DOCUMENTATION

ARTICA v4.30.000000

TABLE OF CONTENTS

INSTALLING ARTICA

REQUIREMENTS

Artica 4 is **only** compatible **Debian 9.x/10.x on a 64-bit system i686**.

Ardware and operating system :

1. Artica is not compatible with **ARM** systems
2. Artica is not compatible with **Redhat** families systems (CentOS, Fedora, Red Hat, Open SuSe).
3. Artica is not compatible with **Unbutu** systems.

Minimal hardware performance:

Artica require minimal Corei3 with 3GB of memory and 20GB of disk space.

Product is "Virtualization aware" .

It can be installed on modern virtualization systems such as VMWare ESXi, Microsoft HyperV, Citrix XenServer, Nutanix, KVM, Proxmox…

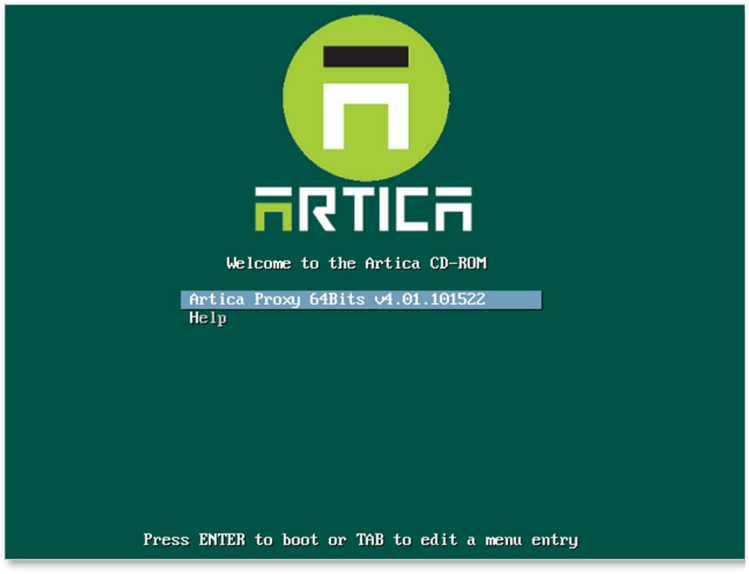
Browsers

- We have found some issue when using **AdBlock** and **Ghostery** plugin in browsers, if you using this plugin
- Artica is not compatible with **Internet Explorer**.

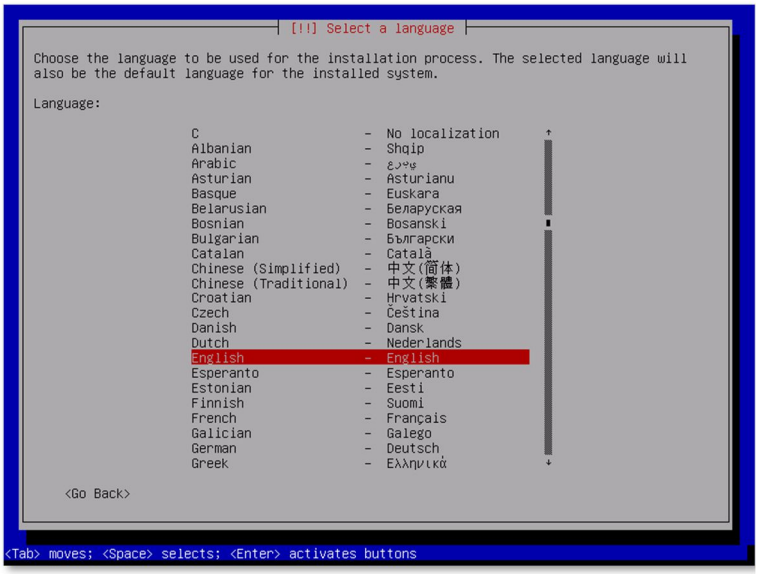
To install Artica, you have 2 ways:

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



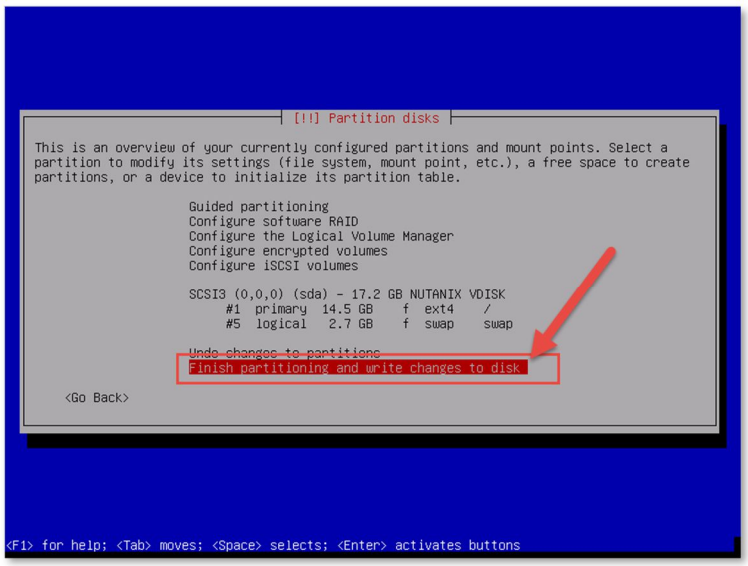
Boot from the ISO, a welcome screen must appear



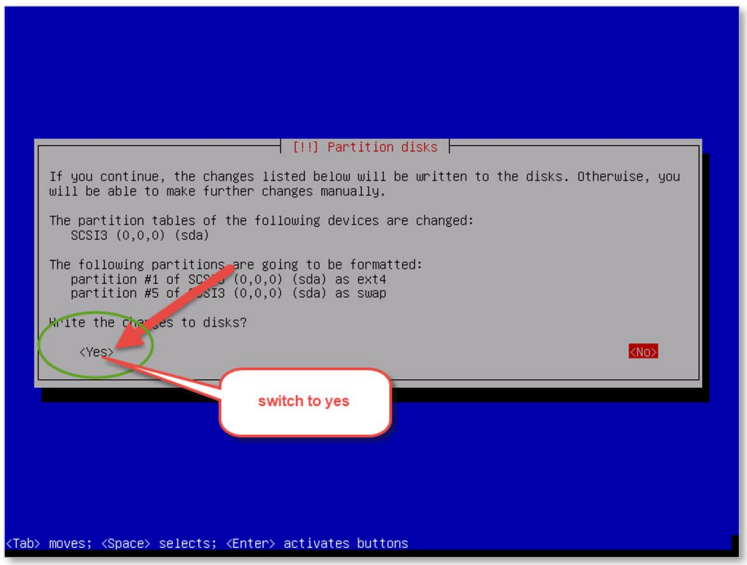
Select your system language, country and the language of the keyboard.

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.

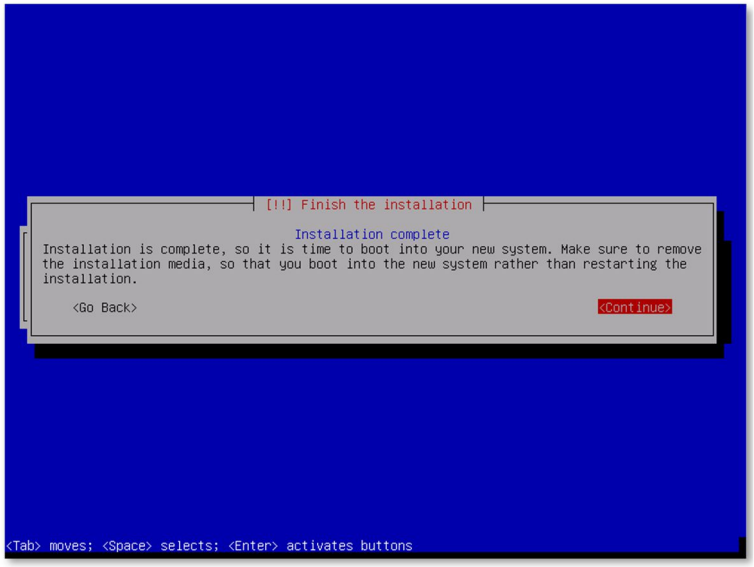
The TCP settings will not be saved after the reboot, you will have to re-enter it after the reboot.



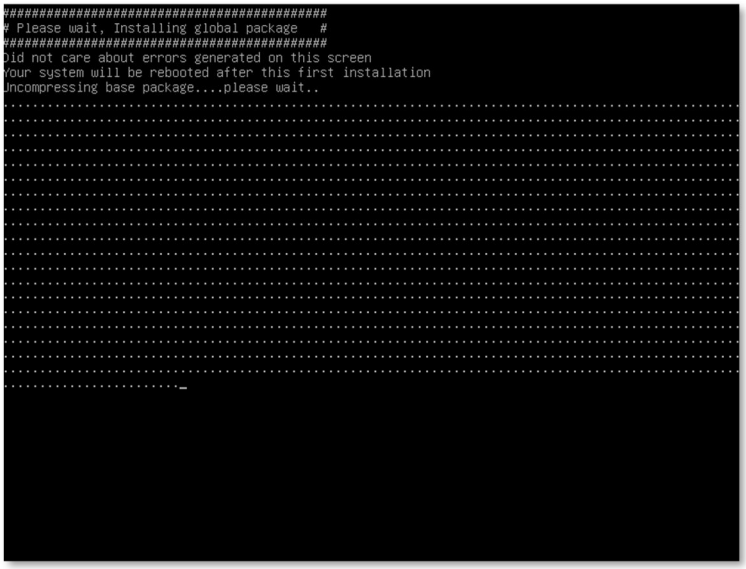
By default, the install tool will create system partitions



Just approve it automatically by type Enter key on the "**Finish partitioning and write changes to disk**



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



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:

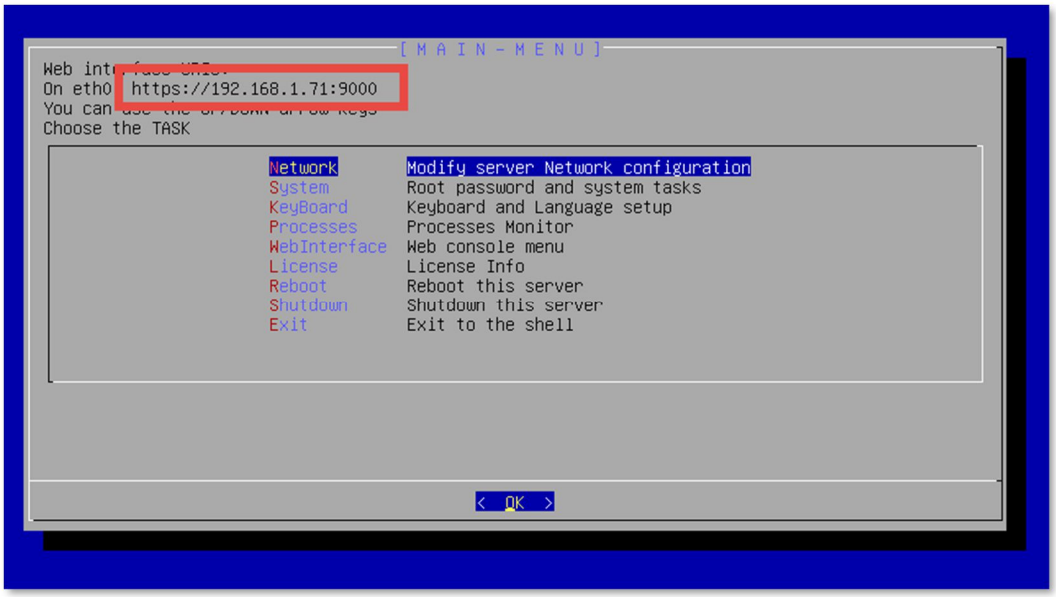
```
wget http://articatech.net/download/v4/install-manuall.sh
chmod 0755 install-manuall.sh
./install-manuall.sh
```

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.

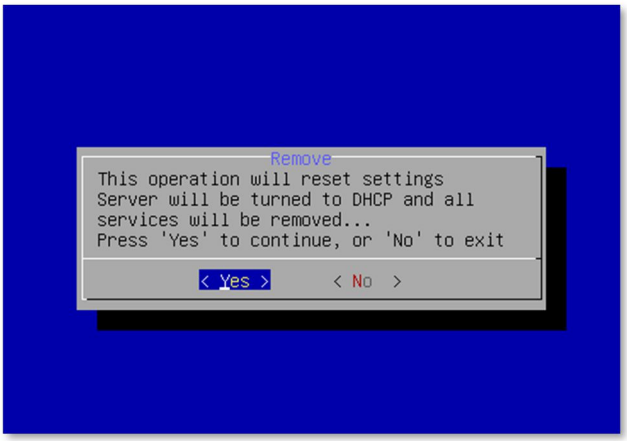
After the installation and on each reboot, a menu console is displayed.
This menu allows you to modify the network configuration, change passwords and set the keyboard language.
On the TOP-left section, the console displays the address to open the Artica Web console



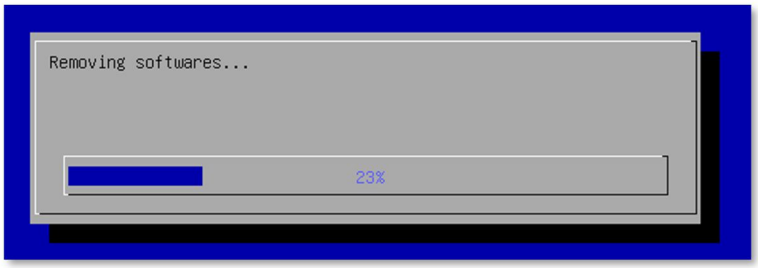
Reset the configuration

If you want to restart Artica from scratch and reset settings, you can reset the configuration in the "System" and choose **Reset parameters**

Confirm the operation to remove all services and parameters.



A progress bar will show you the execution task.

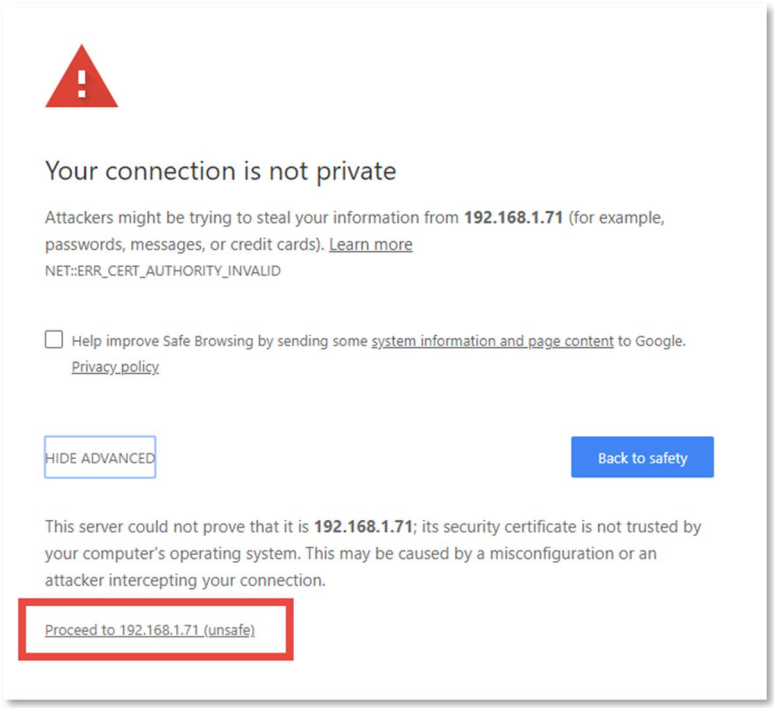


THE WIZARD

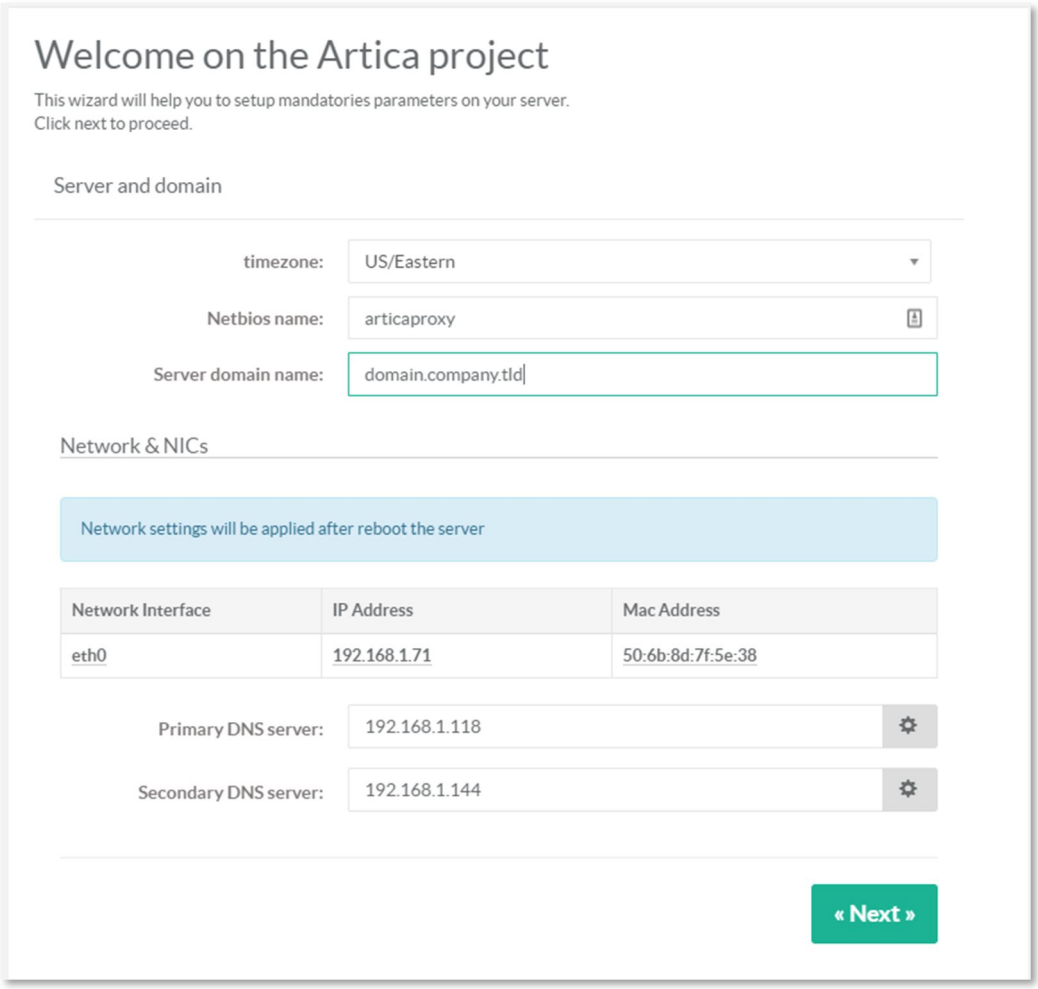
After connecting to the default web page (https://your-server-address:9000) a browser alert is displayed.

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

Ask to the browser to continue anyway.

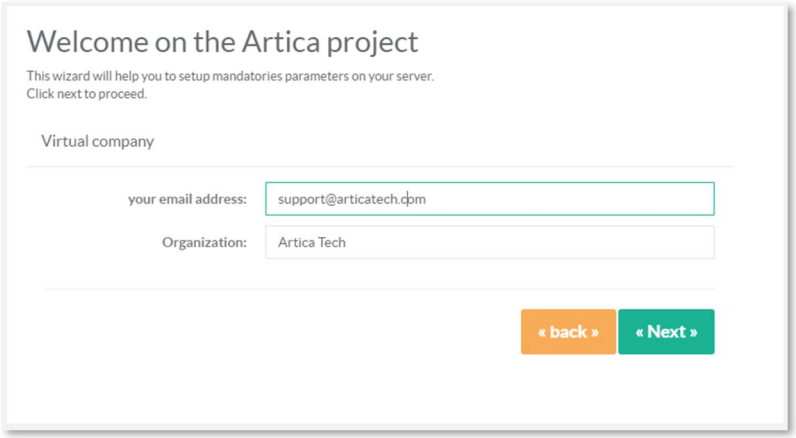


The first wizard page needs you to confirm network parameters such as host name, DNS, network interfaces parameters.

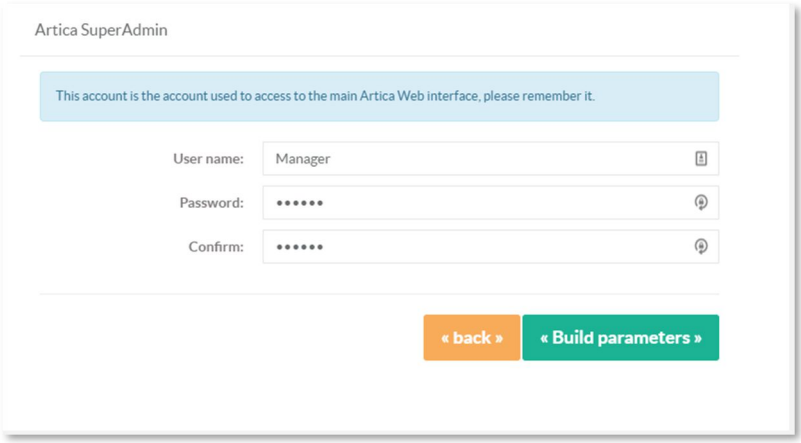


The second step will ask you a "**Virtual information**" such as:

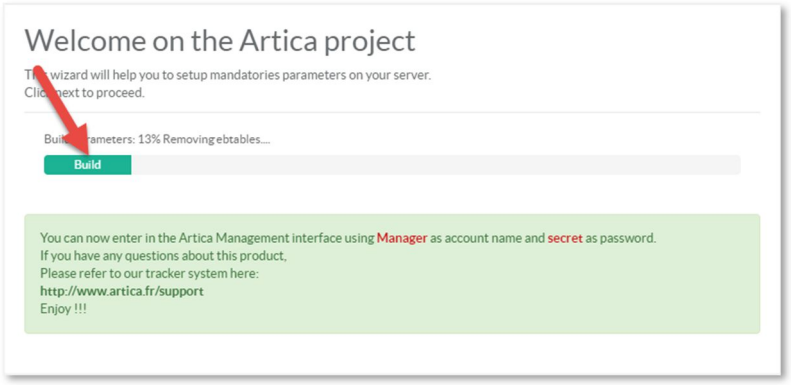
1) The eMail address that will be used by default on all services that require to inform an Administrator.
2) The Organization (company name) that will be displayed on the login screen and on some elements that communicate with your users.



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)



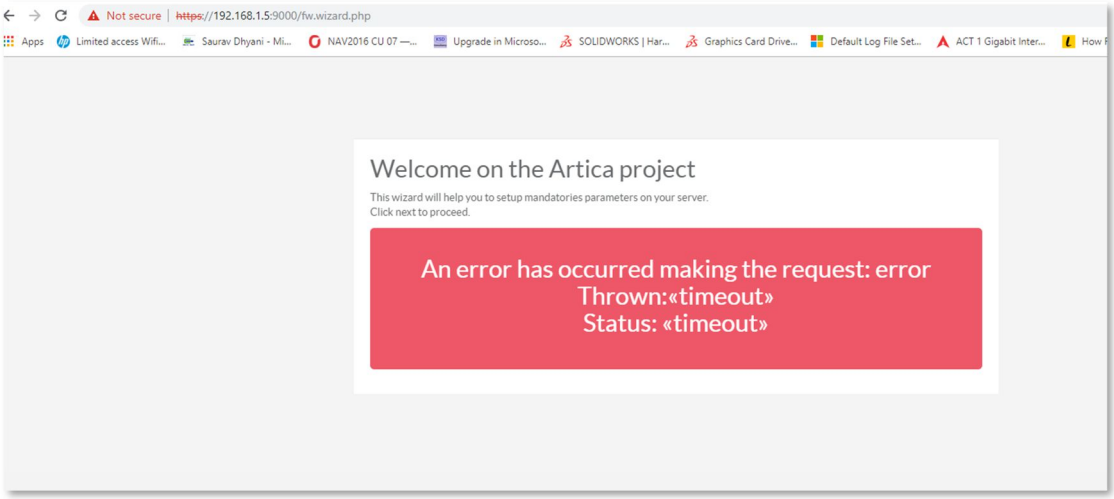
After clicking on the "**Build parameters**" button, a progress bar shows you the installation progress of your new Artica server.



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

Timeout when connecting to the wizard

If you see this message "*An error occurred making the request: Error Thrown "Timeout"*



Return to the Menu console and **setup correctly the DNS servers** used by the system.

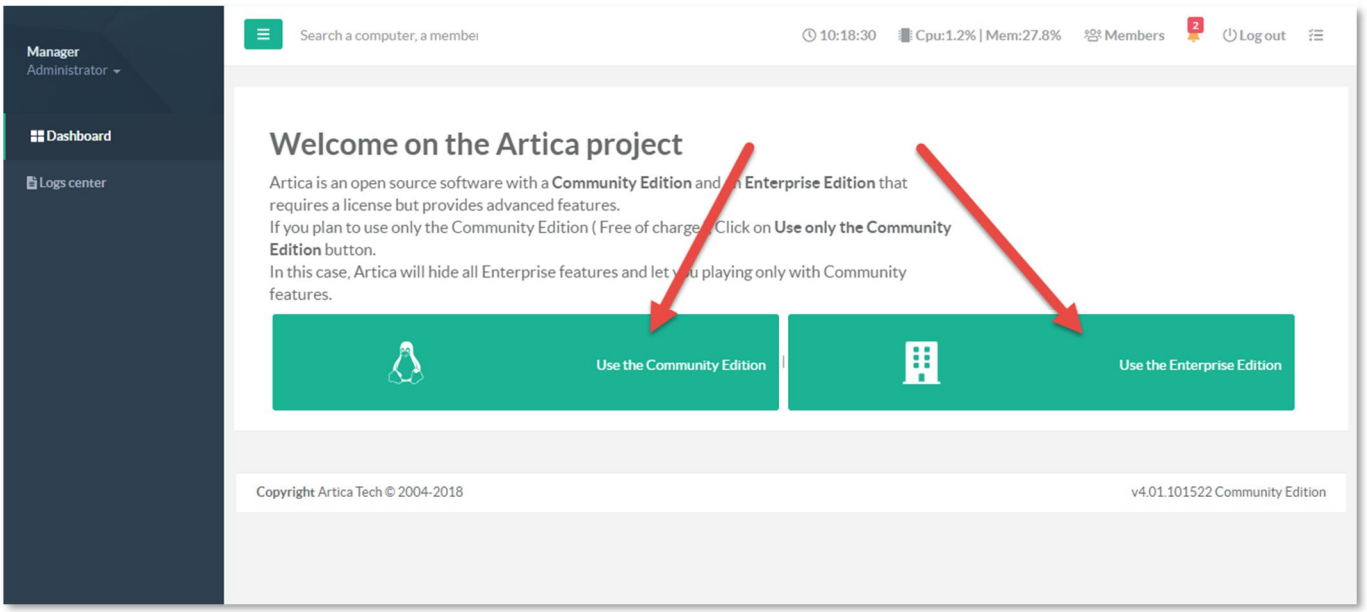
COMMUNITY OR ENTERPRISE EDITION?

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



Download the technical documentation about the license here:

http://articatech.net/download/ARTICA-LICENSE.pdf

Features between Community Edition and Enterprise Edition

Features	Community Edition	Enterprise Edition
Proxy feature	✔	✔
HTTP/HTTPS/FTP Proxy Cache feature		✔
HTTP/HTTPS/FTP Proxy advanced ACLS (WAF)		✔
HTTP/HTTPS/FTP/SSH TCP proxy compressor	✔	✔
HTTPS Secure Proxy	✔	✔
HTTP proxy Compressor	✔	✔
HTTP/HTTPS/FTP Proxy LDAP authentication	✔	✔
RDP/TSE reverse Proxy	✔	✔
HTTP/HTTPS/FTP Kerberos Authentication method		✔
HTTP/HTTPS/FTP Active directory (NTLM) authentication method		✔
Ability to Skin error pages		✔
Cluster (Load-balancing Proxies + Active Directory)		✔
Transparent cluster (Load-balancing Proxies in transparent mode)		✔
Proxy PAC service and Engine		✔
IT Charter service		✔
HTTP Proxy statistics		✔
ICAP security service	✔	✔
Antivirus Service	✔	✔
Standard antivirus databases	✔	✔
Extended antivirus databases		✔
Extended Community databases		✔
Web-Filtering feature	✔	✔
Google Safe Browsing	✔	✔
50 Web-filtering Categories (3Million Web sites)	✔	✔
150 Web-filtering Categories (50 million Web sites)		✔

Ability to Skin error pages		✔
Can create/manage personal categories		✔
Can create groups of categories	✔	✔

Logs retention features	✔	✔
Unlimited logs retention for statistics	5 Days	✔
Unlimited source Logs retention	5 Days	✔
Act as syslog / log server	✔	✔
Send Google Safe Browsing to remote syslog server		✔
Send proxy events to remote syslog server		✔
Send Firewall events to remote syslog server		✔

REST APIs		
REST API For system		✔
REST API For Proxy service		✔
REST API For Web-filtering		✔

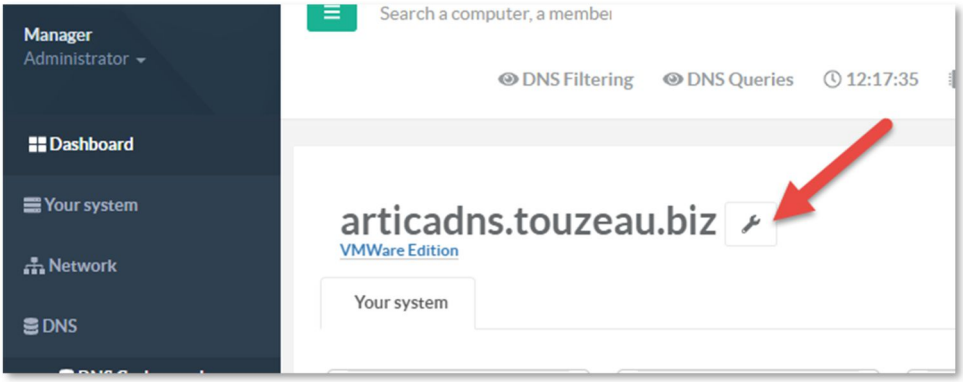
Network feature		
Firewall	✔	✔
Intrusion detection system	✔	✔
Automatic Ban network attacks	✔	✔
DHCP service	✔	✔
DHCP service for multiple Network Interfaces	✔	✔
SSH service	✔	✔
DNS Cache service	✔	✔
DNS Load-balancer service	✔	✔
Advanced ACLS for DNS Load-Balancer service		✔
Advanced DNS service (PowerDNS)	✔	✔
NTP server	✔	✔
Manage Wireless Network Interfaces	✔	✔

System feature	
Backup/export Artica configuration	✔
Restore/Import Artica configuration	✔
Skin the Artica Web console	✔
Administrators tracking	✔

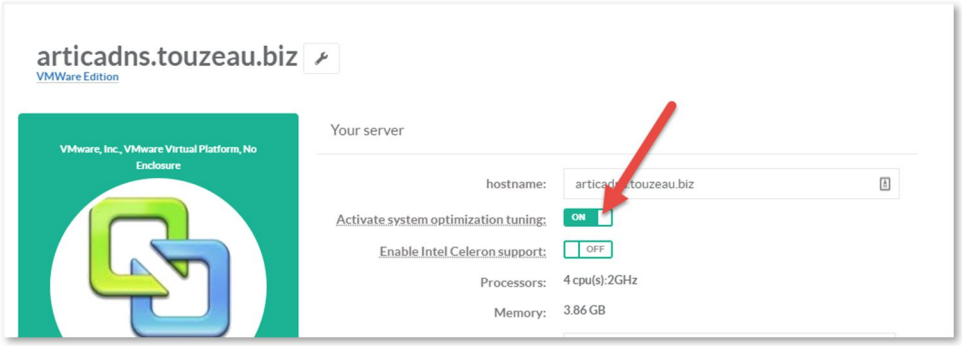
Databases management		
MySQL (Installation / Management)	✔	✔
OpenLDAP (Installation / Management)	✔	✔
PostGreSQL	✔	✔
ElasticsSearch database Management		✔
Kibana database Managemement		✔
Monitoring feature		
SNMP service	✔	✔
Zabbix Agent	✔	✔
Web services		
Possibility to create **Web services**	✔	✔
Dedicated management for **Wordpress**		✔

Optimizations

- On the Dashboard, click on the button near the hostname.



- Turn on the "**Activate system optimization tuning**"
- Click on **Apply** button.



UPGRADING FROM A 3.X VERSION

It is not possible to upgrade directly a server that stores 3.x version to a new 4.x version dues to:

1. Major operating system changes: Debian7 to Debian 9/10
2. Settings are stored in a different way.

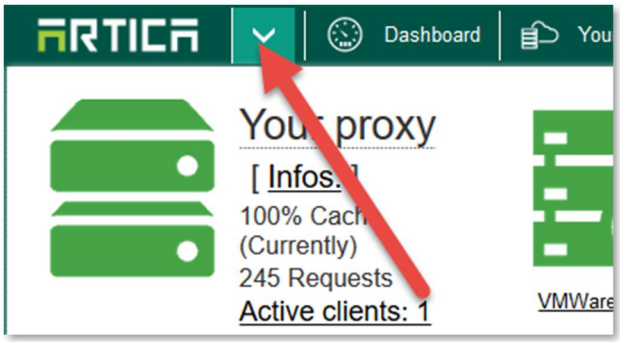
Starting to 3.06.200164 you can export settings to v4x.

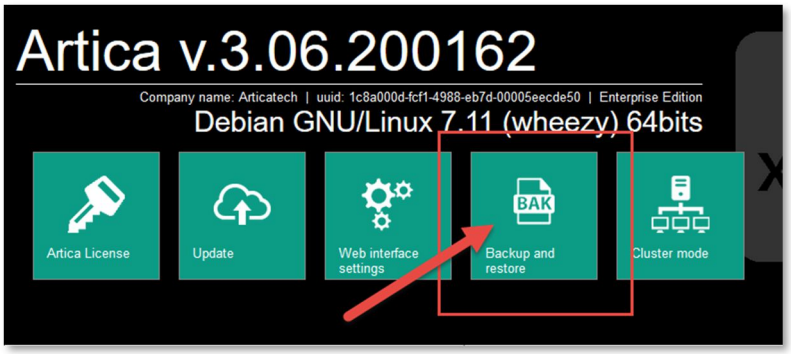
Settings are:

- All ACIs Proxy objects.
- All personal categories.
- All Whitelisted items.
- Acls Deny and Allow in the proxy ACLs

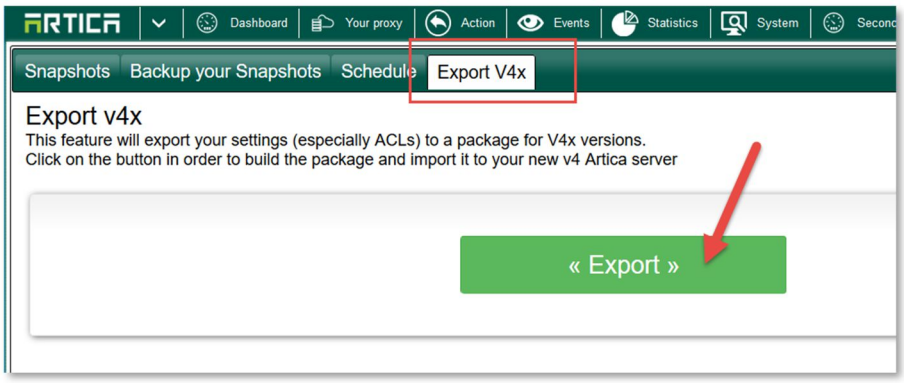
Exporting settings from a 3.x version

- Click on the Arrow on top near the Artica logo and Select the option "**Backup and restore**"





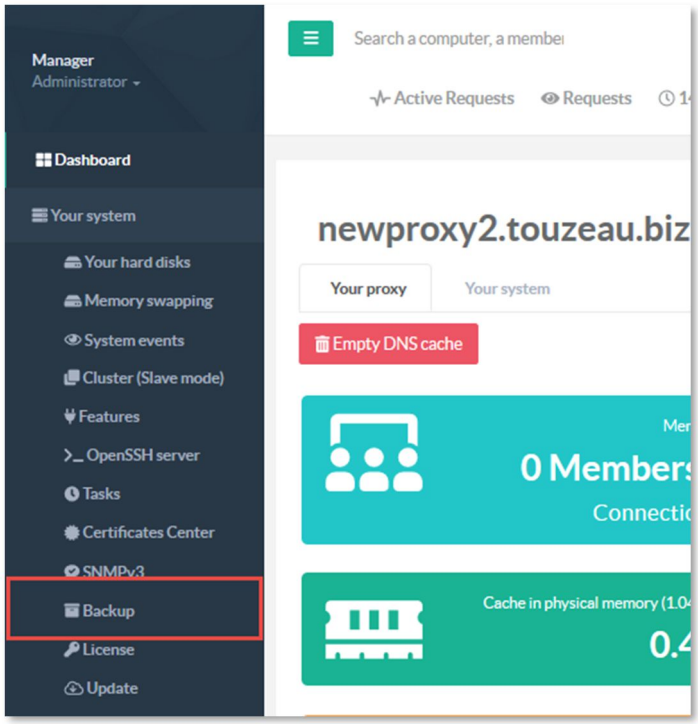
- Select the "**Export V4x**" tab
- Click on the **Export** button.



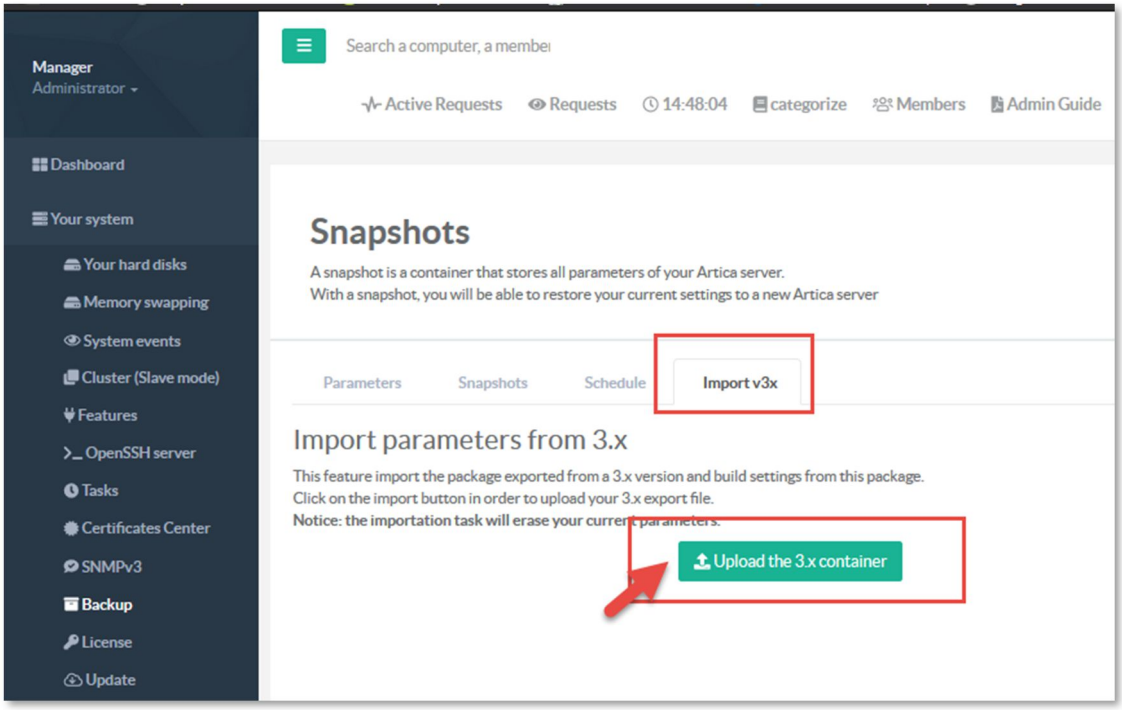
- Download the generated tar.gz file.

Import 3x settings into 4.x

On the Artica Web console 4.x, choose “Your system” and “Backup” left menu.

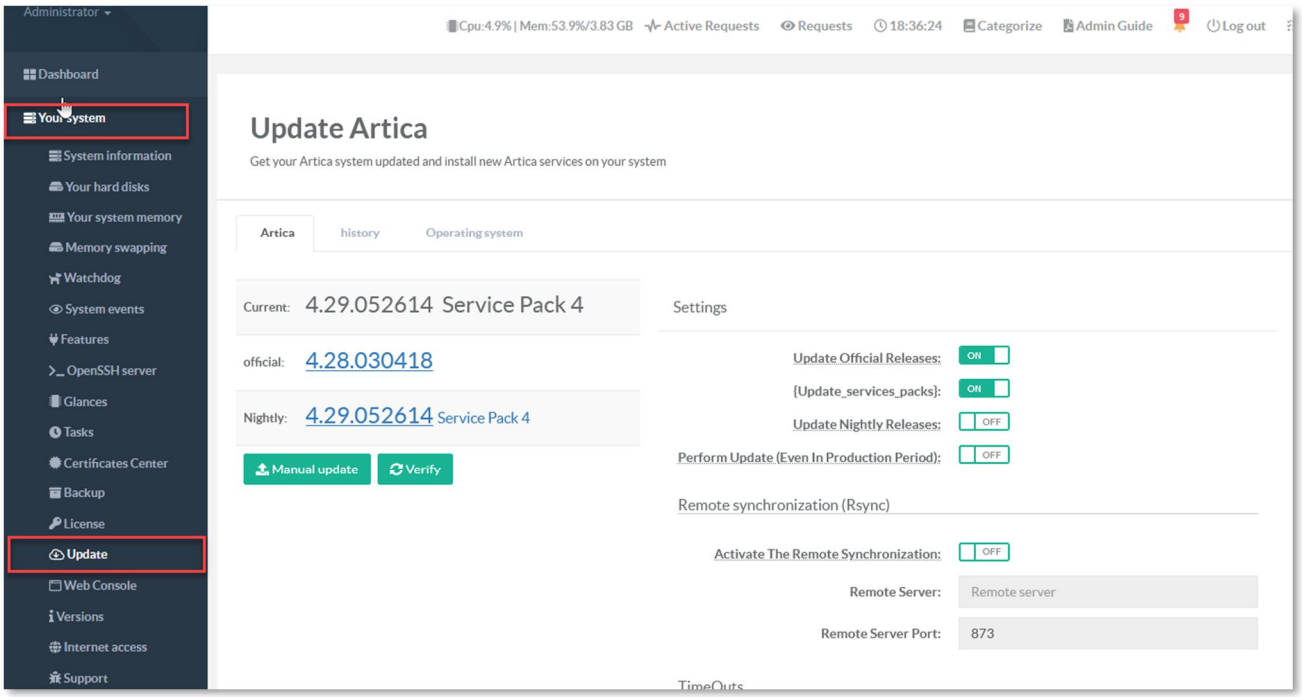


- Select “**Import v3x**” tab.
- Click on the button “**Upload the 3.x container**”
- Choose the downloaded file.



UPGRADING ARTICA

Artica can be updated itself.
Update configuration can be managed in the left menu **Your System /Update**



OFFICIAL RELEASES

By default Artica is configured to only update official releases. Official release are an **even number** in minor version.
So 4.26,4.28,4.30,4.32,4.34,4.36 are official releases.
The automatic update can be controlled by the "**Update Official Releases**" checkbox.

SERVICES PACK

Services pack are patches that are able to fix some issues on the current release or the current nightly.
These services pack can be controlled by the "Update Services Packs" checkbox.

NIGHTLY BUILDS

Nightly build are versions under development, mostly used to add new features that are not totally tested
By default, nightly updates are disabled.
Nightly builds using always **an odd number.**
So 4.27,4.29,4.31,4.33,4.35 are Nightly builds.
The automatic update can be controlled by the "**Update Nightly Releases**" checkbox.

UPDATE IN PRODUCTION

By default, the "Perform Update (Even in production mode)" is disabled.
This means if there is a new update (official, nightly or Service Pack) it will be performed only during 22h PM to 06h AM.

MANUAL UPDATE.

Manual update accept any artica-4.xx.xxxxxx.tgz for full version or ArticaPx.tgz for Services Packs.
With the button Manual update, you can download Artica packages here http://articatech.net/firmwares.php
And upload them to the system.
The manual update button allows you to return back to any version available in the Firmware's table.

THE CERTIFICATES CENTER

The certificate center allows you to store and generates all certificates to build encrypted SSL protocols.
It can be used to enable HTTPS on the proxy and web services, SMTPs and the SMTP service....

The certificate center is compatible with Let's Encrypt that allows you to generate a free of charge public certificate.

BUILD A SELF-SIGNED CERTIFICATE

See the Youtube video.
https://youtu.be/4_mUNB72lu8

BUILD A LET'S ENCRYPT CERTIFICATE.

To build Let's Encrypt certificate **your server needs to be contacted by the Let's Encrypt public web servers** in order to verify that you are the owner of the domain.

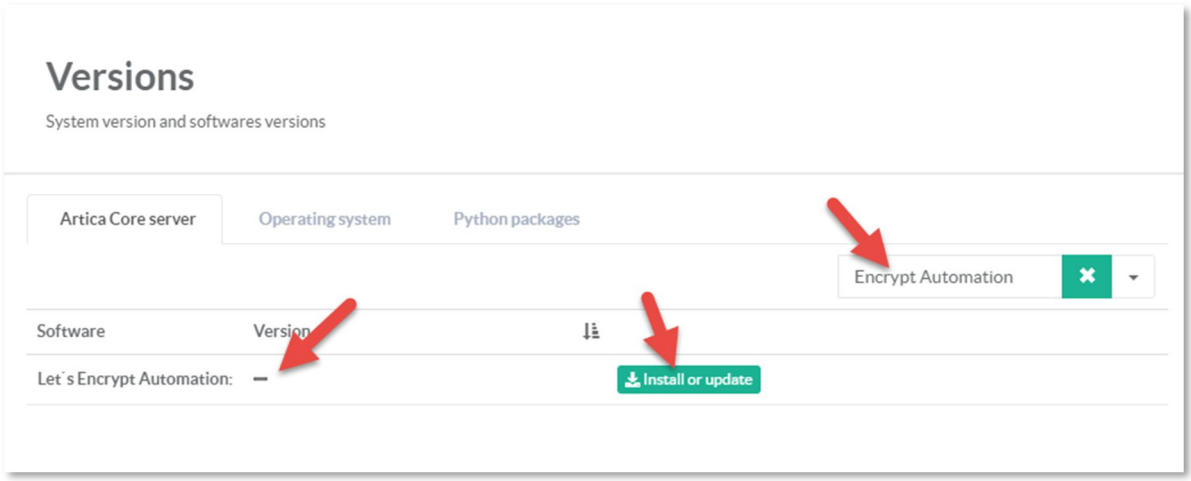
Let's Encrypt is not designed to be used on internal servers.

During the building certificate, the Web service and the Firewall will be shut down in order to let the process running a micro web server to allow Let's Encrypt public servers validating your domain.

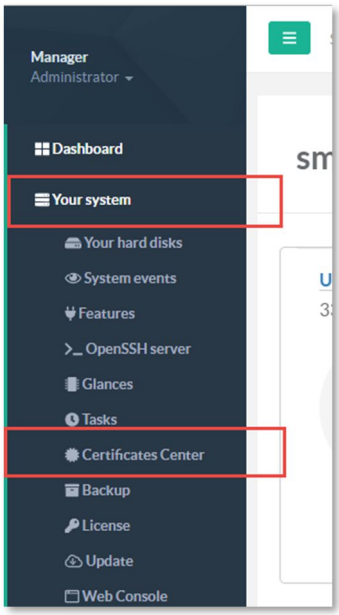
Verify the Let`s Encrypt Automation installation

On the left menu, click on "**Your system**" item and "**Versions**"
On the search field, type **Encrypt Automation**" filter

If no version is displayed on the "**Let's Encrypt Automation**" row, this means it is not installed.
Click on the "**Install or update**" button.

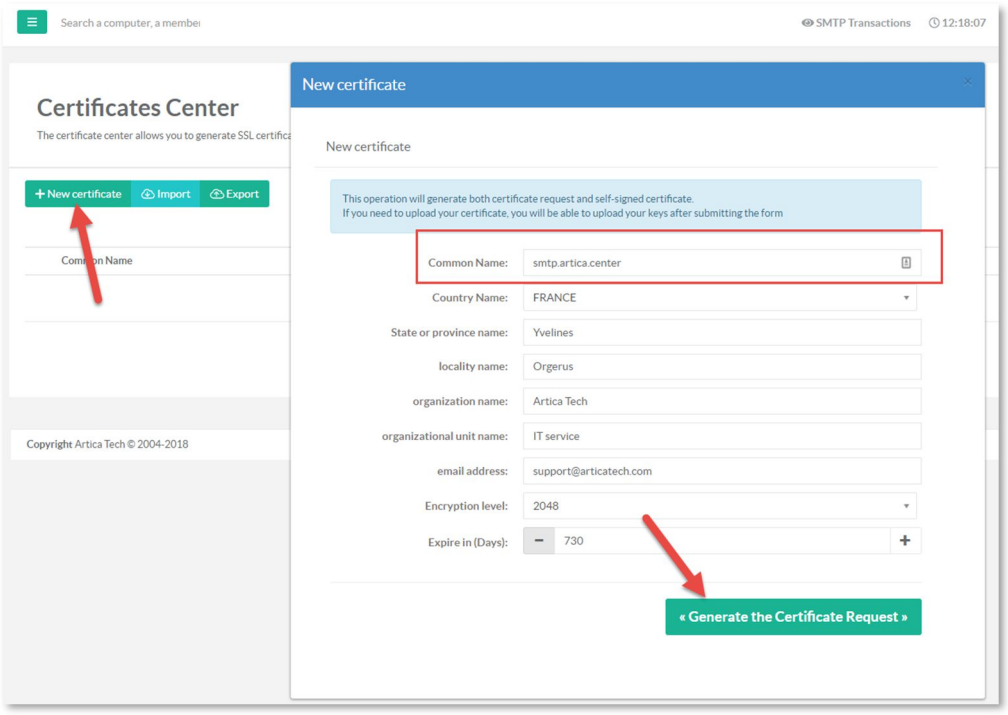


Generate the certificate

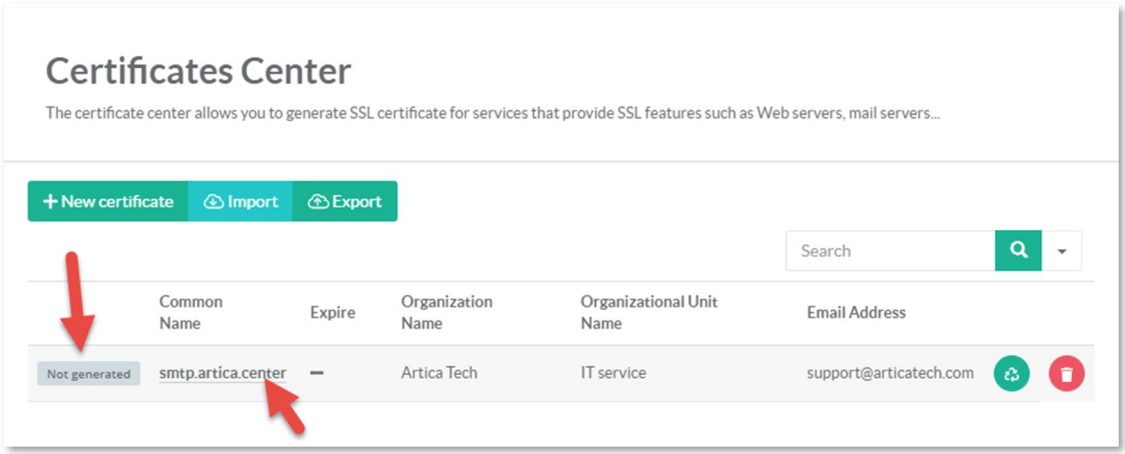


On the left menu, click on "**Your system**" item and "**Certificates Center**"

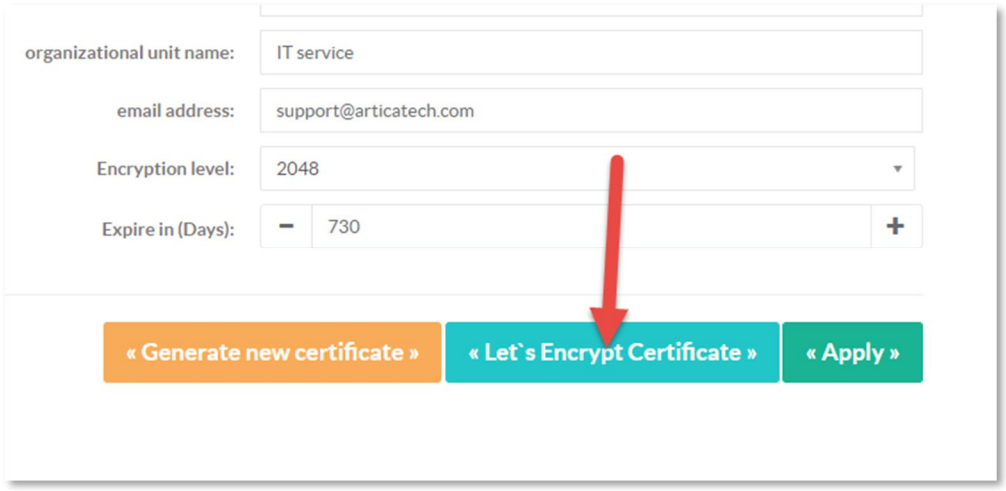
- ✓ On the table, Click on "**New Certificate**"
- ✓ In the Common Name field set the domain or the fully qualified hostname of your server.
  In our case we want to reach the https://smtp.artica.center URL, our domain will be "smtp.artica.center"
- ✓ Fill correctly information on the form
- ✓ Select 2048 for the encryption Level.
- ✓ After finish, click on the "**Generate the Certificate Request**"



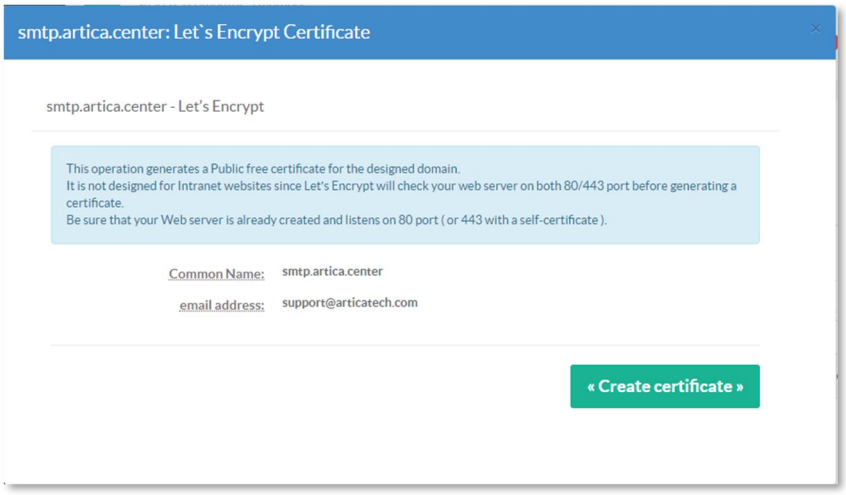
- ✓ You will see in the table your certificate but it is not generated.
  This means only the CR (Certificate Request) is generated.
- ✓ Click on the **certificate name** on the table.



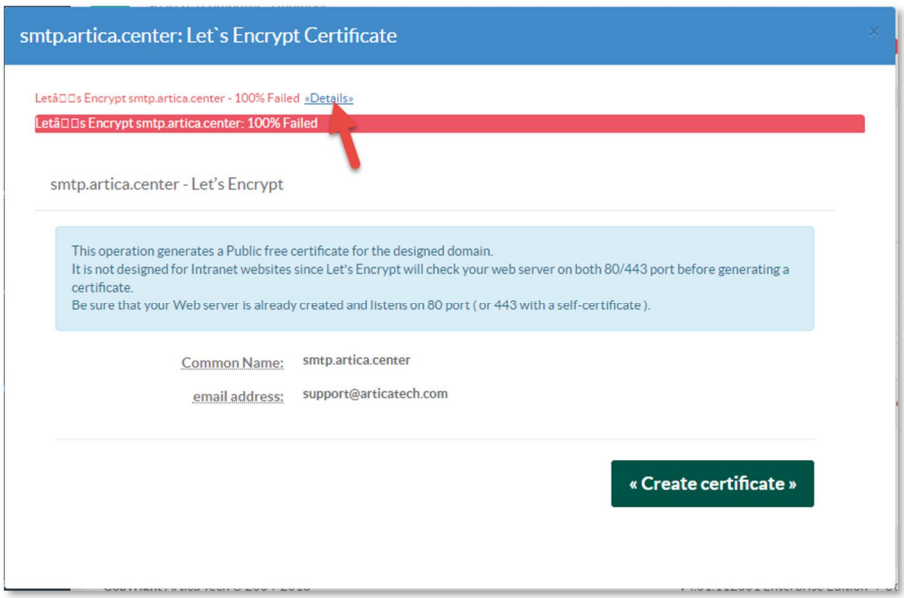
- ✓ At the bottom of the form (if Let`s Encrypt Automation is installed) you should see the "Let's Encrypt Certificate" button.
- ✓ Click on this button.



✓ A confirmation message is displayed.
✓ Click on the "**Create Certificate**" button.



✓ If task is failed, progress will be turned in red.
✓ You can click on the details link to see events.

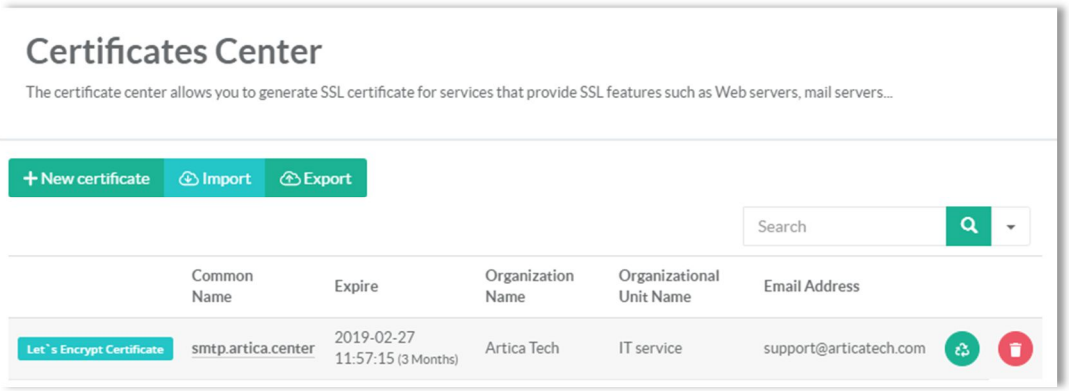


In most cases, you will see this error

```
"Failed authorization procedure. your.server.com (http-01): urn:acme:error:connection :: The server could not
connect to the client to verify the domain :: Fetching http://your.server.com /.well-known/acme-
challenge/G3RoBDc6pX55EqbZrJr6pihcBKIe8A4m2XZAv6dlojk:
Timeout during connect (likely firewall problem)"
```

This means the Let's Encrypt servers could not reach the HTTP 80 port of your server.
You have to check your Firewall rules in order to access

If the generation task is a success, your certificate will have a "Let's Encrypt Certificate" stamp in the table.

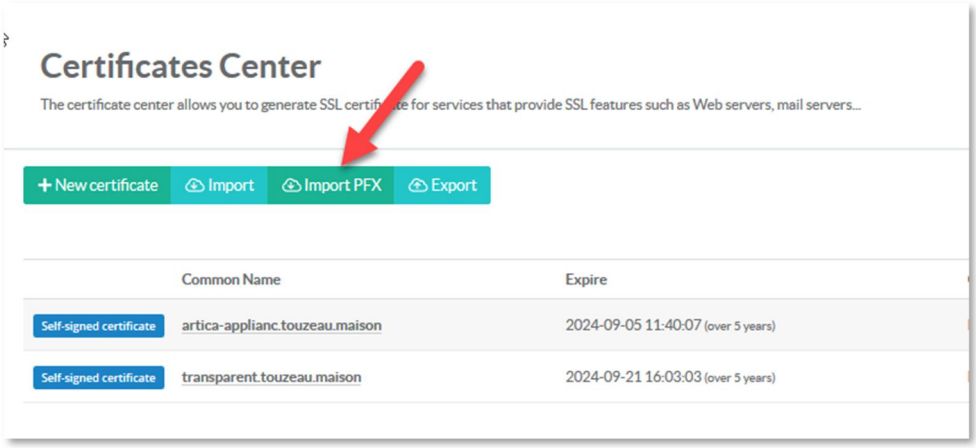


You will see that the certificate is only for 3 months.
You can perform the same procedure to renew it.

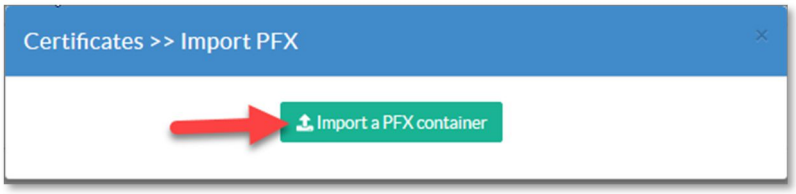
IMPORT A PFX

A PFX file is an encrypted security file that stores secure certificates used to authenticate a person or device, such as a computer or web server; requires a password to be opened; can be installed by right-clicking the file and selecting "Install PFX."
It is usually used on Windows system to export certificates.

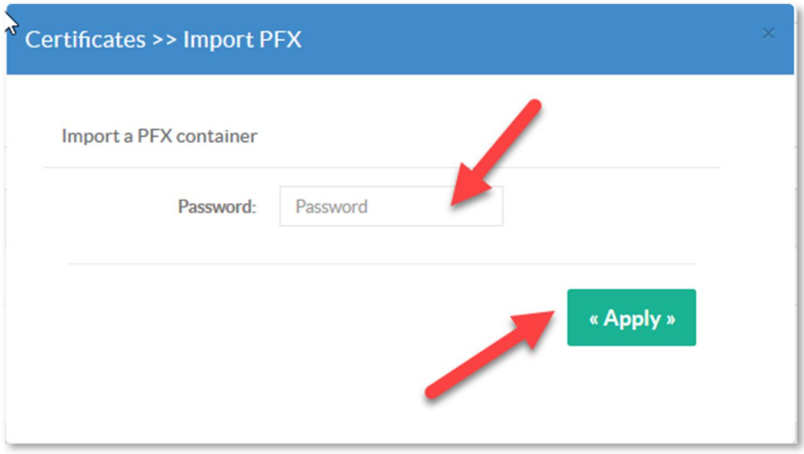
On the main certificates center, click on “Import PFX” button.



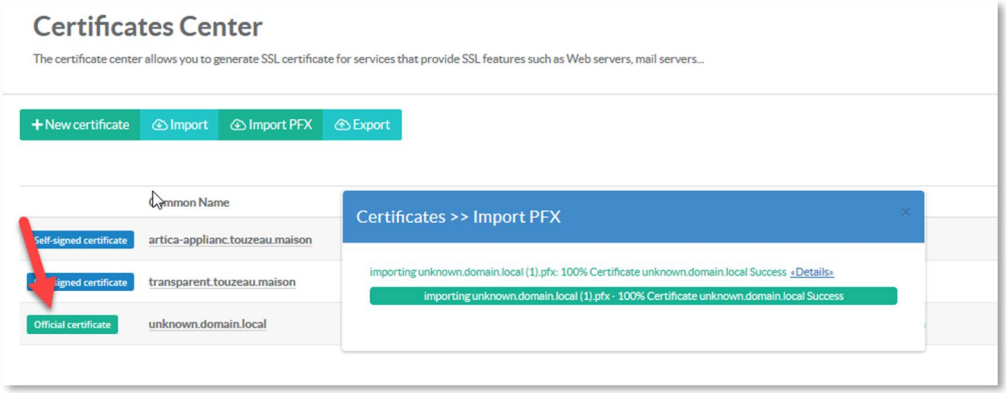
- Click on Import a PFX container button and browse your computer to select the PFX file you want to import



- Once uploaded, set the password protection and click on Apply button



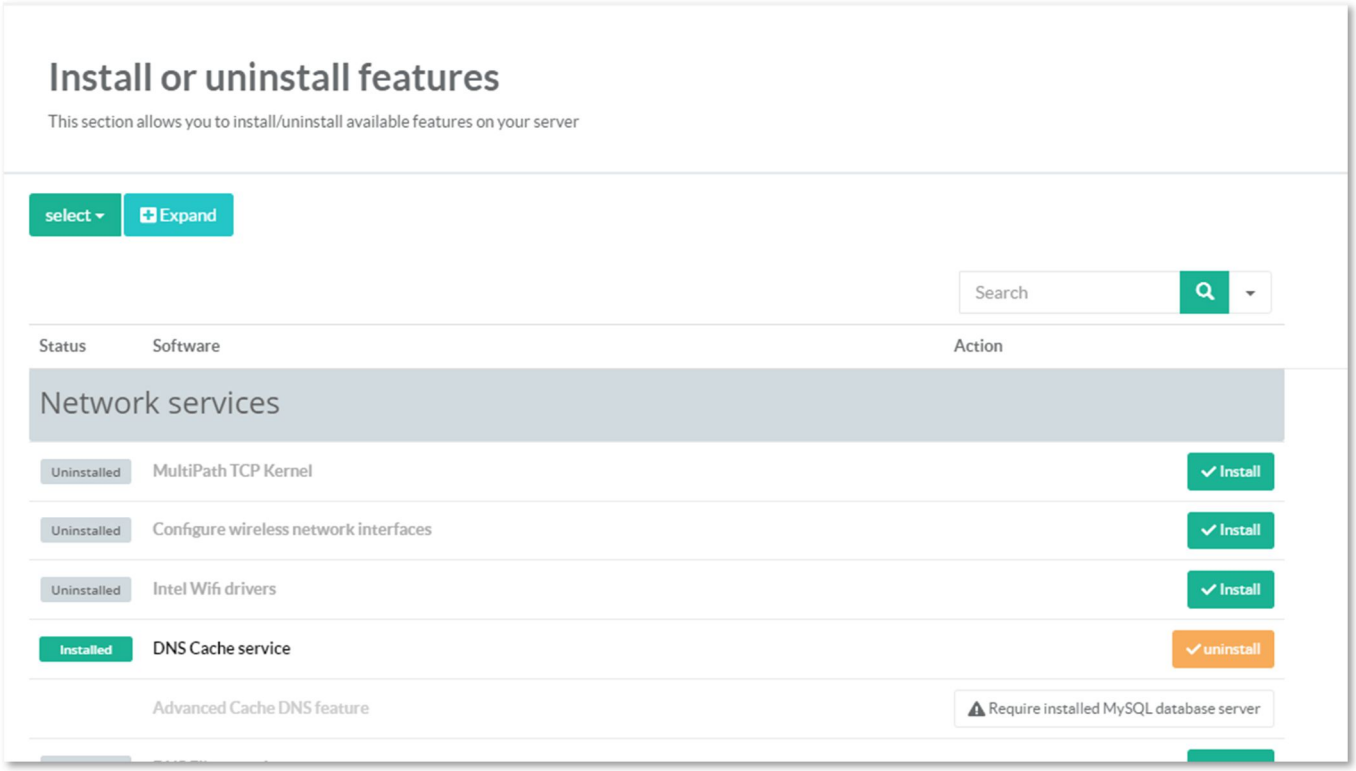
- If the certificate is correctly imported, you will see your certificate as an “**Official Certificate**”



MANAGE THE SYSTEM

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 available software that can be installed and managed on your system.



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

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…

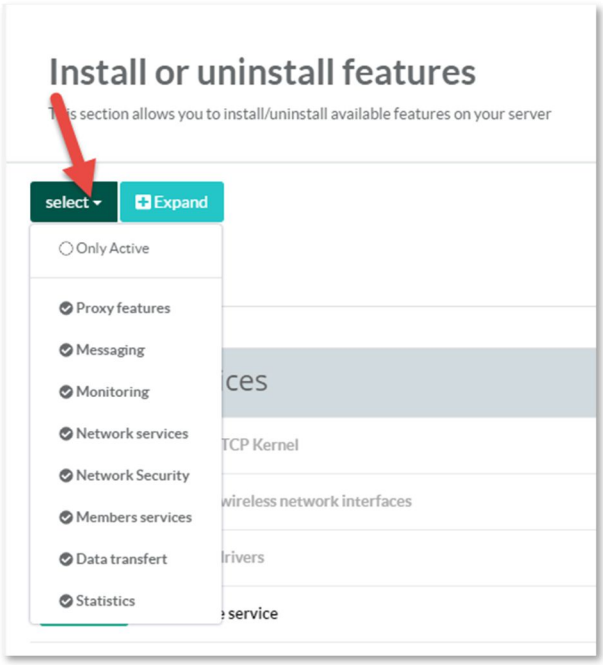
Messaging: Is the main part of the SMTP/IMAP service that can switch your server to an SMTP relay with Anti-SPAM and mailboxes servers.

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

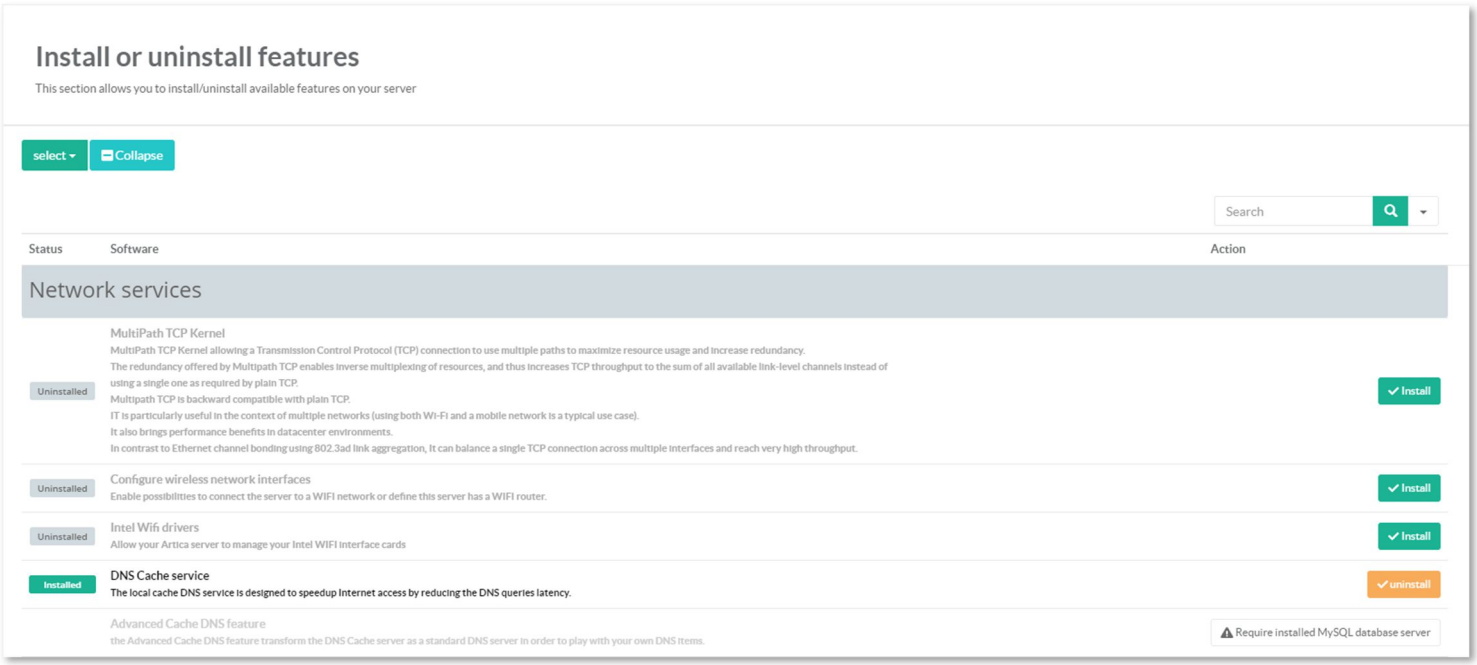
Network service: Allows you to install all services related to a gateway such, the DHCP service, the DNS service, the reverse and Web service, the VPN service…

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.



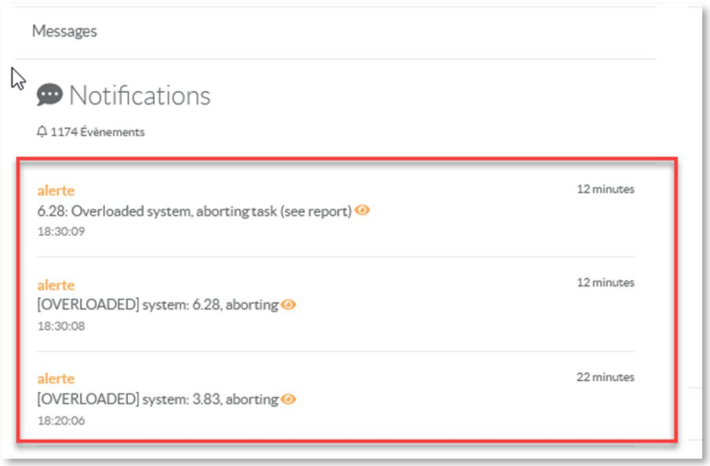
The **Expand/Collapse** button allows you to display/hide the description of each available service.



The expanded table display a description of each available service.

PROCESSES MANAGEMENT (OVERLOADED SYSTEM)

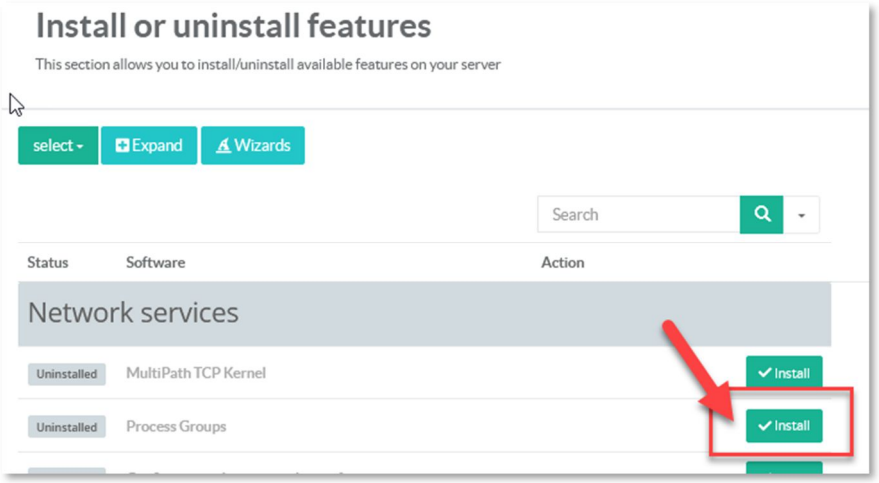
Depend of your hardware performance but sometimes you can see alerts about overloaded system.
If you encounter this behavior, that means some background Artica tasks use some disk and CPUs that consume server performance.



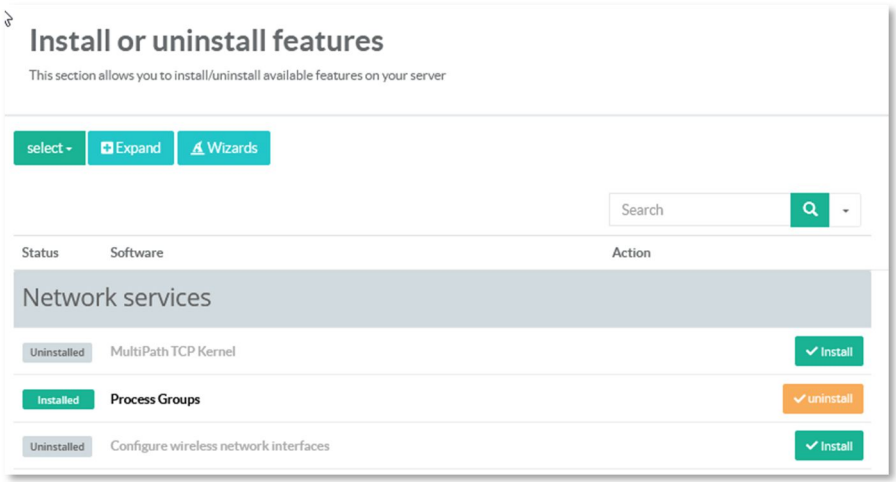
To avoid this issue, you can limit performance of these tasks by enclosing them in a performance bubble by installing "Processes Groups (cgroup)"

Install Processes Group

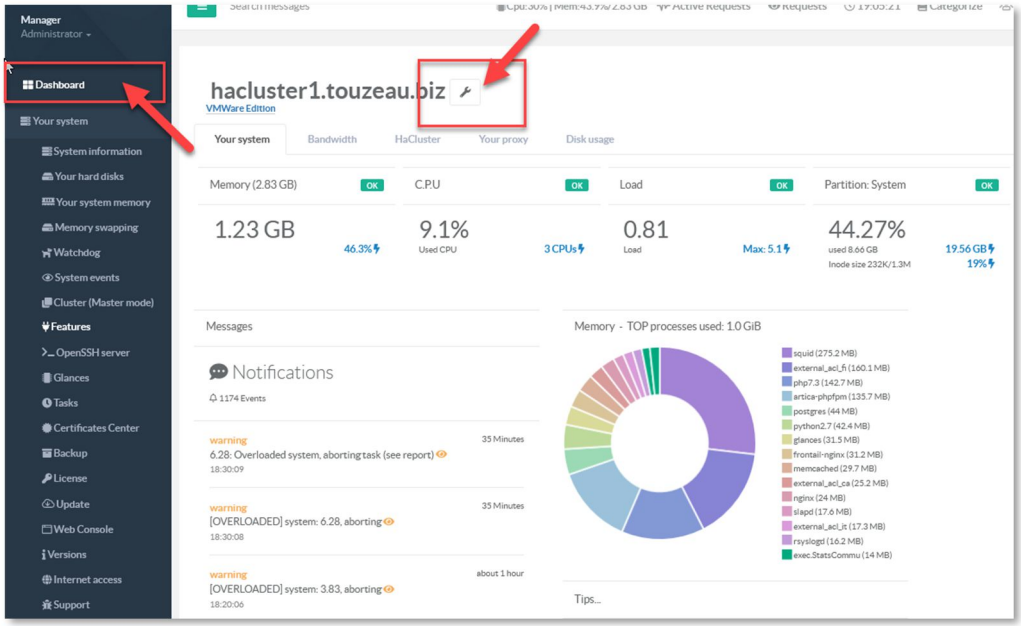
- On the feature section, click on **install** button on "**Processes Group**" row.

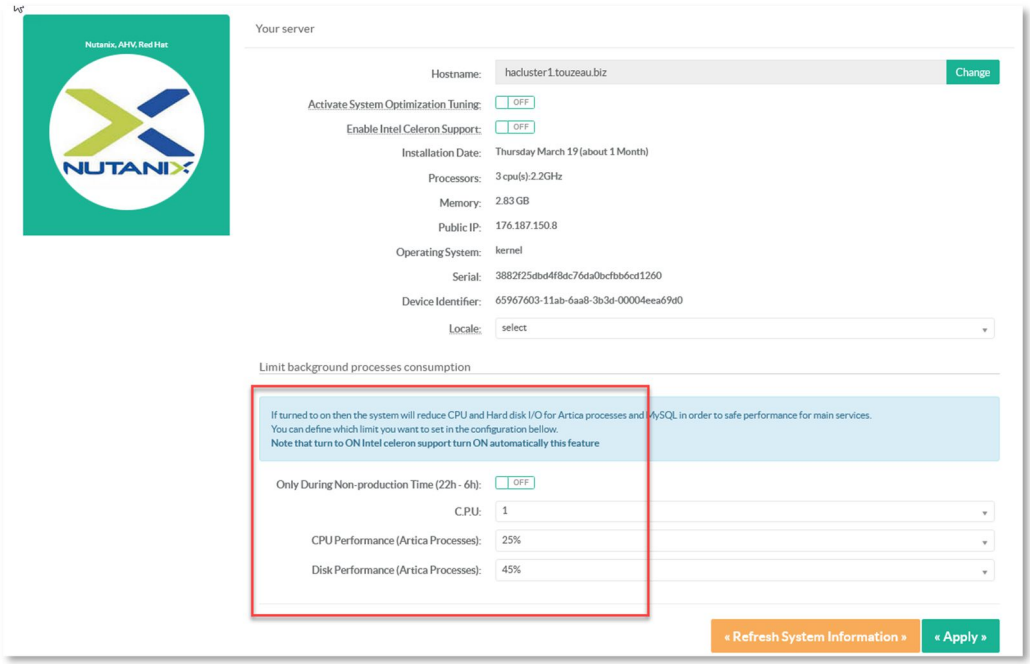


- The feature section must mark "Process Groups" as "**installed**"



- Open the dashboard and click on the **wrench** near the server hostname.(to close section, click again on the wrench)





Configure performances for background tasks

In the **"Limit background processes consumption"** section tune parameters as you like:

- **Only during the production time**:
  Means inside the production time, process are limited but outside the production time, processes are not limited (many tasks are scheduled to be running during the non-production time)

- **CPU**:
  Limit processes to use only one CPU, choose in the drop-down list the CPU that will be used.

- **CPU Performance**:
  Set here the max percentage of CPU a process can be use.

- **Disk performance**:
  Set here the disk access priority rate in percentage.

- **Bandwidth Disk (MB/s)**:
  Set here the read/write bandwidth allocated in MB/s (default 50Mb/s as a SATA)

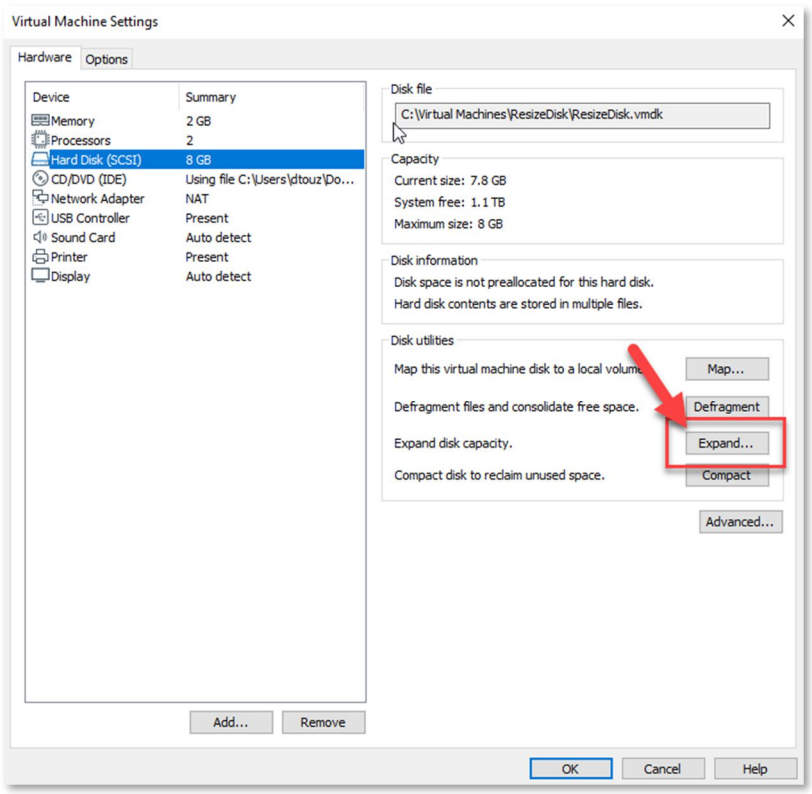
HARD DRIVES MANAGEMENT

Expand disk on a Virtual machine

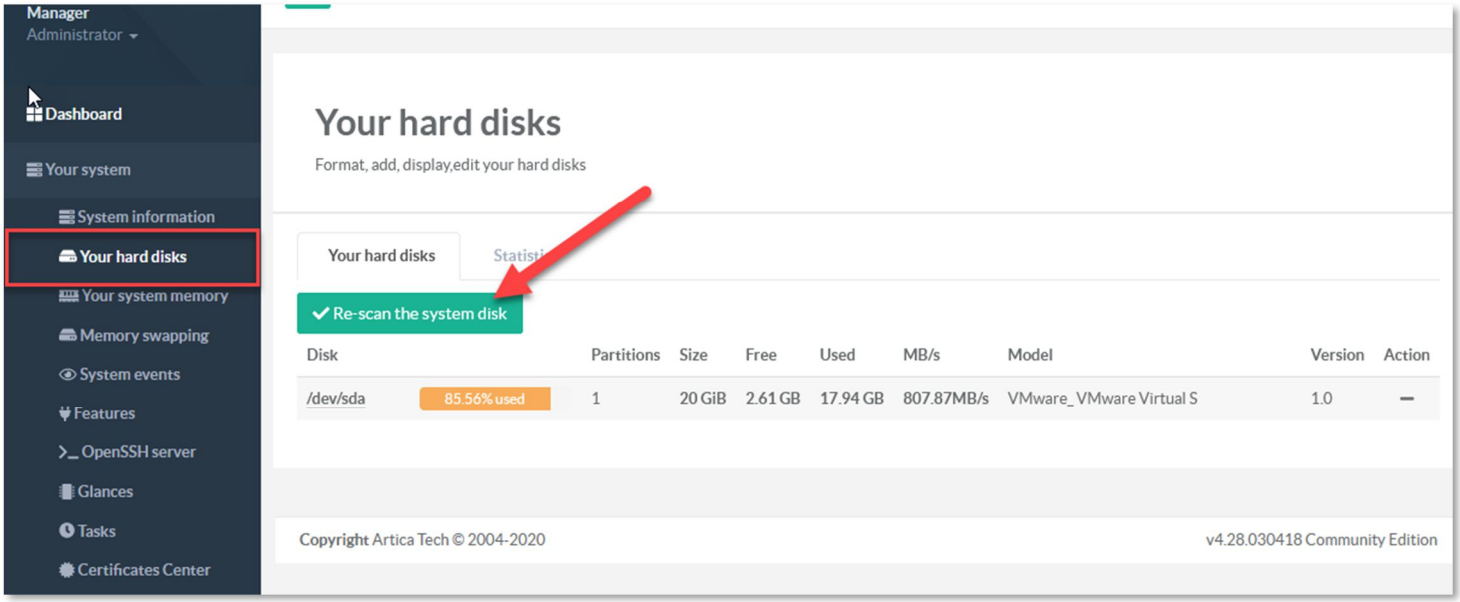
If you using Artica in a virtual environment, you can expand any disk used by Artica.

To expand a disk used by Artica you need to:

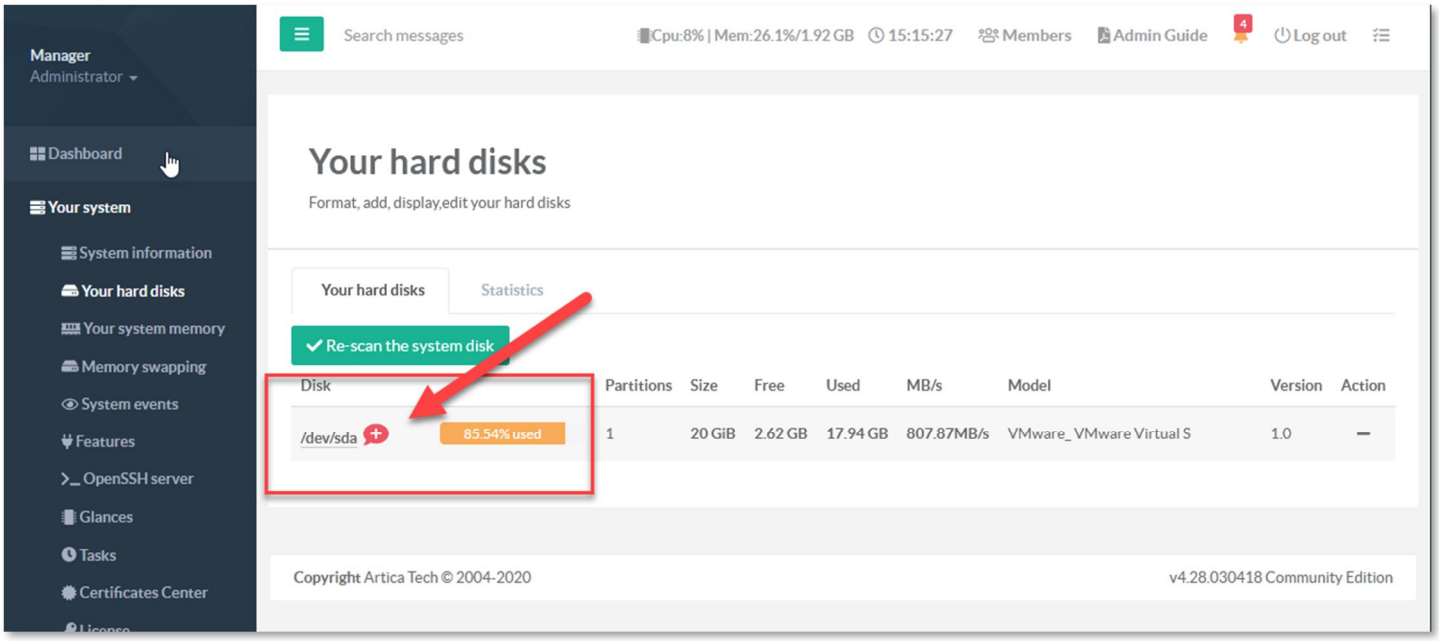
- Shut down the virtual machine.
- On your virtualization system, expand the disk to the desired size.
- Start the Artica Virtual machine.



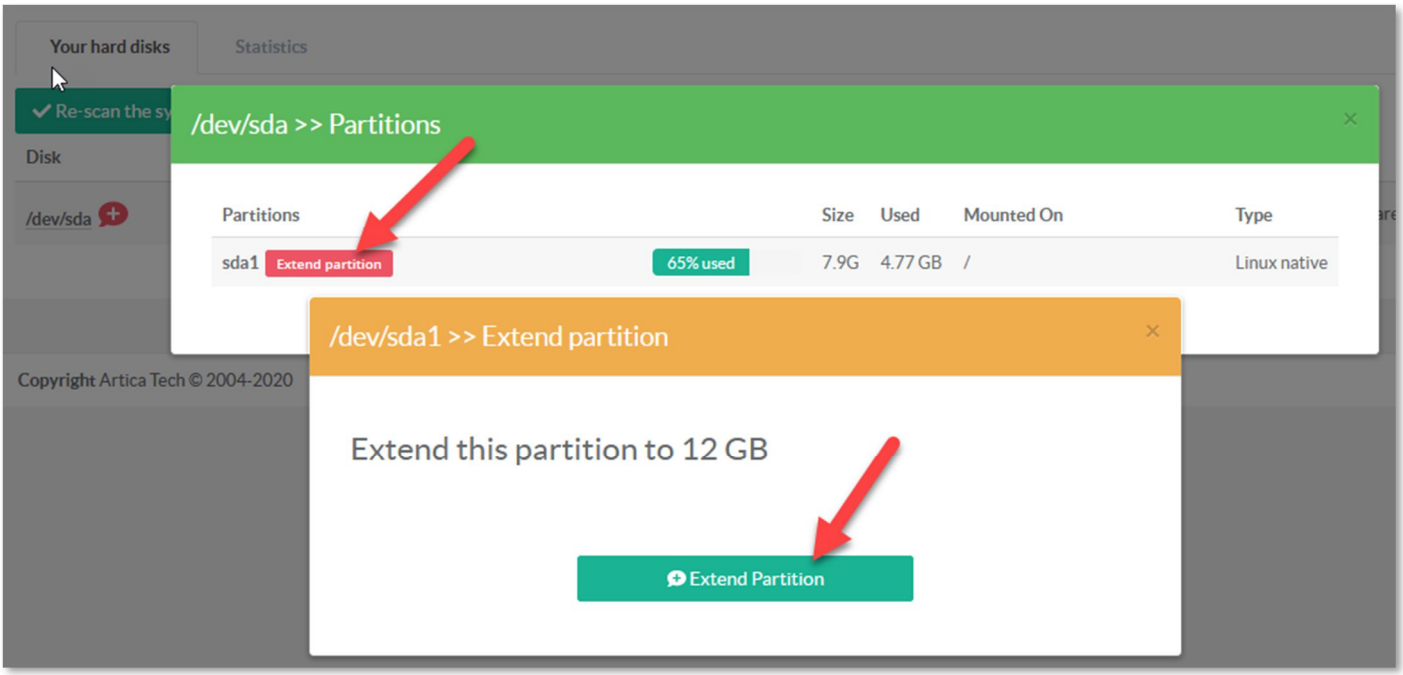
- On the Artica Web console, select **"Your System"** / "**Your hard disk**"
- Click on **Re-scan the system disk** button.



- If the disk can be extend a comment in red is displayed on your disk.
- Click on the disk to see details.



Click on the red label under the partition row that can be extend.
A new popup is displayed that allows you to confirm extend this partition.



A progress is displayed, after the 100% of the progress you will see that your disk will be extended.

A warning notification will be added in the system events section.

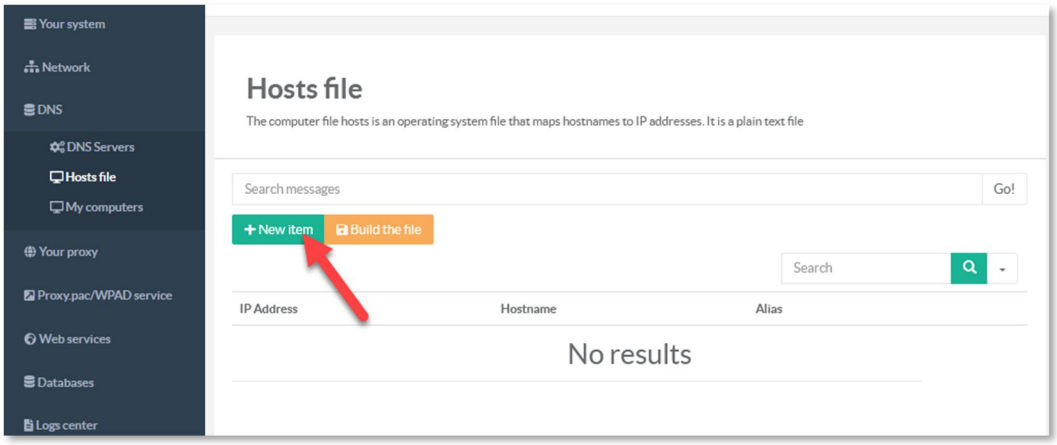
NETWORK

The Hosts file.

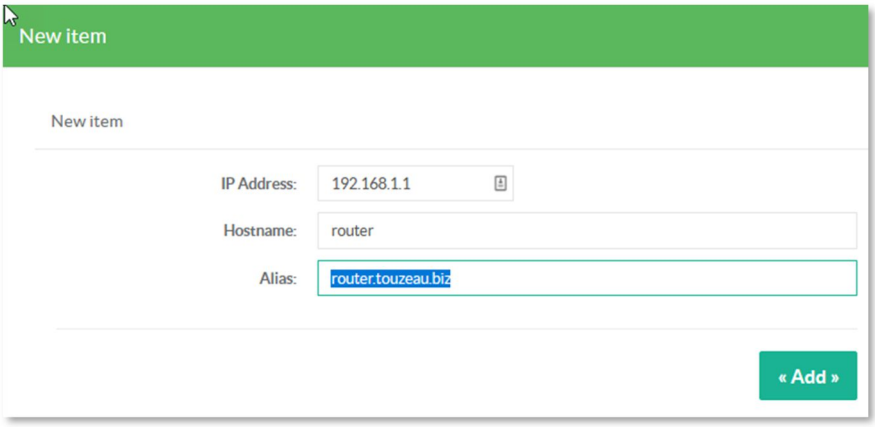
All operating systems with network support have a hosts file in order to translate hostnames to IP addresses.
Whenever you open a website by typing its hostname, your system will read first through the hosts file to check for the corresponding IP and then open it and after, query the available DNS servers.

Manage records in the host file

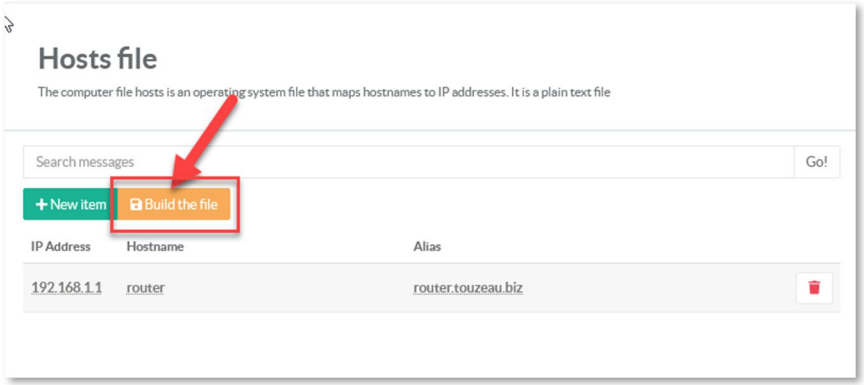
- To Manage the host file, open the left menu **DNS** / **Hosts file**



- To add an record, click on the "**New item**" button.



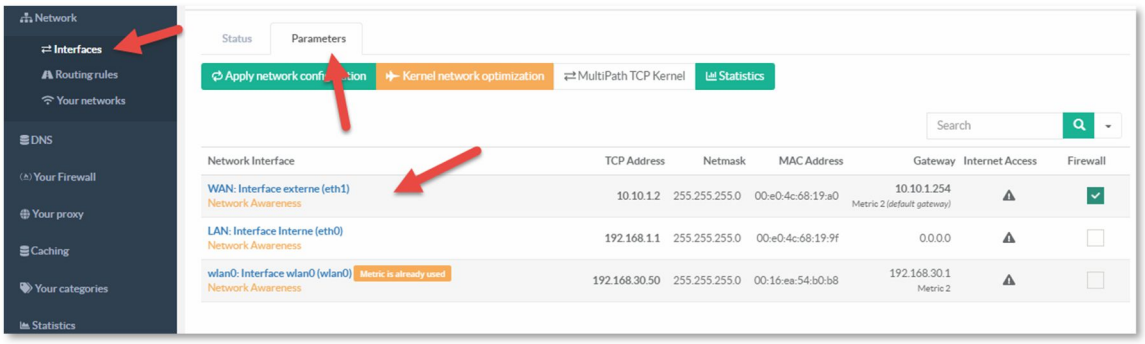
- Set the IP address
- In the hostname, the standard is to add just the "NetBIOS name" and the fully qualified hostname in the **Alias** field.
- Click on **Add** button to save the record
- Click on "**Build the file**" to make your records in production mode



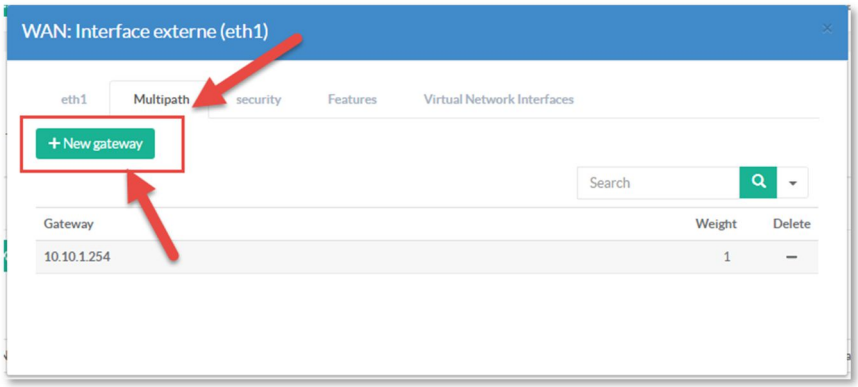
2 gateways for one interface.

It is possible to set up 2 gateways for one single Interface
If a gateway is down, the system will switch to the second one.

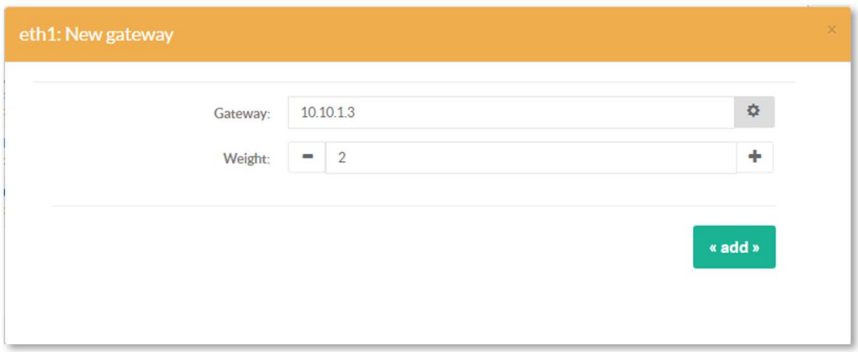
- On the left menu, choose **Network** and **Interfaces**
- Select the **Parameters** tab.



- Click on the desired network interface.
- Click on "**Multipath**" tab
- You will see in the table your main gateway originally assigned to the Interface.
- Click on "**New gateway**"



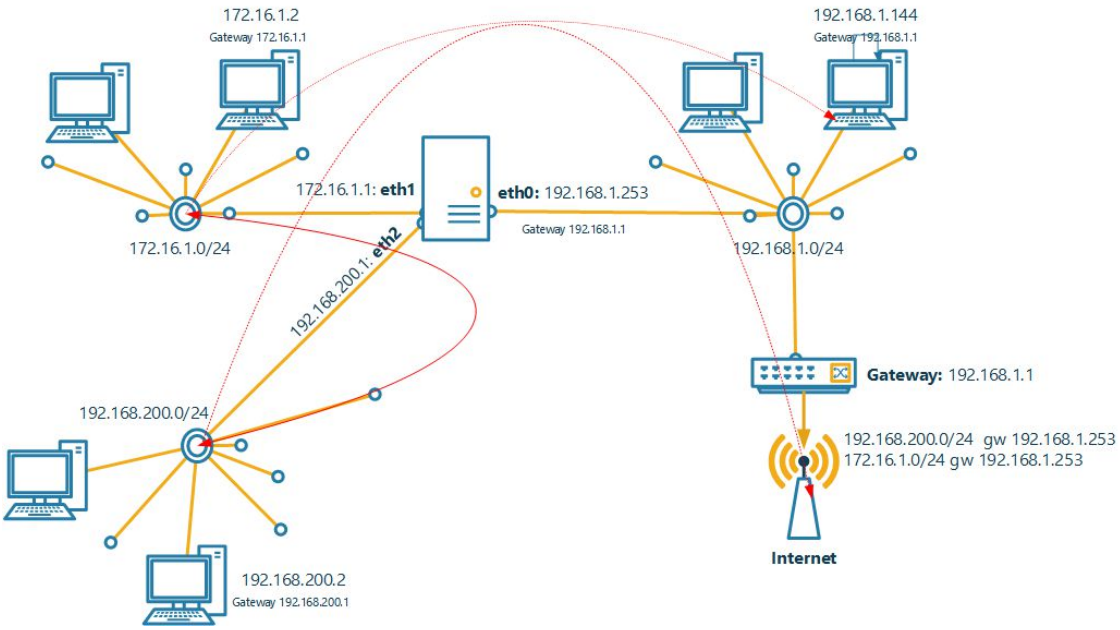
Add the second gateway IP address and set its weight.
If you define the weight as the same value as the main gateway, the system will process in a round-robin way.
If you define the weight up to the main gateway, the gateway 2 will be used only if the main gateway is down;



Using Artica as an advanced gateway

Artica can be used in order to act as gateway and router.

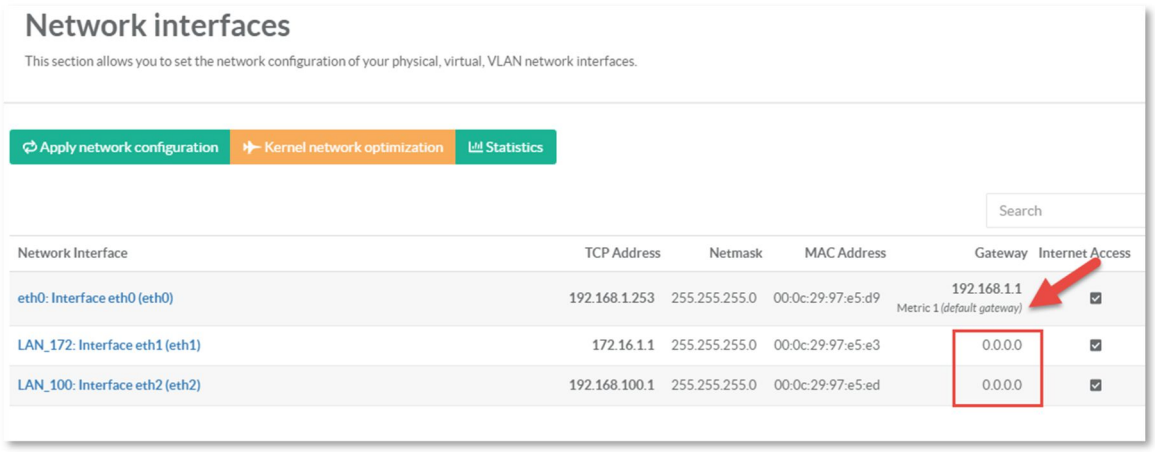
Here it is an example of a network



3 subnets, 172.16.1.0/24, 192.168.200.0/24 and 192.168.1.0/24
Artica uses 3 network interfaces,
Eth1 linked to 172.16.1.0/24 network and is the main gateway (172.16.1.1)
Eth2 linked to 192.168.100.0/24 network and is the main gateway (192.168.100.1)
Eth0 linked to 192.168.1.0/24 network but act just as client of a remote gateway 192.168.1.1 to access to Internet.

172.16.1.0/24 can discuss with 192.168.100.0/24 and 192.168.1.0/24 and have Internet Access
192.168.100.0/24 can discuss with 172.16.1.0/24 and 192.168.1.0/24 and eth have Internet Access
192.168.1.0/24 **cannot discuss** with 192.168.100.0/24 and 172.16.1.0/24

Our eth1 and eth2 is the gateway of their networks, so you have to define 0.0.0.0 in each Internet Address configuration.
Under network interfaces section, make sure that Interfaces act as gateway for the designed network have 0.0.0.0
Make sure that the Interface that use the gateway to access to Internet is marked as "**Default gateway**" on the routing rules
,



IP Masquerading multiple internal networks

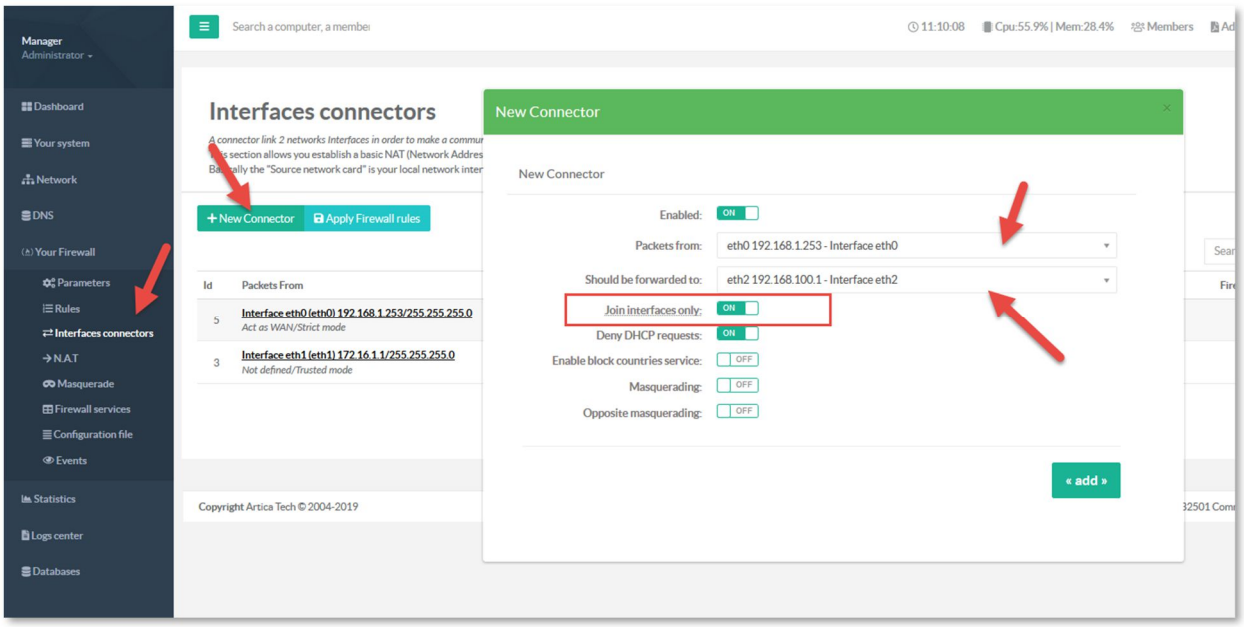
Masquerading more than one internal network is fairly simple. You need to first make sure that all of your networks are running correctly (both internal and external). You then need to enable traffic to pass to both the other internal interfaces and to be MASQued to the Internet.

Next, you need to enable Masquerading on the INTERNAL interfaces.

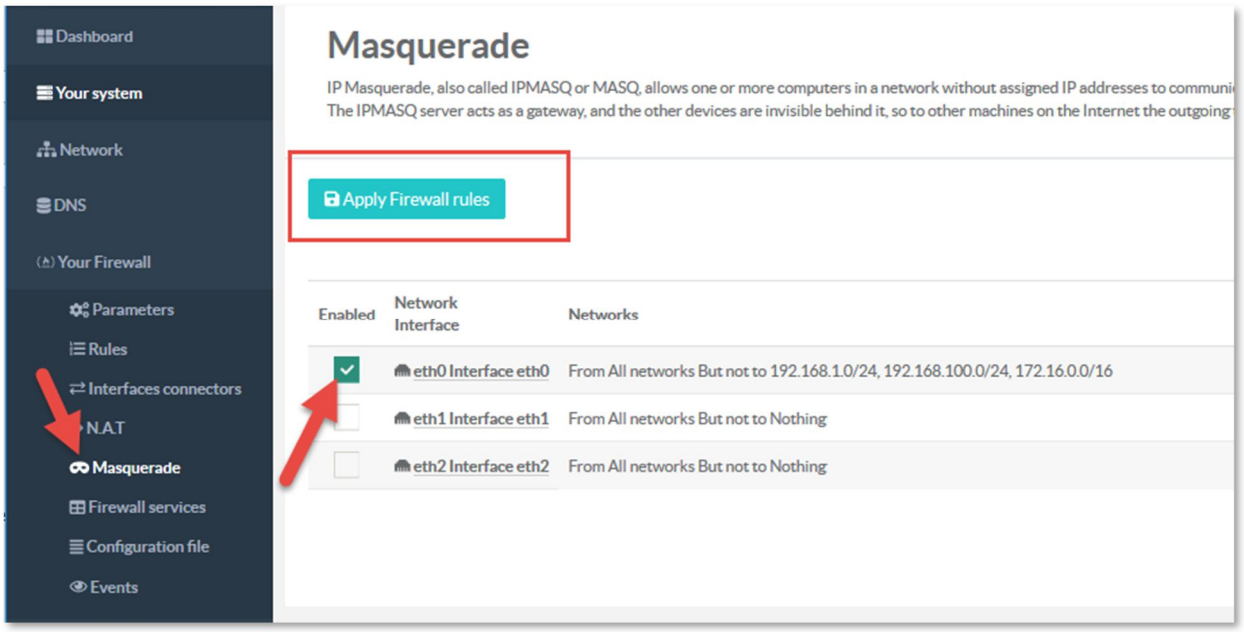
The example uses a total of THREE interfaces: eth0 stands for the eth0 interface which is the EXTERNAL connection to the Internet. LAN_172 stands for the eth1 interface and is the 172.16.1.0 network. Finally, LAN_100 stands for the eth2 interface and is the 192.168.100 network. Both LAN_172 and, LAN_100 will be MASQued out of interface eth0. In your firewall ruleset next to the existing MASQ at the very end of the ruleset, add the following:

Firewall Interfaces connectors

- On the left menu, choose "**Your Firewall**" and **"Interfaces connectors**"
- With the "New connector" button create a rule in order to link interfaces.
- You can enable the "**Join interfaces only**" option that just make Interfaces linking but did not create any Firewall rules on the forward TCP packets.



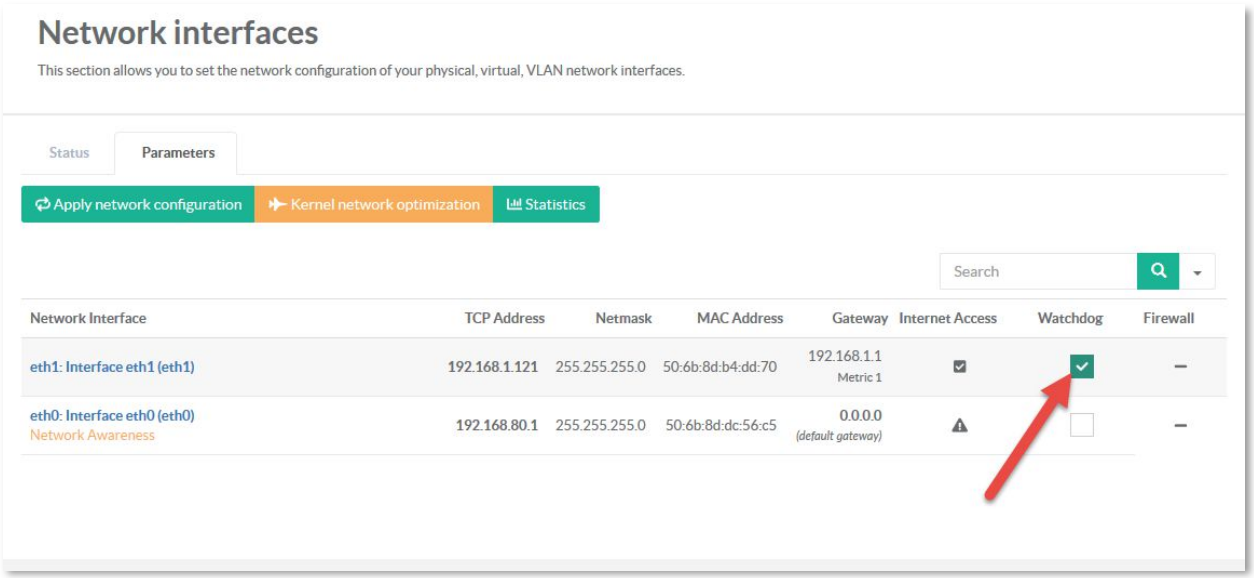
Click on **Masquerade** left menu and enable the checkbox for the Interface that act as WAN in order to masquerade outgoing packets.
Please note that it is CORRECT to have "eth0". The reason for this is the kernel needs to know which interface is used for OUTGOING traffic. Since eth0 in the above examples is the Internet connection, it is must be listed for each internal interface.



Finally, click on "**Apply Firewall rules**"

Interfaces Watchdog

The Interface Watchdog is able to reconfigure network if it detects a failed linked interface (for example an unplugged cable or a reloading driver).



If enabled in the main table, Artica will automatically reconfigure the network on a failed interface and send a notification with the last kernel events to see why the link was suddenly down.

Just click on the watchdog column of the Interface you want to monito
.
r.

Wan optimization

You can optimize TCP connection in Artica by just enable some kernel parameters, especially if Artica is defined as Proxy, Web server or gateway.

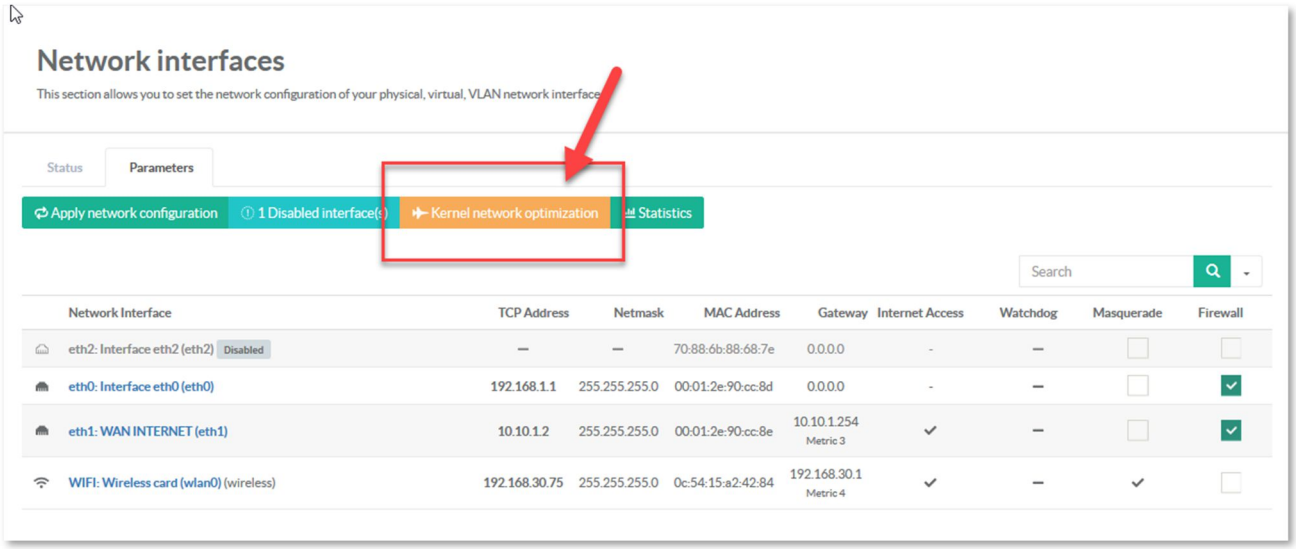
TCP BBR congestion control

TCP BBR is used by Google Cloud platform successfully and increase the traffic by more 14%
https://cloud.google.com/blog/products/gcp/tcp-bbr-congestion-control-comes-to-gcp-your-internet-just-got-faster

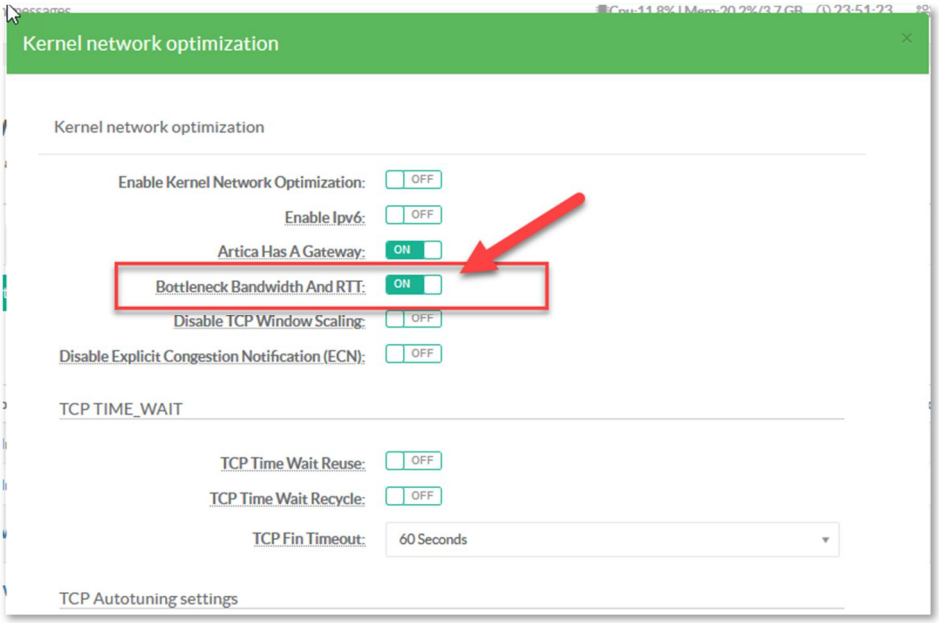
TCP BBR is a TCP congestion control algorithm developed by Google. It tackles shortcomings of traditional TCP congestion control algorithms (Reno or CUBIC). According to Google, it can achieve orders of magnitude higher bandwidth and lower latency.

TCP BBR is already being used on Google.com, YouTube and Google Cloud Platform and the Internet Engineering Task Force (IETF) has been standardizing this algorithm Since July, 2017. BBR stands for Bottleneck Bandwidth and RTT

- To enable TCP BBR, on the network section, choose "**Kernel Network optimization**"



- Turn on the **"Bottleneck Bandwidth And RTT**" option and click on "**Apply**" button



TCP window-size scaling

Sending more data at a time

To increase TCP performance, the way is to send more data at a time.
As the bandwidth of the network increases, more data can fit into the pipe (network), and as the pipe gets longer, it takes longer to acknowledge the receipt of the data.
This relationship is known as the bandwidth-delay product (BDP).
This is calculated as the bandwidth multiplied by the round-trip time (RTT), resulting in a value that specifies the optimal number of bits to send in order to fill the pipe. The formula is this:

```
BDP (bits) = bandwidth (bits/second) * RTT (seconds)
```

Computed BDP is used as TCP window size for optimization.

For example, imagine that you have a **10 Gbps** network with an RTT of **30 milliseconds**.

For the window size, use the value of the original TCP window size (65535 bytes).
This value doesn't come close to taking advantage of the bandwidth capability.

The maximum TCP performance possible on this link is as follows:

- (65535 bytes * 8 bits/byte) = bandwidth * 0.030 second
- bandwidth = (65535 bytes * 8 bits/byte) / 0.030 second
- bandwidth = 524280 bits / 0.030 second
- bandwidth = 17476000 bits / second
-

To state it another way, these values result in throughput that's a bit more than 17 Mbits per second, which is a small fraction of network's 10 Gbps capability.

TCP window-size scaling

To resolve the performance limitations imposed by the original design of TCP window size, extensions to the TCP protocol were introduced that allow the window size to be scaled to much larger values.
Window scaling supports windows up to **1,073,725,440** bytes, or almost 1 GiB.
This feature is outlined in RFC 1323 as TCP window scale option.
The window scale extensions expand the definition of the TCP window to use 32 bits, and then use a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header

You can use the previous example to show the benefit of having window scaling.
As before, assume a 10 Gbps network with 30-millisecond latency, and then compute a new window size using this formula:

```
(Link speed * latency) / 8 bits = window size
```

If you plug in the example numbers, you get this:

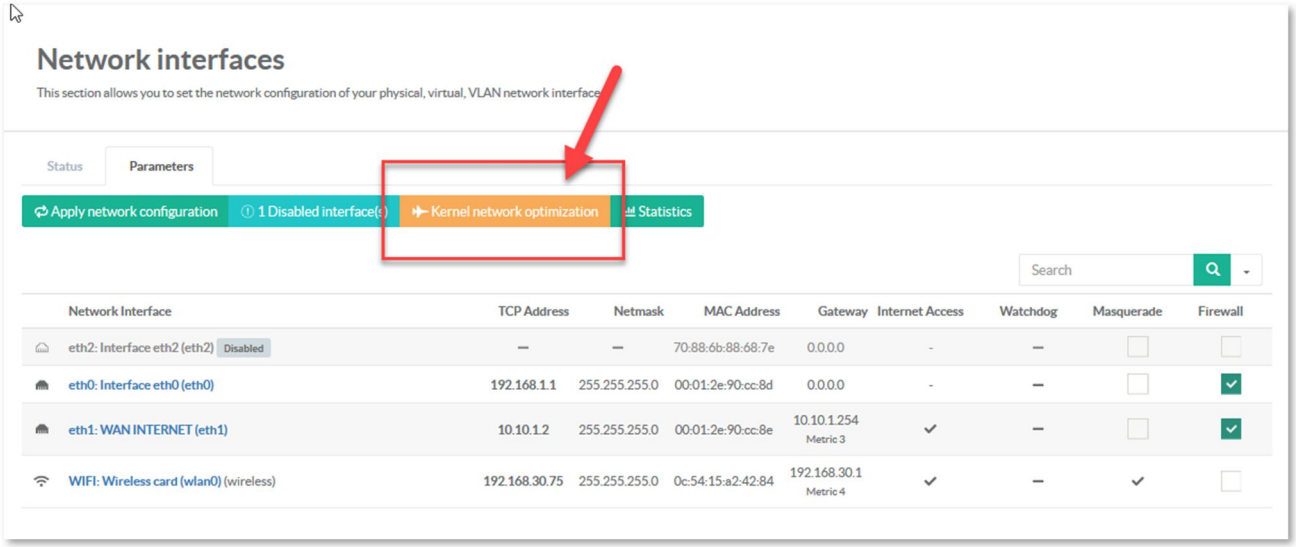
```
(10 Gbps * 30ms/1000sec) / 8bits/byte = window size
(10000 Mbps * 0.030 second) / 8 bits/byte = 37.5 MB
```

Increasing the TCP window size to 37 MB can increase the theoretical limit of TCP bulk transfer performance to a value approaching the network capability.

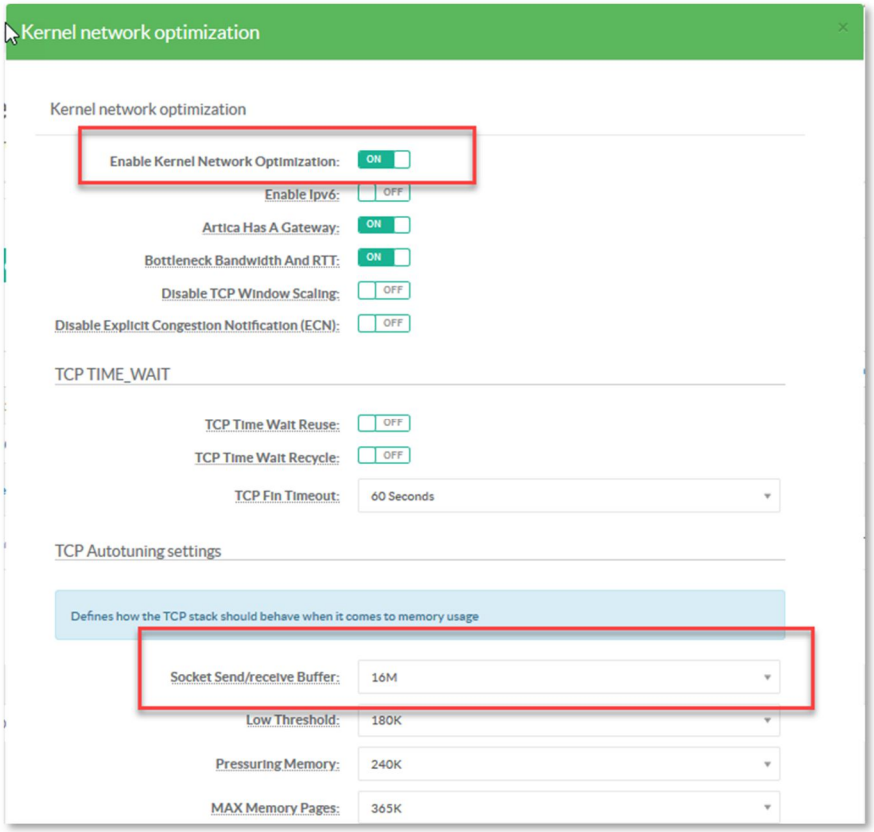
Of course, many other factors can limit performance, including system overhead, average packet size, and number of other flows sharing the link, but as you can see, the window size substantially mitigates the limits imposed by the previous limited window size.

To change the TCP windows size :

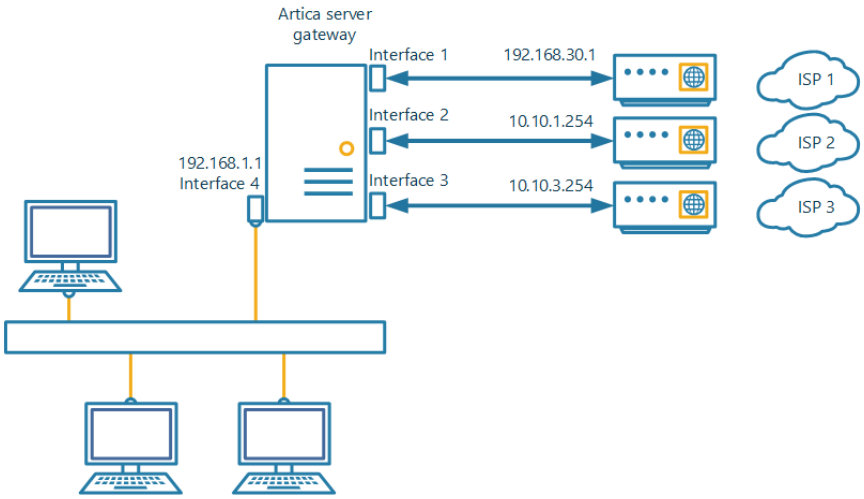
- On the network section, choose "**Kernel Network optimization**"



- Turn on the **"Enable Kernel Network optimization"**
- According the formula about your network capacity, change the value of "**Socket Send/receive buffer**"
- Click on "**Apply**" button



Link Balancer



Link Balancer is a feature to help you manage multiple internet connections, or in-general multiple connections between any two points and apply policy-based routing.

Link Balancer has 4 key functions:

1. **It can check all your gateways, if they are alive**.
   You can even write your own checks for your gateways.
   Link Balancer can continuously monitor them and react to failures.

2. **It can set multiple default gateways that will be used in a weighted round-robin fashion**.
   Link Balancer can configure your routing tables to achieve optimal balancing of all your upstream providers, or balance multiple VPN links.

3. **It can manage your routing tables**.
   Link Balancer will copy routing tables and apply all changes incrementally, after comparing routing tables line by line.

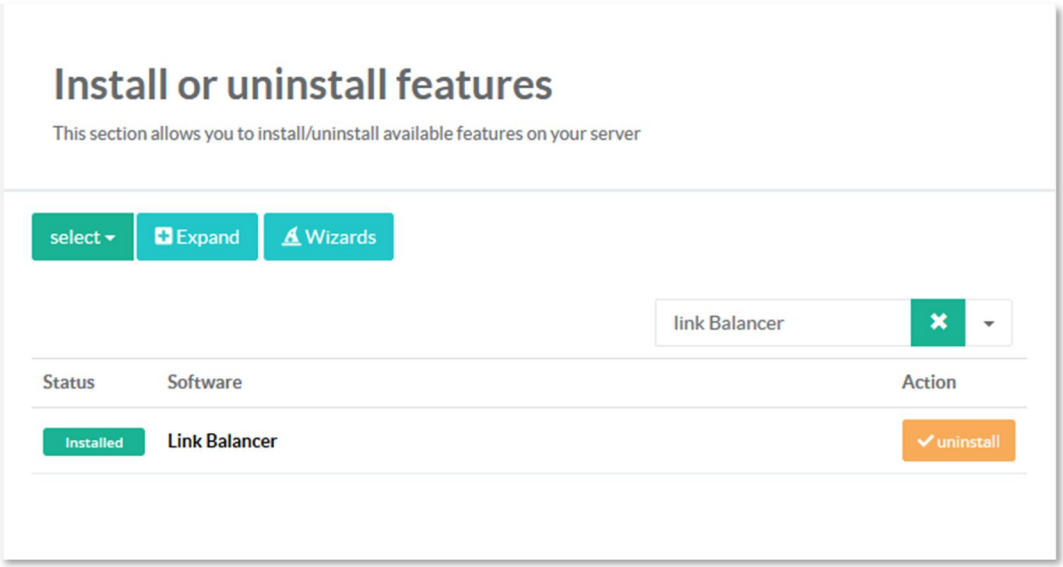
4. **It can apply policy-based routing rules**.
   Link Balancer can configure policy based routing rules, allowing you to configure routes based both on source and destination IPs, on marks, tos, etc.

For example, the following can all be handled by Link Balancer:

- 2+ internet provider links are balanced concurrently.
- Balancing is implemented using weights, so that each provider is getting a percentage of the connections. The links do not need to be of the same speed.
- In cooperation with the Firewall Feature, even individual services may have special routing (for example SMTP goes through DSL A, HTTP through DSL B, anything else through DSL C).

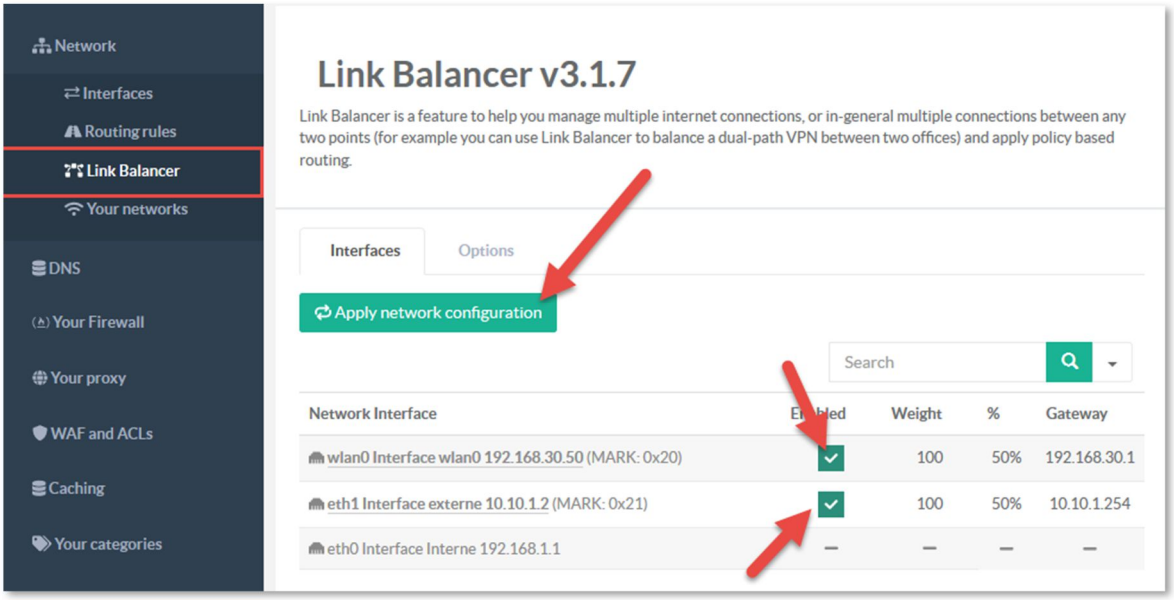
Install Link balancer

- On "**Your System**" left menu, choose "**Features**"
- On the search field, type "**Link balancer**"
- Click on **Install** button



Select load-balanced Interfaces

- After installed the Link Balancer service, on the left menu, choose "Network" and "Link balancer" option.
- The first section "**Interfaces**" list all available Interfaces that have a designed gateway.
- Click on the checkbox of the Interface that are connected to your ISP.
  You must have at least 2 network interfaces with 2 ISPs.

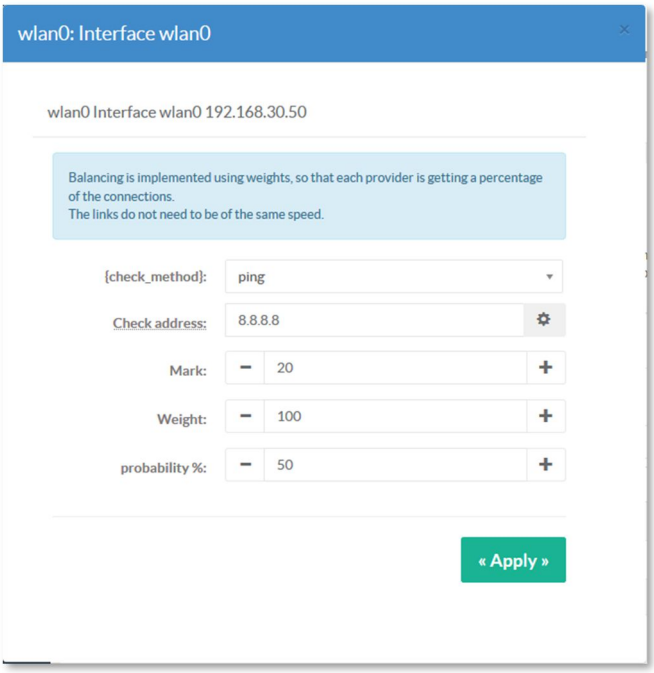


Tune the balance

If you plan to use the proxy in transparent mode, you think that you need balance using the proxy "MARK" Web Application Firewall feature.
The balancing system use 2 methods:

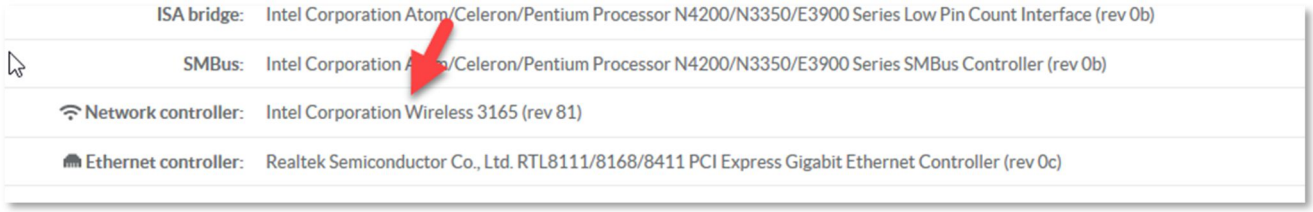
1. The weight that drive the priority of the Interface use.
2. The percentage that drive the probability to mark packets in order to be forwarded to the right Interface.

When clicking on the interface from the table, a parameters layer is displayed.



WIFI Management

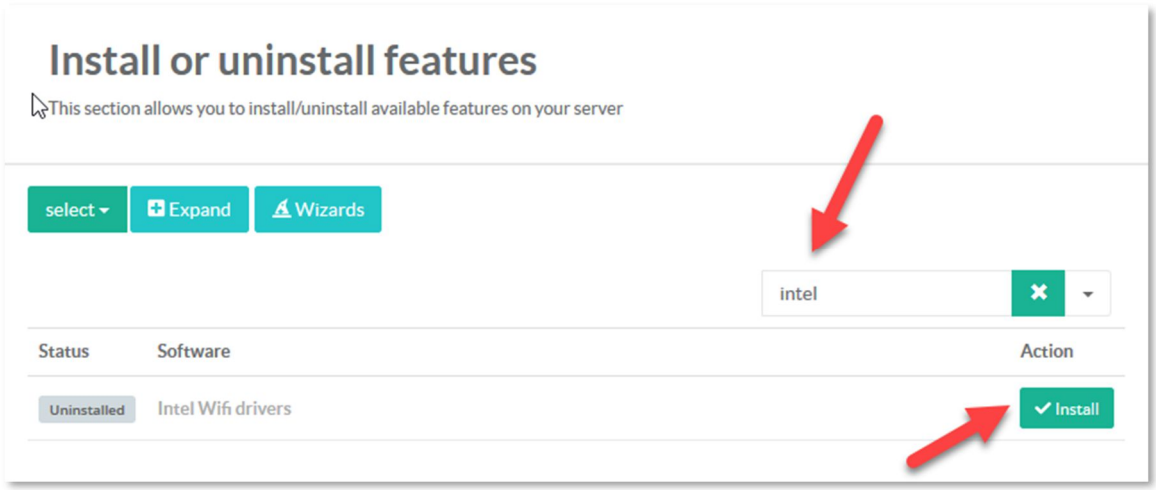
If you install Artica on a physical machine you can manage your WIFI network interface (if it is detected).
You can see your Network Interfaces in the left menu "**Your System / System information**"
A wifi icon is displayed if your server handle a Wireless network interface



Intel WIFI Network interfaces

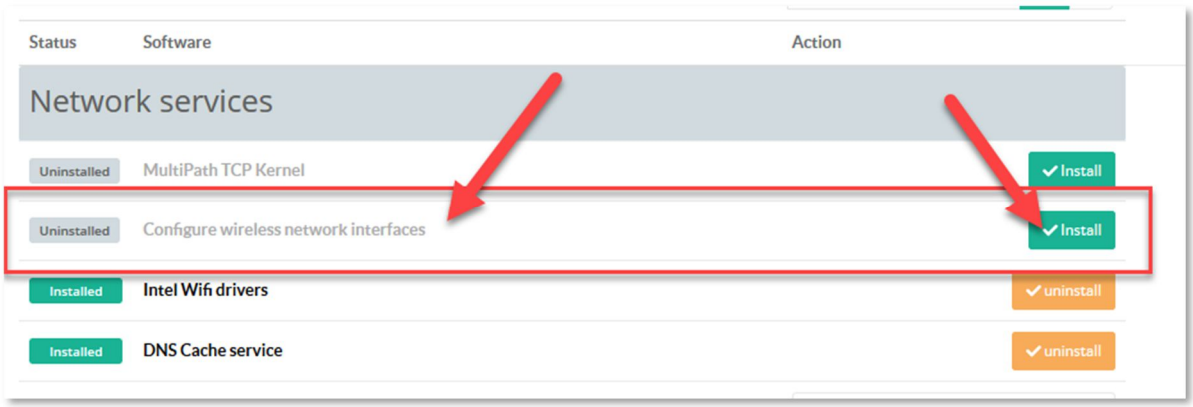
If your server use Intel WIFI, you can install necessaries drivers with the Features section.

1. On the features section, in the search field type "**intel**"
2. Click on **Install** button
3. **Reboot** your server



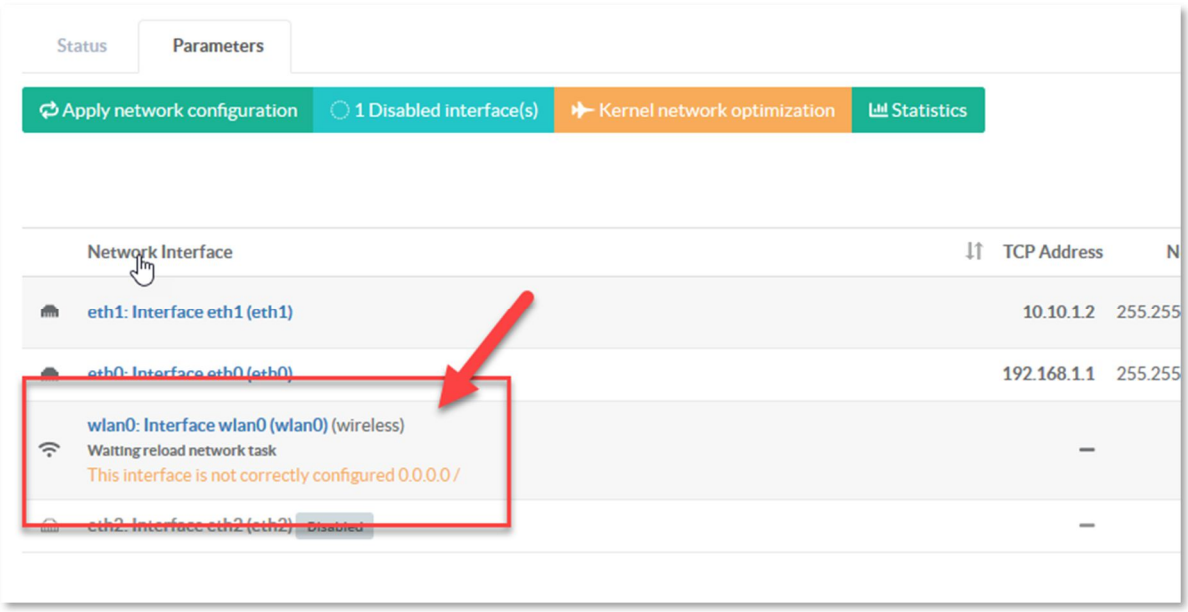
Enable Wireless capabilities

On the Features section, in the search feature, type "wireless"
Click on Install button on "**Configure wireless network interfaces**" row

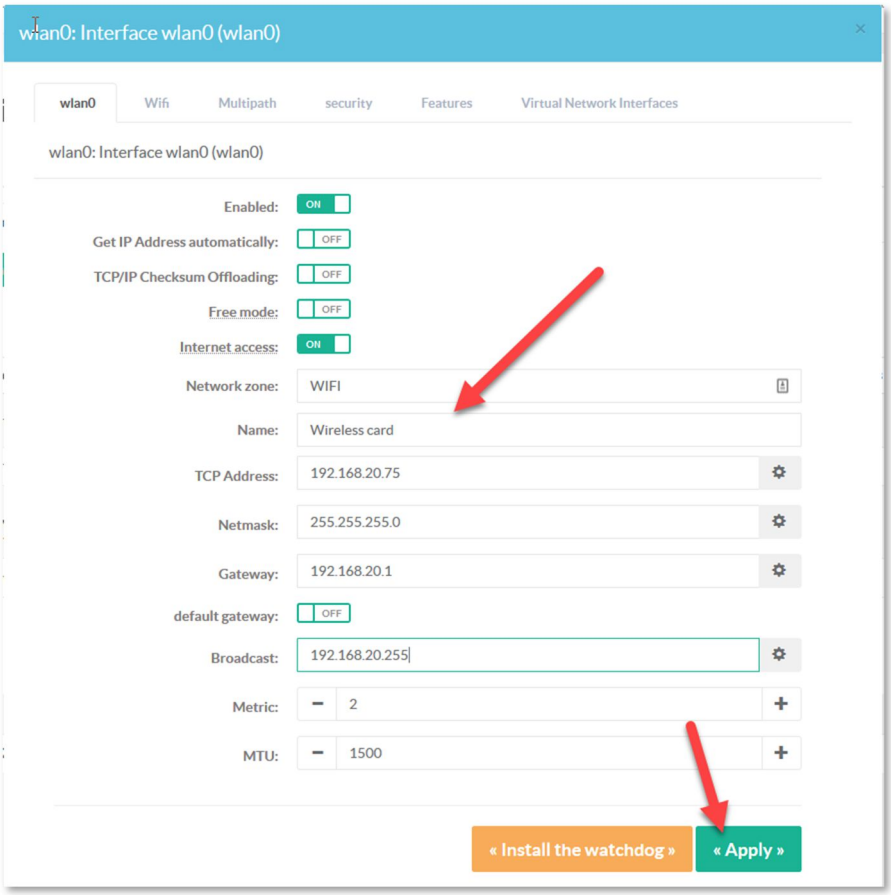


Configure your wireless interface

If your Network wireless card is detected, in Your Network / Interfaces / Parameters table, you should see a Wireless network interface.
Click on the Interface name.

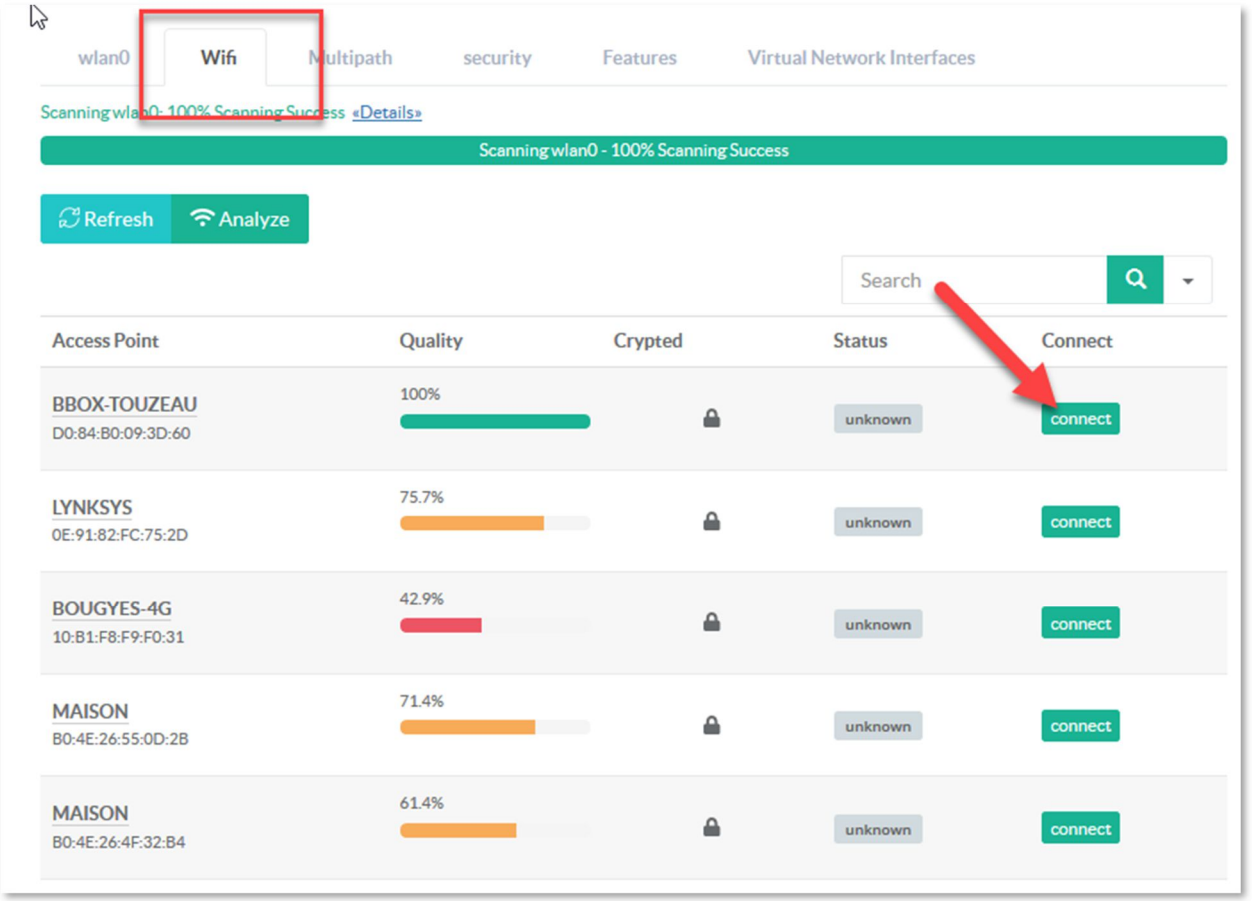


Define global network parameters and click on "**Apply**" button

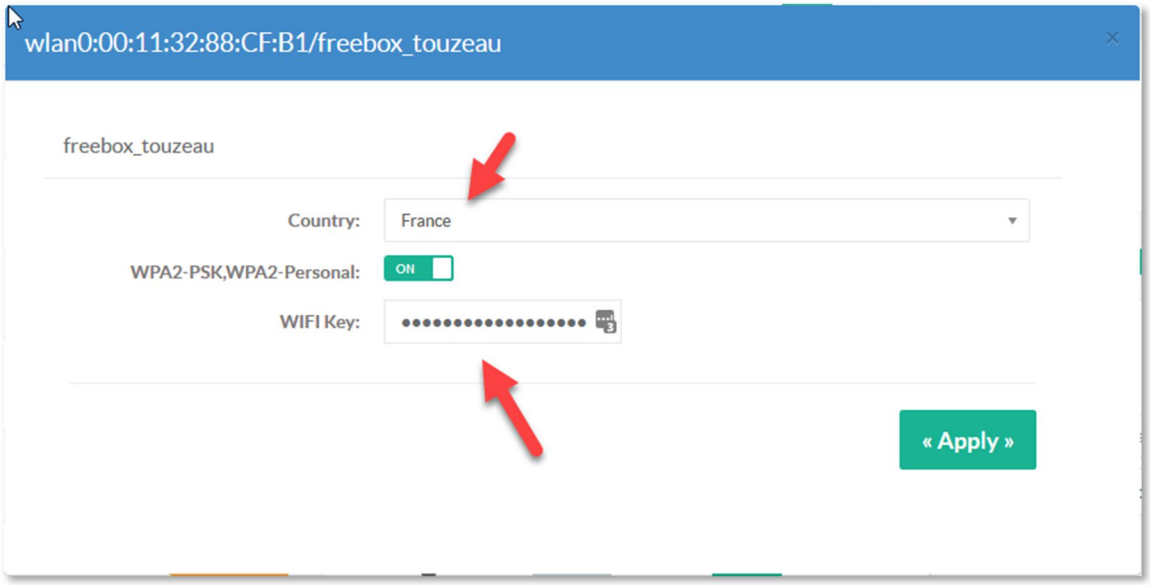


Join a WI-FI network

On the Wireless Interface card settings, click on "Wifi" tab.
A table is displayed and shows you all available network you can join.
You can see the Wireless quality in order to choose the best one.

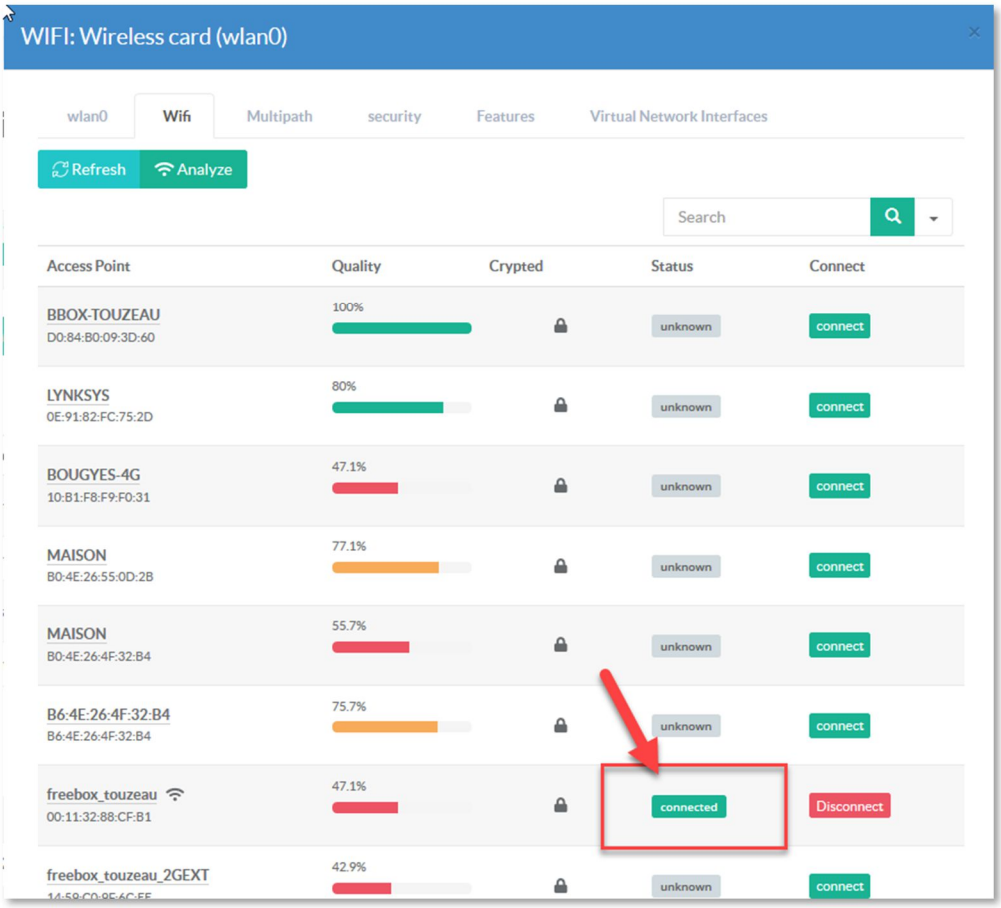


Define WI-FI parameters and click on **Apply** button.



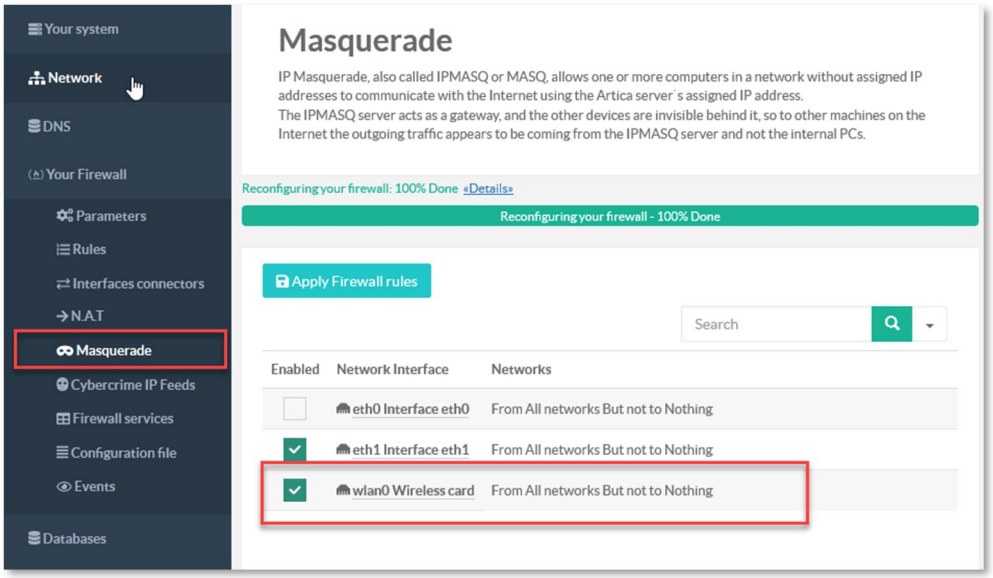
WI-FI status

If the wireless network interface is linked to the WI-FI network, you should see “Connected” in the status column.
You are able to disconnect by using the “Disconnect” button.



Masquerading

If your wireless Interface need to communicate with the Internet access, did not forget to “Masquerade” it.

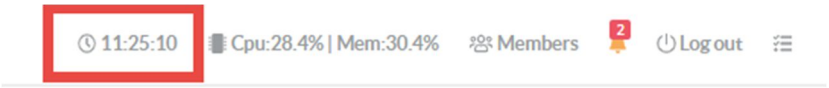


TIME AND CLOCK

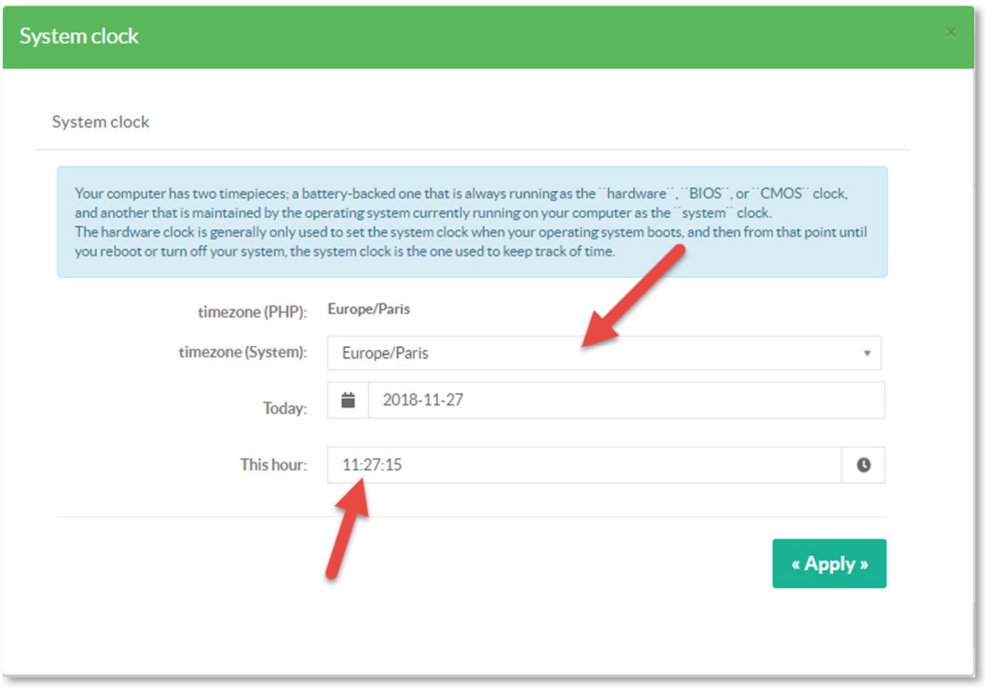
Set the time is important for Artica, events and statistics are based on the system time.

Set the Time zone and clock

A time zone is a region where the same standard time is used,
On the top menu, click on the displayed time



The system clock section is displayed and allows you to change the Time zone country and the system Clock.

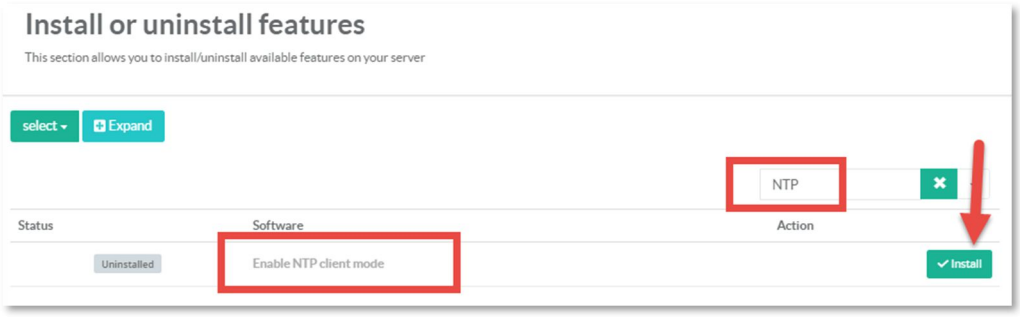


Basically, Artica can act as a time-server for your network or a time client.

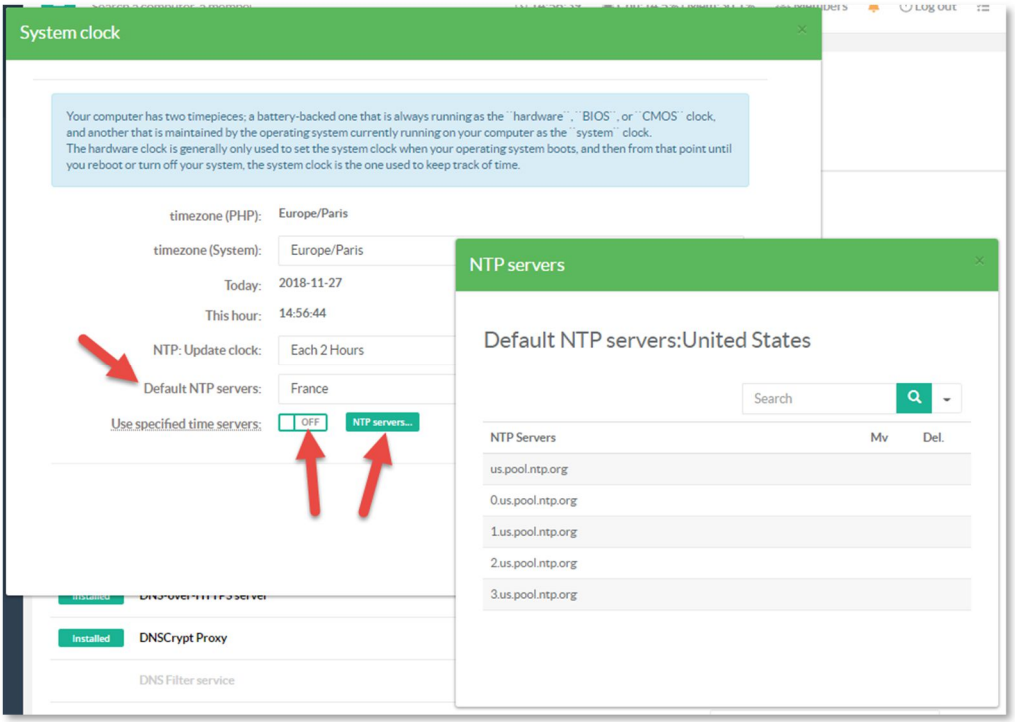
NTP time client.

When installing the Time client, your Artica server is designed to be synchronized automatically with a set of time servers.
This is the reason you did not have to manually change the clock when turning Artica to NTP Time Client
On the Features section search the entry "NTP".

Click on the **Install** button under the **Enable NTP client mode**

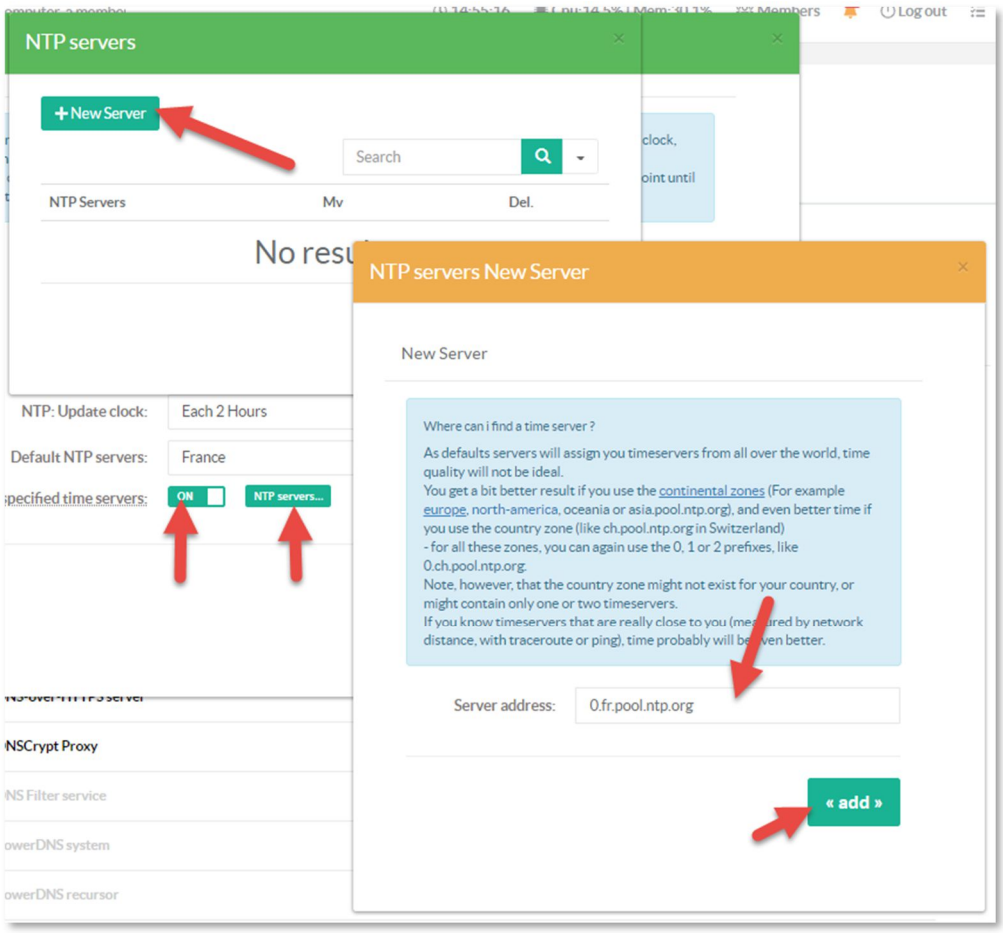


- ✓ After installing the NTP client, return to the top menu, click on the displayed time
- ✓ You can modify the schedule to synchronize the clock (by default each 2 hours)
- ✓ If "**Use Specified time servers**" is **off**, the NTP client will choose a public list of time servers according to the chosen country in the "Default NTP servers" list.
- ✓ You can see the list by clicking on the "NTP servers" mini-button.

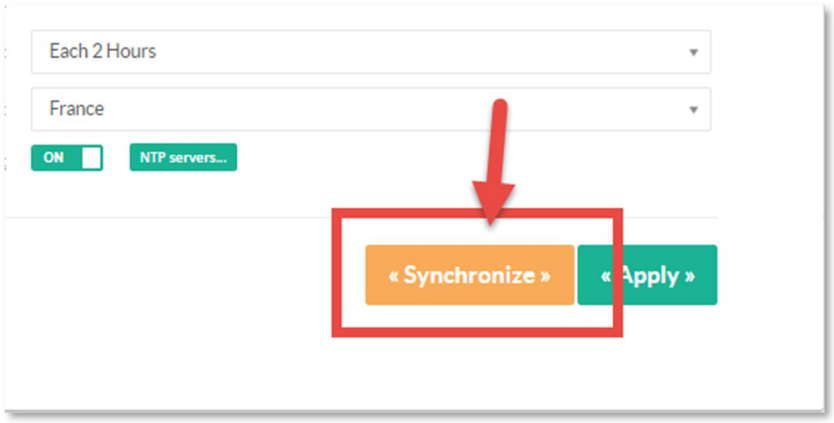


- ✓ If "**Use Specified time servers**" is **ON**, the NTP client will choose a list of time servers you have to define.
- ✓ You can manage the list by clicking on the "NTP servers" mini-button.

The NTP servers section allows you to add an Internal or Public NTP server



After adding your NTP servers, you can click on Synchronize to update your server's clock

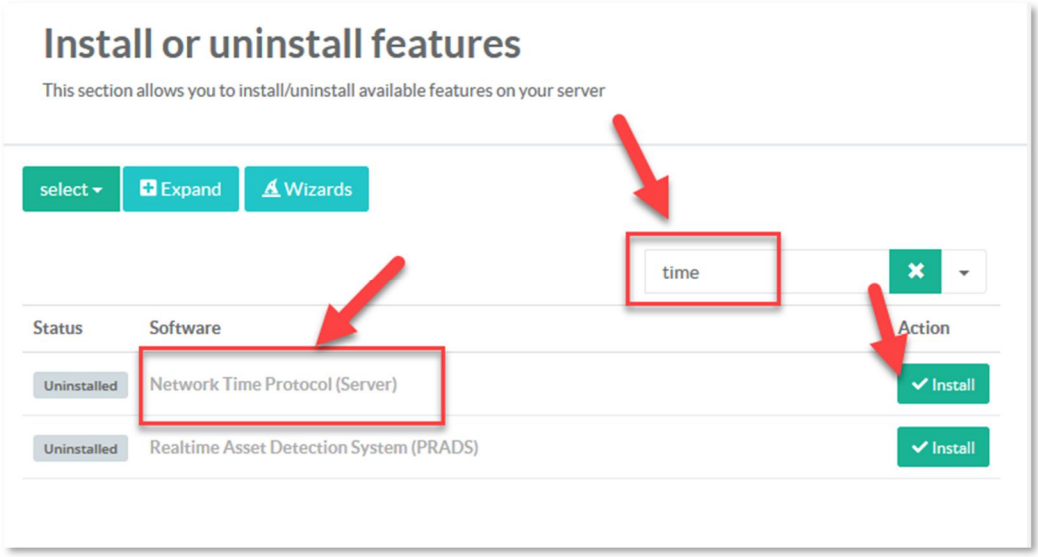


NTP Time server

Install the NTP service

NTP service can be installed using the features section.

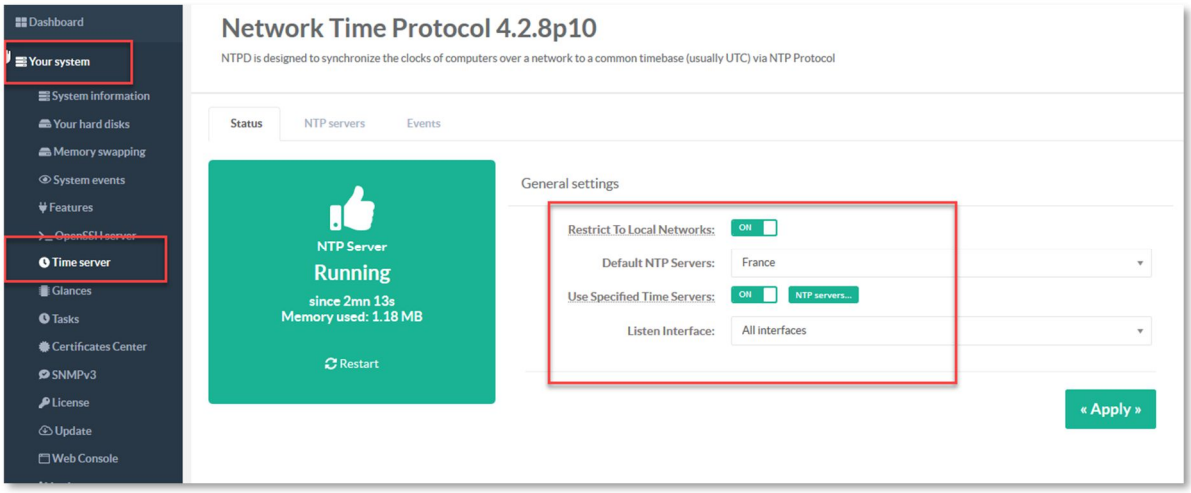
1. On the features section, in the Search field, type "time"
2. Click on Install button on the "Network Time Protocol (server) that will install the NTP server



NTP server options

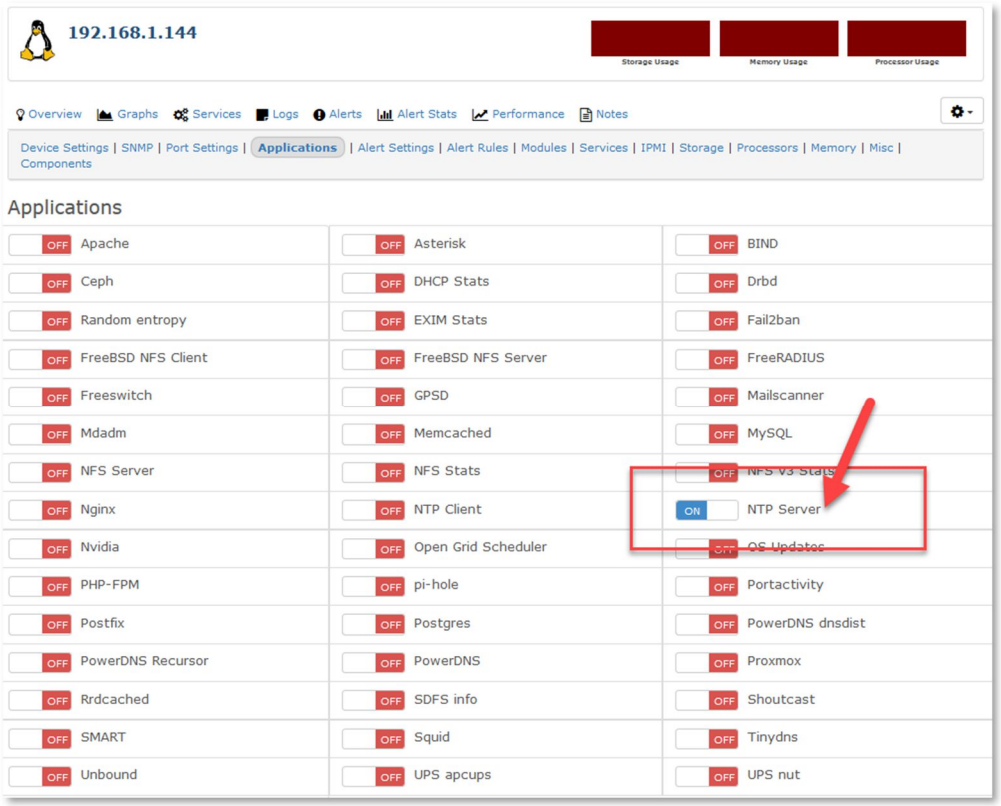
On the left menu, click on "**Your System / Time server**"
Under status button, you can define several options:

- **Restrict to local Networks** : Allow the NTP service to only provide time information for computers inside RFC 1918 private addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 **)**
- **Default NTP Servers:** Allow Artica to automatically set the Internet NTP time server according your country (if Use Specified Time Servers option is disabled)
- **Use Specified Time Servers:** Allow you to add your own list of public/private NTP servers
- **Listen Interface:** Which Network Interface card will bind to**.**



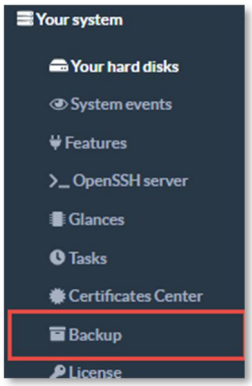
Monitoring the NTP service with LibreNMS

If you using LibreNMS, edit the host configuration and under applications, turn ON the NTP server checkbox option



BACKUP/RESTORE CONFIGURATION.

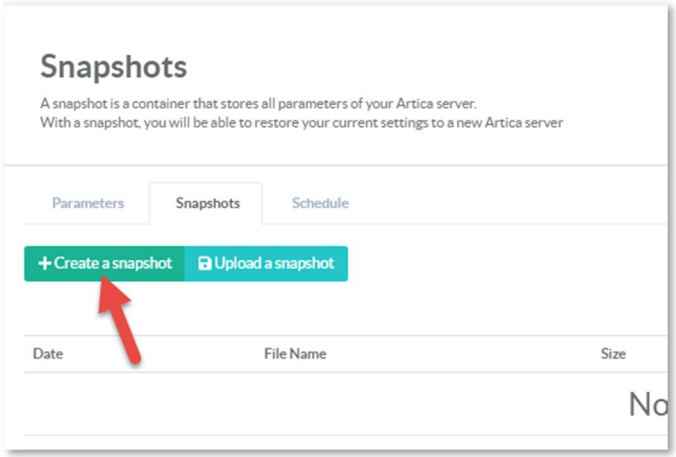
THIS FEATURE IS AVAILABLE IN ENTERPRISE EDITION.



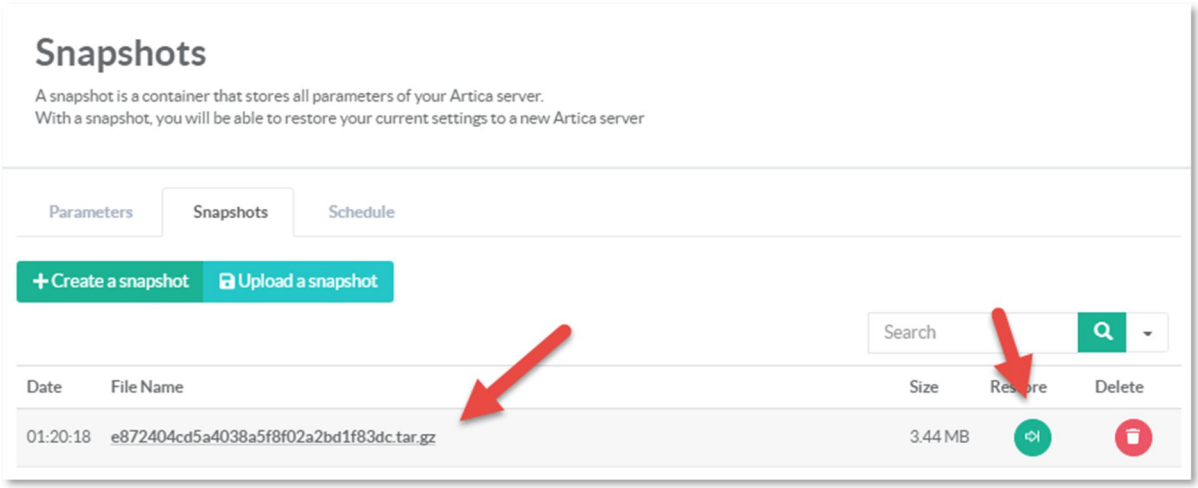
Artica produces containers called "snapshot" . A snapshot is a container that stores all settings that allow you to rebuild the configuration or duplicate the current settings to a new server.
Snapshots can be generated manually or can be scheduled.

Create a snapshot

On the left menu, open "**Your system**" and "**Backup**" link
Select **Snapshots** tab
Click on **Create a snapshot** button



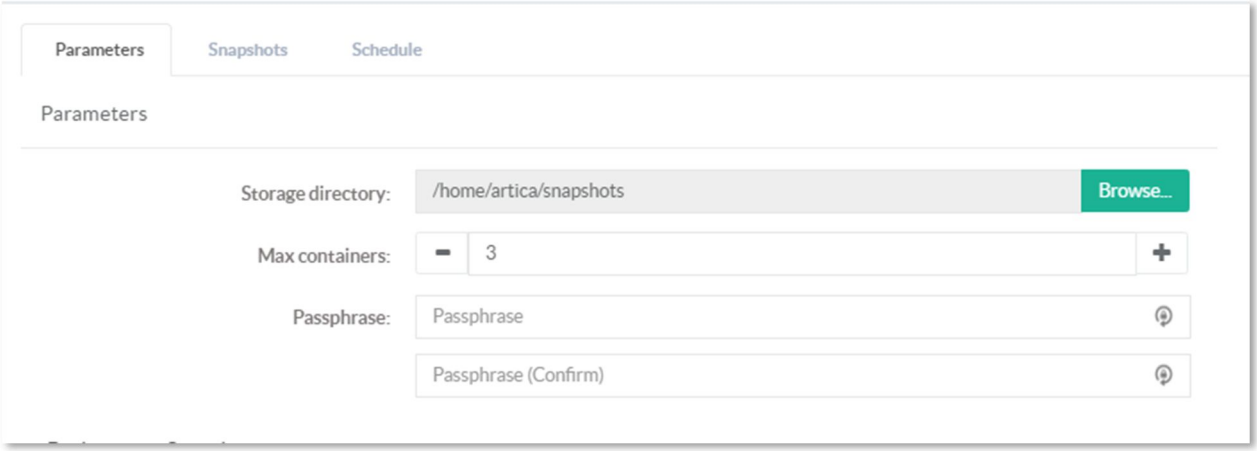
- ✓ After creating, you can see the snapshot container in the table
- ✓ The snapshot can be locally restored by a click on the restore column or downloaded by clicking on the link.



Snapshot parameters

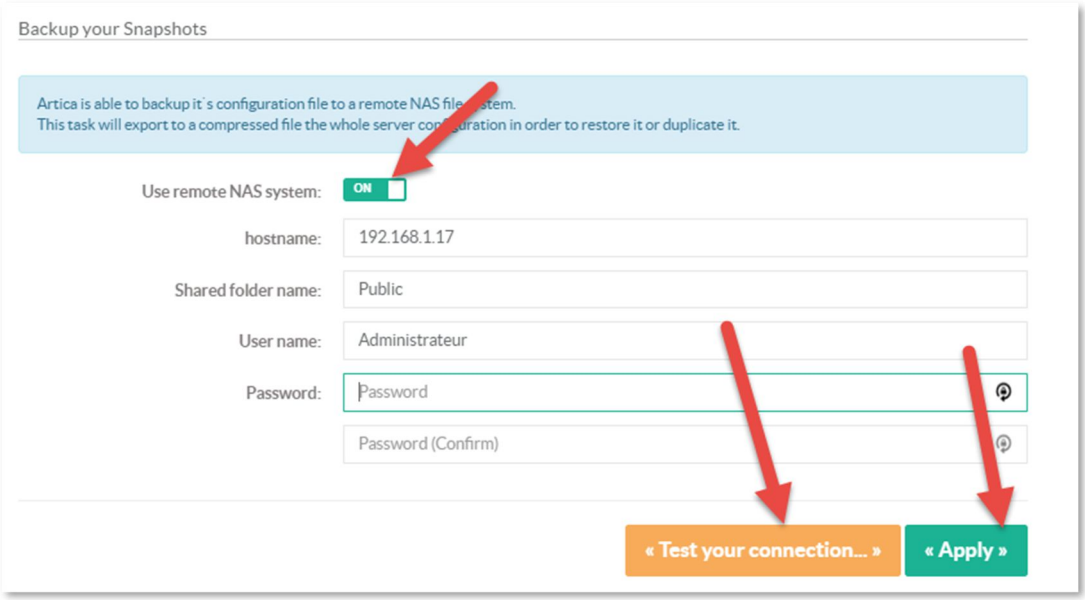
The parameters section allows you to

- ✓ Modify the **storage directory** where your snapshots are stored on the local disk.
- ✓ The **Max containers** allows you to specify how many containers you want to keep in the storage directory
- ✓ If you define a **passphrase**, snapshot container will be encrypted using aes256



Backup your snapshots on a remote NAS

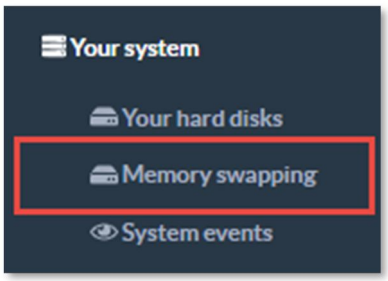
- ✓ You can store your snapshots outside the Artica appliance using an SMB connection to a NAS file system.
- ✓ Fill the form with the credentials that allows Artica to create directories in the shared folder.



- ✓ Artica will create a folder with its hostname and "snapshots" directory.
- ✓ In our example, the target directory will be \\192.168.1.17\Public\artica.domain.tld\snapshots

THE SYSTEM SWAP

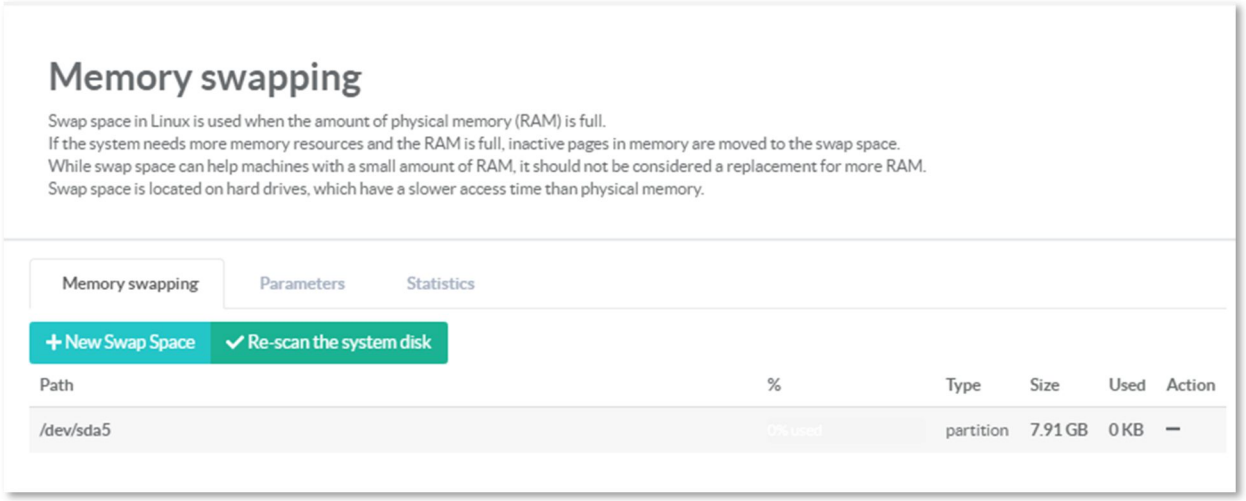
Swap space in Linux is used when the amount of physical memory (RAM) is full.
If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space.
While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM.
Swap space is located on hard drives, which have a slower access time than physical memory.



When installing Artica with the ISO file, the system did not create any SWAP space

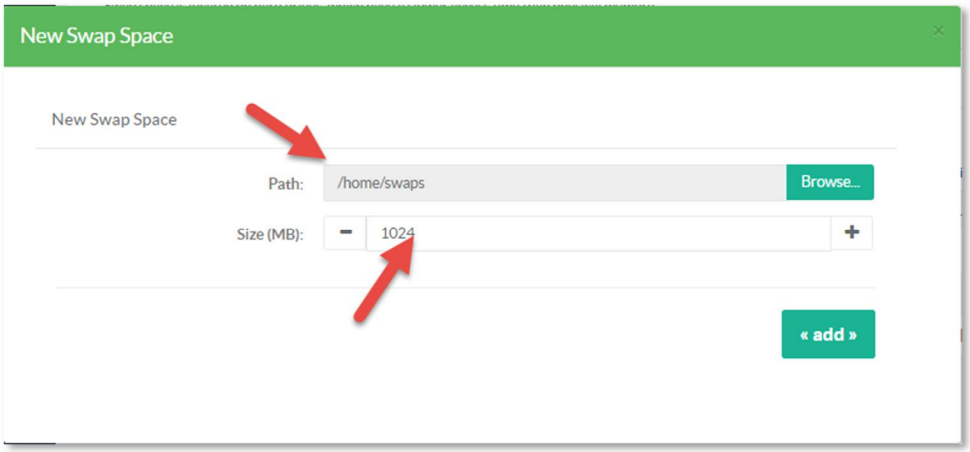
The SWAP can be managed using the left menu under "**Your System/Memory swapping**"

The section will show you the current swap space configured on your system.
if "Munin" feature is installed, you can show statistics of your system SWAP



Adding Swap Space

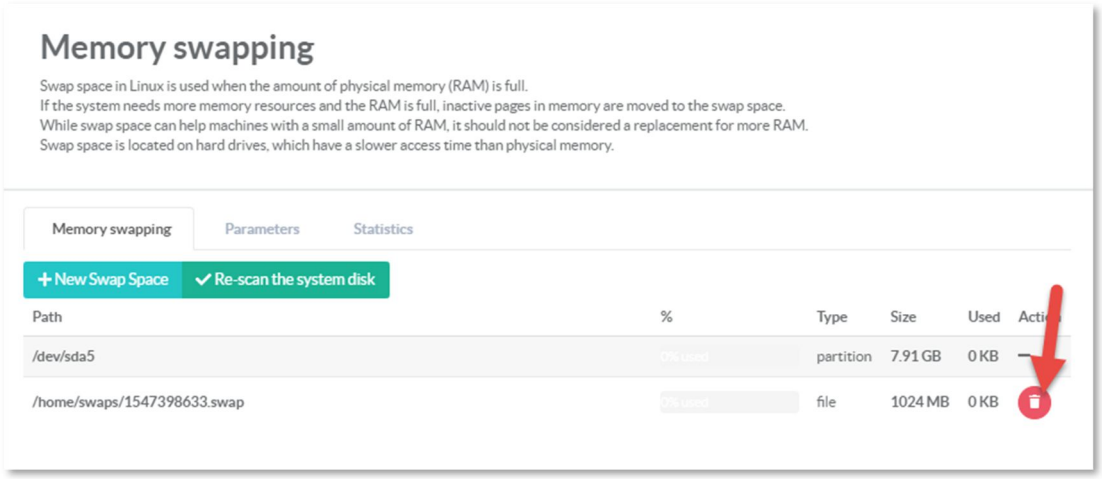
Click on the button "**New Swap Space**"
Define the directory that will store the swap file and set in MB the available space.
Click on **Add** button



Removing a SWAP space

SWAP space using a disk partition cannot be removed

Click on the trash icon on the swap row you want to remove.



MEMORY TUNING

Using SWAP: Modern DRAM has access times of less than 100 Nanoseconds, where a typical spinning disk drive needs a few Milliseconds to access a block on disk.

Writing out a page is even slower, and if the system is already under heavy load, other processes might require access to the precious I/O channels as well.

Using Swap gives the advantage of having more memory available, just in case an application needs momentarily more RAM than physically available. However for a gateway system it severely degrades the performance, if the data needs to be read from disk, then swapped out, and swapped in again. It is best practice not to use swap at all on a proxy server.

THAT'S WHY BY DEFAULT, YOUR ARTICA SERVER DOES NOT HAVE SWAP MEMORY

Overcommitting Memory

In an ideal world, every application would only request as much memory as it currently needs.
And frees memory instantly when it is no longer used.

Unfortunately that is not the case in the real world.
Many applications request more memory - just in case.
Fortunately the Operating System knows about the bad habits of applications, and overcommits memory.

That is, it provisions more memory (both RAM and Swap) than it has available, betting on applications to reserve more memory pages than they actually need.
Obviously this will end in an Out-of-Memory disaster if the application really needs the memory, and the kernel will go around and kill applications.

The error message you see is similar to

```
ERROR: can't execute command of …/..: Cannot allocate memory
```

And sometimes, the Proxy service turn to emergency service.

Overcommitting behavior

To avoid such situations, the overcommit behavior is configurable.

- **Free to overcommit memory:**
  This is the default value in most systems, a heuristic algorithm is applied to figure out if enough memory is available.
  (THIS IS THE DEFAULT VALUE DEFINED BY ARTICA FOR VERSIONS **AFTER** 4.27.022100)
-
- **Always overcommit memory**:
  The system and never check if enough memory is available.
  This increases the risk of out-of-memory situations, but also improves memory-intensive workloads.
- **Not overcommit memory**:
  The system only allocate as much memory as defined in Overcommit Ratio.
  (THIS IS THE DEFAULT VALUE DEFINED BY ARTICA FOR VERSIONS **PRIOR** TO 4.27.022100)

The ratio

If you have defined the Overcommitting behavior to "**Not overcommit memory**", you can define the ratio.
The ratio defines how many percent of the physical RAM are used.
Swap space goes on top of that.
The default Artica value is **95%**

Example 4 GB RAM, no Swap, Not overcommit memory:

Ratio	Memory Free (kB)	Commit Limit (kB)	Breaks at (MB)	Diff Commit Limit and actual break (MB)
10%	3803964	402892	243	69
25%	3802532	1007236	803	40
50%	3799844	2014472	1756	12
75%	3803580	3021708	2708	23
90%	3805424	3626048	3276	48
100%	3804236	4028944	3653	63

- **Memory Free:** Shows the free memory right before the test was started
- **Commit Limit:** Shows the entry returned by the kernel.
- **Breaks at:** Shows how much memory the program was able to allocate.
- **Difference expected and actual break:** Shows the difference between the **Commit Limit** and the actual break, but takes Memory Free into account. that is, it calculates how much memory the test application could possibly allocate based on the free memory before running the test

If you set the ratio to 50%, the test application can only allocate half the memory (50%).
Technically, all applications and daemons on the system can only use 2 GB RAM altogether.
Only if ratio is changed to 100% in this scenario, the entire memory is used.

The Deal

Linux applications allocate more than they really need.
They allocate 8kb to store a couple character string of text.

Applications do this a lot, and this is what overcommitting is designed for.
Basically with **ratio at 100%**, the kernel will not allow applications to allocate any more memory than you have.
Setting it at less than 100 means that you will never use all your memory.
If you are going to set this setting, you should set it higher than 100 because of the fore-mentioned scenario, which is quite common.

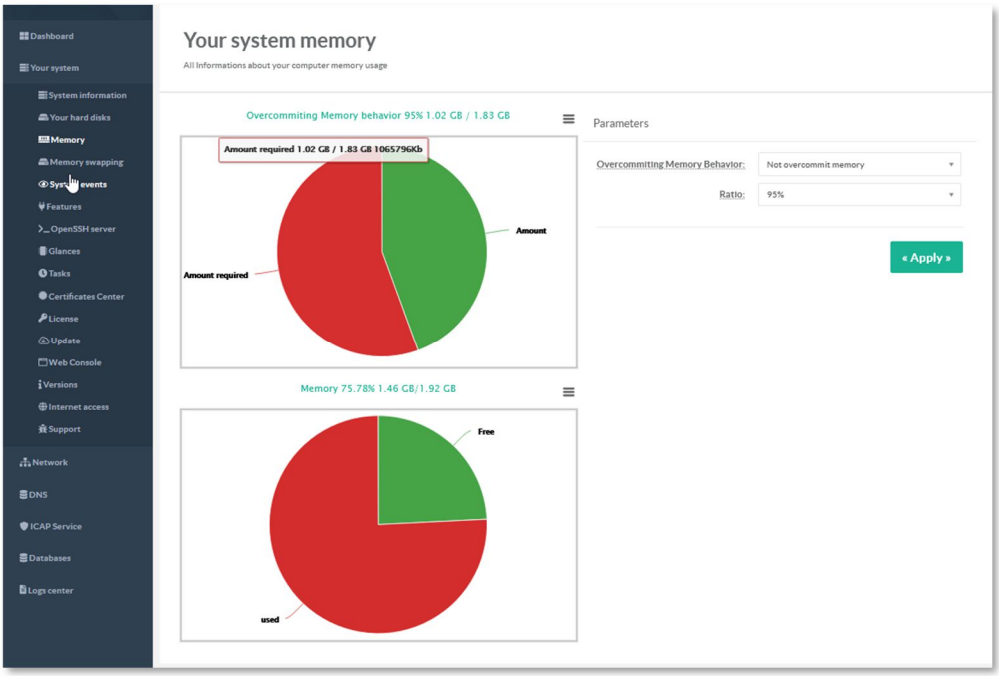
Avoid Cannot allocate memory

On the left, menu click on "**Your System / Memory**"

The first chart give information of

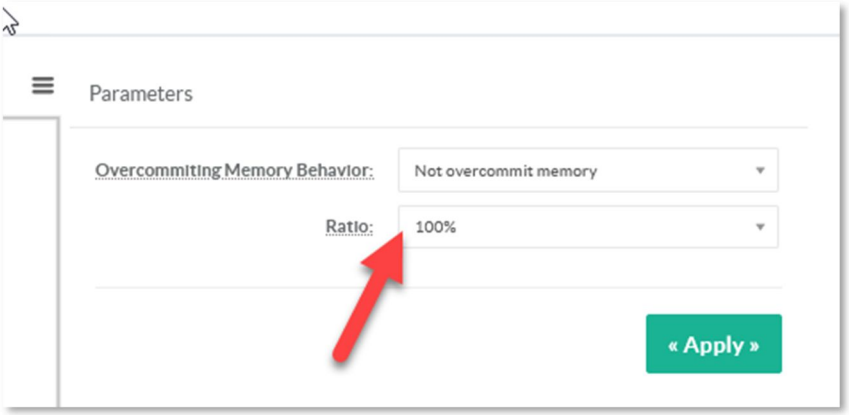
Amount: The total amount of memory, both RAM and SWAP, available to commit to the running and requested applications (not necessarily directly related to the actual physical RAM amount).

Required: The total amount of memory required in the worst case scenario right now if all the applications actually used what they asked for startup!



The second graph displays the memory usage (physical memory and SWAP if set)

On the right side, set the ratio to 100% and click on **apply** button.



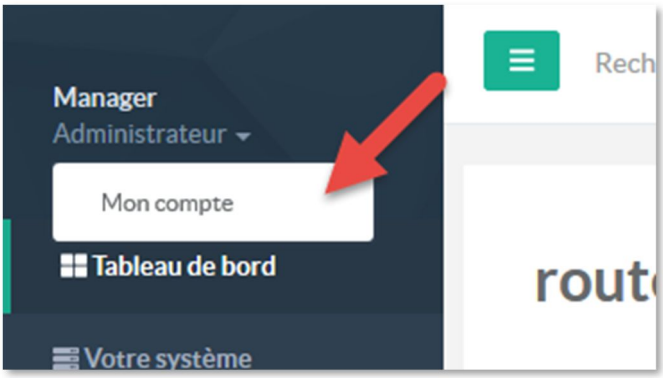
If the "Cannot allocate memory" still exists and your proxy turn to emergency, **add a SWAP partition** in order to let the memory more elastic.

If the "Cannot allocate memory" still exists, turn the option to **Free to overcommit memory**

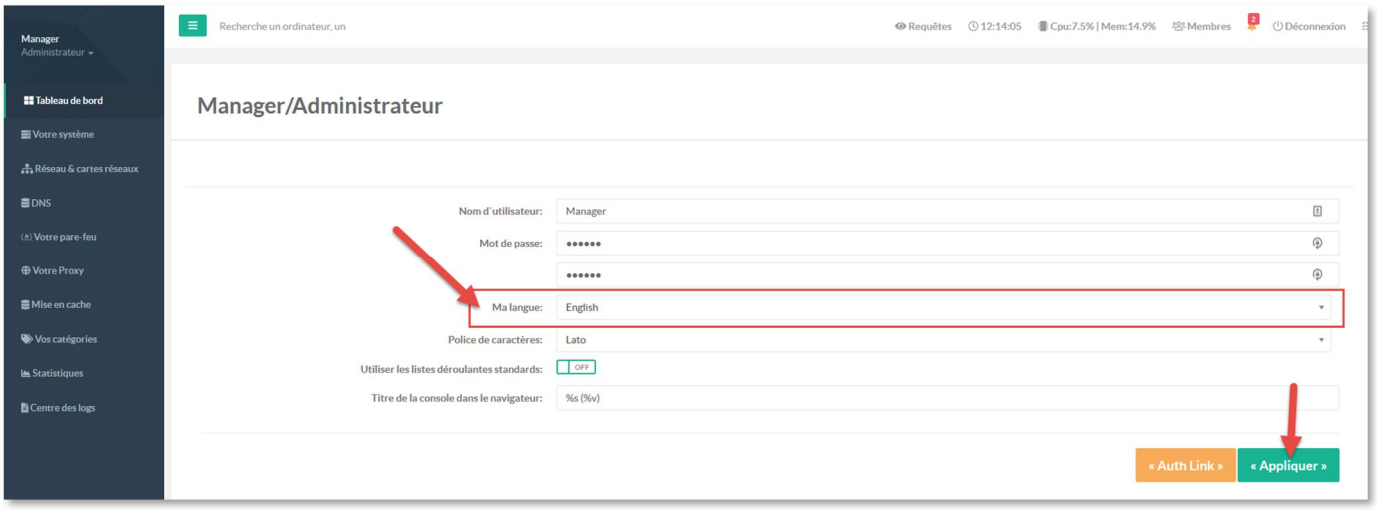
ARTICA WEB CONSOLE

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

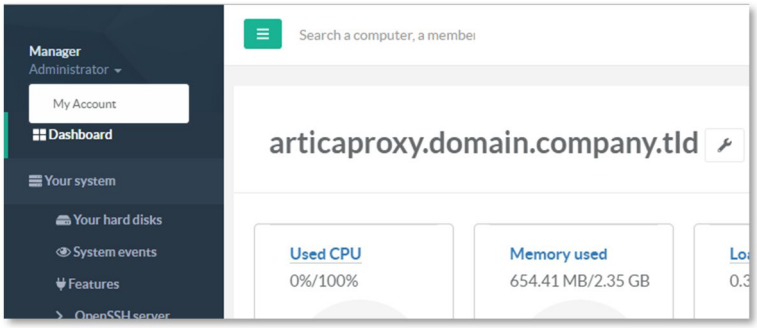


(Not all parts of the web page will be modified, if you want to change all the web page part, click on the F5 key in order to refresh totally the web console.)

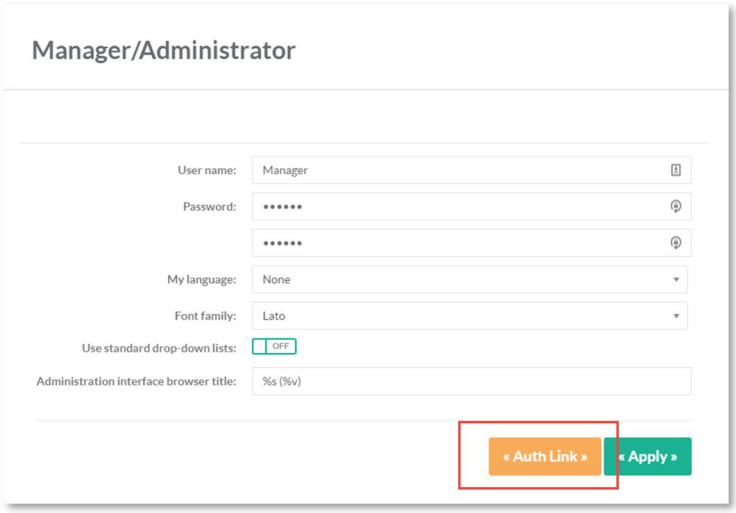
AUTH LINK

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.

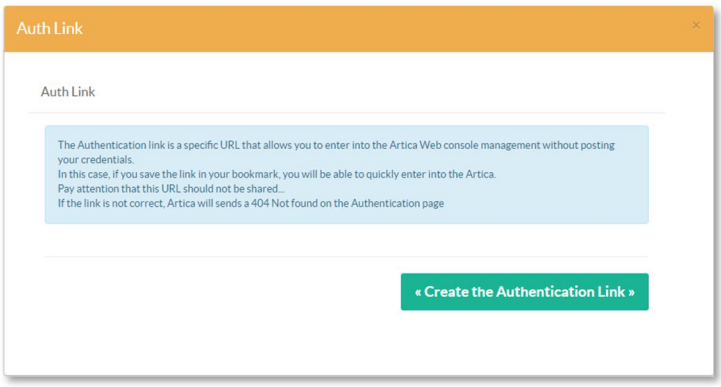
On the left menu, open **Your Account**



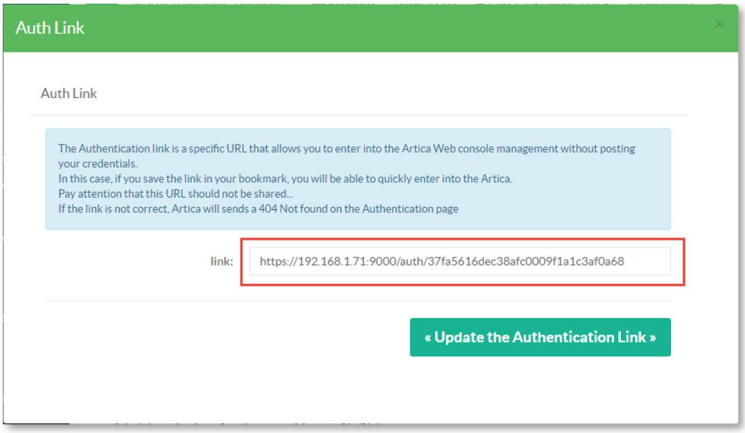
Select the button "**Auth Link**"



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

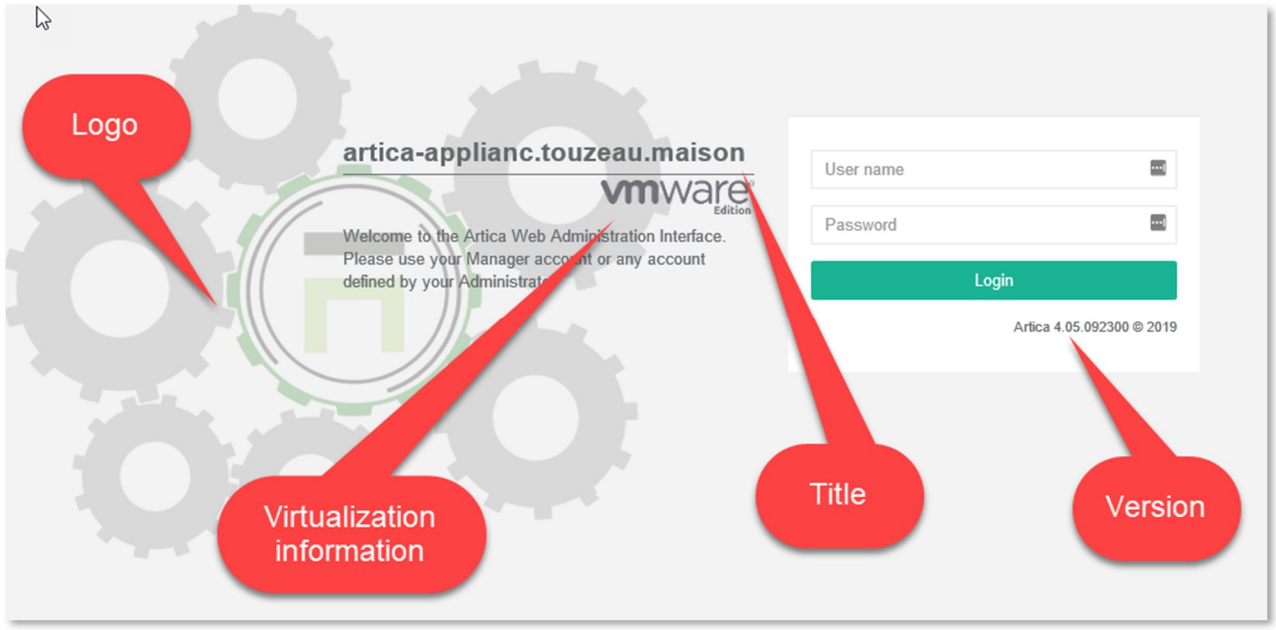


Copy the link, disconnect from the console and type this new link on your browser, you will be logged automatically.

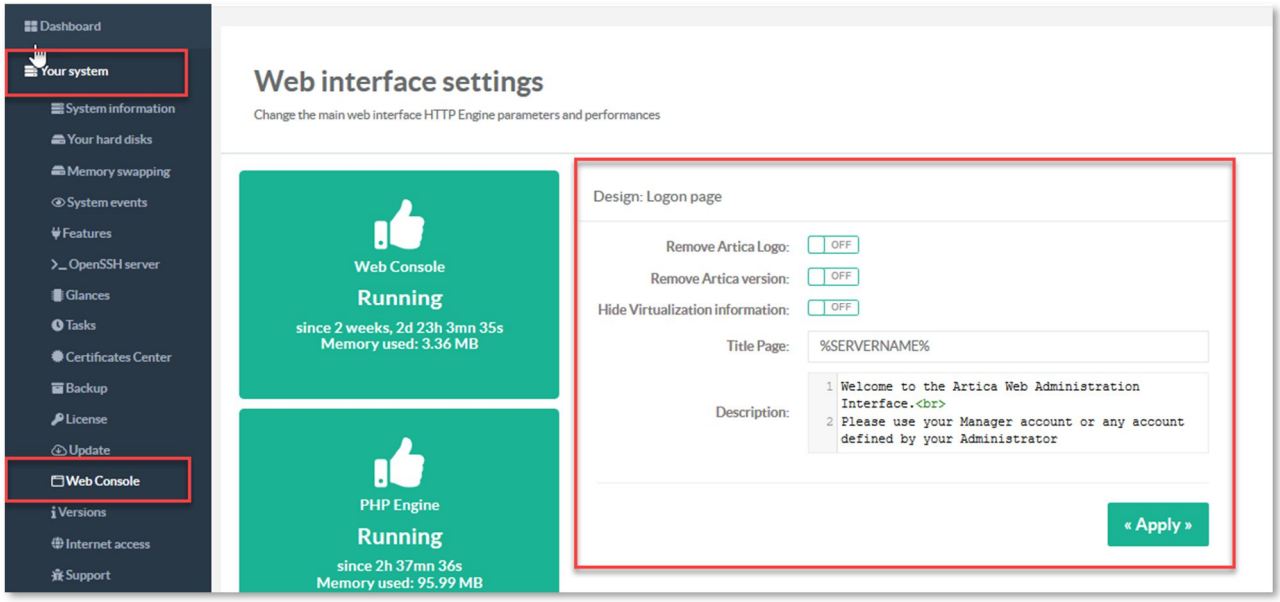


PERSONALIZE/SKIN THE LOGIN PAGE

By default the login page display some elements you can skin if you use a valid Corporate license.



On the left menu, go to **Your System** and **Web Console**



The Design: Logon page section allow you to

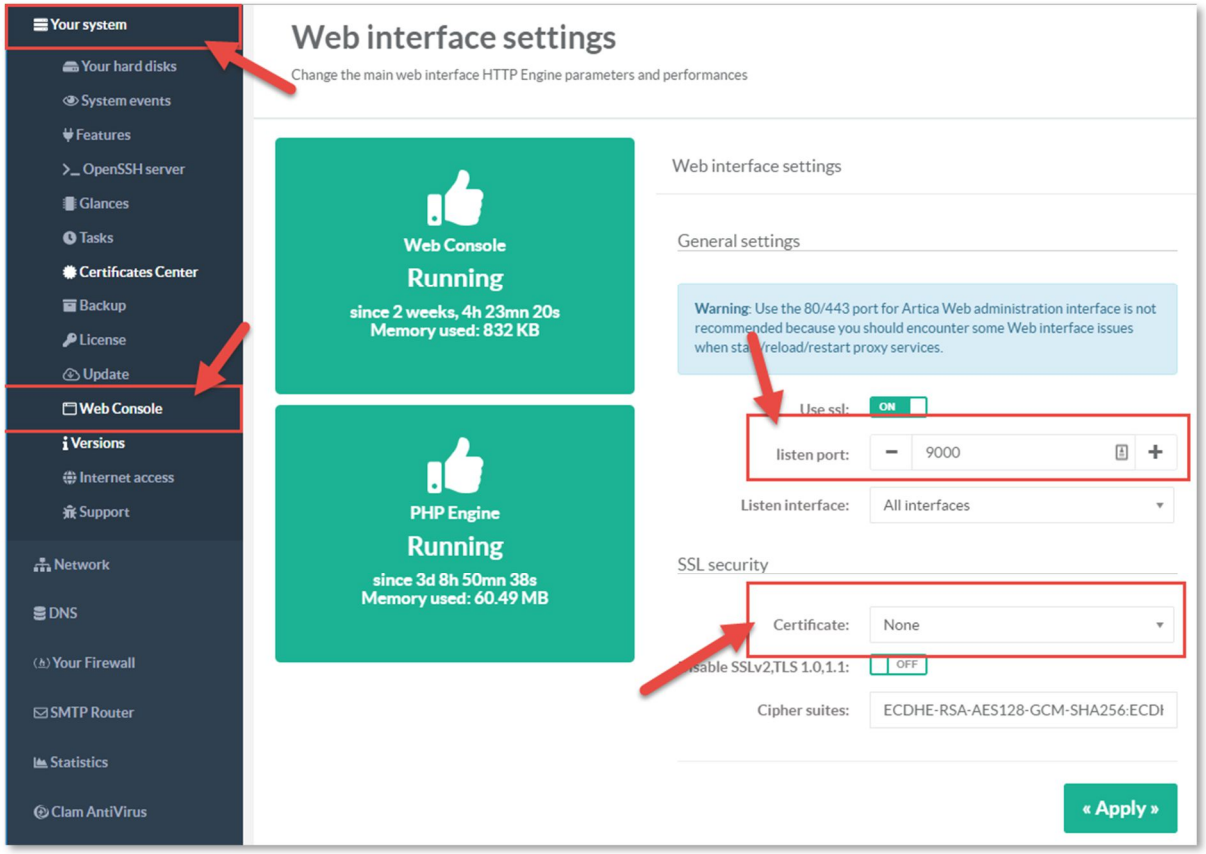
- Remove the background logo
- Remove any information about the version of Artica.
- Remove any information about the logo if you using virtualization.
- Modify the text under the title.
- Change the title page (by default %SERVERNAME% means the hostname of the server)

ARTICA WEB CONSOLE LISTEN PORT AND CERTIFICATE

If you want to run the Artica Web console on the 443 port and use an official certificate (Let's encrypt for example):

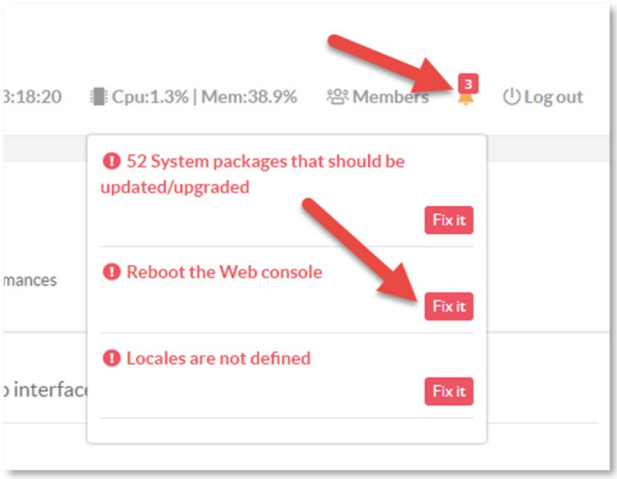
On the left menu, select "**Your system**" and "**Web console**"

Modify the listen port to 443 and select the desired certificate.



If your Web console listens the 443 port, be careful if you using the Web service "Nglnx", you should encounter a port conflict issue.

or use the 2 services on the same port, use 2 networks interfaces in order to bind each service to the specific interface.
Another way is to let the 9000 port open on the Web console and use the reverse-proxy feature in order to redirect the Web console requests to the loop back interface on the 9000 port.



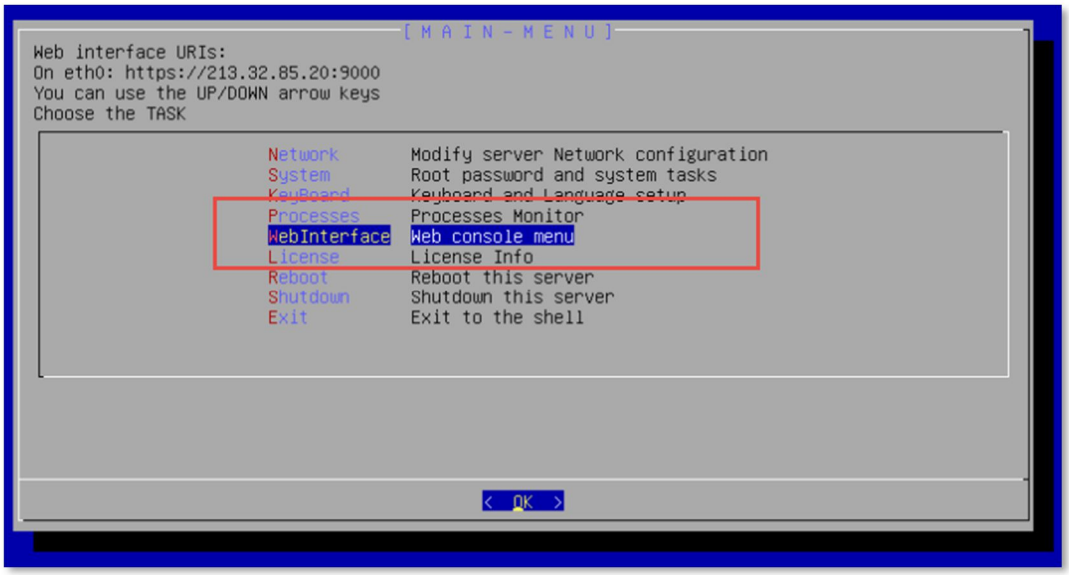
After applying settings the top icon will display a notification to reboot the Web console.

After reboot the console, change to the defined port on your browser to access again to the Artica Web console.

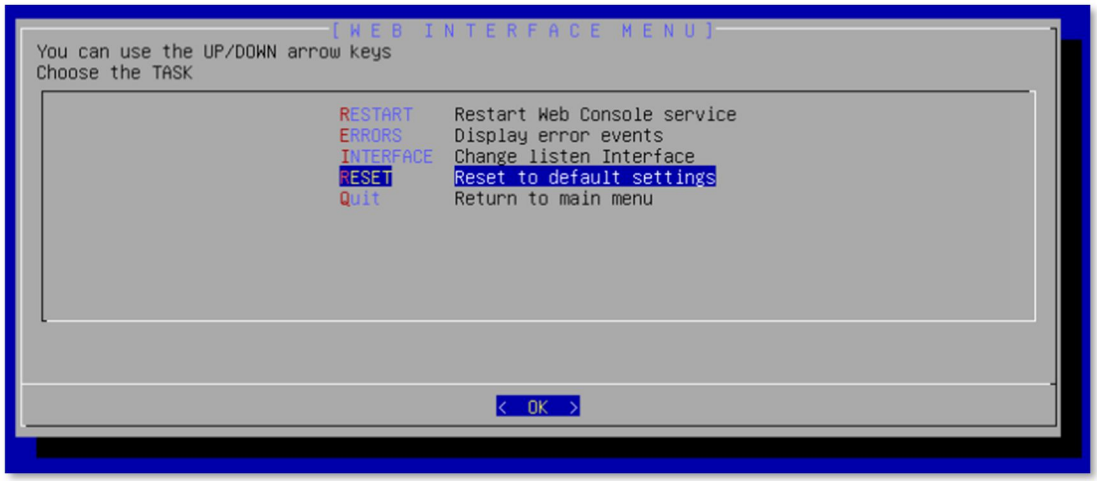
RESET TO DEFAULT SETTINGS

If your Artica Web console is unavailable and you want to reset all settings to the default open the system console.

- ✓ Select the **WebInterface** menu.



- ✓ Choose "RESET" menu in order to return back to the 9000 port and self-signed certificate.



ARTICA PRIVILEGES

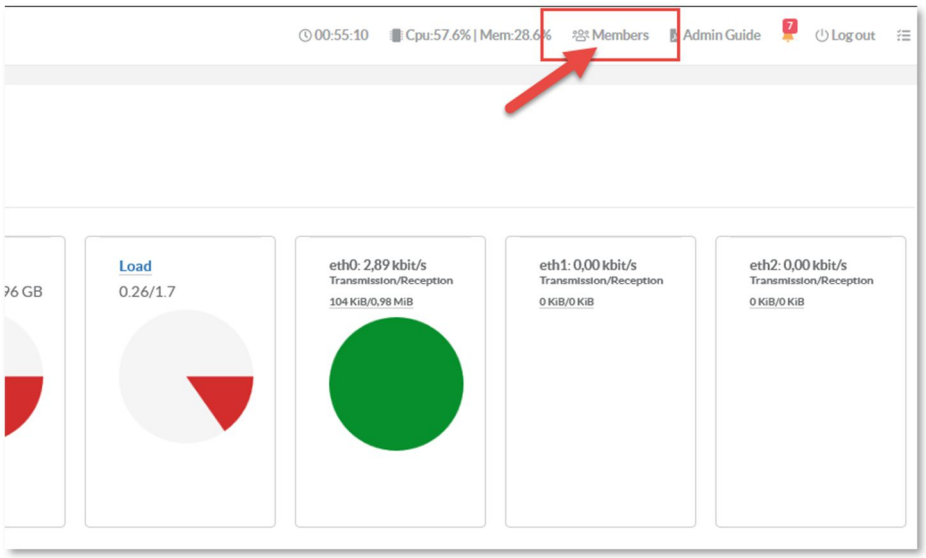
Artica allows you to define privileges based on:

- **Active Directory groups** if the server is connected to an Active Directory server.
- **LDAP** groups if you using the local LDAP service.
- **SQlite** database if you using the "administrators" section.

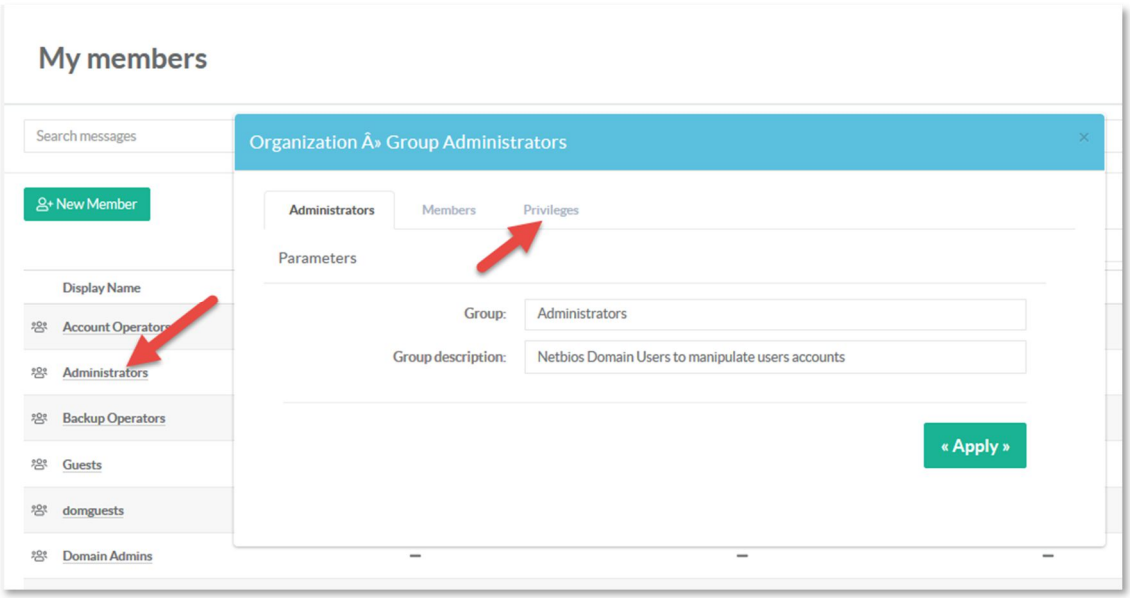
Artica privileges means what privileges are assigned to member after logging to the Artica Web console

LDAP or Active Directory

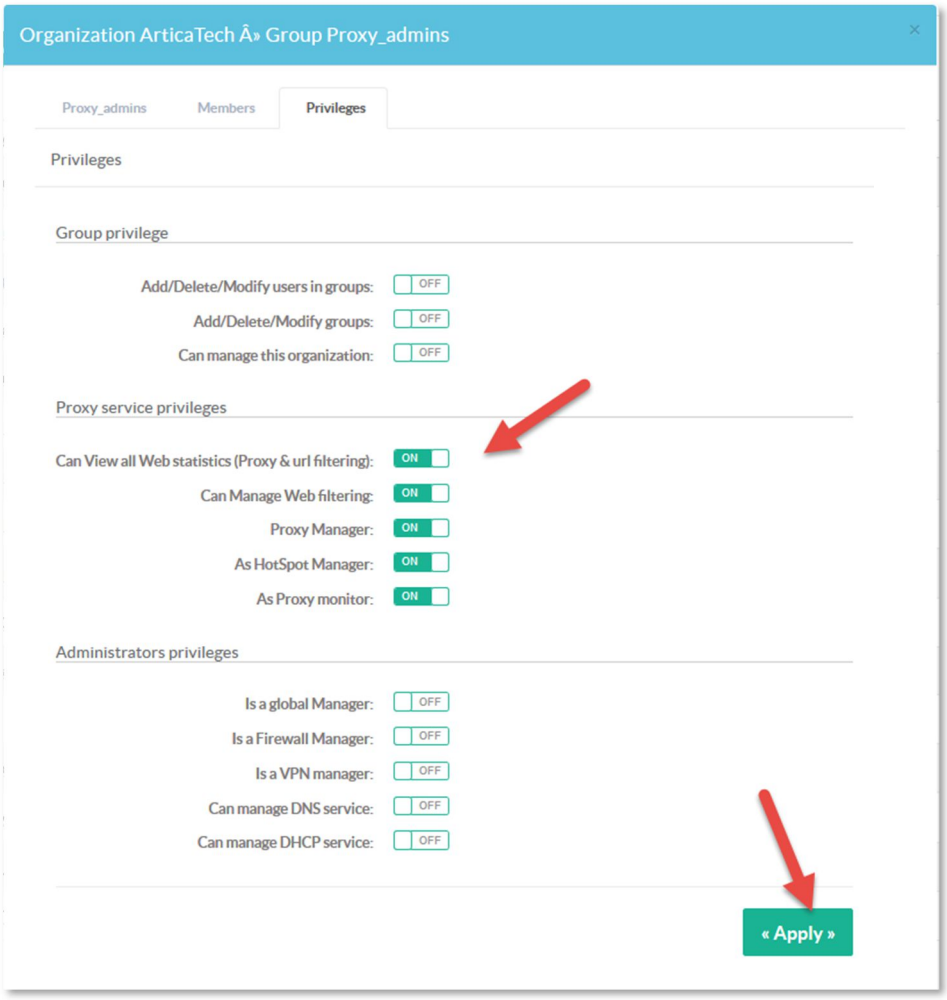
Basically, using LDAP database or Active Directory, the procedure is the same:
Open the Members section on the top menu



On the "**My Members**" section, choose the group you want to assign privileges.
Choose the tab "Privileges"



- Assign the desired privileges



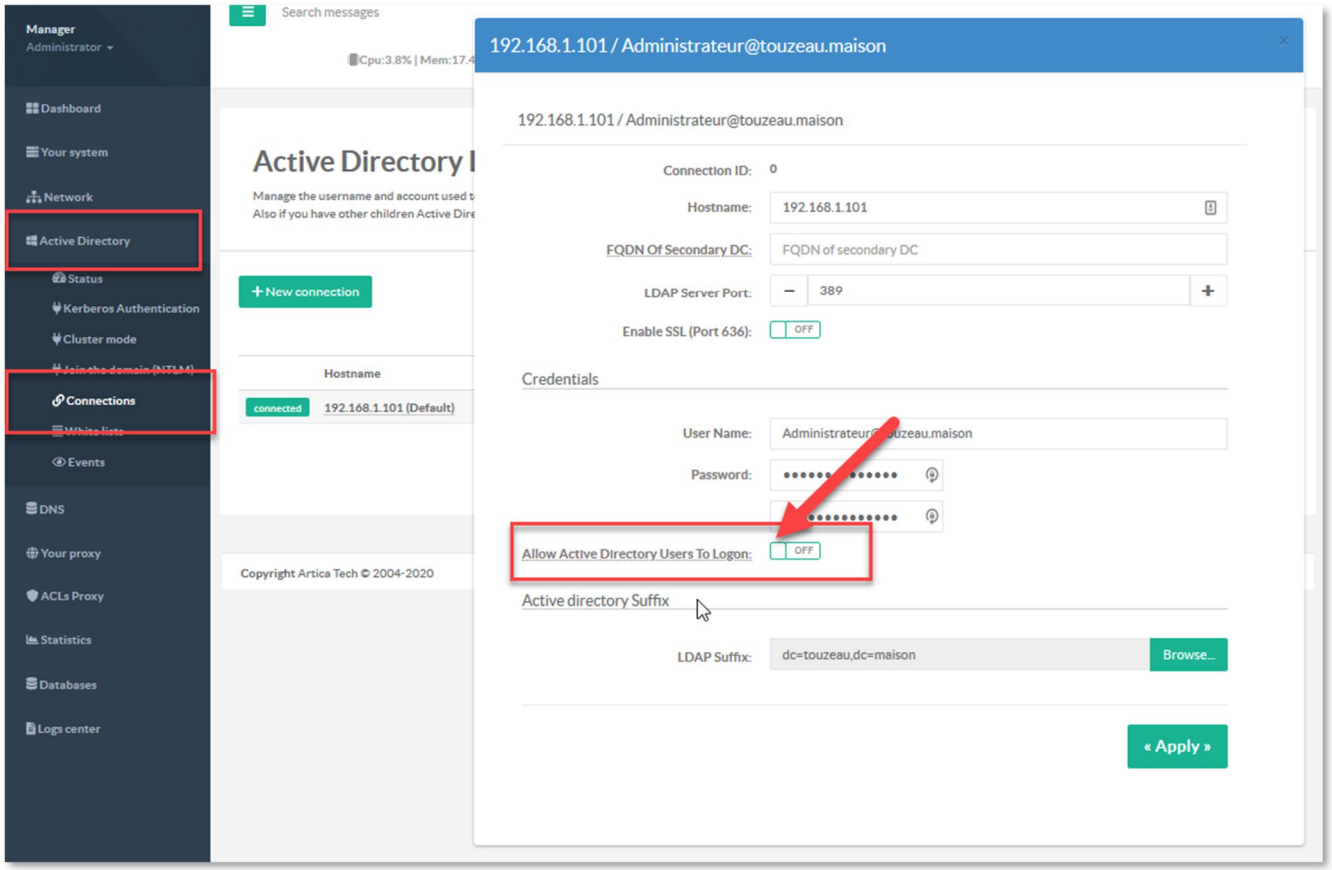
NOTE: IF YOU WANT USERS OF THE GROUP HAVE THE SAME PRIVILEGES AS THE "MANAGER", JUST ENABLE THE "IS A GLOBAL MANAGER" PRIVILEGE

- A proxy administrator will have "Proxy Manager" privilege.
- A DNS administrator will have "Can Manage DNS service" privilege
- A FireWall administrator will have "is a Firewall Manager" privilege

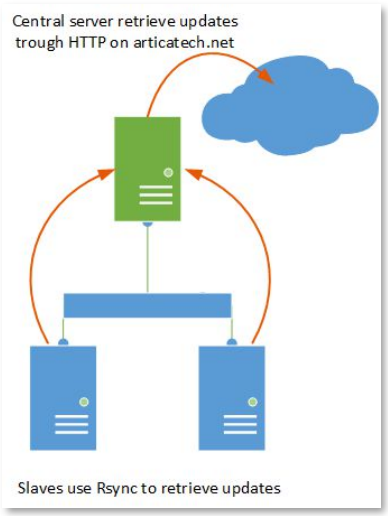
Allow users to connect to the Web console in Active Directory mode.

By default, Active Directory members are not allowed to be connected to the Web console.
You need first to allow it inside the Active Directory connection.

- On The Active Directory left menu, select “Connections”
- Turn on the “**Allow Activbe Directory Users to logon**”checkbox.



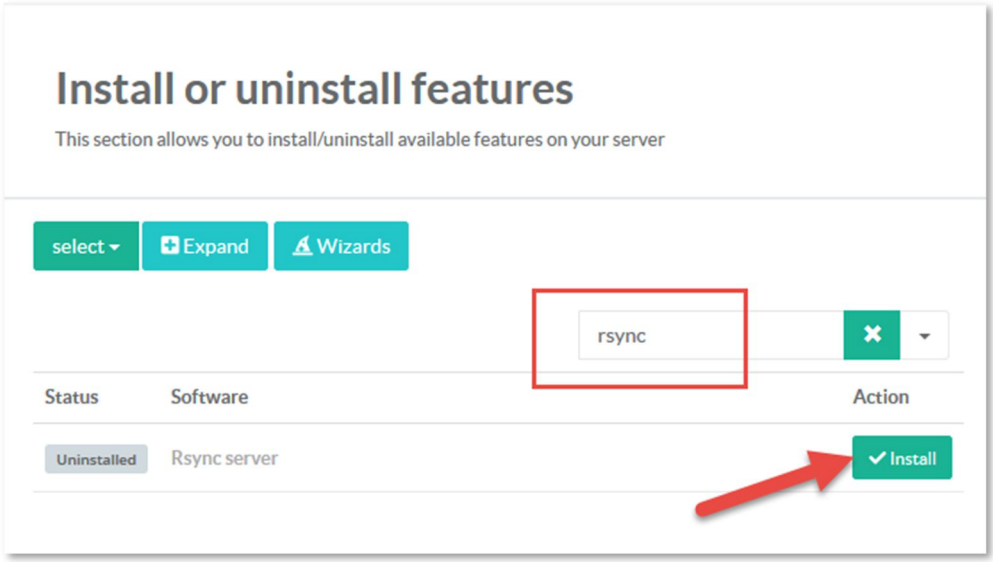
CENTRALIZED UPDATES



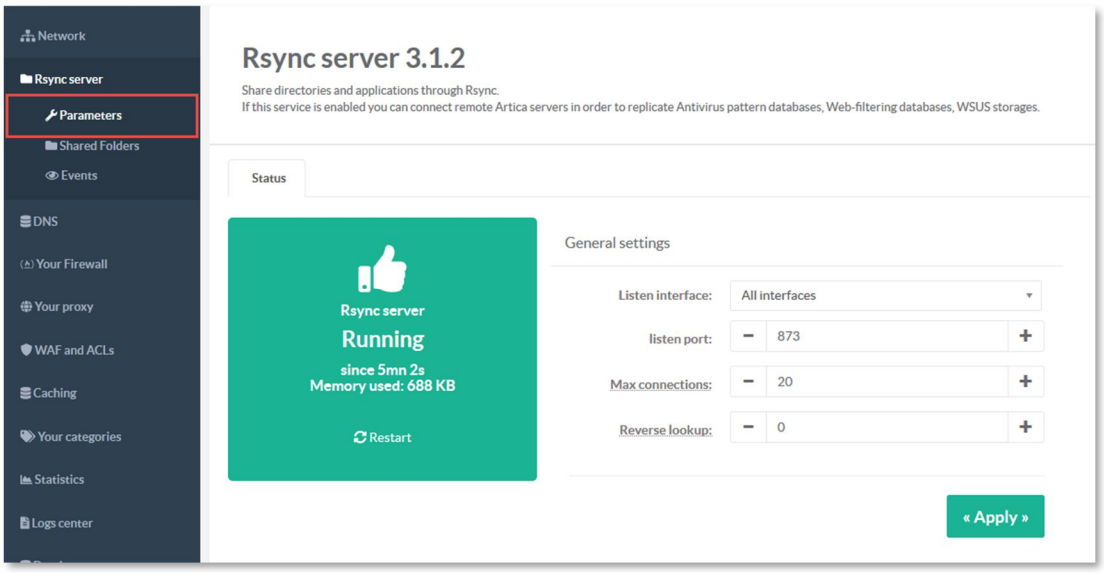
The Artica package is about 100MB, if you have several Artica servers you can limit the bandwidth usage by using a central Artica server that will be able to share its Artica code.
Artica are able to retrieve update use Rsync protocol.

Install Rsync service on the master

- Open the Artica Web console on the server that will act as master
- On the left menu, go into Your **System / Features**
- On the search field, type **Rsync**.
- Click on **install** button on the Rsync server row

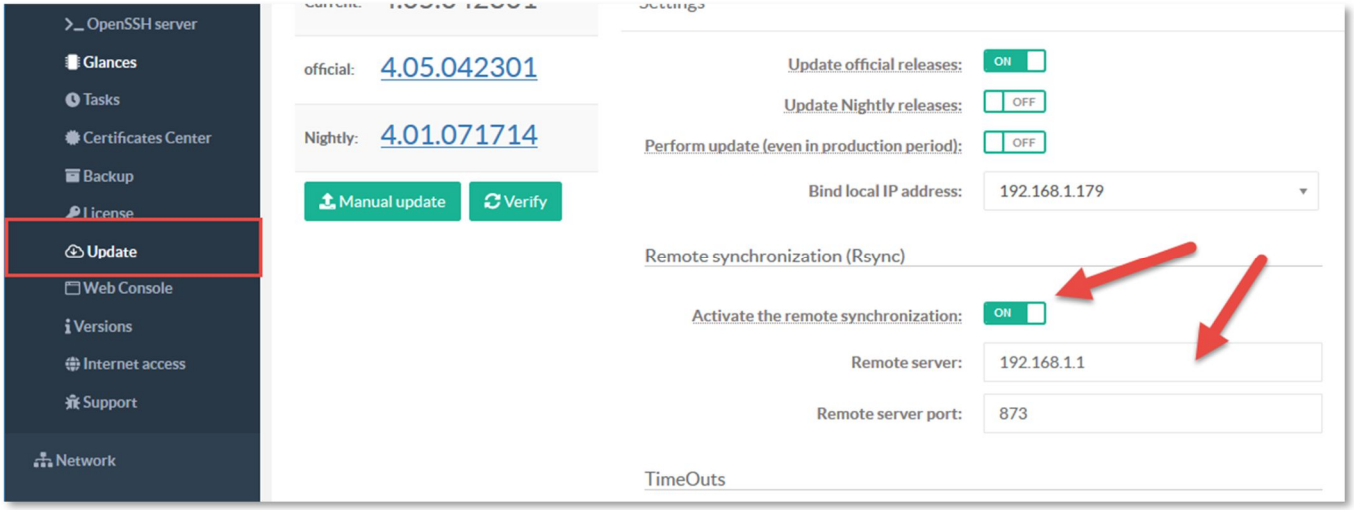


- On the left menu go to **Rsync server/Parameters**
- Verify that the service is running



Enable the Rsync updates on clients.

- Open the Artica Web console on Artica clients.
- Go to **Your system / Update**
- Turn on the **Activate the remote synchronization**
- Give the IP address of the Artica server that act as master
- Click on **Apply**.



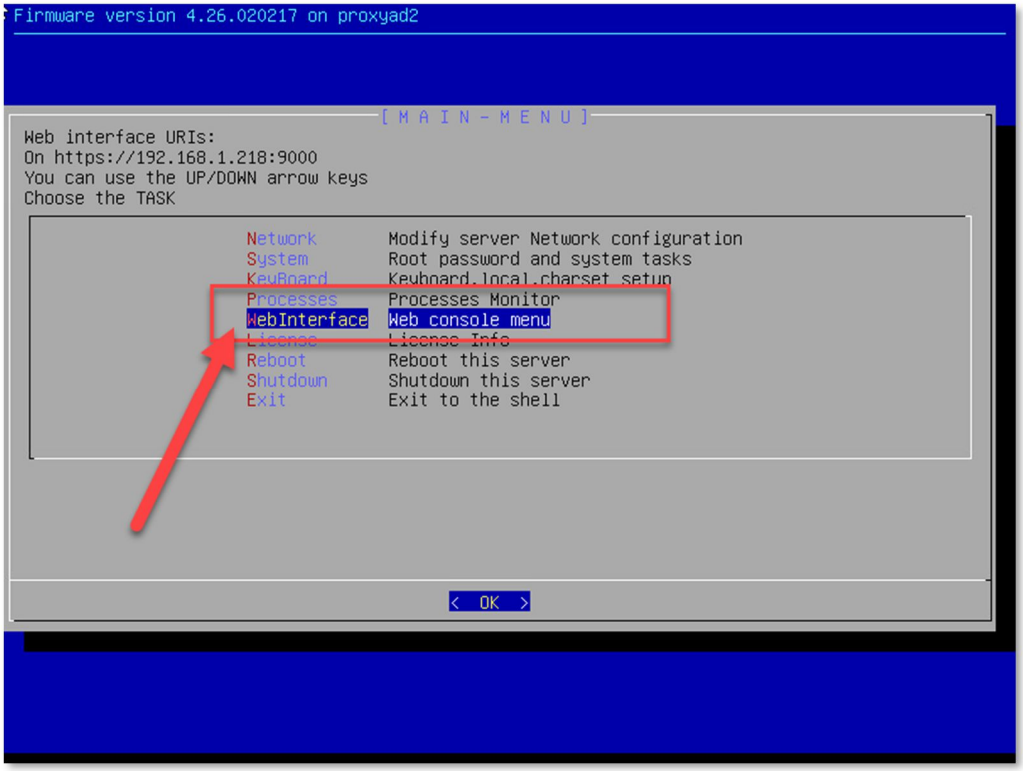
TROUBLESHOOTING

I'm stuck with the web console

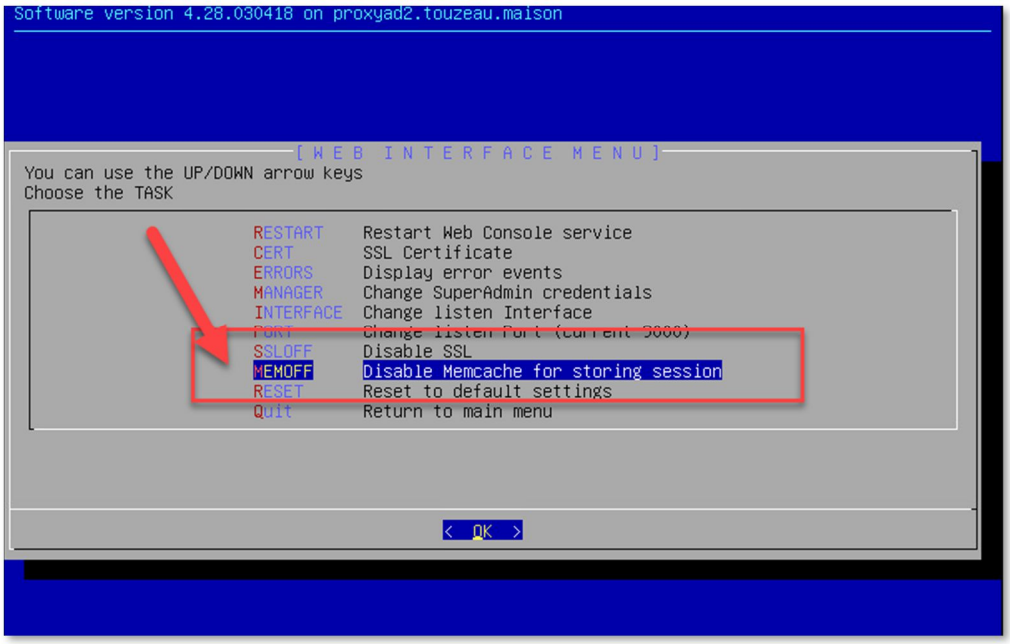
It always asks me to identify ?

This is a memory issue. The web console use "memached" to store sessions. It means the Memcached is unable to store for a long period your session data.
You can disable the use of memcache and force the web console to store sessions data on disk.

- On the server console, choose the menu "Web console menu"



- Choose "**Disable Memcache**" for storing sessions

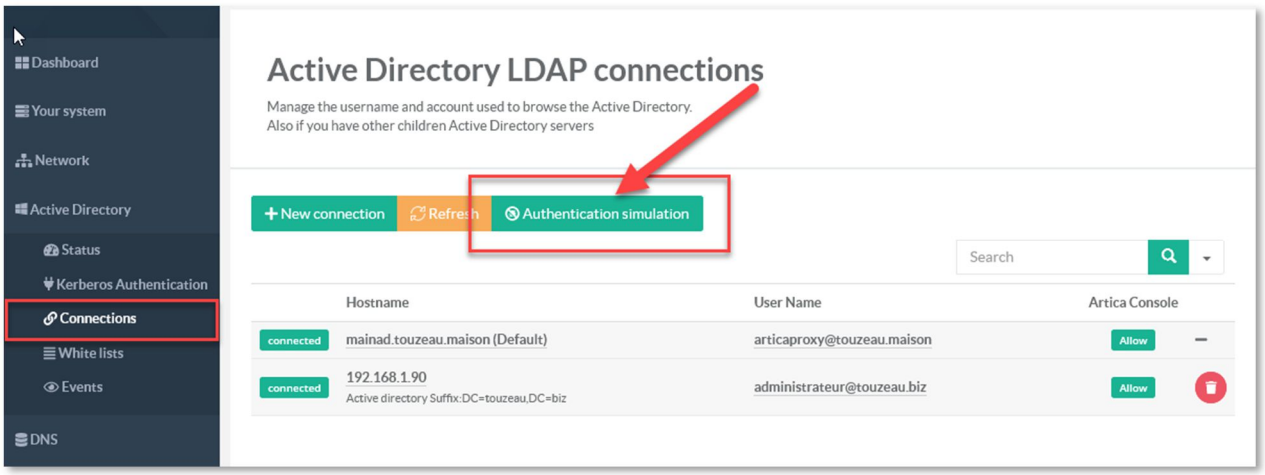


I'm connected to Active Directory but

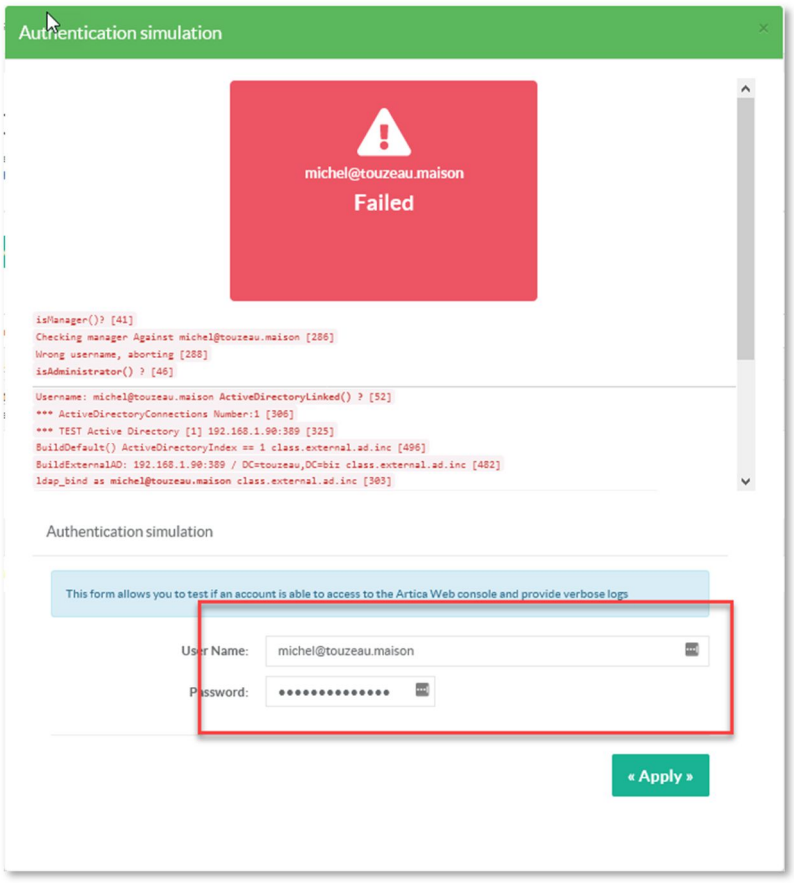
cannot login on the web console ?

If you have correctly set privileges and the Artica logon page did not reflect what you want.

Open the connections in Active Directory section



- Click on the "Button" "**Authentication simulation**"
- Set the username and password in the form and click on "**Apply**"
- You will see result of credentials and generated logs in verbose mode.



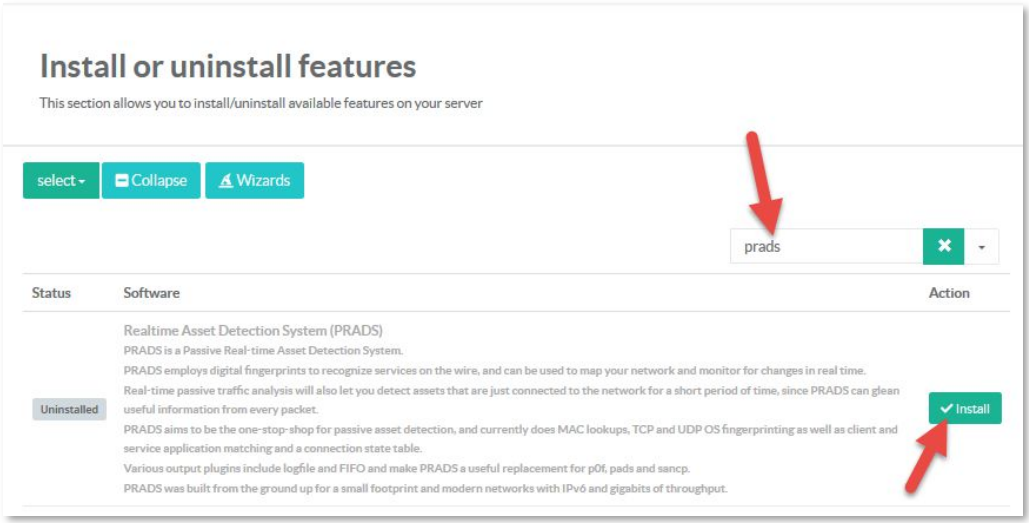
MONITORING THE NETWORK

REALTIME ASSET DETECTION SYSTEM

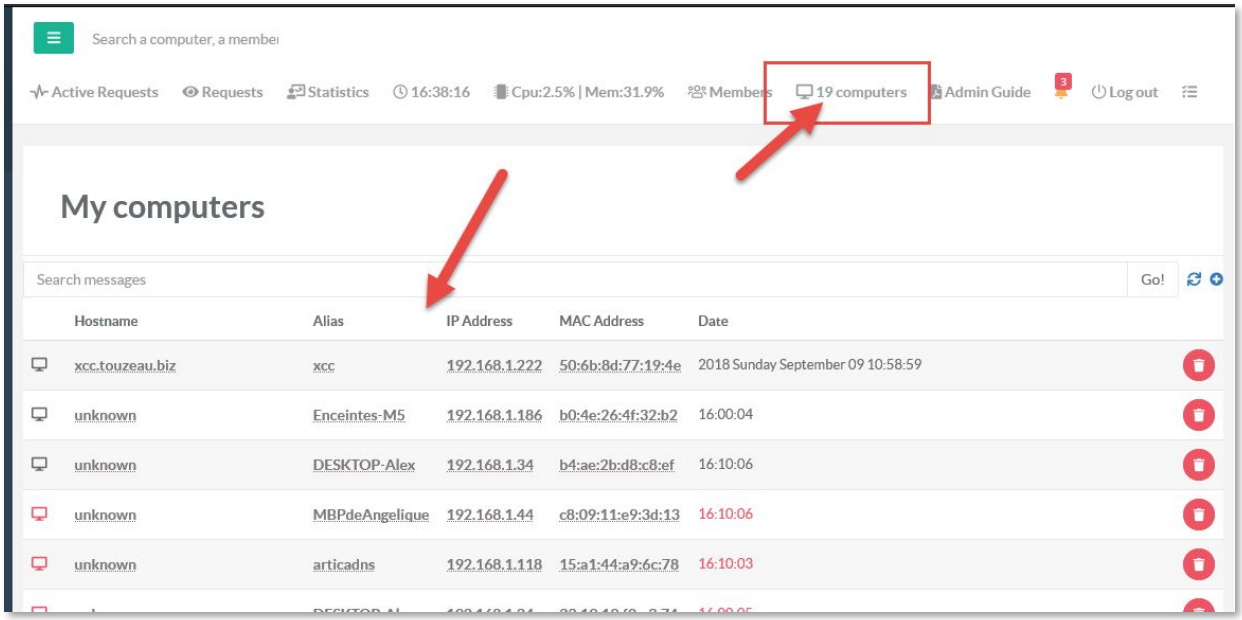
PRADS is a Passive Real-time Asset Detection System.
PRADS employs digital fingerprints to recognize services on the wire, and can be used to map your network and monitor for changes in real time.
Real-time passive traffic analysis will also let you detect assets that are just connected to the network for a short period of time, since PRADS can glean useful information from every packet.
PRADS aims to be the one-stop-shop for passive asset detection, and currently does MAC lookups, TCP and UDP OS fingerprinting as well as client and service application matching and a connection state table.
Various output plugins include logfile and FIFO and make PRADS a useful replacement for p0f, pads and sancp.
PRADS was built from the ground up for a small footprint and modern networks with IPv6 and gigabits of throughput.

Install the Passive Real-time Asset Detection System

- On the left menu choose **Your System / Features**
- On the search engine, type "**prads**"
- Click on install button on the "**Realtime Asset Detection System (PRADS)**"



After few minutes, click on My Computers on the top menu
You will see the list of all detected computers by your Artica server.

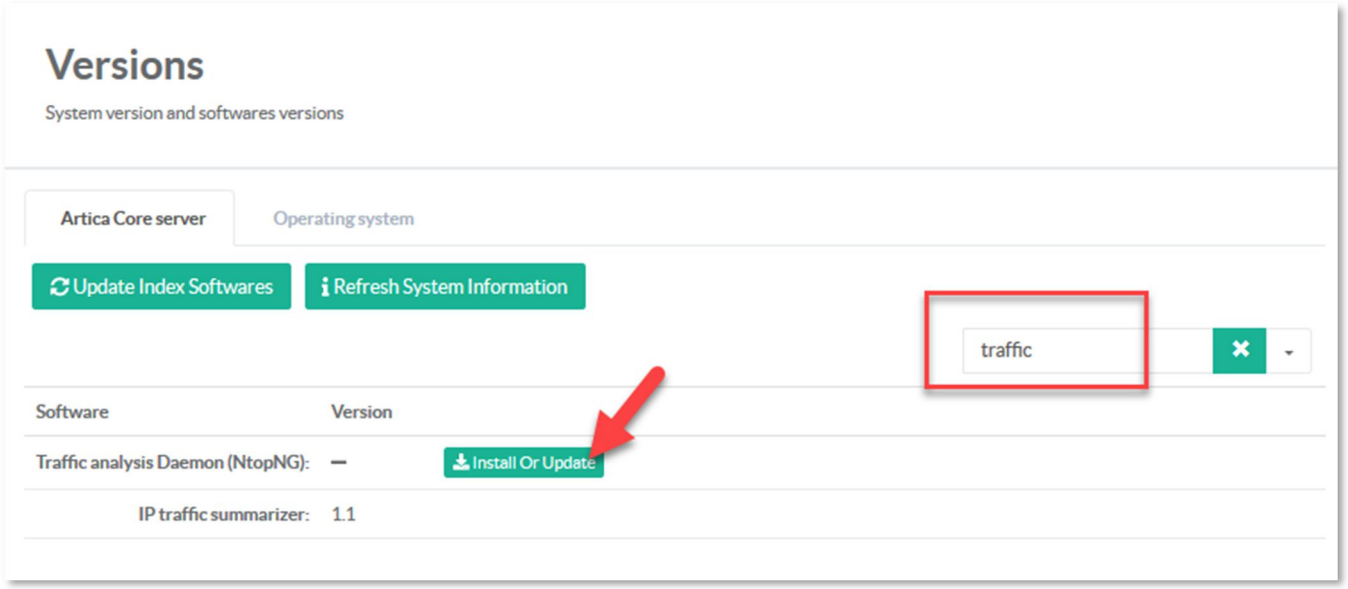


THE TRAFFIC ANALYSIS DAEMON

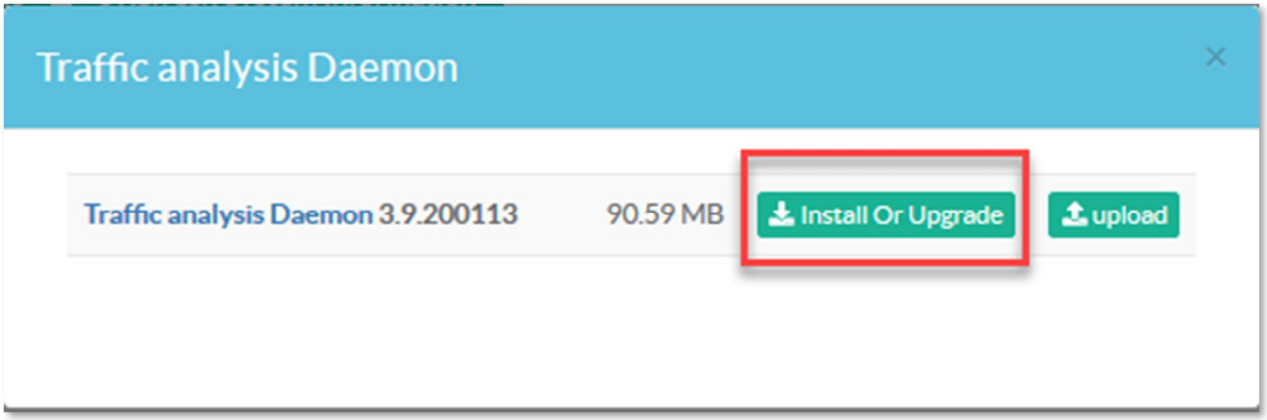
The Traffic analysis Daemon aka (NTOPNG) is a network traffic probe that monitors network usage.
It can be used if your Artica server is installed as a gateway of your network.
Traffic analysis Daemon shows the current network usage.
It displays a list of hosts that are currently using the network and reports information concerning the (IP and non-IP) traffic generated and received by each host.
Traffic analysis Daemon may operate as **a front-end collector** or as a **stand-alone collector**/display program.
It is a hybrid layer 2 / layer 3 network monitor, by default it uses the layer 2 Media Access Control (MAC) addresses AND the layer 3 tcp/ip addresses.
It is capable of associating the two, so that ip and non-ip traffic (e.g. arp, rarp) are combined for a complete picture of network activity.

Update the package

- On the left menu, choose "**Your system / Version**"
- Type "traffic" on the search field
- Click on **Install or Update** button.



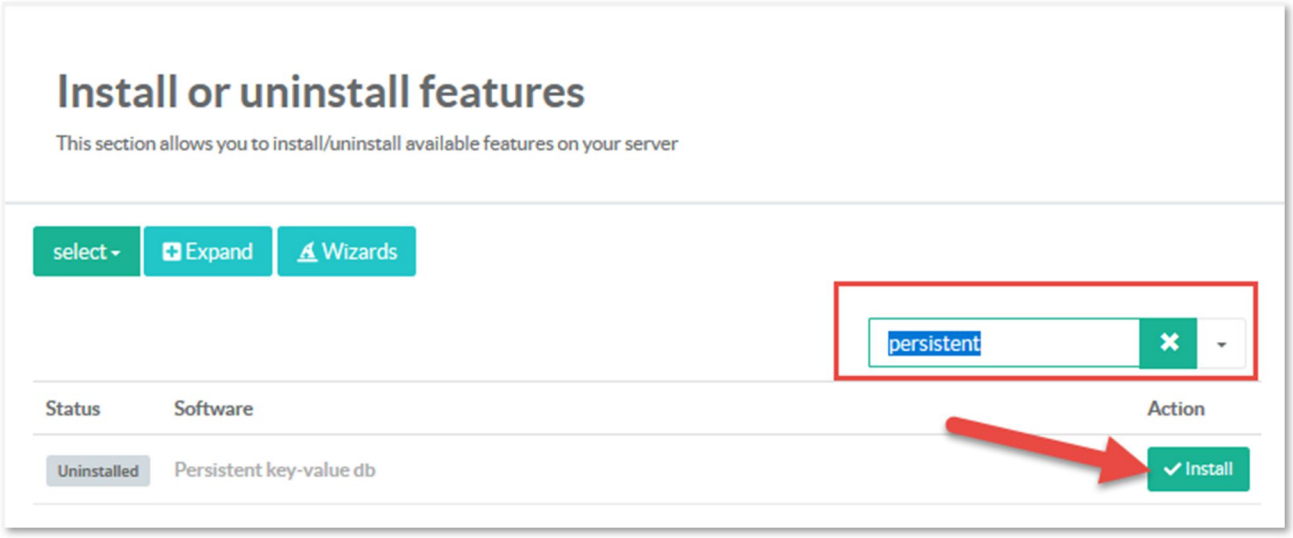
- Click on "Install or upgrade" button on the desired row version.



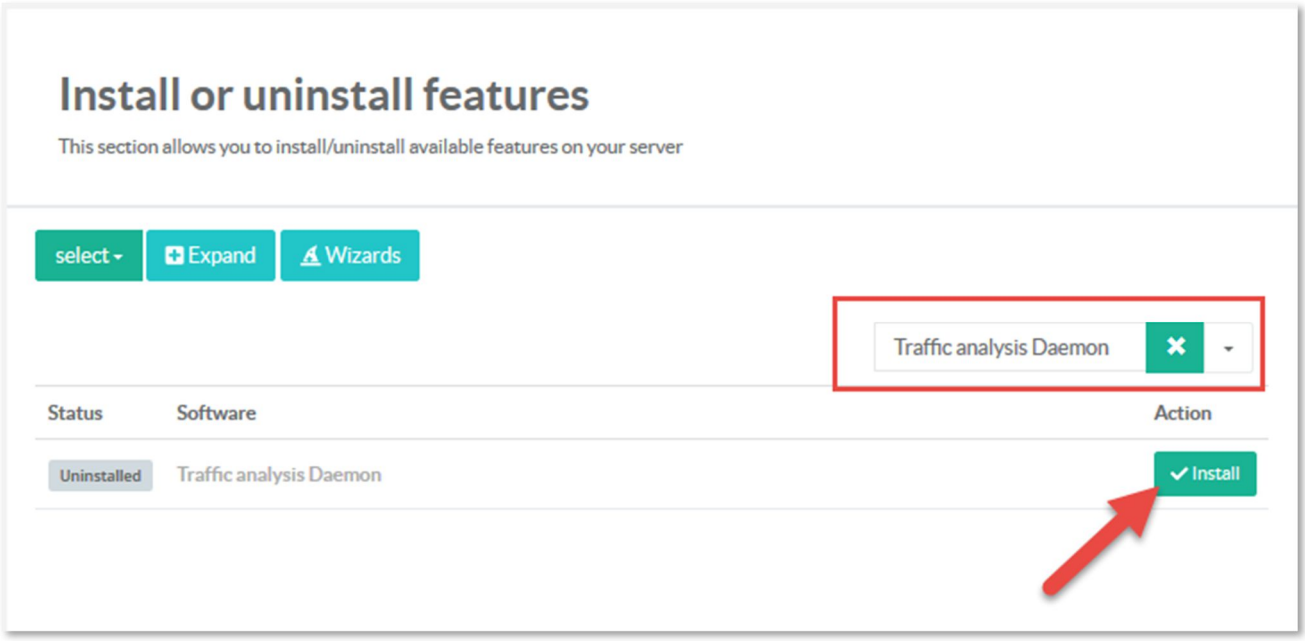
Install the Traffic analysis Daemon

The Traffic analysis Daemon requires the Redis server (Persistent key-value db) to be installed.

- On the left menu choose **Your System / Features**
- On the search engine, type "**persistent**"
- Click on install button on the "**Persistent key-value db**"

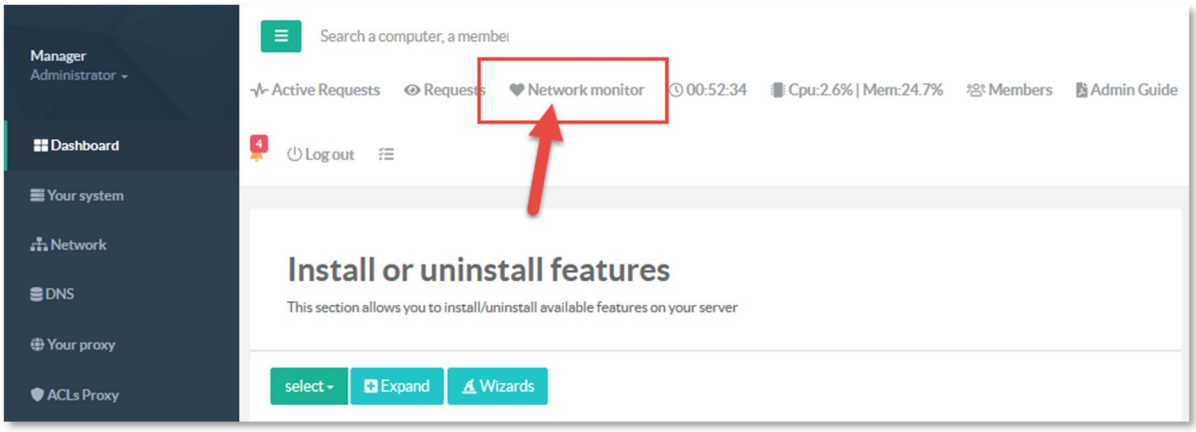


- On the search engine, type "**Traffic analysis"**
- Click on **Install** button. On the **Traffic analysis Daemon** row.

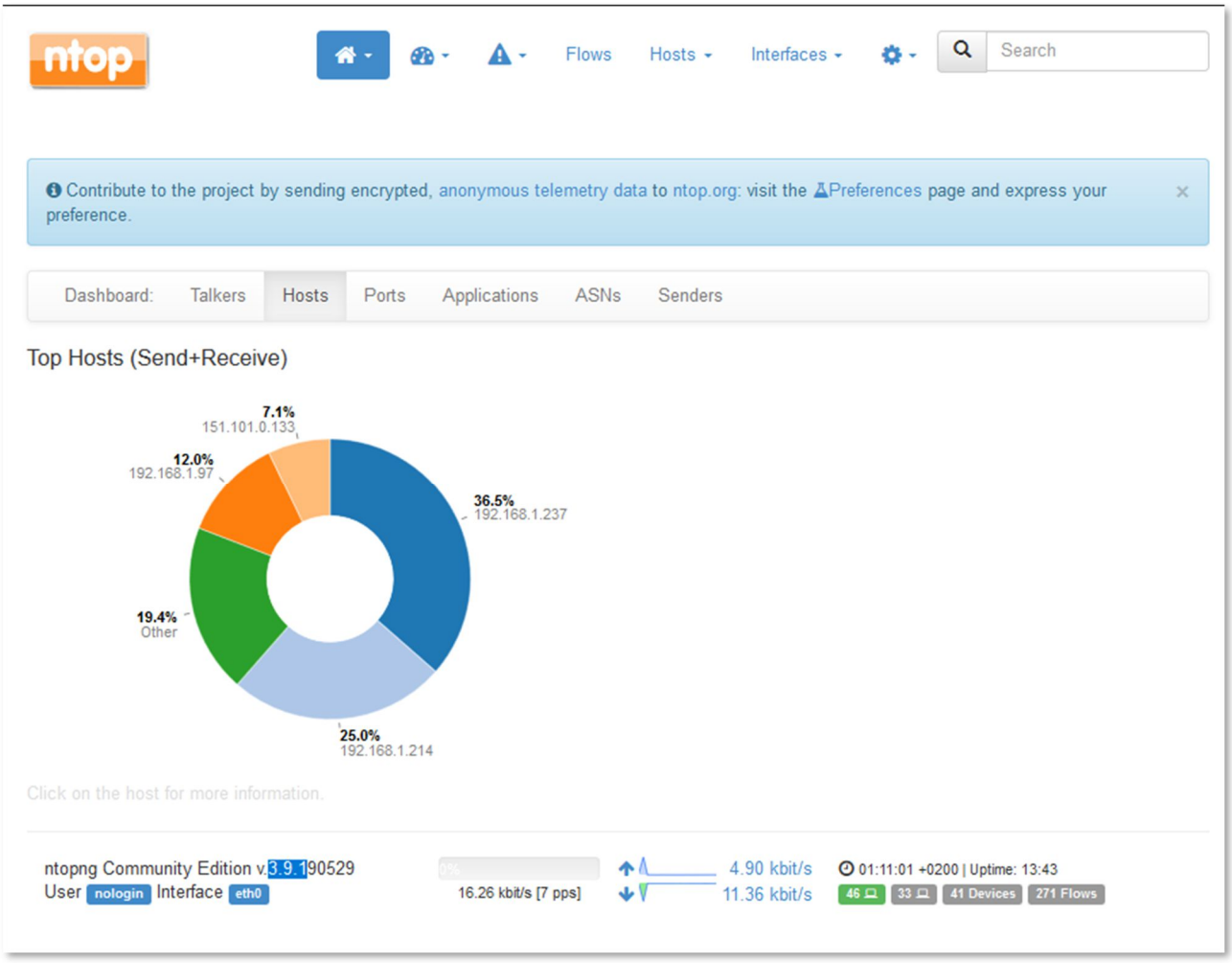


Display statistics

After installing software, click on the "**Network monitor**" top menu.



- A new window will be displayed and shows you the traffic passed through your Artica server.



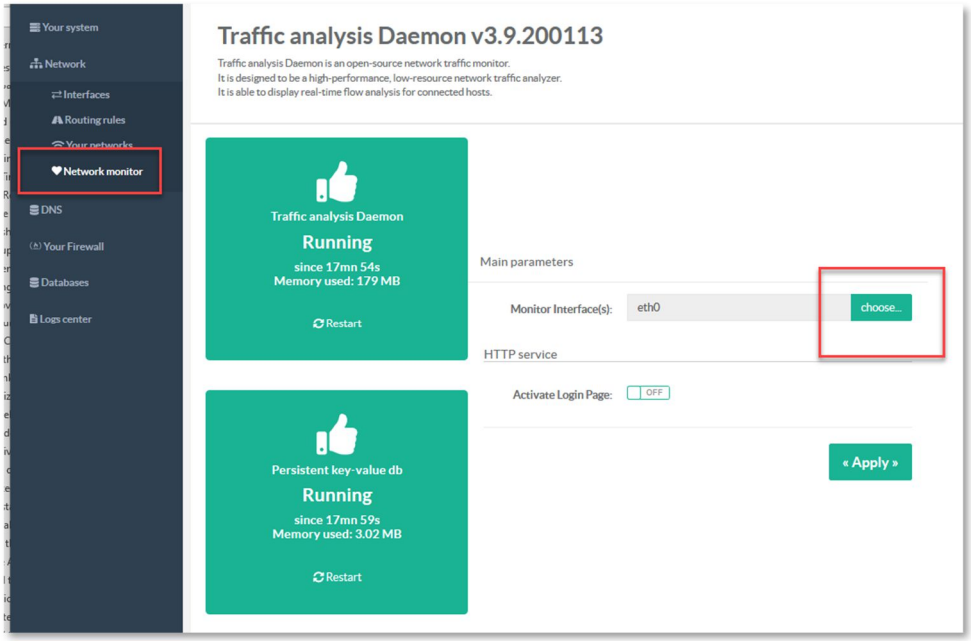
Status and configuration.

On the left menu, choose “Network” and “Network Monitor” menu.

You should see 2 status, the one is the monitoring service, second is the Redis database used to store data.
2 status must be green.

Interfaces to monitor.

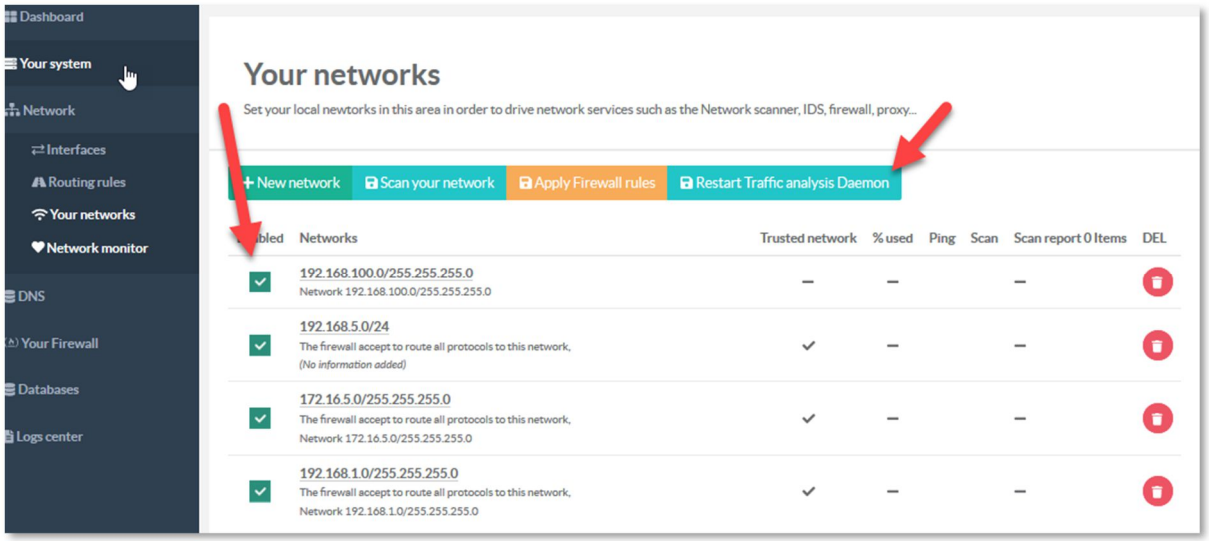
On the main parameters, click on “**Choose**” button under monitor Interface(s) field.
Select Network interfaces cards you want to monitor.
If you want to monitor all interfaces, uncheck all interfaces.



Networks to monitor.

By default, all enabled networks defined in “Network / Your Networks” are monitored by the traffic daemon.
If you did not want to analyze a specific network, disable it and click on the Restart Traffic Analysis Daemon button.

Be careful, a disabled network in this section will be disabled for others managed daemons (firewall for example).

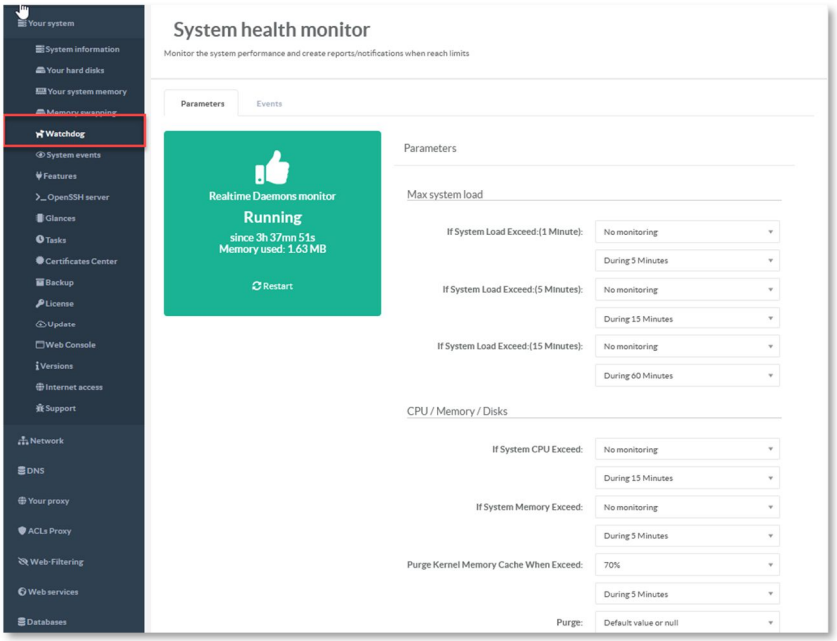


MONITORING THE SYSTEM

SYSTEM HEALTH MONITOR

The Watchdog service (System health monitor
)is in charge to monitor your system health and build an incident report if some elements exceed values.

You will find the watchdog in **Your System** / **Watchdog**



Monitoring the system Load

This monitor the load of your server and if the load exceed the value, Artica will generate a system report in order to investigate which task/service consume the server performance

You have 3 parameters, the 1 minute, 5 minutes and 15 minutes. On each parameters you define how many times the load exceed your value.

You can estimate that if the load is more than 1.5x the number of CPUs, your server seems overloaded.

For example :

```
4 Cpus = 1.5*4 = 6
```

You can define this
For the 5 minutes Load is higher than 6 during 15minutes.

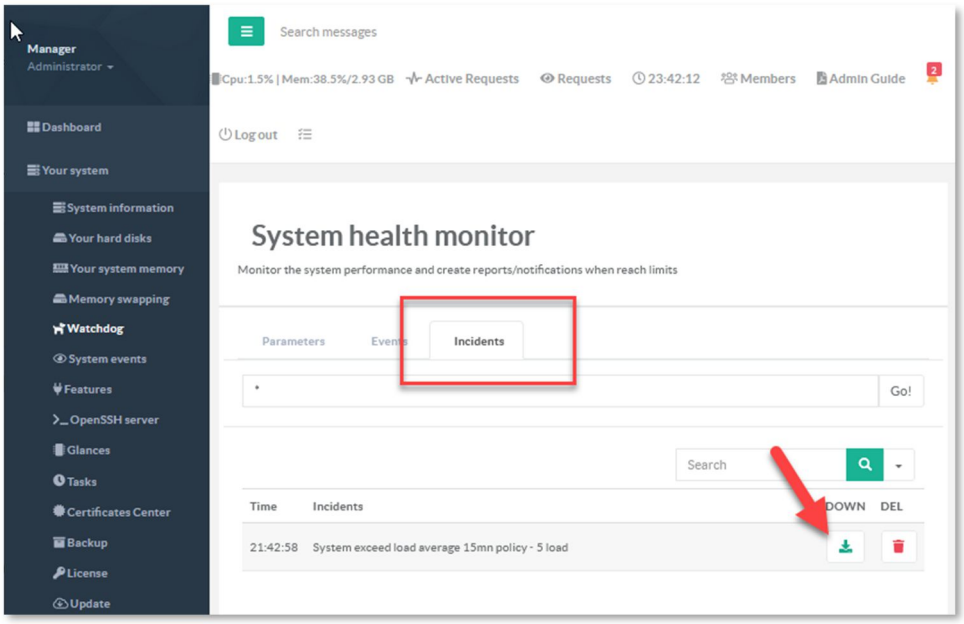
Monitoring CPU / Memory / Disks

- **If system CPU exceed**: Force Artica to create a report if the CPU is higher than a percentage of use during a period in minutes.
- **If system memory exceed**: Force Artica to create a report if the Memory usage is higher than a percentage of use during a period in minutes.
- **Purge Kernel memory cache when exceed**: If the memory usage exceed a percentage, Artica will ask the kernel to purge the non-used affected memory slots.
- **Alert if free space is less than:** If the free space is under a percentage, Artica will add an alert in system events.

Display incidents reports

When Artica build a report, it save all debug information inside a database in order to let you search and analyze why a load/CPU usage, Memory usage was exceed values.

- Click on the **incidents** tab
- Click on the **download** link in order to download reports according to the incident.



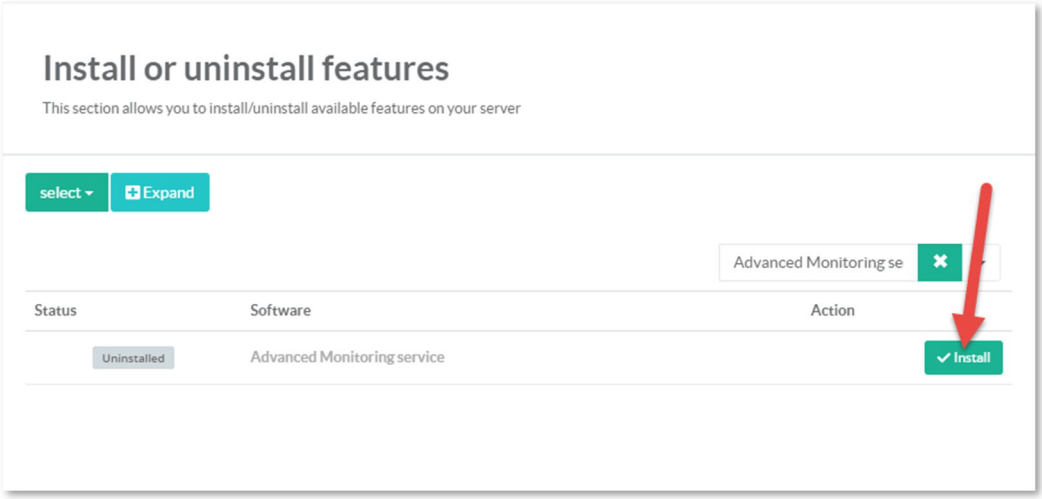
THE ADVANCED MONITORING SERVICE

The Advanced Monitoring service (aka Netdata) is a system for distributed real-time performance and health monitoring.

It provides unparalleled insights, in real time, of everything happening on the systems it runs (including containers and applications such as web and database servers), using modern interactive web dashboards.
A Demo is available here http://london.my-netdata.io/default.html#menu_system_submenu_cpu;theme=slate

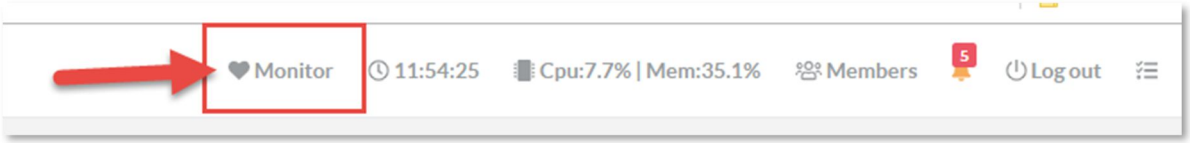
Installing the service

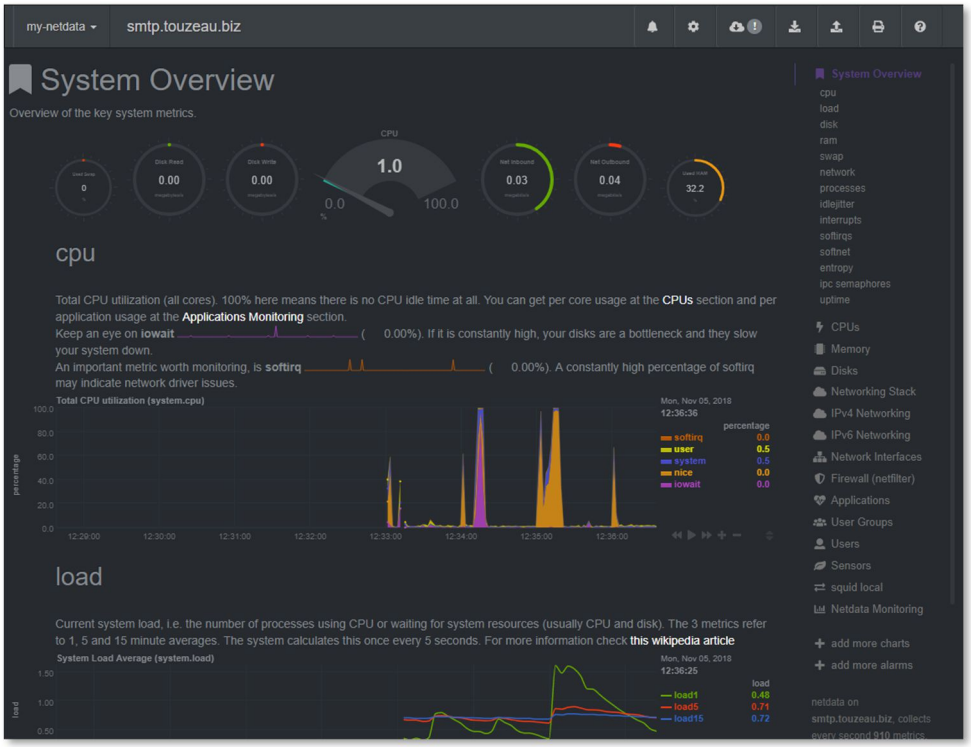
On **Your system**, select "**Features**", type "**Advanced Monitoring service**" in the search field.



Access to statistics

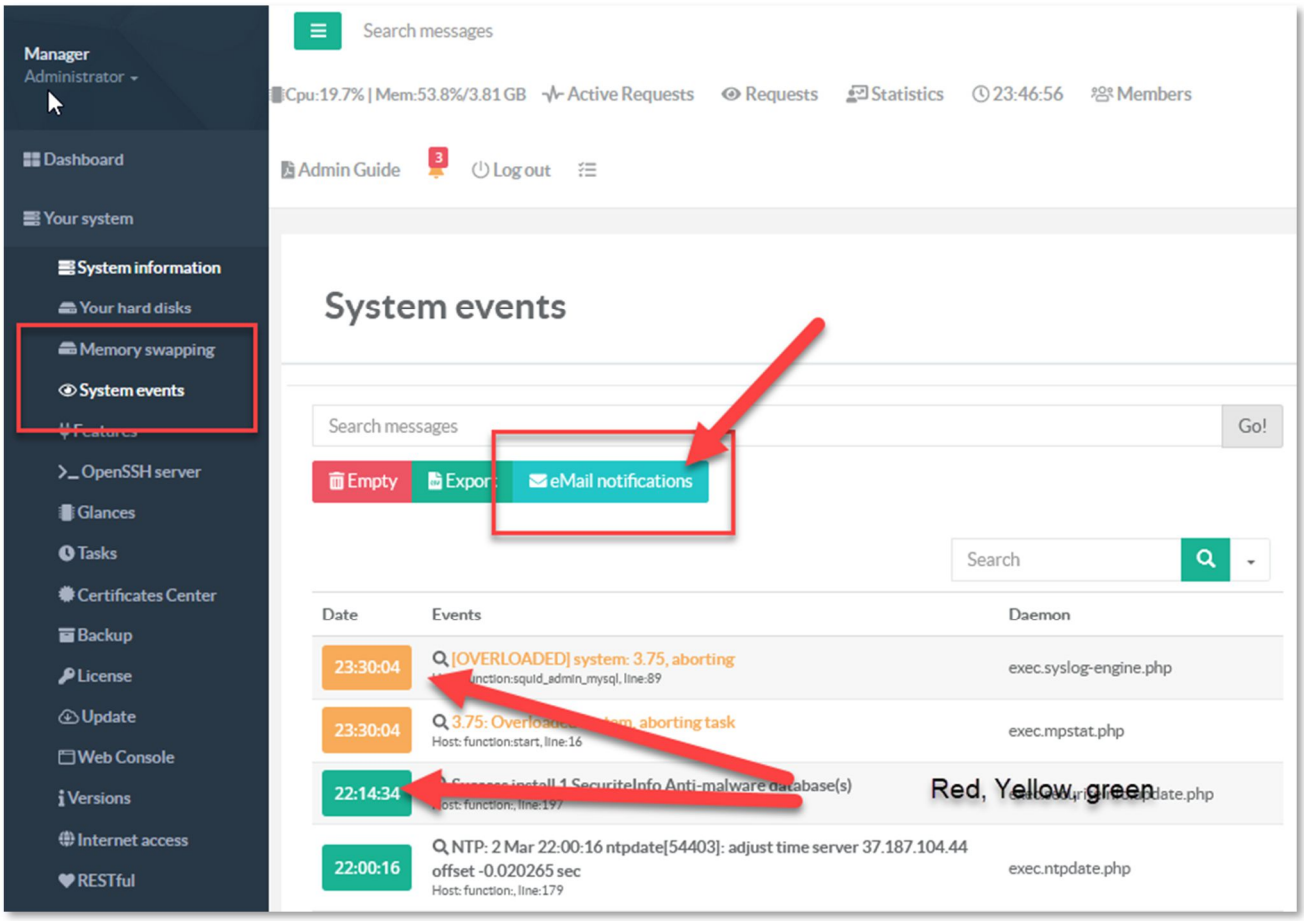
On the TOP menu, a new link "**Monitor**" is displayed, click on it to see statistics of your Artica server.





SMTP NOTIFICATIONS

Artica is able to send by SMTP the content of system events.
You can display events generated by Artica in the system events in "Your system "/ "System events".
Events are categorized in 3 levels : Red for critical issues, yellow for warnings and green for just information.



Configuring notifications

Click on the **eMail notifications** buttons

To enable SMTP notifications, turn on the "**Enable SMTP notifications**" checkbox.

If you want to be notified when an administrator try to logon on the Artica Web console, turn on the "**Web console accesses**" checkbox.

If you want to be notified when something try to logon on the SSH service, turn on "**SSH Login attempts**" checkbox.

By default you are notified only on critical issues (red), if you want to be notified on "**Warning issues too**", turn on the "**Warning events**" checkbox.

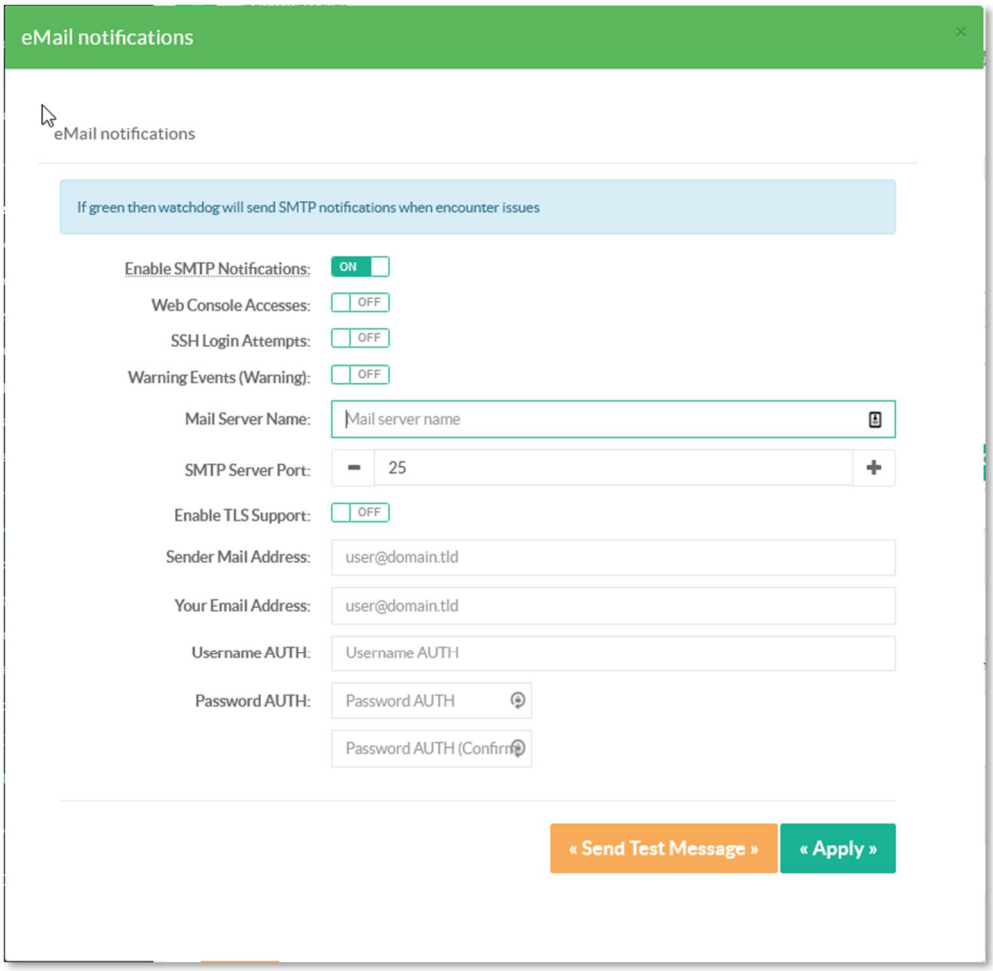
Set the address of the SMTP server that will receive generated events in the "**Mail Server Name**'" field.

If your SMTP service require TLS, enable the TLS support checkbox.

Define the eMail address of the sender of the message.

In **your eMail address** field, define the recipient that will receive notifications messages.
If you want to add more than one recipient, separate them by a comma.

NOTE: BEFORE CLICK ON THE SEND TEST MESSAGE, YOU HAVE TO CLICK ON APPLY BUTTON FIRST



ZABBIX AGENT

Follow this video in order to install the Zabbix Agent inside your Artica server in order to monitor Artica service

Youtube video

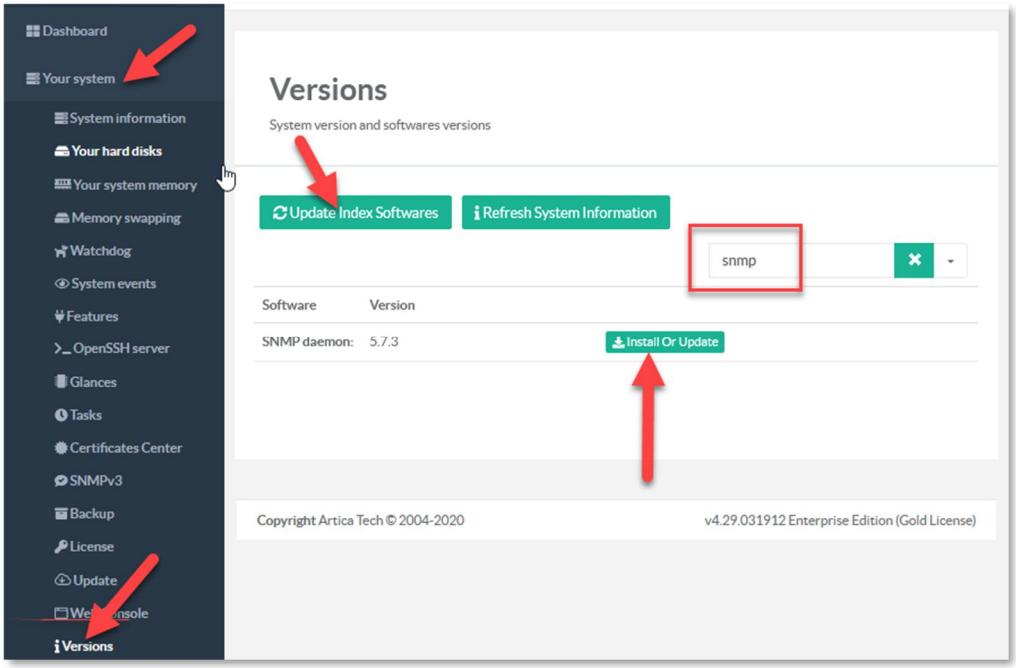
https://youtu.be/Y1xLJeY4308

THE SNMP SERVICE

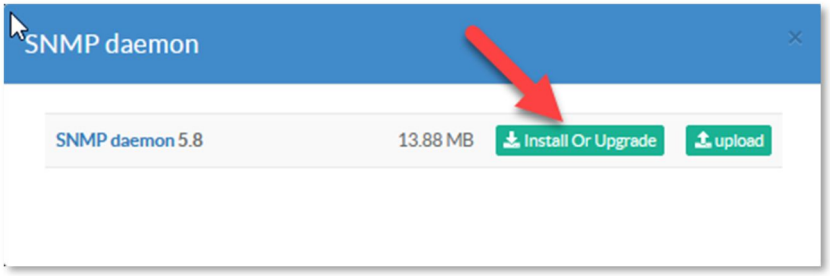
The SNMP service allows you to monitor your Artica server with any SNMP management console.
If you did not have any SNMP console, we suggest to use

Upgrade the SNMP software.

ON the left menu, click on "**Your system / Versions**"
Click on the **Update Index Softwares** button.
On the search field, type "**snmp**"

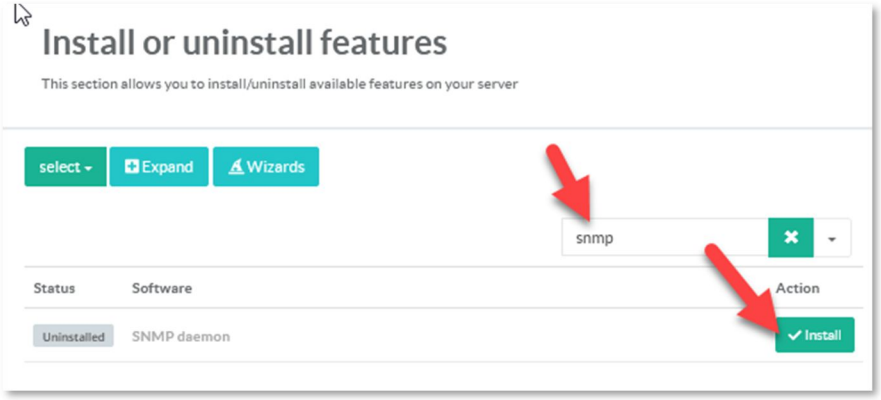


- Click on **Install Or update** button under the **SNMP Daemon** row.
- Choose the latest package and click on **Install or Upgrade** button.



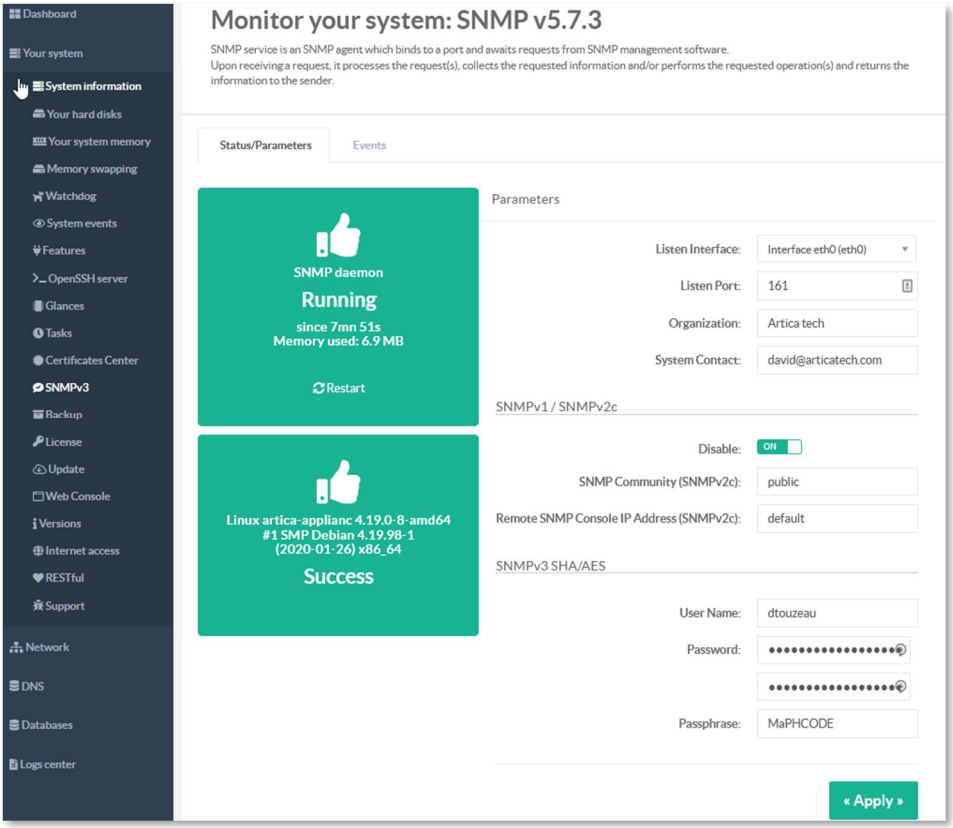
Install the SNMP service

- On the left menu, choose **Your System** / **Features**
- On the features section search the entry **SNMP**



- On the left menu, choose "**Your System / SNMPv3**"

By default the SNMP service listen all interfaces on UDP 161, you can modify this settings by using the **Listen Interface** and **Listen port** fields.



SNMPv2

By default, the SNMP service listen all interface on udp 161 using SNMPv1/SNMPv2

If you need to use SNMPv2/v1,
The Community is defined as "public" by default.

In the **Remote SNMP console IP address** field, the entry "default" means every addresses, you can modifiy by adding a CDIR notation (192.168.1.0/24) or the IP address of your SNMP console (192.168.1.2).

Turn to only SNMPv3

If you want to use only SNMPv3, turn on the "**Disable**" Checkbox in the **SNMPv1/ SNMPv2** section

In this case, the SNMP service will use SHA / AES and authPriv for authentication method.

Set a username and password (minimum 8 characters) And define the Pass Phrase to encrypt the password.

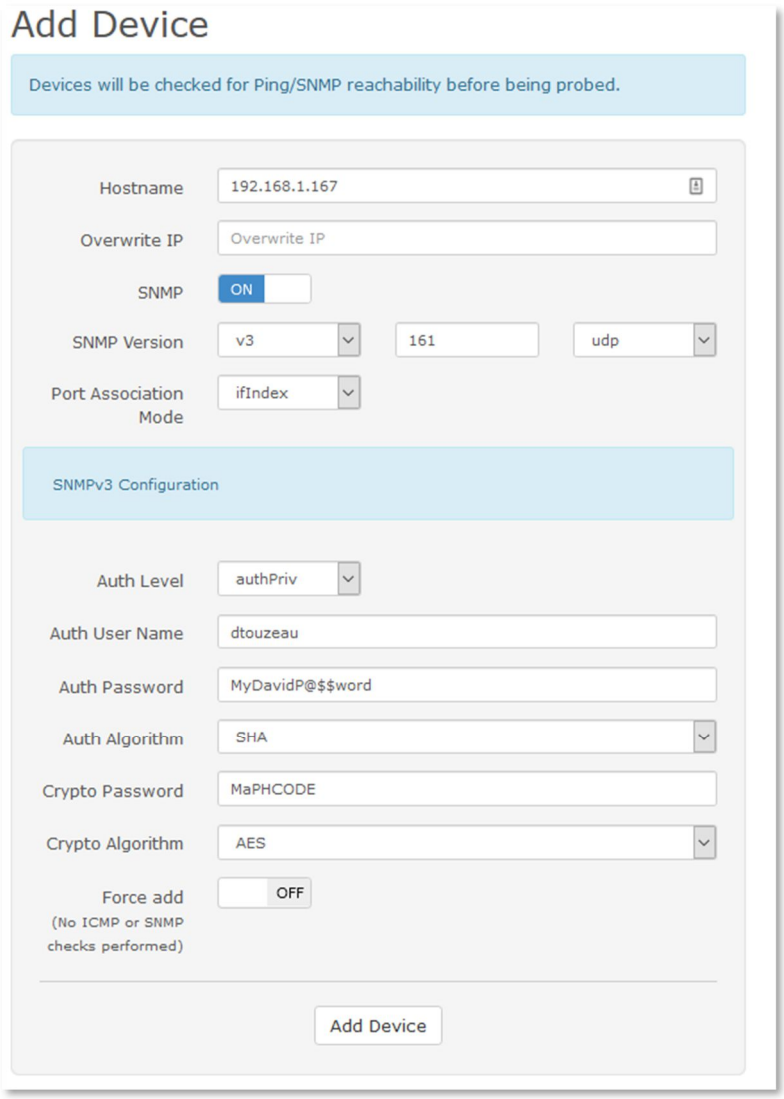
Manage the SNMP service Via RESTful API

The SNMP service can managed via RESTful API, download the documentation about the system RESTful API here:
http://articatech.net/download/SYSTEM-REST-API.pdf

Add host using SNMPv3 on LibreNMS

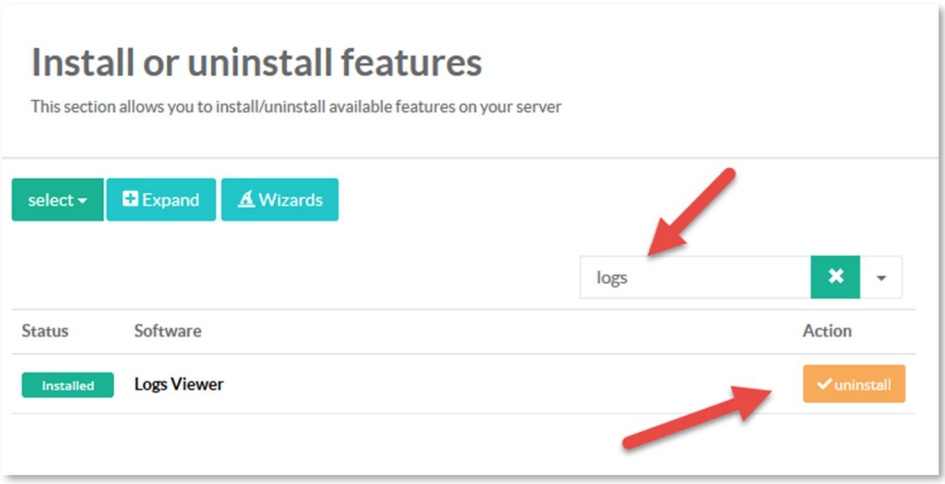
When adding a device on the LibreNMS console, pay attention to use these values:

- **SNMP Version** : Select the **v3** option and use **161** on **udp**
- **Auth Level**: Choose **authPriv**
- **Auth User Name**: Give the **username** defined in Artica.
- **Auth password:** Give the **password** defined in Artica.
- **Auth Algorithm**: Choose **SHA**
- **Crypto Password**: Give the **Pass Phrase** defined in Artica
- **Crypto Algorithm**: Choose **AES**.

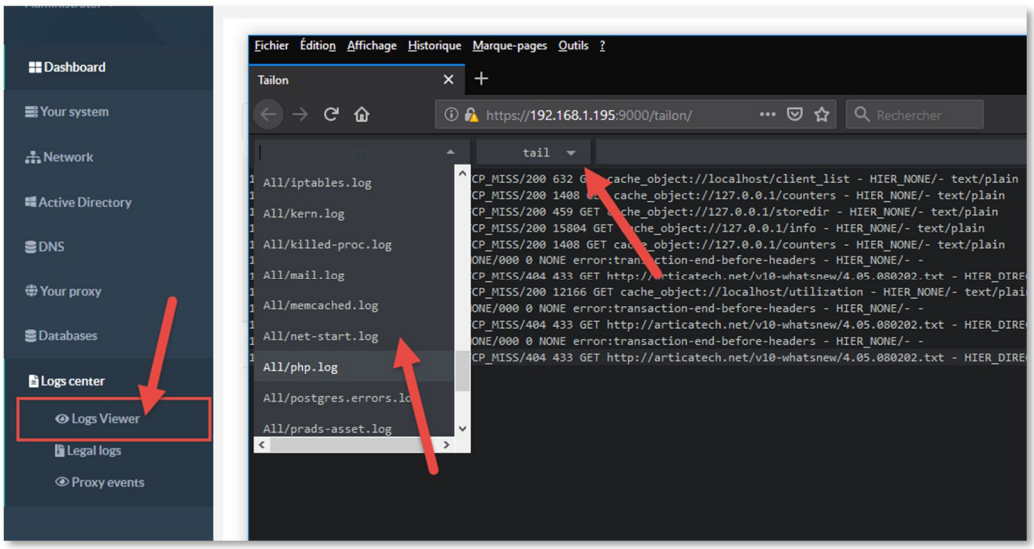


THE LOGS VIEWER

By default, latest Artica versions install the module **"Logs Viewer"**.
Logs Viewer is a feature you can install that allows you to search, tail in logs files of your server.



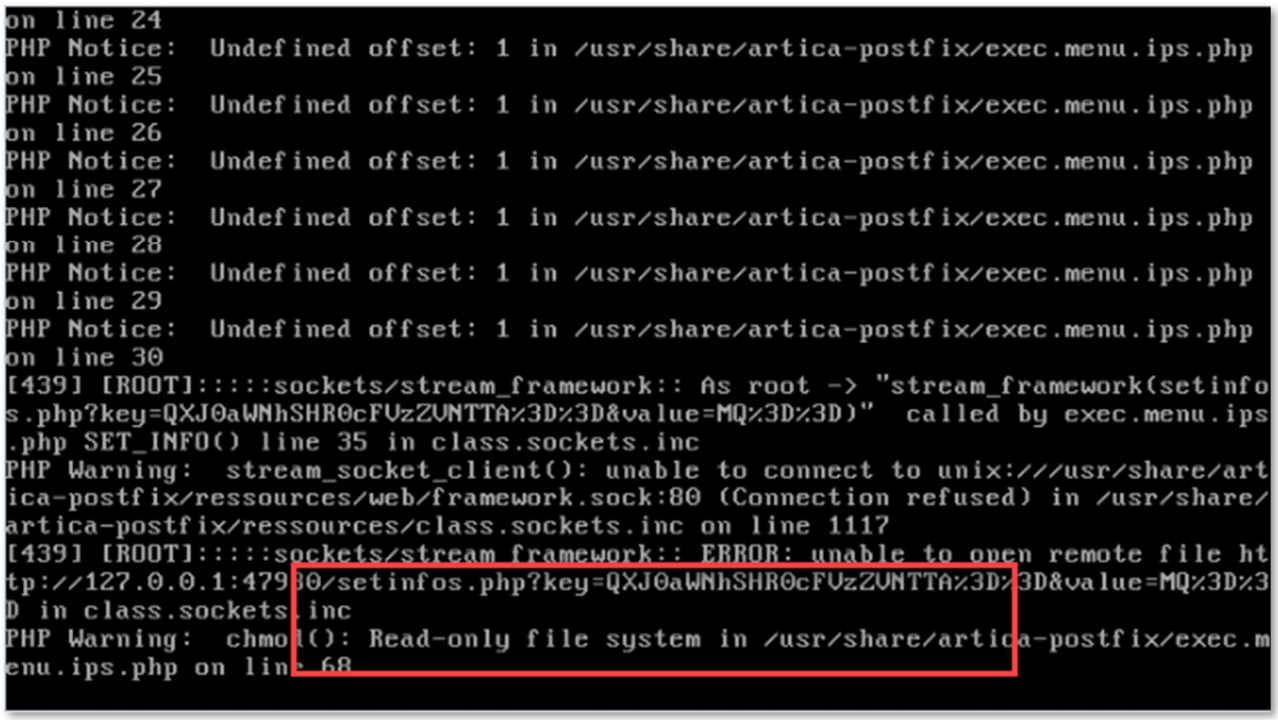
You can display it using the left menu in "**Logs center**"/ "**Logs Viewer**"



TROUBLESHOOTING

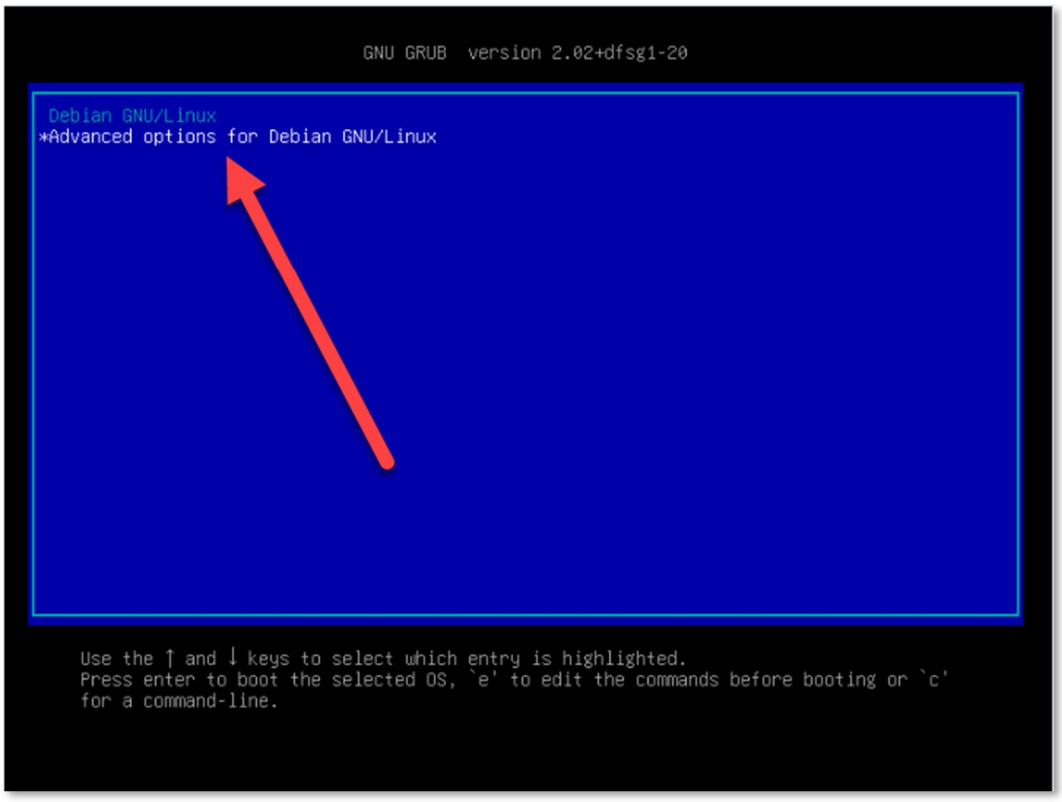
Read-only filesystem

The default behavior for most Linux file systems is to safeguard your data.
When the kernel detects an error in the storage subsystem it will make the filesystem read-only to prevent (further) data corruption

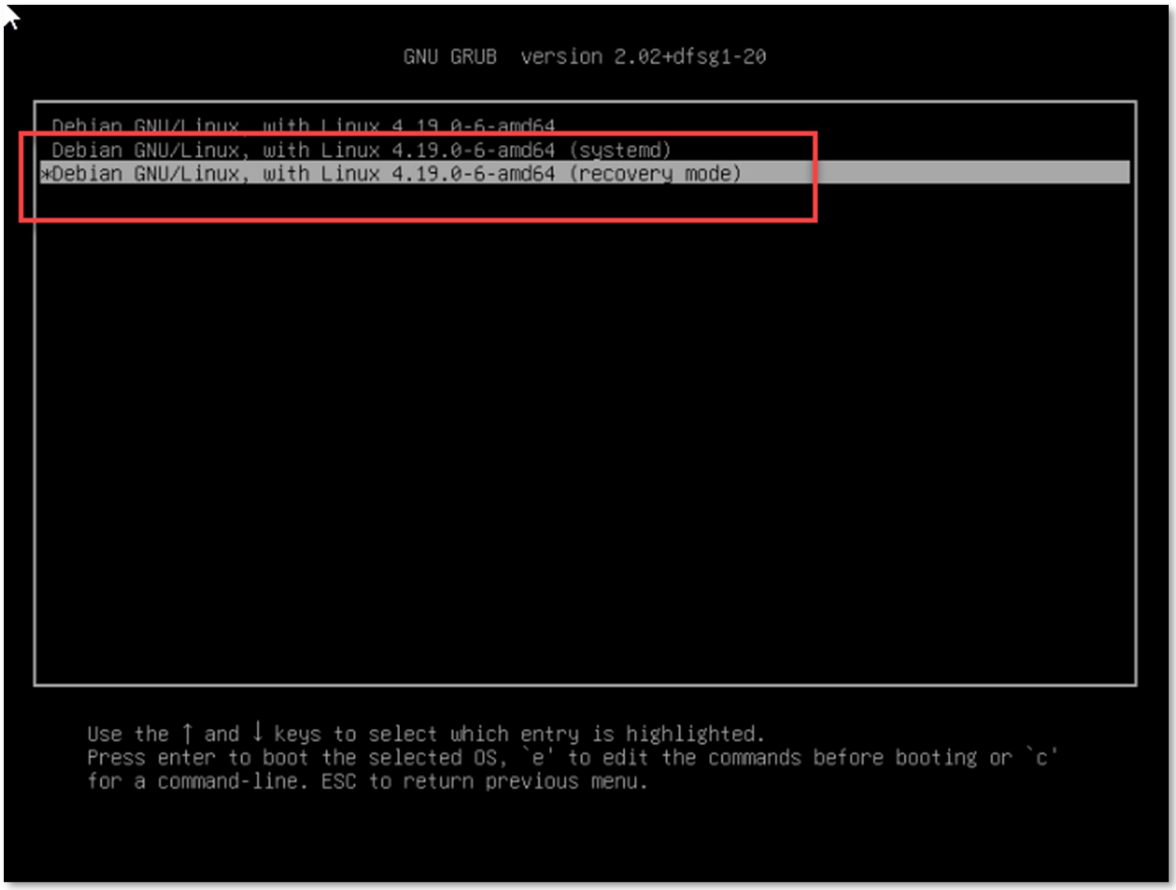


When displaying the Unix Console, you can see these errors on the system.

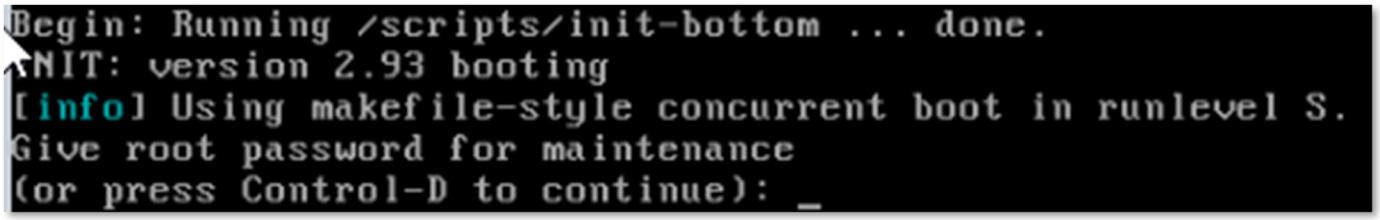
To repair, reboot your Artica server and when the menu screen appears choose the menu “Advanced options for Debian GNU/Linux”



Select the **recovery mode** menu.



The screen will ask you to press **Control-D** or enter the root password.



Enter the root password (by default the keyboard is QWERTY)
Run this command-line

```
fsck -p -f
```

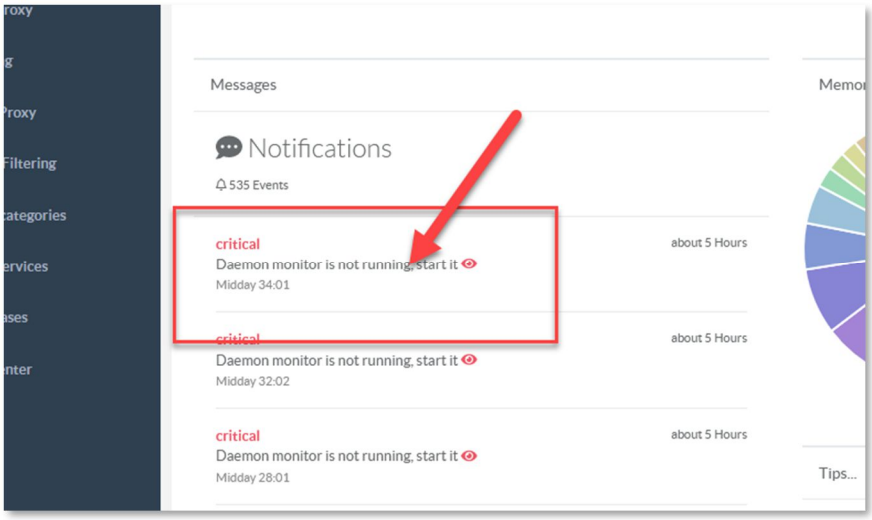
reset your server

The Daemon monitor not running

After updating Artica, you can see in dashboard many critical Events about the Daemon monitor not running.

This caused by an outdated Daemon monitor configuration.

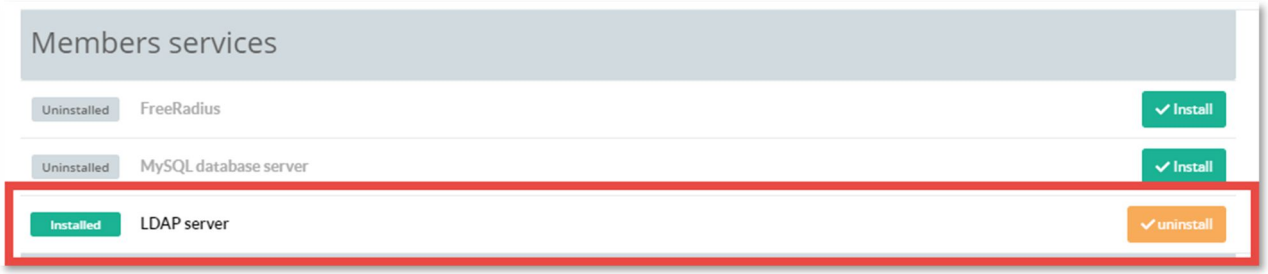
Update to nightly 4.29 or 4.30 Artica release.



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
in "Members services/LDAP Server."



OPENLDAP SERVICE PARAMETERS.

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

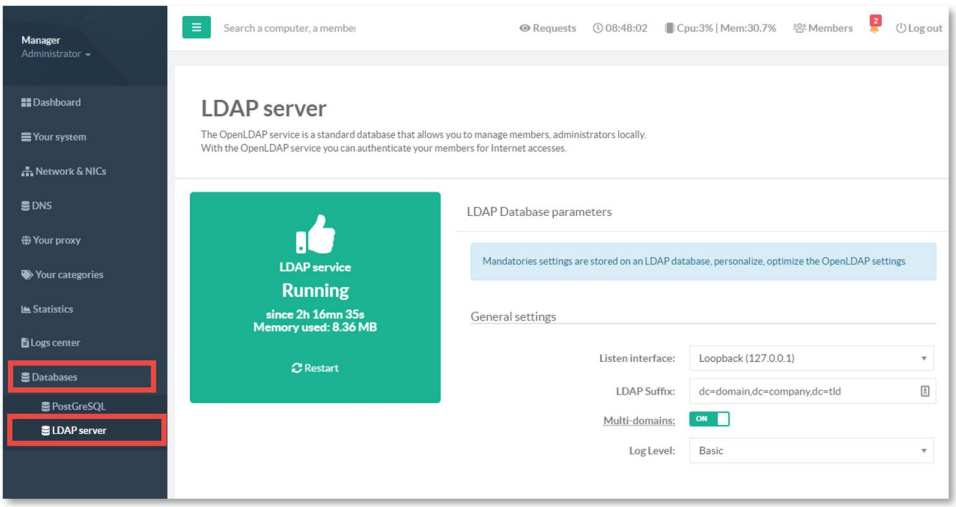
Listen Interface: By default the LDAP server serves only the loop back address because all services used by Artica don't need to access the database externally

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)

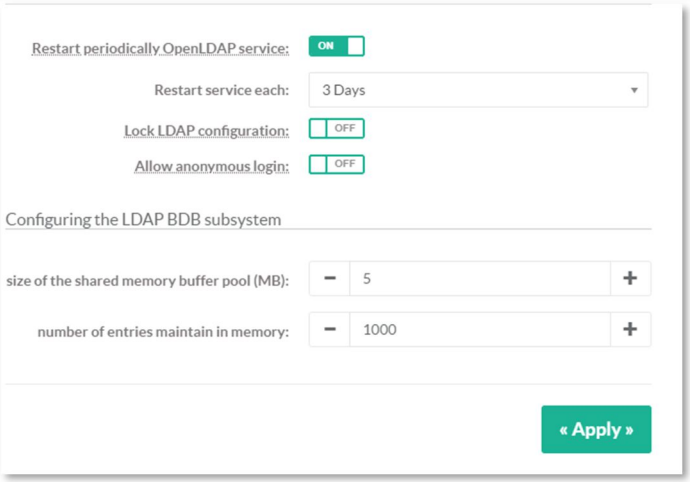
Restart periodically OpenLDAP service: If turned on then Artica will restart OpenLDAP service at 6h30,12h30,3h30



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

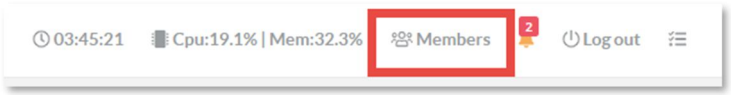
Lock LDAP configuration: If enabled, Artica will not modify the /etc/ldap/slpad.conf and let you change it.

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



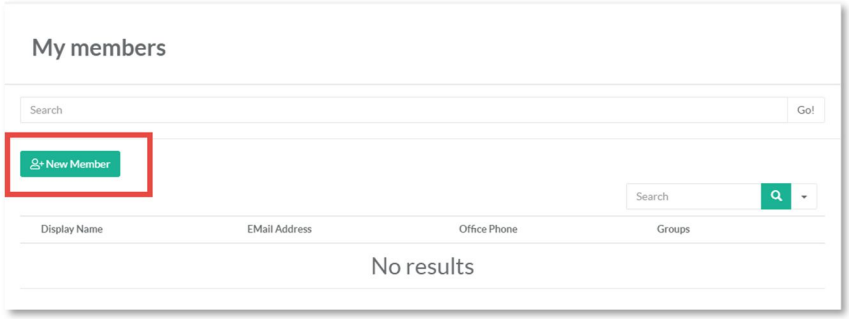
MANAGE LDAP MEMBERS/GROUP

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

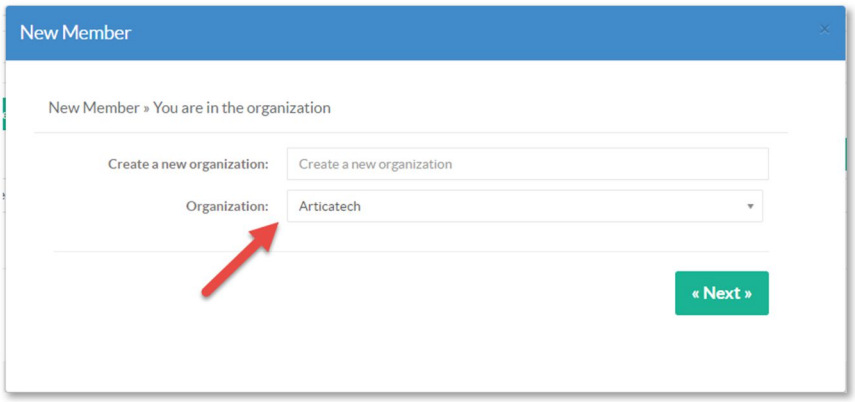


A table is displayed and allows you to search for members and groups.

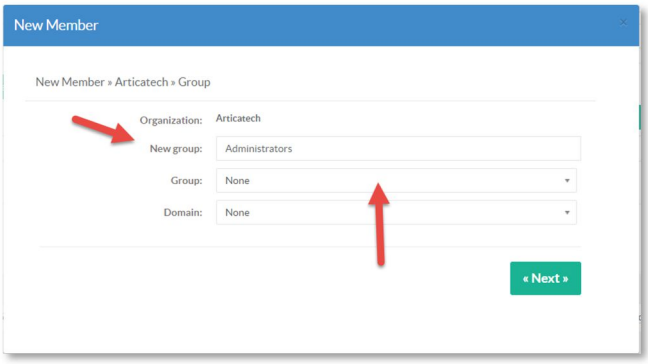
to create a user, click on the button “New member”



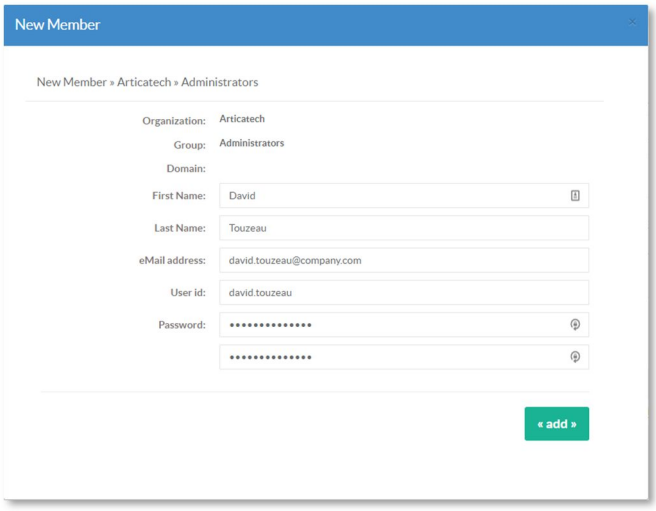
A wizard is displayed and ask to you in which organization the member must be stored.
You can choose in the drop-down list an already organization or you can create a new organization by adding the new organization name in the “Create a new organization” field.



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.

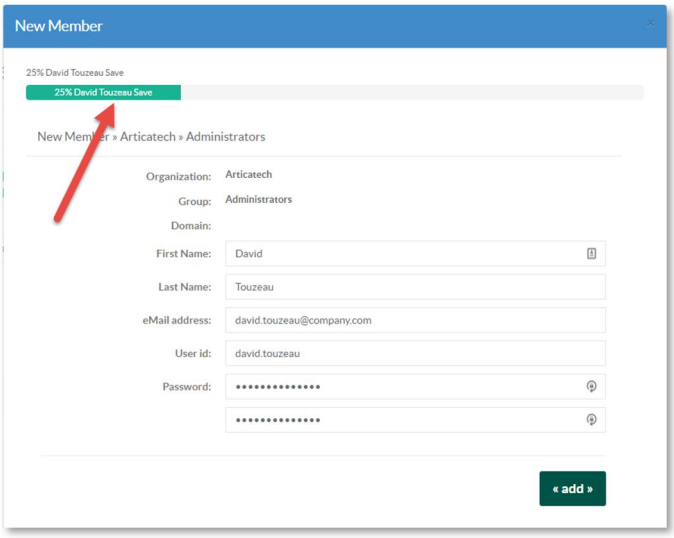


- Set the first name and last name of the new member.
- Set the email address
- **The user id:** is the account that the user will use to be logged on services that use LDAP authentication.
  If you did not see this field, it means the login name using the eMail address.
- Set the user password.

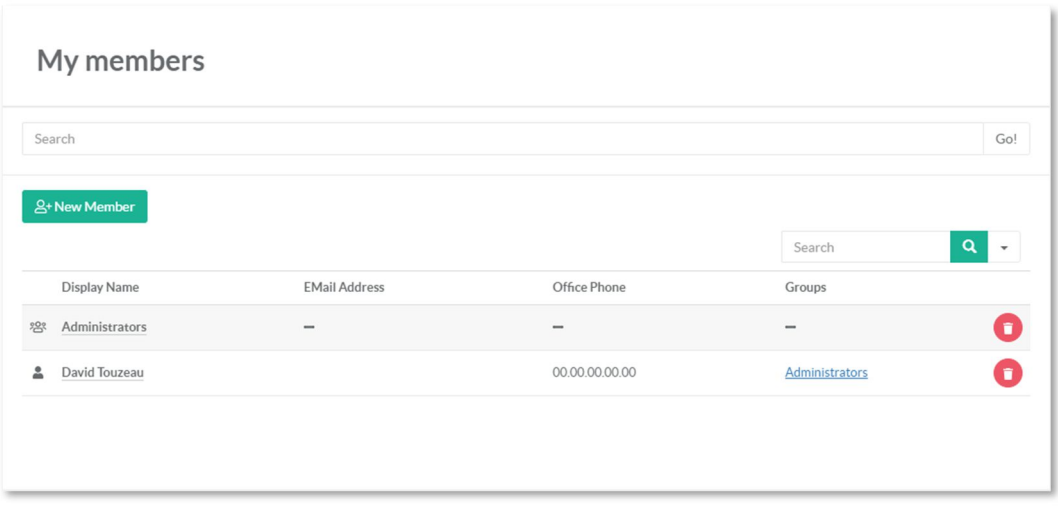


By default the LDAP database is OpenLDAP service parameters.enabled (SEE OPENLDAP SERVICE PARAMETERS.) That enables the eMail address has the login user.

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



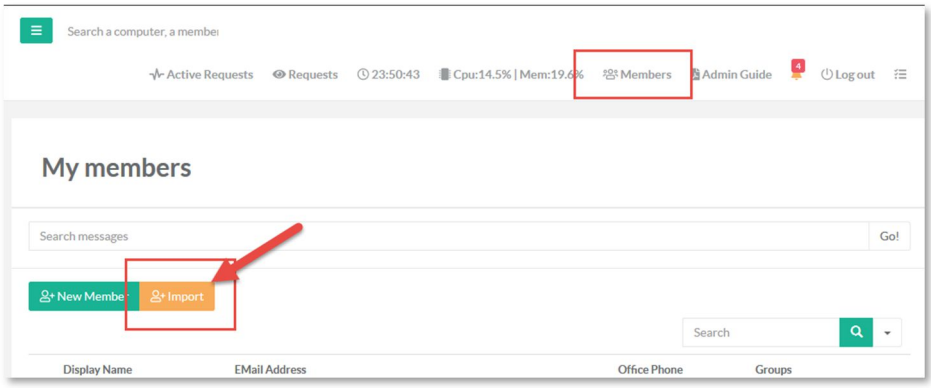
The table will display your new member and the created group.



Import members from a text/CSV file

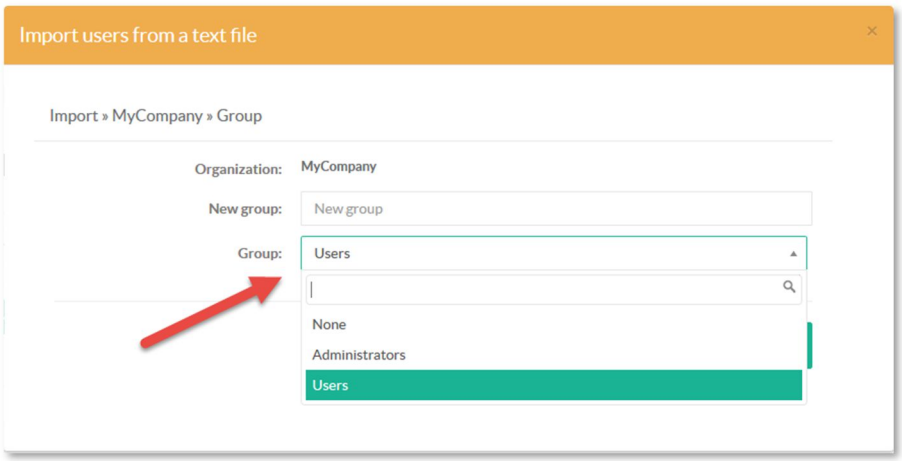
You can import members from a text file.
The importation task run under a group.

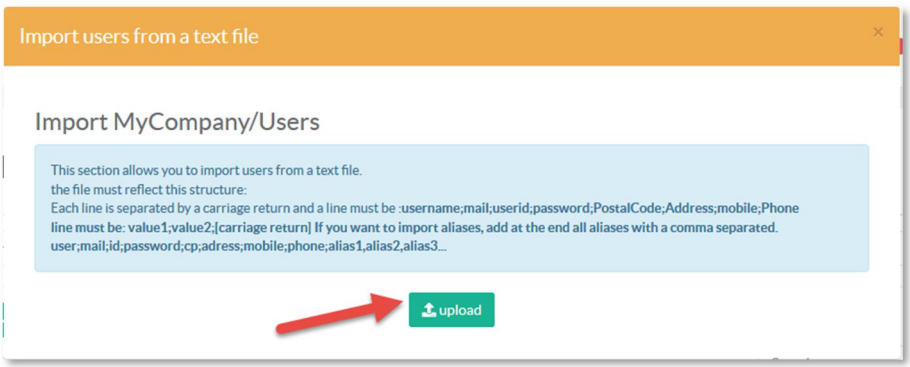
On the members section, click on the button "**import**"



If you want to import users only on a group choose your LDAP group.
If you want to import users inside several groups and let Artica creating groups:

- Do not select any group and continue.
- In this case, provide a CSV file with comma separated using these fields:
  "Username,Password,EmailAddress,Group,Title,GivenName,Surname,StreetAddress,City,ZipCode,TelephoneNumber,Mobile"
- A file example can be downloaded here **http://articatech.net/download/import-members-full.zip**

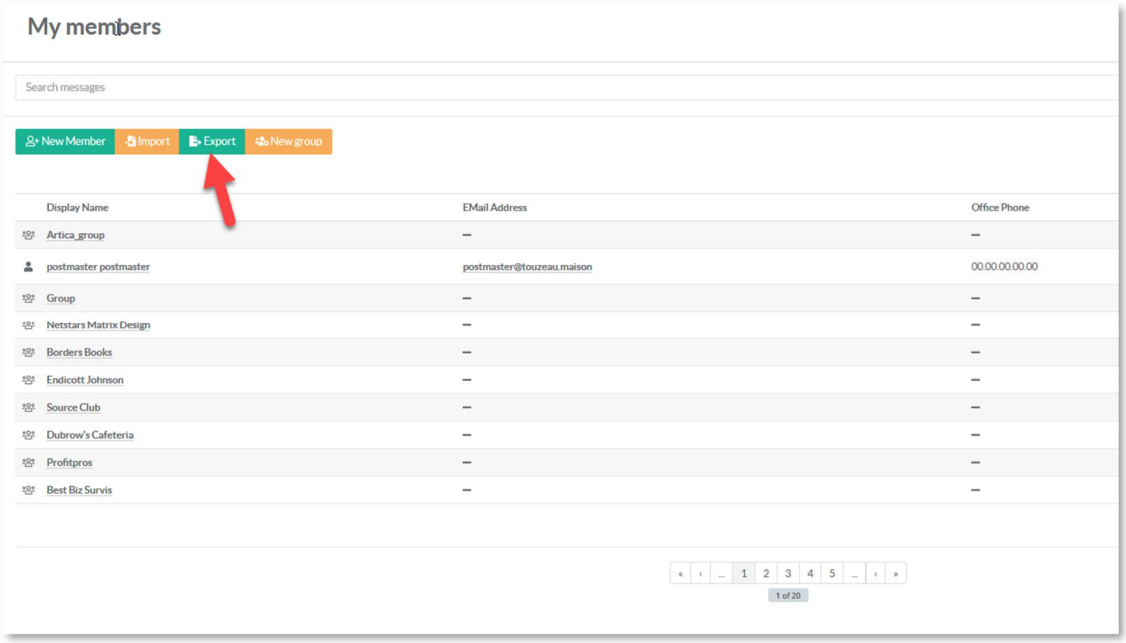




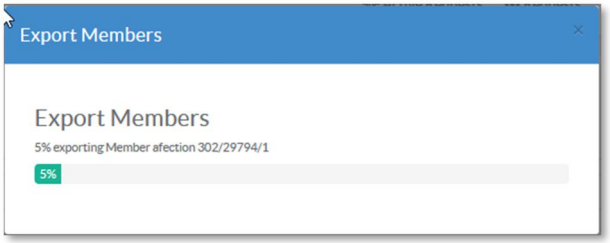
Click on the upload button to browse your data file
It must reflect this structure:
Each line is separated by a carriage return and a line must be :**username;mail;userid;password;PostalCode;Address;mobile;Phone**
line must be: value1;value2;[carriage return] If you want to import aliases, add at the end all aliases with a comma separated.
user;mail;id;password;cp;adress;mobile;phone;alias1,alias2,alias3...
An example of text to import can be downloaded using this url (http://articatech.net/download/import-members-example.txt)

Exporting users to a CSV file

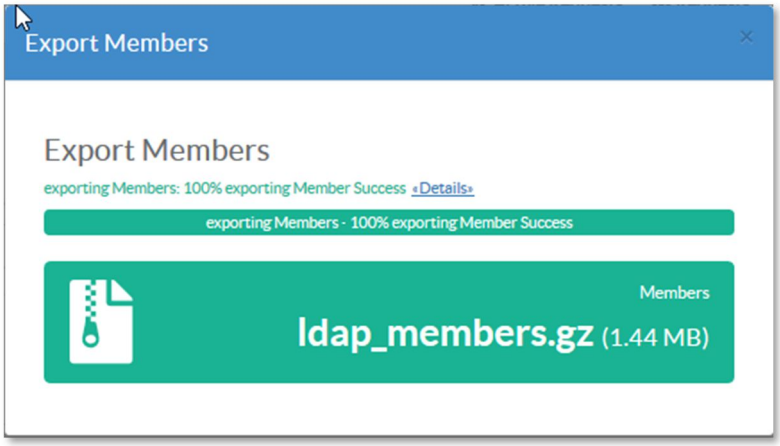
To export all members to a CSV file, click on the "Export" button



- A confirmation message wil ask you to confirm the exportation.

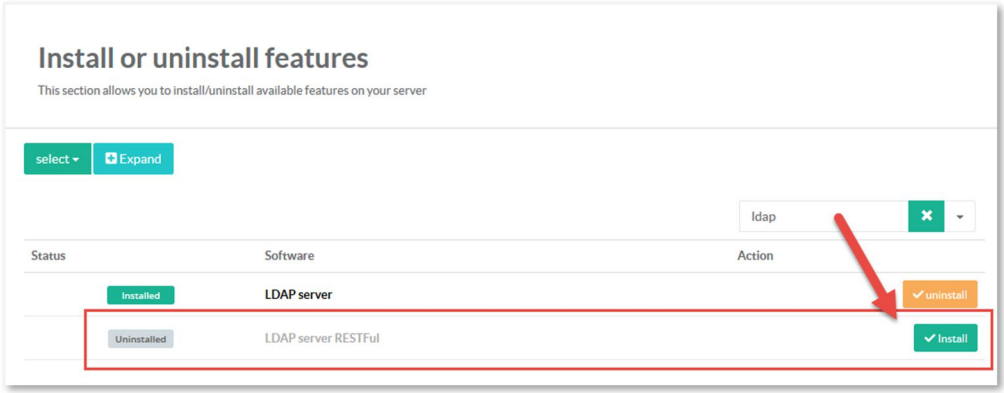


- Wait during the exportation task
- After complete, download the csv compressed file with comma separated using these fields: "**Username,Password,EmailAddress,Group,Title,GivenName,Surname,StreetAddress,City,ZipCode,TelephoneNumber,Mobile**"

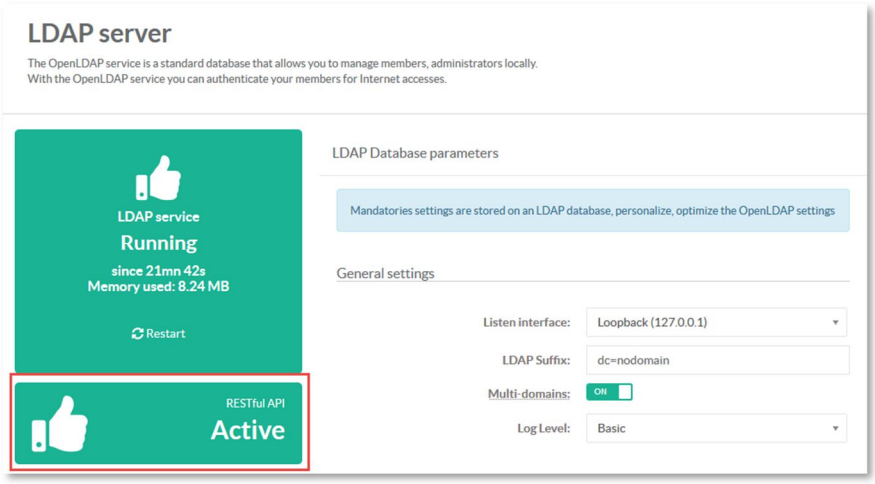


RESTful API for managing LDAP users.

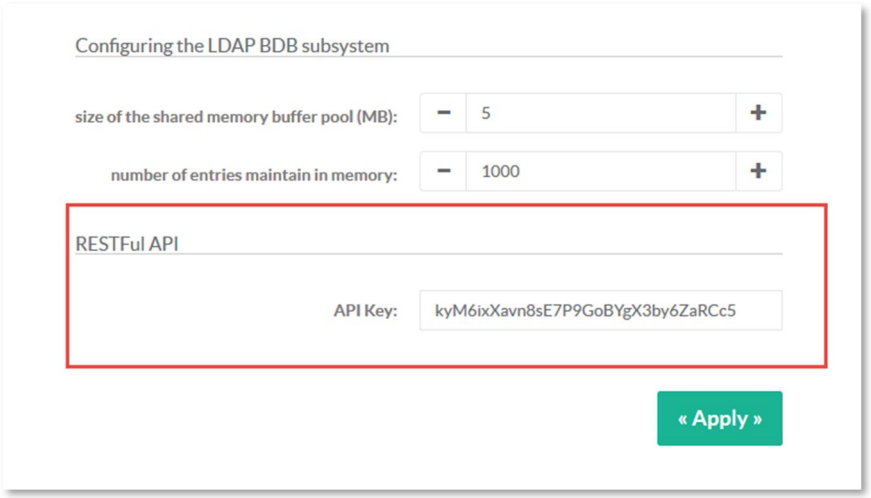
Artica provides RESTful API in order to manage LDAP members (THE REST API SERVICE IS AVAILABLE WITH ENTERPRISE EDITION).
To manage members and groups with REST API, you need to enable the feature thought features service



After installing the feature, on the left menu, use "**Databases/LDAP server**"
You will see that the Restful API is active in the satus.



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



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 sent to indicate 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){
   echo "Error $errno\n".curl_error($ch)."\n";
   curl_close($ch);
   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/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
```

Y

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

```
POST: https://server:9000/api/rest/ldap/organization/MyCompany/groupJKUIs/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){
    echo "Error $errno\n".curl_error($ch)."\n";
    curl_close($ch);
    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:

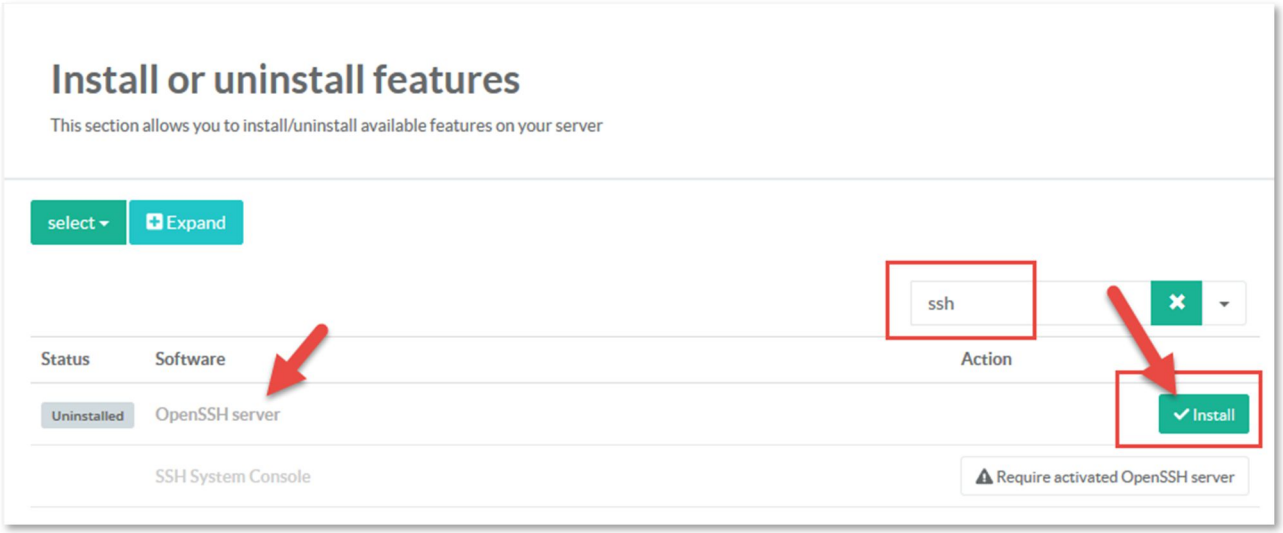
```
    "uid"=>"Jhon.doo",
    "DisplayName"=>"Jhon doo Mhain",
    "givenName"=>"Jhon",
    "name"=>"doo Mhain",
    "password"=>"123456"
```

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.

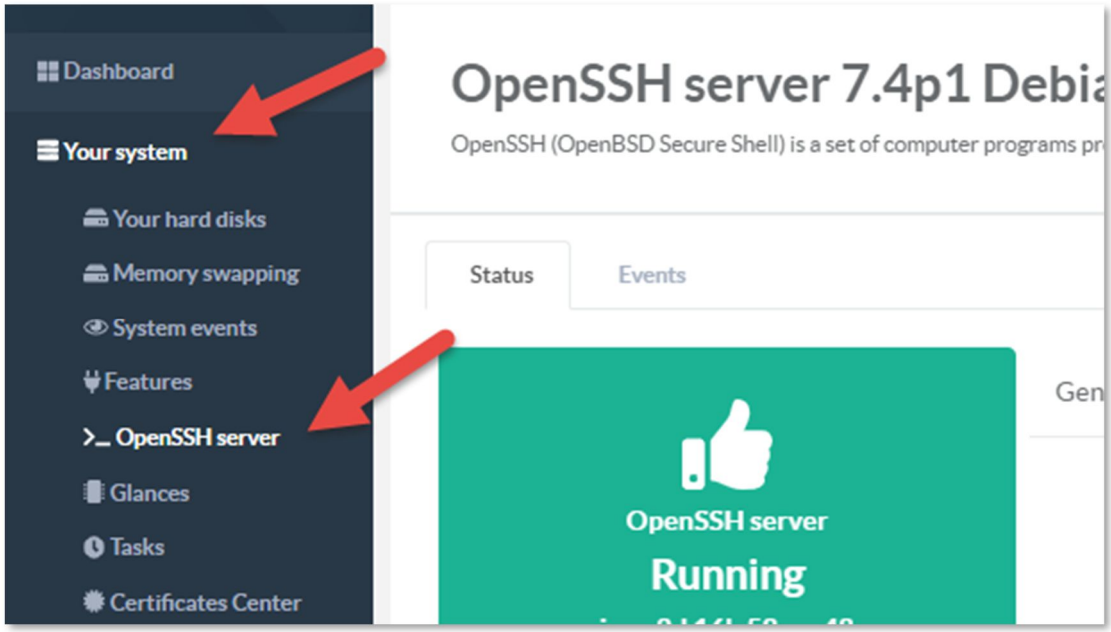
In the search box, type "ssh" and click on the button "Install" under the "OpenSSH server" row.



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

SSH SERVER SECTION

The SSH server section can be found in the left menu "Your System" and "OpenSSH server.

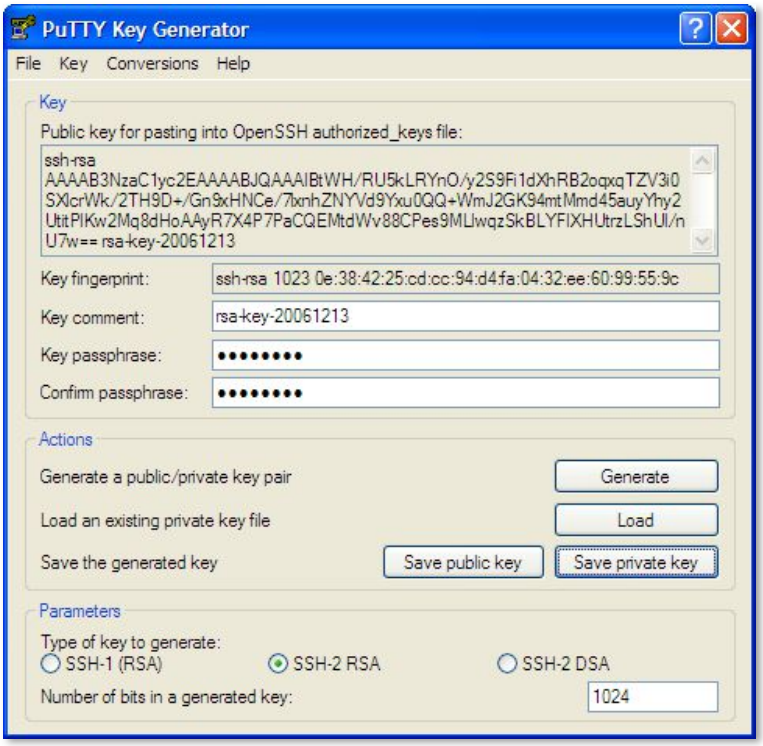


PUBLIC KEY AUTHENTICATION WITH PUTTY

These instructions apply to the PuTTY client on Windows and Artica.
It allows to authenticate your SSH session on the Artica server with a public Key.

Download or execute the puttygen.exe (available here: https://the.earth.li/~sgtatham/putty/latest/w64/puttygen.exe)

Click the **Generate** button.
You will be prompted to move the mouse over the blank area to generate some randomness.
Do so. Shortly thereafter, the program will generate the key and display the result



After keys have been generated.

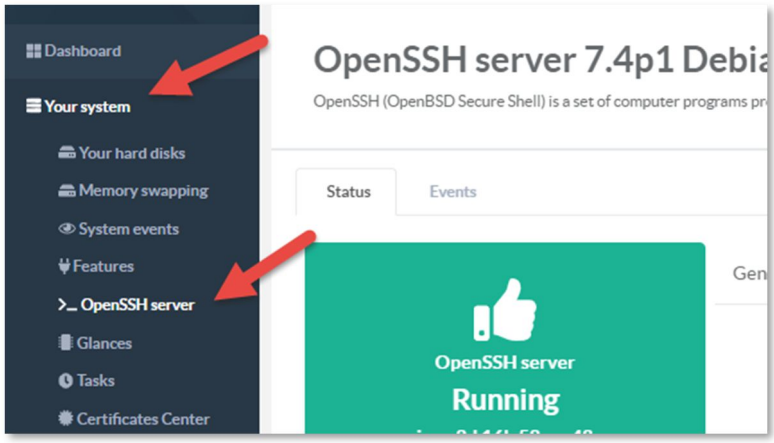
Enter a passphrase in the "**Key passphrase**" and "**Confirm passphrase**" boxes.

Your CCID password makes a good choice since you have probably already committed it to memory and it has withstood password cracking tests.

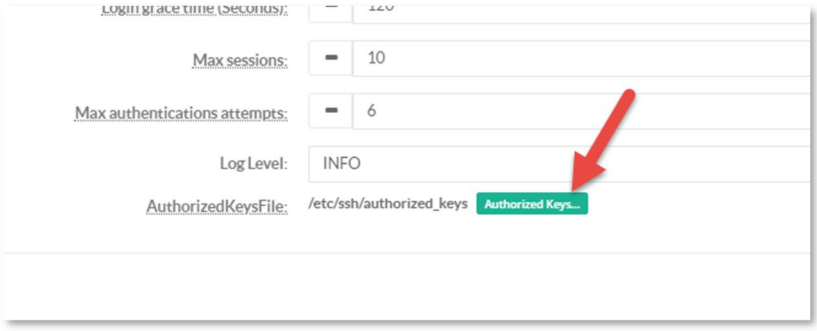
Select *all* of the text in the box labeled "**Public key for pasting into OpenSSH authorized_keys file**" (near the top of the window) by dragging the cursor. Right-click over the selection and choose Copy.

Finally, click the "**Save private key**" button to save the private key to a file

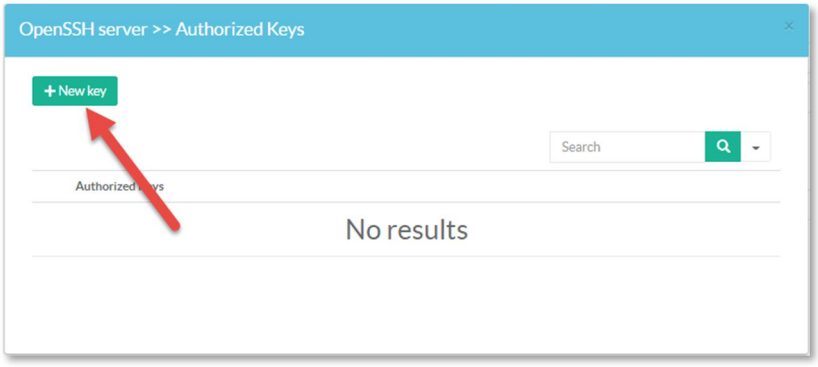
On the Artica server, on the left menu, choose "**Your System**" and "**OpenSSH server**"



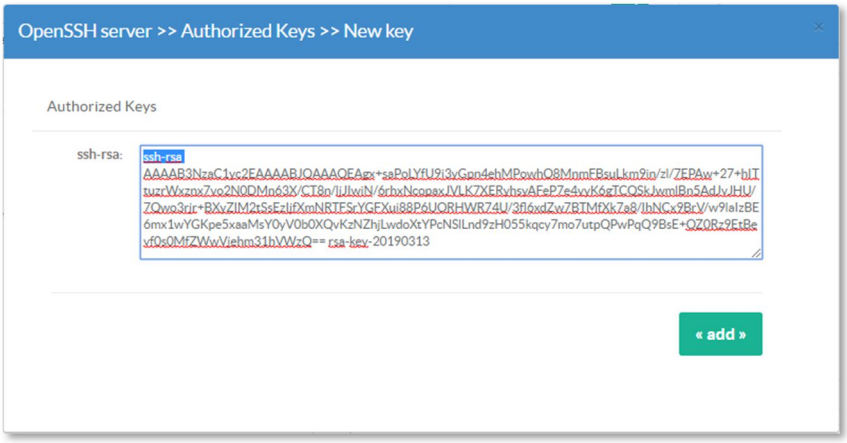
Down to the "**Authorized Key..**" button and click on it.



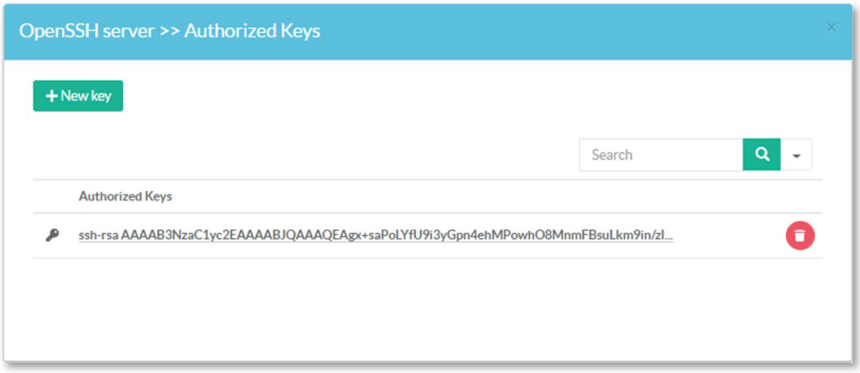
Click on the "**New key**" button



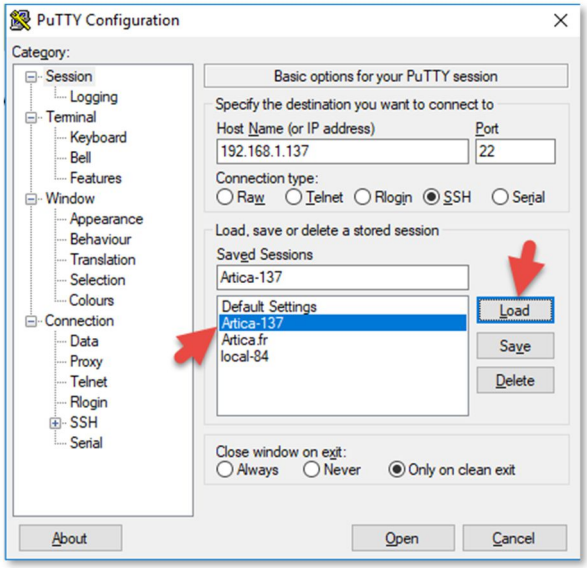
Paste in the text area the full content generated in the "**Public key for pasting into OpenSSH authorized_keys file"** puttygen.exe program
Click on **Add** button



Key is added in the table.

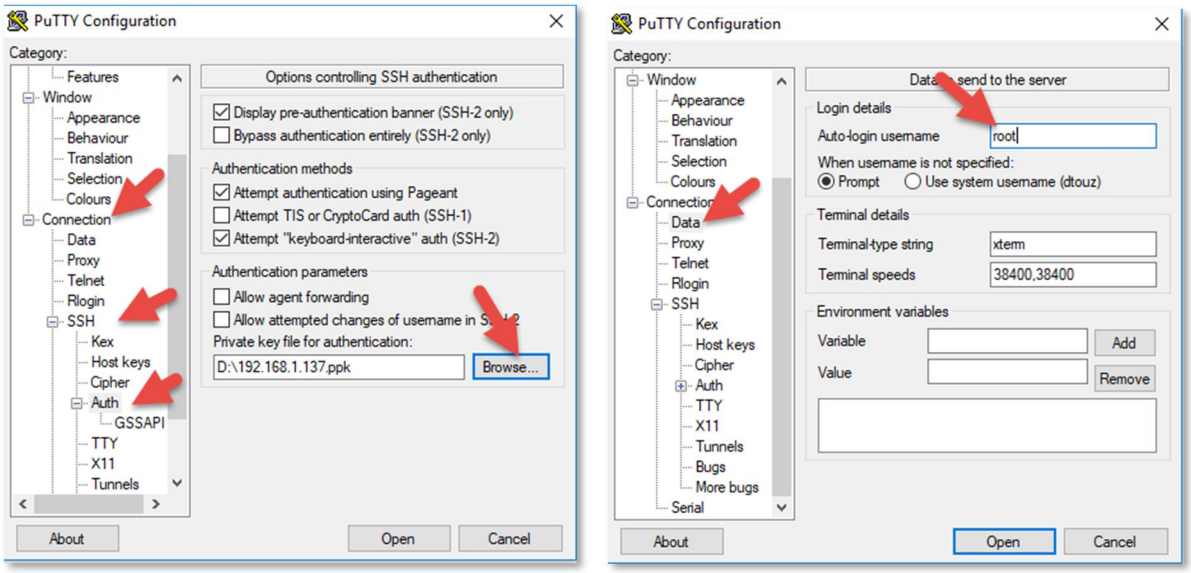


Execute the putty.exe
Basic public key authentication is enabled for a particular session in the Connection > SSH > Auth window.
You must load the session profile before configuring the Auth window



Go to **Connection > SSH > Auth window**.

Browse to select *.ppk in the "Private key file for authentication" text box.
Be sure to go back to the Session window and click Save to update the profile.
The session will use public key authentication
You can also add the user in **Connection > Data > Auto-login username** in order to not be prompted for the Login name**.**

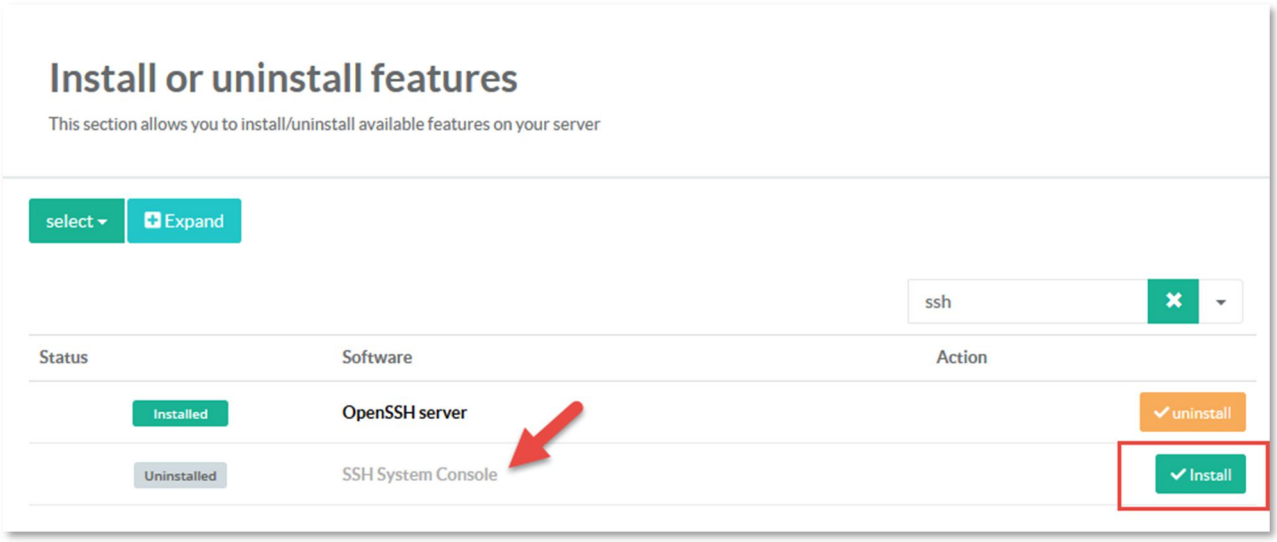


How to replicate Public keys on severals Artica servers ?

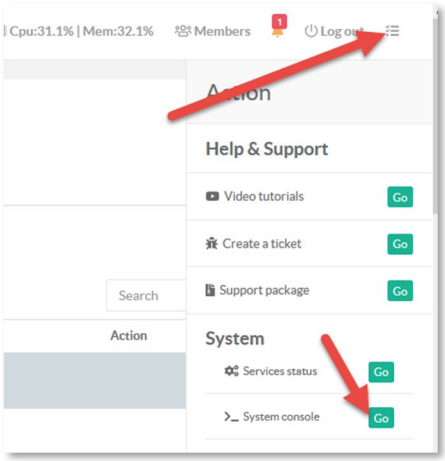
Simply replace the "**/home/artica/SQLITE/sshd.db**" on targets Artica servers and perform a "**/etc/init.d/ssh reload**"

THE SSH WEB CONSOLE

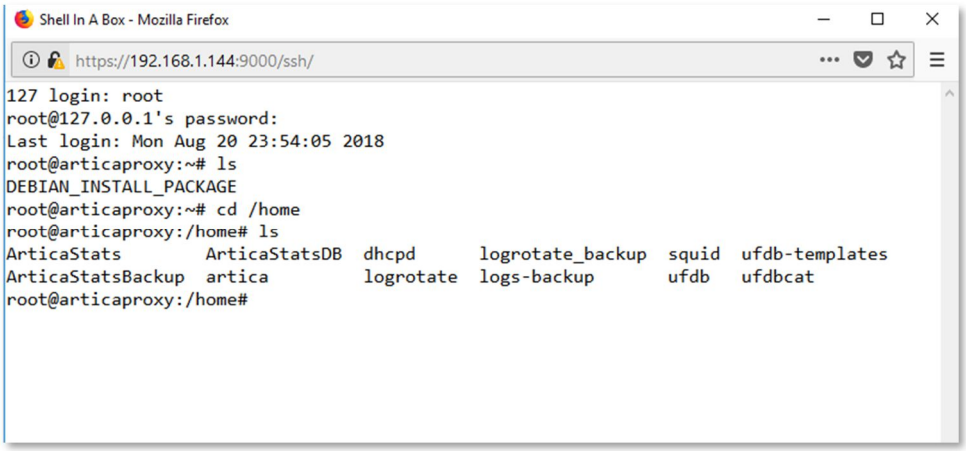
If you want to enter into the system using SSH web console, after installing the OpenSSH server, install the "**SSH system console**".



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

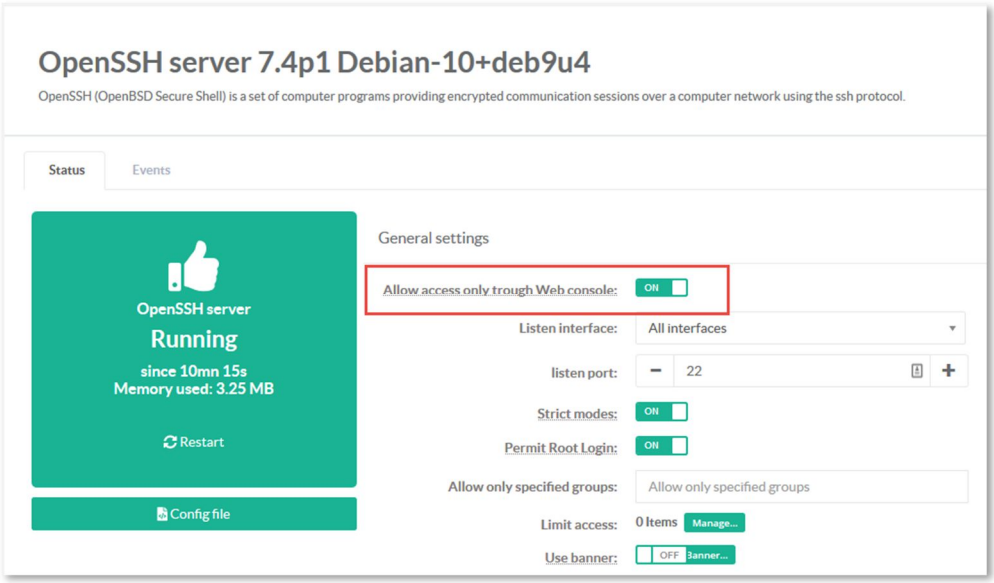


This will open a web console that simulates a connection using SSH client.



Restrict the SSH access to the Web console.

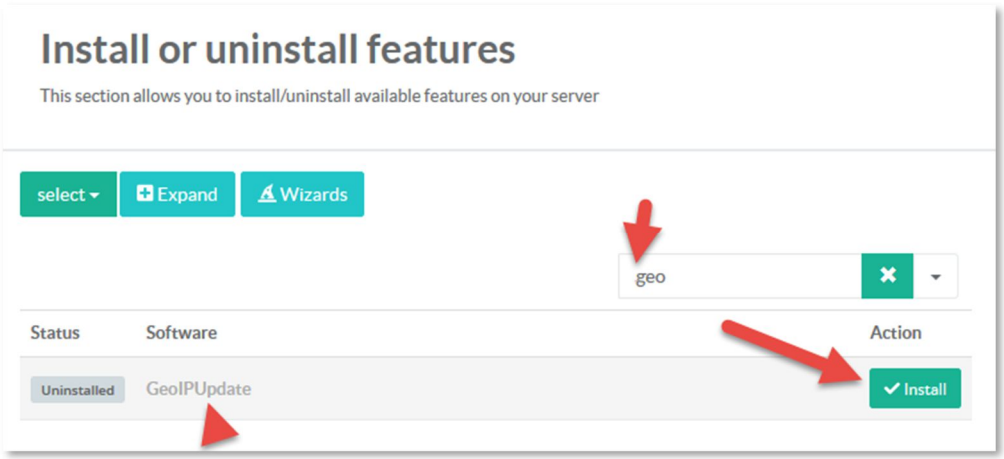
If you did not want to open the TCP 22 port and keep access to the Artica system using only the Web console, on the left pan, choose "**Your System**" and "**OpenSSH server**" menu.
Under the "**General settings**" section, turn on the "**Allow access only through Web console**" and click on "**Apply**"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



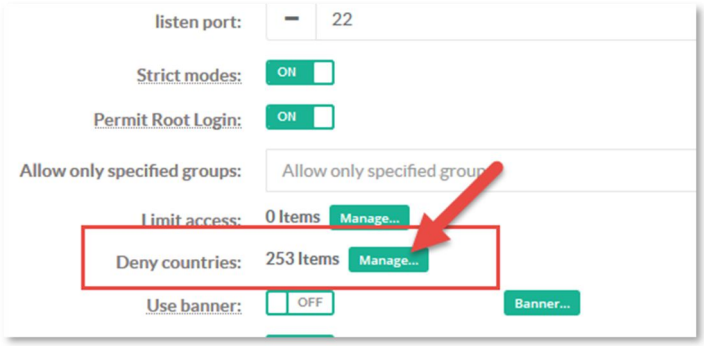
This option will force the OpenSSH server to run only on the loop back interface for the SSH Web console.
Access externally to the SSH server will not be possible.

Restrict Access according Geo-Localization of remote addresses.

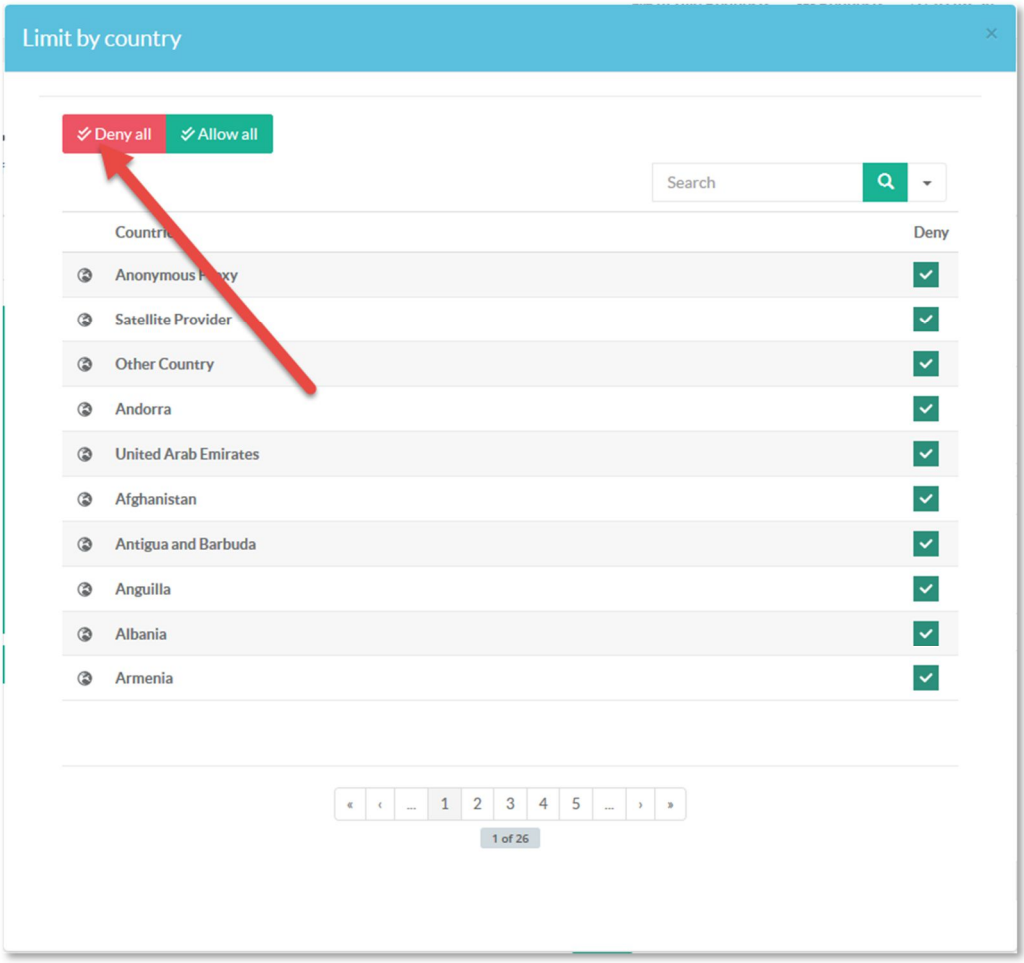
You can enable "**Deny Countries**" inside the OpenSSH section.
To make this feature working, you need to use the latest Debian 10 operating system and enable the **GeoIPUpdate** under features



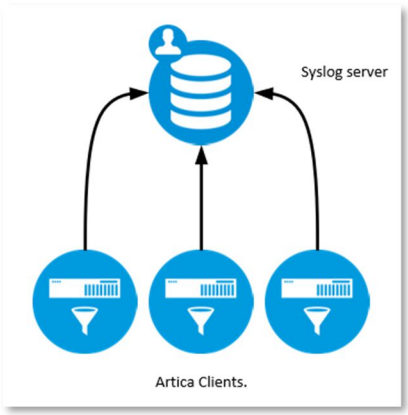
On the OpenSSH section, click on the button "**Manage**" under "**Deny countries**"



Click on the button "Deny all" in order to deny all countries and uncheck only countries you want to allow.



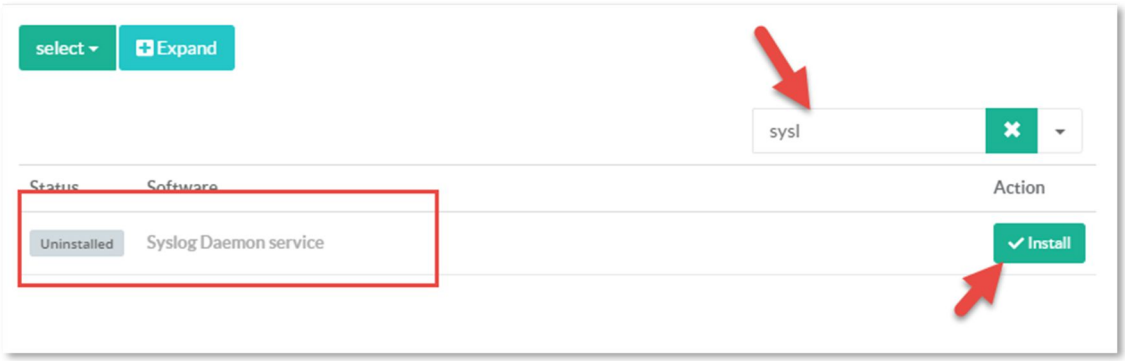
THE SYSLOG SERVICE / LOG SERVER



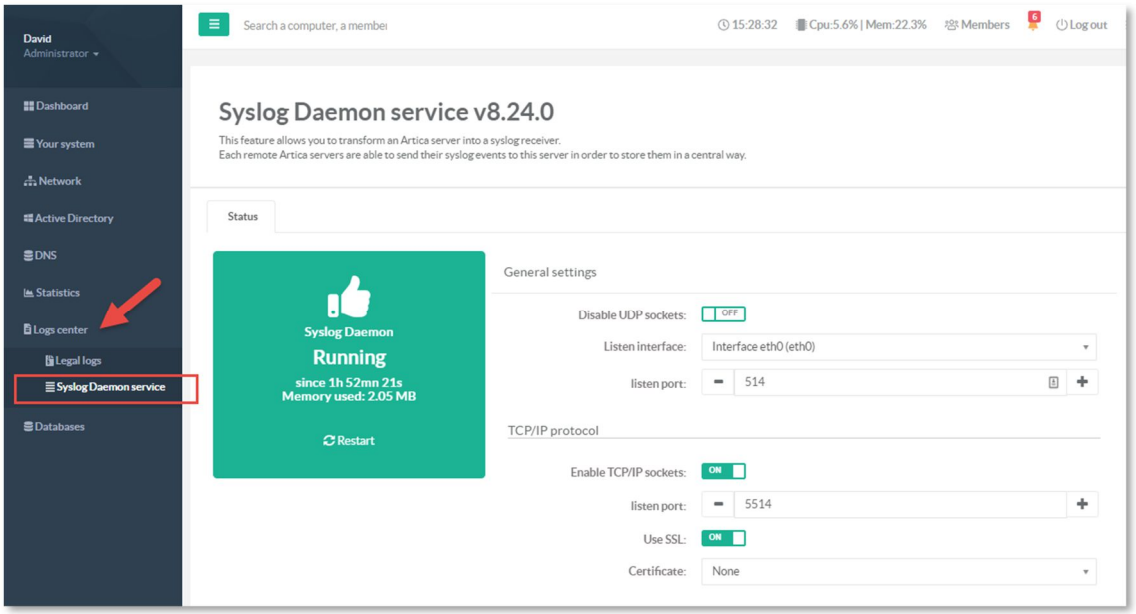
The syslog service is able to receive events from any Linux/Artica servers in order to store them and perform a central syslog server.
By default, Artica use the local syslog service in order to store local events.
Enable this service allows you to transform your Artica server into a syslog receiver.

INSTALL THE SYSLOG FEATURE

- Go into the feature section
- On the search field, type "**syslog**"
- Click on Install button on the **syslog Daemon service** row



- By default, the syslog service wait data on the 514 UDP port.
- You can manage the syslog service by using the left menu "**Logs center**" and "**Syslog Daemon service**"



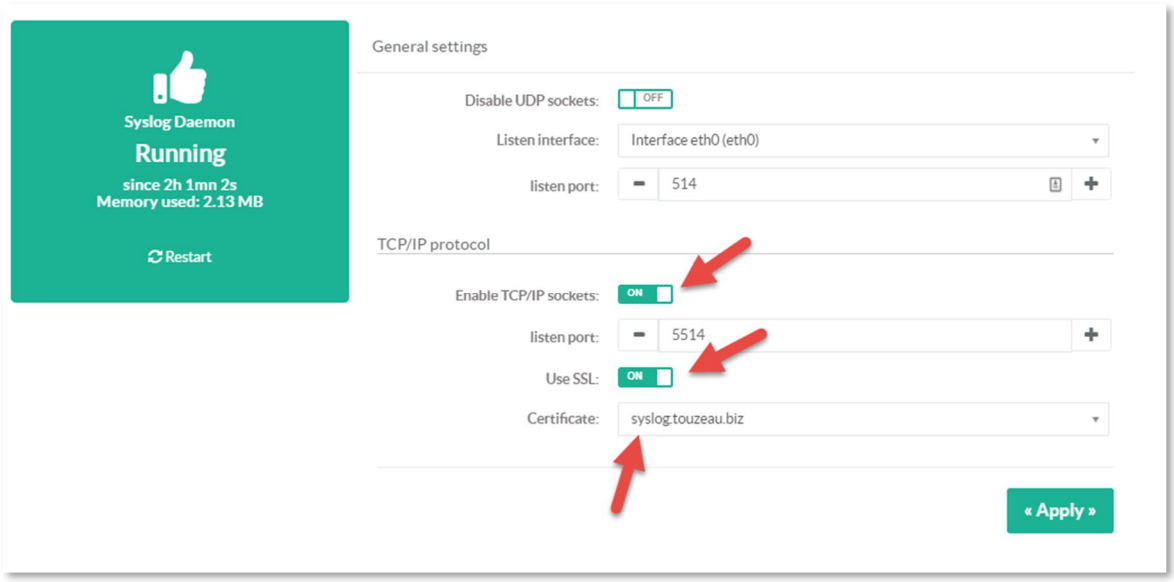
SECURING YOUR SYSLOG SERVER WITH TLS (SSL)

You should want to enable encryption on the syslog stream since private information, including credentials, could be getting passed from client to server in the logs. In this document, we will be using self-signed certificates, including a self-generated CA certificate

- Go to **System** / **certificates center** and generate a new self-signed certificate.

On the syslog service parameters:

- Turn on the Enable TCP/IP sockets option.
- Define the port in the listen port field
- Turn ON "**Use SSL**" option
- On the drop-down list, choose the generated self-signed certificate.
- Click on **Apply**
-



DNS SERVICES.

Artica offer 3 main services for providing DNS services.

1. **The Load-Balancing DNS service:**

   It is a DNS service that is able to cache DNS requests and forward them to a pool of DNS server in load-balancing mode.
   This DNS service can use ACIs to switch DNS requests to a specific pool according to a group source IP addresses and/or a group of destination domains

2. **The PowerDNS system:**

   Is a complete DNS service used by many ISPs and claim to be a Public DNS server.

3. **The DNS Cache service:**

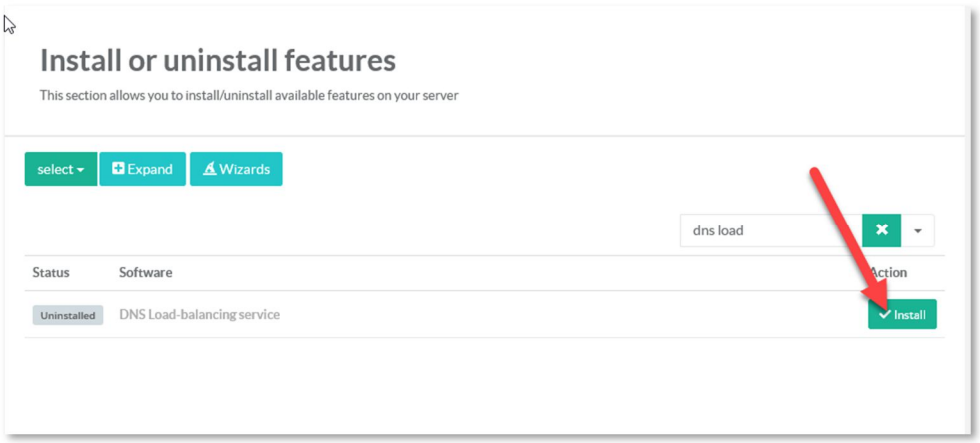
   Is a simpler DNS service used to cache DNS items.
   It provides DNS filtering features and DNS crypt filtering feature.
   It is designed to be an Internal DNS as a real friend of a Windows DNS service.

THE DNS LOAD-BALACING SERVICE

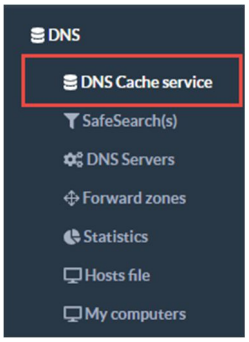
The DNS Load-balancing is a DNS service that is able to cache DNS requests and forward them to a pool of DNS server in load-balancing mode.
This DNS service can use ACIs to switch DNS requests to a specific pool according to a group source IP addresses and/or a group of destination domains

Install the DNS Load-balancing service

1. On the left menu, click on **Your System / Features**
2. On the search box, type "**dns load**"
3. Click on **Install** button
4.



THE DNS CACHE SERVICE



The DNS Cache service (aka Unbound)) is used to accelerates DNS answers for your Artica server or your internal network. It is a very secure validating, recursive, and caching DNS server.
It uses a strong cache system and a prefetch feature in order to prepare DNS answers.
The DNS Cache service is installed and enabled by default when installing Artica for the first time.

The DNS cache service can be extended with the DNS Filter feature.
With this filter feature you can fake resolutions of unwanted sites according categories.

Enable logging.

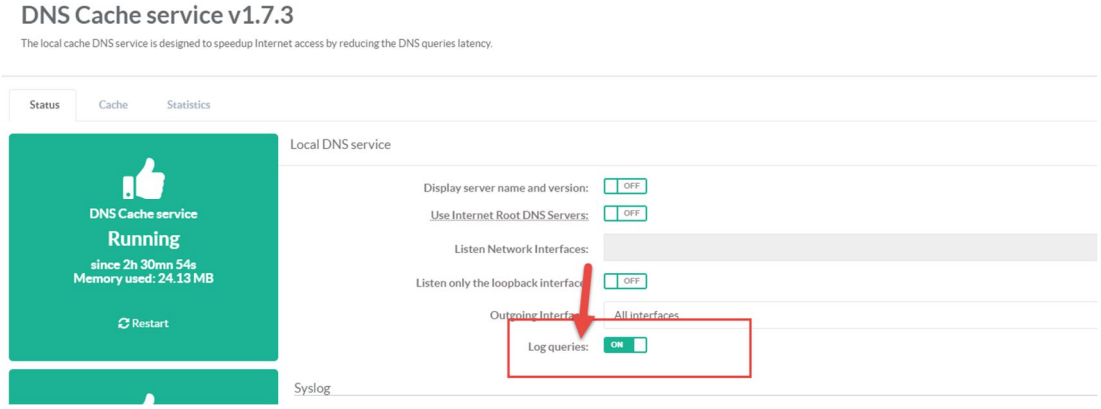
By default, queries are not logged, if you want to get an history of all DNS queries you have 2 ways.

1. Write to a local file.
2. Send queries to a syslog daemon.

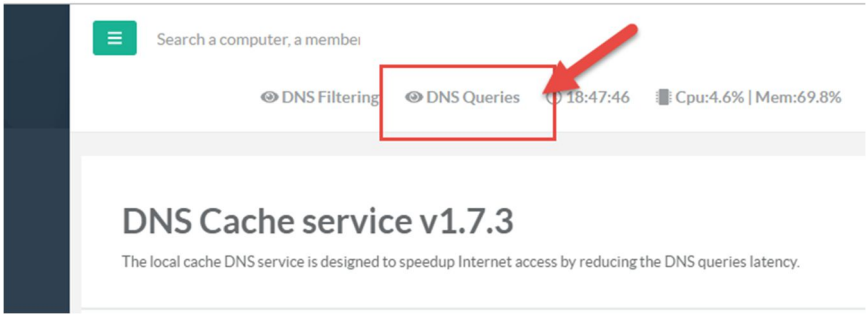
In both ways (log to a file and send to syslog) events will be stored in /var/log/unbound.log file.

Write to a local file

On the DNS Cache service main section, turn ON the "log queries" option.
When using this option, Artica will be able to keep old logs and to store them according to the "Legal logs" feature.



This option will display a new top menu called “DNS Queries”. It allows you to search events and display the last DNS queries from your Network.



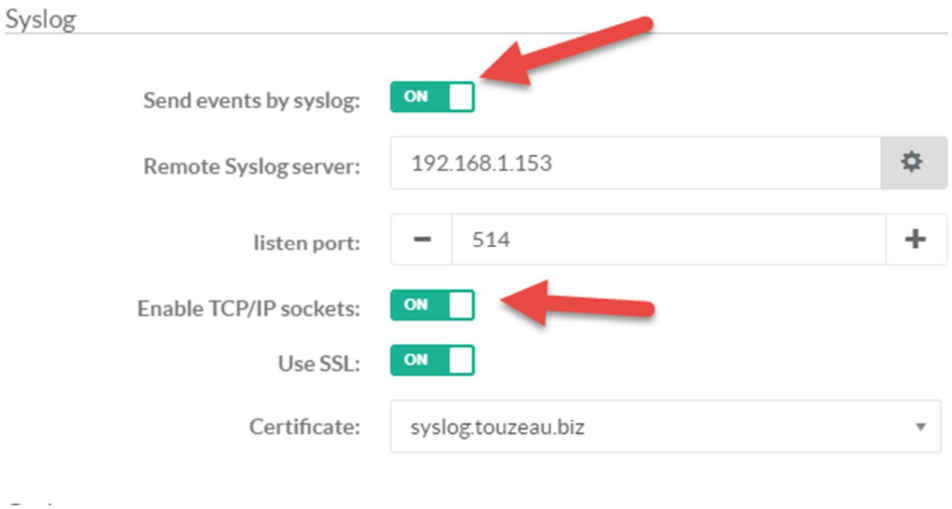
Send to a syslog server.

If you have a valid corporate license, you are able to send DNS queries to a Syslog server.

Turn on the **"Send events by Syslog**" option
Set the IP address and the UDP port of the remote Syslog server.
If you turn on the "**Enable TCP/IP**" sockets option, events will be sent using TCP instead of UDP.
If TCP/IP is enabled, you can use SSL to send events by enabling the **Use SSL** option.

In this case, select the certificate from the **certificate center** that stores the **Certificate Authority** of your **remote Syslog server**.

If you only need to store log on the remote Syslog server and not on the local server, turn on the "**Do not store events locally**" option.

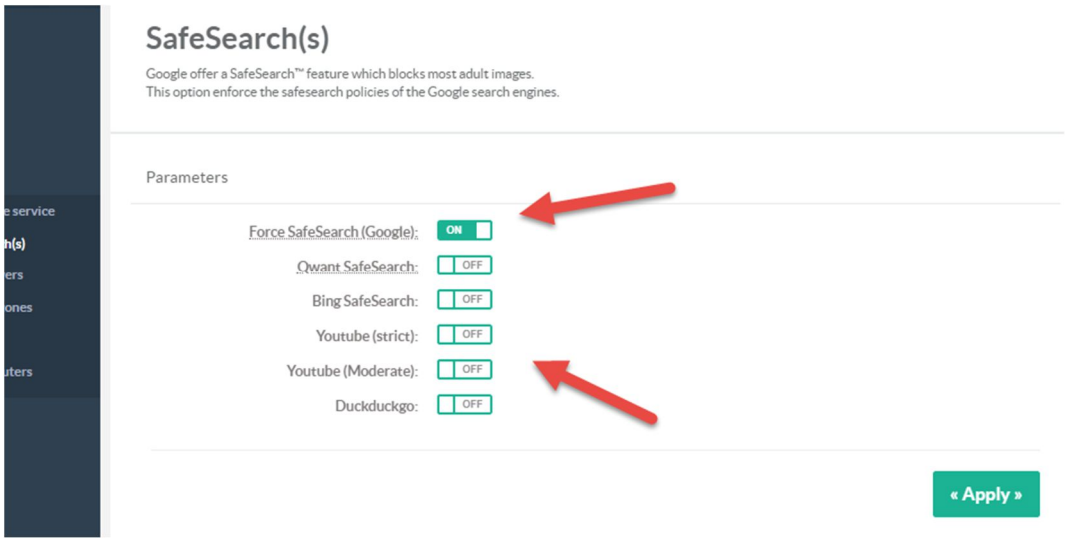


SafeSearch(s)

If you use the DNS cache service, you can enable SafeSearch(s) on the major Web search services. (need a valid Corporate License)
Currently Artica is able to enable SafeSearch for **Google, Qwant, Bing, YouTube, Duckduckgo**
SafeSearch(s) is in the left menu under DNS/SafeSearch(s).
SafeSearch(s) is designed to modify the DNS answer of **your workstations** (if you plan to use Artica as the Internet DNS service) or **your proxy service** if the proxy uses the DNS cache service to resolve the Internet.

The modified DNS answers force search engines to ban any porn, hacking, malware, suspicious indexed Web sites.

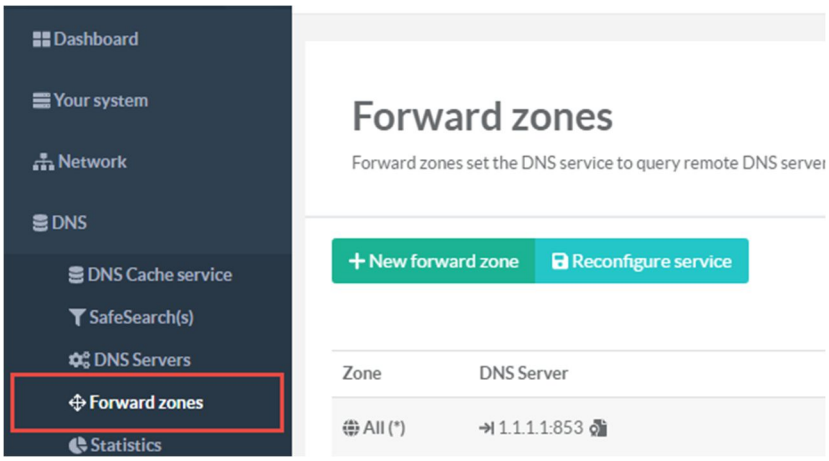
On the main section, choose the Search engine you want to filter and click on **Apply**



Reverse lookup private zone

By default, the DNS Cache service did not perform reverse lookup for your internal network.
To add the reverse lookup on the DNS cache service:

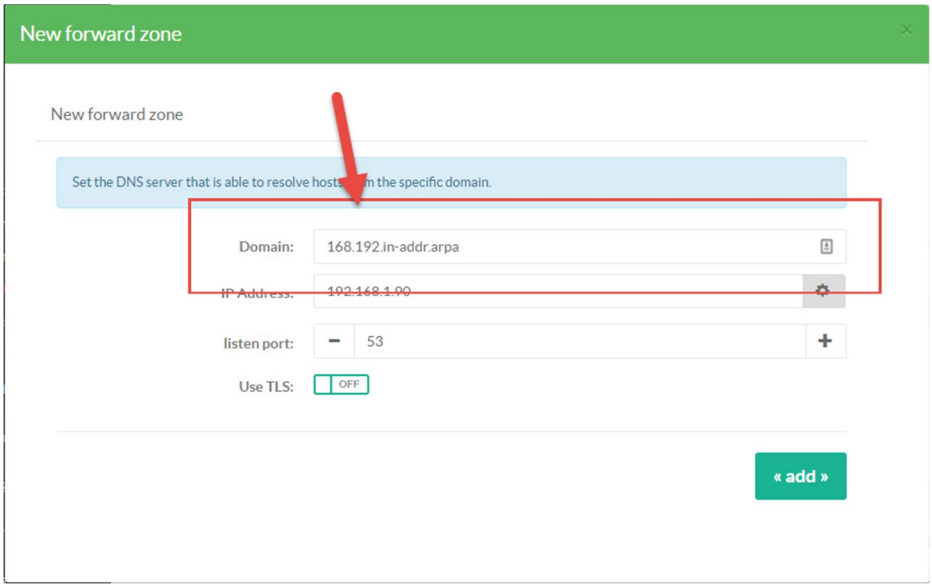
Go into the **Forward zones** section
Click on **New forward zone** button.



Add the inversed network mask with the in-addr.arpa domain.

For examples:

If your network is 192.168.0.0/16, add 168.192.in-addr.arpa
If your network is 192.168.1.0/24 add 1.168.192.in-addr.arpa
If your network is 192.168.2.0/24 add 2.168.192.in-addr.arpa
If your network is 10.10.0.0/16, add 10.10.in-addr.arpa



Set the remote server and port that should receive the reverse DNS lookup query
Click on "**Add**" button.
Click on "**Reconfigure service**" button

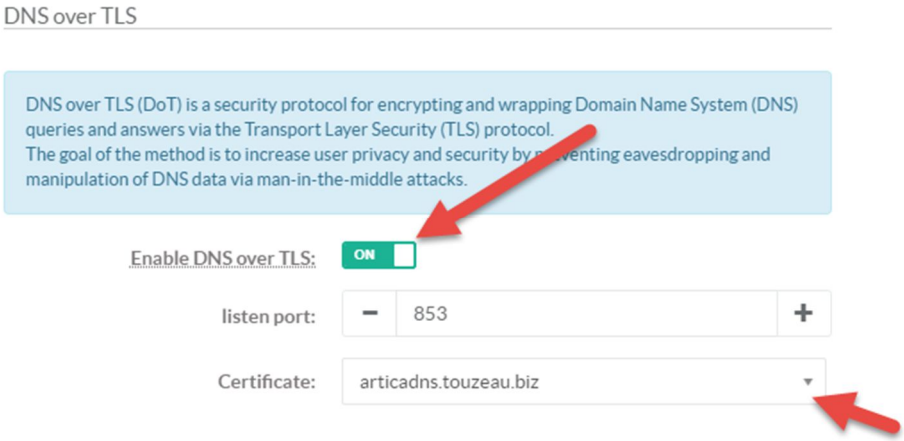
Secure DNS over TLS

By default, DNS is sent over a plaintext connection.
DNS Over TLS is one way to send DNS queries over an encrypted connection.
This feature adds a DNS over TLS option to your DNS Cache service.
For example, Cloudflare supports DNS over TLS on 1.1.1.1 and 1.0.0.1 on port 853

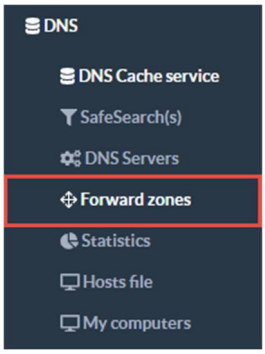
Create a DNS over TLS service. (Server mode)

1) **Create a certificate**:
Go into the certificate center and add/create your certificate.

2) On the main settings; Enable the **DNS over TLS** checkbox and select the generated **certificate**.



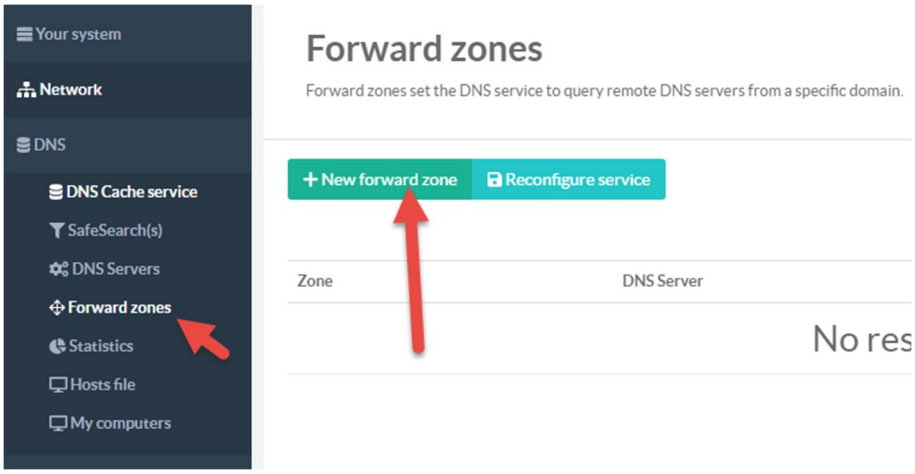
Query DNS over TLS servers.



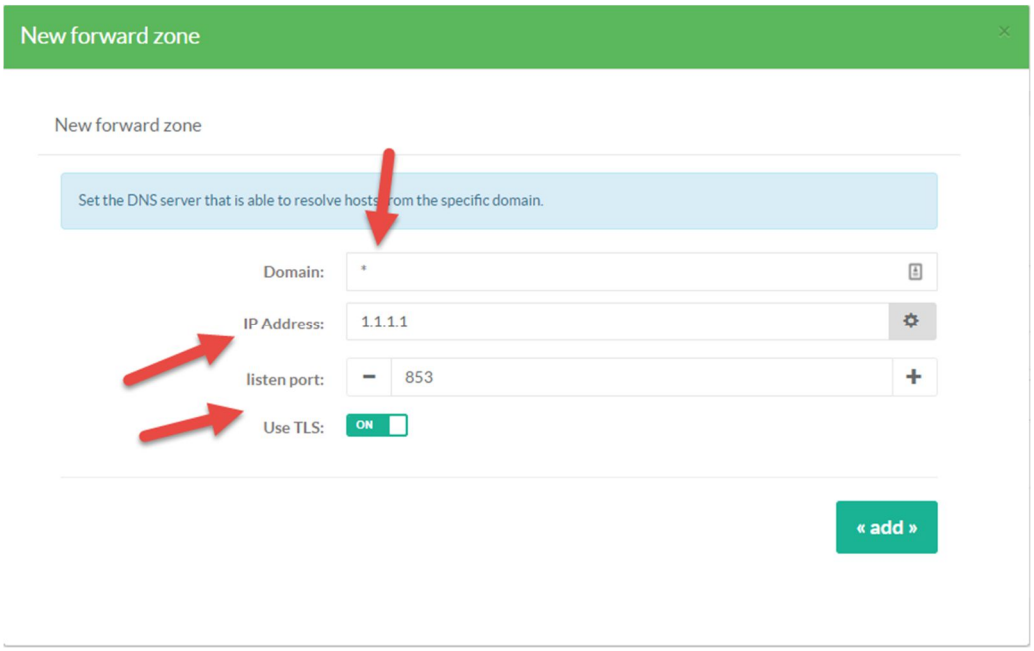
Some free public ISP offers DNS Over TLS public DNS:

- Quad9: 9.9.9.9:853 or 9.9.9.10:583
- Cloudflare: :853 or 1.0.0.1:853
- Google: 8.8.8.8:853 or 8.8.4.4:853
- CleanBrowsing Security Filter: 185.228.168.9:853 and 185.228.169.9:853
- CleanBrowsing Family Filter: 185.228.168.168:853 and 185.228.169.168:853
- CleanBrowsing Adult Filter: 185.228.168.10:853 and 185.228.169.11:853
- Adguard defaiult: 176.10 176.103.130.132 or 176.103.130.134 3.130.130 or 176.103.130.131
- Adguard Family: 176.103.130.132 or 176.103.130.134

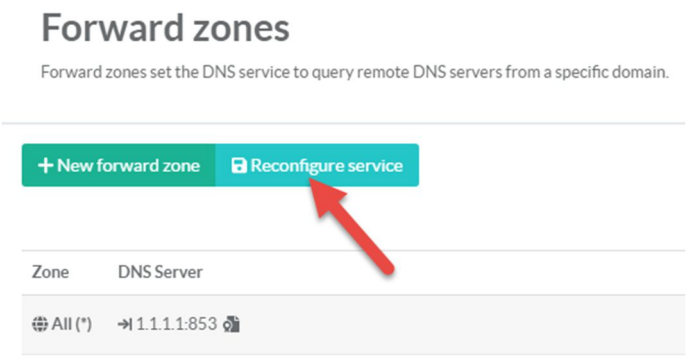
To use these IP address, on the left menu, get **DNS/Forward zones**.
Click on "**New forward zone**"



- Set the domain as "star" "*"
- Set the **IP address** and **port** of the DNS Over TLS server
- Turn on the "**Use TLS**" option
- Click on **Add** button.



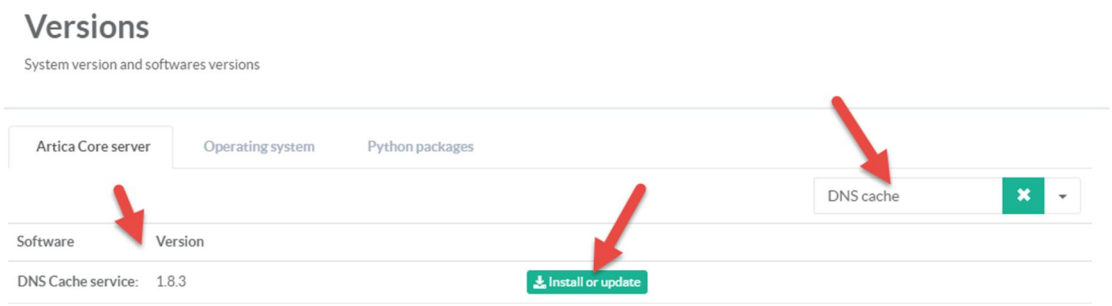
- Click on **reconfigure service** button in order to make rules in production mode.



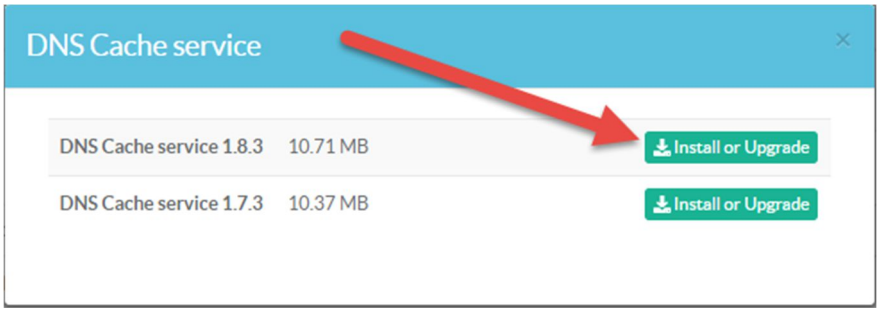
Update the DNS Cache service Software

Regularly, Artica team provide new releases of the DNS Cache service.
To update the Cache DNS Core software, on the left menu, click on **Your System** and **Versions**

- On the search field, type "DNS Cache"
- You can see the current version in production mode.
- Click on the "Install or update" button.



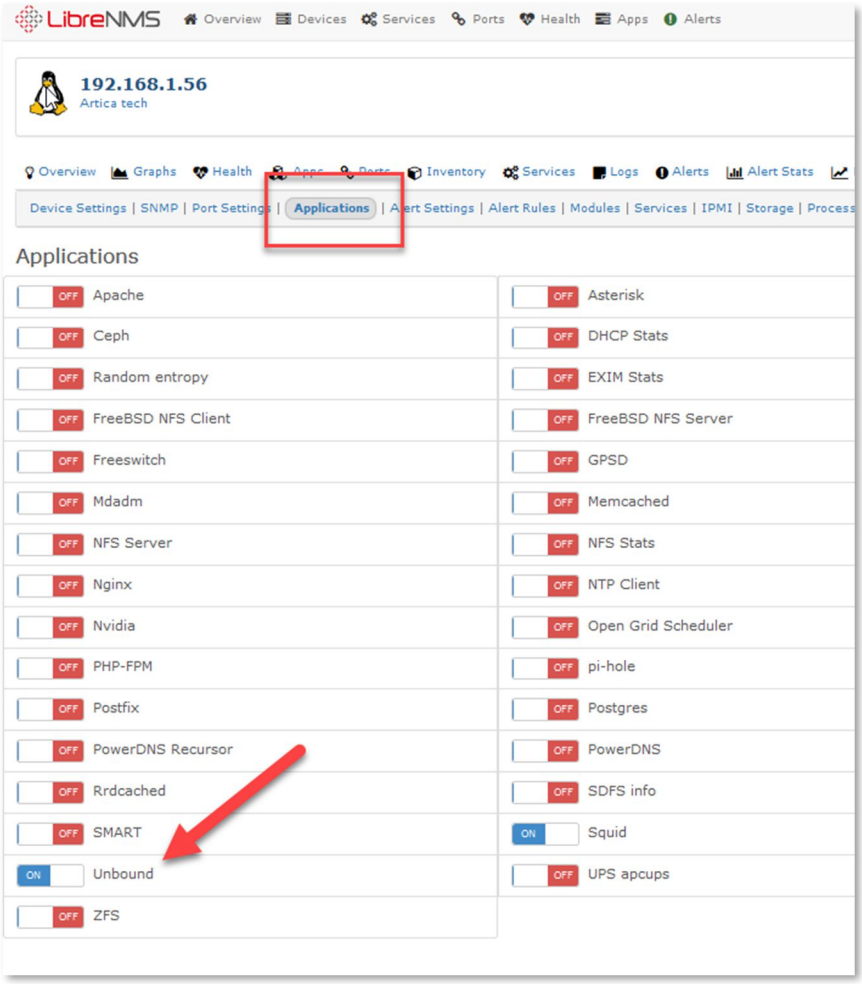
- A new screen lists all available versions.
- Click on the button "**Install or Upgrade**" on the desired version



Monitoring

The DNS Cache service can be monitored using SNMP as it have an extension named “unbound”.
If the SNMP service is installed with Artica feature, this extension is automatically added.

If you using **LibreNMS**, open the node settings and got o Applications, turn to on the **Unbound** checkbox option.



,

POWERDNS

The PowerDNS is a strong DNS server. It is used by many ISPs.
It uses MySQL database engine as backend and provide REST API in order to be fully controlled.

Installing the PowerDNS system.

To understand, the PowerDNS system use 3 components:

- The MySQL database: used to store records.
- The PowerDNS system: used to answer queries only stored in the MySQL database.
- The PowerDNS recursor: used to forward queries to external resolvers if domains are not stored in the MySQL database.

Go into the **features** section and install first the **MySQL database**, then, install the **Power DNS system** in order to get a local DNS system.

If you want your Artica server as a real DNS system (means resolve foreign domains) ,
you have to install the PowerDNS recursor.

Enable the RESTful API.

The RESTful API allows you to send commands and get status of the PowerDNS system using REST protocol.
The PowerDNS Authoritative Server features exposes a JSON/REST API.
This API allows for controlling several functions, reading statistics and modifying zone content, metadata and DNSSEC key material

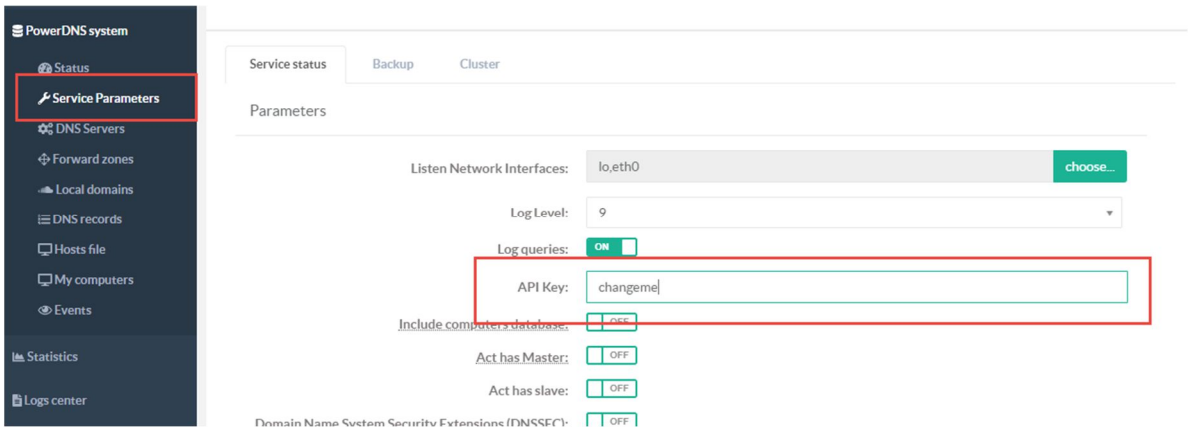
To Enable the ReSTful API, go into the **features** section and install the **RESTful API for PowerDNS**

After installing, you should open the page

```
https://192.168.1.1:9000/pdnsapi/
```

This page allows you to see statistics of your DNS server.

- Select the **PowerDNS system** and **Service parameters** on the left menu.
- Set a passphrase in the **API Key** field.



With the passphrase you need to authenticate the REST by adding the X-API-Key request header:

```
curl -v -H 'X-API-Key: changeme' https://192.168.1.1:9000/pdnsapi/api/v1/servers/localhost | jq .
curl -v -H 'X-API-Key: changeme' https://192.168.1.1:9000/pdnsapi/api/v1/servers/localhost/zones | jq
```

For the full list of REST commands, see the documentation here: https://doc.powerdns.com/authoritative/http-api/index.html#

Reverse DNS

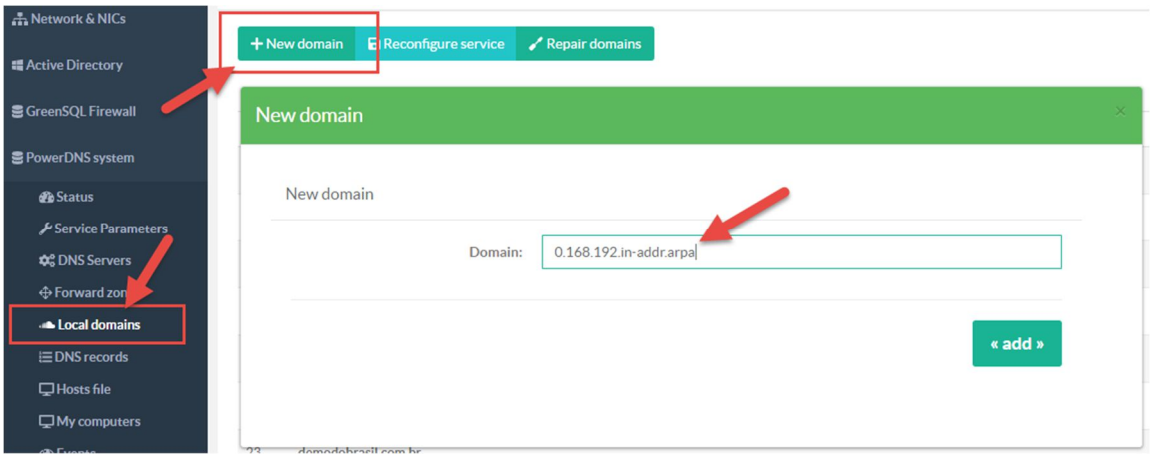
Creating a reverse DNS domain

For the following example we shall assume that we are configuring reverse DNS for an internal network using IP addresses in the 192.168.0.0/24 range. With this in mind the first task is to create an entry in the Internal domains.

Select the "**Local domains**" section and create a new domain.

192.168.0.0/24 will be inversed to 0.168.192 and the **in-addr.arpa** domain.(matches 192.168.0.1 to 192.168.0.255)
Examples:

- ✓ **10.in-addr.arpa** for 10.0.0.0/8
- ✓ **16.172.in-addr.arpa** for 172.16.0.0/12
- ✓ **168.192.in-addr.arpa** for 192.168.0.0/16



Creating SOA and NS records for a reverse DNS domain

In the same way that a forward zone requires an SOA record to indicate that this domain name server has authority to respond on behalf of a zone a reverse zone requires a very similar record.
When creating a new domain, Artica creates automatically the associated SOA but you need to personalize your SOA*

Select the "**DNS records section**" and search your **SOA** entry.

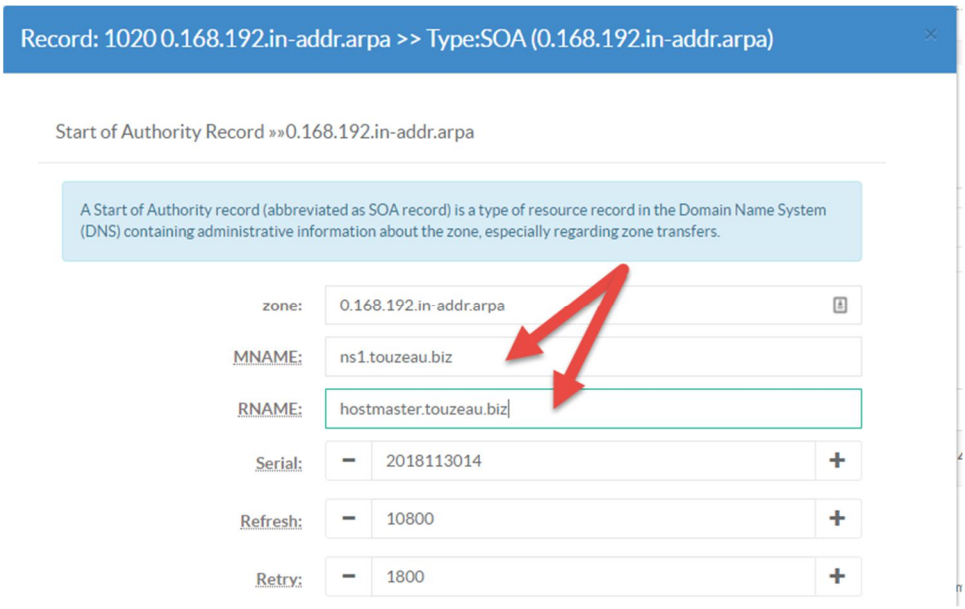
The search engine uses a defined syntax
You can search using "*" character and "**type**" to select the family of the record,

For example:

```
0.168.* type soa
0.168.* type=soa
0.168.* and type soa
0.168.192* type soa
0.168.192* where type soa
```

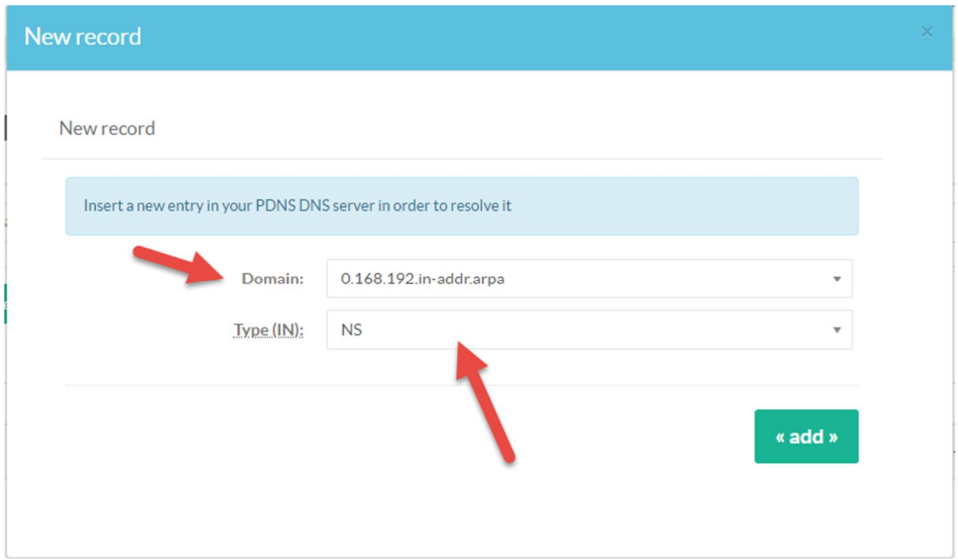
After found the record, click on the link

Modify the MNAME (NS record) and the RNAME with the main domain used by your "A" records (in our case our domain is "Touzeau.biz")

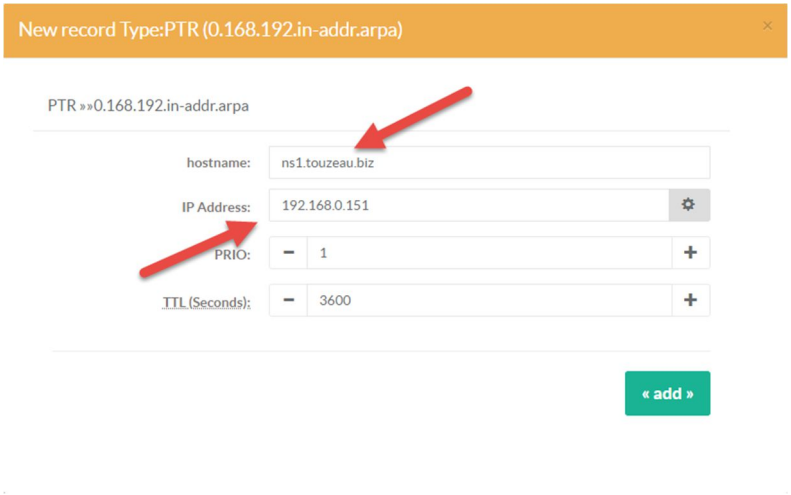


- ✓ The MNAME (NS record) needs a record.
  This record is primarily used to delegate reverse zones to other name servers although every reverse zone, delegated or not, still requires one.

- ✓ On the DNS Records section create a new record
- ✓ In the new record form, choose your **reverse DNS domain** and select **NS** in the type drop-down field.

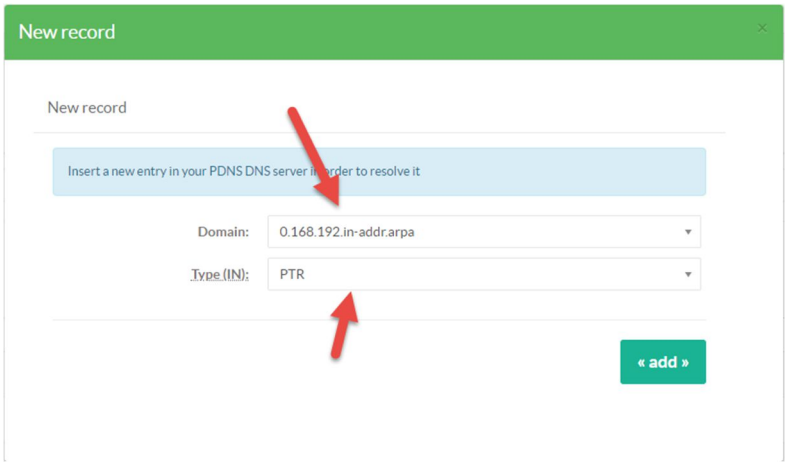


In the value field, set the MNAME you have defined in the SOA for the reverse domain.

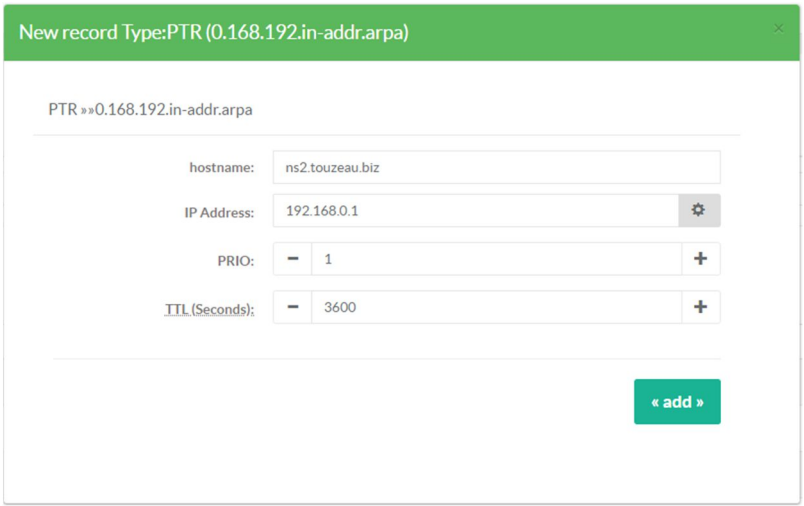


Creating PTR records for a reverse DNS domain

- ✓ In the new record form, choose your **reverse DNS domain** and select **PTR** in the type drop-down field and click on Add button



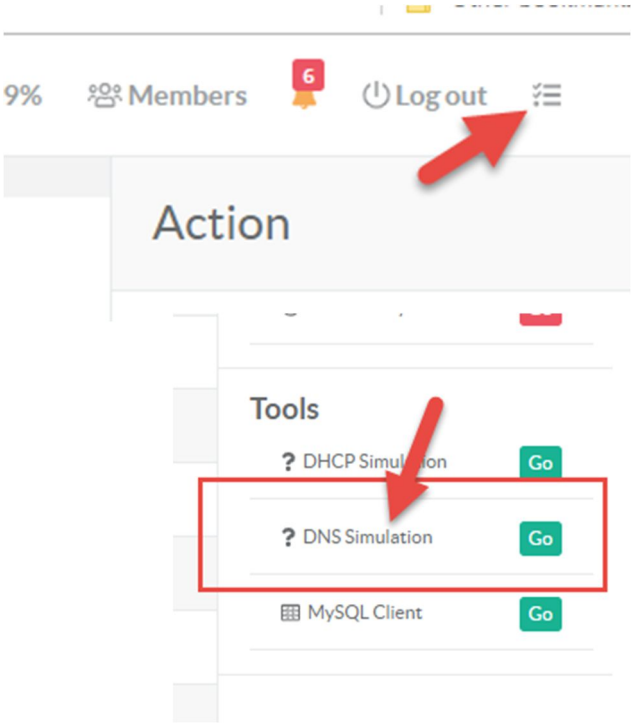
- ✓ In the hostname field, set the fully qualified name of the host you want the PTR to be resolved.
- ✓ In the IP address field, set the IP address of your hostname.
- ✓ Artica will turn your IP address to a valid PTR format.
- ✓



Testing our configuration

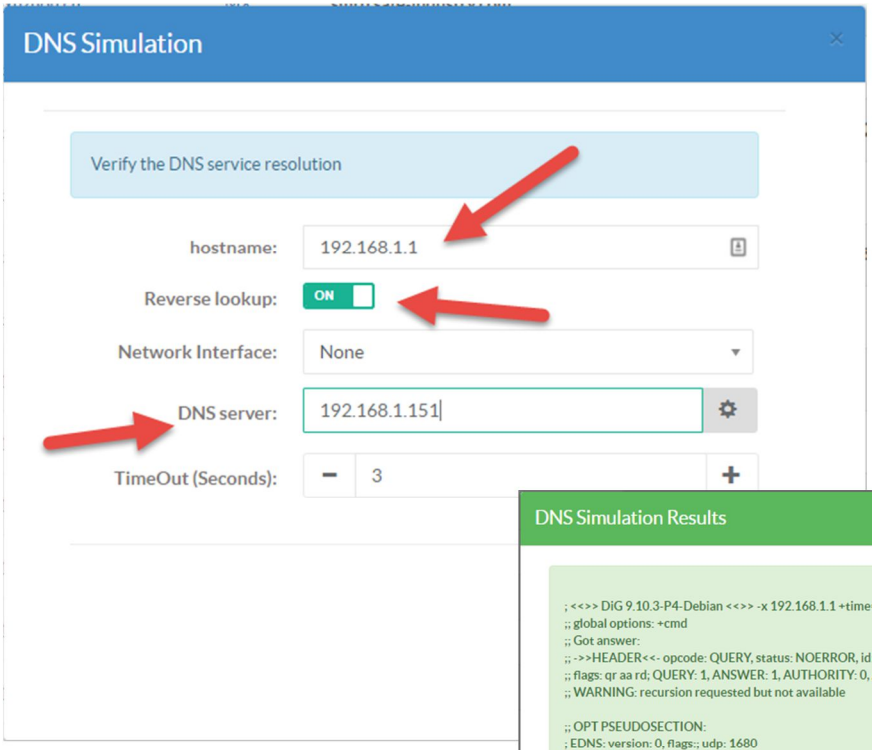
Now that we have a complete configuration, albeit another rather minimal one, we are ready to test to see if our new DNS server is correctly answering reverse DNS queries for our network.

- ✓ On the top menu, click on the icon near the Log out in order to display the right menu.

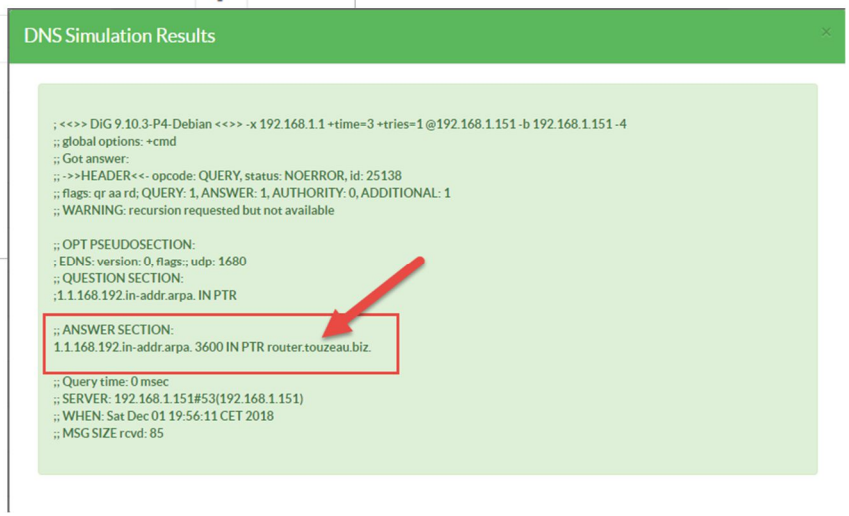


- ✓ Down to "Tools"
- ✓ Click on the "DNS Simulation" item.

- ✓ On the hostname set the IP address of your created item.
- ✓ Turn on the Reverse Lookup switch.
- ✓ On the DNS server, set the IP address of your Artica server.
- ✓ Click on the Run icon.



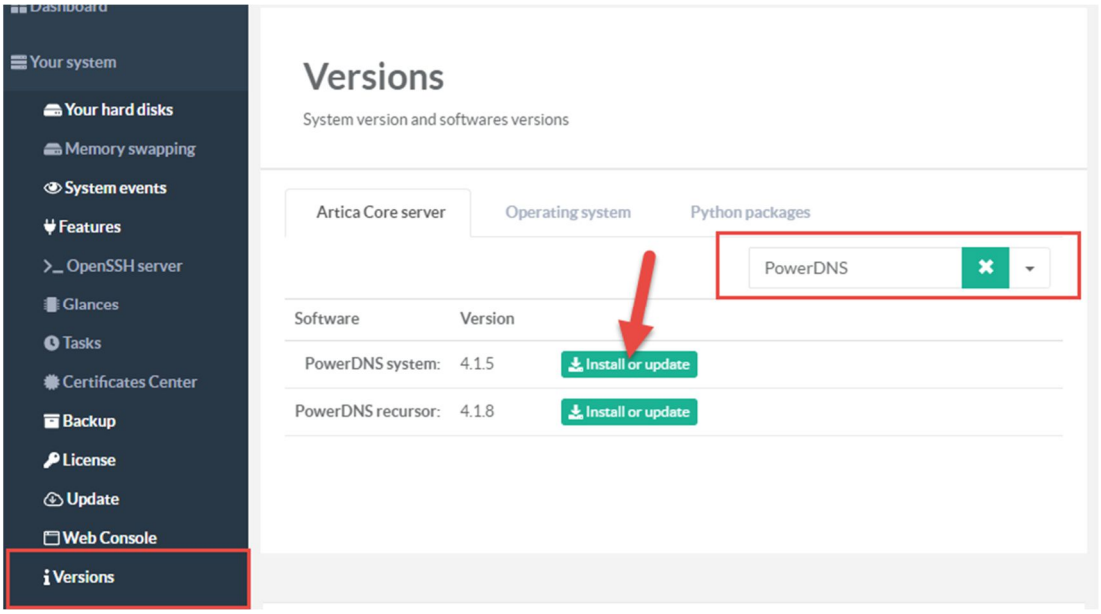
You should see the correct PTR entry in the DNS response.



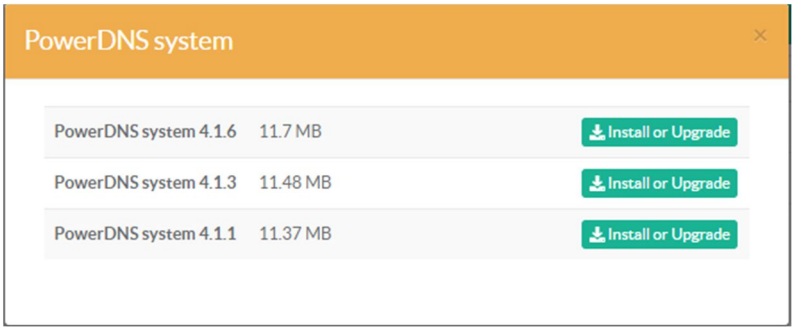
Update the PowerDNS core software.

On the left menu, select "**Your system**" / "**Versions**"

On the search field, type "**PowerDNS**"
Under the **PowerDNS system** row, click on **Install or update** button.



- A new screen is displayed and shows you the list of supported versions.
- Click on the "**Install or Upgrade**" button on the desired version to update it.



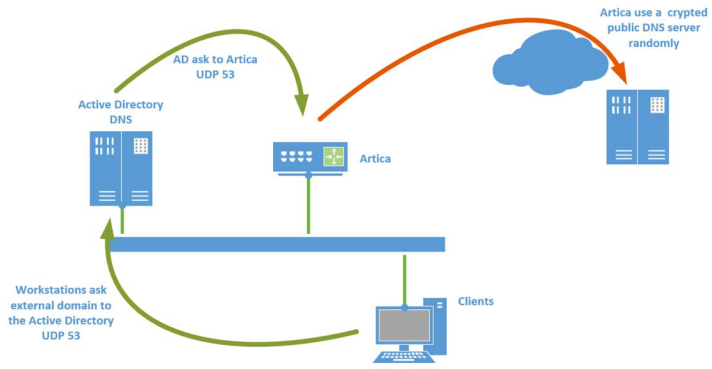
THE DNSCRYPT SERVICE.

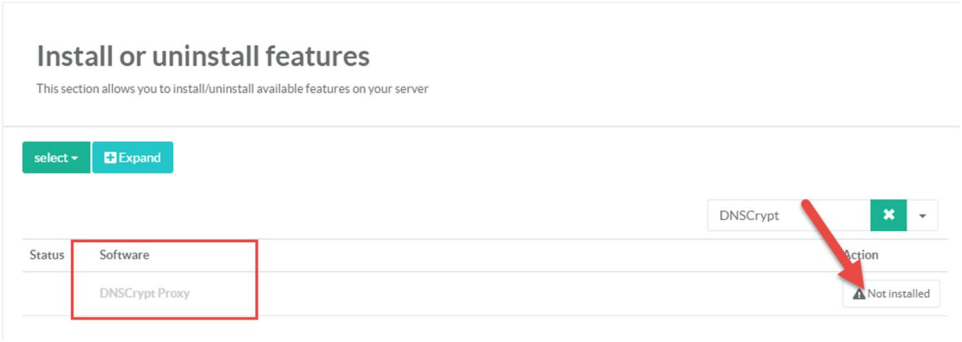
The DNSCrypt service is designed to hide DNS requests from the Internet.
In the same way the SSL turns HTTP web traffic into **HTTPS** encrypted Web traffic, DNSCrypt turns regular DNS traffic into encrypted HTTPS DNS traffic that is secure from eavesdropping and man-in-the-middle attacks.

It doesn't require any changes to domain names or how they work, it simply provides a method for securely encrypting communication between your Artica server and Public DNS servers stored in the Internet.

Technically the DNSCrypt service turn your Artica server to a DOH client (DNS Over HTTPS)

To use DNSCrypt service you have to **enable the Cache DNS service first**.
On the features section, type **DNSCrypt** in the search box.
Click on **Install** button.



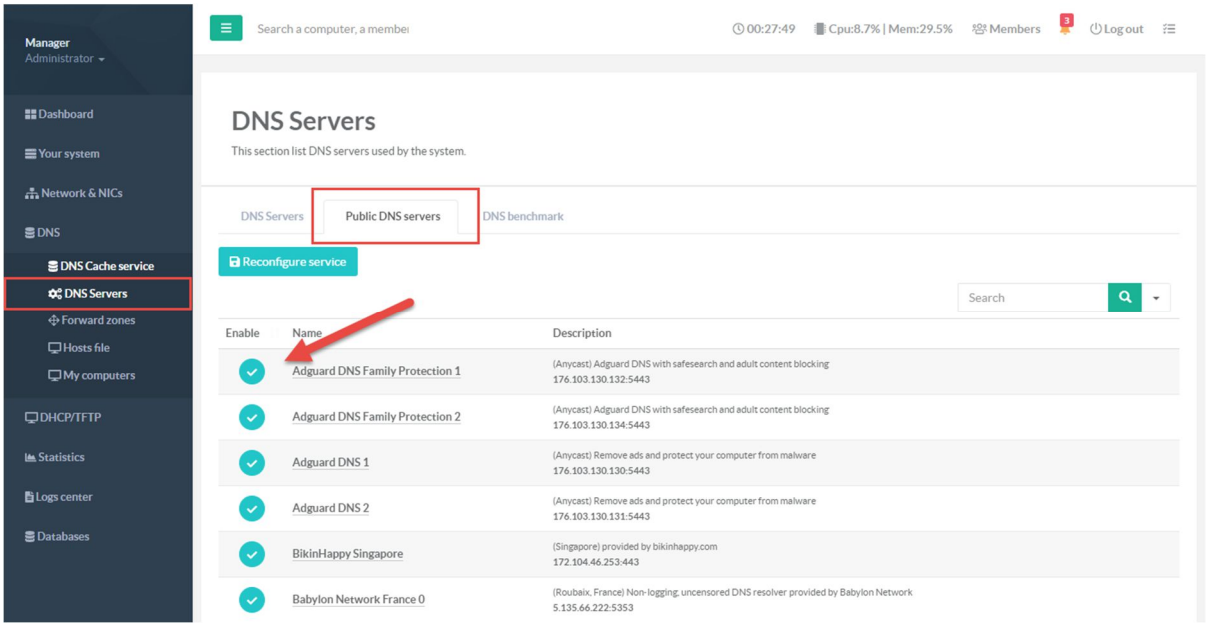


Multiple providers

After installing the **DNSCrypt** service, on the left menu, go into the DNS and DNS servers sub-menu.
Click on "Public DNS servers" tab.

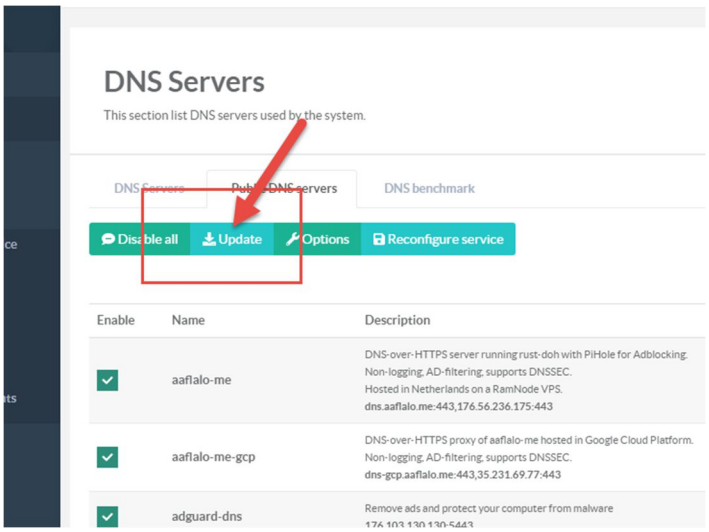
You will see a list of Public Crypted DNS servers used by the DNSCrypt Proxy these servers are chosen randomly from the list.
You can enable or disable some servers to force DNSCrypt Proxy to not use the disabled Public DNS.

Warning: You have to select a minimal of 10 servers to make it run,
if the service turn into error, this means there are no available server to choose, use the "Unique Provider" method.



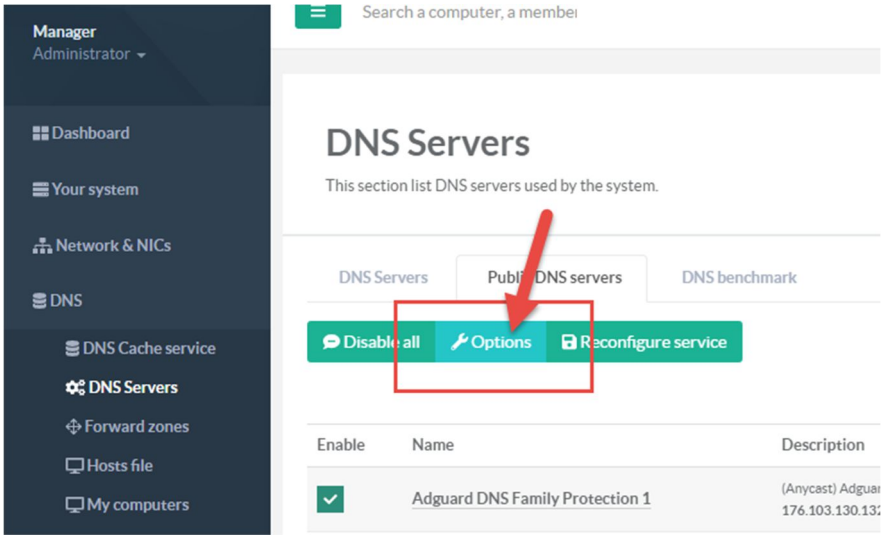
Update the list

The providers list can be updated by clicking on the "**Update**" button.
In this case, new providers that support DoH will be added automatically.

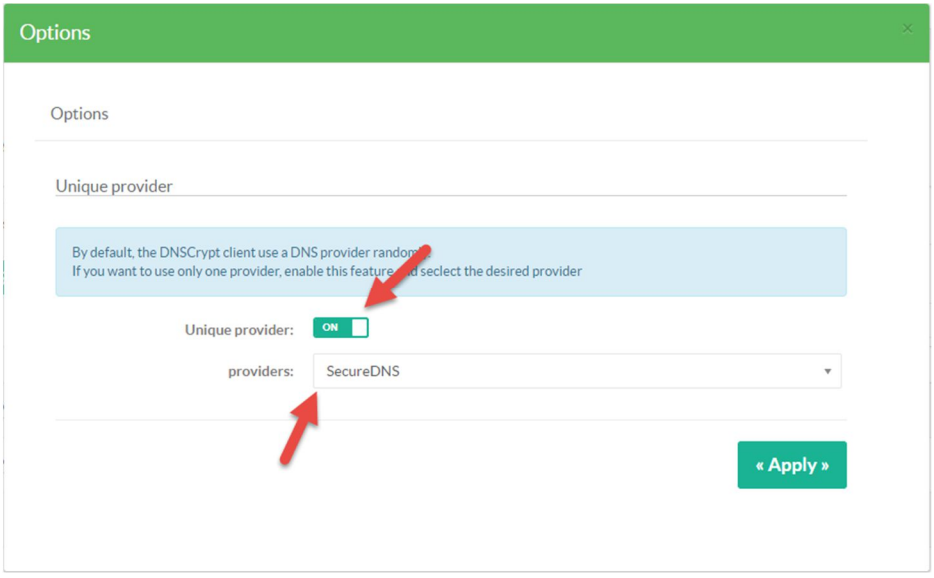


Unique Provider

If you want to select only one service, click on the **option** button



Turn on the option "**Unique Provider**" and select the single provider in the drop-down list.



THE DNS OVER HTTPS SERVICE

The DNS OVER HTTPS service (aka DOH) enable your Artica server act has a DOH DNS service for your clients.
DNS over HTTPS (DoH) is a protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol.
A goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks.
As of March 2018, Google and the Mozilla Foundation are testing versions of DNS over HTTPS.

This service can be installed only if you have a DOH client that is able to use your DNS trough HTTPs.
Some clients on Microsoft Windows are already DOH compatible:

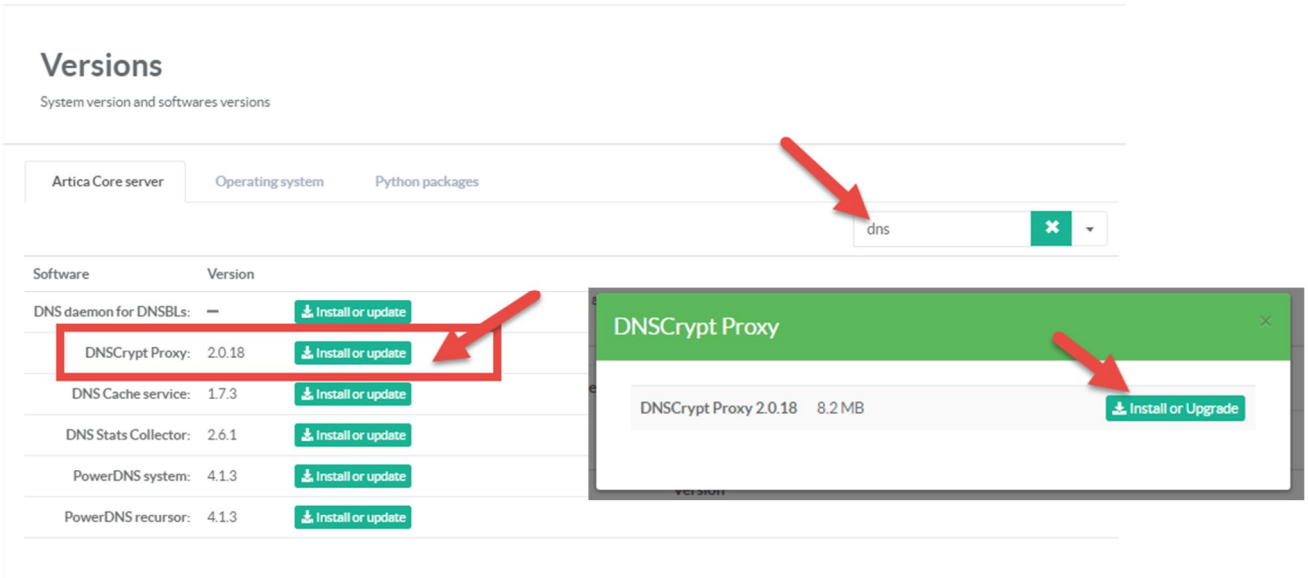
- ✓ Firefox since Version 62 and later.
- ✓ DNSCrypt-proxy
- ✓ Technitium DNS forwarder
- ✓ Google Chrome start to implement it.

Install the DNS Over HTTPs service

Update to the latest version

Artica TECH provide a special package called DNSCrypt-Proxy.
The DNSCrypt-proxy package includes the DOH-Server HTTP plugin, the DOH Client to resolve DNS queries and the DOH forwarder.
On the "Your system" left menu, choose "Versions"

On the search field, type "**dns**"



Under the **DNSCrypt Proxy** row, click on "**Install or update**" button
Choose your desired version and click on "**Install or upgrade.**"

Install the service

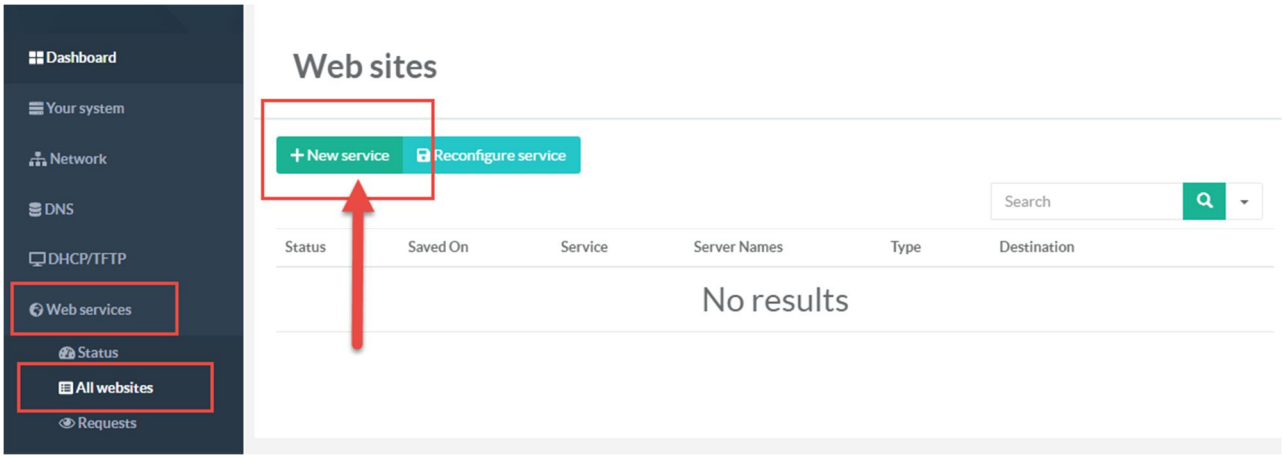
To enable the DNS Over HTTPs, you need to enable first these 2 services using the "**Features**" section:

1. **DNS Cache service.**
2. **NgInx Web engine**

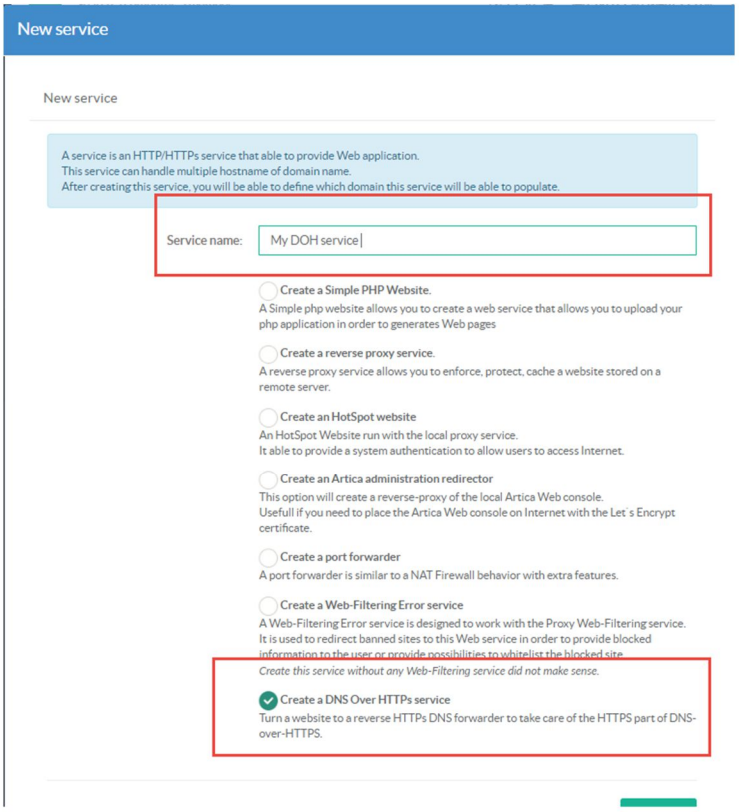
Create the HTTPs service

After installing these 2 services, search the entry "DNS" in the feature's search field.

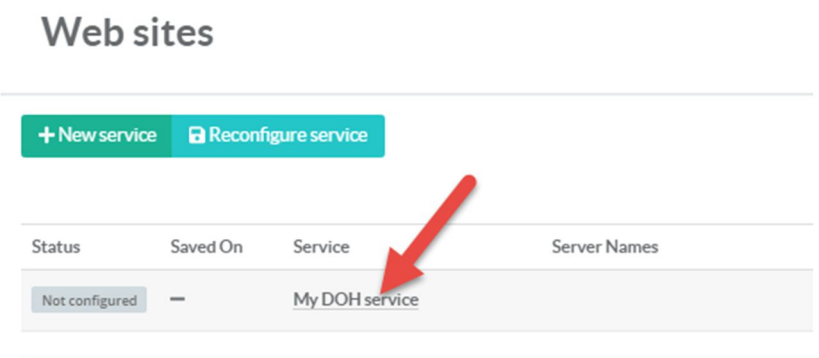
- ✓ Click on "**Install**" button on the **DNS Over HTTPS** server row
- ✓ Create **a new certificate** using the **Certificate Center**
- ✓ On the left, menu choose "**Web services**" and **All websites**.
- ✓ Click on the button "**New service**"


Dashboard
Your system
Network
DNS
DHCP/TFTP
Web services
Status
All websites
Requests
Web sites
+ New service
Reconfigure service
Search
Status
Saved On
Service
Server Names
Type
Destination
No results

- ✓ Set a name of the HTTP service
- ✓ Select the option "**Create a DNS Over HTTPs service**".
- ✓ Click on **Add** button

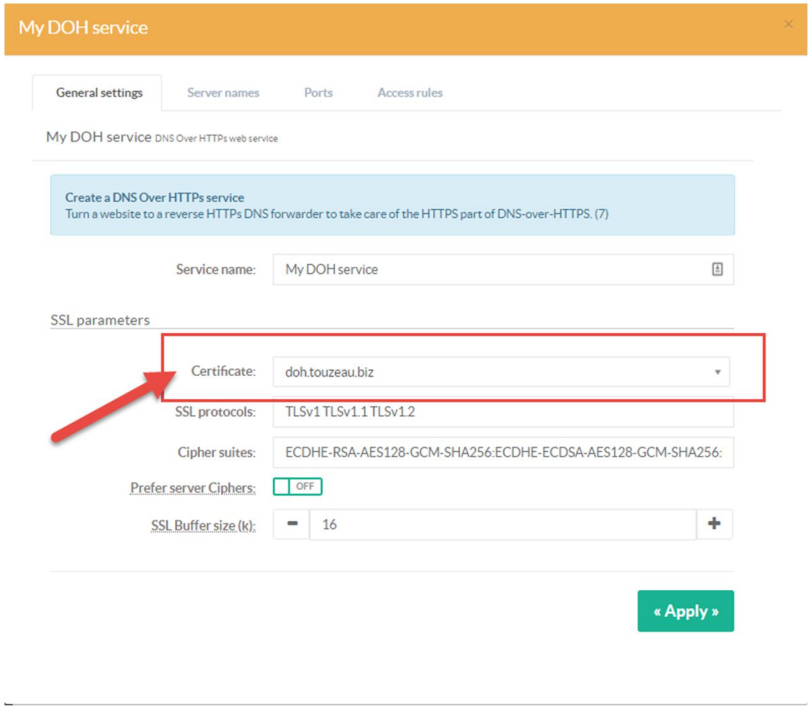


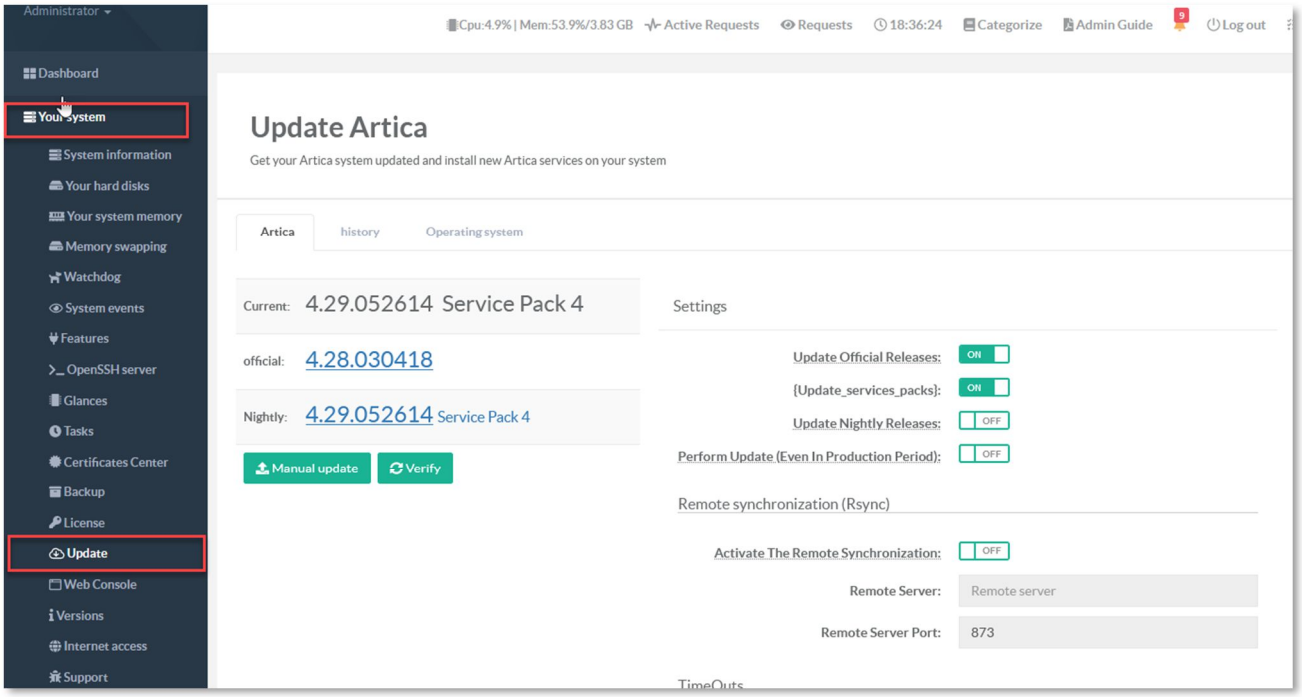
Select your new web service in the table.



On the general settings, choose the certificate created in **Upgrading Artica**

Artica can be updated itself.
Update configuration can be managed in the left menu **Your System /Update**





OFFICIAL RELEASES

By default Artica is configured to only update official releases. Official release are an **even number** in minor version.
So 4.26,4.28,4.30,4.32,4.34,4.36 are official releases.
The automatic update can be controlled by the "**Update Official Releases**" checkbox.

SERVICES PACK

Services pack are patches that are able to fix some issues on the current release or the current nightly.
These services pack can be controlled by the "Update Services Packs" checkbox.

NIGHTLY BUILDS

Nightly build are versions under development, mostly used to add new features that are not totally tested
By default, nightly updates are disabled.
Nightly builds using always **an odd number.**
So 4.27,4.29,4.31,4.33,4.35 are Nightly builds.
The automatic update can be controlled by the "**Update Nightly Releases**" checkbox.

UPDATE IN PRODUCTION

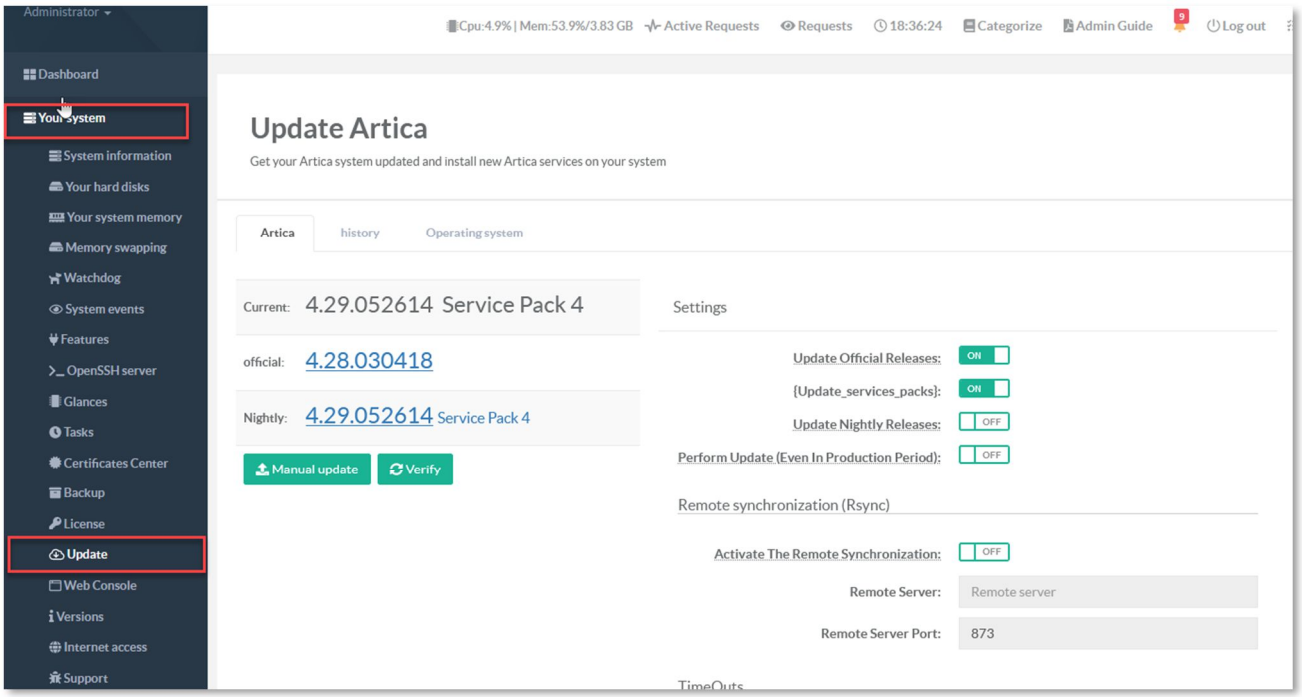
By default, the "Perform Update (Even in production mode)" is disabled.
This means if there is a new update (official, nightly or Service Pack) it will be performed only during 22h PM to 06h AM.

MANUAL UPDATE.

Manual update accept any artica-4.xx.xxxxxx.tgz for full version or ArticaPx.tgz for Services Packs.
With the button Manual update, you can download Artica packages here http://articatech.net/firmwares.php
And upload them to the system.
The manual update button allows you to return back to any version available in the Firmware's table.

THE CERTIFICATES CENTERUPGRADING ARTICA

Artica can be updated itself.
Update configuration can be managed in the left menu **Your System /Update**



OFFICIAL RELEASES

By default Artica is configured to only update official releases. Official release are an **even number** in minor version.
So 4.26,4.28,4.30,4.32,4.34,4.36 are official releases.
The automatic update can be controlled by the "**Update Official Releases**" checkbox.

SERVICES PACK

Services pack are patches that are able to fix some issues on the current release or the current nightly.
These services pack can be controlled by the "Update Services Packs" checkbox.

NIGHTLY BUILDS

Nightly build are versions under development, mostly used to add new features that are not totally tested
By default, nightly updates are disabled.
Nightly builds using always **an odd number.**
So 4.27,4.29,4.31,4.33,4.35 are Nightly builds.
The automatic update can be controlled by the "**Update Nightly Releases**" checkbox.

UPDATE IN PRODUCTION

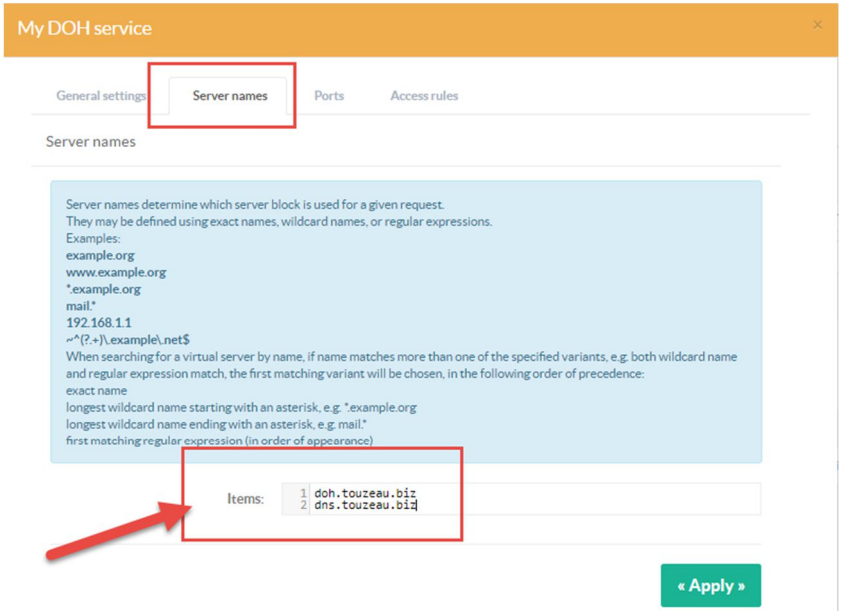
By default, the "Perform Update (Even in production mode)" is disabled.
This means if there is a new update (official, nightly or Service Pack) it will be performed only during 22h PM to 06h AM.

MANUAL UPDATE.

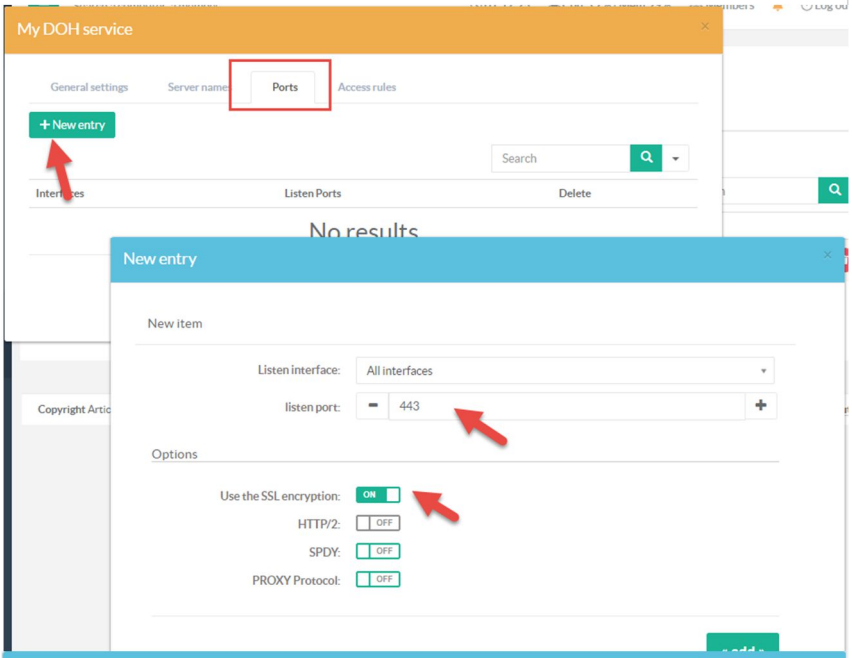
Manual update accept any artica-4.xx.xxxxxx.tgz for full version or ArticaPx.tgz for Services Packs.
With the button Manual update, you can download Artica packages here http://articatech.net/firmwares.php
And upload them to the system.
The manual update button allows you to return back to any version available in the Firmware's table.

The Certificates Center.

On the server names section, set hostnames that will be used for this web service.

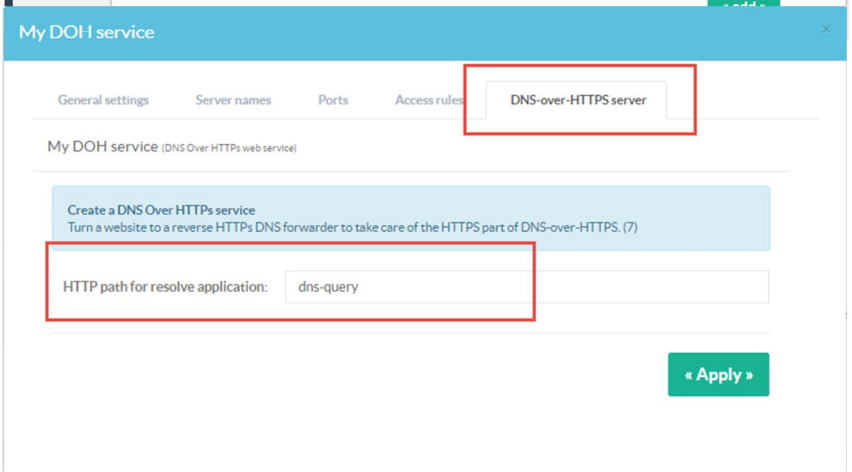


On the Ports section, create a new 443 port and enable the **Use SSL encryption** option.

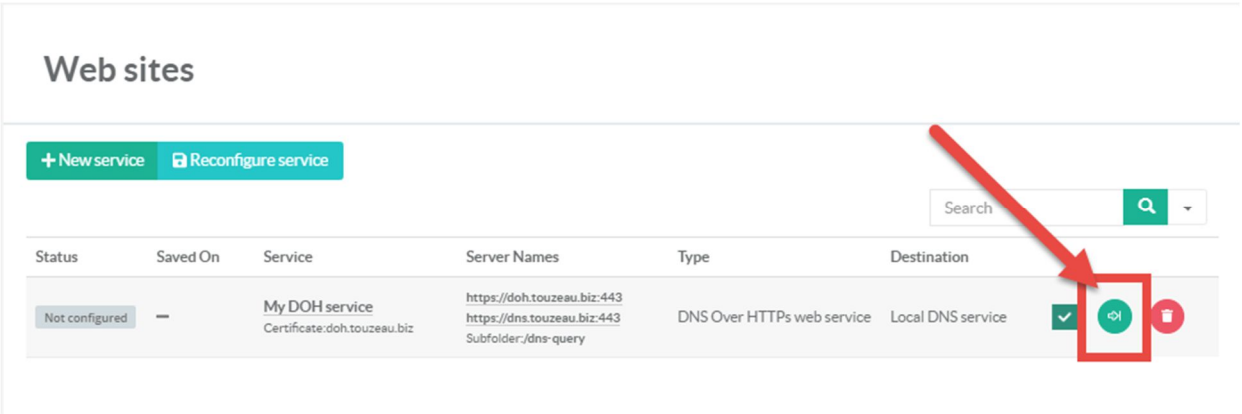


Select the **DNS over HTTPs server** tab.

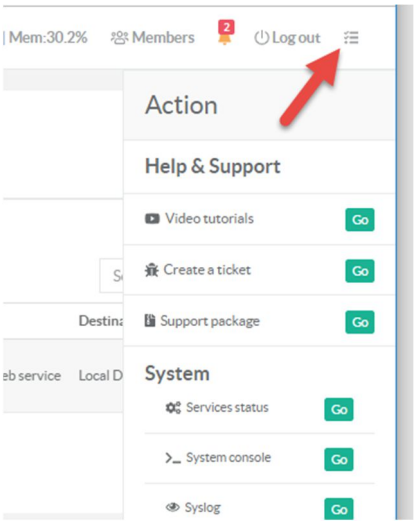
Define the path that will be used by clients to send HTTPs queries and click on **apply**



On the table, you see that your web service is "Not configured", to make the website available, click on the run icon on the right side.

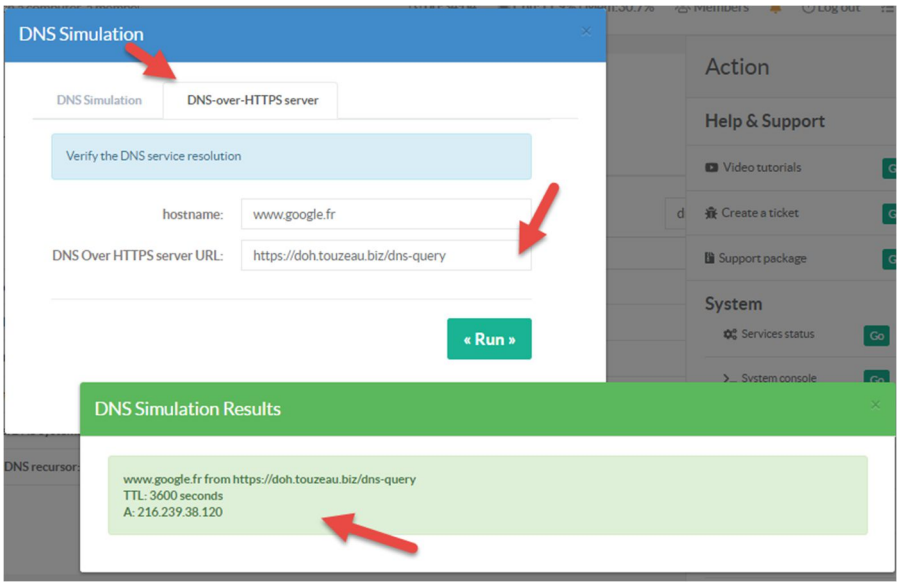


Testing your DOH server resolution



- On the top menu, click on the top-right icon in order to open the right pan.
- Down to the "**DNS Simulation**" link

- Choose the "DNS over HTTPS server" tab
- Set the DNS Over HTTPs URL and click on run.
- The result should be a success that demonstrates your DOH server works as expected.



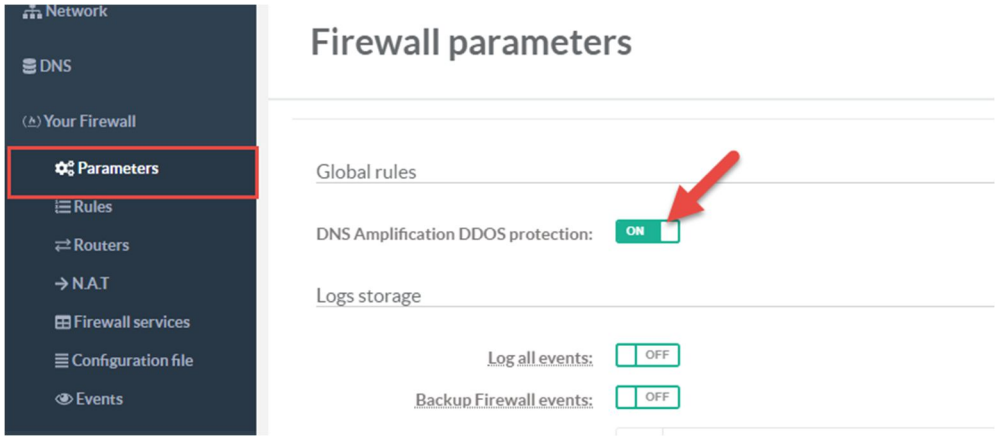
DNS AMPLIFICATION DOS ATTACKS PREVENTION

If you are running a DNS server, then you need to check it is not being co-opted into 'DNS amplification attacks'.
Random nasty servers (typically part of virus created bot-nets) send your DNS server a short request but use a fake source IP address.

1. Your DNS server then sends a (typically) long reply back to that fake source IP address.
2. The fake source IP address gets a lot of traffic from your DNS server.
3. You get abuse complaints.
4. Your server uses a ton of bandwidth

To prevent this behavior, you have to enable the Firewall service using the features section.
In the left menu go to "**Your Firewall**" and "**Parameters**" section.

Under the **Global rules**, turn on the "**DNS Amplification DDOS protection**"



When enabling this option, the firewall will limit the size and the number of requests sent by a remote server.
Usually this prevention will not decrease the DNS answer rate but limit remote systems that try to amplify DNS requests.

Each hour, Artica will update the firewall with a list of bad known domains to be attackers

---

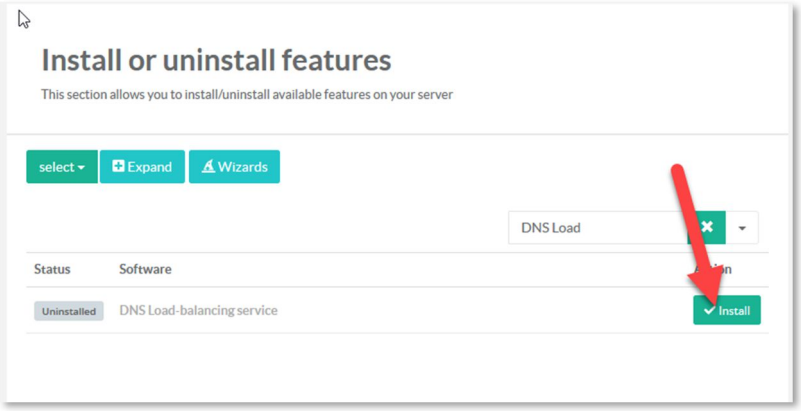
Local networks defined in "Your networks" will not be impacted by these rules.

THE DNS LOAD-BALANCING SERVICE

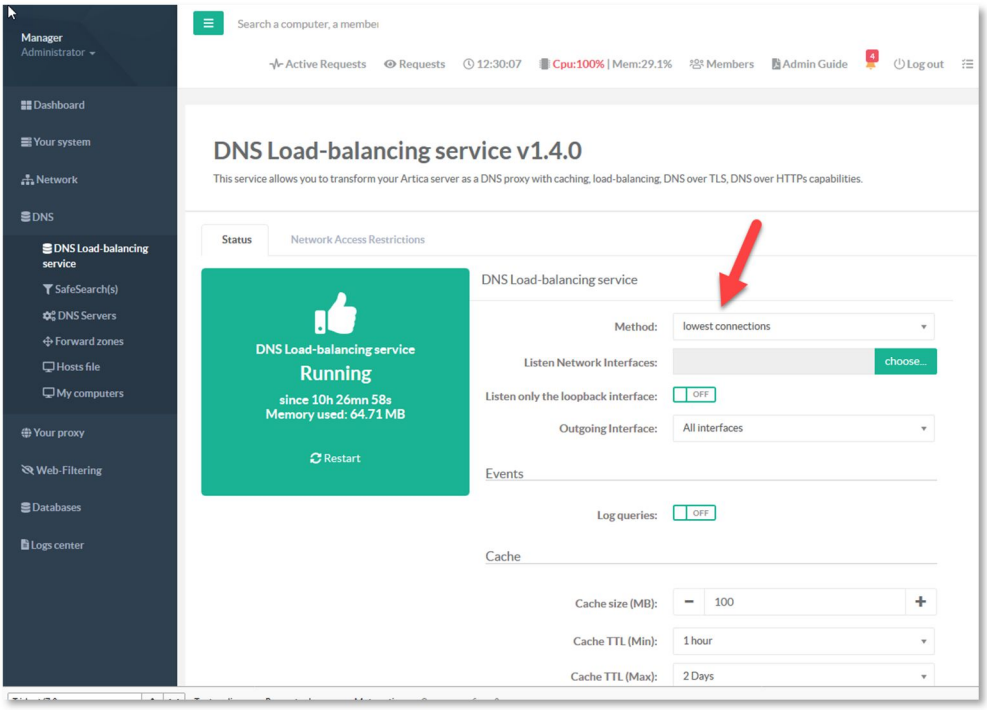
The DNS Load-balancing service allows you to provide a DNS proxy that forward the request to the best DNS server from a list of DNS servers.
This service can increase HTTP proxy performance by choosing dynamically the best server for the lookup query.

Install the service

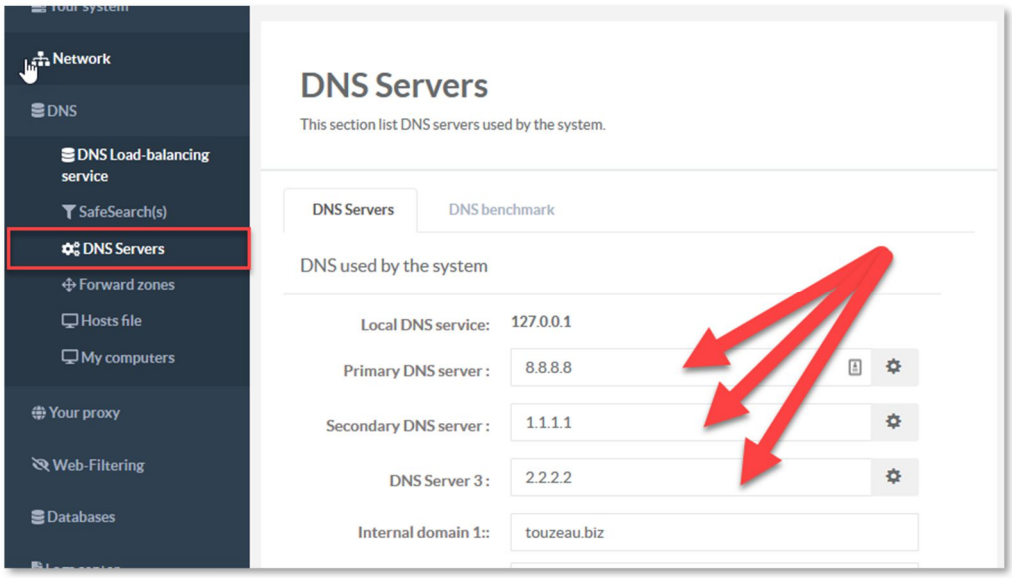
- On the left menu, choose Your System and Features.
- On the search field, type DNS Load.
- Click on Install on the DNS Load-balancing service row



Under "DNS" a new entry called **DNS Load Balancing service** is added.
In this section, you can drive the load-balancing policy and listen interfaces used for the DNS service.

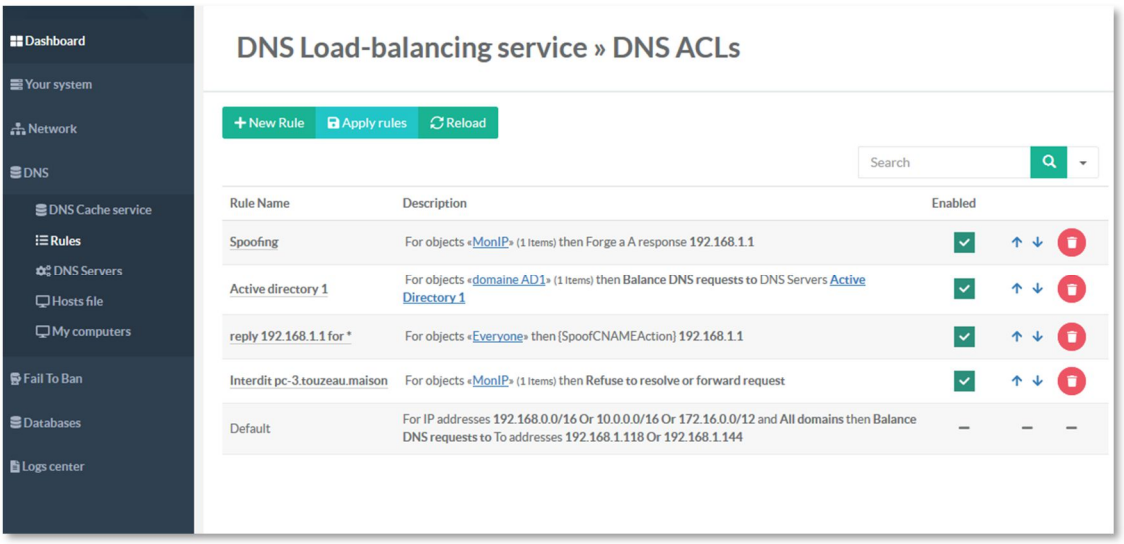


- Servers that are listed in the DNS servers section are now in Load-balancing mode



ACLs For DNS Load-balancer service.

The Rules section allow you to create “ACLs” according the DNS load-balancing service.



A rule is able to modify the behavior of the DNS Load-balancer service.

The DNS Load-balancer service can become the central point of your network DNS.

A Rule can have one of these behavior :

1. Load-balance to a pool of servers.
2. Truncate the request with a given hostname.
3. Truncate the request with a given IP address.
4. Refuse to resolve.
5. Deny the Load-balancer service to cache answers.

THE HTTP/HTTPS PROXY

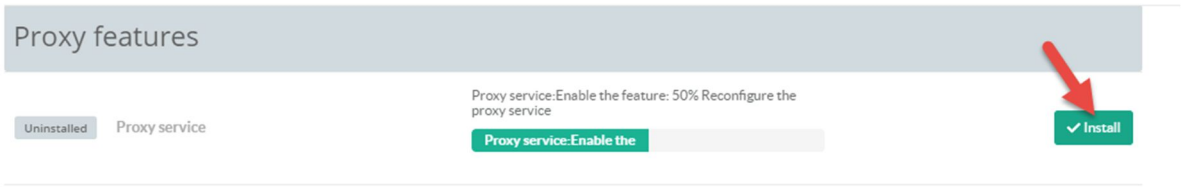
The proxy service is designed to handle the HTTP/HTTPs and FTP over HTTP protocols.
With the proxy service you will be able to secure browser connections through the Internet, manage the bandwidth, authenticate users, use the Web-filtering service, use the Web Application Firewall service (WAF)…

INSTALL THE PROXY SERVICE

Install the single service.

This procedure install only the proxy service without any addon feature.

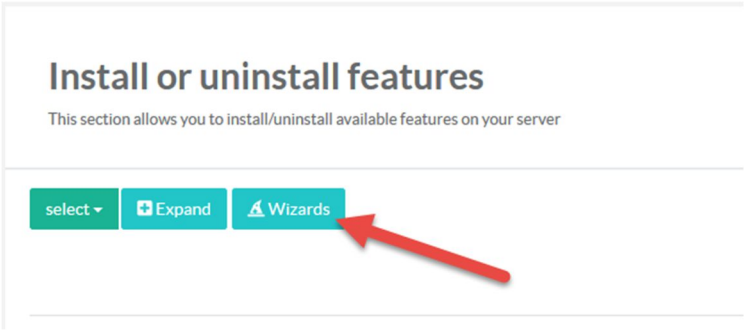
On the left menu, Select "**Your system**" and "**features**"
The proxy service can be enabled in under the "**Proxy features/ Proxy service.**"
Click on install button in order to install the HTTP proxy service.



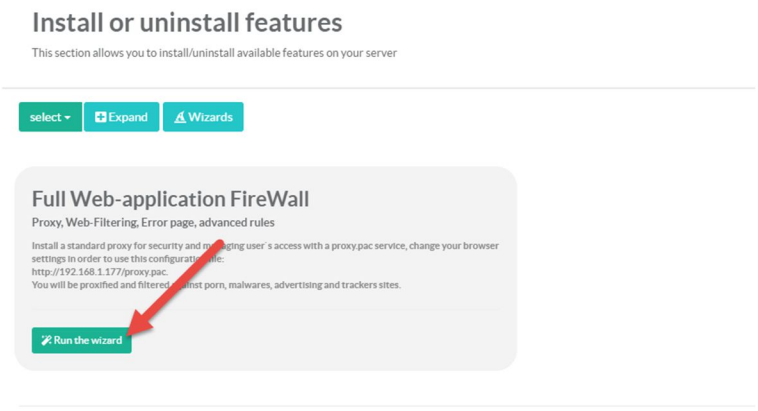
Use the wizards section

If you plan to install the proxy service with full options, you can use dedicated wizards.

- On the left menu, select "**Your system**" and "**features**".
- Click on the **Wizards** button.



The wizards section display a set of "use cases" you can use to install all necessaries services.
Click on "Run the wizard" button the desired topic.



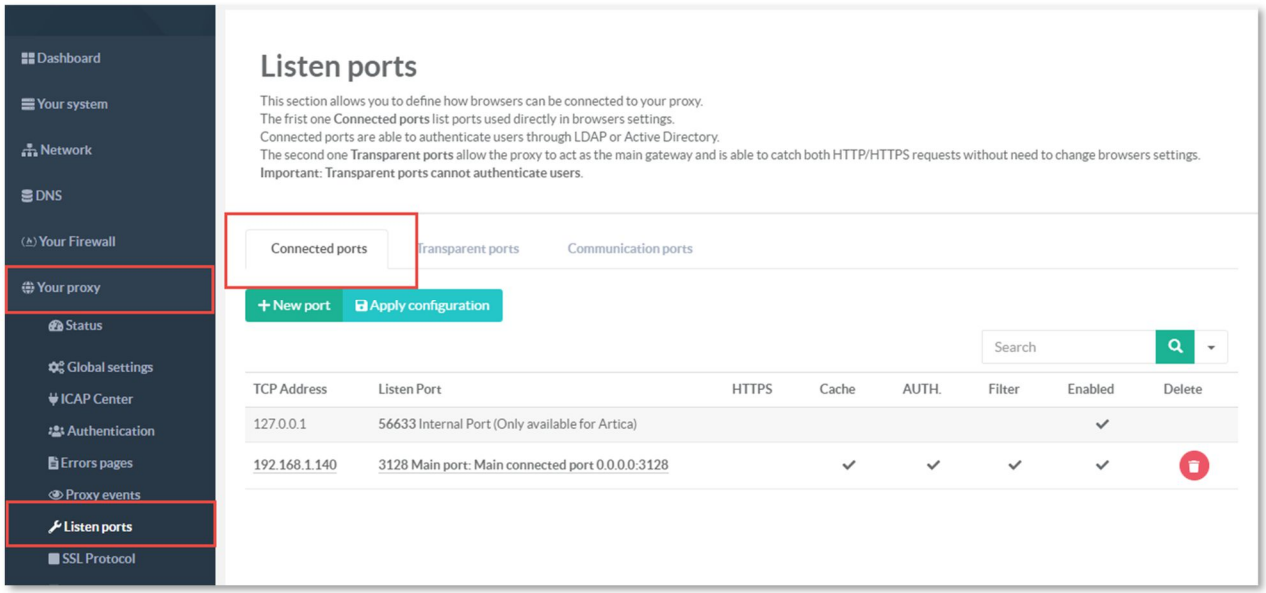
THE PROXY LISTEN PORTS SECTION.

The proxy ports section allows you to set listen ports,the behavior of each port and how clients will connect to the proxy on your network.

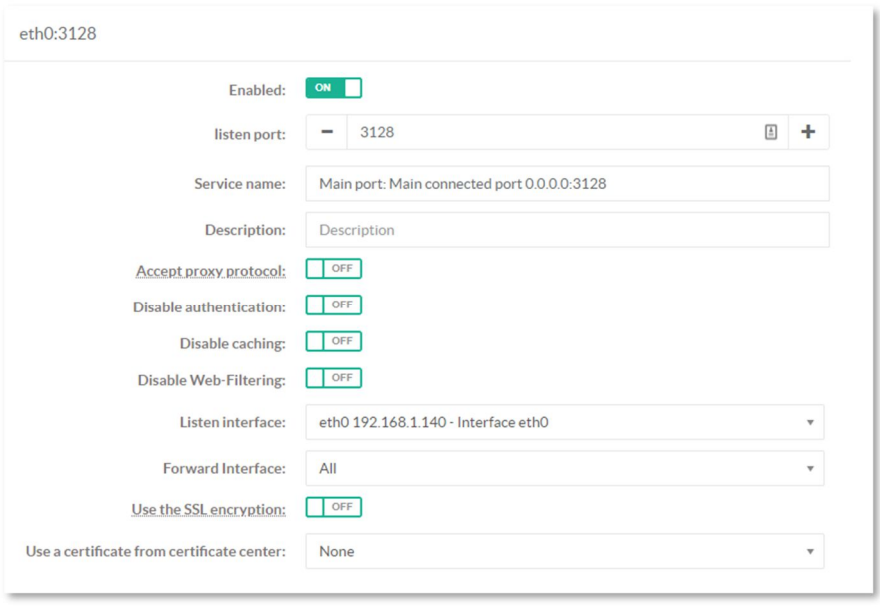
By default, your proxy service run on 3128 for all network interfaces
You can see the section by using the **Your Proxy/Listens ports** left menu.

The Connected ports

The connected ports defines the explicit proxy listening ports.
These ports are defined in browsers settings or with a proxy.pac or wpad



You can add an unlimited ports.
Each port have specifics settings

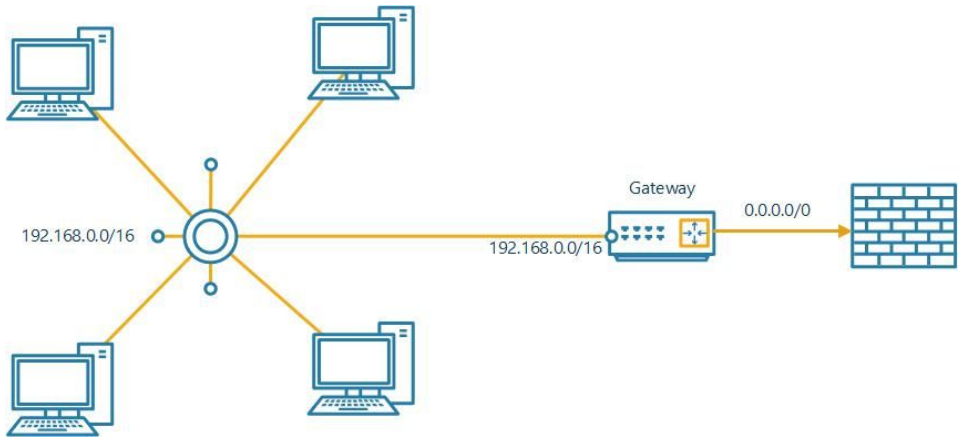


- **Listen port**: A numeric value that defines the port to listen.
- **Service Name**: A description of your port that will be displayed in others sections.
- **Description:** Description used only in the ports table.
- **Accept Proxy protocol**: used only with the load-balancer service.
- **Disable Authentication**: if checked, this port will not ask any authentication.
- **Disable caching:** if checked, Internet objects fetched from this port will not be cached.
- **Disable web filtering:** If checked, the proxy will not query the Web-filtering engine if using this port.
- **Listen Interface:** Which interface to bind in order to listen to client requests
- **Forward Interface:** Which interface to bind in order to fetch internet objects
- **Use SSL encryption:** If checked, the proxy will decrypt SSL protocol using SSL rules and with the associated certificate defined in "**Use a certificate from certificate center**"

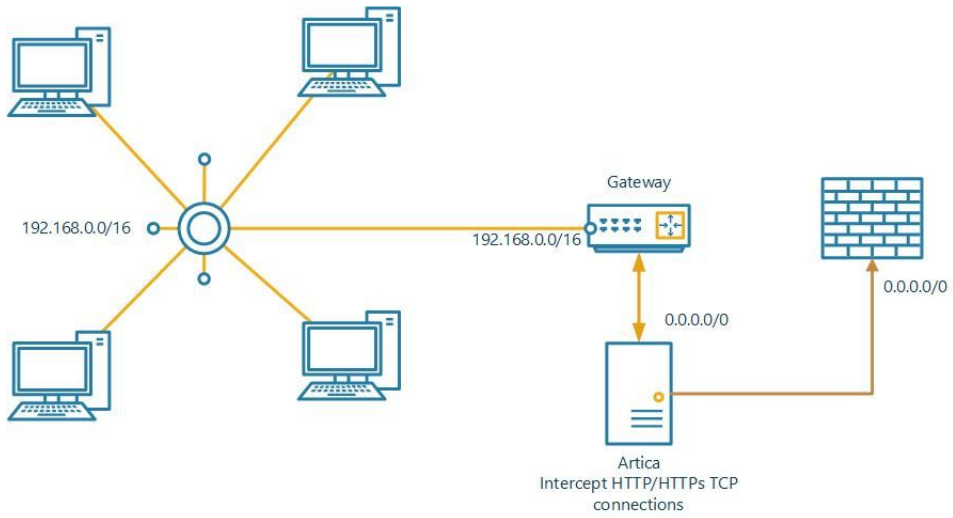
The transparent ports

1. Transparent ports can be used **only if the FireWall service is installed** through the "features" section.
2. To use the transparent method, the proxy must be the "**default gateway**" for unknown networks.
3. You **did not have to set up browsers** because the interception is made directly in the TCP layer.
4. Using transparent method, **you cannot authenticate** users using NTLM/Kerberos/LDAP

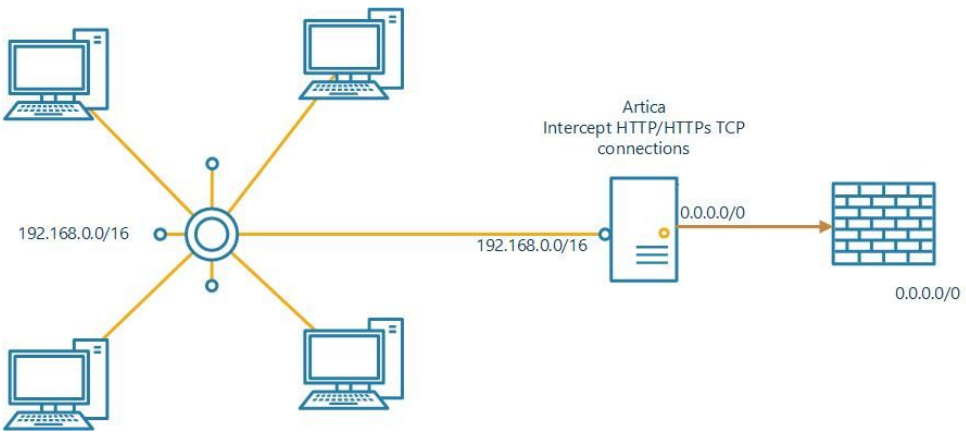
For example this standard network uses a gateway that sends TCP outgoing requests to the Firewall.



Using Artica in transparent mode force the current gateway to use Artica for outgoing requests. Artica will be designed to use the firewall for outgoing requests.

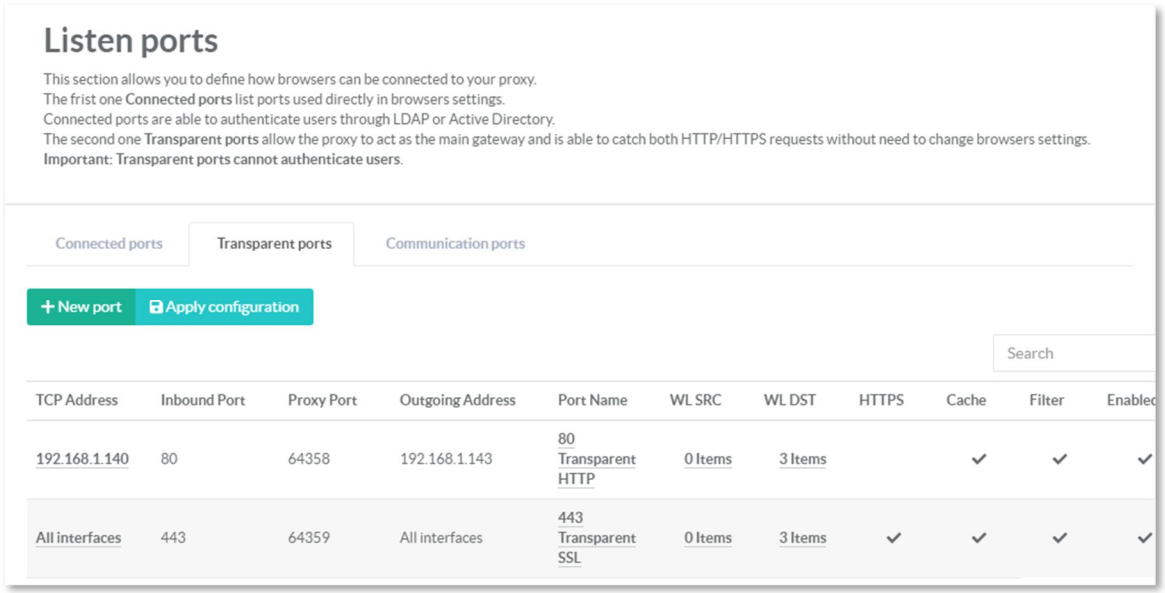


Sure, you are using the firewall as the gateway, Artica should be a new main gateway of the network.

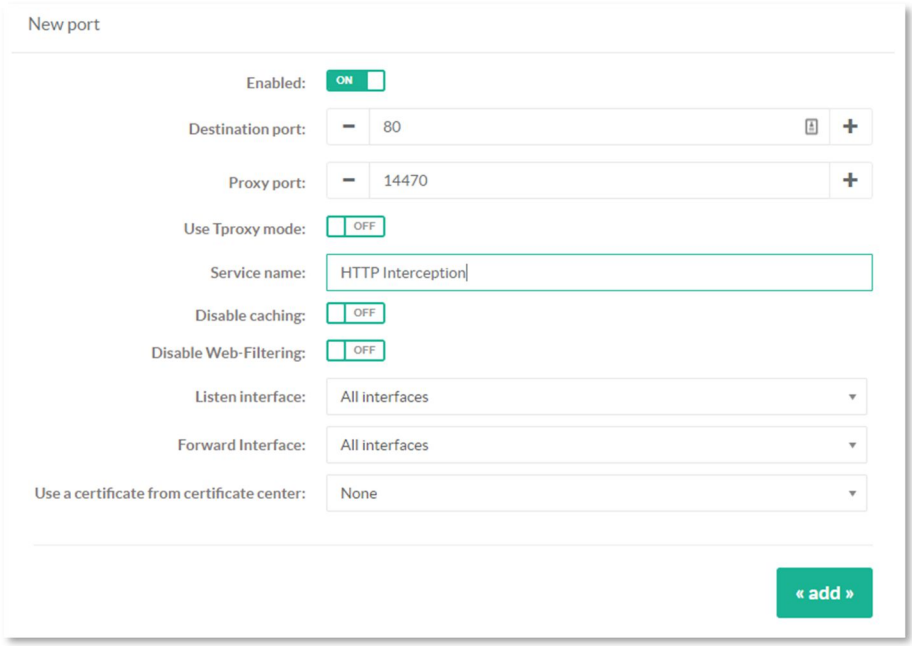


The table displays the ports that are used in interception mode.

You need to create at least 2 transparent ports, one for HTTP and second for SSL.



When you add a new interception port, you need to define:

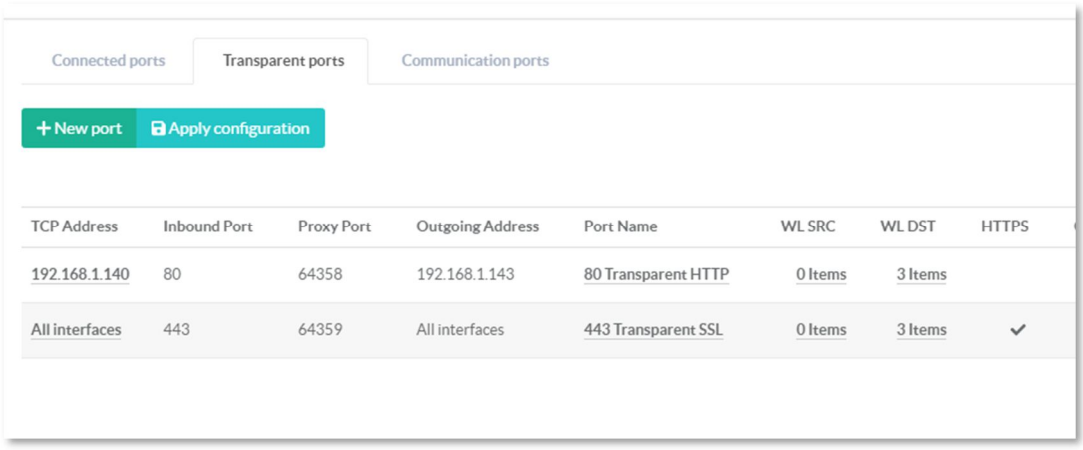


- **Destination port**: The destination port to intercept, for example 80 for http and 443 for SSL.
- **The proxy port**: is the local port used to receive TCP packets from the network interface.
- **Use Tproxy mode**: The Tproxy mode aka (Transparent Proxy Mode) is used especially for routers that require this way (MiKroTiK).
- **Service Name**: A description of your port that will be displayed in other sections.
- **Disable caching:** if checked, Internet objects fetched from this port will not be cached.
- **Disable web filtering:** If checked, the proxy will not query the Web-filtering engine if using this port.
- **Listen Interface:** Which interface to bind in order to listen to TCP requests
- **Forward Interface:** Which interface to bind in order to fetch internet objects
- **Use a certificate from certificate center:** If set, the proxy will decrypt SSL protocol using SSL rules

Network exclusions

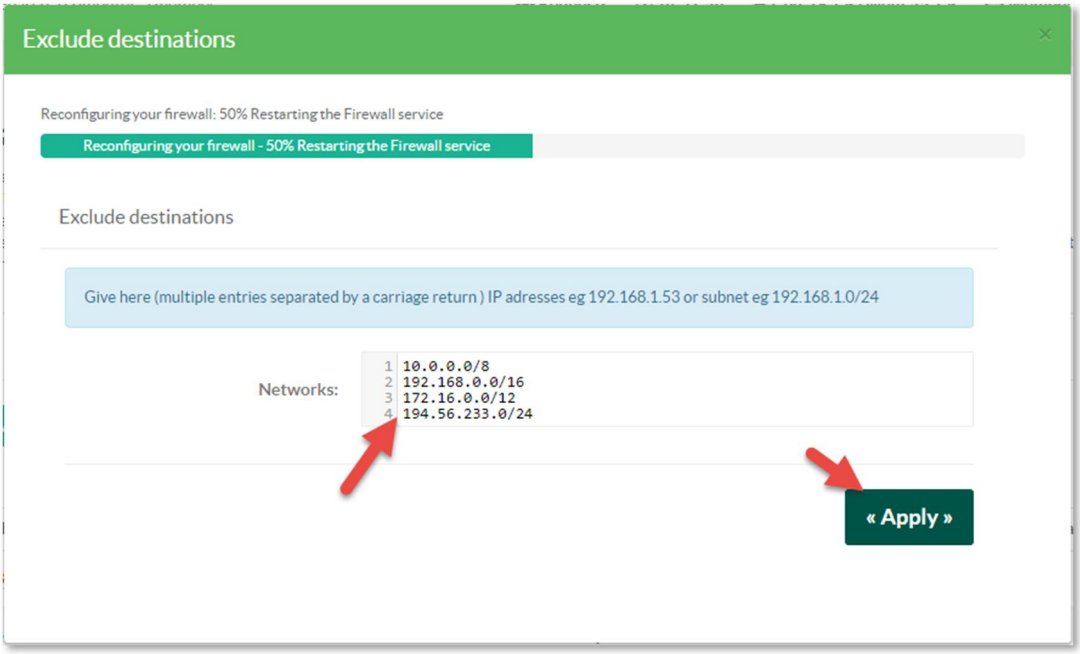
By default, the transparent mode redirects all TCP packets according the requested destination port, except to local RFC 1918 standards networks (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16).

This is why you see 3 items in the WL DST (Whitelisted destinations) after creating a port.

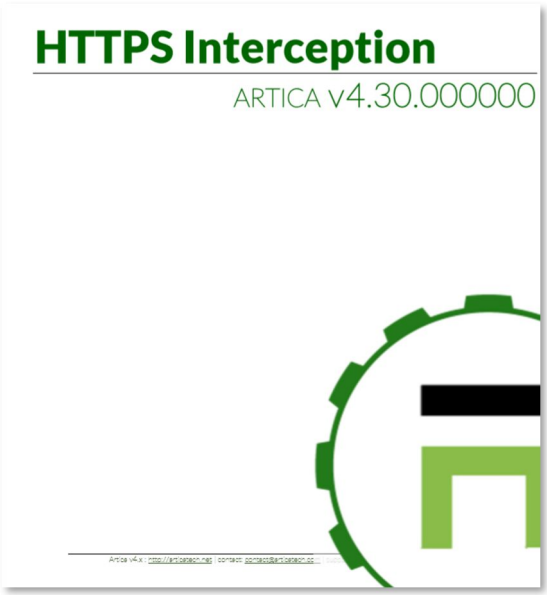


You can bypass the proxy service for specific destination networks or sources.
For example if you have some industrials equipments and you did not want to alter HTTP/SSL connections to the network destination:

1. Click on the Items link in the "WL DST"
2. Add the network to the end of your list.
3. After clicking on **Apply**, Artica will reconfigure the firewall in order to make exclusion in production mode.



SSL Interception



Artica proxy service can inspect HTTPS traffic from your organization.
The service is able to analyze data transactions and apply ACLs policies.
It run as a full SSL proxy, or SSL man-in-the-middle (MITM) proxy.

- SSL encryption is used to hide dangerous content such as viruses, spyware, and other malware.
- Most of unwanted/malicious websites uses SSL encryption.
- Malwares are usually stored into well-known and trusted SSL-enabled sites.
- SSL can be used to hide data leakage; Forward sensitive documents from an organization.
- SSL can be used to hide the browsing by using proxies over Internet

As more and more websites use HTTPS, including social media, the ability to control and inspect traffic to and from these sites is a way to enforce Internet browsing security.

Downoad the dedicated documentation here :

http://articatech.net/download/SSL-PROXY.pdf

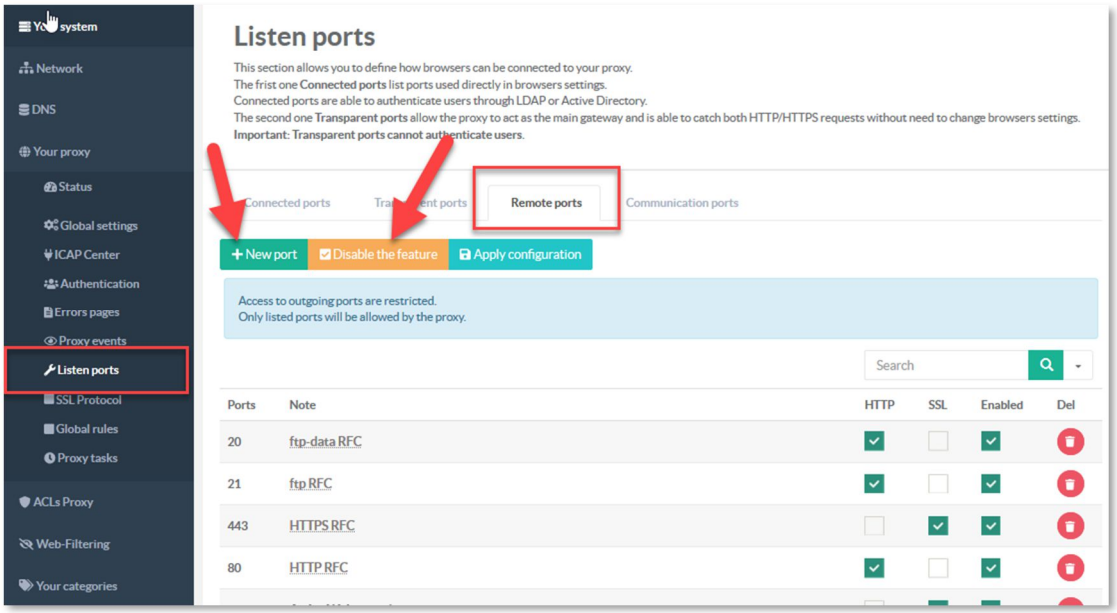
Remote ports

By default, the proxy allow to connect to a limited list of remote ports.
This to prevent access to any suspicious access to Internet.

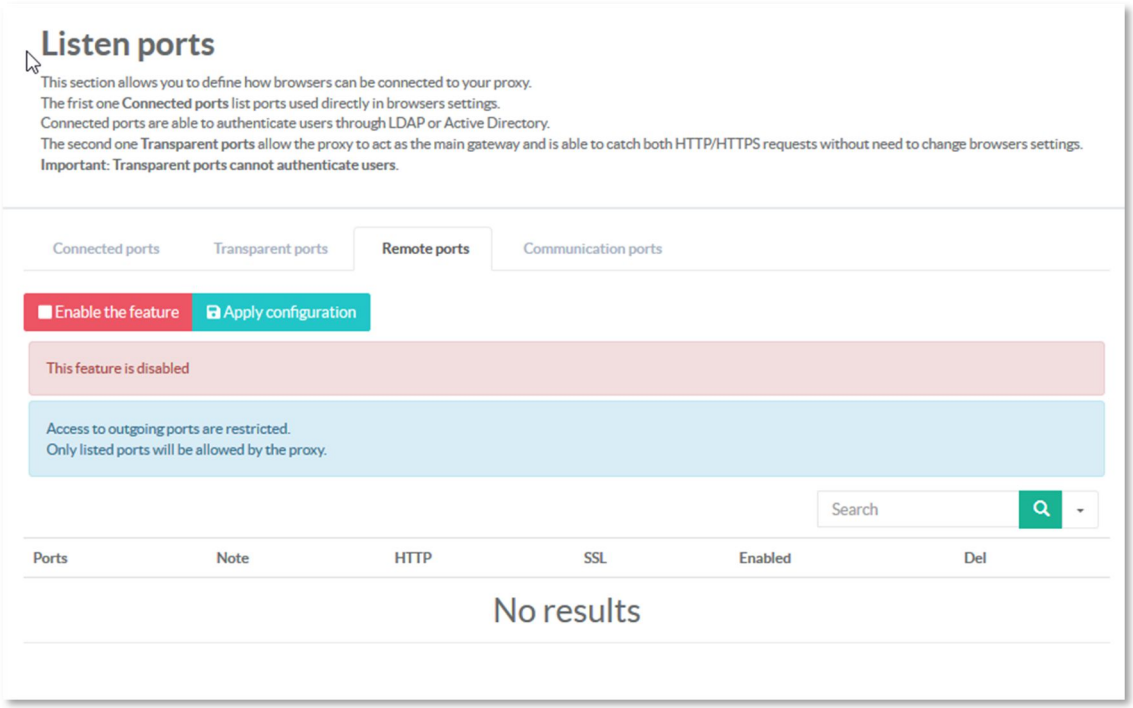
The "**Remote ports**" section manage which port inside which protocol is allowed to be processed by the proxy.
A non-listed port inside this section will be denied by the proxy.

By default the web site http://www.speedtest.net will not working correctly because it require the browser to be connected to a list of unknown ports

If this list is too hard to maintain, you can disable the port checking by clicking on the "Disable the Feature" button. In this way, all ports will be allowed to be processed by the proxy.



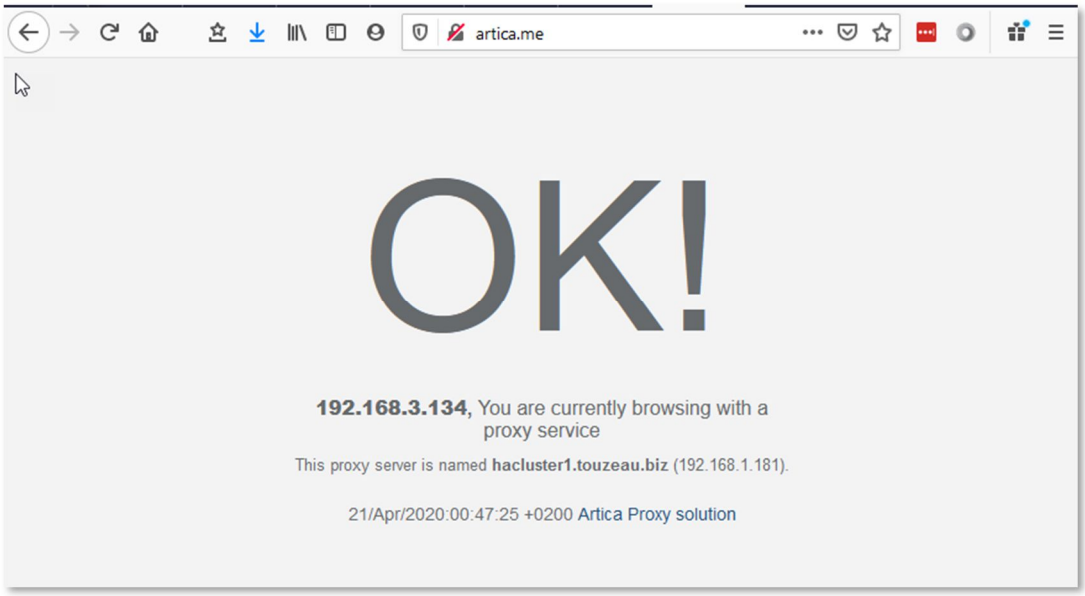
- If the feature is disabled, the table will not display rules ports



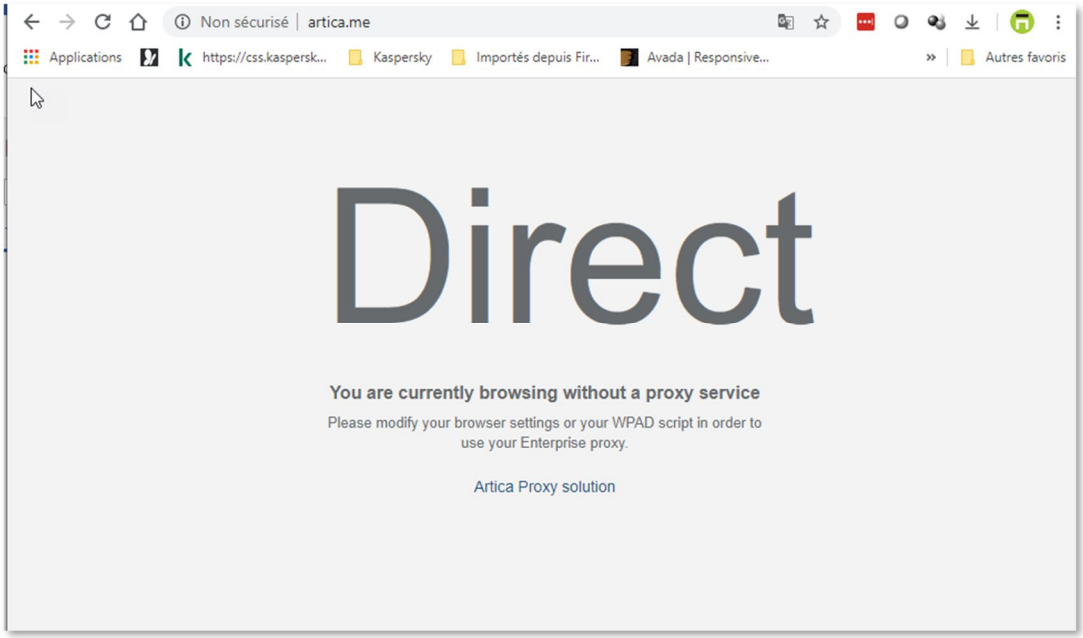
Troubleshooting

How to test if you are using the proxy ?

Open your browser and type http://artica.me
If you using the proxy, you will see this web page

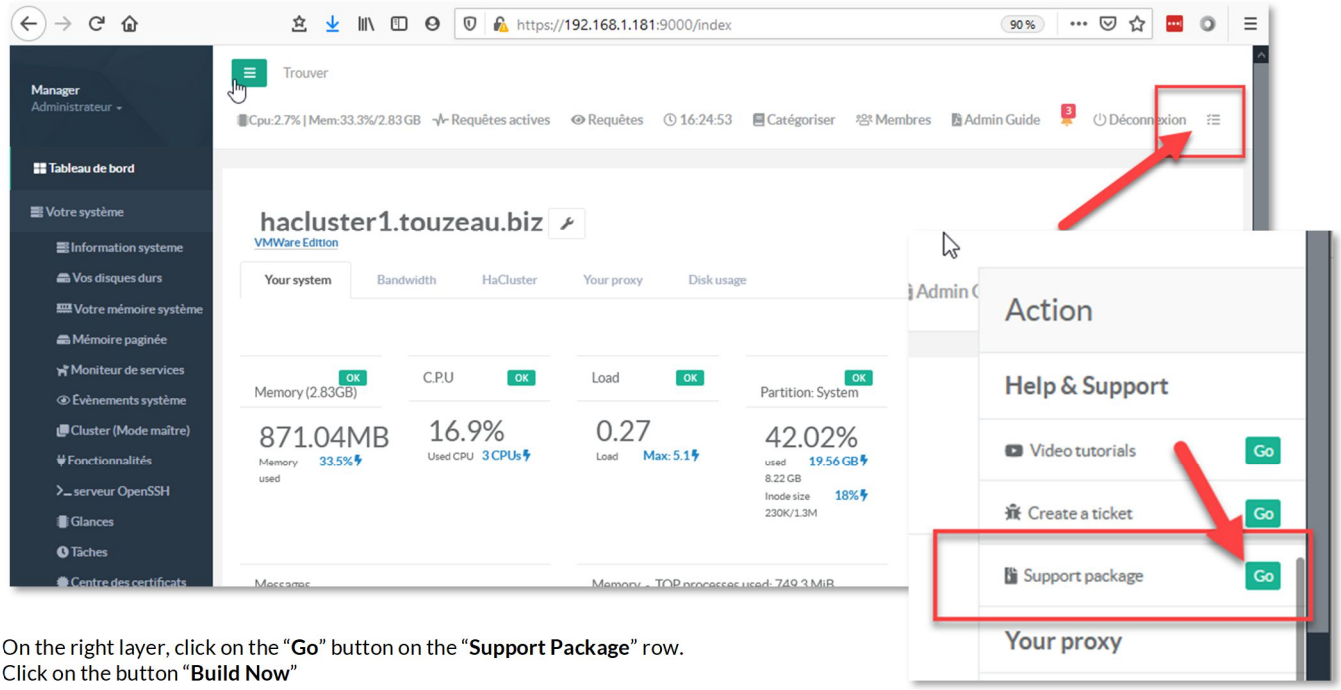


If you did not use the proxy you will see this web page

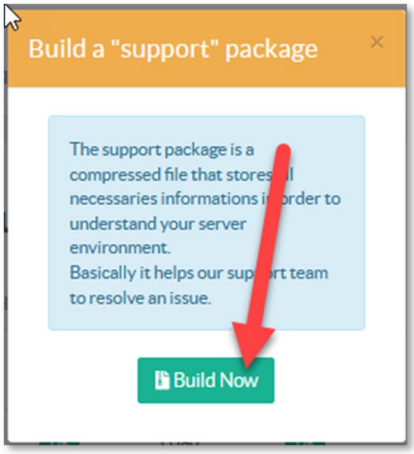


Create a support package

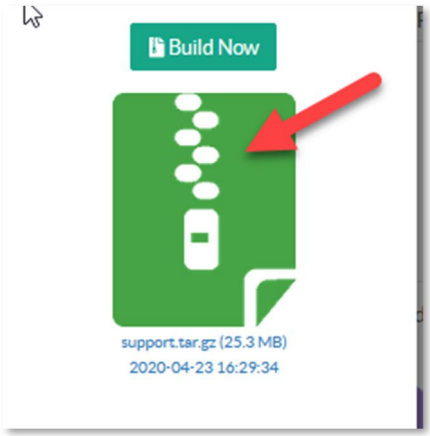
To create a Support Package, click on the "**tasks**" icon on the top right



On the right layer, click on the "**Go**" button on the "**Support Package**" row.
Click on the button "**Build Now**"



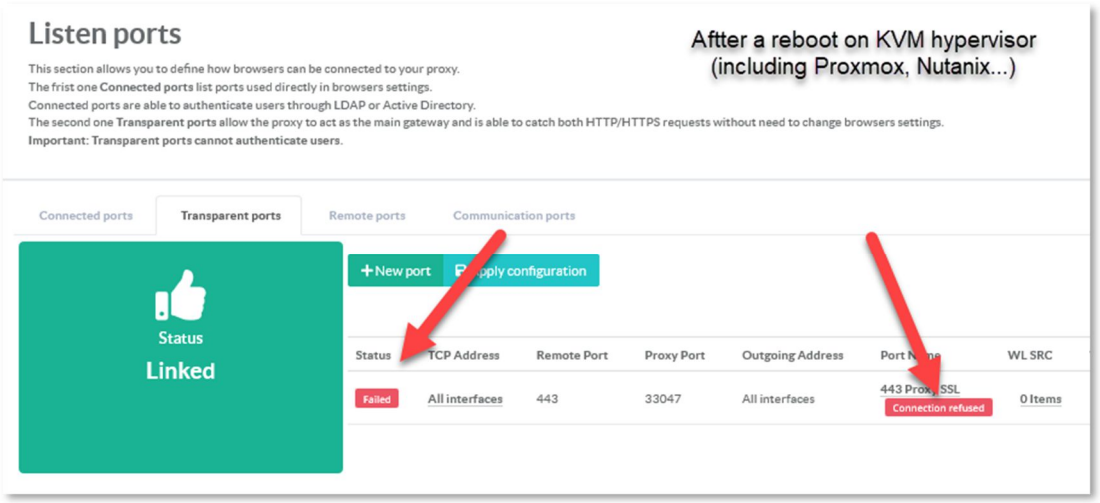
After finish to build the support package, click on the icon in order to download the package



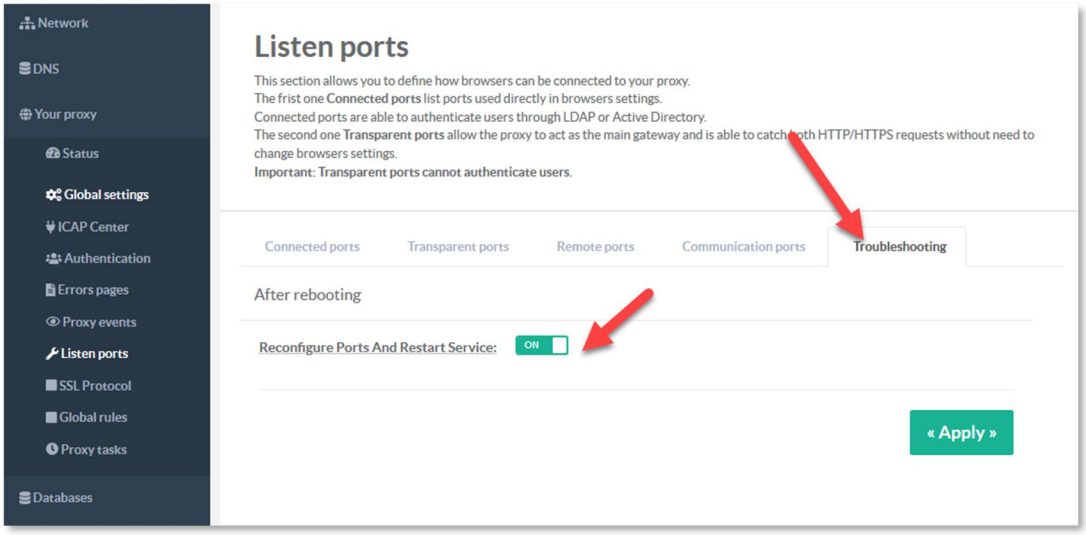
Listen ports freeze after rebooting

Sometimes, when define ports on proxy, the proxy freeze after the boot sequence
This because the network is not really ready to create a sockets

We can see this in the **KVM** based hypervisor (Proxmox, Nutanix for example).



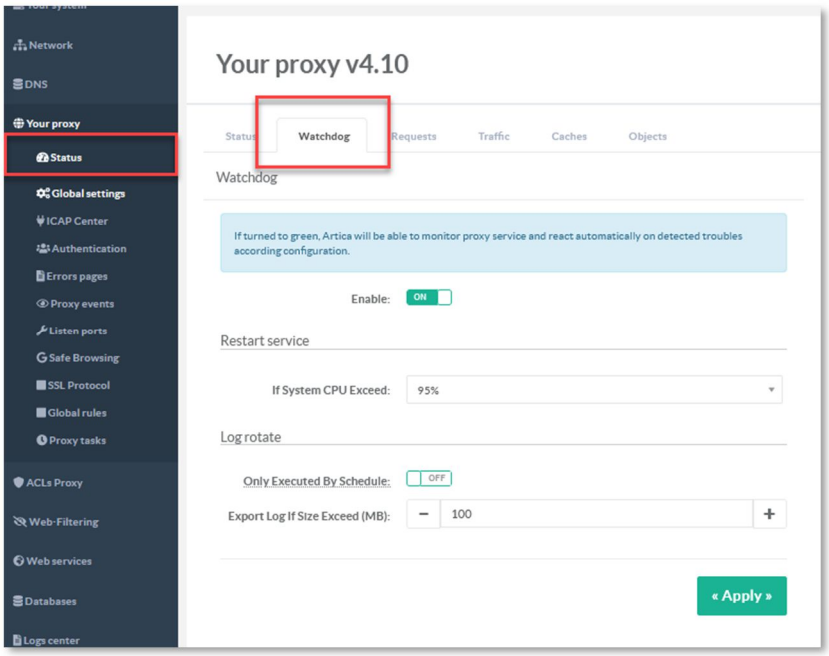
On the Listen ports section, click on **Troubleshooting** tab.



Check the option "**Reconfigure Ports and Restart service**".
Enable this option reconfigure ports and restart the proxy service just after the boot sequence on order to avoid the freeze behavior.

Proxy service monitoring

- You can enable a specific watchdog that able to monitor your proxy service.
- On the left menu, go to "**Your Proxy / Status**"
- Click on the **Watchdog** tab.



Turn on the "**Enable**" option to monitor your Proxy service.

Monitoring the CPU usage

You can ask to restart automatically the service if the Proxy service consume x% of CPU during a period (in minutes)

By default, if the proxy service consume 95% of CPU during 5 minutes, then the daemon service is restarted.

Monitoring the legal log.

If the "**Only executed by schedule**" option is enabled, then the log file is not monitored and only the scheduled log rotation task is in charge to compress and stores the legal log.

If it is disabled, you can define the max size of the legal log to perform the rotation.

By default, if the legal log size is more than 100Mb then the log rotation is executed.

WCCP

About WCCPv2 support

Web Cache Communication Protocol (WCCP) is a technology developed by Cisco that allows transparent re-direction of network traffic in real-time.
This re-direction can be to a cache engine or to a proxy, such as Artica Proxy.

Artica includes support for Web Cache Communication Protocol version 2 (WCCPv2).

WCCPv2 is a content-routing protocol developed by Cisco Systems.
It provides a mechanism to redirect traffic flows in real time.
The primary purpose of the interaction between WCCPv2-enabled routers and an Artica server is to establish and maintain the transparent redirection of selected types of traffic flowing through those routers.

Cisco says: WCCP enables supported Cisco routers and switches to transparently redirect content requests.
With transparent redirection, users do not have to configure their browsers to use a web proxy.
Instead, they can use the target URL to request content, and their requests are automatically redirected to an application engine.
The word transparent means that the end user does not know that a requested file (such as a web page) came from the application engine instead of from the originally specified server.

You can use any "wccp-compatible router" such as Fortinet (Fortigate)

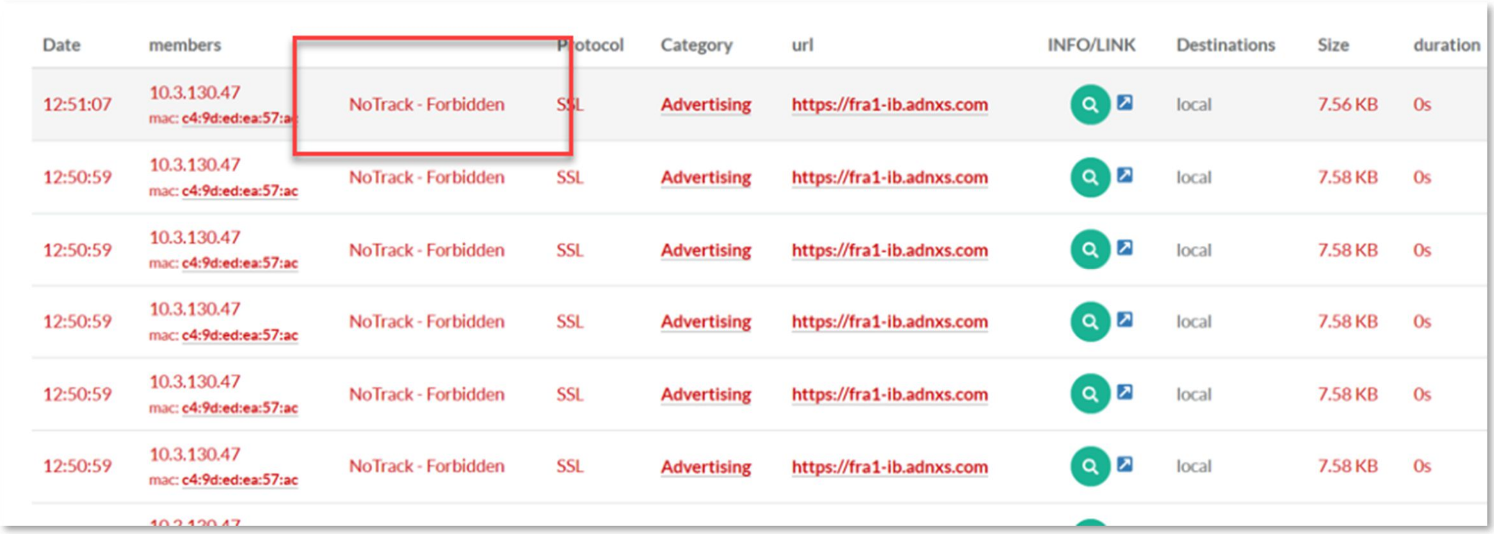
Download the dedicated documentation here:
http://articatech.net/about-wccp.php

NoTrack

NoTrack is an automatic blocking Websites feature. It is designed to prevent online tracking.
It limits or restricts the ability of ads to display themselves and then track you in the browser and blocks unwanted advertisements.

NoTrack prevent your computers from connecting to specific hosts.
This is an easy and effective way to protect you from many types of spyware, reduces bandwidth use, blocks certain pop-up traps, prevents user tracking by way of "web bugs" embedded in spam, provides partial protection to browsers from certain web-based exploits and blocks most advertising you would otherwise be subjected to on the internet.

This feature is enabled by default, you can see in the Realtime requests table URLs in red with the **NoTrack – Forbidden** label.



Date	members		Protocol	Category	url	INFO/LINK	Destinations	Size	duration
12:51:07	10.3.130.47 mac: c4:9d:ed:ea:57:a	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com		local	7.56 KB	0s
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com		local	7.58 KB	0s
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com		local	7.58 KB	0s
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com		local	7.58 KB	0s
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com		local	7.58 KB	0s
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com		local	7.58 KB	0s

URLHaus

URLhaus is a project operated by **abuse.ch**.
The purpose of the project is to collect, track and share malware URLs, helping network administrators and security analysts to protect their network and customers from cyber threats.
This option should consume CPU, be sure using a Core i7 or higher.
This option is disabled by default.

Web site-blocking

Web-site blocking allows you to add a website you want to block for everyone. Mostly used for security reasons.

GOOGLE SAFE BROWSING

What is Safe Browsing?

Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.
Examples of unsafe web resources are social engineering sites (phishing and deceptive sites) and sites that host malware or unwanted software.

With Safe Browsing you can:

- Check pages against Google Safe Browsing lists based on platform and threat types.
- Warn users before they click links in your site that may lead to infected pages.

The Google Chrome, Safari, Firefox, Vivaldi, and GNOME Web browsers use the lists from the Google Safe Browsing service for checking pages against potential threats
Currently, Opera, Internet Explorer, Microsoft Edge are not able to query the Google Safe Browsing reputation server.

You can test the Google Safe Browsing database here:

https://transparencyreport.google.com/safe-browsing/search

The Safe Browsing API is for non-commercial use only and is available with **Artica Community Edition**

Benefits on Artica proxy

Visibility

Potential threats are blocked directly from browsers and administrator did not have any events according blocked threats.
Artica Proxy MARK logs threats with "**GoogleSafe**".
Each threat can be retrieved in logs or events.

Protect any non-compatible browsers

If users that disables Safe Browsing or using any browser that is not able to query Safe Browsing will be still protected by Artica Proxy.

Potential privacy

Technically unfounded rumors accuse Google to use Safe Browsing for tracking purposes (https://www.sitepronews.com/2014/10/01/googles-safe-browsing-service-killing-privacy/)
Using Artica as a Safe Browsing client hides user requests, the Artica cache system ensures inconsistent browsing when leaving the proxy

Download the documentation

Documentation of Google Safe Browsing feature can be downloaded here:

http://articatech.net/download/Google-Safe-Browsing.pdf

AUTHENTICATE MEMBERS

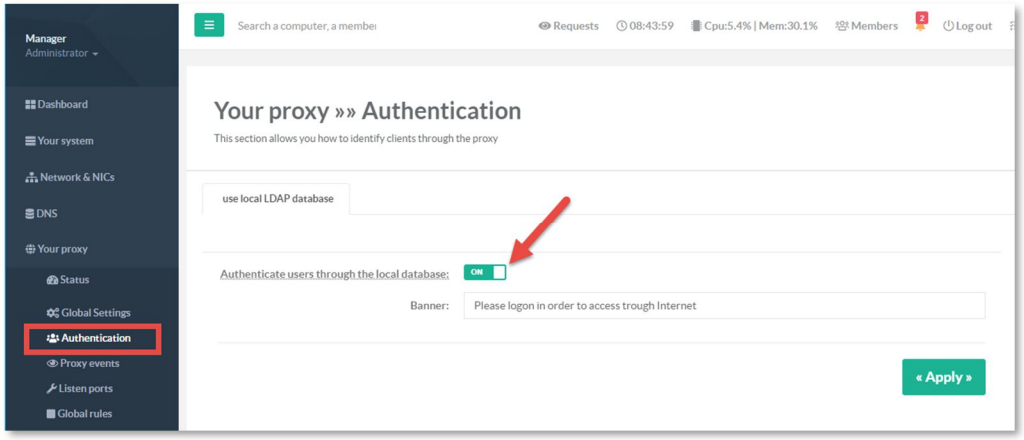
When authenticating users, the proxy is able to trace all requests with the username logged to the system.

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 for multiple Base Distinguished Names (DNs).

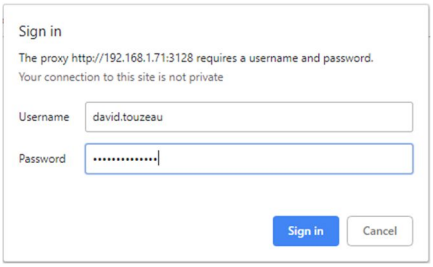
Use the Artica LDAP service.

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**"

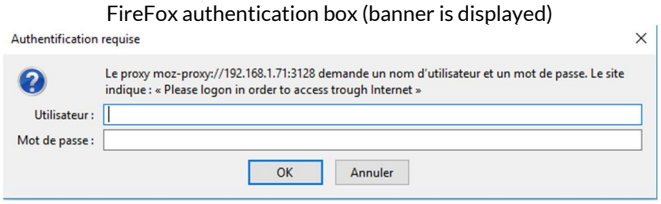


Set the message that will be displayed in the authentication box in the "**Banner**" field

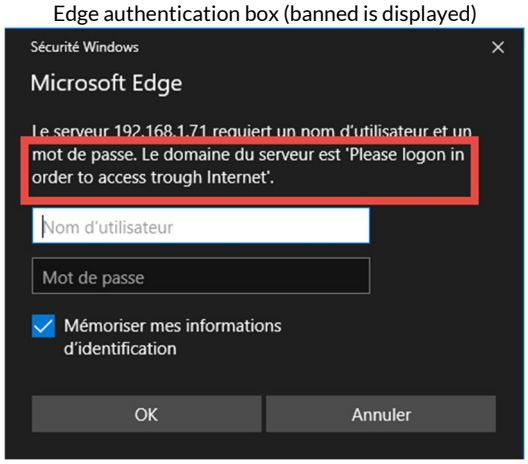
Chrome authentication box (no banner displayed)



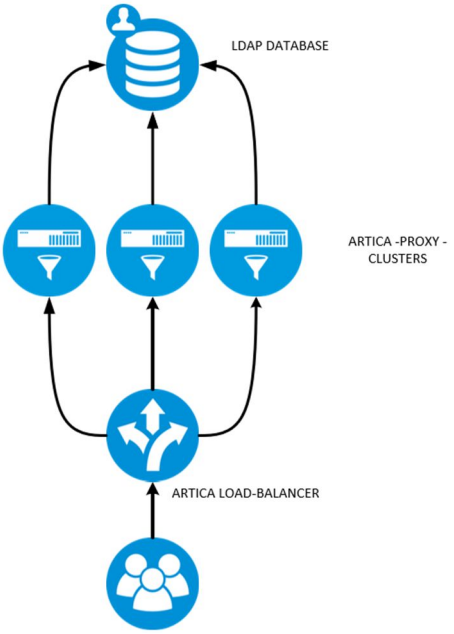
FireFox authentication box (banner is displayed)



Edge authentication box (banned is displayed)



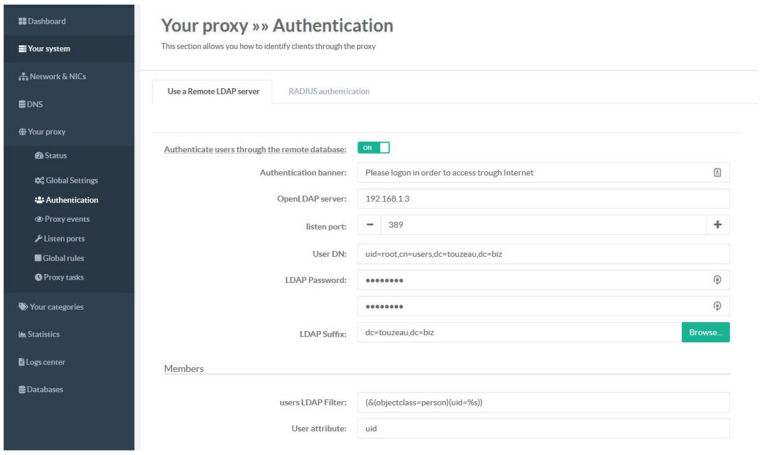
Use a Remote LDAP Database



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 (

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



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

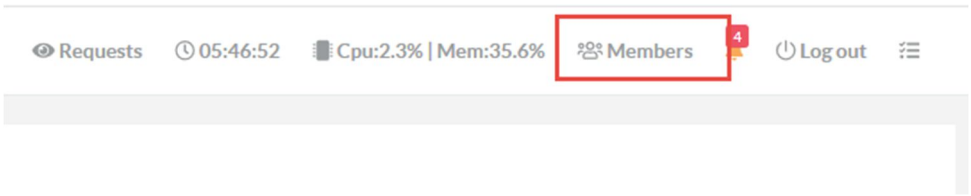
Field	Value
User DN:	uid=root,dc=company,dc=com
Users LDAP Filter:	(&(objectclass=person)(uid=%s))
User attribute:	uid
Search members in groups:	(&(memberUid=%u)(member=*))
Attribute:	member
Groups search filter:	(&(objectclass=posixGroup)(cn=%s))
Group attribute:	cn

Example: Like Active Directory

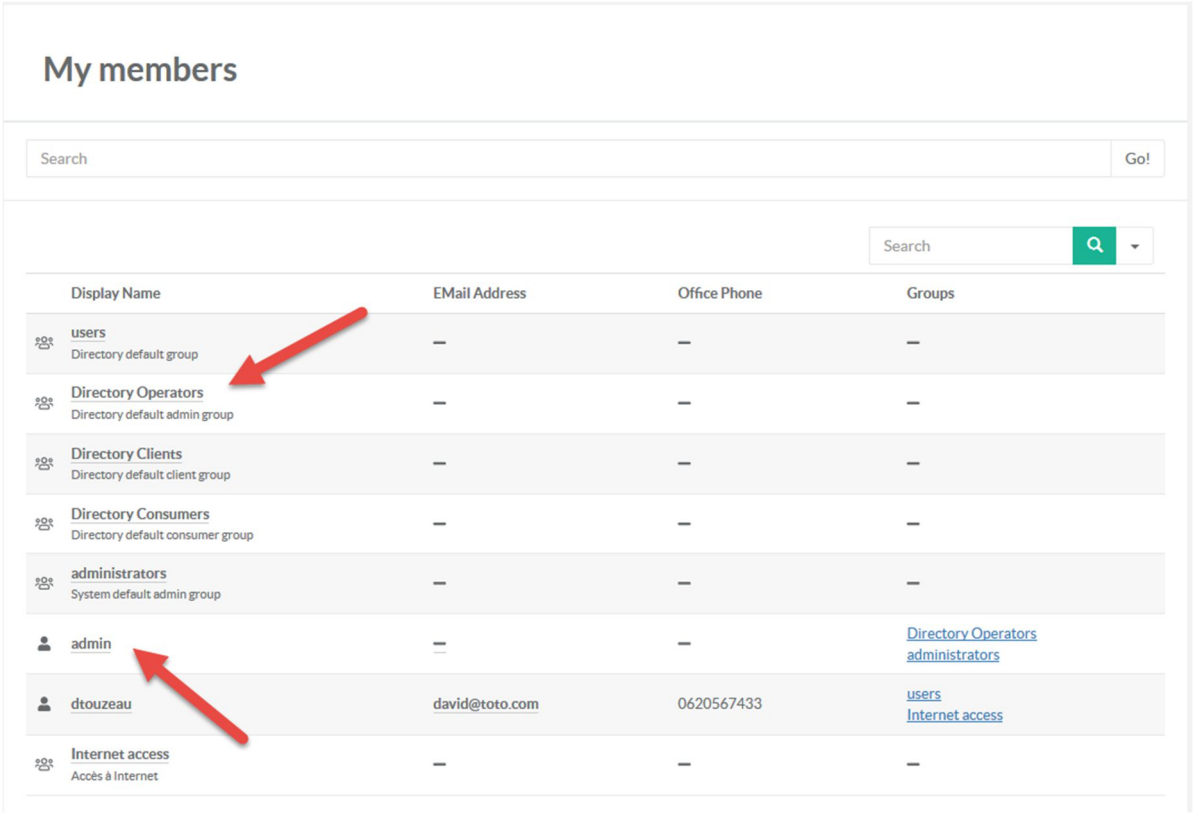
Field	Value
User DN:	root@company.com
Users LDAP Filter:	sAMAccountName=%s
User attribute:	sAMAccountName
Search members in groups:	(&(objectclass=person)(sAMAccountName=%u)(memberof=*))
Attribute:	memberof
Groups search filter:	(&(objectclass=group)(sAMAccountName=%s))
Group attribute:	sAMAccountName

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.

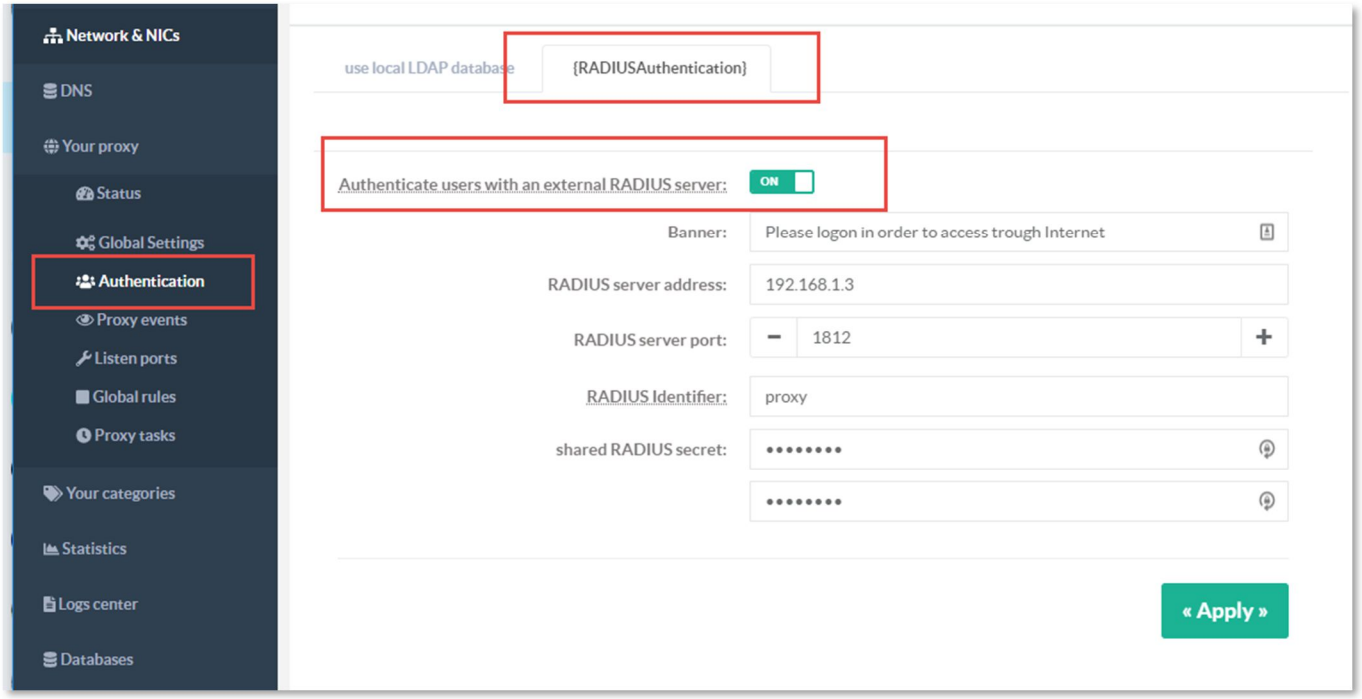


Views are only in read-only mode but if you see correctly your users and groups, this means your LDAP search patterns parameters are correct.

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



- 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.

Use Active Directory

Artica is compatible Active Directory on Microsoft Windows 2000,2003,2008,2012,2016,2019 (THIS FEATURE REQUIRE AN ENTERPRISE LICENSE).
The main benefit using the Active Directory is the "silent authentication" means the browser automatically sends the Windows session credentials to the proxy using NTLM or Kerberos method.
In this case, the user did not have to put its credentials in a login box.

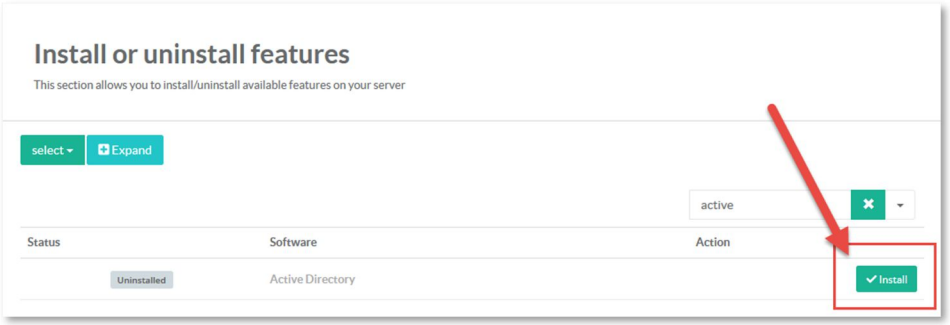
How to join Artica to your Active Directory server?

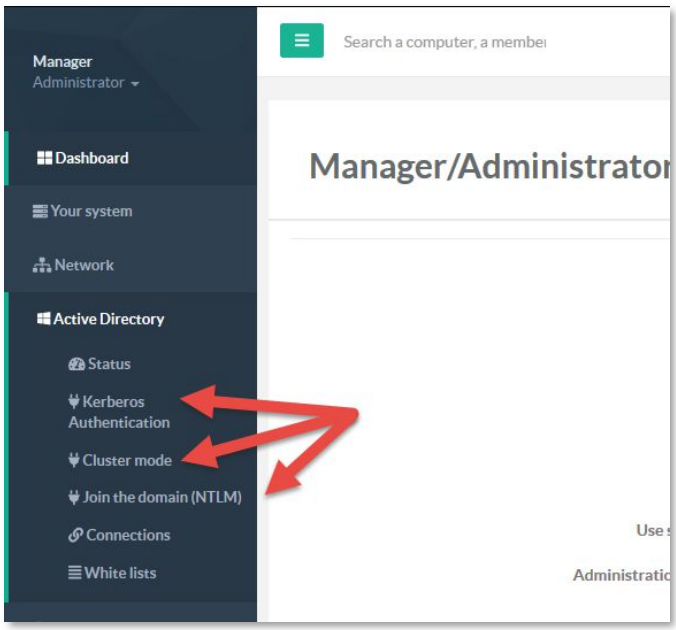
You need to follow these requirements:

- The Artica server hostname must be fewer than 16 characters.
- The server domain name must be the same of your Active Directory domain.
- The Artica server must correctly resolve the Active Directory domain (in most cases the first DNS used by Artica should be the Active Directory server).
- The time must be the same between the Artica server and the Active Directory server name.(in most cases, use the Active Directory as time server)
- The Account used must have "join" domain privileges.

Join the Microsoft domain.

After checking all these topics, go to the "**Your system/Features**" on the left menu, search the item "**Active directory**"
Click on "**Install**" to enable the feature.





After enable the feature, a new "**Active Directory**" menu is displayed.

In this menu, you have 3 main sections:

Kerberos Authentication: Connect your server to a Windows 2003,2008,2012,2016,**2019** using "**Kerberos native connection**"

Cluster Mode: Connect several Artica servers using Kerberos native connection with the Load-balancing service.

Join the domain (NTLM) Connect your server to a Windows 2003,2008,2012,2016 using "NTLM connection"

select the method you want to "**Join the Microsoft domain**".

Each section will ask to you required settings

Note: To obtain all required information, with PowerShell on your Active Directory server, type "`Get-ADDomain`"

- **Allows Active Directory users to logon**: Allow users to be connected to the Artica Web console using their Windows credentials
- **Active Directory full hostname**: Set the Active Directory full server name
- **Netbios AD domain**: Set the Windows workgroup displayed on the network
- **Suffix**: The Active Directory LDAP suffix.
- **Computers AD location**: Which LDAP branch to store the Artica server
- **Windows server type**: Your version of your Active Directory server.
- **Administrator**: The user that have join workstation privileges to the domain.

Kerberos or NTLM ?

There are differences between these 2 methods.

Kerberos native authentication method
Basically, Kerberos Authentication is the modern method to join the domain.

- It is not compatible with old system such as Windows 2000, Windows XP and Windows 2003.
- On browsers settings you must define **the full proxy hostname** (not the IP address)
- See (https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-kerberos)

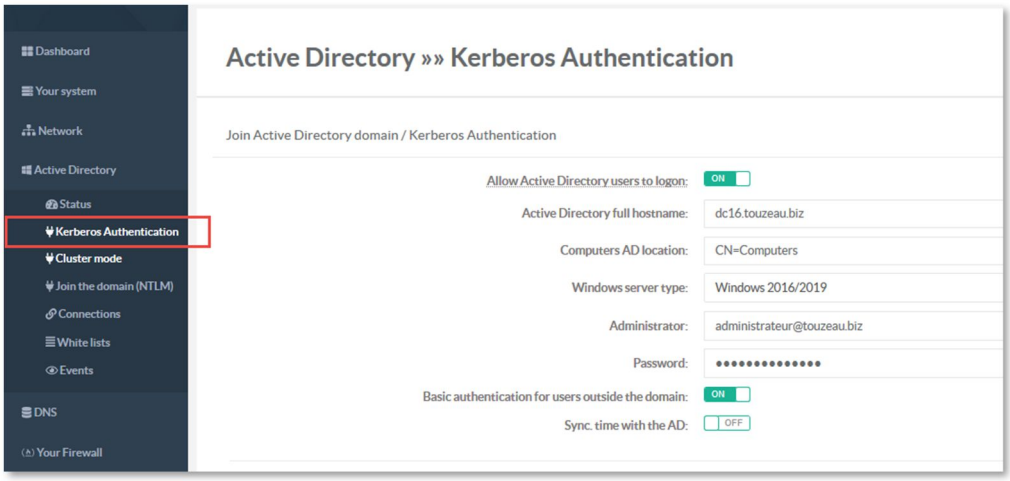
NTLM standard method:

Is a very old method used to communicate in the Microsoft domain
It is compatible with all systems.
It is not compatible with Windows 2019 Active Directory and later
It is less secure (password is in clear text when sniffing the network).
See (https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-ntlm)

Basically, if you did not have any Windows XP/2003 in your network, use the Kerberos method.

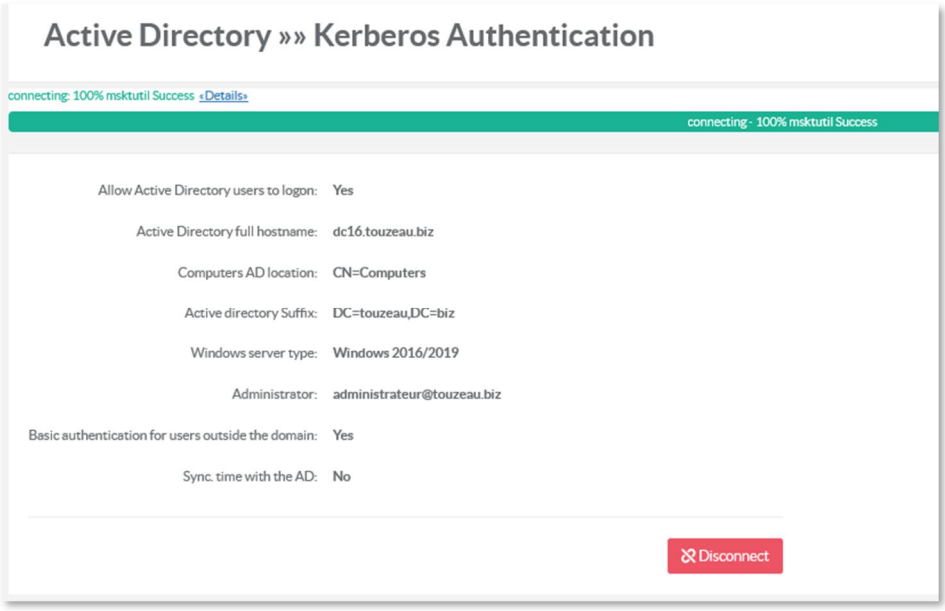
Use the Native Kerberos

The native Kerberos allows you to connect your Artica server to the Active Directory using the Kerberos method.
Fill the form properly



- **Allow Active Directory users to logon**: Active Directory members can logon to the Artica console using their Active Directory credentials.
- **Active Directory full hostname**: The FQDN name (hostname.domainname) of the Active Directory server
- **Computers AD location**: The branch where to store the computer item in the Active Directory
- **Windows server type**: Define the encryption level according the version of your Windows server
- **Administrator**: Administrator (email format) that have **join** privilege
- **Basic authentication for users outside the domain**: Provide a basic authentication (popup) If a computer is not linked to the Active Directory domain (inside the popup, the user must enter the value of the "**sAMAccountName**" ldap attribute
- **Sync. time with the AD**: If the Active Directory provide NTP service, Artica will synchronize it's time with the Active Directory server

If the Active Directory connection is a success, the form will be locked and allows you to only disconnect from the AD.



Dedicated administrator account

If you need to create a dedicated account with limited privileges for Artica, follow this video https://youtu.be/8-V6UanZTew

Use the Native Kerberos for Load-balancing and cluster environments.

If you plan to use a load-balancer or the Artica Load-balancer feature using Kerberos authentication, you have to follow this method.

Create a dedicated user:

Create a new user **that never expires**.
Open users **Properties/Account** tab and set the "Do not require Kerberos preauthentication" checkbox.

Configure IP address and DNS settings

Create A and PTR records for your Artica proxy hostname on your DNS server. (usually the Active Directory itself)
Make sure Windows workstations can resolve your Artica proxy hostname name to IP address and Ip address can be reversely resolved to your Artica proxy hostname.

Synchronize time

For the Kerberos authentication to work correctly it is a MUST to have synchronized time on proxy and your Active Directory domain controllers

On the left menu, choose "**Kerberos Authentication**"

Fill the form properly using this way:

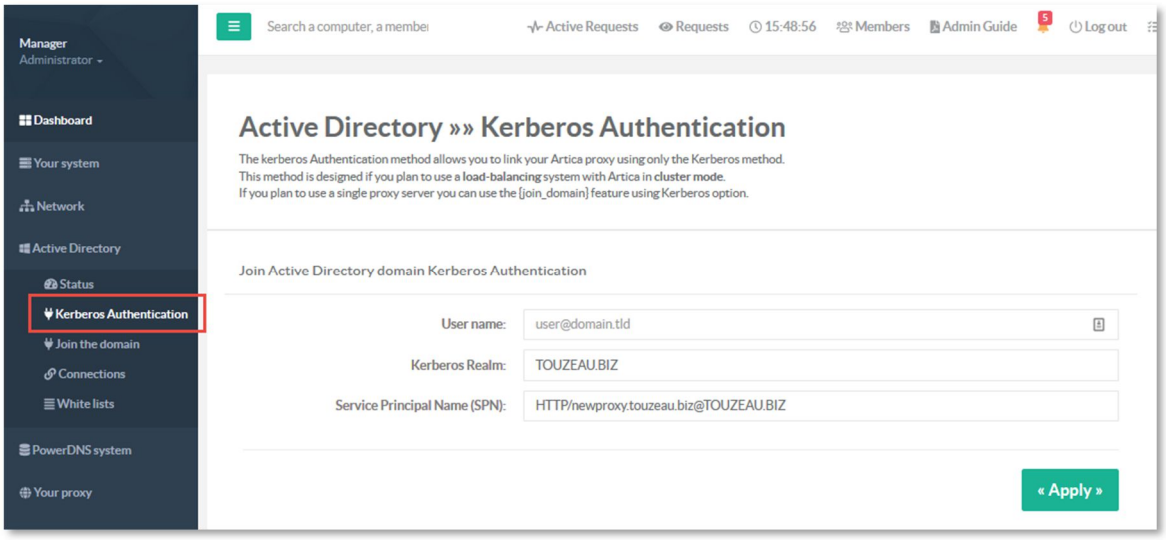
Username and password
This is the username and password you have created with the **Do not require Kerberos preauthentication** option
The username must be set as an email address example: "articaproxy@company.corp"

The Active Directory full hostname
This is the FQDN of your Active Directory server example: dc1.company.corp

FQDN of secondary DC
Fully qualified domain name of your second domain controller. For example, "dc2.company.corp".
This setting is optional and does not need to always be filled in.
If your first domain controller goes down for routine maintenance the application will use second domain controller for LDAP group lookup and authentication.

Kerberos realm
This is usually the UPPERCASE letters of your Active Directory domain. For "company.corp" domain it will be COMPANY.CORP.
Please note that Kerberos realm is always uppercase.

For example:

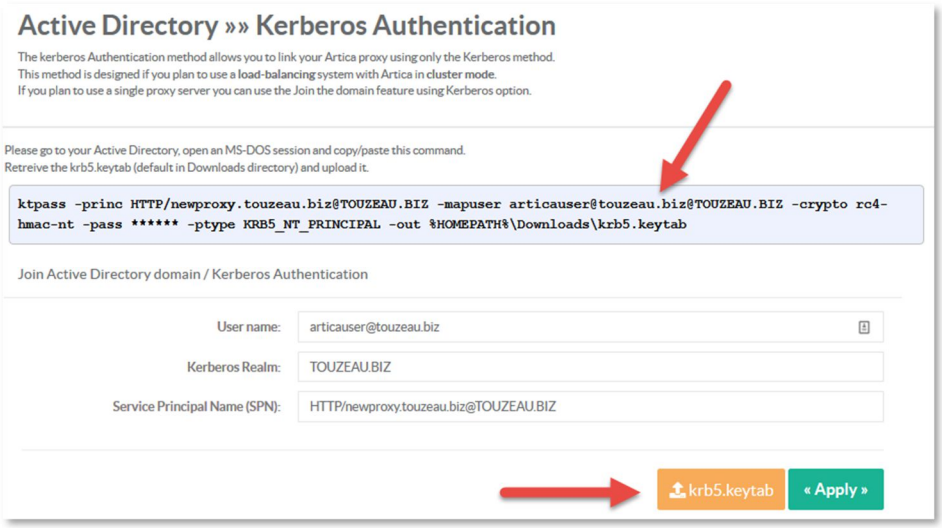


Submit the form.

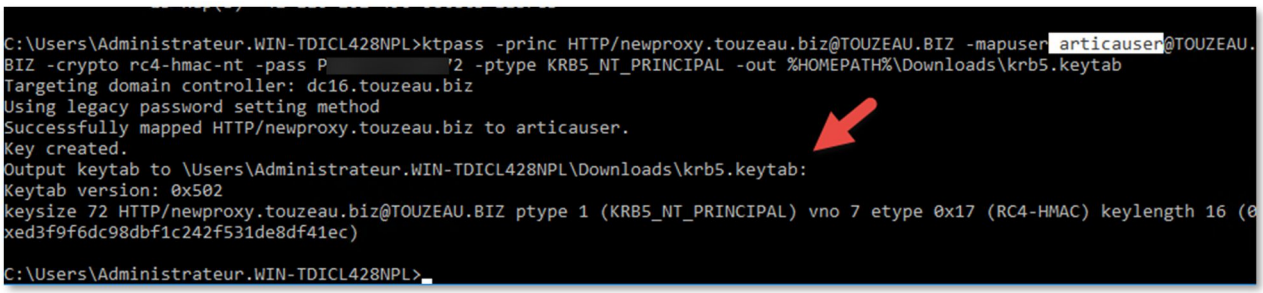
Generate the Kerberos ticket on your Active Directory

After submitting the form, the web page displays a command-line according to the information saved.

It shows you the Service Principal Name (SPN). The Service Principal Name (SPN) - is the Kerberos principal that will be used by the connecting browsers for authentication. It is usually constructed from the FQDN of your Artica proxy and Kerberos realm automatically.



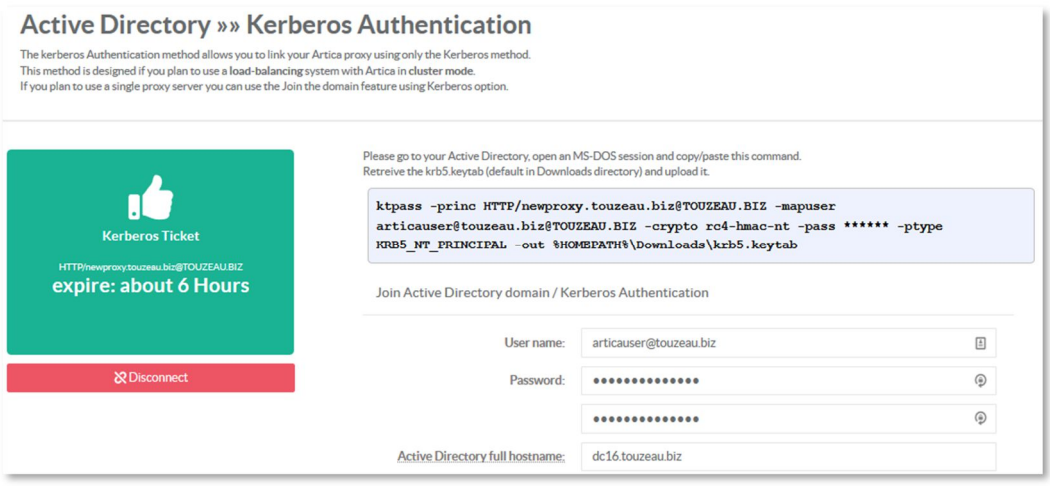
Go to your Active Directory and run the copied command-line:



There should ONLY be ONE user mapped to a given SPN.
If you have two or more different users mapped to a given SPN record Kerberos authentication will ALWAYS FAIL

Upload the Kerberos ticket

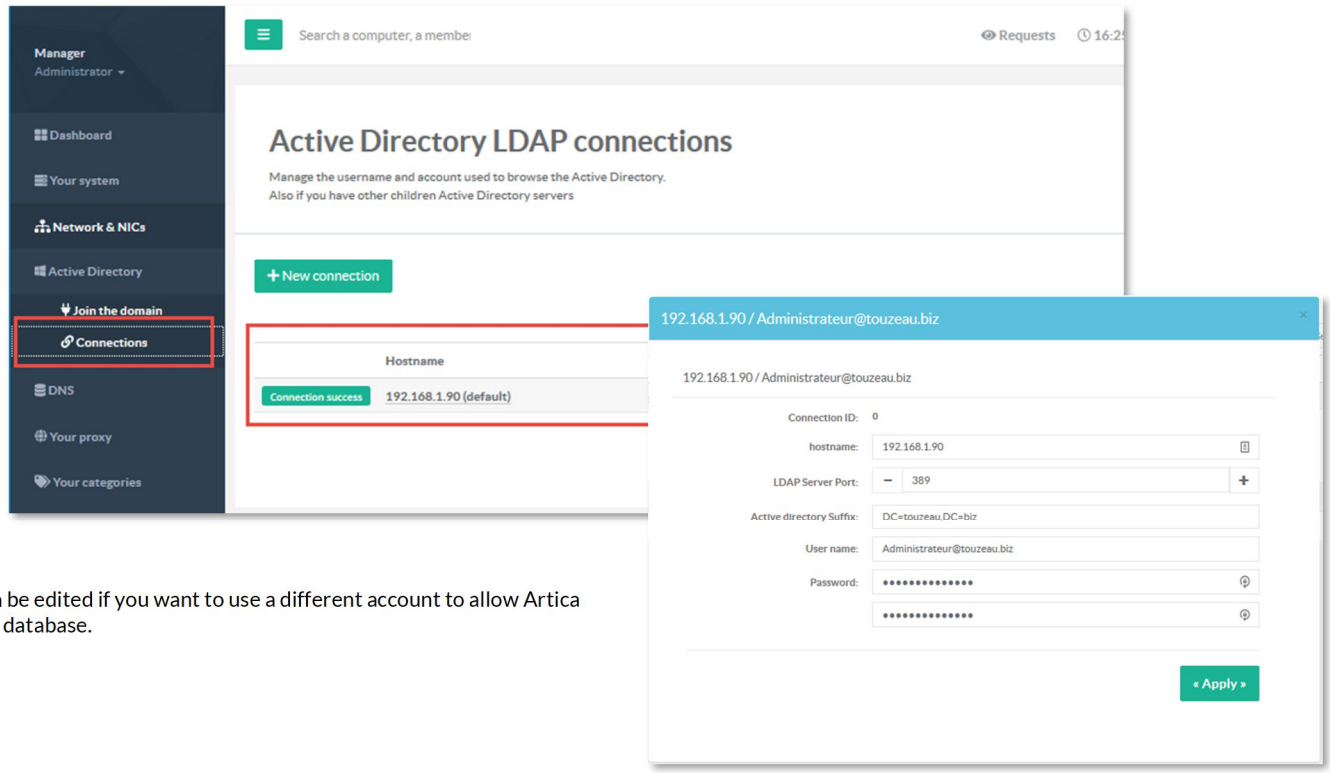
Retrieve the krb5.keytab file and upload it using the button **krb5.keytab**



If the connection is successful you can see the expire time of the Kerberos ticket (automatically renewed)
In a cluster environment if you link the Active Directory from the master, Kerberos ticket and Active Directory information are automatically replicated.

Verify the LDAP connection

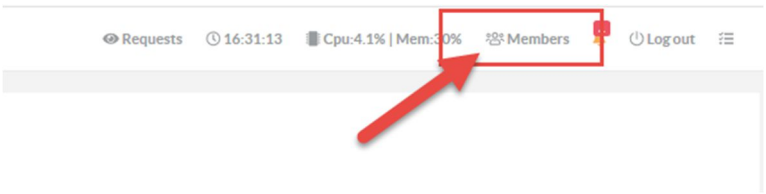
After connecting to the Active Directory domain, open the menu "**Connections**"
This section lists the "**LDAP connections**" to the Active Directory.
It helps Artica to retrieve groups and members thought your Active Directory LDAP service (389 port).
Your Active Directory connection is listed here and must be "success".

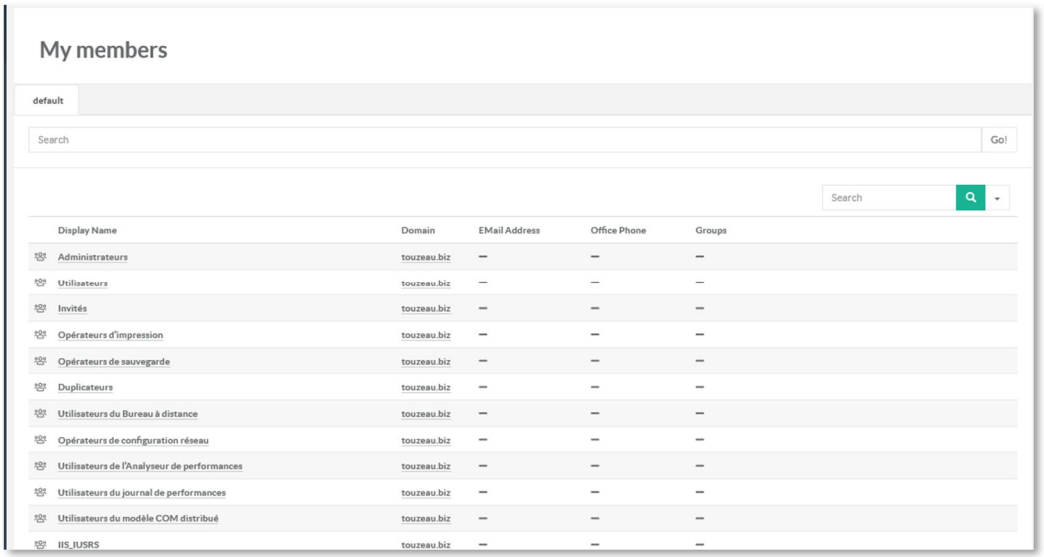


This connection can be edited if you want to use a different account to allow Artica browsing the LDAP database.

Active Directory users and groups

On the TOP menu, click on the "Members" link.
This section allows you to browse the Active Directory database in "read-only" mode.

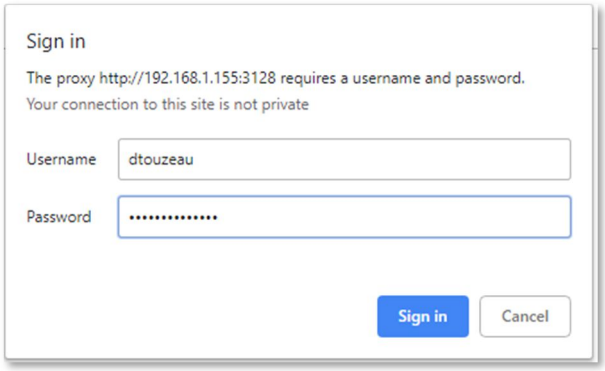




What about users outside the Windows domain?

By default, the proxy is defined in "Mixt mode", Kerberos/NTLM for workstations joined to the Microsoft domain and basic authentication with computers outside the domain such has Linux/Unix boxes/workstations.

User just needs to put its login name and password like this screenshot, do not use DOMAIN\USER or DOMAIN/user or user@domain



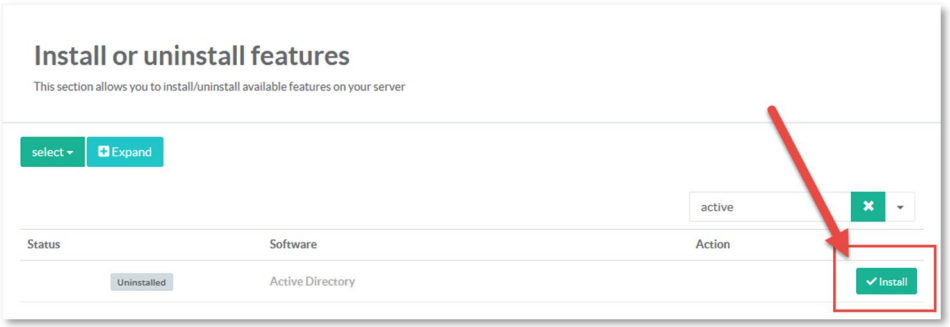
Connect your Artica server using NTLM

You need to follow these requirements:

- You Active Directory server version is 2003,2008,2012 or 2016 (not after 2016 – 2019 is not NTLM compatible)
- The Artica server hostname must be fewer than 16 characters.
- The server domain name must be the same of your Active Directory domain.
- The Artica server must correctly resolve the Active Directory domain (in most cases the first DNS used by Artica should be the Active Directory server).
- The time must be the same between the Artica server and the Active Directory server name.(in most cases, use the Active Directory as time server)
- The Account used must have "join" domain privileges.

Enable the Active Directory feature.

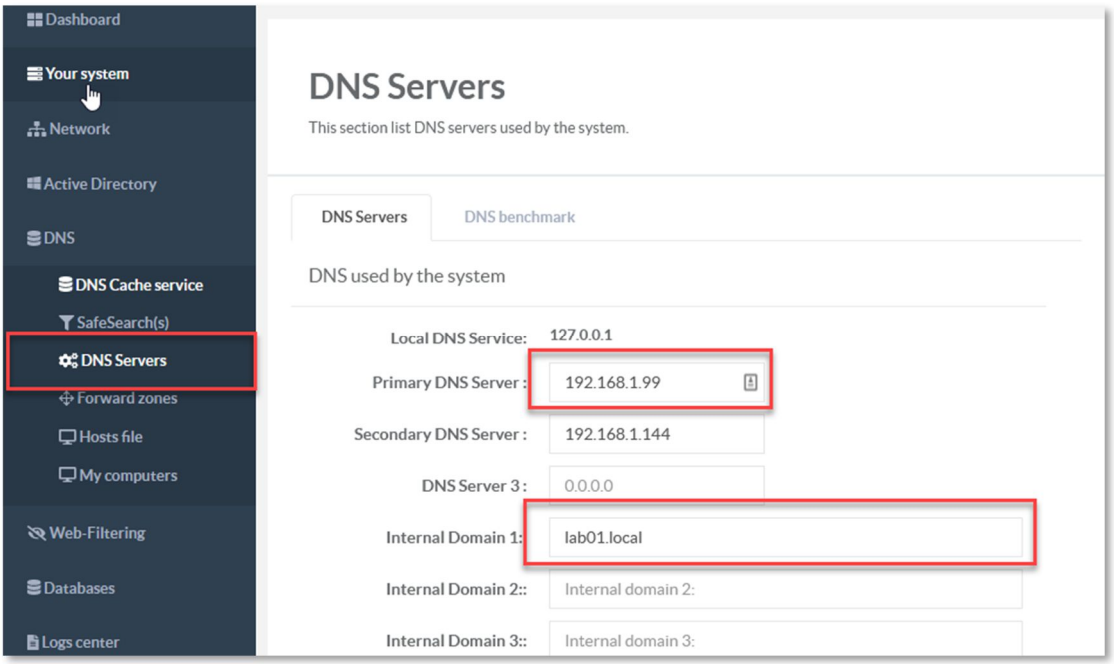
After checking all these topics, go to the "**Your system/Features**" on the left menu, search the item "**Active directory**"
Click on "**Install**" to enable the feature.



Check your DNS settings

Under **DNS/DNS servers**, checks that the Primary DNS server is your Active Directory server and the **Internal Domain 1** is your Active Domain suffix.

Our example: Active Directory server is **192.168.1.99** (DNS service) and or Active Directory hostname is



Join the domain

Select Active Directory/Join the domain (NTLM) on the left-menu

Set the full hostname under “Active Directory Full hostname” field

Set the Workgroup domain name of your Active Directory under “**Netbios AD Domain**” field

Set the domain of your Active Directory server un der the “Active Directory suffix” field

If your Active Directory server require LDAP SSL connection, turn on the “**Enable SSL**” checkbox.

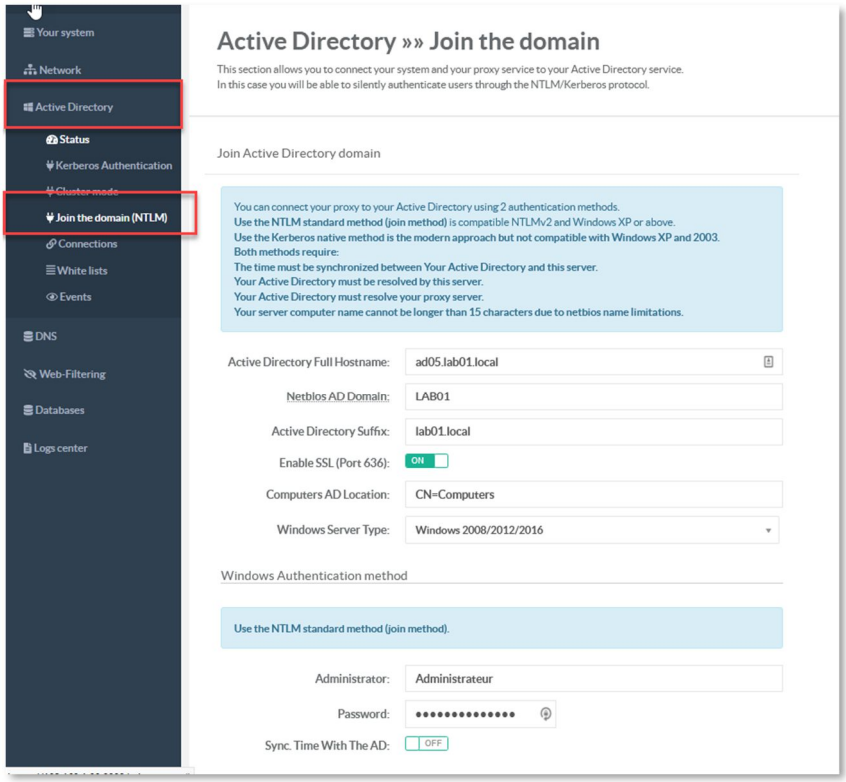
By default, when joining the domain, the Artica server will be saved in the “**CN=Computers**” branch.

If you plan to use a different branch, set it in “**Computers AD Location**” (Without the suffix)

According NTLM is not supported on Windows 2019, choose in the “Windows Server type” drop-down if your Active Directory server is a 2003 or a 2008 (or higher) version.

Define the “**Domain Administrator**” username and password to join the Active Directory domain.

USING SSL STILL REQUIRES THE 389 PORT TO BE OPEN TO THE ACTIVE DIRECTORY.



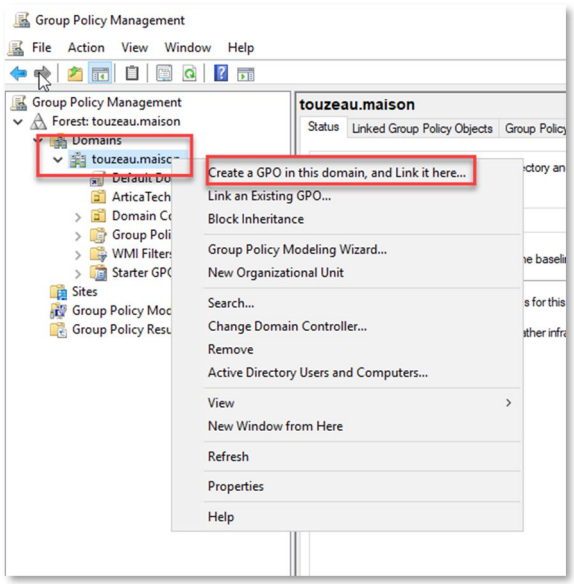
Configuring Proxy Settings via GPO on Windows 10/Windows Server 2016/2019

Use Active Directory Group Policies (GPO) features to configure proxy settings on domain-joined computers running Windows 10 and Windows Server 2019/2016/2012R2. These proxy server settings are used by all modern browsers, including:

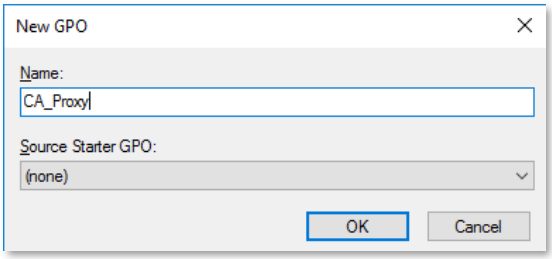
- Internet Explorer 11,
- Google Chrome,
- Chromium-based Edge,
- Opera
- Mozilla Firefox (with the option Use system proxy settings enabled by default).

Create the GPO

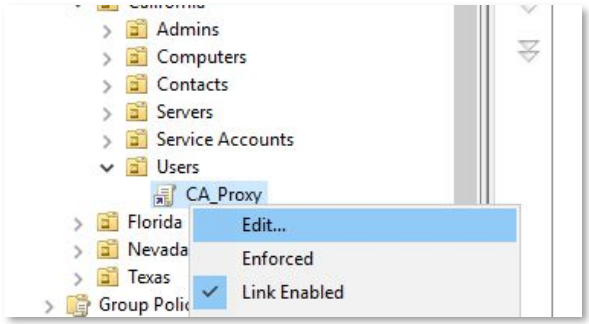
- Open Group Policy Management Console (**gpmc.msc**) on a computer running Windows 10 or Windows Server
- Select the Active Directory organization unit (OU) for which you want to apply the new proxy settings.
- Right-click on OU and select **Create a GPO in this domain and link it** here;



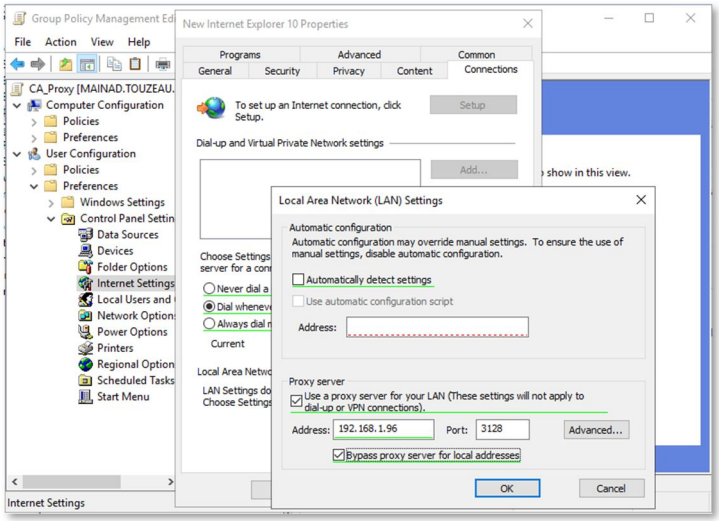
- Specify a policy name, for example **CA_Proxy**;



- Click on the policy and select **Edit**;
- Expand the following section:
  - User Configuration
  - Preferences
  - Control Panel Settings
  - Internet Settings.
  - Right click and select New Internet Explorer 10 (this policy will also be applied for the IE 11);



- On the standard windows with the Internet Explorer settings, go to the **Connections** tab and press **LAN Settings** button.
- Turn ON the checkbox "**Use a proxy server for your LAN**" and specify the Address and Port of your proxy server (for example 192.168.1.11, port 3128).
- To enable this option, **press F6 button** (underline for that setting will change the color from red to green).
- To **disable** specific policy setting press **F7** (disable the option "Automatic detect settings" this way).



TIP. THE GREEN UNDERSCORE FOR THE IE PARAMETER MEANS THAT THIS POLICY IS ENABLED AND WILL **BE APPLIED THROUGH GROUP POLICY**.
RED UNDERLINING MEANS THAT THE SETTING IS CONFIGURED, BUT DISABLED FOR USERS' COMPUTERS.

TO ENABLE ALL SETTINGS ON THE CURRENT TAB, PRESS **F5**. TO DISABLE ALL POLICIES ON THIS TAB USE **F8** KEY.

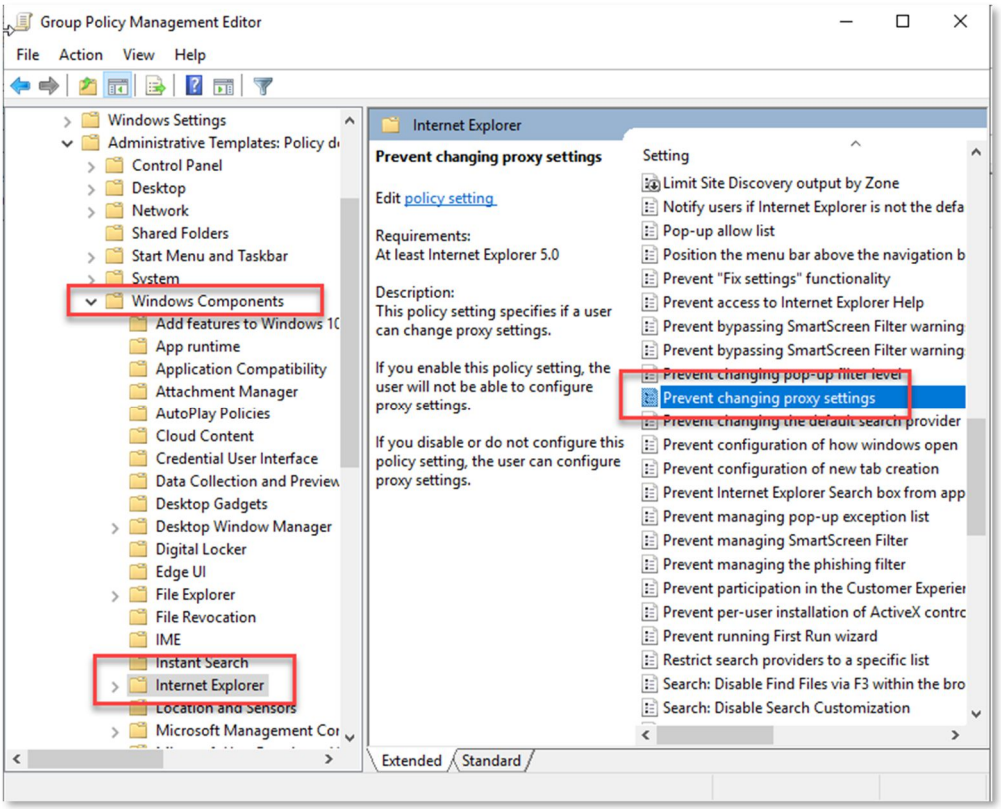
- Press OK twice to save settings.

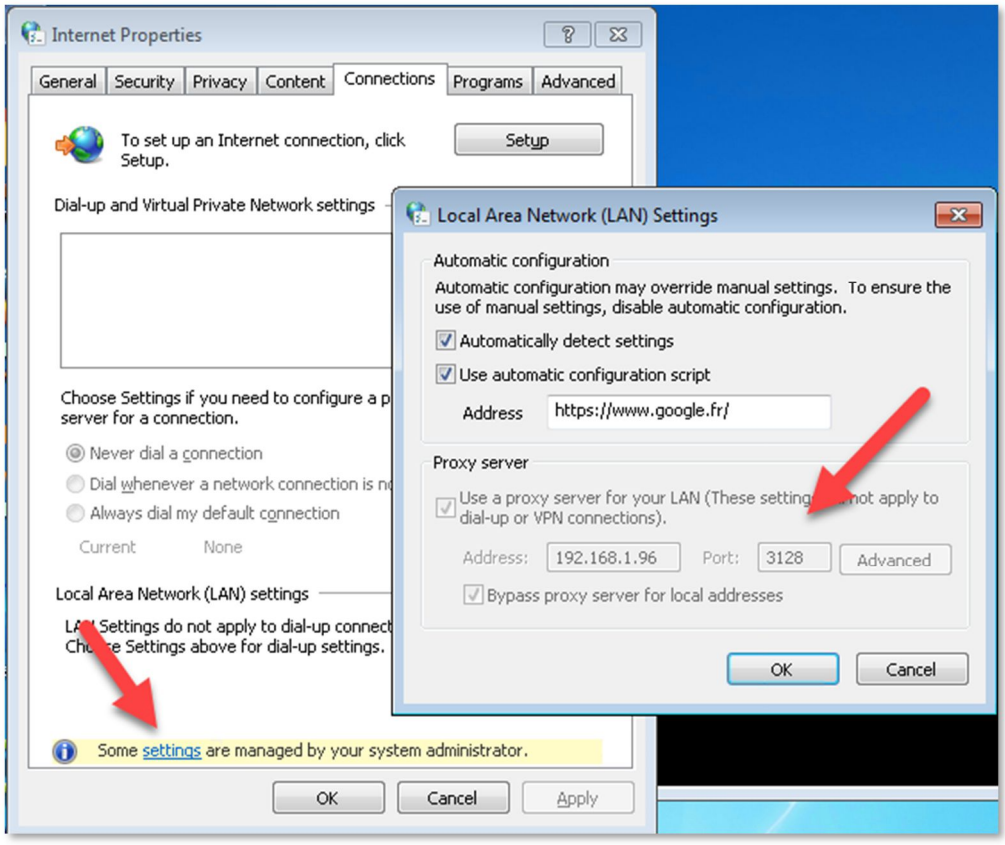
Note. This rule only works for Internet Explorer 10 and Internet Explorer 11. For earlier IE versions, you need to create separate rules.

Prevent Changing IE Proxy Settings Using GPO

In "GPMC.msc" console, create a new GPO and switch to the Edit mode. Open :

- User Configuration
- Policies
- Administrative Templates
- Windows Components
- Internet Explorer section
- Enable the policy **Prevent changing proxy settings**.





Restful API

If the RESTful API is enabled on the "system" section, you can send a REST command to turn ON the Active Directory.
This command adds Active Directory settings and join the Artica server to the domain.

```
POST https://192.168.1.1:9000/api/rest/system/activedirectory/settings
```

Inside the POST, define an array like this example:

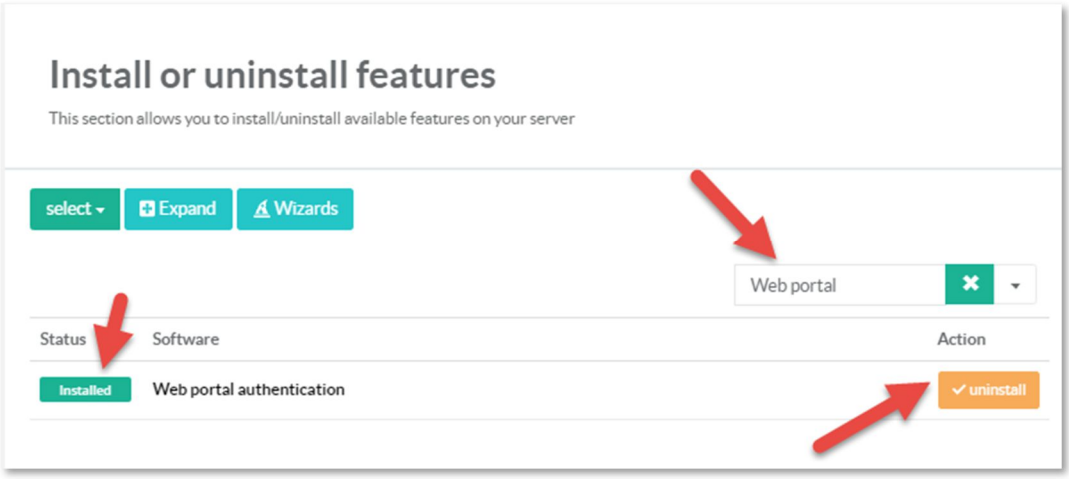
```
$ch = curl_init();
$CURLOPT_HTTPHEADER[]="Accept: application/json";
$CURLOPT_HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT_HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT_HTTPHEADER[]="Expect:";
$CURLOPT_HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5";

$MAIN_URI="https://192.168.1.173:9000/api/rest/system/activedirectory/settings";


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);

//WINDOWS_SERVER_TYPE: WIN_2003 or WIN_2008AES for 2008 > 2016
//WindowsActiveDirectoryKerberos 1 = Full kerberos, 0 = NTLM


$POSTz= array("
WINDOWS_SERVER_TYPE"=>"WIN_2008AES",
"ADNETBIOSDOMAIN"=>"LABO",
"ADNETIPADDR"=>"192.168.1.23"
"fullhosname"=>"dc01.labo.corp",
"WINDOWS_SERVER_NETBIOSNAME"=>"dc01",
"WINDOWS_DNS_SUFFIX"=>"labo.corp",
"COMPUTER_BRANCH"=>"cn=computers",
"WINDOWS_SERVER_ADMIN"=>"Administrator",
"WINDOWS_SERVER_PASS"=>"Password",
"WindowsActiveDirectoryKerberos"=>0);



curl_setopt($ch, CURLOPT_POSTFIELDS, $POSTz);

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

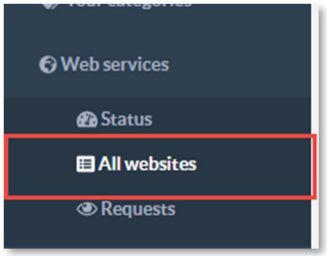
Use an authentication portal (Hotspot)

An authentication portal allows your users to authenticate using a web authentication form.
This feature is useful if you turn your proxy in a "mixed mode" (transparent and connected mode).

Install the "Web portal authentication" service

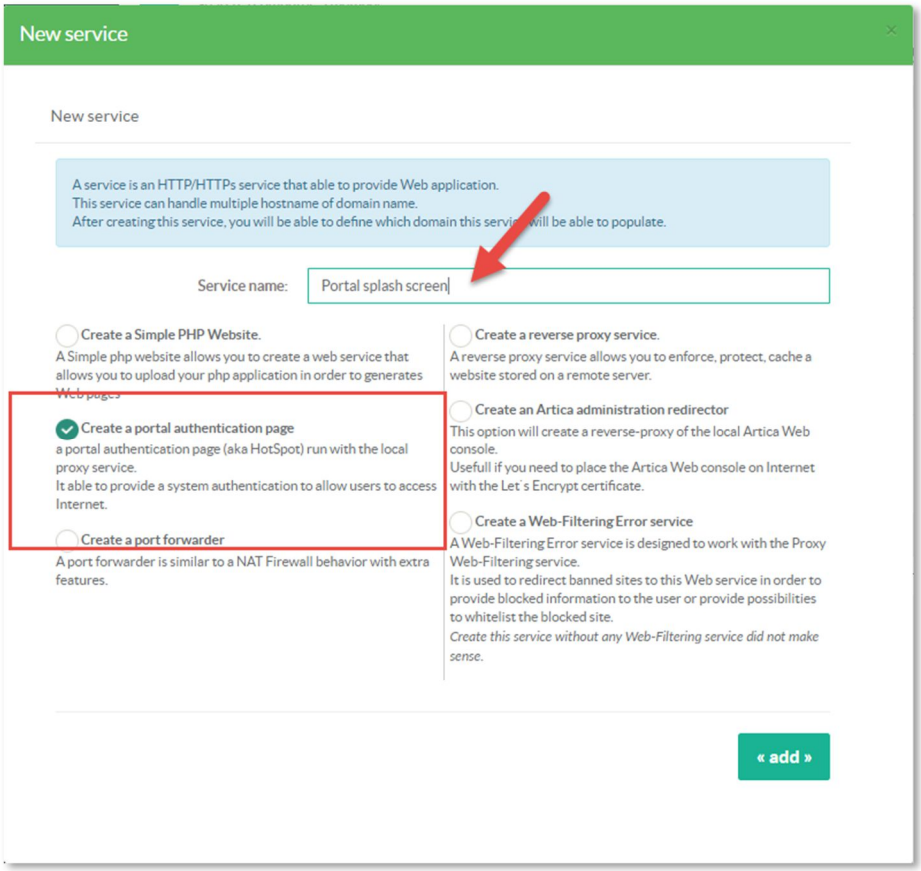
On the features section, in search field, type "**Web portal**"
Click on install button on the "**Web portal authentication**" row.



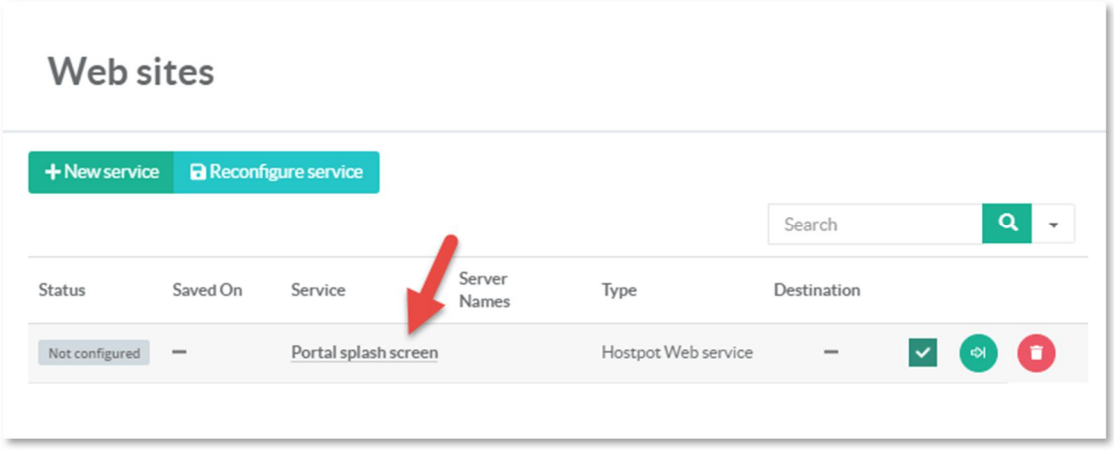


Install the "Web portal splash screen"

The first install trough the features section installs the Nginx service, you will find **"Web services"** on the left menu.
Select the "**All websites**" submenu.
Click on the button "**New service**"
Set the name of the service and choose "**Create a portal authentication page**"

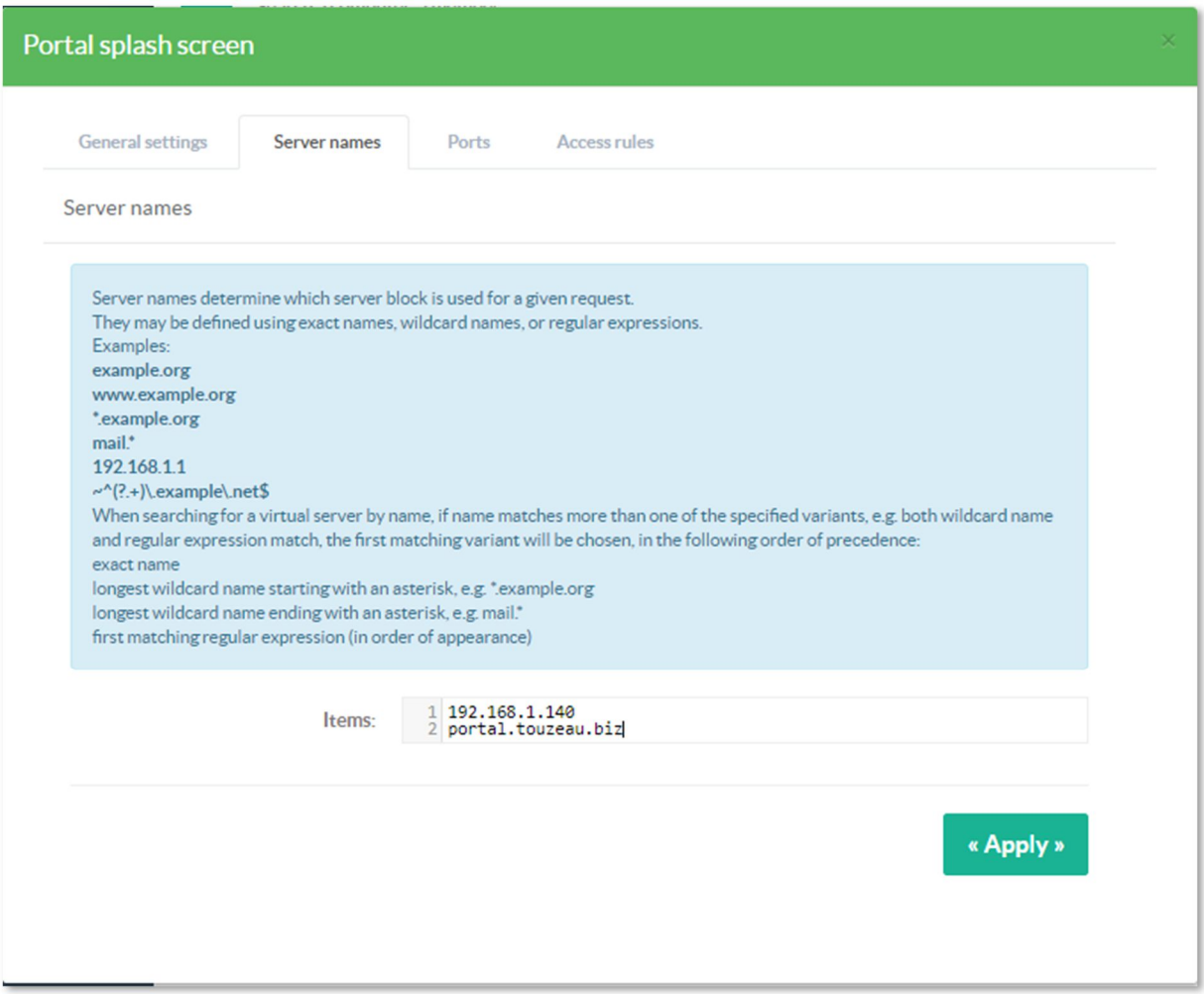


Your Web service appears to "**Not configured**".
You need to setup ports and server names before make the service available.
Click on the added service.



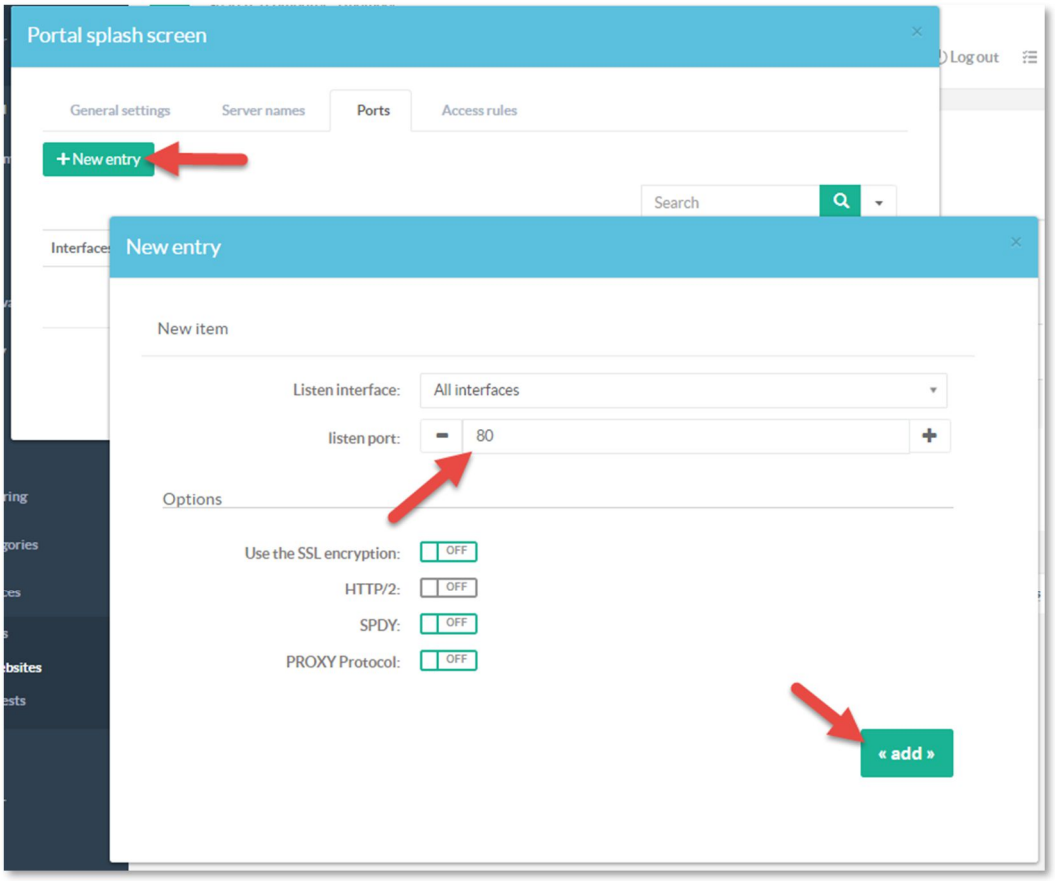
Select the "**Server names**" tab.
Under items, put all hostname or IP addresses that this service can handle as a "**virtual host**"

If you using only this service you can use the "*" character that will catch all requests to the defined ports.

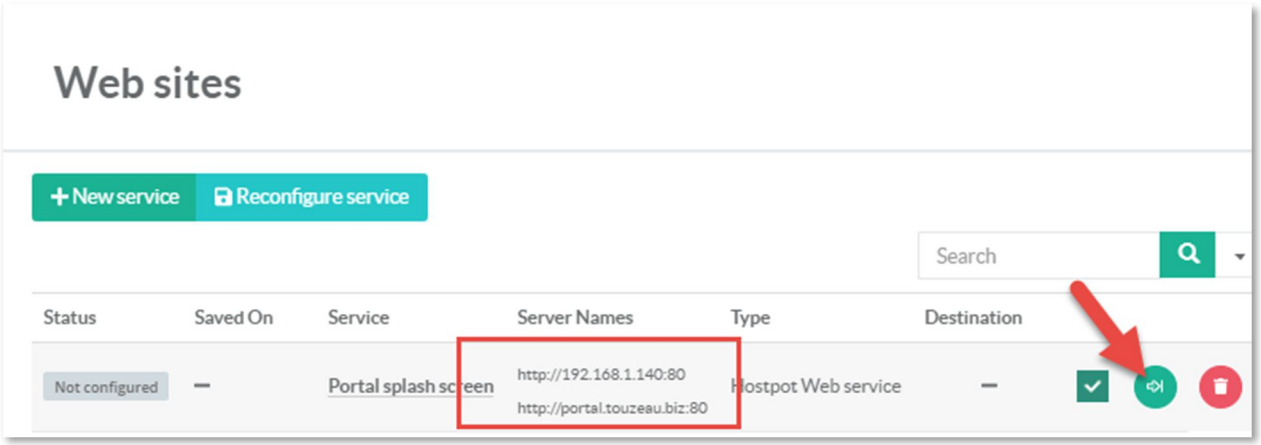


Choose **Ports** tab.

Click on "**New entry**" in order to add a port to listen.
Choose the listen Interface and the port number
Click on Add button.



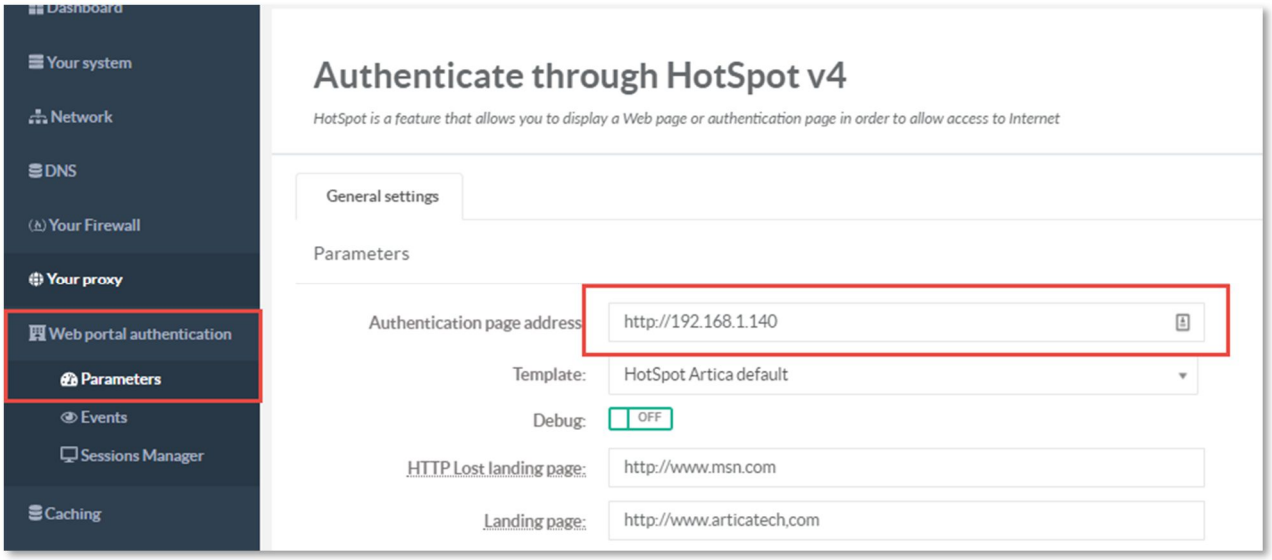
The main table list all addresses of your web service, click on the green arrow in the row in order to compile your new web service and make it available



After the compilation, the status must be turned to "**OK**" instead of "**Not configured**"

Setup the "Web portal authentication"

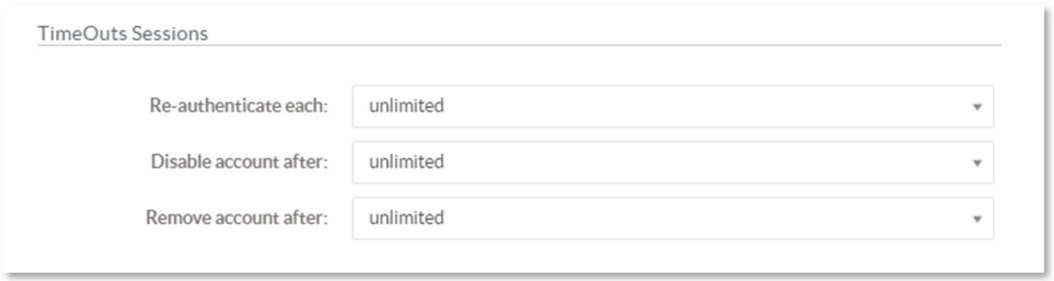
On the left menu, choose "**Web portal Authentication**" and choose "**Parameters**"



Authentication pages addresses

- Define the **URL** to the Web portal splash screen you have defined in the Web services section in the **Authentication page address**.
- Choose the "**Template**" in order to define the **design** of your authentication page.
- Define an HTTP URL in the **Lost landing page field**.
  This URL is used if the Web authentication page did not have necessaries information in order to redirect again the user.
- Define the **Landing page:** When the user is successfully logged, it will redirect to this web page.

Timeouts sessions



Timeous session set the time to live of a session and the account.

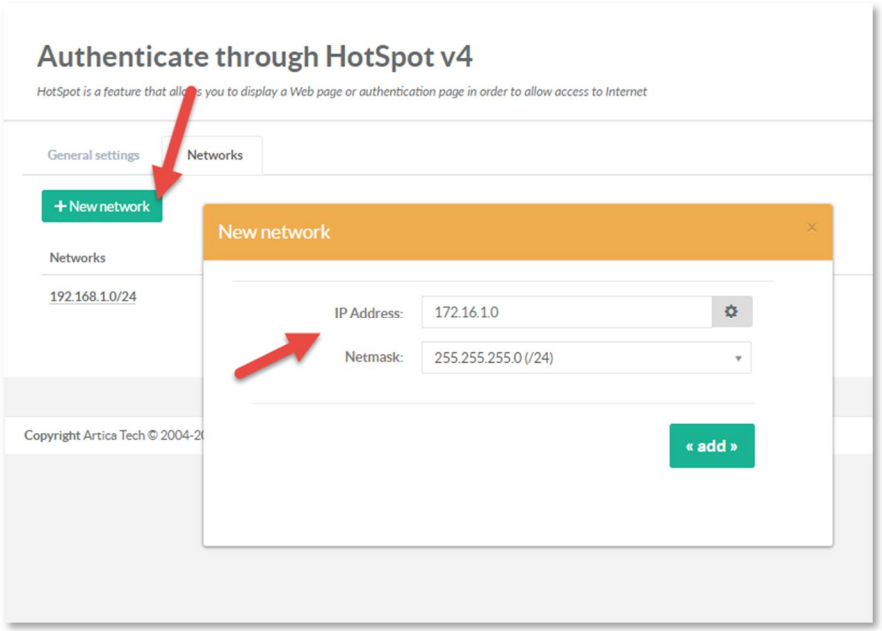
- **Re-authenticate each define** the time of the open session.
  After expired time, the user must be re-authenticated again.
- **Disable account after** define the time to disable the account.
  After expired time, the user cannot use its account to be authenticated.
- **Remove account after** define the time to completely remove the account:
  After expired time, the account will no longer exists on the database.

Note: Disable account and remove account is not used by the engine when account is stored in the Active Directory or LDAP database.

Networks section

By default, the proxy will redirect all anonymous sessions to the Web portal authentication page.
If you want only some networks to be authenticated, click on the **Network** tab.

Add networks you want to authenticate using Web portal authentication page.

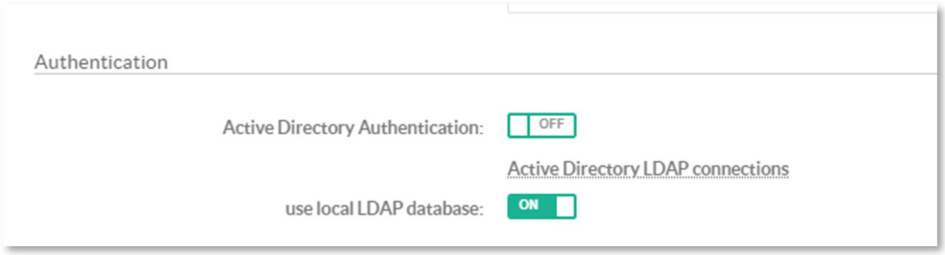


How to Authenticate users?

By default, the Web authentication page check credentials against all members databases connected to Artica.
This means:

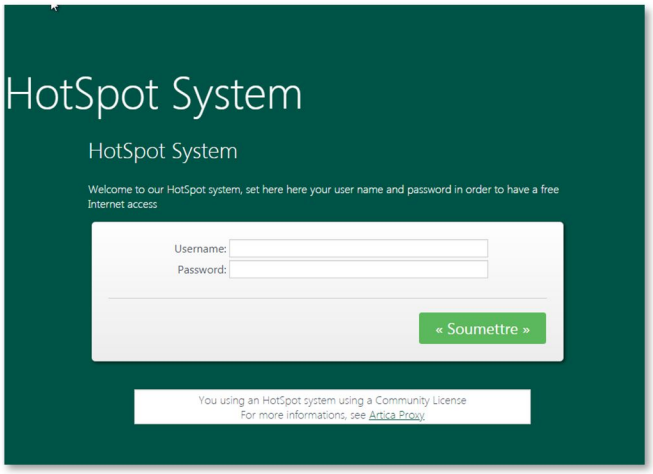
- Any Active Directory connection.
- The Local LDAP database if installed.

The Authentication section allows you to enable user's database engines.



If only authentication is defined, the splash screen displays only the from to be authenticated.

Note: The LDAP users and Active directory will use the user@domain as the username

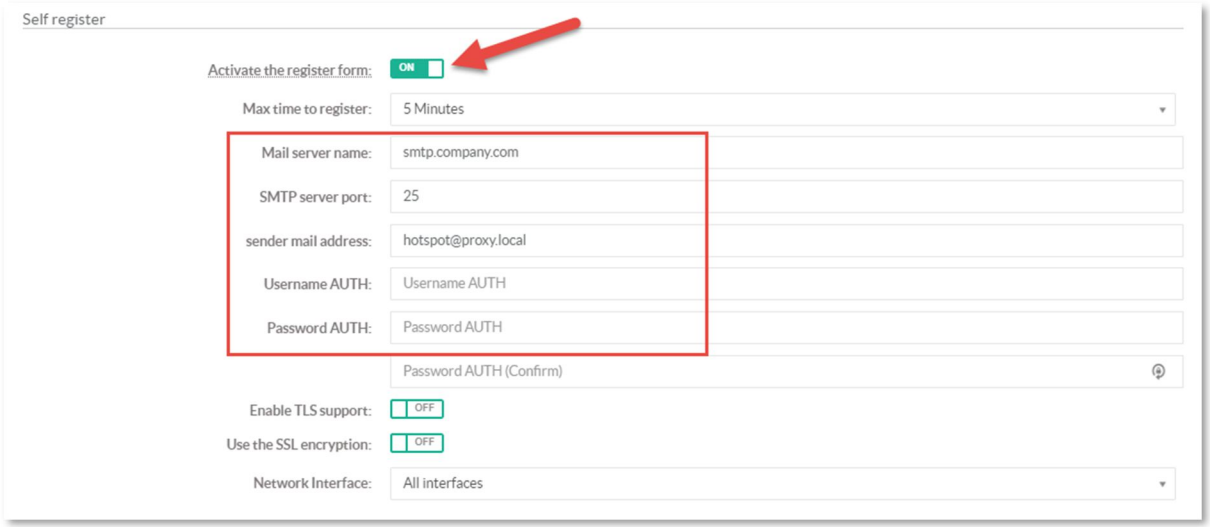


Self register

Self-register is a feature that allows your users to enter their eMail address in order to create their account on the system.
After register the eMail address, members have 5minutes (Max Time to register option) to retrieve the message sent by the proxy in order to confirm the registration.

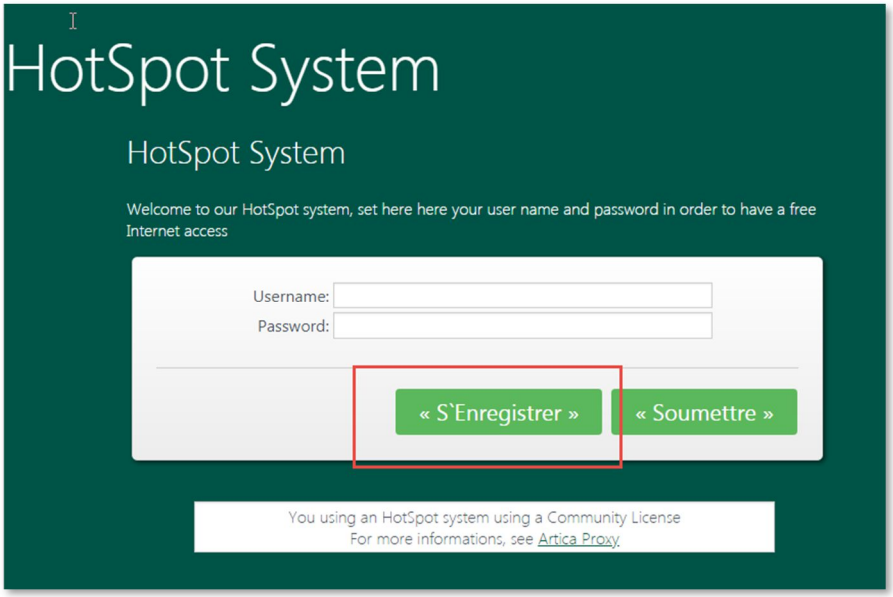
Note:

1. Users that use the registration will be not impacted by the **Re-authenticate each** option.
2. If User did not confirm its registration, it's account will be disconnected and removed from the system.

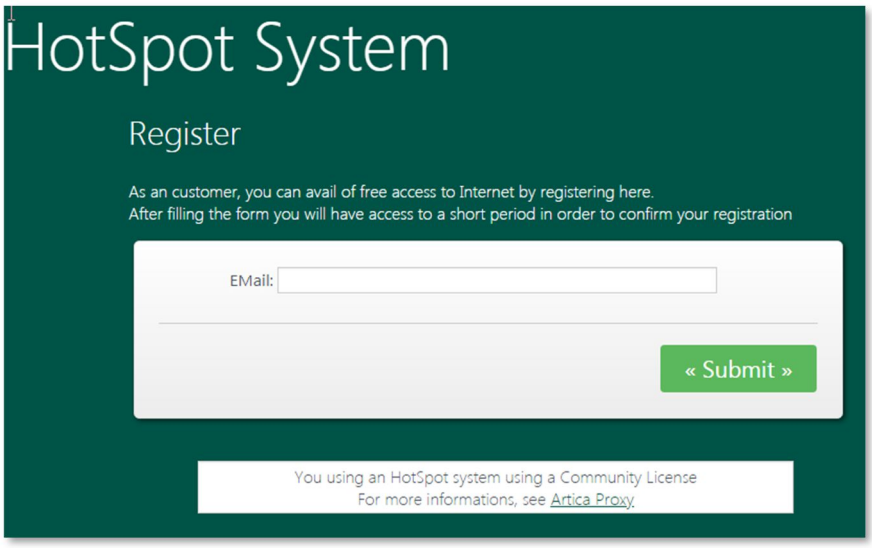


- Turn on the "**Activate the register form**" option.
- Define the **max time to register** in order to let user confirm its email address.
- Fill the SMTP parameters in order to let the proxy sends the confirmation message.

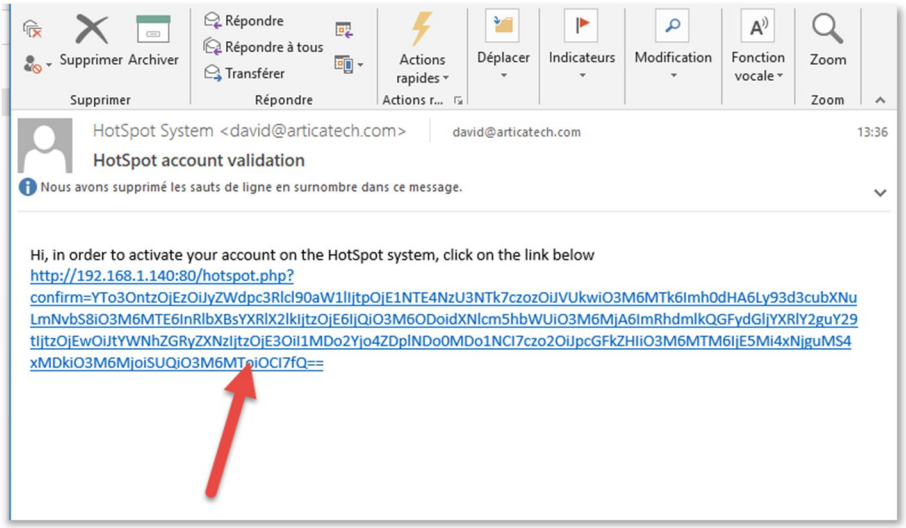
If you activate both LDAP/Active Directory connection and self-register, the Web authentication form add a "" button in order to let user use the self-registration form.



The registration form, just ask the email address to the user



Once send the mail address, the proxy sends an email and let the user surfing on Internet.
User receive an email with a specific link.



IF no authentication is enabled but the self-register is enabled, the screen only display the registration form.

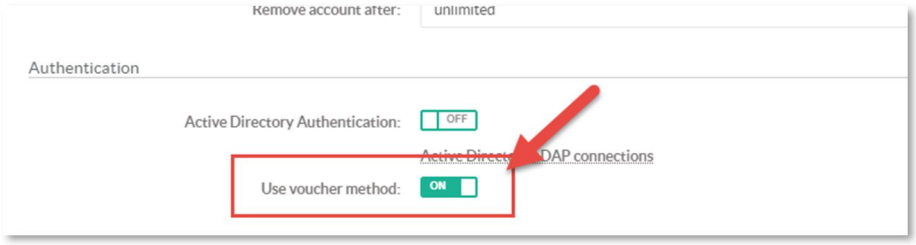
Voucher or Room number.

Voucher or Room number is a dedicated zone that allow you to specify the time to live for each account.
It is designed to run on the needs for Hostels or hospitals that needs to provide Wi-Fi accesses.

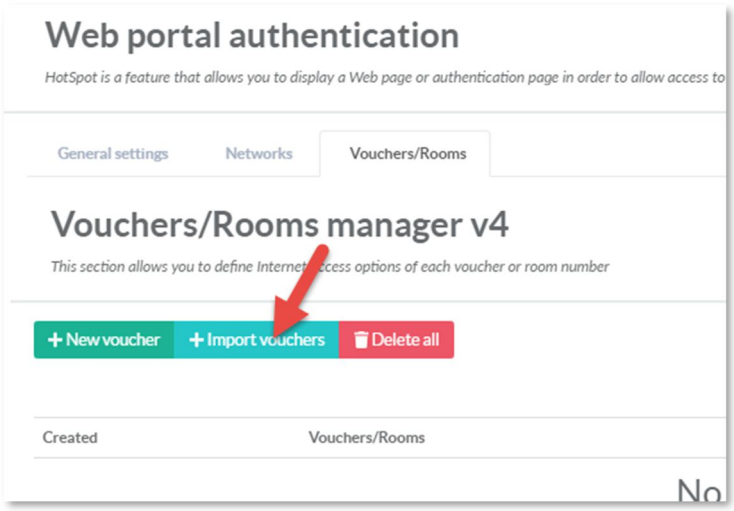
The following process is :

1. You import a set of vouchers into the database.
2. A member with a dedicated HotSpot privilege is able to start the time schedule.
3. After the expired period, the user is not able to access to the Internet.

On the main parameters, turn on the "**Use voucher method**"



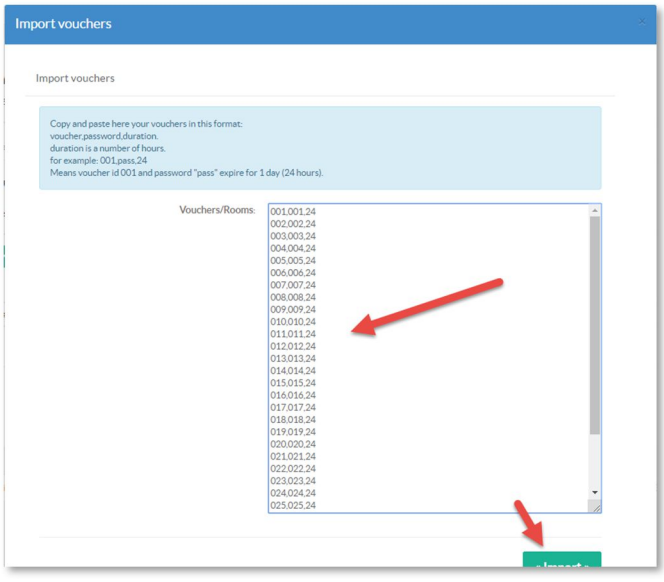
- On the main parameters section, select "**Vouchers/Rooms**" tab.
- Click on the "**Import vouchers**" button



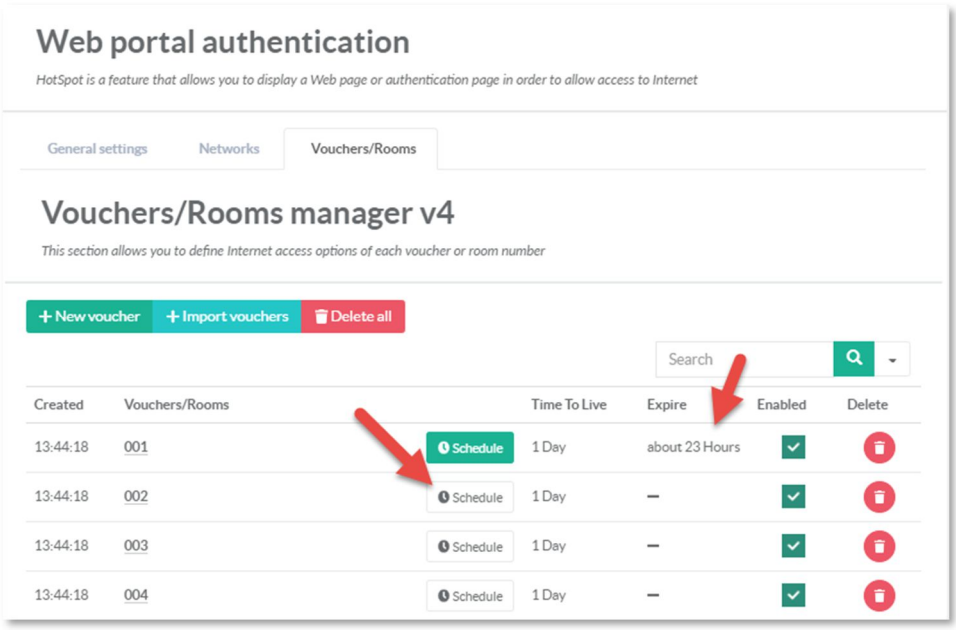
On the text area, add your voucher in this format:
voucher,password,duration.
duration is a number of hours.

```
001,pass,24
```

Means voucher id 001 and password "pass" expire for 1 day (24 hours).



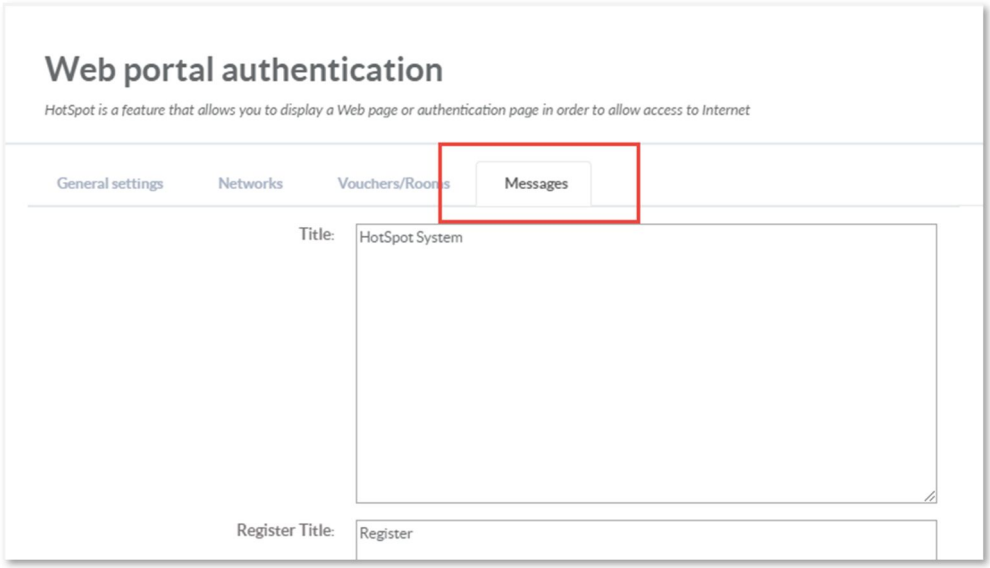
Vouchers will be displayed on the list.
According to the expire column: if the expire is not set, when the user using the voucher, the schedule will start after the login.
In other case, the Hotspot Manager can click on the schedule button in order to calculate the expire time.
After the expired time, the user cannot access to Internet., the HotSpot Manager must click on the schedule button in order to activate the voucher again.



Note: Vouchers or room number are just a label, you can create any value in the voucher section.

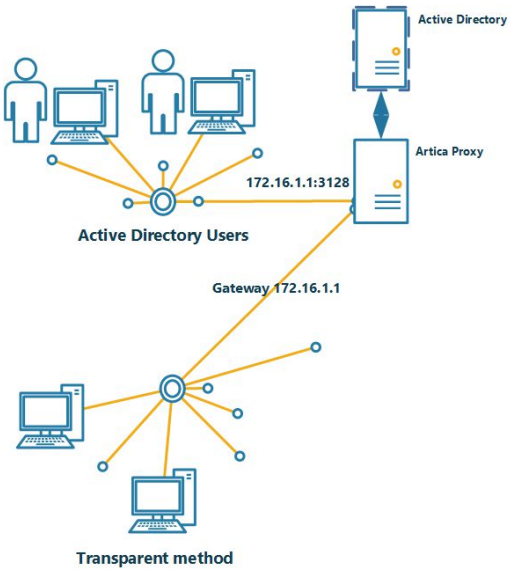
Personalize texts in the portal.

Phrases and labels used in the splash screen can be changed using the "**Messages**" section



Mixed transparent + Active Directory proxy.

Using the portal, you can create a mixed proxy for both connected/transparent users.

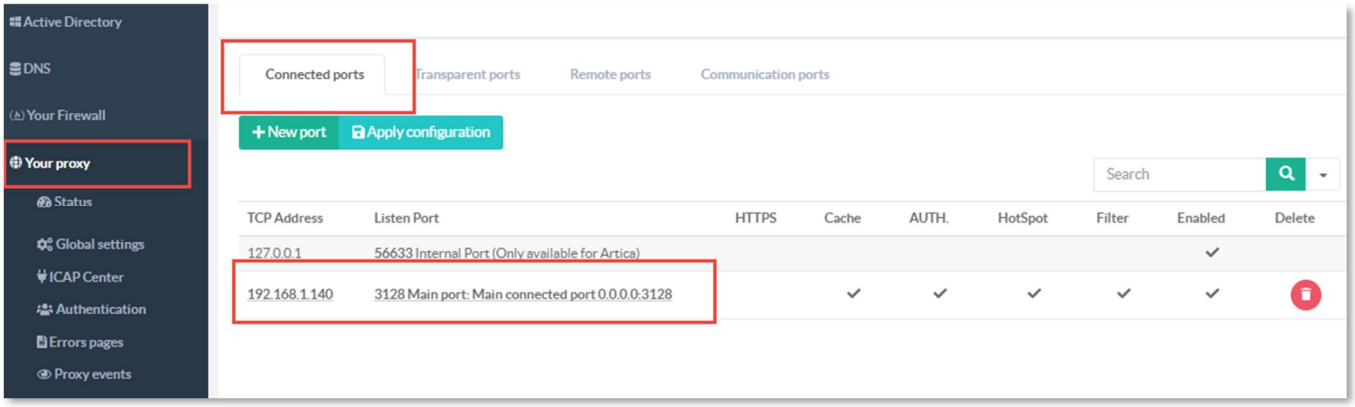


1) Users connected to the Active Directory (according to a GPO) are automatically connected to the proxy port (3128).
The NTLM/Kerberos authentication allow them to silently sends the credentials to the proxy.

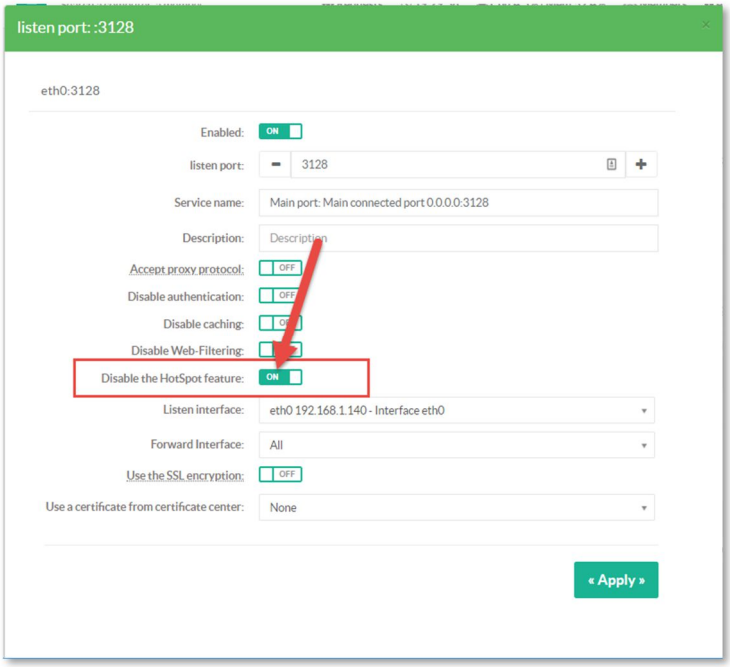
2) Computers that are not connected to the Active Directory will use the proxy as the main gateway.
In this case, the proxy will redirect sessions to the portal in order to help user to be authenticated trough the Active Directory.

To simply allow this method, you need to exclude the Active directory port from the authentication portal:

- On the left menu, choose **Your Proxy** and **Listen ports**
- Select the main port used for authenticate users.



- Turn ON the "**Disable the HotSpot feature**" option.
- Click on the **Apply Configuration** button.



This means users using this port will be not redirected to the Authentication portal page.

LOAD-BALACING FOR PROXIES.

You can load-balance several proxies in order to ensure that Internet access is not available due to a failed/down proxy.
To make the load-balancing working, you need at least 3 Artica servers.

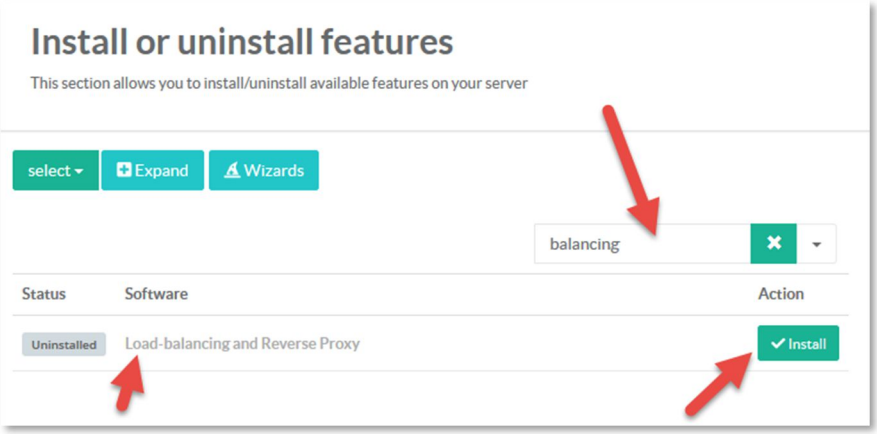
1- Artica act as Load-balancing service
2- Artica Proxy 1 as a master cluster.
3- Artica Proxy 2 as a slave cluster.

HaCluster, Make proxies in cluster with Active Directory.

The HaCluster feature is a good feature if you plan to deploy Artica Proxy in cluster mode using Active Directory and Kerberos.
A dedicated documentation for this feature can be found at
http://articatech.net/download/HACluster.pdf

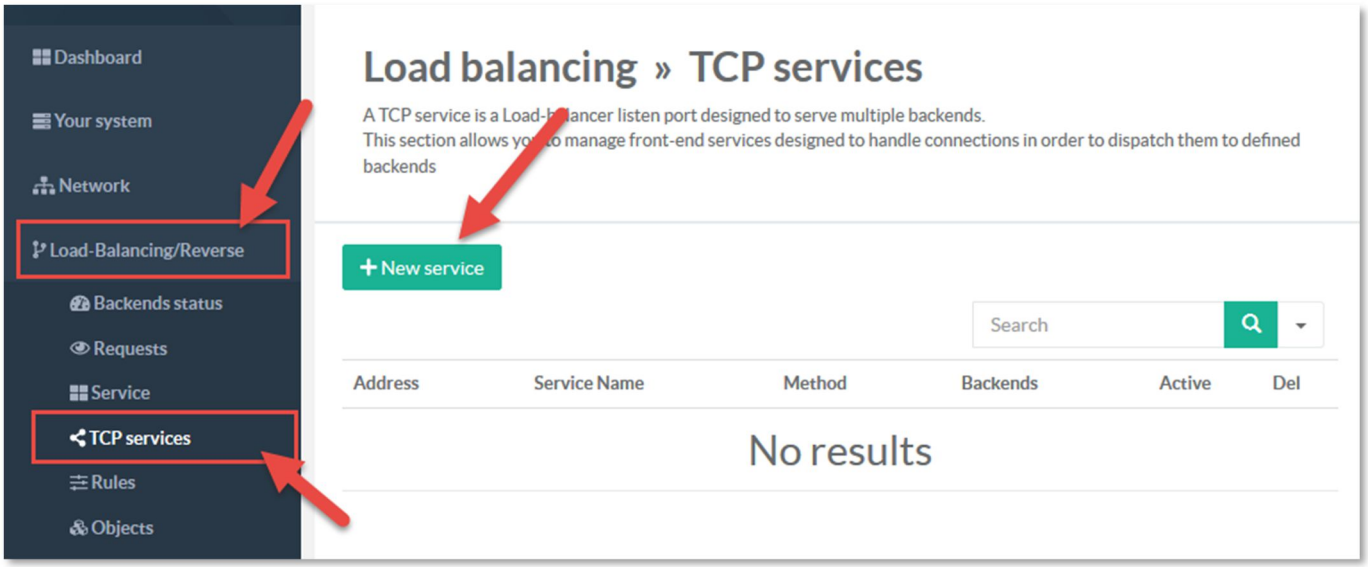
Install the load-balancing service.

- On the Artica that will act as the load-balancing service, click on "**Your System**" / "**Features**" left menu.
- On the search field, type "**balance**"
- Click on Install under the "**Load-Balancing and Reverse Proxy**" row.

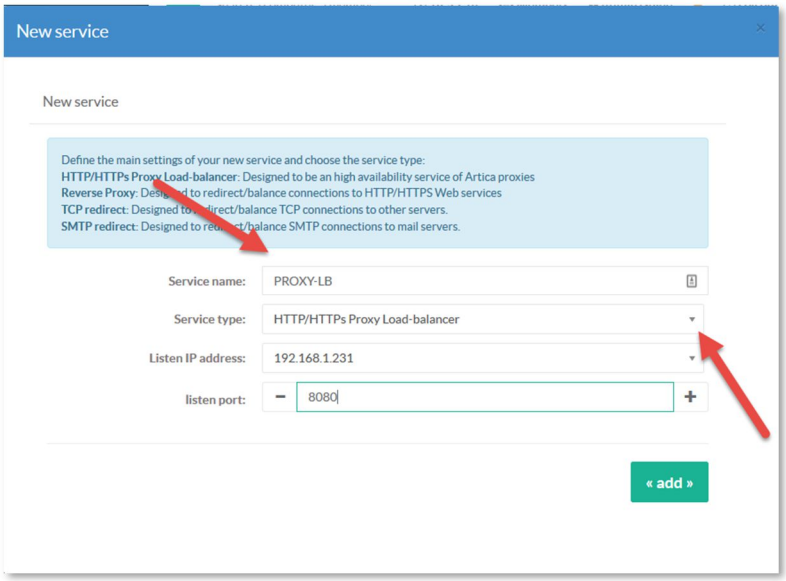


Create the service and add backends

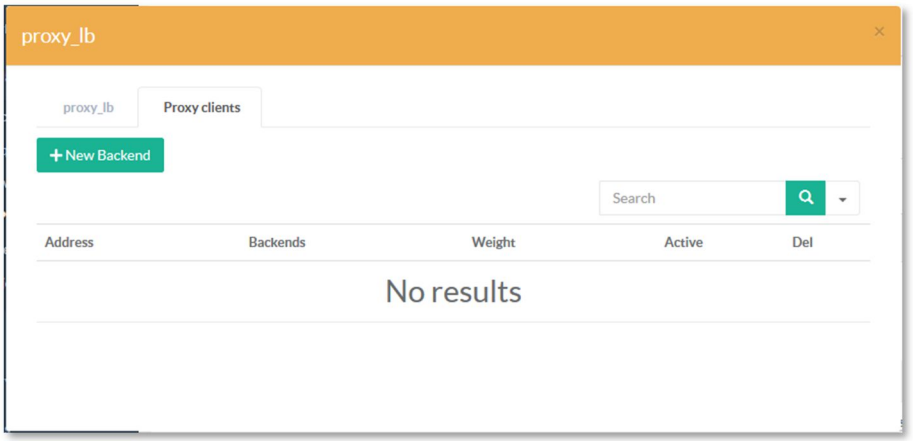
On the left menu, click on "Load-Balancing/Reverse"/ "TCP services" menu
Click on the "New service" button.



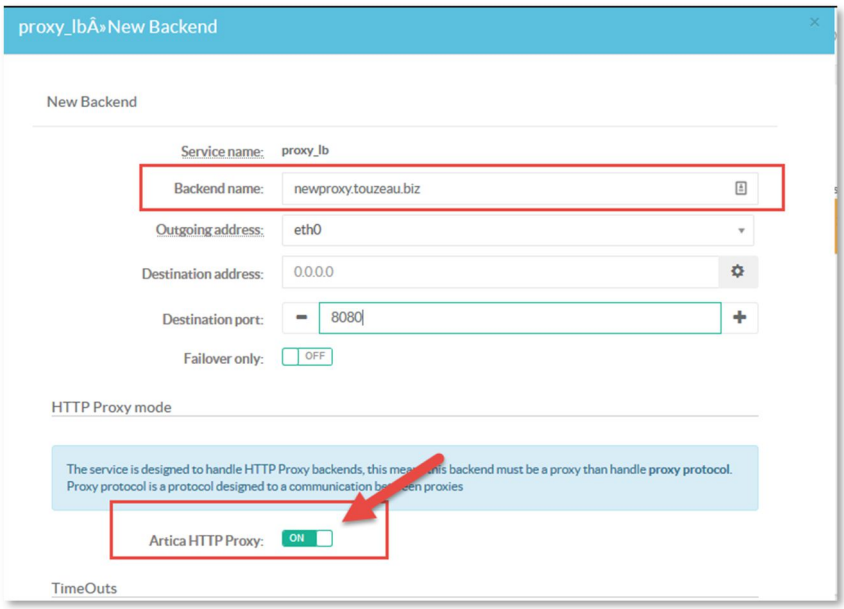
Set the service name, example "PROXY-LB"
Set the service type as "**HTTP/HTTPs Proxy load-balancer**"
Define the listen IP and port,
Click on **Add** button.



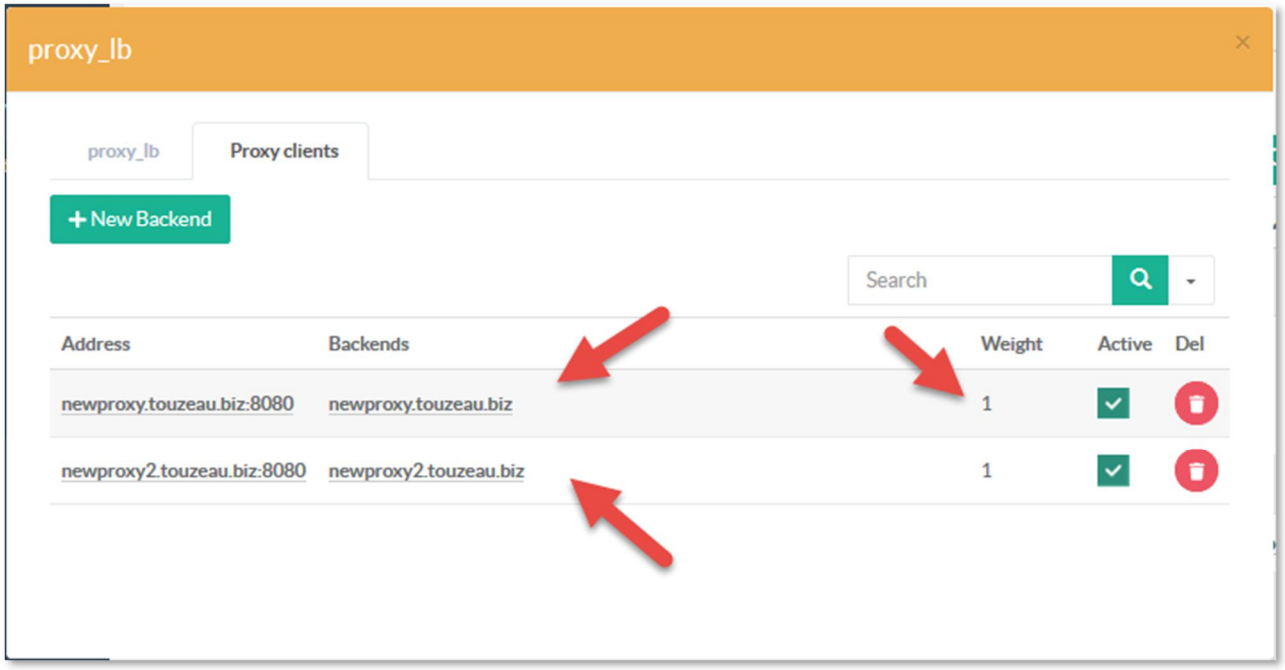
- Click on your new created service on the main table.
- Select "**Proxy Clients**" tab.
- Click on "**New Backend**" button



- Set the hostname in the backend name if you did want to fix the IP address.
- Define the target port of your proxy backend (the port with "Proxy protocol enabled).
- Check the option "**Artica HTTP proxy**"

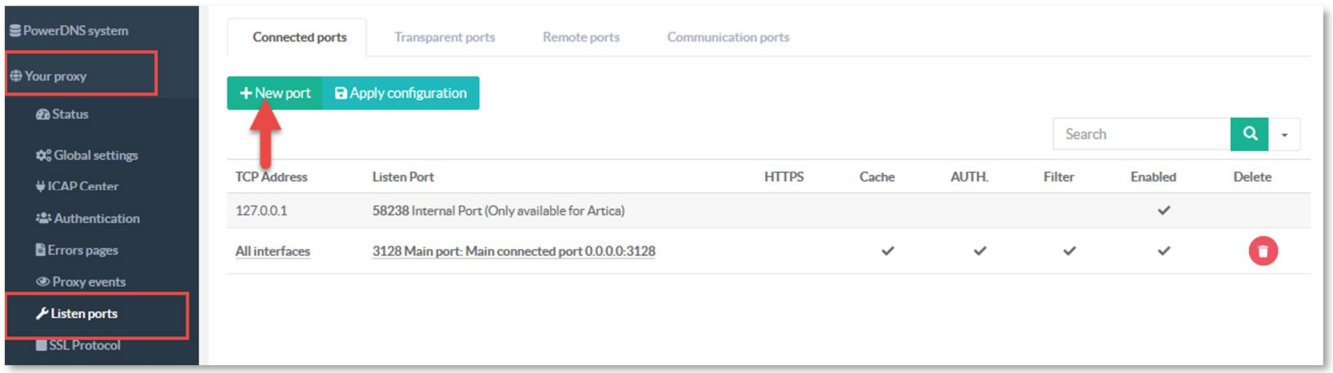


- Do the same for all proxies you need to balance.
- In the picture bellow, we have 2 proxies with the same weight (acting as load-balancing)

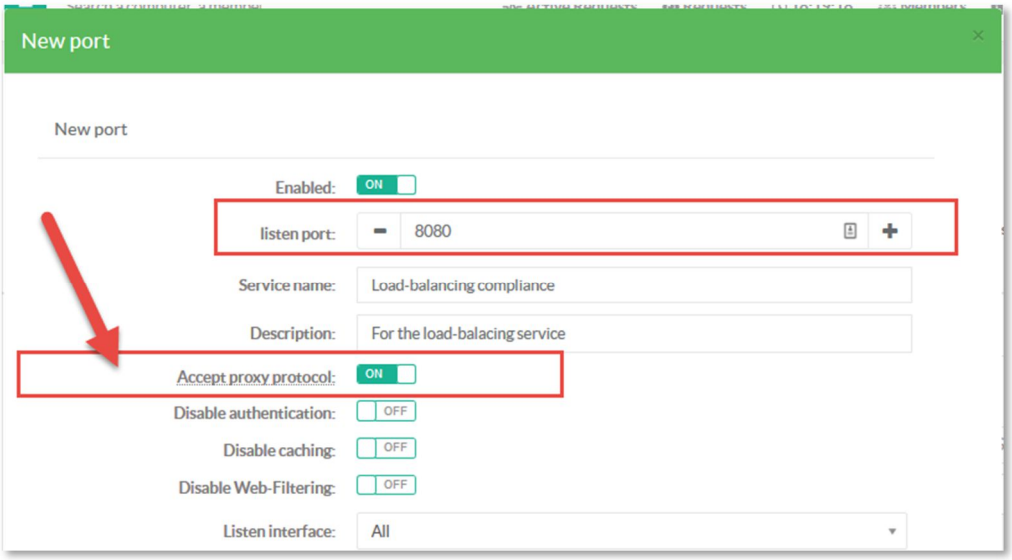


Enable the Load-balancing compliance on your proxies.

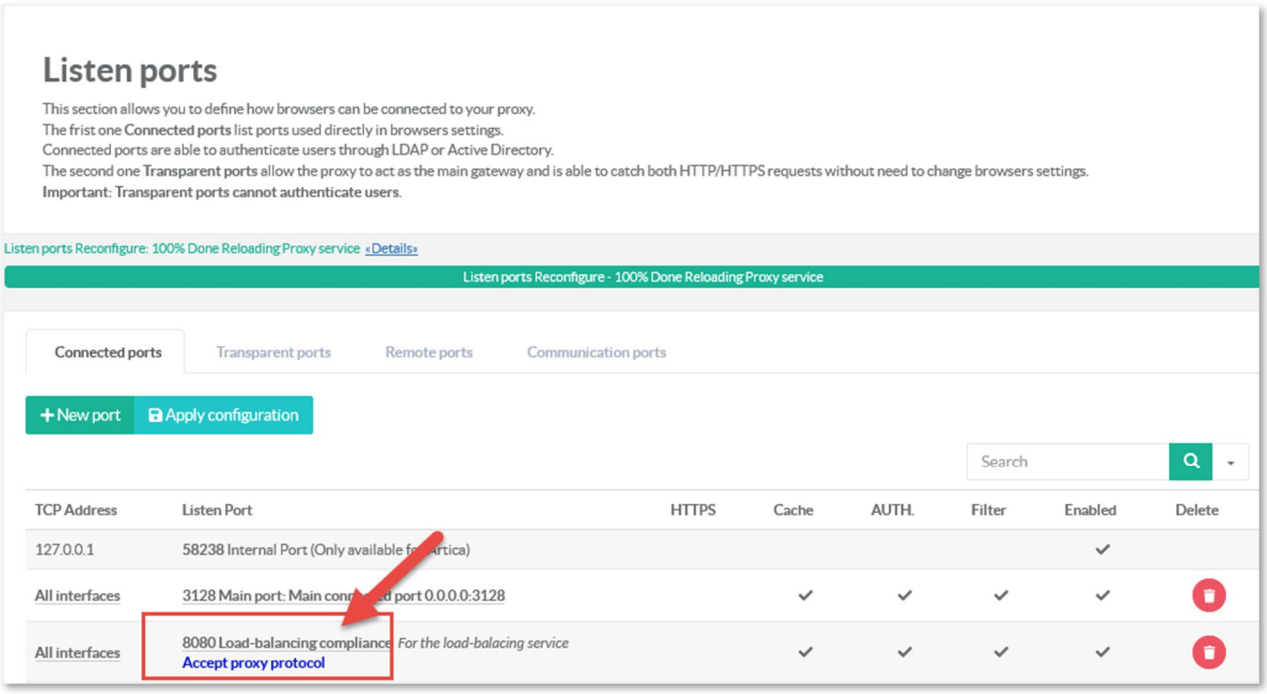
Go to your proxy server act as master cluster.
On the left menu, choose "**Your Proxy**" and "**Listen ports**"
Click on the button "**New port**"



Set the listen port: On our example, our load-balancing will connect to the 8080 port.
Enable the "**Accept proxy protocol**" for Load-balancing compliance
Click on **Add** button
Click on "**Apply configuration**"



You should see the new added port on the main table with "**Accept proxy protocol**" in blue.



Connect your browser to the Load-balancing service port

Load-balancing with Kerberos method.

The Kerberos ticket

You have 2 ways to make the Kerberos ticket compatible with your Load-balancer.

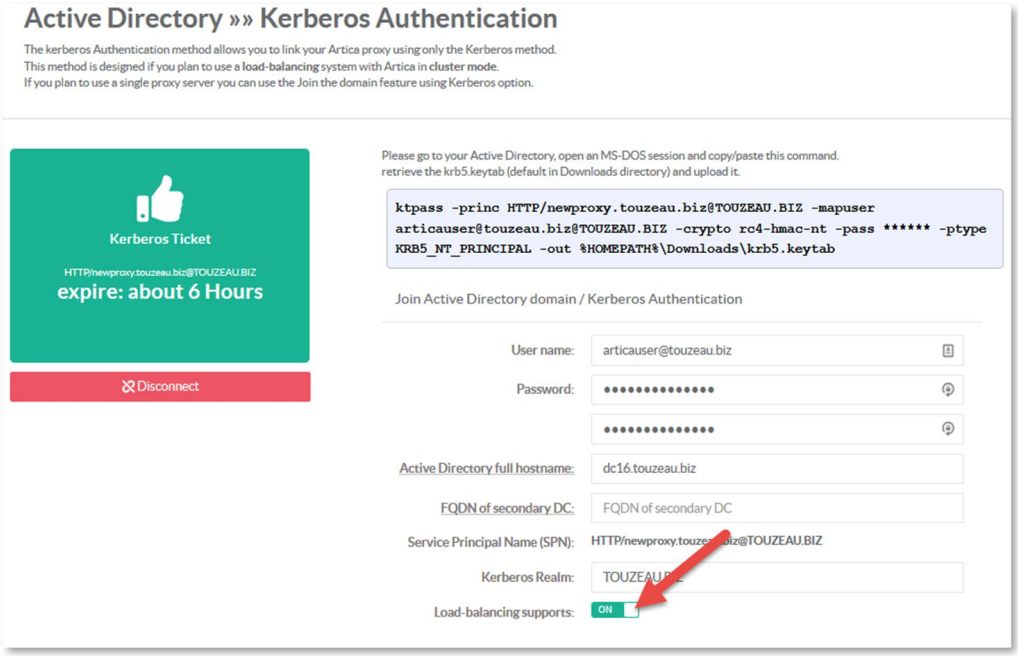
The goal is to generate a key tab file for the FQDN of your Load-balancer.

1) Generates the Kerberos ticket using the Kerberos Authentication **method directly on the Artica Load-balancer**.
Upload the **krb5.keytab** file on each proxy you want to load-balance.

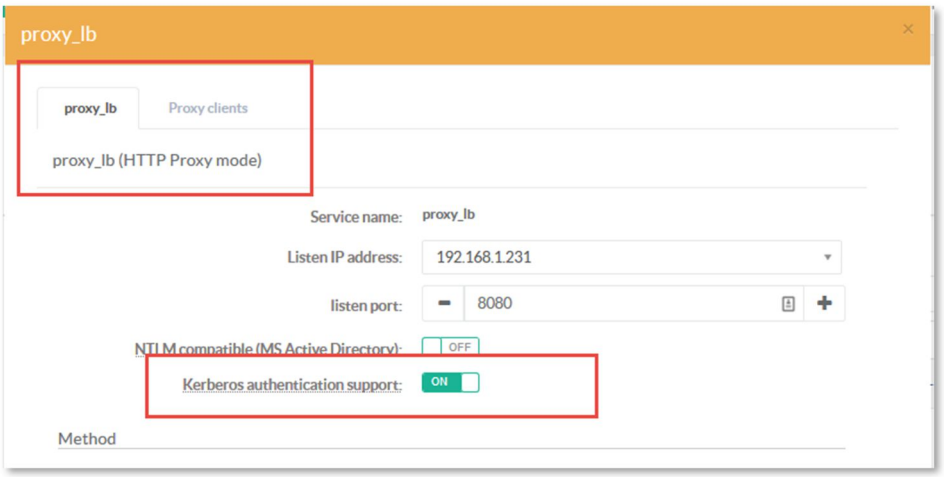
2) Use the master proxy to generate the Kerberos ticket and **invert the IP address in your DNS server**.
For example,
you have created the key tab file on proxy.company.com IP 192.168.110.
Your Load-balancer is proxylb.company.com: IP 192.168.1.100.
Change DNS in order to point proxy.company.com on 192.168.1.100

Minor tweaks.

- On each proxy, under the Kerberos Authentication, enable the "**Load-balancing support**" option.



- On the Artica act as Load-balancing, select the option of your Load-balancing service.
- Enable the "**Kerberos authentication support**".

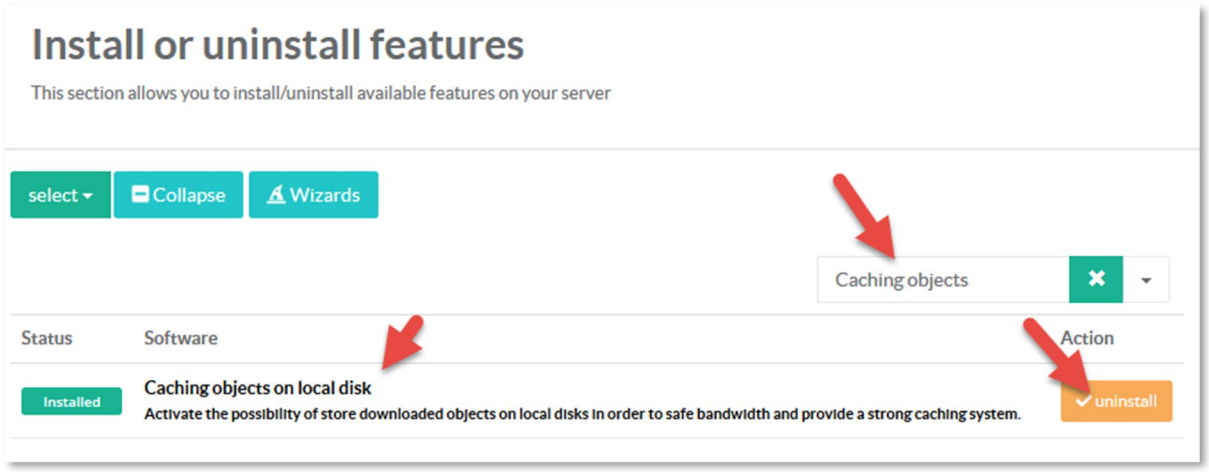


CACHING FEATURE

The caching feature allows you to add the "Caching Internet objects" feature.
This feature allows Artica to safe bandwidth by storing most requested objects in the disk.
In this case, if a stored object is requested by a browser, the proxy sends it directly instead of fetching it from the Internet.
You need a valid corporate License to use this feature

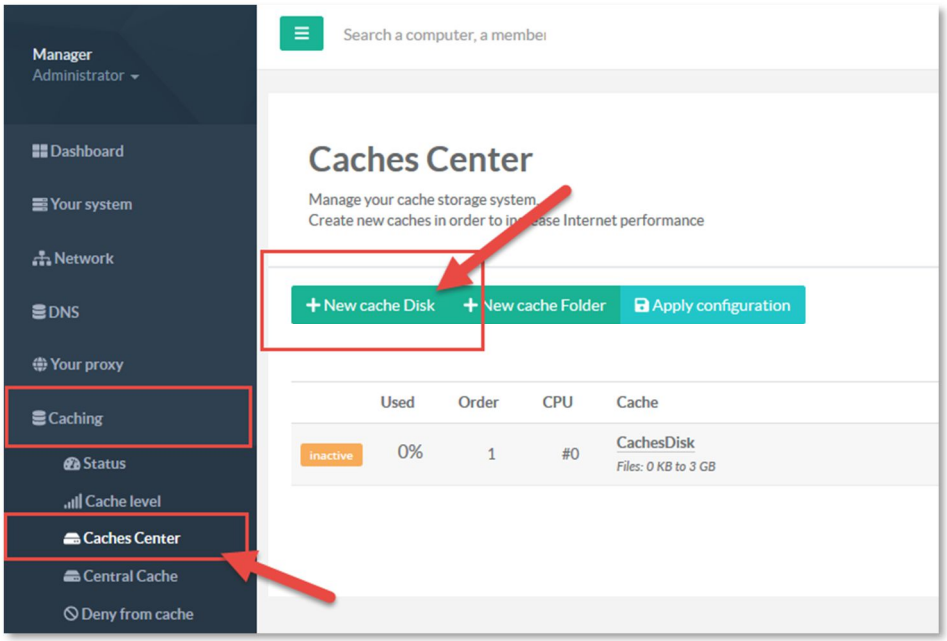
Install the Cache feature.

The cache feature can be installed in the "**Features**" section.
On the search field, type "**Caching objects**"
Click on Install button under the "**Caching objects on local disk**" row

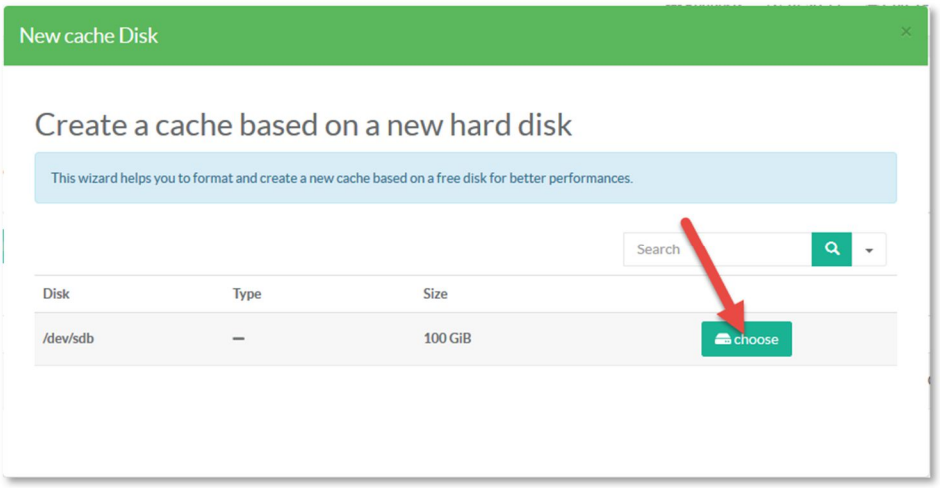


Create Your first cache.

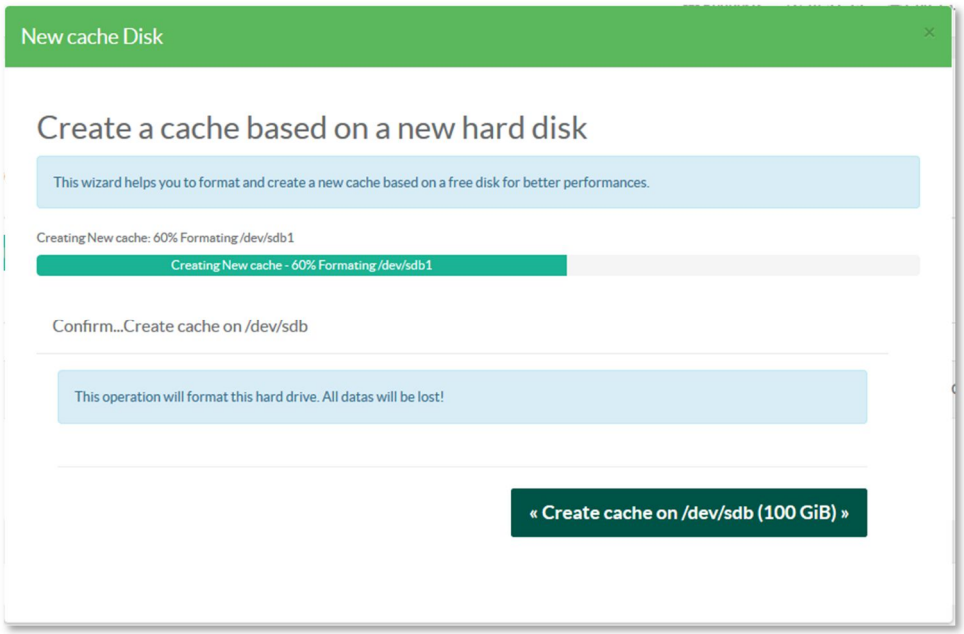
The best way to create a cache is to use a **dedicated hard drive** for the cache.
On your server or your virtual machine, plug a new disk. (you did not need to reboot).
On the left menu, choose "**Caching**" and "**Caches Center**" option
Click on "**New cache Disk**"



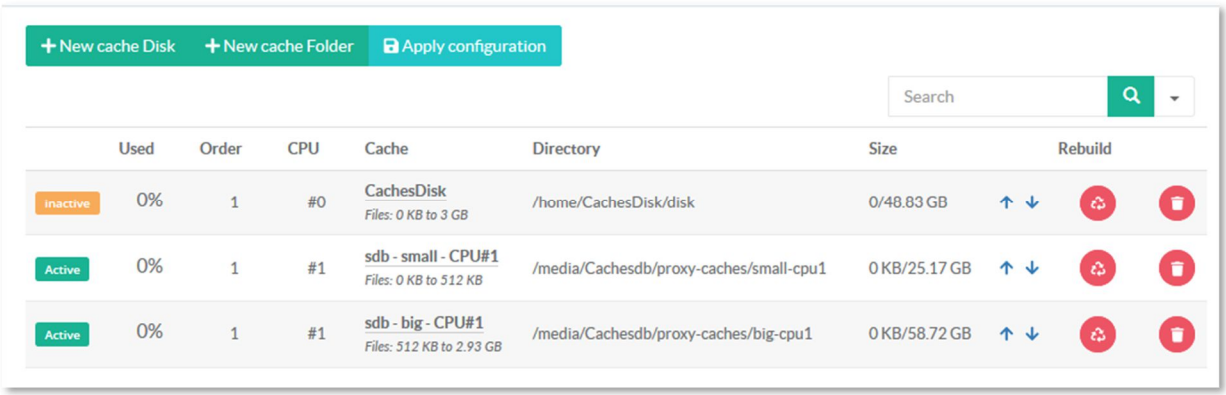
The wizard will scan free disk plugged on your system.
Select the hard drive by clicking on the "**Choose**" button.



After confirming your selection, Artica will format your new disk as a caching disk.



The wizard will create 2 caches, one for small objects (less than 512KB) and second for large objects from 512KB to 3GB

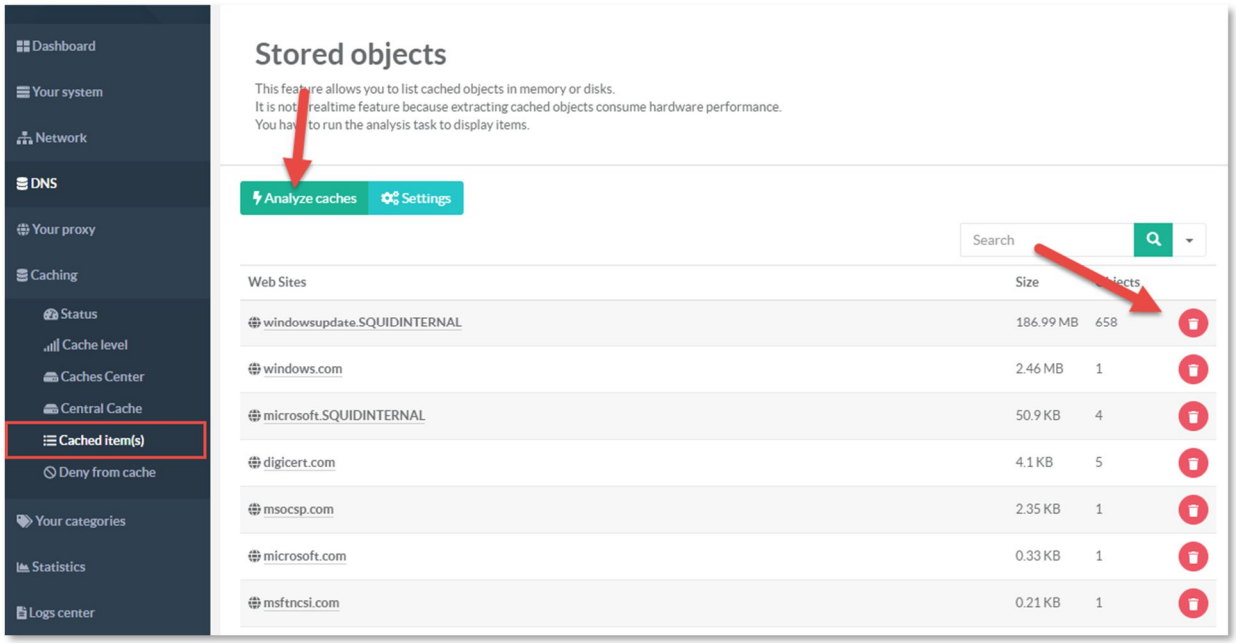


Is Artica cache Microsoft Windows Updates?

Yes, Artica is already designed to cache Microsoft Windows Updates.
You need at least a 200GB of cache in order to let the proxy store all Microsoft updates.

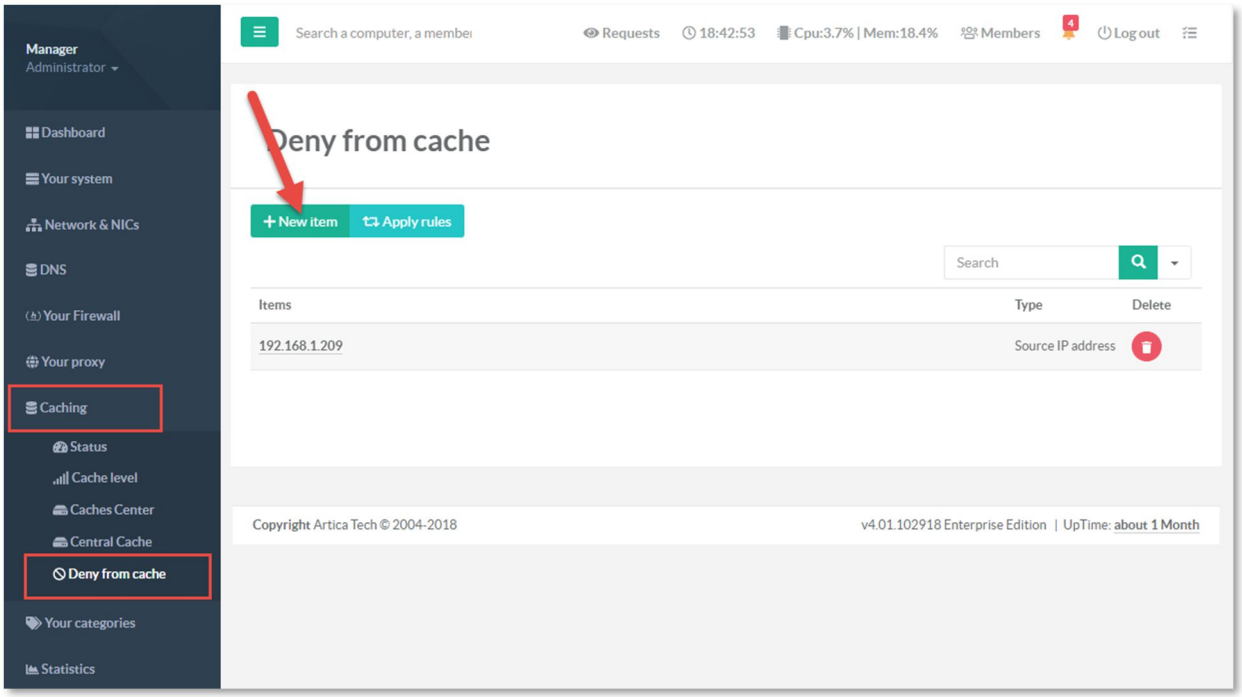
How can I see if caches are working as expected?

On the left menu, choose **Caching** and **Cached items**
Click on the button "**Analyze caches**"
This button run a background task that extract all stored objects from caches in order to display them in a table.
This section allows you to delete stored objects too



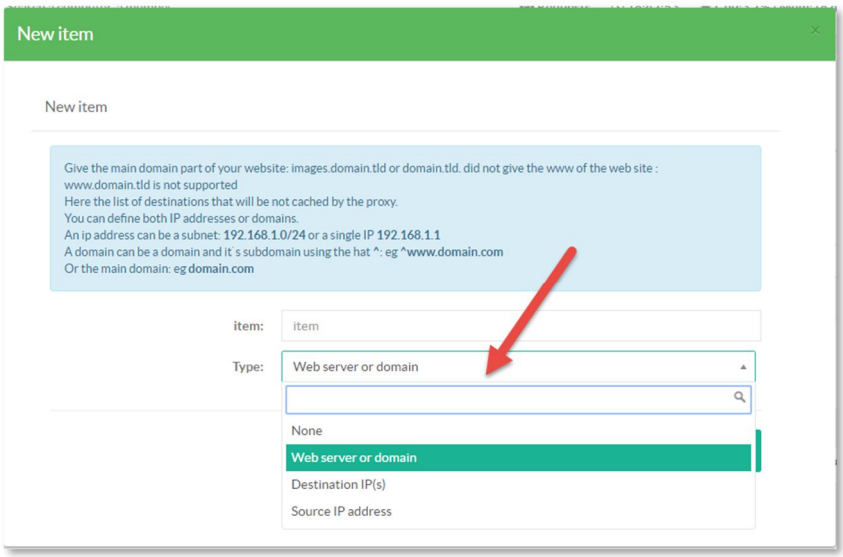
Exclude from caching

In some cases, you need to exclude the proxy to store objects from its cache according items.
The section: "**Caching**" and "**Deny from cache**" allows you to create simple rules to force proxy not to store objects.



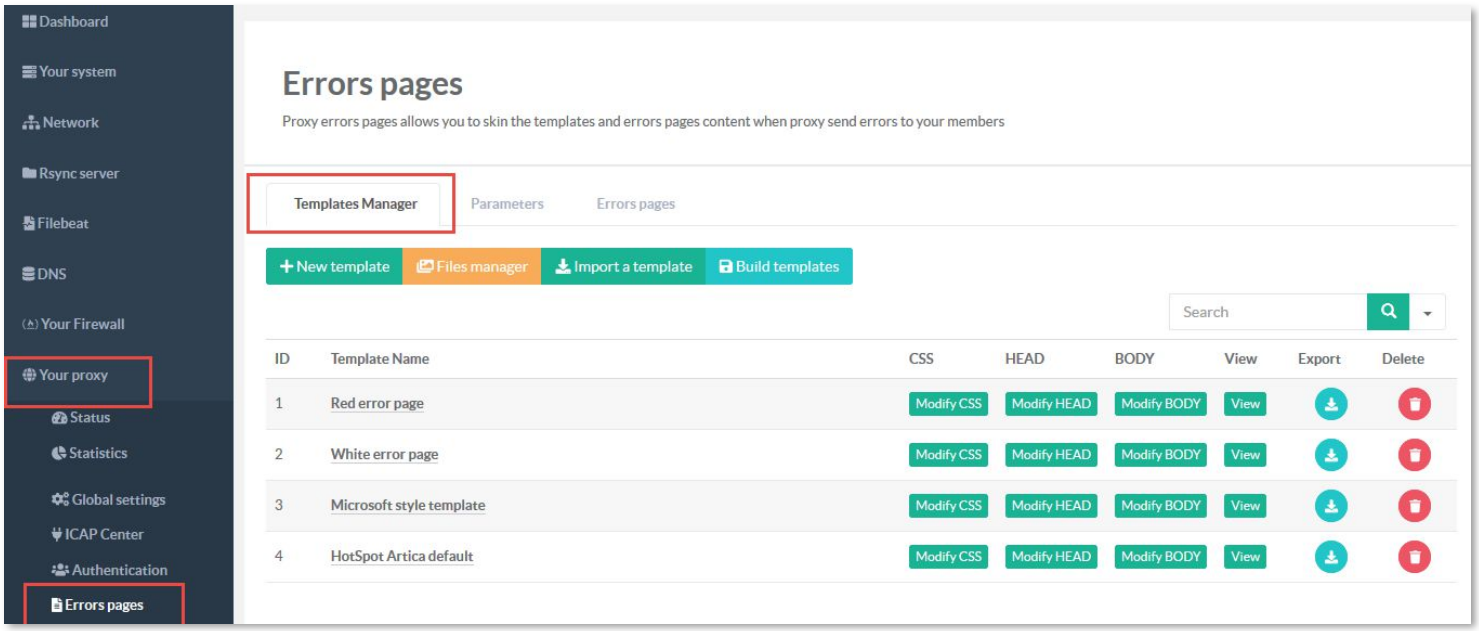
You can add a rule according 3 types of element.

1. **Web server of domain**: Deny from cache based on a domain name.
2. **Destination IP(s)**: Deny from cache according to a range/subnet/IP address of an Internet site.
3. **Source IP address**: Deny from cache according to a range/subnet/IP address of a local computer client.



ERRORS PAGES AND TEMPLATES

If the proxy or the Web-Filtering must display an error page to the browser, it will use the template defined.

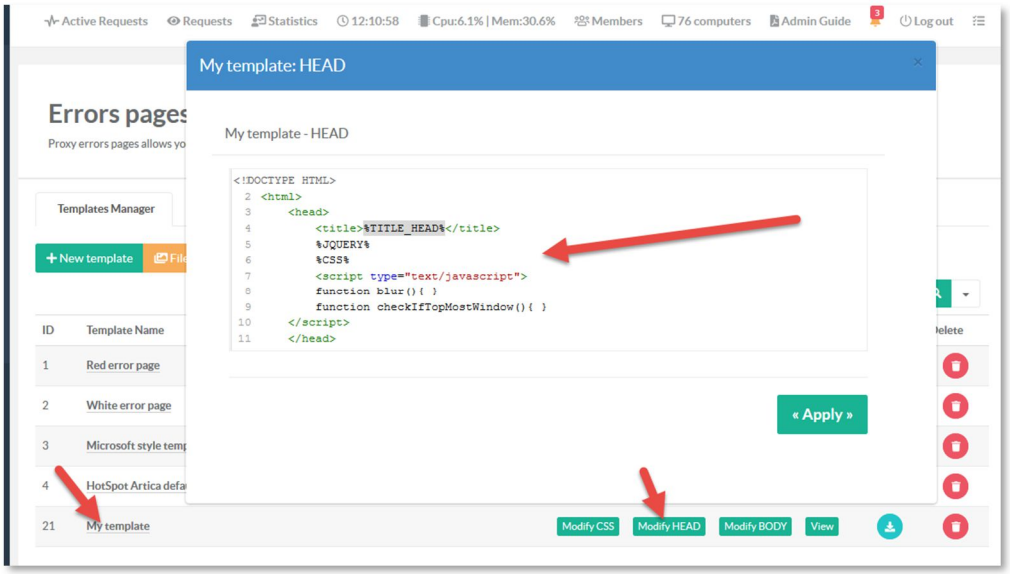


By default, all pages displayed by the proxy are based on "**Red Error page**" template (except for the HotSpot feature that using HotSpot Artica Default).

The Templates Manager

The Templates Manager allows you to add or personalize / skin templates. That will generate errors pages on the proxy and the Web filtering (see Skin the Web-filtering error page)

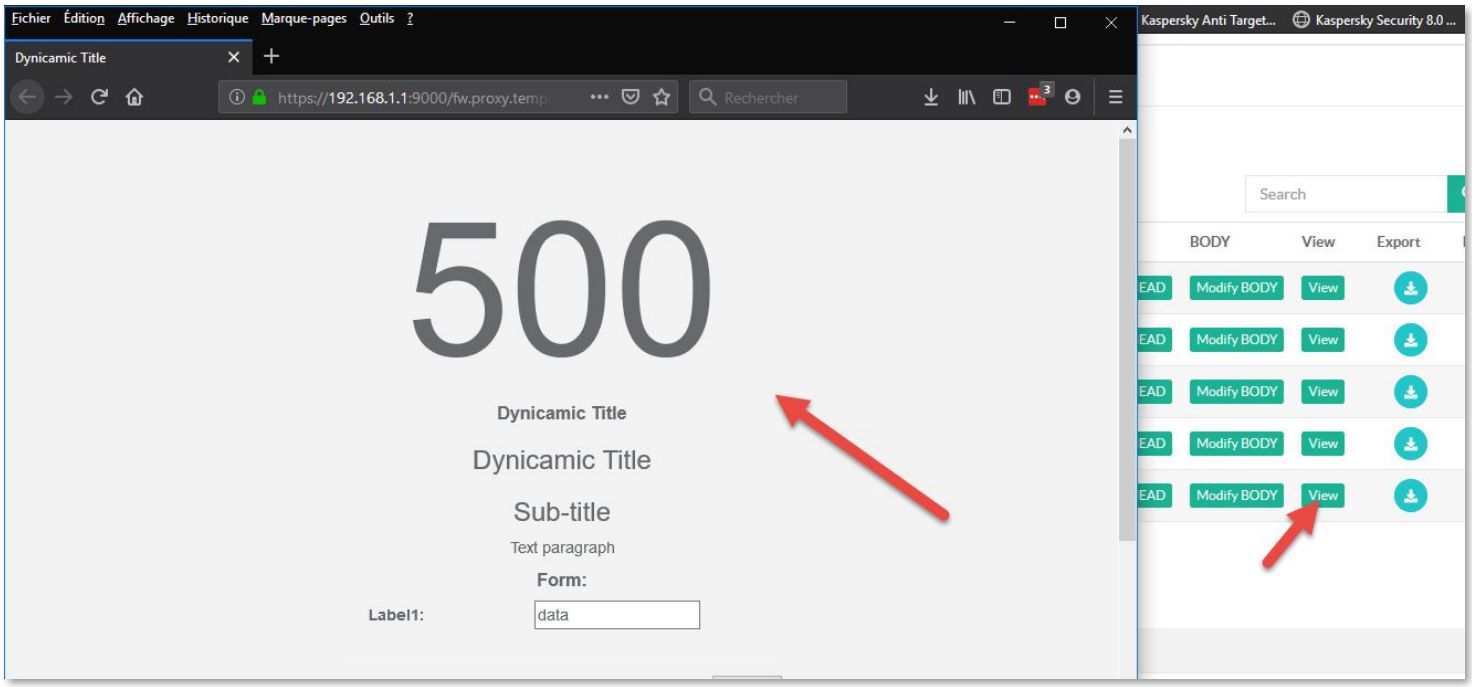
When creating a new template, a template example is displayed.
To modify a template, you need to edit the HTML code in 2 parts, the Head of the web page and the body.



Some specific token can be used:

- **%TITLE_HEAD%**: Will be replaced by the title of the error.
- **%V4HEADS%**: Add CSS and specific head for design of Artica v4 section
- **%JQUERY%**: Will be replaced by jquery javascript APIs.
- **%CSS%**: Will be replaced by the CSS content defined in the template.
- **%DYNAMIC_CONTENT%**: Will be replaced by the content of the error page.
- **%FOOTER%**: Mandatory: the web page footer.

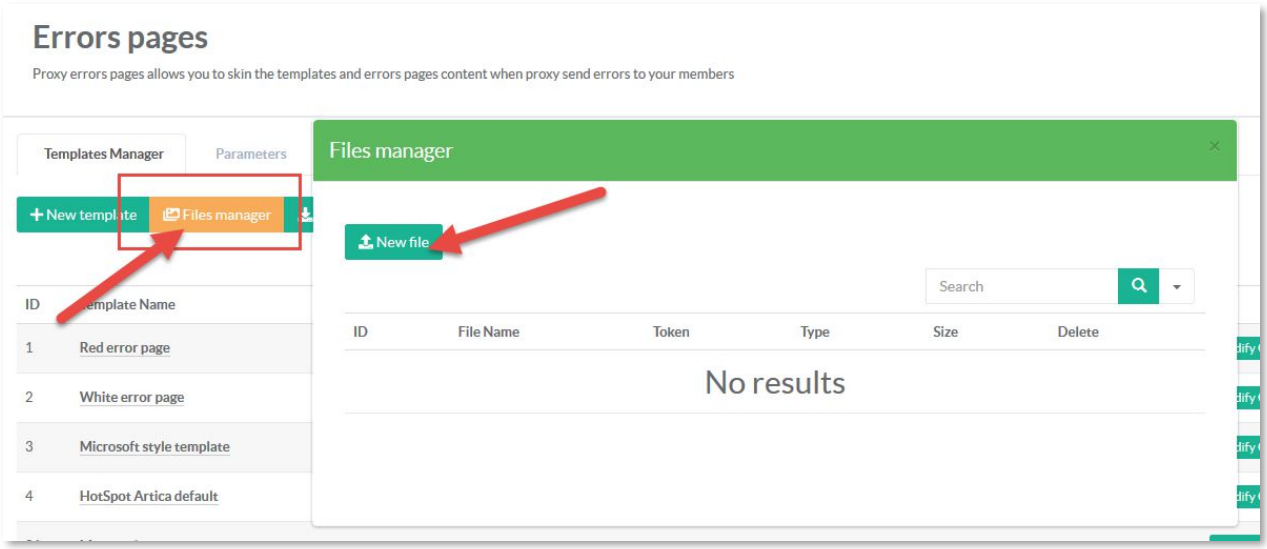
The view section allows you to display the design of the web page with all fields, and text that can be displayed



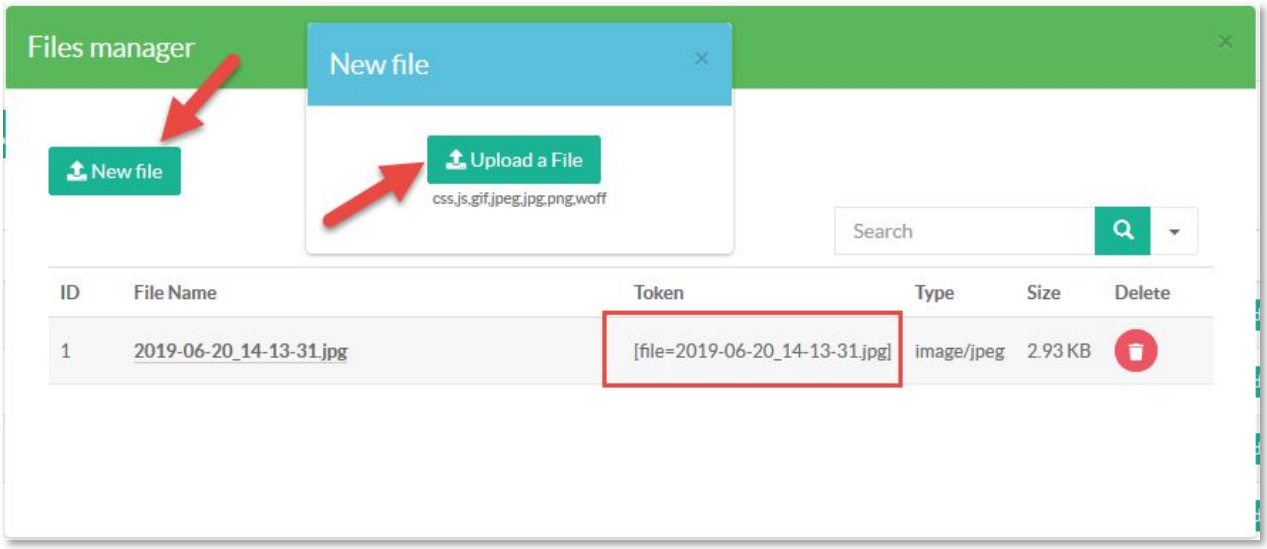
Insert images in templates.

Pictures must be added using the files manager in template section.

- Click on the Files manager button.
- Click on New File



Click on Upload a file and select the picture you want to import.
Take care of the "Token" column, this Token must be added in your HTML code or CSS code.



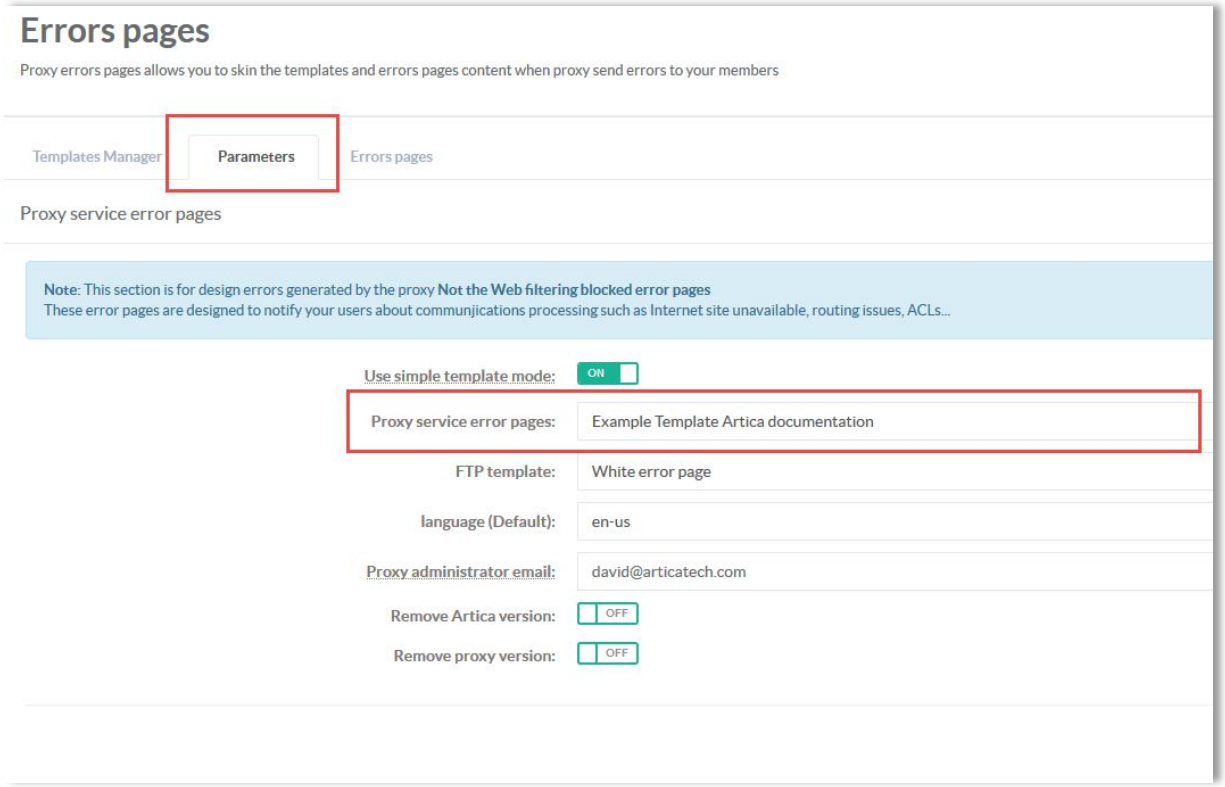
For example:

```
  <div style="background-image:url('[file=2019-06-20_14-13-31.png]');background-repeat:no-repeat;background-
repeat:no-repeat;background-position-x: 10%;background-position-y: 5%;">
```

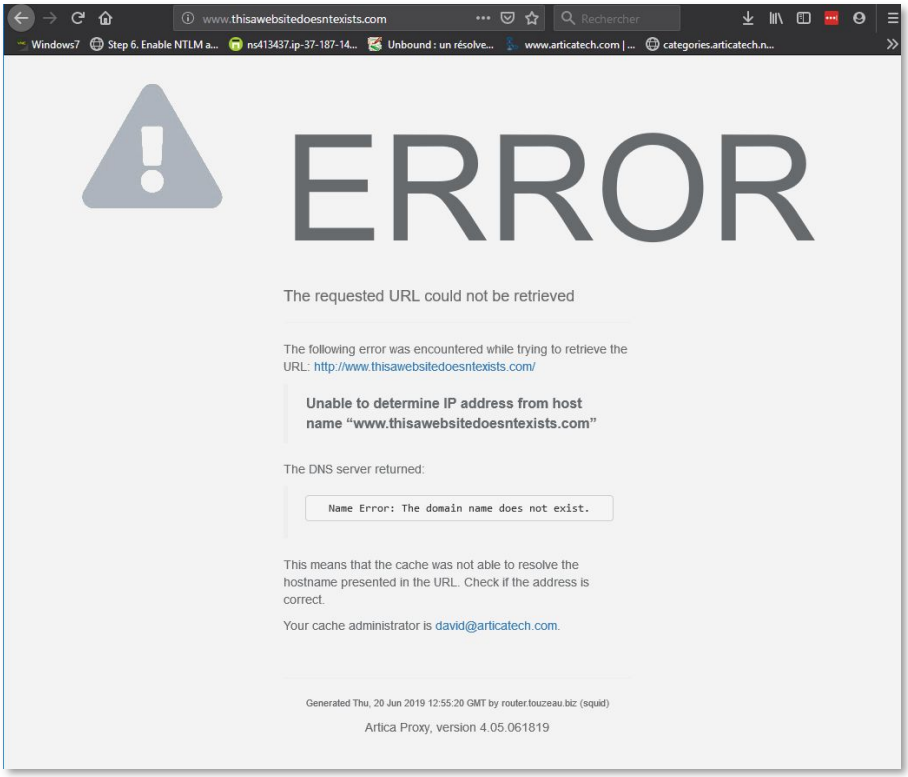
```
<img src="[file=2019-06-20_14-13-31.png]" align=center>
```

Assign your template to the proxy error pages

Once your template personalized, got to "**Parameters**" tab and assign your template to the "**Proxy service error pages**"
Click on **Apply** button.



With your Artica proxy, go to http://thiswebsitedoesntexists.com , this request will generate a DNS error and display the error with your new template.



You can import this template example here (http://articatech.net/download/ExampleTemplateArticadocumentation.tar.gz)

THE ITCHARTER SERVICE

IT Charter feature

Technology Charter feature allows the proxy service to redirect requests to an internal Web page that force members to read the company policy before accessing to Internet.

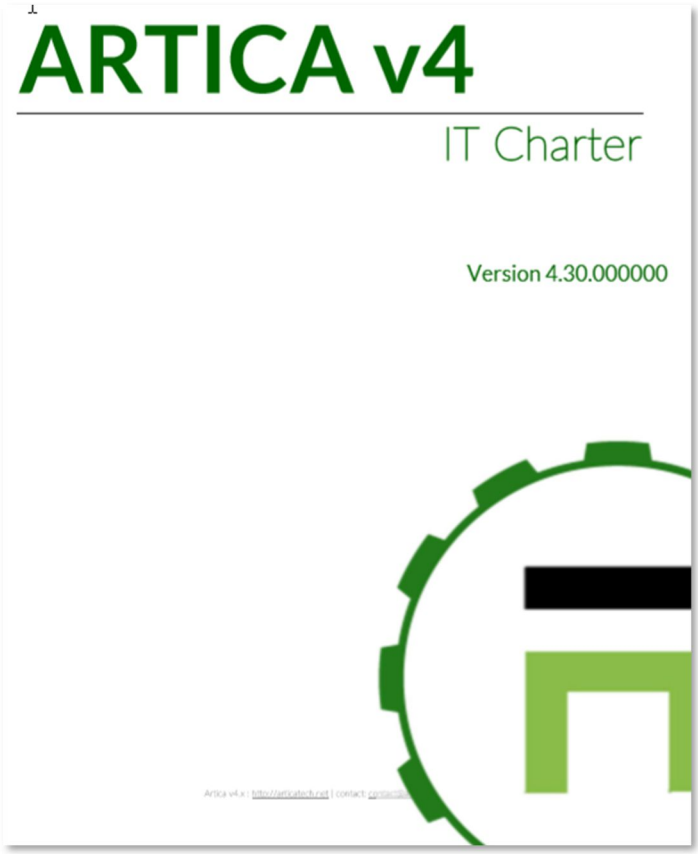
This feature will only display one time the policy page if the user as correctly accept the User Agreement.

Each User Agreement is logged in order to ensure that the policy has been read.

The Artica IT Charter feature is a splash screen provided by the proxy that deny access to Internet until users have not accepted the charter.
The charter can be displayed as HTML page or by PDF.

When an user accept the IT charter an event is created in the database, identity of the user is saved in a memory database in order to not ask again to accept the IT Charter.

You can create multiple charters.
When an user as successfully read a policy agreement, it should be redirected to the next policy agreement.



Download the additional documentation

Download the dedicated documentation on the IT Charter feature here:
http://articatech.net/download/IT_CHARTER.pdf

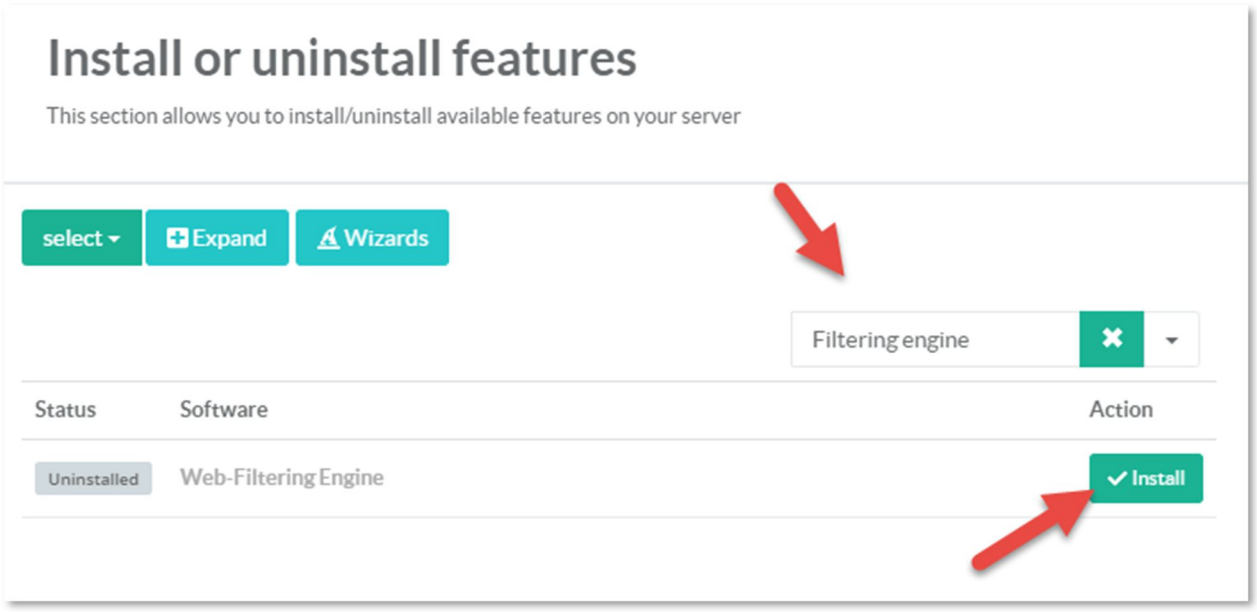
THE WEB FILTERING

The Web Filtering is a module designed to filter million websites against categories.
It cannot be used to filter a small list of websites.
This behavior is important because using the Web-Filtering engine will consume memory.
By default, it should use about 700MB to 2.5GB of memory (depends how many categories you using on rules).

If you plan to filter just 20 or 100 websites for a population, you will have better performance by using the **Web Application FireWall** rules (WAF).
If you plan to protect your users according porn, advertising, malware websites that represents about 5 million websites, the Web-filtering is the needed feature.

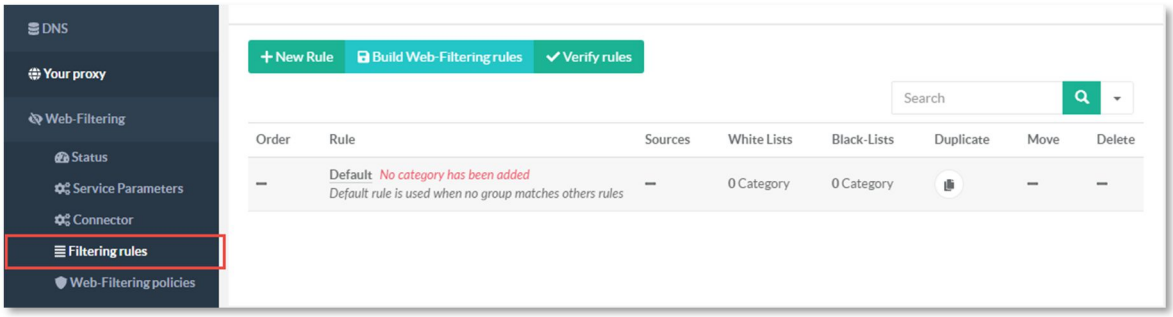
Enable the Web-Filtering engine

On the feature section, in the search field, type "**Filtering Engine**"
Click on "Install" on the **Web Filtering Engine** row.



Web-Filtering rules

Web-Filtering rules are located in "**Web-Filtering**" and Filtering rules section.
By default, no category is defined, means nothing is filtered.



Understand the Web-filtering processing

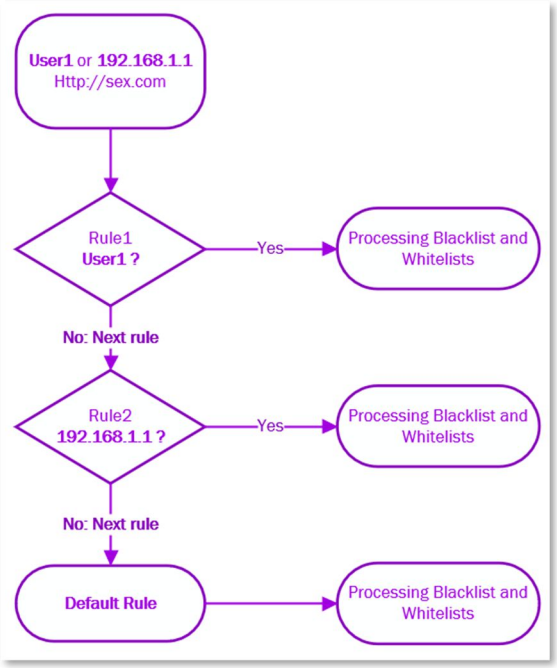
Rules are not analyzed like a Firewall.

In fact, a firewall tries to matches all rules objects as the web filtering rule is focused **only on the source** defined in rules.

When a source is found, the web-filtering will process defined blacklists and whitelists from the rule and return back results to the proxy.

In fact, the rule order is less important than defined sources.

Finally, if not source is found in rules, the default rule will be the last processed rule.



A good way to create Web-filtering rules.

According this behavior, the first rule to personalize is the default rule that represents blacklists and whitelists affected to everybody.

In our case (for example) we want to filter everybody against porn, malwares, advertising, trackers, phishing and socials sites.

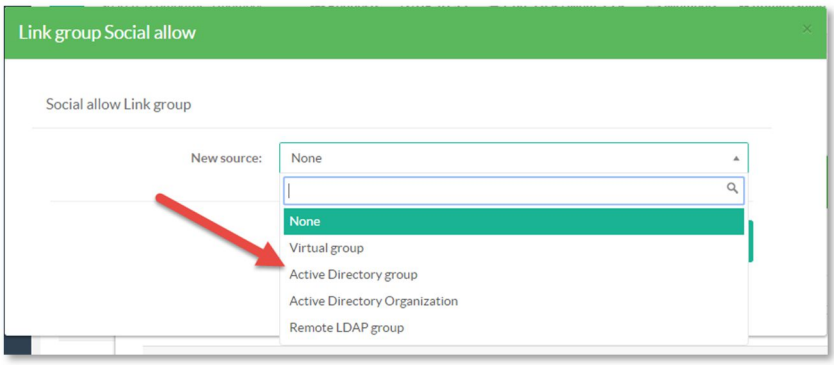
But for a single population we need to allow socials sites.

For the first step, we assign blacklists categories in the default rule, copy the default rule to a new rule.
For the copied rule, we define the source group and remove the socialnet category from the rule.

See the this example: https://youtu.be/XYVWOEax1sk on Youtube

Multiple Sources

A rule can store one of multiple sources



Sources can be

A Virtual group:
Could be an IP address (192.168.1.1), et subnet in CDIR format (192.168.1.0/ 24) or a username (user1)

An Active Directory Group:
If connected to an Active Directory, you can choose an Active Directory group that stores users you wan to filter.
By default users are synchronized each 15 minutes.

An Active Directory Organization:
If connected to an Active Directory, you can choose an OU branch.
All users after the selected OU Branch will be filtered.
By default users are synchronized each 15 minutes.

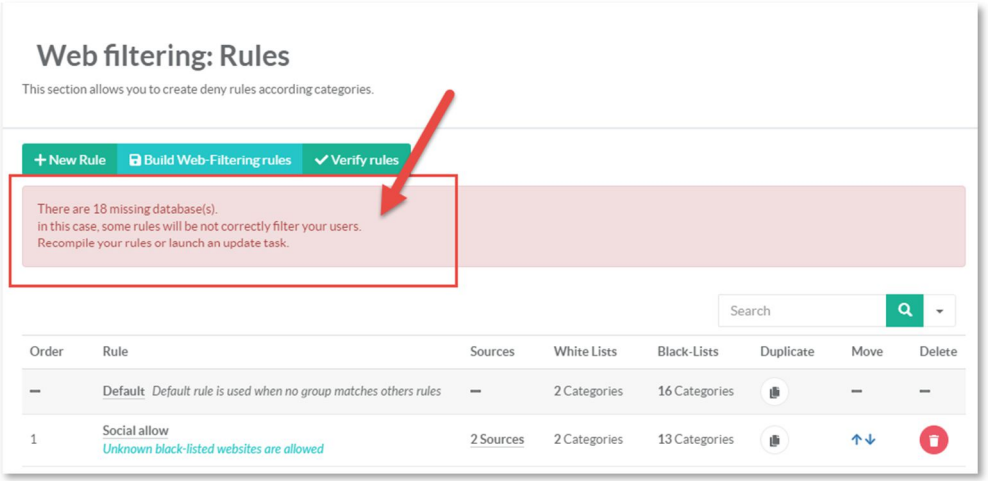
A remote LDAP Group.
If the server is a remote Web-Filtering service, you can select a group stored in a remote LDAP server.

All these sources can be stored in one rule, in this case, you can filter all users from 172.16.1.0/24 and the
Active Directory group INTERNET_USERS.

Verify that databases are updated

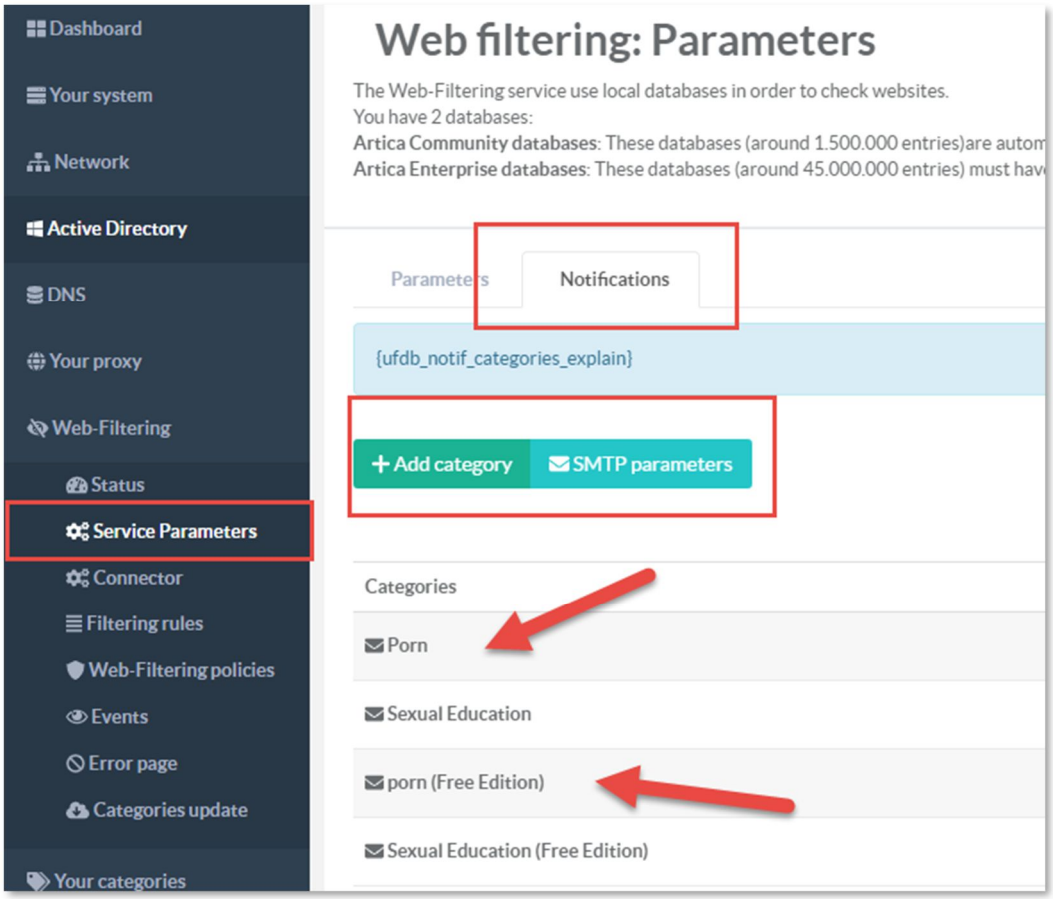
The Web-Filtering needs to download databases and define them in your rules.
If databases are not downloaded or if you have constructed your rules before downloading databases a red screen is displayed.
This read screen display the number of missing databases.

You have to fix it by Building your Web-filtering rules or update Web-filtering databases.



Be notified when members browse on specific categories.

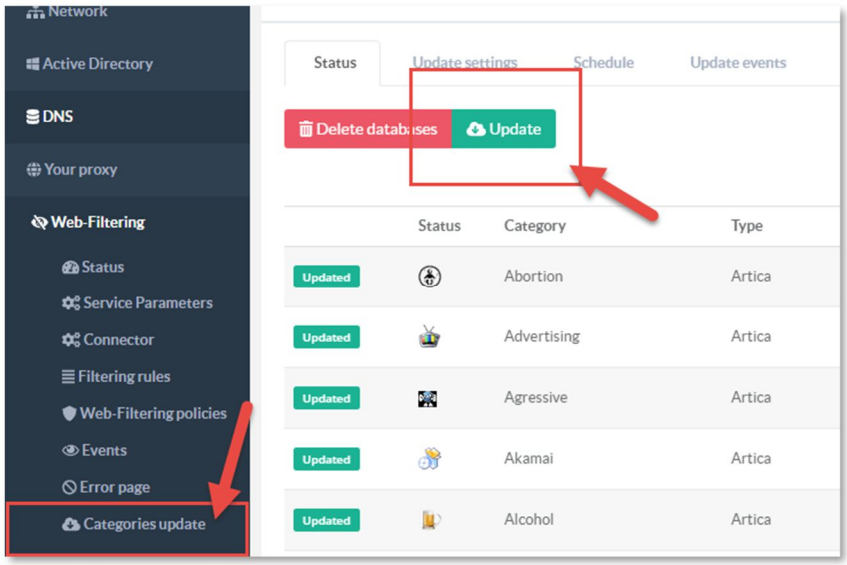
You can be notified when users are blocked on specific categories.
To enable this feature, go into "**Web-filtering**" and **Service Parameters** left menu.



Select the "**Notifications**" tab.
Click on the "**Add category**" button to add the category you want Artica to notify if a member is blocked.
Define the SMTP parameters by using "**SMTP parameters**" button.

Manually update Web-filtering databases

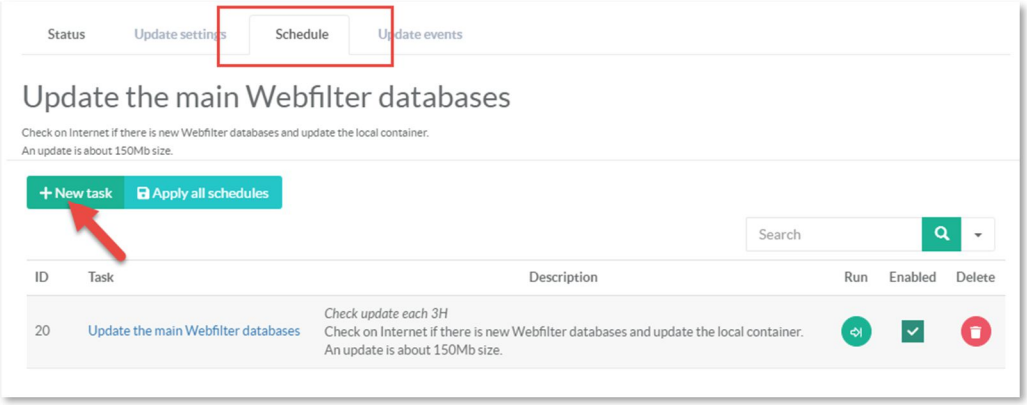
To update manually Web-filtering database, on the left menu, choose "**Web-Filtering**" and "**Categories update**".
Click on the "**Update**" button on the status section.



Schedule Web-Filtering databases update.

By default, the update database task is updated each 3 hours, you can modify or add a new update schedule.

on the left menu, choose "**Web-Filtering**" and "**Categories update**", select the "**Schedule**" tab.

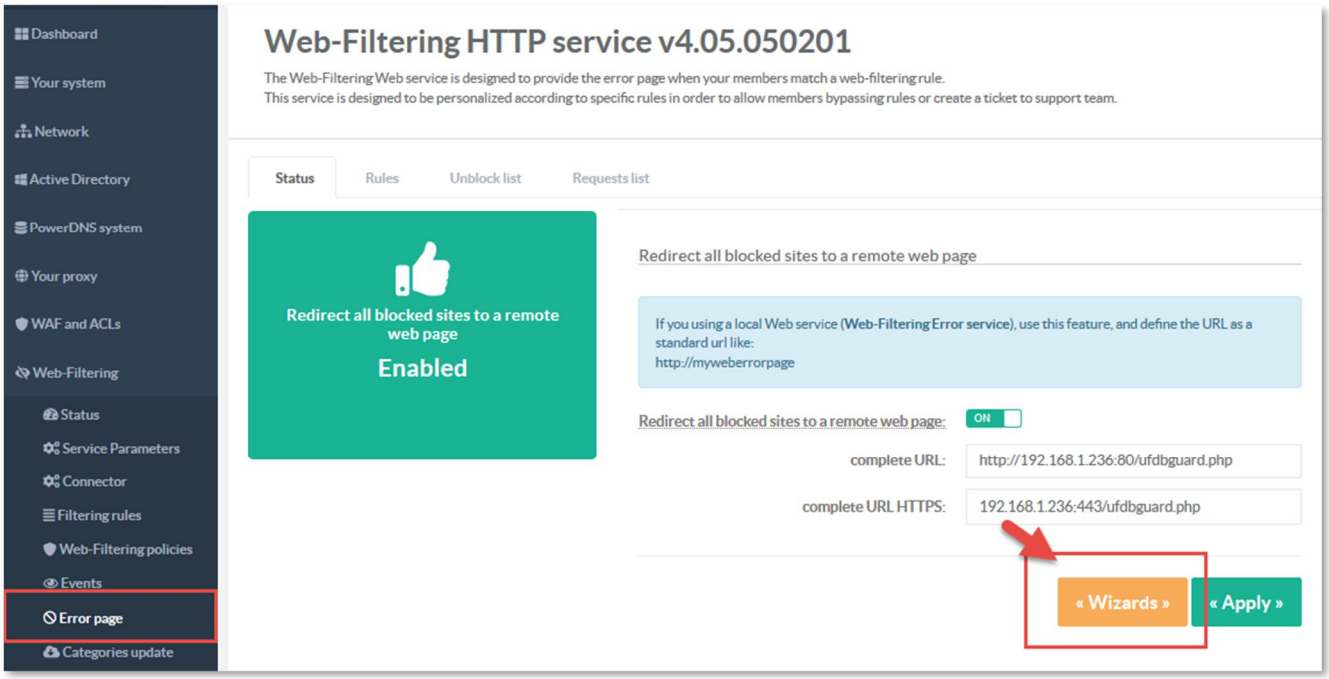


Click on the "**New task**" button to create a new schedule.

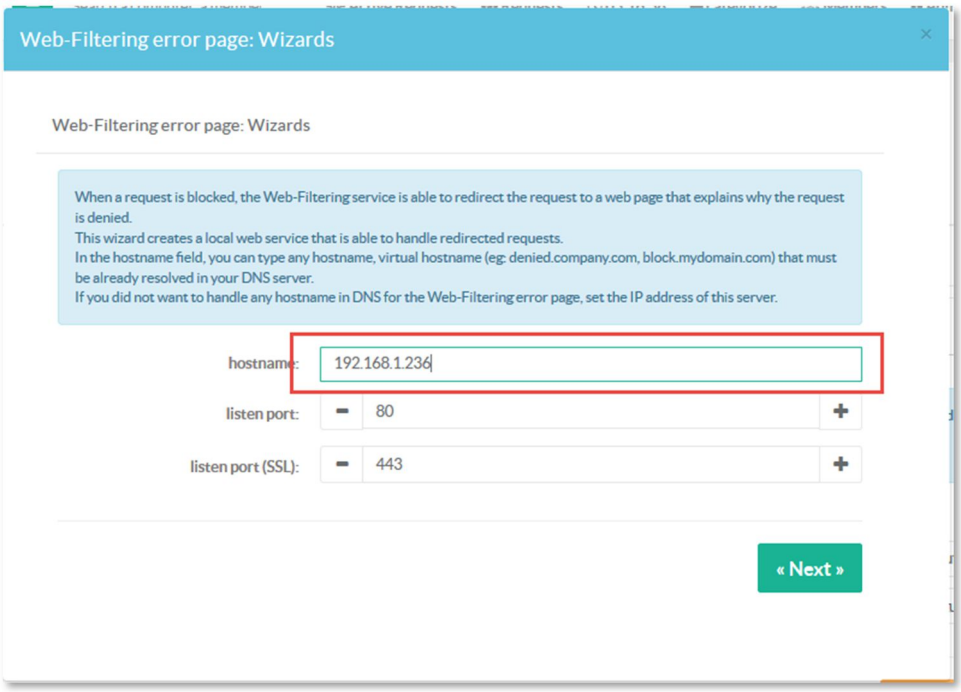
The Web-Filtering error page.

The Wizard

When a request is blocked, the Web-Filtering service is able to redirect the request to a web page that explains why the request is denied.
On the left menu, click on "**Web-Filtering/Error page**"



- Click on "**Wizards**" Button
- This wizard creates a local web service that is able to handle redirected requests.]



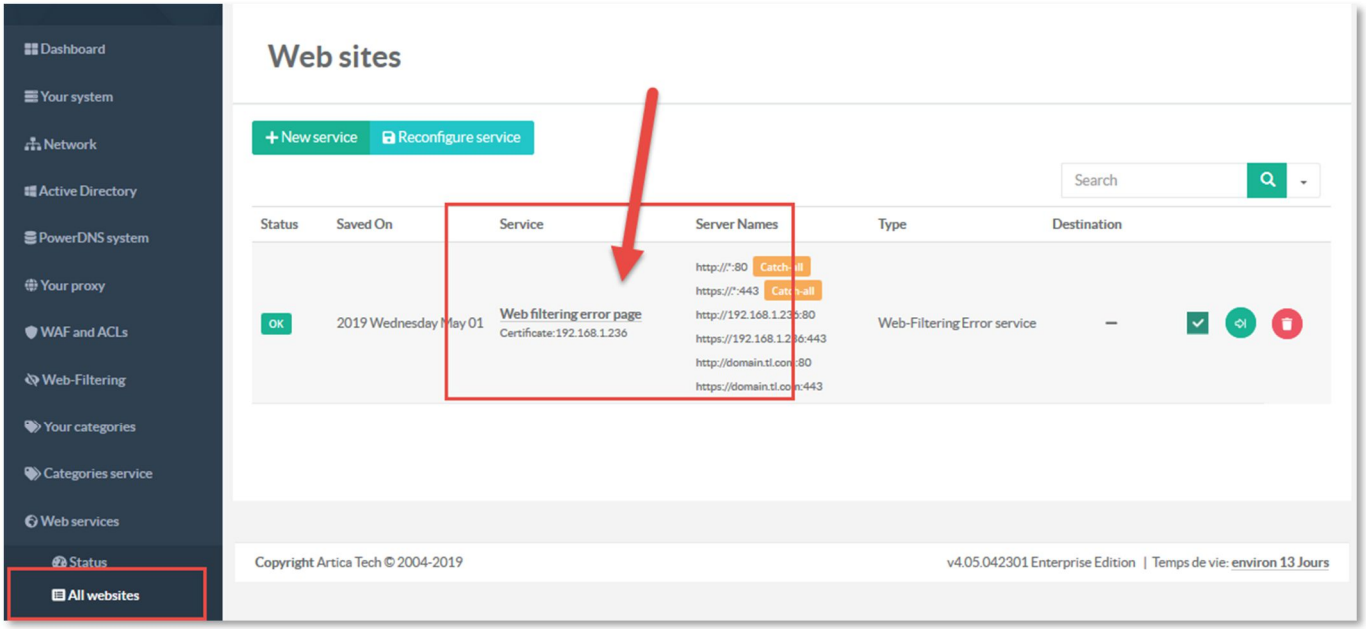
In the hostname field, you can type any hostname, virtual hostname (eg: denied.company.com, block.mydomain.com) that must be already resolved in your DNS server

If you did not want to handle any hostname in DNS for the Web-Filtering error page, set the IP address of this server.

Click on Next to create the Web-filtering Error page service and the redirect address setting on the Web-Filtering service.

Tune the Web-filtering service

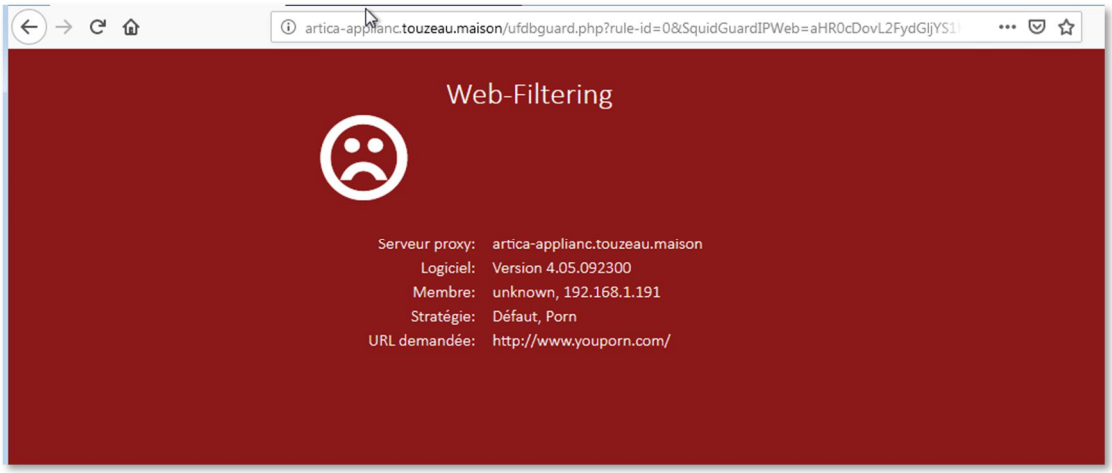
- The wizard simply creates the Web service and add a virtual host.
- You can display created settings using the **"Web services / All websites**" left menu.
- You will see a new service called "**Web filtering error page**"



Skin the Web-filtering error page

The Web-filtering error page use "**Templates** " (see Errors pages and Templates section).

By default, you should see this error page

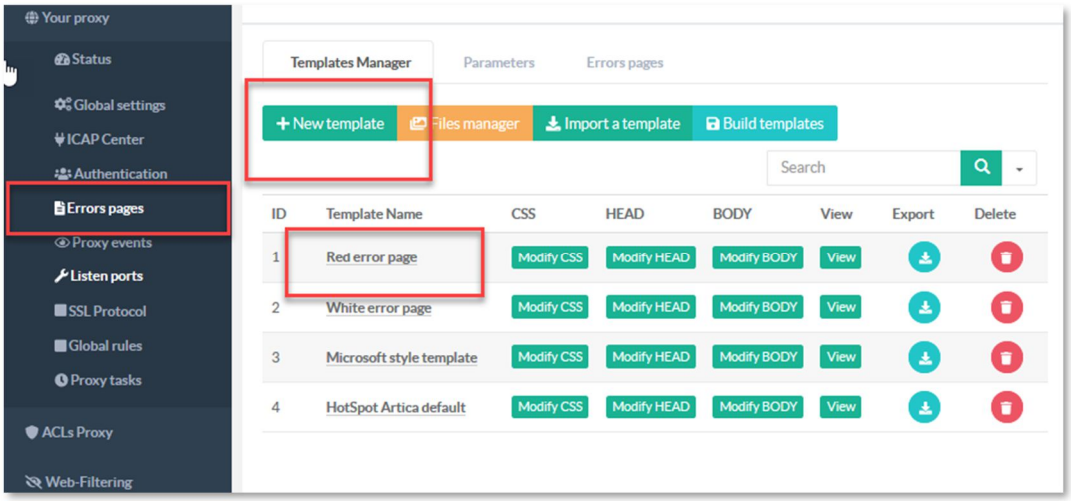


Using the Enterprise license, you can skin this web-filtering error page

Artica using **templates** to generate the error page.

Manage templates

To modify a template, on the left menu, choose "Your Proxy" and "Errors pages"



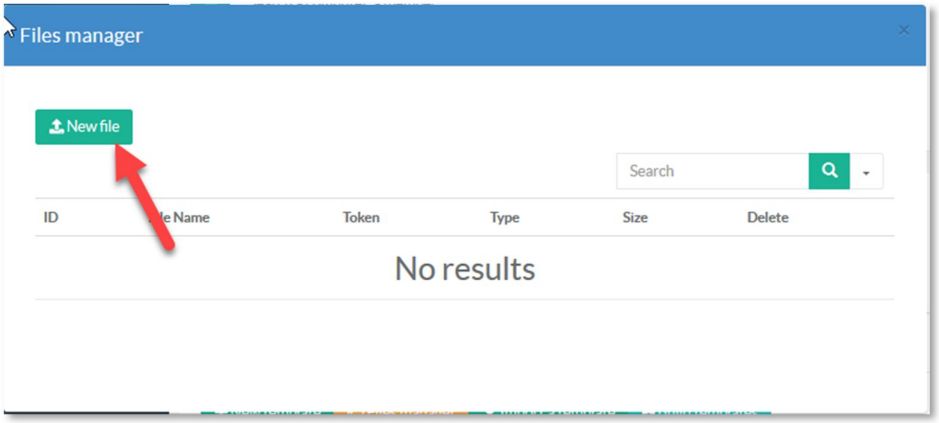
This section display default templates you can use on the Error pages generated by the proxy and by the Web-filtering.

You can create a new template or modify the default called "**Red Error page**".

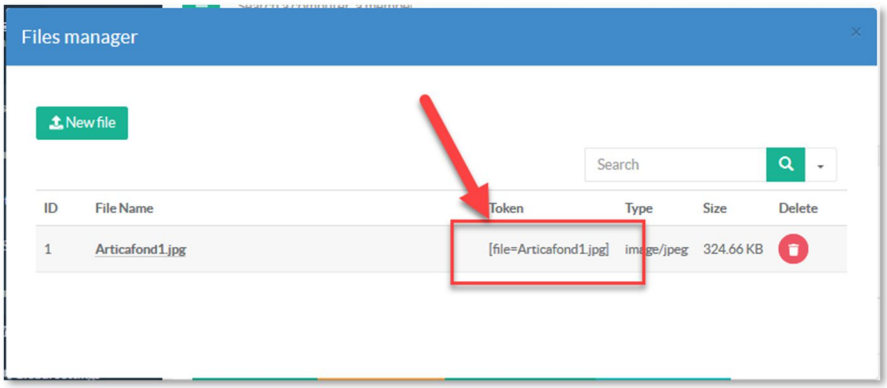
Templates can be modified using HTML code.

Using images in your template

Procedure is simple, click on the button "**Files Manager**"

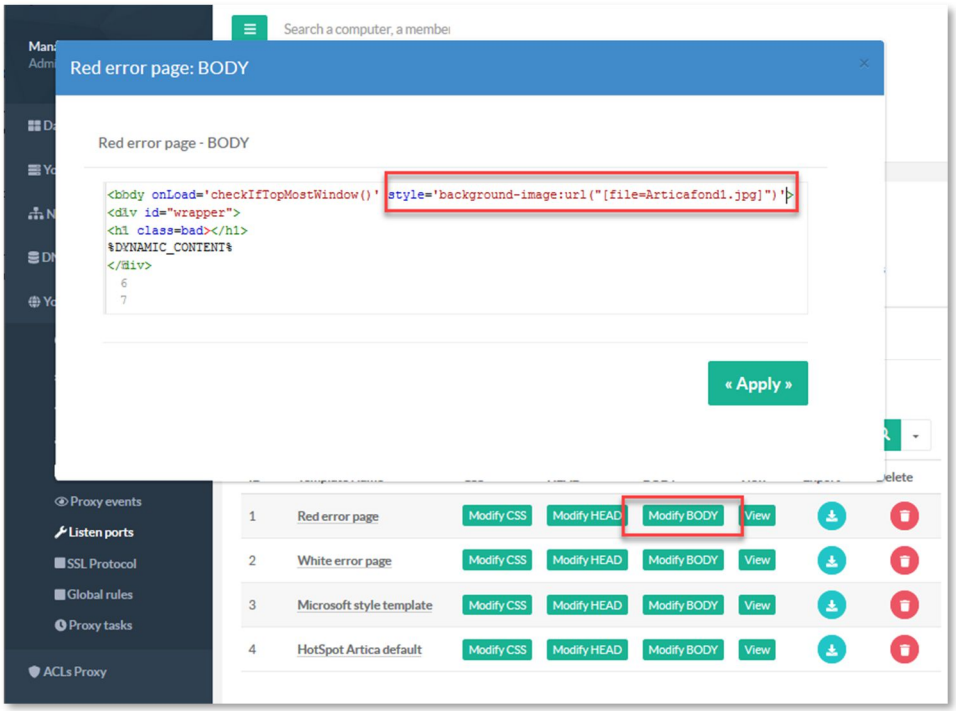


A new page is displayed and allow you to upload your pictures.
Click on the button "**New file**" in order to upload your image file in the File Manager area.



Once your image is uploaded, you can see in the "**Token**" column the code you have to insert in your HTML template, in our case this is **[file=Articafond1.jpg]**
For example, we want to use this image as background, we add in the BODY

```
style='background-color:white;background-image:url("[file=Articafond1.jpg]")'
```



Did not forget to click on "Build templates" button to make changes in production mode.

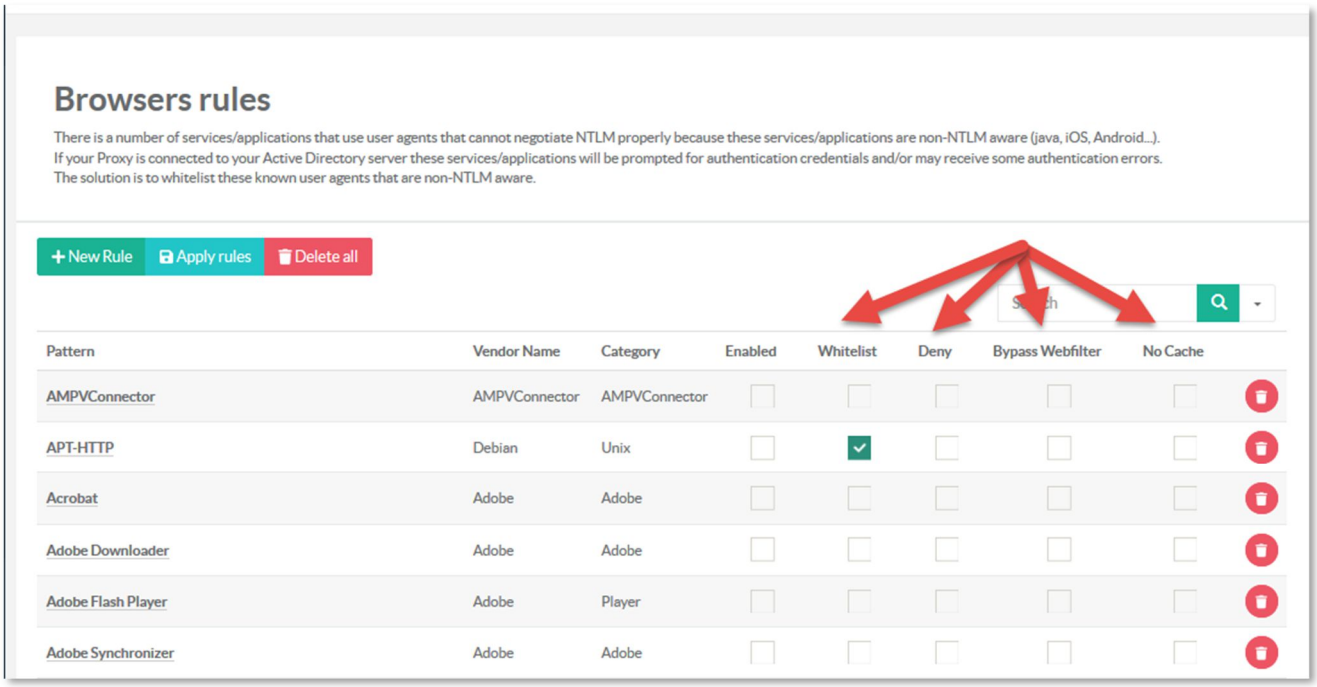
Browsers Rules

Browsers rules is a dedicated section that allows you to define proxy behavior based on User-Agents string.

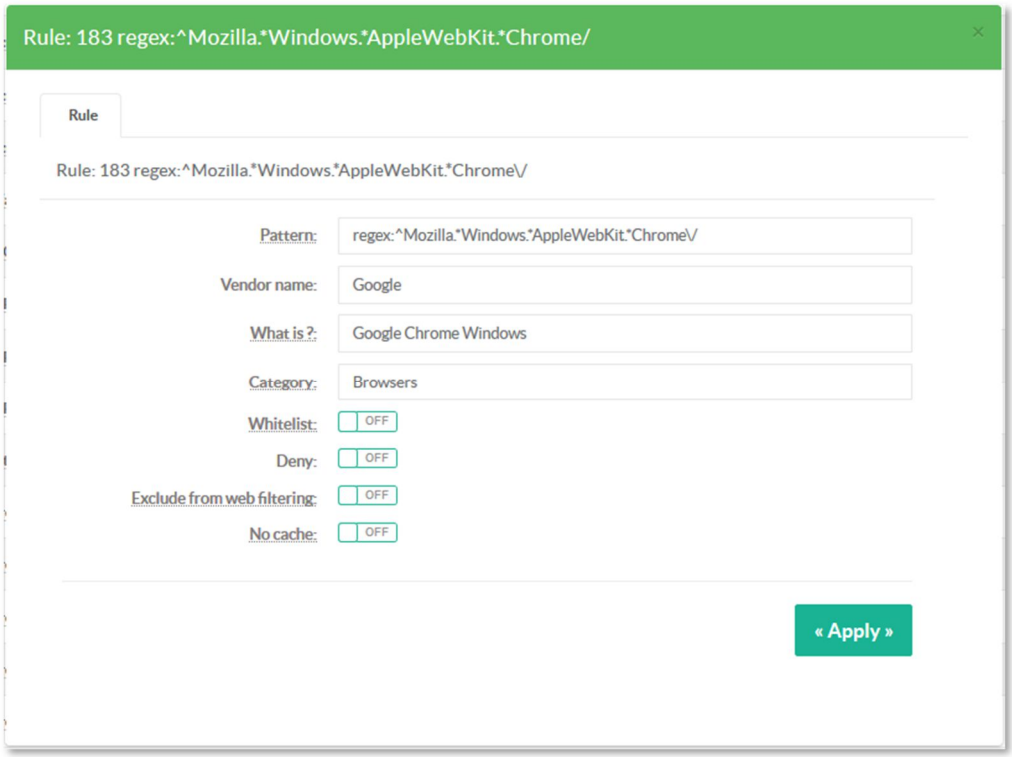
Artica provide for you a set of examples that are not enabled.
The table display privileges that you can define for each pattern that matches the User-Agent string sent by web applications.

Privileges are:

1. **Whitelist**: Means pass trough the proxy processing with any issue (Authentication methods, deny rules…)
2. **Deny**: Deny access When requests use the defined User-Agent string.
3. **Bypass** Web filter: Do not query the Web-Filtering engine when User-Agent string matches.
4. **No Cache** Do not cache content



A rule is defined by a "Pattern" (a regex with the prefix "regex:") that help the proxy to matches the user-Agent string.
Vendor name, category and what is are optional.



Bandwidth rules

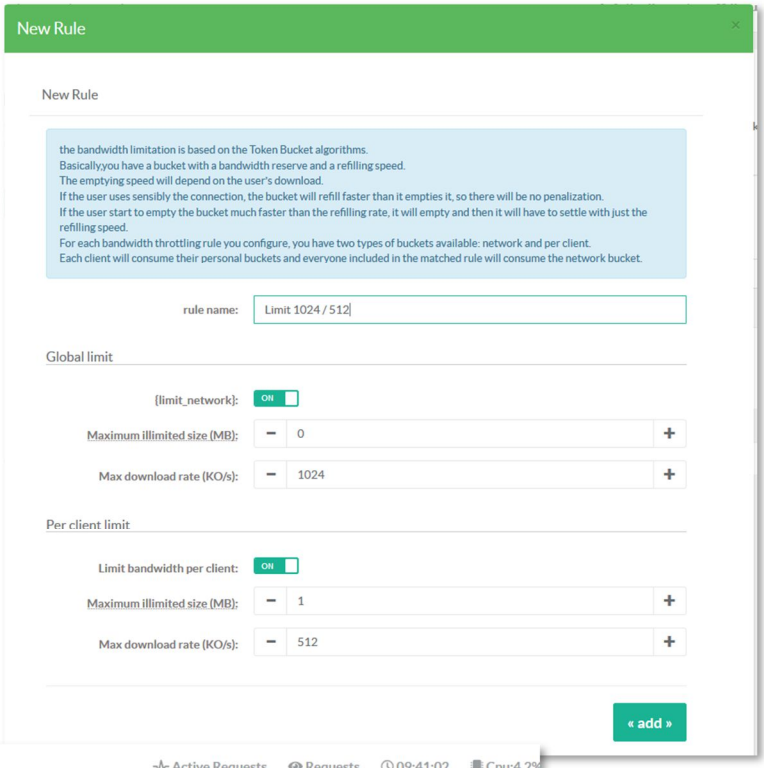
Bandwidth rules allows you to implement a flexible limit to control the bandwidth used by your members during HTTP sessions.
The purpose of the engine is to "reduce" the HTTP bandwidth. The proxy service manages only this protocol.
Others protocols that are not passing through the proxy are not affected.

When you create a new rule, the from allows you to limit the bandwidth according 2 sections:

Limit the network: Set a limit of **all** objects that matches the rule to the defined value after downloading a size in an unlimited bandwidth.

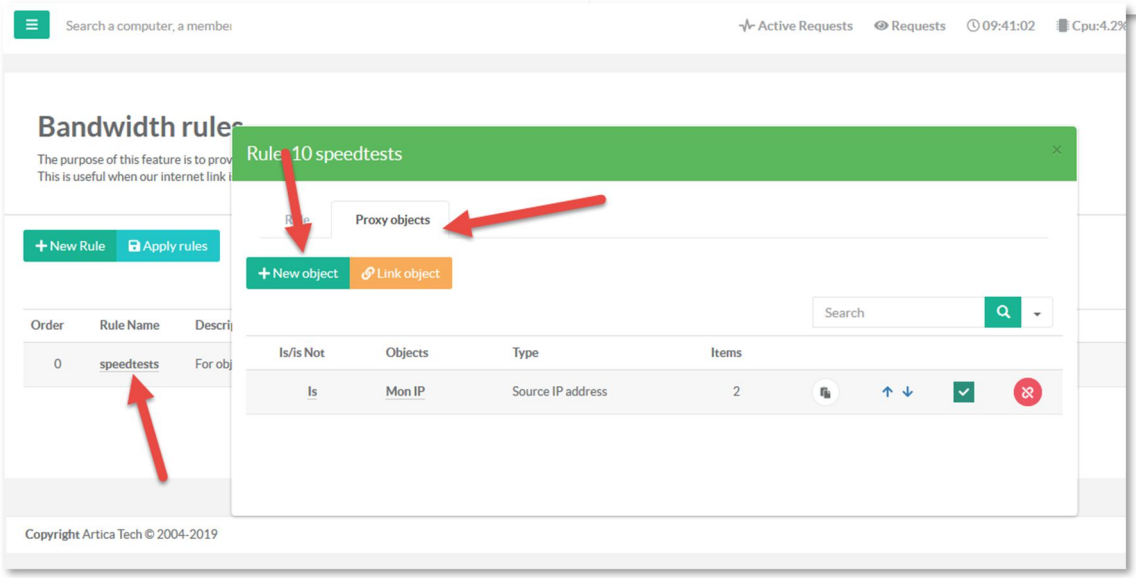
Limit bandwidth per client: Set a limit of each object that matches the rule to the defined after downloading a size in an unlimited bandwidth.

In our example we limit the network to 1024 KO/s immediately (0 unlimited size) and we limit each client to 512 KO/s after downloading 1MB.



Select the new created rule in the table and click on the "**Proxy objects**" tab.

Proxy objects defines when the bandwidth rule is activated by the proxy.



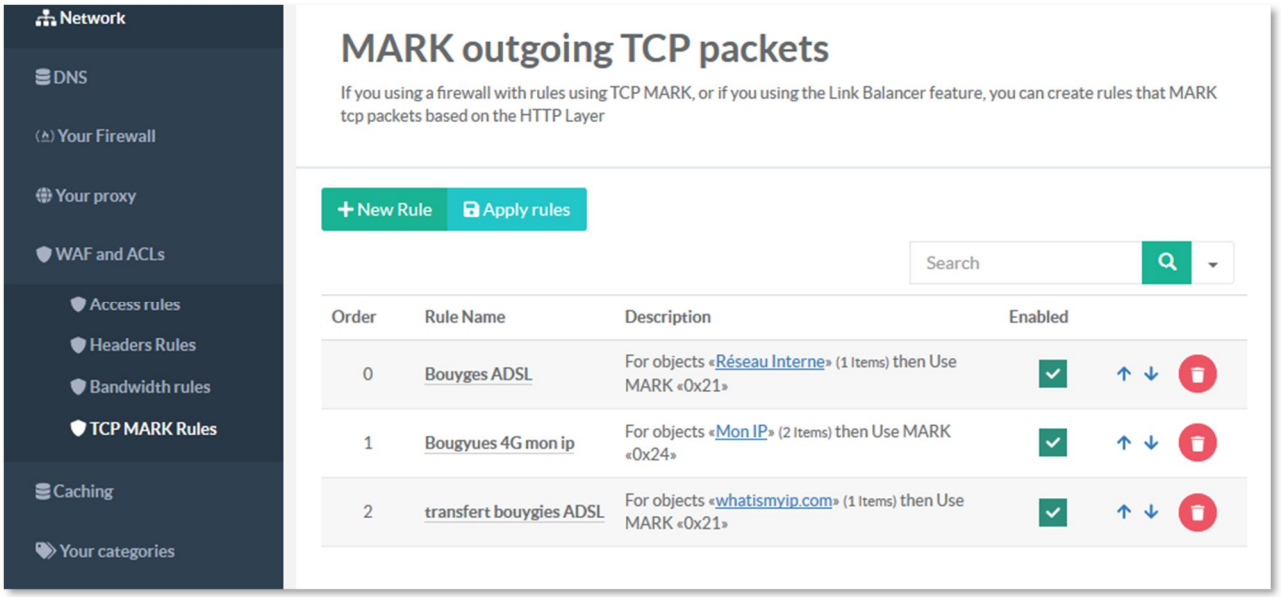
You can add several objects in the same rule, this means that all object must matches to activate the rule.

For example: if you add an "**IP source**" object with 192.168.1.0/24 value and a **Destination Website** object with "googlevideo.com", this means that you will reduce the bandwidth only when a computer that matches the 192.168.1.0/24 network downloading something from googlevideo.com.

TCP MARK Rules

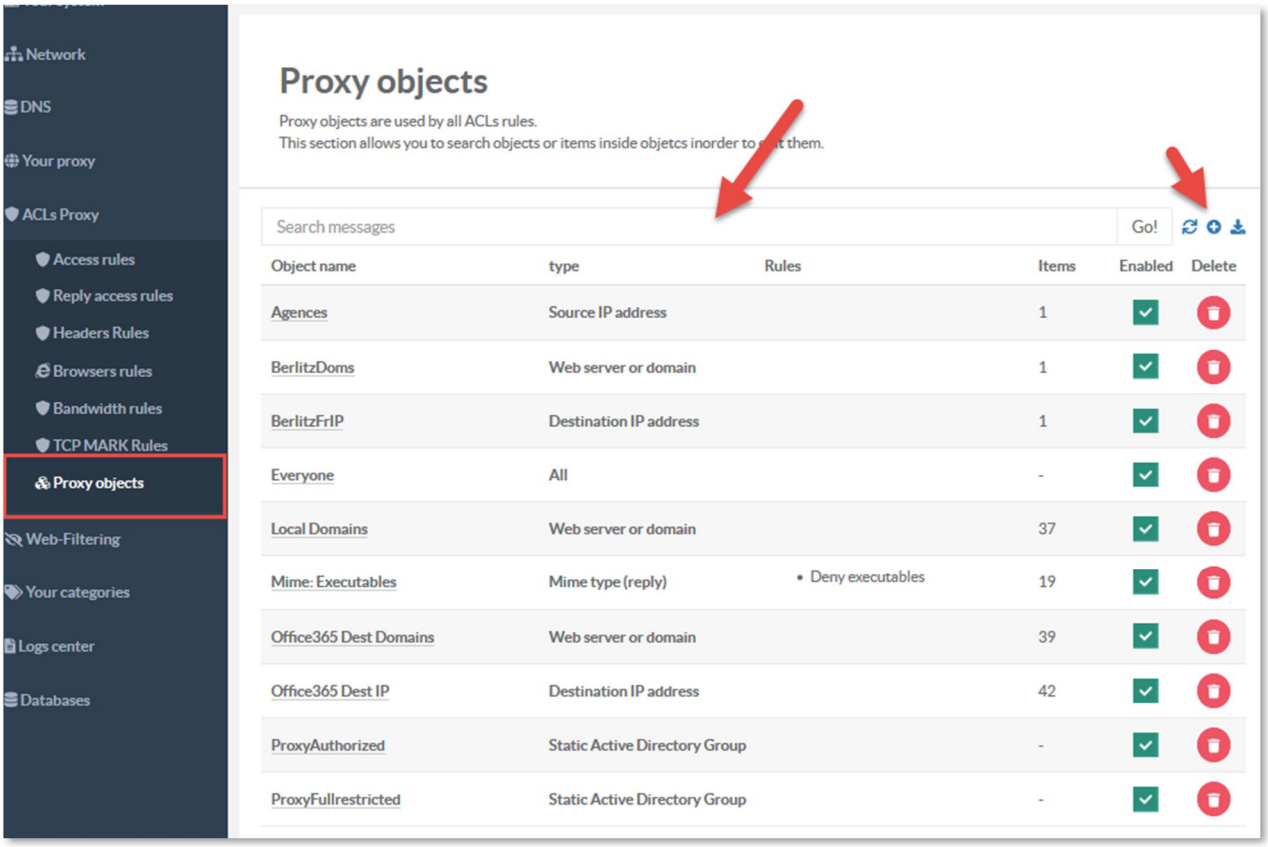
TCP MARK rules allows you to MARK TCP packets for the proxy requests to the Web sites. In this case, you are able to detect TCP Mark in your firewall to balance request to a specified firewall Interface.

You can use these ACLs in combination with **Link Balancer** feature (Link Balancer feature allows you to balance multiple bandwidth)



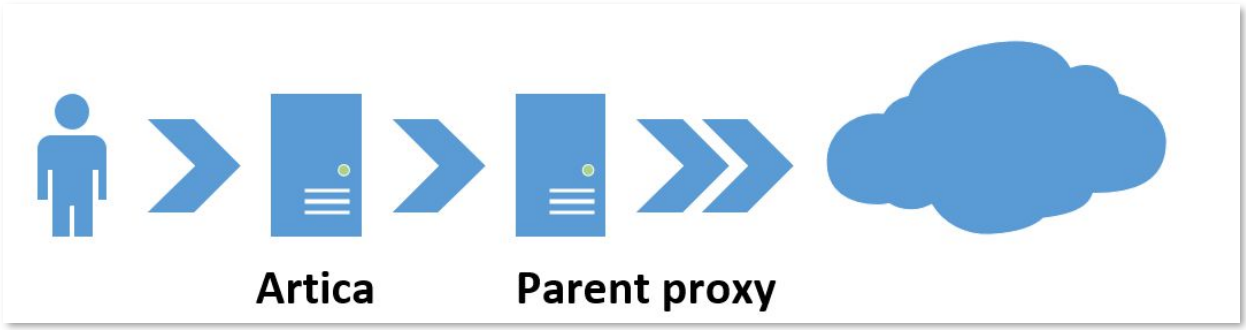
List all ACLS objects

Advanced ACLs use proxy objects in order to operate HTTP rules.
The "Proxy objects" section allows you to search objects or items inside objects (use the "Search field).
This table list all rules used by the same object.
You can delete or disable an object here; it will be removed from all rules.



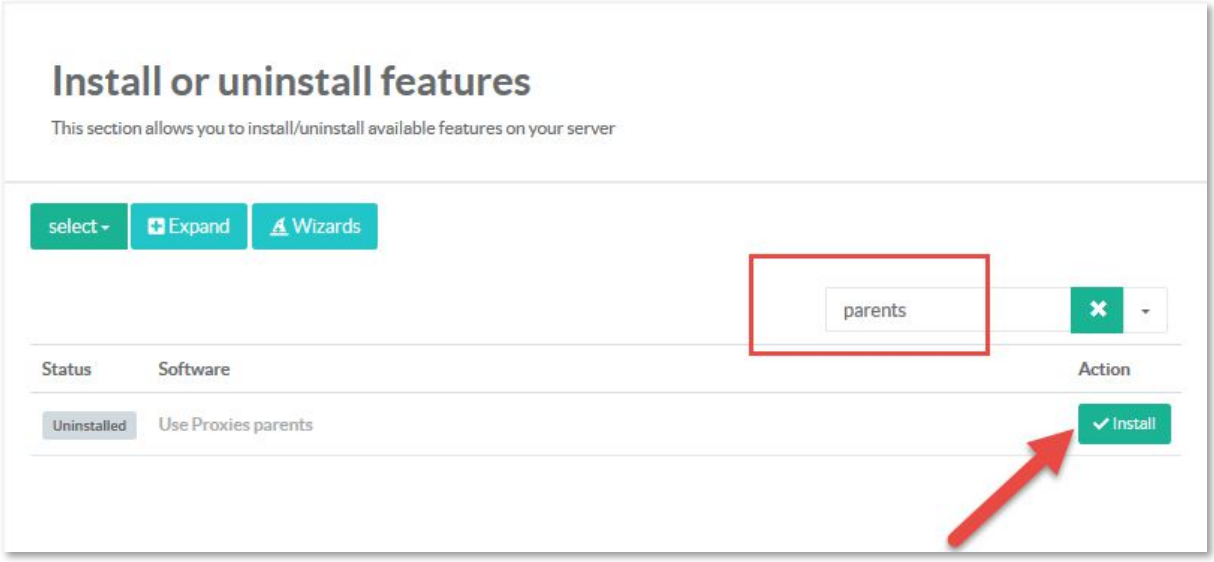
USE UPSTREAM PROXIES

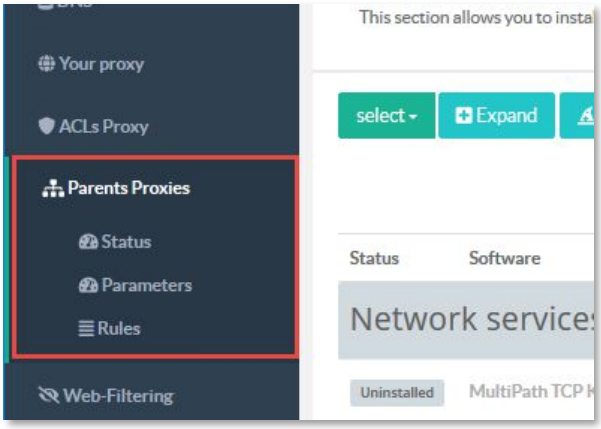
Your Artica server can be installed inside the LAN and for network reasons must use parent proxies in order to access to Internet.



To use parent proxy, you need to install the "**Use Proxies parents**" feature.

- On the left menu, choose **Your system/ Features**
- On the search field, type "**parents**"
- Click on the **Install** button near the "**Use Proxies parents**"



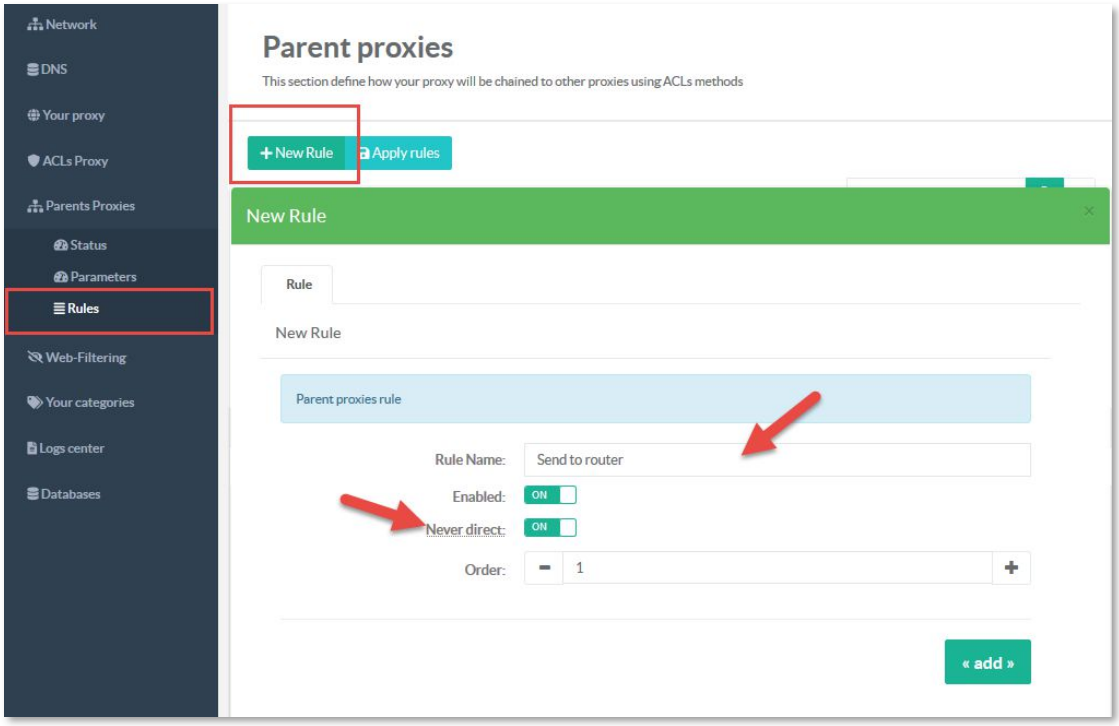


After installation, a new "Parent Proxies" item is added with the following features:

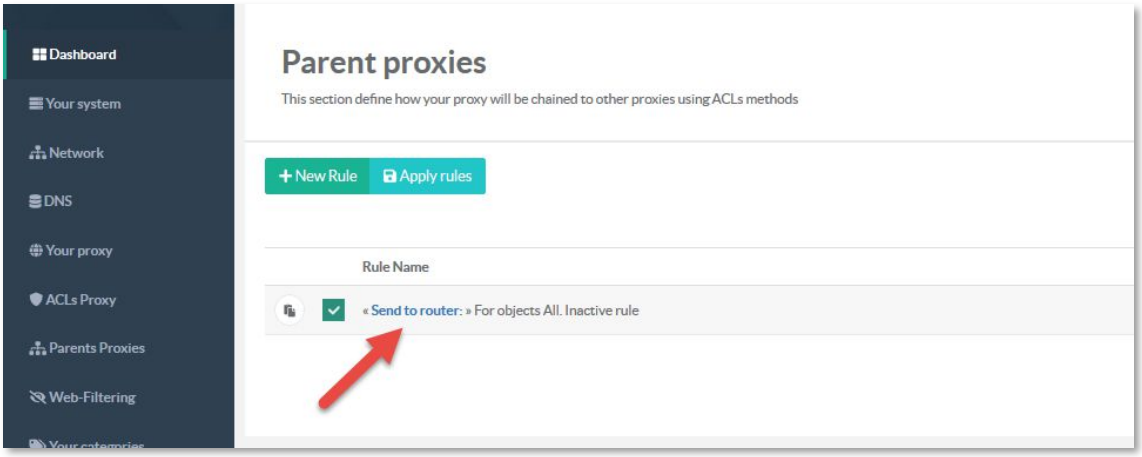
Status: display if your parents proxies are available.
Parameters: General options.
Rules: Rules that define how to redirect requests to parents.

Parent Proxies rules

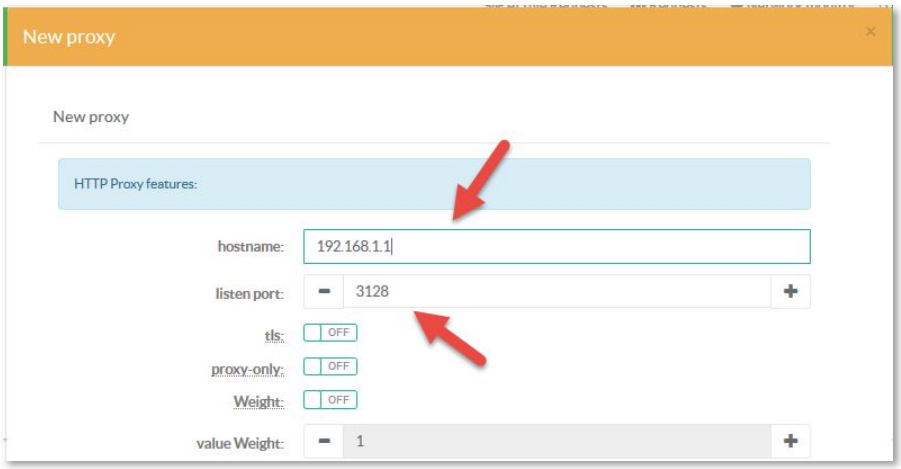
After click on "**New Rule**" a first form asks to you your **Rule Name** and if the rule enforce the proxy to use the parent proxy for any cases, if "**Never direct**" is turn to on, all requests from your Artica server will use the defined proxies.



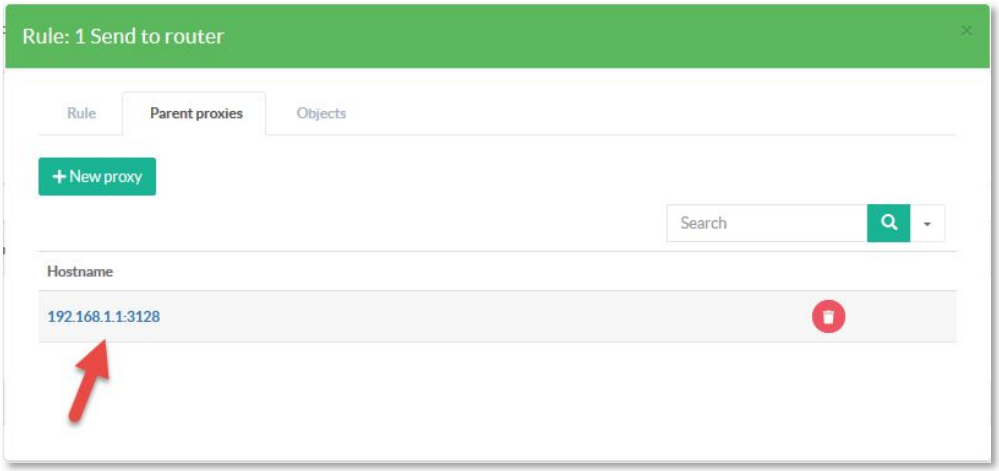
Select you created rule



Choose **Proxies** tab and create a new proxy configuration
Add the address of your parent proxy and port (define options if needed)

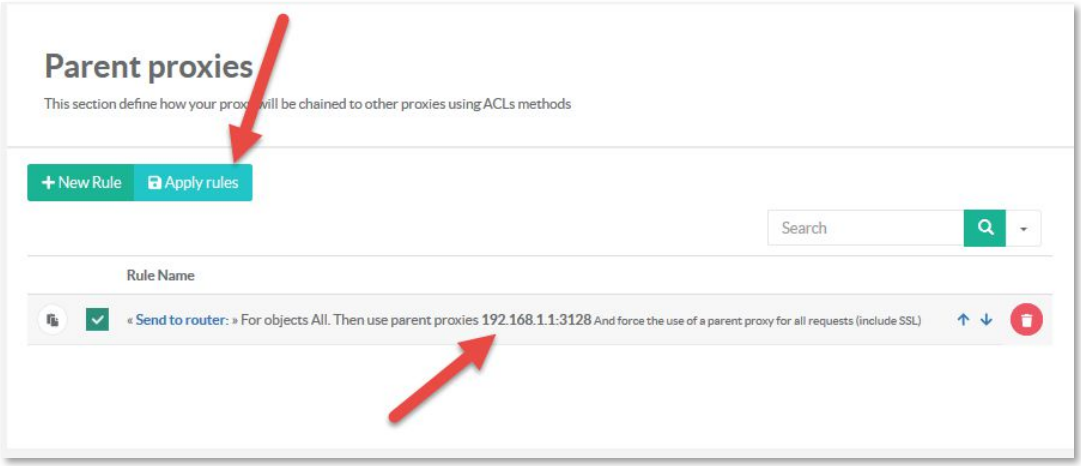


You parent proxy is now affected to your rule.

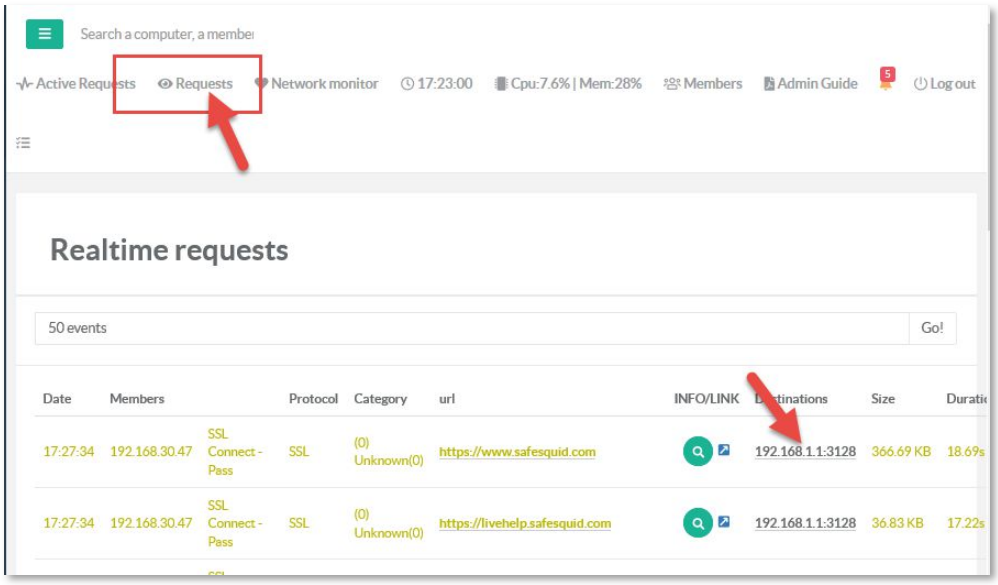


You can enforce the behavior with this proxy by using **objects** section (like a standard ACL), but just add a parent proxy and enforce the use of parent proxy is enough.

Did not forget to "**Apply rules**" after define your proxies.



If you see the "Requests" in real-time, you will see that all requests are forwarded to the defined proxy.

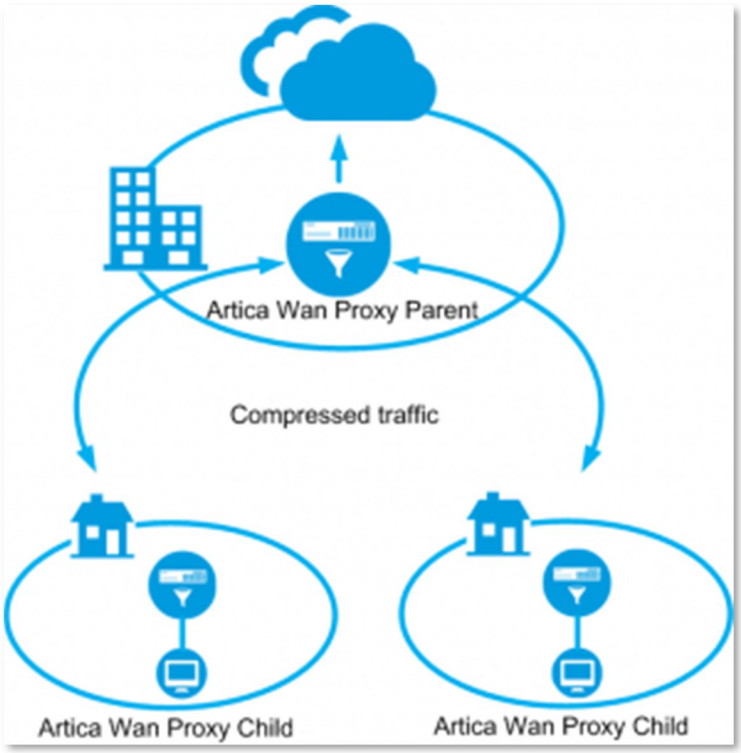

Search a computer, a member
Active Requests
Requests
Network monitor
17:23:00
Cpu:7.6% | Mem:28%
Members
Admin Guide
Log out
Realtime requests
50 events
Go!
Date
Members
Protocol
Category
url
INFO/LINK
Destinations
Size
17:27:34
192.168.30.47
SSL Connect - Pass
SSL
(0) Unknown(0)
https://www.safesquid.com
192.168.1.1:3128
366.69 KB
18.69s
17:27:34
192.168.30.47
SSL Connect - Pass
SSL
(0) Unknown(0)
https://livehelp.safesquid.com
192.168.1.1:3128
36.83 KB
17.22s

WAN PROXY COMPRESSOR

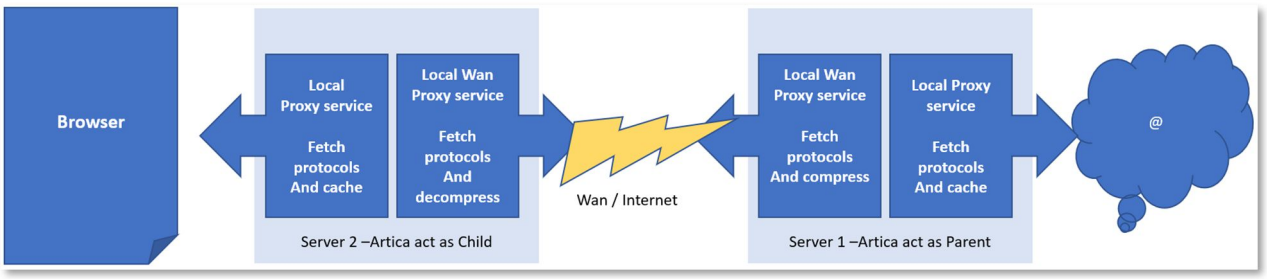
What it is ?

Wan Proxy compressor is designed for companies that use remote offices or using a dedicated cloud.
The feature is designed to compress TCP protocol in order to increase the bandwidth.

The Wan Proxy compressor must use **at least 2 Artica servers**.



1. The first one act as Parent proxy, it is designed to fetch Internet content and compress it.
2. The second is designed to fetch compressed content from the parent proxy, decompress the protocol

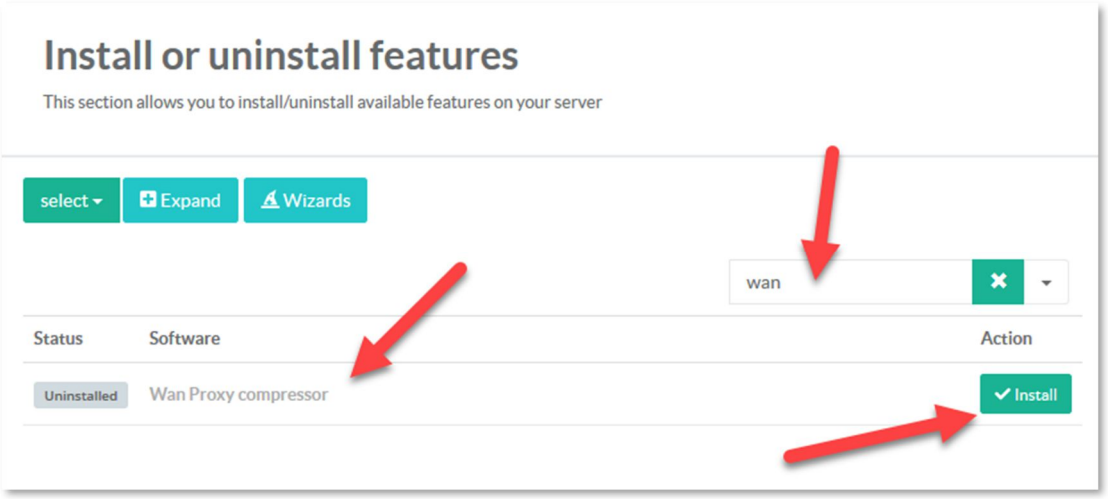


Inside each box the local proxy and the Wan proxy exchange the compressed protocol and is able to cache content.

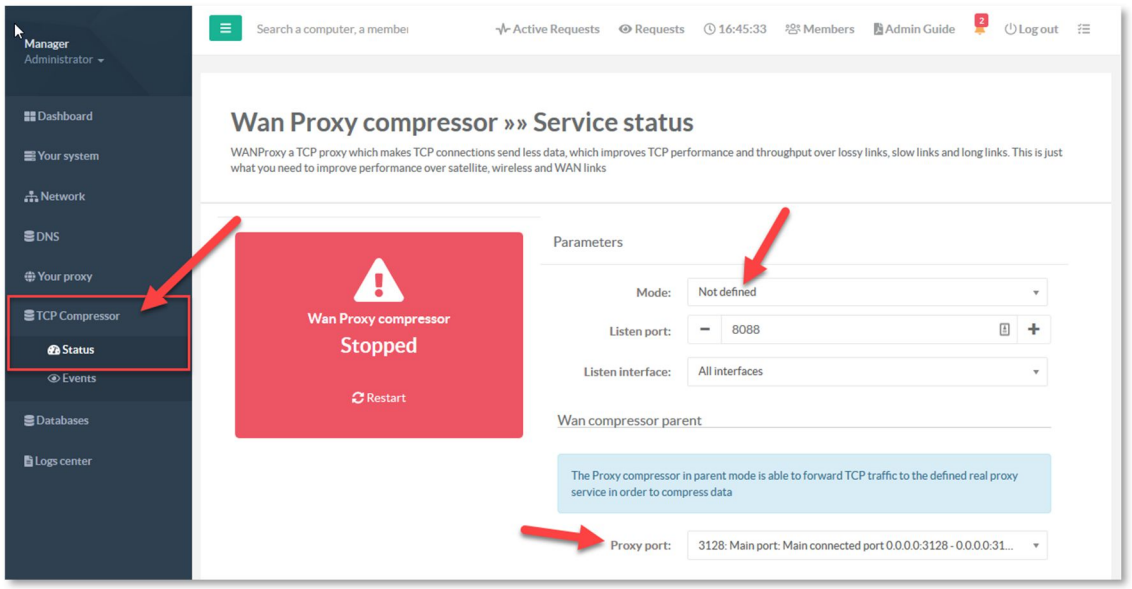
Wan Proxy parent mode.

You needs first to install the proxy service through the Features section

- After installing the proxy service, in the Features section, type "**Wan**" in the search field.
- Click on the **Install** button on the **Wan Proxy Compressor** row.



- On the left menu, click on "**TCP Compressor**" / **Status**
  You will see the status in red mode, this is normal the Wan Proxy compressor must be setup.
- Switch to Wan Compressor parent mode.
- Set the **listen port** that the Wan Compressor client must use
- Define the **listen Interface** to force the service to bind (**mandatory!!!)**
- Select the **Listen port of your HTTP proxy service** in order to let the Wan Proxy compressor to fetch pages.
- Click on **Apply** button.

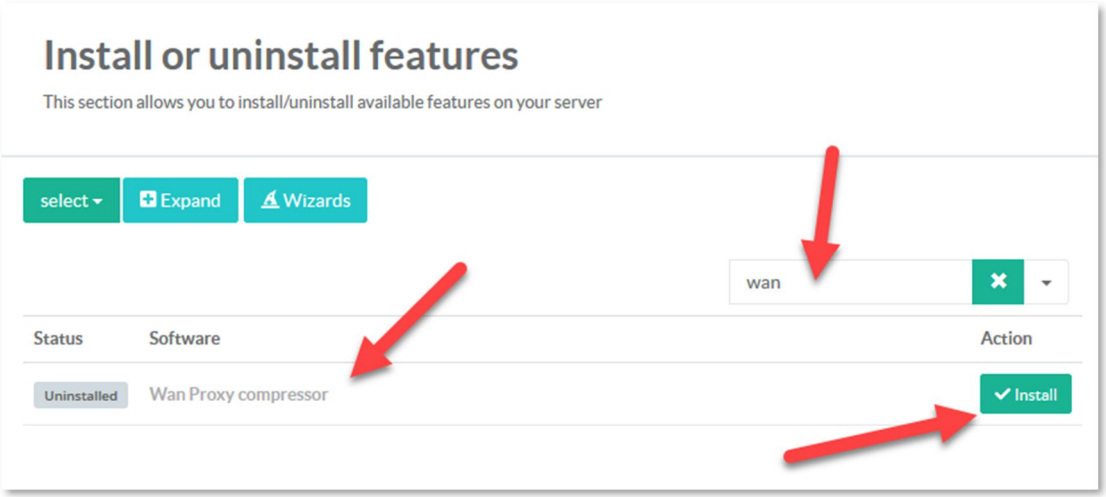


After Apply, the status must be switched to "green"

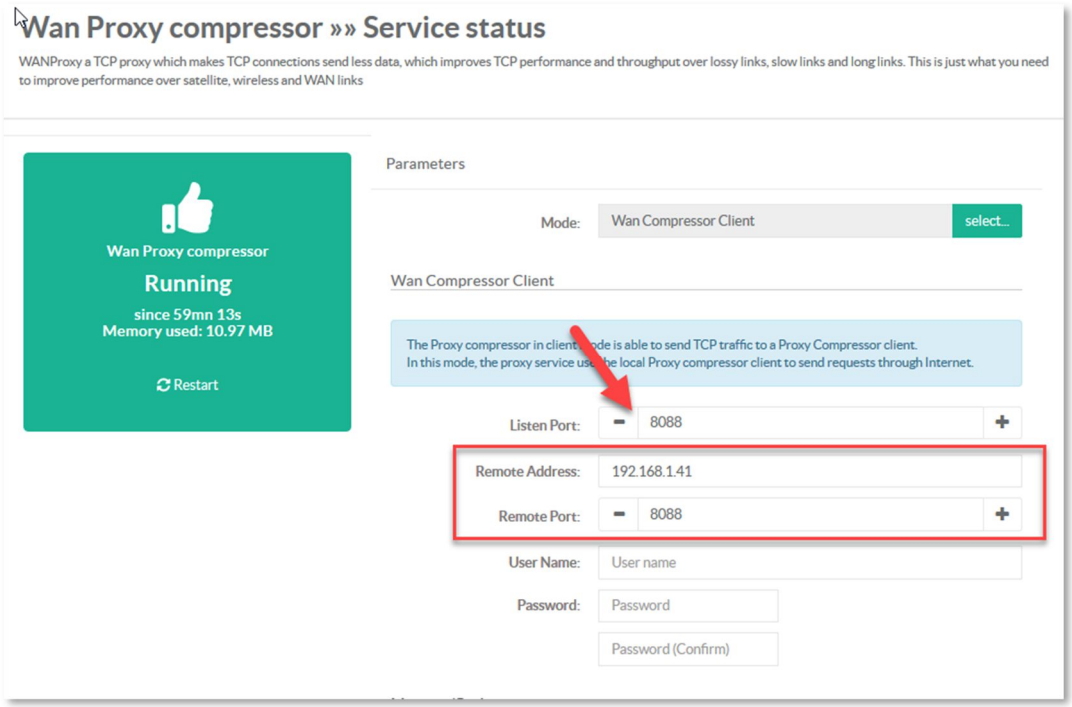
Wan Proxy client mode.

You needs first to install the proxy service through the Features section

- After installing the proxy service, in the Features section, type "**Wan**" in the search field.
- Click on the **Install** button on the **Wan Proxy Compressor** row.



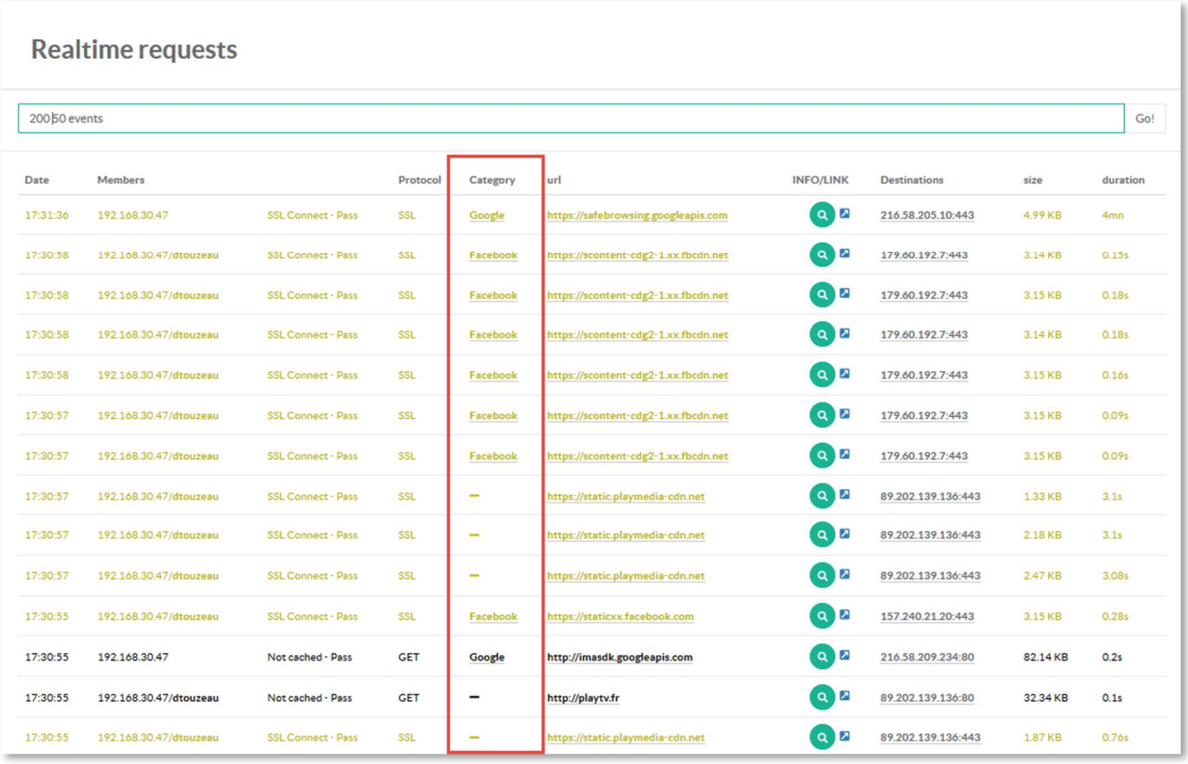
- On the left menu, click on "**TCP Compressor**" / **Status**
  You will see the status in red mode, this is normal the Wan Proxy compressor must be setup.
- Switch to Wan Compressor **Client** mode.
- Set the **listen port** that the local Proxy will use as Compressor client must use
- Select the address and the listen port of the remote WanProxy act as Parent
- Click on **Apply** button.



CATEGORIZATION

Categorization on the proxy is an important topic, Artica team try to categorize all web sites but it is a hard task.
Currently, Artica is able to categorize more than 35.000.000 of main domains/Public IP addresses.

When using the real-time logs, you can see that sometimes a category is associated with a domain.
By default, only a few domains can be categorized, TOP 50 of Internet sites are hard coded inside the Artica engine.



Benefits

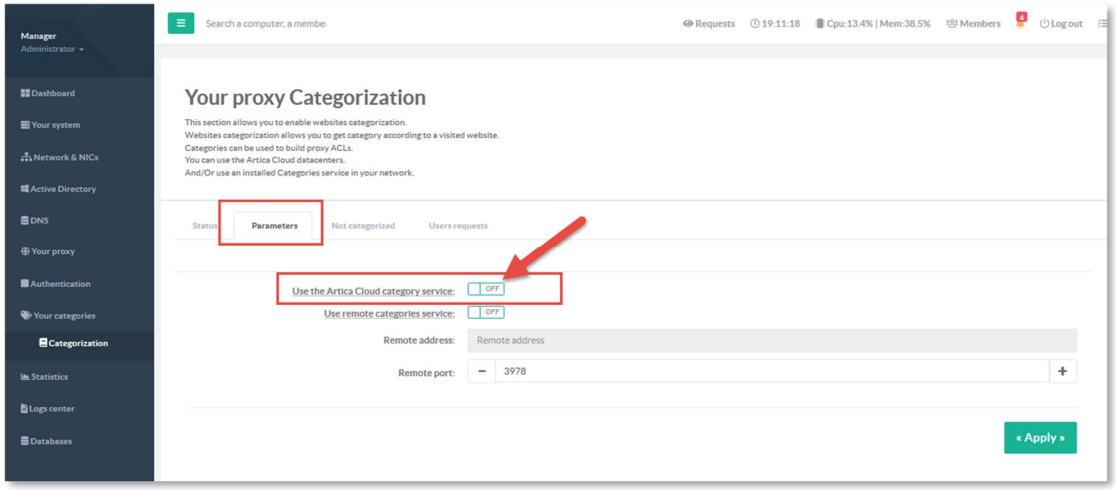
Using categories provide 3 benefits:

1) **For statistics purpose**: You can extract statistics according bandwidth/requests/users per category.
2) **For ACLS in the Web Application Firewall**: You can create deny/allow rules according categories.
3) **For Bandwidth limit**: You can limit bandwidth according categories.

You can increase the categorization rate using 2 methods, **passive** method and **active** method.

The passive method

The passive method (REQUIRE ENTERPRISE LICENSE) use the Artica RESTful API to retrieve the category for each visited site.
In this method, your Artica server use only the "read-only" mode.
Your Artica server request to our servers based on the Internet which category is associated to the current requested site.
To enable the passive method, go to the "**Your categories/categorization**" on the left menu.
Select the "**Parameters**" tab
Enable the option "**Use the Artica Cloud category service**"



The Active Method

The Active method allows your Artica to query categories from a local service.
In this way, you are able to create your own categories.
The local service will be in charge of respond first with your categories and query Artica databases if your categories did not store the queried domain.

Using a local service requires:

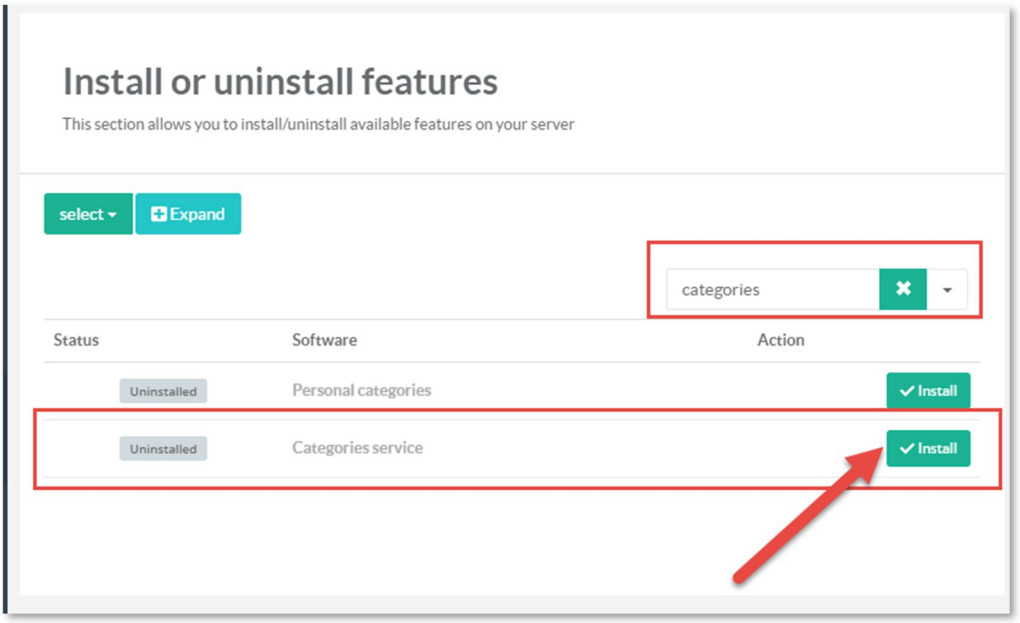
- At least 700 MB memory free. *If you plan to use Artica Databases the service should handle 3 GB of memory.*
- Download ARTICA databases periodically *if you plan to use Artica Databases.*

Benefits:

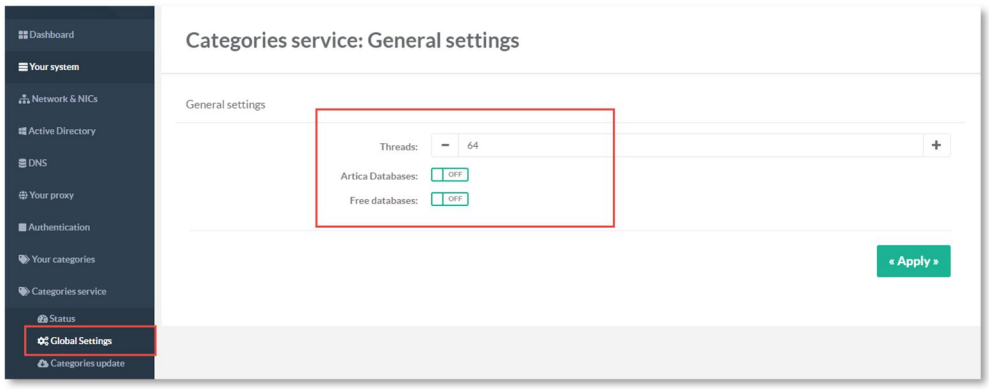
- Retrieve categories is faster than using the Artica cloud service.
- If you have other Artica servers, you can provide a local categories service shared between Artica servers.
- You can create and share your own categorization.

Install the category service.

On the "**features**" section, type "**Categories**" in the search engine.
Install the feature "**Categories service**"



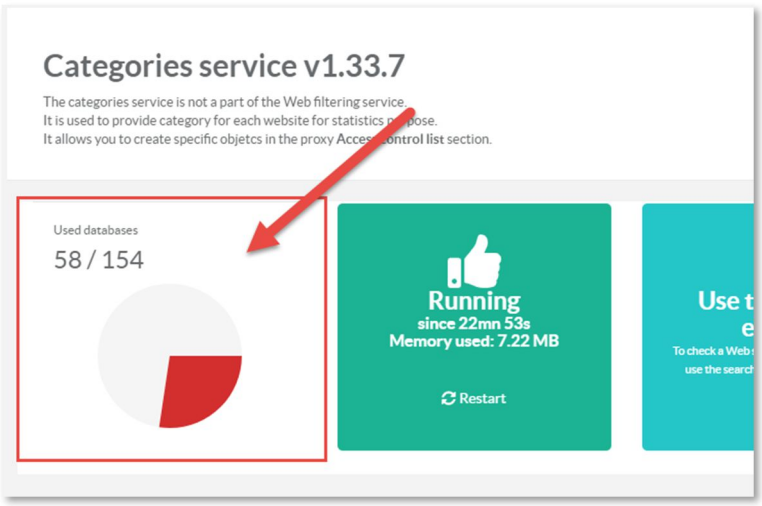
After installing the feature, the service is running using 0 database.
On the left menu, choose "**Categories service**" and "**Global Settings**"



You have to choose which databases you want to add into your category service:

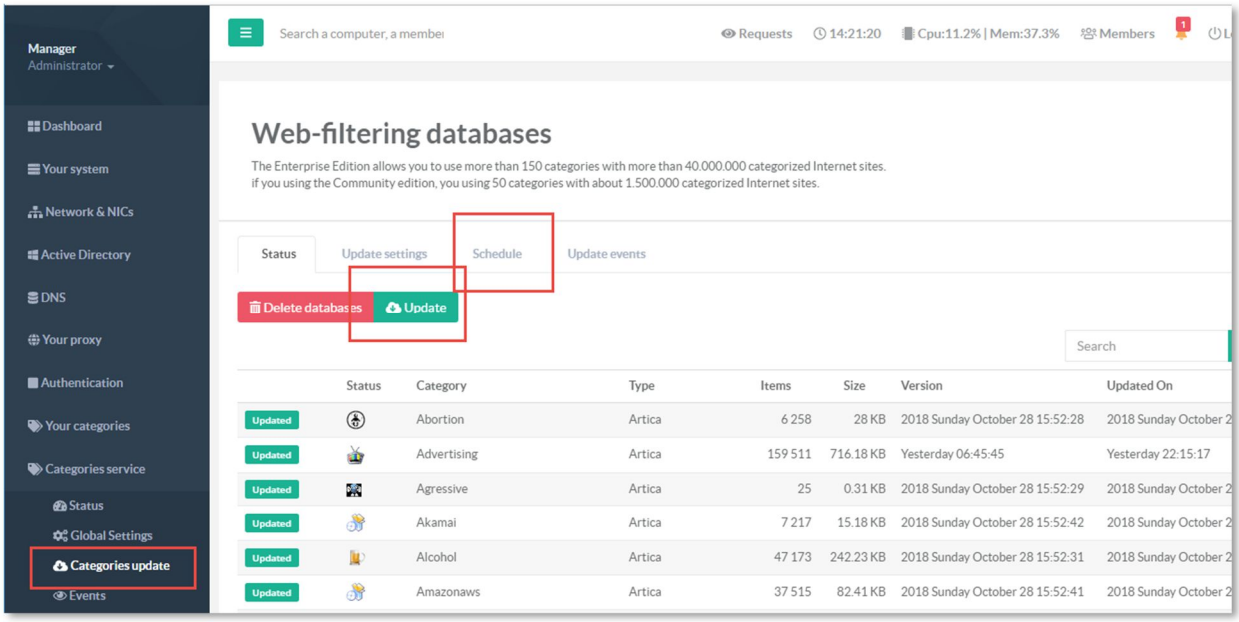
- **Artica database**: 150 categories, 55.000.000 of categorized websites - require 2.7GB of free memory (AVAILABLE WITH A CORPORATE LICENSE)
- **Free database**: 58 categories, 3.000.000 categorized websites - require 700 MB of free memory.

After enabling public databases, the status displays the number of categories used on your server.



Define the schedule for updating database.

Select the menu "**Categories Update**".
The status tab displays all databases downloaded from your server.
By default, Artica updates databases **each day at 03:00 AM**, you can change it inside the "**Schedule**" tab.
If you need to perform update now, click on the "**Update button**"



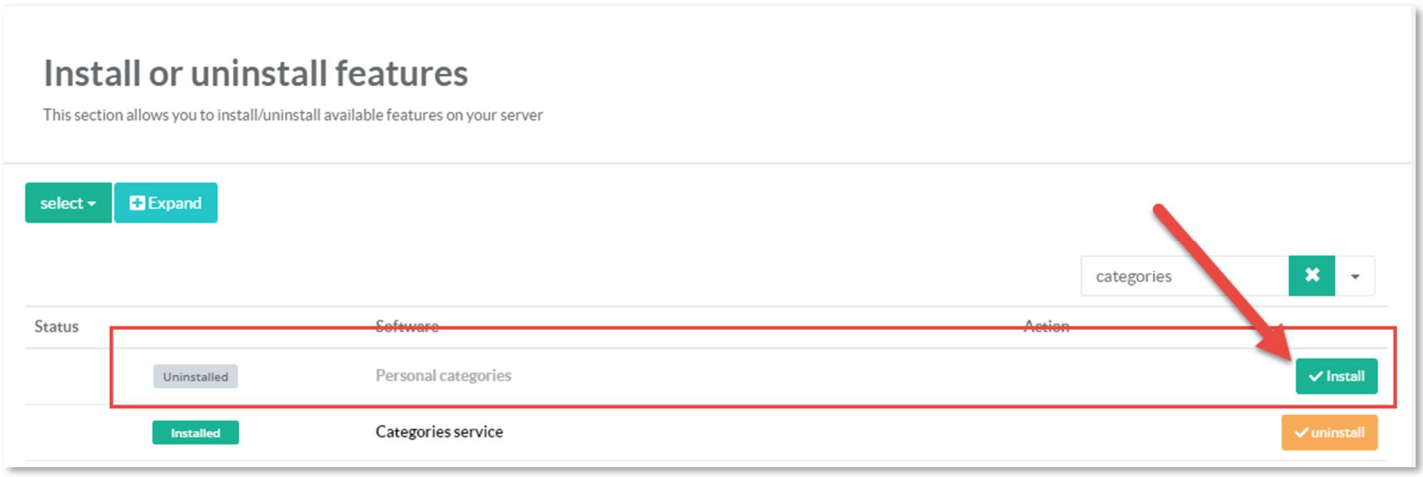
Create your own categories

With Artica you're allowed to build your own categories.
This feature adds several benefits for your Categorization/DNS filter/Web-Filtering service:

1. Your categories overload the public databases, you are able to enforce a website to be categorized in another category.
2. You can categorize a website without need to wait Artica Team to release a new public database.
3. You can manage your categories thought RESTful API.

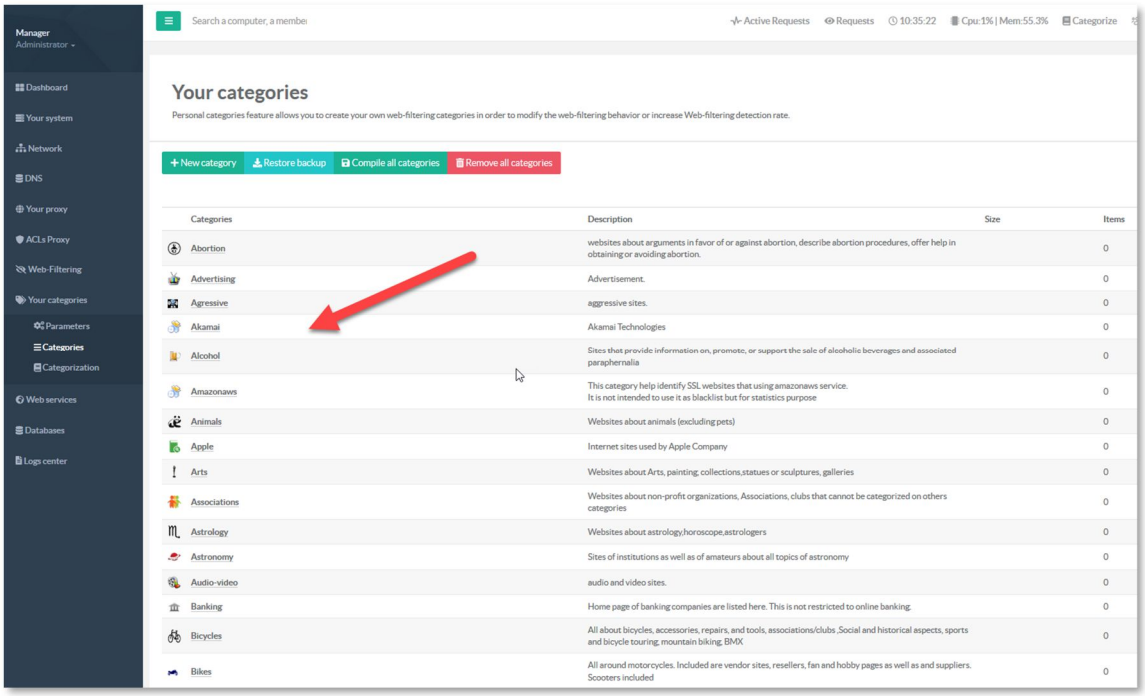
Install the personal categories feature

To enable personal categories, go into the **features** section and install the "**Personal categories**" feature (THIS FEATURE REQUIRES AN ENTERPRISE LICENSE).



List Categories

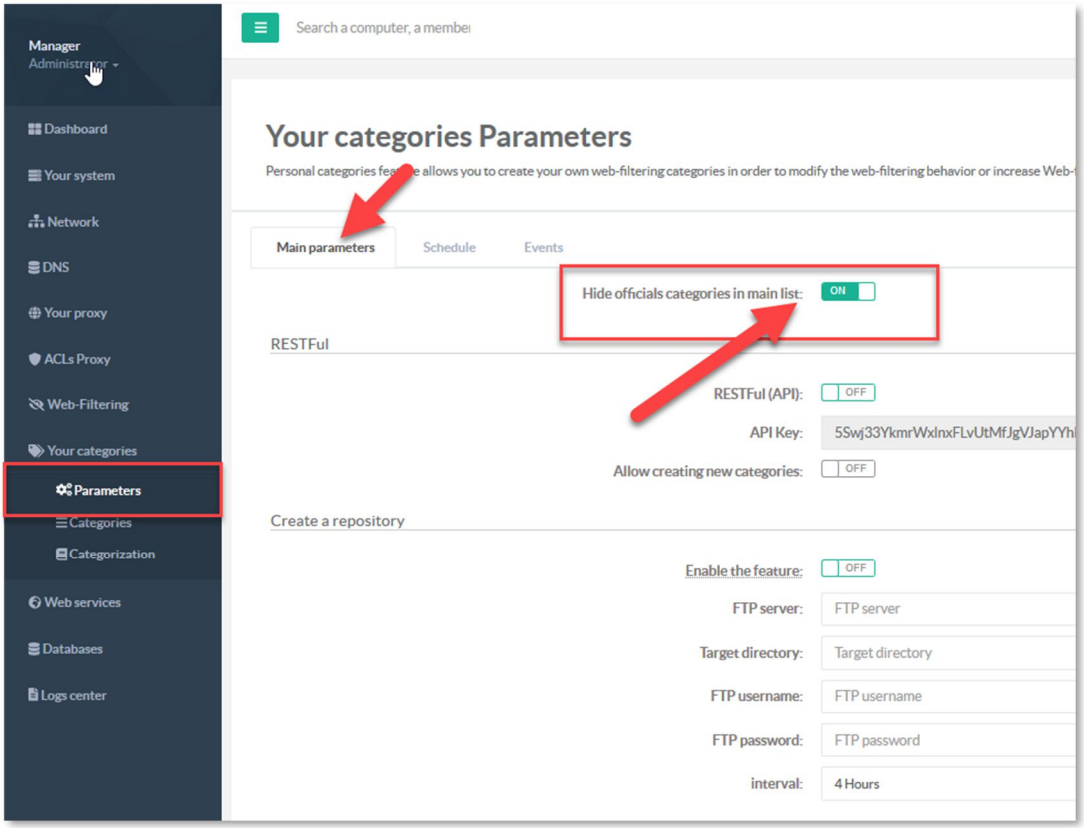
In Your Categories / Categories, you can list all available categories (Officials categories provided by Artica and your categories)



List only your categories

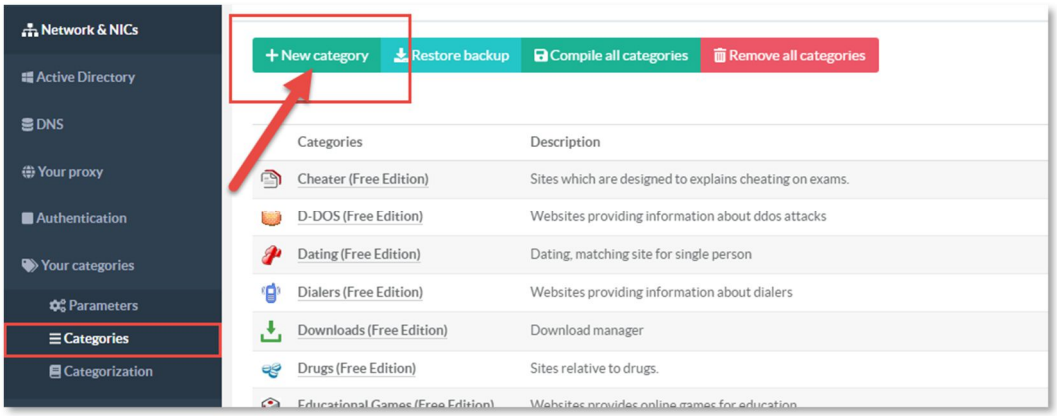
If you wan to hide officials categories, on the left menu click on "Your categories/Parameters" on the left menu.

- Turn on "**Hide officials categories in main list**"
- Click on **Apply** button

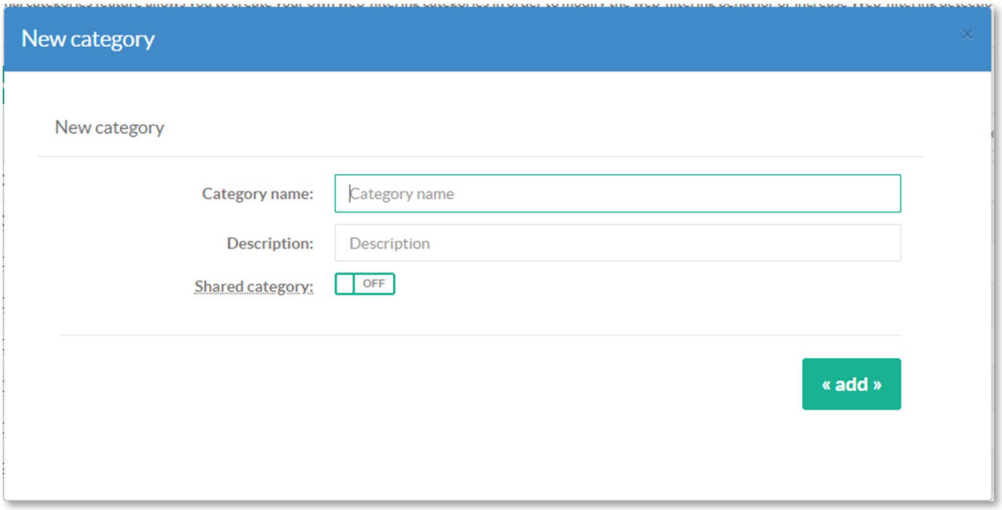


Create your first category

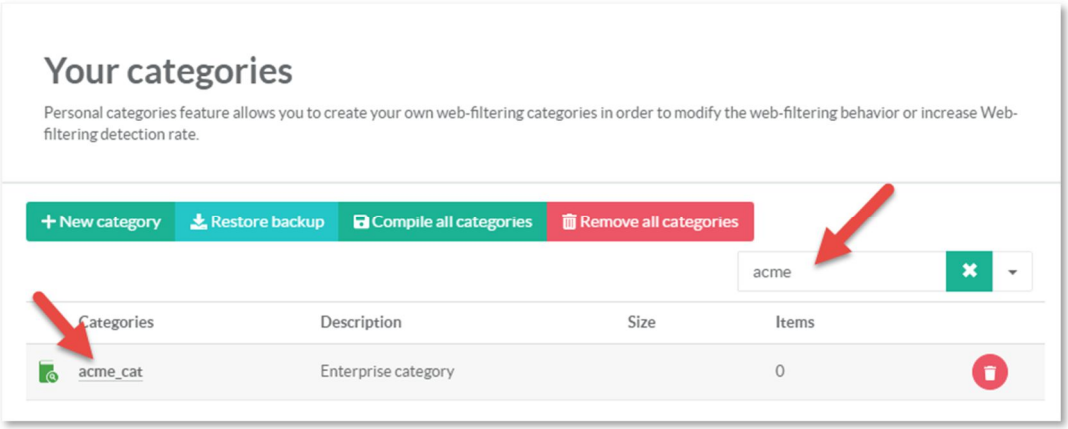
After installing the Personal categories, on the left menu, choose "**Your categories**" and "**Categories**".
In this section, Artica lists all available categories.
When creating a new category, ensure its name will not the same in officials' categories.
If you want to remove officials' categories, go into "Your Categories" and parameters, enable the checkbox "**Hide officials' categories in the main list.**"



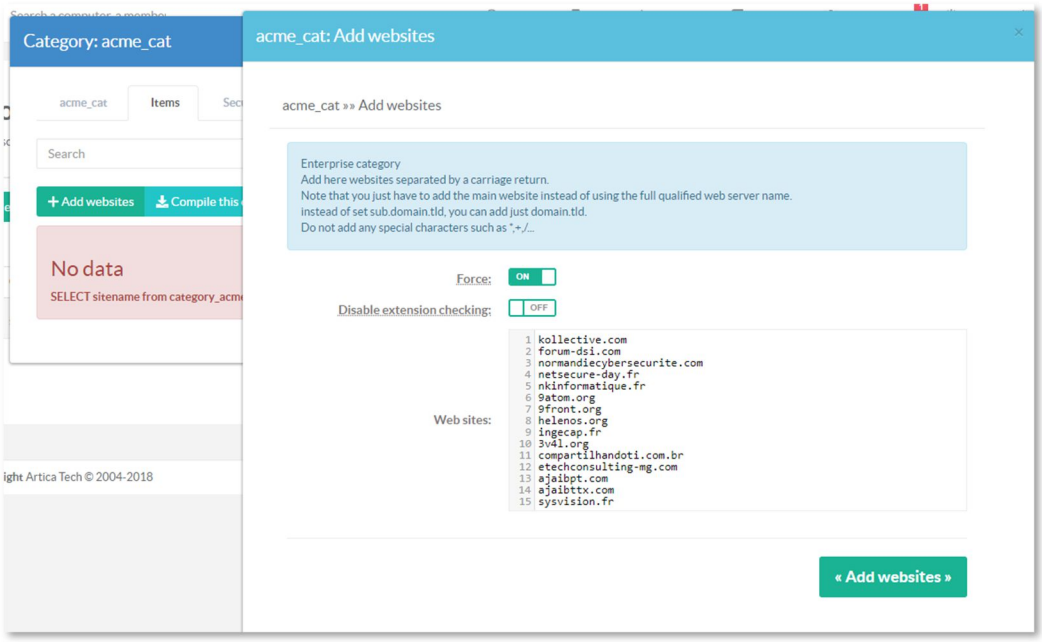
Give the **category name** and the **description**.
The "**Shared**" category allows your members to add/remove items inside this category.



After creating your category, search it inside the table and click on it.

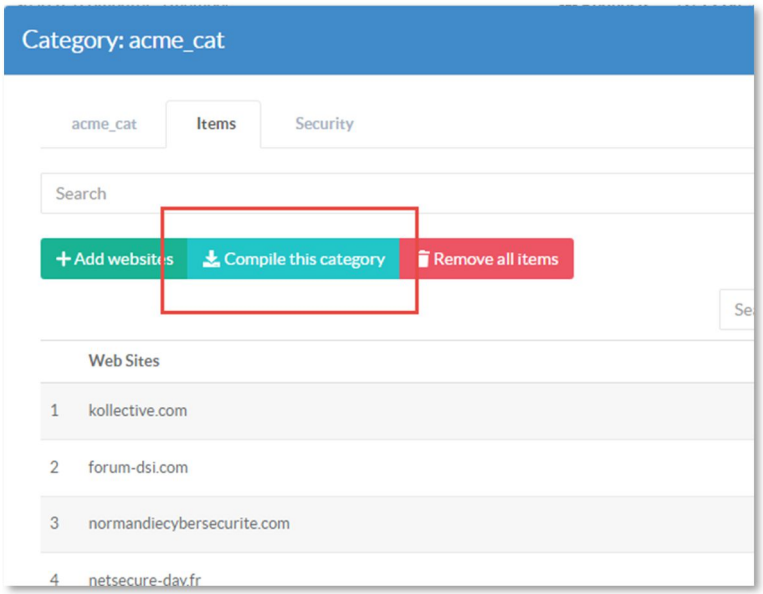


- Select the "**Items**" tab.
- Click on **Add websites**.
- You can add several websites by separate them with a carriage return.
- The **Force** option enforce saving an already categorized website inside the category
- **Disable extension checking** force to store a website without an extension (.com, .fr, .de, .it....)



Compiling your categories.

Add websites inside a category doesn't add them to the Web-Filtering service or the Categories services.
Websites are stored inside the local PostgreSQL database and must be saved on disk inside a preformatted file.
For compiling your categories, you have 3 ways:



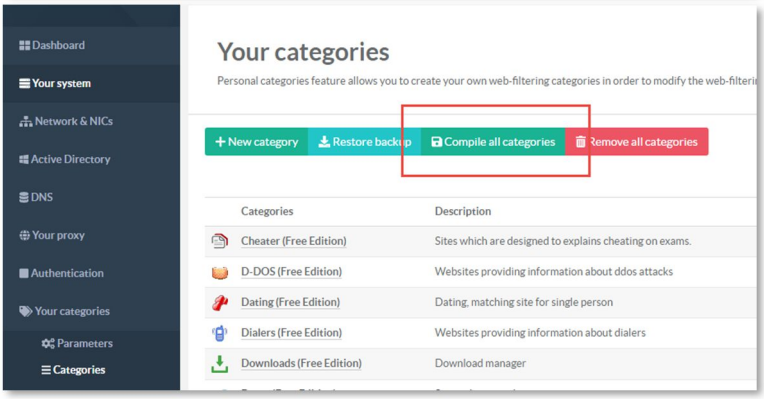
Compiling a defined category

On the category section, click on the button "**Compile this category**".
Artica will compile your category and reconfigure your category service and reload your Web-filtering service.

Compiling all categories

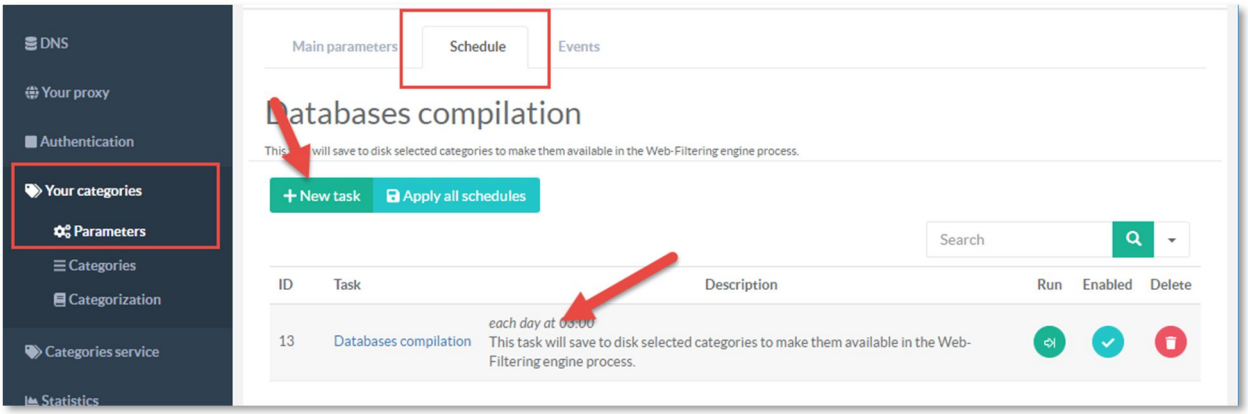
On the list of all available categories, click on the button "**Compile all categories.**"

This task compiles all categories even though there are not changes in your categories.



Compilation Schedules

"**Your Categories**" and **Parameters** click on **schedule** tab.
The scheduled compilation compiles only modified categories, in this case, you are able to create an hourly schedule.
Only modified categories will be compiled. If there is no changes, the task will do nothing.

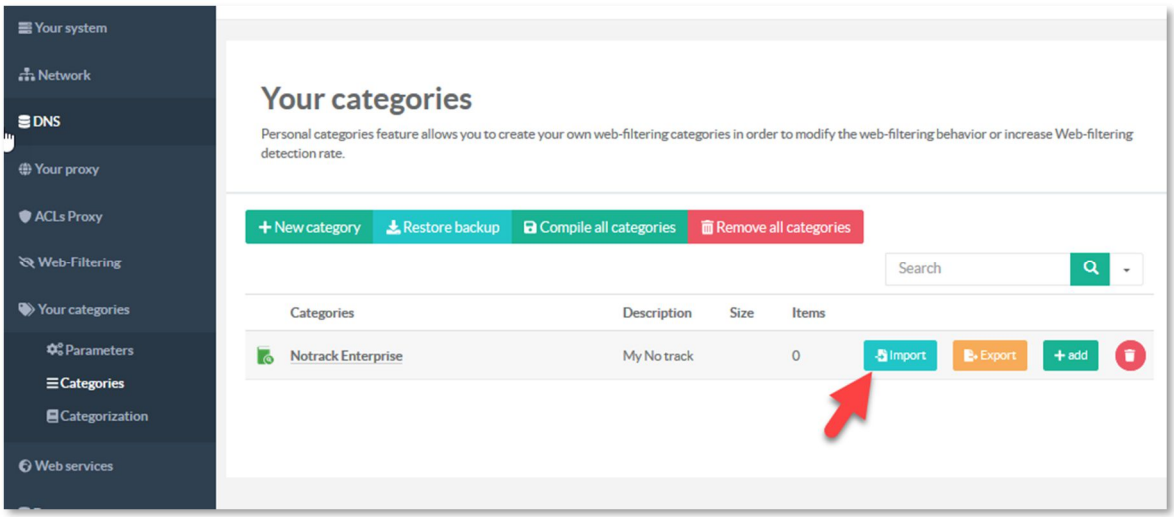


Import/export items.

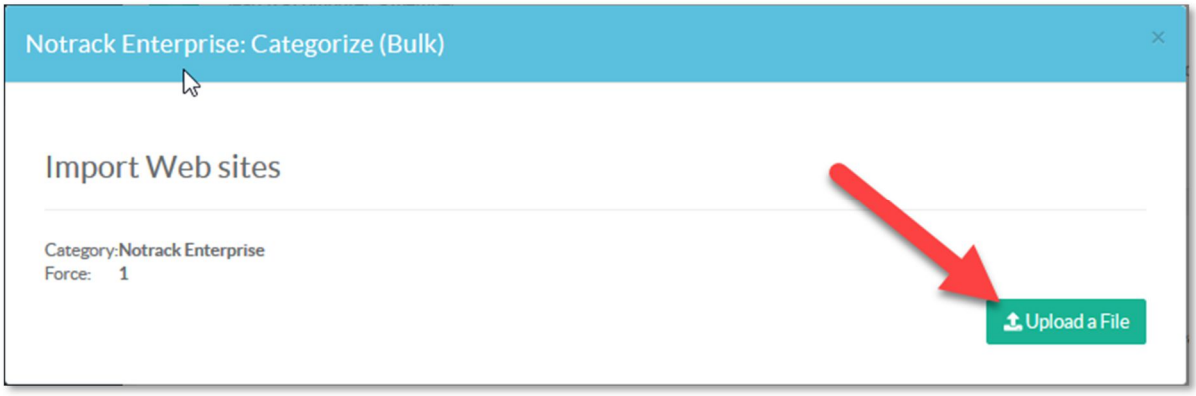
Import items

This feature allow you to import million of websites into a category container.

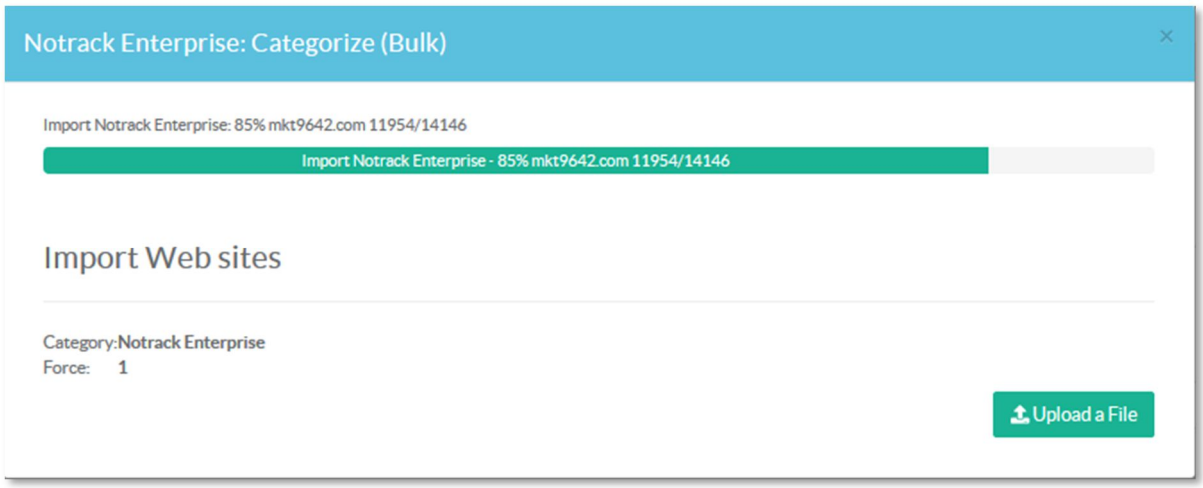
- Prepare a text file with websites separated by a carriage return (the **text** file (*.txt) can be also in **gzip** (*.gz) or zip (*.zip) file type)
- On your Categories section, click on the "**Import**" button



- Upload your file using the button "**Upload a file**"

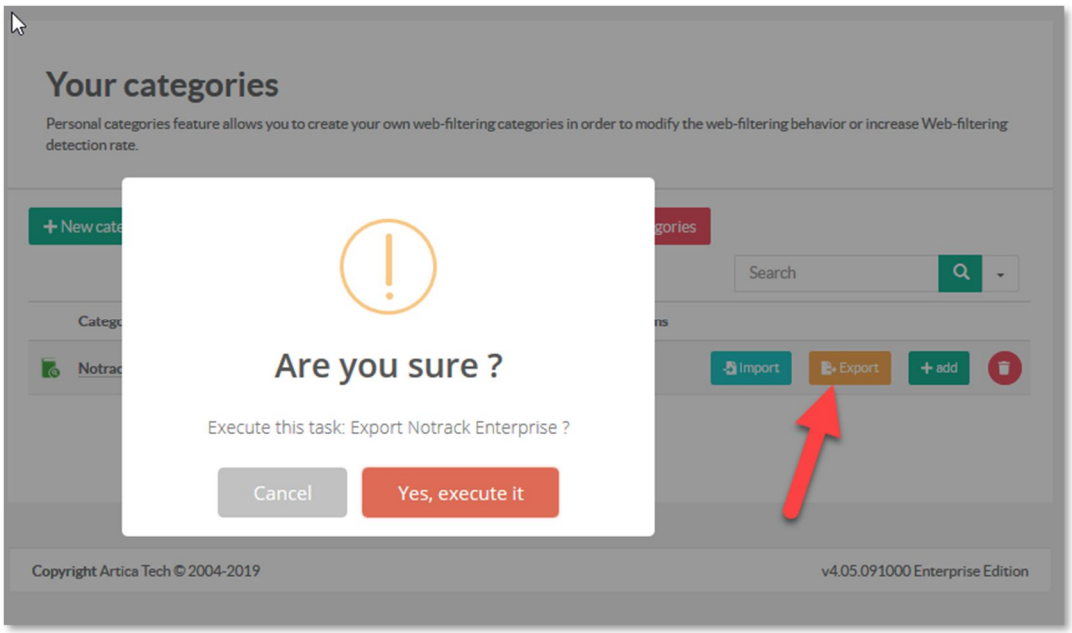


- Artica will display the importation progress.

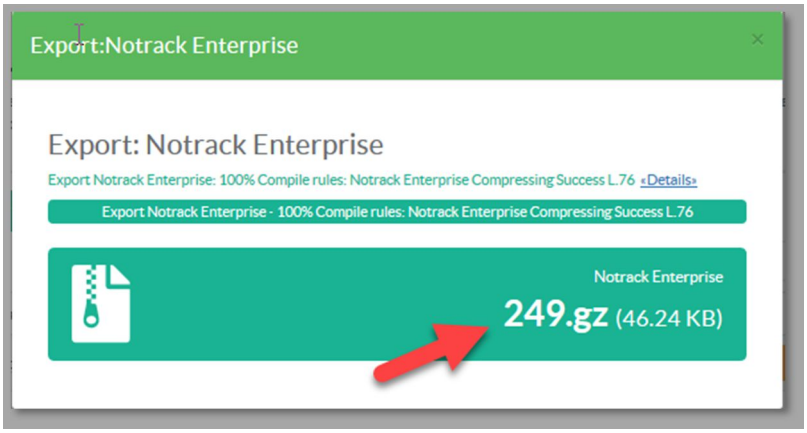


Export items

- On the table, click on the "**Export**" button.
- A confirmation message ask to you to confirm the export task



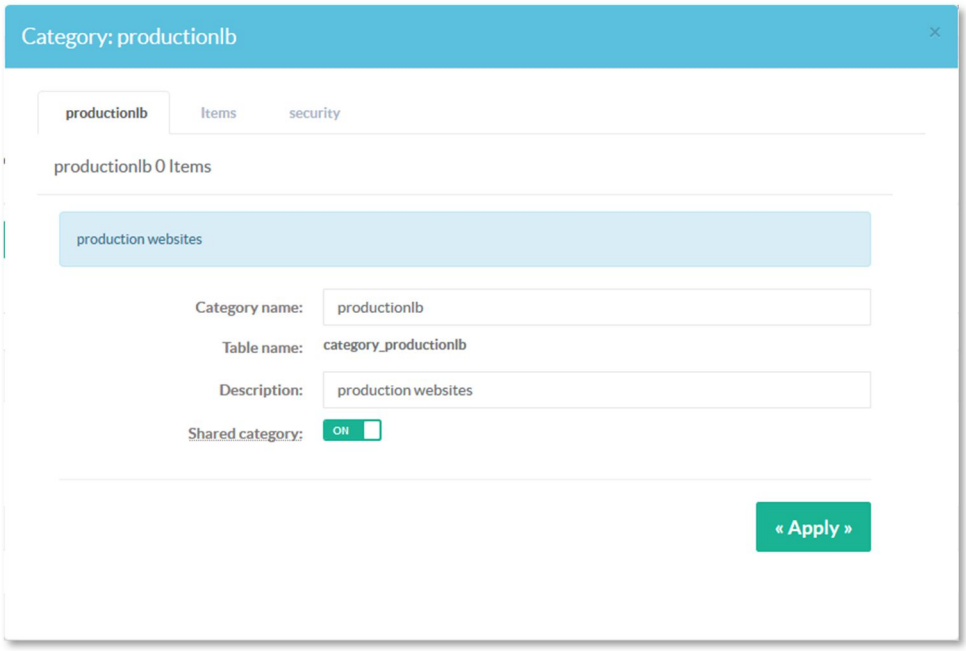
- Wait during the exportation task.
- After exportation complete, a new icon allow you to download the exported file.



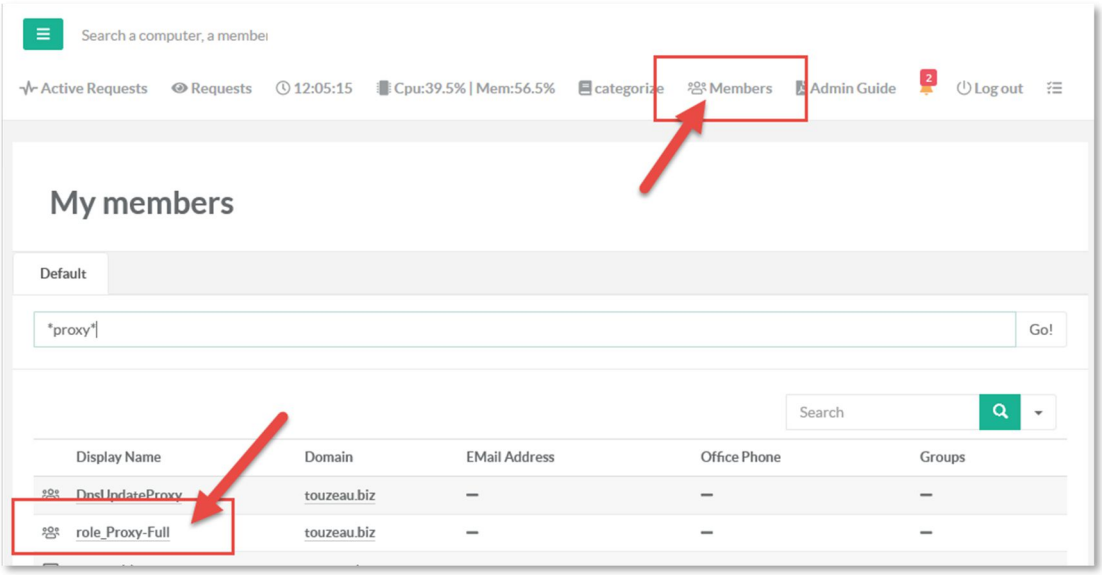
Shared categories

Shared categories allow you to delegate the category to specific groups according to the local Administrators database or Active Directory Database.

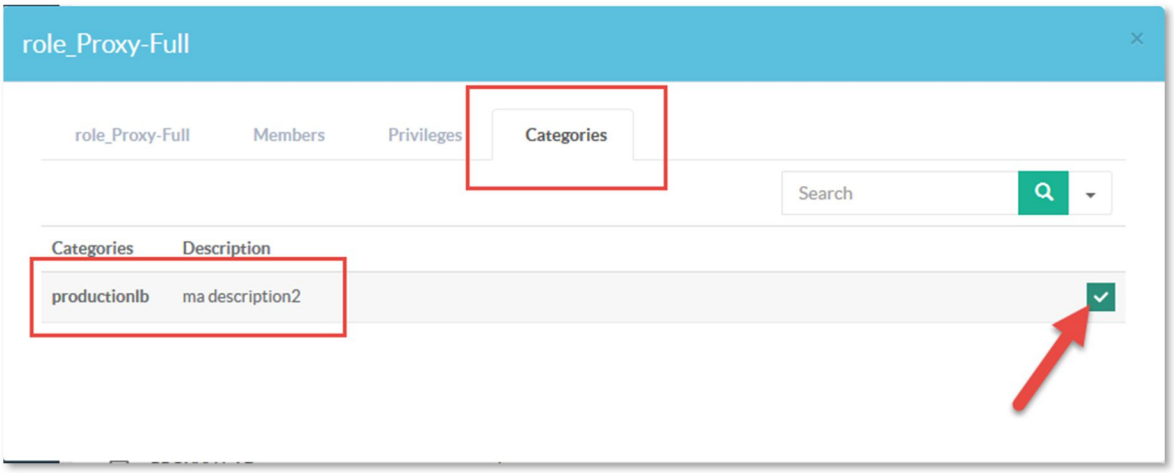
When editing a personal category, enable the "**Shared category**" option.



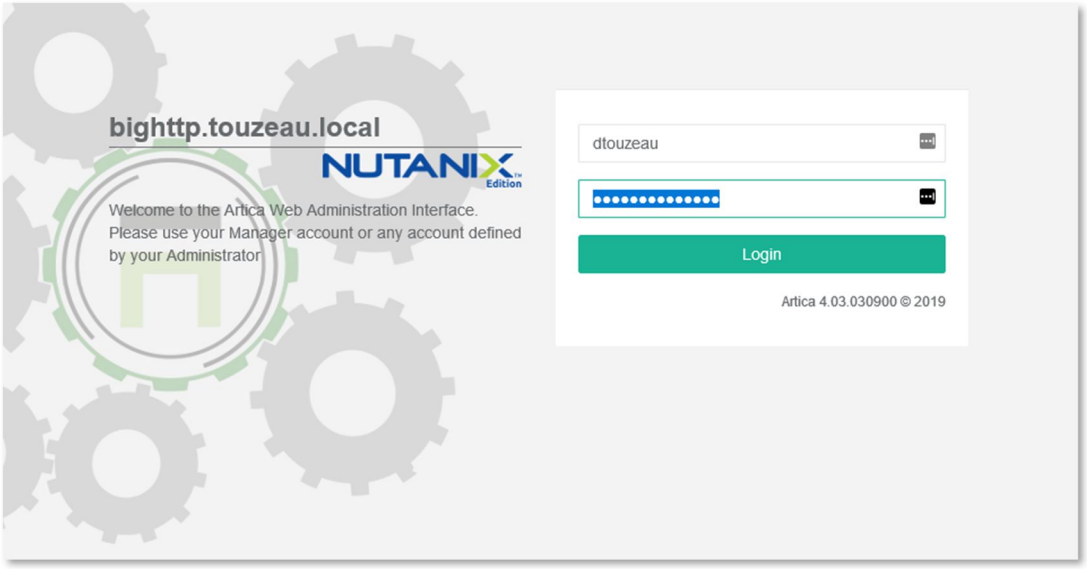
- Enable shared category allows you to add this category in the privilege section.
- Open the members section in order to browse groups
- Find the group of users you want to enable the category management.



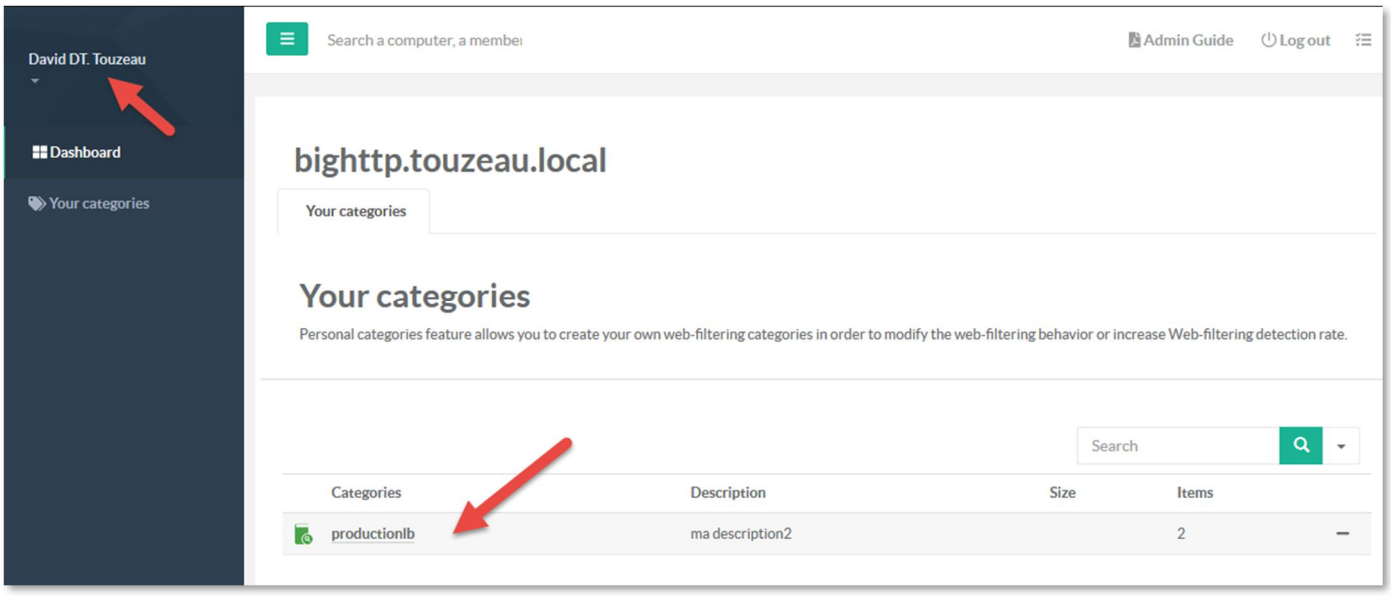
On the group option, click on "**Categories**" tab.
Click on the checkbox in order to let member of this group managing the category.



When an user of this group login on the Artica Web console.



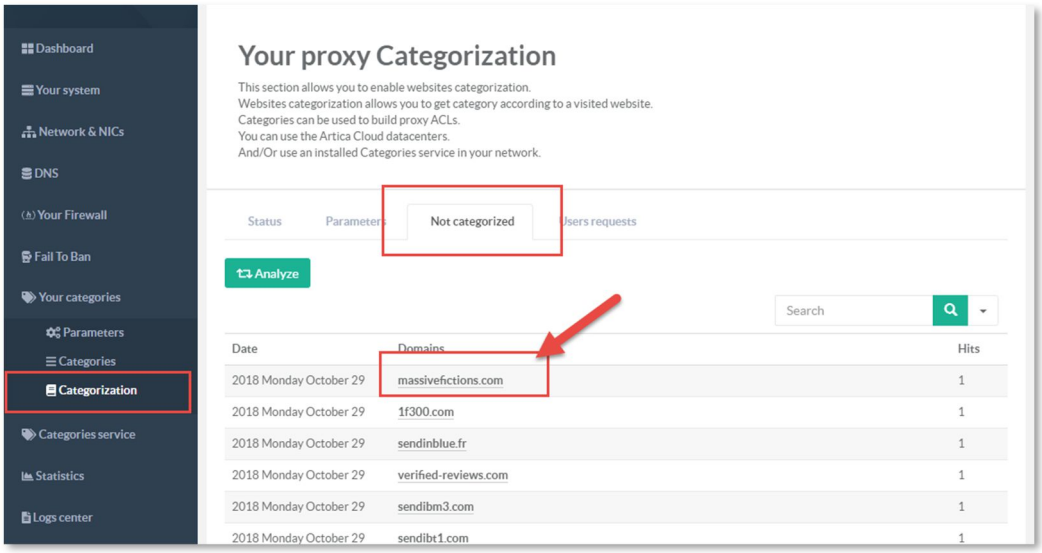
If the group have only the privilege to manage shared categories, the web interface displays only categories allowed to be edited.



Uncategorized websites

If your server act as Categories server for others Artica proxies, your server is able to store all websites that are uncategorized.
To define an uncategorized website, your category server requests the categories on Artica Cloud (if enabled), on the second categories server and on your categories service.

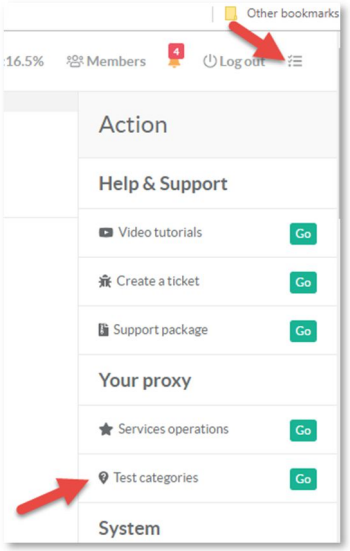
- On the left menu, click on "**Your categories**" and "**Categorization**".
- Select the "**Not categorized**" tab
- You will see the list of uncategorized websites and you are able to categorize it.



This section is available by RESTFul API (see above).

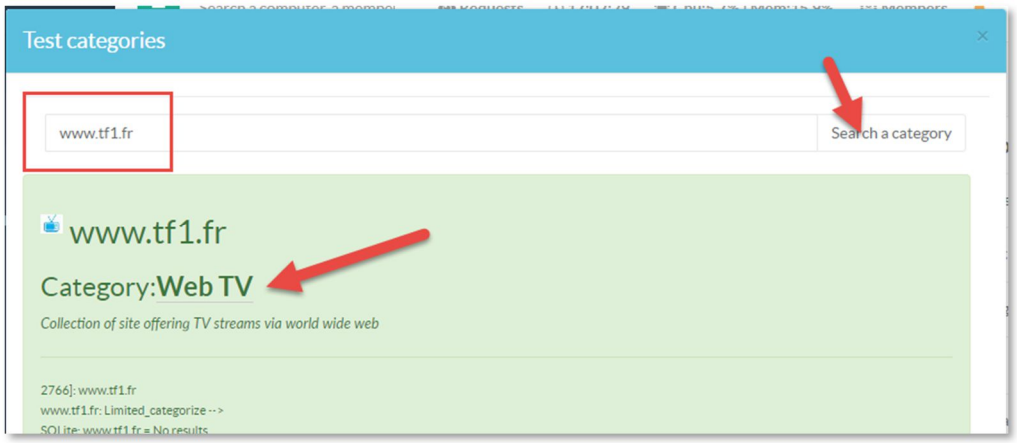
Testing categories

If you are using passive mode or active mode, you can query a category from a website.
Click on the button on the top-right webpage (near the "Log out")
On this right menu, choose "**Your Proxy**" and "**Test categories.**"



A new form is displayed

It allows you to ask which category is associated with the queried domain.



MONITORING AND STATISTICS

Realtime access logs format

The proxy write events in the /var/log/squid/access.log

A typical line is :

```
1569139273.003     33 192.168.1.191 TCP_MISS/200 883 GET
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1
DlgCEAsfjNWeZHRr6uFT7MohBms%3D Jhon HIER_DIRECT/93.184.220.29:80 application/ocsp-response
mac="00:0c:29:e3:a1:9c" category:%20136%0D%0Aclog:%20cinfo:136-SSL_certificates;%0D%0A ua="Microsoft-
CryptoAPI/6.1"
```

Information is formatted in this way:

- 1569139273.003 : Seconds since epoch with subsecond time (milliseconds)
- **33**: Response time (milliseconds)
- **192.168.1.191**: Client IP address
- **TCP_MISS/200**: Proxy request status / HTTP status code sent to the client
- **883**: Total size (bytes) of reply sent to client
- **GET**: Request method (GET/POST etc)
- **http://ocsp.digicert.com/....:** Request URL received (or computed) and sanitized
- **Jhon :** User name (any available)**;** if no user "**-**" is added
- **HIER_DIRECT/93.184.220.29:80:** Proxy Hierarchy and remote address used to fetch data
- **application/ocsp-response**: Content-Type of data sent by the next hope
- mac="00:0c:29:e3:a1:9c": Mac address of the client.

```
category:%20136%0D%0Aclog:%20cinfo:136-SSL_certificates;%0D%0A
```

Extra information sent by Artica plugins.
replace **%20** by space and **%0D%0A** by carriage return

```
category: 136
clog:
cinfo:136-SSL_certificates;
```

Means Website **Category ID = 136**, information retrieved in cinfo that give the category name
Clog is extra log when Artica plugins

```
ua="Microsoft-CryptoAPI/6.1"
```

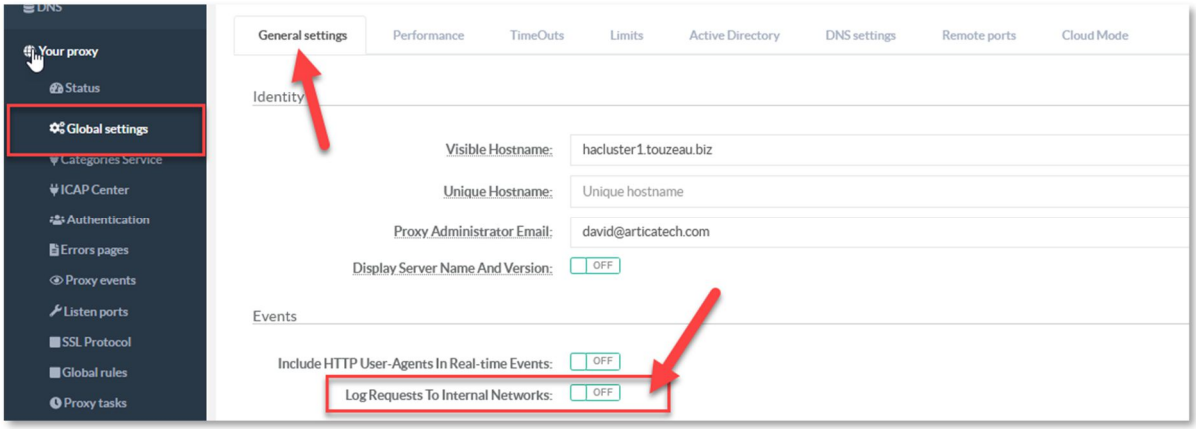
If the option Log User Agent is enabled , the User Agent string is written inside cotes

Logging to Internal networks are disabled

It make sense to not log requests to the internal network, in my cases internal web applications make many requests, use only IP addresses and are in a productive topic.
By default, proxy did not log requests to internal web servers inside private network
All requests to, 172.16.0.0/12, 192.168.0.0/16 are not logged by the proxy.

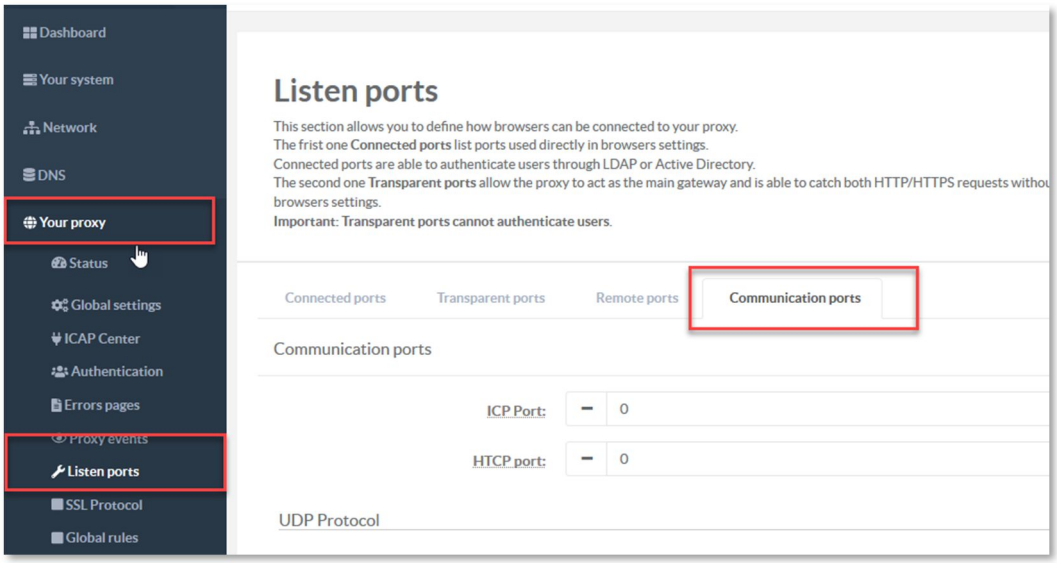
Enable logging to internal networks:

- Under Your Proxy, choose Global settings
- Click on General settings tab
- Under Events section, turn on Log requests to Internal networks.

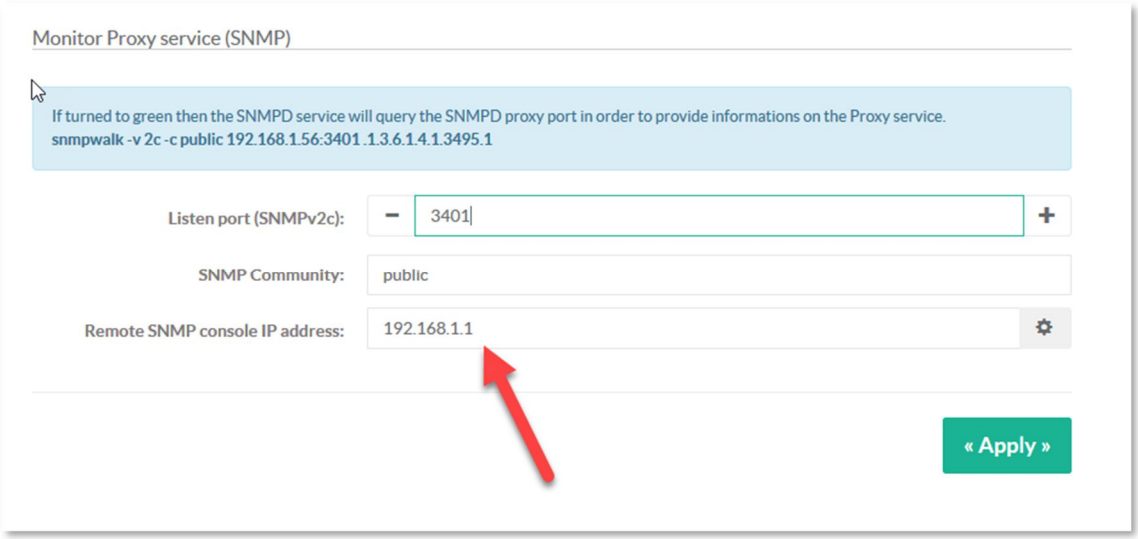


SNMP service dedicated for the proxy

You can connect your SNMP console by enabling some parameters.



- On the left menu, choose "**Your Proxy**" / "**Listen Ports**"
- Select Communication ports.
- Down to Monitor Proxy service (SNMP)
- Define the IP address of your remote server that is able to query the Artica Proxy.



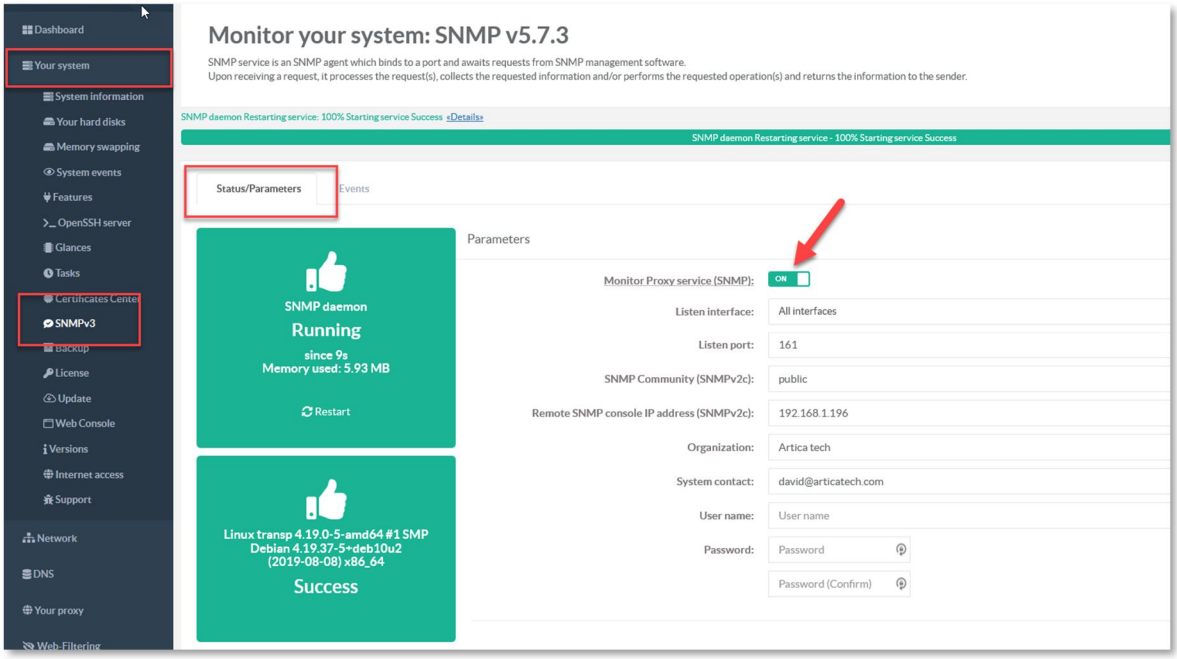
Check the SNMP availability by using this command line

```
snmpwalk -v 2c -c public 192.168.1.56:3401 .1.3.6.1.4.1.3495.1
```

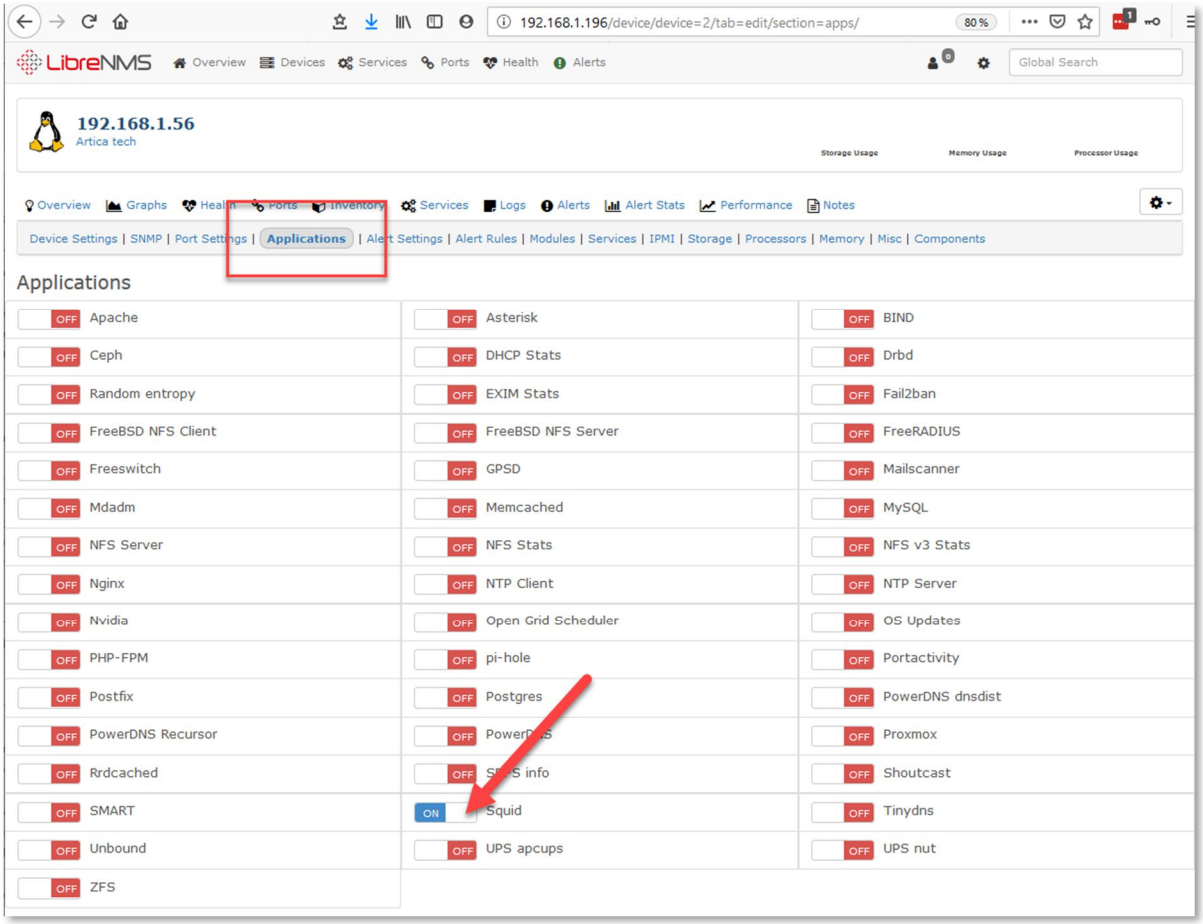
If the SNMP tool answer "No Response from", you should reboot the Artica server

Merge SNMP proxy inside the SNMP service.

If you **have installed the SNMP service in artica features**, the SNMP service can merge data from the proxy SNMP in order to use only one port.
On **Your System / SNMPv3**, enable the check box "**Monitor Proxy service (SNMP)** option.



- If you use LibreNMS, go to your device, choose "**Applications**" and turn ON the **Squid** checkbox option.



Artica Proxy statistics

Artica allows you to display many statistics in order to see when,where,how your users use the bandwitch and the Webs.

Centralized Statistics

You can dedicate a central server that able to receive events from several Artica servers.
Logs will be merged and centralized to an unique Web Interface.

PDF Reports

You can schedule PDF reports that can be sent by eMail to a list of recipients:

- Daily report
- Yesterday report
- Current week report
- Last week report
- Monthly report
- Last month report

Dedicated statistics privileges

You can create specific privileges from Artica local database, LDAP or Active Directory that allows some users to access to proxy statistics.

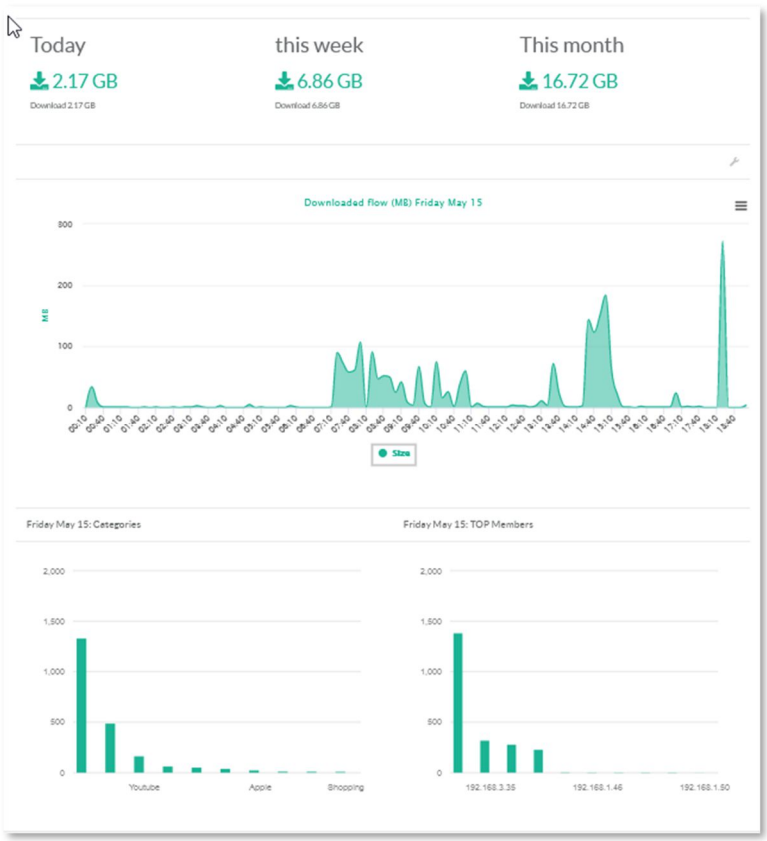
Statistics by categories

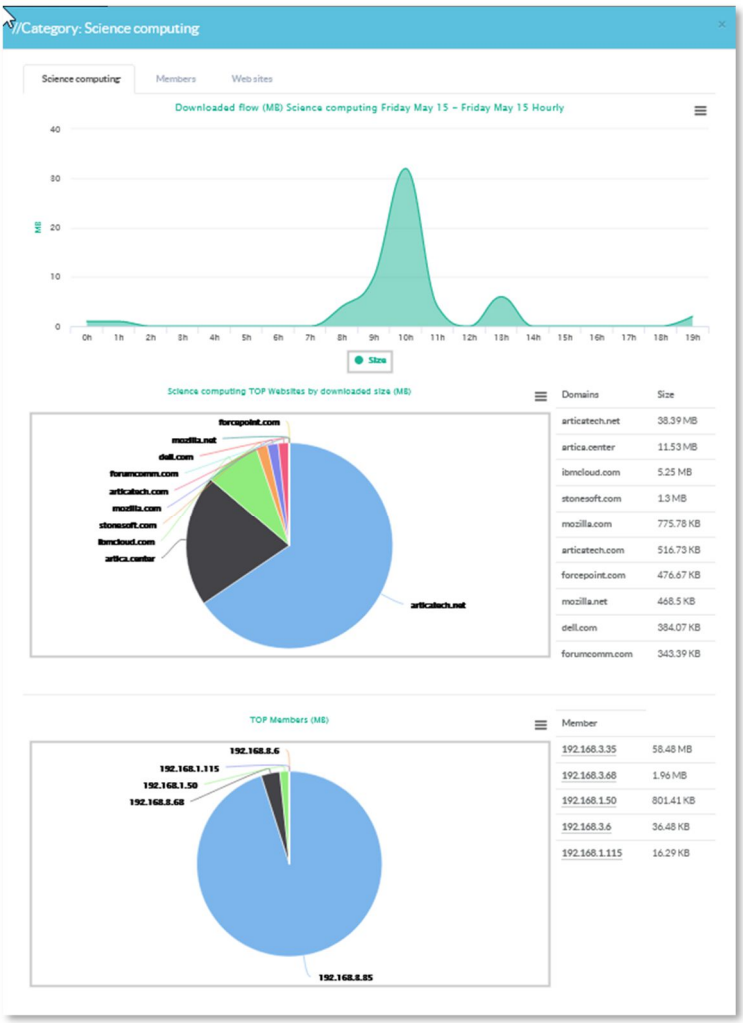
With Artica categorization method statistics can be extracted by topic like Press, pets, society, press, cars, animals...

What, Where, When, who ?

With the query on statistics you will be able to extract graphs, charts, tables of who is using what and when it using some...

The Statistics feature is available with an Artica Enterprise Edition License





Statistics Feature Documentation

Download the documentation here:

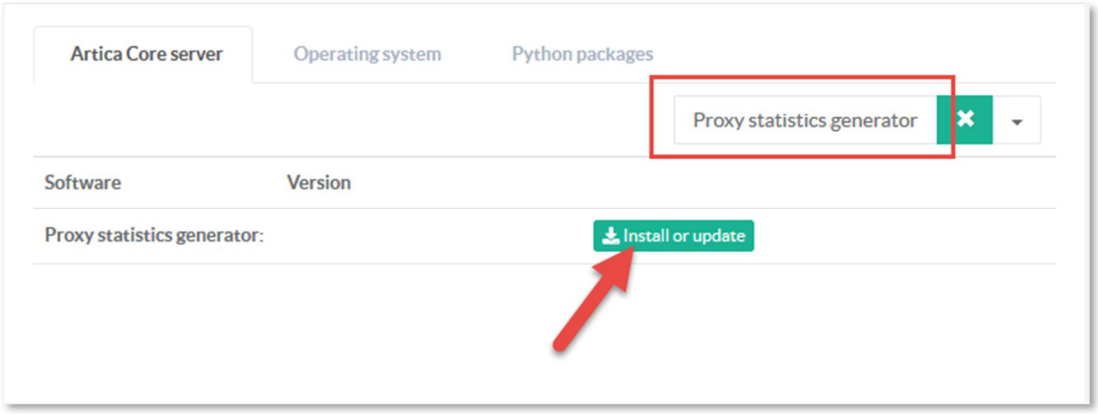
Scheduled reports with **Proxy Statistics Generator**

This feature is designed to parse native access log format of the proxy service and generate general statistics about hits, bytes, users, networks, top url,top second level domain and denied URLs.
Statistic reports are oriented to user and bandwidth control, [b]this is not a pure cache statistics generator.

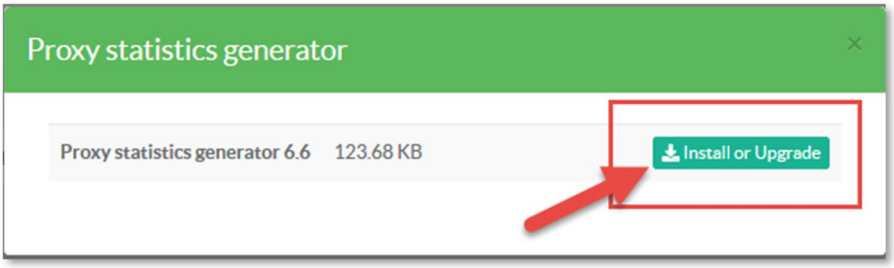
It use flat files to store data.
This feature is limited according it can took several hours to parse a log file more than 1GB of data..

Install the Proxy Statistics Generator

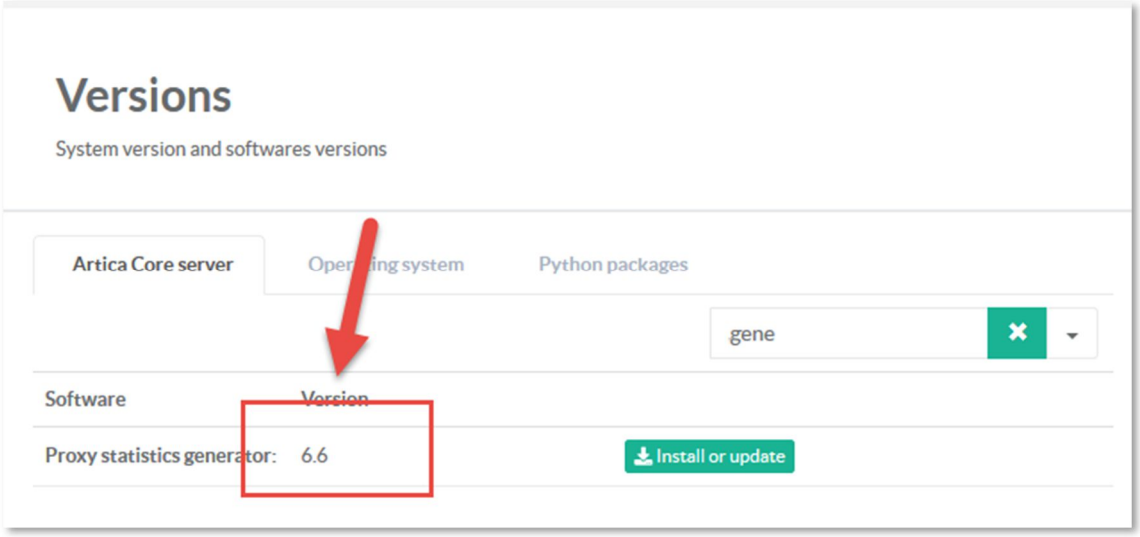
- On the left menu, go to "**Your System/Version**"
- On the search field, type "**Proxy Statistics generator**"
- If you did not see a version, this means the software doesn't exists on the system.
- Click on **Install or upgrade** button.



- Choose the latest version and click on **Install or Upgrade** button.

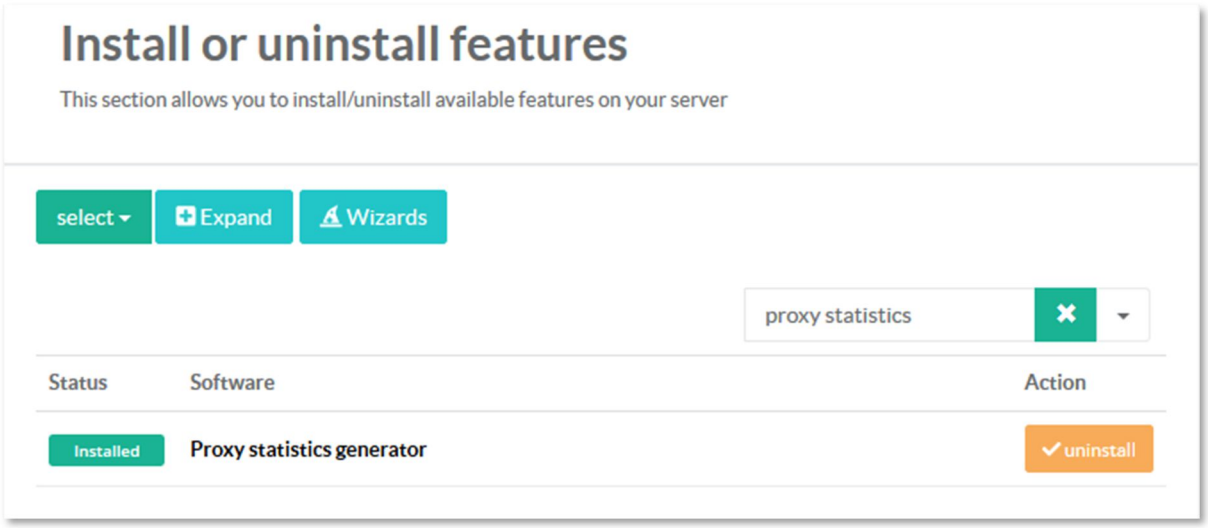


- You should see the version in the Proxy statistics generator row.



Enable the Proxy Statistics Generator feature.

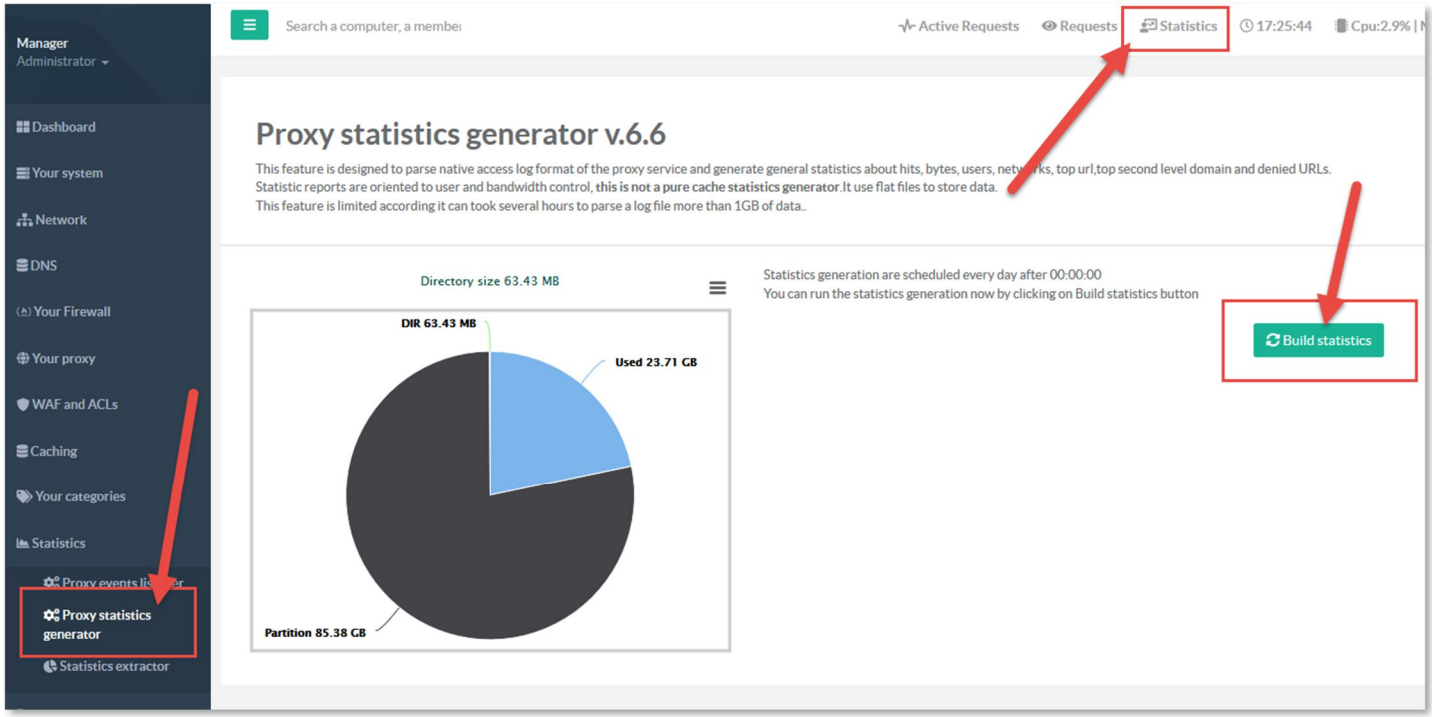
- Once installed, go into "**Your System**" and "**Features**" left menu section.
- On the search file, type **"proxy statistics**"
- Clic on Install button on the "**Proxy statistics generator**" row.



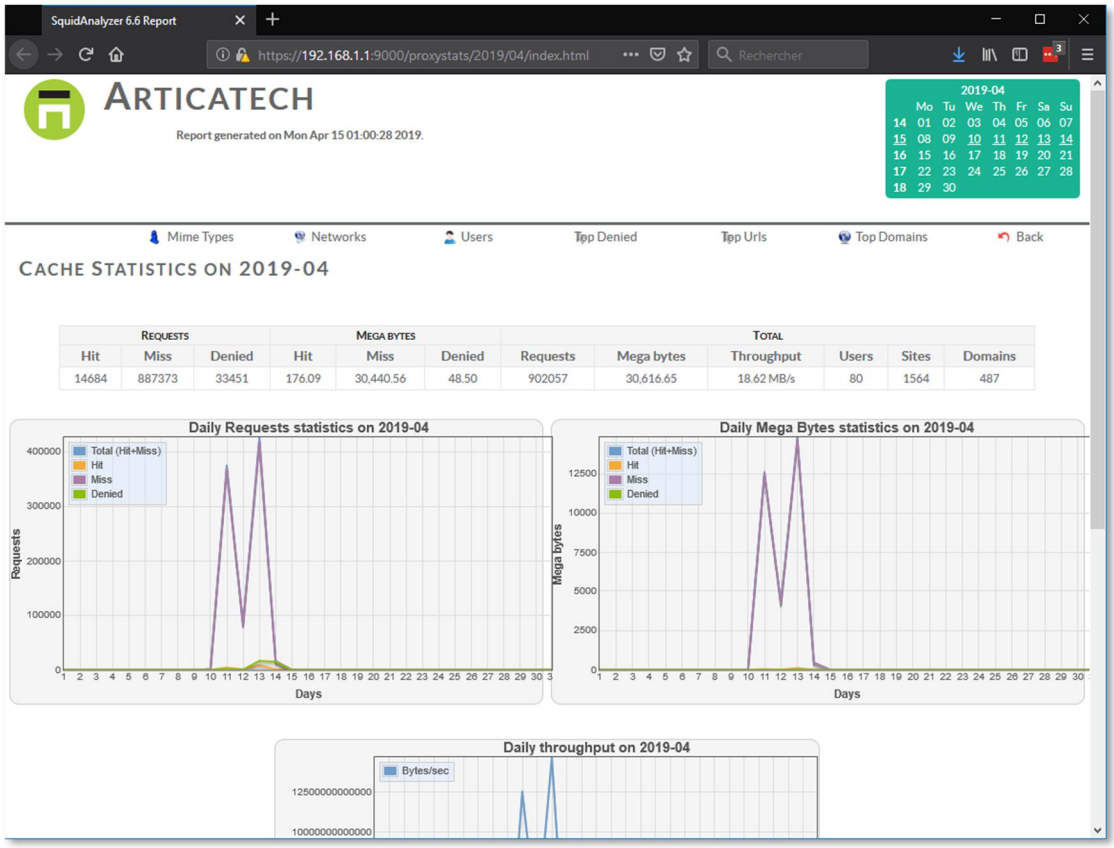
- On the left menu click on "**Statistics**" and "Proxy statistics generator"
- Wait few minutes and click on "**Build statistics**" to have your first report available.
- On the top menu click on "**Statistics**" in order to display reports.

Proxy statistics are automaticaly generated each day after 00:00:00

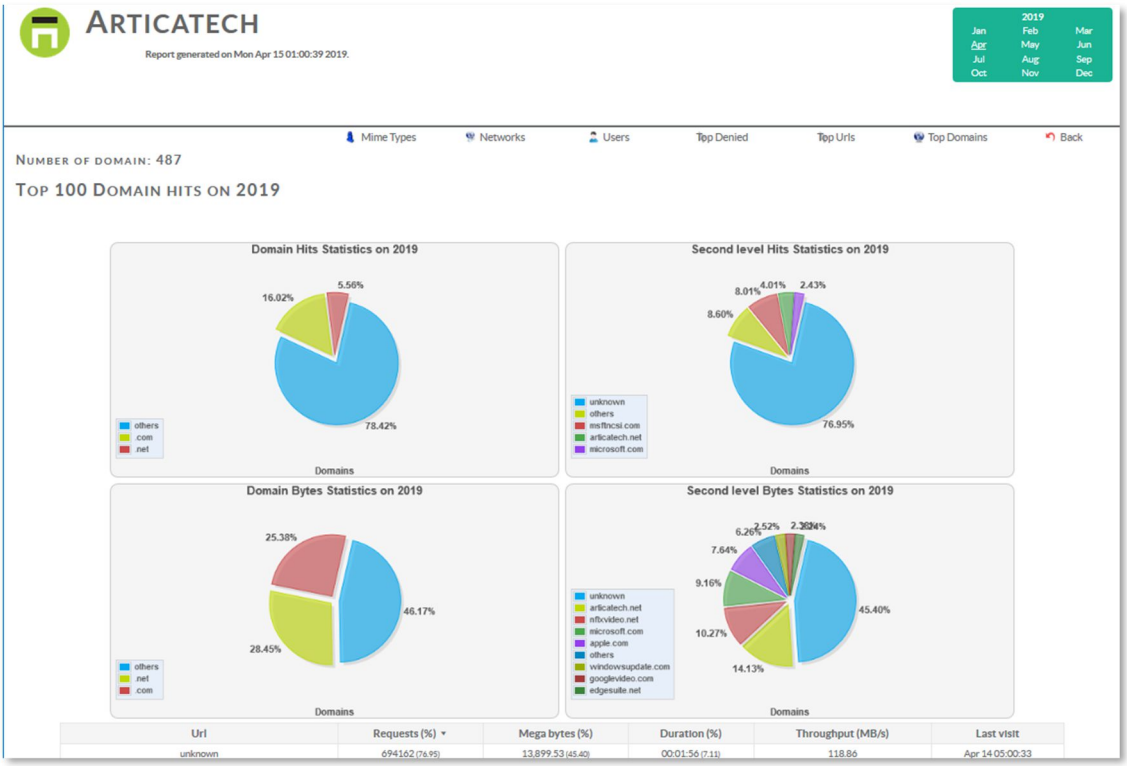
The main section display the disk usage of report..



Generated reports allows you to display bandwidth usage per domain, users, number of hits and downloaded size.
A calendar allows you to display specific reports per week or day.



Requests			Mega bytes			Total					
Hit	Miss	Denied	Hit	Miss	Denied	Requests	Mega bytes	Throughput	Users	Sites	Domains
14684	887373	33451	176.09	30,440.56	48.50	902057	30,616.65	18.62 MB/s	80	1564	487

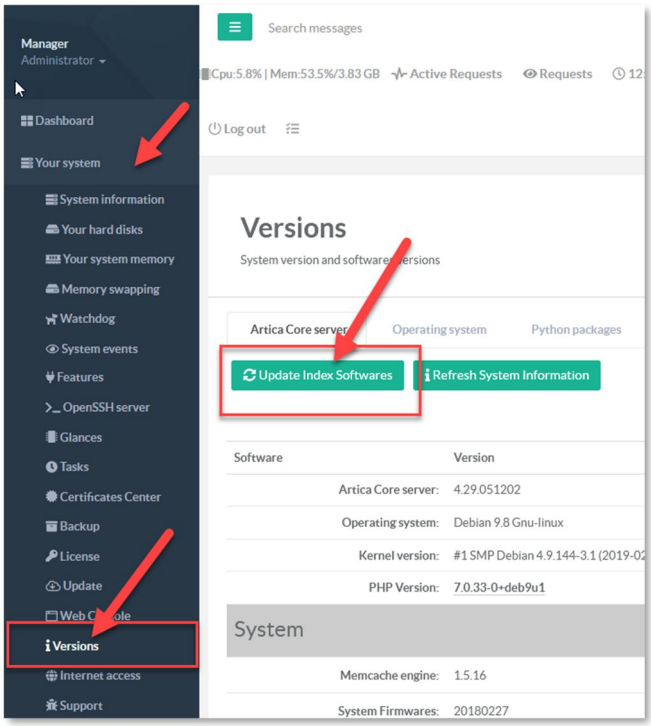


MAINTENANCE

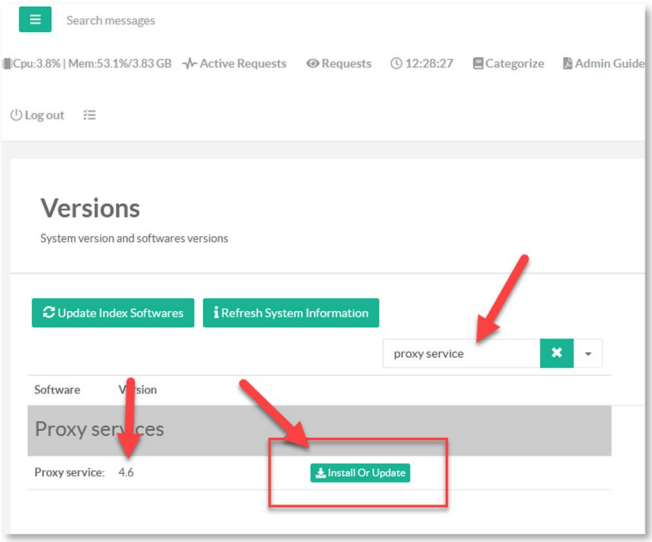
Update the proxy software

Proxy software is not automatically updated, periodically, we suggest to perform this operation in order to upgrade the proxy software .

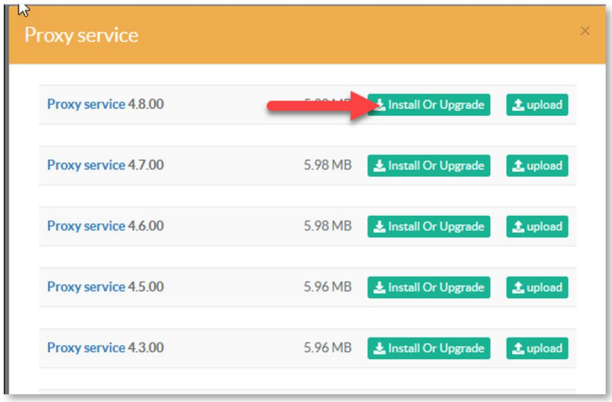
On "**Your System**", select "**Versions**"
Click on the button "**Update Index Softwares**" in order to get latest available versions.



- On the search field, type "**Proxy service**"
- The table displays the current version of your proxy software.
- Click on "**Install or Upgrade**" button on the right column.

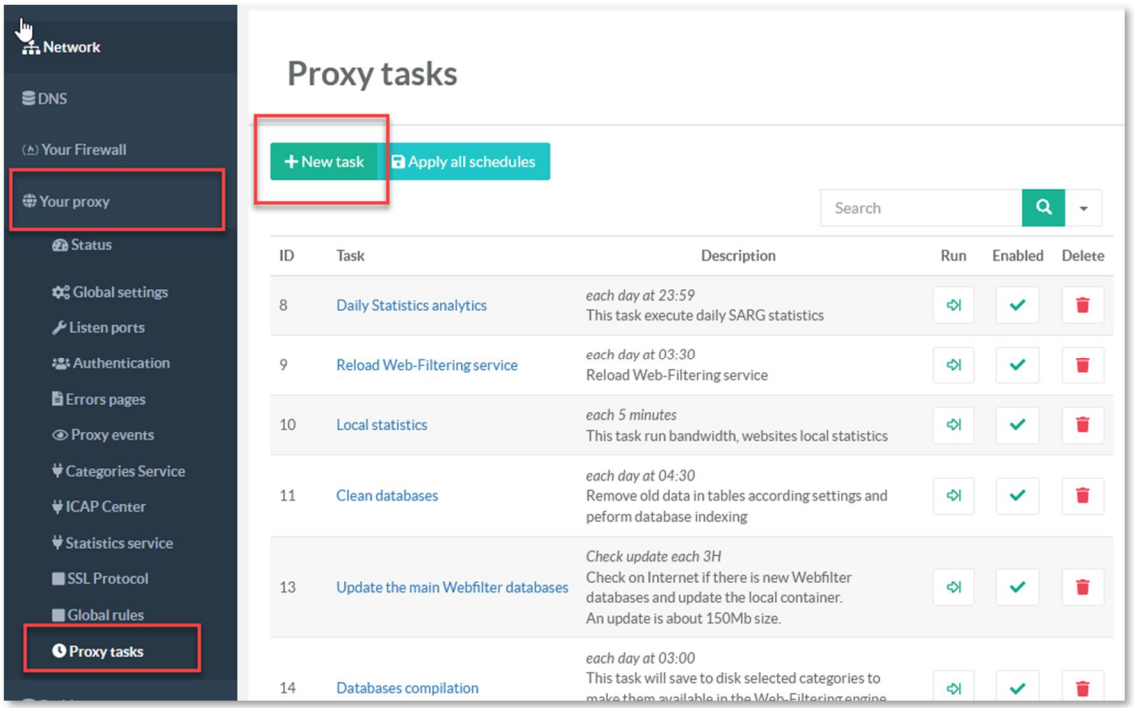


Select the most updated software and click on **"Install or Upgrade"** to let Artica downloading the package and install it.

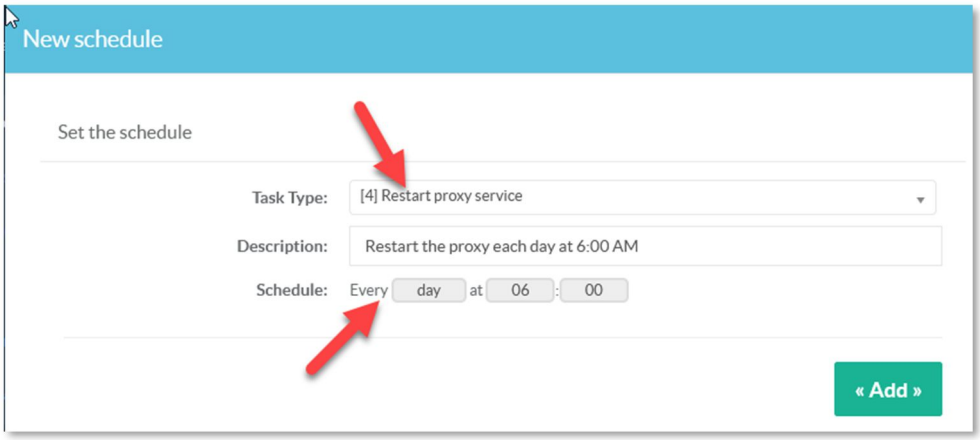


Restart the proxy periodically

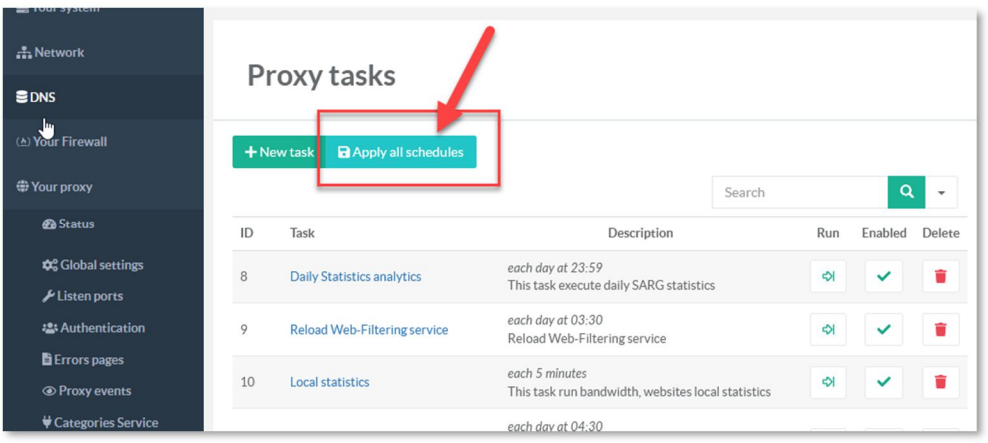
If you need to restart the proxy periodically in order to refresh it's memory, threads; on the left menu, choose "**Your Proxy**" and "**Proxy tasks**"
Click on the button "**New task**"



On the new schedule form, choose the task **[4] Restart Proxy service**.
Set the description and define the schedule (in our example, we restart the proxy each day at 06:00 AM)
Click on **Add** button.



- Click on the **Apply all schedules** button on the main table to make your schedules in production mode.

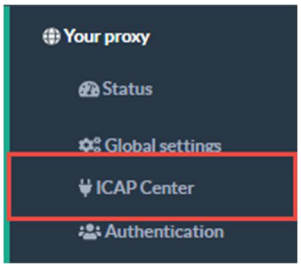


ICAP CENTER

The ICAP center allows you to plug ICAP remote services to your Artica Proxy.
The Internet Content Adaptation Protocol (ICAP) is a lightweight HTTP-like protocol specified in RFC 3507 which is used to extend transparent proxy servers, thereby freeing up resources and standardizing the way in which new features are implemented.

ICAP is generally used to implement virus scanning and content filters in transparent HTTP proxy caches.
Content adaptation refers to performing the particular value-added service (content manipulation) for the associated client request/response.

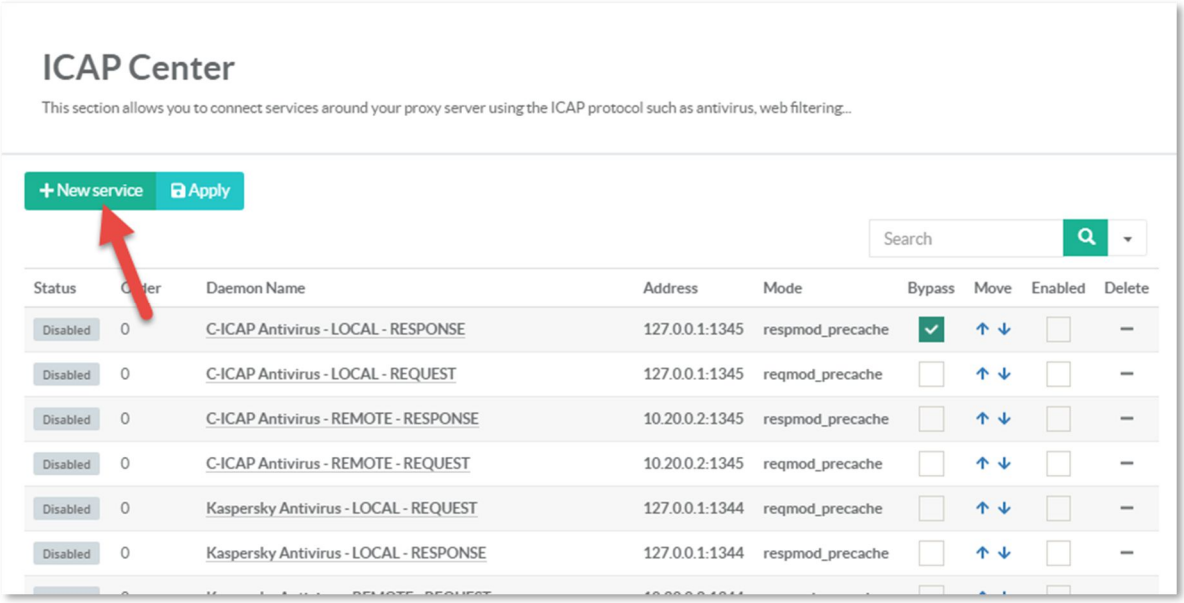
ICAP concentrates on leveraging edge-based devices (caching proxies) to help deliver value-added services.
At the core of this process is a cache that will proxy all client transactions and will process them through web servers.



These ICAP servers are focused on a specific function, for example, ad insertion, virus scanning, content translation, language translation, or content filtering.

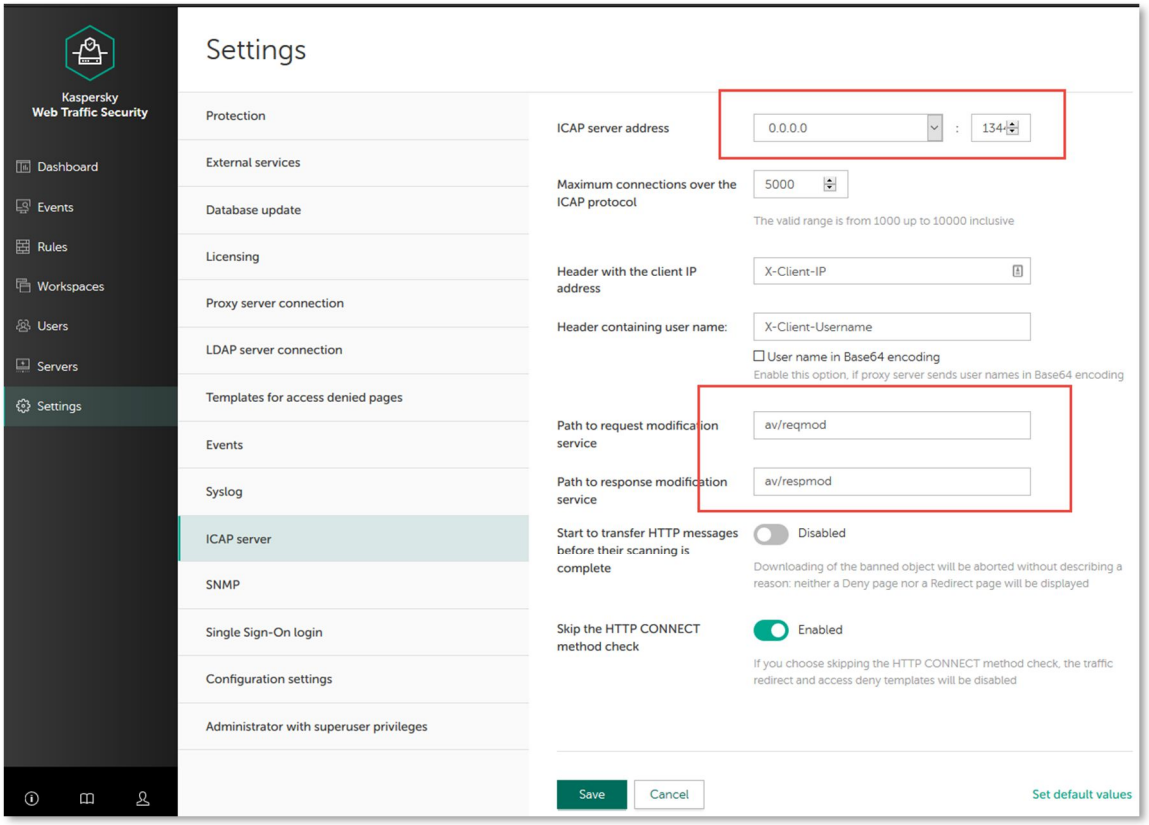
Off-loading value-added services from web servers to ICAP servers allows those same web servers to be scaled according to raw HTTP throughput versus having to handle these extra tasks.

- ✓ On the left menu, choose "**Your Proxy**" and "**ICAP Center**"
- ✓ A table is displayed and show you a list of pre-defined ICAP services examples.
- ✓ The "**Bypass**" column allows the proxy to continue processing requests if the ICAP service is down or failed.
  If enabled, then the proxy can bypass the ICAP service.
  If disabled, then the proxy sends an error page and stop processing requests.

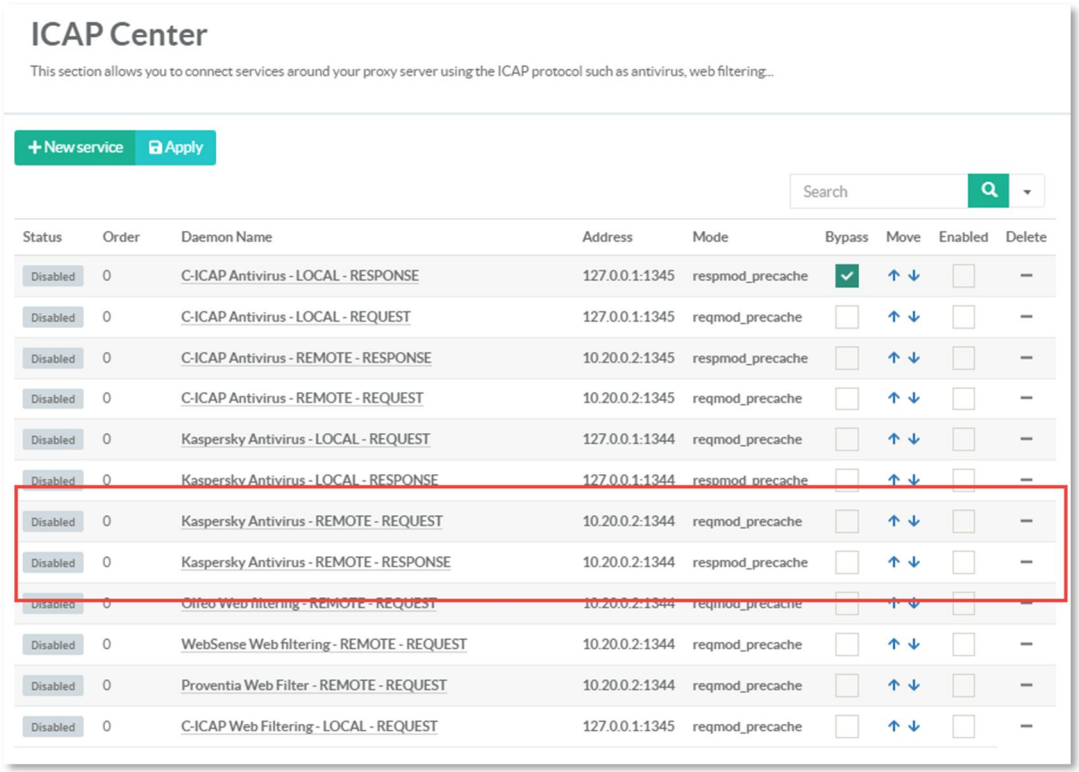


Example: Connect to the Kaspersky Web traffic Security ICAP server

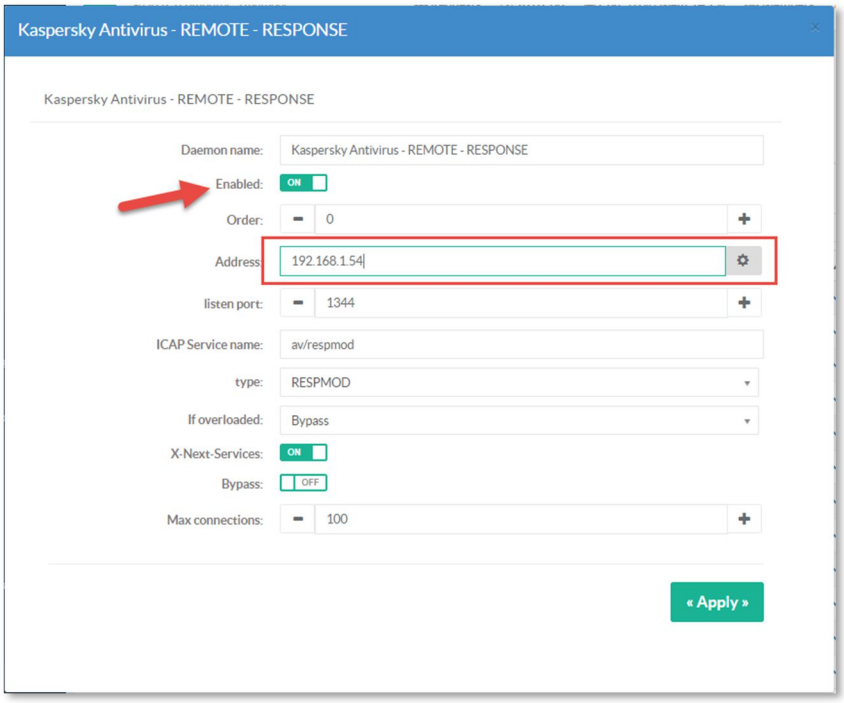
- ✓ On the Kaspersky Web traffic Security console, open the "Settings/ICAP server" menu.
- ✓ Ensure the ICAP server Address listen the 0.0.0.0 (means all IP addresses of the server)
- ✓ Take a look at the listen port (1344 by default), the path to request modification and the path to response modification service



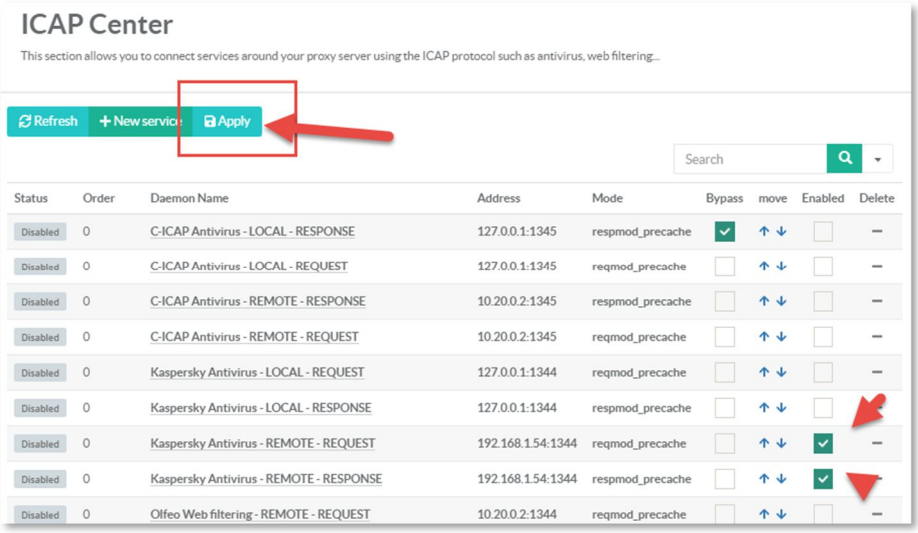
On Artica, search the Kaspersky Antivirus – REMOTE REQUEST and Kaspersky Antivirus – REMOTE RESPONSE
Click on each service.



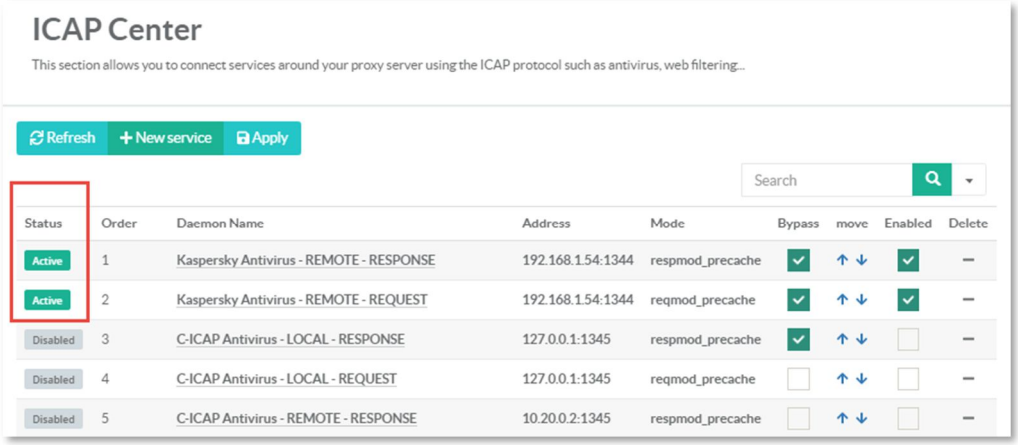
Turn ON the **Enabled** option and modify the **Address** to the IP address used by your Kaspersky Web traffic Security server.
Click on **Apply**



After modify the 2 entries, click on Apply button on the main table to link your proxy to enabled ICAP services.



After a few seconds, status must be turned to “Active”



ICAP ANTIMALWARE/ANTI-PHISHING SERVICE

Kaspersky For Proxy server

Kaspersky Anti-Virus 5.5 for Proxy Server provides anti-virus protection for network traffic routed through proxy servers which support the Internet Content Adaptation Protocol (ICAP).

The program allows:

- **Perform anti-virus scans on objects transferred through the proxy server**.
  Kaspersky Anti-Virus does not scan the data transferred via HTTPS.
- **Cure infected objects**, or block access to infected objects if disinfection fails.
- **Use group settings to define filtration parameters** that are applied depending on the address of the user requesting an object, and the object's address (URL).
- **Log activity** statistics, including information about anti-virus scanning and its results, and application errors and warnings.
- **Notify administrators** about detection of malicious software.
- **Update the anti-virus databases**.
  By default the application uses Kaspersky Lab's update servers as the source of updates.
  But it can be configured to update the databases from a local directory; The anti-virus databases are used in the detection and disinfection of infected objects.
  The application uses database records to analyze every object, checking it for virus presence: its content is compared with code typical for specific viruses.
  Please be aware that new viruses appear every day, and therefore you are advised to maintain the anti-virus databases in an up-to-date state.

New updates are available hourly on Kaspersky Lab's update servers.

THE PROXY PAC SERVICE

A **P**roxy **A**uto-**C**onfig (PAC) file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.

A PAC file contains a JavaScript function "FindProxyForURL(url, host)".
This function returns a string with one or more access method specifications.
These specifications cause the user agent to use a particular proxy server or to connect directly.

Multiple specifications provide a fall-back when a proxy fails to respond.
The browser fetches this PAC file before requesting other URLs.
The URL of the PAC file is either configured manually or determined automatically by the **Web Proxy Autodiscovery Protocol** .

Artica is able to provide and generates on-the-fly a proxy.pac file for your Network.

It extends the native proxy.pac feature by providing multiple configuration scripts based on the source IP address, the proxy itself and the User- Agent string

Download the documentation here:

http://articatech.net/download/PROXY-PAC.pdf

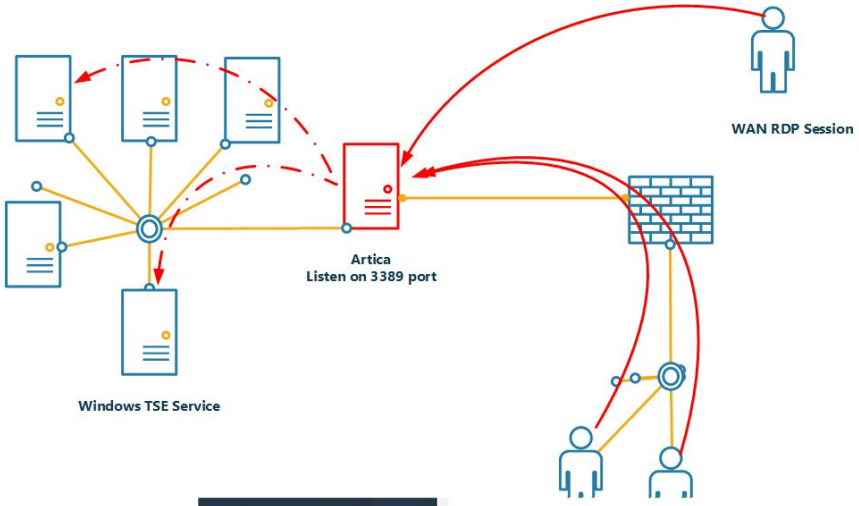
THE REMOTE DESKTOP SERVICE PROXY (RDP)

The RDS Proxy is designed to secure and forward remote desktop connections using RDP protocol or VNC protocol.
It should be called RDS gateway or RDP proxy

It can be used to let Internet users to connect using TSE client to a datacenter from Internet or let administrators from the LAN to be connected to a pool of RDP services.

This service offer several features :

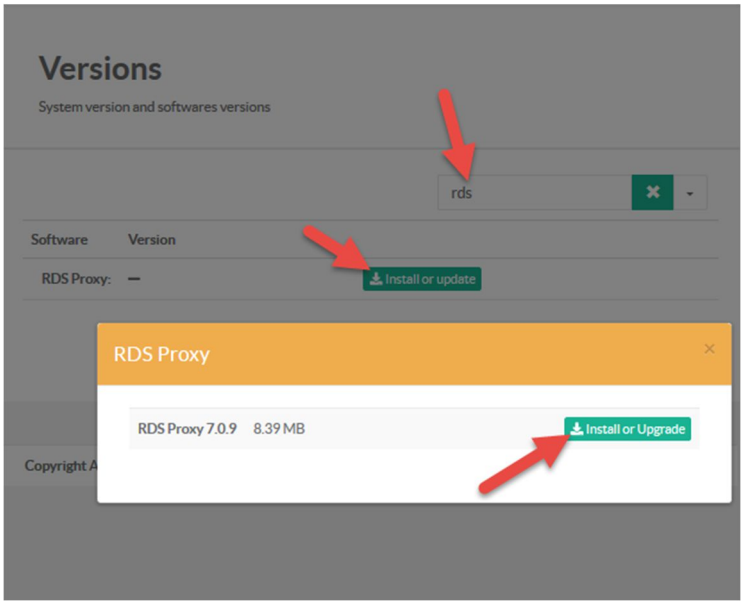
- Centralize and log each connection
- Automatically ban addresses against dictionnary attacks.
- Define schedules to access to a pool of server.
- Hide real TSE services credentials and addresses

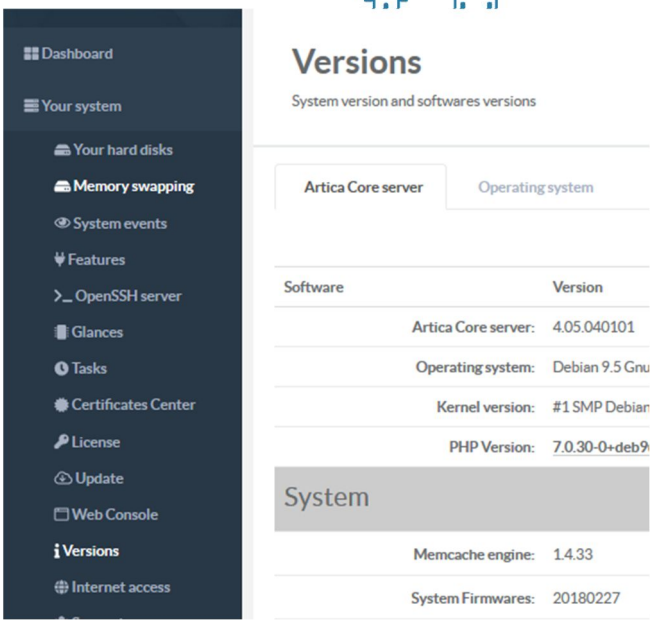


UPDATE THE RDS PROXY SERVICE FROM INTERNET.

If the RDS Proxy is not installed or you want to update it, on the left menu go to "**Your system**" and "**Version**"

On the Search field, type "RDS"
Click on Install or update button.
Choose the latest version and click on "Install or Upgrade"

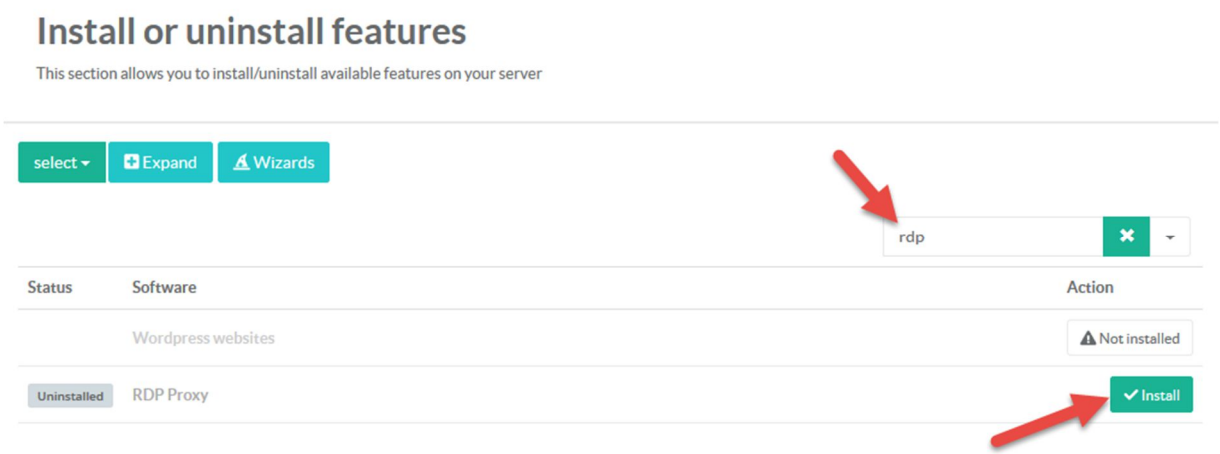




INSTALL THE RDS PROXY SERVICE.

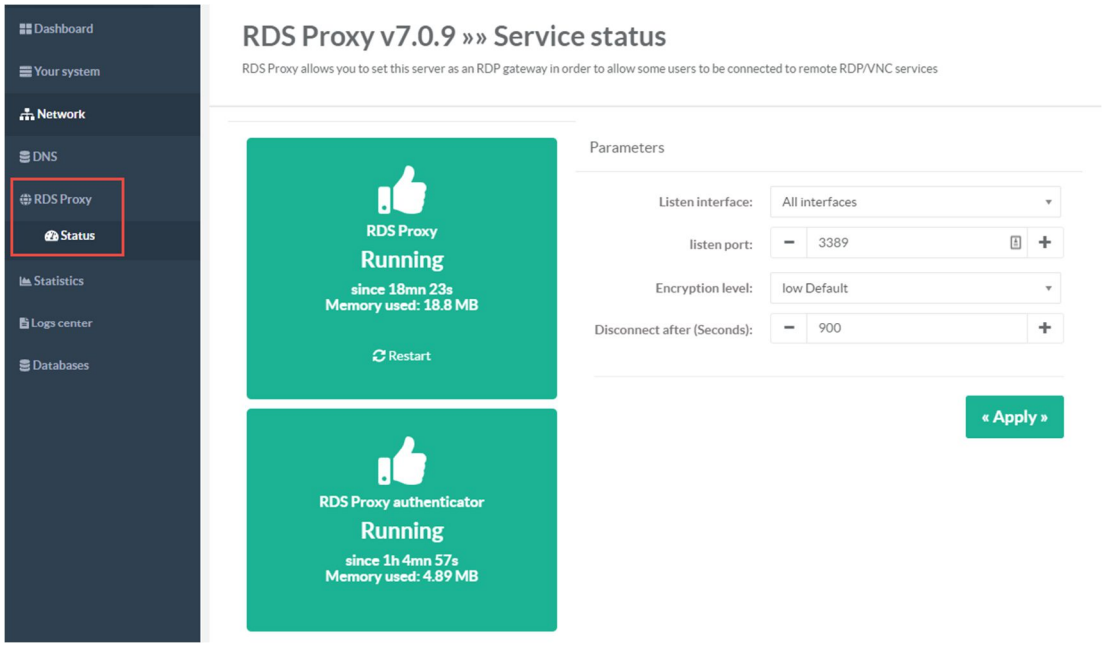
The RDP proxy service can be installed from the features section.

- On the search field, type "**rds**".
- Click on "Install" button on the "**RDS Proxy**" row



SETUP THE MAIN SERVICE

On the left menu, choose RDS Proxy/Status



The left section displays the status of the main proxy and the Authenticator service that will able to manage RDP sessions.

On the right side you can tune parameters of the main service:

- **Listen Interface**: which Interface to listen the RDP protocol.
- **Listen Port**: which port to use (default is 3389)
- **Encryption Level**: the level of encryption between the client and the proxy.
- **Disconnect after**: if there is no activity on the TS Session, then the proxy will automatically disconnect the session.

SETUP POLICIES

To setup connections you need to create groups.
A Group associates:

1) Users: members with internal proxy credentials to allowed to be connected to the proxy service.
2) Target services that are a list of authorized remote services
3) Addresses: Remote IP addresses authorized to be connected in order to be allowed to establish sessions to targets services.

To let you understand how to create a policy, let us use a real case:

David and **jhon** are allowed to be connected to 2 TSE servers :

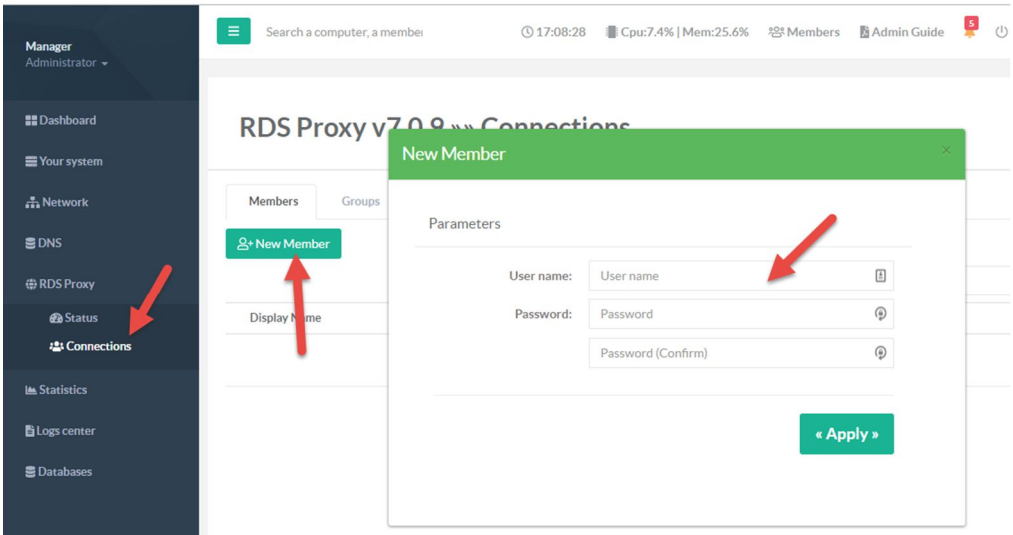
1) **dc16.touzeau.biz (192.168.1.90)** a Windows 2016 server using an hidden credential "**administrator**" and **90IPZJDO9Z** password
2) **(192.168.1.46)** a Windows 2008 r2 server using an hidden credential "**administrator**" and **871IPZJDO9Z** password

David and jhon are allowed to be connected on the proxy only if their IP address is a part of **192.168.1.0/24** and during **production time**

Members, groups, targets can be managed in the "**Policies**" menu.

Create members

On the "**Policies**" left menu, choose "**Members**".
Click on **New member** button.
Add the username and password your require to be connected on the RDS Proxy.

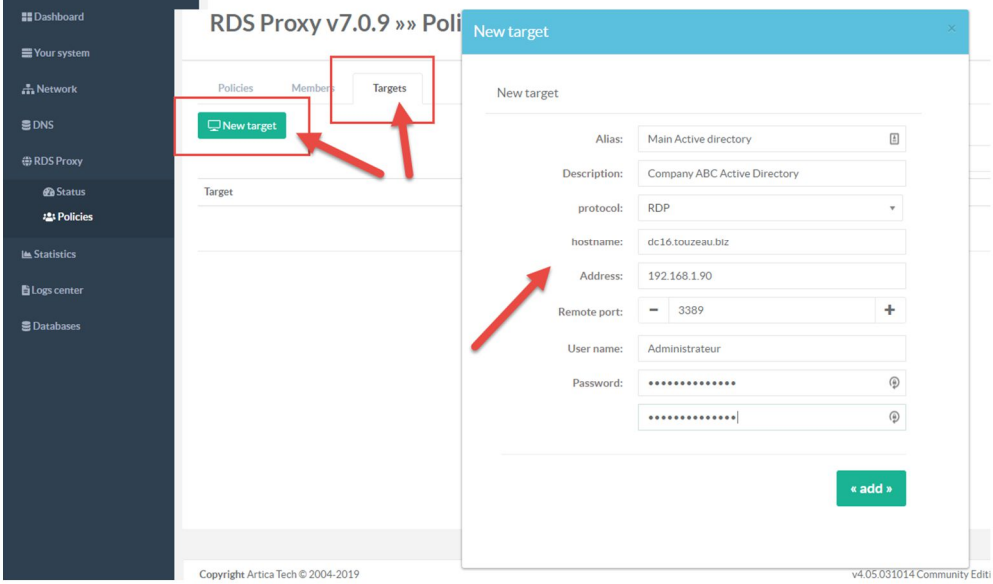


In our case, we create **jhon** and **david**.

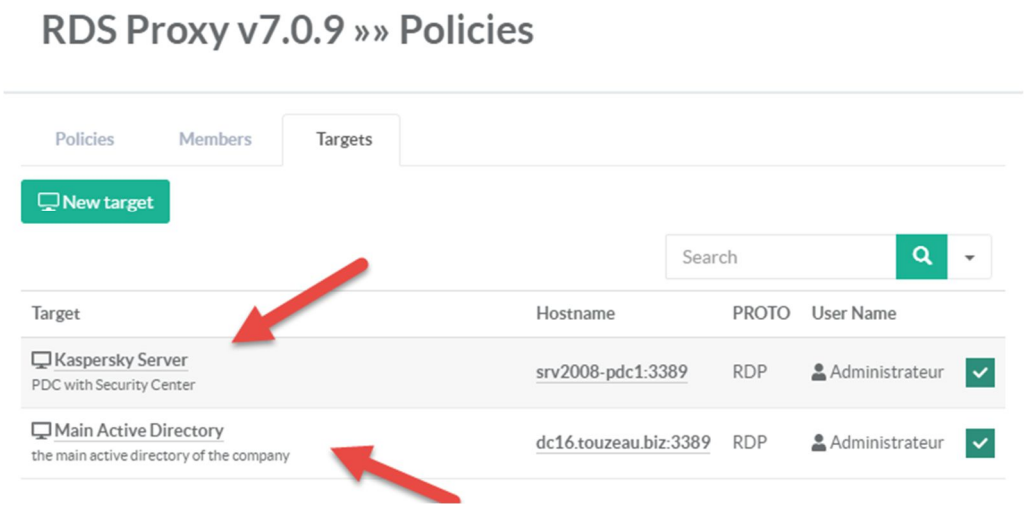
Create Targets

Click on the **targets** tab
Click on **New target** button

- **Alias** : A name that will be displayed in the TSE section
- **Description**: a short description that will be displayed on the TSE section.
- **Protocol**: choose **RDP** or **VNC**
- **Hostname**: The real hostname of the remote server
- **Address**: the FQDN or the IP address of the target server.
- **Remote port**: the listen VNC/RDP port
- **Username**: the real username that will be used in order to access to the target.
- **Password**: The real password that will be used in order to access to the target.

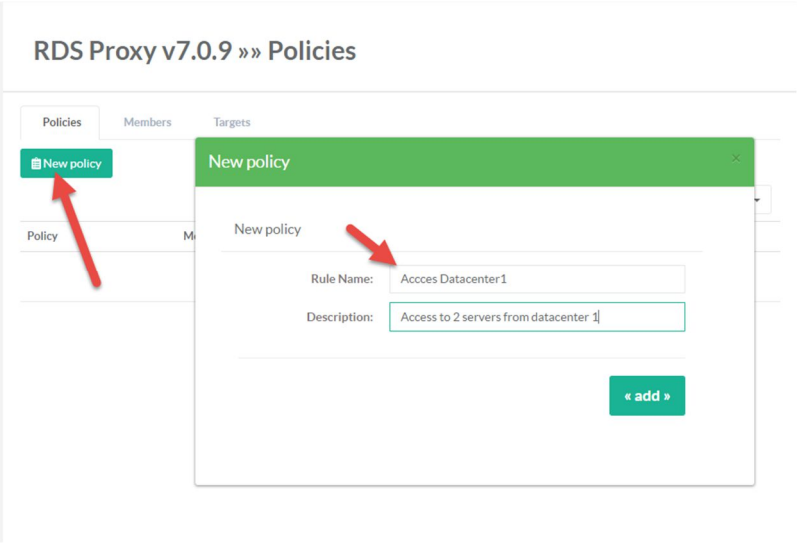


On our case, we will create 2 targets for **dc16.touzeau.biz** and **srv2008-pdc1**

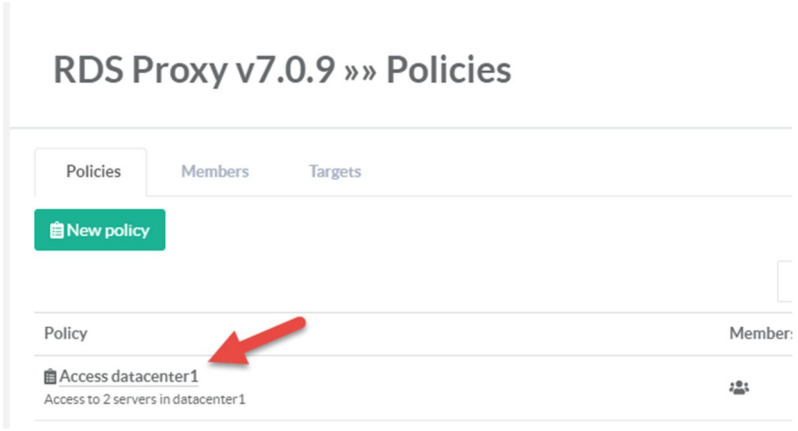


Create the policy

- Click on the **Policy** tab.
- Click on the **New Policy** button
- Give the policy name (rule name) and a short description
- Click on **Add** button.

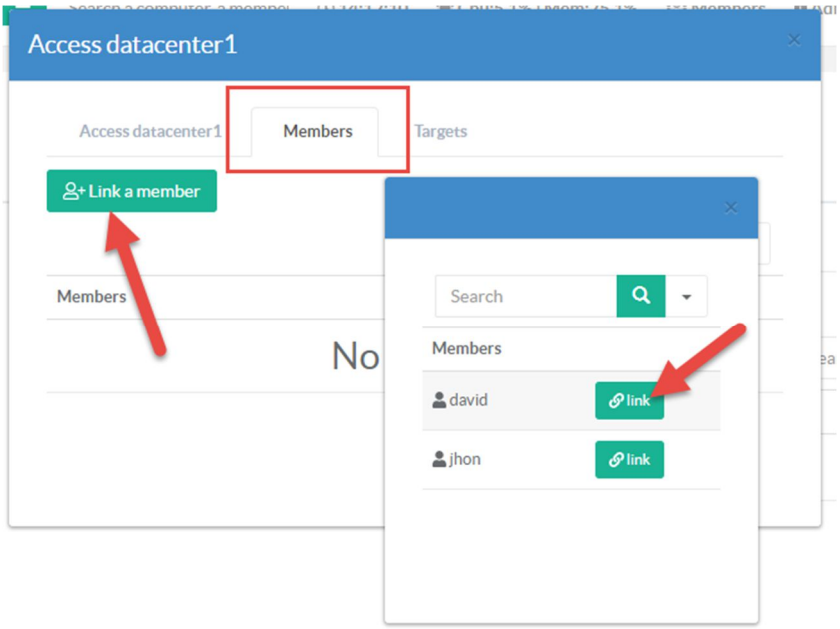


Click on your **New policy** in the table



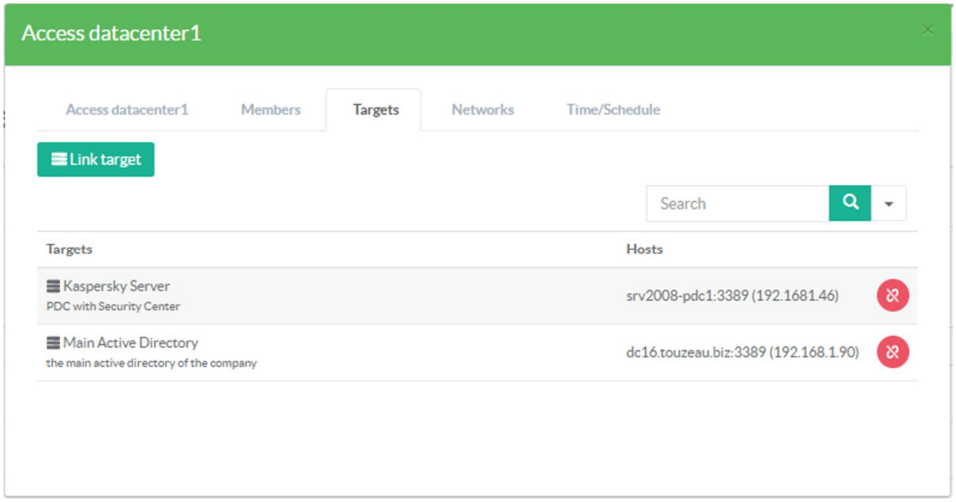
Associates members to the policy

Choose the "**Members**" tab
Click on **Link a member** and choose which member will be associated to this policy.



Associates targets to the policy

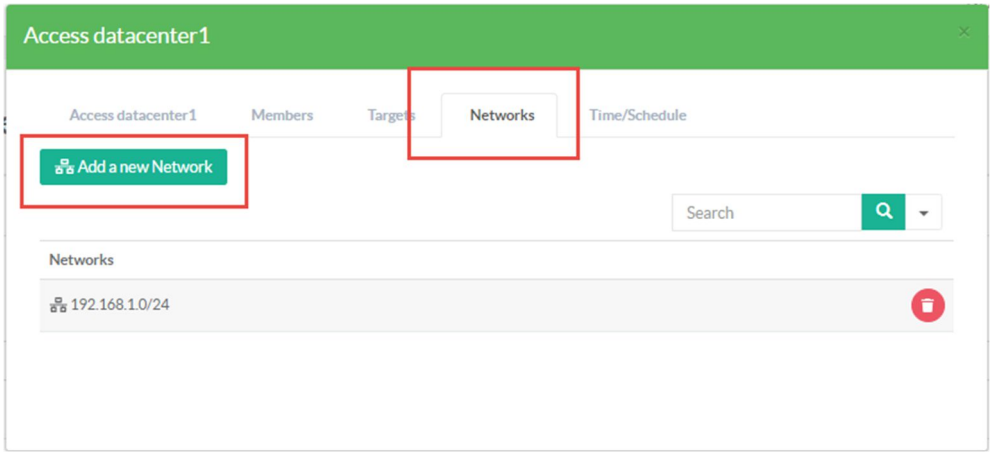
Choose the Targets tab
Click on link Target to link a target server to the policy



Set Network to the policy

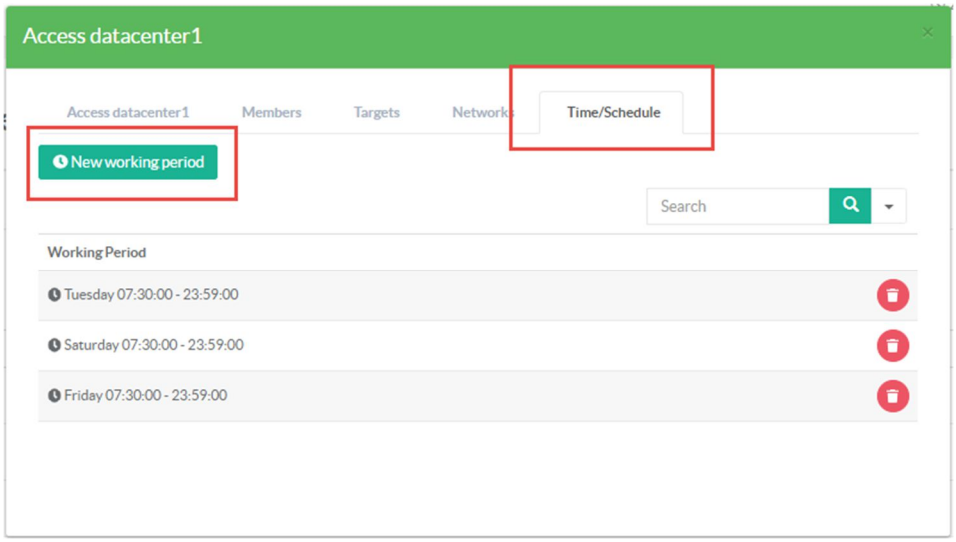
The Network section in the policy defines which sources IP addresses can use the policy
Outside the defined network and if no policy matches the source IP address, the RDP client will be rejected.

You can add a single address : 192.168.1.1 or 192.168.1.1/32 or subnet 192.168.1.0/24 in CDIR notation.



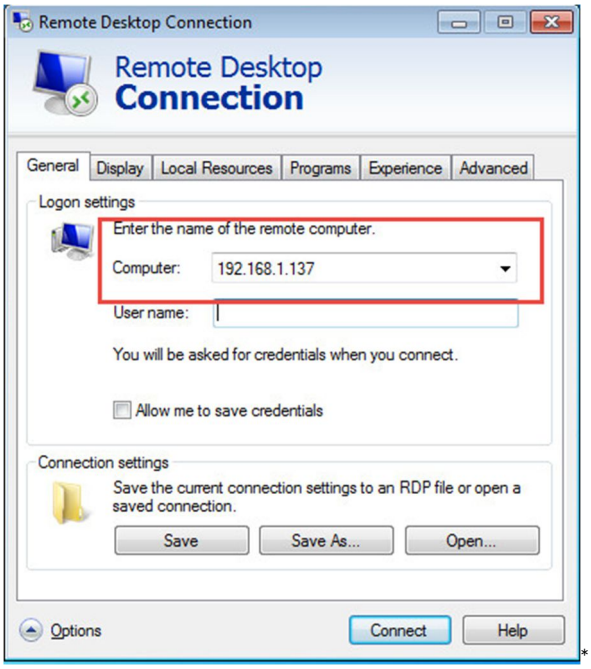
Set working periods

Working periods allows members to be connected to the targets only inside defined periods.
You can add a period defined by a day of week and the period allowed to be connected.

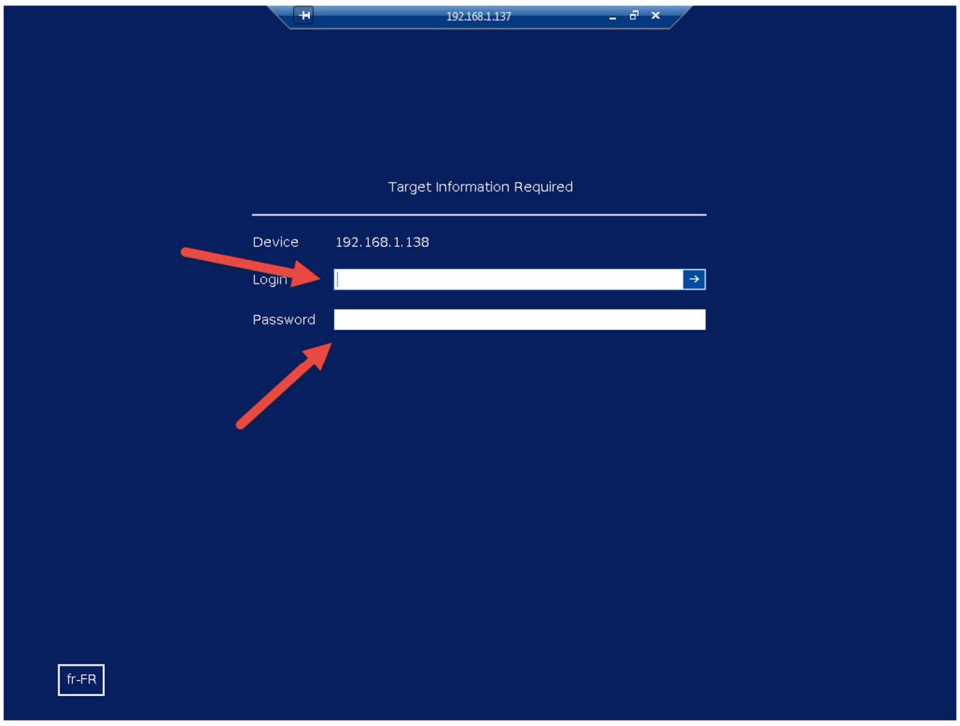


CONNECT TO THE RDS PROXY

Open a TSE client on your computer and type the IP address of your Artica server with RDS Proxy installed.



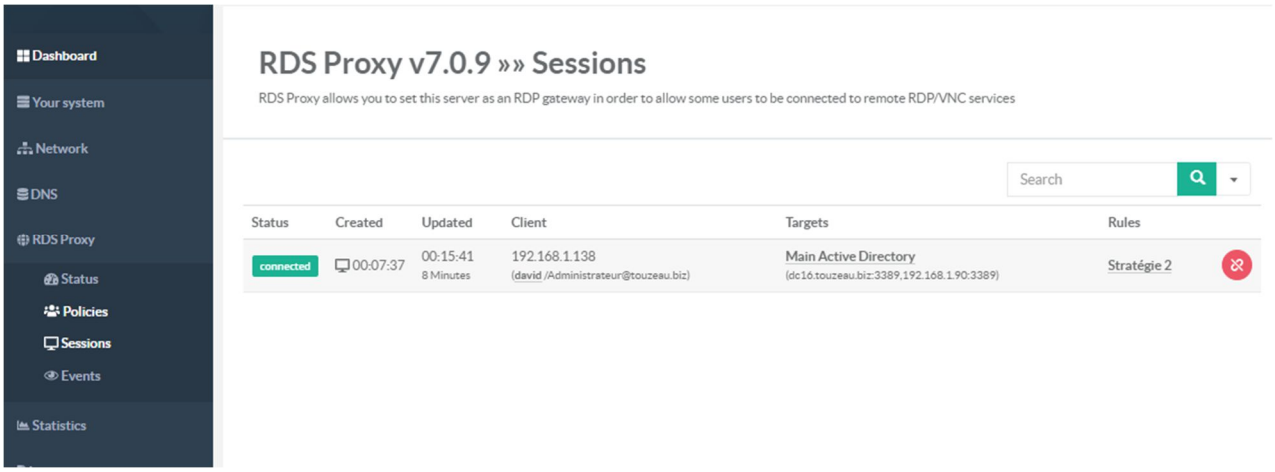
Inside the TSE session a form is displayed and ask credentials of a member defined in a policy.



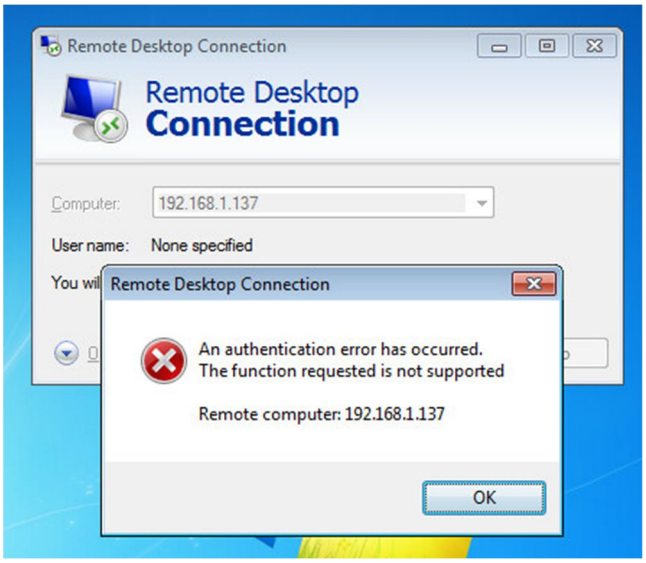
After sends credentials, a table is displayed in the TSE session.
This table display all available targets from all policies

After select with the mouse the target, the session will open to the target server automatically with credentials defined in the Artica targets database.

In Artica, select the sessions on the left menu in order to see the current established session.
You can kill the session by click on the unlink icon on the session row.



Connection Error on Windows 7 or Windows XP



If you encounter this error while connecting to the RDS Proxy:

"An authentication error has occurred. The function requested is not supported"

On the service parameters, change:

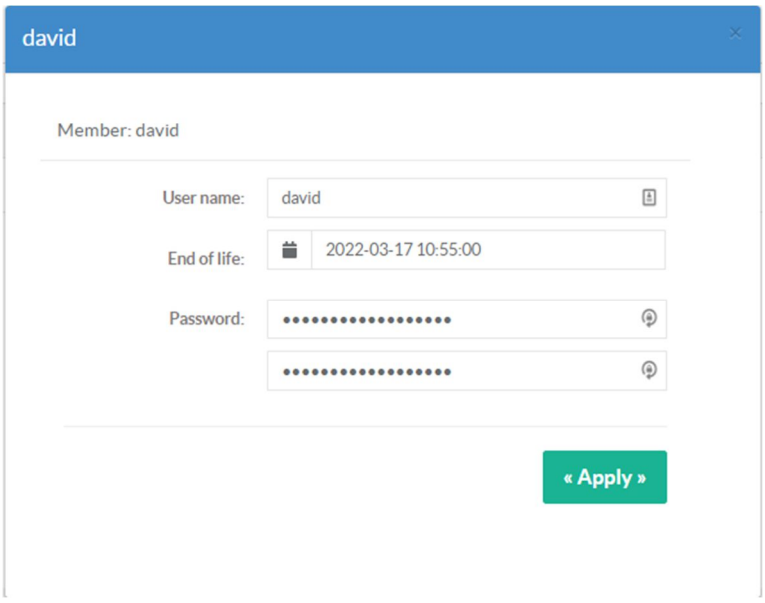
- **Minimal TLS version** to **"No restriction TLS v1.0**"
- **Cipher Suites** to **"More RDP clients (less secure)"**

Is RDS Proxy is Fail To Ban compatible ?.

Yes RDS Proxy is automatically monitored by fail To ban. If there are too much rejected RDP sessions, the fail to ban service will add automatically the source IP address in the local Firewall.

CAN I DEFINE SOME MEMBERS TEMPORARY?

Yes you can define a **End Of life** of each account associated to a policy
End of life is a maximal date a user can use the proxy.
If the time is expired, the user is disabled and cannot use the RDS proxy anymore.

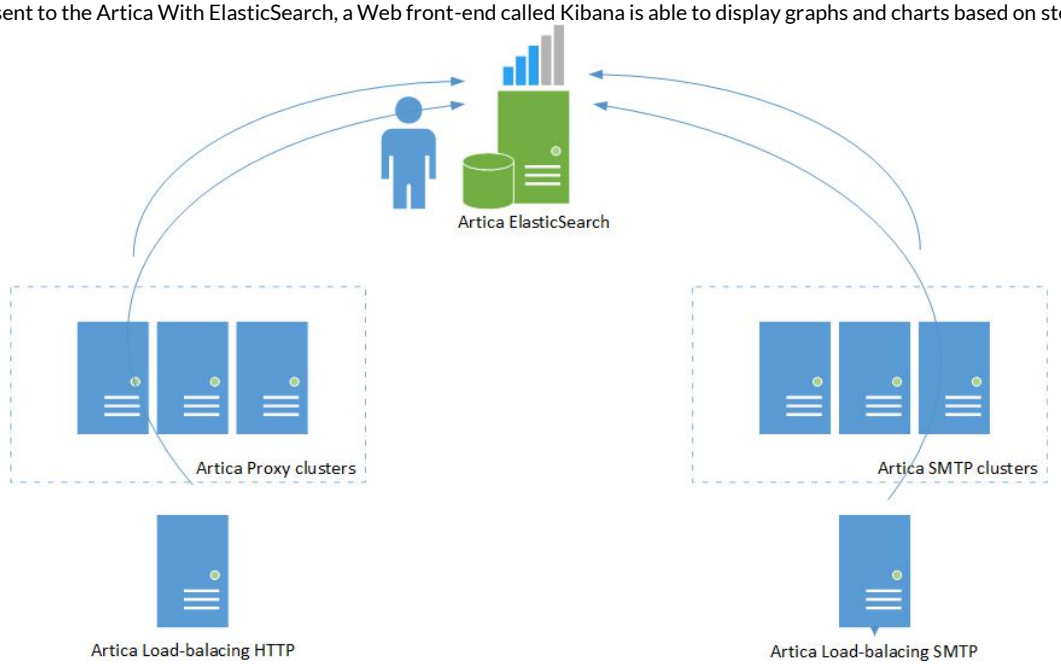


ELASTICSEARCH STATISTICS

Professional statistics are based on ElacsticSearch database.
Artica is able to manage the ElasticSearch service, in this case you can use Artica for this purpose.

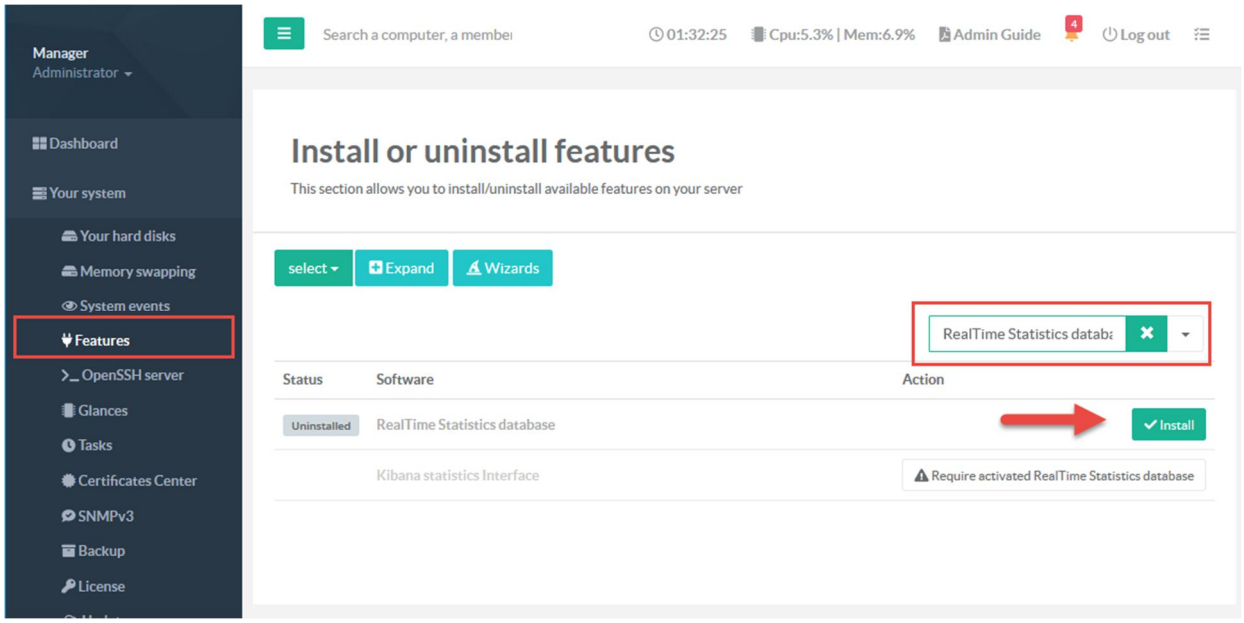
It is recommended to install a dedicated Artica Proxy instance for this purpose.
Use a minimal of 4vcpus, 8GB of memory and 150GB of hard drive.

Basically all events are sent to the Artica With ElasticSearch, a Web front-end called Kibana is able to display graphs and charts based on stored events.



INSTALL THE CORE STATISTICS DATABASE SERVER

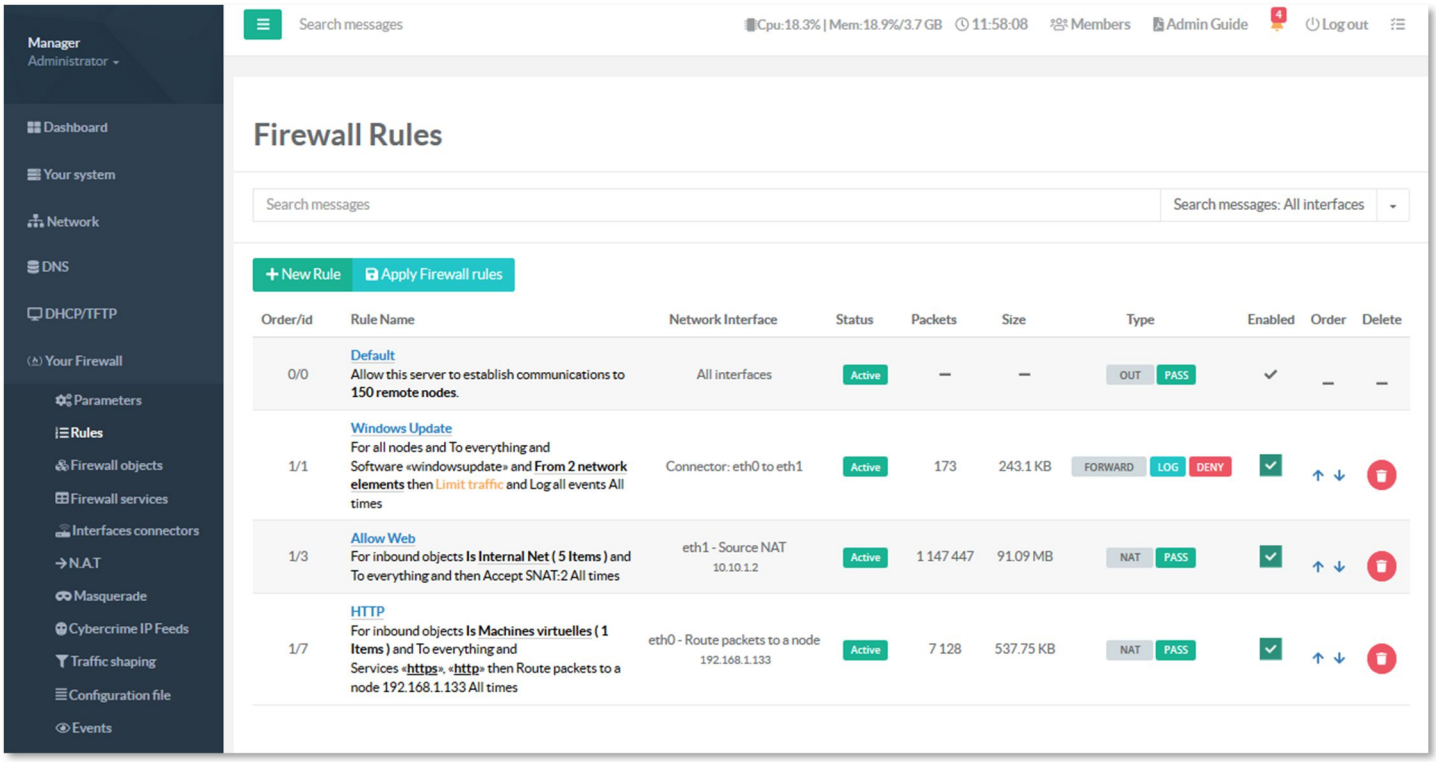
- Go into the features section
- On the search field, type "**ElasticsEarch database**"
- Click on **install** button.



FIREWALL PROTECTION

Artica Firewall feature protects PCs, servers or any other connected devices from hostile intrusions from the Internet and/or external networks.

It enables stateful packet filtering, Network Address Translation (NAT) and Port Address Translation (PAT) and is fully customizable to fit your needs.
There is no need for any UNIX skills, no need to use the command line for anything, and no need to ever manually edit any rule sets.
Users familiar with commercial firewalls catch on to the web interface quickly, though there can be a learning curve for users not familiar with commercial-grade firewalls



IPTABLES(NETFILTER) BASED FIREWALL

Artica Firewall feature is an iptables(netfilter) based firewall system designed around the essential needs of today's Internet deployed servers and the unique needs of custom deployed Artica installations.
The Web administration console is designed to be very informative and present the user with an easy to follow process

- Real-time logging web console.
- **Cybercrime IP Feeds** is a feature that downloads regularly compromised IP addresses found in the Internet. It prevents your server to be attacked by already ban a bulk of IP addresses.
- **Geo-Location** module allows you to define rules against location of Public IP addresses.
- **Deep Packet inspection** module allows you to create rule against more than 239 detected applications in both HTTP/HTTPs protocols.
- **Traffic shapping** module is An high-performance implementation of committed access rate, or simply rate limiting, or policing.
- **Time restriction** module restricting Access By Time Of The Day.It allows you to control access based upon day and time.

INTRUSION DETECTION/PREVENTION SYSTEM

Artica provides Intrusion Detection System (IDS) that analyzes network traffic and tries to detect exploits, leaking data and any other suspicious activity.
Upon detection, alerts are raised and the attacker is immediately blocked.

- Layer 7 application detection
- Multiple rules sources and categories
- Emerging threats database
- IP blacklist database

Firewall documentation can be found here:
http://articatech.net/documentation-firewall.php

SECURIZE YOUR ARTICA SERVER IN CASE OF CORRUPTED SERVER.

Artica can run many services and you can install yourself Web services such as web services or any others services by enter into the system.
If a virus enter into the Artica system you have to be sure that your corrupted Artica server will not spread internet in any ports or any destination.

By default, when you turn the WAN Interface to "**Finally deny all**", *the right way*, Artica automatically allow these protocols:

- ICMP : Accept to send ping to any
- DNS accept to send udp/tcp queries on 53 to any
- HTTPS accept to send HTTPs request on 443 destination port.
- HTTP : accept to send http requests on 80 destination port.
- FTP : accept to send FTP requests on 21 destination port
- NTP accept to send NTP requests on any destination.
- RSYNC accept to contact any rsync server
- SMTP accept to send messages on any SMTP servers on destination port 25
- SMTPS accept to send encrypted messages on any SMTPs server on destination
- cloudufdb accept to send request to 217.182.193.199:6000

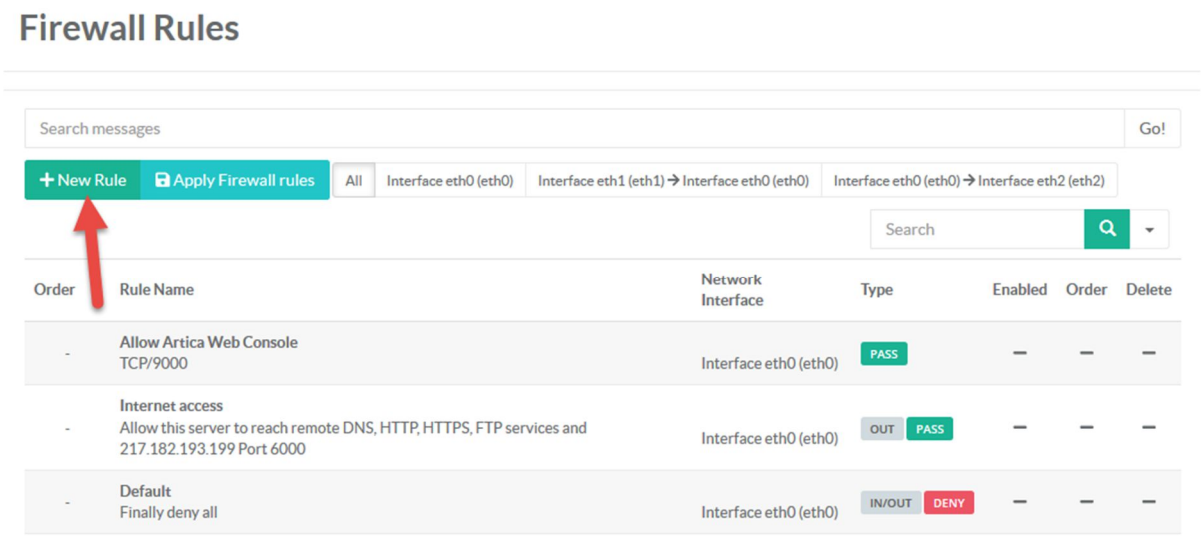
For more details of allowed protocol, see the "**firewall services**" feature.

These rule are default rules and you can overide these rules by your own rule.

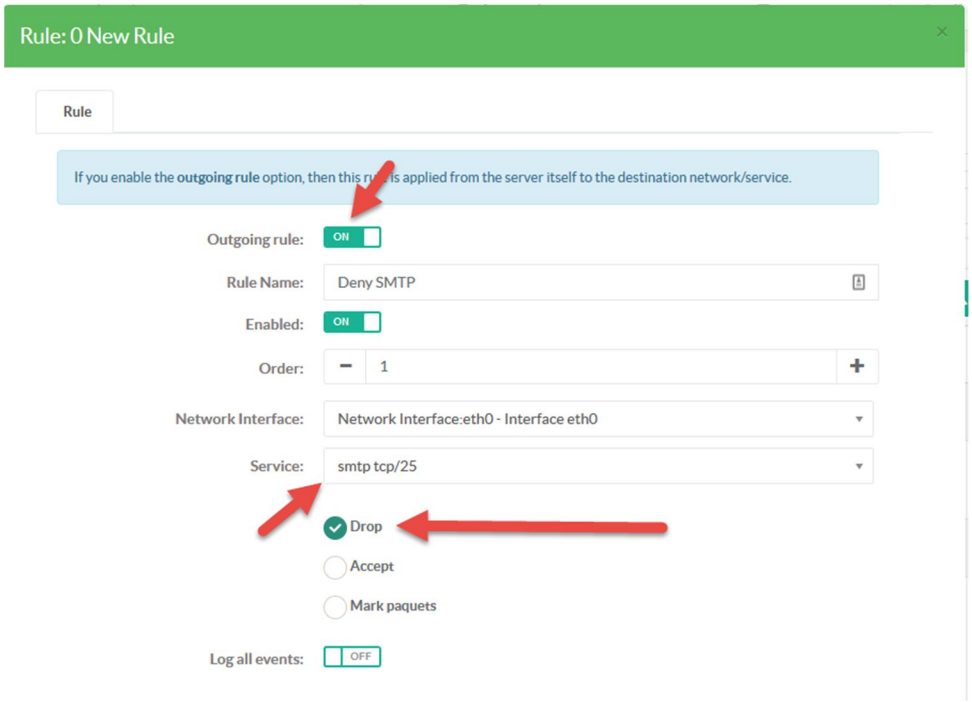
For example:
Our Artica server is not an SMTP relay and we just need Artica to send SMTP notification to our internal server.
Our Artica server use DNS but only to reach the Google DNS on 8.8.8.8 and 4.4.4.4

So we have to **disable** the SMTP/SMTPs protocol and **specify** that the DNS query must **only go to Google**, nothing else.

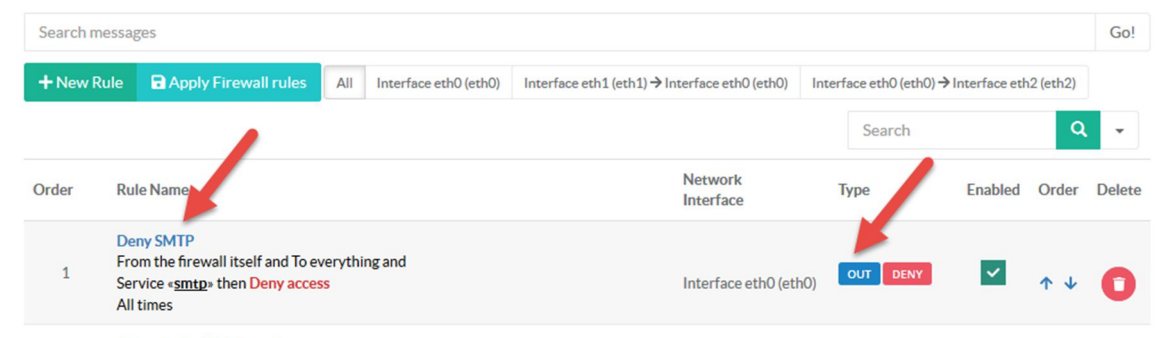
- To override default rules, you have to use the "**Your Firewall**" / "**Rules**" section.
- On the main table, click on **New Rule**



On the new rule form, **choose the Interface** that act as WAN, specifiy that the rule is an "**Outgoing rule**" specify the service (in our case it is the SMTP service) and set the action as "**DROP**" in order to deny connection.



Your rule is added in the table as a DENY "Outgoing" rule.



This rule is designed to erase the default rule (SMTP)

DEEP PACKET INSPECTION

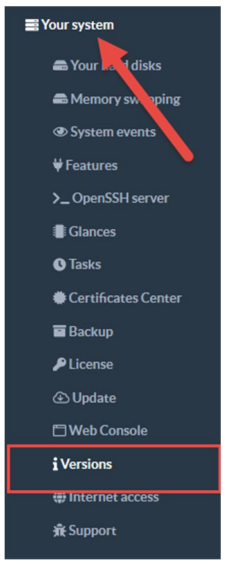
Deep packet inspection (DPI) is a type of data processing that inspects in detail the data being sent over a computer network, and usually takes action by blocking, re-routing, or logging it accordingly.
The Deep packet inspection is able to patch the Firewall in order to add a new module.
This module allows to enrich firewall rules by adding the possibility to detect some applications communication

Currently the Deep packet inspection allows to detects more than **200** applications

List of detected applications

AFP
AJP
AMQP
Aimini
Amazon
AmazonVideo
Apple
AppleJuice
ApplePush
AppleStore
AppleiCloud
AppleiTunes
Armagetron
Ayiya
BGP
BJNP
BattleField
BitTorrent
CHECKMK
CNN
COAP
CSGO
CiscoSkinny
CiscoVPN
Citrix
Cloudflare
Collectd
Corba
Crossfire
DCE_RPC
DHCP
DHCPV6
DNS
DNScrypt
DRDA
Deezer
Diameter
DirectConnect
Direct_Download_LinkDofus
Dropbox
EAQ
EGP
FIX
FTP_CONTROL
FTP_DATA
Facebook
FacebookZero
FastTrack
Fiesta
Florensia
GMail
GRE
GTP
GenericProtocolGit
Github
Gnutella
Google
GoogleDocs
GoogleDrive
GoogleHangout
GoogleMaps
GooglePlus
GoogleServicesGuildwars
H323
HEP
HTTP
HTTP_ActiveSyncHTTP_Connect
HTTP_Download
HTTP_Proxy
HalfLife2
Hotmail
HotspotShield
IAX
ICMP
ICMPV6
IFLIX
IGMP
IMAP
IMAPS
IPP
IP_in_IP
IPsec
IRC
IceCast
Instagram
KakaoTalk
KakaoTalk VoiceKerberos
Kontiki
LDAP
LISP
LLMNR
LastFM
LinkedIn
LotusNotes
MDNS
MGCP
MPEG_TS
MQTT
MSN
MS_OneDrive
MapleStory
Megaco
Memcached
Messenger
Microsoft
MsSQL-TDS
Musical.ly
MySQL
NFS
NOE
NTP
NetBIOS
NetFlix
NetFlow
Nintendo
OCS
OSPF
Office365
Ookla
OpenDNS
OpenFT
OpenVPN
Oracle
Oscar
POP3
POPS
PPLive
PPStream
PPTP
Pando_Media_BoosterPandora
Pastebin
PcAnywhere
PlayStore
Playstation
PostgreSQL
QQ
QQLive
QUIC
RDP
RSYNC
RTCP
RTMP
RTP
RTSP
RX
Radius
Redis
RemoteScan
SAP
SCTP
SIP
SMB
SMPP
SMTP
SMTPS
SNMP
SOCKS
SOMEIP
SSDP
SSH
SSL
SSL_No_Cert
STUN
ShoutCast
Sina(Weibo)
Skype
SkypeCallIn
SkypeCallOut
Slack
Snapchat
Sopcast
Soulseek
SoundCloud
Spotify
Starcraft
Stealthnet
Steam
Syslog
TFTP
TINC
TVUplayer
TeamSpeak
TeamViewer
Telegram
Telnet
Teredo
Thunder
Tor
TruPhone
Tuenti
Tvants
Twitch
Twitter
UBNTAC2
UPnP
UbuntuONE
JabberUsenet
VHUA
VMware
VNC
VRRP
Vevo
Viber
Vidto
Warcraft3
Waze
WeChat
Webex
WhatsApp
WhatsAppFiles
WhatsAppVoice
Whois-DAS
Wikipedia
WindowsUpdate
WorldOfKungFu
WorldOfWarcraftXDMCP
Xbox
Yahoo
YouTube
YouTubeUpload
Zattoo
ZeroMQ

Install the Deep packet inspection

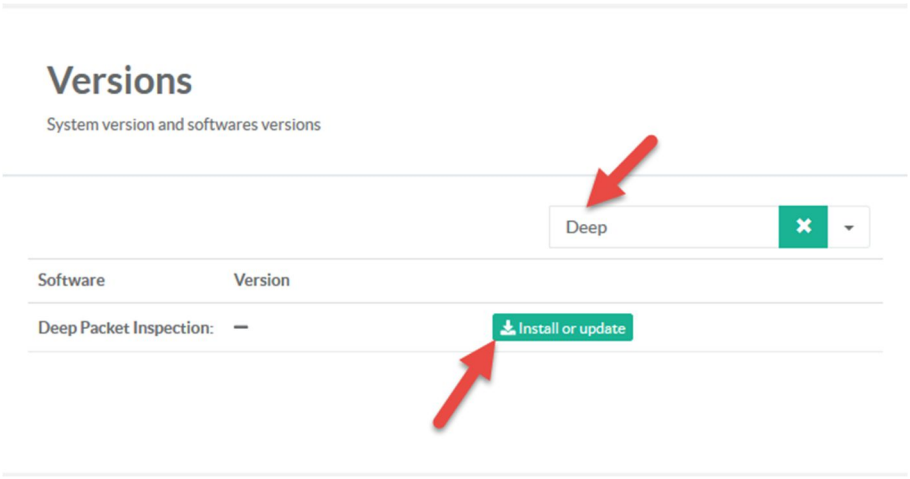


This feature is not compatible with "MultiPath TCP Kernel" feature.

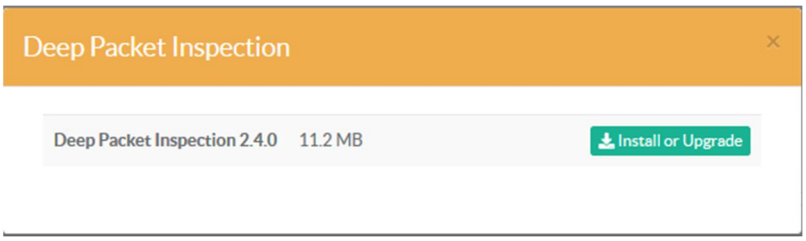
Make sure you have the latest package.

- On the left menu,
- go into "**Your system**"
- Click on "**Versions**" menu.

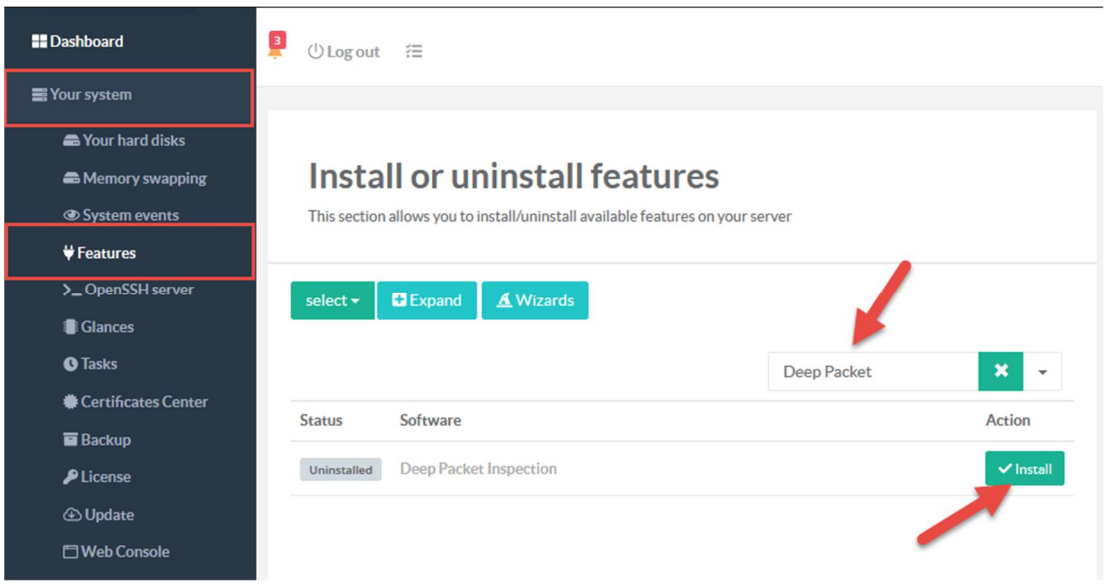
- On the search field type "**Deep**"
- You will see the current installed version.
- If you see a dash, this means the module is not on your server.
- Click on **Install or update** button.



A layer is displayed and shows you available versions
Click on the button **Install or upgrade**.



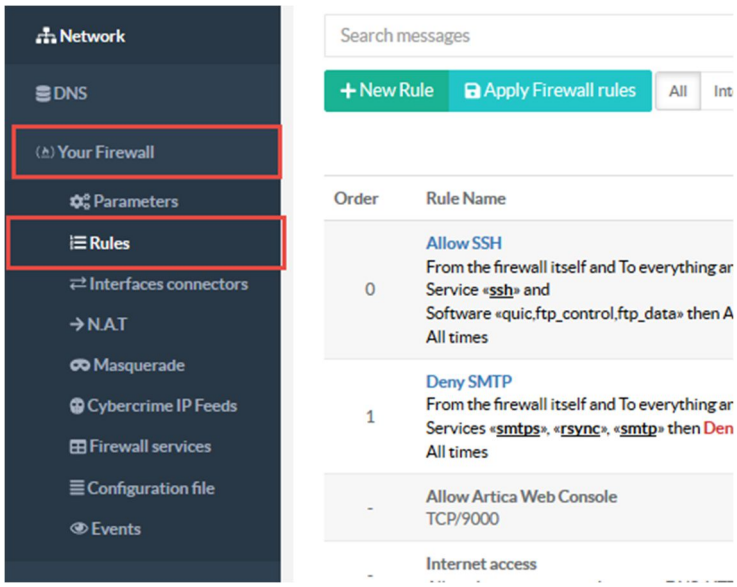
After installing software on your server, go into Your System and features on the left menu.
On the search field, type "**Deep**"
Click on "**Install**" button under "**Deep Packet Inspection**" row.



Use Packet inspection

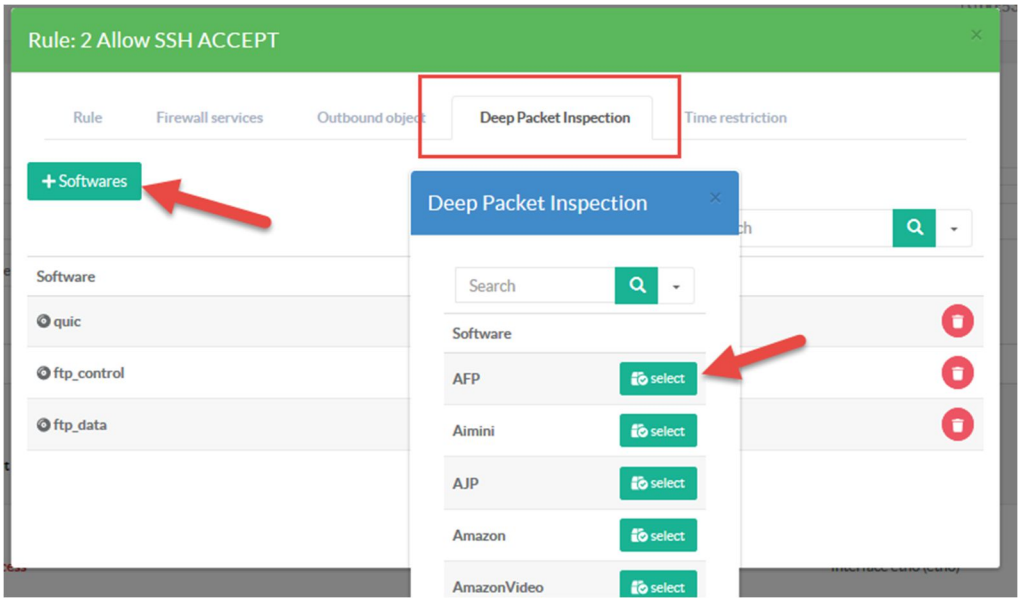
The Packet inspection is used in **FireWall rules**.

- On the left, menu use the "Your FireWall" and Rules.



- Create a new rule and save it.
- Open the new created rule.

Select the "Deep packet inspection" tab.
With the Softwares button, choose which application you want to detect inside your rule.



AUTOMATIC PROTECTION – FAIL TO BAN

The Fail to Ban (aka fail2ban) service is an intrusion prevention software framework that protects your Artica servers from brute-force attacks
Most commonly it is used to block selected IP addresses that may belong to hosts that are trying to breach the system's security.
It can ban any host IP address that makes too many login attempts or performs any other unwanted action within a time frame defined by the administrator.

Install the Fail to ban service.

Go to the features section, in the search box, type “fail to”

Click on **Install** button on the “Fail To Ban” service.

THE SMTP SERVICE

The Artica SMTP service is designed to provide an advanced SMTP routing service and/or Anti-Spam/Antivirus service.

FEATURES

Anti-spam

Artica implements a number of techniques to detect, filter and block spam.
It combines artificial intelligence algorithms and constantly adapts to identify the ever-changing techniques of spammers.
ArticaTech provide advanced antivirus patterns to detects SPAM and phishing.

Protection

Artica is able to fight against phishing, ransomwares, malware, crypto locker and other threats.

Anti-virus

The antivirus service is able to check all incoming messages for viruses, worms, macro and suspicious attachments with potentially dangerous contents.

Quarantine

Artica offers a simple way to review quarantine lists

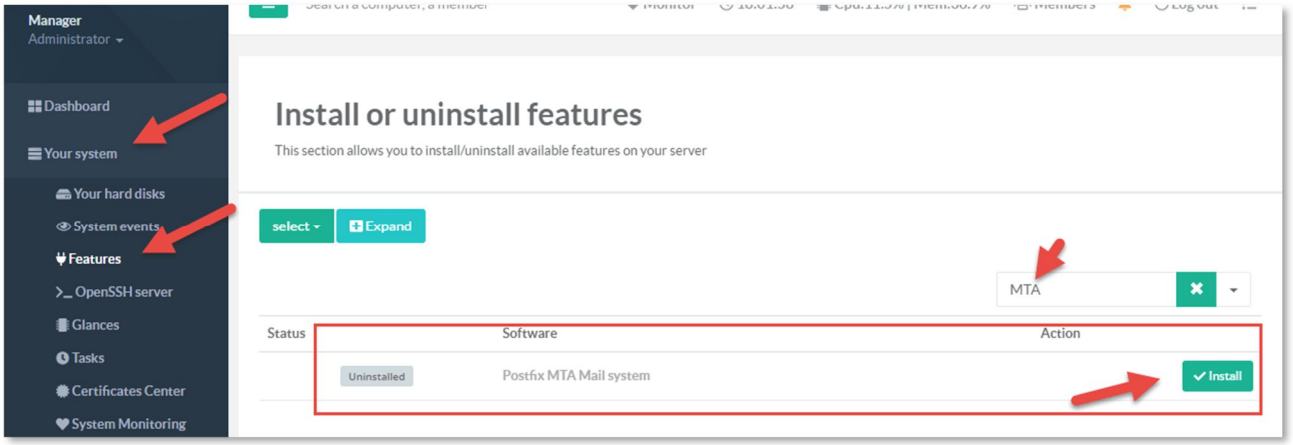
Powerful management

The administrator can keep control of all system settings.
Detailed traffic and filtering reports give the administrator a clear vision of network and mail activity.

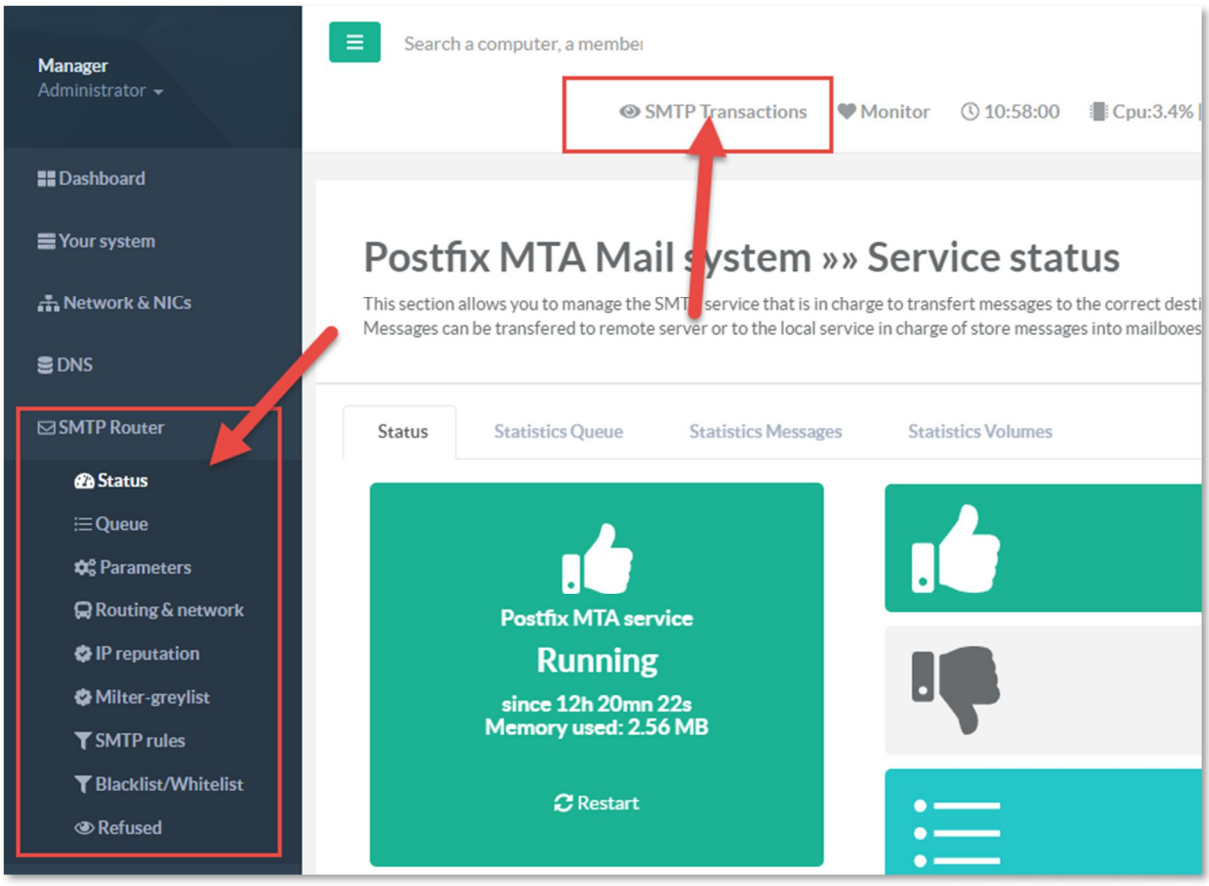
INSTALL THE SMTP SERVICE

The SMTP service is a designed appliance, after installing this service.
All "Appliance services" will be removed and hidden in the Features section.

- On **Your system/Features** in the Search box, type "**MTA**"
- Click on Install on the "**Postfix MTA Mail system**" row.



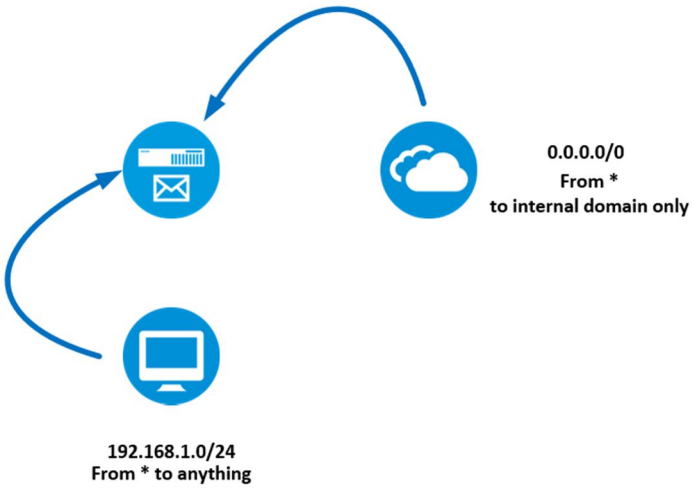
After installing the service, you will be able to show the menu "**SMTP Router**" that displays available options.
On the TOP Menu, a new item "**SMTP Transactions**" is added.
This option is designed to display routed messages in realtime.



First step, set your authorized networks.

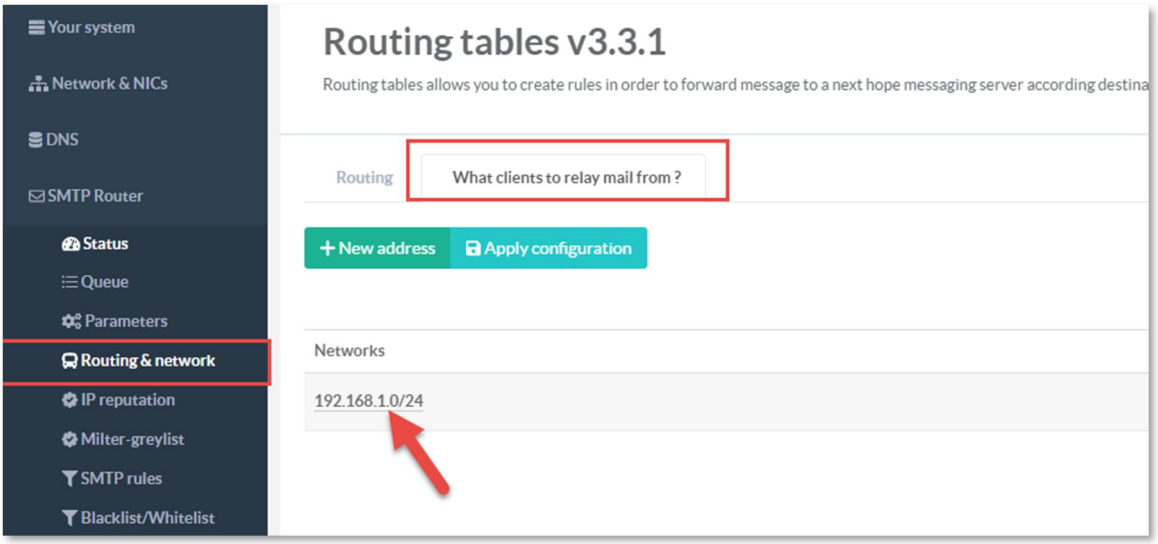
It is important for your MTA service to define which network is allowed to send messages to Internet (any)

To perform this behavior, the MTA service needs to know which computer is able to send a message to be forwarded to foreign domains.



On the **SMTP Router**, **Routing & network**, selec the "**What clients to relay mail from**" tab.

Add all networks or IP addresses of the computers/servers that will be able to send messages to Internet.

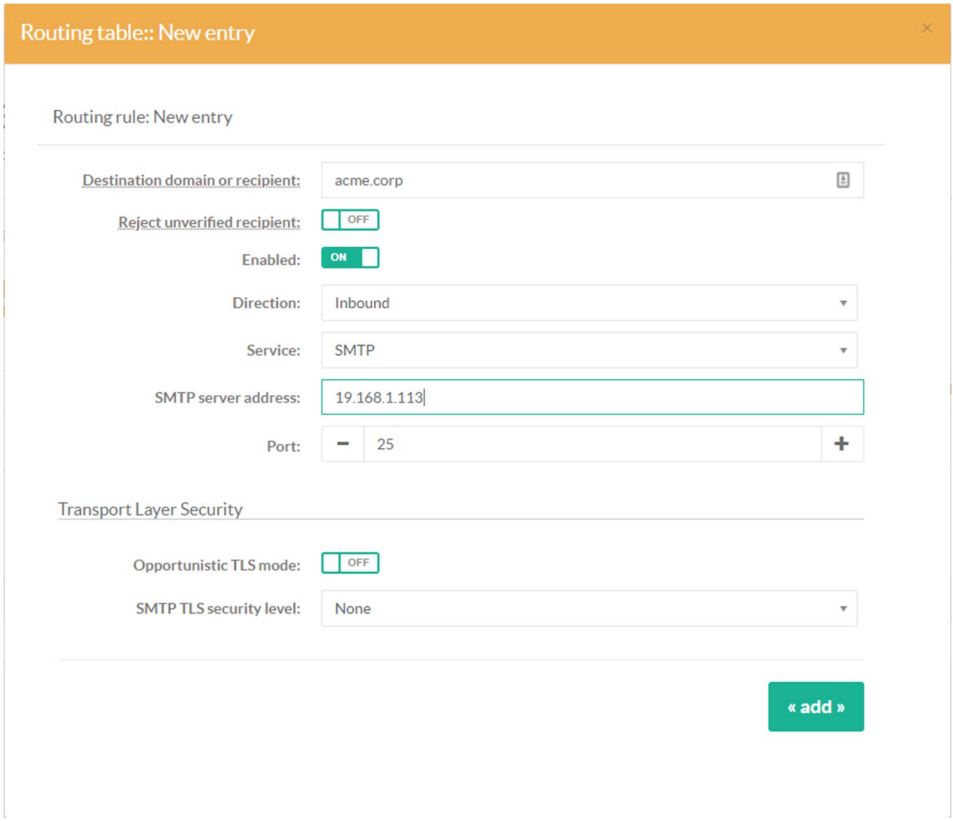


THE ROUTING TABLE

On the **SMTP Router**, **Routing & network**, selec the "**Routing**" tab.

This section instructs the SMTP service where to forward messages according sender email or sender domain or recipient email or recipient domain.
In most cases you want to relay messages according to the destination domain.

Click on **new rule** in order to create a routing rule



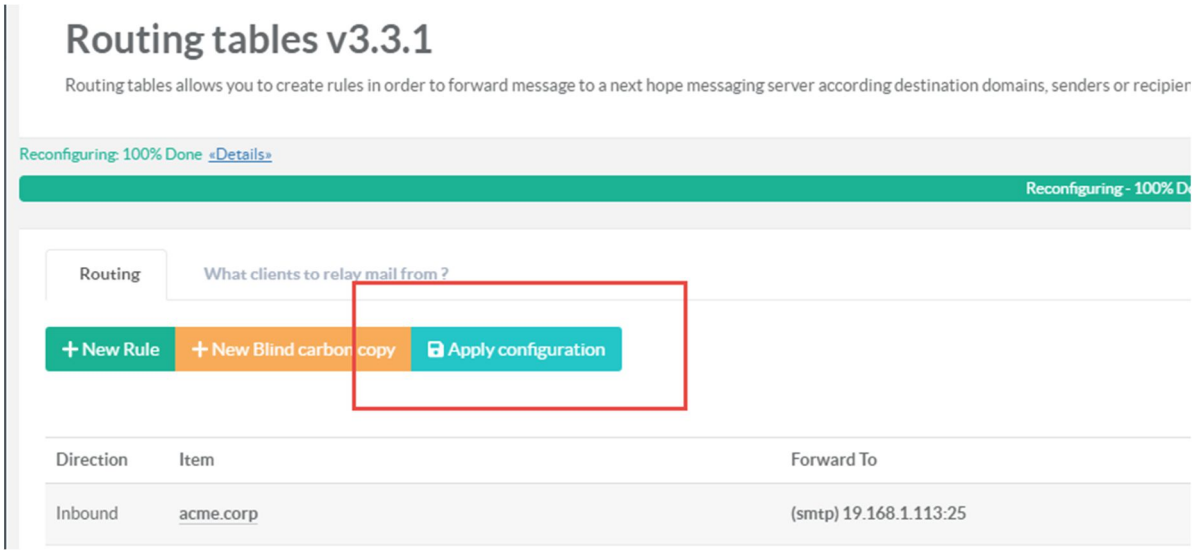
Destination domain or recipients:.
If the option"**Direction**" is "**Inbound**" then this field is the destination address.
It should be:
"dummy@domain.tld or domain.tld or .domain.tld"

If the option "Direction" is "Outbound", then this filed is the sender address.
It should be
"dummy@domain.tld or domain.tld or .domain.tld"

The service
The router service that will be in charge to forward the message from the mail queue.
In most cases this will be the **SMTP** service

The SMTP server address and port:
The hostname or IP address of the destination server.

Opportunistic TLS mode.
If turned to ON your Artica server will try to forward the message using TLS/SSL, you can define the TLS verification method that your Artica server should use.



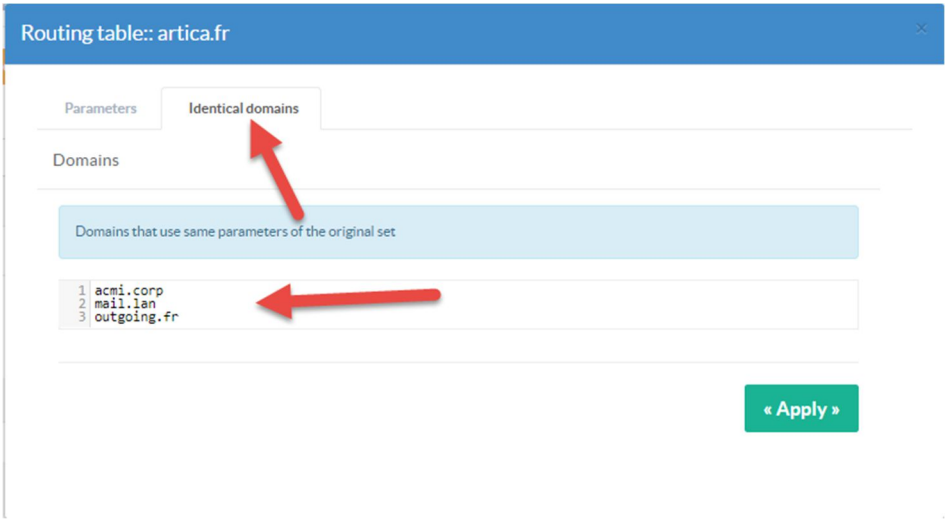
Did not forget to "Apply configuration" after creating all rules.

Many domains in the same routing rule

If you have several SMTP domains that should use the same routing parameters, open the first routing rule you have created.

Open the tab Identical domains.

In the text area, add all domains that will use the same configuration.



Transfert messages to Exchange 2010 using TLS on port 587

QA: SSL ? Get Exchange 2010 Server to listen for SMTP on port 465?
Yes, you can make any SMTP virtual server or Receive connector listen on port 465, but that will not achieve your goal of secure SMTP (SMTPS).

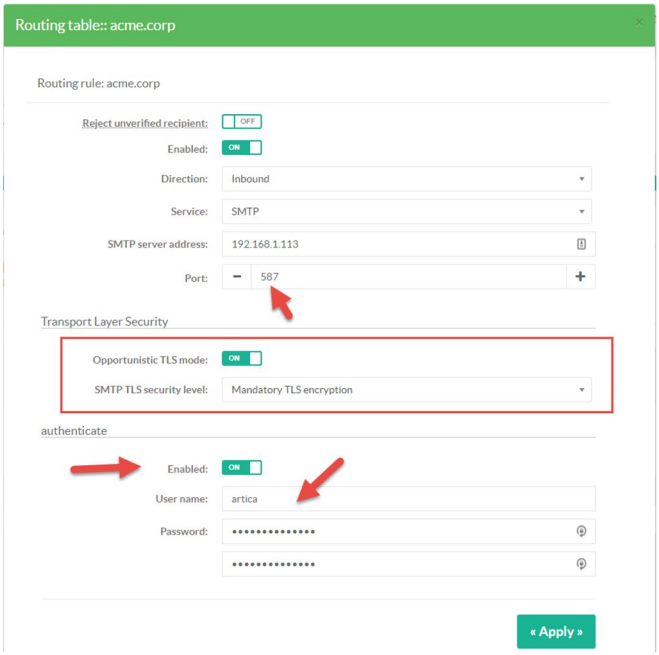
1. Create a user/mailbox like “Artica”
2. Start the Exchange Management Console.
3. In the console tree, click **Recipient Configuration**.
4. In the result pane, select the mailbox for which you want to grant the **Send As permission**.
5. In the action pane, under the mailbox name, click **Manage Send As Permission**. The Manage Send As Permission wizard opens.
6. On the Manage Send As Permission page, click **Add**.
7. In Select User or Group, select the user (artica) to which you want to grant the Send As permission, and then click OK.
8. Click **Manage**.

On the Exchange PowerShell, type this command

```
Get-ReceiveConnector "Name of Connector" | Add-ADPermission -user "ACME\artica" -ExtendedRights "ms-Exch-SMTP-Accept-Any-Sender"
```

On the routing rule

1. Define the target port as 587
2. Enable the TLS method
3. Turn on the Authenticate method
4. Set the username and passord of the user with “Send As permission”



Transfert all outgoing messages to an SMTP relay with authentication.

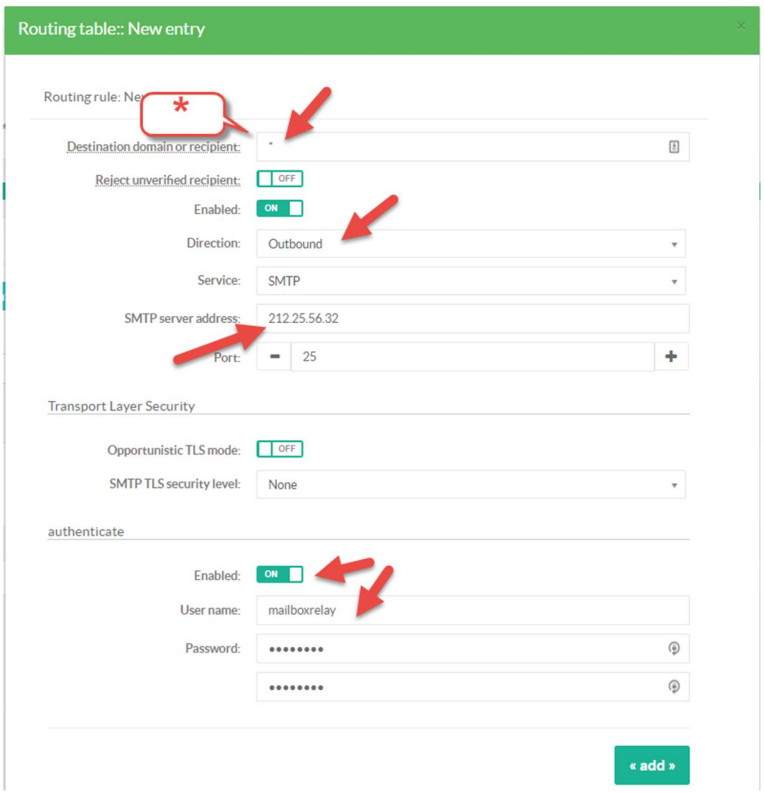
If Artica is designed to be an Internal hub and must forward all outgoing messages to a dedicated SMTP relay with authentication.

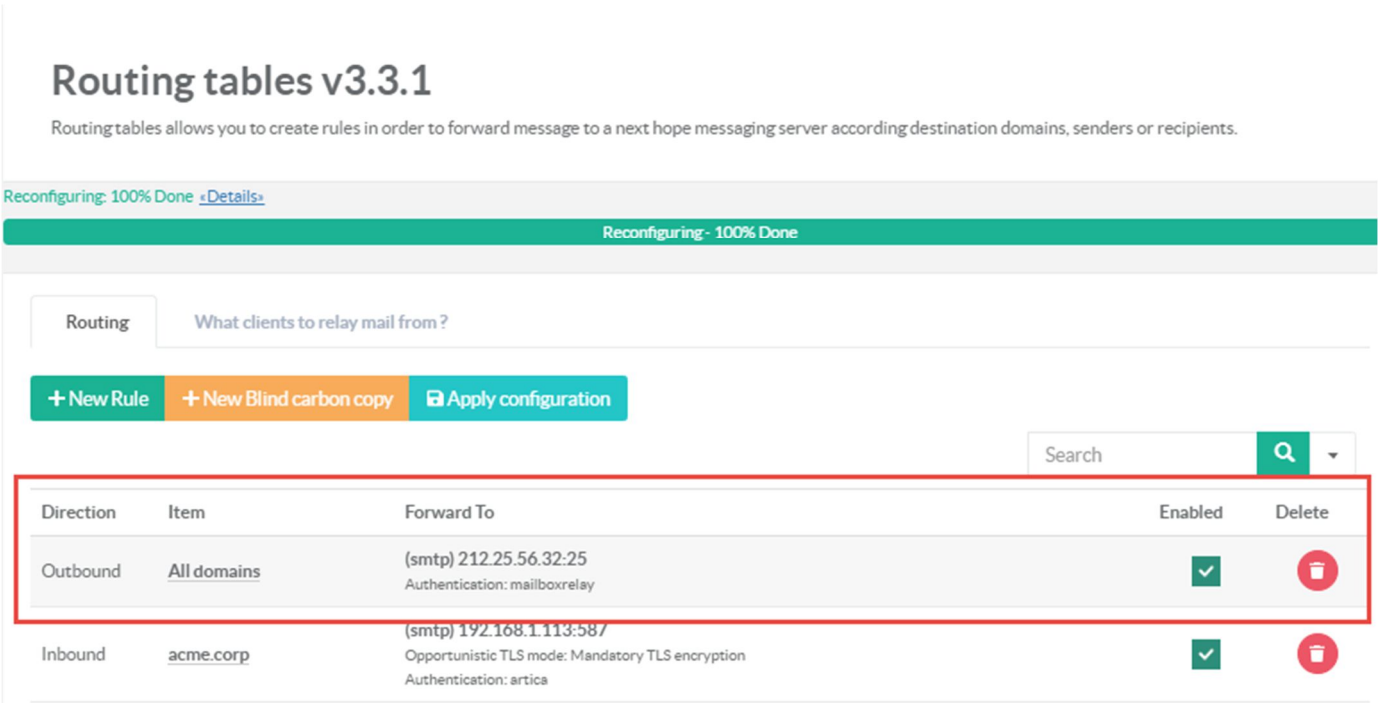
Create an outgoing routing rule with the wild-card "*" character has destination domain.

Select the direction as "Oubound" value.

Set the address of the outgoing relay.

Enable the Authenticate feature and give the username and password to enable your Artica server to authenticate the SMTP session.

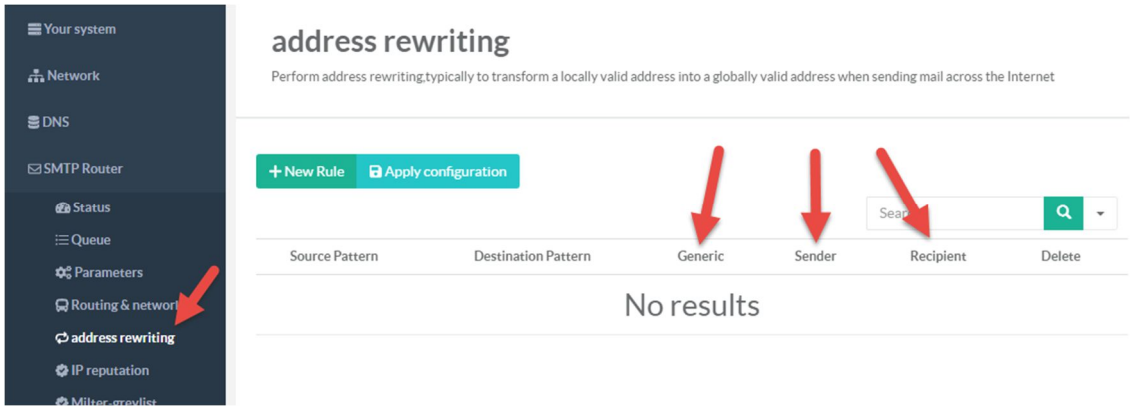




ADDRESSES REWRITING

Adresses Rewritting allows you to perform address rewriting
The menu "**SMTP router"/Addresses Rewriting** allows you to create rules according to 3 methods.

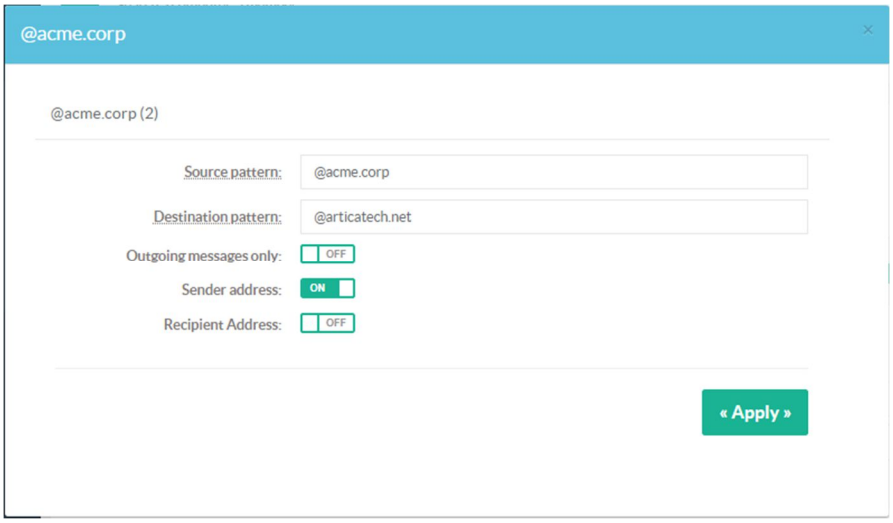
- ✓ **Generic**: Typically to transform a locally valid address into a globally valid address when sending mail across the Internet.
  Generic, means no direction but only for outgoing messages, addresses can be for sender or recipients. If found, it will be replaced.
  This is needed when the local machine does not have its own Internet domain name, but uses something like *localdomain.local* instead.



- ✓ **Sender**: You want to rewrite the SENDER address "user@ugly.domain" to "user@pretty.domain", while still being able to send mail to the RECIPIENT address user@ugly.domain
  Note: This option is processed before **Generic**.

- ✓ **Recipient**: Optional address mapping for envelope and header recipient addresses.
  Note: This option is processed before **Generic**.

Click on **New Rule** to open the Rewriting form.



Source patterns are tried in the order as listed below:

- ✓ **user@domain** address
  Replace user@domain by address.
  This form has the highest precedence

- ✓ **user address:**
  Replace user@site by address when site is equal to hostname, when site is listed in domains

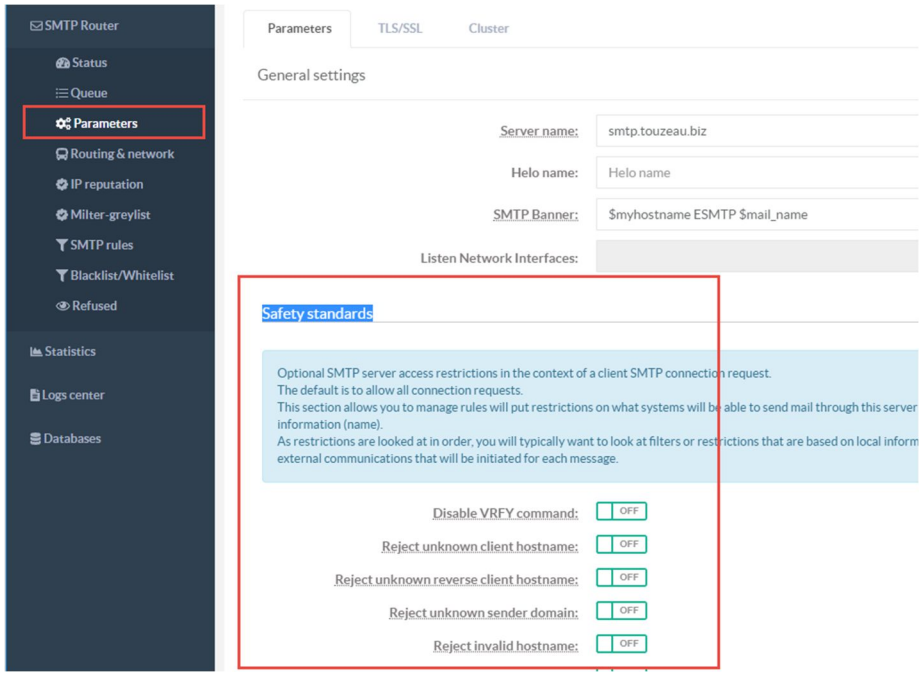
- ✓ **@domain address**:
  Replace other addresses in domain by address.
  This form has the lowest precedence

Examples:

```
his@localdomain.local >> hisaccount@hisisp.example
her@localdomain.local >> heraccount@herisp.example
@localdomain.local >> hisaccount+local@hisisp.example
@localdomain.local >> @validDomain.com
```

SAFETY STANDARDS

If your router is in front of Internet, you should enable some features that enforce SMTP security
On the left menu, select **SMTP router** and **parameters** link.
On the parameters, take a look on "**Safety standards**" section.



Enable these features enforce SMTP senders to be compliance with the SMTP protocol, this force remote service to be real SMTP server.

Disable VRFY command:

The VRFY command can lead to a remote attacker gaining the first and last name registered to any given email account.
This can aid an attacker in social engineering attack.

Reject unknown client hostname:

Reject the client when:

- The client IP address=name mapping fails,
- The name=address mapping fails,
- The name=address mapping does not match the client IP address

Reject unknown reverse client hostname

Reject the SMTP connection when the client IP address has no address=name mapping.
This is a weaker restriction than the reject unknown client hostname rule, which requires not only that the address=name and name=address mappings exist, but also that the two mappings reproduce the client IP address

Reject unknown sender domain

Reject the request when the SMTP service is not final destination for the sender address, and the MAIL FROM address has no DNS or MX record, or when it has a malformed MX record such as a record with a zero-length MX hostname

Reject invalid hostname

Reject the request when the client has a bad hostname syntax

Reject non fqdn sender

Reject the request when the MAIL FROM address is not in fully-qualified domain form, as required by the RFC
This specifies the response code to rejected requests (default: 504)

Enforce restrictions in the HELO

If enabled, the SMTP service will force to correctly send the HELO command and reject if the hostname is not in fully-qualified domain or address literal form or the hostname has no DNS A or MX record

Reject forged emails:

Reject emails that pretend to be sent from your domains but not authenticated and not listed in your network list

Enable Generic rDNS Clients check:

this feature rejects generic reverse DNS patterns covering a large section of ISPs in the US, Canada, Europe, and elsewhere more than 1.600 patterns will try to block mails from computers trying to send mails behind Public ISPs

Reject Internal and External non-existent domains:

Domains with no DNS A or MX record are rejected

Reject senders' domains not listed in local database:

If you turn on this feature **only internals domains are allowed to send mails through this server**.
This means you turn this server to an outgoing mail server only because senders Internet domains such has gmail.com, hotmail. * or yahoo. * will not allowed to send email to this server

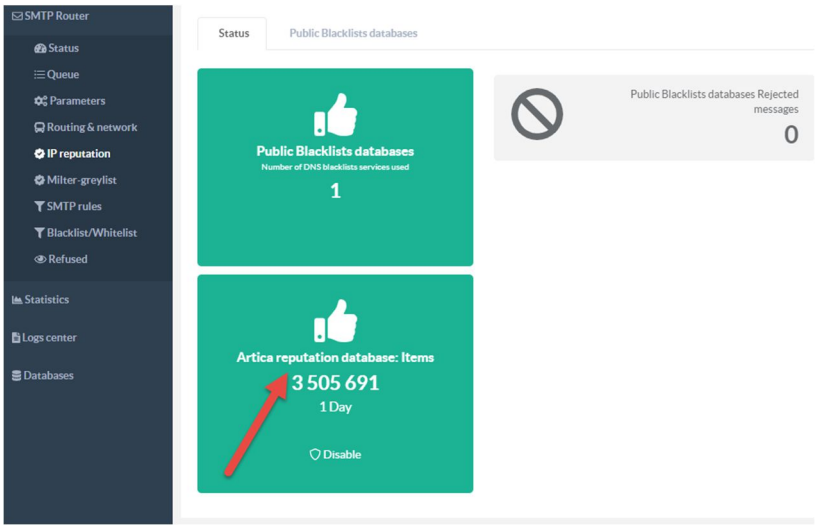
IP REPUTATION.

If your server is in front of internet, using a reputation database increase dramatically the anti-spam rate and decrease the usage of "content filtering".
An IP reputation database (aka RBL, DNSBL) is a cloud server that stores a list of blacklisted IP addresses.
These IP addresses are known to send SPAMs.
If a sender IP address is listed on these databases, the SMTP connection will be automatically refused.

Use the Artica reputation database:

The Artica reputation database is available with an Enterprise License Edition. It allows you to query a database that stores more than 4.000.000 blacklisted IP addresses and 100.000 whitelisted IP addresses.

To use the Artica reputation database, on the left menu choose "**SMTP Router**" and **IP Reputation**.
On the status page, click on the "**Enable**" in the "**Artica reputation database**" widget.



Public Blacklists databases.

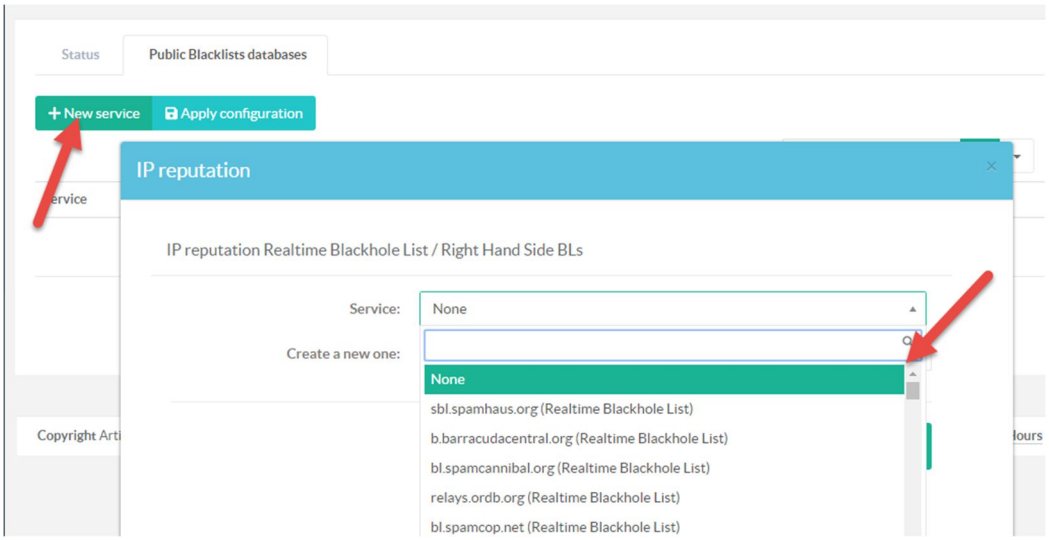
There is a little difference between Public Blacklists databases and Artica reputation database. Public Blacklists databases just offer "Blacklisting" as Artica reputation database leads whitelisting too.

Public Blacklists databases are free of charge databases (RBLs and DNSBLs) available on Internet.
You can use several services your server can query to detects if an SMTP sender is blacklisted or not.

On the IP reputation section, select the "**Public Blacklists databases**" tab

To add a new public service, click on "**New service**"

You can select a pre-defined service in the drop-down list or add your own service using the "**Create a new one**" field.



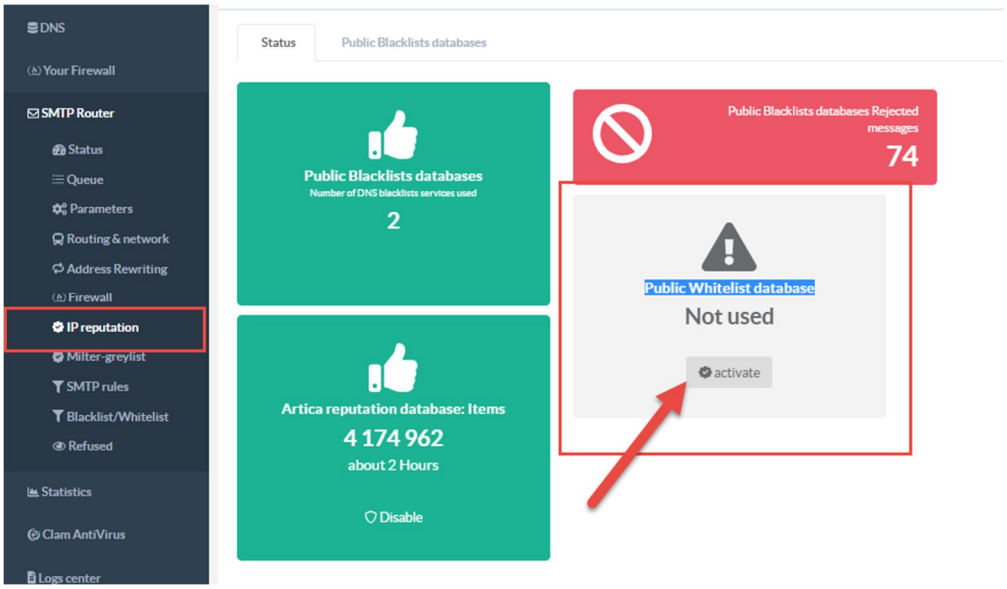
Public Whitelist database

This feature allows Artica server to query dnswl.org.
This organization is active in the anti-spam community.
The editors and administrators of dnswl.org data and systems are located in the UK, the US, Germany, Austria and Switzerland. Former active members came from Sweden, Finland, France, Netherlands, and had various contributors from an even more diverse set of geography.

It maintains a database of IP addresses (net ranges) which are grouped into "DNSWL Records" (identified by a DNSWL Id, which is just an arbitrary number). This data is maintained through a combination of manual and automated actions.

Basically, the DNSWL database stores only "**good SMTP servers**" and claim to **avoid false positives from public blacklists databases**.

To enable the use of DNSWL, on the IP reputation section, click on Activate on the grey "**Public Whitelist database**" section.

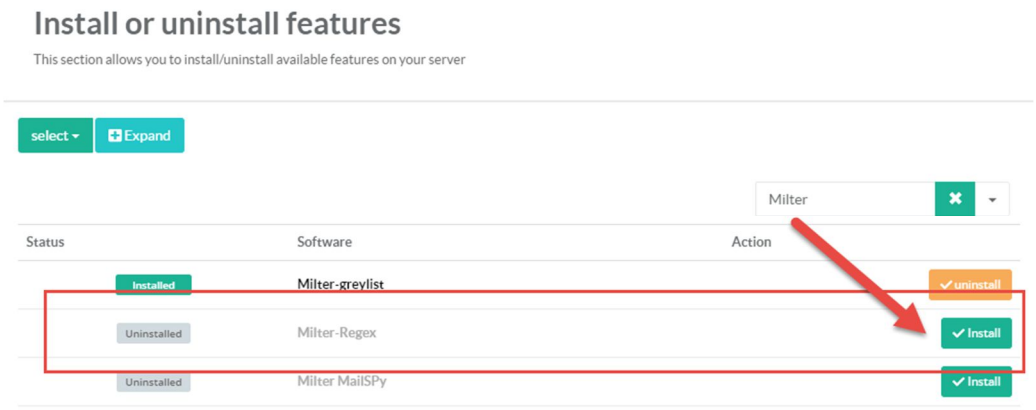


THE MILTER-REGEX MODULE FOR BLACKLISTING PERFORMANCE.

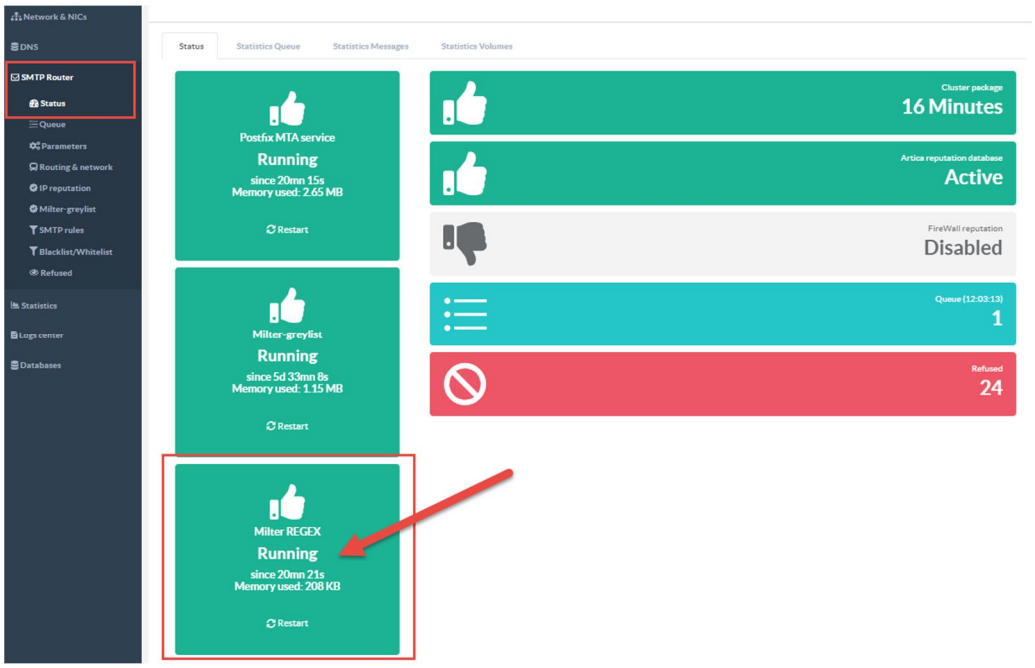
Sometimes you need to blacklist the sender email address or some words in the subject.
The blacklist reputation cannot deny everything came from office365, Gmail, Yahoo and other large ISP that provides free mail accounts.

In this case, you need to trust the sender IP address but deny the sender.
Spammers usually **use sequences on the mail from address** for example johnspamer234@gmail.com, johnspamer456@gmail.com.
The milter-regex module will be able to catch these sequences because it matches sender email addresses using regular expressions.
In this case, johnspamer234@gmail.com will be denied using johnspamer[0-9]+@gmail\.com.
This module is designed to scan a large list of rules using a minimal memory/CPU footprint.

On the **Features** section, in the search field, find the entry "**Milter**"
Click on the Install button on the "**Milter-regex**" row.



After installing the milter-regex module, you should see on the SMTP Router/Status the status of the milter-regex service.



In the Blacklist and whitelist rules you can create a rule with 3 new items:

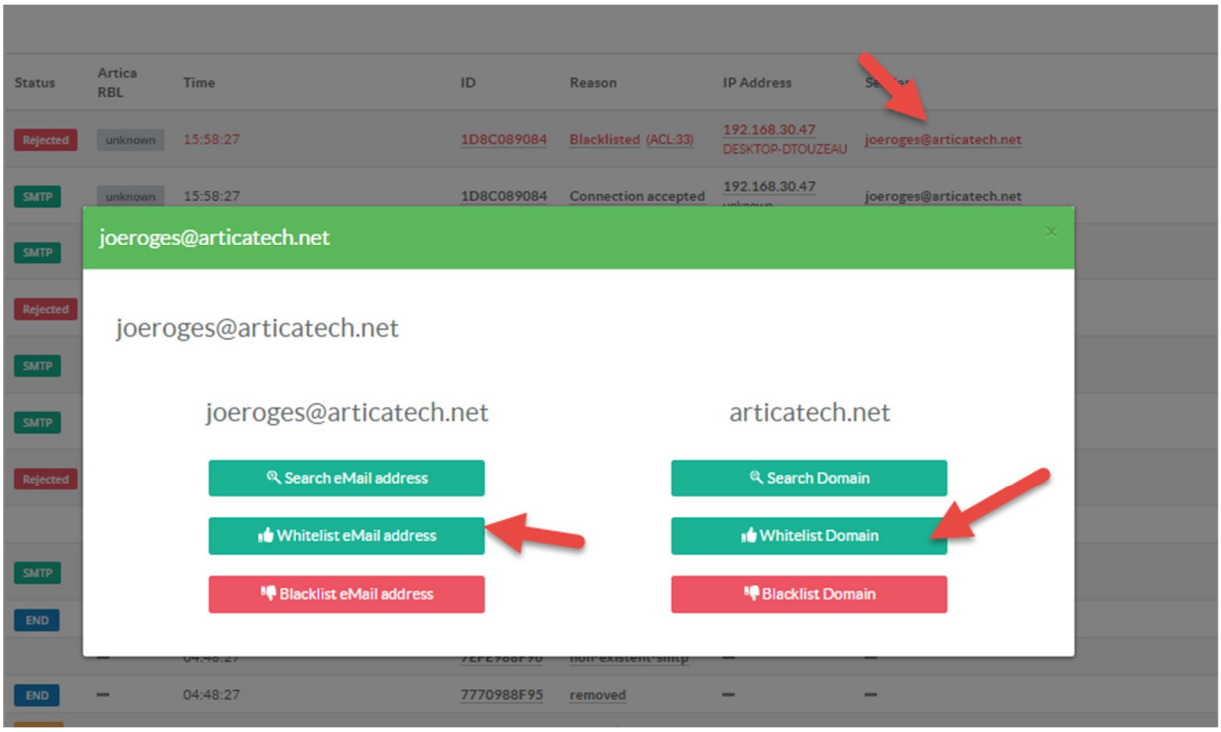
- **Sender: Regular expression**
- **Subject: Regular expression,**
- **Body: Regular expression**

BLACKLISTS AND WHITELISTS RULES

Blacklists rules and Whitelists rules are designed to refuse or allow any SMTP transaction from specifics items.

Basically, you can fill automatically this list from the **SMTP transactions list**

When clicking on the sender email address in the SMTP transactions, you can deny or allow the sender email address or the sender domain address.

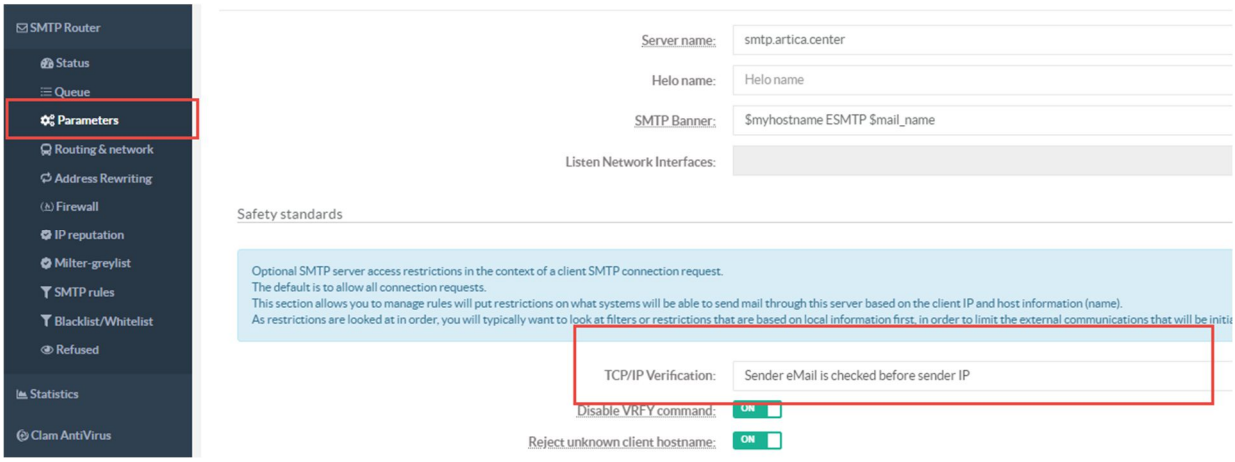


Whitelist checking

By default, the Artica SMTP server checks is a remote connection before any SMTP protocol task.
This means reverse hostname, reverse sender domain name, reputation servers are checked before checking sender eMail address
.
If you need to whitelist a sender eMail address that will not pass connection checking, the message will still be refused.

If you want to trust the sender eMail address, you need to reverse the IP checking method.
This way could be dangerous because the sender domain and eMail address can be easily compromise.

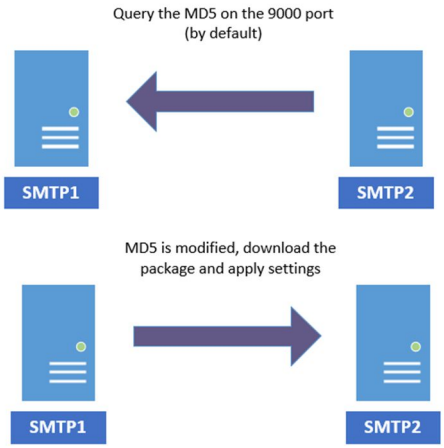
To reverse the IP checking methods, go to "**SMTP router**" and "**Parameters**" section.
Under "Safety standards", switch **TCP/IP verification** dropdown list to "**Sender eMail is checked before sender IP**"



In this case, whitelisted eMails will not be checked against IP addresses and messages will pass all tests.

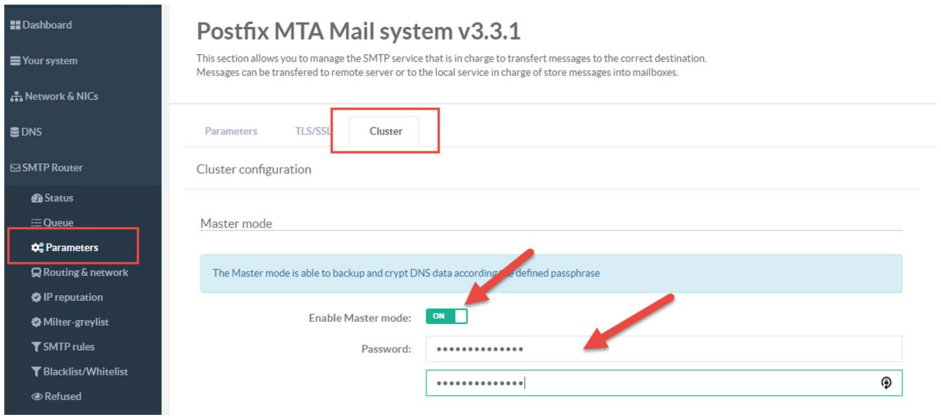
CLUSTER CONFIGURATION.

Cluster configuration allows a slave SMTP server to replicate configurations from a master server.
When administrator modify a parameter on the master, the master create a configuration package with an index file that stores the MD5 of the parameters.
The slave pool periodically the MD5 configuration package to see if there are changes.
If the MD5 is modified, then the slave download the package and apply the whole settings.

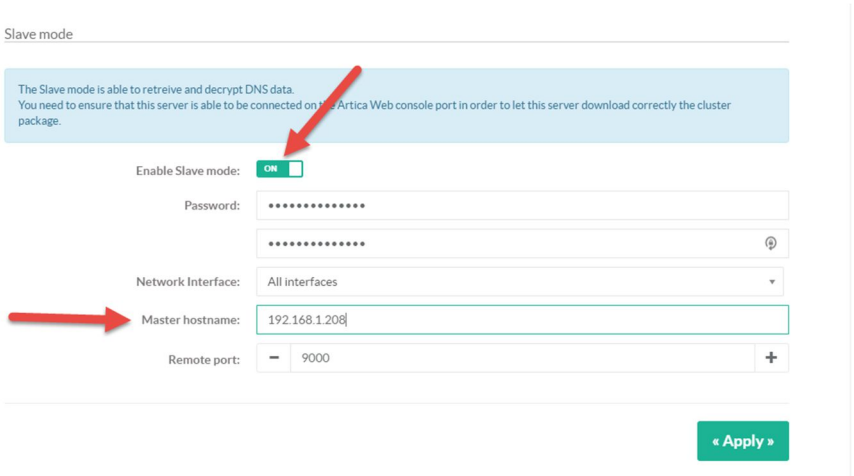


Replication is made through the Artica Web interface (SSL).
The replication package is encrypted with a defined password.

On the Artica server as "**Master server**", select "**SMTP Router**" and "**Parameters**" on the left menu.
Choose "**Cluster**" tab.
Turn on the "**Enable Master mode**"Set a **password** to encrypt the replication package.

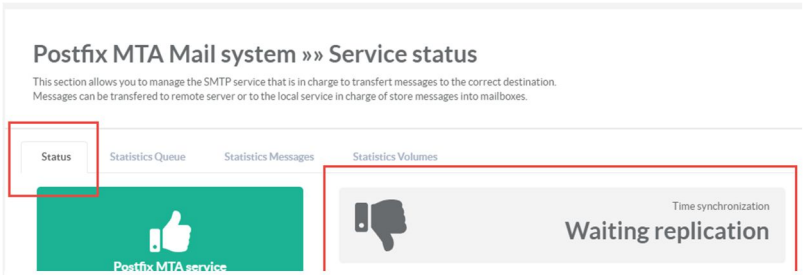


On the **Artica slave**, select "**SMTP Router**" and "**Parameters**" on the left menu.
Choose "**Cluster**" tab.
Turn on the "**Enable Slave mode**"
Set a **password** to decrypt the replication package (the same defined on the master)
Network Interface: If you have several Network interfaces, choose the right one that allow Artica to reach the master.
Master hostname: Set the address of the master server.
Remote port: Set the Web Artica interface port (default 9000).

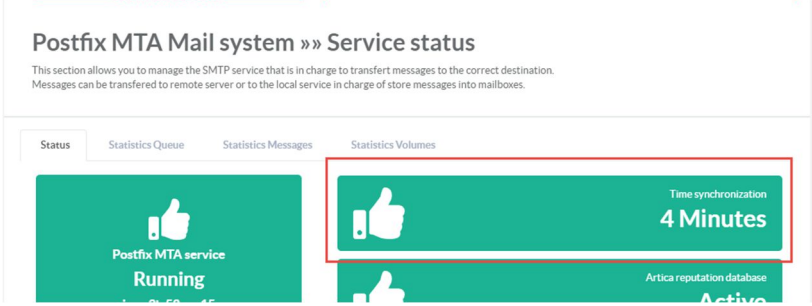


On the Slave, select "**SMTP Router**" and "**Status**" on the left menu.

You should see "**Waiting replication**" status.
This means the slave wait the schedule to synchronize data from the master.



Wait several times (5 minutes), you should see the synchronization delay

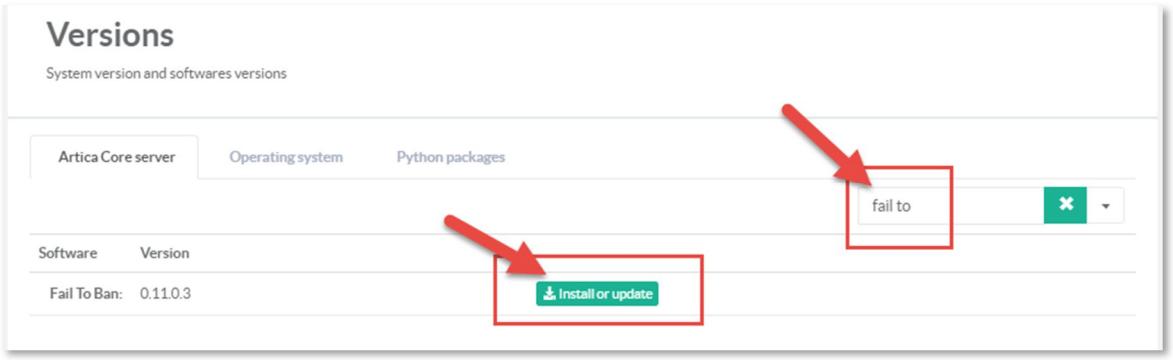


AUTOMATICALLY BAN IP IN FIREWALL BASED ON EVENTS.

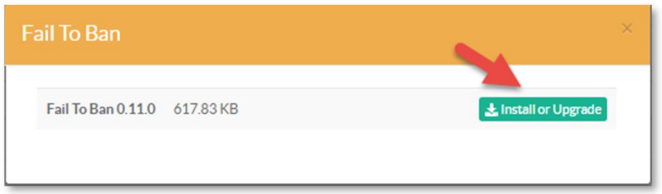
Many spammers did not check that your server refuse connections according to enabled filters.
You have the possibility to directly ban remote addresses during a defined period when the remote IP address is refused multiple times.
The service that is in charge of this feature is called "Fail2ban" .

Install the latest version

- ✓ On the Left menu, choose "**Your System**" and "**Versions**" on left menu.
- ✓ On the search field, type "Fai To"
- ✓ Click on **Install or update** button.

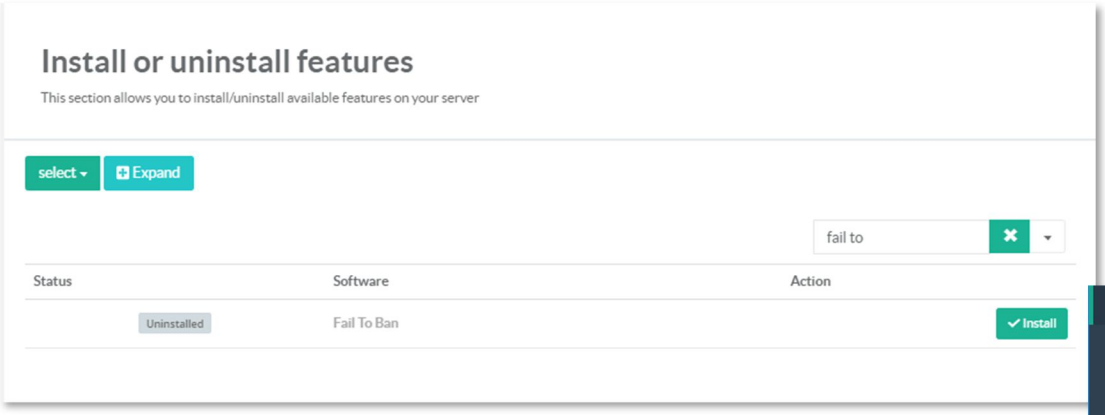


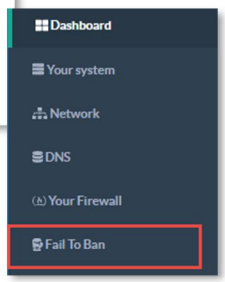
Click on "**Install or Upgrade**" on the desired version.



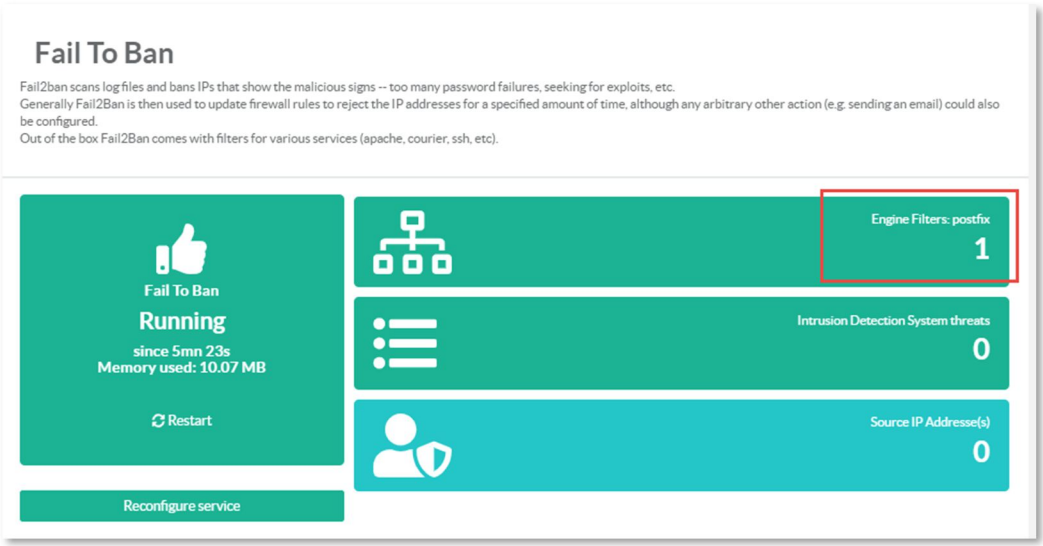
Install the Fail To Ban service

On the "**Features**" section search the entry "**fail to**" and click on "**Install**" button on the "**Fail To Ban**" row.





- ✓ In the left menu, you will see the "Fail To ban" menu entry after the installation.
- ✓ In the Fail To ban dashboard, you should see at least 1 Engine in the status.



- ✓ Basically you did not have to set up something, the service is automatically defined and set up in order to protect your SMTP service.

SECURE OUTGOING MESSAGES WITH SPF, DKIM AND DMARC

Use SPF with DKIM and DMARC

Along with SPF, we recommend setting up **DomainKeys Identified Mail** (DKIM) and **Domain-based Message Authentication**, Reporting & Conformance (DMARC).

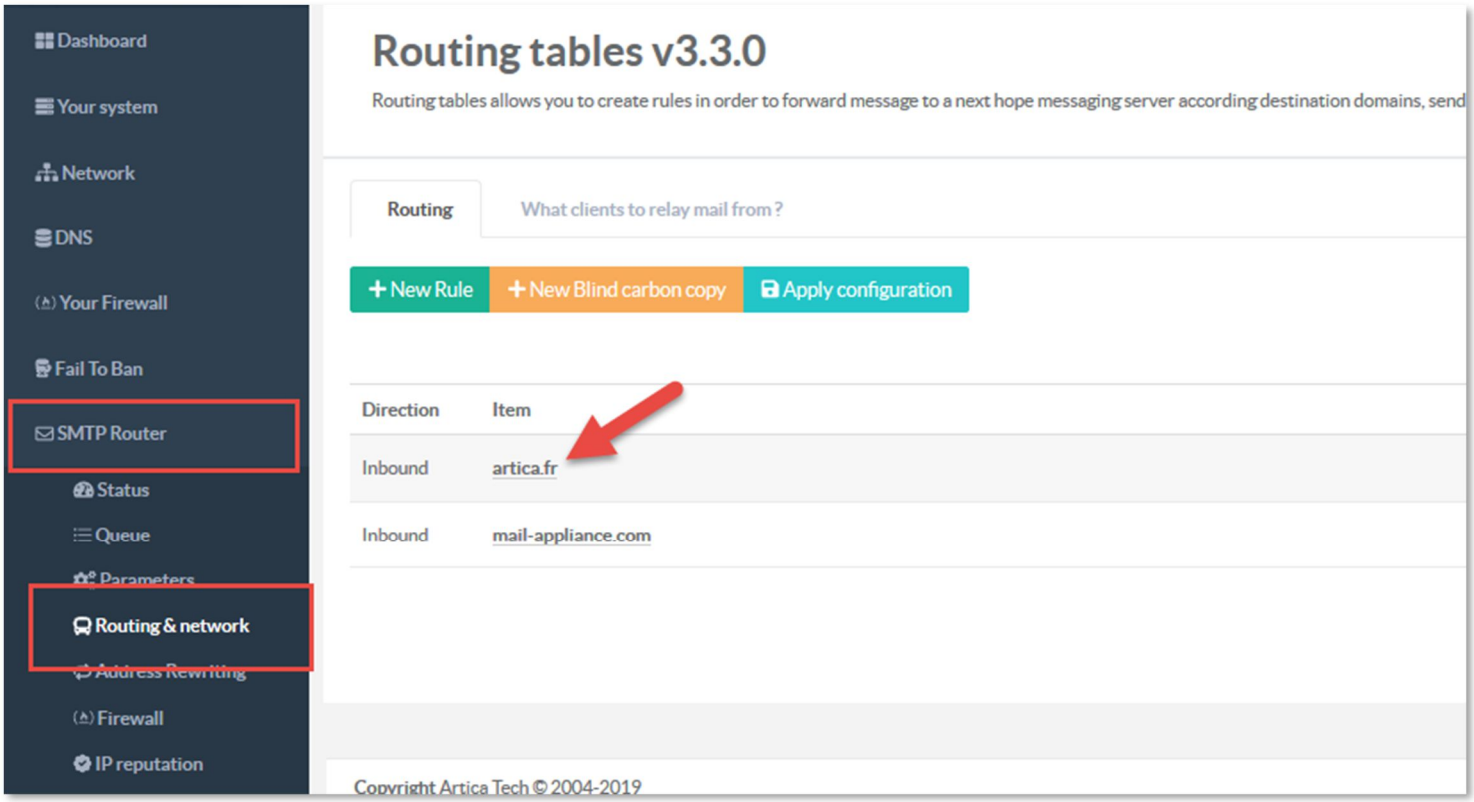
- SPF validates the domains that can send messages.
- DKIM verifies that message content is authentic and not changed.
- DMARC specifies how your domain handles suspicious emails that it gets.

SPF DNS Record

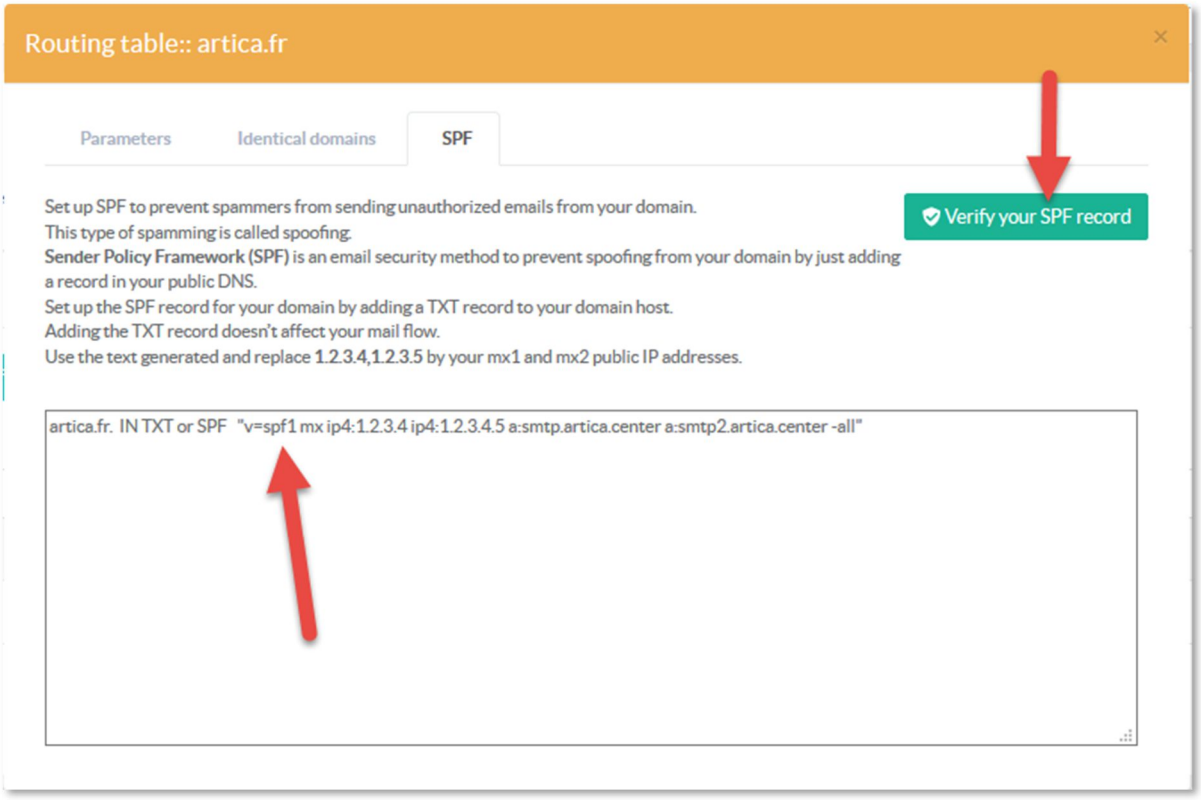
Create an SPF record for your domain

An SPF record is a TXT record that lists the mail servers that are allowed to send email from your domain.
Messages sent from a server that isn't the SPF record might be marked as spam.

On the left menu, choose “SMTP Router” and “Routing & Network”
On the table select the inbound domain.



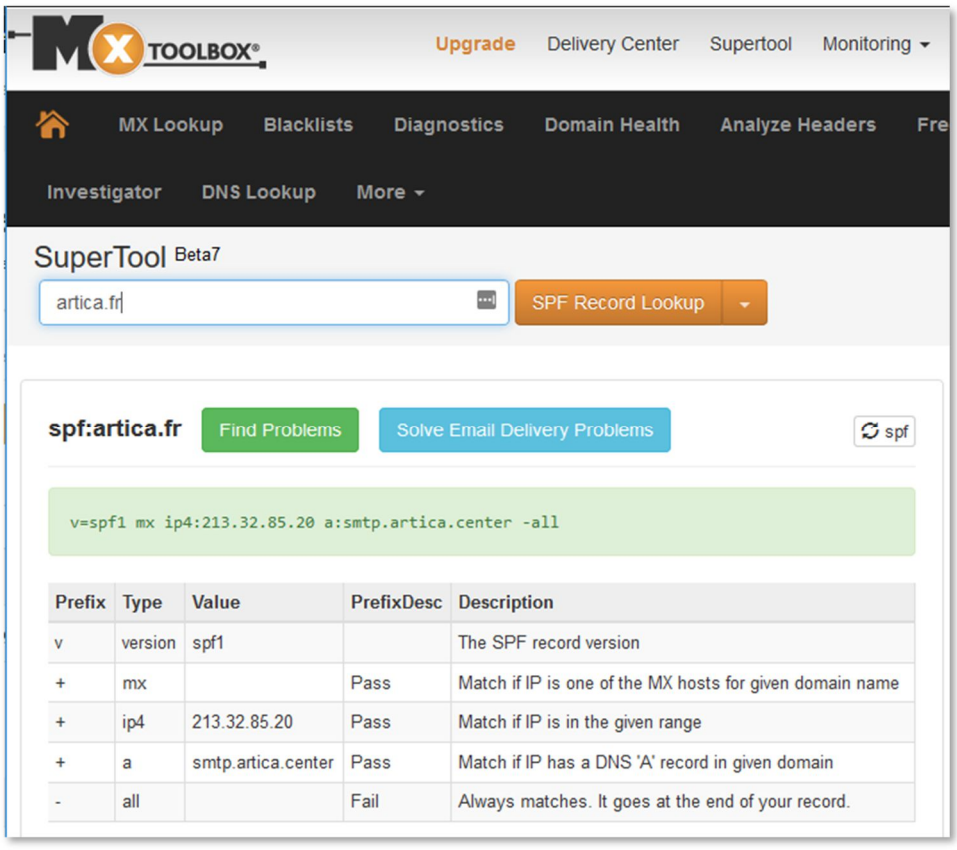
- Click on the **SPF** tab.
- The page shows you an example of SPF DNS entry you have to add in your public DNS server.
  Copy the content of the generated string, replace the 1.2.3.4,1.2.3.5 entries by the real public IP address of your MX1 and MX2 (if you have one)



- After adding your DNS entry, click on the "**Verify your SPF record**" to see if your SPF record is accepted by any SMTP server.

Example for BookMyName (it accepts only TXT record):

```
@ 28800 TXT "v=spf1 mx ip4:1.2.3.4 a:smtp.artica.center -all"
```



The mx Toolbox must display a green report for your SPF checks.

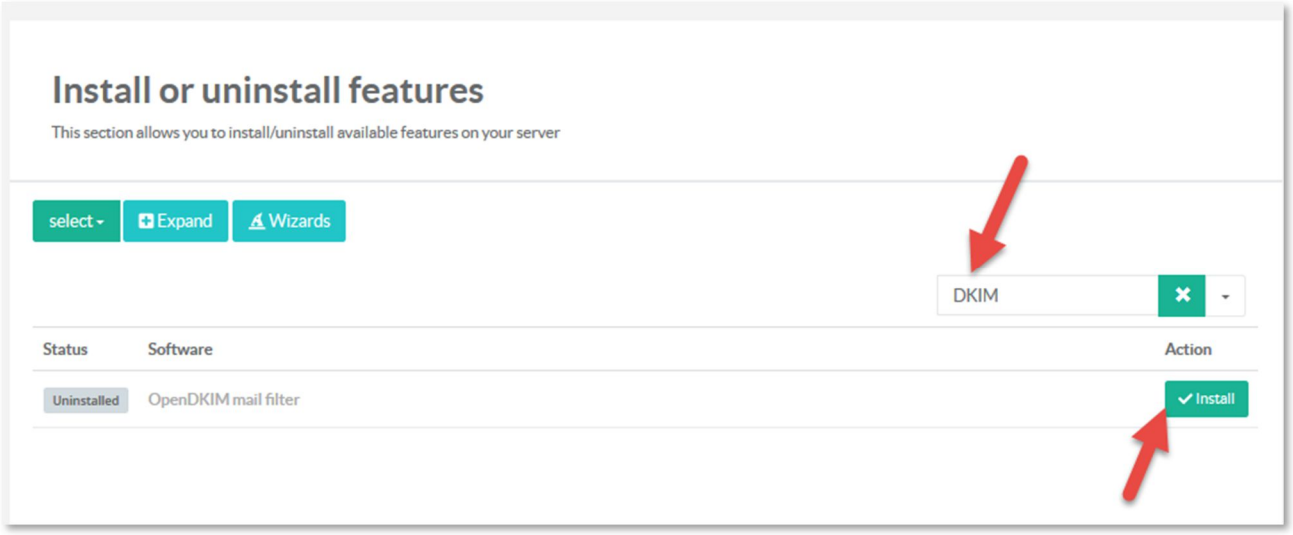
The OpenDKIM service

Use the DomainKeys Identified Mail (DKIM) standard to help prevent email spoofing on outgoing messages.

Email spoofing is when email content is changed to make the message appear from someone or somewhere other than the actual source. Spoofing is a common unauthorized use of email, so some email servers require DKIM to prevent email spoofing.

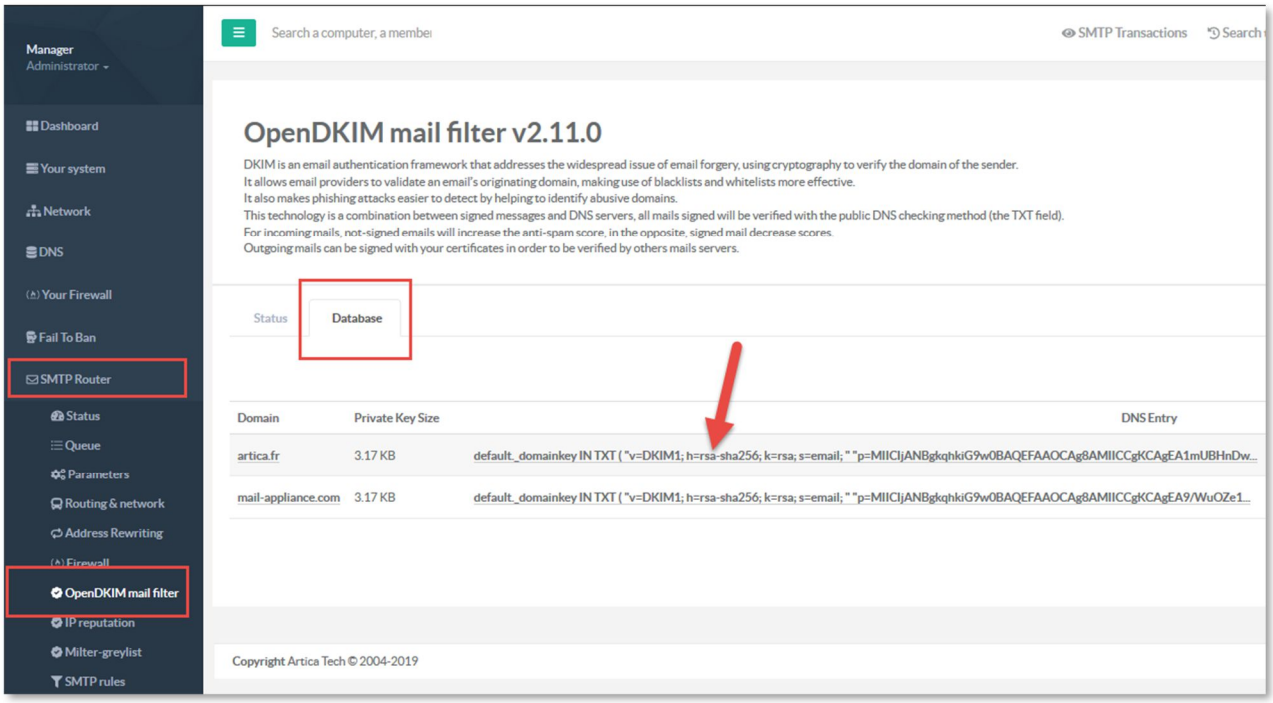
DKIM **adds an encrypted signature** to the **header** of all outgoing messages.
Email servers that get these messages use DKIM to decrypt the message header, and verify the message was not changed after it was sent.

On the left menu, click on **Your System** and **Features** section.
On the search field, type **DKIM**
Click on install button on the OpenDKIM mail filter row



- After installing the OpenDKIM service, all your domains will be signed with a DKIM Key.

- On the left menu, go to **SMTP router / OpenDKIM mail filter**
- Select **Database** tab.
- The section lists all internals domains in order to display the generated DKIM Private key and the DNS entry you should add to your Public DNS server.
- Click on a DNS entry on one of domains.



- A layer displays the data you should add in your public DNS.

- There are 2 forms, the top section is for Bind method and the bottom one is for BookMyName method.
- Copy and past the data into your Public DNS server for each domain in the list.

The DMARC DNS record

DMARC is built upon two other authentication protocols: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

You should have SPF and DKIM on your Envelope From and Friendly From domains before proceeding with DMARC.

Identify email accounts to receive DMARC reports

Through DMARC, you will receive aggregate and forensic (message level) reports daily.
Designate the email account(s) where you want to receive these reports.
You may want to use two separate accounts, as you could get inundated with the data.

DMARC reports are very difficult to parse because they are provided in raw format.
Partnering with a company like Return Path can help you and your team make sense of them

Learn the DMARC tags

DMARC tags are the language of the DMARC standard.
They tell the email receiver (1) to check for DMARC and (2) what to do with messages that fail DMARC authentication.

There are many DMARC tags available, but you do not have to use them all. In fact, we recommend keeping it simple. Focus on the

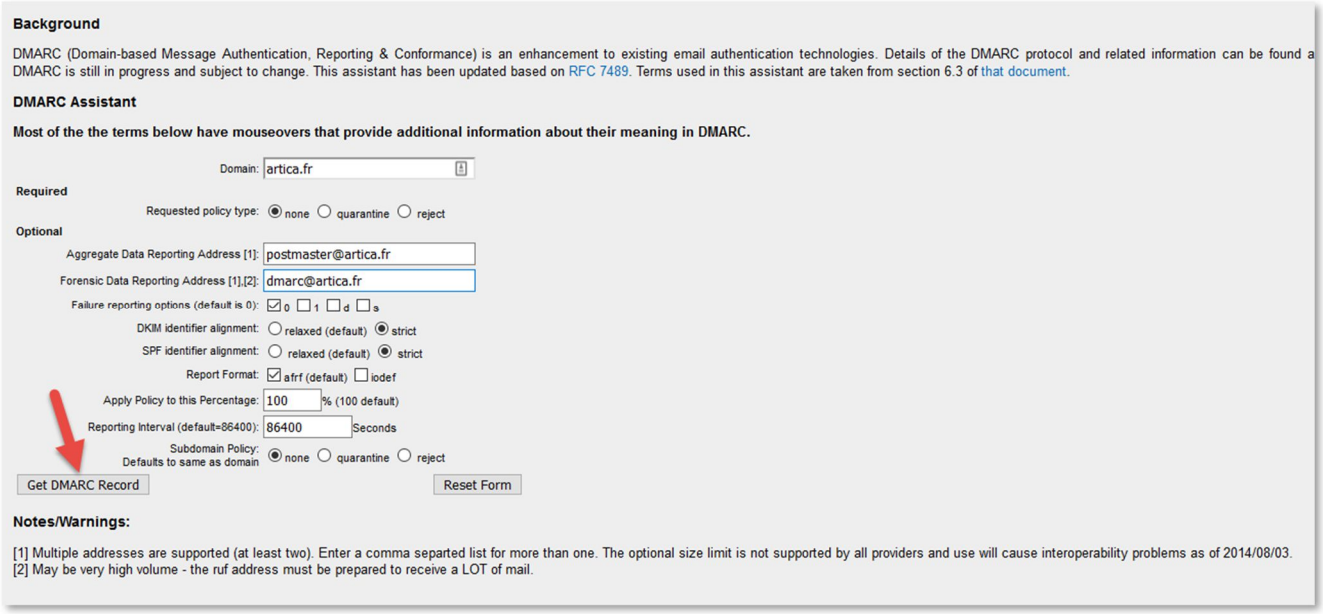
```
v=, p=, fo=, rua, and ruf
```

Generate your DMARC record with DMARC Creation Wizard

Using a DMARC Creation Wizard, (https://www.kitterman.com/dmarc/assistant.html) generate a DMARC text record in your DNS for each sending domain.
Set the mail receiver policy to "none," indicating DMARC's "monitor" mode.

With DMARC in monitor mode, you can gather the information on your entire email ecosystem, including who is sending email on behalf of your brand, what emails are getting delivered, and what emails are not.

Request to receive the daily aggregate and forensic reports by specifying your email address in the rua tag and the ruf tag, respectively.
Use the email address(es) you identified in step three above.



Your record should look something like this:

```
_dmarc.artica.fr TXT "v=DMARC1; p=none; rua=mailto:postmaster@artica.fr; ruf=mailto:dmarc@artica.fr; fo=0;
adkim=s; aspf=s; pct=100; rf=afrf; ri=86400; sp=none"
```

Now, Add the generated entry into your public DNS server.

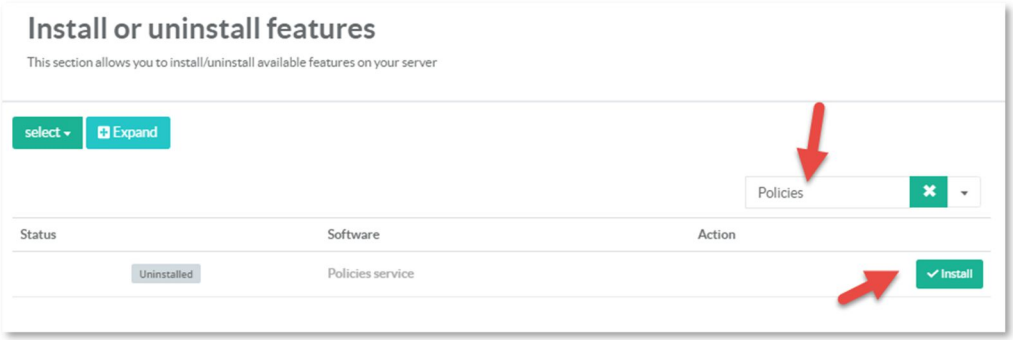
THE POLICIES SERVICE (ANTI-SPAM, ANTIVIRUS…)

The Policies service is a Milter that hook the MTA. It is designed to analyze content messages in order to find spam or malwares.
This service require a valid Corporate License.
It allows you to :

- ✓ Scan messages for Malwares.
- ✓ Scan messages for Anti-Spam.
- ✓ Perform backup messages in the fly.
- ✓ Add disclaimers in messages.
- ✓ Auto-compress messages

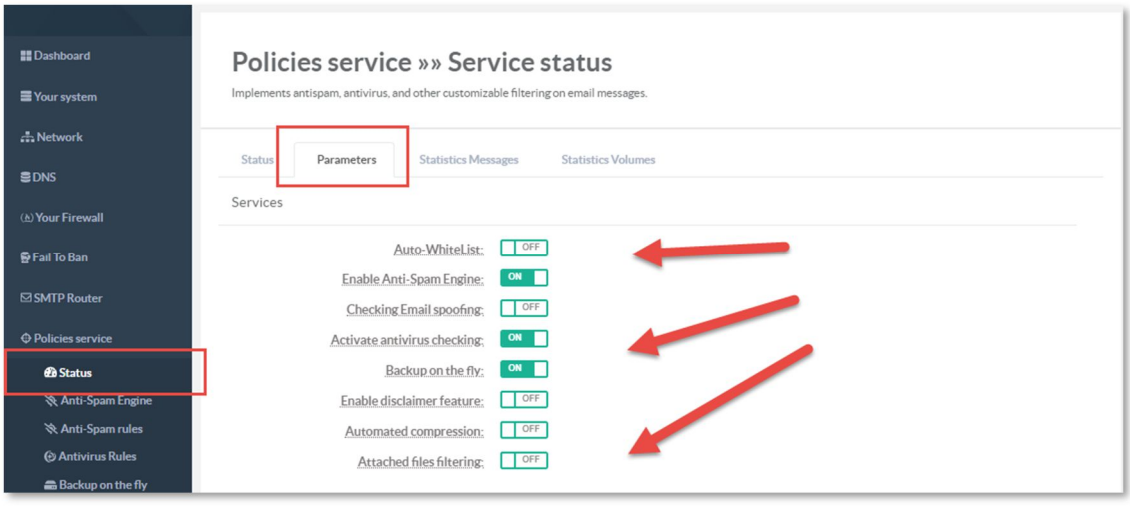
Install the Policies services.

- ✓ On the feature section, in the search field, type "**Policies**"
- ✓ Click on "**Install**" button under the "**Policies service**" row.



Enable SMTP content features.

- ✓ On the left menu, click on **Policies service** and **status**.
- ✓ Select the "**Parameters**" tab.

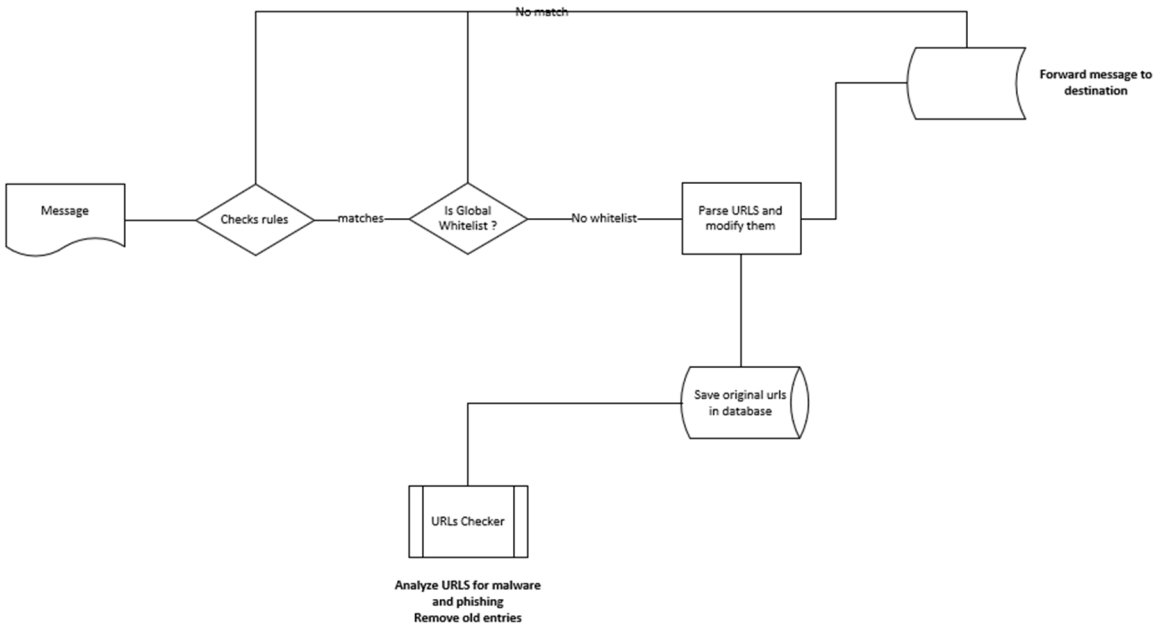


- ✓ **Auto-Whitelist**: Automatically add recipient email address to Whitelist database when your users send an eMail.
- ✓ **Enable Anti-Spam Engine**: Add the bayesien and scoring content Anti-spam engine.
- ✓ **Check eMail spoofing**: A foreign sender cannot use your internal domains to send eMail to your users.
- ✓ **Activate antivirus checking**: Scan message for malwares.
- ✓ **Backup on the fly**: Backup all messages that are forwarded by the SMP relay.
- ✓ **Enable disclaimer feature**: Allows you to add a disclaimer according SMTP rules.
- ✓ **Automated compression**: Allows the SMTP relay to zip compress attachments according SMTP rules.
- ✓ **Attached files filtering**: Remove unwanted files according files extensions.
- ✓ **URL Filtering**: Changes URLS in order to give time to detects phishing and malwares.

URL Filtering in SMTP messages

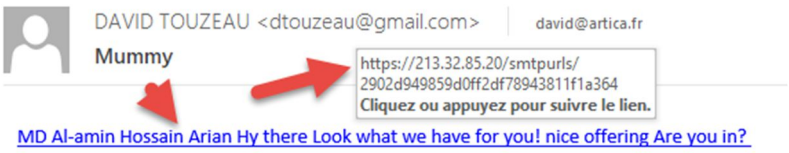
The URL filtering is a feature designed to change URLs in **inbound** messages in order to force users to use a web frontend before accessing to the real URL sended.

URL Filtering process:



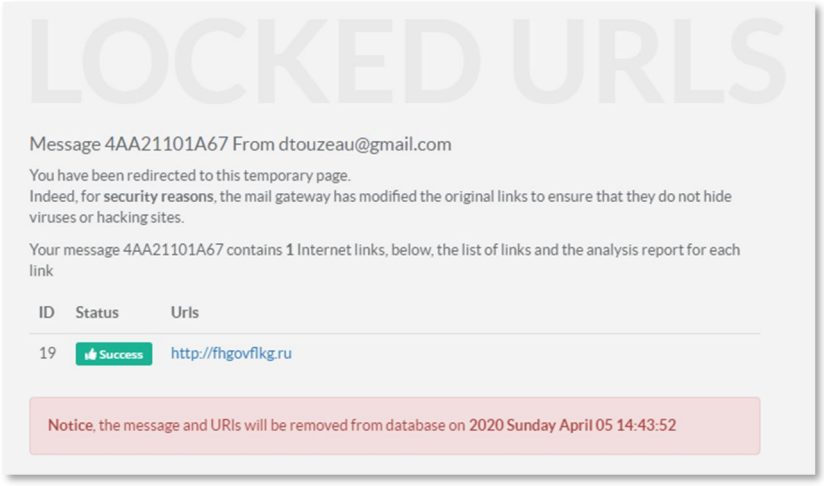
Objectives:

If a user click on a link inside a receive message



It will be redirected to a splash page that display results of URLs analysis
On the splash screen, user can:

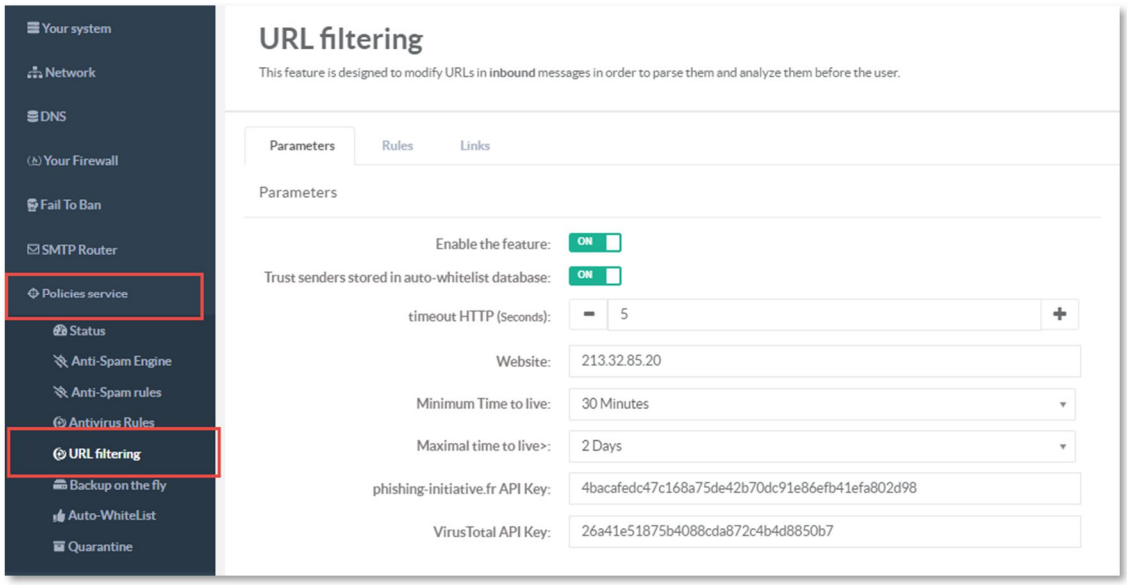
- Add the sender as trusted sender.
- Get the original message if not URLs are marked has phishing or malware.



If one link is a phishing site or a virus, the user will not be able to restore the message or click on links.

Enable Url Filtering

On the left menu, choose "**Policies service**, **URL filtering**"



- Turn on the "**Enable the feature**"

- **Trust senders stored in auto-whitelist…:**
  If the sender matches a rule stored in auto-whitelist database, then URLs will be not modified.
  The user will be able to trust sender in the splash screen too.

- **Timeout HTTP (seconds):**
  The process will try to get the final point of the URLs in order to get the final Content-Type of the Internet object.
  Define here the TimeOut in seconds the HTTP engine will use to be connected on the remote sites.

- **Website:**
  Define here the hostname (https mandatory) to access to the splash screen (the Artica Web Console).
  The best way is to turn Artica Web console on 443 port and set here only the hostname or IP address.
  If you keep the 9000 port of the Artica Web console, set 192.168.1.1:**9000** in the field

- **Minimum Time to live:**
  The time to wait before analysis the message, this time must help RBLs servers such as Virus Total or Artica Tech to add the phishing urls in databases.

- **Maximal Time to live:**
  When URLs are modified, Artica will store URLs and original message to the Artica database.
- After this period all data will be removed.

- **Phishing-initiative.fr API Key:**
  Give here the API key o the https://phishing-initiative.fr/ website.

- **Virus Total API Key:**
  Give here the API key o the *https://www.virustotal.com* website.

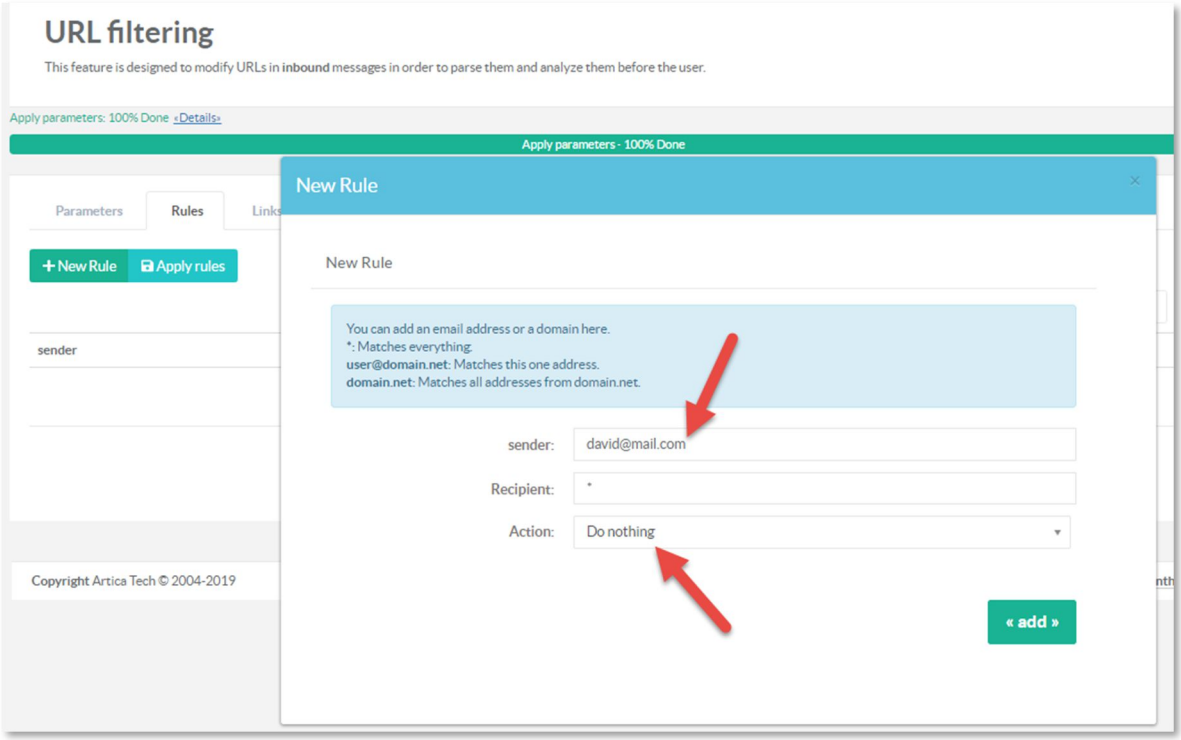
The rules section

The rule section allows you to enforce or whitelist a domain or a user to be or not pass through the URLs engine.

You can add an email address or a domain.

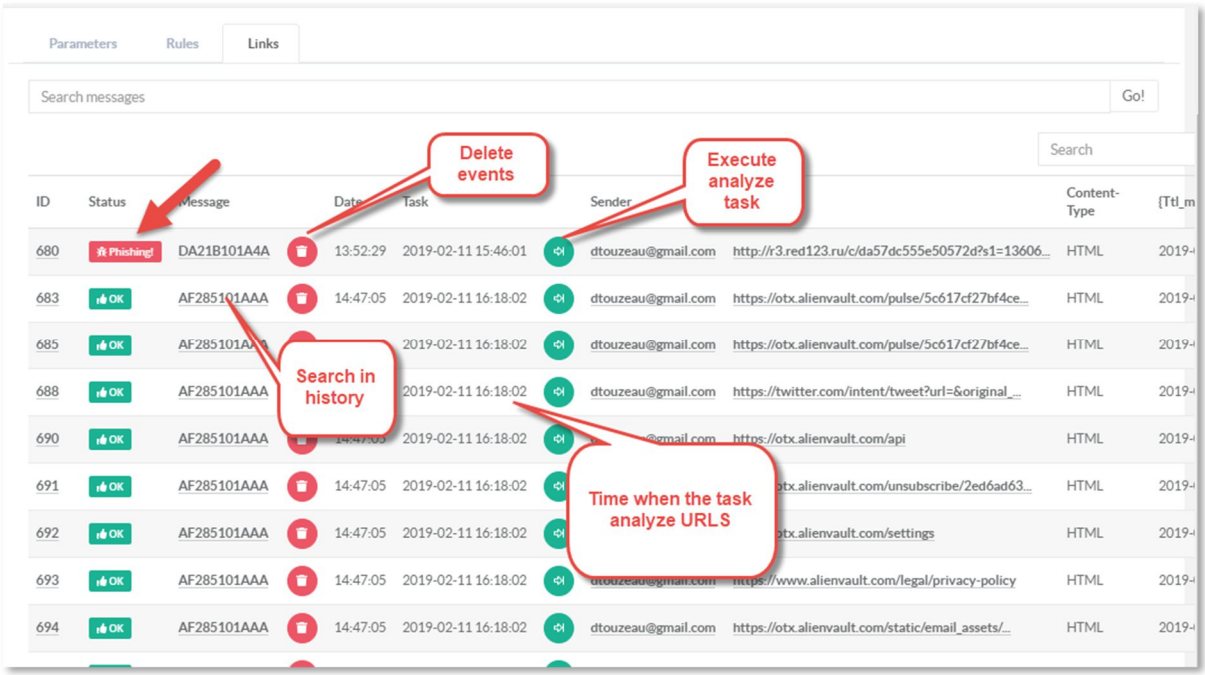
- ***:** Matches everything.
- **user@domain.net**: Matches this one address.
- **domain.net**: Matches all addresses from domain.net.

Action can be "**Do nothing**" (do not modify URLs) or "**Change URLs in messages**" (enforce the action even the sender is stored in auto-whitelist rules).



The Links section

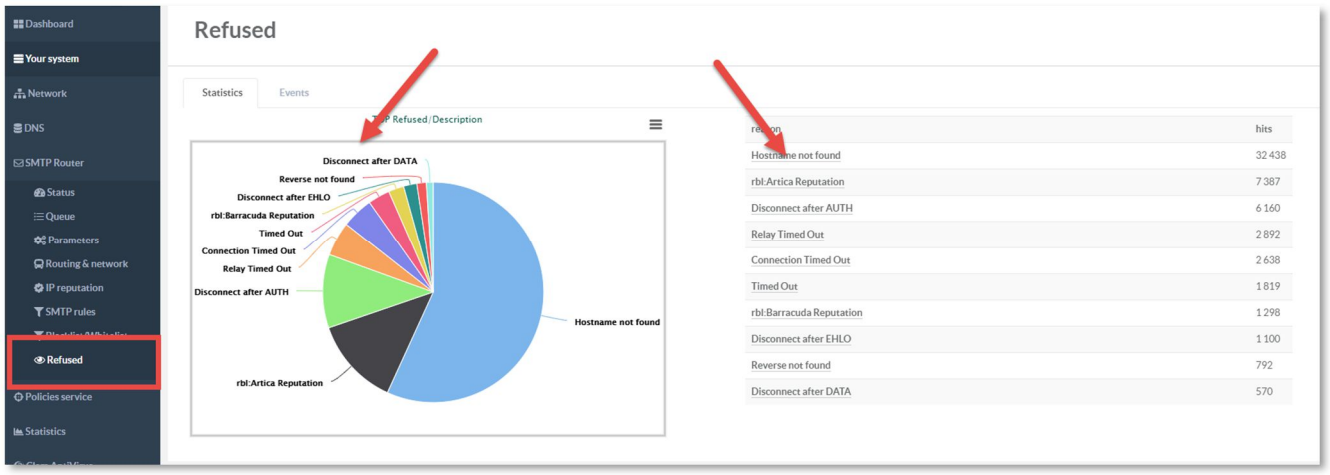
The links section allows you to display all scanned URLs and their status.



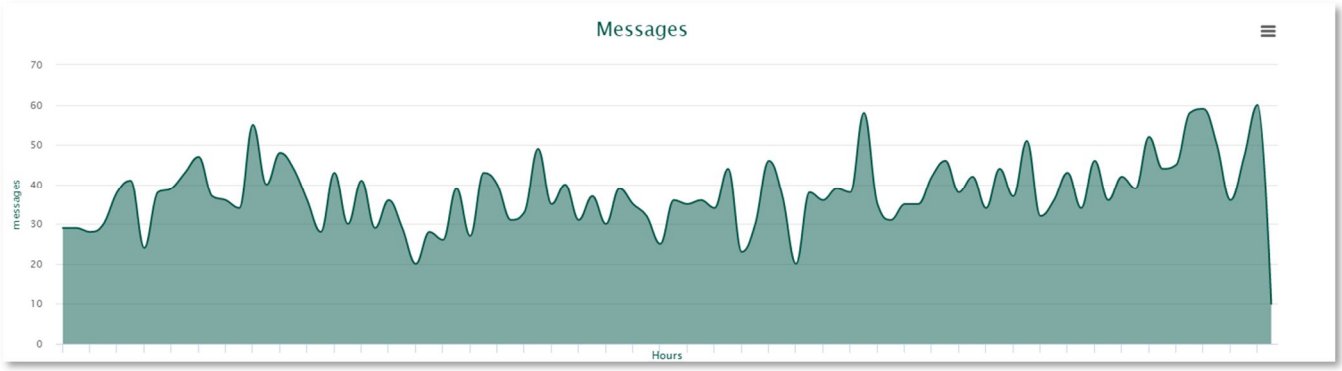
SMTP STATISTICS

Refused messages

- ✓ You can display graphs on refused messages in order to analyze your SMTP security rules.
- ✓ On the left menu, click on SMTP router and refused menu.
- ✓ The first tab allows you ti see a pie chart in the top 10 of blocked reason.
- ✓ On the right side, the table display the number of messages blocked.
- ✓ If you click on the link, you can display all messages that matches the specified blocked reason.



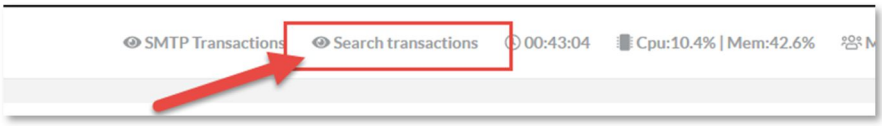
- ✓ You will see a chart that display blocked messages per hour for the current week



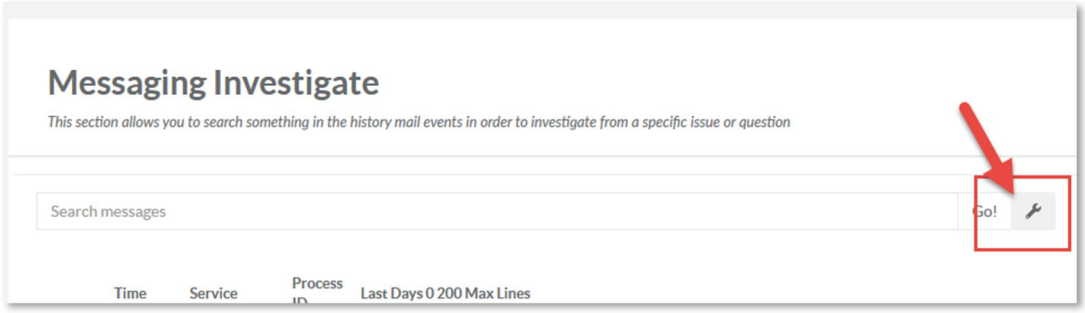
SMTP INVESTIGATION

Each day the SMTP events log is saved in the backup logs directory.
If you need to retreive the history of some SMTP transaction you can use the tool “Investgate”

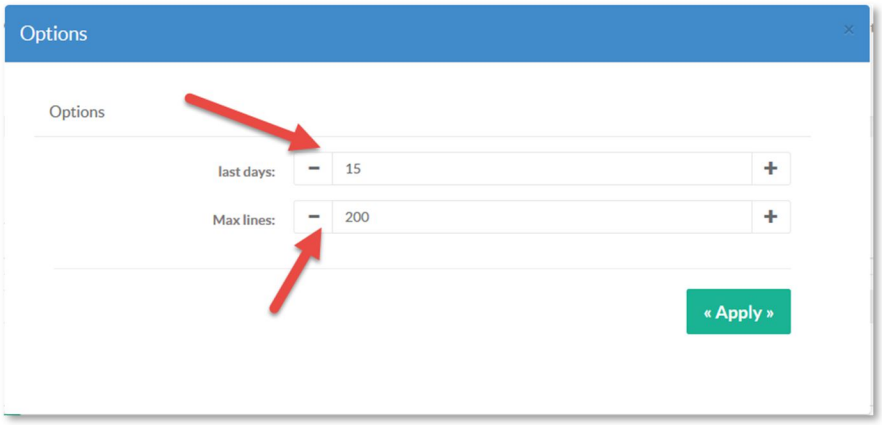
On the top menu, click on **Search transactions**.



Click on the settings icon on the search field



You can define in settings how many last days your search will be found
Define the max lines that will be disaplyed in the final search.

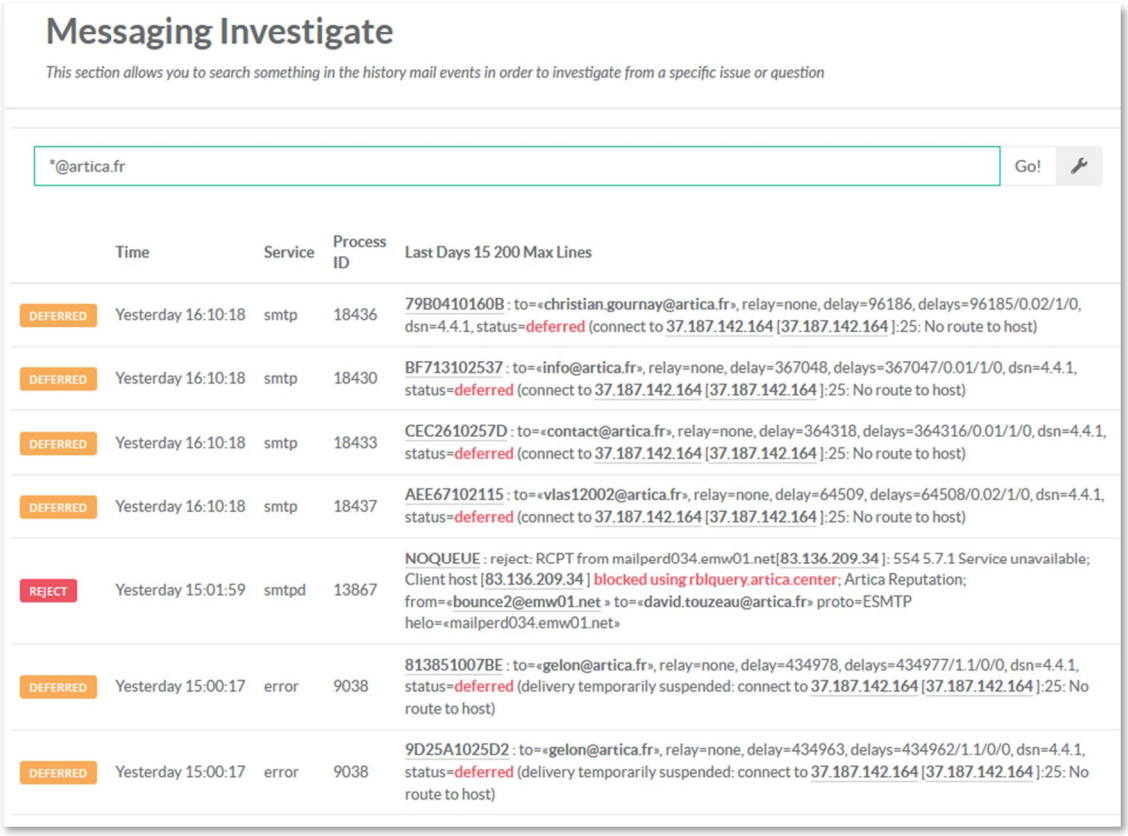


- ✓ In the search messages, put a string that you want to find in events.
- ✓ This should be a name, an email address, a domain…(the “*” character is supported)
- ✓ If you want to put regular expressions, use “**regex**” suffix

Examples:

```
dummy@domain.tld
@domain.tld
*.domain.tld
regex domain.[a-z]+
```

After run the query, a table is displayed and shows you all transactions that matches your search string..



Messaging Investigate

This section allows you to search something in the history mail events in order to investigate from a specific issue or question

*@artica.fr Go!

	Time	Service	Process ID	Last Days 15 200 Max Lines
DEFERRED	Yesterday 16:10:18	smtp	18436	79B0410160B : to=«christian.gournay@artica.fr», relay=none, delay=96186, delays=96185/0.02/1/0, dsn=4.4.1, status=deferred (connect to 37.187.142.164 [37.187.142.164]:25: No route to host)
DEFERRED	Yesterday 16:10:18	smtp	18430	BF713102537 : to=«info@artica.fr», relay=none, delay=367048, delays=367047/0.01/1/0, dsn=4.4.1, status=deferred (connect to 37.187.142.164 [37.187.142.164]:25: No route to host)
DEFERRED	Yesterday 16:10:18	smtp	18433	CEC2610257D : to=«contact@artica.fr», relay=none, delay=364318, delays=364316/0.01/1/0, dsn=4.4.1, status=deferred (connect to 37.187.142.164 [37.187.142.164]:25: No route to host)
DEFERRED	Yesterday 16:10:18	smtp	18437	AEE67102115 : to=«vlas12002@artica.fr», relay=none, delay=64509, delays=64508/0.02/1/0, dsn=4.4.1, status=deferred (connect to 37.187.142.164 [37.187.142.164]:25: No route to host)
REJECT	Yesterday 15:01:59	smtpd	13867	NOQUEUE : reject: RCPT from mailperd034.emw01.net[83.136.209.34]: 554 5.7.1 Service unavailable; Client host [83.136.209.34] blocked using rblquery.artica.center; Artica Reputation; from=«bounce2@emw01.net » to=«david.touzeau@artica.fr» proto=ESMTP helo=«mailperd034.emw01.net»
DEFERRED	Yesterday 15:00:17	error	9038	813851007BE : to=«gelon@artica.fr», relay=none, delay=434978, delays=434977/1.1/0/0, dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to 37.187.142.164 [37.187.142.164]:25: No route to host)
DEFERRED	Yesterday 15:00:17	error	9038	9D25A1025D2 : to=«gelon@artica.fr», relay=none, delay=434963, delays=434962/1.1/0/0, dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to 37.187.142.164 [37.187.142.164]:25: No route to host)

NOTIFICATIONS

- The MTA is able to send notifications to messaging team depends on different context.
- To manage notifications, go into SMTP **Router / Parameters**.
- Select **Postmaster / Template tab.**

The first part of the form allows you to set recipient / Senders of notifications

Postmaster:

The email address used to receive notifications.

Unknown Users:

If you want to relay messages for non-existent users (instead of refuse messages), set an email address.

Notifications Sender address:

The email address used to send notifications (eg: when an email is failed to be routed)
The sender address of postmaster notifications that are generated by the mail system
All mail to this address is silently discarded, in order to terminate mail bounce loops

eMail for sender notifications:

The sender address to use in address verification probes; prior the default was "postmaster"/
To avoid problems with address probes that are sent in response to address probes, the MTA server excludes the probe sender address from all SMTPD access blocks.
Specify an empty value or <> if you want to use the null sender address/
Beware, some sites reject mail from <>, even though RFCs require that such addresses be accepted

Bounce notice recipient:

The recipient of undeliverable mail that cannot be returned to the sender

Notifications error recipient:

The recipient of postmaster notifications about mail delivery problems that are caused by policy, resource problems, software problems or protocol errors

Notifications Delays recipient:

The recipient of postmaster notifications with the message headers of mail that cannot be delivered

Empty recipient address:

The recipient of mail addressed to the null address. The MAT does not accept such addresses in SMTP commands,
but they may still be created locally as the result of configuration or software error"

What trouble to report to the postmaster

You can define here notifications family that the MTA have to send to the **Notifications error recipient**

Undeliverable mail:

Send postmaster copies of undeliverable mail. If mail is undeliverable, a so-called single bounce message is sent, with a copy of the message that was not delivered. For privacy reasons, the postmaster copy of a single bounce message is truncated after the original message headers. If a single bounce message is undeliverable, the postmaster receives a double bounce message with a copy of the entire single bounce message

Double bounces:

Send double bounces to the postmaster

Policy:

Inform the postmaster of client requests that were rejected because of (UCE) policy restrictions.
The postmaster receives a transcript of the entire SMTP session

Protocol:

Inform the postmaster of protocol errors (client or server side) or attempts by a client to execute unimplemented commands.
The postmaster receives a transcript of the entire SMTP session

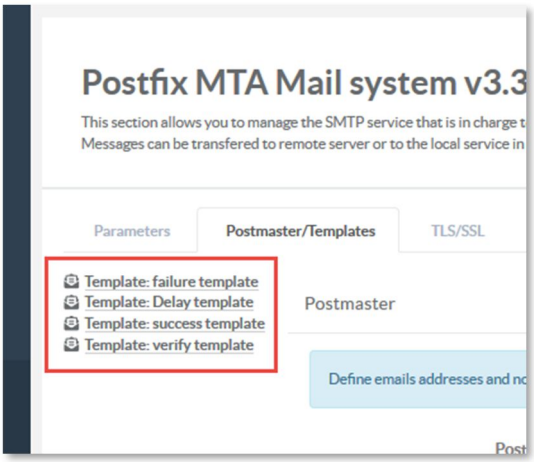
Resource problems:

Inform the postmaster of mail not delivered due to resource problems (for example, queue file write errors)

Software problems:

Inform the postmaster of mail not delivered due to software problems

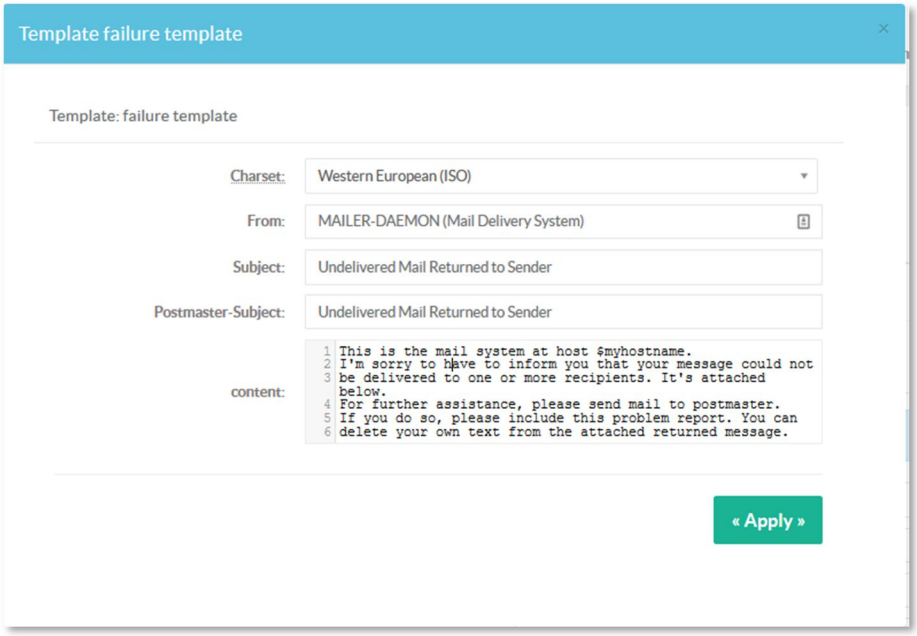
Notifications templates



On the left part of the form, you can personalize 4 notifications templates

On each template you can define:

- The Charset used by the notification.
- The From address
- The Subject of the notification.
- The content of the message



WORDPRESS ADMINISTRATION.

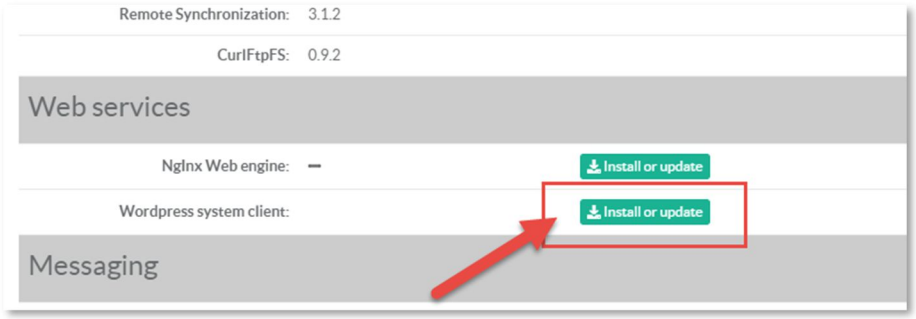
Artica is able to manage Wordpress web sites.
With Artica you are able to easily install/backup/restore Wordpress websites.

PREPARE ARTICA FOR WORDPRESS

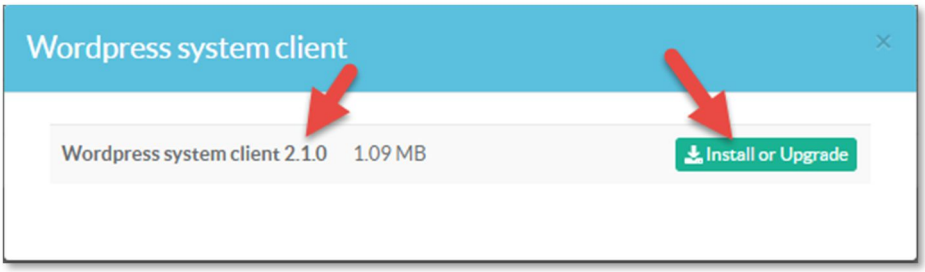
You need to install Wordpress system client, MySQL database, Nginx Web service and finally enable the Wordpress Artica feature

Install Wordpress system client

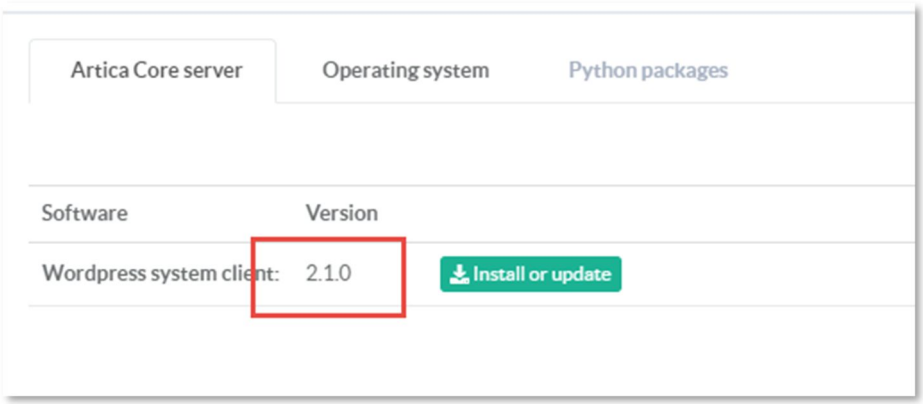
- On the left menu, go to **Your System/Versions**
- Search the item "**Wordpress**"
- Click on "**Install or update**" button on the Wordpress system client row



- Choose the latest version and click on **"Install or Upgrade**" button

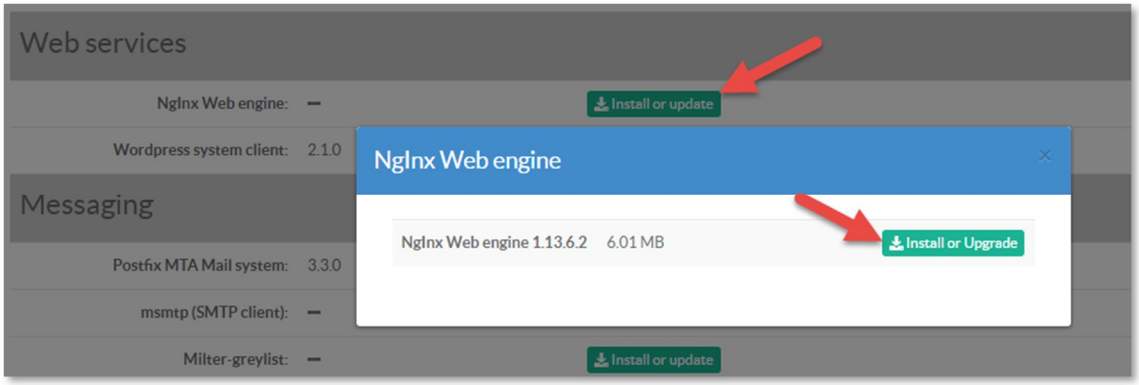


- You should see the version number in the Wordpress system client row

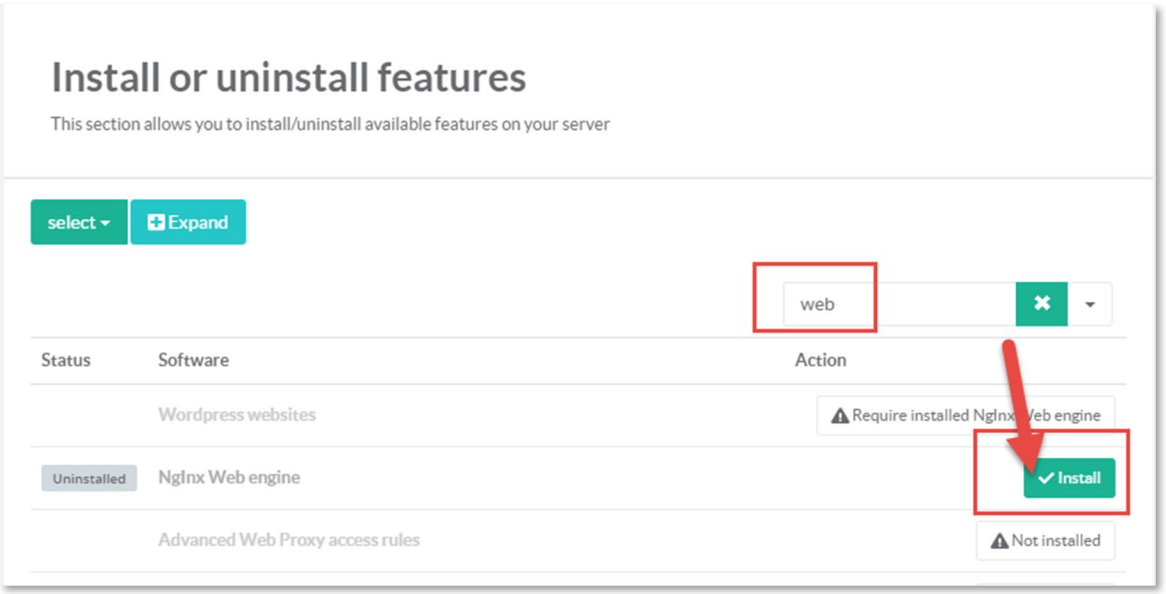


Install the NgInx Web engine

In the same way of the Wordpress client, checks the "**NgInx Web engine**" version and installation



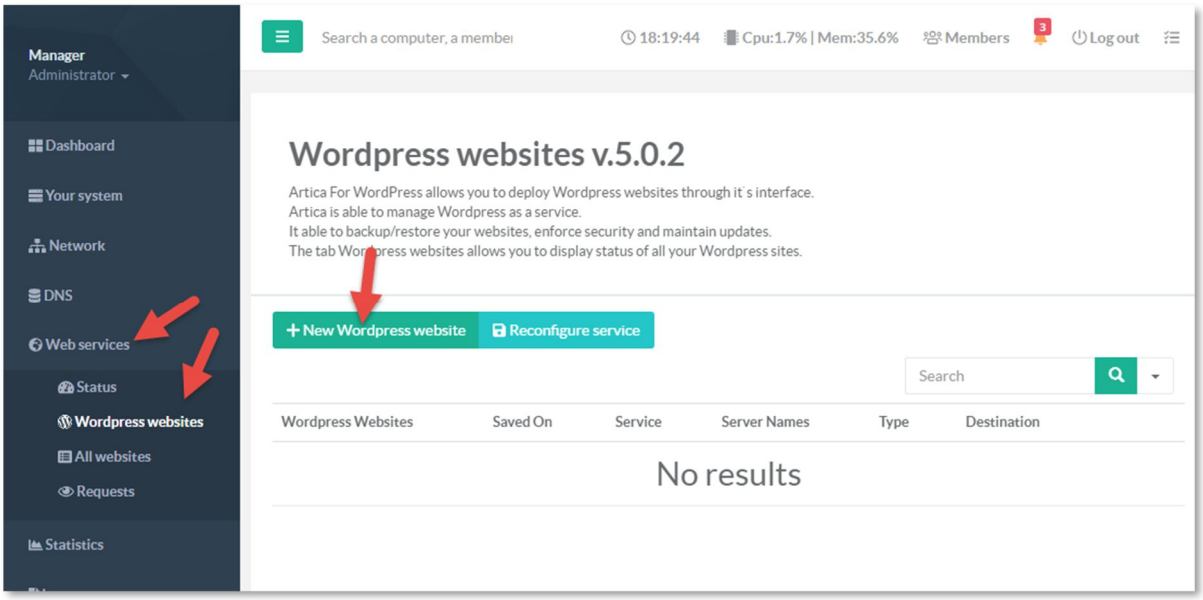
- On the left menu, go into Your **System/Features**
- On the search field, type the word "**web**"
- Click on "**Install**" On the "**Nginx Web engine**" row



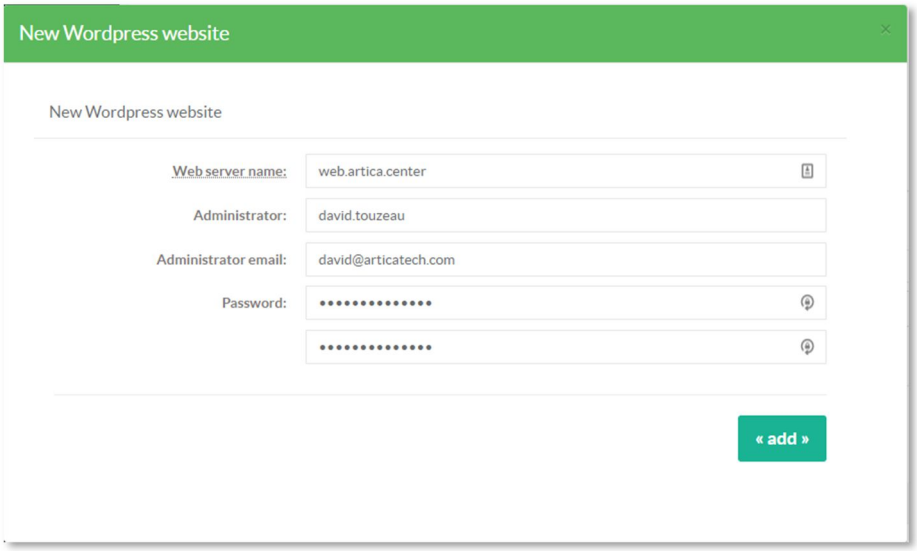
- Click on **Install** on the **Wordpress Websites** row

CREATE YOUR FIRST WORDPRESS WEBSITE

- On the left menu, go to **Web services / Wordpress websites**
- Click on the button "**New Wordpress website**"



- Set your web site name in Web server name field.
- Define the administrator of the new web site name.
- Set it's email in order to create certficate or notifications.



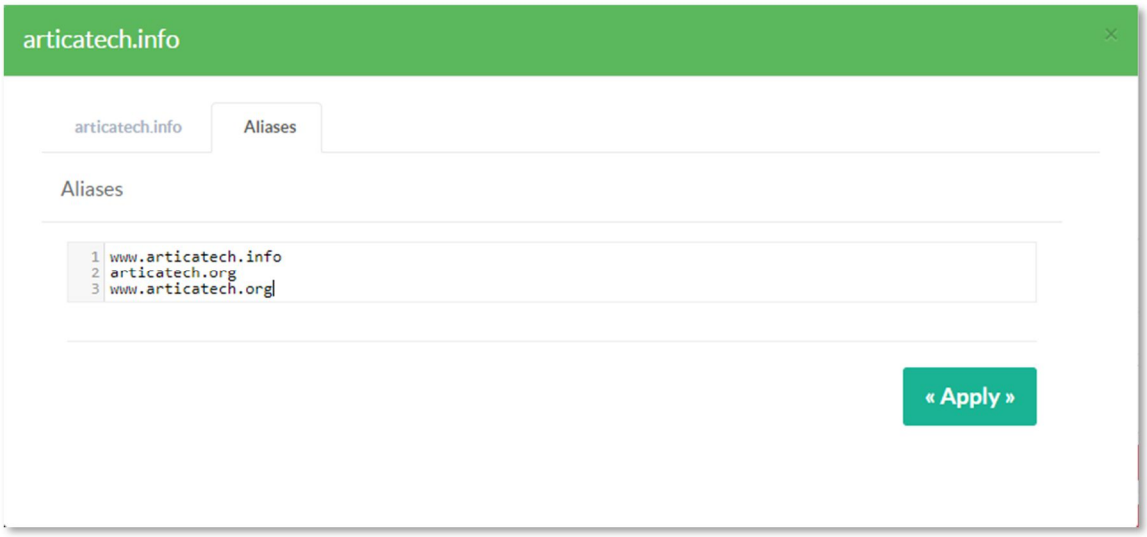
The Wordpress Administrator password is re-defined each time you configure the Web site, in this case you did not have to modify it through the Wordpress Web console.
In this way, modify the password in this section helps you to recovery your Wordpress adminisrator password.

DOMAINS ALIASES

If you plan to accept multiple domains for your wordpress site :

- Click on the sitename in the table.
- Open the aliases tab

Set all domains you want your Wordpress accept.



ENABLE OR DISABLE A WEBSITE

Enable or disable a website make it available or unavailable on the Net.
You can enable/disable by check/unckeck the checkbox in the enabled column.

After enabled or disabled your select websites, click on the “Reconfigure service” button in order to make your changes in production mode.