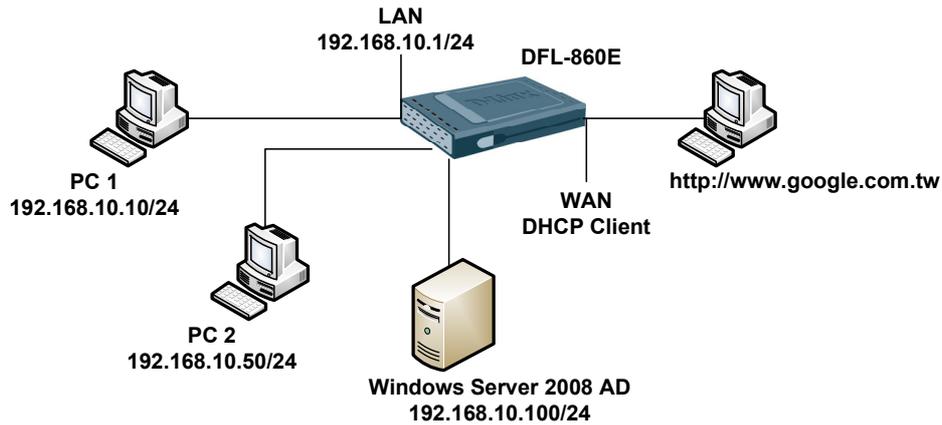


How to design WCF web authentication HTML banner



AD Server Information as below:

Domain name: test.com

Test Group: IT

Test account: test

[DFL-860E] Firmware Version: 2.27.03.25

1. System > Remote Management

Change remote HTTP and HTTPS port.

WebUI HTTP port:	<input type="text" value="8080"/>	Specifies the HTTP port for the web user interface.
WebUI HTTPS port:	<input type="text" value="4433"/>	Specifies the HTTP(S) port for the web user interface.

2. Objects > Address Book

Create a new object for authentication LAN net.

3	IT	192.168.10.0/24	IT
---	----	-----------------	----

3. Objects > ALG

Create a new ALG for our HTTP service.

#	Name	Type	Parameters	Comments
1	http-alg	HTTP ALG		

http-alg
Use an HTTP Application Layer Gateway to filter HTTP traffic.

General | File Integrity | Web Content Filtering | Anti-Virus | URL Filter

General

Mode:

Categories

Web content categories to block

Allowed

- Adult content
- Advertising
- Business oriented
- Chatrooms
- Clubs and Societies
- Computing/IT
- Crime/Terrorism
- Dating sites
- Drugs/Alcohol
- E-Banking
- Educational

Blocked

Options

Non-Managed Action: Action to take for content that hasn't been classified.

Allow Override

Allow Reclassification

OK Cancel

If you want to add picture file in authentication web page.

The picture file must to put in to the internal Web server.

Because our user must to authentication first then will see the internet page.

If your picture file is link to the internet it will not see anything picture when user start the browser.

You can see in our KM this picture is put in to the Windows Server 2008 IIS Server.

6. Rules > IP Rules

Create a special rule for WEB authentication

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	dns	NAT	lan	lannet	wan1	all-nets	dns-all
2	auth-allow	NAT	lan	IT	wan1	all-nets	http-all
3	no-auth-sat	SAT	lan	lannet	wan1	all-nets	all_services
4	no-auth-sat-allow	Allow	lan	lannet	wan1	all-nets	all_services

Index 1 & 3 is a necessary rule for WEB authentication and index 2 rule priorities must high than SAT rule.

no-auth-sat
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT | SLB SAT | SLB Monitors

General

Translate the

Source IP

Destination IP

to:

New IP Address: lan_ip

New Port:

All-to-One

Name	Address
dmz_ip	172.17.100.254
lan_ip	192.168.10.1
wan1_dns1	0.0.0.0
wan1_dns2	0.0.0.0
wan1_ip	1.1.1.1
wan2_ip	192.168.120.254

OK Cancel

7. User Authentication > External User Databases

server2008
External LDAP server used to verify user names and passwords.

General

General

Name: server2008

IP Address: 192.168.10.100

Port: 389

Timeout: 5 seconds

Name Attribute: SAMAccountName

Retrieve Group Membership

Membership Attribute: memberOf

Use Domain Name: Dont Use

Database Settings

Base Object: CN=Users,DC=test,DC=com

Administrator Account: administrator

Password: [masked] Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Confirm Password: [masked]

Domain Name:

Optional

Password Attribute: userPassword

※ “Administrator Account” and “Password”: It must be applied by the user who has Domain controller privilege.

※ “Password Attribute”: It is very important it must setup same as your description of AD group.

You can follow this KM [Server 2008 Setup] step.1 and step.2

8. User Authentication > User Authentication Rules

The screenshot shows the 'server2008-ldap' configuration window with the 'General' tab selected. The window title is 'server2008-ldap' and the subtitle is 'The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.' The 'General' tab is active, and the 'Authentication Options' tab is also visible. The 'Name' field is set to 'server2008-ldap'. The 'Authentication agent' is set to 'HTTP'. The 'Authentication Source' is set to 'LDAP'. The 'Interface' is set to 'lan'. The 'Originator IP' is set to 'all-nets'. The 'Terminator IP' is set to '(None)'. There is a blue information icon with a plus sign and the text 'For XAuth and PPP, this is the tunnel originator IP.' Below the configuration fields is a 'Comments' section with a text area. At the bottom right are 'OK' and 'Cancel' buttons.

The screenshot shows the 'server2008-ldap' configuration window with the 'Authentication Options' tab selected. The window title is 'server2008-ldap' and the subtitle is 'The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.' The 'Authentication Options' tab is active, and the 'General' tab is also visible. The 'General' tab is selected, and the 'Authentication Options' tab is also visible. The 'Name' field is set to 'server2008-ldap'. The 'Authentication agent' is set to 'HTTP'. The 'Authentication Source' is set to 'LDAP'. The 'Interface' is set to 'lan'. The 'Originator IP' is set to 'all-nets'. The 'Terminator IP' is set to '(None)'. There is a blue information icon with a plus sign and the text 'For XAuth and PPP, this is the tunnel originator IP.' Below the configuration fields is a 'Comments' section with a text area. At the bottom right are 'OK' and 'Cancel' buttons.

Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

RADIUS servers

Available Selected

LDAP servers

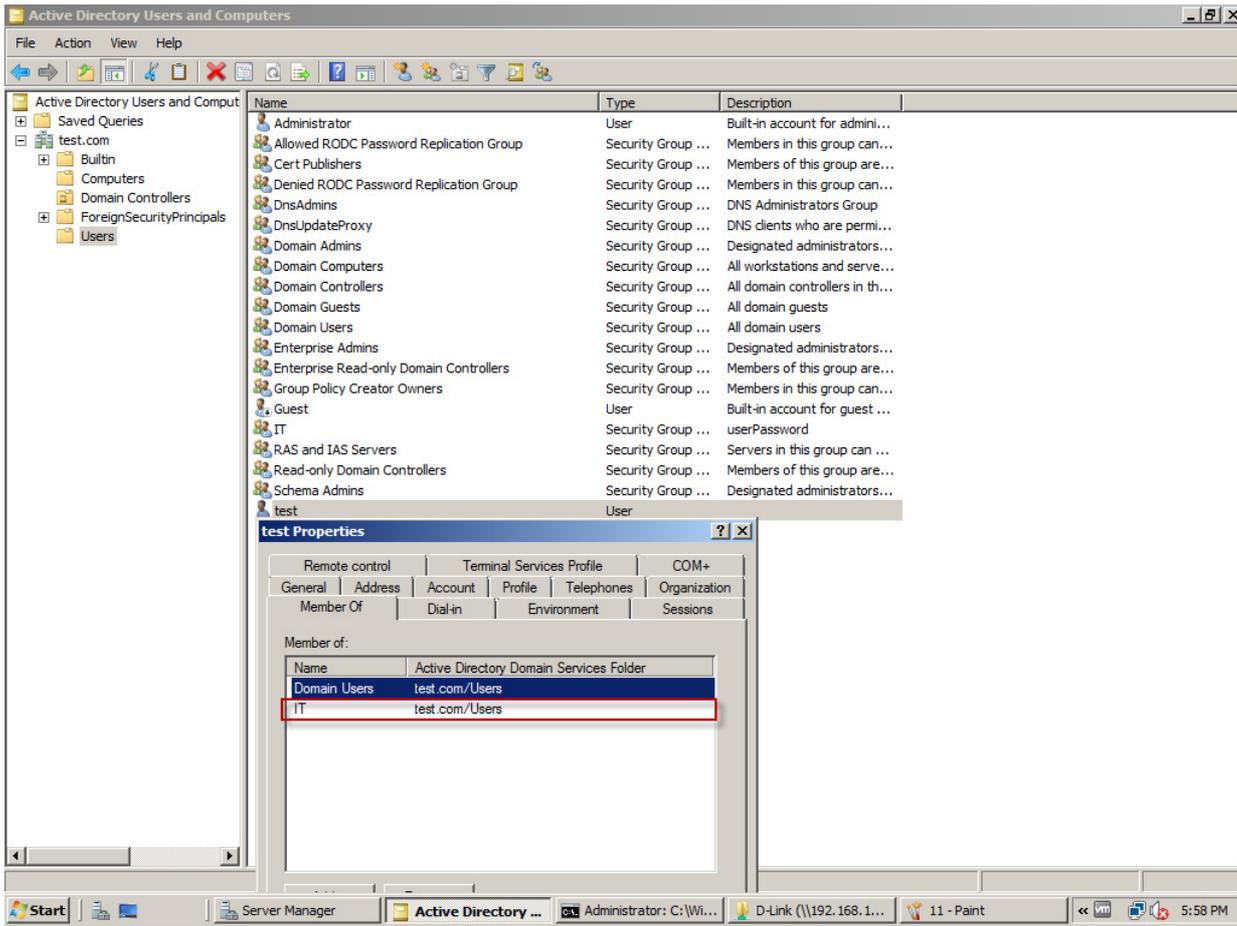
Available Selected

RADIUS Method: Unencrypted password (PAP)

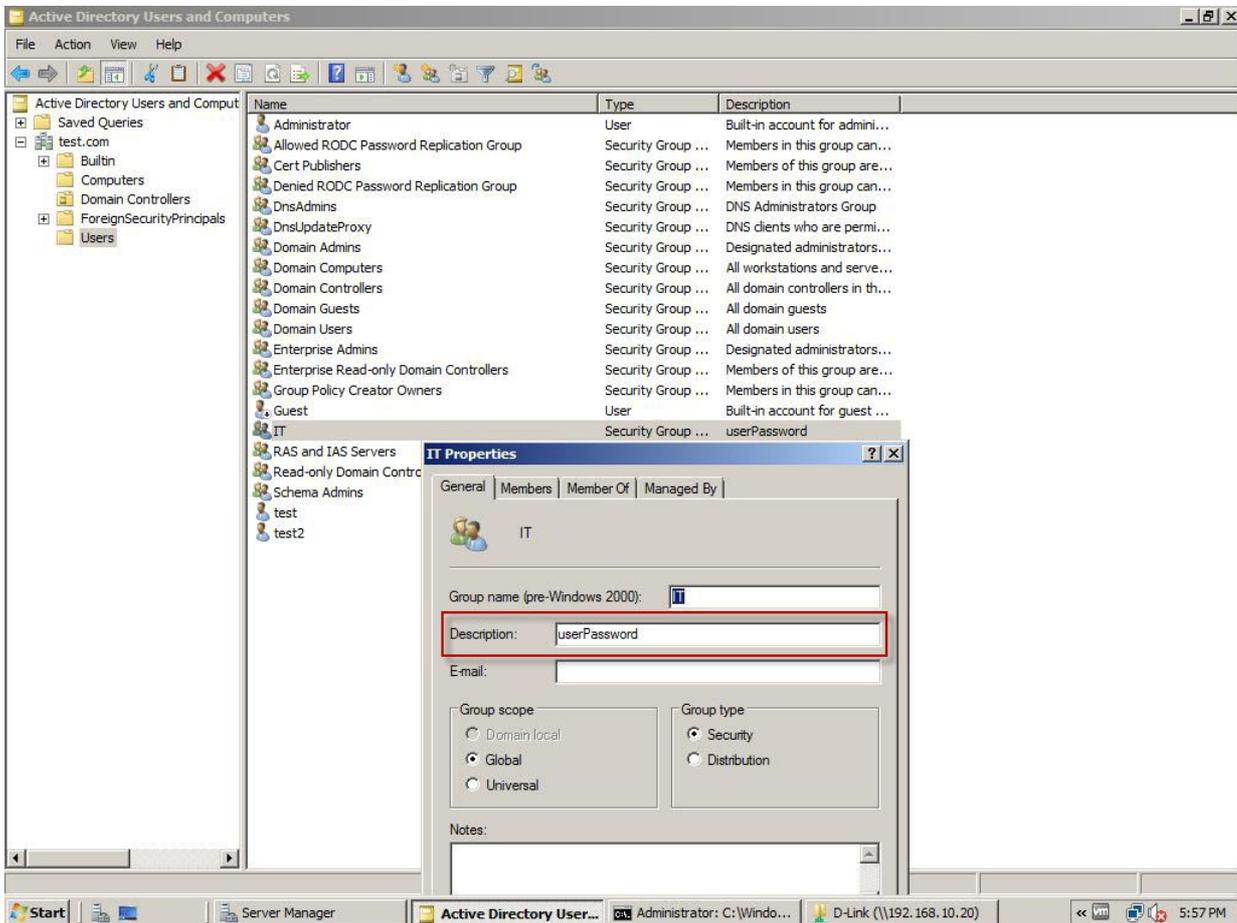
Local User DB: (None)

[Server 2008 Setup]

Step.1



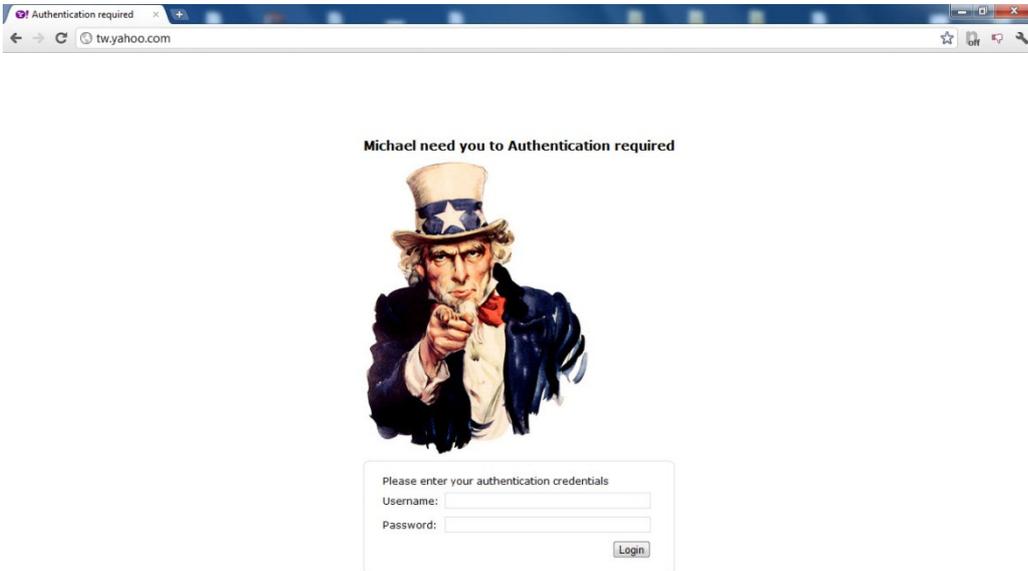
Step.2



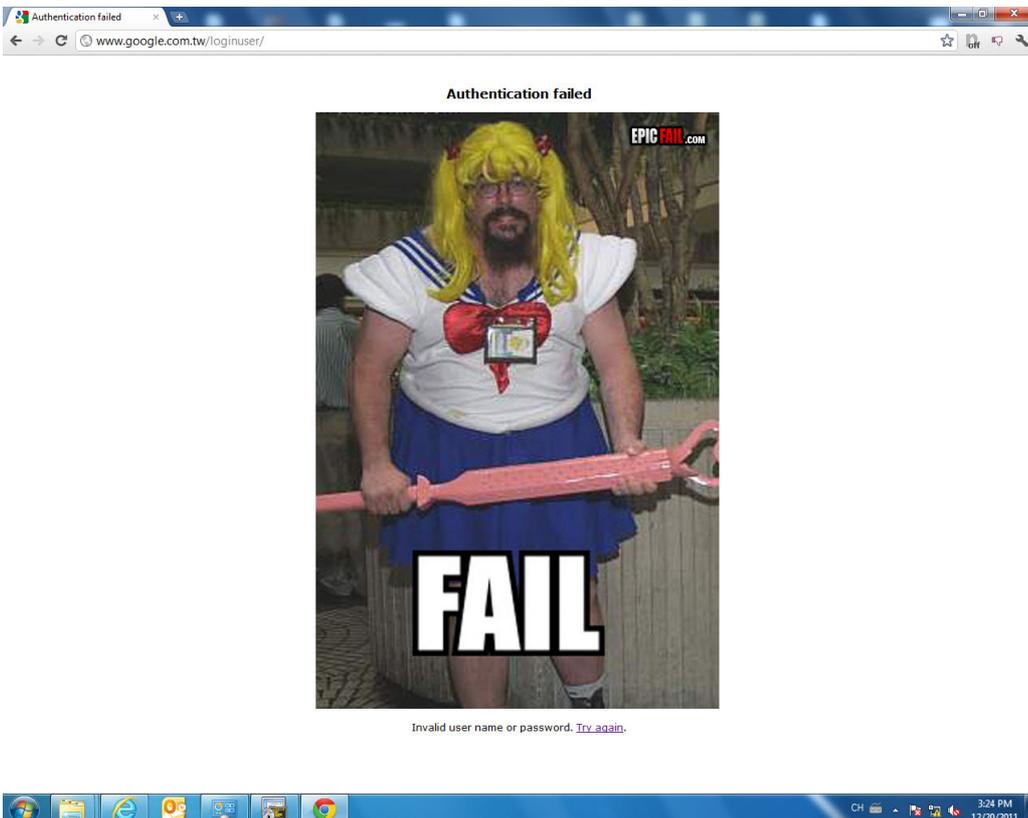
- ✘ Group description must set up as same as External User Databases Password Attribute.
You can check this KM Step.7 “User Authentication > External User Databases > Password Attribute”

[Test]

1. PC type any domain at the browser it will see this picture.



2. If user authentication fail it will got this picture.



END