



BI Office

Kerberos and Delegation

Version 6.5

Copyright BI Office Analytics 2010-2018

- I. Overview..... 3
- II. Delegation Introduction 5
 - A. Kerberos Prerequisites 5
 - B. Application 5
 - C. General Mechanics 6
 - D. Adding DNS Host 7
 - E. Web-Farm Deployment 9
 - F. Effective Tokens 11
 - G. Testing the Configuration 11
- III. Delegation with System Account..... 12
- IV. Delegation with Domain Account..... 15
- V. Appendix..... 22
 - A. Other Documentation & Tools 22
 - B. SQL Server Analysis Services SPN Configuration 22
 - C. Client Browser Settings 23
 - D. IIS Configure Windows Authentication 24
 - E. Access Token Limitation Problem with Kerberos 26
 - F. Verifying the Flow of Kerberos Tickets 27
 - G. General Troubleshooting..... 28
 - H. Windows Authentication Check List 30

I. Overview

When deploying BI Office across multiple servers, Kerberos and Delegation needs to be configured.

NOTE: This is **NOT** necessary in a single machine deployment of BI Office and SQL Server Analysis Services or if installation has been configured to use token authentication (default).

I. Constrained vs. Full Delegation

When setting a server to allow full trust (unconstrained) delegation, a Kerberos token from any service will be transferred to another service on the target server from the source machine. Constrained delegation, a more complicated implementation model, allows you to define which service on which target machine will accept the Kerberos token.

II. Local Service Account vs. Domain Account

When setting up BI Office services, administrators can also elect to use the default local service accounts or domain account. By **default**, the application is installed with the local services account using full delegation.

There are multiple machine deployment scenarios:

- Full delegation under a service account (default)
- Full delegation with a domain account
- Constrained delegation under a service account
- Constrained delegation with a domain account

NOTE: All Active Directory settings must be set by a domain administrator with permissions.

The diagram below provides a conceptual overview of each installation type.

BI Office Delegation Flows



SPN abbreviations
 P.S.A = Pyramid.Server.Application
 P.S.R = Pyramid.Server.Router
 P.S.P = Pyramid.Server.Publisher
 URL = Name of Pyramid website URL

Local Service Account SPN Structure
 Service/{machine NetBios}
 Service/{machine FQDN}

Domain Account SPN Structure
 Service/{machine NetBios} {domain account}
 Service/{machine FQDN} {domain account}

Required SPNs for Delegation
 Full + Constrained Delegation
 Constrained Delegation (extra)

Note: on internal DNS hosted sites, a second "HTTP" SPN needs to be added for the URL using the 'URL FQDN'

II. Delegation Introduction

When the BI Office server applications and/or Analysis Services (SSAS) are deployed on separate machines, administrators must configure Kerberos delegation in the Active Directory for authentication and processing to succeed. The Active Directory provides an option through Kerberos delegation to pass the user's credentials from the client application to the Web server, and then on to other servers and finally to SSAS.

The Double Hop

Kerberos authentication can produce issues when there is a multi-leg or "double-hop" between multiple servers. The *double-hop* problem is an intentional security restriction to discourage Active Directory objects from acting on behalf of other security accounts.

In the BI Office application, a double-hop is created when there is one hop from the client to the Web server (IIS) and one or more other hops from the Web server to one or more application servers (or the data server).

Kerberos is required to solve this problem.

A. Kerberos Prerequisites

Prior to these configuration steps, your environment should have the following prerequisites. If any of these items are not configured, delegation might not function correctly.

- Check your Active Directory Forest and Domain functional levels. They should be set to Native or 2003/2008/2012.
 - Windows 2008 machines should have the Microsoft [hotfix KB969083](#) applied to correct the Kerberos issues with SQL Server SSAS 2005/8/12/14/16. This does not need to be applied to Windows 2008 R2 / 2012 / 2016.
- Kerberos delegation can function between trusted forests and domains.

The resource forest or domain must trust the user forest or domain.

B. Application

Depending on your deployment choices, certain configurations may or may not be possible. The choices include:

- Which authentication option you choose - Basic, Windows, Forms, Federated Forms.
- If you're using an Active Directory or the Local machine security ("local OS").
- If you plan to deploy to a single server or multiple machines.
- The type of browser your clients will use (IE and FireFox on a PC, Safari on a Mac). See [Client Configuration](#) for more information.
- The type of delegation you wish to deploy: constrained or unconstrained delegation.

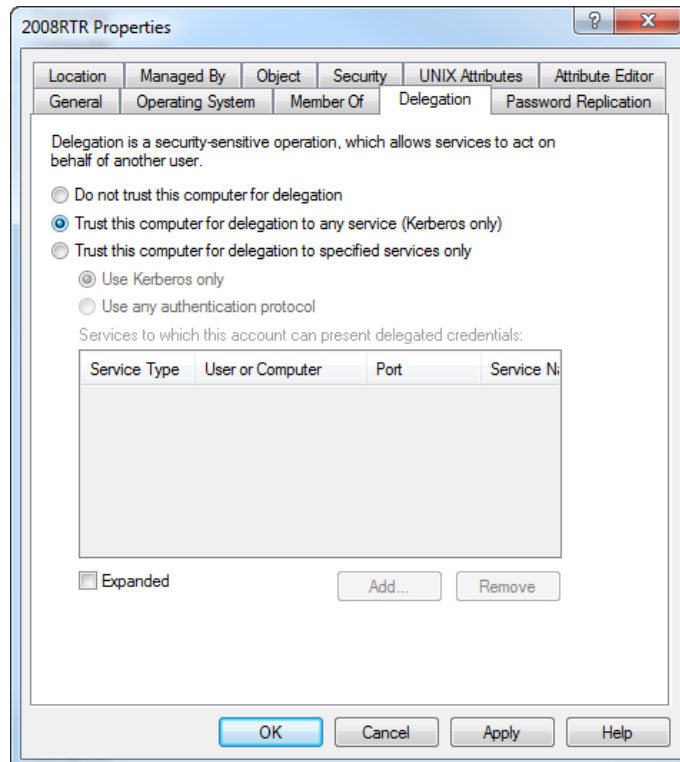
C. General Mechanics

I. Kerberos Delegation on the Active Directory

The “accounts” hosting parts of the application must be able to “delegate” tokens or rights – including the Web servers and servers hosting the router and application services. If the “account” is the “local service” the account is effectively the machine itself. If the account is a domain account, it’s the domain account in the active directory.

To set Full Delegation:

- Open the Active Directory “Users and Computers” panel in the administrative tools on the active directory server (see below).
- From the tabs, choose Delegation and set it to Trust Computer/Account for Delegation to any Service.



Delegation Panel (Win 2008/2012)

II. Setting Service Principal Names (SPNs)

SPNs are “addresses” - they specify the location and type of a specific service running under a specific account in the system. They are **critical** to the delegation process, because they allow the entire platform to direct requests to the right address while also indicating which addresses the source server has the right to delegate to.

Adding an SPN

In a command prompt (with appropriate domain administrative rights) execute the following:

```
Setspn.exe -s SERVICE/<host name> <host account>
Setspn.exe -s SERVICE/<fully qualified domain host name> <host account>
```

- If installing under the local services, the host account is the machine name followed by a “\$” sign.
- If installing under a domain account, the host account is the domain account name.
- If installing an HTTP service the host name is the host header or URL of the website.

Duplicate SPNs break Kerberos Authentication. As such, once completed, run the following to ensure there are no duplicate SPN entries: `Setspn.exe -x` or `-q <SPN>`

III. Client Configuration

User Accounts

User accounts on the Active Directory, by default, should not need additional configuration. You may want verify the *Account is sensitive and cannot be delegated* box is NOT checked in the Active Directory account properties. If checked, the account will be inoperable.

The users should log out and back in to their client machine after changing any properties and before running Kerberos Delegation tests. This will clear cached Kerberos tickets. You may also use the **Kerbtray** utility to clear Kerberos tickets without logging out and back in.

D. Adding DNS Host

A computer that is joined to an Active Directory Domain gets an A-record created automatically. This should be verified. To use a host header for the Pyramid-URL-Site, administrators typically create a DNS host entry. Clients will use the friendly host header name - Pyramid-URL-site - instead of the computer name as the Pyramid URL to make it easier to access. If the site is deployed on the Extranet, the DNS entries are made in the public DNS records. Otherwise, if it's an intranet deployment, the records are made in the local DNS server. If it is multi-domain Active Directory, the DNS entries should be added into the global DNS for the forest.

SPNs

Adding a DNS Host will require new SPNs to be added to correspond to the friendly URL name – if the DNS is being setup internally on the local DNS server and Active Directory. (This usually coincides with the deployment of a Windows Authentication based system).

In a command prompt (with appropriate domain administrative rights) execute the following:

```
Setspn.exe -s HTTP/Pyramid-URL-site <host account>
```

If the URL is an internal URL entered into an internal DNS Server (Active Directory), then add the follow SPN as well:

```
Setspn.exe -s HTTP/Pyramid-URL-site.fully-qualified-name <host account>
```

Ensure there are no duplicate SPN entries:

```
Setspn.exe -x or -q <SPN>
```

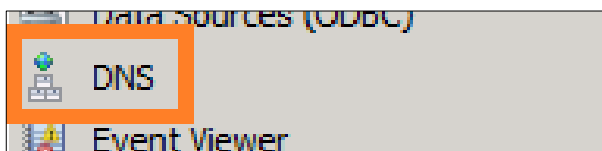
IIS

If using an internal DNS hosted site, make sure that both the short name for the site (*http://mysite*) and the fully qualified domain name for the site (*http://mysite.mycompany.com*) are added to the bindings for that site in IIS.

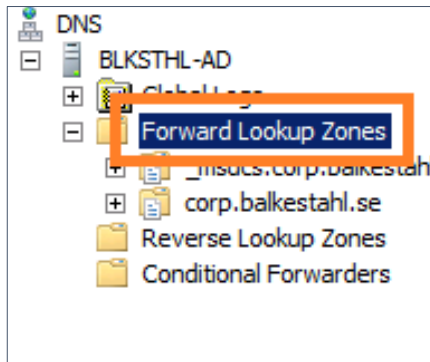
DNS Setup

To create an A-Record in DNS use the following steps.

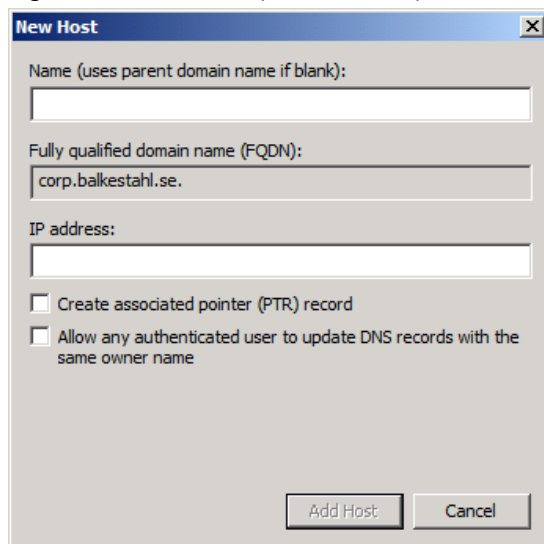
- Open DNS Management in Administrative Tools on a DNS server.



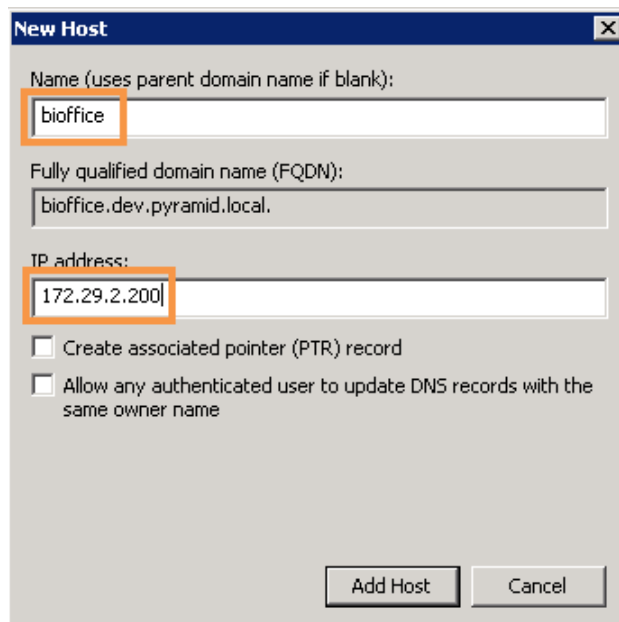
- Expand forward lookup zones container.



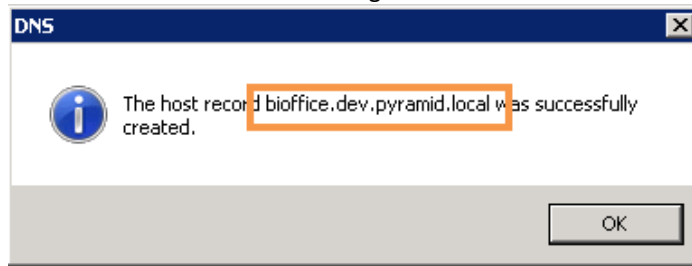
- Right click on the zone (domain name) and click on new host (A or AAAA).



- Type in the name of the record, this is the URL of Pyramid (minus the domain part in a FQDN) and type in the IP address of the BI OFFICE Web Server.



- Click on **Add Host**.
- Click on **Done**.
- You will see this verification dialog.



- Verify that the record has been created.

Host Name	Host Type	IP Address
biooffice	Host (A)	172.29.2.200

Global Names Zone Setup

In case of a Multi-Domain environment, add C-Name (alias) pointing to the A-Record, from previous section, in the Global Names Zone. In this way the BI Office URL friendly name will be supported from other Domains in your network with Kerberos enabled.

Additional reference see: <http://technet.microsoft.com/en-us/library/cc731744.aspx>

E. Web-Farm Deployment

If you deploy your application in a Web farm, you must ensure that the configuration files on each server share the same value for **validationKey** and **decryptionKey**, which are used for hashing and decryption respectively. This is required because you cannot guarantee which server will handle successive requests.

Manual Setup

With manually generated key values, the **<machineKey>** settings should be similar to the following example.

```
<configuration>
<system.web>
<machineKey
validationKey="21F090935F6E49C2C797F69BBAAD8402ABD2EE0B667A8B44EA7DD4374267A75D7
AD972A119482D15A4127461DB1DC347C1A63AE5F1CCFAACFF1B72A7F0A281B"
decryptionKey="ABAA84D7EC4BB56D75D217CECFB9628809BDB8BF91CFCD64568A145BE59719F"
validation="SHA1"
decryption="AES"
/>
</system.web>
</configuration>
```

Generating a new machine key can be done on one of the following links:

<http://aspnetresources.com/tools/machinekey>

<http://www.eggheadcafe.com/articles/GenerateMachineKey/GenerateMachineKey.aspx>

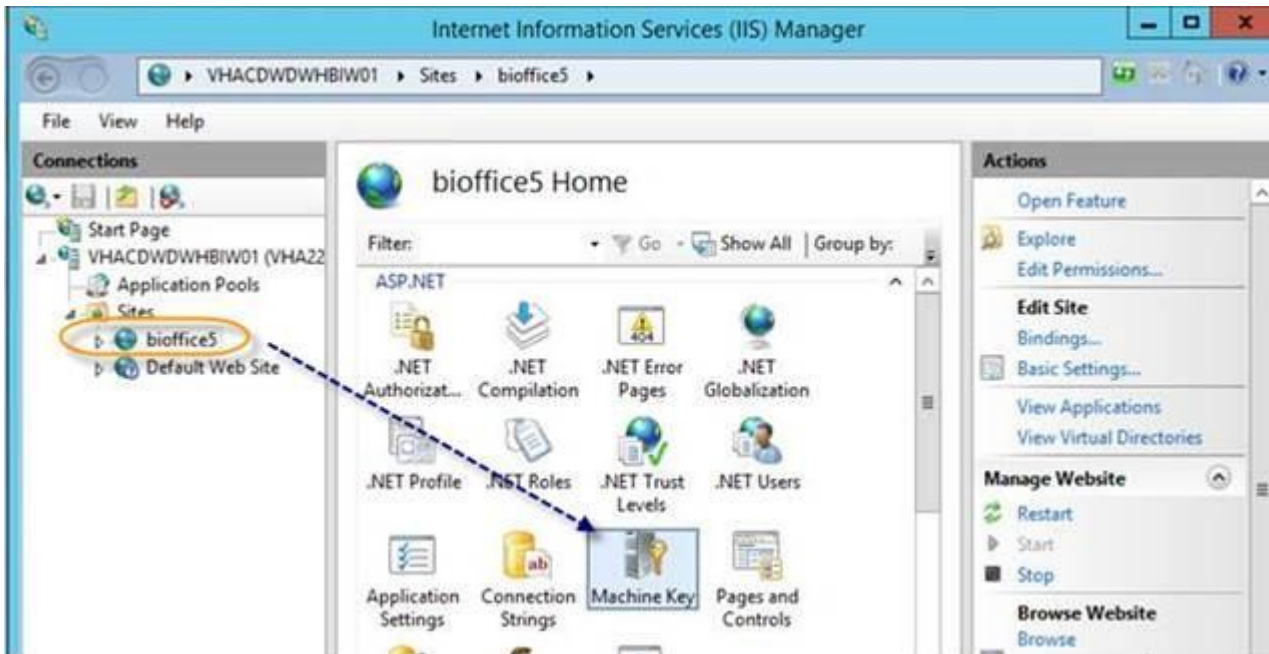
Add the settings to the **web.config** file found usually under:

C:\Program Files\Pyramid Analytics\BI Office 5\websites\paBio\web.config

Use the settings in all the other front-end web server in the web farm.

UI Setup

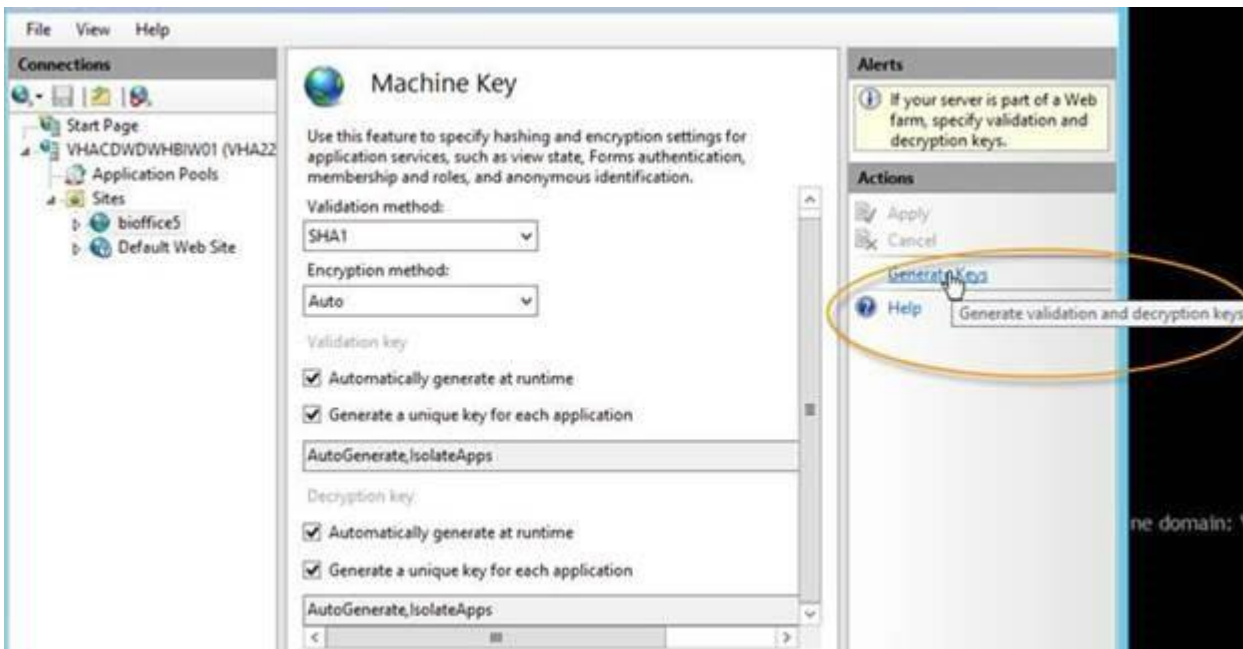
In the IIS Management console click on BI Office site and open the Machine Key screen in the ASP.NET section.



In the Machine Key screen, click on **Generate Keys** and then **Apply**.

Copy/paste the generated validation and decryption keys to the other front-end web server in the web farm.

Uncheck options “Automatically generate at runtime” and “Generate a unique key for each application”.



F. Effective Tokens

BI Office includes an option for “effective tokens” – which will allow authentication to BI Office for specific users without Kerberos. This does not imply that the application is running in a less secure mode. But it does allow for the application to operate in environments where Kerberos tokens fail; are intermittently available; and, complex domain models where Kerberos is not possible. To achieve this, BI Office uses a feature called “Effective User Name” – functionality from Microsoft that allows the query to run as the designated user. The mechanism will kick in whenever a valid Kerberos token cannot be found for the given session.

To turn it on, go to the BI Office admin console and the setting can be found under [Settings > Networking > Token Authentication](#).

For this feature to operate, the following prerequisites are required:

1. The installation must use an Active Directory.
2. The user account set in the “data source user” setting, must have administrative rights on the target Analysis Services.
3. SSAS services must be running under a network user or domain user (Local services/users will not work).

If your implementation does not meet either of these standards, do not enable this new feature or your installation may not connect to Analysis Services successfully.

EffectiveUserName is a SQL Server Analysis Services connection string property that contains the name of the user who is accessing a report or dashboard. In SharePoint, for example, you can use this property to pass the identity of the user who is viewing the report or dashboard to SQL Server Analysis Services. This allows user identification without the need to configure Kerberos delegation.

G. Testing the Configuration

Once you have completed these steps, ensure your SSAS security is set correctly and test the delegation by attempting to access a data view in BI Office application. Do not test from the Web server, application server or data server as this would only be a single-hop test.

If you see an error in the client, please continue to the following troubleshooting section.

III. Delegation with System Account

IV. SPNs

By default, when BI Office is deployed, a service principal name (SPN) is generated for the local services account by default, in the form of:

```
HOST/<NetBIOS-name>
```

```
HOST/<FQDN-name>
```

Changes to the SPNs of BI Office are required when using constrained delegation with Domain Account.

Setting SPNs Manually

In the event the SPNs are not installed correctly, they need to be set manually by a domain administrator.

1. Specify the SPNs in the Active Directory, Use “`SetSpn.exe -s`” to add the following:

```
HOST/NetBIOS-name <machine name>$  
HOST/NetBIOS-name.fully-qualified-name <machine name>$  
HOST/NetBIOS-name <machine name>$  
HOST/NetBIOS-name.fully-qualified-name <machine name>$  
HOST/NetBIOS-name <machine name>$  
HOST/NetBIOS-name.fully-qualified-name <machine name>$  
HTTP/Pyramid-Site-URL <machine name>$
```

If the URL is an internal URL entered into an internal DNS Server (Active Directory), then add the following SPN as well:

```
HTTP/Pyramid-Site-URL.fully-qualified-name <machine name>$
```

2. Verify SPNs by running: “`SetSpn -l`” for each machine.
3. Verify no duplications by running “`SetSpn -x`” or “`SetSpn -q <SPN>`”.
 - Duplicate SPN definitions break the Kerberos authentication process.

V. Full Delegation

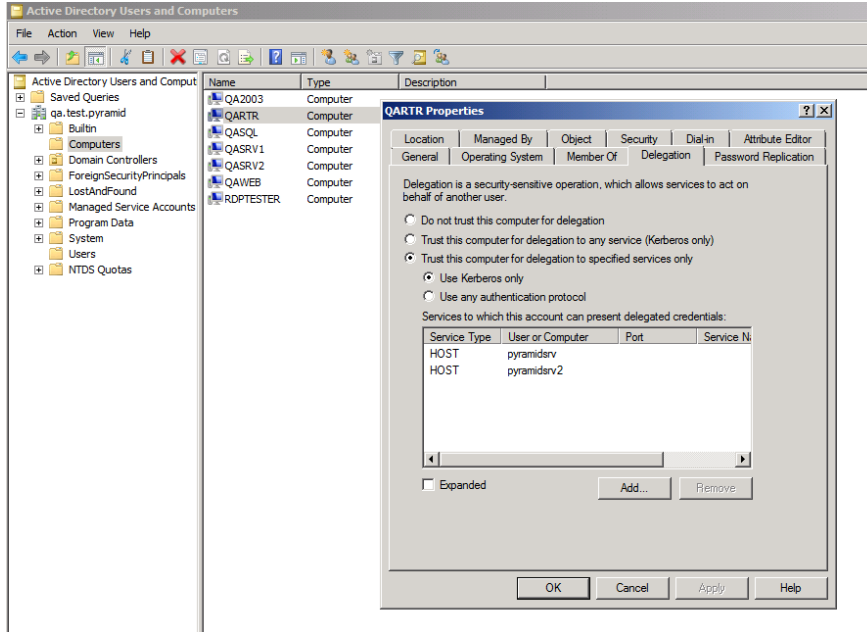
Repeat the following process for each computer running the BI Office Service: Application Server, Publisher Server, Router Server and IIS Web Server.

1. From **Active Directory Users and Computers**, right-click on the <Computer>, and choose **Properties**.
2. Go to the **Delegation** tab.
3. Select the second option **Trust this computer for delegation to any service (Kerberos only)**.

VI. Enforcing Constrained Delegation

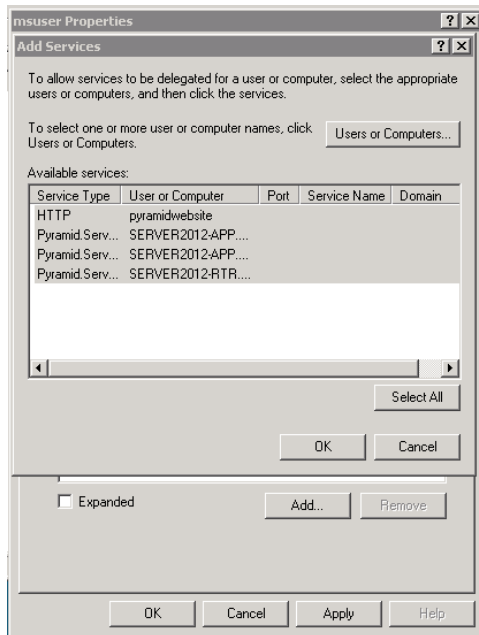
Repeat the following process for each computer running the BI Office Service: Application Server, Publisher Server, Router Server and IIS Web Server.

1. From **Active Directory Users and Computers**, right-click on the <Computer>, and choose **Properties**.
2. Go to the **Delegation** tab.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**.



Active Directory Kerberos delegation configuration

4. Click **Use any authentication protocol**.
5. Click **Add**, and then click **Users and Computers**.
6. Type the name of a computer running a BI Office Service.
7. Click **Select All** and click **OK**.



8. Click **Add**, and then click **Users and Computers**.

VII. Analysis Services SPNs for the Application and Publishing Servers

1. Type the name of the <Username> or <Machine> running MSOLAP, and then click **OK**.
2. Select the SPNs for SSAS shown in this document under “Adding SPNs for SSAS” and click **OK**.

For SSAS SPN registration see <http://msdn.microsoft.com/en-us/library/dn194200.aspx> and for Names Instances see <http://support.microsoft.com/kb/950599>.

Example of SPNs for SSAS with the default instance name:

```
MSOLAPSvc.3/serverHostName.Fully_Qualified_domainName SSAS_Service_Startup_Account  
MSOLAPSvc.3/serverHostName SSAS_Service_Startup_Account
```

Example of SPNs for SSAS with instance name:

```
MSOLAPSvc.3/serverHostName.Fully_Qualified_domainName:instanceName SSAS_Service_Startup_Account  
MSOLAPSvc.3/serverHostName:instanceName SSAS_Service_Startup_Account
```

For Named Instances:

```
MSOLAPDisco.3/serverHostName.Fully_Qualified_domainName Browser_Service_Startup_Account  
MSOLAPDisco.3/serverHostName Browser_Service_Startup_Account
```

Restart all the machines in the deployment and restart the client machine.

IV. Delegation with Domain Account

VIII. SPNs

By default, when BI Office Services are running under LocalSystem, a service principal name (SPN) is generated by default in the form of:

```
HOST/<NetBIOS-name>  
HOST/<FQDN-name>
```

When using constrained delegation with *Domain Account* it is required to change the SPNs of BI Office (see below).

Registering New SPNs

1. Remove the HTTP/Pyramid-Site-URL SPNs from the IIS Server Machine:

```
Setspn.exe -d HTTP/Pyramid-Site-URL Domain\NetBIOS-name$
```

If the URL is an internal URL entered into an internal DNS Server (Active Directory), then remove the following SPN as well:

```
Setspn.exe -d HTTP/Pyramid-Site-URL.fully-qualified-name Domain\NetBIOS-name$
```

2. Specify the SPNs in the Active Directory, Use “SetSpn.exe -s” to add the following:

```
Pyramid.Server.Application/NetBIOS-name <Domain\App Server Username>  
Pyramid.Server.Application/ fully-qualified-name <Domain\App Server Username>  
Pyramid.Server.Publisher/NetBIOS-name <Domain\Pub Server Username>  
Pyramid.Server.Publisher/ fully-qualified-name <Domain\Pub Server Username>  
Pyramid.Server.Router/NetBIOS-name <Domain\Rtr Server Username>  
Pyramid.Server.Router/ fully-qualified-name <Domain\Rtr Server Username>  
HTTP/Pyramid-Site-URL <Domain\app pool Username>
```

If the URL is an internal URL entered into an internal DNS Server (Active Directory), then add the following SPN as well:

```
HTTP/Pyramid-Site-URL.fully-qualified-name <Domain\app pool Username>
```

3. Verify SPNs by running: “SetSpn -l Domain\Username” for each user.
4. Verify no duplications by running “SetSpn -x” or “SetSpn -q <SPN>”
 - Duplicate SPN definitions break the Kerberos authentication process.

IX. Database Update

Manual changes need to be made in the Pyramid SQL Database table `[servers_tbl].[WcfInstances]` where you will find a column named `[SPN]`.

Update values for SPNs according to the following table:

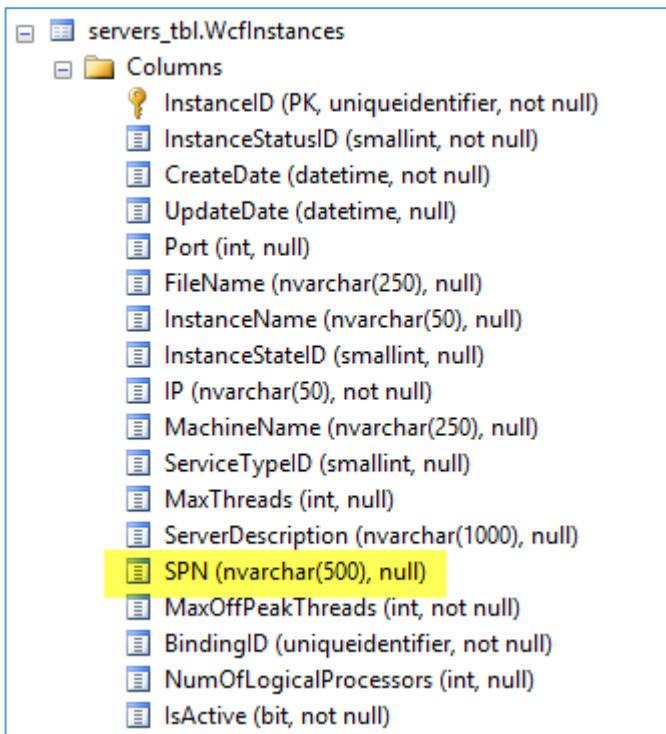
Service	Service Type ID	SPN
BI Office Application Server	1	Pyramid.Server.Application/NetBIOS-name
BI Office Publisher Server	5	Pyramid.Server.Publisher/NetBIOS-name
BI Office Router Server	2	Pyramid.Server.Router/NetBIOS-name

Each NetBIOS-name will be the NetBIOS machine name running the specific Service.

NOTE 1: Client Routers (Web sites) with `[ServiceTypeID]` 3 or 4, cannot have an SPN value and should be left as `NULL`.

NOTE 2: When there are authentication and communication errors in the BI Office system logs (and slowness occurs when showing the data sources when choosing to create a report in Data Discovery), you can define the SPN with a FQDN as part of your troubleshooting efforts.

In some cases the FQDN can be a very long one, and therefore it's necessary to edit the column type of the SPN to be `nvarchar(500)` or greater, as shown below. For all BI Office versions following 6.32, the `nvarchar(500)` setting will be present by default.



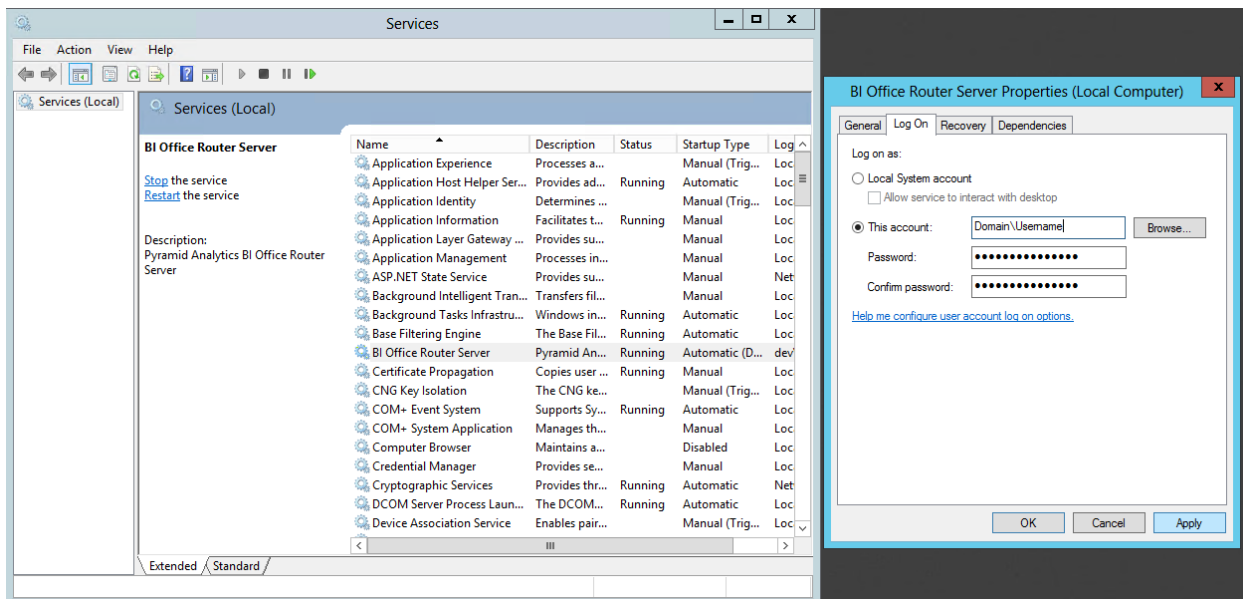
X. Changes for the Domain Account

Configuring the domain account(s)

1. In Active Directory under **Users and Computers**, go to the **Account Options** list on the **Account tab** of the domain account and verify that the **Account is sensitive and cannot be delegated** option is not selected.
2. For each machine in the deployment add the custom account to the local administrators group, and open **Local Security Policy** in the Administrative Tools program group. Expand Local Policies, and click User Rights Assignment. Add the custom service account to the following policies:
 - a. Log on as a service.
 - b. Impersonate a client after authentication.
 - c. Enable computer and user accounts to be trusted for delegation.
 - d. Act as part of the operating system.

Changing all BI Office services deployed to run under the specific domain account(s)

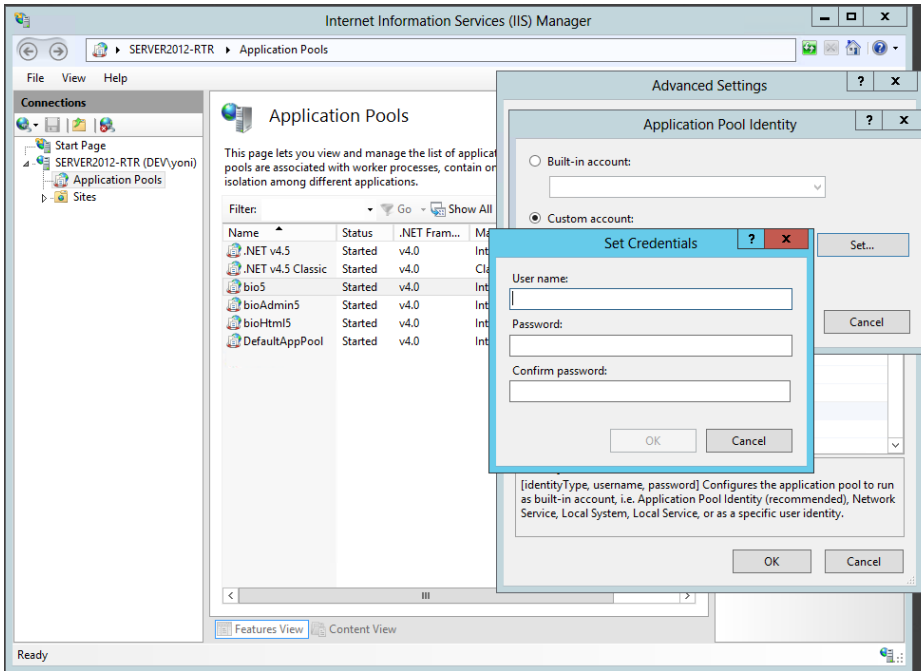
1. BI Office Application Server
2. BI Office Publication Server
3. BI Office Router Server



Changing to custom account

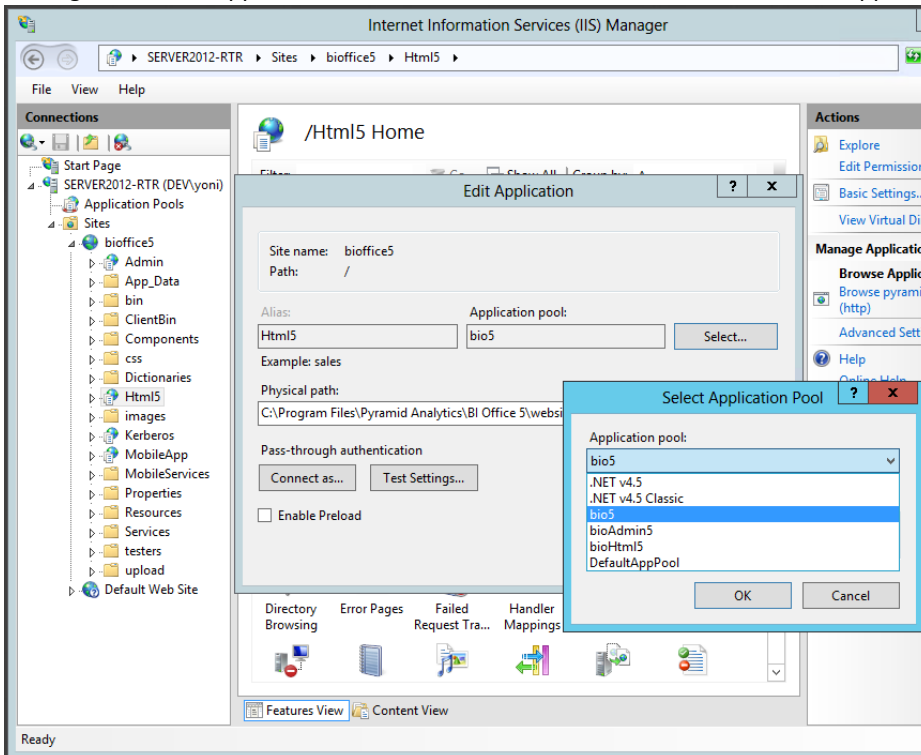
Changing IIS to custom domain account(s)

- a. Change the IIS Application Pool Identities of **bio6** and of **bioAdmin6** to the custom account.



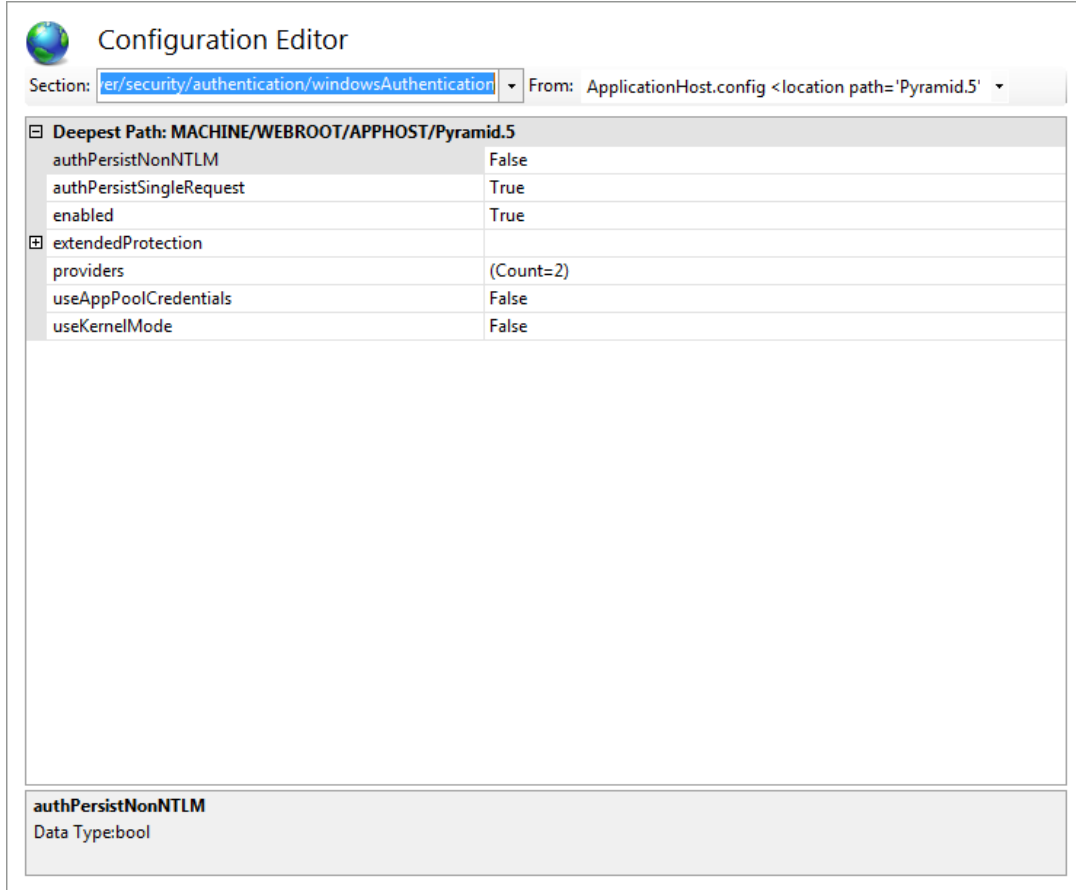
Changing application pool identity

- b. Change the Html5 application under BI Office web site, to run with the same application pool as the core website: **“bio5”**.



Changing Html5 application pool

- c. Changing the “useKernelMode” to false:
 - i. Select the BI Office web site.
 - ii. Under Management, select ‘Configuration Editor’.
 - iii. In the ‘From:’ section above the properties, select ‘ApplicationHost.config <location path=...’
 - iv. For the ‘Section:’ location, select system.webServer > security > authentication > windowsAuthentication.
 - v. In the properties page, set useKernelMode to False, then click Apply.



The screenshot shows the Configuration Editor interface. At the top, there is a globe icon and the title "Configuration Editor". Below the title, there are two dropdown menus: "Section:" with the value "er/security/authentication/windowsAuthentication" and "From:" with the value "ApplicationHost.config <location path='Pyramid.5'".

The main content area is a table with the following properties:

Deepest Path: MACHINE/WEBROOT/APPHOST/Pyramid.5	
authPersistNonNTLM	False
authPersistSingleRequest	True
enabled	True
extendedProtection	
providers	(Count=2)
useAppPoolCredentials	False
useKernelMode	False

At the bottom of the interface, there is a summary box for the selected property:

authPersistNonNTLM
Data Type:bool

Changing useKernelMode value to False

XI. Full Delegation

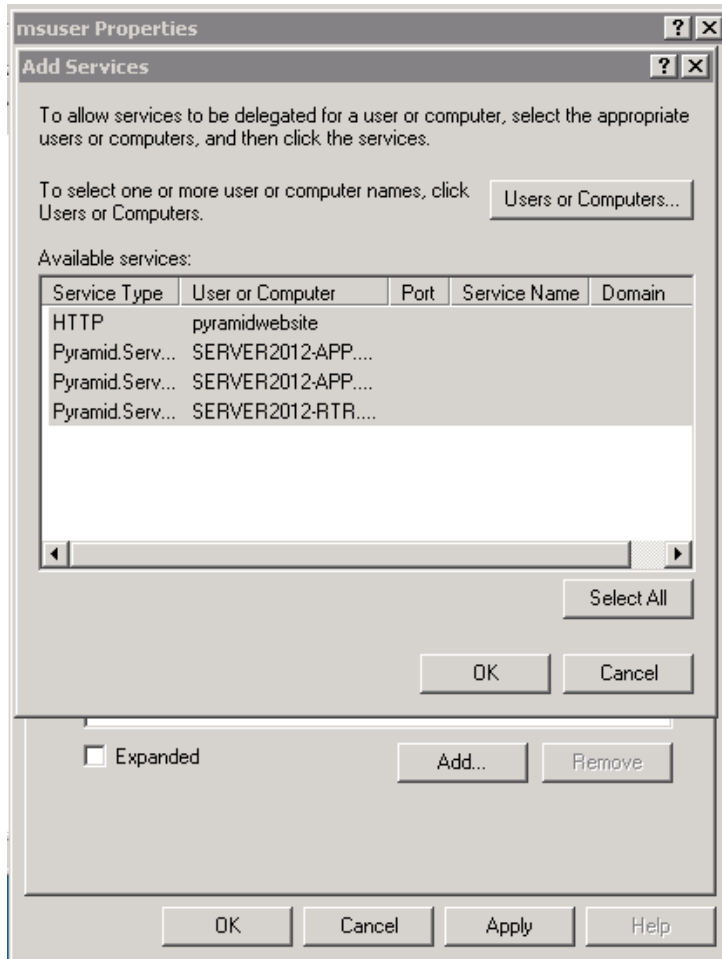
Repeat the process for each user running the BI Office Service: Application Server, Publisher Server, Router Server and IIS Web Server.

1. From **Active Directory Users and Computers**, right-click on the <Username>, and choose **Properties**.
2. Go to the **Delegation** tab.
3. Select the second option **Trust this user for delegation to any service (Kerberos only)**.

XII. Enforcing Constrained Delegation

Repeat the process for each user running the BI Office Service: Application Server, Publisher Server, Router Server and IIS Web Server.

1. From **Active Directory Users and Computers**, right-click on the <Username>, and choose **Properties**.
2. Go to the **Delegation** tab.
3. On the **Delegation** tab, click **Trust this user for delegation to specified services only**.
4. Click **Use any authentication protocol**.
5. Click **Add**, and then click **Users and Computers**.
6. Type the name of a user running a BI Office Service.
7. Click **Select All** and click **OK**.



8. Click **Add**, and then click **Users and Computers**.

XIII. Analysis Services SPNs for the Application and Publishing Servers

1. Type the name of the <Username> or <Machine> running MSOLAP, and then click **OK**.
2. Select the SPNs for SSAS shown in this document under “Adding SPNs for SSAS” and click **OK** (For SSAS SPN registration see <http://msdn.microsoft.com/en-us/library/dn194200.aspx> and for Names Instances see <http://support.microsoft.com/kb/950599>)

Example of SPNs for SSAS with the default instance name:

```
MSOLAPSvc.3/serverHostName.Fully_Qualified_domainName SSAS_Service_Startup_Account  
MSOLAPSvc.3/serverHostName SSAS_Service_Startup_Account
```

Example of SPNs for SSAS with instance name:

```
MSOLAPSvc.3/serverHostName.Fully_Qualified_domainName:instanceName SSAS_Service_Startup_Account  
MSOLAPSvc.3/serverHostName:instanceName SSAS_Service_Startup_Account
```

For Named Instances:

```
MSOLAPDisco.3/serverHostName.Fully_Qualified_domainName Browser_Service_Startup_Account  
MSOLAPDisco.3/serverHostName Browser_Service_Startup_Account
```

Restart all the machines in the deployment and restart the client machine.

V. Appendix

A. Other Documentation & Tools

- For more information see <http://blogs.technet.com/b/askds/archive/2008/03/06/kerberos-for-the-busy-admin.aspx>
- Review the section “Infrastructure Requirements” in Microsoft’s [Troubleshooting Kerberos Delegation](#)
- Review the following Microsoft document - [How to configure SQL Server 2005 Analysis Services to use Kerberos authentication](#).
- There are two common tools for editing SPN entries in Active Directory: [AdsEdit.msc](#) and [setSPN.exe](#).
- Installed with the BI Office application is the Kerberos Tester. It can be found under:
 - The URL “<http://pyramidBIO.mysite.com/admin/diagnostics.aspx>”, where pyramidBIO.mysite.com is the host URL name you provided during installation.

B. SQL Server Analysis Services SPN Configuration

SSAS should already have its SPNs preset as part of its own installation. This section allows administrators to ensure it is correct in the event of impersonation and connection issues.

Before starting, ensure that the end user(s) is a part of the SSAS role for viewing cube data.

XIV. Using a Local Computer Account for SSAS Service

Check the SQL Server Analysis Services (MSSQLSERVER) service to find out what account is being used to start the service.

If your SSAS service is running under a local computer account, such as *LocalSystem*, it is likely this account will already have SPN entries.

```
MSOLAPSvc.3/MachineName MachineName
MSOLAPSvc.3/MachineName.Company.com MachineName
```

XV. Adding SPNs for SSAS

If you do not see the correct SPNs, you can add them. If the SSAS service is using *LocalSystem* and not a domain user account, you must set the computer account for the data server in Active Directory to be trusted for delegation.

```
setspn -s MSOLAPSvc.3/MachineName MachineName
setspn -s MSOLAPSvc.3/MachineName.Company.com MachineName
```

If the SSAS service is running under domain accounts, register these SPNs.

```
setspn -s MSOLAPSvc.3/MachineName domainAccount
setspn -s MSOLAPSvc.3/MachineName.Company.com domainAccount
```

If you are using a **named instance** for SQL Server SSAS, the following SPN formats apply with domain account or machine name as required.

```
setspn -s MSOLAPSvc.3/MachineName:instanceName domainAccount
setspn -s MSOLAPSvc.3/MachineName.Fully_Qualified_domainName:instanceName domainAccount
```

You may have to wait or force replication of the information to other domain controllers in the network.

For Named Instances

```
MSOLAPDisco.3/MachineName Browser_Service_Startup_Account
MSOLAPDisco.3/MachineName.Fully_Qualified_domainName Browser_Service_Startup_Account
```

Where [Browser_Service_Startup_Account](#) is the domain account or machine running SQL Browser Service.

For more details on Names Instances see <http://support.microsoft.com/kb/950599>

All domain account or machines stated above must be trusted for delegation for Kerberos to be enabled.

C. Client Browser Settings

All major client browsers are compatible with the application's framework Silverlight. However, only Internet Explorer and Firefox support Integrated Windows Authentication. All previously mentioned browsers support Basic Authentication with or without SSL certificates.

Enabling Integrated Windows Authentication in Internet Explorer

From the client machine (browser) make sure the following settings are configured:

- BI Office's Web site has been added to the list of TRUSTED SITES in the browser (or INTRANET sites for internal site addresses).
- Update automatic logon through Internet Explorer > Internet Options > *Security* > *Trusted sites* > *Custom level* > *Automatic Logon* with current username and password.
- Make sure Internet Explorer is set to use *Integrated Authentication* in advanced Internet Options.
- These configurations can also be enacted through GPO's on the Active Directory.
- Have the end user log off and log on or use kerbray.exe to clear cached security tickets.

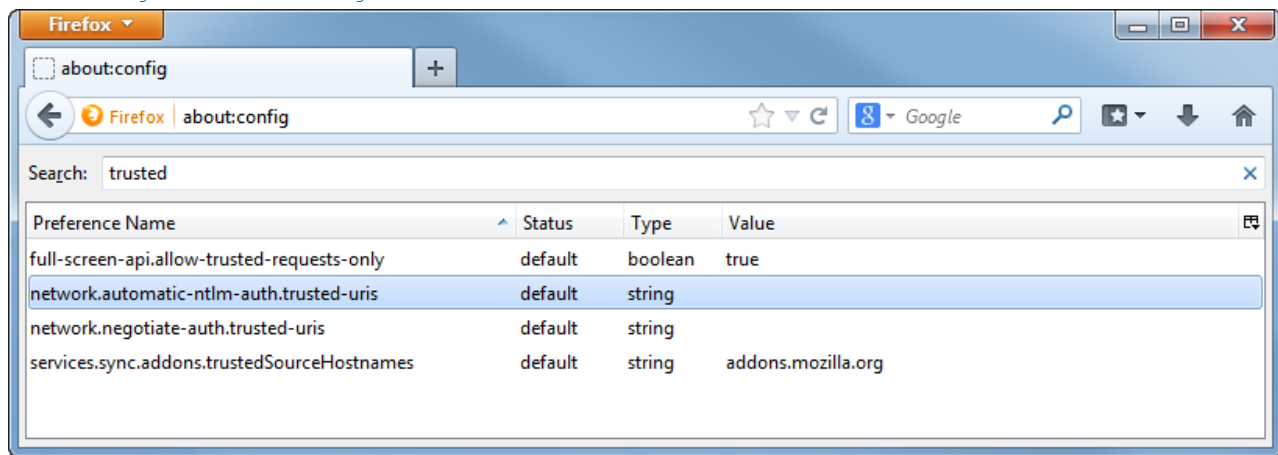
Enabling Integrated Windows Authentication in Firefox

Launch Firefox and go to *about:config* (shown below). Add the URL of the Web site to the following preferences:

`network.automatic-ntlm-auth.trusted-uris`

`network.negotiate-auth.trusted-uris`

`network.negotiate-auth.delegation-uris`



Firefox Integrated Windows Authentication

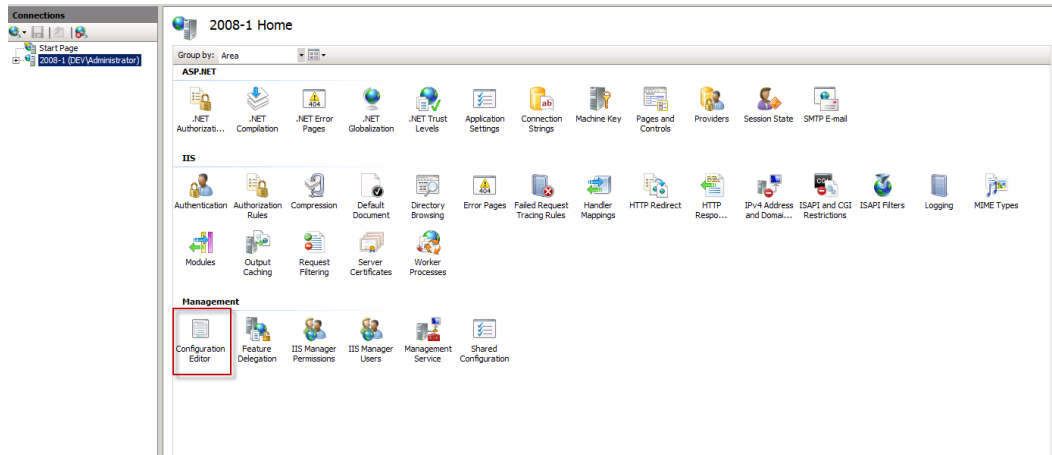
Enabling Integrated Windows Authentication in Chrome

Google Chrome in Windows will use the Internet Explorer settings, so configure within Internet Explorer's Tools, Internet Options dialog, or by going to Control Panel and selecting Internet Options within sub-category Network and Internet.

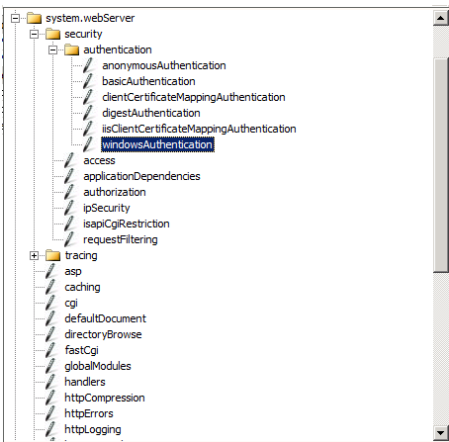
D. IIS Configure Windows Authentication

The following steps can be set directly in the IIS 7.x/8.x console found in the administrative tools on the server. You will need to install the administrative tools for IIS7.x (which can be downloaded from the Web or found under the tools menu on the Pyramid install CD).

Open the IIS 7.x console and select the Web site from the tree on the left. Click on **Configuration Editor**.

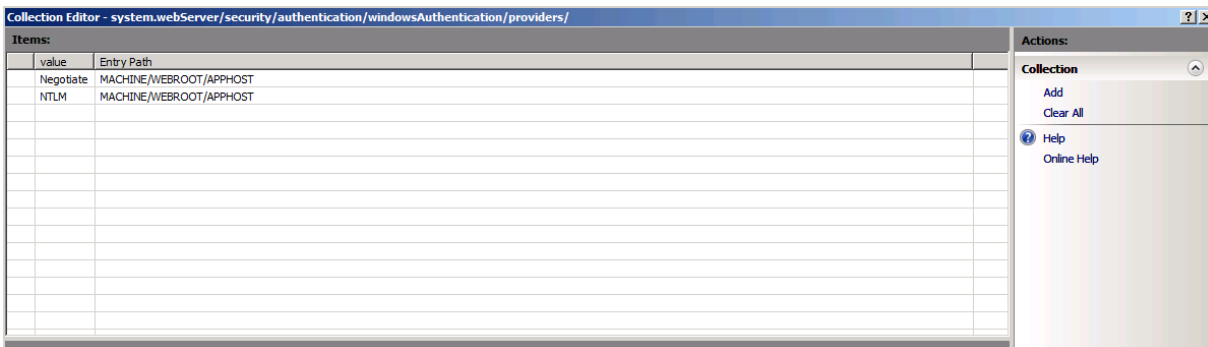


In the panel, click on windows authentication. In the panel, click on providers and then click on the ellipsis at the far right of the screen.

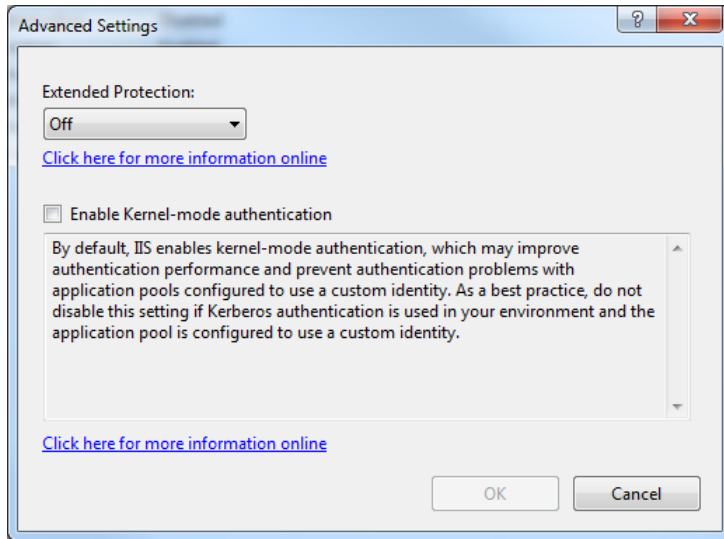


Deepest Path: MACHINE/WEBROOT/APPHOST	
authPersistNonNTLM	False
authPersistSingleRequest	False
enabled	False
providers	(Count=2)
useAppPoolCredentials	False
useKernelMode	True

Providers: Make sure there are two providers listed - Negotiate and NTLM.

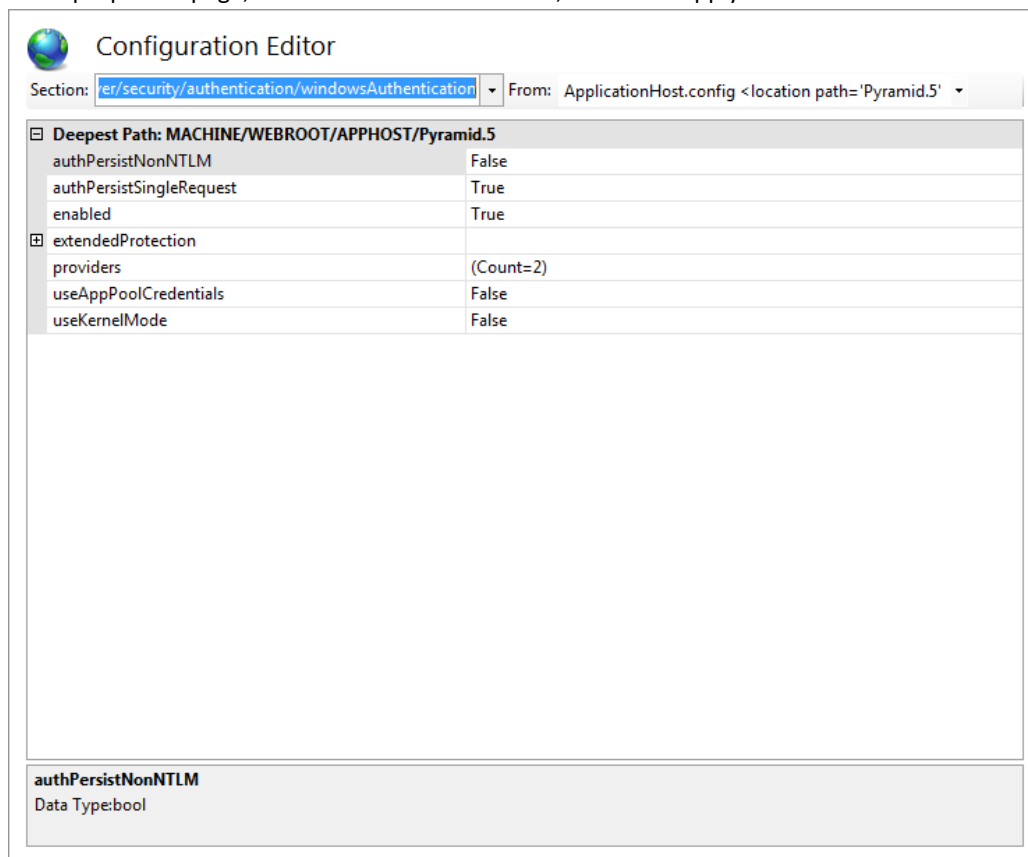


Advanced settings: In the authentication panel, make sure Extended protection is set to "off" in the drop down and make sure the Enable kernel-mode authentication is unchecked.



Changing the "useKernelMode" to false:

- a. Select the BI Office web site.
- b. Under Management, select 'Configuration Editor'.
- c. In the 'From:' section above the properties, select 'ApplicationHost.config <location path=...'
- d. For the 'Section:' location, select system.webServer > security > authentication > windowsAuthentication.
- e. In the properties page, set useKernelMode to False, then click Apply.



Changing useKernelMode value to False

E. Access Token Limitation Problem with Kerberos

Active Directory Token Bloat is an issue in AD where user are is a member of too many security groups.

As such their account exceeds the default 12k token size limit in Windows that is set on their internal AD Security Token.

This is a common problem for many large organization that have many security groups and in most situation this problem is fixed by configuring a larger “MaxTokenSize” registry key on all the computers.

1. Configure on all pyramid servers including the datasource servers’ deployed machines and client machines to accept larger headers.

To increase the header size you need to configure the following registry keys:

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters**

MaxFieldLength

Default Value: 16384

Set value to: 65534 (64kb) bytes

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters**

MaxRequestBytes

Default value: 16384

Set value to: 16777216 (16MB) bytes

2. Configure on all pyramid servers including the datasource servers’ deployed machines and client machines to accept larger token size.

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters**

MaxTokenSize

Default Value: 12000

Set value to: 65535 (64kb) bytes

All values specified are decimal values.

Additional References

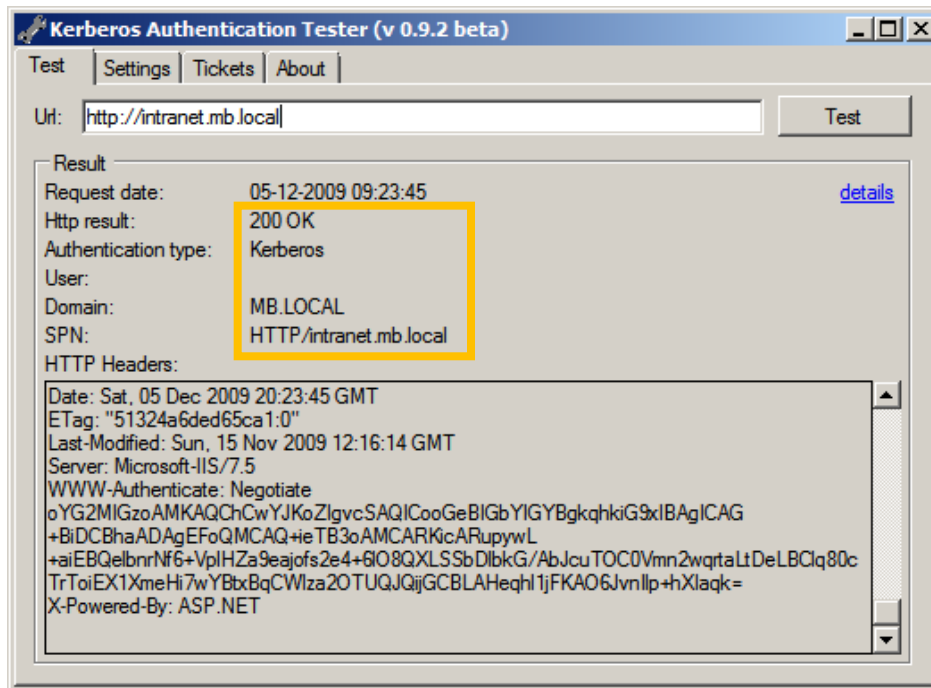
To configure these registry keys with Group Policy see: <http://www.grouppolicy.biz/2013/06/how-to-configure-iis-to-support-large-ad-token-with-group-policy/>

Kerberos Authentication Problem with Active Directory: <http://blogs.technet.com/b/surama/archive/2009/04/06/kerberos-authentication-problem-with-active-directory.aspx>

F. Verifying the Flow of Kerberos Tickets

Use **Kerberos Authentication Tester** tool to verify Kerberos authentication. No installation is required. It shows what authentication method is used in a web request: None, Basic, NTLM or Kerberos.

The tool can be downloaded from here: <http://mbar.nl/michel/archive/2009/12/05/kerberos-authentication-tester.aspx>



Kerberos results when it works

G. General Troubleshooting

Kerberos Issues

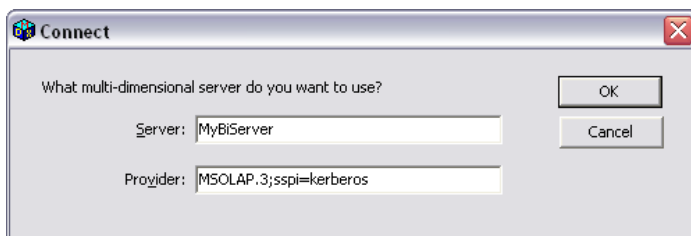
It is important to first check that the Kerberos delegation failure is indeed the cause of the error you are receiving in the client. Many of the other possible causes of this error can be eliminated from consideration using the following steps:

- Restart all machines involved in the Kerberos Delegation setup. This will force services to be restarted, which is required after SPN changes, and Kerberos ticket caches to be cleared.
- Try to access the client by using a browser on the Web server itself. This will eliminate one of the credential hops and you should be able to log in. If you cannot see data, Kerberos delegation may not be the issue.
- Check the *Event Viewer Security* logs on the Web and data servers. The logs will report successes and failures and can identify if Kerberos or NTLM is being used. The audit logs in the BI Office database will highlight what type of authentication the user was using when trying to log into the application.
- Check that cube security is set correctly and that the test user is a member of a role that has access to the cube. It is recommended that you temporarily grant your test user membership to the server administrator role to help eliminate cube security as a cause of any connection problems.
- Check that the Web server can communicate with the data server and that firewall ports are open. It is recommended that you temporarily disable firewalls to help eliminate them as possible causes of any connection problems. If there are firewalls between the client, Web server and data server, be sure that they have the correct ports open.
- Ensure the token “bloat” is not an issue (see above).
- Make sure all BI Office components (Web, app, router servers) are installed and the SSAS needs to be trusted for delegation are in the Active Directory. Go to Active Directory > Users and Computers > Expand the domain > Computers > double-click on computer > Delegation > Mark **Trust this computer for delegation to any service** (Kerberos only) setting.

Troubleshooting Kerberos Authentication to SSAS Service

If the problem appears only when attempting to use Kerberos delegation:

- Review the setup steps above to be sure your SPN entries are correct and that the data server, Web server and client machines have been properly configured for delegation.
- Check your SPNs and test for duplicates using a tool called [DHCheck](#).
- Use the “Kerberos Delegation Tester” on the installed Web site, located:
 - URL “<http://pyramidBIO.mysite.com/admin/diagnostics.aspx>”, where pyramidBIO.mysite.com is the host URL name you provided during installation.
- Use the *MDX Sample Application* from Analysis Services 2000 on the Web server to test a Kerberos connection to Analysis Services. If the tool connects successfully when forced to use Kerberos, then you likely have configured SPN entries for the SSAS service correctly. To test a Kerberos connection, modify the *Provider* field when connecting to a server, as shown below:



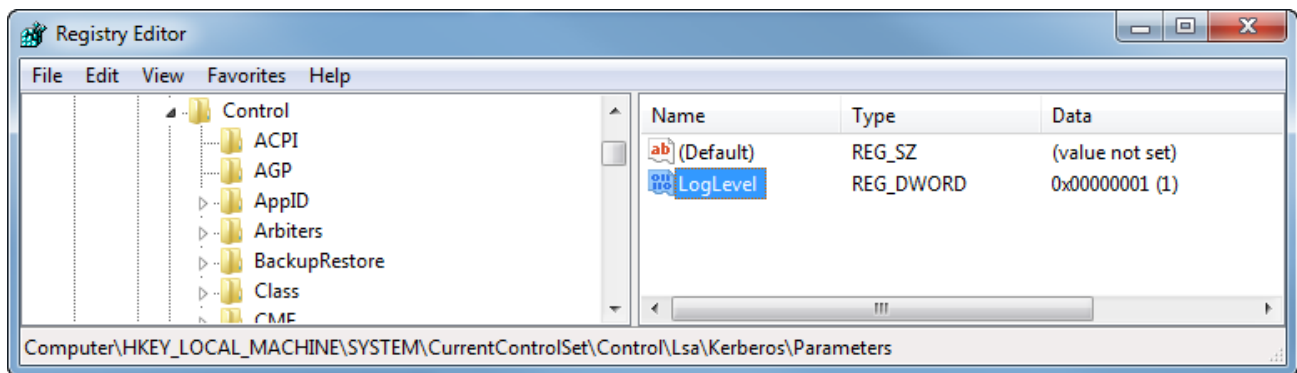
Testing Kerberos with the MDX Sample Application

- Review the section “Diagnosing Delegation Problems: Four Checklists” in Microsoft’s Troubleshooting Kerberos Errors: <http://www.microsoft.com/en-us/download/details.aspx?id=21820>

Troubleshooting Kerberos on the web server

You may also turn on *verbose logging* to capture security traffic on your Web server and data server.

<http://support.microsoft.com/kb/262177>



Log Level Setting in the Registry

If you are using *Constrained Delegation*, temporarily disable the constraint and retest.

- Are you using a split domain where machines can resolve two different FQDNs? For example, when you ping the same server from two different machines and it returns different FQDNs – such as `MyDataServer.Company.com` as well as `MyDataServer.AD.Company.com`. If so, this may defeat the SPNs needed for Kerberos delegation. Please see your network administrator to verify that the DNS names being requested by the browser to the Web server match the SPNs on the server. Also, check that the DNS names requested by the Web server to the data server match the SPNs registered on the data server.
- Troubleshoot with Network Monitor or Wireshark: [Two easy ways to pick Kerberos from NTLM in an HTTP capture.](#)
- *Analysis Services* should be installed, preferably from a fresh install that has not been imaged. It is also preferable that you use a machine that has not been renamed.

H. Windows Authentication Check List

The details behind each of the following steps can be found in the body of this document. The list below is merely a checklist summary to follow.

1. Ensure the application was installed with windows authentication.
2. Ensure that the ports on the server's firewall are not blocking ports required for windows authentication.
3. To ensure the Kerberos authentication does not fail:
 - a. For servers with internal DNS hosting on the Active Directory – ensure that both the website name and the fully qualified domain name of the website are registered as SPNs.
 - b. Ensure there are no duplicate SPNs.
 - c. Ensure there are no duplicate DNS entries for the Host site and IP.
 - d. The delegation has been setup such that both sets of SPN's are registered for the account that will be delegating tokens.
 - e. To check if Kerberos tickets are being issued use the “**Kerberos Authentication Tester**” tool (described above) to check if there is a fall back to NTLM. Windows Authentication will not work under NTLM.
 - f. Check if there is a Kerberos token “bloat” problem.
4. Update the SPN column in the Pyramid Content Store database to match the SPN's used. The default ones suit a full delegation / Local Service Account model. If a domain account is used these need to be updated.
5. If using constrained delegation, remove and then re-add any SPN's that were modified.
6. If using a domain account, the account needs to be a local administrator on the host servers and have certain GPO rights (see above for more detail).
 - a. On the web server, change the “useKernelMode” to false. Also change the app pool used for the “HTML5” virtual application in the BI Office website to use the same one as the main application “bio5”.
7. If using an internal DNS named site, make sure that both the short name for the site and the fully qualified domain name for the site are added to the bindings for that site in IIS.
 - a. If it is multi-domain Active Directory, the DNS entries should be added into the global DNS for the forest.
8. On the client machine, ensure that the website address is trusted in the browser settings and that the authentication is set to automatically pass on the users credentials. Ensure “integrated windows authentication” is enabled.
9. Once all settings have been made, it is a good idea to reboot all hosting servers and any client PCs before attempting to connect.