Before You Begin

Installing K2 for SharePoint involves running the Setup Manager to update the existing K2 components, adding the K2 for SharePoint App to the App Catalog, and then configuring the app.

What gets installed into SharePoint

No components are installed on the SharePoint server, only the K2 for SharePoint App is deployed to the SharePoint App catalog. The following K2 components are installed during the K2 for SharePoint installation process on the applicable servers:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K2 Server</td>
<td>Updates existing K2 blackpearl Server and K2 databases</td>
</tr>
<tr>
<td>K2 Workspace</td>
<td>Security updates to existing K2 Workspace web sites (supports secure communication between K2 and SharePoint)</td>
</tr>
<tr>
<td>K2 smartforms</td>
<td>Security updates to existing K2 smartforms Designer and Runtime web sites (supports secure communication between K2 and SharePoint)</td>
</tr>
<tr>
<td>K2 Client</td>
<td>Updates to existing K2 Client Tools (includes K2 Studio and supported versions of K2 for Visual Studio)</td>
</tr>
<tr>
<td>K2 Setup for SharePoint</td>
<td>K2 for SharePoint Setup Manager files and folders (allows installation maintenance)</td>
</tr>
</tbody>
</table>

Software and Hardware Requirements

Before installing K2 for SharePoint, ensure the following prerequisite software has been installed in your environment.

For hardware requirements, network requirements and topographical considerations, refer to the K2 blackpearl and K2 smartforms documentation on help.k2.com.

K2 for SharePoint is an add-on for K2 blackpearl and requires the following K2 software to be fully installed and configured:

- K2 blackpearl 4.6.7 (4.12060.1590.0)
- K2 smartforms 1.0.6 (4.12165.1625.0)
  - K2 smartforms Control Pack 1.0 (4.13180.1.0)

K2 for SharePoint OnLine requires HTTPS connections. These bindings need to be set up with the installation of K2 blackpearl 4.6.7 or if installing K2 for SharePoint on an existing K2 environment, the K2 prerequisites need to be reconfigured for HTTPS support. SSL enabled sites are default.

SSL is not required for on premises installations but if you’re not using SSL you need to run the PowerShell script to remove SharePoint’s SSL requirement for metadata and OAuth exchange. There is a KB available describing how to do this: http://help.k2.com/en/kb001561.aspx

SharePoint Requirements

SharePoint 2013 Apps must be enabled for the K2 for SharePoint App to work (http://www.sharepointalex.co.uk/index.php/2012/11/enabling-sharepoint-2013-apps/).
For more information see the Microsoft Technet page: http://technet.microsoft.com/en-us/library/fp161232.aspx

Specifically:


SharePoint 2013 Foundation is not supported.

The SharePoint 2013 March Public Update (or later) is required if:

- You are using web apps or site collections with host headers (domain names / ‘friendly’ url's)
- You have other server software installed on the SharePoint server that is using the Default Web Site (i.e. port 80/443)
- You are not using port 80/443 for your web apps

For information on why the March Public update is required see: http://technet.microsoft.com/en-us/library/dn144963.aspx
See this link for information on how to reduce the 5 hours usually needed to instal cumulative updates to 30 minutes.

For OnPremises SharePoint apps (which use server to server authentication) correct set up of the User Profile Service is required. It must also be correctly populated with the user’s information. See the Add the K2 App to the SharePoint Site section of the OnPremises Installation for more information.

Other Software Requirements

- Microsoft Silverlight 4.0.50917.0 or higher (required by the web-based K2 Workflow Designer)

Supported Browsers
SharePoint users/participants need a SharePoint-compatible Internet browser to view and use K2 for SharePoint features.

- Internet Explorer 8, 9, or 10 (versions 6 and 7 are not supported)
- Google Chrome (latest released version)
- Mozilla Firefox (latest released version)
- Apple Safari (latest released version)

Permissions for Installing K2 for SharePoint

When using the K2 for SharePoint App use an account other than the K2 Service account, as this will result in the current user not reflecting but rather the SharePoint App user would be used for all actions in SharePoint. If the K2 Service account is the Administrator, rather make a different user as the K2 Service account.

- **Local admin**, as the appdeployment.exe requires this.
- **K2 Admin**, as the user executing the appdeployment.exe needs to access the high trust certificate from the K2 DB to setup the high trust for the apps.
- **Site Collection Administrator / Contributor** on the required App catalog sites to view and deploy to the catalogs.
- **SharePoint_Shell_ACCESS** role, as the user requires permissions to execute the PowerShell cmdlet as discussed here:
  - $contentDBId = (Get-SPDatabase | ?($_.Name -eq "WSS_Portal"))
  - Add-SPShellAdmin -UserName {DOMAIN\UserName} -database $contentDBId

  - When you run this cmdlet to add a user to the **SharePoint_Shell_ACCESS** role, you must have membership in the **securityadmin** fixed server role on the SQL Server instance, membership in the **db_owner** fixed database role on all affected databases, and local administrative permission on the local computer.
  - This cmdlet is intended only to be used with a database that uses Windows authentication. There is no need to use this cmdlet for databases that use SQL authentication; in fact, doing so may result in an error message.

  - In order to use Windows PowerShell 3.0 for SharePoint 2013, a user must be a member of the **SharePoint_Shell_ACCESS** role on the configuration database and a member of the **WSS_ADMIN_WPG** local group on the computer where SharePoint 2013 is installed. However, the result of running this cmdlet is that the user specified with the **UserName** parameter will have the **db_owner** role access on the affected databases as described below. Therefore, you should carefully plan which users are given this access.
This will give the following database roles:

- **WSS_Portal**
  - Public
  - SharePoint_Shell_Access
  - SPDataAccess

- **SharePoint_AdminContent_{[Guid]}**
  - Public
  - SharePoint_Shell_Access
  - SPDataAccess

- **SharePoint_Config**
  - Public
  - SharePoint_Shell_Access
  - SPDataAccess

**How to set the permissions:**

1. Browse to Central Admin > Manage App Catalog > View site settings
2. In the App Catalog site settings, select Site collection administrators

```
Home
Site Settings

Users and Permissions
People and groups
Site permissions
Site collection administrators
Site app permissions
```

3. Add Administrator user

```
Home
Permissions › Site Collection Administrators

Site Collection Administrators
Site Collection Administrators are given full control over all Web sites in the site collection. They may also receive site use confirmation mail. Enter users separated by semicolons.

Administrator

OK  Cancel
```
Overview and Architecture of K2 for SharePoint

The K2 for SharePoint app is a provider-hosted app for SharePoint 2013. Provider-hosted apps allow for server-side execution, and the K2 for SharePoint app takes advantage of this by surfacing artifacts and pages from a K2 server directly into SharePoint for a rich application experience. Important: Because K2 for SharePoint is an app, your SharePoint 2013 site must first be enabled for apps before you can install it. You must also have a fully-configured K2 server ready to register the app once it is installed and activated to the site. For more information about enabling your SharePoint 2013 site for apps, see the MSDN article Install and manage apps for SharePoint 2013. It is recommended to install a simple, free app from the SharePoint Store in order to test that your SharePoint 2013 site is ready for apps before attempting to install the K2 for SharePoint app.

Architecture
The K2 for SharePoint app itself is relatively lightweight and easy to install. It is the only thing that is required to be installed on the SharePoint server itself and includes:

1. A hidden K2 Settings list that stores the link between the app and the K2 server, along with a few other items like environment library fields.
2. A hidden K2Pages list that stores the pages used to host K2 content.
3. The K2 Worklist App Part which allows users to see their assigned K2 tasks.
4. The K2 Forms Viewer App Part which can be used to display a SmartForm.
5. The Ribbon Bar items for creating a K2 Application on a list or library and for viewing reports.

The K2 for SharePoint app must be registered with a K2 server to show K2 content and functionality in SharePoint. A SharePoint generated app domain hosts an iFrame that surfaces K2 content from the K2 Server. All interaction between SharePoint and K2 takes place via K2 SmartObjects. These, in turn, depend on the K2 for SharePoint Service Brokers that are registered with a K2 server during the Registration Wizard.

Note: The K2 for SharePoint app functions the same online and on-premises (on-prem), however there are different versions of the app. See Versions of the K2 for SharePoint App for more information.

Versions of the K2 for SharePoint App
There are two different versions of the K2 for SharePoint App.
1. The K2 for SharePoint app in the SharePoint Store: This app can be installed directly on any on SharePoint site that is enabled for apps, whether that site is online or on-prem. This app can only request Manage rights when it is installed, so items such as creating sites and SharePoint groups cannot be automated by K2 using this version of the app. See [How To: Deploy a Full Control K2 Application to SharePoint Online](#) for more information.

2. The K2 for SharePoint app in the K2 for SharePoint download: This app is installed with all on-prem versions of SharePoint 2013 using the AppDeployment.exe installer that is chained with the main K2 for SharePoint installer. It can also be run separately. This app requests Full Control rights on the site when it is installed, so all functionality included in the K2 Designer when designing a workflow is functional, such as creating sites and SharePoint groups.

Registering the K2 for SharePoint App with a K2 Server

Once you have the K2 for SharePoint app installed, you must register it with a K2 server. The K2 server must have the version of components that the K2 for SharePoint app requires. The K2 AutoDiscover service allows you to supply any K2-related URL and it will return what the K2 for SharePoint app needs, namely the K2 smartforms Designer and Runtime URLs. You can copy the AutoDiscover IIS application from the K2 server to make it accessible to the internet if necessary. The K2 server, however, must be accessible from that IIS location in order for the AutoDiscover service to query the K2 server for the latest values.

Notes:

- More than one K2 for SharePoint app can be registered with a single K2 server. This means that you can have all of your SharePoint 2013 farms and/or SharePoint Online tenancies being served by a single K2 server.

- You must install and register the K2 for SharePoint app on every site you wish to use it on. The registration wizard will automatically navigate between pages if it discovers that the root site in the site collection has already been configured.

- If you want to walk through the wizard manually, after registering the site with K2 you can go to Settings > Registration Wizard.

How the K2 for SharePoint App Works

Once the K2 for SharePoint app is registered with a K2 server, the K2 Settings hidden list is populated. This list stores the link to the K2 server, what groups have K2 Designer and Participant permissions, the environment library fields for the SmartForms runtime and design time URLs, the version of the K2 for SharePoint application, and a few other details for the K2 for SharePoint app integration.

When a list is integrated with K2 for SharePoint, various pieces of information are recorded depending on what you select for your K2 solution. The Create K2 Application page allows you to select what you want to create.
Portal › Tasks › Create K2 Application

Select the elements that will be part of your solution:

Data

Create SmartObject

A K2 SmartObject will be created for this list/library. In addition to this, additional SmartObjects will be created for any lookup lists, as well as for choice fields. These SmartObjects are used in Forms as well as workflow.

Allow this SmartObject to be used in Workflows for this List/Library

Warning: The following fields are not supported and will not be included in the SmartObjects:
Related Items

Forms

Create SmartForms

SmartForms will be generated for this list/library. This includes New, Edit and Display Forms. Additionally, you have the option to replace the default SharePoint forms with K2 smartforms in order to enhance the user experience for adding, editing and displaying items.

Create Workflow

K2 Workflows can be created for the list/library. This includes a number of ways in which the workflow can be started—automatically or manually. These workflows can also leverage any forms that have been created.

Create Reports

Reports will be created that summarize all workflow activity for this list/library. These can be customized and extended, and all reporting controls can be used directly on SmartForms.

- Data: Creates SmartObjects for the list or library. If the list supports attachments, a separate but associated SmartObject is created for the attachments. If the list or library includes a lookup column, a SmartObject is created for that lookup column. This integration is mandatory for any K2 solution and cannot be unchecked.

- Forms: Forms are created based on the columns in the list or library. You can also choose to replace the existing SharePoint forms with SmartForms. You can switch this back at a later time by clicking Forms Settings from the artifacts page, which is the default page you’ll navigate to after your solution is created and you click the K2 Application button in the Ribbon again.
• Workflow: A workflow is created for the list or library. When selecting this option you are taken directly to the K2 Designer to start designing your workflow. If you do not select this option you are taken to the K2 artifact page.

• Reports: Forms and views are created for reporting on the workflow.

When selecting a workflow, you can choose how the workflow starts. For each event that you select, an event receiver is created for the list or library. This is important because if your K2 server is not available over a secure socket layer (SSL, typically port 443) and you want to automatically start workflows based on list or library events, the event receiver will not be able to find the K2 service to start the workflow. The name of the K2 service is RemoteEventService.svc and is part of the SP15EventService site on the K2 server. For more information, see SharePoint 2013 Integration Requirements.

From the artifacts page you can create, edit and delete parts of the K2 solution. As pictured below, this Tasks list is integrated with K2 and all aspects have been generated. This page is a K2-owned page that is surfaced in SharePoint via an iFrame. If you look at the URL you’ll see something like https://app-6210f94d-b9d1e7.denallixapps.com/.... This URL indicates that SharePoint has given control over to the app registered with that domain. This is inherent to the SharePoint 2013 app model and is how the context switching occurs between SharePoint and a provider-hosted app such as K2 for SharePoint.

Clicking on any of the K2 artifacts on this page and clicking Edit will allow you to edit that item using the K2 Designer. This is surfaced through SharePoint from the K2 Designer, which is installed with K2 smartforms. If you do not have a license for K2 smartforms you cannot edit your forms and views, but can edit your SmartObjects and workflows.
Platform Architecture and Supported Topologies

Understand the platform architecture

K2 for SharePoint leverages the resources of K2 and SharePoint. The following diagram provides an overview of the architectural relationship among K2 for SharePoint, other K2 software, and SharePoint. Forms are retrieved, edited, or created directly from K2 smartforms hosted in SharePoint within a frame on a hosting page (see the yellow line in the diagram).
**K2 for SharePoint App**

- Installs on the SharePoint Site from the SharePoint Store (online) or from the App Catalog (on-premises)
- Contains the K2 Worklist which enables users to complete assigned workflow activities
- Contains the K2 Form Viewer which enables users to view and run forms
- Displays New, Edit, and Display Forms developed in the K2 Designer in SmartForms
- Provides a seamless working view into the K2 Designer in SmartForms for creating and designing SmartObjects, Views, Forms, and Workflows
- Communicates with the K2 Application via the K2 CSOM Broker

**Supported Topologies**

*Simple Installation Scenarios: Small scale installations with little or no redundancy.*
**Standalone Install**

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

All K2 components, IIS, SharePoint, and the database instance are installed on the same physical platform with connection to SharePoint Online if required.

**Considerations**

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

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

**Small Scale Install**

In many cases K2 blackpearl is installed into an existing infrastructure; therefore, the database can be easily installed on an existing SQL server. This is true even when all K2 components are installed on an existing server. This is suitable for small usage, such as a test or training environment.
All K2 components, IIS, SQL Reporting Services, and SharePoint are installed on one server, and the databases are located on a separate server, with connection to SharePoint Online if required.

**Dedicated SQL Server**

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

**Scaling for Data Availability**

Since many business critical processes may be automated using K2 blackpearl, it may be important to have a redundant system for data availability. This scenario is the same as the Small Scale install, but with a SQL cluster as the database back-end rather than a single server.
All of the IIS, K2, SQL Reporting Services, and SharePoint components are installed on one server, with a clustered SQL server instance for data redundancy and connection to SharePoint Online if required.

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

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

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

**Scaling for Better Performance**

This scenario is better suited for small organizations that do not require any redundancy. Although able to support an increasing load on the K2 infrastructure, the K2 Server is separated from the SharePoint server for scalability.
All of the K2 components are separated out from the SharePoint components, with a separate SQL server. Since this scenario deploys the various components onto multiple servers, there are some considerations around Kerberos and location of the components that should be addressed.

**Kerberos**

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

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

**SQL Server**

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

**Medium Installation Scenarios: Medium scale installations, with some redundancy**

**Scaling for Page Rendering**

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

All of the K2, IIS, and SharePoint components are installed on two nodes in an NLB cluster for better page rendering performance and fail over via load balancing. This scenario introduces a NLB cluster into the installation topology; therefore, it is important to understand NLB before installing this scenario.

Network Load Balancing
NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl. When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

SQL Server
The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources or be located on an independent platform, such as in this install. Considering that in most cases K2 is being introduced into an existing environment, the K2 Databases would be installed on an independent server that runs SQL Server. Since this is a common occurrence, the installation documentation takes this into consideration.
**Scaling for Data and Performance**
Both the Scaling for Page Rendering and Scaling for Data Availability scenarios start to address redundancy into the system. This scenario addresses both the data availability, by adding a SQL cluster into the infrastructure, as well as failover via load balancing on the other components.

There is a SQL cluster, and all IIS, SharePoint, SQL Reporting Services, and K2 components are on an NLB cluster.

**Network Load Balancing**
NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.
When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

**SQL Server**
The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it also can be clustered. For more information regarding SQL Server clustering, refer to the [SQL Server Failover Clustering documentation](http://msdn.microsoft.com/en-us/library/ms189134.aspx)
In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.
Medium Scale Install

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

K2 has its own dedicated server separating it from an NLB cluster set up for SharePoint and IIS. A SQL cluster is also introduced for data redundancy.

Kerberos

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

Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.
Network Load Balancing
NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.
When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

SQL Server
The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it also can be clustered. For more information regarding SQL Server clustering, refer to the SQL Server Failover Clustering documentation (http://msdn.microsoft.com/en-us/library/ms189134.aspx)
In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

Maximum Redundancy on Six Servers
This topology adds maximum availability on the fewest number of servers. This scenario is intended for organizations that require redundancy of all application server roles. Having an NLB cluster for the K2 Server and a separate NLB cluster for the Web tier maximizes its availability and performance. A SQL cluster also allows for data redundancy.
Kerberos
Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result.
Whenever credentials must pass more than one “hop” between servers, Kerberos must be configured. This is known as the “double-hop issue.”
Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

Network Load Balancing
NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl.
When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

SQL Server
The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it also can be clustered. For more information regarding SQL Server clustering, refer to the SQL Server Failover Clustering documentation (http://msdn.microsoft.com/en-us/library/ms189134.aspx)
In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.

**Large Installation Scenarios: Fully redundant installations**

**Large Scale Install**

The Large Scale Install scenario is specifically suitable for high work load environments, with components scaled to three tiers. Each component is load balanced, and multiple dedicated databases allow for maximum growth and availability. Multiple databases are dedicated to individual load-balanced components to allow for maximum growth and availability. Kerberos is mandatory for this configuration option. Both NLB and Kerberos must be configured correctly and must be able to communicate before K2 blackpearl is installed.
Not all of the SharePoint features are shown here. Refer to the SharePoint documentation for installation guides and options.

**Considerations**

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

**Kerberos**

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

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

**Network Load Balancing**

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

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

**SQL Server**

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

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

**Segmentation by Site Collections**

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

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

Kerberos is mandatory for this configuration option. Both NLB and Kerberos must be configured correctly and must be able to communicate before K2 blackpearl is installed.
Not all of the SharePoint features are shown here. Refer to the SharePoint documentation for installation guides and options.

**Considerations**

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

**Kerberos**

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

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

**Network Load Balancing**

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

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

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

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

**Multiple SharePoint and K2 farms**

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

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

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

Not all of the SharePoint features are shown here. Refer to the SharePoint documentation for installation guides and options.

**Considerations**

Useful to segment due to:
• Load
• Language
• Geography
• Legal requirements
• Operational ownership/support

**Kerberos**

Since the IIS server does not share a server with the K2 Server, the credentials will be passed as a result. Whenever credentials must pass more than one “hop” between servers, Kerberos must be configured. This is known as the “double-hop issue.” Ensure that all Kerberos settings and necessary configuration takes place before attempting to install K2 blackpearl. To configure Kerberos, refer to the deployment considerations section on Kerberos later in this help file.

**Network Load Balancing**

NLB can be configured by using either the operating system or specific hardware. In either case, NLB configuration should be completed before installing K2 blackpearl. When installing components that will be load balanced, the installation must be performed on each machine independently. In this install, all of the components are on NLB servers; therefore, all of the components need to be installed on each NLB server.

**SQL Server**

The location of the SQL Server is not critical for a K2 installation, as long as the network connection speed to the K2 Server meets minimum requirements. It is also important that the DTC component is configured properly in order for communications between the K2 Server and the SQL Server can function properly. The SQL Server can share physical resources, be located on an independent platform, such as in this install, or it also can be clustered. For more information regarding SQL Server clustering, refer to the [SQL Server Failover Clustering documentation](http://msdn.microsoft.com/en-us/library/ms189134.aspx) In most cases K2 databases are installed on an established SQL Server cluster for an existing environment. This is a common occurrence and the installation documentation takes this into consideration.
SharePoint 2013 Integration Requirements

Overview
The K2 for SharePoint 2013 integration components use the new SharePoint 2013 apps architecture. This architecture allows 3rd party applications, like the K2 for SharePoint app, to be used with SharePoint on-premises, SharePoint Online (Office 365), as well as a mixture of online and on-premises. In each of these scenarios there are certain prerequisites that need to be met in order for the integration to function. This document outlines the required prerequisites for each SharePoint infrastructure scenario.

SharePoint on-premises
This section outlines the K2 and SharePoint requirements for using the K2 for SharePoint app with an on-premises SharePoint environment.

Requirements

SSL for K2 Site
If SharePoint is configured for SSL then K2 also needs to be configured for SSL. The K2 for SharePoint registration wizard will prevent you from proceeding if a mismatch is detected between the SSL settings for SharePoint and K2.

Enable SharePoint for Apps
After you install SharePoint on-premises there are a number of manual configuration steps that must be completed in order to enable your SharePoint environment for apps. These steps are not specific to the K2 for SharePoint app. These steps must be completed in order to install any 3rd party app into your SharePoint environment. The following TechNet article contains a collection of resources to guide you in the configuration and management of apps in your SharePoint environment:


App Upload and Installation Permissions
There are a minimum set of permissions that are required of the user that will upload the K2 for SharePoint app into the SharePoint app catalog and of the user that will install the K2 for SharePoint app onto a SharePoint site.

- Permissions required to upload the K2 for SharePoint app to the SharePoint app catalog
  - Local Administrator on the SharePoint Server
  - K2 Administrator
  - Site Collection Administrator of the App Catalog Site Collection
  - db_owner Access to the SharePoint_Config Database

- Permissions required to install the K2 for SharePoint app onto a SharePoint site
  - Contributor Rights on the SharePoint site
SharePoint online (Office 365)

This section outlines the K2 and SharePoint requirements for using the K2 for SharePoint app with an online SharePoint environment.

Requirements

SSL for K2 Site

SharePoint Online is always SSL enabled and thus it is mandatory for the K2 site to also be enabled for SSL. The K2 for SharePoint app registration wizard will prevent you from proceeding if this configuration has not been completed.

Internet Accessible K2 Sites

When using the K2 for SharePoint app with SharePoint Online there is communication that needs to take place between your on-premises K2 Server and your online SharePoint environment. This may require opening ports and sites through your corporate firewall. There are two scenarios listed below, each with their own requirements. Follow the steps for the scenario that best fits your needs.

- All users of your SharePoint Online environment will be behind your corporate firewall
  - The SP15EventService on the K2 Server that SharePoint will call when SharePoint events occur will need to be publically available on the web. This is the service that is used for initiating workflows from SharePoint events (Example: File Uploaded, Item Added, etc.)

- Some or all of your users will access your SharePoint Online environment from outside your corporate firewall
  - The entire K2 site and your K2 smartforms sites, will need to be made publically available on the web.

Azure Active Directory

SharePoint Online requires the use of Azure Active Directory (AAD). When you register the K2 for SharePoint app K2 will automatically register the appropriate resources against your AAD tenant for the purpose of Authentication and Authorization.

App Upload and Installation Permissions

There are a minimum set of permissions that are required of the user that will upload the K2 for SharePoint app into the SharePoint app catalog and of the user that will install the K2 for SharePoint app onto a SharePoint site.

- Permissions required to upload the K2 for SharePoint app to the SharePoint app catalog
  - Tenant Admin of the SharePoint environment

- Permissions required to install the K2 for SharePoint app onto a SharePoint site
  - Contributor Rights on the SharePoint site

Mixture of SharePoint on-premises and SharePoint Online

It is increasingly common for organizations to have a mixture of SharePoint on-premises and SharePoint online. A single K2 server can support both of these environments at the same time however there are some slight differences to the configuration if your on-premises SharePoint environment is setup in Hybrid mode. You can find more details on enabling Hybrid mode for SharePoint 2013 in the Hybrid for SharePoint 2013 TechNet article. Follow the steps in the SharePoint Server 2013 Hybrid section below if this applies to your environment. If you are not...
configured for Hybrid authentication then the requirements are simply a combination of the two sections listed above for SharePoint on-premised and SharePoint Online.

SharePoint Server 2013 Hybrid

In organizations with both SharePoint on-premises and SharePoint Online there is a configuration mode available to allow these two environments to work more closely together known as Hybrid mode. The excerpt below from the Hybrid for SharePoint Server 2013 TechNet article describes the high level features of enabling Hybrid mode.

“A SharePoint Server 2013 hybrid environment enables identity management and trusted communications between SharePoint Online and SharePoint Server 2013. When you have established this trust framework, you can configure integrated functionality between services and features such as Search, Microsoft Business Connectivity Services, and Duet Enterprise Online for Microsoft SharePoint and SAP.”

When K2 for SharePoint is installed in a SharePoint Server 2013 hybrid environment, the installation experience will be a combination of on-premises and online experiences. The K2 for SharePoint app will be installed to the on-premises and online app catalogs. However, since both the on-premises and online SharePoint environments will be configured for Azure Active Directory, the K2 application will treat the users and authentication the same as in the SharePoint Online scenario.

For more information on upload the K2 for SharePoint App into a SharePoint Server 2013 hybrid environment please review the following KB article: http://help.k2.com/en/kb001443.aspx
On-Premises Installation

Before you install K2 for SharePoint, make sure that the K2 for SharePoint prerequisites have been installed and configured (see the topic Before you Begin) and log into the target machine with the local System Administrator permissions.

Single Server
Installing on a standalone environment will update the existing K2 components and install the K2 for SharePoint component on a single machine.

Hardware prerequisites
As K2 for SharePoint relies on K2 blackpearl 4.6.7 (4.12060.1590.0) and K2 smartforms 1.0.6 (4.12165.1625.0) (with K2 smartforms Control Pack 1.0 (4.13180.1.0)), the hardware requirements for those applications need to be satisfied. Information concerning these requirements can be found in the K2 blackpearl Getting Started Guide and K2 smartforms User Guide.

For the prerequisite hardware and software necessary for the SharePoint 2013 server, see the Hardware and software requirements for SharePoint 2013 on the Microsoft TechNet website.

There are no additional hardware requirements for K2 for SharePoint Application.

Software Prerequisites
The following list of software is required for the K2 for SharePoint Application:

- K2 blackpearl 4.6.7 (4.12060.1590.0)
- K2 smartforms 1.0.6 (4.12165.1625.0)
- K2 smartforms Control Pack 1.0 (4.13180.1.0)
- Microsoft Silverlight 4.0.50917.0 or higher (required by the web-based K2 Workflow Designer)
- .NET Framework 4.5 (is part of the prerequisite check during K2 blackpearl 4.6.7 installation, and needs to be installed)
- Internet Explorer 8, 9, or 10 (versions 6 and 7 are not supported) or
  - Google Chrome (latest released version) or
  - Mozilla Firefox (latest released version) or
  - Apple Safari (latest released version)

Security and Permissions
Be sure to log on to the target machine with local System Administrator rights before beginning the installation. Also see the Permissions section on the Before you begin page.
**Install and configure K2 for SharePoint**

1. Double-click the K2 for SharePoint installation package executable to extract the files to a location on the machine. If a security warning appears, click Run to start the installation (click Cancel to quit the installation).

2. Select the extraction path and then click OK (the default path places the files in a folder on your desktop).

3. After the files extract, a splash screen displays. Click the Launch Setup link located under the “Install and configure K2 for SharePoint” heading.

4. If prompted, click Run

5. After you read the Welcome screen, click Next.

6. After you review and accept the terms in the End User License Agreement, select the check box, and then click Next.

7. On the Update Components screen, all the components to be updated are shown, review them and then click Next.

8. For the K2 Server Database, enter the SQL Server name and database name. Make sure to use the same SQL server as the K2 Server database. Click Test to verify your connection. If successful, click OK, and then click Next from the Setup Manager.

9. Review the installation Configuration Summary. Click Next to continue.

10. Review Additional Actions required. If you would rather perform them manually, you can perform the listed actions from another location and then click Refresh to verify completion. Click Next to have any listed actions performed and continue the installation.

11. On the Install and Configuration screens, the Setup Manager displays the installation and configuration progress for each of the components. When the Finished window appears, check the 'Deploy K2 for SharePoint to you App Catalog' box and click the Finish button to complete the installation and start the K2 App Catalog
Deployment.

The K2 blackpearl server service is stopped during installation and is restarted automatically.

After finishing the Setup Manager, the App Catalog Deployment Wizard appears.

**App Catalog Deployment Wizard**

1. After reading the App Catalog Deployment Welcome screen, click Next.
2. Check the applicable Web Applications (or select all), and then click Next.
3. When the Finished window appears, click the Finish button to complete the installation.


For information describing how to deploy a Full Control K2 for SharePoint App to SharePoint Online, see [KB001443](http://technet.microsoft.com/en-us/library/jj729797(v=office.15).aspx).

**Add the K2 App to the SharePoint Site**

After installing the K2 for SharePoint components using the Setup Manager, you need to add the K2 App to the SharePoint Site.

SharePoint 2013 Apps must be enabled for the K2 for SharePoint App to work (see the following website for information: [Enabling SharePoint 2013 ‘Apps’](http://technet.microsoft.com/en-us/library/jj729797(v=office.15).aspx)).

For On Premises SharePoint apps (which use **server to server authentication**) correct set up of the User Profile Service is required. It must also be correctly populated with the user’s information.

While detailed steps on configuring User Profile Services is outside of the scope of this document, the following excerpt taken from [http://technet.microsoft.com/en-us/library/jj729797(v=office.15).aspx](http://technet.microsoft.com/en-us/library/jj729797(v=office.15).aspx) describes the requirement for UPA when using SharePoint on premises apps.

Server-to-server authentication allows for servers that are capable of server-to-server authentication to access and request resources from one another on behalf of users. Therefore, the server that runs SharePoint Server 2013 and that services the incoming resource request must be able to complete two tasks:

- Resolve the request to a specific SharePoint user
- Determine the set of role claims that are associated with the user, a process known as rehydrating the user’s identity

To rehydrate a user’s identity, a server that can perform server-to-server authentication requests access to SharePoint resources. SharePoint Server 2013 takes the claims from the incoming security token and resolves it to a specific SharePoint user. By default, SharePoint Server 2013 uses the built-in User Profile service application to resolve the identity.

The key user attributes for locating the corresponding user profile are as follows:
- The Windows Security Identifier (SID)
- The Active Directory Domain Services (AD DS) user principal name (UPN)
- The Simple Mail Transfer Protocol (SMTP) address
- The Session Initiation Protocol (SIP) address

Therefore, at least one of these user attributes must be current in user profiles. We recommend a periodic synchronization from identity stores to the User Profile service application.

See the troubleshooting topic for guidance on how to deal with issues arising from the User Profile Service.

**Activating K2 for a SharePoint Site**

1. Launch SharePoint (open a web browser to the Portal URL).

   Opening the Portal for the first time may take a while.

2. When the Portal opens, click **Add lists, libraries, and other apps**. The Site Contents page appears.
3. Click **From Your Organization**.

4. Apps from your organization appear. Click **K2 for SharePoint**
5. A window displays asking you to trust K2 for SharePoint. Click Trust It.

Do you trust K2 for SharePoint?

Let it have full control of this site collection.
Let it access basic information about the users of this site.
Let it share its permissions with other users.

Trust It  Cancel

If an error occurs when the 'Trust It' button is clicked, see this Troubleshooting topic.

6. When the K2 App finishes and installation completes on the SharePoint Site, the K2 for SharePoint App icon appears. Click the icon to configure the application.

K2 for SharePoint Registration Wizard
1. Specify the secure URL for the K2 smartforms site, and then click **Next**.

2. When the K2 for SharePoint configuration completes, the Configure Server page displays the configuration status for OAuth, Claims, and the SharePoint Service Brokers (green check-marks appear), click **Next**. These settings can be maintained from the management site, see the file: K2 for SharePoint Management settings.pdf (available as a download from the K2 for SharePoint article).
3. By default the K2 Permissions are configured in the background for Solution Designers and Solution Participants to Portal Members and Portal Owners Site Collection Groups. **This screen will not be shown by default.** but these permissions can be changed from the K2 for SharePoint > Settings page.

From the Configure K2 Permissions screen, select the groups depending on their role in the workflow:

- **Solution Designers:** create SmartObjects, Forms, and Workflows (default). In addition, they are granted rights to start, view, and action workflows (unless the default rights are altered).

- **Solution Participants:** participate in the workflow by starting, viewing, and actioning workflows.
4. To complete adding the K2 Application to the SharePoint Site, click **Finish**.

5. If prompted to allow the web page to open the site, click Yes.

Security Warning

The current webpage is trying to open a site in your Trusted sites list. Do you want to allow this?

- Current site: https://dlx
- Trusted site: https://app-4b71a52f580245.denallixapps.com

[Yes] [No]

Warning: allowing this can expose your computer to security risks. If you don't trust the current webpage, choose No.
6. Optionally modify General Settings or Permissions, or return to the Portal page.

![Portal](image)

**Portal › K2 for SharePoint**

<table>
<thead>
<tr>
<th>General</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Wizard</td>
<td>Configure K2 Permissions</td>
</tr>
<tr>
<td>Uninstall</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Artifacts</th>
<th>Reports</th>
</tr>
</thead>
</table>

If the App Registration fails with a SAML error, see the troubleshooting topic [SAML Token Error](#).

**SharePoint Permissions**

In SharePoint, permission masks are mapped to an App's permission request. Understanding these SharePoint permissions can assist when configuring the K2 Application so you can easily configure K2 environments with users and groups that have the exact same permissions that the K2 Application can request through OAuth.

To assign the required permission levels to a group, you must first create the permission level and then use it to assign permissions to the new group.

Follow the steps below to create a permission level:

1. Go to Site Settings > Site permissions > Permission Levels and set the following permissions

2. Enter the name of the permission as listed below, select the relevant permission from the list, and click Create.

**GuestPermLevel**

- **Browse User Information**: View information about users of the Web site. Also checks Open: Allows users to open a Web site, list, or folder in order to access items inside that container.)

- **View Application Pages**: View Forms, Views, and Application pages. Enumerate lists.
- **Use Client Integration Features**: Use features which launch client applications. Without this permission, users will have to work on documents locally and upload their changes. Also checks Use Remote Interfaces: Use SOAP, Web DAV, the Client Object Model or SharePoint Designer interfaces to access the Web site.

**ReadPermLevel**
- All GuestPermLevel +
- **View Pages**: View pages in a Web site.
- **View Items**: View items in lists and documents in document libraries.
- **Open Items**: View the source of documents with server-side file handlers.
- **View Versions**: View past versions of a list item or document.

**WritePermLevel**
- All ReadPermLevel +
- **Browse Directories**: Enumerate files and folders in a Web site using SharePoint Designer and Web DAV interfaces.
- **Manage Personal Views**: Create, change, and delete personal views of lists.
- **Add Items**: Add items to lists and add documents to document libraries.
- **Edit Items**: Edit items in lists, edit documents in document libraries, and customize Web Part Pages in document libraries.
- **Update Personal Web Parts**: Update Web Parts to display personalized information.
- **Add/Remove Personal Web Parts**: Add or remove personal Web Parts on a Web Part Page.
- **Delete Items**: Delete items from a list and documents from a document library.
- **Delete Versions**: Delete past versions of a list item or document.
- **Create Alerts**: Create alerts.

**ManagePermLevel**
- AllWritePermLevel +
- **Approve Items**: Approve a minor version of a list item or document.
- **Apply Themes and Borders**: Apply a theme or borders to the entire Web site.
- **Apply Style Sheets**: Apply a style sheet (.CSS file) to the Web site
• **Override List Behaviors**: Discard or check in a document which is checked out to another user, and change or override settings which allow users to read/edit only their own items

• **Manage Lists**: Create and delete lists, add or remove columns in a list, and add or remove public views of a list.

**Unchecked Permissions** (items still unchecked after the ManagePermLevel is created)

• **Manage Permissions**: Create and change permission levels on the Web site and assign permissions to users and groups.

• **Create Subsites**: Create subsites such as team sites, Meeting Workspace sites, and Document Workspace sites.

• **Manage Web Site**: Grants the ability to perform all administration tasks for the Web site as well as manage content.

• **Add and Customize Pages**: Add, change, or delete HTML pages or Web Part Pages, and edit the Web site using a Microsoft SharePoint Foundation-compatible editor.

• **Create Groups**: Create a group of users that can be used anywhere within the site collection.

• **Use Self-Service Site Creation**: Create a Web site using Self-Service Site Creation.

• **Enumerate Permissions**: Enumerate permissions on the Web site, list, folder, document, or list item.

• **Manage Alerts**: Manage alerts for all users of the Web site.

• **Edit Personal User Information**: Allows a user to change his or her own user information, such as adding a picture.

3. When creating a new group in SharePoint you will see these permission levels that can be assigned to the group.

**Distributed Installation**

In a distributed installation of K2 for SharePoint, the Setup Manager must be run on each of the component servers (K2 Server, K2 Workspace server, K2 smartforms server) and on Client machines (update K2 Studio and supported Visual Studio versions) to update each component. The K2 for SharePoint Setup Manager does not need to be run on the SharePoint server as this is only used to add and configure the App.

**MSDTC must be set up correctly as described in the K2 blackpearl Getting Started Guide.**
Once each component has been updated, it is necessary to run the App Deployment Wizard on the SharePoint server. To do this, copy the **K2 for SharePoint 'Installation' folder** from the Setup Manager extraction folder.

Paste the folder to the SharePoint Central Administration server (or in a Farm / NLB setup, copy to one of the SharePoint servers).

From the newly created folder, run the **"AppDeployment.exe"** file to start the App Deployment Wizard. The App Deployment Wizard steps are the same here as for a standalone server, please see the **App Deployment Wizard** topic.

Configuring the K2 for SharePoint App in a distributed environment follows the same process as for a standalone installation, see the **Configure** topic for details.

See also: **Online Installation**
SharePoint Online Installation

The K2 for SharePoint App is available from the SharePoint Store online and must be added to the online SharePoint site but this will only allow the app Managed Rights. The app may also be uploaded from the local system. For information on deploying the app with Full Control, see the KB article: How To: Deploy a Full Control K2 Application to SharePoint Online (http://help.k2.com/en/kb001443.aspx)

The K2 for SharePoint Setup Manager needs to be run on the K2 Servers to update relevant components and the K2 for SharePoint App needs to be configured as it would be on an On-premises site. For configuration details see the topic On-Premises Installation.

Additional Configuration

- The URL for the remote event receiver must be publicly accessible.

Note that the K2 for SharePoint Online installation requires SSL.
Unattended Installation

The unattended installation of K2 for SharePoint follows the same procedure as for K2 blackpearl. See the Unattended Installation section of the K2 blackpearl Getting Started Guide for details.

For convenience a summary is provided below.

**XML File Parameters**

The unattended install XML file is generated by the Setup Manager with the `setup.exe /output: "{filename}"` command.

The table below provides information on the parameters that can be edited in the Installation XML file:

<table>
<thead>
<tr>
<th>Example Installation XML</th>
<th>Parameter used for:</th>
<th>Component Applic-What can be changed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PRODUCT&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;COMPONENTS&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;SP15_SERVER /&gt;</td>
<td>Indicates component to be installed</td>
<td>Server component</td>
</tr>
<tr>
<td></td>
<td>Indicates component to be installed</td>
<td>Workspace component</td>
</tr>
<tr>
<td>&lt;SP15_WEB /&gt;</td>
<td>Indicates component to be installed</td>
<td>Smartforms component</td>
</tr>
<tr>
<td>&lt;SP15_SMARTFORMS /&gt;</td>
<td>Indicates component to be installed</td>
<td>Client component</td>
</tr>
<tr>
<td>&lt;SP15_CLIENT /&gt;</td>
<td>Indicates component to be installed</td>
<td>Setup manager – Required component</td>
</tr>
<tr>
<td>&lt;SP15_SETUP /&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;VARIABLES&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[MACHINEKEY]</td>
<td>Machine Key</td>
<td>All</td>
</tr>
<tr>
<td>[INSTALLDIR]</td>
<td>Installation Directory</td>
<td>All</td>
</tr>
<tr>
<td>[SIMPLEINSTALL]</td>
<td>Load balancing indicator</td>
<td>Server</td>
</tr>
<tr>
<td>[ISNLB]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment Setting</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>[REPORTPORTSITE]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[REPORTSITENAME]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[REPORTSERVERVDIR]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[REPORTPORTSITEURL]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[REPORTSITEPATH]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[FULLREPORTSITEURL]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[SETSITESPN]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[SETSPN]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[USRMRGRTYPE]</td>
<td>User manager type</td>
<td>All</td>
</tr>
<tr>
<td>[HOSTSERVERDBNAME]</td>
<td>SQL Database name</td>
<td>All</td>
</tr>
<tr>
<td>[HOSTSERVERCONNECTIONSTRING]</td>
<td>Hosterver connection string</td>
<td>All</td>
</tr>
<tr>
<td>[HOSTSERVERDBSQLSERVER]</td>
<td>SQL Server name</td>
<td>All</td>
</tr>
<tr>
<td>[LBHOSTSERVERNAME]</td>
<td>Load balancing server name</td>
<td>All</td>
</tr>
<tr>
<td>[LBHOSTSERVERFQDN]</td>
<td>Load balancing server FQDN</td>
<td>All</td>
</tr>
</tbody>
</table>

- AD or Non-AD installation
- DB name and SQL instance
- Connection string can be specified
- SQL Server name
- Load balancing server name
- Fully Qualified Domain name of LB server
Maintenance

Standard maintenance options found in K2 products are present in K2 for SharePoint. See the topics below for details.

Reconfigure
Selecting the Reconfigure option in the Setup Manager will perform the following tasks:

- **K2 Server**: redeploy the SharePoint and Management packages and restore the database updates as if freshly installed.
- **K2 Workspace** and **K2 smartforms** servers: the reconfigure will ensure the correct folders are present in IIS.
- **Clients**: reset the Toolbox in Visual Studio to ensure the new wizards are there.

Repair
This option manages the file system, putting the correct files and folders back in place. It will overwrite any custom changes.

REPAIRING any K2 installation will not preserve any custom files or changes to configuration. The Installer will reset and force the system back to a working state as it would have been after doing a clean installation. If you want to make subtle configuration changes, like changing URLs, ports, users, SMTP Servers, you must choose the CONFIGURE option on the Maintenance panel when re-running the K2 Setup Manager.

Modify
If during a Custom install some components were not included, and this setup is now to be changed to include those components, the Modify option must be used. The Setup Manager will allow you to select the appropriate component to install. To add K2 components, setup must be run from the source media not from the Start Menu.

Uninstall
There are two parts to uninstalling K2 for SharePoint. The first is to remove the K2 artifacts from the SharePoint site they are installed on (this has to be done on each site the K2 for SharePoint App is installed on), the second is to uninstall K2 for SharePoint by running the K2 for SharePoint Setup Manager from Start > Program Files > K2 Black Pearl > K2 for SharePoint Setup Manager and selecting the Remove option.

Removing K2 artifacts from a SharePoint site

1. To remove the K2 artifacts, browse to the K2 for SharePoint Settings page and click the Uninstall link under the General heading.
<table>
<thead>
<tr>
<th>General</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Wizard</td>
<td>Configure K2 Permissions</td>
</tr>
<tr>
<td>Uninstall</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Artifacts</th>
<th>Reports</th>
</tr>
</thead>
</table>
2. The Uninstall K2 for SharePoint page is shown, select Uninstall or Cancel:

Once the actions described on the uninstall page have been performed (green check-marks will show), the page will redirect to the home page.

3. In the previous step, if Uninstall is clicked, the following warning is shown. Select either OK or Cancel.

Uninstalling the K2 for SharePoint components from the K2 environment
1. Launch the K2 for SharePoint Setup Manager from the Start menu.

2. Select the **Remove K2 for SharePoint** option and click Next. Confirm your intention to uninstall by clicking **Yes** on the Warning screen.

3. Review the Additional Actions that will take place (e.g. an IISReset will be performed.)

4. The **Removing Components** screen will show the progress of the uninstall.

5. Click **Finish** on the Finish screen to complete the uninstall.

   In a distributed installation, the Setup Manager must be run on each of the servers in the K2 environment to remove the installed K2 for SharePoint components.
Troubleshooting

1. 404 Error when URL doesn't end in a postfix

   **Issue:** An issue exists where any URL not ending in a postfix (e.g. ".aspx") is not routed to the default asp.net handler by IIS 7.0 or 7.5, resulting in a 404 error.
   
   **Resolution:** After applying this hotfix - [http://support.microsoft.com/kb/980368](http://support.microsoft.com/kb/980368) and restarting the server, the issue is resolved.

2. Internet Explorer 11

   **Issue:** Internet Explorer 11 could have various issues with CRM, SharePoint and K2.
   
   **Resolution:** The best way to avoid these issues is to add all SharePoint, K2 and CRM sites to the Compatibility View list in IE 11.


   **Issue:** With multiple Web Applications defined, some or all are not shown in the App Deployment Wizard.
   
   **Resolutions:** There may be multiple resolutions depending on the underlying problem. Perform the following steps to correct this issue:
   
   - Confirm that each of the Web Applications have App Catalogs set up then re-run App Deployment Wizard (AppDeployment.exe)
   
   - Add the account used to run the K2 App Deployment Wizard, to the Site Collection Administrators for each App Catalog. Then re-run the App Deployment Wizard (AppDeployment.exe). The user doing the install must be a Site Collection Admin.
   

4. Trying to add the K2 App to a SharePoint site raises an error

   **Typical error:** Sorry, something went wrong. The specified application identifier [GUID] is invalid or does not exist.
   
   Reproduce the error by following these steps:
1. From Central Administration, select Apps option in the left-hand menu
2. Select the Configure Apps URLs option. If Apps are not enabled it will result in the following error:

**Sorry, something went wrong**

Settings or services required to complete this request are not currently available. Try this operation again later. If the problem persists, contact your administrator.

**Possible Resolution:** make sure that Apps are enabled for SharePoint 2013 and the permissions are set as in: Permissions

5. **Errors surfaced when installing in a distributed environment**

**Issue:** The error below is surfaced in the K2 for SharePoint Server component as a result of misconfiguration of MSDTC:

```
3832","2014-01-30 02:09:18","Error","15","15002","ERROR","SourceCode.Configuration.SharePoint15.Config","15002 Deployment Error: One or more items was not found","anonymous","0.0.0.0","k2:C:\Install\K2 for SharePoint RC Installers\K2 for SharePoint RC (4.13350.0.0)\In-stallation","3832","9791699e7e948493ef3d324d0a42f6d",""
```

**Resolution:** If K2 for SharePoint is deployed into a fully distributed environment, MSDTC needs to be correctly configured on the K2 Server and the SQL Servers as per K2 blackpearl Getting Started Guide.

6. **Server Error in '/K2Services' Application**

**Issue:** If this error is surfaced, the K2 Services may be incorrectly configured.
Server Error in /K2Services/ Application.

The HttpGetEnabled property of ServiceMetadataBehavior is set to true and the HttpGetUri property is a relative address, d or set HttpGetUri to an absolute address.

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

Exception Details: System.InvalidOperationException: The HttpGetEnabled property of ServiceMetadataBehavior is set to true and the HttpGetUri property is a relative address, but there is no HttpContext accessor. (System.Web.HttpGetBehavior, System.Web, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a) (at System.Web.HttpGetBehavior.HttpGetRequest(HttpContext context) +190)

SAML Token Error

Issue: The App Registration might fail with a SAML error similar to the image below:

Resolution: Make sure the system clocks of the servers involved are set to the same time. Claims requires that tokens be passed between systems within a 5 minute window.

Security Token Issues with IFrames and Cookies in Internet Explorer

Issue: At times in K2 for SharePoint an IFrame pops up requesting Login Method. You select a login method and end up going through the login loop, always ending up back on the login page.

Resolution: This issue is handled in a KB article: KB001556 Security Token Issues with IFrames and Cookies in Internet Explorer
On Premises SharePoint Apps and Configuration or the User Profile Service

Issue: Various authorization issues similar to the following are experienced:

- 401 access denied
- Cannot initialize client context
- Access denied when opening the K2 App from a List or Library

Resolution: The following steps are typical of a support call to determine if the issue is related to the User Profile Service:

1. Execute the following SMO as it will also give a 401 error if the profile is not good and we use this to check of the user is part of a group. (SharePoint/(Site)/Management/Group SMO with method "Is User In Any One Group" to get the Groups to check the permission). Try executing the SMO directly for this user getting the issue.
   Side note: the Method requires a GroupID and Username. Use SPM2013 to get the Group ID's or look at the URL when opening the group.

2. Check that the Profile Synchronization Service is running. Also check that it passed. "User Profile Service Application - System Job to Manage User Profile Synchronization" (Central Admin > Monitoring > Check Job)
3. For us to successfully validate permissions we need to check the SID and UPN (userPrincipalname) in SharePoint User Profiles. To check this, navigate to **Central Admin > Application Management > Service Applications > Manage Service Applications**. Find the User Profile Service Application (top node not the Proxy) “Manage Profile Service: User Profile Service Application” screen should be up now. On the right hand side of the page (see the image below), you can see if the service is running and also the number of profiles. This should not
be 0 if the service is running correctly.

4. If step 3 above is correct, navigate to the “People > Manage User Properties”. In here you’ll see all the properties the SharePoint User Profile synchronizes from Active Directory. Check if the SID and userPrincipalname is there.

Be sure the following properties are set for the user:

- For On Premises installations, we will require at least the SID property to be set on the user’s profile.
- If using external SAML claim users the Identifier claim configured on the trusted provider must be either UPN, email address, SIP address or NameId, and one of these properties must be set on the user’s profile.
K2 App installed with the System Account

**Issue:** An error occurs when the "Trust It" button is clicked when adding the K2 App to the site. The error occurs when the App is installed with the System Account, the SharePoint log file will show the error message that the System Account does not have permissions to perform the action.

**Resolution:** Add the K2 App using an account other than the System Account that has Site Collection rights and read rights in the App Catalog site.
For more information see: the MSDN article Add apps for SharePoint to a SharePoint 2013 site.
Copyright

© 2008-2014 SOURCECODE TECHNOLOGY HOLDINGS, INC. ALL RIGHTS RESERVED. SOURCECODE SOFTWARE PRODUCTS ARE PROTECTED BY ONE OR MORE U.S. PATENTS. OTHER PATENTS PENDING. SOURCECODE, K2, K2 BLACKPEARL, K2 BLACKPOINT AND K2 SMARTFORMS ARE REGISTERED TRADEMARKS OR TRADEMARKS OF SOURCECODE TECHNOLOGY HOLDINGS, INC. IN THE UNITED STATES AND/OR OTHER COUNTRIES. THE NAMES OF ACTUAL COMPANIES AND PRODUCTS MENTIONED HEREIN MAY BE THE TRADEMARKS OF THEIR RESPECTIVE OWNERS.