DOCUMENTATION ARTICA v4.30.000000





TABLE OF CONTENTS

Installing Artica	
Requirements	
Ardware and operating system :	
Minimal hardware performance:	
Product is "Virtualization aware"	
Browsers	
Using the ISO	
Using the install script	
The menu console	
Reset the configuration	
The Wizard	
Timeout when connecting to the wizard	
Community or Enterprise EDITION?	
Features between Community Edition and Enterprise Edition	
Optimizations	
Upgrading from a 3.x version	
Exporting settings from a 3.x version	
Import 3x settings into 4.x	23
Upgrading Artica	24
Official releases	
Services Pack	
Nightly builds	- 24
Update in production	
Manual update	
The Certificates Center	25
Build a self-signed certificate	
Build a Let's Encrypt Certificate	
Verify the Let`s Encrypt Automation installation	
Generate the certificate	
Import a PFX	
Manage the system	
The Features section	30
Processes management (overloaded system)	32
Install Processes Group	32
Configure performances for background tasks	33
Hard drives management	34
Expand disk on a Virtual machine	
Network	
The Hosts file.	
Manage records in the host file	

Page: 1



2 gateways for one interface	
_ gerora, y or	
IP Masquerading multiple internal networks	
Interfaces Watchdog	
Wan optimization	
TCP BBR congestion control	
TCP window-size scaling	
Link Balancer	
Link Balancer has 4 key functions:	
Install Link balancer	
Select load-balanced Interfaces	
Tune the balance	
WIFI Management	
Intel WIFI Network interfaces	
Enable Wireless capabilities	
Configure your wireless interface	
	40 49
Masquerading	49
Time and clock	50
Sot the Time zone and clock	50
Set the Third Zone and Clock	
	53
NTP server options	53
Monitoring the NTP service with LibreNMS	
Backup/Restore configuration	
Create a snanshot	55
Snapshot parameters	56
Backup your snapshots on a remote NAS	
The system SWΔP	57
Adding Swan Shace	57
Removing a SWAP space	58
Momory turing	E0
Overcommitting Memory	
The ratio	59
Fxample 4 GB RAM, no Swap. Not overcommit memory:	59
The Deal	
Avoid Cannot allocate memory	
Artica Web Console	61
Change the Web console language	61
	62
Personalize/Skin the login page	
Artica Web console Listen port and certificate	
Reset to default settings	
Artica Privileges	
LDAP or Active Directory	
Allow users to connect to the Web console in Active Directory mode.	
Centralized updates	

Page: 2

Install Rsync service on the master.....

-	
(Г	

Enable the Rsync updates on clients	
Troubleshooting	
I'm stuck with the web console	
It always asks me to identify ?	
I'm connected to Active Directory but	
cannot login on the web console ?	
Monitoring the Network	73
Realtime Asset Detection System	
Install the Passive Real-time Asset Detection System	
The Traffic analysis Daemon	
, Update the package	
Install the Traffic analysis Daemon	
Display statistics	
Status and configuration	
Interfaces to monitor	
Networks to monitor	
Monitoring the system	
System health monitor	
Monitoring the system Load	
Monitoring CPU / Memory / Disks	
Display incidents reports	
The Advanced Monitoring service	
Installing the service	
Access to statistics	
SMTP Notifications	
Configuring notifications	
Zabbix Agent	
Youtube video	83
The SNMP Service	
Upgrade the SNMP software	
Install the SNMP service	
SNMPv2	
Turn to only SNMPv3	
Manage the SNMP service Via RESTful API	
Add host using SNMPv3 on LibreNMS	
The Logs Viewer	
Troubleshooting	
Read-only filesystem	
The Daemon monitor not running	
The LDAP server service	
OpenLDAP service parameters.	
Manage LDAP Members/group	
Import members from a text/CSV file	94
Exporting users to a CSV file	
RESTful API for managing LDAP users	
 Manage organizations	
	Page: 3



Manage Groups inside an Organization	
Manage members	
SSH service	
Install the SSH service	
SSH server section	
Public Key Authentication With PuTTY	100
How to replicate Public keys on severals Artica servers?	102
The SSH Web console	103
Pertrict the SSH access to the Web console	103
Restrict Access according Geo-Localization of remote addresses	104
The Syslog service / Log server	
Install the Syslog feature	
Securing your SysLog Server with TLS (SSL)	
DNS services	
The DNS Load-balacing service	
Install the DNS Load-balancing service	
The DNS Cache service	
Enable logging	
Write to a local file	
Send to a syslog server	
SafeSearch(s)	
Reverse lookup private zone	
Secure DNS over TLS	
Create a DNS over TLS service. (Server mode)	
Query DNS over TLS servers	
Update the DNS Cache service Software	
	110
PowerDINS	
Installing the PowerDNS system.	
Creating a reverse DNS domain	
Creating SOA and NS records for a reverse DNS domain	
Creating PTR records for a reverse DNS domain	
Testing our configuration	
Update the PowerDNS core software	
The DNSCrypt service.	
Multiple providers	
Update the list	
Unique Provider	
The DNS OVER HTTPS service	
Install the DNS Over HTTPs service	
Update to the latest version	
Install the service	
Create the HTTPs service	
I esting your DOH server resolution	
UNS amplification DoS attacks prevention	
	. 4801 1

Artica v4.x : <u>http://articatech.net</u> | contact: <u>contact@articatech.com</u> | support: http://bugs.articatech.com



Install the service	
ACLs For DNS Load-balancer service.	
	13/
Install the single service.	
Use the wizards section	
The proxy Listen ports section.	
The Connected ports	
The transparent ports	
Network exclusions	
SSL Interception	
Remote ports	
Troubleshooting	
How to test if you are using the proxy ?	
Create a support package	
Listen ports freeze after rebooting	
Proxy service monitoring	
WCCP	145
About WCCPv2 support	
NoTrack	
Url Haus	146
Website blocking	1/4
Google Safe Browsing	
What is Safe Browsing?	
Benefits on Artica proxy	
Visibility	
Protect any non-compatible browsers	
Potential privacy	
Download the documentation	
Authenticate Members	
LDAP Authentication	
Use the Artica LDAP service	
Use a Remote LDAP Database	
Example: Synology LDAP server	
Example: Like Active Directory	
Verify your LDAP patterns	
RADIUS Authentication	
Use Active Directory	
How to join Artica to your Active Directory server?	
Join the Microsoft domain	
Kerberos or NTLM ?	
Use the Native Kerberos	
Dedicated administrator account	
Use the Native Kerberos for Load-balancing and cluster environments	
What about users outside the Windows domain?	155
Connect your Artica server using NTI M	ددا ۱۸۲
Configuring Proxy Settings via GPO on Windows 10/Windows Server 2016/2019	160
Restful API	162
	Page F

Artica V4 Documentation – david@articatech.com

Use an authentication portal (Hotspot)	
Install the "Web portal authentication" service	
Install the "Web portal splash screen"	
Setup the viveb portal authentication	173
Mixed transport + Active Directory provy	174
	174
Load-balacing for Proxies	
HaCluster, Make proxies in cluster with Active Directory	
Install the load-balancing service	
Create the service and add backends	
Enable the Load-balancing compliance on your proxies	
Load-balancing with Kerberos method	
Caching feature	
Install the Cache feature	
Create Your first cache	
Is Artica cache Microsoft Windows Updates?	
How can I see if caches are working as expected?	
Exclude from caching	
Errors pages and Templates	185
The Templates Manager	
	100
Assign your templates to the prove pages	
	100
The ITCharter service	
IT Charter feature	
Download the additional documentation	
The Web Filtering	
Enable the Web-Filtering engine	
Web-Filtering rules	
Understand the Web-filtering processing	
A good way to create Web-filtering rules	
Multiple Sources	
Verify that databases are updated	
Be notified when members browse on specific categories	
Manually update Web-filtering databases	
Schedule Web-Filtering databases update.	
The Web-Filtering error page	
The Wizard	
Tune the Web-filtering service	
Skin the Web-filtering error page	
Browsers Rules	
Bandwidth rules	
TCP MARK Rules	
List all ACLS objects	
Use upstream proxies	
Parent Proxies rules	
Wan Proxy compressor	207
wan Proxy parent mode	
wan Proxy client mode	
Categorization	
Benefits	

Com Laupport: http://burg.articatech.com



The passive method	
The Active Method	
	210
Install the category service.	
Create vour own categories	212
Install the nersonal categories feature	212
List Categories	213
List only your categories	214
Create your first category	215
Compiling your categories	216
Import/export items	218
	218
Export items	219
Shared categories	
Uncategorized websites	
Testing categories	224
Monitoring and statistics	225
Realtime access logs format	
Logging to Internal networks are disabled	
SNMP service dedicated for the proxy	
Merge SNMP proxy inside the SNMP service	
Artica Proxy statistics	
Centralized Statistics	
PDF Reports	229
Statistics by categories	227
What, Where, When, who ?	229
Statistics Feature Documentation	
Scheduled reports with Proxy Statistics Generator	
Install the Proxy Statistics Generator	
Enable the Proxy Statistics Generator feature	
Maintenance	
Update the proxy software	233
Restart the proxy periodically	234
ICAP Conter	235
Example: Connect to the Raspersky web traffic Security ICAP server	
ICAP Antimalware/Anti-phishing service	
Kaspersky For Proxy server	
The program allows:	
The Proxy PAC service	
The Remote Desktop Service Proxy (RDP)	
Update the RDS Proxy service from internet.	
Install the RDS Proxy service	
Sotup the main convice	241
Setup Policies	
Create members	
Create Targets	
Create the policy	
Connect to the RDS Proxy	
Connection Error on Windows 7 or Windows XP	
	Page: 7



Is RDS Proxy is Fail To Ban compatible ?	
Can I define some members temporary?	
Elasticsearch statistics	
Install the core statistics database server	248
	210
Firewall Protection	
lptables(netfilter) based firewall	
Intrusion Detection/Prevention System	
Securize Your Artica server in case of corrupted server	
Deep Packet Inspection	
List of detected applications	
Install the Deep packet inspection	
Use Packet inspection	2
Automatic protection – Fail to ban	
Install the Fail to ban service	
The SMTP service	4 ۸
Anti-snam	
	ч Д
Anti-virus	4
Quarantine	4
Powerful management	
Install the SMTP service	
First step, set your authorized networks.	
The Routing table	
Many domains in the same routing rule	
Transfert messages to Exchange 2010 using TLS on port 587	
Transfert all outgoing messages to an SMTP relay with authentication.	
Addresses Rewriting	
Safety standards	
Disable VRFY command:	
Reject unknown client hostname:	
Reject unknown reverse client hostname	
Reject unknown sender domain	
Reject invalid hostname	
Reject non fqdn sender	
Enforce restrictions in the HELO	
Reject forged emails:	
Enable Generic rDNS Clients check:	
Reject Internal and External non-existent domains:	
Reject senders' domains not listed in local database:	
IP Reputation	
Use the Artica reputation database:	
Public Blacklists databases	
Public Whitelist database	
The milter-regex module for blacklisting performance.	
	Page: 8



Blacklists and whitelists rules	
Whitelist checking	
Cluster configuration	
Automatically ban IP in firewall based on events.	
Install the latest version	
Install the Fail To Ban service	
Secure outgoing messages with SPF. DKIM and DMARC	
Use SPF with DKIM and DMARC	
SPF DNS Record	
Create an SPF record for your domain	
The OpenDKIM service	
The DMARC DNS record	
Identify email accounts to receive DMARC reports	
Learn the DMARC tags	
Generate your DMARC record with DMARC Creation Wizard	
The Policies service (Anti-Spam, Antivirus)	
Install the Policies services.	
Enable SMTP content features	
URL Filtering in SMTP messages	
URL Filtering process:	
Objectives:	
Enable Url Filtering	
The rules section	
The Links section	
SMTP statistics	
Refused messages	
SMTP investigation	
Notifications	
What trouble to report to the postmaster	
Notifications templates	
Vordpress administration	
Prepare Artica for Wordpress	34
Install Wordpress system client	
Install the NoIny Web engine	
Create your first Wordpress website	38
Demoire aliance	
Domains allases	
Enable or disable a website	

V

INSTALLING ARTICA

REQUIREMENTS

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

Ardware and operating system :

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

Minimal hardware performance:

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

Product is "Virtualization aware".

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

Browsers

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

To install Artica, you have 2 ways:

USING THE ISO

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

The ISO file has been tested in both physical servers and virtual environment (ESXi, HyperV, XenServer, Nutanix, KVM). The ISO is in charge to install both the system and Artica framework, in all environments, the procedure is the same

	[!!] Select a language
	choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
	C - No localization * Albanian - Shqip Arabic - EUMA Asturian - Asturianu Basque - Euskara Belarusian - Benapyckan Bosnian - Bosanski
Welcome to the Artica CD-ROM Artica Proxy 64Bits v4.01.101522 Help	Bulgarian - Български Catala - Català Chinese (Simplified) - 中文(荷体) Chinese (Traditional) - 中文(荷体) Chinese (Traditional) - 中文(香像) Croatian - Hrvatski Czech - Čeština Danish - Dansk Dutch - Nederlands anglish - English Esperanto - Esperanto Estonian - Esti
	Finnish - Suomi French - Français Galician - Galego German - Deutsch Greek - Ελληνικά +
	<go back=""></go>
Press ENTER to boot or TAB to edit a menu entry	<tab> moves; <space> selects; <enter> activates buttons</enter></space></tab>

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.

Artica V4 Documentation - david@articatech.com



By default, the install tool will create system partitions

[!!] Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed: SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted: partition #1 of SCS 0(0,0,0) (sda) as ext4 partition #5 of sI3 (0,0,0) (sda) as swap
Write the over set to disks? <yes></yes>
switch to yes
> moves; <space> selects; <enter> activates buttons</enter></space>

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.

Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com

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

Web into 1000 0000 On eth0 https://192.168.1.71:9000 You can use the orypoint arrow Rego Choose the TASK	[MAIN-MENU]
Network System KeyBoard Processes WebInterface License Reboot Shutdown Exit	Modify server Network configuration Root password and system tasks Keyboard and Language setup Processes Monitor Web console menu License Info Reboot this server Shutdown this server Exit to the shell
	K DK >

Reset the configuration

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

Confirm the operation to remove all services and parameters.

Remove This operation will reset settings Server will be turned to DHCP and all services will be removed Press 'Yes' to continue, or 'No' to exit
K Yes > K No >

A progress bar will show you the execution task.

23%	emoving softwares
	23%

Artica V4 Documentation - david@articatech.com



THE WIZARD

After connecting to the default web page (<u>https://your-server-address:9000</u>) 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.

A

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). <u>Learn more</u> NET::ERR_CERT_AUTHORITY_INVALID

Help improve Safe Browsing by sending some <u>system information and page content</u> to Google. <u>Privacy.policy</u>

HIDE ADVANCED

Proceed to 192.168.1.71 (unsafe)

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.

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

ver and domain			
timezone:	US/Eastern		٣
Netbios name:	articaproxy		±
Server domain name:	domain.company.tld		
otwork & NICs			
etwork driftes			
Network settings will be applied a	fter reboot the server		
Network Interface	IP Address	Mac Address	
eth0	192.168.1.71	50:6b:8d:7f:5e:38	
	1021681118	-	¢
Primary DNS server:	172.100.1.110		_
Primary DNS server: Secondary DNS server:	192.168.1.144	-	¢

Page: 14





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:	support@articatech.cbm Artica Tech			
		« 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)

is account is the account used to a	ccess to the main Artica Web interface, ple	ase remember it.
User name:	Manager	Å
Password:	•••••	۹
Confirm:	•••••	٩
	« back »	« Build parameters »

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



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



Timeout when connecting to the wizard

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

← → C ▲ Not secure https://192.168.1.5:9000/fw.wizard	rd.php	
🔢 Apps 🥠 Limited access Wifi 💻 Saurav Dhyani - Mi 🧿 NAV	W2016 CU 07 — 🚆 Upgrade in Microso 🍌 SOLIDWORKS Har 🍌 Graphics Card Drive 🚦 Default Log File Set 🙏 ACT 1 Gigabit Inte	r L How
	Welcome on the Artica project This wizard will help you to setup mandatories parameters on your server. Click next to proceed. An error has occurred making the request: error Thrown: «timeout» Status: «timeout»	

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



COMMUNITY OR ENTERPRISE EDITION?

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

The difference between the Enterprise and Community edition is the Community Edition is "**Enterprise Features**" limited. Some components or some options will not be available in Community Edition. The Community Edition is free of charge and will never expire.

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

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

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

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

Manager Administration	Search a computer, a member	🕚 10:18:30 🛛 📳 Cpu:1.2% Men	n:27.8% 榕 Members 💡 🙂 Log out 泪
Administrator -	Welcome on the Artica project		
E Logs center	Artica is an open source software with a Community Edition arequires a license but provides advanced features. If you plan to use only the Community Edition (Free of charge Edition button. In this case, Artica will hide all Enterprise features and let you features.	nd n Enterprise Edition that Click on Use only the Community playing only with Community	Use the Enterprise Edition
	Copyright Artica Tech © 2004-2018		v4.01.101522 Community Edition



Download the technical documentation about the license here:

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



Features between Community Edition and Enterprise Edition

Features	Community Edition	Enterprise Edition
Proxy feature	✓	✓
HTTP/HTTPS/FTP Proxy Cache feature		✓
HTTP/HTTPS/FTP Proxy advanced ACLS (WAF)		\checkmark
HTTP/HTTPS/FTP/SSH TCP proxy compressor	\checkmark	\checkmark
HTTPS Secure Proxy	\checkmark	\checkmark
HTTP proxy Compressor	✓	\checkmark
HTTP/HTTPS/FTP Proxy LDAP authentication	✓	✓
RDP/TSE reverse Proxy	\checkmark	\checkmark
HTTP/HTTPS/FTP Kerberos Authentication method		\checkmark
HTTP/HTTPS/FTP Active directory (NTLM) authentication method		✓
Ability to Skin error pages		\checkmark
Cluster (Load-balancing Proxies + Active Directory)		\checkmark
Transparent cluster (Load-balancing Proxies in transparent mode)		✓
Proxy PAC service and Engine		\checkmark
IT Charter service		\checkmark
HTTP Proxy statistics		\checkmark

ICAP security service	✓	<
Antivirus Service	✓	<
Standard antivirus databases	\checkmark	✓
Extended antivirus databases		✓
Extended Community databases		\checkmark

Web-Filtering feature	✓	✓
Google Safe Browsing	✓	<
50 Web-filtering Categories (3Million Web sites)	\checkmark	✓
150 Web-filtering Categories (50 million Web sites)		✓



Ability to Skin error pages		✓
Can create/manage personal categories		\checkmark
Can create groups of categories	✓	\checkmark

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

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

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



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

Databases management Image: SQL (Installation / Management) Image: SQL (Installation / Manageme

Optimizations

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





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

articadns.touzeau.biz 🗡

VMWare Edition VMware, Inc., VMware Virtual Platform, No	Your server	/	
Erdoure	hostname: <u>Activate system optimization tuning;</u> <u>Enable Intel Celeron support;</u> Processors; Memory;	articad rtouzeau.biz ou orF 4 cpu(s):2GHz 3.86 GB	



UPGRADING FROM A 3.X VERSION

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

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

Starting to 3.06.200164 you can export settings to v4x.

Settings are:

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

Exporting settings from a 3.x version

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



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

RTICA	~ ©) Dashboard	É Your proxy	Action	🕑 Events	Statistics	System	Secon
Snapshots E	Backup yo	ur Snapsho	ots Schedul	Export \	/4x	_		
Export v4x This feature will Click on the but	c export yo ton in orde	ur settings (e	especially ACL: e package and	s) to a packa import it to y	ge for V4x ve our new v4 A « E	rsions. rtica server Export »		

• Download the generated tar.gz file.



Import 3x settings into 4.x

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



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





UPGRADING ARTICA

Artica can be updated itself.

Update configuration can be managed in the left menu Your System /Update

Administrator 👻	Cpu:4.9% Mem:53.9%/3.83 GB	≁ Active Requests	Categorize Admin Guide	🔋 🕛 Log out 🕴
	Update Artica			
System information	Get your Artica system updated and install new Artica services on your system	stem		
EX Your system memory	Artica history Operating system			
 ☆ Watchdog ③ System events ★ Enatures 	Current: 4.29.052614 Service Pack 4	Settings		
>_ OpenSSH server	official: <u>4.28.030418</u>	<u>Update Official Releases:</u> {Update_services_packs}:		
Tasks	Nightly: <u>4.29.052614</u> Service Pack 4	Update Nightly Releases: Perform Update (Even In Production Period):	OFF	
Errincates Center	A Manual update	Remote synchronization (Rsync)		
Update		Activate The Remote Synchronization:	OFF	
🖿 Web Console i Versions		Remote Server:	Remote server	
⊕ Internet access र Support		Remote Server Port:	873	

OFFICIAL RELEASES

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

The automatic update can be controlled by the **Update Official Releases** checkb

SERVICES PACK

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

NIGHTLY BUILDS

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

UPDATE IN PRODUCTION

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

MANUAL UPDATE.

Manual update accept any artica-4.xx.xxxx.tgz for full version or ArticaPx.tgz for Services Packs. With the button Manual update, you can download Artica packages here <u>http://articatech.net/firmwares.php</u> And upload them to the system.

The manual update button allows you to return back to any version available in the Firmware's table.



THE CERTIFICATES CENTER

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

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

BUILD A SELF-SIGNED CERTIFICATE



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

BUILD A LET'S ENCRYPT CERTIFICATE.

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

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

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

Verify the Let's Encrypt Automation installation

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

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

Versions System version and softv	vares versions		
Artica Core server	Operating system	Python packages	Encrypt Automation
Software	Version	11	
Let's Encrypt Automation	n: —	📩 İnstall or updat	te

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"

	New certificate			
The certificate center allows you to generate SSL certificate	New certificate			
New certificate	This operation will generate both certific If you need to upload your certificate, yo	ate request and self-signed certificate. u will be able to upload your keys after submitting	the form	
Comi, on Name	Common Name:	smtp.artica.center	1	
	Country Name:	FRANCE	Ŧ	
	State or province name:	Yvelines		
	locality name:	Orgerus		
	organization name:	Artica Tech		
pyright Artica Tech © 2004-2018	organizational unit name:	IT service		
	email address:	support@articatech.com		
	Encryption level:	2048	τ.	
	Expire in (Days):	- 730	+	
		« Generat	e the Certificate Request »	
		« Generati	e the Certificate Request »	

Manager Administrator -		
E Dashboard		sm
E Your system	_	
📾 Your hard disks		
System events		U
₩ Features		3:
>_ OpenSSH server		
Glances		- 4
O Tasks		. 1
Certificates Center		
🖬 Backup		
P License		
Opdate		
🗂 Web Console		

- ✓ 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.

Certifi The certificate	cates Cer	nter enerate SSL ce	ertificate for services that	provide SSL features such as Wet) servers, mail servers
+ New certific	cate 🕑 Import	⑦ Export	I		Search Q -
+	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.



	720	
Encryption level: 204	18	Ŧ
email address: sup	port@articatech.com	

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

p.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 bo certificate. Be sure that your Web server is already created and listens on 80 port (or 443 with a self-c	h 80/443 port before generating a vrtificate).
Common Name: smtp.artica.center email.address: support@articatech.com	
	« Create certificate »

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

smtp.artica.center: Let`s Encrypt Certificate	×
Letā⊡Ds Encrypt smtp.artica.center - 100% Failed <u>=Details></u> Letā⊡Ds 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).	
<u>Common Name:</u> smtp.artica.center <u>email address:</u> 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	+ New certificate Import ① Export			Search	٩	•	
	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	*	0

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



IMPORT A PFX

.

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

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

+ New certificate Import Import PFX Export Common Name Expire Self-signed certificate artica-applianc.touzeau.maison 2024-09-05 11:40:07 (over 5 years)	servers	Certificates Center The certificate center allows you to generate SSL certificate for services that provide SSL features such as Web servers, mail servers				
Common Name Expire Self-signed certificate artica-applianc.touzeau.maison 2024-09-05 11:40:07 (over 5 years)			Export	Import PFX	 Import 	+ New certificate
Self-signed certificate artica-applianc.touzeau.maison 2024-09-05 11:40:07 (over 5 years)		-				
Self-signed certificate artica-applianc.touzeau.maison 2024-09-05 11:40:07 (over 5 years)		Expire		ne	Common Nam	
		2024-09-05 11:40:07 (over 5 years)		c.touzeau.maison	artica-applian	Self-signed certificate
Self-signed certificate transparent.touzeau.maison 2024-09-21 16:03:03 (over 5 years)		2024-09-21 16:03:03 (over 5 years)		ouzeau.maison	transparent.te	Self-signed certificate

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

Certificates >> Import PFX	×
Import a PFX container	

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

Certif	icates >> Import P	FX			×
Im	port a PFX container				
	Password:	Password	-		
			/	« Apply »	

If the certificate is correctly imported, you will see your certificate as an "Official Certificate"

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				
	Gmmon Name	Certificates >> Import PFX	×	
Self-signed certificate	artica-applianc.touzeau.maison			
signed certificate	transparent.touzeau.maison	importing unknown.domain.local (1).pfr: 100% Certificate unknown.domain.local Success <u>«Details»</u> importing unknown.domain.local (1).pfx - 100% Certificate unknown.domain.local Success		
Official certificate	unknown.domain.local			



MANAGE THE SYSTEM

THE FEATURES SECTION

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

Insta This section	Il or uninstall features allows you to install/uninstall available features on your server	
select -	C Expand	
		Search Q -
Status	Software	Action
Netwo	rk 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 u	ninstall features
select - Expand	
Proxy features	
 Messaging Monitoring 	ces
 Network services Network Security 	TCP Kernel
Members services	wireless network interfaces
🛇 Data transfert	lrivers
Statistics	service



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

Insta This section	I or uninstall features allows you to install/uninstall available features on your server	
select -	Collapse	
		Search Q -
Status	Software	Action
Netwo	'k services	
Uninstalled	MultiPath TCP Kernel 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 multipleosing of resources, and thus increases TCP throughput to the sum of all available link-level channels instead of using a single one arequired by plan TCP. Multipath TCP is backward compatible with plain TCP. Tf 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 Wifs drivers Allow your Artica server to manage your Intel WIFI interface cards	✓ Install
Installed	DNS Cache service The local cache DNS service is designed to speedup Internet access by reducing the DNS queries latency.	✓ uninstall
	Advanced Cache DNS feature the Advanced Cache DNS feature transform the DNS Cache server as a standard DNS server in order to play with your own DNS items.	Require installed MySQL database server

The expanded table display a description of each available service.

PROCESSES MANAGEMENT (OVERLOADED SYSTEM)

Depend of your hardware performance but sometimes you can see alerts about overloaded system.

If you encounter this behavior, that means some background Artica tasks use some disk and CPUs that consume server performance.

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

🗭 Notifications	
Q 1174 Évènements	
alerte	12 minutes
6.28: Overloaded system, aborting task (see report) 🥹 18:30:09	
alerte	12 minutes
[OVERLOADED] system: 6.28, aborting ↔ 18:30:08	
alerte	22 minutes
[OVERLOADED] system: 3.83, aborting 🥑	

Install Processes Group

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

Install or uninstall features This section allows you to install/uninstall available features on your server				
select - Expand <u>A</u> Wizards				
	Search Q -			
Status Software	Action			
Network services				
Uninstalled MultiPath TCP Kernel	✓ Install			
Uninstalled Process Groups	✓ Install			

• The feature section must mark "Process Groups" as "installed"

Install or uninstall features This section allows you to install/uninstall available features on your server							
select -	Expand A Wizards	Search Q -					
Status	Software	Action					
Netwo	'k services						
Uninstalled	MultiPath TCP Kernel	🗸 Install					
Installed	Process Groups	✓ uninstall					
Uninstalled	Configure wireless network interfaces	✓ Install					



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



Configure performances for background tasks

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

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

Only During Non-production Time (22h - 6h):

CPU Performance (Artica Processes): 25% Disk Performance (Artica Processes): 45%

C.P.U: 1

- CPU:
 - Limit processes to use only one CPU, choose in the drop-down list the CPU that will be used.
- CPU Performance: Set here the max percentage of CPU a process can be use.
- **Disk performance**: Set here the disk access priority rate in percentage.
- Bandwidth Disk (MB/s): Set here the read/write bandwidth allocated in MB/s (default 50Mb/s as a SATA)

« Apply

Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com

Page: 34

HARD DRIVES MANAGEMENT

Expand disk on a Virtual machine

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

To expand a disk used by Artica you need to:

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



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

Manager Administrator -	_										
Dashboard	Your h	ard disks									
🛢 Your system	Format, add, di	splay,edit your hard disk	s								
System information											
🚍 Your hard disks	Your hard dis	sks Statisti									
W Your system memory	✓ Re-scan the	e system disk									
Memory swapping	Disk		Partitions	Size	Free	Used	MB/s	Model		Version	Action
System events	(1	05.544	4	20.010	0.44.00	47.04.00	007.07MD/-			1.0	
₩ Features	/dev/sda	85.56% used	1	20 GIB	2.01 GB	17.94 GB	807.87MB/S	VMware_VMware Virtual S		1.0	-
>_ OpenSSH server											
Glances											
() Tasks	Copyright Artica	Tech © 2004-2020							v4.28.030418	Communit	y Edition
Certificates Center											

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

	Artica V4 Documentation – david@articatech.com
Manager Administrator -	E Search messages ■Cpu:8% Mem:26.1%/1.92 GB ③ 15:15:27 28 Members BAdmin Guide ♀ ① Log out ﷺ
■ Dashboard	Your hard disks Format, add, display,edit your hard disks
System information	Your hard disks Statistics
Your system memory Memory swapping System events	Disk Partitions Size Free Used MB/s Model Version Action // during the system 1 20 GiB 2 62 GB 17 94 GB 807 87MB/s VMware V/Mware V
♥ Features >_ OpenSSH server I Glances	
S Tasks Certificates Center	Copyright Artica Tech © 2004-2020 v4.28.030418 Community Edition

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

Your hard disks	Statistics		
✓ Re-scan the sy Disk	/dev/sda >	> Partitions	×
/dev/sda 🗩	Partitions	Size Used Mounted On	Туре аге
	sda1 Exten	d partition 65% used 7.9G 4.77 GB /	Linux native
		/dev/sda1 >> Extend partition ×	
Copyright Artica Tech	h©2004-2020	Extend this partition to 12 GB	
		€ Extend Partition	

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

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

The Hosts file.

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

Manage records in the host file

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

📰 Your system				
류 Network 을 DNS	Hosts file	operating system file that maps hostnames to IP a	ddresses. It is a plain text file	
¢ [®] DNS Servers				
🖵 Hosts file	Search messages			Go!
My computers				
# Your proxy	+ New item Build the	THE	Search	Q -
Proxy.pac/WPAD service	IP Address	Hostname	Alias	
• Web services		No resu	ılts	
Se Databases				
🖹 Logs center				

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

New item				
	IP Address:	192.168.1.1	±	
	Hostname:	router		
	Alias:	router.touzeau.biz		

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

HOSIS	піе		
The compute	file hosts is an operating system :	hle that maps hostnames to IP addresses. It is a plain text file	
Search mess	ages		Go!
+ New item	Build the file		
P Address	Hostname	Alias	
	router	router.touzeau.biz	



2 gateways for one interface.

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

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

å Network ≓Interfaces	Status Parameters					
A Routing rules	Apply network configuration	≓MultiPath TCP Kernel Let Sta	tistics			
☆ Your networks						
S DNS				Search	1	۹ -
	Network Interface	TCP Address Netma	sk MAC Address	Gateway In	nternet Access	Firewall
(A) Your Firewall	WAN: Interface externe (eth1) Network Awareness	10.10.1.2 255.255.255	0 00:e0:4c:68:19:a0	10.10.1.254 Metric 2 (default gateway)		~
tour proxy	LAN: Interface Interne (eth0)	400.440.44 055.055.055				
Caching	Network Awareness	192.108.1.1 255.255.255	0 00:e0:4c:08:19:91	0.0.0.0	4	
Your categories	wlan0: Interface wlan0 (wlan0) Metric is already used Network Awareness	192.168.30.50 255.255.255	0 00:16:ea:54:b0:b8	192.168.30.1 Metric 2		
🛎 Statistics						

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

eth1	Multipath security	Features	Virtual Network Interfaces			
+ New gat	teway					
				Search		۹ 🗸
Gateway					Weight	Delete
10.10.1.254					1	-

Add the second gateway IP address and set its weight.

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

eth1: New gateway			×
Gateway:	10.10.1.3	٥	
Weight:	- 2	+	
		« add »	



Using Artica as an advanced gateway

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

Here it is an example of a network



3 subnets, 172.16.1.0/24, 192.168.200.0/24 and 192.168.1.0/24 Artica uses 3 network interfaces, Eth1 linked to 172.16.1.0/24 network and is the main gateway (172.16.1.1) Eth2 linked to 192.168.100.0/24 network and is the main gateway (192.168.100.1)

EthO linked to 192.168.1.0/24 network but act just as client of a remote gateway 192.168.1.1 to access to Internet.

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

Our eth1 and eth2 is the gateway of their networks, so you have to define 0.0.0.0 in each Internet Address configuration. Under network interfaces section, make sure that Interfaces act as gateway for the designed network have 0.0.0 Make sure that the Interface that use the gateway to access to Internet is marked as "**Default gateway**" on the routing rules

Network interf	aces itwork configuration of your physical, vi	irtual, VLAN netwo	ork interfaces.				
C Apply network configuration	+ Kernel network optimization	내 Statistics					
						Searc	:h
Network Interface			TCP Address	Netmask	MAC Address	Gateway	Internet Access
eth0: Interface eth0 (eth0)			192.168.1.253	255.255.255.0	00:0c:29:97:e5:d9	192.168.1.1 Metric 1 (default gateway)	
LAN_172: Interface eth1 (eth1)			172.16.1.1	255.255.255.0	00:0c:29:97:e5:e3	0.0.0.0	
LAN_100: Interface eth2 (eth2)			192.168.100.1	255.255.255.0	00:0c:29:97:e5:ed	0.0.0.0	



IP Masquerading multiple internal networks

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

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

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

Firewall Interfaces connectors

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

Manager Administrator +	E Search a computer, a member		© 11:10:08	Cpu:55.9% Mem:28.4%	²⁸ Members	🗈 Ad
Dashboard	Interfaces connectors	New Connector			×	
≣ Your system	A connector link 2 networks Interfaces in order to make a commune to section allows you establish a basic NAT (Network Address Bon ally the "Source network card" is your local network inter	New Connector				
€ DNS	+ New Connector Apply Firewall rules	Enabled:	ON	1		
(A) Your Firewall		Packets from:	eth0 192.168.1.253 - Interface eth0	· ·		Sear
¢ [®] Parameters	Id Packets From	Should be forwarded to:	eth2 192.168.100.1 - Interface eth2			Fire
i≣ Rules	5 Interface eth0 (eth0) 192 168.1253/255.255.255.0	Join interfaces only:	ON			
→ NAT	Interface eth1 (eth1) 172.16.1.1/255.255.255.0	Deny DHCP requests:				
☎ Masquerade	3 Not defined/Trusted mode	Enable block countries service: Masquerading:	OFF			
Firewall services		Opposite masquerading:	OFF			
■Configuration file						
@ Events				« add »		
Less Statistics	Copyright Artica Tech © 2004-2019				325	501 Com
Logs center						
E Databases						

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

■ Dashboard Your system A Network	Ma IP Maso The IPN	squerade Juerade, also called IPMA MASQ server acts as a gate	SQ or MASQ, allows one or more computers in a network without assigned IP addresses to communi eway, and the other devices are invisible behind it, so to other machines on the Internet the outgoing
🛢 DNS (ک) Your Firewall	Appl	y Firewall rules	
¢ ₀º Parameters	Enabled	Network Interface	Networks
i≡ Rules	~	meth0 Interface eth0	From All networks But not to 192.168.1.0/24, 192.168.100.0/24, 172.16.0.0/16
	7	eth1 Interface eth1	From All networks But not to Nothing
∞ Masquerade		eth2 Interface eth2	From All networks But not to Nothing
Firewall services			
■Configuration file			
@ Events			

Finally, click on "Apply Firewall rules"



Interfaces Watchdog

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

Status Parameters							
Apply network configuration	rnel network optimization 止 Sta	tistics					
					Search		۹.
letwork Interface	TCP Address	Netmask	MAC Address	Gateway	Internet Access	Watchdog	Firewall
th1: Interface eth1 (eth1)	192.168.1.121	255.255.255.0	50:6b:8d:b4:dd:70	192.168.1.1 Metric 1		~	-
th0: Interface eth0 (eth0) etwork Awareness	192.168.80.1	255.255.255.0	50:6b:8d:dc:56:c5	0.0.0.0 (default gateway)	A		

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

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

r.



Wan optimization

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

TCP BBR congestion control

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

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

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

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

Network interfaces								
This section allows you to set the network configuration of your physica	al, virtual, VLAN network inte	erface						
Status Parameters								
Apply network configuration ① 1 Disabled interface(;)	► Kernel network optimiza	ation 😃 Stati	stics					
						Search		Q
in the i	TCD Address	Natmack	MAC Address	Colorest	Internet Assess	Watchdog	Masquarada	Firewal
Network Interface	TCP Address	INCUILIDAN	MAC AUDIESS	Gateway	Internet Access	watchuog	Masqueraue	Firewal
Network Interface eth2: Interface eth2 (eth2) Disabled	-	-	70:88:6b:88:68:7e	0.0.0.0	-	-	Masqueraue	Firewa
Network Interface eth2: Interface eth2 (eth2) Disabled eth0: Interface eth0 (eth0)	- 192.168.1.1		70:88:6b:88:68:7e 00:01:2e:90:cc:8d	0.0.0.0 0.0.0.0	-	- -		rirewa
Network Interface eth2: Interface eth2 (eth2) Disabled eth0: Interface eth0 (eth0) eth1: WAN INTERNET (eth1)			70:88:6b:88:68:7e 00:01:2e:90:cc:8d 00:01:2e:90:cc:8e	0.0.0.0 0.0.0.0 10.10.1.254 Metric 3	- - -	- - -		v v

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

rnel network optimization	
Kernel network optimization	
Enable Kernel Network Optimization:	OFF
Enable Ipv6:	OFF
Artica Has A Gateway:	ON
Bottleneck Bandwidth And RTT:	ON
Disable TCP Window Scaling:	OFF
Disable Explicit Congestion Notification (ECN):	OFF
TCP TIME_WAIT	
TCP Time Wait Reuse:	OFF
TCP Time Wait Recycle:	OFF
TCP Fin Timeout:	60 Seconds v
TCP Autotuning settings	

6

TCP window-size scaling

Sending more data at a time

To increase TCP performance, the way is to send more data at a time.

As the bandwidth of the network increases, more data can fit into the pipe (network), and as the pipe gets longer, it takes longer to acknowledge the receipt of the data.

This relationship is known as the bandwidth-delay product (BDP).

This is calculated as the bandwidth multiplied by the round-trip time (RTT), resulting in a value that specifies the optimal number of bits to send in order to fill the pipe. The formula is this:

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

Computed BDP is used as TCP window size for optimization.

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

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

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

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

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

TCP window-size scaling

To resolve the performance limitations imposed by the original design of TCP window size, extensions to the TCP protocol were introduced that allow the window size to be scaled to much larger values.

Window scaling supports windows up to 1,073,725,440 bytes, or almost 1 GiB.

This feature is outlined in <u>RFC 1323</u> as <u>TCP window scale option</u>.

The window scale extensions expand the definition of the TCP window to use 32 bits, and then use a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header

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

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

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

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

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

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

To change the TCP windows size :

• On the network section, choose "Kernel Network optimization"

Network interfaces This section allows you to set the network configuration of your	physical, virtual, VLAN network inte	rface						
Status Parameters	-	5						
C Apply network configuration ① 1 Disabled interface	Kernel network optimiza	ition 🚽 Stati	stics			Search		Q .
Network Interface	TCP Address	Netmask	MAC Address	Gateway	Internet Access	Watchdog	Masquerade	Firewall
eth2: Interface eth2 (eth2) Disabled	-	-	70:88:6b:88:68:7e	0.0.00	-	-		
eth0: Interface eth0 (eth0)	192.168.1.1	255.255.255.0	00:01:2e:90:cc:8d	0.0.00		-		~
eth1: WAN INTERNET (eth1)	10.10.1.2	255.255.255.0	00:01:2e:90:cc:8e	10.10.1.254 Metric 3	~	-		~
WIFI-Wireless card (wan0) (wireless)	192.168.30.75	255.255.255.0	Oc:54:15:a2:42:84	192.168.30.1	~	-	~	

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

rnel netwo	rk optimization	
Kernel netwo	ork optimization	
Enat	ble Kernel Network Optimization:	
	Enable Ipv6:	
	Artica Has A Gateway:	
	Bottleneck Bandwidth And RTT:	
Durch la Frank	Disable ICP Window Scaling:	
Disable Explic	cit Congestion Notification (ECN):	UT .
TCP TIME_V	VAIT	
	TCP Time Walt Reuse: TCP Time Walt Recycle: TCP Fin Timeout;	OFF OFF 60 Seconds
TCP Autotu	ning settings	
Defines how	the TCP stack should behave when it o	comes to memory usage
	Socket Send/receive Buffer:	16M v
	Low Threshold:	180К т
	Pressuring Memory:	240K *
	MAX Memory Pages:	365К т

192.168.1.

Interface

Artica server gateway

Interface 1

Interface 2

Interface 3

Ŀŀ

192.168.30.1

10.10.1.254

10.10.3.254

ISP

ISP 2

ISP

Link Balancer

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

Link Balancer has 4 key functions:

- It can check all your gateways, if they are alive. You can even write your own checks for your gateways. Link Balancer can continuously monitor them and react to failures.
- 2. It can set multiple default gateways that will be used in a weighted round-robin fashion. Link Balancer can configure your routing tables to achieve optimal balancing of all your upstream providers, or balance multiple VPN links.
- It can manage your routing tables. Link Balancer will copy routing tables and apply all changes incrementally, after comparing routing tables line by line.
- 4. It can apply policy-based routing rules. Link Balancer can configure policy based routing rules, allowing you to configure routes based both on source and destination IPs, on marks, tos, etc.

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

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

Install Link balancer

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

This section	n allows you to install/uninstall available features	s on your server	
select -	Expand A Wizards		
		link Balancer	X -
tatus	Software		Action
Installed	Link Balancer		✓ uninstall



Select load-balanced Interfaces

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

A Routing rules Court Link Balancer Or Your networks	Link Balancer v3.1.7 Link Balancer is a feature to help you manage multiple internet connectivo points (for example you can use Link Balancer to balance a dual-prouting.	ctions, or in-gen ath VPN betwee	eral multiple co n two offices)	onnections and apply	between any policy based
€DNS	Interfaces Options				
(≜) Your Firewall	Apply network configuration				
# Your proxy		Sea	rch		۹ -
WAF and ACLs	Network Interface	Er bled	Weight	%	Gateway
• With and Aces	m wlan0 Interface wlan0 192.168.30.50 (MARK: 0x20)	~	100	50%	192.168.30.1
Security Caching	meth1Interface externe 10.10.1.2 (MARK: 0x21)	~	100	50%	10.10.1.254
Your categories	meth0 Interface Interne 192.168.1.1		-	-	-

Tune the balance

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

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

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

Balancing is implemented u	singwe	ights, so that each provide	r is getting a percentage
of the connections. The links do not need to be	of the s	ame speed.	
(sheek method)	nine		
{cneck_method}:	ping	5	*
Check address:	8.8.	8.8	\$
Mark:	-	20	+
Weight:	-	100	+
probability %:	-	50	+



WIFI Management

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

	ISA bridge:	Intel Corporation Atom/Celeron/Pentium Processor N4200/N3350/E3900 Series Low Pin Count Interface (rev 0b)
6	SMBus:	Intel Corporation A Celeron/Pentium Processor N4200/N3350/E3900 Series SMBus Controller (rev 0b)
		Intel Corporation Wireless 3165 (rev 81)
	Ethernet controller:	Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller (rev Oc)

Intel WIFI Network interfaces

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

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

Insta This section	all or uninstall features on allows you to install/uninstall available features on your ser	ver	
select ▼	Expand Mizards	intel	X -
Status	Software		Action
Uninstalled	Intel Wifi drivers		✓ Install

Enable Wireless capabilities

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

Status	Software	Action	
Networ	k services	N	
Uninstalled	MultiPath TCP Kernel	✓ Install	_
Uninstalled	Configure wireless network interfaces	↓ Install	
Installed	Intel Wifi drivers	🗸 uninstall	
Installed	DNS Cache service	✓ uninstall	



Configure your wireless interface

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

C Apply ne	twork configuration	1 Disabled interface(s)	네 Statistics		
Netwo	rk Interface			11	TCP Address	
n eth1: l	Interface eth1 (eth1)				10.10.1.2	255.25
eth0-1	Interface etb0 (etb0)				192.168.1.1	255.25
wlan0 S Watting This in	: Interface wlan0 (wlan greload network task iterface is not correctly	0) (wireless) configured 0.0.0.0/			-	
					_	

Define global network parameters and click on "Apply" button

wlan0	Wifi Mult	ipath	security	Features	Virtual Network Interfaces	
lan0: Interfa	ace wlan0 (wlar	10)				
	Ena	bled:	ON			
Get IP A	ddress automati	cally:	OFF			
TCP/IP (Checksum Offloa	ding:	OFF			
	Freen	node:	OFF			
	Internet ad	cess:	ON			
	Network	zone:	WIFI			۵
	N	lame:	Wireless card	1		
	TCP Add	lress:	192.168.20.7	5		٥
	Netr	nask:	255.255.255.	0		\$
	Gate	eway:	192.168.20.1			٥
	default gate	eway:	OFF			
	Broad	lcast:	192.168.20.2	55		\$
	М	etric:	- 2			+
	1	MTU:	- 1500			+

Join a WI-FI network

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

wlan0 Wifi N	ultipath security	Features Vi	rtual Network Interfaces	
	Scanning	wlan0 - 100% Scanning Succe	255	
CRefresh ?Analyze				
			Search	۹ +
Access Point	Quality	Crypted	Status	Connect
BBOX-TOUZEAU D0:84:B0:09:3D:60	100%	_	unknown	connect
LYNKSYS 0E:91:82:FC:75:2D	75.7%	۵	unknown	connect
BOUGYES-4G 10:B1:F8:F9:F0:31	42.9%	A	unknown	connect
MAISON B0:4E:26:55:0D:2B	71.4%	A	unknown	connect
MAISON 80:4E:26:4F:32:B4	61.4%	A	unknown	connect

Define WI-FI parameters and click on Apply button.

freebox_touzeau	1	
Country:	France	v
WPA2-PSK,WPA2-Personal:	ON	
WIFI Key:	••••••	
		« Apply »



WI-FI status

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

/IFI: Wireless card (wl	an0)			
wlan0 Wifi	Multipath security	Features	Virtual Network Interfaces	
CRefresh ?Analyze				
			Search	۹ 🗸
Access Point	Quality	Crypted	Status	Connect
BBOX-TOUZEAU D0:84:B0:09:3D:60	100%		unknown	connect
LYNKSYS 0E:91:82:FC:75:2D	80%	A	unknown	connect
BOUGYES-4G 10:B1:F8:F9:F0:31	47.1%	_	unknown	connect
MAISON B0:4E:26:55:0D:2B	77.1%	۵	unknown	connect
MAISON B0:4E:26:4F:32:B4	55.7%	_	unknown	connect
B6:4E:26:4F:32:B4 B6:4E:26:4F:32:B4	75.7%	۵	unknown	connect
freebox_touzeau ?	47.1%	۵	connected	Disconnect
freebox_touzeau_2GEXT	42.9%	_	unknown	connect

Masquerading

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





TIME AND CLOCK

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

Set the Time zone and clock

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



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

Your computer has two timepieces; a ba and another that is maintained by the op	ttery-backed one that is always running as the ``hardware``, ``BIOS``, or `` erating system currently running on your computer as the ``system`` cloc	CMOS ^{**} clock, k.
The hardware clock is generally only use you reboot or turn off your system, the s	d to set the system clock when your operating system boots, and then fro ystem clock is the one used to keep track of time.	om that point until
timezone (PHP):	Europe/Paris	
timezone (System):	Europe/Paris	٣
Today:	2018-11-27	
This hour:	11:27:15	0
This hour:	11:27:15	•

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



NTP time client.

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

Click on the Install button under the Enable NTP client mode

Install or unins	tall features		
This section allows you to install/un	install available features on your server		
select + Expand		NTP	×
Status	Software	Action	•
Uninstalled	Enable NTP client mode		✓ Install

- ✓ 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.
- \checkmark You can see the list by clicking on the "NTP servers" mini-button.

Your computer has two timepieces; a ba and another that is maintained by the op The hardware clock is generally only us you reboot or turn off your system, the	attery-backed one that is alw perating system currently ru ed to set the system clock w system clock is the one used	vays running as the "hardware", "BIOS", or "CMOS" clo unning on your computer as the "system" clock. hen your operating system boots, and then from that poin I to keep track of time.	ick, It until		
timezone (PHP):	Europe/Paris				
timezone (System):	Europe/Paris				
Today:	2018-11-27	INTE Servers			
This hour:	14:56:44				
NTP: Update clock:	Each 2 Hours	Default NTP servers:U	nited States		
Default NTP servers:	France		Search		Q
Use specified time servers:	OFF NTP servers.	NTP Servers		Mv	De
	T 7	us.pool.ntp.org			
		0.us.pool.ntp.org			
		1.us.pool.ntp.org			
		2.us.pool.ntp.org			
Instance Divorver-III I Fo Server		3.us.pool.ntp.org			
Installed DNSCrypt Proxy					



- 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

proputor a mombou		(1) 14-55-16	≡ L nu•14.5%	LMom-3(1.1%	YYX Member	s 📮	ULog out	i.
NTP servers					×			
+ New Server		Search	۹.	clock,	_			
t NTP Servers	М	lv D	el.	oint until	_			
	Nores	SU NTP servers Nev	v Server				×	
		New Server						
NTP: Update clock: Default NTP servers: pecified time servers;	Each 2 Hours France ON NTP servers	Where can i find a As defaults serv quality will not t You get a bit bet <u>europe</u> , north-ar you use the cour - for all these zo 0.ch.pool.ntp.or Note, however; n might contact, however; If you know time distance, with tr	time server ? ers will assign you e ideal. ter result if you u merica, oceania oi try zone (like chu es, you can agair z hat the country z hat the country t servers that are r aceroute or ping)	i timeservers fro se the <u>continent</u> , asia.pool.ntp.org in Si use the 0, 1 or 2 one might not ex- eservers. eally close to yo , time probably v	m all over the wi al <u>zones</u> (For exa g), and even bett witzerland) P prefixes, like dist for your cour u (meaning by n will be wen bette	orld, time imple ter time if ntry, or network er.		
NSCrypt Proxy		Server add	dress: 0.fr.p	ool.ntp.org				
NS Filter service						« add	8	
owerDNS system								
owerDNS recursor								

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

France	· · · · · ·
ON NTP servers	1
	« Synchroniz e » « Apply »

6

NTP Time server

Install the NTP service

NTP service can be installed using the features section.

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

Insta This section	Il or uninstall featur allows you to install/uninstall available feature	es es on your server	
select 🕶	Expand & Wizards	time	× -
Status	Software		Action
Uninstalled	Network Time Protocol (Server)		✓ Install
Uninstalled	Realtime Asset Detection System (PRADS)		✓ Install

NTP server options

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

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

■ Dashboard	Network Time Protoco	I 4.2.8p10 ers over a network to a common timebase (usually	UTC) via NTP Protocol	
System information	Status NTP servers Events	•		
 System events Features OpenSElleerver Time server Glances Tasks Certificates Center SNMPv3 	NTP Server Running since 2mn 13s Memory used: 1.18 MB	General settings Restrict To Local Networks: Default NTP Servers: Use Specified Time Servers: Listen Interface:	ON France ON NTP servers_ All interfaces	•
✔ License ③ Update ☐ Web Console				« Apply »



Monitoring the NTP service with LibreNMS

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

192.168.1.144		Storage Usage	Memory Usage	Processor Usage
9 Overview 🕍 Graphs 🐗 Services 📕 Log	gs 🚯 Alerts 🛄 Alert Stats 📈 Performance	Division Notes		
Device Settings SNMP Port Settings Appl Components	ications Alert Settings Alert Rules Modules	Services IPMI Storag	ge Processors Memor	y Misc
pplications				
OFF Apache	OFF Asterisk		OFF BIND	
OFF Ceph	OFF DHCP Stats		OFF Drbd	
OFF Random entropy	OFF EXIM Stats		OFF Fail2ban	
OFF FreeBSD NFS Client	OFF FreeBSD NFS Server		OFF FreeRADIUS	
OFF Freeswitch	OFF GPSD		OFF Mailscanner	
OFF Mdadm	OFF Memcached		OFF MySQL	
OFF NFS Server	OFF NFS Stats		OFF NFS V3 Stats	
OFF Nginx	OFF NTP Client	ON	NTP Server	
OFF Nvidia	OFF Open Grid Scheduler		orr OS Updates	
OFF PHP-FPM	OFF pi-hole		OFF Portactivity	
OFF Postfix	OFF Postgres		OFF PowerDNS dnsd	ist
OFF PowerDNS Recursor	OFF PowerDNS		OFF Proxmox	
OFF Rrdcached	OFF SDFS info		OFF Shoutcast	
OFF SMART	OFF Squid		OFF Tinydns	
OFF Unbound	OFF UPS apcups		OFF UPS nut	



BACKUP/RESTORE CONFIGURATION.

THIS FEATURE IS AVAILABLE IN ENTERPRISE EDITION.

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

Create a snapshot

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

	Artica server
Snapshots Schedule	
File Name	Size
	Snapshots Schedule

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

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		
Parameters Snapshots Schedule + Create a snapshot Image: Upload a snapshot Image: Upload a snapshot		
	Search	Q -
Date File Name	Size Respre	Delete
01:20:18 e872404cd5a4038a5f8f02a2bd1f83dc.tar.gz	3.44 MB	0

📑 Your system

➡ Your hard disks
 ④ System events
 ♥ Features
 >_ OpenSSH server
 ■ Glances
 ● Tasks
 ♥ Certificates Center
 ■ Backup

₽ Lie



Snapshot parameters

The parameters section allows you to

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

r al allicters	Shapshots Schedu		
arameters			
	Storage directory:	/home/artica/snapshots	Browse
	Max containers:	- 3	+
	Passphrase:	Passphrase	۹
		Passphrase (Confirm)	P

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.

to a remote NAS file ustem. whole server consultation in order to restore it or duplicate it.	
ON	
192.168.1.17	
Public	
Administrateur	
Password	P
Password (Confirm)	P
	+
« Test your connection » « A	pply »
	to a remote NAS file stem. whole server conjugration in order to restore it or duplicate it. Intervention of the set of

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



THE SYSTEM SWAP

Swap space in Linux is used when the amount of physical memory (RAM) is full.

If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space. While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM.

Swap space is located on hard drives, which have a slower access time than physical memory.

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

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

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

Memory s	wapping							
Swap space in Linux is u: If the system needs mor While swap space can he Swap space is located or	sed when the amount of e memory resources an elp machines with a sma n hard drives, which hav	physical memory (RA d the RAM is full, inac ill amount of RAM, it s e a slower access time	AM) is full. trive pages in memory are moved should not be considered a repla e than physical memory.	to the swap space. cement for more RAM.				
Memory swapping	Parameters	Statistics						
+ New Swap Space	✓ Re-scan the system	m disk						
Path				%	Туре	Size	Used	Action
/dev/sda5					partition	7.91 GB	0 KB	-

Adding Swap Space

Click on the button "New Swap Space"

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

w swap space		
New Swap Space		
Path:	/home/swaps	Browse
Size (MB):	- 1024	+
	/	« add »



System events

Removing a SWAP space

SWAP space using a disk partition cannot be removed

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

Memory s Swap space in Linux is u If the system needs mo While swap space can h Swap space is located o	wapping sed when the amount of physical memory (R e memory resources and the RAM is full, ina elp machines with a small amount of RAM, it n hard drives, which have a slower access tim	tAM) is full. Ictive pages in memory are moved to the swap space should not be considered a replacement for more ne than physical memory.	ie. RAM.			
Memory swapping	Parameters Statistics					
+ New Swap Space	✓ Re-scan the system disk	%	Туре	Size	Used	Action
/dev/sda5			partition	7.91 GB	0 KB	-
/home/swaps/1547398	i33.swap		file	1024 MB	0 KB	ð

MEMORY TUNING

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

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

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

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

Overcommitting Memory

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

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

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

The error message you see is similar to

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

And sometimes, the Proxy service turn to emergency service.

Overcommitting behavior

To avoid such situations, the overcommit behavior is configurable.

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

The ratio

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

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

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

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

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

The Deal

•

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

Applications do this a lot, and this is what overcommitting is designed for.

Basically with ratio at 100%, the kernel will not allow applications to allocate any more memory than you have.

Setting it at less than 100 means that you will never use all your memory.

If you are going to set this setting, you should set it higher than 100 because of the fore-mentioned scenario, which is quite common.



Avoid Cannot allocate memory

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

The first chart give information of

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

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



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

5			
≡	Parameters		
	Overcommiting Memory Behavior:	Not overcommit memory *	
	Ratio:	100% •	
	/	« Apply »	

On the right side, set the ratio to 100% and click on $\ensuremath{\mathsf{apply}}$ button.

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

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



ARTICA WEB CONSOLE

CHANGE THE WEB CONSOLE LANGUAGE

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



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

Manager	E Recherche un ordinateur, un		Requêtes	① 12:14:05	Cpu:7.5% Mem:14.9%	음 Membres	2 UDéconnexion
Administrateur 🗕							
📰 Tableau de bord	Manager/Administrateur						
Votre système	-						
🚓 Réseau & cartes réseaux							
≣ DNS	Nom d'utilisateur:	Manager					1
(초) Votre pare-feu	Mot de passe:	*****					P
Otre Proxy		*****					Ð
🛢 Mise en cache	Ma langue:	English					*
🏵 Vos catégories	Police de caractères:	Lato					Ŧ
🛎 Statistiques	Utiliser les listes déroulantes standards:	OFF					
🖥 Centre des logs	Titre de la console dans le navigateur:	%s (%v)					
					« A	uth 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.)

Page: 61
Artica v4.x : <u>http://articatech.net</u> | contact: <u>contact@articatech.com</u> | support: http://bugs.articatech.com



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

Manager	E Search a computer, a me	embei	
Administrator 🗸			
My Account			
Dashboard	articaproxy.d	omain.company.tlo	4 1
E Your system	. ,	. ,	
📾 Your hard disks			
System events	Used CPU	Memory used	Loi
₩ Features	0%/100%	654.41 MB/2.35 GB	0.3
> OnenSSH server			

Select the button "Auth Link"

User name:	Manager	E
Password:	*****	P
	•••••	P
My language:	None	•
Font family:	Lato	•
Use standard drop-down lists:	OFF	
Administration interface browser title:	%s (%v)	

Click on the button "Create the Authentication Link."

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

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

th Link	
Auth Link	
The Authentication your credentials. In this case, if you sa Pay attention that th If the link is not corr	link is a specific URL that allows you to enter into the Artica Web console management without posting we the link in your bookmark, you will be able to quickly enter into the Artica. his URL should not be shared ect. Artica will sends a 404 Not found on the Authentication page
	link: https://192.168.1.71.9000/auth/37fa5616dec38afc0009f1a1c3af0a68
	« Update the Authentication Link »

(F)

PERSONALIZE/SKIN THE LOGIN PAGE

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



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

Dashboard		
Your system	Web interface settings	
System information	Change the main web interface HTTP Engine parameters	s and performances
➡ Memory swapping ③ System events ♥ Features		Design: Logon page
>_ OpenSSH server II Glances © Tasks	Web Console Running since 2 weeks 2d 23h 3mn 35s	Remove Artica togo: OFF Hide Virtualization information: OFF
Certificates Center	Memory used: 3.36 MB	Title Page: %SERVERNAME% 1 Welcome to the Artica Web Administration Interface.
✔ License ③ Update ☐ Web Console	14	2 Please use your Manager account or any account defined by your Administrator
i Versions ⊕ Internet access ऋ Support	PHP Engine Running since 2h 37mn 36s Memory used: 95.99 MB	« Apply »

The Design: Logon page section allow you to

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



ARTICA WEB CONSOLE LISTEN PORT AND CERTIFICATE

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

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

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



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

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

proxy feature in order to redirect the Web console requests to the loop back interface on the 9000 port.

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

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

3:18:20	■ Cpu:1.3% Mem:38.9%
	52 System packages that should be updated/upgraded Fix it
mances	Reboot the Web console Fix it
interface	Locales are not defined Fix it



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.

Web interface URIs: On eth0: https://213.32.85.20:9000 You can use the UP/DOWN arrow keys Choose the TASK	-(MA)IN-HENU)
Network System KauBoard Processes kebInterface License Reboot Shutdown Exit	Modify server Network configuration Root password and system tasks Keyboard and Language setup Processes Monitor Web console menu License Info Reboot this server Shutdown this server Exit to the shell
	<mark>< ΩK ></mark>

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

[WEB IN You can use the UP/DOWN arrow keys Choose the TASK	NTERFACE MENU]
RESTART ERRORS INTERFACE RESET Quit	Restart Web Console service Display error events Change listen Interface Reset to default settings Return to main menu

(F)

ARTICA PRIVILEGES

Artica allows you to define privileges based on:

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

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

LDAP or Active Directory

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



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

Μ	ly members		
Sea	rch messages	Organization » Group Administrators	×
<u>8</u> +	New Member	Administrators Members Privileges Parameters	
8 *8	Display Name Account Operators	Group: Administrators Group description: Netbios Domain Users to manipulate users accounts	
容	Backup Operators	s Apply	>>
22	Guests domguests		
e,	Domain Admins		-



Assign the desired privileges •

Proxy_admins Me	embers	Privileges				
Privileges						
Group privilege						
Add/Delete	/Modify u	sers in groups:	OFF			
Ad	d/Delete/I	Modify groups:	OFF			
Cann	nanage thi	s organization:	OFF			
Proxy service privilege	es					
Can View all Web statist	ics (Proxy	& url filtering):	ON			
Ca	an Manage	Web filtering:	ON			
	P	roxy Manager:	ON			
	As Hot	Spot Manager:	ON			
	Asl	Proxy monitor:	ON			
Administrators privile	ges					
	ls a gl	obal Manager:	OFF			
	Is a Fire	wall Manager:	OFF			
	Isa	VPN manager:	OFF			
0	Can manag	e DNS service:	OFF			
Ca	n manage	DHCP service:	OFF			

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

- A proxy administrator will have "Proxy Manager" privilege. •
- ٠
- A DNS administrator will have "Can Manage DNS service" privilege A FireWall administrator will have "is a Firewall Manager" privilege •



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

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

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

	Search messages			
Manager Administrator +	Cpu:3.8% Mem:17.4	.92.168.1.101 / Administrateur@	touzeau.maison	×
Dashboard		192.168.1.101 / Administrateur@tou	zeau.maison	
📑 Your system	Active Directory I	Connection ID:	0	
A Network	Manage the username and account used t Also if you have other children Active Dire	Hostname:	192.168.1.101	۵
Active Directory		FQDN Of Secondary DC:	FQDN of secondary DC	Ξ L
🔁 Status	+ New connection	LDAP Server Port:	- 389	+
₩ Cluster mode		Enable SSL (Port 636):	OFF	
H Jainska damain (NITL N4)	Hostname	Credentials		
	192 168 1 101 (Default)	Credentials		
= White little	Trz.106.1.101 (Delaut)	User Name:	Administrateur uzeau.maison	
Events		Password:	····· •	
EDNS			••••••••••••••	
⊕ Your proxy		Allow Active Directory Users To Logon:	OFF	
ACLs Proxy	Copyright Artica Tech © 2004-2020	Active directory Suffix		
		3		
🖿 Statistics		LDAP Suffix:	dc=touzeau,dc=maison Brows	e
S Databases				
Logs center			« Apply	
			- Apply	



CENTRALIZED UPDATES

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

Install Rsync service on the master

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



Install or uninstall features This section allows you to install/uninstall available features on your server select C Expand Wizards Status Software Cuininstalled Rsync server

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

A Network	Rsync server 312				
Rsync server	Share directories and applications through Rsync.				
	If this service is enabled you can connect remote Arti	ica servers in order to replicate Antivirus	patterr	n databases, Web-filtering	databases, WSUS storages.
Shared Folders					
@ Events	Status				
€ DNS		General settings			
(≜) Your Firewall			All		
Your proxy	Rsync server	Listen interface:	AIII	nterraces	•
WAF and ACLs	Running	listen port:	-	873	+
Caching	since 5mn 2s Memory used: 688 KB	Max connections:	-	20	+
Nour categories	C Restart	Reverse lookup:	-	0	+
🖿 Statistics					
Logs center					« Apply »

(F)

Enable the Rsync updates on clients.

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

>_ OpenSSH server	Current: 1.00.012001	Jettings	
	official: <u>4.05.042301</u>	Update official releases:	
Certificates Center	Nightly: <u>4.01.071714</u>	Update Nightly releases: Perform update (even in production period):	OFF
E Backup Plicense	t Manual update C Verify	Bind local IP address:	192.168.1.179 💌
Update		Remote synchronization (Rsync)	
🗂 Web Console i Versions		Activate the remote synchronization:	ON
Internet access		Remote server:	192.168.1.1
Ĵ∰ Support		Remote server port:	873
A Network		TimeOuts	

TROUBLESHOOTING

I'm stuck with the web console

It always asks me to identify?

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

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

Firmware version 4.26.020217 on prox	yad2
Web interface URIs: On https://192.168.1.218:9000 You can use the UP/DOWN arrow keys Choose the TASK	
Network System KeyBoard Processes Hebinterface	Modify server Network configuration Root password and system tasks Keubnard_local.charset_setup Processes Monitor <mark>Meb_console menu</mark> License Info
Reboot Shutdown E×it	Reboot this server Shutdown this server Exit to the shell

• Choose "Disable Memcache" for storing sessions

Software version 4.28.0 You can use the UP/DOW Choose the TASK	30418 on pr [W E N arrow key	oxyad2.touzeau.maison B INTERFACE MENU] S
	RESTART CERT ERRORS MANAGER INTERFACE CONT SSLOFF MEMOFF RESET Quit	Restart Web Console service SSL Certificate Display error events Change SuperAdmin credentials Change listen Interface Change listen Fort (current 9000) Disable SSL Disable Memcache for storing session Reset to default settings Return to main menu
		<u>< QK ></u>


I'm connected to Active Directory but

cannot login on the web console?

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

Open the connections in Active Directory section

▶									
Dashboard	Active Directory LDAP connections								
🛢 Your system	Manage the username and account used to browse the Active Directory. Also if you have other children Active Directory servers								
👬 Network									
Ctive Directory	+ New connection C Refresh O Authentication simulation								
🔁 Status			Search Q -						
₩Kerberos Authentication	Hostnamo	Lisor Namo	Artica Consolo						
	rostiane	User Hame	Artica Colisole						
≣ White lists	connected mainad.touzeau.maison (Default)	articaproxy@touzeau.maison	Allow						
	connected 192.168.1.90 Active directory Suffix:DC=touzeau,DC=biz	administrateur@touzeau.biz	Allow						
S DNS									

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

		michel@touzeau.maison Failed		
isManager()? [4 Checking manage Wrong username, isAdministrator Username: miche	l] - Agsinst michel@touzeau aborting [288] () ? [46] !@touzeau.maison ActiveD coryConnections Number!	.maison [286] irectoryLinked() > [52]		_
*** TEST Active BuildDefault() J BuildExternalAD Idap_bind as min	Directory [1] 192.168.1 ActiveDirectoryIndex == : 192.168.1.90:389 / DC= :hel@toureau.maison clas	[96:39] .90:355] 1 class.external.ad.inc [496] toureau,DC=biz class.external.ad.inc [48 s.external.ad.inc [303]	82]	
<pre>*** TEST Active BuildBefault() / BuildExternalAD ldap_bind as mid Authenticat</pre>	Directory [1] 192.168.1 LetiveDirectoryIndex == 192.168.1.90:389 / DC= thel@toureau.maison class ion simulation	[200] 00:380 [325] 1 class.external.ad.inc [496] toursauyCD541 class.external.ad.inc [40 s.external.ad.inc [303]	22]	
Active dreed TEST Active BuildDefault() / BuildExternalAD Idap_bind as min Authenticat	Directory [1] 192.188.1 IctiveDirectoryIndex ær 192.188.1.96.196.199 / Oc- chel@touzeau.maison clas ion simulation	(2005) 00:380 [325] 1 class.external.ad.inc [496] touzeau,DCobiz class.external.ad.inc [48 s.external.ad.inc [383] unt is able to access to the Artica Web conso	s2] ble and provide verbose logs	
Authenticat This form a	Directory [1] 192.168.1 IctiveDirectoryIdes re 152.168.1.9519 / Dc- thel@toureau.maison class on simulation	Level 000:350 [325] 1 class.external.ad.inc [496] toursauy.Ocbait class.external.ad.inc [40 s.external.ad.inc [303] unt is able to access to the Artica Web conso michel@touzeau.maison	22] ble and provide verbose logs	
Authenticat Test Active Build@faul() / BuildEsternalAD Idap_bind as min Authenticat This form a	Directory [1] 192.168.1 IctiveDirectoryIndex ar 192.168.1.06.10539 / Do- chel@touzeau.maison clas ion simulation Iows you to test if an accor User Name: Pissword:	Lever, 000:355 [325] 1 class, external, ad.inc [496] toursay, OCbuit class, external, ad.inc [44 s. external, ad.inc [303] unt is able to access to the Artica Web conso michel@touzeau.maison	s2] ble and provide verbose logs	



MONITORING THE NETWORK

REALTIME ASSET DETECTION SYSTEM

PRADS is a Passive Real-time Asset Detection System.

PRADS employs digital fingerprints to recognize services on the wire, and can be used to map your network and monitor for changes in real time.

Real-time passive traffic analysis will also let you detect assets that are just connected to the network for a short period of time, since PRADS can glean useful information from every packet.

PRADS aims to be the one-stop-shop for passive asset detection, and currently does MAC lookups, TCP and UDP OS fingerprinting as well as client and service application matching and a connection state table.

Various output plugins include logfile and FIFO and make PRADS a useful replacement for pOf, pads and sancp.

PRADS was built from the ground up for a small footprint and modern networks with IPv6 and gigabits of throughput.

Install the Passive Real-time Asset Detection System

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

select +	Collapse	1	
		prads	×
Status	Software		Action
	Realtime Asset Detection System (PRADS)		
	Realtime Asset Detection System (PRADS) PRADS is a Passive Real-time Asset Detection System.		
	Realtime Asset Detection System (PRADS) PRADS is a Passive Real-time Asset Detection System. PRADS employs digital fingerprints to recognize services on the wire, and can be used to map you	ur network and monitor for changes in real time	e.
	Realtime Asset Detection System (PRADS) PRADS is a Passive Real-time Asset Detection System. PRADS employs digital fingerprints to recognize services on the wire, and can be used to map you Real-time passive traffic analysis will also let you detect assets that are just connected to the net	ur network and monitor for changes in real time work for a short period of time, since PRADS cr	e. an glean
Uninstalled	Realtime Asset Detection System (PRADS) PRADS is a Passive Real-time Asset Detection System. PRADS employs digital fingerprints to recognize services on the wire, and can be used to map you Real-time passive traffic analysis will also let you detect assets that are just connected to the net useful information from every packet.	ur network and monitor for changes in real tim work for a short period of time, since PRADS c	e. an glean ✔ Inst
Uninstalled	Realtime Asset Detection System (PRADS) PRADS is a Passive Real-time Asset Detection System. PRADS employs digital fingerprinst to recognize services on the wire, and can be used to map you Real-time passive traffic analysis will also let you detect assets that are just connected to the net useful information from every packet. PRADS aims to be the one-stop-shop for passive asset detection, and currently does MAC lookup	ur network and monitor for changes in real tim work for a short period of time, since PRADS cr os, TCP and UDP OS fingerprinting as well as cli	e. an glean ient and
Uninstalled	Realtime Asset Detection System (PRADS) PRADS is a Passive Real-time Asset Detection System. PRADS employs digital fingerprints to recognize services on the wire, and can be used to map you Real-time passive traffic analysis will also let you detect assets that are just connected to the net useful information from every packet. PRADS aims to be the one stop-shop for passive asset detection, and currently does MAC lookup service application matching and a connection state table.	ur network and monitor for changes in real tim work for a short period of time, since PRADS cr ps, TCP and UDP OS fingerprinting as well as cli	e. anglean ient and

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

≡	Search a computer, a member							
-\/- A	ctive Requests 💿 Requests 🚡	Statistics (§ 16:	38:16 📕 Cpu:2	.5% Mem:31.9%	완 Members 및 19 computers	Admin Guide 🔋	() Log out	=
	My computers		1					
Sear	ch messages						Go!	80
	Hostname	Alias	IP Address	MAC Address	Date			
Ģ	xcc.touzeau.biz	xcc	192.168.1.222	50:6b:8d:77:19:4e	2018 Sunday September 09 10:58:59			0
Q	unknown	Enceintes-M5	192.168.1.186	b0:4e:26:4f:32:b2	16:00:04			0
Q	unknown	DESKTOP-Alex	192.168.1.34	b4:ae:2b:d8:c8:ef	16:10:06			0
Q	unknown	MBPdeAngelique	192.168.1.44	c8:09:11:e9:3d:13	16:10:06			0
Q	unknown	articadns	192.168.1.118	15:a1:44:a9:6c:78	16:10:03			0
-		DECUTOR AL	400.470.4.04		47.00.05			A



THE TRAFFIC ANALYSIS DAEMON

The Traffic analysis Daemon aka (NTOPNG) is a network traffic probe that monitors network usage.

It can be used if your Artica server is installed as a gateway of your network.

Traffic analysis Daemon shows the current network usage.

It displays a list of hosts that are currently using the network and reports information concerning the (IP and non-IP) traffic generated and received by each host. Traffic analysis Daemon may operate as a front-end collector or as a stand-alone collector/display program.

It is a hybrid layer 2 / layer 3 network monitor, by default it uses the layer 2 Media Access Control (MAC) addresses AND the layer 3 tcp/ip addresses.

It is capable of associating the two, so that ip and non-ip traffic (e.g. arp, rarp) are combined for a complete picture of network activity.

Update the package

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

Versions System version and softwares vers	ions	
Artica Core server Ope	ating system	traffic 🗶 🗸
Software	Version	
Traffic analysis Daemon (NtopNG)	📥 Install Or Update	
IP traffic summarizer	11	

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

Traffic analysis Daemon			×
Traffic analysis Daemon 3.9.200113	90.59 MB	🛓 Install Or Upgrade	1 upload



Install the Traffic analysis Daemon

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

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

Insta This sectio	all or uninstall features n allows you to install/uninstall available features on your server	
select -	Expand A Wizards	persistent 🗶 🗸
Status	Software	Action
Uninstalled	Persistent key-value db	✓ Install

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

Install or uninstall features This section allows you to install/uninstall available features on your server								
select -	Expand Mizards	Traffic analysis Daemon	× -					
Status	Software		Action					
Uninstalled	Traffic analysis Daemon	/	✓ Install					



Display statistics

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

Manager Administrator -	Search a computer, a member - Active Requests • Requests • Network monitor 3 00:52:34 Cpu:2.6% Mem:24.7% 28 Members Admin Guide
Dashboard	4 ULogout ﷺ
Your system	
🚓 Network	Install or uninstall features
S DNS	This section allows you to install/uninstall available features on your server
# Your proxy	
ACLs Proxy	select - Expand A Wizards

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

Contribute to the propreference.	pject by sending	encrypted, anonyn	 Flows nous telemetry 	Hosts + data to ntop.or	Interfaces ← g: visit the ▲Pre	oferences pag	Q Search	×
Dashboard: Talk	ers Hosts	Ports Applica	tions ASN	s Senders				
Top Hosts (Send+Re 15' 192.168.1.97 192.168.1.97 19.4% - Other	7.1% 1.101.0.133	36 , 192 5.0% 92.168.1.214	% .168.1.237					
ntopng Community Edi User nologin Interface	ition v. <mark>3.9.1</mark> 90529 eth0	0% 16.26	kbit/s [7 pps]	↑ <u>\</u> ↓ <u>\</u>	4.90 kbit/s @ 1.36 kbit/s	01:11:01 +0200 6	0 Uptime: 13:43 41 Devices 271 Flows	



Status and configuration.

On the left menu, choose "Network" and "Network Monitor" menu.

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

Interfaces to monitor.

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

■ Your system	Traffic analysis Daemon v3.9.200113 Traffic analysis Daemon is an open-source network traffic monitor. It is designed to be a high-performance, low-resource network traffic analyzer. It is able to display real-time flow analysis for connected hosts.								
Sourcetwork Your network Vour Firewall Databases Logs center	Traffic analysis Daemon Running Since 17mn 54s Memory used: 179 MB	Main parameters Monitor Interface(s): HTTP service	ethO	choose					
	Persistent key-value db Running since 17mn 59s Memory used: 3.02 MB	Activate Login Page:	OFF	« Apply »					

Networks to monitor.

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

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

Dashboard					
E Your system	Your networks				
Network	Set your local newtorks in this area in order to drive network services such	as the Network scanner, IDS, firewall	, proxy		
≓Interfaces					
A Routing rules	+ New network 🖬 Scan your network 🖬 Apply Firewall rules	Restart Traffic analysis Daem	ion		
			_		
Network monitor	bled Networks	Trusted network	% used Ping	Scan Scan report 0 Items	DEL
DNS	✓ 192.168.100.0/255.255.255.0 Network 192.168.100.0/255.255.255.0	-	-	-	0
Your Firewall	✓ 192.168.5.0/24 The firewall accept to route all protocols to this network, (No information added)	~	-	-	0
Databases	172.16.5.0/255.255.255.0				
Logs center	The firewall accept to route all protocols to this network, Network 172.16.5.0/255.255.255.0	~	-	-	0
	✓ 192.168.10/255.255.25.0 The firewall accept to route all protocols to this network, Network 192.108.10/255.255.0	~	-	-	0



MONITORING THE SYSTEM

SYSTEM HEALTH MONITOR

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

You will find the watchdog in Your System / Watchdog

Monitoring the system Load

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

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

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

For example :

4 Cpus = 1.5*4 = 6

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

Monitoring CPU / Memory / Disks

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





Display incidents reports

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

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

Manager Administrator ↔	■ Search messages ■Cpu:1.5% Mem:38.5%/2.93 GB 小- Active Requests ④ Requests ① 23:42:12 PS Members LAdmin Guide 早
Dashboard	⊕Log out f⊟
📑 Your system	
System information Your hard disks Vour hard disks Memory swapping Your system memory System events Features CopenSSH server Glances Tasks	System health monitor Monitor the system performance and create reports/notifications when reach limits Parameters Even s Incidents • Go!
Certificates Center	Time Incidents DOWN DEL
■ Backup PLicense ④ Update	21:42:58 System exceed load average 15mn policy - 5 load



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.

elect 👻 📑 Expand		
		Advanced Monitoring se \star
atus	Software	Action
atus	Software	Action

Access to statistics

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

Monitor (0 11:54:25) Cp	bu:7.7% Mem:35.1% 浴 Me	embers 🌹	() Log out
my-netdata - smtp.touzeau.biz	≜	• ± ± +	0
System Overview verview of the key system metrics. Image: system down Image: system down <tr< td=""><td>at all. You can get per core usage at the CPUs section a s constantly high, your disks are a bottleneck and they sk (0.00%). A constantly high percentage of softu 122:83.8 mon. Nov 05. 2018</td><td>Cpu toad disk ram swap network processes idejiter interrupts softnet entropy ipc semaphore uptime ow F CPUs Memory ind Disks Networking Disks Iby Networking Iby Networking</td><td>yerview is 9 Stack Arking prking</td></tr<>	at all. You can get per core usage at the CPUs section a s constantly high, your disks are a bottleneck and they sk (0.00%). A constantly high percentage of softu 122:83.8 mon. Nov 05. 2018	Cpu toad disk ram swap network processes idejiter interrupts softnet entropy ipc semaphore uptime ow F CPUs Memory ind Disks Networking Disks Iby Networking Iby Networking	yerview is 9 Stack Arking prking
estimates and the number of processes using CPU or wailing for s to 1, 5 and 15 minute averages. The system calculates this once every 5 sec system.load ()	a contraction of the second s	A for the form A form	ng gerfaces stiffter) a ps anitoring charts slarms

Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com



SMTP NOTIFICATIONS

Artica is able to send by SMTP the content of system events.

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

Manager Administrator -	E Search messages ■Cpu:19.7% Mem:53.8%/3.81 GB √~ Active Requests @ Requests E Statistics ① 23:46:56 ≉2 Members	
Dashboard	BAdmin Guide 📮 () Log out ﷺ	
🚍 Your system		
System information	System events	
System events	Search messages	Go!
>_ OpenSSH server	🛅 Empty 🖺 Expor: 🖾 eMail notifications	
() Tasks	Search Q	•
Certificates Center Backup	Date Events Daemon	
₽ License	23:30:04 QIOVERLOADED] system: 3.75, aborting unction:squid_admin_mysql, line:89 exec.syslog-engine.php	
⊕ Update	23:30:04 Q 3.75: Overloade. them aborting task Host: function:start, line:16 exec.mpstat.php	
	22:14:34 Red, Yellow, rigreepdate.php	
 Internet access RESTful 	22:00:16 Q NTP: 2 Mar 22:00:16 ntpdate[54403]: adjust time server 37.187.104.44 offset -0.020265 sec Host: function:,line:179 exec.ntpdate.php	

Configuring notifications

Click on the eMail notifications buttons	eMail notifications			×
To enable SMTP notifications, turn on the "Enable SMTP notifications" checkbox.				
If you want to be notified when an administrator try to logon on the Artica Web console, turn on	⁶ eMail notifications			
the " Web console accesses " checkbox.	If green then watchdog will send SMTP	notifications when encounter issues		
If you want to be notified when something try to logon on the SSH service, turn on " SSH Login	Enable SMTP Notifications:	ON		
attempts" checkbox.	Web Console Accesses:	OFF		
By default you are notified only on critical issues	SSH Login Attempts:	OFF		
(red), if you want to be notified on "Warning	Warning Events (Warning):	OFF		
issues too", turn on the "Warning events" checkbox.	Mail Server Name:	Mail server name		۵
Set the address of the SMTP server that will	SMTP Server Port:	- 25		+
receive generated events in the "Mail Server Name" field.	Enable TLS Support:	OFF		
	Sender Mail Address:	user@domain.tld		
TLS support checkbox.	Your Email Address:	user@domain.tld		
Define the eMail address of the sender of the	Username AUTH:	Username AUTH		
message.	Password AUTH:	Password AUTH		
In your eMail address field, define the recipient that will receive notifications messages. If you want to add more than one recipient,		Password AUTH (Confirm		
separate them by a comma.				
NOTE: BEFORE CLICK ON THE SEND TEST MESSAGE, YOU HAVE TO CLICK ON APPLY BUTTON FIRST			« Send Test Message »	« Apply »





ZABBIX AGENT

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

Youtube video



https://youtu.be/Y1xLJeY4308



THE SNMP SERVICE

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

Upgrade the SNMP software.

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

Dashboard Tour system System information System memory Memory swapping Watchdog	Versions System version and softwares versions Opdate Index Softwares	snmp × -
⊕ System events	Software Version	
>_ OpenSSH server	SNMP daemon: 5.7.3	Dr Update
₿ Glances O Tasks ♥ Cartificates Cantor	1	
SNMPv3		
■ Backup P License ① Update □ Weithensole	Copyright Artica Tech © 2004-2020	v4.29.031912 Enterprise Edition (Gold License)
iVersions		

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





±

MaPHCODE

Passphrase

Install the SNMP service

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

Insta This sectio	all or uninstall featu	res on your server
select -	Expand <u>A</u> Wizards	simn
Status	Software	Action

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

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

SNMPv2

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

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

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

Turn to only SNMPv3

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

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

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

Jpon receiving a request, it p nformation to the sender. ur hard disks Status/Parameters Events Watchdog Parameters #Features Listen Interface Interface eth0 (eth0) IMP da 161 Listen Port: Running Glance Organization: Artica tech ce 7mn 51s ov used: 6.9 MB **O** Tasks Certificates Cent System Contact: david@articatech.com SNMPv3 SNMPv1/SNMPv2c Backup Disable: ON ⊕ Update SNMP Community (SNMPv2c): public П Web Console Remote SNMP Console IP Address (SNMPv2c): default i Versions 2020-01-26) x86 (Internet ac SNMPv3 SHA/AES **W**RESTful Success R Suppor User Name Pas ord •••••• ••••••

Monitor your system: SNMP v5.7.3

aits requests from SNMP

SNMP service is an SNMP agent which binds to a port and aw

Manage the SNMP service Via RESTful API

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

🛢 Datab

Logs ce



Add host using SNMPv3 on LibreNMS

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

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

Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

V3 ♥ 161 ud	p v
ifIndex v	
authPriv	
dtouzeau	
MyDavidP@\$\$word	
SHA	~
MaPHCODE	
AES	~
OFF	
	ifIndex ifIndex if



THE LOGS VIEWER

By default, latest Artica versions install the module "Logs Viewer".

Logs Viewer is a feature you can install that allows you to search, tail in logs files of your server.

I his sectio	on allows you to install/uninstall available feat	ures on your server	
elect 🗸	Expand & Wizards	logs	× -
tatus	Software		Action
Installed	Logs Viewer		✓ uninstall

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



TROUBLESHOOTING

Read-only filesystem

The default behavior for most Linux file systems is to safeguard your data.

When the kernel detects an error in the storage subsystem it will make the filesystem read-only to prevent (further) data corruption

on line 24				
PHP Notice: U	ndef ined	offset:	1 in	/usr/share/artica-postfix/exec.menu.ips.php
on line 25				
PHP Notice: U	ndef ined	offset:	1 in	/usr/share/artica-postfix/exec.menu.ips.php
on line 26				
PHP Notice: U	ndef ined	offset:	1 in	/usr/share/artica-postfix/exec.menu.ips.php
on line 27				
PHP Notice: U	ndef ined	offset:	1 in	/usr/share/artica-postfix/exec.menu.ips.php
on line 28				
PHP Notice: U	ndef ined	offset:	1 in	/usr/share/artica-postfix/exec.menu.ips.php
on line 29				
PHP Notice: U	ndef ined	offset:	1 in	/usr/share/artica-postfix/exec.menu.ips.php
on line 30				
[439] [ROOT]::	:::socket	s/stream	_fran	mework:: As root -> "stream_framework(setinfo
s.php?key=QXJ0	aWNhSHR0c	FUzZUNTT	A%3D;	%3D&value=MQ%3D%3D)" called by exec.menu.ips
.php SET_INFO() line 35	in clas	5.500	ckets.inc
PHP Warning:	stream_so	cket_cli	entC): unable to connect to unix:///usr/share/art
ica-postfix/re	ssources/	web/fram	ewor]	k.sock:80 (Connection refused) in /usr/share/
artica-postfix	/ressourc	es/class	.socl	kets.inc on line 1117
[439] [ROOT]::	:::socket	s/stream	fra	mework:: ERROR: unable to oven remote file ht
tp://127.0.0.1	:47930/se	tinfos.pl	hp?ke	ey=QXJ0aWNhSHR0cFVzZVNTTA%3D%3D&value=MQ%3D%3
D in class.soc	kets inc			
PHP Warning:	chmol():	Read-only	∫ fi]	le system in /usr/share/artica-postfix/exec.m
enu.ips.php on	lin•68			

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

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



Artica V4 Documentation – david@articatech.com	П
GNU GRUB version 2.02+dfsg1-20	
Debian GNU/Linux with Linux 4 19 0-6-amd64	
Debian GNU/Linux, with Linux 4.19.0-6-amd64 (systemd)	
*Debian GNU/Linux, with Linux 4.19.0-6-amd64 (recovery mode)	
Use the ↑ and ↓ keys to select which entry is highlighted. Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line. ESC to return previous menu.	

The screen will ask you to press $\ensuremath{\textbf{Control-D}}$ or enter the root password.

Begin	i: Runn	ning /scri	ipts∕ini	t-bottom	. done	٥.		
NIT:	versi	ion 2.93 I	booting					
[info] Usir	ng makefil	le-style	concurrent	: boot	in	runlevel	s.
Give	root p	bassword f	or main	tenance				
(or p	oress Ö	Control-D	to cont	inue): _				

Enter the root password (by default the keyboard is $\ensuremath{\mathsf{QWERTY}}\xspace$) Run this command-line

fsck -p -f

reset your server



The Daemon monitor not running

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

This caused by an outdated Daemon monitor configuration.

Update to nightly 4.29 or 4.30 Artica release.

	Messages		Me
ing	Notifications		
	Д 535 Events		
ories			
	critical	about 5 Hours	
	Daemon monitor is not running, start it 📀		
	Midday 34:01		
	critical	about 5 Hours	
	Daemon monitor is not running, start it 🥹		
	Midday 32:02		
	critical	about 5 Hours	
	Daemon monitor is not running, start it 🥹		
	Midday 28:01		Tip



THE LDAP SERVER SERVICE

The LDAP database is used by Artica in order to manage members.

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

The LDAP service can be installed in the Features section

in "Members services/LDAP Server."



OPENLDAP SERVICE PARAMETERS.

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

Listen Interface: By default the LDAP server serves only the loop back address because all services used	Manager Administrator →	Ξ Searc	ch a computer, a membei	Req	uests 🔇 08:48:02 🔳	Cpu:3% Mem:30.7% 양	Members 2	() Log out
by Artica don't need to access the database externally	∷ Dashboard ■ Your system	LDA The OpenL	P server DAP service is a standard database that allows	you to manage members,	administrators locally.			
LDAP suffix: Is the main LDAP branch used to store users	금 Network & NICs 클 DNS	With the O	penLDAP service you can authenticate your me	embers for Internet acces	parameters			-
Multi-Domains: If enabled, Artica will use the eMail address has the login username. In this case, users need to put their eMail address to log in to all	⊕ Your proxy ♥> Your categories		LDAP service Running	Mandatories set	tings are stored on an LDAP d	atabase, personalize, optimize i	the OpenLDAP sett	ings
services that use LDAP. Log level: is the trace level used for the LDAP service (logs are stored in syslog)	🖳 Statistics 🖹 Logs center 🕃 Databases		since 2h 16mn 35s Memory used: 8.36 MB CRestart	General setting	s Listen interface: LDAP Suffix:	Loopback (127.0.0.1) dc=domain,dc=company	y,dc=tld	•
Restart periodically OpenLDAP service: If turned on then Artica will restart OpenLDAP service at 6h30,12h30,3h30	E PostGreSQL				Multi-domains: Log Level:	ON Basic		-
Restart service each: Define the period that will stop an service in order to refresh memory.	d start the LDAP		Restart periodically Oper	hLDAP service:	ON			
Lock LDAP configuration: If enabled, Artica will not mo /etc/ldap/slpad.conf and let you change it.	dify the		Restar Lock LDAP	t service each:	3 Days		Ŧ	
Allow anonymous login: Permit to read the LDAP datab logged as a member.	base without need t	to be	Allow and	onymous login: 3 subsystem	OFF			-
			size of the shared memory bu	ffer pool (MB):	- 5		+	
			number of entries mainta	ain in memory:	- 1000		+	
							« Apply »	



MANAGE LDAP MEMBERS/GROUP

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

	() 03:45:21	📳 Cpu:19.1% Mem:32.3%	² Members	2	() Log out	š	
-				-			-

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

to create a user, click on the button "New member"

My members				
Search				Go!
울+ New Member				
			Search	Q -
Display Name	EMail Address	Office Phone	Groups	
	N	lo results		

A wizard is displayed and ask to you in which organization the member must be stored.

You can choose in the drop-down list an already organization or you can create a new organization by adding the new organization name in the "Create a new organization" field.

New Member » You are in the organ	ization	
Create a new organization:	Create a new organization	
Organization:	Articatech	Ŧ
		« Next »
		« Next »

Define the group that will store the user

You can create a new group. Set the group name in the "new group" field or select an already created group by choosing it in the "Group" drop-down list.

New Member » Articatech » Group		
Organization:	Articatech	
New group:	Administrators	
Group:	None	•
Domain:	None	v
		v bloot v

- 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.



Organization:	Articatech	
Group:	Administrators	
Domain:		
First Name:	David	1
Last Name:	Touzeau	
eMail address:	david.touzeau@company.com	
User id:	david.touzeau	
Password:	•••••	P
	•••••	P

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.

5% David Touzeau Save		
20% David Touzeau Save		
New Member » Articatech » Admi	nistrators	
Organization:	Articatech	
Group:	Administrators	
Domain:		
First Name:	David	A
Last Name:	Touzeau	
eMail address:	david.touzeau@company.com	
User id:	david.touzeau	
Password:		Ð
		۹

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

Sea	arch				Go
2+	New Member				
				Search	۹.
	Display Name	EMail Address	Office Phone	Groups	
3	Administrators	-	-	-	6
	David Touzeau		00.00.00.00	Administrators	6

Artica V4 Documentation – david@articatech.com



Import members from a text/CSV file

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

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

E Search a com	outer, a membei			_					
	- √- Active Requests	Requests	() 23:50:43	📕 Cpu:14.5% Mem:19.6%	²⁸ Members	🗟 Admin Guid	de 🧧	() Log out	1
My mem	bers								Go!
온+ New Membe ·	음+ Import					Search		٩	•

If you want to import users only on a group choose your LDAP group.

If you want to import users inside several groups and let Artica creating groups:

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

	Company » Group	
	Organization:	MyCompany
	New group:	New group
	Group:	Users
		None
		Administrators
		Users
oort users fi	rom a text file	
mport My	Company/Use	rs
This section allo	ws you to import users fror lect this structure:	n a text file.

Click on the upload button to browse your data file

It must reflect this structure:

Each line is separated by a carriage return and a line must be :**username;mail;userid;password;PostalCode;Address;mobile;Phone** line must be: value1;value2;[carriage return] If you want to import aliases, add at the end all aliases with a comma separated. user;mail;id;password;cp;adress;mobile;phone;alias1,alias2,alias3...

An example of text to import can be downloaded using this url (<u>http://articatech.net/download/import-members-example.txt</u>)



Exporting users to a CSV file

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

My members		
Search messages		
& New Member		
Display Name	EMail Address	Office Phone
绺 Artica_group	-	-
postmaster postmaster	postmaster@touzeau.maison	00.00.00.00
榕 Group	-	-
啓 Netstars Matrix Design	-	-
완 Borders Books	-	-
완 Endicott Johnson	-	-
원: Source Club	-	-
総 Dubrow's Cafeteria	-	-
整 Profitpros	-	-
榕 Best Biz Survis	-	-
	« « " 1 2	3 4 5 > » of 20

A confirmation message wil ask you to confirm the exportation.

Export Members	×
Export Members	
5% exporting Member afection 302/29794/1	

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





RESTful API for managing LDAP users.

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

Install or This section allows yo	uninstall features	
select 🕶 🖬 Expan	NG CONTRACTOR OF CONTRACTOR	Idap 🗶 👻 🗸
Status	Software	Action
Installe	d LDAP server	✓ uninstall
Uninsta	LDAP server RESTFul	✓ Install

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

LDAP server The OpenLDAP service is a standard database that allows With the OpenLDAP service you can authenticate your me	you to manage members, administrators locally. mbers for Internet accesses.	
LDAP service	LDAP Database parameters Mandatories settings are stored on an LDAP dat	tabase, personalize, optimize the OpenLDAP settings
Running since 21mn 42s Memory used: 8.24 MB	General settings	
C Restart	Listen interface:	Loopback (127.0.0.1) ▼ dc∝nodomain
RESTINIAPI Active	<u>Multi-domains:</u> Log Level:	ON Basic *

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

Configuring the LDAP BDB subsystem			
ze of the shared memory buffer pool (MB):	-	5	+
number of entries maintain in memory:	-	1000	+
RESTFul API			
RESTFul API API Key:	ky№	lóixXavn8sE7P9GoBY	gX3by6ZaRCc5

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

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

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

Manage organizations

List LDAP organizations

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

Create MyCompany organization:

POST: https://server:9000/api/rest/ldap/organization/create + field= "name"

PHP example width curl:

```
$ch = curl init();
$CURLOPT HTTPHEADER[]="Accept: application/json";
$CURLOPT_HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT HTTPHEADER[]="Expect:";
$CURLOPT_HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5";
$MAIN_URI="https://192.168.1.173:9000/api/rest/ldap/organization/create";
curl_setopt($ch, CURLOPT_HTTPHEADER, $CURLOPT_HTTPHEADER);
curl setopt($ch, CURLOPT TIMEOUT, 300);
curl_setopt($ch, CURLOPT_URL, $MAIN_URI);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYHOST,0);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER,0);
$POSTz=array("name"=>"MyCompany"); // Create the MyCompany Orgnization
curl setopt($ch, CURLOPT POSTFIELDS, $POSTz);
$response = curl exec($ch);
$errno=curl errno($ch);
if($errno>0){
   echo "Error $errno\n".curl error($ch)."\n";
   curl_close($ch);
   die();
}
$CURLINFO HTTP CODE=intval(curl getinfo($ch,CURLINFO HTTP CODE));
if($CURLINFO HTTP CODE<>200){
   echo "Error $CURLINFO HTTP CODE\n";
   die();
$json=json decode($response);
if(!$json->status){echo "Failed $json->message\n";die();}
echo "Success\n";
```

Delete MyCompany organization:

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

List members inside MyCompany organization:

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

Manage Groups inside an Organization

List groups in MyCompany

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

Create a group inside MyCompany

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

Delete the group Administrator inside MyCompany with gidnumber 500

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



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

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

PHP example:

```
$ch = curl init();
$CURLOPT HTTPHEADER[]="Accept: application/json";
$CURLOPT HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT_HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT HTTPHEADER[]="Expect:";
$CURLOPT HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYgX3by6ZaRCc5";
$MAIN URI="https://192.168.1.173:9000/api/rest/ldap/organization/MyCompany/groups/500/add";
curl setopt($ch, CURLOPT HTTPHEADER, $CURLOPT HTTPHEADER);
curl_setopt($ch, CURLOPT_TIMEOUT, 300);
curl_setopt($ch, CURLOPT_URL, $MAIN_URI);
    setopt($ch, CURLOPT RETURNTRANSFER, 1);
curl
curl setopt($ch,CURLOPT SSL VERIFYHOST,0);
curl setopt ($ch, CURLOPT SSL VERIFYPEER, 0);
$POSTz=array(
   "uid"=>"Jhon.doo",
   "DisplayName"=>"Jhon doo Mhain",
   "givenName"=>"Jhon",
   "name"=>"doo Mhain"
   "password"=>"123456"
);
curl setopt($ch, CURLOPT POSTFIELDS, $POSTz);
$response = curl_exec($ch);
$errno=curl errno($ch);
if($errno>0){
   echo "Error $errno\n".curl error($ch)."\n";
   curl close($ch);
   die();
}
$CURLINFO HTTP CODE=intval(curl getinfo($ch,CURLINFO HTTP CODE));
if ($CURLINFO HTTP CODE<>200) {
   echo "Error $CURLINFO HTTP CODE\n";
   die();
}
$json=json decode($response);
if(!$json->status){echo "Failed $json->message\n";die();}
echo "Success\n";
```

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

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

Link user Jhon.doo inside $\ensuremath{\text{MyCompany}}$ 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.

Insta This section	II or unins allows you to install/u	stall feature	Son your server				
select 🕶	C Expand			ssh		×	•
Status	Software			Acti	ion		_
Uninstalled	OpenSSH server					🗸 İnsta	all
	SSH System Consol	e		4	Require activa	ited OpenSSH serve	er

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

SSH SERVER SECTION

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

 Dashboard Your system 	OpenSSH server 7.4p1 Debia OpenSSH (OpenBSD Secure Shell) is a set of computer programs pr
📾 Your hard disks	
Memory swapping	Status Events
System events	
∀ Features	Gen
>_ OpenSSH server	
Glances	
() Tasks	OpenSSH server
Certificates Center	Running



PUBLIC KEY AUTHENTICATION WITH PUTTY

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

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

Click the Generate button.

You will be prompted to move the mouse over the blank area to generate some randomness.

Do so. Shortly thereafter, the program will generate the key and display the result

After keys have been generated.

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

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

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

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

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

PuTTY Key Gene	rator	? 2
e Key Conversions	Help	
Key		
Public key for pasting	into OpenSSH authorized_ke	ys file:
ssh-rsa AAAAB3NzaC1yc2E/ SXIcrWk/2TH9D+/G UtitPIKw2Mq8dHoAA U7w== rsa-key-2006	AAAABJQAAAIBtWH/RU5kLf in9xHNCe/7xnhZNYVd9Yxu0 yR7X4P7PaCQEMtdWv88CF 1213	RYnO/y2S9Fi1dXhRB2oqxqTZV30 IQQ+WmJ2GK94mtMmd45auyYhy2 es9MLIwqzSkBLYFIXHUtrzLShUl/n
Key fingerprint:	ssh-rsa 1023 0e:38:42:25:c	d:cc:94:d4fa:04:32:ee:60:99:55:9c
Key comment:	rsa-key-20061213	
Key passphrase:	•••••	
Confirm passphrase:	•••••	
Actions		
Generate a public/priv	vate key pair	Generate
Load an existing priva	te key file	Load
Save the generated k	ey Sa	ave public key Save private key
Parameters		
Type of key to genera O SSH-1 (RSA)	te:	◯ SSH-2 DSA



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

Login grace time (Seconds):	- 120
Max sessions:	- 10
Max authentications attempts:	- 6
Log Level:	INFO
AuthorizedKeysFile:	/etc/ssh/authorized_keys Authorized Keys

Click on the "New key" button

OpenSSH server >> Authorized Keys			
+ New key Authorized bys		Search	Q -
	No results		

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

OpenSSH ser	ver >> Authorized Keys >> New key	×
Authorized	Keys	
ssh-rsa:	sthrss AAAAB3NzaC1vc2EAAAABJQAAAQEAgx+saPolYfU9i3vGpn4ehMPowhQ8MnmEBsulkm2in/zl/ZEPAw+27+hlT tuzYMxzwx2vc2N0DMn63X/CT8n/iiJlwnN/6rbxNscaas.JVLK7XERvhsvAFze7z=4vxK6zTCQSkJwmBn5AdJvJHU/ ZQwp3rir+BXvZIM2t5sEzitFXmNRTES:YCEXwi88P6UQRHWR74U/3f6xdZw7BTMfXk7s8/lbhCx98r/jvv9lal:BE 6mx1wYGKpe5xsaMsY0yV0b0XQvKsNZhjLwdoXtYPeNSILhd9zH055kqcy7mo7utpQPwPqQ9BsE+QZQRz9EtBe vf0z0MfZWwViehm31bVWzQ== zsa-ksy-20190313	
	« add »	

Key is added in the table.

		Search	۹ -
s			
3NzaC1yc2EAAAABJQAAAQEA	gx+saPoLYfU9i3yGpn4ehN	1PowhO8MnmFBsuLkm9in/zl	C
	s 3NzaC1yc2EAAAABJQAAAQEA	s 3NzaC1yc2EAAAABJQAAAQEAgx+saPoLYfU9i3yGpn4ehN	s 3NzaC1yc2EAAAABJQAAAQEAgx+saPoLYfU9i3yGpn4ehMPowhO8MnmFBsuLkm9in/zl



Execute the putty.exe

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

Session	Basic options for your PuTTY	session
E. Terminal Keyboard Bell	Specify the destination you want to con Host <u>N</u> ame (or IP address) 192.168.1.137	nnect to Port 22
Features Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH	Connection type:	SH Senjal
····· Senal	Close window on e <u>xi</u> t: Always Never Only or	n clean exit

Go to Connection > SSH > Auth window.

Browse to select *.ppk in the "Private key file for authentication" text box.

Be sure to go back to the Session window and click Save to update the profile.

The session will use public key authentication

You can also add the user in Connection > Data > Auto-login username in order to not be prompted for the Login name.



How to replicate Public keys on severals Artica servers?

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



THE SSH WEB CONSOLE

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

select - Expanse		
	•	
		ssh 🗙 🗸
Status	Software	ssh 🗶 🗸
Status	Software OpenSSH server	Action

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

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





Restrict the SSH access to the Web console.

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

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

OpenSSH server 7.4p1 D OpenSSH (OpenBSD Secure Shell) is a set of computer pr	Debian-10+deb9u4	ins over a computer network using the ssh protocol.
Status Events		
	General settings	
OpenSSH server	Allow access only trough Web console:	
Running	Listen interface:	All interfaces v
since 10mn 15s Memory used: 3.25 MB	listen port:	- 22 🗄 +
	Strict modes:	ON
🔁 Restart	Permit Root Login:	ON
	Allow only specified groups:	Allow only specified groups
📓 Config file	Limit access:	Oltems Manage
	Use banner:	OFF Banner

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

Restrict Access according Geo-Localization of remote addresses.

You can enable "Deny Countries" inside the OpenSSH section.

To make this feature working, you need to use the latest Debian 10 operating system and enable the GeoIPUpdate under features

Insta This section	all or uninstall featur	res on your server	
select ▼	Expand A Wizards	geo	X -
Status	Software	-	Action
Uninstalled	GeoIPUpdate		✓ Install



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

listen port:	- 22
Strict modes:	ON
Permit Root Login:	ON
Allow only specified groups:	Allow only specified group
Limit access:	0 Items Manage
Deny countries:	253 Items Manage
Use banner:	OFF Banner

 ${\it Click on the button "Deny all" in order to deny all countries and uncheck only countries you want to allow.}$

it by country		
	50	
$\overline{\mathbf{x}}$	Search	۹ -
Countrie		Deny
Anonymous F xy		~
Satellite Provider		~
Other Country		~
Andorra	•	~
③ United Arab Emirate	25	~
Afghanistan		~
Antigua and Barbud	a	~
Anguilla		~
Albania		~
Armenia		~
	« « … 1 2 3 4 5 … » »	
	1 of 26	



THE SYSLOG SERVICE / LOG SERVER

The syslog service is able to receive events from any Linux/Artica servers in order to store them and perform a central syslog server.

By default, Artica use the local syslog service in order to store local events. Enable this service allows you to transform your Artica server into a syslog receiver.

INSTALL THE SYSLOG FEATURE

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



Status Software Uninstalled Syslog Daemon service	select - Expand		
Uninstalled Syslog Daemon service	Status Coffwara	sysl	× -
	Uninstalled Syslog Daemon service		✓ Install

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

David Administrator -	E Search a computer, a member		() 15:28:32	Cpu:5.6% Mem:22.3%	양 Members	6	() Log out
III Dashboard III Your system Active Directory	Syslog Daemon service v This feature allows you to transform an Artica server into a Each remote Artica servers are able to send their syslogev Status	8.24.0 a systogreceiver. ents to this server in order to store them in a c	central way.				
≣ DNS la: Statistics B Logs center B Legal logs ≣ Svolog Daemon service	Syslog Daemon Running since 1h 52mn 21s	General settings Disable UDP sockets: Listen interface: listen port:	Interface eth0	(eth0)		2	•
S Databases	Memory used: 2.05 MB ♂Restart	TCP/IP protocol Enable TCP/IP sockets:	ON				
		listen port: Use SSL: Certificate:	- 5514 ON None				+



SECURING YOUR SYSLOG SERVER WITH TLS (SSL)

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

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

On the syslog service parameters:

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

	General settings Disable UDP sockets:	OFF	
Syslog Daemon Running	Listen interface:	Interface eth0 (eth0)	٣
since 2h 1mn 2s Memory used: 2.13 MB	listen port:	- 514	+
€ Restart	TCP/IP protocol		
	Enable TCP/IP sockets:	ON	
	listen port:	- 5514	+
	Use SSL:		
	Certificate:	syslog.touzeau.biz	٣
		4	
		<pre>« Appl</pre>	у»


Artica offer 3 main services for providing DNS services.

1. The Load-Balancing DNS service:

It is a DNS service that is able to cache DNS requests and forward them to a pool of DNS server in load-balancing mode.

This DNS service can use ACIs to switch DNS requests to a specific pool according to a group source IP addresses and/or a group of destination domains

2. The PowerDNS system:

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

3. The DNS Cache service:

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



THE DNS LOAD-BALACING SERVICE

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

Install the DNS Load-balancing service

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

This section a	llows you to install/uninstall availabl	e features on your server		
select 🕶 🛛	Expand <u>A</u> Wizards			\
			dns load	×
Status	Software			Action
				-

THE DNS CACHE SERVICE

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

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

Enable	logging.

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

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

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

Write to a local file

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

DNS Cache service v1./. The local cache DNS service is designed to speedup Interr	3 let access by reducing the DNS queries latency.
Status Cache Statistics	
	Local DNS service
	Display server name and version:
DNS Cache service	Use Internet Root DNS Servers:
Running	Listen Network Interfaces:
since 2h 30mn 54s Memory used: 24.13 MB	Listen only the loopback interface
C Restart	Outening Interface All Interfaces
	Log querres.
	Syslog



Page: 109



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





DNS Cache service
 SafeSearch(s)

CONS Servers

Forward zones

Hosts file

Send to a syslog server.

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

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

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

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

Syslog		
Send events by syslog:	ON	
Remote Syslog server:	192.168.1.153	\$
listen port:	- 514	+
Enable TCP/IP sockets:		
Use SSL:	ON	
Certificate:	syslog.touzeau.biz	٣

SafeSearch(s)

If you use the DNS cache service, you can enable SafeSearch(s) on the major Web search services. (need a valid Corporate License)

Currently Artica is able to enable SafeSearch for **Google**, **Qwant**, **Bing**, **YouTube**, **Duckduckgo** SafeSearch(s) is in the left menu under DNS/SafeSearch(s).

SafeSearch(s) is designed to modify the DNS answer of **your workstations** (if you plan to use Artica as the Internet DNS service) or **your proxy service** if the proxy uses the DNS cache service to resolve the Internet.

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

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

	SafeSearch(s) Google offer a SafeSearch [™] feature which blocks This option enforce the safesearch policies of the	most adult in Google searc	lages. h engines.	
	Parameters			
service	Force SafeSearch (Google):	ON 📕		
rs	Owant SafeSearch:	OFF		
es	Bing SafeSearch:	OFF		
	Youtube (strict):	OFF		
rs	Youtube (Moderate):	OFF		
	Duckduckgo:	OFF		
			-	
				« Apply »



Reverse lookup private zone

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

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

E Dashboard			
🚍 Your system	Forw	ard z	ones
👬 Network	Forward zones set the DNS service to query remote DNS serv		
S DNS	_		
S DNS Cache service	+ New forv	ward zone	Reconfigure service
▼ SafeSearch(s)			
CONS Servers	Zone	DNS Se	erver
↔ Forward zones	(A) (*)	111 احد	1.952 5
G Statistics	(#) All (*)	71.1.1	1:053 9

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

For examples:

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

w forward zone		
New forward zone	1	
Set the DNS conver that is able to recolv	a best on the specific domain	
Set the Division of the the to resolv	тиона и не зресинскопали.	_
Domain:	168.192.in-addr.arpa	1
IF Address.	192.168.1.90	
listen port:	- 53 -	F
Use TLS:	OFF	
	« add »	

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

Secure DNS over TLS

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

Create a DNS over TLS service. (Server mode)

1) Create a certificate:

Go into the certificate center and add/create your certificate.

C Statistics L Hosts file My computers

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

	DNS over TLS		
	DNS over TLS (DoT) is a security protoc queries and answers via the Transport L The goal of the method is to increase use manipulation of DNS data via man-in-th	ol for encrypting and wrapping Domain Name System (DN ayer Security (TLS) protocol. er privacy and security by proventing eavesdropping and e-middle attacks.	IS)
	Enable DNS over TLS:	ON	
	listen port:	- 853	+
	Certificate:	articadns.touzeau.biz	·
Ouery DNS over TI S server	- c		
Some free public ISP offers DNS Over T	LS public DNS:		S DNS
 Quad9: 9.9.9.9.853 or 9.9.9.1 Cloudflare: 853 or 1.0.0.185 Google: 8.8.8.853 or 8.8.4.4 CleanBrowsing Security Filte 	0:583 3 1:853 1:852 228 168 9:853 and 185 228 1	169 9-853	 DNS Cache service SafeSearch(s) CNS Servers
 CleanBrowsing Family Filter: CleanBrowsing Adult Filter: 1 Adguard defaiult: 176.10 176 Adguard Family: 176.103.130 	185.228.168.168:853 and 185.228. 185.228.168.10:853 and 185.228.16 5.103.130.132 or 176.103.130.134 3 0.132 or 176.103.130.134	.169.168:853 59.11:853 3.130.130 or 176.103.130.131	♣ Forward zones ♣ Statistics ➡ Hosts file
To use these IP address, on the left Click on " New forward zone "	menu, get DNS/Forward zones.		G My computers
=	Your system	ward zones	
. .	Network Forward	zones set the DNS service to query remote DNS servers from a sp	ecific domain.
9	DNS		
	SDNS Cache service	orward zone 🖬 Reconfigure service	
	▼ SafeSearch(s)	T	
	DNS Servers Zone Forward zones	DNS Server	



No res



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

New forward zone		×	
New forward zone			
Set the DNS server that is able to resolve	hosts from the specific domain.		
Domain:		±	
IP Address:	11.1.1	\$	
listen port:	- 853	+	
Use TLS:	ON		
	_	_	
	« a	dd »	

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

Forward zones

Forward zones set the DNS service to query remote DNS servers from a specific domain.

+ New f	orward zone	Reconfigure service
Zone	DNS Server	
(*) All	→ 1.1.1.1:853	ର୍ଦ୍ଧ



Update the DNS Cache service Software

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

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

Versions

System version and softwares versions

Artica Core server	Operating system	Python packages			
1				DNS cache	* -
Software Ve	rsion				
DNS Cache service: 1.8	.3		🛃 Install or update		

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





Monitoring

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

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

ElbreNMS # Overview E Devices & Services	🗞 Ports 😻 Health 📰 Apps 🕕 Alerts
192.168.1.56 Artica tech	
Overview 🕍 Graphs 😻 Health 🖓 Oppo 🔍 Doctor	ventory 🗞 Services 📕 Logs 🕕 Alerts 🕍 Alert Stats 🛃
Device Settings SNMP Port Settings Applications A ert Set	ttings Alert Rules Modules Services IPMI Storage Proce:
OFF Apache	OFF Asterisk
OFF Ceph	OFF DHCP Stats
OFF Random entropy	OFF EXIM Stats
FreeBSD NFS Client	FreeBSD NFS Server
OFF Freeswitch	GPSD
OFF Mdadm	OFF Memcached
OFF NFS Server	OFF NFS Stats
OFF Nginx	OFF NTP Client
OFF Nvidia	Open Grid Scheduler
OFF PHP-FPM	OFF pi-hole
OFF Postfix	OFF Postgres
OFF PowerDNS Recursor	OFF PowerDNS
OFF Rrdcached	OFF SDFS info
OFF SMART	ON Squid
ON Unbound	OFF UPS apcups
OFF ZFS	

PowerDNS

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

Installing the PowerDNS system.

To understand, the PowerDNS system use 3 components:

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

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

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

Enable the RESTful API.

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

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

After installing, you should open the page

https://192.168.1.1:9000/pdnsapi/

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

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

Se PowerDNS system				
🕰 Status	Service status	Backup Cluster		
	Parameters			
CONS Servers				
⊕ Forward zones		Listen Network Interfaces:	lo,eth0	choose
📥 Local domains				
i≡ DNS records		Log Level:	9	Ŧ
🖵 Hosts file		Log queries:	ON	
G My computers		API Key:	changeme	
@ Events		Include comp uters database.		
🖿 Statistics		Act has Master:	OFF	
Logs center		Act has slave:	OFF	
	Domain Name S	vstem Security Extensions (DNSSEC)-	OFF	

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

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

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

Reverse DNS

Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com



Creating a reverse DNS domain

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

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

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

- ✓ **10.in-addr.arpa** for 10.0.0/8
- ✓ **16.172.in-addr.arpa** for 172.16.0.0/12

A Manuarte C MIC

✓ 168.192.in-addr.arpa for 192.168.0.0/16

Active Directory	+ New domain E Reconfigure service / Repair domains	
SGreenSQL Firewall	New domain	×
Se PowerDNS system		
Status	New domain	
 ✓ Service Parameters ♦ DNS Servers ♦ Forward zon 	Domain: 0.168.192.in-addr.arpa	
← Local domains	« add »	
L Hosts file		
My computers		
(Th Events	22 damadahrasil sam hr	

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 Artica V4 Documentation - david@articatech.com

After found the record, click on the link

DN	NS records					
0.168	.192* and type soa					Go!
+ Nev	w record 🕞 Reconfigu	ire service				
			/		Search	۹ +
ID	Record	Domains	Туре	Content		Delete
<u>1020</u>	0.168.192.in-addr.arpa	0.168.192.in-addr.arpa	<u>SOA</u>	ns.0.168.192.in-addr.arpa hostmaster.0.168.192.in-addr.arpa 2018113014	.0800 1800 60480	0

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: 10200.168.192.in-ad	Ir.arpa >> Type:SOA (0.168.192.in-addr.arpa)	
Start of Authority Record »»0.16	3.192.in-addr.arpa	
A Start of Authority record (abbrevia (DNS) containing administrative info	ted as SOA record) is a type of resource record in the Domain Name System mation about the zone, especially regarding zone transfers.	
zone:	0.168.192.in-addr.arpa]
MNAME:	ns1.touzeau.biz	
RNAME:	hostmaster.touzeau.biz	
<u>Serial:</u>	- 2018113014 +	
Refresh:	- 10800 +	
Retry:	- 1800 +	

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

ew record		
New record		
Insert a new entry in your PDNS DN	S server in order to resolve it	
Domain:	0.168.192.in-addr.arpa	Ŧ
Type (IN):	NS	¥
		« add »
		« add »
	•	

Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com



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

R »»0.168.192.in-addr.arpa		
hostname:	ns1.touzeau.biz	
IP Address:	192.168.0.151	\$
PRIO:	- 1	+
TTL (Seconds):	- 3600	+

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	1	
Insert a new entry in your PDNS DI	NS server it order to resolve it	
Domain:	0.168.192.in-addr.arpa	Ŧ
Type (IN):	PTR	Y
	- 1	

- \checkmark 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.

hostnamor	nc2 touzoau biz	
nostranie.	100.4 (0.0.4	*
IP Address:	192.168.0.1	Ŷ
PRIO:	- 1	+
TTL (Seconds):	- 3600	+

9%



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.



- \checkmark On the hostname set the IP address of your created item.
- ✓ Turn on the Reverse Lookup switch.

Click on the "DNS Simulation" item.

- ✓ On the DNS server, set the IP address of your Artica server.
- ✓ Click on the Run icon.

Down to "Tools"

~

~

DN	IS Simulation			×
				You should see the correct PTR entry in the DNS re
	Verify the DNS service reso	olution		
	hostname:	192.168.1.1	±	
	Reverse lookup:			
	Network Interface:	None	T	
	DNS server:	192.168.1.151	\$	
	TimeOut (Seconds):	- 3	+	
			; <<>> DiG 9:10.3-P4-Debian <<>> x 192.1 ;; global options: +cmd ;; Got answer: ;; >>HEADER<< opcode: QUERY, status: N ;; flags: gr aa rd; QUERY. 1, ANSWER: 1, AU ;; WARNING: recursion requested but not a ;; OPT PSEUDOSECTION: ;: EDNS: version: 0, flags;; udp: 1680 ;; QUESTION SECTION: ;1.1.168.192.in-addr.arpa. 1N PTR ;; ANSWER SECTION: 1.1.168.192.in-addr.arpa. 3600 IN PTR rout ;; QUERYUR: 192.168.1151#53(192.168.115 ;; WHEN: Sat Dec 01 19:56:11 CET 2018 ;; MSG SIZE rcvd: 85	92.168.1.1 +time=3 +tries=1 @192.168.1.151 -b 192.168.1.151 -4 us: NOERROR, id: 25138 L, AUTHORITY: 0, ADDITIONAL: 1 not available router touzeau biz. 3.1.151) 18



Update the PowerDNS core software.

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

On the search field, type "PowerDNS"

Under the **PowerDNS system** row, click on **Install or update** button.

≓ Your system	Versions
🚍 Your hard disks	System version and softwares versions
📾 Memory swapping	
System events	
₩ Features	Artica Core server Operating system Python packages
>_ OpenSSH server	PowerDNS 🗶 🗸
Glances	Software Version
O Tasks	
# Certificates Center	PowerDINS system: 4.1.5
Backup	PowerDNS recursor: 4.1.8
P License	
Opdate	
🗖 Web Console	
iVersions	

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

PowerDNS s	system	×
PowerDNS sys	stem 4.1.6 11.7 MB	📩 Install or Upgrade
PowerDNS sys	stem 4.1.3 11.48 MB	Linstall or Upgrade
PowerDNS sys	stem 4.1.1 11.37 MB	🛓 Install or Upgrade



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.



Inst	tall or uninsta	II features		
This sect	tion allows you to install/uninst	all available features on your server		
select -	Expand			
			DNICCOURT	
			LUNSI EVEN	
		-	Ditscrypt	
Status	Software]	Ditociypt	Action

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 serve**rs 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	E Search a comp	iter, a membei		() 00:27:49	Cpu:8.7% Mem:29.5%	^悠 Members	🔋 🛈 Lo	gout ∛≣
Administrator -								
## Dashboard	DNS Serv	vers						
🚍 Your system	This section list DNS	servers used by the system.						
🚓 Network & NICs	-							
S DNS	DNS Servers	Public DNS servers DNS be	nchmark					
🛢 DNS Cache service	Reconfigure servi	ce						
🗘 DNS Servers						Search		Q 🚽
Forward zones	Enable Name		Description					
🖵 Hosts file 🖵 My computers	Adguard	DNS Family Protection 1	(Anycast) Adguard DNS with safesearch 176.103.130.132:5443	h and adult content b	ocking			
DHCP/TFTP	Adguard	DNS Family Protection 2	(Anycast) Adguard DNS with safesearch 176.103.130.134:5443	h and adult content b	ocking			
🖮 Statistics	Adguard	DNS 1	(Anycast) Remove ads and protect your 176.103.130.130:5443	computer from malw	are			
🖹 Logs center	Adguard	DNS 2	(Anycast) Remove ads and protect your 176.103.130.131:5443	computer from malw	are			
🛢 Databases	BikinHa	ppy Singapore	(Singapore) provided by bikinhappy.com 172.104.46.253:443	n				
	Babylon	Network France 0	(Roubaix, France) Non-logging, uncenso 5.135.66.222:5353	ored DNS resolver pro	ovided by Babylon Network			

Update the list

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



DN:	S Servers	
1115 500	In this bird servers used by the syste	
DNS	Public DNS servers	DNS benchmark
🗩 Disab	le all 📕 Undate 📕 Ontions	D D D D D D D D D D D D D D D D D D D
		Reconfigure service
L		Keconngure service
Enable	Name	Description
Enable	Name	Reconfigure service Description DNS-over-HTTPS server running rust-doh with PiHole for Adbloc has larging to favoring suprame DMSECC.
Enable	Name aafialo-me	Description DNS-over-HTTPS server running rust-doh with PiHole for Adblor Non-logging. AD-filtering: supports DNSSEC. Hosted in Netherlands on a RamMode VPS.
Enable	Name aafialo-me	Description DNS-over-HTTPS server running rust-doh with PIHole for Adblor Non-logging, AD-filtering, supports DNSSEC. Hosted in Netherlands on a RamMode VPS, dns.aaflalo.me.443,176.56.236.175.443
Enable	Name aafialo-me	Description DNS-over-HTTPS server running rust-doh with PiHole for Adolo Non-logging AD-filtering supports DNSSEC. Hosted in Netherlands on a RamNode VPS. dns aaflalo.me:443,176.56.236.175.443 DNS-over-HTTPS proxy of aaflalo-me hosted in Google Cloud PiL
Enable	Name aafialo-me aafialo-me-gcp	Configure service Description DNS-over-HTTPS server running rust-doh with PiHole for Adbio Non-logging AD-fittering supports DNSSEC. Hosted in Netherlands on a RamNode VPS. dms.aaflalo.me.443,176.56.236,175.443 DNS-over-HTTPS provy of aaflalo-me hosted in Google Cloud Pla Non-logging AD-filtering supports DNSSEC. dms-gcp.aaflalo.me.443,35.231,69.77.443
Enable	Name aaflalo-me aaflalo-me-gcp	Recomputerservice Description DNS-over-HTTPS server running rust-doh with PiHole for Adbla Non-logging AD-filtering supports DNSSEC. Hosted in Netherlands on a RamNode VPS. dms.affalo.me.443,376.562.36.175.443 DNS-over-HTTPS proxy of aaffalo-me hosted in Google Cloud Pi Non-logging AD-filtering supports DNSSEC. dms-gep.aaffalo.me.443,35.231.69.77.443 Remove ads and protect your computer from malware

Unique Provider

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

Manager Administrator -	Search a computer, a member	
₩ Dashboard ■ Your system	DNS Servers This section list DNS servers used by the system.	
A Network & NICs	DNS Servers Publi DNS servers DNS benchmar	k
DNS Cache service Construction of the service	Disable all / Options R aconfigure service	
	Enable Name D	Description

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

Options	×
Options	
Unique provider	
By default, the DNSCrypt client use a DNS provider random If you want to use only one provider, enable this feature of a seclect the desired provider	
Unique provider:	
providers: SecureDNS	v
Apply	x



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"

Versions System version and softwa	res versions				
Artica Core server	Operatingsyster	m Python packages		dns	* -
Software	Version				
DNS daemon for DNSBLs:	- 2	Install or update			
DNSCrypt Proxy:	2.0.18	Install or update	DNSCIPPTION		
DNS Cache service:	1.7.3 🛃	Install or update	e DNSCrypt Proxy 2.0.18	8.2 MB	+ Install or Ungrade
DNS Stats Collector:	2.6.1	Install or update	5.13Cl ypt 10xy 2.0.10	0.2110	
PowerDNS system:	4.1.3	Install or update			
PowerDNS recursor:	4.1.3	Install or update	VEISION		

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

Install the service

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

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

Create the HTTPs service

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

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

Dashboard	Web	sites					
E Your system	_						
🚓 Network	+ New serv	ice 🖬 Reconfigure	service				
S DNS	L 4	•				Search	Q +
DHCP/TFTP	Status	Saved On	Service	Server Names	Туре	Destination	
• Web services				No results	5		
🕢 Status							
All websites							
Requests							

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

New service



Select your new web service in the table.

Web sites

+ New service Reconfigure service Status Saved On Service Server Names Not configured My DOH service General settings Server name Ports Access rules My DOH service DNS Over HTTPs web service Create a DNS Over HTTPs servic e HTTPs DNS forwarder to take care of the HTTPS part of DNS-over-HTTPS. (7) ± Service name: My DOH service SSL parameters Certificate: doh.touzeau.biz TLSv1 TLSv1.1 TLSv1.2 SSL protocols: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256: Cinher suites Prefer server Ciphers: OFF - 16 ÷ SSL Buffer size (k): « Apply »

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

Artica can be updated itself.

Update configuration can be managed in the left menu $\ensuremath{\textbf{Your System}}$ / $\ensuremath{\textbf{Update}}$

Artica V4 Documentation - david@articatech.com



OFFICIAL RELEASES

By default Artica is configured to only update official releases. Official release are an even number in minor version. So 4.26,4.28,4.30,4.32,4.34,4.36 are official releases.

The automatic update can be controlled by the "Update Official Releases" checkbox.

SERVICES PACK

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

NIGHTLY BUILDS

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

UPDATE IN PRODUCTION

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

MANUAL UPDATE.

Manual update accept any artica-4.xx.xxxxx.tgz for full version or ArticaPx.tgz for Services Packs. With the button Manual update, you can download Artica packages here http://articatech.net/firmwares.php And upload them to the system.

The manual update button allows you to return back to any version available in the Firmware's table.



THE CERTIFICATES CENTERUPGRADING ARTICA

Artica can be updated itself.

Update configuration can be managed in the left menu Your System /Update

Administrator 👻	Cpu:4.9% Mem:53.9%/3.83 GB	≁ Active Requests	E Categorize Admin Guide 💡 🕛 Log out
III Dashboard L IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Update Artica		
System information	Get your Artica system updated and install new Artica services on your system	stem	
Your system memory Memory swapping	Artica history Operating system		
Watchdog System events	Current: 4.29.052614 Service Pack 4	Settings	
↓ reatures >_ OpenSSH server ■ Classes	official: <u>4.28.030418</u>	Update Official Releases: {Update_services_packs}:	он П
 Grances Tasks Contributions Contour 	Nightly: <u>4.29.052614</u> Service Pack 4	Update Nightly Releases: Perform Update (Even In Production Period):	OFF OFF
Backup	2 Manual update	Remote synchronization (Rsync)	
Update		Activate The Remote Synchronization:	OFF
Web Console Versions		Remote Server:	Remote server
⊕ Internet access र्के Support		Kemote Server Port:	0/3

OFFICIAL RELEASES

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

SERVICES PACK

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

NIGHTLY BUILDS

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

UPDATE IN PRODUCTION

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

MANUAL UPDATE.

Manual update accept any artica-4.xx.xxxxx.tgz for full version or ArticaPx.tgz for Services Packs. With the button Manual update, you can download Artica packages here http://articatech.net/firmwares.php And upload them to the system.

The manual update button allows you to return back to any version available in the Firmware's table.

The Certificates Center.



ly DOH service		×
General settings Server names	Ports Access rules	
Server names	1	
Server names determine which server bloc They may be defined using exact names, wi Examples: example.org "example.org mail" 192.168.1.1 ~^(?.+).example.net\$ When searching for a virtual server by nam and regular expression match, the first mate exact name longest wildcard name starting with an ast longest wildcard name ending with an ast first matching regular expression (in order	ik is used for a given request. Ildcard names, or regular expressions. ne, if name matches more than one of the specified variants, e.g. both wildcard name tching variant will be chosen, in the following order of precedence: erisk, e.g. "example.org risk, e.g. mail." of appearance)	
Items:	1 doh.touzeau.biz 2 dns.touzeau.big	
	« Apply »	
DOH service	×	- O LOS O

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

My DOH serv				×	
General sett	ings Server name Ports Ad	ccess rules		_	
			Search Q -		
Intertices	Listen Ports		Delete	1	٩
	No	results			
	New entry				
	New item				
	Listen interface:	All interfaces		٣	
Copyright Artic	listen port:	- 443		+	
	Options				
	Use the SSL encryption: HTTP/2: SPDY: PROXY Protocol:	ON OFF OFF OFF			
My DOH se	ervice			a add a	×
Generals	ettings Server names Ports	Access rules	DNS-over-HTTPS server		
MyDOH	SETVICE (DNS Over HTTPs web service)				
Create a Turn a w	a DNS Over HTTPs service vebsite to a reverse HTTPs DNS forwarder to	o take care of the HTTPS p	art of DNS-over-HTTPS. (7)		
HTTP pa	ath for resolve application: dns-quer	у			
			1	« Apply »	

Select the DNS over HTTPs server tab.

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



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

Image: New service Reconfigure service Status Saved On Service Server Names Type Destination Not configured - My DOH service Certificate: doh. touzeau.biz: 443 Subfolder:/dns.rouzeau.biz: 443 Subfolder:/dns.rouzeau.biz: 443 Subfolder:/dns.rouzeau.biz: 443 DNS Over HTTPs web service Local DNS service Image: Certificate: doh. touzeau.biz: 443 Subfolder:/dns.rouzeau.biz: 443	Web si	ites				
Status Saved On Service Server Names Type Destination Not configured - My DOH service Certificate: doh. touzeau.biz: 443 Subfolder:/dns. rouzeau.biz: 443 Subfolder:/dns. rouzeau.biz: 443 DNS Over HTTPs web service Local DNS service Image: Control of the con	+ New service	Reconfi	gure service			Search Q -
Not configured My DOH service Certificate:doh.touzeau.biz https://doh.touzeau.biz:443 https://dns.touzeau.biz:443 Subfolder:/dns-query DNS Over HTTPs web service Local DNS service Image: Control of the service	Status	Saved On	Service	Server Names	Туре	Destination
	Not configured	-	My DOH service Certificate:doh.touzeau.biz	https://doh.touzeau.biz:443 https://dns.touzeau.biz:443 Subfolder:/dns-query	DNS Over HTTPs web service	Local DNS service 🔽 🔄 🗊

esti	ng your DOH server resolution	Mem:30.2%	200	Members 📮 🛈 Log out	Æ
•	On the top menu, click on the top-right icon in order to open the right pan.			Action	
•	Down to the " DNS Simulation " link			Help & Support	
				Video tutorials	Go
			S	🟦 Create a ticket	60
		De	stina	Support package	60
		eb service Lo	cal D	System	
				>_ System console	
•	Choose the "DNS over HTTPS server" tab			Syslog	0

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

DN	IS Simulation	×	n:30.7% /æ	Members 🐥 🖰 Log out 😤
	*			Action
	DNS Simulation DNS-over-HTTPS se	ver		Help & Support
	Verify the DNS service resolution			🖬 Video tutorials
	hostname: www.go	ogle.fr	d	🕱 Create a ticket
	DNS Over HTTPS server URL: https://	loh.touzeau.biz/dns-query		Support package
				System
		« Run »		😂 Services status 🛛 🕞
				> Svstem console
	DNS Simulation Results			×
DNS red	www.google.fr from https://doh. TTL: 3600 seconds A: 216.239.38.120	ouzeau biz/dns-query		



DNS AMPLIFICATION DOS ATTACKS PREVENTION

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

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

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

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

👬 Network	Firewall parameters
(≜) Your Firewall	
🗘 Parameters	Global rules
i E Rules	
≈ Routers	DNS Amplification DDOS protection:
→ N.A.T	Logs storage
Firewall services	
≣ Configuration file	Log all events: OFF
𝑁 Events	Backup Firewall events:

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

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

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



THE DNS LOAD-BALANCING SERVICE

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

Install the service

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

Insta	ll or uninstall features		
This section	n allows you to install/uninstall available features on	/our server	
	De la due a		
select -	Expand A Wizards		
		DNS Load	× -
Status	Software		, in
Uninstalled	DNS Load-balancing service		V Install

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

Nanager Administrator →	■ Search a computer, a member → Active Requests @ Requests	③ 12:30:07	% 원 Members 🖹 Admin Guide	🧧 () Log out 泪
E Dashboard				
■Your system	DNS Load-balancing ser	vice v1.4.0		
🚓 Network	This service allows you to transform your Artica server a	as a DNS proxy with caching, load-balancing,	DNS over TLS, DNS over HTTPs capabilitie	es.
SDNS				
DNS Load-balancing service	Status Network Access Restrictions			
▼ SafeSearch(s)		DNS Load-balancing service	1	
¢¢ DNS Servers		Method	lowest connections	*
Forward zones	DNS Load-balancing service	Method.	ionest connections	
Thosts file	Running	Listen Network Interfaces:		choose
G My computers	since 10h 26mn 58s	Listen only the loopback interface:	OFF	
# Your proxy	Memory used: 64.71 MB	Outgoing Interface:	All interfaces	
🕅 Web-Filtering	C Restart	Events		
Databases		Log queries:	OFF	
Logs center		Cache		
		Cache size (MB):	- 100	+
		Cache TTL (Min):	1 hour	¥.
		Cache TTL (Max):	2 Days	Ψ.

F

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

E Tour system Network	DNS Servers This section list DNS servers use	d by the system.	
DNS Load-balancing service			
▼ SafeSearch(s)	DNS Servers DNS ben	chmark	
😂 DNS Servers	DNS used by the system		
♦ Forward zones	Divis used by the system		
🖵 Hosts file	Local DNS service:	127.0.0.1	
G My computers	Primary DNS server :	8.8.8.8	÷ 🕈
# Your proxy	Secondary DNS server :	1.1.1.1	\$
₩Web-Filtering	DNS Server 3 :	2.2.2.2	\$
S Databases	Internal domain 1::	touzeau.biz	



ACLs For DNS Load-balancer service.

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

∷ Dashboard ■ Your system	DNS Load-ba	alancing service » DNS ACLs					
🚓 Network	+ New Rule Apply rul	es CReload					
€ DNS			Search			۹	*
DNS Cache service	Rule Name	Description		Enabled			
i≡ Rules	Spoofing	For objects «MonIP» (1 Items) then Forge a A response 192.168.1.1		~	1	¥	0
✿ DNS Servers 및 Hosts file	Active directory 1	For objects « <u>domaine AD1</u> » (1 Items) then Balance DNS requests to DNS Servers <u>Activ</u> <u>Directory 1</u>	<u>/e</u>	~	↑	¥	0
C My computers	reply 192.168.1.1 for *	For objects « <u>Everyone</u> » then [SpoofCNAMEAction] 192.168.1.1		~	•	¥	0
🗟 Fail To Ban	Interdit pc-3.touzeau.maison	For objects $\ast \underline{MonIP} \ast (\texttt{1 tems})$ then Refuse to resolve or forward request		~	↑	¥	0
Se Databases	Default	For IP addresses 192.168.0.0/16 Or 10.0.0.0/16 Or 172.16.0.0/12 and All domains the DNS requests to To addresses 192.168.1.118 Or 192.168.1.114	ien <mark>Balanc</mark> e	-	-		-
🖺 Logs center							

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

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

A Rule can have one of these behavior :

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



THE HTTP/HTTPS PROXY

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

INSTALL THE PROXY SERVICE

Install the single service.

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

On the left menu, Select "Your system" and "features"

The proxy service can be enabled in under the "Proxy features/ Proxy service." Click on install button in order to install the HTTP proxy service.

Proxy features		
Uninstalled Proxy service	Proxy service:Enable the feature: 50% Reconfigure the proxy service Proxy service:Enable the	✓ Install

Use the wizards section

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

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

Install or uninstall features This section allows you to install/uninstall available features on your server select 🗸 **A** Wizards

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

. ...

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

elect • Expand AWizards	
Full Web-application FireWall Proxy, Web-Filtering, Error page, advanced rules Install a standard proxy for security and releging user's access with a proxy pac service, change your brows ettings in order to use this configurate units: http://1921.06.1177/proxy pac. You will be proxified and filtered winst porn, malwares, advertising and trackers sites.	rser



THE PROXY LISTEN PORTS SECTION.

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

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

The Connected ports

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

BB Dashboard	Listen p	orts						
E Your system	This section allow The frist one Con	rs you to define how browsers can be connected to your nected ports list ports used directly in browsers setting	proxy. s.					
A Network	Connected ports The second one Tr Important: Transi	are able to authenticate users through LDAP or Active E ransparent ports allow the proxy to act as the main gate parent ports cannot authenticate users	Directory. way and is able to catch	h both HTTP/H	TTPS requests	without need t	o change browse	ers settings.
S DNS								
(≜) Your Firewall	Connected port	ts Transparent ports Communication p	ports					
# Your proxy	+ New port	Apply configuration						
🖓 Status						Search		Q -
😂 Global settings								
₩ ICAP Center	TCP Address	Listen Port	HTTPS	Cache	AUTH.	Filter	Enabled	Delete
at Authentication	127.0.0.1	56633 Internal Port (Only available for Artica)					~	
Errors pages	192.168.1.140	3128 Main port: Main connected port 0.0.0.3128		~	~	~	~	0
Proxy events								
€ Listen ports								
SSL Protocol								

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

- Listen port: A numeric value that defines the port to listen.
- Service Name: A description of your port that will be displayed in others sections.
- **Description:** Description used only in the ports table.
- Accept Proxy protocol: used only with the loadbalancer service.
- **Disable Authentication**: if checked, this port will not ask any authentication.
- **Disable caching:** if checked, Internet objects fetched from this port will not be cached.
- Disable web filtering: If checked, the proxy will not query the Web-filtering engine if using this port.

Enabled:	ON	
listen port:	- 3128	+
Service name:	Main port: Main connected port 0.0.0.3128	
Description:	Description	
Accept proxy protocol:	OFF	
Disable authentication:	OFF	
Disable caching:	OFF	
Disable Web-Filtering:	OFF	
Listen interface:	eth0 192.168.1.140 - Interface eth0	٣
Forward Interface:	All	٣
Use the SSL encryption:	OFF	
	Marca	

- Listen Interface: Which interface to bind in order to listen to client requests
- Forward Interface: Which interface to bind in order to fetch internet objects
- Use SSL encryption: If checked, the proxy will decrypt SSL protocol using SSL rules and with the associated certificate defined in "Use a certificate from certificate center"



The transparent ports

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

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



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



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



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

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

Listen	ports									
This section allo The frist one Co Connected port The second one Important: Trar	ows you to define ho onnected ports list p is are able to authen Transparent ports a nsparent ports cann	w browsers can be orts used directly ticate users throug allow the proxy to ot authenticate us	e connected to your proxy. in browsers settings. gh LDAP or Active Directo act as the main gateway ar sers.	ry. nd is able to catch b	ooth HTTP/HTT	"PS requests wi	thout need to	o change brov	wsers settings	
Connected po	orts Transpa	erent ports	Communication ports							
+ New port	Apply configur	ation								
									Search	
TCP Address	Inbound Port	Proxy Port	Outgoing Address	Port Name	WL SRC	WL DST	HTTPS	Cache	Filter	Enable
	80	64359	192 168 1 143	80 Transparent	0 Items	3 Items			~	~
192.168.1.140	80	04330	172.100.1.110	HTTP	ortems	ortenis		~		

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

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

Destination port:	- 80	+
Proxy port:	- 14470	+
Use Tproxy mode:	OFF	
Service name:	HTTP Interception	
Disable caching:	OFF	
Disable Web-Filtering:	OFF	
Listen interface:	All interfaces	Ŧ
Forward Interface:	All interfaces	٣
Use a certificate from certificate center:	None	*

• Use a certificate from certificate center: If set, the proxy will decrypt SSL protocol using SSL rules



Network exclusions

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

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

Connected ports Transparent ports		arent ports	Communication ports						
+ New port	Apply configur	ation							
TCP Address	Inbound Port	Proxy Port	Outgoing Address	Port Name	WL SRC	WL DST	HTTPS		
92.168.1.140	80	64358	192.168.1.143	80 Transparent HTTP	0 Items	3 Items			
All interfaces	443	64359	All interfaces	443 Transparent SSL	0 Items	3 Items	~		

You can bypass the proxy service for specific destination networks or sources.

For example if you have some industrials equipments and you did not want to alter HTTP/SSL connections to the network destination:

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

Reconfiguring your firewall - 50% Resta	arting the Firewall service	
xclude destinations		
Give here (multiple entries separate	d by a carriage return) IP adresses eg 192.168.1.53 or subnet eg 1	92.168.1.0/24
Network	1 10.0.0.0/8 2 192.168.0.0/16 3 172.16.0.0/12 4 194.56.233.0/24	
	/	
	•	« Apply »



SSL Interception

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

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

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

Downoad the dedicated documentation here :

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



Remote ports

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

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

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

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

≡ You system	List	en ports					
👬 Network	This sec	n allows you to define how browsers can be connected t	o your proxy.				
S DNS	Connec	I ports are able to authenticate users through LDAP or A d one Transparent ports allow the proxy to act as the ma Transparent ports allow the proxy to act as the ma	ectings. ctive Directory. in gateway and is able to catch both HTTP/HTTPS requ	ests without I	need to cha	ange browsers s	settings.
# Your proxy		. Transparent ports cannot autrenticate users.					
🙆 Status	Conn	ed ports Transfert ports Remote po	rts Communication ports				
¢ ^o Global settings							
₩ICAP Center	+ New	rt Disable the feature Apply configuration	on				
Authentication							
🖹 Errors pages	Access Only li	outgoing ports are restricted. d ports will be allowed by the proxy.					
Proxy events						_	_
🗲 Listen ports				Search	1		Q +
SSL Protocol	Ports	Note		нттр	SSL	Enabled	Del
■ Global rules O Proxy tasks	20	ftp-data RFC		~		~	0
	21	ftp RFC		~		~	0
ACLs Proxy	443	HTTPS REC.			~	~	0
𝔅 Web-Filtering	110	2.2.2.2.2.2.2.2.2.2.2.2.				-	
Vour categories	80	HTTP RFC		~		~	0
w rour carcegories					_		

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

Connected ports are a he second one Transp mportant: Transparer	ble to authenticate users thro parent ports allow the proxy t nt ports cannot authenticate	ugh LDAP or Active [o act as the main gate users.	Directory. way and is able to catch both H	ITTP/HTTPS request	s without need to change brow	vsers setting
Connected ports	Transparent ports	Remote ports	Communication ports			
Enable the feature	Apply configuration					
This feature is disable	d					
Access to outgoing po Only listed ports will I	orts are restricted. be allowed by the proxy.					
					Search	Q
	Note	нттр	SSL	Enabled	Del	


Troubleshooting

How to test if you are using the proxy?

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



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





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



Click on the button "**Build Now**"

Bı	uild a "support" package	×
	The support package is a compressed file that stores of necessaries informations if order to understand your server environment. Basically it helps our support team to resolve an issue.	
	Build Now	

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





Listen ports freeze after rebooting

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

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

Listen ports This section allows you to define how browsers can be connected to your proxy. The frist one Connected ports list ports used directly in browsers settings. Connected ports are able to authenticate users through LDAP or Active Directory. The second one Transparent ports allow the proxy to act as the main gateway and is able to catch both HTTP/H Important: Transparent ports cannot authenticate users.				ter a reboot of ncluding Prox	n KVM hyperv mox, Nutanix.	isor)
Connected ports Transparent ports	Remote ports Communica	ntion ports				
Status	Status TCP Address	Remote Port	Proxy Port	Outgoing Address	Port N ne	WL SRC
Linked	Failed All interfaces	443	33047	All interfaces	443 Prox, SSL Connection refused	0 Items

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

👬 Network	Listen ports
⊜DNS ⊕ Your proxy	This section allows you to define how browsers can be connected to your proxy. The frist one Connected ports list ports used directly in browsers settings. Connected ports are able to authenticate users through LDAP or Active Directory.
🔁 Status	The second one Transparent ports allow the proxy to act as the main gateway and is able to catch orth HTTP/HTTPS requests without need to change browsers settings. Important: Transparent ports cannot authenticate users.
😂 Global settings	
₩ ICAP Center	
Authentication	Connected ports Transparent ports Remote ports Communication ports Troubleshooting
Errors pages	After rebooting
Proxy events	
🖋 Listen ports	Reconfigure Ports And Restart Service:
SSL Protocol	
Global rules	r Apply »
Proxy tasks	« крру »
Databases	

Check the option "Reconfigure Ports and Restart service".

Enable this option reconfigure ports and restart the proxy service just after the boot sequence on order to avoid the freeze behavior.

њN

⊕ Your

•

ACLs P

SDat

Proxy service monitoring

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

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

Monitoring the CPU usage

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

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

Monitoring the legal log.

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

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

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

k	Your proxy v4.10
xy	Statur Watchdog Requests Traffic Caches Objects
bal settings	
Center	If turned to mean Artise will be able to meniter news require and react sutematically an detected travibler
hentication	according configuration.
rs pages	
ky events	Enable: ON
en ports	Restart service
Browsing	
Protocol	If System CPU Exceed: 95% *
al rules	
ry tasks	Logrotate
ху	Only Executed By Schedule:
tering	Export Log If Stze Exceed (MB): - 100 +
vices	
15	« Apply »
er	

WCCP

About WCCPv2 support

Web Cache Communication Protocol (WCCP) is a technology developed by Cisco that allows transparent re-direction of network traffic in realtime.

This re-direction can be to a cache engine or to a proxy, such as Artica Proxy.

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

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

Cisco says: WCCP enables supported Cisco routers and switches to transparently redirect content requests.

With transparent redirection, users do not have to configure their browsers to use a web proxy.

Instead, they can use the target URL to request content, and their requests are automatically redirected to an application engine. The word transparent means that the end user does not know that a requested file (such as a web page) came from the application engine instead of from the originally specified server.

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

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







Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com

Page: 148



NOTRACK

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

NoTrack prevent your computers from connecting to specific hosts.

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

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

Date	members		Piotocol	Category	url	INFO/LINK	Destinations	Size	duration
12:51:07	10.3.130.47 mac: c4:9d:ed:ea:57:a:	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com	Q 2	local	7.56 KB	Os
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com	Q 🛛	local	7.58 KB	Os
12:50:59	10.3.130.47 mac: <u>c4:9d:ed:ea:57:ac</u>	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com	Q 🛛	local	7.58 KB	Os
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com	Q 🛛	local	7.58 KB	Os
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com	Q 🛛	local	7.58 KB	Os
12:50:59	10.3.130.47 mac: c4:9d:ed:ea:57:ac	NoTrack - Forbidden	SSL	Advertising	https://fra1-ib.adnxs.com	Q 🖻	local	7.58 KB	Os
	10.2.120.47								

URLHAUS

URLhaus is a project operated by abuse.ch.

The purpose of the project is to collect, track and share malware URLs, helping network administrators and security analysts to protect their network and customers from cyber threats.

This option should consume CPU, be sure using a Core i7 or higher.

This option is disabled by default.

WEB SITE-BLOCKING

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

GOOGLE SAFE BROWSING

What is Safe Browsing?

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

With Safe Browsing you can:

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

The Google Chrome, Safari, Firefox, Vivaldi, and GNOME Web browsers use the lists from the Google Safe Browsing service for checking pages against potential threats

Currently, Opera, Internet Explorer, Microsoft Edge are not able to query the Google Safe Browsing reputation server.

You can test the Google Safe Browsing database here:

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

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

Benefits on Artica proxy

Visibility

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

Protect any non-compatible browsers

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

Potential privacy

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

Download the documentation

Documentation of Google Safe Browsing feature can be downloaded here:

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



(F)

AUTHENTICATE MEMBERS

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

LDAP Authentication

Artica supports LDAP v3.

An LDAP directory consists of a simple tree hierarchy.

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

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

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

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

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

Use the Artica LDAP service.

The Artica LDAP service is an OpenLDAP server using for several services such has the proxy but also for the messaging service or the file-sharing service. Artica offers groups and members administration like a full user's management system.

Ensure the Local LDAP service is installed

On the "Features"

Manager Administrator -	Search a computer, a member	Requests	(3 08:43:59	Cpu:5.4% Mem:30.1%	^{ee} Members	2	①Log out	33+
## Dashboard	Your proxy »» Authentication	on						
E Your system	This section allows you how to identify clients through the proxy							
A Network & NICs								
S DNS	use local LDAP database	1						
⊕ Your proxy								
🚯 Status	Authenticate users through the local database:]						
😂 Global Settings	Banner: Please	logon in order to acc	cess trough Inter	net				
Authentication								
Troxy events						«A	pply »	
✓ Listen ports								
Giobarrules								_

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



Chrome authentication box (no banner displayed)

The proxy ht	ttp://192.168.1.71:3128 requires a username and password.
our connec	tion to this site is not private
Jsername	david.touzeau
assword	

Edge authentication box (banned is displayed)

Sécurité Windows	Sécurité Windows					
Microsoft Edge						
Le serveur 192.168.1.71 requier mot de passe. Le domaine du s order to access trough Internet	rt un nom d'utilisateur et un serveur est 'Please logon in t'.					
Nom d'utilisateur						
Mot de passe	Mot de passe					
Mémoriser mes informatio d'identification	ns					
ОК	Annuler					

FireFox authentication box (banner is displayed)

Authentification	requise	×
W tilisateur : Mot de passe :	Le proxy moz-proxy://192.168.1.71:3128 demande un nom d'utilisateur et un mot de passe. Le site indique : « Please logon in order to access trough Internet »	
	OK Annuler	

Use a Remote LDAP Database

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

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

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





You can use the tool <u>LdapAdmin</u> 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: Users LDAP Filter: User attribute: Search members in groups: Attribute: Groups search filter:	uid=root,dc=company,dc=com (&(objectclass=person)(uid=%s)) uid (&(memberUid=%u)(member=*)) member (&(objectclass=posixGroup)(cn=%s))
Group attribute.	

Example: Like Active Directory

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

Verify your LDAP patterns

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

Page: 153



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

Ν	ly members				
Sea	arch				Go!
				Search	۹ -
	Display Name	EMail Address	Office Phone	Groups	
<u>0</u> %	users Directory default group	-	-	-	
300	Directory Operators Directory default admin group	-	-	-	
°6°	Directory Clients Directory default client group	-	-	-	
\$ <u>6</u>	Directory Consumers Directory default consumer group	-	-	-	
300	administrators System default admin group	-	-	-	
*	admin	=	-	Directory Operators administrators	
*	dtouzeau	david@toto.com	0620567433	<u>users</u> Internet access	
給	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

🚓 Network & NICs			
S DNS	use local LDAP database {KADIUSAuthentication}		
# Your proxy			
🖓 Status	Authenticate users with an external RADIUS server:		
😂 Global Settings	Banner:	Please logon in order to access trough Internet	1 1
Authentication	RADIUS server address:	192.168.1.3	
Proxy events	RADIUS server port:	- 1812	+
	RADIUS Identifier	proxy	
© Proxy tasks		ргоду	0
	shared RADIUS secret:	•••••	(a)
Vour categories		•••••	٩
🖿 Statistics			
🖺 Logs center			« Apply »
🛢 Databases			

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



Use Active Directory

Artica is compatible Active Directory on Microsoft Windows 2000,2003,2008,2012,2016,2019 (THIS FEATURE REQUIRE AN ENTERPRISE LICENSE). The main benefit using the Active Directory is the "silent authentication" means the browser automatically sends the Windows session credentials to the proxy using NTLM or Kerberos method.

In this case, the user did not have to put its credentials in a login box.

How to join Artica to your Active Directory server?

You need to follow these requirements:

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

Join the Microsoft domain.

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

Install or unir This section allows you to instal	Install features	
select - Expand		active 🗶 🗸
Status	Software	Action
Uninstalled	Active Directory	✓ Install



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

In this menu, you have 3 main sections:

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

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

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

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



Each section will ask to you required settings

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

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

Kerberos or NTLM?

There are differences between these 2 methods.

Kerberos native authentication method

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

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

NTLM standard method:

Is a very old method used to communicate in the Microsoft domain

It is compatible with all systems.

It is not compatible with Windows 2019 Active Directory and later It is less secure (password is in clear text when sniffing the network).

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

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



Use the Native Kerberos

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

₩ Dashboard ■ Your system	Active Directory »» Kerberos Authentication						
👬 Network	Join Active Directory domain / Kerberos Authentication						
Active Directory	Allow Active Directory users to logon;	ON					
🔁 Status	Active Directory full hostname:	dc16.touzeau.biz					
₩ Kerberos Authentication							
₩ Cluster mode	Computers AD location:	CN=Computers					
₩ Join the domain (NTLM)	Windows server type:	Windows 2016/2019					
	Administrator	administrateur@touzeau biz					
≣ White lists							
Events	Password:	•••••					
	Basic authentication for users outside the domain:	ON					
E DNS	Sync. time with the AD:	OFF					
() Your Firewall							

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

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

Active Directory »» Kerberos Authentication						
connecting: 100% msktutil Success «Details»						
		connecting - 100% msktutil Success				
Allow Active Directory users to logon:	Yes					
Active Directory full hostname:	dc16.touzeau.biz					
Computers AD location:	CN=Computers					
Active directory Suffix:	DC=touzeau,DC=biz					
Windows server type:	Windows 2016/2019					
Administrator:	administrateur@touzeau.biz					
Basic authentication for users outside the domain:	Yes					
Sync. time with the AD:	No					
		& Disconnect				

Dedicated administrator account

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



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

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

Create a dedicated user:

Create a new user **that never expires**.

Open users Properties/Account tab and set the "Do not require Kerberos preauthentication" checkbox.

Configure IP address and DNS settings

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

Synchronize time

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

On the left menu, choose "Kerberos Authentication"

Fill the form properly using this way:

Username and password

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

The Active Directory full hostname

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

FQDN of secondary DC

Fully qualified domain name of your second domain controller. For example, "dc2.company.corp".

This setting is optional and does not need to always be filled in.

If your first domain controller goes down for routine maintenance the application will use second domain controller for LDAP group lookup and authentication.

Kerberos realm

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

For example:

Manager Administrator -	E Search a computer, a member	-√- Active Requests	Requests	() 15:48:56	්සී Members	🖺 Admin Guide	Ş	() Log out	334
- Dashboard	Active Directory »» Ke	rberos Aut	hentica	tion					
Your system	The kerberos Authentication method allows you to lin This method is designed if you plan to use a load-balar	k your Artica proxy using	only the Kerberos	s method.					
击 Network	If you plan to use a single proxy server you can use the	{join_domain} feature usi	ng Kerberos optic	on.					
Active Directory									
🙆 Status	Join Active Directory domain Kerberos Autl	nentication							
₩ Kerberos Authentication	User name:	user@domain.tld						±	
븆 Join the domain									
	Kerberos Realm:	TOUZEAU.BIZ							
≣ White lists	Service Principal Name (SPN):	HTTP/newproxy.tou	zeau.biz@TOUZ	EAU.BIZ					
PowerDNS system									
。 曲 Your proxy							« A	pply »	

Submit the form.



Generate the Kerberos ticket on your Active Directory

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

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

Active Directory »» Ker	rberos Authentication	
The kerberos Authentication method allows you to link This method is designed if you plan to use a load-balan If you plan to use a single proxy server you can use the	cyour Artica proxy using only the Kerberos method. cing system with Artica in cluster mode. Join the domain feature using Kerberos option.	
Please go to your Active Directory, open an MS-DOS sess Retreive the krb5.keytab (default in Downloads directory	ion and copy/paste this command.) and upload it.	
ktpass -princ HTTP/newproxy.touzeau hmac-nt -pass ****** -ptype KRB5_N	u.biz@TOUZEAU.BIZ -mapuser articauser@touzeau.biz@TOUZEAU.BIZ -crypto rc4- T_PRINCIPAL -out %HOMEPATH%\Downloads\krb5.keytab	
Join Active Directory domain / Kerberos Aut	thentication	
User name:	articauser@touzeau.biz	
Kerberos Realm:	TOUZEAU.BIZ	
Service Principal Name (SPN):	HTTP/newproxy.touzeau.biz@TOUZEAU.BIZ	
	Lkrb5.keytab Apply >	

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



There should ONLY be ONE user mapped to a given SPN.

If you have two or more different users mapped to a given SPN record Kerberos authentication will ALWAYS FAIL

Upload the Kerberos ticket

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

erberos Authentication method allows you to link you method is designed if you plan to use a load-balancing; I plan to use a single proxy server you can use the Join 1	r Artica proxy using only the Kerberos method. system with Artica in cluster mode. the domain feature using Kerberos option.		
Kerberos Ticket HTTB/nwysrosystoscesubil@TOUZEAUBI2 expire: about 6 Hours	Please go to your Active Directory, open an M Retreive the krb5 keytab (default in Downloo ktpass -prino HTTP/newproxy articauser@touzeau.biz@TOU HRB5_NT_PRINCIPAL -out %HOU Join Active Directory domain / Ket	NS-DOS session and copy/paste this command. ds directory) and upload it. 7.touzeau.biz@TOUZEAU.BIZ _mapuser ERATH%\Downloads\krb5.keytab	*** -ptype
	User name:	articauser@touzeau.biz	±
& Disconnect	Password:	•••••	Ð
		•••••	Ð

If the connection is successful you can see the expire time of the Kerberos ticket (automatically renewed)

In a cluster environment if you link the Active Directory from the master, Kerberos ticket and Active Directory information are automatically replicated.



Verify the LDAP connection

After connecting to the Active Directory domain, open the menu "**Connections**" This section lists the "**LDAP connections**" to the Active Directory.

It helps Artica to retrieve groups and members thought your Active Directory LDAP service (389 port).

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

Manager	Search a computer, a member		Requests	() 16:2!	
≣≣ Dashboard ■ Your system	Active Directory LDAP connectory and the Active Directory and the Activ	ory.			
🚓 Network & NICs	Also in you have ouner drinki en Adare Dirieddor y servers			_	
iii Active Directory ♥ Join the domain	+ New connection				×
	Hostname	192.168.1.90 / Administrateur@tou	uzeau.Diz		
	Connection success 192.168.1.90 (default)	Connection ID: 0	u.u.z		
S Your categories		LDAP Server Port:	- 389		+
		Active directory Suffix:	DC=touzeau,DC=biz Administrateur@touzeau.biz		
This connection can be edited if you want to	use a different account to allow Artica	Password:			9 9
					« Apply »



()Logout ∄

^않 Members

0%

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 "readonly" mode.

Ν	1y members						
lefa	ult						
Sea	arch						Go!
						Search	۹ -
	Display Name	Domain	EMail Address	Office Phone	Groups		
溶	Administrateurs	touzeau.biz	-	-	-		
121	Utilisateurs	touzeau.biz	-	-	-		
121	Invités	touzeau.biz	-	-	-		
8	Opérateurs d'impression	touzeau.biz	-	-	-		
281	Opérateurs de sauvegarde	touzeau.biz	-	-	-		
绺	Duplicateurs	touzeau.biz	-	-	-		
8	Utilisateurs du Bureau à distance	touzeau.biz	-	-	-		
8	Opérateurs de configuration réseau	touzeau.biz	-	-	-		
8	Utilisateurs de l'Analyseur de performances	touzeau.biz	-	-	-		
쐉	Utilisateurs du journal de performances	touzeau.biz	-	-	-		
8	Utilisateurs du modèle COM distribué	touzeau.biz	-	-	-		
191	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 has Linux/Unix boxes/workstations.

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

he proxy hi our connec	ttp://192.168.1.155:3128 requires a username and password. tion to this site is not private
Username	dtouzeau
Password	



Connect your Artica server using NTLM

You need to follow these requirements:

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

Enable the Active Directory feature.

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

Install or uni	nstall features all/uninstall available features on your server	
select 👻 🖶 Expand		active 🗶 🗸
Status	Software	Action
Uninstalled	Active Directory	✓ Install

Check your DNS settings

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

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

Dashboard					
■ Your system	DNS Servers				
🚓 Network	This section list DNS servers used by the system.				
Ctive Directory	DNS Servers DNS benchmark				
Se DNS					
DNS Cache service	DNS used by the system				
▼ SafeSearch(s)	Local DNS Service: 127.0.0.1				
CONS Servers					
↔ Forward zones	Primary DNS Server : 192.168.1.99				
🖵 Hosts file	Secondary DNS Server: 192.168.1.144				
G My computers	DNS Server 3: 0.0.0.0				
💘 Web-Filtering	Internal Domain 1: lab01.local				
Se Databases	Internal Domain 2:				
Logs center	Internal Domain 3:: Internal domain 3:				



Join the domain

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

Set the full hostname under "Active Directory Full hostname" field

Set the Workgroup domain name of your Active Directory under "Netbios AD Domain" field

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

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

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

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

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

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

Using SSL still requires the $389\ \text{port}$ to be open to the Active Directory.

₩ ■ Your system	Active Directory	»» Join the domain	
# Active Directory	In this case you will be able to silently aut	ystem and your proxy service to your Active Directory service. chenticate users through the NTLM/Kerberos protocol.	
Status Kerberos Authentication	Join Active Directory domain		
 ♦ Cluster made ♦ Join the domain (NTLM) Ø Connections White lists Ø Events 	You can connect your proxy to your A Use the NTLM standard method (joir Use the Kerberos native method is th Both methods require: The time must be synchronized betw Your Active Directory must be resolv Your Active Directory must be resolv Your server computer name cannot t	uctive Directory using 2 authentication methods. In method is compatible NTLMv2 and Windows XP or above. The modern approach but not compatible with Windows XP and 2003. weren Your Active Directory and this server. wed by this server. your proory server. E longer than 15 characters due to netbios name limitations.	
	Active Directory Full Hostname:	ad05.lab01.local	±
Web-Hiltering Databases	Netblos AD Domain:	LAB01	
🖺 Logs center	Active Directory Suffix: Enable SSL (Port 636):	lab01.local	
	Computers AD Location:	CN=Computers	
	Windows Server Type:	Windows 2008/2012/2016	Ψ.
	Windows Authentication metho	d	
	Use the NTLM standard method (join	n method).	
	Administrator:	Administrateur	
	Password: Sync. Time With The AD:	••••••••••••••••••••••••••••••••••••••	



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

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

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

Create the GPO

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

New GPO	×
<u>N</u> ame:	
CA_Proxy	
Source Starter GPO:	
(none)	~
	OK Cancel

Group Policy Management	touzeau.maison	
Forest: touzeau.maison	Status Linked Group Policy Objects	Group Polic
Construction of the second sec	Create a GPO in this domain, and Link it here Link an Existing GPO Block Inheritance Group Policy Modeling Wizard New Organizational Unit Search Change Domain Controller Remove	ne baseli s for this
	Active Directory Users and Computers View New Window from Here Refresh Properties Help	>
> a Construction > a Con > a Con > a Serv > a Serv > a Florida > a Nevada > a Texas	nins nputers tacts ers ice Accounts s CA_Proxy Edit Enforced	¥

- Click on the policy and select **Edit**;
- Expand the following section:
 - o User Configuration
 - o Preferences
 - Control Panel Settings
 - Internet Settings.
 - Right click and select New Internet Explorer 10 (this policy will also be applied for the IE 11);
- On the standard windows with the Internet Explorer settings, go to the **Connections** tab and press **LAN Settings** button.
- Turn ON the checkbox "Use a proxy server for your LAN" and specify the Address and Port of your proxy server (for example 192.168.1.11, port 3128).
- To enable this option, **press F6 button** (underline for that setting will change the color from red to green).
- To **disable** specific policy setting press **F7** (disable the option "Automatic detect settings" this way).

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

To enable all settings on the current tab, press ${\bf F5}.$ To disable all policies on this tab use ${\bf F8}$ key.

• Press OK twice to save settings.

Group Policy Manage ment Ed File Action View Help 🗢 🄿 🛅 🔚 💼 👘 CA_Proxy [MAINAD.TOUZEAU. To set up an Internet conr Setup. ection, dick > Preferences Dial-up and Virtual Private Network setti Policies how in this view Preferences × Local Area Network (LAN) Settings Windows Settings Control Panel Settin Automatic configuration Data Sources Devices Folder Options To ensure the use of Choose Settings server for a con Internet Settings
 Local Users and
 Network Option Automatically detect settings O Never dial a tic configuration Dial whene O Always dial Power Options Address: Current Local Area Net Scheduled Tasks Proxy server LAN Settings do Choose Settings Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). II, Start Menu Address: 192.168.1.96 Port: 3128 Advanced... Bypass proxy server for local addresses ОК Cancel Internet Settings

Group Polic

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

Prevent Changing IE Proxy Settings Using GPO

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

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





Restful API

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

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

Inside the POST, define an array like this example:

```
$ch = curl init();
$CURLOPT_HTTPHEADER[]="Accept: application/json";
$CURLOPT HTTPHEADER[]="Pragma: no-cache,must-revalidate";
$CURLOPT HTTPHEADER[]="Cache-Control: no-cache,must revalidate";
$CURLOPT HTTPHEADER[]="Expect:";
$CURLOPT HTTPHEADER[]="ArticaKey: kyM6ixXavn8sE7P9GoBYqX3by6ZaRCc5";
$MAIN_URI="https://192.168.1.173:9000/api/rest/system/activedirectory/settings";
curl_setopt($ch, CURLOPT_HTTPHEADER, $CURLOPT_HTTPHEADER);
curl_setopt($ch, CURLOPT_TIMEOUT, 300);
curl_setopt($ch, CURLOPT_URL, $MAIN_URI);
curl setopt($ch, CURLOPT RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYHOST,0);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER,0);
//WINDOWS SERVER TYPE: WIN 2003 or WIN 2008AES for 2008 > 2016
//WindowsActiveDirectoryKerberos 1 = Full kerberos, 0 = NTLM
$POSTz= array("
WINDOWS SERVER TYPE"=>"WIN 2008AES",
"ADNETBIOSDOMAIN"=>"LABO",
"ADNETIPADDR"=>"192.168.1.23"
"fullhosname"=>"dc01.labo.corp",
"WINDOWS SERVER NETBIOSNAME"=>"dc01",
"WINDOWS DNS SUFFIX"=>"labo.corp",
"COMPUTER BRANCH"=>"cn=computers",
"WINDOWS_SERVER_ADMIN"=>"Administrator",
"WINDOWS SERVER PASS"=>"Password",
"WindowsActiveDirectoryKerberos"=>0);
curl setopt($ch, CURLOPT POSTFIELDS, $POSTz);
$response = curl_exec($ch);
$errno=curl errno($ch);
if($errno>0){
   echo "Error $errno\n".curl error($ch)."\n";
   curl close($ch);
   die();
}
$CURLINFO_HTTP_CODE=intval(curl_getinfo($ch,CURLINFO_HTTP_CODE));
if ($CURLINFO HTTP CODE<>200) {
   echo "Error $CURLINFO HTTP CODE\n";
   die();
$json=json decode($response);
if(!$json->status){echo "Failed $json->message\n";die();}
echo "Success\n";
```

F

Use an authentication portal (Hotspot)

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

Install the "Web portal authentication" service

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

Insta	all or uninstall features		
soloct -	B Expand	<hr/>	
Scieut V		Web portal	X -
Status	Software		Action
Installed	Web portal authentication		✓ uninstal



Install the "Web portal splash screen"

The first install trough the features section installs the Nginx service, you will find **"Web services**" on the left menu. Select the "**All websites**" submenu. Click on the button "**New service**"

Set the name of the service and choose "Create a portal authentication page"

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: Portal splash screen	
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 website stored on a remote server.	
Webpuges Create a portal authentication page a portal authentication page (aka HotSpot) 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. Web-Filtering Error editect 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.	
« add »	



Your Web service appears to "Not configured".

You need to setup ports and server names before make the service available. Click on the added service.

Web si	ites					
+ New service	Reconfi	gure service			Search	٩
Status	Saved On	Service	Server Names	Туре	Destination	
Not configured	-	Portal splash screen		Hostpot Web service	-	🔽 💿 🧲

Select the "Server names" tab.

Under items, put all hostname or IP addresses that this service can handle as a "virtual host"

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

ortal splash screen						×
General settings	Server names	Ports	Access rules			
Server names						
Server names determ They may be defined of Examples: example.org www.example.org ".example.org mail." 192.168.1.1 ~^(?.+)\example\net When searching for a and regular expressio exact name longest wildcard name longest wildcard name	ine which server blo using exact names, v virtual server by na n match, the first ma e starting with an ast e ending with an ast expression (in orde	nck is used for a gi vildcard names, o me, if name matcl atching variant wi sterisk, e.g. *.exam erisk, e.g. mail.* r of appearance)	iven request. r regular expression: hes more than one of ill be chosen, in the fo uple.org	the specified variants, a lowing order of preced	e.g. both wildcard name dence:	
	Items:	1 192.168.1 2 portal.to	.140 uzeau.biz			
					« Apply »	



Choose Ports tab.

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

Portal sp	olash screen						×	Logout	š.
Gene	ral settings S	erver names	Ports	Access rules					
rr + New	entry	•			Search	Q ,			
Interface	New entry				ocuron -				×
/a	New item								
		Lister	ninterface:	All interfaces			٣		
		1	listen port:	- 80			+		
ring zories	Options	1 lea tha SCI a		OFF					
ces		036 116 332 6	HTTP/2:	OFF					
s :bsites		PROX	SPDY: Y Protocol:	OFF					
ests							« bbe		
-							auu »		

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

Web si	tes					
+ New service	Reconfi	gure service			Search	۹.
Status	Saved On	Service	Server Names	Туре	Destination	
Not configured	-	Portal splash screer	http://192.168.1.140:80 http://portal.touzeau.biz:80	Hostpot Web service	-	

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



Setup the "Web portal authentication"

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

Your system	Authenticate thro HotSpot is a feature that allows you to displa	ugh HotSpot v4 y a Web page or authentication page in order to allow access to Internet		
SDNS	General settings			
(1) Your Firewall	Parameters			
				-
四 Web portal authentication	Authentication page address	http://192.168.1.140	±.	
Parameters	Template:	HotSpot Artica default	٣	
Tevents	Debug:	OFF		
Sessions Manager	HTTP Lost landing page:	http://www.msn.com		
Caching	Landing page:	http://www.articatech.com		

Authentication pages addresses

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

Timeouts sessions

Re-authenticate each-		
ine admenticate each. dinn	mited *	
Disable account after: unli	mited •	
Remove account after: unli	mited •	

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

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

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



Networks section

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

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

General settings Network	s		
+ New network	ew network		×
Networks			
192.168.1.0/24	IP Address:	172.16.1.0	\$
	Netmask:	255.255.255.0 (/24)	Ŧ
rright Artica Tech © 2004-20			« add »

How to Authenticate users?

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

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

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

Authentication	
Active Directory Authentication:	OFF
	Active Directory LDAP connections
use local LDAP database:	Active Directory LDAP connections

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

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

HOTS	pot System		
Welcome Internet a	e to our HotSpot system, set here here you access	ir user name and password in order to have a	free
	Username:		
	Password:		
		" Soumottro »	
		« Journettre »	



Self register

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

Note:

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

Self register		
Activate the register form:	ON	
Max time to register:	5 Minutes	*
Mail server name:	smtp.company.com	
SMTP server port:	25	
sender mail address:	hotspot@proxy.local	
Username AUTH:	Username AUTH	
Password AUTH:	Password AUTH	
	Password AUTH (Confirm)	P
Enable TLS support:	OFF	
Use the SSL encryption:	OFF	
Network Interface:	All interfaces	*

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

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

lotSpc	ot Syst	em	
HotSp	oot System		
Welcome t Internet ac	o our HotSpot system, cess	set here here your user name and p	assword in order to have a free
	Username: Password:		
		« S`Enregistrer »	« Soumettre »
	You using	i an HotSpot system using a Commu for more informations, see Artica Pro	nity License



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

otSpot	: Syster	n		
Registe	r			
As an custome After filling the	r, you can avail of free acce form you will have access t	ss to Internet by regist o a short period in orc	tering here. der to confirm you	r registration
	EMail:			
			«	Submit »
			_	
	You using an Hots For more	pot system using a Co informations, see <u>Artic</u>	ommunity License <u>ca Proxy</u>	

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

Image: Supprimer Archiver	Répondre Répondre à tous Transférer	- Actions rapides -	Déplacer	Indicateurs	Modification	A ³⁾ Fonction vocale *	Zoom	
Supprimer	Répondre	Actions r 🗔					Zoom	
HotSpot System <david@articatech.com> david@articatech.com 1 HotSpot account validation 1<td>13:36</td></david@articatech.com>							13:36	
🚹 Nous avons supprimé les	sauts de ligne en surnombre	dans ce message.						~
Hi, in order to activate http://192.168.1.140:8 confirm=YTo3OntzOjEz LmNvbS8iO3M6MTE6ir tijtzOjEwOiJtYWNhZGR xMDkiO3M6MjoiSUQiC	your account on the Hot O/hotspot.php? OUyZWdpc3Rcl90aW1lij nRlbXBsYXRlX2lkljtZ0JE6I yZXNzljtZ0JE3Oi11MDo21 D3M6MTpiOCI7fQ==	5pot system, clic t <u>pO[E1NTE4NzU</u> (QiO3M6ODoid) (jo4ZDpINDo0M	k on the lir <u>I3NTk7czoz</u> (<u>NIcm5hbW</u> Do1NCI7cz	nk below :OJJVUkwiO3 VUIO3M6Mj/ o2OIJpcGFk2	M6MTk6imh0 A6imRhdmlkQi HiliO3M6MTM	dHA6Ly93d SFydGljYXR I6IjE5Mi4xM	<u>3cubXNu</u> IY2guY29 IjguMS4	

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



Voucher or Room number.

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

The following process is :

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

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

	Remove account after:	unlimited
Authentication		
	Active Directory Authentication:	OFF
	Use voucher method:	

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

Web por HotSpot is a feature	rtal auther	ntication y a Web page or authentication page in order to allow access	s to
General settings	Networks	Vouchers/Rooms	
Voucher	rs/Rooms you to define Internet of + Import vouchers	manager v4 ess options of each voucher or room number Delete all	
Created	Vo	uchers/Rooms	
		N	0

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

001,pass,24

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

mport vouchers					
Copy and paste here your voucher,password,durati duration is a number of h for example: 001,pass,24 Means voucher id 001 an	r vouchers in this format: on. ours. i id password "pass" expire for 1	Lday (24 hours).			
	Vouchers/Rooms:	01.00124 002.00234 003.00324 003.005,005.005,005,005,005,005,005,005,005	~	-	





Vouchers will be displayed on the list.

According to the expire column: if the expire is not set, when the user using the voucher, the schedule will start after the login.

In other case, the Hotspot Manager can click on the schedule button in order to calculate the expire time. After the expired time, the user cannot access to Internet., the HotSpot Manager must click on the schedule button in order to activate the voucher again.

HotSpot is a feature that allows you to display a Web page or authentication page in order to allow access to Internet								
General s	ettings Networks	Vouchers/Rooms						
Vou	chers/Rooms	manager	v4					
This section	allows you to define Internet o	access options of each voi	ucher or room nui	nber				
+ New vo	ucher + Import voucher	rs 👕 Delete all					_	
+ New vo	ucher + Import voucher	s 👕 Delete all			Search		۹.	
+ New vo	ucher + Import voucher Vouchers/Rooms	s 👕 Delete all		Time To Live	Search Expire	Enabled	Q - Delete	
Treated	Vouchers/Rooms	s Delete all	O Schedule	Time To Live	Search Expire about 23 Hours	Enabled	Q - Delete	
- New vo Created 13:44:18 13:44:18	Vouchers/Rooms 001 002	5 Delete all	Schedule Schedule	Time To Live 1 Day 1 Day	Search Expire about 23 Hours	Enabled	Q ~ Delete	
F New vo Created 13:44:18 13:44:18 13:44:18	Vouchers/Rooms 001 002 003	5 Delete all	Schedule Schedule Schedule	Time To Live 1 Day 1 Day 1 Day	Search Expire about 23 Hours	Enabled	Q ~ Delete	

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

Personalize texts in the portal.

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

lotSpot is a feature tha	t allows you to display a	Web page or authentic	ation page in orde	r to allow access	to Internet	
General settings	Networks	Vouchers/Roon s	Messages			
	Title:	HotSpot System				

Mixed transparent + Active Directory proxy.

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

- Users connected to the Active Directory (according to a GPO) are automatically connected to the proxy port (3128).
 The NTLM/Kerberos authentication allow them to silently sends the credentials to the proxy.
- Computers that are not connected to the Active Directory will use the proxy as the main gateway. In this case, the proxy will redirect sessions to the portal in order to help user to be authenticated trough the Active Directory.

To simply allow this method, you need to exclude the $\mbox{Active directory port}$ from the authentication portal:

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

Active Directory									
S DNS	Connected port	Transparent ports Remote ports	Communication ;	ports					
()) Your Firewall	+ New port	Apply configuration							
Our proxy							Search		Q -
🔀 Status	TCP Address	Listen Port	HTTPS	Cache	AUTH.	HotSpot	Filter	Enabled	Delete
¢ ₀ Global settings	127.0.0.1	56633 Internal Port (Only available for Artica)						~	
₩ICAP Center	102 160 1 140	2120 Main part. Main connected part 0.0.0.2120							•
📇 Authentication	172.100.1.140	5126 Main port: Main connected port 0.0.0.5126		Ŷ	Ť	Ŷ	•	Ť	•
Errors pages									
Proxy events									

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

Enabled:	ON	
listen port:	- 3128	+
Service name:	Main port: Main connected port 0.0.0.3128	
Description:	Description	
Accept proxy protocol:	OFF	
Disable authentication:	OFF	
Disable caching:		
Disable Web-Filtering:		
Disable the HotSpot feature:	ON	
Listen interface:	eth0 192.168.1.140 - Interface eth0	٣
Forward Interface:	All	*
Use the SSL encryption:	OFF	
Use a certificate from certificate center:	None	*

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



Active Directory



LOAD-BALACING FOR PROXIES.

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

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

HaCluster, Make proxies in cluster with Active Directory.

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





Page: 178



Install the load-balancing service.

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

Insta This section	all or uninstall featur	es on your server	
select 🕶	Expand A Wizards	balancing	X -
Status	Software		Action
Uninstalled	Load-balancing and Reverse Proxy		✓ Install

Create the service and add backends

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

Dashboard	Load balancing » TCP services										
≣ Your system	A TCP service is a Load-balancer listen port designed to serve multiple backends. This section allows you to manage front-end services designed to handle connections in order to dispatch them to defined backends										
Load-Balancing/Reverse	+ New servic	:e		Search		Q -					
Service	Address	Service Name	Method	Backends	Active	Del					
< TCP services ≅ Rules & Objects	No results										


ew service		×
New service		
Define the main settings of your new see HTTP/HTTPs Proxy Load-balancer: Des Reverse Proxy: Designed to redirect/bala TCP redirect: Designed to redirect/bala SMTP redirect: Designed to redirect/bala	vice and choose the service type: igned to be an high availability service of Artica proxies ance connections to HTTP/HTTPS Web services ne TCP connections to other servers. ance SMTP connections to mail servers.	
Service name:	PROXY-LB	
Service type:	HTTP/HTTPs Proxy Load-balancer	
Listen IP address:	192.168.1.231	K
listen port:	- 8080 +	
	# add »	
	« add »	l

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

proxy_lb	Proxy clients			
+ New Backend	-		Search	Q -
Address	Backends	Weight No results	Active	Del
		No results		

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

	Service name:	proxy_lb	
	Backend name:	newproxy.touzeau.biz	±.
	Outgoing address:	ethO	*
	Destination address:	0.0.0	٥
	Destination port:	- 8080	+
	Failover only:	OFF	
HTTP Prox	y mode		



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

proxy_lb Proxy clie	nts					
+ New Backend		S	earch		Q	•
Address	Backends			Weight	Active	Del
newproxy.touzeau.biz:8080	newproxy.touzeau.biz			1	~	0
newproxy2.touzeau.biz:8080	newproxy2.touzeau.biz			1	~	0

Enable the Load-balancing compliance on your proxies.

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

PowerDNS system	Connected ports	s Transparent ports Remote ports	Communication ports					
Our proxy	+ New port	Apply configuration						
🔁 Status						Search		Q -
🕫 Global settings								
₩ ICAP Center	TCP Address	Listen Port	HTTPS	Cache	AUTH.	Filter	Enabled	Delete
📽 Authentication	127.0.0.1	58238 Internal Port (Only available for Artica)					~	
Errors pages	All interfaces	3128 Main port: Main connected port 0.0.0.3128		~	~	~	~	0
Proxy events								
≁ Listen ports								
SSL Protocol								



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

Click on "Apply configuration"

New port			×
New port			
	Enabled:	ON	
\	listen port:	- 8080 E +	
	Service name:	Load-balancing compliance	
	Description:	For the load-balacing service	
	Accept proxy protocol:	ON	
	Disable authentication:	OFF	
	Disable caching:	OFF	
	Disable Web-Filtering:	OFF	
	Listen interface:	All	

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

Listen po This section allows The frist one Conne Connected ports ar The second one Tra Important: Transpa	DITS you to define how browsers can b coted ports list ports used directly e able to authenticate users throu nsparent ports allow the proxy to rent ports cannot authenticate u	e connected to your prox in browsers settings. gh LDAP or Active Direc act as the main gateway sers.	ty. Story. rand is able to catch l	both HTTP/HT1	'PS requests wit	hout need to ch	ange browsers	settings.	
Listen ports Reconfigure: 10	0% Done Reloading Proxy service 🛓	Details»							
		Listen port	ts Reconfigure - 100%	Done Reloading	Proxy service				
Connected ports	Transparent ports	Remote ports	Communication po	rts					
							Search		۹.
TCP Address	Listen Port			HTTPS	Cache	AUTH.	Filter	Enabled	Delete
127.0.0.1	58238 Internal Port (Only ava	ilable for Artica)						~	
All interfaces	3128 Main port: Main conr	ad port 0.0.0.0:3128			~	~	~	~	0
All interfaces	8080 Load-balancing complia	nce For the load-balacing	service		~	~	~	~	0

Connect your browser to the Load-balancing service port

Load-balancing with Kerberos method.

The Kerberos ticket

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

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

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

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

Minor tweaks.

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

	Please go to your Active Directory open		
	retrieve the krb5.keytab (default in Dow	an MS-DOS session and copy/paste this command. mloads directory) and upload it.	
	ktpass -princ HTTP/newpr	roxy.touzeau.biz@TOUZEAU.BIZ -mapus	er
Kerberos Ticket	articauser@touzeau.biz@T KRB5_NT_PRINCIPAL -out %	<pre>POUZEAU.BIZ -crypto rc4-hmac-nt -pa HOMEPATH%\Downloads\krb5.keytab</pre>	ss ****** -p
expire: about 6 Hours	Join Active Directory domain /	/ Kerberos Authentication	
	User name:	articauser@touzeau.biz	Ē
& Disconnect	Password:	*****	Ģ
		*****	(1)
	Active Directory full hostname:	dc16.touzeau.biz	
	FODN of secondary DC-	FQDN of secondary DC	
	r gorror secondary be.		
	Service Principal Name (SPN):	HTTP/newproxy.touzer_oiz@TOUZEAU.BIZ	
	Service Principal Name (SPN): Kerberos Realm:	HTTP/newproxy.touzer_oiz@TOUZEAU.BIZ	

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

proxy_lb Proxy clients		
proxy_lb (HTTP Proxy mode)		
Service name:	proxy_lb	
Listen IP address:	192.168.1.231	¥
listen port:	- 8080	±
NTI M compatible (MS Active Directory)	OFF	



CACHING FEATURE

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

Install the Cache feature.

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

Insta This section	all or uninstall features on allows you to install/uninstall available features on y	/our server
select -	Collapse 🔏 Wizards	Caching objects 🗶 🗸
Status	Software Caching objects on local disk	Action
Installed	Activate the possibility of store downloaded objects on lo	ocal disks in order to safe bandwidth and provide a strong caching system.

Create Your first cache.

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





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

New cache Disk				×
Create a	cache based o	n a new hard disl	x	
This wizard helps y	you to format and create a new o	ache based on a free disk for better pe	rformances.	
			Search Q -	
Disk	Туре	Size		
/dev/sdb	-	100 GiB	📾 choose	

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

New cache Disk	×
Create a cache based on a new bard disk	
This wizard helps you to format and create a new cache based on a free disk for better performances.	
Creating New cache: 60% Formating /dev/sdb1	
ConfirmCreate cache on /dev/sdb	
This operation will format this hard drive. All datas will be lost!	
« Create cache on /dev/sdb (100 GiB) »	

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

+ New cache Disk +		+ New o	ache Folder	Apply configura	tion				
						Search		٩	•
	Used	Order	CPU	Cache	Directory	Size	I	Rebuild	
inactive	0%	1	#O	CachesDisk Files: 0 KB to 3 GB	/home/CachesDisk/disk	0/48.83 GB	↑ ↓	¢	C
Active	0%	1	#1	sdb - small - CPU#1 Files: 0 KB to 512 KB	/media/Cachesdb/proxy-caches/small-cpu1	0 KB/25.17 GB	↑ ↓	6	C
Active	0%	1	#1	sdb - big - CPU#1 Files: 512 KB to 2.93 GB	/media/Cachesdb/proxy-caches/big-cpu1	0 KB/58.72 GB	↑↓	â	C

Is Artica cache Microsoft Windows Updates?

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

How can I see if caches are working as expected?

On the left menu, choose Caching and Cached items

Click on the button "Analyze caches"

This button run a background task that extract all stored objects from caches in order to display them in a table.

This section allows you to delete stored objects too

## Dashboard	Stored objects			
🚍 Your system	This feature allows you to list cached objects in memory or disks. It is not realtime feature because extracting cached objects consume hardware performance. You hat to run the analysis task to display items.			
A Network				
S DNS				
# Your proxy		Search	٩	•
Security Caching	Web Sites	Size	iects	
B Status	# windowsupdate.SQUIDINTERNAL	186.99 MB	658	0
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	# windows.com	2.46 MB	1	0
📾 Central Cache	microsoft.SQUIDINTERNAL	50.9 KB	4	0
E Cached item(s) O Deny from cache	# digicert.com	4.1 KB	5	0
Nour categories	msocsp.com	2.35 KB	1	0
🛎 Statistics	microsoft.com	0.33 KB	1	0
E Logs center	⊕ msftncsi.com	0.21 KB	1	0



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.

Manager Administrator –	Search a computer, a member	Requests	(18:42:53)	📲 Cpu:3.7% Mem:18.4%	ᄵᄰ Members 📮	()Logout /Ξ
	1					
 Dashboard Your system 	Deny from cache					
🚓 Network & NICs	+ New item t3 Apply rules					
S DNS					Search	۹ +
(h) Your Firewall	Items				Туре	Delete
⊕ Your proxy	192.168.1.209				Source IP a	iddress 📋
Seching						
🕰 Status						
,III Cache level						
Caches Center	Copyright Artica Tech © 2004-2018			v4.01.102918	Enterprise Edition U	Time: about 1 Month
Central Cache						
Sour categories						
🖿 Statistics						

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.

ew item	
New item	
Give the main domain part of your websit www.domain.tld is not supported Here the list of destinations that will be n You can define both IP addresses or dom An ip address can be a subnet: 192.168.1 A domain can be a domain and it's subdon Or the main domain: eg domain.com	e: images domain.tld or domain.tld. did not give the www of the web site : ot cached by the proxy. ins. .0/24 or a single IP 192.168.1.1 main using the hat ^: eg ^ www.domain.com
item:	item
Туре:	Web server or domain
	None
	Web server or domain Destination IP(s)
	Source IP address



ERRORS PAGES AND TEMPLATES

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

📰 Dashboard		
📰 Your system	Errors pages	
👬 Network	Proxy errors pages allows you to skin the templates and errors pages content when proxy send errors to your members	
Rsync server		
쁄 Filebeat	Templates Manager Parameters Errors pages	
S DNS	+ New template Files manager	
()) Your Firewall		Search Q 🗸
# Your proxy	ID Template Name CSS HEAD	BODY View Export Delete
B Status	1 Red error page Modify CSS Modify H	HEAD Modify BODY View 🛓 🌔
C Statistics	2 White error page Modify CSS Modify H	HEAD Modify BODY View
¢ [©] Global settings	3 Microsoft style template Modify CSS Modify H	HEAD Modify BODY View
₩ ICAP Center	4 HotSpot Artica default Modify CSS Modify H	HEAD Modify BODY View
Authentication		

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



The Templates Manager

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

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

-1-A	ctive Requests	@ R	equests	Statistics	12:10:58	Cpu:6.1% Mem:30.6%	[%] Memb	ers 🖵 76 cor	mputers	Admin Guide	3	() Log	out	≣
			My te	mplate: HEA	٨D									
Er Prox	rors pages allo	ges ows yo	My	/ template - HE	AD									
Ter + N	mplates Manager ew template	🗗 File	<	DOCTYPE HTMI 2 <html> 3 <head> 4 <t 5 %J 6 %C 7 <s 8 fu 9 fu</s </t </head></html>	> itle>%TITLE QUERY% SS% cript type= nction blur nction chec	<pre>HEAD% "text/javascript"> ()() tfTonNestWindew()()</pre>				-			x .	•
ID	Template Nam	ne		10 11 <td>pt></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>elete</td> <td></td>	pt>								elete	
1	Red error page	e											0	
2	White error p	age								« Apply »			0	
3	Microsoft styl	le temp											0	
4	HotSpot Artic	a defa						1					0	
21	My template						Modify CSS	Modify HEAD	Modify BO	DY View	e		C	

Some specific token can be used:

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

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

<u>F</u> ichier Éditio <u>n</u> <u>A</u> ffichage <u>H</u> isto	rique <u>M</u> arque-pages <u>O</u> utils <u>?</u>				- 0	× Kaspe	rsky Anti Target	Kaspers	ky Security 8.0
Dynicamic Title	× +								
← → ⊂ ଢ	① A https://192.168.1.1:9000/fw.proxy.temp	₪ ☆	Q Rechercher	∓ ∥	\ 🗉 📑 🛛	=			
						^			
							Sear	ch	
							BODY	View	Export I
	51					EAD	Modify BODY	View	4
						EAD	Modify BODY	View	4
	Dynic	amic Title	×			EAD	Modify BODY	View	2
	Dynica	amic Title				EAD	Modify BODY	View	ڪ
	Su	b-title				EAD	Modify BODY	View	2
	Text	paragraph							
	F	orm:							
	Label1:	ata]						



Insert images in templates.

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

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

Prov	y errors pages allows you to skin the tem	plates and errors p	ages content when proxy send	d errors to your members					
Te	mplates Manager Parameters	Files man	ager						*
+ N	ew templ ite	± 1 New f	ile						
ID	emplate Name					Search	Q	•	
1	Red error page	ID	File Name	Token	Туре	Size	Delete		
2	White error page			No	results				
3	Microsoft style template								

Click on Upload a file and select the picture you want to import.

Take care of the "Token" column, this Token must be added in your HTML code or CSS code.

les n	nanager	New file	×				
1 N	lewfile	css.js.gif.jpeg.jp	a File g.png.woff	Searc	h		۹ -
ID	File Name		Token		Туре	Size	Delete
1	2019-06-20_14-13-3	1.jpg	[file=2019-06-2	0_14-13-31.jpg]	image/jpeg	2.93 KB	0

For example:

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




Assign your template to the proxy error pages

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

Templates Manager	Parameters	Errors pages	
oxy service error p	ages		
Note. This section is fo	ar darim arrars maar	nted by the prove Net the Web Elizer	
Note: This section is fo These error pages are	designed to notify you	ated by the proxy Not the Web filterin Ir users about communjications proces	g blocked error pages sing such as Internet site unavailable, routing issues, ACLs
		Use simple template mode	
		Prove sopulate array pages:	Example Templete Artice documentation
		Proxy service error pages.	Example remplate A tica documentation
			14.0
		FIP template:	White error page
		F I P template: language (Default):	en-us
		F I P template: language (Default): Proxy administrator email:	White error page en-us david@articatech.com
		FIP template: language (Default): <u>Proxy administrator email:</u> Remove Artica version:	White error page en-us david@articatech.com

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

	websitedoesntexists.com	••• 🗟 🗘 Rect	hercher	⊻ ₩\ @ 📟	0
🐣 Windows7 🜐 Step 6. Enable NTLM a 🧊 n	413437.ip-37-187-14 🥳 Unbound : un ré	ésolve 🦾 www.articatech.c	:om 💮 categories.articate	ch.n)
A	ER	R	OF	R	
	The requested URL could	I not be retrieved			
	The following error was encount URL: http://www.thisawebsitedoe Unable to determine IP name "www.thisawebsi	ered while trying to retrieve sntexists.com/ address from host tedoesntexists.com"	e the		
	The DNS server returned:	n name does not exist.			
	This means that the cache was r hostname presented in the URL correct. Your cache administrator is davi	not able to resolve the Check if the address is d@articatech.com.			
	Generated Thu, 20 Jun 2019 12:55:2 Artica Proxy, vers	0 GMT by router louzeau.biz (squik iion 4.05.061819	d)		

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

THE ITCHARTER SERVICE

IT Charter feature

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

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

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

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

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

You can create multiple charters.

When an user as successfully read a policy agreement, it should be redirected to the next policy agreement.

Download the additional documentation

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







THE WEB FILTERING

The Web Filtering is a module designed to filter million websites against categories.

It cannot be used to filter a small list of websites.

This behavior is important because using the Web-Filtering engine will consume memory.

By default, it should use about 700MB to 2.5GB of memory (depends how many categories you using on rules).

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

Enable the Web-Filtering engine

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

Insta This sectio	all or uninstall features	our server	
select -	Expand A Wizards	Filtering engine 🗶 🗸	
Status	Software	Action	
Uninstalled	Web-Filtering Engine	✓ Install	

6

Web-Filtering rules

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

		-					
+ New I	Rule Build Web-Filtering rules Verify rules						
					Search		Q 🗸
Order	Rule	Sources	White Lists	Black-Lists	Duplicate	Move	Delete
-	Default No category has been added Default rule is used when no group matches others rules	-	0 Category	0 Category		-	-
	+ New I Order -	+ New Rule Build Web-Filtering rules Verify rules Order Rule _ Default No category has been added Default rule is used when no group matches others rules	+ New Rule Build Web-Filtering rules ✓ Verify rules Order Rule Sources _ Default No category has been added Default rule is used when no group matches others rules	Hew Rule Build Web-Filtering rules Verify rules Order Rule Sources White Lists _ Default No category has been added Default rule is used when no group matches others rules - 0 Category	+ New Rule Build Web-Filtering rules Verify rules Order Rule Sources White Lists Black-Lists _ Default No category has been added Default rule is used when no group matches others rules _ 0 Category 0 Category	Image: Power were were were were were were were	Image: Problem state Image: Problem state <th< th=""></th<>

Understand the Web-filtering processing

Rules are not analyzed like a Firewall.

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

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

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

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

A good way to create Web-filtering rules.

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

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

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

For the first step, we assign blacklists categories in the default rule, copy the default rule to a new rule.

For the copied rule, we define the source group and remove the socialnet category from the rule.

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



6

Multiple Sources

A rule can store one of multiple sources

nk group Social allow		
Social allow Link group		
New source:	None	*
	1	٩
	None	
	Virtual group	
	Active Directory group	
	Active Directory Organization	
	Remote LDAP group	

Sources can be

A Virtual group:

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

An Active Directory Group:

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

An Active Directory Organization:

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

A remote LDAP Group.

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

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

Verify that databases are updated

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

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

his sectio	b filtering: Rules nallows you to create deny rules according categories.	,					
+ New I	Rule 🖬 Build Web-Filtering rules 🗸 Verify rules	_					
There ar	e 18 missing database(s). ase, some rules will be not correctly filter your users.						
Recomp	ile your rules or launch an update task.						
		-		Se	arch		a -
	Rule	Sources	White Lists	Black-Lists	Duplicate	Move	Dele
Order			2 Catagorias	14 Catagorias			
Order	Default Default rule is used when no group matches others rules	-	z Categories	To Categories	En la	-	-



Be notified when members browse on specific categories.

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

Dashboard	Web filtering: Parameters
🚍 Your system	The Web-Filtering service use local databases in order to check websites. You have 2 databases:
A Network	Artica Community databases: These databases (around 1.500.000 entries)are autom Artica Enterprise databases: These databases (around 45.000.000 entries) must hav
Active Directory	
S DNS	Paramete s Notifications
Our proxy	{ufdb_notif_categories_explain}
🗞 Web-Filtering	
🕰 Status	+ Add category SMTP parameters
🗢 Service Parameters	
Connector	Categories
≣ Filtering rules	Porn
Web-Filtering policies	
Events	Sexual Education
⊗ Error page	Sporn (Free Edition)
💩 Categories update	
> Your categories	Sexual Education (Free Edition)

Select the "Notifications" tab.

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

Manually update Web-filtering databases

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

Active Directory	Status	Update set	ttings Schedule	Update events
S DNS	🗑 Delete dat	ab:ises 📀	Update	
Our proxy				
🐼 Web-Filtering		Status	Category	Туре
፼ Status ✿ Service Parameters	Updated	۲	Abortion	Artica
Connector	Updated	à	Advertising	Artica
≣ Filtering rules ♥ Web-Filtering policies	Updated	1	Agressive	Artica
Events	Updated	3	Akamai	Artica
Categories update	Updated		Alcohol	Artica



Schedule Web-Filtering databases update.

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

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

Jpc	date the main Webf	filter databases				
neck on hupdate	Internet if there is new Webfilter databases and up e is about 150Mb size.	date the local container.				
+ Na	ew task 🕞 Apply all schedules					
+Ne	ew task Apply all schedules					
+ Ne	ew task 🛛 Apply all schedules		Search		Q	۲
+ Ne	Task	Description	Search	Run	C Enabled	Dele

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



The Web-Filtering error page.

The Wizard

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

Dashboard	Web-Filtering HTTP ser	vice v4.05.050201	
Your system	The Web-Filtering Web service is designed to provide the This service is designed to be personalized according to sp	error page when your members match a web-filtering rule. becific rules in order to allow members bypassing rules or creat	te a ticket to support team.
🚓 Network			
Active Directory	Status Rules Unblock list Requ	Jests list	
PowerDNS system			
# Your proxy		Redirect all blocked sites to a remote web pa	ge
WAF and ACLs	Redirect all blocked sites to a remote web page	If you using a local Web service (Web-Filtering Error	service), use this feature, and define the URL as a
🕸 Web-Filtering	Enabled	http://myweberrorpage	
🔁 Status		Redirect all blocked sites to a remote web page:	ON
¢ [©] Service Parameters		complete URL:	http://192.168.1.236:80/ufdbguard.php
¢° Connector ≡ Filtering rules		complete URL HTTPS:	192.168.1.236:443/ufdbguard.php
Web-Filtering policies			
@ Events			
© Error page			« Wizards » « Apply »
Categories update			

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

0		
When a request is blocked, the Web-Filt is denied. This wizard creates a local web service to In the hostname field, you can type any h be already resolved in your DNS server. If you did not want to handle any hostna	ering service is able to redirect the request to hat is able to handle redirected requests. ostname, virtual hostname (eg. denied.comp me in DNS for the Web-Filtering error page,	o a web page that explains why the request any.com, block.mydomain.com) that must set the IP address of this server.
hostname:	192.168.1.236	
listen port:	- 80	+
listen port (SSL):	- 443	+

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

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

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

Tune the Web-filtering service

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

Tashboard	Web sites		
🚍 Your system			
👬 Network	+ New service Reconfigure service		
Active Directory			Search Q -
PowerDNS system	Status Saved On Service	Server Names Type	Destination
⊕ Your proxy	Web filtering error nage	http://*:80 Catch- III https://*:443 Catt -sill http://*:443 Catt -sill	
WAF and ACLs	OK 2019 Wednesday May 01	https://192.168.1216:443	- 🗹 🔮 🚺
◊ Web-Filtering		http://domain.ti.con/80 https://domain.ti.co	
Your categories			
Categories service			
• Web services			
🔁 Status	Copyright Artica Tech © 2004-2019	v4.05.042301 E	Interprise Edition Temps de vie: environ 13 Jours
All websites			



Skin the Web-filtering error page

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

By default, you should see this error page



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

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

Manage templates

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

۲	Your proxy								
b 1	🔁 Status	Te	mplates Manager Para	meters E	rrors pages				
	♥ Global settings	+ N	ew template 🛛 🖻 Files man	ager 🛃 Impo	ort a template	Build templat	tes		
_	Authentication					Sea	rch		۹.
	Errors pages	ID	Template Name	CSS	HEAD	BODY	View	Export	Delete
	Proxy events Listen ports	1	Red error page	Modify CSS	Modify HEAD	Modify BODY	View	2	0
	SSL Protocol	2	White error page	Modify CSS	Modify HEAD	Modify BODY	View		0
	Global rules	3	Microsoft style template	Modify CSS	Modify HEAD	Modify BODY	View		0
	ACL s Proxy	4	HotSpot Artica default	Modify CSS	Modify HEAD	Modify BODY	View	٩	0
8	Web-Filtering								

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

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

Templates can be modified using HTML code.



Using images in your template

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

es mana	lger					
ID	le Name	Token	Turne	Search	Delete	\ •
D	e Name	No	results	Size	Delete	

A new page is displayed and allow you to upload your pictures.

Click on the button "New file" in order to upload your image file in the File Manager area.

Files manager					×
L New file	Sea	arch	ĺ	۹.	
ID File Name	Token	Туре	Size	Delete	
1 Articafond1.jpg	[file=Articafond1.jpg]	image/jpeg	324.66 KB	0	
	-				

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

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

Real Real	ed error page:	BODY							<
D:	Red error page	- BODY							
E Yo N Dh ⊕ Yo	 div id="wrag <hi class="ba<br/">%DNNAHC_CON: </hi> 	='checkIfTc pper"> i> IENT%	pMostWindow()' style=	'background-im	age:url("[fil	e=Articafond]	.jpg]")'þ		
							« Apply »		۲.
	ALL MILLING								_lelete
or⊛ ا⊀	ten ports	1	Red error page	Modify CSS	Modify HEAD	Modify BODY	View	4	0
■ SSI	Protocol	2	White error page	Modify CSS	Modify HEAD	Modify BODY	View		0
	obal rules	3	Microsoft style template	Modify CSS	Modify HEAD	Modify BODY	View	0	0
Glo									

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

Browsers Rules

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

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

Privileges are:

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

Browsers rules

There is a number of services/applications that use user agents that cannot negotiate NTLM properly because these services/applications are non-NTLM aware (java, iOS, Android...). If your Proxy is connected to your Active Directory server these services/applications will be prompted for authentication credentials and/or may receive some authentication errors. The solution is to whitelist these known user agents that are non-NTLM aware.

+ New Rule Apply rules Delete all						sth	<u>م</u>	
Pattern	Vendor Name	Category	Enabled	Whitelist	Deny	Bypass Webfilter	No Cache	
AMPVConnector	AMPVConnector	AMPVConnector						0
APT-HTTP	Debian	Unix		~				0
Acrobat	Adobe	Adobe						0
Adobe Downloader	Adobe	Adobe						0
Adobe Flash Player	Adobe	Player						0
Adobe Synchronizer	Adobe	Adobe						0

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

Rule: 183 regex:^Mozilla.*Windows.*AppleWebKit.*Chrome\/	
Rule: 183 regex: ^Mozilla.*Windows.*AppleWebKit.*Chrome\/	
Dettern, remuch Amille * Minday or * Apple Mich Vit* Chrone /	
Pattern: Tegex: Mozina, Windows, AppleWebkit, Chromev	
Vendor name: Google	
What is ?: Google Chrome Windows	
Category: Browsers	
Whitelist. OFF	
Deny: OFF	
Exclude from web filtering: OFF	
« Арр	ly »

Page: 202

Bandwidth rules

Bandwidth rules allows you to implement a flexible limit to control the bandwidth used by your members during HTTP sessions. The purpose of the engine is to "reduce" the HTTP bandwidth. The proxy New Rule service manages only this protocol. Others protocols that are not passing through the proxy are not affected. the bandwidth limitation is based on the Token Bucket al the bandwidth limitation is based on the Token Bucket algorithms. Basicaliyyou have a bucket with a bandwidth reserve and a refilling speed. The emptying speed will depend on the user's download. If the user uses sensibly the connection, the bucket will refill faster than it empties it, so there will be no penalizatio if the user star to empty the bucket much faster than the refilling rate, it will empty and then it will have to settle v refilling speed. For each bandwidth throttling rule you configure, you have two types of buckets available: network and per client. Each client will consume their personal buckets and everyone included in the matched rule will consume the netwo When you create a new rule, the from allows you to limit the bandwidth according 2 sections: Limit the network: Set a limit of all objects that matches the rule to the defined value after downloading a size in an unlimited bandwidth. rule name: Limit 1024/512 Limit bandwidth per client: Set a limit of each object that matches the rule to Global limit the defined after downloading a size in an unlimited bandwidth. {limit_network}: DN N In our example we limit the network to 1024 KO/s immediately (0 unlimited size) and we limit each client to 512 KO/s after downloading 1MB. Maximum illimited size (MB): - 0 ÷ - 1024 Max download rate (KO/s): Per client limit ON Limit bandwidth per client: + Maximum illimited size (MB): Select the new created rule in the table and click on the "Proxy objects" tab. Max download rate (KO/s): - 512 + Proxy objects defines when the bandwidth rule is activated by the proxy. Search a computer, a member - Active Requests ◎ Requests ③ 09:41:02 ■ Cpu:4.2 Bandwidth rule Rule 10 speedtests The purpose of this feature is to pro This is useful when our internet line Proxy objects Search Rule Name Descri Orde Is/is Not Objects Туре Items For obj 0 spee Source IP address Is Mon IP Copyright Artica Tech © 2004-2019

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

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



TCP MARK Rules

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

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

A Network	MARK outgoing TCP packets									
(▲) Your Firewall	IT you using a frewall with rules using TCP MARK, or if you using the Link Balancer feature, you can create rules that tcp packets based on the HTTP Layer									
Our proxy	+ New	Rule Apply rules								
WAF and ACLs				Search		Q	•			
Access rules	Order	Rule Name	Description		Enabled					
 Headers Rules Bandwidth rules 	0	Bouyges ADSL	For objects « <u>Réseau Interne</u> » (1 Items) th MARK «0x21»	hen Use	~	↑↓				
TCP MARK Rules	1	Bougyues 4G mon ip	For objects «Mon IP» (2 items) then Use «0x24»	MARK	~	↑↓ (
Seching	2	transfert bouygies ADSL	For objects « <u>whatismyip.com</u> » (1 ltems) 1 MARK «0x21»	then Use	~	↑↓ (
Your categories										



List all ACLS objects

Advanced ACLs use proxy objects in order to operate HTTP rules.

The "Proxy objects" section allows you to search objects or items inside objects (use the "Search field).

This table list all rules used by the same object.

You can delete or disable an object here; it will be removed from all rules.

 Network DNS ⊕ Your proxy 	Proxy objects Proxy objects are used by all ACL This section allows you to search	s rules. objects or items inside objetcs inor	der to suit them.			
ACLs Proxy	Search messages				Go!	201
Access rules	Object name	type	Rules	Items	Enabled	Delete
 Reply access rules Headers Rules 	Agences	Source IP address		1	~	0
E Browsers rules	BerlitzDoms	Web server or domain		1	~	0
 Bandwidth rules TCP MARK Rules 	BerlitzFrIP	Destination IP address		1	~	0
& Proxy objects	Everyone	All		-	\checkmark	0
🞗 Web-Filtering	Local Domains	Web server or domain		37	~	0
Your categories	Mime: Executables	Mime type (reply)	Deny executables	19	~	0
Logs center	Office365 Dest Domains	Web server or domain		39	~	0
Databases	Office365 Dest IP	Destination IP address		42	~	0
	ProxyAuthorized	Static Active Directory Gr	oup	-	~	0
	ProxyFullrestricted	Static Active Directory Gr	oup	-	~	0



USE UPSTREAM PROXIES

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



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

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

		wanable reatures on your set	rver		
select -	Expand <u>A</u> Wizards				
				parents	× -
tatus	Software				Action
Uninstalled	Use Proxies parents				✓ Instal



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

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



Parent Proxies rules

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

Antwork	Parent proxies This section define how your proxy will be chained to other proxies using ACLs methods	
# Your proxy		
ACLs Proxy	+ New Rule a Apply rules	
Rarents Proxies	New Rule	×
🔁 Status		
Parameters	Rule	
≣ Rules	NewDele	
≫ Web-Filtering	New Kule	
Nour categories	Parent proxies rule	
Logs center	Rule Name: Send to router	
Databases	Enabled: ON	
	Never direct.	
	Order: - 1 +	
	« add »	

Select you created rule

# Dashboard	Parent proxies
E Your system	This section define how your proxy will be chained to other proxies using ACLs methods
👬 Network	+ New Rule Raphy rules
SDNS	
# Your proxy	Rule Name
ACLs Proxy	👔 🔽 « Send to router: » For objects All. Inactive rule
Parents Proxies	
𝔅 Web-Filtering	
Your externise	

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



еw ргоху		
New proxy		
HTTP Proxy features:		
hostname:	192.168.1.1	
listen port:	- 3128	+
tls:	OFF	
proxy-only:	OFF	
Weight:	OFF	
value Weight:	- 1	+

You parent proxy is now affected to your rule.

Rule Parer	nt proxies	Objects		
+ New proxy			Search	۹.
Hostname				
192.168.1.1:3128				0

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

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

+ New Rul	Apply rules			
		Search	٩	*
	Rule Name			
6	« Send to router: » For objects All. Then use parent proxies 192.168.1.1:3128	And force the use of a parent proxy for all requests (include SSL)	↑↓	C

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



-∿- / ?≣	Sea	rch a computer, uests ④ Rec	a member	Network ma	nitor © 1	7:23:00 🛛 🌒 Cpu: 7.6% Me	em:28% 영상 Members	醫 Admin Guide	ڻ [Log out
	Rea	ltime re	ques	ts						
	50 event	S							G	o!
	Date	Members		Protocol	Category	url	INFO/LINK	Detinations	Size	Duratic
	17:27:34	192.168.30.47	SSL Connect - Pass	SSL	(0) Unknown(0)	https://www.safesquid.com	Q 2	192.168.1.1:3128	366.69 KB	18.69s
	17:27:34	192.168.30.47	SSL Connect - Pass	SSL	(0) Unknown(0)	https://livehelp.safesquid.co	om Q 2	192.168.1.1:3128	36.83 KB	17.22s
			001							



WAN PROXY COMPRESSOR

What it is?

Wan Proxy compressor is designed for companies that use remote offices or using a dedicated cloud. The feature is designed to compress TCP protocol in order to increase the bandwidth.

The Wan Proxy compressor must use at least 2 Artica servers.



- 1. The first one act as Parent proxy, it is designed to fetch Internet content and compress it.
- 2. The second is designed to fetch compressed content from the parent proxy, decompress the protocol



Inside each box the local proxy and the Wan proxy exchange the compressed protocol and is able to cache content.



Wan Proxy parent mode.

You needs first to install the proxy service through the Features section

- After installing the proxy service, in the Features section, type "Wan" in the search field.
- Click on the Install button on the Wan Proxy Compressor row.

Insta This section	all or uninstall features on allows you to install/uninstall available features on your se	rver
select -	Expand Mizards	wan 🗶 🗸
Status	Software	Action
Uninstalled	Wan Proxy compressor	✓ İnstall

- On the left menu, click on "TCP Compressor" / Status
- You will see the status in red mode, this is normal the Wan Proxy compressor must be setup.
- Switch to Wan Compressor parent mode.
- Set the listen port that the Wan Compressor client must use
- Define the listen Interface to force the service to bind (mandatory!!!)
- Select the Listen port of your HTTP proxy service in order to let the Wan Proxy compressor to fetch pages.
- Click on **Apply** button.

Manager	E Search a computer, a member	- √- Active Requests	③ 16:45:33 원 Members	🖪 Admin Guide 📮 🕛 L	og out /Ξ
Administrator 👻					
🔡 Dashboard	Wan Proxy compresso	r »» Service statu	S		
🚍 Your system	WANProxy a TCP proxy which makes TCP connection what you need to improve performance over satellite,	is send less data, which improves TCP per wireless and WAN links	formance and throughput over loss	y links, slow links and long links. Th	is is just
A Network					
EDNS		Parameters			
# Your proxy		Mode:	Not defined		¥
STCP Compressor	Wan Proxy compressor	Listen port-	- 8088	I	+
🙆 Status	Stopped	Listen port			
Events	C Restart	Listen interface:	All interfaces		Y
Se Databases		Wan compressor pare	ent		
🔓 Logs center					
		The Proxy compressor i service in order to comp	n parent mode is able to forward To press data	P traffic to the defined real proxy	
		Proxy port:	3128: Main port: Main connecte	d port 0.0.0.3128 - 0.0.0.0:31	v

After Apply, the status must be switched to "green"



Wan Proxy client mode.

You needs first to install the proxy service through the Features section

- After installing the proxy service, in the Features section, type "Wan" in the search field.
- Click on the Install button on the Wan Proxy Compressor row.

Insta This section	all or un allows you to	nstall features	server	
select -	Expand	A Wizards	wan	X -
Status	Software			Action
Uninstalled	Wan Proxy	compressor		✓ Install

- On the left menu, click on "TCP Compressor" / Status
- You will see the status in red mode, this is normal the Wan Proxy compressor must be setup.
- Switch to Wan Compressor Client mode.
- Set the listen port that the local Proxy will use as Compressor client must use
- Select the address and the listen port of the remote WanProxy act as Parent
- Click on Apply button.

	Deremeters			
	Parameters	>		
		Mode:	Wan Compressor Client	selec
Wan Proxy compressor	Wan Comr	pressor Client		
since 59mn 13s	Wan Com	Jessor Cheft		
Memory used: 10.97 MB	The Proxy	compressor in client	de is able to send TCP traffic to a Proxy Compress	sor client.
	In this mod	de, the proxy service use	be local Proxy compressor client to send reques	ts through Internet.
C Restart				
C Restart		Listen Port:	- 8088	
C Restart	1	Listen Port: Remote Address:	- 8088 192.168.1.41	
€ Restart		Listen Port: Remote Address: Remote Port:	- 8088 192.168.1.41 - 8088	
∂ Restart	[Listen Port: Remote Address: Remote Port: User Name:	 8088 192.168.1.41 8088 User name 	

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

200 50 ev	ents								Go!
					1				
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	Q 2	216.58.205.10:443	4.99 KB	4mn
17:30:58	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net		179.00.192.7:443	3.14 KB	0.155
17:30:58	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net	۵ 🖻	179.60.192.7:443	3.15 KB	0.18s
17:30:58	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net	Q 2	179.60.192.7:443	3.14 KB	0.18s
17:30:58	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net	Q 2	179.60.192.7:443	3.15 KB	0.16s
17:30:57	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net	Q 🛛	179.60.192.7:443	3.15 KB	0.09s
17:30:57	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://scontent-cdg2-1.xx.fbcdn.net	Q 🛛	179.60.192.7:443	3.15 KB	0.09s
17:30:57	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	-	https://static.playmedia-cdn.net	Q 2	89.202.139.136:443	1.33 KB	3.1s
17:30:57	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	.)	https://static.playmedia-cdn.net	Q 2	89.202.139.136:443	2.18 KB	3.1s
17:30:57	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	-	https://static.playmedia-cdn.net	Q 2	89.202.139.136:443	2.47 KB	3.08s
17:30:55	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	Facebook	https://staticxx.facebook.com	Q 2	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	Q 🛛	216.58.209.234:80	82.14 KB	0.2s
17:30:55	192.168.30.47/dtouzeau	Not cached - Pass	GET	-	http://playtv.fr	Q 2	89.202.139.136:80	32.34 KB	0.1s
17:30:55	192.168.30.47/dtouzeau	SSL Connect - Pass	SSL	÷	https://static.playmedia-cdn.net	Q 2	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"

Manager	E Search a computer, a membei	⊕ Requests ① 19:11:18 🛢 Cp	u:13.4% Mem:38.5% 뿅 Members 👂 🖰 Log out 🗐									
Administrator +												
E Dashboard	Your proxy Categorization	Your proxy Categorization										
📑 Your system	This section allows you to enable websites categorization. Websites categorization allows you to get category according to a visited website.											
🚓 Network & NICs	Categories can be used to build proxy ACLs. You can use the Artica Cloud datecenters. And/Or use an installed Categories service in your network.	Categories can be used to build proxy ACLs. You can use the Antica Cloud descenters.										
Active Directory												
≣ DNS	Status Parameters Not categorized Users requests	Status Parameters Not categorized Users requests										
Hour proxy												
Authentication	Use the Artica Cloud category service;											
Nour categories	Use remote categories service;											
Categorization	Remote address: Remote address											
🖿 Statistics	Remote port: - 3978		+									
Logs center												
Databases			« Apply »									

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**"

11

Install or ur This section allows you to in	ninstall features	erver
select - Expand	Software	categories 🗶 🗸
Uninstalled	Personal categories	✓ Install
Uninstalled	Categories service	✓ Install

After installing the feature, the service is running using 0 database. On the left menu, choose "**Categories service**" and "**Global Settings**"

III Dashboard	Categories service: General settings
A Network & NICs	General settings
Active Directory	Threads: - 64 +
⊜ DNS ⊕ Your proxy	Artica Databases: 077 Free database: 077
Authentication	
Your categories	« Apply »
Categories service	
¢¢ Global Settings	
💩 Categories update	

You have to choose which databases you want to add into your category service:

- Artica database: 150 categories, 55.000.000 of categorized websites require 2.7GB of free memory (Available with a Corporate License)
- Free database: 58 categories, 3.000.000 categorized websites require 700 MB of free memory.

After enabling public databases, the status displays the number of categories used on your server.





Define the schedule for updating database.

Select the menu "Categories Update".

The status tab displays all databases downloaded from your server.

By default, Artica updates databases each day at 03:00 AM, you can change it inside the "Schedule" tab.

If you need to perform update now, click on the "Update button"

Manager Administrator –	∃ Sear	ch a computer, a r	nembei		Requests	() 14:21:20	Cpu:11.2% Mem:37.3%	왕 Members 🏮 🕛 Li			
Dashboard	Web	o-filterin	g database	S							
🚍 Your system	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.										
🚓 Network & NICs				1							
Active Directory	Status	Update set	tings Schedule	Update events							
S DNS	Delete (databases 🙆	Update								
# Your proxy								Search			
Authentication		Status	Category	Туре	Items	Size	Version	Updated On			
Your categories	Updated	۲	Abortion	Artica	6 258	28 KB	2018 Sunday October 28 15:52:	28 2018 Sunday October 2			
Categories service	Updated	<u>ه</u>	Advertising	Artica	159 511	716.18 KB	Yesterday 06:45:45	Yesterday 22:15:17			
6 Status	Updated	1	Agressive	Artica	25	0.31 KB	2018 Sunday October 28 15:52:	29 2018 Sunday October 2			
🖵 🗘	Updated	3	Akamai	Artica	7 217	15.18 KB	2018 Sunday October 28 15:52:	42 2018 Sunday October 2			
Categories update	Updated	<u>II</u> P	Alcohol	Artica	47 173	242.23 KB	2018 Sunday October 28 15:52:	31 2018 Sunday October 2			
@ Events	Updated	3	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

List Categories

In Your Categories / Categories, you can list all available categories (Officials categories provided by Artica and your categories)

Manager Administrator -	Search a computer, a member		-√- Active Requests	@Requests () 10:35:22	Cpu:1% Mem:55.3%	E Categorize 영	
## Dashboard	Your categories						
🗮 Your system	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.						
🚓 Network	+ New rategy + Restore backup - D Compile all ra	terrories					
S DNS							
Your proxy	Categories	1	Description		Size	Items	
ACLs Proxy	Abortion		websites about arguments in favor of or against abortion, descri obtaining or avoiding abortion.	ibe abortion procedures, offer help) in	0	
≫ Web-Filtering	Advertising		Advertisement.			0	
Your categories	Agressive		aggressive sites.			0	
\$ [®] Parameters	😚 Akamai		Akamai Technologies			0	
■Categories ■Categorization	Alcohol	N	Sites that provide information on, promote, or support the sale paraphernalia	of alcoholic beverages and associa	ted	0	
Web services	Amazonaws	hî	This category help identify SSL websites that using amazonaws It is not intended to use it as blacklist but for statistics purpose	service.		0	
🛢 Databases	æ Animals		Websites about animals (excluding pets)			0	
Bil ann anntar	Apple		Internet sites used by Apple Company			0	
Logs center	1 Arts		Websites about Arts, painting, collections, statues or sculptures	, galleries		0	
	Associations		Websites about non-profit organizations, Associations, clubs th categories	at cannot be categorized on other		0	
	M. Astrology		Websites about astrology,horoscope,astrologers			0	
	🧈 Astronomy		Sites of institutions as well as of amateurs about all topics of ast	ronomy		0	
	Nudio-video		audio and video sites.			0	
	1 Banking		Home page of banking companies are listed here. This is not res	tricted to online banking.		0	
	Bicycles		All about bicycles, accessories, repairs, and tools, associations/c and bicycle touring, mountain biking, BMX	lubs,Social and historical aspects,	sports	0	
	🛤 Bikes		All around motorcycles. Included are vendor sites, resellers, fan Scooters included	and hobby pages as well as and su	ppliers.	0	



List only your categories

If you wan to hide officials categories, on the left menu click on "Your categories/Parameters" on the left menu. • Turn on "**Hide officials categories in main list**"

- Click on Apply button •

Manager	Search a computer, a member	
Administrator -		
🗱 Dashboard	Your categories Parameters	
📑 Your system	Personal categories feature allows you to create your own web-filtering categories in order to moc	lify the web-filtering behavior or increase Web-
🚠 Network	Main parameters Schedule Events	
⊜ DNS	Hide officials categories in main list:	ON
# Your proxy	RESTEUL	
ACLs Proxy	DESTENIADD	OFF
≫ Web-Filtering	API Key:	5Swj33YkmrWxInxFLvUtMfJgVJapYYhl
Your categories	Allow creating new categories:	OFF
Parameters		
≡ Categories	Create a repository	
Categorization	Enable the feature:	OFF
• Web services	FTP server:	FTP server
🛢 Databases	Target directory:	Target directory
Logs center	FTP username:	FTP username
	FTP password:	FTP password
	interval:	4 Hours



Create your first category

After installing the Personal categories, on the left menu, choose "Your categories" and "Categories".

In this section, Artica lists all available categories.

When creating a new category, ensure its name will not the same in officials' categories.

If you want to remove officials' categories, go into "Your Categories" and parameters, enable the checkbox "Hide officials' categories in the main list."

A Network & NICs			
Active Directory	+ New category & Restore backup	Compile all categories The move all categories	
S DNS	Categories	Description	
(#) Your proxy	Cheater (Free Edition)	Sites which are designed to explains cheating on exams.	
Authentication	D-DOS (Free Edition)	n) Websites providing information about ddos attacks	
Your categories	Dating (Free Edition) Dating, matching site for single person		
🗘 Parameters	Dialers (Free Edition)	Websites providing information about dialers	
≡ Categories	Downloads (Free Edition)	Download manager	
Categorization	Strugs (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		
incon category		
Category name:	Category name	
Description:	Description	
Shared category:	OFF	
		add »

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

Your cat Personal categories filtering detection r	egories feature allows you to create.	eate your own web-filtering cat	egories in order to modify the	e web-filtering beh	avior or increase Web-
+ New category	🛓 Restore backup	Compile all categories	🗑 Remove all categories	acme	× -
Categories	De	scription	Size	Items	
acme_cat	En	terprise category		0	0

(F)

- 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 Items Sec	acme_cat >> Add websites	
K Search	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 ",+/	
No data SELECT sitename from category_acm	Force: OFF Disable extension checking: OFF 1 kollective.com 2 forum-dsi.com 3 normandiecyberscurite.com 4 netscure-day.fr 5 astan.org 9 belance.org 9 ingerg.er 10 3vil.org 11 compartilhandoti.com.br 12 eteckconsulting-mg.com 13 ajslejut.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.

Category: acm	e_cat	
acme_cat	Items Security	
Search		
+ Add websites	Legory	Remove all items
		Se
Web Sites		
1 kollective.co	m	
2 forum-dsi.co	m	
3 normandiecy	bersecurite.com	
4 netsecure-da	av.fr	
₩ Dashboard	Your categories Personal categories feature allows yo	u to create your own web-filtering categories in order to modify the web-filtering
🚓 Network & NICs	+ New category 🛓 Restore bad	ski p 🔒 Compile all categories 🧯 🗃 Remove all categories
Active Directory		
S DNS	Categories	Description
# Your proxy	Cheater (Free Edition)	Sites which are designed to explains cheating on exams.
Authentication	D-DOS (Free Edition)	Websites providing information about ddos attacks
Your categories	Dating (Free Edition)	Dating, matching site for single person
🗢 Parameters	Dialers (Free Edition)	Websites providing information about dialers
≡ Categories	Downloads (Free Edition)	Download manager



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.

S DNS	Mai	n parameters Sche	dule Events				
# Your proxy	Lat	abases com	pilation				
Authentication	This	vill save to disk selected categori	es to make them available in the Web-Filtering engine process.				
Sour categories	+ Ne	w task 🛛 🖬 Apply all sch	nedules				
Carameters				Search		Q	•
■ Categories ■ Categorization	ID	Task	Description		Run I	Enabled	Delete
Categories service	13	Databases compilation	each day at 0500 This task will save to disk selected categories to make them available in th Filtering engine process.	e Web-		0	0
Maintain Statistics							



Import/export items.

Import items

This feature allow you to import million of websites into a category container.

- Prepare a text file with websites separated by a carriage return (the text file (*.txt) can be also in gzip (*.gz) or zip (*.zip) file type)
- On your Categories section, click on the "Import" button

🚍 Your system	
👬 Network	Veux esterories
⊜ DNS	Personal categories feature allows you to create your own web-filtering categories in order to modify the web-filtering behavior or increase Web-filtering
# Your proxy	detection rate.
ACLs Proxy	+ New category 🛃 Restore backup 🖬 Compile all categories 🖀 Remove all categories
💸 Web-Filtering	Search Q -
Your categories	Categories Description Size Items
¢°Parameters ≕Categories	Notrack Enterprise My No track 0 Simport De Export + add
Categorization	7
• Web services	-

• Upload your file using the button "Upload a file"

Notrack Enterprise: Categorize (Bulk)	×
Import Web sites	
Category:Notrack Enterprise Force: 1	ᆂ Upload a File

• Artica will display the importation progress.

Notrack Enterprise: Categorize (Bulk)	×
Import Notrack Enterprise: 85% mkt9642.com 11954/14146 Import Notrack Enterprise - 85% mkt9642.com 11954/14146	
Import Web sites	
Category:Notrack Enterprise Force: 1	
	🔹 Upload a File

Export items

- On the table, click on the "Export" button.
- A confirmation message ask to you to confirm the export task

3		
Your cat	egories	
Personal categories detection rate.	s feature allows you to create your own web-filtering categories in orde	r to modify the web-filtering behavior or increase Web-filtering
+ New cate	(!)	gories Search Q +
Notrac	Are you sure ?	limport B. Export + add
	Execute this task: Export Notrack Enterprise ?	1
	Cancel Yes, execute it	
Copyright Artica Tech	© 2004-2019	v4.05.091000 Enterprise Edition

- Wait during the exportation task.
- After exportation complete, a new icon allow you to download the exported file.

Export:Notrack Enterprise	×			
Export: Notrack Enterprise				
Export Notrack Enterprise: 100% Compile rules: Notrack Enterprise Compressing Success L.76 <u>«Details»</u>				
249.gz (46.24 KB)				



Shared categories

Shared categories allow you to delegate the category to specific groups according to the local Administrators database or Active Directory Database. When editing a personal category, enable the "Shared category" option.

Category: produ	uctionlb		×
productionlb	Items secu	ity	
productionlb 0	Items		
production we	bsites		
	Category name:	productionlb	
	Table name:	category_productionlb	
	Description: Shared category:	on	
		« Apply »	

- Enable shared category allows you to add this category in the privilege section.
- Open the members section in order to browse groups
- Find the group of users you want to enable the category management.

E Search a computer, a	membei			_	
-√- Active Requests	uests (3) 12:05:15	Cpu:39.5% Mem:56.5%	E categorize *왐 Members	🕻 Admin Guide 🙎	() Log out i
My member	S				
Default					
proxy					Go!
	1			Search	۹ +
Display Name	Domain	EMail Address	Office Phone	Gro	ups
28 Dost IndateProxy	touzeau.biz	-	-	-	
왕 role_Proxy-Full	touzeau.biz	-	-	-	



On the group option, click on "Categories" tab.

Click on the checkbox in order to let member of this group managing the category.

role_Proxy-Full			×
role_Proxy-Full Members	Privileges Categories	Search	۹ .
Categories Description productionIb ma description2			

When an user of this group login on the Artica Web console.

bighttp.touzeau.local	dtouzeau
Welcome to the Artica Web Administration Interface. Please use your Manager account or any account defined	•••••••
by your Administrator	Login
	Artica 4.03.030900 © 2019

If the group have only the privilege to manage shared categories, the web interface displays only categories allowed to be edited.

E Search a computer, a member		📙 Admin Guide 🔱 Log out 🛛 🚝
bighttp.touzeau.loca	I	
Your categories		
Your categories Personal categories feature allows you to create	your own web-filtering categories in order to modify	y the web-filtering behavior or increase Web-filtering detection rate.
		Search Q -
Categories	Description	Size Items
oproductionIb	ma description2	2 -
	Search a computer, a member bighttp.touzeau.loca Your categories Your categories Personal categories feature allows you to create Categories productionlb	Search a computer, a member bighttp.touzeau.local Your categories Your categories Personal categories feature allows you to create your own web-filtering categories in order to modified Categories Description categories productionlb ma description2





Uncategorized websites

If your server act as Categories server for others Artica proxies, your server is able to store all websites that are uncategorized. To define an uncategorized website, your category server requests the categories on Artica Cloud (if enabled), on the second categories server and on your categories service.

- On the left menu, click on "Your categories" and "Categorization".
- Select the "Not categorized" tab
- You will see the list of uncategorized websites and you are able to categorize it.

## Dashboard	Your proxy (Categorizatio	n		
Your system	This section allows you to en Websites categorization allo	able websites categorization. ws you to get category accordi	ng to a visited website.		
🚓 Network & NICs	Categories can be used to bu You can use the Artica Cloud And/Or use an installed Cate	ild proxy ACLs. datacenters. gories service in your network			
S DNS			_		
(a) Your Firewall	Status Parameter	Not categorized	Jsers requests		
🖶 Fail To Ban	t] Analyze				
Your categories				Search	۹ -
C Parameters	Date	Domains			Hits
≡ Categories	004014 - 4 - 0 - 4 - 00	1.6.1			
Categorization	2018 Monday October 29	massivenctions.com			1
	2018 Monday October 29	1f300.com			1
Categories service	2018 Monday October 29	sendinblue.fr			1
Les Statistics	2018 Monday October 29	verified-reviews.com			1
Logs center	2018 Monday October 29	sendibm3.com			1
	2018 Monday October 29	sendibt1.com			1

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



Testing categories

If you are using passive mode or active mode, you can query a category from a website. Click on the button on the top-right webpage (near the "Log out") On this right menu, choose "**Your Proxy**" and "**Test categories.**"

A new form is displayed

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

Noarch a computer a member	BAB MOGULOSTS	THE PROPERTY AND	THE DUPS OF LOCODELS MY	ixi Mompore	-
Test categories					×
www.tf1.fr			s	Search a category	
≝ www.tf1.fr	•				
Category:Web TV					
Collection of site offering TV streams via world wide web					
2766): www.tf1.fr					
www.tf1.fr: Limited_categorize>					
SOI ite: www.tf1.fr = No.results					_

	Other bookmarks
16.5%	왕 Members 🔮 () Log out 泪
	Action
	Help & Support
	Video tutorials Go
	🙃 🕅 🙃
	Support package Go
	Your proxy
	Services operations Go
	Test categories Go
_	System

()

MONITORING AND STATISTICS

Realtime access logs format

The proxy write events in the /var/log/squid/access.log

A typical line is :

```
1569139273.003 33 192.168.1.191 TCP_MISS/200 883 GET
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSnR4FoxLLkI7vkvsUIFlZt%2BlGH3gQUWsS5eyoKo6XqcQPAYPkt9mV1
DlgCEAsfjNWeZHRr6uFT7MohBms%3D Jhon HIER_DIRECT/93.184.220.29:80 application/ocsp-response
mac="00:0c:29:e3:a1:9c" category:%20136%0D%0Aclog:%20cinfo:136-SSL_certificates;%0D%0A ua="Microsoft-
CryptoAPI/6.1"
```

Information is formatted in this way:

- 1569139273.003 : Seconds since epoch with subsecond time (milliseconds)
- 33: Response time (milliseconds)
- 192.168.1.191: Client IP address
- TCP_MISS/200: Proxy request status / HTTP status code sent to the client
- 883: Total size (bytes) of reply sent to client
- GET: Request method (GET/POST etc)
- http://ocsp.digicert.com/....: Request URL received (or computed) and sanitized
- Jhon : User name (any available); if no user "-" is added
- HIER_DIRECT/93.184.220.29:80: Proxy Hierarchy and remote address used to fetch data
- application/ocsp-response: Content-Type of data sent by the next hope
- mac="00:0c:29:e3:a1:9c": Mac address of the client.

category:%20136%0D%0Aclog:%20cinfo:136-SSL_certificates;%0D%0A

Extra information sent by Artica plugins. replace **%20** by space and **%0D%0A** by carriage return

```
category: 136
clog:
cinfo:136-SSL_certificates;
```

Means Website **Category ID = 136**, information retrieved in cinfo that give the category name Clog is extra log when Artica plugins

ua="Microsoft-CryptoAPI/6.1"

If the option Log User Agent is enabled, the User Agent string is written inside cotes



Logging to Internal networks are disabled

It make sense to not log requests to the internal network, in my cases internal web applications make many requests, use only IP addresses and are in a productive topic.

By default, proxy did not log requests to internal web servers inside private network All requests to, 172.16.0.0/12, 192.168.0.0/16 are not logged by the proxy.

Enable logging to internal networks:

- Under Your Proxy, choose Global settings
- Click on General settings tab
- Under Events section, turn on Log requests to Internal networks.

EDNS	General setting	Derformance	TimeOute	Limite	Active Directory	DNS settion	Remote ports	Cloud Mode
Cour proxy	General settings	Fertormance	TimeOuts	Linits	Active Directory	Divis securitys	Remote ports	Cloud Mode
🕰 Status	Identity							
✿ Global settings	<u>۱</u>	Visible	Hostname:	hacluster1 touz	reau biz			
♥ Categories Service	-							
₩ICAP Center		Unique	Hostname:	Unique hostnar	ne			
Authentication		Proxy Administr	ator Email:	david@articate	ch.com			
Errors pages				055				
Proxy events	Dis	play Server Name A	nd Version:	OFF				
⊮ Listen ports	Events							
SSL Protocol								
Global rules	Include HTTP U	ser-Agents In Real-ti	me Events:	OFF				
Proxy tasks	Log	Requests To Internal	Networks:	OFF				



SNMP service dedicated for the proxy

You can connect your SNMP console by enabling some parameters.

📰 Dashboard						
🚍 Your system	Listen ports					
🚓 Network	This section allows you to define how browsers c The frist one Connected ports list ports used dire	can be connected to your proxy. irectly in browsers settings.				
€ DNS	Connected ports are able to authenticate users to The second one Transparent ports allow the prov	through LDAP or Active Directory. oxy to act as the main gateway and is able to catch both HTTP/HTTPS requests witho				
# Your proxy	browsers settings. Important: Transparent ports cannot authenticate users.					
🚳 Status 🖑						
✿ Global settings	Connected ports Transparent ports	Remote ports Communication ports				
₩ ICAP Center	Communication ports					
Authentication						
Errors pages	ICP Port:	– 0				
Proxy events	11700	- 0				
🖌 Listen ports	HICP port:	- 0				
SSL Protocol	LIDP Protocol					
Global rules	0011100001					

- On the left menu, choose "Your Proxy" / "Listen Ports"
- Select Communication ports.
- Down to Monitor Proxy service (SNMP)
- Define the IP address of your remote server that is able to query the Artica Proxy.

mpwalk -v 2c -c public 192.168.1.56:3401	1.3.6.1.4.1.3495.1	
Listen port (SNMPv2c):	- 3401	+
SNMP Community:	public	
Remote SNMP console IP address:	192.168.1.1	٥
	R	

Check the SNMP availability by using this command line

snmpwalk -v 2c -c public 192.168.1.56:3401 .1.3.6.1.4.1.3495.1

If the SNMP tool answer "No Response from", you should reboot the $\ensuremath{\mathsf{Artica}}$ server



Merge SNMP proxy inside the SNMP service.

If you have installed the SNMP service in artica features, the SNMP service can merge data from the proxy SNMP in order to use only one port. On Your System / SNMPv3, enable the check box "Monitor Proxy service (SNMP) option.

ting Dashboard ■ Your system	Monitor your system: St SNMP service is an SNMP agent which binds to a port an Upon receiving a request, it processes the request(s), cold	NMP v5.7.3 d awaits requests from SNMP management software. lects the requested information and/or performs the requested operati	on(s) and returns the information to the sender.
System information			
📾 Your hard disks	SNMP daemon Restarting service: 100% Starting service Success eff	Details>	
Memory swapping		SNMP daemon R	estarting service - 100% Starting service Success
	Status/Parameters Events		
>_ OpenSSH server			
Glances		Parameters	
O Tasks	l 🗍	Monitor Proxy service (SNMP):	ON .
Certificates Center	SNMP daemon	Listen interface:	All interfaces
SNMPv3	Running	1 internet	141
ы васкир	since 9s	Listen port:	101
License	Memory used. 5.55 Mb	SNMP Community (SNMPv2c):	public
Opdate Opdate Opdate	<i>€</i> Restart	Remote SNMP console IP address (SNMPv2c):	192.168.1.196
i Versions		Organization:	Artica tech
Internet access		System contact:	david@articatech.com
亲 Support		licer name:	l Icor namo
A Network	Linux transp 4.19.0-5-amd64#1 SMP Debian 4.19.37-5+deb10u2 (2019-08-08) v86 64	Password:	Password
SDNS			Password (Confirm)
Your proxy	Jaccess		

• If you use LibreNMS, go to your device, choose "Applications" and turn ON the Squid checkbox option.

← → ♂ ŵ ±	⊥ III\ III ❷ ③ 192.168.1.196/device/device=2/tab=edit/se	ection=apps/ 🛛 🔊 😁 🗠 📩 📑 🗝
CibreNMS & Overview E Devices	Services 🗞 Ports 😍 Health 🚯 Alerts	🛓 💿 🔅 🛛 Global Search
192.168.1.56		Storage Usage Memory Usage Processor Usage
🖓 Overview 🕍 Graphs 😻 Heal <mark>m 😽 Ports 💓 1994</mark>	smory 📽 Services 📕 Logs 🕒 Alerts 📊 Alert Stats 🛃 Performance	ce 🗟 Notes
Device Settings SNMP Port Settings Applications	Ale t Settings Alert Rules Modules Services IPMI Storage Proces	ssors Memory Misc Components
Applications		
OFF Apache	OFF Asterisk	OFF BIND
OFF Ceph	OFF DHCP Stats	OFF Drbd
OFF Random entropy	OFF EXIM Stats	OFF Fail2ban
OFF FreeBSD NFS Client	OFF FreeBSD NFS Server	OFF FreeRADIUS
OFF Freeswitch	OFF GPSD	OFF Mailscanner
OFF Mdadm	OFF Memcached	OFF MySQL
OFF NFS Server	OFF NFS Stats	OFF NFS v3 Stats
OFF Nginx	OFF NTP Client	OFF NTP Server
OFF Nvidia	OFF Open Grid Scheduler	OFF OS Updates
OFF PHP-FPM	OFF pi-hole	OFF Portactivity
OFF Postfix	OFF Postgres	OFF PowerDNS dnsdist
OFF PowerDNS Recursor	OFF PowerP .S	OFF Proxmox
OFF Rrdcached	OFF ST S info	OFF Shoutcast
OFF SMART	ом Squid	OFF Tinydns
OFF Unbound	OFF UPS apcups	OFF UPS nut
OFF ZFS		

Artica Proxy statistics

Artica allows you to display many statistics in order to see when, where, how your users use the bandwitch and the Webs.

Centralized Statistics

You can dedicate a central server that able to receive events from several Artica servers.

Logs will be merged and centralized to an unique Web Interface.

PDF Reports

You can schedule PDF reports that can be sent by eMail to a list of recipients:

- Daily report
- Yesterday report
- Current week report •
- Last week report .
- Monthly report •
- Last month report

Dedicated statistics privileges

You can create specific privileges from Artica local database, LDAP or Active Directory that allows some users to access to proxy statistics.

Statistics by categories

With Artica categorization method statistics can be extracted by topic like Press, pets, society, press, cars, animals...

What, Where, When, who?

With the query on statistics you will be able to extract graphs, charts, tables of who is using what and when it using some...

The Statistics feature is available with an Artica Enterprise Edition License

<u>here</u>:

Statistics Feature Documentation







Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com

192.168.8.85



Scheduled reports with Proxy Statistics Generator

This feature is designed to parse native access log format of the proxy service and generate general statistics about hits, bytes, users, networks, top url,top second level domain and denied URLs.

Statistic reports are oriented to user and bandwidth control, [b]this is not a pure cache statistics generator.

It use flat files to store data. This feature is limited according it can took several hours to parse a log file more than 1GB of data..

Install the Proxy Statistics Generator

- On the left menu, go to "Your System/Version"
- On the search field, type "Proxy Statistics generator"
- If you did not see a version, this means the software doesn't exists on the system.
- Click on Install or upgrade button.

Artica Core server	Operating system	Python packages		-
			Proxy statistics generator	X -
Software	Version			
Proxy statistics generator	:	🛓 Inst	all or update	

• Choose the latest version and click on Install or Upgrade button.

Proxy statistics generator	×
Proxy statistics generator 6.6 123.68 KB	L install or Upgrade

• You should see the version in the Proxy statistics generator row.

Versions System version and softw	vares versions			
Artica Core server	Operatingsystem	Python packages	gene	× -
Software Proxy statistics generator	Version : 6.6	🛓 İnstall	l or update	

Artica v4.x : http://articatech.net | contact: contact@articatech.com | support: http://bugs.articatech.com



Enable the Proxy Statistics Generator feature.

- Once installed, go into "Your System" and "Features" left menu section. •
- On the search file, type "proxy statistics"
- Clic on Install button on the "Proxy statistics generator" row.

Insta This section	all or uninstall feature on allows you to install/uninstall available feature	es s on your server	
select 🕶	Expand <u>A</u> Wizards		
		proxy statistics 🗙	•
Status	Software	Action	
Installed	Proxy statistics generator	✓ uninst	tall

- ٠
- On the left menu click on "**Statistics**" and "Proxy statistics generator" Wait few minutes and click on "**Build statistics**" to have your first report available.
- On the top menu click on "Statistics" in order to display reports.

Proxy statistics are automaticaly generated each day after 00:00:00

The main section display the disk usage of report..

Manager	Search a computer, a member ✓ Active Requests
Administrator 🗸	
Dashboard	Proxy statistics generator v.6.6
■Your system	This feature is designed to parse native access log format of the proxy service and generate general statistics about hits, bytes, users, net will keep to be a second level domain and denied URLs. Statistic reports are oriented to user and bandwidth control, this is not a pure cache statistics generator. It use flat files to store data.
A Network	This feature is limited according it can took several hours to parse a log file more than 1GB of data
SDNS	Directory size 63.43 MB Statistics generation are scheduled every day after 00:00:00
(≜) Your Firewall	DIR 63.43 MB
# Your proxy	Used 23.71 CB
● WAF and ACLs	
€ Caching	
Nour categories	
🖿 Statistics	
generator	Partition 85.38 C8
Statistics extractor	

Page: 234



Generated reports allows you to display bandwidth usage per domain, users, number of hits and downloaded size. A calendar allows you to display specific reports per week or day.



MAINTENANCE

Update the proxy software

Proxy software is not automatically updated, periodically, we suggest to perform this operation in order to upgrade the proxy software .

On "Your System", select "Versions"

Click on the button "Update Index Softwares" in order to get latest available versions.

Manager Administrator ~	E Search messages ■Cpu:5.8% Mem:53.5%/3.83 GB 小 Active	Requests @Requests ①12:
Dashboard Your system	⊕Logout ﷺ	
System information Output Vour hard disks Vour system memory	Versions System version and software versions	
 Memory swapping Watchdog System events 	Artica Core server Operating	rsystem Python packages
 ♦ Features >_ OpenSSH server I Glances T to be 	Software	Version
Certificates Center	Artica Core server: Operating system:	4.29.051202 Debian 9.8 Gnu-linux
₽ License ③ Update	Kernel version: PHP Version:	#1 SMP Debian 4.9.144-3.1 (2019-02 7.0.33-0+deb9u1
i Versions	System Memcache engine:	1.5.16
Support	System Firmwares:	20180227

- On the search field, type "**Proxy service**"
- The table displays the current version of your proxy software.
- Click on "Install or Upgrade" button on the right column.

E Search messages	Active Requests		12:28:27	Categorize	🖹 Admin Guide
ŮLogout 淫					
Versions System version and softwares ver	rsions			,	
C Update Index Softwares	i Refresh Syster	n Information	proxy service	/	× -
Software Vesion Proxy services					
Proxy service: 4.6		🛓 Install Or U	pdate		



Select the most updated software and click on "Install or Upgrade" to let Artica downloading the package and install it.



Restart the proxy periodically

If you need to restart the proxy periodically in order to refresh it's memory, threads; on the left menu, choose "Your Proxy" and "Proxy tasks" Click on the button "New task"

Network	Pr	oxy tasks					
(A) Your Firewall	+ Ne	ew task 🖬 Apply all schedules					
# Your proxy				Search		٩	-
🙆 Status	ID	Task	Description		Run	Enabled	Delete
✿ Global settings	8	Daily Statistics analytics	each day at 23:59 This task execute daily SARG statistic	s	4	~	
Authentication	9	Reload Web-Filtering service	each day at 03:30 Reload Web-Filtering service		4	~	
 Errors pages Proxy events 	10	Local statistics	each 5 minutes This task run bandwidth, websites loc	al statistics	4	~	
♥ Categories Service ♥ ICAP Center	11	Clean databases	each day at 04:30 Remove old data in tables according s peform database indexing	ettings and	4	~	
♥ Statistics service ■ SSL Protocol ■ Global rules	13	Update the main Webfilter databases	Check update each 3H Check on Internet if there is new Web databases and update the local contai An update is about 150Mb size.	ofilter iner.	쉬	~	
• Proxy tasks	14	Databases compilation	each day at 03:00 This task will save to disk selected cat make them available in the Web-Filter	egories to	4	~	T

On the new schedule form, choose the task [4] Restart Proxy service. Set the description and define the schedule (in our example, we restart the proxy each day at 06:00 AM) Click on Add button.

Set the schedule		N	
	Task Type:	[4] Restart proxy service	
	Description:	Restart the proxy each day at 6:00 AM	
	Schedule:	Every day at 06 : 00	

• Click on the Apply all schedules button on the main table to make your schedules in production mode.

E Tour system							
ANetwork Proxy tasks							
€ DNS	PI	UXY LASKS					
(▲) Your Firewall	+ Ne	ew task 🕞 Apply all schedules					
# Your proxy]	Search		۹	•
🙆 Status	ID	Task	Description		Run	Enabled	Delete
🛱 Global settings	8	Daily Statistics analytics	each day at 23:59		4	~	
🖌 Listen ports			This task execute daily SARG statistic	S			
Authentication	9	Reload Web-Filtering service	each day at 03:30 Reload Web-Filtering service		¢	~	
Errors pages			aach E minutac				
Proxy events	10	Local statistics	This task run bandwidth, websites loc	al statistics	ŝ	~	
♥ Categories Service			each dav at 04:30				



Your proxy

Status

Clobal settings

Authentication

UCAP Center

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"

Apply

C-ICAP Antivirus - REMOTE - RESPONSE

C-ICAP Antivirus - REMOTE - REQUEST

Kaspersky Antivirus - LOCAL - REQUEST

Kaspersky Antivirus - LOCAL - RESPONSE

ICAP Center This section allows you to connect s

+ New service

Status

Disabled

Disabled 0

Disabled 0

Disabled 0

Disabled 0

0

0

- A table is displayed and show you a list of pre-defined ICAP services examples. The "Bypass" column allows the prox
- If enabled, then the proxy can bypas If disabled, then the proxy sends an

n bypass the ICAP service. ends an error page and stop processing request	ts.		laneu.			
er o connect services around your proxy server using the ICAP proto	col such as antiviru:	s, web filtering				
ylqc			Search		٩	•
Daemon Name	Address	Mode	Bypass	Move	Enabled	Delete
C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmod_precac	he 🗸	↑↓		-
C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precach	e	↑ ↓		_

1

Υ

1

↑ ↓

10.20.0.2:1345 respmod_precache

10.20.0.2:1345 reqmod_precache

127.0.0.1:1344 reqmod_precache

127.0.0.1:1344 respmod_precache

Page: 238



Example: Connect to the Kaspersky Web traffic Security ICAP server

- ✓ On the Kaspersky Web traffic Security console, open the "Settings/ICAP server" menu.
- ✓ Ensure the ICAP server Address listen the 0.0.0.0 (means all IP addresses of the server)
- Take a look at the listen port (1344 by default), the path to request modification and the path to response modification service

A	Settings		
Kaspersky Web Traffic Security	Protection	ICAP server address	0.0.0.0 💙 : 134
📧 Dashboard	External services	Maximum connections over the	5000
용 Events	Database update	ICAP protocol	The valid range is from 1000 up to 10000 inclusive
I Rules	Licensing	Header with the client IP	X-Client-IP
Workspaces	Proxy server connection	address	
Servers	LDAP server connection	Header containing user name:	A-Client-Username
Settings	Templates for access denied pages		Enable this option, if proxy server sends user names in Base64 encoding
	Events	Path to request modification service	av/reqmod
	Syslog	Path to response modification service	av/respmod
	ICAP server	Start to transfer HTTP messages before their scanning is	Disabled
	SNMP	complete	Downloading of the banned object will be aborted without describing a reason: neither a Deny page nor a Redirect page will be displayed
	Single Sign-On login	Skip the HTTP CONNECT method check	Enabled
	Configuration settings		If you choose skipping the HTTP CONNECT method check, the traffic redirect and access deny templates will be disabled
	Administrator with superuser privileges		
<u>، محمد محمد المحمد r/></u>		Save Cancel	Set default values

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

ICAI This section	P Cen	ter u to connect services around your proxy server using the ICAP proto	ocol such as antivirus	s, web filtering				
+ New se	rvice 🖬	Apply		S	Search		٩	•
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	10.20.0.2:1344	reqmod_precache		^ ↓		-
Disabled	0	Kaspersky Antivirus - REMOTE - RESPONSE	10.20.0.2:1344	respmod_precache		^ ↓		-
Disabled	0	Offeo Web filtering - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precacie		÷ψ		
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		↑↓		-

Artica V4 Documentation – david@articatech.com



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

Daemon name:	Kaspersky Antivirus - REMOTE - RESPONSE	
Enabled:	ON	
Order:	– 0	+
Address	192.168.1.54	\$
listen port:	- 1344	+
ICAP Service name:	av/respmod	
type:	RESPMOD	Ŧ
If overloaded:	Bypass	•
X-Next-Services:	ON	
Bypass:	OFF	
Max connections:	- 100	+

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

ICAP This section	Cent allows you t + New s	connect services around your proxy server using the ICAP pro	tocol such as antivirus	web filtering				
					Search		Q	•
Status	Order	Daemon Name	Address	Mode	Bypass	move	Enabled	Delete
Disabled	0	C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmod_preca	che 🗸	↑ ↓		-
Disabled	0	C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precac	he	↑ ↓		-
Disabled	0	C-ICAP Antivirus - REMOTE - RESPONSE	10.20.0.2:1345	respmod_preca	che	↑↓		-
Disabled	0	C-ICAP Antivirus - REMOTE - REQUEST	10.20.0.2:1345	reqmod_precacl	he	^ ↓		-
Disabled	0	Kaspersky Antivirus - LOCAL - REQUEST	127.0.0.1:1344	reqmod_precacl	he	↑ ↓		-
Disabled	0	Kaspersky Antivirus - LOCAL - RESPONSE	127.0.0.1:1344	respmod_preca	che	↑ ψ		K
Disabled	0	Kaspersky Antivirus - REMOTE - REQUEST	192.168.1.54:1344	reqmod_precacl	he	↑ ↓	~	-
Disabled	0	Kaspersky Antivirus - REMOTE - RESPONSE	192.168.1.54:1344	respmod_preca	che	↑↓	~	
Disabled	0	Olfeo Web filtering - REMOTE - REQUEST	10.20.0.2:1344	reqmod_precacl	he	Λ Ψ		•_

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

ICAI This section	P Cen	ter to connect services around your proxy server using the ICAP	protocol such as antivi	rus, web filtering.				
C Refres	h + New Order	Daemon Name	Address	Mode	Search Bypass	move	Q	• Delete
Active	1	Kaspersky Antivirus - REMOTE - RESPONSE	192.168.1.54:1344	respmod_preca	che 🗸	↑ ↓	~	-
Active	2	Kaspersky Antivirus - REMOTE - REQUEST	192.168.1.54:1344	reqmod_precac	he 🗸	↑↓	~	-
Disabled	3	C-ICAP Antivirus - LOCAL - RESPONSE	127.0.0.1:1345	respmod_preca	che 🗸	↑ ↓		-
Disabled	4	C-ICAP Antivirus - LOCAL - REQUEST	127.0.0.1:1345	reqmod_precac	he	↑↓		-
Disabled	5	C-ICAP Antivirus - REMOTE - RESPONSE	10.20.0.2:1345	respmod_preca	che	↑ ↓		-



ICAP ANTIMALWARE/ANTI-PHISHING SERVICE

Kaspersky For Proxy server

Kaspersky Anti-Virus 5.5 for Proxy Server provides anti-virus protection for network traffic routed through proxy servers which support the Internet Content Adaptation Protocol (ICAP).

The program allows:

- **Perform anti-virus scans on objects transferred through the proxy server**. Kaspersky Anti-Virus does not scan the data transferred via HTTPS.
- Cure infected objects, or block access to infected objects if disinfection fails.
- Use group settings to define filtration parameters that are applied depending on the address of the user requesting an object, and the object's address (URL).
- Log activity statistics, including information about anti-virus scanning and its results, and application errors and warnings.
- Notify administrators about detection of malicious software.
- Update the anti-virus databases.

By default the application uses Kaspersky Lab's update servers as the source of updates.

But it can be configured to update the databases from a local directory; The anti-virus databases are used in the detection and disinfection of infected objects.

The application uses database records to analyze every object, checking it for virus presence: its content is compared with code typical for specific viruses.

Please be aware that new viruses appear every day, and therefore you are advised to maintain the anti-virus databases in an up-to-date state.

New updates are available hourly on Kaspersky Lab's update servers.

THE PROXY PAC SERVICE

A **P**roxy **A**uto-**C**onfig (PAC) file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.

A PAC file contains a JavaScript function "FindProxyForURL(url, host)". This function returns a string with one or more access method specifications. These specifications cause the user agent to use a particular proxy server or to connect directly.

Multiple specifications provide a fall-back when a proxy fails to respond. The browser fetches this PAC file before requesting other URLs. The URL of the PAC file is either configured manually or determined automatically by the **Web Proxy Autodiscovery Protocol**.

Artica is able to provide and generates on-the-fly a proxy.pac file for your Network.

It extends the native proxy.pac feature by providing multiple configuration scripts based on the source IP address, the proxy itself and the User- Agent string

Download the documentation here:

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



Page: 241



THE REMOTE DESKTOP SERVICE PROXY (RDP)

The RDS Proxy is designed to secure and forward remote desktop connections using RDP protocol or VNC protocol. It should be called RDS gateway or RDP proxy

It can be used to let Internet users to connect using TSE client to a datacenter from Internet or let administrators from the LAN to be connected to a pool of RDP services.

This service offer several features :

- Centralize and log each connection
- Automatically ban addresses against dictionnary attacks.
- Define schedules to access to a pool of server.
- Hide real TSE services credentials and addresses



UPDATE THE RDS PROXY SERVICE

FROM INTERNET.

If the RDS Proxy is not installed or you want to update it, on the left menu go to "**Your** system" and "**Version**"

On the Search field, type "RDS"

Click on Install or update button. Choose the latest version and click on "Install or Upgrade"

Versi System versi	ONS on and softwares versions		
		rds	× -
Software	Version		
RDS Proxy:	-	🛓 Instali or update	
	RDS Proxy		×
Copyright A	RDS Proxy 7.0.9 8.39 MB	/	🛓 Instali or Upgrade

11 Dashboard	
🗮 Your system	
📾 Your hard disks	
Amory swapping	
System events	
₩ Features	
>_ OpenSSH server	
Glances	
🕚 Tasks	
Certificates Center	
P License	
Update	
🗖 Web Console	
i Versions	
Internet access	

Versions

System version and softwares versions

Artica Core serv	ver Operating	rsystem
Software		Version
	Artica Core server:	4.05.040101
	Operating system:	Debian 9.5 Gnu
	Kernel version:	#1 SMP Debiar
	PHP Version:	7.0.30-0+deb9
System		
	Memcache engine:	1.4.33
	System Firmwares	20180227



INSTALL THE RDS PROXY SERVICE.

The RDP proxy service can be installed from the features section.

- On the search field, type "**rds**".
- Click on "Install" button on the "**RDS Proxy**" row

Install or uninstall features

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

select +	Expand & Wizards	rdp 🗶 🛩	
Status	Software	Action	
	Wordpress websites	A Not installed	
Uninstalled	RDP Proxy	✓ Install	



SETUP THE MAIN SERVICE

On the left menu, choose RDS Proxy/Status

45		Parameters			
20.0					
JS Proxy	•	Listen interface:	All interfaces		
😰 Status	RDS Proxy	listen port:	- 3389	<u>ا</u>	4
atistics	KUNNING since 18mn 23s	Encryption level:	low Default		
ਨ center	Memory used: 18.8 MB				
tabases	📿 Restart	Disconnect after (Seconds):	- 900		
				« Apply	ly »
	RDS Proxy authenticator				
	Running				

The left section displays the status of the main proxy and the Authenticator service that will able to manage RDP sessions.

On the right side you can tune parameters of the main service:

- Listen Interface: which Interface to listen the RDP protocol.
- Listen Port: which port to use (default is 3389)
- **Encryption Level**: the level of encryption between the client and the proxy.
- Disconnect after: if there is no activity on the TS Session, then the proxy will automatically disconnect the session.

SETUP POLICIES

To setup connections you need to create groups.

A Group associates:

- 1) Users: members with internal proxy credentials to allowed to be connected to the proxy service.
- 2) Target services that are a list of authorized remote services
- 3) Addresses: Remote IP addresses authorized to be connected in order to be allowed to establish sessions to targets services.

To let you understand how to create a policy, let us use a real case:

David and jhon are allowed to be connected to 2 TSE servers :

- 1) dc16.touzeau.biz (192.168.1.90) a Windows 2016 server using an hidden credential "administrator" and 90IPZJD09Z password
- 2) (192.168.1.46) a Windows 2008 r2 server using an hidden credential "administrator" and 871IPZJDO9Z password

David and jhon are allowed to be connected on the proxy only if their IP address is a part of 192.168.1.0/24 and during production time

Members, groups, targets can be managed in the "Policies" menu.

Artica V4 Documentation – david@articatech.com

Create members

On the "**Policies**" left menu, choose "**Members**". Click on **New member** button. Add the username and password your require to be connected on the RDS Proxy.

In our case, we create **jhon** and **david**.

Create Targets

Click on the **targets** tab Click on **New target** button

- Alias : A name that will be displayed in the TSE section
- **Description**: a short description that will be displayed on the TSE section.
- Protocol: choose RDP or VNC
- Hostname: The real hostname of the remote server
- Address: the FQDN or the IP address of the target server.
- **Remote port**: the listen VNC/RDP port
- Username: the real username that will be used in order to access to the target.
- **Password**: The real password that will be used in order to access to the target.

On our case, we will create 2 targets for dc16.touzeau.biz and srv2008-pdc1

Manager Administrator →	Search a computer, a member	(17:08:28	📳 Cpu:7.4% Mem	:25.6% 양 Members	🖪 Admin Guide	5
EE Dashboard	RDS Proxy v709 ww	Connectio	one			
🚍 Your system	New Mem	ber				
🚓 Network	Members Groups					٦.
≘ DNS	Paramet	ters				
# PDS Prove		User name:	User name		<u>≜</u>	-
A Status	Display Name	Password:	Password		۲	-
Connections			Password (Confirm)		P	
🖿 Statistics						-
🖺 Logs center				« Ap	ply »	
🛢 Databases						
Dashboard	PDS Providy7 0.0 mm Doli					
🚍 Your system	KDS Proxy V7.0.7 »» Poli	New target			>	
🚓 Network	Policies Members Targets	New target				
S DNS	New target					
⇔ RDS Proxy			Alias: Main Active of	lirectory	۵	-
🚳 Status	Target	Descri	ption: Company AB	C Active Directory		
2 Policies		pro	tocol: RDP		Y	
🛎 Statistics		hostr	name: dc16.touzeau	biz		-
E Logs center		Ade	dress: 192.168.1.90			
🛢 Databases		Remote	e port: - 3389		+	
	•	Userr	name: Administrate	ar		
		Pass	word:	••••	P	
			*******	****	P	
					« add »	
	Copyright Artica Tech © 2004-2019				v4.05.031014 Commu	nity Editi

RDS Proxy v7.0.9 »» Policies

Policies Members Targets					
☐ New target					
		Sear	ch	٩	•
Target	Hostname		PROTO	User Name	
DC with Security Center	srv2008-pdc1:33	89	RDP	Administrateur	~
The main active directory of the company	dc16.touzeau.biz	:3389	RDP	Administrateur	~

Create the policy

- Click on the **Policy** tab.
- Click on the **New Policy** button
- Give the policy name (rule name) and a short description
- Click on Add button.



RDS Proxy v7.0.9 »» Policies

New policy		New policy	×
licy	M	New policy	
		Rule Name: Accces Datacenter1	
		Description: Access to 2 servers from datacenter 1	
		¢	add »

Click on your New policy in the table

RDS Proxy v7.0.9 »» Policies

Policies	Members	Targets	
🗎 New policy			
Policy			Member
Policy ≜ Access datacer	nter1		Member

Associates members to the policy

Choose the "Members" tab

Click on Link a member and choose which member will be associated to this policy.

Access datacenter1	I ■ F DUS 1% I&AODU/S 1% IST 84ODDAFE	× .
Access datacenter1 Members	Targets	_
음+ Link a member	×	
Members	Search Q -	
No	Members	9
	Adavid Plink	

Associates targets to the policy

Choose the Targets tab Click on link Target to link a target server to the policy



Access datacenter1	Members	Targets	Networks	Time/Sche	dule
■Link target					Search Q
Targets				ŀ	losts
Kaspersky Server				s	rv2008-pdc1:3389 (192.1681.46)
Main Active Directory	company			d	dc16.touzeau.biz:3389 (192.168.1.90)

Set Network to the policy The Network section in the policy defines which sources IP addresses can use the policy Outside the defined network and if no policy matches the source IP address, the RDP client will be rejected.

 $You \ \text{can add a single address: } 192.168.1.1 \ \text{or } 192.168.1.1/32 \ \text{or subnet } 192.168.1.0/24 \ \text{in CDIR notation.}$

Access datacenter1	Members	Targets	Networks	Time/Sched	lule	
器 Add a new Network				_	Search	0
Networks					Search	~
금 192.168.1.0/24						6

Set working periods Working periods allows members to be connected to the targets only inside defined periods. You can add a period defined by a day of week and the period allowed to be connected.

cess dat	tacenter1					
Access of	latacenter1	Members	Targets	Network	Time/Schedule	
	orkingperiou				Search	۹ -
Working Pe	eriod					
C Tuesday	07:30:00 - 23:59	:00				0
Saturday	07:30:00 - 23:5	9:00				0
C Friday 07	7:30:00 - 23:59:0	0				0



CONNECT TO THE RDS PROXY

Open a TSE client on your computer and type the IP address of your Artica server with RDS Proxy installed.

Remot	e Desktop Con	nection			- 0
A .	Remote Conn	e Desk ectio	top n		
General	Display Local	Resources	Programs	Experience	Advanced
Logon s	ettings				
	Enter the nam	ne of the ren	note comput	er.	
	Computer:	192.168.	1.137		-
	User name:				
	You will be as	sked for crea	dentials whe	n you connec	t.
	Allow me	to save cred	lentials		
Connec	tion settings				
	Save the cur saved conne	rent connection.	tion settings	to an RDP file	e or open a
	Save		Save As		Open
Option	าร			Connect	Help

Inside the TSE session a form is displayed and ask credentials of a member defined in a policy.

*	192.168.1.137	_ 8 ×	_
	Target Information Required		
Device	192 168 1 138		
	101,100,1,100		
Login		→	
Password			
-	1		
· · · · · · · · · · · · · · · · · · ·			
fr-FR			



After sends credentials, a table is displayed in the TSE session. This table display all available targets from all policies

david@192.168.1.138	192.168.1.137 _ 🗗 🛪	Filter
Authorization	Target	Protocol
2.1) Main Active Directory	the main active directory of the company	RDP
2.3) Windows 7	192.168.1.191	RDP
3.2) Kaspersky Server	PDC with Security Center	RDP

After select with the mouse the target, the session will open to the target server automatically with credentials defined in the Artica targets database.

In Artica, select the sessions on the left menu in order to see the current established session. You can kill the session by click on the unlink icon on the session row.

Dashboard	RDS	Proxy	v7.0.9	»» Sessions				
Your system	RDS Proxy	allows you to se	t this server as	an RDP gateway in order to allow some users to	be connected to remote RDP/VNC servic	es		
- Network								-
⊜DNS						Search	٩	•
# RDS Prove	Status	Created	Updated	Client	Targets		Rules	
	connected	Q 00:07:37	00:15:41	192.168.1.138 (david (Advisitentary 2000)	Main Active Directory		Stratégie 2	8
2 Status			o Minutes	(david /Administratedr@cod2ead.biz)	(dc10.touzeau.biz.5367,172.106.1.70.5367)			-
🛎 Policies								
C Sessions								
Events								
🛎 Statistics								

Connection Error on Windows 7 or Windows XP

If you encounter this error while connecting to the RDS Proxy:

"An authentication error has occurred. The function requested is not supported"

On the service parameters, change:

- Minimal TLS version to "No restriction TLS v1.0"
- Cipher Suites to "More RDP clients (less secure)"

Remote I	Desktop Connection	
-	Remote Desktop Connection	
Computer:	192.168.1.137	
You wil Rer	note Desktop Connection	×
© <u>0</u>	An authentication error has occurred. The function requested is not supported Remote computer: 192.168.1.137	
	ОК	

IS RDS PROXY IS FAIL TO BAN COMPATIBLE ?.

Yes RDS Proxy is automatically monitored by fail To ban. If there are too much rejected RDP sessions, the fail to ban service will add automatically the source IP address in the local Firewall.



CAN I DEFINE SOME MEMBERS TEMPORARY?

Yes you can define a End Of life of each account associated to a policy

End of life is a maximal date a user can use the proxy.

If the time is expired, the user is disabled and cannot use the RDS proxy anymore.

Member: david		
User name:	david	۵
End of life:	2022-03-17 10:55:00	
Password:	•••••	Ð
	•••••	P



ELASTICSEARCH STATISTICS

Professional statistics are based on ElacsticSearch database.

Artica is able to manage the ElasticSearch service, in this case you can use Artica for this purpose.

It is recommended to install a dedicated Artica Proxy instance for this purpose. Use a minimal of 4vcpus, 8GB of memory and 150GB of hard drive.

Basically all events are sent to the Artica With ElasticSearch, a Web front-end called Kibana is able to display graphs and charts based on stored events.



INSTALL THE CORE STATISTICS DATABASE SERVER

- Go into the features section
- On the search field, type "ElasticsEarch database"
- Click on install button.

Manager Administrator →	■ Search	a computer, a membei	() 01:32:25	Cpu:5.3% Mem:6.9%	🔁 Admin Guide	🔮 🕛 Log out	=	
∎ Dashboard ■ Your system	Insta This section	Il or uninstall feat allows you to install/uninstall available f	EUTES eatures on your server	r				
 Your hard disks Memory swapping System events 	select +	C Expand A Wizards		Г	RealTime Statist	ics datab:	Ţ	
♦ reatures >_ OpenSSH server	Status	Status Software		Act	Action			
Glances O Tasks	Uninstalled	RealTime Statistics database			_		stall	
Certificates Center		Kibana statistics Interface		Δ	Require activated Rea	alTime Statistics datab	ase	
SNMPv3								
■ Backup P License								


FIREWALL PROTECTION

Artica Firewall feature protects PCs, servers or any other connected devices from hostile intrusions from the Internet and/or external networks.

It enables stateful packet filtering, Network Address Translation (NAT) and Port Address Translation (PAT) and is fully customizable to fit your needs. There is no need for any UNIX skills, no need to use the command line for anything, and no need to ever manually edit any rule sets. Users familiar with commercial firewalls catch on to the web interface quickly, though there can be a learning curve for users not familiar with commercial-grade firewalls

Manager Administrator →	≡ Searc	h messages	Cpu:18.3%	Mem:18.9%/3	.7GB ①11	l:58:08 %	St Members	Admin Guid	e 🕌	() Log o	ut %⊟
## Dashboard	Firew	all Rules									
🚍 Your system	Them										
👬 Network	Search mes	sages						Search mes	sages: All	interface	2S -
S DNS	+ New Rul	e Apply Firewall rules									
DHCP/TFTP	Order/id	Rule Name	Network Interface	Status	Packets	Size	Туре		Enabled	Order	Delete
(ൔ) Your Firewall	0/0	Default Allow this server to establish communications to 150 remote nodes.	All interfaces	Active	_	-	OUT	PASS	~	_	-
i ≣Rules & Firewall objects ⊞Firewall services	1/1	Windows Update For all nodes and To everything and Software «windowsupdate» and From 2 network elements then Limit traffic and Log all events All times	Connector: eth0 to eth1	Active	173	243.1 KB	FORWARD	LOG DENY	~	↑ ↓	0
a Interfaces connectors →NAT	1/3	Allow Web For inbound objects Is Internal Net (5 Items) and To everything and then Accept SNAT:2 All times	eth1 - Source NAT 10.10.1.2	Active	1 147 447	91.09 MB	NAT	PASS	~	^ ↓	0
♥ Masquerade ♥ Cybercrime IP Feeds ♥ Traffic shaping ■ Configuration file ♥ Events	1/7	HTTP For inbound objects Is Machines virtuelles (1 Items) and To everything and Services « <u>https</u> », « <u>https</u> », then Route packets to a node 192.168.1.133 All times	eth0 - Route packets to a node 192.168.1.133	Active	7 128	537.75 KB	NAT	PASS	~	↑↓	0

IPTABLES(NETFILTER) BASED FIREWALL

Artica Firewall feature is an iptables(netfilter) based firewall system designed around the essential needs of today's Internet deployed servers and the unique needs of custom deployed Artica installations. The Web administration console is designed to be very informative and present the user with an easy to follow process

- Real-time logging web console.
- **Cybercrime IP Feeds** is a feature that downloads regularly compromised IP addresses found in the Internet. It prevents your server to be attacked by already ban a bulk of IP addresses.
- Geo-Location module allows you to define rules against location of Public IP addresses.
 Deep Packet inspection module allows you to create rule against more than 239 detected
- applications in both HTTP/HTTPs protocols.
 Traffic shapping module is An high-performance implementation of committed access rate, or
- simply rate limiting, or policing.
- **Time restriction** module restricting Access By Time Of The Day.It allows you to control access based upon day and time.

INTRUSION DETECTION/PREVENTION SYSTEM

Artica provides Intrusion Detection System (IDS) that analyzes network traffic and tries to detect exploits, leaking data and any other suspicious activity. Upon detection, alerts are raised and the attacker is immediately blocked.

- Layer 7 application detection
- Multiple rules sources and categories
- Emerging threats database
- IP blacklist database



ARTICA v4

Firewall documentation can be found here: http://articatech.net/documentationfirewall.php



SECURIZE YOUR ARTICA SERVER IN CASE OF CORRUPTED SERVER.

Artica can run many services and you can install yourself Web services such as web services or any others services by enter into the system. If a virus enter into the Artica system you have to be sure that your corrupted Artica server will not spread internet in any ports or any destination.

By default, when you turn the WAN Interface to "Finally deny all", the right way, Artica automatically allow these protocols:

- ICMP : Accept to send ping to any
- DNS accept to send udp/tcp queries on 53 to any
- HTTPS accept to send HTTPs request on 443 destination port.
- HTTP : accept to send http requests on 80 destination port.
- FTP : accept to send FTP requests on 21 destination port
- NTP accept to send NTP requests on any destination.
- RSYNC accept to contact any rsync server
- SMTP accept to send messages on any SMTP servers on destination port 25
- SMTPS accept to send encrypted messages on any SMTPs server on destination
- cloudufdb accept to send request to 217.182.193.199:6000

For more details of allowed protocol, see the "firewall services" feature.

These rule are default rules and you can overide these rules by your own rule.

For example:

Our Artica server is not an SMTP relay and we just need Artica to send SMTP notification to our internal server. Our Artica server use DNS but only to reach the Google DNS on 8.8.8 and 4.4.4.4

So we have to **disable** the SMTP/SMTPs protocol and **specify** that the DNS query must **only go to Google**, nothing else.

(F)

- To override default rules, you have to use the "Your Firewall" / "Rules" section.
- On the main table, click on New Rule

Firewall Rules

Coorch	massama					Cal
+ New	Rule Roply Firewall rules All Interface eth0 (eth0) Interface et	th1 (eth1) → Interface eth0 (eth0)	Interface eth0 (eth0) →	Interface eth	2 (eth2)	00:
-			Search		Q	•
Order	Rule Name	Network Interface	Туре	Enabled	Order	Delete
-	Allow Artica Web Console TCP/9000	Interface eth0 (eth	nO) PASS	-	-	-
-	Internet access Allow this server to reach remote DNS, HTTP, HTTPS, FTP services and 217.182.193.199 Port 6000	Interface eth0 (eth	OUT PASS	-	-	-
-	Default Finally deny all	Interface eth0 (eth		-	-	-

On the new rule form, **choose the Interface** that act as WAN, specifiy that the rule is an "**Outgoing rule**" specify the service (in our case it is the SMTP service) and set the action as "**DROP**" in order to deny connection.

ıle: 0 New Rule		
Rule		
If you enable the outgoing rule option, t	hen this reaction is applied from the server itself to the destination network/service.	
Outgoing rule:	ON	
Rule Name:	Deny SMTP	<u>ه</u>
Enabled:	ОН	
Order:	- 1	+
Network Interface:	Network Interface:eth0 - Interface eth0	Ŧ
Service:	smtp tcp/25	v
	C Drop	
	Accept	
	Mark paquets	
Log all events:	OFF	

Your rule is added in the table as a DENY "Outgoing" rule.

		<u>.</u>					
+ New F	Rule Rule Apply Firewall rules	All Interface eth0 (eth0)	Interface eth1 (eth1) → Interface eth0 (eth0)	Interface eth0 (eth0) → Interface eth	2 (eth2)	
				Search		Q	-
Order	Rule Name		Network Interface	Туре	Enabled	Order	Delet
1	Deny SMTP From the firewall itself and To e Service « <u>smtp</u> » then Deny acce All times	everything and 255	Interface eth0 (eth	h0) OUT DENY	~	↑↓	0

This rule is designed to erase the default rule (SMTP)



DEEP PACKET INSPECTION

Deep packet inspection (DPI) is a type of data processing that inspects in detail the data being sent over a computer network, and usually takes action by blocking, re-routing, or logging it accordingly.

The Deep packet inspection is able to patch the Firewall in order to add a new module.

This module allows to enrich firewall rules by adding the possibility to detect some applications communication

Currently the Deep packet inspection allows to detects more than 200 applications

List of detected applications

AFP AJP AMQP Aimini Amazon AmazonVideo Apple AppleJuice ApplePush AppleStore AppleiCloud **AppleiTunes** Armagetron Aviva BGP BJNP BattleField BitTorrent СНЕСКМК CNN COAP CSGO CiscoSkinny CiscoVPN Citrix Cloudflare Collectd Corba Crossfire DCE_RPC DHCP DHCPV6 DNS DNScrypt DRDA Deezer Diameter

DirectConnect **ICMPV6** Direct_Download_LinkDofulfLIX Dropbox IGMP IMAP EAQ EGP IMAPS FIX IPP FTP CONTROL IP_in_IP FTP_DATA IPsec Facebook IRC IceCast FacebookZero FastTrack Instagram Fiesta KakaoTalk Florensia KakaoTalk VoiceKerberos GMail Kontiki GRE LDAP GTP LISP LLMNR GenericProtocolGit LastFM Github LinkedIn Gnutella Google LotusNotes GoogleDocs MDNS GoogleDrive MGCP GoogleHangout MPEG TS GoogleMaps MQTT GooglePlus MSN GoogleServicesGuildwars MS_OneDrive H323 MapleStory HEP Megaco HTTP Memcached HTTP_ActiveSyncHTTP_CoMmesstenger HTTP_Download Microsoft HTTP_Proxy MsSQL-TDS HalfLife2 Musical.ly Hotmail MySQL HotspotShield NÉS IAX NOE **ICMP** NTP

NetBIOS SAP NetFlix SCTP NetFlow SIP SMB Nintendo OCS SMPP OSPF SMTP Office365 SMTPS Ookla **SNMP** OpenDNS SOCKS SOMEIP OpenFT . OpenVPN SSDP Oracle SSH Oscar SSL POP3 SSL_No_Cert POPS STUN PPLive ShoutCast Sina(Weibo) PPStream PPTP Skype Pando_Media_BoosterPand6kypeCallIn Pastebin SkypeCallOut PcAnywhere Slack PlayStore Snapchat Playstation Sopcast PostgreSQL Soulseek SoundCloud QQ QQLive Spotify QUIC Starcraft RDP Stealthnet RSYNC Steam RTCP Syslog RTMP TFTP RTP TINC RTSP **TVUplayer** RX TeamSpeak Radius TeamViewer Redis Telegram RemoteScan Telnet

Teredo Thunder Tor TruPhone Tuenti Tvants Twitch Twitter UBNTAC2 UPnP UbuntuONE JabberUsenet VHUA VMware VNC VRRP Vevo Viber Vidto Warcraft3 Waze WeChat Webex WhatsApp **WhatsAppFiles** WhatsAppVoice Whois-DAS Wikipedia WindowsUpdate WorldOfKungFu WorldOfWarcraftXDMCP Xbox Yahoo YouTube YouTubeUpload Zattoo ZeroMQ

Install the Deep packet inspection

This feature is not compatible with "MultiPath TCP Kernel" feature.

Make sure you have the latest package.

- On the left menu,
- go into "Your system"
- Click on "Versions" menu.
- On the search field type "Deep"
- You will see the current installed version.
- If you see a dash, this means the module is not on your server.
- Click on Install or update button.



Versions System version and softw	vares versions		
Software	Version	Deep 🗶 🗸	
Deep Packet Inspection:	-	로 Instali or update	

A layer is displayed and shows you available versions Click on the button **Install or upgrade**.

Deep Packet Inspection		×
Deep Packet Inspection 2.4.0	11.2 MB	

After installing software on your server, go into Your System and features on the left menu. On the search field, type "**Deep**"

Click on "Install" button under "Deep Packet Inspection" row.

Dashboard	🔋 () Log out	
📰 Your system		
📾 Your hard disks		
Memory swapping	Install or uninstall features	
System events	This section allows you to install/uninstall available features on your server	
₩ Features		
>_ OpenSSH server	select - Expand A Wizards	
Glances		
© Tasks	Deep Packet	X -
Certificates Center	Chakura Cofkurara	Action
🖬 Backup	Status Soltwale	Action
₽ License	Uninstalled Deep Packet Inspection	✓ Install
④ Update		
🗂 Web Console		



- Network Search messages **Use Packet inspection** + New Rule Apply Firewall rules Int AII The Packet inspection is used in FireWall rules. On the left, menu use the "Your FireWall" and Rules. ٠ **¢**^e₀ Parameters Order **Rule Name** i≡ Rules Allow SSH From the firewall itself and To everything an 0 Service «ssh» and Software «quic,ftp_control,ftp_data» then A All times Masquerade Deny SMTP Cybercrime IP Feeds From the firewall itself and To everything ar 1 Services «smtps», «rsync», «smtp» then Den Firewall services All times \equiv Configuration file Allow Artica Web Console TCP/9000 Create a new rule and save it. Events . • Open the new created rule. Internet access

Select the "Deep packet inspection" tab.

With the Softwares button, choose which application you want to detect inside your rule.

Rule: 2 Allo	w SSH ACCEPT				
Rule	Firewall services	Outbound object	Deep Packet Inspection	Time restriction	
+ Softwares	-	t.	Deep Packet Inspection	×	Q -
Software			Search Q	•	
O quic			Software		0
O ftp_control			AFP	select	0
O ftp_data			Aimini	select	0
			AJP	select	
			Amazon	select	
			AmazonVideo	select	noc curo (curo)



AUTOMATIC PROTECTION - FAIL TO BAN

The Fail to Ban (aka fail2ban) service is an intrusion prevention software framework that protects your Artica servers from brute-force attacks Most commonly it is used to block selected IP addresses that may belong to hosts that are trying to breach the system's security. It can ban any host IP address that makes too many login attempts or performs any other unwanted action within a time frame defined by the administrator.

Install the Fail to ban service.

Go to the features section, in the search box, type "fail to"

Click on Install button on the "Fail To Ban" service.



THE SMTP SERVICE

The Artica SMTP service is designed to provide an advanced SMTP routing service and/or Anti-Spam/Antivirus service.

FEATURES

Anti-spam

Artica implements a number of techniques to detect, filter and block spam. It combines artificial intelligence algorithms and constantly adapts to identify the ever-changing techniques of spammers. ArticaTech provide advanced antivirus patterns to detects SPAM and phishing.

Protection

Artica is able to fight against phishing, ransomwares, malware, crypto locker and other threats.

Anti-virus

The antivirus service is able to check all incoming messages for viruses, worms, macro and suspicious attachments with potentially dangerous contents.

Quarantine

Artica offers a simple way to review quarantine lists

Powerful management

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

Page: 4



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.

Manager Administrator →	- J	caron a computer, a member	▼ MONITOL	0 10.01.30	. Сраттозо Гысшеосузо	. member 3	,	LUG UUL	•
Tashboard Your system	Ins This se	tall or uninstall fea	atures le features on your server						
 a Your hard disks System events, ↓ Features >_ OpenSSH server 	select	E Expand				МТА		*	•
Glances	Status	Software				Action			
O Tasks		Detfy M	TA Mail system				_	. A lost	
Certificates Center		Uninstalled POStfix M	In Mail Systelli			-	-		
System Monitoring	1								_

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) $% \left({{{\rm{A}}_{{\rm{A}}}} \right)$

To perform this behavior, the MTA service needs to know which computer is able to send a message to be forwarded to foreign domains.

On the SMTP Router, Routing & network, selec the "What clients to relay mail from" tab.

Add all networks or IP addresses of the computers/servers that will be able to send messages to Internet.

🕢 Status

\$ Parameters

Routing & network

Milter-greylist
 SMTP rules
 Blacklist/Whitelist

messages to memer.	192.168.1.0/24 From * to anything	
🚍 Your system	Routing tables v3.3.1	
🚠 Network & NICs	Routing tables allows you to create rules in order to forward message to a next hop	pe n
	Routing What clients to relay mail from ?	

Networks

192.168.1.0/24

+ New address Apply configuration



nessaging server according destina



THE ROUTING TABLE

On the SMTP Router, Routing & network, selec the "Routing" tab.

Click on new rule in order to create a routing rule Destination domain or recipients: If the option "Direction" is "Inbound" then this field is the destination address. It should be: "dummy@domain.tld or domain.tld" If the option "Direction" is "Outbound", then this field is the sender address. It should be "dummy@domain.tld or domain.tld" The service The sorvice that will be in charge to forward the message from the mail queue. In most cases this will be the SMTP service The hostname or IP address of the destination server. Opportunistic TLS mode.	estination domain.	Routing table:: New entry		
Destination domain or recipients:. If the option"Direction" is "Inbound" then this field is the destination address. It should be: "dummy@domain.tld or domain.tld" If the option "Direction" is "Outbound", then this filed is the sender address. ts should be "dummy@domain.tld or domain.tld" If the option "Direction" is "Outbound", then this filed is the sender address. ts should be "dummy@domain.tld or domain.tld" If the option "Direction" is "Outbound", then this filed is the sender address. ts should be "dummy@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. Opportunistic TLS mode.	lick on new rule in order to create a routing rule	Routing rule: New entry		
If the option "Direction" is "Outbound", then this filed is the sender address. It should be "dummy@domain.tld or domain.tld" The service 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. View of the destination of the destination server. With the form the mail queue. In most cases this will be the SMTP service Transport Layer Security Opportunistic TLS mode: Opportunistic TLS mode: View of the destination of the destination server. Opportunistic TLS mode: Opportunistic TLS mode: View of the destination of the destination server. Opportunistic TLS mode: View of the destination of the destination server. Opportunistic TLS mode: View of the destination of the destination server. Opportunistic TLS mode: View of the destination of the destination server. Opportunistic TLS mode: View of the destination of the destination server. Opportunistic TLS mode: View of the destination of the destination server. Opport of the destination of the destination server. Opport of the destination of the destination server. View of the destination of the destination server. None *	Destination domain or recipients:. the option"Direction" is "Inbound" then this field is the estination address. should be: dummy@domain.tld or domain.tld or .domain.tld"	Destination domain or recipient; Reject unverified recipient; Enabled:	acme.corp OFF ON	â
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. Opportunistic TLS mode.	the option "Direction" is "Outbound", then this filed is the ender address. should be dummy@domain.tld or domain.tld or .domain.tld"	Direction: Service: SMTP server address:	Inbound SMTP 19.168.1.113	* *
The SMTP server address and port: Opportunistic TLS mode: Opportunistic TLS mode: Opportunistic TLS mode. Mone *	he service he router service that will be in charge to forward the nessage from the mail queue. n most cases this will be the SMTP service	Port: Transport Layer Security	- 25	+
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.	he SMTP server address and port: he hostname or IP address of the destination server. Opportunistic TLS mode. i turned to ON your Artica server will try to forward the nessage using TLS/SSL, you can define the TLS verification nethod that your Artica server should use.	Opportunistic TLS mode: SMTP TLS security level:	OFF	• add »

This section instructs the SMTP service where to forward messages according sender email or sender domain or recipient email or recipient domain. In most cases you want to rel destination domain.

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 recipier

nfiguring: 100%	Done <u>«Details»</u>					
					Reconfiguring	- 100% D
Routing	What clients to relay mail f	rom ?	_			
+ 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.

Page: 7



In the text area, add all domains that will use the same configuration.

	in tilda.ht	
Parameters	Identical domains	
Domains		
Domains that	use same parameters of the original set	
Domains that	se sume parameters of an original sec	
1 acmi.corp 2 mail.lan 3 outgoing	fr	



Transfert messages to Exchange 2010 using TLS on port 587

QA: SSL ? Get Exchange 2010 Server to listen for SMTP on port 465?

Yes, you can make any SMTP virtual server or Receive connector listen on port 465, but that will not achieve your goal of secure SMTP (SMTPS).

- 1. Create a user/mailbox like "Artica"
- 2. Start the Exchange Management Console.
- 3. In the console tree, click **Recipient Configuration**.
- 4. In the result pane, select the mailbox for which you want to grant the Send As permission.
- 5. In the action pane, under the mailbox name, click Manage Send As Permission. The Manage Send As Permission wizard opens.
- 6. On the Manage Send As Permission page, click Add.
- 7. In Select User or Group, select the user (artica) to which you want to grant the Send As permission, and then click OK.
- 8. Click Manage.

On the Exchange PowerShell, type this command

```
Get-ReceiveConnector "Name of Connector" | Add-ADPermission -user "ACME\artica" -ExtendedRights "ms-Exch-SMTP-Accept-Any-Sender"
```

On the routing rule

- 1. Define the target port as 587
- 2. Enable the TLS method
- 3. Turn on the Authenticate method
- 4. Set the username and passord of the user with "Send As permission"

ing rule: acme.corp		
Reject unverified recipient:	OFF	
Enabled:		
Direction:	Inbound	v
Service:	SMTP	Ť
SMTP server address:	192.168.1.113	±
Port:	- 587	+
Opportunistic TLS mode:	ON	
Opportunistic TLS mode:	ON	
SMTP TLS security level:	Mandatory ILS encryption	•
enticate		
Enabled:	on 🗋	
User name:	artica	
Password:	•••••	P
	*****	۹

Page: 9

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 $\ensuremath{\ensuremath{^{\ast\ast}}}$ character has destination domain.

Select the direction as "Oubound" value.

Set the address of the outgoing relay.

Enable the Authenticate feature and give the username and password to enable your Artica server to authenticate the SMTP session.

uting table:: New entry		
Routing rule: Ner *		
Destination domain or recipient:	. 🧖	±
Reject unverified recipient:	OFF	
Enabled:		
Direction:	Outbound	x
Service:	SMTP	Ŧ
SMTP server address:	212.25.56.32	
Port	- 25	+
-		
Transport Layer Security		
Opportunistic TLS mode:	OFF	
SMTP TLS security level:	None	Ŧ
authenticate		
E 11.1		
Enabled:		
User name:	mailboxrelay	
Password:	******	P
	•••••	P
		and a

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%	econfiguring: 100% Done <u>«Details»</u>					
	Reconfiguring - 100% Done					
Routing	What clients to relay mai	l from ?				
+ New Rule	+ New Blind carbon copy	Apply configuration				
			Search		۹.	
Direction	Item	Forward To		Enabled	Delete	
Outbound	All domains	(smtp) 212.25.56.32:25 Authentication: mailboxrelay		~	0	
Inbound	acme.corp	(smtp) 192.168.1.113:58/ Opportunistic TLS mode: Mandatory TLS encryption Authentication: artica		~	0	



ADDRESSES REWRITING

Adresses Rewritting allows you to perform address rewriting

The menu "SMTP router"/Addresses Rewriting allows you to create rules according to 3 methods.

Generic: Typically to transform a locally valid address into a globally valid address when sending mail across the Internet.
 Generic, means no direction but only for outgoing messages, addresses can be for sender or recipients. If found, it will be replaced.
 This is needed when the local machine does not have its own Internet domain name, but uses something like *localdomain.local* instead.

E Your system	address rev	vriting				
👬 Network	Perform address rewriting	typically to transform a locally valid a	address into a globally	valid address when	sending mail across the	Internet
S DNS						
SMTP Router	+ New Rule Apply	configuration		1	\	
🙆 Status			1	1	Sear	Q -
i≡ Queue	Source Pattern	Destination Pattern	Generic	Sondor	Paciniant	Delete
🕫 Parameters	Source Fattern	Destillation Fattern	Generic	Sender	Recipient	Delete
Routing & network		1	No results	;		
C address rewriting						
IP reputation						
A Miltor-moviet						

- 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.

@	acme.corp		×
	@acme.corp (2)		
	Source pattern:	@acme.corp	
	Destination pattern:	@articatech.net	
	Outgoing messages only:	OFF	
	Sender address:	ON	
	Recipient Address:	OFF	
		« Apply »	

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.

SMTP Router	Parameters TLS/SSL Cluster
& Status ;≡Queue	General settings
😂 Parameters	Server name: smtp.touzeau.biz
Routing & network	Hale name: Hale name
IP reputation	neio name
Milter-greylist	SMTP Banner: \$myhostname ESMTP \$mail_name
▼ SMTP rules	Listen Network Interfaces:
T Blacklist/Whitelist	
Refused	Safety standards
🖿 Statistics	
🗄 Logs center	Optional SM IP server access restrictions in the context of a client SM IP connection request. The default is to allow all connection requests. This section allows you to manage rules will put restrictions on what systems will be able to send mail through this servinformation (name).
🛢 Databases	As restrictions are looked at in order, you will typically want to look at filters or restrictions that are based on local info external communications that will be initiated for each message.
	Disable VRFY command:
	Reject unknown client hostname: OFF
	Reject unknown reverse client hostname:
	Reject unknown sender domain:
	Reject invalid hostname:

Enable these features enforce SMTP senders to be compliance with the SMTP protocol, this force remote service to be real SMTP server.

Disable VRFY command:

The VRFY command can lead to a remote attacker gaining the first and last name registered to any given email account. This can aid an attacker in social engineering attack.

Reject unknown client hostname:

Reject the client when:

- The client IP address=name mapping fails,
- The name=address mapping fails,
- The name=address mapping does not match the client IP address

Reject unknown reverse client hostname

Reject the SMTP connection when the client IP address has no address=name mapping.

This is a weaker restriction than the reject unknown client hostname rule, which requires not only that the address=name and name=address mappings exist, but also that the two mappings reproduce the client IP address

Reject unknown sender domain

Reject the request when the SMTP service is not final destination for the sender address, and the MAIL FROM address has no DNS or MX record, or when it has a malformed MX record such as a record with a zero-length MX hostname

Reject invalid hostname

Reject the request when the client has a bad hostname syntax

Reject non fqdn sender

Reject the request when the MAIL FROM address is not in fully-qualified domain form, as required by the RFC This specifies the response code to rejected requests (default: 504)

Enforce restrictions in the HELO

If enabled, the SMTP service will force to correctly send the HELO command and reject if the hostname is not in fully-qualified domain or address literal form or the hostname has no DNS A or MX record

Reject forged emails:

Reject emails that pretend to be sent from your domains but not authenticated and not listed in your network list



Enable Generic rDNS Clients check:

this feature rejects generic reverse DNS patterns covering a large section of ISPs in the US, Canada, Europe, and elsewhere more than 1.600 patterns will try to block mails from computers trying to send mails behind Public ISPs

Reject Internal and External non-existent domains:

Domains with no DNS A or MX record are rejected

Reject senders' domains not listed in local database:

If you turn on this feature only internals domains are allowed to send mails through this server. This means you turn this server to an outgoing mail server only because senders Internet domains such has gmail.com, hotmail. * or yahoo. * will not allowed to send email to this server

IP REPUTATION.

If your server is in front of internet, using a reputation database increase dramatically the anti-spam rate and decrease the usage of "content filtering". An IP reputation database (aka RBL, DNSBL) is a cloud server that stores a list of blacklisted IP addresses. These IP addresses are known to send SPAMs.

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

Use the Artica reputation database:

The Artica reputation database is available with an Enterprise License Edition. It allows you to query a database that stores more than 4.000.000 blacklisted IP addresses and 100.000 whitelisted IP addresses.

To use the Artica reputation database, on the left menu choose "SMTP Router" and IP Reputation.

On the status page, click on the "**Enable**" in the "**Artica reputation** database" widget.



Page: 13



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.

Status	Public Blacklists databases		
+ New service	Apply configuration		
ervice	P reputation		×
·	IP reputation Realtime Blackhole Li	st / Right Hand Side BLs	
	Service:	None	<u> </u>
	Create a new one:	None	
Copyright Arti		sbl.spamhaus.org (Realtime Blackhole List) b.barracudacentral.org (Realtime Blackhole List)	lours
		bl.spamcannibal.org (Realtime Blackhole List) relays.ordb.org (Realtime Blackhole List) bl.spamcop.net (Realtime Blackhole List)	



Public Whitelist database

This feature allows Artica server to query dnswl.org.

This organization is active in the anti-spam community.

The editors and administrators of dnswl.org data and systems are located in the UK, the US, Germany, Austria and Switzerland. Former active members came from Sweden, Finland, France, Netherlands, and had various contributors from an even more diverse set of geography.

It maintains a database of IP addresses (net ranges) which are grouped into "DNSWL Records" (identified by a DNSWL Id, which is just an arbitrary number). This data is maintained through a combination of manual and automated actions.

Basically, the DNSWL database stores only "good SMTP servers" and claim to avoid false positives from public blacklists databases.

To enable the use of DNSWL, on the IP reputation section, click on Activate on the grey "Public Whitelist database" section.





THE MILTER-REGEX MODULE FOR BLACKLISTING PERFORMANCE.

Sometimes you need to blacklist the sender email address or some words in the subject. The blacklist reputation cannot deny everything came from office365, Gmail, Yahoo and other large ISP that provides free mail accounts.

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

Spammers usually use sequences on the mail from address for example johnspamer234@gmail.com, johnspamer456@gmail.com. The milter-regex module will be able to catch these sequences because it matches sender email addresses using regular expressions. In this case, johnspamer234@gmail.com will be denied using johnspamer[0-9]+@gmail\.com. This module is designed to scan a large list of rules using a minimal memory/CPU footprint.

On the Features section, in the search field, find the entry "Milter" Click on the Install button on the "Milter-regex" row.

Install or uninstall features

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



After installing the milter-regex module, you should see on the SMTP Router/Status the status of the milter-regex service.



In the Blacklist and whitelist rules you can create a rule with 3 new items:

- Sender: Regular expression
- Subject: Regular expression,
- **Body: Regular expression** .



BLACKLISTS AND WHITELISTS RULES

Blacklists rules and Whitelists rules are designed to refuse or allow any SMTP transaction from specifics items.

Basically, you can fill automatically this list from the SMTP transactions list

When clicking on the sender email address in the SMTP transactions, you can deny or allow the sender email address or the sender domain address.

us	Artica RBL	Time	ID	Reason	IP Address	5
jected	unknown	15:58:27	1D8C089084	Blacklisted (ACL:33)	192.168.30.47 DESKTOP-DTOUZEAU	joeroges@articatech.net
TP	unknown	15:58:27	1D8C089084	Connection accepted	192.168.30.47	joeroges@articatech.net
P	joeroge	s@articatech.net				×
ected	joero	oges@articatech.net				
пр		joeroges@articatech.	net		articatech.	net
jected		् Search eMail address			ି Search Doma	in and a second s
		🖕 Whitelist eMail address		-	🐞 Whitelist Don	nain
MTP		👎 Blacklist eMail address			👎 Blacklist Dom	ain
	_	04.46.27	/EFE700F70	nou.existent.auth		
ND	-	04:48:27	7770988F95	removed	-	-

Whitelist checking

By default, the Artica SMTP server checks is a remote connection before any SMTP protocol task. This means reverse hostname, reverse sender domain name, reputation servers are checked before checking sender eMail address

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

If you want to trust the sender eMail address, you need to reverse the IP checking method.
This way could be dangerous because the sender domain and eMail address can be easily compromise

To reverse the IP checking methods, go to " SMTP router " and " Parameters " section.	
Under "Safety standards", switch TCP/IP verification dropdown list to "Sender eMail is checked before sender IP	"

⊠ SMTP Router	Server name: smtp.artica.center
🔁 Status	
⊞ Queue	Helo name Helo name
😂 Parameters	SMTP Banner: \$myhostname ESMTP \$mail_name
Routing & network	Listen Network Interfaces:
Address Rewriting	
(A) Firewall	Safety standards
IP reputation	
Milter-greylist	Optional SMTP server access restrictions in the context of a client SMTP connection request.
▼ SMTP rules	The default is to allow all connection requests. This extronal allows unit manages and use will aur participations on what suprems will be able to send mail through this senser based on the client ID and host information (name).
T Blacklist/Whitelist	As restrictions are looked at in order, you will typically want to look at filters or restrictions that are based on local information first, in order to limit the external communications that will be initial
Refused	
1. C	TCP/IP Verification: Sender eMail is checked before sender IP
Statistics	Disable VRFY command:
@ Clam AntiVirus	Reject unknown client hostname;

In this case, whitelisted eMails will not be checked against IP addresses and messages will pass all tests.



CLUSTER CONFIGURATION.

Cluster configuration allows a slave SMTP server to replicate configurations from a master server. When administrator modify a parameter on the master, the master create a configuration package with an index file that stores the MD5 of the parameters.

The slave pool periodically the MD5 configuration package to see if there are changes. If the MD5 is modified, then the slave download the package and apply the whole settings.

Replication is made through the Artica Web interface (SSL). The replication package is encrypted with a defined password.





On the Artica server as **"Master server**", select **"SMTP Router**" and **"Parameters**" on the left menu. Choose **"Cluster**" tab.

Turn on the "Enable Master mode" Set a password to encrypt the replication package.

## Dashboard	Postfix MTA Mail system v3.3.1
E Your system	This section allows you to manage the SMTP service that is in charge to transfert messages to the correct destination. Messages can be transfered to remote server or to the local service in charge of store messages into mailboxes.
A Network & NICs	
S DNS	Parameters TLS/SSL Cluster
SMTP Router	Cluster configuration
@ Status	
:≡ Queue	Master mode
😂 Parameters	
Routing & network	The Master mode is able to backup and crypt DNS data according and effined passphrase
IP reputation	
🖨 Milter-greylist	Enable Master mode:
▼ SMTP rules	Password:
T Blacklist/Whitelist	
Refused	

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).

e Slave mode is able to retreive a u need to ensure that this server skage.	and decrypt DNS dat r is able to be connec	ia. ted on to Artica Web console port in order to let this server download correctly the o	luster
Enable Sla	ave mode: 🛛 🔊		
F	Password:		
	•••		P
Network	Interface: All	interfaces	٣
Master h	hostname: 192	2.168.1.208	
Rer	mote port: –	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.

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 transfered to remote server or to the local service in charge of store messages into mailboxes.



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 transfered to remote server or to the local service in charge of store messages into mailboxes.

Wait several times (${\bf 5}$ minutes), you should see the synchronization delay





AUTOMATICALLY BAN IP IN FIREWALL BASED ON EVENTS.

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

Install the latest version

- On the Left menu, choose "Your System" and "Versions" on left menu. On the search field, type "Fai To" √
- 1
- ~ Click on Install or update button.

Versions System version and softw	ares versions		
Artica Core server	Operating system	Python packages	fail to 🗶 🗸
Software Version Fail To Ban: 0.110.3		Linstall or update	

Click on "Install or Upgrade" on the desired version.

Fail To Ban		×
Fail To Ban 0.11.0	617.83 KB	🛃 install or Upgrade



Install the Fail To Ban service

select - Expand			
		fail to 🗶 👻	
Status	Software	Action	-
Uninstalled	Fail To Ban	✓ Install	Dashboar
			E Your syste
			- Network
ı, you will see the "Fail To	ban" menu entry after the installati	on.	€ DNS
an dashboard you should	see at least 1 Engine in the status		(초) Your Fire
an dashboard, you should	see at least 1 Engine in the status.		(한) Your Fire 중 Fail To Bar
an dashboard, you should Fail To Ban	see at least 1 Engine in the status.		(b) Your Fire
an dashboard, you should Fail To Ban Fail2ban scans log files and bans IPs th Generally Fail2Ban is then used to upd be configured. Out of the box Fail2Ban comes with fil	see at least 1 Engine in the status. at show the malicious signs too many password failures.s late firewall rules to reject the IP addresses for a specified a ters for various services (apache, courier, ssh, etc).	eeking for exploits, etc. nount of time, although any arbitrary other action (e.g. sending an email) could also	(b) Your Fires
an dashboard, you should Fail To Ban Fail2ban scans log files and bans IPs th Generally Fail2Ban is then used to upd be configured. Out of the box Fail2Ban comes with fil	see at least 1 Engine in the status. at show the malicious signs too many password failures.s late firewall rules to reject the IP addresses for a specified a ters for various services (apache, courier, ssh, etc).	eeking for exploits, etc. nount of time, although any arbitrary other action (e.g. sending an email) could also	نگ Your Fin
an dashboard, you should Fail To Ban Fail2ban scans log files and bans IPs th Generally Fail2Ban is then used to upd be configured. Out of the box Fail2Ban comes with fil	see at least 1 Engine in the status. hat show the malicious signs too many password failures, s late firewall rules to reject the IP addresses for a specified a ters for various services (apache, courier, ssh, etc).	eeking for exploits, etc. nount of time, although any arbitrary other action (e.g. sending an email) could also Engine Filters: postfix	(∆) Your Fi ₽ Fail To f
an dashboard, you should Fail To Ban Fail2ban scans log files and bans IPs th Generally Fail2Ban is then used to upd be configured. Out of the box Fail2Ban comes with fil Fail To Ban	see at least 1 Engine in the status. at show the malicious signs too many password failures, s late firewall rules to reject the IP addresses for a specified a ters for various services (apache, courier, ssh, etc).	eeking for exploits, etc. mount of time, although any arbitrary other action (e.g. sending an email) could also Engine Filters: postfix	(≙) Your Fire
an dashboard, you should Fail To Ban Fail2ban scans log files and bans IPs th Generally Fail2Ban is then used to upd be configured. Out of the box Fail2Ban comes with fil Fail To Ban Running	see at least 1 Engine in the status.	eeking for exploits, etc. nount of time, although any arbitrary other action (e.g. sending an email) could also Engine Filters: postfix 1	(£) Your Fire

-0

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

C Restart

√

On the "Features" section search the entry "fail to" and click on "Install" button on the "Fail To Ban" row.

0



SECURE OUTGOING MESSAGES WITH SPF, DKIM AND DMARC

Use SPF with DKIM and DMARC

Along with SPF, we recommend setting up **DomainKeys Identified Mail** (DKIM) and **Domain-based Message Authentication**, Reporting & Conformance (DMARC).

- SPF validates the domains that can send messages.
- DKIM verifies that message content is authentic and not changed.
- DMARC specifies how your domain handles suspicious emails that it gets.

SPF DNS Record

Create an SPF record for your domain

An SPF record is a TXT record that lists the mail servers that are allowed to send email from your domain. Messages sent from a server that isn't the SPF record might be marked as spam.

On the left menu, choose "SMTP Router" and "Routing & Network" On the table select the inbound domain.

Dashboard Your system	Routing tables allows you to create rules in order to forward message to a next hope messaging server according destination domains, send				
👬 Network	Routing	What clients to relay mail fr	rom?		
Se dns					
(≜) Your Firewall	+ New Rule	+ New Blind carbon copy	Apply configuration		
🗟 Fail To Ban		_			
SMTP Router	Direction	Item			
n Status	Inbound	artica.fr			
i≣ Queue	Inbound	mail-appliance.com			
☆ º Parameters					
Routing & network					
Address Rewriting					
(▲) Firewall					
IP reputation	Copyright Artic	a Tech © 2004-2019			



- Click on the SPF tab.
- The page shows you an example of SPF DNS entry you have to add in your public DNS server.
- Copy the content of the generated string, replace the 1.2.3.4, 1.2.3.5 entries by the real public IP address of your MX1 and MX2 (if you have one)

Routing table:: artica.fr	×
Parameters Identical domains SPF	
Set up SPF to prevent spammers from sending unauthorized emails from your domain. This type of spamming is called spoofing. Sender Policy Framework (SPF) is an email security method to prevent spoofing from your domain by just ac a record in your public DNS. Set up the SPF record for your domain by adding a TXT record to your domain host. Adding the TXT record doesn't affect your mail flow. Use the text generated and replace 1.2.3.4,1.2.3.5 by your mx1 and mx2 public IP addresses.	Verify your SPF record
artica.fr. IN TXT or SPF "v=spf1mx ip4:1.2.3.4 ip4:1.2.3.4.5 a:smtp.artica.center a:smtp2.artica.center -all"	.12

• After adding your DNS entry, click on the "Verify your SPF record" to see if your SPF record is accepted by any SMTP server.

Example for BookMyName (it accepts only TXT record):

28800 TXT	"v=spf1	mx ip4:1	.2.3.4	a:smtp.arti	ca.center	all"			
				OLBOX°	U	pgrade	Delivery Center	Supertool	Monitoring -
		谷	MX Loo	okup Blacklist	s Diagn	ostics	Domain Health	Analyze H	leaders Fi
		Investi	gator	DNS Lookup	More 🗸				
		Super	Tool ^E	Beta7					
		artica.t	fr				SPF Record Lookup	~	
		spf:ar	tica.fr	Find Problems	Solve	Email Del	ivery Problems		S spf
		v=spt	F1 mx ip	4:213.32.85.20 a:	smtp.artica	.center -	all		
		Prefix	Туре	Value	PrefixDesc	Descript	ion		
		v	version	spf1		The SPF	record version		
		+	mx		Pass	Match if I	P is one of the MX hos	sts for given d	omain name
		+	ip4	213.32.85.20	Pass	Match if I	P is in the given range	1	
		+	а	smtp.artica.center	Pass	Match if I	P has a DNS 'A' recor	d in given don	nain
			all		Fail	Always n	natches It goes at the	end of your r	ecord

The mx Toolbox must display a green report for your SPF checks.



The OpenDKIM service

Use the DomainKeys Identified Mail (DKIM) standard to help prevent email spoofing on outgoing messages.

Email spoofing is when email content is changed to make the message appear from someone or somewhere other than the actual source. Spoofing is a common unauthorized use of email, so some email servers require DKIM to prevent email spoofing.

DKIM adds an encrypted signature to the header of all outgoing messages.

Email servers that get these messages use DKIM to decrypt the message header, and verify the message was not changed after it was sent.

On the left menu, click on **Your System** and **Features** section. On the search field, type **DKIM** Click on install button on the OpenDKIM mail filter row

Insta This section	Il or uninstall features allows you to install/uninstall available features on your server	
select -	C Expand <u>A</u> Wizards	DKIM × -
Status	Software	Action
Uninstalled	OpenDKIM mail filter	✓ Insta

- After installing the OpenDKIM service, all your domains will be signed with a DKIM Key.
- On the left menu, go to SMTP router / OpenDKIM mail filter
- Select Database tab.
- The section lists all internals domains in order to display the generated DKIM Private key and the DNS entry you should add to your Public DNS server.
- Click on a DNS entry on one of domains.

Manager Administrator -	E Search a computer, a member		SMTP Transactions	්ා Search 1
Dashboard	OpenDKIM mai	l filter v2.11.0		
■ Your system	DKIM is an email authentication fram It allows email providers to validate a It also makes phisburg attacks easier	ework that addresses the widespread issue of email forgery, using cryptography to verify the domain of the sender. nemail's originating domain, making use of blacklists and whitelists more effective. or detects the bencinstructure details in the busine domains.		
- Network	This technology is a combination bet	ween signed messages and DNS servers, all mails signed will be verified with the public DNS checking method (the TXT field).		
S DNS	Outgoing mails can be signed with yo	vin increase die aitropani score, in die opposie, sogred mai ded ease scores. ur certificates in order to be verified by others mails servers.		
(≜) Your Firewall	Status Database			
🛱 Fail To Ban				
SMTP Router				
🔁 Status	Domain Private Key Siz	e a statistica de la constatistica de la constatistica de la constatistica de la constatistica de la constatist	DNS Entry	
⊞ Queue	artica.fr 3.17 KB	default_domainkey IN TXT ("v=DKIM1; h=rsa-sha256; k=rsa; s=email; " "p=MIICIjANBgkqhkiG9w0BAQEFAAOC	CAg8AMIICCgKCAgEA1mU	JBHnDw
🗢 Parameters 💭 Routing & network	mail-appliance.com 3.17 KB	default_domainkey IN TXT ("v=DKIM1; h=rsa-sha256; k=rsa; s=email; " "p=MIICIjANBgkqhkiG9w0BAQEFAAOC	CAg8AMIICCgKCAgEA9/W	/uOZe1
Address Rewriting				
(A) Firewall				
COpenDRIM mail filter				
Milter-greylist	C			
▼ SMTP rules	Copyright Artica lech © 2004-2019			_

• A layer displays the data you should add in your public DNS.



- There are 2 forms, the top section is for Bind method and the bottom one is for BookMyName method.
- Copy and past the data into your Public DNS server for each domain in the list.

_	N TXT ("v=DKIM1; h=rsa-sha256; k=rsa; s=email; "	
"p=MIICIjANBgkqhki sgwhDM3uDEAfWH OJdYAmS6IB0xDQoo	G9w0BAQEFAAOCAg8AMIICCgKCAgEA1mUBHnDwt3vbN2KRdZ4L3nu +tk/aDY4Lv90ugsUpjRvloapblAujLiU7ReXqym7xw4PMkdH+1frmH4VLchg iceHDMnxSe1b+AekKUXWbSof88" Bind method	SnGlbzps KZYZB
"my6YiQERk7NdyL3 AH0TRiBQtGiwlHscf	QKJd9lKa8jgdL/j1ZcHRdVAWsJGjsjHApHldb1dcvq8Ssjge 77W8cS4fcJcvcWeapJ1MpTCpCO1000DQr YofWNM82FxdIYX96FiDPWfPTCh+0uwPYIRz2AF5mrqDKGLZP6rSCfQXBJIr5xlCdqOQkGjLbsJJtleDLof	avz6WFZfw GrPLopGoDx
"EcZivPK/jnni0/s	eW1c/c+kmE1VFTaV7bbyNb	
The second secon		
/tBYdjzdPvuNMLU18	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OIVPRMZ7ets1MfOROKlugIMW0WcCA	wEAAQ==")
/kvo3+Cr9vyQYrrdP /tBYdjzdPvuNMLU1f ; DKIM key defau	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OlVPRMZ7ets1MfOROKlugIMW0WcCA lt for artica.fr	wEAAQ==")
/tBYdjzdPvuNMLU18 ; DKIM key defau 	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OlVPRMZ7ets1MfOROKluglMW0WcCA lt for artica.fr	wEAAQ==")
/tBVd3+Cr9vyQfrrdF /tBYdjzdPvuNMLU1f ; DKIM key defau BookMyName: default_domainkey 2	gHN4HmY5705DrWZ2hrSiEuCJ2YItYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OIVPRMZ7ets1MfOROKlugIMW0WcCA It for artica.fr 	wEAAQ==")
/tBYdjzdPvuNMLU1f /tBYdjzdPvuNMLU1f ; DKIM key defau BookMyName: default_domainkey 2 p=MIICljANBgkqhki0 gwhDM3uDEAfWH+	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OIVPRMZ7ets1MfOROKlugIMW0WcCA lt for artica.fr 	Glbzpss ZYZBO
/tb3+Cr9vyQtrrdi- /tBYdjzdPvuNMLU1f ; DKIM key defau BookMyName: default_domainkey 2 p=MIICIjANBgkqhki(gwhDM3uDEAFWH+ JdYAMS6IB0xDQo6c (/12rcHR4V0Wc [Gire]	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OIVPRMZ7ets1MfOROKluglMW0WcCA It for artica.fr 3800 TXT "v=DKIM1; h=rsa-sha256; k=rsa; s=email; :9w0BAQEFAAOCAg8AMIICCgKCAgEA1mUBHnDwt3vbN2KRdZ4L3nuyt tk/aDY4Lv90ugsUpjRvloapblAujLiU7ReXqym7xw4PMkdH+1frmH4V1 HDMnxSe1b+AekKUXWbSof88my6ViQERk7NdPJ3QKU6Dp2cbu26WE76w4H0TPiBOrCiv/Hsc2VpP	Glbzps: SYZBO
/tBYdjzdPvuNMLU1f /tBYdjzdPvuNMLU1f ; DKIM key defau BookMyName: defaultdomainkey 2 p=MIICIjANBgkqhki(gwhDM3uDEAfWH+ JdYAMS6IB0xDQo6c /j1ZcHRdVAWsJGjsj YX96FiDPWfPTCh+(3ppMiEcZivPK/inni)	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OIVPRMZ7ets1MfOROKluglMW0WcCA lt for artica.fr 	Glbzpss ZYZBO WNIM82Fxdl J4T21CMJ69
/tbYdjzdPvuNMLU1f /tBYdjzdPvuNMLU1f ; DKIM key defau BookMyName: default_domainkey 2 p=MIICIjANBgkqhki(gwhDM3uDEAfWH+ JdYAMS6IB0xDQo6c /j1ZcHRdVAWsJGjsji YX96FiDPWfPTCh+(3ppMiEcZivPK/jnni0 /RVo3+Cr9vyQYrrdP	gHN4HmY5705DrWZ2hrSiEuCJ2YltYWs5LB8fn4tsMjTCti9XX6hcH0/tEZ+CBLtZmgOpFh2Heb76R zfEfVjFq/XppheHsg7ZZpx3b0xr8hYuXTj9HlpoO2Saozf6+9RV7OIVPRMZ7ets1MfOROKluglMW0WcCA lt for artica.fr 	Glbzpss ZYZBO WNIM82Fxdl J4T21CMJ69

The DMARC DNS record

DMARC is built upon two other authentication protocols: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

You should have SPF and DKIM on your Envelope From and Friendly From domains before proceeding with DMARC.

Identify email accounts to receive DMARC reports

Through DMARC, you will receive aggregate and forensic (message level) reports daily. Designate the email account(s) where you want to receive these reports. You may want to use two separate accounts, as you could get inundated with the data.

DMARC reports are very difficult to parse because they are provided in raw format. Partnering with a company like Return Path can help you and your team make sense of them

Learn the DMARC tags

DMARC tags are the language of the DMARC standard.

They tell the email receiver (1) to check for DMARC and (2) what to do with messages that fail DMARC authentication.

There are many DMARC tags available, but you do not have to use them all. In fact, we recommend keeping it simple. Focus on the

v=, p=, fo=, rua, and ruf



Generate your DMARC record with DMARC Creation Wizard

Using a DMARC Creation Wizard, (<u>https://www.kitterman.com/dmarc/assistant.html</u>) generate a DMARC text record in your DNS for each sending domain. Set the mail receiver policy to "none," indicating DMARC's "monitor" mode.

With DMARC in monitor mode, you can gather the information on your entire email ecosystem, including who is sending email on behalf of your brand, what emails are getting delivered, and what emails are not.

Request to receive the daily aggregate and forensic reports by specifying your email address in the rua tag and the ruf tag, respectively. Use the email address(es) you identified in step three above.

Background

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an enhancement to existing email authentication technologies. Details of the DMARC protocol and related information can be found a DMARC is still in progress and subject to change. This assistant has been updated based on RFC 7489. Terms used in this assistant are taken from section 6.3 of that document.

DMARC Assistant

Most of the the terms below have mouseovers that provide additional information about their meaning in DMARC.



[1] Multiple addresses are supported (at least two). Enter a comma separted list for more than one. The optional size limit is not supported by all providers and use will cause interoperability problems as of 2014/08/03. [2] May be very high volume - the ruf address must be prepared to receive a LOT of mail.

Your record should look something like this:

```
_dmarc.artica.fr TXT "v=DMARC1; p=none; rua=mailto:postmaster@artica.fr; ruf=mailto:dmarc@artica.fr; fo=0; adkim=s; aspf=s; pct=100; rf=afrf; ri=86400; sp=none"
```

Now, Add the generated entry into your public DNS server.



THE POLICIES SERVICE (ANTI-SPAM, ANTIVIRUS...)

The Policies service is a Milter that hook the MTA. It is designed to analyze content messages in order to find spam or malwares. This service require a valid Corporate License. It allows you to :

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

Install the Policies services.

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

Insta This section	Install or uninstall features This section allows you to install/uninstall available features on your server						
select -	C Expand		Policies 🗶 🗸				
Status		Software	Action				
	Uninstalled	Policies service	✓ Install				

Enable SMTP content features.

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

📰 Dashboard	Policies service »» Service status
Your system	Implements antispam, antivirus, and other customizable filtering on email messages.
🚓 Network	
≣DNS	Status Parameters Statistics Messages Statistics Volumes
(a) Your Firewall	Services
🖶 Fail To Ban	Auto-WhiteList.
SMTP Router	Enable Anti-Spam Engine:
	Checking Email spoofing;
Policies service	Activate antivirus checking; OM
🙆 Status	Backup on the fly:
💸 Anti-Spam Engine	Enable disclaimer feature: OFF
🕅 Anti-Spam rules	Automated compression:
Antivirus Rules	Attached files filtering;
📾 Backup on the fly	

- Auto-Whitelist: Automatically add recipient email address to Whitelist database when your users send an eMail.
- Enable Anti-Spam Engine: Add the bayesien and scoring content Anti-spam engine.
- Check eMail spoofing: A foreign sender cannot use your internal domains to send eMail to your users.
- ✓ Activate antivirus checking: Scan message for malwares.
- ✓ Backup on the fly: Backup all messages that are forwarded by the SMP relay.
- Enable disclaimer feature: Allows you to add a disclaimer according SMTP rules.
- Automated compression: Allows the SMTP relay to zip compress attachments according SMTP rules.
- ✓ Attached files filtering: Remove unwanted files according files extensions.
- ✓ **URL Filtering**: Changes URLS in order to give time to detects phishing and malwares.



URL Filtering in SMTP messages

The URL filtering is a feature designed to change URLs in inbound messages in order to force users to use a web frontend before accessing to the real URL sended.

URL Filtering process:



Objectives:

-

If a user click on a link inside a receive message



It will be redirected to a splash page that display results of URLs analysis On the splash screen, user can:

- Add the sender as trusted sender.
 - Get the original message if not URLs are marked has phishing or malware.

Mes	sage 4AA2	1101A67 From dtouzeau@gmail.com
You h Indee viruse	ave been red ed, for securi t es or hacking	rected to this temporary page. y reasons, the mail gateway has modified the original links to ensure that they do not hide sites.
Your link	message 4AA	21101A67 contains 1 Internet links, below, the list of links and the analysis report for each
ID	Status	Urls
19	J Success	http://fhgovflkg.ru
No	otice, the mes	sage and URIs will be removed from database on 2020 Sunday April 05 14:43:52

If one link is a phishing site or a virus, the user will not be able to restore the message or click on links.



Enable Url Filtering

On the left menu, choose "Policies service, URL filtering"

Your system	URL filtering	
🚓 Network	This feature is designed to modify URLs in inbound messages in order to parse them and analyze them before the user.	
S DNS		
(<u>b</u>) Your Firewall	Parameters Rules Links	
🛱 Fail To Ban	Parameters	
SMTP Router	Enable the feature: ON	
Policies service	Trust senders stored in auto-whitelist database:	
🕰 Status	timeout HTTP (seconds): = 5 +	
💸 Anti-Spam Engine	Website: 213.32.85.20	
💸 Anti-Spam rules	Minimum Time to live: 30 Minutes +	
Antivirus Rules Antivirus Rules	Maximal time to live>: 2 Days	
Backup on the fly	phishing-initiative fr API Kev: 4bacafedc47c168a75de42b70dc91e86efb41efa802d98	
💅 Auto-WhiteList 🖬 Quarantine	VirusTotal API Key: 26a41e51875b4088cda872c4b4d8850b7	

- Turn on the "Enable the feature"

- Trust senders stored in auto-whitelist...:

If the sender matches a rule stored in auto-whitelist database, then URLs will be not modified. The user will be able to trust sender in the splash screen too.

- Timeout HTTP (seconds):

The process will try to get the final point of the URLs in order to get the final Content-Type of the Internet object. Define here the TimeOut in seconds the HTTP engine will use to be connected on the remote sites.

- Website:

Define here the hostname (https mandatory) to access to the splash screen (the Artica Web Console). The best way is to turn Artica Web console on 443 port and set here only the hostname or IP address. If you keep the 9000 port of the Artica Web console, set 192.168.1.1:**9000** in the field

- Minimum Time to live:

The time to wait before analysis the message, this time must help RBLs servers such as Virus Total or Artica Tech to add the phishing urls in databases.

- Maximal Time to live:

When URLs are modified, Artica will store URLs and original message to the Artica database.

- After this period all data will be removed.
- Phishing-initiative.fr API Key: Give here the API key o the <u>https://phishing-initiative.fr/</u> website.
- Virus Total API Key:

Give here the API key o the <u>https://www.virustotal.com</u> website.



The rules section

The rule section allows you to enforce or whitelist a domain or a user to be or not pass through the URLs engine.

- You can add an email address or a domain.
 - *: Matches everything.
 user@domain.net: Matche
 - user@domain.net: Matches this one address.
 - domain.net: Matches all addresses from domain.net.

Action can be "Do nothing" (do not modify URLs) or "Change URLs in messages" (enforce the action even the sender is stored in auto-whitelist rules).

URL filtering This feature is designed to modify URLs in	inbound messages in order to parse them and analy	ze them before the user.	
Apply parameters: 100% Done <u>«Details»</u>			
	Apply par	rameters - 100% Done	
Parameters Rules Links	New Rule		×
+ New Rule Apply rules	New Rule		_
sender	You can add an email address or a domai *: Matches everything. user@domain.net: Matches this one add domain.net: Matches all addresses from	in here. dress. . domain.net.	
	sender: Recipient:	david@mail.com	
	Action:	Do nothing 🔻	- 1
Copyright Artica Tech © 2004-2019		« add »	nth

The Links section

The links section allows you to display all scanned URLs and their status.

Search messages Delete events Execute analyze task Search analyze task Search analyze task ID Status Message Date Task Sender Execute analyze task Conte task 680 Message DA21B101A4A 1 13:52:29 2019-02:11 15:46:01 Id dtouzeau@gmail.com http://r3.red123.ru/c/da57dc555e50572d?s1=13606. HTML 683 MCK AF285101AAA 1 14:47:05 2019-02:11 16:18:02 Id dtouzeau@gmail.com https://otx.alienvault.com/pulse/5c617cf27bf4ce. HTML 684 MCK AF285101AAA Search in history 2019-02:11 16:18:02 Id dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 MCK AF285101AAA 1 14:47:05 2019-02:11 16:18:02 Id dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 691 MCK AF285101AAA 1 14:47:05 2019-02:11 16:18:02 Itme when the task analyze URLS txalienvault.com/usetsmizeScale HTML 692 MCK AF285101AAA 1 14	
Delete events Execute analyze task Execute analyze task Sender Execute analyze task Sender Execute analyze task Sender	Go!
ID Status Message Date Fask Sender task Sender task Content 680 A Pressing DA21B101A4A 13.52.27 2019-02-1115-46.01 Gl dtouzeau@gmail.com http://r3.red123.ru/c/da57dc555e50572d?s1=13606. HTMI 683 doK AF285101AAA 14:47.05 2019-02-1116:18:02 Gl dtouzeau@gmail.com http://txalienvault.com/pulse/5c617d27bf4ce HTMI 683 doK AF285101AA 14:47.05 2019-02-1116:18:02 Gl dtouzeau@gmail.com https://otx.alienvault.com/pulse/5c617d27bf4ce HTMI 684 doK AF285101AAA Search in history 2019-02-1116:18:02 Gl dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTMI 690 utok AF285101AAA Search in history 2019-02-1116:18:02 Gl dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTMI 690 utok AF285101AAA 14:47:05 2019-02-1116:18:02 Gl dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTMI 691 utok AF285101AAA 14:47:05	
680 18 Phashing DA21B101A4A 13:52:29 2019-02:11 15:46:01 4 douzeau@gmail.com http://t3:red123:ru/c/da57dc555e50572d?s1=13606. HTML 683 dok AF285101AAA 14:47:05 2019-02:11 16:18:02 68 douzeau@gmail.com http://t3:red123:ru/c/da57dc555e50572d?s1=13606. HTML 683 dok AF285101AA 14:47:05 2019-02:11 16:18:02 68 dtouzeau@gmail.com https://otx.alienvault.com/pulse/5c617df27bf4ce HTML 688 dok AF285101AAA Search in history 2019-02:11 16:18:02 61 dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 dok AF285101AAA Search in history 2019-02:11 16:18:02 61 dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 dok AF285101AAA 14:47:05 2019-02:11 16:18:02 61 dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 691 dok AF285101AAA 14:47:05 2019-02:11 16:18:02 61 Time whenn the task anallyze URLs bxalienvault.com/usub	^{1t-} {Ttl_m
683 idox AF285101AAA idox 14:47:05 2019-02-1116:18:02 idduzeau@gmail.com https://otx.alienvault.com/pulse/5c617cf27bf4ce HTML 685 idox AF285101AA 2019-02-1116:18:02 idduzeau@gmail.com https://otx.alienvault.com/pulse/5c617cf27bf4ce HTML 688 idox AF285101AA Search in history 2019-02-1116:18:02 idduzeau@gmail.com https://otx.alienvault.com/pulse/5c617cf27bf4ce HTML 690 idox AF285101AAA 2019-02-1116:18:02 idduzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 idox AF285101AAA 2019-02-1116:18:02 id douzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 idox AF285101AAA 2019-02-1116:18:02 id reseau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 691 idox AF285101AAA 14:47:05 2019-02-1116:18:02 id trainaliyze URLS trainervault.com/usubscribe/2ed6ad63 HTML 692 idox AF285101AAA 14:47:05 2019-02-1116:18:02 id trainaliyze URLS trainaliyze URLS <t< td=""><td>2019-</td></t<>	2019-
685 14 OK AF285101AA 2019-02-11 16:18:02 31 dtouzeau@gmail.com https://otx.alienvault.com/pulse/5c617cf27bf4ce HTML 688 14 OK AF285101AAA Search in history 2019-02-11 16:18:02 31 dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 14 OK AF285101AAA 14:47:05 2019-02-11 16:18:02 31 email com https://twitter.com/intent/tweet?url=&original HTML 691 14 OK AF285101AAA 14:47:05 2019-02-11 16:18:02 64 Time when the task anallyze URLS btxalienvault.com/settings HTML 692 14 OK AF285101AAA 14:47:05 2019-02-11 16:18:02 64 Time when the task anallyze URLS btxalienvault.com/settings HTML	2019-
688 14 OK AF285101AAA Search in history 2019-02-1116:18:02 Cl dtouzeau@gmail.com https://twitter.com/intent/tweet?url=&original HTML 690 16 OK AF285101AAA 1 4:47:05 2019-02-1116:18:02 Cl Remail com https://twitter.com/intent/tweet?url=&original HTML 691 16 OK AF285101AAA 1 4:47:05 2019-02-1116:18:02 Cl Time when the task analyze URLS btxalienvault.com/unsubscribe/2ed6ad63 HTML 692 16 OK AF285101AAA 1 4:47:05 2019-02-1116:18:02 Cl Time when the task analyze URLS btxalienvault.com/unsubscribe/2ed6ad63 HTML	2019-
690 100K AF285101AAA 14:47:05 2019-02-11 16:18:02 61 Gemail conbttps://otxalienvault.com/api HTML 691 100K AF285101AAA 14:47:05 2019-02-11 16:18:02 61 Dtxalienvault.com/unsubscribe/2ed6ad63 HTML 692 100K AF285101AAA 14:47:05 2019-02-11 16:18:02 61 Dtxalienvault.com/unsubscribe/2ed6ad63 HTML 692 100K AF285101AAA 14:47:05 2019-02-11 16:18:02 61 Dtxalienvault.com/settings HTML	2019-
691 Image: Constraint of the second seco	2019-
692 AF285101AAA (14:47:05 2019-02-11 16:18:02 (analyze URLS ptxalienvault.com/settings HTML	2019-
	2019-
693 et ok AF285101AAA 1 14:47:05 2019-02-1116:18:02 (3) acouzeausgman.com mtps://www.alienvault.com/legal/privacy-policy HTML	2019-
694 AF285101AAA 👔 14:47:05 2019-02-1116:18:02 🔄 dtouzeau@gmail.com https://otx.alienvault.com/static/email_assets/ HTML	2019-

SMTP STATISTICS

Refused messages

- \checkmark You can display graphs on refused messages in order to analyze your SMTP security rules.
- \checkmark On the left menu, click on SMTP router and refused menu.
- ✓ The first tab allows you ti see a pie chart in the top 10 of blocked reason.
- ✓ On the right side, the table display the number of messages blocked.
- ✓ If you click on the link, you can display all messages that matches the specified blocked reason.

## Dashboard	Refused		
E Your system			
A Network	Statistics Events		
S DNS	P Refused/Description	re ou	hits
SMTP Router	Disconnect after DATA	Hostname not found	32 438
🖗 Status	Reverse not found	rbl:Artica Reputation	7 387
	Disconnect after EHLO rbl:Barracuda Reputation	Disconnect after AUTH	6 160
\$ Parameters	Timed Out	Relay Timed Out	2 892
Routing & network	Connection Timed Out Relay Timed Out	Connection Timed Out	2 638
IP reputation	Disconnect after AUTH	Timed Out	1819
▼ SMTP rules	Hostname not found	rbl:Barracuda Reputation	1298
The station All to Bee		Disconnect after EHLO	1 100
Refused		Reverse not found	792
Policies service	rbl:Artica Reputation	Disconnect after DATA	570
Les Statistics			

 \checkmark You will see a chart that display blocked messages per hour for the current week



Page: 31



SMTP INVESTIGATION

Each day the SMTP events log is saved in the backup logs directory. If you need to retreive the history of some SMTP transaction you can use the tool "Investgate"

On the top menu, click on Search transactions.

SMTP Transactions	Search transactions	() 00:43:04	📕 Cpu:10.4% Mem:42.6%	양 N

Click on the settings icon on the search field

Messag	ing inv	estiga	te	
This section allows	you to search so	mething in the	history mail events in order to investigate from a specific issue or question	
				}
Search messages	5			Go!

You can define in settings how many last days your search will be found Define the max lines that will be disaplyed in the final search.

Options				×
Options				
	last days:	- 15	+	
	Max lines:	- 200	+	
	/		« Apply »	

- ✓ In the search messages, put a string that you want to find in events.
- ✓ This should be a name, an email address, a domain...(the "*" character is supported)
- ✓ If you want to put regular expressions, use "regex" suffix

Examples:

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


After run the query, a table is displayed and shows you all transactions that matches your search string..

Mes This secti	ion allows you to search	vesti something	gate	ry mail events in order to investigate from a specific issue or question		
*@artic	a.fr				Go!	¥
	Time	Service	Process ID	Last Days 15 200 Max Lines		
DEFERRED	Yesterday 16:10:18	smtp	18436	$\frac{79B0410160B: to={}^{\circ}christian.gournay@artica.fr*, relay=none, delay=96186, delays=96186, delays=96186, delays=96186, delays=96186, delays=96186, dela$	5/0.02/1 host)	./0,
DEFERRED	Yesterday 16:10:18	smtp	18430	BF713102537: to=«info@artica.fr», relay=none, delay=367048, delays=367047/0.01/1/0, status=deferred (connect to 37.187.142.164 [37.187.142.164]:25: No route to host)	dsn=4.4	.1,
DEFERRED	Yesterday 16:10:18	smtp	18433	CEC2610257D : to=«contact@artica.fr», relay=none, delay=364318, delays=364316/0.01/ status=deferred (connect to <u>37.187.142.164 [37.187.142.164]</u> :25: No route to host)	/1/0, dsn	=4.4.1,
DEFERRED	Yesterday 16:10:18	smtp	18437	AEE67102115 : to=«vlas12002@artica.fr», relay=none, delay=64509, delays=64508/0.02/ status=deferred (connect to <u>37.187.142.164 [37.187.142.164]</u> :25: No route to host)	1/0, dsn	=4.4.1,
REJECT	Yesterday 15:01:59	smtpd	13867	NOQUEUE : reject: RCPT from mailperd034.emw01.net[83.136.209.34]: 554 5.7.1 Service Client host [83.136.209.34] blocked using rblquery.artica.center: Artica Reputation; from=«bounce2@emw01.net » to=«david.touzeau@artica.fr» proto=ESMTP helo=«mailperd034.emw01.net»	unavaila	able;
DEFERRED	Yesterday 15:00:17	error	9038	$\frac{813851007BE: to= \ensuremath{sgelon}\xspace{\ensuremath{gelon}\xspace{\ensuremath{sgelon}\xspace{\ensuremath{gelon}\$, dsn=4.4 . 164]:25	.1, : No
DEFERRED	Yesterday 15:00:17	error	9038	$\label{eq:2.1} \begin{array}{l} 9D25A1025D2: to={$$$$ cselon@artica.fr}, relay=none, delay=434963, delays=434962/1.1/0/(status=deferred (delivery temporarily suspended: connect to $$$ 37.187.142.164 [37.187.142] route to host) \end{array}$	0, dsn=4. . 164]:25	4.1, : No

NOTIFICATIONS

- The MTA is able to send notifications to messaging team depends on different context.
- To manage notifications, go into SMTP Router / Parameters.
- Select Postmaster / Template tab.

The first part of the form allows you to set recipient / Senders of notifications

Postmaster:

The email address used to receive notifications.

Unknown Users:

If you want to relay messages for non-existent users (instead of refuse messages), set an email address.

Notifications Sender address:

The email address used to send notifications (eg: when an email is failed to be routed) The sender address of postmaster notifications that are generated by the mail system All mail to this address is silently discarded, in order to terminate mail bounce loops

eMail for sender notifications:

The sender address to use in address verification probes; prior the default was "postmaster"/ To avoid problems with address probes that are sent in response to address probes, the MTA server excludes the probe sender address from all SMTPD access blocks. Specify an empty value or <> if you want to use the null sender address/ Beware, some sites reject mail from <>, even though RFCs require that such addresses be accepted

Bounce notice recipient:

The recipient of undeliverable mail that cannot be returned to the sender

Notifications error recipient:

The recipient of postmaster notifications about mail delivery problems that are caused by policy, resource problems, software problems or protocol errors

Notifications Delays recipient:

The recipient of postmaster notifications with the message headers of mail that cannot be delivered

Empty recipient address:

The recipient of mail addressed to the null address. The MAT does not accept such addresses in SMTP commands, but they may still be created locally as the result of configuration or software error"

What trouble to report to the postmaster

You can define here notifications family that the MTA have to send to the Notifications error recipient

Undeliverable mail:

Send postmaster copies of undeliverable mail. If mail is undeliverable, a so-called single bounce message is sent, with a copy of the message that was not delivered. For privacy reasons, the postmaster copy of a single bounce message is truncated after the original message headers. If a single bounce message is undeliverable, the postmaster receives a double bounce message with a copy of the entire single bounce message

Double bounces:

Send double bounces to the postmaster

Policy:

Inform the postmaster of client requests that were rejected because of (UCE) policy restrictions. The postmaster receives a transcript of the entire SMTP session

Protocol:

Inform the postmaster of protocol errors (client or server side) or attempts by a client to execute unimplemented commands. The postmaster receives a transcript of the entire SMTP session

Resource problems:

Inform the postmaster of mail not delivered due to resource problems (for example, queue file write errors)

Software problems:

Inform the postmaster of mail not delivered due to software problems



Notifications templates

On the left part of the form, you can personalize 4 notifications templates

On each template you can define:

- The Charset used by the notification.
- The From address
- The Subject of the notification.
- The content of the message

Charset:	Western European (ISO)
From:	MAILER-DAEMON (Mail Delivery System)
Subject:	Undelivered Mail Returned to Sender
Postmaster-Subject:	Undelivered Mail Returned to Sender
content:	 This is the mail system at host \$myhostname. I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below. For further assistance, please send mail to postmaster. If you do so, please include this problem report. You can 6 delete your own text from the attached returned message.
	« Apply »

This section allows you to manage the SMTP service that is in charge t Messages can be transfered to remote server or to the local service in

Parameters	Postma	ster/Templates	TLS/SSL
 Template: failure Template: Delay t Template: success Template: verify t 	template template s template template	Postmaster	
		Define ema	ils addresses and no
			Post



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

Remote Synchronization:	3.1.2			
CurlFtpFS:	0.9.2			
Web services				
NgInx Web engine:	-	🛃 İnstall	orupdate	
Wordpress system client:		🛃 Install	or update	
Messaging				

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

Wordpress system client	×
Wordpress system client 2.1.0 1.09 MB	Install or Upgrade

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

Artica Core server	Operating system Python packages
Software	Version
Wordpress system client:	2.1.0 Linstall or update



Install the NgInx Web engine

In the same way of the Wordpress client, checks the "NgInx Web engine" version and installation

Web services			
NgInx Web engine:	-	🛓 Install or update	
Wordpress system client:	2.1.0	NgInx Web engine	×
Messaging		Natury Web engine 1136.2 601 MB	+ Install or Llograde
Postfix MTA Mail system:	3.3.0		
msmtp (SMTP client):	-		
Milter-greylist:	-	L Install or update	

- 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

Insta This section	Il or uninstall features allows you to install/uninstall available features on your server	
select -	Expand	web 🗶 🗸
Status	Software	Action
	Wordpress websites	Require installed NgInx Veb engine
Uninstalled	NgInx Web engine	✓ Install
	Advanced Web Proxy access rules	▲ Not installed

• Click on Install on the Wordpress Websites row

Uninstalled	Wordpress websites	↓ Install	
Installed	NgInx Web engine	✓ uninstall	



CREATE YOUR FIRST WORDPRESS WEBSITE

- On the left menu, go to **Web services / Wordpress websites** Click on the button "**New Wordpress website**"

Manager Administrator →	E Search a computer, a m	embei	() 18:19:44	📳 Cpu:1.7% Mem:35.6%	² 양 Members	June 10 Logout	š III.
Dashboard	Wordpress v	vebsites v	.5.0.2				
🚍 Your system	Artica For WordPress allows	ou to deploy Wordpr	ess websites thro	ugh it s interface.			
🚓 Network	It able to backup/restore your The tab Wordpress websites a	websites, enforce sec llows you to display s	curity and maintai tatus of all your V	in updates. Vordpress sites.			
S DNS	-						
© Web services	+ New Wordpress website	Reconfigure se	ervice				
🕰 Status					Search	٩	*
Mordpress websites	Wordpress Websites	Saved On	Service	Server Names Typ	e Destinati	on	
All websites			N.1	1.			
Requests			No	results			
🛎 Statistics							
D .							

- Set your web site name in Web server name field.
- Define the administrator of the new web site name.
- Set it's email in order to create certficate or notifications.

lew Wordpress website		
Web server name:	web.artica.center	<u>ا</u> ً
Administrator:	david.touzeau	
Administrator email:	david@articatech.com	
Password:	•••••	Ð
	•••••	۹
		« 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 through the Wordpress Web console.

In this way, modify the password in this section helps you to recovery your Wordpress adminisrator password.



DOMAINS ALIASES

If you plan to accept multiple domains for your wordpress site :

- Click on the sitename in the table.
- Open the aliases tab

Set all domains you want your Wordpress accept.

articatech.info					×
articatech.info	Aliases				
Aliases					
1 www.articat 2 articatech 3 www.articat	ech.info org ech.org				
				« Apply »	

ENABLE OR DISABLE A WEBSITE

Enable or disable a website make it available or unavailable on the Net. You can enable/disable by check/unckeck the checkbox in the enabled column.

After enabled or disabled your select websites, click on the "Reconfigure service" button in order to make your changes in production mode.

+ New W	ordpress website 🔒 Reconfigure service	
		Search Q -
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 🔽 📋

Addresses Rewriting, 11 Advanced Monitoring service, 75 Aes256.51 Artica reputation database, 13 AUTH Link, 59 authentication box, 142, 143, 144, 146 Authentication Portal, 159 Auto-Whitelist, 27 Background logo, 60 Backup on the fly, 27 **Basic Authentication**, 149 Cache, 175 Caching Internet objects, 175 Clock, 45 Cluster, 169 Common Name, 25 Community Edition, 17 CPU usage, 74, 138 Deep packet inspection, 242 Default password, 93 Delete stored objects, 177 Disclaimer, 27 DKIM, 22 DMARC, 22 DNS amplification, 124 DNS Filter, 103 DNS Load-balancing, 103 DNS Over HTTPS, 117, 119 DNS Over TLS, 107 DNSBL, 13 DNSCrypt, 117 DOH. 117. 119 Domain-based Message Authentication, 22 DomainKeys Identified Mail, 22 ElacsticSearch, 238 ElasticSearch database, 238 Enterprise Edition, 17 ESXi. 10 Exchange 2010, 9 Fail to ban, 20 Fail2ban, 3, 20 Gateway, 33 GeoIPUpdate, 98 Gmail, 16 Google Chrome, 156 Gpmc.msc, 156 GPMC.msc, 157 GPO, 156 Graphs, 31 HaCluster, 169 Hospitals, 166 Hostels, 166 Hostname, 60 Hosts file, 31 HotSpot, 166, 168 HTML code, 180, 181, 190 HyperV, 10 Identical domains, 7 In-addr.arpa, 106 Incidents, 74 install-manuall. 12 Interfaces connectors, 34 Internet Explorer 11, 156 ISO, 10 Join interfaces only, 34 Kerberos, 150 krb5.keytab, 151 KVM, 137 language, 58 LDAP, 85, 86, 87, 142, 146 Legal log, 138 Let's Encrypt, 24 LibreNMS, 110, 221 Listen ports, 129 Load, 73 Load-balancing, 125, 169 Log rotation, 138 Login page, 60 Logs Viewer, 82 Malware, 141 Masquerade, 34 Memory swapping, 52 Microsoft Windows Updates, 177 Multi-Domains, 85 Multiple internet connections, 39 Never direct, 197

NTOPNG, 69 NTP server, 48 NTP Time Client, 46 Nutanix, 10, 137 Office365, 16 OpenDKIM mail filter, 24 Optimize, 36 Parent proxies, 196 Pfx file, 28 Phishing, 141 Port 443, 61 Port 465, 9 Postfix MTA Mail system, 5 PowerDNS recursor, 111 PowerDNS system, 111 Privileges, 63 Proxmox, 137 Proxy.pac, 129, 228 Public Blacklists databases, 14 PuTTY, 94 RADIUS, 146 RBL, 13 RDP, 229 RDS, 229 Real-time Asset Detection System, 68 Red Error page, 190 Regular expressions, 16, 32 Remote ports, 134 Reset. 62 Reset parameters, 13 RESTful, 80, 90, 111, 158, 203, 205 Reverse DNS, 112 RFC 1918, 48, 132 Round-robin, 32 Routing, 7 Rsync, 66 Safe Browsing, 141 sAMAccountName, 149 Shared category, 213 Silent Authentication, 147 Skin, 60, 180 Skin Web-filtering error page, 190 Snapshot, 50 SNMP, 220, 242 SNMPv2, 80 SNMPv3,80 SOA record, 112 Spoofing, 27 SSH, 93, 97, 98 Statistics, 222 Support Package, 136 SWAP, 52 Syslog, 100 TCP BBR, 36 TCP Compressor, 201, 202 TCP Packet inspection, 2 TCP performance, 37 TCP windows size, 38 Templates, 179, 190 Templates Manager, 180 Time client, 45 Time server, 45 Time zone, 45 Title, 60 Traffic analysis Daemon, 69 TSE Client, 229 UDP 161, 80 Unbound, 103 Upstream proxy, 196 User-Agent, 192 Version of Artica, 60 Virtual Group, 185 VMware, 10 Voucher, 166 Wan Proxy compressor, 200 Watchdog, 35, 73, 138 Web Proxy Autodiscovery Protocol, 228 Wi-Fi accesses, 166 Windows 2019, 148 Wordpress Administrator password, 38 Wordpress system client, 36 WPAD, 129, 228 www.speedtest.net, 134 XenServer, 10 Yahoo, 16 Zabbix, 78