

Version 4.02.011018

ARTICA v4.x DOCUMENTATION

DRAFT UNDER CONSTRUCTION





TABLE OF CONTENTS

Installing Artica	5
Requirements.....	5
Using the ISO.....	5
Using the install script.....	7
The menu console.....	8
The Wizard.....	9
Community or Enterprise EDITION?	11
The Certificates Center	12
Building a Let's Encrypt Certificate.....	12
Verify the Let's Encrypt Automation installation.....	12
Generate the certificate	13
Manage the system	16
Time and clock.....	16
Set the Time zone and clock.....	16
Set Artica as An NTP time client.....	17
Backup/Restore configuration.....	19
Create a snapshot	19
Snapshot parameters	20
Backup your snapshots on a remote NAS	20
RESTful API.....	21
System information.....	22
Network interface	22
Change a network interface parameter	22
Apply network configuration to the system.....	22
Change the server hostname.....	23
The Features section	24
Artica Web Console	25
Change the Web console language	25
AUTH Link.....	26
Artica Web console Listen port and certificate	27
Reset to default settings	28
Monitoring the system	29
The Advanced Monitoring service	29
Installing the service.....	29
Access to statistics.....	29
The LDAP server service	31
OpenLDAP service parameters.....	31
Manage LDAP Members/group	32
RESTful API for managing LDAP users.....	34



Manage organizations.....	35
Manage Groups inside an Organization.....	35
Manage members.....	36

SSH service37

Install the SSH service.....	37
The SSH Web console	37
Restrict the SSH access to the Web console.	38

DNS services.39

Reverse DNS	39
Creating a reverse DNS domain	39
Creating SOA and NS records for a reverse DNS domain	39
Creating PTR records for a reverse DNS domain	42
Testing our configuration.....	43
The DNSCrypt service.	44
Multiple providers	44
Update the list.....	45
Unique Provider	45
The DNS OVER HTTPS service.....	46
Install the DNS Over HTTPs service	46
Update to the latest version	46
Install the service	48
Create the HTTPs service	48
Testing your DOH server resolution	51

The HTTP/HTTPS Proxy52

Authenticate Members	53
LDAP Authentication	53
Use the Artica LDAP service.....	53
Use a Remote LDAP Database.....	57
Example: Synology LDAP server	58
Example: Like Active Directory	58
Verify your LDAP patterns	58
RADIUS Authentication	60
Use Active Directory	61
How to join Artica to your Active Directory server?.....	61
Join the Microsoft domain.	61
Kerberos or NTLM ?	62
Active Directory users and groups	63
What about users outside the Windows domain?	63
Restful API.....	64

Categorization.....65

Benefits	65
The passive method.....	65
The Active Method	66
Install the category service.	66
Define the schedule for updating database.	67
Create your own categories	68
Install the personal categories feature	68
Create your first category.....	68
Compiling your categories.	70



Uncategorized websites	71
RESTful API for categories	72
Enable the RESTful service for categories.....	72
RESTful commands for categories.....	72
Testing categories	78
Proxy RESTful Api	79
Caching.....	80
Exclude from caching.....	80
RESTful API:	81
Realtime statistics	82
Enable the Realtime statistics	82
Display proxy statistics	82
Proxy Statistics	83
Proxy Statistics: RESTful API	83
ICAP Center	84
Example: Connect to the Kaspersky Web traffic Security ICAP server.....	85
Kaspersky Web Traffic Security.....	87
Features	87
Install Kaspersky Web traffic Security	87
Downloading the package from your Artica server	87
The Firewall.....	88
Manage items	88
Bulk importation.....	88
Find a rule based on an item.....	89
The SMTP service.....	90
Features.....	90
Anti-spam.....	90
Protection	90
Anti-virus	90
Quarantine	90
Powerful management.....	90
Install the SMTP service	91
First step, set your authorized networks.....	92
The Routing table	93
Many domains in the same routing rule	94
Transfert messages to Exchange 2010 using TLS on port 587	95
Transfert all outgoing messages to an SMTP relay with authentication.....	96
Adresses Rewriting	97
Safety standards	98
Disable VRFY command:.....	98
Reject unknown client hostname:	98
Reject unknown reverse client hostname	98
Reject unknown sender domain	98
Reject invalid hostname	98
Reject non fqdn sender	98
Enforce restrictions in the HELO.....	98
Reject forged emails:	98
Enable Generic rDNS Clients check:.....	99
Reject Internal and External non-existent domains:	99



Reject senders' domains not listed in local database:.....	99
IP Reputation.	99
Use the Artica reputation database:.....	99
Public Blacklists databases.	100
Public Whitelist database.....	101
The milter-regexp module for blacklisting performance.	102
Blacklists and whitelists rules	103
Whitelist checking.....	103
Cluster configuration.	104
Automatically ban IP in firewall based on events.	106
Install the latest version	106
Install the Fail To Ban service.....	107
The Policies service (Anti-Spam, Antivirus...).....	108
Install the Policies services.	108
Enable SMTP content features.	108
SMTP statistics	109
Refused messages.....	109
SMTP investigation	110
Wordpress administration.....	112
Prepare Artica for Wordpress	112
Install Wordpress system client	112
Install the Nginx Web engine	113
Create your first Wordpress website	114
Domains aliases.....	115
Enable or disable a website.....	115



INSTALLING ARTICA

REQUIREMENTS

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

Product **is not compatible** with ARM systems and on Redhat families systems (CentOS, Fedora, Red Hat, Open SuSe **are not supported**).

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

To install Artica, you have 2 ways:

USING THE ISO

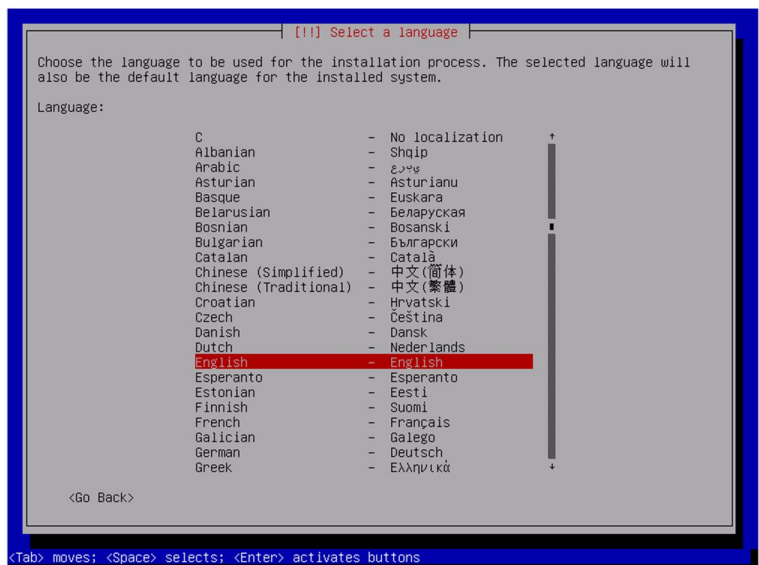
Download the ISO file at <http://articatech.net/betas4.php>

The ISO file has been tested in both physical servers and virtual environment (ESXi, HyperV, XenServer, Nutanix, KVM).

The ISO is in charge to install both the system and Artica framework, in all environments, the procedure is the same



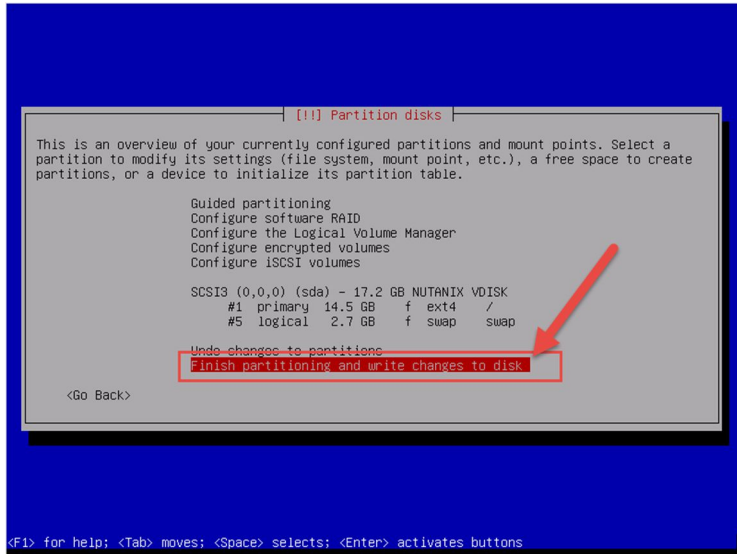
Boot from the ISO, a welcome screen must appear



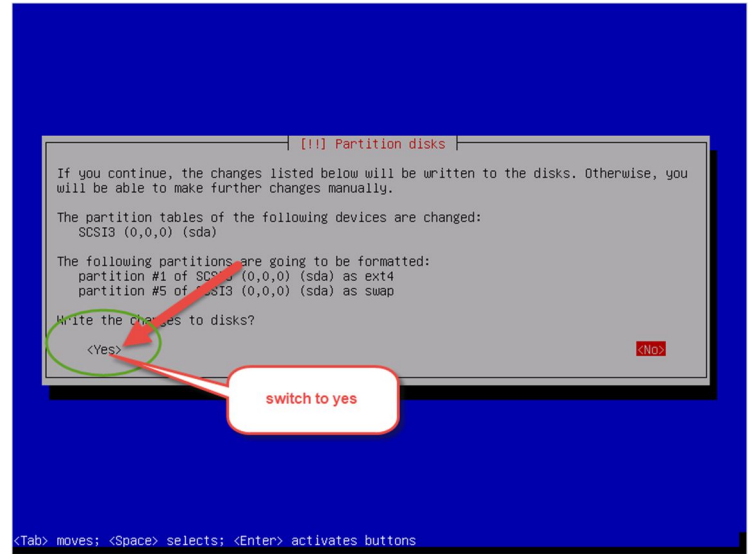
Select your system language, country and the language of the keyboard.

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.

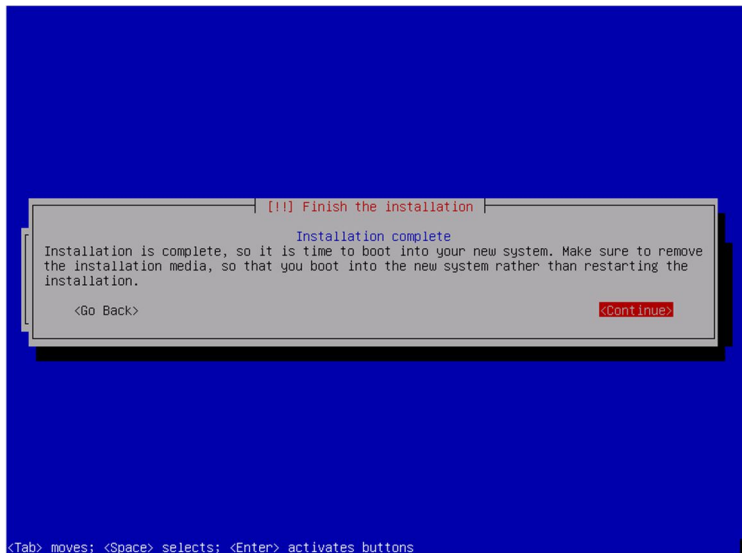
The TCP settings will not be saved after the reboot, you will have to re-enter it after the reboot.



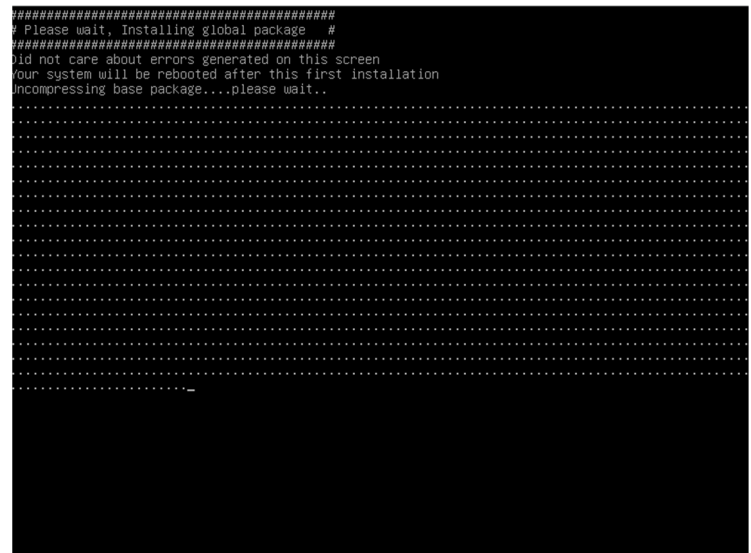
By default, the install tool will create system partitions



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

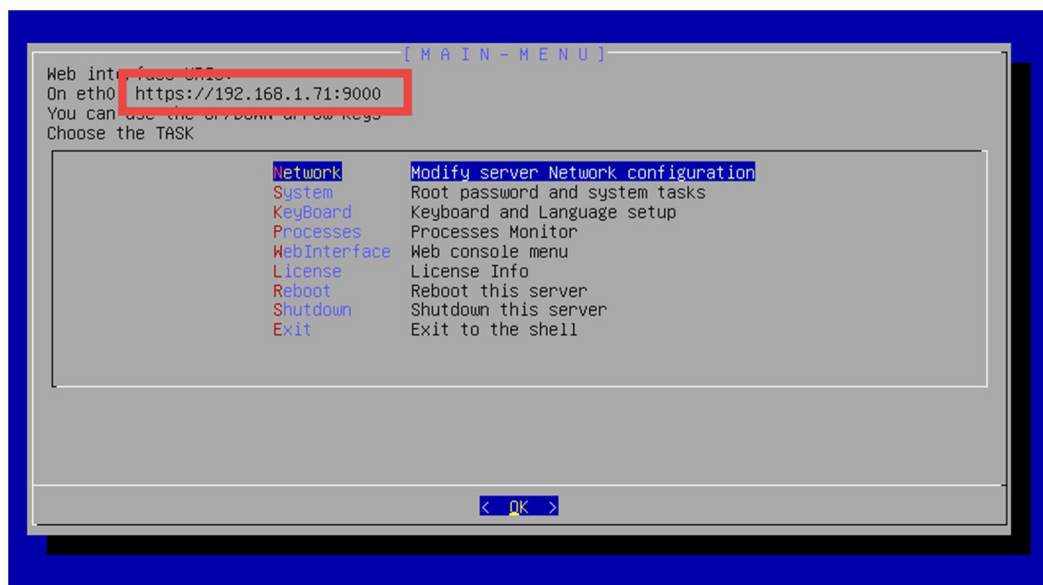


THE MENU CONSOLE.

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





THE WIZARD

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

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

Ask to the browser to continue anyway.



Your connection is not private

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

☐ Help improve Safe Browsing by sending some [system information and page content](#) to Google. [Privacy policy](#)

HIDE ADVANCED

Back to safety

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

[Proceed to 192.168.1.71 \(unsafe\)](#)

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

Welcome on the Artica project

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

Server and domain

timezone:

US/Eastern

Netbios name:

articaproxym

Server domain name:

domain.company.tld

Network & NICs

Network settings will be applied after reboot the server

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

Primary DNS server:

192.168.1.118

Secondary DNS server:

192.168.1.144

« Next »



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.

Welcome on the Artica project

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

Virtual company

your email address:

Organization:

« back » « Next »

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

Artica SuperAdmin

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

User name:

Password:

Confirm:

« back » « Build parameters »

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

Welcome on the Artica project

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

Build parameters: 13% Removing ebttables...

Build

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

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



COMMUNITY OR ENTERPRISE EDITION?

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

The difference between the Enterprise and Community edition is the Community Edition is **“Enterprise Features”** limited. Some components or some options will not be available in Community Edition.

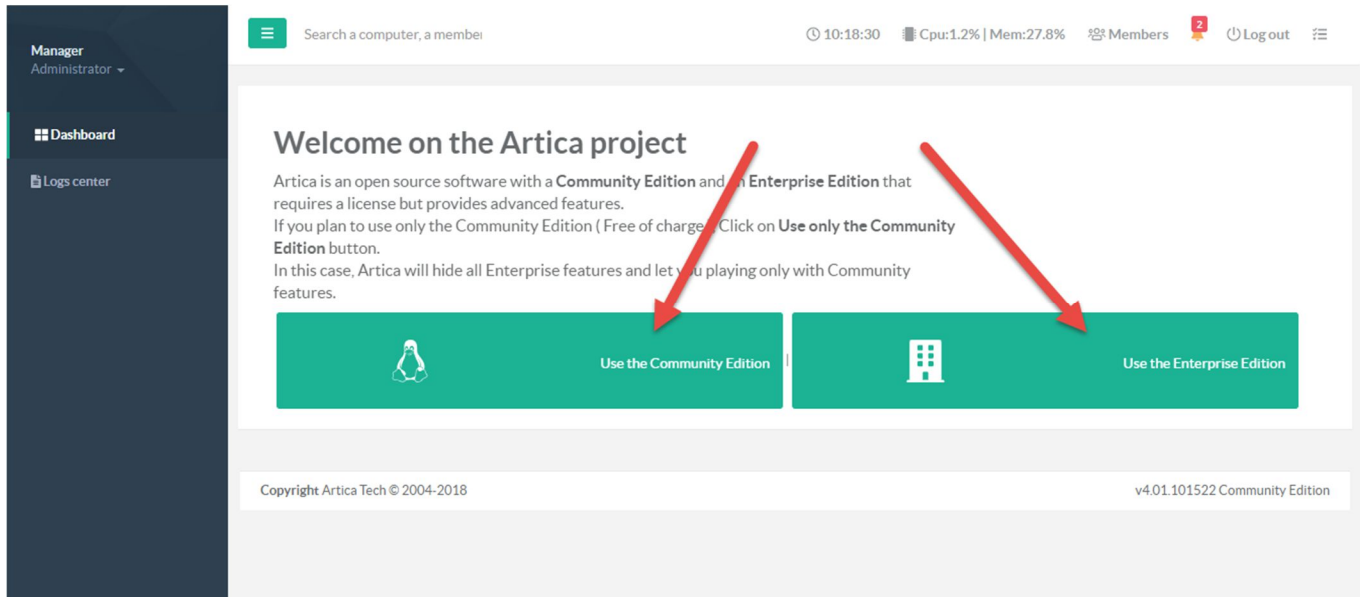
The Community Edition is free of charge and will never expire.

A licensed Artica server can run Enterprise features with a subscription.

When the Enterprise License period is expired, the Artica server will automatically return back to the Community Edition.

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

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





THE CERTIFICATES CENTER

The certificate center allows you to store and generates all certificates generates to build crypted 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 generates a free of charge public certificate.

BUILDING 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 mean it is not installed.

Click on the "**Install or update**" button.

Versions
System version and softwares versions

Artica Core server		Operating system	Python packages
		Encrypt Automation ✕ ▼	
Software	Version		
Let's Encrypt Automation:	—		📄 Install or update



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”

Search a computer, a member

SMTP Transactions 12:18:07

Certificates Center

The certificate center allows you to generate SSL certificates

+ New certificate Import Export

Common Name

Copyright Artica Tech © 2004-2018

New certificate

This operation will generate both certificate request and self-signed certificate.
If you need to upload your certificate, you will be able to upload your keys after submitting the form

Common Name: smtp.artica.center

Country Name: FRANCE

State or province name: Yvelines

locality name: Orgerus

organization name: Artica Tech

organizational unit name: IT service

email address: support@articatech.com

Encryption level: 2048

Expire in (Days): 730

« 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.

Certificates Center

The certificate center allows you to generate SSL certificate for services that provide SSL features such as Web servers, mail servers...

+ New certificate Import Export

Search

	Common Name	Expire	Organization Name	Organizational Unit Name	Email Address	
Not generated	smtp.artica.center	—	Artica Tech	IT service	support@articatech.com	🔄 🗑️

- ✓ 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.

organizational unit name:

email address:

Encryption level:

Expire in (Days):

« Generate new certificate » « Let's Encrypt Certificate » « Apply »

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

smtp.artica.center: Let's Encrypt Certificate

smtp.artica.center - Let's Encrypt

This operation generates a Public free certificate for the designed domain.
It is not designed for Intranet websites since Let's Encrypt will check your web server on both 80/443 port before generating a certificate.
Be sure that your Web server is already created and listens on 80 port (or 443 with a self-certificate).

Common Name: smtp.artica.center
email address: support@articatech.com

« Create certificate »

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

smtp.artica.center: Let's Encrypt Certificate

Let's Encrypt smtp.artica.center - 100% Failed [Details](#)

Let's Encrypt smtp.artica.center: 100% Failed

smtp.artica.center - Let's Encrypt

This operation generates a Public free certificate for the designed domain.
It is not designed for Intranet websites since Let's Encrypt will check your web server on both 80/443 port before generating a certificate.
Be sure that your Web server is already created and listens on 80 port (or 443 with a self-certificate).

Common Name: smtp.artica.center
email address: support@articatech.com

« Create certificate »



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.

Certificates Center

The certificate center allows you to generate SSL certificate for services that provide SSL features such as Web servers, mail servers...

+ New certificate Import Export					
Search					Q
	Common Name	Expire	Organization Name	Organizational Unit Name	Email Address
Let's Encrypt Certificate	smtp.artica.center	2019-02-27 11:57:15 (3 Months)	Artica Tech	IT service	support@articatech.com

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



MANAGE THE SYSTEM

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.

System clock

System clock

Your computer has two timepieces; a battery-backed one that is always running as the "hardware", "BIOS", or "CMOS" clock, and another that is maintained by the operating system currently running on your computer as the "system" clock. The hardware clock is generally only used to set the system clock when your operating system boots, and then from that point until you reboot or turn off your system, the system clock is the one used to keep track of time.

timezone (PHP): Europe/Paris

timezone (System): Europe/Paris

Today: 2018-11-27

This hour: 11:27:15

« Apply »

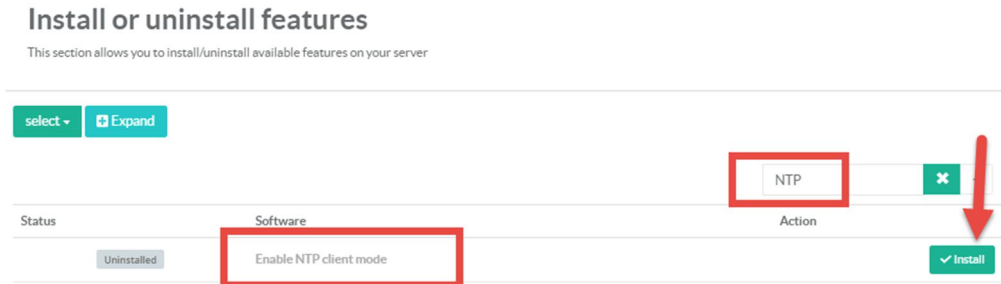
Basically, Artica can act as a time server for your network or a time client.



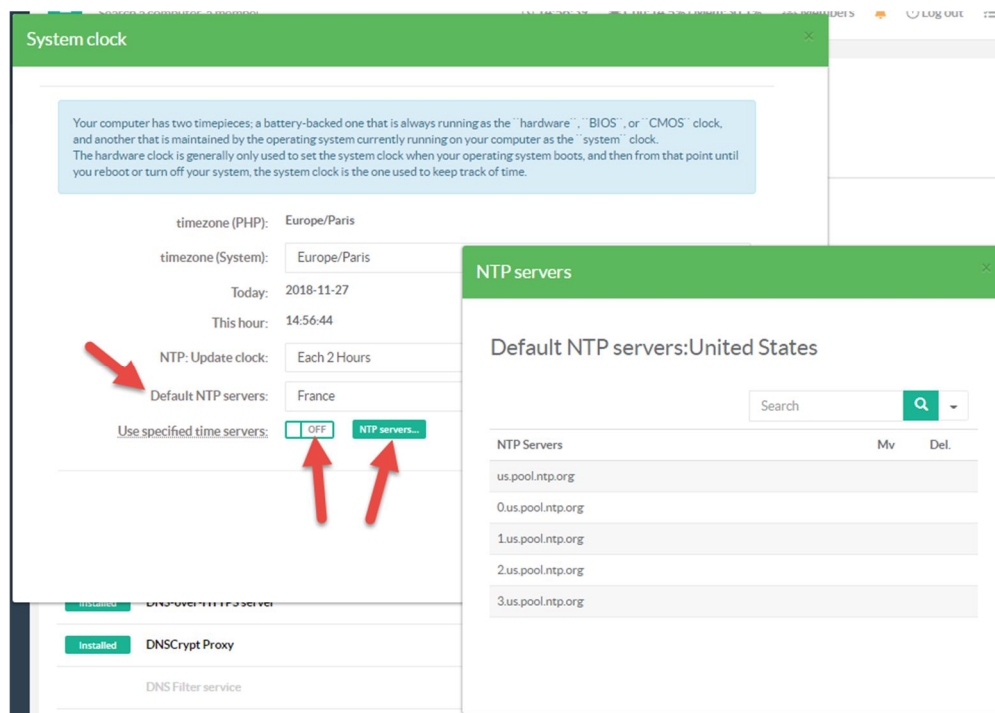
Set Artica as An NTP time client.

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 an NTP Time Client. On the Features section search the entry “NTP”.

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



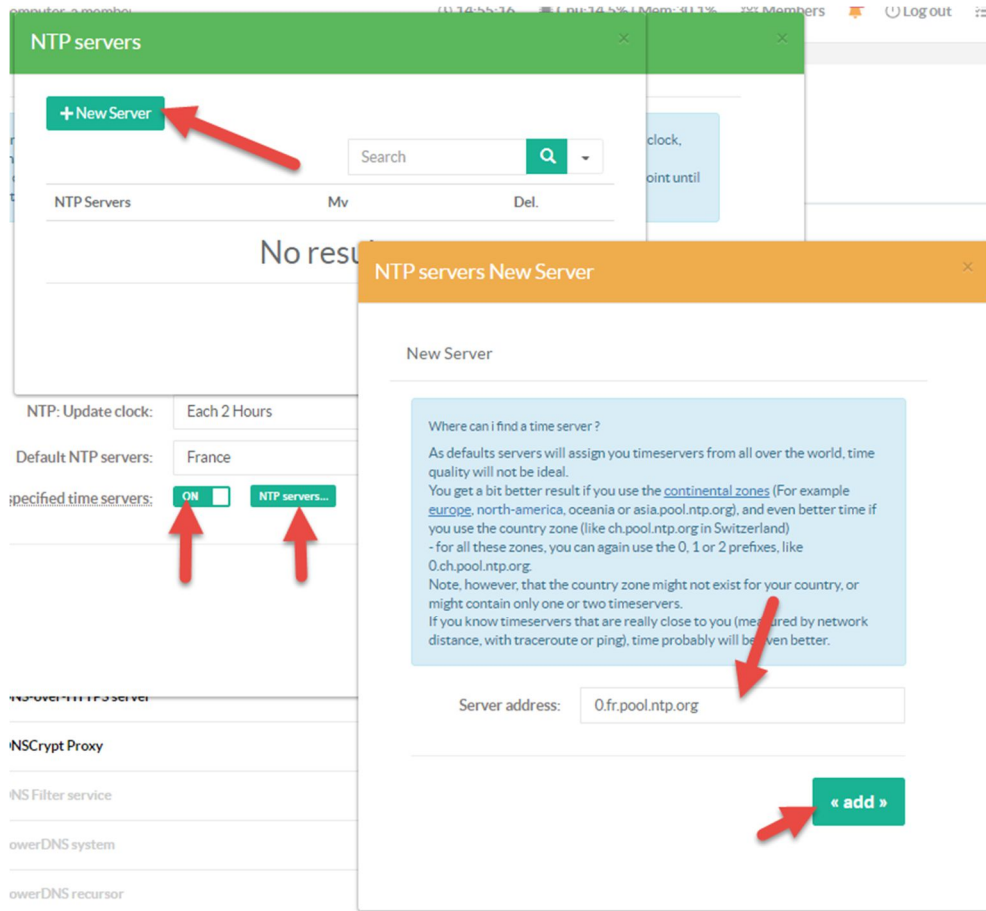
- ✓ After installing the NTP client, return to the top menu, click on the displayed time
- ✓ You can modify the schedule to synchronize the clock (by default each 2 hours)
- ✓ If “**Use Specified time servers**” is **off**, the NTP client will choose a public list of time servers according to the chosen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



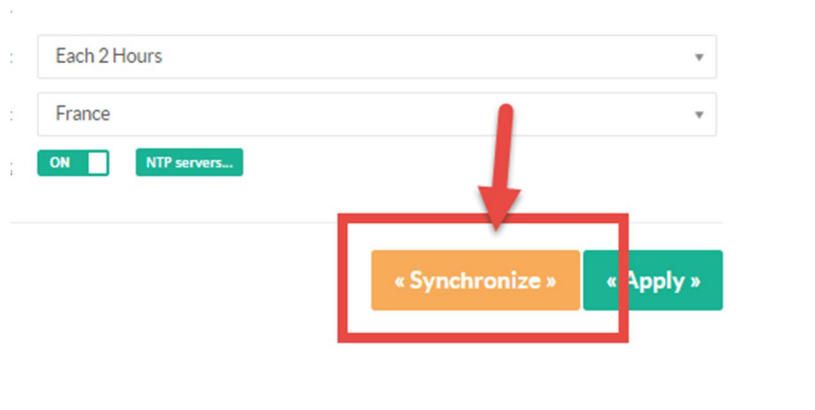


- ✓ If “**Use Specified time servers**” is **ON**, the NTP client will choose a list of time servers you have to define.
- ✓ You can manage the list by clicking on the “NTP servers” mini-button.

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



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





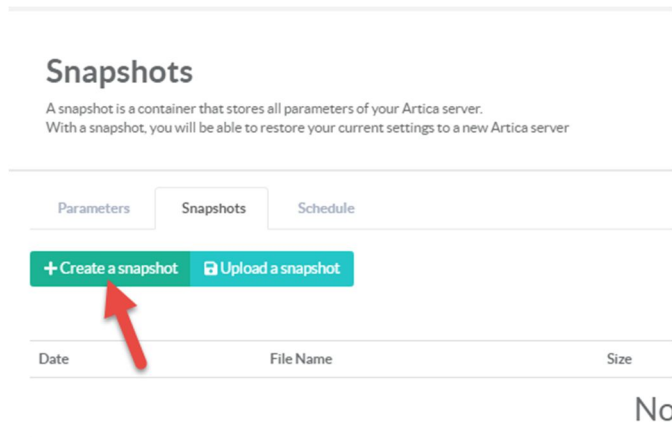
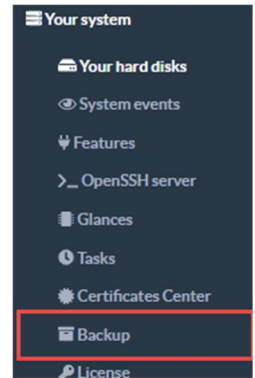
BACKUP/RESTORE CONFIGURATION.

THIS FEATURE IS AVAILABLE IN ENTERPRISE EDITION.

Artica produce container called “snapshot”. A snapshot is a container that stores all settings that allows 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

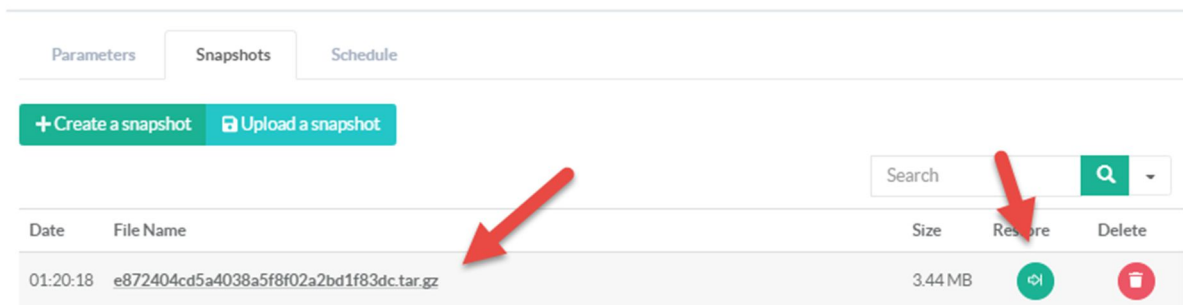
On the left menu, open “**Your system**” and “**Backup**” link
Select **Snapshots** tab
Click on **Create a snapshot** button



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

Snapshots

A snapshot is a container that stores all parameters of your Artica server.
With a snapshot, you will be able to restore your current settings to a new Artica server





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 crypted using aes256

Parameters

Storage directory: /home/artica/snapshots Browse...

Max containers: - 3 +

Passphrase: Passphrase 🔒

Passphrase (Confirm): Passphrase (Confirm) 🔒

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.

Backup your Snapshots

Artica is able to backup its configuration file to a remote NAS file system.
This task will export to a compressed file the whole server configuration in order to restore it or duplicate it.

Use remote NAS system: ON ☒

hostname: 192.168.1.17

Shared folder name: Public

User name: Administrateur

Password: Password 🔒

Password (Confirm): Password (Confirm) 🔒

« Test your connection... » « Apply »

- ✓ 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



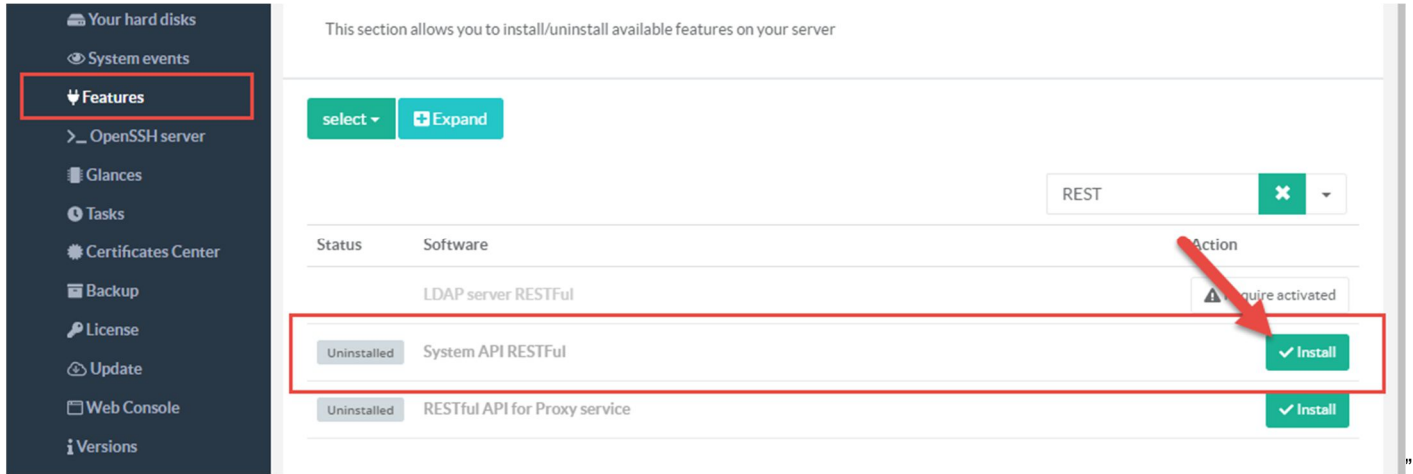
RESTful API

The RESTful API allows you to perform system tasks using RESTful commands. (THE REST API SERVICE IS AVAILABLE WITH ENTERPRISE EDITION).

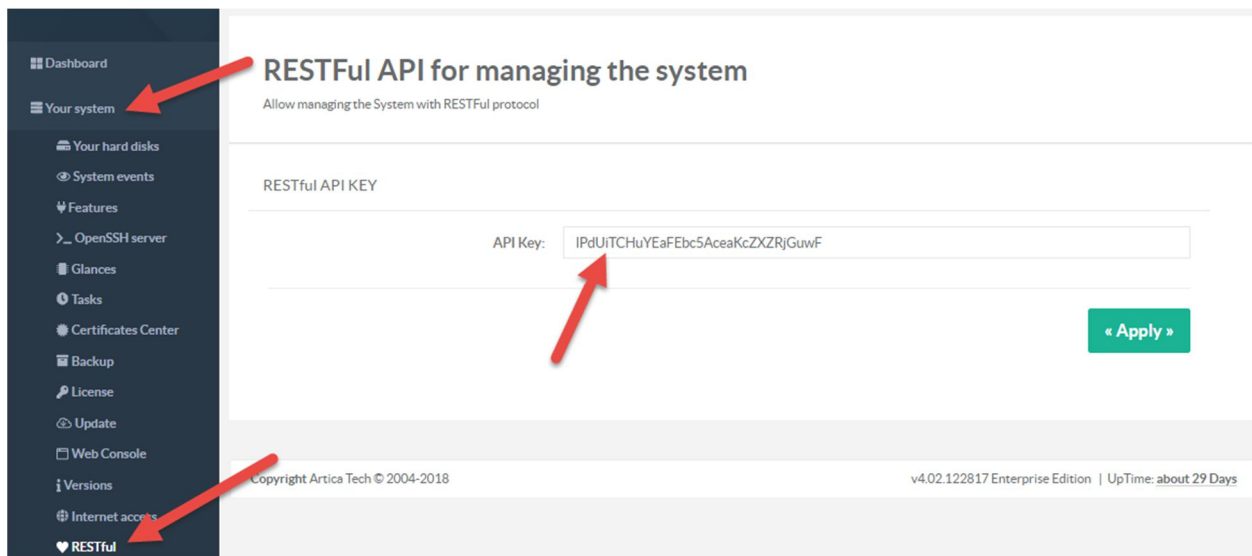
Install the System RESTful service.

On the “**Your system**” and “**Features**”, search RESTful term.

Install the feature “**System API RESTful**”



After installing the RESTful feature, display or edit the REST API KEY in the “**Your System**” and **Restful** section.



This REST API Key can be used to allow query/set all RESTful API section (LDAP database, proxy, categories...)



System information

```
GET https://192.168.1.1:9000/api/rest/system/info
```

Produce an array of system information such as CPU percentage, Memory percentage, memory infos, hardware infos...

Network interface

Change a network interface parameter

```
POST https://192.168.1.1:9000/api/rest/system/interface/[ifname]
```

Where [ifname] is the interface name

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";

//Change the Interface settings of eth0

$MAIN_URI="https://192.168.1.173:9000/api/rest/system/interface/eth0";

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(
  "IPADDR"=>"192.168.1.23",
  "NETMASK"=>"255.255.255.0",
  "GATEWAY"=>"192.168.1.1"
  "BROADCAST"=>"192.168.1.255",
  "METRIC"=>"1",
  "DEFAULT_ROUTE"=>"1");

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";
```

Apply network configuration to the system

```
GET https://192.168.1.1:9000/api/rest/system/interface/reconfigure
```



Change the server hostname

```
GET https://192.168.1.1:9000/api/rest/system/hostname/srvprox01.acme.corp
```



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.

Install or uninstall features

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

select ▾ Expand

Search 🔍 ▾

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

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

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.

Install or uninstall features

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

select ▾ Expand

- ☐ Only Active
- ☒ Proxy features
- ☒ Messaging
- ☒ Monitoring
- ☒ Network services
- ☒ Network Security
- ☒ Members services
- ☒ Data transfert
- ☒ Statistics



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

Install or uninstall features

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

select
Collapse

Q

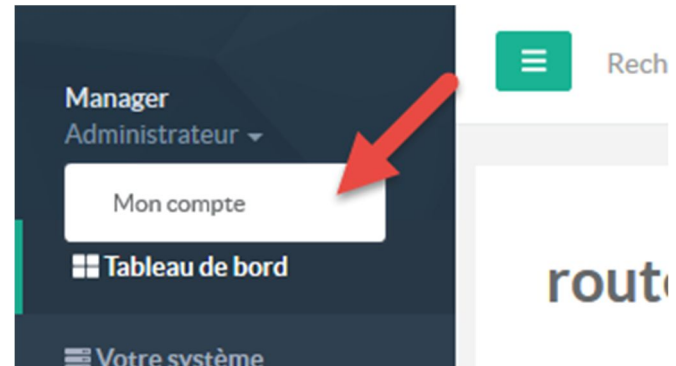
Status	Software	Action
Network services		
Uninstalled	MultiPath TCP Kernel MultiPath TCP Kernel allowing a Transmission Control Protocol (TCP) connection to use multiple paths to maximize resource usage and increase redundancy. The redundancy offered by Multipath TCP enables inverse multiplexing of resources,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

The expanded table display a description of each available service.

ARTICA WEB CONSOLE

CHANGE THE WEB CONSOLE LANGUAGE

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



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

Manager
 Administrateur

Recherche un ordinateur, un

Requetes 12:14:05 Cpu:7.5% | Mem:14.9% Membres 0 Déconnexion

Manager/Administrateur

Tableau de bord
 Votre système
 Réseau & cartes réseaux
 DNS
 Votre pare-feu
 Votre Proxy
 Mise en cache
 Vos catégories
 Statistiques
 Centre des logs

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

« Auth Link » « Appliquer »

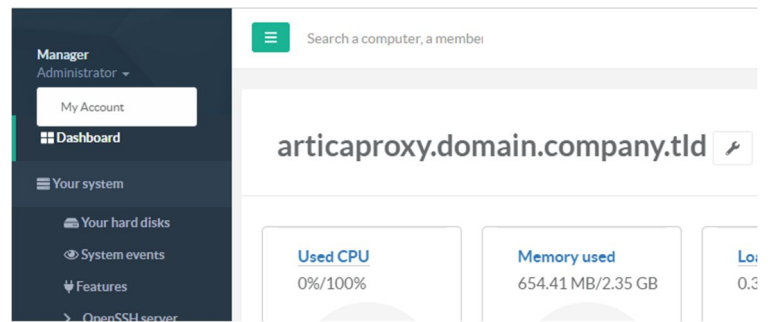
(Not all parts of the web page will be modified, if you want to change all the web page part, click on the F5 key in order to refresh totally the web console.)



AUTH LINK

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

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



Select the button “**Auth Link**”

Manager/Administrator

User name:

Password:

My language:

Font family:

Use standard drop-down lists: ☐

Administration interface browser title:

Click on the button “**Create the Authentication Link.**”

Auth Link

Auth Link

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

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

Auth Link

Auth Link

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

link:



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 use the Web service "Nginx", you should encounter a port conflict issue

To use the 2 services on the same port, use 2 network 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 loopback interface on the 9000 port.

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

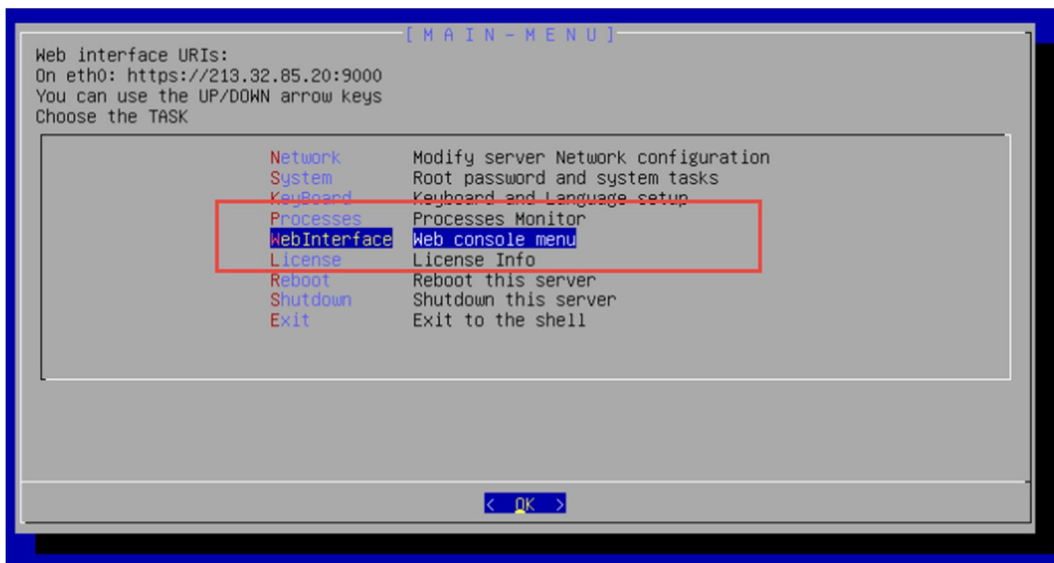
After rebooting the console, change to the defined port on your browser to access again to the Artica Web console.



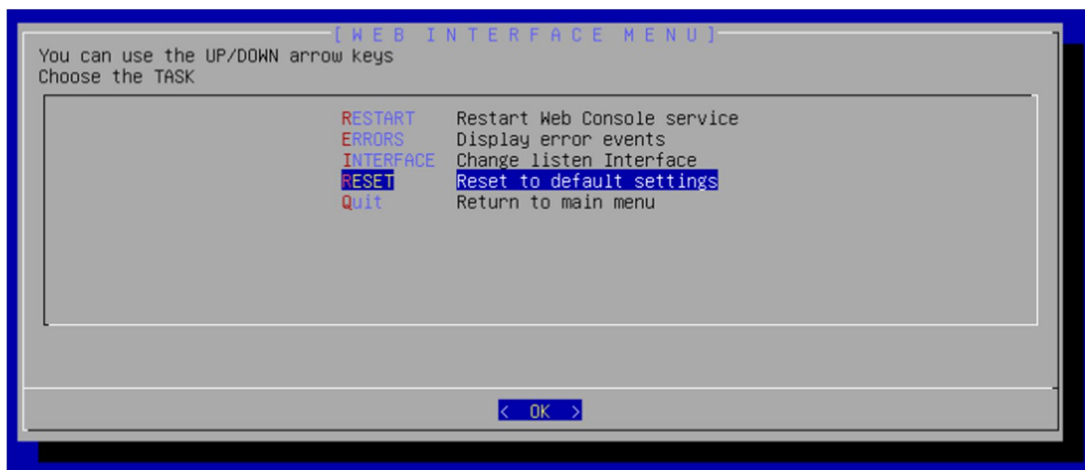
RESET TO DEFAULT SETTINGS

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.





MONITORING THE SYSTEM

THE ADVANCED MONITORING SERVICE

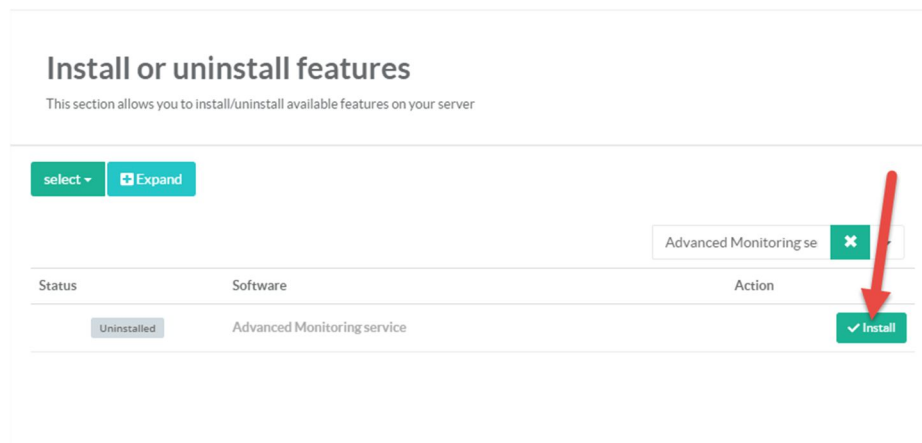
The Advanced Monitoring service (aka Netdata) is a system for distributed real-time performance and health monitoring.

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

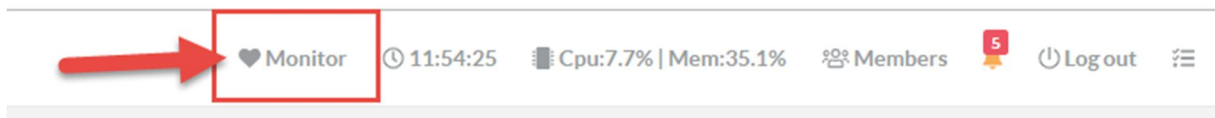
Installing the service

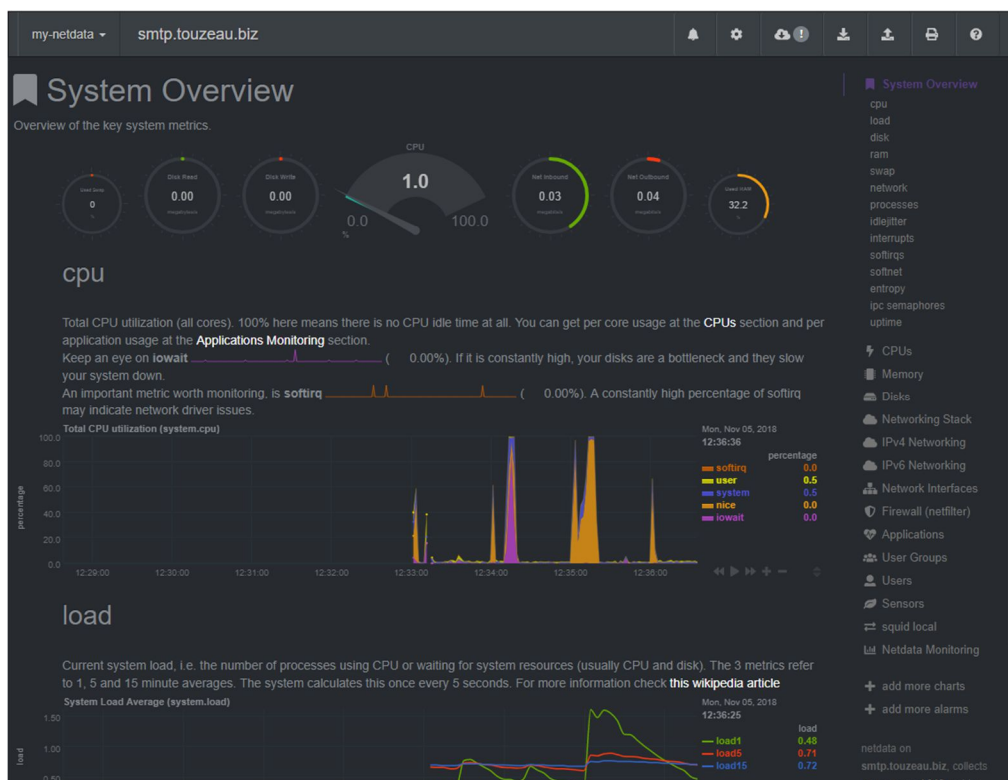
On **Your system**, select “**Features**”, type “**Advanced Monitoring service**” in the search field.



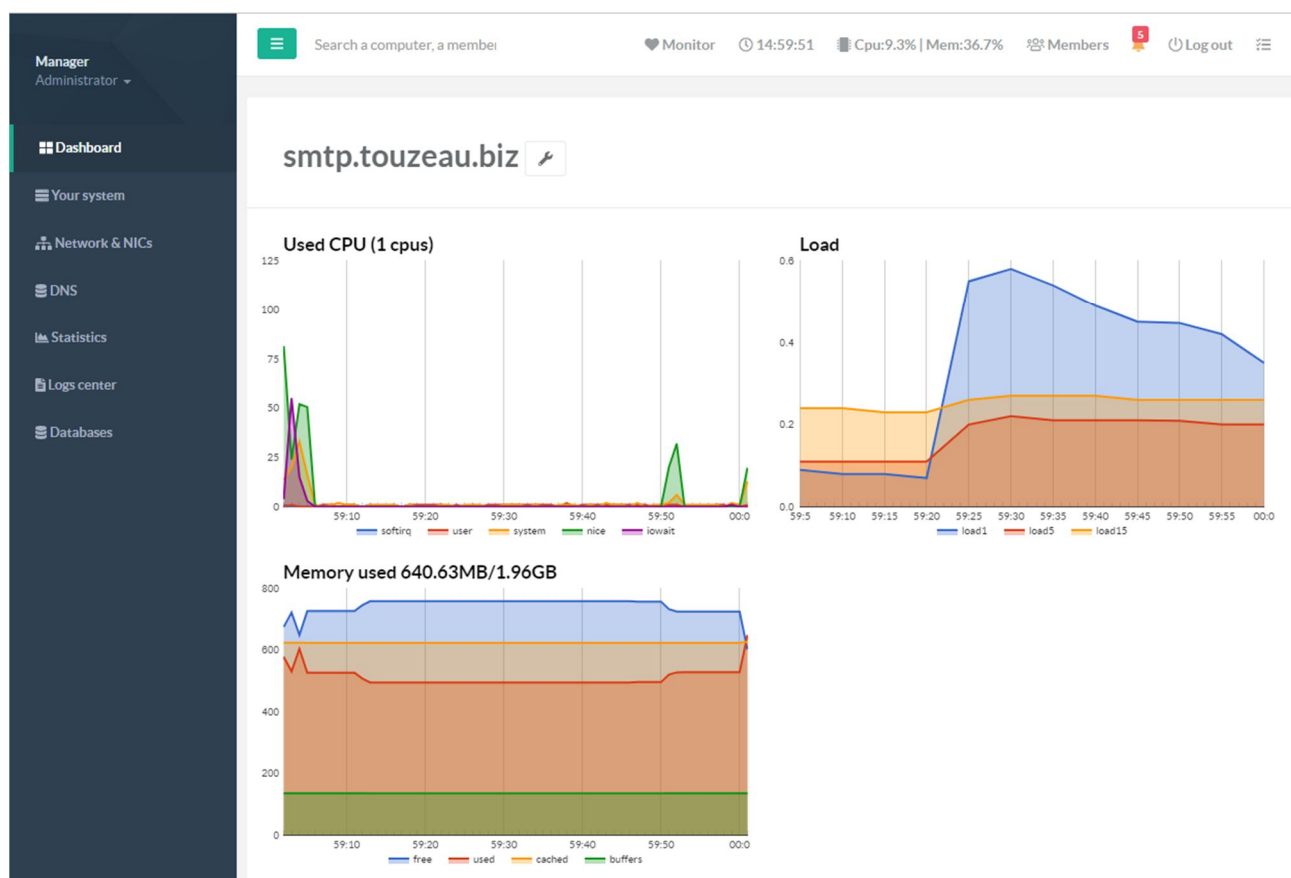
Access to statistics

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





The dashboard will be switched to new realtime graphs:





THE LDAP 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 as the login username. In this case, users need to put their eMail address to log in to all services that use LDAP.

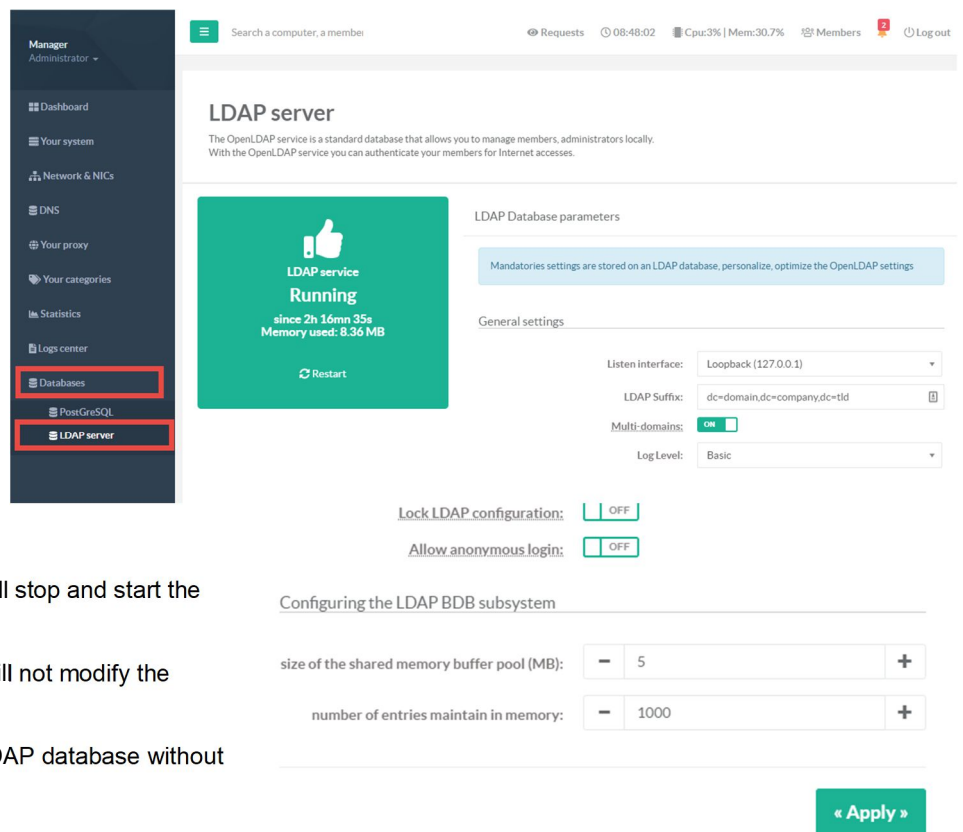
Log level: is the trace level used for the LDAP service (logs are stored in syslog)

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/slapd.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.



New Member

New Member » Articatech » Administrators

Organization: Articatech

Group: Administrators

Domain:

First Name: David

Last Name: Touzeau

eMail address: david.touzeau@company.com

User id: david.touzeau

Password:

« add »

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

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

New Member

25% David Touzeau Save

25% David Touzeau Save

New Member » Articatech » Administrators

Organization: Articatech

Group: Administrators

Domain:

First Name: David

Last Name: Touzeau

eMail address: david.touzeau@company.com

User id: david.touzeau

Password:

« add »

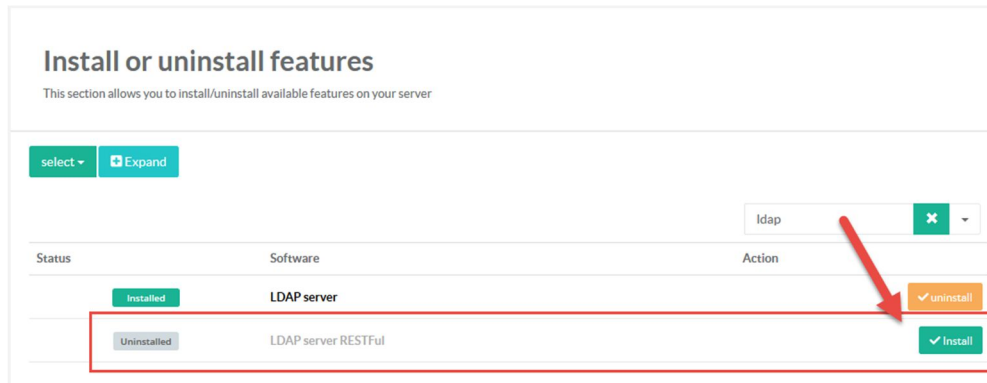
The table will display your new member and the created group.

My members			
Search			Go!
+ New Member Search			
Display Name	EMail Address	Office Phone	Groups
Administrators	—	—	—
David Touzeau		00.00.00.00.00	Administrators

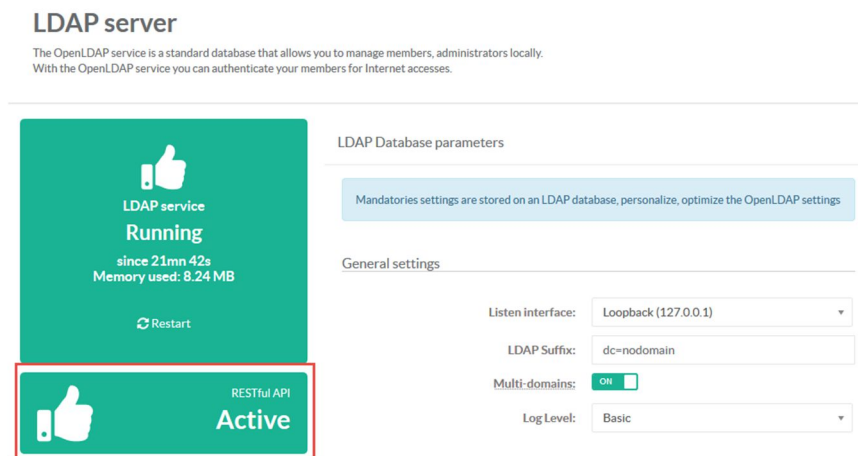


RESTful API for managing LDAP users.

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



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

Configuring the LDAP BDB subsystem

size of the shared memory buffer pool (MB):

number of entries maintain in memory:

RESTful API

API Key:

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 with 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 Organization

curl_setopt($ch, CURLOPT_POSTFIELDS, $POSTz);

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




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

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

PHP example:

```
$ch = curl_init();
$CURLOPT_HTTPHEADER[]="Accept: application/json";
$CURLOPT_HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT_HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT_HTTPHEADER[]="Expect:";
$CURLOPT_HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRcc5";

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

curl_setopt($ch, CURLOPT_HTTPHEADER, $CURLOPT_HTTPHEADER);
curl_setopt($ch, CURLOPT_TIMEOUT, 300);
curl_setopt($ch, CURLOPT_URL, $MAIN_URI);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
$POSTz=array(
    "uid"=>"Jhon.doo",
    "DisplayName"=>"Jhon doo Mhain",
    "givenName"=>"Jhon",
    "name"=>"doo Mhain",
    "password"=>"123456"
);
curl_setopt($ch, CURLOPT_POSTFIELDS, $POSTz);
$response = curl_exec($ch);
$errorno=curl_errno($ch);
if($errorno>0){
    echo "Error $errorno\n".curl_error($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.

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

select ▾ Expand

Status	Software	Action
Uninstalled	OpenSSH server	ssh ✕ ▾ ✓ Install

SSH System Console

⚠ Require activated OpenSSH server

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

THE SSH WEB CONSOLE

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

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

select ▾ Expand

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



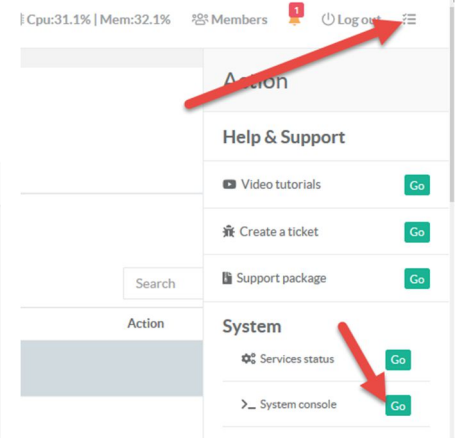
The Web SSH console is available using the right menu and **“System console”** menu.

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

```

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

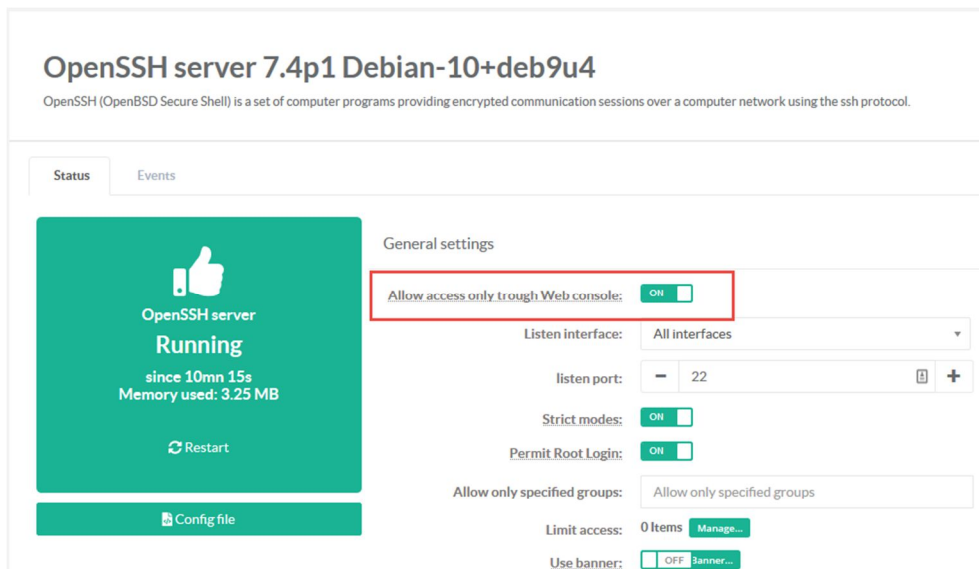
127 login: root
root@127.0.0.1's password:
Last login: Mon Aug 20 23:54:05 2018
root@articaprox:~# ls
DEBIAN_INSTALL_PACKAGE
root@articaprox:~# cd /home
root@articaprox:/home# ls
ArticaStats      ArticaStatsDB  dhcpd          logrotate_backup  squid  ufdb-templates
ArticaStatsBackup artica         logrotate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



Restrict the SSH access to the Web console.

If you did not want to open the TCP 22 port and keep access to the Artica system using only the Web console, on the left pan, choose **“Your System”** and **“OpenSSH server”** menu.

Under the **“General settings”** section, turn on the **“Allow access only through Web console”** and click on **“Apply”** button.



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.



DNS SERVICES.

Artica offer 2 main services for providing DNS services.

1. The PowerDNS system:
Is a complete DNS service used by many ISPs and claim to be a Public DNS server.
2. 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.

REVERSE DNS

Creating a reverse DNS domain

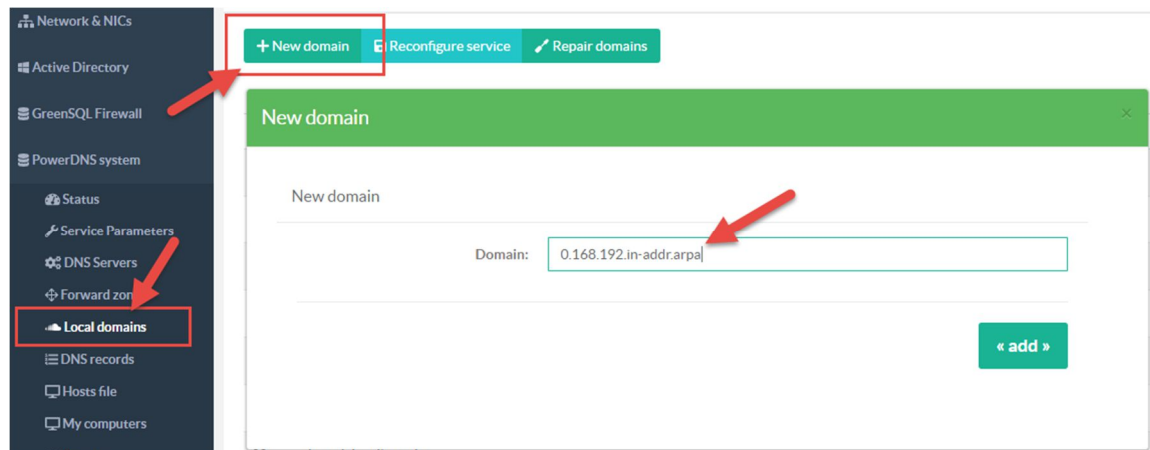
For the following example we shall assume that we are configuring reverse DNS for an internal network using IP addresses in the 192.168.0.0/24 range. With this in mind the first task is to create an entry in the Internal domains.

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

192.168.0.0/24 will be inverted 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

DNS records

0.168.192* and type soa Go!

[+ New record](#) [Reconfigure service](#)

Search Q

ID	Record	Domains	Type	Content	Delete
1020	0.168.192.in-addr.arpa	0.168.192.in-addr.arpa	SOA	ns.0.168.192.in-addr.arpa hostmaster.0.168.192.in-addr.arpa 2018113014 10800 1800 60480...	✓ ✖

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")

Record: 1020 0.168.192.in-addr.arpa >> Type:SOA (0.168.192.in-addr.arpa)

Start of Authority Record » 0.168.192.in-addr.arpa

A Start of Authority record (abbreviated as SOA record) is a type of resource record in the Domain Name System (DNS) containing administrative information about the zone, especially regarding zone transfers.

zone: 0.168.192.in-addr.arpa

MNAME: ns1.touzeau.biz

RNAME: hostmaster.touzeau.biz

Serial: 2018113014

Refresh: 10800

Retry: 1800

- ✓ 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

New record

New record

Insert a new entry in your PDNS DNS server in order to resolve it

Domain: 0.168.192.in-addr.arpa

Type (IN): NS

[« add »](#)



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

New record Type:PTR (0.168.192.in-addr.arpa)

PTR »»0.168.192.in-addr.arpa

hostname: ns1.touzeau.biz

IP Address: 192.168.0.151

PRIOR: - 1 +

TTL (Seconds): - 3600 +

« add »

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

New record

New record

Insert a new entry in your PDNS DNS server in order to resolve it

Domain: 0.168.192.in-addr.arpa

Type (IN): PTR

« add »

- ✓ 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.

New record Type:PTR (0.168.192.in-addr.arpa)

PTR »»0.168.192.in-addr.arpa

hostname: ns2.touzeau.biz

IP Address: 192.168.0.1

PRIOR: - 1 +

TTL (Seconds): - 3600 +

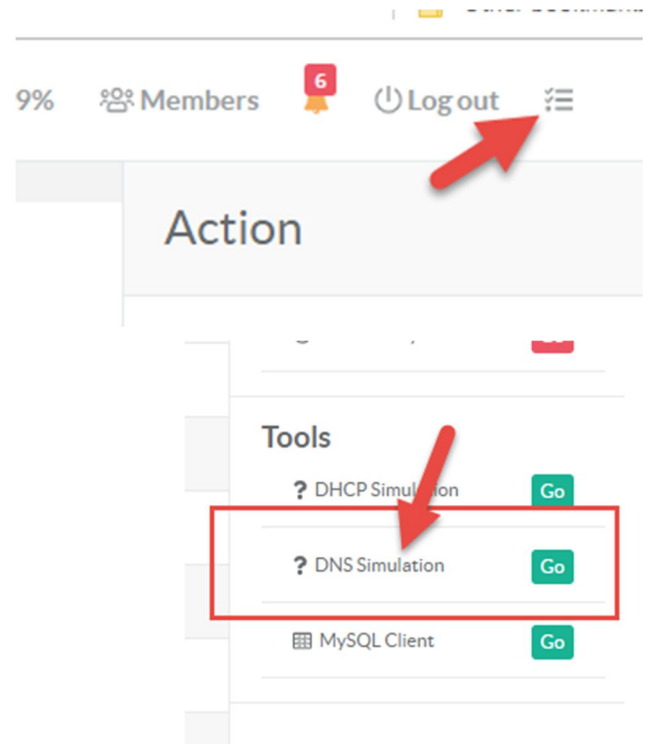
« add »



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 Run.

DNS Simulation

Verify the DNS service resolution

hostname: 192.168.1.1

Reverse lookup: ☒

Network Interface: None

DNS server: 192.168.1.151

TimeOut (Seconds): 3

You should see the correct PTR entry in the DNS response

DNS Simulation Results

```

<<>> DiG 9.10.3-P4-Debian <<>> -x 192.168.1.1 +time=3 +tries=1 @192.168.1.151 -b 192.168.1.151 -4
;; global options: +cmd
;; Got answer:
;;->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25138
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1680
;; QUESTION SECTION:
;1.1.168.192.in-addr.arpa. IN PTR

;; ANSWER SECTION:
1.1.168.192.in-addr.arpa. 3600 IN PTR router.touzeau.biz.

;; Query time: 0 msec
;; SERVER: 192.168.1.151#53(192.168.1.151)
;; WHEN: Sat Dec 01 19:56:11 CET 2018
;; MSG SIZE rcvd: 85
  
```




THE DNSCRYPT SERVICE.

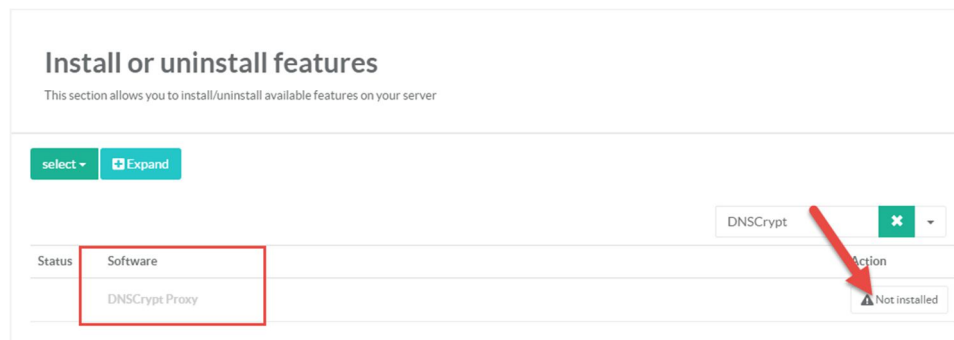
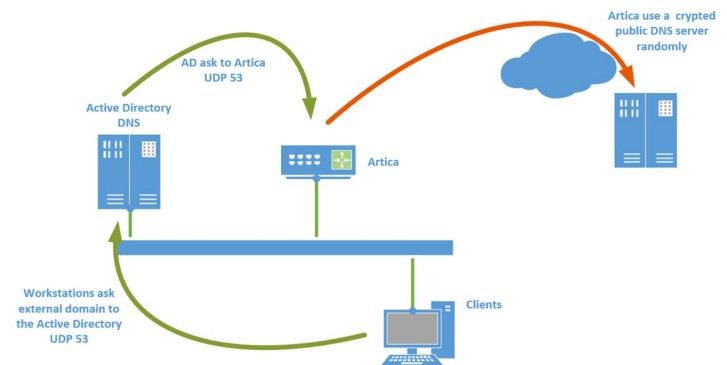
The DNSCrypt service is designed to hide DNS requests from the Internet.

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.



Manager
Administrator

Dashboard
Your system
Network & NICs
DNS
DNS Cache service
DNS Servers
Forward zones
Hosts file
My computers
DHCP/TFTP
Statistics
Logs center
Databases

Search a computer, a member

00:27:49 Cpu:8.7% | Mem:29.5% Members Logout

DNS Servers

This section list DNS servers used by the system.

DNS Servers **Public DNS servers** DNS benchmark

Reconfigure service

Search

Enable	Name	Description
☒	Adguard DNS Family Protection 1	(Anycast) Adguard DNS with safesearch and adult content blocking 176.103.130.132-5443
☒	Adguard DNS Family Protection 2	(Anycast) Adguard DNS with safesearch and adult content blocking 176.103.130.134-5443
☒	Adguard DNS 1	(Anycast) Remove ads and protect your computer from malware 176.103.130.130-5443
☒	Adguard DNS 2	(Anycast) Remove ads and protect your computer from malware 176.103.130.131-5443
☒	BikiniHappy Singapore	(Singapore) provided by bikinihappy.com 172.104.46.253-443
☒	Babylon Network France 0	(Roubaix, France) Non-logging, uncensored DNS resolver provided by Babylon Network 5.135.66.222-5353

Update the list

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

DNS Servers

This section list DNS servers used by the system.

DNS Servers **Public DNS servers** DNS benchmark

Disable all **Update** Options Reconfigure service

Enable	Name	Description
☒	aafalo-me	DNS-over-HTTPS server running rust-doh with PiHole for Adblocking. Non-logging, AD-filtering, supports DNSSEC. Hosted in Netherlands on a RamNode VPS. dns.aafalo.me-443,176.56.236.175-443
☒	aafalo-me-gcp	DNS-over-HTTPS proxy of aafalo-me hosted in Google Cloud Platform. Non-logging, AD-filtering, supports DNSSEC. dns-gcp.aafalo.me-443,35.231.69.77-443
☒	adguard-dns	Remove ads and protect your computer from malware 176.103.130.130-5443

Unique Provider

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

Manager
Administrator

Dashboard
Your system
Network & NICs
DNS
DNS Cache service
DNS Servers
Forward zones
Hosts file
My computers

Search a computer, a member

DNS Servers

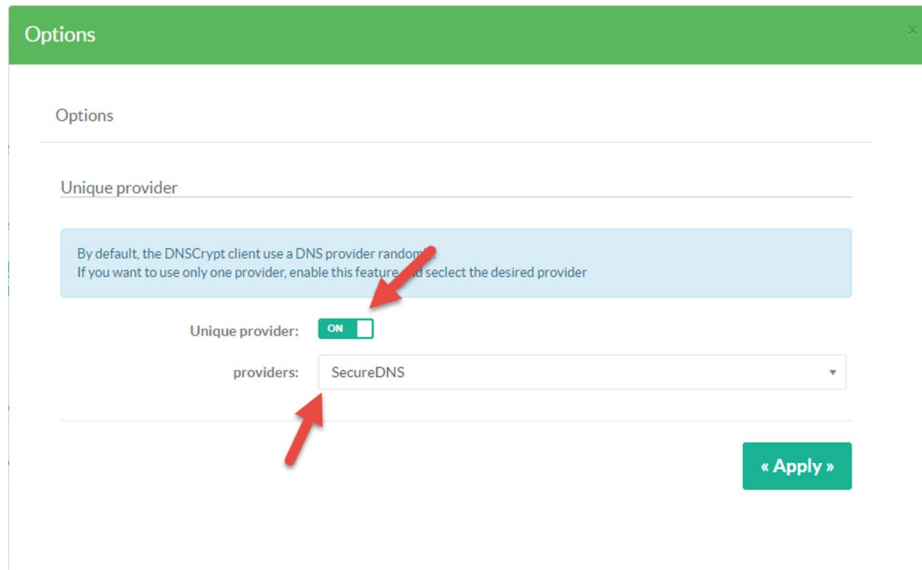
This section list DNS servers used by the system.

DNS Servers **Public DNS servers** DNS benchmark

Disable all **Options** Reconfigure service

Enable	Name	Description
☒	Adguard DNS Family Protection 1	(Anycast) Adguard DNS with safesearch and adult content blocking 176.103.130.132-5443

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:

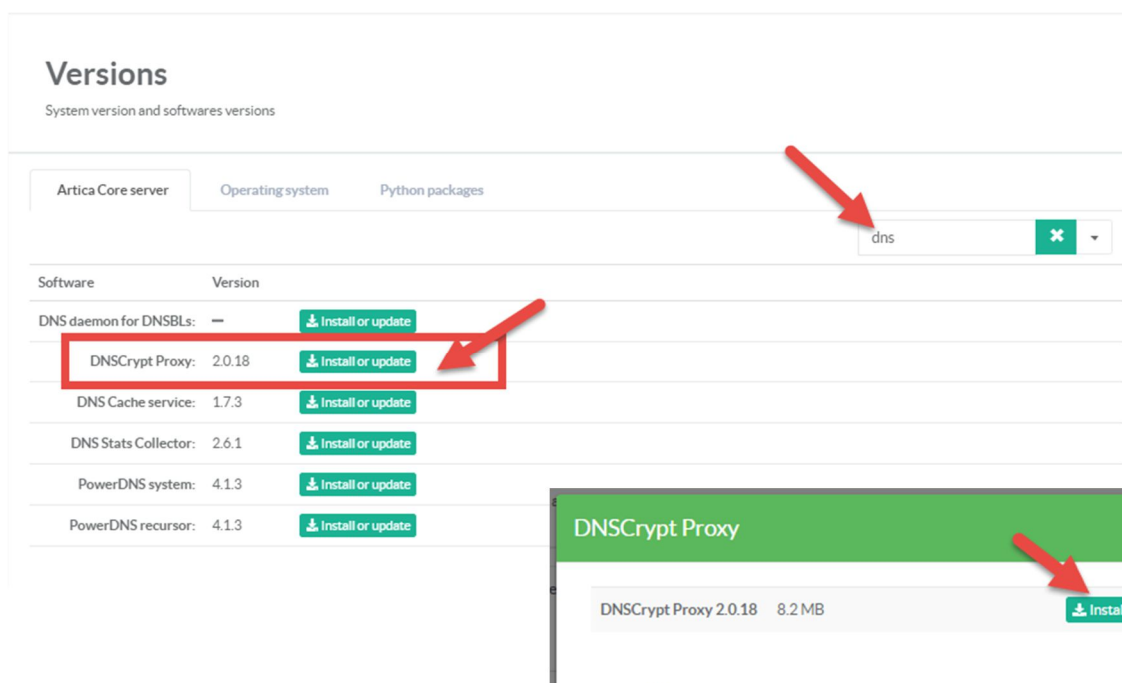
- ✓ Firefox since Version 62 and later.
- ✓ DNSCrypt-proxy
- ✓ Technitium DNS forwarder
- ✓ Google Chrome start to implement it.

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

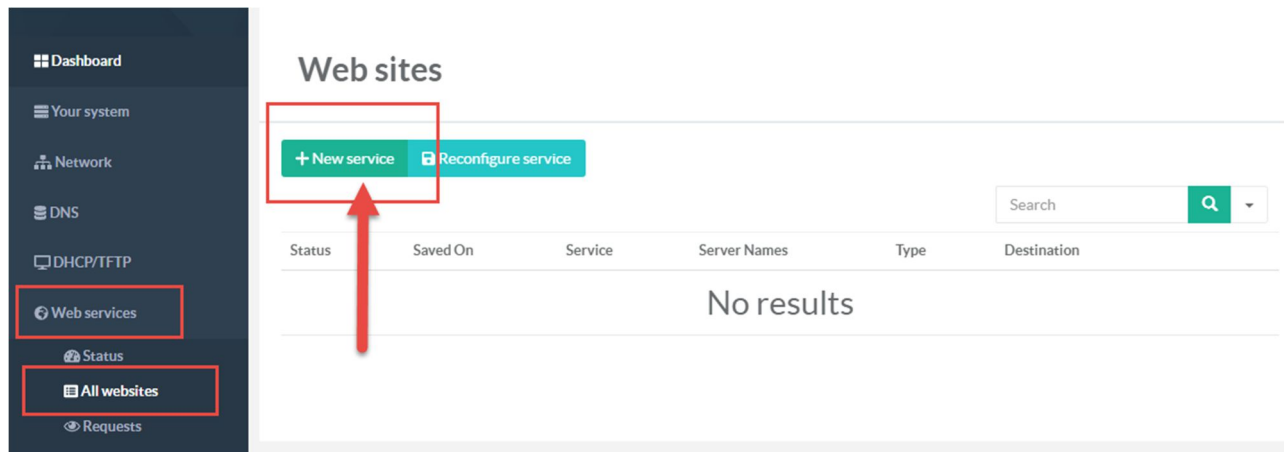
To enable the DNS Over HTTPS, you need to enable first these 2 services using the “**Features**” section:

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

Create the HTTPS service

After installed 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**”





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

New service

New service

A service is an HTTP/HTTPS service that able to provide Web application.
This service can handle multiple hostname of domain name.
After creating this service, you will be able to define which domain this service will be able to populate.

Service name:

☐ Create a Simple PHP Website.
A Simple php website allows you to create a web service that allows you to upload your php application in order to generates Web pages

☐ Create a reverse proxy service.
A reverse proxy service allows you to enforce, protect, cache a website stored on a remote server.

☐ Create an HotSpot website
An HotSpot Website run with the local proxy service.
It able to provide a system authentication to allow users to access Internet.

☐ Create an Artica administration redirector
This option will create a reverse-proxy of the local Artica Web console.
Usefull if you need to place the Artica Web console on Internet with the Let's Encrypt certificate.

☐ Create a port forwarder
A port forwarder is similar to a NAT Firewall behavior with extra features.

☐ Create a Web-Filtering Error service
A Web-Filtering Error service is designed to work with the Proxy Web-Filtering service.
It is used to redirect banned sites to this Web service in order to provide blocked information to the user or provide possibilities to whitelist the blocked site.
Create this service without any Web-Filtering service did not make sense.

☒ **Create a DNS Over HTTPs service**
Turn a website to a reverse HTTPs DNS forwarder to take care of the HTTPS part of DNS-over-HTTPS.

[« add »](#)

Select your new web service in the table.

Web sites

+ New service Reconfigure service			
Status	Saved On	Service	Server Names
Not configured	—	<u>My DOH service</u>	

On the general settings, choose the certificate created in the **The Certificates Center**.

My DOH service

General settings | Server names | Ports | Access rules

My DOH service DNS Over HTTPs web service

Create a DNS Over HTTPs service
Turn a website to a reverse HTTPs DNS forwarder to take care of the HTTPS part of DNS-over-HTTPS. (7)

Service name:

SSL parameters

Certificate:

SSL protocols:

Cipher suites:

Prefer server Ciphers: ☐ OFF

SSL Buffer size (k):

[« Apply »](#)



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

My DOH service

General settings **Server names** Ports Access rules

Server names

Server names determine which server block is used for a given request. They may be defined using exact names, wildcard names, or regular expressions. Examples: example.org www.example.org *.example.org mail.* 192.168.1.1 ~^(?+).example\.net\$ When searching for a virtual server by name, if name matches more than one of the specified variants, e.g. both wildcard name and regular expression match, the first matching variant will be chosen, in the following order of precedence: exact name longest wildcard name starting with an asterisk, e.g. *.example.org longest wildcard name ending with an asterisk, e.g. mail.* first matching regular expression (in order of appearance)

Items: 1 doh.touzeau.biz 2 dns.touzeau.biz

« Apply »

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

My DOH service

General settings Server names **Ports** Access rules

+ New entry

Search

No results

New entry

New item

Listen interface: All interfaces

listen port: 443

Options

Use the SSL encryption: **ON**

HTTP/2: OFF

SPDY: OFF

PROXY Protocol: OFF

« add »

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

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

My DOH service

General settings Server names Ports Access rules **DNS-over-HTTPS server**

My DOH service (DNS Over HTTPs web service)

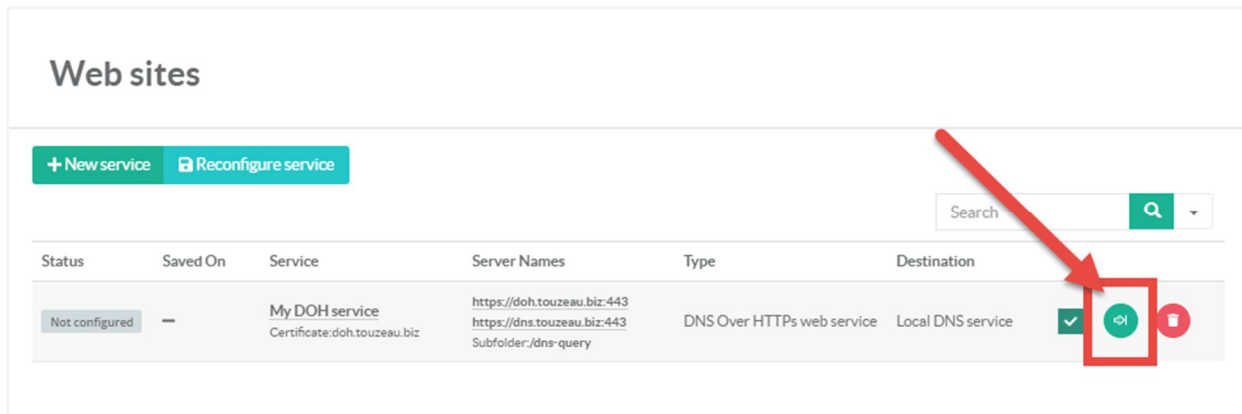
Create a DNS Over HTTPs service
Turn a website to a reverse HTTPs DNS forwarder to take care of the HTTPs part of DNS-over-HTTPS. (7)

HTTP path for resolve application: dns-query

« Apply »

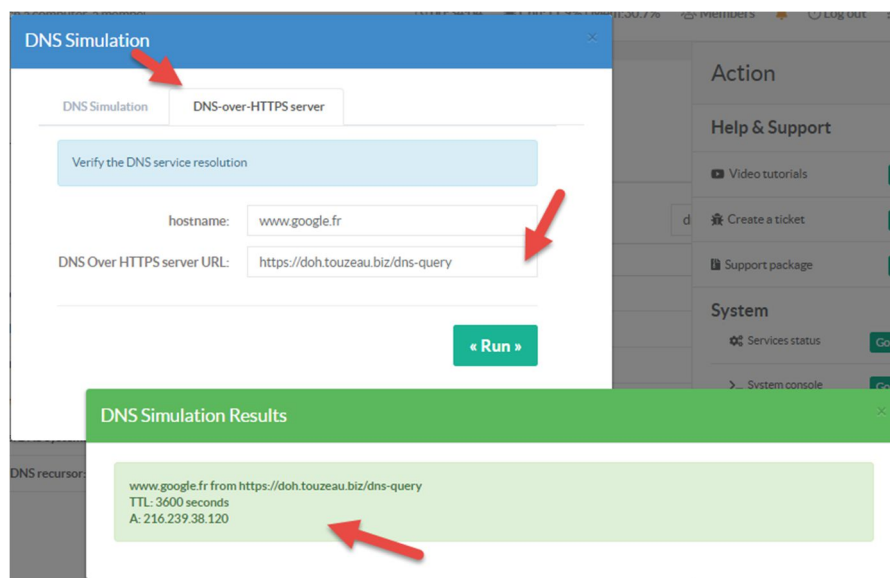
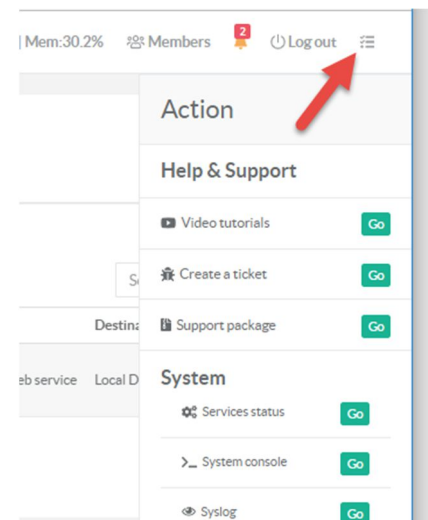


On the table, you see that your web service is “Not configured”, to make the website available, click on the run icon on the right side.



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 demonstrate your DOH server works as expected.





THE HTTP/HTTPS PROXY

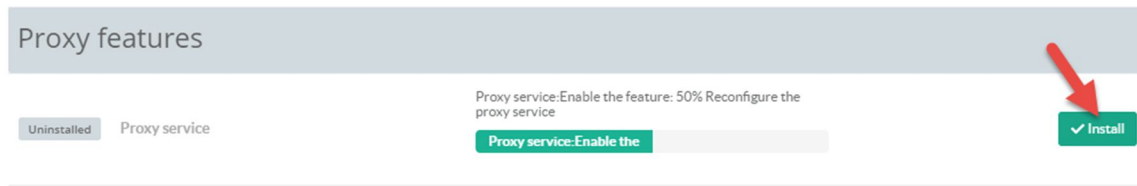
The proxy service is designed to handle the HTTP/HTTPS and FTP over HTTP protocols.

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)...

The proxy service can be enabled in the “**Features**” service (SEE



) under the “**Proxy features/ Proxy service.**”



AUTHENTICATE MEMBERS

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

LDAP Authentication

Artica supports LDAP v3.

An LDAP directory consists of a simple tree hierarchy.

An LDAP directory might span multiple LDAP servers. In LDAP v3, servers can return referrals to other servers back to the client, allowing the client to follow those referrals if desired.

Directory services simplify administration; any additions or changes made once to the information in the directory are immediately available to all users and directory-enabled applications, devices, and Artica.

Artica supports the use of **external LDAP database servers** or the **local OpenLDAP server** to authenticate and authorize users on a per group.

LDAP group-based authentication for Artica can be configured to support any LDAP-compliant directory

Artica also provides the ability to search for a single user in a single root of an LDAP directory information tree (DIT), and to search in multiple Base Distinguished Names (DNs).

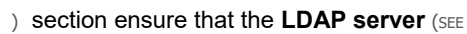
Use the Artica LDAP service.

The Artica LDAP service is an OpenLDAP server using for several services such as the proxy but also for the messaging service or the file-sharing service.

Artica offers groups and members administration like a full user's management system.

Ensure the Local LDAP service is installed

On the “**Features**” (SEE



Manager
Administrator

Dashboard

Your system

Network & NICs

DNS

Statistics

Logs center

Databases

Search a computer, a member

Monitor 14:59:51 Cpu:9.3% | Mem:36.7% 5 Members Logout

smtp.touzeau.biz

Used CPU (1 cpus)

Load

Memory used 640.63MB/1.96GB

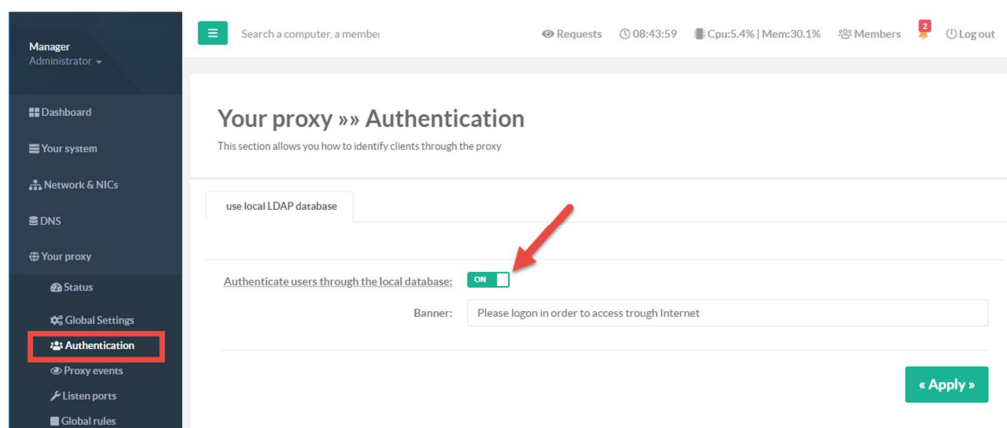
The dashboard displays three performance metrics for the host smtp.touzeau.biz from 59:5 to 00:0.

- Used CPU (1 cpus):** A line chart showing CPU usage for different processes. The y-axis ranges from 0 to 125. The x-axis shows time from 59:5 to 00:0. Processes include softirq (blue), user (red), system (orange), nice (green), and lowlat (purple). There are several spikes, notably a large one at the beginning and another around 59:50.
- Load:** A stacked area chart showing system load. The y-axis ranges from 0.0 to 0.6. The x-axis shows time from 59:5 to 00:0. The legend includes load1 (blue), load5 (red), and load15 (orange). The total load increases significantly starting around 59:20, peaking near 0.6 around 59:30.
- Memory used 640.63MB/1.96GB:** A stacked area chart showing memory usage. The y-axis ranges from 0 to 800 MB. The x-axis shows time from 59:10 to 00:0. The legend includes free (blue), used (red), cached (orange), and buffers (green). The total memory usage is consistently high, around 600-700 MB.



The LDAP server service) is installed inside the “**Members service**” section.

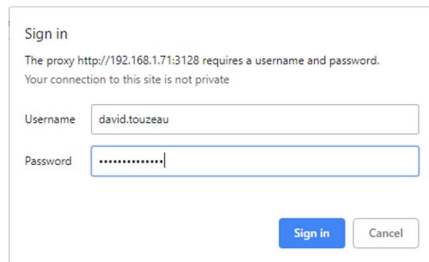
On the left menu, choose “**Your Proxy/Authentication**”, turn on the “**Authenticate users through the local database**” option.



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



Chrome authentication box (no banner displayed)



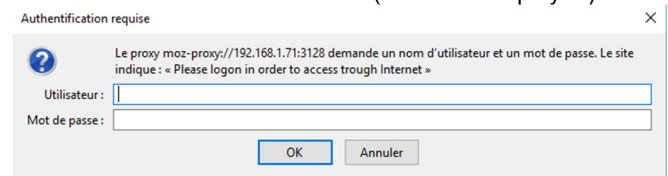
Sign in

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

Username

Password

Firefox authentication box (banner is displayed)



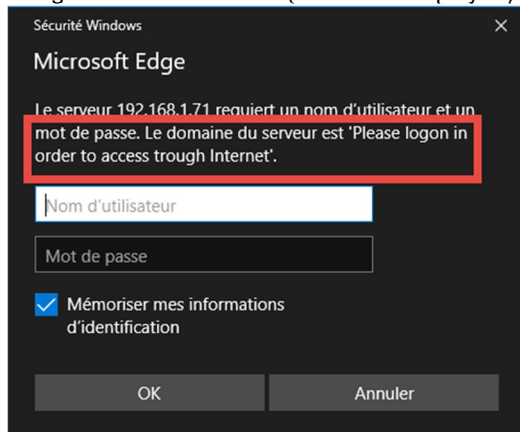
Authentification requise

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

Utilisateur :

Mot de passe :

Edge authentication box (banned is displayed)



Sécurité Windows

Microsoft Edge

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

Nom d'utilisateur

Mot de passe

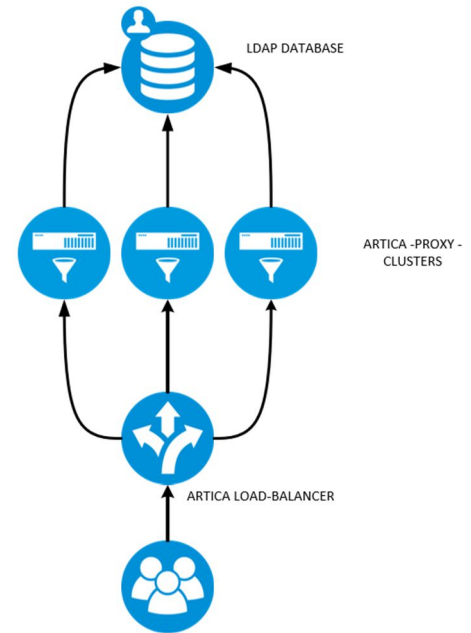
☒ Mémoriser mes informations d'identification



Use a Remote LDAP Database

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

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





)

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.



Requests 05:46:52 Cpu:2.3% | Mem:35.6% **Members** 4 Log out

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

My members

Search Go!

Search Q

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

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



RADIUS Authentication

If you have a RADIUS server, you can connect the Artica proxy to your RADIUS server in order to authenticate users before accessing the Internet.

An authentication popup will be displayed (same as LDAP authentication).

When user sends its credentials, the proxy asks to the radius if the member/password is correct.

On the left menu, choose “Your Proxy/Authentication” and click on the Radius Authentication tab.

Enable the Authenticate users with an external RADIUS server option

The screenshot shows the Artica V4 web interface. On the left, a dark sidebar menu contains various settings categories. The 'Authentication' category is highlighted with a red box. The main content area displays the 'RADIUS Authentication' configuration page. At the top, there's a dropdown menu for 'use local LDAP database' with '{RADIUSAuthentication}' selected, highlighted by a red box. Below this, a checkbox labeled 'Authenticate users with an external RADIUS server:' is checked (ON), also highlighted by a red box. The configuration fields include:

- Banner:** A text field containing 'Please logon in order to access trough Internet'.
- RADIUS server address:** A text field containing '192.168.1.3'.
- RADIUS server port:** A numeric input field with a minus sign on the left and a plus sign on the right, containing the value '1812'.
- RADIUS Identifier:** A text field containing 'proxy'.
- shared RADIUS secret:** Two password fields, each containing a series of dots to represent a hidden secret.

 At the bottom right of the configuration area, there is a green button labeled '« Apply »'.

- 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 (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.

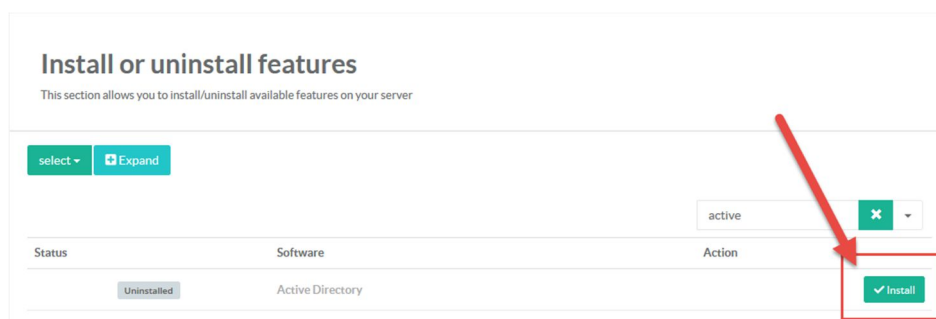
How to join Artica to your Active Directory server?

You need to follow these requirements:

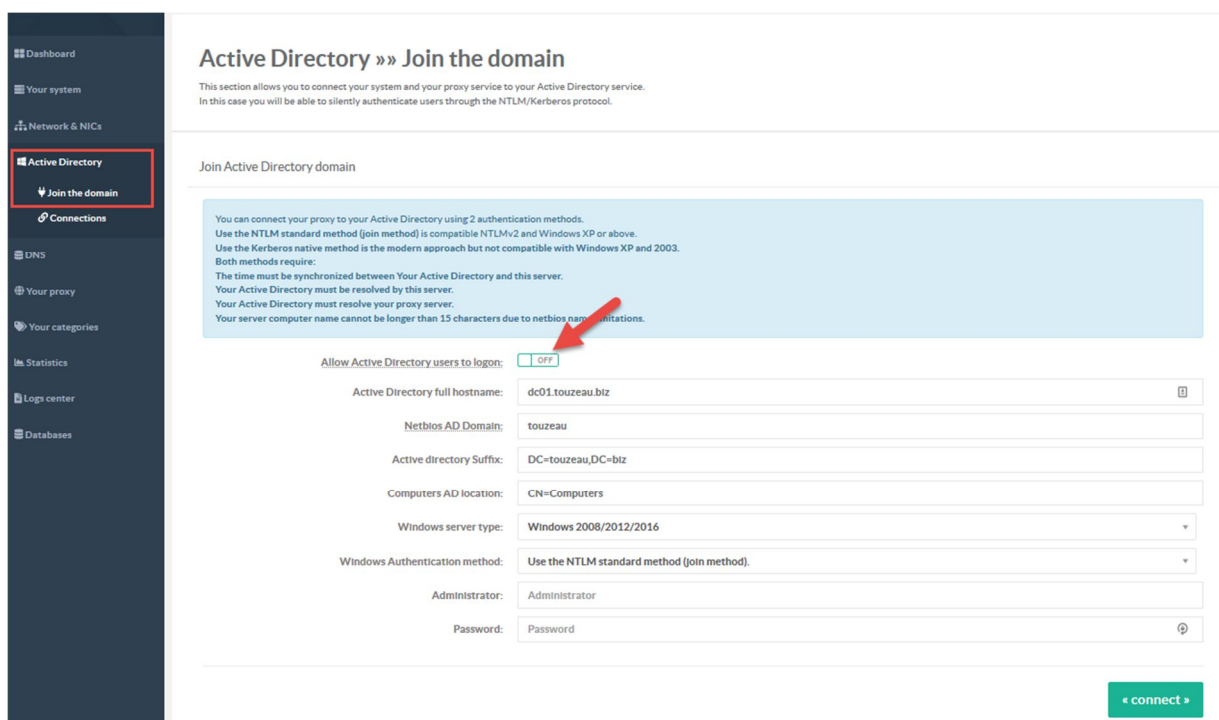
- The Artica server hostname must be fewer than 16 characters.
- The server domain name must be the same of your Active Directory domain.
- The Artica server must correctly resolve the Active Directory domain (in most cases the first DNS used by Artica is the Active Directory server).
- The time must be the same between the Artica server and the Active Directory server name.
- 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, select the “Join the domain” menu option.



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.
- **Windows Authentication method:** Which method to link Artica to the domain (see above)
- **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 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 system.

It is less secure (password is in cleartext when sniffing the network).

See (<https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-ntlm>)

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 through your Active Directory LDAP service (389 port).

Your Active Directory connection is listed here and must be “success”.

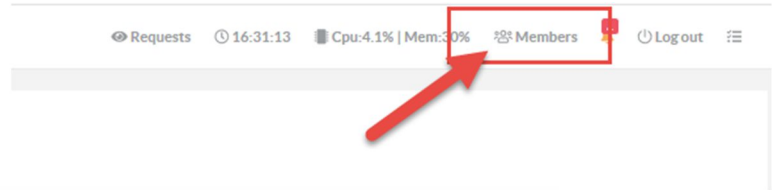
The screenshot displays the Artica Manager interface. On the left, the 'Manager Administrator' sidebar shows a menu with 'Connections' highlighted. The main content area is titled 'Active Directory LDAP connections' and includes a '+ New connection' button. Below this, a table lists existing connections. One connection is shown with the hostname '192.168.1.90 / Administrateur@touzeau.biz' and a status of 'Connection success'. A modal window is open, showing the configuration details for this connection. The modal includes fields for 'Connection ID' (0), 'hostname' (192.168.1.90), 'LDAP Server Port' (389), 'Active directory Suffix' (DC=touzeau,DC=biz), 'User name' (Administrateur@touzeau.biz), and 'Password' (masked with dots). An 'Apply' button is at the bottom right of the modal.

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.



My members

default

Search Go!

Search

Display Name	Domain	E-Mail Address	Office Phone	Groups
Administrateurs	touzeau.biz	—	—	—
Utilisateurs	touzeau.biz	—	—	—
Invités	touzeau.biz	—	—	—
Opérateurs d'impression	touzeau.biz	—	—	—
Opérateurs de sauvegarde	touzeau.biz	—	—	—
Duplicateurs	touzeau.biz	—	—	—
Utilisateurs du Bureau à distance	touzeau.biz	—	—	—
Opérateurs de configuration réseau	touzeau.biz	—	—	—
Utilisateurs de l'Analyseur de performances	touzeau.biz	—	—	—
Utilisateurs du journal de performances	touzeau.biz	—	—	—
Utilisateurs du modèle COM distribué	touzeau.biz	—	—	—
IIS_IUSRS	touzeau.biz	—	—	—

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 as 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

Sign in

The proxy http://192.168.1.155:3128 requires a username and password.
Your connection to this site is not private

Username

Password



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"
"fullhostname"=>"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";
```



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.

Realtime requests

20050 events									
Date	Members	Protocol	Category	url	INFO/LINK	Destinations	size	duration	
17:31:36	192.168.30.47	SSL Connect - Pass	SSL	Google	https://safebrowsing.googleapis.com		216.58.205.10:443	4.99 KB	4mn
17:30:58	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.60.192.7:443	3.14 KB	0.15s
17:30:58	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.60.192.7:443	3.15 KB	0.18s
17:30:58	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.60.192.7:443	3.14 KB	0.18s
17:30:58	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.60.192.7:443	3.15 KB	0.16s
17:30:57	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.60.192.7:443	3.15 KB	0.09s
17:30:57	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.60.192.7:443	3.15 KB	0.09s
17:30:57	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	—	https://static.playmedia-cdn.net		89.202.139.136:443	1.33 KB	3.1s
17:30:57	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	—	https://static.playmedia-cdn.net		89.202.139.136:443	2.18 KB	3.1s
17:30:57	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	—	https://static.playmedia-cdn.net		89.202.139.136:443	2.47 KB	3.08s
17:30:55	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	Facebook	https://staticxx.facebook.com		157.240.21.20:443	3.15 KB	0.28s
17:30:55	192.168.30.47	Not cached - Pass	GET	Google	http://imasdk.googleapis.com		216.58.209.234:80	82.14 KB	0.2s
17:30:55	192.168.30.47/dtousseau	Not cached - Pass	GET	—	http://playtv.fr		89.202.139.136:80	32.34 KB	0.1s
17:30:55	192.168.30.47/dtousseau	SSL Connect - Pass	SSL	—	https://static.playmedia-cdn.net		89.202.139.136:443	1.87 KB	0.76s

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.*

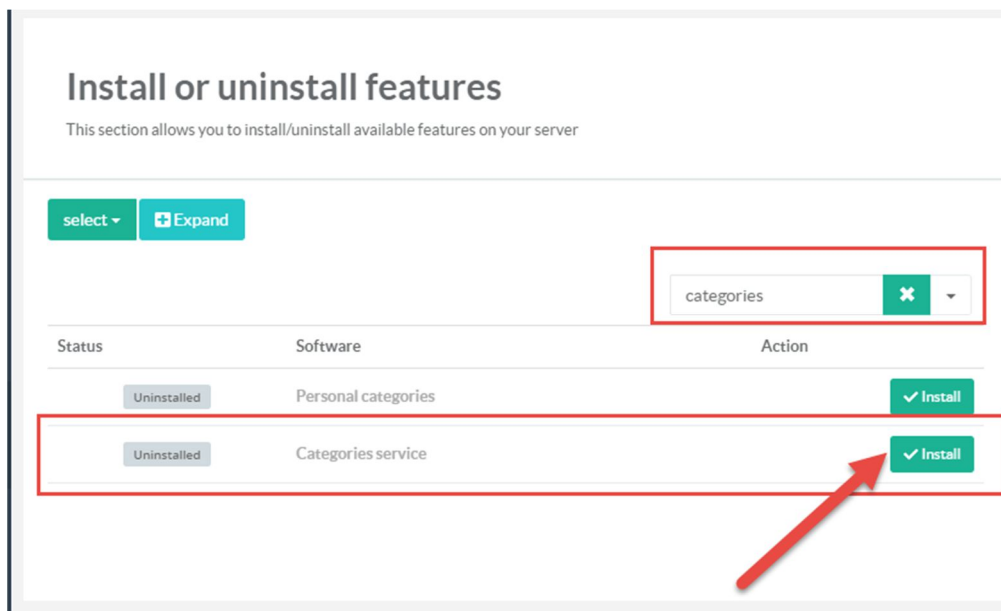
Benefits:

- 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.

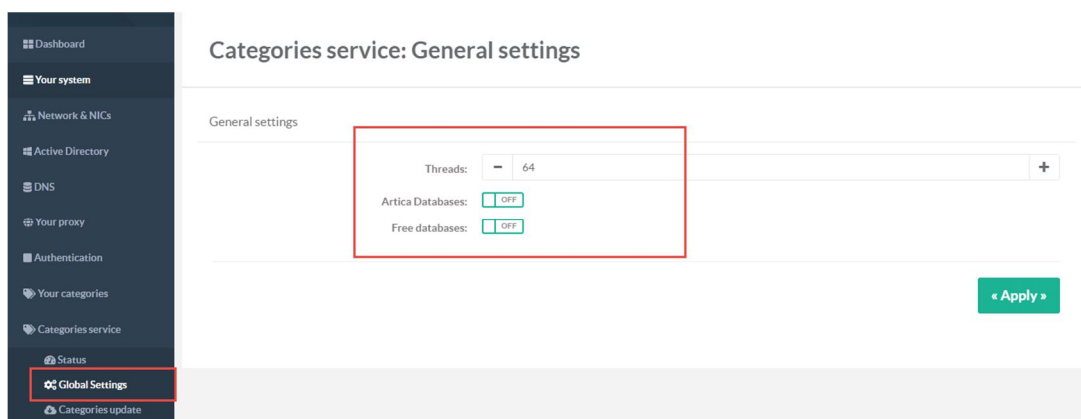
On the “**features**” section, type “**Categories**” in the search engine.

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.

Categories service v1.33.7

The categories service is not a part of the Web filtering service. It is used to provide category for each website for statistics purpose. It allows you to create specific objects in the proxy Access Control list section.

Used databases

58 / 154

Running
since 22mn 53s
Memory used: 7.22 MB

Restart

Use the search

To check a Website, use the search

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**”

Manager
Administrator

- Dashboard
- Your system
- Network & NICs
- Active Directory
- DNS
- Your proxy
- Authentication
- Your categories
- Categories service
 - Status
 - Global Settings
 - Categories update**
 - Events

Search a computer, a member

Requests 14:21:20 Cpu:11.2% | Mem:37.3% Members

Web-filtering databases

The Enterprise Edition allows you to use more than 150 categories with more than 40.000.000 categorized Internet sites. If you using the Community edition, you using 50 categories with about 1.500.000 categorized Internet sites.

Status Update settings **Schedule** Update events

Delete databases **Update**

	Status	Category	Type	Items	Size	Version	Updated On
Updated		Abortion	Artica	6 258	28 KB	2018 Sunday October 28 15:52:28	2018 Sunday October 2
Updated		Advertising	Artica	159 511	716.18 KB	Yesterday 06:45:45	Yesterday 22:15:17
Updated		Aggressive	Artica	25	0.31 KB	2018 Sunday October 28 15:52:29	2018 Sunday October 2
Updated		Akamai	Artica	7 217	15.18 KB	2018 Sunday October 28 15:52:42	2018 Sunday October 2
Updated		Alcohol	Artica	47 173	242.23 KB	2018 Sunday October 28 15:52:31	2018 Sunday October 2
Updated		Amazonaws	Artica	37 515	82.41 KB	2018 Sunday October 28 15:52:41	2018 Sunday October 2



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).

Install or uninstall features

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

select ▾ Expand

categories ✕ ▾

Status	Software	Action
Uninstalled	Personal categories	✓ Install
Installed	Categories service	✓ uninstall

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 be the same in official's categories.

If you want to remove official's categories, go into “Your Categories” and parameters, enable the checkbox “**Hide official's categories in the main list.**”

+ New category Restore backup Compile all categories Remove all categories

Categories	Description
Cheater (Free Edition)	Sites which are designed to explain cheating on exams.
D-DOS (Free Edition)	Websites providing information about ddos attacks
Dating (Free Edition)	Dating, matching site for single person
Dialers (Free Edition)	Websites providing information about dialers
Downloads (Free Edition)	Download manager
Drugs (Free Edition)	Sites relative to drugs.
Educational Games (Free Edition)	Websites provides online games for education

Give the **category name** and the **description**.

The “**Shared**” category allows your members to add/remove items inside this category.



New category

New category

Category name:

Description:

Shared category:

☐ OFF

« add »

After creating your category, search it inside the table and click on it.

Your categories

Personal categories feature allows you to create your own web-filtering categories in order to modify the web-filtering behavior or increase Web-filtering detection rate.

+ New category

Restore backup

Compile all categories

Remove all categories

acme

Categories	Description	Size	Items
acme_cat	Enterprise category		0

- 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....)

Category: acme_cat

acme_cat: Add websites

acme_cat » Add websites

Enterprise category

Add here websites separated by a carriage return.

Note that you just have to add the main website instead of using the full qualified web server name.

Instead of set sub.domain.tld, you can add just domain.tld.

Do not add any special characters such as *,+,...

Force:

ON

Disable extension checking:

OFF

Web sites:

1 kollektive.com
2 forum-dsi.com
3 normandiecybersecurite.com
4 netsecure-day.fr
5 nkinformatics.fr
6 9atom.org
7 9front.org
8 helenos.org
9 ingecap.fr
10 3v4l.org
11 compartilhando.ti.com.br
12 etechconsulting-mg.com
13 ajaibpt.com
14 ajaibttv.com
15 sysvision.fr

« Add websites »

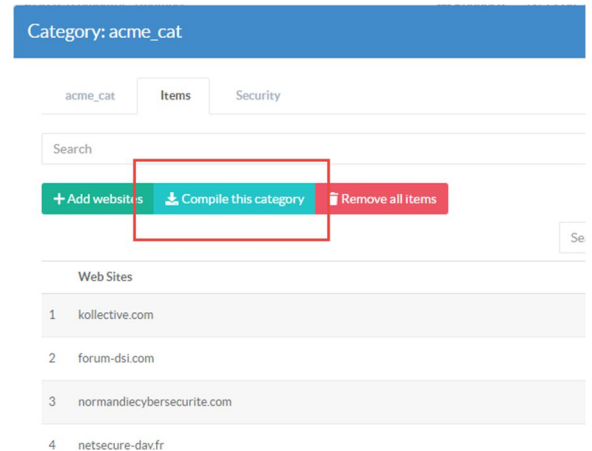


Compiling your categories.

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

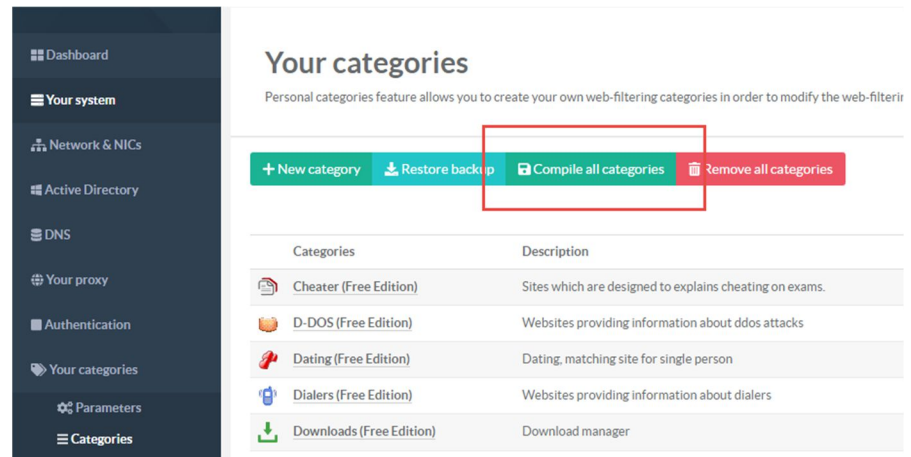
On the category section, click on the button **"Compile this category"**. Artica will compile your category and reconfigure your category service and reload your Web-filtering service.



Compiling all categories

On the list of all available categories, click on the button **"Compile all categories."**

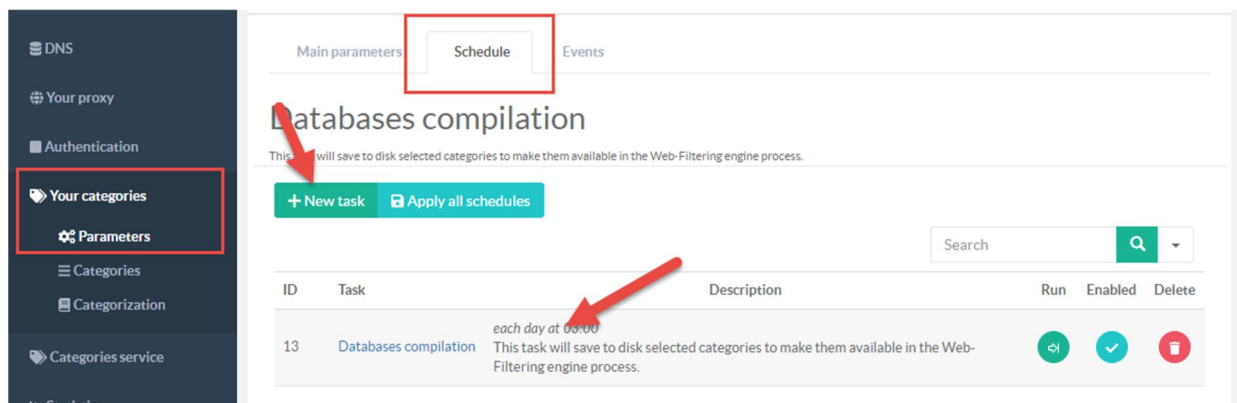
This task compiles all categories even though there are not changes in your categories.



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.





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 request 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.

Your proxy Categorization

This section allows you to enable websites categorization. Websites categorization allows you to get category according to a visited website. Categories can be used to build proxy ACLs. You can use the Artica Cloud datacenters. And/Or use an installed Categories service in your network.

Status Parameters **Not categorized** Users requests

Analyze

Search

Date	Domains	Hits
2018 Monday October 29	massivefictions.com	1
2018 Monday October 29	1f300.com	1
2018 Monday October 29	sendinblue.fr	1
2018 Monday October 29	verified-reviews.com	1
2018 Monday October 29	sendibm3.com	1
2018 Monday October 29	sendibt1.com	1

This section is available by RESTful API (see above).



RESTful API for categories

You can offer RESTful API in order to Add/remove/compile your categories.
In this case, any software compatible with RESTful will be able to maintain your categories in your Artica server.

Enable the RESTful service for categories.

On the left menu, choose “Your categories” and “Parameters.”

Your categories Parameters

Personal categories feature allows you to create your own web-filtering categories in order to modify the web-filtering behavior or increase Web-filtering detection rate.

Main parameters | Schedule | Events

RESTful API KEY

Enable the feature: ☐ OFF

API Key: gsZ8mlXUWNnJ6F5tL0EE0yUbOMuSYwG00FDlInpfDX45mb17MSeeARji9rASb7uQ

1. On the Main parameters, turn on the “**Enable feature**” on the RESTful API KEY section.
2. Change or validate the API Key defined.
3. After Apply the configuration, you can use these commands to manage your categories.

RESTful commands for categories.

List available categories

```
GET https://192.168.1.1:9000/api/rest/category/list
```

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: HgMQCyArV2814wroleCU4UHL";
$MAIN_URI="https://192.168.1.1:9000/api/rest/category/list";

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);

$response = curl_exec($ch);
$errno=curl_errno($ch);
if($errno>0){ echo "Error $errno\n".curl_error($ch)."\n$response\n"; curl_close($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, retrieve the list of categories\n-----\n";

foreach ($json->categories as $category_id=>$line){
    //NAME category Name, KEY: Category Key
    echo "[ID:$category_id]: {$line->NAME}, ({$line->KEY})\n";
}
```



Create a new category

```
POST https://192.168.1.1:9000/api/rest/category/add
Field: name: Name of category
Field: desc: Description of the category
Return array: status (true/false), message (message error), category_id ( new category ID)
```

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: HgMQCyRV2814wro1eCU4UHL ";
$MAIN_URI="https://192.168.1.1:9000/api/rest/category/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);

$POSTz=array("name"=>"My New category","desc"=>"This is my description");
curl_setopt($ch, CURLOPT_POSTFIELDS, $POSTz);

$response = curl_exec($ch);
$errno=curl_errno($ch);
if($errno>0){ echo "Error $errno\n".curl_error($ch)."\n$response\n"; curl_close($ch); die(); }
$CURLINFO_HTTP_CODE=intval(curl_getinfo($ch,CURLINFO_HTTP_CODE));
if($CURLINFO_HTTP_CODE<>200){
    echo "Error $CURLINFO_HTTP_CODE\n";
    $json=json_decode($response);
    if(!$json->status){echo "Failed $json->message\n";die();}
    die();
}
$json=json_decode($response);
if(!$json->status){echo "Failed $json->message\n";die();}

echo "New category id $json->category_id created...\n";
```



Categorize a Web site “oep.org.bo” into the category “My new Category” ID 223

```
GET https://192.168.1.1:9000/api/rest/category/223/oep.org.bo
```

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: HgMQCyaRV2814wroleCU4UHL ";
$MAIN_URI="https://192.168.1.1:9000/api/rest/category/223/oep.org.bo";

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);

$response = curl_exec($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==503){
    // Already categorized, get the current category in json
    $json=json_decode($response);
    echo "Already categorized Category id $json->category_id\nServer said: $json->message\n";
    exit;
}

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

Move Website oep.org.bo from category number 223 to category number 228

```
GET https://192.168.1.1:9000/api/rest/category/228/oep.org.bo/223
```

Delete Website oep.org.bo from category number 228 (put 0 after /category/)

```
GET https://192.168.1.1:9000/api/rest/category/0/oep.org.bo/228
```



List last 250 Websites from category number 223

```
GET https://192.168.1.1:9000/api/rest/category/223/list
```

List last 250 Websites from category number 223 where websites like *.com.br

```
GET https://192.168.1.1:9000/api/rest/category/223/list/.com.br
```

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: HgMQCyaRV2814wroleCU4UHL";

$MAIN_URI="https://192.168.1.1:9000/api/rest/category/223/list/.com.br";

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);

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

if(!$json->status){
    echo "Status Return, Failed with message: $json->message\n";
    die();
}

$count=$json->count;
for($i=0;$i<$json->count;$i++){
    echo "site:".$json->sites[$i]."\n";
}

echo "Success\n";
```




Get the category of oep.org.bo

```
GET https://192.168.1.1:9000/api/rest/category/get/oep.org.bo
```

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: HgMQCyaRV2814wroleCU4UHL ";
$MAIN_URI="https://192.1368.1.1:9000/api/rest/category/get/oep.org.bo";

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);

$response = curl_exec($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==404){
    echo "Not categorized $json->message\n";
    exit;
}

if($CURLINFO_HTTP_CODE<>200){
    echo "Error $CURLINFO_HTTP_CODE\n";
    $json=json_decode($response);
    if(!$json->status){echo "Failed $json->message\n";die();}
    die();
}
$json=json_decode($response);
if(!$json->status){echo "Status Return, Failed with message: $json->message\n";die();}
echo "Success Category:$json->category_id message from server: $json->message\n";
```

Compile all categories

```
GET https://192.168.1.1:9000/api/rest/category/compile
```

Compile only category 228

```
GET https://192.168.1.1:9000/api/rest/category/compile/228
```



Get the list of last 250 uncategorized websites (order by hits)

```
GET https://192.168.1.1:9000/api/rest/category/uncategorized
```

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: HgMQCyaRV2814wro1eCU4UHL";
$MAIN_URI="https://192.168.1.1:9000/api/rest/category/uncategorized";

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);

$response = curl_exec($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";
    $json=json_decode($response);
    if(!$json->status){echo "Failed $json->message\n";die();}
    die();
}
$json=json_decode($response);
//Get the number of items;
$items=$json->count;
echo "$items elements\n";

for($i=0;$i<$items;$i++){
    $sitename=$json->websites[$i]->SITENAME;
    $requests=$json->websites[$i]->RQS;
    $saved_date=$json->websites[$i]->DATE;
    echo "$sitename saved on $saved_date requests:$requests\n";
}
```

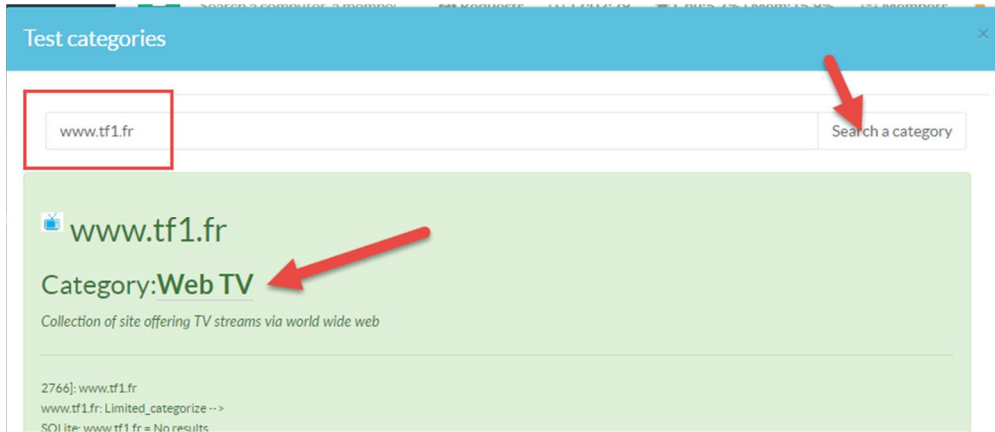
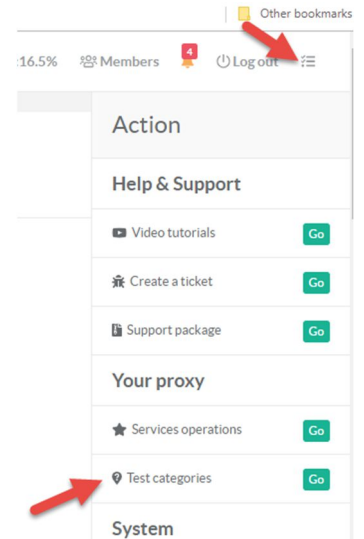


Testing categories

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

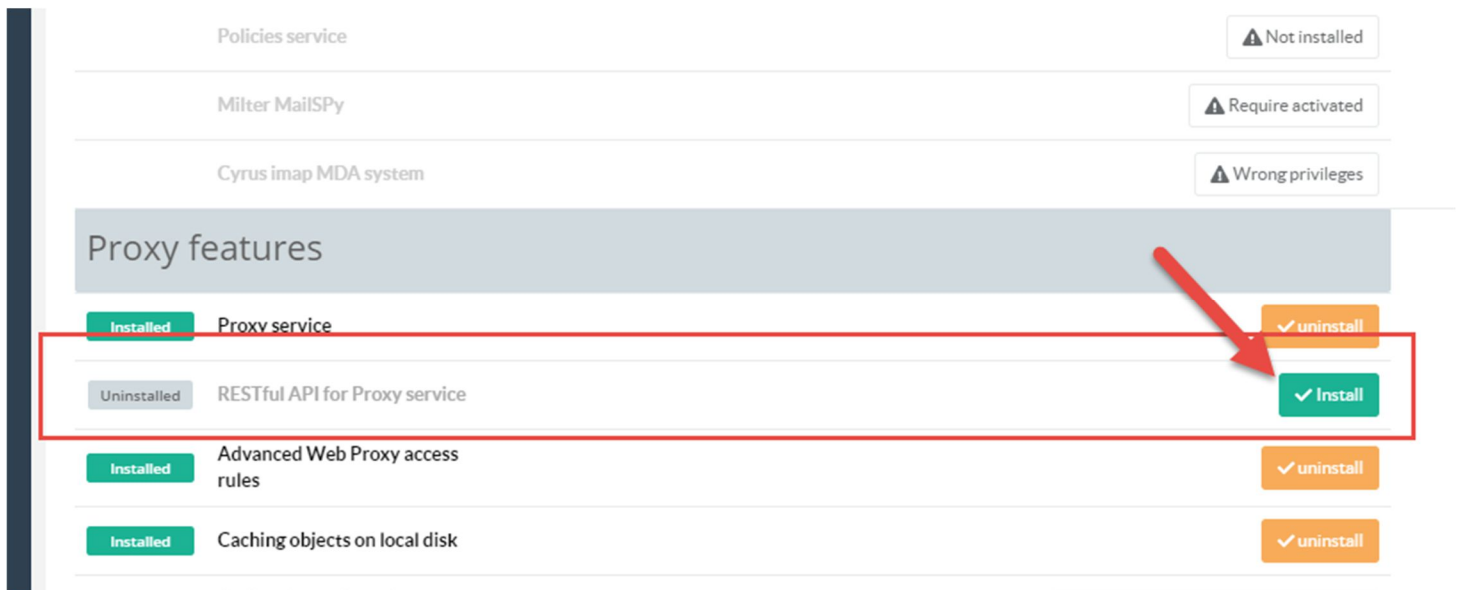
It allows you to ask which category is associated with the queried domain.



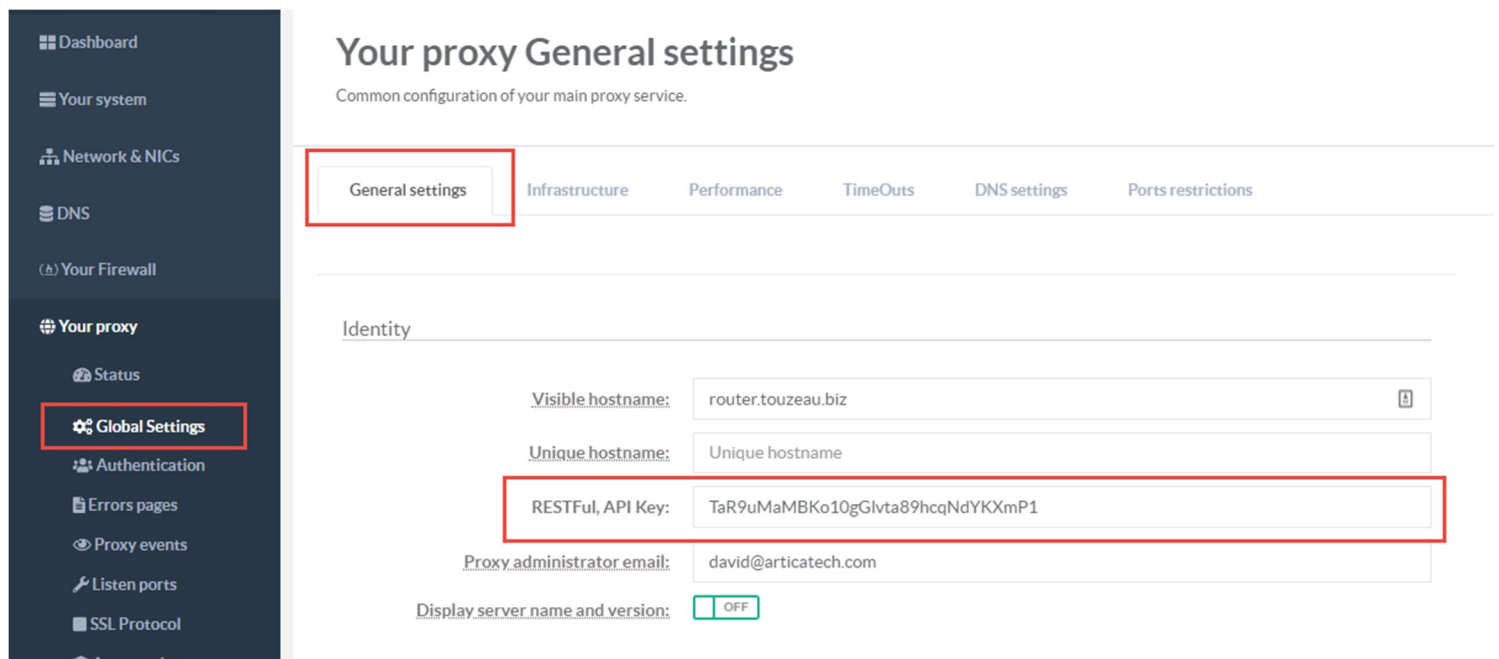


PROXY RESTFUL API

If you want to manage proxy features using RESTful API, you need to install the RESTful API under the features. (THE REST API SERVICE IS AVAILABLE WITH ENTERPRISE EDITION).



After the RESTful API for proxy service installed, on the left menu, go to “**Your Proxy**”, “**Global Settings**.” A field “**RESTful, API key**” is displayed and allows you to modify the default API key to manage your server.



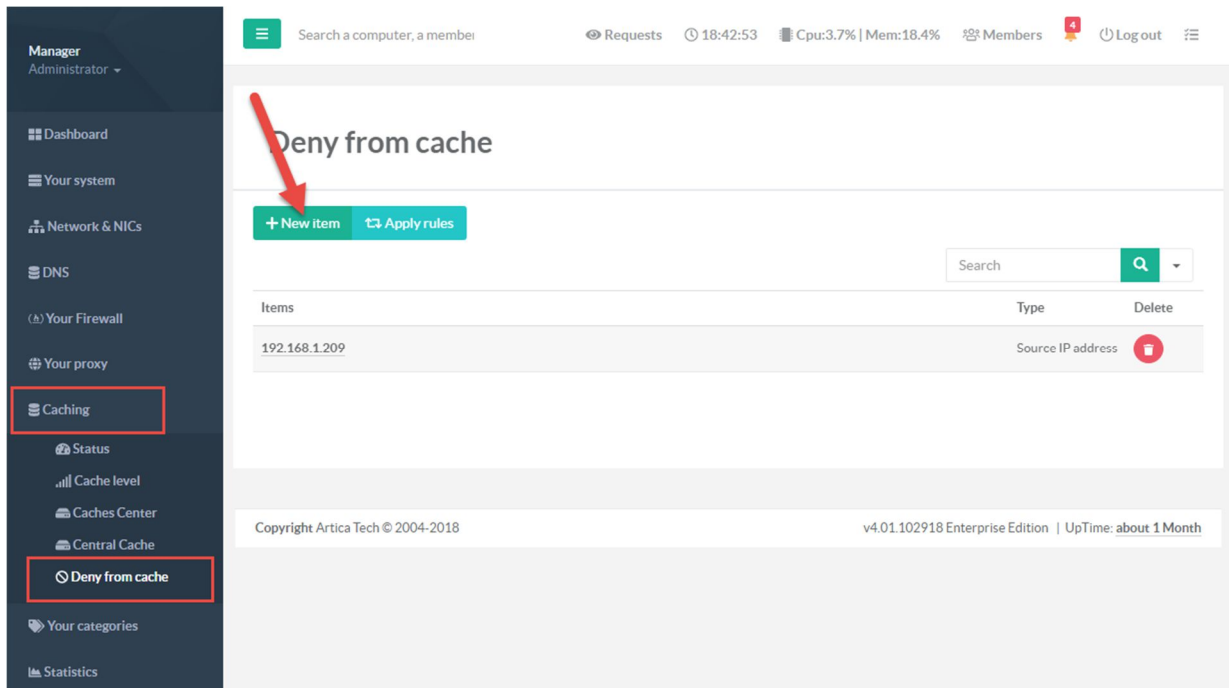


CACHING

Exclude from caching

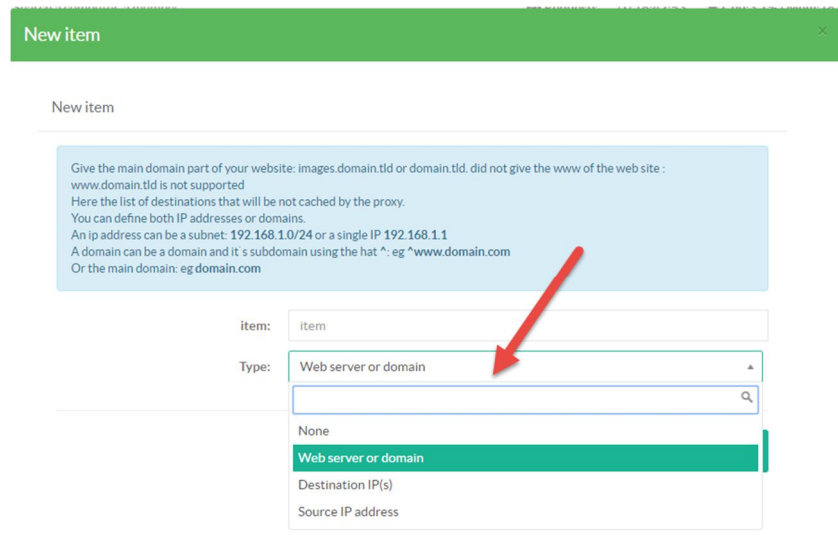
In some cases, you need to exclude the proxy to store objects from its cache according items.

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.





RESTful API:

If the RESTful API is enabled for the Proxy service, you can use these commands to manage the “No cache section”
The RESTful api needs to add the ArticaKey: API Key in the HTTP request header

List “Deny cache rules”

```
GET https://192.168.1.1:9000/api/rest/proxy/cache/deny/list
```

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: TaR9uMaMBKo10gGlvta89hcqNdYKXmPl";
$MAIN_URI="https://192.168.1.1:9000/api/rest/proxy/cache/deny/list";

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);

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

foreach ($json->results as $index=>$line){
    echo "[ $index]: { $line->items}, ({$line->ztype})\n";
}
```

Add a new deny cache rule

```
GET https://192.168.1.1:9000/api/rest/proxy/cache/deny/add/[TYPE]/[item]
```

Where [TYPE] is an integer of

- 0: A destination domain
- 1: A destination IP address or CDIR.
- 2: A source IP address or CDIR

And [item] is the value.

Example: do not cache **clubic.com** website

```
GET https://192.168.1.1:9000/api/rest/proxy/cache/deny/add/0/clubic.com
```

Example: do not cache 23.38.11.195 public IP address

```
GET https://192.168.1.1:9000/api/rest/proxy/cache/deny/add/1/23.38.11.195
```

Delete a deny cache rule:

```
GET https://192.168.1.1:9000/api/rest/proxy/cache/deny/del/[item]
```

Where [item] is the IP address or the domain to remove.

Apply deny cache rules to the proxy server and make them in production

```
GET https://192.168.1.1:9000/api/rest/proxy/cache/deny/apply
```



REALTIME STATISTICS.

It is important to know what's happening in the Internet flow. If need to answer about who using the proxy now, what bandwidth is used, what is the website using the bandwidth...

Enable the Realtime statistics

To enable the realtime statistics, you need to install the Persistent Key-value database service and the

- On the feature section, in the search field, type the **Persistent** word
- Click on Install button on the **Persistent key-value DB** row.

Install or uninstall features

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

Status	Software	Action
Uninstalled	Persistent key-value db	Install

- Search the field **"Proxy events"**
- Click on **install** button on the **"Proxy Events listener"** row

Install or uninstall features

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

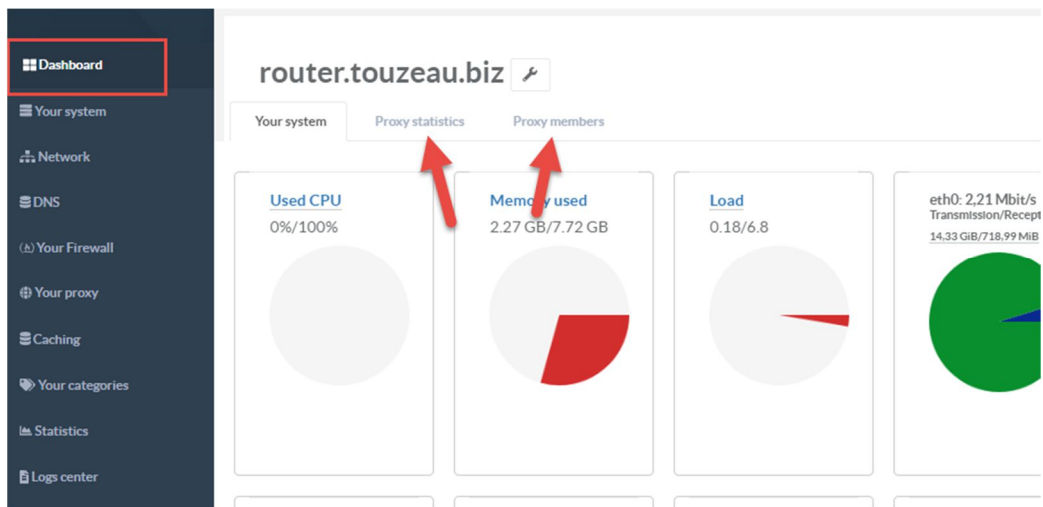
Status	Software	Action
Uninstalled	Proxy events listener	Install

Display proxy statistics

This feature groups statistics each 10minutes, after installing the 2 features, wait about 10minutes.



- On the Dashboard, you will see new tabs: **Proxy statistics** and **Proxy Members**



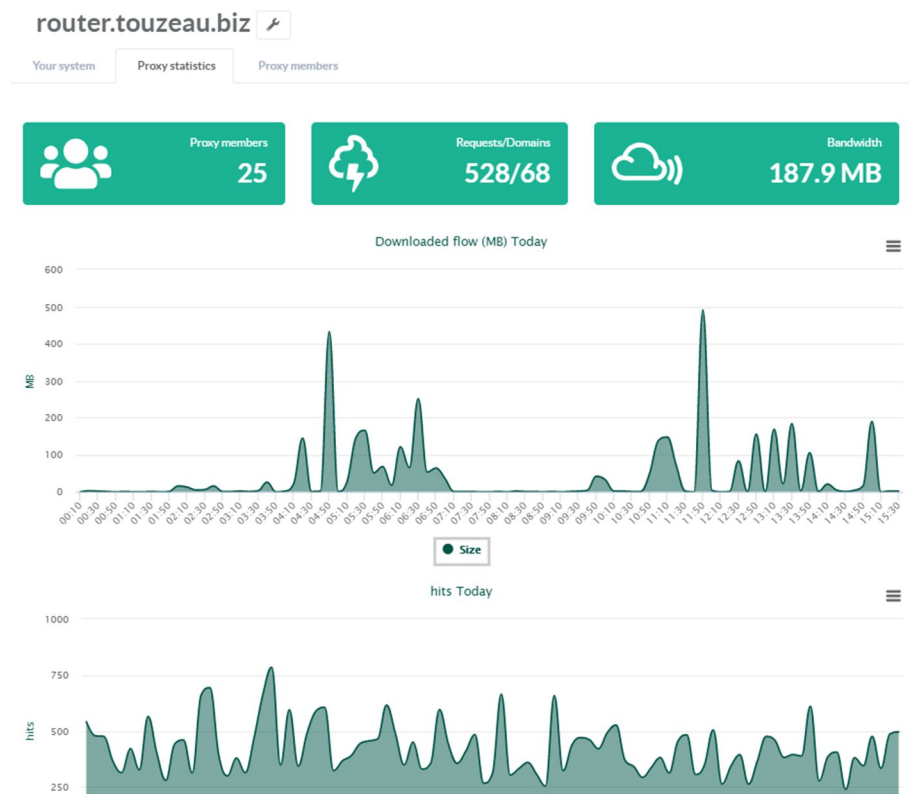
Proxy Statistics

The 3 green box shows you for a period of **10 minutes**:

- The number of Members that using your proxy service
- The number of requests and visisted domains.
- The bandwidth usage.

3 graphs are displayed for the current day.

- The bandwidth usage each 10minutes.
- The number of requests each 10minutes.
- The number of users using the proxy each 10mn



Proxy Statistics: RESTFul API

Produce data to build current day bandwidth,requests, members data

```
GET https://192.168.1.1:9000/api/rest/proxy/stats/today
```

Produce information of the 10 minutes period.

```
GET https://192.168.1.1:9000/api/rest/proxy/stats/status
```




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.

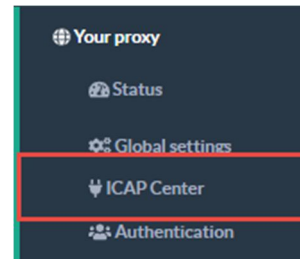
ICAP concentrates on leveraging edge-based devices (caching proxies) to help deliver value-added services.

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.



ICAP Center

This section allows you to connect services around your proxy server using the ICAP protocol such as antivirus, web filtering...

+ New service		Apply		Search					
Status	Order	Daemon Name	Address	Mode	Bypass	Move	Enabled	Delete	
Disabled	0	C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmo _d _precache	☒	↑ ↓	☐	—	
Disabled	0	C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmo _d _precache	☐	↑ ↓	☐	—	
Disabled	0	C-ICAP Antivirus - REMOTE - RESPONSE	10.20.0.2:1345	respmo _d _precache	☐	↑ ↓	☐	—	
Disabled	0	C-ICAP Antivirus - REMOTE - REQUEST	10.20.0.2:1345	reqmo _d _precache	☐	↑ ↓	☐	—	
Disabled	0	Kaspersky Antivirus - LOCAL - REQUEST	127.0.0.1:1344	reqmo _d _precache	☐	↑ ↓	☐	—	
Disabled	0	Kaspersky Antivirus - LOCAL - RESPONSE	127.0.0.1:1344	respmo _d _precache	☐	↑ ↓	☐	—	



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 of the listen port (1344 by default), the path to request modification and the path to response modification service

Settings

ICAP server

ICAP server address: 0.0.0.0 : 1344

Maximum connections over the ICAP protocol: 5000
The valid range is from 1000 up to 10000 inclusive

Header with the client IP address: X-Client-IP

Header containing user name: X-Client-Username
☐ User name in Base64 encoding
Enable this option, if proxy server sends user names in Base64 encoding

Path to request modification service: av/reqmod

Path to response modification service: av/respmo

Start to transfer HTTP messages before their scanning is complete: ☐ Disabled
Downloading of the banned object will be aborted without describing a reason: neither a Deny page nor a Redirect page will be displayed

Skip the HTTP CONNECT method check: ☒ Enabled
If you choose skipping the HTTP CONNECT method check, the traffic redirect and access deny templates will be disabled

Save **Cancel** [Set default values](#)

On Artica, search the Kaspersky Antivirus – REMOTE REQUEST and Kaspersky Antivirus – REMOTE RESPONSE
Click on each service.

ICAP Center

This section allows you to connect services around your proxy server using the ICAP protocol such as antivirus, web filtering...

[+ New service](#) [Apply](#)

Search

Status	Order	Daemon Name	Address	Mode	Bypass	Move	Enabled	Delete
Disabled	0	C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmo_precache	☒	↑ ↓	☐	—
Disabled	0	C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	C-ICAP Antivirus - REMOTE - RESPONSE	10.20.0.2:1345	respmo_precache	☐	↑ ↓	☐	—
Disabled	0	C-ICAP Antivirus - REMOTE - REQUEST	10.20.0.2:1345	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - LOCAL - REQUEST	127.0.0.1:1344	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - LOCAL - RESPONSE	127.0.0.1:1344	respmo_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - REMOTE - RESPONSE	10.20.0.2:1344	respmo_precache	☐	↑ ↓	☐	—
Disabled	0	Orfeo Web filtering - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	WebSense Web filtering - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	Proventia Web Filter - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	C-ICAP Web Filtering - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precache	☐	↑ ↓	☐	—



Turn ON the **Enabled** option and modify the **Address** to the IP address used by your Kaspersky Web traffic Security server.
Click on **Apply**

Kaspersky Antivirus - REMOTE - RESPONSE

Daemon name: Kaspersky Antivirus - REMOTE - RESPONSE

Enabled: ☒

Order: 0

Address: 192.168.1.54

listen port: 1344

ICAP Service name: av/respmod

type: RESPMOD

If overloaded: Bypass

X-Next-Services: ☒

Bypass: ☐

Max connections: 100

« Apply »

After modify the 2 entries, click on Apply button on the main table to link your proxy to enabled ICAP services.

ICAP Center

This section allows you to connect services around your proxy server using the ICAP protocol such as antivirus, web filtering...

Refresh + New service Apply

Search

Status	Order	Daemon Name	Address	Mode	Bypass	move	Enabled	Delete
Disabled	0	C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmod_precache	☒	↑ ↓	☐	—
Disabled	0	C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	C-ICAP Antivirus - REMOTE - RESPONSE	10.20.0.2:1345	respmod_precache	☐	↑ ↓	☐	—
Disabled	0	C-ICAP Antivirus - REMOTE - REQUEST	10.20.0.2:1345	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - LOCAL - REQUEST	127.0.0.1:1344	reqmod_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - LOCAL - RESPONSE	127.0.0.1:1344	respmod_precache	☐	↑ ↓	☐	—
Disabled	0	Kaspersky Antivirus - REMOTE - REQUEST	192.168.1.54:1344	reqmod_precache	☐	↑ ↓	☒	—
Disabled	0	Kaspersky Antivirus - REMOTE - RESPONSE	192.168.1.54:1344	respmod_precache	☐	↑ ↓	☒	—
Disabled	0	Olfeo Web filtering - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precache	☐	↑ ↓	☐	—

After few seconds, status must be turned to "Active"

ICAP Center

This section allows you to connect services around your proxy server using the ICAP protocol such as antivirus, web filtering...

Refresh + New service Apply

Search

Status	Order	Daemon Name	Address	Mode	Bypass	move	Enabled	Delete
Active	1	Kaspersky Antivirus - REMOTE - RESPONSE	192.168.1.54:1344	respmod_precache	☒	↑ ↓	☒	—
Active	2	Kaspersky Antivirus - REMOTE - REQUEST	192.168.1.54:1344	reqmod_precache	☒	↑ ↓	☒	—
Disabled	3	C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmod_precache	☒	↑ ↓	☐	—
Disabled	4	C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precache	☐	↑ ↓	☐	—
Disabled	5	C-ICAP Antivirus - REMOTE - RESPONSE	10.20.0.2:1345	respmod_precache	☐	↑ ↓	☐	—



KASPERSKY WEB TRAFFIC SECURITY

Kaspersky Web Traffic Security is a solution (hereinafter also referred to as "application") for protecting HTTP, HTTPS, and FTP traffic passing through your Artica proxy server using the ICAP protocol.

The application protects users of a corporate network when accessing Internet resources.

For example, it deletes malware and other threats from the data stream that enters the corporate network via the HTTP(S) and FTP protocols, blocks infected and phishing websites, and controls access to Internet resources based on Internet resource categories and content types.

The application has been developed for corporate users.

Features

- Protects the IT infrastructure of your organization from most **modern malware and encrypting ransomware** thanks to **machine-learning algorithms** and operating system data emulation technology.
- Blocks access to **infected** and **phishing** websites.
- Uses Kaspersky Security Network data to obtain information about the **reputation of files** and Internet resources, ensure that Kaspersky Lab applications react to threats faster without waiting for an application database update, and reduce the likelihood of false positives.
- Performs **content filtering of incoming and outgoing files** based on the **URL**, file name, MIME type, size, type of source file (the application can determine the true format and type of the file, regardless of its extension), and checksum (MD5 or SHA256).
- Lets you **restrict access** to various **categories** of Internet resources, for example: Gambling, lotteries, sweepstakes; Adult content; Internet for children; Prohibited by legislation of the Russian Federation.
- Lets you **monitor** the application operating status, the network traffic processed by the application, the number of scanned and detected objects, most recent threats, blocked users and URLs in the application web interface.
- Lets you **create workspaces** for configuring individual rules for processing traffic of departments of organizations or managed organizations (for Internet service providers).
- Lets you configure **access permissions of administrators** for working with managed organizations.
- Adjusts **traffic processing conditions** in cases when traffic processing does not match the defined rules.
- Integrates with **Microsoft Active Directory** to assign roles and manage access and protection rules. Supports NTLM- and Kerberos authentication in Active Directory for access to the web interface.
- Publishes application events to a **SIEM** system that is already in use in your organization over the Syslog protocol. Relays information about each event as a separate syslog message in CEF format.
- Lets you access application information over the **SNMP** protocol.

Kaspersky Web Traffic Security is compliant with the **General Data Protection Regulation** (GDPR) and applicable European Union laws on confidential information, personal data, and data protection

Install Kaspersky Web traffic Security

To install Kaspersky Web Traffic Security, you need:

- A valid Kaspersky License (serial number)
- Install the **Nginx Web service**.

Downloading the package from your Artica server



THE FIREWALL

MANAGE ITEMS

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

A search engine (the first search field) allows you to find the item.

The interface list is limited to 150 rows, if your item is not displayed in the first rows you have to use the search engine.

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

Bulk importation.

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

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

The top screenshot shows the 'Items - Group: Mes addresses IP' interface. It has a search bar with '192.168.1*' and a 'Go!' button. Below the search bar are '+ New item' and 'Import' buttons. A table lists items with columns: Date, Items, Members, Enable, and Delete. The table contains two rows: one for '2018 Tuesday October 09 11:31:52' with item '98.25.1.4' and another for '192.168.1.10'. The bottom screenshot shows the 'Import - Group: Mes addresses IP' dialog box. It contains a message: 'Click on browse button in order to import a text file with each item separated by a carriage return.' and an 'Upload a File' button.



Find a rule based on an item

The global search engine on the firewall-rule list allows you to find a rule according to a defined item.

The wildcard is supported, if you need to find a specific IP string or subnet, the table will display rules that stores the group with the desired item.

Firewall Rules

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

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



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 combining 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 checks 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

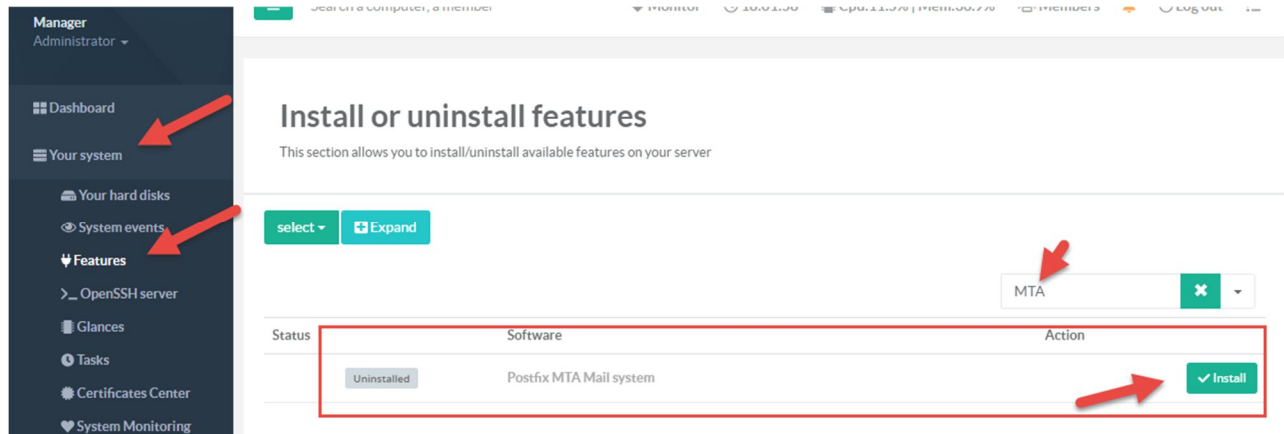
The administrator can keep control of all system settings. Detailed traffic and filtering reports give the administrator a clear vision of network and mail activity.



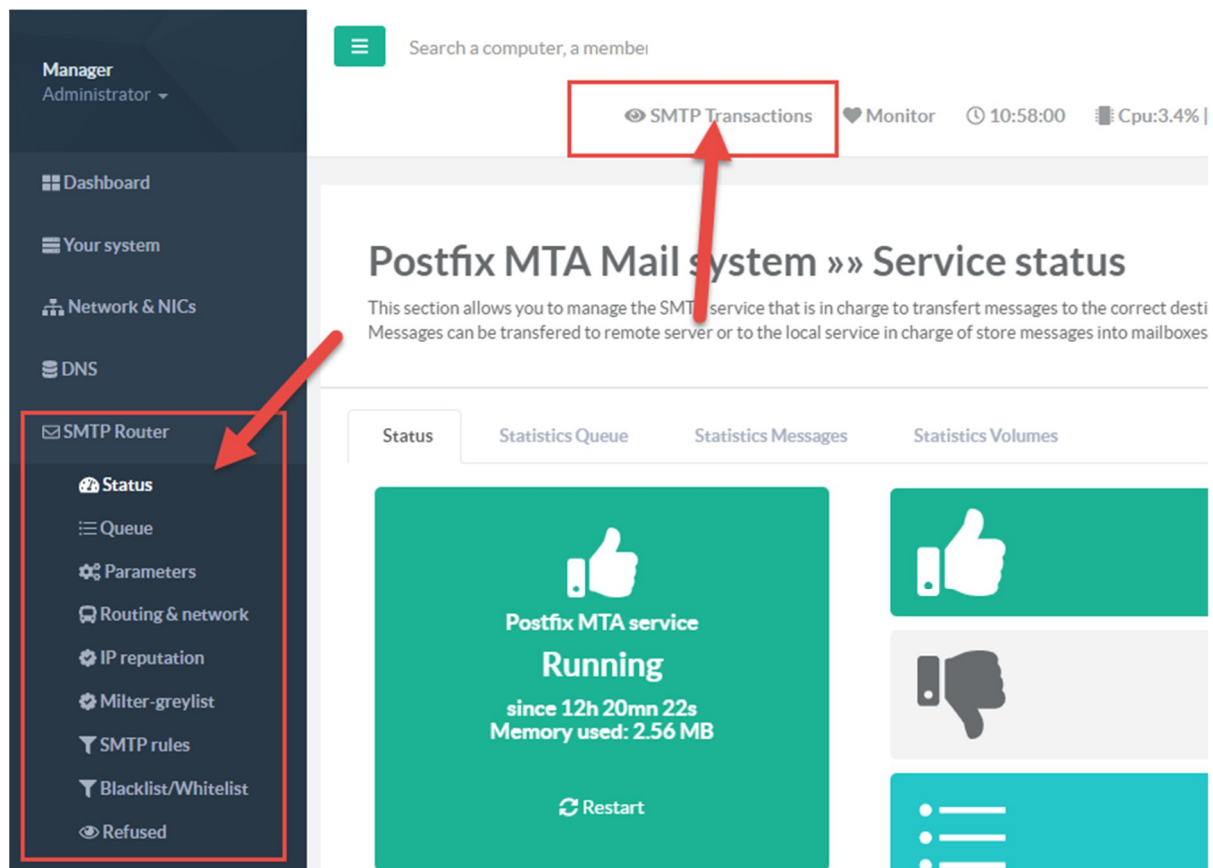
INSTALL THE SMTP SERVICE

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.





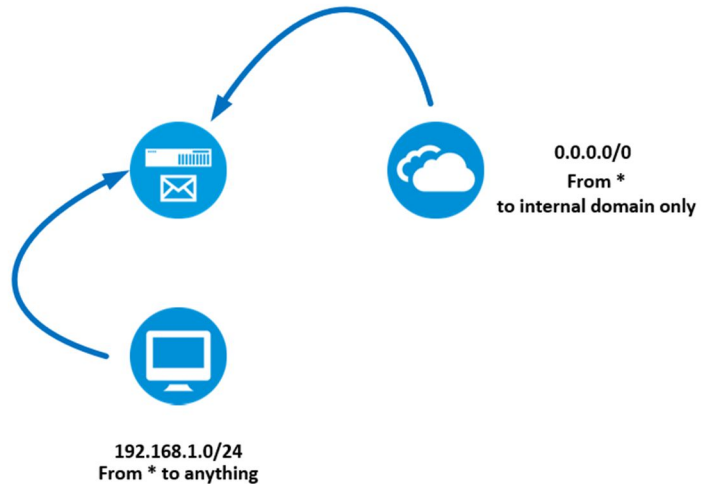
First step, set your authorized networks.

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**, select 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**, select the “**Routing**” tab.

This section instruct 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 recipient:

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 field 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.

Routing tables v3.3.1

Routing tables allows you to create rules in order to forward message to a next hope messaging server according destination domains, senders or recipient

Reconfiguring: 100% Done [«Details»](#)

Reconfiguring - 100% Done

Routing

What clients to relay mail from ?

+ New Rule

+ New Blind carbon copy

Apply configuration

Direction	Item	Forward To
Inbound	acme.corp	(smtp) 19.168.1.113:25

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.

Routing table:: artica.fr

Parameters Identical domains

Domains

Domains that use same parameters of the original set

1 acmi.corp
2 mail.lan
3 outgoing.fr

« Apply »



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 password of the user with "Send As permission"

Routing rule: acme.corp

Routing rule: acme.corp

Reject unverified recipient: ☐ OFF

Enabled: ☒ ON

Direction: Inbound

Service: SMTP

SMTP server address: 192.168.1.113

Port: 587

Transport Layer Security

Opportunistic TLS mode: ☒ ON

SMTP TLS security level: Mandatory TLS encryption

authenticate

Enabled: ☒ ON

User name: artica

Password: *****

Apply



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 "Outbound" 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.

Routing table: New entry

Routing rule: New *

Destination domain or recipient: *

Reject unverified recipient: ☐ OFF

Enabled: ☒ ON

Direction: Outbound

Service: SMTP

SMTP server address: 212.25.56.32

Port: 25

Transport Layer Security

Opportunistic TLS mode: ☐ OFF

SMTP TLS security level: None

authenticate

Enabled: ☒ ON

User name: mailboxrelay

Password: *****

« add »

Routing tables v3.3.1

Routing tables allows you to create rules in order to forward message to a next hope messaging server according destination domains, senders or recipients.

Reconfiguring: 100% Done [Details](#)

Reconfiguring: 100% Done

Routing

What clients to relay mail from ?

+ New Rule

+ New Blind carbon copy

Apply configuration

Search



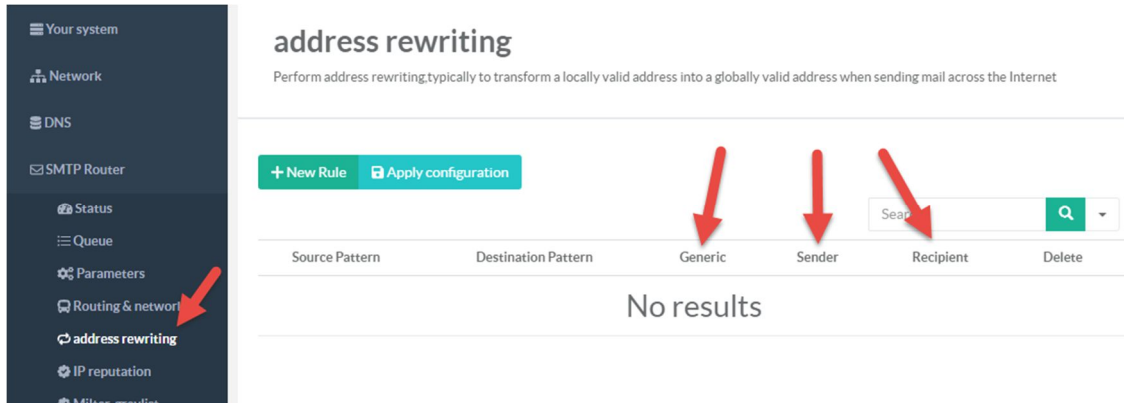
Direction	Item	Forward To	Enabled	Delete
Outbound	All domains	(smtp) 212.25.56.32:25 Authentication: mailboxrelay	☒	
Inbound	acme.corp	(smtp) 192.168.1.113:587 Opportunistic TLS mode: Mandatory TLS encryption Authentication: artica	☒	



ADDRESSES REWRITING

Addresses Rewriting 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

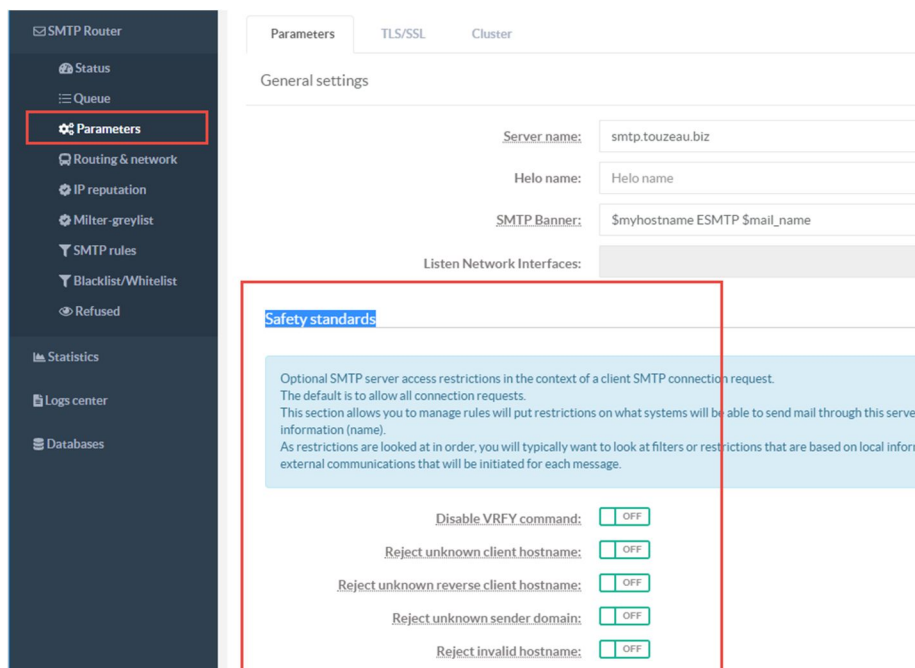
Examples:

```
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 as gmail.com, hotmail. * or yahoo. * will not be 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.

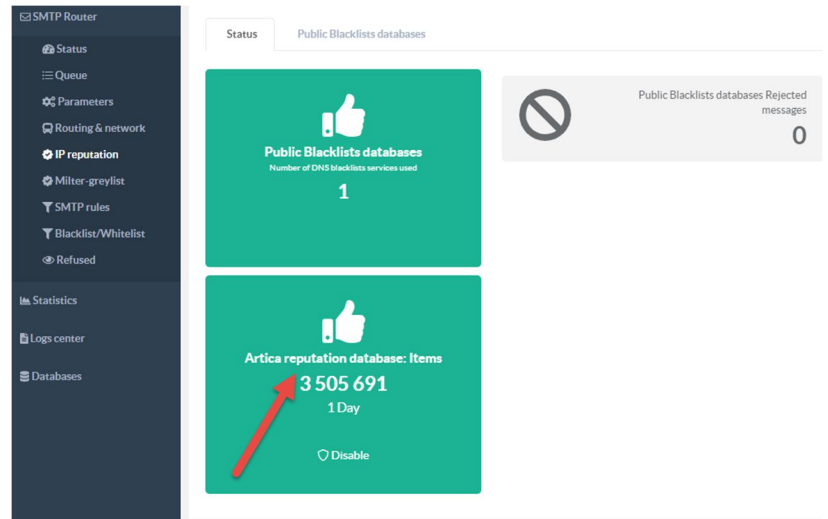
If a sender IP address is listed on these databases, the SMTP connection will be automatically refused.

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.

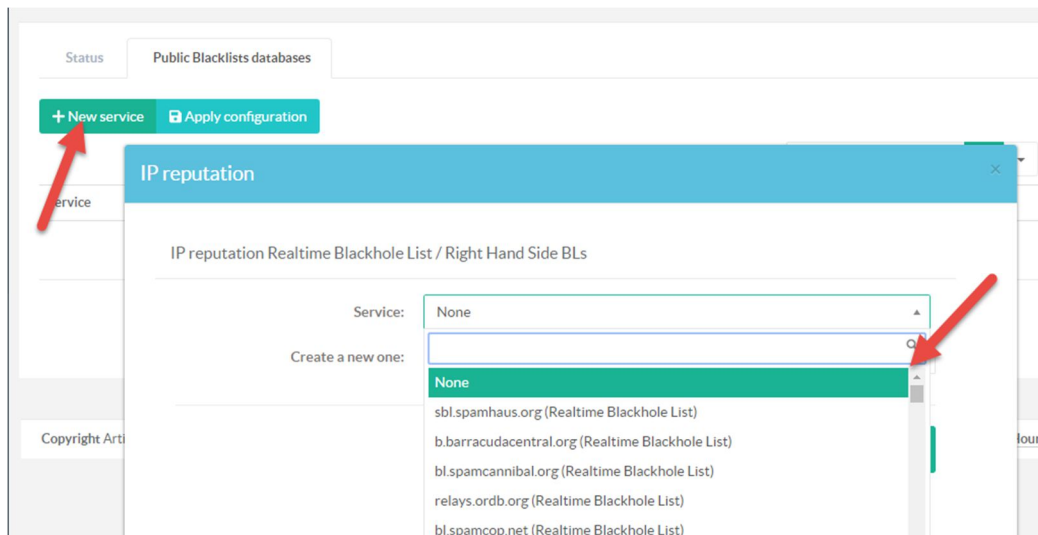
There is a little difference between Public Blacklists databases and Artica reputation database. Public Blacklists databases just offer “Blacklisting” as Artica reputation database leads whitelisting too.

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 dnsbl.org.

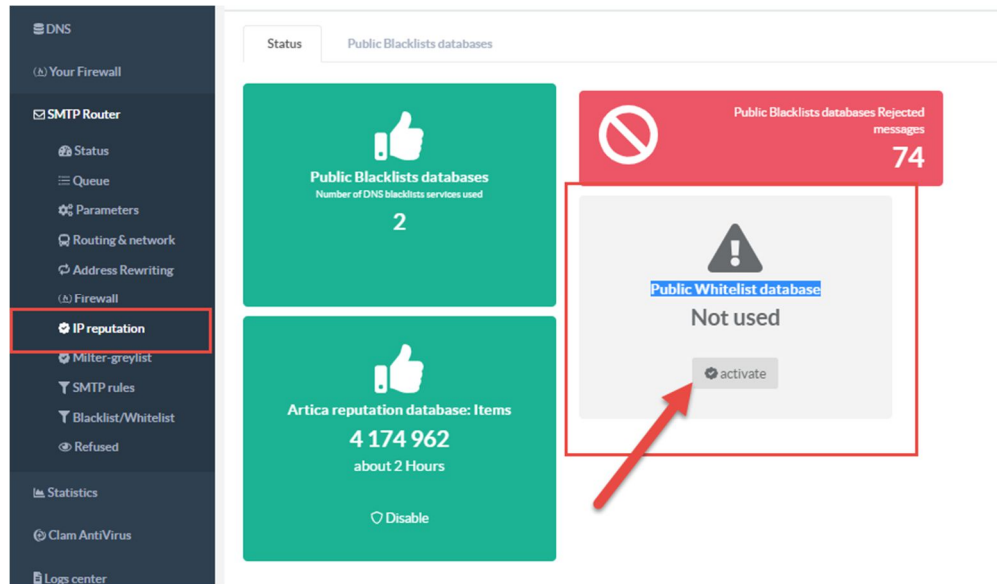
This organization is active in the anti-spam community.

The editors and administrators of dnsbl.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 geographies.

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.

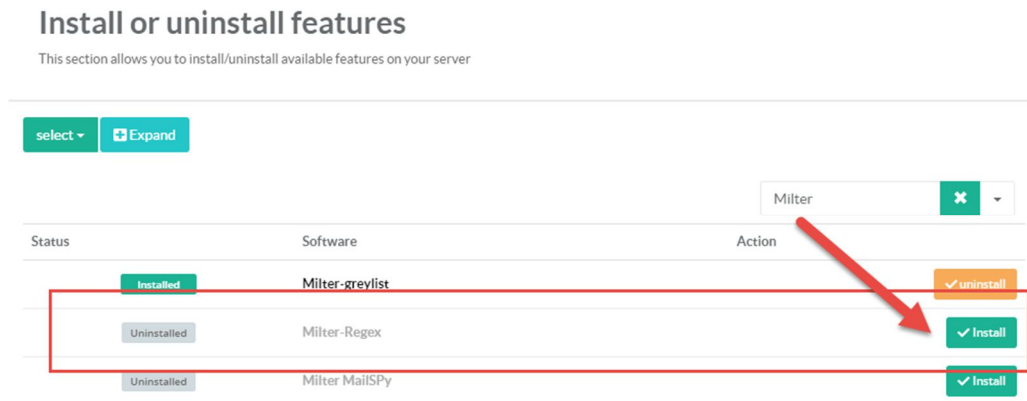
In this case, you need to trust the sender IP address but deny the sender.

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.

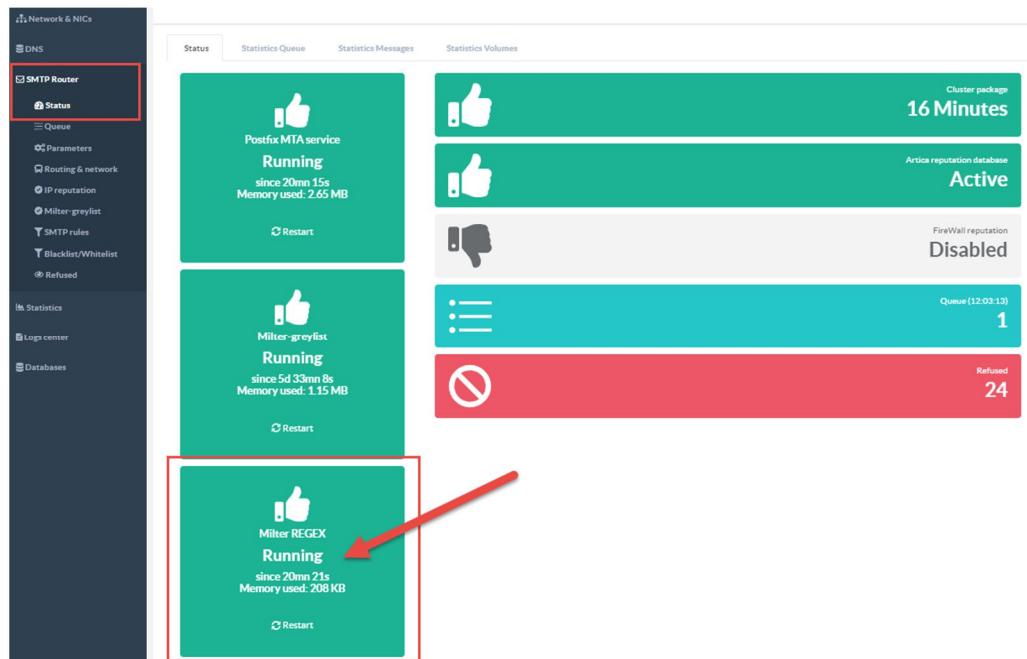
In this case, johnspamer234@gmail.com will be denied using johnspamer[0-9]+@gmail.com.

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**

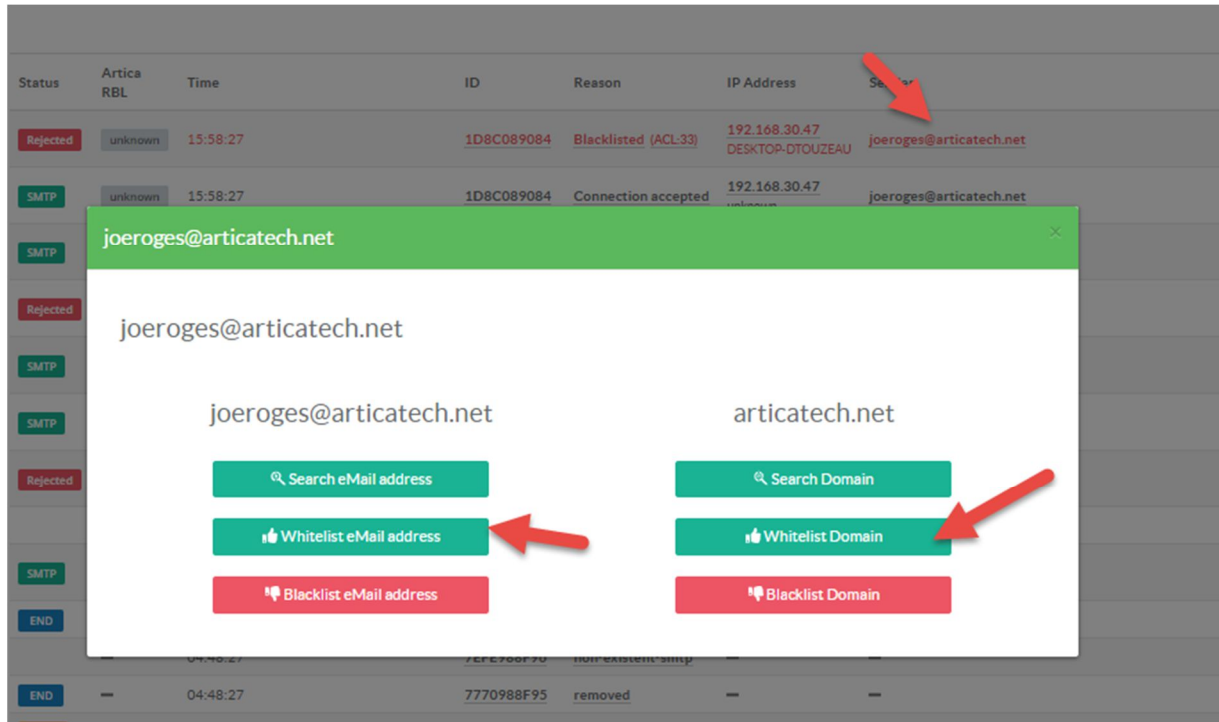


BLACKLISTS AND WHITELISTS RULES

Blacklists rules and Whitelists rules are designed to refuse or allow any SMTP transaction from specific 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, reputations servers are checked before checking sender eMail address.

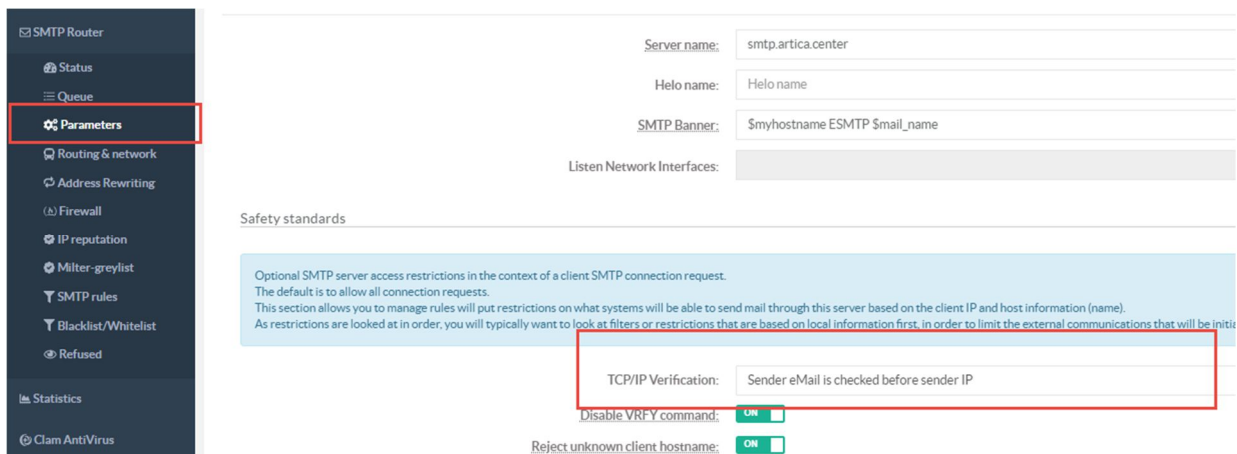
If you need to whitelist a sender eMail address that will not pass connection checking, the message will still be refused.

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 be not checked against IP addresses and messages will pass all tests.



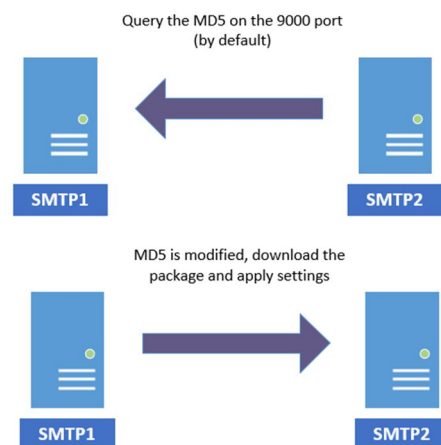
CLUSTER CONFIGURATION.

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 crypted 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

Postfix MTA Mail system » Service status
This section allows you to manage the SMTP service that is in charge to transfert messages to the correct destination. Messages can be transferred to remote server or to the local service in charge of store messages into mailboxes.

Status | Statistics Queue | Statistics Messages | Statistics Volumes

Postfix MTA service
Running

Time synchronization
Waiting replication

Artica reputation database

Postfix MTA Mail system » Service status
This section allows you to manage the SMTP service that is in charge to transfert messages to the correct destination. Messages can be transferred to remote server or to the local service in charge of store messages into mailboxes.

Status | Statistics Queue | Statistics Messages | Statistics Volumes

Postfix MTA service
Running

Time synchronization
4 Minutes

Artica reputation database
Active

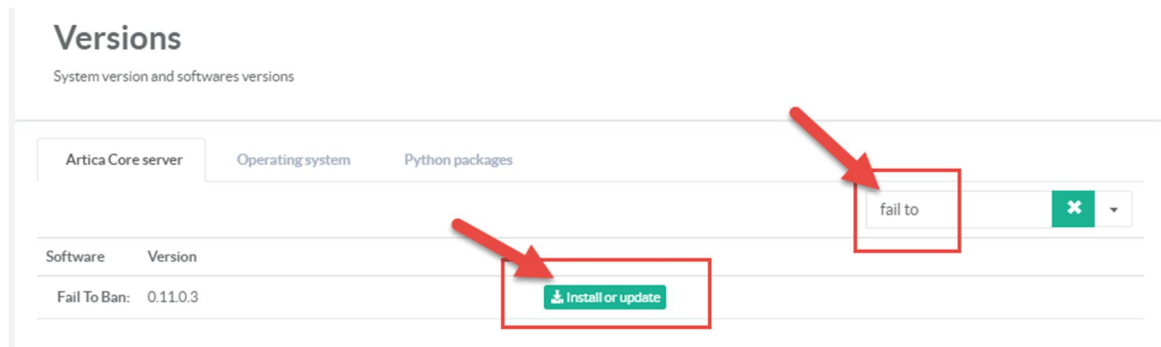


AUTOMATICALLY BAN IP IN FIREWALL BASED ON EVENTS.

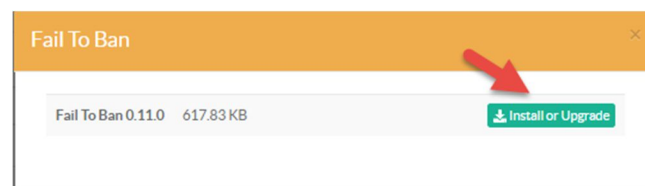
Many spammers did not checks that your server refuse connections according to enabled filters. You have possibility to directly ban remote addresses during a defined period when the remote IP address is refused multiple times. The service that is in charge of this feature is called “Fail2ban” .

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.

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

select ▾ Expand

fail to ✕ ▾

Status	Software	Action
Uninstalled	Fail To Ban	✓ Install

Fail To Ban
Fail2ban scans log files and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with filters for various services (apache, courier, ssh, etc).

Fail To Ban
Running
since 5mn 23s
Memory used: 10.07 MB

Restart

Reconfigure service

Engine Filters: postfix
1

Intrusion Detection System threats
0

Source IP Address(es)
0

- ✓ Basically you did not have to setup something, the service is automatically defined and setup in order to protect your SMTP service.



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 :

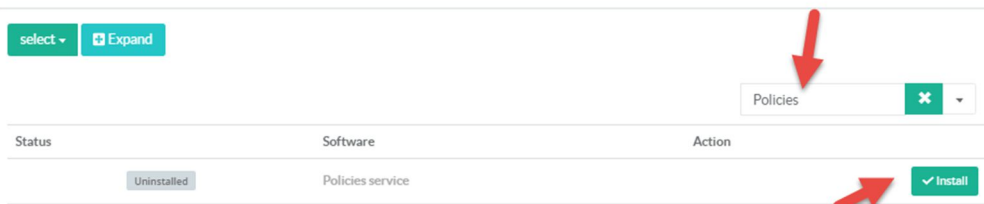
- ✓ Scan messages for Malwares.
- ✓ Scan messages for Anti-Spam.
- ✓ Perform backup messages in the fly.
- ✓ Add disclaimers in messages.
- ✓ Auto-compress messages

Install the Polcies services.

- ✓ On the feature section, in the search field, type “Policies”
- ✓ Click on “Install” button under the “Policies service” row.

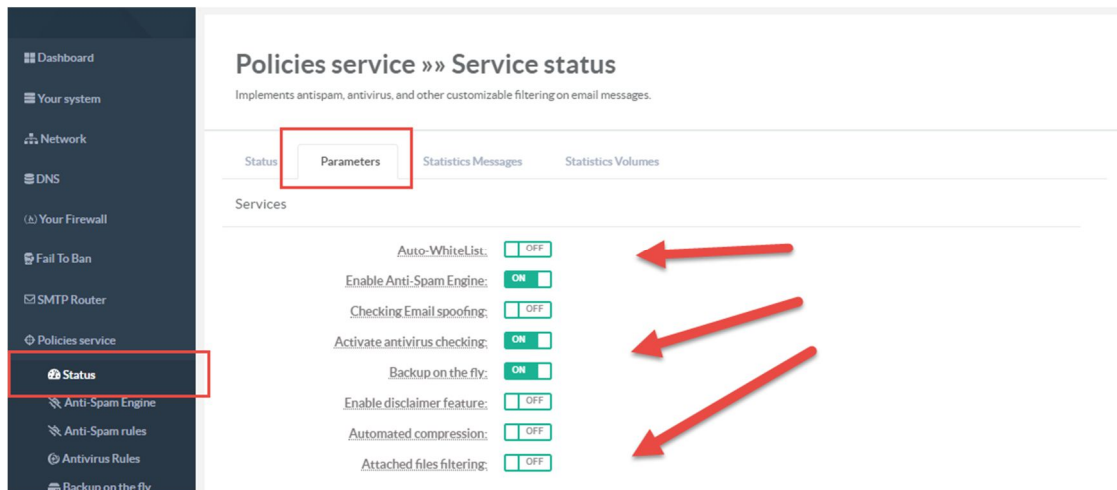
Install or uninstall features

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



Enable SMTP content features.

- ✓ On the left menu, click on **Policies service** and **status**.
- ✓ Select the “Parameters” tab.



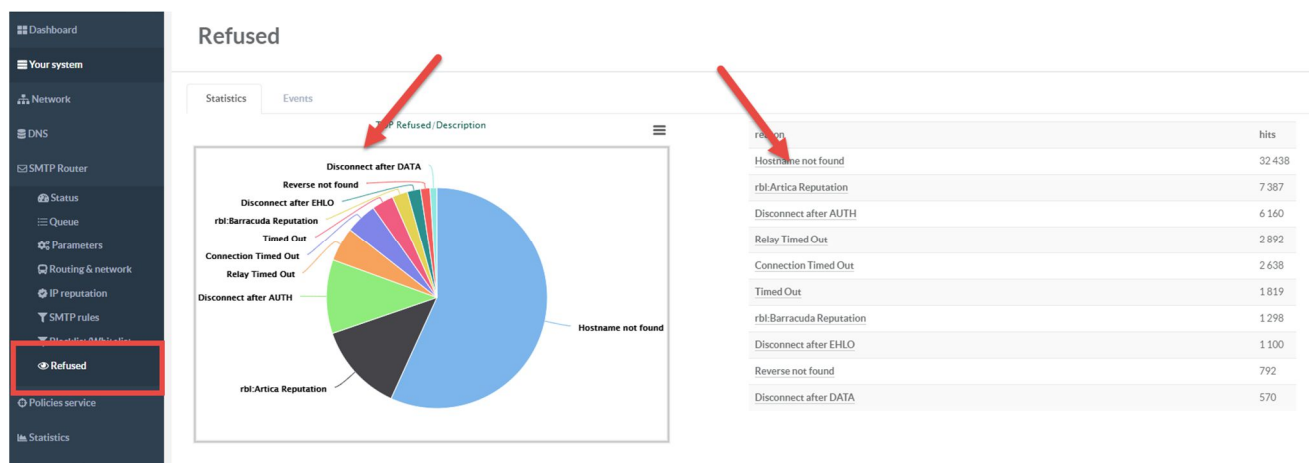
- ✓ **Auto-Whitelist:** Automatically add recipient email address to Whitelist database when your users send an eMail.
- ✓ **Enable Anti-Spam Engine:** Add the bayesian and scoring content Anti-spam engine.
- ✓ **Check eMail spoofing:** A foreign sender cannot use your internal domains to send eMail 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.



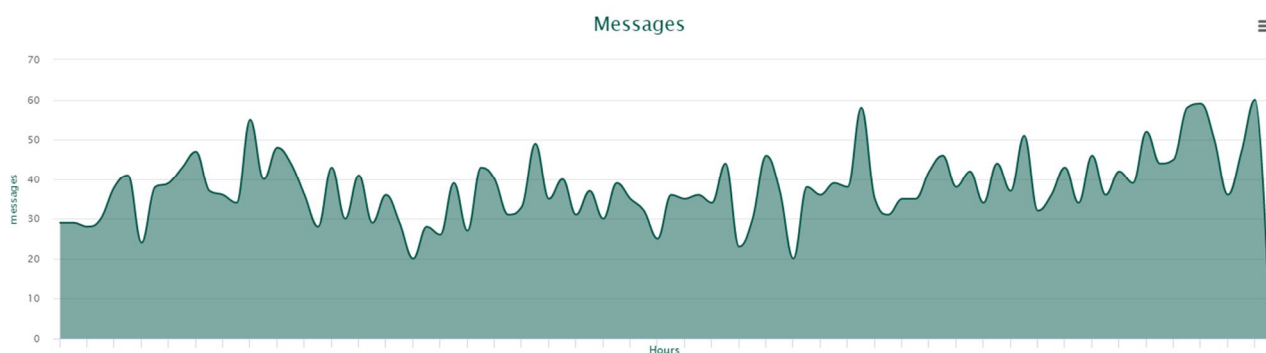
SMTP STATISTICS

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 to see a pie chart about the top 10 of blocked reason.
- ✓ On the right side, the table displays the number of messages blocked.
- ✓ If you click on the link, you can display all messages that match the specified blocked reason.



- ✓ You will see a chart that displays 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 retrieve the history of some SMTP transaction you can use the tool “Investgate”

On the top menu, click on the icon near the log out item.

Under the “Messaging” section, select the “Investigate” option.

You can create a **new query** that allows you to parse events in current and backed logs

Messaging Investigate
This section allows you to search something in the history mail events in order to investigate from a specific issue or question

New Query

Give here a string (a domain, an email address) to find in all events history if you want to use a regular expression use "regex" word as prefix.

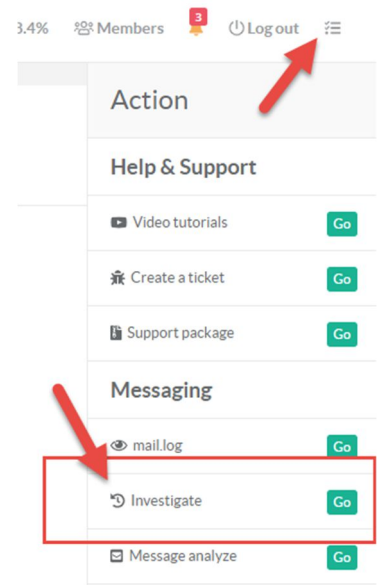
From date: 2018-12-01

From time: 00:00

Max lines: 200

Search messages: etienne

« Search messages »



- ✓ Set the start date of your query and the time start.
- ✓ Define the max number of lines
- ✓ 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 a regular expression, use “**regex**” suffix

Examples:

```
dummy@domain.tld
@domain.tld
*.domain.tld
regex domain.[a-z]+
```



After run the query, a download icon can be displayed in your query history.

Your search pattern is turned to **blue**.

This means you have found events in history and you can download the extracted events.

If the search pattern is "**red**", it's means nothing was found in your query.

New Query Run search

Search Q ▼

	From Date	Size	Search Messages		
Completed	2018 Monday October 01 00:00:00	0 KB	2F62728216C	—	
Completed	2018 Wednesday August 01 00:00:00	0 KB	46.229.214.157	—	
Completed	2017 Friday December 01 00:00:00	67.66 KB	109.234.162.14		
Completed	2017 Friday December 01 00:00:00	11.15 KB	etienne		
Completed	2017 Sunday October 29 00:00:00	0 KB	46.229.214.157	—	



WORDPRESS ADMINISTRATION.

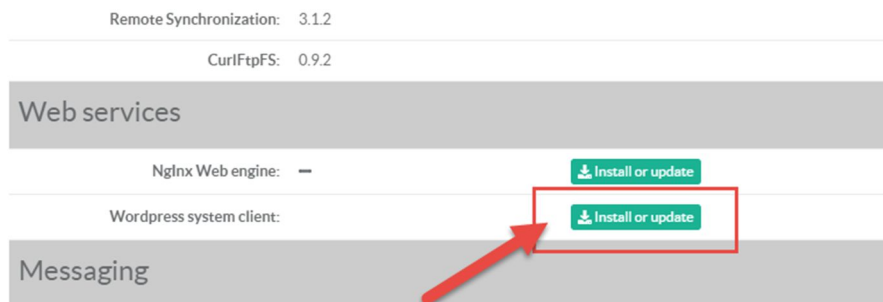
Artica is able to manage Wordpress web sites.
With Artica you are able to easily install/backup/restore Wordpress websites.

PREPARE ARTICA FOR WORDPRESS

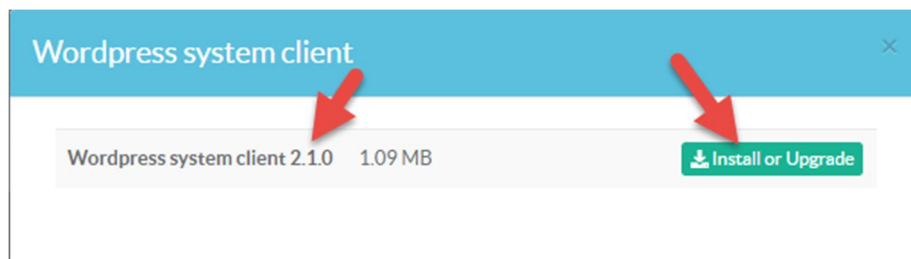
You need to install Wordpress system client, MySQL database, Nginx Web service and finally enable the Wordpress Artica feature

Install Wordpress system client

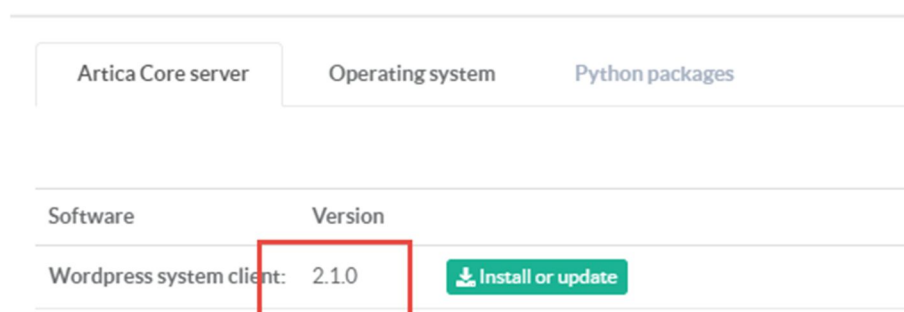
- On the left menu, go to **Your System/Versions**
- Search the item **"Wordpress"**
- Click on **"Install or update"** button on the Wordpress system client row



- Choose the latest version and click on **"Install or Upgrade"** button



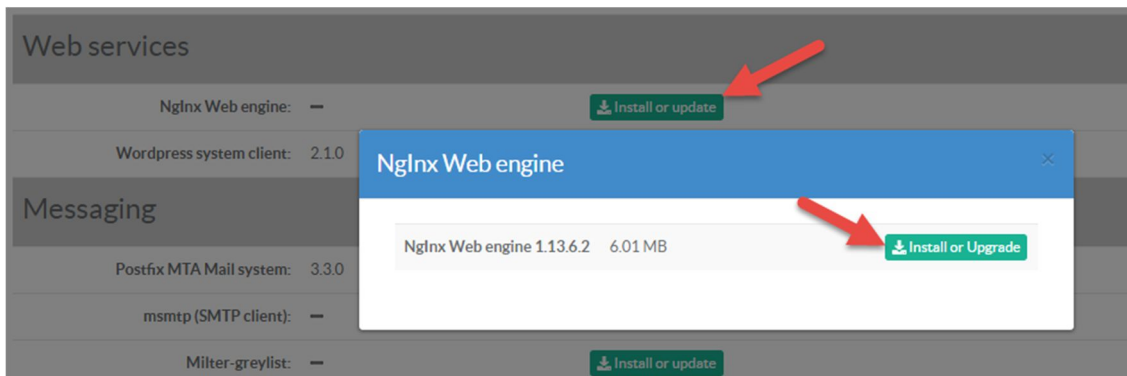
- You should see the version number in the Wordpress system client row



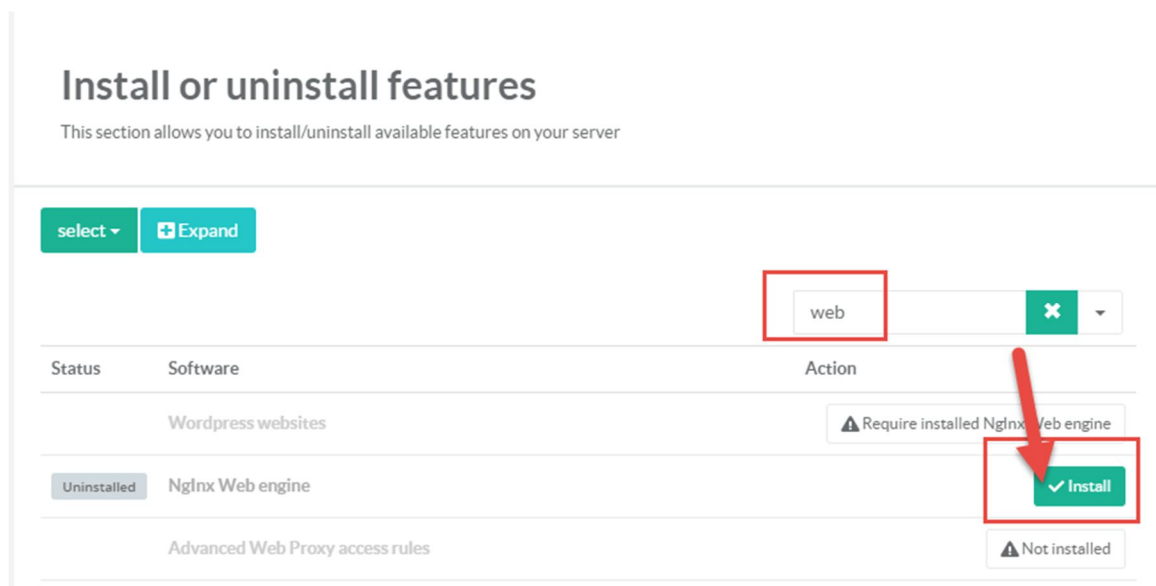


Install the Nginx Web engine

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



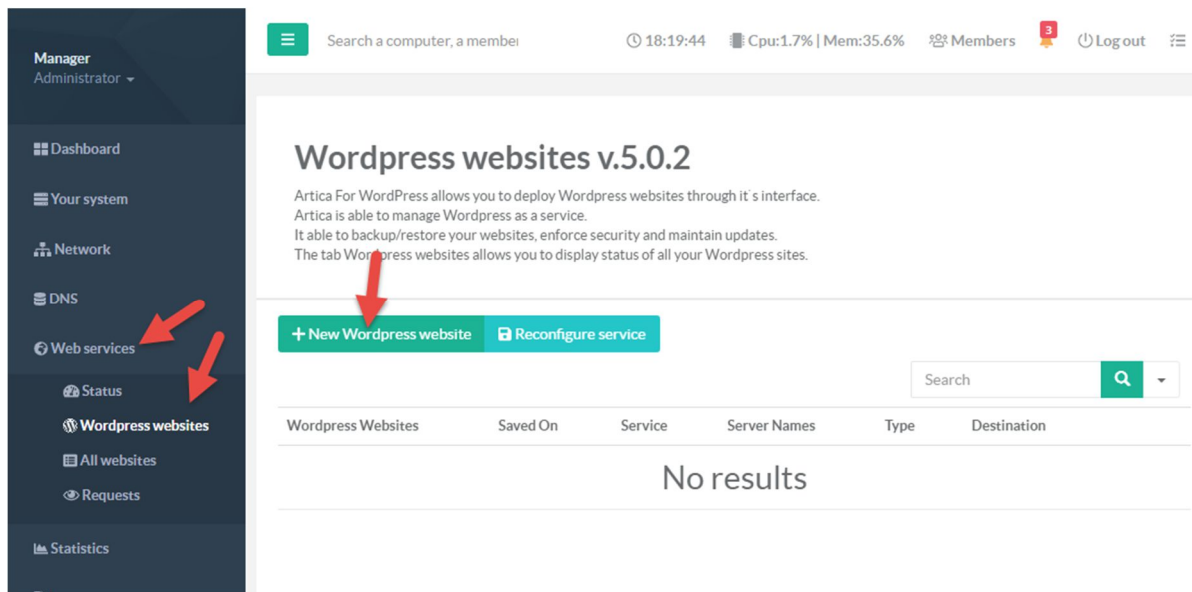
- Click on **Install** on the **Wordpress Websites** row





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 certificate or notifications.

New Wordpress website
✕

New Wordpress website

Web server name:

Administrator:

Administrator email:

Password:

🔑

« add »

The Wordpress Administrator password is re-defined each time you configure the Web site, in this case you did not have to modify it trough 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/uncheck 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.

Status	Wordpress Websites	Saved On
Installed	articatech.info www.articatech.info, articatech.org, www.articatech.org	2019 Thursday January 10 ☒
Installed	web.artica.center	2019 Sunday January 06 ☒



Adresses Rewriting, 97
Advanced Monitoring service, 29
Aes256, 20
Artica reputation database, 99
AUTH Link, 26
authentication box, 55, 56, 58, 60
Auto-Whitelist, 108
Backup on the fly, 108
Clock, 16
Common Name, 13
Community Edition, 11
Default password, 37
Disclaimer, 108
DNS Over HTTPS, 44, 48
DNSBL, 99
DNSEncrypt, 44
DOH, 44, 46
Enterprise Edition, 11
ESXi, 5
Exchange 2010, 95
Fail to ban, 106
Fail2ban, 106
GDPR, 87
Gmail, 102
Graphs, 109
HyperV, 5
ICAP, 87
Identical domains, 94
install-manual, 7
Investigate, 110
ISO, 5
Kaspersky Web Traffic Security, 87

language, 25
LDAP, 31, 32, 33, 53, 54, 55, 60
Let's Encrypt, 12
Multi-Domains, 31
NTP Time Client, 17
Nutanix, 5
Office365, 102
Persistent key-value DB, 82
Port 443, 27
Port 465, 95
Postfix MTA Mail system, 91
Public Blacklists databases, 100
RADIUS, 60
RBL, 99
regular expressions, 102
Reset, 28
Reverse DNS, 39
Routing, 93
Silent Authentication, 61
Snapshot, 19
SOA record, 39
Spoofing, 108
SSH, 37, 38
Time client, 16
Time server, 16
Time zone, 16
VMware, 5
Wordpress Administrator password, 114
Wordpress system client, 112
XenServer, 5
Yahoo, 102