nirva

How-to: Single Sign-On

Document version: 1.02

This document describes how to use the Single Sign-On (SSO) features of Nirva. It addresses specialists of computer security. It implies that the security configuration of your organization is defined properly and that involved components are correctly set up. Any support issue regarding SSO will be accepted from security specialists only and after proving that the problem doesn't come from the environment

Overview

Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can allow a user to access all computers and systems according to access permission, without the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable.

Nirva supports Single Sign-On thereby avoiding already identified users of a domain to re-enter credentials to access Nirva applications.

SSO is currently available on Windows platforms only (client and server) for the following clients:

- Web browser (IE and Firefox)
- Nirva client connectors using the nvc.dll library (Java, command line, C, C++, Perl, PHP, .Net, Cold Fusion, ActiveX, Virtual Printer).
- Web services or XML HTTP clients implementing the SSO standard protocols “Negotiate”, “Kerberos” or “NTLM”. The Negotiate protocol is a Microsoft specific protocol allowing to automatically choosing between Kerberos or NTLM following the configuration and availability of security components in the target environment.

When an access to Nirva requires the client to sign on, Nirva sends some special information to the client over HTTP, telling it that an authentication is required and that the “Negotiate”, “Kerberos” and “NTLM” protocols are accepted. According to available capabilities, the client will choose one of these protocols. The Nirva Windows clients using the nvc library will use the “Negotiate” protocol. The client browsers (IE and Firefox) also use the “Negotiate” protocol.

In this document whereas “Kerberos” is mentioned, one must understand “Kerberos” or “Kerberos over Negotiate”. When “NTLM” is mentioned, one must understand “NTLM over Negotiate”.

SSO involves three parts:

- The domain controller. This is a Microsoft Active Directory server on this example. This domain controller also acts as a Kerberos server when Kerberos is to be used.
- The Nirva server is the computer running the Nirva application to be used with SSO.
- The client computer is the client connecting to the Nirva application using SSO.

This example uses the following information:

- Domain controller = NIRVADC

- Domain = nirvalyon.local
- Nirva server = BENJ
- Nirva service account = ssotest
- Nirva application = SSOTEST

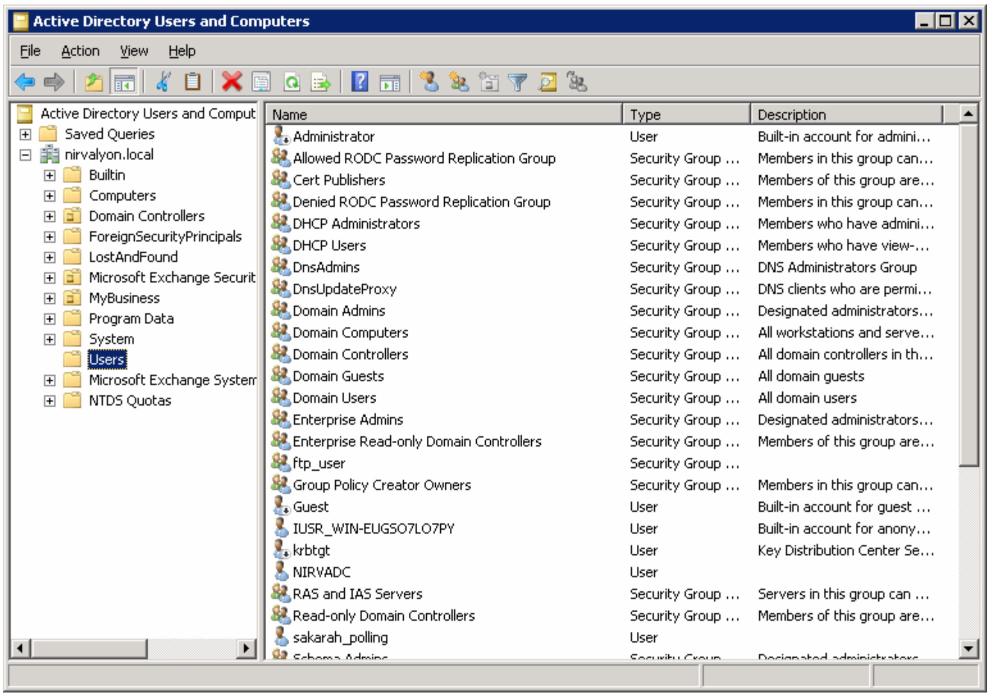
Configuring the domain controller

Creating a special user account

This part is required only when “Kerberos” protocol is to be used.

For each Nirva server that needs to be SSO (Kerberos) enabled, a special user account must be created. This user account is called a Service Principal Name account (SPN account). This user acts as the connection between the Kerberos server, the Active Directory and the Nirva server. This user account will be used to run the Nirva service on the Nirva server.

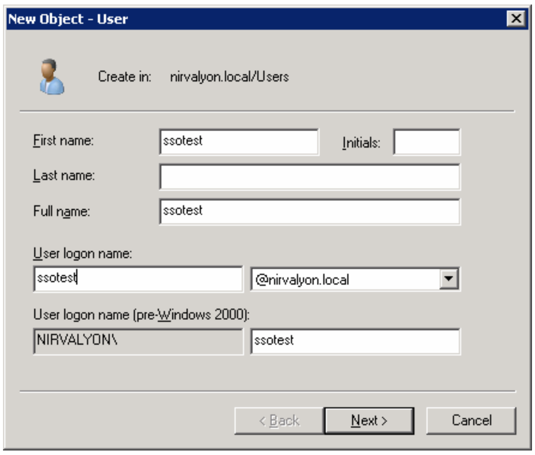
Start the Active Directory User and Computers from the Administration tools menu.



- Active Directory Users and Comput
  - Saved Queries
  - nirvalyon.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - Microsoft Exchange Securit
    - MyBusiness
    - Program Data
    - System
    - Users
    - Microsoft Exchange System
    - NTDS Quotas

Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed RODC Password Replication Group	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Replication Group	Security Group ...	Members in this group can...
DHCP Administrators	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domain Controllers	Security Group ...	Members of this group are...
ftp_user	Security Group ...	
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
IUSR_WIN-EUGSO7LO7PY	User	Built-in account for anony...
krbtgt	User	Key Distribution Center Se...
NIRVADC	User	
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
sakarah_polling	User	
Schema Admins	Security Group	Designated administrators

Right click the Users folder and select new - user



New Object - User

Create in: nirvalyon.local/Users

First name: ssotest

Initials:

Last name:

Full name: ssotest

User logon name: ssotest @nirvalyon.local

User logon name (pre-Windows 2000): NIRVALYON\ ssotest

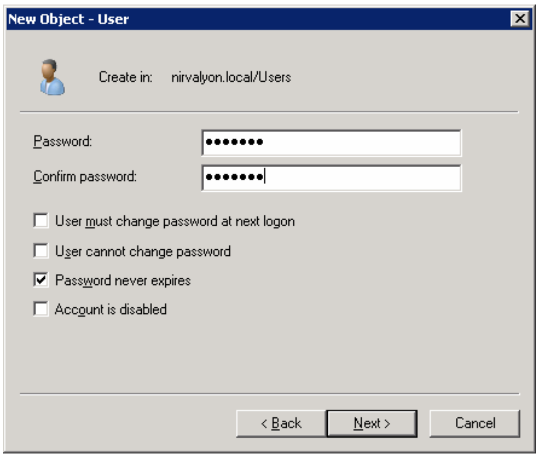
The user name should be a specific user name in the domain that will be used for starting the Nirva service. A computer or user with the same name must not exist on the domain.

Here the domain is nirvalyon.local and the user is ssotest.

Enter the name into the User logon name

Press next.

Enter the password and select Password never expires.



New Object - User

Create in: nirvalyon.local/Users

Password: •••••••

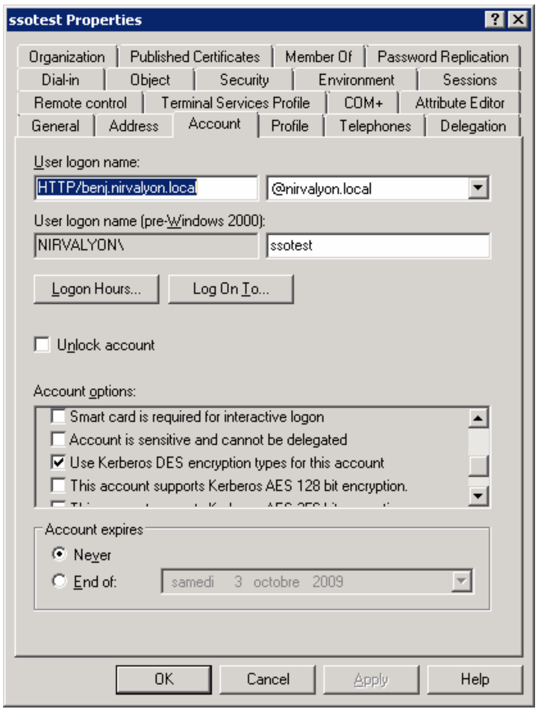
Confirm password: •••••••

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☑ Password never expires
- ☐ Account is disabled

Click Next and then Finish in order to confirm the new user account

Now we need to modify the user account in order to specify the encryption algorithm.

Open the newly created user account. Select the account tab.



User logon name: HTTP/benj.nirvalyon.local @nirvalyon.local

User logon name (pre-Windows 2000): NIRVALYON\ ssotest

□ Unlock account

Account options:

□ Smart card is required for interactive logon
□ Account is sensitive and cannot be delegated
☑ Use Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.

Account expires
● Never
○ End of: samedi 3 octobre 2009

Scroll down to the bottom of the Accounts options section.

Select the Use DES encryption types for this account.

When changing the ‘Use DES encryption…’ checkbox on a user account, the password MUST be reset after the change has been done.
To reset the password, right click on the user account and select the option Reset Password, re-enter the password and press the OK button.

Setting principal names

This part is only required if the “Kerberos” protocol is to be used.

Now that the user account has been created and updated, we need to create a service principal setting for the created user account.

The service principal name is a unique key identifying the SSO target

It has the following format: `Service/Server`

The service for Nirva clients using nvc library can be set to “NIRVA”.

The service for browsers connecting Nirva must be set to “HTTP”. For example if, from your web browser, you want to access via SSO to a Nirva resource located on the url “`http://benj:1081/....`” Then you must set the SPN to “`HTTP/benj`”.

The server must be set to the DNS name of the target server (Nirva server). This DNS name must be unique and the reverse lookup DNS table must also have a single entry for the server.

So in our example, enter the following commands:

```
setspn –A HTTP/benj nirvalyon.local\ssotest
setspn –A NIRVA/benj nirvalyon.local\ssotest
```

A given SPN must be associated with only one account otherwise the “Kerberos” protocol will fail. More generally, when using the “Negotiate” protocol, if a valid SPN corresponding to the requested resource exists, windows will use “Kerberos”. If not, windows may use “NTLM”.

You can list the SPNs associated to a given account with the “setspn –L account“ command. For example:

setspn –L nirvalyon.local\ssotest.

For urls using a DNS name instead of a direct machine name, the same DNS name must be registered as SPN with the HTTP service. For example, if you have a url “http://mysiteweb.com/” and you have defined that “mysiteweb.com” points to your nirva server (benj) in the DNS, then the “HTTP/mysiteweb.com” must be registered as SPN via setspn:

```
setspn –A HTTP/mysiteweb.com nirvalyon.local\ssotest
```

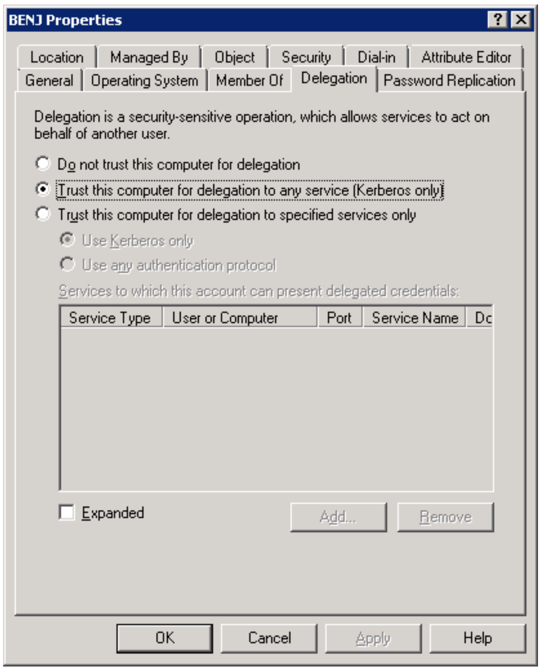
The port is not used by the browser to evaluate the principal name so if the url is “http://benj:1081/” the SPN will be “HTTP/benj”.

Allowing delegation

This part is only required if the “Kerberos” protocol is to be used.

If the nirva server is not the domain controller itself, make sure to set the nirva server machine as Trust computer for delegation:

Go to the Administrative Tools -> Active Directory Users and Computers. Expand the domain and click on Computers. Locate the nirva server computer and right click on “Properties”, then open the “Delegation” tab:



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:

Service Type	User or Computer	Port	Service Name	Dc

□ Expanded

Enable the “Trust this computer for delegation to any service (Kerberos only)” check box.

Configuring the Nirva server

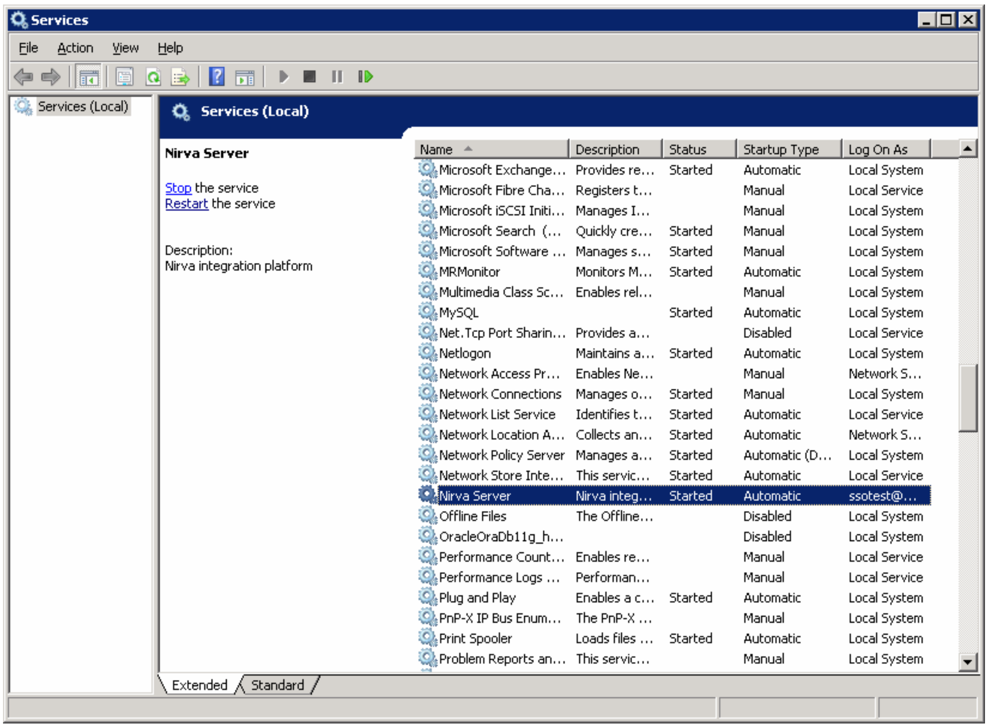
Running Nirva as the special user account.

This part is only required if the “Kerberos” protocol is to be used.

Nirva must be running in the context of the special user (ssotest) defined on the domain controller in previous step.

If you run Nirva in console mode, just start Nirva from this special user account session (ssotest).

If you run Nirva as a service, go to the control panel and open the “Services” window:



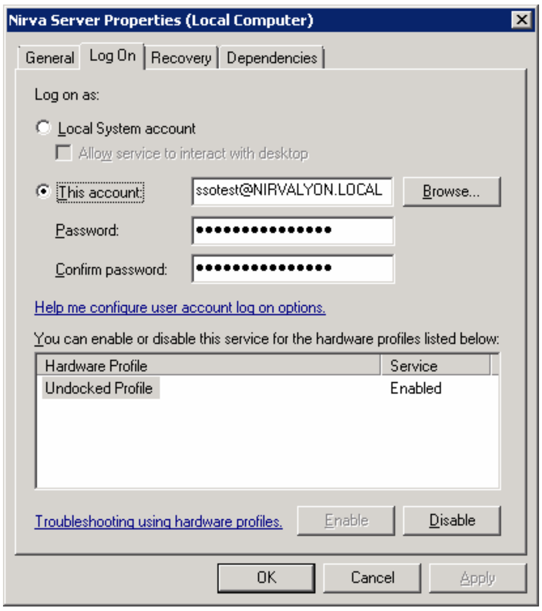
Nirva Server

Stop the service
Restart the service

Description:
Nirva integration platform

Name	Description	Status	Startup Type	Log On As
Microsoft Exchange…	Provides re…	Started	Automatic	Local System
Microsoft Fibre Cha…	Registers t…		Manual	Local Service
Microsoft iSCSI Initi…	Manages I…		Manual	Local System
Microsoft Search (…	Quickly cre…	Started	Manual	Local System
Microsoft Software …	Manages s…	Started	Manual	Local System
MRMonitor	Monitors M…	Started	Automatic	Local System
Multimedia Class Sc…	Enables rel…		Manual	Local System
MySQL		Started	Automatic	Local System
Net.Tcp Port Sharin…	Provides a…		Disabled	Local Service
Netlogon	Maintains a…	Started	Automatic	Local System
Network Access Pr…	Enables Ne…		Manual	Network S…
Network Connections	Manages o…	Started	Manual	Local System
Network List Service	Identifies t…	Started	Automatic	Local Service
Network Location A…	Collects an…	Started	Automatic	Network S…
Network Policy Server	Manages a…	Started	Automatic (D…	Local System
Network Store Inte…	This servic…	Started	Automatic	Local Service
Nirva Server	Nirva integ…	Started	Automatic	ssotest@…
Offline Files	The Offline…		Disabled	Local System
OracleOraDb11g_h…			Disabled	Local System
Performance Count…	Enables re…		Manual	Local Service
Performance Logs …	Performan…		Manual	Local Service
Plug and Play	Enables a c…	Started	Automatic	Local System
PnP-X IP Bus Enum…	The PnP-X …		Manual	Local System
Print Spooler	Loads files …	Started	Automatic	Local System
Problem Reports an…	This servic…		Manual	Local System

Then right click on the “Nirva server” entry and select “Properties” and the “Log On” tab:


Nirva Server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.
Troubleshooting using hardware profiles.
Enable
Disable
OK
Cancel
Apply

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: ssotest@NIRVALYON.LOCAL

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

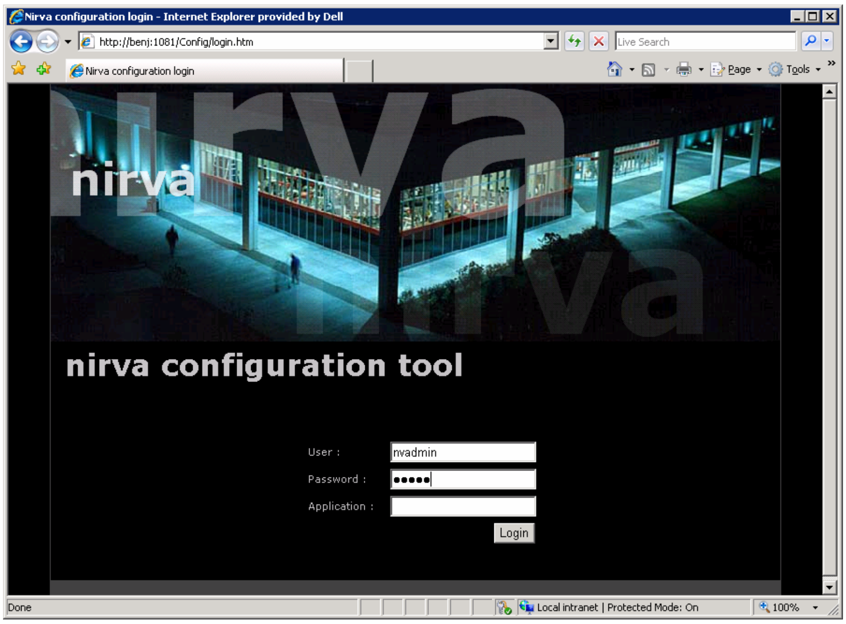
You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Undocked Profile	Enabled

Enable the “This account” check box and enter the name of the special user you have defined in the domain control (fully qualified user name). Enter the password and click OK. Then you can start the service.

Configuring Nirva

On Nirva, you must enable SSO for your Nirva application(s). For that, open the Nirva administration tool with nvadmin account:



Nirva configuration login - Internet Explorer provided by Dell

http://benj:1081/Config/login.htm

nirva configuration tool

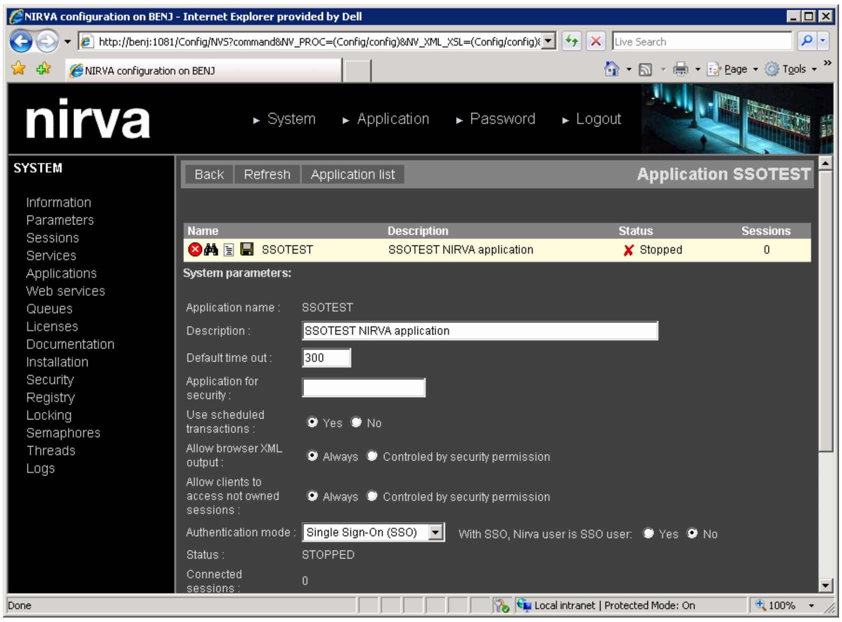
User : nvadmin

Password : •••••

Application :

Login

Then go the main System menu, select the “Applications” item in order to display the application list, then click on your application name (here SSOTEST) and stop the application if it was running:



NIRVA configuration on BENJ - Internet Explorer provided by Dell

http://benj:1081/Config/NVS?command&NV_PROC=(Config/config)&NV_XML_XSL=(Config/config)(

Application SSOTEST

Name	Description	Status	Sessions
SSOTEST	SSOTEST NIRVA application	✗ Stopped	0

System parameters:

Application name : SSOTEST

Description : SSOTEST NIRVA application

Default time out : 300

Application for security :

Use scheduled transactions : ● Yes ○ No

Allow browser XML output : ● Always ○ Controled by security permission

Allow clients to access not owned sessions : ● Always ○ Controled by security permission

Authentication mode : Single Sign-On (SSO) With SSO, Nirva user is SSO user: ○ Yes ● No

Status : STOPPED

Connected sessions : 0

In order to enable SSO, you must modify the “Authentication mode” line. You have 3 modes:

- **Nirva**. SSO is disabled.
- **Single Sign-On (SSO)**. SSO is enabled and mandatory. This is the only mode allowing SSO from browsers.
- **Nirva or Single Sign-On**. SSO is enabled only on client request. In this mode, Nirva clients using the nvc library must give a parameter in order to enable SSO on the session. This is a parameter in the connection string (see the documentation for the Nirva connectors).

When using SSO, you can choose to have the SSO user equal to the Nirva user or not. If not, the SSO is only used for authentication and the security is based on the Nirva user. The password for the Nirva user is not checked and can be omitted. If yes, the Nirva user becomes the SSO user and this SSO user must exists in the table of Nirva users. The nvadmin user never use SSO.

In any case, the SSO user and domain is available in the session context as session variables named “NV_SSO_USER” and “NV_SSO_DOMAIN”.

In our example, we choose “Single Sign-On (SSO) mode” and the Nirva user is not the SSO user.

Then start the Nirva application.

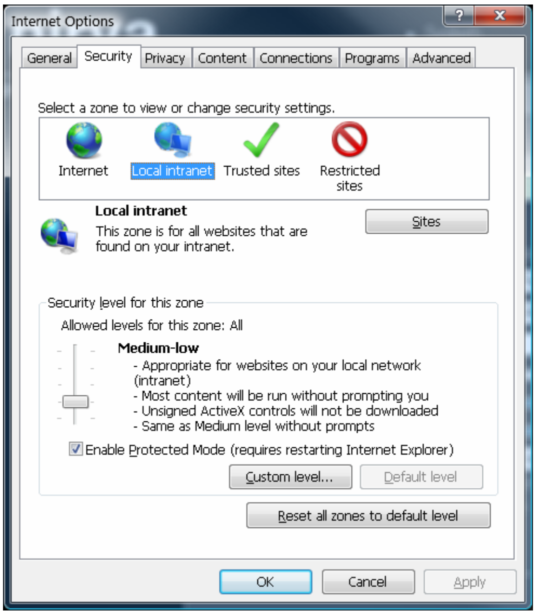
For the NVDEF application, you must go into the Systems parameters in order to enable SSO and you must stop and restart Nirva.

Configuring Clients

Browsers

Following your browser, you may have to do some specific configuration.

With internet explorer for example, you should add the website to the list of trusted web site on your local intranet. For that, go to the Tools menu, Internet options, Security. Click on local intranet and then “Sites” button:



Select a zone to view or change security settings.

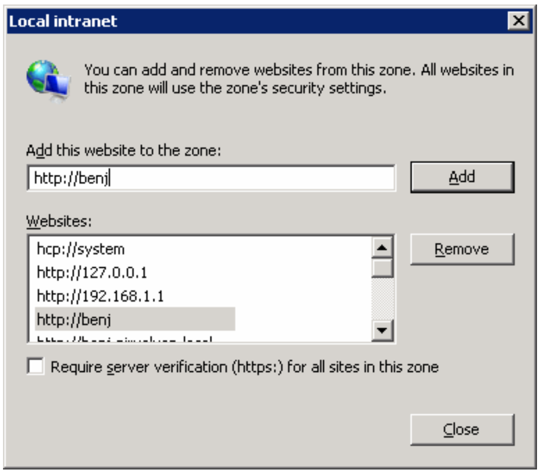
Local intranet
This zone is for all websites that are found on your intranet.

Security level for this zone
Allowed levels for this zone: All

Medium-low
- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

☑ Enable Protected Mode (requires restarting Internet Explorer)

Click on the site button and add the website (you may have an intermediate window for local intranet options):



Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

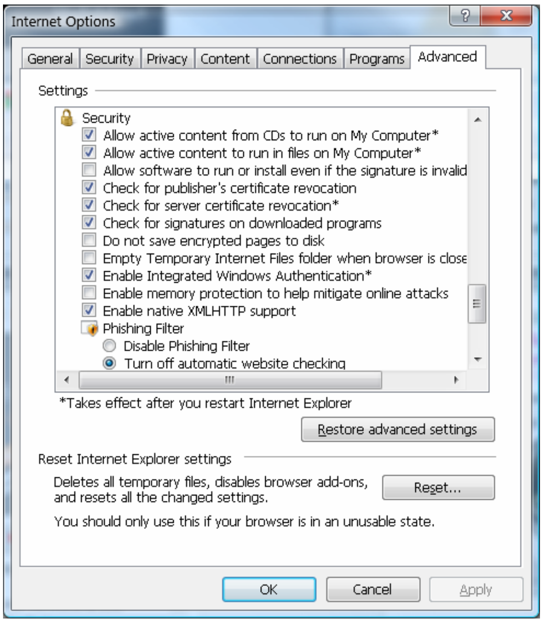
Add this website to the zone: http://benj

Websites:

hcp://system
http://127.0.0.1
http://192.168.1.1
http://benj

□ Require server verification (https:) for all sites in this zone

You must also be sure that in the internet options advanced tab, the line "Enable Integrated Windows Authentication" is checked:



Internet Options

Settings

Security
☑ Allow active content from CDs to run on My Computer*
☑ Allow active content to run in files on My Computer*
□ Allow software to run or install even if the signature is invalid
☑ Check for publisher's certificate revocation
☑ Check for server certificate revocation*
☑ Check for signatures on downloaded programs
□ Do not save encrypted pages to disk
□ Empty Temporary Internet Files folder when browser is close
☑ Enable Integrated Windows Authentication*
□ Enable memory protection to help mitigate online attacks
☑ Enable native XMLHTTP support
Phishing Filter
○ Disable Phishing Filter
● Turn off automatic website checking

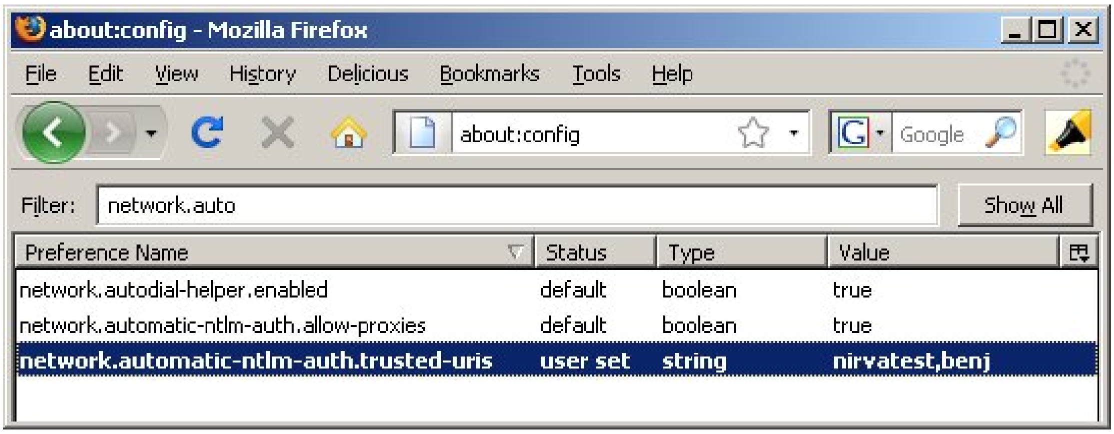
*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Deletes all temporary files, disables browser add-ons, and resets all the changed settings.

You should only use this if your browser is in an unusable state.

With Firefox, type "about:config" in the navigation bar and then search for "network.automatic-ntlm-auth.trusted-uris". Add the site server to it (separate from others with a comma character)



about:config - Mozilla Firefox

Filter: network.auto

Preference Name	Status	Type	Value
network.autodial-helper.enabled	default	boolean	true
network.automatic-ntlm-auth.allow-proxies	default	boolean	true
network.automatic-ntlm-auth.trusted-uris	user set	string	nirvatest,benj

Nirva clients

Nirva clients have 2 options for SSO.

The first option is the flag for enabling SSO when the application mode has been set to “Nirva or Single Sign-On”. This is generally part of the connection string as “Sso=YES” or “Sso=NO”. For the nvcc (command line connector) this is a string “(SSO)” in the –a option after the server address.

The second option is the SSO principal name when using Kerberos. This is generally part of the connection string as “SsoPrincipal=SPN”. The SPN must be an existing SPN as defined on the domain controller using the setspn command (see chapter “Configuring the domain controller”). For the nvcc (command line connector) this is a string “(SSO:SPN)” in the –a option after the server address.

Examples with nvcc (when Nirva application SSOTEST is in mode “Nirva or Single Sign-On”):

SSO using Kerberos (the SPN “NIRVA/benj” must have been defined in the domain controller otherwise NTLM will be automatically used):

```
Nvcc -p SSOTEST -a benj(SSO:NIRVA/benj) -z “NV_CMD=|MISC:NOP|”
```

SSO using NTLM:

```
Nvcc -p SSOTEST -a benj(SSO) -z “NV_CMD=|MISC:NOP|”
```

No SSO:

```
Nvcc -p SSOTEST -a benj -z “NV_CMD=|MISC:NOP|”
```

These examples use the Nirva default nvdef user.

In order to verify if SSO works, you can define a password to the nvdef user on the SSOTEST application. In this case the last command should return an error “invalid password” but the other ones should succeed.