One CA Plaza
Islandia, NY 11749

T +1 631 342 6000
F +1 631 342 6800
ca.com

June 20, 2013

Customer Request Number:	N/A
System/Application:	Policy Server
Module:	Siteminder Policy Store with DXmanager
Request Classification:	Technical Note
Versions:	SiteMinder Policy Serve R12.5 & above CA Directory r12.0 SP11 (build 7065) CA DXManager 12.0.7066

Version	Date	Author	Manager	Description
0.1	18 June 2013	Stephen McQuiggan		

Setup and Configure the Siteminder Policy Store with Dxmanager

Disclaimer

TABLE OF CONTENTS

Contents

1. Overview

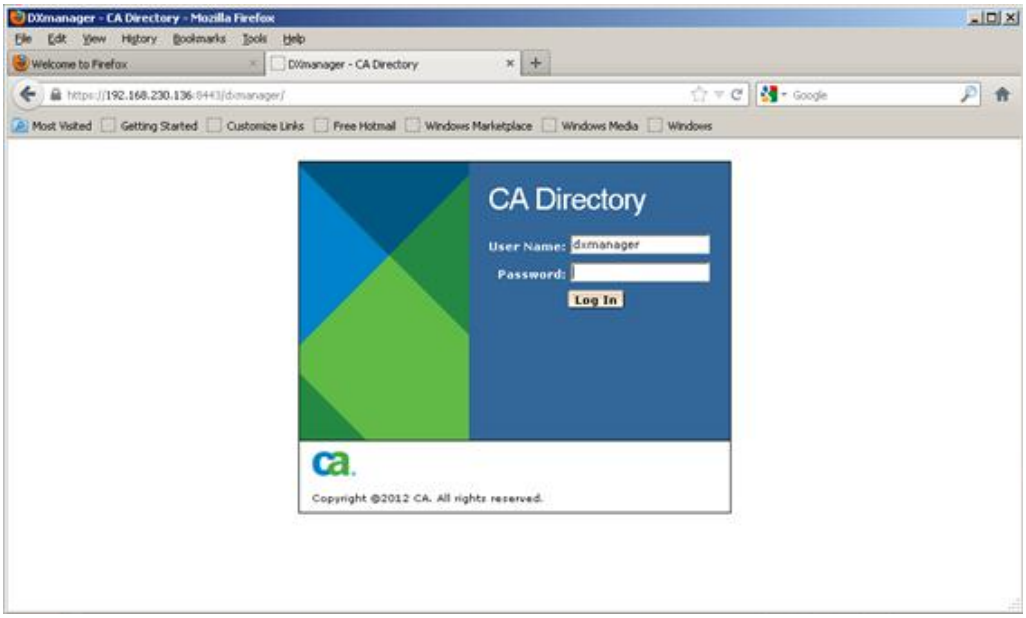
This document describes how to setup and configure a Siteminder Policy Store using CA Directory and the DXmanager interface to configure the policy store DSAs. It is assumed the reader understands X.500 and directory terminology, as well as how to use CA Directory and CA DXmanager and that they are both installed on the respective servers.

The examples in this document describe setting up and configuring a standalone policy store configuration with one router DSA and one data DSA in one site. Mention will be made

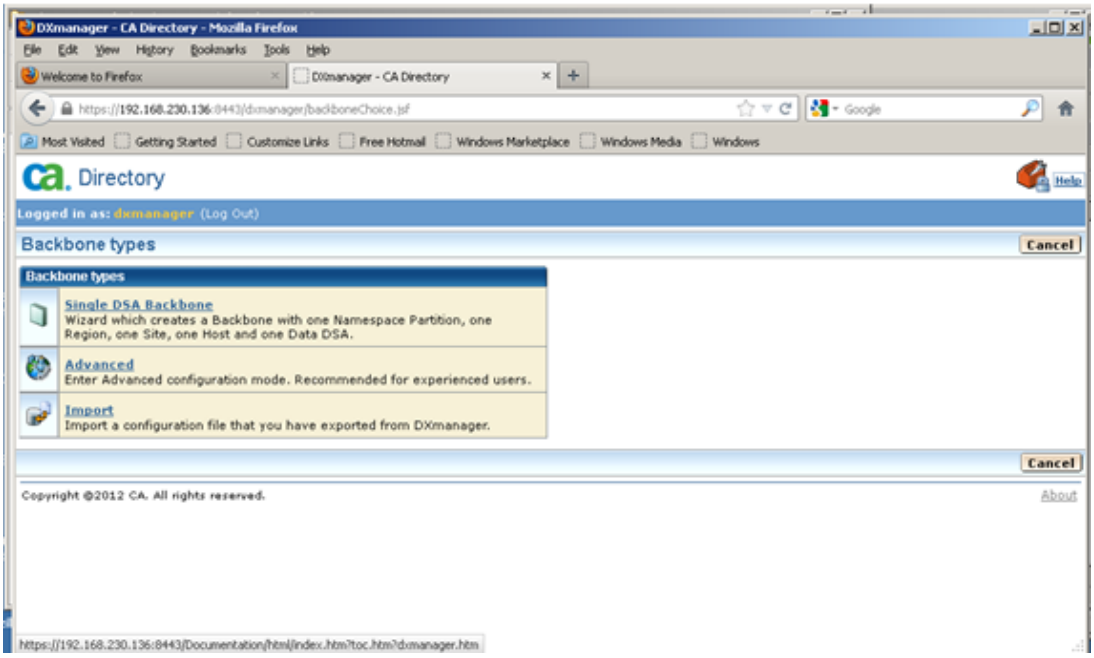
throughout on how to configure more than one instance, though direct instructions will not be provided.
Integration of a policy store instance with a user store instance within DXmanager requires further discussions and testing.

2. Initial setup

A. DXmanager Login



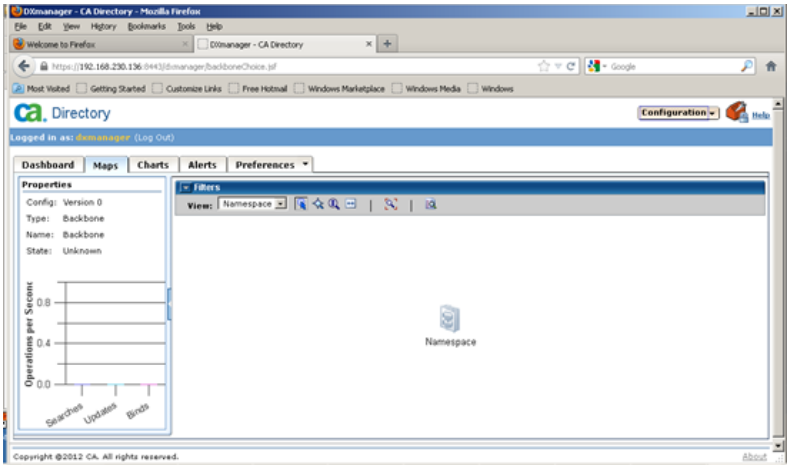
1. Login to DXmanager with the password as defined during CA Directory installation. https://<host>:8443/dxmanager/



2. If this is the first access to DXmanager, select ‘Advanced’ for the ‘backbone’ type

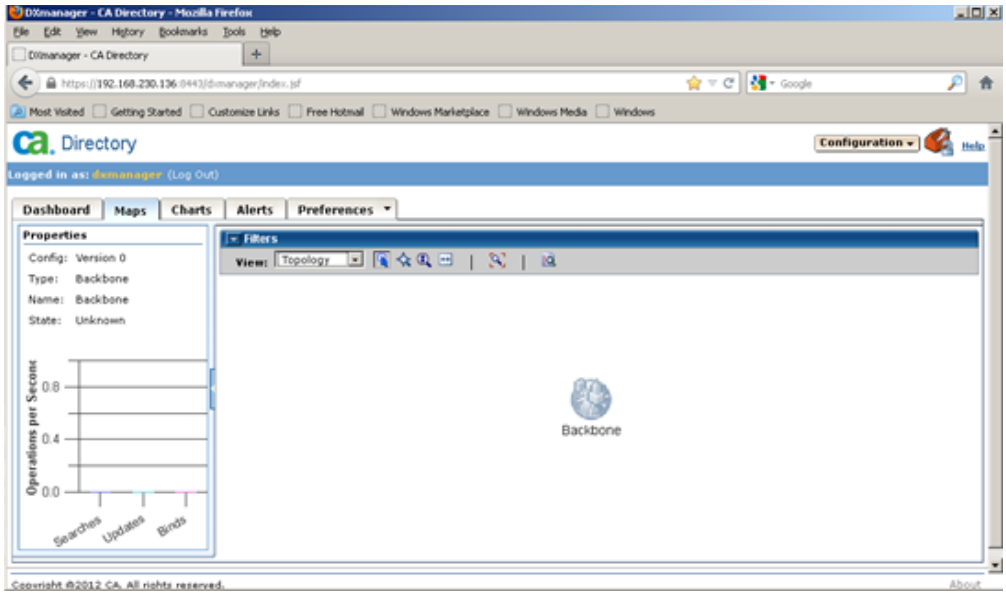
3. Always trust content from this publisher

4. Allow the applet to run. Select ‘permanently’ if available on the pop-up.

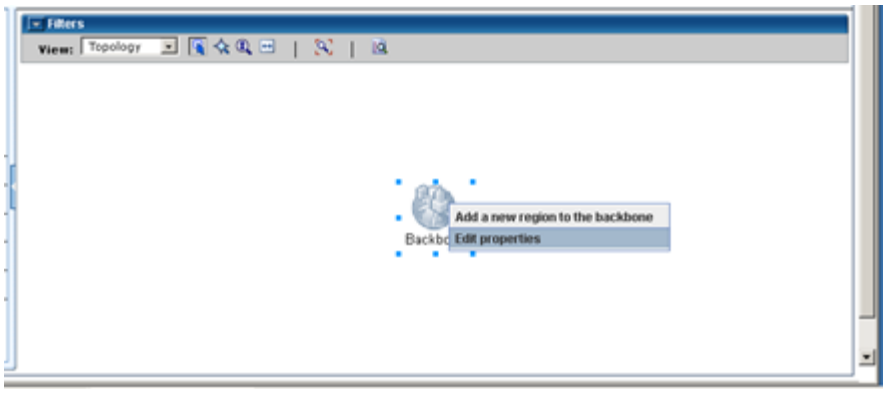


5. The ‘Namespace’ icon will be displayed.

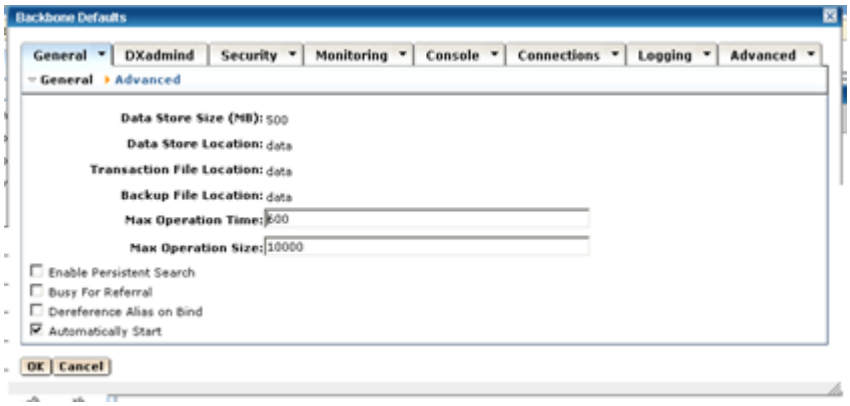
B. Define the Backbone defaults



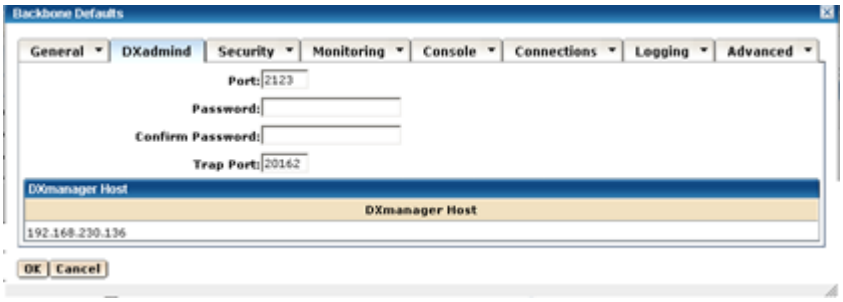
1. From the ‘Views’ pulldown list, select ‘Topology’. The ‘Backbone’ icon is displayed. It is necessary to define the Backbone general configuration before all else.



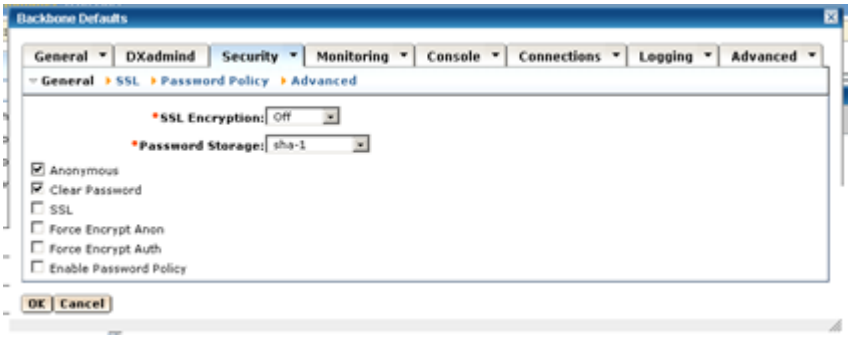
2. Select ‘Edit properties’



3. The ‘Backbone Defaults’ pop-up is displayed

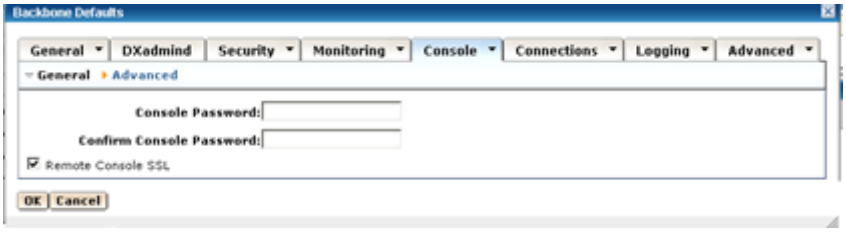


4. Click on the ‘DXadmind’ tab and enter the password and confirmation as defined during the CA Directory installation.

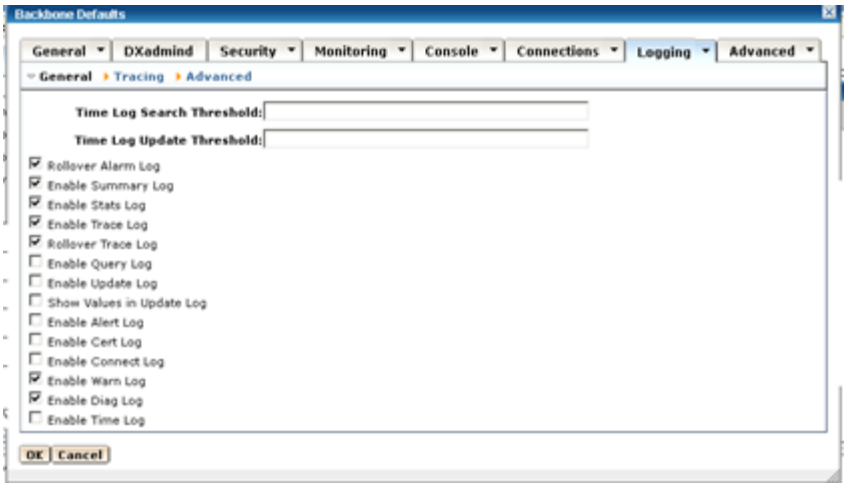


5. Click on the 'Security' tab and check the 'Anonymous' checkbox. This is required to allow access to create the initial DIT structure. This can be removed once a valid user has been created and appropriate access controls have been defined.

6. Optionally, click on the 'Monitoring' tab and select any additional actions which should be reported to the logfiles. (i.e. Report Multiwrite Errors)

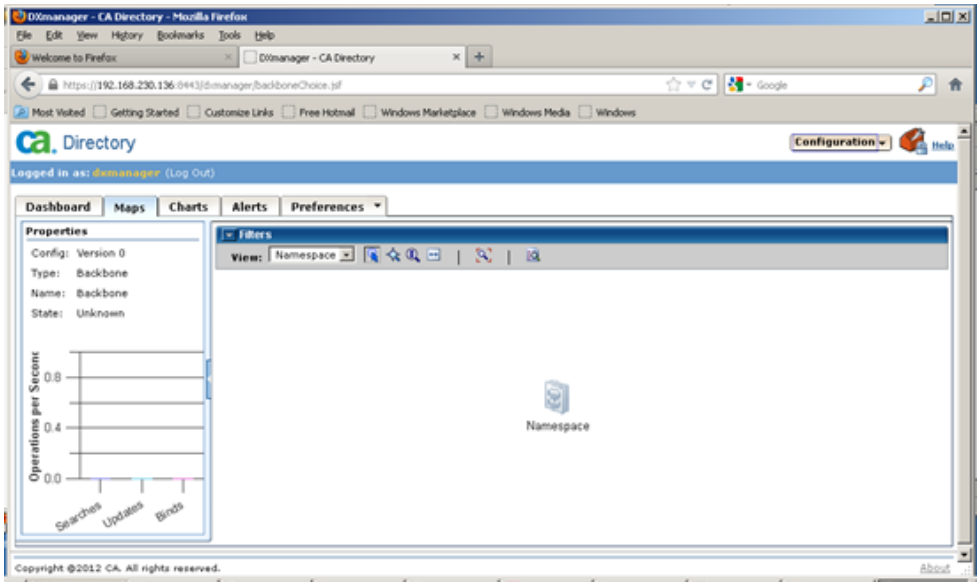


7. Click on the 'Console' tab and enter a password to access the DSA console.

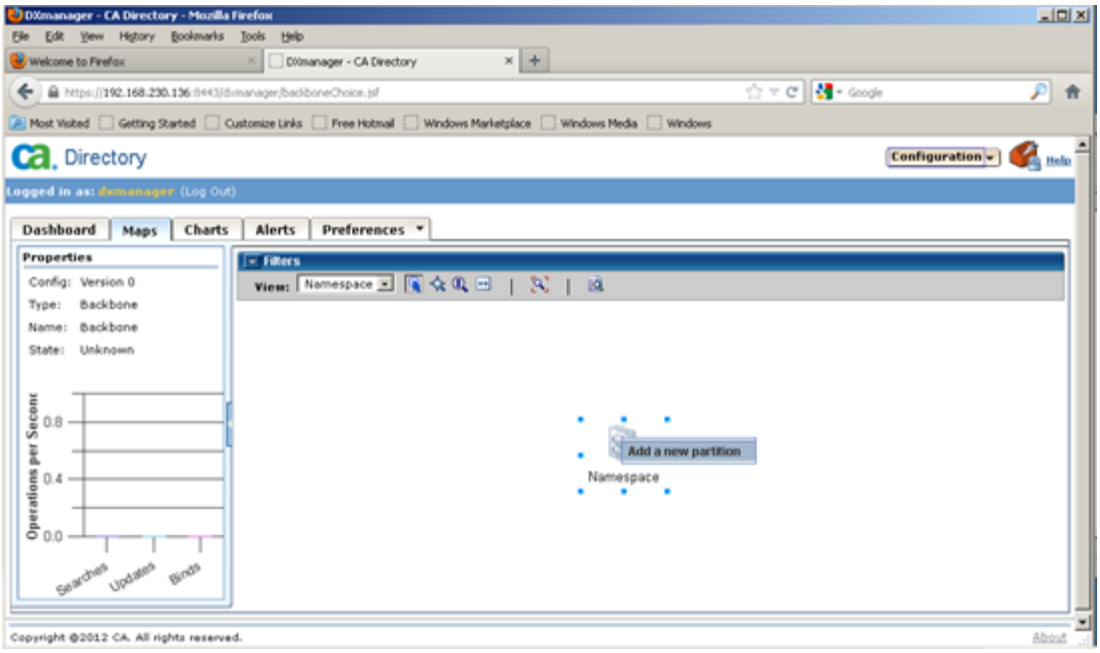


8. Click on the ‘Logging’ tab and select any additional logging. Recommended is to check the ‘Rollover Alarm Log’ and ‘Rollover Trace Log’ checkboxes.
9. Then click OK in the lower left corner of the pop-up to return to the ‘Backbone’ icon.

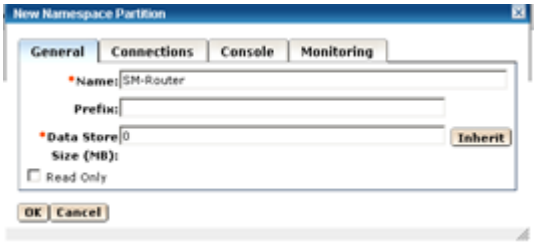
C. Define the Namespaces



1. From the ‘Backbone’ icon, select ‘Namespace’ from the ‘Views’ pull-down list. The ‘Namespace’ icon is displayed.
   There are 2 phases to creating the DSAs. One, is to define the logical namespaces and the other is to define the physical backbone. Please refer the CA Directory Administration Guide for further details.

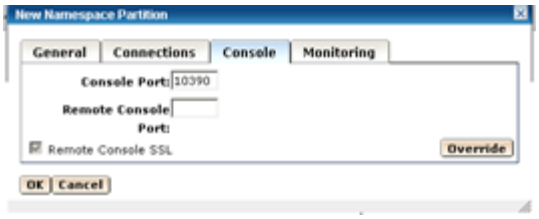


2. Right-click the ‘Namespace’ icon and select ‘Add a new partition’. The ‘New Namespace Partition’ pop-up is displayed.



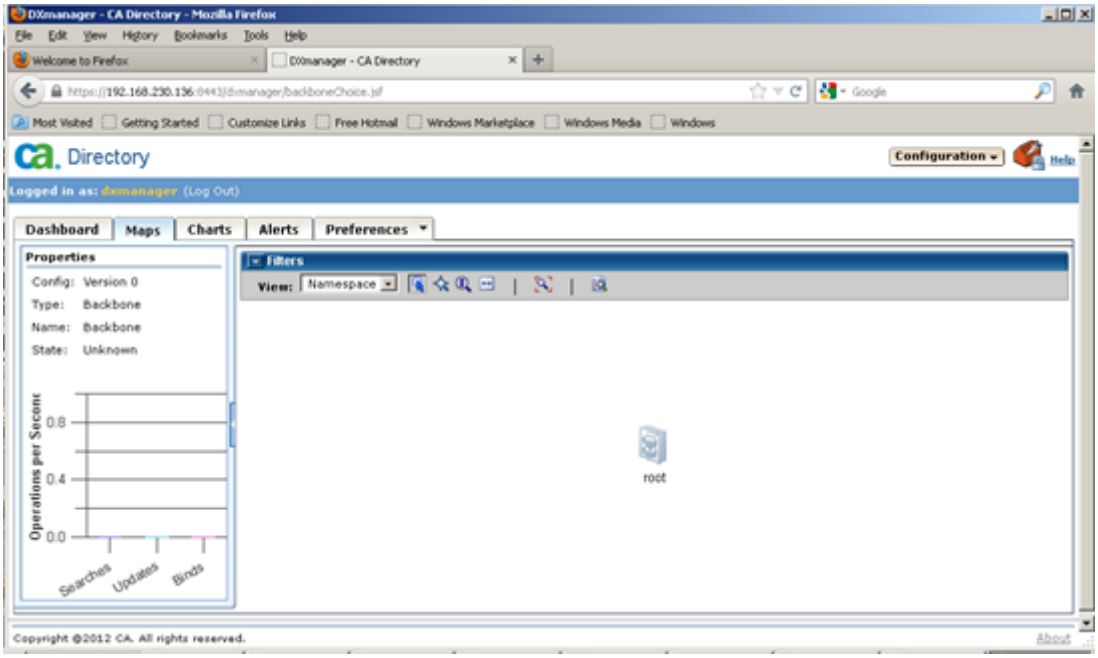
3. Fill in the appropriate details in the ‘General’ tab:
    a. Enter a generic name for the first namespace in the ‘Name’ field. For example, ‘SM-Router’ for the router DSA.
    b. Leave the ‘Prefix’ field blank
    c. Click on the ‘override’ button for the ‘Data Store’ size and make it zero (0).

4. Click on ‘Connections’ and enter an LDAP port. (e.g. 10389)

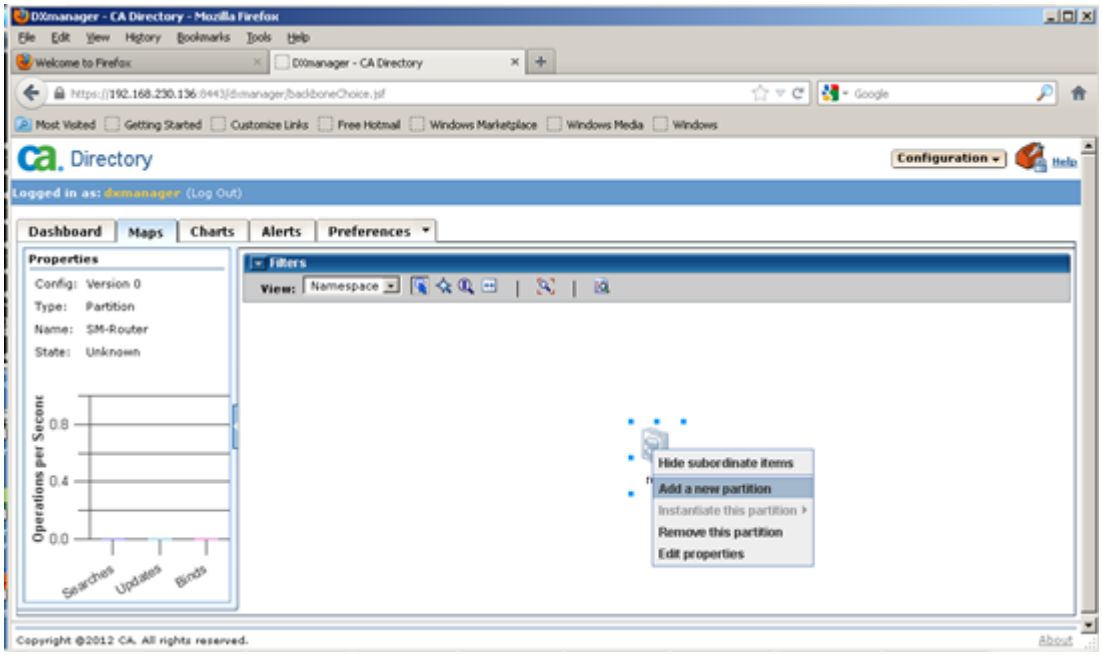


5. Click on the 'Console' tab and enter the telnet port for the DSA console; typically one port higher than the LDAP port. (e.g. 10390) Leave the 'Remote Console' port blank if no remote access is desired for added security.

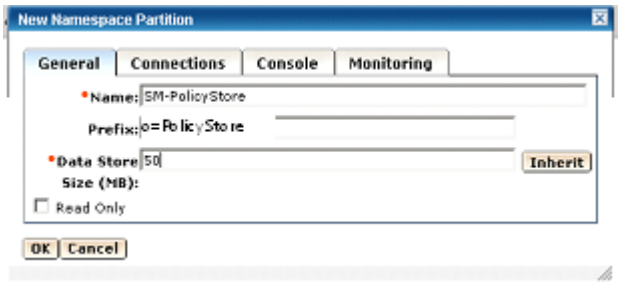
6. Click on 'Monitoring' tab and enter a port for SNMP monitoring. (e.g. 10389) This is normally the same as the LDAP port, but can be different if desired.



7. Click 'OK' and the 'Namespace' icon should now read 'root'.

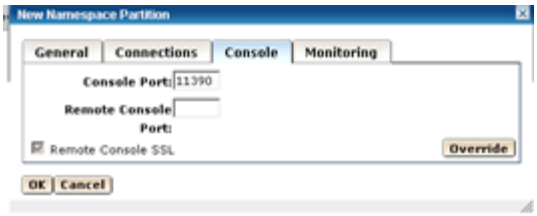


8. To create the Policy Store data namespace, right-click the 'root' icon and select 'Add a new partition'. The 'New namespace Partition' is displayed.



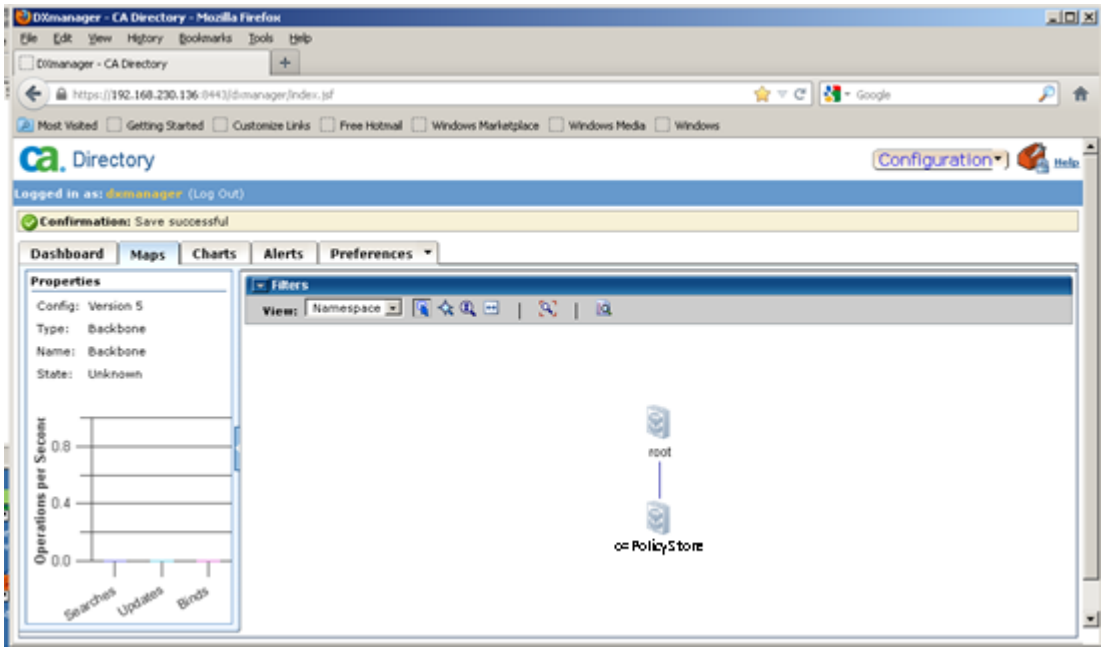
9. Fill in the fields appropriately as for the previous namespace.
    a. Enter a generic name for the Policy Store DSA namespace. (e.g. SM-PolicyStore)
    b. Enter a context prefix (i.e. start point) of the policy store DSA. (e.g. o=PolicyStore)
    c. Modify the 'Data Store' size as required, leaving the default of 500MB or click 'Override' to change the datasiore size to the appropriate sizing in MB.

10. Click on the 'Connections' tab and enter the LDAP port for the policy store data DSA. (e.g. 11389)



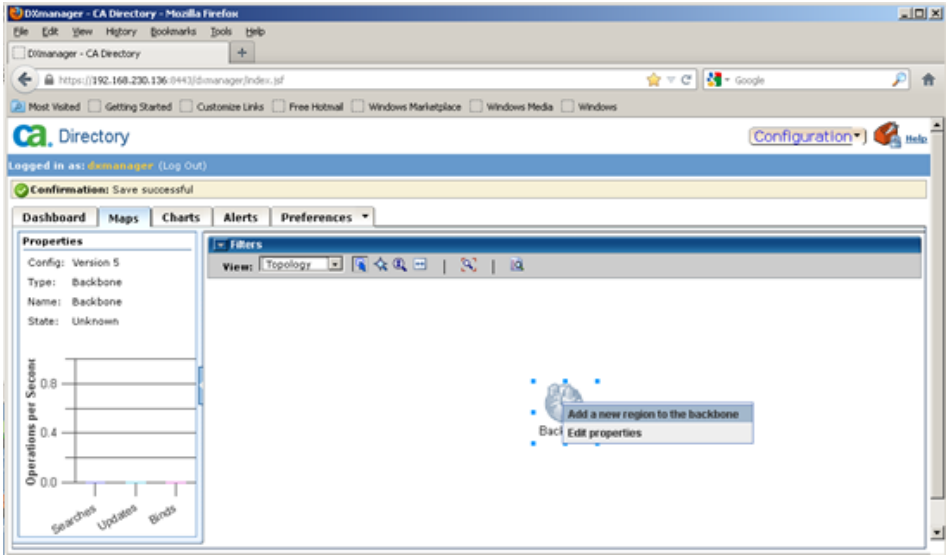
11. Click on the 'Console' tab and enter the telnet port for DSA console access. (e.g. 11390)

12. Click on 'Monitoring' tab and enter the port for SNMP monitoring. (e.g. 11389)
13. Click 'OK' and return to the 'Namespace view with both namespaces displayed. (i.e. root and o=PolicyStore)



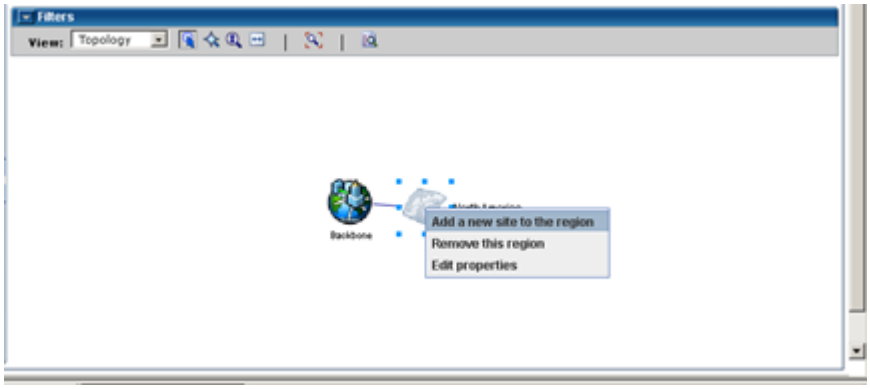
14. From the 'Namespace' view, select 'Topology' from the 'View' pulldown list. The 'Backbone' icon is displayed.

D. Define the Backbone Topology

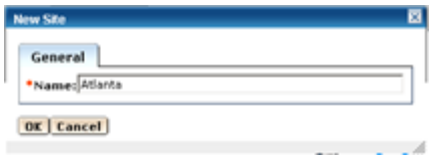


1. Right-click the 'Backbone' icon and select 'Add a new region to the backbone'. The 'New Region' pop-up appears.

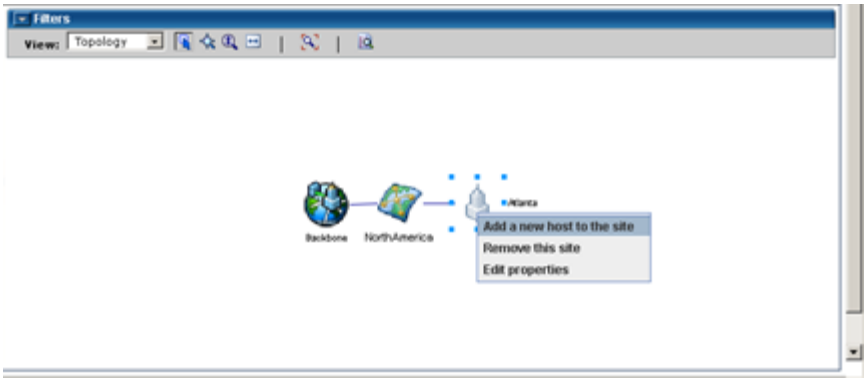
2. Enter a name for the new region. This is normally a geographical region. (e.g. NorthAmerica) Click 'OK'. The 'Region' icon is displayed along with the 'Backbone' icon.
3. Optionally, perform steps 1 and 2 for an additional region.



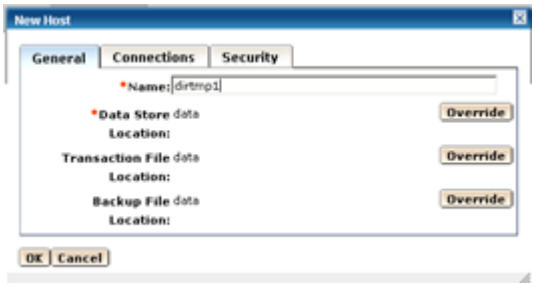
4. Right-click the 'Region' icon and select 'Add a new site to the region'. The 'new Site' pop-up appears.



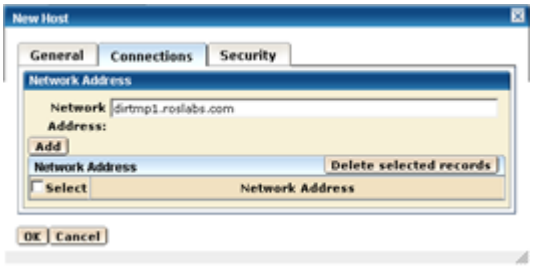
5. Enter a name for the site. This is normally a location (i.e. city, building, etc.). Click 'OK'.
6. Optionally, perform steps 4 and 5 for additional sites.



7. Right-click the 'Site' icon and select 'Add a new host to the site'. The 'new Host' pop-up appears.

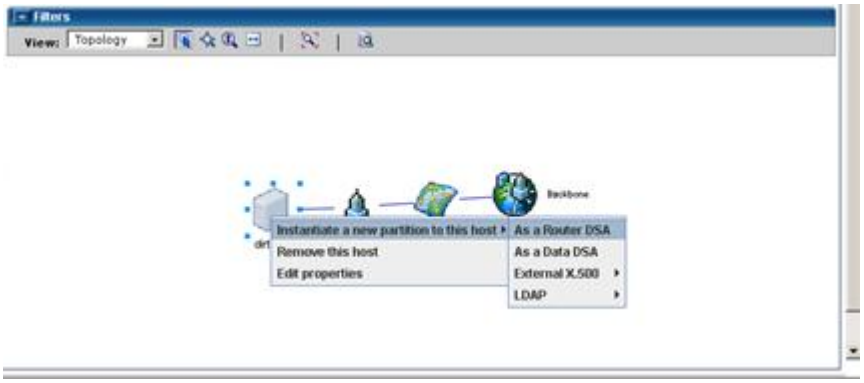


8. Enter the name of the host where the DSAs will reside in the 'Name' field. Optionally, change the locations of the datastore, transaction logfile and any backup files as appropriate with the 'Override' button.

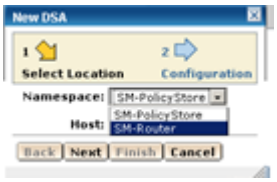


9. Click on the 'Connections' tab and enter the network address of the host in the appropriate filed and click 'Add'. Click 'OK' and the overall backbone is displayed.

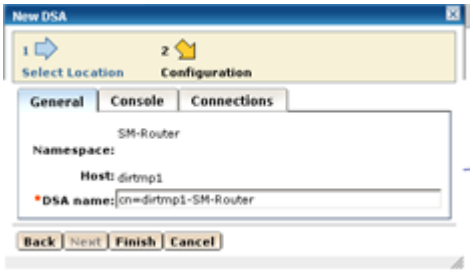
10. Optionally, perform steps 7-9 for additional hosts.



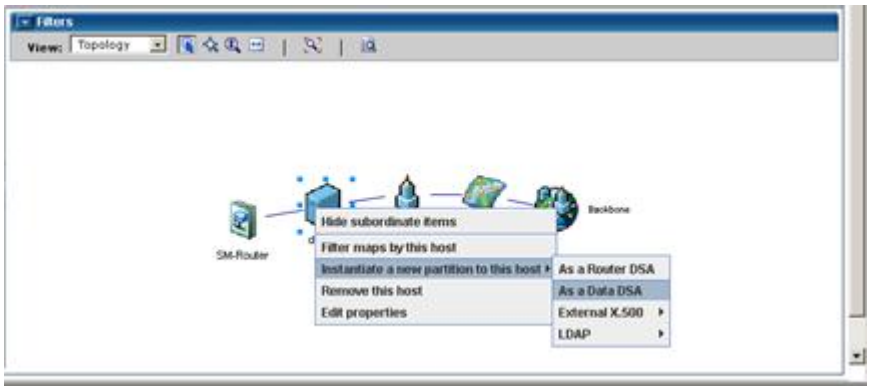
11. From the overall backbone view, right-click the 'Host' icon and select 'Instantiate a new partition to this host > As a Router DSA. The 'New DSA' pop-up appears.



12. Select the Router DSA (e.g. SM-Router) from the pull-down list.

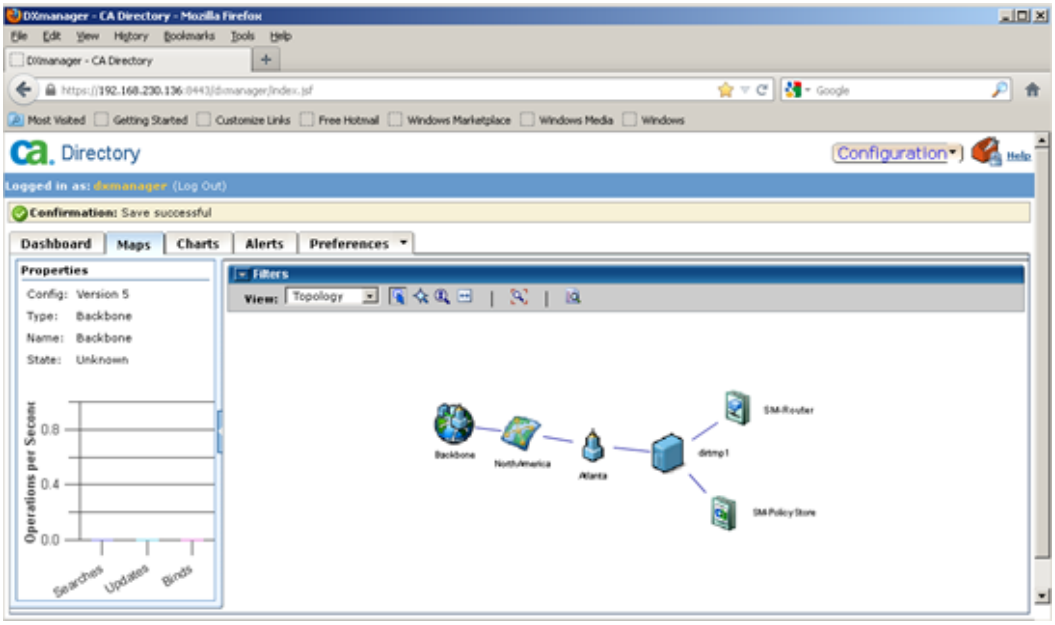


13. Select 'Finish'. The Router DSA icon is displayed.



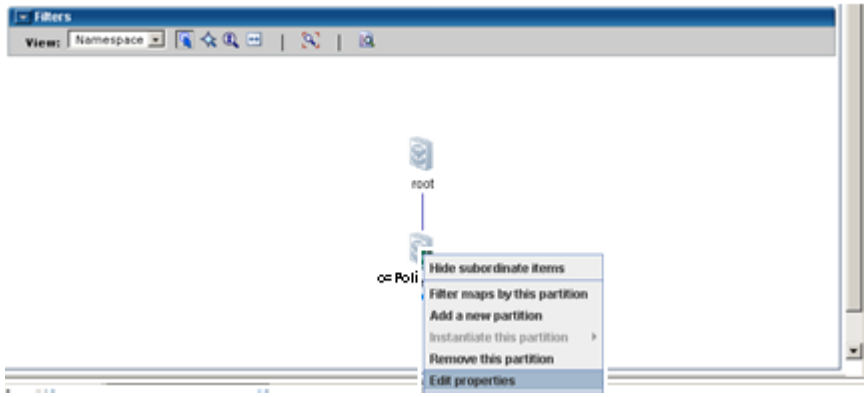
14. Again right-click the 'Host' icon, select Instantiate a new partition to this host > As a data DSA. The 'New DSA' pop-up appears.

15. Click Next, then Finish.
16. Optionally, perform steps 11-15 for configuring DSAs on additional hosts.

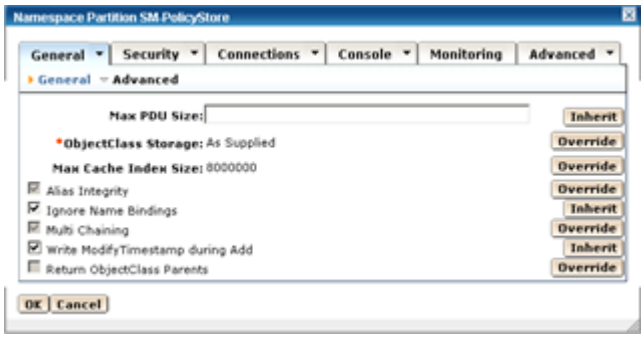


17. The completed backbone should then be displayed.

E. Refine the Configuration for Siteminder



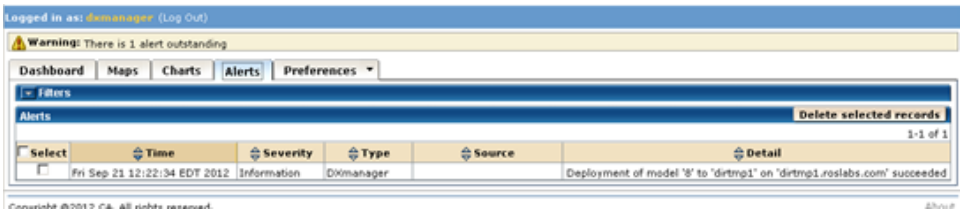
1. Return to the 'Namespace' view and select 'Edit properties' from the 'o=PolicyStore' icon. The Namespace pop-up is displayed.



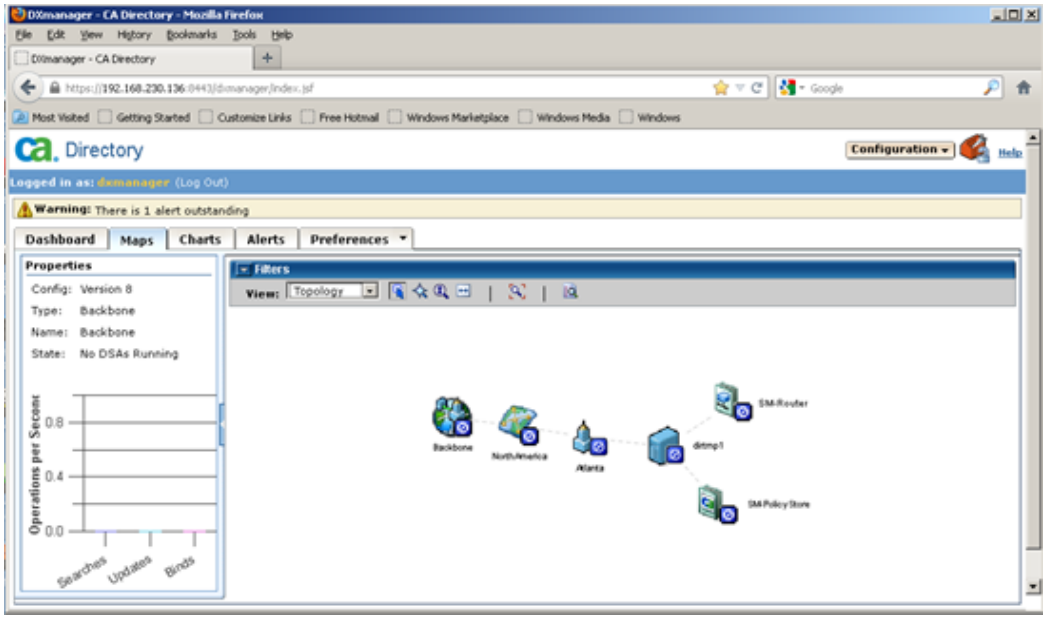
2. Check the 'Ignore Name Bindings' and 'Write Modify Timestamp during Add' checkboxes. (NOTE need to clock Override button to edited fields)
    a. 'Ignore Name Bindings' allows the SM objects to be imported in an unsorted fashion
    b. 'Write Modify Timestamp during Add' adds the modify timestamp during 'Add' operations, which Siteminder requires for policy store objects.
3. Click OK to return to the 'namespace' view

F. Deploy the configuration

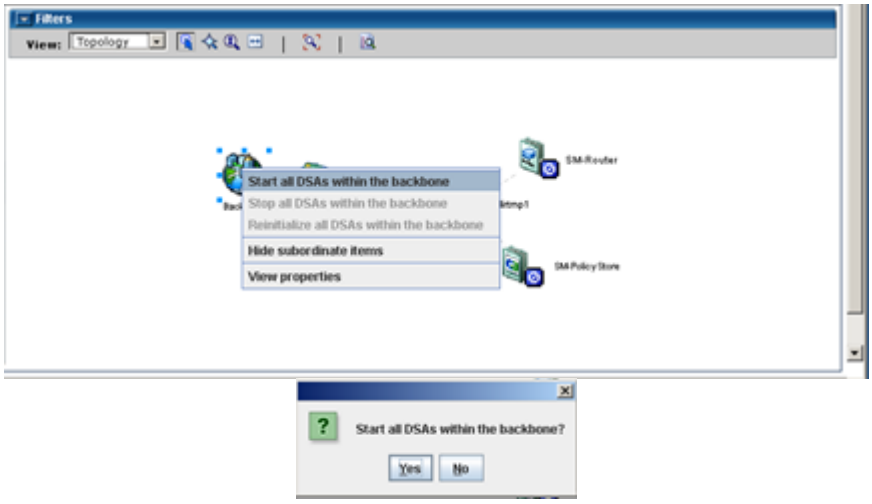
1. From the 'Configuration' menu, select 'Deploy' and enter a comment in the 'Comments' Field when prompted. (e.g. Initial SM Policy Backbone 20120921)



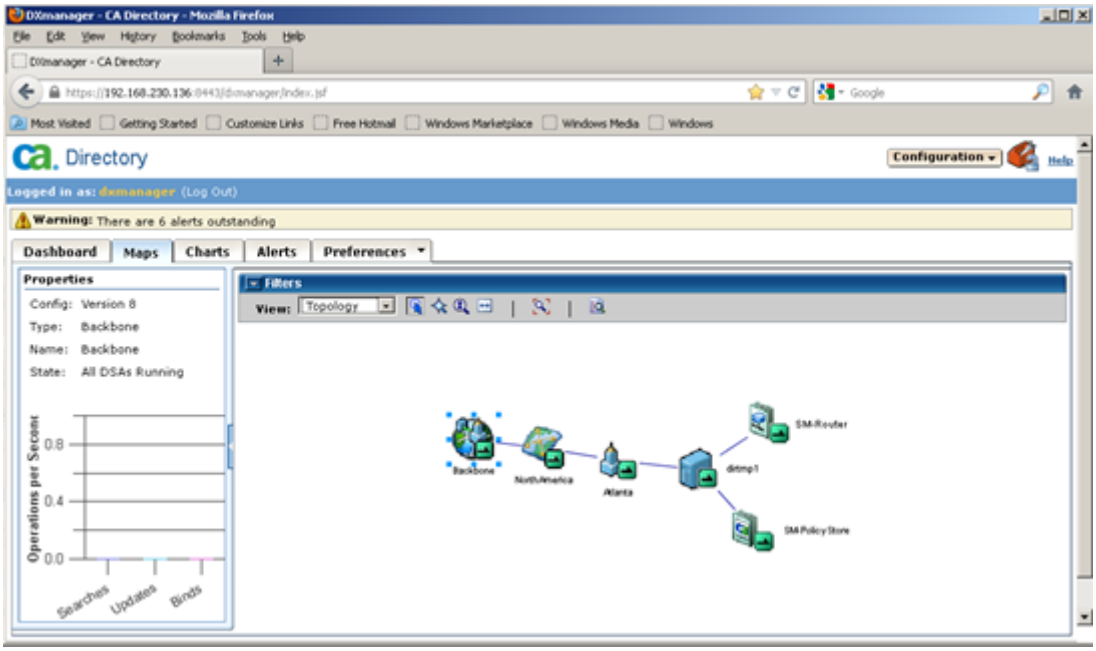
2. Check the status bar and 'Alerts' tab for deployment information.



3. The Backbone with blue indicators next to the icons is displayed upon successful deployment.



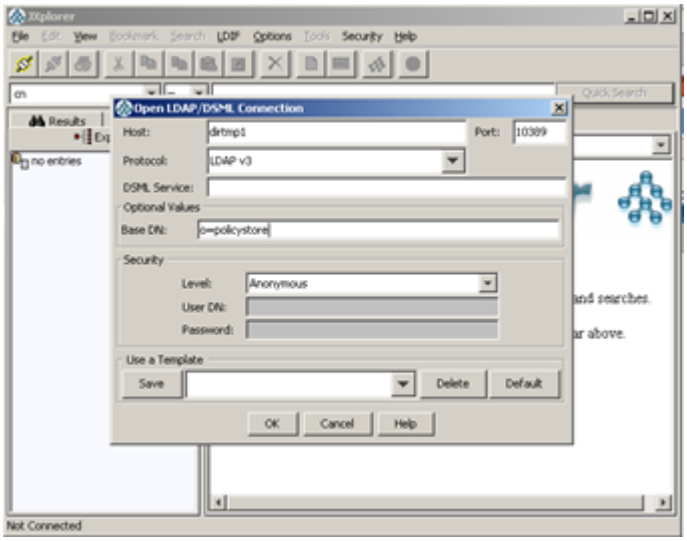
4. Right-click the ‘Backbone’ icon and select ‘Start all DSAs within the backbone’ and click ‘Yes’ at the prompt.



5. When all DSAs have started successfully, green 'lazy 1' indicators will appear next to all icons.

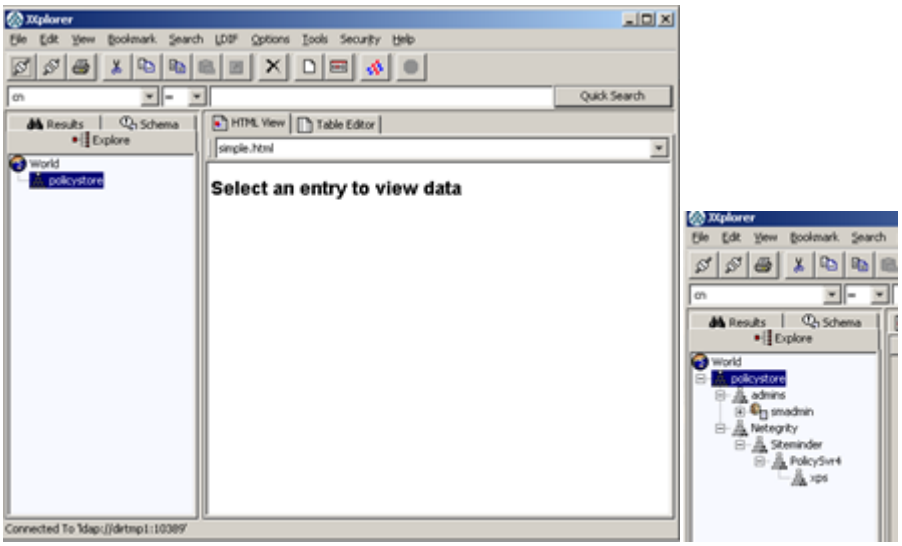
3. Build the base DIT structure

With an LDAP utility, such as JXplorer, build the initial Siteminder DIT structure as described in the Siteminder Installation guide. An example follows:



1. After JXplorer start, click the connect button at the top right corner and the connection pop-up appears.
2. Enter the appropriate information to connect to the policy store.
    a. Host of the policy store directory
    b. LDAP port of the router DSA (e.g. 10389)

c. The base DN of the policy store (e.g. o=policystore)
d. Upon initial access, use 'anonymous' access in order to build the DIT structure.



3. Build the structures:

- ou=xps,ou=PolicySvr4,ou=SiteMinder,ou=Netegrity,o=PolicyStore (For policy store objects)

4. Create the ADMIN account:

Be sure that the administrator is of object type inetOrgPerson.
Take note of the administrator DN and password. You use these credentials when pointing the Policy Server to the policy store.

- Example:
- ou=admins,o=policystore (For the SM policy store user – e.g. cn=smadmin,ou=admins,o=policystore)

4. Complete the Policy Store Directory configuration

To complete the configuration, add the Siteminder schema and appropriate access controls so only the SM user may access the policy store. (NOTE: If all traffic/connections go to router DSA changes need to be made to all router DSA's and Data DSA's)

A. Policy Store schema

1. Copy the policy store schema file as directed in the Siteminder Installation guide to the CA Directory schema configuration location.

- Two files from the policy server: *siteminder_home*\eTrust\netegirty.dxc & *siteminder_home*\xps\db\etrust.dxc to
  i. unix/linux - $DXHOME/config/schema
  ii. windows - %DXHOME%\config\schema

2. Copy the dxmanager.dxg file in the schema location to a new name and ensure it is write enabled. (e.g. pstoreSchema.dxg)
3. Add the Siteminder schema file to the new .dxg files
   e.g.

```
# CA Directory - DXserver/config/schema
#
# This is a the default group file for schema for servers
created
# by DXmanager. As these setting become available in future
releases
# they will be removed from here.
#

source "x500.dxc";
source "cosine.dxc";
source "umich.dxc";
source "inetop.dxc";
source "dxserver.dxc";

#Siteminder schema
source "netegrity.dxc";
source "etrust.dxc";
```

4. Edit the DSA startup files (*.dxi) in the servers configuration location for the new schema file to load.
   a. unix/linux - $DXHOME/coonfig/servers
   b. windows - %DXHOME\config\servers

   Note: The filenames will be the same as the DSA names as seen with the 'dxserver status' command with '.dxi' extensions. – NOTE: Changes to Router and Data DSA's (SM-PolicyStore-smserver.dxi & SM-Router-smserver.dxi)

```
dxserver status
SM-PolicyStore-dirtmp1 started
SM-Router-dirtmp1 started
```

Example .dxi file for new schema

```
clear schema;
#source "../schema/dxmanager.dxg";
source "../schema/pstoreSchema.dxc";

# access controls
clear access;
source "../access/dxmanager.dxc";

# logging and tracing
# operational settings
# service limits
# ssl
# knowledge
clear dsas;
source "../dsaconfig.xml";
```

B. Define access controls

To secure the policy store DSA, add an access control for the Siteminder user, which will automatically lock out any other users.

1. In the access control location, copy the dxmanager.dxc file to another name and ensure it is write enabled. (e.g. pstoreAccess.dxc)
2. Modify the contents to let the SM user be the superuser, which is higher access than admin user. Since the SM user is the only account to access the policy store, it can also be the superuser.

Example access control file

```
# Computer Associates
#
# config/access/rackaccess.dxc ($Revision: 1.0.0 $)
#
# The following security configuration files should be
loaded
# to support the web single sign sign on of Canon's B2C
project.
#
# 20120919 - created

clear access;

# static access controls
set access-controls = true;
# set access-controls = false;

# dynamic access controls
set dynamic-access-control = false;

        #
        # Setting super-user status to Roles subtree
        #
set super-user = {
user = <o policystore><ou "admins"><cn smadmin>
};
```

3. Edit the DSA startup files (*.dxi) in the servers configuration location for the new schema file to load, as previously described for schema.

Example of final DSA startup files (.dxi)

```
# CA DXserver
#
# Initialization file written by DXmanager
#

# schema
clear schema;
#source "../schema/dxmanager.dxg";
source "../schema/pstoreSchema.dxc";

# access controls
clear access;
```

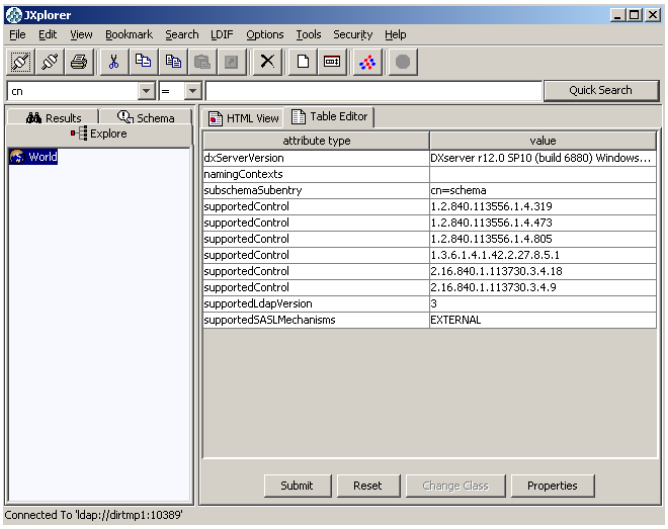
```
#source "../access/dxmanager.dxc";
source "../access/pstoreAccess.dxc";

# logging and tracing
# operational settings
# service limits
# ssl
# knowledge
clear dsas;
source "../dsaconfig.xml";
```

4. Enter 'dxsyntax' at the command line level to ensure no syntactical errors are present in the configuration file. (No output means all is well.)

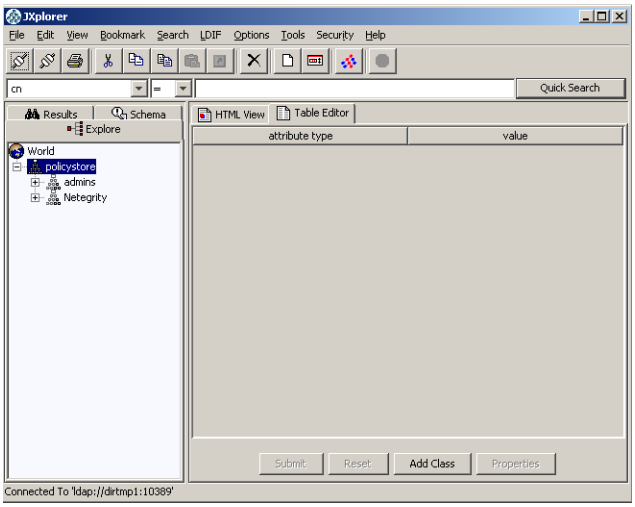
C. Restart the DSAs

Restart the DSAs to pick up the SM schema and access controls.

1. After logging in to DXmanager, right-click the Backbone icon and select 'Stop all DSAs'. Confirm at the pop-up.
2. Again, right-click the 'Backbone' icon and select 'Start all DSAs…' and confirm at the pop-up.



3. Login with anonymous access should result in no access to the policy store

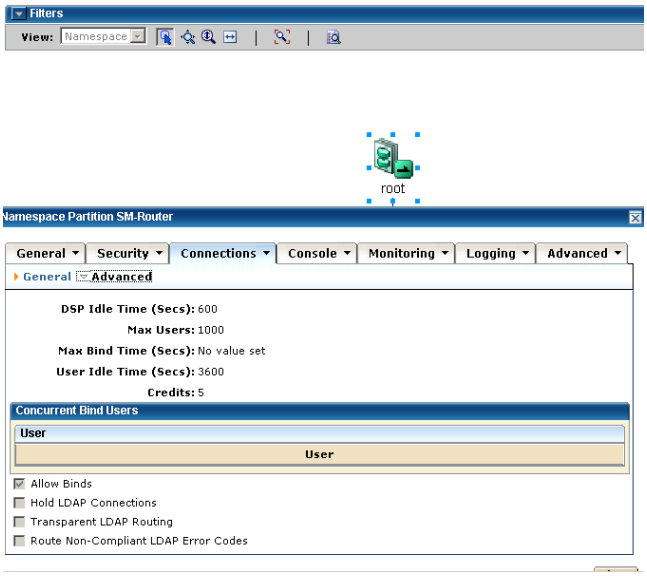


4. Login again with the respective SM user and the DIT should be accessible. Note, a test update operation can be performed using an LDAP GUI or command line. (e.g. modify the description of the SM user entry)

5. SiteMinder Specific changes

Need to make the changes for both root and o=PolicyStore (Namespace in DX Manager)

- Configuration – Edit mode
- Namespace right click “root” then “View properties”
- Click Connections/Advanced – Change max Users from 255 to 1000 (NOTE Make same change to o=PolicyStore branch)
- No Changes need for `max-op-size or max-local-ops`



6. End of Policy Store setup with Dxmanager

The policy store directory is now ready to accept Siteminder objects.

Please refer to the Siteminder guides for further activities.

- smreg -su <password for super user>l
- XPSDDInstall "c:\program files\ca\siteminder\xps\dd\SmMaster.xdd"
- XPSImport "c:\program files\ca\siteminder\db\smpolicy.xml" -npass

7. Troubleshooting

CA Directory comes with a configuration and log gathering tool.

DXINFO: The command is the same regardless of Operating System:

NOTE: On UNIX/Linux run this as 'dsa' user.

```
c:\scripts>dxinfo -x logs
Collecting DXinfo Version
Collecting Operating System Version
Collecting Windows User Environment Variables
Collecting DXserver Home
Collecting DXserver Version
Collecting DXwebserver Tomcat Version
Collecting Registry Data
Collecting DXserver Config
Collecting Additional Custom Files
------------------------------------------------------------
-----------
The following files have been created:

cadir_dxinfo.log
cadir_config.cab
Please attach them to your CA support issue for analysis.
```

DX manager get exported (unencrypted) dsaconfig.xml to view knowledge.

'dxinfo' does not capture 'dsaconfig.xml' file.