Enabling single sign-on for Cognos 8/10 with Active Directory

Overview

QueryVision Note:

This document pulls together information from a number of QueryVision and IBM/Cognos material that are publically available on the internet. The main source is the following IBM Cognos document, with some corrections and related IBM/Cognos material incorporated to provide a fuller picture of the SSO options.

https://www-304.ibm.com/support/docview.wss?uid=swg21341889

It covers 3 scenarios for Active Directory/SSO

- [Cognos] Native Active Directory using Kerberos
- [Cognos] Native Active Directory using NTLM/Remote User
- [Cognos] LDAP access for Active Directory using NTLM/Remote User

Overview

Single Signon (SSO) from Windows Users to ReportNet or Cognos 8 configured to authenticate to an Active Directory facilitating an Active Directory Authentication Provider (AD AP) is achievable in two different ways. This document briefly describes both approaches and lists the exact prerequisites for successfully implementing them.

The task however is challenging and is mainly focused on Microsoft Windows Security knowledge rather than Cognos. For more detailed information and detailed steps, refer to the documents listed in the Related Information section below

Symptom

No error message, but Single Signon fails. Users get prompted for authentication information, the username may be pre-set like DOMAIN\USER.

Cause

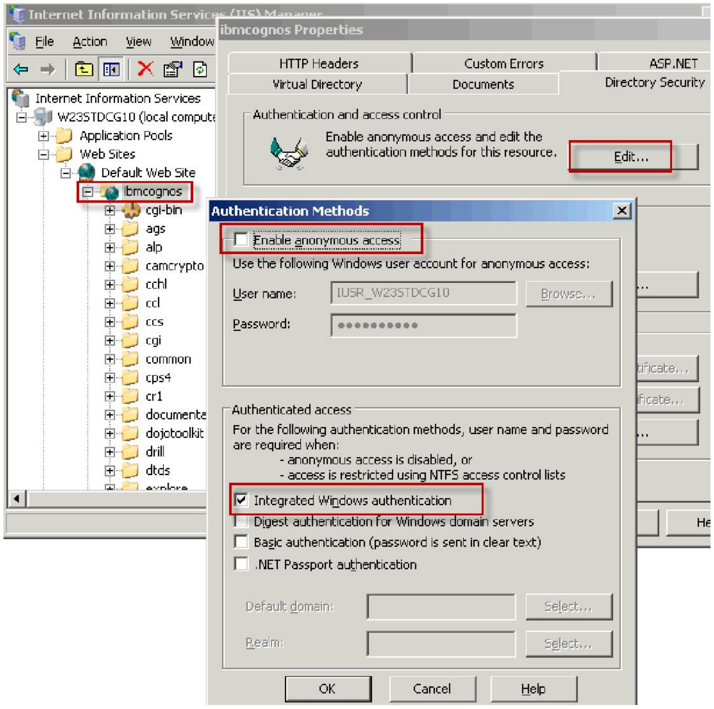
Depending on the scenario, one or more prerequisites are not met.

QueryVision Notes:

The single most important issues are:

SSO in general

- Disable anonymous access in IIS for the Cognos Virtual Directories/URLs and enable Integrated Windows Authentication



Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_W23STDCG10

Password: ●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

Ensure these security settings propagate to cgi-bin, etc.

- Set the Gateway namespace to the Active Directory namespace.

Kerberos SSO

- Enable Kerberos Delegation for the IIS server and Cognos server service accounts (computer or domain user account used as service account)
- Remove the singleSignOnOption = IdentityMapping for the Active Directory Namespace
- Reboot all machines (see below)

NTLM SSO

- ensure **singleSignOnOption** = **IdentityMapping** are added exactly as shown (case sensitive)

It is highly recommended to re-boot the Cognos Server, IIS server and any workstation(s) used for browser testing for SSO – particularly after changes to Active Directory (e.g. change user account or service account “trust for delegation” properties).

These (type of) changes appear to take some time to propagate from the Active Directory Domain Controller to other computers (or VMs) in the domain. Rebooting ensures that the machines re-sync/re-login to Active Directory for up to date properties. The symptoms are that changes to either AD or Cognos Configuration for Kerberos related properties don’t act as expected.

Environment

ReportNet, Cognos 8 or Cognos 10 running on Windows (2003, 2008, 2008 R2)

Authentication Source: Active Directory

Web server: Microsoft IIS 5.x, 6.x, 7.X

Resolving the problem

Once a user connects their Internet Explorer browser to IIS, their Windows credentials will be passed to the web server by the browser. The web server will authenticate the user and is able to pass on the users credentials hence forth. Through a Gateway or Dispatcher component, authentication information eventually is passed down to the Cognos security layer which sits with the Content Manager component. There, an Active Directory authentication provider can be configured to handle authentication.

By default, Cognos' Active Directory Authentication Provider facilitates Microsoft's implementation of the Kerberos protocol to obtain authentication information and authenticate the user. By using Kerberos, the concept of delegated authentication in turn enables Cognos to pass on user credentials to other services again. This is leveraged when connecting to Microsoft SQL Server Analysis Services for example. In addition, using Kerberos is considered to be the most secure way of integrating with Windows security. Using Kerberos adds some prerequisites to the setup and inherits some restrictions from it as well.

If you do not or cannot use the Microsoft Kerberos protocol, the Active Directory provider can be configured to obtain authentication information from the HTTP CGI standard environment variable REMOTE_USER instead.

This still allows single signon to the Cognos environment to occur as the user name is passed down but prevents Cognos from impersonating the user in line with the delegated authentication. Cognos will not be able to pass on the users credentials to other services as only a username is obtained. This renders single signon to Microsoft SQL Server Analysis Services impossible as this would require username and password or Kerberos information. However, other signon methods based on the 'external' Active Directory Namespace are still possible.

For details about Configuring Data Sources for Microsoft Analysis Services, refer to the Administration and Security Guide, Chapter 5.

Scenario 1: [Cognos] Native Active Directory SSO using Kerberos

1. Establish a Realm in IIS

For the Cognos virtual directories configured as described in "Configure the Web Server" in Chapter 6 of the Installation and Configuration Guide, enable *Windows Integrated Authentication* and disable *Anonymous Access* on the IIS Web server.

Make sure the following prerequisites are met:

General

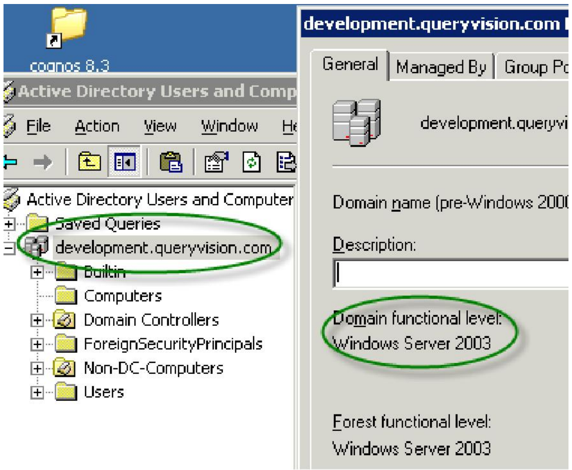
+ The Active Directory targeted for authentication must be running in native mode (at least native Windows 2003.

The modes are

Domain Functional Levels (domainFunctionality)	Forest Functional Levels(forestFunctionality)

0 - Windows 2000 mixed	0 — Windows 2000
0 - Windows 2000 native	0 — Windows 2000
1 - Windows Server 2003 interim	1 — Windows Server 2003 interim
2 - Windows Server 2003	2 — Windows Server 2003
3 - Windows Server 2008	3 - Windows Server 2008

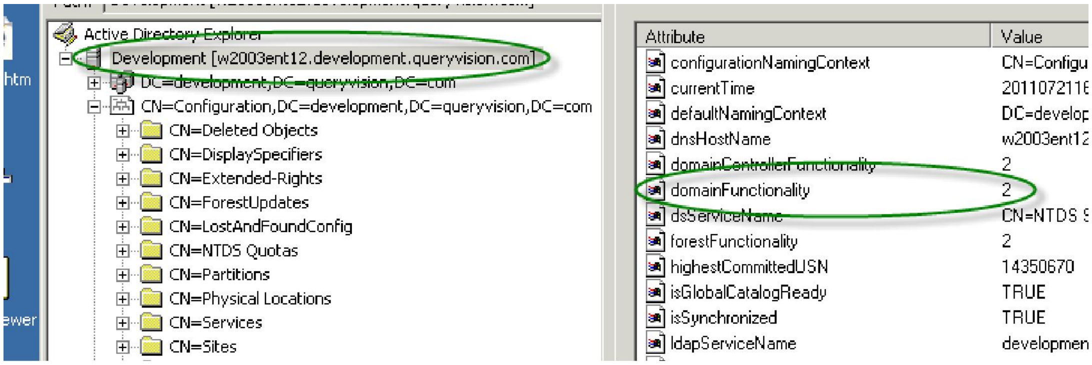
TIP: To verify, check the domain properties in the Microsoft Active Directory - Users and Computers console.


cognos 8.3
Active Directory Users and Comp
File Action View Window He
Active Directory Users and Computer
Saved Queries
development.queryvision.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Non-DC-Computers
Users
development.queryvision.com
General Managed By Group Po
development.queryvi
Domain name (pre-Windows 2000
Description:

Domain functional level:
Windows Server 2003

Forest functional level:
Windows Server 2003

Or us ADSI edit, AD Explorer similar tool and look for the property domainFunctionality on the domain object



Attribute	Value
configurationNamingContext	CN=Configu
currentTime	2011072116
defaultNamingContext	DC=develop
dnsHostName	w2003ent12
domainControllerFunctionality	2
domainFunctionality	2
dsServiceName	CN=NTDS S
forestFunctionality	2
highestCommittedUSN	14350670
isGlobalCatalogReady	TRUE
isSynchronized	TRUE
ldapServiceName	developmen

+ The Active Directory may be running in Mixed mode as well as long as the authenticating Domain Controller is running AD/Kerberos rather than NTLM BDC. If the Active directory is running in native mode this is true by default.

+ None of the computers participating in the authentication (web server, CM computer, client computer) is part of the Internet Zone regarding the user's Microsoft IE browser security settings.

QueryVision Note:

IE considers a web site to be Internet if the URL contains one or more "." (dots). So http://192.168.0.23 and http://w23stdcg10.development.queryvision.com are considered to be Internet, while http://w23stdcg10 is considered Intranet. Of course this can be overridden through adding the site via the Sites option in the intranet security settings in IE.

*+ The web server computer is in the **Trusted** or **Local Intranet** zone regarding the user's Internet Explorer security settings.*

+ All the computers participating in the authentication are time synchronized or within a skew of 5 minutes

+ All URLs specified in Cognos Configuration and user?s browsers use the fully qualified domain naming scheme. For example:

***http ://server.company.com/Cognos8** will work*

***http://servername/Cognos8** may cause issues*

IIS Web Server

*+ The IIS web server is running on a computer which is part of a domain within the **same** forest as the Active Directory Server targeted for authentication.*

*+ The IIS web server is **using HTTP Keep alives**, as this is required for Kerberos to work (this is default).*

+ The IIS web server is correctly configured to support Kerberos authentication! NTLM will work for SSO but will cause issues in multi-domain setups and prevent impersonation.

QueryVision Note:

IIS 6 and 7 are configured for Kerberos as default.

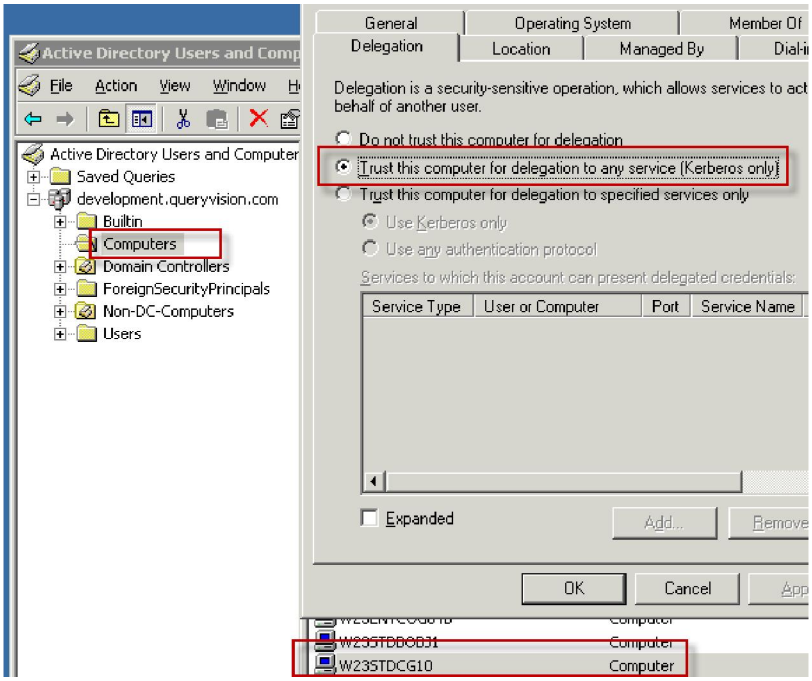
*+ If IIS is running as **Local System** or **Network Service** account, then the machine IIS is running on has the **trusted for delegation** property set. If IIS is running as a domain account, that account has the **trusted for delegation** property set.*

QueryVision Note:

This is the key setting.

This is “unconstrained” delegation. A more sophisticated and secure choice is Kerberos Constrained Delegation (KCD) which can be used to authenticate Extranet or even Internet users via Protocol Transition (which is enabled for IIS if KCD is used.

Kerberos Delegation:



Active Directory Users and Computer
- Saved Queries
- development.queryvision.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Non-DC-Computers
  - Users

Delegation is a security-sensitive operation, which allows services to act behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

○ Use Kerberos only

○ Use any authentication protocol

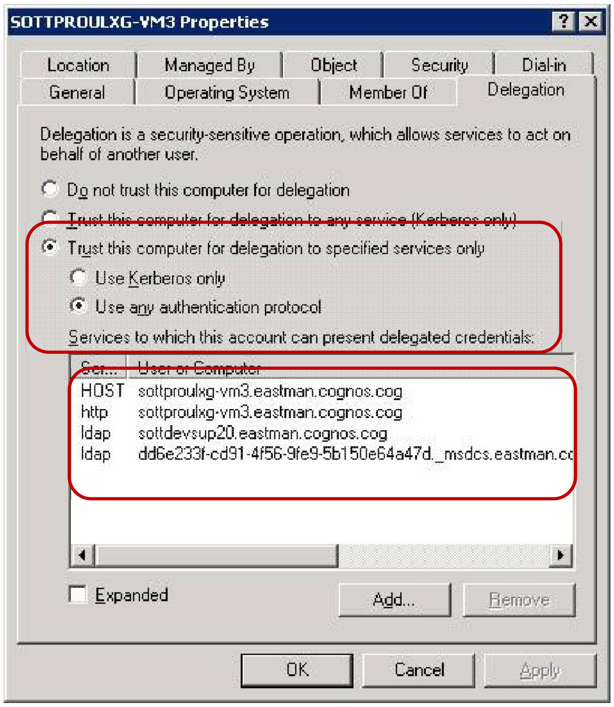
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name

□ Expanded

W23STDBDB31	Computer
W23STDCG10	Computer

Kerberos Constrained Delegation for Cognos 8/10:



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

Ser...	User or Computer
HOST	sottproulxg-vm3.eastman.cognos.cog
http	sottproulxg-vm3.eastman.cognos.cog
ldap	sottdevsup20.eastman.cognos.cog
ldap	dd6e233f-cd91-4f56-9fe9-5b150e64a47d._msdcs.eastman.cc

□ Expanded

QueryVision Note: KCD for Cognos will be covered in more depth in a coming blog/white paper.

Content Manager component:

+ Content Manager is installed on a computer which runs Windows 2003 server or Windows 2008 or 2008 R2 server. Note: Technically Content Manager may be installed on Windows XP as well, but there are known issues in Microsoft's Kerberos implementation which may hinder stability. Microsoft itself does not consider XP a server OS and will only fix Kerberos issues if reproducible on a server OS as well. This has officially been stated to Cognos and hence we exclude Windows XP to prevent customers from getting trapped.

+ Content Manager is installed on a computer which is member of a domain within the ***same*** *forest as the Active Directory Server targeted for authentication.*

+ If Content Manager is running as ***Local System*** *or* ***Network Service*** *account, then the computer account has the* ***trusted for delegation*** *property set*

+ If Content Manager is running as a domain account, that account has the ***trusted for delegation*** *property set.*

TIP: To determine the account Content Manager is running at, go to Computer Management -> Services and look for the value in the "Logon As" column of the "Cognos 8..." Service entry.

Users

+ All users which will authenticate to the IIS and eventually Cognos 8 are members of domains within the ***same*** *forest as the Active Directory Server targeted for authentication.*

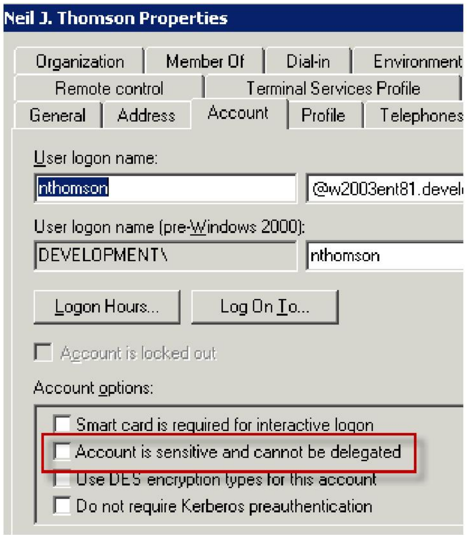
QueryVision Note:

Use of Kerberos Constrained Delegation can extend the reach to Extranet and Internet users.

+ Additional properties may need to be configured for the Active Directory authentication provider if Users come from a different domain than the Active Directory Server targeted for authentication, see 3).

All users which will authenticate to the IIS and eventually Cognos 8 must not have the ***Account is sensitive and cannot be delegated*** *setting enabled.*

TIP: To verify, check the account properties in the Microsoft Active Directory -> Users and Computers console.



User logon name: nthomson @w2003ent81.devel

User logon name (pre-Windows 2000): DEVELOPMENT\ nthomson

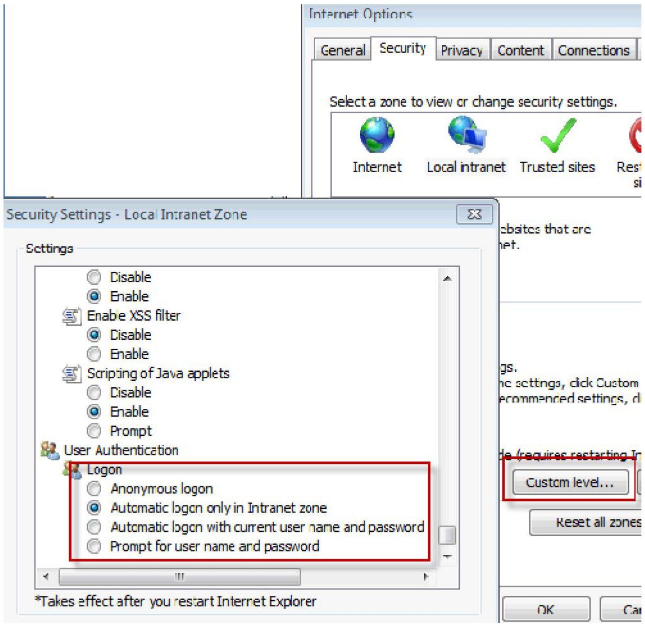
□ Account is locked out

Account options:

□ Smart card is required for interactive logon
□ Account is sensitive and cannot be delegated
□ Use DES encryption types for this account
□ Do not require Kerberos preauthentication

+ All the users acce … *8 use a supported Microsoft Internet E* … ***ted Windows Authentication*** *sett*

TIP: To verify check … *section.*



○ Disable
● Enable

Enable XSS filter
● Disable
○ Enable

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

*Takes effect after you restart Internet Explorer

+ On each Content Manager component in the system, configure an Active Directory namespace and point it at the Active Directory Server targeted for authentication or at any domain Controller in the same forest or to the domain name only to leverage Windows build-in DNS based failover, given the required advanced properties ***chaseReferrals*** *and/or* ***MultiDomainTrees*** *are set.*

For details see section "Configure an Active Directory Namespace" in the Cognos 8 Installation and Configuration Guide or later in Scenario 2, below.

+Start Microsoft Internet Explorer Browser and enter the fully qualified URL of the Cognos 8 Gateway. If prompted, select the Active Directory Namespace.

+You will get authenticated automatically now.

Scenario 2: [Cognos] Native Active Directory using NTLM/Remote User

1. Establish a Realm in IIS

For the Cognos virtual directories configured as described in "Configure the Web Server" in Chapter 6 of the Installation and Configuration Guide, enable any of the supported authentication methods on the IIS Web server

2. Make sure the following prerequisites are met:

General

+ All URIs specified in Cognos Configuration and user?s browsers use the fully qualified domain naming scheme. For example:

http ://server.company.com/Cognos8 will work

http://servername/Cognos8 may cause issues

+ All users which will authenticate to the IIS and eventually Cognos 8 are members of domains within the same forest as the Active Directory Server targeted for authentication.

Note: Additional properties may need to be configured for the Active Directory authentication provider if Users come from a different domain than the Active Directory Server targeted for authentication, see 3).

+ All the users accessing the web server and eventually Cognos8 use a supported browser and can successfully authenticate to the webserver for the configured method.

IIS Web Server

+ The IIS web server is running on a computer which is part of a domain within the same forest as the Active Directory targeted for authentication

Content Manager component

+ Content Manager is installed on a computer which runs Windows XP, Windows 2000 or Windows 2003.

+ Content Manager is installed on a computer which is member of a domain within the same forest, or within a forest which has full trust to the forest, the Active Directory Server targeted for authentication is in.

+On each Content Manager component in the system, configure an Active Directory namespace and point it at the Active Directory Server targeted for authentication or at any domain Controller in the same forest or to the domain name only to leverage Windows build-in DNS based failover, given the required advanced properties chaseReferrals and/or MultiDomainTrees are set.

From the Cognos 10 Installation & Configuration Manual

Include or Exclude Domains Using Advanced Properties
When you configure an authentication namespace for IBM® Cognos®, users from only one domain
can log in. By using the Advanced properties for Active Directory Server, users from related (parent-
child) domains and unrelated domain trees within the same forest can also log in.

Authentication in One Domain Tree

If you set a parameter named **chaseReferrals** to true, users in the original authenticated domain and
all child domains of the domain tree can log in to IBMCognos. Users **above the original authenticated domain** or in a different domain tree cannot log in.

Authentication in All Domain Trees in the Forest

If you set a parameter named **MultiDomainTrees** to true, users in all domain trees in the forest can
log in to IBM Cognos.
Steps
1. In every location where you installed Content Manager, open IBM Cognos Configuration.
2. In the Explorer window, under Security > Authentication, click the Active Directory namespace.
3. In the Properties window, specify the Host and port property:

- For users in one domain, specify the host and port of a domain controller for the single domain.
- For users in one domain tree, specify the host and port of the top-level controller for the
domain tree.
- For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.

4. Click in the Value column for Advanced properties and click the edit button.
5. In the Value - Advanced properties window, click Add.
6. Specify two new properties, chaseReferrals and MultiDomainTrees, with the values from the
following table:

MultiDomainTrees	chaseReferrals	Authentication for
False	False	One domain
False	True	One domain tree
True	False (would be redundant)	All domain trees in the forest

For more information see:

https://www-304.ibm.com/support/docview.wss?uid=swg21366722&aid=1

Alternate:

http://queryvision.com/wp-content/uploads/2011/07/Cognos-8-Kerberos-chaseReferrals-and-MultiDomainTrees-KB-1041799.pdf

+ In addition to those steps, an advanced property needs to be set using Cognos Configuration to disable the use of Microsoft Kerberos for single signon like this:

+ In the Explorer window, under Security, Authentication, click the Active Directory namespace.

+ Click in the Value column for advanced properties and then click the edit button

+ In the Value - Advanced properties window, click Add.

*+ In the Name column, type **singleSignonOption** (Case sensitive)*

*+ In the Value column, type **IdentityMapping** (Case sensitive)*

+ Click OK.

+ Save configuration and restart Service for the setting to take effect

*TIP: To switch back to Kerberos delegation, edit Advanced properties again and either delete the property or in the Value column, type **KerberosAuthentication**.*

QueryVision Note:

Just remove the singleSignonOption

4. Start Microsoft Internet Explorer Browser and enter the URL of the Cognos 8 Gateway.

+ If IIS was configured for Basic or Digest Authentication you will get prompted by IIS for authentication. Provide valid credentials and hit Enter.

+ If IIS was configured for Integrated Windows Authentication, no prompting for credentials will occur. If prompted by Cognos 8 to select a Namespace, select the Active Directory Namespace.

You will get authenticated to Cognos 8 automatically now.

Scenario 3 - [Cognos] LDAP access for Active Directory using NTLM/Remote User

1. Establish a Realm in IIS

For the Cognos virtual directories configured as described in "Configure the Web Server" in Chapter 6 of the Installation and Configuration Guide, enable any of the supported authentication methods on the IIS Web server

2. Make sure the following prerequisites are met:

General

+ All URIs specified in Cognos Configuration and user?s browsers use the fully qualified domain naming scheme. For example:

http ://server.company.com/Cognos8 will work

http://servername/Cognos8 may cause issues

+ All users which will authenticate to the IIS and eventually Cognos 8 are members of domains within the same forest as the Active Directory Server targeted for authentication.

Note: Additional properties may need to be configured for the Active Directory authentication provider if Users come from a different domain than the Active Directory Server targeted for authentication, see 3).

+ All the users accessing the web server and eventually Cognos8 use a supported browser and can successfully authenticate to the webserver for the configured method.

IIS Web Server

+ The IIS web server is running on a computer which is part of a domain within the same forest as the Active Directory targeted for authentication

Content Manager component

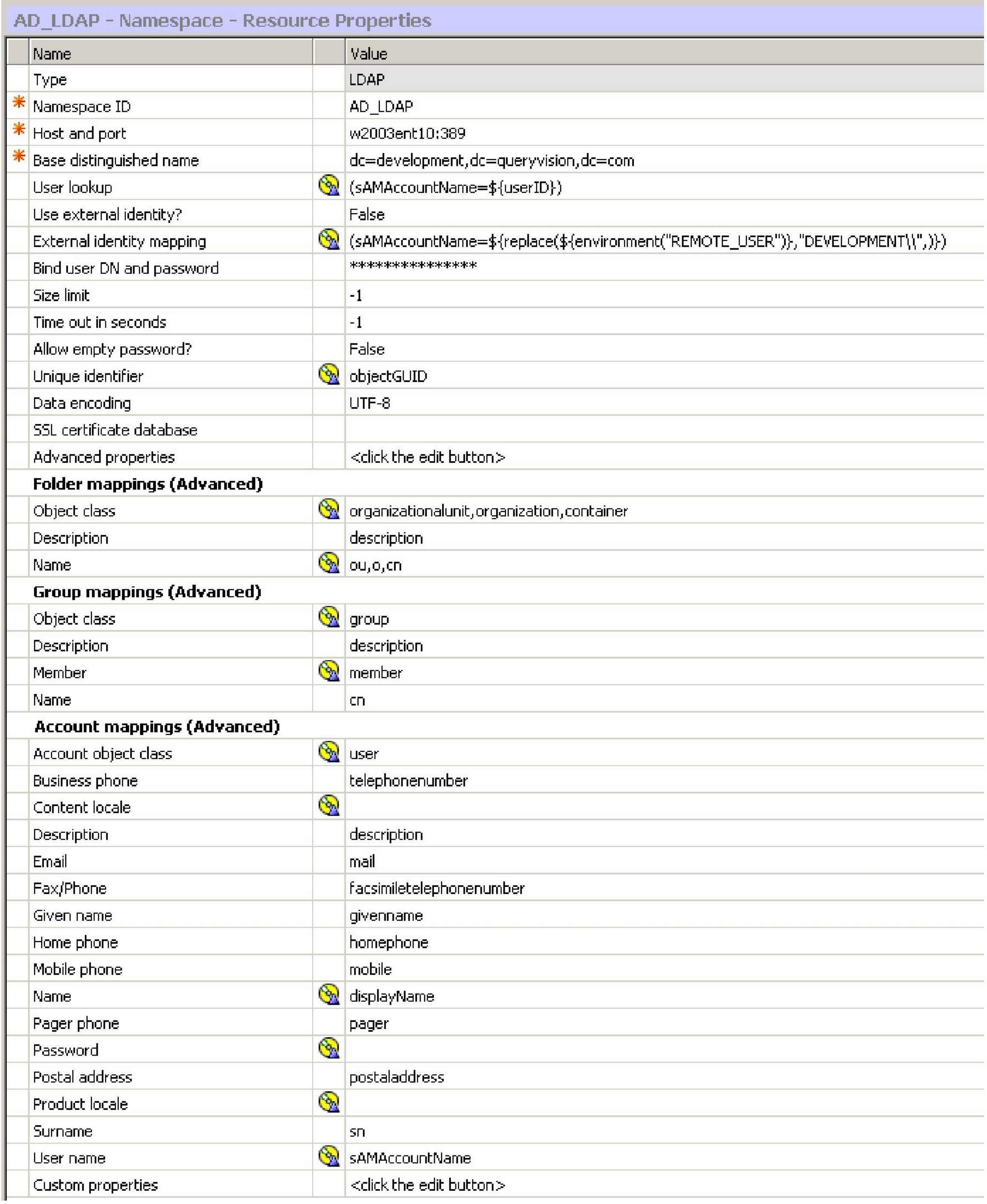
+ Content Manager is installed on a computer which runs Windows XP, Windows 2000 or Windows 2003.

+ Content Manager is installed on a computer which is member of a domain within the same forest, or within a forest which has full trust to the forest, the Active Directory Server targeted for authentication is in.

+On each Content Manager component in the system, configure an LDAP namespace and point it at the Active Directory Server targeted for authentication or at any domain Controller in the same forest or to the domain name only to leverage Windows build-in DNS based failover.

+Set up the LDAP namespace properties. The following screen shot of Cognos Configuration is an example of configuration against an AD DC (w2003ent10) on a domain (FQDN) development.queryvision.com. As a guide to what requires changing from the default/initial settings, look for the “changed” symbol . The following fields will need values specific to your installation:

- Namespace ID
- Host and port (for Active Directory Domain Controller)
- Base distinguished name
- User lookup
- External identity mapping



AD_LDAP - Namespace - Resource Properties

	Name		Value
	Type		LDAP
*	Namespace ID		AD_LDAP
*	Host and port		w2003ent10:389
*	Base distinguished name		dc=development,dc=queryvision,dc=com
	User lookup		(sAMAccountName=${userID})
	Use external identity?		False
	External identity mapping		(sAMAccountName=${replace(${environment("REMOTE_USER")},"DEVELOPMENT\\",)})
	Bind user DN and password		***************
	Size limit		-1
	Time out in seconds		-1
	Allow empty password?		False
	Unique identifier		objectGUID
	Data encoding		UTF-8
	SSL certificate database		
	Advanced properties		<click the edit button>
	Folder mappings (Advanced)		
	Object class		organizationalunit,organization,container
	Description		description
	Name		ou,o,cn
	Group mappings (Advanced)		
	Object class		group
	Description		description
	Member		member
	Name		cn
	Account mappings (Advanced)		
	Account object class		user
	Business phone		telephonenumber
	Content locale		
	Description		description
	Email		mail
	Fax/Phone		facsimiletelephonenumber
	Given name		givenname
	Home phone		homephone
	Mobile phone		mobile
	Name		displayName
	Pager phone		pager
	Password		
	Postal address		postaladdress
	Product locale		
	Surname		sn
	User name		sAMAccountName
	Custom properties		<click the edit button>

What is key here is the remote user (external identity mapping) script which is used to remove the sub-domain (e.g. remove DEVELOPMENT from DEVELOPMENT\<userid>). The expression shown is a string macro that performs this solution.

Bind user DN and password.

The Bind user DN and password needs to be provided to connect to AD via LDAP. You will be prompted for an administration authentication to run under and the password.

The entry for the User ID needs to be in LDAP form, for example:

cn=Administrator,cn=users,dc=development,dc=queryvision,dc=com

Note that order is important

Single Sign-on vs. Authenticated

The only difference for the above settings between single sign-on and challenge response is the setting

Use external identity?

True - single sign-on

False - challenge/response

4. Start Microsoft Internet Explorer Browser and enter the URL of the Cognos 8 Gateway.

+ If IIS was configured for Basic or Digest Authentication you will get prompted by IIS for authentication. Provide valid credentials and hit Enter.

+ If IIS was configured for Integrated Windows Authentication, no prompting for credentials will occur. If prompted by Cognos 8 to select a Namespace, select the Active Directory Namespace.

You will get authenticated to Cognos 8 automatically now.