Version 4.01.102208

ARTICA v4.x DOCUMENTATION

DRAFT UNDER CONSTRUCTION

TABLE OF CONTENTS

INSTALLING ARTICA

REQUIREMENTS

Artica 4 is compatible **Debian 9.x on a 64-bit system i686**.
Product **is not compatible** with ARM systems and on Redhat families systems (CentOS, Fedora, Red Hat, Open SuSe **are not supported**).

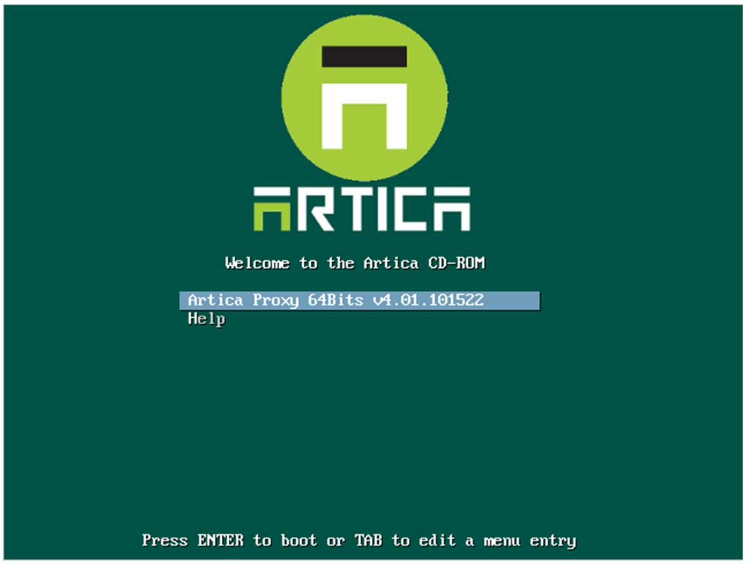
Product is “Virtualization aware” . It can be installed on modern virtualization systems such as VMWare ESXi, Microsoft HyperV, Citrix XenServer, Nutanix, KVM, Proxmox…

To install Artica, you have 2 ways:

USING THE ISO

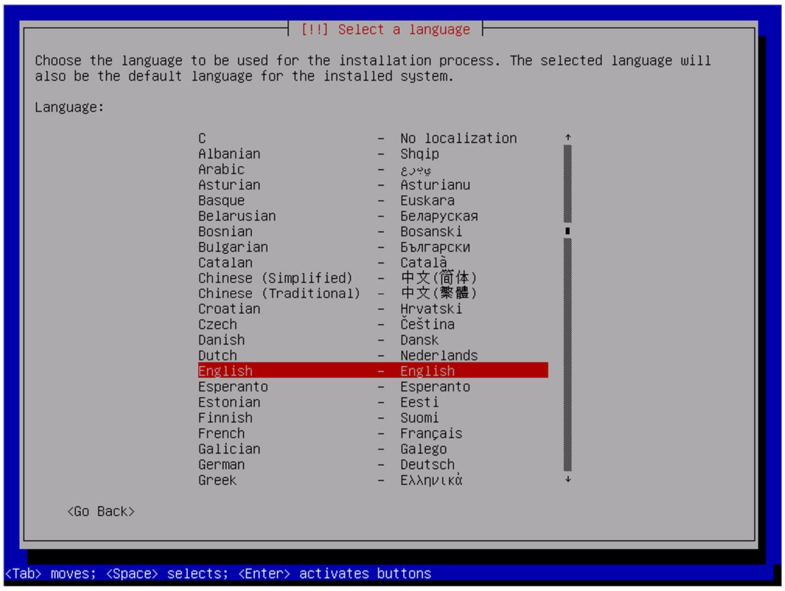
Download the ISO file at http://articatech.net/betas4.php
The ISO file has been tested in both physical servers and virtual environment (ESXi, HyperV, XenServer, Nutanix, KVM).
The ISO is in charge to install both the system and Artica framework, in all environments, the procedure is the same.

Boot from the ISO, a welcome screen must appear



```
Welcome to the Artica CD-ROM

Artica Proxy 64Bits v4.01.101522
Help

Press ENTER to boot or TAB to edit a menu entry
```

Select your system language, country and the language of the keyboard.

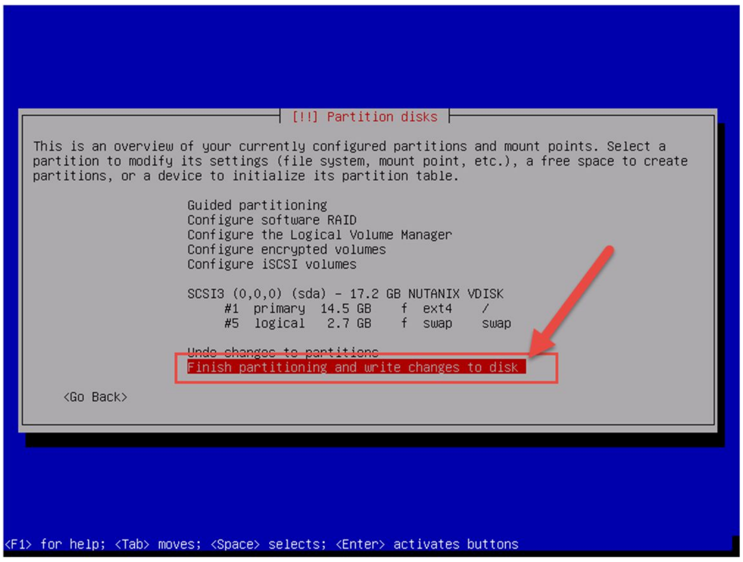


```
[!!] Select a language

Choose the language to be used for the installation process. The selected language will
also be the default language for the installed system.

Language:

                     C                        -  No localization
                     Albanian                 -  Shqip
                     Arabic                   -  عربي
                     Asturian                 -  Asturianu
                     Basque                   -  Euskara
                     Belarusian               -  Беларуская
                     Bosnian                  -  Bosanski
                     Bulgarian                -  Български
                     Catalan                  -  Català
                     Chinese (Simplified)     -  中文(简体)
                     Chinese (Traditional)    -  中文(繁體)
                     Croatian                 -  Hrvatski
                     Czech                    -  Čeština
                     Danish                   -  Dansk
                     Dutch                    -  Nederlands
                     English                  -  English
                     Esperanto                -  Esperanto
                     Estonian                 -  Eesti
                     Finnish                  -  Suomi
                     French                   -  Français
                     Galician                 -  Galego
                     German                   -  Deutsch
                     Greek                    -  Ελληνικά

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

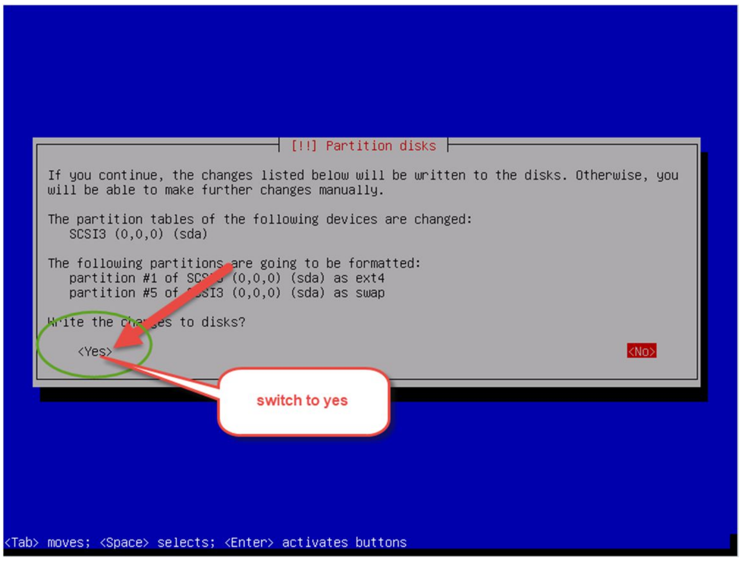
The ISO installer is DHCP client by default it will try to find an IP address through the DHCP. If there is no DHCP, it will ask to enter the IP address.

The TCP settings will not be saved after the reboot, you will have to re-enter it after the reboot.

By default, the install tool will create system partitions, just approve it automatically by type Enter key on the "**Finish partitioning and write changes to disk.**"



```
[!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                    Guided partitioning
                    Configure software RAID
                    Configure the Logical Volume Manager
                    Configure encrypted volumes
                    Configure iSCSI volumes

                    SCSI3 (0,0,0) (sda) - 17.2 GB NUTANIX VDISK
                         #1  primary  14.5 GB    f  ext4    /
                         #5  logical   2.7 GB    f  swap    swap

                    Undo changes to partitions
                    Finish partitioning and write changes to disk

    <Go Back>

<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons
```

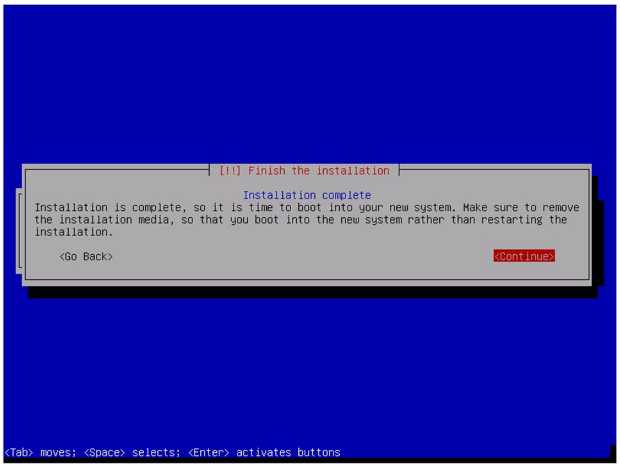


```
[!!] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you
will be able to make further changes manually.

The partition tables of the following devices are changed:
   SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
   partition #1 of SCSI3 (0,0,0) (sda) as ext4
   partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

    <Yes>                                                              <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

switch to yes

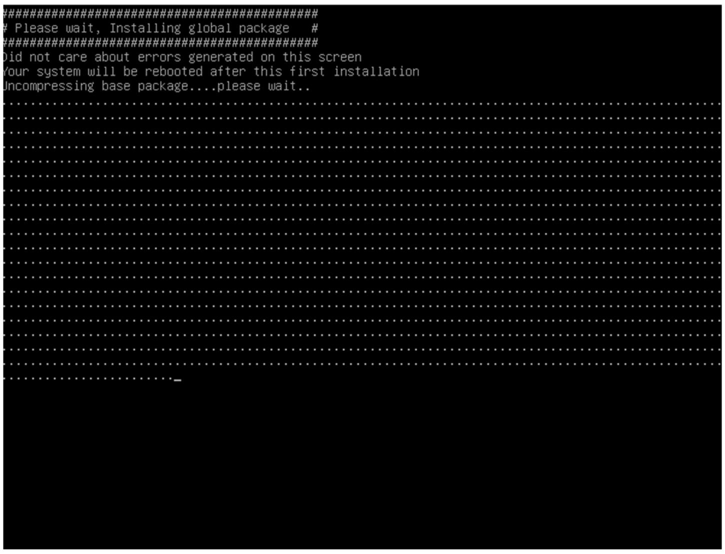
Confirm the disk format task by the switch from No to yes

Wait during the installation packages task.



```
[!!] Finish the installation

Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove
the installation media, so that you boot into the new system rather than restarting the
installation.

<Go Back>                                                                   <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

At the end of the installation, type Enter key to continue message in order to reboot the server.



```
############################################
# Please wait, Installing global package   #
############################################
Did not care about errors generated on this screen
Your system will be rebooted after this first installation
Uncompressing base package....please wait..
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
....................................................................................................
........................_
```

During the first boot, Artica is extracted and installed on the system

The computer will be rebooted again.

USING THE INSTALL SCRIPT.

You must understand that Artica is a product that skin, modify the Linux system according to its needs.
It is not intended to install Artica on an already production server.
Uninstalling of Artica is not possible.

If you need to install Artica on an already Debian 9 system, you can use this procedure:
Open a terminal on your installed system.
Run these commands:

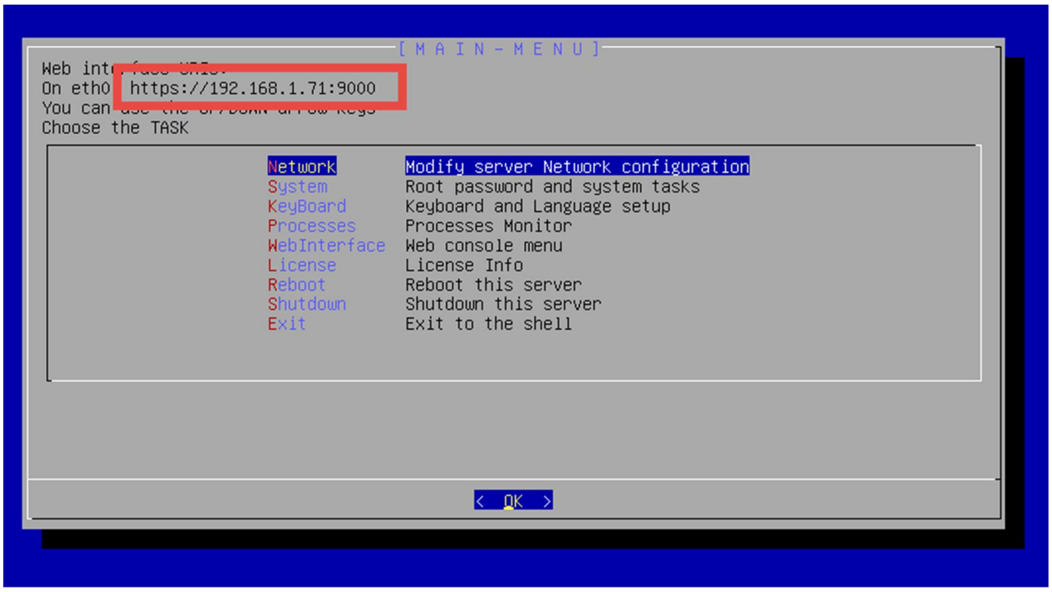
```
wget http://articatech.net/download/v4/install-manuall.sh
chmod 0755 install-manuall.sh
./install-manuall.sh
```

The install-manuall script will be able to download and install all the required packages.

After installing all packages, reboot the system

THE MENU CONSOLE.

After the installation and on each reboot, a menu console is displayed.
This menu allows you to modify the network configuration, change passwords and set the keyboard language.
On the TOP-left section, the console displays the address to open the Artica Web console



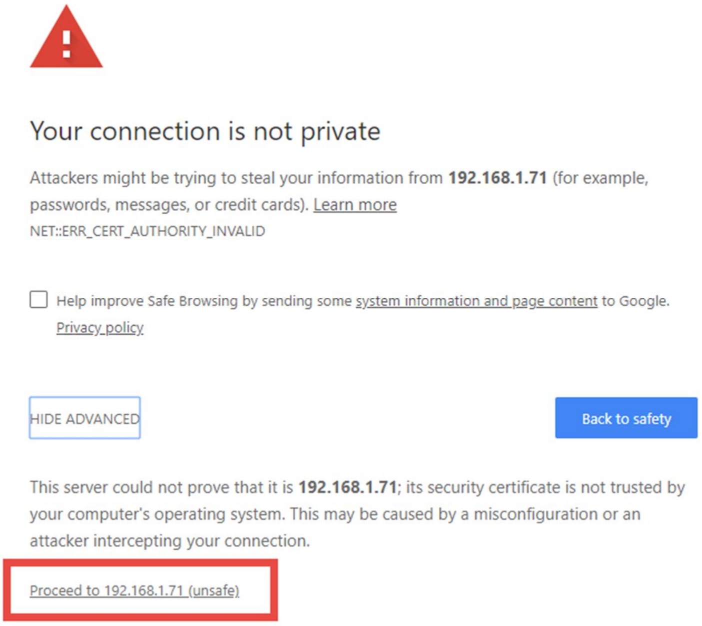
```
[ M A I N - M E N U ]
Web interface URIs:
On eth0  https://192.168.1.71:9000
You can use the UP/DOWN arrow keys
Choose the TASK

          Network        Modify server Network configuration
          System         Root password and system tasks
          KeyBoard       Keyboard and Language setup
          Processes      Processes Monitor
          WebInterface   Web console menu
          License        License Info
          Reboot         Reboot this server
          Shutdown       Shutdown this server
          Exit           Exit to the shell

                    < OK >
```

THE WIZARD

After connecting to the default web page (https://your-server-address:9000) a browser alert is displayed.

This behavior is normal because the certificate generated by Artica is a self-signed certificate.

Ask to the browser to continue anyway.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.71** (for example, passwords, messages, or credit cards). Learn more

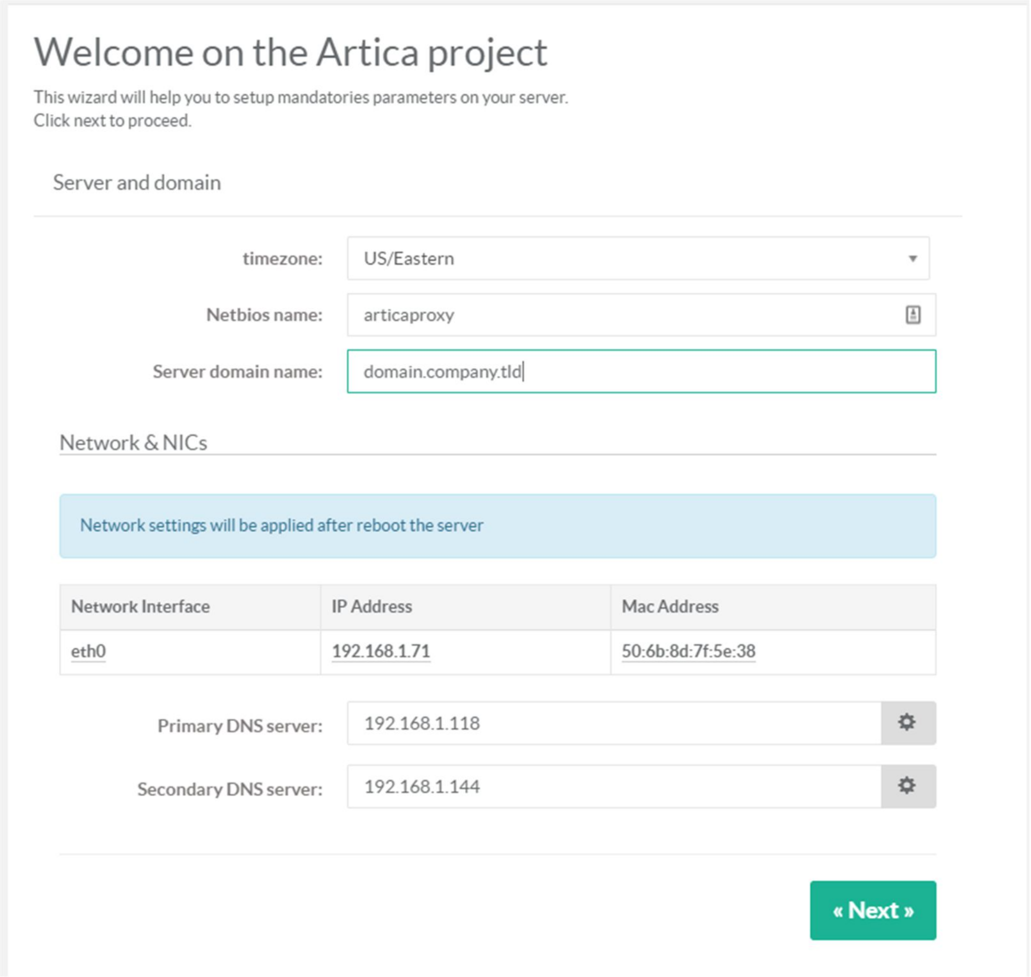
NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **192.168.1.71**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.71 (unsafe)

The first wizard page needs you to confirm network parameters such as host name, DNS, network interfaces parameters.



Welcome on the Artica project

This wizard will help you to setup mandatories parameters on your server.
Click next to proceed.

Server and domain

timezone: US/Eastern

Netbios name: articaproxy

Server domain name: domain.company.tld

Network & NICs

Network settings will be applied after reboot the server

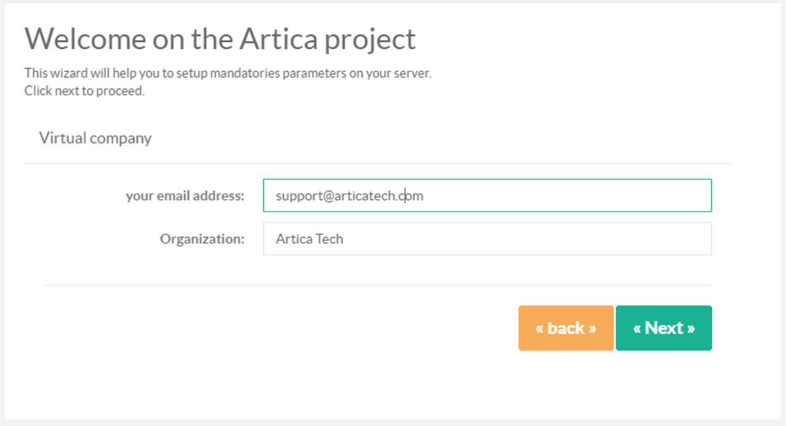
Network Interface	IP Address	Mac Address
eth0	192.168.1.71	50:6b:8d:7f:5e:38

Primary DNS server: 192.168.1.118

Secondary DNS server: 192.168.1.144

The second step will ask you a “**Virtual information**” such as:

1) The eMail address that will be used by default on all services that require to inform an Administrator.
2) The Organization (company name) that will be displayed in the login screen and on some elements that communicate with your users.



Welcome on the Artica project

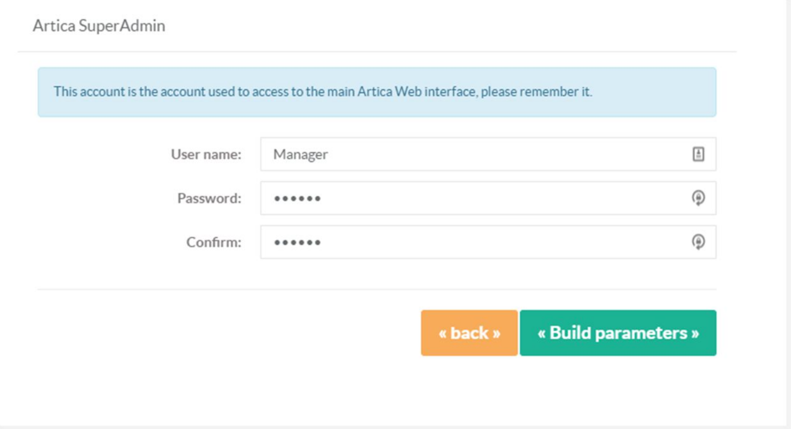
This wizard will help you to setup mandatories parameters on your server.
Click next to proceed.

Virtual company

your email address: support@articatech.com

Organization: Artica Tech

The final step allows you to define the “**Manager**” account username and password.
The Manager account is a Super-Administrator that has full right on the system (except SSH service)



Artica SuperAdmin

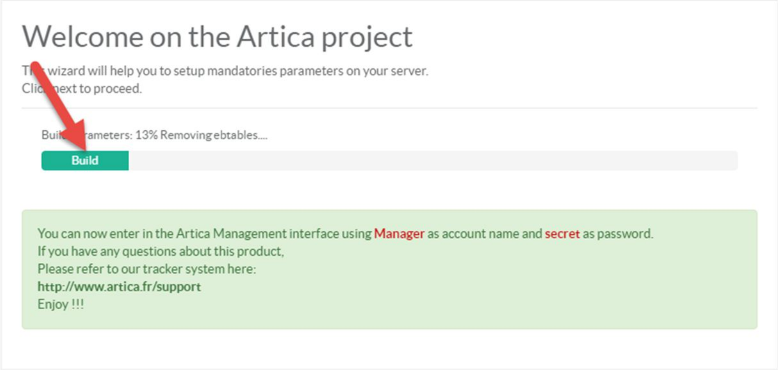
This account is the account used to access to the main Artica Web interface, please remember it.

User name: Manager

Password: ••••••

Confirm: ••••••

After clicking on the “**Build parameters**” button, a progress bar shows you the installation progress of your new Artica server.



Welcome on the Artica project

Th wizard will help you to setup mandatories parameters on your server.
Clic next to proceed.

Buil rameters: 13% Removing ebtables....

You can now enter in the Artica Management interface using Manager as account name and secret as password.
If you have any questions about this product,
Please refer to our tracker system here:
http://www.artica.fr/support
Enjoy !!!

After the installation, you will be redirected to the login screen.

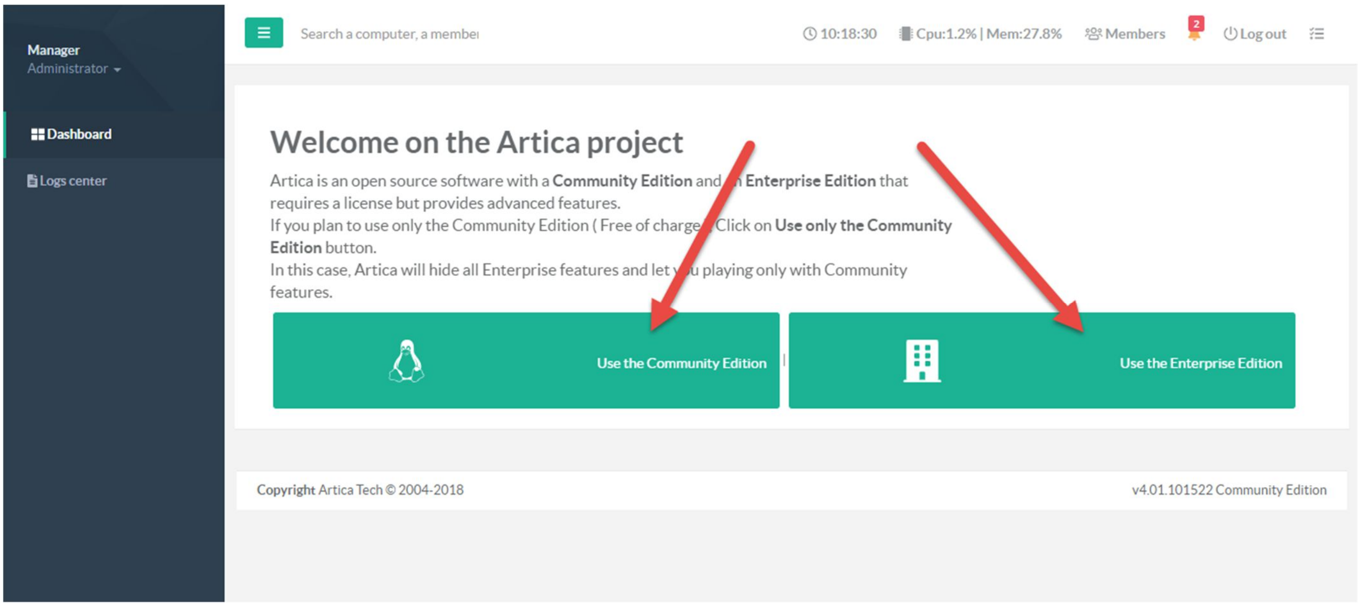
COMMUNITY OR ENTERPRISE EDITION?

After logins for the first time the Artica Web console ask to you if you want to use Artica in Community Edition or Enterprise Edition.

The difference between the Enterprise and Community edition is the Community Edition is “Enterprise Features” limited. Some components or some options will not be available in Community Edition.
The Community Edition is free of charge and will never expire.
A licensed Artica server can run Enterprise features with a subscription.
When the Enterprise License period is expired, the Artica server will automatically return back to the Community Edition.

In any cases, Artica will never shut down a main service for an expired Enterprise license.

The whole documentation specifies if the feature is available only with Enterprise License



Welcome on the Artica project

Artica is an open source software with a **Community Edition** and an **Enterprise Edition** that requires a license but provides advanced features.
If you plan to use only the Community Edition (Free of charge) Click on **Use only the Community Edition** button.
In this case, Artica will hide all Enterprise features and let you playing only with Community features.

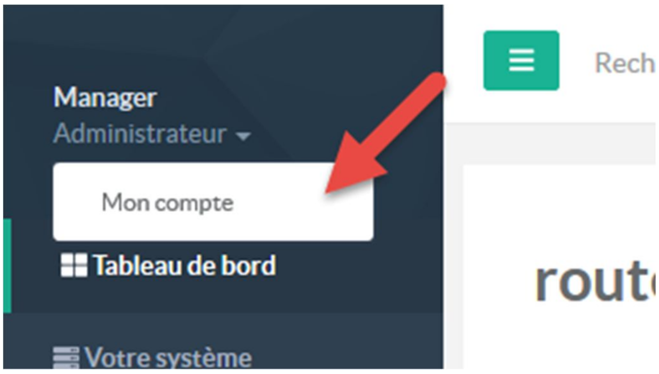
Copyright Artica Tech © 2004-2018

v4.01.101522 Community Edition

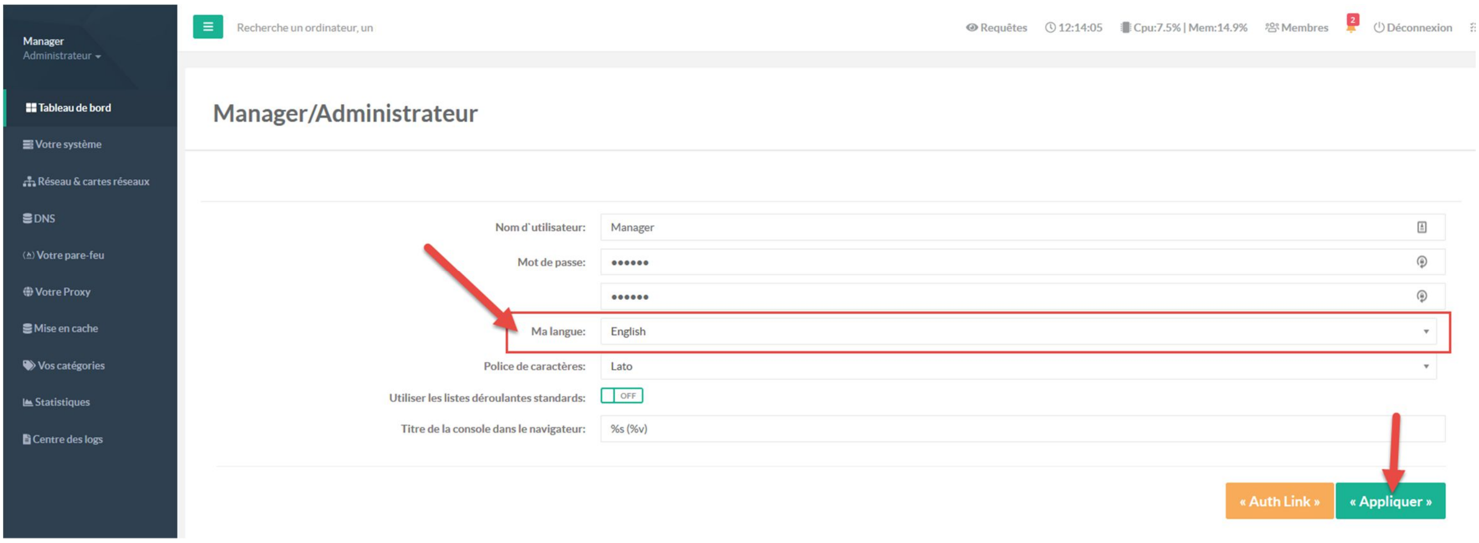
ARTICA WEB CONSOLE

CHANGE THE WEB CONSOLE LANGUAGE

Language can be modified by created account.
After logging on the Web console
On the left menu click on the member name.



On the “language” drop-down list, select the desired language and click on apply button



Manager/Administrateur

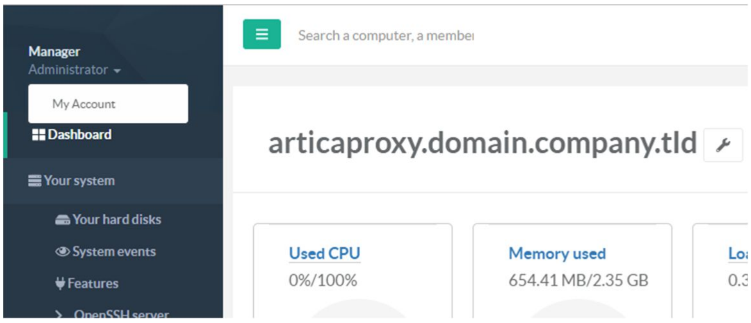
Nom d'utilisateur: Manager
Mot de passe: ••••••
••••••
Ma langue: English
Police de caractères: Lato
Utiliser les listes déroulantes standards: OFF
Titre de la console dans le navigateur: %s (%v)

(Not all parts of the web page will be modified, if you want to change all the web page part, click on the F5 key in order to refresh totally the web console.)

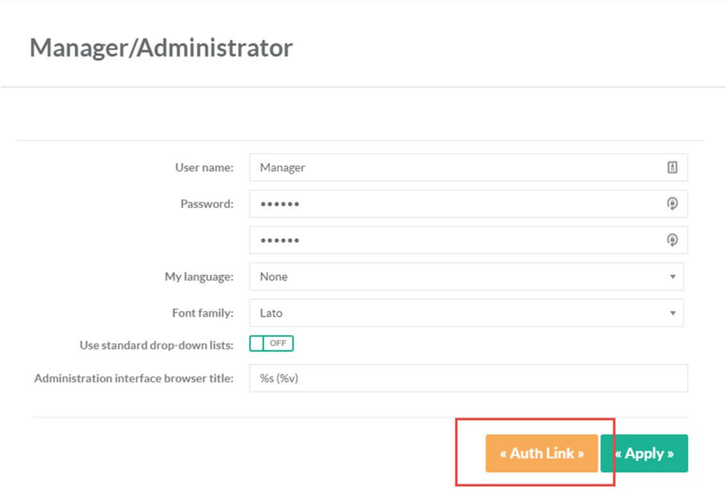
AUTH LINK

AUTH Link allows you to enter the Artica Web console without need to login. It creates a link that automatically sends your credentials to the Artica system.

On the left menu, open **Your Account**



Select the button "**Auth Link**"



Manager/Administrator

User name: Manager

Password: ••••••

••••••

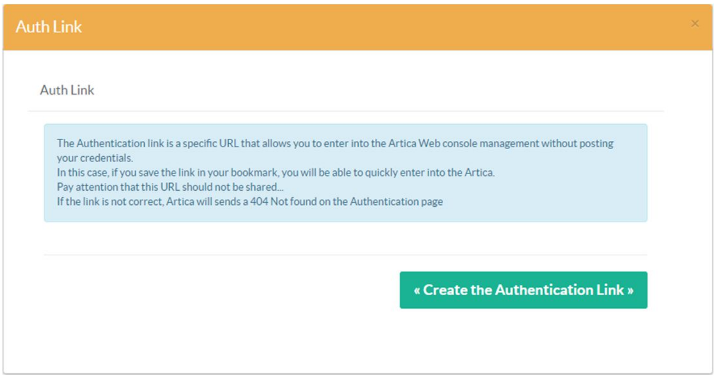
My language: None

Font family: Lato

Use standard drop-down lists: OFF

Administration interface browser title: %s (%v)

Click on the button "**Create the Authentication Link.**"

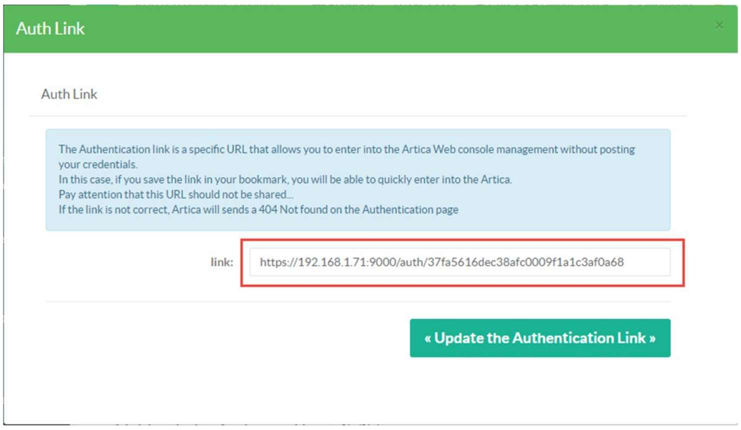


Auth Link

Auth Link

The Authentication link is a specific URL that allows you to enter into the Artica Web console management without posting your credentials.
In this case, if you save the link in your bookmark, you will be able to quickly enter into the Artica.
Pay attention that this URL should not be shared...
If the link is not correct, Artica will sends a 404 Not found on the Authentication page

Copy the link, disconnect from the console and type this new link on your browser, you will be logged automatically.



Auth Link

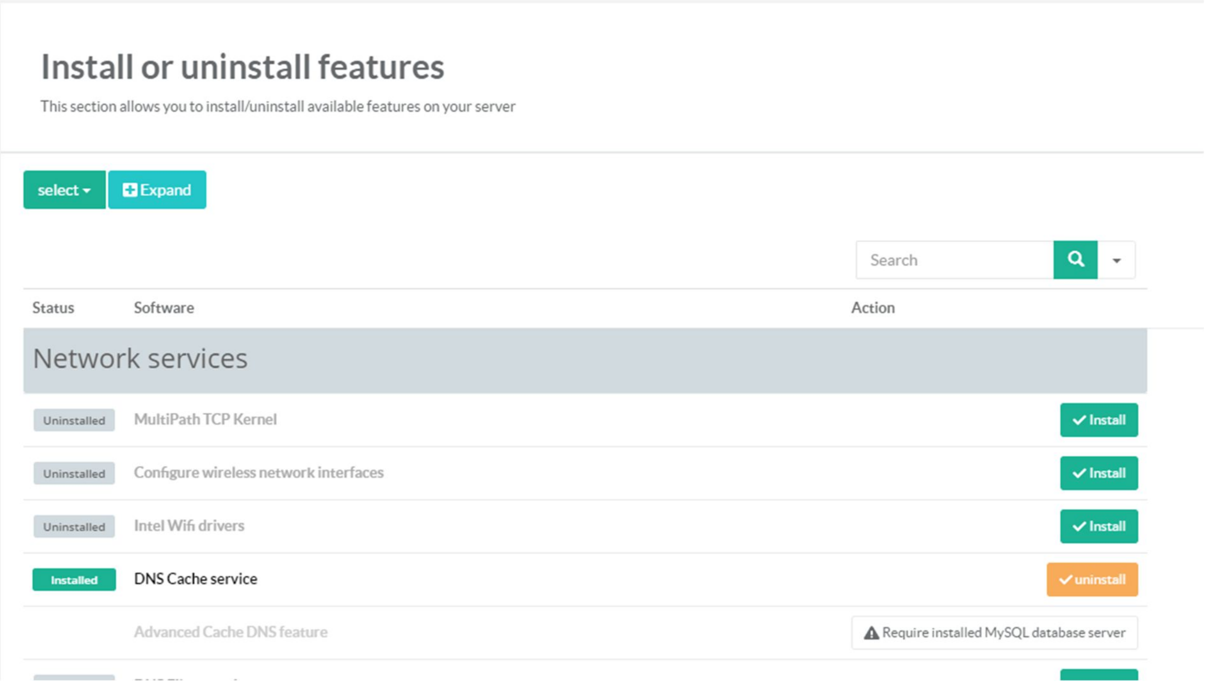
Auth Link

The Authentication link is a specific URL that allows you to enter into the Artica Web console management without posting your credentials.
In this case, if you save the link in your bookmark, you will be able to quickly enter into the Artica.
Pay attention that this URL should not be shared...
If the link is not correct, Artica will sends a 404 Not found on the Authentication page

link: https://192.168.1.71:9000/auth/37fa5616dec38afc0009f1a1c3af0a68

The Features section

The features section (located in “Your System/Features”) is the central point that helps you to create your Artica server behavior. It lists the available software that can be installed and managed on your system.

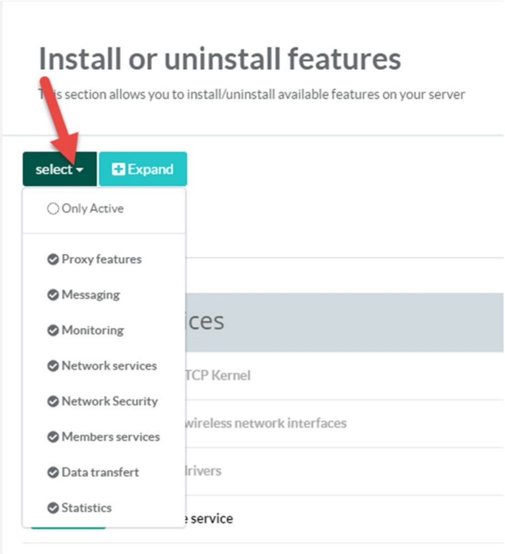


Install or uninstall features

This section allows you to install/uninstall available features on your server

Status	Software	Action
Network services		
Uninstalled	MultiPath TCP Kernel	✓ Install
Uninstalled	Configure wireless network interfaces	✓ Install
Uninstalled	Intel Wifi drivers	✓ Install
Installed	DNS Cache service	✓ uninstall
	Advanced Cache DNS feature	⚠ Require installed MySQL database server

The table store 8 features you can filter with the “select” button:



Install or uninstall features

T is section allows you to install/uninstall available features on your server

Proxy features: Is the main part of the HTTP/SQL/Load-balancing proxy and can switch your server to an “Artica Proxy” server.
You will find here the Web-filtering feature, the Web-application-Firewall feature…

Messaging: Is the main part of the SMTP/IMAP service that can switch your server to an SMTP relay with Anti-SPAM and mailboxes servers.

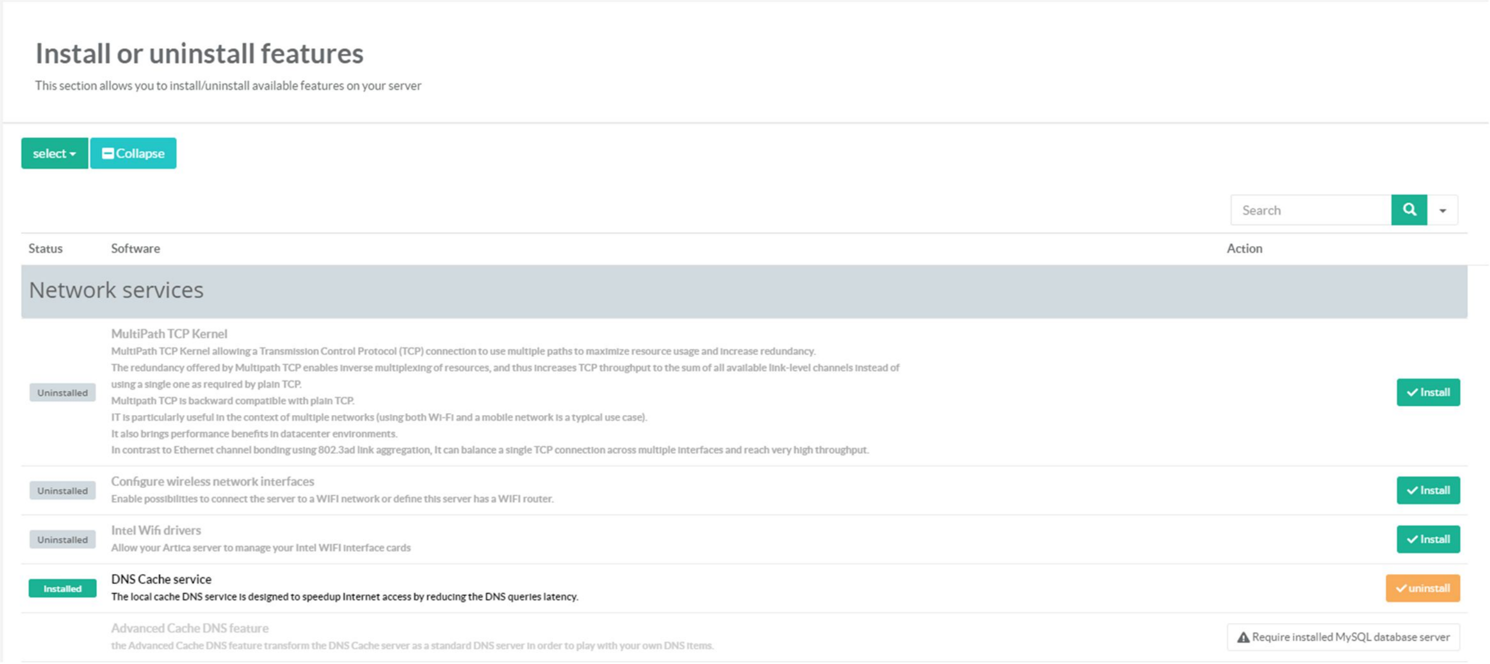
Monitoring: Allows you to install service to help you monitor your Artica server performance.

Network service: Allows you to install all services related to a gateway such, the DHCP service, the DNS service, the reverse and Web service, the VPN service…

Network security: Allows to securize a network or the Artica Network with the Firewall, the Universal Proxy server,the antivirus, the IDS…

Members services: Allows you to install “Members databases” such has MySQL service and the local OpenLDAP database.

The expand button allows you to display a description of each available service.



Install or uninstall features

This section allows you to install/uninstall available features on your server

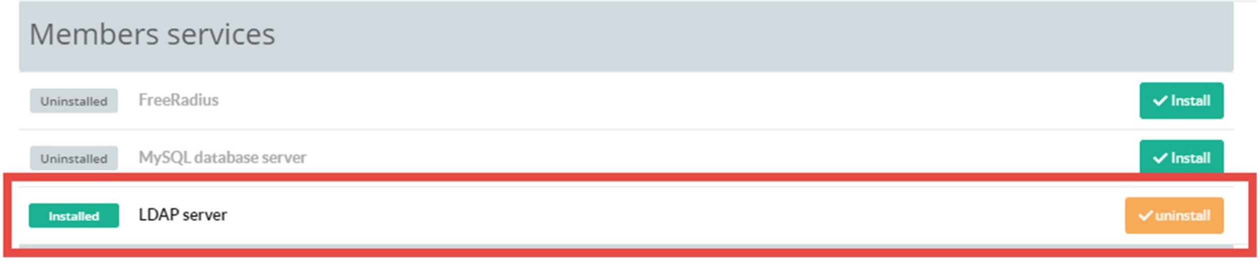
Status	Software	Action
	Network services	
Uninstalled	MultiPath TCP Kernel MultiPath TCP Kernel allowing a Transmission Control Protocol (TCP) connection to use multiple paths to maximize resource usage and increase redundancy. The redundancy offered by Multipath TCP enables inverse multiplexing of resources, and thus increases TCP throughput to the sum of all available link-level channels instead of using a single one as required by plain TCP. Multipath TCP is backward compatible with plain TCP. IT is particularly useful in the context of multiple networks (using both Wi-Fi and a mobile network is a typical use case). It also brings performance benefits in datacenter environments. In contrast to Ethernet channel bonding using 802.3ad link aggregation, It can balance a single TCP connection across multiple interfaces and reach very high throughput.	✓ Install
Uninstalled	Configure wireless network interfaces Enable possibilities to connect the server to a WIFI network or define this server has a WIFI router.	✓ Install
Uninstalled	Intel Wifi drivers Allow your Artica server to manage your Intel WIFI interface cards	✓ Install
Installed	DNS Cache service The local cache DNS service is designed to speedup Internet access by reducing the DNS queries latency.	✓ uninstall
	Advanced Cache DNS feature the Advanced Cache DNS feature transform the DNS Cache server as a standard DNS server in order to play with your own DNS items.	⚠ Require installed MySQL database server

The expanded table display a description of each available service.

THE LDAP SERVER SERVICE

The LDAP database is used by Artica in order to manage members. This database can be used by the proxy service (see LDAP Authentication), the messaging service, the file-sharing service and the Artica Web console itself to manage administrators privileges.

The LDAP service can be installed in the Features section (see The Features section) in “Members services/LDAP Server.”

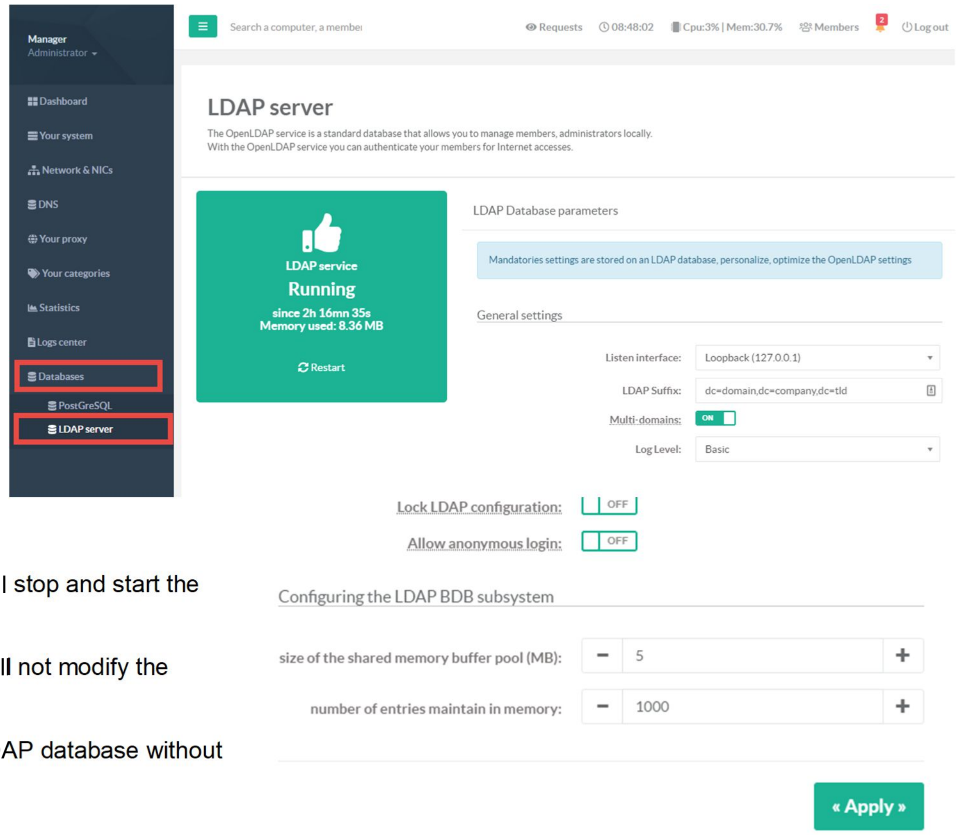


Members services

Uninstalled	FreeRadius	✓ Install
Uninstalled	MySQL database server	✓ Install
Installed	LDAP server	✓ uninstall

OpenLDAP service parameters.

Main settings of the LDAP service can be displayed on the left menu “**Databases/LDAP server**.”



LDAP server

The OpenLDAP service is a standard database that allows you to manage members, administrators locally.
With the OpenLDAP service you can authenticate your members for Internet accesses.

LDAP service
Running
since 2h 16mn 35s
Memory used: 8.36 MB
Restart

LDAP Database parameters

Mandatories settings are stored on an LDAP database, personalize, optimize the OpenLDAP settings

General settings

Listen interface: Loopback (127.0.0.1)

LDAP Suffix: dc=domain,dc=company,dc=tld

Multi-domains: ON

Log Level: Basic

Lock LDAP configuration: OFF

Allow anonymous login: OFF

Configuring the LDAP BDB subsystem

size of the shared memory buffer pool (MB): 5

number of entries maintain in memory: 1000

« Apply »

Listen Interface: By default the LDAP server serves only the loop back address because all services used by Artica don’t need to access the database externally

LDAP suffix: Is the main LDAP branch used to store users

Multi-Domains: If enabled, Artica will use the eMail address has the login username. In this case, users need to put their eMail address to log in to all services that use LDAP.

Log level: is the trace level used for the LDAP service (logs are stored in syslog)

Restart periodically OpenLDAP service: If turned on then Artica will restart OpenLDAP service at 6h30,12h30,3h30

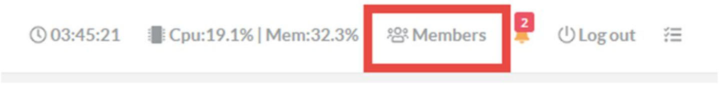
Restart service each: Define the period that will stop and start the LDAP service in order to refresh memory.

Lock LDAP configuration: If enabled, Artica will not modify the /etc/ldap/slpad.conf and let you change it.

Allow anonymous login: Permit to read the LDAP database without need to be logged as a member.

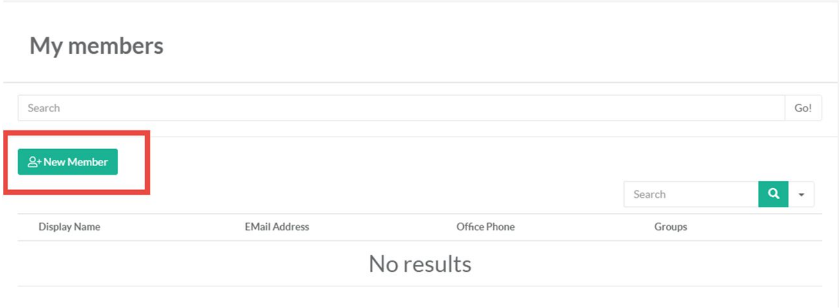
MANAGE LDAP MEMBERS/GROUP

On the TOP menu, you will find a link called “Members” that allows you to manage Members items.



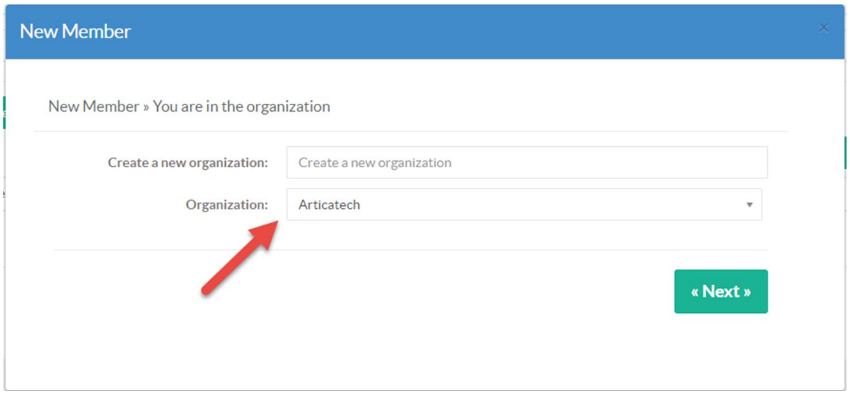
A table is displayed and allows you to search for members and groups.

to create a user, click on the button “New member”



Display Name	EMail Address	Office Phone	Groups
No results			

A wizard is displayed and ask to you in which organization the member must be stored.
You can choose in the drop-down list an already organization or you can create a new organization by adding the new organization name in the “Create a new organization” field.

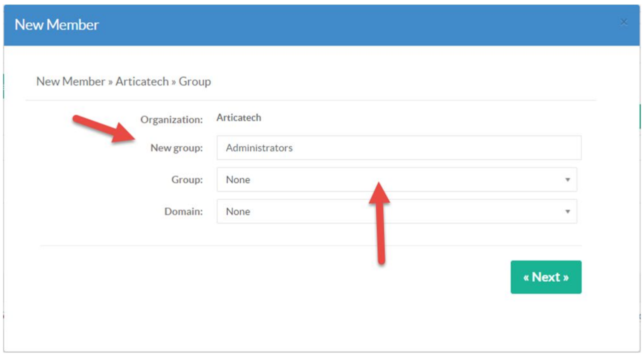


New Member » You are in the organization

Create a new organization: Create a new organization

Organization: Articatech

Define the group that will store the user
You can create a new group. Set the group name in the “new group” field or select an already created group by choosing it in the “Group” drop-down list.



New Member » Articatech » Group

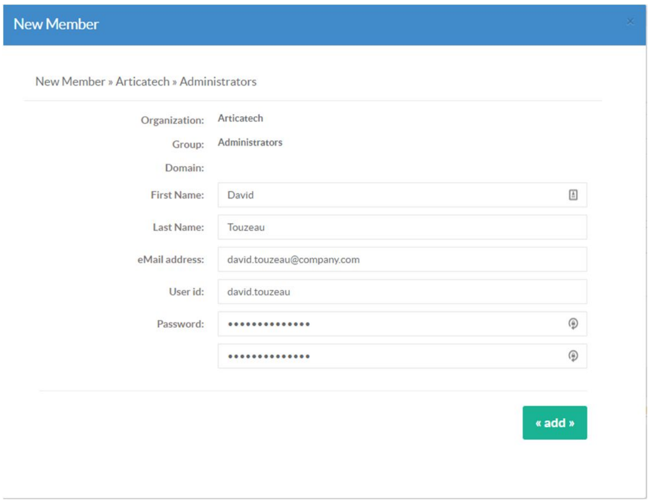
Organization: Articatech

New group: Administrators

Group: None

Domain: None

- Set the first name and last name of the new member.
- Set the email address
- **The user id:** is the account that the user will use to be logged on services that use LDAP authentication.
  If you did not see this field, it means the login name using the eMail address.
- Set the user password.



New Member

New Member » Articatech » Administrators

Organization: Articatech

Group: Administrators

Domain:

First Name: David

Last Name: Touzeau

eMail address: david.touzeau@company.com

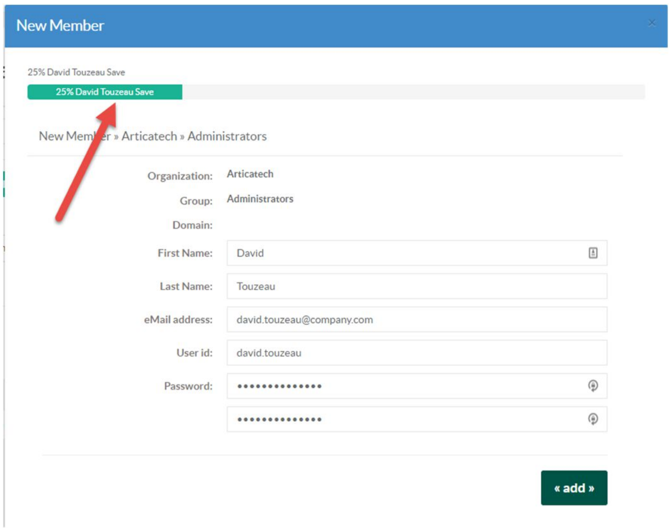
User id: david.touzeau

Password: ••••••••••••••

••••••••••••••

By default the LDAP database is OpenLDAP service parameters.enabled (SEE OPENLDAP SERVICE PARAMETERS.) That enables the eMail address has the login user.

After click on the Add button, a progress bar is displayed that shows you the progress of creating the user.



New Member

25% David Touzeau Save

25% David Touzeau Save

New Member » Articatech » Administrators

Organization: Articatech

Group: Administrators

Domain:

First Name: David

Last Name: Touzeau

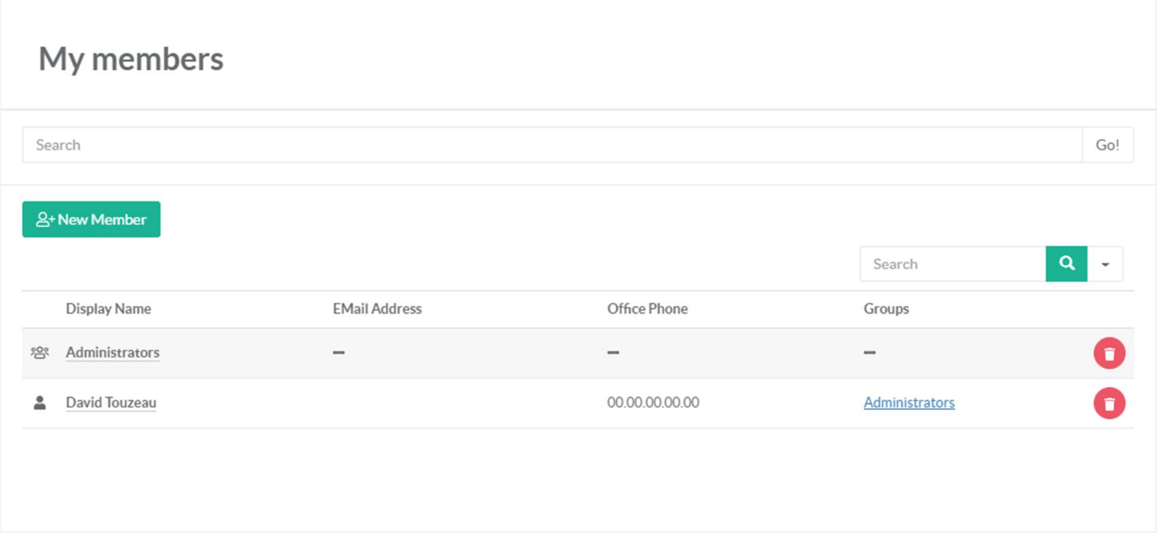
eMail address: david.touzeau@company.com

User id: david.touzeau

Password: ••••••••••••••

••••••••••••••

The table will display your new member and the created group.

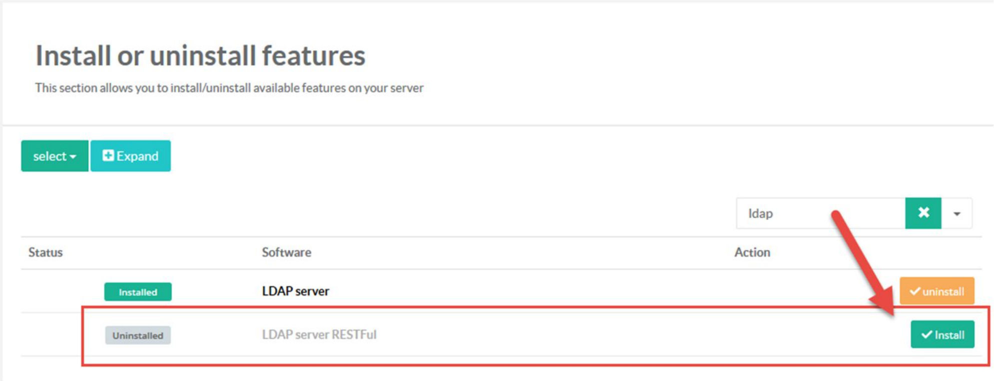


My members

Display Name	EMail Address	Office Phone	Groups
Administrators	–	–	–
David Touzeau		00.00.00.00.00	Administrators

RESTful API for managing LDAP users.

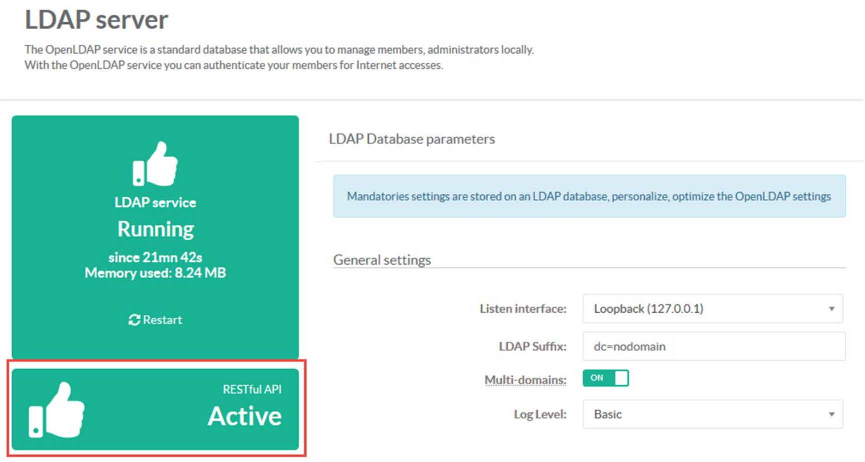
Artica provides RESTful API in order to manage LDAP members (The REST API service is available with Enterprise Edition).
To manage members and groups with REST API, you need to enable the feature thought the Features service. (see The Features section)



Install or uninstall features

This section allows you to install/uninstall available features on your server

After installed the feature, on the left menu, use “**Databases/LDAP server”**
You will see that the Restful API is active on the satus.



LDAP server

The OpenLDAP service is a standard database that allows you to manage members, administrators locally.
With the OpenLDAP service you can authenticate your members for Internet accesses.

LDAP service
Running
since 21mn 42s
Memory used: 8.24 MB

RESTful API
Active

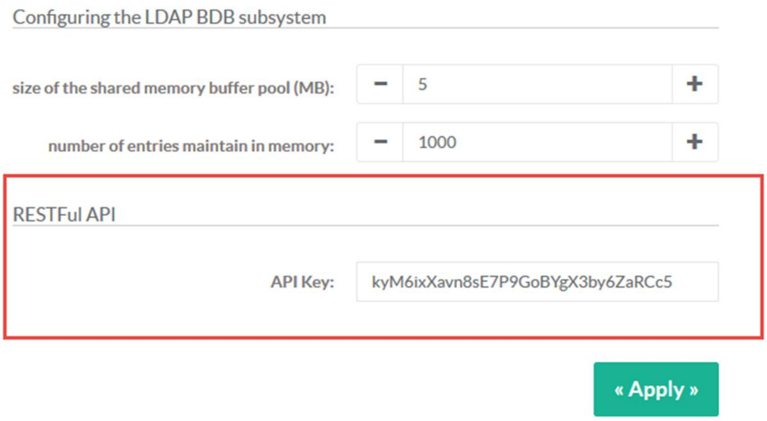
LDAP Database parameters

Mandatories settings are stored on an LDAP database, personalize, optimize the OpenLDAP settings

General settings

Listen interface: Loopback (127.0.0.1)
LDAP Suffix: dc=nodomain
Multi-domains: ON
Log Level: Basic

On the right side, in the form you can see the RESTful API Key. You can modify it if you want.



Configuring the LDAP BDB subsystem

size of the shared memory buffer pool (MB): 5

number of entries maintain in memory: 1000

RESTFul API

API Key: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5

This api key must be added in the HTTP header of the request, the header name is “ArticaKey”
Using curl, you need to run :

```
curl --header "ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5" https://192.168.1.250:9000/api/rest/ldap/[function]
```

The response will be a json and a boolean field status (true/false) is sended to indicates if the command is a success

Manage organizations

List LDAP organizations

```
GET: https://server:9000/api/rest/ldap/organization/list
```

Create MyCompany organization:

```
POST: https://server:9000/api/rest/ldap/organization/create + field= “name”
```

PHP example width curl:

```
$ch = curl_init();
$CURLOPT_HTTPHEADER[]="Accept: application/json";
$CURLOPT_HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT_HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT_HTTPHEADER[]="Expect:";
$CURLOPT_HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5";

$MAIN_URI="https://192.168.1.173:9000/api/rest/ldap/organization/create";


curl_setopt($ch, CURLOPT_HTTPHEADER, $CURLOPT_HTTPHEADER);
curl_setopt($ch, CURLOPT_TIMEOUT, 300);
curl_setopt($ch, CURLOPT_URL, $MAIN_URI);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYHOST,0);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER,0);
$POSTz=array("name"=>"MyCompany"); // Create the MyCompany Orgnization

curl_setopt($ch, CURLOPT_POSTFIELDS, $POSTz);

$response = curl_exec($ch);
$errno=curl_errno($ch);
if($errno>0){
    curl_close($ch);
    echo "Error $errno\n".curl_error($ch)."\n";
    die();
}

$CURLINFO_HTTP_CODE=intval(curl_getinfo($ch,CURLINFO_HTTP_CODE));

if($CURLINFO_HTTP_CODE<>200){
    echo "Error $CURLINFO_HTTP_CODE\n";
    die();
}
$json=json_decode($response);
if(!$json->status){echo "Failed $json->message\n";die();}
echo "Success\n";
```

Delete MyCompany organization:

```
GET: https://server:9000/api/rest/ldap/organization/delete/MyCompany
```

List members inside MyCompany organization:

```
GET: https://server:9000/api/rest/ldap/organization/delete/MyCompany/members
```

Manage Groups inside an Organization

List groups in MyCompany

```
GET: https://server:9000/api/rest/ldap/organization/MyCompany/groups/list
```

Create a group inside MyCompany

```
POST: https://server:9000/api/rest/ldap/organization/MyCompany/groups/create + field= “name”
```

Delete the group Administrator inside MyCompany with gidnumber 500

```
GET: https://server:9000/api/rest/ldap/organization/MyCompany/groups/delete/500
```

Create a member **Jhon.doo** inside **MyCompany** and the group with gidNumber **500**

```
POST: https://server:9000/api/rest/ldap/organization/MyCompany/groups/500/add + fields
```

PHP example:

```
$ch = curl_init();
$CURLOPT_HTTPHEADER[]="Accept: application/json";
$CURLOPT_HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT_HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT_HTTPHEADER[]="Expect:";
$CURLOPT_HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5";

$MAIN_URI="https://192.168.1.173:9000/api/rest/ldap/organization/MyCompany/groups/500/add";

curl_setopt($ch, CURLOPT_HTTPHEADER, $CURLOPT_HTTPHEADER);
curl_setopt($ch, CURLOPT_TIMEOUT, 300);
curl_setopt($ch, CURLOPT_URL, $MAIN_URI);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYHOST,0);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER,0);
$POSTz=array(
    "uid"=>"Jhon.doo",
    "DisplayName"=>"Jhon doo Mhain",
    "givenName"=>"Jhon",
    "name"=>"doo Mhain",
    "password"=>"123456"

);
curl_setopt($ch, CURLOPT_POSTFIELDS, $POSTz);
$response = curl_exec($ch);
$errno=curl_errno($ch);
if($errno>0){
    curl_close($ch);
    echo "Error $errno\n".curl_error($ch)."\n";
    die();
}

$CURLINFO_HTTP_CODE=intval(curl_getinfo($ch,CURLINFO_HTTP_CODE));

if($CURLINFO_HTTP_CODE<>200){
    echo "Error $CURLINFO_HTTP_CODE\n";
    die();
}

$json=json_decode($response);
if(!$json->status){echo "Failed $json->message\n";die();}
echo "Success\n";
```

Unlink **Jhon.doo** inside **MyCompany** from the group with gidNumber **500**

```
POST: https://server:9000/api/rest/ldap/organization/MyCompany/groups/500/unlink + field= “uid”
```

Link user **Jhon.doo** inside **MyCompany** to the group with gidNumber **500**

```
GET: https://server:9000/api/rest/ldap/organization/MyCompany/groups/500/Jhon.doo
```

Manage members

Get **Jhon.doo** member information

```
GET: https://server:9000/api/rest/ldap/member/Jhon.doo
```

Remove **Jhon.doo** from database

```
GET: https://server:9000/api/rest/ldap/member/Jhon.doo/delete
```

Update **Jhon.doo** informations

```
POST: https://server:9000/api/rest/ldap/member/Jhon.doo/update
```

Fields are:

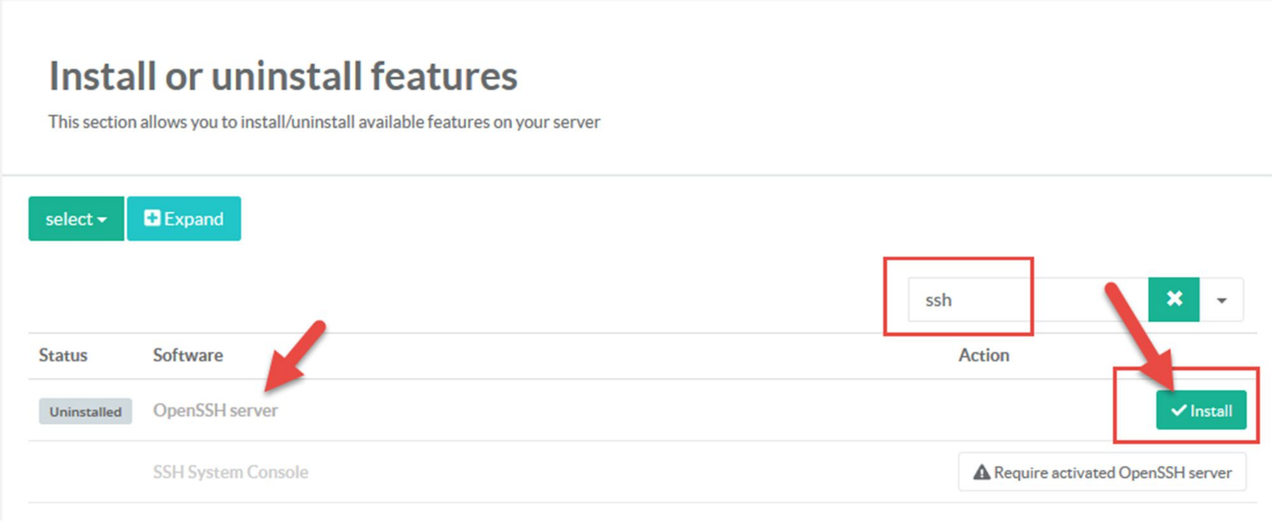
```
    "uid"=>"Jhon.doo",
    "DisplayName"=>"Jhon doo Mhain",
    "givenName"=>"Jhon",
    "name"=>"doo Mhain",
    "password"=>"123456"
```

SSH SERVICE

INSTALL THE SSH SERVICE

If you need to enter the Artica system using SSH, you have to install the OpenSSH server.
On the left menu, use “**Your system**” and “**features**” option to open the features section.

In the search box, type “ssh” and click on the button “Install” under the “OpenSSH server” row.



Install or uninstall features

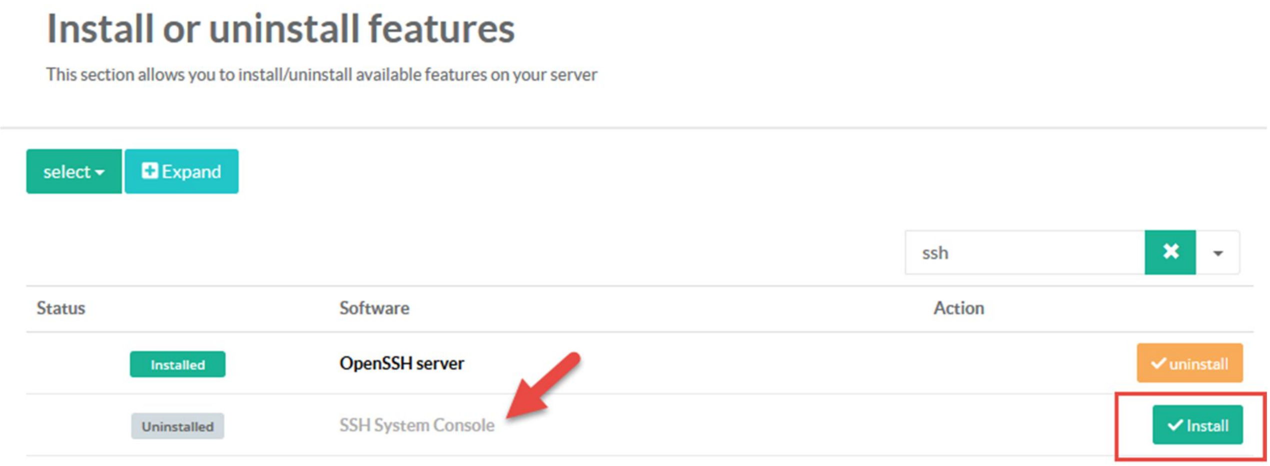
This section allows you to install/uninstall available features on your server

Status	Software	Action
Uninstalled	OpenSSH server	✓ Install
	SSH System Console	Require activated OpenSSH server

This feature allows you to enter into the system with “root” account and “artica” as the default password with an SSH client.

THE SSH WEB CONSOLE

If you want to enter into the system using SSH web console, after installing the OpenSSH server, install the “**SSH system console**”.



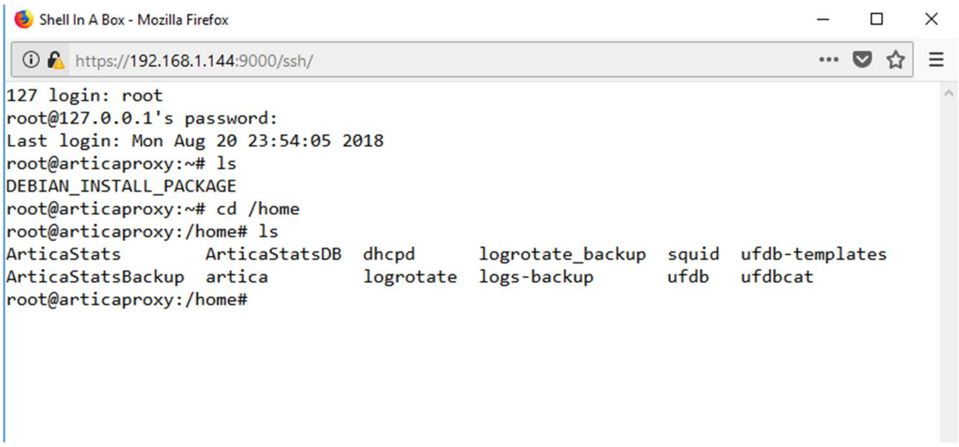
Install or uninstall features

This section allows you to install/uninstall available features on your server

Status	Software	Action
Installed	OpenSSH server	✓ uninstall
Uninstalled	SSH System Console	✓ Install

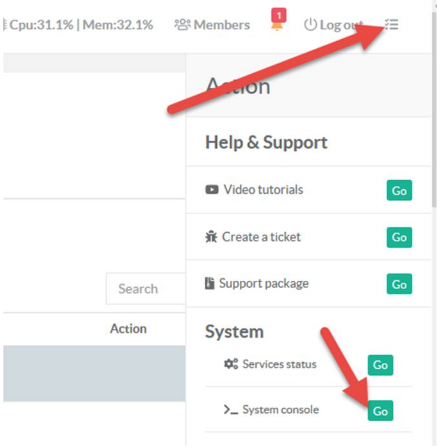
The Web SSH console is available using the right menu and “**System console**” menu.

This will open a web console that simulates a connection using SSH client.



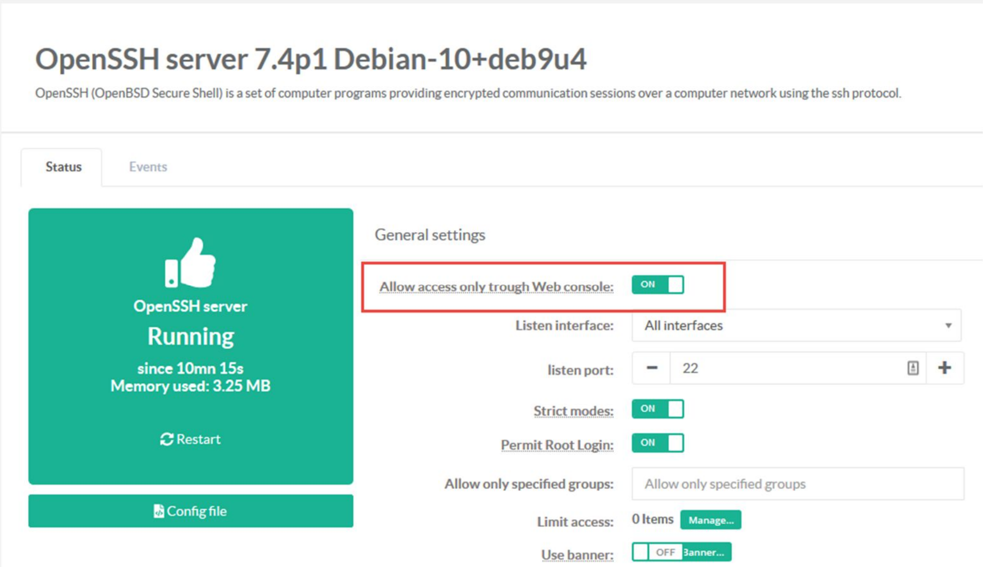
Shell In A Box - Mozilla Firefox
https://192.168.1.144:9000/ssh/

```
127 login: root
root@127.0.0.1's password:
Last login: Mon Aug 20 23:54:05 2018
root@articaproxy:~# ls
DEBIAN_INSTALL_PACKAGE
root@articaproxy:~# cd /home
root@articaproxy:/home# ls
ArticaStats         ArticaStatsDB  dhcpd      logrotate_backup  squid  ufdb-templates
ArticaStatsBackup   artica         logrotate  logs-backup       ufdb   ufdbcat
root@articaproxy:/home#
```



Restrict the SSH access to the Web console.

If you did not want to open the TCP 22 port and keep access to the Artica system using only the Web console, on the left pan, choose “Your System” and “OpenSSH server” menu.
Under the “General settings” section, turn on the “**Allow access only through Web console**” and click on “Apply” button.



OpenSSH server 7.4p1 Debian-10+deb9u4

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the ssh protocol.

General settings

Allow access only trough Web console: ON

Listen interface: All interfaces

listen port: 22

Strict modes: ON

Permit Root Login: ON

Allow only specified groups: Allow only specified groups

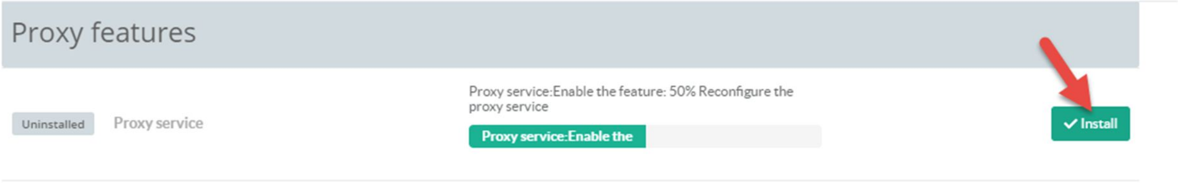
Limit access: 0 Items Manage...

Use banner: OFF Banner...

This option will force the OpenSSH server to run only on the loop back interface for the SSH Web console.
Access externally to the SSH server will not be possible.

THE HTTP/HTTPS PROXY

The proxy service is designed to handle the HTTP/HTTPs and FTP over HTTP protocols.
With the proxy service you will be able to secure browser's connections through the Internet, manage the bandwidth, authenticate users, enable the Web-filtering service, enable the Web Application Firewall service (WAF)…
The proxy service can be enabled in the “Features” service (SEE THE FEATURES SECTION) under the “**Proxy features/ Proxy service.**”



AUTHENTICATE MEMBERS

When authenticating users, the proxy is able to trace all requests with the username logged to the system.

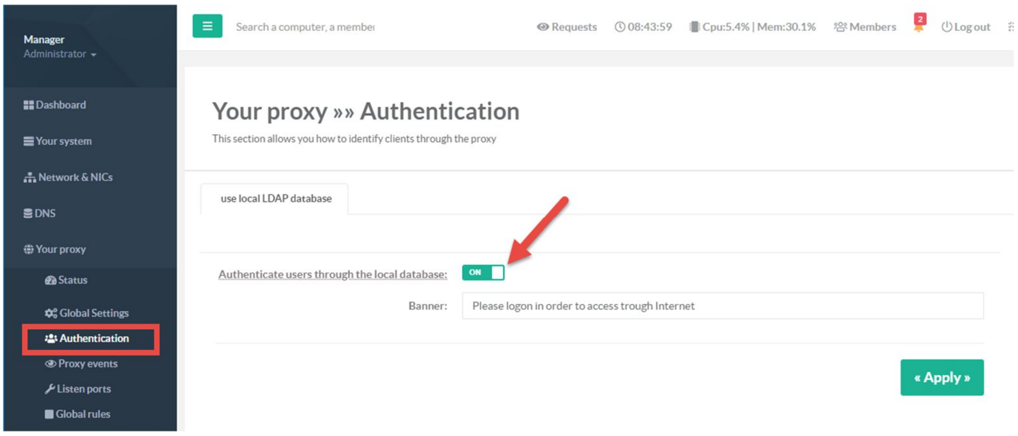
LDAP Authentication

Artica supports LDAP v3.
An LDAP directory consists of a simple tree hierarchy.
An LDAP directory might span multiple LDAP servers. In LDAP v3, servers can return referrals to other servers back to the client, allowing the client to follow those referrals if desired.
Directory services simplify administration; any additions or changes made once to the information in the directory are immediately available to all users and directory-enabled applications, devices, and Artica.
Artica supports the use of **external LDAP database servers** or the **local OpenLDAP server** to authenticate and authorize users on a per group.
LDAP group-based authentication for Artica can be configured to support any LDAP-compliant directory
Artica also provides the ability to search for a single user in a single root of an LDAP directory information tree (DIT), and to search in multiple Base Distinguished Names (DNs).

Use the Artica LDAP service.

The Artica LDAP service is an OpenLDAP server using for several services such has the proxy but also for the messaging service or the file-sharing service.
Artica offers groups and members administration like a full user’s management system.
Ensure the Local LDAP service is installed
On the “**Features**” (SEE THE FEATURES SECTION) section ensure that the **LDAP server** (SEE THE LDAP server service) is installed inside the “**Members service**” section.

On the left menu, choose “**Your Proxy/Authentication**”, turn on the “**Authenticate users through the local database**” option.

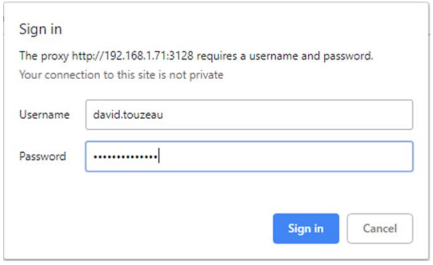


Your proxy »» Authentication
This section allows you how to identify clients through the proxy

Authenticate users through the local database: ON
Banner: Please logon in order to access trough Internet

Set the message that will be displayed in the authentication box in the “**Banner**” field

Chrome authentication box (no banner displayed)



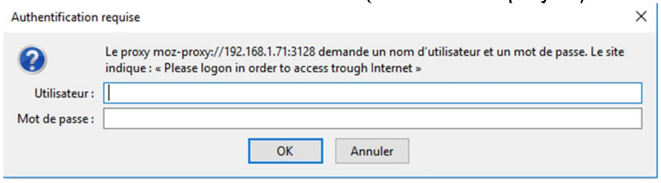
Sign in

The proxy http://192.168.1.71:3128 requires a username and password.
Your connection to this site is not private

Username: david.touzeau

Password: ••••••••••••••

FireFox authentication box (banner is displayed)



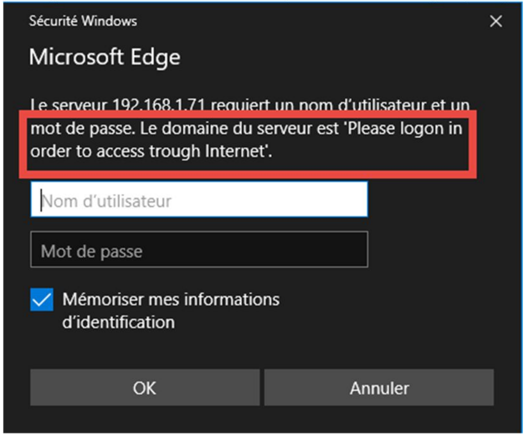
Authentification requise

Le proxy moz-proxy://192.168.1.71:3128 demande un nom d'utilisateur et un mot de passe. Le site indique : « Please logon in order to access trough Internet »

Utilisateur :

Mot de passe :

Edge authentication box (banned is displayed)



Sécurité Windows

Microsoft Edge

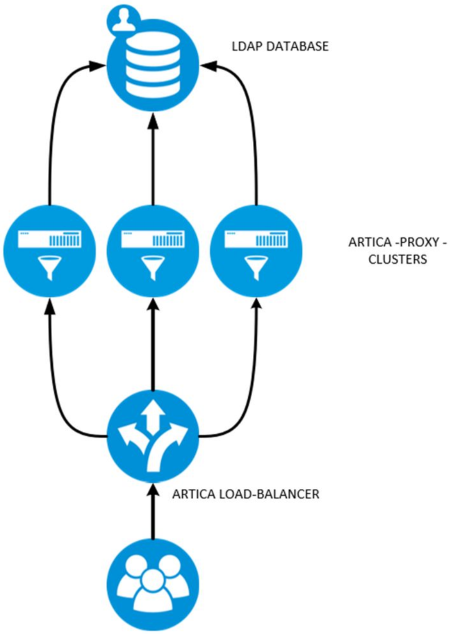
Le serveur 192.168.1.71 requiert un nom d'utilisateur et un mot de passe. Le domaine du serveur est 'Please logon in order to access trough Internet'.

Nom d'utilisateur

Mot de passe

☑ Mémoriser mes informations d'identification

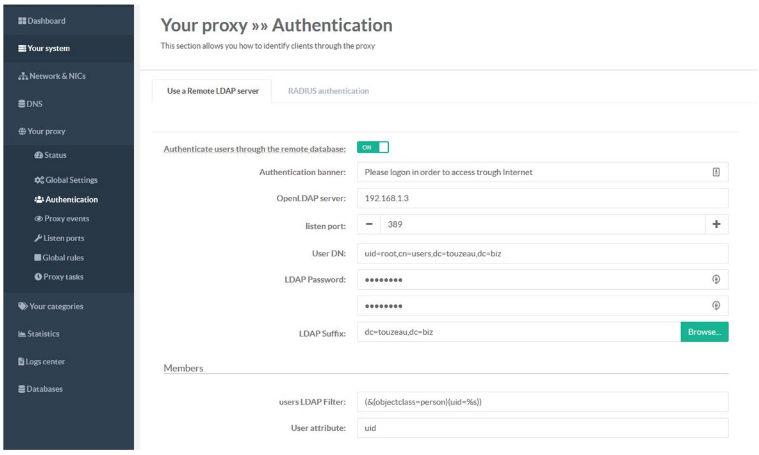
Use a Remote LDAP Database



A remote LDAP server is useful when you need to add Artica servers in cluster mode. In this case, all Artica server share the same user’s database in order to authenticate users.

If you use a remote LDAP database, this means you did not need the Local LDAP Service.
To access to remote LDAP database authentication, you need to uninstall the LDAP server with in the features section (seeThe Features section)

On the left menu, choose “**Your Proxy/Authentication**” and click on the “**Use Remote LDAP server.**”



Your proxy »» Authentication

This section allows you how to identify clients through the proxy

Authenticate users through the remote database: ON

Authentication banner: Please logon in order to access trough Internet

OpenLDAP server: 192.168.1.3

listen port: 389

User DN: uid=root,cn=users,dc=touzeau,dc=biz

LDAP Password: ••••••••

••••••••

LDAP Suffix: dc=touzeau,dc=biz

Members

users LDAP Filter: (&(objectclass=person)(uid=%s))

User attribute: uid

You can use the tool LdapAdmin to browse your LDAP server in order to find the correct information.
Turn ON the “**Authenticate users through the remote database**.”

You have to help Artica to find item using the %s (search string), %u (login user name).

- Define the remote server address and LDAP port.
- **Authentication banner**: The message that will be displayed in the authentication box.
- **User DN**: The LDAP DN for the user that has privileges to read the entire database.
- **LDAP Password**: The LDAP Password for the user that has privileges to read the entire database.
- **LDAP Suffix**: The LDAP database main branch (suffix). If you did not know which "suffix,” click on Browse.
- **Users LDAP Filter**: The search pattern to find the user based on its login name.
- **User attribute**: The LDAP attribute that stores the login name.
- **Search members in groups**: The search pattern to find users in the group entry.
- **Attribute**: the LDAP attribute to find the member in the search pattern.
- **Groups search filter**: the LDAP pattern to find the group based on its group’s name.
- **Group attribute**: The LDAP attribute to find the group name.

Example: Synology LDAP server

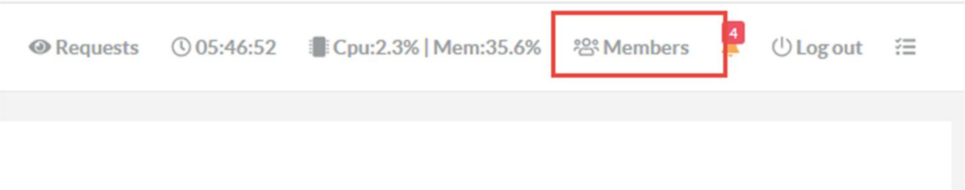
Field	Value
User DN:	uid=root,dc=company,dc=com
Users LDAP Filter:	(&(objectclass=person)(uid=%s))
User attribute:	uid
Search members in groups:	(&(memberUid=%u)(member=*))
Attribute:	member
Groups search filter:	(&(objectclass=posixGroup)(cn=%s))
Group attribute:	cn

Example: Like Active Directory

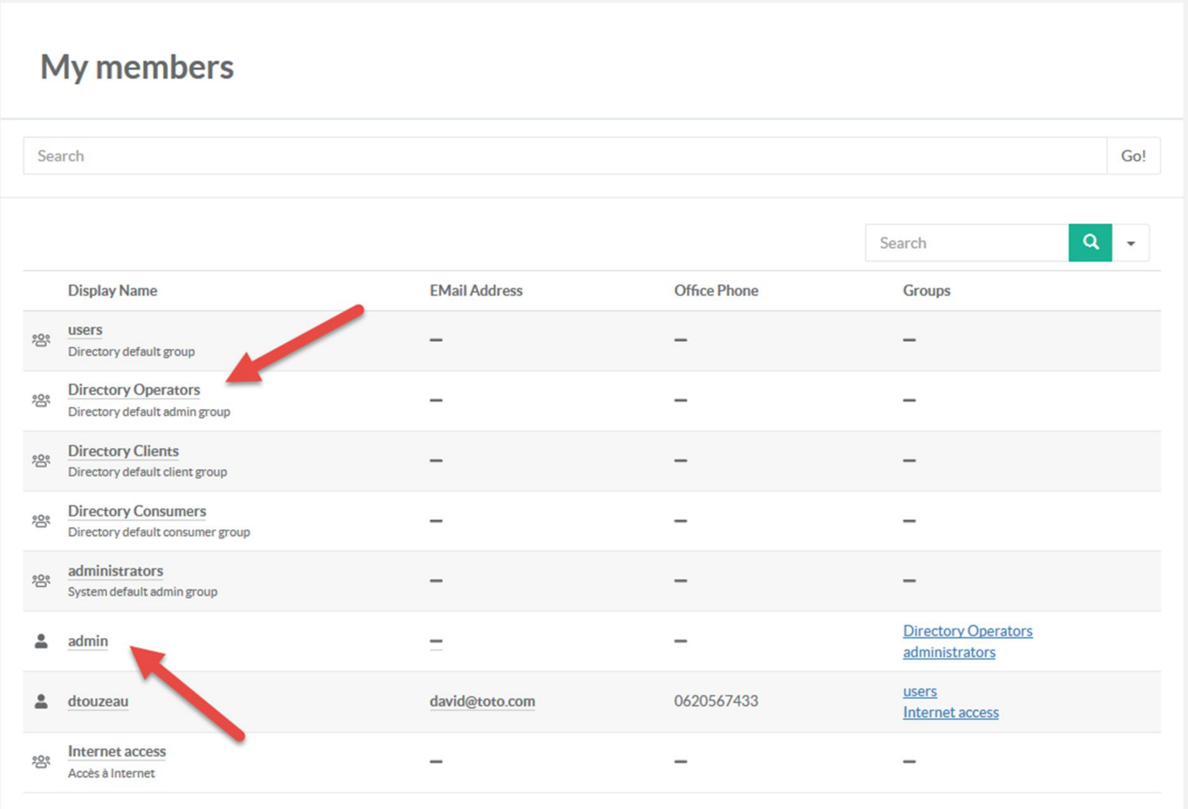
Field	Value
User DN:	root@company.com
Users LDAP Filter:	sAMAccountName=%s
User attribute:	sAMAccountName
Search members in groups:	(&(objectclass=person)(sAMAccountName=%u)(memberof=*))
Attribute:	memberof
Groups search filter:	(&(objectclass=group)(sAMAccountName=%s))
Group attribute:	sAMAccountName

Verify your LDAP patterns

When enabling the Remote LDAP server option, the TOP menu display a "**Members**" option.



This "Members section" display a table that parses your remote LDAP server in order to find users and groups.



My members

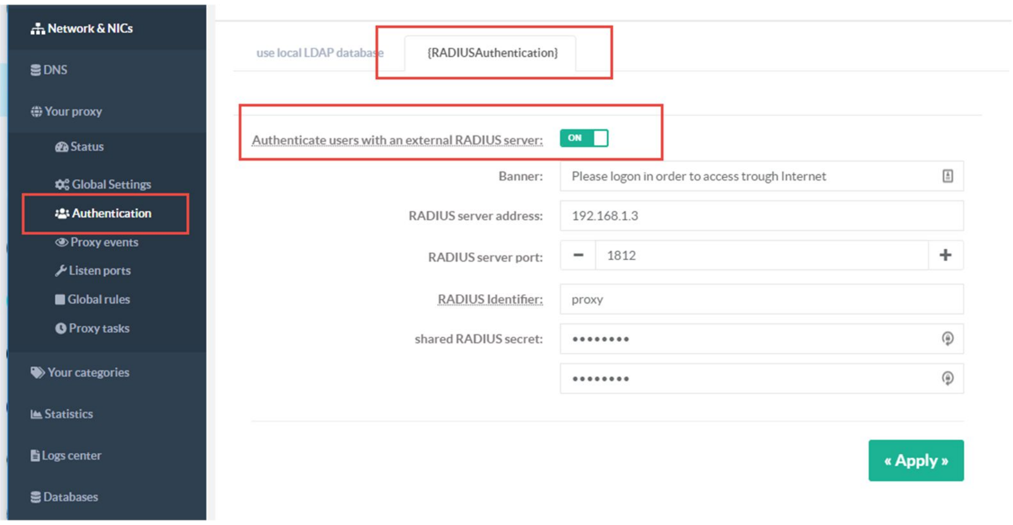
Display Name	EMail Address	Office Phone	Groups
users Directory default group	–	–	–
Directory Operators Directory default admin group	–	–	–
Directory Clients Directory default client group	–	–	–
Directory Consumers Directory default consumer group	–	–	–
administrators System default admin group	–	–	–
admin	–	–	Directory Operators administrators
dtouzeau	david@toto.com	0620567433	users Internet access
Internet access Accès à Internet	–	–	–

Views are only in read-only mode but if you see correctly your users and groups, this means your LDAP search patterns parameters are correct.

RADIUS Authentication

If you have a RADIUS server, you can connect the Artica proxy to your RADIUS server in order to authenticate users before accessing the Internet.
An authentication popup will be displayed (same as LDAP authentication).
When user sends its credentials, the proxy asks to the radius if the member/password is correct.

On the left menu, choose “Your Proxy/Authentication” and click on the Radius Authentication tab.
Enable the Authenticate users with an external RADIUS server option



Authenticate users with an external RADIUS server: ON

Banner:	Please logon in order to access trough Internet
RADIUS server address:	192.168.1.3
RADIUS server port:	1812
RADIUS Identifier:	proxy
shared RADIUS secret:	••••••••
	••••••••

- Set the message that will be displayed in the authentication box in the “**Banner**” field
- **RADIUS server address:** specifies the name or address of the RADIUS server to connect to.
- **RADIUS server port:** Specifies the port number or service name where the proxy should connect. (default to 1812)
- **RADIUS identifier:** specifies what the proxy should identify itself as to the RADIUS server.
  This directive is optional.
- **Shared RADIUS secret:** specifies the shared RADIUS secret.

THE FIREWALL

MANAGE ITEMS

When create a group inside a rule, you can manage several items.

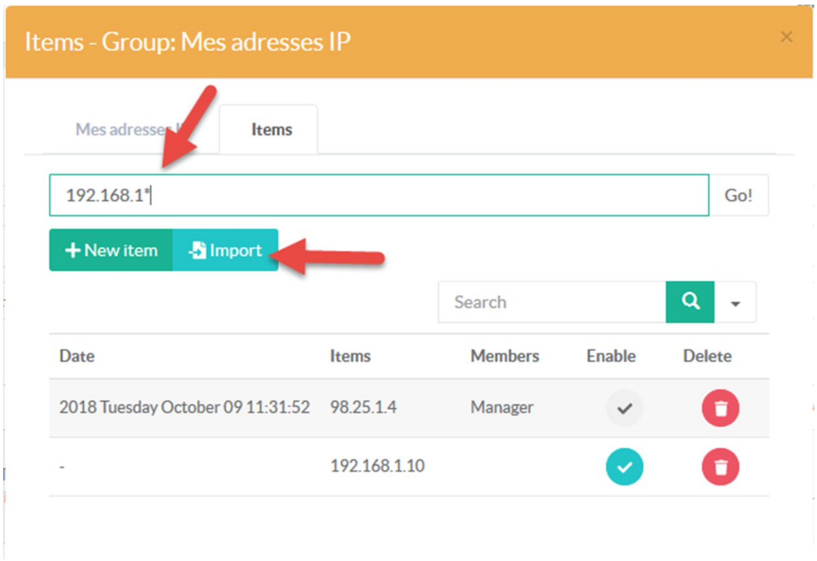
A search engine (the first search field) allows you to find the item.
The interface list is limited to 150 rows, if your item is not displayed in the first rows you have to use the search engine.

An item can be enabled or disabled, when the item is disabled, it will be not add into the FireWall rules but still available on the Web interface.

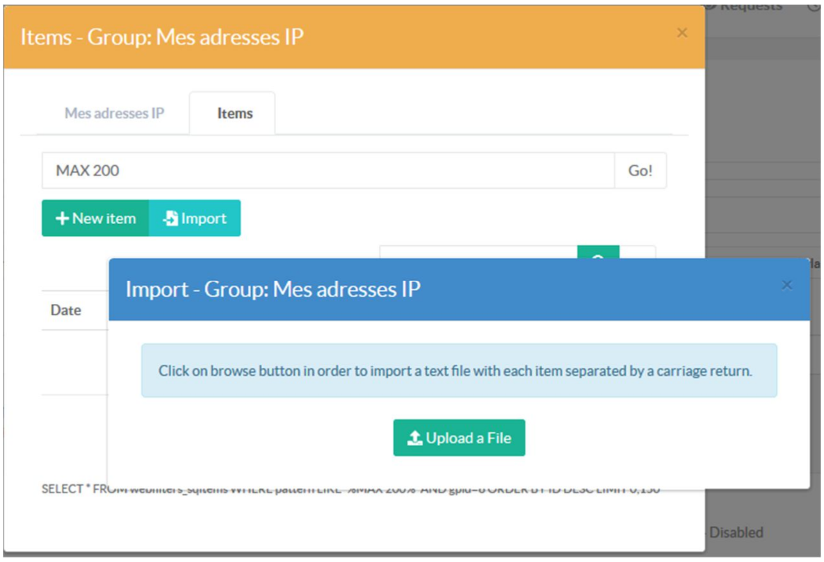
Bulk importation.

The Import button allows you to massively import items in the group.
Items must be stored in a text file separated by a carriage return.

A group has no item limits, you just have to think about memory used by the firewall according to 25,000 elements takes up about 350k of memory.



Date	Items	Members	Enable	Delete
2018 Tuesday October 09 11:31:52	98.25.1.4	Manager	✓	🗑
-	192.168.1.10		✓	🗑

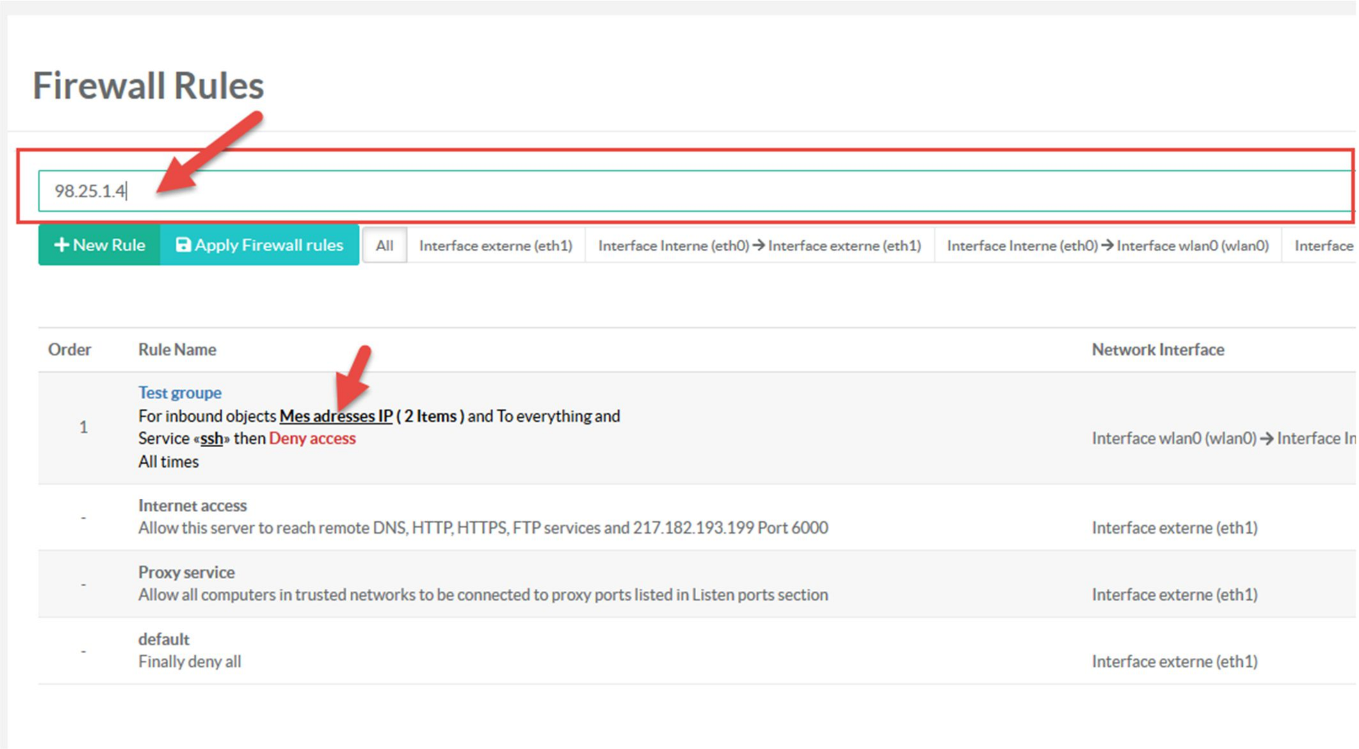


Click on browse button in order to import a text file with each item separated by a carriage return.

```
SELECT * FROM webfilters_sqitems WHERE pattern LIKE '%MAX 200%' AND gpid=0 ORDER BY ID DESC LIMIT 0,150
```

Find a rule based on an item

The global search engine on the firewall-rule list allows you to find a rule according to a defined item.
The wildcard is supported, if you need to find a specific IP string or subnet, the table will display rules that stores the group with the desired item.


+ New Rule
Apply Firewall rules
All
Interface externe (eth1)
Interface Interne (eth0) → Interface externe (eth1)
Interface Interne (eth0) → Interface wlan0 (wlan0)
Interface

Firewall Rules

98.25.1.4

Order	Rule Name	Network Interface
1	Test groupe For inbound objects Mes adresses IP (2 Items) and To everything and Service «ssh» then Deny access All times	Interface wlan0 (wlan0) → Interface In
-	Internet access Allow this server to reach remote DNS, HTTP, HTTPS, FTP services and 217.182.193.199 Port 6000	Interface externe (eth1)
-	Proxy service Allow all computers in trusted networks to be connected to proxy ports listed in Listen ports section	Interface externe (eth1)
-	default Finally deny all	Interface externe (eth1)