# logo-sql08.gif

Manage Kerberos Authentication Issues in a Reporting Services Environment

SQL Server Technical Article

**Writers:** Bhejpal Singh, Rama Raman, Reagan Templin

**Technical Reviewers:** Adam Saxton, Lukasz Pawlowski, Shawn Hernan, Carl Rabeler

**Contributors:** Chaitanya Medikondur, Marianne Willumsen, Vijay Krishnan

**Published:** April 2010

**Applies to:** SQL Server 2008

**Summary:** Using Kerberos authentication in a SQL Server 2008 Reporting Services service environment provides a mechanism for mutual authentication between client and server before a secure network connection is established. This article describes how to configure and troubleshoot a Reporting Services service environment to use Kerberos authentication with full delegation.

Copyright

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, SQL Server, Windows, Windows Server, SharePoint, Office, Internet Information Services (IIS), and Internet Explorer, are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[ 1](#_Toc260850681)

[Introduction 5](#_Toc260850682)

[Software Requirements 6](#_Toc260850683)

[Overview of Kerberos Authentication in Reporting Services 7](#_Toc260850684)

[Configure Kerberos Authentication for Reporting Services 9](#_Toc260850685)

[Configure the Domain Controller 10](#_Toc260850686)

[Obtain Environment Information 11](#_Toc260850687)

[Configure Service Principal Names (SPNs) 12](#_Toc260850688)

[Configure Trust for Delegation 14](#_Toc260850689)

[Configure Kerberos with Full Delegation 15](#_Toc260850690)

[Configure Authentication Types for Reporting Services 17](#_Toc260850691)

[Verify Service Account Group Membership or Local Security Policy Settings 17](#_Toc260850692)

[Verify Kerberos Authentication 18](#_Toc260850693)

[Configuration Scenarios Related to SPNs 18](#_Toc260850694)

[Access Required SPNs in Reporting Services Native Mode 18](#_Toc260850695)

[Access Required SPNs in Reporting Services Integration Mode 20](#_Toc260850696)

[Troubleshoot Kerberos Authentication Issues 21](#_Toc260850697)

[Troubleshoot Servers and Service Accounts 21](#_Toc260850698)

[Troubleshoot Browser Settings 22](#_Toc260850699)

[Troubleshoot Time Synchronization 22](#_Toc260850700)

[Troubleshoot Server and Configuration and Authentication Issues 23](#_Toc260850701)

[Troubleshoot Tools And Solutions 25](#_Toc260850702)

[Conclusion 26](#_Toc260850703)

[Glossary 27](#_Toc260850704)

# Introduction

When deploying Reporting Services in an environment that requires more than one server, such as a scale-out deployment or a deployment in a server farm, you may need to configure Kerberos authentication. Kerberos is particularly important when you require domain accounts to authenticate users but don’t need to pass user credentials to the database that is making the server connection.

**Note:** The goal of this paper is to provide information on how to configure, manage and troubleshoot Kerberos authentication. It does not cover specific deployment topologies for Reporting Services nor does it cover distributed environments like Scale Out deployment. It also does not cover SQL Reporting Services 2008 R2 / MOSS 2010/ IIS 7 (kernel mode authentication).

Kerberos authentication is supported in both Reporting Services deployment modes: Native and SharePoint integrated. With native mode, you can use a Web-based tool such as Report Manager, to upload and manage reports, models, and other items. With SharePoint integrated mode, you can integrate a Reporting Services service environment with a SharePoint product or technology to upload and manage reports, models, and other items.

Configuring Kerberos authentication also helps to avoid authentication failures that can occur because of a double-hop issue. Double-hop is an authentication issue in which a client’s domain credentials cannot be passed to two or more servers to process the client’s request.



**Figure 1:** A distributed environment with a security implementation that uses Kerberos authentication.

With the double-hop issue, NTLM credentials are valid for only one network “hop” from the place of log on. Each subsequent hop results in anonymous authentication.

For example, a client’s request, such as processing a report, must go through a Web server on its way to a database server for processing. Kerberos authentication enables the Web server to request a service ticket from the domain controller; impersonate the client when passing the request to the database server; and then restrict the request based on the user’s permissions. Each time a server is required to pass the request to another server, the same process must be used. This enables the server to act on behalf of the client for the next connection in the processing flow.



**Figure 2:** Overview of the steps to obtain a service ticket with Kerberos authentication.

When a client authenticates against a service using the Kerberos protocol, the process is as follows:

1. The client requests a ticket granting ticket (TGT) from the key distribution center (KDC).
2. The authentication service (domain controller) sends the encrypted TGT and session key to the client.
3. The client requests server access from the ticket granting service (TGS).
4. TGS sends the encrypted session key and service ticket to the client.
5. The client sends the service ticket to the server.
6. Optionally, the server can send an encrypted time stamp for client validation.

When users access reports that have data sources configured for Windows Integrated Authentication, their log on credentials are passed from the report server to the backend server that is hosted on a different computer. They cannot access reports from the backend server, until delegation is set on the middle tier computer such as the report server or the SharePoint server and service principal names (SPNs) are set for services like HTTP/MSSQLSvc (configured to use the domain account).

# Software Requirements

To deploy a Reporting Services service environment, you must first install the required products and technologies. If you chose to integrate your Reporting Services instance with a SharePoint product or technology, there are additional requirements over a native mode integration.

To determine the requirements for configuring Reporting Services, review the table below. To find the latest patches for your products and technologies, go to the [Microsoft Download Center](http://www.microsoft.com/downloads/en/default.aspx).

|  |  |  |
| --- | --- | --- |
| **Product or Technology** | **Mode** | **Requirement** |
| Operating System | N/A | Windows Server 2003, Windows Server 2008, 2008 R2 or Windows Vista (x86 or x64) |
| SQL Server Reporting Services | N/A | SQL Server 2008 Reporting Services instance |
| SQL Server Database Engine | N/A | SQL Server 2005 or SQL Server 2008 Database Engine instance that hosts the report server databases |
| Internet Information Services (IIS) | SharePoint integrated mode | IIS 6.0 running in worker process isolation mode (Windows Server 2003) or IIS 7.0 running in classic mode (Windows Server 2008) |
| SharePoint Product or Technology | SharePoint integrated mode | Windows SharePoint Services (WSS) 3.0 SP1 or Microsoft Office SharePoint Server (MOSS) 2007 SP1 |

**Table 1:** Software requirements for Reporting Services. N/A indicates that native and SharePoint integrated modes have the same requirements.

For more information, see the following:

[Hardware and Software Requirements for Installing SQL Server 2008](http://msdn.microsoft.com/en-us/library/ms143506.aspx)

[Requirements for Running Reporting Services in SharePoint Integrated Mode](http://msdn.microsoft.com/en-us/library/bb283190.aspx)

[Planning a Deployment Topology](http://msdn.microsoft.com/en-us/library/ms157293.aspx)

# Overview of Kerberos Authentication in Reporting Services

By default, Reporting Services uses Windows Integrated Authentication, which includes the Kerberos and NTLM protocols for network authentication. Additionally, Windows Integrated Authentication includes the negotiate security header, which prompts the client to select Kerberos or NTLM for authentication.

The client can access reports which have the appropriate permissions by using Kerberos for authentication. Servers that use Kerberos authentication can impersonate those clients and use their security context to access network resources.

You can configure Reporting Services to use both Kerberos and NTLM authentication; however this may lead to a failure to authenticate. With negotiate, if Kerberos cannot be used, the authentication method will default to NTLM. When negotiate is enabled, the Kerberos protocol is always used except when:

* Clients/servers that are involved in the authentication process cannot use Kerberos.
* The client does not provide the information necessary to use Kerberos.

The following illustration shows an overview of the NTLM authentication process and request flow.**Figure 3:** Overview of a request process using NTLM authentication.

When a client attempts to connect to the report server by making a request from a browser or other applications such as a custom application, Report Manager or a SharePoint site, the connection process begins with authentication. With NTLM authentication, client credentials are presented to Computer 2. However Computer 2 can’t use the same credentials to access Computer 3. To access Computer 3 it is necessary to configure the connection string with stored credentials (Reporting Services provides a feature to store your credentials).

The next illustration shows an overview of the Kerberos authentication process and request flow. When a client computer first attempts to connect to the report server, such as by making a request from a browser or other application such as a custom application, Report Manager or a SharePoint site, the connection process begins with authentication. With Kerberos authentication, the client and the server must demonstrate to one another that they are genuine, at which point authentication is successful and a secure client/server session is established.

**Figure 4:** Overview of Kerberos authentication request process.

In the illustration above, the tiers (computers) represent the following:

* Client tier (computer 1): The client computer from which an application, such as Report Manager, Report Builder, or SQL Server Management Studio, makes a request.
* Middle tier (computer 2): The Web server or farm where the client’s request is directed. Both the SharePoint and Reporting Services server(s) comprise the middle tier.

Native mode - Reporting Services server or farm.

Integration Mode (SharePoint) - WSS 3.0/MOSS 2007 server/farm might be on a different computer(s) than the Reporting Services server/farm.

* Back end tier (computer 3): The Database/Analysis Services server/Cluster where the requested data is stored. In a simple deployment, the middle tier and the back end tier are on the same computer.

# Configure Kerberos Authentication for Reporting Services

To enable Kerberos authentication it is necessary to:

* Configure the domain controller.
* Obtain environment information.
* Configure the SPNs.
* Configure trust for delegation for service accounts or servers.
* Configure Kerberos with full delegation.
* Configure authentication types for Reporting Services.
* Verify the service account group membership or local security policy settings.

## Configure the Domain Controller

The first step in the authentication process is to configure your domain controller. If you use a cross-domain environment, the domain controller must operate at the Windows Server 2003 functional level or the Windows Server 2008 functional level.

**Note:** You must be a domain administrator to complete the tasks in this article that pertain to active directory.

For more information on setting up a domain controller computer, see the [Windows Server 2003 or Windows Server 2008](http://technet.microsoft.com/en-us/library/cc733027%28WS.10%29.aspx) online product documentation on Microsoft TechNet or MSDN.

**To verify the functional level of the domain controller**

1. Go to the **Control Panel**.
2. From **Administrative Tools**, open **Active Directory Domain and Trust**.
3. Right-click the appropriate domain, and then click **Raise Domain Functional Level**.
4. Under **Current** **Domain functional level**, verify that it must be **Windows Server 2003** or **Windows Server 2008** is listed.



**Figure 5:** Windows 2003 domain functional level interface.



**Figure 6:** Windows 2008 domain function level interface.

## Obtain Environment Information

To continue configuring authentication, obtain the following information:

* The report server and database computer names. **Note:** In a SharePoint integrated mode deployment you also need the name of the Web front-end computer(s) and the database computer(s) that are hosting the content and configuration databases.
* The backend server names and connection information. You also need information on the service accounts used to configure the services, such as the connection string and server name.
* The service account: In both a native mode deployment and a SharePoint integrated mode deployment, you need the Reporting Services service account. In a SharePoint integrated mode deployment, you also need the application pool identity for SharePoint central administration and the SharePoint site(s) which will host reports.
* URLs for the report server’s Web service or SharePoint application URL: In a native mode deployment and a SharePoint integrated mode deployment, you need the report server Web service URL. In a SharePoint integrated mode deployment, you also need the SharePoint application URL.
* Alternate access mapping URL: In SharePoint integrated mode, you can configure multiple URLs for single internal URL. You will need a URL to host reports.

**To find the report server and database computer names and their URLS**

1. From the report server, open the **Reporting Services configuration manager,** and then connect to the Reporting Services instance where you need to verify information.

**Note:** For more information, see [How to: Start Reporting Services Configuration](http://msdn.microsoft.com/en-us/library/ms159644.aspx).

1. Select **Service account**, and then note the service account that is specified.
2. Select **Web service URL**, and then note the URL or URLs listed under **Report server Web service URLs** including their port numbers.
3. Select **Report manager URL**, and then note the URL or URLs listed under **Report manager URLs** including their port numbers (this is not required in SharePoint Integration Mode.)

**Note:** SQL Server 2008 Reporting Services uses a single service for executing both Web and Windows services and doesn’t depend on IIS, but rather interacts directly with HTTP.sys and establishes URL reservations.

**To find the application pool identity in IIS 6.0 for SharePoint Web sites that will host reports**

1. On the SharePoint Web front end WFE computer, open **IIS Manager**.
2. In the left pane, expand the server node, and then expand **Application pools**.
3. Right-click **SharePoint central admin v3,** and then click **Properties**. Repeat for the other SharePoint site that will host reports.
4. On the **Identity** tab, under **Application pool identity**, make a note of the account that is listed.

**To find the application pool identity in IIS 7.0 for SharePoint Web sites that will host reports**

1. On the SharePoint WFE computer, open **IIS Manager**.
2. In the **Connections** pane, expand the server node, and then click **Application Pools**.
3. On the **Application Pools** page, locate the **SharePoint site** application pool, and then make a note of the account listed in the **Identity** column.

Capture all the above mentioned details in the table; computer(s) names, Service accounts, URLs and AAMs. This will avoid a lot of repeated task and will help for your future references.

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Native/SharePoint mode** | **Delegation set (Computer/user)** | **SPNs set (Host/service account)** |
| **Server names** |  |  |  |
| **Server connections** |  |  |  |
| **Service accounts** |  |  |  |
| **URLs**  |  |  |  |
| **Alternate access mapping** |  |  |  |

**Table 2:** Table for recording the report server, URLs and database computer names.

##

## Configure Service Principal Names (SPNs)

SPNs are unique identifiers for services that run on servers; they are registered with a service class that identifies the account’s type of service. The SPN identifies information such as the computer on which the service runs, the account under which the service runs, and in some cases the port on which it runs. There are host SPNs that cover default services, when the local system or network service built-in accounts are used and the URL uses the computer name.

If built-in accounts are not used for application pool identities, then HTTP SPN must be set. Additionally, when a virtual URL is used with built-in accounts, and the service is configured with a domain account, each service that requires Kerberos authentication must have an HTTP SPN configured so that clients can identify the service on the network. If an SPN is not configured for a service, a client account will be unable to authenticate to the servers using Kerberos.

Before you configure or add SPNs, confirm that you are a domain administrator. You can then continue to configure the SPNs by using the SetSPN command-line utility. You can also access it directly from the domain controller.

**Note:** The SetSPN utility is installed by default on Windows Server 2008, but not on Windows Server 2003. You can install the utility from [Windows Server 2003 Service Pack 2 32-bit Support Tools](http://www.microsoft.com/downloads/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90) from the Microsoft Download Center or from the \Support\Tools folder on the Windows Server 2003 installation media. Alternately, you can use ADSI Edit, which is a Microsoft Management Console (MMC) snap-in.

**To add/list SPNs, use the following syntax**

Add SPN: setspn -A *ServiceClass*/*Host*:*Port* Domain\*ServiceAccount*

 List SPN: setspn -L Domain\*ServiceAccount*

The parameters for this syntax include:

* ServiceClass: There are different types of SPNs, and each service that runs on a computer must have the appropriate SPN service class assigned to it. If a Reporting Services service account is a domain account, you must use the HTTP SPN service class.
* Host: The host parameter specifies the name (either the computer name or a virtual name (alias)) on which the service is running. These names are defined by DNS Host records or your local Hostfile (host.ini). An SPN must be set for each name that is referenced in a URL, such as the NetBIOS name or the fully qualified domain name (FQDN).

Example: If report server is hosted on server (Contoso), then you need SPNs for NetBIOS (Contoso) and FQDN (Contoso.Domain.Corp.Company.com).

* ServiceAccount: Specifies the domain user name under which the service runs. If you are in a cross-domain environment, you must also include the domain in the format *domain\user*. If you are using the local system or network service built-in account with a virtual name, you must enter the machine name rather than a built-in account for Service account.
* Port: Specifies the port on which the service runs. Although you can omit this for services that use a default port (such as port 80 for HTTP), it is recommended to always include this parameter. Port is required for other SPNs, but not for HTTP SPNs. To fix this issue you can configure Web sites (Reporting Services /SharePoint Sites) to use Host Header. This avoids conflicts between SPNs.

For example, to add an SPN for a domain user account called **rssvcacct** on a computer named **contoso** in a domain named **domain.corp.company.com** andset theHost Header to **APP1** (Host Record in DNS) you would run the following commands:

**To add SPN with computer name**

setspn -A HTTP/contoso domain\rssvcacct

setspn -A HTTP/contoso.domain.corp.company.com domain\rssvcacct

**To add SPN With Host Header (App1)**

setspn -A HTTP/App1 domain\rssvcacct

setspn -A HTTP/App1.domain.corp.company.com domain\rssvcacct

Add the SPNs of any service accounts that need to process report requests. If you need to get data from a source (such as SQL Server or Analysis Services) that uses a different account to access the data, you must also add a SPN for that account. For example, if you have a report that pulls data from an Analysis Services cube, you must add the SPN using domain account that pulls the data. Use below links to know how to register SPNs for

SQL Server: <http://support.microsoft.com/kb/319723>

<http://technet.microsoft.com/en-us/library/ms191153.aspx>

Analysis Services: <http://support.microsoft.com/kb/917409>

To add an SPN for a server name or Host Header, use the following syntax at the command prompt, replacing **Host** with (NetBIOS or Host Header) and **ServiceAccount** with the account for which you want to register an SPN. You should add two SPNs: One for NetBIOS and one for FQDN.

**To create SPNs run the following command**

Setspn -A HTTP/**Host** **ServiceAccount**

**To list SPNs**

To verify that SPNs have been set for the service accounts, use the following syntax at the command prompt, and then replace ***ServiceAccount*** with the name of the service account for which you want to verify SPNs:

setspn -L Domain\*ServiceAccount*

To learn whether you have duplicate SPNs set for the service accounts, use the following syntax at the command prompt, and then replace ***ServiceAccount*** with the name of the service account for which you want to verify SPNs. X is a new command and available with Windows 2008 Server tools. To use the X command on Windows 2003 Server download the SetSPN utility from [Microsoft support](http://support.microsoft.com/kb/970536).

setspn –X Domain\*ServiceAccount*

When you add a computer to a domain, a new computer account is created in Active Directory and by default, host SPNs are automatically added for built-in accounts such as Network Service and Local Service. When you list the SPNs, you should see those HOST SPNs. If there are no SPNs listed for your service account, or an SPN is missing or incorrectly registered, use the **setspn** commands to correct the problem.

## Configure Trust for Delegation

If you want to use the Kerberos credentials against the backend server (such as Reporting Services to SQL Server) it is necessary to configure trust for delegation. In this context, *delegation* refers to enabling a computer to impersonate an authenticated user to services on another computer.

### Delegation Requirements

The following list describes the requirements for delegation.

|  |  |
| --- | --- |
| **Location** | **Description** |
| Client | 1. The requesting application must support the Kerberos authentication protocol.
2. The user account making the request must be configured on the domain controller. Confirm that the following option is not selected: **Account is sensitive and cannot be delegated**.
 |
| Servers | 1. The service accounts must be trusted for delegation on the domain controller.
2. The service accounts must have SPNs registered on the domain controller. If the service account is a domain user account, the domain administrator must register the SPNs.
 |

**Table 3:** Delegation requirements in the Reporting Services deployment.

Use the following procedures to configure the domain controller for delegation.

**To verify settings for domain user accounts used to access reports/application**

1. Go to the **Control Panel**.
2. From **Administrative Tools**,open **Active Directory Users and Computers**.
3. Locate the domain user account, right-click the user account, and then click **Properties**.
4. On the **Account** tab, under **Account options**, verify that the following option is not selected: **Account is sensitive and cannot be delegated**.



**Figure 7:** The **Account** tab in the **User Properties** dialog box.

## Configure Kerberos with Full Delegation

**To configure the middle tier computer/user account to use Kerberos with full delegation**

1. Go to the **Control Panel**.
2. From **Administrative Tools**, open **Active Directory Users and Computers**.
3. Locate the middle tier computer/user account, right-click it and then click **Properties**.
4. On the **Delegation** tab, verify that the following options isselected: **Trust this computer for delegation to any service (Kerberos only)**.

**Note:** If the **Delegation** tab is not visible, there is no SPN configured for the account. Add an SPN and then perform the procedure.

**To verify the middle tier computer is trusted for delegation**

1. Go to the **Control Panel**.
2. From **Administrative Tools**, open **Active Directory Users and Computers**.
3. Locate the middle tier computer. Right-click the computer, and then click **Properties**.
4. On the **Delegation** tab, verify that the following option is selected:**Trust this computer for delegation to any service (Kerberos only)**



**Figure 8:** The **Delegation** tab in the **Computer Properties** dialog box.

**To verify that the domain account used as the service account on the middle tier is trusted for delegation**

1. Go to the **Control Panel**.
2. From **Administrative Tools**, open **Active Directory Users and Computers**.
3. Locate the domain account used as the service account, right-click the user account, and then click **Properties.**
4. On the **Delegation** tab, verify that the following options isselected: **Trust this computer for delegation to any service (Kerberos only)**.

****

**Figure 9:** The **Delegation** tab in the **SQL Service Properties** dialog box

## Configure Authentication Types for Reporting Services

For Reporting Services to use Kerberos authentication, you must ensure that the authentication types are configured correctly in the Reporting Services configuration file (**rsreportserver.config**) of each individual browser.

For Internet Explorer, use **RSWindowsNegotiate for Authentication Type** which is specific to Windows/SPNEGO. For other browsers use **RSWindowsKerberos**.

**To configure authentication types for Reporting Services**

1. On the middle tier computer(s), go to: *drive*:\Program Files\Microsoft SQL Server\MSRS10.*InstanceName*\Reporting Services\ReportServer then open **rsreportserver.config** with a text editor such as Notepad.
2. To enable RSWindowsNegotiate, locate the **Authentication** section, and then ensure that the section is configured as follows:

<Authentication>

 <AuthenticationTypes>

 <RSWindowsNegotiate/>

 </AuthenticationTypes>

 <EnableAuthPersistence>true</EnableAuthPersistence>

</Authentication>

## Verify Service Account Group Membership or Local Security Policy Settings

After installation, the Reporting Services Service Account SID is assigned to the SQLServerReportServerUser$Server$MSRS10.MSSQLSERVER local group, which is then assigned to the IIS group. If they are not added by default, add the account to the groups mentioned below.

* IIS\_WPG group (if you have a SharePoint integrated mode deployment and are using IIS 6.0).
* IIS\_IUSRS group (if you have a SharePoint integrated mode deployment and are using IIS 7.0).
* The appropriate local policy rights (if you have a native mode deployment). The appropriate local policy rights are: Log on as a service; Access this computer from the network; and Impersonate a client after authentication.

The IIS\_WPG user group provides the minimum set of privileges and permissions that are required to start and run worker processes in IIS. For more information about the IIS\_WPG group, see [Configuring Application Pool Identity in IIS 6.0 (IIS 6.0)](http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/12a3d96c-65ea-4210-96ad-86a801f6a88c.mspx?mfr=true).

**To verify membership in the IIS\_WPG or IIS\_IUSRS group (IIS 6.0 or IIS 7.0 only)**

1. On the middle tier computer or computers, open **Local Users and Groups**.
2. Click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
3. In the tree, expand **Local Users and Groups**, and then click **Groups**.
4. Right-click **IIS\_WPG** or **IIS\_IUSRS**;verify that the **Members** list includes the service account.

**To verify local policy rights**

1. On the middle tier computer(s), open **Local Security Policy**.
2. Click **Start**, point to **Administrative Tools**, and then click **Local Security Policy**.
3. In the tree, expand **Local Policies**, and then click **User Rights Assignment**.
4. In the right pane, verify that the **Security Setting** column includes the service account next to the appropriate policies.

# Verify Kerberos Authentication

Once you have configured the middle tier and back end tier computers in your environment, verify that Kerberos authentication is working.

**To verify Kerberos authentication**

1. Open **Report Manager** (if in a native mode deployment) or a SharePoint library (if in a SharePoint integrated mode deployment) that contains reports or report items.
2. To browse **Report Manager** or the SharePoint library, use a client or a server in your current domain.
3. Run a report that uses a data source that is configured for Windows Integrated Authentication.

If there is a log on problem (either from a remote server or in SharePoint integration mode) or if the report fails to render, the possible errors include a 401.1 Access Denied page or a blank page. To fix the problem, add a registry key for the disableloopbackcheck by following the instructions in the support article: [You receive error 401.1 when you browse a Web site...](http://support.microsoft.com/kb/896861). If method 1 in the article solves the problem, delete the key that was added in method 1, and then add a new key by following method 2 in same article.

# Configuration Scenarios Related to SPNs

The following sections illustrate how to configure SPNs for Kerberos authentication with Reporting Services in native and SharePoint integrated modes. Other configurations such as Delegation for Service Account (or machine) or modifying config files with appropriate authentication type (RSWindowsNegotiate, RSWindowsKerberos) were documented in the previous section.

## Access Required SPNs in Reporting Services Native Mode

**Scenario 1:** Access reports through the report manager using the machine’s name.

When Reporting Services runs under a domain’s user account instead of under the default network service account, set the SPN for the HTTP service under the domain account. In this scenario, you access the Reporting Services by using either the NetBIOS name or the FQDN of the Reporting Services server.

**A)** Service Account use: Built-in account (network service/local system)

When you run the Reporting Services service under a default account such as the network service account, the local service account, or the local system account, by default Kerberos will use Host SPNs (which register themselves).

HOST/NETBIOS

HOST/FQDN\_OF\_SERVER

**B)** Service Account uses: Domain user account (domain\user)

When you run the Reporting Services service under a domain user account, use the following command:

setspn –A HTTP/NETBIOS\_NAME\_OF\_SERVER *domain\username*

In this command, *NETBIOS\_NAME\_OF\_SERVER* is the NetBIOS name of the Reporting Services server.

To access the Reporting Services sites by using the NetBIOS name, use the following command, where *NETBIOS\_NAME\_OF\_SERVER* is the NetBIOS name of the Reporting Services server:

setspn –A HTTP/ NETBIOS\_NAME\_OF\_SERVER *domain\username*

Example: Setspn –A HTTP/RSserver mydomain\rssvcacct

To access the Reporting Services sites by using the FQDN, use the following command, where *FQDN\_OF\_SERVER* is the FQDN of the Reporting Services server:

setspn –A HTTP/FQDN\_OF\_SERVER domain\username

Example: Setspn –A HTTP/RSserver.mydomain.com mydomain\rssvcacct

**Scenario 2:** Access reports where Reporting Services is using a Host Header.

When you access a Reporting Services instance by using a Host Header, you must set an SPN for the HTTP service.

**A)** Service Account use: Built-in account (network service/local system)

When you run the Reporting Services service under a default account such as the network service account, the local service account, or the local system account, use the following command:

setspn –A HTTP/*HOSTHEADER\_OR\_DNS\_ALIAS NETBIOS \_NAME\_OF \_SERVER*

In this command, *HOST\_HEADER* is the Host Header that you type in a browser window to access the Reporting Services sites, and *NETBIOS\_NAME\_OF \_SERVER* is the NetBIOS name of the server where we installed Reporting Services.

Example: setspn –A HTTP/www.test.com Contoso

**B)** Service Account uses: Domain user account (domain\user)

When you run the Reporting Services service under a domain user account, use the following command:

setspn –A HTTP/*HOSTHEADER\_OR\_DNS\_ALIAS domain\username*

In this command, *HOSTHEADER\_OR\_DNS\_ALIAS* is the Host Header or DNS alias that you use to access the Reporting Services sites.

Example: setspn –A HTTP/www.test.com mydomain\rssvcacct

## Access Required SPNs in Reporting Services Integration Mode

**Scenario 1:** When you want to configure one server in SharePoint integrated mode that has Reporting Services in SharePoint integrated mode and a single SharePoint WFE installed.

In this scenario, you must use the same domain user account to run the Reporting Services service and the application pool identity of the SharePoint site.

The report server Web service runs in HTTP.SYS. A by-product of creating an SPN for HTTP is that all Web applications on the same computer that run in HTTP.SYS (including applications hosted in IIS) will be granted tickets based on the domain user account. If those services run under a different account, the authentication requests will fail. To avoid this problem, configure all HTTP applications to run under the different domain accounts, or consider creating Host Headers for each application and then creating separate SPNs for each Host Header. When you configure Host Headers, DNS changes are required regardless of the Reporting Services configuration.

**Scenario 2:** When Reporting Services in SharePoint integrated mode and a SharePoint WFE are installed on different servers.

In this scenario, you will need to follow the steps mentioned in Reporting Services configuration in native mode; setting up of the HTTP service SPNs.

Set SPNs for Reporting Services, SharePoint and SQL Server on different servers

**Reporting Services:**

Server Name: ReportingServices (Default Instance)

URL:  [http://ReportingServices/reportserver](http://reportingservices/reportserver)

Service Account: mydomain\rssvcacct

**SharePoint:**

Server Name: SPS1

Services: Central Administrator

 Web Application Services

Application Pool Identity: mydomain\sharepointsvc

Central Admin URL: [Http://SPS1/\_default.aspx](http://SPS1/_default.aspx)

SharePoint site: <http://Test.mydomain.com>

Test: It is a Host Header for the Web site and it is an A-Record in DNS

**SQL Server:**

Server Name: sqlserver

Service Account: mydomain\sqlsvc

Steps for configuring SPNs for the above environment: Set SPNs for the SharePoint Site, Central Administrator site, Reporting Services and SQL Server.

**SharePoint Site:**

Setspn –a http/test  mydomain\sharepointsvc

Setspn –a http/test.mydomain.com mydomain\sharepointsvc

**Note**: Because a Host Header is used for the Web site, create an SPN for the URL.

**Central Administrator:**

Setspn –a http/SPS1  mydomain\sharepointsvc

Setspn –a http/SPS1.mydomain.com mydomain\sharepointsvc

**Note**: Because no Host Header is used for the central administrator site, create the SPNs for the computer where the central administrator is hosted.

**Reporting Services:**

Setspn –a http/ReportingServices mydomain\rssvcacct

Setspn –a http/ReportingServices.mydomain.com  mydomain\rssvcacct

**Note:** Because no Host Header is used for the report server, it is necessary to create SPNs for the computer where the report server is hosted.

**SQL Server:**

Setspn –a MSSQLSvc/sqlserver:1433  mydomain\sqlsvc

Setspn –a  MSSQLSvc/sqlserver.mydomain.com:1433  mydomain\sqlsvc

**Note:** Provide the port on which the SQL Server is listening and the server name. For the default instance the port is: 1433.

# Troubleshoot Kerberos Authentication Issues

This section provides troubleshooting tips for server and service accounts, browser settings, time synchronization, and configurations that were missed or set incorrectly.

## Troubleshoot Servers and Service Accounts

If you encounter issues with Kerberos authentication in your Reporting Services service environment, verify that:

* The SPNs are configured correctly for the service accounts. For more information, see [Configure Service Principal Names (SPNs)](#_Configure_Service_Principal_1) in this article.
* The service accounts for the middle tier computer(s) are trusted for delegation in the Active Directory on the domain controller. For more information, see [Configure Trust for Delegation](#_Configure_Trust_for_1) in this article.
* The Reporting Services configuration file is configured with the RSWindowsNegotiate authentication type. For more information, see [Configure Authentication Types for Reporting Services](#_Configure_Authentication_Types_1) in this article.
* The service accounts for the middle tier computer or computers are part of the right group or have the appropriate local policy settings. For more information, see [Verify Service Account Group Membership or Local Security Policy Settings](#_Verify_service_account) in this article.

## Troubleshoot Browser Settings

Authentication can fail due to certain settings in Internet Explorer (IE).

**Problem:** Your Windows credentials are not being accepted. This is most likely because the **Enable Integrated Windows Authentication (requires restart)** setting is not selected in IE 6.0.

**Solution:** Enable IE 6.0 to pass your Windows credentials.

**Note:** This occurs only with IE 6.0 on Windows XP or 2000 Server (Kerberos Authentication is the default protocol for IE 6.0 or later). For more information, see [Internet Explorer does not support Kerberos authentication with proxy servers](http://support.microsoft.com/kb/321728/) on the Microsoft Support site.

**To change the Windows Authentication setting**

1. In IE, on the **Tools** menu, click **Internet Options**.
2. Click **Advanced**, click **Security**, select **Enable Integrated Windows Authentication (requires restart),** and then click **OK**.
3. Close and then restart IE.

**Problem:** IE is accessing a site in the Internet zone instead of the intranet zone.

**Solution:** Add an Internet site to the local intranet sites list**.**

**To add an Intranet site**

1. On the **Tools** menu, click **Internet Options**.
2. Click **Security**, click **Local Intranet**, click **Sites**, and then click **Advanced**.
3. In the box under **Add this Web site to the zone**, type the name of the Web site that you want to authenticate with Kerberos authentication, then click **Add**.
4. Click **Close**, and then click **OK**.

## Troubleshoot Time Synchronization

**Problem:** Kerberos authentication won’t work if the time (on both the client and the domain) isn't synchronized.

**Solution:** Synchronize time on the client and the domain**.**

**To synchronize time on the client and the domain**

1. On the domain controller, open the **Local Group Policy Editor** MMC snap-in. You can open the editor by running the gpedit.msc command in the **Run** dialog box.
2. Click **Computer Configuration**.
3. Expand **Windows Settings**, click **Account Policy**, and then click **Kerberos Policy**.
4. Configure the security setting for **Maximum tolerance for computer clock synchronization**.

For more information, see [How to manually sync time between domain client and local time server](http://support.microsoft.com/kb/555225) and [Maximum tolerance for computer clock synchronization](http://technet.microsoft.com/en-us/library/cc779260%28WS.10%29.aspx) on the Microsoft Support site.

## Troubleshoot Server and Configuration and Authentication Issues

Computer 1

Computer 2

Windows Integrated

Authentication

Computer 2

Windows Integrated Authentication

Windows Integrated Authentication

Computer 1

Computer 3

Anonymous!

NTLM

**Figure 10:** A one box and a multiple box deployment and their security implementations. Windows Integrated security requires Kerberos authentication in a double-hop scenario.

### Authentication Type Is Not Configured Correctly

Reports can fail when using Windows Integrated Authentication (they may work locally, but fail when run remotely). Users receive error messages such as:

Login failed for User ‘(null)’

Login failed for User ‘NT Authority\Anonymous’

Login failed for User ‘ ‘

**Problem:** The Authentication Type in the Reporting Services configuration file, respeportserver.config, is not configured correctly.

**Solution**: Set the **Authentication Type** element in rsreportserver.config to RSWindowsNegotiate or RSWindowsKerberos (for browsers that don’t support Windows/SPNEGO). If using an IE browser, set the value to RSWindowsNegotiate. If using a browser other than IE, set the value to RSWindowsKerberos. For more information, see [Authentication Types in Reporting Services](http://msdn.microsoft.com/en-us/library/cc281310.aspx) in the MSDN library.

### Delegation Is Not Enabled

Reports can fail if they are obtaining data from a remote server. You may be unable to browse the reports URL or the report server URL and you may receive the following errors:

Login failed for User ‘(null)’

Login failed for User ‘NT Authority\Anonymous’

Login failed for User ‘ ‘

**Problem:** Middle tier servers or service accounts are not configured for delegation.

**Solution:** Verify that the delegation is enabled for the machine account or user account depending on which service the account is configured for (for example, a local system would require the machine account to delegate because it would be under the context of the machine account).

### **SPNs are configured or spelled incorrectly**

An inability to authenticate is often related to SPN issues. For example, you can access a database hosted on the report server, but when accessing a database on a remote server, one of the following occurs: You receive the error “Login failed for NT Authority\Anonymous;” you are unable to view reports; you are prompted for credentials three times and either receive a blank page or the error, “HTTP Error 401.1 – Unauthorized: Access is denied due to invalid credentials, on the remote computer.”

**Problem:** An SPN is registered for computer and service accounts with different ports being configured with the same SPN using the same Service Account.

Errors can include: MSSQLSvc/appsql01.coadvantage.com:1433

MSSQLSvc/appsql01.coadvantage.com:2746. SQL is configured to listen only on port 2746.

The SPN’s HTTP/appsql:8080 and HTTP/appsql.

**Solution:** Configure the SPN for the correct port and remove any duplicate SPNs.

**Problem:** SPNs are misspelled or missing.

Common misspellings include omitting spaces or using backslashes instead of slashes. For example, HTTP\pcrmc-webrpt2 instead of HTTP/pcrmc-webrpt2 or MSSQLSvs/Server:49536 instead of MSSQLSvc/Server:49536.

**Solution:** Verify that the SPNs exist and that their format and spelling are correct. Create a new SPN if it is missing.

For more information see [Configuration Scenarios Related to SPNs](#_Configuration_Scenarios_Related) in this article.

### Kerberos Authentication Not Configured During Installation of Reporting in SharePoint Integrated Mode

If you click the **Set Server Defaults** page during configuration of the Reporting Services add-in for SharePoint technologies and receive the error "Server was unable to process request. ---> The request failed with HTTP status 401: Unauthorized" the issue is probably related to configuration of Kerberos during installation.

**Problem:** Kerberos authentication was not configured when Reporting Services was installed in SharePoint integrated mode, or SharePoint sites aren’t configured for Kerberos, or the sites are not in the Default zone.

**Solution**: Change the authentication providers on the SharePoint sites used by Reporting Services to use Kerberos.

**To check and configure SharePoint site for Kerberos authentication**

1. Open **Central Administration,** and then click **Application Management.**
2. Under **Application Security**, click **Authentication Providers**.
3. Click the zone to modify (Default Zone).
4. In the **IIS Authentication Settings,** select **Negotiate** (Kerberos).
5. Click **Save**. Repeat these steps for other sites that require a change of authentication.

**Note:** It is beyond the scope of this paper to discuss other SharePoint configurations that may not work as expected. For more information, see [Reporting Services SharePoint Integration Troubleshooting](http://msdn.microsoft.com/en-us/library/ee384252.aspx) in the SQL Server Developer Center.

##

## Troubleshoot Tools And Solutions

Additional Kerberos authentication troubleshooting tools and solutions are available, including:

* Windows event logs provide tracing of detailed Kerberos events. For more information, see [How to enable Kerberos event logging](http://support.microsoft.com/kb/262177).
* Kerbtray.exe displays the Kerberos tickets that are acquired by a computer, and can purge Kerberos tickets if necessary. For more information, see [Windows Server 2003 Resource Kit Tools](http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd).
* To help find Kerberos related errors, Network Monitor captures network traces. To download, go to the [Microsoft Download Center](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=983b941d-06cb-4658-b7f6-3088333d062f). For more information about using Network Monitor, see [How to capture network traffic with Network Monitor](http://support.microsoft.com/kb/148942) (article ID 148942).
* DelegConfig (Delegation / Kerberos Configuration Tool) is an ASP.NET application used to configure Kerberos and delegating credentials. **Note:** IIS must be installed on any server that is using Kerberos authentication. For more information, see [Delegation / Kerberos Configuration Tool](http://www.iis.net/downloads/default.aspx?tabid=34&g=6&i=1887).
* The LDIFDE tool captures import/export information from or to the Active Directory. For more information, see [Using the LDIFDE Tool](http://msdn.microsoft.com/en-us/library/ms870068%28EXCHG.65%29.aspx).
* The SetSPN utility allows you to create and view SPNs. For more information, see [Setspn.exe support tool update for Windows Server 2003](http://support.microsoft.com/kb/970536), [Setspn Overview](http://technet.microsoft.com/en-us/library/cc773257%28WS.10%29.aspx), and [Windows 2000 Resource Kit Tool: Setspn.exe](http://www.microsoft.com/downloads/details.aspx?FamilyID=5fd831fd-ab77-46a3-9cfe-ff01d29e5c46&displaylang=en).

# Conclusion

Whether you have a native mode deployment or a SharePoint integrated mode deployment in your Reporting Services service environment, you can successfully configure and troubleshoot Kerberos authentication issues. Correct configuration of service accounts is critical to ensuring that these accounts can successfully impersonate the requesting user during request processing. When these accounts are incorrectly configured, you can use the tools and information in this paper to uncover additional information and troubleshoot problems.

**For more information, see the following:**

[Active Directory Domain Services Overview](http://technet.microsoft.com/en-us/library/cc731053.aspx)

[Deploying a Business Intelligence Solution Using SharePoint, Reporting Services, and PerformancePoint Monitoring Server with Kerberos](http://sqlcat.com/technicalnotes/archive/2009/10/13/deploying-a-business-intelligence-solution-using-sharepoint-reporting-services-and-performancepoint-monitoring-server-with-kerberos.aspx)

[Kerberos Authentication Technical Reference](http://technet.microsoft.com/en-us/library/cc739058.aspx)

[Kerberos Enhancements](http://technet.microsoft.com/en-us/library/cc749438%28WS.10%29.aspx)

[Kerberos Protocol Transition and Constrained Delegation](http://technet.microsoft.com/en-us/library/cc739587.aspx)

[Microsoft CRM 3.0: Additional Setup Tasks Required if Reporting Services Is Installed on Different Server](http://www.microsoft.com/downloads/en/confirmation.aspx?familyId=51bf9f20-bd00-4759-8378-b38eefda7b99&displayLang=en)

[Microsoft Negotiate](http://msdn.microsoft.com/en-us/library/aa378748%28VS.85%29.aspx)

[Microsoft NTLM](http://msdn.microsoft.com/en-us/library/aa378749%28VS.85%29.aspx)

[Microsoft Kerberos](http://msdn.microsoft.com/en-us/library/aa378747%28VS.85%29.aspx)

[Microsoft SQL Server 2008](http://www.microsoft.com/sqlserver/)

[Microsoft SQL Server Developer Center](http://msdn.microsoft.com/en-us/sqlserver/default.aspx)

[Microsoft SQL Server TechCenter](http://technet.microsoft.com/en-us/sqlserver/)

[Registering a Service Principal Name](http://technet.microsoft.com/en-us/library/ms191153.aspx)

[Reporting Services SharePoint Integration Troubleshooting](http://msdn.microsoft.com/en-us/library/ee384252.aspx)

[SQL CAT Site](http://sqlcat.com/tags/Reporting%2BServices/default.aspx)

[Troubleshooting Kerberos Delegation](http://www.microsoft.com/downloads/details.aspx?familyid=99b0f94f-e28a-4726-bffe-2f64ae2f59a2&displaylang=en)

[What is Kerberos Authentication?](http://technet.microsoft.com/en-us/library/cc780469.aspx)

[Windows Authentication](http://technet.microsoft.com/en-us/library/cc755284.aspx)

**Feedback:**

Did this paper help you? Please give us your feedback. Tell us on a scale of 1 (poor) to 5 (excellent), how would you rate this paper and why have you given it this rating? For example:

* Are you rating it high due to having good examples, excellent screen shots, clear writing, or another reason?
* Are you rating it low due to poor examples, fuzzy screen shots, or unclear writing?

This feedback will help us improve the quality of white papers we release.

Send feedback.

# Glossary

Active Directory: A Windows directory service that provides a distributed database, which stores and manages information about network resources and application-specific data from directory-enabled applications. For example, Active Directory stores information about user accounts, such as names, passwords, and phone numbers, and enables other authorized users on the same network to access this information. The computer that runs Active Directory is referred to as the domain controller.

Constrained delegation: An extension to the Kerberos protocol that allows a service to obtain service tickets (under the delegated user’s identity) to a subset of other services after it has been presented with a service ticket that is obtained from either the TGS\_REQ protocol (as defined in IETF RFC 1510) or in the protocol transition extension.

Domain Name System (DNS): A system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP networks, such as the Internet, to locate computers and services through user-friendly names. When a user enter a DNS name in an application, DNS services can resolve the name to other information associated with the name, such as an IP address.

Double-hop: an authentication problem in which a client’s domain credentials cannot be passed to two or more servers, to process the client’s request. With the double hop issue, NTLM credentials are valid for only one network “hop” from the place of log on. Each subsequent hop results in anonymous authentication.

Kerberos: An authentication protocol that defines how client computers interact with a network authentication service. Clients obtain tickets from the Kerberos Key Distribution Center (KDC), and they present these tickets to server computers when connections are established. Kerberos tickets represent the client’s network credentials.

Negotiate: An authentication protocol that selects either Kerberos or NTLM to handle authentication requests to the report server.

NTLM: An authentication protocol that uses a challenge-response mechanism to authenticate a user.

Native mode: Describes the installation mode of a Reporting Services service environment that is not integrated with a SharePoint farm.

SharePoint integrated mode: Describes the installation mode of a Reporting Services service environment that is integrated with a SharePoint farm.

Service Principal Name (SPN): The name by which a client can uniquely identify an instance of a service.

Protocol transition: An extension to the Kerberos protocol that allows a service that uses Kerberos to obtain a service ticket on behalf of a Kerberos principal to the service without requiring the principal to initially authenticate to the Kerberos Key Distribution Center (KDC) with a credential.

Service SID: A new process isolation mechanism in Windows Vista and Windows Server 2008 that enables a service to restrict ACLs on resources, preventing other processes running within the same service from accessing the service’s resources by default.

Unconstrained delegation: Method of delegation that is not constrained to a specific set of services on a system.

Web Front End (WFE): The architectural tier to which clients connect in order to access reports and the reporting environment. In SharePoint integrated mode, this refers to the SharePoint site that is integrated with Reporting Services and from which users access the reporting environment.