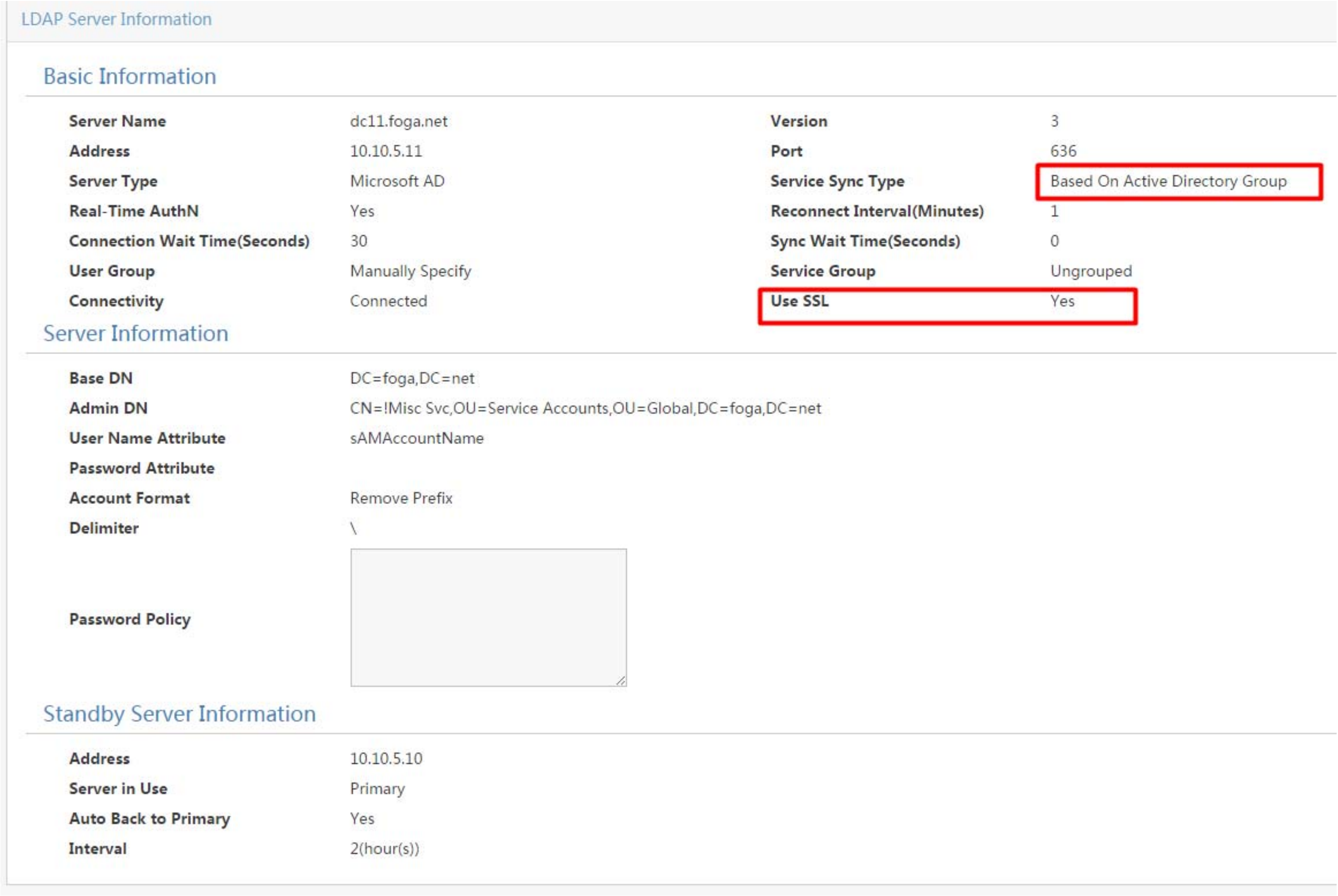
LDAP setup for IMC

Enter information for domain controller



LDAP Server Information

Basic Information

Server Name	dc11.foga.net	Version	3
Address	10.10.5.11	Port	636
Server Type	Microsoft AD	Service Sync Type	Based On Active Directory Group
Real-Time AuthN	Yes	Reconnect Interval(Minutes)	1
Connection Wait Time(Seconds)	30	Sync Wait Time(Seconds)	0
User Group	Manually Specify	Service Group	Ungrouped
Connectivity	Connected	Use SSL	Yes

Server Information

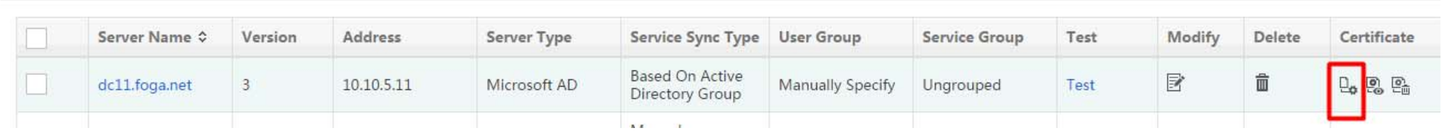
Base DN	DC=foga,DC=net
Admin DN	CN=!Misc Svc,OU=Service Accounts,OU=Global,DC=foga,DC=net
User Name Attribute	sAMAccountName
Password Attribute	
Account Format	Remove Prefix
Delimiter	\
Password Policy	

Standby Server Information

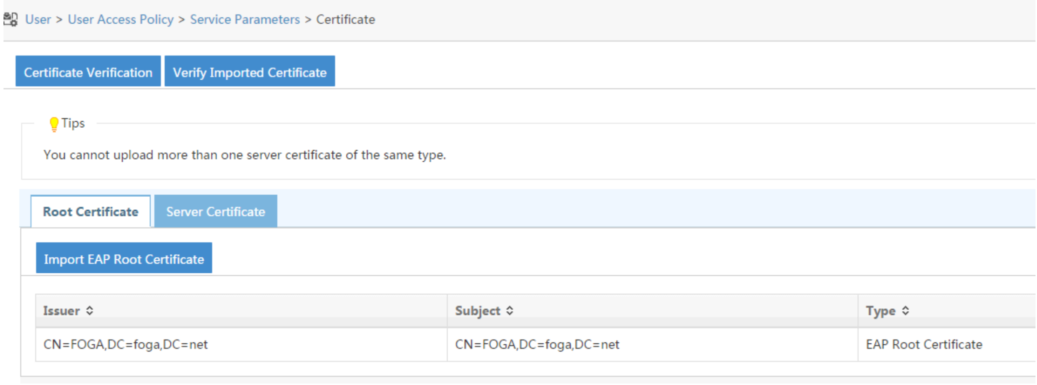
Address	10.10.5.10
Server in Use	Primary
Auto Back to Primary	Yes
Interval	2(hour(s))

Set base DN and provide access account information. I chose service sync type based on AD group so I could use AD to determine access service assignment to users.

To start use SSL OFF – then test the configuration. Then import SSL root certificate to match Base DN



□	Server Name ⇕	Version	Address	Server Type	Service Sync Type	User Group	Service Group	Test	Modify	Delete	Certificate
□	dc11.foga.net	3	10.10.5.11	Microsoft AD	Based On Active Directory Group	Manually Specify	Ungrouped	Test			

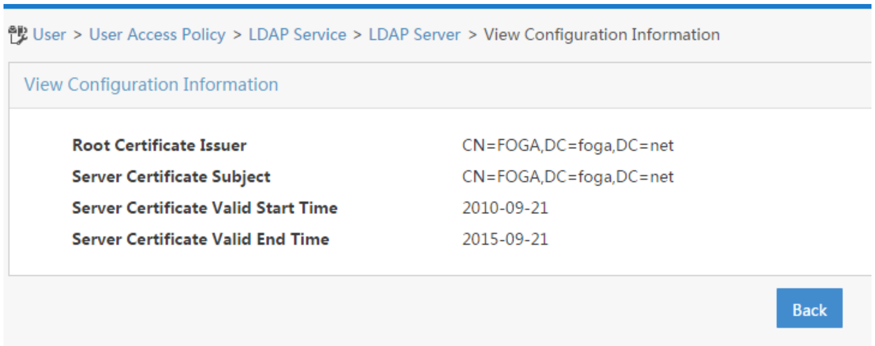


User > User Access Policy > Service Parameters > Certificate

Tips

You cannot upload more than one server certificate of the same type.

Issuer ⇕	Subject ⇕	Type ⇕
CN=FOGA,DC=foga,DC=net	CN=FOGA,DC=foga,DC=net	EAP Root Certificate

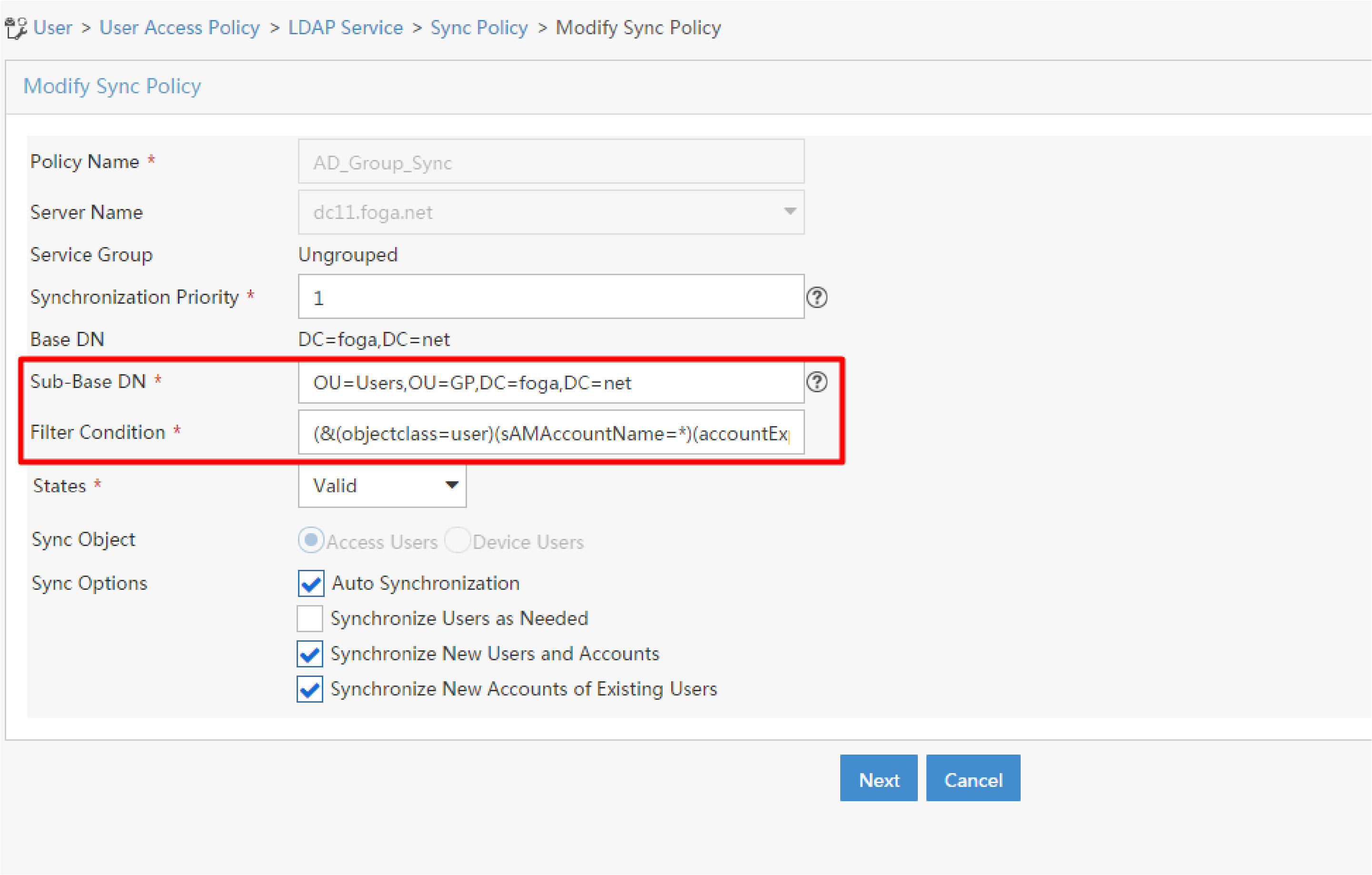

User > User Access Policy > LDAP Service > LDAP Server > View Configuration Information
Back

View Configuration Information

Root Certificate Issuer	CN=FOGA,DC=foga,DC=net
Server Certificate Subject	CN=FOGA,DC=foga,DC=net
Server Certificate Valid Start Time	2010-09-21
Server Certificate Valid End Time	2015-09-21

Then check SSL On and test again. This will help isolate certificate problem from other issues

Configure Sync Policy


User > User Access Policy > LDAP Service > Sync Policy > Modify Sync Policy
Next
Cancel

Modify Sync Policy

Policy Name *	AD_Group_Sync
Server Name	dc11.foga.net
Service Group	Ungrouped
Synchronization Priority *	1
Base DN	DC=foga,DC=net
Sub-Base DN *	OU=Users,OU=GP,DC=foga,DC=net
Filter Condition *	(&(objectclass=user)(sAMAccountName=*)(accountEx
States *	Valid
Sync Object	● Access Users ○ Device Users
Sync Options	☑ Auto Synchronization ☐ Synchronize Users as Needed ☑ Synchronize New Users and Accounts ☑ Synchronize New Accounts of Existing Users

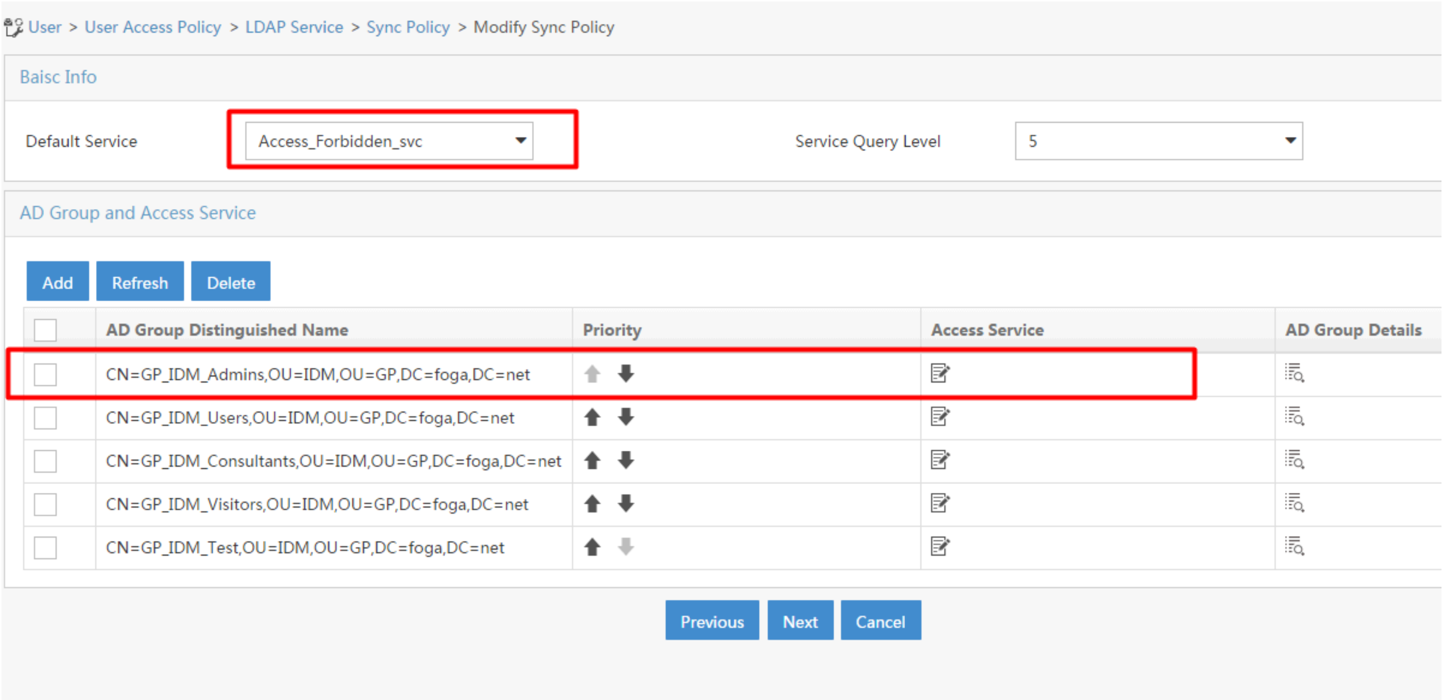
Specify sub base DN to start where users will be synched from. Create separate synch polices to access other parts of tree.

Filters can also be applied to users – you can test this in AD utility. Use ADSI edit to view parameters for users. I added userAccountControl value to filter only enabled users.

(&(objectclass=user)(sAMAccountName=*)(accountExpires>=now)(userAccountControl=512))

I tried Synchronize users as needed but this didn't work reliably with the AD group synch – without using AD groups it works fine.

Next add the synch policies to use



User > User Access Policy > LDAP Service > Sync Policy > Modify Sync Policy

Baisc Info

Default Service: Access_Forbidden_svc

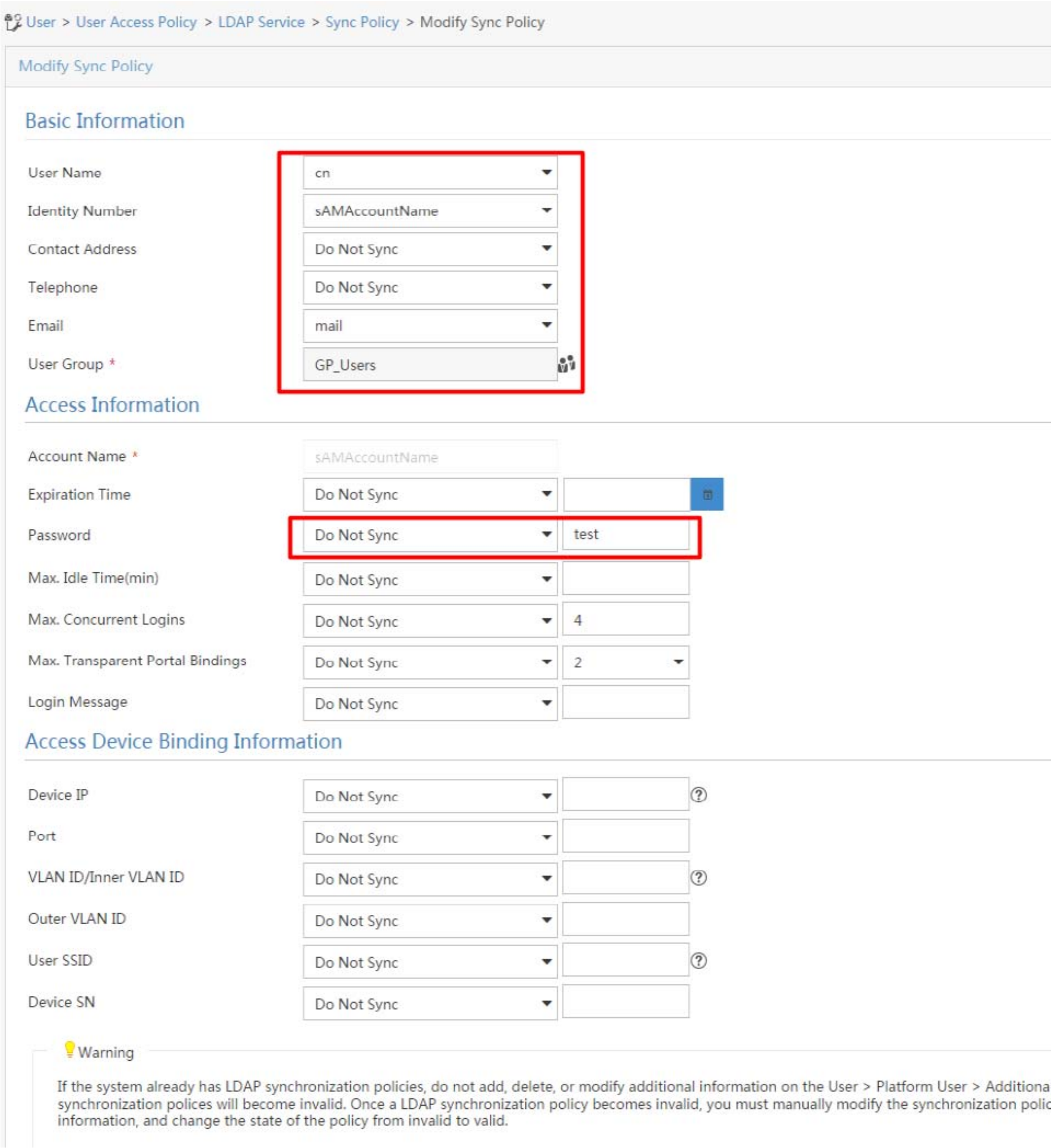
Service Query Level: 5

AD Group and Access Service

□	AD Group Distinguished Name	Priority	Access Service	AD Group Details
□	CN=GP_IDM_Admins,OU=IDM,OU=GP,DC=foga,DC=net	↑ ↓	✎	🔍
□	CN=GP_IDM_Users,OU=IDM,OU=GP,DC=foga,DC=net	↑ ↓	✎	🔍
□	CN=GP_IDM_Consultants,OU=IDM,OU=GP,DC=foga,DC=net	↑ ↓	✎	🔍
□	CN=GP_IDM_Visitors,OU=IDM,OU=GP,DC=foga,DC=net	↑ ↓	✎	🔍
□	CN=GP_IDM_Test,OU=IDM,OU=GP,DC=foga,DC=net	↑ ↓	✎	🔍

Specify default service and then add the LDAP DN info for groups and assign access service for each group.

Then specify how to synch info from AD



User > User Access Policy > LDAP Service > Sync Policy > Modify Sync Policy

Modify Sync Policy

Basic Information

User Name	cn
Identity Number	sAMAccountName
Contact Address	Do Not Sync
Telephone	Do Not Sync
Email	mail
User Group *	GP_Users

Access Information

Account Name *	sAMAccountName	
Expiration Time	Do Not Sync	
Password	Do Not Sync	test
Max. Idle Time(min)	Do Not Sync	
Max. Concurrent Logins	Do Not Sync	4
Max. Transparent Portal Bindings	Do Not Sync	2
Login Message	Do Not Sync	

Access Device Binding Information

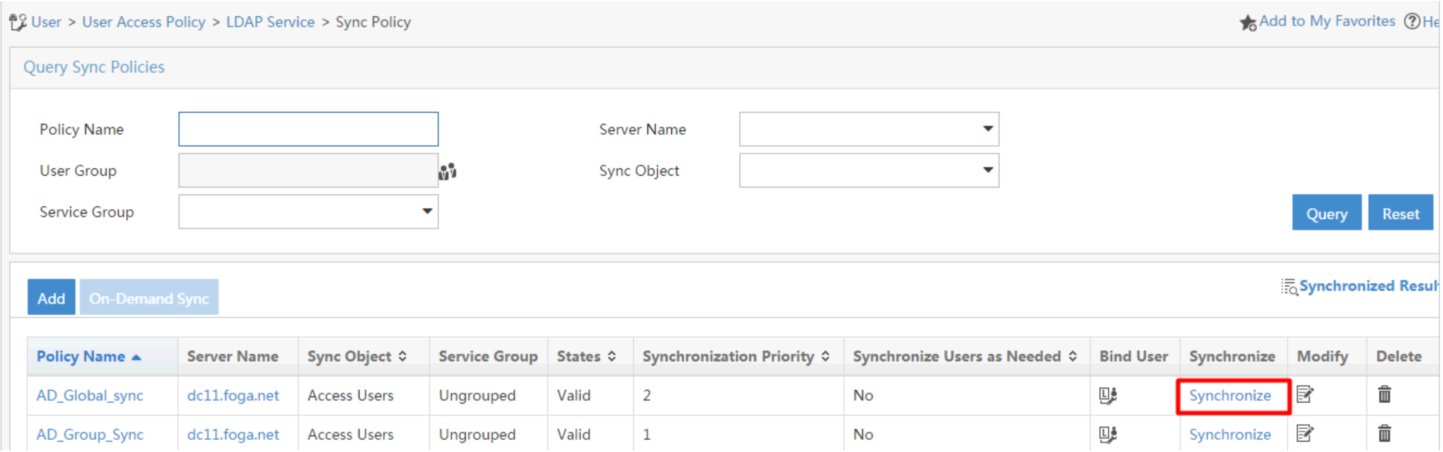
Device IP	Do Not Sync	
Port	Do Not Sync	
VLAN ID/Inner VLAN ID	Do Not Sync	
Outer VLAN ID	Do Not Sync	
User SSID	Do Not Sync	
Device SN	Do Not Sync	

Warning

If the system already has LDAP synchronization policies, do not add, delete, or modify additional information on the User > Platform User > Additiona synchronization polices will become invalid. Once a LDAP synchronization policy becomes invalid, you must manually modify the synchronization polic information, and change the state of the policy from invalid to valid.

Apply a destination user group. For some reason not all values synch properly. A dummy password is required, but not used.

Now you can synchronize and see results. If errors occur there is a download log file link



Policy Name

User Group

Service Group

Server Name

Sync Object

Policy Name ▲	Server Name	Sync Object ⇕	Service Group	States ⇕	Synchronization Priority ⇕	Synchronize Users as Needed ⇕	Bind User	Synchronize	Modify	Delete
AD_Global_sync	dc11.foga.net	Access Users	Ungrouped	Valid	2	No		Synchronize		
AD_Group_Sync	dc11.foga.net	Access Users	Ungrouped	Valid	1	No		Synchronize		