One CA Plaza Islandia, NY 11749 T +1 631 342 6000 F +1 631 342 6800 ca.com

June 20, 2013



Customer Request Number: System/Application: Module: Request Classification: Versions:

18 June 2013

N/A Policy Server Siteminder Policy Store with DXmanager Technical Note SiteMinder Policy Serve R12.5 & above CA Directory r12.0 SP11 (build 7065) CA DXManager 12.0.7066 Manager Description

Setup and Configure the Siteminder Policy Store with Dxmanager

Author

Stephen McQuiggan

Disclaimer

Version Date

0.1

Copyright © 2006 CA, Inc. All rights reserved.

CA products and associated documentation are protected by copyright and are distributed under a licensing agreement. CA, Inc. has prepared this document for use by CA, Inc. employees, licensees, and customers. No part of this document may be reproduced, translated, or transmitted in any form or by any means, electronic, mechanical, photocopying, optical magnetic, or otherwise, without prior written permission from CA, Inc. CA, Inc. reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications.

This product contains encryption technology. Exporting these encryption algorithms to certain countries may be prohibited or restricted by the laws of the United States.

Some portions of the code are licensed from RSA Data Security, Inc.

SiteMinder and eTrust are U.S. registered trademarks of CA, Inc. and the SiteMinder and CA logos are trademarks of CA, Inc.

All other trademarks or registered trademarks mentioned in this document are the property of their respective owners.

CA, INC. SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERROR OR OMISSION CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE PERFORMANCE OR USE OF THIS MATERIAL.

TABLE OF CONTENTS

Contents



1
2
2
3
3
5
8
. 13
. 16
. 17
. 19
. 20
. 20
. 22
. 23
. 24
. 25
. 25

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

😊 DXmanager - CA Directory - Mozilla Firefox	x III x
Die Edit View Higtory goolmarks Jock Belp Welcome to Pirefox × Divinanager - CA Directory × +	
(←)	☆ = C 🛃 - Google 🔎 🏦
🙆 Most Visited 📋 Getting Started 🔛 Customice Links 🔛 Free Hotmal 💭 Windows Marketplace	Windows Media 🔲 Windows
CA D User Nam Passwor Copyright ©2012 CA. All rights reserved.	irectory e: dumanager d: . Log In

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



OXmanager - CA Directory - Mozilla Firefox	
Ele Edt Yew History Bookmarks Isols Help	
Welcome to Firefox COMmanager - CA Directory	× +
A https://192.168.230.136-0443/domanager/backboneChoice.jsf	☆ マ C 🚼 - Google 👂 🎓
Pree Hotmal Windows Market	place 🗌 Windows Media 🔛 Windows
Ca. Directory	🥰 Hele
Logged in as: dumanager (Log Out)	
Backbone types	Cancel
Backbone types	
Single DSA Backbone Wizard which creates a Backbone with one Namespace Partition, one Region, one Site, one Host and one Data DSA.	
Advanced Enter Advanced configuration mode. Recommended for experienced users.	
Import a configuration file that you have exported from DXmanager.	
	Cancel
Copyright @2012 CA. All rights reserved.	About
https://192.168.230.136:8443/Documentation/html/index.htm?toc.htm?domanager.htm	

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



3. Always trust content from this publisher

Do y	ou want t	to run this	application?			
	0	Names	hiddenApplet			
	1	Publisher:	UNENOWN			
		From:	https://192.168.230.136-8	0443		
	personal info Hore Inform	ormation at risk. I ation	Run this application only if y	ou trust the p	ubisher.	
Selec	personal info Hore Inform t the box be	ormation at risk. I ation low, then click	Run this application only if y	ou trust the p	ublisher.	

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



🕴 DXmanager - CA Directory - Mc	uzilla Firefox		
Ele Edit Yew Higtory Bookm	arks Iools Help		
Welcome to Firefax	COmanager - CA Directory × +		
https://192.168.230.136.0	H3jd:manager;backboneChoice.jsf	습 🔻 😋 🛃 - Google	<u> </u>
A Most Visited 🗌 Getting Started	Custonize Links 🔄 Pree Histmal 🔄 Windows Marketplace 📄 Windows Media 📄 Window	\$	
Ca. Directory		Configurati	on 🗸 🍕 Helo
ogged in as: demanager (Los	(Out)		
Dashboard Maps Ch	arts Alerts Preferences *		
Properties	💌 fitters		
Config: Version 0	View: Namespace 🗉 💽 🛠 🔍 😁 🕺 🖄		
Type: Backbone			
Name: Backbone			
State: Unknown			
. <u> </u>			
5.0.8			
2 Second) j		
8			
e 0.4	Namespace		
2			
5 0.0 L	-		
100 100 - 100			
Stran Aborn Bru			
Conversionly (\$2001.0. Co., All clother res-	anad		dhout .

5. The 'Namespace' icon will be displayed.

B. Define the Backbone defaults

🔁 DXmanager - CA Directory - Mozilla	Firefox		LO X
Ele Edit Yew History Bookmarks	Toop Rep		
Dilmanager - CA Directory	+		
(https://192.168.230.136-0443/s	imanager, Index, Jsf	👷 🗸 😋 🚮 - Google	۶ 👂
🖉 Most Visited 🗌 Getting Started 🗌 🤅	Customize Links 🛄 Pree Histmail 🛄 Windows Marketplace 📄 Windows Media 📄 Windows		
Ca. Directory		(Configuration 🗸 🎉 Help
Logged in as: dxmanager (Log Ou	0		
Dashboard Maps Charts	Alerts Preferences -		
Properties	T Filters		
Config: Version 0	View: Topology 💌 💽 🛠 🔍 😁 🛛 🚫 🛛		
Type: Backbone			
Name: Backbone			
State: Unknown			
*			
5 0.8	675		
N N			
e e	Backbone		
6 U.4			
60.0 <u> </u>			
13105 13105 5005			
98° - 190 - 0			_
	·		
Coovright @2012 CA, All rights reserve	id,		About

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.



1	🖂 Filters	
I	View: Topology 💌 🙀 🛠 🔍 🖂 🕺 🖄	
I		
I		
I		
l		
J		
]		
1	Add a new region to the backbone	
1	Backbo tidit properties	
ł		
ł		
I		٣
1		
1	ji	1

2. Select 'Edit properties'

General	• DX	admind	Securi	y •	Monitoria	ng *	Console	•	Connectio	ns *	Logging	•	Advanced	
uenera	, Nov	anceo						_				_		_
	D-at	a Store S	ize (MB):	500										
	Da	ta Store I	location:	data										
	Transac	tion File I	Location:	data										
	Bac	kup File I	Location:	data										
	Ma	x Operati	on Time:	600						1				
	N.	ax Operat	ion Size:	10000						1				
Enable	Persister	t Search												
Dusy Fo	or Referr	al												
Derefe	rence Alia	is on Bind												
Z Automa	tically St	419												

3. The 'Backbone Defaults' pop-up is displayed

1	Backbone Defaults
	General * DXadmind Security * Monitoring * Console * Connections * Logging * Advanced * Port:[2123 Password: Confirm Password: Trap Port:[20162
	DXmanager Host
	DXmanager Host
	192.168.230.136
	OK Cancel

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



	General * DXadmind Security * Monitoring * Console * Connections * Logging * Advanced
	General > SSL > Password Policy > Advanced
	*SSL Encryption: Off
	Password Storage: sho-1
	Anonymous
ļ	Clear Password
	SSL
	Force Encrypt Anon
	Force Encrypt Auth
P	Enable Password Policy

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.



General > Tracing > Advanced Time Log Search Threshold:	
Time Log Search Threshold:	
Time Log Update Threshold:	
Rollover Alarm Log	
Enable Summary Log	
Enable Stats Log	
Enable Trace Log	
Rollover Trace Log	
Enable Query Log	
Enable Update Log	
Show Values in Update Log	
Enable Alert Log	
Enable Cert Log	
Enable Connect Log	
Fanble Disa Los	
 rushe mail mail 	

- 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

🍪 DXmanager - CA Directory - Mozilla I	Firefax		
Bie Edit View Higtory Bookmarks	Jools Help		
😫 Welcome to Firefax	X Ditmanager - CA Directory X +		
A https://192.168.230.136/0443/de	manager/backbone/hoice.jsF	습 코 😋 🛃 - Google .	P 🕈
🔎 Most Visited 🗌 Getting Started 🗌 O	ustonize Links 🔄 Pree Hotmal 🔄 Windows Marketplace 📄 Windows Media 📄 Windows 👘		
Ca. Directory		Configuration -	a Helo
Logged in as: demanager (Log Out)			
Dashboard Maps Charts	Alerts Preferences *		
Properties	Filters		
Config: Version 0 Type: Backbone Name: Backbone State: Unknown	View: Namespace 🖃 💽 🛠 🔍 🖂 🕅		
0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	S Namespace		
Copyright @2012 CA. All rights reserved	4.		About:

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.



<pre>e Ext teget teget teget teget teget teget</pre>	DXmanager - CA Directory - Mozil	la Firefox			_101
webcome to Firefax X Interce [1192_160_220_126_644]]d=manager_BaddoreChoice.jd Interce for X Not Voted Outcombe Links	e Edit Yew History Bookmark	s Jools Help			
Protection Protection Properties Propertie	Welcome to Firefax	× Ditimanager - CA Directory	× +		
Not Vuited Gutting Rated Customize Links Pree Histmal Windows Marketplace Windows pred in ass: demonstrater (Log Out) Dashbaard Maps Charts Alerts Preferences Properties Configuration Interespace Interespace Properties Configuration Interespace Properties Views: Namespace Namespace Interproperties Views: Namespace Interproperties	https://192.168.230.136:0443	(dimanager,backbone/Choice.)sf		습 🔻 😋 🛃 - Google	P 1
Configuration Co	Most Visited Getting Started	Customize Links 📄 Pree Hotmail 📄 Windows M	tarletplace 🗌 Windows Media 🗌 Window	6	
properties Config: Version 0 Type: Backbone Name: Backbone State: Unknown 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	a Directory				Configuration - 🍕 Melo
Dashbaard Mags Charts Alerts Preferences Properties Config: Version 0 Type: Backbone State: Unknown Undot updot updot State: Unknown State: Un	<mark>gged in as: demanager</mark> (Log O	ut)			
Properties Config: Version 0 Type: Backbone Name: Backbone State: Unknown 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	Dashboard Mans Chart	Alerts Preferences *			
Config: Version 0 Type: Backbone Name: Backbone State: Unknown 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	Properties				
Type: Backbone Name: Backbone State: Unknown	Config: Version 0	View: Namespace 💌 💽 🔆 🔍	⊟ <u>%</u> ⊠		
Name: Backbone State: Unknown 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	Type: Backbone				
State: Unknown	Name: Backbone				
Add a new partition Namespace	State: Unknown				
Add a new partition Namespace					
Add a new partition Namespace add a new partition Namespace	5 0.8	.[1.2.1		
Namespace Namespace		J,	Add a new pa	vition	
egeneration of the second of t	804		Namespace		
South Secure Secured.	ation]			
como un como como como como como como como com	be	1			
call d'all de la calla de la c	0.0	1			
pyright 62012 CA. All rights reserved.	and a section and steps				
pyright @2012 CA. All rights reserved. About	ê	1			
	ouright @2012 CA. All rights reser	ved.			About

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

General	Connections	Console	Monitoring	
•Na	me: SM-Router			
Pre	fix:			
Data St	ore 0			Taba
Size (h	48):			Inne
- next or	de la			

- 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).

w Namesp	vace Partition			
General	Connections	Console	Monitoring	
	•Port: 1038	9		

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

General	Connections	Console	Monitoring	
Co	nsole Porti 1039	0		
Remo	te Console			
	Port			
Remote	Console SSL			Overrie



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.

General	Connections	Console	Monitoring	
	SNMP Port: 1038	त्र		

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.

🔮 DXmanager - CA Directory - Mozilla Firefox		
Ele Edit Yew Higtory Bookmarks Ipols Help		
Swelcome to Firefox × Dismanager - CA Directory × +		
(a https://192.168.230.136/0443/domanager/backboneChoice.jsf	合 🔻 😋 🛃 • Google	۶ 🎓
Anst Visted Getting Started Customize Links Pree Histmal Windows Marletplace Windows Media Windows		
Ca, Directory	Co	nfiguration 🚽 🍕 Helo ⁺
Logged in as: finmanager (Log Out)		
Dashboard Maps Charts Alerts Preferences *		
Properties Filters		
Config: Version 0 View: Namespace 🖃 💽 🔆 🔍 😁 💸 🔯		
Type: Backbone		
Name: Backbone		
State: Unknown		
š T		
§ 0.8		
1 2		
2 0.4 root		
0.0 <u></u>		
and the day		
Selace Above Bur		
Copyright @2012 CA. All rights reserved.		About

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



DXmanager - CA Directory - Mozil	a Firefox				
jie Edit Yew Higtory Bookmark	Iools Help				
Welcome to Firefax	× Dismanager - CA Directory	× +			
https://192.168.230.136-0443	dimanager/backbone/Choice.jsf		승 🔻 😋 🛃 - Google	P	1
Most Visited Getting Started	Customize Links 🔅 Pree Hotmal 🔅 Windows M	arketplace 🗌 Windows Media 🗌 Windows			
Ca. Directory				Configuration +	telp
i <mark>gged in as: dxmanager</mark> (Log O	<i>R</i>)				
Dashboard Maps Chart	s Alerts Preferences *				
Properties	💌 Filters				٦
Config: Version 0	View: Namespace 💌 💽 🔩 🔍	3 X B			
Type: Partition					
Name: SM-Router					
State: Unknown					
20 P					
8.0.8	*	C29a			
ž	1	Idea subor	dinate items		
£ 0.4		Party Source	anate nems		
atio		 Add a new 	this partition b		
be		Demon the	in partition		
0.0		Edit remove to	is partition		
200 . 100		contraction of the second			
Sunce About Bu					
					_
spyright @2012 CA. All rights reser	ed.			Abs	out

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.

General	Connections Console Monitoring	
*Na	me: SM-PolicyStore	
Pre	fix: o=PolicyStore	
Data S	are 50	Tabasi
Size (N	(B):	Inter
Read Or	de	

- 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)
 - 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.

New Namespa	ce Partition			×
General	Connections	Console	Monitoring	
	• Port: 11389			
OK Cance	I			

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

General	Connections	Console	Monitoring	
Co	nsole Porti 1139	0		
Remo	te Console			
	Port			
Remote	Console SSL			Overri



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)

🔁 DXmanager - CA Directory - Mozilla	Firefox		LID X
Elle Edit Yew Higtory Bookmarks	Jools Help		
Dilmanager - CA Directory	+		
🗧 🔶 🗎 https://192.168.230.136-0443/d	manager/index.jsf	👷 🔻 😋 🛃 - Google	P 🕇
🔎 Most Visited 🗌 Getting Started 🗌 🤇	ustonize Links 📋 Free Hotmail 🛄 Windows Marketplace 📄 Windows Media 📄 Windows		
Ca. Directory		(Configuration*)	telo -
Logged in as: demanager (Log Out			
Confirmation: Save successful			
Dashboard Maps Charts	Alerts Preferences *		
Properties	Filters		
Config: Version 5	View: Namespace		
Type: Backbone			
Name: Backbone			
State: Unknown			
	8		
	reat		
be			
£ 0.4	3		
1 10			
8 _{0.0}	c≃ Policystone		
Searcher Updater Binos			-

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.

New Region	8
General	
*Name: NorthAmerica	

- 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.

💌 Filters	
View: Topology 🖃 💽 🛠 🔍 🖂 🔀 🔯	
Backtone NortVAmerica Add a new host to the site Remove this site Edit properties	
	-
	•

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

General Connections Security	
Name: dirtmp1	
*Data Store data	Overr
Location:	
Transaction File data	Overr
Location:	
Backup File data	Overr
Location:	

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.

General	Connections	Security	
Network Ad	dress		
Address Add	k dirtmp1.roslabs s:	L.com	
Network A	ddress		Delete selected records
Select		Networ	Address

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.



	New DSA	×
	1 🖒 2 🖄 Select Location Configuration	
New DSA	General Console Connections	
1 2 D	SM-PolicyStore Namespace:	
Namespace: SM-PolicyStore Host: dirtmp1	Host: dirtmp1 DSA name: cn=dirtmp1-SM-PolicyStore,o=Siteminder	
Back Next Finish Cancel	Back Next Finish Cancel	

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

🔮 DXmanager - CA Directory - Mozilla Firefox	ad a
Bie Edit Yew History Bookmarks Isols Help	
Dilmanager - CA Directory +	
(a https://192.160.230.136-0441/dowarager/index.jsf	👷 🛡 🤁 - Google 🖉 🎓
Nost Visited Getting Started Customize Links Free Hotmal Windows Marketplace Windows Media Win	kows
Ca. Directory	(Configuration*) 🕰 া 🗠
Logged in as: demanager (Log Out)	
Confirmation: Save successful	
Dashboard Maps Charts Alerts Preferences *	
Properties - Filters	
Config: Version 5 View: Topology 🗉 💽 🛠 🔍 😁 😒 🔍	
Type: Backbone	
Name: Backbone	
State: Unknown	
	dstrap1 BM Policy Bore
1000 1000	-
Contraction of the second seco	_ _

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

Co	nfiguration -	🔗 Hels			
	New				
	Edit				
0	Close		Save Configuration		×
6	Save		·= Required		
	Revert		*Comment:		
	Deploy	_			
	Import				OF Course
()	Export Version				UK Cancel

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

pgged in as: dominister (Log Out)					
warning: There is 1 alert outstanding					
Dashboard Maps Charts Alerts Preferences *					
I Filters					
Alerts Delete selected records					
				1-1 of 1	
□ Select 🗘 🗘 Time	Severity	😂 Type	Source	🕀 Detail	
Fri Sep 21 12:22:34 EDT 2012	Information	DXmanager		Deployment of model '8' to 'dirtmp1' on 'dirtmp1.roslabs.com' succeeded	

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



🍪 DXmanager - CA Directory - Mozilla i	irefox	
Bie Edit View Higtory Bookmarks	Jook 1980	
Dilmanager - CA Directory	+	
https://192.168.230.136-0443/de	manager/index.jsf 👷 🕫 🕅 🛃 - Google	۶
Most Visited Getting Started O	stonize Links 🔄 Pree Hotmail 🛄 Windows Marketplace 📃 Windows Media 🔛 Windows	
Ca. Directory	Configura	ation 🗸 🍕 Help 🕇
Logged in as: domanager (Log Out)		
A warning: There is 1 alert outstan	ống	
Dashboard Maps Charts	Alerts Preferences *	
Properties	- Filters	
Config: Version 8	View: Topology	
Type: Backbone		
Name: Backbone		
2008	Bosbori Bosbori Bosbori Atera Atera BarbicyBove	_
Gener Upr. tr		

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.



😌 DXmanager - CA Directory - Mozilla	Tirefox	
Ele Edit Yew Higtory Bookmarks	Jook Help	
Dilmanager - CA Directory	+	
E https://192.168.230.136-0443/d	manager/index.jsf 🦙 🐨 😭 🚮 - Google	P 🔒
Most Visited Getting Started C	stonize Links 📋 Free Histmal 📋 Windows Marletplace 📄 Windows Media 📄 Windows	
Ca. Directory		Configuration - 🍕 Help
Logged in as: dxmanager (Log Out		
Awarning: There are 6 alerts outs	anding	
Dashboard Maps Charts	Alerts Preferences *	
Properties	I Filters	
Config: Version 8	View: Topology 💌 💽 🛠 🔍 😁 📔 🔀 📔 🔯	
Type: Backbone		
State: All DSAs Running		
0.0 Oberations Second	SM-Royter Backbore North-West/s Alarts SM Poley Bore	-

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:

🐼 Xiplorer		
Blo Edit Yew (Sodimark. Search LDBF Options Tools Security Help	
5 5 5		
on		Quick Search
Al out of	Open LDAP/DSML Connection	
• Eq	Host: dronp1 Port: 10309	
C no entries	Protocol: LDAP v3	
	DSML Service:	1 A 1
	Optional Values	649
	Base DN: 0=policystore	
	Security Level: Anorymous User DN: Password:	and searches. ar above.
	Use a Template	
	Save Delete Default	
	OK Cancel Help	
Not Connected	×	¥

- 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
```

```
# 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";
#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-dirtmpl started
SM-Router-dirtmpl 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.

🛞 JXplorer			_ 🗆 🗙
Eile Edit View Bookmark Search	h LDIF Options Tools Security Help		
Ø \$ 6 \$ 6			
cn 💌 = 💌			Quick Search
👪 Results 🔍 Schema	HTML View Table Editor		
- E Explore	attribute type	va	ue
😘 World	dxServerVersion	DXserver r12.0 SP10 (b	uild 6880) Windows
	namingContexts		
	subschemaSubentry	cn=schema	
	supportedControl	1.2.840.113556.1.4.31	19
	supportedControl	1.2.840.113556.1.4.47	73
	supportedControl	1.2.840.113556.1.4.80)5
	supportedControl	1.3.6.1.4.1.42.2.27.8.	5.1
	supportedControl	2.16.840.1.113730.3.4	l.18
	supportedControl	2.16.840.1.113730.3.4	1.9
	supportedLdapVersion	3	
	supportedSASLMechanisms	EXTERNAL	
	SubmitC	Thange Class	perties
Connected To 'ldap://dirtmp1:10389'			

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



🐼 JXplorer		
Eile Edit Yiew Bookmark Sear	th LDIF Options Iools Security Help	
🖉 🖉 🎒 👗 🖻 🖻		
cn 💌 =	3	Quick Search
👪 Results 🔍 🖓 Schema	HTML View 🗋 Table Editor	
Explore	attribute type	value
E the polystore ⊕ ∰ admins ⊕ ∰ Netegrity		
	Submit Reset	Add Class Properties
Connected To 'ldap://dirtmp1:10389'	J [

 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.

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

Please attach them to your CA support issue for analysis.

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

