SANGFOR

IAM

Password-based authentication with AD

Version 12.0.18

Change Log

Date	Change Description
Aug 2, 2019	Version 12.0.18 document release.

CONTENT

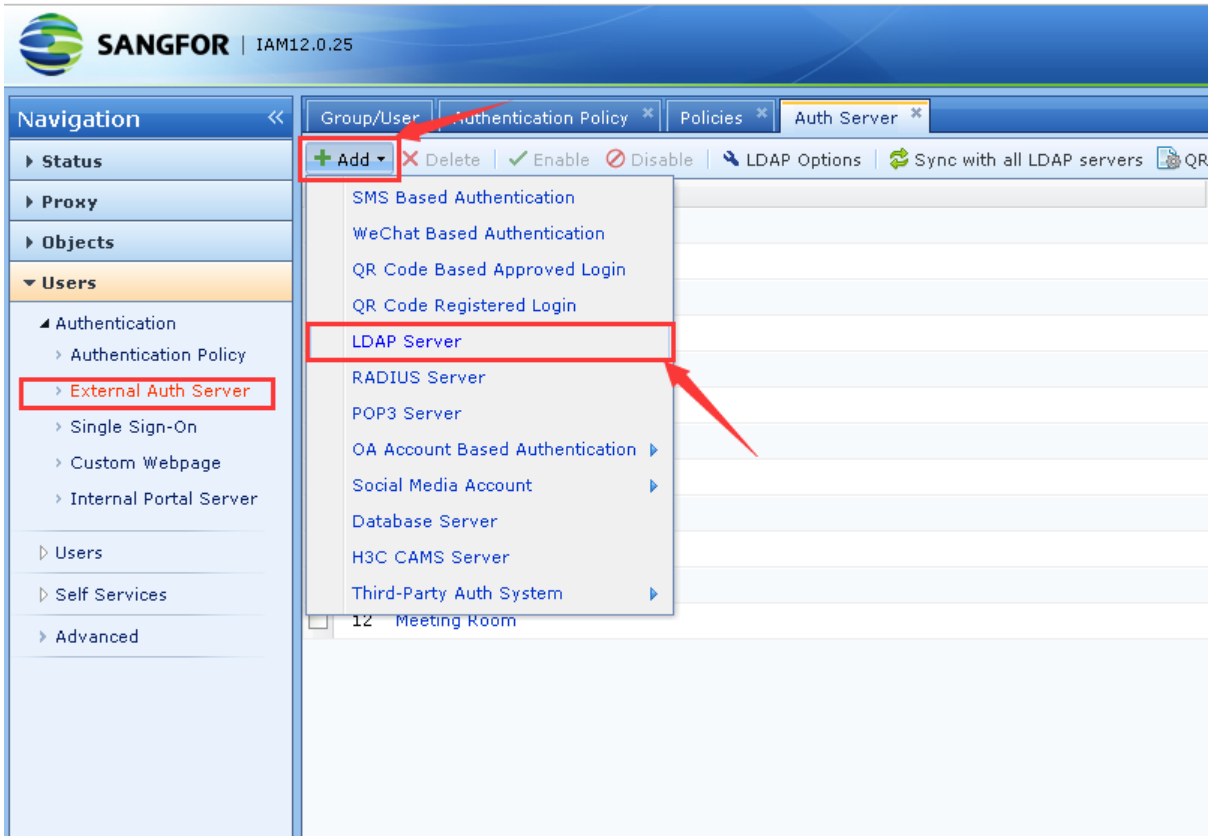
Chapter 1 Content requirement

1. IAM device, PC, and AD domain server.
2. Deploy all the network environment, make sure all the devices and AD domain server can connect to IAM.

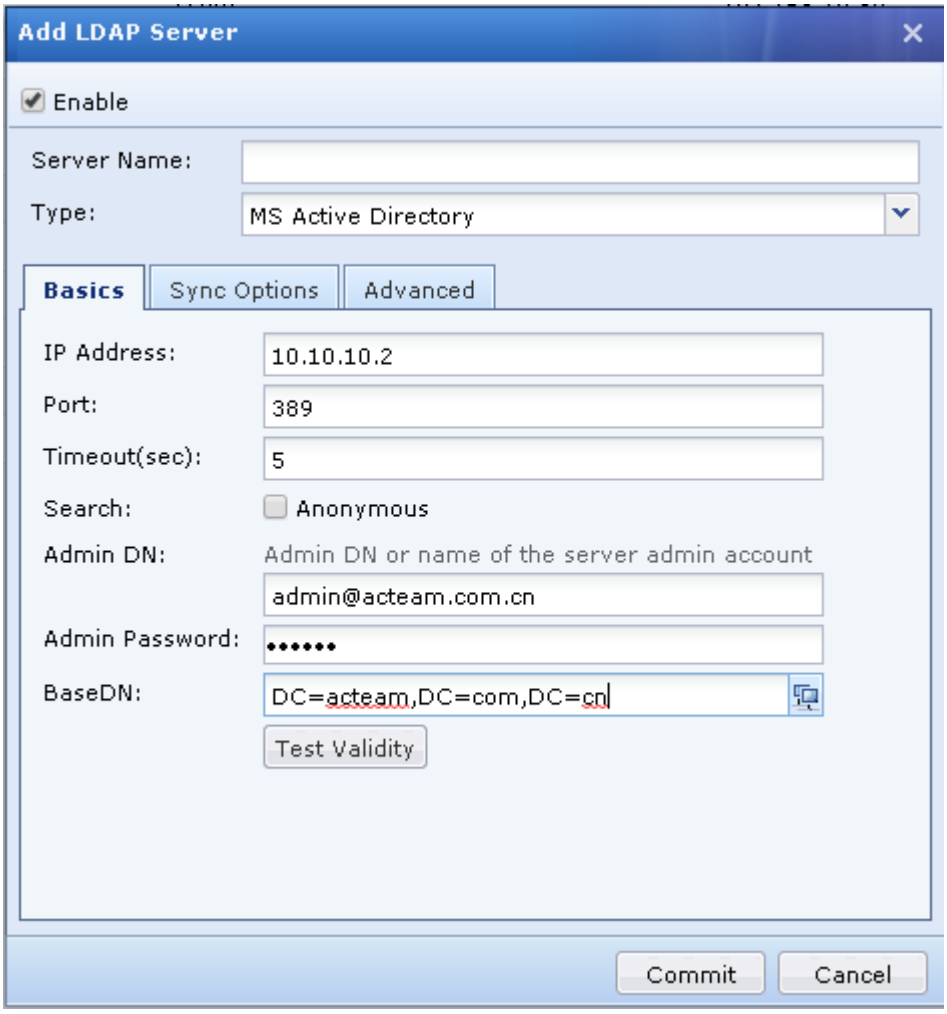
Chapter 2 Configuration and Snap shot

2.1 LDAP Configuration

1. Edit (User) > (External Auth Server) > (Add) > (LDAP Server)



2. Configure LDAP server information



(IPaddress): Ip address of LDAP server.

(Authentication port): Port which connected to LDAP server, for example, AD domain is 389.

(Time out): Set the timeout period of the authentication request. After the system forwards the authentication request to the LDAP server, if there is no response after this time, the authentication is considered to be invalid. If the network between the device and the LDAP server is slow, you can try Set the timeout to be larger (for example, 10 seconds).

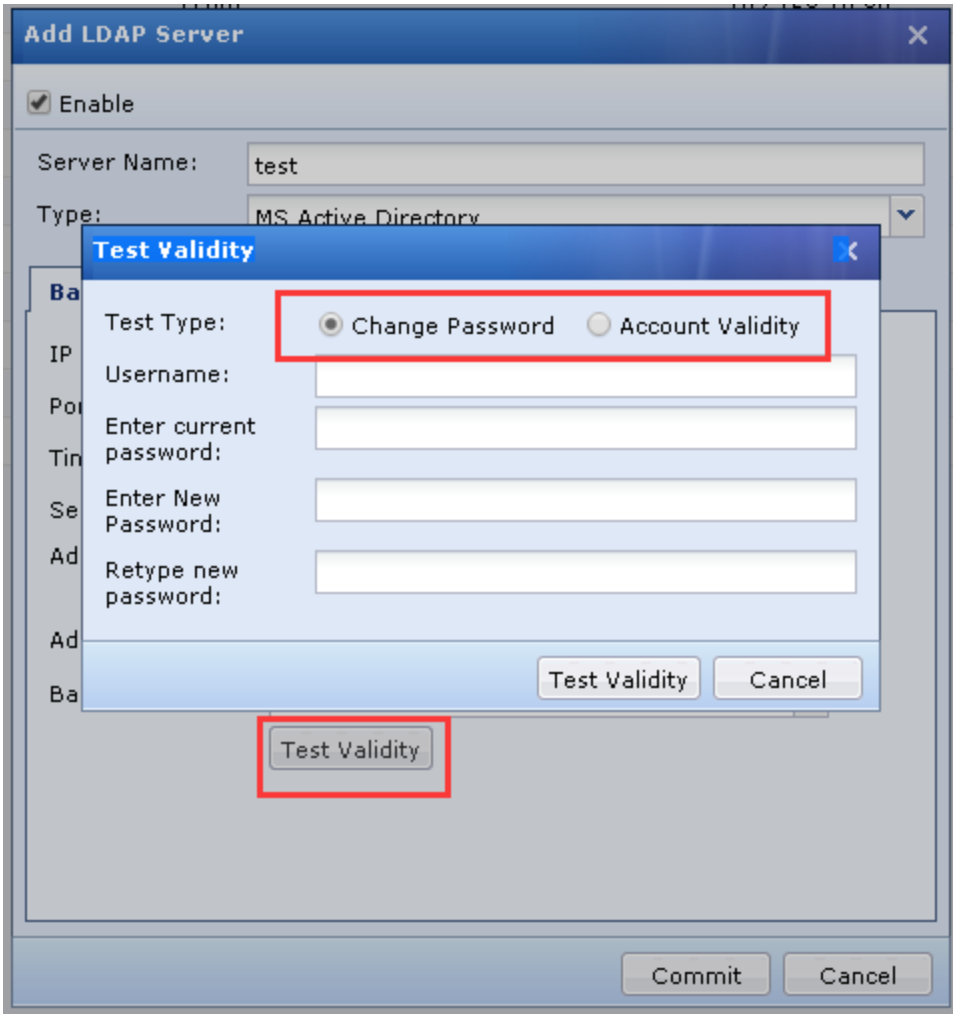
(Search): This option is available when the LDAP server supports anonymous search.

(Admin DN): User account used for querying and synchronizing to the LDAP server; for example, the account is: administrator, the domain name is sangfor.com, then the format is: username@domain, administrator@sangfor.com.cn

(Admin Password): The password corresponding to the user who is used to bind the server.

(BaseDN): Specify the starting point of the domain search path, which determines the effective scope of the LDAP rule. If the user is outside the specified BaseDN, the user cannot be authenticated by the external server, and the configured policy will not take effect for the user. Therefore, you can use BaseDN to divide the area of different administrators.

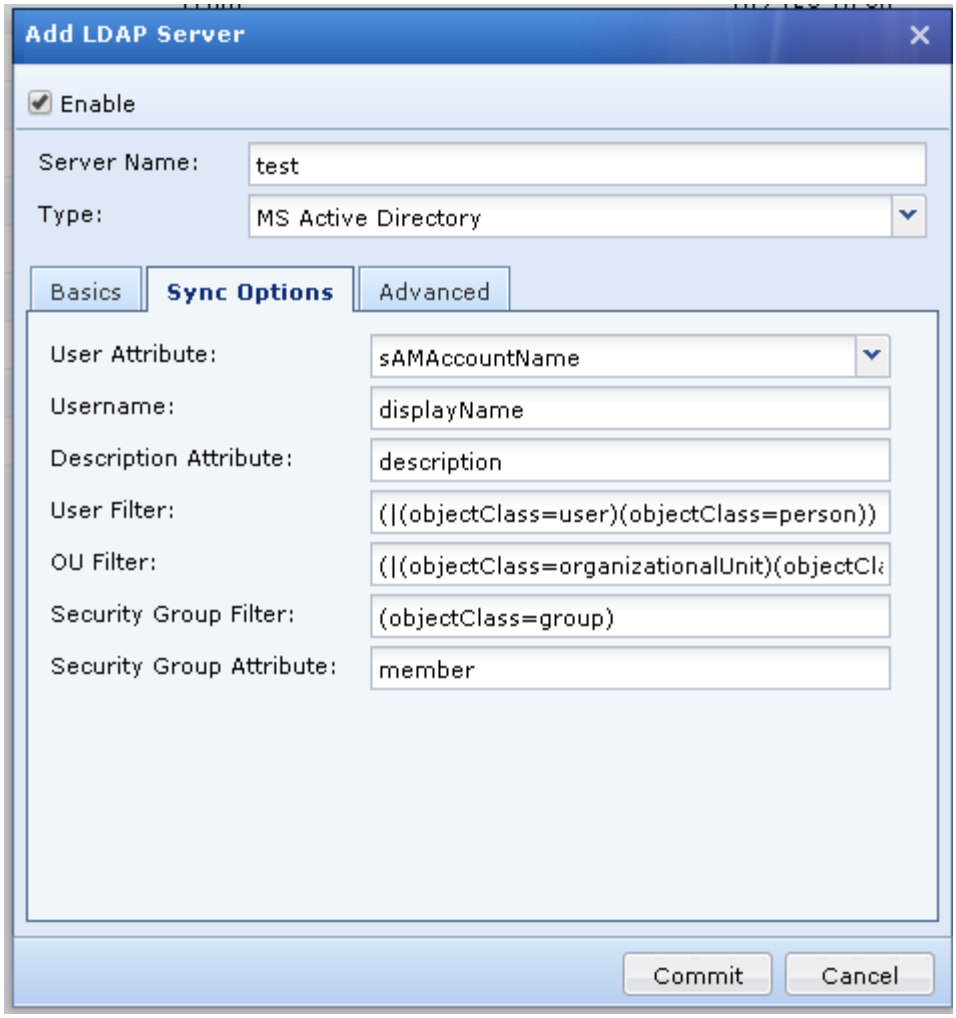
3. Test validity (test validity)



(Change Password): AD domain account If you select the first time authentication to change the password, then you can change the password directly here.

(Account Validity): Tests whether the AC device can communicate directly with the AD domain and verify that the account is valid.

Edit(sync options)（If there is no special requirement, it is not recommended to edit and modify, keep the default.）



(User Attribute): Specifies the attribute field on the LDAP server that uniquely identifies the user. For example, the sAMAccountName attribute on the AD domain identifies the user, and on the Novell LDAP, the uid attribute identifies the user.

(Username): Specifies the attribute field on the LDAP server that uniquely identifies the user display name. For example, the displayName attribute on the AD domain identifies the user's display name.

(Description Attribute): Specifies the attribute field on the LDAP server that uniquely identifies the user description. For example, the description attribute on the AD domain identifies the user's description.

(User Filter): Specifies the user filtering condition of the LDAP server. That is, you can determine whether a node is a user. For example, you can filter whether a node is a user by filling in "(|(objectClass=user)(objectClass=person))" .

(OU Filter): Specifies the organizational unit filter condition of the LDAP server, that is, whether the node can be an organizational unit by using this condition. For example, the AD domain can be filled in by "(|(objectClass=organizationalUnit)(objectClass=organization)(objectClass=domain)(objectClass =domainDNS)(objectClass=container))" to filter whether a node is an organizational unit.

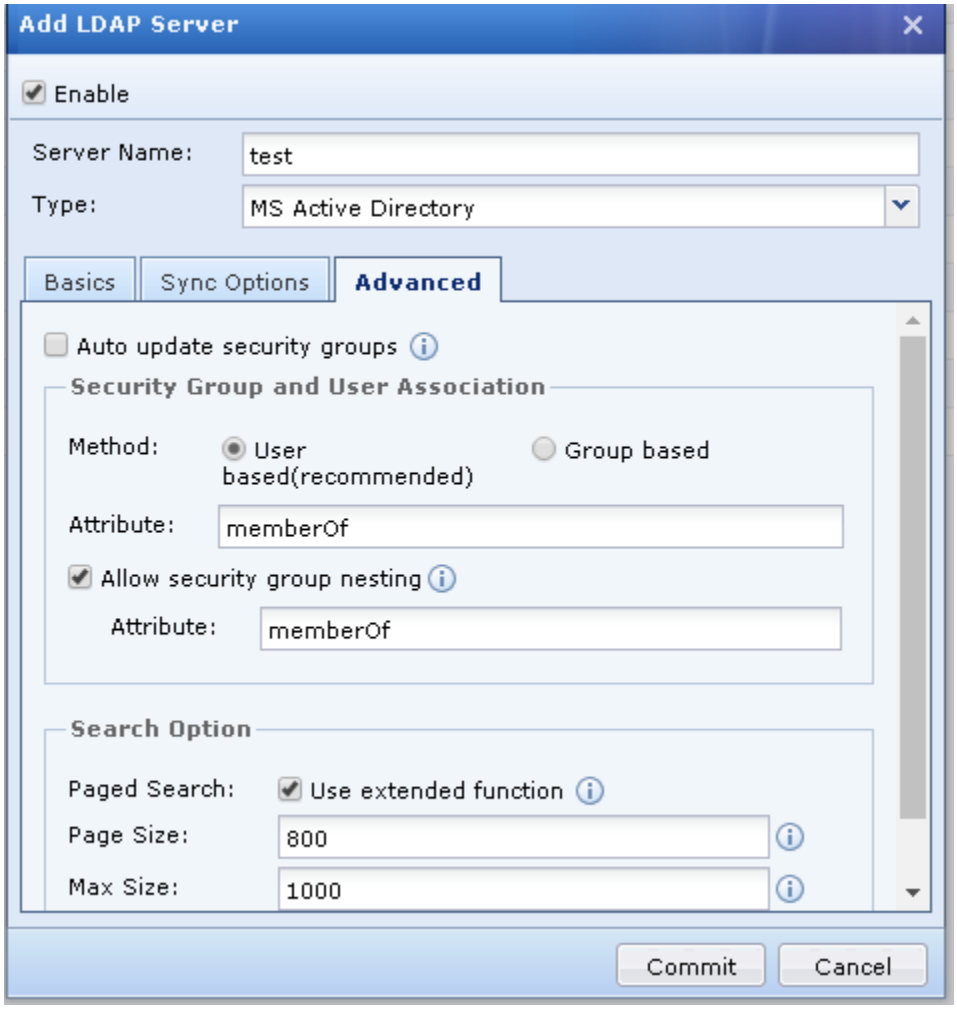
(Security Group Filter): Specify the (security) group filter condition of the LDAP server (Note: for the AD domain, here is the security group, for the non-AD domain, here is the group), that is, through this condition, it can be determined Whether the node is a (secure) group, for example, the AD domain can be used to filter whether a node is a security group by filling in "(objectClass=group)".

(Security Group Attribute): Specifies which attribute on the AD domain server identifies the member list of the security group. This attribute takes effect only when the LDAP server is an AD domain. If there is no special case in this field, you can usually fill in the member.

When the server type selects "MS Active Directory", the above parameters are set. Generally, the default parameters can be used. If the server is other types of LDAP, it needs to be adjusted according to the

actual situation, so that the device can read the correct LDAP.

4. Edit (Advance) configuration



(Auto update security groups): After checking, the LDAP server will be requested in real time to synchronize the contents of the required synchronization to the local, but will increase the pressure on the LDAP server. This option is only valid for the AD domain.

(Security Group and User Association): The default configuration is recommended here.

(Method): You can choose "users to find (recommended)" or "group to find users". If the user has an attribute on the LDAP server that holds the group to which it belongs, you can select "User Group (Recommended)" because this method will provide better performance and reduce the performance pressure on the LDAP server. If there is no information stored between the user and the group on the LDAP server, only the group saves the user. In this case, you need to check the group to find the user.

(Attribute): If the "User based" mode is selected, this field needs to fill in the group on the LDAP server or the user saves the attributes of its parent group. For example, the memberOf attribute on the AD domain identifies the parent group of a node, so when searching, the memberOf attribute is used to search for its parent group. If "Group based" is selected, this field needs to fill in the attributes of the group save subuser on the LDAP server. For example, the member attribute on the AD domain identifies a sub-user of a group, so when searching, the member attribute is used to search for a sub-user of a group.

(Allow security group nesting): The check box determines whether the configuration (security) group is valid for the users under the group, or whether the users and subgroups under the group are recursive. If you select this field, the user and sub-groups of the corresponding (secure) group will be recursively effective. If unchecked, it means that only the subordinate users in the configured (secure) group are valid, and all subgroups are ignored.

(Nesting Attribute): Nested properties can only be filled after "Allow security group nesting" is

checked. This option indicates which attribute is used by the group that needs to be searched for when recursively looking up. If the "User based" mode is selected, this field only needs to be consistent with the "Associated Properties". If "Group based" is selected, this field needs to fill in the attributes of the group save subgroup on the LDAP server. For example, the member attribute on the AD domain identifies all subgroups of a group, so when searching, the member attribute is used to search all subgroups of a group.

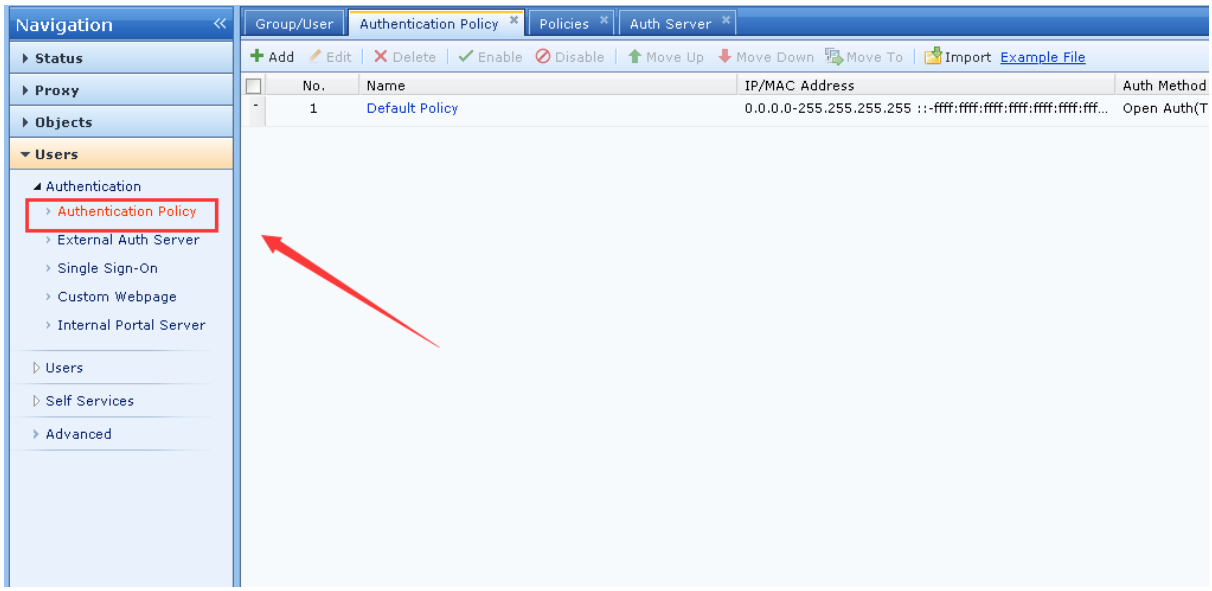
(Page search): To search the LDAP server using the extension API, it is recommended to keep the default configuration.

(Page size): The size returned when LDAP is paged, 0 means no limit, it is recommended to keep the default configuration.

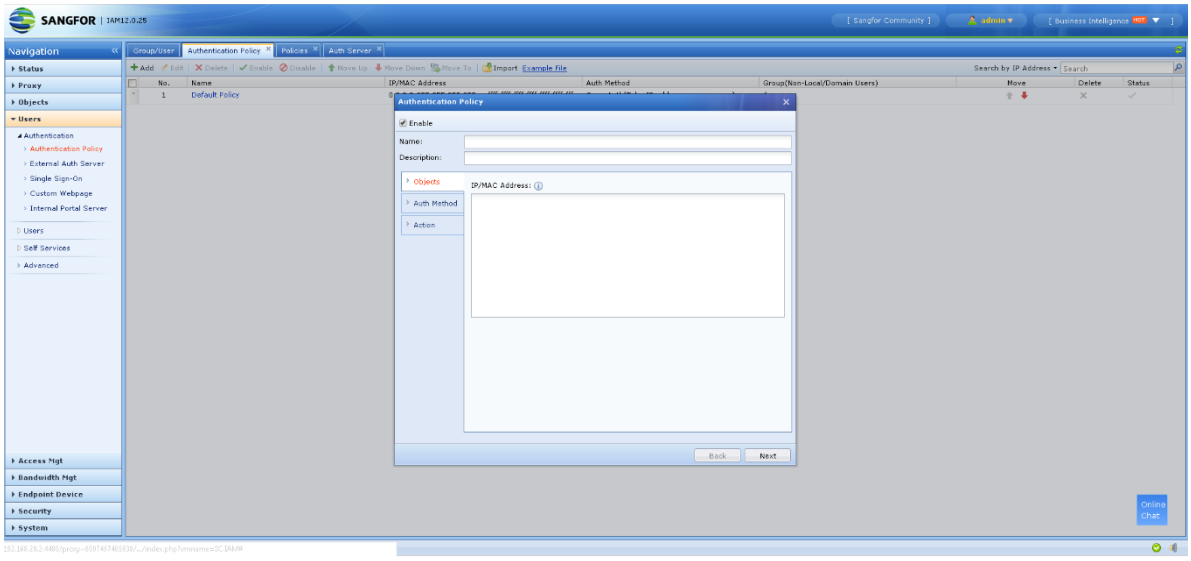
(Max size): The size limit option when synchronizing LDAP, it is recommended to keep the default configuration.

2.2 User authentication configuration

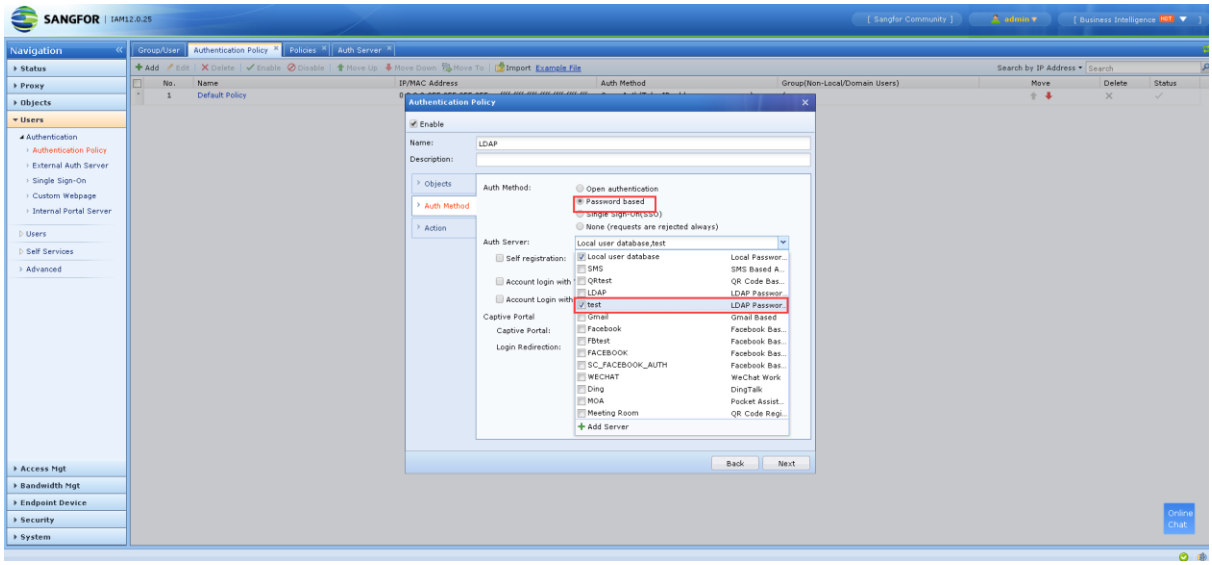
1. Edit(User) > (Authentication) > (Authentication policy)



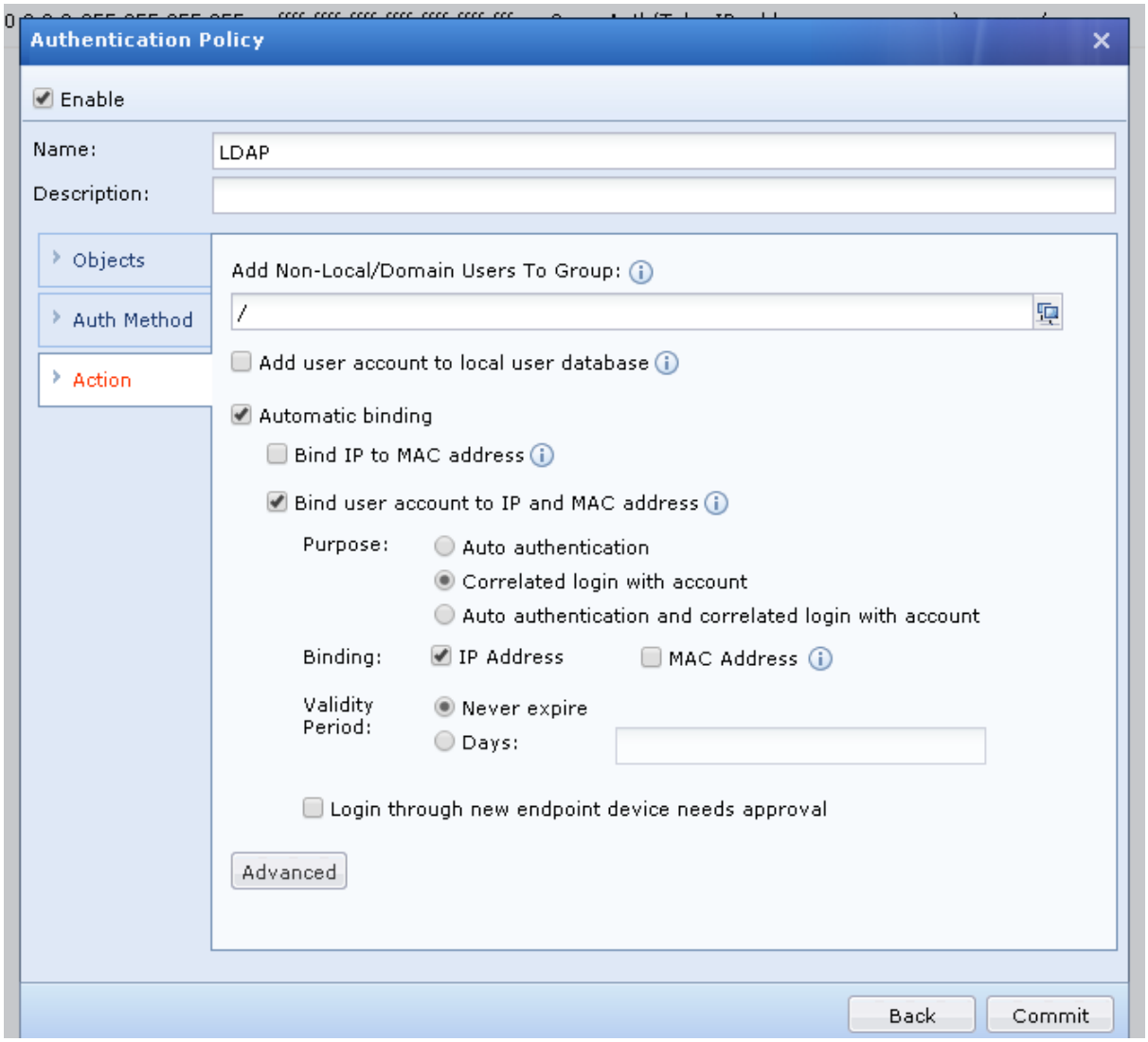
2. (Add) > (Authentication Policy) - It is recommended to test the process at the beginning of the test for a single address. After the test is successful, gradually expand the test range.



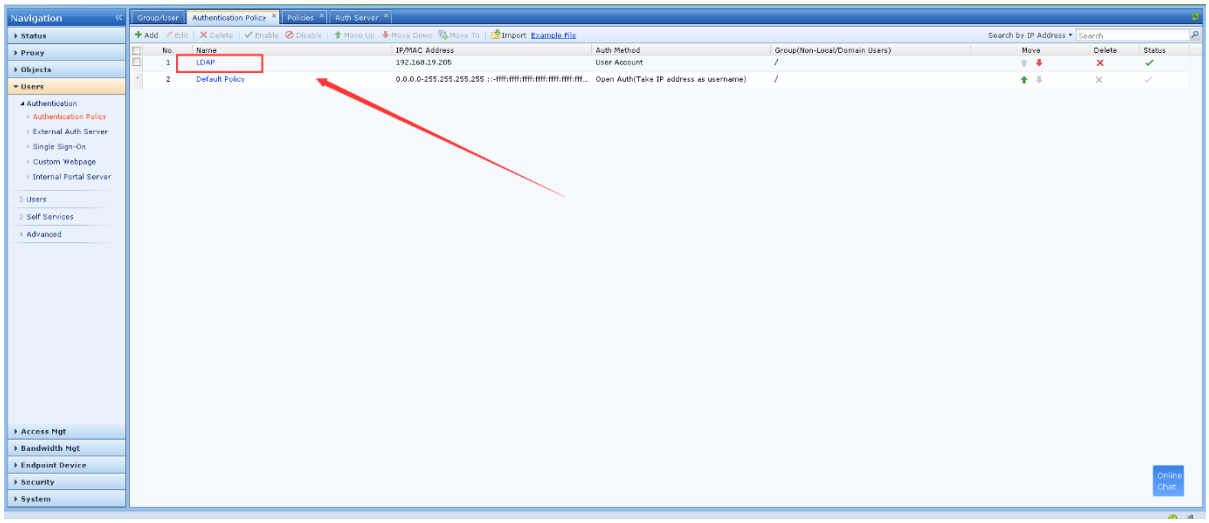
3. (Authentication method): Choose authentication method: Password based. Auth server: Select the - LDAP domain server created in the external auth server.



4. Action configuration requirement after authentication process.

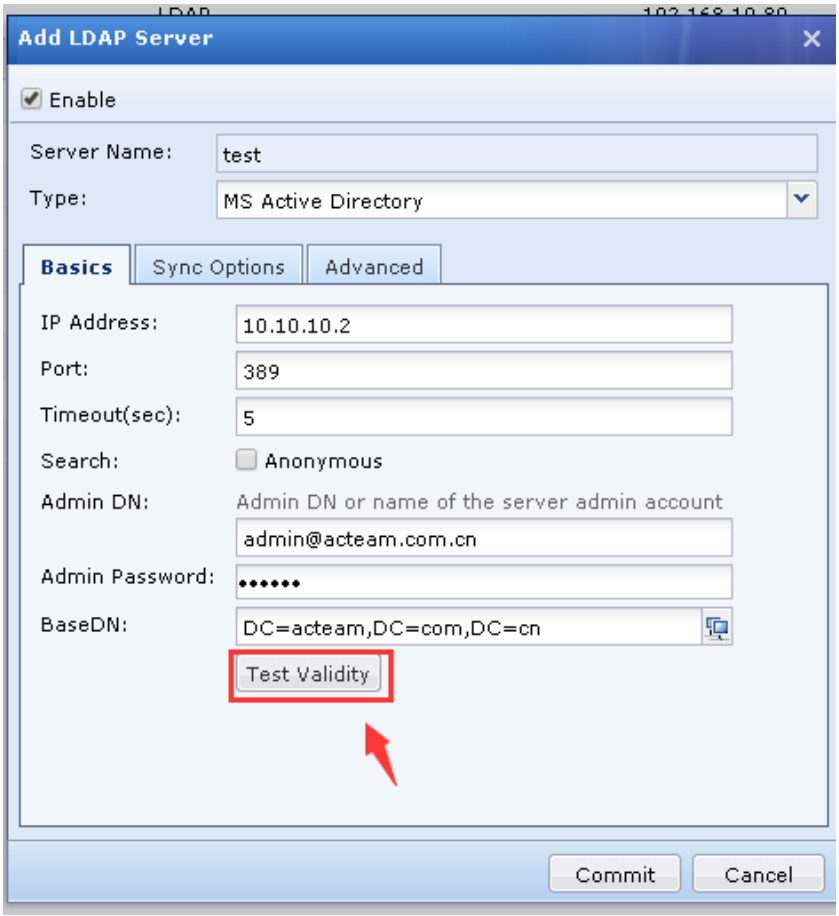


5. You can see the new policy in the authentication policy interface.

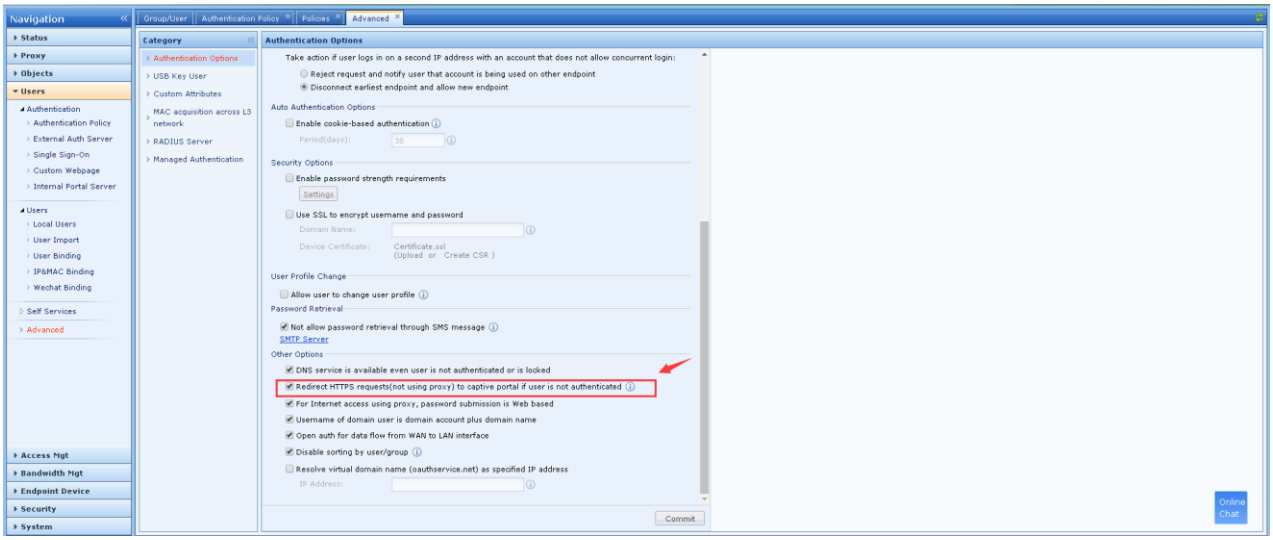


Chapter 3 Precaution

1. When configuring the external authentication server administrator account and password, it is recommended to click - [test validity] to ensure that it is available. as the picture shows:



2. The client opens the web page to pop up the authentication page. If it is domain URL link to open the link, you need to be able to resolve the domain name and open the URL of http. If you need to open the URL of https, you need to go to the authentication page. You need to select the authentication option. The options on the image below:


Navigation
Status
Proxy
Objects
Users
Authentication
Authentication Policy
External Auth Server
Single Sign-On
Custom Webpage
Internal Portal Server
Users
Local Users
User Import
User Binding
IP&MAC Binding
Wechat Binding
Self Services
Advanced
Access Mgt
Bandwidth Mgt
Endpoint Device
Security
System
Group/User
Authentication Policy
Policies
Advanced
Category
Authentication Options
USB Key User
Custom Attributes
MAC acquisition across L3 network
RADIUS Server
Managed Authentication
Authentication Options
Take action if user logs in on a second IP address with an account that does not allow concurrent login:
Reject request and notify user that account is being used on other endpoint
Disconnect earliest endpoint and allow new endpoint
Auto Authentication Options
Enable cookie-based authentication
Period(days):
Security Options
Enable password strength requirements
Settings
Use SSL to encrypt username and password
Domain Name:
Device Certificate:
Certificate.asl
(Upload or Create CSR)
User Profile Change
Allow user to change user profile
Password Retrieval
Not allow password retrieval through SMS message
SMTP Server
Other Options
DNS service is available even user is not authenticated or is locked
Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated
For Internet access using proxy, password submission is Web based
Username of domain user is domain account plus domain name
Open auth for data flow from WAN to LAN interface
Disable sorting by user/group
Resolve virtual domain name (oauthservice.net) as specified IP address
IP Address:
Commit
Online Chat