PERMISSIONS IN K2

2013/03/11

DOCUMENT CONTROL

Change	**Version**	**Person Responsible**
Updates from reviewers – 1st Draft	1st Draft – 5 February 2013	Andre Pretorius
Updates from MarkG	2.1 – 6 February 2013	Andre Pretorius
Updates from Johnny Fang	2.2 – 8 February 2013	Andre Pretorius

PERMISSIONS FOR INSTALLATION

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.

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 in the Getting Started Guide at: *Installation and Configuration > Installation > Post installation common tasks > K2 Environment > Adding Multiple Active Directory Domains*

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.
Permissions required to set up SQL jobs for index rebuilds	
Permission	**Used For**
sysadmin or **SQLAgentUserRole** or **SQLAgentReaderRole** or **SQLAgentOperatorRole**	The **sp_start_job** stored procedure instructs the SQL Agent to immediately execute a job, one of the permissions mentioned are needed. The **sysadmin** role can start all jobs, the **Operator** role can start all local jobs. **Reader** and **User** roles can only start jobs they own.
ALTER	To execute ALTER INDEX, at a minimum, ALTER permission on the table or view is required.

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. For information on how to set this permission, see the topic K2 Server - Configuring 'log on as service' rights.
Log on as a batch job	This permission needs to be set for PTA (pass through authentication)
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, and work with the SharePoint Workflow Integration features, 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

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 none of the OOTB reports use the SSRS server except those directly deployed to an SSRS instance and executed there.

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.
Browse rights	Users need these to execute reports.

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

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. This only applies to the SharePoint web applications on which K2 components are activated.

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. The SharePoint Service account can be added to the BUILTIN/Administrators group.
Rights	**Folder or Registry Key**
Modify	%SYSTEMROOT%\temp
Write	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\14\Layouts\Features
Write	%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\14\ISAPI

Note that the **14**\ in the folders mentioned above will be **12**\ on systems with previous versions of Microsoft SharePoint Server.

K2 Server	
Permission	**Used For**
Impersonation	Required to execute K2 components.

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 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	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

database	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

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. 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 2005 > Configuration Tools > Reporting Services Configuration)
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)
6. Close the Reporting Services Configuration Manager window
7. 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

POST INSTALLATION PERMISSION SETTINGS

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 View	N/A
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	Specifies under K2 site settings	Be assigned an Approve workflow task by the Out 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 activated; access to SharePoint Central Admin	N/A	N/A
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 service in his Personal certificate store.	N/A
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 the troubleshooting topic: “Using the AD wizard on Windows 2008 and the LDAP requirement” in the Getting Started Guide online help.	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.

For permissions and rights necessary for the K2 OOTB service objects, please see the online documentation http://help.k2.com/helppages/k2blackpearlUserGuide4.6.4/webframe.html#Reference-WS_MCon-SO_Services.html under the section **Management and Administration** > **Workspace Management** > **Management Console** > **SmartObject Services** > **Management Console: SmartObject Services**.

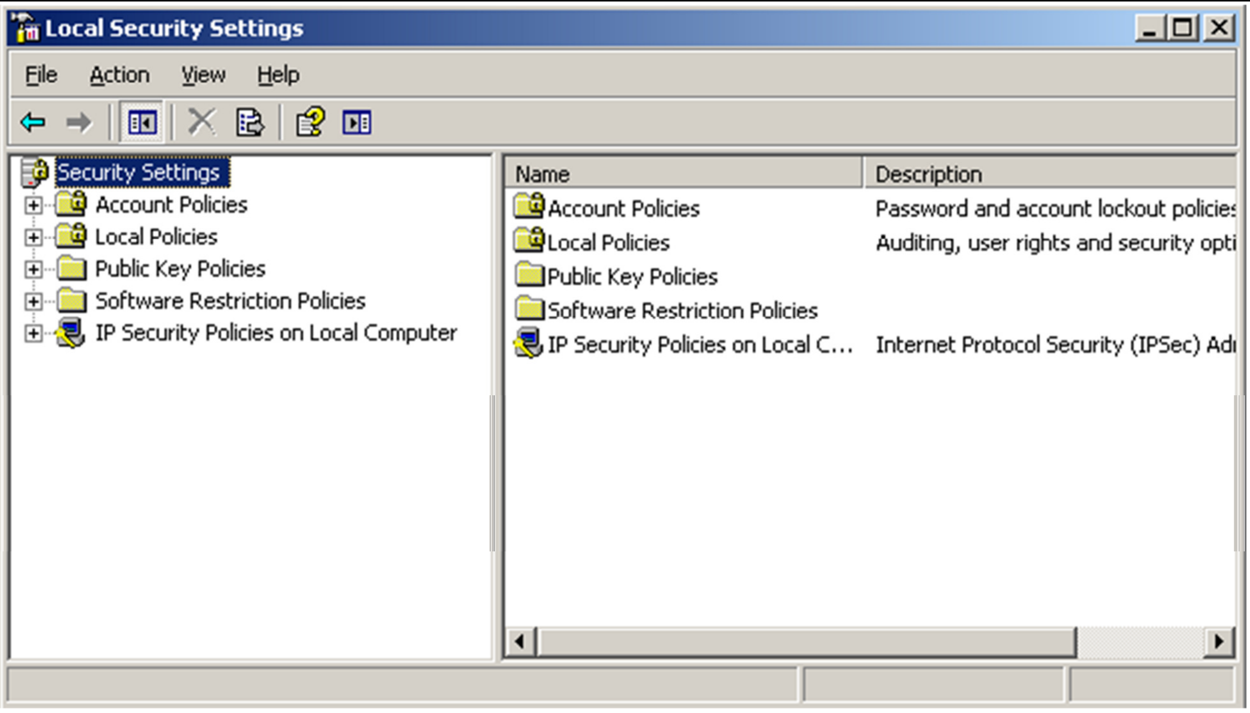
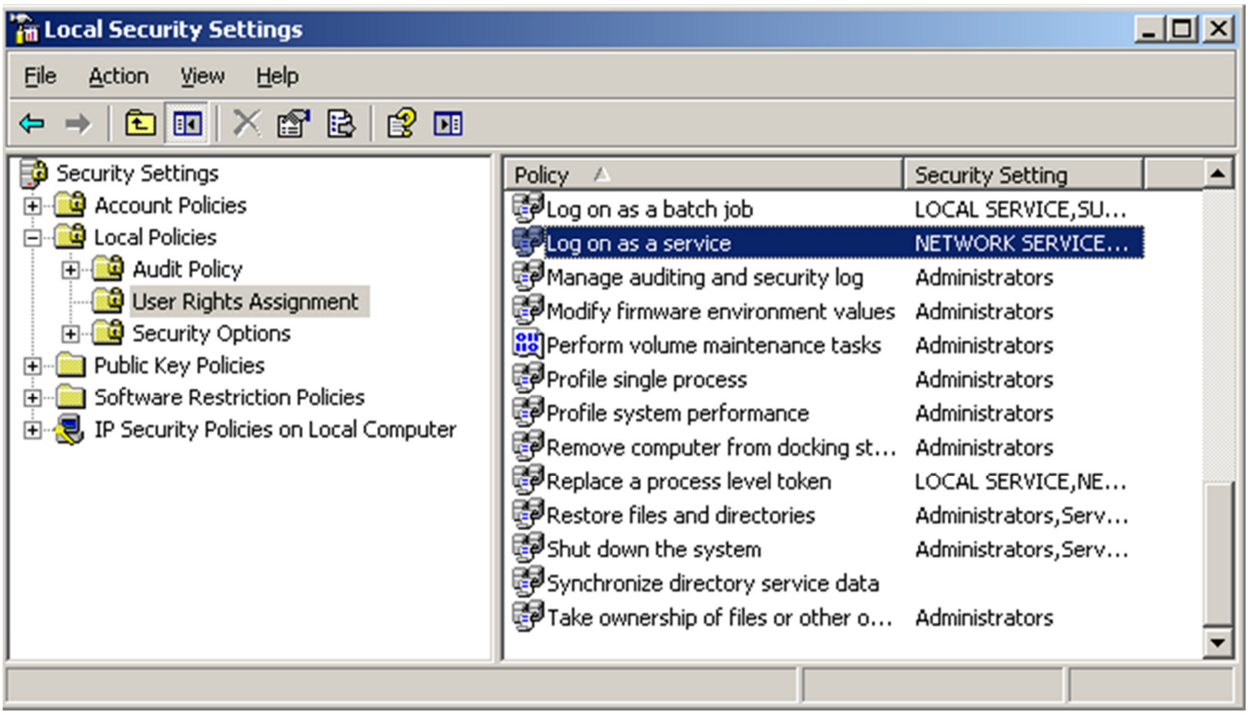
K2 Server – Configuring ‘log on as service’ rights

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

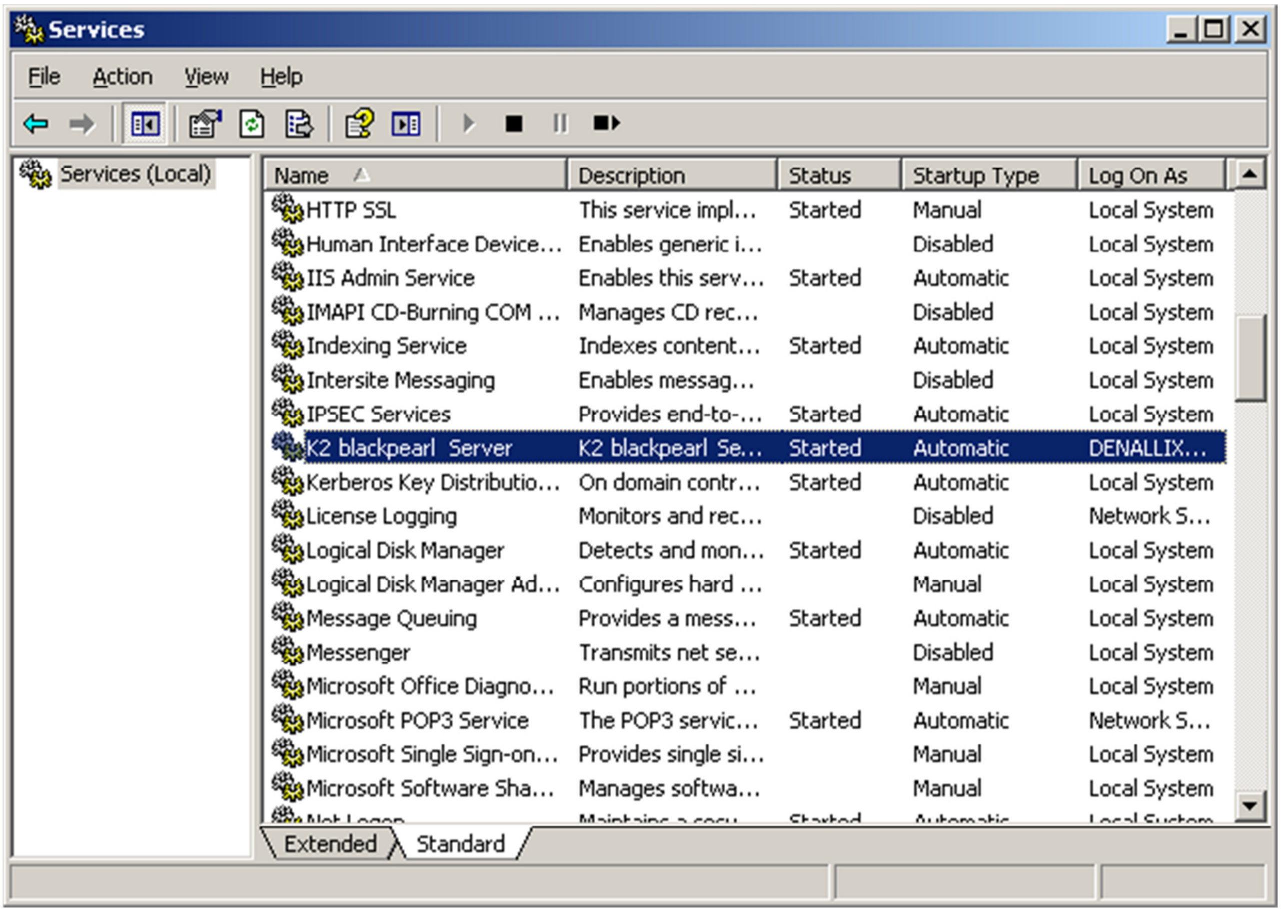
	 Security Settings Account Policies Local Policies Public Key Policies Software Restriction Policies IP Security Policies on Local Computer Name — Description Account Policies — Password and account lockout policies Local Policies — Auditing, user rights and security opti Public Key Policies Software Restriction Policies IP Security Policies on Local C... — Internet Protocol Security (IPSec) Adı
2	Expand the Local Policies node, then click on the User Rights Assignment node  Security Settings Account Policies Local Policies Audit Policy User Rights Assignment Security Options Public Key Policies Software Restriction Policies IP Security Policies on Local Computer 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
4	Click the **Add User or Group** button, enter domain\K2 Service Account in the Names to select text box and click OK

5 Click **OK** on the Log in as a service Properties dialog and then close Local Security Settings window

Using the Windows Services Management Console

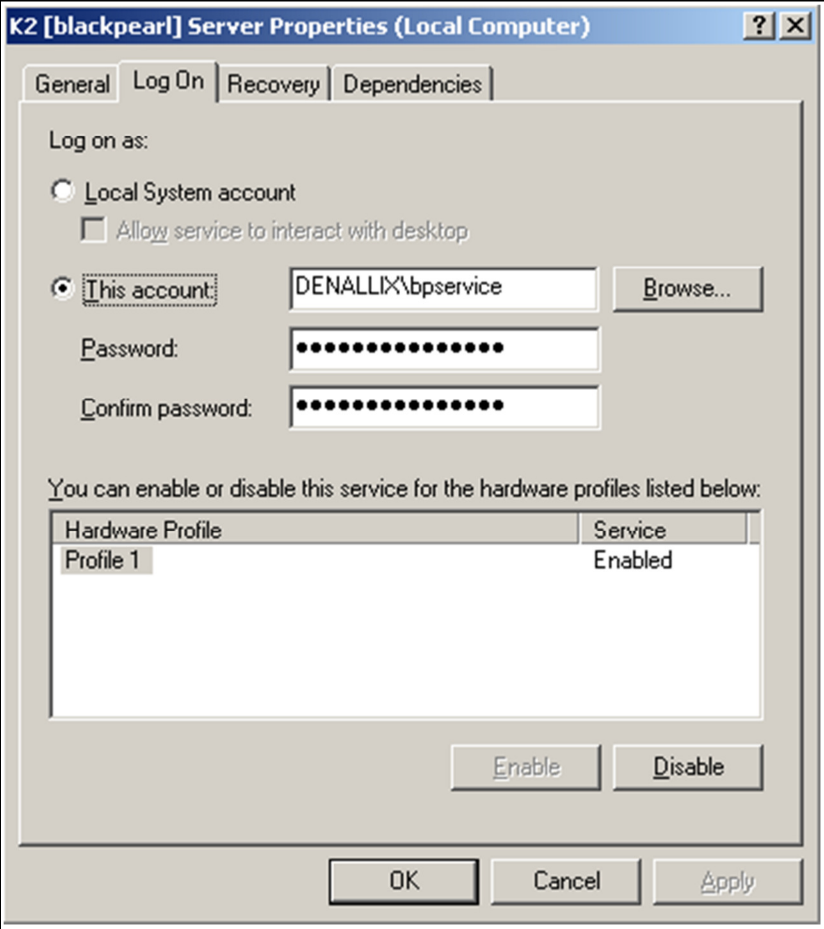
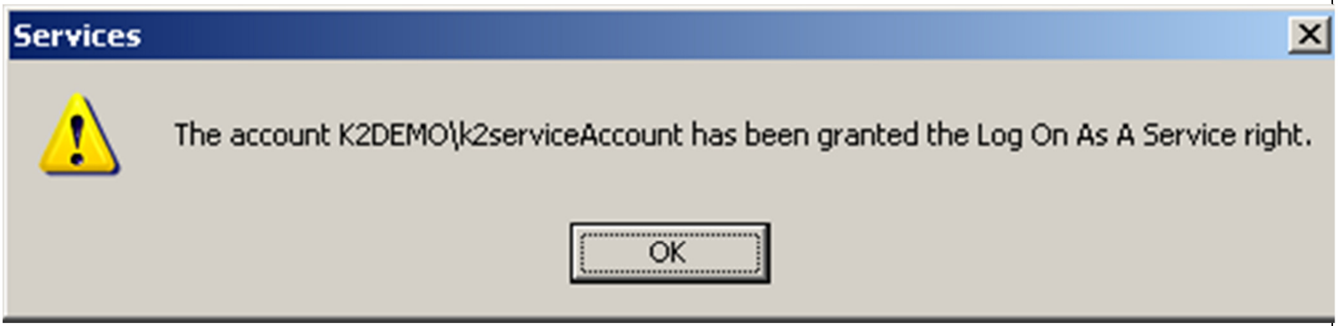
After K2 blackpearl has been installed, you will see the K2 blackpearl Server Service listed in the Services running on the K2 Server. You can then grant the Log on as a Service right by performing the following steps:

1 Open the Services console by clicking Start > Administrative Tools > Services



Name	Description	Status	Startup Type	Log On As
HTTP SSL	This service impl...	Started	Manual	Local System
Human Interface Device...	Enables generic i...		Disabled	Local System
IIS Admin Service	Enables this serv...	Started	Automatic	Local System
IMAPI CD-Burning COM ...	Manages CD rec...		Disabled	Local System
Indexing Service	Indexes content...	Started	Automatic	Local System
Intersite Messaging	Enables messag...		Disabled	Local System
IPSEC Services	Provides end-to-...	Started	Automatic	Local System
K2 blackpearl Server	K2 blackpearl Se...	Started	Automatic	DENALLIX...
Kerberos Key Distributio...	On domain contr...	Started	Automatic	Local System
License Logging	Monitors and rec...		Disabled	Network S...
Logical Disk Manager	Detects and mon...	Started	Automatic	Local System
Logical Disk Manager Ad...	Configures hard ...		Manual	Local System
Message Queuing	Provides a mess...	Started	Automatic	Local System
Messenger	Transmits net se...		Disabled	Local System
Microsoft Office Diagno...	Run portions of ...		Manual	Local System
Microsoft POP3 Service	The POP3 servic...	Started	Automatic	Network S...
Microsoft Single Sign-on...	Provides single si...		Manual	Local System
Microsoft Software Sha...	Manages softwa...		Manual	Local System
Net Logon	Maintains a secu...	Started	Automatic	Local System

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:

	 K2 [blackpearl] Server Properties (Local Computer) General | Log On | Recovery | Dependencies Log on as: ○ Local System account □ Allow service to interact with desktop ● This account: DENALLIX\bpservice [Browse...] Password: ••••••••••••••• Confirm password: ••••••••••••••• You can enable or disable this service for the hardware profiles listed below: Hardware Profile: Profile 1 — Service: Enabled [Enable] [Disable] [OK] [Cancel] [Apply]
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  Services The account K2DEMO\k2serviceAccount has been granted the Log On As A Service right. [OK]

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	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 2005 > Configuration Tools > Reporting Services Configuration)
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)
⑥	Close the Reporting Services Configuration Manager window

⑦	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

There have been reports of the Configuration Manager not retrieving the list of SSRS sites correctly. This might be related to the *SecureConnectionLevel* setting in the RSReportServer.config file.

```
<Add Key="SecureConnectionLevel" Value="0"/>
```

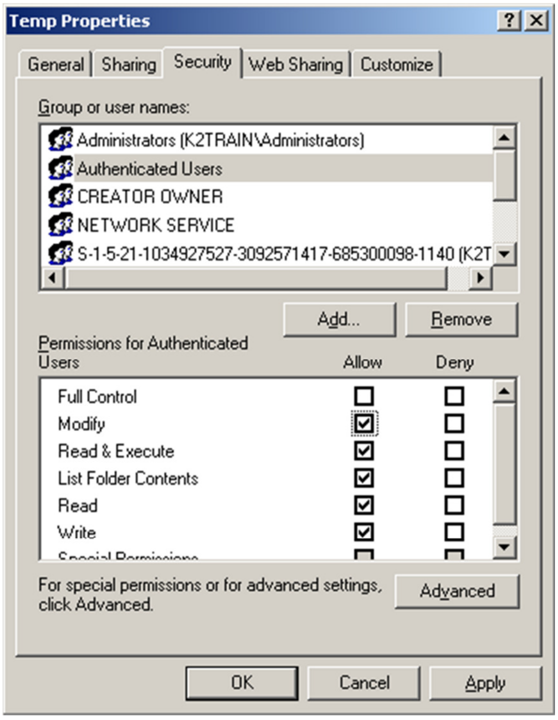
Depending on the SSRS setup, if SSL is specified, the value can get set to either 2 or 3 (see http://technet.microsoft.com/en-us/library/cc304416.aspx for description of value settings). Try setting this back to 0 if you are having difficulty getting the list of SSRS sites to populate correctly.

For information on setting up IIS 7.0, SSRS 2008 with Kerberos in a distributed environment with host headers, see the article: “Some differences when configuring Kerberos with Host Headers on a SSRS 2008 Setup with 0807v3.0 on Windows 2008” (http://www.k2underground.com/blogs/johnny/archive/2009/08/19/some-differences-when-configuring-kerberos-with-host-headers-on-a-ssrs-2008-setup-with-0807v3-0-on-windows-2008.aspx)

IIS Server – Modify permissions on Temp folder

Because we are using Integrated Authentication for stronger security, we need to assign all authenticated users Modify permissions on the temporary folder. This folder is used at runtime by the web site, and if all users do not have access to this folder, they cannot interact with items.

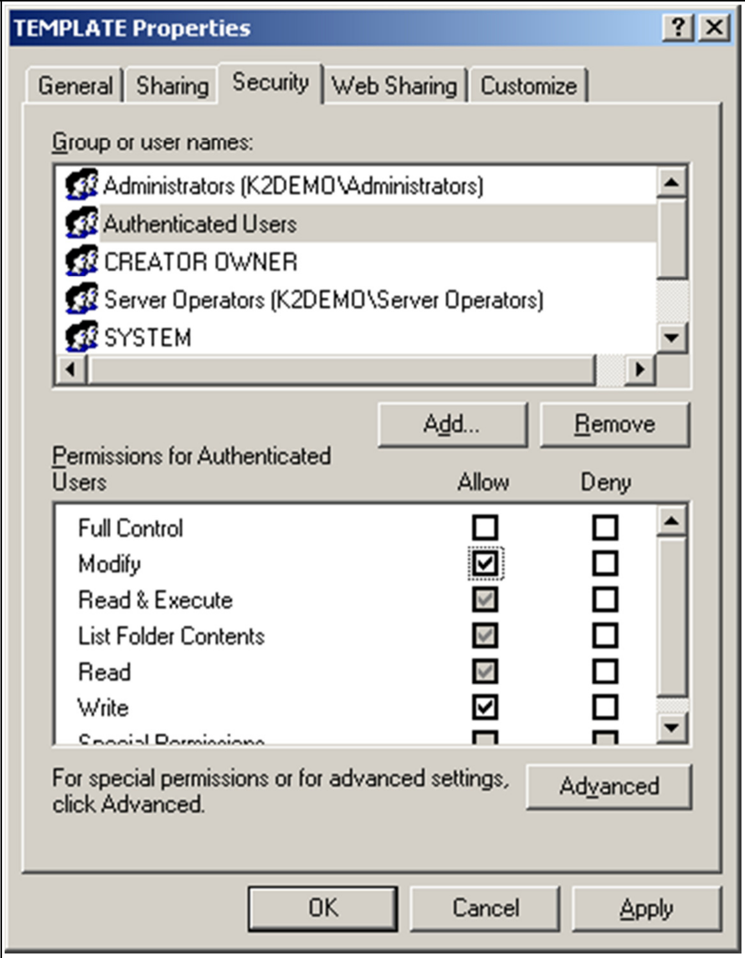
①	Open Windows Explorer and browse to **C:\Windows\**
②	Scroll down to the **Temp** folder, right-click on it and select **Properties**
③	On the Security tab, select the **Authenticated Users** in the group list, and check the **Modify** check box If the Authenticated Users group is not listed, click 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

	 Temp Properties General Sharing Security Web Sharing Customize Add... Remove Advanced OK Cancel Apply Group or user names: Administrators (K2TRAIN\Administrators) Authenticated Users CREATOR OWNER NETWORK SERVICE S-1-5-21-1034927527-3092571417-685300098-1140 (K2T Permissions for Authenticated Users — Allow / Deny Full Control □ □ Modify ☑ □ Read & Execute ☑ □ List Folder Contents ☑ □ Read ☑ □ Write ☑ □ Special Permissions □ □ For special permissions or for advanced settings, click Advanced.
4	Click **OK**, and when prompted, click **Yes.** Also, be sure that the Service Accounts have been set up properly.

SharePoint Server - Template folder

In order to deploy SharePoint Workflow Integration processes, all authenticated users will need permissions on the SharePoint Template folder. This directory is used to deploy the workflow features, and without permission, SharePoint Workflow Integration processes will not deploy properly.

1	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.
2	Scroll down to the **TEMPLATE** folder, right-click on it and select **Properties**
3	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



TEMPLATE Properties

Group or user names:

- Administrators (K2DEMO\Administrators)
- Authenticated Users
- CREATOR OWNER
- Server Operators (K2DEMO\Server Operators)
- SYSTEM

Permissions for Authenticated Users	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐
Special Permissions	☐	☐

For special permissions or for advanced settings, click Advanced.

4	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.

SharePoint Server - Database Permissions

✎	This step requires that the user logging in to SQL Server Management Studio has sufficient permissions to grant permissions to other user accounts.

The account running the K2 installation requires permissions on the SharePoint_AdminContent_[GUID ID] database. These permissions must be set **before** (refer to SharePoint Services Account under the Permissions for install section) 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_[GUI ID] *
Service Account	K2Service **
Permissions Requirement	• 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_AdminConent_[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

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: • Install the K2 for SharePoint files on SharePoint Web Front-Ends • Deploy K2 Solutions to SharePoint Farm	• Domain user account (Note: This should not be the SharePoint System Administrator Account) • Member of the SharePoint Farm Administrators group ○ 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: ○ SharePoint Configuration Database[SharePoint_Config]
K2 Central Admin	The K2 Central Admin account is used to perform the following tasks: • Use links on the K2 for SharePoint admin page (does not include K2 Designer for SharePoint links)	• Full Control permissions on the Central Admin Site Collection is required to open the page. • Admin rights on K2 server ○ 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: • Use links on the K2 Site Settings page	• 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: • Create/Modify/Delete Webs • Create/Modify/Delete Lists and Libraries • Create/Modify/Delete List Items and Documents • Create/Modify/Delete	• 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	The K2 Runtime Services Application Pool account is used to perform the following tasks: • Interact with K2 processes at runtime via Web services	• Impersonate rights on K2 server
K2 Thick-client Designers (K2 Studio, K2 for Visual Studio)	The account of the person using the thick-client designer is used to perform the following tasks: • Deploy SharePoint Workflow Integration designed processes	• The thick-client designer account requires the following security configuration. ○ 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. ○ SharePoint Farm Administrators group membership ○ Full Control permission on the Site Collection ○ Modify rights on the Features folder on the SharePoint web front ends

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: • Activate features and K2 site settings	All K2 for SharePoint Core permissions, plus the following: • Full Control permission on the default or selected Site Collection is required to open the page. o Activating All K2 Features o Creating and configuring hidden K2 lists o 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) o securityadmin (required on K2 Server and SharePoint Server) o dbcreator (required on K2 Server and SharePoint Server) o 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: • Navigate to K2 Designer links on the K2 for SharePoint admin page	• Full Control permissions on the Central Admin Site Collection is required to open the page. • Admin rights on K2 server o Retrieving Host Server configuration settings • SQL Server server role on K2Server o securityadmin o dbcreator or o 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 following tasks: • Deploy K2 Designer for	The following security configurations are done automatically when the Deployment Application Pool account is configured: • SharePoint Farm Administrators group membership (this permission is needed for deployment of processes only, not their execution) • Site Collection Administration

	SharePoint designed processes **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. With SPWFI version 2 this is no longer a requirement. 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. 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.	• Export rights on K2 server • SQL Server database role -- db-owner (Server > Databases > {database name} > Security > Logins): o 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): o SharePoint Central Admin content database o SharePoint Shared Services content database o SharePoint Site Collection content database o SharePoint Configuration database o 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	Users in the K2 Designer for SharePoint groups can perform the following tasks:	• 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.

	• Access the Create K2 Process menu to design and deploy a process with K2 Designer for SharePoint	• 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 Participant	Users in the Process Participant groups can perform the following tasks: • Participate in deployed K2 processes	• 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 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.

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	Reader	Server Admin, Process Admin

Detail		
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

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.

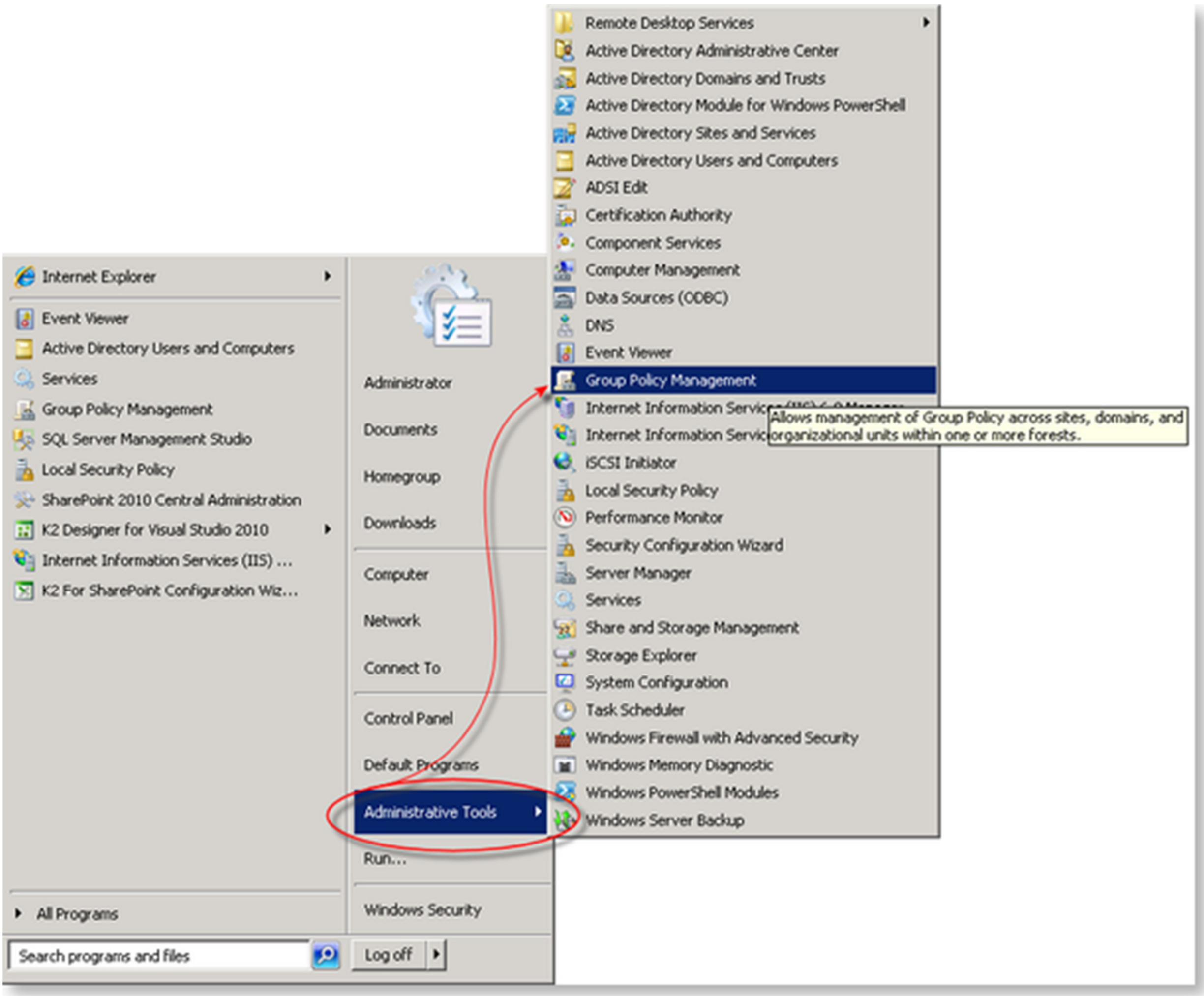
For further information on the LOGON32_LOGON_BATCH method used, see the topics **Machine Interaction** (K2 blackpearl user guide: Designing > Designers > K2 Designer for Visual Studio > Design Tools > Toolbox > Event Wizards > Server Events > Run As > Run time vs Design Time > Machine Interaction) and **Local Security Policy** (K2 blackpearl user guide: Designing > Designers > K2 Designer for Visual Studio > Design Tools > Toolbox > Event Wizards > Server Events > Run As > Security Considerations > Local Security Policy).

Prerequisites

A 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 ...

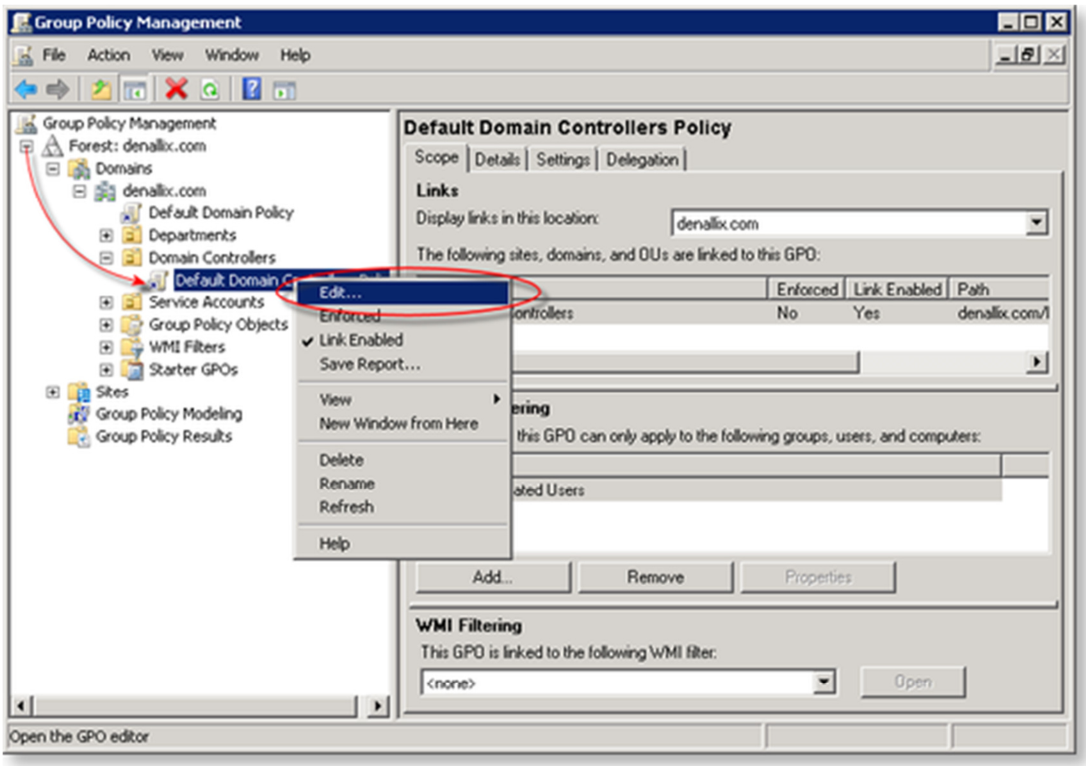
The steps below make user of a User Account called RunAsUser which will be added to the Group Policy to enable the **Machine Interaction**: LOGON32_LOGON_BATCH.

1	Click on Start > Administration Tools > Group Policy Management 

Internet Explorer
Event Viewer
Active Directory Users and Computers
Services
Group Policy Management
SQL Server Management Studio
Local Security Policy
SharePoint 2010 Central Administration
K2 Designer for Visual Studio 2010
Internet Information Services (IIS) ...
K2 For SharePoint Configuration Wiz...
All Programs
Search programs and files
Administrator
Documents
Homegroup
Downloads
Computer
Network
Connect To
Control Panel
Default Programs
Administrative Tools
Run...
Windows Security
Log off
Remote Desktop Services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Data Sources (ODBC)
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) 6.0 Manager
Internet Information Servic
iSCSI Initiator
Local Security Policy
Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell Modules
Windows Server Backup

Allows management of Group Policy across sites, domains, and organizational units within one or more forests.

2 Once the Group Policy Management Editor opens, locate the Default Domain Controller policy, right click and select **Edit...**



Default Domain Controllers Policy

Display links in this location: denallix.com

The following sites, domains, and OUs are linked to this GPO:

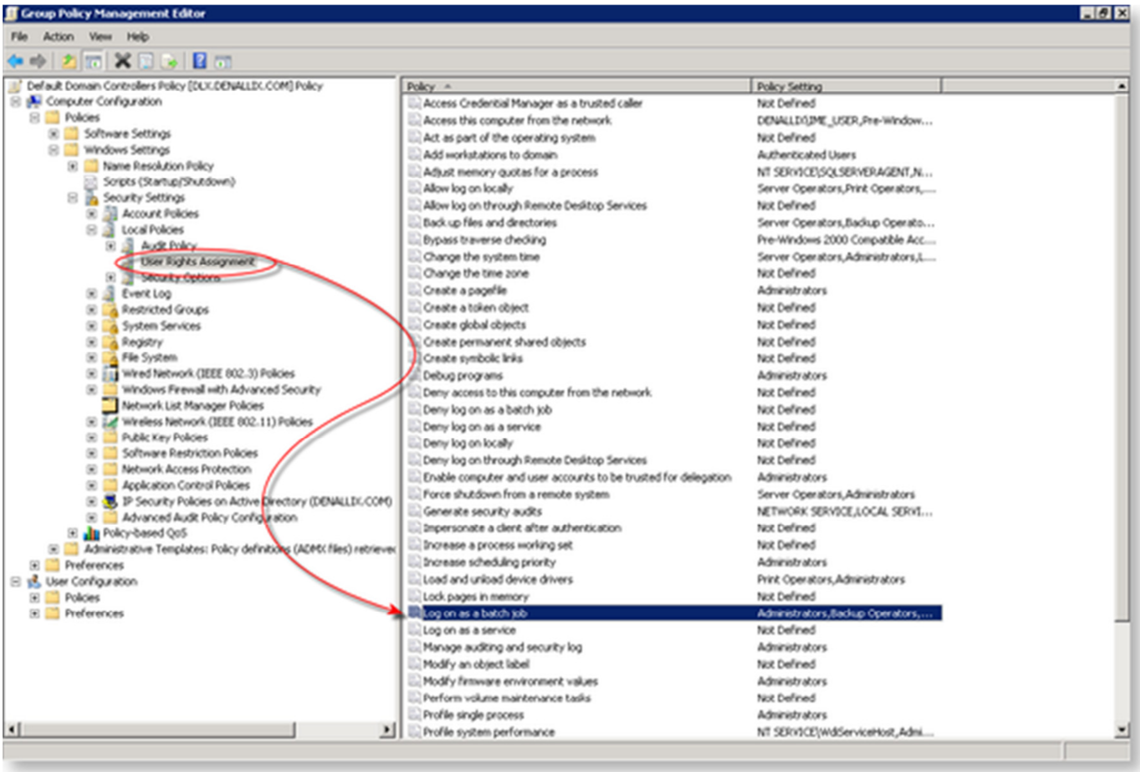
	Enforced	Link Enabled	Path
...ontrollers	No	Yes	denallix.com/I

...this GPO can only apply to the following groups, users, and computers:

...ated Users

This GPO is linked to the following WMI filter: <none>

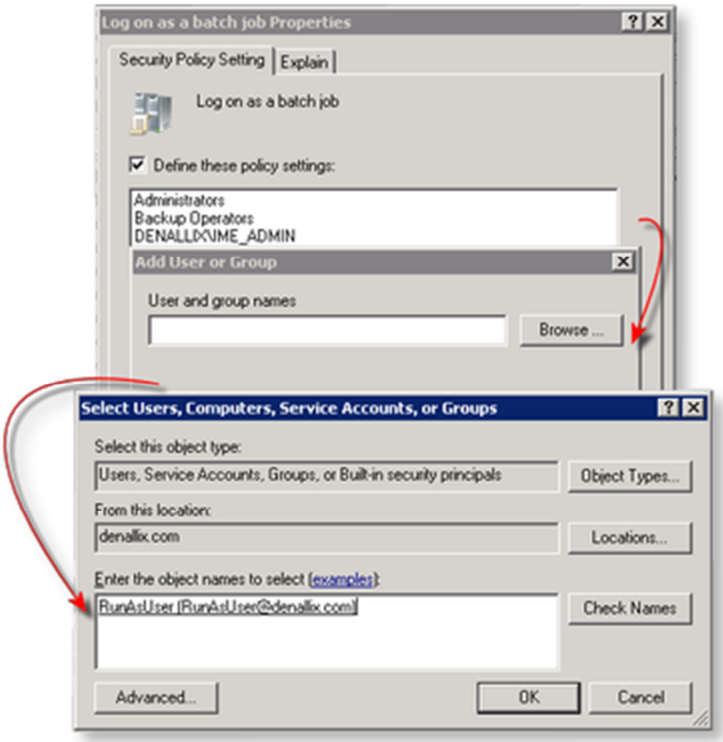
3 Expand the Computer Configuration nodes as shown in the image (click on the link) and then select User Rights Assignment > Logon As Batch Job


Group Policy Management Editor
File
Action
View
Help
Default Domain Controllers Policy [DLX.DENALLIX.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (DENALLIX.COM)
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrievec
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	DENALLIX\IME_USER,Pre-Window...
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	NT SERVICE\SQLSERVERAGENT,N...
Allow log on locally	Server Operators,Print Operators,...
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Server Operators,Backup Operato...
Bypass traverse checking	Pre-Windows 2000 Compatible Acc...
Change the system time	Server Operators,Administrators,L...
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from a remote system	Server Operators,Administrators
Generate security audits	NETWORK SERVICE,LOCAL SERVI...
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Administrators
Load and unload device drivers	Print Operators,Administrators
Lock pages in memory	Not Defined
Log on as a batch job	Administrators,Backup Operators,...
Log on as a service	Not Defined
Manage auditing and security log	Administrators
Modify an object label	Not Defined
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Not Defined
Profile single process	Administrators
Profile system performance	NT SERVICE\WdiServiceHost,Admi...

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**



Log on as a batch job Properties

Log on as a batch job

☑ Define these policy settings:

Administrators
Backup Operators
DENALLIX\ME_ADMIN

Add User or Group

User and group names:

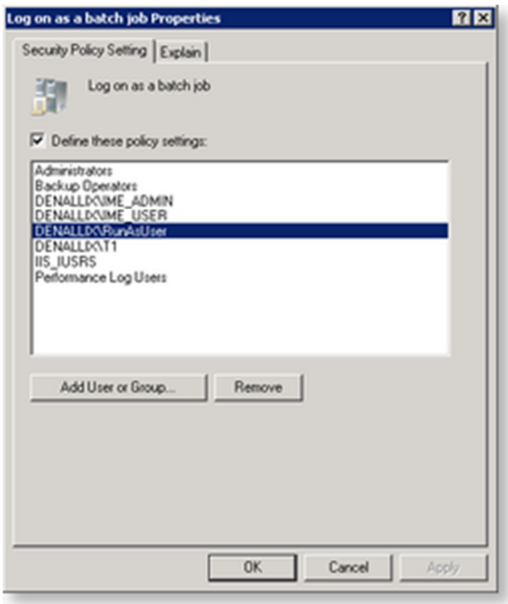
Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
denallix.com

Enter the object names to select (examples):
RunAsUser (RunAsUser@denallix.com)

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.



Log on as a batch job Properties

Log on as a batch job

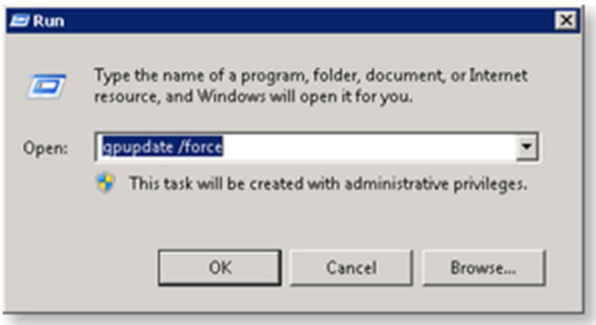
☑ Define these policy settings:

Administrators
Backup Operators
DENALLIX\ME_ADMIN
DENALLIX\ME_USER
DENALLIX\RunAsUser
DENALLIX\T1
IIS_IUSRS
Performance Log Users

Depending on the environment, the changes may propagate quickly, and in some cases take longer. The changes will not take effect immediately unless forced.

To force the update do the following:

1. Click on **Start** > **Run**
2. Enter **gpupdate** /**force**
3. Click **Ok**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpupdate /force

This task will be created with administrative privileges.

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	Admin Impersonate

Manual Configuration

In the table below, the additional permissions required are listed:

Necessary Permissions	
SharePoint Application Pool	Admin Impersonate Export

K2 Workspace Application Pool	• Admin • Impersonate
K2 Administration Account	• Admin
Developer Accounts	• 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**

K2 RUNTIME PERMISSIONS

Be sure to consult the table under the Required Permissions for K2 Components heading for the list of permissions necessary for managing K2.

ACTIVE DIRECTORY

In order for the K2 Active Directory Events to perform the action that has been configured, the correct user permissions must be available to the action. There are two possible ways to provide these:

1) The K2 Service account needs to have at least Account Operator permissions, i.e. be a part of the Account Operator group.

OR

2) The wizard needs to be configured with the credentials of a user that has at least Account Operator permissions.

Be aware that Account Operators can't manage the Administrator user account, the user accounts of administrators, or the group accounts Administrators, Server Operators, Account Operators, Backup Operators, and Print Operators. Account Operators also can't modify user rights.

If you wish to use the wizard to perform any of these tasks, you will need to give the K2 Service Account Administrator permission, or run the Wizard as a user with Administrator permissions. However, it is advised that great care be taken when adding users to this group (See http://technet.microsoft.com/en-us/library/bb726982.aspx)

> If the K2 Service account does not have Account Operator permissions and you manually add them, the K2 Host Server needs to be restarted before the changes will be in effect. This is needed because the server caches the K2 Service Account credentials.

K2 FOR SHAREPOINT PROCESS PORTALS - PROCESS RIGHTS

The K2 for SharePoint Process Portal solution is deployed during the installation of K2 blackpearl. Once the solution has been deployed, a SharePoint user may create a K2 Process Portal site to manage the processes that they have rights to.

A K2 Process Portal allows users and managers to access and manage business critical process information. Some of the features of the K2 Process Portal include:

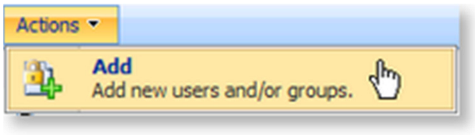
- the ability to manage and access process information from within SharePoint Server
- the ability to view all information pertaining to one process and all its instances
- valuable information translated into easy to use reports
- Process Instance Management, Reports, Worklists and Administration pertaining to a specific process in one location

A K2 Process Portal can be configured for a single process, or for multiple K2 processes.

The Security node allows a manager to **Add**, **Edit**, and **Remove** users' process permissions. Process user permissions control the extent to which users or groups are able to interact with the process - enabling them to have full view of the process or limiting them to their worklist only.

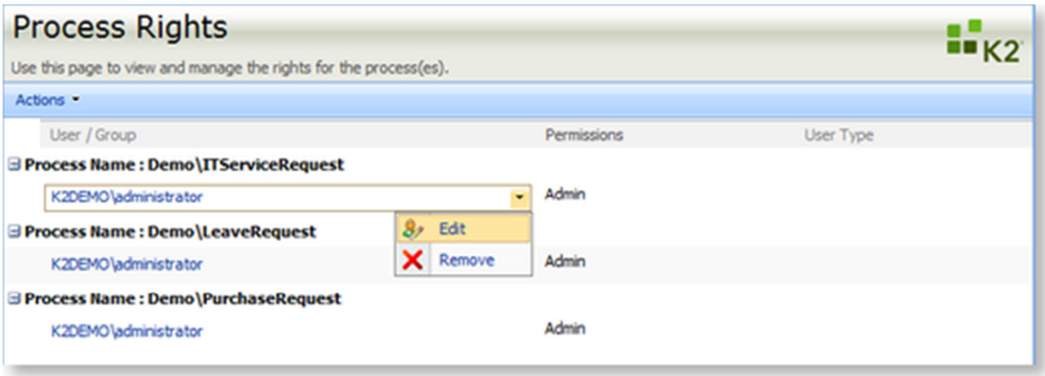
Add Permissions for a User or Group

To add process user permissions click on the Actions drop-down and select **Add**.



Edit User Process Permissions

To edit a user's process permissions click on the user link under the required process name and select **Edit**.

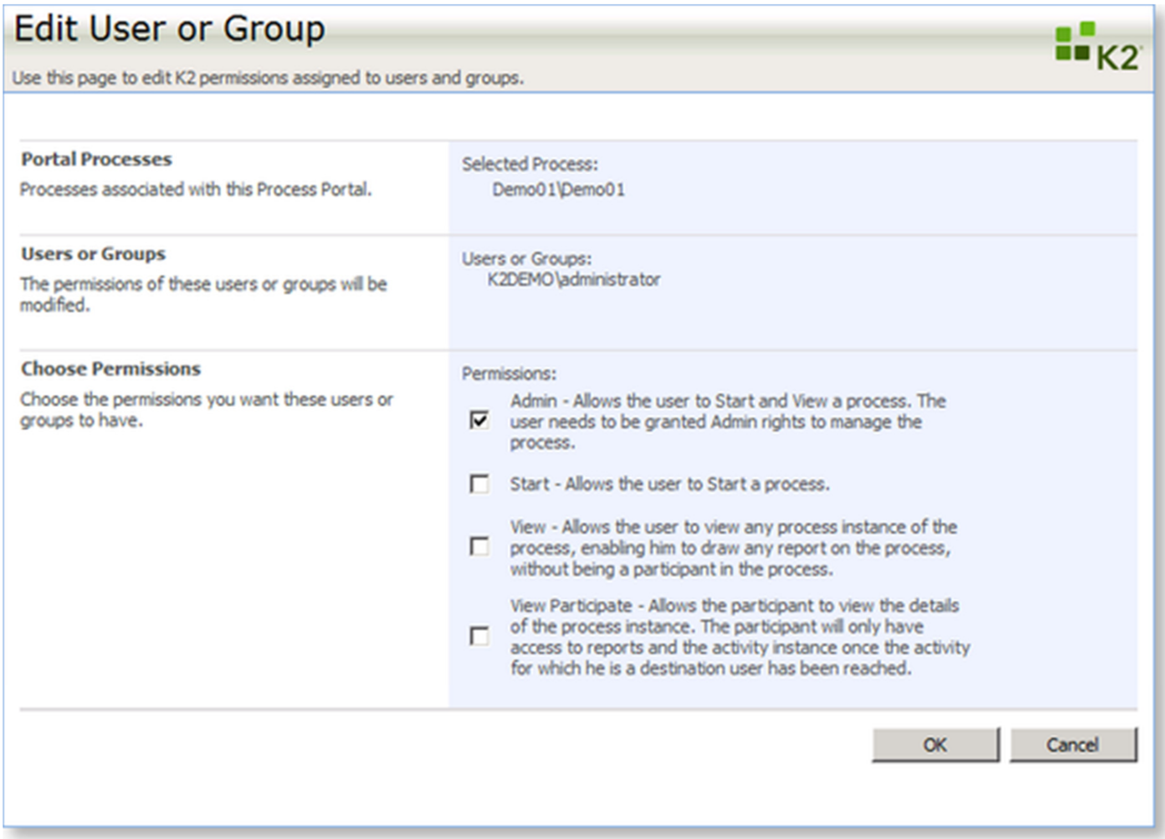


Process Rights

Use this page to view and manage the rights for the process(es).

User / Group	Permissions	User Type
Process Name : Demo\ITServiceRequest		
K2DEMO\administrator	Admin	
Process Name : Demo\LeaveRequest		
K2DEMO\administrator	Admin	
Process Name : Demo\PurchaseRequest		
K2DEMO\administrator	Admin	

Now select the required level of user process permissions and click on **OK**.



Edit User or Group

Use this page to edit K2 permissions assigned to users and groups.

Portal Processes
Processes associated with this Process Portal.

Selected Process:
Demo01\Demo01

Users or Groups
The permissions of these users or groups will be modified.

Users or Groups:
K2DEMO\administrator

Choose Permissions
Choose the permissions you want these users or groups to have.

Permissions:

☑ Admin - Allows the user to Start and View a process. The user needs to be granted Admin rights to manage the process.

☐ Start - Allows the user to Start a process.

☐ View - Allows the user to view any process instance of the process, enabling him to draw any report on the process, without being a participant in the process.

☐ View Participate - Allows the participant to view the details of the process instance. The participant will only have access to reports and the activity instance once the activity for which he is a destination user has been reached.

K2 blackpearl User Permissions

Permission	Description
Admin	Allows the user to **Start** and **View** a process. The user needs to be granted **Admin** rights to manage the process from the Management Console within the Administration node
Start	Allows the user to start a process - without it the user will receive an error if attempting to start a process
View	Allows the user to view any process instances of the process, enabling them to draw any report on the process in K2 Workspace, without being a participant in the process
View Participate	Allows a participant, i.e. the user defined as the destination user for one of the process activities, to view the details of the process instance. The user will only be able to access process reports and the activity instance once it has reached the activity for which they are a destination user

Remove a User from the Process Permissions View

To completely remove a user's process permissions click on the user link under the required process name and select **Remove**

> Process Rights can be assigned to Active Directory Users or Groups. In addition, Process Rights can be assigned to **SharePoint Groups** which contain AD Groups and Users.

EXCHANGE SERVER

Exchange Event Wizard - Overview

For most enterprises, e-mail is the mission-critical communication tool that allows their employees to produce their work. This greater reliance on e-mail has increased the number of messages sent and received, the variety of work getting done, and even the speed of business itself. Microsoft Exchange Server meets these challenges and addresses the needs of the different groups who have a stake in the messaging system.

The K2 Exchange Event Wizard was created to make the configuration and use of the Microsoft Exchange Server a part of the workflow process. It provides the workflow creator with the ability to create and disable mailboxes on the Microsoft Exchange Server, and to create meeting requests and tasks as part of a K2 Process.

> The Exchange Event Wizard requires Microsoft Exchange Management Tools from the Microsoft Exchange Server 2007 SP2 or SP3 installer.

Permissions

The K2 Service Account must have View-Only Administrator rights on the Microsoft Exchange Server.

In the Object Browser, in order to be able to expand the Exchange Server field into the Storage Group and Mailbox Database nodes, the K2 Service account will need Exchange View Only Administrator rights.

To be able to execute the Create Mailbox and Disable Mailbox actions, the Exchange Event should be configured to run as a service or user account with Exchange Organization Administrator rights.

To be able to execute the Send Meeting Request and Send Task actions the Exchange Event should be configured to run as a service or user account with impersonation rights and NOT Exchange Organization Administrator rights. The service or user account should also have a trusted server certificate from the Exchange web service in his Personal certificate store.

Troubleshooting

If the Microsoft Exchange Server that is configured for a particular K2 Exchange action is not available on the network during the runtime of the event, the process will enter an error state. If the process is in error state, make sure that the Exchange Server is started and available and then retry the process.

Exchange Wizard - Design-time Operational Rights

The K2 Service Account needs Exchange View-Only Administrator rights. These rights are needed because the K2 Studio Object Browser uses the K2 Service account to view the Storage Groups and Mailbox Databases on an Exchange server.

In order for these rights to take effect, the K2 Server needs to be restarted.

Rights Specific to Microsoft Exchange 2010

INSTALLATION ACCOUNT

This account should have View-Only rights for Exchange to be able to browse Exchange servers and mailbox databases.

Also give the account Execute rights on the Microsoft.PowerShell configuration, by running the following command in the Exchange Management Shell:

Set-PSSessionConfiguration Microsoft.PowerShell –ShowSecurityDescrtiptorUI

K2 SERVICE ACCOUNT

This account should have Recipient Management rights for Exchange to be able to create and disable mailboxes and browse Exchange servers and mailbox databases.

Also give the account Execute rights on the Microsoft.PowerShell configuration, by running the following command in the Exchange Management Shell:

Set-PSSessionConfiguration Microsoft.PowerShell –ShowSecurityDescrtiptorUI

IMPERSONATION ACCOUNT

This account should be assigned the Application Impersonation role to be able to impersonate users for sending meeting requests and creating tasks.

Run the following command in the Exchange Command Shell to give impersonation rights:

new-ManagementRoleAssignment -Name: _suImpersonateRoleAsg -Role: ApplicationImpersonation -User: "impersonation account name"

Give this account "Log on as batch job" rights on the K2 Server machine to be able to run Exchange Events as this account.

CONFIGURING WINRM

The following commands should be run through the Exchange Management Shell on the Exchange server machine:

Enable-PSRemoting

Set-Item wsman:\localhost\client\trustedhosts "k2server machine fan"

Configure IIS on the Exchange server machine:

By default, WinRM uses http and connects through the Default Web Site on port 80.

Add bindings to http port 80, with no host name and All Unassigned if they don't exist.

\PowerShell should not have SSL enabled.

\PowerShell should have only anonymous access enabled.

TROUBLESHOOTING

To resolve possible connection issues with WinRM, try the following:

On the Exchange server, edit group policy and under Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service, set IPv4 & IPv6 filters = *

IPv6 should be enabled

On the K2 server machine, run the following cmd let in PowerShell

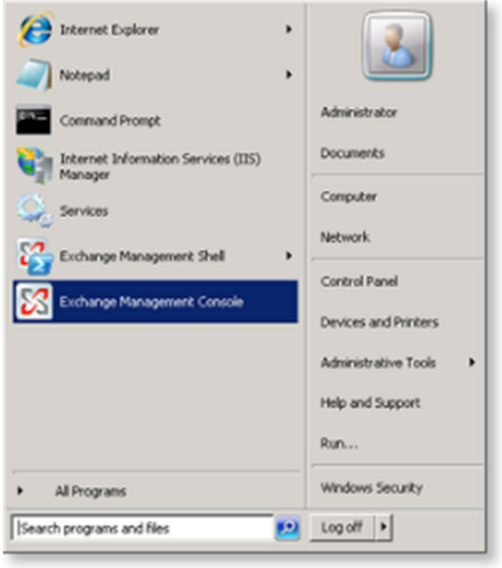
Set-ExecutionPolicy Unrestricted

PowerShell can't connect to host headers, so the Exchange certificate should be issued to the Exchange server machine name and the Exchange service instances should point to the machine name as well

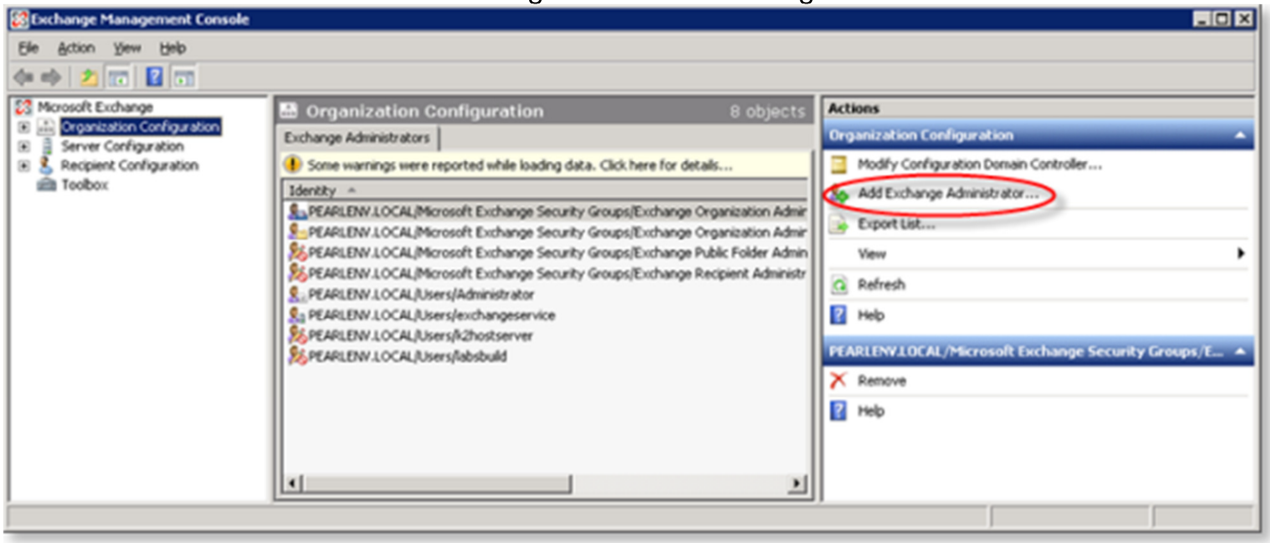
Exchange Organization and View-Only Administrator Rights

Configuring Exchange Organization and View-Only Administrator rights can be done through the Exchange Management Console:

1. Open the Exchange Management Console



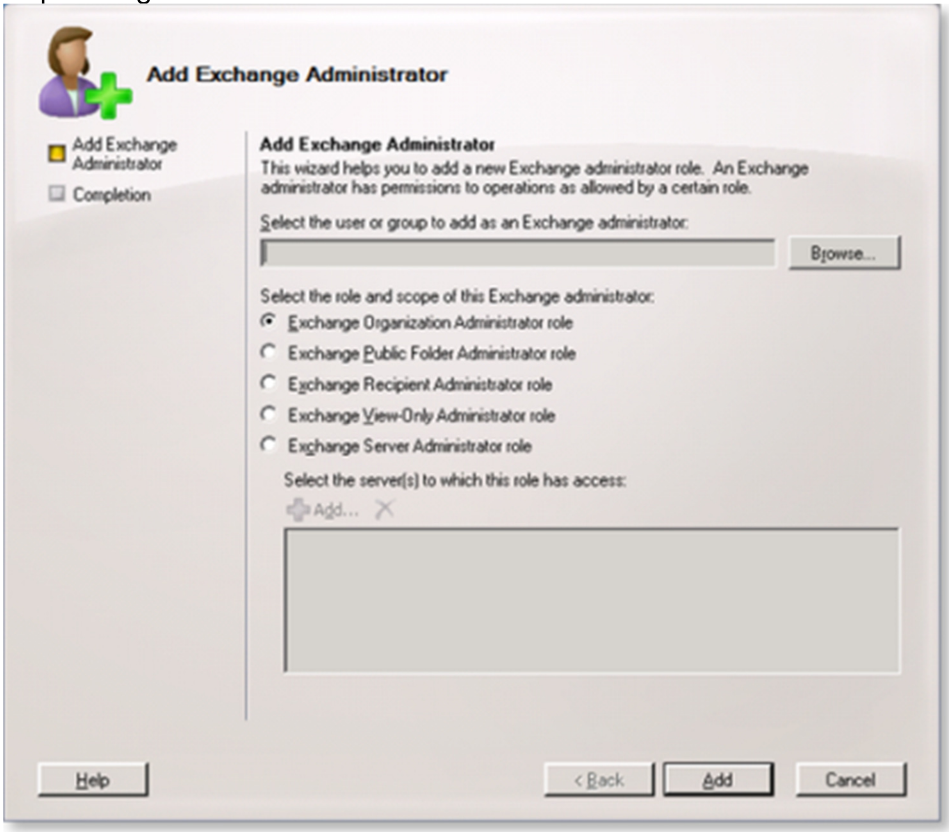
2. Select the user account that will be configured with the new rights


Exchange Management Console
File Action View Help
Microsoft Exchange
Organization Configuration
Server Configuration
Recipient Configuration
Toolbox
Organization Configuration
8 objects
Exchange Administrators
Identity
Actions
Organization Configuration
Modify Configuration Domain Controller...
Add Exchange Administrator...
Export List...
View
Refresh
Help
PEARLENV.LOCAL/Microsoft Exchange Security Groups/E...
Remove
Help

Some warnings were reported while loading data. Click here for details...

Identity
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Organization Admir
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Organization Admir
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Public Folder Admin
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Recipient Administr
PEARLENV.LOCAL/Users/Administrator
PEARLENV.LOCAL/Users/exchangeservice
PEARLENV.LOCAL/Users/k2hostserver
PEARLENV.LOCAL/Users/labsbuild

3. Then click on the **Add Exchange Administrator** link in the right hand column and select the required rights.



Add Exchange Administrator

This wizard helps you to add a new Exchange administrator role. An Exchange administrator has permissions to operations as allowed by a certain role.

Select the user or group to add as an Exchange administrator:

Select the role and scope of this Exchange administrator:

- ● Exchange Organization Administrator role
- ○ Exchange Public Folder Administrator role
- ○ Exchange Recipient Administrator role
- ○ Exchange View-Only Administrator role
- ○ Exchange Server Administrator role

Select the server(s) to which this role has access:

4. Click on the **Add** button to complete the account configuration

Exchange Wizard - Runtime Operational Rights

1. An Exchange administrator account should be created and given Exchange Organization administrator rights.

    a. When the Create/Disable mailbox action is selected, the wizard should be configured to Run As the Exchange administrator account.

2. An Exchange service account should be created and given Exchange impersonation rights.
    a. When a Meeting Request or a Send Task action is selected in the Exchange Event Wizard, the wizard should be configured to Run As the Exchange service account.
3. Using the Exchange Web Service requires the K2 server machine to trust the EWS certificate and its signing Certificate Authority. This is required for the following operations:
    a. Exchange Calendar SmartObject (used by Send Meeting Request)
    b. Exchange Task SmartObject (used by Send Task)
    c. Exchange Meeting SmartObject (for using the Get Meeting Suggestions and Get Specific Time methods)

> For more information on Run As, see the K2 blackpearl online help at http://help.k2.com/en/k2blackpearluserguide.aspx Designing > Designers > K2 Designer for Visual Studio > Design Tools > Toolbox > Event Wizards > Server Events > Run As

Rights Specific to Microsoft Exchange Server 2010

K2 Service Account

This account should have Recipient Management rights for Exchange to be able to create and disable mailboxes and browse Exchange servers and mailbox databases.

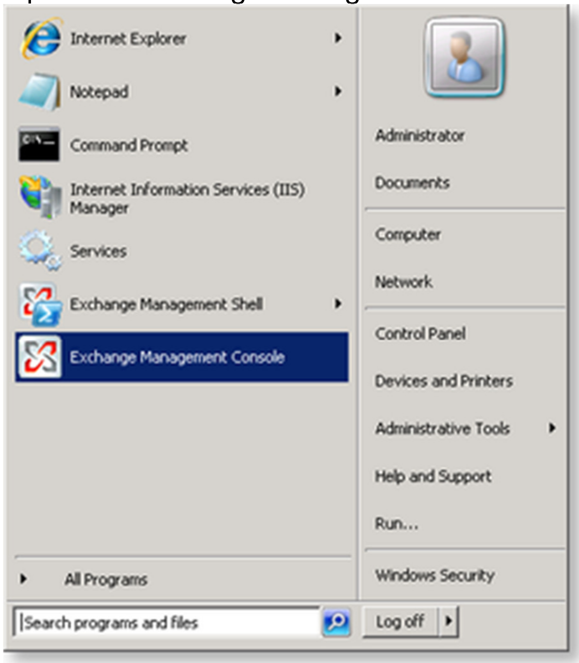
Also give the account Execute rights on the Microsoft.PowerShell configuration, by running the following command in the Exchange Management Shell:

Set-PSSessionConfiguration Microsoft.PowerShell –ShowSecurityDescrtiptorUI

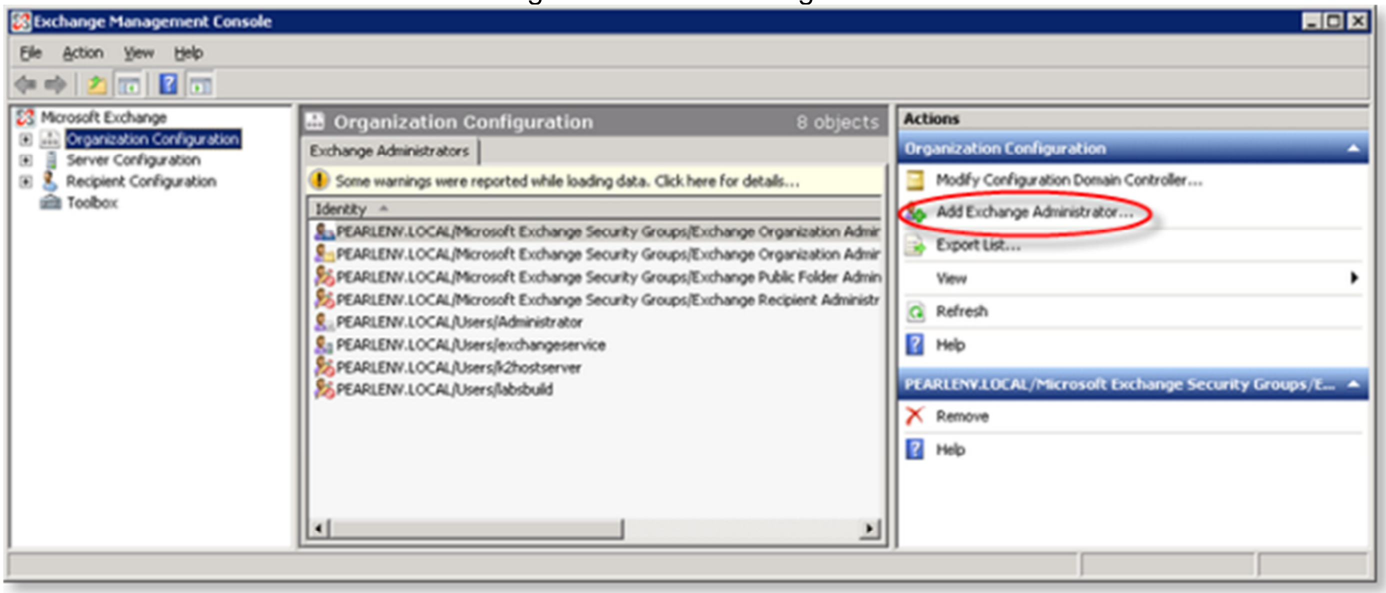
Exchange Organization and View-Only Administrator Rights

Configuring Exchange Organization and View-Only Administrator rights can be done through the Exchange Management Console:

1. Open the Exchange Management Console



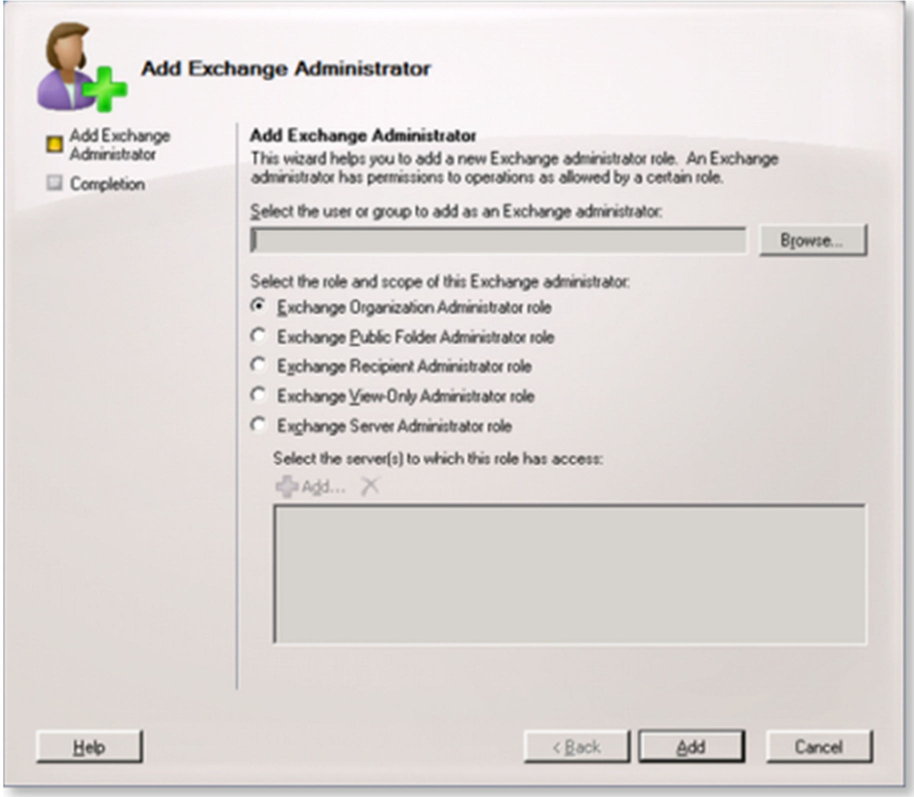
2. Select the user account that will be configured with the new rights


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Organization Configuration
Server Configuration
Recipient Configuration
Toolbox
Organization Configuration
8 objects
Exchange Administrators
Identity
Actions
Organization Configuration
Modify Configuration Domain Controller...
Add Exchange Administrator...
Export List...
View
Refresh
Help
PEARLENV.LOCAL/Microsoft Exchange Security Groups/E...
Remove
Help

Some warnings were reported while loading data. Click here for details...

PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Organization Admir
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Organization Admir
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Public Folder Admin
PEARLENV.LOCAL/Microsoft Exchange Security Groups/Exchange Recipient Administr
PEARLENV.LOCAL/Users/Administrator
PEARLENV.LOCAL/Users/exchangeservice
PEARLENV.LOCAL/Users/k2hostserver
PEARLENV.LOCAL/Users/labsbuild

3. Then click on the **Add Exchange Administrator** link in the right hand column and select the required rights.



Add Exchange Administrator

This wizard helps you to add a new Exchange administrator role. An Exchange administrator has permissions to operations as allowed by a certain role.

Select the user or group to add as an Exchange administrator:

Select the role and scope of this Exchange administrator:

● Exchange Organization Administrator role
○ Exchange Public Folder Administrator role
○ Exchange Recipient Administrator role
○ Exchange View-Only Administrator role
○ Exchange Server Administrator role

Select the server(s) to which this role has access:

4. Click on the **Add** button to complete the account configuration

Exchange Impersonation Rights

Giving Exchange impersonation rights for an account requires the account to NOT be part of the Exchange Organization Administrator group.

The rights are given to a user for a specific server.

	The user running the Exchange Management Shell to execute these commands should be an Exchange Organization Administrator.

The following commands should be run in the Exchange Management Shell, replacing <ExchangeServer> with the Exchange server's name where the Exchange web service is running and replacing <ExServiceAccount> with the name of the Exchange service account which the rights should be given to:

Add-ADPermission -Identity (get-exchangeserver -identity <ExchangeServer>).DistinguishedName -User (Get-User -Identity <ExServiceAccount> | select-object).identity -AccessRights GenericAll -InheritanceType Descendents

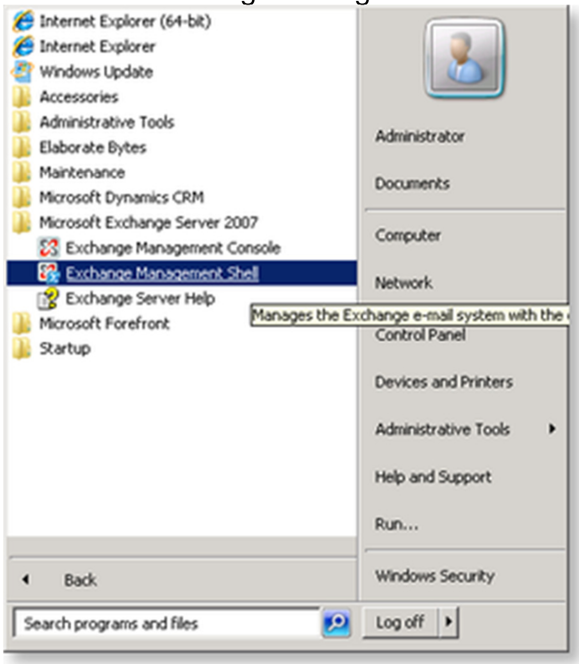
Add-ADPermission -Identity (get-exchangeserver -identity <ExchangeServer>).DistinguishedName -User (Get-User -Identity <ExServiceAccount> | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation

Add-ADPermission -Identity (get-exchangeserver -identity <ExchangeServer>).DistinguishedName -User (Get-User -Identity <ExServiceAccount> | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate

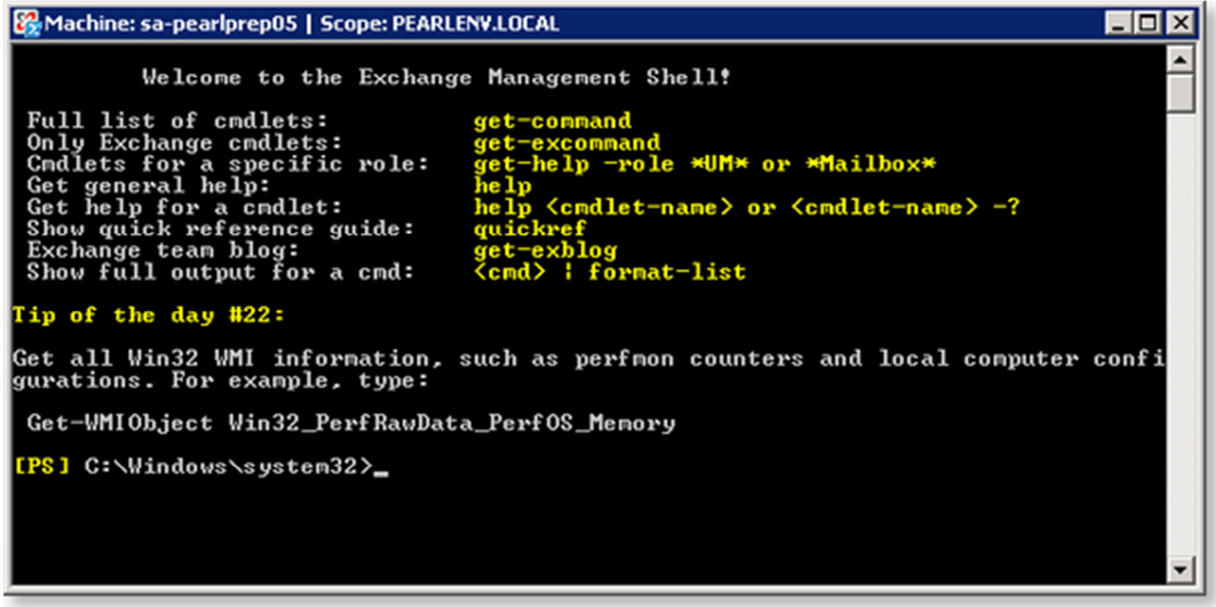
Add-ADPermission -Identity (get-exchangeserver -identity <ExchangeServer>).DistinguishedName -User (Get-User -Identity <ExServiceAccount> | select-object).identity -ExtendedRights Send-As

Add-ADPermission -Identity (get-exchangeserver -identity <ExchangeServer>).DistinguishedName -User (Get-User -Identity <ExServiceAccount> | select-object).identity -ExtendedRights Receive-As

1. Select the Exchange Management Shell from the Start menu



2. This will open the console window, within which the above commands can be executed



```
        Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #22:

Get all Win32 WMI information, such as perfmon counters and local computer confi
gurations. For example, type:

 Get-WMIObject Win32_PerfRawData_PerfOS_Memory

[PS] C:\Windows\system32>_
```

Authenticating with Microsoft Exchange as the User Making the SmartObject Call

The Exchange SmartObject methods that use PowerShell to communicate with Exchange now support authenticating with Exchange as the user making the SmartObject call. The following conditions must be met for the call to succeed:

- The account making the call must be a Windows account and it must use the security label that uses SSPI for authentication (by default this security label is called “K2”).
- The Windows account making the call must have a cached credential.
  - This can be done in Workspace.
  - Alternatively when Run As is used the credential will be cached automatically.
- The service object must be set up to use “Impersonation” and “Enforce Impersonate”.
  - Currently additional configuration required (SPNs etc.) is not known for “Impersonation” without “Enforce Impersonate”. In theory this would be used to avoid having to cache credentials.

We recommend that this method is used, as using the K2 service account for the Exchange PowerShell calls is a security concern.

Large Number of Method Calls

The WinRM architecture (which PowerShell uses to communicate with Exchange) limits the number of connections that a single user is allowed to open concurrently (by default this is 18). If a large number of concurrent calls are made to the SmartObjects this limit may be reached and the call will fail.

AFFECTED SERVICES/METHODS

- ExchangeAdminService
  - EnableMailbox
  - DisableMailbox
- ExchangeMetadataService
  - GetExchangeServer
  - GetMailboxDatabase
  - GetCurrentUser
- ExchangeService
  - EnableMailbox
  - DisableMailbox
  - GetExchangeServer
  - GetMailboxDatabase
  - GetCurrentUser

The following commands demonstrate two ways to increase the default number of connections:

winrm set winrm/config/winrs @{MaxShellsPerUser="50"}

or

Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 50

K2 WORKSPACE SECURITY REQUIREMENTS

The security of information and processes are critical to the ultimate success of every Enterprise.
K2 Workspace identifies the requirement to protect data internally and externally, by offering Domain security.

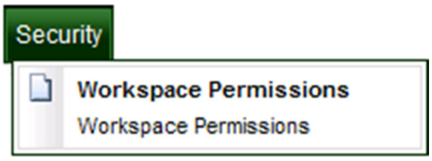
Domain Security

Users are able to access K2 Workspace with the following credentials:

Display	Description
Windows Authentication	If the user has a valid user name and password the system will automatically log the user into Workspace using the active directory credentials.

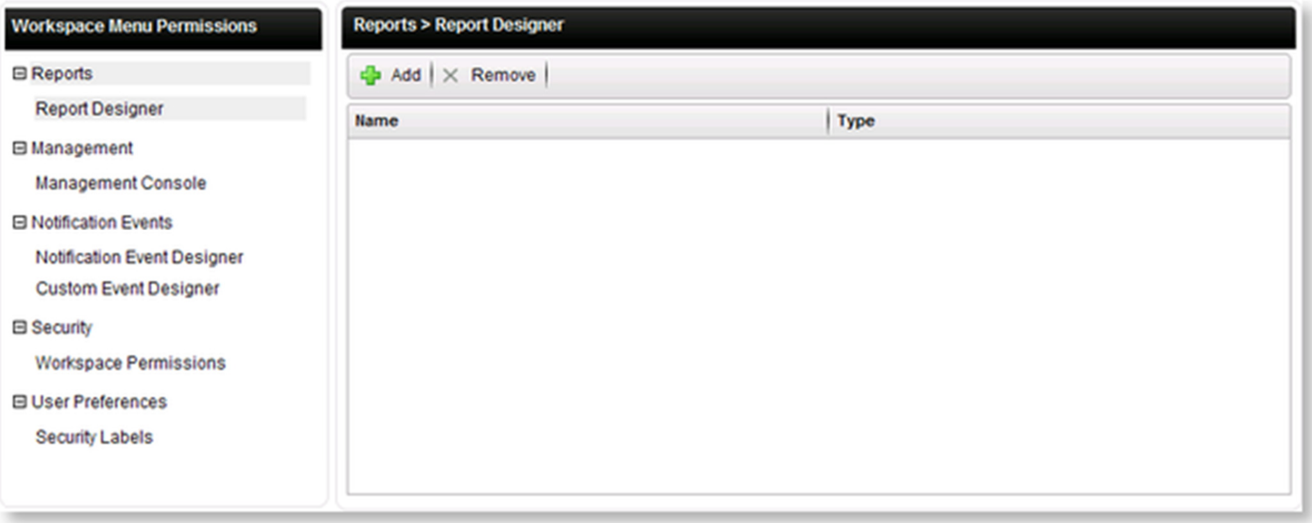
Permissions

For users to have access to the various components in K2 Workspace permissions need to be assigned to users or groups. The administrator will assign the required permissions on an Menu Item Level through the following menu:



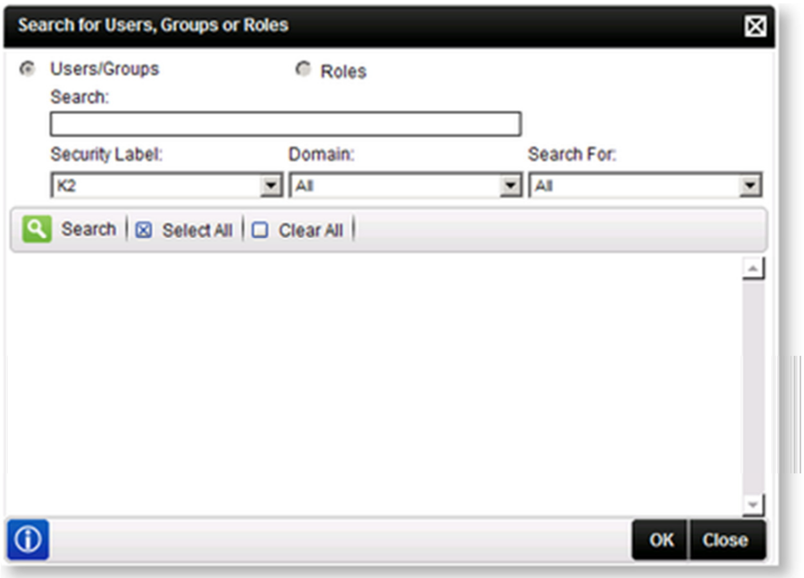
✎	If a user does not have a valid user name and password or is unable to login to K2 Workspace contact the Network administrator.

The user with access to the **Security** menu can configure the Workspace Menu Permissions for all users.



To configure the permissions perform the following steps:

1	Expand the menu on the left of the Workspace Menu Permissions screen
2	Click on the menu item to be assigned to a user
3	Click on the **Add** button to open the **Select Users/Groups** window

	 Search for Users, Groups or Roles ● Users/Groups ○ Roles Search: Security Label: K2 Domain: All Search For: All Search ☒ Select All □ Clear All OK Close
④	Type the user's name in the **Search** field
⑤	Click on the **Search** button. The user name will be displayed in the **Name** section
⑥	Select the check box next to the user's name
⑦	Click **OK** to give the user permissions to view and use the selected menu item

✎	Workspace Menu permissions must be configured per user or group. Without configuring the permissions the menus and menu items will not display in Workspace

K2 PROCESS PORTALS - OUT OF THE BOX REPORTS

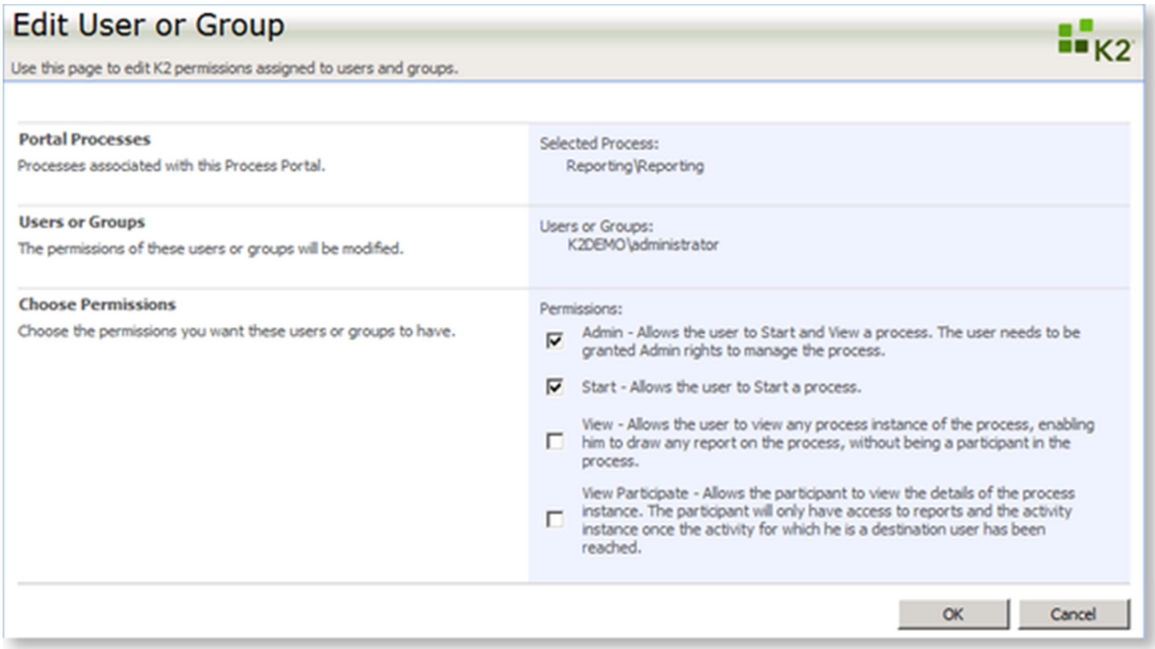
These reports provide status and statistical data on K2 workflow processes.

✎	It is important to note that **Microsoft Report Viewer 2008 SP1 Redistributable** is required in order to view the K2 reports. This can be found in the following location: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=bb196d5d-76c2-4a0e-9458-267d22b6aac6

Permissions

The reports have a level of security to ensure that the data is seen by authorized individuals within the organization. Permissions are based on the process rights assigned to the user in Process Management - Process Rights:

- Users with **Admin**, **Start** or **View** permissions have access to the Standard Reports.
- Users with **View Participate** permissions will be permitted to view the Standard Report from the point where the user has been part of the workflow process.



Edit User or Group

Use this page to edit K2 permissions assigned to users and groups.

Portal Processes
Processes associated with this Process Portal.

Selected Process:
Reporting\Reporting

Users or Groups
The permissions of these users or groups will be modified.

Users or Groups:
K2DEMO\administrator

Choose Permissions
Choose the permissions you want these users or groups to have.

Permissions:

☑ Admin - Allows the user to Start and View a process. The user needs to be granted Admin rights to manage the process.

☑ Start - Allows the user to Start a process.

□ View - Allows the user to view any process instance of the process, enabling him to draw any report on the process, without being a participant in the process.

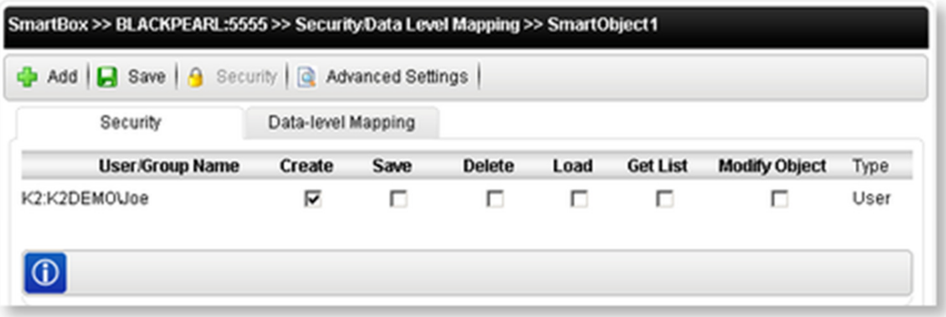
□ View Participate - Allows the participant to view the details of the process instance. The participant will only have access to reports and the activity instance once the activity for which he is a destination user has been reached.

Image: Process Management - Process Rights

	It is important to note that these permissions need to be assigned for each separate process by the System Administrator.

SMARTBOX - SMARTOBJECT SECURITY OPTIONS

The SmartObject Security Options allow an administrator to assign permissions to users for each of the SmartObject Methods.



SmartBox >> BLACKPEARL:5555 >> Security/Data Level Mapping >> SmartObject1

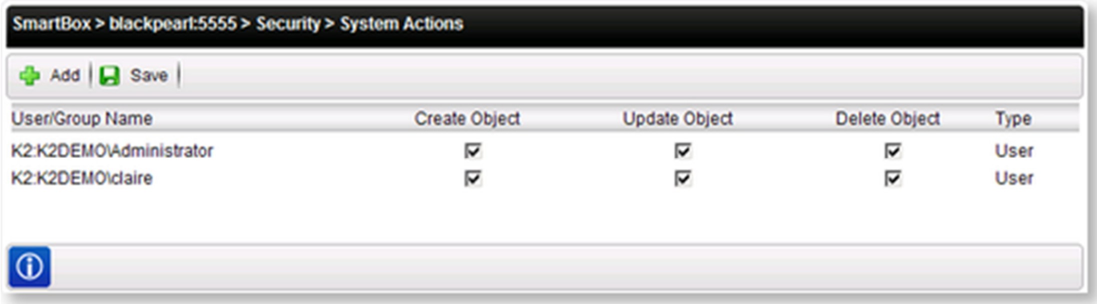
User/Group Name	Create	Save	Delete	Load	Get List	Modify Object	Type
K2:K2DEMO\Joe	☑	□	□	□	□	□	User

Option	**What it is**
User/Group Name	Lists the names of the users or groups with permissions associated with the SmartObject

SmartObject Methods Check Boxes [Create, Save, Delete, Load, Get List]	Presents the SmartObject Methods with corresponding check boxes, allowing the user to assign or remove permissions. Check the box to assign the User/Group permissions for the associated method
Modify Object	Check this box to assign the User/Group permission to Modify the SmartObject
Field Type	User or Group designation
Buttons	**What it is**
Add	Adds a user or group with particular permissions for the selected SmartObject See Add User
Save	Saves the configuration of users and/or groups for the selected SmartObject
Advanced Settings	Allows an administrator to configure the SmartObject Lookup Method See Data-level Mapping

SMARTBOX - SYSTEM ACTIONS

The System Actions dialogue screen allows an administrator to grant **Create Object**, **Update Object**, and **Delete Object** rights to a User or Group.



SmartBox > blackpearl:5555 > Security > System Actions

User/Group Name	Create Object	Update Object	Delete Object	Type
K2:K2DEMO\Administrator	☑	☑	☑	User
K2:K2DEMO\claire	☑	☑	☑	User

Image: System Action Permissions

Option	What it is	How to use it
User/Group Name	Lists the names of the users or groups with permissions associated with the Object System Actions	User Reference
Create Object	Check this box to assign the User/Group permission to create Objects	Click on the check box
Update Object	Check this box to assign the User/Group permission to update	Click on the check box

	Objects	
Delete Object	Check this box to assign the User/Group permissions to Delete Objects	Click on the check box
Type	User or Group Designation	User Reference
Button	**What it is**	**How to use it**
Add	Adds a user or group with particular permissions for the selected process See Add Users	Click **Add Users**
Save	Stores and activates the configuration of users and/or groups for the selected process	Click **Save**

K2 WEB PARTS - ACTIVITY GRAPH

Prerequisites

The following are required before using the Activity Graph web part:

- .NET 3.5 Framework
- Microsoft Silverlight 4 - The latest version of Silverlight can be found here http://www.silverlight.net/

Permissions

The following permissions are required:

- At least Designer permissions on the SharePoint page to edit the page and add the web part
- View permissions is sufficient to view the details of the Activity Graph web part
- View rights and/or View Participate rights on the K2 Server in order to see the data

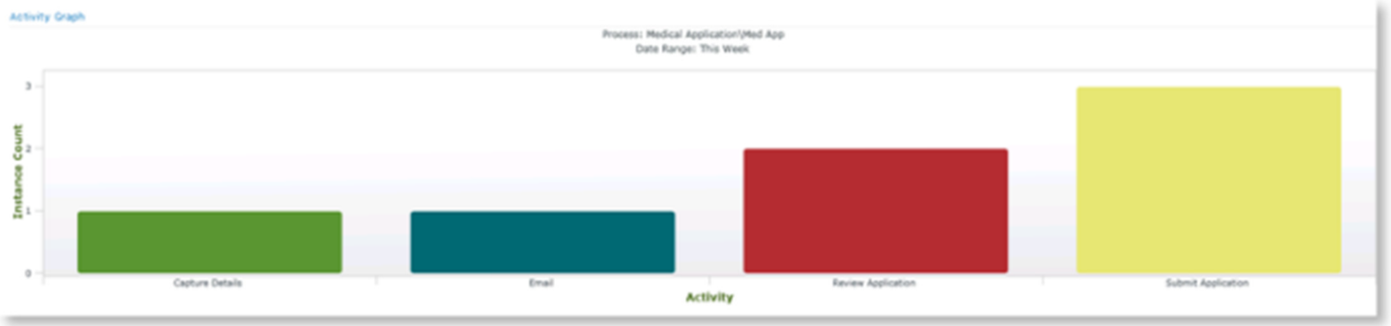
Process Portal Settings Inheritance

If the Activity Graph web part is added to a K2 Process Portal site, the user has the option to choose if the K2 Process Portal Settings should apply or if all the processes should be listed.

If the Activity Graph web part is added to a site which is not a K2 Process Portal site, the list of processes will automatically be displayed and the K2 Process Portal Settings won't apply.

Activity Graph

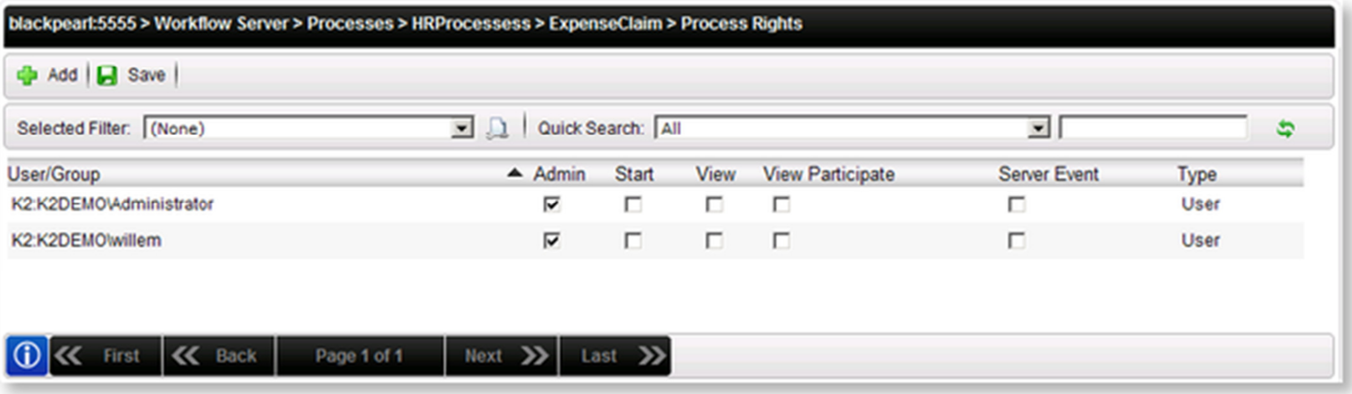
The **Activity Graph** displays the activities of the process instances. These can include process instances in progress and/or process instances completed. The Activity Graph Configuration window provides an interface where Filters can be added to only view specific processes/process instances according to the specified criteria, where Parameters can be set to define what the report should display and in what format, and where Settings can be set to define which process instances should be included.



PERMISSIONS TO PARTICIPATE IN WORKFLOWS

WORKFLOW SERVER - PROCESS RIGHTS

User Permissions control the extent to which Users or User Groups are able to interact with the process - enabling them to have full view of the process or limiting them to their worklist only.



blackpearl:5555 > Workflow Server > Processes > HRProcessess > ExpenseClaim > Process Rights

Selected Filter: (None)

Quick Search: All

User/Group	Admin	Start	View	View Participate	Server Event	Type
K2:K2DEMO\Administrator	☑	□	□	□	□	User
K2:K2DEMO\willem	☑	□	□	□	□	User

Image: Process User List

Name	What it is
User/Group	The name of the user or group
Admin	Process Administration permission rights
Start	Process Start permission rights
View	Process View permission rights
View Participate	Process View Participate permission rights
Server Event	Process Server Event permission rights
Type	User or Group designation
Add	Click the **Add** button to add a user to the Process User list
Save	Click the **Save** button to save the user configuration to the K2 Workflow Server
Permission	**Description**
Admin	Allows the user to **Start** and **View** a process. The user needs to be granted **Admin** rights to manage the process from the Management Console

Start	Allows the user to start a process - without it the user will receive an error if attempting to start a process
View	Allows the user to view any process instance of the process, enabling them to draw any report on the process in K2 Workspace, without being a participant in the process
View Participate	Allows a participant, i.e. the user defined as the destination user for one of the process activities, to view the details of the process instance. The user will only be able to access process reports and the activity instance once it has reached the activity for which they are a destination user
Server Event	Asynchronous server events wait for a call-back from the external system to finish the server event. The user account used by the external system must be granted Server Event permissions for it to be allowed to finish the server event

Process Admin rights encompasses all the permissions listed below:

- Start
- View
- View Participate
- Server Event

The user requires **Server Admin and Export** rights in order to have Process Admin rights.

Process Rights can be assigned to Active Directory Users or Groups. In addition, Process Rights can be assigned to **SharePoint Groups** which contain AD Groups and Users.

APPENDIX - AUTHENTICATION

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 alongside 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	• 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	• The K2 Server Service Account must have Log on as a Service permissions
Client Machines	Internet Access	• User must have Internet Explorer • Internet Explorer must be configured properly

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.

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 loopup 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 a 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.

A disadvantage of CNAMEs is that they can cause issues with Kerberos, using A Record is recommended.

MX Records / Mail Records

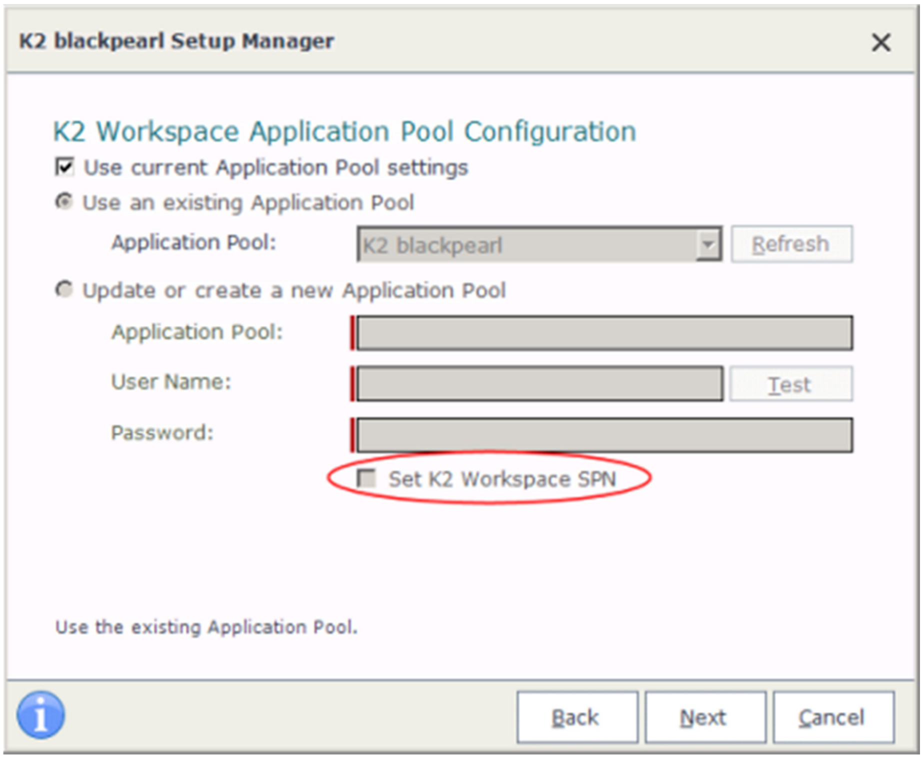
MX Records (Mail eXchanger record) tells mail systems how to handle mail that is addressed to a particular domain. Like CNAME records, the MX record maps a domain name to another domain name.
In the example, we use our primary machine as a server for mail to xyx@example.com.
Every MX record is tagged 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

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.

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 (Service Principle Name). 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".


K2 blackpearl Setup Manager

K2 Workspace Application Pool Configuration

☑ Use current Application Pool settings

● Use an existing Application Pool

Application Pool: K2 blackpearl

○ Update or create a new Application Pool

Application Pool:

User Name:

Password:

□ Set K2 Workspace SPN

Use the existing Application Pool.

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 exist 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 installation, 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

K2 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.

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 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

REPORTING SERVICES SERVICE ACCOUNT

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
6. In the Available Services section, select the K2HostServer item.
7. Click OK. The "Trust this user for delegation to specified service only" and "Use Kerberos only" options should be selected.
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.

1. Open Active Directory Users and Computers (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

K2 WORKSPACE SERVICE ACCOUNT

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.
>
> Note that If you are using Kerberos, and setting SPNs, you have to set “useAppPoolCredentials” to true in IIS, or Kerberos will fail. This is only if using kernel mode as by default K2 Server sets this in all *web.config* files.

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 (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.
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 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.

SHAREPOINT SERVICE ACCOUNT

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

SQL SERVER SERVICE ACCOUNT

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 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".