the components as it installs.



When the installation has completed, you will see a finished screen. There will also be a link to the created configuration log file. When you click Finish, you will be prompted to restart now (click Yes) or restart later (click No). It is important to restart in order to complete the installation and configuration of K2 blackpearl.



Recommendation: When the K2 Server is run in console mode make sure to be logged in as the correct user and make use of the "Run as Administrator" option to ensure that the correct elevated privileges are utilized.

K2 Service Account

In a distributed environment where components are installed on more than one server, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

There are two sets of SPNs that need to be set up for the K2 Service Account:

- K2Server
- K2HostServer

The following placeholders are used in the commands:

- domain\K2 Service Account - The K2 Service Account that runs the K2 Service
- MachineName - The name of the computer on which the K2 Service is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the K2 Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly. The SPNs listed below are for K2 blackpearl.



If you have a K2 Server farm running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A K2Server/MachineName:5252 domain\K2 Service Account
- setspn -A K2Server/MachineName.FQDN:5252 domain\K2 Service Account
- setspn -A K2HostServer/MachineName:5555 domain\K2 Service Account
- setspn -A K2HostServer/MachineName.FQDN:5555 domain\K2 Service Account



If you are installing K2 blackpearl on an **NLB environment**, the MachineName will change to the the LBHostServerName

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\K2 Service Account



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

After installing and configuring the K2 Server component, you can easily validate that the K2 Server is functioning properly by running the K2 Service in console mode. Console mode is a useful troubleshooting tool, as all error and informational messages are sent to the console window so you can watch what is going on. It is important that you run the service as the Service Account in order to accurately troubleshoot permissions and other errors.

To run in console mode, perform the following steps:

- 1**
- 2**
- 3**
- 4**
- 5**

- Open the **Services** manager (Start > All Programs > Administrative Tools > Services)
- Scroll down to the **K2 blackpearl Server** service, select it and click the **Stop Service** button
- Once the service shows as stopped, you can close the Services manager
- Right-click on the **K2 blackpearl Server** item in the Start menu (under Start > All Programs > K2 blackpearl) and select **Run as...**
- Select **The following user** option, and type in the domain\K2 Service Account as the User Name and password, and click OK

The K2 Server will start and initialize. You will see several messages starting the various components. Once you see the line stating "Info 7010 MSMQ Thread Listing", you know the service has started successfully.



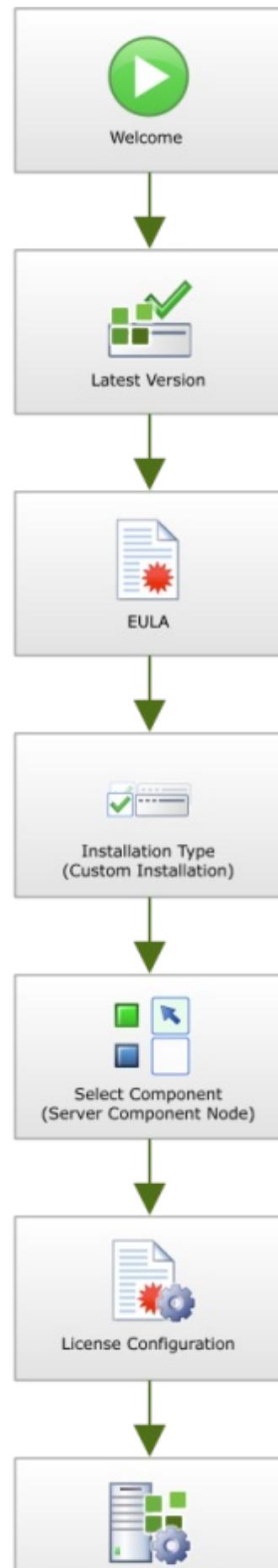
If you see the following error messages, the SPNs for the K2 Service Account were not set properly:

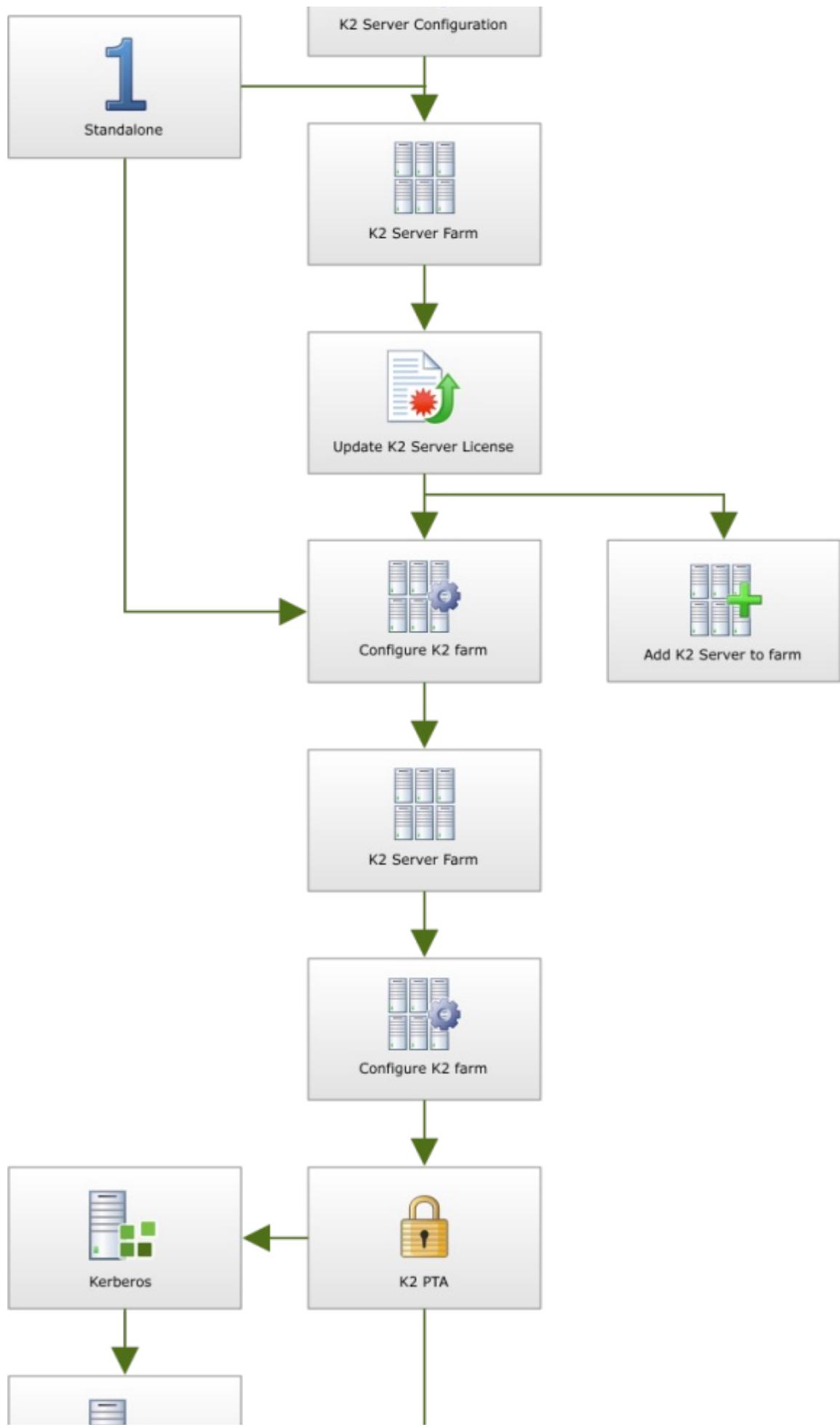
- Info 7003 SourceCode.SmartObjects.Runtime.SmartObjectClientServer not yet Loaded...
- Error 8060 ProcessPacket Error, Authentication With Server Failed : SEC_E_LOGON_DENIED

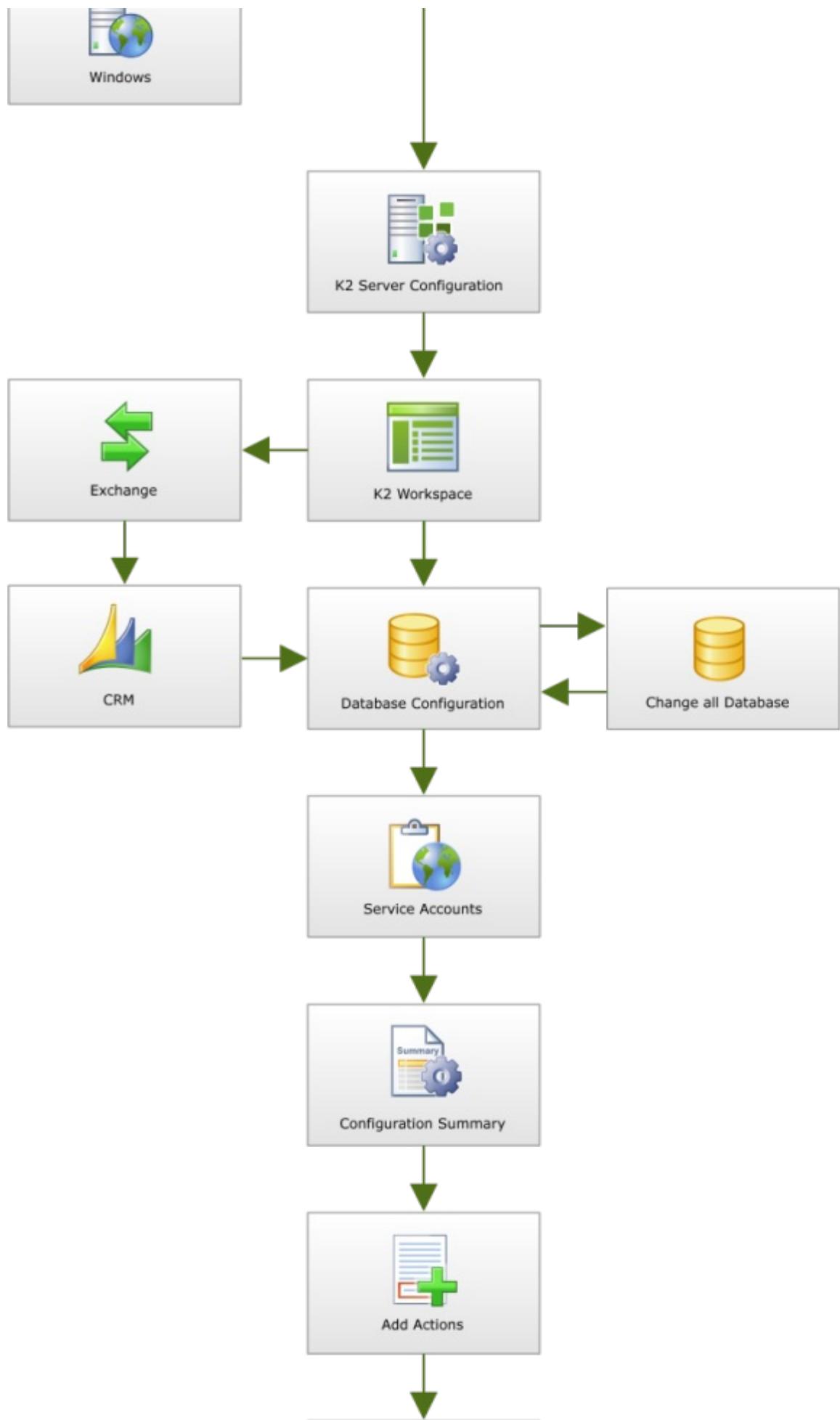


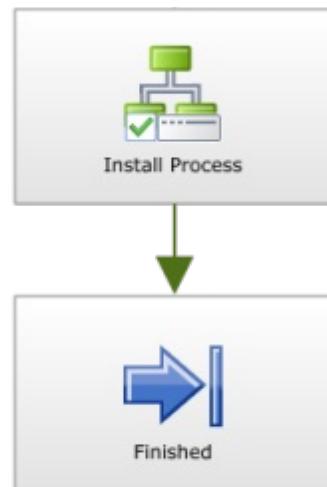
Be sure to see the section on Post installation common tasks once done with the install.

1.6.3.1.1 K2 Server Installation Flow Diagram









1.6.3.2 Install the K2 for Reporting Services component

Install the K2 for Reporting Services component



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Prerequisites



The Microsoft SQL Server 2008 Reporting Services component is now optional for all K2 blackpearl installations and can only be installed during a custom K2 blackpearl installation. The K2 for Reporting Services component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 for Reporting Services component	
Operating System	<ul style="list-style-type: none"> *** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 *Latest security patches *32-bit and 64-bit support
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software	<ul style="list-style-type: none"> Microsoft SQL Server 2012 Reporting Services or Microsoft SQL Server 2008 Reporting Services Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en <p>NOTE: K2 Reports Runtime and K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2008 SP1</p> <ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 Redistributable Package and Microsoft .Net Framework 4 http://www.microsoft.com/downloads/details.aspx?FamilyID=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en Microsoft Internet Explorer 8 or 9 or 10 (Plug-in support is only available in Internet explorer 10 on the desktop, and this version of Internet Explorer 10 must be used for items built on Silverlight, such as the K2 designer for SharePoint). Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server)



Important: You must be running Reporting Services in Native mode. K2 blackpearl does not currently support SharePoint Integrated mode.



The minimum requirement is Microsoft .NET Framework 3.5 SP1

Rights and Permissions

The Reporting Services Service Account is the account that the Reporting Services application pool (called ReportServer) will

run under. This account probably already exists in your environment, but there are some permissions that should be validated to ensure that the K2 integration with Reporting Services functions properly.

The rest of this guide will use domain\Reporting Services Service Account as a placeholder for the Reporting Services Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

Application Pool Rights

The SQL Reporting Services Service Account will require elevated permissions to run the application pool. We will use the aspnet_regiis command to configure this. This tool ships with the .NET Framework, and takes the pain out of configuring all the required NTFS permissions, IIS_WPG group membership, security policy user rights assignments, and IIS metabase access rights. For more information, see the MSDN article on setting security rights for .NET Applications, at <http://msdn2.microsoft.com/en-us/library/ms998297.aspx>.

To use the aspnet_regiis command, perform the following steps:

- 1 Open a command prompt (Start > Run > cmd)
- 2 Change directories to the .NET Framework folder (C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727)
- 3 Type aspnet_regiis -ga domain\Reporting Services Service Account and hit Enter
- 4 After the command completes, type **iisreset** and hit Enter

Reporting Services Permissions

The SQL Reporting Services Service Account will also require permissions on the SQL Reporting Services databases. To set these permissions, perform the following steps:

- 1 Open **Reporting Service Configuration** (Start > All Programs > Microsoft SQL Server 2008 > Configuration Tools > Reporting Services Configuration Manager)
- 2 Connect to the appropriate Instance
- 3 On the Web Service Identity tab, confirm that Reporting Services picked up the new service account and listed it in the **ASP.NET Service Account** text box
- 4 Make sure the SQLRS Service Account is selected, and click **Apply**
- 5 The Task Status will update, and the icon next to the Web Service Identity will change to Configured (a green check mark). Check that the Web Services URL and Report Manager URL are correct
- 6 Change or create a new database on the Database tab
- 7 Close the Reporting Services Configuration Manager window

Additional Configuration.

In order for users to browse the reports on the server, the following permissions must be configured:

Server Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role System User

Home Folder Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role Browser



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Kerberos / Pass Through Authentication

When components are installed on separate servers, credentials must be passed between the services. This can be accomplished by setting up **Kerberos**, which should be configured prior to installing K2. Any time where two or more hops are required for user authentication, Kerberos must be configured.

Pass Through Authentication is a K2 proprietary authentication methodology specifically for authenticating users whose credentials need to be passed between machines that interact with the K2 APIs. This authentication model can be used as an alternative to Kerberos, but is not in any way intended to be a replacement for Kerberos within the overall infrastructure.

Steps to install

After you have installed all the **prerequisites**, created the **service accounts**, **enabled DTC** and **installed MSMQ**, you are now ready to install the K2 for Reporting Services component on the Reporting Services Server.

Once the installation is done, the **Configuration Analysis tool** will be available to help troubleshoot any errors detected during the installation.



It is important to copy the installation files local to the server before installing. Do not install from a network share or UNC path. The installation will not work properly.



It is recommended to install all K2 components using the K2 Service Account. Log on to the server as the K2 Service Account before installing.

To install the K2 for Reporting Services component, follow the below steps:



From the local installation folder, double-click on the **Setup.exe** file



On the **Welcome** screen, click Next

- (3)** On the **End User License Agreement** screen, read through the EULA. You must select the **I agree to the terms and conditions of the license** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next
- (4)** On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder, and click Next
- (5)** On the **Select Components** screen, you should see that the only components for which the prerequisites are met are:
- K2 for Reporting Services
 - K2 blackpearl Setup Manager
- You will also see a link to Check Dependencies for the other components.
-  **Note:** If you want to install one of the components on this server that have a Check Dependencies action, cancel the installation and fix the dependency. Then, restart the installation and you should be able to select that component.
- (6)** Once you have verified the components, click Next.
-  The SQL Server Reporting Services web site can be slow to respond if it has not been accessed in a while. This can cause the Configuration Manager's connection to Reporting Services to time out. To counter this, open Internet Explorer and access the Reporting Services web site (such as <http://localhost/Reports>). When the home page displays, proceed with the K2 blackpearl Configuration Manager. Make sure that you can access the Reporting Services home page before proceeding.
- (7)** On the **K2 Database** screen, type in the name of the SQL Server where you installed the K2 Database. This points the K2 component to the K2 database set up by the K2 Server, to share configuration information. If you changed the Host Server database name, update it here and click Next
- (8)** On the **SQL Reporting Services Configuration** screen, select the Web Site and enter the Virtual Directory that is used for the Reporting Services Web Site. If this is a default installation of SQL Reporting Services, the Virtual Directory is **ReportServer**. You can test the connection, and when successful, click Next
- (9)** On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Install.
- (10)** The Setup Manager will update and show you the progress of the components as it installs.
- (11)** When the installation has completed, you will see a finished screen. There will also be a link to the created configuration log file. When you click Finish, you will be prompted to restart now (click Yes) or restart later (click No). It is important to restart in order to complete the installation and configuration of K2 blackpearl.

Reporting Services Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order to access the K2 Reports from the K2 Workspace, you need to set the SPNs for the Reporting Services Service Account.

The following placeholders are used in the commands:

- domain\Reporting Services Service Account - The Reporting Services Service Account that runs the Reporting Services application pool
- MachineName - The name of the computer on which Reporting Services is running
- MachineName.FQDN - The fully qualified domain name of the computer on which Reporting Services is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you are using **Host Headers** to access your Reporting Services Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- `setspn -A HTTP/MachineName domain\Reporting Services Service Account`

- setspn -A HTTP/MachineName.FQDN domain\Reporting Services Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\Reporting Services Service Account

Configure Delegation for Reporting Services Service Account

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.



Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)



Find the domain\Reporting Services Service Account and view its properties



On the Delegation tab, select the **Trust this user for delegation to specified services only** option



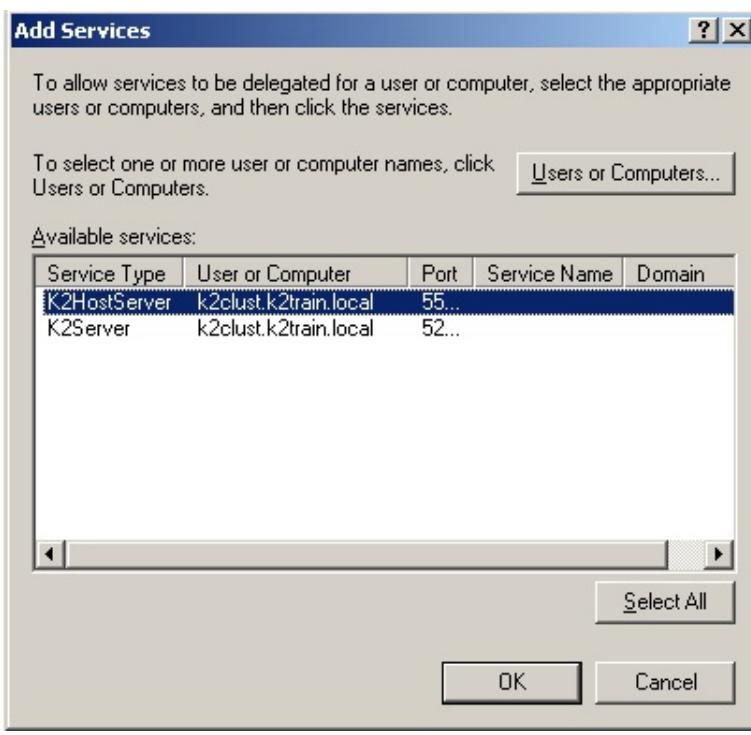
Select the **Use Kerberos only** option, and click on **Add**



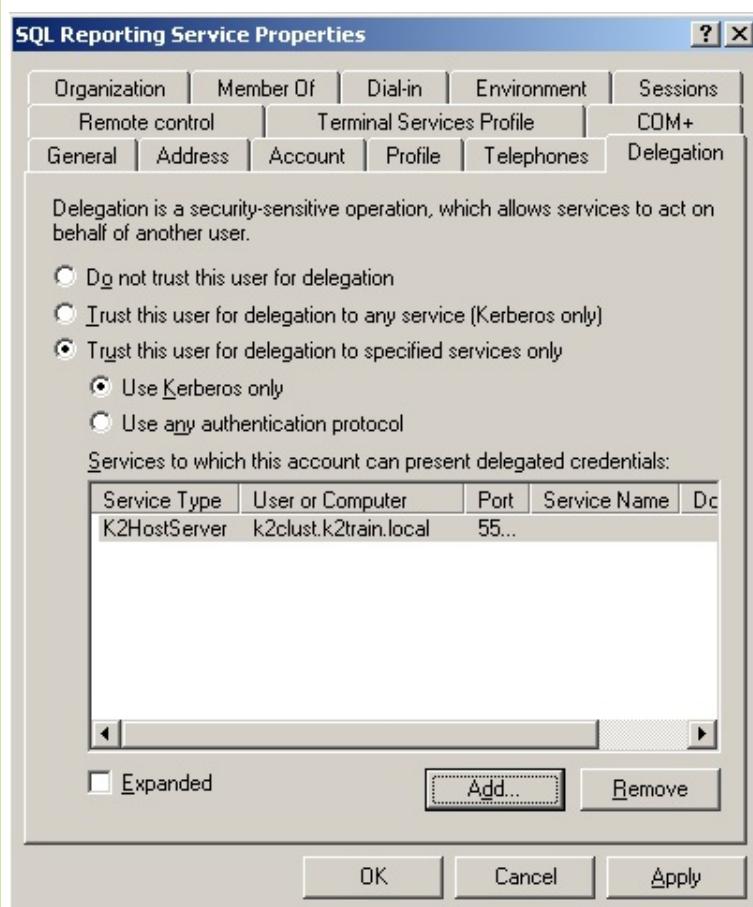
Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account



In the Available Services section, select the **K2HostServer** item listed:



7 Click **OK**. Your properties should resemble the following:



8 Click **OK**

Configure Delegation for the K2 Service Account

In order to use the SQL Server Reporting Services Service Object to schedule Reporting Services reports and include SmartObject data, you will need to configure the K2 Service Account with delegation.



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.

1 Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)

2 Find the domain\K2 Service Account and view its properties

3 On the Delegation tab, select the **Trust this user for delegation to specified services only** option

4 Select the **Use Kerberos only** option, and click on **Add**

5 Click on **Users or Computers** and select the domain\Reporting Services Service Account you created as the SQL Server Reporting Services Service Account

6 In the Available Services section, select the **HTTP** item listed

7 Click **OK** twice to exit the dialog windows



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

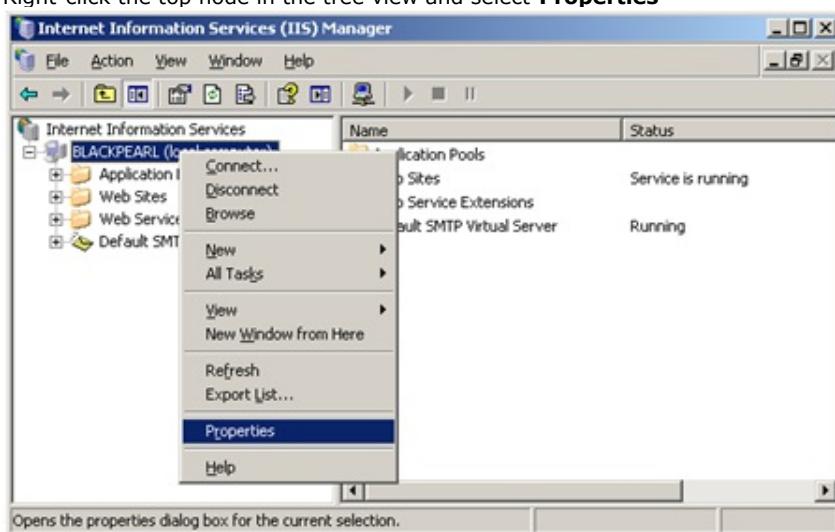
Enable Direct Metabase Edit



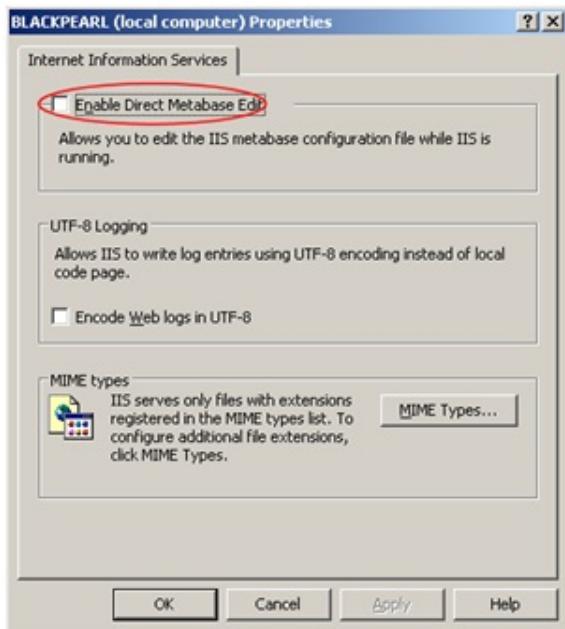
Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

In order to allow Kerberos authentication on the Reporting Services web site, you need to first enable the metabase edit in IIS:

1. Open the Internet Information Services (IIS) Manager (Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager)
2. Right-click the top node in the tree view and select **Properties**



3. Check the check box next to the **Enable Direct Metabase Edit** option



4. Click **OK** and when prompted, click **OK** to confirm

Configure Reporting Services Web Site to use Kerberos

After allowing the Service Account to use delegation, the Reporting Services web site still needs to be configured to use Kerberos as an authentication method. This will be done by using the ADSUTIL script.

To configure the Reporting Services Web Site to use Kerberos, follow the below steps:

1. Still in IIS Manager, click on the **Web Sites** node
2. On the right hand side, you will see all of the configured Web Sites on this server. Locate the Site **Identifier** for the Reporting Services web site. In the script below, this will be identified as Site Identifier Be sure to replace this place holder with your actual identifier in the below scripts.
3. Open a **command prompt** (Start > Run > cmd)
4. Change directories to **C:\Inetpub\AdminScripts**

- To force IIS to use Kerberos for the site, execute the following command:

```
cscript adsutil.vbs set w3svc/NTAuthenticationProviders "Negotiate,NTLM"
cscript adsutil.vbs set w3svc/Site Identifier/NTAuthenticationProviders "Negotiate,NTLM"
```



Important: This command and the parameters are case sensitive. Ensure that the case is correct and that you typed everything correctly. Pay particular attention to the spelling of Negotiate and use double quote marks, these are common errors.

- Type **iisreset** and hit Enter

After installing and configuring the K2 for Reporting Services component, you can validate that the K2 Reports are functioning properly by running the K2 Service in console mode and then accessing the K2 Reports from Reporting Services. Console mode is a useful troubleshooting tool, as all error and informational messages are sent to the console window so you can watch what is going on. It is important that you run the service as the Service Account in order to accurately troubleshoot permissions and other errors.

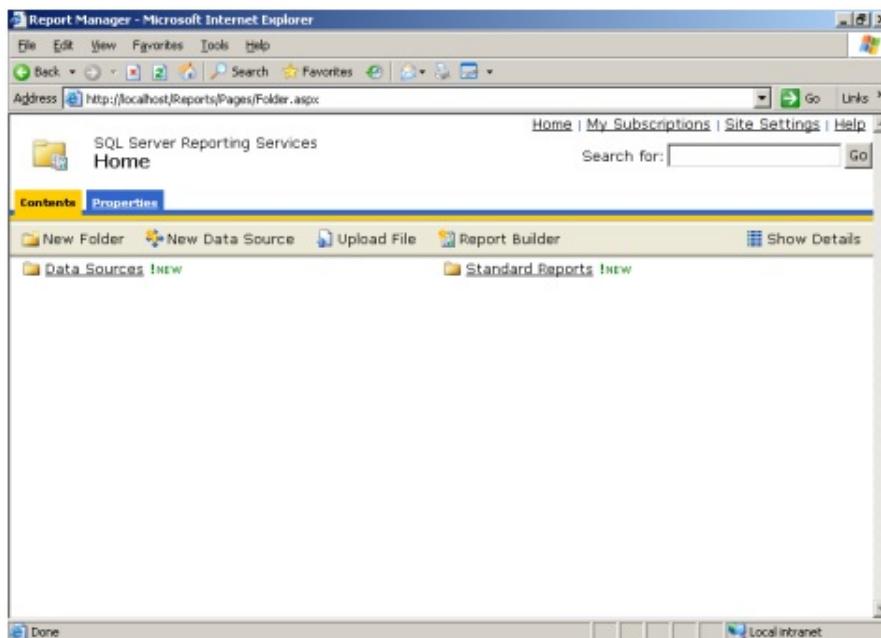
To run in console mode, perform the following steps:

- Open the **Services** manager (Start > All Programs > Administrative Tools > Services)
- Scroll down to the **K2 blackpearl Server** service, select it and click the **Stop Service** button
- Once the service shows as stopped, you can close the Services manager
- Right-click on the **K2 blackpearl Server** item in the Start menu (under Start > All Programs > K2 blackpearl) and select **Run as...**
- Select **The following user** option, and type in the domain\K2 Service Account as the User Name and password, and click OK

The K2 Server will start and initialize. You will see several messages starting the various components. Once you see the line stating "Info 7010 MSMQ Thread Listing", you know the service has started successfully.

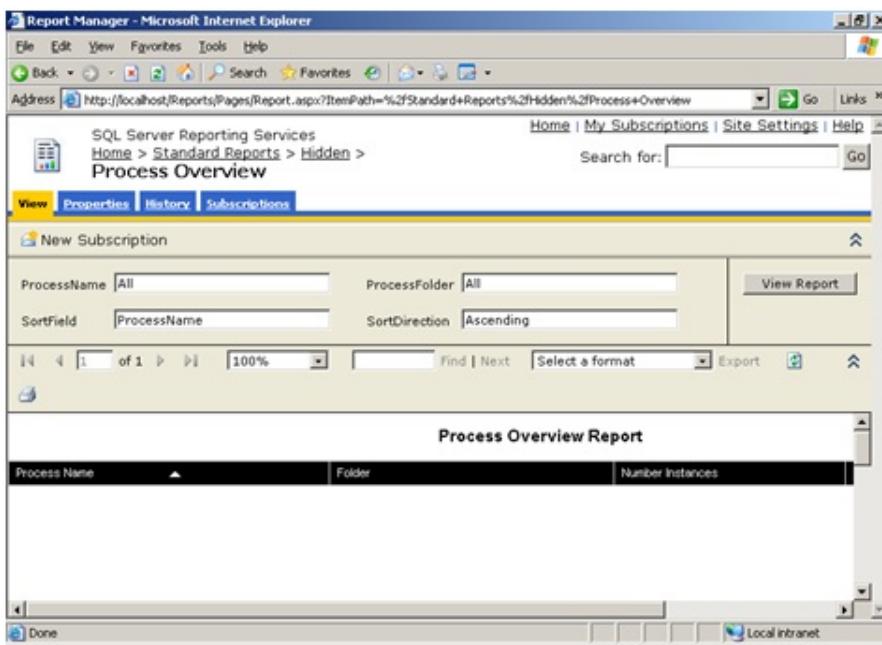
- Next, open Internet Explorer from the K2 Server machine. Access the SQL Server Reporting Services home page.

You will see the new Data Sources and Standard Reports folders listed, as shown below. These are the standard, out-of-the-box reports that ship with K2 blackpearl. When you create new reports and publish them to Reporting Services, you will also see those reports listed here.



- Click on the **Standard Report** link, the **Hidden** link, and then click on **Process Overview**

This will display the out-of-the-box Process Overview Report, as shown below:



8. Also, you should see a message in the K2 Server console window showing that Kerberos was used for authentication:

```

Info 27128 K2 Server was successfully started
Info 10000 SmartObject Runtime Server starting up.....
Info 10001 SmartObject Runtime Connecting to Store Database on K2TRAINSQ...
Info 10003 SmartObject Runtime successfully connected to Database on K2TRAINS...
QL
Info 10004 SmartObject Runtime Store using integrated security.
Info 10021 SmartObject Runtime Event Handler initialized successfully.
Info 10010 SmartObject Object Factory initialized with cache time of 0
Info 10019 SmartObject Runtime Server successfully initialized and running.
Info 2004 All Dependencies Loaded
Info 2021 Assembly Execution Path successfully updated
Info 2023 Loading Event Bus Server
Info 2005 Configuration settings initialized
Info 2032 Initialization Check Successfull
Info 2013 Service registered with ID:5 running on machine: K2TRAINX2-01
Info 2022 Event Bus Server Loaded Successfully
Info 7010 MSMQ Thread Listing
Info 1028 Starting Session B5B1B54AA449761151CE99F111CE989
Info 3000 Authenticating K2TRAIN\Administrator for session B5B1B54AA449761151CE99F111CE989
Info 10514 Name: .sourcecode.SmartObjects.runtime Version: 4.7263.1.0 Date: '11/12/2007 8:32:18 AM'
Info 1025 Ending Session B5B1B54AA449761151CE99F111CE989

```

Be sure to see the section on Post instillation common tasks once done with the install.



1.6.3.3 Install K2 Workspace on the IIS Server

Install K2 Workspace on the IIS Server



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Prerequisites



The K2 Workspace is a web based application used to manage processes and the K2 environment. The K2 Workspace requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Workspace	
Operating System	<ul style="list-style-type: none"> * *** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 * latest security patches *32-bit and 64-bit support
Windows Components	<ul style="list-style-type: none"> IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager Distributed Transaction Coordinator (DTC) IPv4 (IPv6 can exist, but IPv4 must also be configured) ASP.NET Windows Authentication Role Services
Additional Software	<ul style="list-style-type: none"> Microsoft .NET Framework 3.5 SP1 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 Microsoft Report Viewer Redistributable 2005 SP1 <ul style="list-style-type: none"> Full installation: http://www.microsoft.com/downloads/details.aspx?FamilyID=E7D661BA-DC95-4EB3-8916-3E31340DDC2C&displaylang=en Upgrade installation: http://www.microsoft.com/downloads/details.aspx?FamilyId=35F23B3C-3B3F-4377-9AE1-26321F99FDF0&displaylang=en and http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en or http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en Microsoft Report Viewer Redistributable 2008 http://www.microsoft.com/downloads/details.aspx?familyid=6AE0AA19-3E6C-474C-9D57-05B2347456B1&displaylang=en Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en <p>NOTE: K2 Reports Runtime – requires Microsoft Report Viewer Redistributable 2008 SP1 K2 SSRS Service Broker – requires Microsoft Report Viewer Redistributable 2005 SP1</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). Microsoft Silverlight 4 or 5: (required for View Flow) http://www.silverlight.net/getting-started

Rights and Permissions

The K2 Workspace Service Account is the account that the K2 Workspace application pool will run under.

The rest of this guide will use domain\K2 Workspace Service Account as a placeholder for the K2 Workspace Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

The K2 Workspace Service Account will need the following permissions:

Web Server	
Permission	Used For
IIS_WPG	In order to function properly as an application pool within IIS, the K2 Workspace Service Account needs to be

Local Group	a member of this group if Windows Server 2003 is used.
IIS_IUSRS	In order to function properly as an application pool within IIS, the K2 Workspace Service Account needs to be a member of this group if Windows Server 2008 is used
Rights	Folder or Registry Key
Modify	%SYSTEMROOT%\temp

In K2 blackpearl 4.5 the K2 Workspace Report Designer does not use the SSRS server.

SSRS integration is still supported for customers:

- Who wish to use the SSRS server to expose reports in other contexts other than K2 Workspace or K2 Process Portals
- Who wish to use other design tools and then import reports into K2 Workspace Report Designer

Reporting Services Server	
Permission	Used For
Content Manager	The K2 Workspace Application pool Account (i.e. the Service Account) must be added in the Content Manager role on the SQL Server Machine, where the SSRS Server has been installed and configured.

Application Pool Rights

The K2 Workspace Service Account will require elevated permissions to run the application pool. We will use the aspnet_regiis command to configure this. This tool ships with the .NET Framework, and takes the pain out of configuring all the required NTFS permissions, IIS_WPG group membership, security policy user rights assignments, and IIS metabase access rights. For more information, see the MSDN article on setting security rights for .NET Applications, at <http://msdn2.microsoft.com/en-us/library/ms998297.aspx>.

To use the aspnet_regiis command, perform the following steps:

1. Open a command prompt (Start > Run > cmd)
2. Change directories to the .NET Framework folder (C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727)
3. Type aspnet_regiis -ga domain\K2 Workspace Service Account and hit Enter
4. After the command completes, type **iisreset** and hit Enter



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Kerberos / Pass Through Authentication

When components are installed on separate servers, credentials must be passed between the services. This can be accomplished by setting up **Kerberos**, which should be configured prior to installing K2. Any time where two or more hops are required for user authentication, Kerberos must be configured.

Pass Through Authentication is a K2 proprietary authentication methodology specifically for authenticating users whose credentials need to be passed between machines that interact with the K2 APIs. This authentication model can be used as an alternative to Kerberos, but is not in any way intended to be a replacement for Kerberos within the overall infrastructure.

Install Steps

After you have installed all the prerequisites, created the service accounts, and enabled DTC, you are now ready to install the K2 Workspace.

Once the installation is done, the **Configuration Analysis tool** will be available to help troubleshoot any errors detected during the installation.



It is important to copy the installation files local to the server before installing. Do not install from a network share or UNC path. The installation will not work properly.



It is recommended to install all K2 components using the K2 Service Account. Log on to the server as the K2 Service Account before installing.

To install the K2 Workspace component, follow the below steps:

- 1 From the local installation folder, double-click on the **Setup.exe** file
- 2 On the **Welcome** screen, click Next
- 3 On the **End User License Agreement** screen, read through the EULA. You must select the **I agree** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next
- 4 On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder, and click Next
- 5 On the **Select Components** screen, you should see that the components for which the prerequisites are met are:
 - K2 blackpearl Server,

- K2 Workspace,
- K2 blackpearl Setup Manager

You will want to **uncheck** the box next to K2 blackpearl Server, as you will not be installing the K2 Server on this machine. You will also see a link to Check Dependencies for the other components.



If you want to install one of the components on this server that have a Check Dependencies action, cancel the installation and fix the dependency. Then, restart the installation and you should be able to select that component.

(6)

Before the K2 Workspace can be installed, an IIS Reset will be done to release the assemblies. You will be prompted to reset IIS, if you click No, you cannot continue the installation. If you click Yes, a command window will open and reset IIS, and then the Setup Manager will automatically continue.

(7)

On the **HostServer Database** screen, type in the name of the SQL Server where you installed the K2 Databases. This points the K2 Workspace to the HostServer database set up by the K2 Server, to share configuration information. If you changed the Host Server database name, update it here and click Next

(8)

On the **K2 Workspace Configuration** screen, select the IIS Web Site to install the K2 Workspace on. If you do not have a K2 Workspace Web Site created, you can type into the drop down list the name of a web site. You will be prompted that the web site does not exist, and K2 will create it for you.

Also, type in the following user name and password:

- **K2 Workspace Application Pool Account.** The account that the K2 Workspace application pool will run under. domain\K2 Workspace Service Account

You can test that the user name and password is valid by clicking on the Test button. When you finished entering in the accounts, click Next to continue.

(9)

On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Install.

(10)

The Setup Manager will update and show you the progress of the components as it installs.

(11)

When the installation has completed, you will see a finished screen. There will also be a link to the created configuration log file. When you click Finish, you will be prompted to restart now (click Yes) or restart later (click No). It is important to restart in order to complete the installation and configuration of K2 blackpearl.

K2 Workspace Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order to access the K2 Workspace from another machine, you need to set the SPNs for the K2 Workspace Service Account.

The following placeholders are used in the commands:

- domain\K2 Workspace Service Account - The K2 Workspace Service Account that runs the K2 blackpearl application pool
- MachineName - The name of the computer on which the K2 Workspace is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the K2 Workspace is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have the K2 Workspace running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.



If you are using **Host Headers** to access your K2 Workspace, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\K2 Workspace Service Account
- setspn -A HTTP/MachineName.FQDN domain\K2 Workspace Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\K2 Workspace Service Account

Configure for Delegation

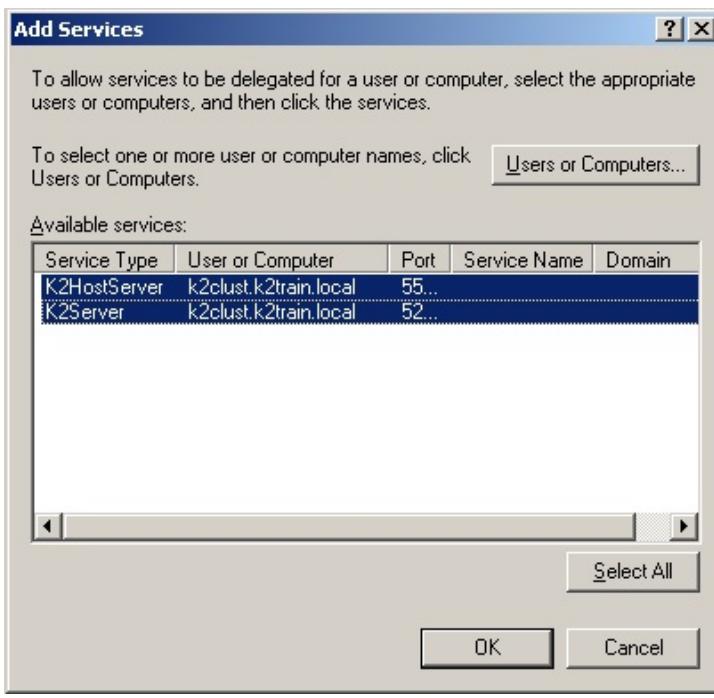
After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



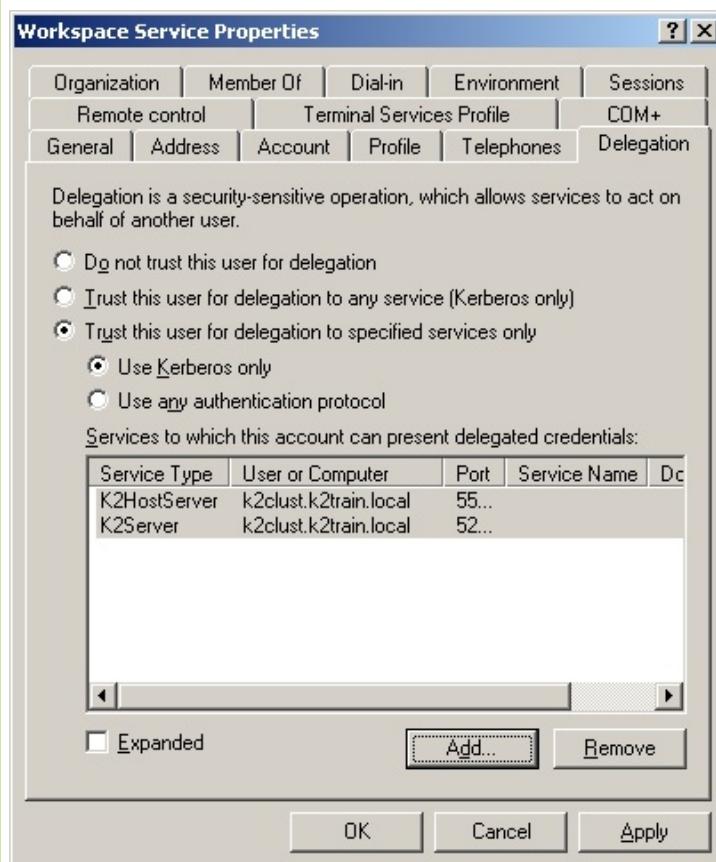
If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a **Trust this user for delegation** check box.

- 1
- 2
- 3
- 4
- 5
- 6

- 1 Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)
- 2 Find the domain\K2 Workspace Service Account and view its properties
- 3 On the Delegation tab, select the **Trust this user for delegation to specified services only** option
- 4 Select the **Use Kerberos only** option, and click on **Add**
- 5 Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account
- 6 In the Available Services section, select both the **K2HostServer** and **K2Server** items listed:



Click **OK**. Your properties should resemble the following:



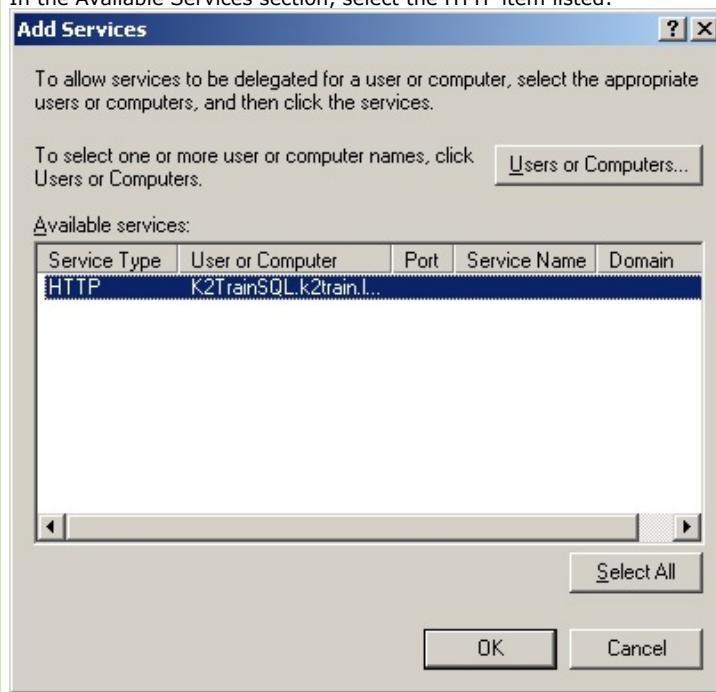
Click **OK**. This will allow the K2 Workspace Service Account to delegate to the K2 Server Service Account.

Also, since the SQL Reporting Services reports will also be rendered in the K2 Workspace, the K2 Workspace Service Account should also be allowed to delegate to the SQLRS Account.

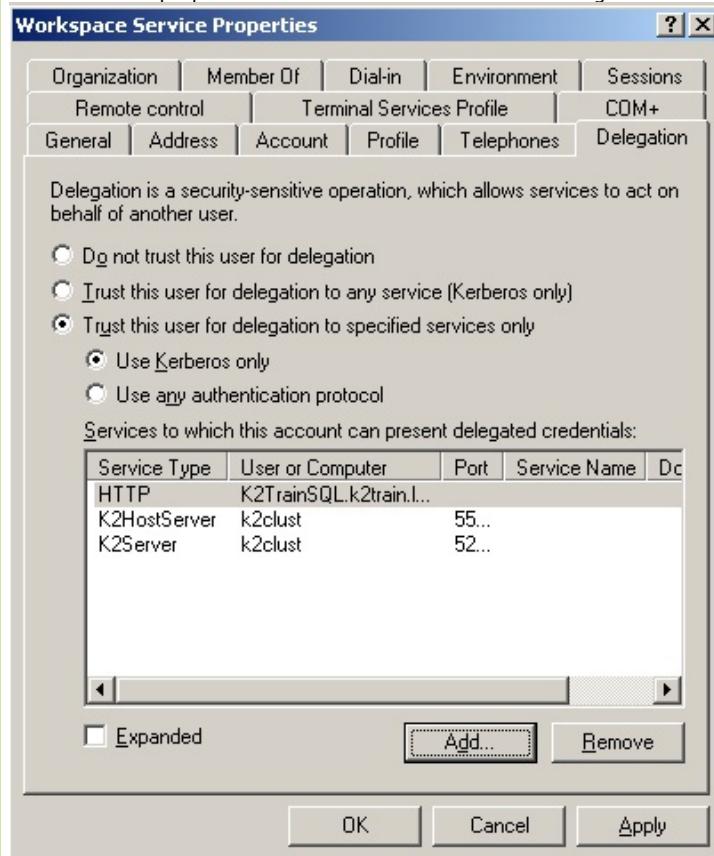
Click **Add** again

Click on **Users or Computers** and select the domain\Reporting Services Service Account you created as the SQL Reporting Services Service Account

In the Available Services section, select the HTTP item listed:



Click **OK**. Your properties should now resemble the following:



If you are using SharePoint Integrated process, K2 Workspace Service Account should also be allowed to delegate to the MOSS Account

Click **Add** again

Click on **Users or Computers** and select the domain\MOSS Account you created as the MOSS Server Account

In the Available Services section, select the HTTP item listed

Click **OK**



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

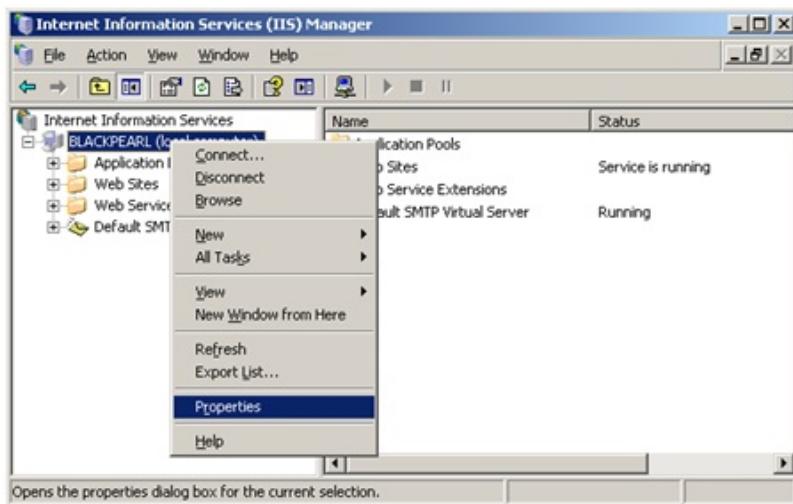
Enable Direct Metabase Edit



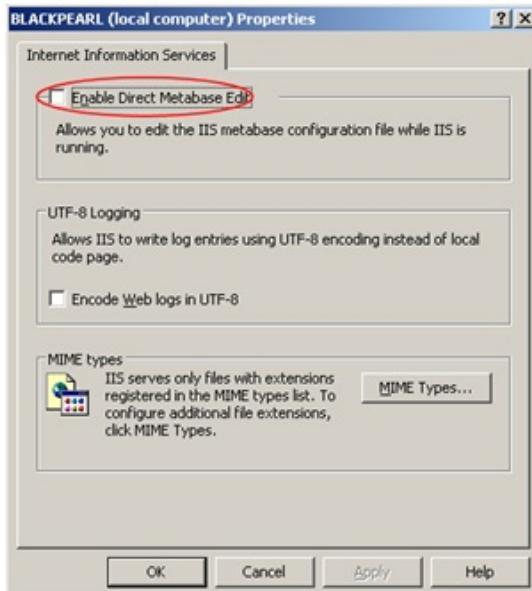
Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

In order to allow Kerberos authentication on the K2 Workspace web site, you need to first enable the metabase edit in IIS:

1. Open the Internet Information Services (IIS) Manager (Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager)
2. Right-click the top node in the tree view and select **Properties**



- Check the check box next to the **Enable Direct Metabase Edit** option



- Click **OK** and when prompted, click **OK** to confirm

Configure K2 Workspace Web Site to use Kerberos

After allowing the Service Account to use delegation, the K2 workspace Web Site still needs to be configured to use Kerberos as an authentication method. This will be done by using the ADSUTIL script.

To configure the K2 Workspace Web Site to use Kerberos, follow the below steps:

- Still in IIS Manager, click on the **Web Sites** node
- On the right hand side, you will see all of the configured Web Sites on this server. Locate the **Site Identifier** for the K2 Workspace web site. In the script below, this will be identified as Site Identifier. Be sure to replace this place holder with your actual identifier in the below scripts.
- Open a **command prompt** (Start > Run > cmd)
- Change directories to **C:\Inetpub\AdminScripts**
- To force IIS to use Kerberos for the site, execute the following command:

```
cscript adsutil.vbs set w3svc/NTAuthenticationProviders "Negotiate,NTLM"
cscript adsutil.vbs set w3svc/Site Identifier/NTAuthenticationProviders "Negotiate,NTLM"
```



Important: This command and the parameters are case sensitive. Ensure that the case is correct and that you typed everything correctly. Pay particular attention to the spelling of Negotiate and use double quote marks, these are common errors.

- Type **iisreset** and hit Enter

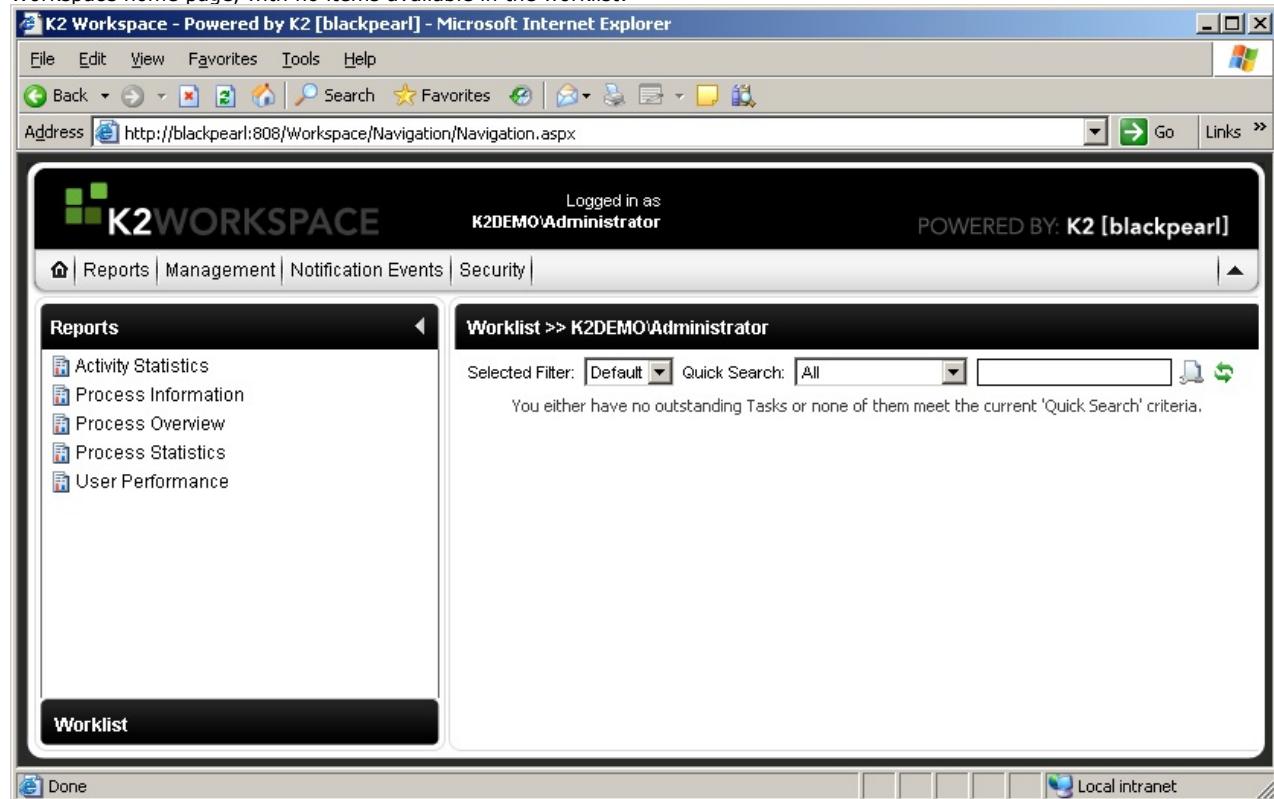
After installing and configuring the K2 Workspace component, you can validate that the Workspace is functioning properly by running the K2 Service in console mode and then accessing the K2 Workspace from a different machine. Console mode is a useful troubleshooting tool, as all error and informational messages are sent to the console window so you can watch what is going on. It is important that you run the service as the Service Account in order to accurately troubleshoot permissions and other errors. It is also important that you have your **browser settings configured correctly** to pass through your credentials.

To run in console mode, perform the following steps:

1. Open the **Services** manager (Start > All Programs > Administrative Tools > Services)
2. Scroll down to the **K2 blackpearl Server** service, select it and click the **Stop Service** button
3. Once the service shows as stopped, you can close the Services manager
4. Right-click on the **K2 blackpearl Server** item in the Start menu (under Start > All Programs > K2 blackpearl) and select **Run as...**
5. Select **The following user** option, and type in the domain\K2 Service Account as the User Name and password, and click OK

The K2 Server will start and initialize. You will see several messages starting the various components. Once you see the line stating "Info 7010 MSMQ Thread Listing", you know the service has started successfully.

6. Next, open Internet Explorer from the K2 Server machine. Access the K2 Workspace home page. You should see the K2 Workspace home page, with no items available in the worklist:



7. Also, you should see a message in the K2 Server console window showing that Kerberos was used for authentication:

```

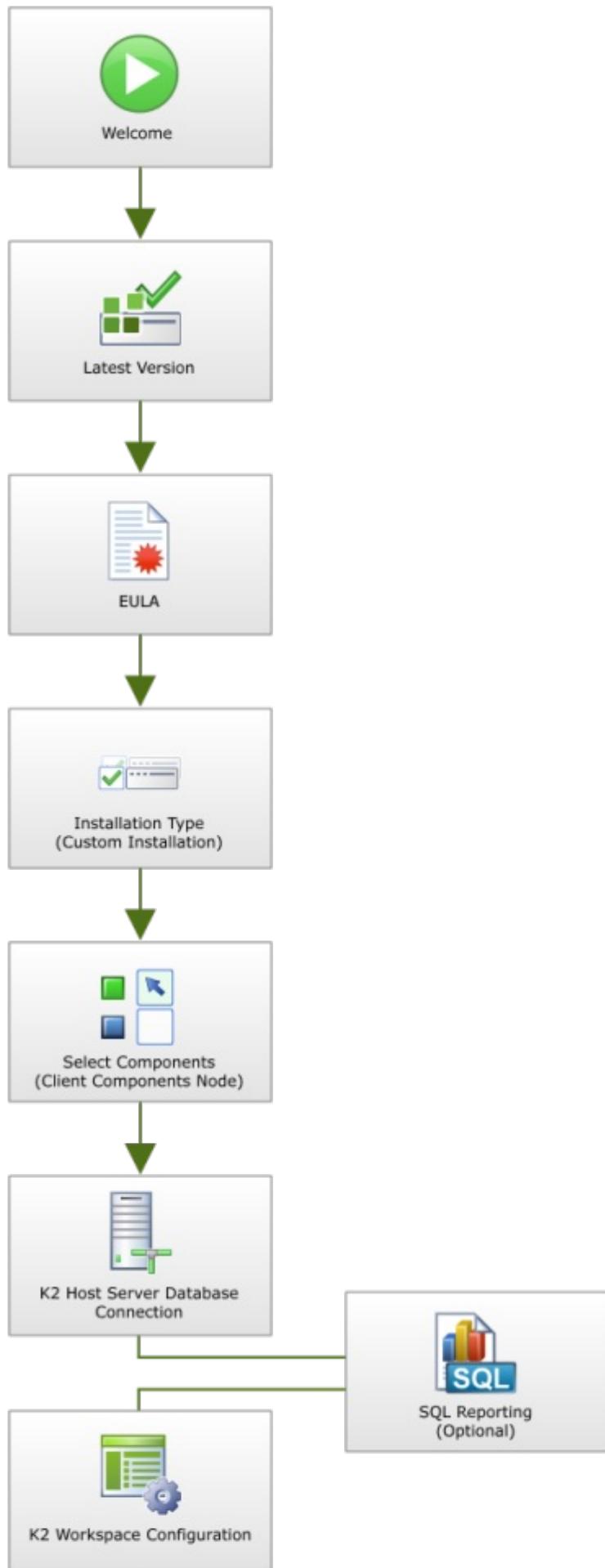
Info 27120 K2 Server was successfully started
Info 10000 SmartObject Runtime Server starting up.....
Info 10001 SmartObject Runtime Connecting to Store Database on K2TRAINSQL ...
Info 10003 SmartObject Runtime successfully connected to Database on K2TRAINSQL
Info 10004 SmartObject Runtime Store using integrated security.
Info 10021 SmartObject Runtime Event Handler initialized successfully.
Info 10019 SmartObject Object Factory initialized with cache time of 0
Info 10019 SmartObject Runtime Server successfully initialized and running.
Info 2004 All Dependencies Loaded
Info 2021 Assembly Execution Path successfully updated
Info 2023 Loading Event Bus Server
Info 2005 Configuration settings initialized
Info 2032 Initialization Check Successful
Info 7013 Service registered with ID:5 running on machine: K2TRAINH2-01
Info 7022 Event Bus Server Loaded Successfully
Info 7018 MSMQ Thread Listing
Info 1020 Starting Session BSB1B54AA449761151C0E99F111CE989
Info 3000 Authenticating K2TRAIN\Administrator for session BSB1B54AA449761151C0E99F111CE989
Info 10514 Name: SourceCode.SmartObjects.Running Version: 4.7.05.1.0 Date:
e: '11/12/2007 8:32:10 AM'
Info 1025 Ending Session BSB1B54AA449761151C0E99F111CE989

```

Be sure to see the section on Post installation common tasks once done with the install.



1.6.3.3.1 K2 Workspace Install Flow Diagram





1.6.3.4 Install K2 for SharePoint component on the SharePoint Server

Install K2 for SharePoint on the SharePoint server

See these sections of this topic too:

Set SPNs for the SharePoint Service Account

Configure SharePoint to use Kerberos

Validate the K2 for SharePoint Component

Prerequisites



The SharePoint Server role is defined to be the server on which the K2 for SharePoint component will be installed, and is already running either Microsoft Office SharePoint Server 2007, Windows SharePoint Services 3.0, SharePoint 2010 Foundation or SharePoint Server 2010. The K2 for SharePoint component, configuration manager, and K2 documentation will be installed on this server.

The SharePoint Server role requires the following prerequisites:

K2 blackpearl Prerequisites for the SharePoint Server	
Operating System	<ul style="list-style-type: none"> • * ** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 <ul style="list-style-type: none"> *Latest security patches *32-bit and 64-bit support
Windows Components	<ul style="list-style-type: none"> • IIS 7.0 with IIS 6.0 Compatibility or IIS 7.0 Management Tools or IIS 8 Manager • Distributed Transaction Coordinator (DTC) • IPv4 (IPv6 can exist, but IPv4 must also be configured) • ASP.NET • Windows Authentication Role Services
Additional Software	<ul style="list-style-type: none"> • Microsoft .NET Framework 4 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=ab99342f-5d1a-413d-8319-81da479ab0d7 • Microsoft Windows SharePoint Services 3.0 (WSS) SP2 or Microsoft Office SharePoint Server 2007 (MOSS) Standard, Enterprise SP3 or SharePoint 2010 Foundation or SharePoint 2010 Foundation SP1 or SharePoint Server 2010 or SP1 or SharePoint Server 2013 (supported for upgraded Sites still in compatibility mode) • SharePoint Foundation 2010 Client Side Object Model Redistributable (required for CSOM Service Broker and is installed on the K2 Server) • Microsoft Report Viewer Redistributable 2008 SP1 http://www.microsoft.com/downloads/details.aspx?FamilyID=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=en • Microsoft Internet Explorer 8 or 9 or Microsoft Internet Explorer 10 (Plug-in support is only available in Internet Explorer on the desktop, and this version of Internet Explorer 10 must be used for items built in Silverlight, such as the K2 Designer for SharePoint). • Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en • Visual Studio 2010 Web Deployment Projects (required for Forms Technology): http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24509

Rights and Permissions

The SharePoint Service Account is the account that the SharePoint application pool will run under. This account probably already exists in your environment, but there are some permissions that should be validated to ensure that the K2 integration with SharePoint functions properly.

The rest of this guide will use domain\SharePoint Service Account as a placeholder for the SharePoint Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

The SharePoint Service Account will need the following permissions:

SharePoint Server	
Rights	Folder or Registry Key
Modify	%SYSTEMROOT%\temp
Write	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\Layouts\Features
Write	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\ISAPI



Note that the \12\ in the folders mentioned above will be \14\ on a Microsoft SharePoint Server 2010 system.

SQL Server	
Permission	Used For
db_DataReader on the K2WebDesigner database	For the K2 Designer for SharePoint to function properly, the SharePoint Service Account needs read permission on this database.
db_DataWriter on the K2WebDesigner database	For the K2 Designer for SharePoint to function properly, the SharePoint Service Account needs write permission on this database.
Execute on Stored Procedures in the K2WebDesigner database	<p>For the K2 Designer for SharePoint to function properly, the SharePoint Service Account needs to be able to execute the Stored Procedures on this database. The easiest way to do this is to create a new role (i.e., db_executor), grant stored procedure execute rights to that role, and assign the SharePoint Service account to that role.</p> <p>Here is an example script for creating the role.</p> <pre>/* select K2WebDesigner database */ use K2WebDesigner /* create a new role */ create role db_executor /* grant execute to the role */ grant execute to db_executor</pre>

Authenticated Users	
Rights	Folder or Registry Key
Modify	C:\Users and all folders below. (Applicable to Windows 2008 Servers). Apply this to all SharePoint Web Front Ends



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Kerberos / Pass Through Authentication

When components are installed on separate servers, credentials must be passed between the services. This can be accomplished by setting up **Kerberos**, which should be configured prior to installing K2. Any time where two or more hops are required for user authentication, Kerberos must be configured.

Pass Through Authentication is a K2 proprietary authentication methodology specifically for authenticating users whose credentials need to be passed between machines that interact with the K2 APIs. This authentication model can be used as an alternative to Kerberos, but is not in any way intended to be a replacement for Kerberos within the overall infrastructure.

Install Steps

After you have installed all the **prerequisites**, created the **service accounts**, and **enabled DTC**, you are now ready to install the K2 for SharePoint component.

Once the installation is done, the **Configuration Analysis tool** will be available to help troubleshoot any errors detected during the installation.



It is important to copy the installation files locally to the server before installing. Do not install from a network share or UNC path. The installation will not work properly.



It is recommended to install all K2 components using either the K2 Service Account or the Central Administration Application Pool User. Log on to the server as the K2 Service Account or Central Administration Application Pool User before installing. When using a SharePoint Farm environment, the K2 for SharePoint component must be installed on each SharePoint Server in the Farm.

Important note: Run the installer on the Central Administration server first and then on all the web front ends in the SharePoint farm BEFORE starting the [K2 for SharePoint Configuration Wizard](#) on the Central Administration server.

To install the K2 for SharePoint component, follow the below steps:

- 1
- 2
- 3
- 4
- 5

- From the local installation folder, double-click on the **Setup.exe** file
- On the **Welcome** screen, click Next
- On the **End User License Agreement** screen, read through the EULA. You must select the **I agree** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next
- On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder, and click Next
- On the **Select Components** screen, you should see that the components for which the prerequisites are met are:
 - K2 blackpearl Server,
 - K2 Workspace,
 - K2 for SharePoint (MOSS or WSS),
 - K2 Designer for SharePoint
 - K2 Documentation, and
 - K2 blackpearl Setup Manager

You will want to **uncheck** the box next to K2 blackpearl Server and the K2 Workspace, as you will not be installing the K2 Server or Workspace on this machine. You will also see a link to Check Dependencies for the other components.



If you want to install one of the components on this server that have a Check Dependencies action, cancel the installation and fix the dependency. Then, restart the installation and you should be able to select that component.

- 6
- 7
- 8
- 9

- On the **HostServer Database** screen, type in the name of the SQL Server where you installed the K2 Databases. This points the K2 for SharePoint component to the HostServer database set up by the K2 Server, to share configuration information. If you changed the Host Server database name, update it here and click Next.
- On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Install.
- The Setup Manager will update and show you the progress of the components as it installs.
- When the installation has completed, you will see a finished screen. There will also be a link to the created configuration log file as well as an option to launch the SharePoint Configuration, see the topic [K2 for SharePoint Configuration Wizard](#) in the Integration Configuration > SharePoint section of this help file.

SharePoint Service Account

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order for the K2 Worklist Web Part and K2 Designer for SharePoint to function properly from another machine, you

need to set the SPNs for the SharePoint Service Account.

The following placeholders are used in the commands:

- domain\SharePoint Service Account - The SharePoint Service Account that runs the SharePoint application pool
- MachineName - The name of the computer on which SharePoint Service is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the SharePoint Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have SharePoint running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.



If you are using **Host Headers** to access your SharePoint Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\SharePoint Service Account
- setspn -A HTTP/MachineName.FQDN domain\SharePoint Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\SharePoint Service Account

Configure for Delegation

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.



Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)



Find the domain\SharePoint Service Account and view its properties



On the Delegation tab, select the **Trust this user for delegation to specified services only** option

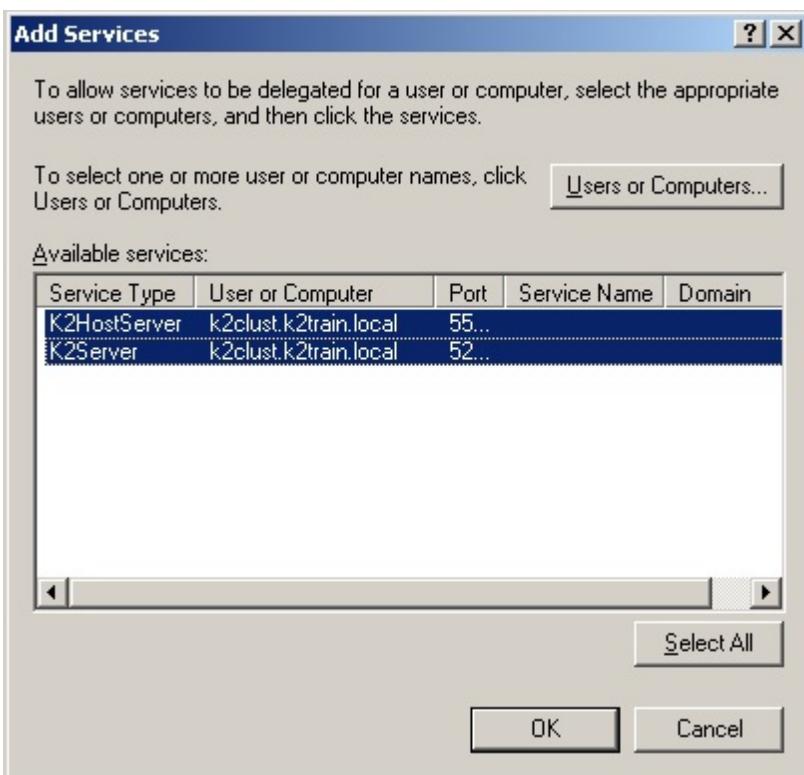


Select the **Use Kerberos only** option, and click on **Add**

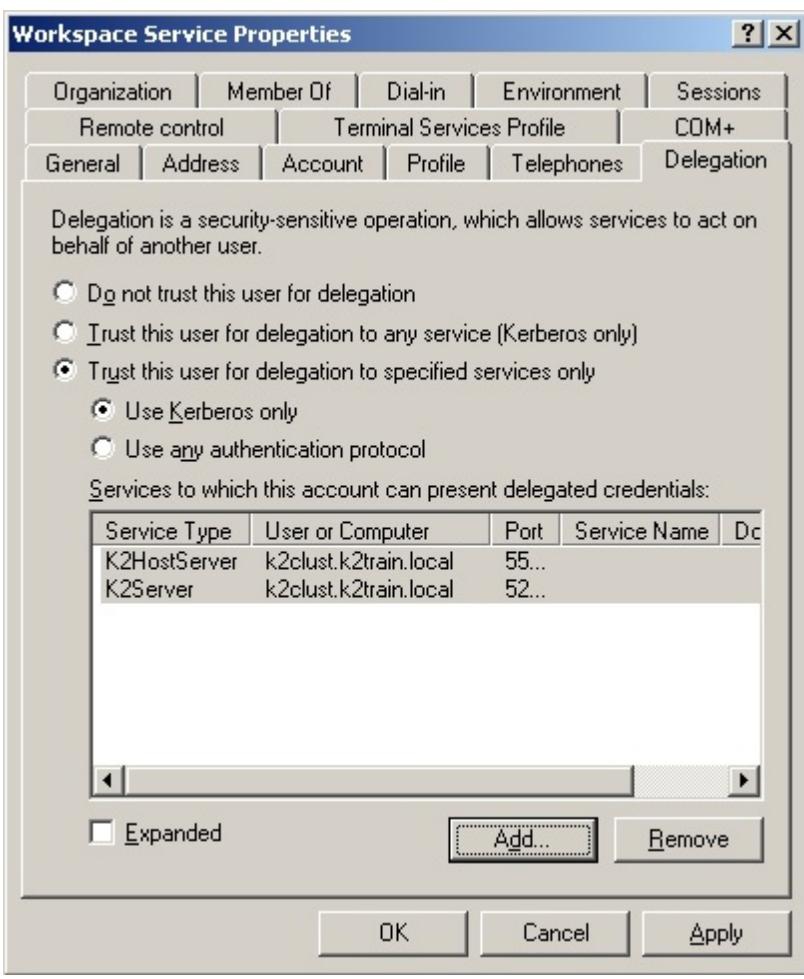


Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account

In the Available Services section, select both the **K2HostServer** and **K2Server** items listed:



Click **OK**. Your properties should resemble the following:





- 8 Click **Add** again
- 9 Click on **Users or Computers** and select the domain\K2 Workspace Account you created as the K2 RuntimeServices Account
- 10 In the Available Services section, select the HTTP item listed
- 11 Click **OK**. This will allow the SharePoint Service Account to delegate to the K2 Workspace Account.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Configure SharePoint to use Kerberos

In a distributed environment where components are installed on more than one server or if host headers are used, Kerberos security must be configured. One of the components of Kerberos is the Service Principal Name (SPN). Whenever user credentials must be passed from one system to another, the system that is attempting to pass the credentials must be trusted for delegation. For this step to take place successfully, Kerberos delegation must be configured.



Configuring SPNs is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Set SPNs

In order for the K2 Worklist Web Part and K2 Designer for SharePoint to function properly from another machine, you need to set the SPNs for the SharePoint Service Account.

The following placeholders are used in the commands:

- domain\SharePoint Service Account - The SharePoint Service Account that runs the SharePoint application pool
- MachineName - The name of the computer on which SharePoint Service is running
- MachineName.FQDN - The fully qualified domain name of the computer on which the SharePoint Service is running



Be sure to set all the SPNs as listed below. Also, the service account is required so be sure to specify the account properly.



If you have SharePoint running on a cluster, be sure to use the name of the cluster and the fully qualified cluster name instead of a single node's machine name.



If you are using **Host Headers** to access your SharePoint Service, use the HostHeader value instead of the MachineName in the below commands. An SPN for each Host Header will need to be created.

Open a command prompt on a server that has the Windows Support Tools installed, and execute the following commands:

- setspn -A HTTP/MachineName domain\SharePoint Service Account
- setspn -A HTTP/MachineName.FQDN domain\SharePoint Service Account

After the commands have successfully executed, you can verify the SPNs were set by executing the following command:

- setspn -L domain\SharePoint Service Account

Configure for Delegation

After the SPN has been set, a new Delegation tab is available in Active Directory Users and Computers for the Service Account. By default, the option selected is the Do not trust this user for delegation. You need to set the account to be trusted for delegation, by following the below steps:



If you are running your Active Directory domain in Windows 2000 native mode, the Delegation tab will not be present. Instead, on the **Account** tab, you will see a Trust this user for delegation check box.

- 1**
- 2**
- 3**
- 4**
- 5**
- 6**

Open **Active Directory Users and Computers** (Start > All Programs > Administrative Tools > Active Directory Users and Computers)

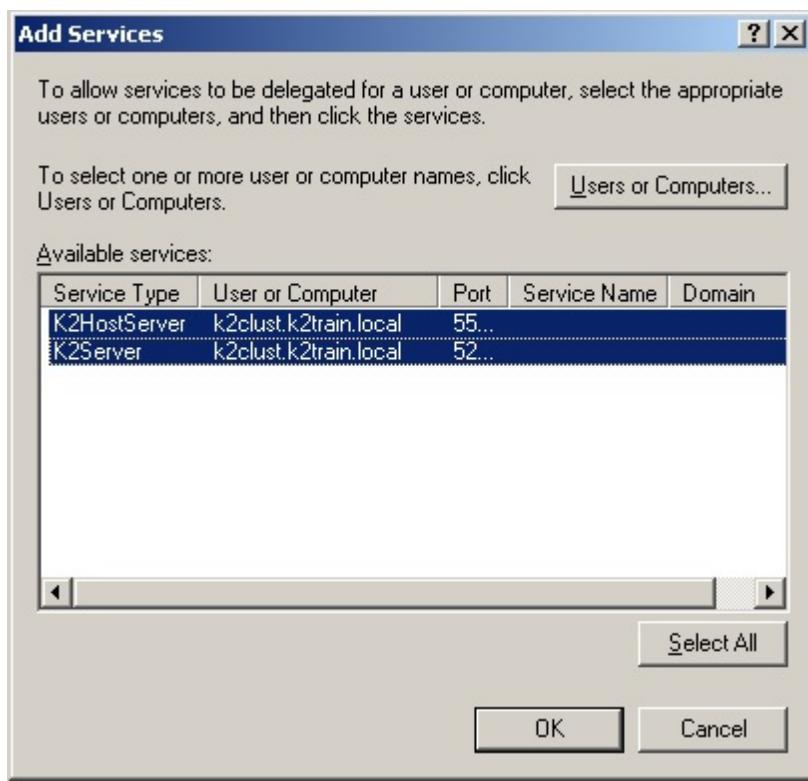
Find the domain\SharePoint Service Account and view its properties

On the Delegation tab, select the **Trust this user for delegation to specified services only** option

Select the **Use Kerberos only** option, and click on **Add**

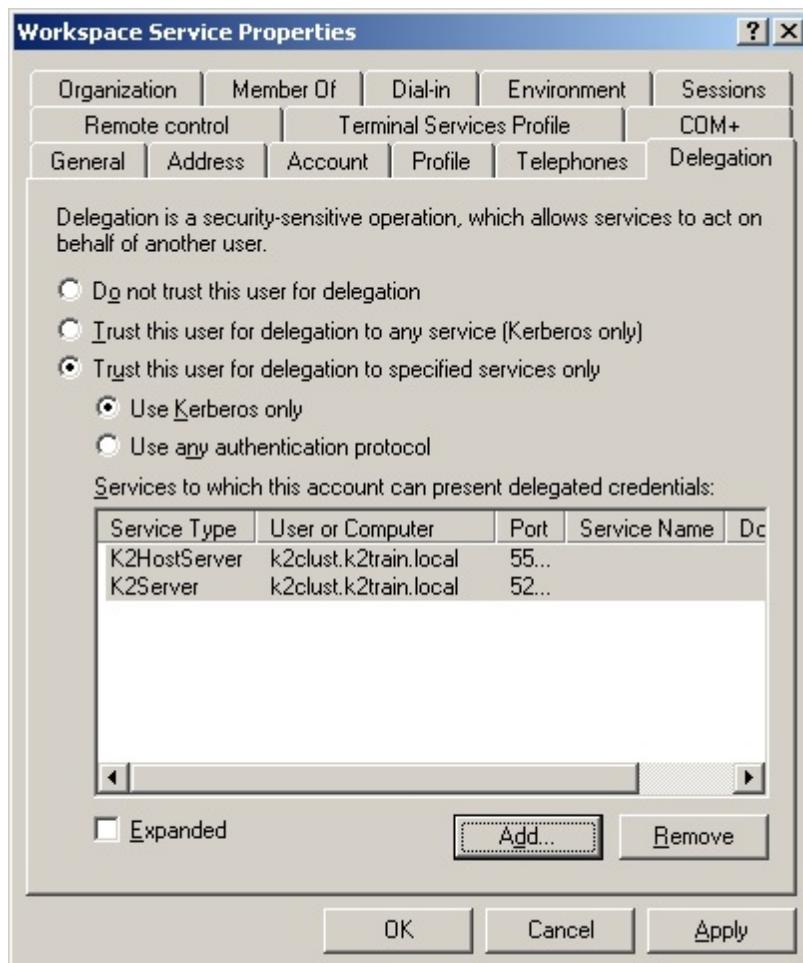
Click on **Users or Computers** and select the domain\K2 Service Account you created as the K2 Server Service Account

In the Available Services section, select both the **K2HostServer** and **K2Server** items listed:



(7)

Click **OK**. Your properties should resemble the following:



(8)

Click **Add** again

(9)

Click on **Users or Computers** and select the domain\K2 Workspace Account you created as the K2 RuntimeServices Account

(10)

In the Available Services section, select the HTTP item listed

(11)

Click **OK**. This will allow the SharePoint Service Account to delegate to the K2 Workspace Account.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

Validate the K2 for SharePoint component

After installing and configuring the K2 for SharePoint component, you can check a few things to ensure that the component was set up properly:

1. Open Windows explorer and navigate to **C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\FEATURES**. You should see several K2 folders for the various K2 features.

To validate that the **K2 Designer for SharePoint** has installed:

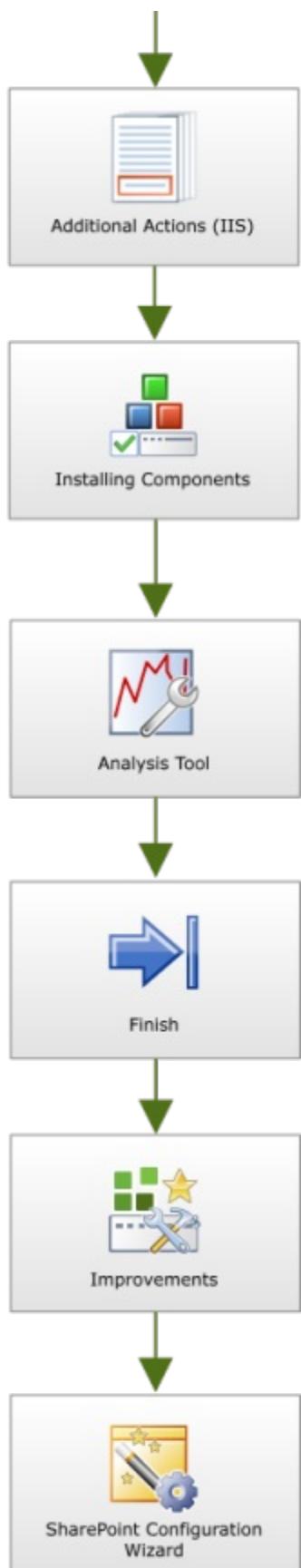
1. Browse to the **SharePoint Central Administration > K2 for SharePoint tab > K2 Designer for SharePoint** link
2. The **Activate Feature** page will be displayed. Activate the K2 Designer for SharePoint feature if needed.



Be sure to see the section on Post installation common tasks once done with the install.

1.6.3.4.1 K2 for SharePoint Component Flow Diagram





1.6.3.5 Installing the Client Components

1.6.3.5.1 Install the K2 for Visual Studio component

Install the K2 for Visual Studio component



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Prerequisites



K2 for Visual Studio

The K2 for Visual Studio component installs the K2 Designer for Visual Studio. This designer allows developers to use a tool they are familiar with (Visual Studio) to develop, design, and deploy K2 applications. The K2 for Visual Studio component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 for Visual Studio component	
Operating System	<ul style="list-style-type: none"> • * ** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 • Microsoft Windows Vista with SP1 or SP2 (Business or Ultimate) or Windows 7 with or without SP1 or Microsoft Windows 8 (Windows 8 / Pro / Enterprise) <p>*Latest security patches *32-bit and 64-bit support</p>
Additional Software	<ul style="list-style-type: none"> • Microsoft .NET Framework 4 (.NET Framework 4.5 is supported but not required): For more information on .NET framework and K2, please see the topic: .NET Technologies • Microsoft Visual Studio 2010 (Professional / Premium / Ultimate) with or without Sp1 • A User Manager: Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. • Windows Powershell • Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a266aae9df&displaylang=en • OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx • Excel Web and Calculation Services with Trusted file locations for Excel spreadsheets or Microsoft SharePoint Server 2010 and Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets

You can validate that you have the appropriate extensions installed by going into Visual Studio and selecting Help > About. You should see the following extensions listed:

- Extensions for Windows WF

Install Steps

After you have installed all the **prerequisites**, you are now ready to install the K2 for Visual Studio component.



It is important to copy the installation files local to the server before installing. Do not install from a network share or UNC path. The installation will not work properly.



It is recommended to install this component on the client machine with an account with Local Administrator rights.

To install the K2 for Visual Studio component, follow the below steps:



From the local installation folder, double-click on the **Setup.exe** file



On the **Welcome** screen, click Next



On the **End User License Agreement** screen, read through the EULA. You must select the **I agree** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next



On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder, and click Next



On the **Select Components** screen, you should see that the only components for which the prerequisites are met are:

- K2 for Visual Studio,
- K2 Documentation, and
- K2 blackpearl Setup Manager

There may be additional components available depending on what is installed on your client machine. You will want to **uncheck** the box next to the other components.



Once you have verified the components, click Next



On the **Client Components** screen, you can select from the following options for the connection to an environment:



The environment refers to an Environment Library, which is used for storing all information about your various environments (such as server names, URLs, SharePoint Servers and sites) external to the process. This allows users to easily build the same process for any of the available environments configured without needing to rework the process by changing these common variables.

- **Connect to an existing environment.** This allows you to select an existing HostServer Database to connect to. On the next page, you will see the HostServer Database screen, where you can connect to a database to use its configuration information.
- **Manually configure an environment.** This allows you to type in a K2 Server name to connect to. On the next page, you will see the K2 blackpearl Server Configuration screen, where you can type in a Server Name and the ports.



On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Install.



The Setup Manager will update and show you the progress of the components as it installs.



When the installation has completed, you will see a finished screen. There will also be a link to the created configuration log file. When you click Finish, you will be prompted to restart now (click Yes) or restart later (click No). It is important to restart in order to complete the installation and configuration of K2 blackpearl.



Be sure to see the section on Post installation common tasks once done with the install.

1.6.3.5.2 Install the K2 Studio component

Install the K2 Studio component



Download: You can download an Excel Workbook to help you organize your K2 blackpearl installation by [clicking here](#). Use this checklist to ensure that all topics have been read, understood and implemented successfully before, during and after K2 blackpearl installation. The checklist includes all possible items for both Standalone and Distributed installations. Please read the Reference Topic to determine if the item applies to your environment.

There is also a worksheet where users can record their configured settings as reference.

Prerequisites



The K2 Studio component installs the K2 Designer for Visual Studio. This designer allows developers to use a tool they are familiar with (Visual Studio) to develop, design, and deploy K2 applications. The K2 Studio component requires the following prerequisites:

K2 blackpearl Prerequisites for the K2 Studio component	
Operating System	<ul style="list-style-type: none"> • * ** Microsoft Windows Server 2008 Standard, Enterprise SP2 or Microsoft Windows 2008 R2, RTM and SP1 or Windows Server 2012 • Microsoft Windows Vista with SP1 or SP2 (Business or Ultimate) or Windows 7 with or without SP1 or Microsoft Windows 8 (windows 8 / Pro / Enterprise) <p>*Latest security patches *32-bit and 64-bit support</p>
Additional Software	<ul style="list-style-type: none"> • Microsoft .NET Framework 4 or Microsoft .NET Framework 4.5
 For more information on .NET framework and K2, please see the topic: .NET Technologies • Active Directory Server (Windows 2000 Functional Level or greater). The default User Manager is Active Directory (AD), but a custom user manager may be configured for use with K2 blackpearl. • Microsoft Exchange Server 2007 SP3 (required for Exchange Wizard) or Microsoft Exchange Server 2007 Management Tools SP3 or Microsoft Exchange 2010 SP1 or Microsoft Exchange 2010 SP2 • Windows Powershell • Microsoft Dynamics CRM 4.0 SDK or Microsoft Dynamics CRM 2011 and CRM 2011 Redistributable (installed on the K2 Server) http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en • OpenXML SDK 2.0 Redistributable (required for Inline Functions) http://msdn.microsoft.com/en-us/office/bb265236.aspx • Microsoft Office SharePoint Server (MOSS) 2007 SP3 <ul style="list-style-type: none"> • Excel Web and Calculation Services • Trusted file locations for Excel spreadsheets • Microsoft SharePoint Server 2010 RTM or SP1 • Excel Services Application (only available in SharePoint 2010 Enterprise and MOSS 2007) with Trusted file locations for Excel spreadsheets • Either Visual Studio 2012 or Visual Studio 2010 Web Deployment Projects is required to deploy projects in K2 Studio (http://www.microsoft.com/en-us/download/details.aspx?id=25163) <p>Windows SDK v7.0A is required when the 'Generate ASP Pages' option is used. This is installed and configured when Visual Studio 2010 or 2012 is installed.</p>

You can validate that you have the appropriate extensions installed by going into Visual Studio and selecting Help > About. You should see the following extensions listed:

- Extensions for Windows WF

Install Steps

After you have installed all the [prerequisites](#), you are now ready to install the K2 Studio component.



It is important to copy the installation files local to the server before installing. Do not install from a network share or UNC path. The installation will not work properly.



It is recommended to install this component on the client machine with an account with Local Administrator rights.

To install the K2 Studio component, follow the below steps:



Be sure to see the section on Post installation common tasks once done with the install.



From the local installation folder, double-click on the **Setup.exe** file



On the **Welcome** screen, click Next



On the **End User License Agreement** screen, read through the EULA. You must select the **I agree** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next



On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder, and click Next



On the **Select Components** screen, you should see that the only components for which the prerequisites are met are:

- K2 Studio,
- K2 Documentation, and
- K2 blackpearl Setup Manager

There may be additional components available depending on what is installed on your client machine. You will want to **uncheck** the box next to the other components.



Once you have verified the components, click Next



On the **Client Components** screen, you can select from the following options for the connection to an environment:



The environment refers to an Environment Library, which is used for storing all information about your various environments (such as server names, URLs, SharePoint Servers and sites) external to the process. This allows users to easily build the same process for any of the available environments configured without needing to rework the process by changing these common variables.

- **Connect to an existing environment.** This allows you to select an existing HostServer Database to connect to. On the next page, you will see the HostServer Database screen, where you can connect to a database to use its configuration information.
- **Manually configure an environment.** This allows you to type in a K2 Server name to connect to. On the next page, you will see the K2 blackpearl Server Configuration screen, where you can type in a Server Name and the ports.



On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Install.



The Setup Manager will update and show you the progress of the components as it installs.



When the installation has completed, you will see a finished screen. There will also be a link to the created configuration log file. When you click Finish, you will be prompted to restart now (click Yes) or restart later (click No). It is important to restart in order to complete the installation and configuration of K2 blackpearl.

1.6.3.6 Distributed Installation of K2 View Flow via Group Policy

Installation of K2 View Flow via Group Policy

Distributing packages via Group Policy can be done on Computer or User levels. On a Computer level the software can be installed per computer on your domain. However, you would then need to assign rights for each computer. We recommend that you use the User level and create a group of the users that will require the installation. The following instructions apply to a user level If you wish to use the computer level please refer to the links at the bottom of this topic.

Creating a Group for the View Flow Users

Create an AD Group that contains all the users that will require access to the view flow. This group will be referred to as **K2ViewFlowUsers** in this article.

Extracting the View Flow MSI and creating a shared folder

Find the K2ViewflowDeployer.cab and extract it to a folder on the Domain controller server.

This file is located in one of the two places below:

1. MOSS/WS install location:
C:\Program Files\Common Files\microsoft shared\Web Server Extensions\12\TEMPLATE\LAYOUTS\K2\TaskList\K2ViewflowDeployer.cab
2. From a Workspace install location:
C:\Program Files\K2 blackpearl\WorkSpace\Site\TaskListControl\K2ViewflowDeployer.cab

Share this folder and give read access to the K2ViewFlowUsers group. Also modify the security settings on this folder and give read access to the K2ViewFlowUsers group.

Creating a Group Policy Object (GPO) and assigning the K2 View Flow Software installation package

The policy will take time to update on the clients. If you wish to fast track this you can run the gpupdate /force command on the client

Useful Links

Creating a group policy object (Window Server 2008)

[http://technet.microsoft.com/en-us/library/cc947817\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc947817(WS.10).aspx)

Troubleshooting Event Log entries relating to Group policy deployment

[http://technet.microsoft.com/en-us/library/cc727267\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc727267(WS.10).aspx)

- 
- 1 Click on the Start button, select Administrative Tools and then select Group Policy Management
 - 2 Right-click your domain name in the console tree and Create a GPO in this domain and Link it here...
 - 3 Type in a name for example "K2ViewFlowGPO" and select (none) for the Source Starter GPO
 - 4 Expand Group Policy Objects and right click on the GPO you just created
 - 5 Under GPO Status select "All Settings Disabled"
 - 6 On the right panel under Security Filtering Add the K2ViewFlowUsers group
 - 7 Right click the GPO again and click Edit
 - 8 Under User Configuration expand Policies
 - 9 Expand Software Settings
 - 10 Right Click Software installation

- (11) Click New
- (12) Click Package
- (13) Type in the UNC path of the share created under Extracting the View Flow MSI and creating a shared folder
- (14) Select K2ViewFlow
- (15) Choose Assigned
- (16) On the right panel right click the K2 View Flow item
- (17) Click the Deployment Tab
- (18) Check the box stating Install this application at logon
- (19) Select Basic under Installation user interface options
- (20) Close the Group Policy Management Editor window
- (21) Under Group Policy Objects in Group Policy Management
- (22) Right Click the GPO
- (23) Under GPO Status select "Enabled"

1.6.4 Post installation common tasks

1.6.4.1 Required Permissions in K2 blackpearl

Required Permissions for K2 Components



Changing the permission level does not remove users who already have rights on the K2 Server. Use Management Console to remove these users.

Feature	Task	SharePoint Site Server Rights	K2 blackpearl Server Rights	Windows / Other Rights
K2 Server	Send receive emails	N/A	N/A	Access to a mail account, user name and password
K2 Studio	Create Workflow	N/A	N/A	Write access to where you are saving the process
K2 Studio	Deploy Workflow	N/A	Export Rights	N/A
Process Portals	Create Process Portal	Manage Hierarchy on the top site where the Process Portal is created	N/A	N/A
Process Portals	Access Process Portal	At least Read rights on the Process Portal	N/A	N/A
Process Portals	Management Worklist	At least Read rights on the Process Portal	Admin on the Process	N/A
Process Portals	Reports	At least Read rights on the Process Portal	View Part or View rights on the Process	N/A
Process Portals	View Reports	At least Read rights on the Process Portal	Process Admin, Process View, Process View Participate	N/A
Process Portals	Instance Management (including Instances Summary)	At least Read rights on the Process Portal	View rights on the Process	N/A
Process Portals	Instances Summary Web Part	At least Read rights on the Process Portal	Server Admin, Admin on the Process, Process View	N/A
Process Portals	Start Process Instance	At least Read rights on the Process Portal	Admin on the Process, Start Process	N/A
Process Portals	Add Process to Portal	At least Contributor rights on the Process Portal	Server Admin, Admin on the Process	N/A
Process Portals	Process Instances	At least Read rights on the Process Portal	Server Admin, Admin on the Process, Process View	N/A
Process Portals	Process Management - View Detail	At least Read rights on the Process Portal	Server Admin, Admin on the Process	N/A
Process Portals	Process Management - View Detail - Roles	At least Read rights on the Process Portal	Server Admin, Admin on the Process	N/A
Process Portals	Process Management – Perform Action – Roles	At least Read rights on the Process Portal	Server Admin, Admin on the Process	N/A
Process Portals	Process Instances - View Detail	At least Read rights on the Process Portal	Server Admin, Admin on the Process, Process	N/A

			View	
Process Portals	Process Instances - Perform Action	At least Read rights on the Process Portal	Server Admin, Admin on the Process	N/A
Process Portals	Administration	At least Read rights on the Process Portal	Admin for the K2 Server	N/A
Process Portals	Settings (including show/hide/adding process)	At least Read rights on the Process Portal	View Part or View rights on the Process	N/A
Process Portals	Processes Web Part	At least Read rights on the Process Portal	Admin for the K2 Server, Process Admin	N/A
Process Portals	View landing page - Processes Web part or Management Worklist	At least Read rights on the Process Portal	Admin for the K2 Server, Process Admin	N/A
Process Portals	Administration Links (Central/Site)	At least Read rights on the Process Portal	Admin for the K2 Server	N/A
Process Portals	Process Scheduler	N/A	The K2 Service Account requires Start rights on the Process that is being scheduled to start	N/A
K2 Designer for SharePoint	See the K2 Web Designer Menu item in the List Settings menu	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Create New Workflow	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Edit a workflow	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Reuse one of my workflows	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Reuse a shared workflow	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Save Template	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Publish a workflow	Default is SharePoint Owners Group or specify a group under K2 site settings	N/A	N/A

K2 Designer for SharePoint	Export a workflow	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	Write access to where you are exporting to
K2 Designer for SharePoint	Share a workflow	Default is SharePoint Members Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Start a Workflow on Form Library	Rights to access the Form	Start rights on the Process	N/A
K2 Designer for SharePoint	Start a Workflow on a List or Document Library	Rights to access the document in the library	N/A	N/A
K2 Designer for SharePoint	Submit a workflow for approval	Default is SharePoint Owners Group or specify a group under K2 site settings	N/A	N/A
K2 Designer for SharePoint	Approve a workflow	Specified under K2 site settings	Be assigned an Approve workflow task by the Out of the Box process	N/A
InfoPath Integration	Start a workflow	Contributor on the library	Start rights on the Process	N/A
InfoPath Integration	Deploy an InfoPath Process	Contributor rights on SharePoint Site	Export Rights	N/A
InfoPath Integration	Destination user retrieves and updates the temp XML file	Contribute rights on the site	N/A	N/A
SharePoint Workflow Integration	Start a workflow	Contributor on the list or library	Start rights on the Process	N/A
SharePoint Workflow Integration	K2 Service Account Rights Needed	Full Control on the list or library	Impersonate on the K2 Server	N/A
SharePoint Workflow Integration	SharePoint Service Account Rights Needed	Full Control on the list or library	Impersonate on the K2 Server	N/A
K2 Process Management for Visual Studio	Use the Process Management tool	N/A	Admin on the Process	N/A
K2 Data Provider	Access SmartObjects	Read access to the list or library. This depends on the methods that get executed. An update, insert or delete will require contributor rights	N/A	N/A
K2 Site Settings	Events Integration Management (Activate/Deactivate)	Full control on the site	Admin Rights	N/A
K2 Site Settings	Workflow Integration Management (Activate/Deactivate)	Full control on the site	Admin Rights	N/A
K2 Site Settings	SmartObject Service Management	Read access to the list or library	Export Rights and Admin Rights	N/A
K2 for SharePoint Tab in central Admin	K2 Site Settings Link	Full control on the site collection where the feature is being	N/A	N/A

		activated; access to SharePoint Central Admin		
K2 for SharePoint Tab in central Admin	K2 for SharePoint Management Console	Full control on the site collection where the feature is being activated; access to SharePoint Central Admin	N/A	N/A
K2 for SharePoint Tab in central Admin	K2 SmartObject Service Integration	Full control on the site collection where the feature is being activated; access to SharePoint Central Admin	N/A	N/A
K2 for SharePoint Tab in central Admin	K2 Web Designer Version 2.0	Full control on the site collection where the feature is being activated; access to SharePoint Central Admin	N/A	N/A
K2 for SharePoint Tab in central Admin	K2 Workflow Integration Content Types	Full control on the site collection where the feature is being activated; access to SharePoint Central Admin	N/A	N/A
K2 for SharePoint Tab in central Admin	K2 for SharePoint tab in Central Admin	Full control on the site collection where the feature is being activated; access to SharePoint Central Admin	N/A	N/A
K2 for SharePoint tab in Central Admin	Add Settings to Site Collection	Full control on the site collection where the feature is being activated; access to SharePoint Central Admin	N/A	N/A
K2 Exchange Event Wizard	Object Browser - Exchange Server Field	N/A	The K2 Service account will need Exchange View Only Administrator rights for the Microsoft Exchange Server	N/A
K2 Exchange Event Wizard	Create Mailbox and Disable Mailbox actions	N/A	The Exchange Event should be configured to run as a service or user account with Exchange Organization Administrator rights	N/A
K2 Exchange Event Wizard	Send Meeting Request and Send Task actions	N/A	The Exchange Event should be configured to run as a service or user account with impersonation rights with NO Exchange Organization Administrator rights. The service or user account should also have a trusted server certificate from the Exchange web	N/A

			service in his Personal certificate store.	
CRM Event Wizard	Create, Update and Delete CRM Entities in the K2 Designer for SharePonit	N/A	N/A	The AppPool account used for the K2 Designer for SharePoint must have full rights on the CRM server
Active Directory Event Wizard	Create and Update Active Directory Users	See Using the AD wizard on Windows 2008 and the LDAP requirement	N/A	N/A

There are several additional permissions that should be set up prior to installing K2 blackpearl. These permissions are as follows:

Server Role	Permission
K2 Server	The K2 Service Account will need permission to Log on as a Service.
Reporting Services Server	In order to access the temporary directory during runtime, some permissions are required for all authenticated users.
IIS Server	In order to access the temporary directory during runtime, some permissions are required for all authenticated users.
SharePoint Server	In order for K2 workflow processes to be able to be deployed, some permissions are required on the SharePoint directory.

1.6.4.1.1 Configuring Log on as a Service Rights

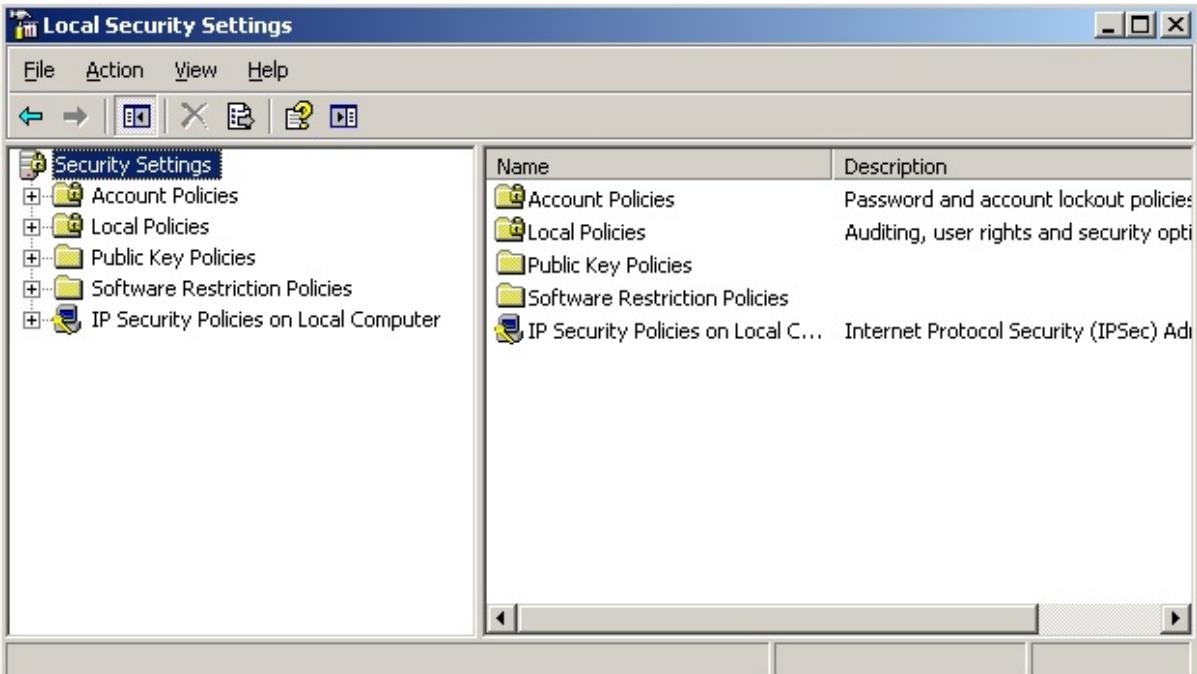
K2 Server

The K2 blackpearl service will not start automatically unless the K2 Service Account is configured to start as a service. There are two ways to grant the service account this privilege:

Using the Local Security Policy dialog:

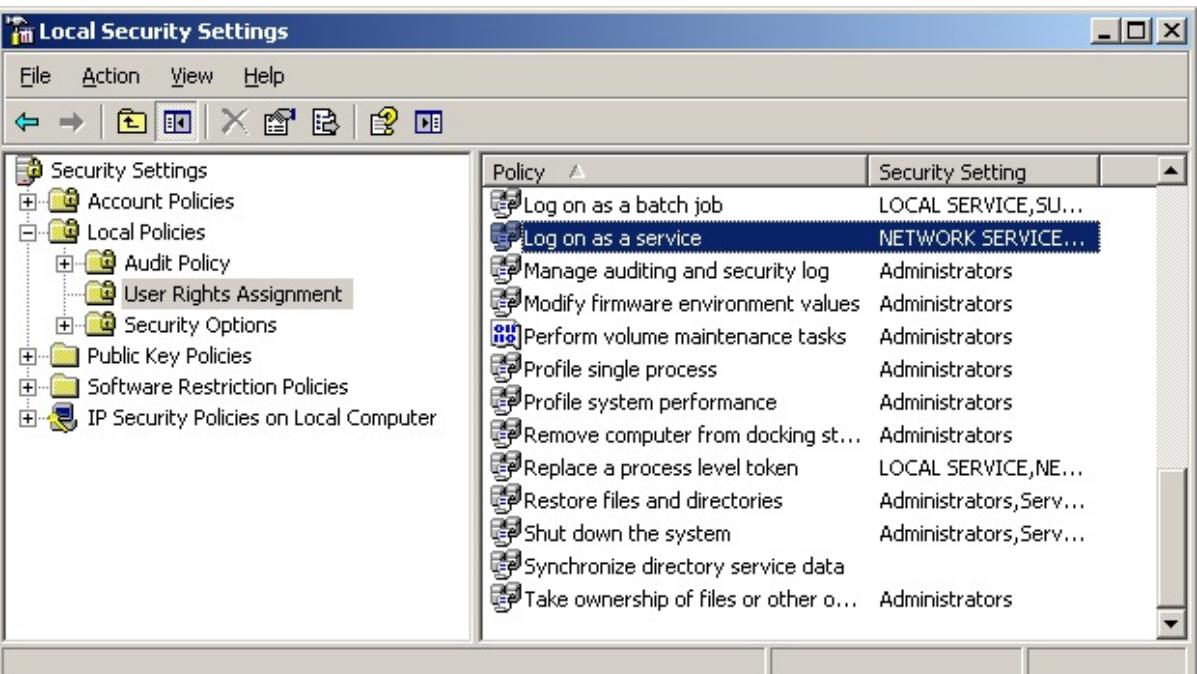
Prior to installing K2 blackpearl, you can grant the K2 Service Account this permission by performing the following steps:

① Open the dialog by clicking Start > Administrative Tools > Local Security Policy



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options
Public Key Policies	
Software Restriction Policies	
IP Security Policies on Local Computer	Internet Protocol Security (IPSec) Ad

② Expand the Local Policies node, then click on the User Rights Assignment node



Policy	Security Setting
Log on as a batch job	LOCAL SERVICE,SU...
Log on as a service	NETWORK SERVICE...
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking st...	Administrators
Replace a process level token	LOCAL SERVICE,NE...
Restore files and directories	Administrators,Serv...
Shut down the system	Administrators,Serv...
Synchronize directory service data	
Take ownership of files or other o...	Administrators

③ Locate and double-click the **Log on as a service** policy



Click the **Add User or Group** button, enter domain\K2 Service Account in the Names to select text box and click OK



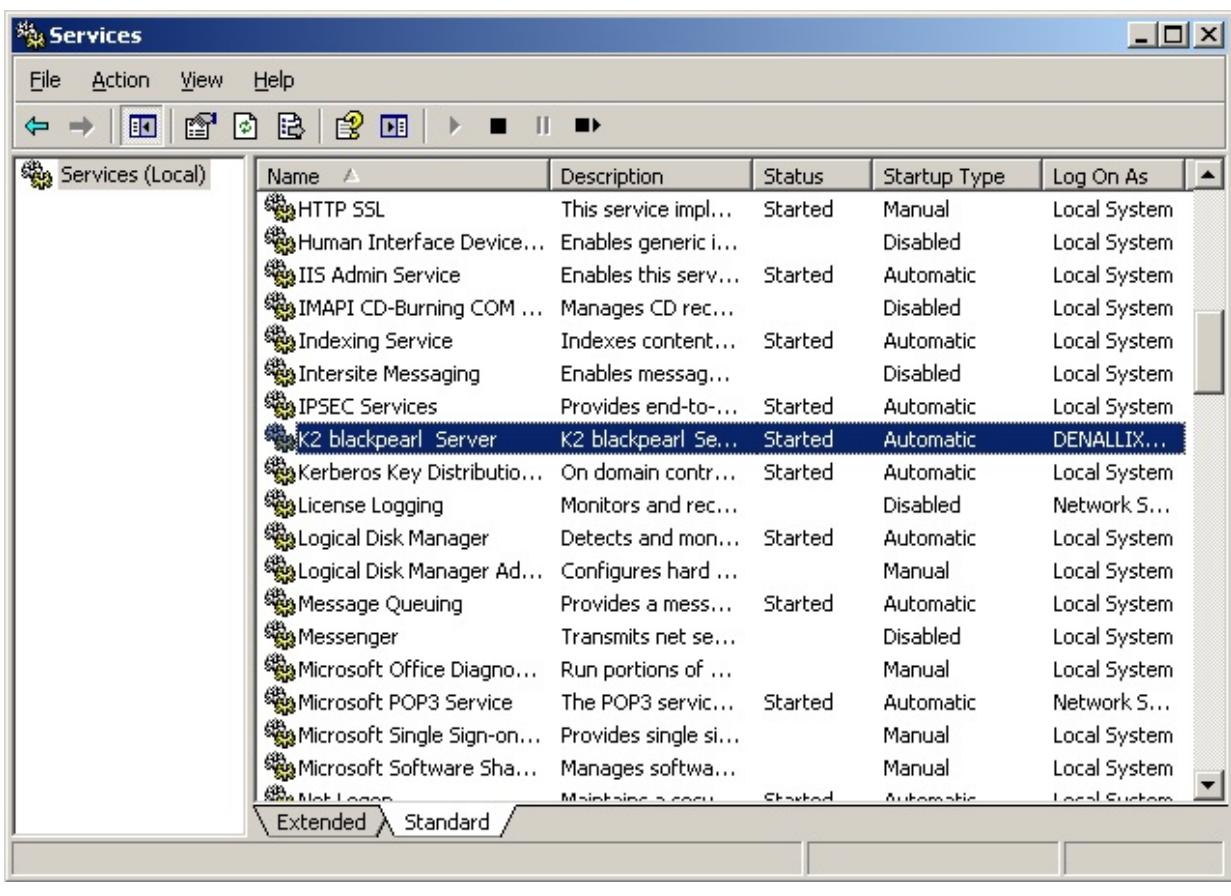
Click **OK** on the Log in as a service Properties dialog and then close Local Security Settings window

Using the Windows Services Management Console:

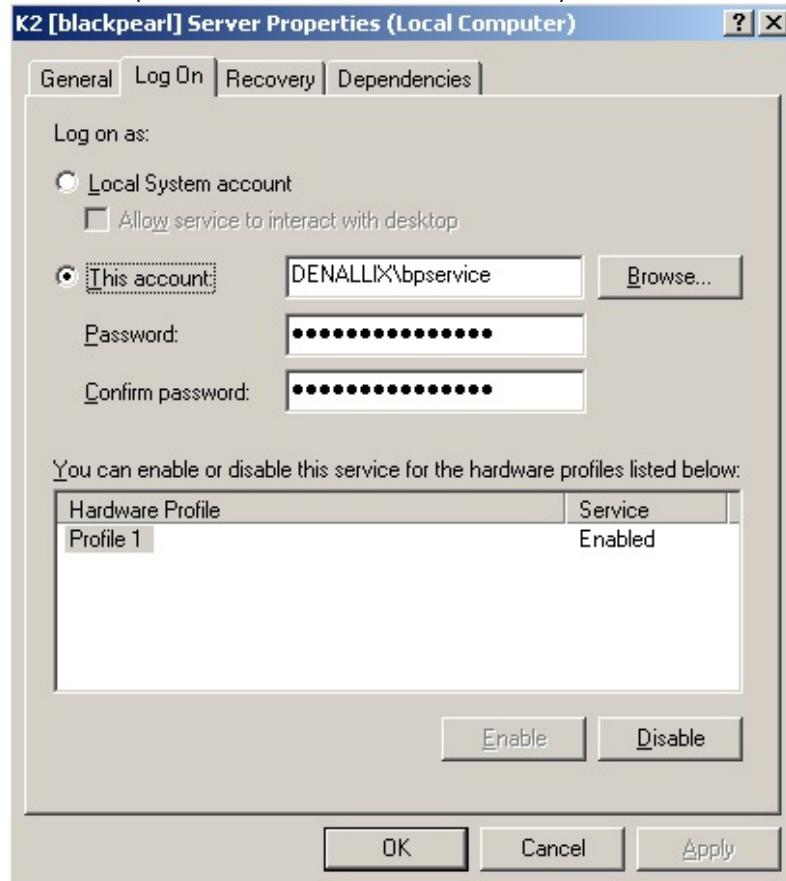
After K2 blackpearl has been installed, you will see the K2 blackpearl Server Service listed in the Services running on the K2 Server. You can then grant the Log on as a Service right by performing the following steps:



Open the Services console by clicking Start > Administrative Tools > Services



(2) Scroll down to the K2 blackpearl Server service, double click to open it and click the Log On tab. You should see the domain\K2 Service account listed as the identity:



(3) Enter the password for the domain\K2 Service Account account in the Password and Confirm password text boxes and click OK

(4) A confirmation message will be displayed that the required right has been assigned to the service account. Click OK



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.6.4.1.2 Set up the Reporting Services Service Account

The Reporting Services Service Account is the account that the Reporting Services application pool (called ReportServer) will run under. This account probably already exists in your environment, but there are some permissions that should be validated to ensure that the K2 integration with Reporting Services functions properly.

The rest of this guide will use domain\Reporting Services Service Account as a placeholder for the Reporting Services Service Account name. When installing K2 in your environment, replace this placeholder with your actual account name.

Application Pool Rights

The SQL Reporting Services Service Account will require elevated permissions to run the application pool. We will use the aspnet_regiis command to configure this. This tool ships with the .NET Framework, and takes the pain out of configuring all the required NTFS permissions, IIS_WPG group membership, security policy user rights assignments, and IIS metabase access rights. For more information, see the MSDN article on setting security rights for .NET Applications, at <http://msdn2.microsoft.com/en-us/library/ms998297.aspx>.

To use the aspnet_regiis command, perform the following steps:

- 1
- 2
- 3
- 4

- Open a command prompt (Start > Run > cmd)
- Change directories to the .NET Framework folder (C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727)
- Type aspnet_regiis -ga domain\Reporting Services Service Account and hit Enter
- After the command completes, type **iisreset** and hit Enter

Reporting Services Permissions

The SQL Reporting Services Service Account will also require permissions on the SQL Reporting Services databases. To set these permissions, perform the following steps:

- 1
- 2
- 3
- 4
- 5
- 6
- 7

- Open **Reporting Service Configuration** (Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration)
- Connect** to the appropriate Instance
- On the Web Service Identity tab, confirm that Reporting Services picked up the new service account and listed it in the **ASP.NET Service Account** text box
- Make sure the SQLRS Service Account is selected, and click **Apply**
- The Task Status will update, and the icon next to the Web Service Identity will change to Configured (a green check mark)
- Close the Reporting Services Configuration Manager window
- Open a command prompt and perform an **IIS Reset** again (type iisreset and hit Enter)

Additional Configuration.

In order for users to browse the reports on the server, the following permissions must be configured:

Server Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role System User
 Home Folder Properties => Permissions, add <DOMAIN>\Domain Users place a check in the box for the role Browser



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.6.4.1.3 Permissions Necessary for the IIS and Reporting Services Server

IIS Server

Because we are using Integrated Authentication for stronger security, we need to assign all authenticated users Modify permissions on this temporary directory. This directory is used at runtime by the web site, and if all users do not have access to this folder, they cannot interact with items.



Open Windows Explorer and browse to **C:\Windows**

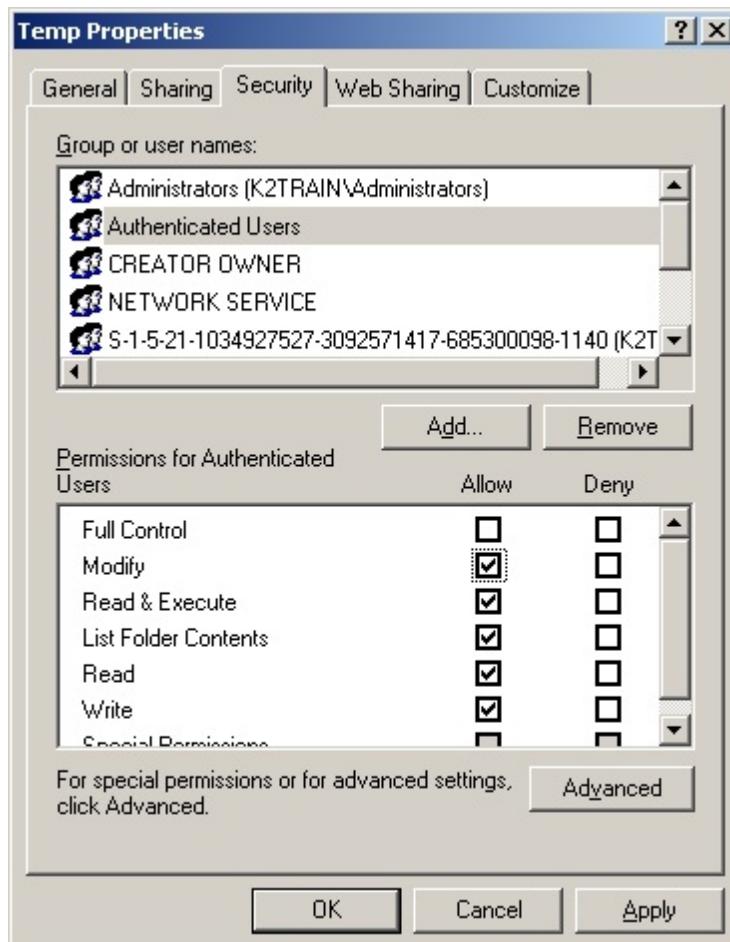


Scroll down to the **Temp** folder, right-click on it and select **Properties**



On the Security tab, select the **Authenticated Users** in the group list, and check the **Modify** check box

If the Authenticated Users group is not listed, click the **Add** button, and type in Authenticated in the text box. Clicking Check Names will validate the group, and you can close the Add dialog by clicking OK



Click **OK**, and when prompted, click **Yes**. Also, be sure that the Service Accounts have been set up properly.



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.6.4.1.4 MOSS Database Rights



This step requires that the user logging in to SQL Server Management Studio has sufficient permissions to grant permissions to other user accounts.

Setting Database Permissions

The account running the K2 installation requires permissions on the SharePoint_AdminContent_[GUID ID] database. These permissions must be set **before** the installation is started and may be set automatically if the same K2 Service Account has already been used by the MOSS Installer.

Item	Requirement
SharePoint Database	SharePoint_AdminContent_[GUID ID] *
Service Account	K2Service **
Permissions Requirement	<ul style="list-style-type: none"> ● db-owner (for installation) ● datareader and datawriter (for normal usage)

* The GUID ID is supplied by the MOSS Installer
** "K2 Service" refers to the Service account which has been assigned to the K2 Server Service

To verify the permissions have been set, or if they need to be set the database can be found in the following location:

1. Open Microsoft SQL Server Management Studio
2. Open the node **Databases** > **SharePoint_AdminContent_[GUID]**
3. Locate the **Security** > **Users node** > **[domain] \ [K2 Service]**
4. Verify the permissions for the **[K2 Service]** account
 - a. If the permissions have not been set, then they must be set
 - b. If they are set there is nothing further to do



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.6.4.1.5 Permissions Necessary for the SharePoint Server

SharePoint Server

In order to deploy SharePoint Workflow Integration processes, all authenticated users will need permissions on the SharePoint Template directory. This directory is used to deploy the workflow features, and without permission, SharePoint Workflow Integration processes will not deploy properly.



Open Windows Explorer and browse to **C:\Program Files\Common Files\Microsoft Shared\web server extensions\12** or **C:\Program Files\Common Files\Microsoft Shared\web server extensions\14** depending on the version of Windows Server that you are using.

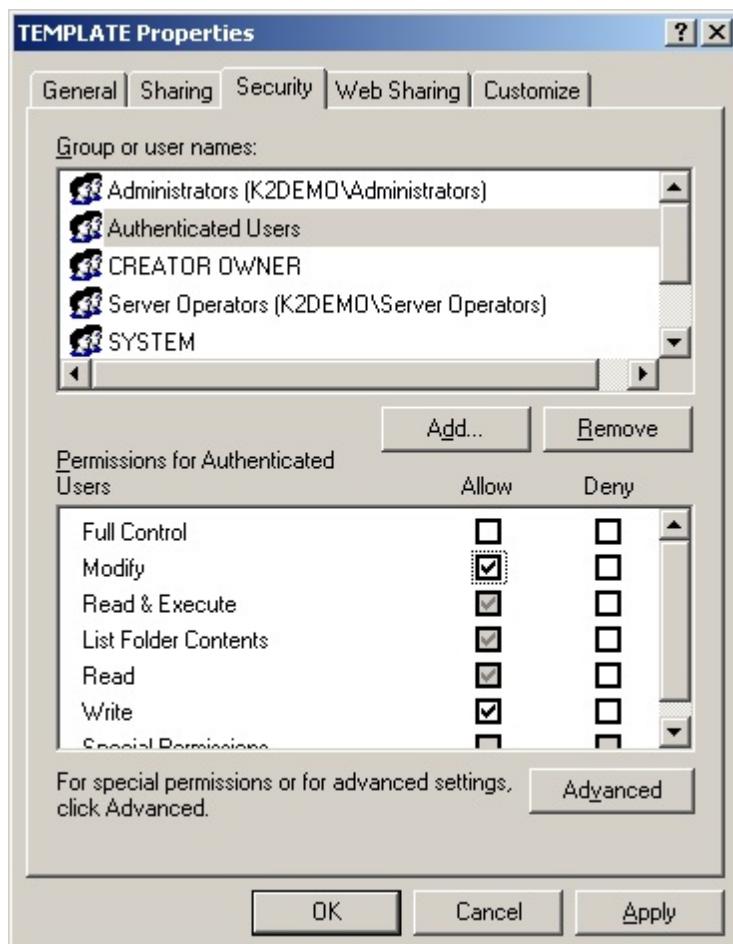


Scroll down to the **TEMPLATE** folder, right-click on it and select **Properties**



On the Security tab, select the **Authenticated Users** in the group list, and check the **Modify** check box

If the Authenticated Users group is not listed, click the **Add** button, and type in Authenticated in the text box. Clicking Check Names will validate the group, and you can close the Add dialog by clicking **OK**



Click **OK**, and when prompted, click **Yes**

Also, be sure that the Service Accounts have been set up properly.



For Windows 2008 Servers, the Authenticated Users also need Modify rights on the C:\Users folder and all folders below this. Apply this to all SharePoint Web Front Ends



While infrastructure changes are required by K2, each environment is different and has its peculiarities which must be taken into account. Modifying the infrastructure could have unforeseen results if the changes are not appropriately understood or managed. Given the broad spectrum of underlying infrastructure utilized, it is recommended that a panel or committee with appropriate skill in each area concerned be assembled to outline the underlying infrastructure changes and gauge the impact of the required changes.

1.6.4.1.5.1 K2 for SharePoint - Required Permissions-SP Core

K2 for SharePoint Required Permissions

When installing and working with the K2 for SharePoint components you must provide credentials for several different accounts. The following tables describe the accounts that are used to install, configure, and run the various K2 for SharePoint components.

K2 for SharePoint - Core

K2 for SharePoint components have a set of core features and security requirements that are required regardless of which features are actually activated in the target SharePoint farm.



A check is done to verify if the Setup user is part of the Farm Admin group, in which case the K2 SharePoint Integration features will be added to the system using this account. If the Setup user is not part of the Farm Admin group, then the Web App Pool identity is impersonated and used to add the K2 SharePoint Integration features.

Account	Purpose	Requirements
Setup user	The Setup user account is used to perform the following tasks: <ul style="list-style-type: none"> • Install the K2 for SharePoint files on SharePoint Web Front-Ends • Deploy K2 Solutions to SharePoint Farm 	<ul style="list-style-type: none"> • Domain user account (Note: This should not be the SharePoint System Administrator Account) • Member of the SharePoint Farm Administrators group <ul style="list-style-type: none"> • Installing and deploying the K2 solutions on the farm • Configuring global K2 settings in Central Admin • Database permissions - dbo_owner permission on all the following SharePoint databases: <ul style="list-style-type: none"> • SharePoint Configuration Database[SharePoint_Config]
K2 Central Admin	The K2 Central Admin account is used to perform the following tasks: <ul style="list-style-type: none"> • Use links on the K2 for SharePoint admin page (does not include K2 Designer for SharePoint links) 	<ul style="list-style-type: none"> • Full Control permissions on the Central Admin Site Collection is required to open the page. • Admin rights on K2 server <ul style="list-style-type: none"> • Retrieving Host Server configuration settings • Setting Export rights for Deployment Application Pool account for K2 Designer for SharePoint
K2 Site Settings	The K2 Site Settings account is used to perform the following tasks: <ul style="list-style-type: none"> • Use links on the K2 Site Settings page 	<ul style="list-style-type: none"> • Full Control permission on the Site Collection with the K2 Site Settings link
K2 Service account	The K2 Service account is used to perform the following tasks: <ul style="list-style-type: none"> • Create/Modify/Delete Webs • Create/Modify/Delete Lists and Libraries • Create/Modify/Delete List Items and Documents • Create/Modify/Delete 	<ul style="list-style-type: none"> • Full Control permission on all Site Collections that are part of any K2 process that will Create/Modify/Delete a Web or Create/Modify/Delete user permissions • Designer permission on all Site Collections/Webs that are part of any K2 process that will Create/Modify/Delete a List or Library • Contributor permission on all Site Collections/Webs that are part of any K2 process that will Create/Modify/Delete a List Item or Document • The K2 runtime assumes the appropriate rights are granted to the K2 Service account based on the K2 process needs. If rights are not sufficient at runtime the process will enter an error state and the process will be halted. The process error state can be recovered via a retry operation after the rights have been corrected.

User Permissions

Account	Purpose	Requirements
K2 Runtime Services Application Pool	<p>The K2 Runtime Services Application Pool account is used to perform the following tasks:</p> <ul style="list-style-type: none"> • Interact with K2 processes at runtime via Web services 	<ul style="list-style-type: none"> • Impersonate rights on K2 server
K2 Thick-client Designers (K2 Studio, K2 for Visual Studio)	<p>The account of the person using the thick-client designer is used to perform the following tasks:</p> <ul style="list-style-type: none"> • Deploy SharePoint Workflow Integration designed processes 	<ul style="list-style-type: none"> • The thick-client designer account requires the following security configuration. <ul style="list-style-type: none"> • Export rights on K2 server • Additionally, either the thick client designer account or the SharePoint Application Pool account of the target SharePoint URL (Site Collection) requires the following security configuration. <ul style="list-style-type: none"> • SharePoint Farm Administrators group membership • Full Control permission on the Site Collection • Modify rights on the Features folder on the SharePoint web front ends

1.6.4.1.5.2 K2 for SharePoint - Required Permissions-K2 designer for SP

K2 for SharePoint Required Permissions

When installing and working with the K2 for SharePoint components you must provide credentials for several different accounts. The following tables describe the accounts that are used to install, configure, and run the various K2 for SharePoint components.

K2 Designer for SharePoint

The K2 Designer for SharePoint requires additional rights for installation, configuration and execution.



The application pool account used for the installation of the K2 Designer for SharePoint may be different from the application pool account used to set the K2 SharePoint Integration features. This application pool account must be part of the Farm Admin group.

– this is only for deployment not execution.

Account	Purpose	Requirements
Setup user	The Setup user account is used to perform the following tasks: <ul style="list-style-type: none">• Activate features and K2 site settings	All K2 for SharePoint Core permissions, plus the following: <ul style="list-style-type: none">• Full Control permission on the default or selected Site Collection is required to open the page.<ul style="list-style-type: none">• Activating All K2 Features• Creating and configuring hidden K2 lists• Examples: members of Site Collection Administrators and Portal Owners have the Full Control permission mask• SQL Server server role – securityadmin (Server > Security > Logins or Server > Security > Server Roles)<ul style="list-style-type: none">• securityadmin (required on K2 Server and SharePoint Server)• dbcreator (required on K2 Server and SharePoint Server)• db_owner for the webdesigner database (only required on K2 Server)• Rights to set security on the All Users temp folder (%SYSTEMROOT%\System32\config\systemprofile\AppData\Local\Temp)
K2 Central Admin	The K2 Central Admin account is used to perform the following tasks: <ul style="list-style-type: none">• Navigate to K2 Designer links on the K2 for SharePoint admin page	<ul style="list-style-type: none">• Full Control permissions on the Central Admin Site Collection is required to open the page.• Admin rights on K2 server<ul style="list-style-type: none">• Retrieving Host Server configuration settings• SQL Server server role on K2Server<ul style="list-style-type: none">• securityadmin• dbcreatoror• db_owner for the webdesigner database• Rights to set security on the All Users temp folder (%SYSTEMROOT%\System32\config\systemprofile\AppData\Local\Temp)
Deployment Application Pool account	The Deployment Application Pool account is used to perform the	The following security configurations are done automatically when the Deployment Application Pool account is configured: <ul style="list-style-type: none">• SharePoint Farm Administrators group membership (this permission is needed for deployment of processes only, not their execution)• Site Collection Administration

	<p>following tasks:</p> <ul style="list-style-type: none"> • Deploy K2 Designer for SharePoint designed processes <p>Note: The Farm admin group permissions are required for legacy processes that use the old Workflow Integration method where a feature needed to be added to the Farm for each process deployed.</p> <p>With SPWFI version 2 this is no longer a requirement.</p> <p>The user can remove the farm admin permission and then check that everything is still working i.e. that they can deploy a process, as this is the only place this permission was required.</p> <p>The user should bear in mind that if they make use of a generated Workflow Integration then they will have to be Farm admin, but this requirement is only for deployment and not execution.</p>	<ul style="list-style-type: none"> • Export rights on K2 server • SQL Server database role -- db-owner (Server > Databases > {database name} > Security > Logins): <ul style="list-style-type: none"> • K2 Designer for SharePoint database • Add deployment application pool to SharePoint Application Pool collection which sets SQL Server database role -- db_owner for the following (Server > Databases > {database name} > Security > Logins): <ul style="list-style-type: none"> • SharePoint Central Admin content database • SharePoint Shared Services content database • SharePoint Site Collection content database • SharePoint Configuration database • db_owner for the webdesigner database • Modify rights created on the All Users temp folder (%SYSTEMROOT%\System32\config\systemprofile\AppData\Local\Temp)
K2 Designer for SharePoint	<p>Users in the K2 Designer for SharePoint groups can perform the following tasks:</p> <ul style="list-style-type: none"> • Access the Create K2 Process menu to design and deploy a 	<ul style="list-style-type: none"> • All groups with at least Design permissions (Design and Full Control) are included by default. • Full Control permissions are required on the Site Collection to change the groups configured for Process Designer. This link is available on the K2 Site Settings page. • The user deploying the process will be given Export rights on the K2 server. • The user deploying the process will be given Admin and Start rights on the process.

	process with K2 Designer for SharePoint	
Process Participant	<p>Users in the Process Participant groups can perform the following tasks:</p> <ul style="list-style-type: none"> • Participate in deployed K2 processes 	<ul style="list-style-type: none"> • All groups with at least Contribute permissions (Contribute, Design and Full Control) are included by default. • Full Control permissions are required on the Site Collection to change the groups configured for Process Participant. This link is available on the K2 Site Settings page. • Process Participant groups will be given Start and View Participate rights on process.



For upgrade scenarios where multiple k2 databases still exists, the db_owner rights required for webdesigner, will still be applied on the the webdesigner database. For new installations where a single K2 database exists, the db_owner rights for webdesigner will be applied on the webdesigner schema instead.

1.6.4.1.5.3 K2 for SharePoint - Required Permissions-K2 Process Portals

K2 for SharePoint Required Permissions

When installing and working with the K2 for SharePoint components, it is required to have certain rights to perform K2 Process Portal actions.

K2 Process Portals

The following is a summary of the SharePoint and K2 rights necessary to perform various K2 Process Portal actions.

Action	SharePoint Rights	K2 Rights
Processes Web Part	Reader	Server Admin, Process Admin
Instances Summary Web Part	Reader	Server Admin, Process Admin, Process View
Process Instances - View Detail	Reader	Server Admin, Process Admin, Process View
Process Instances - Perform Action	Reader	Server Admin, Process Admin
Start Process Instance	Reader	Process Admin, Process Start
View Reports	Reader	Process Admin, Process View, Process View Participate
Process Management - View Detail	Reader	Server Admin, Process Admin
Process Management - Perform Action	Reader	Server Admin, Process Admin
Process Management - View Detail - Roles	Reader	Server Admin, Process Admin for all processes in Project
Process Management - Perform Action - Roles	Reader	Server Admin, Process Admin for all processes in Project
Add Process to Portal	Contributor	Server Admin, Process Admin
Administration Links (Central/Site)	Reader	Server Admin

1.6.4.1.6 Adding Users

Group Policy: Adding Users

This topic provides brief step by step instructions on how to add a User to the Group Policy for the K2 Server Machine and then to force the policy update across the network. These instructions are provided only as a guideline on how this change can be performed and if there are any concerns or queries the organization Administrator should be contacted and or the relevant Microsoft product documentation must be consulted first before implementing these steps.

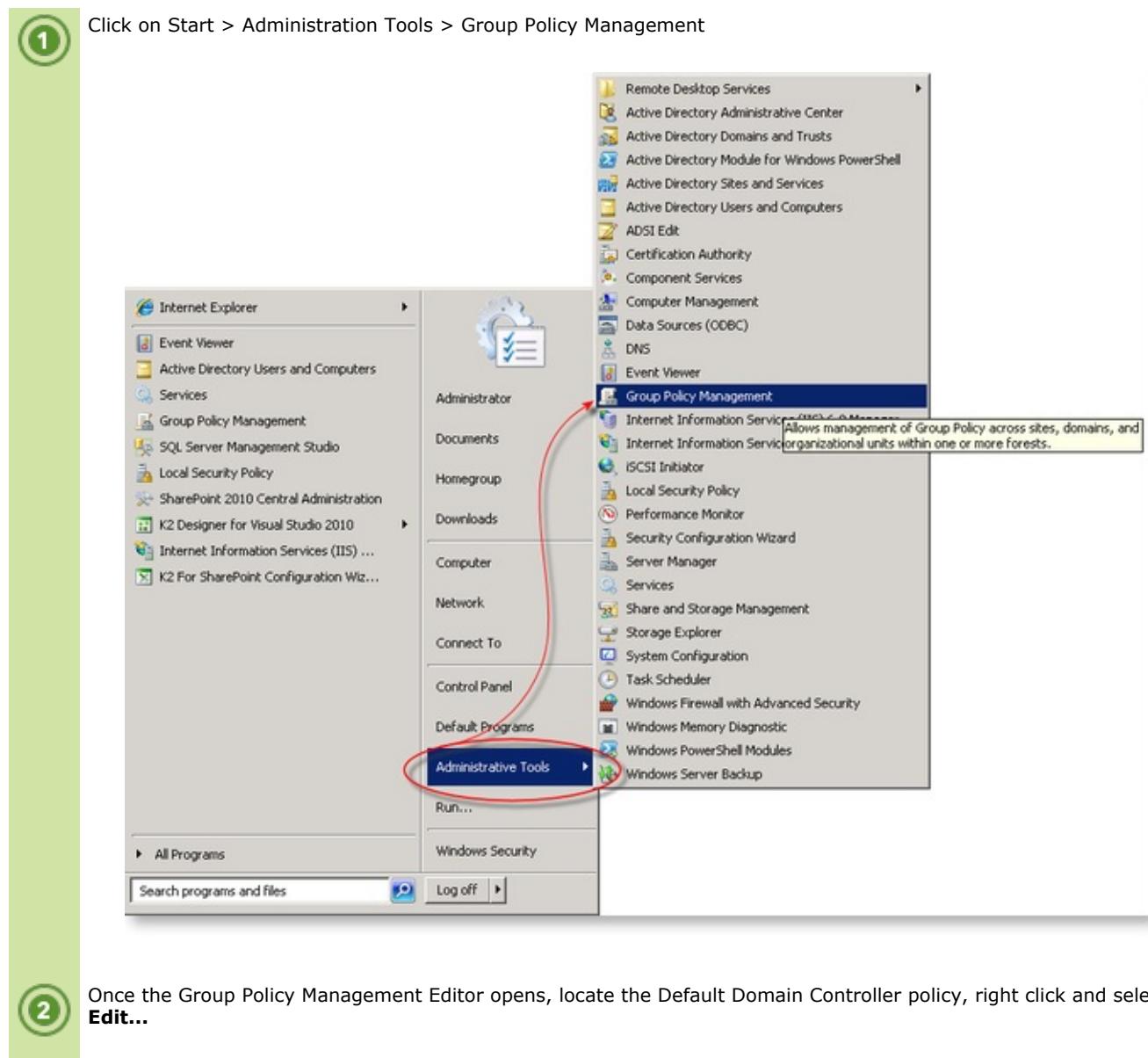
For further information on the LOGON32_LOGON_BATCH method used, see the topics [Machine Interaction](#) and [Local Security Policy](#).

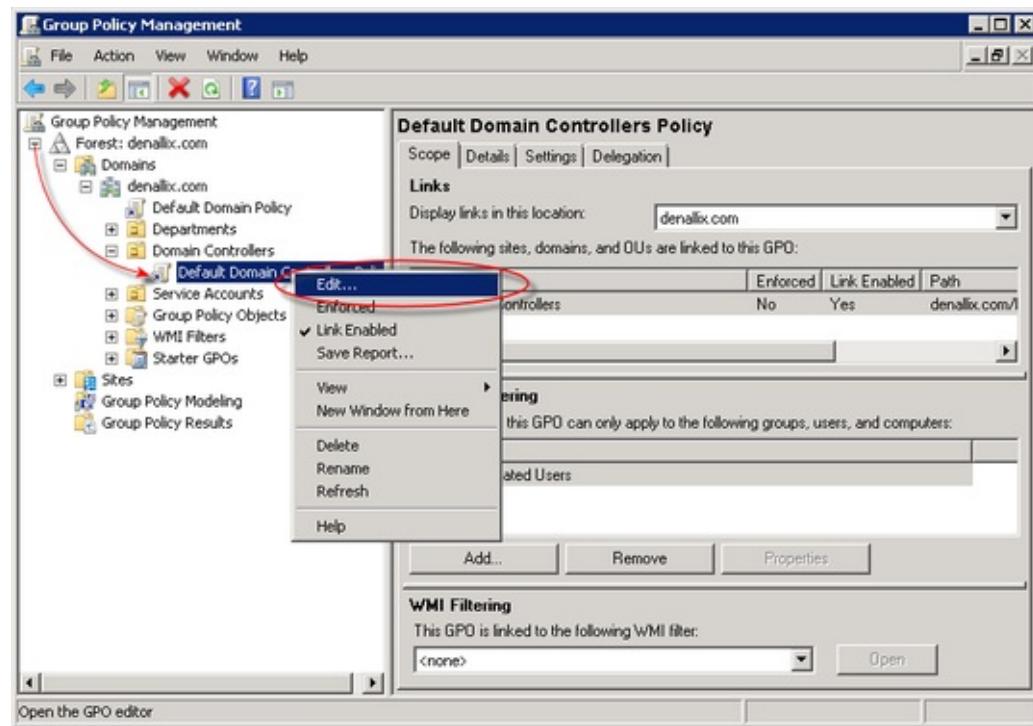
Prerequisites

1 User Account is required with the appropriate permissions to access the network and network resources. For further information and a description of the user permissions required, see the K2 blackpearl Getting Started Guide.

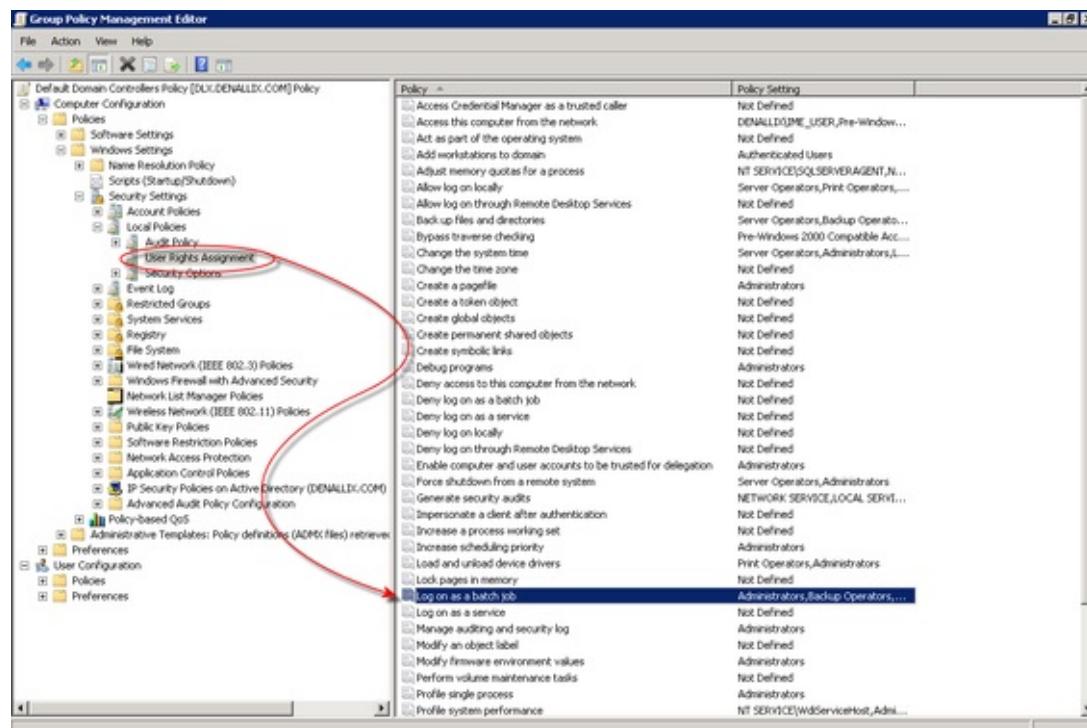
How to add users: What to do ...

The steps below make use of a User Account called RunAsUser which will be added to the Group Policy to enable the [Machine Interaction](#): LOGON32_LOGON_BATCH.



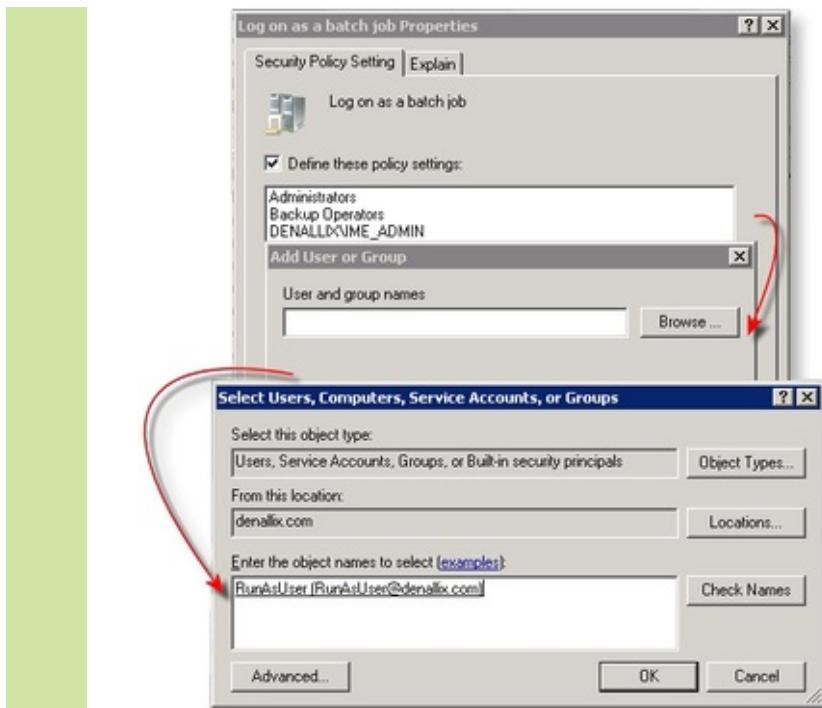


③ Expand the Computer Configuration nodes as shown in the image (click on the link) and then select User Rights Assignment > Logon As Batch Job

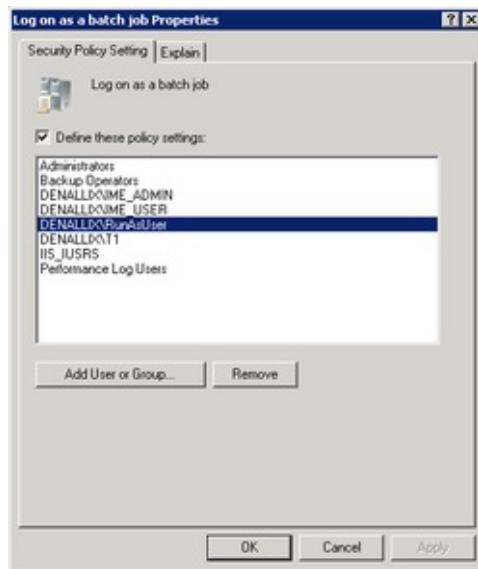


④ Select the option to Add a User.

1. From the Add User or Group dialog, click **Browse**
2. Enter the name of the user, ie for this discussion only enter **RunAsUser** and click **Check Names**
3. Once the user resolves ie, the user name is underlined then click **Ok**



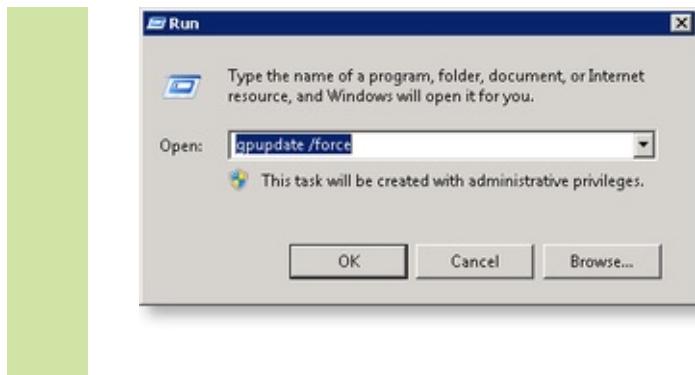
5 If the user was added successfully, then the new user name will appear listed in the **Log on as Batch job Properties**. Click Ok to close the dialog.



6 Depending on the environment, the changes may propagate quickly, and in some cases take longer. The changes will not take affect immediately unless forced.

To force the update do the following:

1. Click on **Start > Run**
2. Enter **gpupdate /force**
3. Click **Ok**



1.6.4.2 K2 Server

1.6.4.2.1 K2 Performance

1.6.4.2.1.1 K2 Service Startup

K2 Service Startup

If the K2 Service takes a while to startup. The time taken may be from 2 - 3 minutes which is a noticeable delay in startup. See the possible options below:

Certificate Authority

If a trust relationship exists between machines which uses authenticode signing then the recommended way forward is to download and install the root Certificate Authority. Although acceptable, disabling i.e. bypassing the CA effectively breaks the trust relationship between the machines.

The K2 Administrator has two options:

1. Download and install the Root Certificate Authority
2. Disable or bypass the Root Certificate Authority

How to bypass the Root Certificate Authority



Implementing the following configuration change is at the discretion of the K2 System Administrator.

Copy

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

Certificate Authority

True	The K2 Server boots using the Root Certificate Authority. Warning: Unless the Root Certificate Authority has been downloaded and installed, the K2 Service Account may experience delays of up to 3 minutes before starting.
False	When set to <i>False</i> the K2 Server boots without using the Root Certificate Authority Warning: When set to False, the trust between machines is broken

1.6.4.2.1.2 Tweaking identity cache performance for the K2 Server

Configuration settings for tweaking identity cache performance for the K2 Server.

The Identity Service is a new cache mechanism that has been introduced from K2 4.5 KB001370. This new cache mechanism is designed to work with Active Directory groups, SharePoint Groups and also K2 roles. Previously one configured the Cache Timeout value on the Active Directory User Manager (ADUM) settings. Note that this will now be set to zero for future releases to disable the ADUM cache.

To examine the internals of the Identity Framework, we will discuss the following backend tables used in the K2HostServer database.

- Identity.CacheConfiguration
- Identity.RoleItem
- Identity.Identity
- Identity.IdentityMember
- Identity.IdentityUpdate

The Identity.CacheConfiguration table

The [Identity].[CacheConfiguration] table sets the time parameters of the Role Provider (K2, K2SQL, CUSTOM) identity caches and the Microsoft SQL command timeout setting. The default properties of these settings are as follows:

□	Identity.CacheConfiguration
□	Columns
鑰匙	Name (PK, nvarchar(128), not null)
	Value (nvarchar(max), null)

	Name	Value
1	DynamicGroupCacheTimeout	30s
2	DynamicRoleCacheTimeout	30s
3	DynamicUserCacheTimeout	30s
4	GroupCacheTimeout	8h
5	GroupContainersCacheTimeout	8h
6	GroupMembershipCacheTimeout	1h
7	ResolvedExpiredIdentities	0m
8	RoleCacheTimeout	8h
9	RoleMembershipCacheTimeout	1h
10	SqlCommandTimeout	10m
11	UserCacheTimeout	8h
12	UserContainersCacheTimeout	8h

These settings may be defined in milliseconds (ms), seconds (s), minutes (m), or hours (h). The maximum value will be 24 days, 20 hours, 31 Minutes, 23, Seconds and 6470000 milliseconds. This is a .NET restriction on wait handles that does not accept longer periods than int.MaxValue specified in milliseconds. In other words 2147483647 milliseconds translates to this value 24.20:31:23.6470000 (d,h,m,s,ms). A configuration of 0s will turn the setting off. A higher value will increase the time between reloading -reducing the load on the server but increasing the latency of up-to-date information.

The three types of identities that are cached within the K2 Server are the **User**, the **Role**, and the **Group**.

The **CacheTimeout** settings configure when the cached properties of that identity will expire. After this configured time period has expired the K2Server will resolve the identity against the provider.

In regard to the **dynamicCacheTimeout**, a normal user will be resolved on the thread according to the CacheTimeout configuration. Dynamic identities will be excluded from this timed resolving and will resolve on demand. When a worklist item is opened, all dynamic identities will be resolved before the server queries the current user membership, in case the user is included in the result. For example, a dynamic identity would be an online users whose identity needs to be checked every time the worklist is requested. This has a performance impact on worklist, and should only be used for true dynamic cases. The dynamicCacheTimeout setting therefore configures the time to expiration of the cached dynamic identity.

The **ContainersCacheTimeout** setting configures the duration until expiration of the K2 server cache that contains the external relational identity settings, i.e. all the groups that a particular group also belongs to.

The **MembershipCacheTimeout** setting configures the duration of the K2 server cache that contains the internal

relational identity settings, i.e. all the users within a group.

The **resolvedExpiredIdentities** setting configures the period of time that the server checks for expired identities and resolve them.

The **sqlCommandTimeout** setting configures the maximum amount of time the calling application should wait for an identity to be cached, before a timeout exception is raised.

The Identity.RoleItem table

This table holds the configuration of the SmartObject/Groups/Users defined in a K2 role.

	IdentityID	FQN	Type	Exclude	Data	LastModified
▶	14	TestUsers	4	False	<smartobject name="TestUsers" guid="679a3cf...>	10/3/2011 11:3...
▶	14	K2:DENALLIX\Anthony	1	False	NULL	10/3/2011 11:3...
▶	14	K2:DENALLIX\Administrators	3	False	NULL	10/3/2011 11:3...
*	NULL	NULL	NULL	NULL	NULL	NULL

The table contains records that match up with the items as configured in the Management Console.

User/Group	Include	Role Type
TestUsers	<input checked="" type="checkbox"/>	SmartObject
K2:DENALLIX\Anthony	<input checked="" type="checkbox"/>	User
K2:DENALLIX\Administrators	<input checked="" type="checkbox"/>	Group
K2:Portal\Approvers	<input checked="" type="checkbox"/>	Group

The Type column uses the following values.

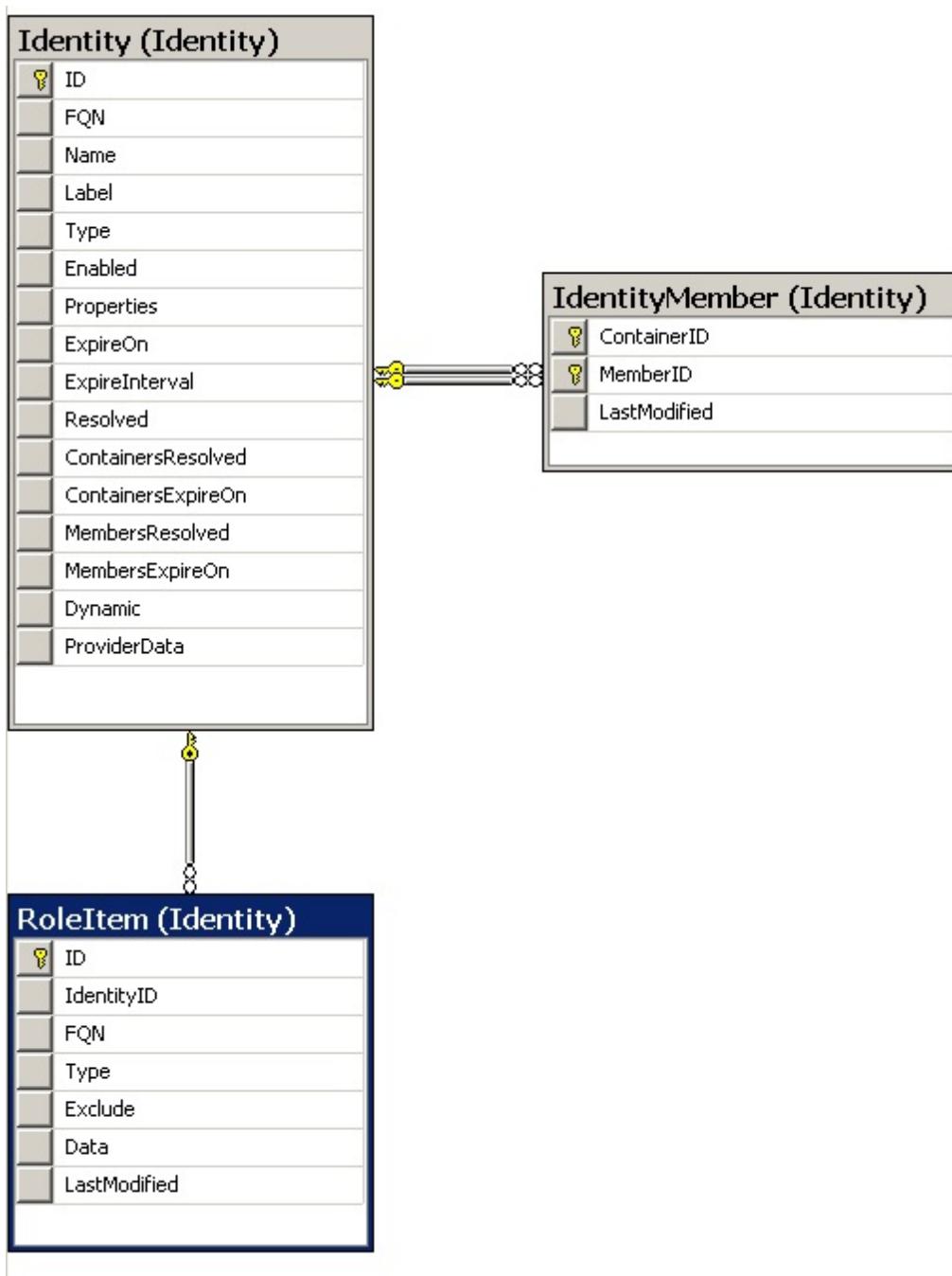
1 - User

3 - Group

4 - SmartObject (The Data column contains the SmartObject connection details. It also includes the method, property and filter values to use). Here's an example of the XML string contained in the Data column.

```
<smartobject name="TestUsers" guid="679a3cf...>
connectionString="Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False
;Host=blackpearl;Port=5555" methodName="GetList" isListMethod="True" propertyName="UserID"
expectedType="1" xmlns="<a href="http://schemas.k2.com/roles/smartObjectdefinition"><inputs>
<input>http://schemas.k2.com/roles/smartObjectdefinition"><inputs><input name="TestUsers"
type="0">denallix\codi</input></inputs></smartobject>
```

From the Identity.RoleItem table, the IdentityID column links back to the Identity.Identity table ID column for the role's cache settings. The Identity.RoleItem table acts as the definition for the role, and the Identity.Identity table stores the role item and also the members. The linkage between the role and the members is contained in the Identity.IdentityMember table.



The Identity.Identity table

This table stores the cache expiry information for the User/Groups/Roles. You can force expire the relevant User/Group/Role cache by modifying the relevant expiry datetime value.

BLACKPEARL.Identity.Identity									
On	ExpireInterval	Resolved	ContainersRes...	ContainersExpi...	MembersResolved	MembersExpireOn	Dynamic	ProviderData	
011 0:21:...	28800	True	True	9/1/2011 7:11:0...	False	9/1/2011 7:10:5...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
011 0:45:...	28800	True	False	9/1/2011 7:11:1...	False	9/1/2011 7:11:1...	False	NULL	
011 11:3:...	5	False	False	9/1/2011 7:12:4...	True	9/1/2011 7:12:13:...	True	NULL	
011 8:45:...	28800	True	False	9/1/2011 7:13:1...	False	9/1/2011 7:13:1...	False	NULL	
011 6:24:...	28800	True	False	9/1/2011 7:13:1...	False	9/1/2011 7:13:1...	False	NULL	
011 10:5:...	28800	True	False	9/8/2011 8:10:4...	False	9/8/2011 8:10:4...	False	NULL	
011 11:3:...	28800	True	False	9/9/2011 11:21:...	False	9/9/2011 11:21:...	False	NULL	
011 8:45:...	28800	True	False	9/29/2011 6:32:...	True	9/30/2011 1:45:...	False	NULL	
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	

For every item there are three different expiry fields (*ExpireOn*, *MembersExpireOn* and *ContainersExpireOn*). There are then three main methods on the Identity Service, namely *GetIdentity*, *GetIdentityMembers*, and *GetIdentityContainers*. These relate to the three expiry timestamps mentioned above.

1. *ExpireOn* will be updated if the *GetIdentity* method is called (e.g. a Get User Details call on UMUser SmartObject).
2. *MembersExpireOn* will be updated when *GetIdentityMembers* is called. (e.g. Get Group Users call on UMUser SmartObject).
3. *ContainersExpireOn* will be updated when *GetIdentityContainers* is called (e.g OpenWorklist call). This will return all the groups and roles for a user and recursively get roles and groups for each of the direct containers (recursively).

For a group, notice that the *MembersExpireOn* and *ExpireOn* fields gets refreshed when a group is requested to be resolved. For example when a new client event is hit which utilizes the group (refreshes the group membership and group properties respectively), or an E-mail event that sends an e-mail to the specific group. Other possibilities will include the UMUser SmartObject when executing the *GetGroupUsers* method. On the other hand, when a user accesses his task list, the user's *ExpireOn* and the *ContainersExpireOn* fields are refreshed. *ExpireOn* refreshes the identity Properties XML field and *ContainersExpireOn* refreshes the groups and roles that the user belongs to. The *MembersExpireOn* field does not change and its value is from the first time the Identity Service is used for the user.



If you want to refresh cache items, set all the three expiry dates to some time in the past for the relevant identity items.

You will also note that there is a Dynamic flag for each record. Currently this only applies to K2 roles. If it is set to *True*, it will ignores the CacheTimeout settings and instead use the dynamicCacheTimeout settings (i.e. 30s by default). Queries will be queried fresh after 30 seconds from the last query. This is useful for keeping task items current when users are removed or added from the K2 role. However, the flip side is that this will have a performance impact when identities are resolved as all dynamic identities gets refreshed before members or containers are selected.



NEVER delete anything from the *Identity.Identity* table – there are other K2 modules that rely on the ID's in this table and in the future other components will also rely on these ID's in regard to users/groups/roles.

This is also where the K2 roles get saved, so if you delete all the records, you will delete all your roles as well.

The *Identity.IdentityMember* table

This table holds the linkages between the Roles/Groups and the individual users (many-to-many relationship). In the *Identity.IdentityMember* table, both the *ContainerID* and *MemberID* columns link back to the *Identity.Identity* table ID primary key column. If you are familiar with K2.net 2003 destination queues (which is the predecessor to K2 roles), you will note that this is similar to the relationship between the *DestQueue* and *DestQueueUser* tables in the K2Server database. The only difference is that it stores the ID of the user instead of the user name for performance reasons.

BLACKPEARL.H..IdentityMember			
	ContainerID	MemberID	LastModified
▶	2	1	9/1/2011 11:10:54 AM
	3	1	9/1/2011 11:10:54 AM
	4	1	9/1/2011 11:10:54 AM
	5	1	9/1/2011 11:10:54 AM
	6	1	9/1/2011 11:10:54 AM
	7	1	9/1/2011 11:10:54 AM
	8	1	9/1/2011 11:10:54 AM
	9	1	9/1/2011 11:10:54 AM
	10	1	9/1/2011 11:10:54 AM
	11	1	9/1/2011 11:10:54 AM
	12	4	9/1/2011 11:11:00 AM
	14	15	9/1/2011 11:13:19 AM
	14	16	9/1/2011 11:13:19 AM
	19	15	9/30/2011 12:45:31 PM
	19	16	9/30/2011 12:45:31 PM
*	NULL	NULL	NULL

The Identity.IdentityUpdate table

This table should be empty most of the time. The table is used for when identities gets updated. The result from the providers are moved to this table (Bulk Insert) and the Identity.Identity and Identity.IdentityMember table will be updated in transaction. This table will be cleared once the update has completed. You will see that this table is used by the bulk container and member update stored procedure calls.



Editing the database tables can be a risky business, so create a backup of your database if you plan to modify any settings here. This gives you a safety net in case anything goes wrong.

1.6.4.2.2 Installing additional nodes

1.6.4.2.2.1 Adding another K2 Server to the farm

If you are running the K2 Server in a clustered K2 farm, follow the below steps to install the K2 Server component on an additional K2 Server:

1. First install all the **prerequisites**, **enable DTC** and **install MSMQ**
2. Copy the installation files local to the second K2 server
3. On the **Welcome** screen, click Next
4. On the **End User License Agreement** screen, read through the EULA. You must select the **I agree** option before you can continue with the installation. You can print out the EULA for your records. Once you have read the EULA, click Next
5. On the **Installation Setup** screen, select the Custom Installation option and type in a Installation Folder name, and click Next
6. On the **Select Components** screen, you should see that the only components for which the prerequisites are met are:
 - K2 blackpearl Server
 - K2 blackpearl Setup Manager

You will also see a link to Check Dependencies for the other components.



If you want to install one of the components on this server that have a Check Dependencies action, cancel the installation and fix the dependency. Then, restart the installation and you should be able to select that component.

7. On the **License Configuration** screen, the System Key will be automatically generated for you. Type in the License Key that matches this System Key, and click Next



If you do not have a license key, you can request one by opening Internet Explorer and going to <https://portal.k2.com/licensekey/Default.aspx>. You will need an internet connection, and you will also need a Customer and Partner portal account. Enter in the appropriate information, and the license key will be generated automatically for you.

8. On the **K2 Server Configuration screen**, select the appropriate option:
 - **K2 Server Farm.** Multiple K2 Servers in your environment.
 - **Add K2 Server to existing Farm.** Select this option if a K2 Server Farm already exists, and you are connecting an additional server to the farm.
Click Next to continue the wizard
9. On the **HostServer Database** screen, type in the name of the SQL Server where you installed the K2 Databases. This points the second node to the HostServer database set up by the first node, to share configuration information. If you changed the Host Server database name, update it here and click Next
10. On the **Service Accounts Configuration** screen, enter in the following user accounts:
 - **K2 Administrator Account.** This account will be given **Administrative rights to the K2 Server for the Administrator to perform administrative functions.** domain\K2 Administrator Account
 - **K2 Service Account.** This account is the dedicated account for the K2 Service. domain\K2 Service Account

You can test that the user name and passwords are valid by clicking on the Test button. Be sure to uncheck the **Set K2 Host Server SPN** check box. Because you already set the SPNs when configuring the first K2 Server in the farm, you do not need to set them now.

When you finished entering in the accounts, click Next to continue.

11. On the **Configuration Summary** screen, validate the settings. You can go back to make any necessary changes, and you can print this page for reference later. Once you are satisfied with your settings, click Configure.
The Setup Manager will update and show you the progress of the components as they are configured.
12. When the configuration has completed, you will see a finished screen. There will also be a link to the created configuration log file. When you click Finish, you will be prompted to restart now (click Yes) or restart later (click No). It is important to restart in order to complete the installation and configuration of K2 blackpearl.

1.6.4.3 K2 Workspace

1.6.4.3.1 K2 Workspace Security

K2 Workspace Menu Items

By default, all users have access to menu items in K2 Workspace. Unless permissions are specified for a menu item for a specific group or list of users, that item is open to all users.

It is recommended that only a limited group of people be granted access to the Security tab. The administrator should restrict access to this tab as soon as possible after installation to ensure that people can't add themselves and lock out everyone else.



If you open the user permissions screen (in Security > Workspace Permissions) for a particular menu group, and there are no users listed, it means that all users are authorized. Adding a user to this menu group will grant permissions to that user AND revoke permissions from all other users.



If you do not specify user permissions for the Management Console, and a user gives them self permissions, it will appear as though the Management Console has disappeared from all other user's workspace areas as all other user's permissions will then be removed.

1.6.4.3.2 View Flow validation

View Flow Validation

The IIS installation requires the Static Content Windows feature to be enabled to ensure that View Flow and other Silverlight components function properly.

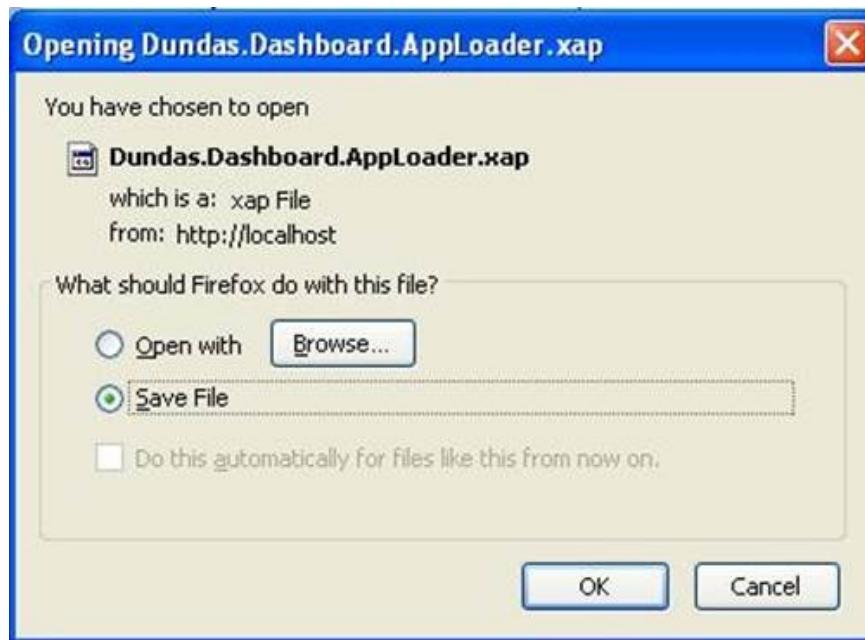
Symptom

View Flow will load a blank page and no Silverlight control will be loaded on the page

Analyze

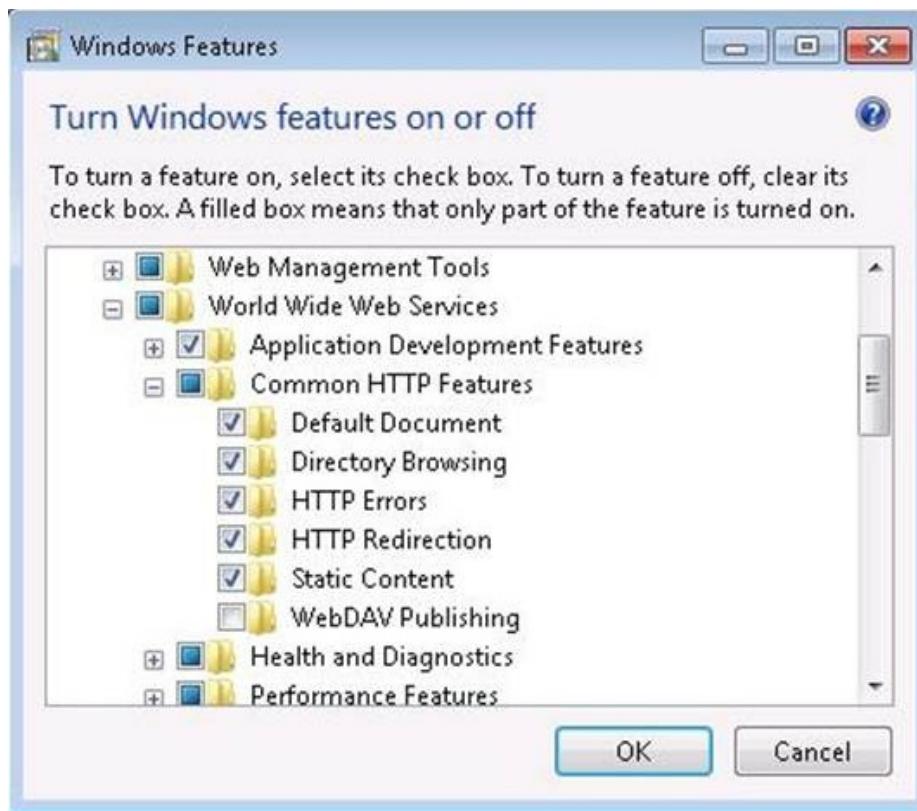
- Right-click on the page where a View Flow link is available. If you don't see the **Silverlight** menu, continue with the next step.
- Navigate to <http://iisserver:81/Viewflow/ClientBin/SourceCode.Viewflow.SLViewer.xap>.

If you are not presented with the option to download the XAP file and you don't receive an **HTTP 404 Not Found** error from your web server, your IIS installation may not be configured to Server Static Content. If you are running IIS 7.x and have initially configured IIS to host web applications, the Static Content option is not enabled by default.



Resolution - Windows 7 environment

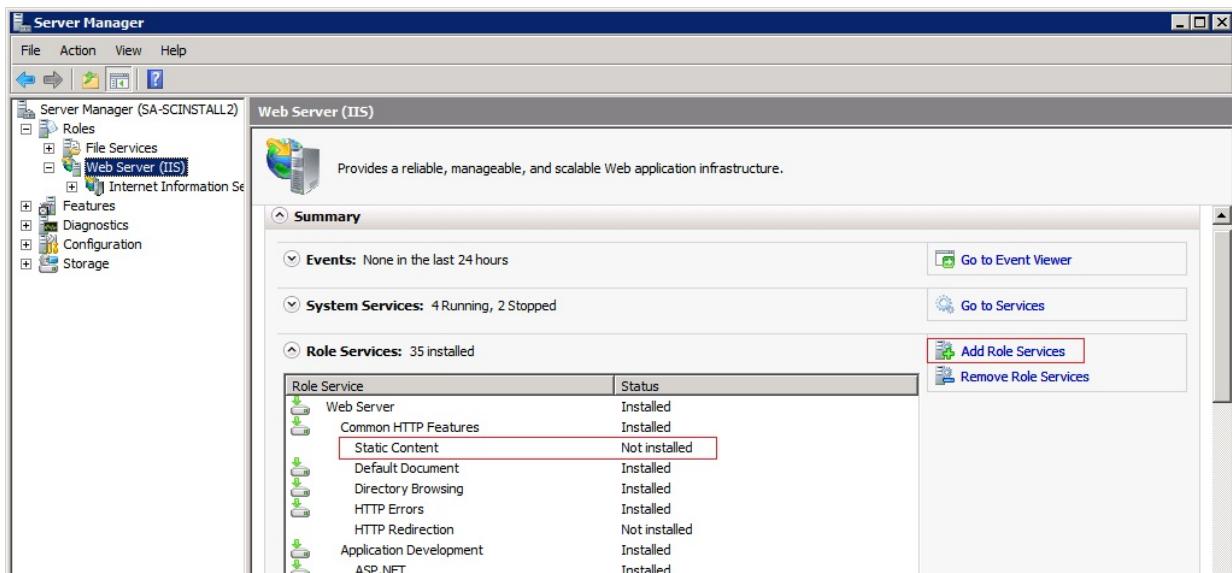
1. Navigate to Start > Control Panel > Programs and Features, and select the **Turn Windows Features On or Off** option.
2. Expand Internet Information Services > World Wide Web Services > Common HTTP Features



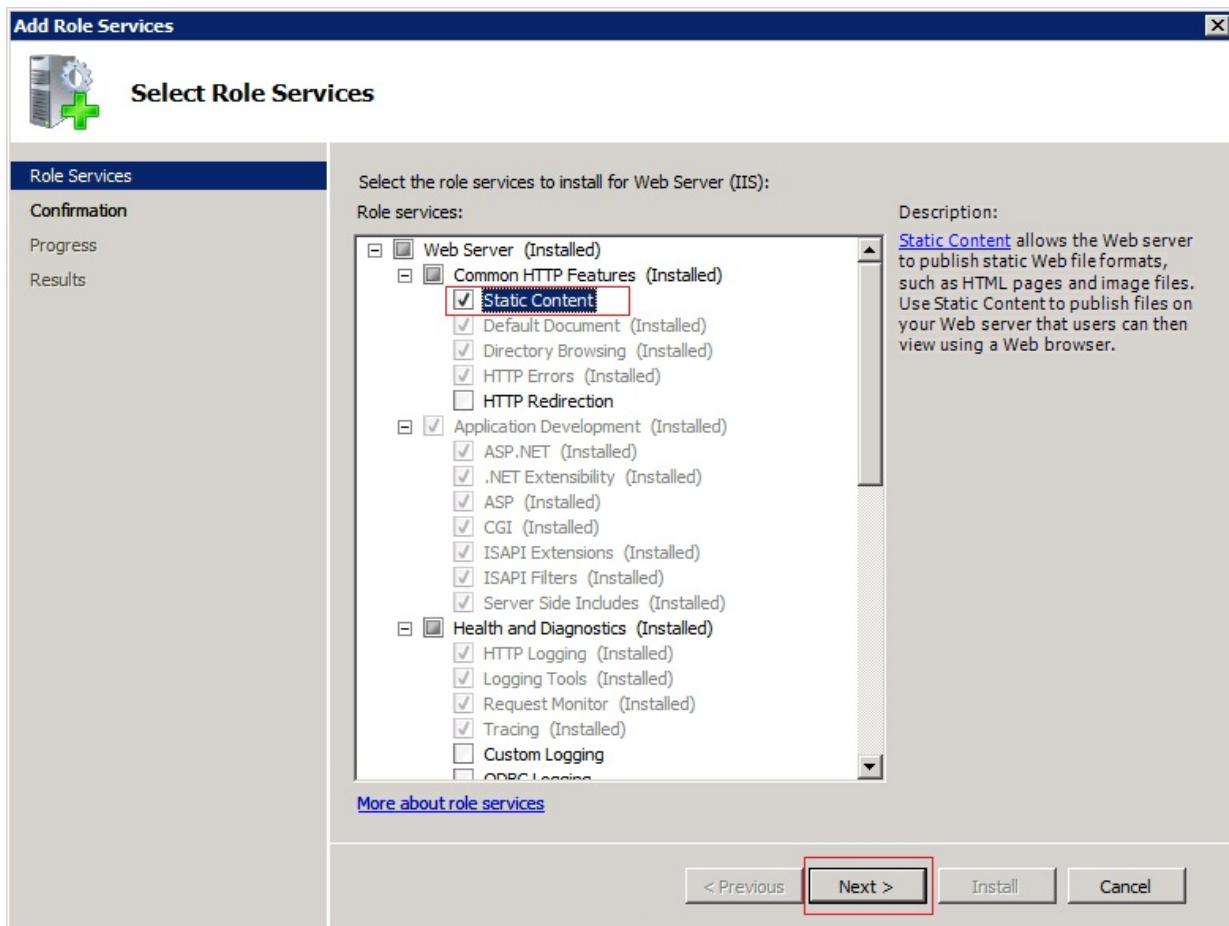
3. Enable **Static Content** by selecting the check box to the left of this item.
4. Click the OK button at the bottom of this screen to complete the installation of this option. To confirm that this option has been enabled you should browse to the XAP file mentioned above to ensure you are presented with the option to download.

Resolution - Windows 2008 environment

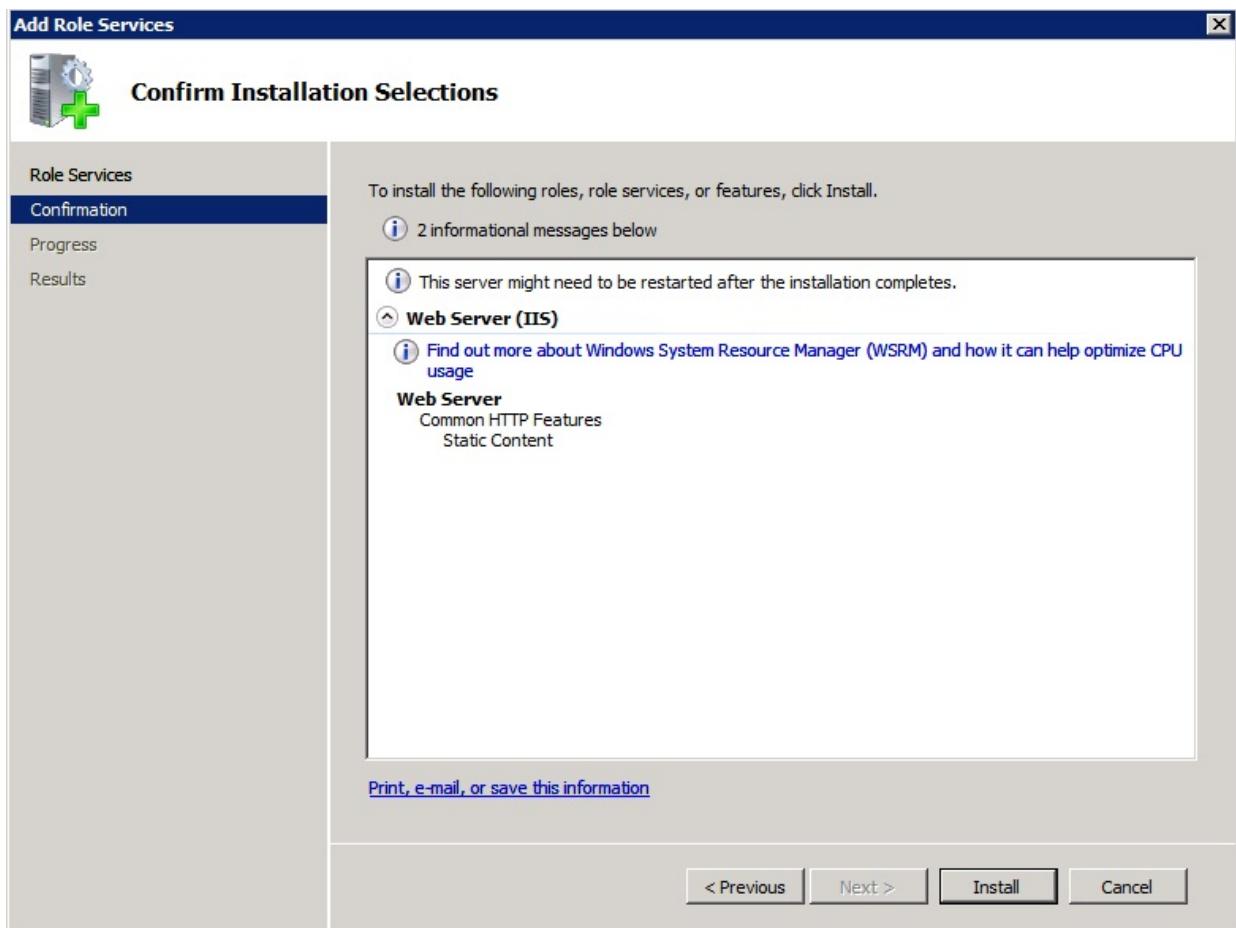
1. Open the Server Manager under the **Roles** tree view item
2. Select the **Web Server** node (might take a few moments to refresh once you click on it.) Notice Static Content is not installed.
3. Click on the **Add Role Services** button on the right. This will open the **Add Role Services** window.



4. Check the Static Content checkbox and click the **Next** button at the bottom.



5. Click the **Install** button to install the feature. You might be required to restart the server once the installation is completed.



1.6.4.3.3 Configuring Additional K2 Workspace Nodes

In order to add another K2 Workspace server, first make sure that the [NLB cluster is set up properly for the K2 Workspace](#) and that [DNS is set up for the cluster](#).

Once this is completed and all the prerequisites are installed on another IIS Server, install the K2 Workspace component on the second node, following the [instructions in the distributed installation guide](#).

1.6.4.4 K2 Environment

1.6.4.4.1 K2 Environment Security

K2 Environment Security and Permissions

After installing K2 blackpearl, there are some manual steps to configure the additional service accounts with permissions in K2. The K2 Service Account is granted Admin and Impersonate rights during configuration, which allows you to grant the additional rights necessary.



If you cannot set security rights in the K2 Workspace, try logging on as the K2 Service Account.

Default Permissions

The following permissions are set up during the Configuration process:

Default Permissions	
K2 Service Account	<ul style="list-style-type: none"> • Admin • Impersonate

Manual Configuration

In the table below, the additional permissions required are listed:

Necessary Permissions	
SharePoint Application Pool	<ul style="list-style-type: none"> • Admin • Impersonate • Export
K2 Workspace Application Pool	<ul style="list-style-type: none"> • Admin • Impersonate
K2 Administration Account	<ul style="list-style-type: none"> • Admin
Developer Accounts	<ul style="list-style-type: none"> • Export*

* To deploy a process the Export permission is required

To grant these permissions, perform the following steps:

1. Open Internet Explorer
2. Browse to the K2 Workspace Web Site
3. Click on **Management > Management Console**
4. Expand the node next to your K2 Server
5. Expand the node next to **Workflow Server**
6. Click on **Server Rights**
7. Click the **Add** button
8. In the dialog that opens, search for your service accounts
9. Check the box next to the accounts you want to give permission to, and click **OK**
10. Check the box(es) under the appropriate permission, as described in the table above
11. Click **Save**

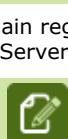
1.6.4.4.2 Adding Multiple Active Directory Domains

Introduction

K2 blackpearl supports the use of multiple domains. However, there can be only one label for an AD Provider.



The steps in this document refer to K2 blackpearl with Service Pack 1 or greater. Do not use these steps with pre-SP1 installations. K2 recommends upgrading to the latest service pack.



This document assumes some programming knowledge and familiarity with SQL Server 2005 or higher.

Domain registration is performed by inserting the domain name and associated label into the **SecurityLabels** table in the **HostServer** database. The label has two components: Authentication Provider and Role Provider.

If you have sub domains or domains in a different forest, you will have to add those domains to the same security label by modifying the **AuthInit** and **RoleInit** fields in the **SecurityLabels** table in the **HostServer** database.

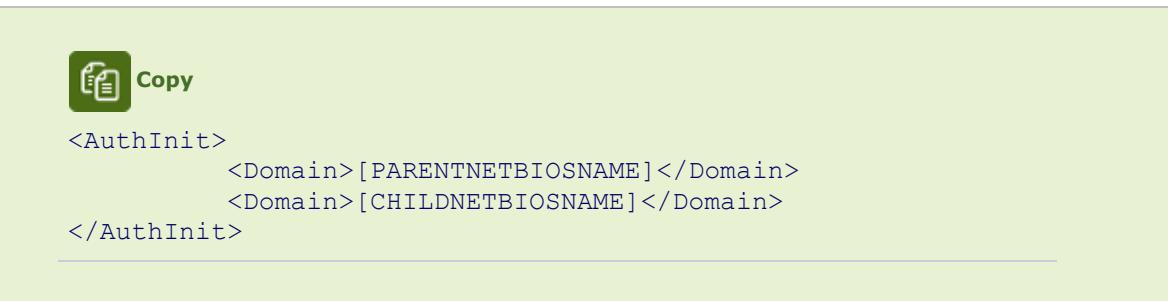
The following two placeholders are used in the examples below:

NETBIOS Name	LDAP String
[PARENTNETBIOSNAME]	LDAP://DC=ParentDomain,DC=COM
[CHILDNETBIOSNAME]	LDAP://DC=ChildDomain1,DC=ParentDomain,DC=COM



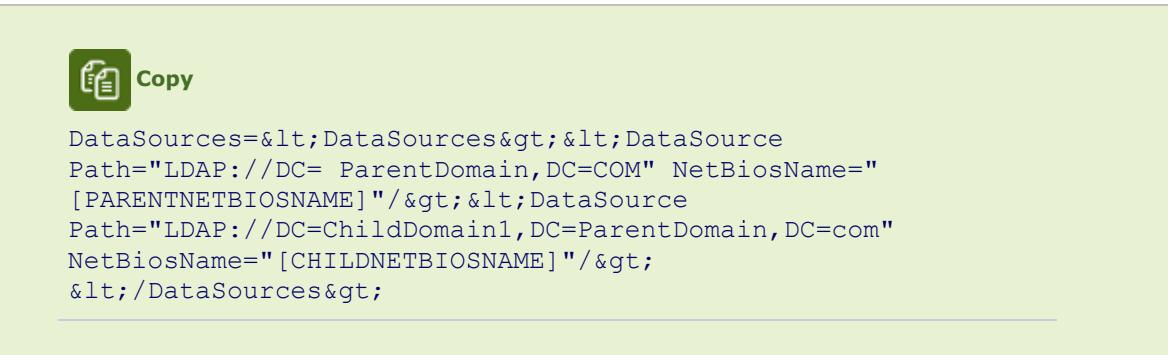
While the examples use a parent-child domain relationship, this is not required. If using domains in different forests, a one- or two-way trust relationship must be established. The type of relationship required depends on your environment.

The **AuthInit** field for the security label being modified should contain both domain NETBIOS names.



The **RoleInit** field for the same security label should be modified as follows:

1. Set the "MultiDomain" property to "True"
2. Edit the DataSources property by following the example below:



The escape characters "<" and ">" must be used as specified in the example above. Be careful to replace only the DataSources substring of the RoleInit string.

Implementation through K2 WorkSpace

See the following topic for how to add these domains to the same security label through the K2 Workspace interface: [K2 Management Console - Add Domains](#)

Implementation Script

The following query can be run to modify the security label to be updated. Note the placeholder values in the script are the

same as those used above. Additionally, the [LABELNAME] placeholder at the end of the script should be replaced with an actual value. This value is typically "K2" when using the security label for the default Active Directory provider.



```
Use K2HostServer
Update SecurityLabels
Set AuthInit = '<AuthInit><Domain>[PARENTDOMAIN]</Domain><Domain>
[CHILDDOMAIN]</Domain></AuthInit>',
Roleinit = '<roleprovider> <init>ADCache=10;LDAPPath=LDAP://DC=
[PARENTDOMAIN],DC=
[PARENTDC];ResolveNestedGroups=False;IgnoreForeignPrincipals=False;
IgnoreUserGroups=False;MultiDomain=True;DataSources=&lt;DataSources&gt;
&lt;DataSource Path="LDAP://DC=[PARENTDOMAIN],DC=[PARENTDC]" 
NetBiosName="[PARENTNETBIOSNAME]"&gt;
&lt;DataSource Path="LDAP://DC=[CHILDDOMAIN],DC=[PARENTDOMAIN],DC=
[PARENTDC]" NetBiosName="[CHILDNETBIOSNAME]"&gt;
&lt;/DataSources&gt;
</init>
<login />
<implementation assembly="ADUM, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=16a2c5aaaa1b130d" type="ADUM.K2UserManager2" />
<properties><user><property name="Name" type="System.String" />
<property name="Description" type="System.String" /><property
name="Email" type="System.String" /><property name="Manager"
type="System.String" /><property name="SipAccount" type="System.String"
/><property name="ObjectSID" type="System.String" /></user><group>
<property name="Name" type="System.String" /><property
name="Description" type="System.String" /></group>
</properties>
</roleprovider>
where SecurityLabelName='[LABELNAME]'
```

The following details about the database structure may or may not be useful, depending on modifications made to your database. Do not update database values beyond what is specified in this article unless instructed to do so by a support representative.

- **SecurityLabelID** is related to the SecurityLabelID field in the **SecurityCredentialCache** table. It is first generated in the SecurityLabels table so you can generate this manually if necessary.
- SecurityLabelName is the name of the particular SecurityLabel. It should be unique.
- **AuthSecurityProviderID** and **RoleSec** are the provider GUIDs found in SecurityProviders table.

Modifying the Workspace Web Site

When using multiple domains it is also important to modify the Workspace Web site to authenticate for each domain. To do this, follow these steps:

1. Open web.config file corresponding to the Workspace Web site, typically located at C:\Program Files\K2 blackpearl\Workspace\Site
2. Add a new AD Connection String in the **connectionString** section. For example:



```
<add name="ADConnectionString2"
connectionString="LDAP://Domain2.com" />
```

3. In the **membership** section add a new provider pointing to the newly added connection string. The name of the string needs to be unique and match the other example in Step 2. For example:



```
<add connectionStringName="ADConnectionString2"
connectionProtection="Secure" enablePasswordReset="false"
enableSearchMethods="true" requiresQuestionAndAnswer="false"
applicationName="/" description="Default AD connection"
requiresUniqueEmail="false" clientSearchTimeout="30"
serverSearchTimeout="30" attributeMapUsername="sAMAccountName"
name="AspNetActiveDirectoryMembershipProvider_Domain2"
type="System.Web.Security.ActiveDirectoryMembershipProvider, System.Web,
Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
```

1.6.4.4.3 Configure Workflow Tasks and History Lists

In order for SharePoint Workflow Integration processes to function properly, a Workflow History and Tasks list must be created in the SharePoint Site Collection where you will use this K2 feature.

The simplest way to configure this is to enable a SharePoint out-of-the-box workflow, which will create a Workflow History and Tasks list for you. For more information, see the following article: <http://office.microsoft.com/en-us/sharepointserver/HA101720071033.aspx#3>

1.6.4.5 Enable K2 Features

Once the K2 for SharePoint components are installed, they must be enabled manually from the K2 for SharePoint page within SharePoint Central Administration.

The following features are available after installation. The K2 features are enabled from SharePoint Central Administration and are enabled for a site collection.

K2 Features	
K2 Site Settings	Adds the K2 Site Settings link to the Site Actions menu, allowing for configuration of K2 components in the site collection.
K2 Management Console	Adds the Management Console link to the K2 for SharePoint page in Central Administration, K2 Process Portals and the K2 Site Settings page in the site collection.
K2 Designer for SharePoint	Adds the K2 Designer for SharePoint link to lists and libraries on a SharePoint site, allowing users with Contribute permissions to design and deploy K2 processes in SharePoint.
SmartObject Management	Adds the SmartObject Service Management link to the K2 Site Settings page, allowing for the configuration of SharePoint lists and libraries as K2 SmartObjects in the site collection.
K2 Web Parts	Enables the K2 Web Parts feature for a site collection.
K2 Web Designer	Adds a menu item to every list in a site collection in order to add or edit K2 workflow processes.
K2 Workflow Integration Content Types	Adds the necessary content types, mappings and the proxy which is used by K2 for SharePoint Workflow Integration.

To enable or disable these features, perform the following steps:

1. Open **SharePoint Central Administration** (Start > All Programs > Microsoft Office Server > SharePoint 3.0 Central Administration)
2. Click on the **K2 for SharePoint** tab
3. Select the applicable feature from the Features list and click the link
4. Select the site collection where the K2 SharePoint feature will be activated from the **Activation Location** drop down menu and click **Activate**



When a SharePoint site is extended it is necessary to "Activate All K2 Features and K2 Configuration Settings" on the main site in Central Administration>K2 for SharePoint to ensure that the K2 Features are applied to the extended sites.

1.6.4.5.1 Configuring the K2 Worklist SharePoint Web Part

1.6.4.5.1.1 Deploy the K2 Worklist Web Part

K2 blackpearl ships with a worklist web part for SharePoint. This enables users to see their worklist items directly in SharePoint. This way, the users do not have to go to a new, unfamiliar web site (the K2 Workspace) to interact with their worklist items.

To deploy the K2 Worklist web part, do the following steps:

1. Open **SharePoint Central Administration** (Start > All Programs > Microsoft SharePoint 2010 Products > SharePoint 2010 Central Administration)
2. Click on the **System Settings** option on the left
3. Click on **Manage farm solutions** under the **Farm Management** section, as shown below:

The screenshot shows the SharePoint 2010 Central Administration interface. The left navigation bar has 'System Settings' selected. In the main content area, there are three sections: 'Servers', 'E-Mail and Text Messages (SMS)', and 'Farm Management'. Under 'Farm Management', the 'Manage farm solutions' link is highlighted with a red box.

On the Manage Farm Solution page, you will see the k2worklistwebpart.wsp solution with a status of "Not Deployed"

4. Click on the **k2worklistwebpart.wsp** link. The solution page will load as per the image below:

The screenshot shows the SharePoint 2010 Central Administration interface, specifically the 'Solution Properties' page for the 'k2worklistwebpart.wsp' solution. The 'Deploy Solution' button is highlighted with a red box. The solution details table includes fields like Name, Type, Deployment Server Type, etc.

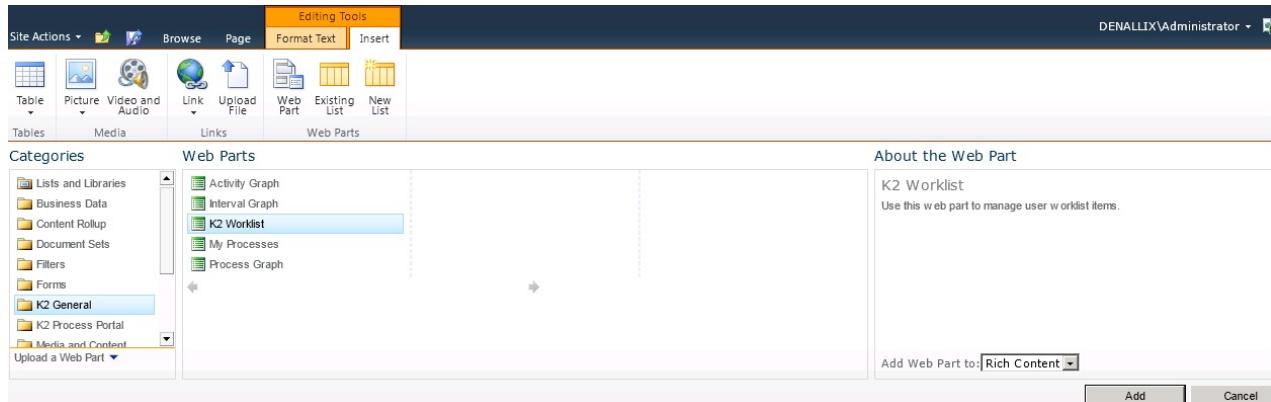
	Deploy Solution	Remove Solution	Back to Solutions
Name:	k2worklistwebpart.wsp		
Type:	Core Solution		
Contains Web Application Resource:	Yes		
Contains Global Assembly:	Yes		
Contains Code Access Security Policy:	No		
Deployment Server Type:	Front-end Web server		
Deployment Status:	Not Deployed		
Deployed To:	None		
Last Operation Result:	No operation has been performed on the solution.		

5. Click **Deploy Solution**
6. Select the correct Web Application to deploy the solution to, and click **OK** in the Deploy Solutions window

1.6.4.5.1.2 Add the K2 Worklist Web Part to a SharePoint page

Now that the Web Part solution has been deployed, you can add the Web Part to the SharePoint pages. The steps below will add the web part to the SharePoint portal home page, but it could just as easily be added to any page in your SharePoint environment:

1. Open the SharePoint Site where the K2 Worklist Web Part needs to be added
2. Click on the **Page** tab at the top of the SharePoint page
3. Click on the **Edit Page** icon
4. Click on the **Insert** tab at the top of the SharePoint page
5. Click on the **Web Part** icon
6. Select **K2 General** from the **Categories** section
7. Select **K2 Worklist** from the **Web Parts** section and click on **Add**. See image below:



8. The K2 Worklist web part will load as per the image below:



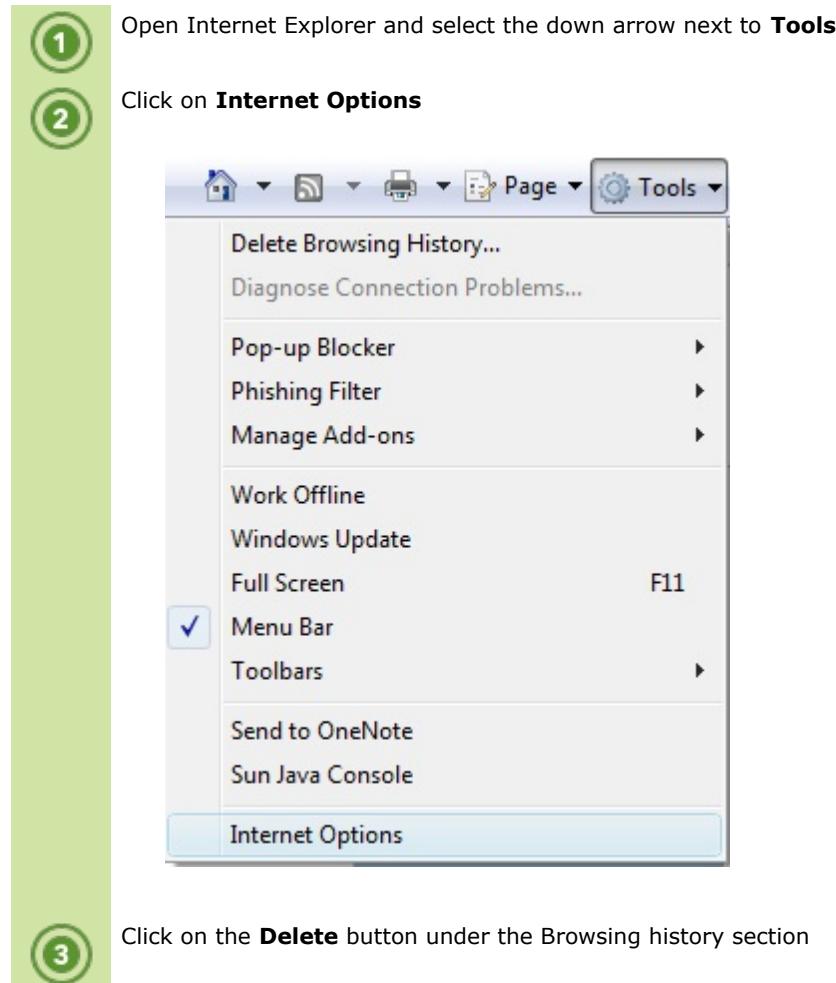
9. Click on the **Page** tab again and click on **Save and Close**
10. The **K2 Worklist** web part is now ready for use

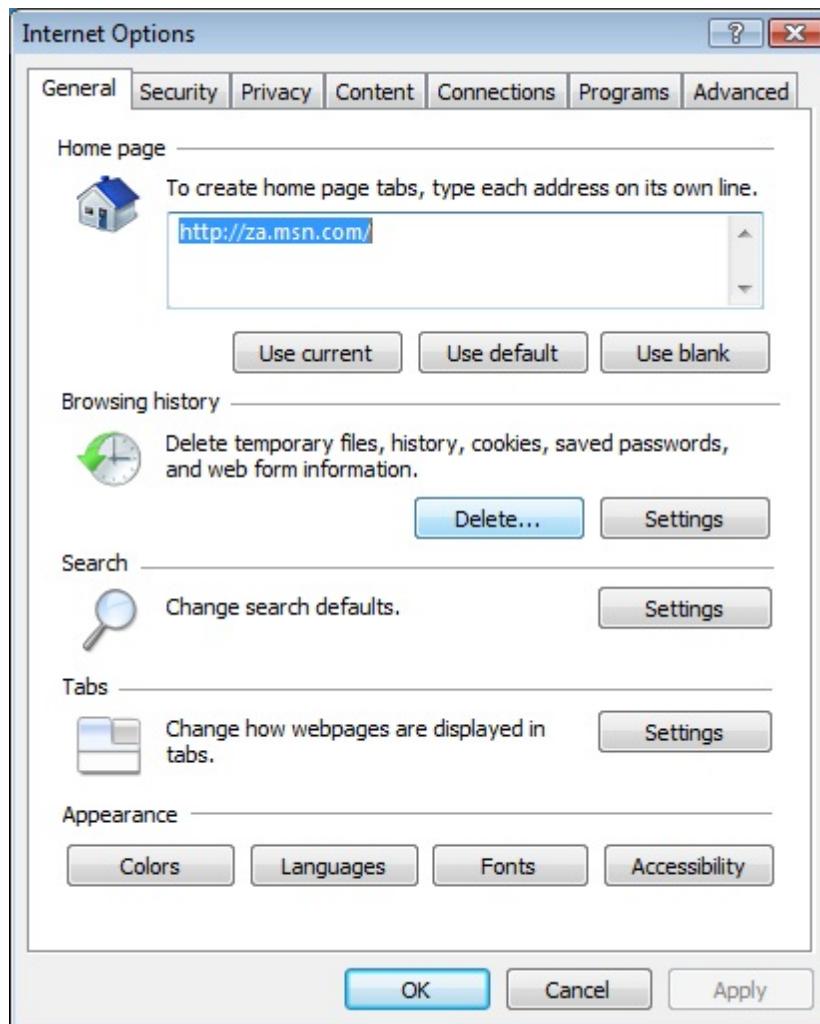
It is also important to test the K2 Worklist Web Part from a remote server, meaning a server or client machine other than the SharePoint server. This will test that Kerberos has been set up properly for the SharePoint Service Account. First, be sure to [set the Internet Options](#) on your browser correctly. Then, access the SharePoint page with the K2 Worklist Web Part, and make sure it renders properly. If no items are displayed and yet items should be, check the K2 Server in console mode for authentication errors. If you see authentication errors, be sure to double check the [SPNs for the SharePoint Service Account](#).

1.6.4.6 Clear cache after deploying K2 blackpearl

Clear cache after deploying K2 blackpearl

For this step the users are required to clear their Internet Explorer cache when a **change** is made to K2 Designer for SharePoint. It is recommended that the cache is also cleared after an upgrade to K2 blackpearl where the K2 Designer for SharePoint is updated. Below is an example of clearing the cache in Internet Explorer 7.





Click on the **Delete All...** button



(5)

Click **Yes**



Be sure to clear the cache after an upgrade or modifying the install of K2 designer for SharePoint, see the topic [Clear cache after deploying K2 blackpearl](#) for more information.

1.6.5 Introduction

What is the K2 blackpearl Configuration Analysis Tool ?

The K2 blackpearl Configuration Analysis Tool is an automated system analysis tool that will be available post installation if errors are detected. Owing to the complex nature of target environments and the large number of possible environments where a K2 blackpearl installation may take place, the tool's primary role is to provide visual representation of the component that has encountered an error catering to most possible scenarios. This enables the individual performing the installation to troubleshoot the error at the time of installation.

How and when to run the tool

The Configuration Analysis tool is available only after a K2 blackpearl installation takes place. It is available under the following circumstances

1. The Configuration Manager has detected an error and runs the tool after the installation completes
2. A user (no specific user rights are required to run the tool from the desktop), from the Start Menu runs the Configuration Analysis tool

K2 Server or Custom Installation vs Client Tools Only Installations

K2 Server and custom installations (no Designers installed) include servers and services that will require configuration and may encounter errors related to permissions, configuration and dependencies. These are the type of errors that the configuration tool was intended to detect and assist in resolving. If the installation only consisted of the [Client Components](#), then the Analysis Tool although available will not detect any components that will require a configuration analysis.

1.6.5.1 Summary of tool checks

The Configuration Analysis Tool checks a large number of tasks, with different sets of tasks checked depending on the installation type. The list shown here is not exhaustive but shows typical checks.

For a list of all tasks checked and notes on individual checks, see the "[Configuration Analysis tool all tasks.txt](#)" text file. The file shows an example of the output of the tool with task check successes and failures and the duration the check took. There are also notes concerning many of the checks with further instructions.



Definition of variables used in the explanation below:

[USERSNAME] = The user that is used to run the K2HostServer Service.
 [K2SITENAME] = The name that the user chose for the K2 site during installation (usually the name is just K2)
 [WORKSUSER] = The user under which the Workspace Application pool has been configured to run.
 [SHAREUSER] = The user under which the SharePoint Deployment Application Pool is running.

Server

File System Permissions

The file permissions task checks if the requested user has the rights that is required on the specified path.

- %SYSTEMROOT%\Temp – FullControl - [USERSNAME]
- %INSTALLDIR%\Host Server\Bin – Modify - [USERSNAME]
- %INSTALLDIR%\ServiceBroker – FullControl – Authenticated Users

Registry Permissions

- LocalMachine\SOFTWARE\SourceCode\Logging – FullControl - [USERSNAME]
- LocalMachine\System\CurrentControlSet\Services\EventLog – FullControl - [USERSNAME]
- LocalMachine\System\CurrentControlSet\Services\Winsock2 – FullControl - [USERSNAME]
- LocalMachine\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing – FullControl - [USERSNAME]
- LocalMachine\Software\Microsoft\Windows NT\CurrentVersion\Tracing\MSDTC – ReadKey; - [USERSNAME]
- LocalMachine\Software\Microsoft\Windows NT\CurrentVersion\Tracing\MSDTC\Misc – ReadKey; - [USERSNAME]
- LocalMachine\Software\Microsoft\MSMQ\Parameters – ReadKey;SetValue;CreateSubKey; - [USERSNAME]
- LocalMachine\Software\Microsoft\MSMQ\Parameters\MachineCache – ReadKey;SetValue;CreateSubKey; - [USERSNAME]
- LocalMachine\Software\Microsoft\MSMQ\Parameters\Security – ReadKey;SetValue;CreateSubKey; - [USERSNAME]
- LocalMachine\SYSTEM\CurrentControlSet\Services\Eventlog\Application – ReadKey;SetValue;CreateSubKey; - [USERSNAME]

Message Queue Enabled

Checks if MSMQ is installed correctly and checks that Directory Integration is installed.

As a test the tool tries to create a temporary queue with a random name and then tries to delete the queue.

MSDTC

MSDTC Network access

- Checks if MSDTC is configured correctly on the machine.

MSDTC Server is Running

- Checks if the MSDTC Service is running on the machine.

K2 blackpearl Server Running

- This task checks if the K2 Host Server Service is running on the machine.

Database Rebuild Indexes

Executes the DatabaseCheckIndexes stored procedure to ensure indexes have been rebuilt on K2Server, K2ServerLog and K2SmartBroker databases.

Visit [KB001281](#) to learn more about Rebuilding Indexes.

Database Symmetric Key checks

Symmetric keys for the K2HostServer, K2SmartBroker, K2SQLUM, K2SmartBox databases need to be detected.

K2 Workspace

Loopback Host Headers

- This task checks in the registry if loopback host headers are enabled on the machine.

IIS Permissions

1. [K2SITENAME] – Set Site Negotiation

This task checks the sites negotiation settings. If a SPN is detected for the Workspace Application Pool User ([WORKSUSER]) then it should be "Negotiate, NTLM". If a SPN is not detected it should be "NTLM". If it is on a workgroup machine it should be Anonymous Authentication.

• Workspace – Set Virtual Directory Negotiation

This task checks the virtual directories negotiation settings. If a SPN is detected for the Workspace Application Pool User ([WORKSUSER]) then it should be "Negotiate, NTLM". If a SPN is not detected it should be "NTLM". If it is on a workgroup machine it should be Anonymous Authentication.

• RuntimeServices – Set Virtual Directory Negotiation

This task checks the virtual directories negotiation settings. If a SPN is detected for the Workspace Application Pool User ([WORKSUSER]) then it should be "Negotiate, NTLM". If a SPN is not detected it should be "NTLM". If it is on a workgroup machine it should be Anonymous Authentication.

2. K2 Application Pool Settings

This task checks that the K2 Application Pool has been created and that it is running under the [WORKSUSER] account.

3. K2 Application Pool Account Permissions

Checks that the [WORKSUSER] is in the following group:

- IIS 6: IIS_WPG
- IIS 7: IIS_IUSRS

File System Permissions

The file permissions task checks if the requested user has the rights that is required on the path specified.

- %SYSTEMROOT%\Temp – Modify - [WORKSUSER]
- %SYSTEMROOT%\Temp – Modify – Authenticated Users
- %INSTALLDIR%\WebServices\RuntimeServices – ReadAndExecute – [WORKSUSER]
- %INSTALLDIR%\WorkSpace\ClientEventPages} – Traverse; ListDirectory; Append; WriteData; DeleteSubdirectoriesAndFiles; Delete – Authenticated Users

Web Deployment Projects

Checks if the Visual Studio 2008 Web deployment projects are installed on the machine

Reporting Indexing

Check the K2ServerLog database to see if the table indexes are created. Also gives information to the user on how to create the indexes if they are incorrect.

K2 Designer for SharePoint

File System Permissions

The file permissions task checks if the requested user has the rights that is required on the specified path.

- %INSTALLDIR%\Processes – Modify – Authenticated Users
- %COMMONAPPDATA%\SourceCode – FullControl – Authenticated Users

Database Permissions

The Central Application Pool User account must be one of the Server Roles on the SQL Server Instance

- Security Administrator
- System Administrator

Web Deployment Projects

Checks if the Microsoft Visual Studio 2008 Web Deployment Project is installed on the machine.

SharePoint

K2 Server Service Account

The K2 Server Service Account must be a member of the Site Collection Administrators Group for all site collections where the K2 features have been deployed

Loopback Host Headers

This task checks in the registry if loopback host headers are enabled on the machine.

Rights required to run the Analysis Tool on the SharePoint installation

This task checks if the logged on user is a Farm Administrator on SharePoint. The child tasks are dependant on the success of this task.

- Permission required to deploy SPWI processes

This is an informative item that informs the user that the users that deploy workflow integration processes need to be part of the Farm Admin and Site Collection Admin groups.

- Cross-Domain Data Connections

This task checks if Forms Services allows cross-domain data connections.

- File System Permissions

The file permissions task checks if the requested user has the rights that is required on the specified path.

1. %SYSTEMROOT%\Temp – Modify – Authenticated Users
2. %COMMONFILES%\Microsoft Shared\web server extensions\14\Template\Features – FullControl – Authenticated Users
3. %COMMONFILES32%\Microsoft Shared\web server extensions\14\Template\Features – FullControl – Authenticated Users. (Only on 64-bit systems)
4. %COMMONFILES%\Microsoft Shared\web server extensions\14\ISAPI – FullControl – Authenticated Users
5. %COMMONFILES32%\Microsoft Shared\web server extensions\14\ISAPI – FullControl – Authenticated Users. (Only on 64-bit systems)
6. %COMMONFILES%\Microsoft Shared\web server extensions\14\Template\Layouts – FullControl – Authenticated Users
7. %COMMONFILES32%\Microsoft Shared\web server extensions\142\Template\Layouts – FullControl – Authenticated Users. (Only on 64-bit systems)

- Web Deployment Projects

Checks if the Microsoft Visual Studio 2008 Web Deployment Project is installed on the machine.

K2 for Visual Studio and K2 Studio

File System Permissions

The file permissions tasks check if the requested user has the rights that is required on the path specified.

- %PROGRAMDATA%\SourceCode – FullControl – Authenticated Users

Web Deployment Projects

Checks if the Visual Studio 2008 Web Deployment Project is installed on the machine.

Exchange Integration Permissions

K2 Service Account

- Checks that the K2 Service Account is a member of the Exchange View-Only Administrators Active Directory group.

Example result: The K2Service account is a member of the Exchange Organization Administrators Active Directory group and has cached credentials. All server events where Create or Disable Mailbox are used should be configured to use this account in the "Run As" dialog.

- The K2Service account has the necessary Exchange Impersonation permissions on the Exchange server.

PowerShell 2.0 and WinRM Installed

- Checks for the correct version of PowerShell and WinRM. These features are required for permissions check and assignment on the Exchange Administration and Standard tasks.

CRM PrivUserGroup Permissions

The INSTALL\k2server account needs to be in the Organization's PrivUserGroup for CRM.

This is a requirement in CRM when using K2 Pass-Through Authentication (ClientWindows) where the K2Service Account needs to impersonate as the Application Pool account when the account is anonymous.

This change needs to be made in Active Directory.

1.6.5.2 Analyze Configuration



The Configuration Analysis tool will only check and analyze items that are present. It will not report on items that are absent or not installed.

Configuration Analysis

The Configuration Analysis tool shown below has been used to analyze an installation. Items with errors have been flagged by a red X, indicating that this item has not been configured correctly and requires repair. Items that have been installed and configured correctly are indicated by the green validation mark while items with warnings are indicated with the yellow exclamation mark. In all cases more information is supplied in the right-hand pane.

K2 blackpearl Configuration Analysis

Configuration Analysis

Analyze All Analyze Repair All Repair Export

Standard - Exchange Integration Permissions

Analysis Result: Warning.

The user DENALLIX\Administrator does not have the required permissions on the Exchange server DLX.denallix.com. The account must have these permissions in Exchange in order for the K2 integration to function properly.

The following rights are still required for Impersonation:

Select Repair to attempt to grant these permissions. If the permission cannot be granted automatically, you can run the following command from the Exchange

Back Next Cancel

Item	Description	How to use it
Analyze All	Starts the automatic analysis of a installation	If the Analysis tool is being run for the first time, or if verification is required that changes have repaired errors, click the Analyze All button to analyze your installation.
Analyze	Starts the analysis of the selected branch	If verification is required that a change has repaired an error, select the relevant branch and click the Analyze button to analyze your installation. Please note that the Analyze button is only available for child nodes.
Repair	Repairs the selected item	Select a specific item that has an error and then click Repair to attempt a repair on the item.
Repair All	Repairs all items where there is an error	No individual items need be selected. Clicking on the Repair All option automatically tries to repair all items in Error or in Warning state starting at the top and working down the list.
Export	Exports the error report	The information reported by the Configuration Analysis tool can be exported to a text file. The file will be in plain formatting and contain a printer friendly and e-

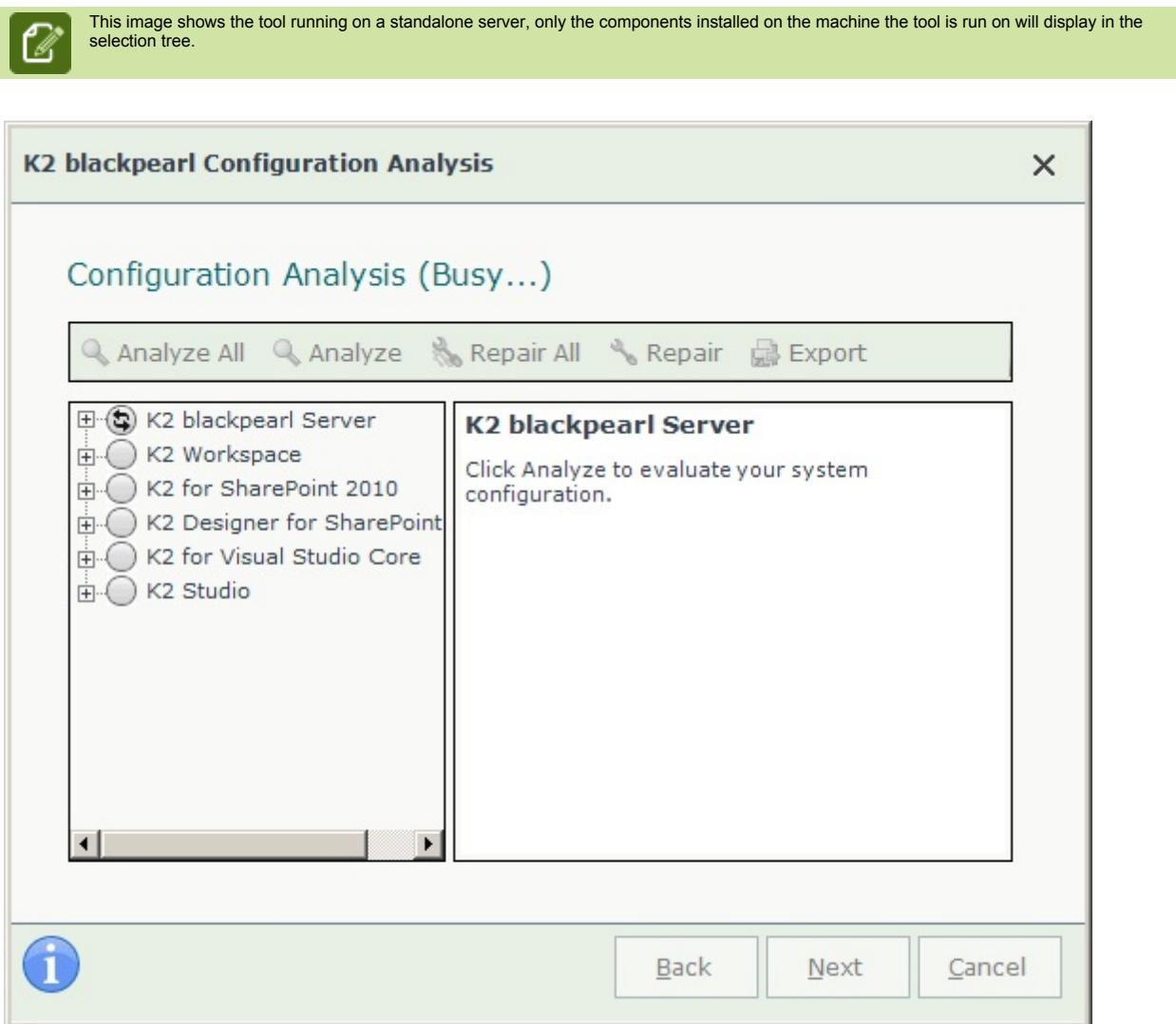
		mail friendly version of the information displayed graphically by the tool.
Icons		
	Information	This shows information relating to the node indicated.
	No Errors	This icon is used for the parent node or for a node item that has no errors and is installed and configured correctly.
	Attention Required	This icon appears only at a parent node, when an error has been detected on a sub item.
	Errors	The item with an error is indicated with the White X on red icon.
	Warnings	The item with a warning is indicated with the an exclamation mark icon.
User Page Controls for the tool running in the Setup Manager		
	Opens help	Opens the help system to the Configuration Analysis tool section.
Back	Steps backwards	During Setup, indexes to the previous setup step.
Next	Steps forwards	During Setup, indexes to the following setup step.
Cancel	Cancels Setup	Cancels installation and closes down the setup manager.
User Page Controls for the tool running from the Start menu		
Close	Closes the page	Click the Close button to close and exit the analysis tool

1.6.5.3 Which Machines to Analyze

Which Machines to Analyze

The machine(s) that can be analyzed for configuration errors are the following, K2 Server, K2 Workspace, K2 Designer for Visual Studio, K2 Studio, or the K2 for SharePoint Server. Certain components will not return any configuration reporting information and these are the machines where the installation included Client components or are Client Components Machines; reporting detail on the server or service components will still be returned however.

An example of the Analysis Tool in operation is shown below.



1.6.6 Unattended Installer

Unattended Installer

The unattended installation uses an XML file to install and configure the operating system, there is minimal interaction by administrators or technicians during the setup process.

Greater consistency during a rollout

By using the same XML file to install and configure the operating system, you can ensure that all of the computers in your organization are set up exactly the same way.

Limitations

The installer does not support Modify or Repair. To perform a repair and modify open the K2 Setup Manager and perform the actions through the UI.

Shorter installation times

The unattended installation is faster than interactive setup because Setup does not have to prompt administrators or technicians for configuration information and wait for them to enter it; instead, Setup reads configuration settings from the XML file.

[Unattended Installation Dependencies](#)

[Generate System Key](#)

[Generate Silent / Unattended Installation XML File](#)

[Silent/Unattended Installation \(using the XML File\)](#)

[Unattended Distributed Installation](#)

[Unattended Installer - Upgrade](#)

[Setup Options](#)

[Additional Notes](#)

1.6.6.1 Unattended Installation Dependencies

Unattended Installer Dependencies

To perform an unattended installation, you need the following:

- System Key - [Generate System Key](#)
- License Key
- Operating system files, including the Windows Setup programs installed (K2 Component Dependencies)
- XML File - [Generate Silent / Unattended Installation XML File](#)



The Setup Manager is a wizard-like tool that prompts you for a series of configuration parameters, and then writes your responses to a XML file.

1.6.6.2 Generate System Key

Unattended Installer - Generate System Key

Run **setup.exe /systemkey:"{path}"** from the command prompt, this will generate the System Key.

Parameters	
{path}	This is the path where the application will be installed. This is required to generate the System Key.

Output:

Prints the System Key to the Command prompt in this format **System Key: xxxxxxxxxxxxxxxx**

1.6.6.3 Generate Silent / Unattended Installation XML File

Generate Silent / Unattended Installation XML File

Run **setup.exe /output:"{filename}"** which will open the Setup wizard to obtain all settings from user, click on **Finish** to generate an XML file with user-specific settings.



The XML configuration file is used for silent/unattended installation.

The following command does not install, just builds the XML file:

Syntax:

`setup.exe /output:"{filename}"`

Parameters	
<code>{filename}</code>	This is the name of the XML file that will be generated.

Output:

Launches the Installer UI, gathers all the information, and then closes upon creating the XML file containing all the options as specified in the Installation wizard.

1.6.6.4 Silent/Unattended Installation (using the XML File)

Silent / Unattended Installation (using the XML File)

Install K2 without any user input, by simply running **setup.exe /install:"{filename}" /loglevel:{loglevel}** with a valid XML configuration file.

Parameters	
{filename}	The name of the XML file with all the installation options (including System Key and License Key).
{loglevel}	An optional parameter that specifies the Log Level, based on the following list: 1 – Verbose Logging 2 – Information, Warning and Errors 3 – Warning and Errors Only (Default) 4 – Errors Only Note: If this parameter is not specified, the default is '3'.

Output:

Print the progress and any errors for the installation/configuration to the command window.



The Setup.exe command can determine whether the setup being run is for a new installation, or for a configuration.

1.6.6.5 Unattended Distributed Installation

Unattended Installer - Unattended Distributed Installation

A distributed installation XML file can be created by removing certain components from a Full Installation XML file.



The K2 Pass-Through Authentication option is only valid for a distributed installation see the section on [Additional Notes](#)

Distributed Installation Steps:



Open the **Command Prompt**, and type the following syntax: **C:\Pearl>setup.exe /output:unattended.xml** to start building the XML file.



The **K2 Setup Manager** will start.



It is recommended to do a **Full Installation** (all components selected on the Select Components screen).



This will not install the components, it only builds the XML file.



When the installation is complete, the XML file can be edited by using a text editor such as Notepad.



A distributed installation XML file can then be saved by deleting components from the 'Full Installation' XML file, as required.



Please note that the **Configuration** component is required to be installed with all the other components.



After the XML file is built and edited the following command will start the installation:

Syntax: c:\Pearl>setup.exe /install:unattended.xml

1.6.6.6 Unattended Installer - Upgrade

Unattended Installer - Upgrade

When upgrading using the Unattended Installer, the component section of the XML file is ignored, only previously installed components will be upgraded. With the exception of K2 blackpoint, where the K2 Workspace component will be installed when upgrading to K2 blackpearl.

Upgrading from K2 blackpoint to K2 blackpearl

When upgrading from K2 blackpoint to K2 blackpearl, the following must be noted:

- The Installation path will be the original path used when K2 blackpoint was installed, for example: "C:\Program Files\K2 blackpoint"
- A new license key is required when upgrading from K2 blackpoint to K2 blackpearl
- K2 Workspace will be installed when upgrading from K2 blackpoint to K2 blackpearl

To run the Unattended Upgrade installer the following command is used:

Syntax:

setup.exe /upgrade:"{filename}"

Parameters	
{filename}	This is the name of the XML file that will be used for the upgrade installation.

Output:

Launches the Setup Manager and then starts the upgrade.

Upgrade Steps:



It is recommended to use the **XML file** that was used during a **Full Installation** for the XML Upgrade file.



This will not install new components, it only upgrades the installed components.



The following XML file variables can be edited as required to create the XML Upgrade file:



Copy K2 Service User name and password variables

```
<add key="[USERSNAME]" value="K2WORKFLOW\User"/>
<add key="[USERSPASS]" value="Pass"/>
```



Copy K2 Host Server

```
<add key="[HOSTSERVERDBNAME]" value="K2HostServer"/>
<add key="[HOSTSERVERCONNECTIONSTRING]" value="Data Source=SA-SCINSTALL2\instance01;Initial Catalog=K2HostServer;integrated security=sspi"/>
<add key="[HOSTSERVERDBSQLSERVER]" value="SA-SCINSTALL2\instance01"/>
```



After editing the XML file, open the **Command Prompt**, and type the following syntax:
C:\Pearl>setup.exe /upgrade:"Upgrade.xml" to start the XML file.



The **K2 Setup Manager** will start.



When the upgrade installation is complete, the XML file can be edited by using a text editor such as Notepad.

1.6.6.7 XML File Parameters

Unattended Installer - XML File Parameters

The table below provides information on the parameters that can be edited in the Installation XML file:

Example Installation XML File	Parameter Used For:	Component Applicable For:	What can be changed?
<PRODUCT>	N/A	N/A	N/A
<COMPONENTS>	Components Group	N/A	N/A
<CORE>			
<SERVER>	Installing K2 Host Server Component	Server	Can be removed to NOT install server
<STUDIO>	Installing K2 for Visual Studio Components	K2 for Visual Studio 2010	Required for K2 for Visual Studio 2010
<VS2010>	Installing K2 for Visual Studio 2010 Components	K2 for Visual Studio 2010	Requires <STUDIO/> but can be removed to NOT install K2 for Visual Studio 2010
<K2STUDIO>	Installing K2 Studio Component	K2 Studio	Can be removed to NOT install K2 Studio
<MOSS2010>	Installing K2 for SharePoint Component	K2 for SharePoint	Can be removed to NOT install server
<WEBDESIGNER2010>	Installing Web Designer Component	K2 Web Designer	Requires <MOSS2010/> and can be removed to NOT install K2 Web Designer
<WORKSPACE>	Installing K2 Workspace Component	K2 Workspace	Can be removed to NOT install K2 Workspace
<CONFIGURATION>	Installing K2 Setup Manager Component	All	Should NOT be removed otherwise the install will
<COMPONENTS>	End of components section	N/A	N/A<
<VARIABLES>	Variables Group	N/A	N/A
<add key="[INSTALLDIR]" value="C:\Program Files\K2 blackpearl\"/>	This is the installation location of the components.	All	This can be any fully qualified path and must end in '\'
<add key="[WORKFLOWSERVERPORT]" value="5252"/>	Workflow server port	All	Any unassigned port
<add key="[LBDISCOVERYPORT]" value="49600"/>	Host Server Discovery port	K2 Host Server	Can be any available port but in a load balanced environment this should not be 49600.
<add key="[LICENSEKEY]" value="16B41C8D03430F6ED325"/>	K2 Host Server	K2 Host Server	License Key
<add key="[MACHINEKEY]" value="D29A0A0B174E7CD3"/>	K2 Host Server	K2 Host Server	Machine specific key empty if using trial license for K2 blackpoint.
<add key="[LICENSEUSER]" value="" />	K2 Host Server	K2 Host Server	User name used to obtain the license key from the portal for evaluation
<add key="[LICENSETYPE]" value="SOFTWARE"/>	K2 Host Server	K2 Host Server	EVALUATION, DEVELOPER,

			ENTERPRISE, SOFTWARE, TEAM, STANDARD, PARTNER (note if the license type is incorrect the K2 Host Server may not function as expected)
<add key="[LICENSEDPRODUCT]" value="K2BLACKPEARL"/>	K2 Host Server	K2 Host Server	Licensed product type
<add key="[LICENSEPASS]" value="D29A0A0B174E7CD3"/>	K2 Host Server	K2 Host Server	Password used to obtain the license key from the portal for evaluation
<add key="[LBHOSTSERVERNAME]" value="demo"/>	Load Balanced Host Server name	All	Load Balanced Host Server name. This must be the same as the [HOSTSERVERNAME] in a non-clustered environment.
<add key="[ISNLB]" value="false"/>	Variable stating if the there is a K2 Host Server Farm	K2 Host Server	True, false
<add key="[HOSTSERVICENAME]" value="K2 blackpearl Server"/>	K2 Host Server Service name	K2 Host Server	K2 blackpearl Server
<add key="[SMTP]" value="zamail"/>	Mail server name	All	The mail server the K2 must use
<add key="[HOSTSERVERNAME]" value="demo"/>	Current host server	All	Current host server name
<add key="[K2SITENAME]" value="" />	K2 Workspace Site Name	K2 Host Server, K2 Workspace	The is K2 Website Name (This site MUST already exist)
<add key="[K2SITEURL]" value="" />	K2 Workspace site UR	K2 Host Server, K2 Workspace	The is K2 Workspace URL (i.e. http://servername:80)
<add key="[K2SITEID]" value="" />	K2 Workspace Site ID	K2 Host Server, K2 Workspace	The is K2 Workspace site ID
<add key="[K2APPPPOOL]" value="K2 blackpearl Application Pool"/>	K2 Workspace Application Pool name	K2 Host Server, K2 Workspace	Application Pool Name
<add key="[WORKSUSER]" value="K2DEMO\Administrator"/>	Application Pool User name	K2 Host Server, K2 Workspace	The Domain\UserName to be used for the application pool identity
<add key="[WORKSPASS]" value="bPHNUsx068icmiWTpB1VaA=="/>	Application Pool password	K2 Host Server, K2 Workspace	The password to be used for the application pool identity, this can be plain text or the encrypted value obtained using the setup.exe.
<add key="[WORKSPSID]" value="S-1-5-21-1746230864-3757964239-881876598"/>	The security identifier of the Application pool user	K2 Host Server, K2 Workspace	The security identifier of the Application pool user
<add key="[REPORTPORTSITE]" value="demo:80"/>	Name of the report website	K2 Host Server, K2 for Reporting	Name of the report website without the http:// or https://
<add key="[REPORTSITENAME]" value="http://DEMO:80"/>	Report Site URL	K2 Host Server, K2 for Reporting	Report Site URL
<add key="[REPORTSERVERVDIR]" value="ReportServer"/>	Report Server virtual directory	K2 Host Server, K2 for Reporting	Report Server virtual directory
<add key="[REPORTPORTSITEURL]" value="http://DEMO:80"/>	Report Site URL	K2 Host Server, K2 for Reporting	Report Site URL

<add key="[FULLREPORTSITEURL]" value="http://DEMO:80/ReportServer"/>	Complete report server URL	K2 Host Server, K2 for Reporting	Report Site URL including the report server virtual directory
<add key="[REPORTSITEPATH]" value="c:\Program Files\Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting Services\ReportServer"/>	Path to the RSrvpolicy.config file in reporting services	K2 for Reporting	Path to the RSrvpolicy.config file in reporting services
<add key="[HOSTSERVERDBNAME]" value="HostServer"/>	Host server database name	All	The existing database name or a unique name
<add key="[HOSTSERVERDBSQLSERVER]" value="DEMO"/>	Host Server SQL server	All	The SQL server where the host server database resided
<add key="[HOSTSERVERCONNECTIONSTRING]" value="Data Source=DEMO;Initial Catalog=HostServer;integrated security=sspi"/>	The database connection string	K2 Host Server	The database connection string<
<add key="[ADMINUSER]" value="K2DEMO\Administrator"/>	K2 Administrator Name	K2 Host Server	Domain\User
<add key="[ADMINPASS]" value="bPHNUsx068icmiWTpB1VaA=="/>	K2 Administrator password	K2 Host Server	The password to be used for the K2 Administrator, this can be plain text or the encrypted value obtained using the setup.exe.
<add key="[USERSNAME]" value="K2DEMO\Administrator"/>	K2 Service account Name	K2 Host Server, K2 for Workspace	Domain\User
<add key="[USERSPASS]" value="bPHNUsx068icmiWTpB1VaA=="/>	K2 Service account password	K2 Host Server	The password to be used for the K2 Service account, this can be plain text or the encrypted value obtained using the setup.exe.
<add key="[FULLUSERSNAME]" value="K2DEMO\Administrator"/>	K2 Administrator Name	K2 Host Server, K2 for Workspace<	Domain\User
<add key="[SOURCECODECOMMONAPPDATA]">C:\ProgramData\SourceCode\</add>	Path to SourceCode config file	All	N/a
<add key="[SETSPN]">False</add>	Set site SPN indicator	Workspace	Whether to set service principal name on Workspace server
<add key="[LBSITENAME]">http://DLX:81</add>	Load balancing site name	Workspace	Name of load balancing site
<add key="[VS8DIR]">C:\Program Files (x86)\Microsoft Visual Studio 8\Common7\IDE\</add>	VS2008 location	K2 for VS2008	N/A
<add key="[SETSPN]">False</add>	Set K2 Server SPN indicator	K2 Server	Whether to set service principal name on K2Server
<add key="[VS10DIR]">c:\program files (x86)\microsoft visual studio 10.0\common7\IDE\</add>	VS2010 location	K2 for VS2010	N/A
<add key="[INSTALLUSER]">DENALLIX\Administrator</add>	K2 Installation user	K2 Installation	User that runs K2 installation
<add key="[WORKSPACEDISTRIBUTED]">false</add>	Indicates a distributed Workspace installation	Workspace	Single or distributed Workspace installation
<add key="[SIMPLEINSTALL]">false</add>	Indicates a Simple Full install	All	Simple or custom installation
<add key="[USRMGRTYPE]">UMTYPE_ADUM</add>	User manager type	All	ADUM or SQLUM
<add key="[PTA_OPTION]">ClientWindows</add>	Pass through authentication indicator	All	Whether pass through authentication will be used or not

<add key="[NOTIFYEMAIL]">k2service@denallix.com</add>	e-mail address for task notifications	K2 Server	e-mail address used for notifications
<add key="[HOSTSERVERPORT]">5555</add>	Hostserver port	All	Any unassigned port
<add key="[PREVK2SITENAME]" />	Legacy Workspace site name	Workspace	N/A
<add key="[K2SITEPORT]">81</add>	Workspace port	All	Any unassigned port
<add key="[XML_SHAREPOOL]"> <variables> <farm value="99e871a8-b181-4233-8458-2c66e104a220"> <XML_SHAREPOOL>K2 for SharePoint</XML_SHAREPOOL> </farm> </variables> </add>	K2 for SharePoint application pool name	K2 for SharePoint	K2 for SharePoint application pool
<add key="[CRMURL]">http://crm.denallix.com</add>	CRM site URL	K2 Server	CRM Site URL
<add key="[CRMORGANIZATION]">Denallix</add>	CRM organization	K2 Server	CRM organization setting
<add key="[K2HOSTCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=DLX;Port=5555</add>	Connection string for K2 Hostserver	All	Connection string for K2 Hostserver
<add key="[K2WFCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=DLX;Port=5252</add>	Connection string for K2 Workflow server	All	Connection string for K2 Workflow Server
<add key="[INCOMING_EXCH_SVR]">DLX.denallix.com</add>	Incoming Exchange server name	K2 Server, Client components	Name of incoming Exchange server
<add key="[INCOMING_EXCH_PORT]">25</add>	Incoming Exchange Server port	K2 Server, Client components	Any unassigned port
<add key="[INCOMING_EXCH_TLS]">BootTls</add>	Exchange server BootTLS setting	K2 Server	BootTLS/None
<add key="[SMTPCONNECTIONSTRINGANONYMOUS]">Port=25;TLS=BootTls;HostName=DLX.denallix.com;Authentication=Anonymous</add>	Anonymous SMTP connection string	K2 Server	Anonymous SMTP connection string
<add key="[EXCHANGECONNECTIONSTRING]">Autodiscover=True</add>	Exchange autodiscover setting	K2 Server, Client components	N/A
<add key="[SMTPCONNECTIONSTRING]">Port=25;TLS=BootTls;HostName=DLX.denallix.com;Authentication=Windows</add>	Connection string for SMTP server	K2 Server	Connection string for SMTP server
<add key="[SMTPUSER]">DENALLIX\K2Service</add>	SMTP user name	K2 Server	The Domain\User name to be used for the SMTP server
<add key="[SMTPUSERPASS]">1ZGFq4Yt3n2uHAqsw36jSA==</add>	SMTP user password	K2 Server	The password to be used by the SMTP user. This can be plain text or the encrypted value obtained using the setup.exe.
<add key="[SERVICEACCOUNTK2FQN]">K2:DENALLIX\K2Service</add>	FQDN for Server service account user	K2 Server	FQDN for Server service account user
<add key="[INCOMINGNOTIFYEMAIL]">k2service@denallix.com</add>	Incoming notifications e-mail address	K2 Server	Incoming notifications e-mail address
<add key="[SMARTACTIONSENABLED]">true</add>	SmartActions enabled/disabled	K2 Server	Usage of SmartActions
<add key="[EXCHANGEDEFAULTSERVER]">DLX.denallix.com</add>	Default Exchange server name	K2 Server	Default Exchange server name
<add key="[EXCHANGEDEFAULTSTORAGEGROUP]" />	Default Exchange storage group	K2 Server	Default Exchange storage group
<add key="[EXCHANGEDEFAULTMAILBOXDATABASE]">mailbox database 0679148940</add>	Default Exchange mailbox database	K2 Server	Default Exchange mailbox database
<add key="[EWSURL]">https://dlx.denallix.com/EWS/Exchange.asmx</add>	EWS URL	K2 Server	EWS URL

<add key="[ExchangeVersion]">Exchange2010</add>	Exchange version	K2 Server	Version of Exchange installed on environment
<add key="[ISEXCH2007]">false</add>	Exchange 2007 indicator	K2 Server	Version of Exchange installed
<add key="[ISEXCH2010]">true</add>	Exchange 2010 indicator	K2 Server	Version of Exchange installed
<add key="[USEAUTODISCOVER]">False</add>	Autodiscover	Exchange	Set Autodiscovery
<add key="[USEEXCHANGE]">True</add>	Exchange indicator	Exchange	Set whether Exchange will be used
<add key="[USESMTP]">False</add>	SMTP indicator	Exchange	Set whether SMTP will be used
<add key="[VS11DIR]"/> <add key="[INSTALLUSER]">GOLF\K2Server</add>	VS2012 location	K2 for VS2012	N/A
<add key="[CRMVERSION]">CRM 2011</add>	CRM Version	CRM	Version of CRM Installed on Environment
<add key="[EXCH_ADMINISTRATION]">true</add>	Enable Administrative Exchange Integration indicator	Exchange	Enable Administrative Exchange Integration
<add key="[EXCH_MANAGEMENT]">true</add>	Enable Standard Exchange Integration indicator	Exchange	Enable Standard Exchange Integration
<add key="[EXCHANGEADMINUSER]">GOLF\K2hostserver</add>	Exchange administrator	Exchange	Set Exchange Administrator
<add key="[EXCHANGEAUTODISCOVERENABLE]">False</add>	Exchange Autodiscover indicator	Exchange	N/A
<add key="[EXCHANGECONNECTIONSTRING]">Autodiscover=True;URL=https://sa-ex01.k2workflow.com/EWS/Exchange.asmx</add>	Exchange Connection String	Exchange	Full Exchange Connection String
<add key="[EXCHANGEDEFAULTSERVER]">blackstone.golf.com</add>	Default Exchange Server	Exchange	Set Default Exchange Server
<add key="[EXCHANGEEMAIL]">K2hostserver@Golf.COM</add>	On-Premises Exchange email	Exchange	On-Premises Exchange email address
<add key="[EXCHANGEONLINE]">False</add>	Exchange Online indicator	Exchange	Indicate whether Exchange Online will be used
<add key="[EXCHANGESTANDARDUSER]">GOLF\K2hostserver</add>	Standard Exchange Username	Exchange	Set standard Exchange username
</VARIABLES>	End of configuration variables	N/A	N/A
</PRODUCT>	N/A	N/A	N/A

1.6.6.7.1 Full Installation XML - Example

Unattended Installer - Full Installation XML File

The following XML code is an example of a Full installation:



Copy Full Installation XML

```

<PRODUCT>
  <COMPONENTS>
    <CORE/>
    <SERVER/>
    <STUDIO/>
    <VS2010/>
    <K2STUDIO/>
    <WORKSPACE/>
    <MOSS2010/>
    <WEBDESIGNER2010/>
    <CONFIGURATION/>
  </COMPONENTS>
<VARIABLES>
  <add key="[SOURCECODECOMMONAPPPDATA]">C:\ProgramData\SourceCode</add>
  <add key="[SETSITESPN]">False</add>
  <add key="[INSTALLDIR]">C:\Program Files (x86)\K2 blackpearl</add>
  <add key="[K2SITEURL]">http://DLX:81</add>
  <add key="[LBSITENAME]">http://DLX:81</add>
  <add key="[VS8DIR]">C:\Program Files (x86)\Microsoft Visual Studio
8\Common7\IDE</add>
  <add key="[SETSPN]">False</add>
  <add key="[VS10DIR]">c:\program files (x86)\microsoft visual studio
10.0\common7\IDE</add>
  <add key="[VS11DIR]" />
  <add key="[INSTALLUSER]">DENALLIX\Administrator</add>
  <add key="[WORKSPACEDISTRIBUTED]">false</add>
  <add key="[MACHINEKEY]">xxxxxxxxxxxxxxxxxx</add>
  <add key="[SIMPLEINSTALL]">false</add>
  <add key="[USRMGRTYPE]">UMTYPE_ADUM</add>
  <add key="[LICENSEUSER]" />
  <add key="[LICENSETYPE]">SOFTWARE</add>
  <add key="[LICENSEDPRODUCT]">K2BLACKPEARL</add>
  <add key="[LICENSEDADATA]" />
  <add key="[LICENSEPASS]">xxxxxxxxxxxxxxxxxxxx</add>
  <add key="[LICENSEKEY]">xxxxxxxxxxxxxxxxxxxx</add>
  <add key="[LBHOSTSERVERNAME]">DLX</add>
  <add key="[ISNLB]">false</add>
  <add key="[PTA_OPTION]">ClientWindows</add>
  <add key="[HOSTSERVICENAME]">EventSystem</add>
  <add key="[HOSTSERVERNAME]">DLX</add>
  <add key="[HOSTSERVERPORT]">5555</add>
  <add key="[WORKFLOWSERVERPORT]">5252</add>
  <add key="[LBDISCOVERYPORT]">49599</add>
  <add key="[DLX]"><Vars><Var Name=""[PREVK2SITENAME]"
Value="" /></Vars></add>
  <add key="[K2SITEPORT]">81</add>
  <add key="[K2SITENAME]">K2Workspace</add>
  <add key="[K2SITEID]">-1</add>
  <add key="[K2APPPPOOL]">K2 blackpearl</add>
  <add key="[XML_SHAREPOOL]"><variables><farm value=""99e871a8-b181-4233-
8458-2c66e104a220""><XML_SHAREPOOL>K2 for SharePoint</XML_SHAREPOOL></farm>
</variables></add>
  <add key="[WORKSUSER]">DENALLIX\k2webservice</add>
  <add key="[WORKSPASS]">1ZGFq4Yt3nqsw36jSA==</add>
  <add key="[WORKSPSID]">S-1-5-21-1182838845-2098967006-2361148536</add>
  <add key="[LBHOSTSERVERFQDN]">DLX.denallix.com</add>
  <add key="[REPORTPORTSITE]" />
  <add key="[REPORTSITENAME]" />
  <add key="[REPORTSERVERVDIR]" />
  <add key="[REPORTPORTSITESURL]" />
  <add key="[REPORTSITESPATH]" />
  <add key="[FULLREPORTSITESURL]" />

```

```

<add key="[CRMURL]">http://crm.denallix.com</add>
<add key="[CRMORGANIZATION]">Denallix</add>
<add key="[CRMVERSION]">4.0</add>
<add key="[HOSTSERVERDBNAME]">K2</add>
<add key="[HOSTSERVERDBSQLSERVER]">DLX</add>
<add key="[HOSTSERVERCONNECTIONSTRING]">Data Source=DLX;Initial Catalog=K2;integrated security=sspi;Pooling=True</add>
<add key="[K2SQLUMDBSQLSERVERPARSED]">DLX</add>
<add key="">
[K2HOSTCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True
;EncryptedPassword=False;Host=DLX;Port=5555</add>
<add key="">
[K2WFCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;E
ncryptedPassword=False;Host=DLX;Port=5252</add>
<add key="[ADMINUSER]">DENALLIX\Administrator</add>
<add key="[ADMINPASS]">1ZGFq4Y2uHAqsw36jSA==</add>
<add key="[USERSNAME]">DENALLIX\k2service</add>
<add key="[USERSPASS]">1ZGF3n2uHAqsw36jSA==</add>
<add key="[FULLUSERSNAME]">DENALLIX\k2service</add>
<add key="[USEAUTODISCOVER]">True</add>
<add key="[EWSURL]">https://dlx.denallix.com/EWS/Exchange.asmx</add>
<add key="[SMTP]">dlx.denallix.com</add>
<add key="[NOTIFYEMAIL]">k2service@denallix.com</add>
<add key="[USEEXCHANGE]">True</add>
<add key="[EXCHANGEEMAIL]">K2Service@denallix.com</add>
<add key="[EXCHANGEONLINE]">False</add>
<add key="">
[SMTPCONNECTIONSTRING]">URL=https://dlx.denallix.com/EWS/Exchange.asmx;User
ID=K2Service@denallix.com;Password=K2pass!;Authentication=Windows</add>
<add key="">
[SMTPCONNECTIONSTRINGANONYMOUS]">URL=https://dlx.denallix.com/EWS/Exchange.asmx
;User ID=K2Service@denallix.com;Password=K2pass!;Authentication=Anonymous</add>
<add key="">
[EXCHANGECONNECTIONSTRING]">Autodiscover=True;URL=https://dlx.denallix.com/EWS/
Exchange.asmx</add>
<add key="[USESMTPOPTIONS]">False</add>
<add key="[EXCH_ADMINISTRATION]">true</add>
<add key="[EXCHANGEADMINUSER]">DENALLIX\k2service</add>
<add key="[EXCH_MANAGEMENT]">true</add>
<add key="[EXCHANGESTANDARDUSER]">DENALLIX\k2service</add>
<add key="[EXCHANGEDEFAULTSERVER]">DLX.denallix.com</add>
<add key="[EXCHANGEAUTODISCOVERENABLE]">True</add>
<add key="[ExchangeVersion]">Exchange2010_SP1</add>
<add key="[SMTPUSER]">DENALLIX\k2service</add>
<add key="[SMTPUSERPASS]">1ZGFq4Yt3n2uHAqsw36jSA==</add>
<add key="[SERVICEACCOUNTK2FQN]">K2:DENALLIX\k2service</add>
<add key="[INCOMINGNOTIFYEMAIL]">k2service@denallix.com</add>
<add key="[SMARTACTIONSENABLED]">True</add>
</VARIABLES>
</PRODUCT>

```

1.6.6.7.2 Server Installation XML - Example

Unattended Installer - Server Installation XML File

The following XML code is an example of a Server Installation:



[Copy Example Workspace Installation XML File](#)

```
<?xml version="1.0" encoding="utf-8" ?>
<PRODUCT>
<COMPONENTS>
  <CORE/>
  <SERVER/>
  <CONFIGURATION/>
</COMPONENTS>
<VARIABLES>
<add key="[SOURCECODECOMMONAPPDATA]">C:\ProgramData\SourceCode\</add>
<add key="[SETSPN]">False</add>
<add key="[INSTALLDIR]">c:\Program Files (x86)\K2 blackpearl\</add>
<add key="[K2SITEURL]">http://workspace</add>
<add key="[LBSITENAME]">http://workspace</add>
<add key="[VS8DIR]">c:\program files (x86)\microsoft visual studio 8\common7\IDE\</add>
<add key="[SETSPN]">False</add>
<add key="[VS10DIR]">c:\program files (x86)\microsoft visual studio 10.0\common7\IDE\</add>
<add key="[VS11DIR]">c:\program files (x86)\microsoft visual studio 11.0\common7\IDE\</add>
<add key="[INSTALLUSER]">INSTALL\peter</add>
<add key="[WORKSPACEADISTRIBUTED]">false</add>
<add key="[MACHINEKEY]">xxxxxxxxxxxxxxxx</add>
<add key="[SIMPLEINSTALL]">false</add>
<add key="[USRMGRTYPE]">UMTYPE_ADUM</add>
<add key="[LICENSEUSER]" />
<add key="[LICENSETYPE]">SOFTWARE</add>
<add key="[LICENSEDPRODUCT]">K2BLACKPEARL</add>
<add key="[LICENSEDATA]" />
<add key="[LICENSEPASS]">xxxxxxxxxxxxxxxx</add>
<add key="[LICENSEKEY]">xxxxxxxxxxxxxxxx</add>
<add key="[LBHOSTSERVERNAME]">SA-DC-PETER</add>
<add key="[ISNLB]">false</add>
<add key="[PTA_OPTION]">ClientWindows</add>
<add key="[HOSTSERVICENAME]">EventSystem</add>
<add key="[HOSTSERVERNAME]">SA-DC-PETER</add>
<add key="[HOSTSERVERPORT]">5555</add>
<add key="[WORKFLOWSERVERPORT]">5252</add>
<add key="[LBDISCOVERYPORT]">49599</add>
<add key="[SA-DC-PETER]"><Vars><Var Name=""[PREVK2SITENAME]"" Value="" /></Vars></add>
<add key="[K2SITENAME]">K2</add>
<add key="[K2APPPPOOL]">K2 blackpearl</add>
<add key="[XML_SHAREPOOL]"><variables><farm value="&quot;c85760fc-76e6-4b95-a3ea-d7f6be3668cd&quot;">
<XML_SHAREPOOL>K2 for SharePoint</XML_SHAREPOOL></farm></variables></add>
<add key="[CRMVERSION]" />
<add key="[CRMURL]" />
<add key="[CRMORGANIZATION]" />
<add key="[HOSTSERVERDBNAME]">K2</add>
<add key="[HOSTSERVERCONNECTIONSTRING]">Data Source=SA-DC-PETER\installtest;Initial Catalog=K2;integrated security=sspi;Pooling=True</add>
<add key="[HOSTSERVERDBSQLSERVER]">SA-DC-PETER\installtest</add>
<add key="[K2SQLUMDBSQLSERVERPARSED]">SA-DC-PETER\installtest</add>
<add key="
[K2HOSTCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=SA-DC-PETER;Port=5555</add>
<add key="
[K2WFCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=SA-DC-PETER;Port=5252</add>
<add key="[WORKSPUSER]">INSTALL\administrator</add>
<add key="[WORKSPASS]">1ZGFq4Yt3nHAqsw36jSA==</add>
<add key="[ADMINUSER]">INSTALL\administrator</add>
<add key="[ADMINPASS]">1ZGFq4Yt3n2qsw36jSA==</add>
<add key="[USERSNAME]">INSTALL\administrator</add>
<add key="[USERSPASS]">1ZGFq4YtHAqsw36jSA==</add>
<add key="[FULLUSERSNAME]">INSTALL\administrator</add>
<add key="[EWSURL]">https://dbxpr05.outlook.com/EWS/Exchange.asmx</add>
<add key="[USEAUTODISCOVER]">True</add>
<add key="[SMTP]">smtp.outlook.office365.com:587</add>
<add key="[NOTIFYEMAIL]">k2service@k2jhb.onmicrosoft.com</add>
<add key="[USEEXCHANGE]">True</add>
<add key="[EXCHANGEEMAIL]">k2service@k2jhb.onmicrosoft.com</add>
<add key="[EXCHANGEONLINE]">True</add>
<add key="[SMTPCONNECTIONSTRING]">Port=587;TLS=BootTls;Host Name=outlook-namwest.office365.com;Authentication=Anonymous</add>
<add key="[SMTPCONNECTIONSTRINGANONYMOUS]">Port=587;TLS=BootTls;Host Name=outlook-namwest.office365.com;Authentication=Anonymous</add>
<add key="[EXCHANGECONNECTIONSTRING]">SMTPCONNECTIONSTRING</add>
<add key="[USESMTMP]">False</add>
```

```
<add key="[EXCH_ADMINISTRATION]">true</add>
<add key="[EXCHANGEADMINUSER]">k2service@k2jhb.onmicrosoft.com</add>
<add key="[EXCH_MANAGEMENT]">true</add>
<add key="[EXCHANGESTANDARDUSER]">k2service@k2jhb.onmicrosoft.com</add>
<add key="[EXCHANGEDEFAULTSERVER]">dbxpr05.outlook.com</add>
<add key="[EXCHANGEAUTODISCOVERENABLE]">True</add>
<add key="[ExchangeVersion]">Exchange2013</add>
<add key="[SMTPUSER]">peter</add>
<add key="[SMTPUSERPASS]"/>
<add key="[SERVICEACCOUNTK2FQN]">SA-DC-PETER</add>
<add key="[INCOMINGNOTIFYEMAIL]">NOTIFYEMAIL</add>
<add key="[SMARTACTIONSENABLED]">false</add>
<add key="[INCOMING_EXCH_SVR]">outlook-namwest.office365.com</add>
<add key="[INCOMING_EXCH_PORT]">587</add>
<add key="[INCOMING_EXCH_TLS]">false</add>
</VARIABLES>
</PRODUCT>
```

1.6.6.7.3 Client Installation XML - Example

Unattended Installer - Client Installation XML File

The following XML code is an example of a Client Installation:

```

 Copy Visual Studio Installation

<?xml version="1.0" encoding="utf-8" ?>
<PRODUCT>
  <COMPONENTS>
    <CORE/>
    <STUDIO/>
    <VS2010/>
    <VS2012/>
    <K2STUDIO/>
    <CONFIGURATION/>
  </COMPONENTS>
</PRODUCT>
<VARIABLES>
<add key="[SOURCECODECOMMONAPPPDATA]">C:\ProgramData\SourceCode\</add>
<add key="[SETSPN]">False</add>
<add key="[INSTALLDIR]">C:\Program Files (x86)\K2 blackpearl\</add>
<add key="[K2SITEURL]" />
<add key="[LBSITENAME]" />
<add key="[VS8DIR]">c:\program files (x86)\microsoft visual studio 8\common7\IDE\</add>
<add key="[SETSPN]">False</add>
<add key="[VS10DIR]">c:\program files (x86)\microsoft visual studio 10.0\common7\IDE\</add>
<add key="[VS11DIR]">c:\program files (x86)\microsoft visual studio 11.0\common7\IDE\</add>
<add key="[INSTALLUSER]">INSTALL\peter</add>
<add key="[WORKSPACEIDISTRIBUTED]">false</add>
<add key="[MACHINEKEY]" />
<add key="[SIMPLEINSTALL]">false</add>
<add key="[USRMGRTYPE]">UMTYPE_ADUM</add>
<add key="[HOSTSERVERNAME]">SA-DC-PETER</add>
<add key="[HOSTSERVERPORT]">5555</add>
<add key="[WORKFLOWSERVERPORT]">5252</add>
<add key="[LBDISCOVERYPORT]">49599</add>
<add key="[LBHOSTSERVERNAME]">SA-DC-PETER</add>
<add key="

[K2HOSTCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=SA-DC-PETER;Port=5555</add>
<add key="

[K2WFCONNECTIONSTRING]">Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=SA-DC-PETER;Port=5252</add>
</VARIABLES>
</PRODUCT>

```

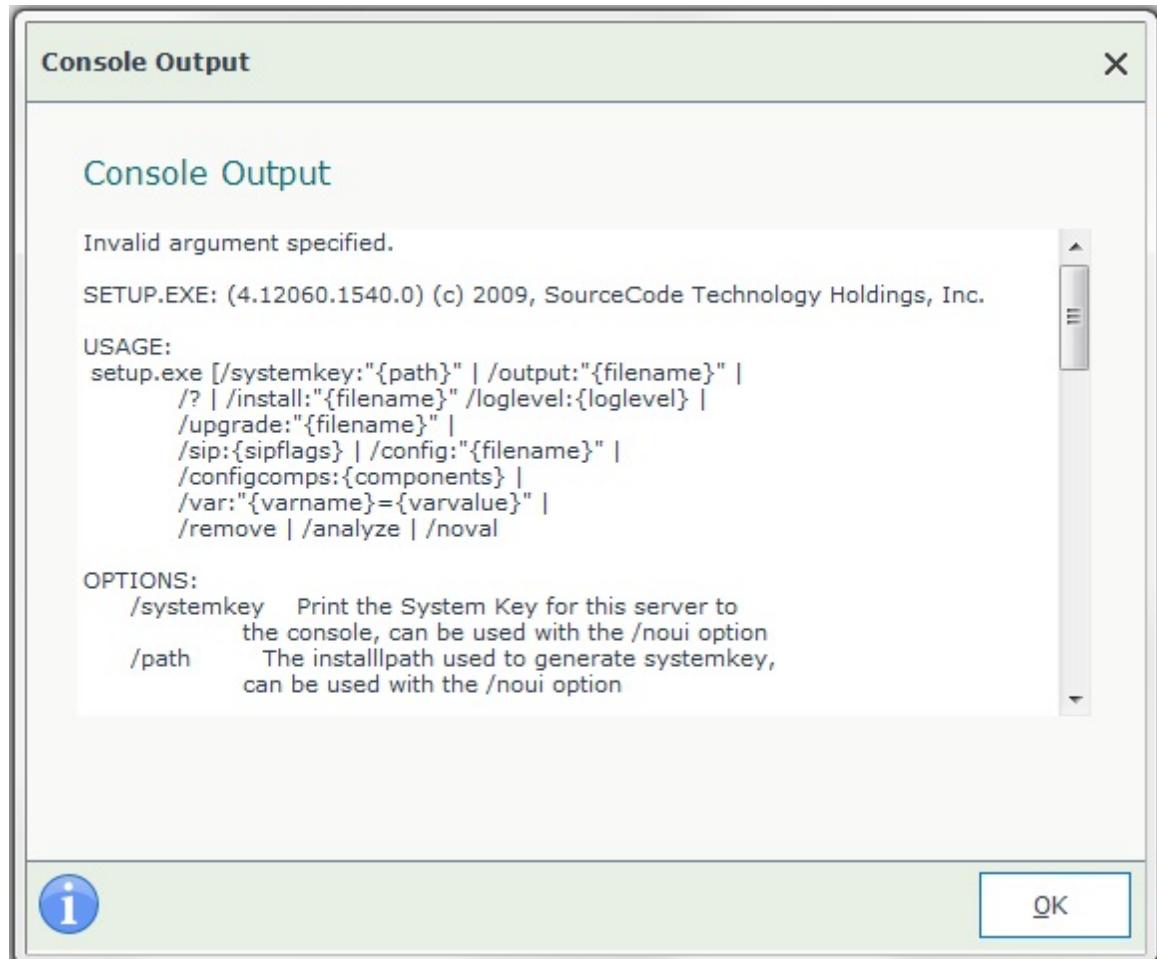
1.6.6.8 Setup Options

Get a list of Setup.exe Options

Run **setup.exe /?** to determine all command line options

Output:

Print the following text to the Console Output:



Usage	
setup.exe	[/systemkey:"{path}" /output:"{filename}" /? /install:"{filename}" /loglevel:{loglevel} /upgrade:"{filename}" /config:"{filename}" /configcomps:{components} /var:"{varname}={varvalue}" /remove /analyze /noui /noval]

Options	
/systemkey	Print the System Key for this server to the console.
/output	Generate an XML Configuration File after gathering info.
/install	Run the silent installer with the specified XML file.
/loglevel	Specify the Log Level to be used (Optional).
/upgrade	Run the silent installer with the specified XML file.
/config	Configure an existing installation.
/configcomps	Configure specified components.
/var	Override a configuration variable during installation.

/remove	Remove an existing installation.
/analyze	Analyze an existing installation to see if it is valid.
/noui	Hides the user interface (Console Output screen).
/noval	Strips validation from the Next button on 3 installer panels: CRM, Exchange & SmartActions. This means that no validation will take place when the Next button is clicked.  Note that the Test button on those panels will still perform validation. This action is also logged for troubleshooting purposes.

Parameters	
path	The path to the folder where K2 will be installed.
filename	The filename (and path) to the XML file that will contain the installation configuration.
components	Comma separated list of components to configure.  This is not silent but will bring up the configuration wizard for the selected components. Setup.exe /configcomps:SERVER Possible component names to use for the /configcomps command: SERVER - K2 blackpearl Server WORKSPACE - K2 Workspace config MOSS - K2 for SharePoint config WEBDESIGNER - K2 Designer for SharePoint STUDIO - K2 for Visual Studio config K2STUDIO - K2 Studio
loglevel	The log level to be used for the installation log. 1 – Verbose Logging 2 – Information, Warning and Errors 3 – Warning and Errors Only (Default) 4 – Errors Only
varname	Configuration variable name to override during installation.
varvalue	Value to set the specified configuration variable to during installation.

Examples	
setup.exe /?	Will open this Console Output screen.
setup.exe /output:MyConfig.xml	Launch the Setup wizard and output the settings to 'MyConfig.xml' file.
setup.exe /systemkey:"C:\Program Files\K2 blackpearl"	Output the System Key to the Console.

1.6.6.9 Additional Notes

Unattended Installer - Additional Notes

All command line parameters are case insensitive. For example, both of these will work identically:

- setup.exe /SystemKey
- setup.exe /systemkey

All command line parameters can use either "/" or "-" to indicate a switch. For example, both of these will work identically:

- setup.exe /systemkey /path:{installpath}
- setup.exe -systemkey -path:{installpath}

If the names of files contain spaces, then the user must enclose them in quotes. For example: setup.exe /output:"**My Output File.xml**"

If the user does not specify a path (but rather just the filename), it is assumed that the file will be created in the same directory as 'setup.exe' - this applies to all parameters that accept a filename. Alternatively, any 'filename' parameter will also function if the user has specified a path.

- **Example:** setup.exe /output:"C:\My Configs\My File.xml" 1



The Setup Manager will verify that the path is valid and immediately raise an error (to the console) if it is incorrect.

K2 Pass Through Authentication



K2 Pass-Through Authentication is only available for K2 Server when installed in a distributed configuration

K2 Pass-Through Authentication can be configured using the unattended installer however, the default behavior of the unattended installer differs from the normal installer. By default the XML file will generate with the K2 Pass-Through Panel set to Kerberos, but this setting differs from the Installer which is set to Windows. This setting has been enabled as a precaution to ensure that for existing environments where Kerberos has been configured, these environments are not affected negatively by the introduction of K2 Pass-Through Authentication.

To correct this, the XML file must be regenerated with the following :

- Alter the K2 Pass-Through Authentication Option to : Windows
- Change the XML file Path to "Setup.exe" /output:MyFile.xml

1.6.7 K2 documentation

K2 Documentation



Ensure that any antivirus software is disabled for the duration of the K2 documentation installation. Active anti-virus software may prohibit the successful installation of the product documentation.

The K2 blackpearl documentation is split into three parts:

1. The Getting Started Guide (this guide) which is installed as part of the installer package
2. The K2 blackpearl User Guide
3. The K2 blackpearl Developers Reference

The K2 blackpearl User Guide and Developers Reference are available as separate installation packages.

1.6.8 Integration Configuration

1.6.8.1 SharePoint

1.6.8.1.1 K2 for SharePoint Configuration Wizard

K2 for SharePoint Configuration

The K2 for SharePoint Configuration Wizard runs from within **SharePoint > Central Administration** and will enable the user to do the following:

1. Install and deploy the K2 for SharePoint components automatically after the K2 Setup Manager is complete
2. Manage the K2 for SharePoint solutions that are installed
3. Activate the K2 Features

The Wizard will run automatically once the K2 Setup Manager has completed if the check box is selected on the Finish screen. A shortcut, linking the user to the K2 for SharePoint Configuration wizard will be saved to the desktop of the machine where the installation was performed.



Ensure that the SharePoint Application Pool Service is running before attempting to run this wizard.

The K2 for SharePoint Configuration Wizard landing page will prompt the user to select the method of configuration. For first time use or an upgrade, only the installation and deployment wizard is available. The management portion of the wizard is available after the initial usage of the wizard.

K2 for SharePoint Configuration

Certain options may not be available until such time as additional steps have been completed.

K2 for SharePoint Configuration Wizard will display as shown below. Consider the on page instructions carefully as they describe the available options.

K2 for SharePoint Configuration Wizard - Windows Internet Explorer

http://dlx:44544/_admin/k2/configwelcome.asp

Central Administration > K2 for SharePoint Configuration Wizard

Please select whether you wish to use the wizard to configure the K2 for SharePoint components.

Welcome

Welcome to the K2 for SharePoint Configuration Wizard. There are two options available for configuring the K2 integration:

- For a first time installation, the K2 for SharePoint Configuration Wizard is required to deploy and configure the K2 for SharePoint components.
- For an upgrade installation or after you have completed the wizard, you can use the SharePoint Solution Management page to upgrade and manage the K2 for SharePoint components.

For more information see the K2 documentation located at Start > All Programs > K2 blackpearl or K2 blackpoint > K2 Documentation. Search for the K2 for SharePoint Configuration Wizard.

K2 for SharePoint Configuration Wizard

Use the K2 for SharePoint Configuration Wizard to configure the K2 for SharePoint components

Use the Solutions Management page to manage existing K2 for SharePoint components (advanced)

Next ->

K2 For SharePoint Configuration

Use the K2 for SharePoint Configuration The K2 for SharePoint configuration wizard will

wizard to configure the K2 for SharePoint components	step the user through the required steps to configure the K2 for SharePoint solutions
Use the Solutions management page to manage existing K2 for SharePoint components (advanced)	This option enables the user to manage the K2 for SharePoint Solutions package that is installed and deployed by the K2 for SharePoint Wizard. This option is not available immediately and does require existing solutions to be upgraded or for the K2 for SharePoint components to be installed.

What to do ?

If the K2 for SharePoint solutions have not been installed or require an upgrade do the following :

1. If the **Use the Solutions Management page to manage existing K2 for SharePoint components (Advanced)** option is disabled (grayed out), click **Next** to install the K2 for SharePoint components
2. Click **Next**

If the K2 for SharePoint solutions have been configured and the user needs to retract or redeploy a solution i.e. the K2 for SharePoint configuration wizard has been run, do the following:

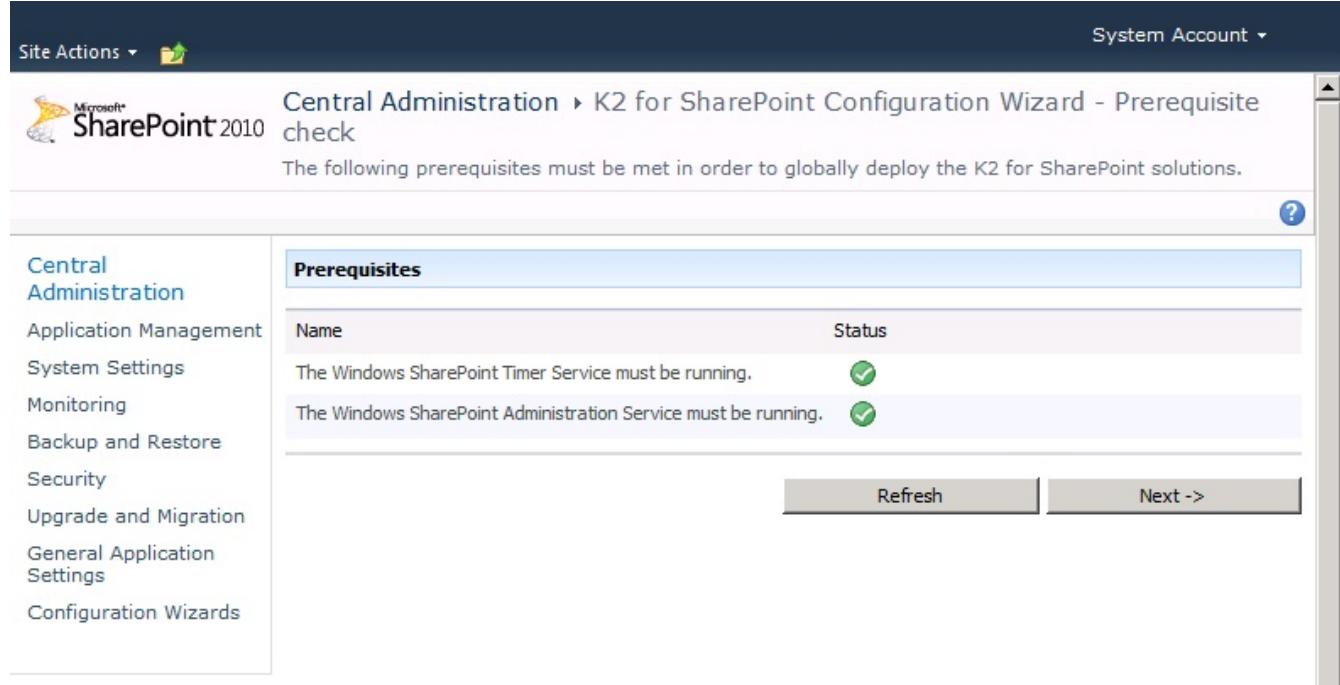
1. If the **Use the Solutions Management page to manage existing K2 for SharePoint components (Advanced)** option is disabled (grayed out), then refer to the steps above
2. Select the option to **Use the Solutions Management page to manage existing K2 for SharePoint components (Advanced)**
3. Click **Next**, for the K2 for SharePoint - Prerequisite Check (Advanced)

1.6.8.1.1.1 K2 for SharePoint Prerequisite Check

K2 for SharePoint Prerequisite Check

The prerequisite check will verify that the current installation meets the configuration requirements. Items that are not correct will have a red X in the status column and this will prevent the process from proceeding. The **Next** button will also remain disabled (grayed out) until such time as the status of the prerequisites has changed. When a change has been made, click the Refresh button to refresh the page. The prerequisites check that the required services are available and running.

 **Distributed Installation:** When installing a distributed installation and deploying solutions to WFEs, ensure that the services listed below are running on the remote machines. This check must be done manually for the WFEs.



The following prerequisites must be met in order to globally deploy the K2 for SharePoint solutions.

Prerequisites	
Name	Status
The Windows SharePoint Timer Service must be running.	✓
The Windows SharePoint Administration Service must be running.	✓

Refresh
Next ->

K2 for SharePoint Configuration - Prerequisites check

Prerequisites	There are two services which must be available for the installation to continue. If either of the two services listed above are not running rectify this problem and then the process can proceed.
----------------------	--

What to do?



1 Refresh the page if required and this would only be required if a prerequisite has not been met

2 Click **Next**

1.6.8.1.1.2 K2 for SharePoint Configuration Wizard - Installation

K2 for SharePoint - Solution Installation

The Solution Installation page provides a list of solutions that will be installed automatically. This list is the entire K2 for SharePoint components package and there may be inter-dependencies so no individual selection is permitted.

Solutions

Name	Status	Next Action	Details
K2 for SharePoint - Core Components.wsp	Not Installed	Install	
K2 for SharePoint - Management Console.wsp	Not Installed	Install	
K2 for SharePoint - Process Portals.wsp	Not Installed	Install	
K2 for SharePoint - Workflow Core.wsp	Not Installed	Install	
K2WorklistWebPart.wsp	Not Installed	Install	
K2 Reporting Web Parts.wsp	Not Installed	Install	
K2 for SharePoint - Web Designer.wsp	Not Installed	Install	

Next Step

The solutions that do not exist in the solution store will be added to it.

Refresh **Next ->**

Solution Installation	
Name	The name of the solution
Status	The solutions current status
Next Action	The next action which will be to install the solution
Details	Details if available will be displayed here

What to do?

There is nothing for the user to do, except click Next to proceed.



Click **Next**

1.6.8.1.1.3 K2 for SharePoint Configuration Wizard - Solution Deployment

K2 for SharePoint - Solution Deployment

Once the solutions have been installed, the next step is to deploy them. As shown in the screen shot below the status of the solution indicates that deployment is required. The next step is to schedule the deployment by clicking **Next** for the following user page.



The SharePoint page may at times appear to be unresponsive, seemed to have timed out or a "503 : Service Unavailable" error may display. Manually refresh the page when this takes place.

This step spans across more than one user page, and this topic discusses the pages that apply directly to each other for ease of use. Once the Solutions have been installed, the deployment schedule can be created.

► Solutions Not Deployed

Solutions			
Name	Status	Next Action	Details
K2 for SharePoint - Core Components.wsp	Not Deployed	Schedule deployment immediately	
K2 for SharePoint - Management Console.wsp	Not Deployed	Schedule deployment in 1 minutes	
K2 for SharePoint - Process Portals.wsp	Not Deployed	Schedule deployment in 2 minutes	
K2 for SharePoint - Workflow Core.wsp	Not Deployed	Schedule deployment in 3 minutes	
K2WorklistWebPart.wsp	Not Deployed	Schedule deployment in 4 minutes	
K2 Reporting Web Parts.wsp	Not Deployed	Schedule deployment in 5 minutes	
K2 for SharePoint - Web Designer.wsp	Not Deployed	Schedule deployment in 6 minutes	

Next Step

The solutions that have not been deployed will be scheduled to deploy in a staggered sequence.

Refresh **Next ->**

The deployment schedule lists each item and the time at which the deployment may take place.

When or if there are errors, the SharePoint page will provide the user with tooling to retry the deployment process and repair the error

► Error Repair

Shown below, the solution deployment failed and the status has been set to **Error**. Details are provided and the user can attempt a **Retry**.

K2 for SharePoint Configuration - Solution Deployment - Windows Internet Explorer

http://demo:14877/_admin/K2/ConfigDeployment.aspx

Central Administration

Central Administration

Home Operations Application Management K2 for SharePoint Site Actions

K2 for SharePoint Configuration - Solution Deployment

Solutions

Name	Status	Details	Action
K2 for SharePoint - Core Components.wsp	Deployed		
K2 for SharePoint - Management Console.wsp	Deployed		
K2 for SharePoint - Process Portals.wsp	Deployed		
K2 for SharePoint - Workflow Core.wsp	Error	Some of the files failed to copy during deployment of the solution.	Retry
K2WorklistWebPart.wsp	Deployed		
K2 for SharePoint - Web Designer.wsp	Deployed		

Comments

If the timer job for any Web Front End server takes more than a couple of minutes to complete, please check the following for each of those Web Front End servers:

- The server is available on the network and can be connected to from this server.
- Windows SharePoint Timer Service is running
 - If the service is not running, please start it.
 - If the service is running, restart it.
- Windows SharePoint Administration Service is running
 - If the service is not running, please start it.
 - If the service is running, restart it.
- Use the stsadm command to force the deployment. Use as following:
 - stsadm -o execadmsvcjobs

Refresh Finish

What to do?

To deploy the solutions do the following



Click Next, to proceed to the deployment scheduling

▶ Click Next

Site Actions System Account

Microsoft SharePoint 2010 Central Administration > K2 for SharePoint Configuration Wizard - Solution Installation

The following solutions will be installed as part of the configuration.

Solutions

Name	Status	Next Action	Details
K2 for SharePoint - Core Components.wsp	Not Deployed	Schedule deployment immediately	
K2 for SharePoint - Management Console.wsp	Not Deployed	Schedule deployment in 1 minutes	
K2 for SharePoint - Process Portals.wsp	Not Deployed	Schedule deployment in 2 minutes	
K2 for SharePoint - Workflow Core.wsp	Not Deployed	Schedule deployment in 3 minutes	
K2WorklistWebPart.wsp	Not Deployed	Schedule deployment in 4 minutes	
K2 Reporting Web Parts.wsp	Not Deployed	Schedule deployment in 5 minutes	
K2 for SharePoint - Web Designer.wsp	Not Deployed	Schedule deployment in 6 minutes	

Next Step

The solutions that have not been deployed will be scheduled to deploy in a staggered sequence.

Refresh Next ->



Select an item to set a specific time for when the solution will be deployed. If left as is, the deployment will take place immediately a minute between each deployment.



When deployed, the solutions Status will display as Deployed, click Next to proceed to the Post Deployment Configuration page.

▶ Click Next

Site Actions  System Account ▾

 SharePoint 2010 Central Administration ▶ K2 for SharePoint Configuration Wizard - Solution Deployment

?

Solutions			
Name	Status	Details	Action
K2 for SharePoint - Core Components.wsp	Deployed		
K2 for SharePoint - Management Console.wsp	Deployed		
K2 for SharePoint - Process Portals.wsp	Deployed		
K2 for SharePoint - Workflow Core.wsp	Deployed		
K2WorklistWebPart.wsp	Deployed		
K2 Reporting Web Parts.wsp	Deployed		
K2 for SharePoint - Web Designer.wsp	Deployed		

Next Step

Continue to the Post Deployment Configuration Page.

Refresh Next ->

1.6.8.1.1.4 K2 for SharePoint Configuration Wizard - Solutions Deployed

K2 for SharePoint - Solutions Deployed

As shown below, if all the solutions have been installed successfully, the status will be changed to **Deployed**. Once this is complete, the final step is for the User to activate the SharePoint Features and deploy them to the Web Front ends. Within K2 there is a K2 Workflow Failover SharePoint Job definition. It is essentially a timer job that runs every minute and checks a queue for Workflow modifications that need to be run against the K2 SharePoint Workflow. Every time a K2 workflow is modified (i.e. task created, workflow completed) a check is performed to ensure the workflow is ready to accept the modification. If the workflow is not ready to be modified it will be queued for later execution by the Job Definition.



If the Job Definition is not registered the following issues can be experienced:

- When there is high volume certain tasks will not appear in Worklist.
- Under high volume certain tasks will not complete.

It is therefore recommended that the Job Definition is registered on all installations

Site Actions ▾

Microsoft SharePoint 2010 Central Administration > K2 for SharePoint Configuration Wizard - Post Deployment Configuration

Central Administration

Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Configuration Wizards
K2 for SharePoint

Job Definitions

Name	Status	Details	Action
K2 Workflow Failover	Registered		

Comments

Job definitions:

- To register job definitions individually, click the "Register" link for the corresponding job definition.

Next Step

Navigate to 'Activate All K2 Features and K2 Configuration Settings' page in order to activate the K2 features to the first site collection.
 Navigate to 'K2 for SharePoint' page in Central Administration.

Job Definitions

Name	Description
Status	Status of the solutions
Details	Details related to the solution
Actions	Actions that can be taken depending on the status of the solution

Next Step

Navigate to 'Activate All K2 Features and K2 Configuration Settings'...	Allows the user to activate the K2 for SharePoint features automatically. Selecting this option results in all the K2 Features being automatically activated.
Navigate to 'K2 for SharePoint' page in central Administration.	The K2 for SharePoint features can be activated manually in Central Administration. This allows a user to select which feature must be activated or not.

What to do?

- 1 Select one of the options listed under the heading **Next Step**.
- 2 Click **Finish**
- 3 If the first option is selected the Activate All K2 Features and K2 Configuration Settings page will open in Central Administration . Configure the various settings according to your environment setup.

▶ Click Finish

Activate All K2 Features and K2 Configuration Settings

Site Actions

System Account

Central Administration > Activate All K2 Features and K2 Configuration Settings

Activate K2 Features and deploy K2 Configuration Settings to a site collection.

Activation Location

Choose a site collection where you want to activate the K2 Features and K2 Configuration Settings.

Site Collection: <http://sa-docs-03:105>

General Settings

Displays general settings for the K2 for SharePoint components and specifies whether all the settings below will be updated to the associated sub sites.

Installed Product: K2 blackpearl
Version: 4.10320.10300.1
 Update settings for all sub webs

Feature Activation Settings

Specify whether all K2 Features will be activated to the selected site collection.

Activate all K2 Features to selected site collection

Connection Settings

Specify whether the K2 Connection Settings will be deployed to the selected site collection.

Add K2 Connection Settings to selected site collection

Host Server: SA-DOCS-03

OK Cancel

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Configuration Wizards
- K2 for SharePoint

1.6.8.1.1.5 K2 for SharePoint Configuration Wizard - Features Activation

K2 for SharePoint - Features Activation

This topic is also discussed in greater detail in the SharePoint Integration > [Activate All K2 Features and K2 Configuration Settings](#), help file.

 The features associated with the K2 for SharePoint installation must be activated per site collection.

Site Actions ▾ 

System Account ▾

 Microsoft® SharePoint® 2010 Central Administration ▶ K2 for SharePoint

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Configuration Wizards
- K2 for SharePoint**

-  **General**
[Run the K2 for SharePoint Configuration Wizard](#) |
[Activate All K2 Features and K2 Configuration Settings](#) |
[Management Console](#)
-  **Settings Management**
[K2 for SharePoint Configuration](#) |
[K2 Designer for SharePoint Configuration](#)
-  **Features Management**
[K2 Management Console](#) | [K2 Site Settings](#) |
[SmartObject Management](#) |
[K2 Designer for SharePoint](#) |
[K2 Workflow Integration Content Types](#) | [K2 Web Parts](#)
-  **Data Management**
[SQL Connections for SmartObjects](#) |
[CRM Server Connections for SmartObjects](#)

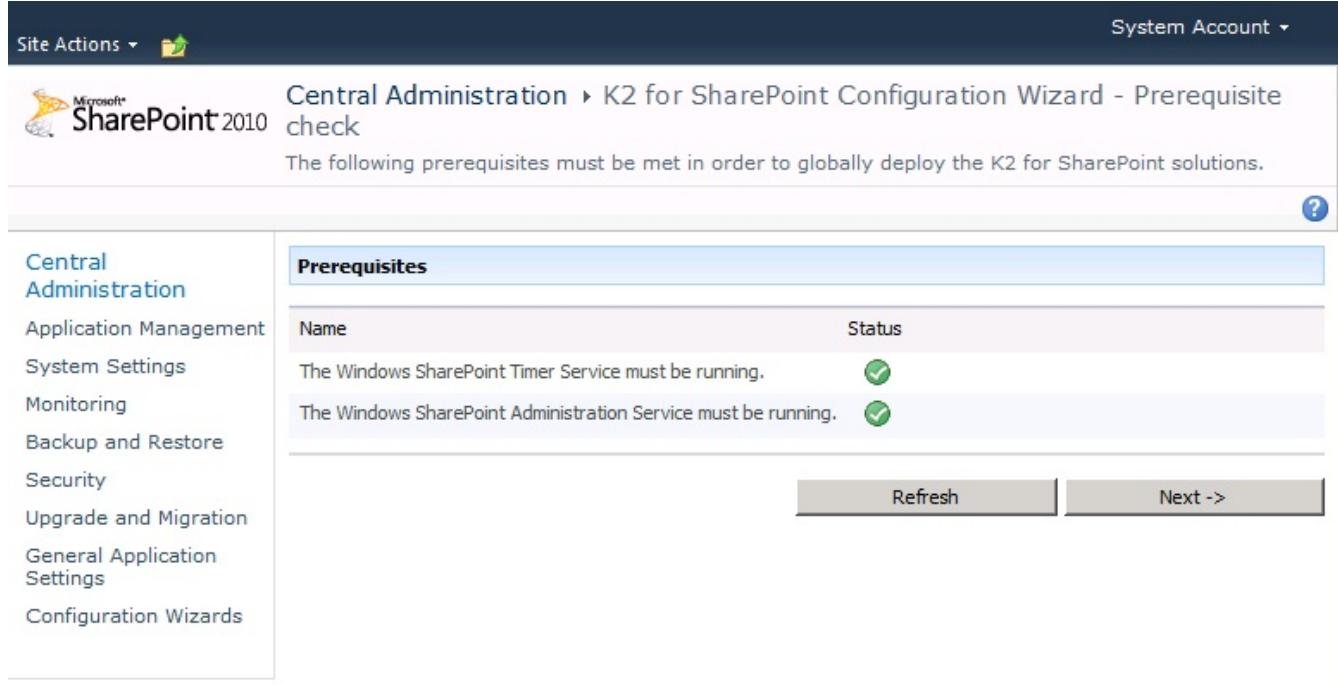
1.6.8.1.1.6 K2 for SharePoint Solutions Management (Advanced)

1.6.8.1.1.6.1 K2 for SharePoint - Prerequisite Check (Advanced)

K2 for SharePoint Prerequisite Check (Advanced)

The prerequisite check will verify that the current installation meets the configuration requirements. Items that are not correct will have a red **X** in the status column and this will prevent the configuration check from proceeding. The **Next** button will also remain disabled (grayed out) until such time as the status of the prerequisites has changed. When a change has been made, click the refresh button to refresh the page.

 **Distributed Installation:** When installing a distributed installation and deploying solutions to WFEs, ensure that the services listed below are running on the remote machines. This check must be done manually for the WFEs.



The following prerequisites must be met in order to globally deploy the K2 for SharePoint solutions.

Prerequisites	
Name	Status
The Windows SharePoint Timer Service must be running.	
The Windows SharePoint Administration Service must be running.	

[Refresh](#)
[Next ->](#)

K2 for SharePoint Configuration - Prerequisites check

The Windows SharePoint...	There may be more than one item containing this lead in wording, and the required number of services will be listed along with a status indication.
----------------------------------	---

What to do?

-  Refresh the page if required and this would only be required if a prerequisite has not been met
-  Click **Next**

1.6.8.1.1.6.2 K2 for SharePoint - Solution Deployment (Advanced)



The solutions have been installed and deployed automatically. This portion of the wizard only enables the user to manage the existing solutions.

K2 for SharePoint Solution Deployment (Advanced)

The Solutions Management Page lists all the K2 for SharePoint solutions that have been installed and then subsequently installed by the automated portion of the K2 for SharePoint Wizard. This portion of the wizard only enables the user to perform a solution retraction of an existing solution.

Name	Status	Deployed To
k2 for sharepoint - core components.wsp	Deployed	Globally deployed.
k2 for sharepoint - management console.wsp	Deployed	Globally deployed.
k2 for sharepoint - process portals.wsp	Deployed	http://sa-docs-03:777/...
k2 for sharepoint - web designer.wsp	Deployed	Globally deployed.
k2 for sharepoint - workflow core.wsp	Deployed	Globally deployed.
k2 reporting web parts.wsp	Deployed	http://sa-docs-03:777/...
k2worklistwebpart.wsp	Deployed	http://sa-docs-03:777/...

Solution Management	
Name	The name of the K2 for SharePoint Solutions
Status	The status, which after a successful automated deployment will be Deployed . If there had been any errors the status message would reflect the error.
Deployed to	The location where the solution was deployed which may be to a specific location or Globally deployed.

What to do?

To manage a solution, click the name of the solution.

1.6.8.1.1.6.3 K2 for SharePoint - Retract a solution (Advanced)

K2 for SharePoint - Retract a Solution (Advanced)

All the Solution Properties are displayed as displayed below, describing the solution and the particulars of where it was deployed, the location operational results and so on.

The screenshot shows the SharePoint 2010 Central Administration interface. The left navigation menu includes options like Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Configuration Wizards, and K2 for SharePoint. The main content area is titled 'Retract Solution' and shows the properties of a solution named 'k2 for sharepoint - core components.wsp'. The properties listed are:

Name:	k2 for sharepoint - core components.wsp
Type:	Core Solution
Contains Web Application Resource:	No
Contains Global Assembly:	Yes
Contains Code Access Security Policy:	No
Deployment Server Type:	Front-end Web server
Deployment Status:	Deployed
Deployed To:	Globally deployed.
Last Operation Result:	The solution was successfully deployed.
Last Operation Details:	SA-DOCS-03 : The solution was successfully deployed.
Last Operation Time:	11/2/2010 2:06 PM

What to do ?



Escape Action: To avoid retracting a solution click **Back to Solutions**



To retract the solution click **Retract Solution**



The next step enables the user to configure the **Retract Solution** properties

From the **Central Administration | Retract Solutions** page the user is required to configure the following items:

1. The time for retraction
2. The location where the solution has been deployed

Solution Information

Name: k2 for sharepoint - core components.wsp
Locale: 0
Deployed To: Globally deployed.
Deployment Status:

Retract When?

A timer job is created to retract this solution. Please specify the time at which you want this solution to be retracted.

Choose when to retract the solution:
 Now
 At a specified time:
 11/2/2010 4 PM 00

Retract From?

The solution contains no Web application scoped resource, and therefore cannot be retracted from a particular web application. It can only be retracted globally.

OK Cancel

Retract Solution Properties

Retract When?	The user can select the time to be either immediate, ie Now or at a specified time. Since the removal of a solution will require a recycling of the application pools the SharePoint Application Pool will be unavailable for a short time. To avoid any user interruption the option to retract At a specified time is recommended.
Retract from?	Select from the drop down to remove from a specific web portal or all front ends. Note: The location where the solution was deployed to would have been user configured during the automated deployment configuration step.

When ready, click **Ok**

The browser will navigate back to the solutions listing, where the information pertaining to the Solution Retract process will be displayed.

Name	Status	Deployed To
k2 for sharepoint - core components.wsp	Retracting(scheduled at 11/2/2010 3:13 PM)	Globally deployed.
k2 for sharepoint - management console.wsp	Deployed	Globally deployed.
k2 for sharepoint - process portals.wsp	Deployed	http://sa-docs-03:777/...
k2 for sharepoint - web designer.wsp	Deployed	Globally deployed.
k2 for sharepoint - workflow core.wsp	Deployed	Globally deployed.
k2 reporting web parts.wsp	Deployed	http://sa-docs-03:777/...
k2worklistwebpart.wsp	Deployed	http://sa-docs-03:777/...



During the Retraction process, the SharePoint Service may be unavailable momentarily. This is expected behavior, while the application pools are being cycled. To rectify this, refresh the browser until the SharePoint Central Administration page displays once more.

1.6.8.1.2 Central Administration

1.6.8.1.2.1 K2 Designer for SharePoint Administration Settings

K2 Designer for SharePoint - Administration Settings

All the K2 Designer for SharePoint features for SharePoint are activated manually and individually.

How to activate the K2 SharePoint Integration features in SharePoint Central Administration

1 Browse to the **SharePoint Central Administration > K2 for SharePoint tab > K2 Designer for SharePoint and K2 Workflow Integration Content Types** respectively.



Fig. 1. K2 for SharePoint tab > Features Management

2 The **Activate Feature** page will be displayed. Activate the **K2 Designer for SharePoint** and the **K2 Workflow Integration Content Types** feature.



Fig. 2. K2 Workflow Integration Content Types

How to activate the K2 Designer for SharePoint features in a SharePoint Site Collection

1 Open the SharePoint Site Collection

Click on **Site Actions > Site Settings**

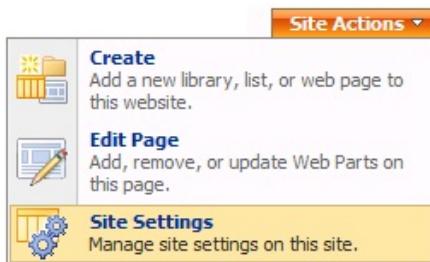


Fig. 1. Site Actions Menu

Click on **Modify All Site Settings**.

The following **Site Settings** page will be displayed:

The screenshot shows the 'Site Settings' page with the 'Site Administration' tab selected. The page lists various site settings under categories like 'Users and Permissions', 'Look and Feel', 'Galleries', and 'Site Administration'. The 'Site Administration' section is expanded, showing options such as 'Regional settings', 'Site libraries and lists', 'User alerts', 'RSS', 'Search visibility', 'Sites and workspaces', 'Delete this site', 'Related Links scope settings', 'Site output cache', 'Content and structure', and 'Content and structure logs'. The 'Site Collection Administration' section is also visible on the right.

Fig. 2. Site Settings

Click on **Site features** under the **Site Administration** menu.

The screenshot shows the 'Site Administration' menu with several options listed: 'Regional settings', 'Site libraries and lists', 'Site usage reports', 'User alerts', 'RSS', 'Search visibility', 'Sites and workspaces', 'Site features' (which is circled in red), 'Delete this site', 'Related Links scope settings', and 'K2 Events Integration'.

Fig. 3. Site Administration Menu

The **Site Features** page will be displayed. Activate the **K2 Designer for SharePoint Menu Item** feature.

The screenshot shows the 'Site Features' page with one item listed: 'K2 Process Designer Menu Item'. The item description is 'Adds the K2 Process Designer link to lists and libraries on a SharePoint site, allowing users with Contribute permissions to design and deploy K2 processes in SharePoint.' There is an 'Activate' button next to the item.

Fig. 4. Site Features

Click on **Site collection features** under the **Site Collection Administration** menu.

Site Collection Administration

- Search settings
- Search scopes
- Search keywords
- Recycle bin
- Site directory settings
- Site collection usage reports
- **Site collection features**
- Site hierarchy
- Portal site connection
- Site collection audit settings
- Audit log reports
- Site collection policies
- K2 Workflow Integration

Fig. 5. Site Collection Administration Menu

The **Site Collection Features** page will display, activate the **K2 Designer for SharePoint Task Content Type** feature.

Site Collection Features

Name	Status
K2 Process Designer Task Content Type Adds Content Types to a SharePoint Site that enable K2 Workflow Integration Process Designer processes to display forms.	<input type="button" value="Activate"/>

Fig. 6. Site Collection Features

1.6.8.1.2.2 Activate All K2 Features and K2 Configuration Settings

K2 for SharePoint - Activate All K2 Features and K2 Configuration Settings



Note: see the new SharePoint Timer Activation Feature topic before completing these steps.

K2 Features and K2 Configuration Settings are automatically activated and configured on the SharePoint site as provided in the K2 installer.

The K2 Features and K2 Configuration Settings can however be activated and configured manually as well. Specific rights are required for the user running the **Activate All K2 Features and K2 Configuration** page. The required rights are:

- User must be a Farm Administrator
- User must be a Site Collection Administrator
- User must be assigned K2 Administrator rights
- User must be assigned K2 Database rights as a DBOwner

To activate K2 Features and configure K2 Configuration Settings manually, select the **K2 for SharePoint** tab in SharePoint 3.0 Central Administration, and click on the **Activate All K2 Features and K2 Configuration Settings** link.

Fig. 1. K2 for SharePoint tab > General



When a MOSS or SharePoint 2010 site is extended it is necessary to "Activate All K2 Features and K2 Configuration Settings" on the main site in Central Administration>K2 for SharePoint to ensure that the K2 Features are applied to the extended sites.

Activate All K2 Features and K2 Configuration Settings

The following screen is displayed where all K2 Features activation and Configuration Settings can be performed at once.



The K2 for SharePoint Administration wizard will direct the user to this page once it has installed and deployed the solutions. This page must be used to configure the K2 for SharePoint features for each site collection manually one at a time.

Activate All K2 Features and K2 Configuration Settings - Windows Internet Explorer

http://demo:14877/_admin/K2/ActivateComponents.aspx

Activate All K2 Features and K2 Configuration Settings

Central Administration

Home Operations Application Management K2 for SharePoint

Central Administration > K2 for SharePoint > Activate All K2 Features and K2 Configuration Settings

Activate All K2 Features and K2 Configuration Settings

Activate K2 Features and deploy K2 Configuration Settings to a site collection.

Activation Location
Choose a site collection where you want to activate the K2 Features and K2 Configuration Settings.

General Settings
Displays general settings for the K2 for SharePoint components and specifies whether all the settings below will be updated to the associated sub sites.

Feature Activation Settings
Specify whether all K2 Features will be activated to the selected site collection.

Connection Settings
Specify whether the K2 Connection Settings will be deployed to the selected site collection.

Environment Library Settings
Specify whether a SharePoint Server field will be created in the K2 Environment Library for the selected site collection.

SharePoint Group Provider Settings
Specify whether a SharePoint group provider is created for the site collection. This allows users within SharePoint groups to be used for rights management on the K2 server and K2 processes, as well as for assigning user tasks.

Deployment Application Pool
Choose the application pool to use when deploying processes. The associated security account will be used when deploying processes. This account must be a member of the SharePoint Farm Administrators group (Central Administration > Operations > Update farm administrators group). You can choose an existing application pool or create a new one.

Process Designers
Specify the groups that can design and deploy processes to the server. These groups receive deploy rights on the server.

Process Participants
Specify the groups that, at time of process deployment, will be able to start processes and view information about processes they participate in. These groups receive Start and View Participate rights in the K2 server. To modify these rights, use Management Console or the Process Rights link in a process portal.

Site Collection Groups

Approvers
 Collaboration Portal Members
 Collaboration Portal Owners
 Collaboration Portal Visitors

Site Collection Groups

Approvers
 Collaboration Portal Members
 Collaboration Portal Owners
 Collaboration Portal Visitors

OK Cancel

Done

Local intranet | Protected Mode: Off

Activate All K2 Features and K2 Configuration Settings

Activate K2 Features and deploy K2 Configuration Settings to a site collection.



		OK	Cancel
Activation Location Choose a site collection where you want to activate the K2 Features and K2 Configuration Settings.		Site Collection: <input type="text" value="http://demo:112"/>	
General Settings Displays general settings for the K2 for SharePoint components and specifies whether all the settings below will be updated to the associated sub sites.		Installed Product K2 blackpearl Version 4.10020.1.0 <input type="checkbox"/> Update settings for all sub webs	
Feature Activation Settings Specify whether all K2 Features will be activated to the selected site collection.		<input checked="" type="checkbox"/> Activate all K2 Features to selected site collection	
Connection Settings Specify whether the K2 Connection Settings will be deployed to the selected site collection.		<input checked="" type="checkbox"/> Add K2 Connection Settings to selected site collection Host Server <input type="text" value="DEMO"/> Host Server Port <input type="text" value="5555"/> Runtime Services URL <input type="text" value="http://DEMO:81"/>	

Fig. 2. Activate and Configure K2 Features and Configuration Settings

Register SharePoint Group Provider

A SharePoint Group Provider is automatically registered by the K2 installer on the site provided as per the installer. If another SharePoint Group Provider is to be registered to another site collection, this can be done by creating another process portal site and registering the Group Provider manually on the new site collection. **SharePoint Groups** can then be added to this site and used as destination users for example.

Environment Library Settings Specify whether a SharePoint Server field will be created in the K2 Environment Library for the selected site collection.	<input checked="" type="checkbox"/> Add Settings SharePoint Server Field Name <input type="text" value="Collaboration Portal"/> <input type="checkbox"/> Set as default
SharePoint Group Provider Settings Specify whether a SharePoint group provider is created for the site collection. This allows users within SharePoint groups to be used for rights management on the K2 server and K2 processes, as well as for assigning user tasks.	<input checked="" type="checkbox"/> Add group provider for site collection SharePoint Group Provider Label <input type="text" value="SPSGroupProvider"/> K2 label <input type="text" value="K2"/>

Fig. 3. SharePoint Group Provider Settings

Process Designers and Process Participants

The group permissions must be allocated according to the tasks assigned roles of the users as process designers or process participants. Enabling the site collection groups allows the members the rights to design and deploy processes to the server for the Process Designer section. Process Participants for the members of the enabled site collection groups will be assigned process start rights as well as view participate rights for the processes they participate in.

1.6.8.1.2.2.1 SharePoint Timer Activation Feature

SharePoint Timer Activation Feature when activating K2 Features and Configuration Settings

The SharePoint Timer Activation feature is for customers with sub sites per site collection, with counts in excess of 2500.

Activation Location: Choose a site collection where you want to activate the K2 Features and K2 Configuration Settings. Site Collection: <http://dx:10899/sites/K2GenSite0>

General Settings: Displays general settings for the K2 for SharePoint components and specifies whether all the settings below will be updated to the associated sub sites.

Important: Timer Activation executes under the SharePoint Farm Service Account, ensure that the required permissions are configured as per the K2 Documentation : Installation and Configuration > Prerequisites > Security > Permissions for K2 Components > SharePoint Server > K2 for SharePoint - Required Permissions-K2 Designer for SharePoint, under K2 Central Admin account details.

Feature Activation Settings: Specify whether all K2 Features will be activated to the selected site collection.

Connection Settings: Specify the K2 Connection Settings that will be applied to the site collection.

Update settings for all sites in the site collection: Use a SharePoint Timer Job to update sites (K2 Activate All - <http://dx:10899/sites/K2GenSite0>)

Activate all K2 Features to selected site collection:

Add K2 Connection Settings to selected site collection: Host Server: Host Server Port:



For customers not in this category, the recommendation is to use the normal activation and not this option.

The SharePoint Timer Activation executes under the Central Administration App pool user as this is a timer service job, and therefore requires some rights to function correctly.

- The Central Administration App pool user must be granted K2webdesigner DB owner, reader and writer
- The Central Administration App pool user must be granted K2 Administrator rights in host server
- The Central Administration App pool user must be a site collection administrator on the site they are activating to



For more information on permissions required, see [Installation and Configuration > Installation > Post installation common tasks > Permissions for K2 Components > SharePoint Server > K2 for SharePoint - Required Permissions-K2 designer for SP](#)

When the activation starts, the Status page does not immediately show the running job, it will start in approximately 60 seconds from when the Ok button is clicked. This pause depends on the speed of the machine and the load on the Timer Service. If the job does not start in between 1and 2 minutes, something has possibly gone wrong and the event log needs to be reviewed or the activation restarted.

It is also important to note that only one timer activation can run at any one time. Validation will try prevent the user from starting multiple timer activations but in the event of two timer jobs being started, they will interfere with each other and cause one or both jobs to fail. All Errors are logged to the event log, viewable with the Event Viewer.

The screenshot shows the 'Job History' section of the SharePoint Central Administration. A specific timer job titled 'K2 Activate All - http://portal.denallix.com' has failed. The error message in the details pane states: 'An error has occurred, review the application event log, source: 'K2 SharePoint' for more information'. The 'Status' column for this job is 'Failed'.

Job Title	Server	Web Application	Duration (hh:mm:ss)	Status	Completed
K2 Activate All - http://portal.denallix.com	DLX	SharePoint Central Administration v4	0:00:10	Failed	3/26/2012 3:12 AM
Update K2 Global Resources(Deploy Process Portal Global)	DLX	SharePoint Central Administration v4	0:00:00	Succeeded	3/26/2012 3:11 AM

Figure 1: Note the Error Message, then see the Application Event Log (figure 2)

Opening the Application Event Log and selecting an error with K2 SharePoint in the Source column (as indicated in Figure 1) will display the error information in the pane below. The user will also see other errors pointing to the cause, for example in Figure 2 K2SharePoint Administration and K2 SharePoint Process Portal also show errors.

The screenshot displays the Application Event Log with 1,109 events. An error from 'K2 SharePoint' is highlighted, showing the following details:

Event 0, K2 SharePoint

General | **Details**

An error has occurred in a K2 for SharePoint component.

Error details:
User K2:DENALLIX\SPFarmService does not have Administrator rights.

Assembly: SourceCode.SharePoint.ApplicationPages.Administration.dll
Class: ApplicationPoolSection
Method: Execute

Stack trace details:
at SourceCode.Workflow.Management.WorkflowManagementServer.GetAdminPermissions()
at SourceCode.ServerManagement.ServerRightsManagement.AddK2User(String username, Boolean admin, Boolean export, Boolean impersonate)
at SourceCode.SharePoint.ApplicationPages.ApplicationPoolSection.Execute()
Logging verbosity level: Detailed

Figure 2: Application Event Log

Testing a timer activation on a site collection with a small number of sub sites at first is recommended because the timer will only display errors once the entire activation has been attempted. This test will help sort out any common issues quickly.

Three known issues

1

Manifest Issue: The located assembly's manifest definition does not match the assembly reference.

Sometimes the Timer Service does not pick up the newly dropped assemblies during install

Resolution:

Do an IISRESET and restart the SharePoint 2010 Timer, then try the activation again.

Event 6398, SharePoint Foundation

General | **Details** | X

The Execute method of job definition
SourceCode.WebDesigner.SharePoint.Runtime.ConfigureIisSettings (ID fae7cf31-dc3c-439f-b950-af731d327991) threw an exception. More information is included below.

The located assembly's manifest definition does not match the assembly reference. (Exception from HRESULT: 0x80131040)

Log Name:	Application		
Source:	SharePoint Foundation	Logged:	2012/02/01 10:20:46 AM
Event ID:	6398	Task Category:	Timer
Level:	Critical	Keywords:	
User:	VMQA\Administrator	Computer:	SAV-MSBeta.VMQA.local
OpCode:	Info		
More Information: Event Log Online Help			

2

Issue: Central Administration App pool user is not K2 Admin

Resolution: Add the user via Workspace or Management Console

3

Issue: Central Administration App pool does not have rights on the K2 web designer DB.

Application Number of events: 1,127

Level	Date and Time	Source	Event ID	Task Category
Information	3/26/2012 3:20:31 AM	K2 SharePoint	0	None
Critical	3/26/2012 3:20:29 AM	SharePoint Foundation	6398	Timer
Information	3/26/2012 3:20:29 AM	K2 SharePoint: Administration	0	None
Error	3/26/2012 3:20:28 AM	K2 SharePoint	0	None
Information	3/26/2012 3:20:28 AM	MSSQLSERVER	18456	Logon
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None
Information	3/26/2012 3:20:24 AM	Unspecified	0	None

Event 0, K2 SharePoint

General | Details |

An error has occurred in a K2 for SharePoint component.

Error details:
The server principal "DENALLIX\SPFarmService" is not able to access the database "K2WebDesigner" under the current security context.

Assembly: SourceCode.SharePoint.ApplicationPages.Administration.dll
Class: ApplicationPoolSection
Method: Execute

Stack trace details:
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection)
at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj)
at System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj)
at System.Data.SqlClient.SqlCommand.RunExecuteNonQueryTds(String methodName, Boolean async)
at System.Data.SqlClient.SqlCommand.InternalExecuteNonQuery(DbAsyncResult result, String methodName, Boolean sendToPipe)

Resolution: Grant the following rights

Login Properties - DENALLIX\SPFarmService

Select a page: General, Server Roles, User Mapping, Securables, Status

Script | Help

Users mapped to this login:

Map	Database	User	Default Schema
<input type="checkbox"/>	K2ServerLog		
<input type="checkbox"/>	K2SmartBox		
<input type="checkbox"/>	K2SmartBroker		
<input type="checkbox"/>	K2SQLUM		
<input checked="" type="checkbox"/>	K2WebDesigner	DENALLIX\SPFarmSer...	
<input type="checkbox"/>	K2Workflow		
<input type="checkbox"/>	K2Workspace		
<input checked="" type="checkbox"/>	Managed Metadata Se...	dbo	dbo
<input type="checkbox"/>	master		
<input type="checkbox"/>	model		

Guest account enabled for: K2WebDesigner

Database role membership for: K2WebDesigner

<input type="checkbox"/> db_accessadmin
<input type="checkbox"/> db_backupoperator
<input checked="" type="checkbox"/> db_datareader
<input checked="" type="checkbox"/> db_datawriter
<input type="checkbox"/> db_ddladmin
<input type="checkbox"/> db_denydatareader
<input type="checkbox"/> db_denydatawriter
<input checked="" type="checkbox"/> db_owner
<input type="checkbox"/> db_securityadmin
<input checked="" type="checkbox"/> public

Connection: Server: DLX, Connection: DENALLIX\Administrator, [View connection properties](#)

Progress: Ready

OK | Cancel

1.6.8.1.2.3 Add Settings to Site Collection-K2 for SharePoint

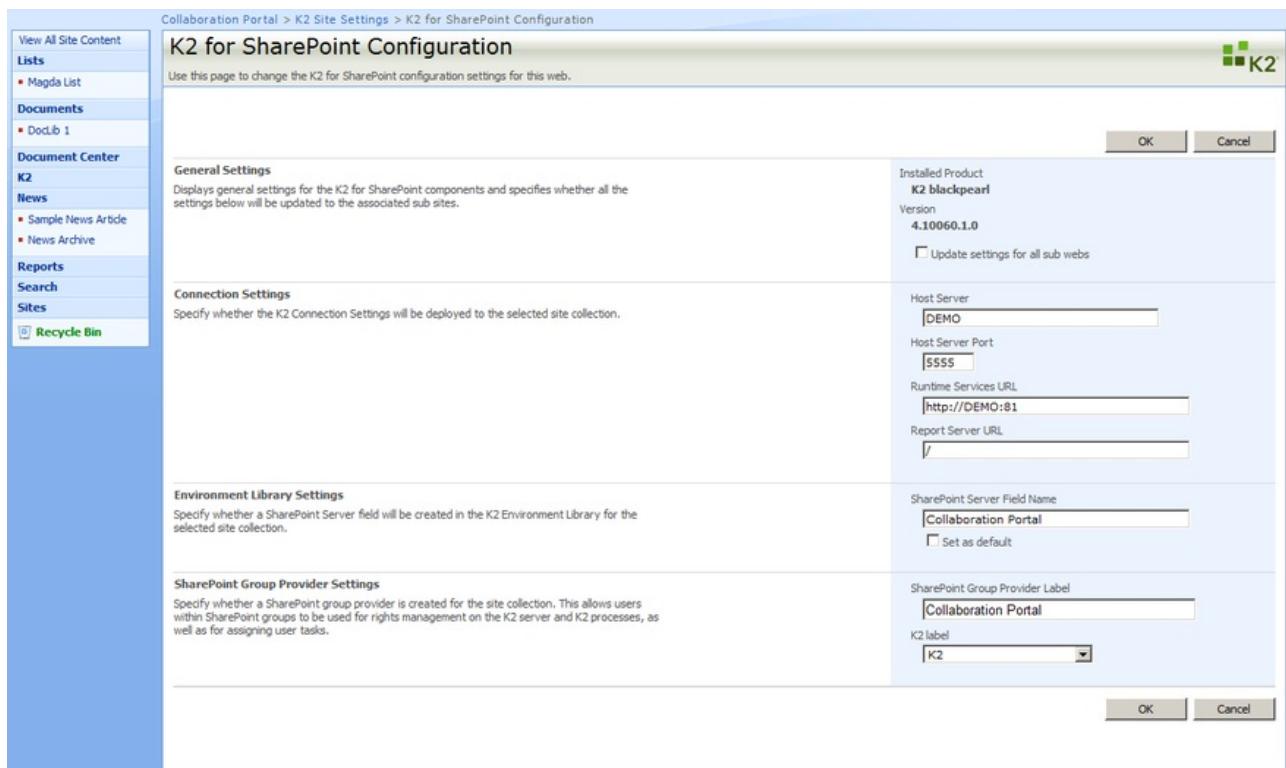
K2 for SharePoint - K2 for SharePoint Configuration

The **K2 for SharePoint Configuration** screen in Central Administration and K2 Site Settings is used to add the K2 Site Settings to a Site Collection within a SharePoint site.

The screenshot shows the 'K2 for SharePoint Configuration' dialog box within the SharePoint Central Administration interface. The dialog box is titled 'K2 for SharePoint Configuration' and contains several sections for configuring K2 features across a selected site collection:

- Activation Location:** Set to 'Site Collection: http://demo:112'.
- General Settings:** Includes fields for 'Installed Product' (K2 blackpearl), 'Version' (4.10060.1.0), and a checkbox for 'Update settings for all sub webs'.
- Feature Activation Settings:** A checkbox for 'Activate all K2 for SharePoint Features to the selected Site Collection' is checked.
- Connection Settings:** Includes fields for 'Host Server' (DEMO), 'Host Server Port' (5555), 'Runtime Services URL' (http://DEMO:81), and 'Report Server URL' (empty).
- Environment Library Settings:** A checkbox for 'Add Settings' is checked, with a field for 'SharePoint Server Field Name' (Collaboration Portal) and an unchecked 'Set as default' option.
- SharePoint Group Provider Settings:** A checkbox for 'Add group provider for site collection' is checked, with fields for 'SharePoint Group Provider Label' (Collaboration Portal) and 'K2 label' (K2).

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.



Function	What it does
Activation Location	Specifies the site collection where the features and settings will be activated
General Settings	Specifies general settings for the K2 for SharePoint component and specifies whether the settings will be updated to the associated sub sites
Feature Activation Settings	Specifies whether all K2 Features will be activated to the selected site collection
Connection Settings	Specifies whether the K2 Connection Settings will be deployed to the selected site collection
Environment Library Settings	Specifies whether a SharePoint Server field will be created in the K2 Environment Library for the selected site collection
SharePoint Group Provider Settings	Specifies whether a SharePoint group provider is created for the site collection.

1.6.8.1.2.4 Add Settings to Site Collection-K2 Designer for SharePoint

K2 for SharePoint - K2 Designer for SharePoint Configuration

The **K2 Designer for SharePoint Configuration** screen in Central Administration and K2 Site Settings is used to add the K2 Designer for SharePoint Settings to a Site Collection within a SharePoint site.

The screenshot shows the 'K2 Designer for SharePoint Configuration' dialog box. At the top right are 'OK' and 'Cancel' buttons. On the left, a navigation bar includes 'Home', 'Operations', 'Application Management', and 'K2 for SharePoint'. The main area has a title 'K2 Designer for SharePoint Configuration' and a sub-instruction 'Deploy the K2 Designer for SharePoint Configuration Settings to the selected site collection.' Below this are several configuration sections:

- Activation Location:** A dropdown menu set to 'http://demo:112'.
- General Settings:** Includes a note about updating settings to sub-sites and a checkbox for 'Update settings for all sub webs'.
- Feature Activation Settings:** A checkbox for 'Activate all K2 Designer for SharePoint Features to the selected Site Collection'.
- Deployment Application Pool:** Offers options to 'Use existing application pool' (selected, pointing to 'K2 for SharePoint (K2DEMO\Administrator)'), or 'Create new application pool' with fields for 'Application pool name' and 'Select a security account for this application pool' (User name and Password fields).
- Process Designers:** A section for specifying groups that can design and deploy processes.
- Process Participants:** A section for specifying groups that can start and view processes.
- Site Collection Groups:** Two separate lists of groups: one for 'Process Designers' and one for 'Process Participants', each with checkboxes for 'Approvers', 'Collaboration Portal Members', 'Collaboration Portal Owners', and 'Collaboration Portal Visitors'.

The screenshot shows the 'K2 Designer for SharePoint Configuration' dialog box. At the top, it says 'This Site: Collaboration Portal'. Below that, there are sections for 'Deployment Application Pool' (set to 'K2 for SharePoint') and 'Site Collection Groups' (listing 'Approvers', 'Collaboration Portal Members', 'Collaboration Portal Owners' (checked), and 'Collaboration Portal Visitors'). There are also sections for 'Process Designers' and 'Process Participants', both with similar settings. Buttons for 'OK' and 'Cancel' are at the bottom right.

Function	What it does
Activation Location	Specifies the site collection where the features and settings will be activated
General Settings	Specifies general settings for the K2 for SharePoint component and specifies whether the settings will be updated to the associated sub sites
Feature Activation Settings	Specifies whether all K2 Features will be activated to the selected site collection
Deployment Application Pool	Specifies the Application Pool to be used when deploying processes
Process Designers	Specifies the groups that can design and deploy processes to the server
Process Participants	Specifies the groups that, at the time of process deployment, will be able to start processes and view information about processes they participate in

1.6.8.1.2.5 K2 Web Parts

K2 for SharePoint - K2 Site Settings Link

The K2 Workflow Integration ASP.NET Page Content Types screen is used to activate K2 features on a SharePoint Site Collection. The SharePoint site can be selected from the **Site Collection** drop-down list. Clicking on the **Activate** button will activate the K2 features on the selected site collection. The K2 Workflow Integration screen is used by the K2 Workflow Integration Default task page and will activate the K2 Default Task Form on the selected Site Collection.

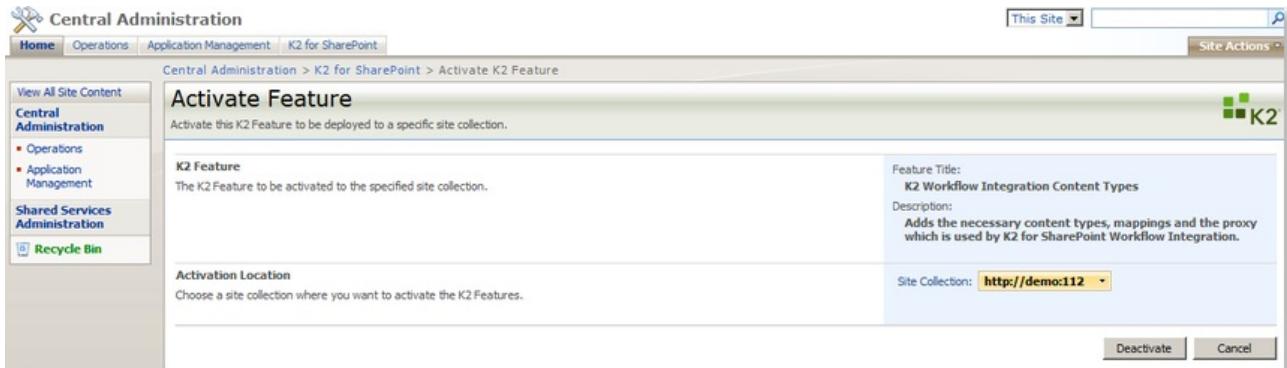


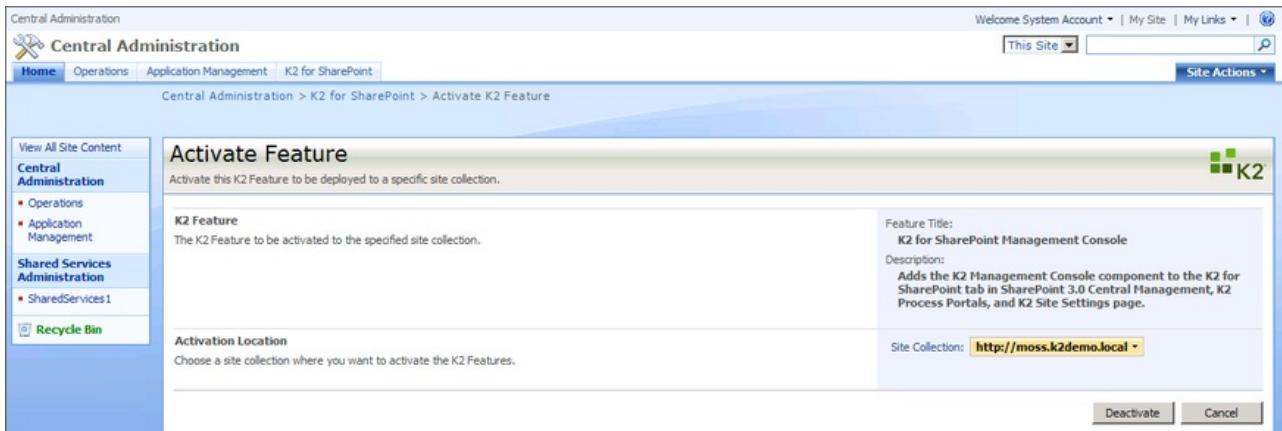
Fig. 1. K2 for SharePoint tab > Features Management

Function	What it does
Title	Displays the title of the current page
Description	Displays the description of the current page
Site Collection	Stipulates the site collection where the K2 features will be activated on. To choose a different site collection, click on the down arrow and select Change Site Collection.
Activate	Click this button to activate the K2 features for the stipulated site collection.
Cancel	Click this button to cancel the activation

1.6.8.1.2.6 Important Considerations

K2 for SharePoint - K2 for SharePoint Management Console

The K2 for SharePoint Management Console screen is used to activate the K2 Management Console component to the K2 for SharePoint tab in SharePoint 3.0 Central Administration, K2 Process Portals, and K2 Site Settings pages. The SharePoint site can be selected from the **Site Collection** drop-down list. Clicking on the **Activate** button will activate the K2 features on the selected site collection.

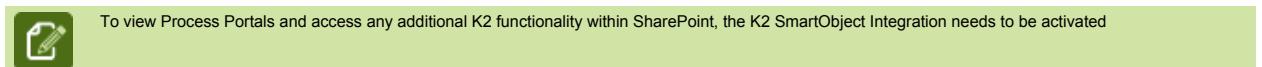


Function	What it does
Feature Title	Displays the title of the current page
Description	Displays the description of the current page
Site Collection	Stipulates the site collection where the K2 features will be activated on. To choose a different site collection, click on the down arrow and select Change Site Collection.
Activate	Click this button to activate the K2 Management Console for the stipulated site collection.
Cancel	Click this button to cancel the activation

1.6.8.1.2.7 K2 Designer for SharePoint

K2 for SharePoint - K2 Designer for SharePoint

The K2 Designer for SharePoint screen is used to add the K2 Designer for SharePoint link to lists and libraries on a SharePoint site, allowing users with Contribute permissions to design and deploy K2 processes in SharePoint. The SharePoint site can be selected from the **Site Collection** drop-down list. Clicking on the **Activate** button will activate the K2 features on the selected site.



Function	What it does
Title	Displays the title of the current page
Description	Displays the description of the current page
Site Collection	Stipulates the site where the K2 features will be activated on. To choose a different site, click on the down arrow and select Change Site Collection.
Activate	Click this button to activate the K2 features for the stipulated site.
Cancel	Click this button to cancel the activation

Activating K2 Designer for SharePoint Task Content Type

After the activation of the K2 Designer for SharePoint on the SharePoint Central Administration you have to activate the content type under **Site Settings/ Site collection features**.

1.6.8.1.2.8 K2 Web Parts

K2 for SharePoint - K2 Site Settings Link

The K2 Workflow Integration ASP.NET Page Content Types screen is used to activate K2 features on a SharePoint Site Collection. The SharePoint site can be selected from the **Site Collection** drop-down list. Clicking on the **Activate** button will activate the K2 features on the selected site collection. The K2 Workflow Integration screen is used by the K2 Workflow Integration Default task page and will activate the K2 Default Task Form on the selected Site Collection.

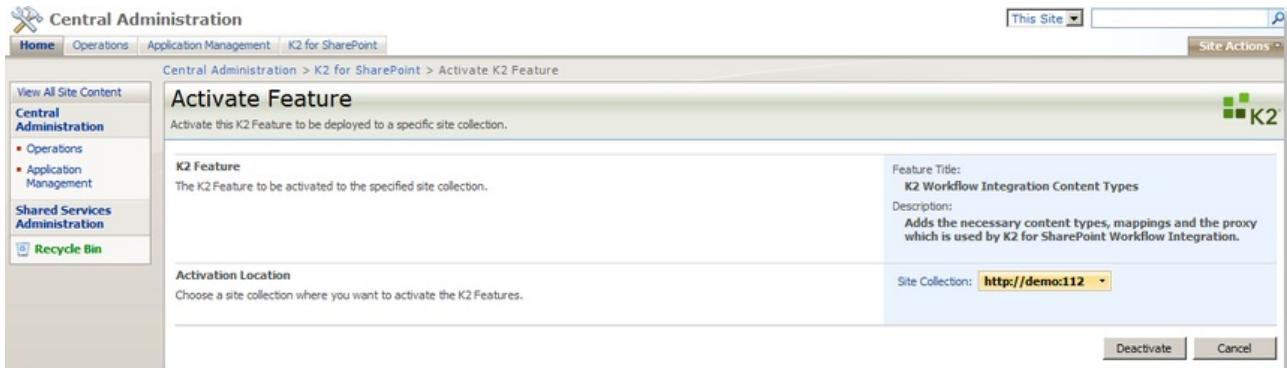


Fig. 1. K2 for SharePoint tab > Features Management

Function	What it does
Title	Displays the title of the current page
Description	Displays the description of the current page
Site Collection	Stipulates the site collection where the K2 features will be activated on. To choose a different site collection, click on the down arrow and select Change Site Collection.
Activate	Click this button to activate the K2 features for the stipulated site collection.
Cancel	Click this button to cancel the activation

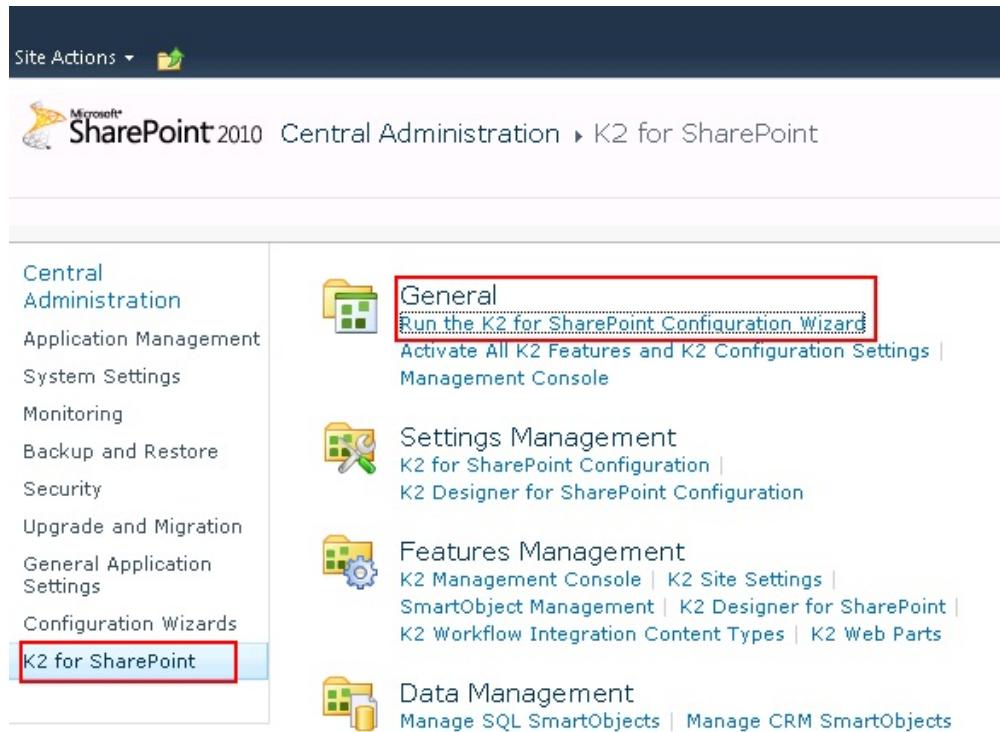
1.6.8.1.2.9 How to register the K2 Failover Job Definition for a new Web Application

Dow to register the K2 Failover Job Definition for a new Web Application

The K2 Failover Job Definition is registered during the running of the SharePoint configuration wizard. If a site does not exist at the time at which the failover is registered it will not activate to the site and will not execute the K2 Workflow Job Definition when tasks are scheduled for creation. Therefore, if a new web application is created after K2 is fully installed it will be necessary to firstly Activate the K2 Features and then manually register the K2 Failover Job Definition for any sites in the new web application.

To register the K2 Failover Job Definition for a web application created after K2 has already been installed follow the steps below:

- 1 Click on the **K2 for SharePoint** Tab in Central Administration
- 2 On the Admin Page under the **General** section select the **Run the K2 for SharePoint Configuration Wizard** link.



- 3 Click Next through the Wizard until the final page is reached. This is the page on which registration automatically occurs for each web application.
- 4 To verify click the **Register** link.
- 5 Select the option Navigate to **K2 for SharePoint** page in Central Administration.
- 6 Click the **Update All** button.

Central Administration

Features

Name	Status	Details
K2AdminLinks	Pending	
K2ProcessPortalsConfiguration	Pending	
K2ManagementConsole	Pending	
K2ConfigWizard	Pending	
K2ProcessPortals	Pending	
K2WebDesignerConfiguration	Pending	

Job Definitions

Name	Status	Details
K2 Workflow Failover	Registered	

Comments

Features:

- Use this page to upgrade existing features across the farm. The Features will only be upgraded on site collections.
- The time required to upgrade these features depends on the number of site collections in the farm that currently have them installed.
- Use the Upgrade link to upgrade features individually, or use the Upgrade All button to upgrade all features.
- Note that feature upgrade is not required to complete this wizard. However, it is recommended to perform the upgrade.

Job definitions:

- The required K2 Job definitions have been registered in SharePoint when this page loaded.

Next Step

Navigate to 'Activate All K2 Features and K2 Configuration Settings' page in order to activate the K2 features to the farm.
 Navigate to 'K2 for SharePoint' page in Central Administration.

Report - K2 Workflow Failover

The following information is available for the selected item.

Time	Result	Message	Scope	Target
8/3/2011 9:03:42 AM	Registered	Job Definition Exists	WebApplication	SharePoint - 21879
8/3/2011 9:03:42 AM	Registered	Job Definition Exists	WebApplication	SharePoint - 80

OK Cancel



On clean installs the page will show the features being **Pending**, this can just be ignored, and the wizard can be finished with the second radio button choice.

Site Actions ▾ **Browse** Page

SharePoint 2010 Central Administration ▶ Monitoring

Central Administration

Monitoring

Health Analyzer
Review problems and solutions | Review rule definitions

Timer Jobs
Review job definitions | Check job status

Reporting
View administrative reports | Configure diagnostic logging | Review Information Management Policy Usage Reports | View health
Configure usage and health data collection | View Web Analytics reports

Timer Links			
Timer Job Status			
Scheduled Jobs	Scheduled		
Running Jobs	Job Title	Server	Web Application
Job History	Application Server Administration Service Timer Job	sav-docs-leesyl	
Job Definitions	Scheduled Unpublish	sav-docs-leesyl	SharePoint - 21879
Central Administration	Workflow	sav-docs-leesyl	
	Scheduled Unpublish	sav-docs-leesyl	SharePoint - 80
	K2 Workflow Failover	sav-docs-leesyl	SharePoint - 21879
	K2 Workflow Failover	sav-docs-leesyl	SharePoint - 80
	User Profile Service Application - System Job to Manage User Profile Synchronization	sav-docs-leesyl	
	User Profile Service Application - User Profile Language Synchronization Job	sav-docs-leesyl	
	Scheduled Approval	sav-docs-leesyl	SharePoint - 21879
	Scheduled Approval	sav-docs-leesyl	SharePoint - 80
	Running		
	Job Title	Server	Progress

If the Failover is not manually registered for the new site, users might experience some tasks that are being created and some that are not. The ones that are not being created are being scheduled for creation but since there is no K2 Workflow Failover registered for that site the job definition will never fire and the tasks will never get created.

1.6.8.1.3 Activating Process Approval

Process Approval - Activating Process Approval

To make use of the Process Approval feature in the K2 Designer for SharePoint it first needs to be activated. This can be done in either:

- **SharePoint Site Actions**
- within the **SharePoint Central Administration** under the Activate All K2 Features and K2 Configuration Settings
- in the **K2 Designer for SharePoint Configuration** page.

To activate the Process Approval feature in the K2 Designer for SharePoint Configuration perform the following steps:



The Browser User that is configuring the K2 Process Approval feature in Central Administration or on the Site Collection Settings requires K2 Admin rights.

Rights and Permissions

If activating from SharePoint central Administration, the following is required:

- Application Pool User: K2 Admin rights
- Logged on user: Local Admin Rights, K2 Admin

If activating from a site collection, the following is required

- Site Application pool User: Local Administration rights



Local Administration rights are only required on Site Collections if Process Activation was never performed on the site from SharePoint Central Administration

- Logged on User: K2 Admin Rights

How to Activate Process Approval



On the SharePoint home page browse to **Site Actions > K2 Site Settings** or if using SharePoint Central Administration, click on the **K2 for SharePoint** tab.

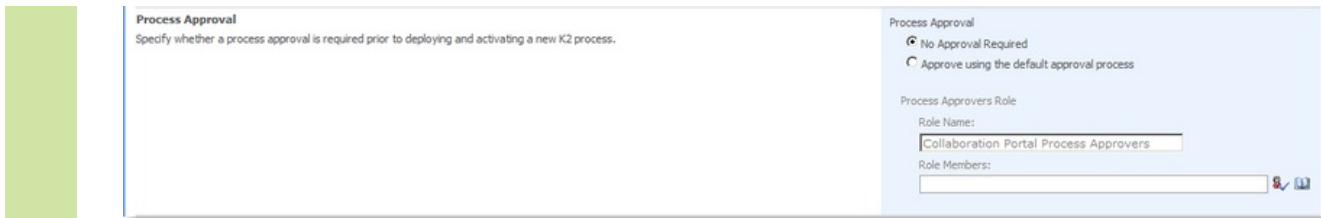


Select **K2 Designer for SharePoint Configuration**. The following screen will be displayed:

The screenshot shows the 'K2 Designer for SharePoint Configuration' dialog box. It includes sections for Deployment Application Pool (set to 'K2 blackpearl'), Site Collection Groups (checkboxes for Designers, Hierarchy Managers, Quick Deploy Users), Process Participants (checkboxes for Approvers, Collaboration Portal Members, Collaboration Portal Owners, Collaboration Portal Visitors), and Process Approval (radio button selected for 'Approve using the default approval process').



On the **Process Approval** section of the page, select the **Approve using the default approval process** option.



4 Modify the Process Approvers Role name if required.

5 Use the People Picker to assign Role Members to the Process Approval process.



The Role Members defined here will be the destination users for the process. This is stored in a K2 Role and can be modified using the Management Console. The members of this Role can consist of SharePoint Group, Active Directory Group, a user or an e-mail distribution list.

6 Click **OK**

1.6.8.1.4 Process Portal - Web Parts

K2 Process Portals - Web Parts

There are several K2 for SharePoint features that need to be activated in order to take full advantage of the K2 integration with SharePoint. These features are activated in SharePoint Central Administration, and must be activated on each Site Collection on which you wish to use the K2 integration, see [Activate Web Parts](#). The K2 Installer will automatically deploy the solutions required for activation of the K2 features.

Should the need arise to manually deploy the solutions, it can be done from SharePoint Central Administration. For manual deployment, do the following steps:

- 1
- 2
- 3

Open **SharePoint Central Administration** (Start > All Programs > Microsoft Office Server > SharePoint 3.0 Central Administration)

Click on the **Operations** tab

Click on the **Solution Management** link under the Global Configuration section, as shown below:

The screenshot shows the 'Operations' page in SharePoint Central Administration. The 'Global Configuration' section is expanded, and the 'Solution management' link is highlighted with a red box. Other links in this section include Timer job status, Timer job definitions, Master site directory settings, Site directory links scan, Alternate access mappings, Manage farm features, and Quiesce farm.

On the Solution Management page, you will see the different solutions. If a specific solution has not been deployed by the K2 Installer, the status will be **Not Deployed**

- 4

Click on the solution link. The solution page will load, and look like the following:

The screenshot shows the 'Solution Properties' page for the solution 'k2worklistwebpart.wsp'. The deployment status is listed as 'Deployed' with the URL 'http://demo:112/'. The last operation result is 'The solution was successfully deployed.' and the last operation details show two identical entries: 'DEMO : http://demo:112/ : The solution was successfully deployed.' and 'DEMO : http://demo:112/ : The solution was successfully deployed.'. The last operation time is '6/2/2009 8:32 AM'.

Click **Deploy Solution**

Leave the default settings, and click **OK** in the Deploy Solutions window

- 5
- 6

1.6.8.1.4.1 PP-Web Parts-Activate Web Parts

K2 Process Portals - Activate K2 Web Parts

The **K2 Web Parts** feature and **K2 Configuration Settings** need to be activated on each Site Collection on which you wish to use the K2 Integration. The **K2 Web Parts** feature adds a link to the **Site Actions** menu in SharePoint to access the K2 Web Parts page. On this page, you can manage the K2 Web Parts on each Site Collection.

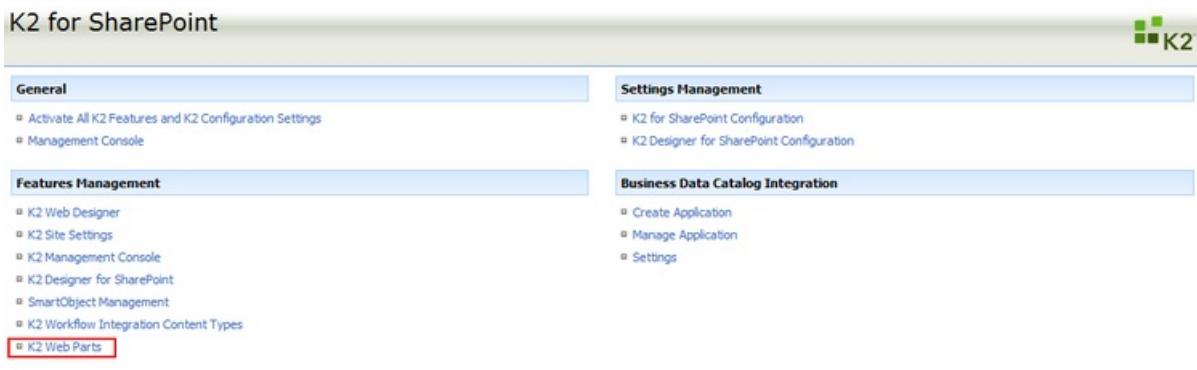
To activate, perform the following steps:

① Open **SharePoint Central Administration**

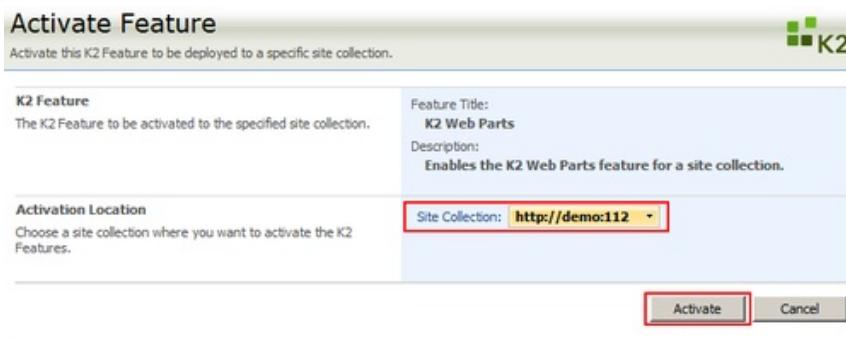
② Click on the **K2 for SharePoint** tab:



③ Click on the **K2 Web Parts** link:



④ Select the **Site Collection** where you wish to deploy the K2 Web Parts Link, and click **Activate**:



⑤ The K2 Web Parts feature will activate.

⑥ Click on the **K2 for SharePoint Configuration** link:

K2 for SharePoint



General

- Activate All K2 Features and K2 Configuration Settings
- Management Console

Features Management

- K2 Web Designer
- K2 Site Settings
- K2 Management Console
- K2 Designer for SharePoint
- SmartObject Management
- K2 Workflow Integration Content Types
- K2 Web Parts

Settings Management

- K2 for SharePoint Configuration
- K2 Designer for SharePoint Configuration

Business Data Catalog Integration

- Create Application
- Manage Application
- Settings

7

Verify that all the connection settings are correct based on your K2 installation. Select the **Site Collection** where you wish to add the K2 settings, and click **OK**:

Central Administration

Central Administration

Home Operations Application Management K2 for SharePoint

Central Administration > K2 for SharePoint > K2 for SharePoint Configuration

K2 for SharePoint Configuration

Deploy the K2 for SharePoint Configuration Settings to the selected site collection.

Activation Location
Choose a site collection where you want to activate the K2 Features and K2 Configuration Settings.

Site Collection: http://demo:112

General Settings
Displays general settings for the K2 for SharePoint components and specifies whether all the settings below will be updated to the associated sub sites.

Installed Product: K2 blackpearl
Version: 4.10060.10
 Update settings for all sub webs

Activate all K2 for SharePoint Features to the selected Site Collection

Feature Activation Settings
Specify whether all K2 Features will be activated to the selected site collection.

Add K2 Connection Settings to selected site collection

Host Server: DEMO
Host Server Port: 5555
Runtime Services URL: http://DEMO:81
Report Server URL: /

Connection Settings
Specify whether the K2 Connection Settings will be deployed to the selected site collection.

Environment Library Settings
Specify whether a SharePoint Server field will be created in the K2 Environment Library for the selected site collection.

Add Settings
SharePoint Server Field Name: Collaboration Portal
 Set as default

SharePoint Group Provider Settings
Specify whether a SharePoint group provider is created for the site collection. This allows users within SharePoint groups to be used for rights management on the K2 server and K2 processes, as well as for assigning user tasks.

Add group provider for site collection
SharePoint Group Provider Label: Collaboration Portal
K2 label: K2

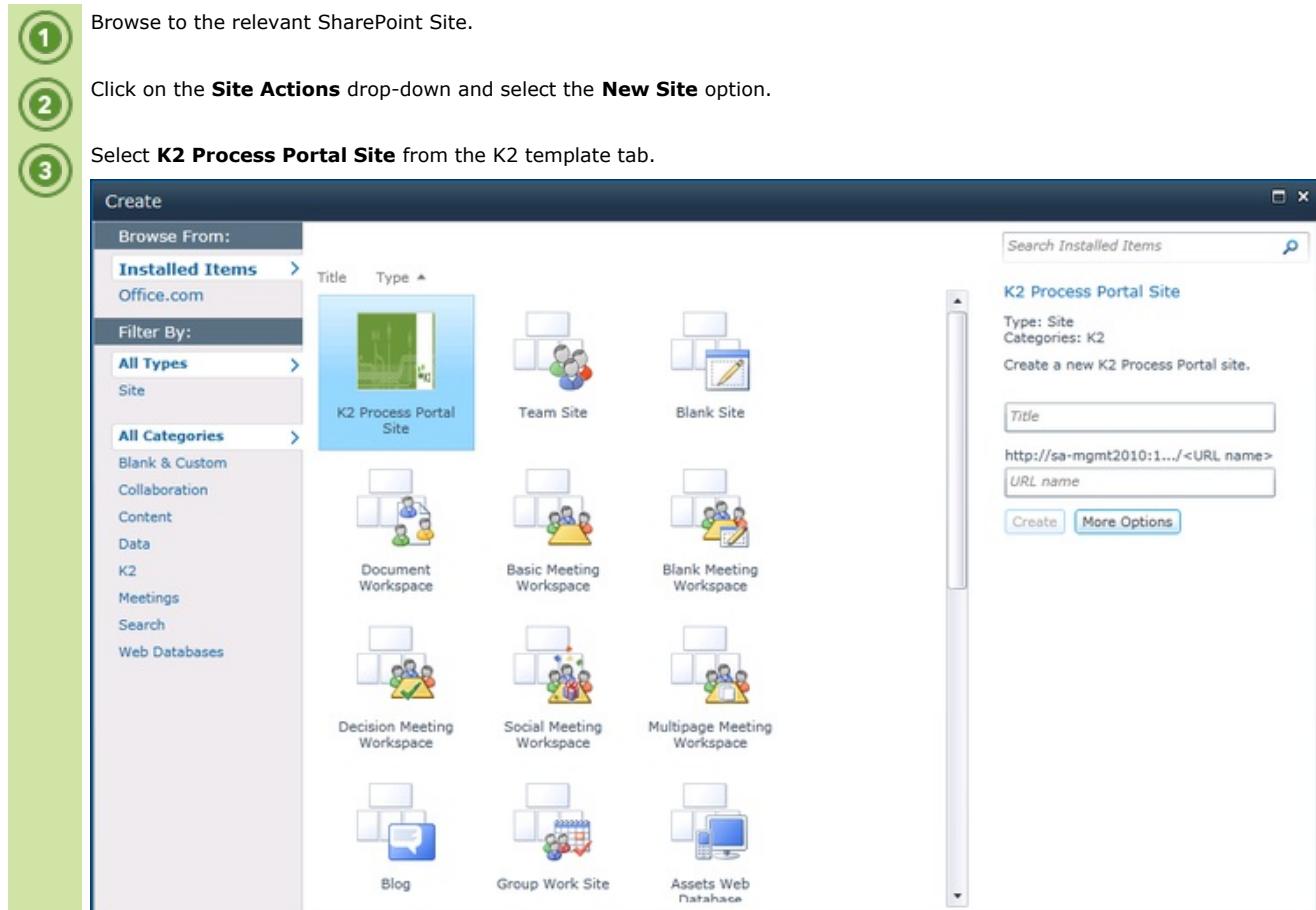
OK Cancel

1.6.8.1.4.2 Creating a Process Portal

K2 for SharePoint 2010 - Creating a Process Portal

The K2 for SharePoint Process Portal solution is deployed during the installation of K2 for SharePoint 2010. Once the solution has been deployed, a K2 Process Portal site can be created to manage processes.

Perform the following steps to create a Process Portal:



The screenshot shows the SharePoint 'Create' dialog. On the left, there's a sidebar with 'Browse From:' (Installed Items, Office.com), 'Filter By:' (All Types, Site), and 'All Categories' (Blank & Custom, Collaboration, Content, Data, K2, Meetings, Search, Web Databases). In the center, a grid of site templates is displayed. The 'K2 Process Portal Site' template is highlighted with a blue border. To its right are other templates: Team Site, Blank Site, Document Workspace, Basic Meeting Workspace, Blank Meeting Workspace, Decision Meeting Workspace, Social Meeting Workspace, Multipage Meeting Workspace, Blog, Group Work Site, and Assets Web Database. On the right side of the dialog, there's a panel titled 'K2 Process Portal Site' with fields for 'Title' (set to 'http://sa-mgmt2010:1.../ <URL name>') and 'URL name'. At the bottom are 'Create' and 'More Options' buttons.

- 1 Browse to the relevant SharePoint Site.
- 2 Click on the **Site Actions** drop-down and select the **New Site** option.
- 3 Select **K2 Process Portal Site** from the K2 template tab.
- 4 Provide the Process Portal site with a **Title** and **URL Name** in the provided fields and click **Create**.

1.6.8.1.4.3 PP-Web Parts-Add Web Parts

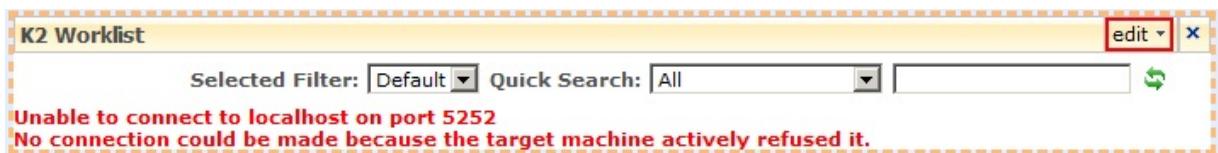
K2 Process Portals - Adding K2 Web Parts

Now that the Web Part solution has been deployed and activated, you can add the Web Parts to the SharePoint pages. The steps below will add the web part to the **K2 Management Process Portal** home page, but it could just as easily be added to any page in your SharePoint environment. The following web parts are added to a Process Portal by default:

- K2 Worklist
- Processes
- Management Worklist
- Instances Summary

To add additional web parts, perform the following steps:

- 1 Open an Internet Explorer browser
- 2 Navigate to your **K2 Management Process Portal** home page
- 3 Click **Site Actions > Edit Page**
- 4 In a Zone, click Add a Web Part
- 5 In the dialog that opens, scroll down to the **K2 Web Parts** section. The available web parts are listed here
- 6 Select the **Action Rights** web part for example
- 7 Click **Add**. The page will refresh with the new web part. An error will be displayed as shown below if your K2 Server service is not running or if the K2 Server details are not up to date:



- 8 To update the K2 Server details, click **Edit > Modify Shared Web Part** to open the tool pane with the properties for the web part
- 9 In the **K2 Server Name** and **Host Server Name** text boxes, type in the name of your K2 Server or K2 Cluster
- 10 Change the value of the **Report Server URL** to the URL of your Reporting Services web site
- 11 Click **OK**. The page will refresh and you should see any items waiting on you in the worklist, or a message that no worklist items are available.
- 12 If you're still getting the error as reflected above, ensure that your K2 Server service is running. This service can be found in Internet Information Services (IIS) Manager
- 13 Click on **Exit Edit Mode** to finalize the changes
- 14 Select the process(s) from the **Settings** page if required

Web Parts

The following Web Parts are available:

- Action Rights
- Error Logs
- K2 Worklist
- Management Worklist
- Process Connections
- Process Instances
- Process Instance Summary
- Process Rights
- Roles
- Versions

1.6.8.1.4.4 Web Parts Solution Deployment in SharePoint 2010

K2 Process Portals - Web Parts Solution Deployment in SharePoint 2010

There are several K2 for SharePoint features that need to be activated in order to take full advantage of the K2 integration with SharePoint. These features are activated in SharePoint Central Administration, and must be activated on each Site Collection on which you wish to use the K2 integration, see [Activate Web Parts](#). The K2 Installer will automatically deploy the solutions required for activation of the K2 features.

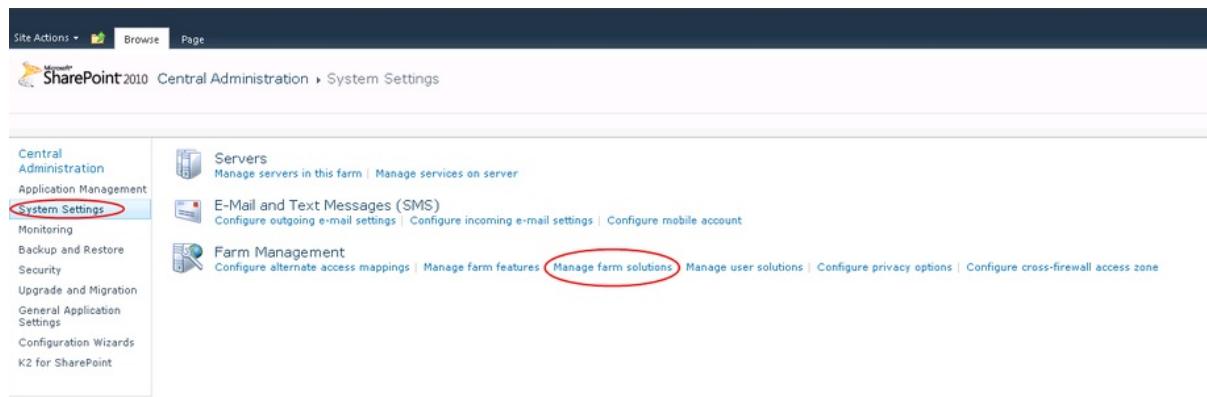
Should the need arise to manually deploy the solutions, it can be done from SharePoint Central Administration. For manual deployment, do the following steps:

- 1
- 2
- 3

Open **SharePoint Central Administration** (Start > All Programs > Microsoft SharePoint 2010 Products > SharePoint 2010 Central Administration)

Click on the **System Settings** link

Click on the **Manage farm solutions** link under the Farm Management section, as shown below:



On the Solution Management page, you will see the different solutions. If a specific solution has not been deployed by the K2 Installer, the status will be **Not Deployed**

Name	Status	Deployed To
k2 for sharepoint - bcs smartobject service.wsp	Deployed	Globally deployed.
k2 for sharepoint - core components.wsp	Deployed	Globally deployed.
k2 for sharepoint - management console.wsp	Deployed	Globally deployed.
k2 for sharepoint - process portals.wsp	Deployed	http://sav-docs2010pea:105/
k2 for sharepoint - web designer.wsp	Deployed	Globally deployed.
k2 for sharepoint - workflow core.wsp	Deployed	Globally deployed.
k2 reporting web parts.wsp	Deployed	http://sav-docs2010pea:105/
k2worklistwebpart.wsp	Deployed	http://sav-docs2010pea:105/...

Click on the solution link. The solution page will load, and look like the following:

- 4

Central Administration

Solution Properties

Name: k2 for sharepoint - process portals.wsp
Type: Core Solution
Contains Web Application Resource: Yes
Contains Global Assembly: Yes
Contains Code Access Security Policy: No
Deployment Server Type: Front-end Web server
Deployment Status: Deployed
Deployed To: http://sav-docs2010pea:105/
Last Operation Result: The solution was successfully deployed.
Last Operation Details: sav-docs2010pea : http://sav-docs2010pea:105/ : The solution was successfully deployed.
Last Operation Time: 10/18/2010 9:48 AM

Click **Deploy Solution**

Leave the default settings, and click **OK in the Deploy Solutions window**

5
6

1.6.8.1.4.5 Activate K2 Web Parts in SharePoint 2010

K2 Process Portals - Activate K2 Web Parts in SharePoint 2010

The **K2 Web Parts** feature and **K2 Configuration Settings** need to be activated on each Site Collection on which you wish to use the K2 Integration. The **K2 Web Parts** feature adds a link to the **Site Actions** menu in SharePoint to access the K2 Web Parts page. On this page, you can manage the K2 Web Parts on each Site Collection.

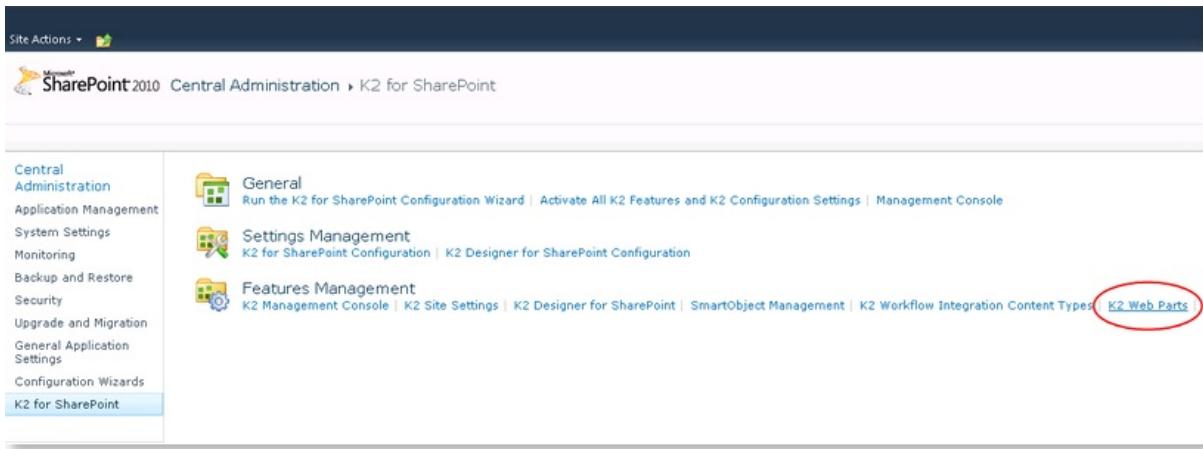
To activate, perform the following steps:

① Open **SharePoint 2010 Central Administration**

② Click on the **K2 for SharePoint** link:



③ Click on the **K2 Web Parts** link:



④ Select the **Site Collection** where you wish to deploy the K2 Web Parts Link, and click **Activate**:

The K2 Web Parts feature will activate.

5

6

Click on the **K2 for SharePoint Configuration** link under the **Settings Management** section:

7

Verify that all the connection settings are correct based on your K2 installation. Select the **Site Collection** where you wish to add the K2 settings, and click **OK**:

Site Actions:

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Configuration Wizards

K2 for SharePoint

Activation Location

Choose a site collection where you want to activate the K2 Features and K2 Configuration Settings.

Site Collection: <http://sav-docs2010pea:105>

General Settings

Displays general settings for the K2 for SharePoint components and specifies whether all the settings below will be updated to the associated sub sites.

Installed Product: K2 blackpearl

Version: 4.10203.11130.0

Update settings for all sub webs

Feature Activation Settings

Specify whether all K2 Features will be activated to the selected site collection.

Activate all K2 for SharePoint Features to the selected Site Collection

Connection Settings

Specify whether the K2 Connection Settings will be deployed to the selected site collection.

Add K2 Connection Settings to selected site collection

Host Server: SAV-Docs2010Pearl

Host Server Port: 5555

Runtime Services URL: http://SAV-DOCS2010PEA:81

Report Server URL: SAV-Docs2010Pearl

Environment Library Settings

Specify whether a SharePoint Server field will be created in the K2 Environment Library for the selected site collection.

Add Settings

SharePoint Server Field Name: MOSS

Set as default

SharePoint Group Provider Settings

Specify whether a SharePoint group provider is created for the site collection. This allows users within SharePoint groups to be used for rights management on the K2 server and K2 processes, as well as for assigning user tasks.

Add group provider for site collection

SharePoint Group Provider Label: MOSS

K2 label: K2

OK | Cancel

1.6.8.1.4.6 Adding K2 Web Parts in SharePoint 2010

Adding K2 Web Parts in SharePoint 2010

Now that the Web Part solution has been deployed and activated, you can add the K2 Web Part to the SharePoint pages. The steps below will add the web part to the **K2 Process Portal** home page, but it could just as easily be added to any page in your SharePoint environment. The following web parts are added to a K2 Process Portal by default:

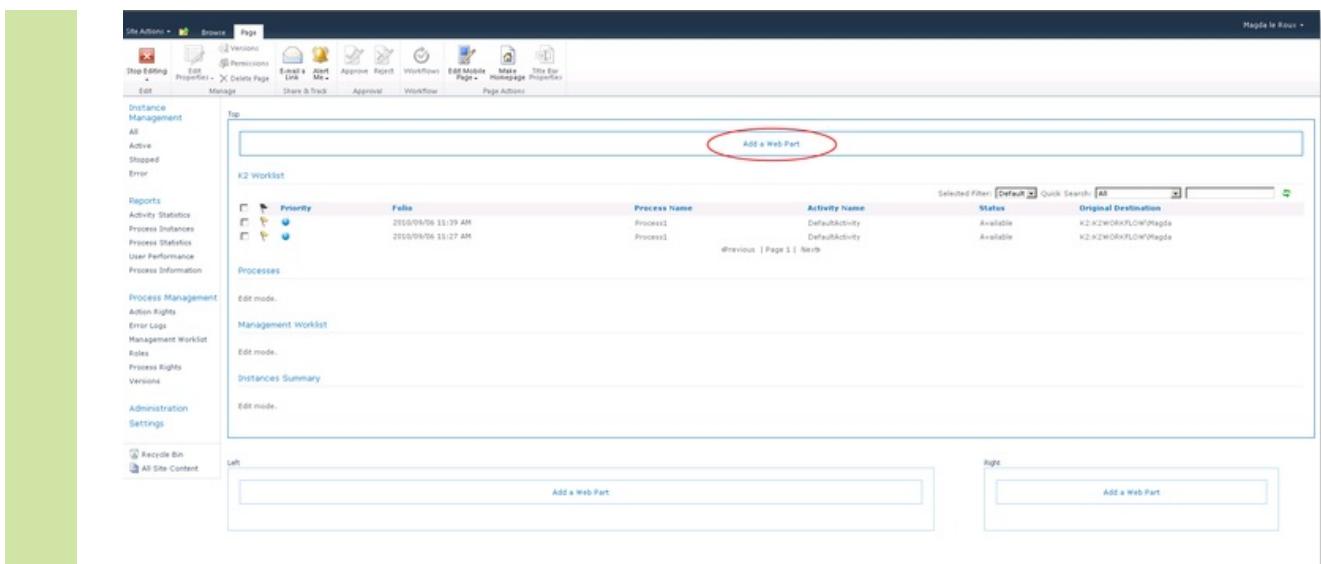
- K2 Worklist
- Processes
- Management Worklist
- Instances Summary

To add additional web parts, perform the following steps:

- 1 Open an Internet Explorer browser
- 2 Navigate to your **K2 Process Portal** home page
- 3 Click **Site Actions > Edit Page**

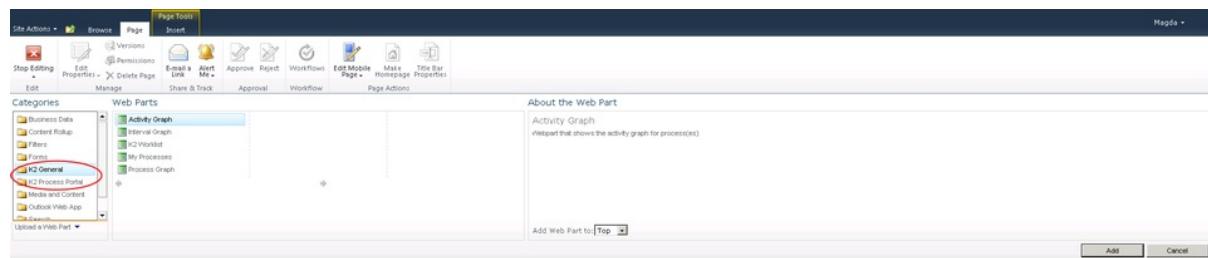


- 4 In a Zone, click **Add a Web Part**



5 In the **Categories** section, scroll down to the **K2 General or K2 Process Portal** folder. The available web parts are listed here

5



6 Select the **K2 Web Part** you want to add

6

7 Click **Add**. The page will refresh with the new web part. An error will be displayed if your K2 Server service is not running or if the K2 Server details are not up to date.

Ensure that your K2 Server service is running. This service can be found in Internet Information Services (IIS) Manager

8 Click on **Stop Editing** to finalize the changes

9 Select the process(s) from the **Settings** page if required

7

8

9

Web Parts

The following Web Parts are available:

See this topic in the online K2 blackpearl help for descriptions: <http://help.k2.com/helppages/K2blackpoint1370/SPI01.html>

- Action Rights
- Error Logs
- K2 Worklist
- Management Worklist
- Process Connections
- Process Instances
- Process Instance Summary
- Process Rights
- Roles
- Versions
- My Processes
- Activity Graph
- Process Graph
- Interval Graph

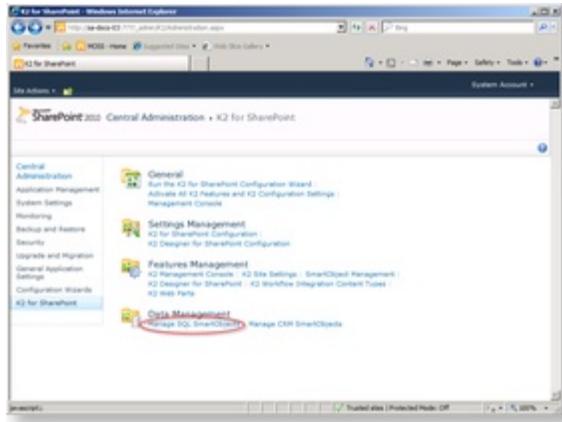
1.6.8.1.5 How to Create a SharePoint SmartObject

Managing SharePoint SmartObject Connections



The individual administering the SharePoint SmartObject connection must be a SharePoint Administrator to be able to perform the registration process.

The process starts from within **SharePoint Administration > K2 for SharePoint > Data Management | Manage SQL SmartObjects**. Once the page is loaded, all registered service instances will be displayed here and the user can make the required selection.



Data Management	
Manage SQL SmartObjects	Enables the user to Manage a SQL SmartObject connection to an existing SQL Server Instance
Manage CRM SmartObjects *	Enables the user to Manage a SQL SmartObject connection to an existing Microsoft CRM Server (CRM SmartObjects)
* Beyond the scope of this topic	

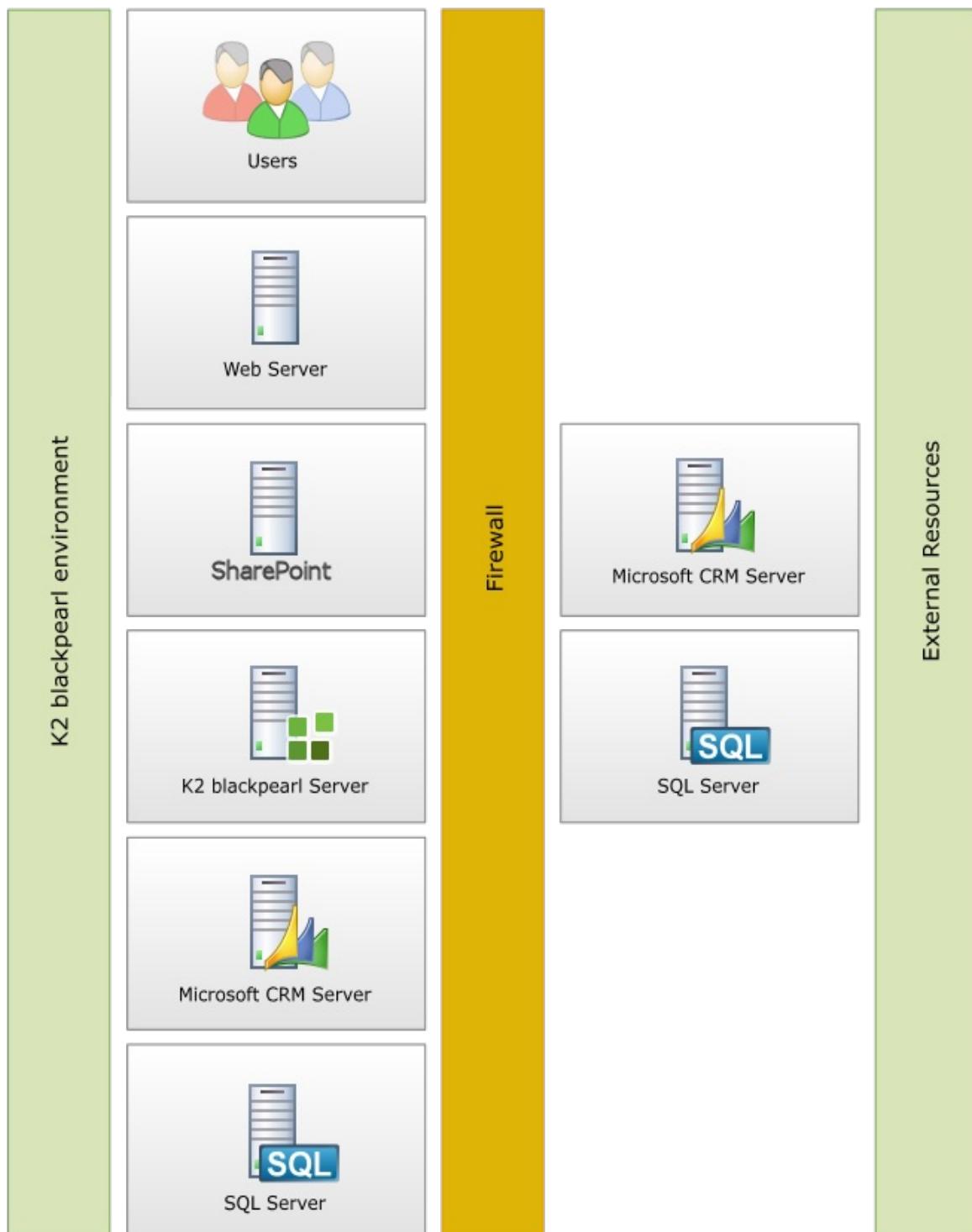
1.6.8.1.5.1 Introduction

Introduction

K2 provides the ability to create and manage Service Instances and SmartObjects for SharePoint, SQL Server and CRM via management pages found in SharePoint. SmartObjects in SharePoint are managed at the Site Collection level via the **K2 Site Settings** pages while SQL Server and CRM are managed at the Central Administration level via the **K2 for SharePoint Data Management** pages.

SmartObject Sources

The SmartObjects that are generated within SharePoint can be from an internal resource (SharePoint, SQL Server or CRM) or an external resource (SQL Server or CRM). If the resource is external and the internet connection is protected by a proxy server, the appropriate user rights would be required to access this resource as well. The external source, such as a SQL Server database or CRM organization, provides the underlying objects/entities that will become SmartObjects.



1.6.8.1.5.2 SharePoint SmartObjects

1.6.8.1.5.2.1 Introduction

K2 for SharePoint - K2 SmartObject Service Management

SmartObjects generated from SharePoint or created in K2 Designer for Visual Studio or K2 Studio can be used in the K2 Designer for SharePoint.

Creating SmartObjects using SharePoint Site Lists and Libraries

A SmartObject containing the properties and methods for a particular Microsoft SharePoint site can be created by the user. Follow the steps below to create a SmartObject using Site Lists and Libraries.

1. Open the SharePoint Central Administration and select the K2 for SharePoint tab.

The screenshot shows the SharePoint 2010 Central Administration interface. The left navigation menu is visible, and the main content area displays several management sections under the 'K2 for SharePoint' tab. The sections include General, Settings Management, Features Management, and Data Management, each with their respective sub-links.

2. Activate the SmartObject Management and the K2 Site Settings features.
3. Open the relevant SharePoint site.
4. Click on the drop-down arrow on Site Actions.
5. Click K2 Site Settings.

The screenshot shows the SharePoint Site Actions menu. The 'Site Actions' dropdown is open, displaying various options like Sync to SharePoint Workspace, New Page, New Document Library, New Site, More Options..., View All Site Content, Edit in SharePoint Designer, Site Permissions, Site Settings, and K2 Site Settings. The 'K2 Site Settings' option is highlighted with a blue selection bar.

6. Select K2 SmartObject Site Lists and Libraries from the SmartObject Management section.

The screenshot shows the 'Site Actions' menu with 'MOSS > Site Settings'. The 'Home' tab is selected. In the 'K2 SmartObject Management' section, there are two main categories: 'General' and 'SmartObject Management'. Under 'General', there is a link to 'K2 for SharePoint Configuration Management Console'. Under 'SmartObject Management', there are links for 'K2 SmartObject Site Lists and Libraries', 'Export SmartObjects Configuration', and 'Import SmartObjects Configuration'. To the right, there are sections for 'Integration Management' (Events Integration Management, Workflow Integration Management) and 'K2 Designer for SharePoint Management' (K2 Designer for SharePoint Configuration, Set Restricted Wizards, Configure SmartObject Access).

7. Select the Site Lists and Libraries that must be used to create the SmartObject. Click the Create button.

The screenshot shows the 'Site Actions' menu with 'MOSS > K2 SmartObject Site Lists and Libraries'. The 'Home' tab is selected. The page lists various document libraries and lists available for use with K2 SmartObjects. Under 'Document Libraries', it shows 'Customized Reports', 'DocLib1', 'DocLib2', and 'DocLib3'. Under 'Lists', it shows 'Announcements', 'Calendar', 'Customer', 'Department', 'Links', 'Product', 'Region', 'Tasks', and 'Workflow History'. There are checkboxes for selecting items, and descriptions for each library or list. At the bottom, there are buttons for 'Create' and 'Cancel'.

Option	Description
Security	Check this option if you require impersonation by the K2 Server
Dynamic	Check this option to if you want to reuse SmartObjects for multiple sites
Advanced	Check this option if you do not want to create SmartObjects, but only create the Service Object Instance
Create	Click the Create button

8. Open the Object Browser in K2 Studio and check in the Environment>SmartObject Server(s)>SmartObject Server for the newly created SmartObject. Expand the SmartObject to view the SmartObject Methods and Properties.



Keep a record of the site where the Service Instance was created

Creating SmartObjects using Visual Studio or K2 Studio

SmartObjects that are created in K2 Designer for Visual Studio and K2 Studio can be made available for use in the K2 Designer for SharePoint. To enable these SmartObjects in the K2 Designer for SharePoint, see [Configure SmartObject Access](#)

For more detail on SmartObjects in K2 Designer for Visual Studio or K2 Studio, see the following topics:

SmartObject Design Concepts
K2 Designer for Visual Studio SmartObjects

1.6.8.1.5.2.2 Using SmartObjects in SharePoint

SmartObjects in SharePoint

K2 SmartObjects can be associated with SharePoint Lists and Document Libraries.

SharePoint Lists

SharePoint Lists can be associated with the following K2 SmartObject methods:

SmartObject Method	Description
Get List	Will return all matching meta data information of the List Item. If no search parameters are provided the Get List method will return all meta data information for the List Item.
Load	Will load the specified List Item from the List Item ID provided
Create	Creates a new List Item on the SharePoint List
Update	Updates the specified List Item on the SharePoint List
Delete	Deletes the specified List Item on the SharePoint List
Add Attachment	Adds an attachment to the specified List Item on the SharePoint List
List Folders	Lists the Folders located in the specified SharePoint List

SharePoint Document Libraries

SharePoint Document Libraries can be associated with the following K2 SmartObject methods:

SmartObject Method	Description
Get List	Will return all matching meta data information of the Document. If no search parameters are provided the Get List method will return all meta data information for the Document.
Load	Will load the specified Document meta data from the Document meta data specified
Create	Creates a new Document on the SharePoint Document Library
Update Document	Updates the specified Document on the SharePoint Document Library
Update Document meta data	Updates the specified Document's meta data on the SharePoint Document Library
Delete document	Deletes the specified Document on the SharePoint Document Library
Retrieve document	Retrieves the specified Document from the SharePoint Document Library
Check In	Checks in the specified Document on the SharePoint Document Library
Check Out	Checks out the specified Document from the SharePoint Document Library
List Folders	Lists the Folders located in the specified SharePoint Document Library

K2 SmartObjects and SharePoint Content Types integration

Content Types can be defined as a collection of meta data fields. To learn more about how Content Types work see Microsoft's documentation on Content Types <http://office.microsoft.com/en-us/sharepointtechnology/HA101215701033.aspx>.

When Content Types are enabled on a List , and SmartObjects are created in SharePoint a SmartObject will be created for each Content Type in that SharePoint List. If a Content Type is therefore deleted the other Content Types and SmartObjects will continue to function. The SmartObject for that specific Content Type will however not function any more.

When Content Types are not enabled on a List at the time of creating a SmartObject only one SmartObject will be created for that SharePoint List. If Content Types should be enabled at a later stage this SmartObject will no longer function and the SmartObjects will have to be recreated or refreshed for this SharePoint List.

1.6.8.1.5.2.3 Configure SmartObject Access

K2 Designer for SharePoint - Configure SmartObject Access

Configuring which SmartObjects and which methods are surfaced in the K2 Designer for SharePoint is an important administrative step. This occurs at the SharePoint Site Collection level, meaning that if multiple Site Collections exist in an enterprise, only those Site Collections that have configured SmartObject methods will be able to use them and the actual available SmartObject methods will be different per Site Collection.

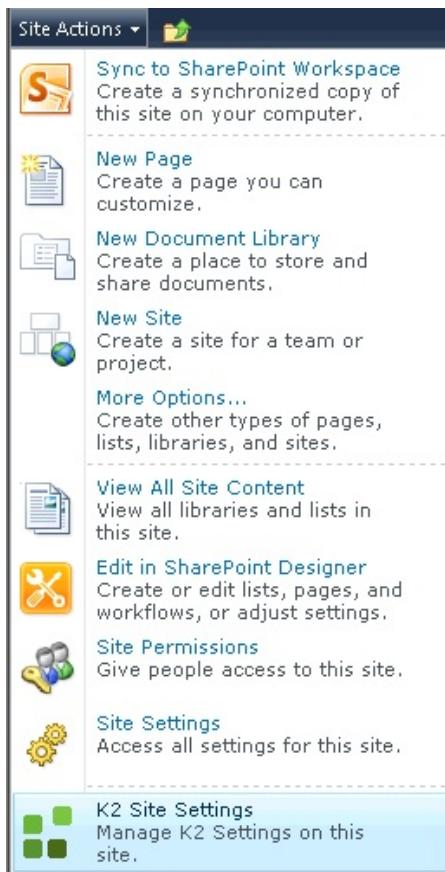


The individual configuring the SmartObject in SharePoint must be a SharePoint Site Collection Administrator to be able to perform the configuration

SmartObjects generated from SharePoint or created in K2 Designer for Visual Studio or K2 Studio can be used in the K2 Designer for SharePoint. To enable this feature, the SmartObjects have to be configured on the SharePoint site.

Perform the following steps to make the SmartObjects available on the SharePoint site:

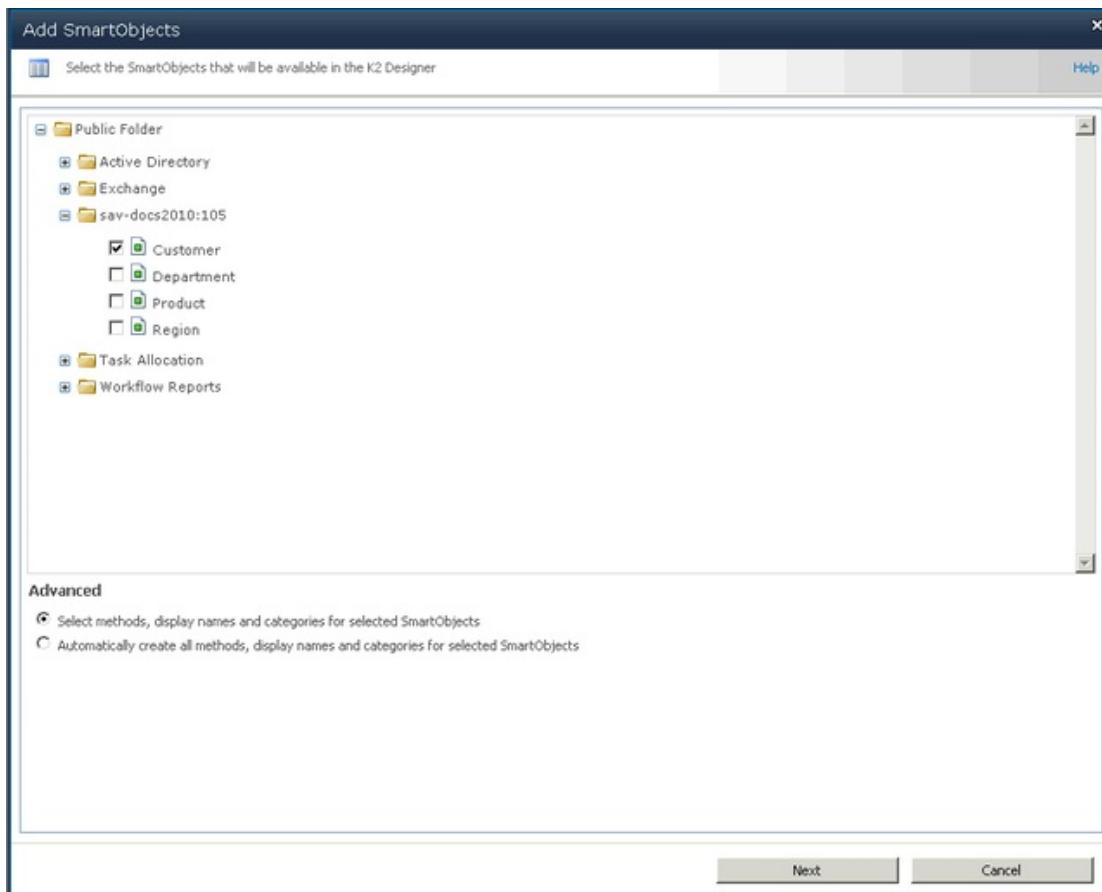
1. Open the relevant SharePoint site.
2. Click on the drop-down arrow on Site Actions
3. Click K2 Site Settings



4. Select Configure SmartObject Access from the K2 Designer for SharePoint Management section.

The screenshot shows the 'Site Settings' page in a browser. The left navigation bar includes links for Libraries, Site Pages, Shared Documents, Lists, Discussions, Recycle Bin, and All Site Content. The main content area has sections for General, SmartObject Management, and K2 Designer for SharePoint Management. Under K2 Designer for SharePoint Management, there are links for K2 Designer for SharePoint Configuration, Set Restricted Wizards, and Configure SmartObject Access. The 'Configure SmartObject Access' link is highlighted with a red circle.

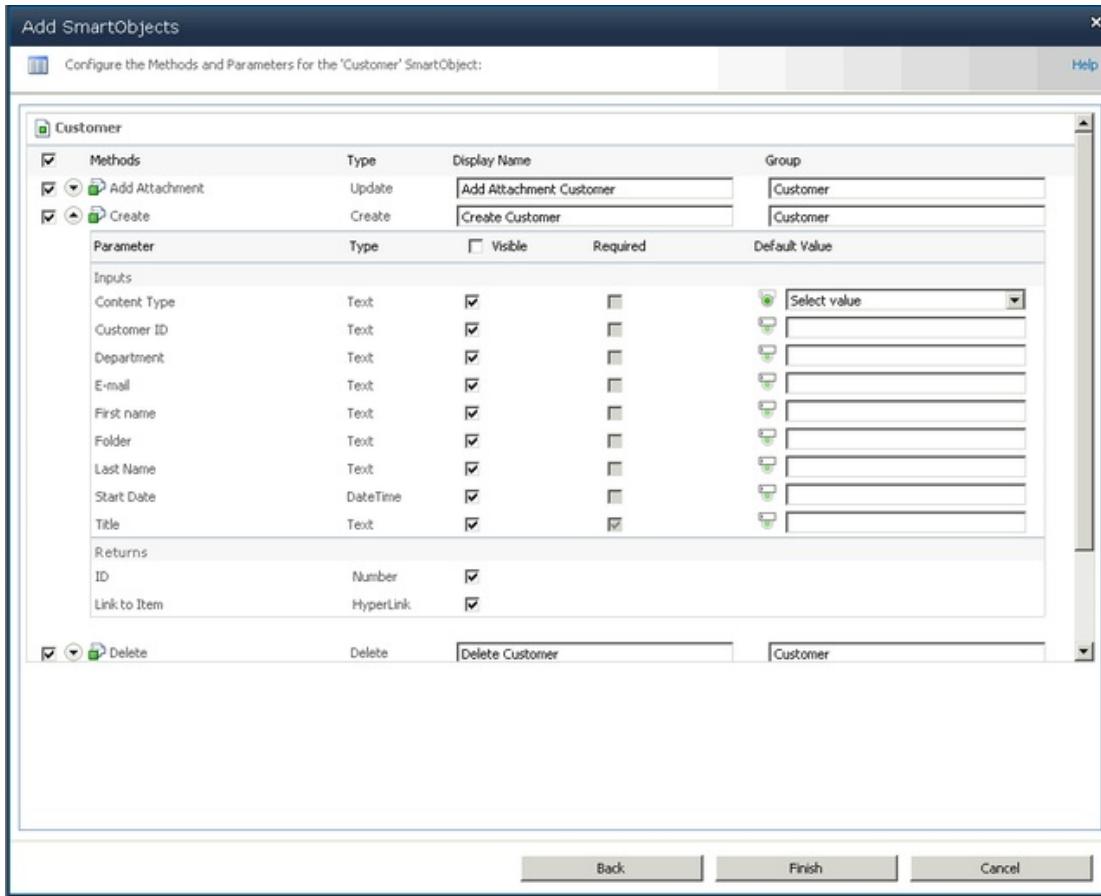
5. Click **Add new item** on the SmartObject Access screen.
6. Expand the SharePoint site folder and select the SmartObject that should be made available in the K2 Designer for SharePoint.



Advanced	Description
Select methods, display names and categories for selected SmartObjects	This option enables the user to configure the specific SmartObject and decide what should be available in K2 Designer for SharePoint
Automatically create all methods, display names and	This option automatically performs the configuration using defaults.

categories for selected SmartObjects

- Click Next to display the configuration options.



Advanced	Description
Methods	Select which methods should be made available in the K2 Designer for SharePoint
	Click on this icon to expand the method and display the SmartObject properties and parameters
Display Name	Displays the default Display Name. Type another Name to change this
Group	Displays the default Group. Type another Group to change this
Visible	If the property/parameter is ticked, it will be visible to the user in the K2 Designer for SharePoint
Required	Indicates whether the property/parameter is a required field
Default Value	Click on the icon next to the Default value text box to change between the input box and the environment field dropdown

- Configure the methods and click Finish. The SmartObjects available for configuration in the K2 Designer for SharePoint are listed

The screenshot shows the 'SmartObjects Access' page in MOSS. The left navigation bar includes 'Home', 'Production', 'Libraries' (with 'FormLib1', 'DocLib2', 'DocLib1'), 'Lists' (with 'Customer', 'Department', 'Region', 'Product'), 'Discussions' (with 'Team Discussion'), and links to 'Recycle Bin' and 'All Site Content'. The main content area is titled 'MOSS > SmartObjects Access' with the sub-instruction 'Select the SmartObjects that will be available in the K2 Designer'. It lists 'SmartObject' items: 'Customer' (Methods: 7) and 'DocLib1' (Methods: 10). A blue callout box points to the 'DocLib1' item.

To edit or delete a SmartObject, click on the SmartObject. Select the option from the drop down menu. Deleting the SmartObject from this list will result in the SmartObject methods not being available in the K2 Designer for SharePoint. This will have no impact on processes already using these methods as it is only the link between the SmartObject and the K2 Designer for SharePoint that is deleted. If configured again, the methods will be available again for use in the K2 Designer for SharePoint.

This screenshot is identical to the one above, but the 'DocLib1' SmartObject is now highlighted with a yellow selection bar. A context menu is open over the 'DocLib1' item, showing two options: 'Edit item' (with a pencil icon) and 'Delete Item' (with a red X icon).

1.6.8.1.5.2.4 Import and Export SQL and CRM SmartObjects

CRM and SQL Smart Object Export | Import

The CRM and SQL Export | Import SmartObject Import feature enables users to import SmartObject definitions which were created from a similar K2 for SharePoint source. The feature is especially useful when moving processes and their respective dependencies i.e. SmartObjects, between environments. A common example of this would be moving SmartObjects from a development environment across to a similar production environment where the SmartObjects would need to persist as a dependency. The feature can also be used to synchronize existing deployed SmartObjects with a new definition template.

During the process development cycle, K2 SharePoint SmartObjects are created using a SQL Server's Databases or CRM Servers Entities. These items, exposed as SmartObjects are used in the development of processes within a development environment. When the SmartObjects are migrated, the SQL or CRM Export feature acts as the export vehicle to move the SmartObject definitions from the existing server to the new server.



When performing the export, for SQL the databases must be exported with the *.XML file as well

Why use this feature?

When a SmartObject is created for example in the , a GUID is assigned to the SmartObject; this is used to uniquely identify the SmartObject. If another SmartObject is created in an adjacent environment with the same name, the GUID will not be the same. Processes deployed from a development environment to the production environment will not be able to locate the SmartObjects that they need even if the names are the same, the GUIDs are not.

The export SmartObject feature ensures that when the SmartObject definition is imported into the target environment, the definition will be used to recreate the definition as exact copies. The deployed processes will be able to identify them owing to the duplicated GUID and proceed as per normal.

1.6.8.1.5.2.4.1 Export Import Pre-requisites and Preparation

Export the SmartObject

Exporting SmartObjects requires that there are existing connections with either a SQL server or a CRM Server and that SmartObjects have already been deployed based on those connections. The export process exports only the following items:

- Service Type Guide
- Service Guide
- Service Name
- Configuration Settings
 - SQL
 - SQL server Name
 - SQL Server Database Name
 - CRM
 - CRM Server URL
 - Organizations Name



Exporting the SmartObject may require that source backend resources for example SQL Database must be backed up and exported to the destination SQL server in the new environment.

Export Permissions and Rights

Exporting and importing SQL and CRM SmartObjects requires access to SharePoint central administration as well as Administrator level access to both the SQL and CRM servers.

Import the SmartObject

Importing the SmartObjects into the target environment will require Administrator access to both the SQL Server and CRM Server. The individual performing the import process, must also be familiar with editing XML files and be able to make changes to XML tags to enter alternative values where required. Access to SharePoint Central Admin is mandatory to facilitate the process.

Considerations for SQL SmartObject Import

The databases on the source system must be backed up and moved to the destination system. If an update is being performed to a previous import or if the databases on the target system were created manually the net result being that the database structure is different to what is expected by the XML file being imported the import process will be stopped by the system.

Considerations for CRM SmartObject Import

The organization name on the destination system must be the same as what is defined in the XML file being imported. If there are discrepancies between what is expected by the XML file and the destination system ie expected entities not found on the destination system, this will not prohibit the import process.

1.6.8.1.5.2.4.2 SmartObject Import Export Troubleshooting

SmartObject Import and Export Troubleshooting

The expectation is that the export and import processes will take place on two different machines. Owing to this, there may and will always be differences between the two environments which can result in the import process from completing successfully.

Import Checklist

The following items should be verified to ensure that the checking takes place as smoothly as possible:

Resource	SQL Server	CRM Server	Check
Servers	SQL Server name must be the server of the target environment	CRM Server must be the URL of the target environment and the organization name found in the XML file must be the same as the target environment	
Repository	The SQL Databases must be backed up from the source SQL Server and restored to the target SQL server *	The same entities must be available on the target CRM Server.	
Service Instances	If the SQL Server versions are not the same, but they are forwards compatible, this may result in the error that the service instance is not found. This is however a result of differences with the XML file output.		
Credentials	SmartObjects exported with the Specified User credentials entered will need to do the following: <ul style="list-style-type: none"> • For a first time import and service instance creation, the specified user credentials must be re-entered by editing the connection • For an upgrade, the password is removed from the display field but the user name remains. The password must be updated later 		

*Standard SQL backup and restore compatibility procedures and protocol apply

Service Instance Import Errors

The following error may be encountered and this happens for a number of reasons: **Unable to create a new ServiceInstance as one already exists with the same name**

Listed below are a number of example scenarios where the above error is known to occur. The error is not limited to these scenarios. When importing a service instance and the error occurs, consider the following:

1. An existing serviceinstance of the same type (SQL/CRM) with the same compared config exists. (Matching)
 - a. Existing serviceinstance will be updated. Only the GUID is updated with the imported value
2. An existing serviceinstance of the same type (SQL/CRM) with the same compared config does not exist
 - a. Check if serviceinstance name to be imported is unique
 - a. Yes – Create new serviceinstance
 - b. No – Give an error that the name already exists
3. If credentials were specified for the SmartObject, and later the SmartObject is updated. The update procedure removes the password, and this must be updated again manually



Sensitive information ie domain credentials are not exported as part of the XML based configuration file. These values must be entered manually once the import process is complete and the service instance has been created. This applies to both SQL and CR SmartObjects.

SQL Server Compatibility

When backing up and restoring databases between a source and a destination environment the source environment must either be the same version of SQL Server or a more recent version. If the destination environment's SQL Server

version is older than the source environment, the databases will not be able to be restored and subsequently the SmartObject import will not be possible either.

If the error: **Unable to create a new ServiceInstance as one already exists with the same name**, occurs it may be that the XML output of the file is in an order that the import Server does not recognizes or there are differences. This is a result of differences between SQL Server versions. To resolve this, the compare flag in the configuration file can be set to false to prevent comparisons from taking place which will result in the existing SmartObjects being overwritten.

1.6.8.1.5.2.4.2.1 SQL | CRM SmartObject Import & Export Troubleshooting

SQL | CRM SmartObjects Import & Export

Database Security Mappings and Permissions



Security Mappings and Permissions on the source environment must be mirrored on the target environment.

When Restoring a Database on the target SQL Server, Security > User Mappings> DB Owner rights need to be added for the following users.

1. K2Hostserver Service Account
2. Application Pool Account User

If the correct user rights are not added the following error will be encountered:

Updating server...
Deserializing from XML...
Validate mappings...
Updating Service Instance...

Error importing SmartObject settings:
A connection was successfully established with the server, but could not connect to the database supplied or database could not be found.

Specified Users

SmartObjects that have been configured to use a specified set of credentials, must have those credentials manually validated after an update. Every time a SmartObject is updated using the import function, the specified user's credentials are overwritten. The user name is retained, but the password is removed from the database and must be re-entered. If the password is not re-entered, at run time errors will surface when the Service attempts to access the database or CRM server using the specified user account.



Owing to the security risk, specified credentials ie user name and password are not included in the configuration for travel between the source and target systems.

When the existing SQL or CRM SmartObject service instance is configured to use credentials of the specified user the password is originally encrypted and stored within the database. However, when an update is performed and an update is simply re-importing a new or the original version of the configuration file, the password is not retained and is cleared from the database. The user name is however retained.

SQL SmartObject	CRM SmartObject
<p>Authentication:</p> <p><input type="radio"/> Impersonate the User Account</p> <p><input type="radio"/> Use the K2 Server Service Account</p> <p><input checked="" type="radio"/> Use the specified SQL Account</p> <p>Login:</p> <p><input type="text" value="SA"/></p> <p>Password:</p> <p><input type="password" value="*****"/></p> <p>Authentication:</p> <p><input type="radio"/> Use the current User Account</p> <p><input type="radio"/> Use the K2 Server Service Account</p> <p><input checked="" type="radio"/> Use the specified SQL Account</p> <p>Login:</p> <p><input type="text" value="SA"/></p> <p>Password:</p> <p><input type="password" value="*****"/></p>	<p>Authentication</p> <p><input type="radio"/> Impersonate the User Account</p> <p><input type="radio"/> Use the K2 Server Service Account</p> <p><input checked="" type="radio"/> Use the specified Windows Account</p> <p>User Name (e.g. domain\user):</p> <p><input type="text" value="vmqa\Administrator"/></p> <p>Password:</p> <p><input type="password" value="*****"/></p> <p>Authentication</p> <p><input type="radio"/> Use the current User Account</p> <p><input type="radio"/> Use the K2 Server Service Account</p> <p><input checked="" type="radio"/> Use the specified Windows Account</p> <p>User Name (e.g. domain\user):</p> <p><input type="text" value="vmqa\Administrator"/></p> <p>Password:</p> <p><input type="password" value="*****"/></p>

Errors that may be encountered are shown below, but may not be isolated to these few examples.



If "Specified Credentials" are configured, then the passwords must be re-entered once an update has taken place.

K2Project1 \CRM SMO Test	12/1/2011 3:13 PM	Get	Owner	Message: The request failed with HTTP status 401: Unauthorized.; ServiceName: MSKristofCRM; ServiceGuid: 5d5ccd28-a381-4f4d- b9d6-fbd23290b82b; InnerExceptionMessage: ;
K2Project2 \Manage SQL Process	12/1/2011 5:13 PM	CREATE		Message: Login failed for user 'SA'; ServiceName: KristofDB1; ServiceGuid: 19cef6fe- bc0c-4e8f-bbe1-ac48091dad2d; InnerExceptionMessage: ;

1.6.8.1.5.3 Configure Synchronization

SharePoint SmartObject Configuration Synchronization

When switching between environments, it is important to keep the SharePoint SmartObject configuration in sync. Certain SmartObjects contain GUID's and association mappings which should stay in sync between the environments to ensure a stable environment.

SharePoint SmartObject configuration can be exported from one environment and imported into another.

Important Considerations

It is important to note the following with regard to synchronization of SharePoint SmartObjects between environments:

- A Service Instance is created per site (not per site collection) when SmartObjects are created via the [SmartObject Service Management](#) link.
- SharePoint Lists and Libraries should be identical on the target environment to enable successful synchronization. If the export is done from a SharePoint Library called Timesheets, the exact same Library should exist in the target environment. The SmartObjects for that specific Library will be synchronized. If the SharePoint Lists and Libraries are not exactly the same on the target environment for the site you wish to synchronize the SmartObjects, the SmartObjects will not be created.
- SmartObjects do not have to exist on the target environment in order to be created. But the SharePoint List or Library and the columns within that List or Library must be the same and have the same data types as the source SharePoint List or Library in order to be imported.

1.6.8.1.5.3.1 SharePoint SmartObject Configuration Export

Export SmartObjects Configuration

The Export SmartObjects Configuration feature can be found by navigating to the K2 Site Settings page (in the Site Actions dropdown) and clicking on the Export SmartObjects Configuration link.

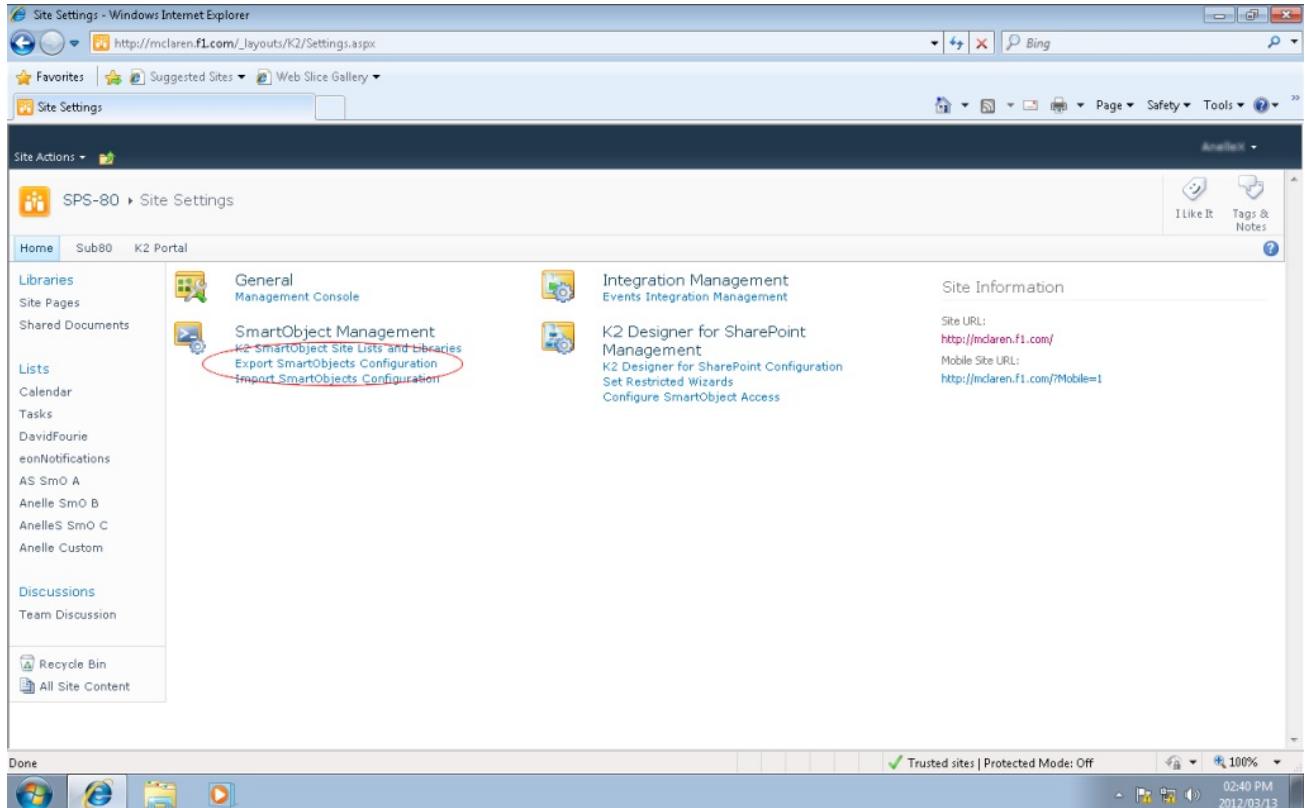


Fig. 1. Export SmartObjects Configuration

The following screen will open:

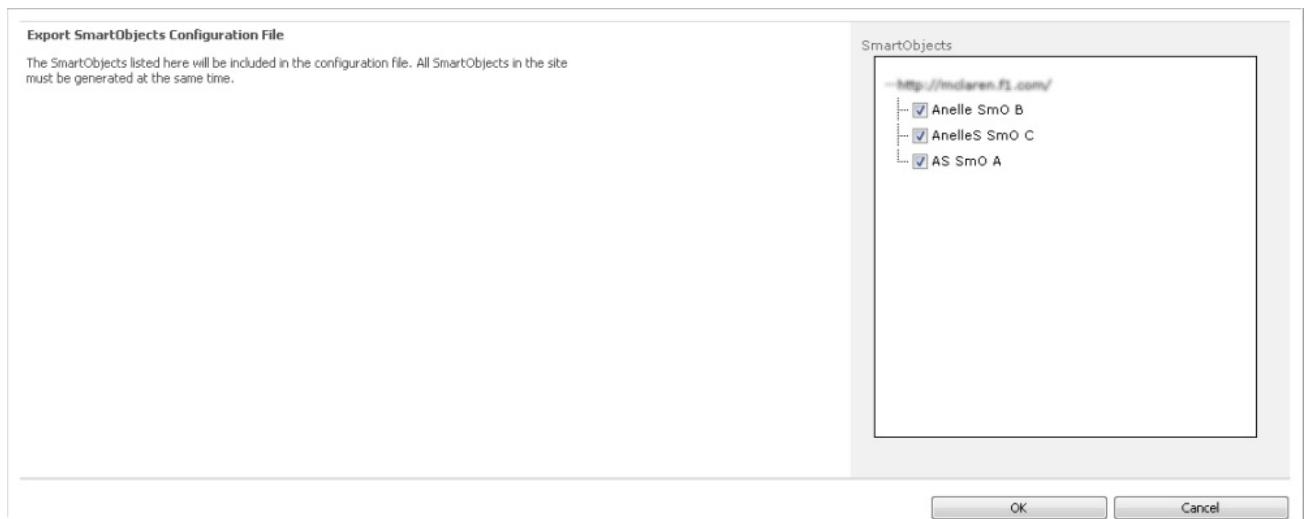


Fig. 2. Export screen

All the SmartObjects for the current site collection are listed. This list does **NOT** include the SmartObjects for sub sites. Should you wish to export SmartObjects from sub sites, the same operation will have to be performed on those sub sites directly. The list of SmartObjects displayed is the same as the list of checked items found under the SmartObject Service Management link.

Select the SmartObjects you wish to export and click OK.

The File Download screen is displayed. Specify a location to Save the Config.xml to or Open the File.



Fig. 3. File Download screen

The SmartObject Configuration Export Finished screen is displayed:

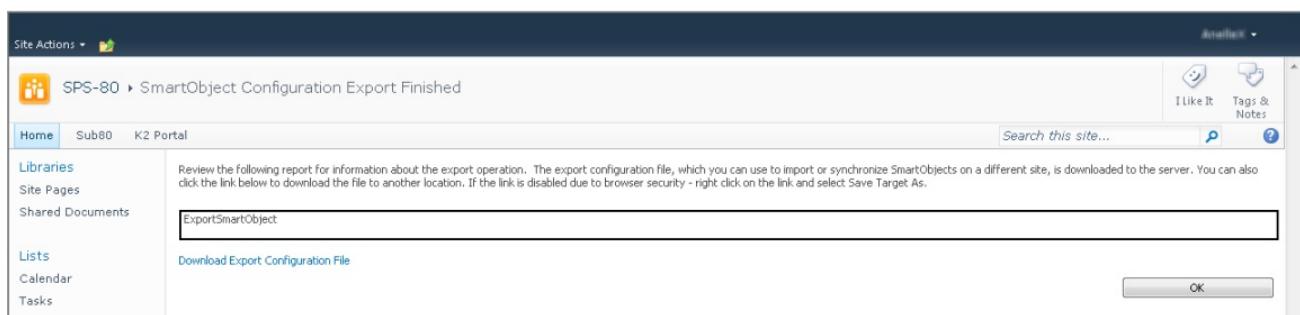


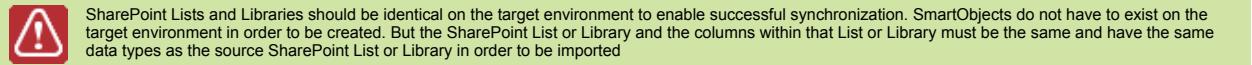
Fig. 4. Export Finished screen

Click on the **Download Export Configuration File** link if you want to download this file. Should you wish to download it later, it can be found in the location you specified upon File Downloading. This file will be used to import the SmartObject Configuration from the current environment to another environment. This would typically be used when creating SmartObjects in a development environment, then moving to a production environment.

1.6.8.1.5.3.2 SharePoint SmartObject Configuration Import

Import SmartObjects Configuration

This feature would typically be used when creating SmartObjects in a development environment, then moving to a production environment. To export the SmartObjects Configuration and generate a file to import on the target environment , see [Export SmartObjects Configuration](#). Save the export file in a location on the environment you wish to import the SmartObjects Configuration.



The Import SmartObjects Configuration feature can be found by navigating to the K2 Site Settings page (found in the Site Actions dropdown) and clicking on the Import SmartObjects Configuration link.

The screenshot shows the SharePoint Site Settings page. In the center, under the 'General Management Console' section, there is a link labeled 'Import SmartObjects Configuration'. This link is circled in red. The page also includes links for 'K2 SmartObject Site Lists and Libraries', 'Export SmartObjects Configuration', and 'Integration Management'.

Fig. 1. Import SmartObjects Configuration

The following screen will open:

The screenshot shows the 'Import SmartObjects Configuration' dialog box. It has a left sidebar with library and list items. The main area contains instructions for importing configuration files, a 'Browse...' button for selecting the XML file, a 'Test Import' button, and 'OK' and 'Cancel' buttons.

Fig. 2. Import screen

Select the import file from the location where you saved it by clicking on the Browse button and navigating to the specific location. A Test Import button is available if you want to test the import first. Click **Test Import**.

The SmartObject Configuration Import Test Results page is displayed where you can review the information of the import that is about to take place. Click Back and then OK on the Import SmartObjects Configuration screen to continue with the Import.

The screenshot shows the 'Import SmartObjects Configuration' dialog box again. The 'xml file name' field now contains the path 'C:\Users\anelle\Downloads\Config.xml'. The 'Test Import' button is visible below the file selection field.

Fig. 3. Ready to Import

The SmartObject Configuration Import Finished screen is displayed:



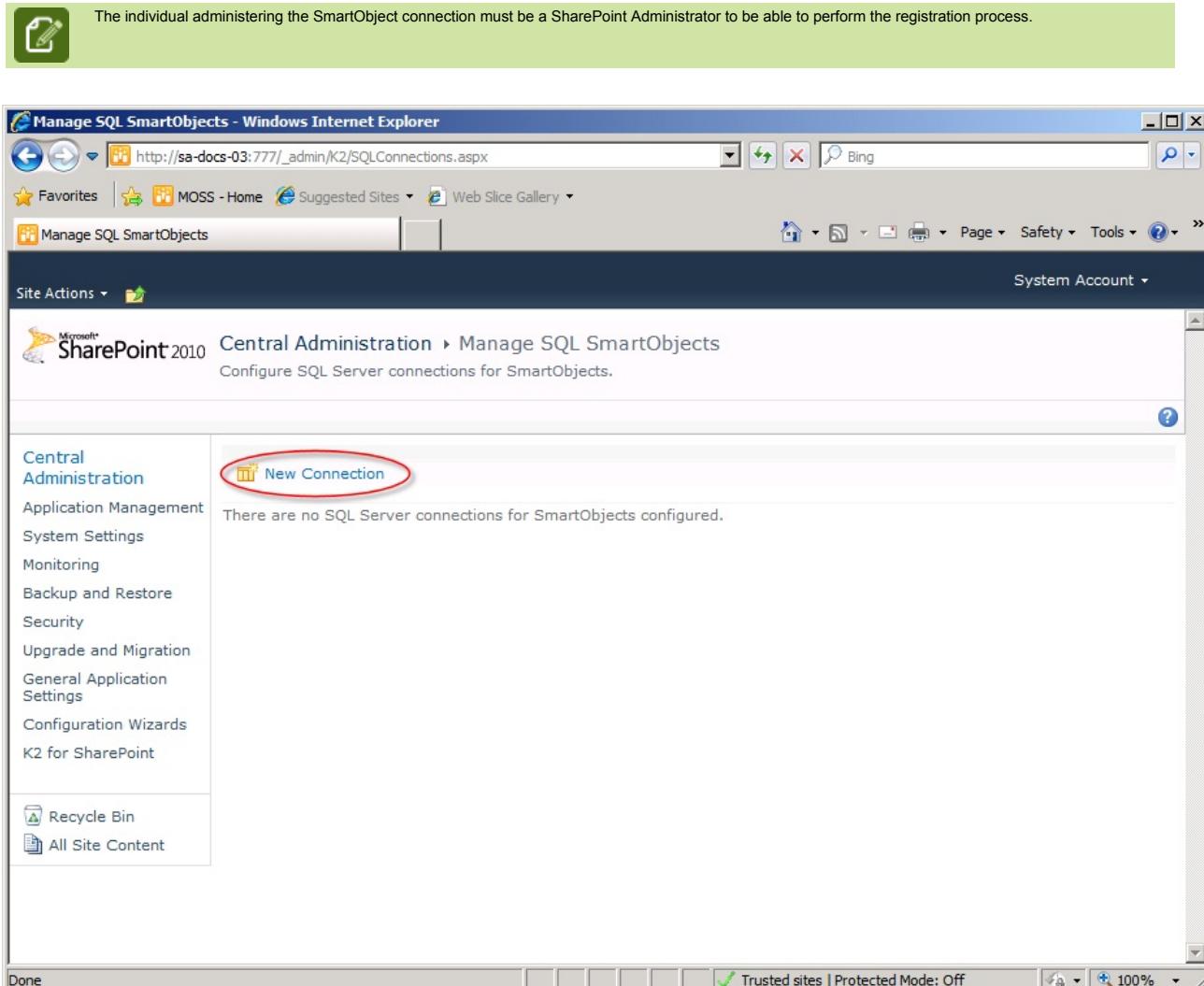
Fig. 4. Import Finish screen

The import of the SmartObjects Configuration has been completed. If SmartObjects already existed in the specific Library or List, it would have been updated. If not, new SmartObjects would have been created.

1.6.8.1.5.4 -using a SQL Server Instance

Manage SQL Connections for SmartObjects

The **Manage SQL Connections** for SmartObjects page lists the existing connections to SQL Server instances and the connections listed below represent a relationship with a SQL Server Instance and the specified database. The SQL Server instances and Databases can be reused for each connection depending on requirements. The connection to the SQL Server instance and the database(s) is configured manually and there is no automated checking or verification as to the continual availability of the SQL Server Instance.



The screenshot shows the 'Manage SQL SmartObjects' page in SharePoint Central Administration. The URL is http://sa-docs-03:777/_admin/K2/SQLConnections.aspx. On the left, the navigation menu includes 'Central Administration', 'Application Management', 'System Settings', 'Monitoring', 'Backup and Restore', 'Security', 'Upgrade and Migration', 'General Application Settings', 'Configuration Wizards', and 'K2 for SharePoint'. Below this is a link to 'Recycle Bin' and 'All Site Content'. The main content area displays the title 'Central Administration > Manage SQL SmartObjects' and the sub-instruction 'Configure SQL Server connections for SmartObjects.' A red circle highlights the 'New Connection' button, which is located next to the text 'There are no SQL Server connections for SmartObjects configured.' At the bottom of the page, there is a status bar showing 'Done' and various browser controls.

Image 1 - SQL Connections for SmartObjects

Item	Description
New	Starts the registration process of a new SmartObject
Refresh	Refreshed the listing of existing registrations
Registration Listing	
Name	This is the display name for the connection
Description	The description is entered during the process of registration

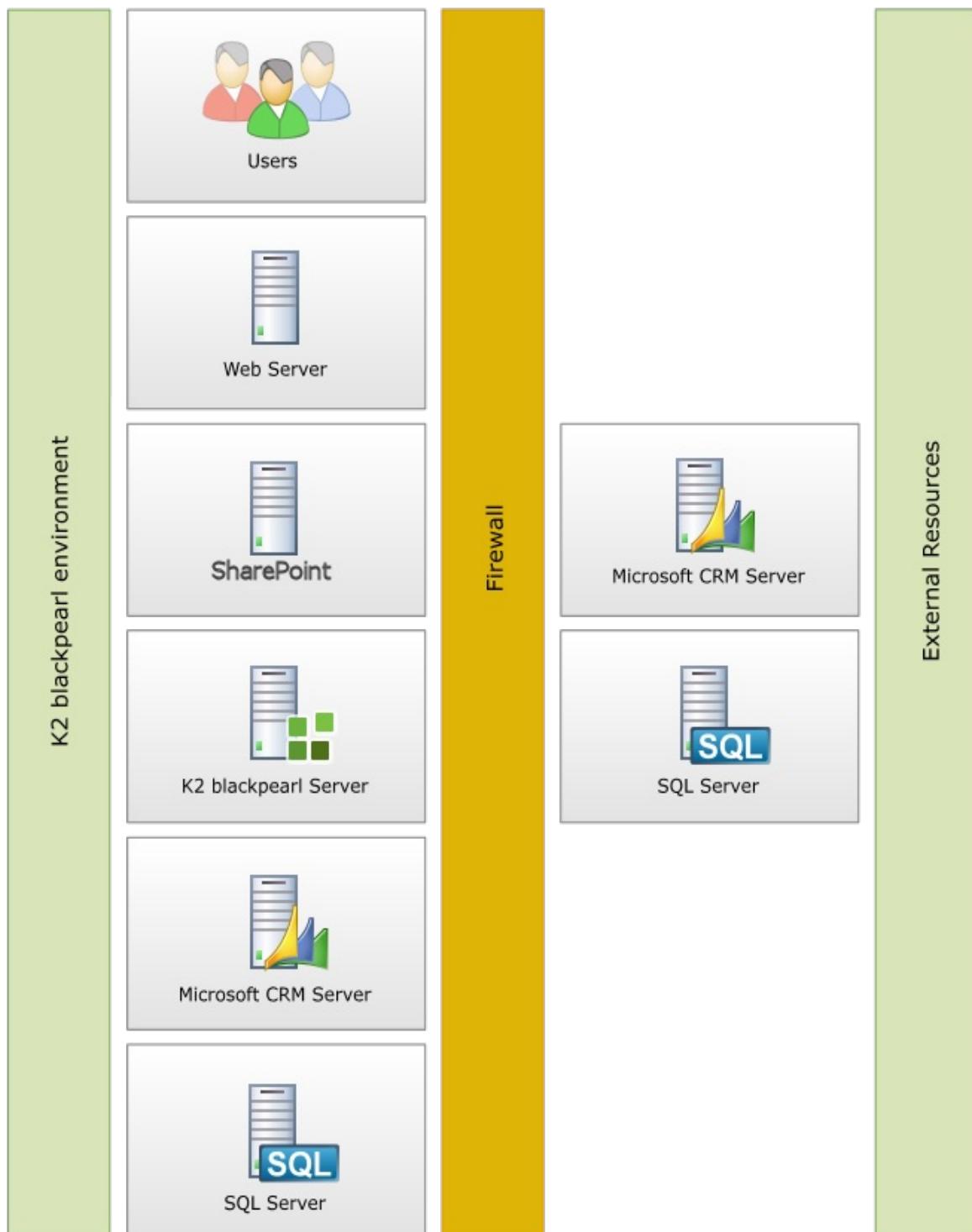
1.6.8.1.5.4.1 Introduction

Introduction

K2 provides the ability to create and manage Service Instances and SmartObjects for SharePoint, SQL Server and CRM via management pages found in SharePoint. SmartObjects in SharePoint are managed at the Site Collection level via the **K2 Site Settings** pages while SQL Server and CRM are managed at the Central Administration level via the **K2 for SharePoint Data Management** pages.

SmartObject Sources

The SmartObjects that are generated within SharePoint can be from an internal resource (SharePoint, SQL Server or CRM) or an external resource (SQL Server or CRM). If the resource is external and the internet connection is protected by a proxy server, the appropriate user rights would be required to access this resource as well. The external source, such as a SQL Server database or CRM organization, provides the underlying objects/entities that will become SmartObjects.



1.6.8.1.5.4.2 Registration Requirements

Registration Requirements

The registration requirements for both types are similar, and both can be performed via the SharePoint Central Administration. The SharePoint Central Administration will surface and display all exposed registered service instances including items that were registered via K2 Workspace.



If the SQL Server Instance is accessed via proxy, the user account used would require permissions to the proxy server as well.

SQL Server Instances

The following requirements must be met for the SQL Server to be used:

- A database and database table must be available
- The Service Account used to create the Service object must have the correct permissions to access the table



The user account may require read / write access to the database > database table depending on the usage requirements.

1.6.8.1.5.4.2.1 User Rights and Permissions



Unless the correct permissions are set in K2 Server and SharePoint, the user will experience errors when attempting the registration process.

User Rights and Permissions

The following user permissions are required to create SQL SharePoint SmartObject.

K2 Product	SQL Server
SQL Server	The user must have access to the SQL Server with permissions to
SharePoint Permissions	As an Administrator, the following rights must be assigned to a User <ul style="list-style-type: none"> ● Site Collections Administrator ● Farm Administrator
Authentication Method	The method chosen to authenticate the user, when the service call is made to K2 SmartObject.

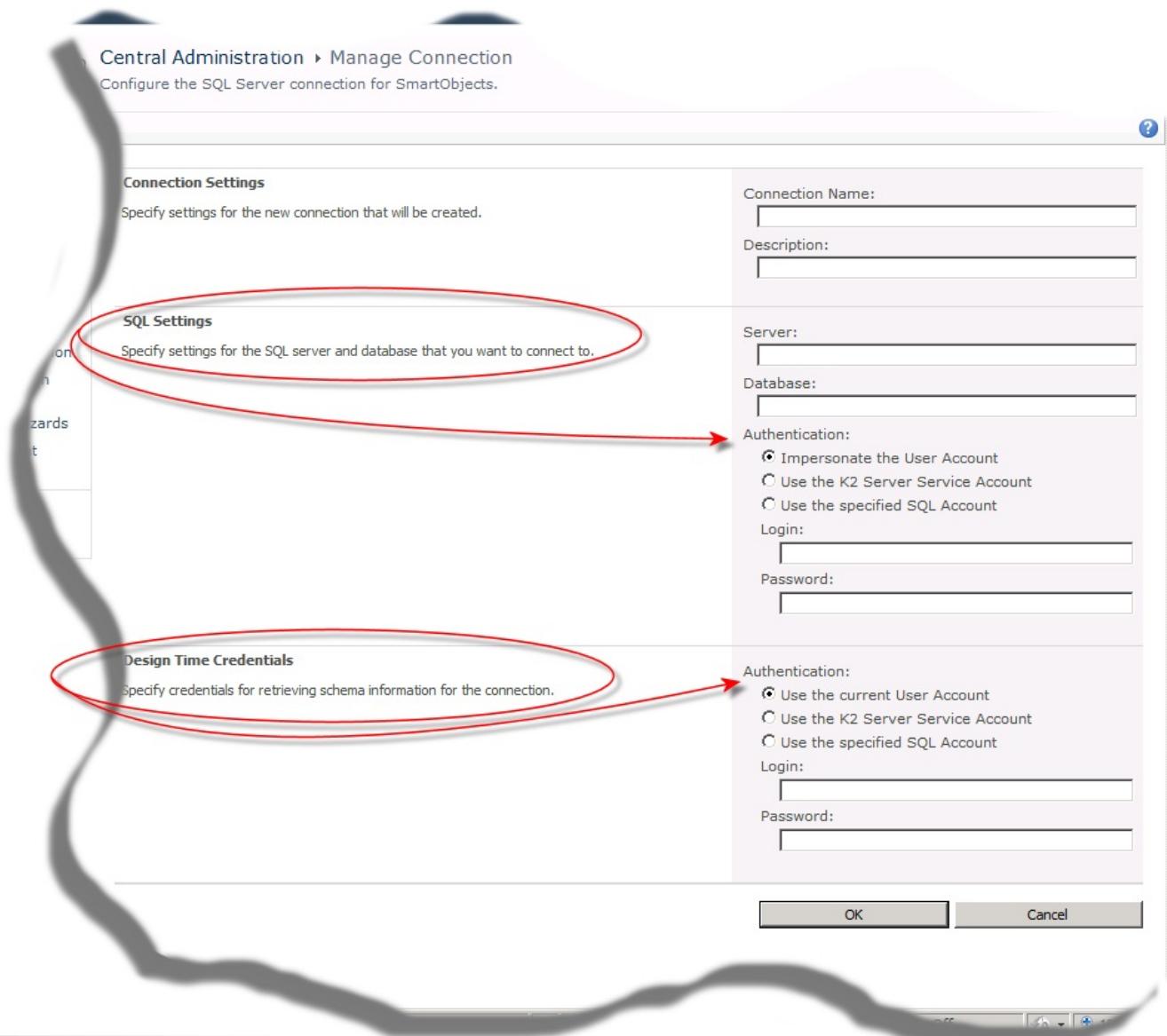
1.6.8.1.5.4.2.1.1 Authentication Method

Authentication Method

The user, when configuring the SQL Service SmartObject connection must specify an authentication method for two scenarios where credentials would be required. The first instance is where the K2 Server Account or User is accessing the SQL Smart Object at run time. The second instance is where the developer accesses the SQL Server Instance and retrieves the Database schema for use at design time.

For the two instances where the credentials would need to be specified, there are three methods available and each method has different implications with regards to authentication. See in the amended screen shot (click the link), the user is required to provide an authentication option for the following scenarios:

- SQL Settings
- Design Time



The user selects one of the following methods:

- Allow user account impersonation by the K2 Server
- Use the K2 Server Account
- Use the specified account

Authentication Method	Description
Allow user account impersonation by the K2 Server	When the service call is made, the K2 Server will impersonate the user but pass the users credentials.
Use the K2 Service Account	The K2 Service Accounts credentials are used and passed to the SQL Server Instance to authenticate the service call.

Use the Specified Account

When this option is selected, it functions similarly to SQL Authentication. When this option is processed, a SQL Service Instance is created in the K2 Service Broker to manage the service call between the K2 Server and the SQL Server Instance.

1.6.8.1.5.4.2.1.2 Adding a Connection

Adding a Connection

The wizard style configuration within the SharePoint environment makes creating SQL connections easy:

1. Select Parameters
2. Register new service instance
3. Customize SmartObject Parameters
4. Create the Smart Object

Registration Types



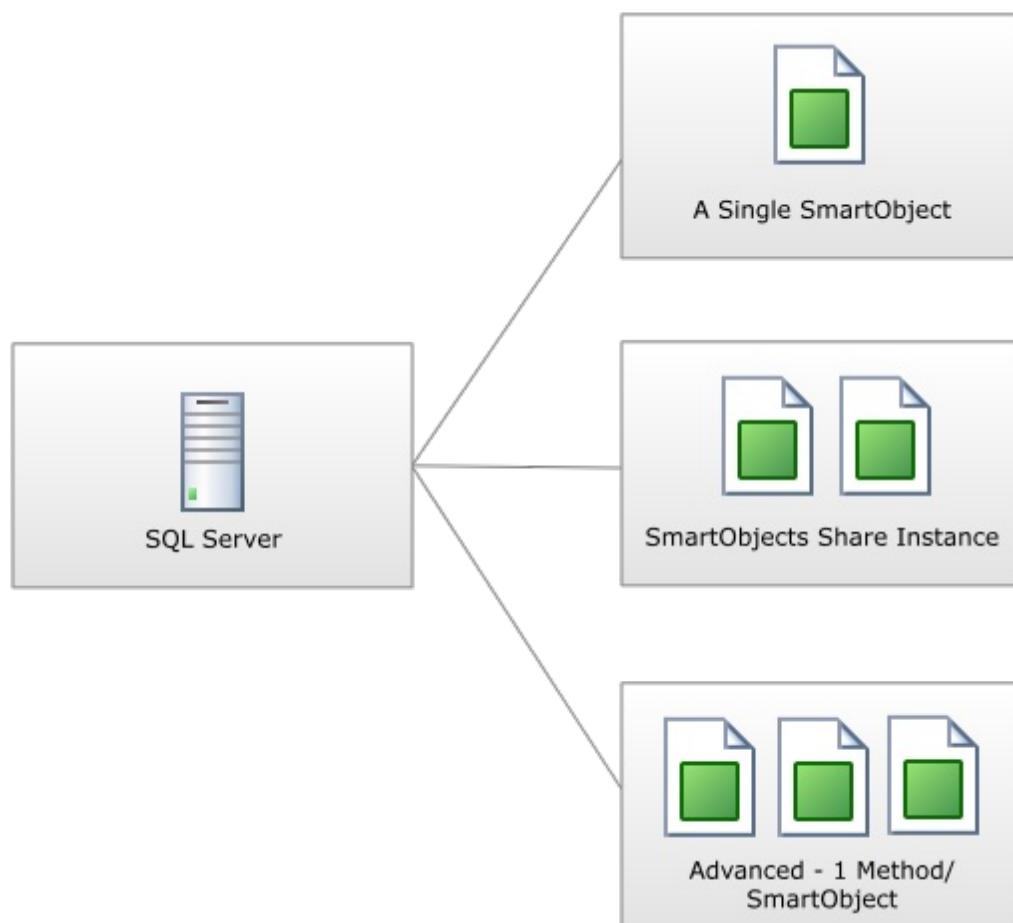
There is a mechanism to DELETE, REMOVE or DEREGISTER a service instance once it has been created. However, doing so may and can result in system errors which may be unrecoverable.

When registering the service instance, the eventual aim is to create a SmartObject. The SmartObject contains methods and the methods require configuration. When configuring the SmartObject, the SharePoint SmartObjects web page creates the SmartObject and the properties and methods; no custom SmartObject creation is possible.

The following types can be created

The types listed below are the principle types that can be created using a single service instance to create the SmartObject

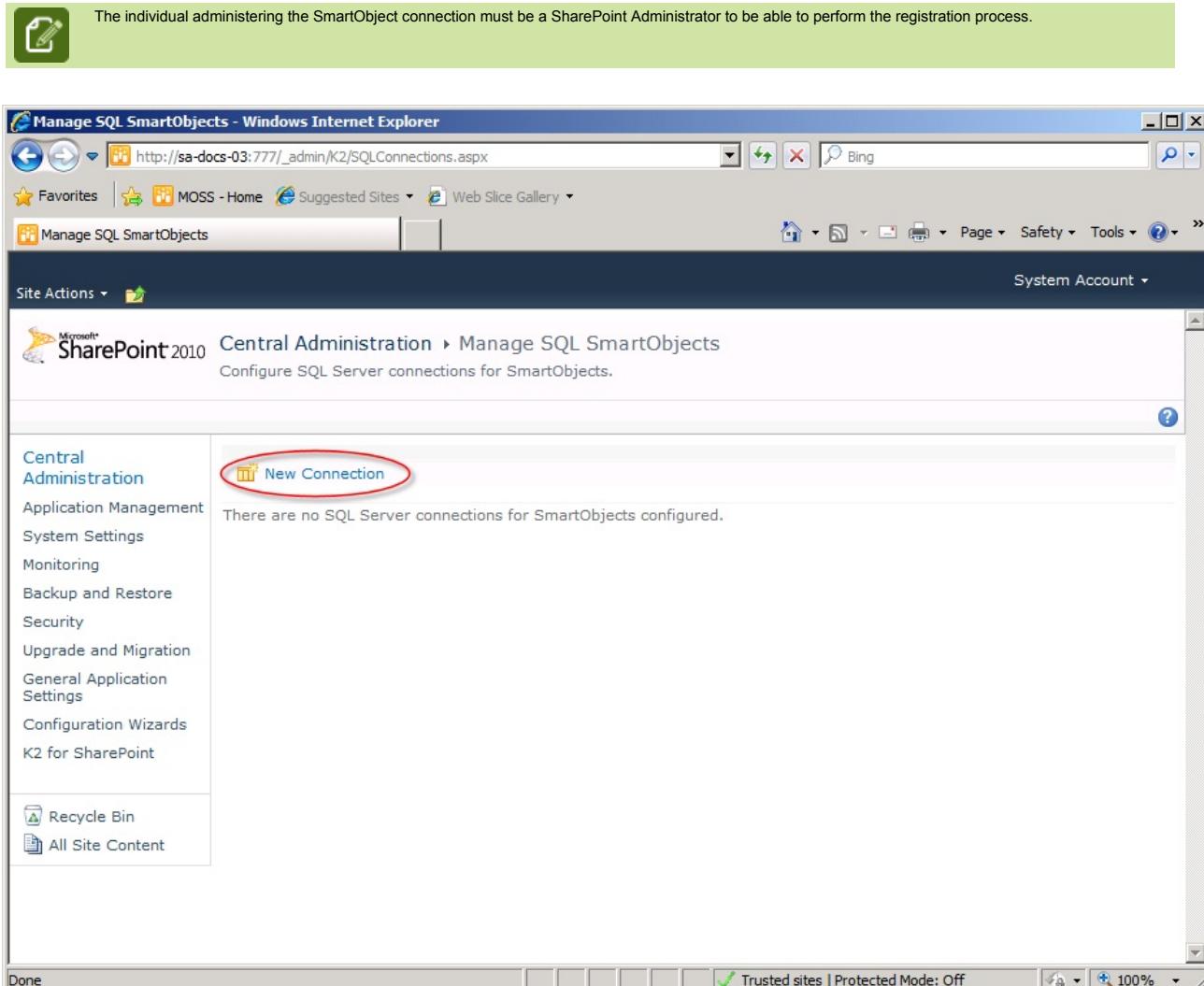
- 1 Service Instance per K2 SmartObject
- Shared Service Instance creating multiple SmartObjects
- 1 Method per SmartObject (this option is a subset of the above option, advanced functionality performs part of the process for the user)



1.6.8.1.5.4.2.2 -using a SQL Server Instance

Manage SQL Connections for SmartObjects

The **Manage SQL Connections** for SmartObjects page lists the existing connections to SQL Server instances and the connections listed below represent a relationship with a SQL Server Instance and the specified database. The SQL Server instances and Databases can be reused for each connection depending on requirements. The connection to the SQL Server instance and the database(s) is configured manually and there is no automated checking or verification as to the continual availability of the SQL Server Instance.



The screenshot shows the 'Manage SQL SmartObjects' page in a Windows Internet Explorer browser. The URL is http://sa-docs-03:777/_admin/K2/SQLConnections.aspx. The page title is 'Manage SQL SmartObjects'. On the left, there's a navigation menu for 'Central Administration' with links like Application Management, System Settings, Monitoring, etc. The main content area says 'There are no SQL Server connections for SmartObjects configured.' A blue button labeled 'New Connection' is highlighted with a red oval. At the bottom, there's a status bar with 'Trusted sites | Protected Mode: Off' and a zoom level of '100%'.

Image 1 - SQL Connections for SmartObjects

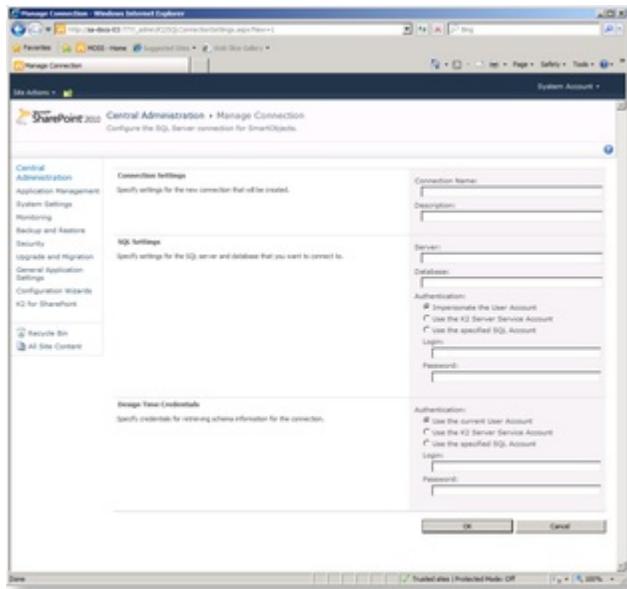
Item	Description
New	Starts the registration process of a new SmartObject
Refresh	Refreshed the listing of existing registrations
Registration Listing	
Name	This is the display name for the connection
Description	The description is entered during the process of registration

1.6.8.1.5.4.2.3 SQL Connection Settings

SQL Connection Settings for SharePoint 2010

The connection settings to create a connection to a SQL Server and the respective database are entered using the page below. The user is required to provide the following details:

- A name for the connection, which will be displayed in the connection listing ie the previous page
- The name and location of the SQL Server
- The Authentication method must also be specified along with credentials, if required



Connection Settings	
Connection Name	Display name for the SharePoint SQL SmartObject Connection
Description	Text description that will accompany the Name of the SharePoint SQL SmartObject connection
SQL Settings	
Server	Enter the name of the SQL Server Instance or the location of the SQL Server
Database	Enter the name of the database hosted by the SQL Server identified in the above field
Authentication Method	Depending on the source used for the SQL SmartObject the Authentication method can be selected
Design Time Credentials	
Authentication Method	The design time credentials refer to the same SQL Server instance listed under SQL Settings. This set of credentials however, are intended to provide the developer with greater access to the SQL Database ie to extract the XML Schema for example.



Windows Authentication requires that the user account has the required permissions

What to do ?

This step requires the user to enter the connection settings for the SQL Server.



Enter a name for the SQL connection and a description for it



Enter the name of the SQL Server and the name of the Database



Ensure that the Database contains data when the connection is created.



Select the Authentication Method for SQL Settings, specify credentials if necessary ie when "**Use the specified SQL Account**" has been selected.



Select the Authentication Method for **Design Time Credentials**, specify credentials if necessary ie when "**Use the specified SQL Account**" has been selected



Click **Ok**

1.6.8.1.5.4.2.4 SQL SmartObject Method Creation

SQL SmartObjects Method Creation

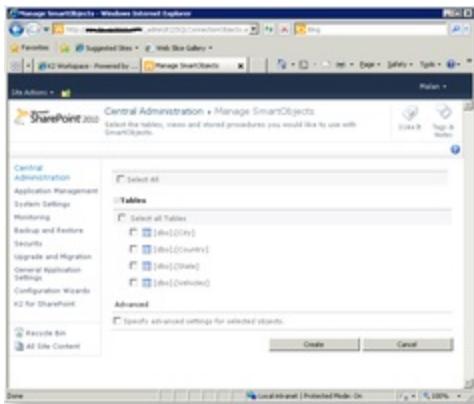
Once the connection settings have been entered correctly, the user page is able to access the database's tables and stored procedures. These items are displayed on page and the user selects which items they require to create a SharePoint SmartObject.

When the **Create** button is clicked the following will take place

- Each item selected will have a separate SmartObject created for it
- Stored Procedures
 - Stored procedures that require input parameters to run will be created as SmartObjects with that dependency
- Tables
 - Each selected table is created as an independent SmartObject
 - Each SmartObject will contain a (one) GetList() method
 - If tables are related to each other using foreign keys, a SmartObject association will be created automatically maintaining the association



The actual items listed may vary depending on the contents of the database and not all options may be listed in the image below.



Tables and Stored Procedures	
Select All	If all items are to be used enable this option
Stored Procedures	Each listed stored procedure receives an option to enable it for use when creating the SmartObject. Only required items should be enabled
Tables	Each Table within the database
Advanced	
Specify Advanced...	Enable this setting to configure advanced options of the SmartObject Methods at later stage

What to Do ?

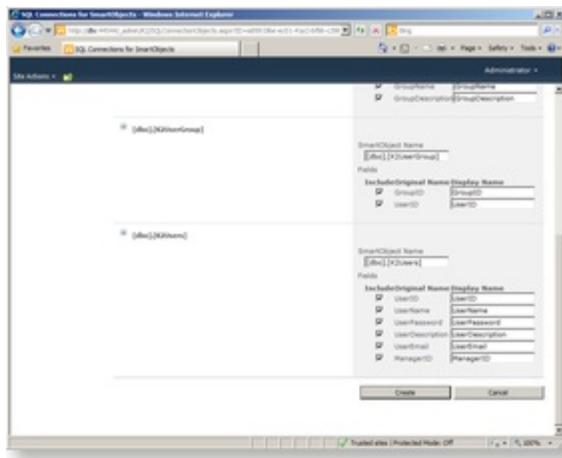
- | | |
|--|---|
| 

Optional Step | <p>Select to use all SmartObject Methods by enabling Select All, or</p> <p>Select only the database table, stored procedure or view that will be used for the SmartObject(s) creation</p> <p>Advanced: Enable the Specify advanced settings for selected objects</p> |
|--|---|

1.6.8.1.5.4.2.5 SQL SmartObject Method Configuration

SmartObject Method Configuration

The methods that were created in the previous step, are configured in this step. Once the configuration is complete the SmartObject will be created.



[dbo].[Title]

SmartObject Name	This name is generated automatically based on the name of the database table. It can be altered by entering a new name	What to Do ?
Fields	The fields are the database columns that reside within the table. The GetList method will retrieve and display the data from the SmartObject according to this layout.	
Include Original Name	The name of the column (field) from the database table, which will surface later visually if this option is enabled	
Display Name	The name of the field that will surface for display	



These steps must be repeated for every SmartObject that will be created.



From the **SmartObject Name** field, retain the existing name or enter a new one



Disable the option to **Include Original Name**, if required or leave as is



From the Display Name field, retain the original naming or enter new custom naming

1.6.8.1.5.4.3 Managing Existing SQL SmartObject Connections (Edit)

Manage Existing SQL SmartObject Connections

The existing SQL SmartObject connections can be managed ie edited by selecting one of the options shown in the drop down below.

Connection Name	Description	Server	Database
1230Vehicles		dbVehicle	sav-fp-sql\k2
SQLServer	SQL Server	dbVehicle	sav-fp-sql\k2

figure 1 - Manage Existing SQL SmartObject Connections

Alterations to SQL Databases



The following content must be implemented if any changes are made to the SQL Database Tables.

When changes are made to the SQL Server Database that has been used or consumed to create a SQL SmartObject, the Administrator must implement the following to ensure that the changes are reflected.

1. The SmartObject Service instance must first be refreshed
2. The SQL SmartObject Connection must be recreated



The procedure above must be followed in order owing to the fact that the SmartObject is created based on the data provided by the Service Instance and not directly from the SQL Database.

1.6.8.1.5.4.3.1 Edit Connection



The feature to change the K2 SQL SmartObject does not return the items that already exist within the K2 SQL SmartObject.

How to Edit an Existing K2 SQL SmartObject Connection

The K2 SQL SmartObject Connection details can be edited from the SharePoint Central Administration page by locating the SmartObject to change and the selecting the option to change the connection.

What to Do ?



These steps must be repeated for every SmartObject that will be created.

- 1
- 2

From **Central Administration > SQL Connections for SmartObjects**, locate the SQL SmartObject to update

Click on the drop down and select the option to **Edit Connection**

Connection Name	Description	Server	Database
1230Vehicles		dbVehicle	sav-fp-sql\k2



When the Edit Connection page loads, select the options required and then select Create.

1.6.8.1.5.4.3.2 Edit SmartObject



The feature to change the K2 SQL SmartObject does not return the items that already exist within the K2 SQL SmartObject.

How to Edit an Existing K2 SQL SmartObject

The K2 SQL SmartObject can be edited from the SharePoint Central Administration page by locating the SmartObject to change and then selecting the option to change the SmartObject.

What to Do ?



These steps must be repeated for every SmartObject that will be created.

①

From **Central Administration > SQL Connections for SmartObjects**, locate the SQL SmartObject to update

Connection Name	Description	Server	Database
1230Vehicles		dbVehicle	sav-fp-sql\nk2
SQLServer	SQL Server	dbVehicle	sav-fp-sql\nk2

②

Click on the drop down and select the option to **Edit SmartObjects**



When the Edit SmartObject page loads, select the options required and then select **Create**.

1.6.8.1.5.4.4 Import and Export SQL SmartObjects

1.6.8.1.5.4.4.1 Import SQL SmartObject

Import SmartObject Definition

The Import SmartObjects option enables the user to select a SmartObject definition and import the definition to create a SQL SmartObject. To start the Import Process, click Import SmartObjects.



The Import SmartObjects contains Testing functionality that will enable the user to verify that the import process will function as expected before they proceed with the process.

①

From **Central Administration > Manage SQL SmartObjects**, select Import SmartObjects.

②

Click browse to locate the XML file. The import processes outcome can be first tested by clicking the **Test Import** button. This feature generates a report to describe the potential outcome.

The screenshot shows the 'Import SmartObjects Configuration' page in SharePoint Central Administration. The left navigation bar includes links like Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Configuration Wizards, and K2 for SharePoint. The main content area has a heading 'Import SmartObjects Configuration File' with instructions about synchronizing unique identifiers between environments. It includes a note about creating SmartObjects if they don't exist and a warning about updating existing ones. A 'Please select xml file name:' input field with a 'Browse...' button is present. Below it is a note about testing the import before modifications. At the bottom are 'OK' and 'Cancel' buttons. The status bar at the bottom shows 'Status: Running'.

③

To proceed, click Ok. A report is generated by the system once the process is complete.

1.6.8.1.5.4.4.2 Export SQL SmartObject

How to export the SmartObject



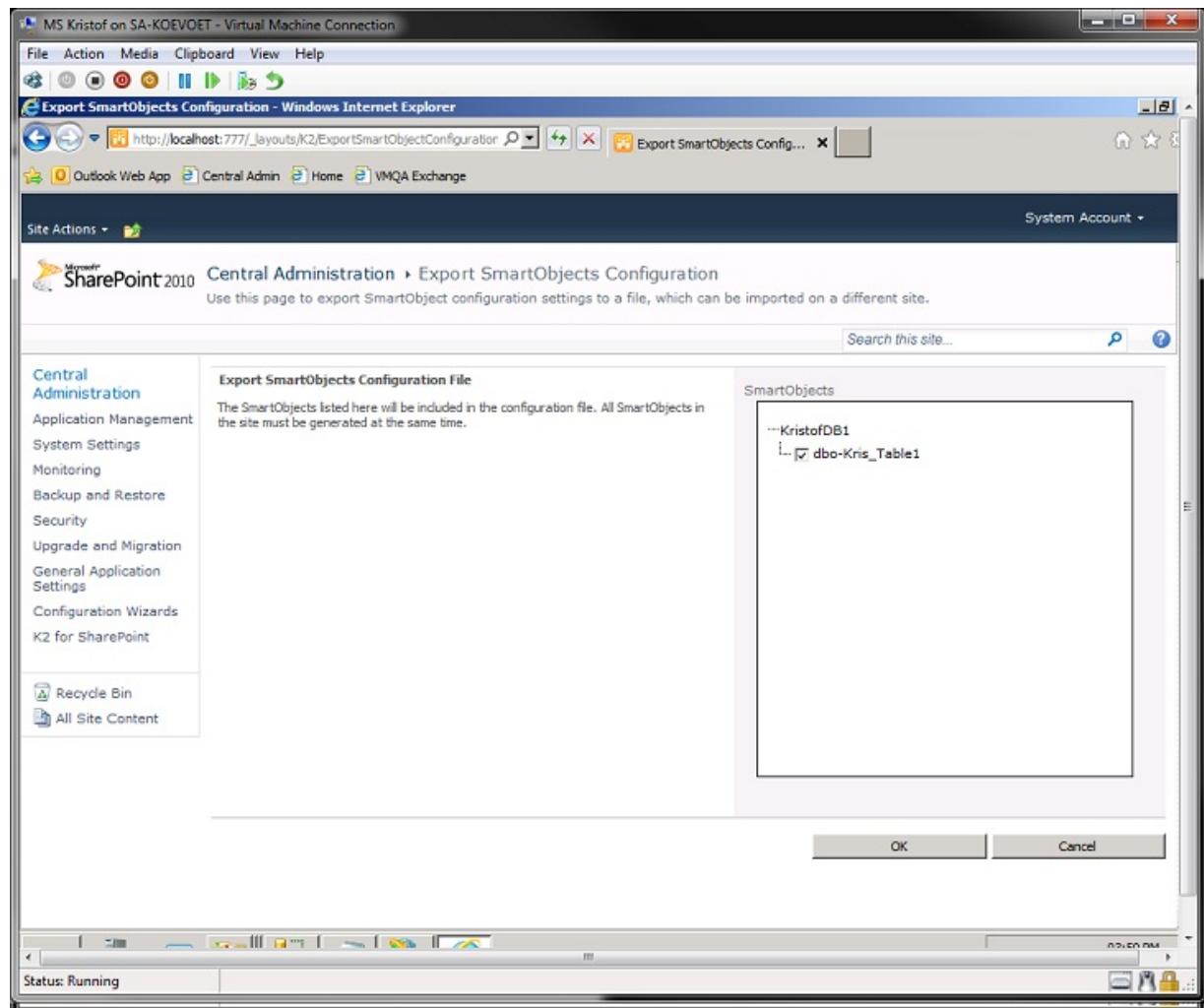
At least one SmartObjects must be present with in the listing below for them to be exported.

- The SmartObjects that are available under the manage SmartObjects page will be listed in the SmartObjects box. The SmartObject is granularized; all items are selected default, and the user is able to manually determine which items they want to export.
- 1 From **Central Administration > Manage SQL SmartObjects**, select a SmartObject to export by left clicking and selecting Export SmartObjects.
 - 2 From the Manage SQL SmartObjects Page, locate the SQL SmartObjec to export and from the drop down list select Export SmartObject

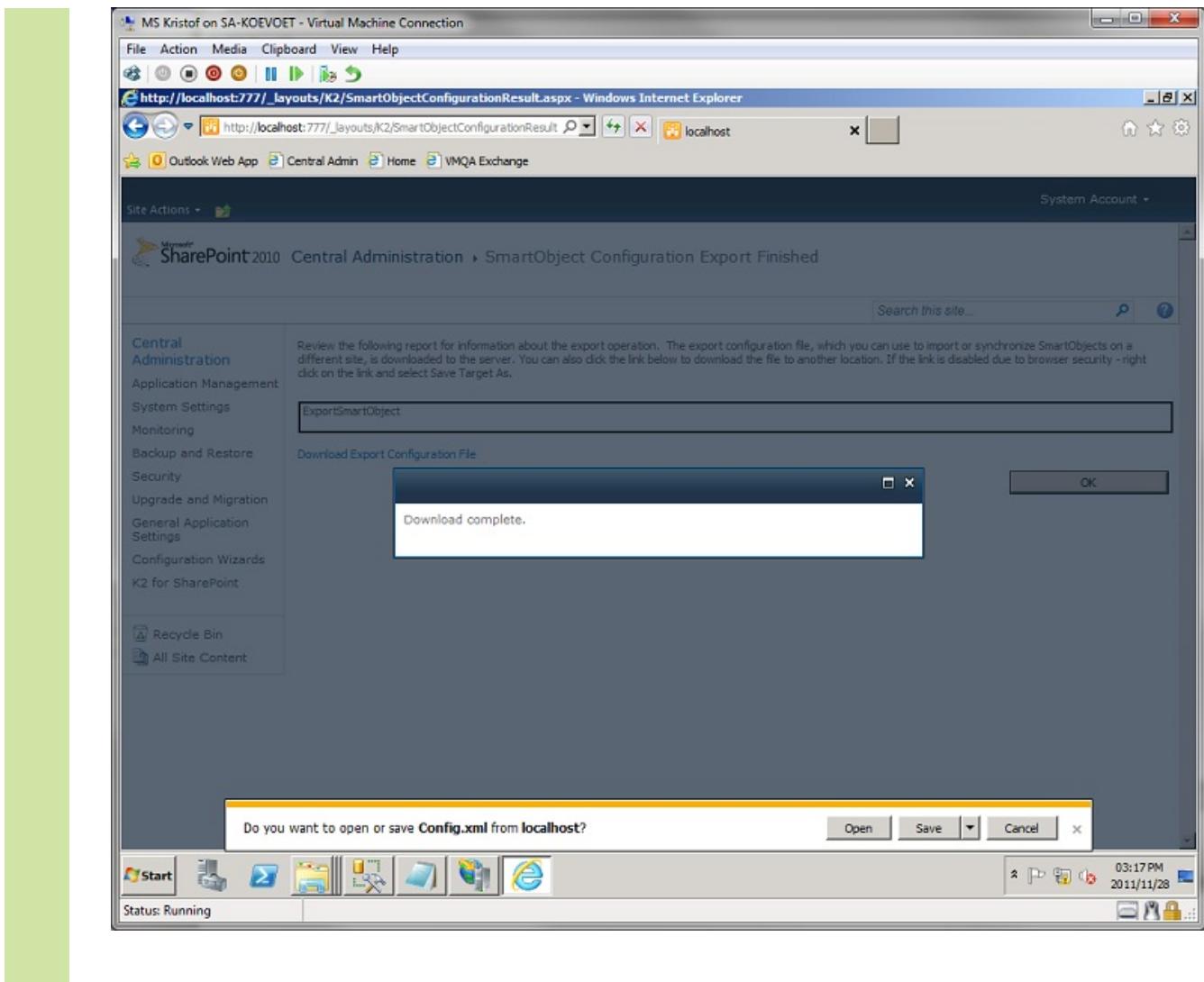
Connection Name	Description	Server	Database
SP		sav-msbeta	KristofDB1
T A		sav-msbeta	KristofDB1
KristofDB1	DB1	sav-msbeta	KristofDB1



- 3 All available items are enabled by default. If there are unwanted items, disable them. Click Ok to proceed with the SmartObject export



④ Download the XML file to your local machine.



1.6.8.1.5.5 CRM SmartObjects

Dynamic CRM SmartObject

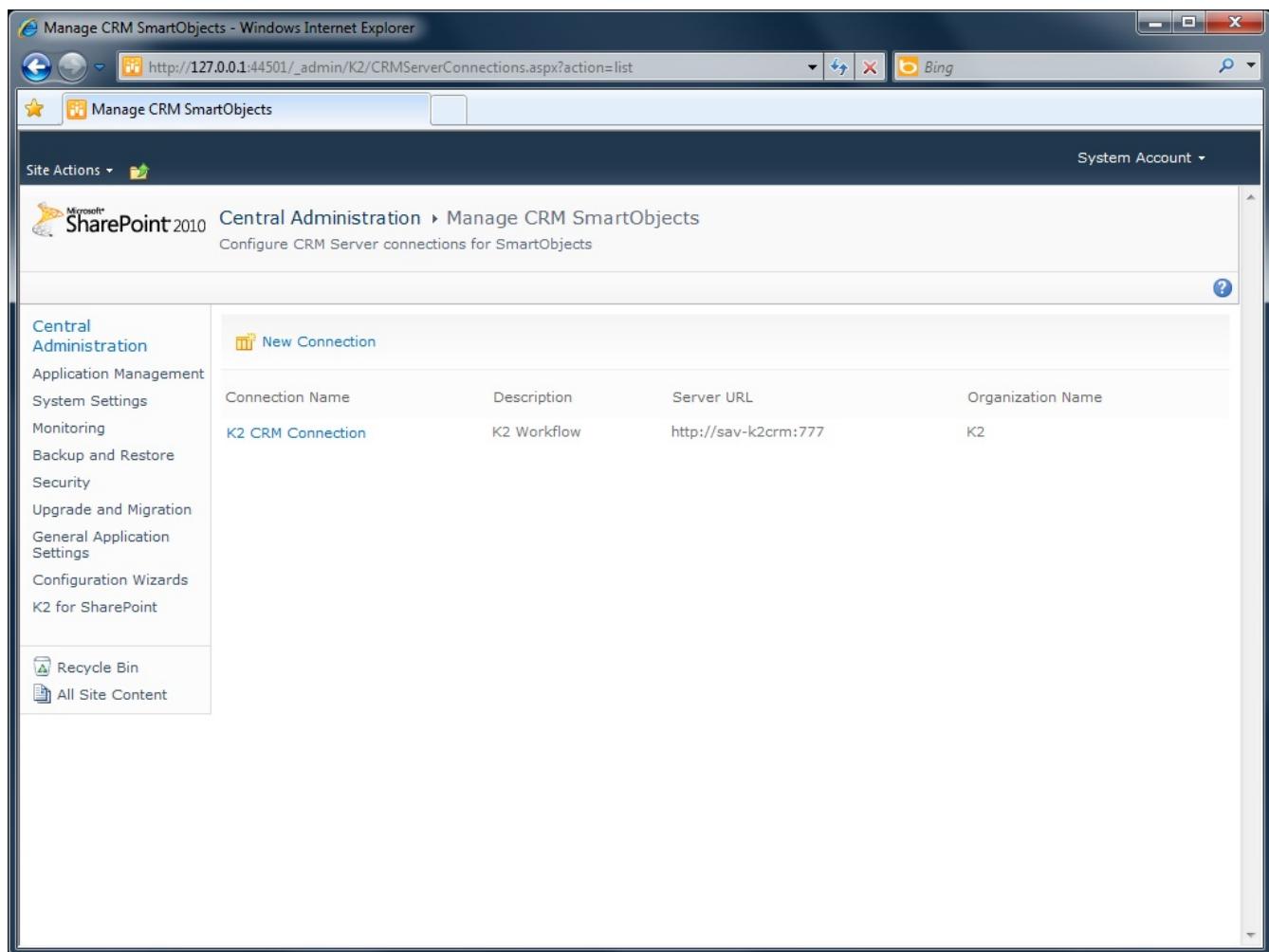
	The individual administering the SmartObject connection must be a SharePoint Administrator to be able to perform the registration process.
	A Microsoft CRM Server must be installed prior to being able to configure the CRM SmartObject. Detail on how to configure such a server is beyond the scope of this topic and this Help file.

The Dynamic CRM SmartObject is configured from within SharePoint and enables the user to generate a SmartObject or Service Instance based on the availability of Entities from within Microsoft CRM Server and the items selected by the User. The Dynamis CRM SmartObject does not enable the user to create new entities but rather enables the user to leverage the existing CRM Entities.

For the user to take advantage of the the Microsoft CRM Server, entities must first be created and then populated with data to enable the SmartObject to be used. The Dynamic CRM SmartObject functions as per normal as a standard SmartObect and is consumed in the usual way by the K2 Environment when used.

Configuring the CRM Server Connections for SmartObjects

The CRM Server Connections for SmartObjects are configured from within SharePoint Central Administration. Shown below is an example of a listing are where the SmartObjects will be listed when they are created. New CRM SmartObjects will be listed here and any changes to the existing listings will be made from the same location.



Connection Name	Description	Server URL	Organization Name
K2 CRM Connection	K2 Workflow	http://sav-k2crm:777	K2

1.6.8.1.5.5.1 How to create new CRM server connection

How to create a New CRM Server Object



A Microsoft CRM Server must be installed and configured before a CRM Server SmartObject can be configured.

From SharePoint Central Administration do the following:

CRM Server Connection Settings		
Connection Settings	Connection Name	The name given to the CRM Connection which is displayed.
CRM settings	CRM Server URL	The Server URL or IP Address of the CRM Server
	Organization Name	The Organization Name given to the server

- 1 Click **New**
- 2 Shown in the image below is an example of how to populate the Connection settings. The settings range from connection name to the CRM Server URL.

Site Actions ▾

Central Administration > Manage CRM SmartObjects
Configure CRM Server connection for SmartObjects

Central Administration

Connection Settings

Specify settings for the new connection that will be created.

Connection Name: Description:

CRM Settings

Specify the URL, Organization Name and authentication information for the connection.

Server URL: Organization Name:

Authentication

Impersonate the User Account
 Use the K2 Server Service Account
 Use the specified Windows Account

User Name (e.g. domain\user):
Password:

Design Time Credentials

Specify credentials for retrieving schema information for the connection.

Authentication

Impersonate the User Account
 Use the K2 Server Service Account
 Use the specified Windows Account

User Name (e.g. domain\user):
Password:

OK Cancel

- 3 Click **Ok** to continue.

1.6.8.1.5.5.2 CRM Server Entities Selection

CRM Server Entities Selection



This step requires an active CRM server instance to call the CRM entities.

Shown below is an EXAMPLE selection of CRM Entities which have been extracted from the available CRM Server. The SmartObject is created based on the selection made from this page. Items not selected will be excluded.

The screenshot shows the 'Manage SmartObjects' interface in SharePoint Central Administration. The 'Entity Relationships' section is expanded, showing various CRM entities like Account, Address, Appointment, Case, Contact, Contract, Email, Fax, Invoice, Lead, and Opportunity. A red arrow points to the 'Select All' checkbox at the top of the list.

The User can **Select All**, or the user can do the following

1. Click on **Entity Relationships**
2. The User can Select all for this **Entity Subsection**, as indicated by the red arrow
3. For individual selection, select just the items that is required

The screenshot shows the 'Manage SmartObjects' interface in SharePoint Central Administration. The 'Entity Relationships' section is expanded, showing individual entity checkboxes. A red arrow points to the 'Select All' checkbox under the 'Entity Relationships' heading.

To complete the selection scroll down for final configuration and SmartObject completion

Advanced Settings: To disable SmartObject generation enable the setting below. This will however still result in the Service Objects being generated

The screenshot shows the 'Advanced' settings dialog box. It contains a single checkbox labeled '(D) Do not generate SmartObjects, only create Service Objects for selected entities'. There are 'Create' and 'Cancel' buttons at the bottom.

Click **Create** to complete the K2 SmartObject generation

1.6.8.1.5.5.3 Export and Import CRM SmartObject

1.6.8.1.5.5.3.1 Export CRM SmartObject

How to export the SmartObject

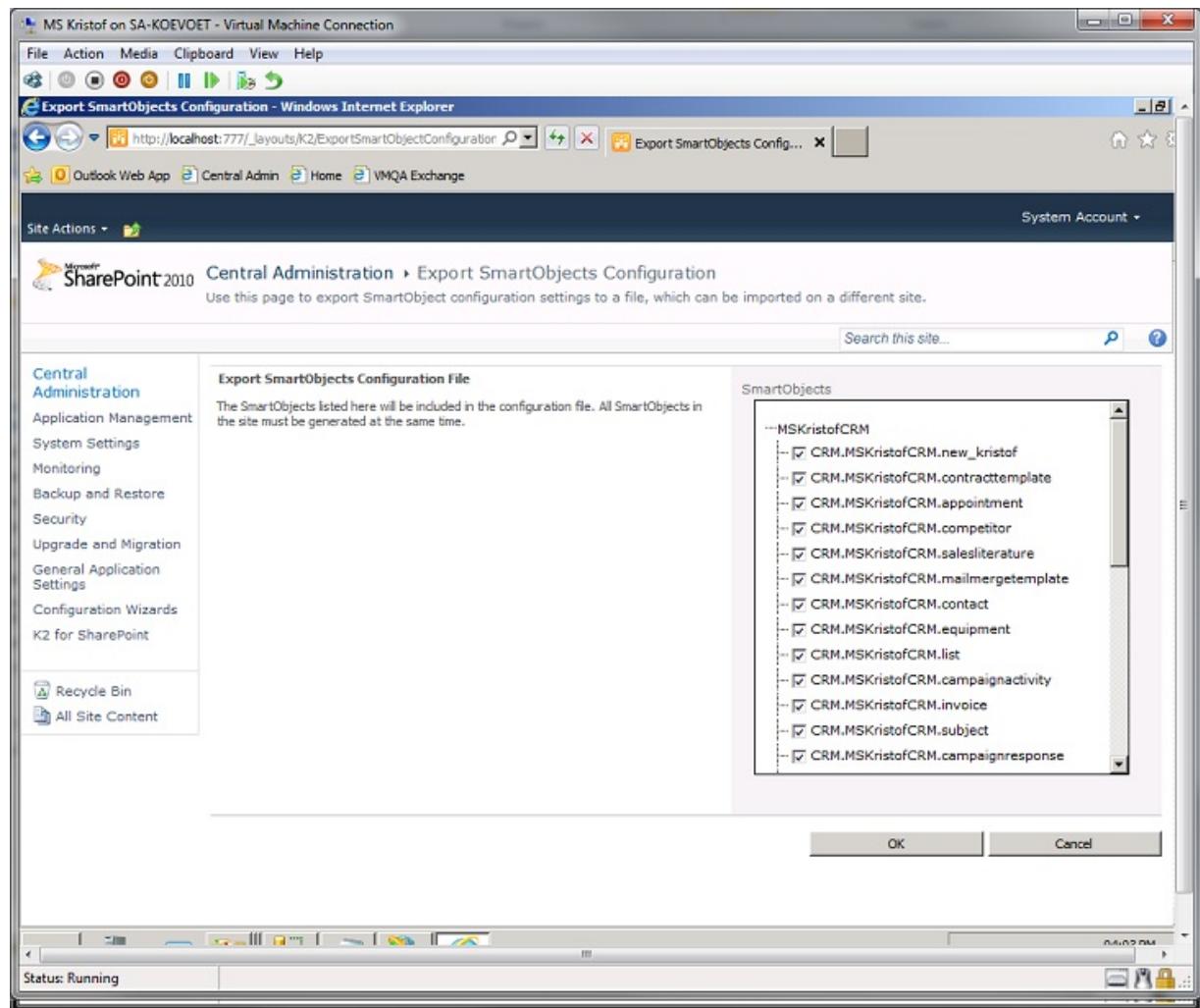


At least one SmartObjects must be present with in the listing below for them to be exported.

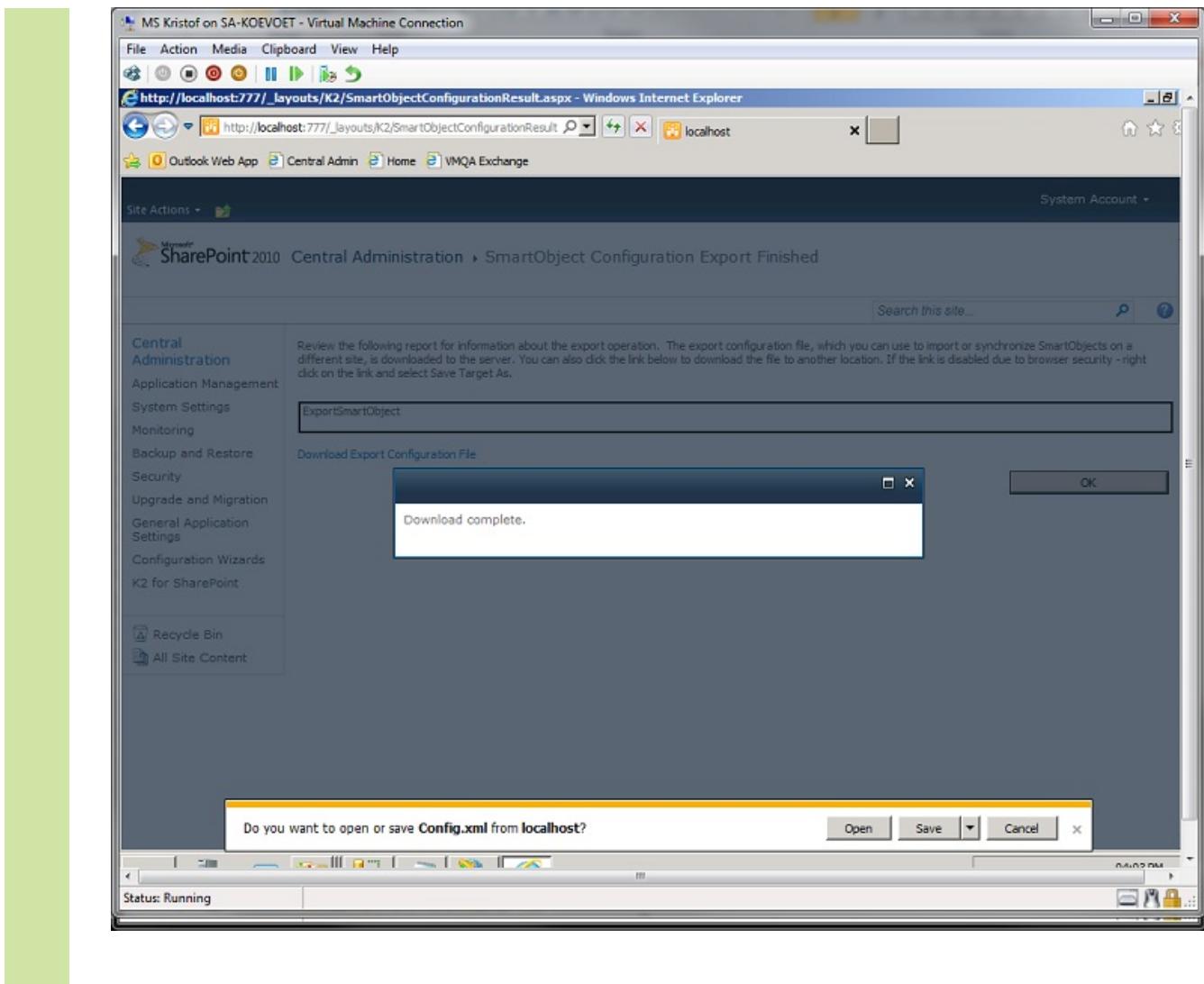
- The SmartObjects that are available under the manage SmartObjects page will be listed in the SmartObjects box. The SmartObject is granularized; all items are selected default, and the user is able to manually determine which items they want to export.
- 1 From **Central Administration > Manage SQL SmartObjects**, select a SmartObject to export by left clicking and selecting Export SmartObjects.
 - 2 From the Manage SQL SmartObjects Page, locate the SQL SmartObjec to export and from the drop down list select Export SmartObject

The screenshot shows the 'Manage CRM SmartObjects' page in SharePoint Central Administration. A dropdown menu is open over a connection entry for 'MSKristofCRM'. The 'Export SmartObjects' option is highlighted. The status bar at the bottom indicates 'Status: Running'.

- 3 All available items are enabled by default. If there are unwanted items, disable them. Click Ok to proceed with the SmartObject export



④ Download the XML file to the local machine.



1.6.8.1.5.5.3.2 Import CRM SmartObject

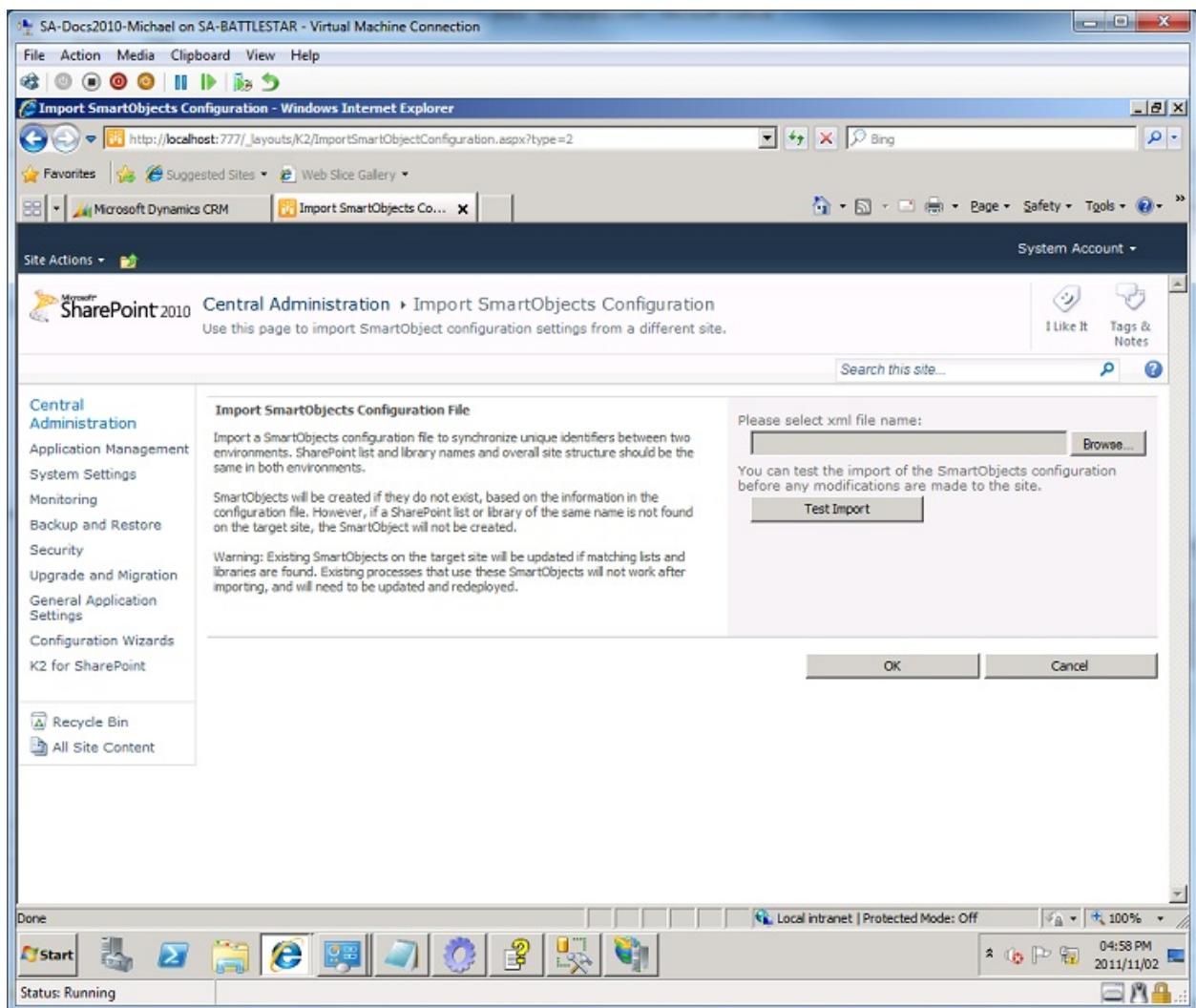
Import SmartObject Definition

The Import SmartObjects option enables the user to select a SmartObject definition and import the definition to create a CRM SmartObject. To start the Import Process, click Import SmartObjects.

 The Import SmartObjects contains Testing functionality that will enable the user to verify that the import process will function as expected before they proceed with the process.

① From **Central Administration > Manage CRM SmartObjects**, select **Import SmartObjects**.

② Click browse to locate the XML file. The import processes outcome can be first tested by clicking the **Test Import** button. This feature generates a report to describe the potential outcome.



③ To proceed, click Ok. A report is generated by the system once the process is complete.

1.6.8.1.6 Overview

Overview

Claims-based authentication is built on Windows Identity Foundation (WIF), a framework for building claims-aware applications and security token service (STS) that is standards-based and interoperable. Interoperability is provided through reliance on industry standard protocols such as WS-Federation, WS-Trust, and Security Assertion Markup Language 1.1 (SAML).

In claims-based authentication, an identity provider, or security token service, responds to authentication requests and issues SAML security tokens that include any number of claims about a user, such as a user name and groups the user belongs to. A relying party application receives the SAML token and uses the claims inside to decide whether to grant the client access to the requested resource. Claims-based authentication can be used to authenticate your organization's internal users, external users, and users from partner organizations.

K2 relies on the configuration of a K2 user manager to provide authentication and user and group resolution for identity stores such as Active Directory, SQL, LDAP or Custom. For more information see [User Managers](#)

K2 provides the ability for incoming claims-based authentication through configuration of mappings between claims-based identity providers and K2 user managers.

For more information, see [References](#)



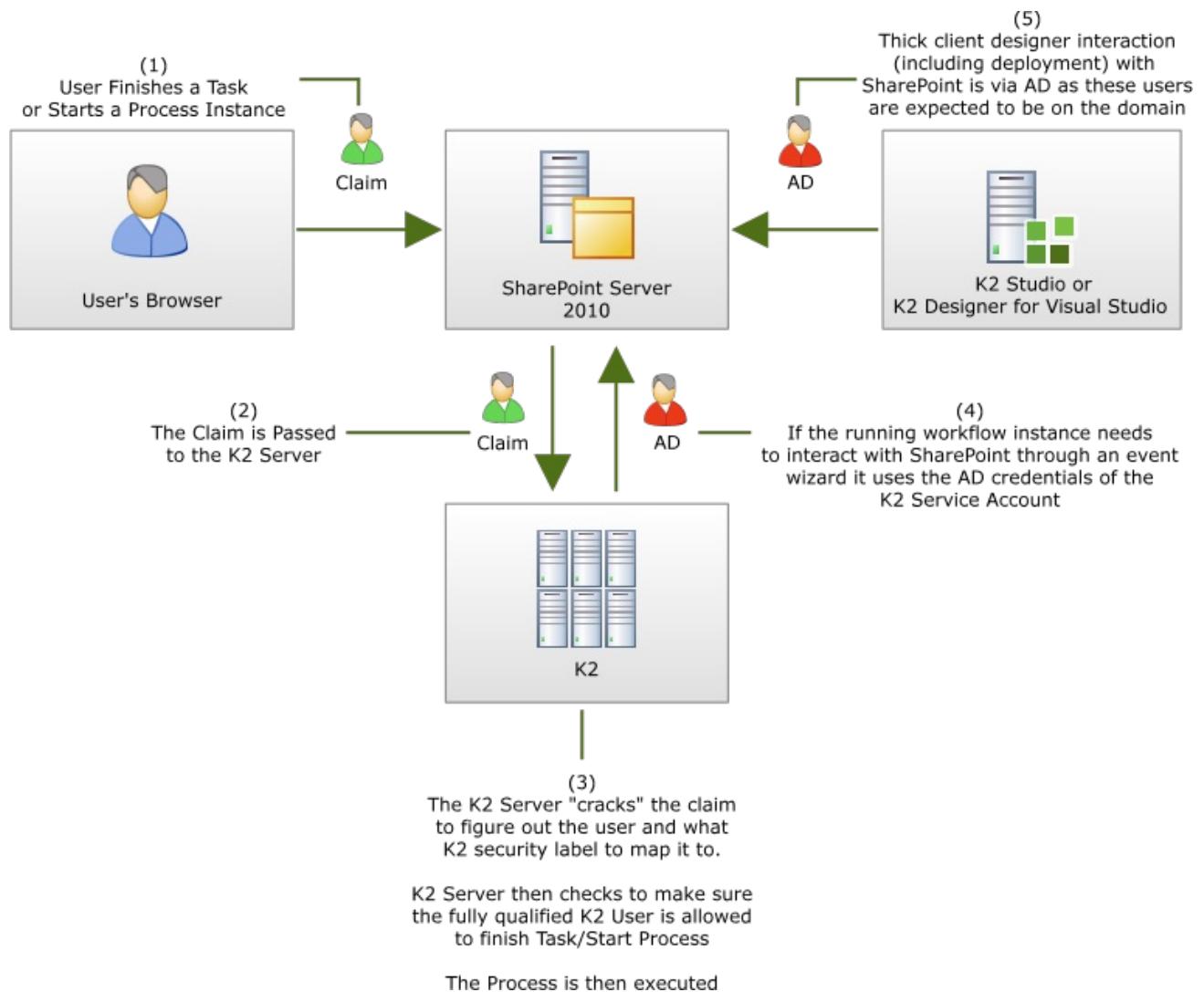
Do not register multiple security labels against the SSPI (Windows Security Provider). Doing so will result in users being resolved incorrectly.

1.6.8.1.6.1 User Token Flow and Terminology

User Token Flow and Terminology

Claims and Active Directory User Tokens

The following diagram illustrates the flow of claims based and Active Directory based user tokens in an environment configured with K2 and SharePoint 2010 claims based authentication.



Terminology

Claims Related Terms

Term	Definition
Claim	A statement that one subject makes about itself or another subject. For example, the statement can be about a name, identity, key, group, privilege, or capability. Claims have a provider that issues them, and they are given one or more values. This data about users is sent inside security tokens (SAML).
Claim rule	A rule that is written in the claim rule language of the provider that defines how to generate, transform, pass through, or filter claims.
Security Assertion Markup Language (SAML)	A protocol that specifies how to use HTTP Web browser redirects to exchange assertions data. SAML tokens are XML representations of claims.
Identity Provider (IP)	A Web service that handles requests for trusted identity claims and issues SAML tokens. An identity provider uses a database called an identity store to store and manage identities and their associated attributes.
Relying Party (RP)	An application that consumes claims to make authentication and authorization decisions. For example, the K2 server receives claims that determine if the issuer user can access K2 data.

Claims-aware application	A relying party software application that uses claims to manage identity and access for users.
Security Token Store (STS)	A Web service that issues security tokens. SharePoint implements a STS to authorize activities within the application from multiple authentication providers
Secure Sockets Layer (SSL)	A protocol that improves the security of data communication by using a combination of data encryption, digital certificates, and public key cryptography. SSL enables authentication and increases data integrity and privacy over networks. SSL does not provide authorization or nonrepudiation.
Active Directory Federation Services (AD FS)	A component of Windows Server 2008 that supports identity federation and Web single sign-on (SSO) for Web browser-based applications.
Federation server	A computer running Windows Server 2008 or Windows Server 2008 R2 that has been configured using the AD FS 2.0 Federation Server Configuration Wizard to act in the federation server role. A federation server issues tokens and serves as part of a Federation Service.
Federation Service	A logical instance of a security token service such as AD FS 2.0.

SharePoint 2010 Terms

Term	Definition
Web Application Authentication Modes	
Classic Mode Authentication	Default mode. "Classic" Windows Authentication (NTLM, Negotiate (Kerberos)) and Anonymous support.
Claims Based Authentication (CBA)	Support for non-Windows authentication. Ensures that all users are SAML token based for every Authentication Type. Note: SharePoint creates SAML 1.1 tokens for all authentication types.
Claims Authentication Types	
Windows Authentication (NTLM, Negotiate (Kerberos))	Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used.
Forms Based Authentication (FBA)	ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA).
Trusted Identity Provider	Trusted Identity Provider Authentication enables federated users in this Web application. This authentication is Claims token based and the user is redirected to a login form for authentication.

1.6.8.1.6.2 Supported Configuration

Supported Configurations

K2 supports integration with SharePoint 2010 web applications in either classic mode authentication or claims-based authentication when configured according to the details in this section.

Bootstrap Tokens

SharePoint 2010 claims-based authentication web sites by default are configured to allow the saving of the bootstrap tokens in the IClaimsIdentity and Sessions after token validation. K2 requires the bootstrap token to be present for proper validation of original claim issuers. The `<service saveBootstrapTokens="true">` setting can be found in the `<microsoft.identityModel>` section of the web.config for the claims-based web site and must be set to **true**.

SharePoint 2010 Claims Authentication Types

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

Trusted Identity Provider Authentication enables federated users in this Web application. This authentication is Claims token based and the user is redirected to a login form for authentication.

<input checked="" type="checkbox"/> Enable Windows Authentication	1
<input checked="" type="checkbox"/> Integrated Windows authentication	
<input type="button" value="Negotiate (Kerberos)"/>	
<input type="checkbox"/> Basic authentication (credentials are sent in clear text)	
<input checked="" type="checkbox"/> Enable Forms Based Authentication (FBA)	2
ASP.NET Membership provider name <input type="text" value="LdapMembershipProvider"/>	
ASP.NET Role manager name <input type="text" value="LdapRoleProvider"/>	
<input checked="" type="checkbox"/> Trusted Identity provider	3
<input type="button" value="Trusted Identity Provider"/>	
<input checked="" type="checkbox"/> ADFS LDAP	

- 1 Windows Authentication (Windows)
- 2 Forms Based Authentication (FBA)
- 3 Trusted Identity Provider (Trusted)

Windows (Required)

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication is a sub-option of Windows authentication and is used as a fallback if Integrated Windows authentication is selected and not available.

Basic authentication method passes user credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.



Important: K2 requires that Windows authentication is configured for Integrated Windows authentication using either NTLM or Negotiate (Kerberos) on all zones of claims enabled web applications that have K2 for SharePoint integration components activated.

Forms

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for a Web application. After you create an FBA Web application, additional configuration is required. For more information, see **Configure forms-based authentication for a claims-based Web application (SharePoint Server 2010)**: <http://technet.microsoft.com/en-us/library/ee806890.aspx>

K2 has tested Forms Based Authentication configured for Microsoft's LDAP Providers.

- Membership Provider: Microsoft.Office.Server.Security.LdapMembershipProvider
- Role Provider: Microsoft.Office.Server.Security.LdapRoleProvider



Disclaimer: K2 is expected to be configurable for any Forms Authentication Providers that have been properly configured and proven to work with SharePoint 2010. However, only Microsoft's LDAP Membership and Role Providers have been tested.

Trusted

Trusted Identity Provider Authentication enables federated users for a Web application. This authentication is Claims token based and the user is redirected to a login form for authentication.

K2 has tested Trusted Identity Provider configured for AD FS 2.0 with Active Directory and LDAP attribute stores. For more information, see **Configuring SharePoint 2010 and ADFS v2 End to End**: <http://blogs.technet.com/b/speschka/archive/2010/07/30/speschka.aspx>

The claim rules tested vary based on the attribute store used.

Active Directory

Rule: Windows Claim

- Claim rule template: Pass Through or Filter an Incoming Claim
- Claim rule name: Windows Account Name Claim
- Incoming claim Type: Windows account name
- Pass through all claim values: Selected

Claim rule name:	Windows Account Name Claim
Rule template:	Pass Through or Filter an Incoming Claim
Incoming claim type:	Windows account name
Incoming name ID format:	Unspecified
<input checked="" type="radio"/> Pass through all claim values	

Rule: LDAP Claims

- Claim rule template: Send LDAP Attributes as Claims
- Claim rule name: LDAP Claims
- Attribute Store: Active Directory
- Mapping of LDAP attributes to outgoing claim types

LDAP Attribute	Outgoing Claim Type
Token-Groups – Qualified by Domain Name	Role
E-Mail-Addresses	E-Mail-Addresses

Claim rule name:
LDAP Claims

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	Token-Groups - Qualified by Domain Name	Role
	E-Mail-Addresses	E-Mail Address

LDAP

Rule: LDAP Claims

- Claim rule template: Send LDAP Attributes as Claims
- Attribute Store: LDAP
- Mapping of LDAP attributes to outgoing claim types

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	Name
Token-Groups- Unqualified Names	Role
E-Mail-Addresses	E-Mail-Addresses

Claim rule name:
LDAP Claims

Rule template: Send LDAP Attributes as Claims

Attribute store:
LDAP

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
	SAM-Account-Name	Name
	Token-Groups - Unqualified Names	Role
	E-Mail-Addresses	E-Mail Address



Disclaimer: K2 is expected to be configurable for any Trusted Identity Providers that have been properly configured and proven to work with SharePoint 2010. However, only Microsoft's AD FS 2.0 has been tested.

SharePoint Multi-Authentication

SharePoint supports implementing more than one claims authentication type on a single web application zone. Microsoft recommends when using claims authentication and implementing more than one type of authentication, that you implement multiple types of authentication on the default zone. This results in the same URL for all users. For more information, see **Planning Zones for Web applications:** <http://technet.microsoft.com/en-us/library/cc262350.aspx#section6>.

The Microsoft SharePoint Search crawl component requires that Windows authentication is configured for Integrated Windows authentication using either NTLM or Negotiate (Kerberos) to access the content of the Web application.

K2 also requires that Windows authentication is configured for Integrated Windows authentication using either NTLM or Negotiate (Kerberos) on all zones of claims enabled web applications that have K2 for SharePoint integration components activated.

The SharePoint crawl component and K2 server utilize the Protocol Discovery Request defined in the Office Forms Based Authentication Protocol Specification to interact with claims based Web applications from Windows based service accounts. The specification provides for the use of request headers to enable authentication through services without login forms.

For more information, see the Protocol Discovery Requests topic in the Office Forms Based Authentication Protocol Specification: [http://msdn.microsoft.com/en-us/library/dd773463\(v=office.12\).aspx](http://msdn.microsoft.com/en-us/library/dd773463(v=office.12).aspx).

Multi-Authentication Combinations

Supported

The following SharePoint 2010 multi-authentication combinations are supported by K2.

Classic Mode

- Windows

Claims Mode

- Windows
- Windows + FBA
- Windows + Trusted
- Windows + FBA + Trusted

Not Supported

The following SharePoint 2010 multi-authentication combinations are not supported by K2.

- FBA (requires Windows on same zone, see above)
- Anonymous
- FBA + Anonymous
- Trusted (requires Windows on same zone, see above)

SharePoint 2007 forms-based authentication is not supported by K2.

Multi-Authentication – Single Login

Claims customers are required to implement Windows Authentication on the same zone as they plan to utilize for process design time and runtime. Designing against one SharePoint URL and executing against another SharePoint URL is currently not supported. Not having Windows Authentication enabled on the design time URL is not supported. The following article includes some potential workarounds: <http://msdn.microsoft.com/en-us/library/hh237665.aspx>. However, it is not necessary to complete all steps that this article describes as there is no need for custom code. The two configuration steps below will enable Windows Authentication for K2 and suppress the Windows Authentication from the designers and runtime users in SharePoint.



Step 1 can be followed if Active Directory users in the people picker are not necessary. Step 2 can be followed if the Active Directory users in the people picker are indeed necessary.

Step 1 – Disable AD in People Picker

- Run the following commands from a SharePoint Management Shell to disable AD users from appearing in People Picker


```
$cprm = Get-SPClaimProviderManager
$cad = Get-SPClaimProvider -Identity "AD"
$cad.IsEnabled = $false
$cadm.Update()
```

Step 2 – Configure Single Login

- Navigate to Central Administration > Manage Web Applications
- Select the claims-based web application and click Authentication Providers
- Select the zone with Windows Authentication + (Trusted and/or Forms Based Authentication)
- Change the Sign In Page URL to Custom Sign In Page and enter the URL for either Trusted or Forms Based Authentication.

NOTE: One provider needs to be picked to bypass the drop down.

- Trusted – replace {ProviderName} with the name of your provider, for example: ADFS LDAP

**Copy**

```
/_trust/default.aspx?trust=
{ProviderName}&ReturnUrl=/_layouts/Authenticate.aspx?
Source=%2F&Source=%2F
```

1.6.8.1.6.3 Claims Authentication Configuration

Configuration

Overview

K2 allows for the use of incoming claims from SharePoint 2010 claims authentication enabled sites. K2 must be configured to register the SharePoint Security Token Service (STS) certificates and map the incoming claims that contain user and group information to the appropriate K2 User Manager. This section explains the configuration settings required and how to determine them.

The configurations are added as a <configuration><sourcecode.security.claims> section in the K2HostServer.config file. The physical path to this file is [Installation Directory]\Host Server\Bin\K2HostServer.config.

Example

The following example is for the fictitious Denallix.com SharePoint claims based site on a single server with user mappings configured for Windows (Active Directory), Forms (LDAP) and a Trusted Provider (AD FS for LDAP).



```
<sourcecode.security.claims>
    <!-- The combination of issuers and claimTypeMappings allows K2 to ensure
        incoming claims are valid and have not been tampered with -->
    <issuers>
        <!-- An entry for each certificate (signing or encrypting) for a trusted STS --
    >
        <issuer name="SharePoint Security Token Service"
        thumbprint="8BD27388714EC92EA0433BE660BA7698430CE4FF" />
        <issuer name="SharePoint Security Token Service Encryption"
        thumbprint="54722E70106DF64E48DD2FF2AFC8BC4F8DE231B1" />
    </issuers>
    <claimTypeMappings>
        <!--K2ADFS Security/Role Provider for Trusted Provider-->
        <claimTypeMapping securityLabel="K2ADFS">
            <!-- Claim that represents the system issuing the identity and role claims to
                be mapped to the K2 security label-->
            <identityProviderClaim originalIssuer="SecurityTokenService"
            claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
            claimValue="trusted:ADFS LDAP" />
            <!-- Claim that represents the user for the K2 security label-->
            <identityClaim originalIssuer="TrustedProvider:ADFS LDAP"
            claimType="http://schemas.k2.com/identity/claims/name" />
            <!-- Claim that represents the groups for the K2 security label-->
            <roleClaim originalIssuer="TrustedProvider:ADFS LDAP"
            claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" />
        </claimTypeMapping>
        <!--K2 Security/Role Provider for Windows Authentication-->
        <claimTypeMapping securityLabel="K2">
            <!-- Claim that represents the system issuing the identity and role claims to
                be mapped to the K2 security label-->
            <identityProviderClaim originalIssuer="SecurityTokenService"
            claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
            claimValue="windows" />
            <!-- Claim that represents the user for the K2 security label-->
            <identityClaim originalIssuer="Windows"
            claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname" />
            <!-- Claim that represents the groups for the K2 security label-->
            <roleClaim originalIssuer="Windows"
            claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid" />
        </claimTypeMapping>
        <!--K2FORMS Security/Role Provider for Forms Authentication-->
        <claimTypeMapping securityLabel="K2FORMS">
            <!-- Claim that represents the system issuing the identity and role claims to
                be mapped to the K2 security label-->
            <identityProviderClaim originalIssuer="SecurityTokenService"
            claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
            claimValue="forms:LdapMembershipProvider" />
            <!-- Claim that represents the user for the K2 security label-->
            <identityClaim originalIssuer="Forms:LdapMembershipProvider"
            claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname" />
            <!-- Claim that represents the groups for the K2 security label-->
            <roleClaim originalIssuer="Forms:LdapRoleProvider"
            claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" />
        </claimTypeMapping>
    </claimTypeMappings>
```

```
</sourcecode.security.claims>
```

Issuers

K2 supports a one-to-many mapping between K2 and the certificates that the SharePoint STS uses to sign (SharePoint Security Token Service) and encrypt (SharePoint Security Token Service Encryption) the security tokens it issues. The default installation of SharePoint will generate and store individual certificates for both signing and encrypting on each server in the farm. The image highlights the values required for an <issuer> entry – the name and thumbprint for each individual signing and encrypting certificate for the STS.

```
<issuers>
  <!-- An entry for each certificate (signing or encrypting) for a trusted STS -->
  <issuer name="SharePoint Security Token Service" thumbprint="8BD27388714EC92EA0433BE660BA7698430CE4FF" />
  <issuer name="SharePoint Security Token Service Encryption" thumbprint="54722E70106DF64E48DD2FF2AFC8BC4F8DE231B1" />
</issuers>
```

Claim Type Mappings

K2 recommends a one-to-one mapping between a K2 User Manager (UM) and an incoming claim set Identity Provider (IP). Each <claimTypeMapping> will contain an entry for the Security Label of the associated K2 UM and three claim types to be mapped from the IP: Identity Provider, Identity and Role.



It is recommended that one K2 User Manager is mapped to a single Identity Provider. However, if more than one mapping is required, the runtime resolution of users is determined by the order they are registered in the <sourcecode.security.claims> configuration. Furthermore, it is recommended that the Windows Identity Provider, typically used for service accounts only, be the last one registered in the <sourcecode.security.claims> configuration.

The image below highlights the values required for a <claimTypeMapping>. The claimTypeMapping requires a unique K2 UM securityLabel to be configured. The identityProviderClaim requires an originalIssuer, claimType and claimTypeValue to be configured while the identityClaim and roleClaim require originalIssuer and claimType to be configured.

Legend

- 1 Identity Provider
- 2 Identity
- 3 Role

```
<!--K2ADFS Security/Role Provider for Trusted Provider-->
<claimTypeMapping securityLabel="K2ADFS">
  <!-- Claim that represents the system issuing the identity and role claims to be mapped to the K2 security label-->
  1 <identityProviderClaim originalIssuer="SecurityTokenService" claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
     claimValue="trusted:ADFS LDAP" />

  2 <!-- Claim that represents the user for the K2 security label-->
  <identityClaim originalIssuer="TrustedProvider:ADFS LDAP" claimType="http://schemas.k2.com/identity/claims/name" />

  3 <!-- Claim that represents the groups for the K2 security label-->
  <roleClaim originalIssuer="TrustedProvider:ADFS LDAP" claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" />
</claimTypeMapping>
```



K2 requires the claimType for the identityClaim to match the claim mapping configured in SharePoint as the Identifier Claim. The K2 Server Configuration section provides automatic and manual approaches that aid in configuring the appropriate identity claim type mapping for K2.

K2 Server Configuration

The <sourcecode.security.claims> section must be manually added to the K2HostServer.config file. However, the method used to generate the configuration section values can be automatically generated or manual. Using the automatically generated approach is recommended.

Automatically Generated Approach

This option requires the use of PowerShell scripts available as a download for this topic that will interrogate a SharePoint 2010 claims configuration and automatically generate all the resulting <sourcecode.security.claims> configuration section for K2HostServer.config.

SharePoint Central Administration

Run these commands on the SharePoint Central Administration server or for single server farm configurations.

1. Download and extract the **Get-ClaimTypeMappings.ps1** script
2. Start SharePoint 2010 Management Shell
3. Execute Get-ClaimTypeMappings.ps1 and provide the values requested at the prompts
 - a. For more information on the options available, execute:
Get-Help .\Get-ClaimTypeMappings.ps1
 - b. NOTE: The script will stop executing if the SharePoint environment is not properly configured for K2 claims support. For more information, see [Claims-based Authentication](#)Open the [Installation Directory]\Host Server\Bin\K2HostServer.config. file.
4. Add the resulting <sourcecode.security.claims> XML to the end of the <configuration> section
5. Save the file and restart the K2 blackpearl Server service

SharePoint Web Front Ends

Additionally, run these commands on the SharePoint web front ends for multi-server farm configurations.

1. Download and extract the **Get-AdditionalIssuers.ps1**
2. Start SharePoint 2010 Management Shell
3. Execute Get-AdditionalIssuers.ps1
4. Open the [Installation Directory]\Host Server\Bin\K2HostServer.config. file
5. Add the resulting <issuer> XML to the end of the <configuration><sourcecode.security.claims><issuers> section
6. Save the file and restart the K2 blackpearl Server service
7. Once the K2 Server has restarted an IISRESET will be required



[Download:](#) You can download the SourceCode.Security.Claims sample scripts by clicking here.

Manually Generated Approach

This option requires extensive knowledge of the SharePoint claims configuration and optionally the use of the community provided SourceCode.Samples.Claims.WebPart.

The image below highlights the values required in K2HostServer.config as returned by the SourceCode.Samples.Claims.WebPart.

Legend

- 1 Identity Provider
- 2 Identity
- 3 Role

Original Issuer	Claim Type	Claim Value	K2 Claim Type Mapping
SharePoint	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	administrator	
2 TrustedProvider:ADFS LDAP	http://schemas.k2.com/identity/claims/name	Administrator	Identity
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Group Policy Creator Owners	Role
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Domain Users	Role
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Domain Admins	Role
3 TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Enterprise Admins	Role
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Schema Admins	Role
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Organization Management	Role
TrustedProvider:ADFS LDAP	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	administrator@denalix.com	
SecurityTokenService	http://schemas.microsoft.com/sharepoint/2009/08/claims/userid	0&t adfs ldap administrator	
SecurityTokenService	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0&t adfs ldap administrator	
1 SecurityTokenService	http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider	trusted:ADFS LDAP	Identity Provider
SecurityTokenService	http://sharepoint.microsoft.com/claims/2009/08/isauthenticated	True	
ClaimProvider:System	http://schemas.microsoft.com/sharepoint/2009/08/claims/farmid	99e871a8-b181-4233-8458-2c66e104a220	

1. Download and install the **SourceCode.Samples.Claims.WebPart**

2. Open the [Installation Directory]\Host Server\Bin\K2HostServer.config file

3. Add the example <sourcecode.security.claims> XML from this topic to the end of the <configuration> section

4. Update the values in the example with the values from your environment for

- Issuers – certificate name and thumbprint for SharePoint Security Token Service and SharePoint Security Token Service Encryption certificates for all servers in the farm. These values can be determined by using the MMC Certificates Snap-in and navigating to the Local Computer\SharePoint\Certificates node or using the SharePoint 2010 Management Shell and executing the following PowerShell commands.



```
(Get-SPServiceApplication -Name
SecurityTokenServiceApplication).SigningCertificateThumbprint
(Get-SPServiceApplication -Name
SecurityTokenServiceApplication).EncryptionCertificateThumbprint
```

- Claim Type Mappings – identity provider claim, identity claim and role claim for each authentication provider associated with the web application. These values can be determined from the scripts used to configure SharePoint for claims authentication or the community provided web part.

5. Save the file and restart the K2 blackpearl Server service

6. Once the K2 Server has restarted an IISRESET will be required



[Download:](#) You can download the SourceCode.Sample.Claims.WebParts sample scripts by clicking here.



The SourceCode.Sample.Claims.WebPart is provided as an example only and is not supported.

1.6.8.1.6.4 Claims User Identity Flow

Claims User Identity Flow

This section explains how a claims-based user identity flows in a specific environment with the following systems configured in a particular manner as described throughout this topic:

- SharePoint 2010 Web application using Trusted Provider claims-based authentication
- AD FS 2.0 using the LDAP attribute store
- K2 blackpearl with trusted Issuer, Identity Provider, Identity and Role claim mappings

For more information on configuration, see [Configuration](#)

AD FS 2.0 Configuration

AD FS 2.0 is configured to provide the following claims from the LDAP attribute store.

LDAP Attribute	Outgoing Claim Type
SAM-Account-Name	Name
Token-Groups - Unqualified Names	Role
E-Mail-Addresses	E-Mail Address

SharePoint 2010 Configuration

SharePoint 2010 is configured for claims authentication using AD FS as a trusted provider mapping the `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name` claim type as the Identifier Claim and E-mail Address and Role as additional claims.

Copy

```
$map1 = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" -
IncomingClaimTypeDisplayName "Name" -LocalClaimType
"http://schemas.k2.com/identity/claims/name"
$map2 = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
-IncomingClaimTypeDisplayName "Email Address" -SameAsIncoming
$map3 = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -
IncomingClaimTypeDisplayName "Role" -SameAsIncoming

$ip = New-SPTrustedIdentityTokenIssuer -Name $trustedName -
Description $trustedDescription -realm $realm -
ImportTrustCertificate $cert -ClaimsMappings $map1, $map2, $map3 -
SignInUrl $signInUrl -IdentifierClaim $map1.InputClaimType
```



SharePoint has several reserved claim types that require mapping to a unique, non-reserved claim type. For more information, see the `SPTrustedClaimTypeInformation.IsClaimTypeReserved` Method: <http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.administration.claims.sptrustedclaimtypeinformation.isclaimtypreserved.aspx>.

The default claim type provided by AD FS for Name is reserved in SharePoint and must be mapped to a unique claim type. The Name claim type is configured to map to the `http://schemas.k2.com/identity/claims/name` claim type in SharePoint. K2 receives the claim set from SharePoint and therefore must be configured to use the mapped claim type value of the identity claim.

The following PowerShell command is used to determine the MappedClaimType of Identity Claim Type configured for a Trusted Provider in SharePoint.



```
(Get-SPTokenIssuer).IdentityClaimTypeInformation

DisplayName : Name
InputClaimType :
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
MappedClaimType :
http://schemas.k2.com/identity/claims/name
IsIdentityClaim : True
AcceptOnlyKnownClaimValues : False
ClaimValueModificationAction : None
ClaimValueModificationArgument :
KnownClaimValues : {}
UpgradedPersistedProperties :
```

K2 Configuration

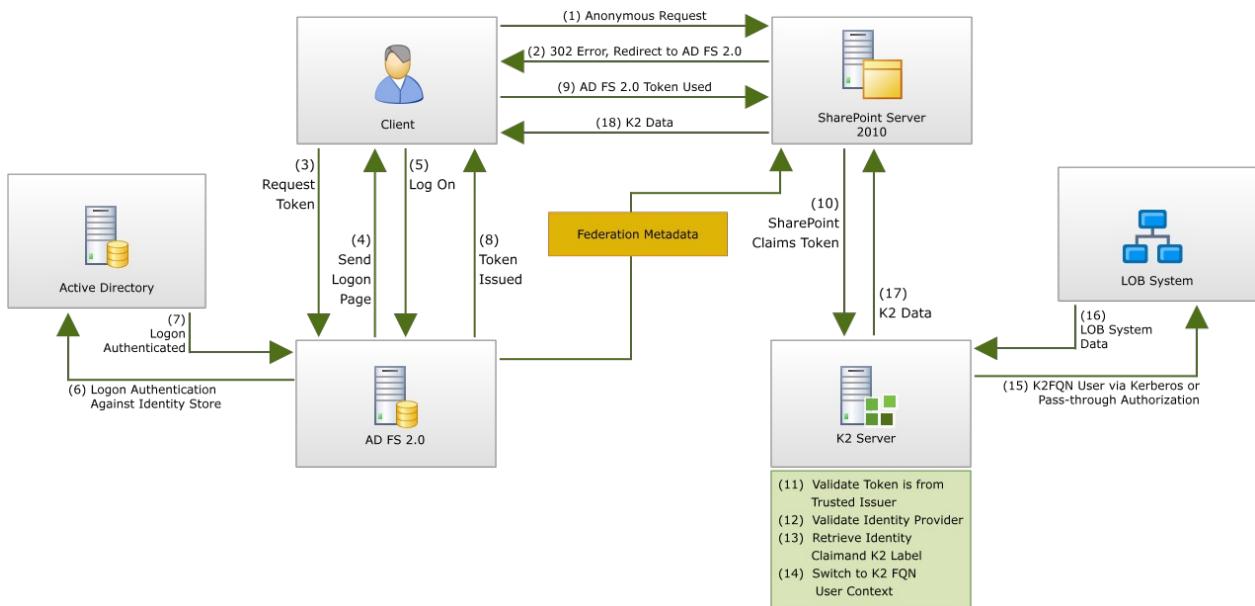
K2 is configured to map identity and role claims from the [trusted:ADFS LDAP](#) identity provider to the [K2 LDAP](#) user manager with the K2ADFS security label. Additionally, identity and role claims from the [windows](#) identity provider are configured to map to the K2 Active Directory user manager with the [K2](#) security label.



```
<sourcecode.security.claims>
    <issuers>
        <issuer name="SharePoint Security Token Service"
thumbprint="8BD27388714EC92EA0433BE660BA7698430CE4FF" />
        <issuer name="SharePoint Security Token Service Encryption"
thumbprint="54722E70106DF64E48DD2FF2AFC8BC4F8DE231B1" />
    </issuers>
    <claimTypeMappings>
        <claimTypeMapping securityLabel="K2ADFS">
            <identityProviderClaim originalIssuer="SecurityTokenService"
claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
                claimValue="trusted:ADFS LDAP" />
            <identityClaim originalIssuer="TrustedProvider:ADFS LDAP"
claimType="http://schemas.k2.com/identity/claims/name" />
            <roleClaim originalIssuer="TrustedProvider:ADFS LDAP"
claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" />
        </claimTypeMapping>
        <claimTypeMapping securityLabel="K2">
            <identityProviderClaim originalIssuer="SecurityTokenService"
claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
                claimValue="windows" />
            <identityClaim originalIssuer="Windows"
claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname" />
            <roleClaim originalIssuer="Windows"
claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid" />
        </claimTypeMapping>
    </claimTypeMappings>
</sourcecode.security.claims>
```

Logical Flow

User requests for content and data from SharePoint and K2 will follow this flow.



1. The client sends a request to access the SharePoint 2010 site.
2. IIS refuses the connection and redirects the user to the trusted claims provider for SharePoint 2010 – AD FS 2.0.
3. The client sends a request for a token from AD FS 2.0.
4. AD FS 2.0 returns a logon page to the client prompting users for credentials.



If the client already has a valid Kerberos ticket on the network, and AD FS 2.0 is setup for Integrated Windows Authentication, then this ticket is presented to AD FS 2.0 in the first request, skipping steps 4-7.

5. The user provides their credentials.
6. AD FS 2.0 validates the credentials with the identity store, in this case Active Directory.
7. Active Directory validates the client.
8. AD FS 2.0 provides a claim for access to SharePoint 2010 data.
9. The client presents the claim from AD FS 2.0 to the SharePoint 2010 server.
10. The SharePoint 2010 server decrypts and validates the claim, then encrypts the claim with additional SharePoint claims and provides the claims for access to K2 data.
11. The K2 server validates the claim is from a trusted issuer (the SharePoint STS) and decrypts the claim.
12. The K2 server matches the identity provider in the claim to one registered in K2 configuration.
13. The K2 server retrieves the K2 user manager security label and the identity claim value to construct the K2 fully qualified name user.
14. The K2 server switches the context to the K2 FQN user.
15. (Optional) The K2 server accesses LOB system data via Kerberos or Pass-through Authentication using the context of the K2 FQN user.
16. (Optional) The LOB system requested data is returned to the K2 server.
17. The K2 data is returned to the SharePoint 2010 server.
18. The SharePoint 2010 server presents the K2 FQN user with the requested information.



K2 does not implement an STS and therefore does not retain or pass-on to external LOB systems any of the claims provided with the user from SharePoint. K2 utilizes the configured claim mappings to determine the appropriate K2 fully qualified name user. Once the K2 fully qualified user name context has been determined, all processing in K2 occurs using that same user context just as it does for non-claims-based users.

Validation of Flow

The display of the `SourceCode.Sample.Claims.WebPart` can be used to understand the flow of user context between SharePoint, AD FS and K2.

The three claim types configured for the claim rule in AD FS have resulted in a total of 4 claims. One for the Name, one for the E-mail Address and two for Role which corresponds to the two Active Directory groups that Joe is a member – Domain Users and Legal.

- **Identity claim (1):** `http://schemas.k2.com/identity/name` (mapped claim for `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`)
- **Role claim (2):** `http://schemas.microsoft.com/ws/2008/06/identity/claims/role`
- **Email address claim (1):** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

Original Issuer	Claim Type	Claim Value
SharePoint	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	joe
TrustedProvider:ADFS LDAP	http://schemas.k2.com/identity/claims/name	Joe
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Domain Users
TrustedProvider:ADFS LDAP	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Legal
TrustedProvider:ADFS LDAP	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	joe@denallix.com
SecurityTokenService	http://schemas.microsoft.com/sharepoint/2009/08/claims/userid	06:t adfs ldap:joe
SecurityTokenService	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	06:t adfs ldap:joe
SecurityTokenService	http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider	trusted:ADFS LDAP
SecurityTokenService	http://sharepoint.microsoft.com/claims/2009/08/isauthenticated	True
ClaimProvider:System	http://schemas.microsoft.com/sharepoint/2009/08/claims/farmid	99e871a8-b181-4233-8458-2c661e104a220 06:t adfs ldap:joe,06:t adfs ldap:joe,1,296-3724-5226-4f9d19-PGc38HMsF6R+BWQJdGU3D0AEfkszknD9bYWhpSfnsSr3eW6QOQJldAFtCMgVuUHQyvC4tqfjdts/cvsKvCSbMeLunLfXF1bpGafj0XK0mnn4LZKxeSe+3lwEh0ChtrRjMK35xfC+Un2qUp1QNDFsSAk6MVsBjg00HGwYJ2Jk2AUEScyrwQ2SGIzLZvlnXbfTrVgf/fovg3oIn0Q1sT1Y1tkT72vDAt61L Ko6MEDVpxkLHAvt2zGSzivMdKcovIT14fJApTkLZ +/WMT +3FMTS09FFN8Z1aztJYAn26RTTXkZg= =,https://claims.denallix.com:444/
SharePoint	http://sharepoint.microsoft.com/claims/2009/08/tokenreference	

In addition, SharePoint has added several claims, including the identity provider claim used by K2 to determine which K2 user manager and security label to map the incoming user.

In the end the K2 server correctly transformed the logged in SharePoint claims user to a K2 fully qualified name user using the LDAP user manager with the K2ADFS security label.

K2 Mapped User

K2 FQN: K2ADFS:Joe

1.6.8.1.6.5 Mapping User

Mapping Users

SharePoint user to K2 user (Classic Mode Authentication)

In classic mode all integration with K2 is done using the Windows authentication mechanism, either NTLM or Kerberos. Users who access K2 or SharePoint resources in this configuration will likely utilize Integrated Windows Authentication to allow their current logged in Windows credentials to automatically logon to SharePoint or K2. A user will be prompted with a Windows Security dialog to provide credentials whenever integration is not available.



Once users have been authenticated with Windows credentials, they are granted access or authorization to SharePoint or K2 based on their configured permissions.

SharePoint maps the authorized user from an underlying information store, in this case Active Directory, to a SharePoint-specific user name, represented in the image below as Account.

Account	DENALLIX\joe
Name	Joe Bocardo

Similarly, K2 maps the authorized user from the underlying information store to a K2 fully qualified name user in the format of [Security Label]:[Domain\Username], represented as a K2 field part in the image below.

Name	Type
K2:DENALLIX\joe	User

SharePoint user to K2 user (Claims Mode Authentication)

In claims mode integration, K2 depends on the claims authentication type configured for the current SharePoint user, Windows, Forms or Trusted. Users who access K2 or SharePoint resources in this configuration will either utilize Integrated Windows Authentication or a login form to logon to SharePoint or K2.

SharePoint 2010 provides a SharePoint Security Token Service (STS) that is a specialized Web service designed to respond to requests for security tokens and provide identity management. After authentication, the SharePoint STS issues a trusted security token that it can then present to a relying party application such as K2. K2 establishes a trust relationship with the SharePoint STS. This enables K2 to validate the security tokens issued by the SharePoint STS and examine security tokens presented by SharePoint and determine the validity of the identity claims they contain.

The SharePoint STS maps the authorized user from the underlying information store, for example claims-based

Active Directory, to a SharePoint encoded claim user name, represented as Account in the image below.

Account	i:0#.w denallix\joe
Name	Joe Bocardo

The SharePoint encoded claim user name is a combination of the values for two main claims – Identity Provider and Identity. The identity provider claim type is populated by the SharePoint STS with the value of the provider that performed the authentication. The identity claim type will vary based on the configuration of the authentication provider. SharePoint pre-configures the claim type for Windows and Forms determines the claim type for Trusted providers when they are registered with SharePoint.

Identity Provider Claim Type

Windows/Forms/Trusted: <http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider>

Identity Claim Type

Windows/Forms: <http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname>

Trusted: provider specific

Original Issuer	Claim Type	Claim Value
SharePoint	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	denallix\joe
Windows	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid	S-1-5-21-1182838845-2098967006-2361148 536-1132
Windows	http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid	S-1-5-21-1182838845-2098967006-2361148 536-513
Windows	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	joe@denallix.com
Windows	http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname	DENALLIX\joe
SecurityTokenService	http://schemas.microsoft.com/sharepoint/2009/08/claims/userid	0#.w denallix\joe
SecurityTokenService	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0#.w denallix\joe
SecurityTokenService	http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider	windows
SecurityTokenService	http://sharepoint.microsoft.com/claims/2009/08/isauthenticated	True
ClaimProvider:System	http://schemas.microsoft.com/sharepoint/2009/08/claims/farmid	99e871a8-b181-4233-8458-2c66e104a220 0 .w s-1-5-21-1182838845-2098967006-2361148 1148536-1132,0#.w denallix\joe,129630769 096121538,True,CnguAXH2xtbjOuFkYGA3C4jr MhCvDQ9jnZI/iaYEfY123+rsaK9RgB8UDx2/X WtU14KIKu/pNT4SgzYvIRnNULzOiyVkyGOIQ yh1V90LJ0crBS26vd4QIKPVLfrMCOSyZzSF9Lcw em+XSojzloLCr44iCMw3dF1GyEYIX4zyzsIc1Q/ +rayAozcnrl7+2iCS12dOpI6Xj3uv/XV6eOh7vj vKHzM+Onvcrf5SDm14rOo/SEvV7EyldAYWF1 patmZZ7oI63AvIpanqduSbMrsvYklDz70a5vS QRy1lQeOp/SmteYB2sn6lh2YyagZ1z61QRW 7K2StP4PNBxg==,https://claims.denallix.co m:444/SitePages/Home.aspx
SharePoint	http://sharepoint.microsoft.com/claims/2009/08/tokenreference	
Windows	http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-21-1182838845-2098967006-2361148 536-513
Windows	http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-21-1182838845-2098967006-2361148 536-1171
Windows	http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-1-0
Windows	http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid	S-1-5-11
SharePoint	http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows
SharePoint	http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2011-10-14T04:41:49.607Z

For more information on SharePoint claims users encoding, see the **AttributeValue** topic in the SharePoint Security Token Service Web Service Protocol Specification: [http://msdn.microsoft.com/en-us/library/dd932259\(v=office.12\).aspx](http://msdn.microsoft.com/en-us/library/dd932259(v=office.12).aspx).

K2 implements a similar claims type mapping concept for the relationship between the SharePoint claims user and the K2 fully qualified name user. K2 does not implement an STS and therefore does not retain or pass on any of the claims provided with the user from SharePoint. K2 utilizes the configured claim mappings to determine the appropriate K2 fully qualified name user. Once the K2 fully qualified user name context has been determined, all processing in K2 occurs using that same user context just as it does for non-claims-based users.

For more information on configuring the trust relationship and user mappings between SharePoint and K2, see **Installation and Configuration > Configuration > SharePoint > Claims-based Authentication > Configuration**

For more information on available K2 user managers, see **Installation and Configuration > Configuration > User Managers**

Inline Functions

K2 provides several inline functions to assist process designers in converting between SharePoint claims users and K2 fully qualified name users.

Conversion

- » To Base-64 String(Value)(String)
- » To Binary(Value)(Binary)
- » To Boolean(Value)(Boolean)
- » To Bytes(Value)(Binary)
- » To DateTime(Value)(DateTime)
- » To Decimal(Value)(Decimal)
- » To Double(Value)(Double)
- » To Integer(Value)(Integer)
- » To K2 FQN User(Host Server Connection String, SharePoint Site URL, Value)(String)
- » To K2 FQN User(Host Server Connection String, SharePoint Site URL, Value)(String[])
- » To Long(Value)(Long)
- » To SharePoint Claims User(Host Server Connection String, SharePoint Site URL, Value)(String)
- » To SharePoint Claims User(Host Server Connection String, SharePoint Site URL, Value)(String[])
- » To Short(Value)(Short)
- » To String(Value)(String)

Each function requires input information about the K2 Server, the SharePoint Site URL and user to convert, as either a string or an array of strings.

To use an array of SharePoint claims users as a destination K2 will require the users be converted to an array of K2 fully qualified name users. The **To K2 FQN User() (String[])** can be used to do just that.

ToK2FQNUser(Host Server Connection String,SharePoint Site URL,Value)

Configure Function

Function Name: **To K2 FQN User(Workflow Management Server,Portal (Claims),SharePoi** i

Return Type: String

Name	Type	Value
Host Server Con...	String	Workflow Management Server e(x)
SharePoint Site...	String	Portal (Claims) e(x)
Value	String[]	SharePoint User Array e(x)

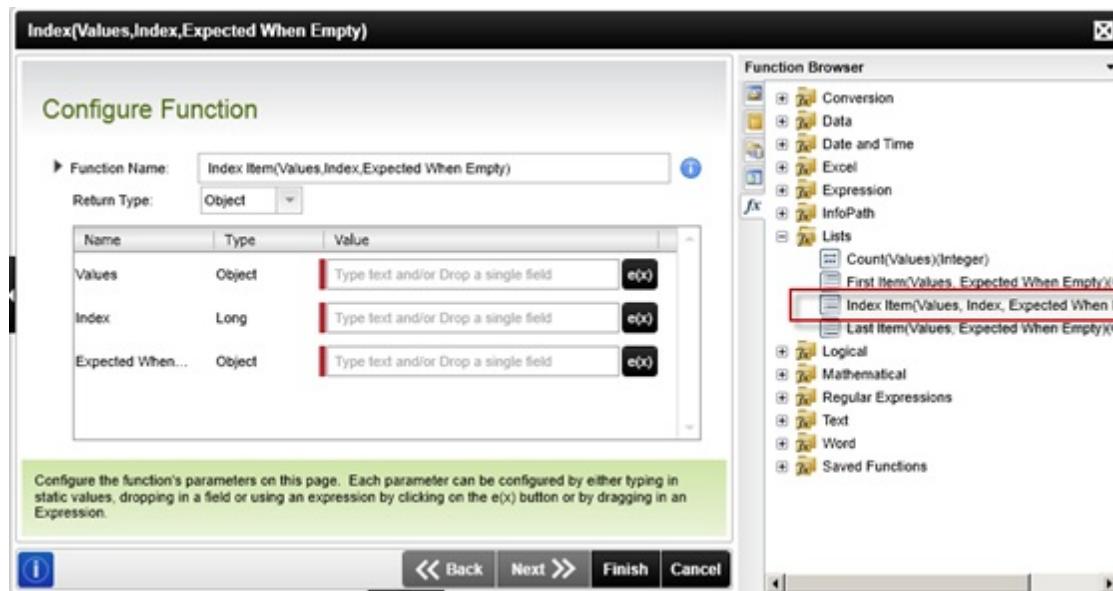
Configure the function's parameters on this page. Each parameter can be configured by either typing in static values, dropping in a field or using an expression by clicking on the e(x) button or by dragging in an Expression.

Back Next > Finish Cancel

For more information, see [Conversion](#)

In addition to the specific user conversion functions the standard Text and List functions, such as Split, Join and Index, can be used to parse the SharePoint Claim User string for values such as the identity provider and identity claims. The SharePoint claims user value for Bob using the Forms Authentication provider will be in the following format: **i:0#.f|ldapmembershipprovider|bob**.

The Index inline function will provide access to the third element in the array that we create by using the Split function to retrieve the elements between the pipe ("|") character.



The Values will be the results of the Split function using the | character as the separator.



The Index is set to 3 to retrieve the identity claim value.

Index(Values,Index,Expected When Empty)

Configure Function

▶ Function Name: `Index Item(Split(i:0#.f|ldapmembershipprovider|bob,),3,unknown)` i

Return Type: Object ▼

Name	Type	Value
Values	Object	<code>Split(i:0#.f ldapmembershipprovider bob,)</code> e(x)
Index	Long	3 e(x)
Expected When...	Object	unknown e(x)

Configure the function's parameters on this page. Each parameter can be configured by either typing in static values, dropping in a field or using an expression by clicking on the e(x) button or by dragging in an Expression.

i << Back Next >> Finish Cancel

The result of this inline function at runtime will be just the identity claim value portion of the SharePoint claims user.

`Index Item(Split(i:0#.f|ldapmembershipprovider|bob,),3,unknown)`

For more information on SharePoint claims users encoding, see the [AttributeValue](#) topic in the [SharePoint Security Token Service Web Service Protocol Specification](#): [http://msdn.microsoft.com/en-us/library/dd932259\(v=office.12\).aspx](http://msdn.microsoft.com/en-us/library/dd932259(v=office.12).aspx).



K2 recommends using the user Conversion functions (To K2 FQN User and To SharePoint Claims User) when working with claims based authentication users in K2 or SharePoint

1.6.8.1.6.6 InfoPath Integration

InfoPath Integration

InfoPath forms published to SharePoint Form Libraries introduce new requirements when the form libraries are on claims authentication sites. It is necessary to understand these requirements to properly utilize K2 InfoPath integration with claims authentication based form libraries. The following topics cover the requirements and the steps required:

[InfoPath Form Services](#)

[InfoPath Client](#)

[Troubleshooting](#)

1.6.8.1.6.6.1 InfoPath Forms Services

InfoPath Forms Services

InfoPath Forms that utilize InfoPath Forms Services (IPFS) require the use of an IPFS Web service proxy to execute external data source Web services from claims authentication sites.

The following steps will enable InfoPath Forms Services Web service proxy in your environment.

Enable InfoPath Form Services Web Service Proxy

Via PowerShell

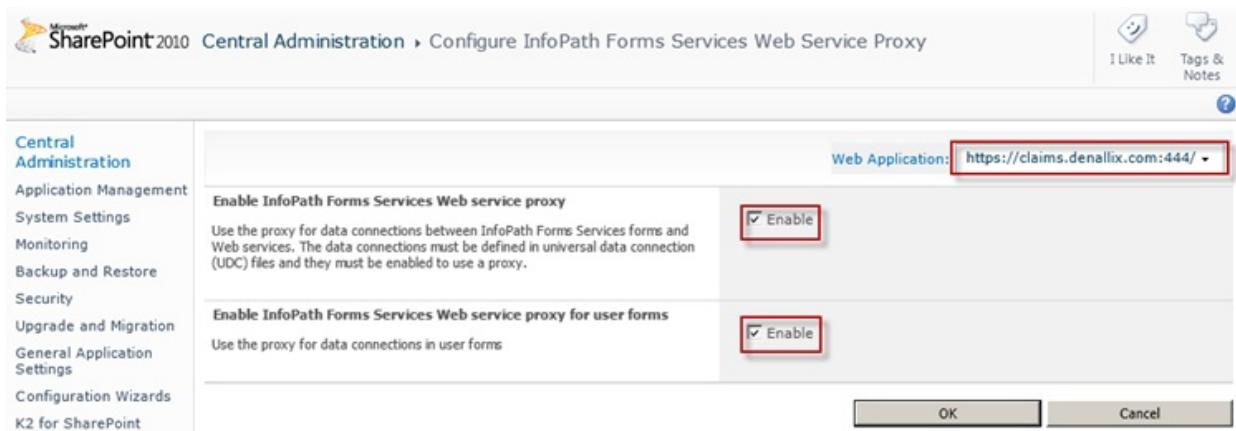
1. Start SharePoint 2010 Management Shell
2. Replace {WebAppURL} in the script below with the URL to the claims authentication web application
3. Run the script

```
Copy Script

Add-PsSnapin Microsoft.SharePoint.PowerShell
Set-SPInfoPathWebServiceProxy -Identity {WebAppURL} -
AllowWebServiceProxy $true
Set-SPInfoPathWebServiceProxy -Identity {WebAppURL} -
AllowForUserForms $true
```

Via Central Administration

1. Navigate to Central Administration > General Application Settings > Configure InfoPath Forms Services Web Service Proxy
 - Web Application: {select the appropriate web application}
 - Enable InfoPath Forms Services Web service proxy: Checked
 - Enable InfoPath Forms Services Web service proxy for user forms: Checked



Register Claims Web Site Certificates

InfoPath Forms Services Web service proxy must have access to the certificates utilized by the web application using claims authentication's web site when it is enabled for SSL.

NOTE: All the certificates in the Certification Path must be registered.

The following steps will register a certificate with one parent certificate in the certification path. Adjust the scripts based on the certification path.

1. Retrieve the required certificates in the DER encoded binary X.509 (CER) file format for import into SharePoint 2010. The method required to export the certificates may vary depending on environment. Steps 1 a-g will illustrate how to export the certificates for a claims authentication web site on IIS 7.
 - a. Start Internet Information Services (IIS) Manager
 - b. Select Server Certificates from the Features View
 - c. Select the certificate associated with the web site enabled for claims authentication and select View...
 - d. Select the Details tab for the certificate and click the Copy To File... button
 - e. The Certificate Export Wizard will start. Navigate through the wizard using the following values.
 - Export Private Key: No, do not export the private key
 - Export File Format: DER encoded binary X.509 (CER)
 - File to Export: Specify a {CertificateFilePath}
 - f. Once the file has been exported, select the Certification Path tab

- g. Double click on any other certificates in the certification path and repeat steps 1.d and 1.e for each one.
2. Start SharePoint 2010 Management Console
 3. Replace `{CertificationFilePath}` and `{CertificationParentFilePath}` in the script below with the path to the claims authentication site certificates.

```

 Copy Script

# Register the claims site certificates for IPFS Web services proxy
calls
$root = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("
{CertificationFilePath}")
New-SPTtrustedRootAuthority -Name "Claims Site Certificate Parent" -
Certificate $root

$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("
{CertificationParentFilePath}")
New-SPTtrustedRootAuthority -Name "Claims Site Certificate" -
Certificate $cert

iisreset

```

K2 Form Client Options

InfoPath client applications cannot use a data connection (UDCX) that is configured to use the Web service proxy – this only works for IPFS forms. Unfortunately, the UDCX does not support the option to use the Web service proxy from IPFS and not use the proxy from InfoPath Client – it is locked to one or the other. Therefore, the option that K2 integration provides to enable the Form Client to utilize “InfoPath, Web browser if InfoPath not available” cannot be supported for InfoPath forms on claims authentication sites. This issue has been logged with Microsoft but a resolution is outstanding.

Edit the InfoPath Form Template

InfoPath Form Deployment Location

Specify where the form should be deployed

Publish to:

Specify the location details

SharePoint Site URL: ...

Form Library: ...

Add as library template Add as content type

Form Client:

Specify the location where the InfoPath form template must be published to, when the project is deployed.

 Back Next > Finish Cancel

If this option is selected, the data connection will be configured to only support InfoPath client when deploying to a claims authentication site. The form will not function properly if opened in the browser. If browser support is desired on a claims authentication site, you must select Web browser and redeploy your solution.

1.6.8.1.6.6.2 InfoPath Client

InfoPath Client

InfoPath Client Office applications, including InfoPath, look for authentication cookies in the persistent store when they are opened from SharePoint. When the cookie is not found, a login prompt is presented to the user in the Office application to get the cookie for that session.

InfoPath has an issue with cookie retrieval that causes the cookies to be retrieved incorrectly and the login prompt not appearing when using InfoPath from a SharePoint Form Library that has been configured to "Open in the client application" (InfoPath 2007 or InfoPath 2010 Filler). This issue has been logged with Microsoft but a resolution is outstanding. This topic provides workaround details to enable InfoPath client applications to work properly with SharePoint 2010 claims authentication.

The issue manifests in one of two ways depending on the SharePoint Server configuration of the `UseSessionCookies` value. To determine which setting you currently have, run the following command from a SharePoint 2010 Management Shell.



Copy Command

```
(Get-SPSecurityTokenServiceConfig).UseSessionCookies
```

This will return either False (the default and preferred option) or True. Refer to the section that matches your configuration for more details on working with InfoPath client in your environment.

`UseSessionCookies=False`

This setting causes SharePoint to write the `FedAuth` cookie value to the local cookies folder on the client. However, the default forms authentication login page provides the ability to override this value causing the cookie to not be persisted to disk. The "Sign me in automatically" check box determines if the cookie is persisted or not. When it is checked the cookie is persisted, otherwise it is not.

To ensure that the `FedAuth` cookie is correctly passed from SharePoint to the Office client applications, such as InfoPath Filler, the cookie needs to be persisted to disk. To make this happen, the "Sign me in automatically" check box must be **checked**.



Sign In

User name: bob

Password: *****

Sign me in automatically

Optional Configuration – Sign in Automatically by Default

You may prefer to change the default login page to ensure that the **Sign me in automatically** option is checked by default.



WARNING: The steps below are provided for illustrative purposes. A custom login page should be created and registered to ensure compatibility with future upgrades.

1. Backup "C:\inetpub\wwwroot\wss\VirtualDirectories\{Your Claims WebApp Directory}_forms\Default.aspx"
2. Open "C:\inetpub\wwwroot\wss\VirtualDirectories\{Your Claims WebApp Directory}_forms\Default.aspx"
3. Add this script block after the `</asp:login>` control



Copy Script

```
<script type="text/javascript" language="javascript" >
document.getElementById("ctl00_PlaceHolderMainSignInControl_RememberMe").checked
= true;
</script>
```

UseSessionCookies=True

This setting causes SharePoint to store the FedAuth cookie value in the browser's local cache. This cache is not available to Office client applications, forcing them to create their own FedAuth cookie via a login prompt. However, InfoPath may incorrectly try to use an existing cookie, potentially from a different form-based user, from the local cache which will cause errors when interacting with web services.

Workaround Option 1 – Set UseSessionCookies to False

The preferred option when using SharePoint 2010 with Office client applications is to configure SharePoint to **not** use session cookies and follow the guidance in the **UseSessionCookies=False** section. If this is not possible in your environment, see **Workaround Option 2**.

1. Start SharePoint 2010 Management Console
2. Execute the following commands



Copy Command

```
$sts = Get-SPSecurityTokenServiceConfig
$sts.UseSessionCookies = $false
$sts.Update()
iisreset
```

Workaround Option 2

To ensure that all web service calls from InfoPath Filler are executed with the correct FedAuth cookie, you must make a call to the SharePoint List and Library service in InfoPath. The communication with this service correctly forces InfoPath to provide a login prompt to get the FedAuth cookie with the current user's information.

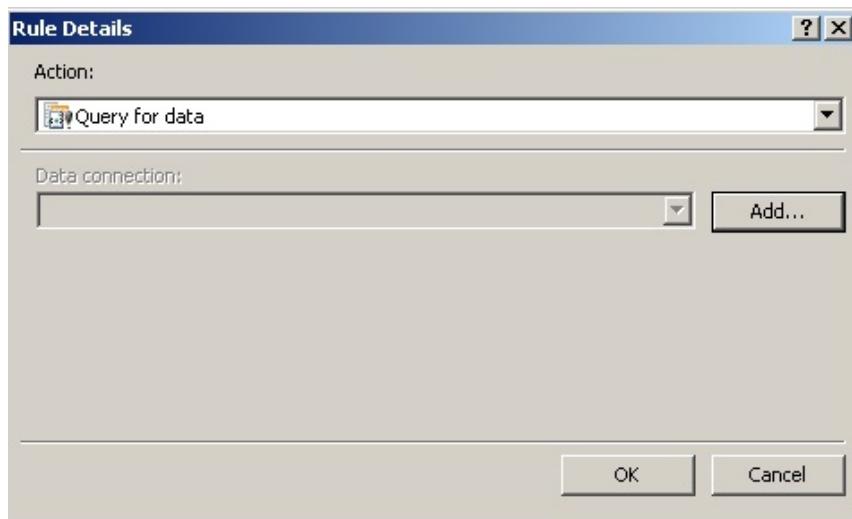


Sign In

Select the credentials you want to use to logon to this SharePoint site:



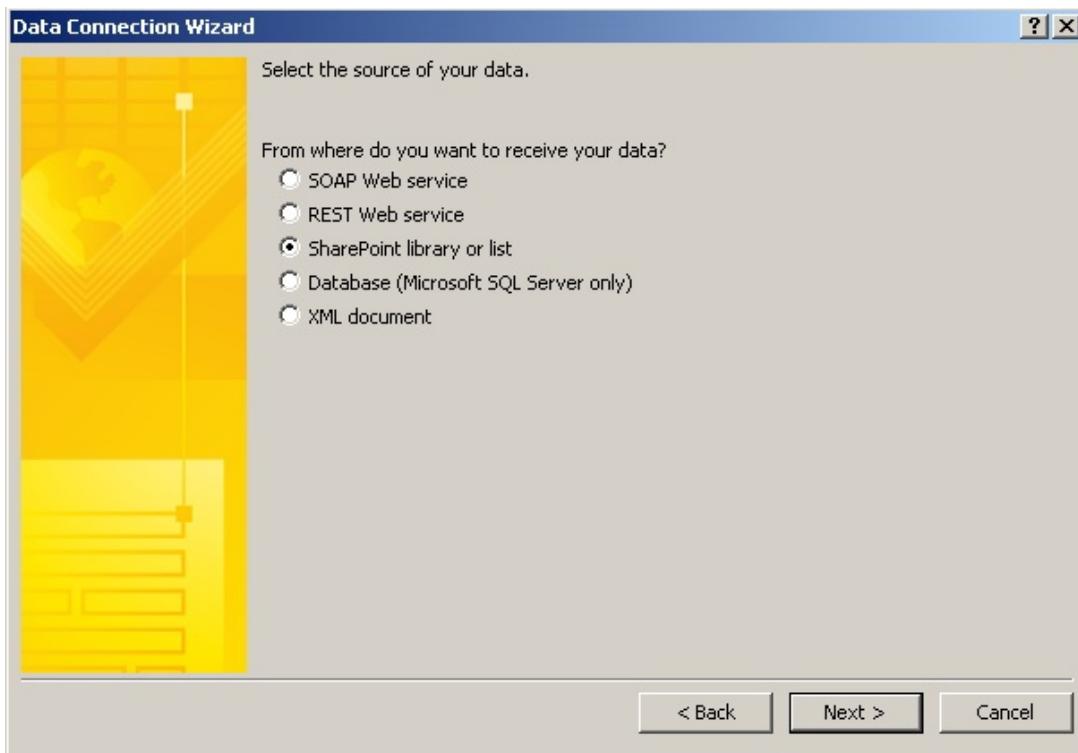
1. Open the InfoPath form in Design mode:
 - a. Before integrating with K2, via the InfoPath designer directly
 - b. After integrating with K2, open the form in K2 Studio or Visual Studio via the InfoPath Process Wizard Design button
2. Access the Form Load Rules
3. Add a new Action rule that will run when the form is opened
4. Add Query for Data action



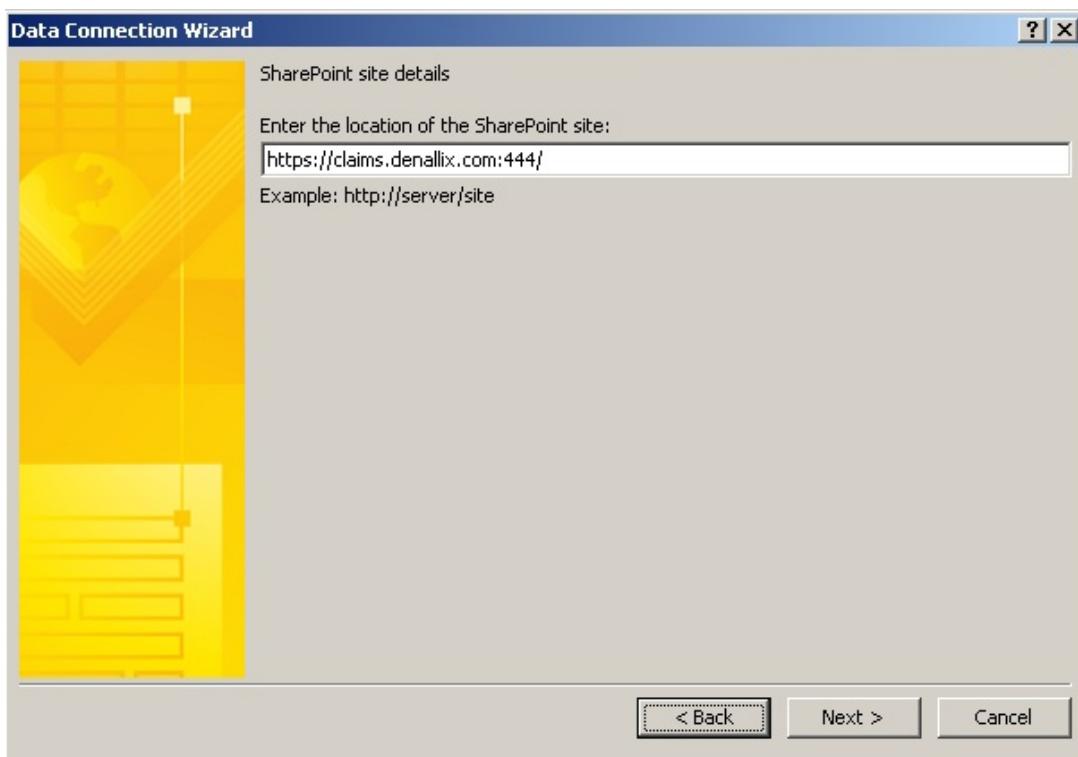
5. Create a new connection to: Receive data



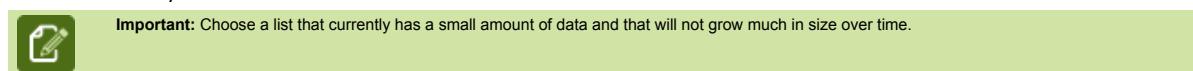
6. Select SharePoint library or list as your source of data

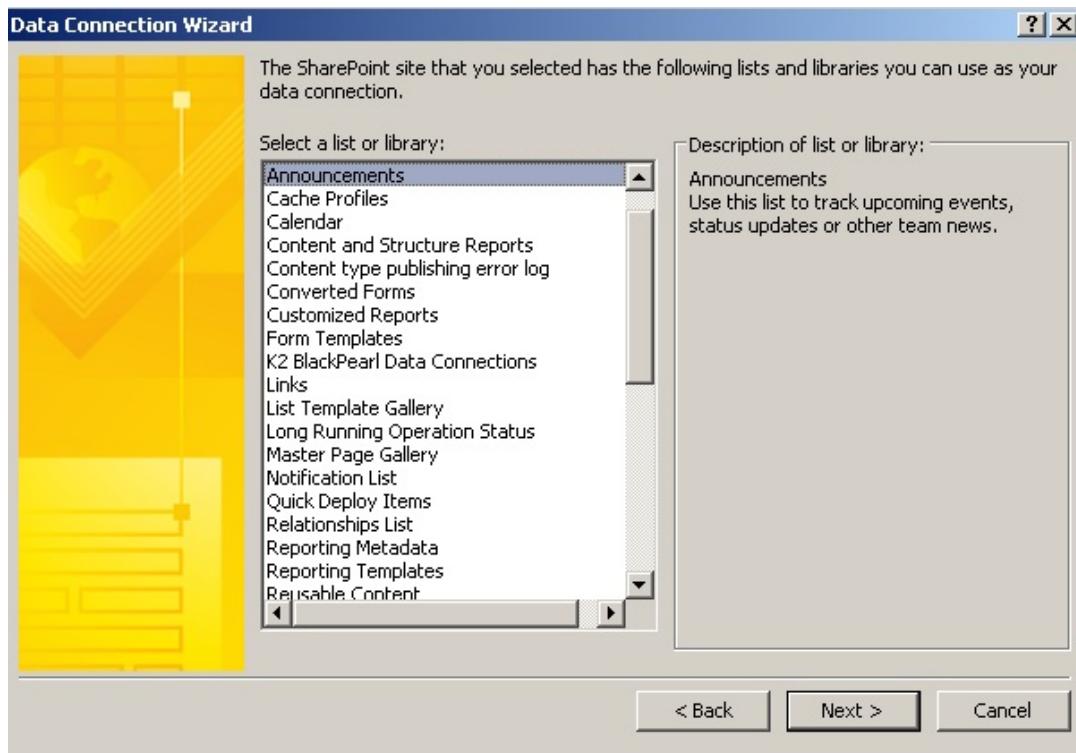


7. Provide your SharePoint site details

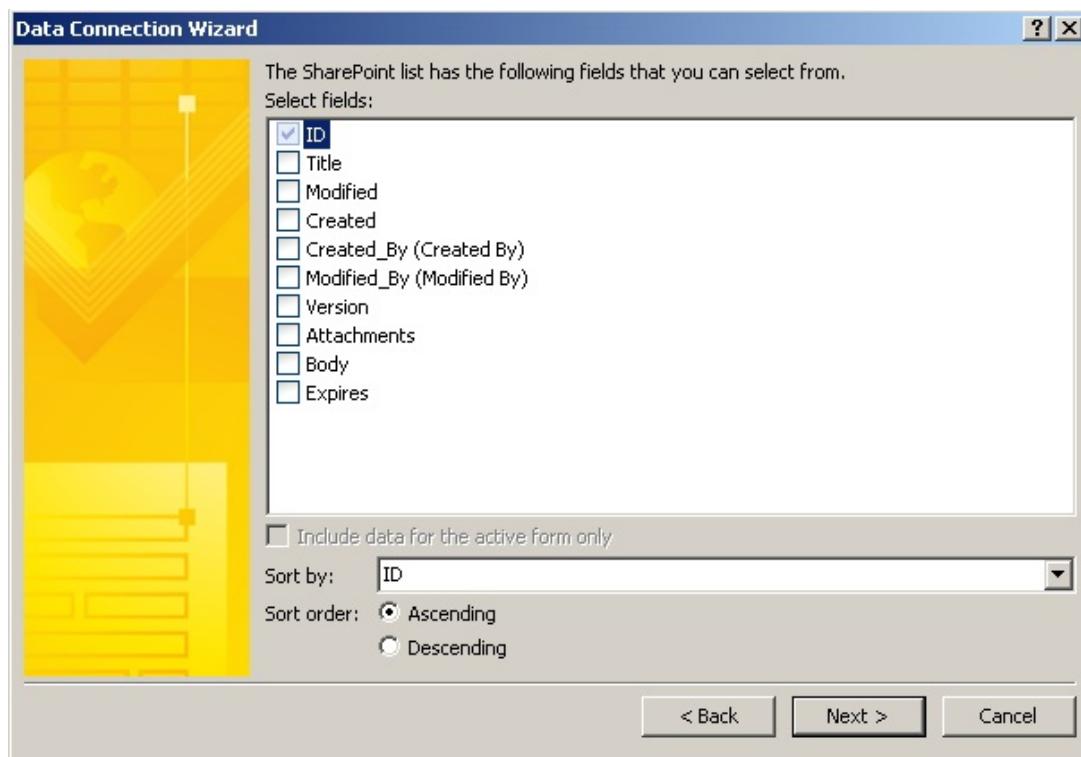


8. Select a list or library that has limited data and that all users will have access to such as Announcements.

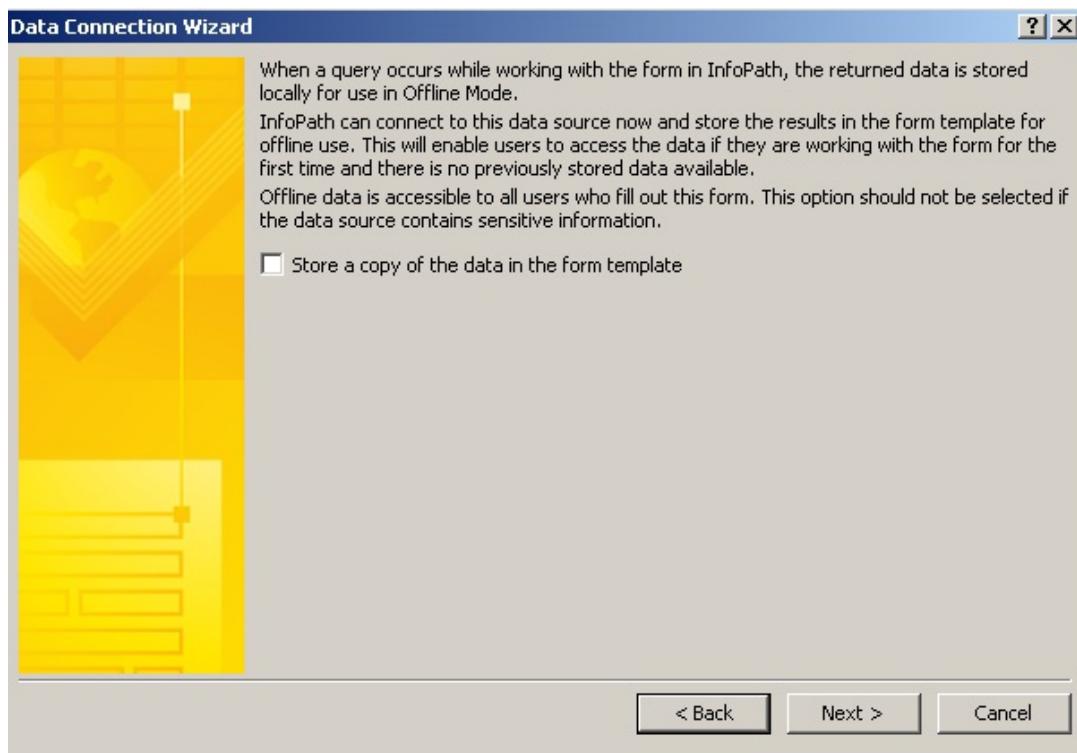




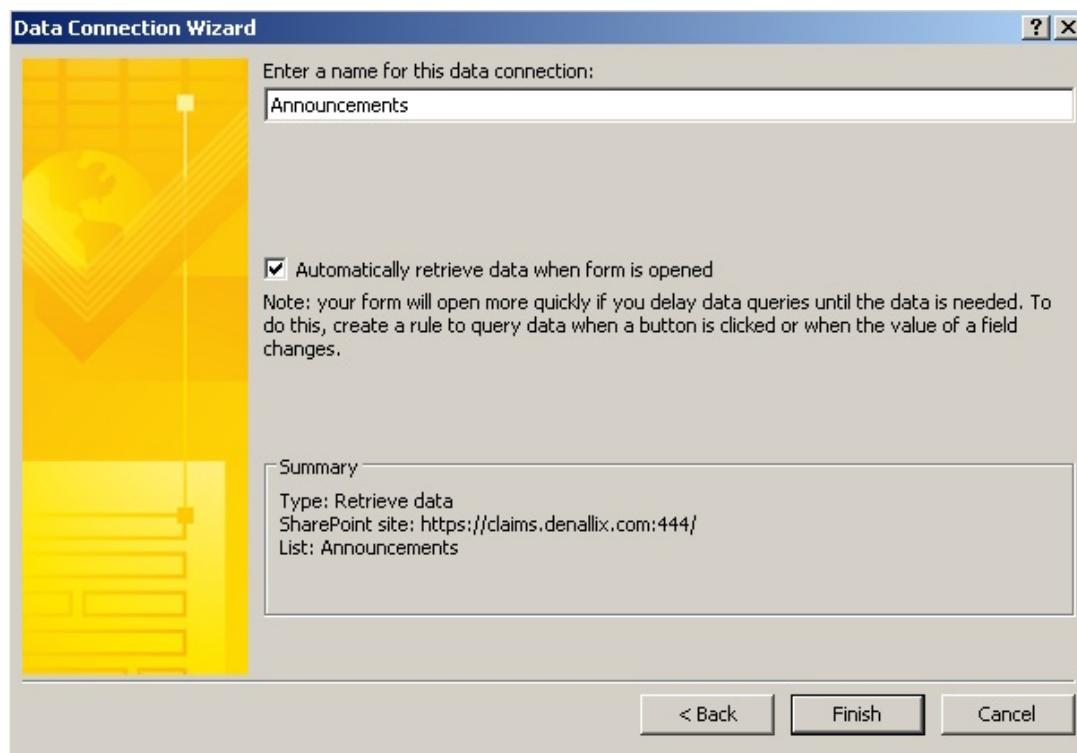
9. Leave the default ID selected on Select fields



10. Do **not** select the option to Store a copy of the data in the form template



11. Select the option to **Automatically retrieve data when form is opened**



12. Save the form
 13. Publish the form
 - a. From InfoPath designer, publish as you did before
 - b. From K2 Studio or Visual Studio
 - i. Close InfoPath designer and wait for the confirmation that your process changes have been received



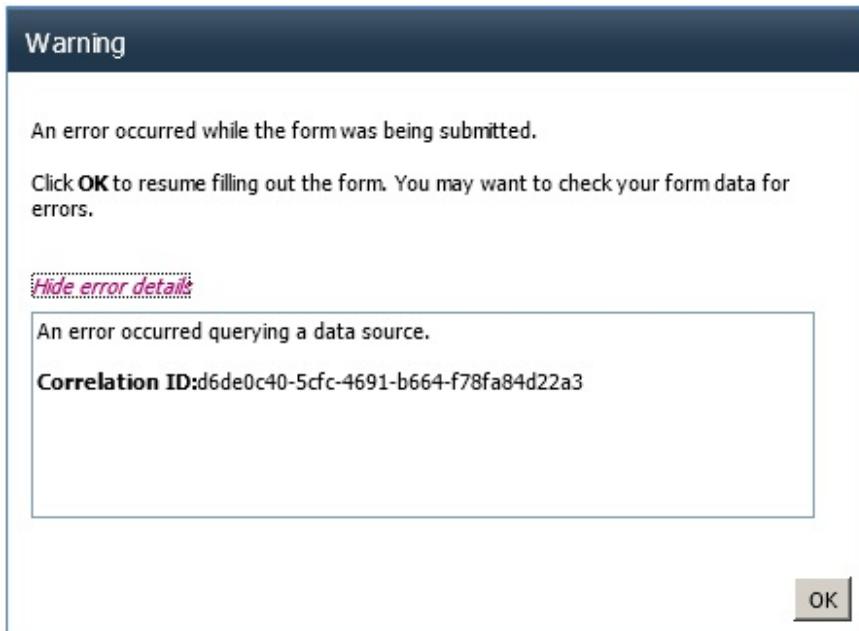
ii. Redeploy the process

1.6.8.1.6.6.3 Troubleshooting

Troubleshooting

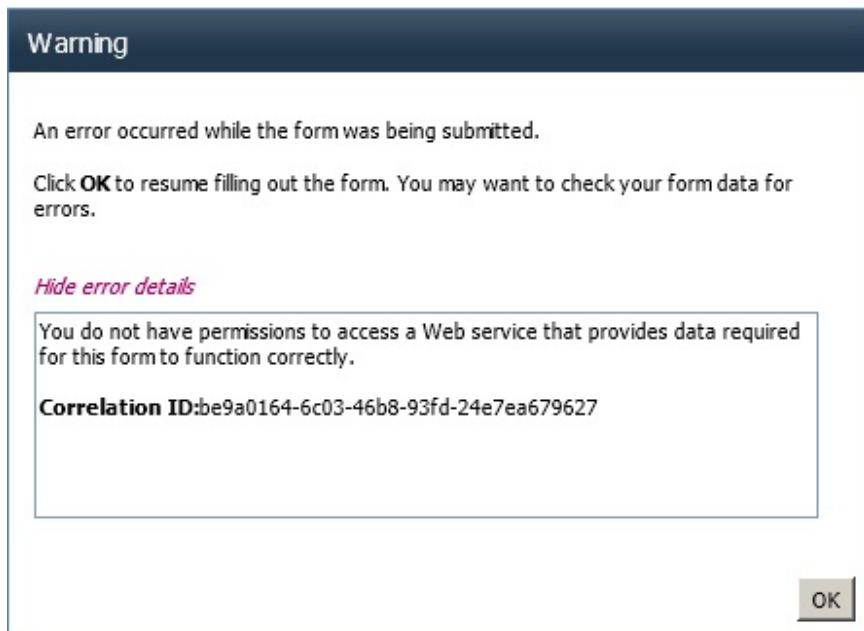
Verify the InfoPath, InfoPath Forms Services and K2 Form Client configurations if any of the following errors occur.

- Error: An error occurred querying a data source.**



This error can occur when the InfoPath form has been configured for IPFS support and the IPFS Web service proxy has not been configured. Review the [Enable InfoPath Forms Services Web Service Proxy](#) section for more details.

- Error: You do not have permissions to access a Web service that provides data required for this form to function correctly.**



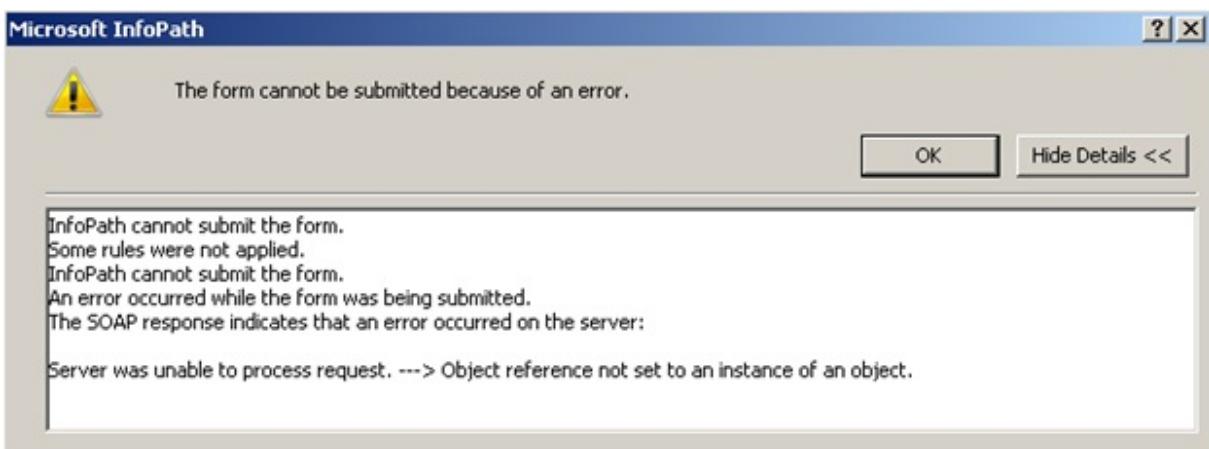
Error in ULS log:

Server was unable to process request. ---> There was no endpoint listening at <https://dlx:32844/542b89d09b5e49778e7d978780786c9e/SecureStoreService.svc/https> that could accept the message. This is often caused by an incorrect address or SOAP

action. See InnerException, if present, for more details. ---> The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel. ---> The remote certificate is invalid according to the validation procedure.

This error can occur when the InfoPath form has been configured for IPFS support and the InfoPath Forms Services Web service proxy service does not have access to the certificates utilized by the web application using claims authentication when it is **enabled for SSL**. Review the [Register Claims Web Site Certificates](#) section for more details.

3. **Error: Server was unable to process request. --> Object reference not set to an instance of an object.**



This error can occur when the InfoPath form has been configured for IPFS support and the form is opened in InfoPath Client. You must explicitly select either InfoPath Client or Web browser support when using InfoPath forms on a claims authentication site. Review the [K2 Form Client Options](#) section for more details.

References

Article	Link
Selecting the "Sign me in automatically" Check Box at Logon	http://msdn.microsoft.com/en-us/library/bb977430(v=office.12).aspx#MOSSFBAPart3_AutomaticSignIn
Persistent cookies are not shared between Internet Explorer and Office applications	http://support.microsoft.com/kb/932118
Office 2010 prompts for credentials despite the use of persistent cookies	http://support.microsoft.com/kb/2538896
SharePoint 2010: Create Custom Login page with persistent cookies	http://atulchhoda.wordpress.com/2010/10/28/wordpress/
Change to session cookies for Claims Based Authentication	http://blog.sharepointsite.co.uk/2010/11/change-to-session-cookies-for-claims.html
Configure Web service proxy for InfoPath Forms Services (SharePoint Server 2010)	http://technet.microsoft.com/en-us/library/ff621101.aspx
About Data Connections, Authentication, and Alternate Access Mapping	http://msdn.microsoft.com/en-us/library/ms771995.aspx
Universal Data Connection v2.0 Reference and	http://msdn.microsoft.com/en-us/library/ms772017.aspx

Schema	
Advanced Server-Side Authentication for Data Connections in InfoPath 2007 Web-Based Forms	http://msdn.microsoft.com/en-us/library/bb787184(v=office.12).aspx

1.6.8.1.6.7 SharePoint People Picker

People Picker

The SharePoint People Picker control can be used to find and select users and groups when assigning permissions to resources such as sites and lists and libraries. K2 uses the People Picker control in several areas such as permission management and task assignment. It is important to understand how the People Picker control resolves special users (aka, All Users) and claims users. For more information, see People Picker overview: <http://technet.microsoft.com/en-us/library/gg602068.aspx>

Resolving Names

The People Picker control has two modes for resolving names. The Check Names (Ctrl+K) option tries to match the provided text against all registered providers for the web site.



When the text provided can be resolved against more than one provider, the text is underlined in red and a list of available providers is presented in a popup when the text is selected.



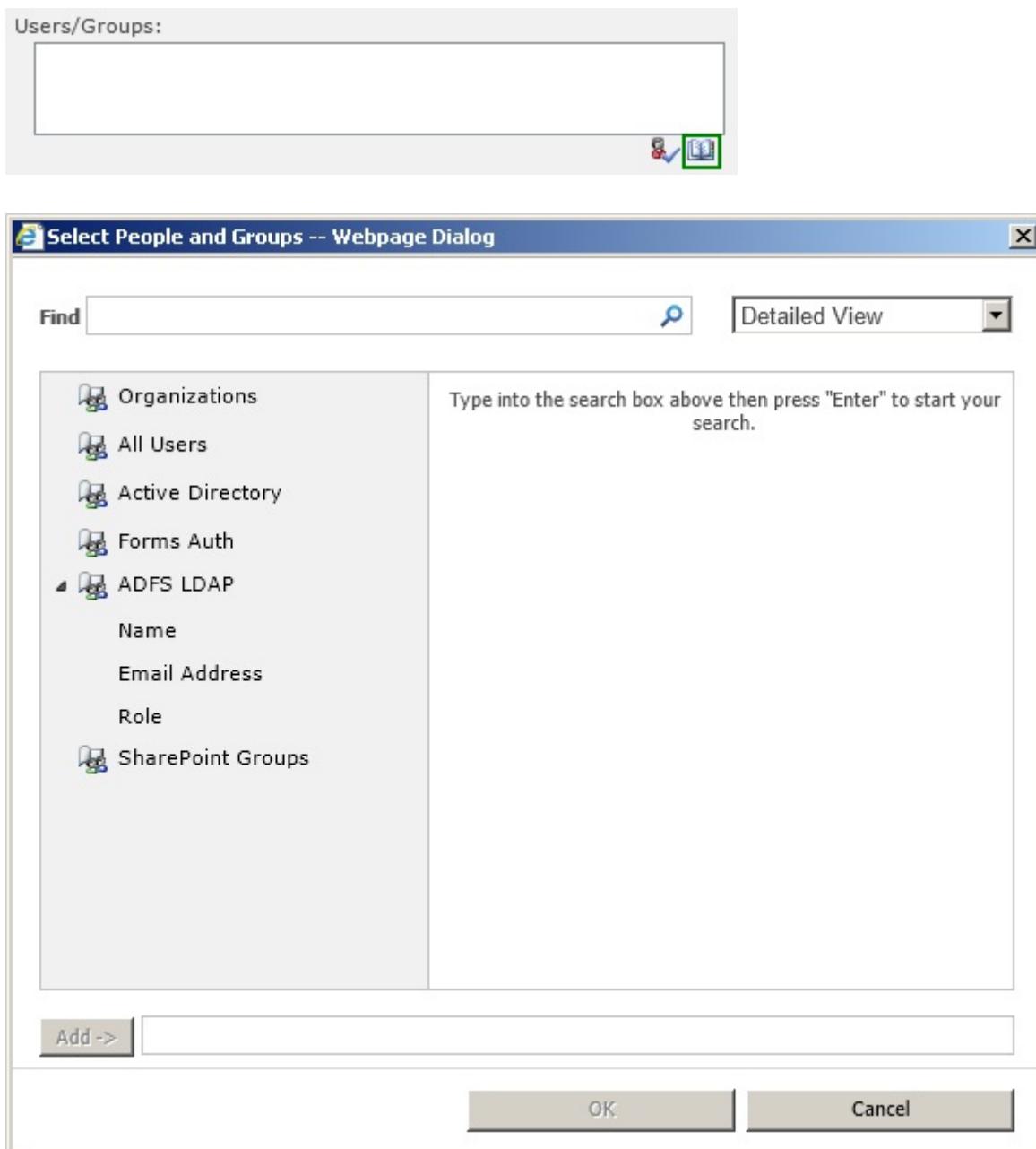
This works well when all the claims providers have implemented search and name resolution. However, when claims providers, such as the default SharePoint provided SPTTrustedClaimProvider, do not implement search and name resolution, all queries entered in the text box are automatically displayed as if they had been resolved, regardless of whether they are valid users or groups.

The following note is taken directly from the SharePoint product documentation. For more information, see Custom claims providers for People Picker (SharePoint Server 2010): <http://technet.microsoft.com/en-us/library/gg602072.aspx>



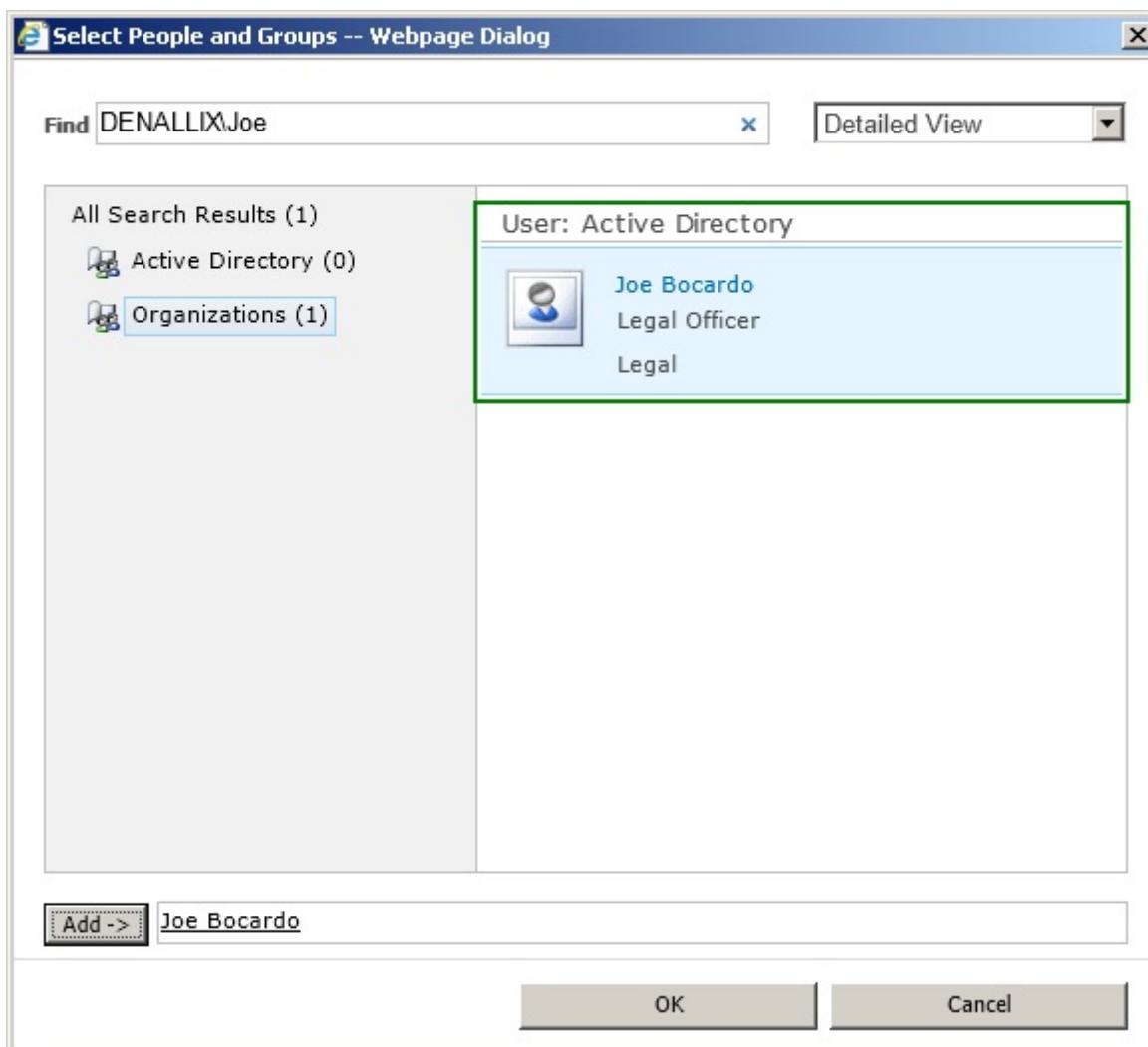
When a Web application is configured to use SAML token-based authentication, the SPTTrustedClaimProvider class does not provide search functionality to the People Picker control. Any text entered in the People Picker control will automatically be displayed as if it had been resolved, regardless of whether it is a valid user, group, or claim. If your SharePoint Server 2010 solution will use SAML token-based authentication, you should plan to create a custom claims provider to implement custom search and name resolution.

It is recommended to utilize the Browse option when using the People Picker to ensure that the appropriate user or group is selected and assigned against the desired provider and claim.

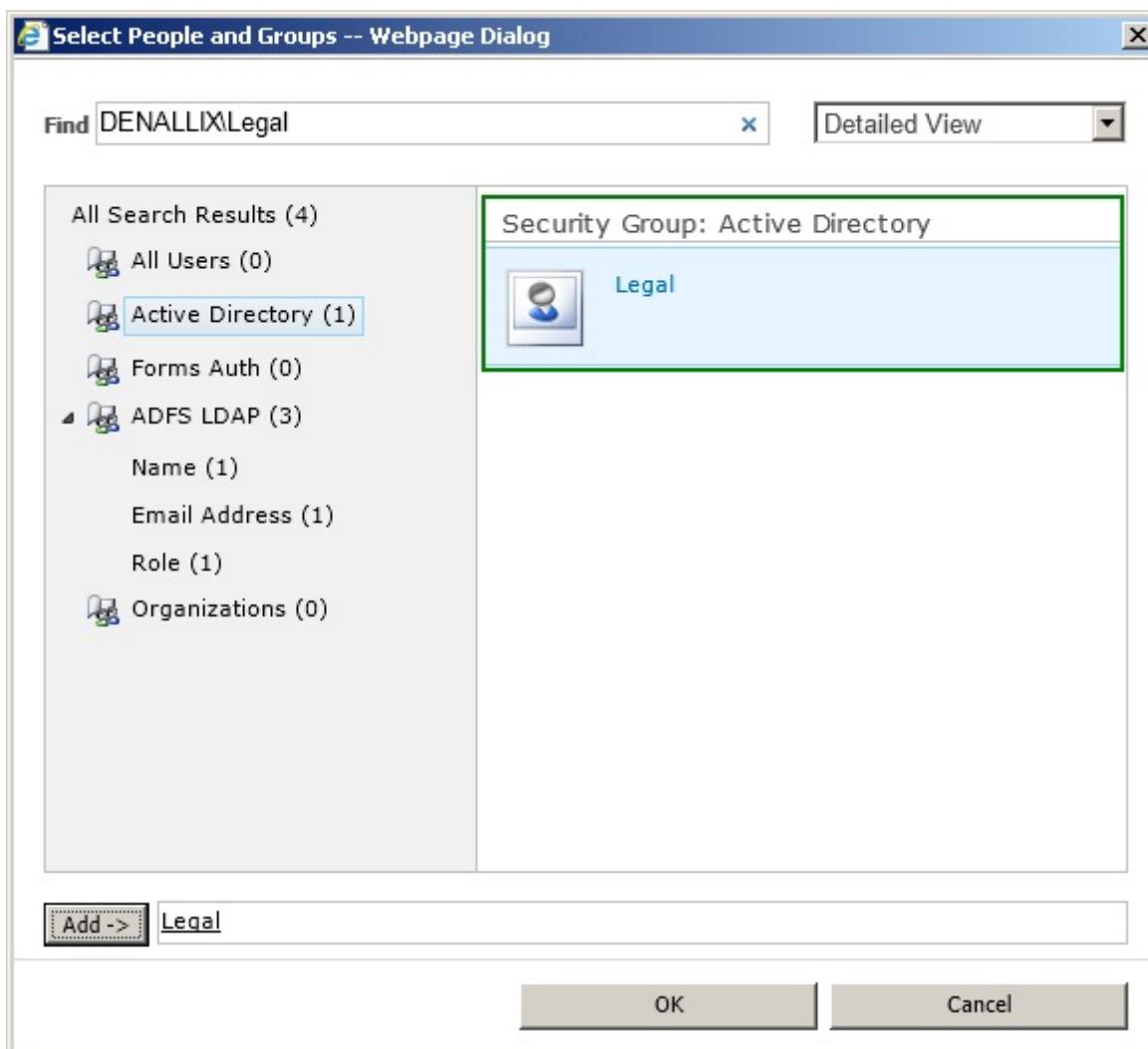


Active Directory Users and Groups

Active Directory users are typically resolved by searching on the Windows user logon name or DOMAIN\Username format. Depending on the People Picker configuration, the user may appear in the Active Directory, the Organizations, or both search results. The key is to ensure that the user selected is the one for the User: Active Directory result.

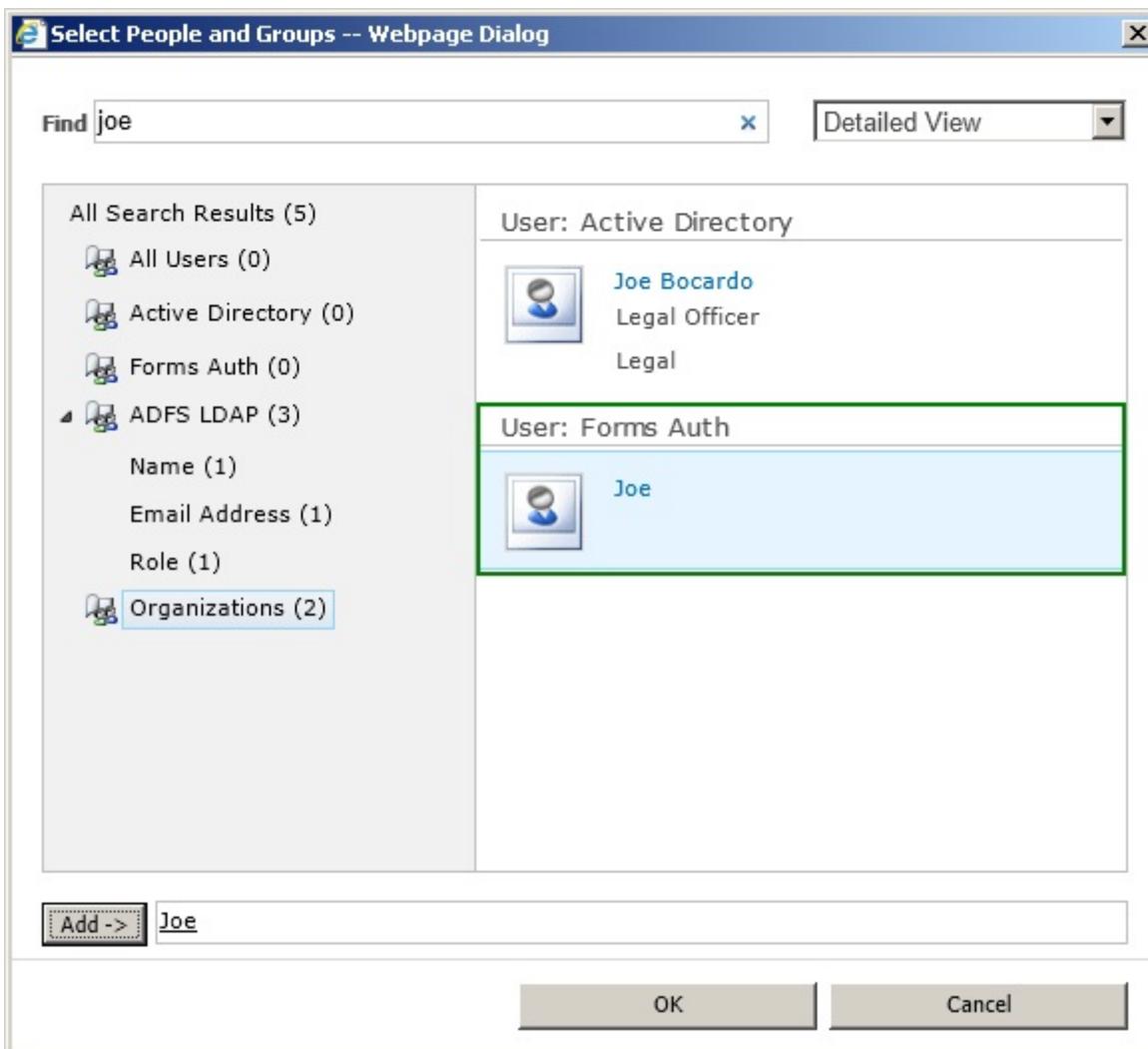


Active Directory *groups* are typically resolved by searching on the Windows group name or DOMAIN\GroupName format. Depending on the People Picker configuration, the group may appear in the Active Directory, the Organization or both search results. The key is to ensure that the group selected is the one for the Security Group: Active Directory result.

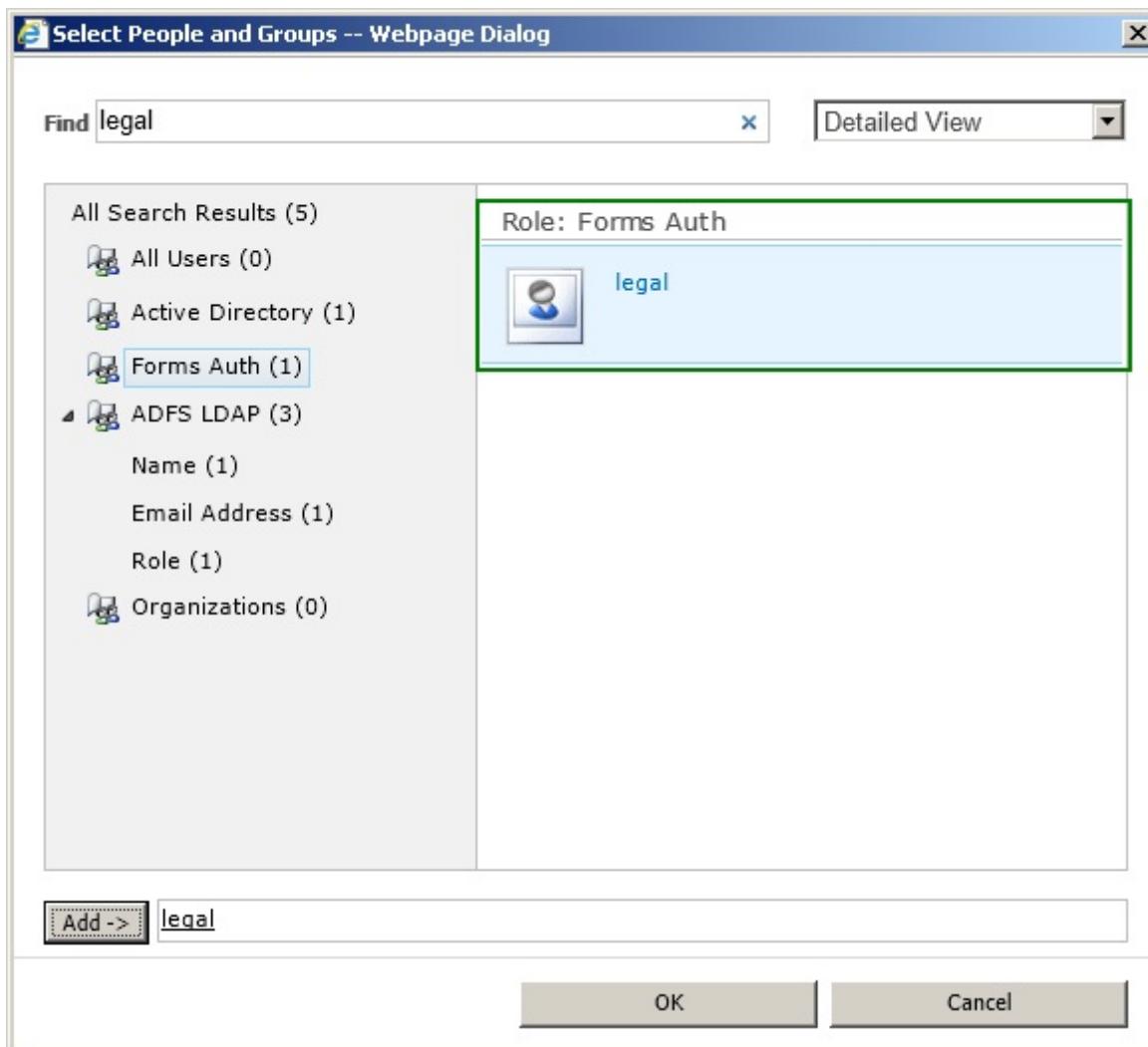


Forms Authentication Users and Groups

Forms-based authenticated users are typically resolved by searching on the user logon name. Depending on the People Picker configuration, the user may appear in the Forms Auth, the Organizations, or both search results. The key is to ensure that the user selected is the one for the User: Forms Auth result.

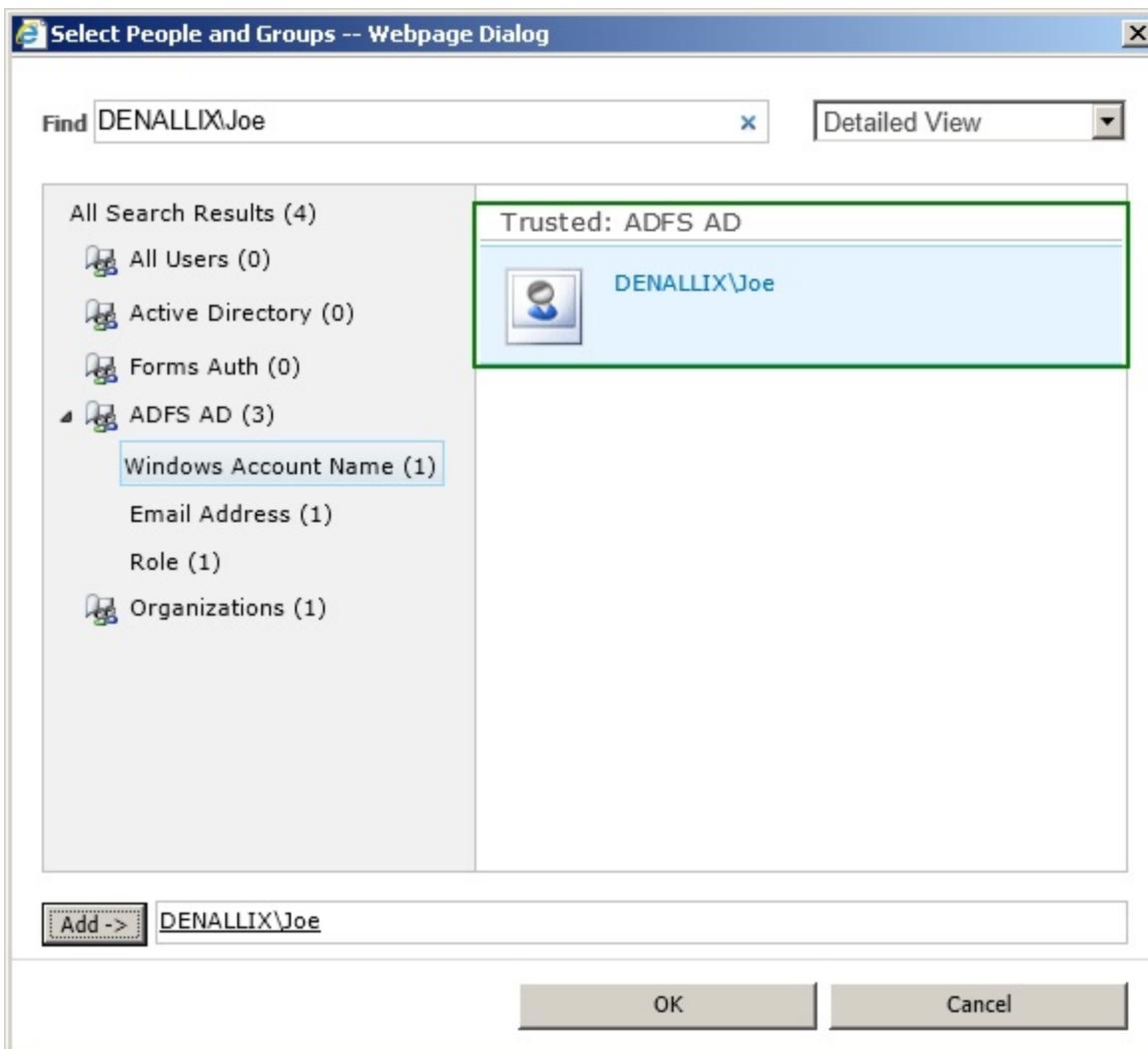


Forms-based authentication *groups* are typically resolved by searching on the group name. Depending on the People Picker configuration, the group may appear in the Forms Auth, the Organizations, or both search results. The key is to ensure that the group selected is the one for the Role: Forms Auth result.

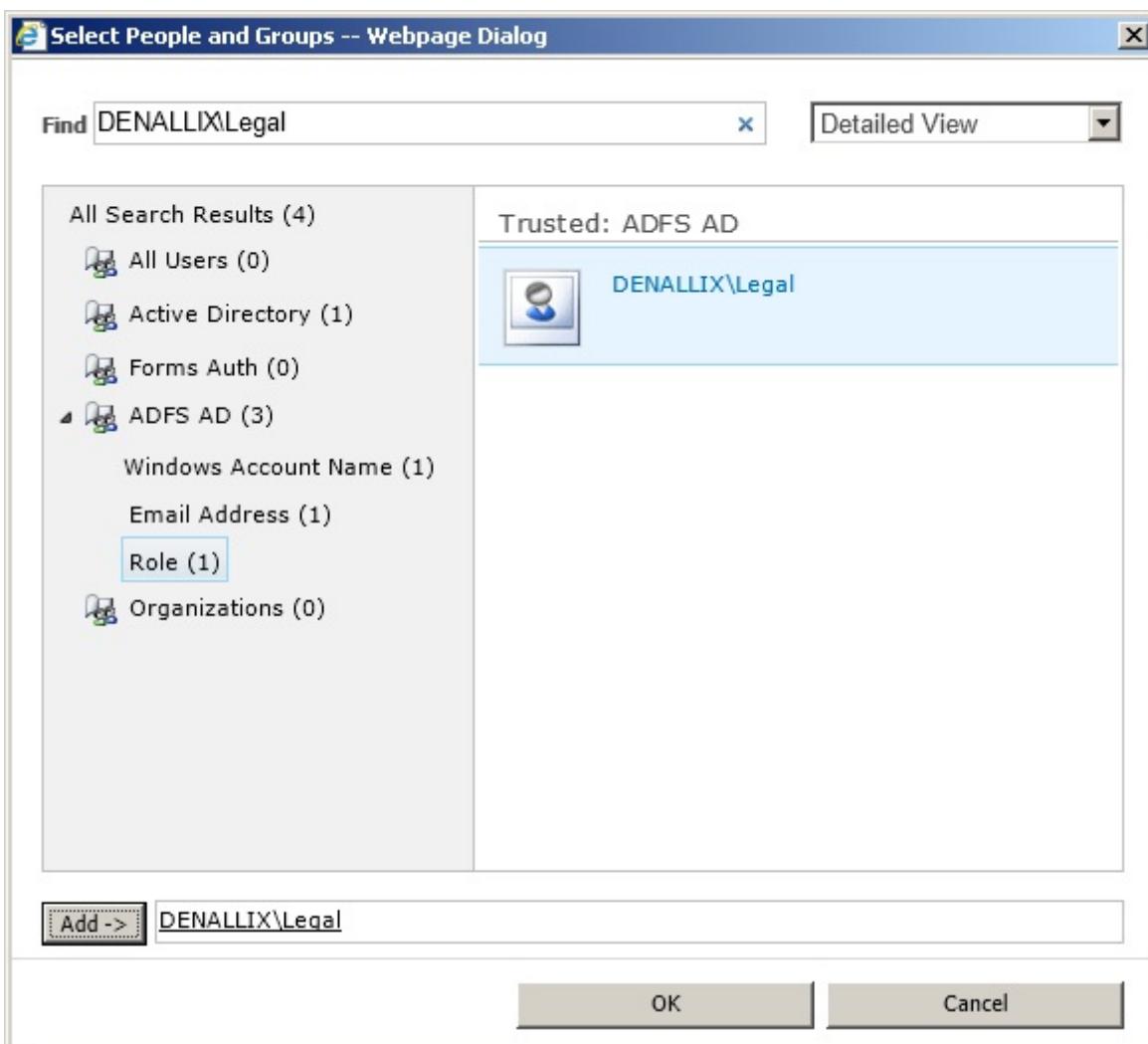


Trusted Provider Users and Groups (AD FS for Active Directory)

Trusted Provider based authentication provided by AD FS configured for the Active Directory attribute store users are typically resolved by searching on the DOMAIN\Username. Depending on the People Picker configuration, the user may appear in the Trusted Provider search results for each claim configured, in this example ADFS AD. The key is to ensure that the user selected is mapped to the search result for the identity claim, in this example Windows Account Name.



Trusted Provider based authentication provided by AD FS configured for the Active Directory attribute store groups are typically resolved by searching on the DOMAIN\GroupName. Depending on the People Picker configuration, the group may appear in the Trusted Provider search results for each claim configured, in this example ADFS AD. The key is to ensure that the group selected is mapped to the search result for the role claim, in this example Role.

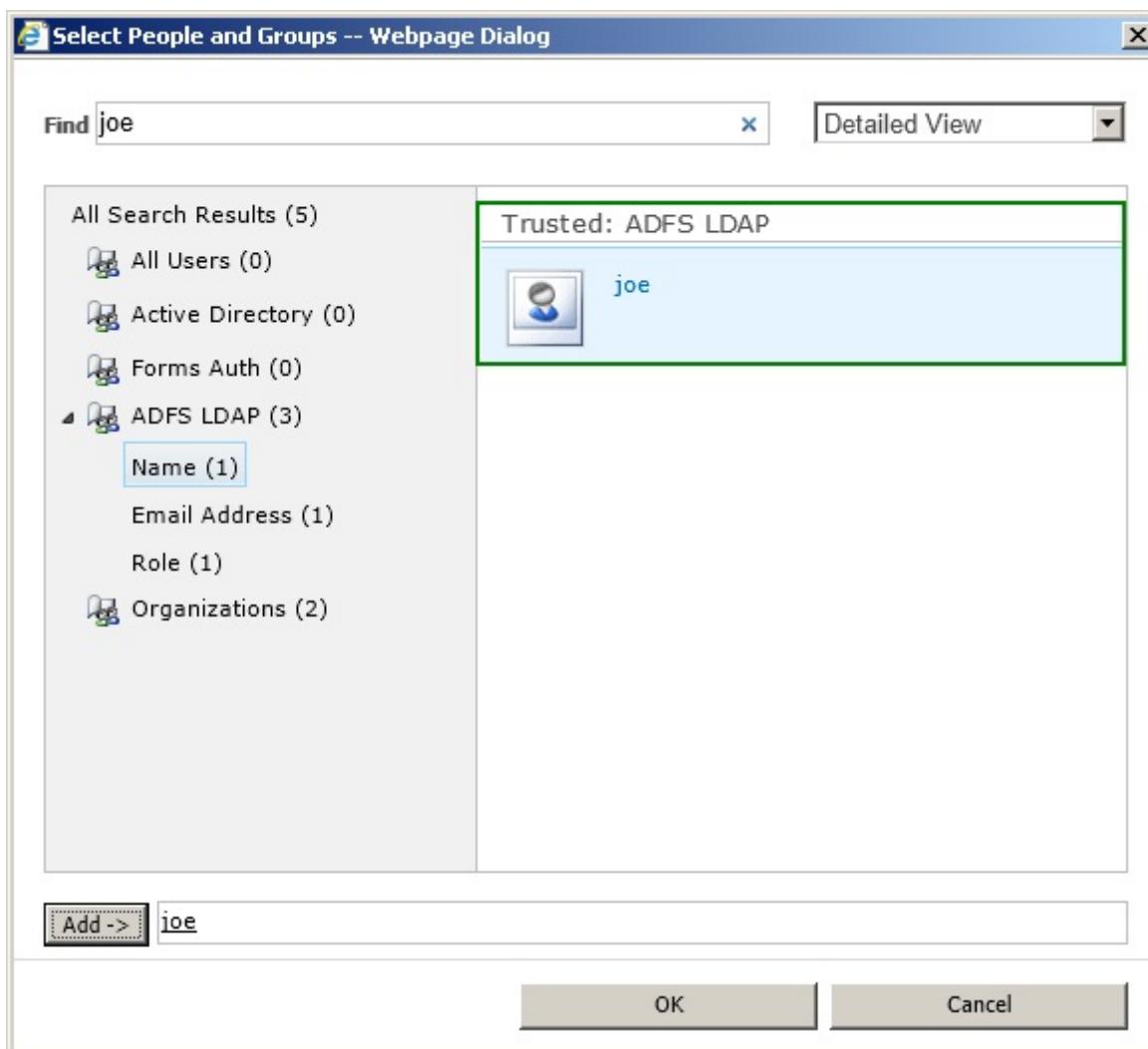


The search text must match the text in claims provided by the trusted provider. For example, if the claim is in the format of DOMAIN\Username or DOMAIN\GroupName then the DOMAIN name must be used when executing the search. If the claim values do not contain the DOMAIN information then omit that when executing the search.

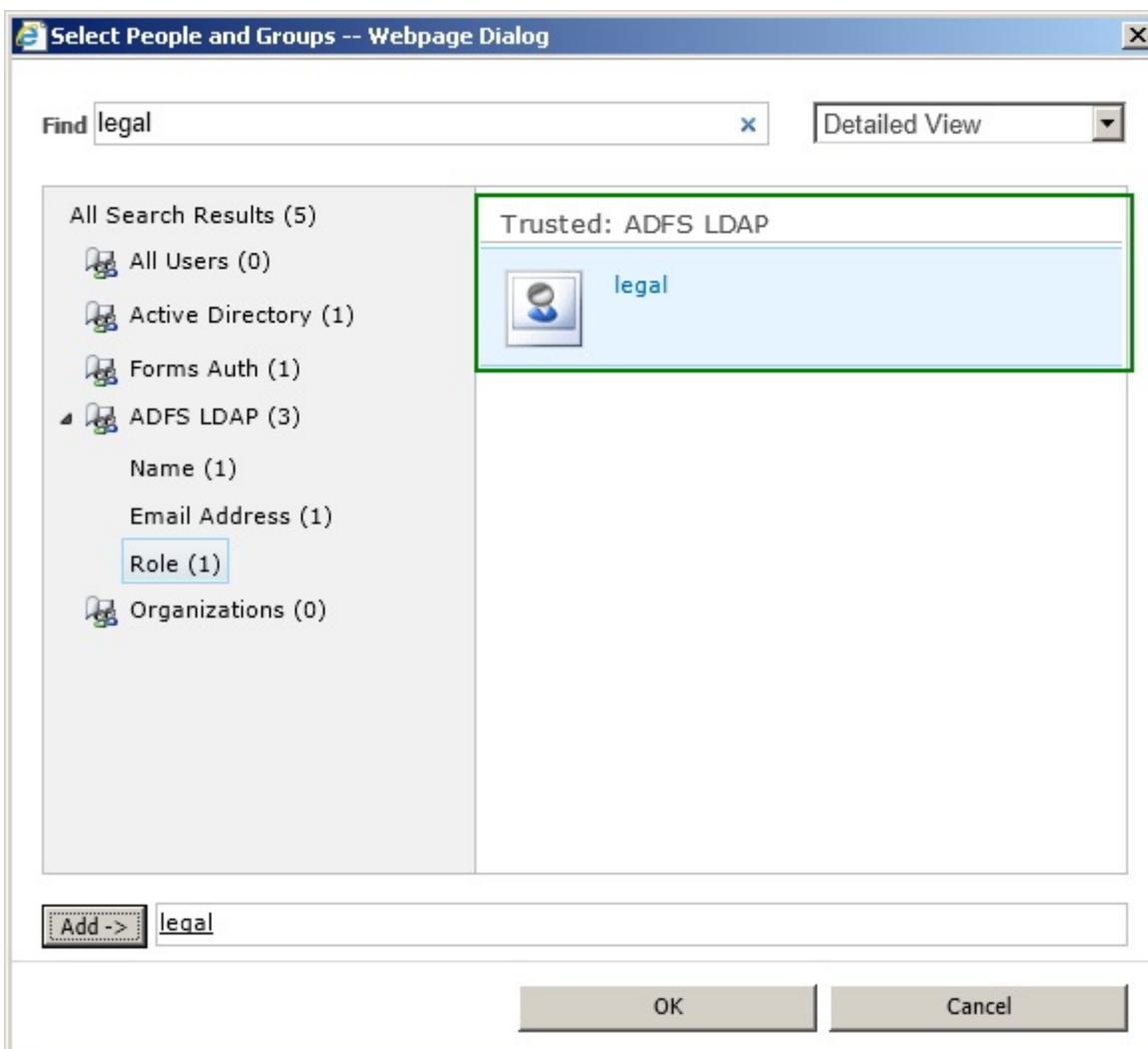
For more information on configuring AD FS for Active Directory, see [Concepts > Integration > SharePoint 2010 > Claims-based Authentication > Supported Configurations](#)

Trusted Provider Users and Groups (AD FS for LDAP)

Trusted Provider based authentication provided by AD FS configured for the LDAP attribute store users are typically resolved by searching on the user logon name. Depending on the People Picker configuration, the user may appear in the Trusted Provider search results for each claim configured, in this example ADFS LDAP. The key is to ensure that the user selected is mapped to the search result for the identity claim, in this example Name.



Trusted Provider based authentication provided by AD FS configured for the LDAP attribute store *groups* are typically resolved by searching on the group name. Depending on the People Picker configuration, the group may appear in the Trusted Provider search results for each claim configured, in this example ADFS LDAP. The key is to ensure that the group selected is mapped to the search result for the role claim, in this example Role.



The search text must match the text in claims provided by the trusted provider. For example, if the claim is in the format of DOMAIN\Username or DOMAIN\GroupName then the DOMAIN name must be used when executing the search. If the claim values do not contain the DOMAIN information then omit that when executing the search.

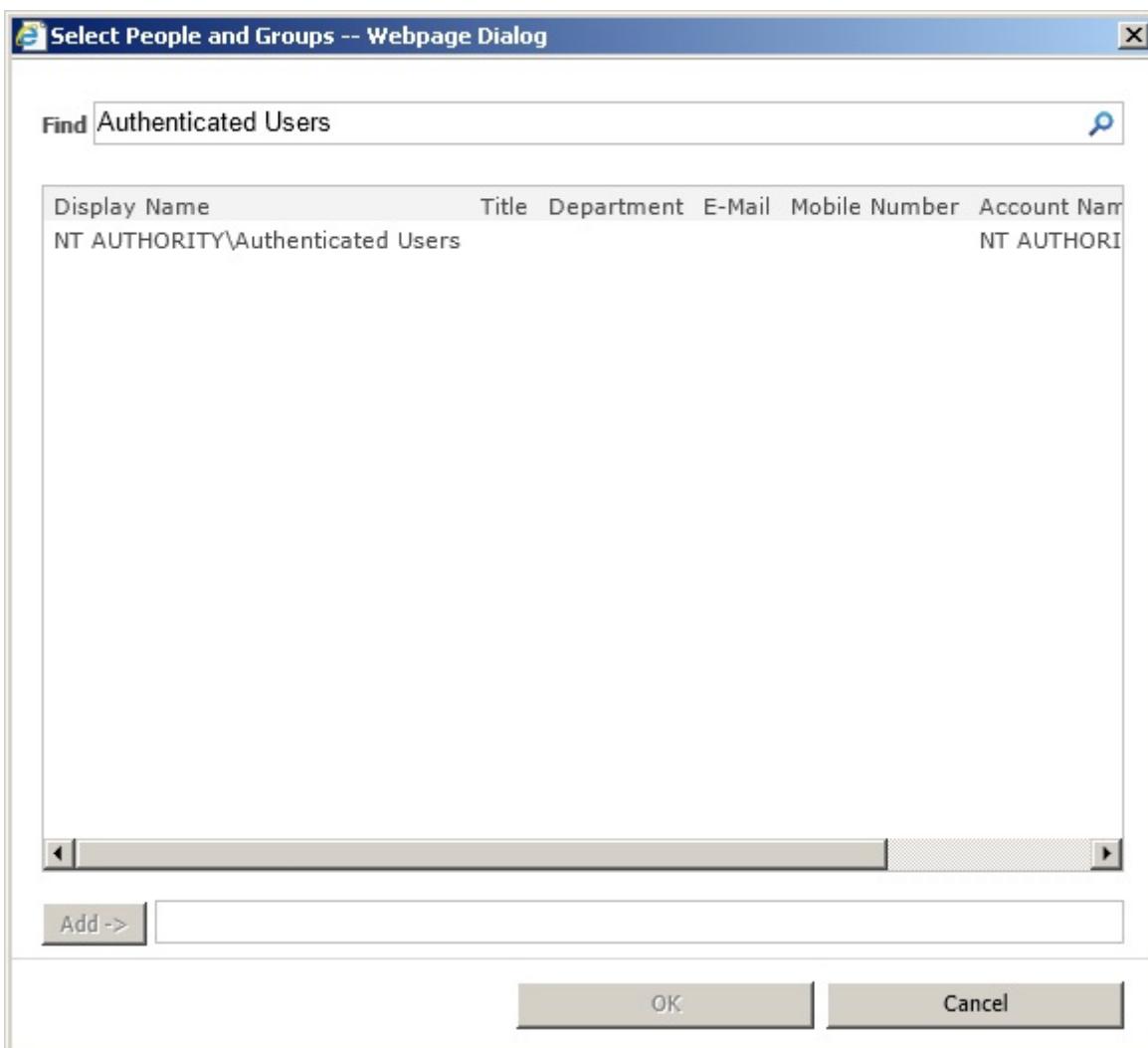
For more information on configuring AD FS for LDAP, see [Concepts > Integration > SharePoint 2010 > Claims-based Authentication > Supported Configurations](#)

All Users

K2 does not support a concept of "All Users" for assigning tasks, interacting with tasks or assigning permissions. Built-in or configured groups for the appropriate K2 user manager, for example Domain Users for Active Directory, must be used instead.

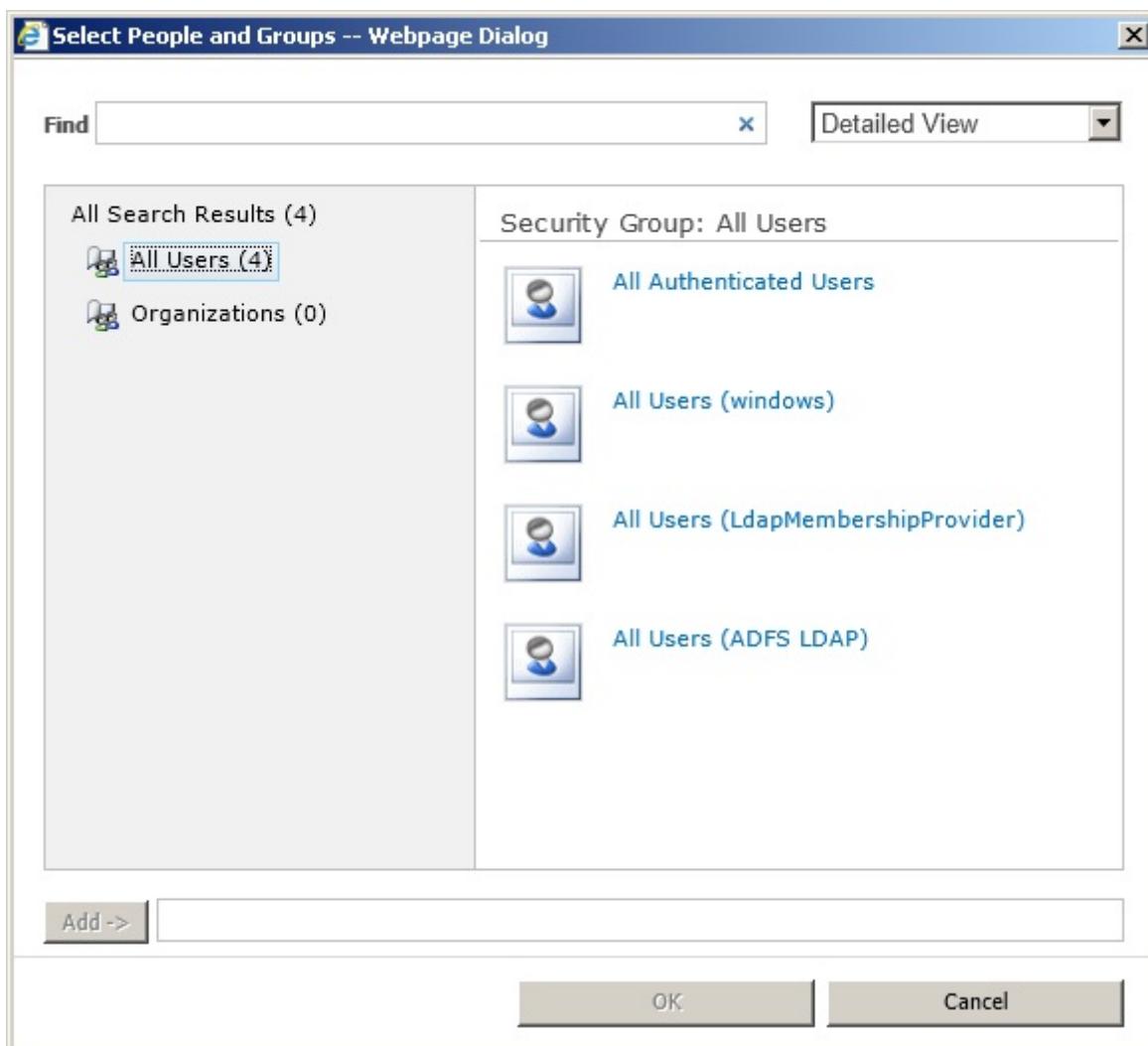
The following "All Users" containers are not supported by K2.

Active Directory, SharePoint 2007 and SharePoint 2010 classic-mode



- NT Authority\Authenticated Users

SharePoint 2010 claims-mode



- All Authenticated Users
- All Users ({WindowsProvider}), that is NT AUTHORITY\Authenticated Users
- All Users ({FormsProvider})
- All Users ({TrustedProvider})

Runtime Participants

Processes designed to utilize Runtime Participants make use of the People Picker control at runtime. The recommendations and limitations discussed in this topic apply when selecting additional participants. To remove existing participants, select the user or group from the list and click Remove as indicated below.

Manager Approval	<input type="text" value="legal :"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Add Remove <div style="background-color: #0070C0; color: white; padding: 2px 5px; margin-top: 5px;">K2:DENALLIX\Joe</div> </div>
To remove an account, or group, select it above and click 'Remove'	

1.6.8.1.6.8 Troubleshooting

K2

The K2 Server will log an Info event (Enrolling Type: SourceCode.Security.Providers...) for each configured user manager. Verify the expected user managers are loading correctly.

The following errors may occur when K2 is not configured correctly for claims-based authentication.

- Error: ID4175: The issuer of the security token was not recognized by the IssuerNameRegistry. To accept security tokens from this issuer, configure the IssuerNameRegistry to return a valid name for this issuer.**

This is an error from the Identity Framework when it validates the claims tokens against the trusted issuers name and thumbprint. This indicates that the values provided in K2HostServer.config do not match what SharePoint returns. There is a known issue with copying from the certificate properties window in MMC into the config file and getting an extra non-printable character in the text string, which causes the thumbprint match to fail. To resolve this, delete the entire thumbprint tag in the K2HostServer.config file, including the double-quotes, to ensure that there are no special characters left. Then use the thumbprint value returned from the SharePoint PowerShell command as recommended in Configuration {link to: Installation and Configuration > Configuration > SharePoint > Claims-based Authentication}.

- Errors: Token of type X not supported. or A valid [SAML1.1/SAML2] Token is required. or Not a valid [SAML1.1/SAML2] claims token.**

This is an error from K2 indicating the claims token type is not supported or K2 was not able to process the claims token. K2 supports SAML 1.1 (which SharePoint 2010 provides) and SAML 2.0 claims token types. For more information, see Configuration {link to: Installation and Configuration > Configuration > SharePoint > Claims-based Authentication}.

- Error: System.Exception: Deploying user '[Security Label]:[Domain\Username]' does not have impersonate rights.**

This error will appear in K2 Designer for SharePoint at deployment and indicates that after the claims changes were applied to the K2HostServer.config the K2 server needed to be restarted followed by an IISRESET.

SharePoint 2010

There are less configuration options available for K2 for SharePoint integration when working with web applications configured for classic based authentication. It is recommended to ensure that SharePoint and K2 integration is working end-to-end with classic based authentication before configuring claims based authentication integration.

It can be difficult to configure SharePoint 2010 for claims based authentication when the claims used for security cannot be validated. The SharePoint Claims Enumeration HttpModule can help in these scenarios by providing access to the claim values in the ULS log before the page is rendered. For more information, see Figuring Out What Claims You Have in SharePoint 2010: <http://blogs.technet.com/b/speschka/archive/2010/02/13/figuring-out-what-claims-you-have-in-sharepoint-2010.aspx>

SharePoint 2010 provides configurable diagnostic logging options. Ensure that the SharePoint Foundation > Claims Authentication and/or SharePoint Portal Server > Claims Authentication diagnostic logs are enabled when troubleshooting SharePoint claims authentication issues.

AD FS 2.0

AD FS 2.0 can be challenging to get configured and running smoothly. For more information, please refer to the numerous articles listed in [References](#).

A generic error message is displayed when AD FS encounters an issue with the user login.

Error

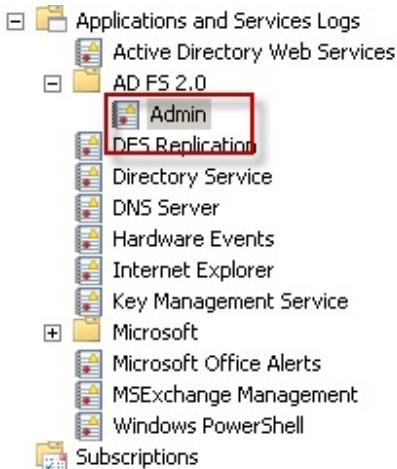
adfs.denallix.com

There was a problem accessing the site. Try to browse to the site again.

If the problem persists, contact the administrator of this site and provide the reference number to identify the problem.

Reference number: 15f9fa05-250a-421a-8613-ebef91d7d231

Open Event Viewer and navigate to the Applications and Services Logs > AD FS 2.0 > Admin log to see more detailed information on the error.



In addition to the Admin log, AD FS 2.0 provides detailed trace information through debug logging. For more information, see How to Enable Debug Logging for Active Directory Federation Services 2.0 (AD FS 2.0): <http://social.technet.microsoft.com/wiki/contents/articles/1407.aspx>

Some changes in AD FS configuration require a recycling of the user cookies, the AD FS service and the IIS site hosting AD FS.

1. Expire Cookies: Navigate to [IISWebSite]/adfs/ls/idpinitiatedsignon.aspx and click on Sign Out from all sites.

The screenshot shows a web page titled 'Sign-In Page' for the URL 'adfs.denallix.com'. The page displays a message 'You are signed in.' followed by two 'Sign Out' buttons. The top button is labeled 'Sign Out - Sign out from all the sites that you have accessed.' and the bottom button is labeled 'Sign Out - Sign out from this site.'. A red rectangular box highlights the top 'Sign Out' button.

2. Restart the AD FS service:
net stop adfssrv
net start adfssrv
3. Restart IIS web site:
iisreset

1.6.8.1.6.9 References

References

The following articles provide additional information on various claims-related topics.



Articles and links were current at the time of publishing and may change. Please send feedback if broken links are discovered.

Windows Identity Framework and Claims

Article	Link
Claims and Security Technical Articles for SharePoint 2010	http://msdn.microsoft.com/en-us/library/gg430136.aspx
What is WIF?	http://msdn.microsoft.com/en-us/library/ee748475.aspx
An introduction to Claims	http://msdn.microsoft.com/en-us/library/ff359101.aspx
Claims-Based Identity for Windows.pdf	http://go.microsoft.com/fwlink/?LinkId=209773
A Guide to Claims-based Identity and Access Control	http://go.microsoft.com/fwlink/?LinkId=188049
Claims Based Identity & Access Control Guide	http://claimsid.codeplex.com/
Introduction to Membership	http://msdn.microsoft.com/en-us/library/yh26yfzy(v=VS.90).aspx
WIF Questions and Answers	http://social.technet.microsoft.com/wiki/contents/articles/1898.aspx

Certificates

Article	Link
Application Security – Certificates	http://go.microsoft.com/fwlink/?LinkId=200774
Certificate Requirements for Federation Servers	http://go.microsoft.com/fwlink/?LinkId=182466

SharePoint 2010

Article	Link
SharePoint 2010 Claims and Security: Technical Articles	http://msdn.microsoft.com/en-us/library/gg430136.aspx
SharePoint Claims-based Identity	http://msdn.microsoft.com/en-us/library/ee535242.aspx
SharePoint 2010 Security (videos)	http://channel9.msdn.com/learn/courses/SharePoint2010Developer/SharePoint2010Security
SharePoint Front-End Protocols > Core > Security and Identity	http://msdn.microsoft.com/en-us/library/ff830402(v=office.12).aspx
Office Forms	http://msdn.microsoft.com/en-us/library/cc313069(v=office.12).aspx

Based Authentication Protocol Specification [MS-OFBA]	
SharePoint Security Token Service Web Service Protocol [MS-SPSTWS]	http://msdn.microsoft.com/en-us/library/dd959418(v=office.12).aspx
SharePoint Claim Provider Web Service Protocol [MS-CPSWS]	http://msdn.microsoft.com/en-us/library/dd921005(v=office.12).aspx
Configure forms-based authentication for a claims-based Web application (SharePoint Server 2010)	http://technet.microsoft.com/en-us/library/ee806890.aspx
SharePoint 2010 Certificates and Certificate Authority	http://blogs.msdn.com/b/besidethepoint/archive/2010/11/30/sharepoint-2010-certificates.aspx
Procedure: Determine thumbprint of the SharePoint Security Token Service certificate	http://blogs.msdn.com/b/ericwhite/archive/2010/06/18/ericwhite.aspx
Claims based Authentication in SharePoint 2010	http://www.harbar.net/presentations/spevo/DD109%20Claims.pdf

AD FS 2.0

Article	Link
UPDATED: How To Add ADFS 2.0 as a Federated Identity Provider in SharePoint 2010	http://blogs.pointbridge.com/Blogs/nielsen_travis/Pages/Post.aspx?_ID=42
Configuring SharePoint 2010 and ADFS v2 End to End	http://blogs.technet.com/b/speschka/archive/2010/07/30/speschka.aspx
Figuring Out What Claims You Have in SharePoint 2010	http://blogs.technet.com/b/speschka/archive/2010/02/13/speschka.aspx
Configuring Claims Based Authentication for SharePoint with AD FS 2.0	http://shannonbray.wordpress.com/2010/05/29/wordpress/
SharePoint 2010 and ADFS 2.0 the complete Step-by-Step guide	http://marcvaneijk.wordpress.com/2010/06/12/wordpress/
Updating SP Claim	http://lindstrom.nullsession.com/?p=236

Mappings	
How to Enable Debug Logging for Active Directory Federation Services 2.0	http://social.technet.microsoft.com/wiki/contents/articles/1407.aspx
AD FS 2.0 Step-by-Step and How To Guides	http://go.microsoft.com/fwlink/?LinkId=180357
Using Active Directory Federation Services 2.0 in Identity Solutions	http://go.microsoft.com/fwlink/?LinkId=209776

InfoPath

Article	Link
Configure Web service proxy for InfoPath Forms Services (SharePoint Server 2010)	http://technet.microsoft.com/en-us/library/ff621101.aspx
About Data Connections, Authentication, and Alternate Access Mapping	http://msdn.microsoft.com/en-us/library/ms771995.aspx
Universal Data Connection v2.0 Reference and Schema	http://msdn.microsoft.com/en-us/library/ms772017.aspx
Advanced Server-Side Authentication for Data Connections in InfoPath 2007 Web-Based Forms	http://msdn.microsoft.com/en-us/library/bb787184(v=office.12).aspx

1.6.8.1.6.10 K2 and Claims - FAQ

K2 and Claims - FAQ

What claims are mapped from SharePoint to K2?

Legend

1 Identity Provider

2 Identity

3 Role

```
<!--K2ADFS Security/Role Provider for Trusted Provider-->
<claimTypeMapping securityLabel="K2ADFS">

 1 <!-- Claim that represents the system issuing the identity and role claims to be mapped to the K2 security label-->
<identityProviderClaim originalIssuer="SecurityTokenService" claimType="http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider"
  claimValue="trusted:ADFS LDAP" />

 2 <!-- Claim that represents the user for the K2 security label-->
<identityClaim originalIssuer="TrustedProvider:ADFS LDAP" claimType="http://schemas.k2.com/identity/claims/name" />

 3 <!-- Claim that represents the groups for the K2 security label-->
<roleClaim originalIssuer="TrustedProvider:ADFS LDAP" claimType="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" />

</claimTypeMapping>
```



K2 requires the **claimType** for the **identityClaim** to match the claim mapping configured in SharePoint as the Identifier Claim. The K2 Server Configuration section provides automatic and manual approaches that aid in configuring the appropriate identity claim type mapping for K2.

For more information, see [Claim Type Mappings](#).

Can K2 work without access to the source identity store?

K2 needs to map to the same identity store as the source of the claim to fully implement user and group browsing and user property (e.g., email or manager) lookups. However, user and group browsing and property lookups are not requirements for K2 to function. Strings representing the K2 label and the FQN can be used throughout K2 for rights and work assignment, and properties can be stored and retrieved from other places, such as SharePoint User Profile DB.

K2 provides support for AD, LDAP and SQL source identity stores. A custom user manager can be created to support other identity stores.

Does K2 need to communicate with source identity store?

Yes. K2 does not retain claim set data and only uses the identity claim at runtime. K2 needs access to the identity store directly to retrieve user details, similar to the SharePoint User Profile store.

Can K2 support multiple Claims Authentication Types (aka, providers) for the zone you wish to work with?

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

Trusted Identity Provider Authentication enables federated users in this Web application. This authentication is Claims token based and the user is redirected to a login form for authentication.

1

Enable Windows Authentication

Integrated Windows authentication

Negotiate (Kerberos)

Basic authentication (credentials are sent in clear text)

2

Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name
LdapMembershipProvider

ASP.NET Role manager name
LdapRoleProvider

3

Trusted Identity provider

Trusted Identity Provider

ADFS LDAP

Yes. K2 **requires** #1 ([Windows Authentication](#)) and can support any combination of #2 ([Forms](#)) and/or #3 ([Trusted](#)).

For more information, see [Supported Configuration](#).

Can K2 for SharePoint components work on a SharePoint web application zone that does not have Windows Authentication enabled?

No. The K2 service account and any K2 Studio or Visual Studio based designer accounts require access to the claims-based zone via Windows Authentication.

Can K2 use one zone configured for Windows Authentication for designer rights and another zone without Windows Authentication for runtime?

No. K2 does not support the use of multiple zones or alternate access mappings. K2 must utilize the same zone (aka, URL) for both design time and runtime integration.

Can K2 leverage the SharePoint User Profile database?

Yes. K2 can utilize the data in the user profile database to retrieve attributes for claims-based users via custom code.

Can K2 work with federated AD FS (e.g., multiple domains)?

No. K2 requires a one-to-one mapping from an identity store to a K2 user manager. Therefore, a single AD FS endpoint that has federated multiple identity stores cannot be configured. K2 supports the development of custom user managers which can manage federated identity stores.

1.6.8.2 InfoPath Configuration Notes

InfoPath Integration - InfoPath Configuration Notes



If InfoPath 2013 forms are going to be used, the forms must be set to InfoPath 2010 compatibility mode in the forms options. Further, Microsoft Office 2013 installations need to be licensed as unlicensed installations cause forms publishing issues.

If an error is received when using **InfoPath Forms Services** the following Configuration steps need to be taken.

Configuring your SharePoint to run InfoPath Forms Services:

- 1 Open **SharePoint Central Administration**
- 2 Open the **Application Management** page
- 3 Go to the InfoPath Forms Services section and click on the **Configure InfoPath Forms Services** link
- 4 In the **User Browser-Enabled Form Templates** section, make sure both check boxes are ON:
 - Allow users to browser-enabled form templates
 - Render form templates that are browser-enabled by users
- 5 In the **HTTP Data Connections** section, if the InfoPath web services has not been installed on a web that uses SSL, make sure the check box is OFF:
 - Require SSL for HTTP authentication to data sources
- 6 In the **Cross-Domain Access for User Form Templates** section, make sure the check box is ON:
 - Allow cross-domain data access for user form templates that use connection settings in a data connection file

Configuring your browser to open any InfoPath form (client or web form):

- 1 Open **IE**
- 2 Go to **Tools > Options**
- 3 Go to the **Security Tab**
- 4 Add the following URLs to the trusted sites list:
 - If the form has been published to a SharePoint site, add the SharePoint site URL
 - The InfoPath web service site URL
- 5 Reset the security level to **LOW**

1.6.8.3 Salesforce Integration

Salesforce Integration

Salesforce.com is a Client Relationship Management (CRM) Services company which markets its product and services online via a web based interface. Users are quickly able to setup an account with Salesforce and thereafter provide the site's many business oriented tools with data related to their company's operations. This data is then processed and organized into useful information revolving around their company operations.

K2 blackpearl manages the Salesforce integration using the Service Broker and K2 blackpearl SmartObjects. The data is exposed via the K2 blackpearl environment manager architecture as a SmartObject. Managed in this way, the Salesforce account surfaces and is made available as a native component of the K2 blackpearl environment.

Salesforce Integration Resources

There are various additional resources and extensive documentation available on the Salesforce web site which are accessible once an account has been created.

K2 blackpearl Salesforce Documentation

The focus of the sections in this help file is to assist the developer to integrate their processes with the Salesforce site. Therefore the documentation discusses the K2 blackpearl Integration features, configuration requirements and usage.

For an in depth discussion on the technical aspects of the Salesforce web site, refer to the documentation provided by [Salesforce](#).

Salesforce Documentation

The Salesforce site is replete with documentation. You have access to

- Online help
- Salesforce PDF download

Salesforce Account and System Administration

Once the WSDL (Web Services Description Language) has been downloaded the Administrator is required to generate the required infrastructure for the Salesforce instance. Beyond facilitating a level of integration with the Salesforce site, Administrator level tasks are performed from the Salesforce site and are beyond the scope of this documentation.

[Getting Started with Salesforce](#)

1.6.8.3.1 Getting Started with Salesforce

Sales Force Integration - Getting started

The process to integrate your organization with Salesforce is divided into a number of definite steps.

1. Create a Salesforce user account and generate a security token for your password
2. Download the service WSDL
3. Prepare to generate the service instance
4. Generate the service instance of Salesforce in the K2 blackpearl Service Broker
5. Cache the Salesforce credentials
6. Create a K2 blackpearl SmartObject and the required property mappings
7. Build a user form that enables client users to interact with the K2 blackpearl Salesforce centric SmartObject

1. Salesforce Account

The Salesforce user account is created on the site <http://developer.salesforce.com>. The individual representing the organization or company creates a user account using an e-mail address and password . Once registered, Salesforce will send a confirmation email to the user account, follow the instructions therein.

The login credentials are important as they are used later on in the integration process to authenticate against the Salesforce site.

Once the account has been created, a security token for the chosen password must be generated.

The image and steps below describe how to do this:

Reset Security Token

Clicking the button below invalidates your existing security token.

Your security token is tied to your password and will be invalidated if you change your password. Your new security token is also reset.

For security reasons, your security token is delivered to the following email address:

Reset Security Token

A new security token has been sent to andrew.murphy@k2.com, which is the email address associated to your user.

How to enter your security token:

When accessing salesforce.com either via a desktop client or the API from outside of your company's trusted networks:

If your password = "mypassword"
And your security token = "XXXXXXXXXXXX"
You must enter "mypasswordXXXXXXXXXXXX" in place of your password

Note that you do not enter a security token in place of your password when logging into salesforce.com via a browser.

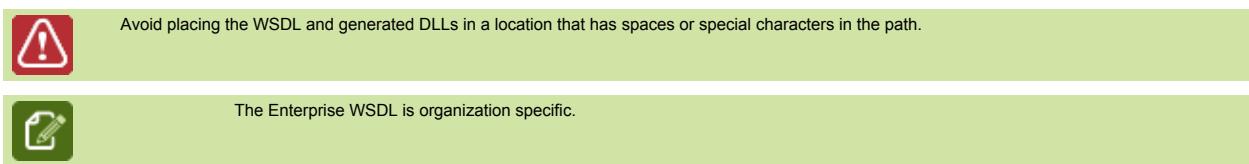
1. Log into the Salesforce web site. At the time of this writing, the Getting Started Salesforce page is displayed.
2. Click the **login name** in the upper right corner of the page, this displays a menu. Select **Setup** from this menu.
3. Click **My Personal Information** in the navigation bar on the left of the page to expand the menu, then select the **Reset Security Token** item. Read the important information on the page.
4. Salesforce will send an email with the new security token. This token must be appended to the account password to access Salesforce from within K2 blackpearl.

2. Generate and download the service WSDL

Salesforce supplies a Web Services Description Language (WSDL) file to its customers. The WSDL file enables the developer to integrate with Salesforce using the Salesforce API.

The method of generating the WSDL file is beyond the scope of this document but full details can be found on this site:

http://www.salesforce.com/us/developer/docs/api/Content/sforce_api_quickstart_steps.htm



Once you have the WSDL file you can:

- Distribute the WSDL file amongst the developers with your organization.
- Use the WSDL file to generate the files required for developing solutions in conjunction with Salesforce.

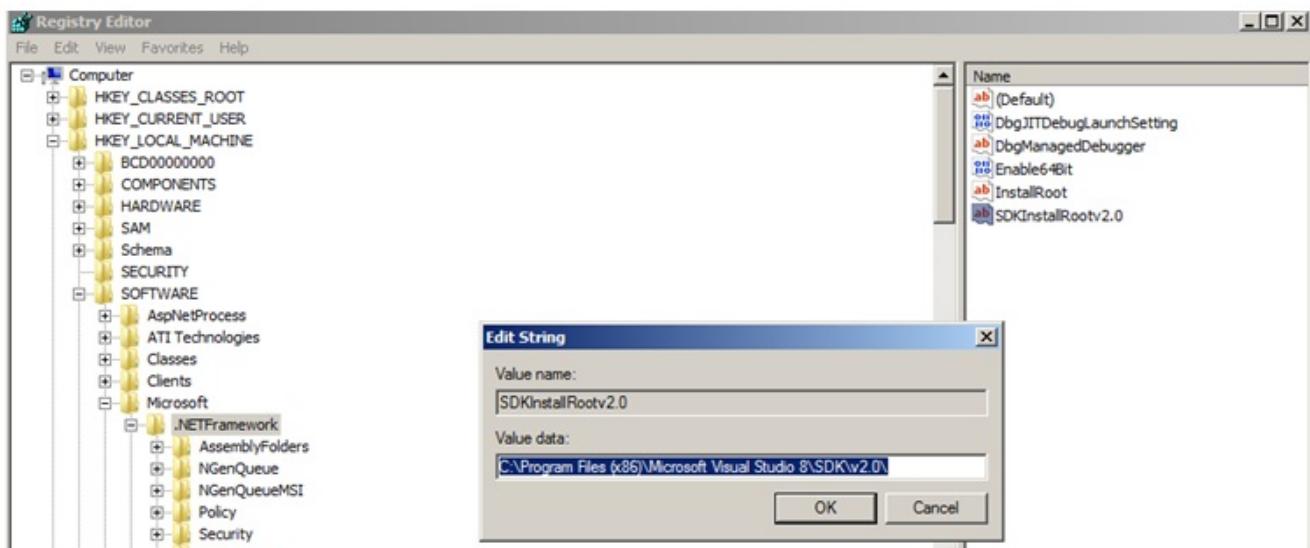
3. Prepare to generate the service instance

As a prerequisite to generating the service instance, the .NET 2.0 SDK must be installed. For more information see: <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=19988>

A Windows Registry entry of type String must be created in the following branch, **HKLM > Software > Microsoft > .NETFramework** with the following data:

Value name: SDKInstallRootv2.0

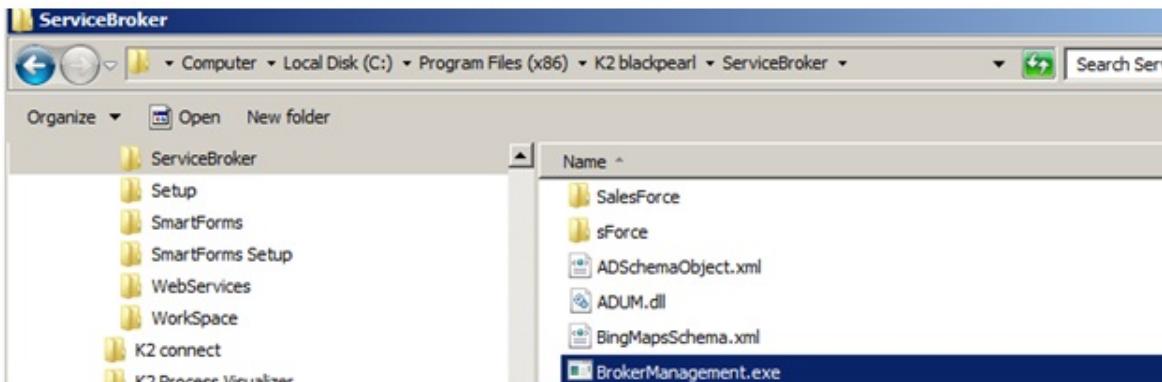
Value data: <path of the .NET v2 root installation> (this is the folder the SDK installed to)



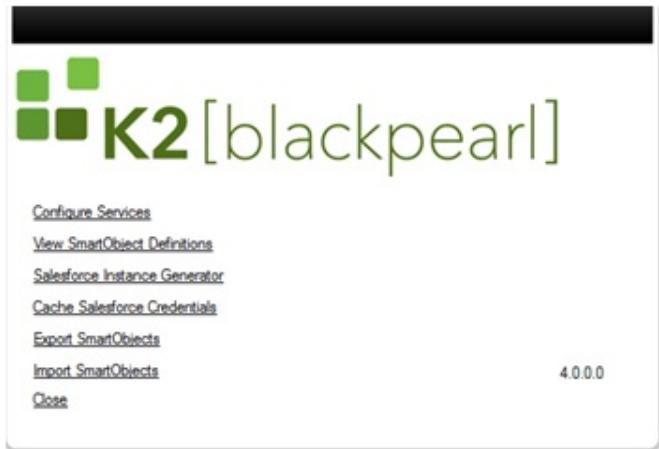
4. Generate the service instance of Salesforce in the K2 blackpearl Service Broker

Before the service instance can be registered and used, it needs to be generated. This is done by starting the Broker Manager.

- The Broker Manager is started by browsing to the ServiceBroker folder in the K2 blackpearl installation folder and running the **BrokerManager.exe** file.



- Select the Salesforce Instance Generator from the list:



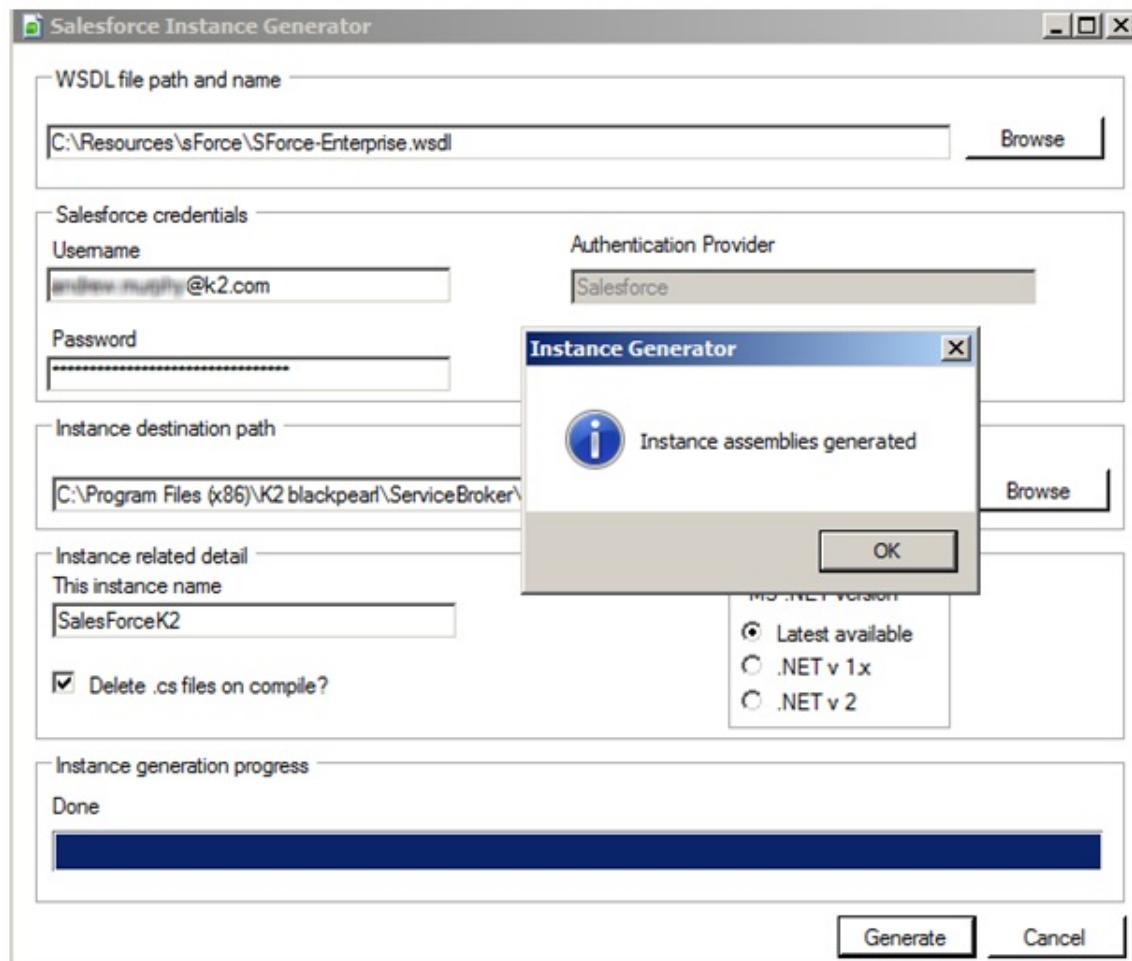
Service Broker	
Configure Service	Configure a new Service
View SmartObject Definitions	Enables the SmartObject Definition viewing
Salesforce Instance Generator	Generates an Instance of a Salesforce related service
Cache Salesforce Credentials	Creates a user profile for Salesforce users using their credentials Note: Used only once an instance of Salesforce has been created
Export SmartObjects	Creates SmartObject Deployment Package for export to another environment
Import SmartObjects	Imports SmartObjects from another environment

- Fill in the Salesforce Instance Generator page remembering to append the security token generated earlier to your password.

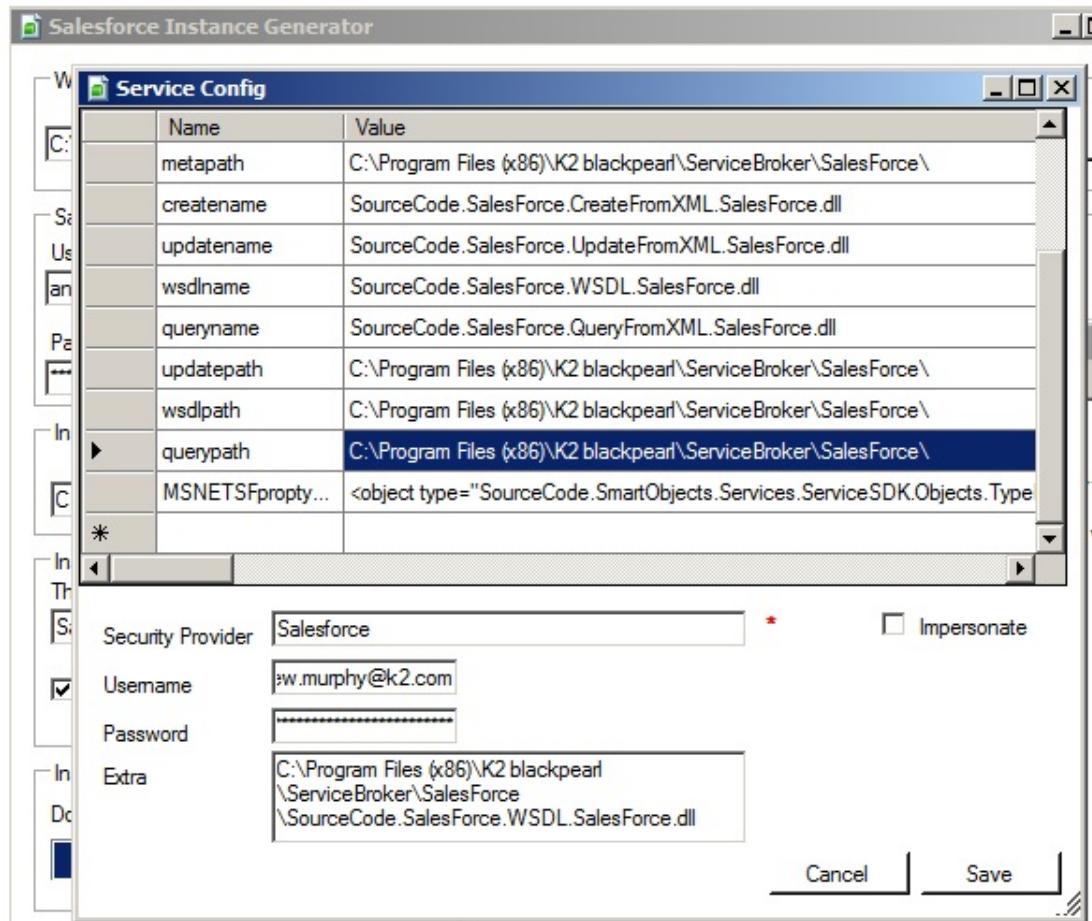


In the screen shot below, the Instance destination path is a long format path with spaces and () in it, this will cause an error. Rather point to a short path for example: c:\k2SalesForce

Once the files have been generated, they can be copied to C:\Program Files (x86)\K2 blackpearl\ServiceBroker\Salesforce and registered from there.



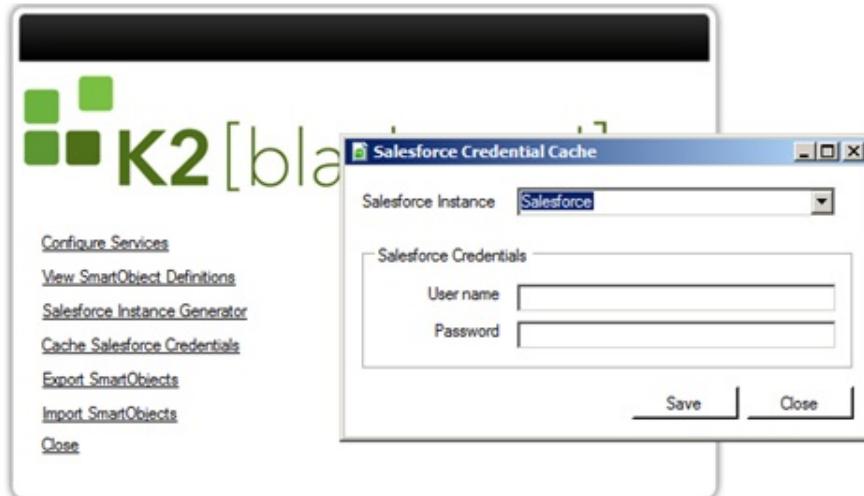
- Choose to register the DLLs and enter credentials (remember that security token with the password)



- Once the DLLs have been registered it is important to **restart the server** to ensure the following step (caching credentials).

5. Cache Salesforce Credentials

The final step is to cache your credentials by selecting the Cache Salesforce Credentials, again, remember to append the token to the password.



1.6.8.3.2 Configuring credentials to execute Salesforce SmartObject methods

Configuring credentials to execute Salesforce SmartObject methods

Problem Summary:

A Salesforce service instance is created and some smart objects are built from it.

The application that uses the smart objects can not execute their methods unless the end user has cached the Salesforce credentials in Workspace while being logged in as themselves. The application needs to use impersonation, so as long as the impersonated user has cached his credentials beforehand, the smart object methods will execute successfully. If the user did not cache his credentials, the exception thrown is "No Credentials Cached for this label".

Workaround:

To avoid the requirement that each end user needs to cache Salesforce.com credentials in order for a smart object method to execute, do the following:

1. Ensure that the web application using the smart objects is running under an app pool account that is in turn configured to run under a service account user identity (ie. not a predefined service).
2. In your browser, log into workspace as that app pool service account user and drill into "K2 Management > Smart Objects > Services > Salesforce Service". Select the service instance that you are using and click 'Credentials', then enter the Salesforce credentials. Ensure that you append the Salesforce token to your password.
3. In the web application code, you need to:
 - (i) remove impersonation,
 - (ii) sign into the smart object server,
 - (iii) execute the smart object method(s), then once you are done with the connection,
 - (iv) resume impersonation. By removing impersonation during sign in, the k2 server will pick up the service account user in the app pool that this application is running under.

Web application code:



```
using SourceCode.SmartObjects.Client;
.

.

object retVal = null, paramValue = "Some_Value";

// Stop impersonation
System.Security.Principal.WindowsImpersonationContext ctx =
System.Security.Principal.WindowsIdentity.Impersonate(IntPtr.Zero);

SmartObjectClientServer clientServer = new SmartObjectClientServer();
clientServer.CreateConnection();
clientServer.Connection.Open("Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=[YOUR_K2_HOST];Port=5555"); // conn string hard-coded for simplicity.
SmartObject soOpportunity = clientServer.GetSmartObject("sfOpportunity"); // or whatever your smart object is named.

try
{
// replace quoted values with your own values.
smartObject.Methods["methodToExecute"].Parameters["paramName"].Value = (string)paramValue;
smartObject.MethodToExecute = "methodToExecute";
clientServer.ExecuteScalar(soOpportunity);
retVal = smartObject.Properties["returnPropertyName"].Value;
.

.

}

catch (SourceCode.Hosting.Exceptions.AuthenticationException authEx)
{
if (ctx != null)
{
ctx.Undo();
}
throw new Exception("SourceCode.Hosting.Exceptions.AuthenticationException: " + authEx.Message);
} */
catch (Exception ex)
{
// Resume impersonation
if (ctx != null)
{
ctx.Undo();
}
throw new Exception(ex.Message);
}
finally
{
// Resume impersonation
if (ctx != null)
{
ctx.Undo();
}
}
```

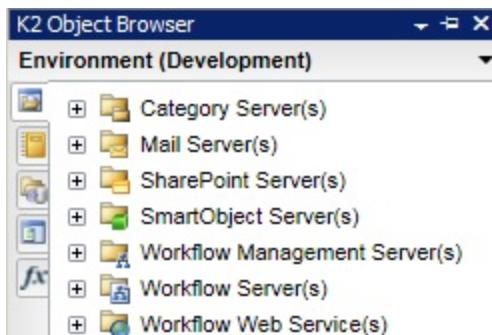
1.6.8.4 Environment Library

1.6.8.4.1 Environment

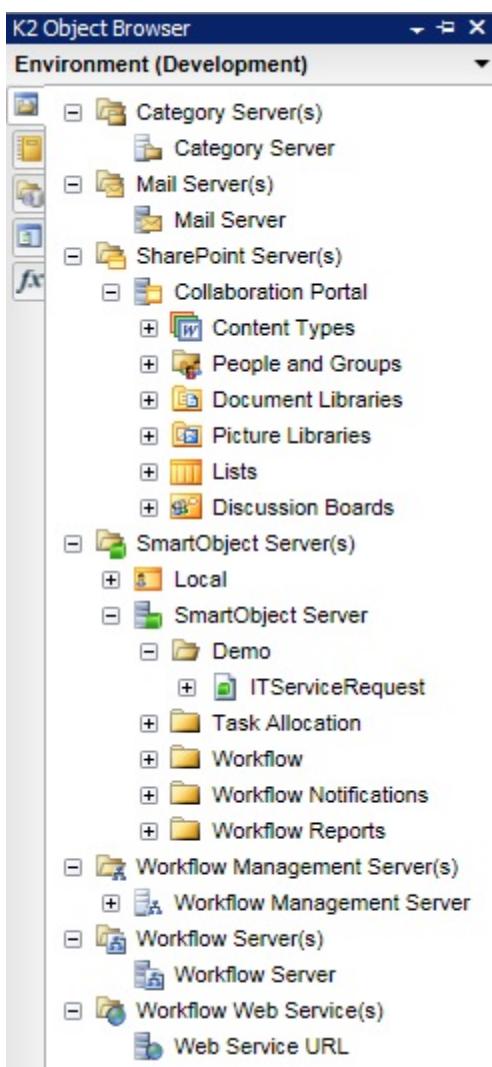
K2 Environment

The Environment Browser manages the services and servers that host the resources of the K2 Platform.

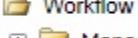
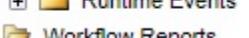
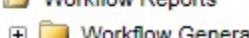
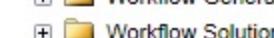
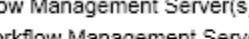
The K2 Environment consists of a variety of Servers and Services that host the resources that any given process will require to access the data silos and environmental resources required to complete the process successfully.



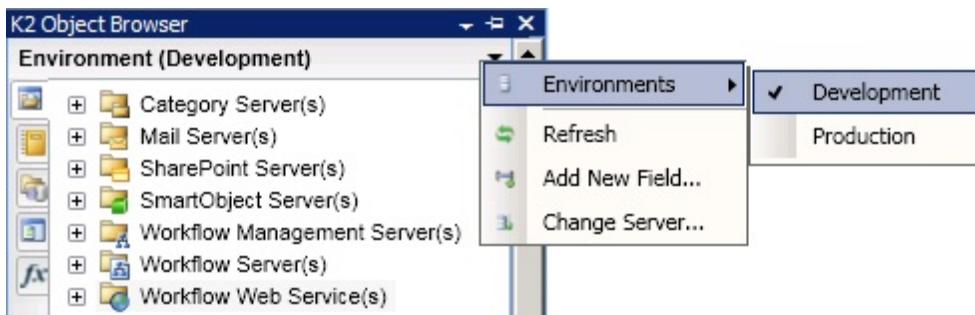
The environment is managed in terms of the role that the servers and services play. By default an Environment called Development is available to populate with servers and services for design time requirements. For runtime deployment a separate environment can be created, allowing the developer to toggle between the development and production environments.



Server	What it is	How to use it
--------	------------	---------------

 Category Server(s)  Category Server	Presents the Category Server connection details	Select the required Category Server
 Mail Server(s)  Mail Server	Presents the Mail Server connection details	Select the required Mail Server
 SharePoint Server(s)  Collaboration Portal  Content Types  People and Groups  Document Libraries  Picture Libraries  Lists  Discussion Boards	Presents SharePoint Sites from the SharePoint Server. The default Site can be selected here See K2 for SharePoint	Select the required SharePoint Site from the desired folder location or add a new Site
 SmartObject Server(s)  Local  SmartObject Server  Demo  ITServiceRequest  Single Method  Create  Save  Delete  Load  List Method  Get List  Task Allocation  RoundRobinSO  Single Method  List Method  Workflow  Workflow Notifications  Management Events  Runtime Events  Workflow Reports  Workflow General  Workflow Solutions	Presents SmartObjects from the SmartObject Server and from the Local environment (those loaded in an open K2 for Visual Studio project). Each SmartObject node will contain the SmartObject Methods as subnodes See Introduction to SmartObjects	Select the required SmartObject from the desired folder location OR Select the required SmartObject Method from the SmartObject node
 Workflow Management Server(s)  Workflow Management Server  Zone(s)	Presents the Workflow Management Server connection details	Select the required Workflow Management Server
 Workflow Server(s)  Workflow Server	Presents the Workflow Server connection details	Select the required Workflow Server
 Workflow Web Service(s)  Web Service URL	Presents the Workflow Web Services connection details	Select the required Workflow Web Service

Clicking on the drop down arrow will display the following options:



Drop Down	What it is	How to use it
Environments	<p>Displays a list of configured Environments The labelling for this option alternates depending on the environment selected.</p> <p>The Environment is configured to develop against one of two default environments which are Production and Development. Although available by default, the servers and services must be configured manually</p>	Click on the drop down arrow and select Environments , then select the Environment to load into the Object Browser
Refresh	Selecting refresh, will refresh the link between the browser and the registered items in the browser	Click on the drop down arrow and select Refresh
Add New Field...	Select this option to register a New server or service with the Environment Browser	Click on the drop down arrow and select Add New Field
Change Server...	Opens the Change Environment Server Connection dialogue, allowing a different Environment Server to be loaded, or connection details to be changed	Click on the drop down arrow and select Change Server...

For in-depth technical information on this topic, visit

http://k2underground.com/files/folders/technical_product_documents/entry27110.aspx

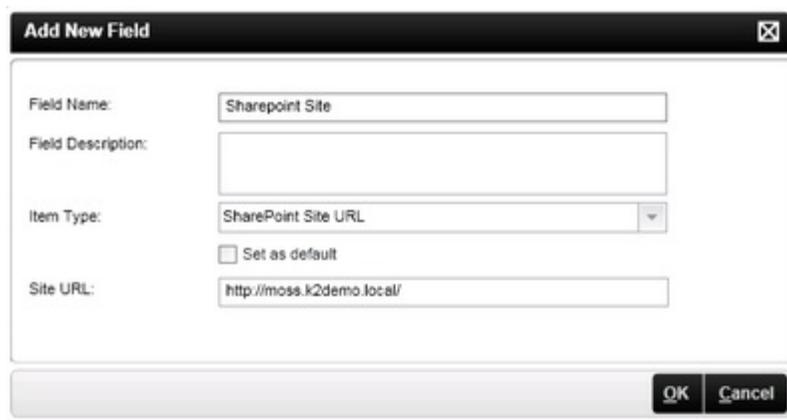
Adding a SharePoint server

K2 blackpearl for SharePoint offers a complete business process management solution, supporting all aspects of the business process lifecycle. Built on the Microsoft .NET Framework, the Web-enabled technologies of the K2 blackpearl for SharePoint solution seamlessly integrate human and technology resources to provide workflow information to users via any device at any time. The K2 automated process environment is scalable and extensible with the flexibility to interoperate across platforms and with disparate legacy systems. See [K2 for SharePoint Integration](#) for more technical detail.

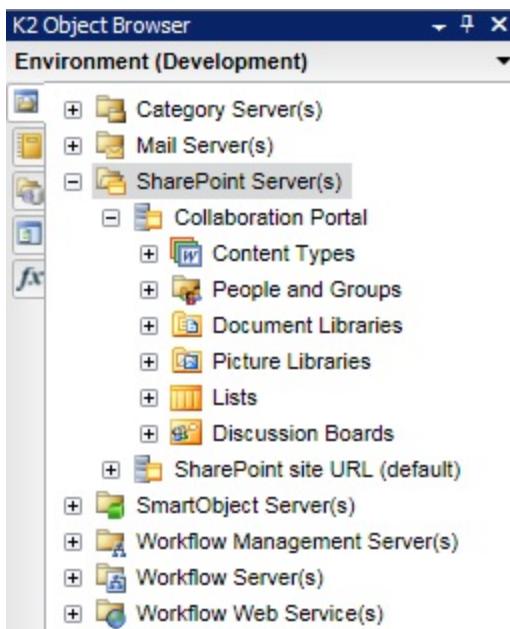
The Environment variables need to be configured so that K2 for Visual Studio knows where the SharePoint environment is located. When installing K2 blackpearl, a default SharePoint site is added, and is listed as SharePoint Site URL. Additional SharePoint Environment Fields must be added if there is more than one site collection that will be used in the K2 processes.

To configure the Environment, perform the following steps:

1. In K2 for Visual Studio, click on the Object Browser tab
2. Click the drop down arrow next to Environment (Development) and select Add New Field...
3. Enter the following information in the Add New Field dialog window:
 - **Name** - The name you want to give to the SharePoint Site Collection you are configuring
 - **Description** - The description of the Site Collection (optional)
 - **Item Type** - Select SharePoint Site URL from the drop down menu
 - **Site URL** - The URL for the top-level SharePoint Site collection to which you wish to deploy K2 Processes



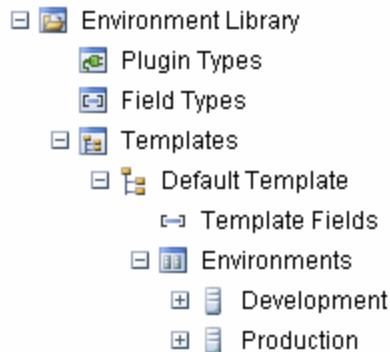
Your SharePoint Site will now display under the SharePoint Server(s) node in the Object Browser



If you have more than one site collection where you want to deploy K2 Processes, repeat this step on each site collection.

1.6.8.4.2 Environment Library Management

K2 Management Console - Environment Library



Node	Description
Plugin Types	Configures the Environment Library Plugins
Field Types	Configures the Environment Library Field Types
Templates	Configures the Environment Library Templates

1.6.8.5 SSL

1.6.8.5.1 Introduction to SSL

Introduction to SSL

SSL (Secure Socket Layer) is a method of identifying secure communications that inherits its robustness from the IP protocol stack. SSL is not K2's proprietary standard but rather an industry recognized method of authentication for client and server machines using a certificate based system.

K2 blackpearl and K2 blackpoint implement the protocol in a manner that enables the system to authenticate users based on system configuration and the exchange of valid, verifiable certificates.

SSL Integration

K2 blackpearl supports SSL integration. SSL requires that a certificate must be attached to the communication simply to establish that when interaction between the server and the web based resources takes place, the communication is from an authorized source.

K2 blackpearl Server does not support SSL Authentication, therefore the SSL allows for protocol compliance only when K2 blackpearl Server places a service call to one of the available web services.

Additional Resources

For further information on how to perform the steps on the Web Server to generate the certificate request file, see the URLs below:

- How to implement SSL in IIS
See here: <http://support.microsoft.com/kb/299875>
- Generating a Certificate Request File Using the Certificate Wizard in IIS 5.0
See here: <http://support.microsoft.com/kb/228821>
- Using Certificate Server 2.0 to Generate a Server Certificate for Use with IIS 5.0
See here: <http://support.microsoft.com/kb/228984>
- How To Renew VeriSign SSL Certificate with New Key in IIS 5.0 MMC
See here: <http://support.microsoft.com/kb/295329>
- Creating Server Certificates Using Certificate Services Web Forms
See here: <http://support.microsoft.com/kb/248107>
- Configure InfoPath Forms Services for Office SharePoint Server
See here: <http://technet.microsoft.com/en-us/library/cc262263.aspx>
- Advanced Server-Side Authentication for Data Connections in InfoPath 2007 Web-Based Forms
See here: <http://msdn.microsoft.com/en-us/library/bb787184.aspx>

1.6.8.5.2 SSL Certificates

Certificates

Two types of certificates exist, a server certificate and a client certificate. The purpose of the certificate is simply to identify that either the client or server making the service request is authorized to do so. The certificate is issued once off, and that certificate is valid in terms of the issuing authority. Certificates may expire but this would be determined by the issuing authority.

When are certificates required?

The certificate passing is required when K2 blackpearl Server initiate a service request to one or more web service applications. These include IIS, MOSS, Reporting Services and K2 Workspace. The presence of the certificate is part of the service request transaction and identifies both server and client machines as authorized to make the service request by the signing authority and a source that can be trusted. Certificates are used when initiating a process or submitting an item to workflow for example using InfoPath Forms Services. When setting up SharePoint for example to work in conjunction with InfoPath Forms services, only server certificates are required.



InfoPath Forms services do not support the use of client certificates

Generating Certificates

The certificate is generated by an issuing authority, which can be internal to an organization. Specialized software is used to generate the certificate, however this type of certificate is a self signed certificate and although usable the internet browser will report errors.

K2 blackpearl and K2 blackpoint will support the Microsoft Certificate Services managers natively.

Installed Certificates

Once the certificate has been installed, it displays on the bottom of the Internet Browser when secure transactions are taking place. If it does not display, then the certificate has not been installed correctly.

Storing Certificates

Certificates are installed locally on both server and client machines. Once the certificate has been issued it is loaded onto the machine, and retained in the local store. In some instances the client and server certificates are stored on their respective local machines, in other both server and client certificates are stored on the client machine.

Using Certificates

Certificate usage is dependent on how the environment has been configured. The server will always store the server certificate locally. The client machine may only have a client certificate, but may also store a server certificate as well. These certificates are attached to the communication and passed for identification purposes.

1.6.8.5.3 K2 Requirements for AD

K2 requirements for Active Directory

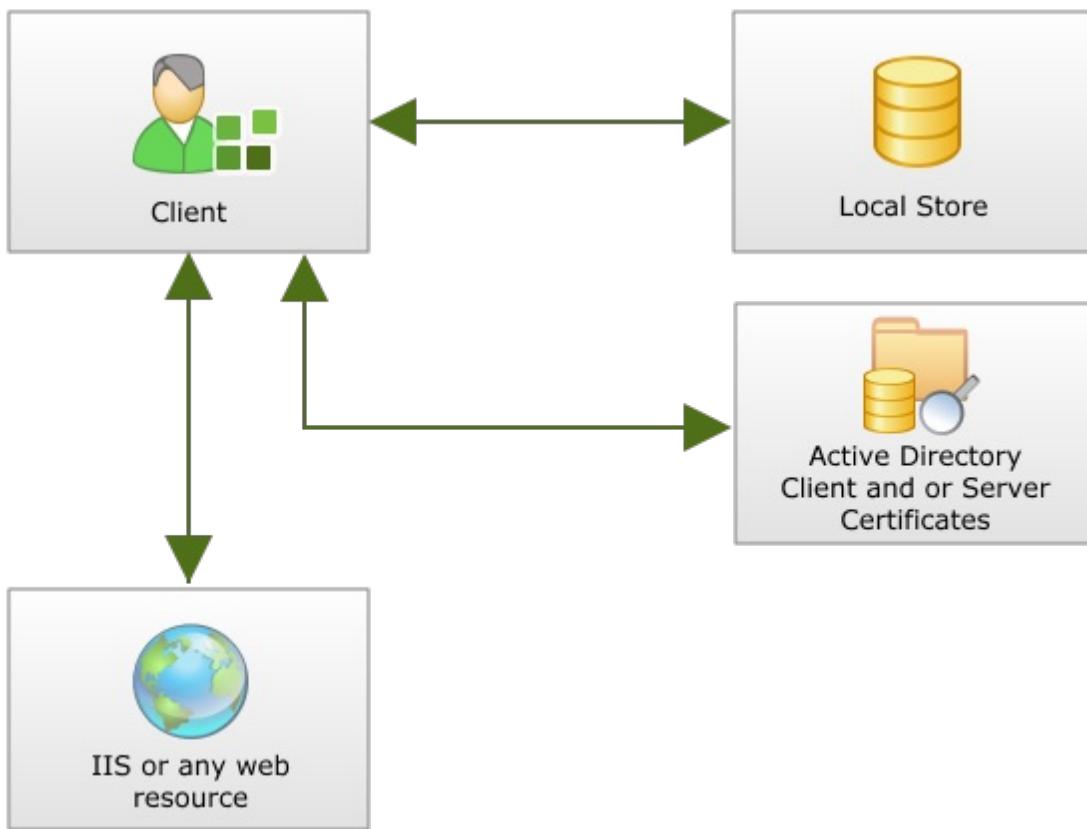
Active Directory is interrogated for a few parameters when a client side certificate is passed. The items that will be required are:

1. the URL from which the service call is made,
2. the User's display name and then
3. a common name and or e-mail address.

If any of the items listed are not available, then an error will be thrown and the certified communication thread will not be established.

Shown in the diagram below, the client which may be internal or external to the domain passes a web resource service request. For the connection to be established the client must do the following:

1. Provide a Client and or Server Certificate
 - a. Client Certificate enables Authentication
 - b. Server Certificate identifies the service request as from a trusted source
2. Once the authenticity of the certificates has been verified, the certificate is attached as part of the communication and passed so that interaction between the client and the requested resources can take place.



1.6.8.5.4 SQLUM Requirements

SQLUM

K2 blackpearl's alternative natively supported user manager, supports Server Certificate based SSL only. Client side certificate SSL is not supported as the users need to be authenticated against Active Directory by default which will not be available when SQLUM is used. Client side certificates cannot be authenticated against SQLUM as this feature is not implemented.

1.6.8.6 Pre-Installation

K2 SmartActions Pre-Installation



The requirements mentioned in this topic must be in place before the K2 SmartActions is implemented. Certain aspects of the pre-installation requirements will be verified by the installer at install time. It is therefore more advantageous to implement these updates prior to attempting the installation.

K2 SmartActions, which utilizes e-mail as a means of notifying the end user of a worklist item may encounter a limitation owing to the number of e-mails that the Microsoft Exchange server will permit the K2 Server to send per minute. This limitation may not be encountered as much under previous circumstances as not all process instances would have relied on e-mail. The differentiator for K2 SmartActions is that e-mail is one of the primary means of user notification with the potential for multiple e-mails being sent per process instance per default activity.

The information contained in the accompanying document will enable a System Administrator to reconfigure the Microsoft Exchange server to permit a higher volume of e-mail messaging to be permitted by the K2 Server Service Account : [KB001269 - How to Reconfigure Microsoft Exchange Server Maximum E-mails per minute limitation File](#)

Listener Mail box

By default, K2 SmartActions uses the Exchange mailbox associated with the K2 Service account. However, any dedicated account can be used and ensures that the K2 Server will respond only to the incoming K2 SmartActions e-mail. Using a non-dedicated mailbox for SmartActions may result in erroneous notifications and responses, and could impact server performance.

During installation, the K2 Setup Manager will query Exchange for the mailbox of the K2 Service Account, by default, or for the mailbox associated with the specified user. If a mailbox is not found, the entry in the configuration file is left empty. If a mailbox is found the configuration file is updated but can be changed at a later time without re-running the K2 Setup Manager. For information on how to do this, see the [K2 SmartActions Installation](#) topic.

Messaging Protocols Supported

K2 SmartActions supports the following protocol, which is installed and configured at the time of installation:

- Exchange Server: Installs automatically as part of the K2 installation and is supported out of the box



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.

1.6.8.6.1 K2 Server Configuration File Updates

K2 Server Configuration File

Once K2 SmartActions has been installed, the messaging customization for the K2 Server needs to be configured. All messaging is managed according to what is contained with the K2 Server configuration file. The K2 Server configuration file (**K2HostServer.config**) is located at <install drive>:\Program Files (x86)\K2\blackpearl\Host Server\Bin. The configuration file enables the Administrator to configure the operation of K2 SmartActions.

K2 [blackpearl or blackpoint]\Host Server\Bin\K2HostServer.config, is used to configure the following items, which are configured by editing the file as illustrated below. The following items can be configured:

1. K2 SmartActions that action the process
2. Synonyms which can be used in addition to the prescribed Actions
3. Help for the Information Worker
4. Error handling Messaging

K2 Server Configuration File Example

Shown below is an example code sample for SmartActions. This section contains tags which configure the following:

- The messaging files that the K2 Server uses: each text file is an individual message template
- Standard Actions and their synonyms. The tag is actionsStandard.
- Configured actions which have the same affect as a standard action except that they are user configured and standard actions will take precedence over them. The tag name is actionsConfigured

Code Sample to Edit the K2 Host Server Configuration File

```
<messageBus>
    <!--
        If you do not use the Service Account for MessageBus, remember to update
        the connection
        strings.
    -->
    <system self="K2:DENALLIX\Administrator" enableListeners="true"
allowAmbiguity="true" />
    <messages>
        <help filename="Templates\Messages\MessageBus.Help" />
        <unhandledError filename="Templates\Messages\MessageBus.UnhandledError" />
        <error filename="Templates\Messages\MessageBus.Error" />
        <replyFormat filename="Templates\Messages\MessageBus.ReplyFormat" />
    </messages>
    <smartActions>
        <messages>
            <help filename="Templates\Messages\SmartActions.Help" />
            <actions filename="Templates\Messages\SmartActions.Actions" />
            <unhandledError filename="Templates\Messages\SmartActions.UnhandledError" />
            <error filename="Templates\Messages\SmartActions.Error" />
            <actionExecuted filename="Templates\Messages\SmartActions.ActionExecuted" />
            <standardActions filename="Templates\Messages\SmartActions.StandardActions" />
        </messages>
        <standardActionsWithDescriptions
filename="Templates\Messages\SmartActions.StandardActionsWithDescriptions" />
            <sleep filename="Templates\Messages\SmartActions.Sleep" />
            <sleepError filename="Templates\Messages\SmartActions.SleepError" />
            <redirect filename="Templates\Messages\SmartActions.Redirect" />
            <redirectError filename="Templates\Messages\SmartActions.RedirectError" />
            <delegate filename="Templates\Messages\SmartActions.Delegate" />
            <delegateError filename="Templates\Messages\SmartActions.DelegateError" />
            <itemNotFound filename="Templates\Messages\SmartActions.ItemNotFound" />
        </messages>
        <synonyms>
            <actionsStandard>
                <!-- Supported synonyms for the Redirect action -->
                <action value="redirect">
                    <!-- Shorthand -->
                    <synonym value="r" />
                </action>
                <!-- Supported synonyms for the Delegate action -->
                <action value="delegate">

```

```

<!-- Shorthand -->
<synonym value="d" />
</action>
<!-- Supported synonyms for the Sleep action -->
<action value="sleep">
    <!-- Shorthand -->
    <synonym value="s" />
</action>
<!-- Supported synonyms for the Help action -->
<action value="help">
    <synonym value="h" />
    <synonym value="?" />
</action>
<!-- Supported synonyms for the Actions action -->
<action value="actions">
    <synonym value="a" />
</action>
</actionsStandard>
<actionsConfigured>
    <!-- Common configured actions and allowable alternatives -->
    <!--
        <action value="approve">
            <synonym value="approved" />
        </action>
        <action value="decline">
            <synonym value="declined" />
            <synonym>reject</synonym>
            <synonym value="rejected" />
        </action>
    -->
</actionsConfigured>
</synonyms>
</smartActions>
</messageBus>

```

Configuration File Description	
<actionsStandard>	Standard or system actions that are used by the K2 Server to process messaging notifications
<actionsConfigured>	A user configured action which is used by the K2 Server to process messaging notifications*
<synonym>	A single character or word that the K2 Server is instructed to associate with a actionConfigured or actionSystem.
<messages>	Messages sent by the system which are extracted from template files which contain pre configured messages. These can be customized to suit individual needs.

* actionsStandard take precedence over actionsConfigured ie if both are entered at the same time then the actionsStandard would be processed and the actionsConfigured will be ignored.

K2 SmartAction Messaging Template Files

The messages that are used by the K2 Server are all located in the following location ...**K2 blackpearl\Host Server\Bin\Templates\Messages**. Located in the folder is a collection of text files which can be updated to include information to fit your organization's needs. When the files are opened you will notice that the text file is a combination of plain text and fields which are populated when the message is sent to the Information Worker. Shown below is an image of the folder along with a list of the text files that can be expected and found in that location.

- Message Bus System Error Messaging Templates
 - MessageBus.Error
 - MessageBus.Help
 - MessageBus.ReplyFormat
 - MessageBus.UnHandledError
- For SmartActions Messaging
 - SmartActions.ActionExecuted

- SmartActions.Actions
- SmartActions.Delegate
- SmartActions.DelegateError
- SmartActions.Error
- SmartActions.Help
- SmartActions.ItemNotFound
- SmartActions.Redirect
- SmartActions.RedirectError
- SmartActions.Sleep
- SmartActions.SleepError
- SmartActions.StandardActions
- SmartActions.StandardActionsWithDescriptions
- SmartActions.UnhandledError



The text files are system files and designed to work in conjunction with the K2 Server. Although they can be modified, it is recommended that the messaging remains as is unless specific organizational requirements require that they be changed.

Shown below is an example of one of the text files namely the **SmartActions.ActionExecuted.txt** file. The fields indicated by the {} brackets are populated at run time when the e-mail is sent to the information worker. The wording can be change, but if these fields are removed from the text crucial information relating the worklist item will be lost.



If the text file is changed to include HTML for corporate branding purposes, this feature is currently unsupported and the html would appear as plain text in the e-mail received by the information worker.

Action Executed

```
On {date} you successfully actioned the worklist item:  
Action: {action}  
Serial Number: {serial number}
```

1.6.8.6.1.1 SmartAction Synonyms

K2 SmartAction Synonyms

Synonyms are used to cater for scenarios where the respondent may enter a similar word to one that has been designated as an Action. Synonyms apply equally for actionsStandard or actionsConfigured. A synonym does not have to be similar to the action word in any way. The Synonym is mapped to the Action and the K2 Server will respond to the synonym as if it were an action.

The following guidelines should be applied when deciding which synonyms to use:

- The case of the lettering is not important as SmartAction is case in-sensitive
- Single words preferred as best practice
- phrases or clauses are not supported ie **approve this item**
- underscores between words are supported for example **approve_this_item**



Synonyms must be unique for each action, if there are duplicate synonyms shared by more than one action the K2 Server will throw an exception. Duplicate synonyms are not allowed.

Synonyms Configuration

```
<action value="decline">
    <synonym value="declined" />
    <synonym value="reject" />
    <synonym value="rejected" />
</action>
```

Reserved Words

Strictly speaking, the concept of reserved words does not apply to K2 SmartActions. The following words are used as system actions, but not reserved as such. They can be used as synonyms however to ensure that the user gets the expected results and not anomalous results it is recommended that they be treated as reserved words..

- Help
- Redirect
- Delegate
- Sleep

1.6.8.6.2 E-mail ProtocolSetup



This topic outlines the messaging protocols which require additional setup post installation in order to be SmartActions-enabled. The Exchange Server option is omitted from this section as it is supported out of the box.



For all options supported, the K2 Server requires a unique e-mail address to be configured before the K2 installation or upgrade proceeds. If no e-mail address is available and K2 SmartActions is a requirement for installation, it is advised that the installation be postponed or the K2 SmartActions option not be installed until the e-mail address is available.

Overview to Manual E-mail Configuration

Configuring the e-mail options manually requires that connection strings are added to the K2 Server configuration file (K2hostserver.exe.config). The <connectionStrings> section of the config file is encrypted. To edit the connection strings the user needs to delete the entire section:



Copy Delete the encrypted connection string

```
<!-- Host Server DB Connection Settings -->
<connectionStrings configProtectionProvider="K2ConfigurationKey">
    ...
</connectionStrings>
```

And replace it with a copy of the commented-out section at the bottom of the file under the text:

****** USE THE SETTINGS BELOW TO REPLACE ENCRYPTED SECTION..
**** CONNECTION STRINGS WILL AUTOMATICALLY BE ENCRYPTED ON STARTUP..**



Copy Replace it with this section:

```
<connectionStrings>
    <add name="HostserverDB" connectionString="Data Source=SERVERNAME;Initial Catalog=K2HostServer;integrated security=sspi;Pooling=True" />
    <add
        name="SourceCode.MessageBus.Ews.ExchangeWebServicesConnection:administrator@denallix.com"
        connectionString="Autodiscover={True/False};Url={EWS URL, not supported if Autodiscover is True};User ID={Login User,optional};Password={Password,optional}" />
        <add name="SourceCode.Net.Mail.SmtpConnection:administrator@denallix.com"
        connectionString="Host Name={SMTP Server};Port={Port;Default 25};Tls={BootTls/None};Authentication={Windows/Plain};User ID={Login User,optional};Password={Password,optional}" />
        <add name="SourceCode.Net.Mail.SmtpConnection" connectionString="Host Name={SMTP Server};Port={Port;Default 25};Tls={BootTls/None};Authentication=Anonymous" />
    </connectionStrings>
```

Then the user needs to edit the section to match the local environment and restart the server to re-encrypt the connection strings section.

It is best-practice to back-up the K2hostserver.exe.config file before editing it.

Use the following guidelines for populating the connection strings manually:

- Multiple accounts per origin (listener, e.g. Exchange Web Services) and destination (e.g. SMTP) are supported
- Specify the type of connection using the connection string name, for example:
 - SourceCode.MessageBus.Ews.ExchangeWebServicesConnection:K2Service@Denallix.com
 - The first portion (before ':') of the name is the connection type.
 - The second portion (after ':') is the account for the connection.
- The accounts as per the second portion are the e-mail addresses returned by the URM.

EWS



Exchange Autodiscover must be set up on the domain for "Autodiscover=True" to work.

Each EWS connection is started at server boot time, it is recommended to only have one – but multiple accounts are supported. The connection string takes the format:



Copy Connection String Format

```
Autodiscover={True/False};Url={EWS URL, not supported if Autodiscover is True};User ID={Login User,optional};Password={Password,optional};Poll
```

```
Interval={Optional, Default 30S}
```

- User ID and Password are optional
- Url is required if Autodiscover is "False"
- Url is not supported if Autodiscover is "True".

Thus valid connection strings are:



Copy Valid Connection String Examples

```
<connectionStrings>
  <add name="HostserverDB" connectionString="Data Source=SERVERNAME;Initial Catalog=K2HostServer;integrated security=sspi;Pooling=True" />

  <add
  name="SourceCode.MessageBus.Ews.ExchangeWebServicesConnection:system@k2.local"
  connectionString="Autodiscover={True/False};Url={EWS URL,not supported if
  Autodiscover is True};User ID={Login User,optional};Password=
  {Password,optional};Poll Interval={Optional, Default 30S}" />

  <add name="SourceCode.Net.Mail.SmtpConnection:system@k2.local"
  connectionString="Host Name={SMTP Server};Port={Port;Default 25};Tls=
  {BootTls/None};Authentication={Windows/Plain};User ID={Login
  User,optional};Password={Password,optional}" />

  <add name="SourceCode.Net.Mail.SmtpConnection" connectionString="Host
  Name={SMTP Server};Port={Port;Default 25};Tls=
  {BootTls/None};Authentication=Anonymous" />
</connectionStrings>
```

String definitions:

- **HostServerDB:** the string for connecting to the host server.
- **ExchangeWebServicesConnection:** this is the EWS string the user would modify to set the polling interval.
- **SmtpConnection 1:** This is the authenticated SMTP account (a match is made according to email). The user may add multiple accounts.
- **SmtpConnection 2:** This is the fallback account in case direct account match is found. In 90% of cases it should be anonymous (SMTP relay).

Poll Interval: You can use S, M, H, D for the units (seconds, minutes, hours, days respectively). Remember if you manually update the connection strings you need to replace the old connectionStrings element. It is also recommend that you keep a backup of what you paste in as the section automatically gets encrypted when HostServer boots. Remember that the poll interval is also ignored if the previous check resulted in mail – it only comes into play when a check for mail returned nothing.

SMTP

SMTP accounts are discovered (using the connection string type "SourceCode.Net.Mail.SmtpConnection") when a message is sent via SMTP; if no connection string can be found for a specific address a connection string with the exact name "SourceCode.Net.Mail.SmtpConnection" is used (it is recommended that this connection string is present and anonymous). The connection strings take the format:



Copy Connection String Format

```
Host Name={SMTP Server};Port={Port};Tls={BootTls/None};Authentication=
{Windows/Plain/Anonymous};User ID={Login User};Password={Password}
```

- Port is optional and defaults to 25
- User ID and Password are optional and are only valid when Authentication is "Plain"
- STARTTLS is always used when the server supports it. If connecting to a SSL port (Boot TLS) specify BootTls.

Thus valid connection strings are:



Copy Valid connection string examples

```
<add name="SourceCode.Net.Mail.SmtpConnection" connectionString="Host
Name=mail.denallix.com;Authentication=Anonymous" />
```

'It is recommended to have an anonymous connection string, such as this example, unless all the ""addresses that all the K2 processes use are known '(notably, mail events) -in this scenario specify a connection string for each from address.

```
<add name="SourceCode.Net.Mail.SmtpConnection:K2Service@Denallix.com"  
connectionString="Host Name=mail.denallix.com;Authentication=Windows" />  
  
<add name="SourceCode.Net.Mail.SmtpConnection:SmartActions@Denallix.com"  
connectionString="Host Name=mail.denallix.com;Authentication=Plain;User  
ID=SmartActions;Password=K2pass" />  
  
<add name="SourceCode.Net.Mail.SmtpConnection:K2Service@Denallix.com"  
connectionString="Host  
Name=mail.denallix.com;Port=567;Tls=BootTls;Authentication=Windows" />
```



It is recommended to use authenticated SMTP for known accounts (Authentication is not "Anonymous") as most mail servers will not spam filter authenticated SMTP messages.

Further Notes

Remember to retain any database connection strings, for example "HostServerDB".

1.6.8.6.3 K2 SmartActions E-mail Security

Customizing the E-mail Security

Discussed below are some of the options for customizing the e-mail security. These settings are configurable by the K2 Administrator using settings in the K2HostServer.config file. The expectation is that e-mail communication is between authenticated e-mail servers, but since this may not always be the case, the following settings and options need to be considered when configuring K2 SmartActions.

The settings can be located in the configuration > messageBus > system element, and the details are as follows.

Sample Configuration Code

```
<system self="K2:DENALLIX\K2Service" enableListeners="false" ambiguity="true">
    <security spamSecurity="InternalMail">
        <authorizedDomains />
    </security>
</system>
```

A primary consideration for the K2 Administrator is to ensure that the inter K2 Server - Client user e-mail communication remains safe and spoof / spam and phishing proof.

System Self

This main element holds the identity of the FQN for the K2 Server and remains the same unless integrated authentication is not used. Only the SMTP protocol is currently supported for K2 SmartActions and if integrated authentication is used then the FQN is required.

In most cases the K2 Service's domain account is the same as the internal domain.

Example Title

```
system self = " [security label]: [FQN] \ [Service Account Name]"
```

The listeners are the e-mail servers and Exchange is enabled by default. This element is either true or false. This setting is enabled in the K2 Configuration file and a change in the config file require a server restart.

Example Title

```
enableListeners="false"
```

spamSecurity

The spamSecurity element leverages the Exchange SCL (Spam Confidence Level) header to reject messages that may not be from authenticated users. To configure the spamSecurity setting its value can either be one of the constants, or an integer.

Setting Description	
Internal Mail (SCL -1)	Only mail sent to the Exchange server by an authenticated account controlled by the Exchange server receives this SCL rating
Low	SCL 0
High	SCL 1
Custom value	An integer greater than -1
Off	Disables the SCL Header rejection feature. No messages will be rejected as the SCL header is being completely ignored.



If a message does not contain an SCL Header, and the spamSetting is set to "Off" a message with no SCL header can be accepted. If there is no SCL header and the SCL header settings are enabled, the message is rejected.

authorizedDomains

This portion of K2 SmartActions security uses the receive header of the incoming e-mail to verify its authenticity. The received header is used to validate that the mail traversed trusted servers only. For this feature to be usable it requires that the header is completely valid as per RFC822 (<http://www.ietf.org/rfc/rfc0822.txt>). Not all servers are compliant with this standard and some mail servers do not create valid Received headers.

This setting also supports the slight variation that Exchange adds. The following portions of the incoming e-mail are checked by, from and via parts are checked if they are present. If the element is empty or not present all domains are trusted, meaning this security check is skipped.

Example Code

```
<authorizedDomains>
  <add domain="*.denallix.com" />
  <add domain="*.google.com" />
  <add domain="*.gmail.com" />
  <add domain="*.live.com" />
</authorizedDomains>
```

Security Recommendations

Since each process contains a unique serial number, the threat level which may result in a breach of security needs to be determined by your organization. The K2 Server will only action processes for which there has been an instantiation and the incoming e-mail contains a valid serial number. Unless the K2 Server can authenticate the incoming message and associate the serial number with an existing valid process instance, a spoof e-mail will have no impact on the corporate operations.

Two examples are shown below offering opposite extremes of security. The first is the most secure and the second is the least secure. Most secure configuration, using the fictitious Denallix domain as an example.

High Level SPAM Security Example

```
<security spamSecurity="InternalMail">
  <authorizedDomains>
    <add domain="*.denallix.com" />
  </authorizedDomains>
</security>
```

The least secure configuration is as follows. This option is not recommended as it completely disables mail security and may expose the network to attacks.

Low Level SPAM Security Example

```
<security spamSecurity="Off" />
```

Ambiguity Configuration

The K2 environment can be configured to allow for multiple Labels to use the same provider. Each label would have an e-mail address associated with it. This means that multiple e-mail addresses could be found for the same user with each address being associated with a single label and unique to that label.

The following logic would apply:

1. Get all the users under all the labels which have the incoming email address
2. Sort the returned list of users according to their label alphabetically
3. Place the default label first in the list
4. Attempt to action the worklist item using the users in the list; in order

The outcome is that the end user would receive an e-mail notification for each of their email addresses that are found by the K2 Server. Each e-mail notification is however an independent notification with a unique serial number. If for example the end user actions an e-mail for the default label that item has been actioned and no further actions will be processed for the default label.

Shown below is the ambiguity configuration setting which is set be default to true. When true, the above functionality is operational. To disable, set the flag to false.

Sample Configuration Code

```
<system allowAmbiguity="true" self="K2:POINTDISTRO\smartactions"
enableListeners="true" >
  <security spamSecurity="Off"/>
</system>
```

Ambiguity Tags	
<ambiguity>	When true enables support for ambiguous environments where 2 Labels e.g. K2 and a Claims based environments would use the same provider.

1.6.8.7 Introduction to User Managers

Introduction to User Managers

Use this topic to familiarize yourself with user authentication, authorization and labels in K2.

Definitions

The following key terms are used throughout this section.

User Manager: All configurations necessary to associate K2 with an identity store, such as the security provider, security label, authentication provider and role provider.

Security Label: Also called K2 Label, User Label and simply Label, it is the token string that is pre-pended to the user's identity, for example the 'K2' label is used for Active Directory users by default, which appear in the K2 context as K2:[Domain\Username]. The context for the label does not extend beyond the K2 platform. The Security Label identifies specific instances of Authentication Providers and/or Role Providers.

Security Provider: The implementation of an authentication mechanism represented by a set of interfaces for interacting with an identity store and authenticating users located in that store.

Authentication Provider: The mechanism to confirm the identity of a user when they login or interact with services and data sources. User authentication is performed by passing a set of user credentials. Authentication can be integrated or require the use of a prompt or a web-based form.

Role Provider: The mechanism by which users and groups are resolved in K2 from the identity store.

Fully Qualified Name (FQN): The FQN is the user or role value in [Security Label]:[User/Role Name] format used by K2 for authorization such as assigning tasks, interacting with tasks or assigning permissions.



K2 will prepend the security label for the default user manager when an authentication request occurs without a security label.

Available User Managers

Active Directory (Default): requires access to Active Directory domain functional level Windows 2003 or higher to provide authentication and roles. Active Directory (AD) must be installed and available at the time of installation to configure the AD user manager.

SQL: requires access to the SQL user manager database, K2SQLUM by default, to provide authentication and roles. SQL user manager can be configured as a non-default user manager or as the default user manager either during or post installation.

LDAP: requires access to a LDAP-compatible system with protocol version 3 or higher to provide authentication and roles. LDAP user manager can be configured as a non-default user manager.

Custom: requires access to the custom identity store to provide authentication and roles. Custom user manager can be configured as a non-default user manager or as the default user manager post installation.

User Managers				
	Active Directory	SQL	LDAP	Custom
Security Label – Default Value	K2	K2SQL	K2LDAP	{Custom}
Can be configured as default during installation?	Yes	Yes	No	No
Can be configured as default post installation?	No	Yes*	No	Yes*
Can be configured as non-default post installation?	No	Yes	Yes	Yes
Can be configured with multiple security labels?	No	Yes	Yes ⁺	Yes ⁺

* For more information, please refer to Changing the Default User Manager.
 +The LDAP User Manager implements two IHostableSecurityProviders .NET types -
 SourceCode.Security.Providers.LdapProvider.Forms.Ldap and
 SourceCode.Security.Providers.LdapProvider.Trusted.Ldap - each can only be configured for a single security label. Each Custom User Manager .NET type that implements IHostableSecurityProvider can only be configured for a single security label.

Installing K2

The following default user manager installation scenarios are available out of the box:

- Active Directory
- SQL

Additional user managers can be added post-installation:

- SQL
- LDAP
- Custom



The installation procedure requires that a User Manager is available during the course of the installation; prompts for user credentials form part of the process and must be validated before the installation can be completed.



Only one security label can be registered for each User Manager .NET type that implements `IHostableSecurityProvider`. See the User Managers table above for more information.

Refresh the User Manager Cache

Any change in the configuration of user managers will require an update of the existing user cache. Download and execute the SQL command against the K2HostServer database.



```
UPDATE [K2HostServer].[Identity].[Identity]
SET [ExpireOn] = GETDATE()
, [Resolved] = 0
, [ContainersResolved] = 0
, [ContainersExpireOn] = GETDATE()
, [MembersResolved] = 0
, [MembersExpireOn] = GETDATE()
```

GO

Additional Considerations

The K2 Event Bus utilizes MSMQ and Active Directory. Because of this the K2 Event Bus will be unable to function if SQL or a custom user manager is used in place of AD unless a custom Event Recorder is introduced as well. For more information, see [How to add a 3rd-party event recorder to the K2 blackpearl Server](#).

K2 configuration for non-AD users and SharePoint 2010 requires a claims based SharePoint web application. For more information see [Claims - based Authentication](#).

K2 configuration for non-AD users and SharePoint 2007 is not supported.

All Users

K2 does not support a concept of "All Users" for assigning tasks, interacting with tasks or assigning permissions. Built-in or configured groups for the appropriate K2 user manager, for example Domain Users for Active Directory, should be used instead.

The following "All Users" containers are not supported by K2.

Active Directory, SharePoint 2007 and SharePoint 2010 classic-mode

- NT Authority\Authenticated Users

SharePoint 2010 claims-mode

- All Authenticated Users
- All Users (*{WindowsProvider}*), aka NT AUTHORITY\Authenticated Users
- All Users (*{FormsProvider}*)
- All Users (*{TrustedProvider}*)

1.6.8.7.1 Introduction to User Managers

Introduction to User Managers

Use this topic to familiarize yourself with user authentication, authorization and labels in K2.

Definitions

The following key terms are used throughout this section.

User Manager: All configurations necessary to associate K2 with an identity store, such as the security provider, security label, authentication provider and role provider.

Security Label: Also called K2 Label, User Label and simply Label, it is the token string that is pre-pended to the user's identity, for example the 'K2' label is used for Active Directory users by default, which appear in the K2 context as K2:[Domain\Username]. The context for the label does not extend beyond the K2 platform. The Security Label identifies specific instances of Authentication Providers and/or Role Providers.

Security Provider: The implementation of an authentication mechanism represented by a set of interfaces for interacting with an identity store and authenticating users located in that store.

Authentication Provider: The mechanism to confirm the identity of a user when they login or interact with services and data sources. User authentication is performed by passing a set of user credentials. Authentication can be integrated or require the use of a prompt or a web-based form.

Role Provider: The mechanism by which users and groups are resolved in K2 from the identity store.

Fully Qualified Name (FQN): The FQN is the user or role value in [Security Label]:[User/Role Name] format used by K2 for authorization such as assigning tasks, interacting with tasks or assigning permissions.



K2 will prepend the security label for the default user manager when an authentication request occurs without a security label.

Available User Managers

Active Directory (Default): requires access to Active Directory domain functional level Windows 2003 or higher to provide authentication and roles. Active Directory (AD) must be installed and available at the time of installation to configure the AD user manager.

SQL: requires access to the SQL user manager database, K2SQLUM by default, to provide authentication and roles. SQL user manager can be configured as a non-default user manager or as the default user manager either during or post installation.

LDAP: requires access to a LDAP-compatible system with protocol version 3 or higher to provide authentication and roles. LDAP user manager can be configured as a non-default user manager.

Custom: requires access to the custom identity store to provide authentication and roles. Custom user manager can be configured as a non-default user manager or as the default user manager post installation.

User Managers				
	Active Directory	SQL	LDAP	Custom
Security Label – Default Value	K2	K2SQL	K2LDAP	{Custom}
Can be configured as default during installation?	Yes	Yes	No	No
Can be configured as default post installation?	No	Yes*	No	Yes*
Can be configured as non-default post installation?	No	Yes	Yes	Yes
Can be configured with multiple security labels?	No	Yes	Yes ⁺	Yes ⁺

* For more information, please refer to Changing the Default User Manager.
 +The LDAP User Manager implements two IHostableSecurityProviders .NET types -
 SourceCode.Security.Providers.LdapProvider.Forms.Ldap and
 SourceCode.Security.Providers.LdapProvider.Trusted.Ldap - each can only be configured for a single security label. Each Custom User Manager .NET type that implements IHostableSecurityProvider can only be configured for a single security label.

Installing K2

The following default user manager installation scenarios are available out of the box:

- Active Directory
- SQL

Additional user managers can be added post-installation:

- SQL
- LDAP
- Custom



The installation procedure requires that a User Manager is available during the course of the installation; prompts for user credentials form part of the process and must be validated before the installation can be completed.



Only one security label can be registered for each User Manager .NET type that implements `IHostableSecurityProvider`. See the User Managers table above for more information.

Refresh the User Manager Cache

Any change in the configuration of user managers will require an update of the existing user cache. Download and execute the SQL command against the K2HostServer database.



```
UPDATE [K2HostServer].[Identity].[Identity]
SET [ExpireOn] = GETDATE()
, [Resolved] = 0
, [ContainersResolved] = 0
, [ContainersExpireOn] = GETDATE()
, [MembersResolved] = 0
, [MembersExpireOn] = GETDATE()
```

GO

Additional Considerations

The K2 Event Bus utilizes MSMQ and Active Directory. Because of this the K2 Event Bus will be unable to function if SQL or a custom user manager is used in place of AD unless a custom Event Recorder is introduced as well. For more information, see [How to add a 3rd-party event recorder to the K2 blackpearl Server](#).

K2 configuration for non-AD users and SharePoint 2010 requires a claims based SharePoint web application. For more information see [Claims - based Authentication](#).

K2 configuration for non-AD users and SharePoint 2007 is not supported.

All Users

K2 does not support a concept of "All Users" for assigning tasks, interacting with tasks or assigning permissions. Built-in or configured groups for the appropriate K2 user manager, for example Domain Users for Active Directory, should be used instead.

The following "All Users" containers are not supported by K2.

Active Directory, SharePoint 2007 and SharePoint 2010 classic-mode

- NT Authority\Authenticated Users

SharePoint 2010 claims-mode

- All Authenticated Users
- All Users (*{WindowsProvider}*), aka NT AUTHORITY\Authenticated Users
- All Users (*{FormsProvider}*)
- All Users (*{TrustedProvider}*)

1.6.8.7.2 Active Directory User Manager

Active Directory User Manager (ADUM)

The Active Directory user manager is the default user manager that is installed on most systems.



- K2 blackpearl supports the use of multiple domains. However, there can be only one label for an AD Provider. See also [Adding Multiple Active Directory Domains](#)
- Only one AD user manager can be registered in an environment, but multiple SQL, LDAP and Custom user managers are supported.

1.6.8.7.2.1 Configuring the Active Directory User Manager

Configuring the Active Directory User Manager



All values below are by default disabled; default cache timeout is set to 10 minutes.

The Settings node implements features that may impact performance from caching users to excluding certain operations. These options are discussed in greater detail in the relevant topics. The following features provide performance enhancements for the AD user manager.

User Manager Settings

- Click on the **Settings** option.
- The following **K2 Settings** screen will open:

Fig. 1. K2 User Manager Settings

When a query is passed to the AD user manager, it will return all results in the query unless the number of users is limited or one of the other settings affects the number of users returned. Limiting the number of users and groups returned will enhance performance by ensuring that a manageable number of items are returned.



There is a **Settings** node directly under User Managers node that is used to limit the number of items returned from any registered user manager. The default for this is 100.



Keep in mind that when granting rights to all users in the domain, it is more efficient to use the built-in Domain Users group rather than an AD group that may contain all domain users.

Service Instance Properties

The number of users are limited by configuring the Service Instance Properties.

Settings	Description
Cache Timeout	When a user's credentials are used for the first time, they are cached. If the user credentials are required again within the timeout period, the cached credentials will be supplied. If the timeout period has expired, the system will interrogate the AD user manager to return user authentication. The timeout interval is specified in whole minutes only.
Resolve Nested Groups	Groups within AD user manager may contain sub or nested groups within a group. The users within these nested groups will be resolved when this option is enabled.

Ignore Foreign Principals	This setting will either allow (if False) or deny (if True) membership principals from foreign domains resolving on K2 Server. Also referred to as Cross-Domain or Cross-Forest membership. ForeignSecurityPrincipals allows users from a different domain (i.e. DOMAIN-B) to become members of groups on another domain (i.e. DOMAIN-A). If a group contains a foreign principal, and this setting is False, the user will be resolved against K2. If the setting is set to True, the user/group will not be resolved.
Ignore User Groups	This option enables the Administrator to exclude user groups from being resolved and only the user accounts will be resolved as part of the current domains.

Additional Information

For further information on the Active Directory User Manager, see the following resource:

- How to register labels against multiple domains: <http://help.k2.com/en/KB000182.aspx>

1.6.8.7.3 Introduction to K2 LDAP Provider

Introduction to K2 LDAP Provider

The K2 LDAP user manager is designed for LDAP-compatible systems with protocol version 3 or higher. It has been tested with Active Directory domain functional level Windows 2003.



Disclaimer: The K2 LDAP user manager is expected to be configurable for any LDAP-compatible system with protocol version 3 or higher. However, only Microsoft's Active Directory LDAP store has been tested.

1.6.8.7.3.1 Configuring the LDAP User Manager

Configuring the LDAP User Manager

Use this topic to configure the K2 LDAP user manager.

The script, included below, is for the fictitious Denallix.com domain, and returns Denallix AD-based LDAP users and groups. You can modify this file to suit your environment.

There are many settings available mainly due to the nature of LDAP and the various implementations. Each user directory implements different methodologies, and, for example, very few AD-based LDAP queries work on Novell. Once you understand these settings, you should be able to make K2 work with your user directory.

LdapConnection

- **LdapServer:** This is the server or directory name (e.g. "denallix.com" or "mydns"). This setting is like the server setting in the SharePoint configuration.
- **LdapServerPort:** This is the port for the connection. This can be 0 for the default (usually 389) or you can set a different one, such as for SSL (usually 636). This setting is like the port setting in the SharePoint configuration.
- **LdapAuthTypeConnect:** This is the type of connection K2 makes whenever it queries the directory (e.g. for user information, group membership etc.). "Negotiate" would be the simplest for AD, but if you need a username and password then Basic would be an alternative. For more information see [AuthType Enumeration \(MSDN\)](#)



This value should be set to Negotiate as it will use NTLM or Kerberos depending on the underlying requirement.

- **LdapAuthTypeAuthenticateUser:** This is the type of connection K2 makes whenever it authenticates a user (giving their credentials). "Negotiate" would be the simplest for AD, but if you need a username and password then Basic would be an alternative. For more information see [AuthType Enumeration \(MSDN\)](#)



This value should be set to Negotiate as it will use NTLM or Kerberos depending on the underlying requirement.

- **LdapResolveAuthenticationUserToDistinguishedName:** In some directories (e.g. Novell) users are logged on with their distinguished name instead of their actual user name. If this is true, K2 takes the user's name and query the directory in order to retrieve the distinguished name. If users are logging in with their distinguished names (e.g. passing it in the K2 connection string), then this should be false as there's no need to resolve it.
- **LdapAutoBind:** Whether or not explicit binding is avoided in the connection (LDAP connects first, and then binds to validate the connection). This is a compatibility setting and can usually be left false.
- **LdapScope:** This is the scope of user searches. Unless you have specific requirements (such as only searching in a root OU), then "Subtree" would be the recommended option. For more information see [SearchScope Enumeration \(MSDN\)](#). This setting is like the scope setting in the SharePoint configuration.
- **LdapConnectIntegrated:** Whether or not the connection has integrated authentication. If LdapAuthTypeConnect is something like "NTLM", this would need to be true. This only correlates to K2's own connections, as end users will not make integrated connections.
- **LdapConnectUserName:** If the LDAP directory doesn't support integrated connections or you want to use an account different to the K2 Service account, then K2 will use this user to connect to query the directory. Some directories support connections with blank username/password for general queries, but you may find that you only receive a limited number of attributes.
- **LdapConnectUserPassword:** The password for the above user.
- **LdapTimeout:** A timeout for LDAP queries (in seconds). 0 means to use the default.
- **LdapProtocolVersion:** The LDAP protocol version to use. 3 is recommended, but 2 should also work.
- **LdapSsl:** Whether the connection uses SSL (ensure that the port used reflects this). This setting is like the `useSSL` setting in the SharePoint configuration.
- **LdapServerCertificatePath:** If you are using SSL, this is an optional value that allows you to verify the LDAP server's SSL certificate (to ensure someone isn't spoofing your user directory). This provides a local path (on the K2 server) where the certificate can be found. If no certificate is supplied and you're doing SSL, then K2 will assume that you don't want to check it and SSL will proceed regardless.

LdapUserSearchFormatString

This is the LDAP query used to search for users. It should include a placeholder "{0}" for where the users ID should be inserted. Don't include any wildcards, as these are handled automatically. As this is in XML, any reserved XML characters (e.g. &) should be escaped. For example:

```
(&objectClass=Person)(objectCategory=User)(samAccountName={0})
```

LdapUserGroupSearchFormatString

This is the LDAP query used to search for users that belong to a specific group. It should include a placeholder "{0}" for where the group's ID should be inserted. Don't include any wildcards, as these are handled automatically. As this

is in XML, any reserved XML characters (e.g. &) should be escaped. For example, to return users from this specific group and all nested groups:

```
(memberOf :1.2.840.113556.1.4.1941:={0})
```

For more information see [Search Filter Syntax \(MSDN\)](#).

LdapGroupSearchFormatString

This is the LDAP query used to search for groups. It should include a placeholder "{0}" for where the user's ID should be inserted. Don't include any wildcards, as these are handled automatically. As this is in XML, any reserved XML characters (e.g. &) should be escaped. For example:

```
(&(objectCategory=Group)(samAccountName={0}))
```

LdapGroupMemberSearchFormatString

This is the LDAP query used to search for groups of which the user is a member. It should include a placeholder "{0}" for where the user's ID should be inserted. Don't include any wildcards, as these are handled automatically. As this is in XML, any reserved XML characters (e.g. &) should be escaped. For example, to return groups and all nested groups of which the user is a member :

```
(member:1.2.840.113556.1.4.1941:={0})
```

For more information see [Search Filter Syntax \(MSDN\)](#).

LdapUserBaseObject

This is the LDAP base object from which all user searches are made. Make sure that this correlates correctly to your LdapScope setting above. This setting is like the **userContainer** setting in the SharePoint configuration. For example:

```
dc=denallix,dc=com
```

LdapGroupBaseObject

This is the LDAP base object from which all group searches are made. Make sure that this correlates correctly to your LdapScope setting above. This setting is like the **groupContainer** setting in the SharePoint configuration. For example:

```
dc=denallix,dc=com
```

LdapUserAttributes

The following is the set of attributes that are used in your directory. The available settings for each attribute are:

K2Name: If K2 supports this attribute, then this is the name it knows it by. You should stick to the names supplied otherwise K2 will not know how to use the property. This name is case sensitive.

LDAPName: This is the name used in the LDAP directory (e.g. samAccountName). LDAP is generally case insensitive, however care should be taken with setting these properties as it is possible to have case sensitive implementations. If this value is blank, K2 will take the distinguished name of the object.

ObjectType: This is so that K2 knows what it's retrieving from this property. Currently, only System.String (a string value) and System.Collections.ArrayList (a collection of values) are supported.

Multiline: Typically, properties are only found on the first line. However, some values (such as description) can be on multiple lines and therefore setting this property will make K2 concatenate these values.

FullOnly: If this item is of something that is time consuming to retrieve (e.g. group members, which all have to be resolved), setting this to true means it will only be retrieved in full searches such as when one specific user is retrieved and not when a set of users are being searched for. If you find delays in searches, set this to true on as many properties as possible unless you find issues in K2 functionality.

SearchQuery: Some LDAP properties only include a distinguished name (e.g. memberOf). If you want to search for the user/group of that distinguished name, in order to replace this value with one K2 will recognize, you can supply a query here and it will use this for the search. This is always a distinguished name and because of that there is no need for any placeholders, so it should be a complete query.

SearchResultProperty: If you are using a SearchQuery, this specifies the property of the returned object you'd like to retrieve (e.g. samAccountName). This will then replace the distinguished name originally retrieved for the attribute.

The minimum set of required attributes for resolving users and groups is ID, Name, DistinguishedName and Description (where ID and Name are usually the same). Others may be used in K2 and therefore should be included where possible (e.g. e-mail, manager), but they are not required for base functionality.

If you find that your queries are returning only a small number of attributes, it may mean that your connection user does not have sufficient privileges.

LdapGroupAttributes

As above, except these attributes would be the ones returned for groups.



The K2LDAP label will be visible in K2 where labels normally appear such as Management Console in K2 Workspace with the exception of Microsoft SharePoint 2010.

Example

The following example is for the fictitious Denallix.com domain and is inserted into the SecurityLabels table of the K2HostServer database. You must change some of the values below to match your environment. This is the same XML that is included in the downloadable script file.



```
<AuthInit>
  <LdapConnection
    LdapServer="dlx.denallix.com"
    LdapServerPort="389"
    LdapSsl="false"
    LdapAuthTypeConnect="Negotiate"
    LdapAuthTypeAuthenticateUser="Negotiate"
    LdapResolveAuthenticationUserToDistinguishedName="false"
    LdapAutoBind="false"
    LdapScope="Subtree"
    LdapConnectIntegrated="true"
    LdapConnectUserName=""
    LdapConnectUserPassword=""
    LdapTimeout="0"
    LdapProtocolVersion="3"
    LdapServerCertificatePath="" />
  <LdapUserBaseObject>dc=denallix,dc=com</LdapUserBaseObject>
  <LdapUserSearchFormatString>(& (objectClass=Person)
  (objectCategory=User) (samAccountName={0}))</LdapUserSearchFormatString>
  <LdapUserGroupSearchFormatString>
  (memberOf:1.2.840.113556.1.4.1941:={0})</LdapUserGroupSearchFormatString>
  <LdapUserAttributes>
    <K2LdapMapping K2Name="ID" LdapName="samAccountName"
    ObjectType="System.String" />
    <K2LdapMapping K2Name="Name" LdapName="samAccountName"
    ObjectType="System.String" />
    <K2LdapMapping K2Name="Description" Multiline="true"
    LdapName="description" ObjectType="System.String" />
    <K2LdapMapping K2Name="Email" LdapName="mail"
    ObjectType="System.String" />
    <K2LdapMapping K2Name="DistinguishedName"
    LdapName="distinguishedName" ObjectType="System.String" />
    <K2LdapMapping K2Name="ObjectSID" FullOnly="true"
    LdapName="objectSID" ObjectType="System.String" />
    <K2LdapMapping K2Name="CommonName" LdapName="cn"
    ObjectType="System.String" />
    <K2LdapMapping K2Name="UserPrincipalName"
    LdapName="userPrincipalName" ObjectType="System.String" />
    <K2LdapMapping K2Name="Manager" FullOnly="true"
    LdapName="manager" ObjectType="System.String" SearchQuery="(& (objectClass=Person) (objectCategory=User))"
    SearchResultProperty="samAccountName" />
    <K2LdapMapping K2Name="SipAccount" LdapName="msRTCSIP-
    PrimaryUserAddress" ObjectType="System.String" />
    <K2LdapMapping K2Name="DisplayName"
    LdapName="displayName" ObjectType="System.String" />
    <K2LdapMapping K2Name="TelephoneNumber"
```

```

        LdapName="telephoneNumber" ObjectType="System.String" />
            <K2LdapMapping K2Name="Mobile" LdapName="mobile"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="HomePage" LdapName="wWWHomePage"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="FaxNumber"
        LdapName="facsimileTelephoneNumber"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="HomePhone" LdapName="homePhone"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="IPPhone" LdapName="ipPhone"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="StreetAddress"
        LdapName="streetAddress" ObjectType="System.String" />
            <K2LdapMapping K2Name="City" LdapName="l"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Country" LdapName="c"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="State" LdapName="st"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Title" LdapName="title"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Department" LdapName="department"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Company" LdapName="company"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Office"
        LdapName="physicalDeliveryOfficeName"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="ManagedUsers" FullOnly="true"
        LdapName="managedUsers" SearchQuery="(&#
        (objectClass=Person) (objectCategory=User))"
        SearchResultProperty="samAccountName"
        ObjectType="System.Collections.ArrayList" />
            <K2LdapMapping K2Name="Groups" FullOnly="true"
        LdapName="memberOf" SearchQuery="(objectCategory=Group)"
        SearchResultProperty="samAccountName"
        ObjectType="System.Collections.ArrayList" />
    </LdapUserAttributes>

<LdapGroupBaseObject>dc=denallix,dc=com</LdapGroupBaseObject>
    <LdapGroupSearchFormatString>(&#
        (objectCategory=Group)
        (samAccountName={0}))</LdapGroupSearchFormatString>
        <LdapGroupMemberSearchFormatString>
        (member:1.2.840.113556.1.4.1941:={0})
    </LdapGroupMemberSearchFormatString>
        <LdapGroupAttributes>
            <K2LdapMapping K2Name="ID" LdapName="samAccountName"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Name" LdapName="cn"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="Description" Multiline="true"
        LdapName="description" ObjectType="System.String" />
            <K2LdapMapping K2Name="Email" LdapName="mail"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="DistinguishedName"
        LdapName="distinguishedName" FullOnly="true"
        ObjectType="System.String" />
            <K2LdapMapping K2Name="ObjectSID" LdapName="objectSID"
        FullOnly="true" ObjectType="System.String" />

```

```

<K2LdapMapping K2Name="Member" LdapName="member"
FullOnly="true" SearchQuery="(objectClass=Person)
(objectCategory=User)" SearchResultProperty="samAccountName"
ObjectType="System.Collections.ArrayList" />
</LdapGroupAttributes>
</AuthInit>
```

Register the User Manager

To register a user manager, two tables in the Host Server database must be modified.

- SecurityProviders – stores the security providers and their .NET type that implements IHostableSecurityProvider
- SecurityLabels – stores the security label, security provider and authorization/role initialization data for the user manager

The example SQL scripts allow you to setup and remove an LDAP user manager. Be sure to edit the scripts to fit your configuration before executing them.

1. Download and extract the K2 User Managers sample scripts
2. Open the "K2 LDAP User Manager (Forms - Setup).sql" script and edit it for your environment
3. Execute the "K2 LDAP User Manager (Forms - Setup).sql" script from Microsoft SQL Server Management Studio against the K2 Host Server database
4. Refresh the User Manager Cache
5. Restart the K2 Server service



Download: You can download the K2 User Managers sample scripts by clicking here.



The example scripts contain references to the DLX SQL instance, the K2HostServer database and the denallix.com domain. Please edit the .sql files to replace these values before executing.

1.6.8.7.4 SQL User Manager

SQL User Manager

The K2 SQL User Manager allows user information to be stored in a SQL database. K2 uses that SQL database for authentication and authorization of K2 tasks.

Note that the [Changing the Default User Manager](#) topics are required if you are using the newly-registered SQL user manager as the default user manager and you did not install using the SQL user manager.

Example

The following example is for the fictitious Denallix.com domain and is inserted into the SecurityLabels table of the K2HostServer database. You must change the values below to match your environment. This is the same XML that is included in the downloadable script file.

 Copy

```
<AuthInit>
  <init>DLX, K2SQLUM</init>
  <login/>
  <implementation assembly="SQLUM, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=16a2c5aaa1b130d"
type="SQLUM.K2UserManager"/>
</AuthInit>
```

Register the User Manager

To register the SQL user manager, one table in the Host Server database must be modified.

- SecurityLabels – stores the security label, security provider and authorization/role initialization data for the user manager

The example SQL scripts allow you to setup and remove a SQL user manager. Be sure to edit the scripts to fit your configuration before executing them.

1. [Download](#) and extract the K2 User Managers sample scripts
2. Open the "K2 SQL User Manager (Setup).sql" script and edit it for your environment
3. Execute the "K2 SQL User Manager (Setup).sql" script from Microsoft SQL Server Management Studio against the K2 Host Server database
4. Refresh the User Manager Cache
5. Restart the K2 blackpearl Server service



Download: You can download the K2 User Managers sample scripts by [clicking here](#).



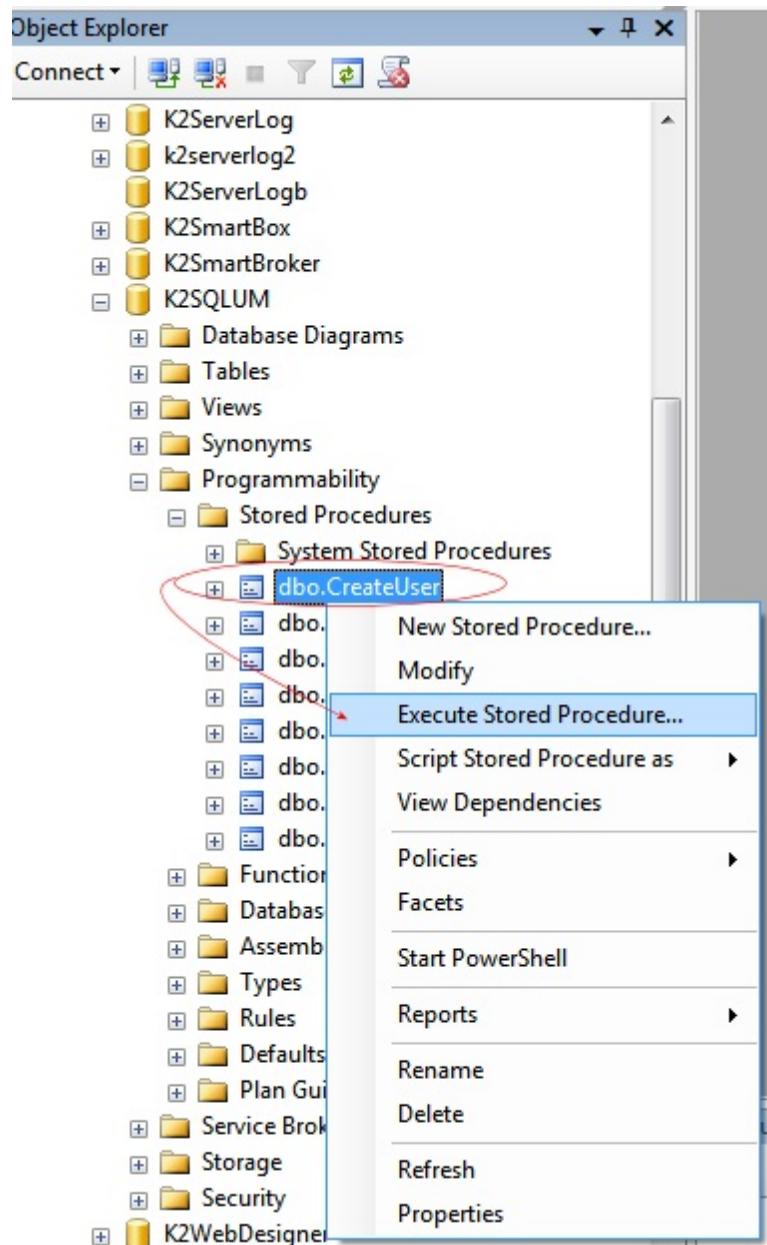
The example scripts contain references to the DLX SQL instance and the K2HostServer database. Please edit the .sql files to replace these values before executing.

1.6.8.7.4.1 Creating a user

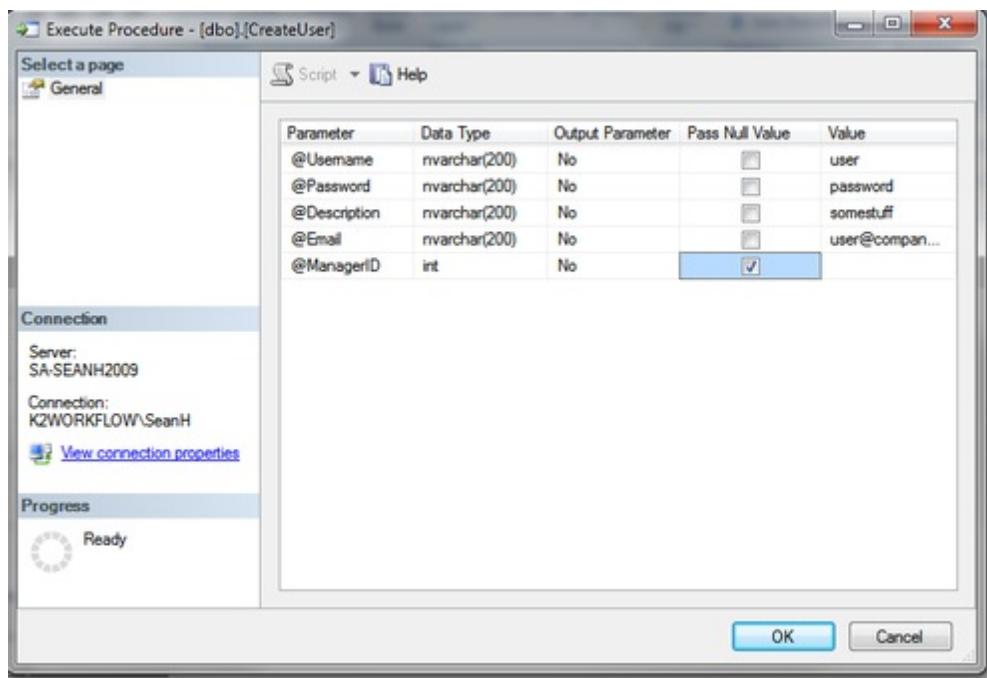
Creating a User

Users must be added manually to the SQL database. For security purposes, a stored procedure has been provided which will encrypt the password for each user name that will be entered.

1. Open Microsoft SQL Server Management Studio
2. Connect to the Server where the K2 Databases are installed
3. Expand the databases and open the K2SQLUM database
4. Locate the following path **K2SQLUM > Programmability > Stored Procedures**
5. Locate the stored procedure **dbo.CreateUser**, right click and select **Execute Stored Procedure**



6. The **Execute Procedure Dialog** will display and the user can enter the required values for a user



7. Once the user has been entered, click OK for the stored procedure to run

Optional: This process should be completed for each individual user

1.6.8.7.4.2 Adding a User to a Group

Adding a Users to a Group

To add a user to a group it is necessary to create the group first in the K2SQLUM database. Create the Group manually by:

1. Open Microsoft SQL Server Management Studio
2. Connect to the Server where the K2 Databases are installed.
3. Expand the K2SQLUM database
4. Right click on dbo.K2Groups and select **Edit Top 200 Rows**
5. Enter the Group details in the table

The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left shows a tree structure of databases and tables. The 'Tables' node under 'K2SQL1' has 'dbo.K2Groups' selected. The main pane displays a table named 'DLX.K2SQL1 - dbo.K2Groups' with two rows. The first row has GroupID = 1, GroupName = 'Finance', and GroupDescription = 'Finance Group'. The second row is a new entry with GroupID = NULL, GroupName = NULL, and GroupDescription = NULL. The Properties pane on the right shows the properties for a query named 'Query1.dtq'. The 'Query Designer' section is expanded, showing settings like Destination Table, Distinct Values (No), GROUP BY Extension (<None>), Output All Columns (No), and SQL Comment (***** Script for SelectTopNR). The 'Top Specification' is set to Yes.

GroupID	GroupName	GroupDescription
1	Finance	Finance Group
NULL	NULL	NULL

6. Locate the dbo.K2UserGroup table, right click and select **Edit Top 200 Rows**
7. Enter the Groups ID and the User's ID in the table. E.g
Group = Finance User = John
GroupID = 1 UserID = 4
8. Commit these changes to the database

The screenshot shows the Microsoft SQL Server Management Studio interface. The left pane displays the Object Explorer with a tree view of database objects under 'K2SQL1'. The central pane shows a table named 'dbo.K2UserGroup' with two rows of data:

	GroupID	UserID
1	1	4
*	NULL	NULL

The right pane shows the Properties window for a query named 'Query1.dtq'. The 'Query Designer' section is expanded, displaying the following settings:

- Destination: <None>
- Distinct Val: No
- GROUP BY: <None>
- Output All: No
- Query Par: No parameters
- SQL Comm: ***** Script fo
- Top Specif: Yes

1.6.8.7.4.3 Adding a User to a Role

Adding a User to a Role

To add a SQL user to a role, add the user to the required role through K2 Workspace> Management Console>Roles



The user's browsers connection string is located in the configurationmanager.config file in <install drive>:\Program Data\ folder.

1.6.8.7.5 Custom User Manager

Custom User Manager

Custom user managers can be used in the K2 platform to provide authentication and role resolution for a custom identity store or one that is not supported by K2 out of the box. For more information, see [Creating a Custom User Manager](#), in the K2 Developer Reference

1.6.8.7.6 Changing the Default User Manager

Changing the Default User Manager

Introduction

Changing the default user manager after installing K2 involves multiple steps, mainly to change the connection strings throughout the platform but also to register the default user manager in the database. These topics detail what needs to change for switching the default user manager, and use AD to SQL as the example but the steps would be similar for AD to Custom.



Note: Existing, deployed processes rely on string tables versus Environment Library variables. Ensure that you update these string tables, as appropriate, with the same connection information used for updating the Environment Library variables.

Important: The steps in this section should be done at the same time. A K2 server restart is necessary after all the changes have been made.

It is recommended that before changing to a new default provider, at least one user from that provider has been granted administration rights on the K2 server.

Follow the steps below, in order, to change the default user manager.

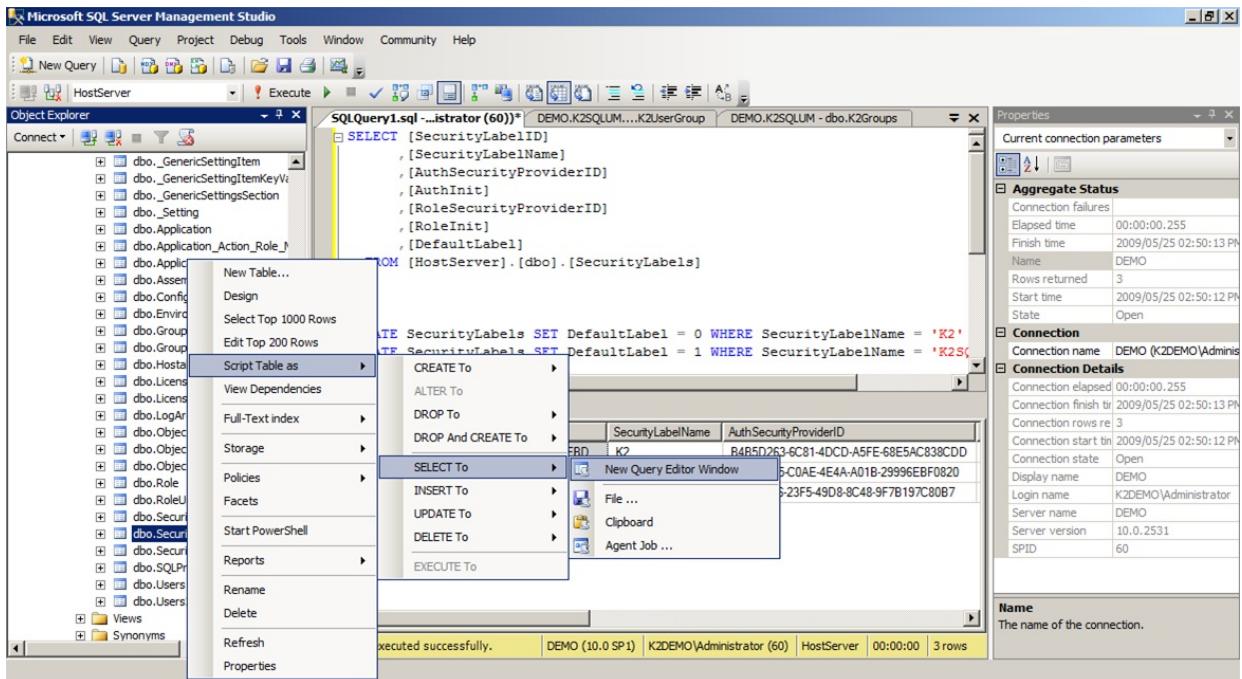
1. Configure Security Labels
2. Configure K2 Workspace
3. Configure Workflow Server
4. Configure Environment Library
5. Configure User Role Manager
6. Configure Windows Designers
7. Configure Out of Office
8. Refresh the User Manager Cache

1.6.8.7.6.1 Configure Security Labels

Configure Security Labels

The default user manager is the user manager that has a value of 1 in the DefaultLabel column of the SecurityLabels table. User managers that have a Null or 0 are non-default. To switch from AD to SQL follow these steps:

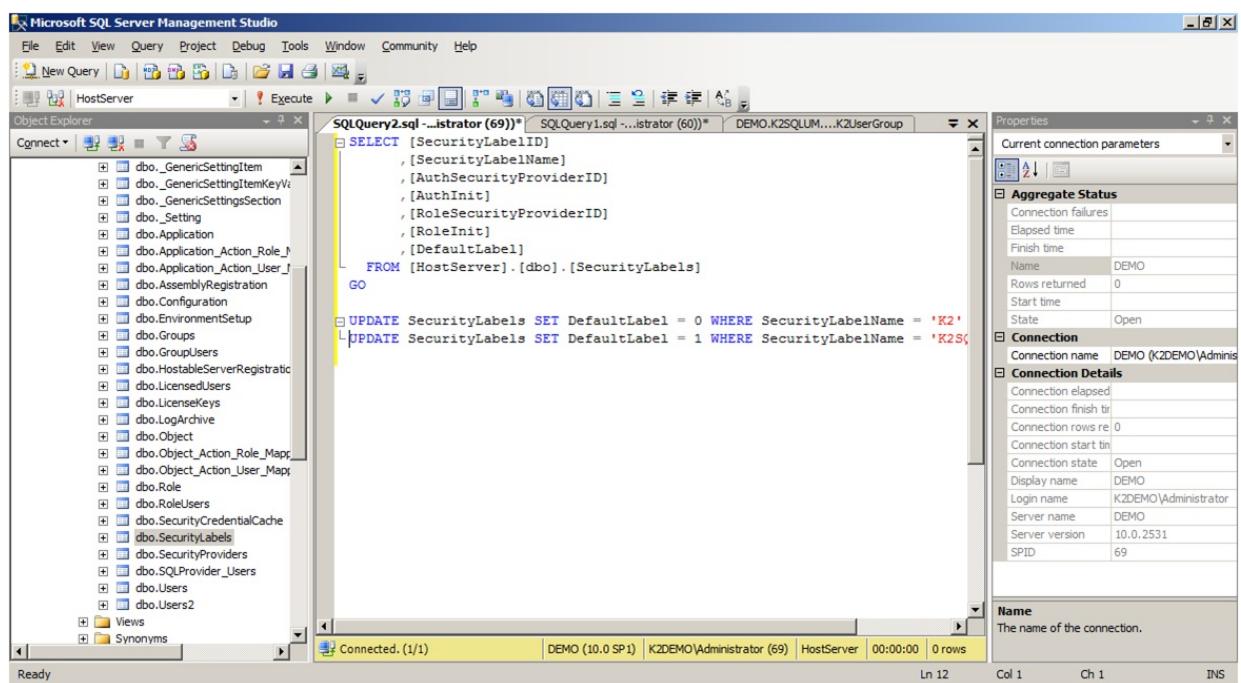
1. Stop the K2 blackpearl Server
2. Open Microsoft SQL Server Management Studio.
3. Connect to the server where the K2 Databases are installed.
4. Open the K2HostServer database.
5. Browse to the SecurityLabels table (dbo.SecurityLabels)
6. Right-click and select Script Table as > SELECT To > New Query Editor Window.



7. Execute the following two scripts:

```
UPDATE SecurityLabels SET DefaultLabel = 0 WHERE SecurityLabelName = 'K2'
UPDATE SecurityLabels SET DefaultLabel = 1 WHERE SecurityLabelName = 'K2SQL'
```

Note: The example uses AD to SQL and you must change these values if you are switching from or to a different user manager.



8. Restart K2 blackpearl Server service.

1.6.8.7.6.2 Configure K2 Workspace

Configuring K2 Workspace

K2 Workspace includes a configuration file located in the K2 blackpearl root directory (<install drive>:\Program Files (x86)\K2 blackpearl\WorkSpace\Site\web.config). You must modify this to enable SQL user manager-based logins to K2 Workspace.



When running in single authentication mode (SQL or Custom) only, you will need to enable **Anonymous** and disable **Integrated Windows Authentication** access for the Workspace site. The site also needs to run under an ApplicationPool identity of **Local System** or **Network Service**.

However, when running in mixed mode (Active Directory and any other user manager), only **Integrated Windows Authentication** should be enabled for the K2 Workspace site. In this scenario, the Workspace site should run under an Active Directory ApplicationPool Identity which has Administrative permissions within K2.

Name	Status	Response Type
Active Directory Client Certificate Aut...	Disabled	HTTP 401 Challenge
Anonymous Authentication	Enabled	
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



These instructions may vary dependant on the version of IIS

- Locate the line below:

```
<add key="authenticationMode" value="Windows" />
```

change the value from "Windows" to "Forms" as shown below:

```
<add key="authenticationMode" value="Forms" />
```

- Locate the line below

```
<add key="DefaultSecurityLabel" value="K2" />
```

change the value from "Windows" to "K2SQL" as shown below:

```
<add key="DefaultSecurityLabel" value="K2SQL" />
```

- Ensure that the following key is present:

```
<add key="ExtraAuthData" value="1" />
```

- Locate the line below:

```
<membership defaultProvider="AspNetActiveDirectoryMembershipProvider"
userIsOnlineTimeWindow="1600">
    <!--<membership defaultProvider="MembershipProvider" userIsOnlineTimeWindow="1600">-->
```

Change the lines to the following by commenting out the top line

```
<!--<membership defaultProvider="AspNetActiveDirectoryMembershipProvider"
userIsOnlineTimeWindow="1600">-->
<membership defaultProvider="MembershipProvider" userIsOnlineTimeWindow="1600">
```

5. Locate the line below:

```
<authentication mode="Windows">
```

Change mode from "Windows" to "Forms"

```
<authentication mode="Forms">
```

6. Locate the line below and comment it out

```
<!--<add connectionName="ADConnectionString" connectionProtection="Secure"
enablePasswordReset="false" enableSearchMethods="true" requiresQuestionAndAnswer="false"
applicationName="/" description="Default AD connection" requiresUniqueEmail="false"
clientSearchTimeout="30" serverSearchTimeout="30" attributeMapUsername="sAMAccountName"
name="AspNetActiveDirectoryMembershipProvider"
type="System.Web.Security.ActiveDirectoryMembershipProvider, System.Web, Version=2.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />-->
```

7. Save and close the web.config file.

8. Perform an IIS reset

Verify Changes



A default user is added on install when the SQL user manager is used (Username: k2, Password: k2).

1. Open a browser and navigate to K2 Workspace where a login page will be displayed.
2. Enter the username, password and the Security Label.



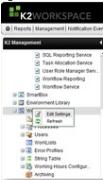
The name and password provided must match that entered into the dbo.K2Users table.

1.6.8.7.6.3 Configure Workflow Server

Configure Workflow Server

Follow the steps below to change the connection string for the Workflow Server:

1. Open K2 Workspace
2. Click Management > Management Console
3. Right click on the Workflow Server Node and select Edit Settings



4. Select the User Settings Tab
5. Change the connection string in the Data Field to :

Copy Connection String

```
Integrated=False;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=localhost;Port=5555;UserID=k2;Password=k2;SecurityLabelName=[K2SQL];AuthData=1
```

K2WORKSPACE

Logged in as K2DEMO/Administrator POWERED BY K2 blackpearl

Reports | Management | Notification Events | Security | User Preferences |

K2 Management Workflow Server > DEMO5555 > Configuration Settings

Save | General Database Settings Advanced Settings User Settings

Name: K2

Assembly: SourceCode.Security.K2UMInterop

Type: SourceCode.Security.K2UMInterop.K2UMBWrapper

Data: Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=localhost;Port=5555;

1.6.8.7.6.4 Configure Environment Library

Configure Environment Library

It is necessary to update the environment library connection strings for all fields except Mail Server and Web Service URL. You can update these in K2 Workspace or from K2 Studio or K2 for Visual Studio.

Method 1 – Using K2 Workspace

Follow the steps below to change the connection string for the Environment Library :

1. Open K2 Workspace
2. Select Management > Management Console
3. Browse to Environment Library > Templates > Default Template > Environments > [Development, Production or other environment] > Environment Fields
4. Select the Category Server and click Edit

Selected	Name	Description	Default	Field Type	Value
<input type="radio"/>	Category Server	Category Server	True	Category Server	Integrated=True; IsPrimaryLogin=True; Authenticate=True; EncryptedPassword=False; Host=DEMO; Port=5555 demo
<input type="radio"/>	Mail Server	Mail Server	True	Mail Server	Integrated=True; IsPrimaryLogin=True; Authenticate=True; EncryptedPassword=False; Host=DEMO; Port=5555
<input type="radio"/>	ServiceObject Server	ServiceObject Server	True	ServiceObject Server	Integrated=True; IsPrimaryLogin=True; Authenticate=True; EncryptedPassword=False; Host=DEMO; Port=5555
<input type="radio"/>	SmartObject Server	SmartObject Server	True	SmartObject Server	Integrated=True; IsPrimaryLogin=True; Authenticate=True; EncryptedPassword=False; Host=DEMO; Port=5555
<input type="radio"/>	Web Service URL	Web Service URL	True	Web Service URL	http://DEMO:81

5. Change the connection string in the Field Value to :

Copy Connection String

```
Integrated=False; IsPrimaryLogin=True; Authenticate=True; EncryptedPassword=False;
Host=localhost; Port=5555; UserID=k2; Password=k2; SecurityLabelName=
[K2SQL]; AuthData=1
```



The **SecurityLabelName** in the connection string is the SQL user manager name. Substitute the placeholder value [K2SQL] with the correct value for your system.

6. Repeat steps 4 and 5 for each of the following environment fields:

- a. Category Server
- b. ServiceObject Server

- c. SmartObject Server
- d. Workflow Management Server
- e. Workflow Server (note the port number is 5252 by default, not 5555 like the other fields)

Method 2 - K2 Studio or K2 for Visual Studio

Follow the steps below to configure the environment fields in K2 Studio or K2 for Visual Studio:

1. Open K2 Studio or the K2 Designer for Visual Studio
2. Open the K2 Object Browser
3. Expand the Category Server(s)
4. Right-click on Category Server and select Edit Field...
5. Change the connection string to the following:

 **Copy Connection String**

```
Integrated=False;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;  
Host=localhost;Port=5555;UserID=k2;Password=k2;SecurityLabelName=[K2SQL];AuthData=1
```



The **SecurityLabelName** in the connection string is the SQL user manager name. Substitute the placeholder value [K2SQL] with the correct value for your system, for example K2SQL.

1. Repeat steps 4 and 5 for each of the following servers in the K2 Object Browser:
 - a. Category Server
 - b. ServiceObject Server
 - c. SmartObject Server
 - d. Workflow Management Server
 - e. Workflow Server (note the port number is 5252 by default, not 5555 like the other fields)

1.6.8.7.6.5 Configure User Role Manager

Configure User Role Manager

Follow the steps below to change the connection string for the User Role Manager Service instance:

1. Open K2 Workspace
2. Select Management > Management Console
3. Browse to SmartObjects > Services
4. Select the User Role Manager Service on the Left, then select URM Service on the right, and then click the Edit button to modify the connection string

The screenshot shows the K2 Management Console interface. The left sidebar is titled 'K2 Management' and contains a tree view of service instances under 'DLX:5555'. The 'User Role Manager Service' is selected. The main pane is titled 'DLX:5555 > SmartObjects > Services > Service Instance > User Role Manager Service'. It displays a table with one row for 'URM Service'. The table has columns for 'Selected', 'Display Name', and 'Description'. The 'Display Name' column shows 'URM Service' and the 'Description' column shows 'URM Service from User and Group resolution against tables'. Below the table are buttons for 'Add', 'Edit', 'Credentials', and 'Remove'.

5. Change the connection string in the HostServerConnectionString to :

Copy

```
Integrated=False;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;
Host=localhost;Port=5555;UserID=k2;Password=k2;SecurityLabelName=
[K2SQL];AuthData=1
```



The SecurityLabelName in the connection string is the SQL user manager name. Substitute the placeholder value [K2SQL] with the correct value for your system, for example DenallixPartners.

Edit Service Instance

HostServerConnectionString:	Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=D
FindUsersDefaultFilter:	groupname=null;size=100
Security Provider:	
User Name:	
Password:	
Extra:	
Impersonate:	<input type="checkbox"/>
Enforce Impersonation	<input checked="" type="checkbox"/>

**Next** | **Close**

1.6.8.7.6.6 Configure Windows Designer

Configure Windows Designers

You must update the configuration files and the connection to the Environment Library from K2 Studio and K2 for Visual Studio in order to see items in the context browser.

Update Configuration Files

It is necessary to change a line in the configurationmanager.config (location: <install drive>:\Program Data \SourceCode) for the user browser to render:

Change

```
Copy Existing Code

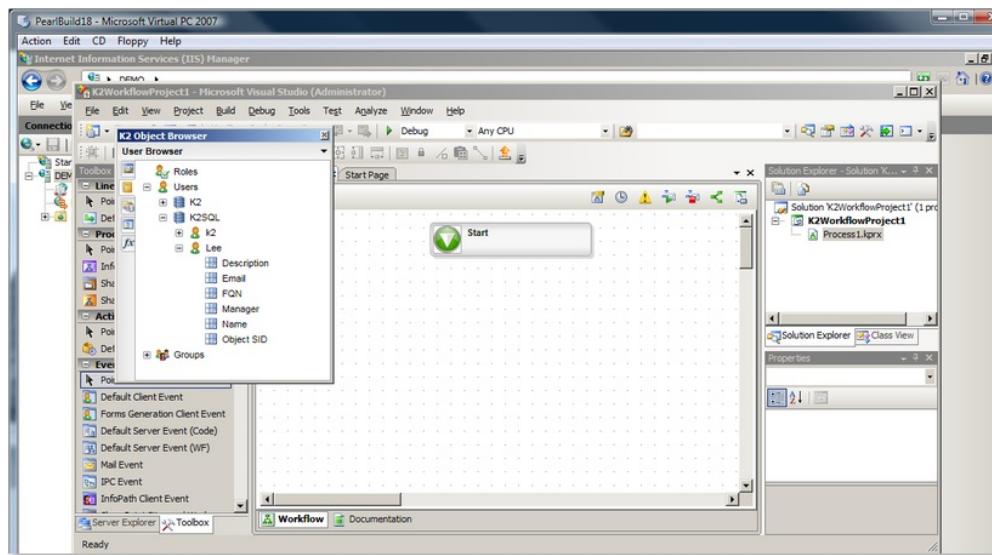
<settings>
  <add key="UserBrowserServer"
  value="Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=DEMO;Port=5555"
  />
</settings>
```

To

```
Copy Change To

<settings>
  <add key="UserBrowserServer"
  value="Integrated=False;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Host=DEMO;Port=5555;
  UserID=k2;Password=k2;SecurityLabelName=[K2SQL] " />
</settings>
```

The K2SQL node is now displayed in the Object and Context Browsers under the User Browser.



The following fields are available:

Field	Description
Email	The user's email address.
FQN	The user's fully qualified name.
Manager	The user's manager.
Name	The user's name.
Object SID	The Security ID of the user.

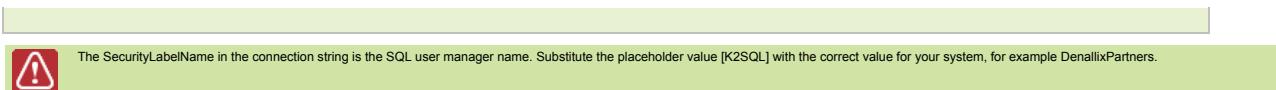
Update Environment Library Connection

You must also update the connection to the Environment Library from K2 Studio and K2 for Visual Studio in order to see items in the context browser. This is done by clicking on the upper right corner of the Object Browser and clicking Change Server.

In the **Change Environment Server Connection** dialog that appears, type the connection string to connection to the server using the security label and user information.

```
Copy Connection String

Integrated=False;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;
Host=localhost;Port=5555;UserID=k2;Password=k2;SecurityLabelName=[K2SQL];AuthData=1
```



Note: Each user should type in their username and password to connect to the Environment Library.

1.6.8.7.6.7 Configure Out of Office

Configure Out of Office

When configured for AD, the Out of Office service performs its required method calls using the Application Pool identity, which gives the system the elevated user rights to perform the Management API call for OOF. When a non-AD user manager is configured, the resources that are available when Active Directory is used are no longer available. The default label as the Application Pool account user is not an AD user and there are no administration credentials stored and it must be embedded in the connection string.

Enter a new connection string

A new connection string must be added to the Workspace web.config configuration file. Once the entry has been updated, the connection string can be encrypted for security purposes.

Copy Updated Connection String

```
<add name="WorkflowManagementAdminConnectionString"
connectionString="IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False;Integrated=False;Host=localhost;Port=5555;UserID=k2;Password=k2;
SecurityLabelName=[K2SQL]" />
```



The SecurityLabelName in the connection string is the SQL user manager name. Substitute the placeholder value [K2SQL] with the correct value for your system, for example DenalixPartners.

Encrypt the Connection String

The following command is run from the command prompt and is used to encrypt the connection string that was updated in the section above. It will update the web.config file with encrypted information.

Copy Encryption Command

```
"%WinDir%\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe" -pe "connectionStrings" -app "[WorkspaceVirtualDirectoryPath]" -site "[WorkspaceSiteNameOrID]"
```

Tagged Definitions

[WorkspaceVirtualDirectoryPath]	The virtual directory path you specified on installation for example: "Workspace"
---------------------------------	---

[WorkspaceSiteNameOrID]	The virtual directory path you specified on installation for example: "K2"
-------------------------	--

Decrypt the Connection String

If settings need to be changed and the Workspace web.config file must be amended, use the following command to decrypt the connection string. Performed similar to the encryption command, replace -pe with -pd in the encryption command.

Copy Decryption Command

```
"%WinDir%\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe" -pd "connectionStrings" -app "[WorkspaceVirtualDirectoryPath]" -site "[WorkspaceSiteNameOrID]"
```

Additional Information

For further information on encrypting and decrypting connection strings, see the following resource
<http://msdn.microsoft.com/en-us/library/ms998283.aspx>

1.6.8.7.6.8 Refresh the User Manager Cache

Refresh the User Manager Cache

Any change in the configuration of user managers will require an update of the existing user cache. Download and execute the SQL command against the K2HostServer database.



```
UPDATE [K2HostServer].[Identity].[Identity]
    SET [ExpireOn] = GETDATE()
        , [Resolved] = 0
        , [ContainersResolved] = 0
        , [ContainersExpireOn] = GETDATE()
        , [MembersResolved] = 0
        , [MembersExpireOn] = GETDATE()

GO
```

1.6.8.8 Config File Changes

1.6.8.8.1 K2 Auditing and Logging

K2 Auditing and Logging

K2 blackpearl provides native logging framework and auditing features that enables administrators to monitor and troubleshoot the K2 blackpearl environment. System Event Logging is initiated automatically (default operation) from product installation and is active through to runtime. System auditing features are initiated manually by the developer per individual process at design time and leveraged during runtime.

The logging and auditing features of K2 blackpearl are built into the platform but operate and are configured in different ways.

Enable Logging

The steps described in this section will enable an administrator to enable logging, but without a full discussion of system requirements and possible implications. Be advised that the steps should only be pursued after reviewing the accompanying document or under the direction of a K2 Consultant.

Perform the following steps to enable **HostServer Logging**:



Open the following file in notepad:

[SystemDrive]:\Program Files\K2 blackpearl\Host Server\Bin\HostServerLogging.config



Find the following section:



```
<ApplicationLevelLogSettings>
    <ApplicationLevelLogSetting Scope="Default">
        <LogLocationSettings>
            <LogLocation Name="ConsoleExtension"
Active="True" LogLevel="Info" />
            <LogLocation Name="FileExtension"
Active="False" LogLevel="All" />
            <LogLocation Name="EventLogExtension"
Active="False" LogLevel="Debug" />
            <LogLocation Name="ArchiveExtension"
Active="False" LogLevel="Debug" />
            <LogLocation Name="MSMQExtension"
Active="False" LogLevel="Debug" />
        </LogLocationSettings>
    </ApplicationLevelLogSetting>
</ApplicationLevelLogSettings>
```



Change the following line from:

Change
`<add key="IncludeStackTrace" value="False" />`
 to
`<add key="IncludeStackTrace" value="True" />`

Change

`<LogLocation Name="ConsoleExtension" Active="True" LogLevel="Info" />`
 to
`<LogLocation Name="ConsoleExtension" Active="True" LogLevel="Debug" />`

Change

`<LogLocation Name="FileExtension" Active="False" LogLevel="All" />`
 to
`<LogLocation Name="FileExtension" Active="True" LogLevel="All" />`



Save and close the file

Restart the K2 service

By default the newly generated log file will be in the same directory as the modified config file. Alternatively verify the path in 'LogFilePath' setting in the config file. The log files will be in the `[SystemDrive]:\Program Files\K2 blackpearl\Host Server\Bin\directory`

Perform the following steps to enable **SmartObject Server Logging**:

On all K2 Servers in the farm, you can enable detailed logging to help with SmartObject runtime debugging. To turn on the detailed, follow the below steps:



Open the following file in notepad:

```
'%http:http://help.k2.com/files/1628%\K2 [blackpearl\blackpoint]\Host Server\Bin\SourceCode.SmartObjects.Runtime.config'
```

Change:



Copy

```
<logging>
    <serviceauthentication log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\serviceauth.log"
overwrite="no" />
    <timestamping log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\timestamp.log"
overwrite="no" />
    <brokerpackagein log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\brokerpackagein.log"
overwrite="no" />
    <brokerpackageout log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\brokerpackageout.log"
overwrite="no" />
    <servicepackagein log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\servicepackagein.log"
overwrite="no" />
    <servicepackageout log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\servicepackageout.log"
overwrite="no" />
</logging>
```

To:

**Copy**

```

<logging>
    <serviceauthentication log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\serviceauth.log"
overwrite="no" />
    <timestamping log="no"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\timestamp.log"
overwrite="no" />
    <brokerpackagein log="yes"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\brokerpackagein.log"
overwrite="no" />
    <brokerpackageout log="yes"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\brokerpackageout.log"
overwrite="no" />
    <servicepackagein log="yes"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\servicepackagein.log"
overwrite="no" />
    <servicepackageout log="yes"
path="%http:http://help.k2.com/files/1628%\K2
[blackpearl\blackpoint]
    \ServiceBroker\Logs\servicepackageout.log"
overwrite="no" />
</logging>
```



Save your changes to the config file.



Restart the K2HostServer service



The log files will be created in the 'path' attribute for each setting.

Advanced Information:

For additional information regarding Auditing and Logging read the [K2 blackpearl Logging and Auditing white paper](#).

1.6.8.8.2 Tweaking identity cache performance for the K2 Server

Configuration settings for tweaking identity cache performance for the K2 Server.

The Identity Service is a new cache mechanism that has been introduced from K2 4.5 KB001370. This new cache mechanism is designed to work with Active Directory groups, SharePoint Groups and also K2 roles. Previously one configured the Cache Timeout value on the Active Directory User Manager (ADUM) settings. Note that this will now be set to zero for future releases to disable the ADUM cache.

To examine the internals of the Identity Framework, we will discuss the following backend tables used in the K2HostServer database.

- Identity.CacheConfiguration
- Identity.RoleItem
- Identity.Identity
- Identity.IdentityMember
- Identity.IdentityUpdate

The Identity.CacheConfiguration table

The [Identity].[CacheConfiguration] table sets the time parameters of the Role Provider (K2, K2SQL, CUSTOM) identity caches and the Microsoft SQL command timeout setting. The default properties of these settings are as follows:

□	Identity.CacheConfiguration
□	Columns
鑰匙	Name (PK, nvarchar(128), not null)
	Value (nvarchar(max), null)

	Name	Value
1	DynamicGroupCacheTimeout	30s
2	DynamicRoleCacheTimeout	30s
3	DynamicUserCacheTimeout	30s
4	GroupCacheTimeout	8h
5	GroupContainersCacheTimeout	8h
6	GroupMembershipCacheTimeout	1h
7	ResolvedExpiredIdentities	0m
8	RoleCacheTimeout	8h
9	RoleMembershipCacheTimeout	1h
10	SqlCommandTimeout	10m
11	UserCacheTimeout	8h
12	UserContainersCacheTimeout	8h

These settings may be defined in milliseconds (ms), seconds (s), minutes (m), or hours (h). The maximum value will be 24 days, 20 hours, 31 Minutes, 23, Seconds and 6470000 milliseconds. This is a .NET restriction on wait handles that does not accept longer periods than int.MaxValue specified in milliseconds. In other words 2147483647 milliseconds translates to this value 24.20:31:23.6470000 (d,h,m,s,ms). A configuration of 0s will turn the setting off. A higher value will increase the time between reloading -reducing the load on the server but increasing the latency of up-to-date information.

The three types of identities that are cached within the K2 Server are the **User**, the **Role**, and the **Group**.

The **CacheTimeout** settings configure when the cached properties of that identity will expire. After this configured time period has expired the K2Server will resolve the identity against the provider.

In regard to the **dynamicCacheTimeout**, a normal user will be resolved on the thread according to the CacheTimeout configuration. Dynamic identities will be excluded from this timed resolving and will resolve on demand. When a worklist item is opened, all dynamic identities will be resolved before the server queries the current user membership, in case the user is included in the result. For example, a dynamic identity would be an online users whose identity needs to be checked every time the worklist is requested. This has a performance impact on worklist, and should only be used for true dynamic cases. The dynamicCacheTimeout setting therefore configures the time to expiration of the cached dynamic identity.

The **ContainersCacheTimeout** setting configures the duration until expiration of the K2 server cache that contains the external relational identity settings, i.e. all the groups that a particular group also belongs to.

The **MembershipCacheTimeout** setting configures the duration of the K2 server cache that contains the internal

relational identity settings, i.e. all the users within a group.

The **resolvedExpiredIdentities** setting configures the period of time that the server checks for expired identities and resolve them.

The **sqlCommandTimeout** setting configures the maximum amount of time the calling application should wait for an identity to be cached, before a timeout exception is raised.

The Identity.RoleItem table

This table holds the configuration of the SmartObject/Groups/Users defined in a K2 role.

BLACKPEARL.Identity.RoleItem						
	IdentityID	FQN	Type	Exclude	Data	LastModified
▶	14	TestUsers	4	False	<smartobject name="TestUsers" guid="679a3cf...>	10/3/2011 11:3...
▶	14	K2:DENALLIX\Anthony	1	False	NULL	10/3/2011 11:3...
▶	14	K2:DENALLIX\Administrators	3	False	NULL	10/3/2011 11:3...
▶	14	K2:Portal\Approvers	3	False	NULL	10/3/2011 11:3...
*	NULL	NULL	NULL	NULL	NULL	NULL

The table contains records that match up with the items as configured in the Management Console.

The Type column uses the following values.

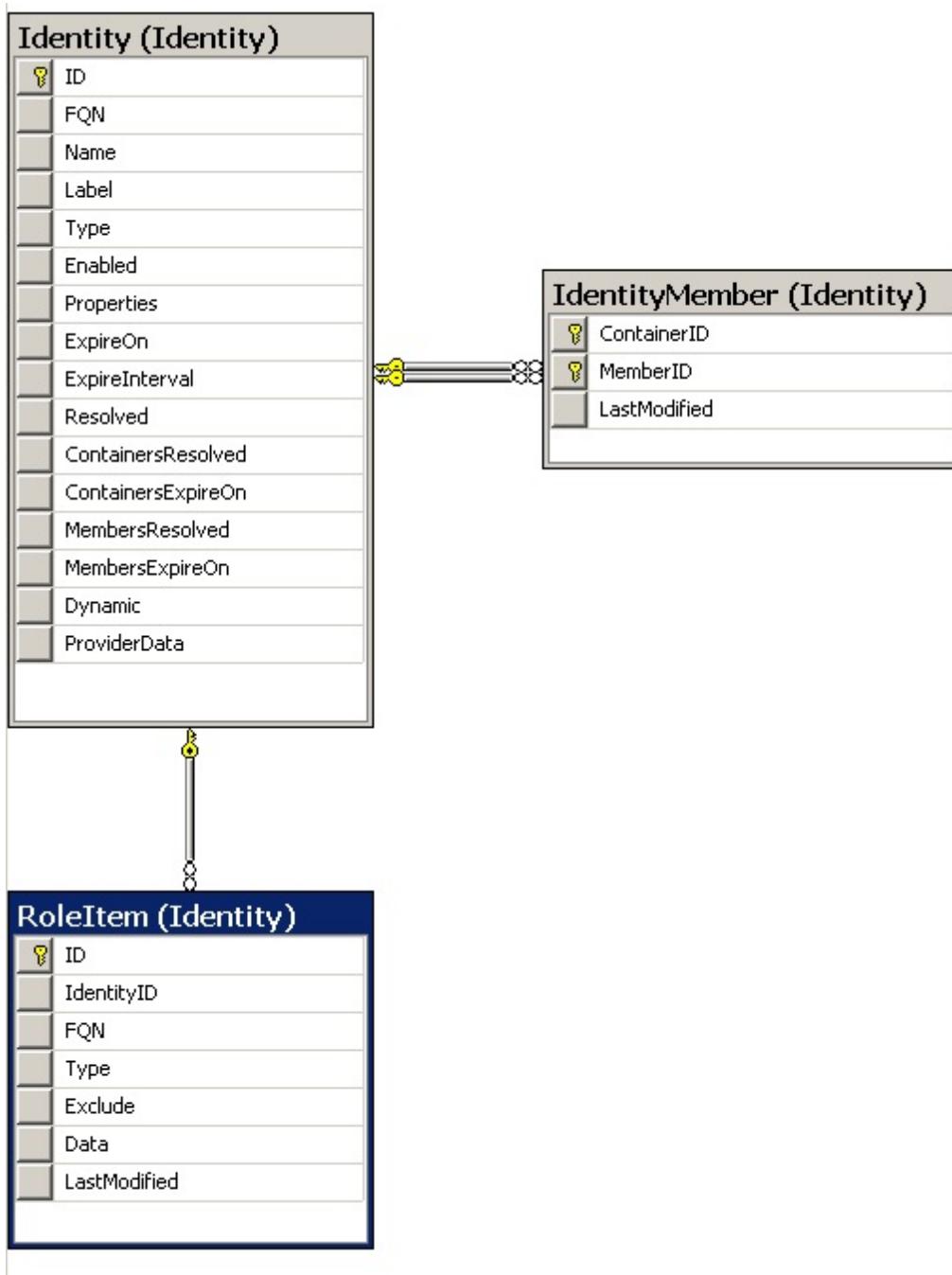
1 - User

3 - Group

4 - SmartObject (The Data column contains the SmartObject connection details. It also includes the method, property and filter values to use). Here's an example of the XML string contained in the Data column.

```
<smartobject name="TestUsers" guid="679a3cf...>
connectionString="Integrated=True;IsPrimaryLogin=True;Authenticate=True;EncryptedPassword=False
;Host=blackpearl;Port=5555" methodName="GetList" isListMethod="True" propertyName="UserID"
expectedType="1" xmlns="<a href="http://schemas.k2.com/roles/smartObjectdefinition"><inputs>
<input>http://schemas.k2.com/roles/smartObjectdefinition"><inputs><input name="TestUsers"
type="0">denallix\codi</input></inputs></smartobject>
```

From the Identity.RoleItem table, the IdentityID column links back to the Identity.Identity table ID column for the role's cache settings. The Identity.RoleItem table acts as the definition for the role, and the Identity.Identity table stores the role item and also the members. The linkage between the role and the members is contained in the Identity.IdentityMember table.



The Identity.Identity table

This table stores the cache expiry information for the User/Groups/Roles. You can force expire the relevant User/Group/Role cache by modifying the relevant expiry datetime value.

BLACKPEARL.Identity.Identity									
On	ExpireInterval	Resolved	ContainersRes...	ContainersExpi...	MembersResolved	MembersExpireOn	Dynamic	ProviderData	
011 0:21:...	28800	True	True	9/1/2011 7:11:0...	False	9/1/2011 7:10:5...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
11 7:11:0...	28800	False	True	9/1/2011 7:11:0...	False	9/1/2011 7:11:0...	False	NULL	
011 0:45:...	28800	True	False	9/1/2011 7:11:1...	False	9/1/2011 7:11:1...	False	NULL	
011 11:3:...	5	False	False	9/1/2011 7:12:4...	True	9/1/2011 7:12:13:...	True	NULL	
011 8:45:...	28800	True	False	9/1/2011 7:13:1...	False	9/1/2011 7:13:1...	False	NULL	
011 6:24:...	28800	True	False	9/1/2011 7:13:1...	False	9/1/2011 7:13:1...	False	NULL	
011 10:5:...	28800	True	False	9/8/2011 8:10:4...	False	9/8/2011 8:10:4...	False	NULL	
011 11:3:...	28800	True	False	9/9/2011 11:21:...	False	9/9/2011 11:21:...	False	NULL	
011 8:45:...	28800	True	False	9/29/2011 6:32:...	True	9/30/2011 1:45:...	False	NULL	
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	

For every item there are three different expiry fields (*ExpireOn*, *MembersExpireOn* and *ContainersExpireOn*). There are then three main methods on the Identity Service, namely *GetIdentity*, *GetIdentityMembers*, and *GetIdentityContainers*. These relate to the three expiry timestamps mentioned above.

1. *ExpireOn* will be updated if the *GetIdentity* method is called (e.g. a Get User Details call on UMUser SmartObject).
2. *MembersExpireOn* will be updated when *GetIdentityMembers* is called. (e.g. Get Group Users call on UMUser SmartObject).
3. *ContainersExpireOn* will be updated when *GetIdentityContainers* is called (e.g OpenWorklist call). This will return all the groups and roles for a user and recursively get roles and groups for each of the direct containers (recursively).

For a group, notice that the *MembersExpireOn* and *ExpireOn* fields gets refreshed when a group is requested to be resolved. For example when a new client event is hit which utilizes the group (refreshes the group membership and group properties respectively), or an E-mail event that sends an e-mail to the specific group. Other possibilities will include the UMUser SmartObject when executing the *GetGroupUsers* method. On the other hand, when a user accesses his task list, the user's *ExpireOn* and the *ContainersExpireOn* fields are refreshed. *ExpireOn* refreshes the identity Properties XML field and *ContainersExpireOn* refreshes the groups and roles that the user belongs to. The *MembersExpireOn* field does not change and its value is from the first time the Identity Service is used for the user.



If you want to refresh cache items, set all the three expiry dates to some time in the past for the relevant identity items.

You will also note that there is a Dynamic flag for each record. Currently this only applies to K2 roles. If it is set to *True*, it will ignores the CacheTimeout settings and instead use the dynamicCacheTimeout settings (i.e. 30s by default). Queries will be queried fresh after 30 seconds from the last query. This is useful for keeping task items current when users are removed or added from the K2 role. However, the flip side is that this will have a performance impact when identities are resolved as all dynamic identities gets refreshed before members or containers are selected.



NEVER delete anything from the *Identity.Identity* table – there are other K2 modules that rely on the ID's in this table and in the future other components will also rely on these ID's in regard to users/groups/roles.
This is also where the K2 roles get saved, so if you delete all the records, you will delete all your roles as well.

The *Identity.IdentityMember* table

This table holds the linkages between the Roles/Groups and the individual users (many-to-many relationship). In the *Identity.IdentityMember* table, both the *ContainerID* and *MemberID* columns link back to the *Identity.Identity* table ID primary key column. If you are familiar with K2.net 2003 destination queues (which is the predecessor to K2 roles), you will note that this is similar to the relationship between the *DestQueue* and *DestQueueUser* tables in the K2Server database. The only difference is that it stores the ID of the user instead of the user name for performance reasons.

BLACKPEARL.H..IdentityMember			
	ContainerID	MemberID	LastModified
▶	2	1	9/1/2011 11:10:54 AM
	3	1	9/1/2011 11:10:54 AM
	4	1	9/1/2011 11:10:54 AM
	5	1	9/1/2011 11:10:54 AM
	6	1	9/1/2011 11:10:54 AM
	7	1	9/1/2011 11:10:54 AM
	8	1	9/1/2011 11:10:54 AM
	9	1	9/1/2011 11:10:54 AM
	10	1	9/1/2011 11:10:54 AM
	11	1	9/1/2011 11:10:54 AM
	12	4	9/1/2011 11:11:00 AM
	14	15	9/1/2011 11:13:19 AM
	14	16	9/1/2011 11:13:19 AM
	19	15	9/30/2011 12:45:31 PM
	19	16	9/30/2011 12:45:31 PM
*	NULL	NULL	NULL

The Identity.IdentityUpdate table

This table should be empty most of the time. The table is used for when identities gets updated. The result from the providers are moved to this table (Bulk Insert) and the Identity.Identity and Identity.IdentityMember table will be updated in transaction. This table will be cleared once the update has completed. You will see that this table is used by the bulk container and member update stored procedure calls.



Editing the database tables can be a risky business, so create a backup of your database if you plan to modify any settings here. This gives you a safety net in case anything goes wrong.

1.6.8.9 Restricted Wizards

1.6.8.9.1 Restricted Wizards

SharePoint Restricted Wizards

There is an extra level of security that is available in the K2 Designer for SharePoint. This is a design-time security check that allows site administrators to filter out a set of wizards of their choosing. This enables them to remove some wizards from the design canvas and only expose them to the SharePoint users that they specify. If they don't specify any users that can see these "restricted" wizards, then nobody using the K2 Designer for SharePoint will see these wizards. By default, however, all wizards are visible to all process designers.



The Restricted Wizards can be found by navigating to K2 Site Settings on the specific site and clicking on the **Set Restricted Wizards** link in the K2 Designer for SharePoint Management section of this page as shown below.

The screenshot shows the 'Site Settings' page for a site named 'Site 105'. In the 'K2 Designer for SharePoint Management' section, the 'Set Restricted Wizards' link is highlighted with a red circle.

Fig. 1. Site Settings

The K2 Restricted Wizards page opens when clicking on the link.

The screenshot shows the 'K2 Restricted Wizards' dialog box. It displays a list of available wizards on the left and a list of restricted wizards on the right. An 'Add' button is used to move wizards between the two lists. Below the lists, there is a 'Restricted Users' section where users and groups can be selected to restrict the wizards.

Fig. 2. K2 Restricted Wizards

Feature	Description
Available Wizards	List of wizards available for restriction
Restricted Wizards	List of wizards to be restricted
Add	Select a wizard in the Available Wizards column and click Add. The wizard will be added to the list in the Restricted Wizards column on the right
Remove	Select a wizard to be removed from the Restricted Wizards column and click Remove. The wizard will be moved back into the Available

	Wizards column on the left
Users/Groups	Type text to search for the required users
 Only AD Users are supported (no AD Groups, SharePoint Users, or SharePoint Groups)	

1.7 K2 blackpearl Maintenance

Once you have K2 blackpearl up and running in your environment, there may be times when you need to modify components or change configuration settings. This can be accomplished by re-running the Setup Manager (to add or remove components), or re-running the Setup Manager (to change configuration settings).

When you run the K2 Setup Manager again, you will see three options:

K2 Maintenance	
Configure	Re-configures the existing K2 Installation
Remove	Removes the existing K2 Installation completely (including all components) from the target system.
Modify	Modifies the existing installation by either adding or removing components ¹
Repair	The repair option re-installs the components currently installed on the local, target system.

¹ The K2 Setup Manager may need to be run once the changes have been made.



- Once the changes have been made, with the exception of the **Remove** option, the configuration tool must be run to reconfigure the installation.
- If any change is made to the K2 Designer for SharePoint the users must clear their IE cache for the changes to reflect.

Managing K2 Components from Add / Remove Programs

The K2 blackpearl components are listed in the **Add or Remove Programs**. However, the components are not managed from this location. The K2 Setup Manager will be opened in order to manage the components.



Keep a copy of the Installation folder on the local machine where a K2 component has been installed. The Setup manager is required to add K2 Components.



Any modifications in Windows Add/Remove Programs will point to the Start > Programs navigation area or to the original installation source

1.7.1 Repair

1.7.1.1 Repairing an Existing Component

Repairing a K2 component is completed by rerunning the K2 Setup Manager and selecting repair. All the currently installed components on the server will be repaired.



Repairing a K2 blackpearl installation should be done only when absolutely necessary and only when components have been damaged by external circumstances.



You cannot repair a single component. Selecting the Repair option will reinstall all K2 components that are currently installed on that server.

After you select repair, you will be prompted to stop any running programs and services that use K2 components. The Setup Manager can stop the K2 Service for you, but you will need to close other programs manually.



You will not be able to repair components when the K2 Designer for Visual Studio is running. Be sure to save all your work and close the designer before continuing.

After the components are repaired, you will not need to reconfigure the components. All of the configuration data is kept. You should validate your environment, however, after a repair to ensure that your system is functioning properly.

1.7.1.2 Configure Components

Configure Components

If, after the initial installation of K2 blackpearl, some K2 blackpearl components still need to be configured, rerunning the K2 Setup Manager will allow you to configure those components. After selecting Configure from the initial screen, you can configure all the installed components. Follow the prompts through the wizard and restart after the configuration is finished.

The Configure K2 blackpearl option configures all the installed K2 component configuration files and db scripts. Currently this requires you to configure everything.

1.7.2 Modify

1.7.2.1 Adding Components

If, after the initial installation of K2 blackpearl, additional components are to be added to an existing server, rerunning the K2 Setup Manager will allow you to add new components.

After selecting Modify from the initial screen, you can select components to add (by checking the check box next to the listed component), or remove an existing component (by unchecking the check box next to an installed component).

The Modify option allows you to selectively add and remove K2 blackpearl components. If you add components using this option, it will run the configuration automatically after that.

You can install and remove different components during the same session of Modify. For example, you can select to uninstall a component while at the same time installing a different component. After that it will automatically run the Configuration option for the components.

Please note the following important facts regarding Modify:

1. When running Setup.exe from a temporary folder (where you copied/extracted the installer to), and components have been installed previously, the modify option will show you all the components, because it detects the msi files in the Setup folder.
2. When running the Setup.exe from the folder where K2 blackpearl had been installed to, the Modify option will only show those components that are installed. You can then select which ones to remove. It will NOT show you components that have not been installed. This is because the msi files are not installed to the K2 blackpearl install directory. This means you cannot add components by running Setup.exe from this folder. You have to run it from the original setup folder that contains the msi files.



If you want to install one of the components on this server that have a Check Dependencies action, cancel the installation and fix the dependency. Then, restart the installation and you should be able to select that component.

Before adding a new component, you should evaluate your K2 environment and make sure that the target server is a good fit for your requirements. Then, determine if all the prerequisites are met, and then run the K2 Setup Manager to add and configure the new components.



After selecting Modify from the initial screen, you can only select components to add if you open the K2 Setup Manager from the C:\ K2 blackpearl installation folder (by checking the check box next to the listed component), or by removing an existing component (by unchecking the check box next to an installed component).



Be sure to clear the cache after adding components, see the topic [Clear cache after deploying K2 blackpearl](#) for more information.

1.7.2.2 Updating the K2 License Key

There are two ways to update the K2 License Key:

- Using the License Management functionality in K2 Workspace. For more information, please refer to the K2 Workspace portion of the [K2 blackpearl User Guide](#)
- Another way to update the K2 License Key is to re-run the Setup Manager. A user will need their System Key and License Key before they can complete the Setup Manager. To update, run the Setup Manager on the K2 Server and select the Configure option, then select the Update K2 Server License option.

1.7.3 Remove

1.7.3.1 Remove Components

Removing K2 Components

Removing K2 blackpearl is essentially a reversal of the Installation and Configuration process. The **Setup Manager** will identify the components installed and remove them completely from the target system. The process starts by running the K2 blackpearl installer application and selecting the option to **Remove K2 blackpearl**.



This article walks through the steps to remove K2 blackpearl from a single server. For a distributed environment, perform these steps on all servers that have K2 blackpearl installed.

If you have installed K2 blackpearl in a distributed environment, uninstall all client components first. Then, uninstall the server components in the following order:

- K2 for Reporting Services
- K2 Workspace
- K2 for SharePoint
- K2 Server



Be sure to uninstall all other components first, ending with the K2 Server.

To uninstall, perform the following steps:

1. Shut down all K2 related processes (K2 Designer for Visual Studio, K2 Designer for SharePoint, K2 Web Designer (Legacy), K2 blackpearl Server service)



You will not be able to remove a component when the K2 Designer for Visual Studio is running. Be sure to save all your work and close the designers before continuing.

2. Run the Setup Manager (Setup.exe) and select **Remove K2 blackpearl**

Follow the prompts through the wizard and reboot after the uninstall is finished.



This will remove all components from the target system. You will be prompted to continue. If you want to remove just a single component, select Modify from the maintenance home page.

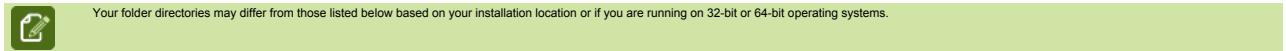


If the components are being removed from a distributed environment, removing the components from the Target System may cause issues in the associated environment. There are several manual clean up steps to ensure the environment works properly, be sure to follow these closely.

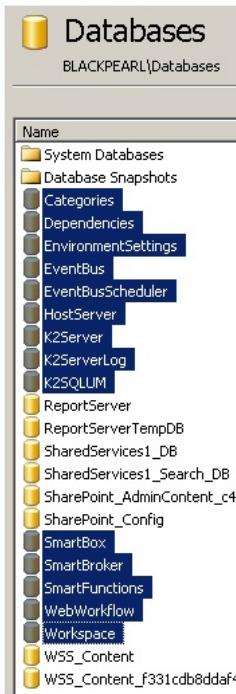
1.7.3.2 Manual Environment Clean Up

After uninstalling the components, there are some manual steps to clean up the environment. These are as follows:

Step 1: Manually remove remnants



1. The K2 Workspace Icon is left on the desktop. Delete this desktop icon.
2. The K2 blackpearl menu item is left in the Start Menu. Delete this menu item by right-clicking the **Start** menu and selecting **Explore All Users**. Then browse to the **K2 blackpearl** folder and delete it.
3. The SourceCode assemblies remain in the Global Assembly Cache (GAC). Delete all SourceCode assemblies from the **C:\Windows\Assembly** folder.
4. The SourceCode registry key remains. Delete this registry key, located at **HKEY_LOCAL_MACHINE > SOFTWARE > SourceCode**
5. The K2 blackpearl folder structure remains. Delete the folder structure located at **C:\Program Files\K2 blackpearl** (this may differ depending on your installation location)
6. The databases remain in SQL Server. This is so that data is preserved. To restore the server to a clean state, delete the databases highlighted below. If you need to preserve process or logged information, make a backup copy before deleting the databases.

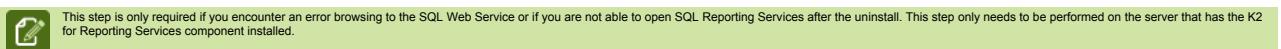


7. The **machine.config** file has remaining SourceCode entries. Edit the machine.config file, located at **C:\Windows\Microsoft.NET\Framework\v2.0.50727\config**, and remove all sections that mention SourceCode, including the `<sourcecode.configuration>` node. Be sure to save your changes to the file.
8. The K2 hidden lists are left in the sites K2 was activated to. SharePoint APIs or tools such as **SharePoint Manager** can be used to find and delete the hidden lists. K2 hidden lists utilize a GUID {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} as part of their name and can be further identified by the description which will contain text similar to "Internal list used by K2...".
9. Some "SourceCode.SharePoint.WebPart..." features installed in the following location: <install drive>:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\FEATURES
10. The following directory: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\ISAPI\SourceCode.ReportDataService
11. Remove the following from the RSReportDesigner.config located in C:\Program Files\Microsoft Visual Studio 9.0\Common7\IDE\PrivateAssemblies\RSReportDesigner.config:

Copy

```
<Extensions>
<Data>
<Extension Name="SOURCECODE"
Type="SourceCode.Data.SmartObjectsClient.SOConnection,SourceCode.Data.SmartObjectsClient, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=16A2C5AAAA1B130D" />
</Data>
<Designer>
<Extension Name="SOURCECODE"
Type="Microsoft.ReportingServices.QueryDesigners.GenericQueryDesigner,Microsoft.ReportingServices.QueryDesigners" />
</Designer>
</Extensions>
```

Step 2: SQL Reporting Services fix



1. After uninstalling K2 blackpearl, browse to **C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer** (this location may vary depending on where you installed SQL Server Reporting Services)
2. Edit the **rsrvpolicy.config** file in a text editor such as Notepad

3. Find the CodeGroup node, and edit it as specified below:



`<CodeGroup class="FirstMatchCodeGroup" version="1" PermissionSetName="Nothing">
<IMembershipCondition class="AllMembershipCondition" version="1">
</IMembershipCondition>
</CodeGroup>`

4. Save your changes to the file.

1.7.3.3 Validating the Uninstall

After uninstalling K2 blackpearl and performing the manual steps, reboot the machine. Then, to ensure the environment does not have any K2-related components, use the following checklist:

1. No K2 Databases are present on the SQL Server
2. The K2 blackpearl menu items are not present under Start > Programs
3. No K2 components are present in Add/Remove programs (Start > Control Panel > Add/Remove Programs)
4. No SourceCode nodes are present in the machine.config file
5. No SourceCode assemblies are in the GAC (C:\Windows\Assembly)
6. No K2 blackpearl folder is located under Program Files
7. No K2 For SharePoint tab in the SharePoint 3.0 Central Administration Site
8. No K2WorklistWebpart.wsp located in the SharePoint 3.0 Central Administration Site
9. No issues opening the SQL Server Reporting Services home page

1.7.4 K2 Upgrade Options

K2 Upgrade Options

K2 blackpearl has a number of versions spanning from the release version of K2 blackpearl to the current version. Each release of the platform has provided either enhancements, bug fixes or new features. The platform, which has undergone extensive evolutionary growth since its original release, is now poised for the next step in the current release iteration of version K2 blackpearl 4.6.

Existing Products	Upgrade Option
K2 blackpearl 4.6.3 (4.12060.1530.0)	K2 blackpearl 4.6.4 (4.12060.1540.0)
K2 blackpearl 4.6.2 (4.12060.1520.0)	K2 blackpearl 4.6.3 (4.12060.1530.0)
K2 blackpearl 4.6.1 (4.12060.1500.0)	K2 blackpearl 4.6.2 (4.12060.1520.0)
K2 blackpearl 4.6 (4.12060.1.0)	K2 blackpearl 4.6.1 (4.12060.1500.0)
K2 blackpoint 0902 + KB00610	K2 blackpearl 4.6 (4.12060.1.0)
K2 blackpearl 0807 () + KB00690 *	K2 blackpearl 4.5 (4.10060.1.0)

* See the compatibility matrix for the versions of K2 supported for a full upgrade to K2 blackpearl 4.6 (4.20060.1.0).

Prerequisites Check



Ensure that the installed prerequisites are correct before the upgrade proceeds.

Since the K2 blackpoint 0902 release, changes may have been made to the prerequisite or there may be additional software components that can be installed. To verify that your existing system is configured correctly, or if there are any additional components that can be used in the K2 blackpearl environment, consult the [Prerequisites by Component](#) listing or the [Prerequisites by Role](#) listing.



Be sure to clear the cache after an upgrade, see the topic [Clear cache after deploying K2 blackpearl](#) for more information.

Permissions

Ensure that you have the correct permissions to run the upgrade to avoid installation issues such as upgrading the workstations using a local domain admin will result in the client not being registered in the database. For the correct installation and upgrade permissions refer to the [permissions](#) topic.

1.7.4.1 Installing a New Version as an Upgrade

Installing a new version as an upgrade

When a new release of K2 blackpearl is available an upgrade can be performed of the current system using the installation program of the new version. To ensure that the current version can be upgraded, see the following link: [K2 blackpearl Upgrade Options](#).



- Read through the release notes provided with the new release as they will contain the necessary items to be aware of before performing the upgrade.
- Ensure that you have the correct permissions to run the upgrade to avoid installation issues such as upgrading the workstations using a local domain admin will result in the client not being registered in the database. For the correct installation and upgrade permissions refer to the [permissions](#) topic.



When performing an upgrade, only those K2 components that are installed on that specific computer will be upgraded. If you need to install other components, run the original setup from the source installation file location and select the [Modify](#) option.

Upgrading from a version prior to K2 blackpearl

Upgrade options are available for customers who are currently using K2.net 2003 and who want to upgrade their system to K2 blackpearl 4.6. Owing to the complexity of the products and the differences between them i.e. the new feature available in K2 blackpearl, there is no direct upgrade path. A Migration Utility is available which MUST be used to first migrate the K2.net 2003 installation to be compatible with K2 blackpearl to ensure a smooth transition between two versions of the product.



There is currently no direct upgrade path from K2 2.4* or K2.net 2003 to K2 blackpearl.

*Certain versions of the product may be either close to end of life or be unsupported as they have been superseded by a new version

1.7.4.2 Upgrade K2 blackpoint > K2 blackpearl

Upgrade requirements



Read KB001386 - How to Upgrade from K2 blackpoint 4.6.4 to K2 blackpearl 4.6.5 before reading this topic to understand the upgrade path in K2 4.6.5.

Prerequisite

Only K2 blackpoint 4.6.4 is upgradable to K2 blackpearl 4.6.5. All prior versions of K2 blackpoint must first be upgraded to K2 blackpoint 4.6.4 before they can be upgraded to K2 blackpearl 4.6.5.

License Keys

When upgrading, the K2 blackpoint license key is no longer valid for a K2 blackpearl installation. During the course of the upgrade, the K2 Installer will prompt the installer for a license key. The machine key is still valid and is used to obtain the new valid license key for your K2 blackpearl installation. If you attempt to use the K2 blackpoint license key, it will notify you that the license key is invalid and prohibit the installation's progress. Once a new license key has been obtained and entered, the installation can proceed.

K2 blackpoint Databases

The upgrade will run database scripts that ensure the existing databases are updated for use by K2 blackpearl. When upgrading a distributed installation, the K2 Server must be upgraded before any of the other K2 components that are distributed. The databases must be updated at the same time, but this is done at the same time as the K2 Server is upgraded. Minor updates are made to the databases, which do not impact on the database structure, the data integrity or the time required to upgrade your system.

Installation Folder

The K2 blackpoint installation folder naming is retained when K2 blackpearl is used to upgrade K2 blackpoint. This is done purposefully to retain the system configuration found in the various configuration files. Owing to this if your K2 blackpearl installation was formerly a K2 blackpoint installation, this must be remembered to avoid future confusion.

Permissions

Ensure that you have the correct permissions to run the upgrade to avoid installation issues such as upgrading the workstations using a local domain admin will result in the client not being registered in the database. For the correct installation and upgrade permissions refer to the [permissions](#) topic.

How to upgrade



The setup manager must be run from the desktop of the local machine.

The two basic iterations of K2 blackpoint that would be upgraded are a standalone installation and a distributed installation.

Upgrade a standalone installation

With the standalone installation upgrading the machine, upgrades the entire deployment.

Upgrade a distributed installation

When a distributed installation is being upgraded, you always start with the K2 Server before upgrading the other components for example WSS or SharePoint. Always upgrade in the following order:

1. K2 Servers
2. Reporting services
3. Workspace
4. Other components in any order

When you upgrade the K2 Server the databases are upgraded at the same time, which means that the SQL server must be up and running during the upgrade of the K2 Server.



Running K2 blackpoint on the same farm as K2 blackpearl, or visa versa, is not possible or supported if attempted.

Steps to upgrade

Locate the executable and double click the file. The installation will initialize and the K2 blackpearl Maintenance screen will display.

Select your option and continue through the Setup Manager steps as described in the [Installation](#) section of this help.

Before the installation begins, the Upgrade Summary page will be shown, showing what components were previously installed and what will be upgraded or added.

1.7.4.3 Upgrading a Farm in a Distributed Environment

Upgrading a Farm in a Distributed Environment

In its simplest form, the process of upgrading a server farm in a distributed environment involves running the Setup Manager on the primary K2 server and selecting Upgrade. Once the primary server is upgraded, the Setup Manager must be run on secondary servers and upgrade selected. Once the server components are upgraded, the SharePoint



There is no need to stop a server before running the upgrade as the Setup Manager will stop and restart the K2 service appropriately. It is important to note that the production environment should not be used during upgrade.

- There are varying levels of complexity and the following points need to be taken into consideration. It is recommended that K2 Support should be contacted and be involved in the upgrade procedure.
- If there are database schema changes to be made as part of an upgrade, access to the entire farm should be prevented during upgrade. All access to the production environment must be stopped beforehand to prevent issues during the upgrade. The ideal order would be to upgrade each K2 server one at a time, where the first server will have the database schema upgrade.
 - If the servers are only being patched and there will be no changes to the database, it is possible to remove a server from the farm NLB/cluster, upgrade that server and place it back in the farm NLB/cluster and then performing this step on each node in the farm.
 - Upgrades should be performed on Development, INT and UAT environments before attempting a live environment with adequate regression testing being performed. This is important when upgrading a number of software versions up from what is currently in use.
 - If SharePoint is in the environment, an upgrade time window must also be factored in as the K2 Setup Manager will perform IIS resets and the WSP deployments will stop and restart each web application on each server in the farm.

1.8 Introduction

Disaster Recovery - Introduction

Disaster recovery is described as the process, policies and procedures put in place to deal with potential natural or human-induced disasters. A disaster is an event that creates chaos and could prevent the continuation of normal functions. A disaster recovery plan forms part of a business continuity plan (BCP) or business process contingency plan (BPCP), and is essential to any organization that wants to either maintain or quickly resume mission-critical functions after such a disaster. The disaster recovery plan should typically include an analysis of business processes and continuity needs, and especially planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. Attention should also be given to disaster prevention. As K2 blackpearl interacts with other external systems such as SharePoint or other line-of-business (LOB), it is important to include all related systems in your disaster recovery planning for K2.

- Scenario 1: Simple K2 backup and restore
- Scenario 2: Running a K2 Standby Server within the same environment
- Scenario 3: Restoring a K2 blackpearl environment
- Scenario 4: SQL Mirroring - manual failover

Disaster Recovery - K2 blackpearl Disaster Recovery

Specific components need to be addressed when creating a Disaster Recovery Plan (DRP) for K2 blackpearl.

K2 Components



Note that since K2 blackpearl 4.5 RTM, the databases have been consolidated and a fresh install of K2 blackpearl will only have one database. Upgrades from previous versions will still have multiple databases.
In general, this document reflects a fresh install.

The following K2 Components need to be considered:

- K2 database
- K2 Web Components
- K2 blackpearl Server
- K2 for Reporting
- K2 for SharePoint

Non K2-specific Components

The following non K2-specific Components need to be considered in addition:

- Forms (ASP.NET/ InfoPath)
- External databases utilized by your K2 processes

If any ASP forms generation client events are used in the K2 processes, it is important to backup these pages. By default, K2 deploys these forms to **C:\Program Files\K2 blackpearl\Workspace\ClientEventpages**

Any ASP pages/sites or InfoPath design files that are used with K2 processes, should also be backed up.

Windows Server Machine

It is assumed that you have a working baseline Windows 2008 Server

Disaster Recovery - SQL Server 2008 Disaster Recovery Options

It is of the utmost importance to back up K2 databases as this forms the core of the K2 functionality and data related information. The following presents a short description of the different options catered for by SQL Server 2008 when backing up the K2 database.

SQL Disaster Recovery Options	
Backup and Restore	<p>Backup refers to the copying of data so that these additional copies may be restored after a data loss event. Backups differ from archives and backup systems differ from fault-tolerant systems. Backups are useful primarily for two purposes:</p> <ul style="list-style-type: none"> • To restore a computer to an operational state following a disaster • To restore small numbers of files after they have been accidentally deleted or corrupted <p>This option supports both full and incremental backups.</p>
Log Shipping	Log shipping allows you to automatically send transaction log backups from a primary database on a primary server instance to one or more secondary

	<p>databases on separate secondary server instances. The transaction log backups are applied to each of the secondary databases individually. An optional third server instance, known as the monitor server, records the history and status of backup and restore operations and, optionally, raises alerts if these operations fail to occur as scheduled. There is however no guarantee that the various databases will be in sync after restoration due to the fact that K2 blackpearl server is writing entries from the K2Server database to K2ServerLog database as the backup of the logs for each database occurs. This method is therefore not the preferred disaster recovery option for K2 blackpearl.</p>
Database Mirroring	<p>Database mirroring is a primarily software solution for increasing database availability. Mirroring is implemented on a per-database basis and works only with databases that use the full recovery model. The simple and bulk-logged recovery models do not support database mirroring. Database mirroring is supported in SQL Server Standard and Enterprise. Database mirroring offers substantial availability and provides an easy-to-manage alternative or supplement to failover clustering or log shipping. When a database mirroring session is synchronized, database mirroring provides a hot standby server that supports rapid failover with no loss of data from committed transactions. During a typical mirroring session, after a production server fails, client applications can recover quickly by reconnecting to the standby server. As this method is similar to Log Shipping mentioned above, and could result in databases being slightly out of sync, it is not the preferred disaster recovery method for K2 blackpearl.</p>
Database Clustering	<p>A failover cluster is a combination of one or more physical disks in a Microsoft Cluster Service (MSCS) cluster group, known as a resource group, that are participating nodes of the cluster. The resource group is configured as a failover clustered instance that hosts an instance of SQL Server. A SQL Server failover clustered instance appears on the network as if it were a single computer, but has functionality that provides failover from one node to another if one node becomes unavailable. Failover clusters provide high-availability support for an entire Microsoft SQL Server instance, in contrast to database mirroring, which provides high-availability support for a single database. It is however recommended to not change the cluster names with restoration as the K2 worklist tables will be out of sync and this will result in errors related to the client events.</p>



Another option that is available within SQL Server, is called replication. This option is however not supported by K2.

For in-depth technical information on SQL Server, visit the following website <http://msdn.microsoft.com/>

Disaster Recovery - SQL Server 2008 R2 Support

Support has been added for the following SQL Server 2008 R2 feature. Note that K2 4.6 or later is required:

- Mirroring – provided for single database scenarios

Disaster Recovery - SQL Server 2012 Support

Support has been added for the following SQL Server 2012 feature. Note that K2 4.6 or later is required:

- Database Services – provided for multiple databases and single database
- AlwaysOn – provided for single database scenarios (be sure to point to the correct SQL Server Always on Listener/Instance)
- Mirroring – provided for single database scenarios

Support has been added for the following SQL Server 2012 feature. Note that K2 4.6.1 or later is required:

- Reporting Services integration – provided for multiple databases and single database scenarios

1.8.1 Scenario 1: Simple K2 Backup and Restore

1.8.1.1 Backing up Keys and Certificates

Disaster Recovery - Backing up Keys and Certificates

It is important to back up SQL Server Keys and Certificates separately as not doing so can result in data loss.

Symmetric Key

The way that K2 uses the Symmetric key is based on K2's use of Certificates. Certificates are built into SQL Server and K2 is leveraging off the SQL Server platform. Hierarchically, it can be depicted in the following way:

- Operating System Level: Windows DPAPI
- SQL Server Level: Service Master Key (SMK)
- SQL Server Level: Database Master Key (DMK)
 - K2: Certificate
 - K2: Symmetric Keys

The encryption is applied in a top down manner, so the Operating System level secures the Service Master Key (SMK), etc.

As discussed in [Database Disaster Recovery Options](#), there are four SQL Disaster Recovery Options which are supported by K2. In all options, the domain should be changed as the Operating System level uses the Service Account or SPN to encrypt the Service Master Key

Backup and Restore

As long as the SQL instance is still functional, the Service Master Key and Database Master Key will still be functional. Recreate the Certificate and Symmetric Keys and the data will be accessible.

Log Shipping

Visit the following link [http://technet.microsoft.com/en-us/library/ms366281\(SQL.90\).aspx](http://technet.microsoft.com/en-us/library/ms366281(SQL.90).aspx) for information on how to create identical symmetric keys on two servers

Both servers should have the same Service Master Key

Database Mirroring

The same applies as in Log Shipping

Database Clustering

The same applies as in Log Shipping, although a Microsoft Cluster Server will not need the identical symmetric keys created as, due to its nature, it is aware of the other nodes and will likely use the same key by design.

Visit the following links for information on backup of Certificates and Keys:

- **Backup the Master Key:** [http://msdn.microsoft.com/en-us/ms174387\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/ms174387(SQL.90).aspx)
- **Backup the Certificate:** [http://msdn.microsoft.com/en-us/ms178578\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/ms178578(SQL.90).aspx)
- **How to backup the Service Master Key:** <http://technet.microsoft.com/en-us/library/aa337561.aspx>
- **How to restore the Service Master Key:** <http://technet.microsoft.com/en-us/library/aa337510.aspx>
- **SQL 2005 Symmetric Encryption:** <http://blog.sqlauthority.com/2009/04/28/sql-server-introduction-to-sql-server-encryption-and-symmetric-key-encryption-tutorial-with-script/>

1.8.1.2 K2 blackpearl databases Backup and Restore

Disaster Recovery - K2 blackpearl Databases Backup and Restore



Prior to a backup or restore of a database, always remember to stop the K2 Service on all K2 Servers first

Backup of databases

Depending on the specific components your organization utilize to integrate with K2, the following databases need to be included in the backup and restoration process:

- K2 databases
- SharePoint databases (if any)
- SQL Reporting Services databases
- Custom Application databases (if any)
- SQL Server databases

default **K2 databases** which should be backed up:

- K2HostServer
- K2SmartFunctions (this db has been removed since K2 blackpearl 4.5 RTM. The db will however still show if an upgrade is performed from a previous version)

If any customized reports have been created, the following **SQL Reporting Service** databases should be backed up:

- ReportServer
- ReportServerTempDb

In addition, the following **SQL Server system databases** should be backed up regularly:

- Master
- Model
- Msdb

If you are using any SharePoint components, it is also advisable to back up any **SharePoint databases**. Any other custom application databases should also be backed up.

Backup of K2 Servers and IIS

Certain customizations of the K2 Servers and IIS are saved in the following files:

- IIS Configuration files
- K2 Configuration files (changes to .config or .setup files)
- Logging files
- Custom DLL's such as custom security providers or SmartObject Services
- Other application files

It is therefore important to backup the entire **K2 blackpearl installation directory** of which the default is **C:\Program Files\K2 blackpearl**

SharePoint features are deployed to **C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\FEATURES**. It might be useful to backup this directory as well.

It is also important to note which K2 version is currently installed and all additional hotfixes or updates are installed on the system.

Restore

It is fairly easy to restore a database using the SQL Server user interface.



Restoring a database will overwrite all changes since the previous backup!

For the different database disaster recovery options provided by SQL Server and supported by K2, see [Introduction](#)

What if I don't want to stop my K2 servers during backup/restore?

The solution to this would be to perform complete backups including transaction log backups which will allow you point-in-time restore.

Use Enterprise Backup software solutions which provide continuous protection. This allows you to restore to any point in time up to the hardware or software failure.

As an alternative, if you are restoring standard backups using the default SQL backup tools, you can opt to restore to a particular point-in-time to prevent database inconsistencies. For more information on this option, visit <http://msdn.microsoft.com/en-us/library/ms190982.aspx>

1.8.2 Scenario 2: Running a K2 Standby Server within the same environment

1.8.2.1 Recommended Procedure

Scenario 2 : Running a K2 Standby Server within the same environment

Scenario 2 describes a method of redundancy in which a secondary backup system located within the same environment is called upon in the event of the primary system failing.

Recommended Procedure:

1. Create a 2 node farm for the K2 Server in which Node 1 has the active license and Node 2 is the standby server.
2. Once the farm has been setup, turn off Node 2 (standby node) in order to adhere to the K2 licensing terms.
3. Plan for failover by using load balancing technology or another approach involving a technology that supports TCP heartbeat checking. See [Setting up NLB](#)
4. In the event of Node 1 failing, launch the K2 blackpearl Server service on Node 2 (standby server) and redirect all traffic to second node.
5. Once Node 1 (primary server) has been restored, the K2 blackpearl Server service on Node 2 (standby server) must be shutdown.

1.8.3 Scenario 3: Running a Parallel Standby Environment

1.8.3.1 Restoring a K2 blackpearl environment

Disaster Recovery - Restoring a K2 blackpearl environment

The following scenarios are addressed with restoration of a K2 blackpearl environment:

Scenarios	
Cold Standby	A method of redundancy in which the secondary (i.e., backup) system is only called upon when the primary system fails. The system on cold standby receives scheduled data backups, but less frequently than a warm standby. Cold standby systems are used for non-critical applications or in cases where data is changed infrequently. The Disaster Recovery server names are the same as the server names currently in use.
Hot Standby	A method of redundancy in which the primary and secondary (i.e., backup) systems run simultaneously. The data is mirrored to the secondary server in real time so that both systems contain identical information. The Disaster Recovery server names are different to the server names currently in use. See Database Disaster Recovery Options for issues when using SQL Log Shipping and Database Mirroring.
Warm Standby	A method of redundancy in which the secondary (i.e., backup) system runs in the background of the primary system. Data is mirrored to the secondary server at regular intervals, which means that there are times when both servers do not contain the exact same data. See Database Disaster Recovery Options for issues when using SQL Log Shipping and Database Mirroring.



If loss of data is a concern, another option would be to perform SAN (system area network) mirroring, i.e. everything that is written to a SAN in the main site is replicated via the SAN link to the disaster recovery site. This is however an expensive option.

Restoring to a Cold Standby environment

Follow the steps below to restore to a cold standby:

1. Ensure that the Windows machine is in working order
2. Install the K2 Server and K2 Web Components
3. Apply service packs and/or updates
4. Restore the K2 blackpearl installation directory from backup
5. Restore databases from backup
6. Restore K2 servers and IIS servers from backup
7. Restore any other files for your K2 processes
8. Run the K2 blackpearl Configuration Manager to update the new license key
9. Start your K2 server
10. Test your K2 processes and data
11. Check the K2 Workspace and the server event log for any errors

Preparing a Hot or Warm Standby environment for restoration

It is important to note that preparation of the Hot or Warm Standby environment is required prior to the disaster occurring, as K2 stores configuration and licensing information within the K2 configuration databases. Follow the steps below to prepare the environment for a Hot or Warm Standby restoration:

1. Install K2 blackpearl on the Disaster Recovery servers
2. Perform a full system backup of the K2 Disaster Recovery servers
3. Perform a backup of the data in the following two tables in the K2 databases:
 - _Server table in K2Server database
 - LicenseKeys table in HostServer database
4. Take the Hot or Warm Standby servers offline

Restoration of a Hot or Warm Standby environment

Follow the steps below to restore a Hot or Warm Standby environment:

1. Bring the Hot or Warm Standby environment online
2. Restore the K2 blackpearl ServiceBroker directory(K2 blackpearl\ServiceBroker) from backup
3. Restore any other custom assemblies that your processes may require to the machine
4. Restore the backed up databases
5. Restore the K2 Disaster Recovery Servers
6. Restore the data from the two tables backed up earlier

7. Update all references to the old machine such as ASPX pages, links to the Workspace, Worklist Web parts in SharePoint etc to point to the new machine name
8. Start the K2 blackpearl Service
9. Test your K2 processes and data
10. Check the K2 Workspace and the server event log for any errors

Restoring the K2 for Reporting Services Components

Follow the steps below to restore the K2 for Reporting Services Components:

1. Return the Windows machine to a working state
2. Install the K2 Reporting Components
3. Restore Reporting Services databases



If you need to reinstall the K2 Server Components, a new license key is required. The machine keys will probably change if the servers are on new hardware (except when using VM environments). You need to re-run the K2 blackpearl Configuration Manager to generate the new machine keys and then request new license keys.

1.8.3.2 Disaster Recovery - Recommended Procedure

Recommended Disaster Recovery Procedure

This topic covers the K2 recommended procedures to enable Disaster Recovery (DR) within the infrastructure that leverage physically different data centers for production and disaster scenarios.

The following parameters are assumed:

- Accepted data loss of 4 hours
- K2 system data is consistent upon a cut over to the DR site

Should the window of accepted data loss need to be adjusted, the scheduled jobs laid out below should be recalculated accordingly.

The procedure below leverage an initial set of database backups and then transaction log shipping with a point-in-time recovery to allow for consistent K2 data in the event of a disaster event.

Prerequisite

The following should be done,

- Within the **DR** site:
 1. Record the K2 licensing information in the following SQL tables:
 - K2Server._Server
 - K2HostServer.LicenceKeys

 The data should be similar in both locations
 2. Create a SQL Script that will reapply this information during an actual disaster recovery event.

 This is required because the K2 licensing is stored within the database and is bound to a specific environment. As such restoring databases across environments as in a DR scenario will replace the DR license with the PRODUCTION license. Creating a SQL script to restore the original DR license, while not always necessary, will make this a more repeatable procedure should it be desired.

3. Keep the K2 host server nodes turned off until a DR cut over is required. This ensures that the DR site does not try to process transactions based upon its copy of the K2 database.

Initial Setup

The following setup is required,

- Within the **PRODUCTION** site:
 1. Turn off the K2 service on all nodes within the K2 farm. This insures no K2 data manipulation.
 2. Create Full Database Backups of all K2 product databases as mentioned in [K2 blackpearl databases Backup and Restore](#). Alternatively, incremental backups may also be used . Either way, compression of databases is advised for efficiency.
 3. Script out all external database server artefacts, e.g. database logins, users, etc.
 4. Backup additional database(s) leveraged by the solution.
 5. Turn on the K2 service on all nodes within the K2 farm.
 6. Move the database backups to the DR site.
- Within the **DR** site:
 1. Restore the PRODUCTION database backups.
 2. Reapply external artefacts (logins, etc).
 3. Re-apply K2 licensing, as identified in the Prerequisite step.

Ongoing

- Within the **PRODUCTION** site:
 1. Create a scheduled SQL Agent job (recommended hourly) within the SQL Server that backs up the transaction logs for the following:
 - All K2 product databases
 - Solution database(s)
 2. Schedule a Log Shipping job to transmit these logs to the DR site.
- Within the **DR** site:
 1. Within the DR site create a scheduled job (recommended hourly) that will apply any transaction log backups for the databases that are greater than 3 hours old.
- Archive the just-applied Transaction Log files.

Disaster Recovery Cutover Procedure

1. If possible, backup the 'tail end' of the log(s) from the primary site and transmit them to the secondary site.
2. Determine the time of the disaster at the production site and subtract 2 hours. Choose an exact time of recovery that makes sense, for instance 13:35:00:000.
3. Recover queued transaction logs for all databases to that same specific point in time (the chosen time may or may not include the 'tail end' backups obtained in 1). In this example, all databases should be recovered until 13:35:00:000.
4. Reapply the appropriate K2 server licenses within the DR environment (preferably leveraging the script file recommended in the Prerequisite section, point number 2)



As a result of the time difference, there will always be 1 (or 2 or 3 as need be) log difference. This allows a restore to a point in time operation on the final log in the event of a DR event. After this restore to a point in time operation all databases will be consistent.

Testing

A manual failover process should be executed during development/QA to ensure that the procedure works as expected. All K2 operations should be tested in order to confirm that the primary data files and external artefacts (such as logins) are valid.

1.8.4 Scenario 4: SQL Mirroring - manual failover

1.8.4.1 SQL Mirroring - manual failover

SQL Mirroring - manual failover

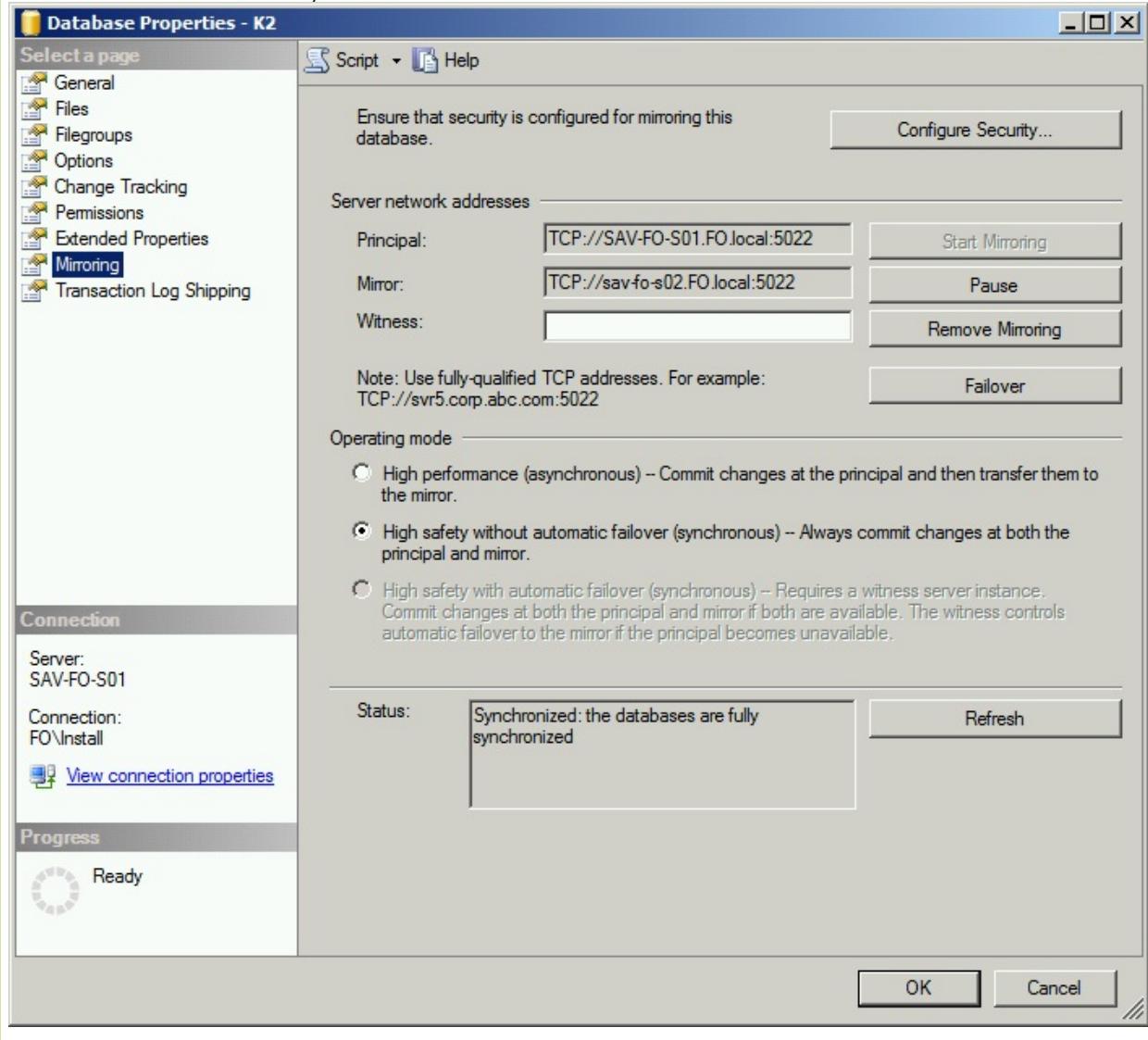
The following steps show a quick description of the process of installing K2 with a standby system using SQL mirroring:

- 1
- 2
- 3

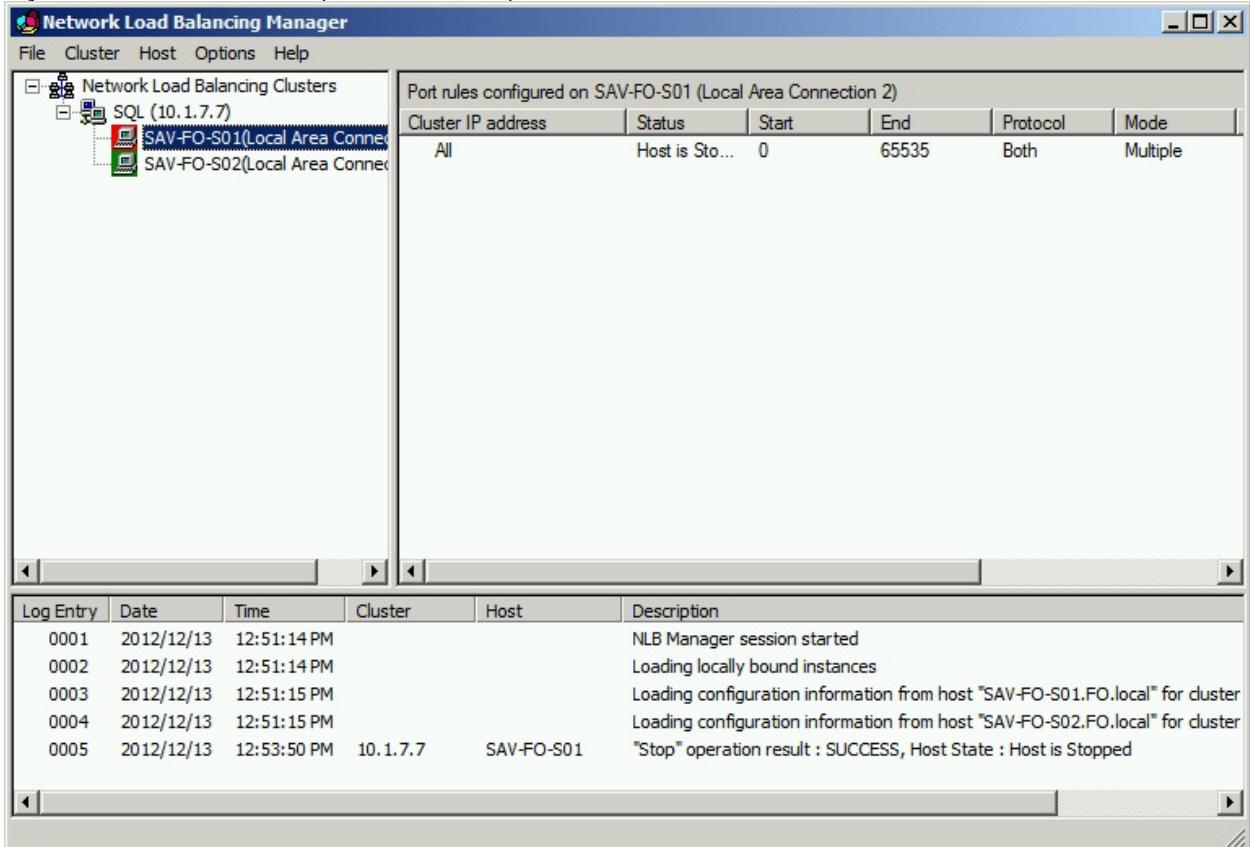
Install and configure K2 on the primary environment - the K2 database would be mirrored to the standby environment. Use the SQL alias in the K2 configuration to the SQL box. Also install the SharePoint components.

Stop K2 services on primary environment.

Fail-over the mirror to the standby environment.



Adjust the load balanced URL to point to the standby environment.



Install K2 on the standby environment ensuring that the SQL alias is used and the NLB address is used.

Disable K2 services on the standby environment.

Adjust the load balanced URL to the primary environment again.

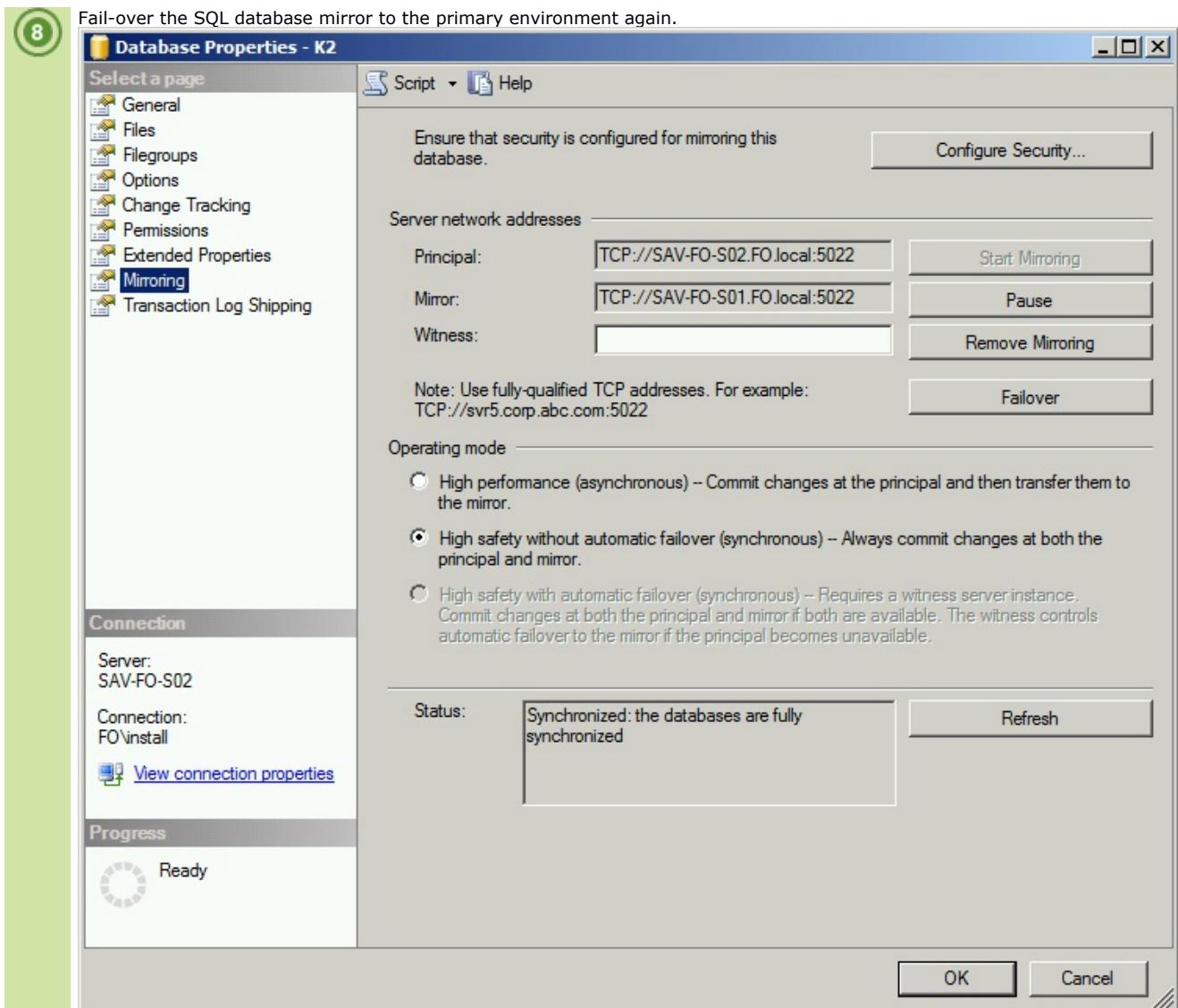
4

5

6

7

Fail-over the SQL database mirror to the primary environment again.



Start the K2 services on the primary environment and check the log files to be sure no errors were encountered.



1.9 Troubleshooting

1.9.1 InfoPath

1.9.1.1 InfoPath - Access is Denied Error

Troubleshooting - Access is denied error in InfoPath Integration

When opening an InfoPath document from an InfoPath event, an error occurs when clicking on the "Continue" button to submit the form.

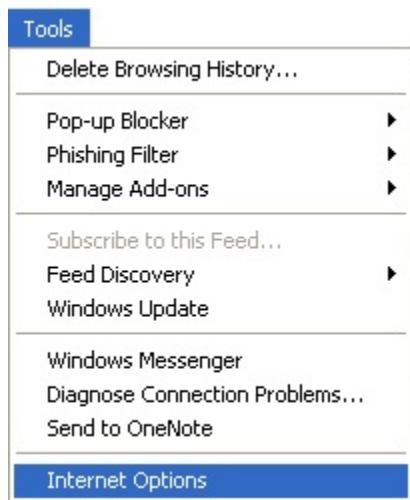
The following error message is displayed:

InfoPath can not submit the form. An error occurred while the form was being submitted. Access is denied.

To rectify this problem perform the following steps:

(1)

Open **Internet Explorer**.



(2)

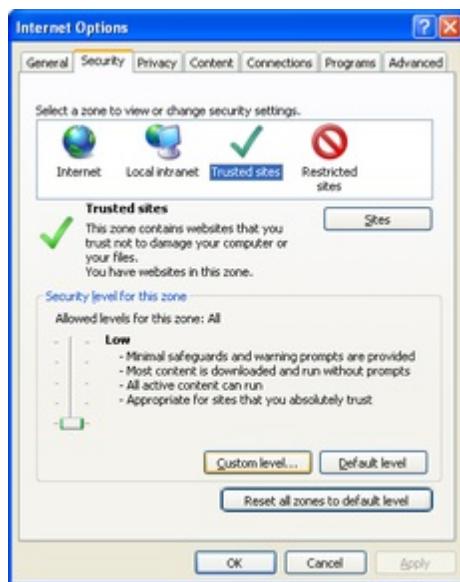
Click on **Tools > Internet Options**

(3)

Click on the **Security Tab**.

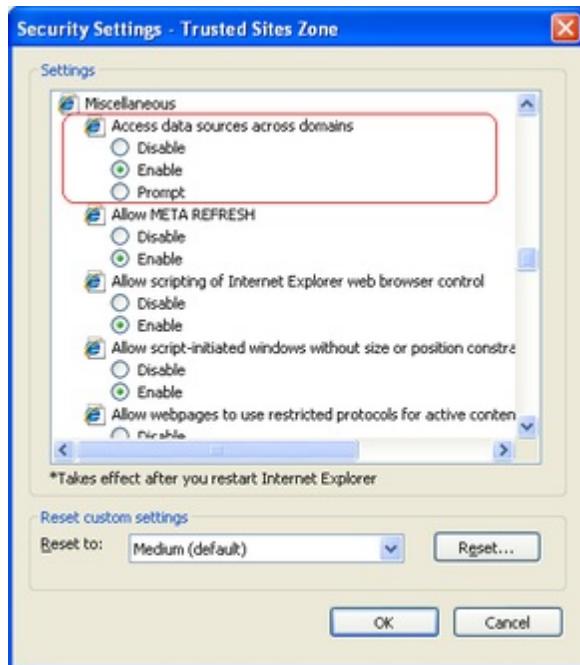
(4)

Click on **Trusted Sites** and click on **Custom Level**.



(5)

Enable the "Access data sources across domains".



Repeat the above steps for a **Local Intranet**.



1.9.1.2 Action not found error in InfoPath

Troubleshooting - Action not found OR Some rules were not applied error in InfoPath

When an InfoPath client event requires only one outcome, i.e. there is only one possible route to the next activity, an error may occur if the user is unaware of how the K2 platform assigns **Actions**. Regardless of the type of outcome selected, an error occurs in InfoPath displaying the **Some rules were not applied** dialog box:

InfoPath cannot submit the form.

An error occurred while the form was being submitted.

The SOAP response indicates that an error occurred on the server:

```
System.Web.Services.Protocols.SoapException: Server was unable to process request. ---> System.Exception: The
worklist item cannot be completed due to the following reason: Action not found
   at SourceCode.Workflow.RuntimeServices.InfoPathFunctions.HandleException(Exception ex)
   at SourceCode.Workflow.RuntimeServices.InfoPathFunctions.SubmitInfoPathData(Object infoPathFormXml)
   at SourceCode.Workflow.RuntimeServices.InfoPathService.SubmitInfoPathData(Object infoPathFormXml)
--- End of inner exception stack trace ---
```

However, when using the **Action(s) > Task Complete** option from the folio dropdown in K2 Workspace the task item completes successfully.

Solution:



Create a data field in the Form with a default value equal to the action that is created in K2. For example: If the action is equal to **Yes**, then the default value of the Data Field will also be equal to **Yes**. In this example this error can therefore be resolved by changing a **Task Completed** action to **Yes** and setting the data field **Completed** to a default value of **Yes**.



Run the InfoPath client event wizard and set the Task Action Field to the **Completed** data field in the **XML/Process/my:myFields** structure. If the wizard asks to create the control, click **No**. Complete the wizard setup.



When running the InfoPath wizard, K2 automatically creates a rule under the form **Submit Options** called **Set Workflow Task Action** in which it sets the value of the ActionName field to be the name of the DataField in which it will look for the action result. Check that the wizard has created the rule.

Explanation:

In K2 blackpearl the **WorklistItem** object contains a collection property called **Actions**. This property can be used by the UI to get a list of actions that is not only available on the activity but also available for a specific user. This increases the functionality of the **WorklistItem** and decreases the maintenance requirements.

For example; if an activity has 2 destinations (i.e. Bob and Joe), they can both execute or complete the task by selecting any one of the actions available. In an escalation we can set permissions on an action for a user (even one that was not even part of the original destination rule) to escalate the task to a higher authority, without having to redirect or loop back onto the activity to get the task to the **new** user. A user may also be given permissions to open the task in **View** format which will allow the user to open the task but not execute any one of the actions.

The **WorklistItem** drop down is populated with the available actions, so the InfoPath Form simply needs to call the **Execute** method of the Action object.



The **WorklistItem.Finish** method, however, is still available for backwards compatibility.

1.9.1.3 InfoPath - An error occurred accessing a data source

Troubleshooting - An error occurred accessing a data source

The following error can occur when a user attempts to submit an InfoPath form:

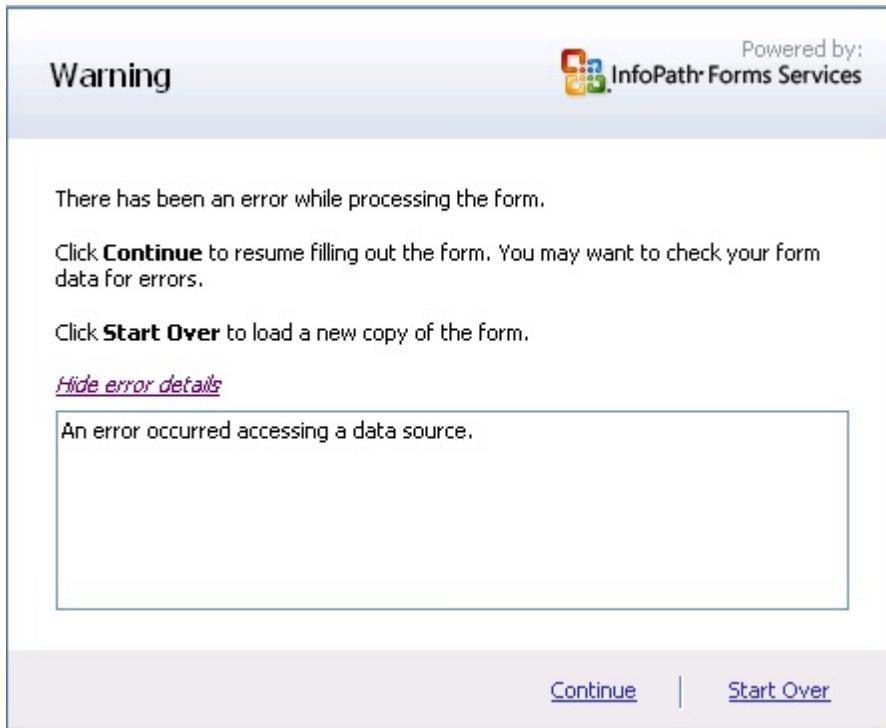


Fig. 1. InfoPath Error

This error is caused by the user not having rights on the parent site but only on the sub site. As the K2 blackpearl Data Connections Library is created on the parent site and not on the sub site the user can access the form but cannot submit the form.

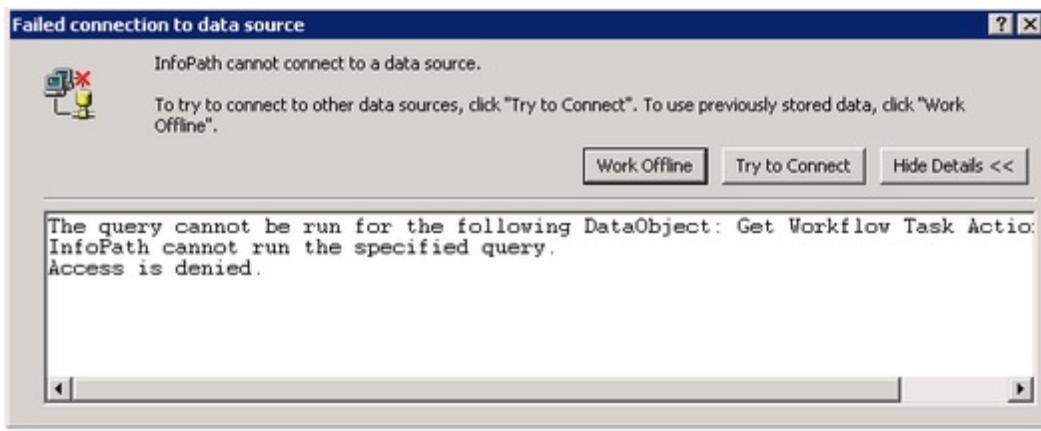
Resolution

Assign 'Read' permissions for the user directly on the K2 blackpearl Data Connections Library in the parent site (View All Site Content). The user will not be able to access the parent site but will no longer encounter the error when trying to submit the InfoPath form.

1.9.1.4 InfoPath - Failed Connection to Source

Troubleshooting - InfoPath Integration Failed connection to data source

While opening a worklist item in a remote desktop an **Access Denied** error is received as shown below:



This error will be displayed while trying to open a worklist item from a user, where the user does not have the necessary Internet Security rights. To rectify this problem perform the following steps:

On the Administrator Machine



Open **Users and Groups** in Active Directory



On the Domain, right-click and select **Properties**



Click on the **Group Policy** tab, and edit the current Group Policy



Navigate to User Configuration > Windows Settings > Internet Explorer Maintenance > Security



Right click on **Security Zones and Content Rating** and select **Properties**

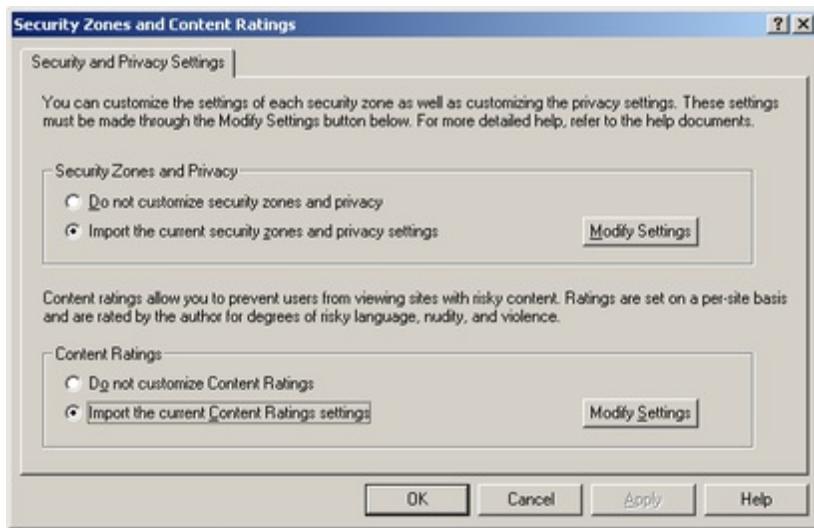


Click Continue on the message



7 Select **Import the current security zones and private settings** on both the tabs

8 On the Security zones and privacy tab, click on the **Modify Settings** button and add the trusted sites and set the required Security level.



9 Select **OK** and run the gpupdate/force command on the remote desktop.

1.9.1.5 InfoPath - Form Error

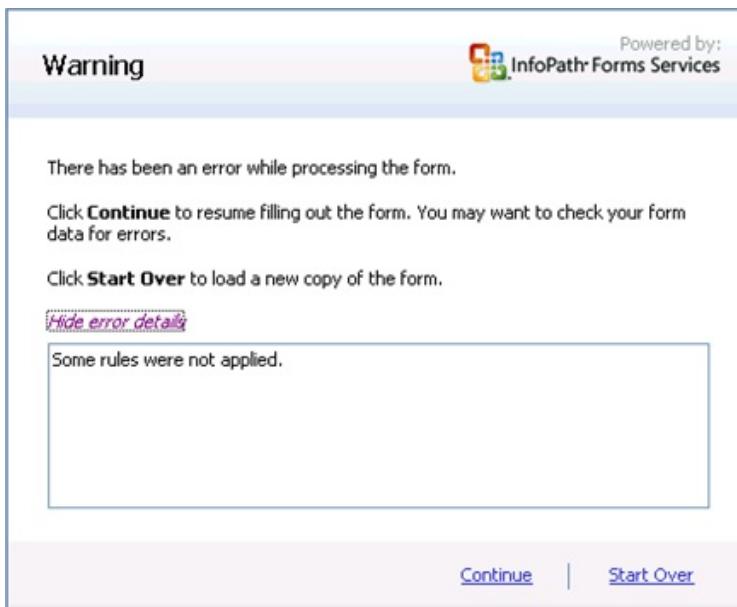
Troubleshooting - InfoPath Integration Form Error

When using Forms Server with InfoPath Forms the following errors might be received:

While opening an InfoPath Form in a browser, the following error is displayed:



While opening an InfoPath Form in SharePoint, the following error is displayed:



To rectify this problem perform the following steps:

- 1 On the main SharePoint Site, browse to Site Actions > Site Settings > Modify all Site Settings. Select the **Modify All Site Settings** in SharePoint
- 2 Select **Advanced Settings**
- 3 Under Browser-enabled Documents, select the **Open in the client application** option

Browser-enabled Documents
 Specify how to display documents that are enabled for opening both in a browser and a client application. If the client application is unavailable, these documents will always be displayed as Web pages in the browser.

Opening browser-enabled documents
 Open in the client application
 Display as a Web page
- 4 Open the InfoPath Document. If the error is still displayed, perform the following steps:

On the Administrator Machine

- 1 Open Central Administration
- 2 Click on the **Application Management** tab
- 3 Click on **Configure InfoPath Form Services**
- 4 Ensure that the **Allow cross-domain data access for user form templates that use connection settings in a data connection file** option is selected

InfoPath Forms Services

- Manage form templates
- [Configure InfoPath Forms Services](#)
- Upload form template
- Manage data connection files
- Manage the Web service proxy

Cross-Domain Access for User Form Templates

Form templates can contain data connections that access data from other domains. Select this check box to allow user form templates to access data from another domain.

Allow cross-domain data access for user form templates that use connection settings in a data connection file

1.9.1.6 InfoPath - Form cannot be displayed error

Troubleshooting - InfoPath Form cannot be displayed error

A **The form cannot be displayed because the session state is not available** error is received when attempting to open an InfoPath Form in a browser. This occurs in scenarios where a Web Enabled InfoPath Form connects to a WebService which is located on another server. The problem is experienced due to the Form not being able to pass the current user's credentials.

Workaround:

Refer to the following Microsoft links to rectify this problem:

<http://blogs.msdn.com/infopath/archive/2006/10/30/the-anatomy-of-a-udc-file.aspx>

<http://blogs.msdn.com/infopath/archive/2006/10/02/Data-Connections-in-Browser-Forms.aspx>

<http://msdn2.microsoft.com/en-us/library/ms771995.aspx>

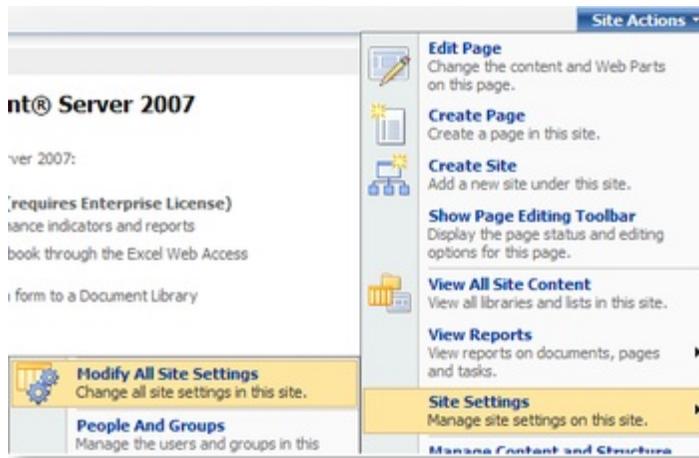
1.9.1.7 InfoPath - InfoPath Form is not displayed on Worklist

Troubleshooting - InfoPath Form is not displayed on SharePoint Worklist

After submitting an InfoPath Form in SharePoint, it is not displayed on the SharePoint Worklist. This may be because the incorrect users are stipulated in the Site Collection Administrators list. To rectify the problem perform the following steps:

1

On the main SharePoint Site, browse to Site Actions > Site Settings > Modify all Site Settings.



2

Click on **Site Collection Administrators** and add the Administrator and Service Account information in the text box

1.9.1.8 InfoPath - Integrate with SmartObject

Troubleshooting - InfoPath Integration with SmartObject

When using InfoPath with SmartObject Integration to retrieve data from a SmartObject and viewing the form in a browser, an error displaying a message stating **An error occurred accessing a Data Source**. When viewing the form in the InfoPath client, the connections to the SmartObject works correctly.

Solution:

If the **Integrate with SmartObject** option is used the following steps must also be followed as this is not automatically done by the standard InfoPath publishing functions:

- 1** In InfoPath browse to **Tools > Data Connections**.
- 2** Select the first SmartObject Data Connection and click **Convert** and Browse to the relevant SharePoint Data Connection Library.
- 3** Type the MOSS URL as the File Name and click **Save**.
- 4** From the list select a valid **Data Connection Library** from the list. If there are no Data Connection Libraries, open SPS and create one in the same way a Form Library is created in SharePoint. The **Data Connection Library** template is listed under the **Libraries** section.
- 5** Provide the Data Connection Library with a relevant name and click **Save** to continue.
- 6** Ensure that the **Relative to site collection** option is selected.

 If it is not possible to create a Data Connection Library open Services and stop the **System Event Notification** service
- 7** Once the first connection has been converted the .udcx file can be reused for all other SO Data Connections as the file does not contain information specific to the SO Method.

 The deploy task that is part of the InfoPath Workflow integration does this automatically, so these steps are not needed when using Workflow Integration with InfoPath.

1.9.1.9 InfoPath - Invalid date error in Data Event wizard

Issue:

When using a suggested "Format DateTime - Inline function" with a K2 Date field and the "yyyy-MM-dd" format as a parameters for a mapping source, and an InfoPath "Date" XML node as the destination, the mapping during runtime resolves the source value correctly for example,"2010-07-20" but casts the value to a DateTime object which then adds a TimeSpan to the already correct Date value resulting in "2010-07-20 12:00:00 AM". This is not expected in the InfoPath schema for the Node , which causes InfoPath to raise an error on opening stating that the "value is not a valid date".

The destination value type can be determined as the InfoPath schema for the node is available when the mapping is being authored, this will allow the Data Mapper to determine whether the source value should be used as a string or as a datetime object during runtime.

Workaround:

1. Copy the code from the file PerformMappings by right clicking then go to definition on "PerformMappings()".
2. Paste it into a new Server Event.
3. Alter the code not to do the date conversions.

1.9.1.10 InfoPath - URL Not Found

Troubleshooting - InfoPath Integration URL not valid

When publishing an InfoPath form to SharePoint from InfoPath, an error is displayed stating; **The Following URL is not valid <URL>**.

To rectify the problem stop the **System Event Notification** service and restart the service.

SQL Server VSS Wri...	Provides th...	Started	Automatic	Local System
System Event Notifi...	Monitors s...	Started	Manual	Local System
Task Scheduler	Enables a...	Started	Automatic	Local System

1.9.1.11 InfoPath - Workflow Unable to Deploy

Troubleshooting - InfoPath Integration Workflow Unable to Deploy

While attempting to deploy an InfoPath process the following error is displayed:

Error 4 Server was unable to process request.

Activation could not be completed because the InfoPath Forms Services support feature is not present.

Solution:

Perform the following steps to rectify the problem:



From the appropriate site, navigate to **Site Actions > Site Settings > Modify All Site Settings**

Select **Site Features** from the **Site Administration** column.

Deactivate **Office SharePoint Server Enterprise Site features**

Reactivate the **Office SharePoint Server Enterprise Site features**



The above steps needs to be performed for the specific sub site and not at the top-level site collection

1.9.1.12 InfoPath and SmartObjects issue with Re-publish

Troubleshooting - InfoPath and SmartObjects issue with Re-publish

An issue occurred while using InfoPath and SmartObjects and attempting to Re-publish the InfoPath form.

Scenario

The following scenario existed:

An InfoPath process integrated with a K2 process with a number of SmartObjects as secondary data sources. While attempting to deploy from development to a testing environment, the following steps were performed:

1. Changed the K2 Object Browser to the target environment.
2. Performed a clean up of the project.
3. Performed a deployment to the target environment (just to make sure the project is all setup for the proper environment).
4. 'Designed' the InfoPath Form from the InfoPath Integration Wizard in the process.
 - a. Changed something on the form.
 - b. Reviewed the Data Sources (the data sources were all pointing at the proper staging target .asmx file)
 - c. Saved and closed the InfoPath Form
5. The K2 InfoPath Wizard then auto-refreshed.
6. Stepped through the wizard and completed the wizard.
7. Performed a clean up of the project.
8. Re-publish the project (just the particular process).

Problem

So at this point, an XSN should exist that fully points to the target (staging) environment. The problem is, however, that this is not the case. The actual data source xml files (when you extract the innards of the published XSN) all still have the <_soServer> node pointing at the development environment.

Since the forms needed to be code-signed, the Re-publishing was done manually. Unfortunately the wrong form was used (the xsn from the K2 project was used instead of the xsn from SharePoint)

Solution

To fix the <_soServer> data source XML inside the InfoPath form so that it points to the new environment's correct SmartObject Server, it is important to note the following.



The xsn in the K2 project folder doesn't represent what was published to SharePoint. The xsn published into SharePoint has all the correct values. So if you need to do a manual Re-publish as a result of needing full-trust code-signing and/or form services, retrieve the xsn out of SharePoint and modify that one, not the one from within the K2 solution.

1.9.1.13 InfoPath - Troubleshooting Deployment Error in K2 Studio

Scenario

The following scenario is an example of where a deployment error in K2 Studio occurred:

- K2 Server is running in domain A, K2 Studio is in domain B with a logged on user from domain A
- Processes that don't use InfoPath deploys successfully
- Processes integrated into InfoPath fails on deploy

Troubleshooting Tips

If you are experiencing problems when trying to deploy a process in K2 Studio after an installation, use the following checklist to identify issues:

- Check the MSMQ configuration on the K2 Server
- Launch the K2 Configuration Analysis tool and check if any errors are reported
- Check the permissions of the K2 Service Account on the K2 Server
- Check to see if authenticated users and local administrators have rights on c:\windows\temp and on the %SharePoint%\template directories
- Check if the user (used to deploy the Workflow) has access to the K2 installation folder
- Check if the K2 Service account has FULL access to the K2 installation folder
- When using more than one domain, check the trust between the domains
- Check if the deployment user has permissions in SharePoint

Checks specific to the scenario which can be performed:

- Deploy the InfoPath process using a deployment package on the K2 Server (which is in domain A) whilst logged on as a user in domain A in other words eliminating domain B factor
- Remove all SmartObject methods from your InfoPath form, or try to deploy a simple "test" process with a simple InfoPath Form that don't use SmartObjects
- Try to disable the creation of Reporting SmartObjects in the MSBuild file

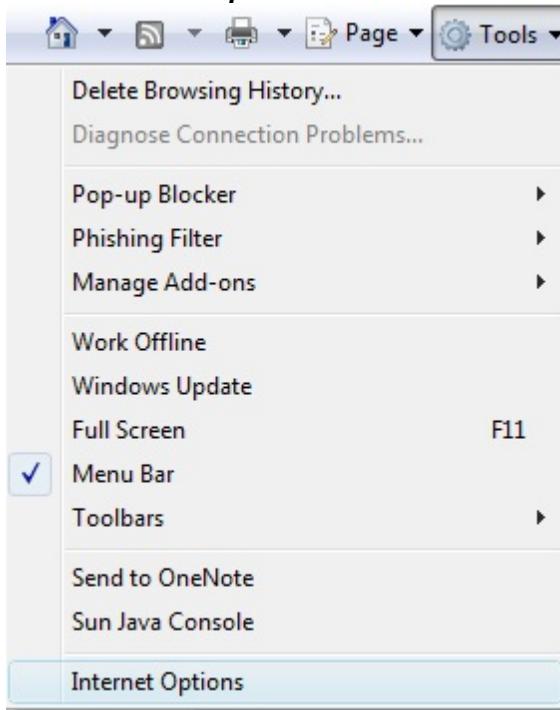
1.9.2 Internet Explorer

1.9.2.1 Clearing Internet Explorer Cache

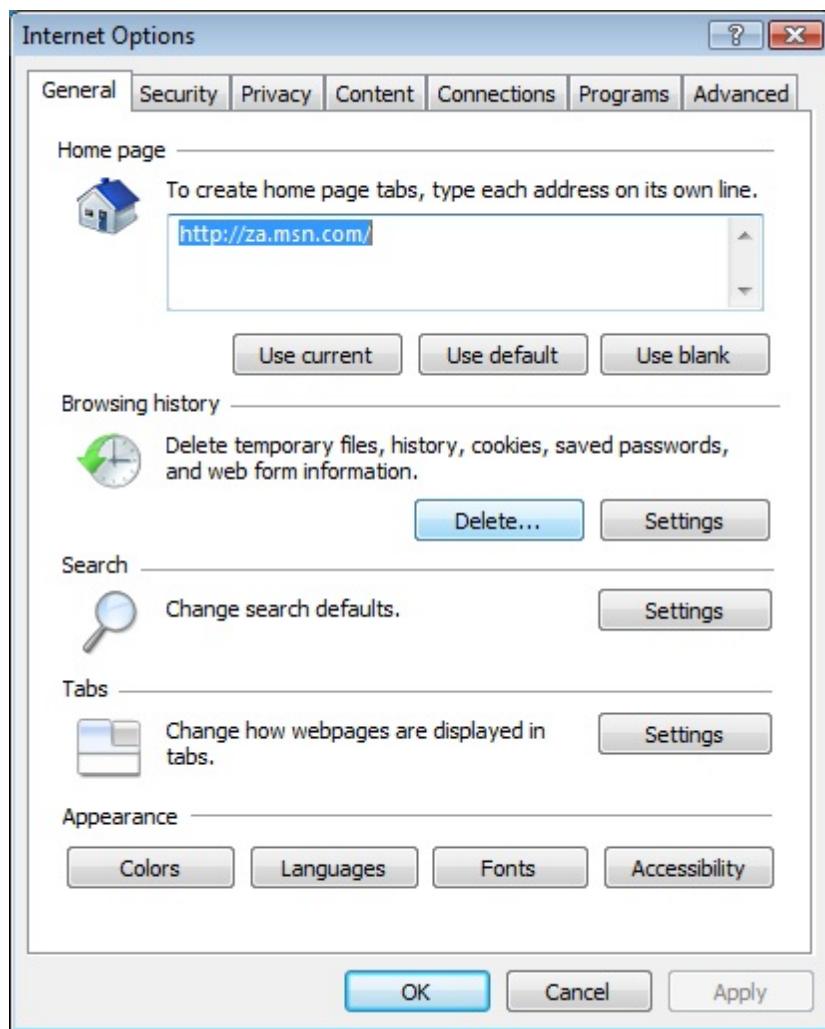
Clear cache after deploying K2 blackpearl

If users cannot see the K2 features after installing and configuring K2 blackpearl, one thing to try is to clear their internet cache. The below example is for clearing the cache in Internet Explorer 7:

1. Open Internet Explorer and select the down arrow next to **Tools**
2. Click on **Internet Options**



3. Under the Browsing history section, click on the **Delete** button



4. Click on the **Delete All...** button



5. On the warning dialog, click **Yes**



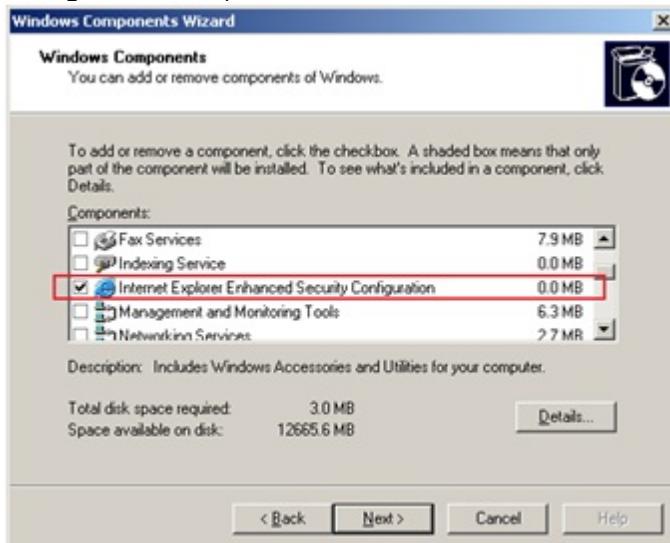
6. When the cache has been deleted, close Internet Explorer
7. Reopen the browser, and try accessing the K2 feature again

1.9.2.2 Removing Internet Explorer Enhanced Security

Certain K2 blackpearl components, like the K2 Designer for SharePoint and the Notification Designer, require the Internet Explorer Enhanced Security Configuration (IE ESC) to be disabled. The IE ESC restricts rendering the interactive javascript used by the AJAX controls used to give users a Windows-like feel in the designers. This is a known issue and will be fixed in a future update.

To disable the Internet Explorer Enhanced Security configuration, perform the following steps on the K2 Workspace and SharePoint servers:

1. Open **Add/Remove Programs** by clicking Start > Control Panel > Add or Remove Programs
2. Click **Add/Remove Windows Components**
3. In the Windows Components dialog, scroll down until you see the **Internet Explorer Enhanced Security Configuration** component:



4. **Uncheck** the checkbox next to the Internet Explorer Enhanced Security Configuration item
5. Click **Next**, and the wizard will configure the components
6. Once the configuration has been completed, click **Finish**. You can close the Add or Remove Programs window.

1.9.2.3 Settings for Internet Explorer

In order to access the K2 Workspace in a distributed environment, there are some settings that need to be configured on the client's Internet Explorer browser.



These settings must be set for all users who access the K2 Workspace remotely (meaning, not on the K2 Workspace server). You can set these permissions via Group Policy. Be sure that you set these permissions for the accounts you are testing with, as using the "run as" command does not keep the Internet Explorer options of the previous account.

First, you will need to turn on Windows Integrated Authentication:

1. Open **Internet Explorer**
2. From the Internet Explorer menu, select **Tools > Internet Options**
3. Click on the **Advanced** tab, and then scroll down to the Security section
4. Check the **Enable Integrated Windows Authentication** check box
5. Click **OK**
6. Close Internet Explorer

Secondly, you have a choice to make. There are two options, you can either add the K2 Workspace URL to the Local Intranet Zone, or to the Trusted Sites and allow pass through integration of the user's credentials. These options are described below. Please note, you can only select one of the options (meaning, Local Intranet Zone or Trusted Sites, but not both).

Local Intranet Zone

To add the K2 Workspace site to the Local Intranet Zone, perform the following steps:

1. Open **Internet Explorer**
2. From the Internet Explorer menu, select **Tools > Internet Options**
3. Click on the **Security** tab, and then select the **Local Intranet Zone**
4. Click **Sites**
5. Click **Advanced** to open the list of sites in the Local Intranet Zone
6. Type in the **K2 Workspace URL** and click **Add**
7. After the site has been added, click **Close** and then **OK** twice to exit the Internet Options dialog

Trusted Sites

To add the K2 Workspace site to the Trusted Sites, perform the following steps:

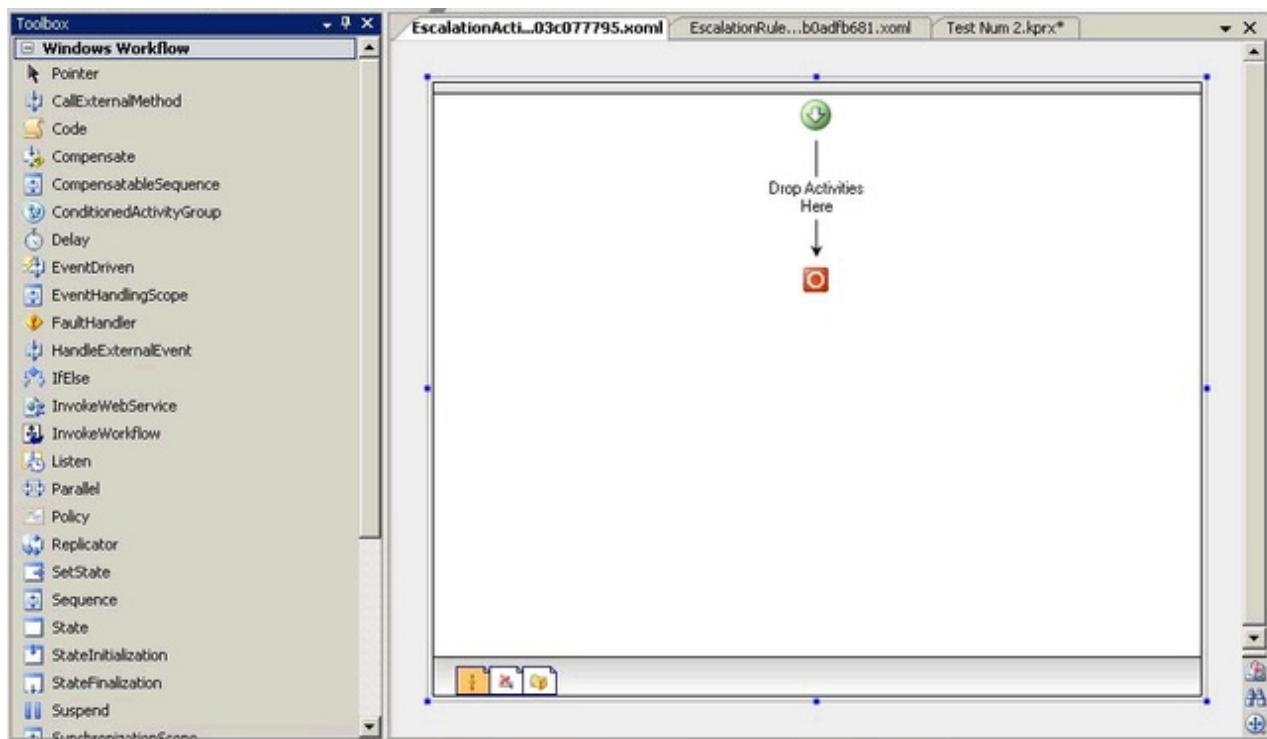
1. Open **Internet Explorer**
2. From the Internet Explorer menu, select **Tools > Internet Options**
3. Click on the **Security** tab, and then select the **Trusted Sites**
4. Click **Sites**
5. Click **Advanced** to open the list of sites in the Local Intranet Zone
6. Type in the **K2 Workspace URL** and click **Add**
7. After the site has been added, click **Close**
8. Click on the **Custom level...** button on the Security tab
9. Scroll down to the User Authentication section, and select **Automatic logon with current user name and password**
10. Click **OK** twice to exit the Internet Options dialog

1.9.3 K2 Designer for Visual Studio

1.9.3.1 Default Escalation Code Block Doesn't Generate

Troubleshooting - Default Escalation Code Block Fails To Generate

When creating a default escalation rule and selecting the **view all code** option, a Windows Workflow schedule that simply has a green arrow followed by a **Drop Activities Here**, and a red circle, as displayed in the image below, is displayed. Users may expect to see a code block with the appropriate K2 context object so that they could write their own escalation code.



Solution:



Open the Microsoft Visual Studio 2005 toolbox and drop a **Code** item onto the **Drop Activities Here** space. It will now be populated with **CodeActivity1**.

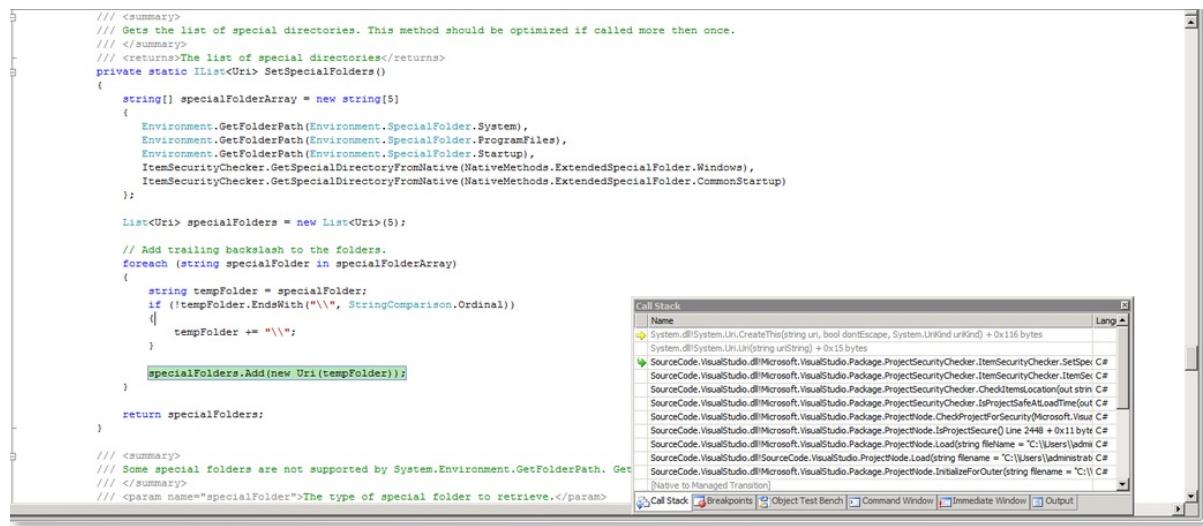


Double click on **CodeActivity1**, and the code window will appear - code can now be entered.

1.9.3.2 Visual Studio - Invalid URI

Troubleshooting - Invalid URI: The format of the URI could not be determined

While running Visual Studio as another user, and no profile exists for the user on the particular machine, the common folders are not available on the machine. These folders are used in MSBuild in the VisualStudio SDK code files. This will give an error displaying the following message: **Invalid URI: The format of the URI could not be determined.**



The screenshot shows a debugger interface with two windows. The left window displays a portion of the `Uri.cs` source code, specifically the `GetSpecialFolders` method. The right window is a "Call Stack" window showing a stack trace. The stack trace lists several frames from the `SourceCode.VisualStudio` assembly, indicating the call chain leading to the exception. The top frame is `System.dll!System.Uri.CreateFromPath(string urlString, bool dontEscape, System.UriKind uriKind) + 0x16 bytes`.

```

    /// <summary>
    /// Gets the list of special directories. This method should be optimized if called more than once.
    /// </summary>
    /// <returns>The list of special directories</returns>
    private static IList<Uri> GetSpecialFolders()
    {
        string[] specialFolderArray = new string[5];
        {
            Environment.GetFolderPath(Environment.SpecialFolder.System),
            Environment.GetFolderPath(Environment.SpecialFolder.ProgramFiles),
            Environment.GetFolderPath(Environment.SpecialFolder.Startup),
            ItemSecurityChecker.GetSpecialDirectoryFromNative(NativeMethods.ExtendedSpecialFolder.Windows),
            ItemSecurityChecker.GetSpecialDirectoryFromNative(NativeMethods.ExtendedSpecialFolder.CommonStartup)
        };

        List<Uri> specialFolders = new List<Uri>(5);

        // Add trailing backslash to the folders.
        foreach (string specialFolder in specialFolderArray)
        {
            string tempFolder = specialFolder;
            if (!tempFolder.EndsWith("\\\", StringComparison.Ordinal))
            {
                tempFolder += "\\";
            }

            specialFolders.Add(new Uri(tempFolder));
        }

        return specialFolders;
    }

    /// <summary>
    /// Some special folders are not supported by System.Environment.GetFolderPath. Get
    /// </summary>
    /// <param name="specialFolder">The type of special folder to retrieve.</param>
}

```

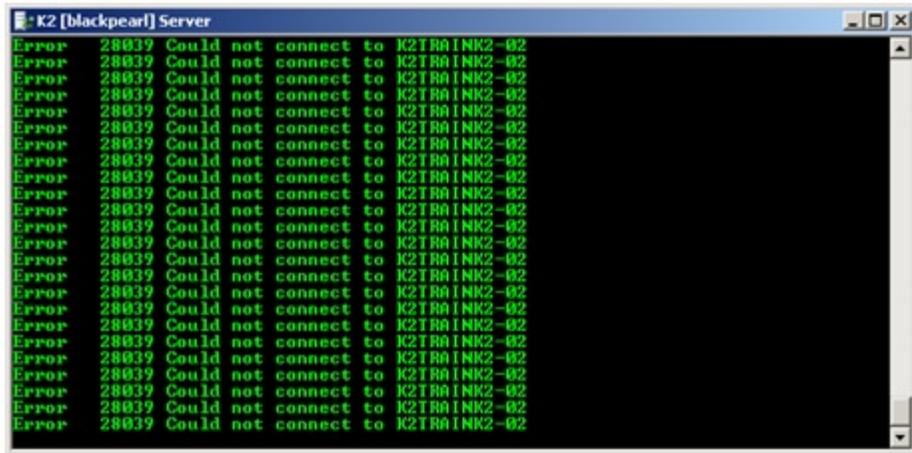
Solution:

Log on to the particular machine and ensure that the Startup and Common Startup folders exists when running VisualStudio as another user.

1.9.4 K2 Server

1.9.4.1 Connection Errors with Unicast NLB

You may have noticed that in the K2 blackpearl Server console window there are some periodic connection errors displayed, as shown below. The problem is that for nodes in Unicast NLB environments, the Network Interface cards (NIC) are allocated and they cannot ping other nodes. You can verify this by pinging one NLB node from the other. This is a problem for a clustered K2 Host Server as all the nodes in a cluster need to be informed if any updates occur (for example, a new process version has been deployed). The usual workaround for this would be to add an additional NIC for the nodes to accommodate the "heartbeat," but this is not always possible.



To work around this, we can enable the heartbeat by a registry entry. Do the following steps on each node in your NLB cluster:

1. Open the Registry Editor (Start > Run > regedit)
 2. Navigate to the following node:

HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > WLBS > Parameters > Interface > {GUID}

Note: The {GUID} placeholder represents the unique identifier of the particular NLB instance. You can also use the ClusterIPAddress subkey in this hive to identify different NLB clusters.

3. Right-click on the {GUID} item and Create a new DWORD entry with the following properties:

Value Name: UnicastInterHostCommSupport
Value: 1

4. Close the Registry Editor
 5. Open a command prompt (Start > Run > cmd)
 6. Type in NLB RELOAD and hit Enter

You should now be able to ping the machines again. You should find that the ping now gets a response, and that the connection errors should disappear from the K2 blackpearl Server console window.

1.9.4.2 Enable K2 Logging

On the K2 Server, you can enable detailed logging options to help with debugging. To turn on the detailed logging, follow the below steps:

1. Open **%programfiles%\k2 blackpearl\Host Server\Bin\HostServerLogging.config** with a text editor
2. Change


```
<add key="IncludeStackTrace" value="False" />
to
<add key="IncludeStackTrace" value="True" />
```
3. Change


```
<LogLocation Name="ConsoleExtension" Active="True" LogLevel="Info" />
to
<LogLocation Name="ConsoleExtension" Active="True" LogLevel="Debug" />
```
4. Change


```
<LogLocation Name="FileExtension" Active="False" LogLevel="All" />
to
<LogLocation Name="FileExtension" Active="True" LogLevel="All" />
```
5. Save your changes to the config file

The K2 Service will need to be restarted in order for this change to take affect. You can see the detailed logging by running the K2 Server in console mode.

To run in console mode, perform the following steps:

1. Open the **Services** manager (Start > All Programs > Administrative Tools > Services)
2. Scroll down to the **K2 blackpearl Server** service, select it and click the **Stop Service** button
3. Once the service shows as stopped, you can close the Services manager
4. Right-click on the **K2 blackpearl Server** item in the Start menu (under Start > All Programs > K2 blackpearl) and select **Run as...**
5. Select **The following user** option, and type in the domain\K2 Service Account as the User Name and password, and click OK

1.9.4.3 K2 Service will not start

Error

The K2 Service does not start after the server reboots.

Causes

Log on Failure, the account does not have the correct permissions to log on as a service.

Resolution

Edit the permissions and enable the permission "Log on as a service" to the service account. See the [Configure Log on as a Service Rights](#) topic for more information.

If the K2 Server is a node in a cluster, check that the service is running under the same service account on all nodes in the cluster, and that the above permission has been enabled on all nodes.

If the above steps have been followed and the user right appears to be removed, a Group Policy Object (GPO) associated with this server might be removing the right. Check with the Domain Administrator to find out if this is happening.

1.9.5 K2 Studio

1.9.5.1 Drop-down List Box Options not visible

Troubleshooting - Drop-down List Box Options not visible

In certain instances the drop-down list box options in K2 Studio screens are displayed behind the main window. The drop-down list is unable to be displayed correctly and no values can be selected. In some cases no options will be displayed, but in some instances only a few options are displayed behind the main window.

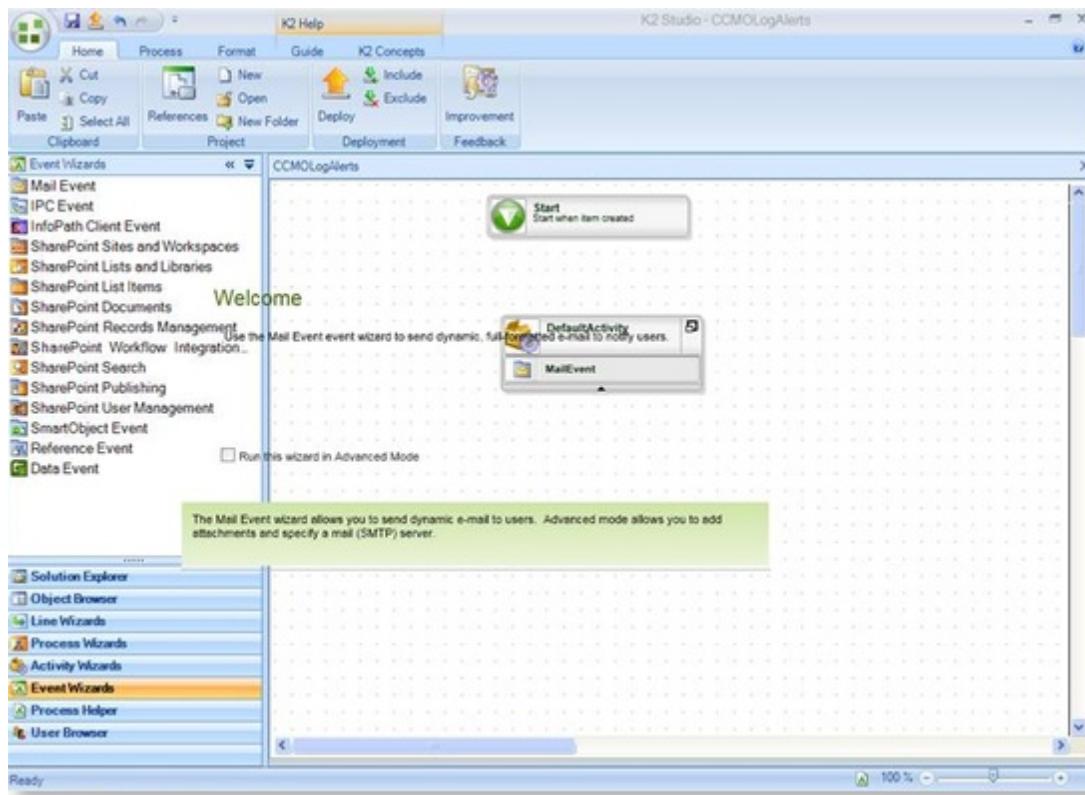
Solution:

This error occurs due to Win32k.sys driver displaying the order of layered windows incorrectly. For a work around see <http://help.k2.com/en/KB000251.aspx>

1.9.5.2 K2 Studio - Wizard Rendering Issue

K2 Studio - Wizard rendering issue

In some instances the wizards are not rendered correctly in K2 Studio when working on a virtual pc, as displayed in the following image:



Solution:

To rectify this problem disable 3D acceleration in the VMWare workstation.

- 1
- 2
- 3
- 4
- 5

- Shutdown the Virtual Machine
- Open the settings for the Virtual Machine.
- Navigate to Display.
- Under **3D Graphics**, unselect the Accelerate 3D graphics option.
- Restart the Virtual Machine.

1.9.6 Performance

1.9.6.1 Slow startup for K2 components when machine has no internet access

Slow startup for K2 components when the machine has no internet access

Issues:

1. Some start performance issues can be experienced when the machine does not have internet access, for example, a virtual machine configured to have "local" network settings. This causes a number of components to startup slowly such as K2Setup, K2HostServer or K2 Designer for Visual Studio.
2. Custom Web Services that use any of the client assemblies such as the SourceCode.SmartObjects.Client assembly might experience time outs after an App-Pool recycle.

Cause:

The K2 Client.dlls are signed with an Authenticode certificate for Windows 7 Certification. By Default the CLR performs a publisher verification on Authenticode signed assemblies, via the Internet and therefore on a machine with no internet it eventually times out on the connection and continues.

Resolution:

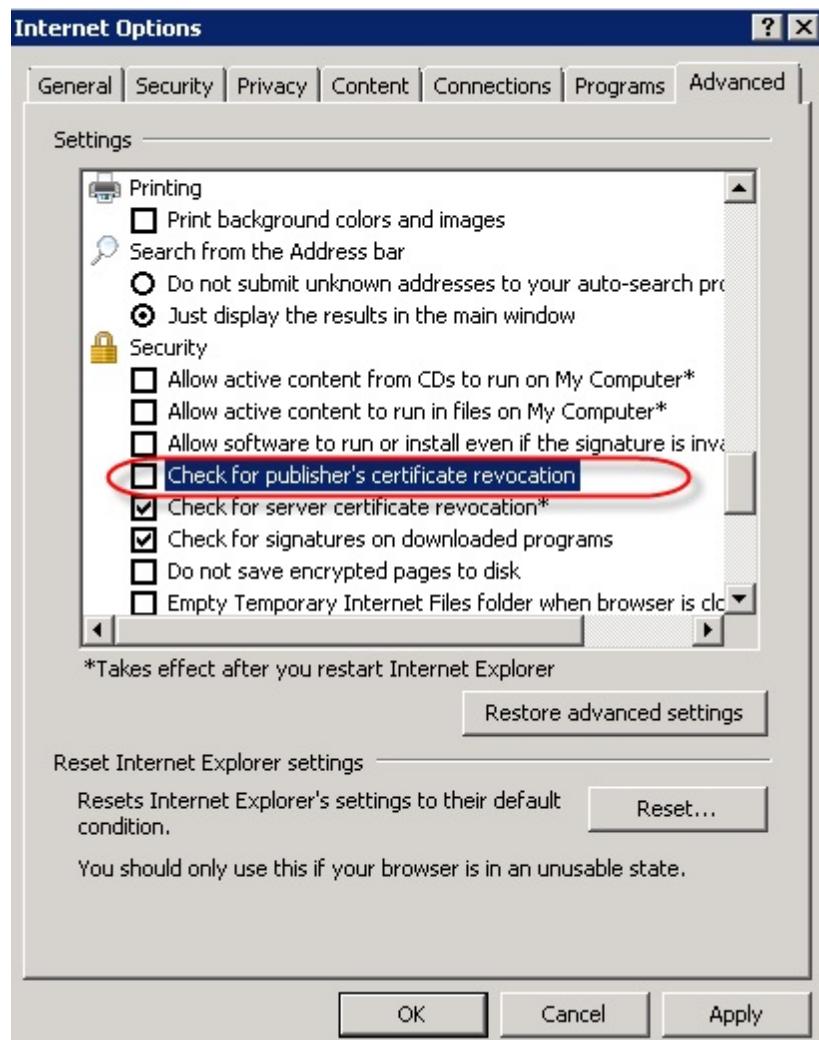
1. Disable publisher verification for the K2 Setup and K2 Host Server by modifying the "Machine.Config" on the relevant servers, or for asp.net the "aspnet.config" in the .NET Framework dir. as follows:



Copy

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

2. K2 Designers that startup slowly with no internet access also need the publisher verification disabled in Internet Explorer. Uncheck the "Check for publisher's certificate revocation" setting in the Internet Explorer options.



1.9.7 K2 Workspace

1.9.7.1 K2 Workspace - Invalid Packet Header Error

Troubleshooting - K2 Workspace Invalid Packet Header Error

The following **Invalid Packet Header Received** error will be displayed when running SharePoint Central Administration on port 5555 which conflicts with the K2 blackpearl Host Server Port 5555.



1.9.7.2 K2 Workspace - Report Error

Troubleshooting - K2 Workspace Report Error

While trying to view a report within K2 Workspace the following error is displayed:

An error has occurred during report processing.

Query execution failed for data set ''.

Server Exception: Requested registry access is not allowed.

Requested registry access is not allowed.

This error is displayed when the user trying to view the Reports does not have the necessary rights to modify or write to the log files.

Solution:

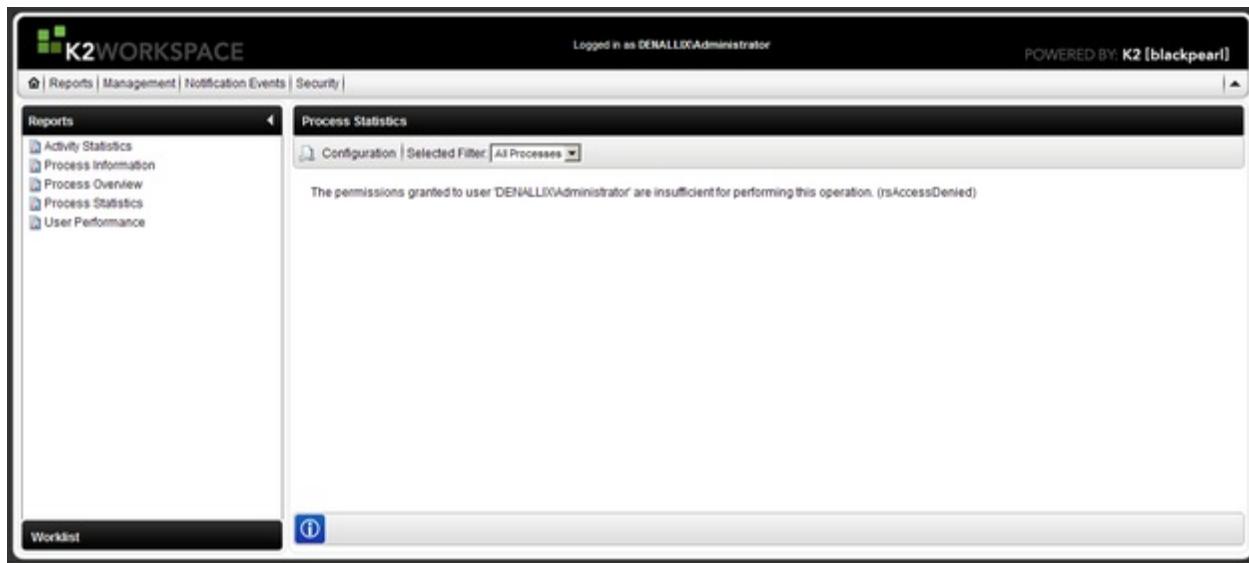
Perform the following steps to rectify the problem:

-  1 Navigate to **C:\Program Files\K2 blackpearl\ServiceBroker\logs**
-  2 Open the Sharing and Security for the log folder
-  3 Open Security
-  4 Go to Authenticated Users, and check the check box to modify the settings to assign the correct rights to the relevant user

1.9.7.3 K2 Workspace - Report Rights Error

Troubleshooting - K2 Workspace Report Insufficient Rights Error

While trying to view a report within K2 Workspace the following error is displayed:



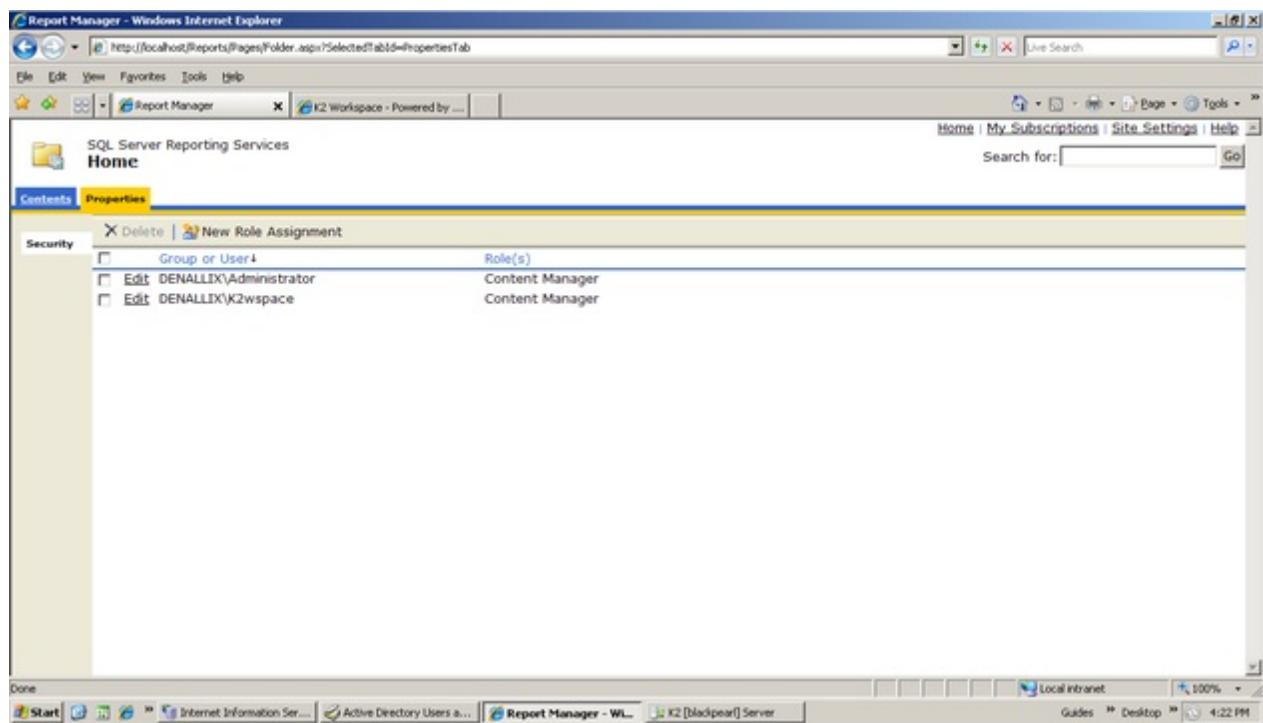
The permission granted to user ... are insufficient for performing the operation. (rsAccessDenied)

This error is displayed due to current user not having sufficient rights in SQL Server Reporting Services.

Solution:

Perform the following steps to rectify the problem:

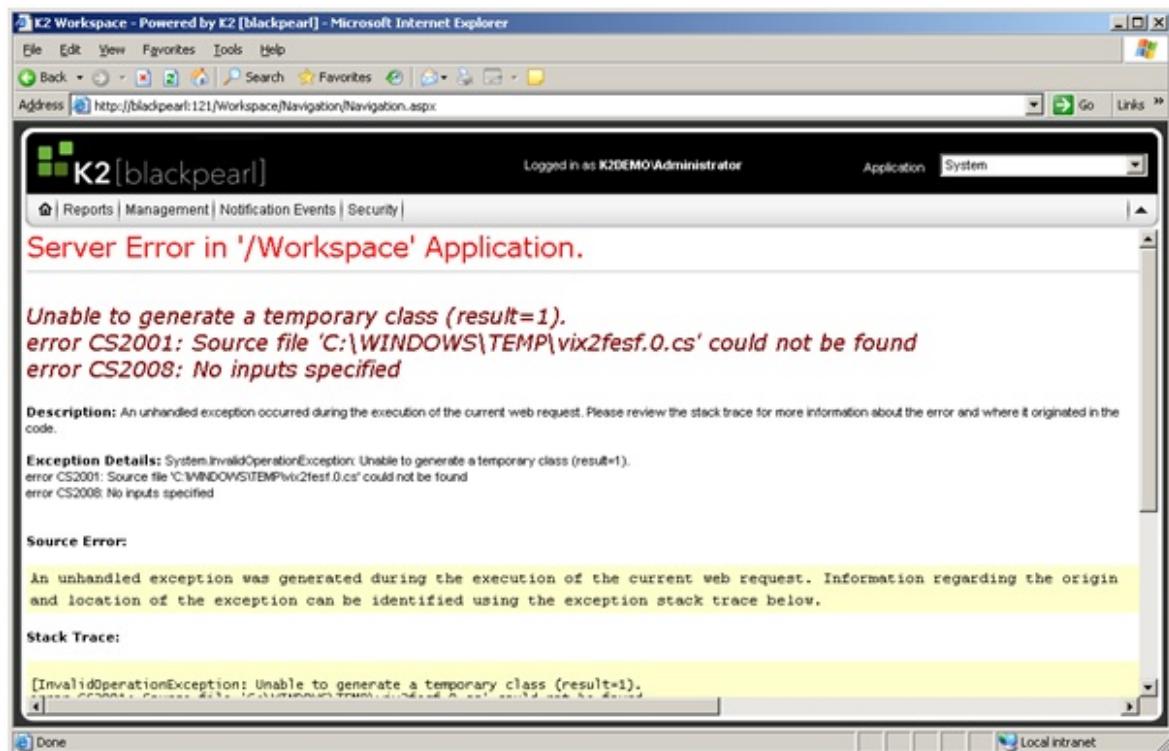
- 1 Navigate to **SQL Server Reporting Services**
- 2 Click on the Properties Tab
- 3 Add the user and provide the necessary rights



1.9.7.4 K2 Workspace - User with Insufficient Permissions

Troubleshooting K2 Workspace Temporary Permissions Error

The following errors might be displayed when working with K2 Workspace:

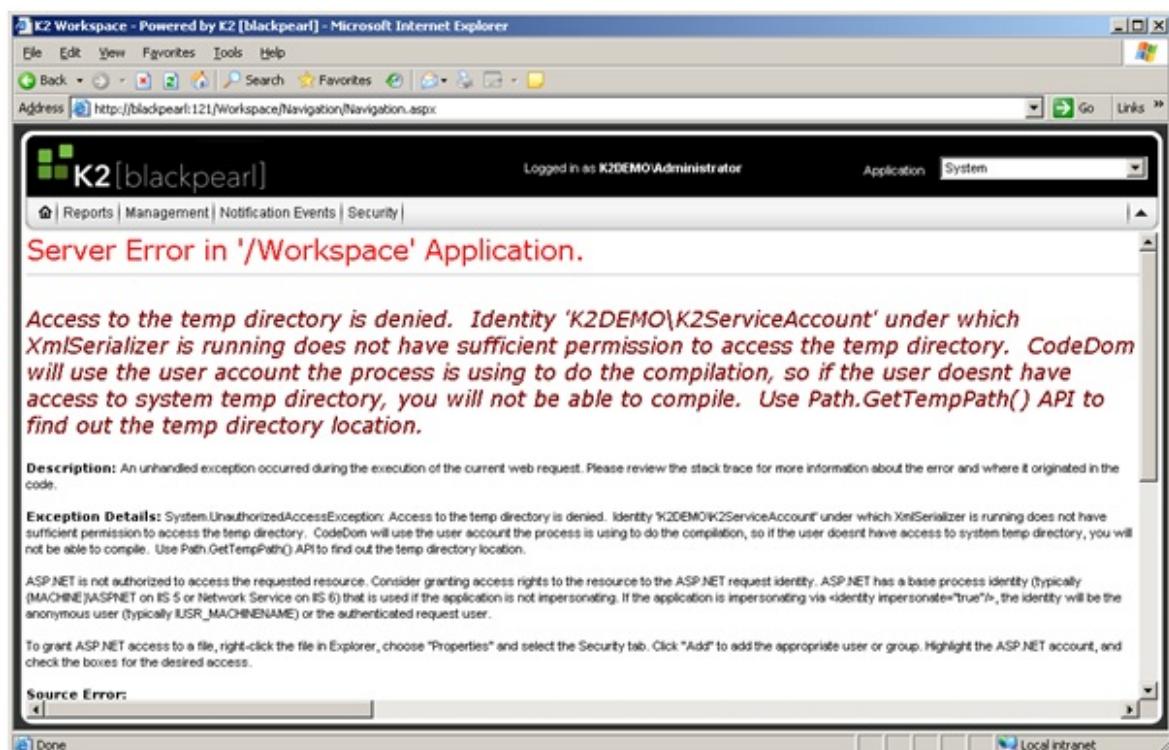


This is due to temporary files being created for the first time that K2 Workspace is used (this is native to ASP.NET). The error occurs when K2 Workspace is running under a user who does not have sufficient permissions on **C:\Windows\Temp**

If only the following permissions are assigned to **C:\Windows\Temp**:

- Read & Execute
- List Folder Contents
- Read

The following error will be returned:



Solution:

Provide all **Authenticated Users** the following **C:\Windows\Temp** permissions:

- Read & Execute
- List Folder Contents
- Read
- Write

1.9.8 Reporting Services

1.9.8.1 Configuration file changes for the K2 for Reporting Services component

If you are encountering issues with the Reporting Services component, validate that the following configuration changes were made to the appropriate files, located in the below folder:

C:\Program Files\Microsoft SQL Server\MSSQL.1\Reporting Services\ReportServer



In the location above, note that the MSSQL.1 directory depends on your specific environment. Your folder may differ depending on where Reporting Services was installed.

rsreportserver.config file:



```
<Configuration>
  <Extensions>
    <Data>
      <Extension Name="SOURCECODE"
        Type="SourceCode.Data.SmartObjectsClient.SOConnection,
        SourceCode.Data.SmartObjectsClient,
        Version=4.0.0.0,Culture=neutral,
        PublicKeyToken=16a2c5aaaa1b130d"/>
    </Data>
  </Extensions>
</Configuration>
```

rssrvpolicy.config file:



```
<CodeGroup class="UnionCodeGroup" version=""
  Name="CustomDataExtensionCodeGroup" Description="Code group for the Custom
  Data Extension" PermissionSetName="FullTrust">
  <IMembershipCondition class="UrlMembershipCondition" version="1"
    Url="C:\Program Files\Microsoft SQL Server\MSSQL.1
    \ReportingServices\ReportServer\bin\SourceCode.Data.SmartObjectsClient.dll"/>
</CodeGroup>
```

1.9.8.2 Troubleshooting 401 error with Reporting Services

Error description:

- When preparing to install or configure K2 for Reporting Services, you receive a 401 error when you try to connect to the Reporting Services web site on the K2 for Reporting Services screen in the Setup Manager.
- You still receive the same 401 error no matter what changes you make to permissions or even use different user accounts.

Solution

1. Start a command prompt.
2. Locate and then change to the directory that contains the Adsutil.vbs file. By default, this directory is C:\Inetpub\Adminscripts.
3. Type the following command, and then press ENTER:
cscript adsutil.vbs set w3svc/NTAuthenticationProviders "NTLM"
4. To verify that the NtAuthenticationProviders metabase property is set to NTLM, type the following command, and then press ENTER:
cscript adsutil.vbs get w3svc/NTAuthenticationProviders

The following text should be returned:

```
NTAuthenticationProviders      : (STRING) "NTLM"
```

1.9.8.3 Troubleshooting Access Issues with K2 Reports

If the K2 for Reporting Services component is installed on a different server than the K2 Workspace, there are multiple hops for authentication, and therefore the reports will not display. Therefore, you need to set up the SPNs for the Reporting Services Service Account.

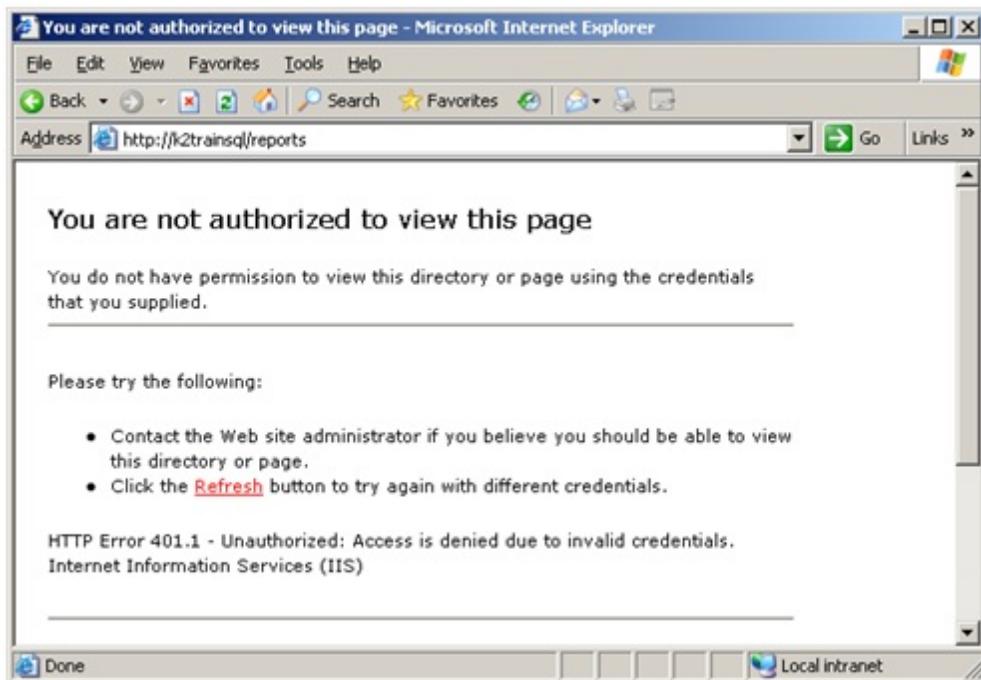
Common Symptoms

This issue can manifest in several ways:

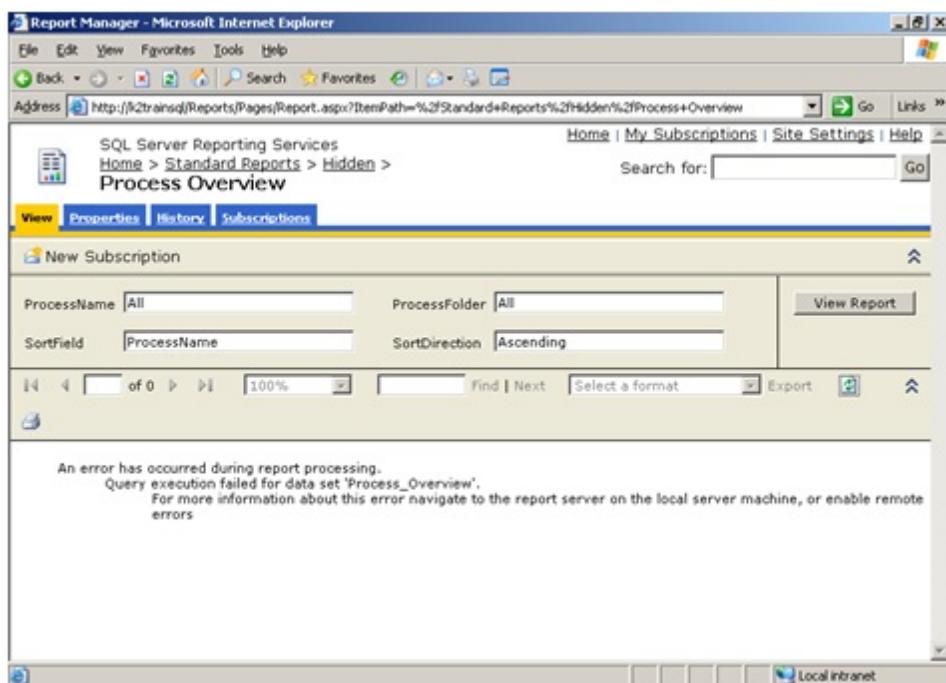
- When accessing the Reporting Services home page from a separate machine, you may be prompted for your credentials. This dialog will appear three times, even if you enter your user name and password correctly:



- After failing three times, a 401.1 "You are not authorized to view this page" error will display, as shown below:



- Alternatively, you may successfully open the Reporting Services Home page, but the report will not render. This is because no identity is passed through, causing an authentication error:



4. This error can also be seen in the K2 blackpearl Server console window, with an Authentication required message, as shown below:

The screenshot shows a command-line interface window titled "K2 [blackpearl] Server". The console output is as follows:

```

Info 10010 SmartObject Object Factory initialized with cache time of 0
Info 10019 SmartObject Runtime Server successfully initialized and running.
Info 7003 SourceCode.SmartObjects.Runtime.SmartObjectClientServer not yet loaded..
Info 7004 All Dependencies Loaded
Info 7021 Assembly Execution Path successfully updated
Info 7023 Loading Event Bus Server
Info 7005 Configuration settings initialized
Info 7032 Initialization Check Successfull
Info 7013 Service registered with ID:4 running on machine: K2TRAINK2-01
Info 7022 Event Bus Server Loaded Successfully
Info 7010 MSMQ Thread Listing
Info 1020 Starting Session B57052F7C7E8F0856226AA3AD827FB84
Info 10514 Name: 'SourceCode.SmartObjects.Runtime' Version: '4.7285.1.0' Date: '11/12/2007 8:32:10 AM'
Error 2025 Error Marshalling SourceCode.SmartObjects.Runtime.SmartObjectClientServer.GetSmartObject, Authentication required for session B57052F7C7E8F0856226AA3AD827FB84
Error 2025 Error Marshalling SourceCode.SmartObjects.Runtime.SmartObjectClientServer.GetSmartObject, Authentication required for session B57052F7C7E8F0856226AA3AD827FB84
Error 8060 ProcessPacket Error, Authentication required for session B57052F7C7E8F0856226AA3AD827FB84
Info 1025 Ending Session B57052F7C7E8F0856226AA3AD827FB84

```

Resolution

Ensure that the proper SPNs were set for the Reporting Services Service Account

1.9.8.4 Validating the SQL Business Intelligence Development Studio

If you are encountering issues when designing custom reports using the SQL Business Intelligence Development Studio on top of Microsoft Visual Studio, check the following configuration file:



If you have installed K2 for Visual Studio before you installed SQL Business Intelligence Development Studio, just re-run the K2 Configuration Manager to update your Visual Studio environment with the below config section.

The installer will update the following assembly *SourceCode.Data.SmartObjectsClient.dll* at the location: C:\Program Files\Microsoft Visual Studio 8\Common7\IDE\PrivateAssemblies In the RSReportDesigner.config file, the following section is added:



```
<Configuration>
  <Extensions>
    <Data>
      <Extension Name="SOURCECODE"
Type="SourceCode.Data.SmartObjectsClient.SOConnection,SourceCode.Data.SmartObjectsClient, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=16A2C5AAAA1B130D"/>
    </Data>
    <Designer>
      <Extension Name="SOURCECODE"
Type="Microsoft.ReportingServices.QueryDesigners.GenericQueryDesigner,Microsoft.ReportingServices.QueryDesigners"/>
    </Designer>
  </Extensions>
</Configuration>
```

1.9.8.5 View Flow - Report does not display

View Flow - Report does not display

The View Flow Report does not display when the report page is refreshed. This is due to dynamic compression being activated in Internet Information Services (IIS)7.

Solution:

Disable Dynamic Compression in Internet Information Services (IIS) 7.

1.9.9 Kerberos

1.9.9.1 Enabling Kerberos Logging



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Kerberos Logging can be very helpful in diagnosing Kerberos authentication issues. In order to enable logging for Kerberos, you will edit the registry settings. Modifying the registry should be done carefully, so please double check the settings below and follow the steps carefully:

1. On the server you wish to enable Kerberos logging, open the **Registry Editor** (Start > Run > regedit)
2. Navigate to the following node:
HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Lsa > Kerberos > Parameters
3. Right-click on the **Parameters** item and **Create** a new **DWORD** entry with the following properties:

Name: LogLevel
Value: 1

Note: If the LogLevel parameter already exists, change the value to 1

4. Close the Registry Editor
5. You will need to restart the server in order for this change to take effect

Kerberos Logging will display errors and notifications in the System Event log. It is a good idea to clear the Events in the System event log so that new errors and warnings are easier to see.

1.9.9.2 Troubleshooting Kerberos Issues



Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

If you are experiencing Kerberos issues, use the following checklist to look for issues:

1. Run ldifde.exe on the domain controller to get a list of all the SPNs that has been set up in the environment.
 - This is a command line tool and can be found in the system folder
 - Command to run: ldfide -d "CN=Users,DC=[DomainNETBIOSname]" -l servicePrincipalName -F c:\SPNoutput.txt
 - Replace [DomainNETBIOSname] with your Domain NetBIOS name
 - This should give you a full list of all SPNs that exist on the domain
 - Repeat for as many Domains as are in your environment
2. Run the following commands on each IIS server where you have K2 Workspace, SharePoint, and SQL Server Reporting Services installed:
 - cscript C:\Inetpub\Adminscripts\adsutil.vbs get w3svc/NTAuthenticationProviders
 - cscript C:\Inetpub\Adminscripts\adsutil.vbs get w3svc/[SiteID]/NTAuthenticationProviders
 - Replace [SiteID] with each of the site Identifiers for:
 - The K2 Workspace site
 - The Reporting Services site
 - The SharePoint site
3. Check delegation in Active Directory on each of the service accounts:
 - domain\K2 Service Account
 - domain\K2 Workspace Service Account
 - domain\SharePoint Service Account
 - domain\SQL Server Account
 - domain\Reporting Services Service Account
4. Check that DTC has been setup correctly on the K2 Server, SQL Server, Reporting Services Server, SharePoint Server, and K2 Workspace Server
5. Check MSMQ on the K2 Server
6. Check that the NIC used in NLB is not listed in DNS. Only the NLB IP address and the IP address of the NIC not used in NLB must be visible in DNS.

1.9.9.3 Using KerbTray to Troubleshoot Kerberos Tickets

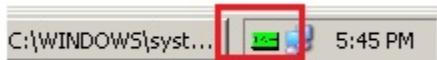


Configuring Kerberos is an advanced task and should only be performed by an appropriately trained professional. The steps and configurations given in this help file are to be used as a guide - your system may require additional configuration due to different hardware and software compatibilities.

Occasionally the existing Kerberos tickets are used when trying to delegate and thus cause delegation to fail. You can force renewal of the Kerberos tickets by using a tool called KerbTray which is part of the [Windows Server 2003 Resource Kit](#).

To use KerbTray:

1. On the K2 server, open KerbTray (double-click on kerbtray.exe)
2. The application will open and an icon will display in the system tray:



3. Right-click on the icon and select **Purge Tickets**
4. Repeat on the second machine (the K2 Workspace server or Reporting Services server, whichever layer you are troubleshooting)
5. Close any open Internet Explorer instances and try accessing the web site again



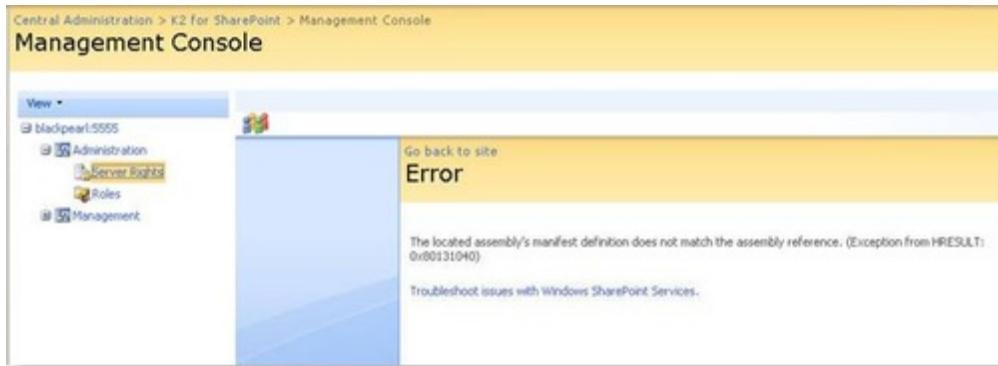
In your environment, you will need to ensure that the SPNs are replicated across all the domain controllers in your domain. Default replication interval for site links is set to 180 minutes (<http://technet2.microsoft.com/windowsserver/en/library/c238f32b-4400-4a0c-b4fb-7b0febefcf731033.mspx?mfr=true>). You can either force the replication using a tool such as KerbTray or change the site link replication interval via the Active Directory Sites and Services console.

1.9.10 SharePoint

1.9.10.1 Assembly Reference Error

Troubleshooting - Assembly Reference Error

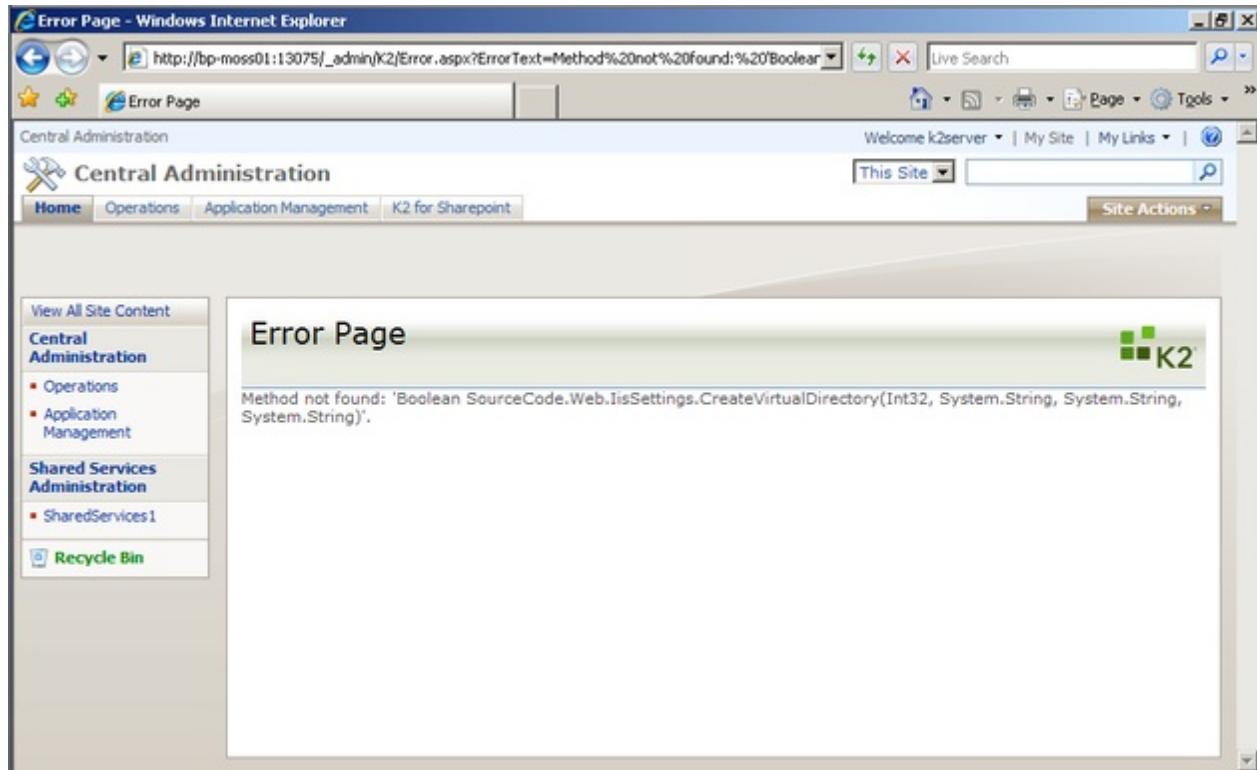
When the following error is displayed in either Management Console or on the Manage Process Portals pages, close all the web browser windows and perform an IIS reset. This should resolve the problem.



1.9.10.2 Method not Found

Troubleshooting - Method Not Found Error

When the following Method Not Found error is displayed you have to reset IIS. This should only occur if the machine was not restarted after the install.



1.9.10.3 Multiple System Accounts - Task actioning

Troubleshooting - Task actioning when there are multiple System Accounts

When installing and working with the K2 for SharePoint components you must provide credentials for several different accounts. Using the incorrect Account may result in errors while using those components. The following links describe the accounts that are used to install, configure, and run the various K2 for SharePoint components:

[K2 for SharePoint - Core](#)

[K2 Designer for SharePoint](#)

[K2 Process Portals](#)

Example: Actioning a task with multiple System Accounts

Consider the following example. User A is a Farm Administrator and has been set as the destination user. User B is a Farm Administrator and has been set as the SharePoint Application Pool Account of the current Web Application. When User A logs in and opens his task he receives an error because the program does not consider him to be the destination user, instead it expects User B to be the destination user.

Problem:

The problem in this case is because the user logging in to Workspace is the SharePoint\System or the Application Pool Account, which SharePoint logs in as SharePoint\System Account automatically. Because both accounts will display as **System account**, SharePoint cannot tell the difference.

Solution:

It is bad practice to use an actual User account as the Application Pool Account, however, a workaround is available in the event where this cannot be prevented.

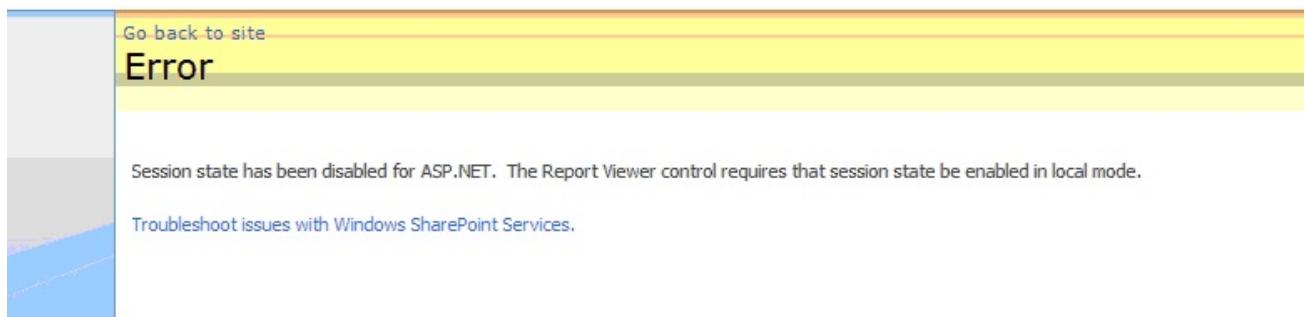
Use the **stsadm** command line utility that ships with SharePoint to run the command **stsadm -o updatefarmcredentials -identitytype NetworkService**.

This will change the identity type to **NetworkService Service Account**. The Application Pool Account will stay the same.

1.9.10.4 Process Portal Report Error

Troubleshooting - Process Portal Report Error

When running reports in the Process Portal, the following error is displayed.



When this error is displayed, perform the following steps to resolve this issue:

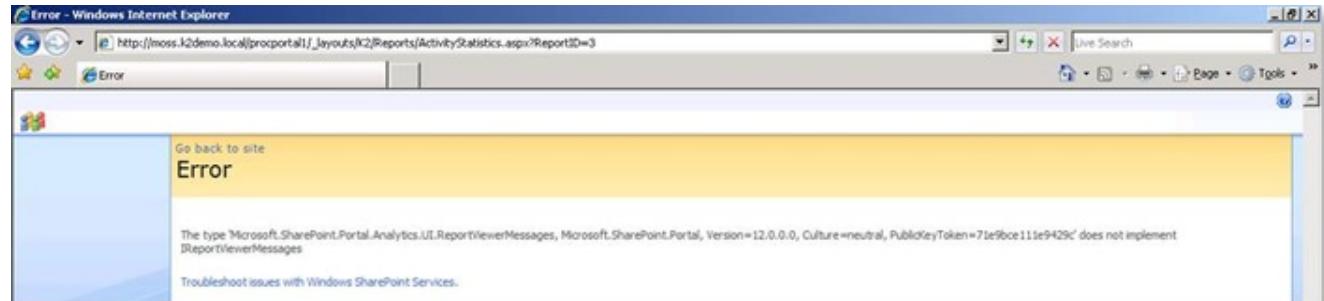
- ① Find the web.config file for SharePoint. This file is typically located in **C:\Inetpub\wwwroot\wss\VirtualDirectories\[portalnameorport]\web.config**
- ② Uncomment the line **<!--<add name="Session" type="System.Web.SessionState.SessionStateModule"/>--!>** by removing the **<!--** and **--!>**
- ③ Ensure that the enableSessionState is set to "true" in the **<pages enableSessionState="true" enableViewState="true" enableViewstateMac="true" validateRequest="false" pageParserFilterType="Microsoft.SharePoint.ApplicationRuntime.SPPageParserFilter, Microsoft.SharePoint, Version=12.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"asyncTimeout="7">** line
- ④ Perform an iisreset

1.9.10.5 Report Error

Troubleshooting - Report Error

When the following Report Error is displayed, you have to look in your SharePoint web.config file, and remove the following:

```
<add key="ReportViewerMessages" value="Microsoft.SharePoint.Portal.Analytics.UI.ReportViewerMessages,
Microsoft.SharePoint.Portal, Version=12.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c" />.
```



1.9.10.6 SharePoint - Attachment icons not displaying

SharePoint - Attachment icons not displaying

The attachment icons do not display correctly in the SharePoint lists. This issue only occurs on sub-sites.

Solution:

Never install the RuntimeServices in the MOSS web site. If this was done, set the web site AppPool back to **SharePoint 80** which will resolve the issue.

1.9.10.7 SharePoint - Document Information Panel unable to load

SharePoint - Document Information Panel unable to load

While trying to open the forms created in the Process Designer through a SharePoint site an error stipulating **The Document Information Panel was unable to load** is displayed.

Solution:

This error can be resolved by disabling the SENS service on the server. To do this open a command prompt and type **net stop sens**

1.9.10.8 SharePoint - SharePoint Central Administration Error

Troubleshooting - SharePoint Central Administration Error

When accessing the SharePoint Central Administration page the following error is displayed:

[Go back to site](#)

Error

```
The resource object with key 'Administration_PageTitle' was not found. at System.Web.Compilation.ResourceExpressionBuilder.ParseExpression
(String expression, Type propertyType, ExpressionBuilderContext context)
at System.Web.UI.BoundPropertyEntry.ParseExpression(ExpressionBuilderContext context)
at System.Web.UI.ControlBuilder.FillUpBoundPropertyEntry(BoundPropertyEntry entry, String name)
at System.Web.UI.ControlBuilder.AddBoundProperty(String filter, String name, String expressionPrefix, String expression, ExpressionBuilder
expressionBuilder, Object parsedExpressionData, Boolean generated, String fieldName, String formatString, Boolean twoWayBound)
at System.Web.UI.ControlBuilder.PreprocessAttribute(String filter, String attribname, String attribvalue, Boolean mainDirectiveMode)
at System.Web.UI.ControlBuilder.PreprocessAttributes(ParsedAttributeCollection attrs)
at System.Web.UI.ControlBuilder.Init(TemplateParser parser, ControlBuilder parentBuilder, Type type, String tagName, String id, IDictionary attrs)

at System.Web.UI.ControlBuilder.CreateBuilderFromType(TemplateParser parser, ControlBuilder parentBuilder, Type type, String tagName, String
id, IDictionary attrs, Int32 line, String sourceFileName)
at System.Web.UI.ControlBuilder.CreateChildBuilder(String filter, String tagName, IDictionary attrs, TemplateParser parser, ControlBuilder
parentBuilder, String id, Int32 line, VirtualPath virtualPath, Type& childType, Boolean defaultProperty)
at System.Web.UI.TemplateParser.ProcessBeginTag(Match match, String inputText)
at System.Web.UI.TemplateParser.ParseStringInternal(String text, Encoding fileEncoding)
```

[Troubleshoot issues with Windows SharePoint Services.](#)

Solution:

Run a `stsadm -o copyappbincontent` command, which will copy the missing files to the correct places.

1.9.10.9 SharePoint - Task Error

SharePoint - Task Error: System.Exemption: Error occurred adding the feature to the farm.

When deploying a process the following error is displayed:

```
1 Error(s)
Task Error: System.Exception: Error occurred adding the feature to the farm. ---> System.Web.Services.Protocols.SoapException:
Server was unable to process request. ---> The EXECUTE permission was denied on the object 'proc_putObject', database
'SharePoint_Config', schema 'dbo'.
   at System.Web.Services.Protocols.SoapHttpClientProtocol.ReadResponse(SoapClientMessage message, WebResponse response,
Stream responseStream, Boolean asyncCall)
   at System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(String methodName, Object[] parameters)
   at SourceCode.SharePoint.WebServices.K2SPFeatures.AddWorkflowFeature(String featureTitle, String description, Boolean
isDefaultForms, K2SPStartForms startForms, K2SPTaskForm[] taskForms, K2SPModificationForm[] modForms)
   at SourceCode.Workflow.SharePoint.Common.Features.AddWorkflowFeature(String featureTitle, Boolean isDefaultForms, String
FeatureDescription, K2SPStartForms startForms, List`1 taskForms, List`1 modForms, CredentialCache CredCache)
   at SourceCode.DeploymentTasks.SharePoint.WorkflowIntegration.ConfigureEvent.AddFeature(IntegrationObject integration)
   at SourceCode.DeploymentTasks.SharePoint.WorkflowIntegration.WorkflowIntegrationService.Execute(IntegrationObject
integration, Boolean testMode, Boolean createDependancies)
--- End of inner exception stack trace ---
   at SourceCode.DeploymentTasks.SharePoint.WorkflowIntegration.WorkflowIntegrationService.Execute(IntegrationObject
integration, Boolean testMode, Boolean createDependancies)
   at SourceCode.DeploymentTasks.SharePoint.WorkflowIntegration.WorkflowIntegrationTask.Execute()
```

0 Warnings(s)

Solution:

Ensure that the K2 Service Account is a SharePoint Farm Administrator.

1.9.10.10 'Unknown Error' on the K2 for SharePoint tab

SharePoint - Unknown Error on the K2 for SharePoint Tab

After installing K2 blackpearl an **Unknown Error** is displayed on the K2 for SharePoint tab within SharePoint. This will occur when the SharePoint admin port was changed after installing SharePoint Server.

Solution:

This error can be resolved by manually copying the file from C:\Program Files\K2 blackpearl\Configuration\AdminResource.resx to the new App_GlobalResources folder.

1.9.10.11 SharePoint - Authentication is required for session error

SharePoint - Authentication is required for session error

When connecting to Central Administration from a client machine to for instance **Activate All K2 Features and K2 Configuration Settings** you may run into an **Authentication is required for session xxx** error caused by the double authentication hop. This means that the Kerberos configuration was not done correctly, but this may be accomplished by checking the follow:

Solution:

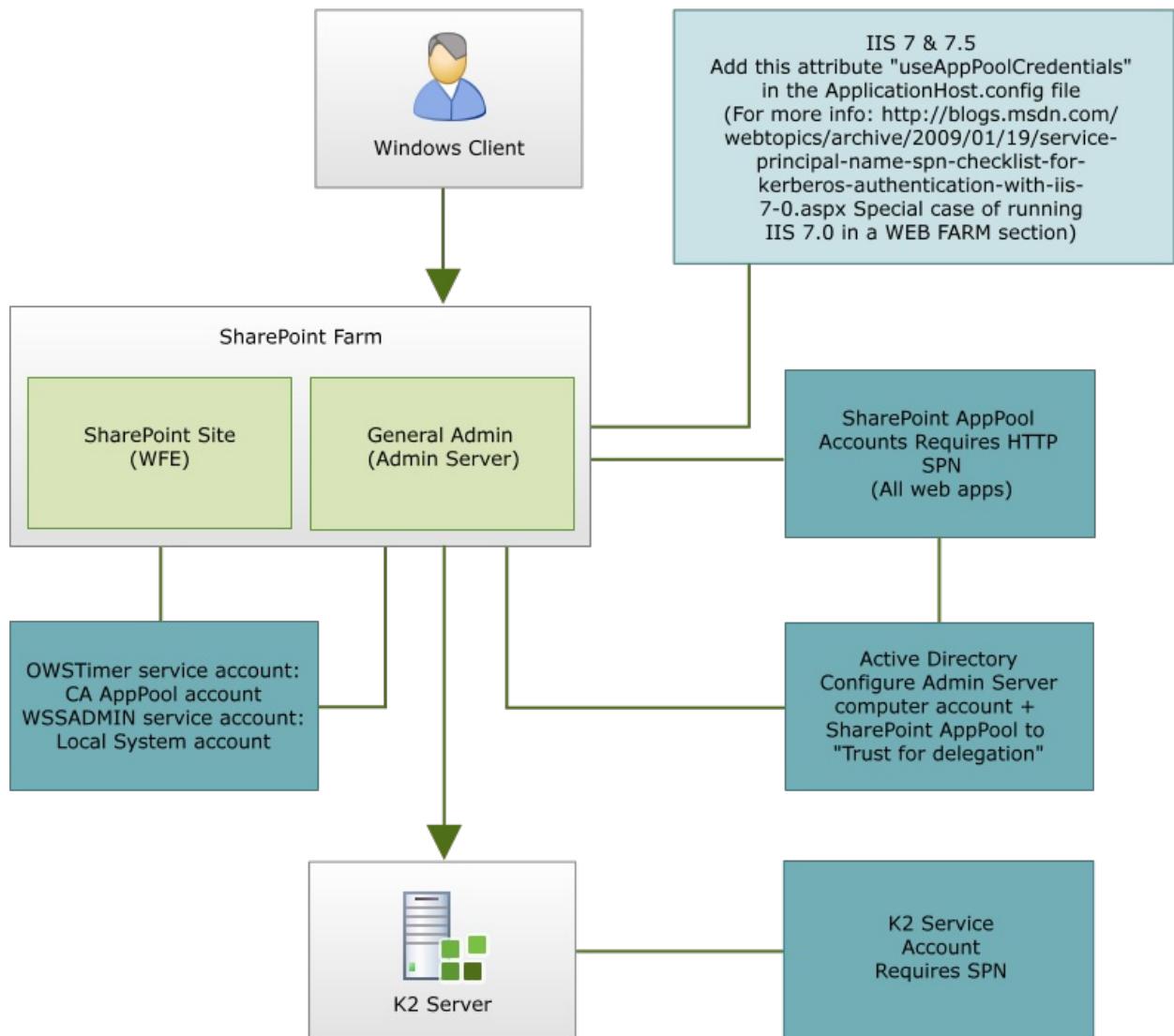
1. **For IIS 7 or IIS 7.5 Only:** Add this attribute **useAppPoolCredentials** in the ApplicationHost.config file. (For more information, click [here](#) and navigate to the **Special case of running IIS 7.0 in a WEB FARM** section)
2. Add HTTP SPN for Central Admin application pool account – for NetBIOS and FQDN
3. In Active Directory:
 - a. Configure the Admin Server computer account to **Trust this computer for delegation to any service (Kerberos only)**;
 - b. Configure the Central Admin application pool account to **Trust this computer for delegation to any service (Kerberos only)**
4. Make sure that the K2 Server service SPN is correctly setup. (This should have been done by the K2 installation if the option was selected.)



Ensure that the Administration and Timer services are running on ALL SharePoint servers (AppServer + WFE's)

- The Timer service account should be setup as the same account as which the central administration application pool is running
- The Administration service account should be set as LocalSystem

See the following diagram as quick reference guide:



1.9.10.12 SharePoint - Solution stays in deployment state

SharePoint - Solution stays in deployment state

After solution deployment in a distributed SharePoint Farm environment, the deployment stays in a deploying state.

Solution:

This is due to the WFE not responding in a timely fashion. To rectify this problem run the following command on each WFE server:

stsadm -o execadmsvcjobs

1.9.10.13 Troubleshooting using SharePoint Logs

A common challenge when troubleshooting SharePoint and Forms Server issues is when the client receives "An error has occurred" message with no additional detail. There is, however, additional error detail logged within the SharePoint logs.

In SharePoint 2007 there is a unified logging system for the various components. Typically, these logs are found on the SharePoint Server under **C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\LOGS** and **C:\Program Files\Microsoft Office Servers\12.0\Logs**.

To make sure that you are logging the appropriate message, check the logging settings in SharePoint Central Administration:

1. Open SharePoint Central Administration
2. Click on the Operations Tab
3. Under Logging and Reporting, click on **Diagnostic Logging**
4. Use the settings on this page to change the logging level on the SharePoint Server

After you have the logging set properly and have errors logged, one trick is to Microsoft Office Excel 2007 to open the logs. If Excel is installed on the server, this makes it easy to open and parse through the logs quickly.

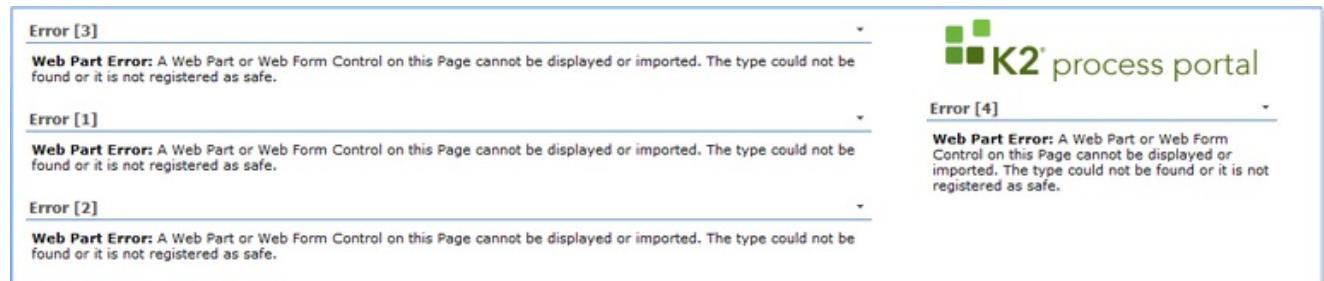
Once you have the logs open, look for items that have "error" in the title or description. From there, look at the errors for configuration settings that can be changed, such as "cross domain support", "timeout", "external datasource". These settings can be changed in the SharePoint Central Administration page for Forms Server.

Changes to settings in Central Administration do not require an IIS Reset, so with a little trial and error you should be able to troubleshoot the SharePoint errors.

1.9.10.14 Web Part Error

Troubleshooting - Web Part Error on main page of MOSS

After activating the K2 components within central administration, a WebPart error is displayed on the main page of MOSS.



The screenshot shows the K2 process portal homepage. At the top right, the K2 logo is visible. Below it, there are four error messages listed under dropdown menus:

- Error [3]**: **Web Part Error:** A Web Part or Web Form Control on this Page cannot be displayed or imported. The type could not be found or it is not registered as safe.
- Error [1]**: **Web Part Error:** A Web Part or Web Form Control on this Page cannot be displayed or imported. The type could not be found or it is not registered as safe.
- Error [2]**: **Web Part Error:** A Web Part or Web Form Control on this Page cannot be displayed or imported. The type could not be found or it is not registered as safe.
- Error [4]**: **Web Part Error:** A Web Part or Web Form Control on this Page cannot be displayed or imported. The type could not be found or it is not registered as safe.

Solution:

This error occurs due to the WebPart solution not being deployed yet. Perform the following steps to deploy the WebPart solution:

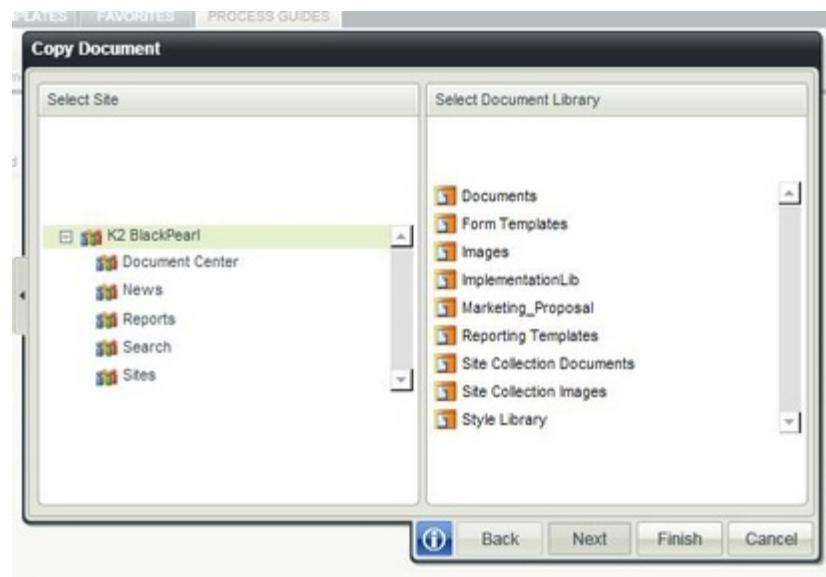
- 1 Open Central Administration
- 2 Click on the **System Settings** option on the left
- 3 Click on **Manage Farm Solutions** in the **Farm Management** section
- 4 Click on **k2processportalwebparts.wsp**
- 5 Click on **Deploy Solution** and click **OK** on the Deploy Solution screen
- 6 Click on **k2worklistwebpart.wsp**
- 7 Click on **Deploy Solution**, select the correct SharePoint Site Collection and click **OK** on the Deploy Solution screen

1.9.11 K2 Designer for SharePoint

1.9.11.1 Copy and Move Document screen rendering issue

K2 Process Designer - Copy and Move Document screen rendering issue

While using the Copy Document and Move Document wizard screens, the wizard screens are not displayed correctly.



Solution:

Select the compatibility view in Internet Explorer 8. This will resolve this issue.

1.9.11.2 E-mail Event rendering issue

K2 Process Designer - E-mail Event rendering issue

When adding a process field through the context browser the high-lighted text continues onto the newly typed text.

Solution:

Select the compatibility view in Internet Explorer 8. This will resolve this issue.

1.9.11.3 Silverlight Designer (Troubleshooting the Silverlight Designer)

Troubleshooting - Silverlight Designer not displaying

If the Silverlight Designer is not displaying, the following checks can be done to troubleshoot the issue:

- Check that the WebDesigner and WebDesigner/EventWeb folders under _Layouts are Virtual Directories
- Check permissions on SQL and that the SharePoint Application Pool identity is db_owner on the K2WebDesigner database
- Add the following in the webdesigner\web.config within the system.web node

```
<sessionState mode="InProc" stateConnectionString="tcpip=127.0.0.1:42424"
partitionResolverType="" sqlConnectionString="data
source=127.0.0.1;Trusted_Connection=yes" cookieless="true" timeout="20"/>
```



Session State is disabled from the SharePoint side and K2 inherits the SharePoint web.config settings because K2's site is a sub virtual directory to the SharePoint site

1.9.12 Smartactions

1.9.12.1 SmartActions fail: mailbox full error

Error

SmartActions fail with the error: Mailbox Full (or similar).

Resolution

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.

1.9.13 SmartObjects

1.9.13.1 Connection not made

SmartObjects - Connection not made

The **K2 Data Source (SmartObjectsClient)** fails to connect, and displays the following message:

No connection could be made because the target machine actively refused it.

Solution:

This is due to the K2 Server which did not start. The following actions can be followed to correct this problem:

- Ensure that the K2 Server has started
- Ensure that the correct Service Account permissions have been applied to the K2 Server Service Account
- The K2 Server license might have expired, contact your Regional Support

1.9.13.2 SmartObjectServer Exception - 401 Unauthorized error

SmartObjectServer Exception - 401 Unauthorized error

The SmartObject Service Instance Synchronization Tool fails and displays the following message:



Solution:

The following actions can be followed to correct this problem:

- Check the IIS logs for the 401 error to see what user is being passed to runtime services
- You might also want to try opening the relevant asmx URL in the browser from the machine you are running the tool. This is just to verify that there are no odd permission or configuration issues. This is usually a cause if there is no Kerberos delegation issues involved (especially for IIS7)

1.9.13.3 SmartObject Exception

SmartObjects - Microsoft Data Transaction Coordinator (MSDTC) Exception

K2 blackpearl is a modular application that can be distributed into independent components. Therefore it is imperative that the failure of one component should not corrupt the operation of other components. Transactions provide us with modular execution and thus can be used to manage failovers and fault handling between all these components. If this is not configured correctly, the SmartObject Server will present this error.

SmartObjectServer Exception: Dependency could not be created: Network access for Distributed Transaction Manager (MSDTC) has been disabled. Please enable DTC for network access in the security configuration for MSDTC using the Component Services Administrative tool.

```
at SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObject(SmartObjectDefinition
smartObjectDefinition, Guid guid, String categoryName)
at SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObject(SmartObjectDefinition
smartObjectDefinition, String categoryName)
at
SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObjectSetLocalFalse(SmartObjectDefi
nition smartObjectDefinition, String category)
at
SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObjectFromLocal(SmartObjectDefiniti
on smartObjectDefinition, String categoryName)
at SourceCode.DeploymentTasks.SmartObjects.SmartObjectDeployTask.PublishObject(SmartObjectDefinition
soDef)
```

Explanation:

To support distributed transaction management between the K2 Host Server and our Databases on the SQL server, MSDTC (Microsoft Data Transaction Coordinator) must be enabled. When working in an environment where the K2 Host Server reside on a different physical machine than the K2 databases the Network DTC must be enabled between these servers.

This error will occur if MSDTC has already been activated on the servers, but the network DTC has not been setup on both the K2 Host server and the SQL cluster. Activate Network DTC on both.

To activate the network DTC please follow the Microsoft guide on activating it in the knowledge base article 817064: **How to enable network DTC access in Windows Server 2003** <http://support.microsoft.com/kb/817064/>

1.9.13.4 SmartObjectServer Exception

Error

If the following error is encountered:

```
SmartObjectServer Exception: Dependency could not be created: Network access for Distributed Transaction Manager (MSDTC) has been disabled. Please enable DTC for network access in the security configuration for MSDTC using the Component Services Administrative tool. at  
SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObject(SmartObjectDefinition smartObjectDefinition, Guid guid, String categoryName) at  
SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObject(SmartObjectDefinition smartObjectDefinition, String categoryName) at  
SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObjectSetLocalFalse(SmartObjectDefinition smartObjectDefinition, String category) at  
SourceCode.SmartObjects.Authoring.SmartObjectAuthoringServer.PublishSmartObjectFromLocal(SmartObjectDefinition smartObjectDefinition, String categoryName) at  
SourceCode.DeploymentTasks.SmartObjects.SmartObjectDeployTask.PublishObject(SmartObjectDefinition soDef)
```

Cause

MSDTC has not been configured properly.

Resolution

K2 blackpearl's modular architecture enables individual components to be distributed onto independent servers or systems. When distributed in this manner; should one component fail, the distributed operation should not prevent or hinder the operation of the distributed components. Transactions are executed per module.

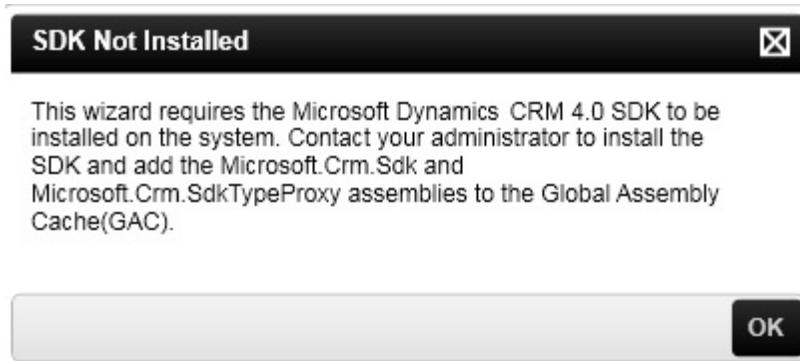
DTC (Distributed Transaction Coordinator) must be enabled to support distribution transaction management between the K2 components. See the [Enable and Configure the DTC Components](#) topic for more information.

1.9.14 Wizards and Rules

1.9.14.1 CRM SDK Error

Error when dragging the CRM wizard onto the design canvas

The following error may be encountered when the CRM wizard is dragged onto the design canvas in K2 Studio or K2 Designer for Visual Studio. When the OK button is clicked the wizard's Welcome screen will be displayed and the user can select NEXT, however, this error will then reappear. The only option is to cancel the wizard.



In K2 Designer for SharePoint the error below will be displayed



Solution

1. Install Microsoft Dynamics CRM 4.0 SDK available at <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=82e632a7-faf9-41e0-8ec1-a2662aae9dfb&displaylang=en> on to the server.
2. Add the Microsoft.Crm.Sdk.Dll and the Microsoft.Crm.SdkTypeProxy.Dll to the Global Assembly Cache (GAC).

1.9.14.2 Destination Rule - Multiple slots created but not executed

Troubleshooting - Multiple slots created but not executed

It is reasonable to expect that if the **Plan per slot (no destinations)** Destination Rule has been selected and **multiple slots** are created, that the activity will only complete once all slots have completed. This, however, is not always the case. An Activity will complete once the first slot has completed, even though the remaining slots will be reflected in reports, but will have an empty status. To prevent the Activity from completing if there is more than one slot, it is important to define additional Succeeding conditions that ensure that the Activity completes only after all slots have completed.

Example: Process with IPC Event

Consider the example of a process that uses a filtered SmartObject Getlist method in the destination rule to asynchronously kick off X number of sub process instances using an IPC Event.

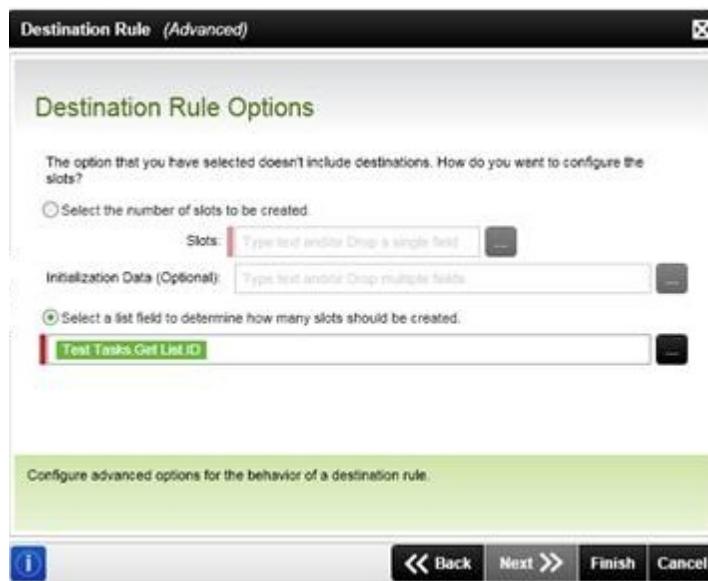


Fig.1. Destination Rule Options - Plan per slot (no destinations)

At first glance it is easy to see that multiple slots can be created with the return of the Getlist method. The Destination Rule has been configured to start the IPC Event asynchronously, which in effect means that the parent process starts the child process and continues down its logical path.

Problem:

As soon as the first slot is complete, the parent process will continue down its logical path, leaving the remaining slots in limbo.

Solution:

Add a Succeeding Rule that checks whether all slots have been completed before continuing with the activity. Below is an example of a Succeeding Rule that checks the statuses of the slots.



Fig.2. Add/Edit Rule Dialog - Succeeding Rule

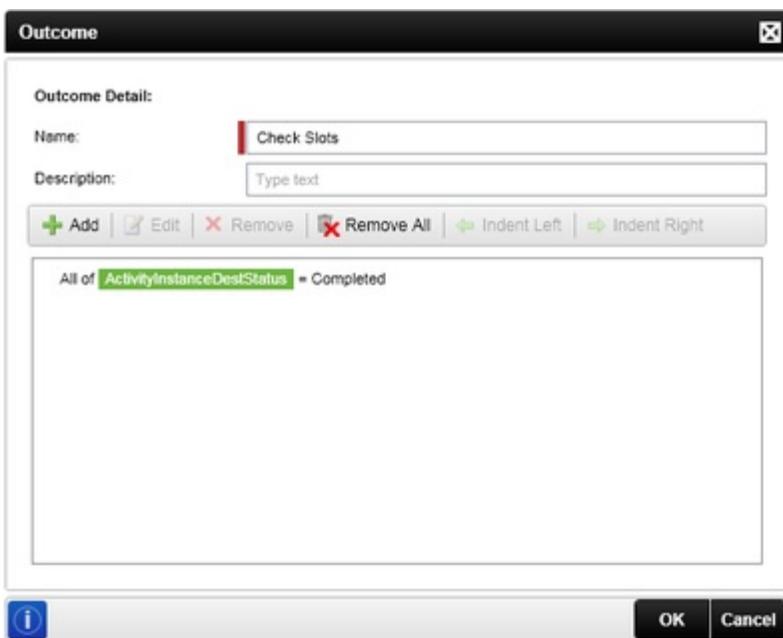
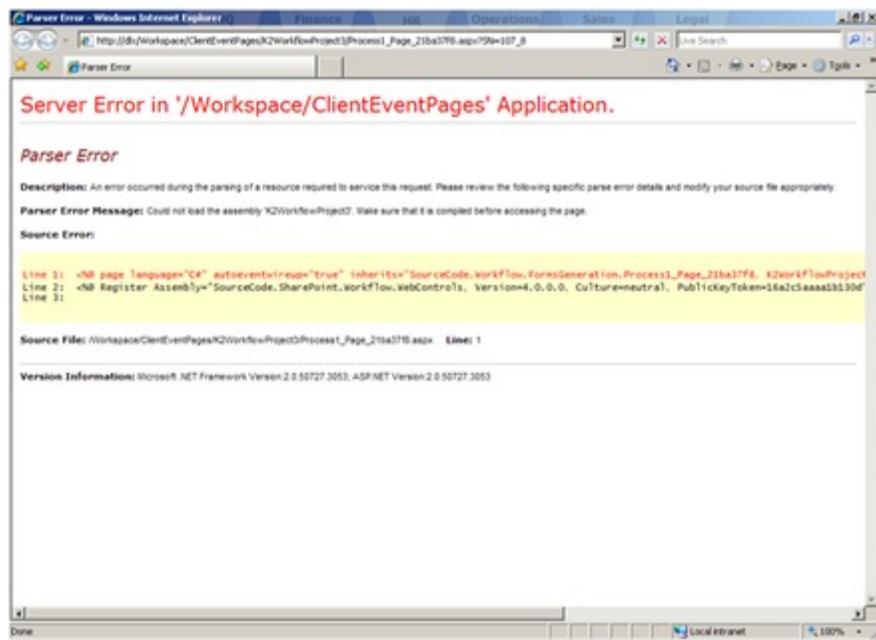


Fig.3. Succeeding Rule

1.9.14.3 Forms Generation - Parser Error

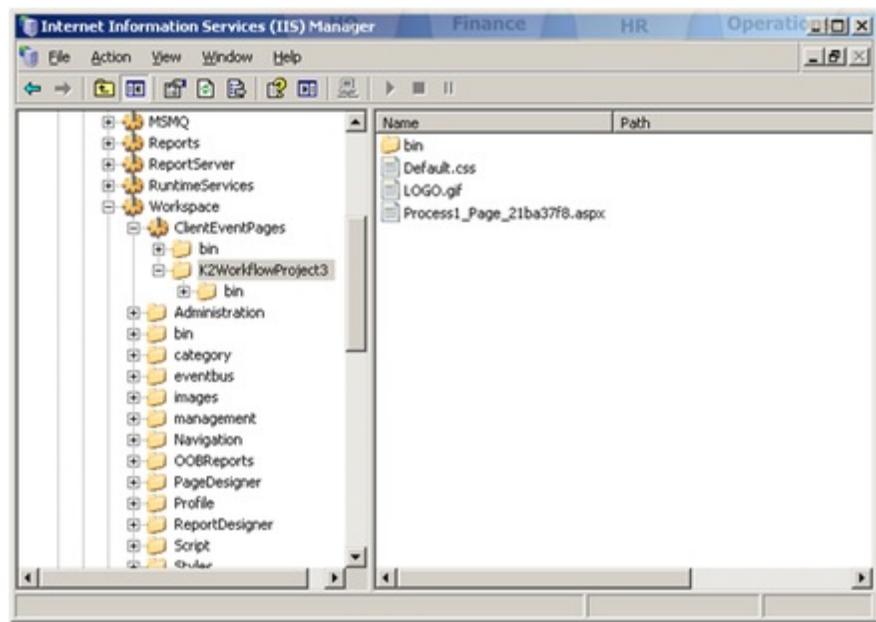
Troubleshooting - Parser Error

Using Host Headers are not supported with Forms Generation in K2 blackpearl. When using Host Headers with Forms Generation will cause the client ASPX page created by the Forms Generation wizard to display the following errors when launched:



Solution:

A developer with administrator rights on the IIS machine where the newly created Forms Generation website is hosted must create a web application out of the newly created Forms Generation virtual directory in IIS.



1.9.14.4 Troubleshooting the Succeeding Rule

Troubleshooting - Succeeding Rule Error

Logically an Activity completes when all tasks/events associated with the Activity have been completed. However, it is easy to assume that the Succeeding Rule will prevent the Process from continuing.



Do not rely on the Process to continue because all events have been completed. Plan the process logic carefully and use a combination of Succeeding Rules and Line Rules to cater for all eventualities

Thus the logic of the Succeeding Rule needs to be interpreted in the context of all completing conditions.

(Activity completes) IF (Defined Succeed Conditions(Activity)=TRUE) OR (All Events Complete(Activity)=TRUE)

Example: Student Admission

Students are admitted to the School of Management based on a Board Review of their application. The approval decision can be either Approved, Declined or Pending.

The Succeeding Rule requires that:

- A minimum of 3 board members Approve the admission
- A minimum of 2 board members Decline the admission
- All the board members must lodge a decision other than Pending for the Approve Application activity to complete

However, the Approve Application activity completes even if a decision of Pending is recorded

Problem:

The All Events Complete criteria of the Succeeding Rule evaluates to TRUE and the Approve Application activity completes, even if some of the board members record the Approval Decision as Pending

Solution:

Option 1: Remove Pending from the options for the Approval Decision

This is a simple solution but may not provide the flexibility required. Be sure to modify the Succeeding Rule.

Option 2: Handle the Pending outcome for the Approval Decision specifically

Understand why the approval decision could be Pending - let us assume that the board feels there is insufficient information in the application. The process could loop back to collect more information. Be sure to check the line rules to cater for all the scenarios.



Recommended Practice

- Always define a Succeeding Rule when there are more destination users than destination slots
- Use Line Rules to direct the flow of the process when there is a destination slot for each destination user

1.9.14.5 Word Document - Error with Word Document Conversion

Error with Word Document Conversion

The following error may be encountered when trying to perform a Word Document Conversion:

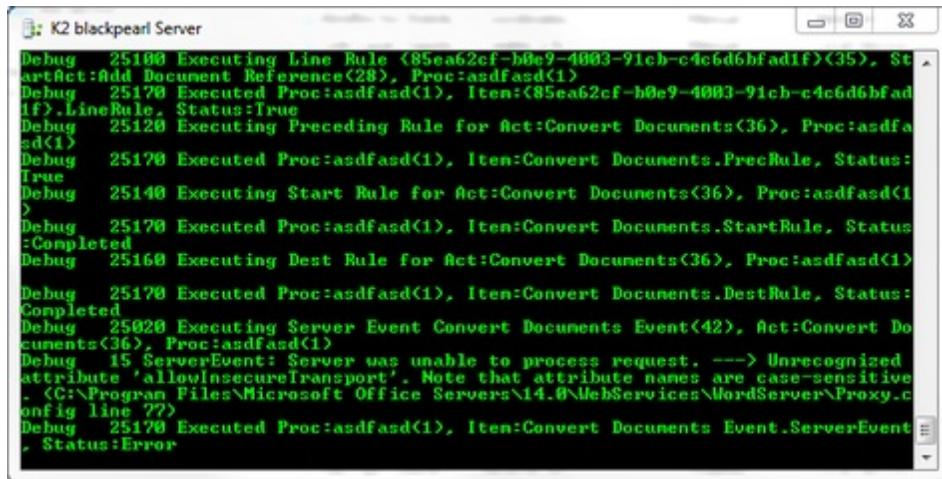
Unrecognized attribute 'allowInsecureTransport'

This issue mostly occurs when SharePoint 2010 is installed on a Windows 7 or Windows Server 2010 R2 machine:

If you encounter this error, installing the following Microsoft patch should resolve the error:

<http://support.microsoft.com/kb/976462>

Example of the Error



```

K2 blackpearl Server
Debug 25100 Executing Line Rule <85ea62cf-b0e9-4003-91cb-c4c6d6bfad1F>(35), St
artAct:Add Document Reference(28), Proc:asdfasd(1)
Debug 25170 Executed Proc:asdfasd(1), Item:<85ea62cf-b0e9-4003-91cb-c4c6d6bfad
1F>.LineRule, Status:True
Debug 25120 Executing Preceding Rule for Act:Convert Documents(36), Proc:asdfa
sd(1)
Debug 25170 Executed Proc:asdfasd(1), Item:Convert Documents.PrefRule, Status:
True
Debug 25140 Executing Start Rule for Act:Convert Documents(36), Proc:asdfasd(1
)
Debug 25170 Executed Proc:asdfasd(1), Item:Convert Documents.StartRule, Status
:Completed
Debug 25160 Executing Dest Rule for Act:Convert Documents(36), Proc:asdfasd(1)
Debug 25170 Executed Proc:asdfasd(1), Item:Convert Documents.DestRule, Status:
Completed
Debug 25020 Executing Server Event Convert Documents Event(42), Act:Convert Do
cuments(36), Proc:asdfasd(1)
Debug 15 ServerEvent: Server was unable to process request. ---> Unrecogniz
ed attribute 'allowInsecureTransport'. Note that attribute names are case-sensi
tive. <C:\Program Files\Microsoft Office Servers\14.0\WebServices\WordServer\Proxy.c
onfig line ???
Debug 25170 Executed Proc:asdfasd(1), Item:Convert Documents Event.ServerEvent
, Status:Error

```

Fig. 1. Example of error

1.9.14.6 Word Document - Troubleshooting Error Codes for Word Document Conversion Issues

Troubleshooting Error Codes for Word Document Conversion Issues

A common challenge when troubleshooting Word Document Conversion issues is when the client receives error code messages with no additional detail. There is, however, additional error detail in the SharePoint Database Server.

To find the matching error message, do the following:

1. On your SharePoint Database Server, find the Word Automation database. If it was created by default, it would be named something like **WordAutomationServices_7a95f9714da6478ca60a03173db67eb6**.
2. Open the **Items** table, look for the relevant item and check the **errorCode** column.
3. Compare the error code to the table below, or follow this link: <http://msdn.microsoft.com/en-us/library/ff512774.aspx>

ConversionItemInfo.ErrorCode Number	ConversionItemInfo.ErrorMessage String	Related Event ID
131174	"The file could not be converted; it may be corrupt or otherwise invalid. Please try opening the file in Microsoft Word, resaving it, and then resubmitting the file for conversion. If this does not resolve the issue, contact your system administrator."	N/A
131173	"There was an internal error with the system. Please contact your system administrator."	N/A
131179	"The file is protected by Information Rights Management (IRM). To convert the file on the server, any IRM protection must be removed in Microsoft Word."	
131181	"The file type is currently blocked by the system administrator."	N/A
131182	"The file type is not supported by Word Automation Services."	N/A
131183	"The 3rd party PDF converter failed. Please contact your system administrator."	8004
131184	"The 3rd party XPS converter failed. Please contact your system administrator."	8005
6	"The file could not be downloaded from the input library due to a technical problem. Please contact your system administrator."	1001
2	"The file could not be downloaded from the SharePoint library because the user's permissions have recently changed. Please contact your system administrator to determine how adequate permissions can be restored."	N/A
3	"The file could not be downloaded from the input library because the supplied user permissions expired before the file could be retrieved. This likely indicates that the system is under heavy load. Please try resubmitting the job, and contact your system administrator if the error reoccurs."	N/A
7	"The file converted successfully, but the output file could not be uploaded to the SharePoint library due to a technical problem. Please contact your system administrator for additional support."	1001
4	"The file converted successfully, but the output file could not be uploaded to the output SharePoint library because the user's permissions have recently changed. Please contact your system administrator to determine how adequate permissions can be restored."	N/A

5	"The file converted successfully, but could not be uploaded to the output library because the supplied user permissions expired before the file could be uploaded. This likely indicates that the system is under heavy load. Please try resubmitting the job, and contact your system administrator if the error reoccurs."	N/A
1	"The input file could not be found in the SharePoint library. Check that the file still exists and resubmit the file for conversion."	N/A
131070	"The conversion failed because of a service configuration problem. Please contact your system administrator."	N/A
65545	"The file could not be converted; it may be corrupt or otherwise invalid (the conversion process stopped responding). Please try opening the file in Microsoft Word, resaving it, and then resubmitting the file for conversion. If this does not resolve the issue, contact your system administrator."	N/A
65543	"The file could not be converted; it may be corrupt or otherwise invalid (the conversion process failed). Please try opening the file in Microsoft Word, resaving it, and then resubmitting the file for conversion. If this does not resolve the issue, contact your system administrator."	N/A
65544	"The file could not be converted; it may be corrupt or otherwise invalid (the conversion process crashed). Please try opening the file in Microsoft Word, resaving it, and then resubmitting the file for conversion. If this does not resolve the issue, contact your system administrator."	N/A
131074	"The conversion failed for unknown reasons. Please contact your system administrator."	N/A
65538	"The conversion failed because of a service configuration problem. Please contact your system administrator."	N/A
131185	"The Word 97-2003 document scan failed when trying to open this file; it may be corrupt or otherwise invalid."	N/A
131186	"This document could not be converted because it contains ActiveX controls. This document must be converted using Microsoft Word."	N/A

1.9.15 Worklist

1.9.15.1 Troubleshooting Activity Slots

Troubleshooting - Activity Does Not Complete

It is reasonable to expect that if all users with allocated work items in their worklists complete their tasks that the activity will complete. This, however, is not always the case. An Activity will not complete when the number of destination users exceeds the number of destination slots. To prevent the Activity remaining permanently active it is important to define additional Succeeding conditions that ensure that the Activity completes.

Example: Project Concept Approval

Consider the example of five managers reviewing a project proposal. The project proposal needs to be:

- Approved by three managers for it to be taken to the next phase (planning)
- Turned down by two manager for it to be shelved

At first glance it is easy to see at least three slots are required to ensure the project can reach approval, and two slots for the project to be declined. Assuming three slots will be enough, consider the case where three managers have opened the item - i.e. all slots have been allocated - and one manager turns the project proposal down:

- The task item remains in two managers worklists - if both approve the proposal - the proposal can not be considered approved or declined, it is in limbo
- There are also two managers still available to review the proposal

Increasing the number of destination slots to four ensures that the stalemate above is resolved. The fourth manager now holds the deciding vote.

So in this scenario *four slots need to be created*.

Problem:

For the *Review Proposal* Activity to complete, without a Succeeding Rule, it requires that all instances complete the associated approving action. In the example above five activity instances are created but only four users will complete the approving action - so the Activity remains in an active state. This will stop the process from continuing.

Solution:

Add a Succeeding Rule that sets the Activity status to complete when:

- Three managers have Approved the project concept, **OR**
- Two managers have Declined the project concept



The particular path taken by the process is determined by the Line Rules defined for the *Approved* and *Declined* line

1.9.15.2 ASP.NET Validation on Start Process Action Property

Troubleshooting - ASP.NET Validation on Start Process Action Property

When starting a process, an Action property is created that is available on the load event. Starting a process from an ASP.NET driven page exposes the Action property through the ASP.NET default page security. If the property is visible on the worklist item and the user selects an action to update it, the update will fail and give a 'Dangerous Request error'.

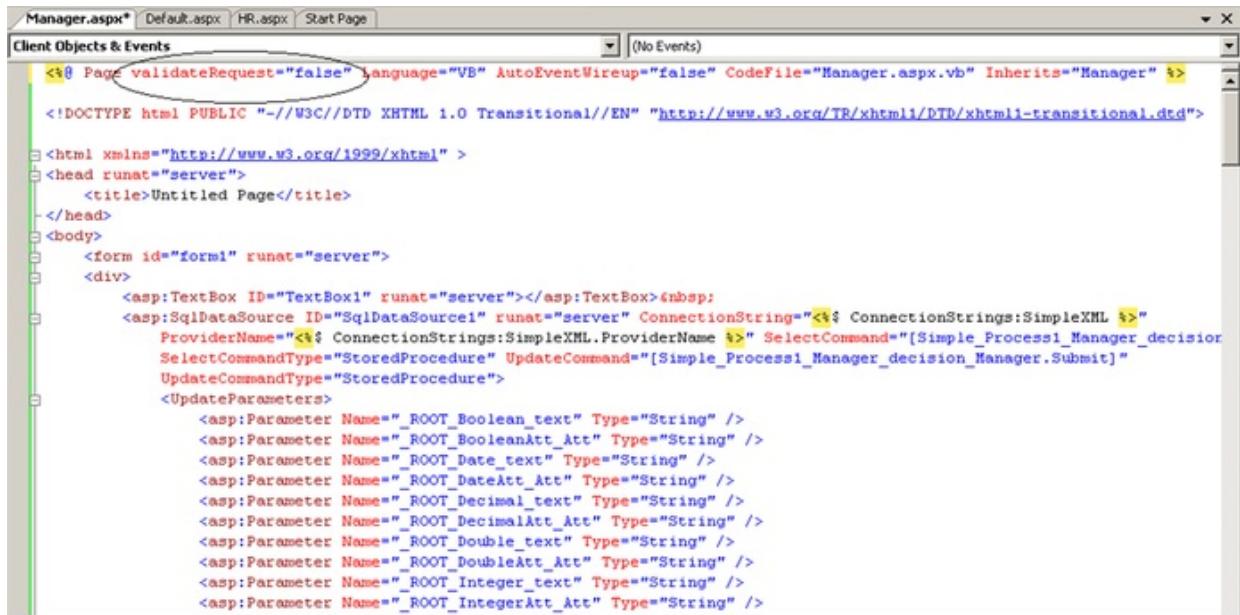
Explanation:

ASP.NET pages have default level protection that requires validation for the load event.

Solution:

There are two ways to avoid this.

- Edit the fields on the DetailsView, delete the field from the form.
- In the ASP.NET pages source code, within the Page property insert: validateRequest="false"



```

<%@ Page validateRequest="false" Language="VB" AutoEventWireup="false" CodeFile="Manager.aspx.vb" Inherits="Manager" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
        <div>
            <asp:TextBox ID="TextBox1" runat="server"></asp:TextBox>&nbsp;
            <asp:SqlDataSource ID="SqlDataSource1" runat="server" ConnectionString="<%$ ConnectionStrings:SimpleXML %>" ProviderName="<%$ ConnectionStrings:SimpleXML.ProviderName %>" SelectCommand="[Simple_Process1_Manager_decision_SelectCommand]" SelectCommandType="StoredProcedure" UpdateCommand="*[Simple_Process1_Manager_decision_Manager.Submit]" UpdateCommandType="StoredProcedure">
                <UpdateParameters>
                    <asp:Parameter Name="_ROOT_Boolean_text" Type="String" />
                    <asp:Parameter Name="_ROOT_BooleanAtt_Att" Type="String" />
                    <asp:Parameter Name="_ROOT_Date_text" Type="String" />
                    <asp:Parameter Name="_ROOT_DateAtt_Att" Type="String" />
                    <asp:Parameter Name="_ROOT_Decimal_text" Type="String" />
                    <asp:Parameter Name="_ROOT_DecimalAtt_Att" Type="String" />
                    <asp:Parameter Name="_ROOT_Double_text" Type="String" />
                    <asp:Parameter Name="_ROOT_DoubleAtt_Att" Type="String" />
                    <asp:Parameter Name="_ROOT_Integer_text" Type="String" />
                    <asp:Parameter Name="_ROOT_IntegerAtt_Att" Type="String" />
                </UpdateParameters>
            </asp:SqlDataSource1>
        </div>
    </form>
</body>

```

1.9.15.3 Error with Forms Generation Client Event

Error with Forms Generation Client Event

The following error may be encountered when trying to open a worklist item that contains a Forms Generation Client Event:

Unable to retrieve K2 Blackpearl data please check connection and that you have rights to the worklist item

This issue mostly occurs when using IIS6 and Web Deployment Projects 2005 on a Windows Server 2003 machine.

Example of the Error

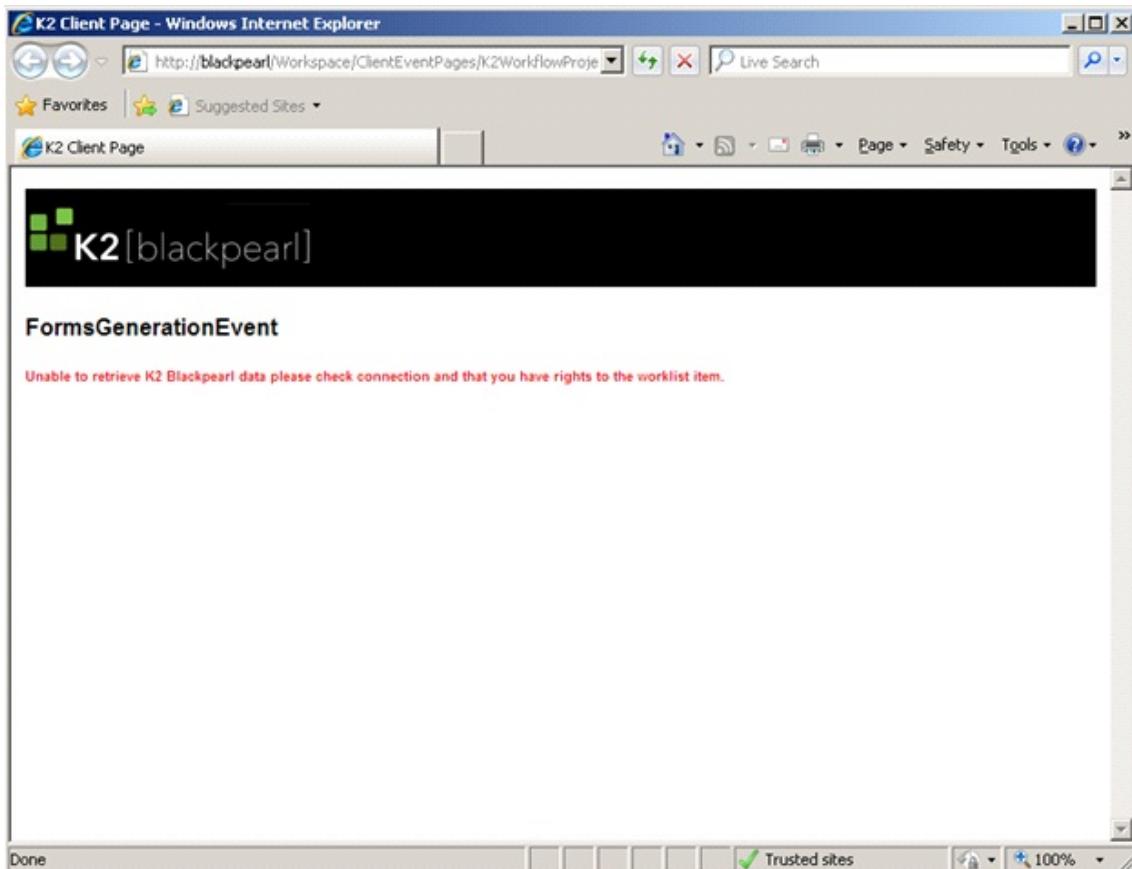


Fig. 1. Example of error

Resolution

If you encounter this error, perform the following steps to resolve the error:

1. Open IIS
2. Open the web site where the K2 Workspace resides
3. Right-click the project and select Properties
4. In the Authentication and access control section, click Edit
5. On the Authentication Methods screen, check that the **Enable anonymous access** is disabled. If it is not disabled, disable it by unselecting the option
6. Click OK and try to open the worklist item

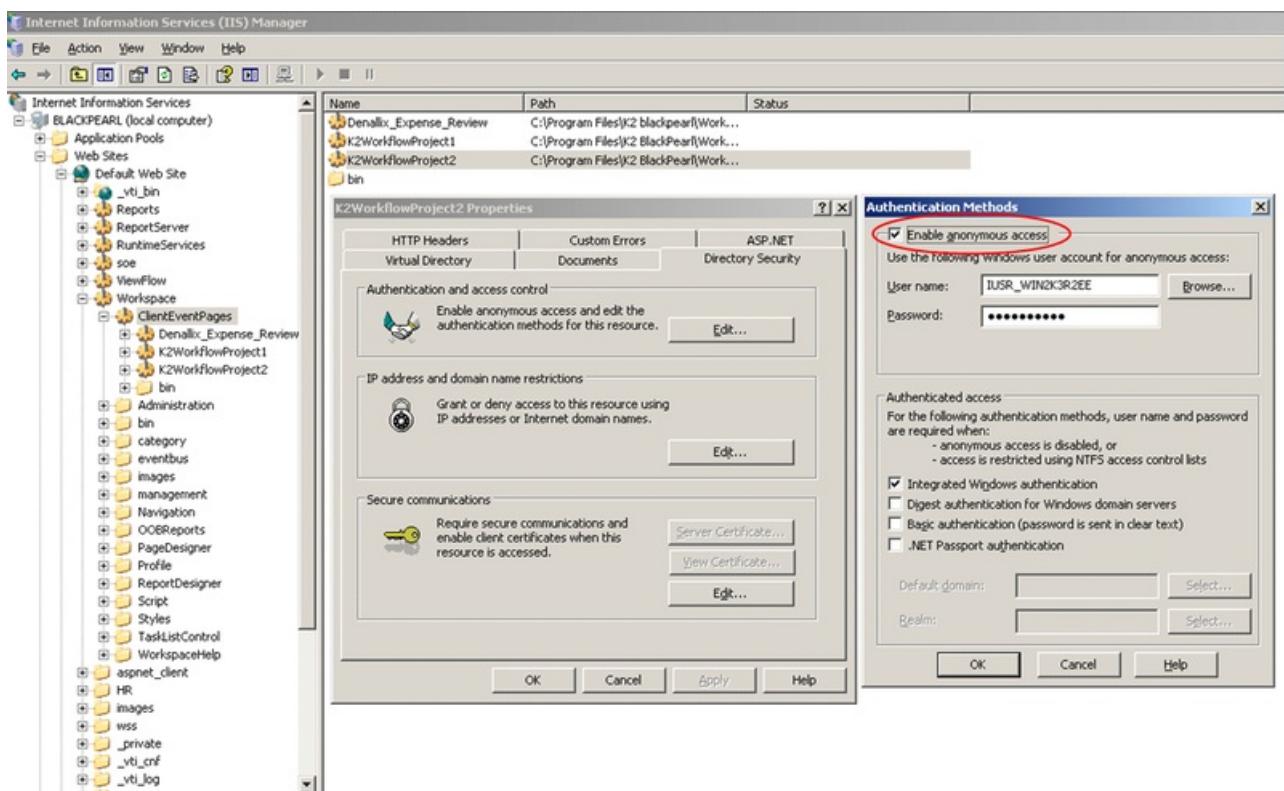


Fig. 2. IIS

1.9.15.4 Troubleshooting Start Permissions

Troubleshooting - Start Permissions

The following error is displayed when trying to start a process:

User Does Not Have Start Permissions

This error typically occurs when a user without the necessary permissions tries to start a process, or when such permissions have not been set. In order for a user to start a process successfully they need to be given Start Permissions. The User Permissions can be set in K2 Management Console.

1.9.15.5 Troubleshooting Database CPU Utilization

When the K2 Database CPU utilization regularly uses maximum capacity

When running in a high load environment with large numbers of worklist retrievals (mostly in a clustered environment), the K2 database server may utilize 100% of the CPU capacity. This may result in worklist timeouts.

If there are a large amount of worklist items, the Microsoft SQL server's CPU(s) might run at 100% when opening a worklist. This is due to a default behavior of MSSQL that takes one SQL query and executes it over all available CPU's to try and execute it faster. Therefore, while executing one large query, no one else can connect to the worklist because MSSQL is using all the CPU capacity.

In order to manage this behavior a setting has been added to the K2Server.setup file. The new setting is called 'MAXDOP' (MAXimum Degree Of Parallelism) and it allows an administrator to specify how many CPU's to use for a single SQL query. This setting is however only applicable to the worklist. If the MAXDOP setting is set to '0' (default), then the MSSQL server continues using the default behavior (where MSSQL determines how many CPU's to use), but if the MAXDOP value is set it to 1, for example, it will force MSSQL to only use one CPU to execute a SQL query.

For more information on the Microsoft SQL MAXDOP option read the following links:

- <http://support.microsoft.com/kb/329204>
- <http://msdn.microsoft.com/en-us/library/ms188611.aspx>

1.9.15.6 Troubleshooting Worklist Item Not Found

Troubleshooting Worklist Item Not Found

Only active Worklist Items can be opened. This means Worklist Items need to be opened before they are completed or expire.

Worklist Item Not Found

This error occurs when a user is attempting to open a worklist item that has already been completed or been expired.

Check to see if the activity was expired too early by an escalation, or if there was some other intervention such a GoToActivity method being called.



Remember, the GoToActivity method expires all active activities - not just the one it was called from

1.9.15.7 Troubleshooting: User Not Allowed to Open Worklist

Troubleshooting: User Not Allowed to Open Worklist

The serial number identifying the Worklist Item uniquely identifies a Worklist item for each destination user. Users may only open their own Worklist Items or those allocated to their subordinates (Managed Users). The following error might be seen:

User Not Allowed to Open Worklist Item

This error occurs when a user is attempting to open a worklist item sent to someone else. This may mean that the wrong serial number has been used. The serial number belongs to a different worklist item than the user wanted to open. In the Training VPC this happens often when multiple Internet Explorer windows are open and a worklist is opened without ensuring all other windows have been closed - thus the worklist item is requested by a user other than the intended destination user.

This error might also be displayed when using the regular OpenWorklist if the worklist item has been delegated to another user via the out of office functionality.

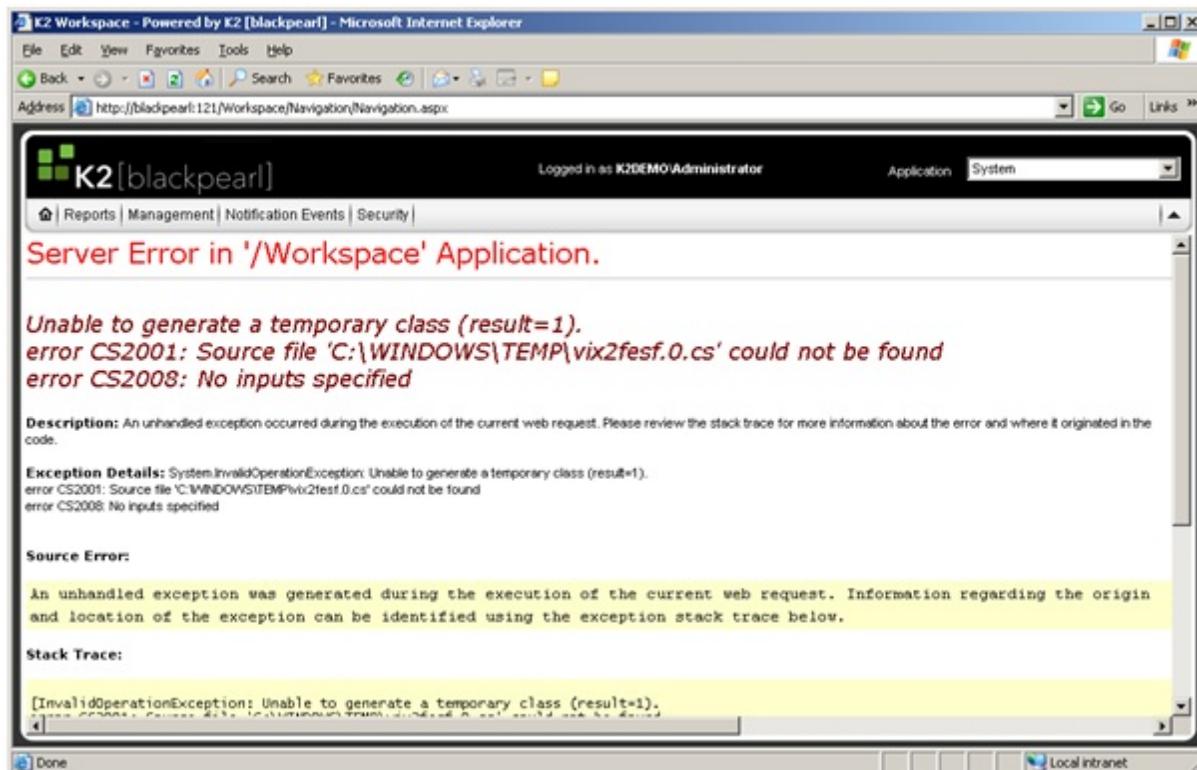
1.9.16 Workspace

1.9.16.1 Workspace Server Errors

Error

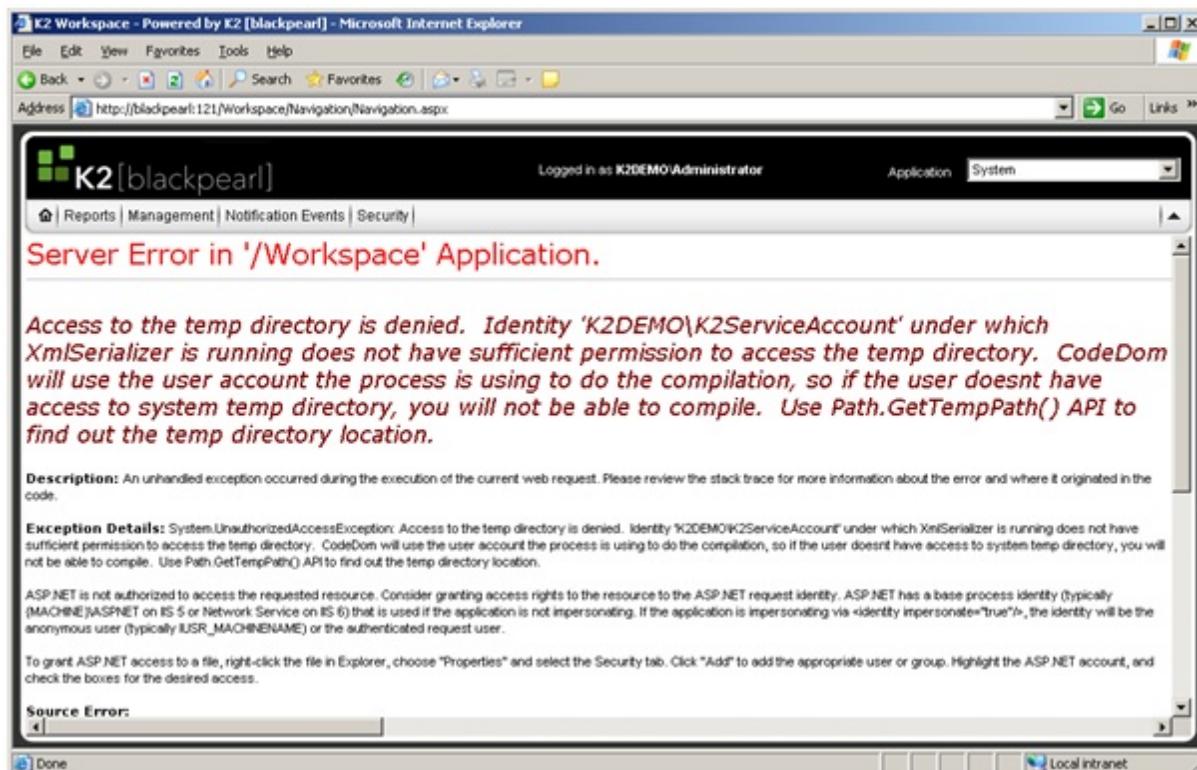
Shown below are two errors that may be encountered when insufficient permissions are given to a user to access the **C:\Windows\Temp** folder. If the user has no user permissions on the folder, the following error is encountered:

- ▶ No User Permissions (Click here to view)



If insufficient permissions are given for the **C:\Windows\Temp** folder, the following error is encountered:

- ▶ Access to the temp directory is denied (Click here to view)



Cause

Inadequate or insufficient permissions have been given to the user on the K2 Workspace server.

Resolution

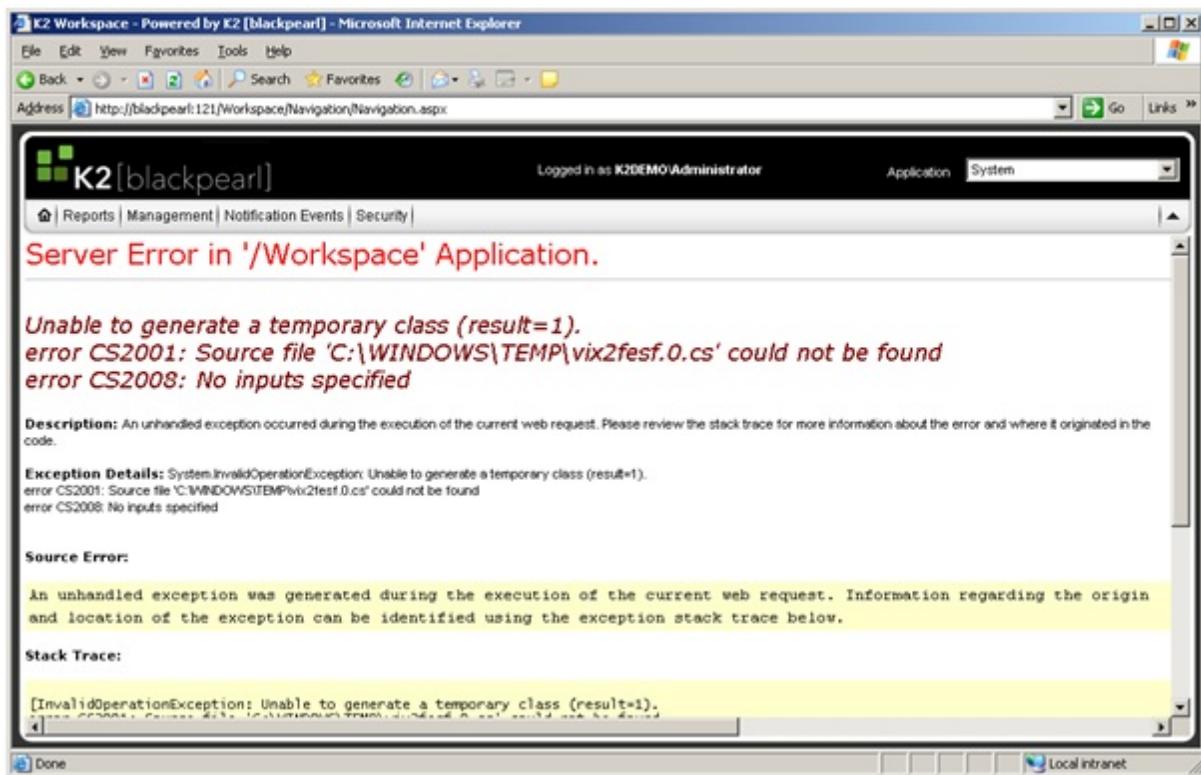
To resolve this error, make sure that the K2 Workspace server permissions have been set properly. See the [Set up Permissions > IIS Server](#) topic for more information.

1.9.16.2 Workspace folder permissions

Trouble shooting Workspace folder permissions

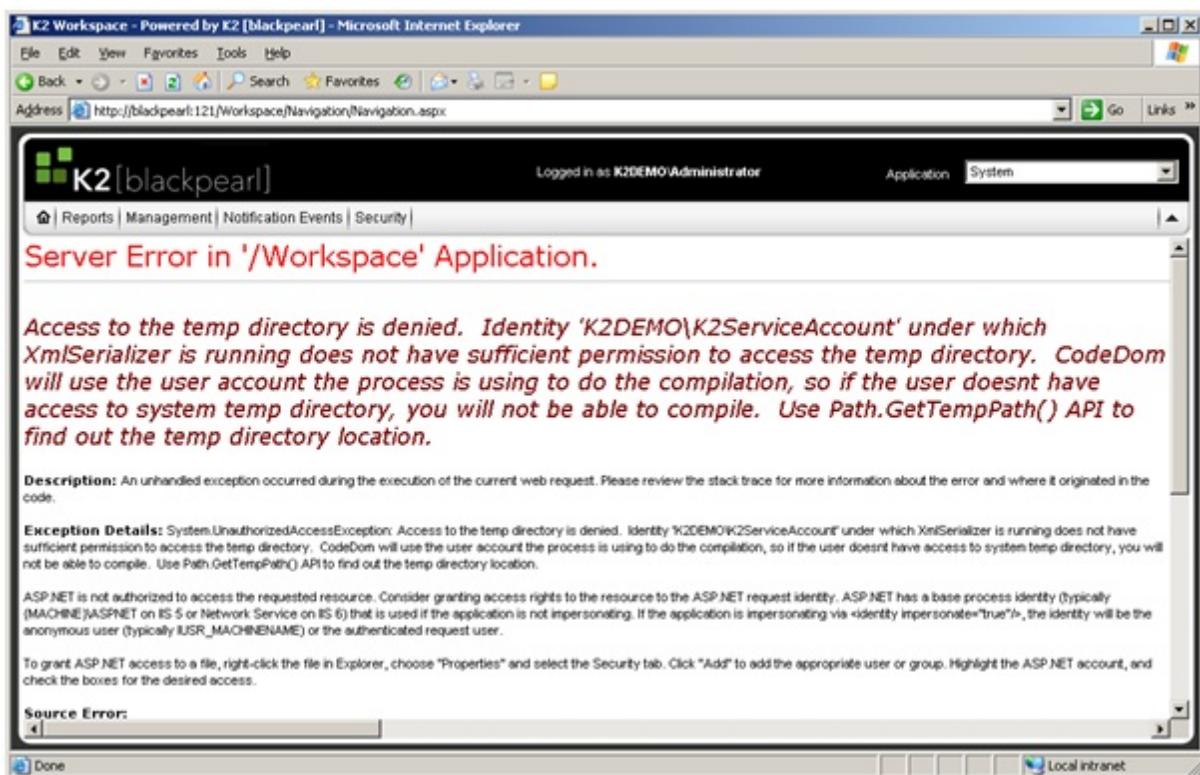
Shown below are two errors that may be encountered when insufficient permissions are given to a user to access the **C:\Windows\Temp** folder.

If the user has no user permissions on the folder the following error is encountered:



If only the following permissions are given for **C:\Windows\Temp**:

- Read & Execute
- List Folder Contents
- Read



To resolve this ensure that the following permissions are given to the users.

User Permissions	
Give all "Authenticated Users" the following C:\Windows\Temp permissions:	<ul style="list-style-type: none"> ● Read & Execute ● List Folder Contents ● Read ● Write

1.9.17 Checklist: Environment Validation

You have now installed your K2 blackpearl environment and have validated some of the areas which frequently experiences issues. But how do you ensure that your environment is working as expected?

Below are the recommended steps one should follow to validate that your environment is working as expected:

On the K2 Server

1. Stop the K2 blackpearl Service

On the SQL Server

2. Backup K2 databases (if desired)

On the K2 Server

3. Start the K2 blackpearl Service in console mode
 - Be sure to do a run as and use credentials of the K2 blackpearl Service (Service Account) shortcut
 - Watch the console window, are there any error messages?
4. Open K2 Workspace
 - Does it open?
 - If Workspace was installed on another server, view it directly from the server to verify the installation without the use of Kerberos

On the Developer Machine

This is recommended to be physically different computer than K2 Server if you need to validate Kerberos.

5. Open K2 Workspace
 - Are you prompted for credentials? Then the site is probably not trusted in IE
 - Are proper user credentials displayed? If not, Kerberos is probably not setup correctly
6. Test Visual Studio
 - Open Visual Studio and create a new Project
 - Do the K2 Project templates exist?
 - Create a new Process
 - View the Visual Studio Toolbox
 - Do the K2 wizards exist?
 - View the K2 Object Browser
 - Are you able to connect to an Environment?
 - Build out a simple process that contains at least one client event.
 - Below are some things you may consider when building out the test process:
 1. Set the destination of that client event to Process Originator to make testing easier
 2. Consider having multiple activities with client events so the process instance does not complete. This way you can delete the test instance(s) from the database via Workspace
 3. Include an e-mail event to make sure the SMTP connection is working.
 - Build and Export the process
 - Does it build OK?
 - Does it export to the server OK?
 - If you have a previously designed K2 Visual Studio Solution, try opening it up on the new machine.
7. Test the newly deployed Process within K2 Workspace
 - Open K2 Workspace \ Management
 - Assign the test account Admin permissions on newly deployed process
 - Start a new process instance under the Instances section
 - Does it start OK?
 - Go to the Worklist (home icon in Workspace)
 - Does the task appear here?
 - Check the Viewflow for this worklist item
 - Does it appear correctly?
 - Action this item (via checkbox or the context menu)

8. Test Reports within K2 Workspace
 - Click the Home icon
 - Select the Process Overview report
 - Does the report appear?
 - Does it contain the data for the new process instance?
9. Test Notification Events and E-mail
 - Within K2 Workspace browse to the Notification Events \ Notification Event Designer module
 - Create a new event notification for the OnProcessStarted event for the test process previously created
 - It is recommended to use an e-mail address of the current user so it can be easily verified
 - Start a new process instance via K2 Workspace
 - Does an e-mail get sent via the K2 event bus?
 - If not:
 - Check console for specific errors
 - Make sure MSMQ is configured correctly
 - Make sure K2 has correct SMTP configuration
10. Test SmartObject Deployment
 - In Visual Studio, create a SmartObject
 - Add some properties
 - Deploy
 - Does this deploy correctly?
11. Test K2 Worklist web part in SharePoint (Note: This is optional, only required if the web part has been deployed to a SharePoint environment)
 - Do K2 tasks appear there?
 - If not:
 - Check Kerberos configuration between SharePoint and K2 (for a distributed install)
 - Check Web Part configuration settings
12. Test K2 Designer for SharePoint (Note: This is optional, only required if the feature has been deployed to a SharePoint environment)
 - Build and deploy a simple workflow within this designer
 - As stated in the Visual Studio section, you may consider having multiple activities with client events so the process instance does not complete. This way you can delete the test instance(s) from the database via Workspace.
 - Confirm that this builds and deploys correctly.
 - Test the starting of this process as appropriate (e.g., upload a new document)
13. In K2 Workspace, delete any unwanted, active test process instances
 - If the intent is to restore the original, clean backed up databases, this step can be skipped.

On the K2 Server

14. Close the K2 Server console window

On the SQL Server

15. Restore the original, clean backed up databases, if desired.

On the K2 Server

16. Startup the K2 blackpearl Server service via Windows Services

1.9.18 Using the AD wizard on Windows 2008 and the LDAP requirement

LDAPS settings for the Active Directory Wizard

In Windows Server 2008 LDAP over SSL (LDAPS) is not configured by default, so a configuration issue may occur due to the missing LDAPS support as the environment will not have a certification authority (CA) installed and also will not have the appropriate server authentication certificate configured.

Enabling LDAP over SSL in Windows Server 2008

Use this Microsoft support article as a guide to get LDAPS working: [How to enable LDAP over SSL with a third-party certification authority](#)

2 Community Extensions

2.1 Community Extensions Overview

Community Extensions Overview

Community Extensions enables a range of community features to be automatically and seamlessly included in the K2 documentation. These features are designed to allow users to interact with the documentation as well as provide additional information, tips and tricks for the benefit of the K2 community.

The features consist of the following:

1. Community Features Feature Selector
2. Ratings Bar
3. Private Notes
4. Public Comments

For information on each of the features view the [Community Extensions Topic](#).

2.2 Community Features

Community Features

Below is a brief outline of the Community Extensions features and steps on how to use each feature.

1. The **Community Features Feature Selector** in the page header allows you to enable or disable particular Community Features according to preference



Check the box next to the feature you would like displayed on the page. This setting is user specific and display as such each time you sign in.

1. The **Ratings Bar**, in the page header, shows the average rating this page has been awarded to date.



Simply click on the desired star to submit a rating for the current page.

1. **Private Notes**, in the page footer, allows you to store private notes against a particular page - e.g. reminders of best practices, additional information specific to your environment. Private Notes are only visible to the person who created them, namely yourself.

(no notes defined)

Add a new Private Note

A large text area for entering a private note, with scroll bars on the right side.

Save **Cancel**

- Click the **Add a new Private Note** link.
- If you are not already signed in, you will be prompted to sign in.
- You can register as a new user from the Sign In page if you have not already registered.
- To **edit** an existing Private Note:
 - Click the Sign In link to Sign In.
 - Click on the edit button (a pencil icon).
 - Edit the private note in the edit field displayed.
 - Click Save to save your changes, or Cancel to abandon your changes.
- To **delete** an existing Private Note:
 - Click the Sign In link to Sign In.
 - Click on the delete button (a cross mark icon) next to the item you want to delete.

1. **Public Comments**, also in the page footer, provides a way to build community amongst our users by allowing you to comment and share information on the help content being viewed. Public Comments are visible to all users of the K2 documentation in the various formats.

(no community comments defined)

Add a new Community Comment

A large text area for entering a community comment, with scroll bars on the right side.

Save **Cancel**

- Click the **Add** a new Community Comment link. If you are not already signed in, you will be prompted to sign in. You can register as a new user from the Sign In page if you have not already registered.
- To **edit** an existing Community Comment:
 - Click the Sign In link to Sign In.
 - Click on the edit button (a pencil icon).
 - Edit the public note in the edit field displayed.
 - Click Save to save your changes, or Cancel to abandon your changes.
- To **delete** an existing Community Comment:
 - Click the Sign In link to Sign In.
 - Click on the delete button (a cross mark icon) next to the item you want to delete.



You can only edit or delete Community Comments created by you

2.3 Registering as a user and then sign in

Registering as a user and then sign in

When you open or click on the rating bar or comment sections of the Community Content list you will be prompted to sign in using your Community user details or to register as a new user.

Community Login

User Name:

Password:

Remember me next time.

[Register](#) | [Recover Password](#)

- To **sign in** enter your user name and password.
- To **register** click on the “Register link”. Enter the required fields and click the “Create User” button.

Sign Up for Your New Account

User Name:

Password:

Confirm Password:

E-mail:

Security Question:

Security Answer:



The password requires one non – alphanumeric character for example #

Once you have register the Community Login screen will appear and you can sign in with the user name and password you just created.

2.4 Usage policy for Community Extensions

Usage policy for Community Extensions

The K2 documentation provides information about the latest software developments for the K2 platform, the Community Extensions offers the K2 community the chance to contribute in a meaningful way to the existing documentation. We welcome your feedback and contribution to the documentation that will benefit the K2 community.

We invite you to register and add valuable information to a variety of topics. While doing so, we ask that you follow a few simple guidelines, as outlined below.

1. Do not post personal information in the comments. The posting of personal information of yourself or anyone else including, but not limited to phone numbers, e-mail addresses, physical addresses, names, or other personally identifying information is strictly prohibited. To keep your identity and personal information safe and to keep from being added to a spammer's e-mail list, it is recommended that you not include e-mail addresses or other personal information in your posts.
2. Be polite. These comments are designed to build a positive, thriving community. Positive, constructive comments and information that are on the topic will maintain a positive spirit. Please give the same consideration and tolerance to others that you would like to receive from them.
3. Stay on topic. Always stick to the original topic. If you have a suggestion or comment that is on a different topic, please add it to the relevant topic page.
4. Do not flame. Flaming is the act of posting messages that are deliberately hostile and insulting. These types of posts are not allowed and will result in the immediate revocation of one's comment posting privileges.
5. Do not post rude or offensive messages for the purpose of disrupting a discussion or to upset other participants. These comments will be deleted and the person may be banned from participating.
6. Do not spam. Repeated posting of a message (or very similar messages) multiple times is considered spamming and is not welcome here. When making a comment, please post it only one time in the most appropriate topic of your comment. Multiple posts will be locked or deleted, and continued abuse of this guideline may result in having your posting privileges revoked.
7. Do not post inappropriate or offensive content. Messages containing insults, profanity or religiously, racially, or sexually offensive content will be removed immediately and will result in having your posts edited or deleted and your posting privileges revoked. This includes religious debates.
8. Please practice good "netiquette." This includes respecting others, refraining from typing in all Caps, avoiding flame wars, refraining from "bumping" posts and keeping a level head at all times. Together, we can make the community safe and fun for everyone!

The K2 Community Moderators reserve the right to edit, move, lock, or delete any comment(s) that we deem to be inappropriate or disruptive to the community or ban any user at our sole discretion.

3 Further Information and Support

Further Information

K2 Websites:

- www.k2.com - Company and Product Information
- www.k2underground.com - Community Site
- help.k2.com - Knowledge Center site

Support

K2 Support:

- <https://portal.k2.com> - Customer Support Portal

4 K2 blackpearl Copyright and Trademark Statement

© 2008 - 2013 SOURCECODE TECHNOLOGY HOLDINGS, INC. ALL RIGHTS RESERVED. SOURCECODE SOFTWARE PRODUCTS ARE PROTECTED BY ONE OR MORE U.S. PATENTS. OTHER PATENTS PENDING. SOURCECODE, K2, K2 BLACKPEARL AND K2 BLACKPOINT ARE REGISTERED TRADEMARKS OR TRADEMARKS OF SOURCECODE TECHNOLOGY HOLDINGS, INC. IN THE UNITED STATES AND/OR OTHER COUNTRIES. THE NAMES OF ACTUAL COMPANIES AND PRODUCTS MENTIONED HEREIN MAY BE THE TRADEMARKS OF THEIR RESPECTIVE OWNERS.

5 Index

InfoPath Client, 545-551
.NET 3.0 Technologies, 31
.NET Framework, 116 , 31
.NET Technologies, 31
32-bit and 64-bit , 78
32-bit, 78
401 Error, 731
401.1 Error, 732-733
64 bit mode, 78
64-bit installation, 87
64-bit, 98
Access Denied Error, 687-688
Action not found error in InfoPath, 689
Action not found, 689
Activate All K2 Features and K2 Configuration Settings, 435-437
Activate Delegation for the Application Pool Account, 176
Activate delegation settings for IIS 7.0 web application , 177-179
Activate Delegation Settings for SharePoint Account, 185-187
Activate K2 Designer for SharePoint, 432-434
Activate K2 Web Parts in SharePoint 2010, 462-464
Activate K2 Web Parts, 456-457
Activate web parts , 462-464
Activating K2 Web Designer for Silverlight Task Content Type, 448
Activating Process Approval, 453-454
Activation, 377
Active Directory User Manager, 609
Active Directory Users and Computers, 121-123
Active Directory, 106-107 , 71 , 121-123 , 738
Activity Does Not Complete, 776
Activity Slots, 776
Add Settings to Site Collection, 442-443
Add Settings to Site Collection-K2 Designer for SharePoint, 444-445
Add Settings to Site Collection-K2 for SharePoint, 442-443
Add the K2 Worklist Web Part to a SharePoint page, 380
Adding a Connection, 497
Adding a User to a Group , 621-622
Adding a User to a Role, 623
Adding another K2 Server to the farm, 363
Adding Components, 656
Adding DNS Entries, 118 , 144
Adding K2 Web Parts in SharePoint 2010, 465-466
Adding K2 Web Parts, 459
Adding Multiple Active Directory Domains, 373-375
Adding Users, 350-353
Adding web parts, 465-466
Additional Actions, 246-247

Additional Notes, 411
additional permissions, 133
Additional Planning Considerations, 65
Additional Resources for Kerberos, 69

Administration

Creating a Process Portal, 458

Affinity, 134-135

AJAX, 707

AlwaysOn, 253-254

Analysis Tool, 390

Analyze Configuration, 388-389

APIs, 31

Application Pool - Validate, 269-270

Application Pool Account, 164

Application Pool Rights, 112 , 116

Application Pool, 269-270 , 176

application programming interfaces, 31

Architecture, 37

ASP Page Generate option, 106-107

ASP.NET Validation on Start Process Action Property, 777

Assembly Reference Error, 741

Assigning approvers, 453-454

Auditing and Logging, 640-642

authenticated, 341

Authentication Method, 495-496

Authentication Settings, 184

Available Web Parts, 459

Backing up Keys and Certificates, 671

Before you begin

Adding DNS Entries, 118

Before you begin, 108

Configuring Log on as a Service Rights, 337-339

IIS Group Membership, 113-114

Installation Account, 110

K2 for SharePoint - Required Permissions-K2 designer for SP, 346-348

K2 for SharePoint - Required Permissions-K2 Process Portals , 349

K2 for SharePoint - Required Permissions-SP Core , 344-345

MOSS Database Rights, 342

Permissions Necessary for the IIS and Reporting Services Server, 341

Permissions Necessary for the SharePoint Server, 343

Service Account Requirements and Permissions, 109

Set up NLB, 134-135

Set up Permissions, 133

Set up the K2 Service Account, 111

Set up the K2 Workspace Service Account, 112

Set up the Reporting Services Service Account, 116

Set up the SharePoint Service Account, 115

Before you begin, 332-336 , 108

cache, 704-706 , 357-361

Category Server, 17

Cell, 84-86

Changing the Default User Manager, 625

Check Dependencies, 302-309 , 278

Checklist: Environment Validation, 789-790

Claims

InfoPath Client, 545-551

Claims Authentication Configuration, 530-532

Claims User Identity Flow, 533-536

Configuring the LDAP User Manager, 613-617

InfoPath Forms Services, 543-544

InfoPath Integration, 542

Introduction to K2 LDAP Provider, 612

K2 and Claims - FAQ, 572-573

Mapping User , 537-541

Overview, 522

References, 569-571

SharePoint People Picker, 555-566

Supported Configuration, 525-529

Troubleshooting, 552-554 , 567-568

User Token Flow and Terminology, 523-524

Claims Authentication Configuration, 530-532

Claims User Identity Flow, 533-536

Clear cache after deploying K2 blackpearl, 381-383

clear Internet Explorer cache, 381-383

Clearing Internet Explorer Cache, 704-706

Client Components, 10 , 252

Client Installation XML - Example, 408

Client Installation XML File, 408

Client Machine, 106-107

Client Tools Only install, 251

Client Tools, 225-226

Client, 9

Clustered, 53-55

clusters, 66-67

collation setting, 29

Collations, 29

Community Extensions

Community Extensions Overview, 793

Community Features, 794-795

Registering as a user and then sign in, 796

Usage policy for Community Extensions, 797

Community Extensions Overview, 793

Community Features, 794-795

Computer, 77

Configuration Analysis , 388-389

Configuration file changes for the K2 for Reporting Services component, 730

Configuration Summary, 244-245

configuration, 392

Configure Components, 654

Configure Environment Library, 631-632

Configure for Delegation, 124-128 , 129-131

Configure InfoPath Forms Services, 693-694
Configure K2 Workspace, 628-629
Configure Out of Office, 637
Configure Security Labels, 626-627
Configure SmartObject Access, 475-478
Configure Synchronization, 485
Configure User Role Manager, 633-634
Configure Windows Designer, 635-636
Configure Workflow Server, 630
Configure Workflow Tasks and History Lists, 376
Configuring Additional K2 Workspace Nodes, 370
Configuring credentials to execute Salesforce SmartObject methods, 581
Configuring Log on as a Service Rights, 337-339
Configuring the Active Directory User Manager, 610-611
Configuring the LDAP User Manager, 613-617
Connecting to the K2 Server, 192-193
Connection Errors with Unicast NLB, 713
connection errors, 713
Connection not made, 762
Content Manager, 112
Content, 84-86
Convert Document, 84-86
Copy and Move Document screen rendering issue, 756
Create Document, 84-86
Create Folder in List, 84-86
Creating a Process Portal, 458
Creating a user , 619-620
Creating SmartObjects, 471-473
Credentials , 732-733
Credentials Delegation, 194
CRM Configuration , 231-232
CRM Entity, 106-107
CRM prerequisites, 79-82
CRM SDK Error, 767
CRM Server Entities Selection, 516
CRM SmartObjects, 514
cross-domain access for user form templates, 693-694
cross-domain access, 693-694
Custom Install, 256-257
Custom Installation Flow Diagram, 258-262
Custom Installation, 225-226
Custom User Manager, 624
Database Access, 75
Database Configurations, 273-275
Database Connection, 273-275
Database Fundamentals, 75
Database Permissions, 342
Database renamed, 165
Database Renaming During Installation, 165
Database Server, 105
Database Sizing, 75 , 65
Database, 90 , 75 , 363 , 253-254
databases, 58-60

DataSource Connection Error, 762
debugging, 714
Default Escalation Code Block Doesn't Generate, 710
Default Escalation Code Block Fails to Generate, 710
Default Permissions, 372
Delegation, 71 , 176 , 177-179 , 185-187
Dependency Server, 17
Deploy Solution, 379
Deploy the K2 Worklist Web Part, 379
Deploy web parts, 460-461
deploy, 379
Deployment Scenarios, 40-41
Designers, 24
Destination Rule - Multiple slots created but not executed, 768-769
Developer Machine, 789-790
diagnose kerberos, 737
Diagnostic Logging, 753
Directory, 84-86
Disaster Recovery - Recommended Procedure, 679-680
Disaster Recovery
 Backing up Keys and Certificates, 671
 Disaster Recovery - Recommended Procedure,
 679-680
 Introduction, 668-669
 K2 blackpearl databases Backup and Restore, 672-
 673
 Recommended Procedure, 675
 Restoring a K2 blackpearl environment, 677-678
 SQL Mirroring - manual failover, 682-684
Disaster Recovery, 672-673 , 671 , 668-669
Distributed Install
 Add the K2 Worklist Web Part to a SharePoint page, 380
 Adding another K2 Server to the farm, 363
 Adding Multiple Active Directory Domains, 373-375
 Clear cache after deploying K2 blackpearl, 381-
 383
 Configure Workflow Tasks and History Lists, 376
 Configuring Additional K2 Workspace Nodes, 370
 Deploy the K2 Worklist Web Part, 379
 Distributed Installation of K2 View Flow via Group Policy, 329-330
 Enable K2 Features, 377
 Install K2 blackpearl Host Server, 282-287
 Install K2 for SharePoint component on the SharePoint Server, 313-320
 Install K2 Workspace on the IIS Server, 302-309
 Install the K2 for Reporting Services component, 293-301
 Install the K2 for Visual Studio component, 325-
 326
 Install the K2 Studio component, 327-328
 K2 documentation, 412
 K2 Environment Security, 372
 K2 Workspace Security, 365

Set SPNs for the K2 Service Account, 120
Set SPNs for the K2 Workspace Service Account, 124-128
Set SPNs for the Reporting Services Service Account, 121-123
Set SPNs for the SharePoint Service Account, 129-131
Set SPNs for the SQL Server Service Account, 132
View Flow validation, 366-369

Distributed Installation of K2 View Flow via Group Policy, 329-330

Distributed Transaction Coordinator , 138-141

DNS Basics, 72

DNS Beyond the Basics, 73-74

DNS lookup zones, 118

DNS Management Console, 118

DNS, 118

Document Information Panel unable to load, 747

Document Library, 474

Documentation, 14

Domain Configuration, 65 , 71

Domain Policies, 71

double-hop issue, 69

Dropdown list box options not visible, 717

Drop-down List Box Options not visible, 717

DTC, 28 , 738

Dynamic SQL Server Configuration Requirements, 199-200

Dynamic SQL Service Impersonation, 198

Edit Connection, 505-506

Edit SmartObject, 507-508

E-mail Event rendering issue, 757

E-mail ProtocolSetup, 598-600

Enable and Configure DTC Components, 159-161

Enable and Configure the DTC Components, 138-141

Enable K2 Features, 377

Enable K2 Logging, 714

Enabling , 640-642

Enabling Kerberos Logging, 737

End User License Agreement, 223-224

Enforce Impersonation, 196

Entity, 84-86

Environment Browser, 583-586

Environment Library Management, 587

Environment Library, 17 , 587

Environment, 583-586

Error 4 Server was unable to process request, 700

error CS2001, 785-786

error CS2008, 785-786

Error Page, 742

Error with Forms Generation Client Event, 778-779

EULA, 223-224

Event Bus Server, 32

Event Bus, 17

Exchange Integration, 237-239

Exchange Server Configuration, 233-236
Exchange Server prerequisites, 237-239
Exchange, 84-86 , 106-107 , 71
Export CRM SmartObject, 518-520
Export Import Pre-requisites and Preparation, 480
Export SQL SmartObject, 511-513
extend SharePoint Site, 435-437
Extend SharePoint, 435-437
extend, 435-437
extended sites, 377
Failed connection to data source, 691-692
Farm configuration for Kerberos delegation , 182
Form Open Error, 693-694
Forms Generation - Parser Error, 770
FQDN, 176
Full Installation XML - Example, 404-405
Full Installation XML File, 404-405
Full Installation, 225-226
Functional Roles, 24
Further Information and Support, 798
General Reference
 DNS Basics, 72
 DNS Beyond the Basics, 73-74
Generate ASP Page, 106-107
Generate Silent / Unattended Installation XML File, 394
Generate System Key, 393
Get Cell with Input, 106-107
Get Cell, 106-107
Get Content Control, 106-107
Get Range with Input, 106-107
Get Range, 106-107
Get, 84-86
Getting Started Home Page, 1-2
Getting Started with Salesforce, 576-580
Getting started, 576-580
Global Assembly Cache, 78
Group Policy Object, 715
Hardware Prerequisites, 77
HomePage
 Getting Started Home Page, 1-2
 How to use this Getting Started Guide, 4-5
 Introduction, 3
 K2 blackpearl Installation Guide, 205-206
 Optional installation logging for troubleshooting,
 207-208
Host Server Database, 253-254
HostServer, 363
How K2 Pass-Through Works, 191
How to Create a SharePoint SmartObject, 467
How to create new CRM server connection, 515
How to register the K2 Failover Job Definition for a new Web Application , 450-452
How to use this Getting Started Guide, 4-5
Identity Settings, 357-361
IE ESC, 707

IIS 7 Configuration, 142
IIS 8 Configuration, 162
IIS administrator, 70
IIS Group Membership, 113-114
IIS Reset, 246-247
IIS, 341, 65, 70, 142, 173, 175, 177-179, 185-187
IIS_IUSRS, 113-114
IIS_WPG, 113-114
Import and Export SQL and CRM SmartObjects, 479
Import CRM SmartObject, 521
Import SQL SmartObject, 510
Important Considerations, 447
InfoPath - Access is Denied Error, 687-688
InfoPath - An error occurred accessing a data source, 690
InfoPath - Failed Connection to Source, 691-692
InfoPath - Form cannot be displayed error, 695
InfoPath - Form Error, 693-694
InfoPath - InfoPath Form is not displayed on Worklist, 696
InfoPath - Integrate with SmartObject, 697
InfoPath - Invalid date error in Data Event wizard, 698
InfoPath - Troubleshooting Deployment Error in K2 Studio, 702
InfoPath - URL Not Found, 699
InfoPath - Workflow Unable to Deploy, 700
InfoPath 2013, 84-86
InfoPath Access Denied, 687-688
InfoPath and SmartObjects issue with Re-publish, 701
InfoPath Configuration Notes, 574
InfoPath Configuration, 574
InfoPath form not displaying on SharePoint Worklist, 696
InfoPath Form Open Error, 693-694
InfoPath Forms Services, 543-544
InfoPath Integration, 332-336, 542
InfoPath Troubleshooting, 689, 697, 700, 691-692, 696, 699
InfoPath URL not valid, 699
Information and Error Messages, 201
Insert into Document, 84-86
Install K2 blackpearl Host Server, 282-287
Install K2 for SharePoint component on the SharePoint Server, 313-320
Install K2 Workspace on the IIS Server, 302-309
Install the K2 for Reporting Services component, 293-301
Install the K2 for Visual Studio component, 325-326
Install the K2 Studio component, 327-328
Install, 302-309
Installation Account, 110
Installation and Configuration Settings, 190
Installation Guide, 205-206
Installation Scenarios, 40-41
installation status, 248-249

Installation Type, 225-226

Installation XML File, 394

Installer

Activate Delegation Settings for SharePoint Account, 185-187

Additional Notes, 411

Generate Silent / Unattended Installation XML File, 394

Generate System Key, 393

Setup Options, 409-410

Silent/Unattended Installation (using the XML File), 395

Site authentication to Kerberos for SharePoint site, 184

Unattended Installer - Upgrade, 397-398

Installing a distributed K2 blackpearl system, 281

Installing a New Version as an Upgrade, 664

Installing a standalone K2 blackpearl system, 209-215

Installing Components, 248-249

Installing the Database, 75

InstallPath, 393

Integrate with SmartObject error, 697

Integration, 84-86

Internet Explorer 7, 33

Internet Explorer 8, 33

Internet Explorer Enhanced Security Configuration, 707

Internet Explorer Settings, 708

Internet Explorer, 33 , 704-706

Internet Information Service (IIS), 70

Introduction to K2 LDAP Provider, 612

Introduction to SSL, 589

Introduction to User Managers, 168-170

Introduction, 468-469 , 7-8 , 4-5 , 3 , 384 , 668-669 , 471-473 , 189

Invalid Packet Header Error, 723

K2 Administration Account , 109

K2 Administrator Account, 276-277

K2 and Claims - FAQ, 572-573

K2 Architecture, 37

K2 Architecture: Client, 39

K2 Architecture: Server, 38

K2 Auditing and Logging, 640-642

K2 Auditing, 640-642

K2 blackpearl 4.5 Support for Microsoft 2008

Technologies, 25

K2 blackpearl Components Overview, 9

K2 blackpearl Components, 87

K2 blackpearl Copyright and Trademark Statement, 799

K2 blackpearl databases Backup and Restore, 672-673

K2 blackpearl Documentation, 14

K2 blackpearl Installation Guide, 205-206

K2 blackpearl Installation, 205-206

K2 blackpearl Maintenance, 651

K2 Configuration Analysis Tool

Analyze Configuration, 388-389

Introduction, 384

- Summary of tool checks, 385-387
- Which Machines to Analyze, 390
- K2 Database Configuration, 263**
- K2 Designer for SharePoint Administration Settings, 432-434**
- K2 Designer for SharePoint, 13 , 129-131 , 448**
- K2 Designer for Visual Studio, 11**
- K2 documentation, 412**
- K2 Environment Security, 372**
- K2 Environment, 583-586**
- K2 for Reporting Services, 20**
- K2 for SharePoint - Prerequisite Check (Advanced), 426**
- K2 for SharePoint - Required Permissions-K2 designer for SP, 346-348**
- K2 for SharePoint - Required Permissions-K2 Process Portals , 349**
- K2 for SharePoint - Required Permissions-SP Core , 344-345**
- K2 for SharePoint - Retract a solution (Advanced), 428-430**
- K2 for SharePoint - Solution Deployment (Advanced), 427**
- K2 for SharePoint**
 - Configure Synchronization, 485
 - Export Import Pre-requisites and Preparation, 480
 - Import and Export SQL and CRM SmartObjects, 479
 - Introduction, 471-473
 - Restricted Wizards, 649-650
 - SharePoint SmartObject Configuration Export, 486-487
 - SharePoint SmartObject Configuration Import, 488-489
 - SmartObject Import Export Troubleshooting, 481-482
 - SQL
 - CRM SmartObject Import & Export Troubleshooting, 483-484
- K2 for SharePoint Central Administration Wizard**
 - K2 for SharePoint - Prerequisite Check (Advanced), 426
 - K2 for SharePoint - Retract a solution (Advanced), 428-430
 - K2 for SharePoint - Solution Deployment (Advanced), 427
 - K2 for SharePoint Configuration Wizard - Features Activation, 424
 - K2 for SharePoint Configuration Wizard - Installation, 418
 - K2 for SharePoint Configuration Wizard - Solution Deployment, 419-421
 - K2 for SharePoint Configuration Wizard - Solutions Deployed, 422-423
 - K2 for SharePoint Configuration Wizard, 415-416
 - K2 for SharePoint Prerequisite Check, 417
- K2 for SharePoint Component Flow Diagram, 321-323**
- K2 for SharePoint Configuration Wizard - Features Activation, 424**
- K2 for SharePoint Configuration Wizard - Installation,**

418

- K2 for SharePoint Configuration Wizard - Solution Deployment, 419-421**
- K2 for SharePoint Configuration Wizard - Solutions Deployed, 422-423**
- K2 for SharePoint Configuration Wizard, 415-416**
- K2 for SharePoint Prerequisite Check, 417**
- K2 for SharePoint tab error, 750**
- K2 for SharePoint, 19 , 377 , 471-473 , 442-443 , 448**
- K2 for Visual Studio, 94 , 11 , 325-326**
- K2 Logging, 640-642**
- K2 Management Console, 587**
- K2 Pass-Through Authentication**
 - Connecting to the K2 Server, 192-193
 - Credentials Delegation, 194
 - Dynamic SQL Server Configuration Requirements, 199-200
 - Dynamic SQL Service Impersonation, 198
 - Enforce Impersonation, 196
 - How K2 Pass-Through Works, 191
 - Information and Error Messages, 201
 - Installation and Configuration Settings, 190
 - Introduction, 189
 - Scenario Walkthrough, 202-204
 - SharePoint Impersonation, 197
 - Single Sign On, 195
- K2 Pass-Through Authentication, 68 , 267-268**
- K2 Platform Licensing, 83**
- K2 Process Portal, 455**
- K2 Process Portals, 456-457 , 459**
- K2 Requirements for AD, 591**
- K2 Server , 789-790**
- K2 Server Configuration File Updates, 594-596**
- K2 Server Configuration, 255**
- K2 Server Installation Flow Diagram, 288-292**
- K2 Server, 88-89 , 17 , 16**
- K2 servers in distributed environment, 282-287**
- K2 Service Account, 111 , 109 , 337-339 , 276-277 , 146**
- K2 Service Startup, 356**
- K2 Service will not start, 715**
- K2 Setup Manager, 15 , 653 , 654**
- K2 SharePoint Integration feature, 432-434**
- K2 Site Settings Link, 446**
- K2 Site Settings, 475-478 , 471-473**
- K2 SmartActions**
 - E-mail ProtocolSetup, 598-600
 - K2 Server Configuration File Updates, 594-596
 - K2 SmartActions E-mail Security, 601-602
 - K2 SmartActions Installation, 240-241
 - Pre-Installation, 593
 - SmartAction Synonyms, 597
- K2 SmartActions E-mail Security, 601-602**
- K2 SmartActions Installation, 240-241**
- K2 SmartObject Service Management, 471-473**

K2 SmartObject Site Lists and Libraries, 471-473
K2 Studio - Wizard Rendering Issue, 718
K2 Studio, 96 , 12
K2 Upgrade Options, 663
K2 User Account, 229-230
K2 Web Designer Administration Settings, 471-473
K2 Web Designer, 448
K2 Web Parts, 446
K2 Wizards, 11
K2 Worklist web part, 380 , 129-131
K2 Worklist, 379
K2 Workspace - Invalid Packet Header Error, 723
K2 Workspace - Report Error, 724
K2 Workspace - Report Rights Error, 725-726
K2 Workspace - User with Insufficient Permissions, 727-728
K2 Workspace Install Flow Diagram, 310-312
K2 Workspace Permissions Requirements, 164
K2 Workspace Report Error, 724
K2 Workspace Security, 365
K2 Workspace Service Account, 109 , 112 , 149-150
K2 Workspace Troubleshooting, 727-728
K2 Workspace Web Site Configuration, 229-230
K2 Workspace, 97 , 18 , 708 , 164
K2Server, 75
K2ServerLog, 75
Kerberos for Windows Server 2008, 172
Kerberos Setup and Configuration, 69
Kerberos, 58-60 , 53-55 , 56-57 , 65 , 69 , 70 , 120 , 121-123 , 124-128 , 129-131 , 132 , 739 , 737 , 738 , 188 , 175 , 172
KerbTray, 739
Kernel Mode, 175
key performance indicators, 32
KPIs, 32
Large Scale Install, 58-60
Latest Version Validation, 221-222
LDAP, 373-375
License Configuration, 363 , 227-228
License Key, 83
License, 657 , 227-228
Local Administrator, 110
Local DTC, 138-141
Local Security Policy, 337-339
Log File, 250
Log on Failure, 715
logging, 737 , 753
Mail Server, 242-243
Maintenance
 Adding Components, 656
 Installing a New Version as an Upgrade, 664
 K2 blackpearl Maintenance, 651
 Manual Environment Clean Up, 660-661
 Remove Components, 659
 Repairing an Existing Component, 653

Updating the K2 License Key, 657
 Validating the Uninstall, 662
Managing Existing SQL SmartObject Connections (Edit), 503-504
Manual Environment Clean Up, 660-661
Mapping User , 537-541
Maximum Redundancy on Six Servers, 56-57
Medium Scale Install, 53-55
Medium Scale, 53-55
Messaging, 32
MetaBase, 70
Method not found error, 742
Method not Found, 742
Microsoft 2008 Support and Configuration Requirements
 Database Renaming During Installation, 165
 Enable and Configure the DTC Components, 138-141
 IIS 7 Configuration, 142
 K2 Workspace Permissions Requirements, 164
 Microsoft 2008 Support and Configuration Requirements, 117
 MSMQ, 136-137
 Service Accounts, 171
 Set SPN, 119
 SQL Reporting Services, 166
 Troubleshooting and Resources, 188
Microsoft 2008 Support and Configuration Requirements, 117
Microsoft 2008 Technologies Support, 26-27
Microsoft Data Transaction Coordinator (MSDTC) Exception, 764
Microsoft Message Queuing , 136-137
Microsoft Office SharePoint Server (MOSS), 26-27
Microsoft Office SharePoint Server 2007 (MOSS), 36
Microsoft Office SharePoint Server, 95
Microsoft Office technologies , 36
Microsoft Office technologies, 36
Microsoft SharePoint Server 2007 (MOSS), 19
Microsoft SQL Server & Reporting Services, 29
Microsoft SQL Server 2005, 20
Microsoft SQL Server 2008, 29
Microsoft Visual Studio 2010, 34
Microsoft Windows Server, 28
Microsoft Windows Vista or later, 30
Microsoft Windows XP SP3, 30
Miscellaneous, 380
Modify, 112 , 656
MOSS Database Rights, 342
MOSS, 95 , 342 , 47-48
MSDTC, 765 , 138-141
MSIL, 78
MSMQ Settings, 157-158
MSMQ, 136-137
multiple domains, 373-375
Multiple SharePoint and K2 Farms, 63-64

Multiple System Accounts - Task actioning, 743
Netbios, 373-375
Network Interface cards, 713
Network Load Balancing Setup and Configuration, 66-67
Network Load Balancing vs Clustering, 66-67
Network Load Balancing, 134-135 , 49-50 , 51-52 , 53-55 , 65
NIC, 713
NLB SharePoint, 53-55
NLB, 134-135 , 58-60 , 49-50 , 51-52 , 56-57 , 65 , 66-67 , 713
NTFS, 116
Operations, 379
Operators, 24
Option 3: Utilizing the AdminPack for IIS7.0, 180-181
Optional installation logging for troubleshooting, 207-208
Output, 393
Overview, 522
Permissions Necessary for the IIS and Reporting Services Server, 341
Permissions Necessary for the SharePoint Server, 343
Permissions, 133 , 372
Physical Network Environment, 66-67
Planning Guide
.NET Technologies, 31
Additional Planning Considerations, 65
Client Components, 10
Database, 75
Deployment Scenarios, 40-41
Domain Configuration, 71
Functional Roles, 24
Internet Explorer, 33
Internet Information Service (IIS), 70
K2 Architecture, 37
K2 Architecture: Client, 39
K2 Architecture: Server, 38
K2 blackpearl 4.5 Support for Microsoft 2008 Technologies, 25
K2 blackpearl Components Overview, 9
K2 blackpearl Documentation, 14
K2 Designer for SharePoint, 13
K2 for Reporting Services, 20
K2 for SharePoint, 19
K2 for Visual Studio, 11
K2 Pass-Through Authentication, 68
K2 Platform Licensing, 83
K2 Studio, 12
Kerberos Setup and Configuration, 69
Large Scale Install, 58-60
Maximum Redundancy on Six Servers, 56-57
Medium Scale Install, 53-55
Messaging, 32
Microsoft 2008 Technologies Support, 26-27
Microsoft Office technologies, 36

Microsoft Visual Studio 2010, 34
 Microsoft Windows Server, 28
 Microsoft Windows Vista or later, 30
 Network Load Balancing Setup and Configuration, 66-67
Planning the Environment, 7-8
Prerequisites, 76
Scaling for Better Performance, 47-48
Scaling for Data and Performance, 51-52
Scaling for Data Availability, 45-46
Scaling for Page Rendering, 49-50
Server Components, 17 , 16
Setup Manager, 15
Small Scale Install, 43-44
Standalone Install, 42
Technology Requirements, 23
Version Support and Backwards Compatibility 2010 , 35
Web Components, 18

Planning the Environment, 7-8

Planning, 7-8 , 65

PP-Web Parts-Activate Web Parts, 456-457

PP-Web Parts-Add Web Parts, 459

Pre Install, 108

Pre-Installation, 593

Prereqs K2 Designer for SharePoint , 91-92

Prerequisites

Hardware Prerequisites, 77
 K2 Studio, 96
 Prereqs K2 Designer for SharePoint , 91-92
 Prerequisites by Component, 87
 Prerequisites by Role, 98
 Prerequisites for the Client Machine role, 106-107
 Prerequisites for the Database Server role, 105
 Prerequisites for the K2 Database component, 90
 Prerequisites for the K2 for Reporting Services component, 93
 Prerequisites for the K2 for SharePoint component, 95
 Prerequisites for the K2 for Visual Studio component, 94
 Prerequisites for the K2 Server role, 88-89
 Prerequisites for the K2 Workspace, 97
 Prerequisites for the Reporting Services Server role, 103-104
 Prerequisites for the SharePoint Server role, 102
 Prerequisites for the Web Server role, 101
 Software Prerequisites, 79-82

Prerequisites by Component, 87

Prerequisites by Role, 98

Prerequisites for the Client Machine role, 106-107

Prerequisites for the Database Server role, 105

Prerequisites for the K2 Database component, 90

Prerequisites for the K2 for Reporting Services component, 93

Prerequisites for the K2 for SharePoint component, 95

Prerequisites for the K2 for Visual Studio component, 94

Prerequisites for the K2 Server role, 88-89

Prerequisites for the K2 Workspace, 97

Prerequisites for the Reporting Services Server role, 103-104

Prerequisites for the SharePoint Server role, 102

Prerequisites for the Web Server role, 101

Prerequisites, 76 , 205-206 , 663

Process Approval

Activating Process Approval, 453-454

Process Approval, 453-454

Process Designer Administration Settings, 432-434

Process Portal - Web Parts, 455

Process Portal Report Error, 744

Processor, 77

Proxy servers, 71

Range, 84-86

Recommended Procedure, 675

Redundancy, 56-57

Reference - Architecture and Infrastructure

K2 Auditing and Logging, 640-642

Required Permissions in K2 blackpearl, 332-336

Reference - BlackPearl

Further Information and Support, 798

Integration, 84-86

K2 blackpearl Copyright and Trademark Statement, 799

Reference - InfoPath

InfoPath Configuration Notes, 574

Reference - K2 Process Portals

PP-Web Parts-Activate Web Parts, 456-457

PP-Web Parts-Add Web Parts, 459

Process Portal - Web Parts, 455

Reference - K2 Web Designer Mail Wizards

K2 Designer for SharePoint Administration Settings, 432-434

Reference - Salesforce

Configuring credentials to execute Salesforce SmartObject methods, 581

Getting Started with Salesforce, 576-580

Salesforce Integration, 575

Reference - SmartObjects

Configure SmartObject Access, 475-478

Using SmartObjects in SharePoint, 474

Reference - Studio ObjectBrowser

Environment, 583-586

Reference - Troubleshooting

Action not found error in InfoPath, 689

ASP.NET Validation on Start Process Action Property, 777

Assembly Reference Error, 741

Connection not made, 762

Copy and Move Document screen rendering issue, 756

Default Escalation Code Block Doesn't Generate,

710
Destination Rule - Multiple slots created but not executed, 768-769
Drop-down List Box Options not visible, 717
E-mail Event rendering issue, 757
Error with Forms Generation Client Event, 778-779
Forms Generation - Parser Error, 770
InfoPath - Access is Denied Error, 687-688
InfoPath - Failed Connection to Source, 691-692
InfoPath - Form cannot be displayed error, 695
InfoPath - Form Error, 693-694
InfoPath - InfoPath Form is not displayed on Worklist, 696
InfoPath - Integrate with SmartObject, 697
InfoPath - Invalid date error in Data Event wizard, 698
InfoPath - URL Not Found, 699
InfoPath - Workflow Unable to Deploy, 700
InfoPath and SmartObjects issue with Re-publish, 701
K2 Studio - Wizard Rendering Issue, 718
K2 Workspace - Invalid Packet Header Error, 723
K2 Workspace - Report Error, 724
K2 Workspace - Report Rights Error, 725-726
K2 Workspace - User with Insufficient Permissions, 727-728
Method not Found, 742
Multiple System Accounts - Task actioning, 743
Process Portal Report Error, 744
Report Error, 745
SharePoint - Attachment icons not displaying, 746
SharePoint - Document Information Panel unable to load, 747
SharePoint - SharePoint Central Administration Error, 748
SharePoint - Task Error, 749
Silverlight Designer (Troubleshooting the Silverlight Designer), 758
SmartObject Exception, 764
SmartObjectServer Exception - 401 Unauthorized error, 763
Troubleshooting Activity Slots, 776
Troubleshooting Start Permissions, 780
Troubleshooting the Succeeding Rule, 771
Troubleshooting Worklist Item Not Found, 782
Troubleshooting: User Not Allowed to Open Worklist, 783
'Unknown Error' on the K2 for SharePoint tab, 750
Using the AD wizard on Windows 2008 and the LDAP requirement, 791
View Flow - Report does not display, 735
Visual Studio - Invalid URI, 711
Web Part Error, 754
Word Document - Error with Word Document Conversion, 772
Word Document - Troubleshooting Error Codes for Word Document Conversion Issues, 773-774
Workspace folder permissions, 787-788

Reference - Workspace Management Console

Environment Library Management, 587

References, 569-571

Refresh the User Manager Cache, 638

Registering as a user and then sign in, 796

Registration Requirements, 493

Registry Key, 660-661

Remove Components, 659

Remove K2 blackpearl, 659

Removing Internet Explorer Enhanced Security, 707

Removing, 659

Repair, 388-389

Repairing an Existing Component, 653

Repairing, 653

Report does not display, 735

Report Error, 745

Report Processing error, 724

Reporting Instance Name, 271-272

Reporting Services Permissions, 116

Reporting Services Server, 103-104

Reporting Services Service Account, 109 , 116 , 121-123 , 732-733 , 147-148

Reporting Services, 93 , 730 , 731

Reporting Web Part

Activate K2 Web Parts in SharePoint 2010, 462-464

Adding K2 Web Parts in SharePoint 2010, 465-466

Web Parts Solution Deployment in SharePoint 2010, 460-461

Required Permissions in K2 blackpearl, 332-336**Requirements, 76 , 24 , 23**

Restoring a K2 blackpearl environment, 677-678

Restricted Wizards, 649-650

retract solution, 428-430

roles, 98

Run As

Adding Users, 350-353

runtime Web services, 142

runtime, 17

Sales Force Integration, 576-580

Salesforce Integration Resources, 575

Salesforce Integration, 575

SAN, 66-67

Scaling for Better Performance, 47-48

Scaling for Data and Performance, 51-52

Scaling for Data Availability, 45-46

Scaling for Page Rendering, 49-50

Scenario Walkthrough, 202-204

Security, 372

Segmentation by Site Collection, 61-62

Select Components, 264-265

Selected Components, 244-245

Server Components, 17 , 16

Server Error in '/Workspace' Application, 727-728

Server Installation XML - Example, 406-407

Server Installation XML File, 406-407
Server, 9
Service Account Requirements and Permissions, 109
Service Accounts Configuration, 276-277
service accounts, 109 , 171
Service Principal Name, 120 , 121-123 , 129-131 , 132
Services, 84-86
Session state has been disabled, 744
Set SPN, 119
Set SPNs for the K2 Service Account, 120
Set SPNs for the K2 Workspace Service Account, 124-128
Set SPNs for the Reporting Services Service Account, 121-123
Set SPNs for the SharePoint Service Account, 129-131
Set SPNs for the SQL Server Service Account, 132
Set up NLB, 134-135 , 155-156
Set up Permissions, 133 , 154
Set up SPNs, 145
Set up the K2 Service Account, 111
Set up the K2 Workspace Service Account, 112
Set up the Reporting Services Service Account, 116
Set up the SharePoint Service Account, 115
SetSPN, 119
Setting up SSRS with a Domain user as an application pool account, 174
Settings for Internet Explorer, 708
Setup Kerberos delegation for IIS 7.0, 175
Setup Manager
 Additional Actions, 246-247
 Check Dependencies, 278
 Client Components, 252
 Client Tools Only install, 251
 Configuration Summary, 244-245
 Configure Components, 654
 CRM Configuration , 231-232
 Custom Install, 256-257
 Database Configurations, 273-275
 End User License Agreement, 223-224
 Exchange Integration, 237-239
 Exchange Server Configuration, 233-236
 Host Server Database, 253-254
 Installation Type, 225-226
 Installing a distributed K2 blackpearl system, 281
 Installing a standalone K2 blackpearl system, 209-215
 Installing Components, 248-249
 K2 Database Configuration, 263
 K2 Pass-Through Authentication, 267-268
 K2 Server Configuration, 255
 K2 Workspace Web Site Configuration, 229-230
 Latest Version Validation, 221-222
 License Configuration, 227-228
 Select Components, 264-265

Service Accounts Configuration, 276-277
Setup Manager Finished, 250
 SMTP Settings (outgoing mail), 242-243
 SQL Reporting Services, 271-272
 User Manager Settings, 279-280
 Welcome Screen, 220
 Workspace Application Pool Configuration, 269-270

Setup Manager Finished, 250

Setup Manager prerequisites, 79-82

Setup Manager, 392, 15, 313-320, 325-326

Setup Options, 409-410

setup.exe /?, 409-410

SharePoint - Attachment icons not displaying, 746

SharePoint - Authentication is required for session error, 751

SharePoint - Document Information Panel unable to load, 747

SharePoint - SharePoint Central Administration Error, 748

SharePoint - Solution stays in deployment state, 752

SharePoint - Task Error, 749

SharePoint 2010

- Edit Connection, 505-506
- Edit SmartObject, 507-508
- Managing Existing SQL SmartObject Connections (Edit), 503-504
- SQL Connection Settings, 499-500
- SQL SmartObject Method Configuration, 502
- SQL SmartObject Method Creation, 501

SharePoint Central Administration, 377, 753, 184, 432-434

SharePoint Central Administrator Error, 748

SharePoint error, 748

SharePoint Group Provider, 435-437

SharePoint Groups, 435-437

SharePoint Impersonation, 197

SharePoint Integration

- Activate All K2 Features and K2 Configuration Settings, 435-437
- Add Settings to Site Collection-K2 Designer for SharePoint, 444-445
- Add Settings to Site Collection-K2 for SharePoint, 442-443
- How to register the K2 Failover Job Definition for a new Web Application, 450-452
- Important Considerations, 447
- K2 Designer for SharePoint, 448
- K2 Web Parts, 446

SharePoint Integration Considerations, 447

SharePoint List, 474

SharePoint People Picker, 555-566

SharePoint Server, 102

SharePoint Service Account, 109

SharePoint Service Account, 115, 151-152

SharePoint Site Collection, 475-478

SharePoint SmartObject Configuration Export, 486-487

SharePoint SmartObject Configuration Import, 488-489
SharePoint Task Error, 749
SharePoint Timer Activation Feature, 438-441
SharePoint Troubleshooting, 750 , 747
SharePoint Web Application, 185-187
SharePoint Workflow Integration, 343
SharePoint, 95 , 753
Silent Installation, 395
Silent/Unattended Installation (using the XML File), 395
Silverlight Designer (Troubleshooting the Silverlight Designer), 758
Simple Installation, 225-226
Single Sign On, 195
Site authentication to Kerberos for SharePoint site, 184
Slow startup for K2 components when machine has no internet access , 720-721
Small Scale Install, 43-44
SmartAction Synonyms, 597
SmartActions fail: mailbox full error, 760
SmartObject Configuration, 475-478
SmartObject Exception, 764
SmartObject Import Export Troubleshooting, 481-482
SmartObject Methods, 475-478
SmartObject Server, 17
SmartObjects Troubleshooting, 764 , 762
SmartObjectServer Exception - 401 Unauthorized error, 763
SmartObjectServer Exception , 765
SmartObjectServer Exception, 765
SMTP Settings (outgoing mail), 242-243
SMTP, 32
Software Prerequisites, 79-82
Some rules were not applied error, 689
SourceCode Assemblies, 660-661
SourceCode registry key, 660-661
SPN, 120 , 121-123 , 124-128 , 129-131 , 132 , 739 , 119
SPNs, 70 , 732-733
SQL
 CRM SmartObject Import & Export Troubleshooting, 483-484
SQL 2008, 26-27
SQL Business Intelligence, 734
SQL Cluster, 56-57
SQL Connection Settings, 499-500
SQL Mirroring - manual failover, 682-684
SQL Reporting Services Service Account, 116
SQL Reporting Services web site, 293-301
SQL Reporting Services, 271-272 , 166
SQL Server 2012 AlwaysOn, 253-254
SQL Server Reporting Services Service Object, 121-123
SQL Server Reporting Services, 173
SQL Server Service Account, 132 , 153
SQL Server, 110 , 58-60 , 43-44 , 45-46 , 47-48 , 49-50 , 51-52 , 789-790

SQL service, 132
SQL SmartObject Method Configuration, 502
SQL SmartObject Method Creation, 501
SQL User Manager, 618
SQLUM Requirements, 592
SSL
 Introduction to SSL, 589
 K2 Requirements for AD, 591
 SQLUM Requirements, 592
 SSL Certificates, 590
SSL Certificates, 590
SSRS, 166 , 173 , 174
Standalone Install Flow Diagram, 216-219
Standalone Install, 42
Standalone installations, 42
Start Permissions Error, 780
storage area network, 66-67
Succeeding Rule Error, 771
Summary of tool checks, 385-387
Supported Configuration, 525-529
System Event Notification, 699
System Key, 83 , 393
Task Error, 749
Task Error: System.Exemption: Error occurred adding the feature to the farm , 749
Technology Requirements, 23
temp XML, 332-336
topologies, 87 , 40-41
Troubleshooting
 Checklist: Environment Validation, 789-790
 Clearing Internet Explorer Cache, 704-706
 Configuration file changes for the K2 for Reporting Services component, 730
 Connection Errors with Unicast NLB, 713
 Enable K2 Logging, 714
 Enabling Kerberos Logging, 737
 InfoPath - An error occurred accessing a data source, 690
 InfoPath - Troubleshooting Deployment Error in K2 Studio, 702
 K2 Service will not start, 715
 Removing Internet Explorer Enhanced Security, 707
 Settings for Internet Explorer, 708
 SharePoint - Authentication is required for session error, 751
 SharePoint - Solution stays in deployment state, 752
 Slow startup for K2 components when machine has no internet access , 720-721
 SmartObjectServer Exception, 765
 Troubleshooting 401 error with Reporting Services , 731
 Troubleshooting Access Issues with K2 Reports, 732-733
 Troubleshooting Database CPU Utilization, 781
 Troubleshooting Kerberos Issues, 738

Troubleshooting using SharePoint Logs, 753
Tweaking identity cache performance for the K2 Server, 357-361
Using KerbTray to Troubleshoot Kerberos Tickets, 739
Validating the SQL Business Intelligence Development Studio, 734
Workspace Server Errors, 785-786

Troubleshooting 401 error with Reporting Services , 731

Troubleshooting Access Issues with K2 Reports, 732-733

Troubleshooting Activity Slots, 776

Troubleshooting and Resources, 188

Troubleshooting Database CPU Utilization, 781

Troubleshooting Kerberos Issues, 738

Troubleshooting Start Permissions, 780

Troubleshooting succeeding rule, 771

Troubleshooting the Succeeding Rule, 771

Troubleshooting using SharePoint Logs, 753

Troubleshooting Worklist Item Not Found, 782

Troubleshooting, 188 , 776 , 552-554 , 567-568

Troubleshooting: User Not Allowed to Open Worklist, 783

Tweaking identity cache performance for the K2 Server, 357-361

Unable to generate a temporary class, 727-728

Unattended Distributed Installation, 396

Unattended Installation Dependencies, 392

Unattended Installation using the XML File, 395

Unattended Installer - Upgrade, 397-398

Unattended Installer , 406-407

Unattended Installer additional notes, 411

Unattended Installer Dependencies, 392

Unattended Installer, 391 , 399-403 , 404-405 , 408

unhandled exception, 785-786

Uninstall Checklist , 662

Uninstall, 656 , 659

uninstalling, 662

'Unknown Error' on the K2 for SharePoint tab, 750

Unknown Error, 750

Update Group Policy, 691-692

Updating SmartObjects, 471-473

Updating the K2 License Key, 657

Upgrade K2 blackpoint > K2 blackpearl, 665-666

Upgrade K2 blackpoint, 665-666

Upgrade Options

K2 Upgrade Options, 663

Upgrade K2 blackpoint > K2 blackpearl, 665-666

Upgrading a Farm in a Distributed Environment, 667

Upgrade, 26-27 , 663

Upgrading a Farm in a Distributed Environment, 667

URL not valid, 699

Usage policy for Community Extensions, 797

User Manager

Active Directory User Manager, 609
 Adding a User to a Group , 621-622
 Adding a User to a Role, 623
 Changing the Default User Manager, 625
 Configure Environment Library, 631-632
 Configure K2 Workspace, 628-629
 Configure Out of Office, 637
 Configure Security Labels, 626-627
 Configure User Role Manager, 633-634
 Configure Windows Designer, 635-636
 Configure Workflow Server, 630
 Configuring the Active Directory User Manager,
 610-611
 Creating a user , 619-620
 Custom User Manager, 624
 Introduction to User Managers, 168-170
 SQL User Manager, 618
User Manager Cache, 168-170
User Manager Settings, 279-280
User Manager, 279-280
User not allowed to Open Worklist, 783
User Rights and Permissions, 494
User Rights Management Server, 17
User Token Flow and Terminology, 523-524
Users, 24
-using a SQL Server Instance, 490
Using KerbTray to Troubleshoot Kerberos Tickets, 739
Using SmartObjects in SharePoint, 474
Using the AD wizard on Windows 2008 and the LDAP requirement, 791
Validating the SQL Business Intelligence Development Studio, 734
Validating the Uninstall, 662
Version Support and Backwards Compatibility 2010 , 35
View Flow - Report does not display, 735
View Flow Troubleshooting, 735
View Flow validation, 366-369
Visual Studio - Invalid URI, 711
VLAN, 66-67
WCF, 31
Web Components, 18
Web Part Error, 754
**Web Parts Solution Deployment in SharePoint 2010,
 460-461**
Web Parts, 455
Web Server, 101
Web Service SmartObject
 Adding a Connection, 497
 Authentication Method, 495-496
 CRM Server Entities Selection, 516
 CRM SmartObjects, 514
 Export CRM SmartObject, 518-520
 Export SQL SmartObject, 511-513
 How to Create a SharePoint SmartObject, 467
 How to create new CRM server connection, 515

Import CRM SmartObject, 521
 Import SQL SmartObject, 510
 Introduction, 468-469
 Registration Requirements, 493
 User Rights and Permissions, 494
 -using a SQL Server Instance, 490

Web Site Name, 271-272

Web site Settings, 229-230

Web Site Virtual Directory, 271-272

Welcome Screen, 220

WF, 31

What is Kerberos, 69

What is new in this release, 6

Which Machines to Analyze, 390

Windows 7, 30

Windows Communication Foundation, 31

Windows Identity Foundation Redistributable, 88-89

Windows Integrated Authentication, 75

Windows Network Load Balancing Manager, 134-135

Windows Presentation Foundation, 31

Windows Server 2008 , 28

Windows Server 2008 and Kerberos

- Activate Delegation for the Application Pool Account, 176
- Activate delegation settings for IIS 7.0 web application , 177-179
- Farm configuration for Kerberos delegation , 182
- Kerberos for Windows Server 2008, 172
- Option 3: Utilizing the AdminPack for IIS7.0, 180-181
- Setting up SSRS with a Domain user as an application pool account, 174
- Setup Kerberos delegation for IIS 7.0, 175
- SQL Server Reporting Services, 173

Windows Server 2008 R2 , 88-89

Windows Server 2008, 88-89 , 25 , 26-27 , 117

Windows Server 2012 Configuration Requirements, 143

Windows Services Management Console, 337-339

Windows SharePoint Services (WSS), 19 , 36 , 26-27

Windows SharePoint Services, 95

Windows Vista, 30

Windows Workflow Foundation, 31

Wizard display incorrectly on vpc , 718

Wizard not displaying correctly, 718

Wizard rendering issue, 718

Word Document - Error with Word Document Conversion, 772

Word Document - Troubleshooting Error Codes for Word Document Conversion Issues, 773-774

Workflow Server, 17

Workflow unable to deploy, 700

Worklist error, 783

Workspace Application Pool Configuration, 269-270

Workspace folder permissions, 787-788

Workspace Icon, 660-661

Workspace Nodes, 370

Workspace Server Errors, 785-786

Workspace, 302-309

WPF , 31

WSS, 43-44 , 47-48

XML File Parameters, 399-403

XML file, 391

XML, 31