

DHCP plugin

[How to setup the dhcp-plugin \(since 1.0.5\)](#)

[How to configure dhcpcd](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/dhcp_plugin

Last update: **2015/09/18 09:25**



How to setup the dhcp-plugin

Requirements

In order to use dhcp plugin, you need to have a dhcp server installed and configured in your infrastructure environnement. You can do that installing the following:

Debian

Lenny

```
root@dhcp-server:~# apt-get install dhcp3-server-ldap
```

Squeeze

```
root@dhcp-server:~# apt-get install isc-dhcp-server-ldap
```

RPM

```
yum install isc-dhcp-server-ldap
```

In order to install dns plugin, you need to have installed and configured Systems plugin. If you don't know how to install him, you can take a look at:

- [How to setup systems-plugin \(since 1.0.5\)](#)

Install required packages

Debian

```
root@fd-server:~# apt-get install fusiondirectory-plugin-dhcp
```

RPM <TODO>

```
rpm user, please edit
```

Install required schemas

Debian

```
root@fd-server:~# apt-get install fusiondirectory-plugin-dhcp-schema
root@fd-server:~# fusiondirectory-insert-schema -i
/etc/ldap/schema/fusiondirectory/dhcp-fd.schema
```

RPM

```
yum install fusiondirectory-plugin-dhcp-schema
fusiondirectory-insert-schema -i /etc/openldap/schema/fusiondirectory/dhcp-
fd.schema
```

Configure related services

debian

In your dhcp-server add at the end of /etc/dhcp/dhcpd.conf file the following ldap configuration lines :

```
ldap-server "localhost";
ldap-port 389;
ldap-username "cn=ldapadmin,dc=my-domain,dc=com";
ldap-password "secret";
ldap-base-dn "dc=my-domain,dc=com";
ldap-method dynamic;
ldap-debug-file "/var/log/dhcp-ldap-startup.log";
```

Note: Adjust ldap-server, ldap-port, ldap-username, ... to your environment.

rpm <TODO>

```
rpm user, please edit
```

Add dhcp service to a system in fusiondirectory

1. If not already done, create a new server in fusiondirectory. If you don't know, see [how to create a new server](#).
2. Click on the new server:

List of systems							
	Name	IP	MAC	Description	Services	Release	Actions
<input type="checkbox"/>	dhcp-server	192.168.56.3	08:00:27:0b:15:b1	Main dhcp server			

3. Click on Services:

cn=dhcp-server,ou=servers,ou=systems,dc=openSIDES,dc=be

Generic NIS Netgroup FAI Argonaut Logs Argonaut client Services **Services** ACL References

Properties

Name* dhcp-server
Description Main dhcp server
Location
Base /
Lock this server

Action

Action

Servers

Syslog server default

NTP servers

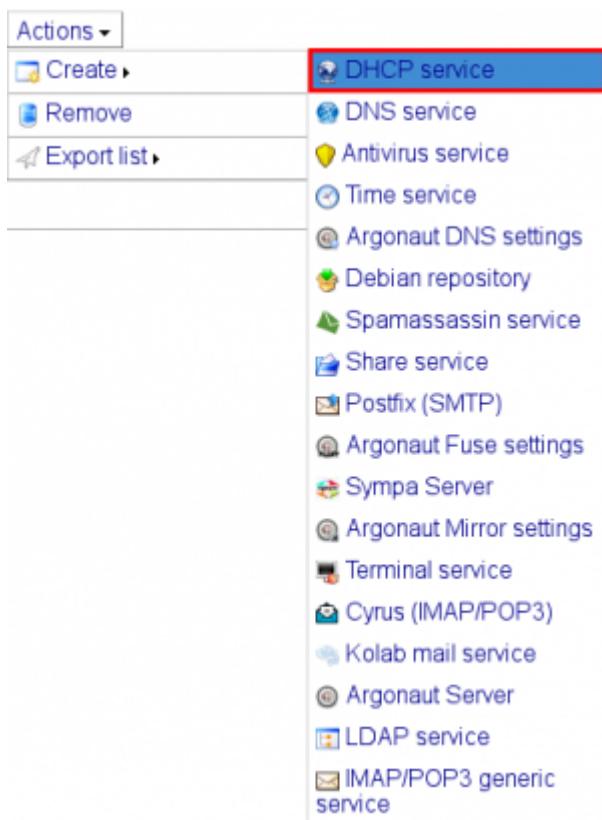
LDAP servers

Network settings

IP-address* 192.168.56.3
MAC-address* 08:00:27:0b:15:b1
 Enable DNS for this device
 Enable DHCP for this device

Ok Apply Cancel

4. Create DHCP Service via Actions -> Create:



5. Insert a new dhcp section:

DHCP sections

- Global options

Save **Cancel**

6. Choose new section “subnet” and click “Create”:

Create new DHCP section

Please choose one of the following DHCP section types.

Section **Class**

- Class
- DNS update key
- DNS update zones
- Group
- Host
- Shared network
- Subnet**

Create **Cancel**

7. Fill in required fields and click “Save”:

cn=dhcp-server,ou=servers,ou=systems,dc=opensides,dc=be

Generic

Network address*

Netmask*

Network configuration

Router
Netmask
Broadcast

Domain Name Service

Domain

DNS server
 Add **Delete**

Bootup

Filename
Next server

Domain Name Service options

Assign hostnames found via reverse mapping
 Assign hostnames from host declarations

Show advanced settings

Save **Cancel**

8. Click “Save” again:

The screenshot shows the 'Services' tab selected in the top navigation bar. Under 'DHCP sections', a global option 'dhcp' is expanded, showing a subnet configuration for 'Subnet '192.168.56.0''. The subnet table includes columns for IP range, lease time, and other parameters. At the bottom right, the 'Save' button is highlighted with a red box.

9. Click "Ok":

The screenshot shows the 'Services' tab selected in the top navigation bar. The main area displays a table of services, with one entry for 'DHCP service'. The 'Actions' column for this entry contains an edit icon. At the bottom right, the 'Ok' button is highlighted with a red box.

NOTE: The hostname of the dhcp-server (machine running dhcpcd) MUST BE the same as the name of the server you assigned the dhcp service in fusiondirectory !! Check your /etc/hosts and the interface defined in /etc/default/isc-dhcp-server

Note on tftp setup and ddns

The tftp settings may need to be set at the Global Option 'dhcp' level of the DHCP Service.

If you define it in the subnet, make sure to save all screens until the one listing all system's services

The Dynamic DNS update style need to be set at the Global Option level.

The screenshot shows the 'Services' tab selected in the top navigation bar. The configuration page for a specific service is displayed, containing several sections: 'Generic' (with 'Authoritative service' checked), 'Network configuration' (with fields for Router, Netmask, and Broadcast), 'Bootup' (with fields for Filename and Next server), and 'Domain Name Service' (with fields for Domain and DNS server). At the bottom right, the 'Save' button is highlighted with a red box.

Generic section:

- check out “Authoritative service”
- Dynamic DNS update: “interim”

Bootup section :

Must include

- “filename”: Path/to/your/pixelinux.0 within your tftp root
- “next server”:servername or IP

From:
<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:
https://documentation.fusiondirectory.org/en/documentation/plugin/dhcp_plugin/how_to_setup_dhcp_plugin_1.0.5

Last update: **2016/02/12 21:29**



How to configure dhcpcd

In order to have your DHCP server connected on LDAP, you have to install the LDAP backend.

On EL6 (and CentOS 6), the LDAP backend is provided by default with the dhcp service, so:

```
yum install dhcp
```

On debian and ubuntu, you have to install it explicitly:

```
apt-get install dhcp3-server-ldap
```

Now, just edit your dhcpcd.conf file (/etc/dhcp/dhcpcd.conf) with something like this:

[dhcpcd.conf](#)

```
ldap-server "ldap.domain.test";
ldap-port 389;
ldap-username "cn=dhcp,ou=DSA,dc=domain,dc=test";
ldap-password "p@ssw0rd";
ldap-base-dn "dc=domain,dc=test";
ldap-method dynamic;
ldap-ssl start_tls;
```

In this example:

- Our LDAP server's DNS name is ldap.domain.test
- It's listening on the default port (389)
- DHCP will bind to LDAP using a DSA account named dhcp (DN cn=dhcp,ou=DSA,dc=domain,dc=test)
- the password of the dhcp DSA account is p@ssw0rd
- We'll lookup in the whole LDAP database for dhcp entries (you could restrict it to one server, using cn=dhcp,ou=servers,ou=systems,dc=domain,dc=test as base-dn for example)
- We'll use TLS to bind on LDAP

ldap-method can be either static or dynamic. With the dynamic method, the DHCP service will lookup in LDAP for each DHCP requests it receive, so changes in LDAP are applied immediatly. With the static method, the DHCP server will read it's config from LDAP at startup, and will keep it in memory (so you have to restart the DHCP service to propagate changes in LDAP)

Here are the slapd ACL I use for dhcp entries:

```
# Access to DHCP settings
access to dn.subtree=ou=servers,ou=systems,dc=domain,dc=test
filter=(|(objectClass=dhcpSubnet)(objectClass=dhcpService)(objectClass=dhcpServer)(objectClass=dhcpHost))
        by dn=cn=dhcp,ou=DSA,dc=domain,dc=test peername.ip="127.0.0.1" read
        by dn=cn=dhcp,ou=DSA,dc=domain,dc=test peername.ip="[:1]" read
```

```
by dn=cn=dhcp,ou=DSA,dc=domain,dc=test ssf=256 read
by group.exact="cn=admins,ou=Groups,dc=domain,dc=test"
peername.ip="127.0.0.1" write
by group.exact="cn=admins,ou=Groups,dc=domain,dc=test"
peername.ip="[:1]" write
by group.exact="cn=admins,ou=Groups,dc=domain,dc=test" ssf=256 write
by * none
```

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/dhcp_plugin/configure_dhcpd

Last update: **2014/06/27 21:16**



DNS plugin

- [How to setup the dns-plugin](#)
- [Configure bind sdb \(since 1.0.7\)](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/dns_plugin



Last update: **2014/06/27 21:16**

How to setup Dns plugin

Starting from 1.0.5, argonaut-ldap2zone is the program used to create bind zone files and refresh the bind service.

Argonaut-ldap2zone is in development stage, so you need to take him from fusiondirectory development repository. Add argonaut development repository in your system, reload your list of packages and install:

debian

```
root@dhcp-server:~# echo "deb http://repos.fusiondirectory.org/argonaut/ wheezy main" >> /etc/apt/sources.list
root@dhcp-server:~# echo "deb http://repos.fusiondirectory.org/argonaut-libs/ wheezy main" >> /etc/apt/sources.list
root@dhcp-server:~# apt-get update
root@dhcp-server:~# apt-get install bind9 bind9-host argonaut-ldap2zone ldap-utils
root@fd-server:~# apt-get install fusiondirectory-plugin-dns
fusiondirectory-plugin-dns-schema
```

rpm <TODO>

```
rpm user, please edit
```

Requirements

In order to use dns plugin, you need to have a dns server installed and configured in your infrastructure environnement. You can do that installing the following:

debian

```
apt-get install bind9 bind9-host ldap-utils
```

rpm <TODO>

```
rpm user, please edit
```

In order to install dns plugin, you need to have installed and configured Systems plugin. If you don't know how to install him, you can take a look at:

- [How to setup systems-plugin \(since 1.0.5\)](#)

Install required packages

debian

```
apt-get install fusiondirectory-plugin-dns
```

rpm <TODO>

```
rpm user, please edit
```

Install required schemas

debian

```
apt-get install fusiondirectory-plugin-dns-schema  
fusiondirectory-insert-schema -i  
/etc/ldap/schema/fusiondirectory/dnszone.schema  
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/dns-fd-  
conf.schema
```

rpm <TODO>

```
rpm user, please edit
```

Configure related services

Configure your /etc/ldap/ldap.conf according to your environment:

debian

```
BASE      dc=opensides,dc=de  
URI       ldap://fd-server
```

rpm <TODO>

```
rpm user, please edit
```

(Re)Start related service

debian

(Re)Start slapd:

```
root@fd-server:~# service slapd stop
root@fd-server:~# service slapd start
```

rpm <TODO>

```
rpm user, please edit
```

How to use the dns plugin

Add dns service to a system in fusiondirectory

In our exemple the dns service is in dhcp-server.

1. If not already done, create a new server in fusiondirectory. If you don't know, see [how to create a new server](#).
2. Click on the dhcp-server:

List of systems							
	Name	IP	MAC	Description	Services	Release	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> dhcp-server	192.168.56.3	08:00:27:0b:15:b1	Main dhcp server			

3. Click on Services:

Properties

Name*: dhcp-server
Description: Main dhcp server
Location:
Base: /
Lock this server:

Action

Action:

Servers

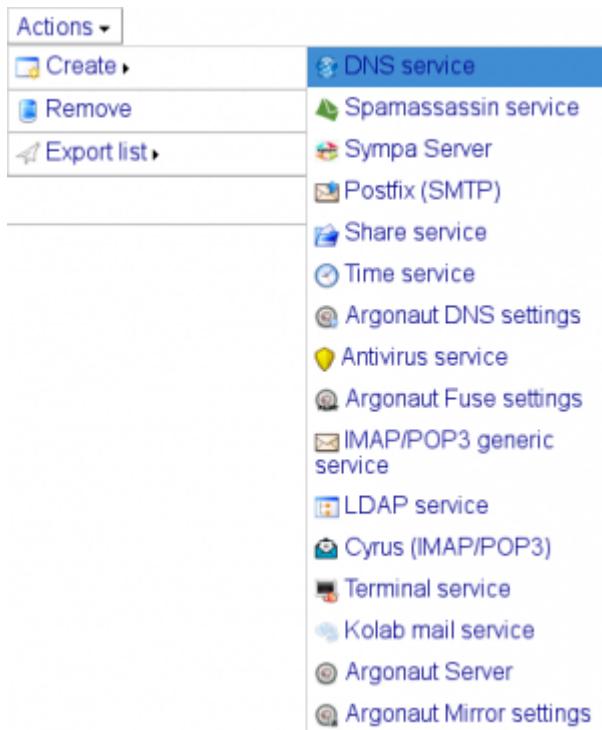
Syslog server: default
NTP servers:
LDAP servers:

Network settings

IP-address*: 192.168.56.3
MAC-address*: 08:00:27:0b:15:b1 Autodetect
 Enable DNS for this device
 Enable DHCP for this device

Ok | Apply | Cancel

4. Create DNS service via Actions -> Create:



5. Add a new dns-zone:

Zones

Add

Save | Cancel

6. Fill in all required fields and click "Save":

cn=dhcp-server,ou=servers,ou=systems,dc=opensides,dc=be

Generic

Zone name* opensides.be

Network address* 192.168.56.0

Netmask 255.255.255.0 (Class C)

Zone is in use, network settings can't be modified.

SOA record

Primary dns server for this zone* dhcp-server

Mail address* admin@opensides.be

Serial number (automatically incremented)* 2013051505

Refresh* 3600

Retry* 1800

Expire* 720000

TTL* 6400

MxRecords

Global zone records

Add

Save **Cancel**

Note: There will be data to type in for the DNS service. All of it is just the usual information.

NOTE: Make sure you fill in “Primary dns server for this zone” as a HOSTNAME, NOT AN IP! Otherwise, zone file (in /var/cache/bind/db.your.zone.) will be badly formatted and won’t be loaded.

7. Click “Save” again:

cn=dhcp-server,ou=servers,ou=systems,dc=opensides,dc=be

Zones

opensides.be.	Reverse zone : 192.168.56	TTL : 6400	Class : IN	
---------------	---------------------------	------------	------------	--

Add

Save **Cancel**

8. Click “Ok”:

cn=dhcp-server,ou=servers,ou=systems,dc=opensides,dc=be

List of services

	Description	Actions
<input type="checkbox"/> !	DHCP service	
<input type="checkbox"/>	DNS service	

Ok **Apply** **Cancel**

9. Enter the server again, check the 'Enable DNS for this device' checkbox and click “Ok”:

Properties

Name*: dhcp-server
Description: Main dhcp server
Location:
Base: /
Lock this server:

Action

Action: Execute

Servers

Syslog server: default
NTP servers:
LDAP servers:

Network settings

IP-address*: 192.168.56.3
Propose ip:
MAC-address*: 08:00:27:0b:15:b1 Autodetect
 Enable DHCP for this device

Enable DNS for this device
Zone: DHCP-SERVER/opensides.be.
TTL:
Dns records:

Ok Apply Cancel

10. You are back to main “Systems” screen now, and ready to continue with last step(s).

Update dns zone

If not already done, [add argonaut DNS service](#) to your dns server in fusiondirectory interface.

Every time that you add or change your dns zone in your dns-server, you need to update bind. You can do that directly in FusionDirectory GUI or manually from dns-server command line.

run argonaut-ldap2zone from FusionDirectory

After you have saved all your changes in your dns server, click on dns settings icon:

List of systems							
	Name	IP	MAC	Description	Services	Release	Actions
<input type="checkbox"/>	fd-server.opensides.be	192.168.56.102	08:00:27:18:c7:db				

then you can reload the zone's clicking on button highlighted in red:

Zones

Zone	Reverse zone : 192.168.56 Reverse zone : 10.1	TTL : 6400 TTL : 6400	Class : IN Class : IN	Actions
opensides.be. fusiondirectory.org.				

Add Save Cancel

run manually argonaut-ldap2zone

On the dns server:

```
root@dhcp-server:~# argonaut-ldap2zone --verbose <name-of-the-zone>
```

If you want to test your zone before enabling it and dump it on another directory

```
root@dhcp-server:~# argonaut-ldap2zone --verbose --norestart --dumpdir dnszone/ master.fdi <name-of-the-zone>
```

In my exemple I've created 2 zones, that give me :

```
root@dhcp-server:~# argonaut-ldap2zone --verbose labo.opensides.be
Searching DNS Zone 'labo.opensides.be.'
Found 1 results
Added record ns @ IN localhost
Added record SOA @ IN localhost root.fd-install. 201211211 3600 1800 720000
6400 500
Reverse zone is 56.168.192.in-addr.arpa.
Found 1 results
Added record ns @ IN localhost
Added record SOA @ IN localhost root.fd-install. 201211211 3600 1800 720000
6400 500
server reload successful

root@dhcp-server:~# argonaut-ldap2zone --verbose acme.com
Searching DNS Zone 'acme.com.'
Found 1 results
Added record ns @ IN dhcp-server
Added record SOA @ IN dhcp-server admin.acme.com. 201211212 3600 1800 720000
6400 500
Reverse zone is 1.0.10.in-addr.arpa.
Found 1 results
Added record ns @ IN dhcp-server
Added record SOA @ IN dhcp-server admin.acme.com. 201211212 3600 1800 720000
6400 500
server reload successful
```

From:
<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:
https://documentation.fusiondirectory.org/en/documentation/plugin/dns_plugin/how_to_setup_dns_plugin_1.0.5

Last update: **2015/01/31 17:18**



Configure bind sdb

[bind-sdb](#) is an LDAP backend for bind. It can be used as an alternative to `ldap2zone`. Instead of building a standard flat file from the LDAP content, bind will do an LDAP lookup fore each DNS request it receives.

Install bind-sdb

Depending on your distribution, `bind-sdb` might be available in the default repositories. It's the case with EL6, so installation is just a mater of:

```
yum install bind-sdb
```

Configure FD not to store final dots in zone names

With `bind-sdb`, when bind performs lookups in LDAP, it doesn't add the final dot in zone names. So you have to configure FD not to add the final dots in the LDAP tree, or `bind-sdb` will never find a match. To do so, go in the main configuration menu, then `plugins`, and make sure the "Store final dot in domains" is not selected. This option is available since 1.0.7.



Create your zones as usual

Now, you can create your zones in FD interface as usual

Configure bind-sdb

We'll now configure bind to use the LDAP backend, to do so, just declare your zones in `named.conf` like this:

```
zone "domain.test." IN {
    type master;
    database "ldap
ldap://127.0.0.1/dc=domain,dc=test????!bindname=cn=dns%2cou=DSA%2cdc=domain%
2cdc=test,!x-bindpw=password 172800";
};
zone "10.10.in-addr.arpa." IN {
```

```

        type master;
        database "ldap
ldap://127.0.0.1/dc=domain,dc=test????!bindname=cn=dns%2cou=DSA%2cdc=domain%
2cdc=test,!x-bindpw=password 172800";
} ;

```

In this example:

- Bind runs on the same box than the LDAP service (<ldap://127.0.0.1>)
- Our zone is domain.test, and its using the 10.10.0.0/16 network
- To access DNS data, we're using a DSA account named dns. It's DN is cn=dns,ou=DSA,dc=domain,dc=test, and we have to enter it URI escaped, so it become cn=dns%2cou=DSA%2cdc=domain%2cdc=test
- the password for this DSA account is “password”
- 172800 is the default TTL for entries which doesn't have a TTL defined

 **Fix Me!**: I couldn't get TLS working between bind-sdb and slapd. It should be possible to enable TLS adding the option !x-tls in the LDAP URI

slapd acl

Here're the slapd ACL I've added to restrict access to DNS entries to the dns DSA account:

```

# Access to DNS entries
access to dn.subtree=ou=servers,ou=systems,dc=domain,dc=test
filter=(objectClass=dNSZone)
    by dn=cn=dns,ou=DSA,dc=domain,dc=test peername.ip="127.0.0.1" read
    by dn=cn=dns,ou=DSA,dc=domain,dc=test peername.ip="[:1]" read
    by dn=cn=dns,ou=DSA,dc=domain,dc=test ssf=256 read
    by group.exact="cn=admins,ou=Groups,dc=domain,dc=test" write
    by * none

```

Just adjust it to your need.

DNS Cache

With this setup, bind won't do any caching of responses, it'll just query LDAP each time it has to answer. This is not optimal, and can put a high load on your LDAP server. In order to prevent this, you can configure:

- bind to only listen on the loopback of your DNS server
- a DNS cache can listen on the network interface and manage queries:
 - Requests for example.test are forwarded to bind
 - Requests for any other domain are forwarded to another DNS (or directly resolved recursively)
 - Replies are cached

You can use unbound for example as a DNS cache. Here are some sample config files:

[named.conf](#)

```

options {
    listen-on port 53 { 127.0.0.1; };
    directory      "/var/named";
    dump-file      "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { localhost;};
    recursion no;

    dnssec-enable no;
    dnssec-validation no;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";
};

logging {
    channel default_file {
        file "/var/log/named.log" size 10m;
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category default{ default_file; };
};

zone "domain.test." IN {
    type master;
    database "ldap
ldap://127.0.0.1/dc=domain,dc=test????!bindname=cn=dns%2cou=DSA%2cdc=do
main%2cdc=test,!x-bindpw=password 172800";
};
zone "10.10.in-addr.arpa." IN {
    type master;
    database "ldap
ldap://127.0.0.1/dc=domain,dc=test????!bindname=cn=dns%2cou=DSA%2cdc=do
main%2cdc=test,!x-bindpw=password 172800";
};

```

[unbound.conf](#)

```

server:
    verbosity: 1
    statistics-interval:

```

```
statistics-cumulative: no
extended-statistics: yes
num-threads: 2
interface: 10.10.4.10
interface-automatic: no
do-ip6: no
access-control: 127.0.0.1 allow
access-control: 10.10.0.0/16 allow
chroot: ""
username: "unbound"
directory: "/etc/unbound"
log-time-ascii: yes
pidfile: "/var/run/unbound/unbound.pid"
hide-identity: yes
hide-version: yes
harden-glue: yes
harden-dnssec-stripped: yes
harden-below-nxdomain: yes
harden-referral-path: yes
use-caps-for-id: no
unwanted-reply-threshold: 10000000
do-not-query-localhost: no
prefetch: yes
prefetch-key: yes
dlv-anchor-file: "/etc/unbound/dlv.isc.org.key"
trusted-keys-file: /etc/unbound/keys.d/*.key
auto-trust-anchor-file: "/etc/unbound/root.anchor"
val-clean-additional: yes
val-permissive-mode: no
val-log-level: 1
local-zone: "domain.test." transparent
local-zone: "10.10.in-addr.arpa." transparent
include: /etc/unbound/local.d/*.conf
remote-control:
control-enable: no
server-key-file: "/etc/unbound/unbound_server.key"
server-cert-file: "/etc/unbound/unbound_server.pem"
control-key-file: "/etc/unbound/unbound_control.key"
control-cert-file: "/etc/unbound/unbound_control.pem"
include: /etc/unbound/conf.d/*.conf
stub-zone:
name: "domain.test"
stub-addr: 127.0.0.1
stub-zone:
name: "10.10.in-addr.arpa."
stub-addr: 127.0.0.1
forward-zone:
name: "."
forward-addr: 88.191.254.60
forward-addr: 88.191.254.70
```

With this example:

- All the queries for domain.test and its reverse zone (10.10.in-addr.arpa) will be forwarded to bind-sdb (and then cached by unbound)
- Every other requests will be forwarded to 88.191.254.60 and 88.191.254.70

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/dns_plugin/bind_sdb

Last update: **2014/06/27 21:16**



Dovecot plugin

- [How to install Dovecot plugin](#)
- [Add Dovecot service](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/dovecot_plugin

Last update: **2015/10/12 10:11**



Howto install Dovecot plugin

Requirements

In order to install dovecot plugin, you need to have installed and configured mail plugin. If you don't know how to install him, you can take a look at:

[Howto install mail plugin](#)

Installation

Archlinux

```
yaourt -S fusiondirectory-plugin-dovecot  
yaourt -S fusiondirectory-plugin-dovecot-schema
```

Debian

```
apt-get install fusiondirectory-plugin-dovecot  
apt-get install fusiondirectory-plugin-dovecot-schema
```

RHEL / SL

```
yum install fusiondirectory-plugin-dovecot  
yum install fusiondirectory-plugin-dovecot-schema
```

SLES / Suse

```
zypper install fusiondirectory-plugin-dovecot  
zypper install fusiondirectory-plugin-dovecot-schema
```

Insert schema

Archlinux / SL / SLES / Suse

```
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/dovecot-  
fd.schema
```

RHEL / CentOS

```
fusiondirectory-insert-schema -i  
/etc/openldap/schema/fusiondirectory/dovecot-fd.schema
```

Debian

```
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/dovecot-  
fd.schema
```

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

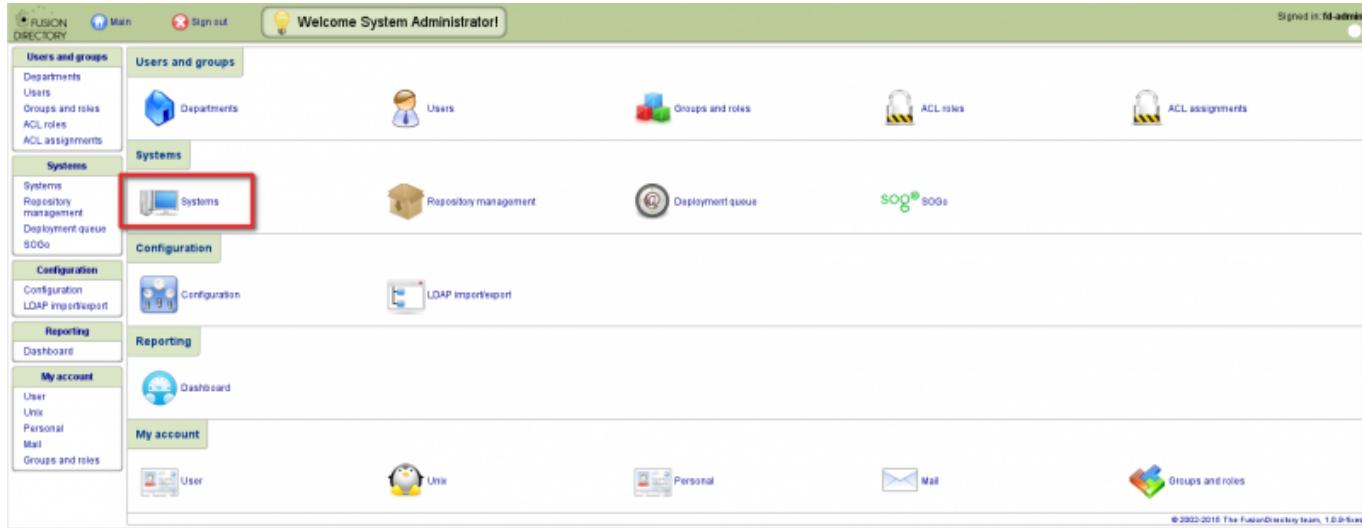
https://documentation.fusiondirectory.org/en/documentation/plugin/dovecot_plugin/installation

Last update: **2016/02/12 21:34**



Add Dovecot service

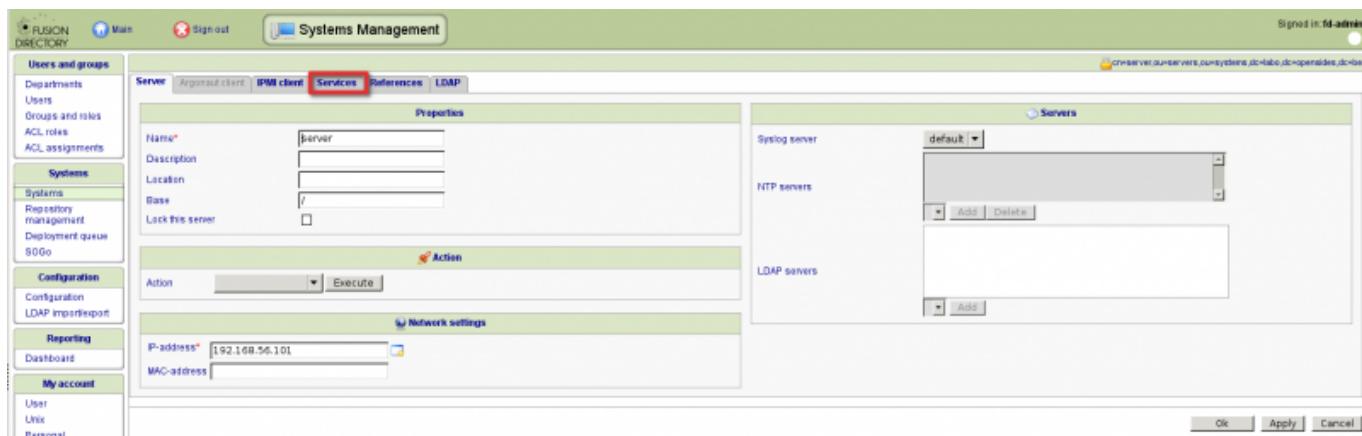
Go to systems



Create your server or edit an server



Click on services tab



Add the Dovecot service

The screenshot shows the 'Systems Management' section of the FusionDirectory web interface. On the left, a sidebar lists various management categories like 'Users and groups', 'Systems', 'Configuration', etc. The 'Services' tab is selected. In the main area, a table lists several services, with 'Dovecot (IMAP/POP3)' highlighted by a red box. A context menu is open over this service, showing options like 'Actions', 'Create', 'Remove', and 'Expandlist'.

Fill the fields for the Dovecot plugin and save it:

- Hostname: the hostname of the server
- Port: port for the connexion
- Option: tls or not
- Validate certificate: if we validate the certificate or not

This screenshot shows the configuration dialog for a Dovecot connection. It has two main sections: 'Dovecot connection' and 'Master credentials'. In the connection section, fields are filled with 'servername' for Hostname, '993' for Port, 'tls' for Option, and 'no-validate' for Validate certificates. In the master credentials section, 'admin' is listed as Admin user and 'passDovecot' as Password. The 'Save' button at the bottom right is highlighted with a red box.

Click on ok to save your server

This screenshot shows the 'List of services' page again. The 'Dovecot (IMAP/POP3)' service is now listed in the table under the 'Description' column. The 'Ok' button at the bottom right of the main area is highlighted with a red box.

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/dovecot_plugin/service

Last update: **2015/10/12 09:33**



Freeradius plugin

- [How to setup the Freeradius plugin](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/freeradius_plugin



Last update: **2014/06/27 21:16**

How to setup Freeradius plugin

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

FreeRADIUS is the most widely deployed RADIUS server in the world.

This plugin is used in the management of freeradius groups and accounts.

Install required packages

debian:

```
apt-get install fusiondirectory-plugin-freeradius
```

RHEL / CentOS:

```
yum install fusiondirectory-plugin-freeradius
```

Install required schemas

debian:

```
apt-get install fusiondirectory-plugin-freeradius-schema  
fusiondirectory-insert-schema -i  
/etc/ldap/schema/fusiondirectory/freeradius.schema
```

RHEL / CentOS:

```
yum install fusiondirectory-plugin-freeradius-schema  
fusiondirectory-insert-schema -i  
/etc/openldap/schema/fusiondirectory/freeradius.schema
```

How to use Freeradius plugin

From now you can create [Freeradius user](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/freeradius_plugin/how_to_setup_freeradius_plugin

Last update: **2016/02/12 21:54**



Ipmi Plugin

- [How to setup Ipmi plugin](#)
- [How add an Ipmi client](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/ipmi_plugin

Last update: **2015/10/15 09:42**



Howto setup Ipmi plugin

How to install GPG plugin

Requirements

- How to setup systems-plugin (since 1.0.5)

Install

Debian

```
apt-get install fusiondirectory-plugin-ipmi
apt-get install fusiondirectory-plugin-ipmi-schema
```

RHEL

```
yum install fusiondirectory-plugin-ipmi
yum install fusiondirectory-plugin-ipmi-schema
```

SLES

```
zypper install fusiondirectory-plugin-ipmi
zypper install fusiondirectory-plugin-ipmi-schema
```

Archlinux

```
yaourt -S fusiondirectory-plugin-ipmi
yaourt -S fusiondirectory-plugin-ipmi-schema
```

Insert schemas

Debian

```
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/ipmi-
fd.schema
```

Others

```
fusiondirectory-insert-schema -i /etc/openldap/schema/fusiondirectory/ipmi-
fd.schema
```

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/ipmi_plugin/how_to_setup

Last update: **2015/10/15 09:28**



How add an Ipmi client

Go to systems

The screenshot shows the Fusion Directory web interface. The left sidebar has sections for 'Users and groups', 'Systems' (which is selected and highlighted with a red box), 'Configuration', 'Reporting', 'Dashboard', and 'My account'. The main content area shows various system management icons: 'Departments', 'Users', 'Groups and roles', 'ACL roles', 'ACL assignments', 'Systems' (with a red box), 'Repository management', 'Deployment queue', 'Configuration', 'LDAP import/export', 'Reporting', 'Dashboard', 'User', 'Unix', 'Personal', and 'Groups and roles'. The top right shows the user is signed in as 'fd.admin'.

Edit or create a new server

The screenshot shows the 'List of systems' page. The left sidebar includes 'Systems' under 'Configuration'. The main area displays a table of systems with columns: Name, IP, MAC, Description, Services, and Release. One row is selected and highlighted with a red box. On the right, there is a 'Filter' sidebar with checkboxes for various system types and a 'Name' search bar.

Click on Ipmi client tab

The screenshot shows the 'Server' configuration page. The left sidebar includes 'Systems' under 'Configuration'. The main area has tabs for 'Server', 'IPMI client' (which is selected and highlighted with a red box), 'Argonaut client', 'Services', 'References', and 'LDAP'. The 'IPMI client' tab shows fields for 'Name' (server), 'Description', 'Location', 'Base', and 'Lock this server'. It also includes sections for 'Action', 'Network settings' (IP-address: 192.168.56.101, MAC-address), and a 'Servers' panel for 'Syslog server', 'NTP servers', and 'LDAP servers'.

Add the Ipmi client tab

The screenshot shows the 'Server' configuration page with tabs for 'Server', 'IPMI client', 'Argonaut client', 'Services', 'References', and 'LDAP'. A message in blue text says: 'This account has IPMI client settings disabled. You can enable them by clicking below.' Below this message is a red button with the text 'Add IPMI client settings'.

Fill IP, user login and user password Click on ok to save it

Signed in as admin

FUSION DIRECTORY Main Sign out Systems Management

Users and groups

Departments

Users

Groups and roles

ACL rules

ACL assignments

Systems

Systems

Repository management

Deployment queue

Configuration

LDAP import/export

Server IPMI client ArgonClient Services References LDAP

This account has IPMI client settings enabled. You can disable them by clicking below.

Remove IPMI client settings

IPMI client settings

IP*: 192.168.56.102

User login*: admin

User password*: *****

Ok Apply Cancel

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/ipmi_plugin/how_add_ipmi_client

Last update: **2015/10/15 09:45**



Pureftpd plugin

- [How to setup the Pureftpd plugin](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/pureftpd_plugin

Last update: **2014/06/27 21:16**



How to setup Pureftpd plugin

This plugin is used to manage pureftpd account inside the LDAP directory.

Requirements

In order to use pureftpd from ldap, you need to install and configure correctly pure-ftpd and pure-ftpd-ldap paquets. If you need some help, see [here](#).

Install required packages

debian

```
apt-get install fusiondirectory-plugin-pureftpd
```

RHEL / CentOS

```
yum install fusiondirectory-plugin-pureftpd
```

Install required schemas

debian

```
apt-get install fusiondirectory-plugin-pureftpd-schema  
fusiondirectory-insert-schema -i  
/etc/ldap/schema/fusiondirectory/pureftpd.schema
```

RHEL / CentOS

```
yum install fusiondirectory-plugin-pureftpd-schema  
fusiondirectory-insert-schema -i  
/etc/openldap/schema/fusiondirectory/pureftpd.schema
```

How to use the Pureftpd plugin

From now you can create [Pureftpd user](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/pureftpd_plugin/how_to_setup_pureftpd_plugin

Last update: **2016/02/12 22:03**



Quota plugin

- How install quota plugin
- How use quota plugin

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/quota_plugin

Last update: **2015/09/21 09:47**



How install quota plugin

Install

Requirements

[How to setup systems plugin](#)

Debian

```
apt-get install fusiondirectory-plugin-quota
```

RHEL

```
yum install fusiondirectory-plugin-quota
```

Suse

```
zypper install fusiondirectory-plugin-quota
```

Archlinux

```
yaourt -S fusiondirectory-plugin-quota
```

Install the schemas and insert it

Debian

```
apt-get install fusiondirectory-plugin-quota-schema  
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/quota*
```

RHEL

```
yum install fusiondirectory-plugin-quota-schema  
fusiondirectory-insert-schema -i /etc/openldap/schema/fusiondirectory/quota*
```

Suse

```
zypper install fusiondirectory-plugin-quota-schema  
fusiondirectory-insert-schema -i /etc/openldap/schema/fusiondirectory/quota*
```

Archlinux

```
yaourt -S fusiondirectory-plugin-quota-schema  
fusiondirectory-insert-schema -i /etc/openldap/schema/fusiondirectory/quota*
```

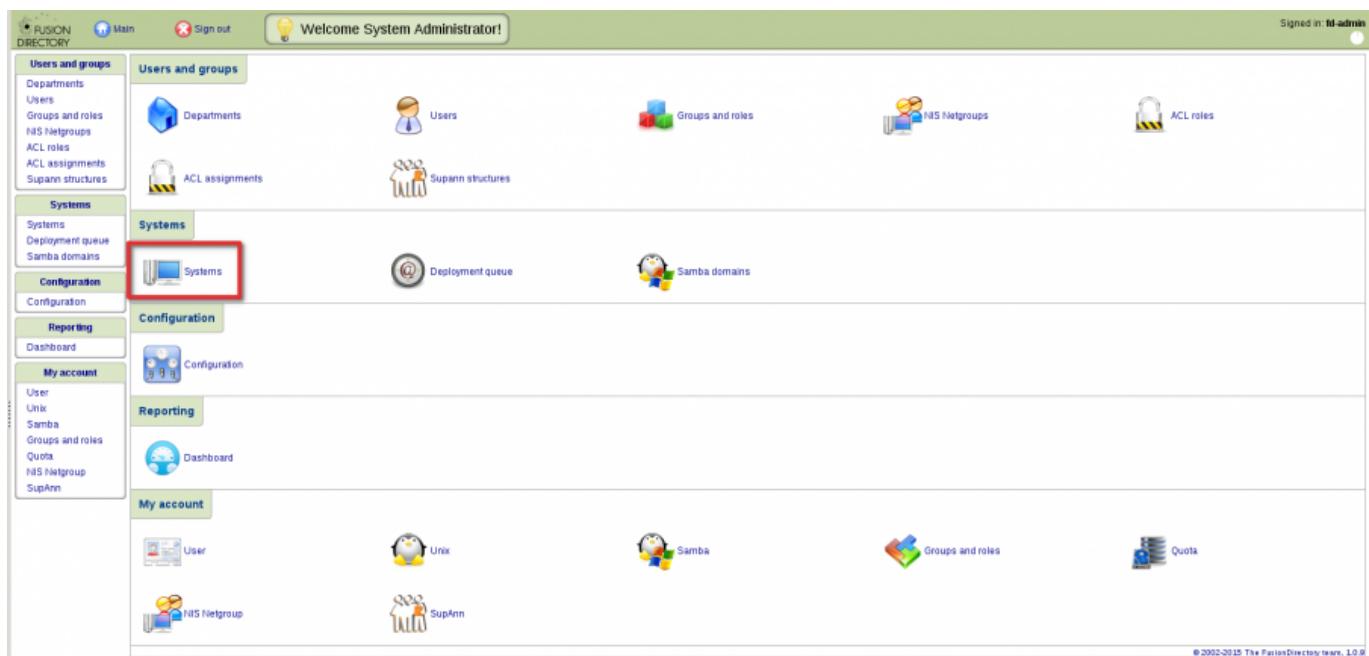
From:
<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:
https://documentation.fusiondirectory.org/en/documentation/plugin/quota_plugin/how_install_quota_plugin

Last update: **2015/09/21 09:45**



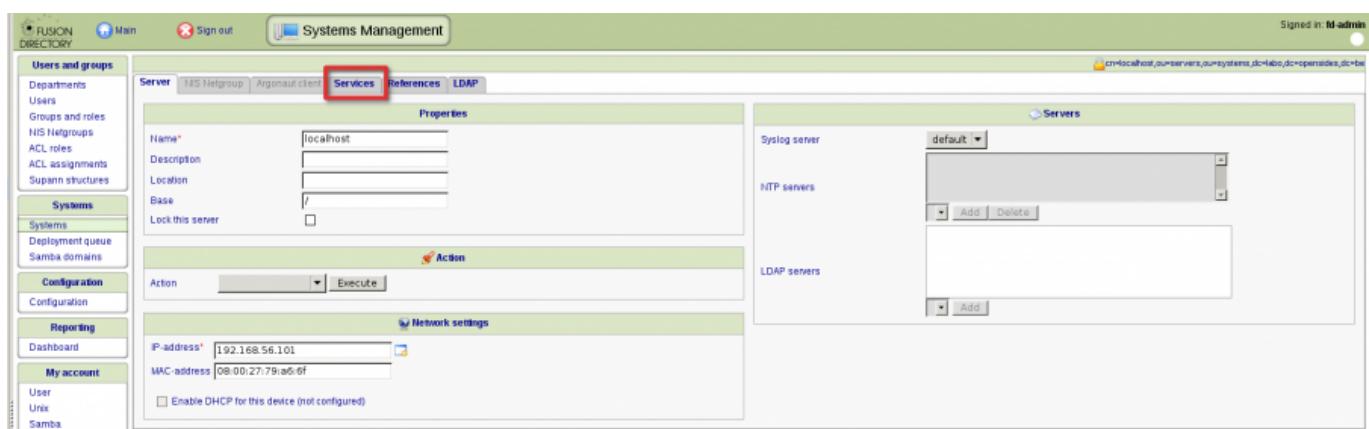
How use quota plugin



Click on systems icon.



Click on the the server where you will add a share, ldap or quota service



Click on the service tab.

To make the plugin quota work, you must have:

- Create share service
- Create ldap service
- Create quota service

You can now create [quota users](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/quota_plugin/how_use_quota_plugin

Last update: **2015/09/21 14:54**



Samba plugin

- [Howto setup Samba plugin](#)
- [Howto create a Samba user](#)
- [Howto create a Samba group](#)
- [Howto create a winstation](#)

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/samba_plugin

Last update: **2015/10/20 13:43**



How to install Samba plugin

Requirements

In order to install samba plugin, you need to have installed and configured Systems plugin. If you don't know how to install him, you can take a look at:

- [How to setup systems-plugin \(since 1.0.5\)](#)

Install

Debian

```
apt-get install fusiondirectory-plugin-samba  
apt-get install fusiondirectory-plugin-samba-schema
```

RHEL

```
yum install fusiondirectory-plugin-samba  
yum install fusiondirectory-plugin-samba-schema
```

SLES

```
zypper install fusiondirectory-plugin-samba  
zypper install fusiondirectory-plugin-samba-schema
```

Archlinux

```
yaourt -S fusiondirectory-plugin-samba  
yaourt -S fusiondirectory-plugin-samba-schema
```

Insert schemas

Debian

```
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/samba-fd-  
conf.schema  
fusiondirectory-insert-schema -i  
/etc/ldap/schema/fusiondirectory/samba.schema
```

Others

```
fusiondirectory-insert-schema -i /etc/openldap/schema/fusiondirectory/samba-fd-conf.schema  
fusiondirectory-insert-schema -i  
/etc/openldap/schema/fusiondirectory/samba.schema
```

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

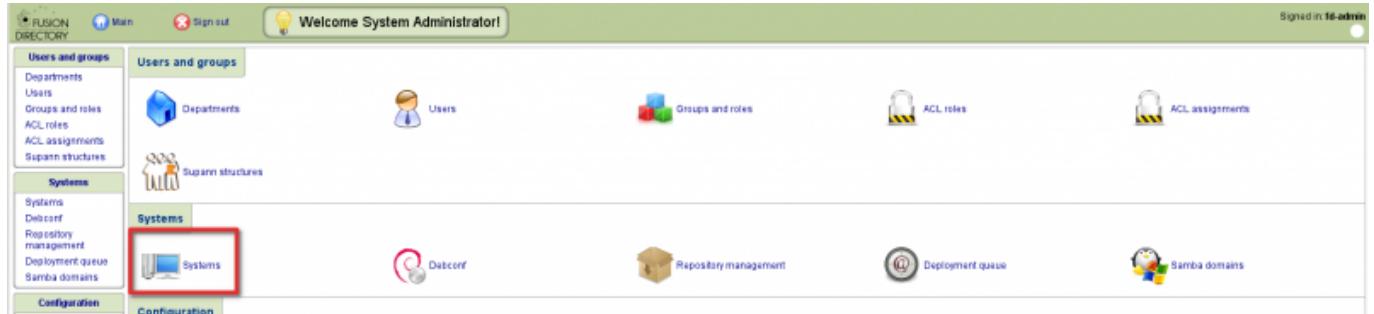
https://documentation.fusiondirectory.org/en/documentation/plugin/samba_plugin/howto_setup_samba_plugin

Last update: **2015/10/20 12:37**

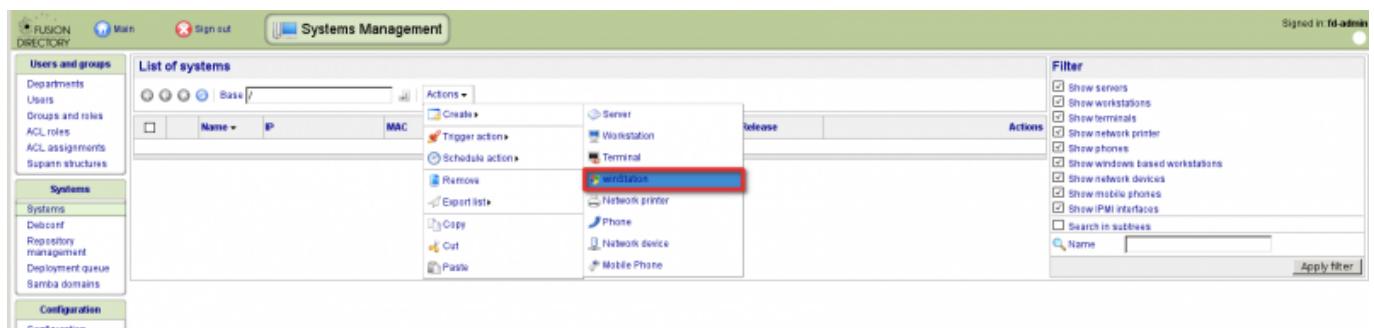


Howto create a winstation

Click on systems



Go to Actions → Create → winstation



Fill all the informations that you need and click on ok

Name*	nameinstation
Description	
Domain*	DOMSMB
Location	
Base	/

Action	<input type="button" value="Execute"/>
--------	--

IP-address*	192.168.56.101
MAC-address*	00:0C:7F:31:33:F1

Your winstation is create

The screenshot shows the 'Systems Management' section of the FusionDirectory web interface. On the left, a sidebar lists 'Users and groups' with options like 'Departments', 'Users', 'Groups and roles', 'ACL rules', 'ACL assignments', and 'Supann structures'. The main area is titled 'List of systems' and contains a table with columns: Name, IP, MAC, Description, Services, and Release. A single row is selected, highlighted with a red border, showing the entry 'namewinstation\$' with IP '192.168.56.101' and MAC '00:0C:7F:31:33:F1'. To the right of the table is a 'Filter' panel with several checkboxes: 'Show servers' (unchecked), 'Show workstations' (checked), 'Show terminals' (unchecked), 'Show network printer' (unchecked), 'Show phones' (unchecked), 'Show windows based workstations' (unchecked), and 'Show nonwindows workstations' (unchecked). At the bottom of the table area, there is a toolbar with icons for actions like edit, delete, and search.

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/samba_plugin/create_a_winstation

Last update: **2015/10/20 14:00**



Squid plugin

- How to setup the Squid plugin

From:

<https://documentation.fusiondirectory.org/> - FusionDirectory Documentation

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/squid_plugin

Last update: **2014/06/27 21:16**



How to setup Squid plugin

The Squid plugin provides management for squid proxy users in your infrastructures.

Install required packages

debian

```
apt-get install fusiondirectory-plugin-squid
```

RHEL / CentOS

```
yum install fusiondirectory-plugin-squid
```

Install required schemas

debian

```
apt-get install fusiondirectory-plugin-squid-schema  
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/proxy-  
fd.schema
```

RHEL / CentOS

```
yum install fusiondirectory-plugin-squid-schema  
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/proxy-  
fd.schema
```

How to use Squid plugin

From now you can create [Squid user](#)

From:
<https://documentation.fusiondirectory.org/> - FusionDirectory Documentation

Permanent link:
https://documentation.fusiondirectory.org/en/documentation/plugin/squid_plugin/how_to_setup_squid_plugin

Last update: **2016/02/12 22:06**



SSH plugin

- How to setup the SSH plugin

From:

<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:

https://documentation.fusiondirectory.org/en/documentation/plugin/ssh_plugin

Last update: **2014/06/27 21:16**



How to setup SSH plugin

The SSH plugin provides management for ssh public key in your infrastructures.

Install required packages

debian

```
apt-get install fusiondirectory-plugin-ssh
```

RHEL / CentOS

```
yum install fusiondirectory-plugin-ssh
```

Install required schemas

debian

```
apt-get install fusiondirectory-plugin-ssh-schema  
fusiondirectory-insert-schema -i /etc/ldap/schema/fusiondirectory/openssh-lpk.schema
```

RHEL / CentOS

```
yum install fusiondirectory-plugin-ssh-schema  
fusiondirectory-insert-schema -i  
/etc/openldap/schema/fusiondirectory/openssh-lpk.schema
```

How to use SSH plugin

From now you can create [SSH user](#)

From:
<https://documentation.fusiondirectory.org/> - **FusionDirectory Documentation**

Permanent link:
https://documentation.fusiondirectory.org/en/documentation/plugin/ssh_plugin/how_to_setup_ssh_plugin

Last update: **2016/02/12 22:07**

