Protect Business Data From Theft and Ransomware, and monitor for intrusions with alerts using:

Authonet Zero Trust Network Access (ZTNA) Cybersecurity

Authonet ZTNA Gateway Cybersecurity Protection and Product Operation Manual

November 2023

Protect Business Data From Theft and Ransomware, and monitor for intrusions with alerts using:

Authonet
Zero Trust Network Access
(ZTNA) Cybersecurity Gateway

Authonet ZTNA Gateway
Cybersecurity Protection and Product Operation Manual

This manual was prepared by Fire4 Systems (UK) Ltd for the Authonet ZTNA range of cybersecurity products

Last revision: September 2023

If you have any questions or comments about the contents of this manual please send them to: info@authonet.com

Authonet Zero Trust Network Access (ZTNA) Cybersecurity Gateway: Cybersecurity Protection and Product Operation Manual

Contents

PART 1:

What is Cybersecurity and why do we need it?

All Businesses are at Risk from Cyber Criminal Theft

Businesses always have a risk of physical theft; criminals can break into the building and steal items or money. Businesses respond by putting locks on doors and windows, and installing CCTV with intruder alarms. Physical security has a cost but it is much less than the losses due to theft. If a business owner wants property insurance then the insurers will first verify that the business has physical security systems in place, and if not will request security measures before issuing the insurance. The insurer will also check periodically that the security measures are being used correctly.

Now businesses rely on computers to operate; the business information is stored on the business computer network. This business data is a target for cyber criminals who can break into the computer system and commit crimes.

- Theft: Steal the business data and sell it, data has a value if it has proprietary information about some product that the business makes, or else it has personal information about people that can be sold such as credit card information or social security information that can be used for identity theft.
- Extortion: Cyber criminals use a technique called ransomware to lock the business data and make it inaccessible. This will stop the business operating. The criminal will then demand a ransom to give the key, which will release the data so that the business can continue operating. Ransomware attacks are increasing quickly as ransomware extortion has become very popular with cyber criminals because it puts a lot of pressure on the business owner to quickly pay what the criminal is demanding. Ransomware is an easy method of extortion for the criminal and most small businesses pay the ransom, as they are not prepared for the attack.
- Some cyber criminals will use both theft and extortion when they attack a business.

The first cyber attackers were individuals and small groups of individuals who hacked into businesses to cause disruption rather than theft. Criminals saw what the hackers were doing and began using the techniques of breaking into a business or government computer network to steal information that they could then sell. At some point the criminals developed a method of extortion using ransomware techniques. Today cyber criminals can be identified in three groups.

- Gangs of criminals with programming skills who use the skills to break into business computer networks to steal and extort a ransom.
- Organized crime gangs that can contract technical services for theft and extortion, the criminals with programming skills offer “ransomware-as-a-service” (RaaS) to the organized crime gangs and take a percentage pf the money extorted. The gangs and organized crime are located in rogue states where law enforcement has no access.

- Rogue states that operate criminal activities to steal information, usually trade secrets, to copy products, and also theft of crypto currency and extortion to fund criminal activities. These states are known and many governments restrict or ban commerce with these states.

In the past, cyber criminals attacked only large businesses so that they could steal or extort millions or tens of millions of dollars. Today most large businesses have invested in cybersecurity; hiring specialists and purchasing security tools. It is now very difficult for a cyber criminal to attack a large business.

Cyber criminals instead began attacking small and medium businesses that did not invest in cybersecurity and so were very easy to attack with theft and extortion. The value of the theft or extortion on a small business is less than the attacks on big businesses and is in the range of tens to hundreds of thousands of dollars. The cyber criminals make up for their reduction in the money obtained with each attack by attacking many more businesses. The cyber criminals have automated the attack process so that each attack can be done much faster.

The small businesses that are most at risk are those that store personal client information, because they will pay the ransom quickly to recover that information. Some examples of target business that store a large amount of personal and business client information are listed below.

- Healthcare.
- Law firms.
- Financial firms.
- Education.

Small businesses that have proprietary information are also at risk. Release of confidential information might seriously damage the business, which pressures the business owner to pay the ransom quickly. Examples of these businesses are listed below.

- Manufacturing.
- Software.

Some interesting statistics about cyber crime attacks on small and medium businesses are listed below.

- 120% increase of business ransomware attacks year over year.
- 20% of attacked businesses paid the ransom but did not recover the data.
- 12 days average business downtime during a ransomware attack.
- 85% of successful ransomware attacks are made via phishing.
- 51% of small businesses have no cybersecurity measures.
- 20% of global cyber crimes in 2022 were due to ransomware.

- 47% of 2022 ransomware attacks were to US businesses.
- $570K was the average small business ransomware payment in 2021.
- 60% of executives believe the ransomware threat is exaggerated.
- 20% of small businesses have implemented multi-factor authentication.
- 82% of ransomware attacks in 2021 were to smaller businesses.
- 22% of small businesses increased cybersecurity spending in 2021.
- 87% of small businesses attacked had customer data compromised.
- 700,000+ small businesses suffered cyber attacks in 2020.
- 55% of people in the U.S. are less likely to buy from a breached business.

Cybersecurity has a cost like physical security, but that cost is much less than the cost of a data theft or a ransomware attack. A business owner can get cyber attack loss insurance, however the insurers will first verify that the business has cybersecurity systems in place, and if not will request cybersecurity measures before issuing the insurance. The insurer will also check periodically that the cybersecurity measures are being used correctly.

No cybersecurity measures can stop a highly skilled and determined cyber criminal, however the probability of a cyber attack will be much lower. Comprehensive cybersecurity measures will be a strong deterrent to persuade most attackers to move on. In the estimate of many cybersecurity professionals a properly structured and implemented cybersecurity plan can reduce the probability of a cyber attack on a business by 98%. A business always needs a ransomware recovery plan for the small chance that the cyber attack will be successful.

Any type of cybersecurity product or system can only be effective when configured correctly by a cybersecurity professional. Businesses that are upgrading their cybersecurity installation must ensure that they hire qualified professionals to install and configure the equipment.

Methods of Computer Network Attack Used by Cyber Criminals

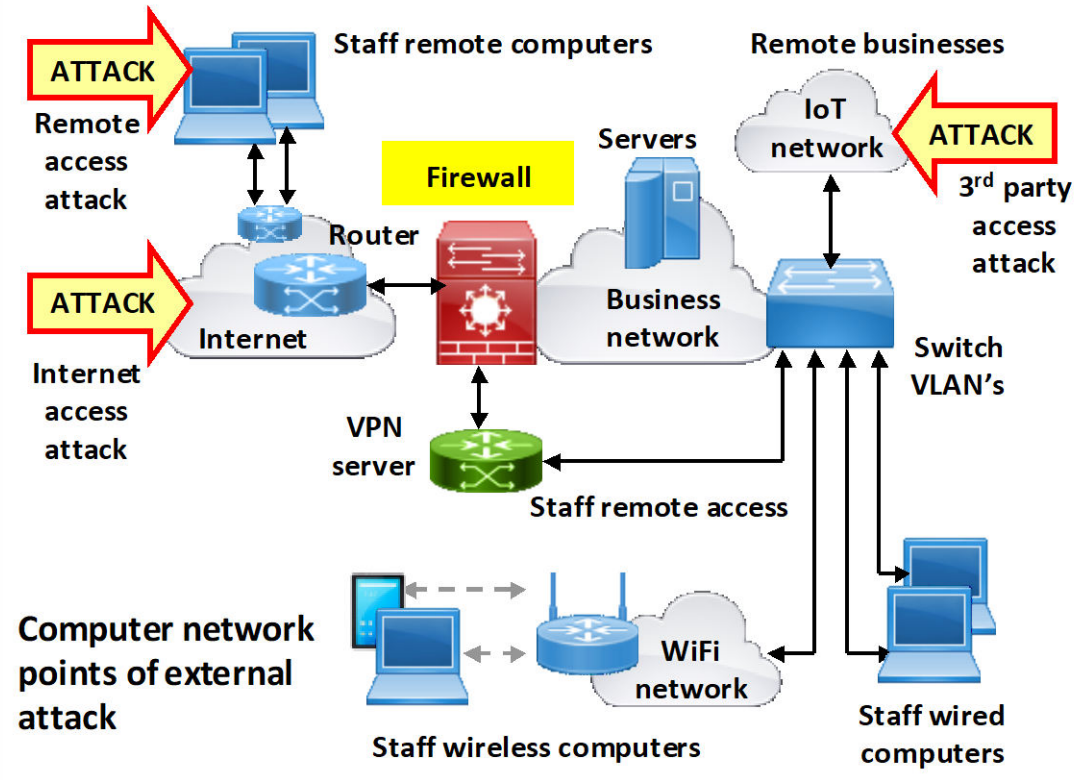
There are two methods of cyber attack, an external threat, and an internal threat. An external cyber attack is an attempt by the cyber criminal to access the business network remotely, there are several channels.

- Break through the Internet router using a known exploit.
- Break into an access port that is used by remote employees, usually by stealing a password through social engineering.
- Break into a third party computer system that is connected to the business network (e.g. B2B) and then get access to the business network.

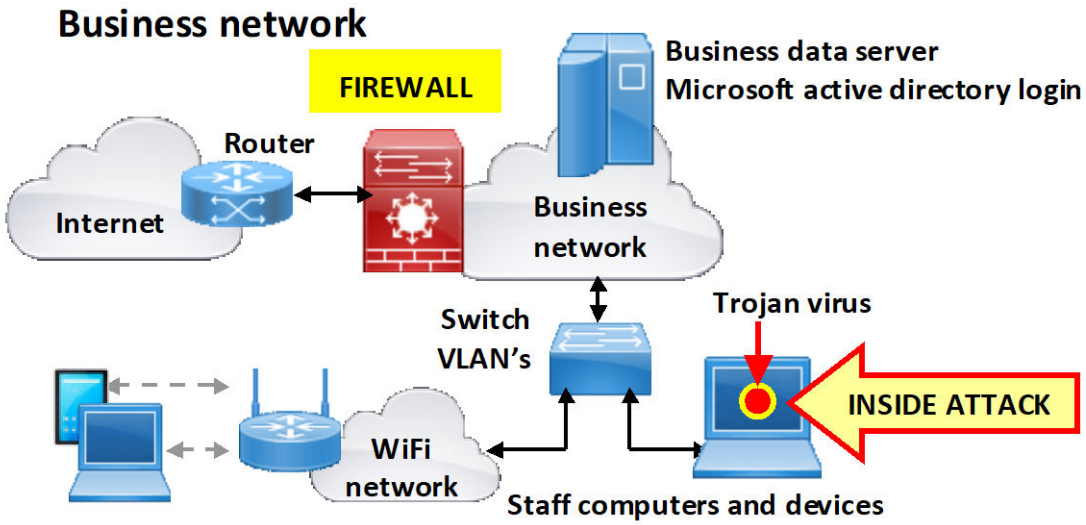
The success or failure of the external attack depends on how well the business has installed cybersecurity.

- A firewall will block access from the Internet.
- Multi-factor authentication to protect remote employee access, a code (one time password, OTP) is obtained from a mobile phone to get access.
- An authentication method for a 3rd party data connection that imposes strict access rules.

Without cybersecurity the attack is easy. With good cybersecurity an external attack is almost impossible.



An internal attack is made when the cyber criminal is able to install software on a computer inside the business network, which gives the criminal remote access to that computer. This method permits the criminal to bypass the firewall and also bypass the server login credential because the criminal can access the server operating system directly and access the database through a known operating system weakness, called an exploit. The internal method of attack is very popular with cyber criminals and internal attacks account for approximately 85% of all successful ransomware attacks.

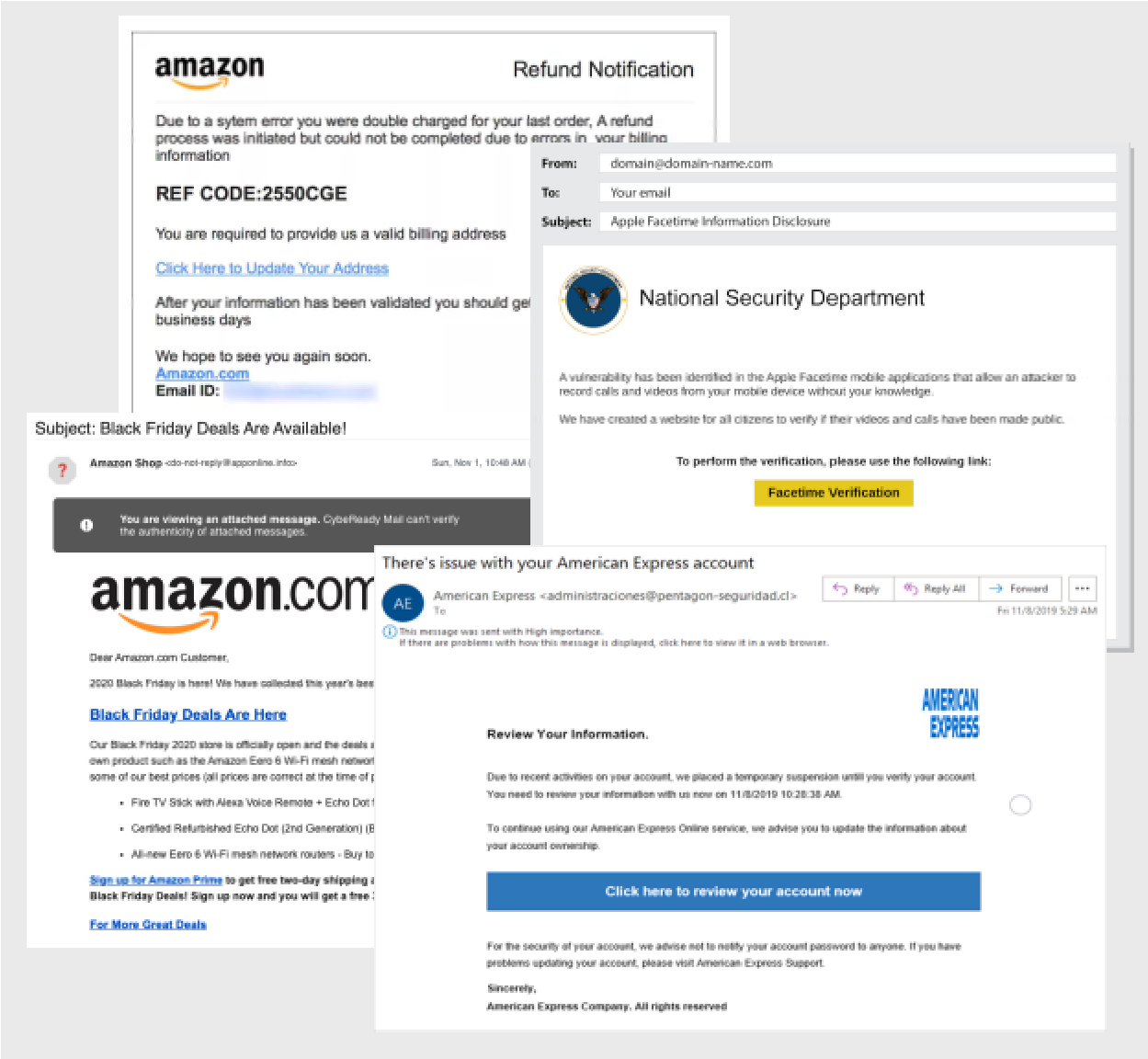


An internal attack requires the cyber criminal to trick a member of staff to install software on the computer that will give the criminal access to the computer and bypass the firewall. The cyber criminal uses a method called phishing to trick the business employee into installing the Trojan virus.

A phishing attack requires sending emails to many business employees. The messages impersonate some business or entity that the user recognizes. The message describes some problem that requires an urgent solution by clicking a link in the message.

The email link will call the cyber criminals computer server to download and install a Trojan virus. A Trojan virus is a small software program that gives the cyber criminal remote access to the users computer. The cyber criminal then has access to the computer network and data servers. The user is not aware that the remote criminal is using the computer to steal business data or plant ransomware to lock the business data.

The Trojan virus attack will bypass most security measures including the firewall and the server login such as Microsoft active directory. Phishing message examples are shown in the next figure.



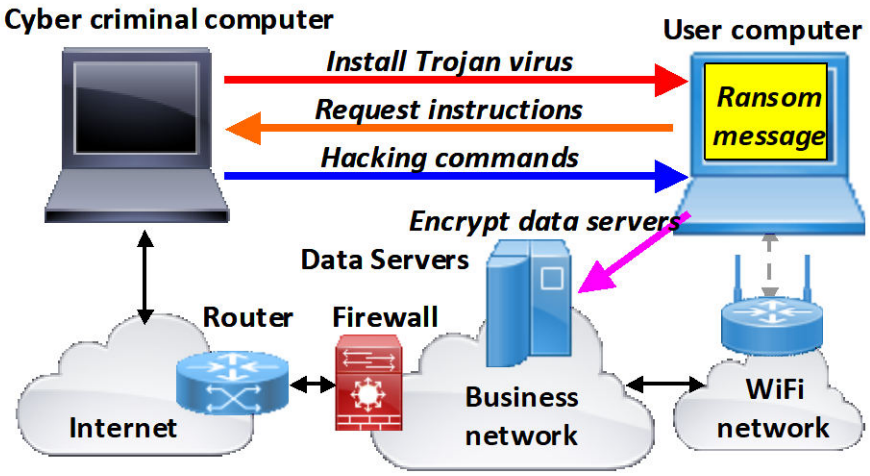
Phishing is the most frequently used method that criminals choose to launch a cyber attack for data theft or ransomware extortion and this method is successful 98% of the time. After installation, the Trojan virus gives the cyber criminal remote access to the computer and to all other computers and servers in the business network. The attacker will then look for known exploits with the server operating system. Quite often the business server has not been patched with the latest security updates. The procedure used by the cyber criminal after installation of the Trojan virus is listed below.

- The computer calls the cyber criminal bypassing the firewall.
- The cyber criminal replies to the message with instructions.

- The cyber criminal programs the computer to get access to the data servers.
- The user is not aware that the cyber criminal is using the computer in the background.
- The cyber criminal encrypts the server data files with ransomware.

Finally the cyber criminal puts a ransom message on the computer screen demanding a payment in crypto-currency to get the key that unlocks the data.

The phishing procedure is illustrated in the next diagram.



The steps of a Trojan virus ransomware attack:

1. **Criminal sends phishing emails with virus links**
2. **User is tricked to install the Trojan virus**
3. **Virus calls the criminal for programming commands**
4. **User is not aware the criminal is programming**
5. **The criminal encrypts the data servers**
6. **The criminal displays the ransom message**

In summary, a business faces two types of threat that cyber criminals use frequently to access the business network that has the minimum cybersecurity protection of a firewall.

- External attack via access through the network router or via a remote access channel using a stolen password.
- Internal attack using the phishing method.

Of these two the phishing method is the most common and used in 85% of successful ransomware attacks.

Protecting Businesses from Cyber Criminal Attacks

There are two important actions that a business must take in order to reduce the probability of a cyber attack.

- Employee training to recognize and alert a potential cyber attack. Most cyber criminals plan an attack through employees, with password theft or phishing. The employees are the first line of defense and so must be aware of attack techniques and must have access to a cybersecurity expert to report a potential attack that must be investigated immediately. The training should be repeated periodically. A business can call a cybersecurity consultant who can provide the staff training. Some cybersecurity consulting businesses offer on-line training courses for staff cyber attack awareness. Call us to provide contacts for staff cybersecurity training.
- Technical cybersecurity upgrades for the business network are required that will block access to what are considered the weak points where cyber criminals will try to attack. Most small and medium businesses do not have the technical network upgrades that are required to protect the business data. The technical upgrades are described in the section that follows.

In addition there are two further actions, listed below, that will help a business to minimize the probability of a successful attack.

- Move applications software and data to cloud storage. Cloud vendors spend a lot of money on cybersecurity and have some of the more talented professionals in the industry. Data is safer from attack in a cloud. Some software vendors have cloud versions of software that a business is using. Proprietary software will require migrating to the cloud by a specialist software business.
- Prepare a recovery plan to restore the business data in the case that a ransomware attack is successful and avoid paying the ransom. An IT service business or managed service provider can develop a recovery plan for any small or medium size business. The recovery plan includes making daily or hourly offsite backups, preparing hard drives for all computers and testing the plan.

Staff Cybersecurity Awareness Training

Business employees are the first line of defense. Cyber criminals will most likely attack the staff to get access to the business data; often with a phishing attack or attempted password theft.

The training helps staff recognize the signs of a cyber attack. Staff should have a hotline to call if an attack attempt is recognized. The hotline should be to a skilled IT person who can immediately investigate the threat. This person might be an external IT service provider or cybersecurity consultant. Once a threat is

identified the clock is counting until the criminal installs ransomware, so it is necessary to act quickly to remove the threat before it is too late.

The cybersecurity awareness staff training should include the following subjects;

- What is a cyber attack?
- Methods that cyber criminals will use to attack.
- Social engineering for password theft.
- The phishing process and how to recognize this attack.
- A ransomware attack explained and what the criminals expect.
- Damage that a cyber attack will do to the business.
- Additional security procedures required for cybersecurity protection.
- Precautions that staff must follow.
- Cybersecurity awareness document.
- Ask staff to report a possible attack using the hotline to the cybersecurity consultant.
- Ask staff members to identify improvements for the cybersecurity procedures.

It is important to encourage and reward staff support for participation with the cybersecurity awareness training, as staff are the first line of defense to identify potential risks. Never admonish a staff member who allows a phishing attack by mistake; criticism will prevent people alerting attacks.

Technical Cybersecurity Upgrades for the Business Network Infrastructure

Network infrastructure in any business usually has several weak points where the cyber criminal will attack. Each of the weak points is described in this section with a recommendation for a 6-step infrastructure plan to remedy the weaknesses.

The 6-step network infrastructure upgrade plan is as follows.

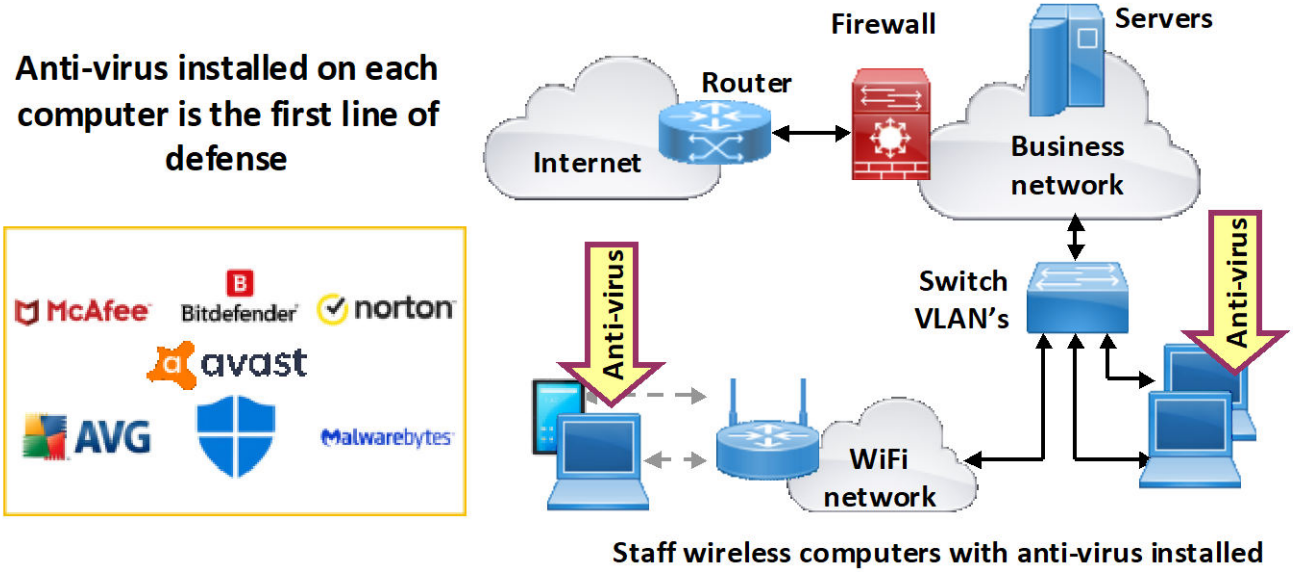
1) All staff computers must have anti-virus, and must be frequently updated.
2) Frequently update security patches for all software and firmware.
3) Install a firewall between the network and Internet and configure correctly.
4) Install a Zero Trust network access (ZTNA) security gateway between the network and all devices, local users, remote users and 3rd party connections with authentication rules for trusted devices and user access.

5) Allow users to access the network via the ZTNA gateway only with multi-factor authentication. At the minimum 2-factor authentication to ensure that only trusted people have network access.
6) Monitor network accesses at the end-point security and alert any attempted unauthorized access; use cloud management for remote monitoring by the IT service provider.

1) Install Anti-virus on each User Computer, Update Frequently

The attack technique most frequently used by cyber criminals is to install a Trojan virus on a user computer through a phishing message. The cyber criminal then has control of the computer. Anti-virus may block an attempt to install a Trojan virus if the user clicks on a phishing link. When this happens the user must advise IT security. The important anti-virus steps are listed bellow.

- Do not permit a computer to connect to the network without anti-virus installed.
- Ensure that all anti-virus installations are frequently updated with the latest versions.

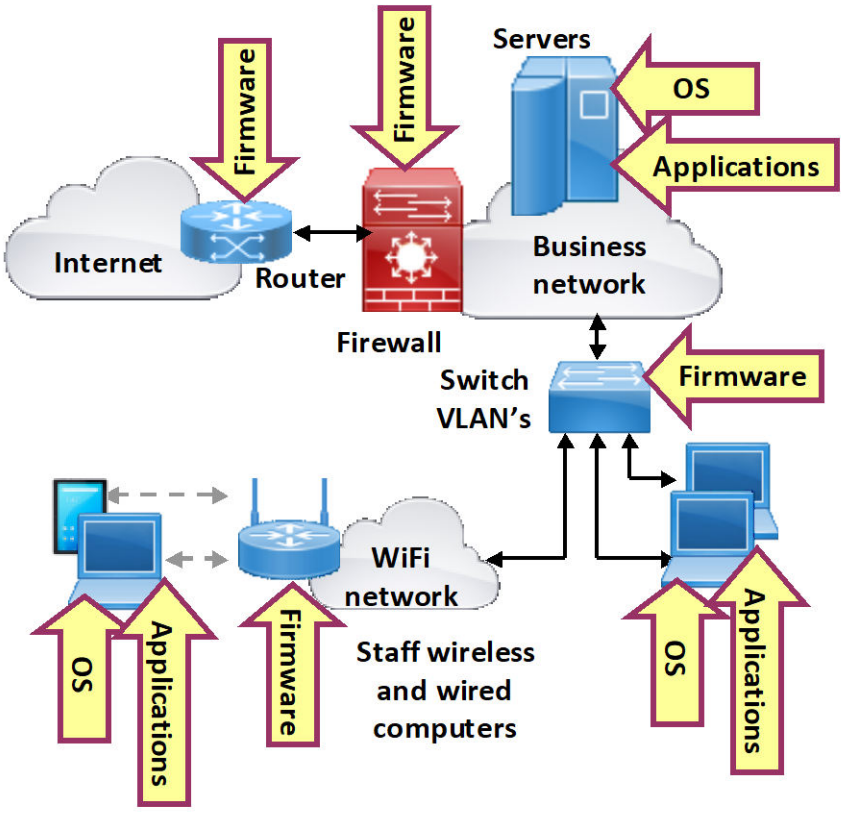


2) Frequently Update Software and Firmware Security Patches

All software and equipment vendors issue security patches when a security weakness has been found. Cyber criminals exploit the security weaknesses to attack the network. Some software vendors have automatic security patch updates; Microsoft Windows has automatic updating and cloud applications are updated automatically. However older versions of Windows must be updated to the most recent version as older copies are not updated. Most equipment vendors do not have automatic firmware updates.

Every company should have IT staff or an IT service provider who is checking for available software and firmware updates and installing them. The upgrade process should be a weekly exercise for all businesses. Big company IT departments will automate the process to roll out updates.

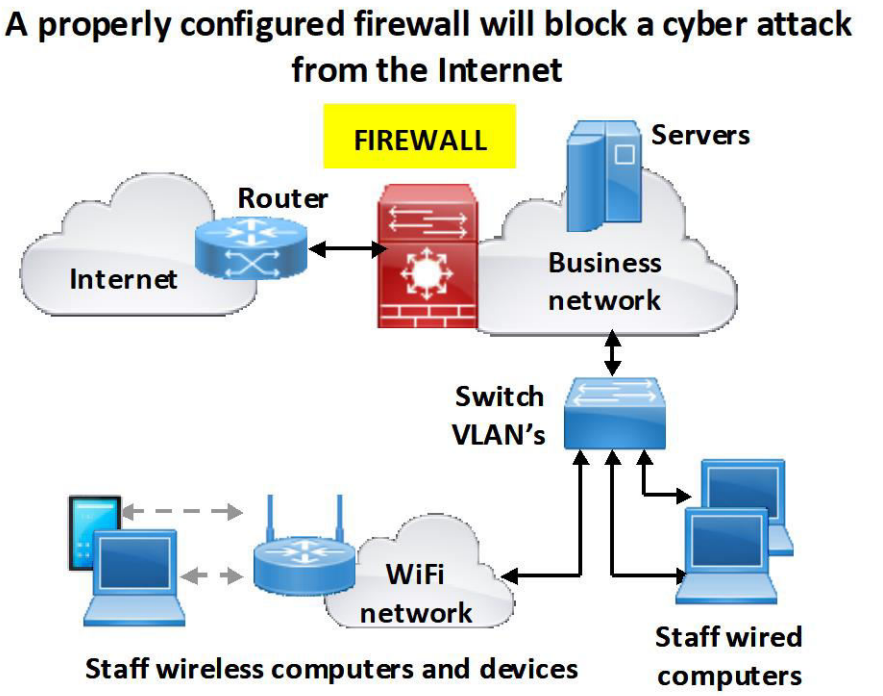
The arrows indicate the upgrade points where security patches should be checked on a weekly basis to ensure that the network is protected



3) Install a Firewall Between the Network and Internet

Reduce or eliminate the risk of an external attack to the network from the Internet by installing a firewall, many different firewall products are available. With no firewall installed the ISP router can be easily attacked because the cyber criminal identifies the router type and the vulnerabilities. Businesses do not update router firmware with the latest security patches so they are easy to attack. Once the cyber criminal has access to the router then server IP addresses can be identified for the ransomware attack. The cyber criminal then attacks the server using known software vulnerabilities. This is easy for the criminal if the business did not update the server software with security patches.

The firewall effectiveness depends on the configuration, so it is essential to call an expert to configure the product. The firewall firmware requires periodic updates with security patches.



4) Authenticate Devices and Users with Zero Trust Network Access

Zero Trust network access (ZTNA) security is implemented using a dedicated gateway product. Any device or user connecting to the network must always be authenticated before access is granted. 2-factor user authentication is essential.

Zero Trust Network Access (ZTNA) cybersecurity technology has the following characteristics.

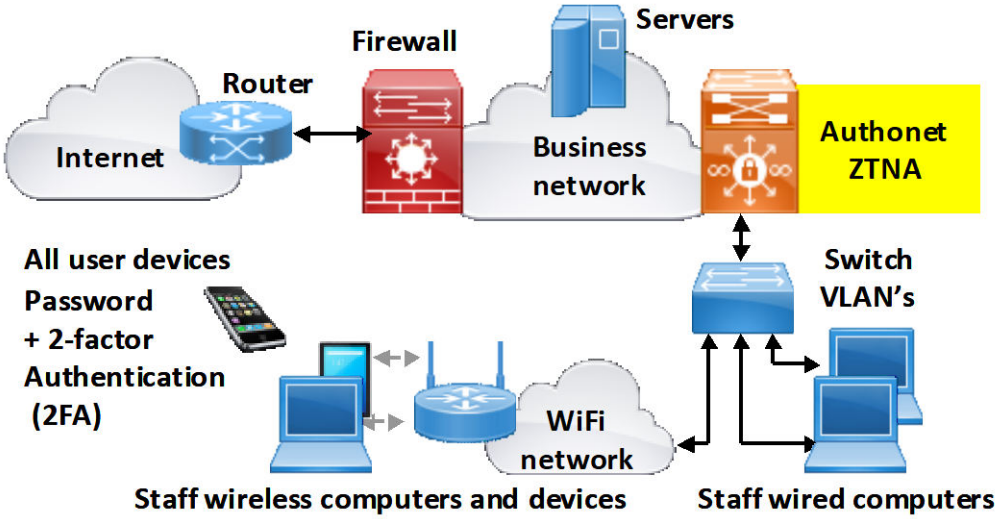
- Zero Trust network cybersecurity means never trust, always verify.
- All devices and users must connect through Zero Trust cybersecurity, which protects business data, software and infrastructure using strict protocols, and monitors network traffic for suspicious behavior or potential threats.
- Zero Trust has four principles that are implemented by a Zero Trust end-point firewall.
- Identity verification and authentication of every user and device that is attempting to access the network. Verification uses device identity checks and multi-factor authentication (MFA) of users.
- Users and devices are given access only to the specific network resources they need to perform their tasks in order to limit the potential damage that can be caused by a compromised device.
- Users have restrictions imposed for access to Internet services that block interaction with potential attack vectors and compromised websites.
- Continuous monitoring of network activity can identify potential threats and provides the opportunity to take effective action quickly.

Features of the Authonet Zero Trust gateway are listed below.

- Authentication rules.
    - Verify the MAC of the device, connection allowed.
    - Verify the MAC of the device, connection blocked.
    - Verify the MAC of the device, login required.
    - Unlisted MAC’s are always blocked.
    - Verify the user password, connection allowed.
    - Verify the user password, connection blocked.
    - Verify the user password, user requires MFA with OTP.
    - Optionally user access only with an allowed MAC (3FA).
- Filtering rules.
    - Specify allowed / blocked network IP range.
    - Specify allowed / blocked Internet public IP’s /domains.
- Monitoring.
    - Monitor status of devices in the LAN network.
- Reporting.

- List the authenticated users.
- List IP requests but not authenticated, check for intruder.
- List failed authentication, send alert to admin.

The details of the Authonet Zero Trust network access gateway that incorporates the network access rules is described in the next part of this manual.



Authonet Zero Trust Network Access (ZTNA)

- **All devices and/or users are physically isolated from the network until authenticated**
- **Once authenticated all devices and users are controlled and monitored**

5) Multi-factor Authentication and 2-factor Authentication

Cybersecurity experts agree that Zero Trust security with multi-factor authentication is the single most important investment that gives the biggest cybersecurity benefit. Many large businesses already have Zero Trust security with MFA. Most small and medium businesses do not have Zero Trust security and have no MFA.

With a Zero Trust Network Access end-point security gateway installed, user network access can be verified using multi-factor authentication. 2-factor authentication (2FA) is a subset of multi-factor authentication (MFA). Multi-Factor authentication is an essential part of Zero Trust.

Many people are familiar with 2FA as most banks require it to access account information. The procedure is simple and illustrated in the following figure.

- The user opens a login screen and enters a password.
- A one-time password (OTP) is obtained from the users personal phone, usually a 6-digit numerical code that is valid for a limited time.
- The user then enters the code in the login screen and gets network access.

2-Factor authentication procedure

2-factor authentication blocks cyber criminal access after a password theft as the stolen password cannot be used without the one time password (OTP) obtained from the users personal mobile phone. 2-factor authentication is a deterrent; when most cyber criminals see that the network has 2FA they give up and move on to the next victim. In addition, any business seeking cybersecurity insurance will be requested by the insurers to install 2FA network protection.

Most large businesses implement 2-factor authentication as part of their cybersecurity plan to protect the business data files from cyber attack. However most small businesses do not have 2-factor authentication and are therefore susceptible to cyber attacks.

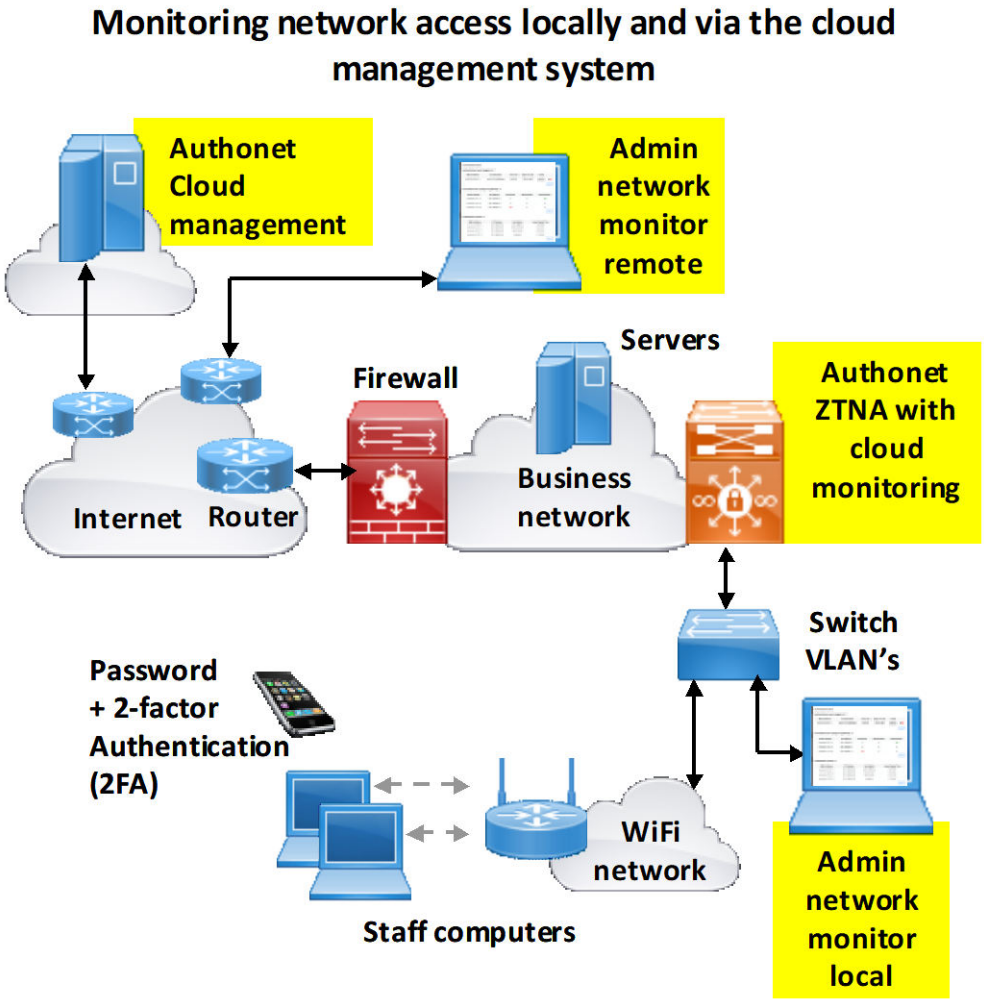
3-factor authentication adds a third parameter to authenticate the user; this is the identifying parameter of the computer that the user is connecting with. The identifier can be a MAC address, which is unique; a combination of MAC plus OS plus browser identifiers; or it can be an authentication app installed on the computer with an encrypted key that is recognized by the cybersecurity system.

6) Monitor Network Access Locally and via the Cloud

Network access is monitored using the Zero Trust security gateway that logs network access to provide a real time display.

- Authenticated devices.
- Connected devices, requested an IP but not authenticated.
- Unrecognized devices.
- Failed authentication attempts.
- Alerts of failed access attempts.

When failed access attempts are persistent it is essential to call a security expert to investigate. A cloud managed ZTNA end-point security gateway allows the IT service provider to monitor the business network remotely.



Additional Points to Note for the Network Infrastructure Update

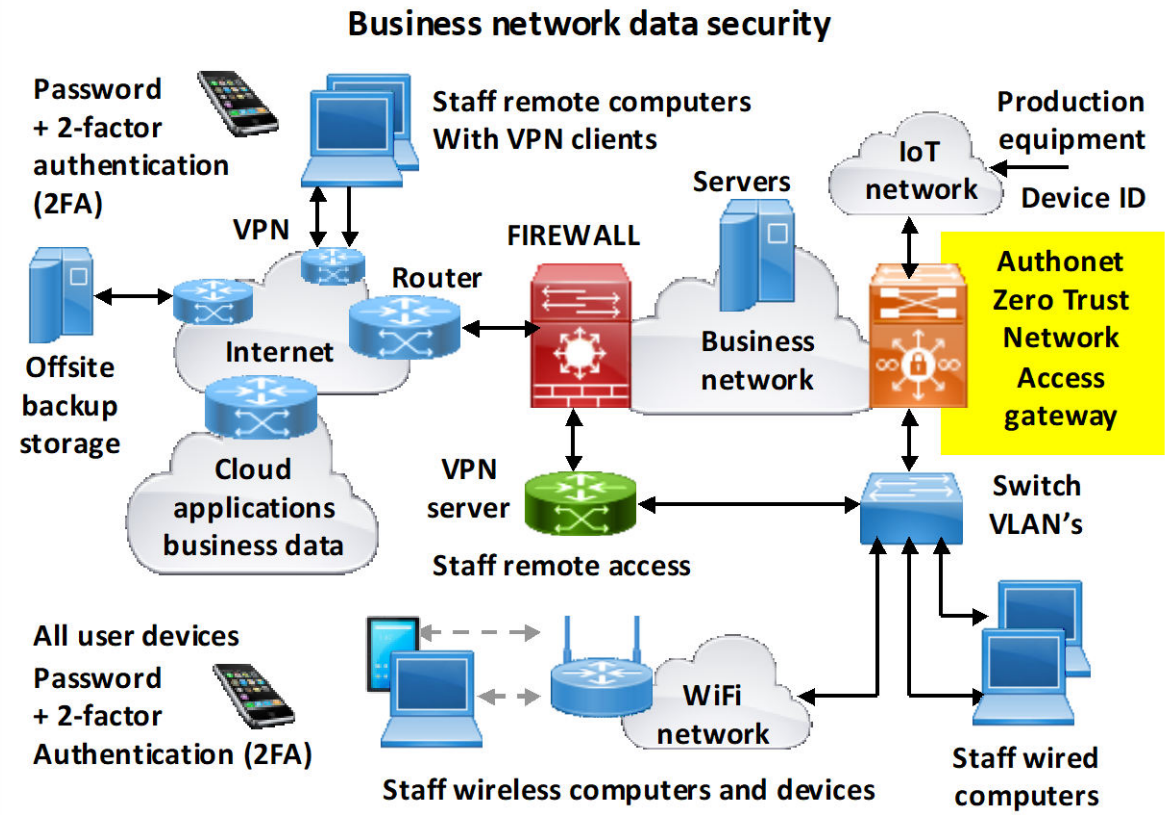
There are some additional points to note when upgrading the network infrastructure.

The first point is that any remote access to the network for staff outside the business must use virtual private network (VPN) security and must also be subject to 2-factor authentication. If possible eliminate remote access by moving data and applications to the cloud so that remote access staff are connecting to the cloud applications.

Internet of things (IoT) devices installed in the network are a security risk and must be verified. Some IoT devices connect with suppliers for support or maintenance purposes. These devices may be the method that a cyber criminal uses to access the network as IoT devices have no cybersecurity protection. The ZTNA gateway can be configured to authorize access to the Internet for IoT devices but block access to the local network.

Ensure that all cybersecurity products are installed by a qualified cybersecurity professional, as cybersecurity products are only effective when configured correctly.

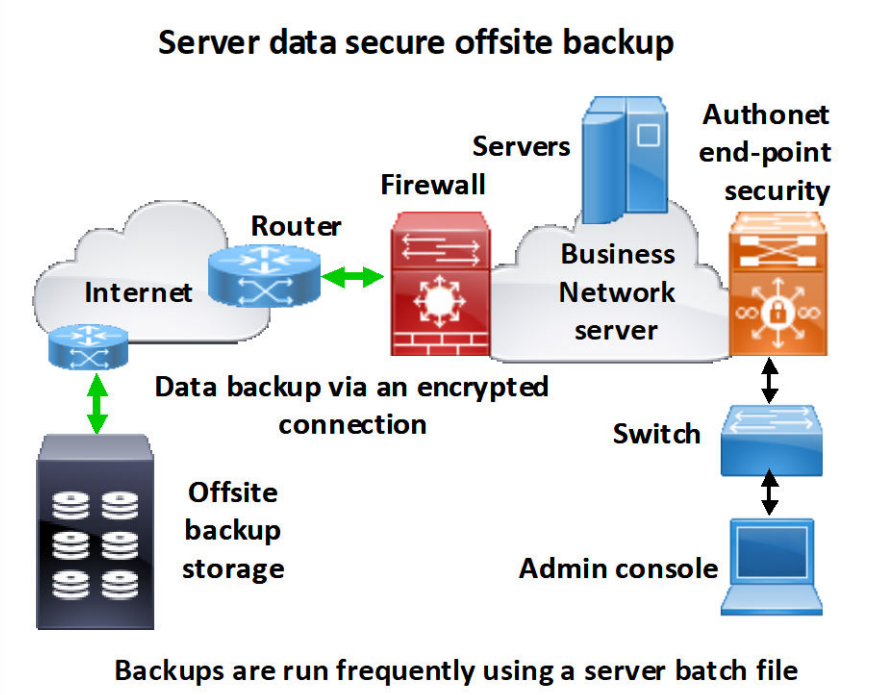
A business network with a comprehensive cybersecurity upgrade is shown in the next diagram.



Prepare a Ransomware Attack Recovery Plan for the Business Data

Even with the best cybersecurity precautions there remains a small probability of a successful ransomware attack, usually due to human error. All businesses should prepare and test a recovery plan that will restore business operations in a short time without paying the ransom demand. Small and medium businesses can work with an IT service provider to prepare the recovery plan. It is essential that the plan is tested and updated periodically, for example, each quarter. In addition to restoring business operations it is necessary to investigate how the criminal was able to access the network and block that path, if this is not done the criminal will attack again.

A ransomware recovery plan requires backup hard drives to be kept for all computers and data backups of the business data. Frequent data backups are the first step and essential to implement a recovery plan. Backup data must not be stored in the local network, as the cyber criminal will attempt to encrypt the backups before encrypting the database. The data backups must be offsite and must not be accessible on-line. Data files are backed up frequently, daily or hourly. Previous data backups are kept for some time, 1 month or more. If a cyber criminal attacks with ransomware then the last few backups may be corrupted. All staff should store personal files on a cloud account for easy restoration.



Prepare and test a ransomware attack recovery plan with the following points.

- Write an attack recovery procedure; plan a budget.
- Backup business data daily or hourly to offsite storage.
- Keep 1 to 3-months of backups for a recovery history.
- Have multiple drives prepared to install on computers.
- Have the IT service provider ready for a recovery.
- Test the procedure periodically.

If an attack occurs disconnect the network from the Internet. Next replace the server and workstation drives and finally restore the data from backups. Do not connect the Internet until the attackers point of entry is found, the cyber criminal will try to attack the restored system. The method of access may have been a user computer, but this is difficult to identify. The only sure method for protection from future attacks is to change all workstation hard drives in addition to the server hard drives.

Cyber Attack Risks Summary

All businesses are at risk from a cyber attack, there are no exceptions. The cost of cybersecurity is much less than the expense of an attack. Businesses face a large financial loss when a cyber attack is successful.

- The cost of the ransom to release locked data.
- The additional cost of recovering the business if the cyber criminal does not release the data.
- Reputation cost for a business that is attacked, loss of customer trust.
- When the cyber criminal sells the business data there is a risk of lawsuits against the business.
- Healthcare businesses have a legal obligation to report a data breach to the HHS, and then pay a fine according to the number of patient records breached (HIPAA security).

The essential cybersecurity checklist for a business network is listed below.

- Staff cybersecurity awareness training is essential to recognize a potential attack, frequently repeated.
- A recovery plan will minimize the damage if an attack is successful.
- Vigilance; the network admin should be aware of who is using the network and what is being accessed.
- Install Zero Trust network access (ZTNA) gateway to monitor network use; Authonet is an accessible product for smaller businesses.

- Install 2-factor authentication, an essential deterrent.
- A security expert should make regular checkups.
- Ensure that software security patches are always installed.
- Allow only approved people and devices to access the network.
- Computers should be used only on the business network, not removed and used elsewhere.
- Don’t allow mobile devices on the network as they connect to other networks and may have a virus.
- Ensure that connected devices have anti-virus and that USB ports are locked to prevent installation of a virus via USB memory.
- Control access to high-risk websites, personal email, etc.
- Access data remotely through cloud storage, do not bring storage devices, like flash drives, into the business.
- If staff has to work outside the business give two computers.
- Get cybersecurity insurance.

Businesses can protect against the costly damage of a ransomware attack with cybersecurity insurance. Cybersecurity insurance can mitigate the ransomware risk, however the insurers will require cybersecurity investments. Insurers will want proof that six cybersecurity measures have been implemented.

- Internet firewall installed and configured properly.
- 2-factor authentication (2FA) with Zero Trust cybersecurity.
- Staff training.
- Frequent software security patch update plan.
- All computers and devices must have anti-virus software with updating.
- A tested recovery plan has been prepared.

If a claim is made the insurers will make an inspection to ensure that cyber security measures have been maintained. If cybersecurity measures have not been maintained the insurer will not pay out.

Unfortunately cyber attacks are increasing very quickly and eventually every business may be attacked. However businesses with good cybersecurity will never know that a cyber criminal tried to attack and gave up.

PART 2:

Authonet ZTNA Gateway Installation and Operation

Introduction to Authonet Zero Trust Network Access Operation

The purpose of a firewall is to block any external attack to the business network. The purpose of a Zero Trust Network Access (ZTNA) gateway is to block internal attacks, such as.

- Phishing.
- Password theft.
- Interfaces with 3rd party systems.

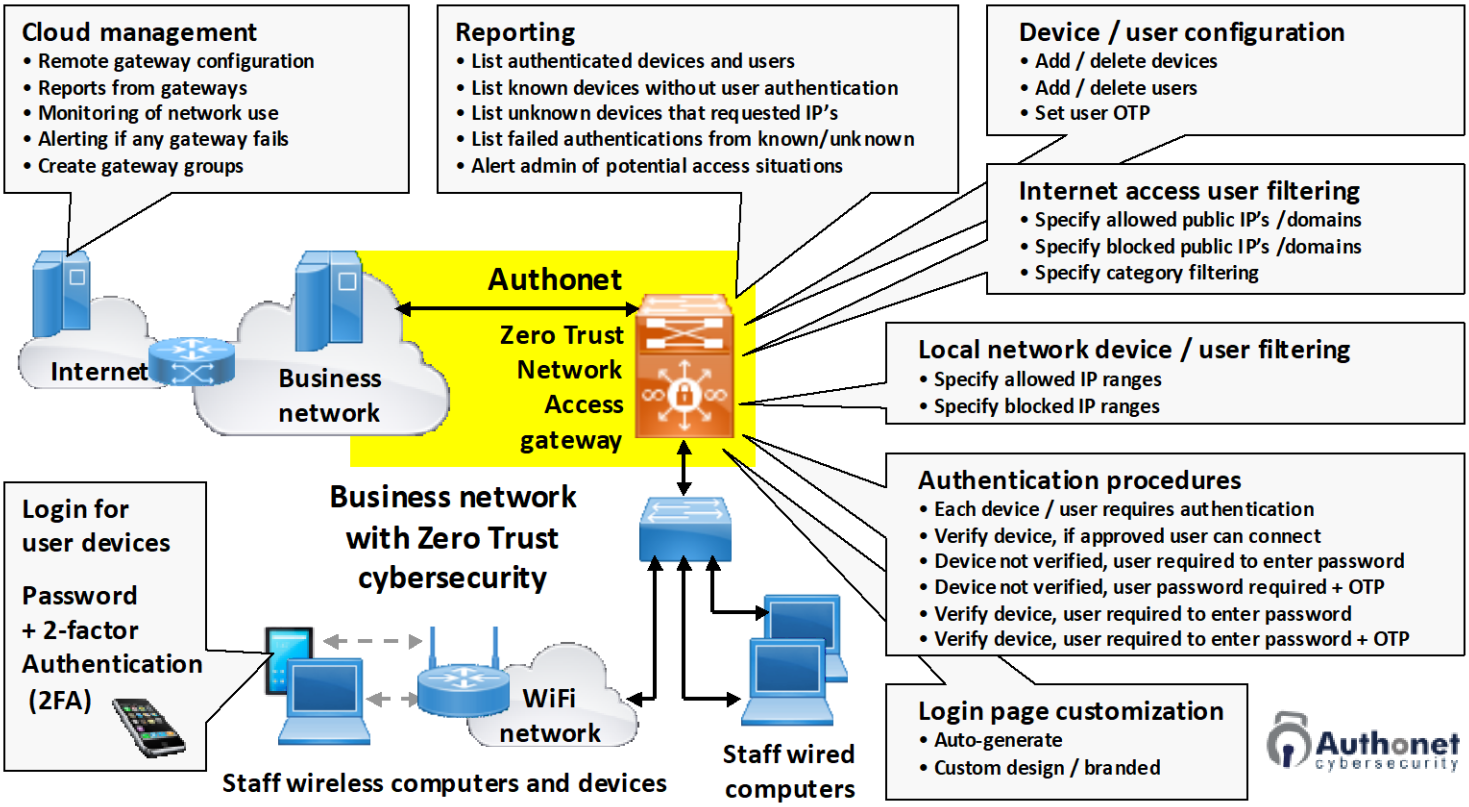
ZTNA imposes controls on the access to the network from devices that are connected to the network; a summary of the controls is listed below.

- Configure devices and users that will be accessing the network.
- Authenticate devices onto the network; verify the identity of approved devices and block access to devices that are not approved.
- Authenticate people onto the network; verify the identity of approved people and block access to people not approved.
- Use multi-factor authentication to authenticate people, this can be 2-factor or 3-factor authentication.
- Determine what each device and user can access within the network, by setting ranges of allowed and blocked IP addresses.
- Determine what each device and user can access with the Internet, by setting lists of allowed and approved public IP's and domain names.
- Monitor all types of connections to the network.
    - Approved devices.
    - Unknown devices.
    - Authenticated users.
    - Authentication failures.
- Alert conditions that need further investigation by the cybersecurity professional.
    - Unknown devices.
    - Multiple authentication failures.
    - Attempting access to an unauthorized area of the network.
- Configure and monitor via the gateway admin port and also via the cloud service.

ZTNA offers better security than a server password, such as Microsoft active directory login. Once the criminal has access to the user computer and the network the criminal does not need a server password as the attack will be made

to an unprotected part of the operating system to get direct access to the data files on the storage devices.

A diagram of the Authonet ZTNA gateway configuration features is shown in the next diagram.



Access of any user or device to the network is blocked until the authentication process has been completed. In the case of 3-factor authentication, login requires the following steps.

- Connection from a known and authorized device (something that the user has access to).
- User provided login password (something that the user knows).
- User provided one time password (OTP) obtained from a personal mobile phone (something that the user owns).

Password theft will not give network access because the criminal does not have access to the mobile phone with the OTP code.

In the case where the criminal is able to install a Trojan virus onto the user computer then the criminal will have access to the network after the user has been authenticated. For this reason it is important to set rules to restrict network access. For example set IP block ranges that include data storage servers but allow access to applications servers.

The installation of a Trojan virus requires the user computer to have access to the criminals Internet server after a phishing message link has been clicked in order to download and install the virus. If a user computer does not have access to the criminal's server then the Trojan virus will not get installed and so the business is protected from a phishing attack. There are two methods to achieve this.

The first method is to allow the user computer to have access only to the public IP's or domains that are necessary for the business to operate. This is configured with the ZTNA gateway and might include the following.

- The business applications cloud server.
- The websites of the business vendors.
- The business e-commerce website.
- The email and software servers, such as Microsoft 365.

An alternative method is to provide staff with two computers; one for the business systems with access blocked to the Internet, and a second computer that has full access to the Internet but all access to the local network is blocked. This is configured with the ZTNA gateway. The user can share files between Internet systems and business systems through a shared file store system that checks for viruses.

Either of the configurations described above will prevent a phishing attack.

Although the two methods might seem complicated for staff to use, many large businesses have implemented one or the other of these configurations in order to be protected from a ransomware phishing attack.

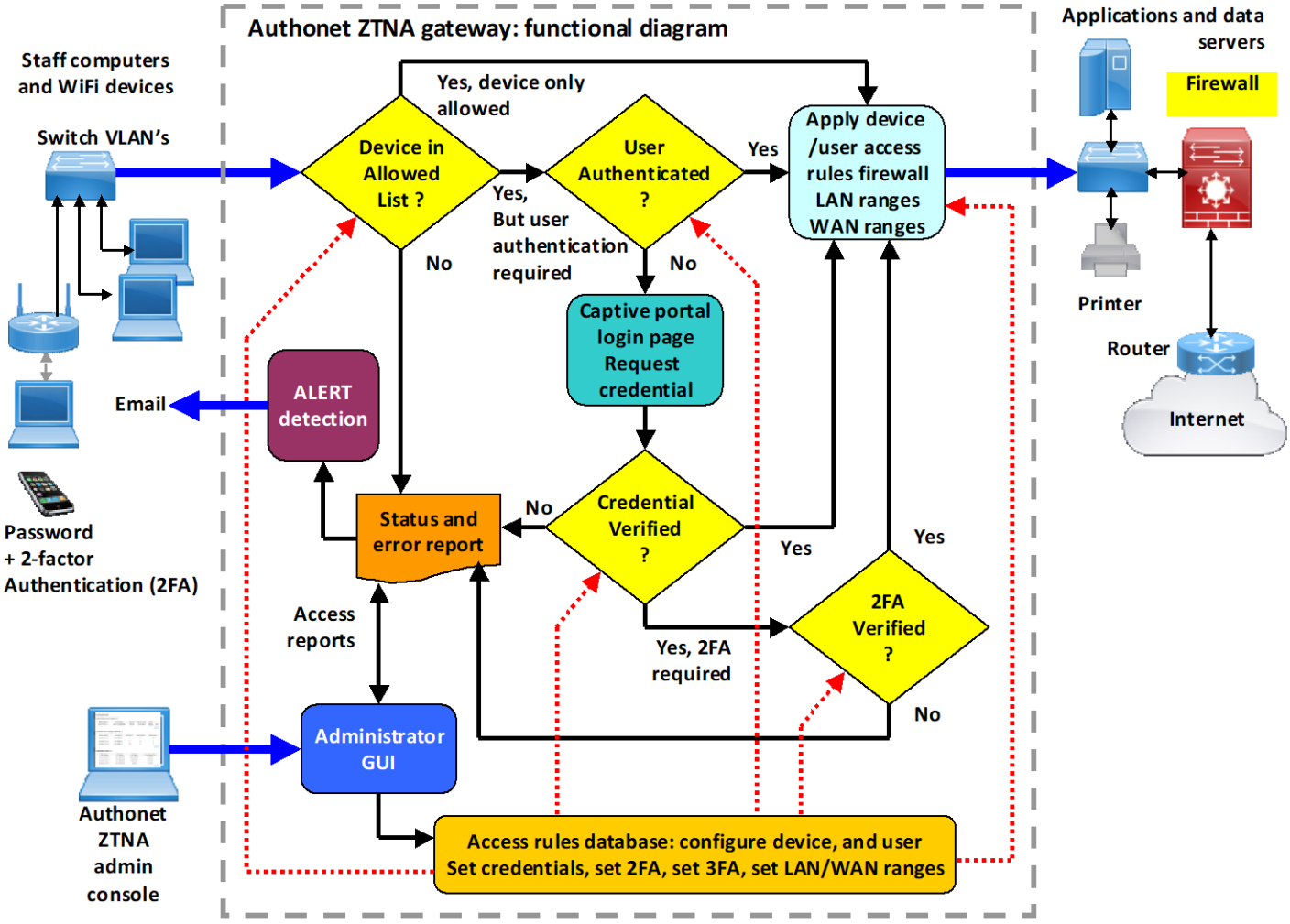
Authonet ZTNA Gateway Functional Overview

The purpose of the Authonet gateway is to protect the business network from a cyber attack, especially a password theft attack or a phishing attack. The Authonet ZTNA gateway has five principal functions:

- Authenticate pre-approved devices; only pre-approved devices get network access
- Authenticate users with password only, or with password plus one time password (OTP) obtained from a personal mobile device (2FA and 3FA is strongly recommended).
- Impose pre-configured LAN IP range restrictions on each device and user.

- Impose pre-configured WAN public IP and domain name restrictions on each device and user.
- Monitor the network traffic for intrusions and attempted unauthorized access and alert the supervisor.

The block diagram shown below illustrates the internal operation of the Authonet ZTNA gateway. All rules are configured into the database using the administrator GUI. The administrator connects via a dedicated admin port (out of band). The admin port **must not** be connected to the LAN network.



Installing the Authonet ZTNA Gateway in a Business Network

The Authonet ZTNA gateway is installed in the network so that all user devices are connected to the gateway LAN ports, with the exception of LAN4, which is only for administrator use. The WAN port connects to the business network, which includes printers, servers and the firewall, which provides access to the Internet via the router.

The Authonet ZTNA gateway is configured using the administrator computer, which connects to the software user interface (UI). The administrator UI is accessible only through the LAN4 port.

WARNING

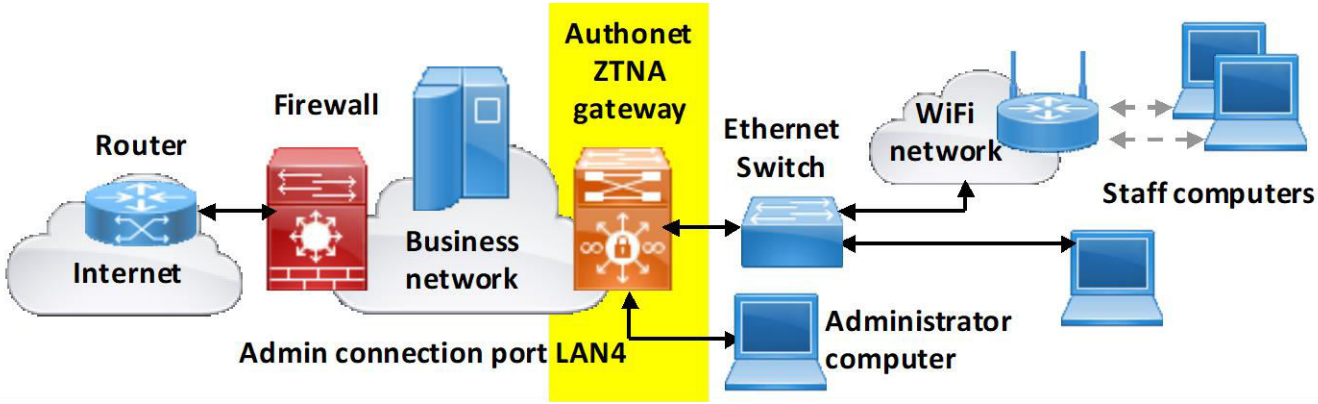
The LAN4 port must not be connected to any part of the network. The LAN4 port must be isolated to prevent any unauthorized attempt to access the software UI from the network. Connecting the LAN4 port to the network is a serious security risk.

The isolated management port is called out-of-band management. The Authonet gateway is also accessible via the Authonet cloud account.

The administrator computer can be removed after product configuration, as it is not required in normal operation. The administrator computer is required only for the following tasks.

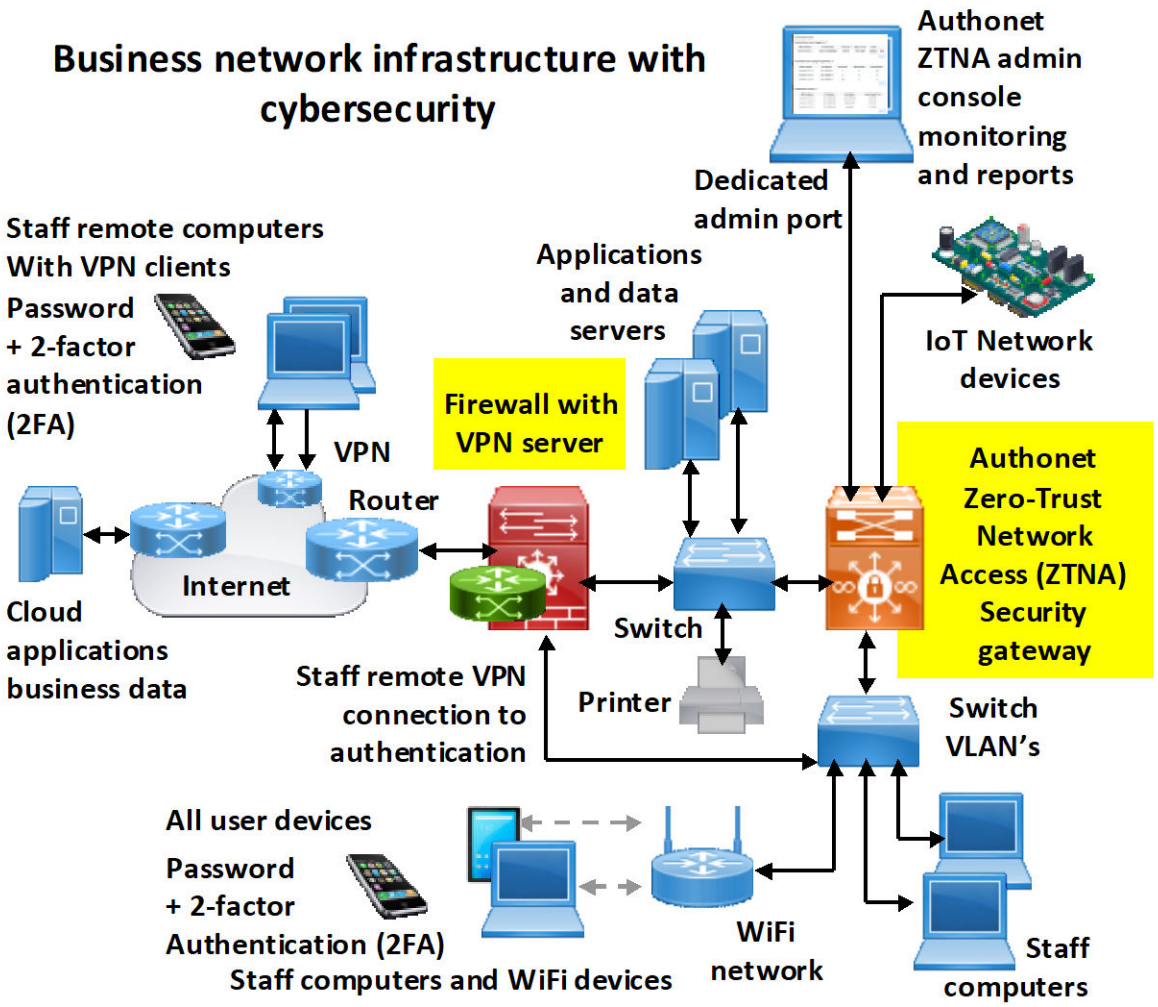
- Add or remove devices.
- Add or remove users.
- Change access credentials.
- Monitor network access and use.
- Alerts are sent to the designated administrator email.

The next diagram illustrates the installation of the Authonet ZTNA gateway in the network.



When configuring the network infrastructure follow these rules.

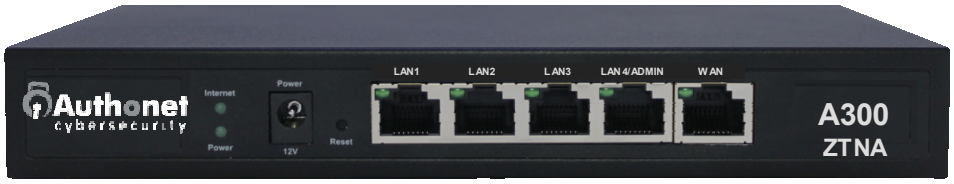
- The Authonet admin console is connected to the dedicated out-of-band port (LAN4), this port must not be connected to the network infrastructure.
- All local users should be configured for 2FA or 3FA, a registered device with password and OTP for authentication, except where users connect from multiple devices, and access to the local network and Internet is restricted.
- Remote computers must be connected via the firewall VPN server, the firewall VPN server must be routed to an independent firewall port and connected to the ZTNA gateway via the switch to implement 2FA for remote users.
- IoT devices should be connected to the ZTNA network connection and access to the local area network must be restricted or blocked.



Authonet ZTNA Products

The Authonet ZTNA products are network appliances for installation in the business network. The Authonet A300 Zero Trust Network Access (ZTNA) gateway is designed for small business cybersecurity protection.

- There is no limit for the number of devices and users that can be authenticated.
- The administrator graphic user interface (GUI) can only be accessed via LAN4, other LAN and WAN ports do not have administrator access
- The LAN4 port is dedicated for the administrator console and must not be connected to the user network.
- The Authonet cloud service will be available for remote management and monitoring.



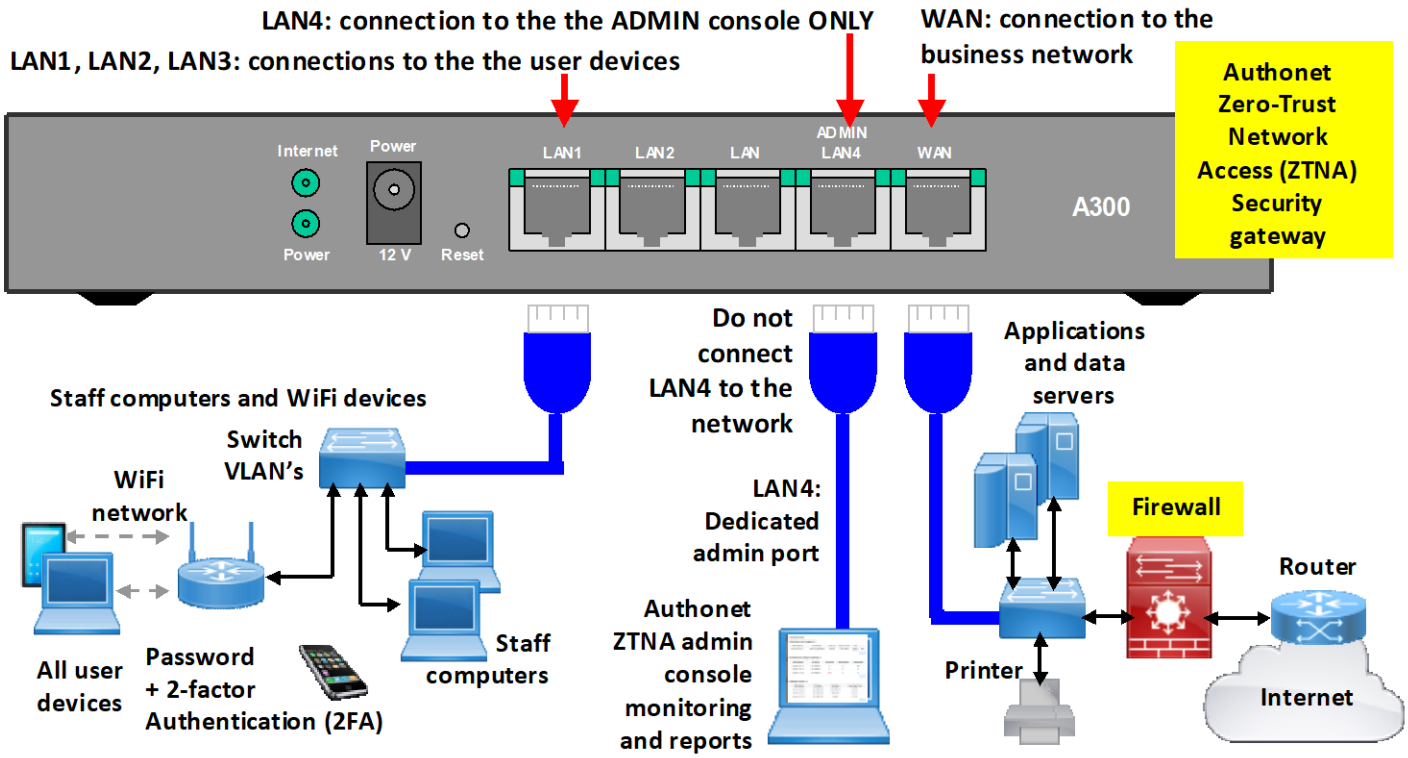
The Authonet A1000 Zero Trust Network Access (ZTNA) gateway is designed for small and medium business cybersecurity protection.

- There is no limit for the number of devices and users that can be authenticated.
- The administrator graphic user interface (GUI) can only be accessed via LAN4, other LAN and WAN ports do not have administrator access.
- The LAN4 port is dedicated for the administrator console and must not be connected to the user network.
- The Authonet cloud service will be available for remote management and monitoring.
- Contact Authonet for information about products for larger businesses.

A300: Product Connections

The Authonet A300 is designed to provide Zero Trust Network Access cybersecurity for smaller businesses. There is no limit to the number of devices and users that can be registered with the A300.

Connect the ports as shown in the diagram. The WAN port should connect to the business network that includes the servers, printers and the firewall, which connects the network to the Internet. The ports LAN1, LAN2 and LAN3 connect to user devices, which can be wired computers, WiFi devices and IoT devices. Any type of device that has a MAC address and is a DHCP client that requests an IP address can be connected. The port LAN4 must be connected only to the administrator console. LAN4 must not be connected to the network. The administrator can connect only to LAN4, which is the administrator graphic user interface (GUI) and this is not available on any other port. This is a security requirement. IT service businesses and managed IT service providers wishing to have remote management and monitoring access to the A300 should open an Authonet cloud account subscription.

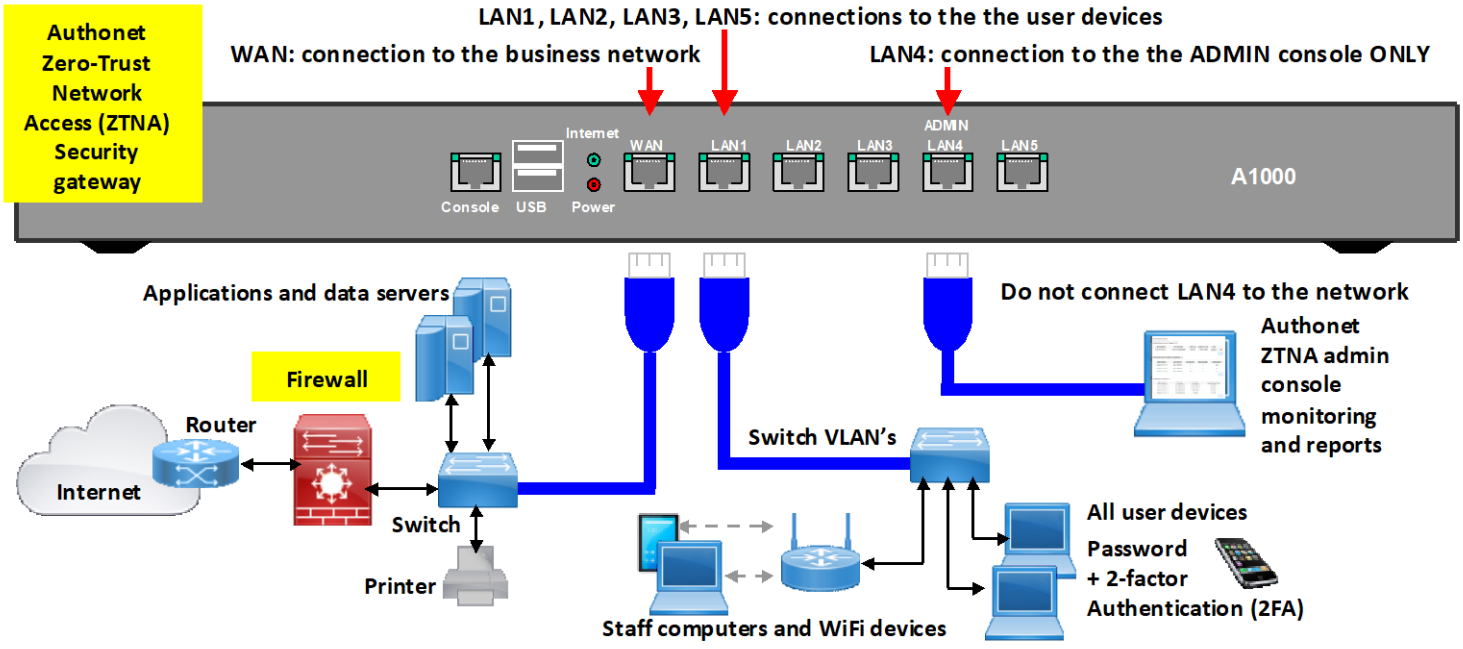


The A300 product is shipped with a quick start guide. Follow the quick start guide instructions when powering the product for the first time. Online support is available via the Authonet website, always provide the product serial number when contacting support.

A1000: Product Connections

The Authonet A1000 is designed to provide Zero Trust Network Access cybersecurity for smaller businesses. There is no limit to the number of devices and users that can be registered with the A1000.

Connect the ports as shown in the diagram. The WAN port should connect to the business network that includes the servers, printers and the firewall, which connects the network to the Internet. The ports LAN1, LAN2, LAN3 and LAN5 connect to user devices, which can be wired computers, WiFi devices and IoT devices. Any type of device that has a MAC address and is a DHCP client that requests an IP address can be connected. The port LAN4 must be connected only to the administrator console. LAN4 must not be connected to the network. The administrator can connect only to LAN4, which is the administrator graphic user interface (GUI) and this is not available on any other port. This is a security requirement. IT service businesses and managed IT service providers wishing to have remote management and monitoring access to the A300 should open an Authonet cloud account subscription.



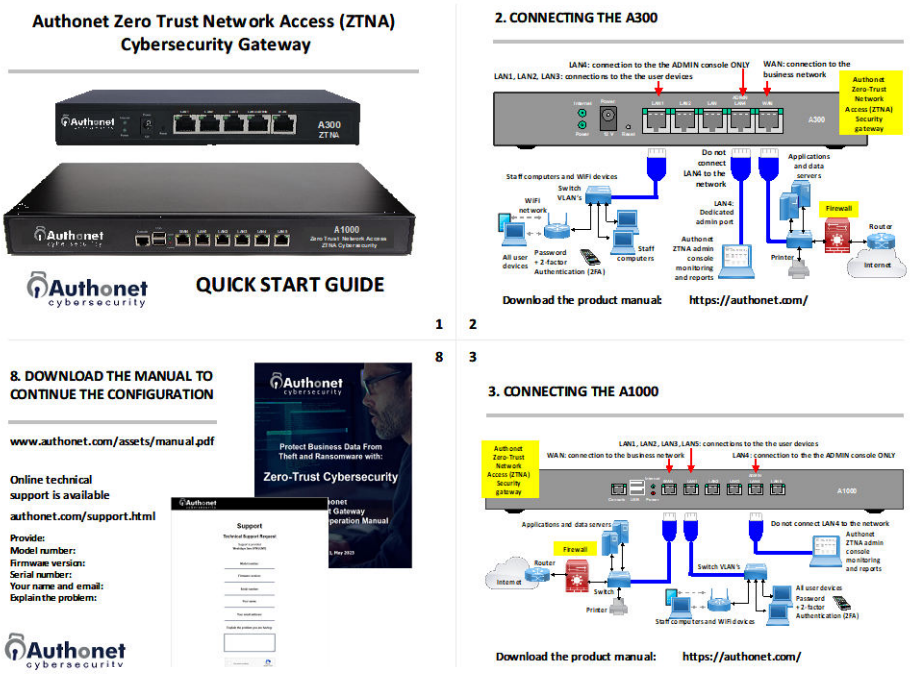
The A1000 product is shipped with a quick start guide. Follow the quick start guide instructions when powering the product for the first time. Online support is available via the Authonet website, always provide the product serial number when contacting support.

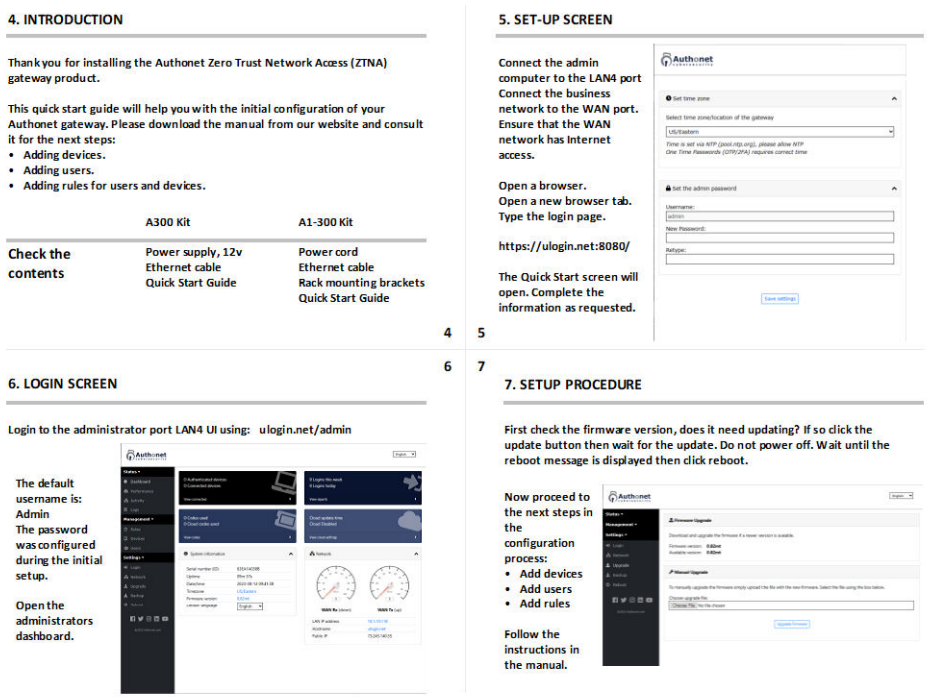
PART 3:

Initial Product Configuration and Administrator Login

Quick Start Guide

Each Authonet product includes a quick start guide; this is shown in the figures below. The quick start guide has eight sections that will help the customer with the product initialization process. On completion this manual should be consulted to configure the product. The quick start guide can be downloaded from the Authonet website.



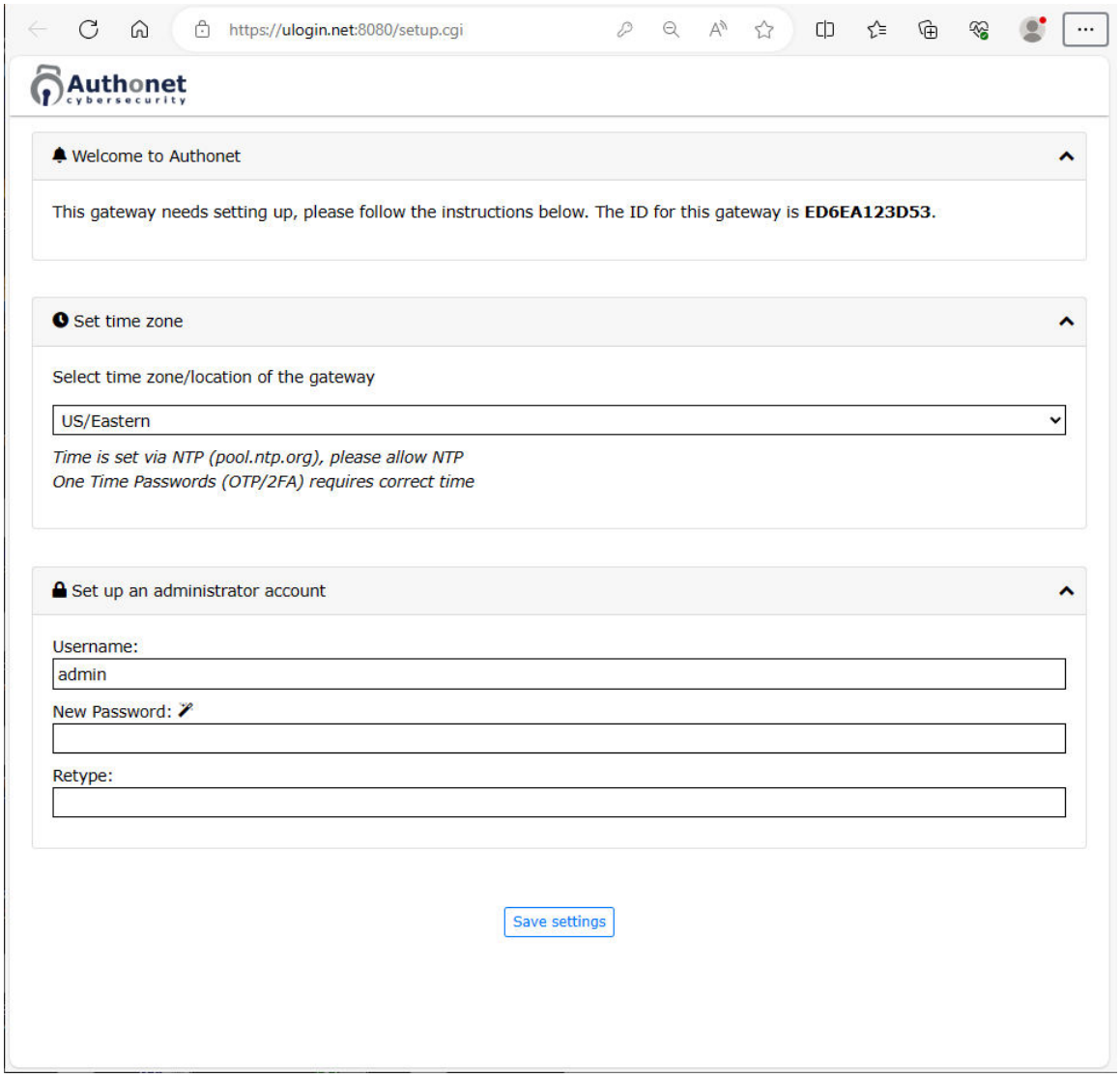


Product Setup

Connect the Authonet ZTNA product WAN port to the business network and the LAN4 is connected to the administrator's computer using an Ethernet cable.

- Open a browser; open a new browser tab.
- If the Authonet setup page does not open automatically then type the login page name: **www.ulogin.com.**

The Authonet setup; page will open; the screen is shown in the next figure.



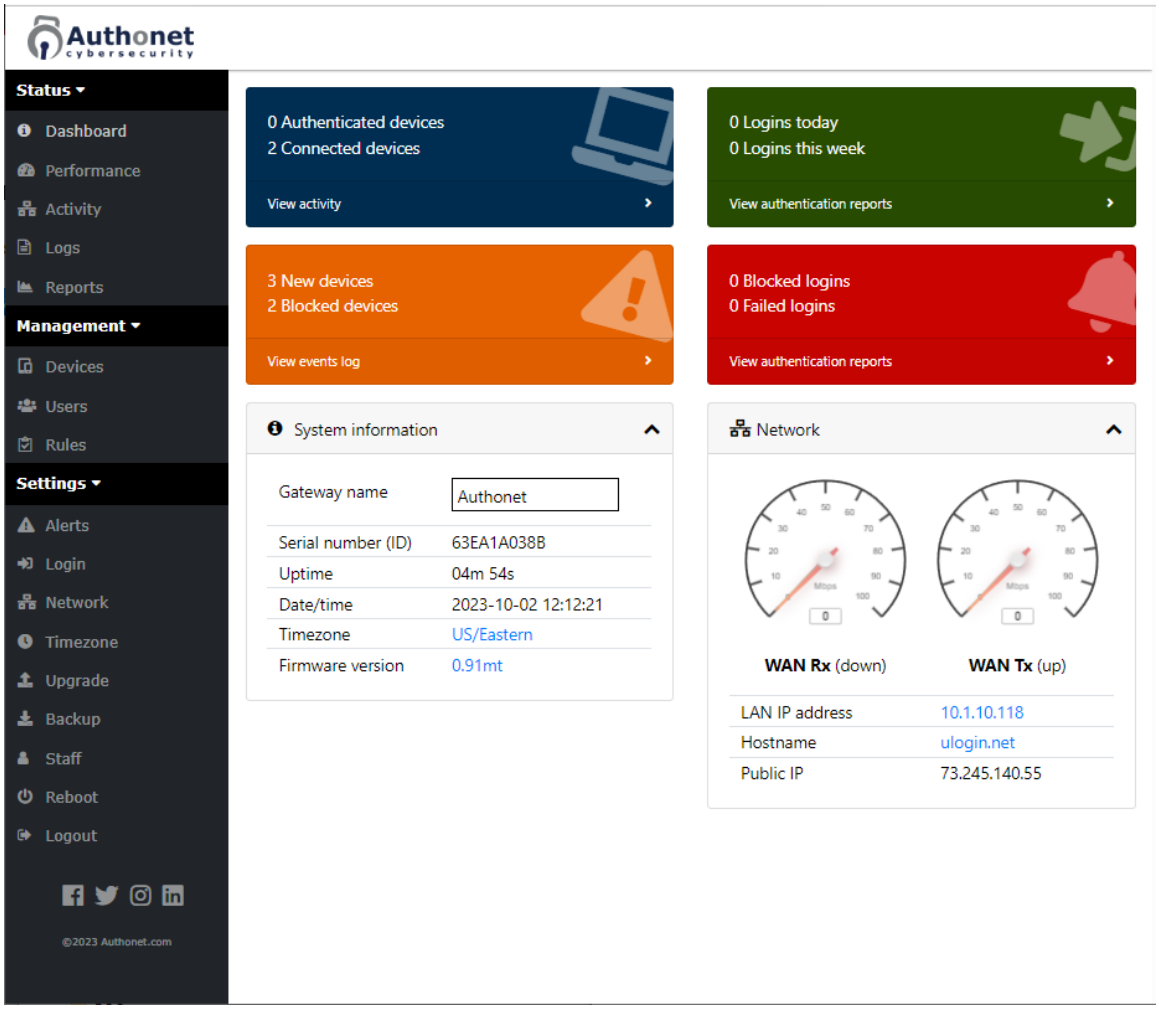
Select the time zone and set the administrators password. Use the password generator to generate a strong password. The requirements are:

- Upper and lower case letters, numbers, symbols.

Click the save settings button.

When the administrator setup page has been completed the dashboard screen will be displayed, this is shown in the next figure. The administrator will see this display after each administrator login on the LAN4 port.

The administrator will require network down-time to configure all network devices and users during the installation of the Authonet ZTNA gateway before the users can connect to the network. The administrator will have configured 2FA for the users (recommended) and so each user will configure the mobile device 2FA code generator using the QR code provided by the administrator.

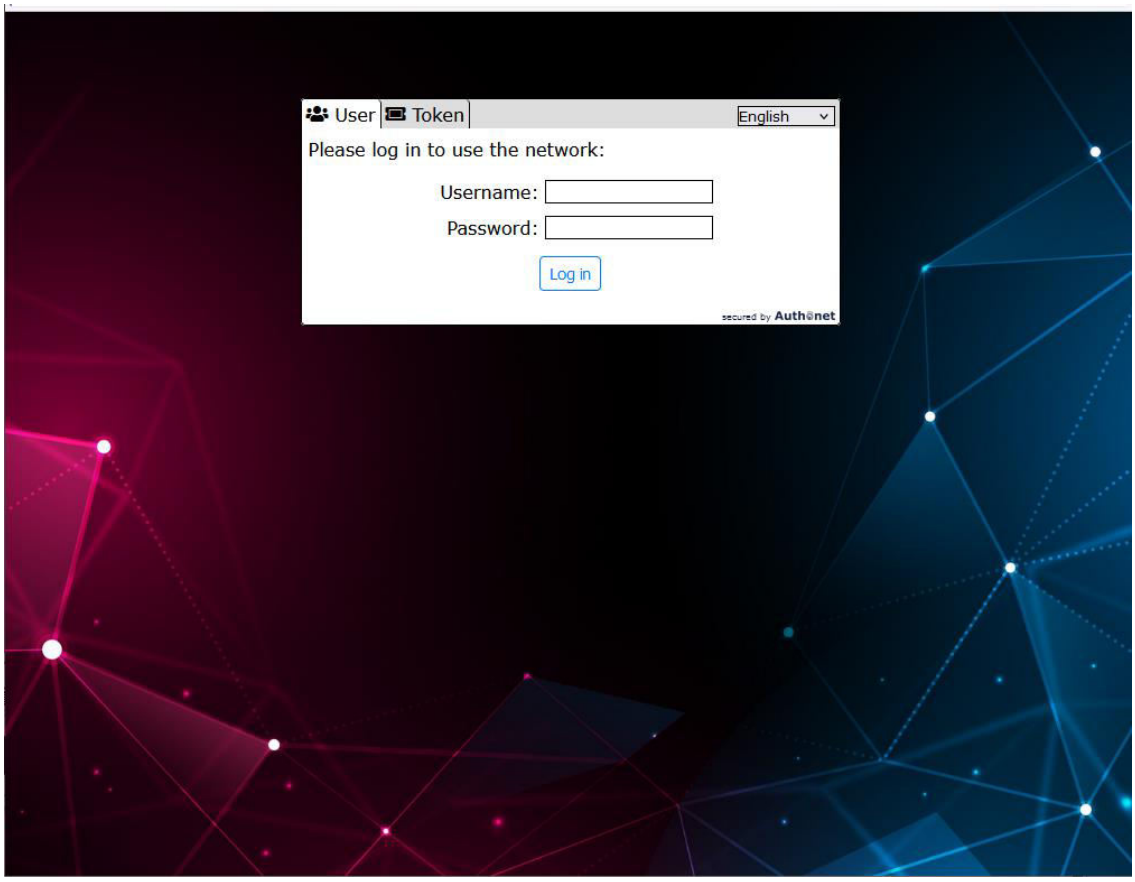


The dashboard gives an overview of the computer network security.

- Four reports.
- System connection.
- Network performance.

The menu to select the configuration functions has 14 entries. The configuration functions are described on the following pages.

Before the administrator has configured the initial setup page a user computer that is connected to any of the network LAN ports will get an IP address from the network, however a browser will show no connection. After the administrator adds the devices then configures "login" a user computer browser will display the default login page, shown in the next figure. The user has no login credentials configured at this point and so the user cannot connect to the network.



The User Interface (UI) Configuration Parameters

The graphic user interfaces is accessed upon login. The management functions are divided into three sections as shown in the figure.

Status: Information about the network utilization and performance.

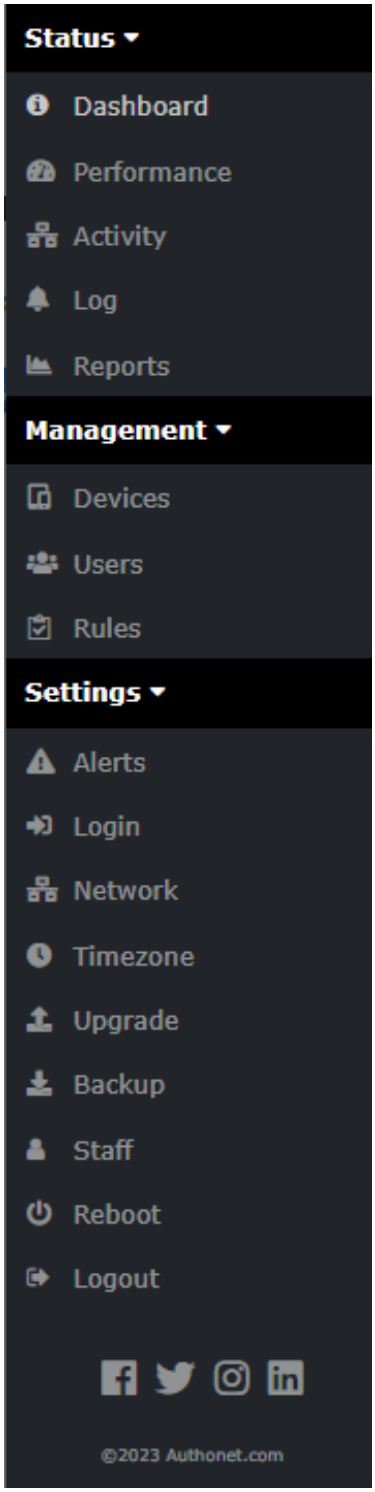
- Dashboard: an overview of current utilization and fast access to operational reports.
- Performance: throughput and network use graphical information.
- Activity: network activity includes connected devices and authenticated users.
- Logs: network access log for business records.

Management: Zero Trust Network Access.

- Devices: recognition and authentication of devices that are connected to the business network.
- Users: credentials for authentication of users, access password and 2-factor authentication.
- Rules: rules of access and authentication that are applied to devices and users.

Settings: Configuration and operation parameters.

- Alerts: send alerts via email
- Login: customization of the login screen presented to users who have a login rule.
- Network: change the default network setting from DHCP to static IP's.
- Timezone: set the location timezone
- Upgrade: install the latest firmware version.
- Backup: create a settings file backup; restore a settings file backup.
- Staff: add staff to the admin login.
- Reboot: configuration change reboot.
- Logout.



Administrator Login

With the administrator computer connected to LAN4, open the browser with a new tab. The username and password box will open to enter the administrator credentials. There is no administrator login page.

If the login box is not displayed then type the following to open the login page:

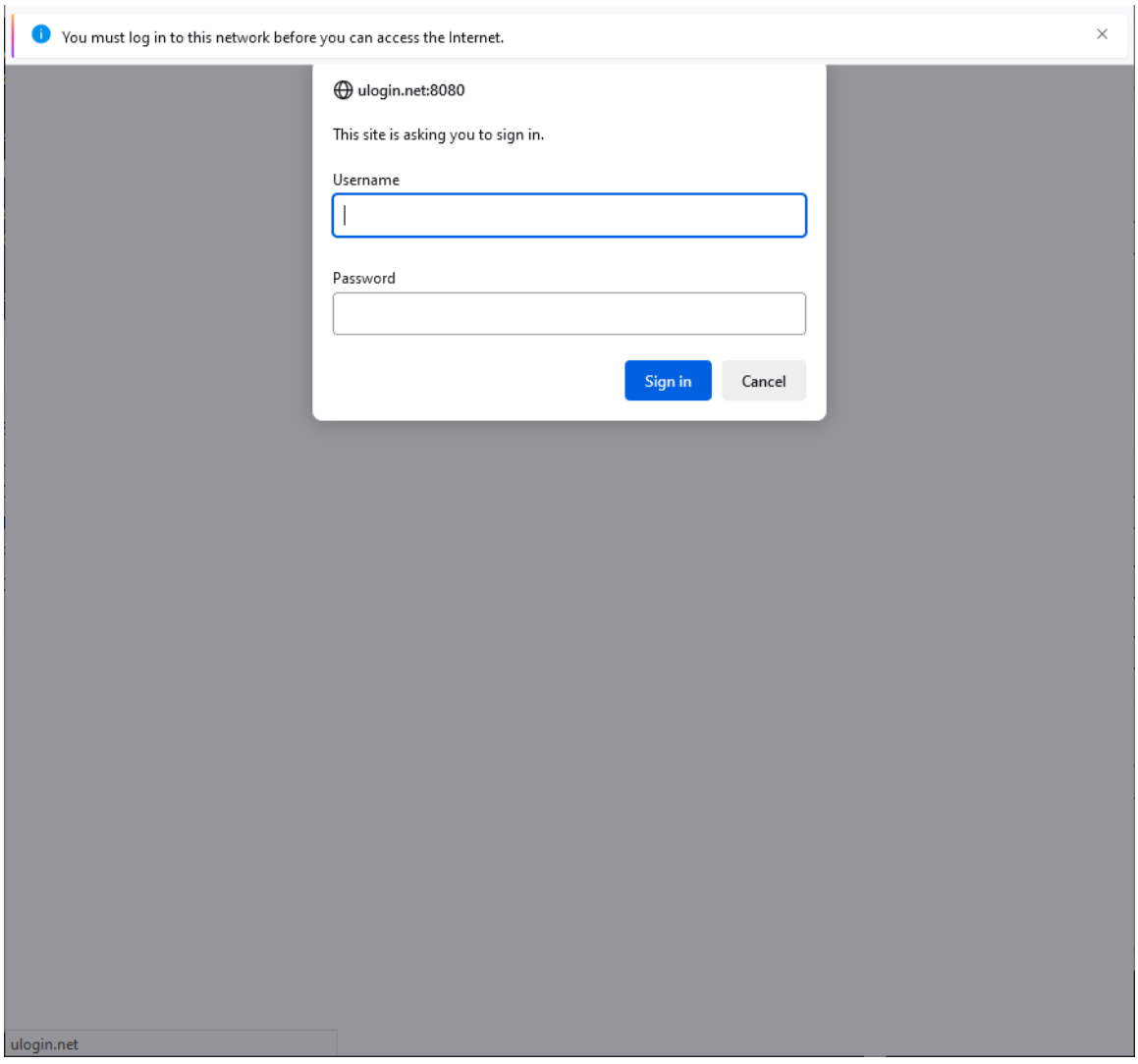
https://ulogin.net/admin

The administrator will enter the credentials using the browser login box.

Username: admin, password: entered during the initial setup

If the password is forgotten or lost the Authonet ZTNA gateway will have to be reset to the factory default setting.

An example of the browser login box is shown in the next figure.



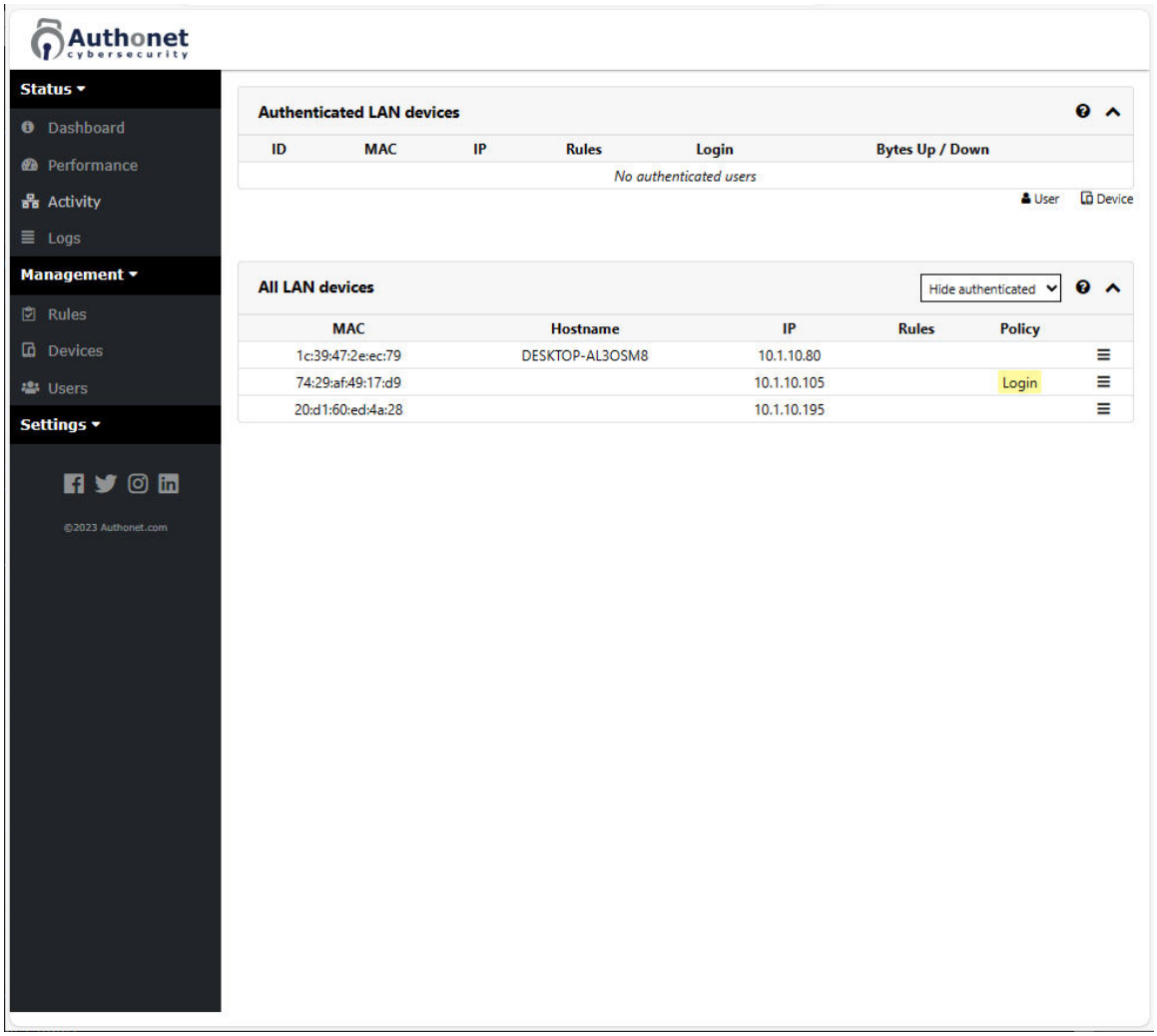
Administrator Access to the Internet

Administrators can request access to the Internet, however this action is not advisable as it is a security risk. See the warning later in this section.

After login, the administrator has access to the configuration UI, however the administrator does not have access to the Internet.

If the administrator requires access to the Internet follow the procedure to allow access.

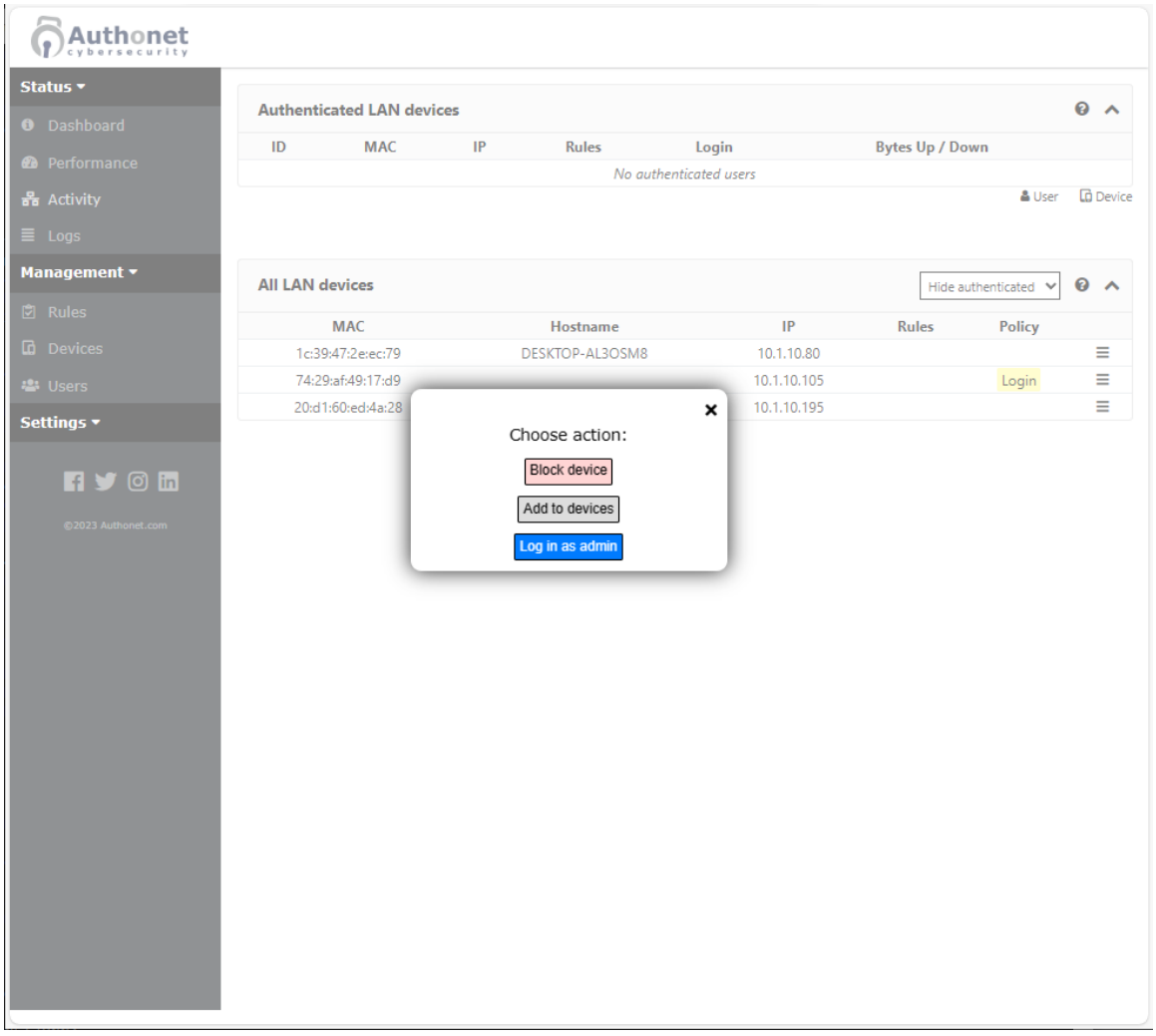
Open the activity page and identify the administrator workstation, in the example below this computer has the IP address 10.1.10.80



Next click on the three horizontal bars to the right of the workstation IP address. This opens a window that is shown in the next figure.

Click the button “Log in as admin”

This will give the administrator access to the Internet.

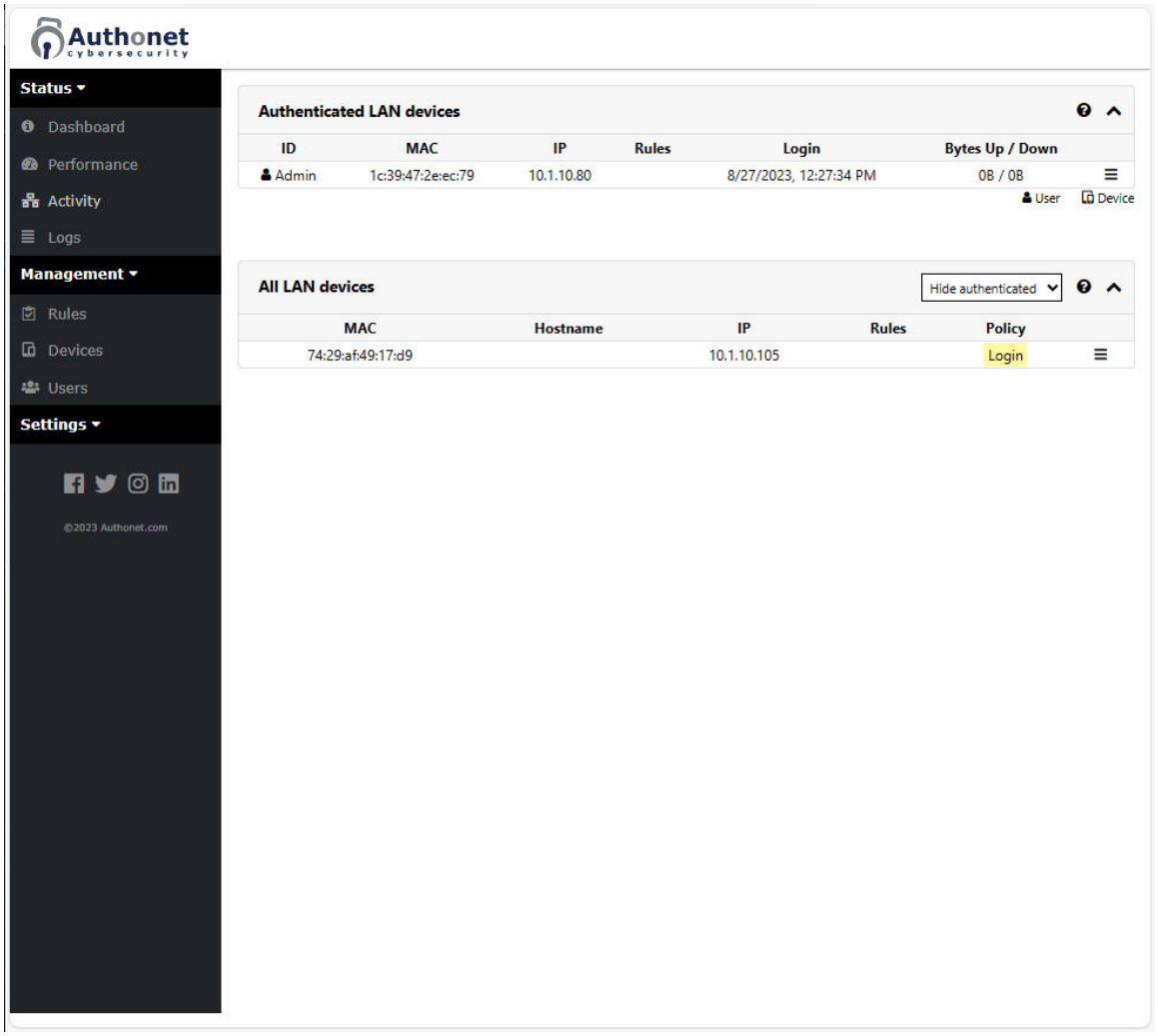


The next screen shows that the administrator computer has been moved to the section “Authenticated LAN devices”

The administrator can configure the Authonet gateway and has full access to the Internet.

WARNING

Giving Internet access to the administrator's computer is a serious security risk. If the administrator clicks on a phishing link then a cyber criminal will have access to the administrator’s computer, to the Authonet cybersecurity configuration, and to the network without restriction.



PART 4:
Status and Reporting

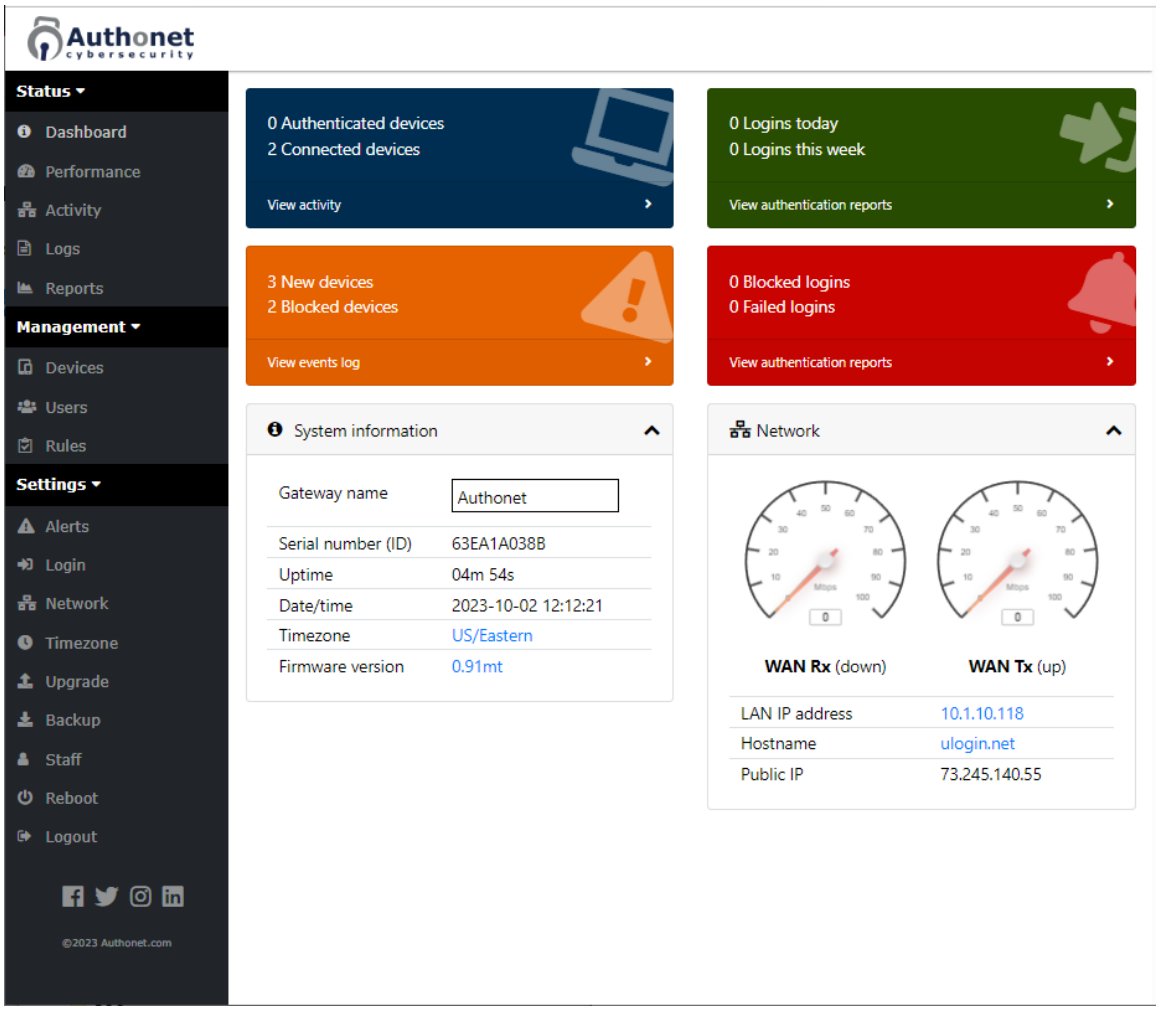
The Dashboard

The dashboard is the first screen that is displayed when the administrator logs in to the UI.

The dashboard provides an overview of current utilization and gives fast access to operational information.

If the administrator wishes to open a support ticket first get the serial number and current firmware version from this page to submit with the support ticket request.

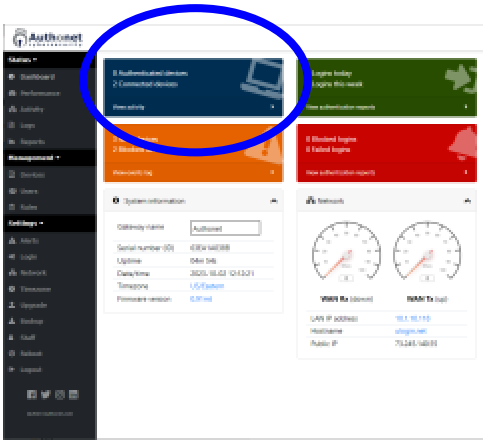
Note that the Authonet gateway is given a name, this name is used when sending out alert emails and communicating with the cloud.

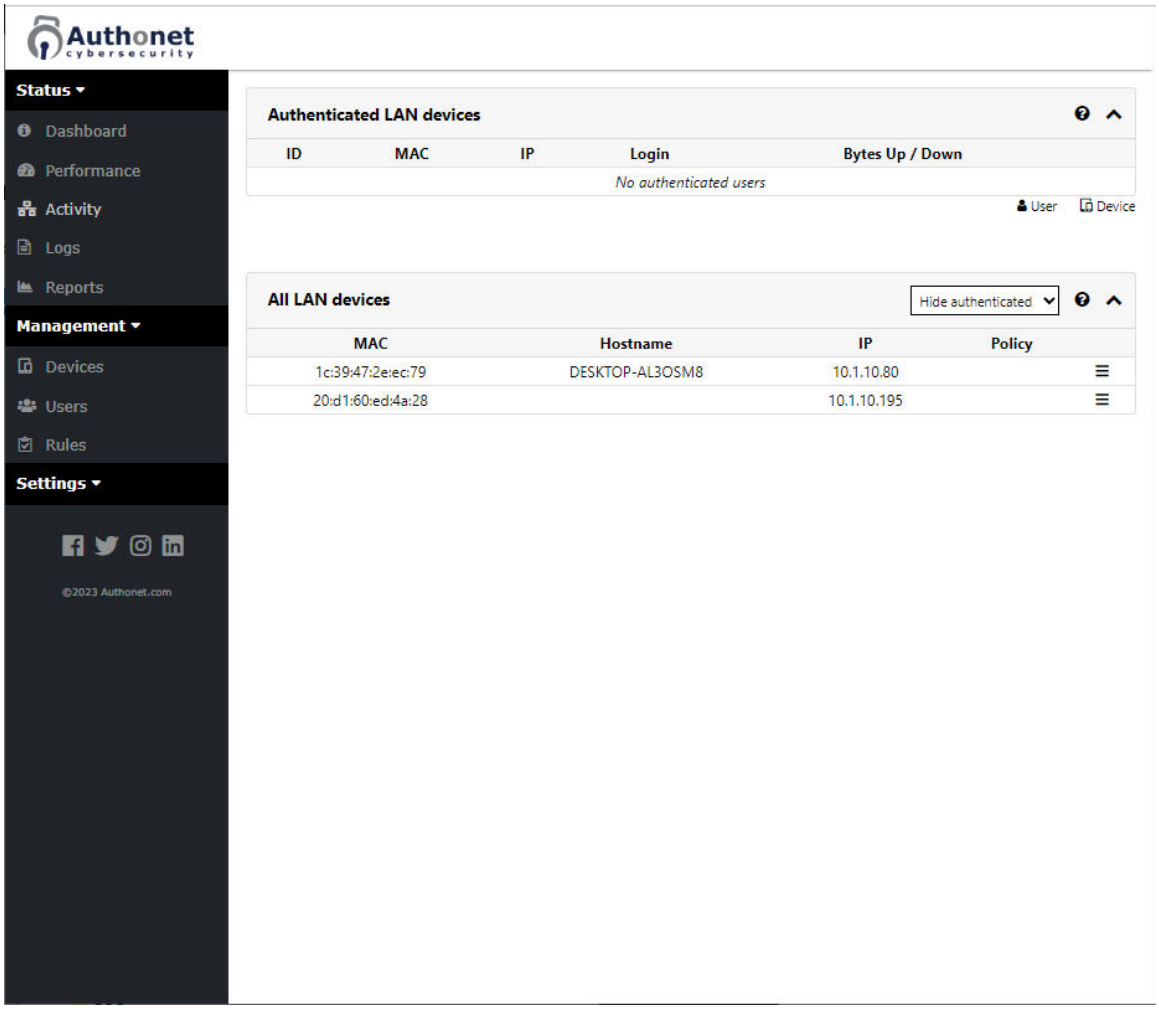


Information Bars: Authenticated devices, connected devices

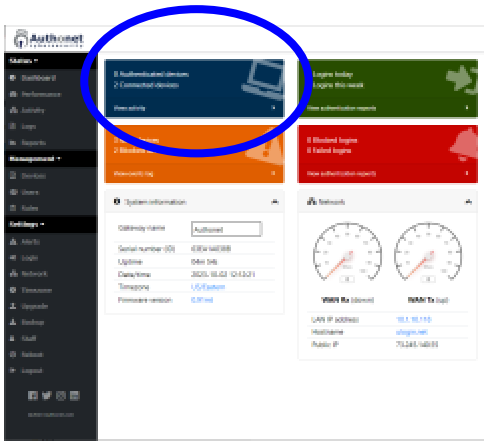
The dashboard has four colored information bars. Each bar opens a report page when clicked.

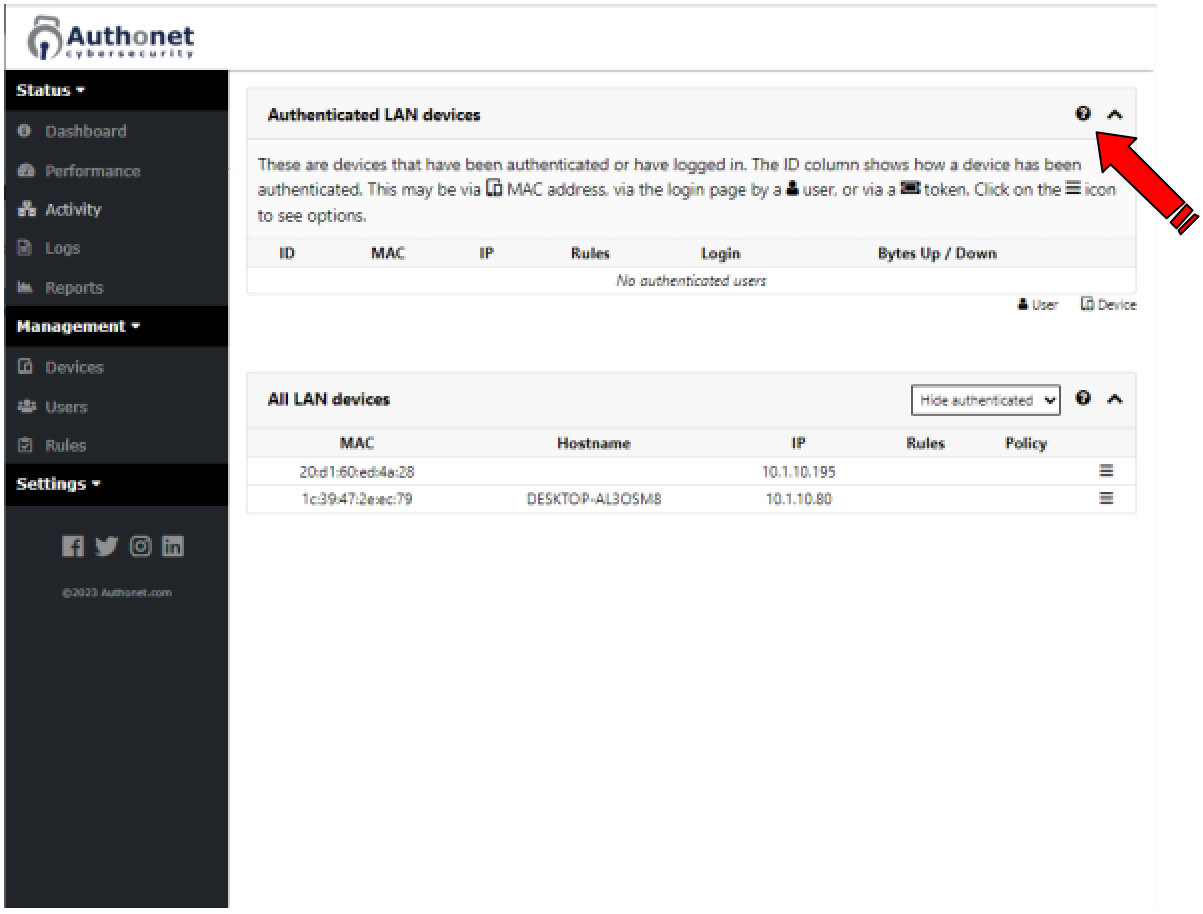
The top left information bar is a shortcut to the activity page and shows both authenticated and connected devices.





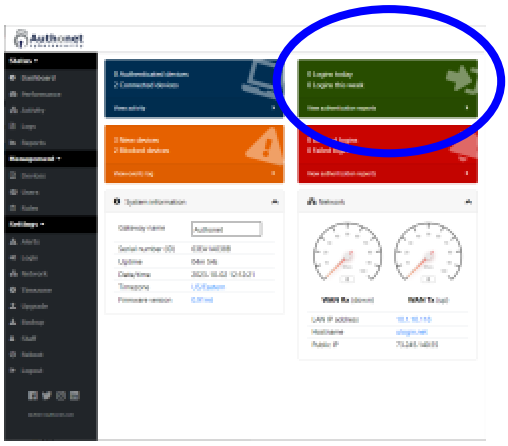
Clicking the question mark symbol displays additional information about the data being displayed.

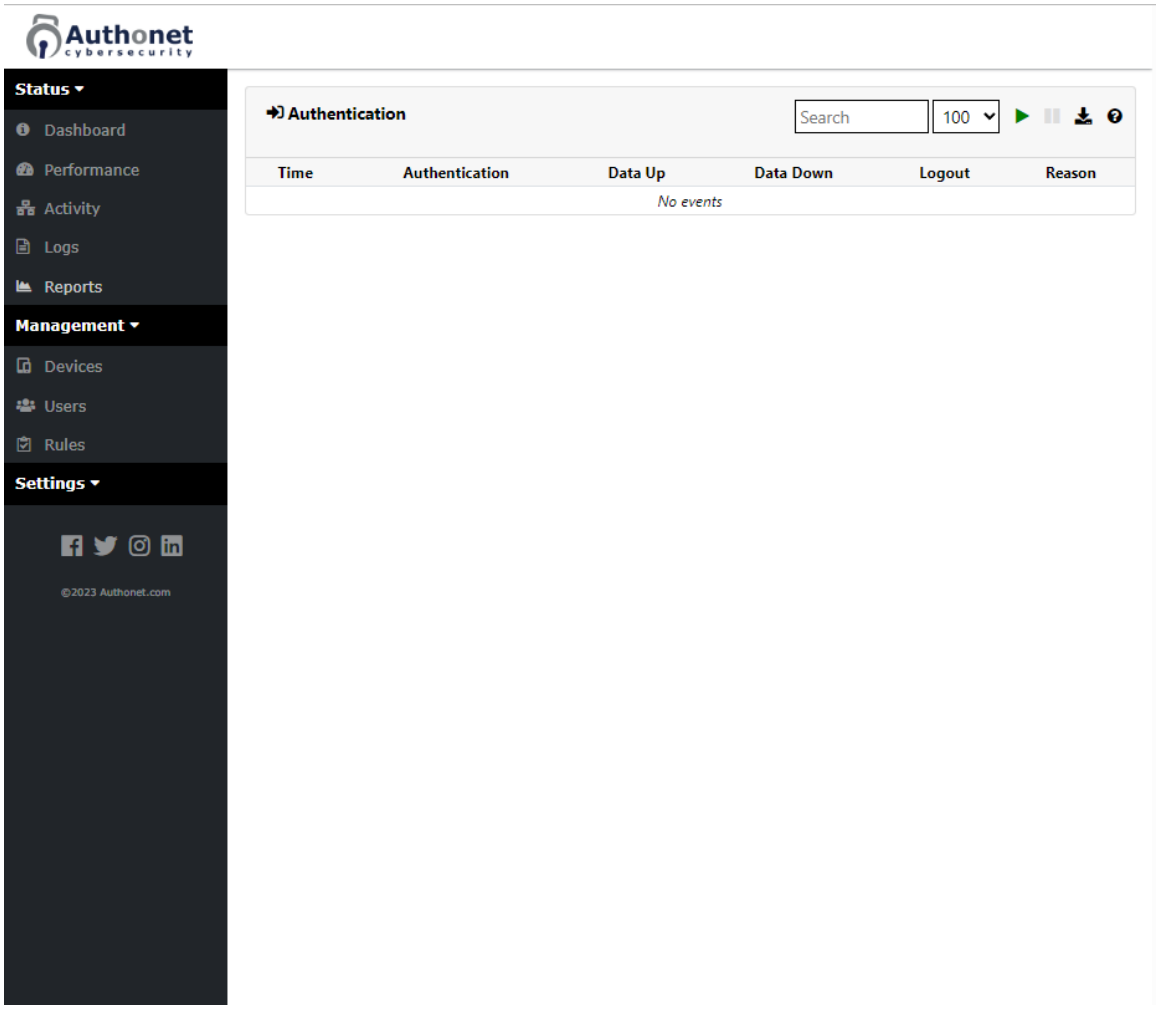




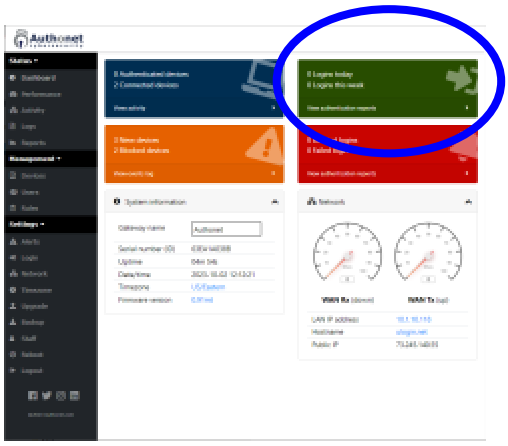
Information Bars: Logins today, logins this week

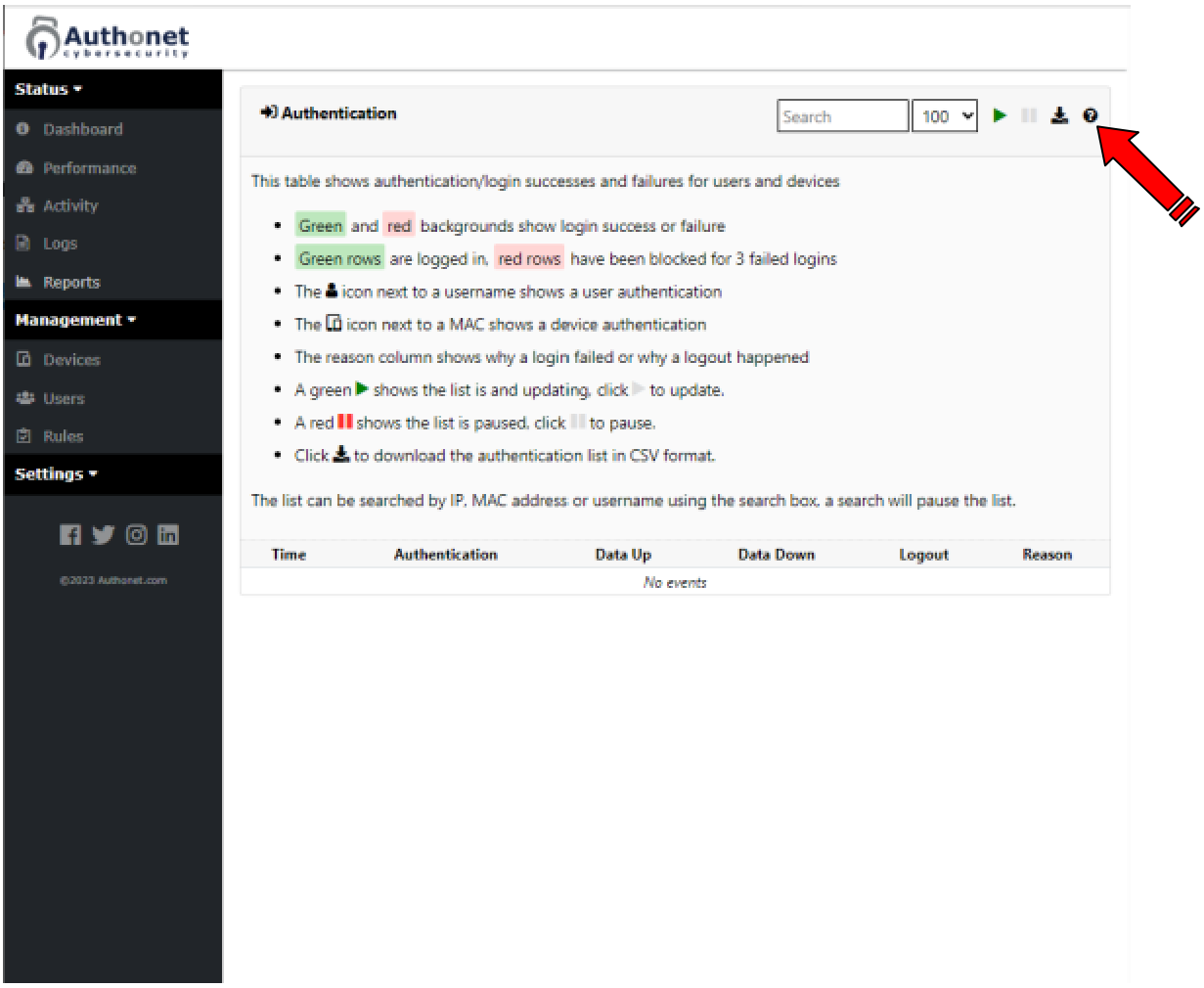
The top right information bar is a shortcut to the authentication reports. Data statistics for authenticated devices and users is listed in the report.





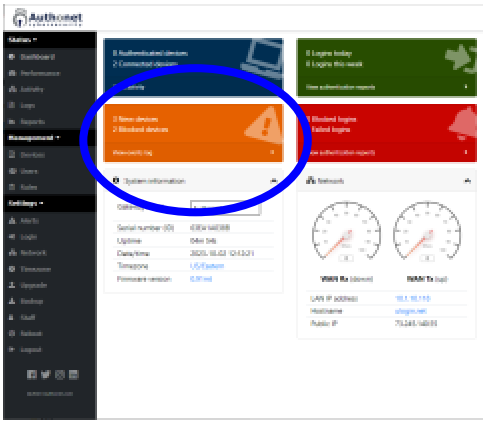
Clicking the question mark symbol displays additional information about the data being displayed.

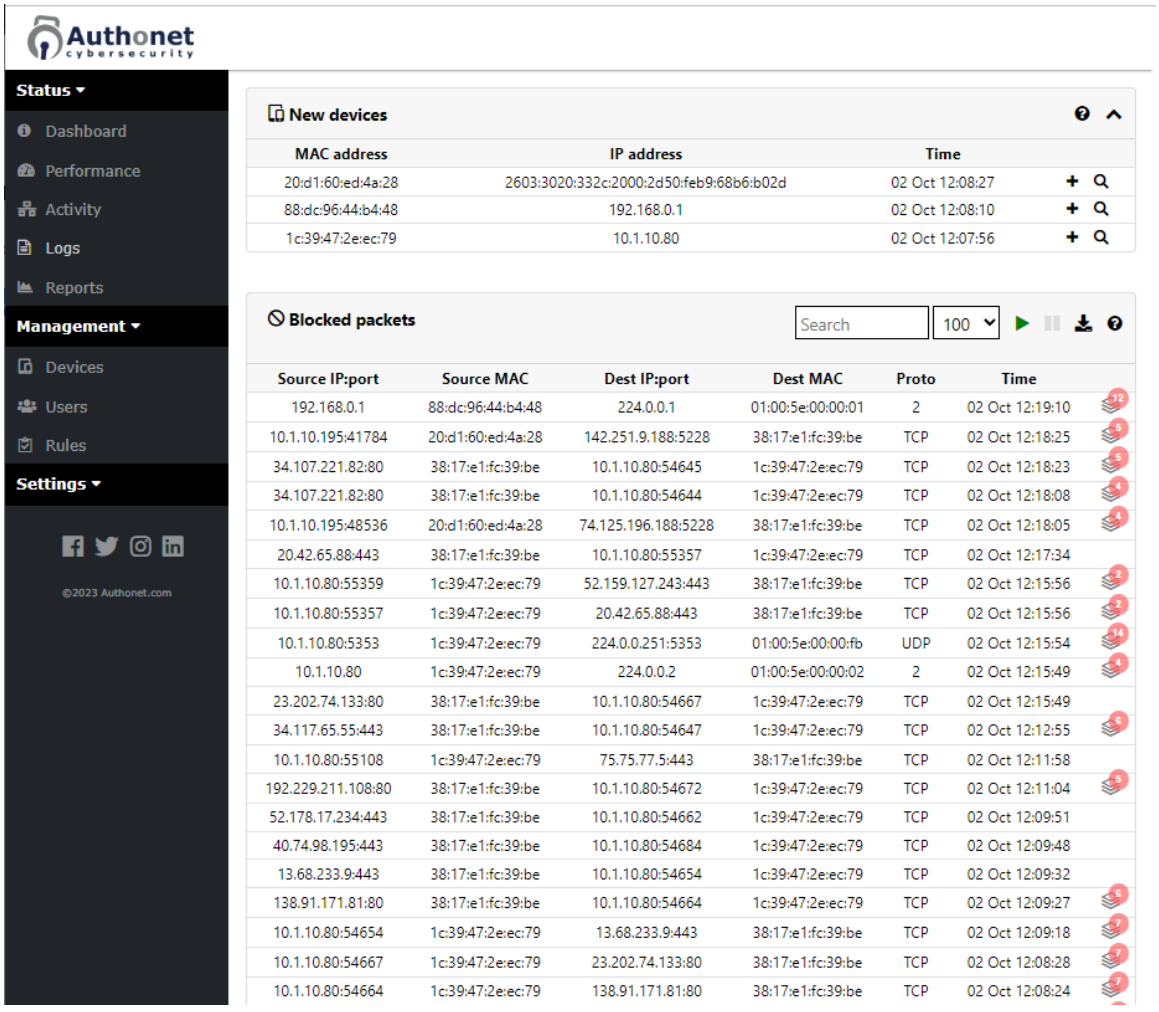




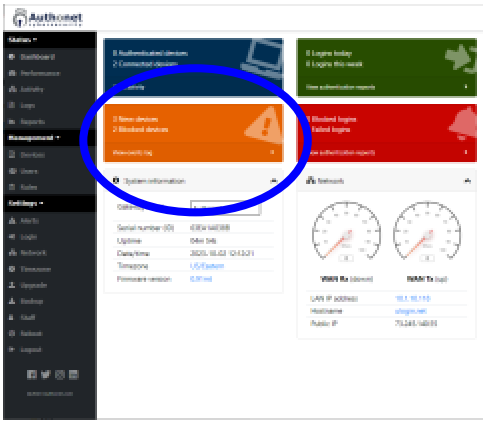
Information Bars: New devices, blocked devices

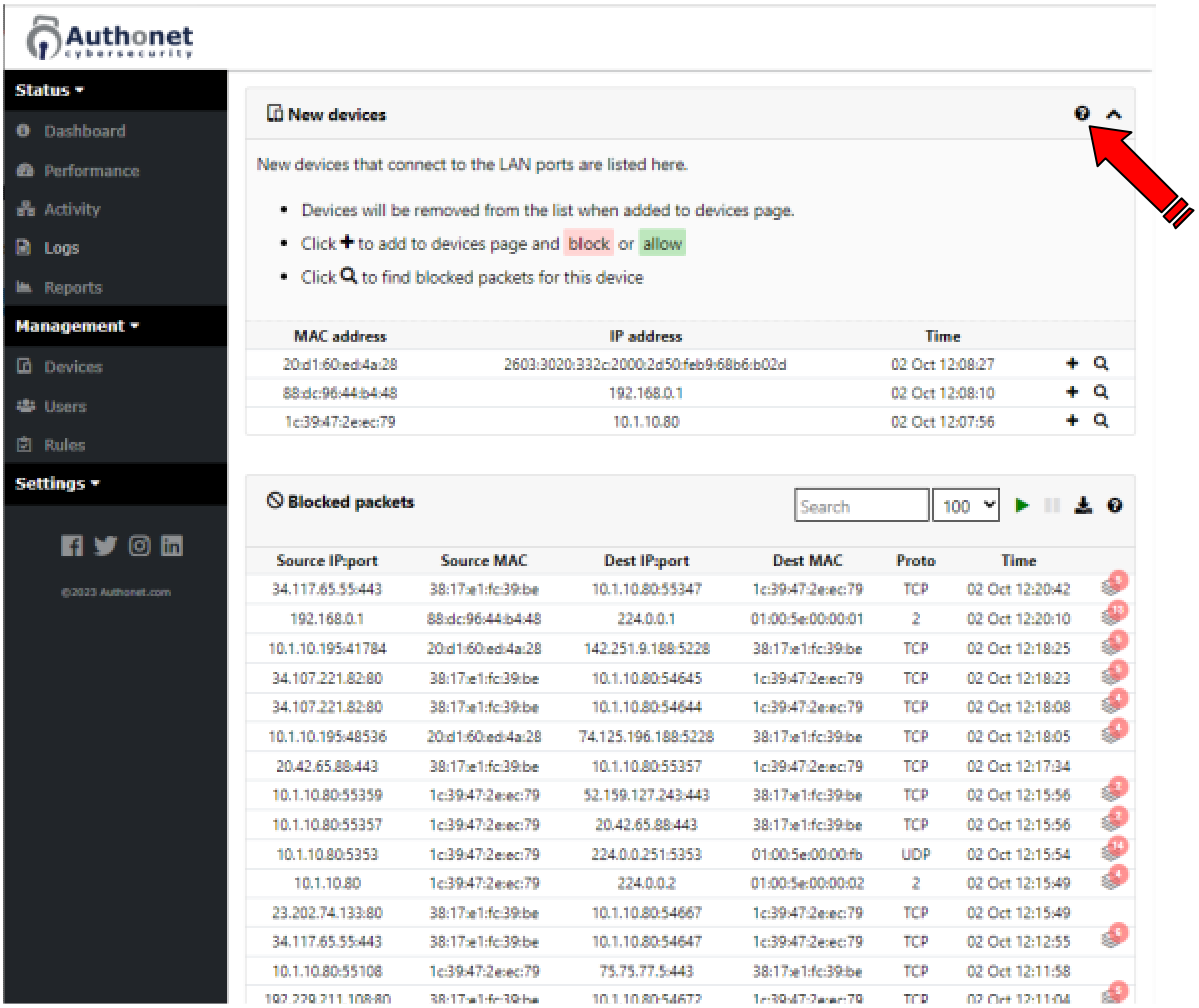
The bottom left information bar is a shortcut to the events log page. The last 10,000 events are displayed. Older events are deleted. The cloud service stores the event history up to 1 year.





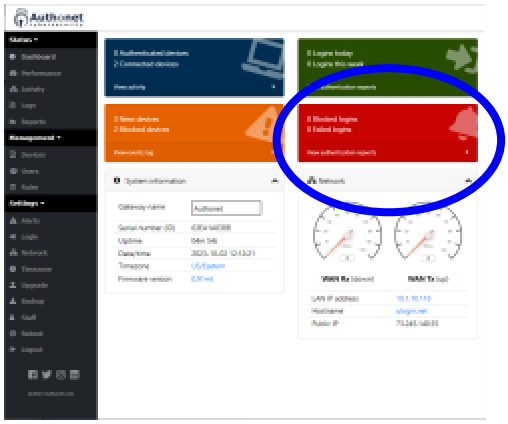
Clicking the question mark symbol displays additional information about the data being displayed.

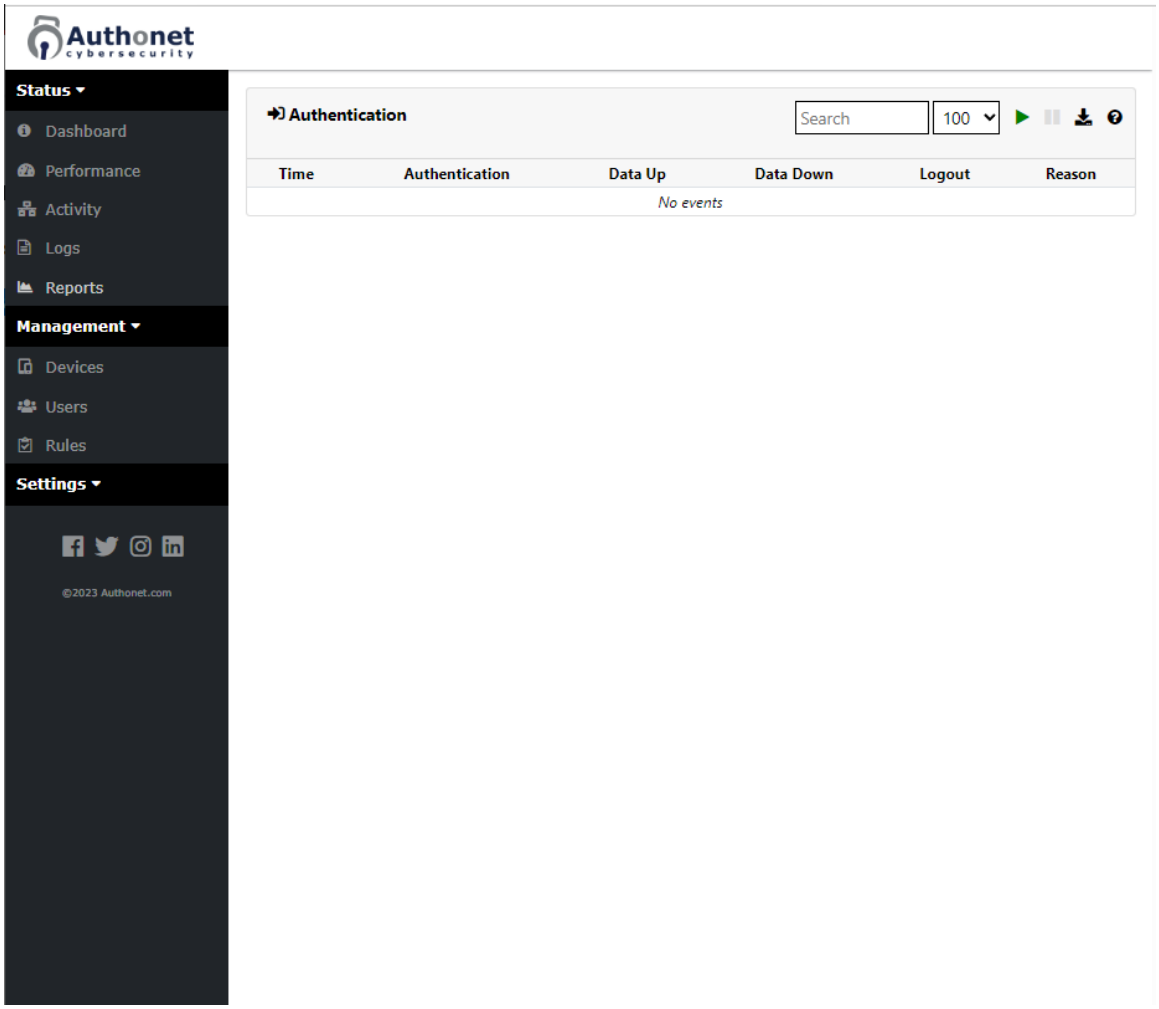




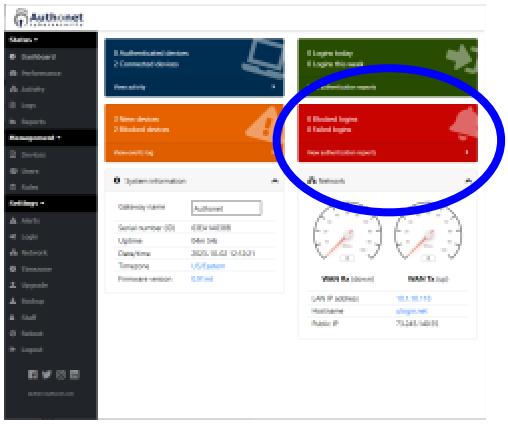
Information Bars: Blocked logins, failed logins

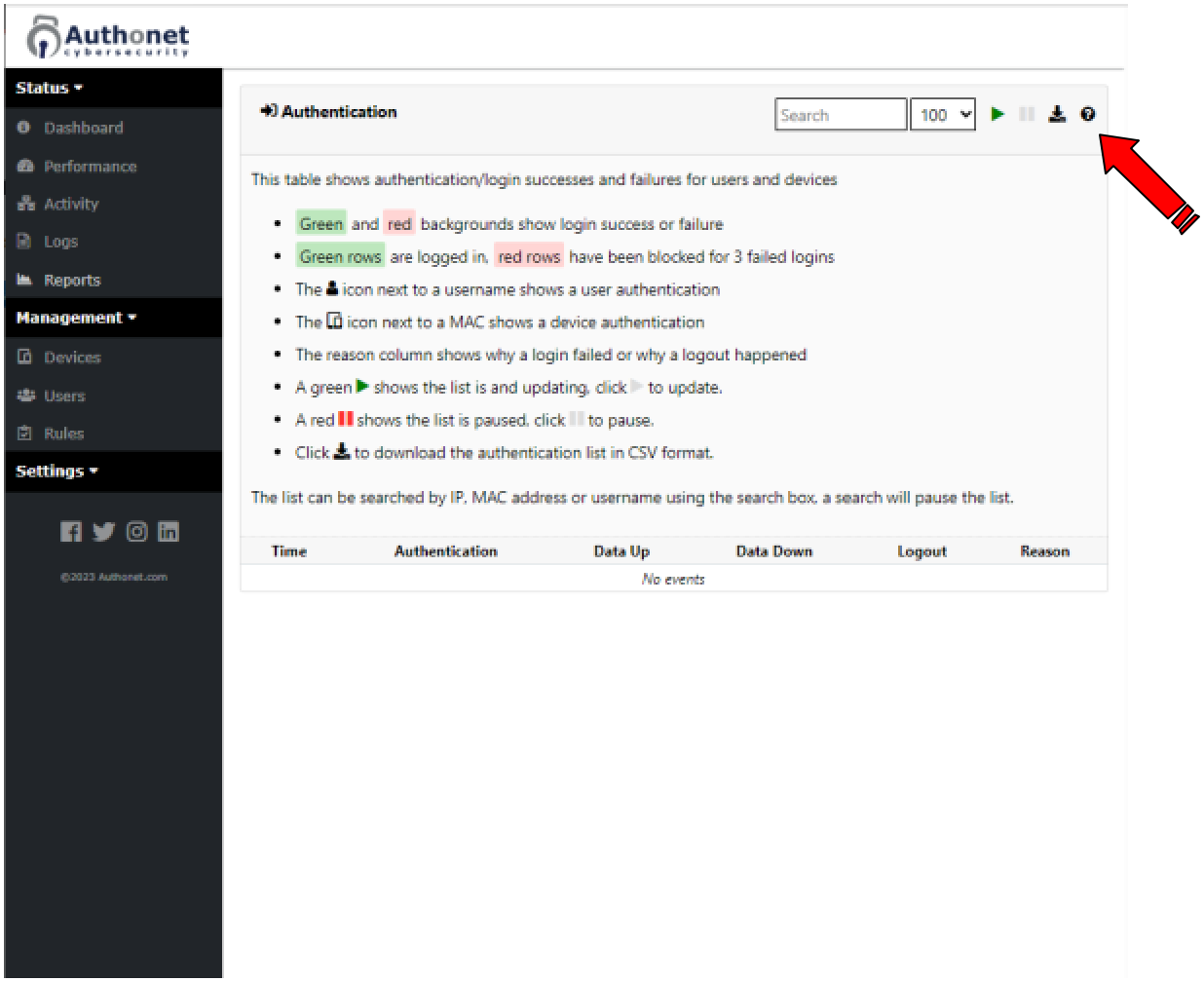
The bottom right information bar is a shortcut to the authentication report page.





Clicking the question mark symbol displays additional information about the data being displayed.



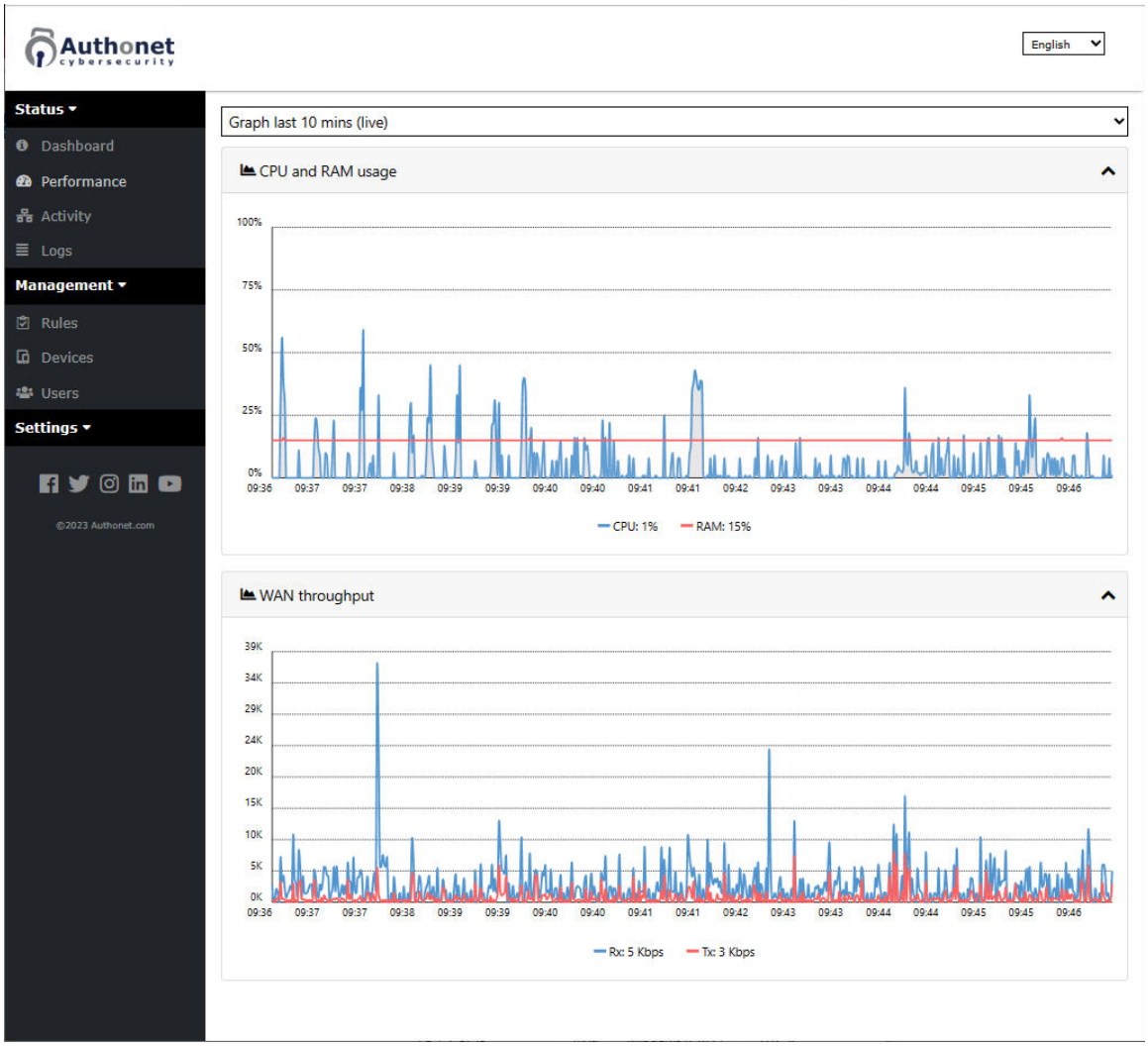


Performance Charts

The performance charts show two parameters.

- CPU and RAM usage: indicates the processing overhead of the Authonet ZTNA gateway, the processing overhead is determined by the type of data traffic over the business network.
- WAN throughput: indicates the utilization of the WAN circuit for data download and data upload. The user Internet access frequency and software applications determine the data bandwidth utilization. With cloud based applications the WAN utilization will be higher than with applications installed on a LAN server.

Verify that the gateway utilization is not constantly operating at the maximum. If this is the case then it is necessary to upgrade to an Authonet gateway with a higher throughput.



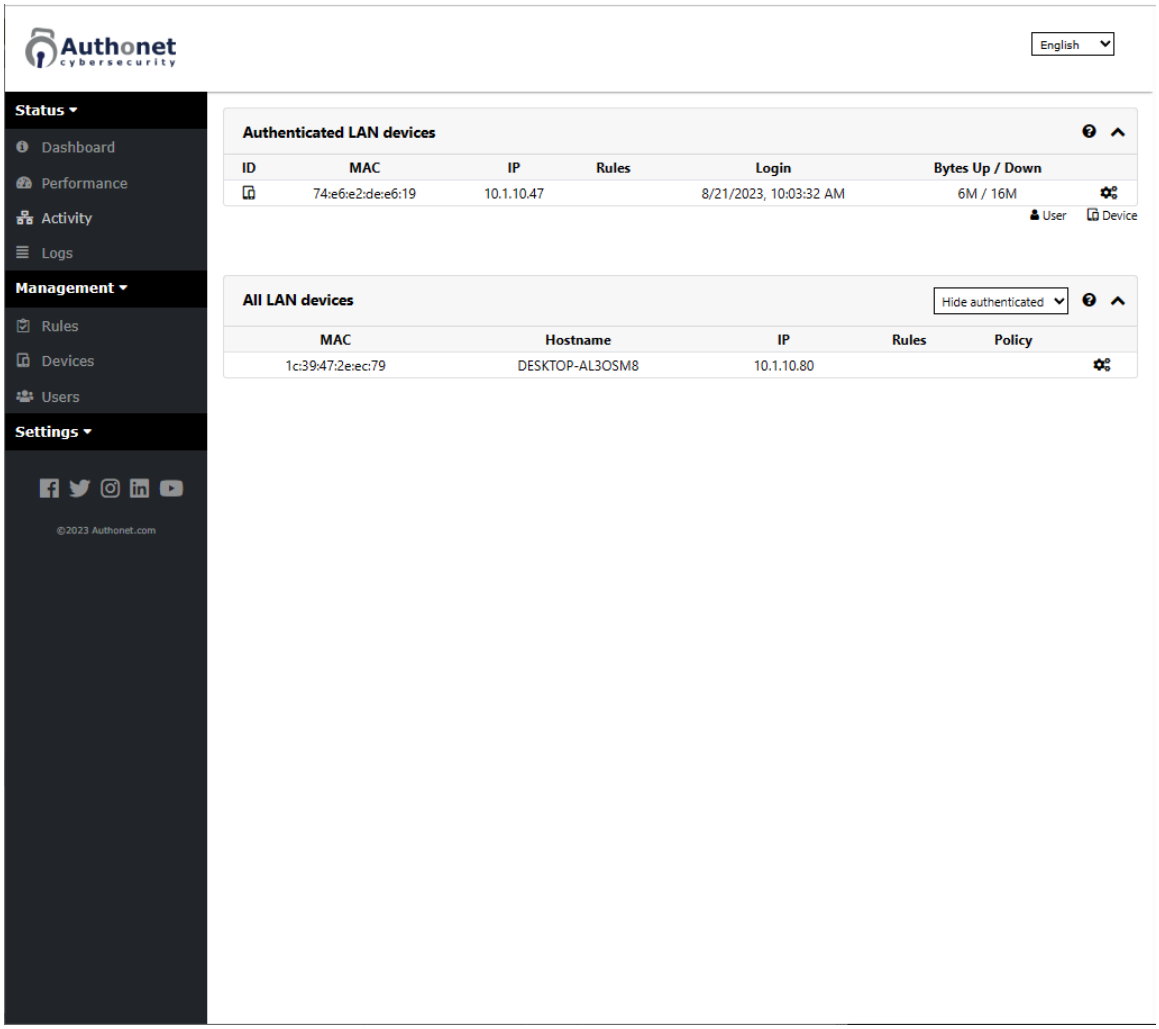
Verify that the WAN transmit and receive operating speeds are not at the maximum for the ISP circuit. If so then it is necessary to upgrade to a faster service.

Network Activity

Two data groups are shown on the activity chart.

- Authenticated LAN devices: devices and users that have been authenticated and have access to the LAN and to the Internet are listed.
- All LAN devices: devices that are connected to the Authonet user LAN ports are listed; this list includes both recognized devices and unrecognized devices.

The administrator can consult network activity to identify devices and users accessing the business network.

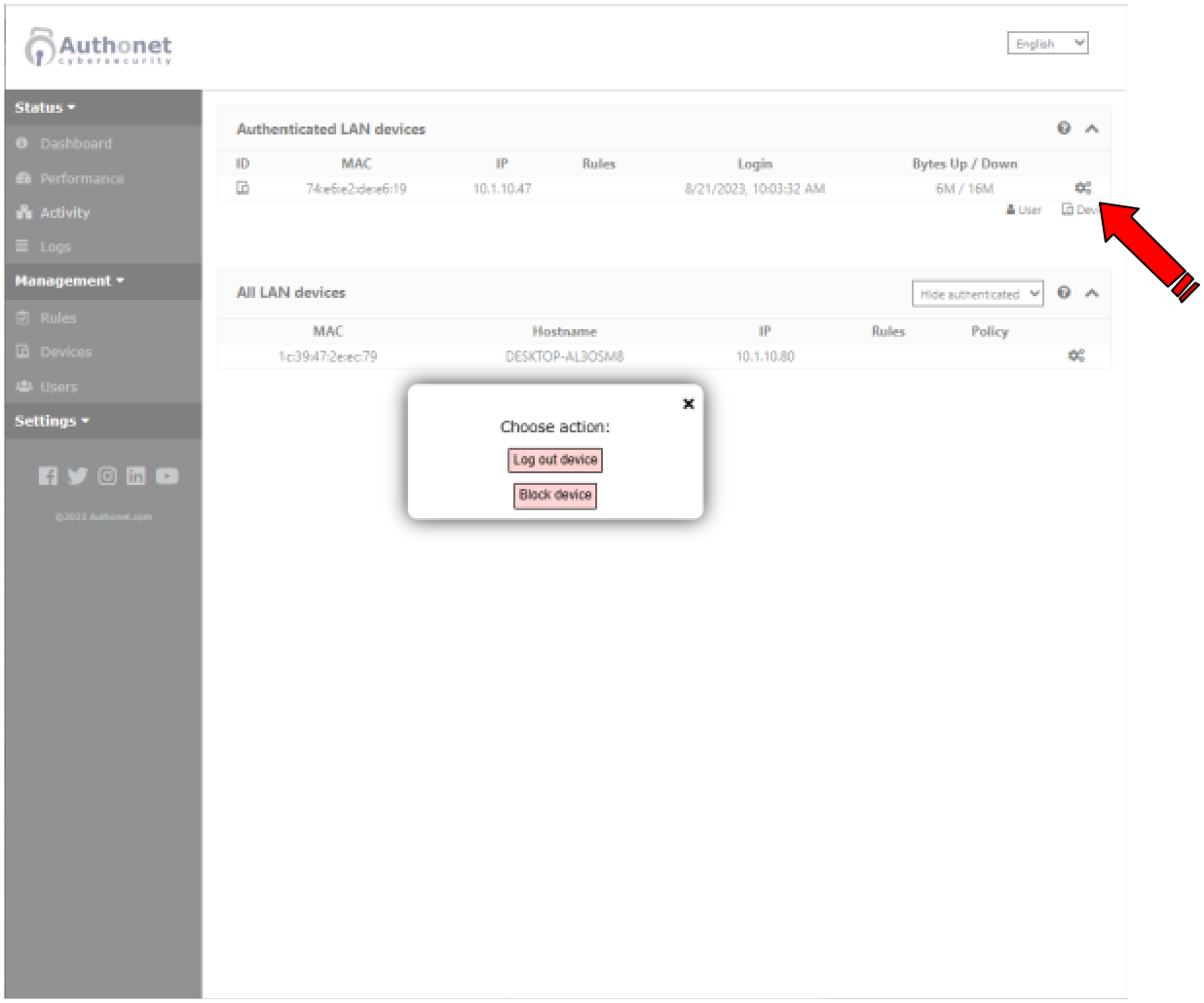


The status of any devices listed in ‘authenticated LAN devices' can be changed. Click on the gear symbol shown to open a box with two status change options.

- Log out device.
- Block device.

This is a useful tool for use when the administrator identifies traffic characteristics that might indicate the device has a virus. Blocking the device will protect the network and give an opportunity to examine the device.

The configuration command is shown in the next figure.



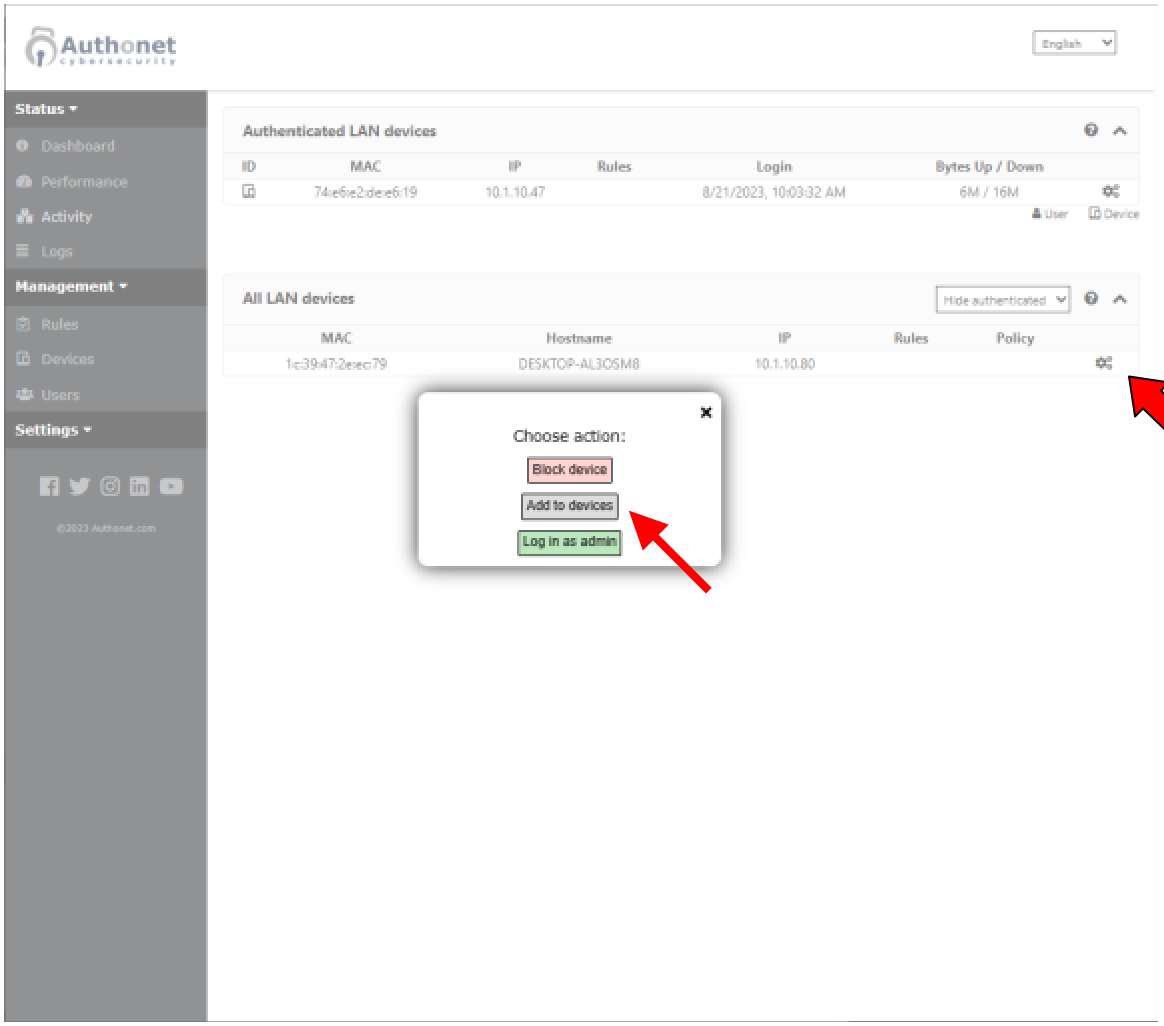
The status of any devices listed in ‘all LAN devices’ can be changed. The status options are listed below.

- Block access.
- Add to devices.
- Login as admin.

When the 'add to devices' option is clicked the device is added to the device list.

This feature provides a quick method of adding all network devices into the device list when the Authonet ZTNA gateway is first installed in the business network.

The configuration command is shown in the next figure.

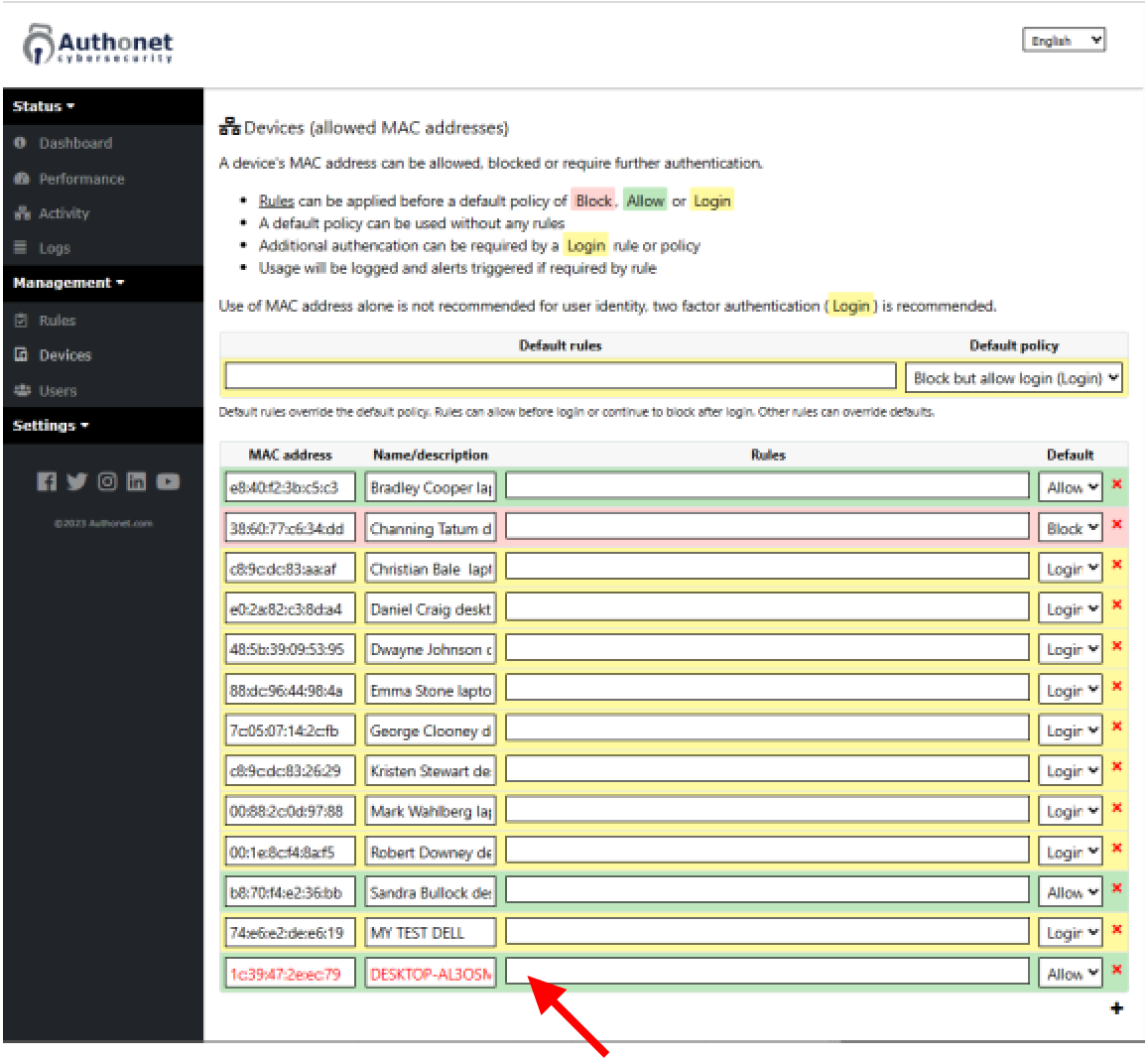


When the ‘add to devices’ button is clicked the device appears on the device list. This new device entry shown in red is illustrated in the next figure.

Click the update devices button to add the MAC to the list permanently.

The new device entry is allowed access to the network and to the Internet. It is necessary to set rules for the device to determine what it can and cannot access.

Administrators and Network IT installers should follow this procedure to add devices during the Authonet ZTNA gateway installation and configuration process.

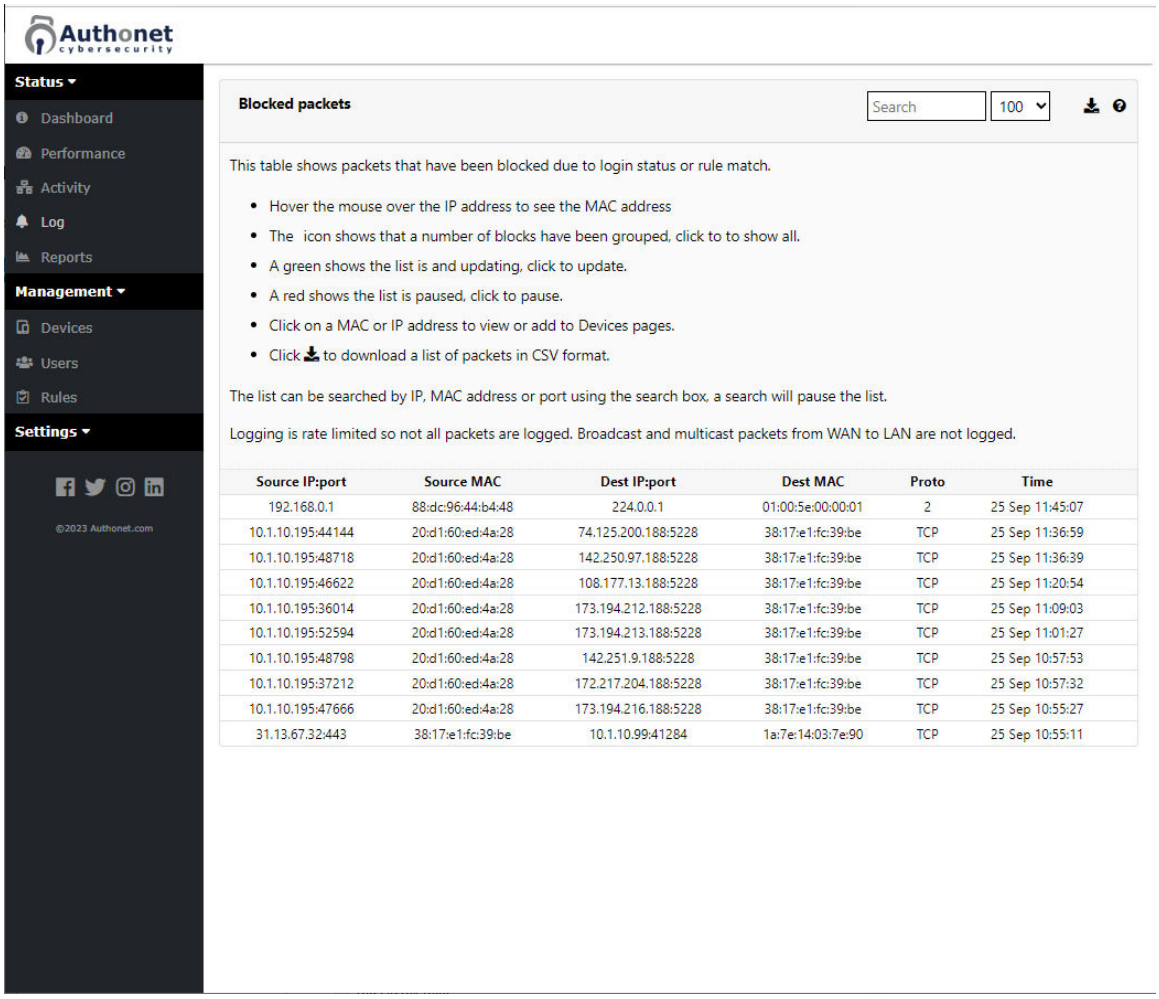


Network Access Log

The log of events records each device access to the network with the action that was taken and a time stamp. The device log stores the last 10,000 records. The cloud log stores up to 1 year of records.

The log is valuable when a security specialist is diagnosing potential network attacks.

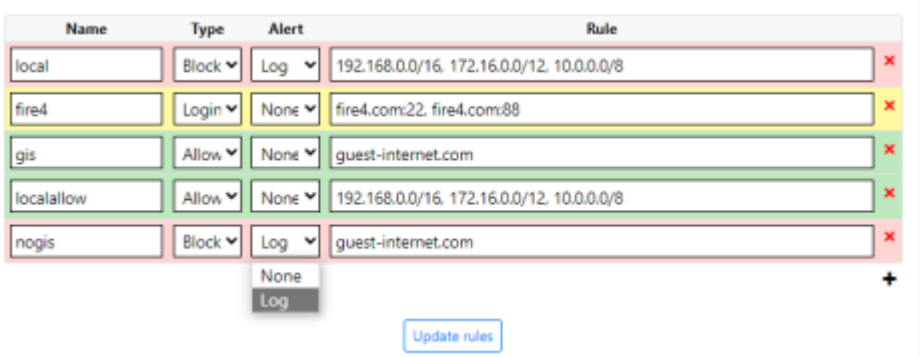
For example, a device that is not authorized to access a server but has a Trojan virus installed will show a series of blocked actions to the IP address of the server.

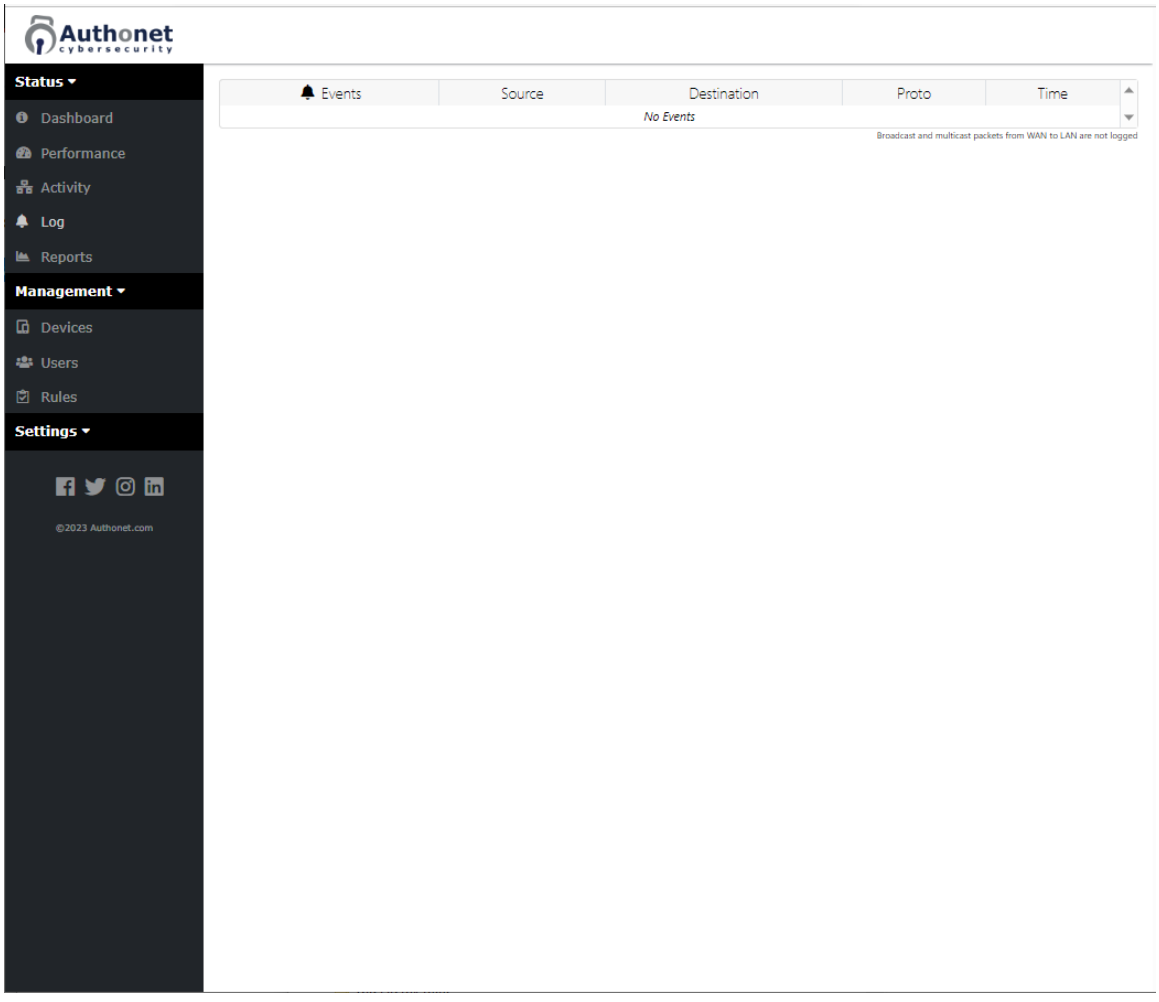


Source IP:port	Source MAC	Dest IP:port	Dest MAC	Proto	Time
192.168.0.1	88:dc:96:44:b4:48	224.0.0.1	01:00:5e:00:00:01	2	25 Sep 11:45:07
10.1.10.195:44144	20:d1:60:ed:4a:28	74.125.200.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 11:36:59
10.1.10.195:48718	20:d1:60:ed:4a:28	142.250.97.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 11:36:39
10.1.10.195:46622	20:d1:60:ed:4a:28	108.177.13.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 11:20:54
10.1.10.195:36014	20:d1:60:ed:4a:28	173.194.212.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 11:09:03
10.1.10.195:52594	20:d1:60:ed:4a:28	173.194.213.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 11:01:27
10.1.10.195:48798	20:d1:60:ed:4a:28	142.251.9.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 10:57:53
10.1.10.195:37212	20:d1:60:ed:4a:28	172.217.204.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 10:57:32
10.1.10.195:47666	20:d1:60:ed:4a:28	173.194.216.188:5228	38:17:e1:fc:39:be	TCP	25 Sep 10:55:27
31.13.67.32:443	38:17:e1:fc:39:be	10.1.10.99:41284	1a:7e:14:03:7e:90	TCP	25 Sep 10:55:11

Reports

Reports show events that were selected for the log and reporting when a rule was created. The attempt to break a rule might indicate an attempted intrusion.





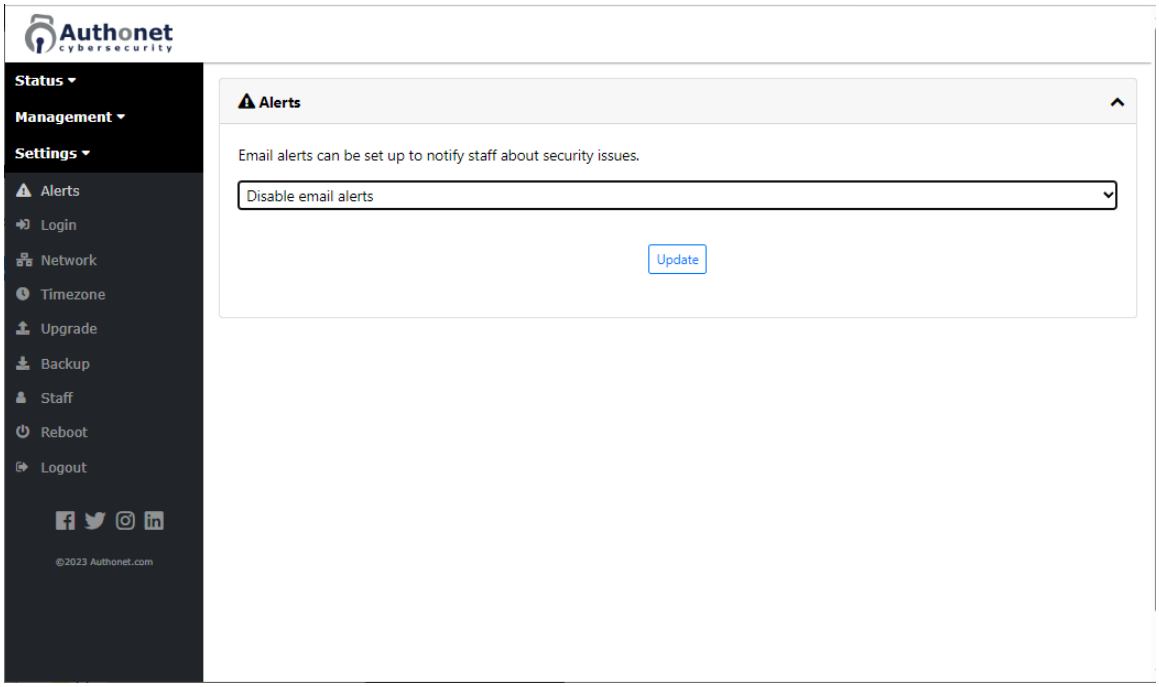
PART 5:

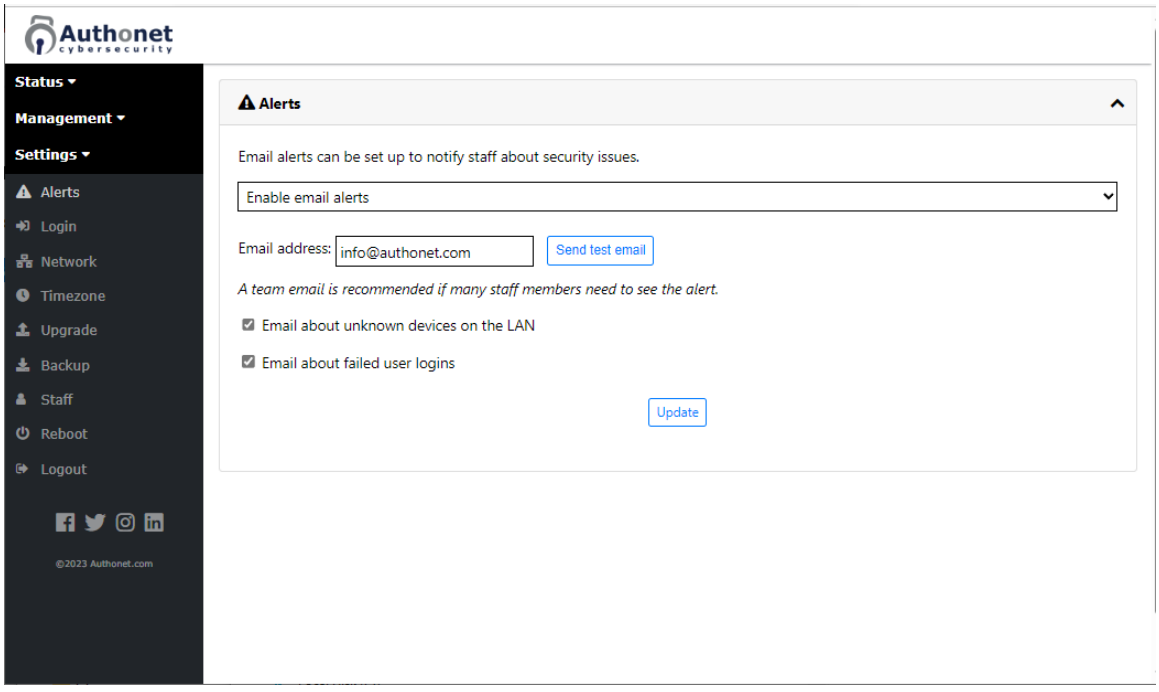
Configuring the Authonet ZTNA Gateway for Use

Sending Email Alerts

Potential intrusion situations that require urgent attention can be notified to the administrator with an email alert. There are two situations that are of concern., unknown devices that connect to the LAN network, and user authentications that have failed multiple times

The email addresses to which the alert will be sent is put in the email address box and tested prior to use. The alerts are selected using check boxes. This is shown in the following screens.

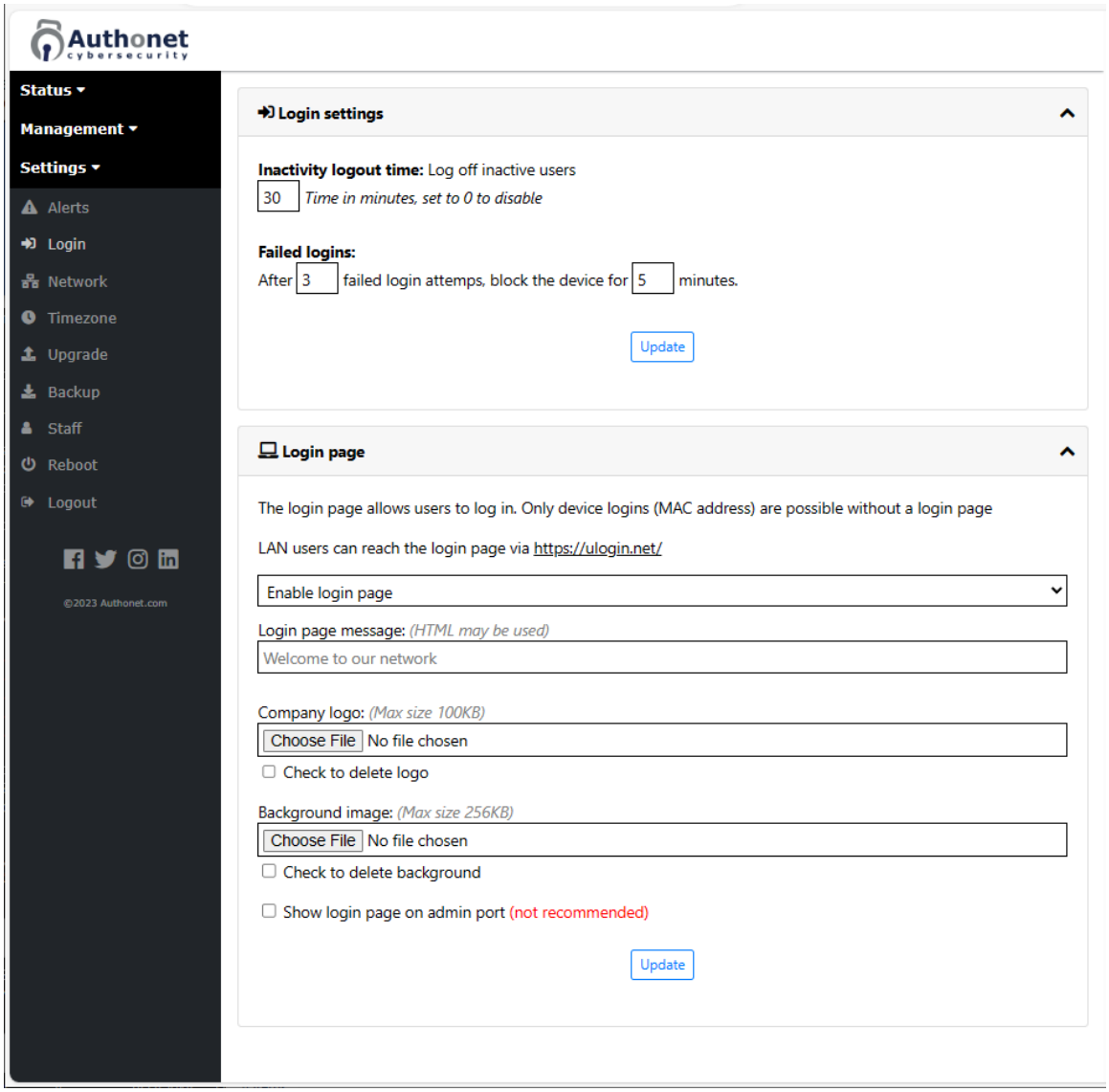




There are two conditions to send out email alerts to the administrator.

- Unknown devices that have connected to the LAN
- Multiple failed authentication logins

The login page specifies the number of failed attempts that are tried before the access is blocked and an email alert is sent to the supervisor. Multiple failed authentication attempts may indicate that a password has been stolen and an intruder is attempting to gain access.



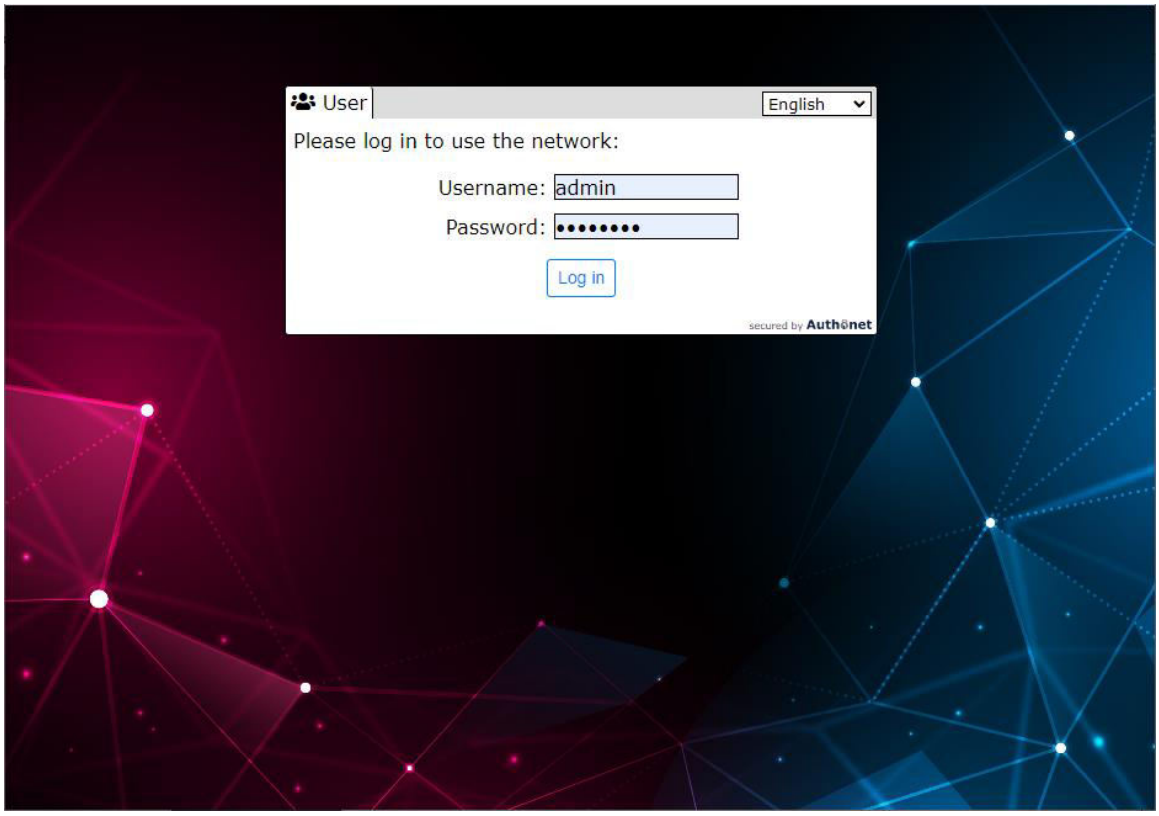
Customizing the Login Page

Any user device that connects to a user LAN port will obtain an IP address from the LAN network and when a new browser tab is opened the login page will be displayed by default. As no devices or users have been configured yet the user will have no login credentials.

Using the configuration tools, the login page can be selected for some users, or eliminated for all users.

The login page can be branded for the customer by uploading a background image and a logo image. Alternatively a business can create a custom image that includes the business logo.

The default login page is shown in the next figure. The default login page has a background image but no logo.

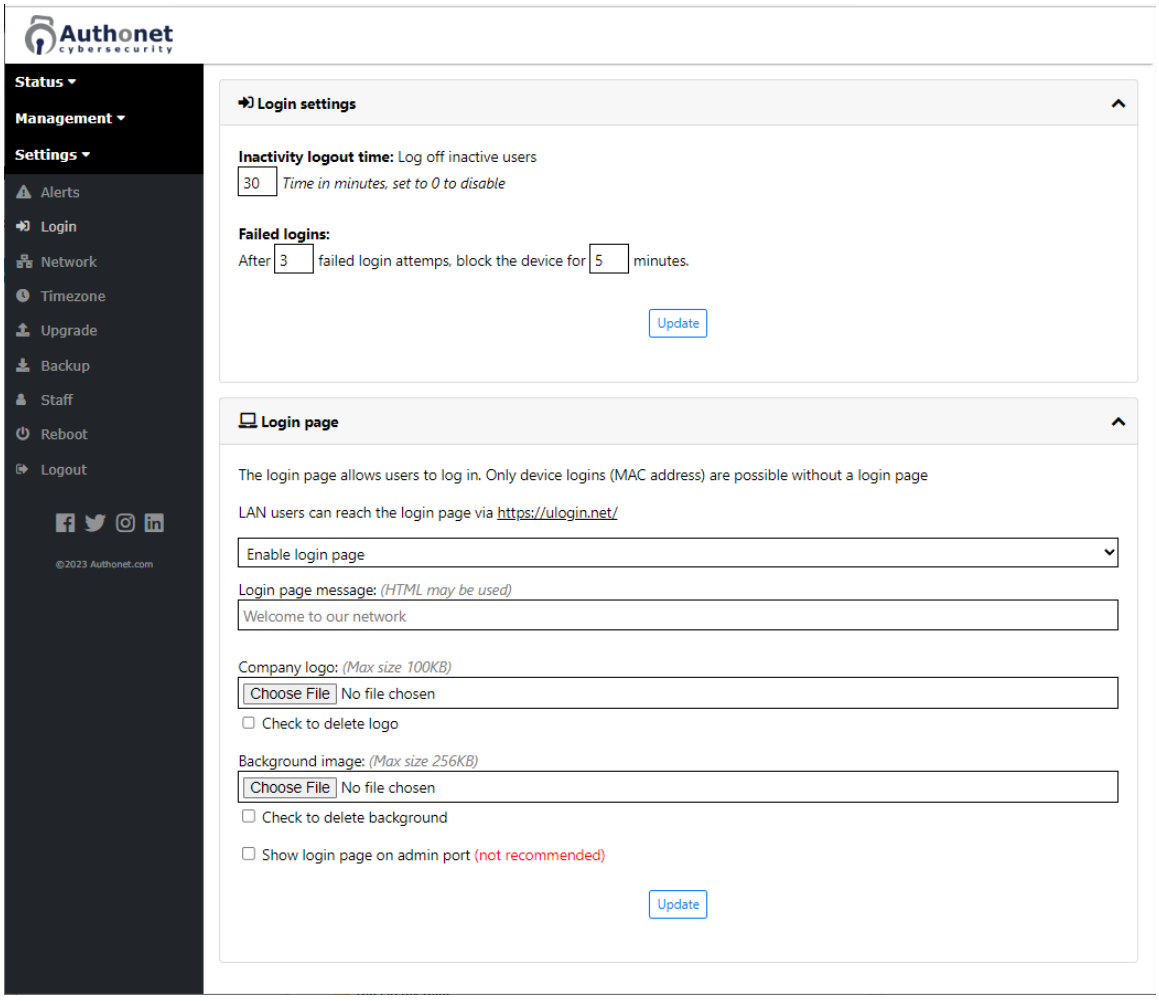


The login page customization has six parameters.

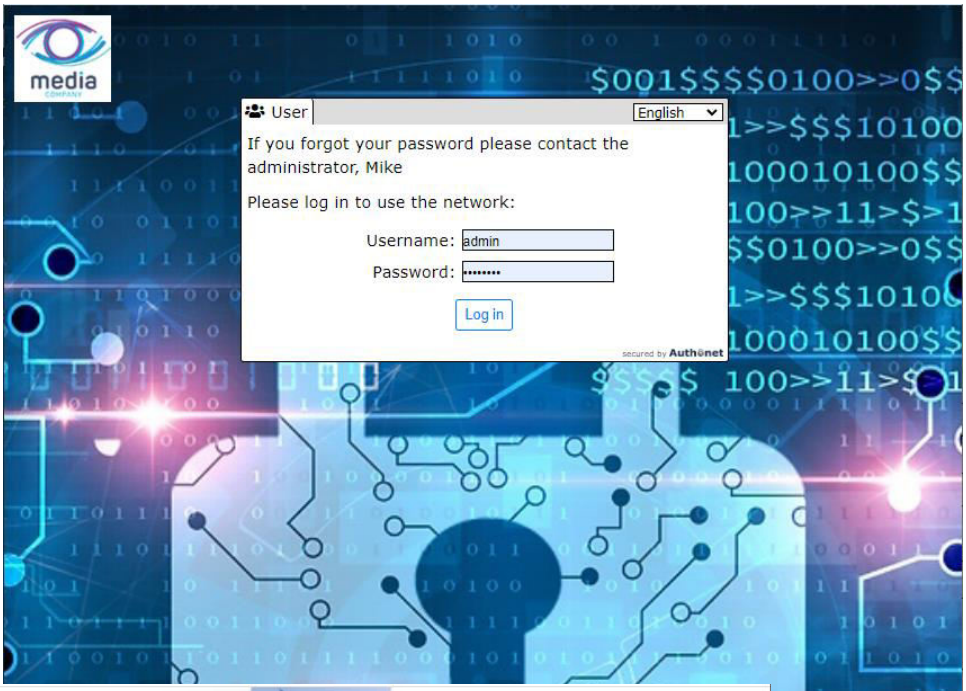
- Inactivity logout time; this is the time in minutes that a user will be logged out if there is no data transfer activity. This timer can be setting to zero to disable it. As most devices have apps that constantly communicate with the Internet it is likely that a device will have to be switched off to logout.

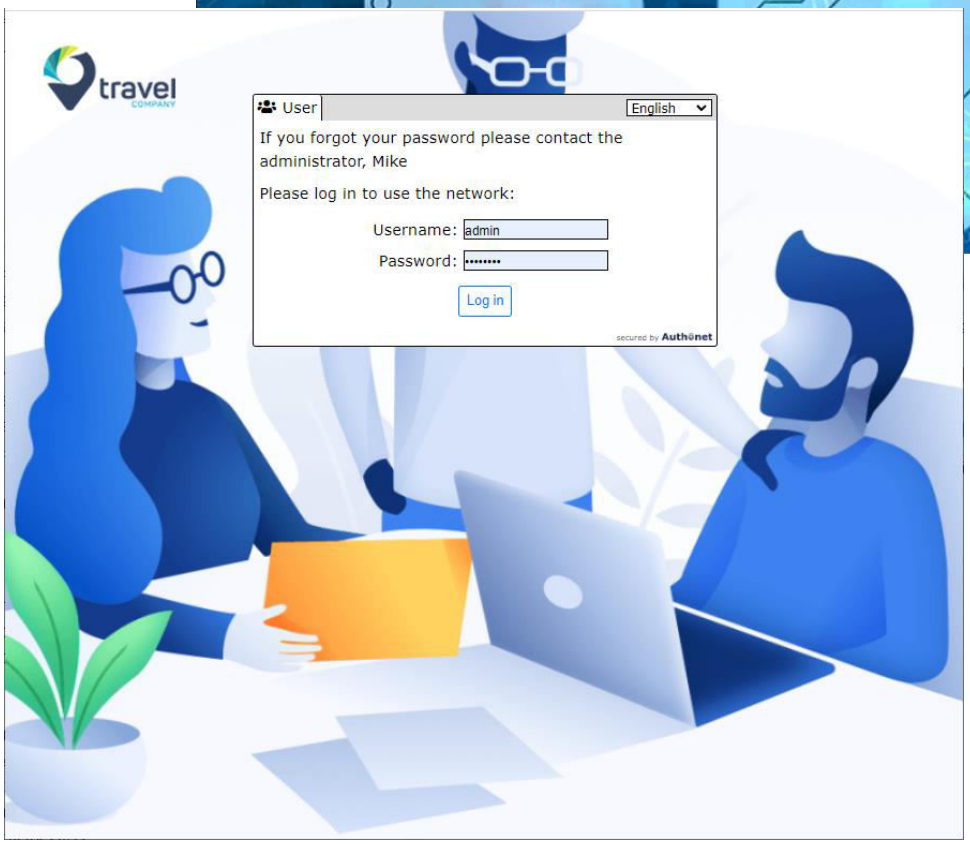
- Failed login attempts; if a number of login attempts (e.g. 3) has failed then the user must wait for the specified time before attempting a login again. An alert email to the administrator can be triggered by failed logins.
- Enable / disable login page; when enabled the login page can be selectively enabled for any device or user. When disabled using the drop down menu, the login page is not displayed even when a device or user is configured for login.
- Login page message; a personalized message is seen on all login pages, this might be the administrator contact for a case when a user cannot login.
- Upload a company logo to the login page.
- Upload a background image to the login page.
- Enable a login page for the administrator, this is not recommended because the login page does not accept administrator or staff credentials, only user credentials, permitting user login on LAN4.

The customization menu for login page is shown in the following screen shot.



Examples of customized login pages are shown in the following two figures. The business logo is displayed on the upper left of the screen. A customer can create a customized background image that incorporates the business logo plus additional information, such as instructions for use.





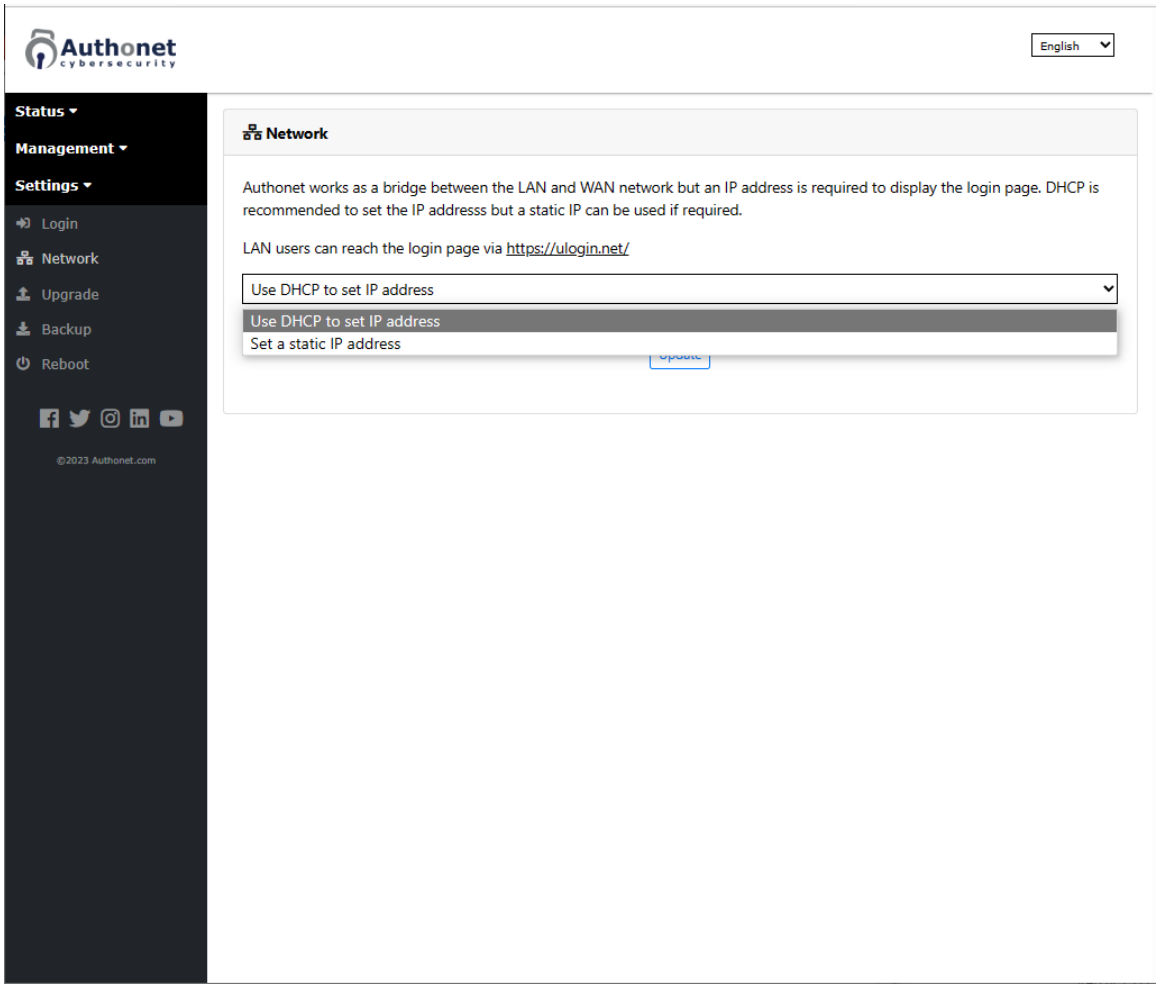
Network Configuration

The Authonet ZTNA gateway is a network bridge. DHCP requests from user computers connected to the Authonet gateway user LAN ports are forwarded to the network DHCP server that is usually the ISP network router. The ISP router will be configured for one of the private address ranges:

- 192.168.xx.xx.
- 172.16.xx.xx.
- 10.xx.xx.xx.

Some networks may be configured for all devices to have static IP's. This is not a common configuration as IP administration has to be done manually. However if the customers network uses a static IP configuration then the network page drop down menu should be changed from the default "use DHCP to set IP address" to "set a static IP address". With a static IP set, DHCP requests will no longer be forwarded from the USER LAN ports to the WAN port.

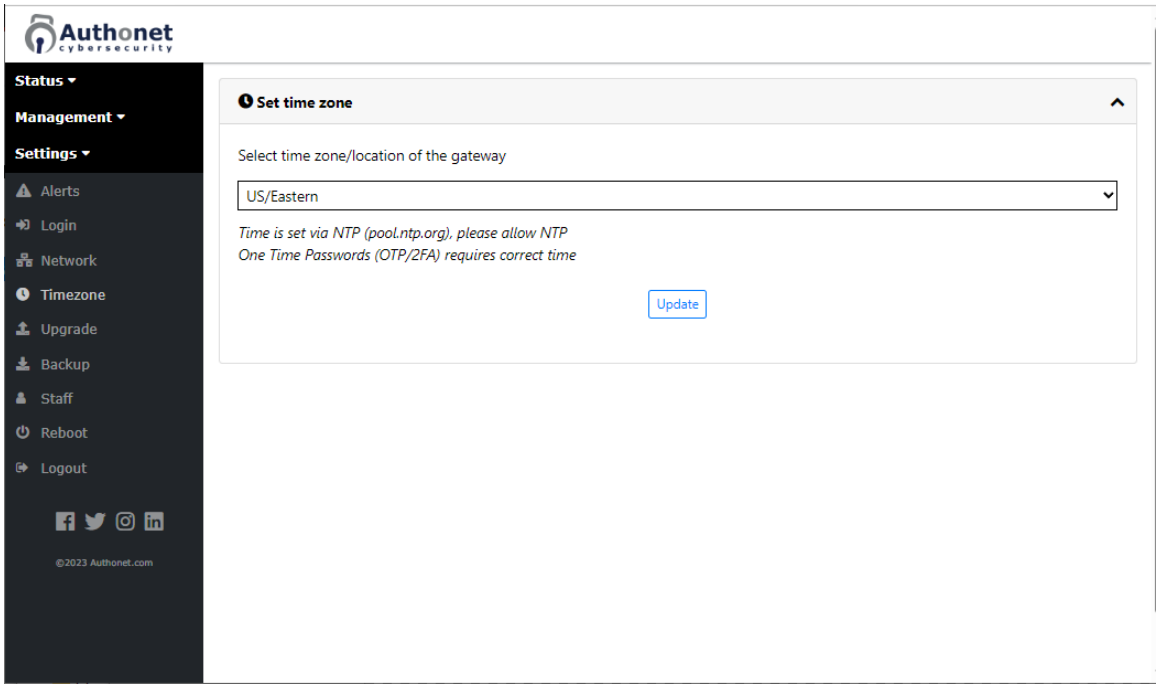
The next figure shows the network configuration page with the drop down menu for the IP address setting.

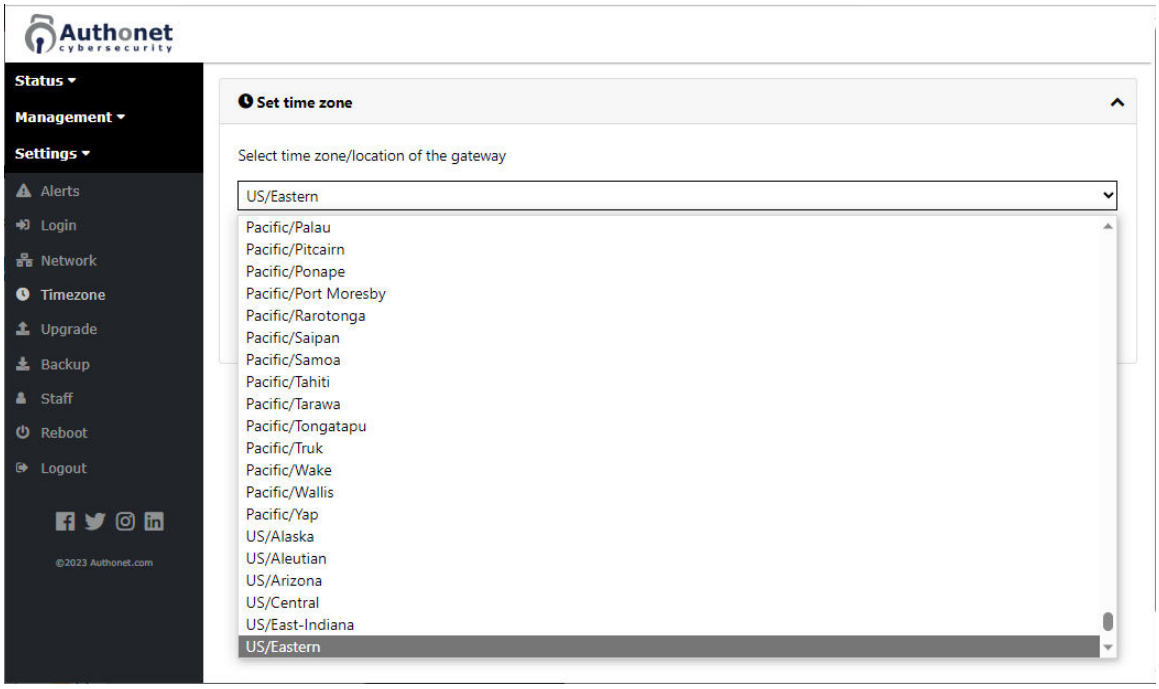


Set the Time Zone

The time zone has to be set for the region where the Authonet gateway is installed. The functioning of the one time password (OTP) phone app depends on the correct setting of the time zone, which must correspond to the time zone of the mobile phone.

The screen for the time zone setting is shown below.





Upgrade Firmware

Authonet frequently release firmware upgrades for the ZTNA gateway products. There is no charge for the firmware upgrades.

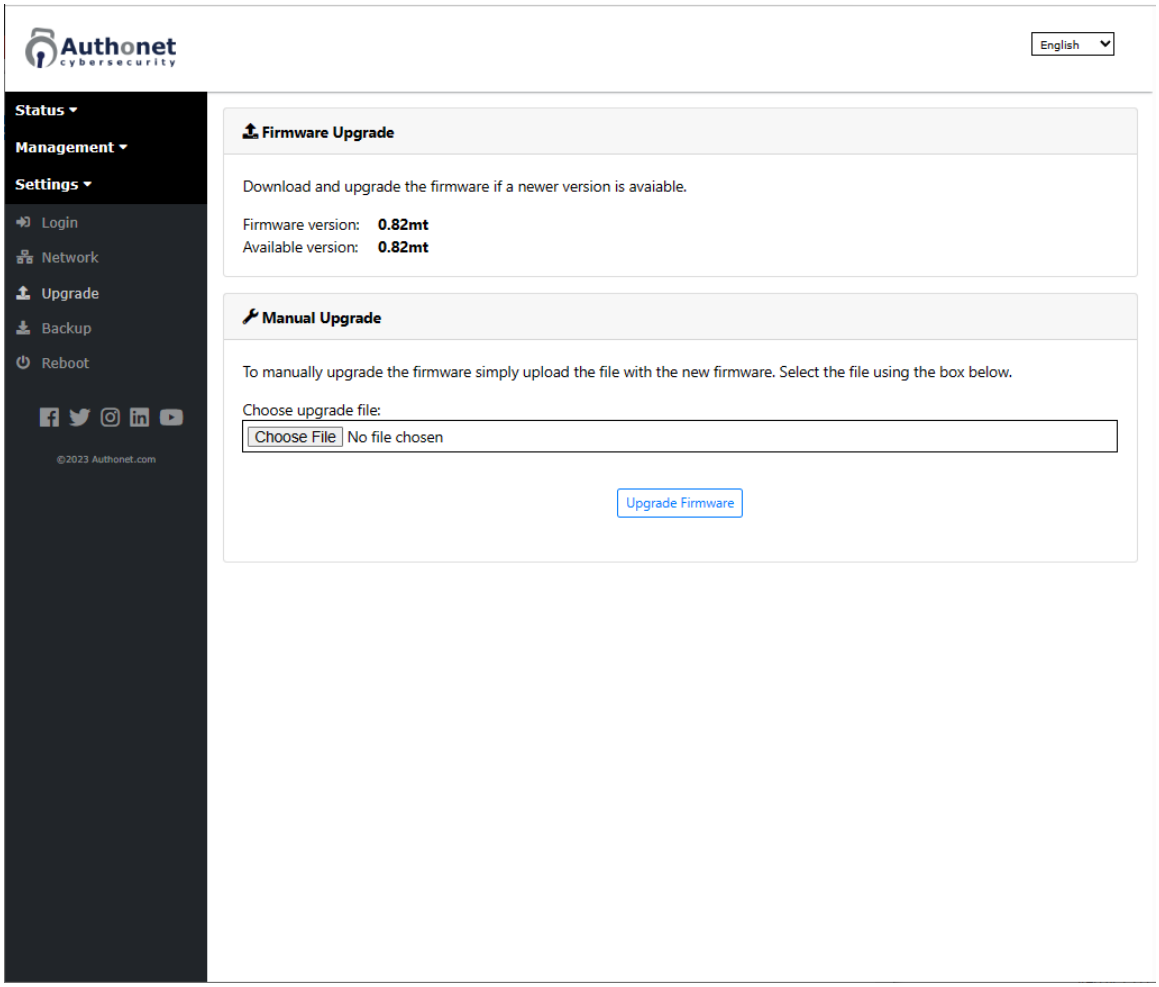
Upon receiving and configuring an Authonet gateway the administrator should check the firmware upgrade page to verify the version of the installed firmware and the latest version that is currently available. If a firmware upgrade is required then the administrator should contact our support page to request the upgrade.

https://authonet.com/support.html

The administrator will receive a link to download the firmware and then the firmware is installed using the upgrade page. Select the file on the administrator computer then click the upgrade button. When the upgrade is completed a message will prompt to reboot the product.

WARNING: Do not disconnect power to the Authonet gateway during the upgrade process until the reboot message is displayed, which may take several minutes. If disconnected the program memory will become corrupted. Wait for the reboot prompt.

The firmware upgrade screen is shown in the following figure.



Backup Settings

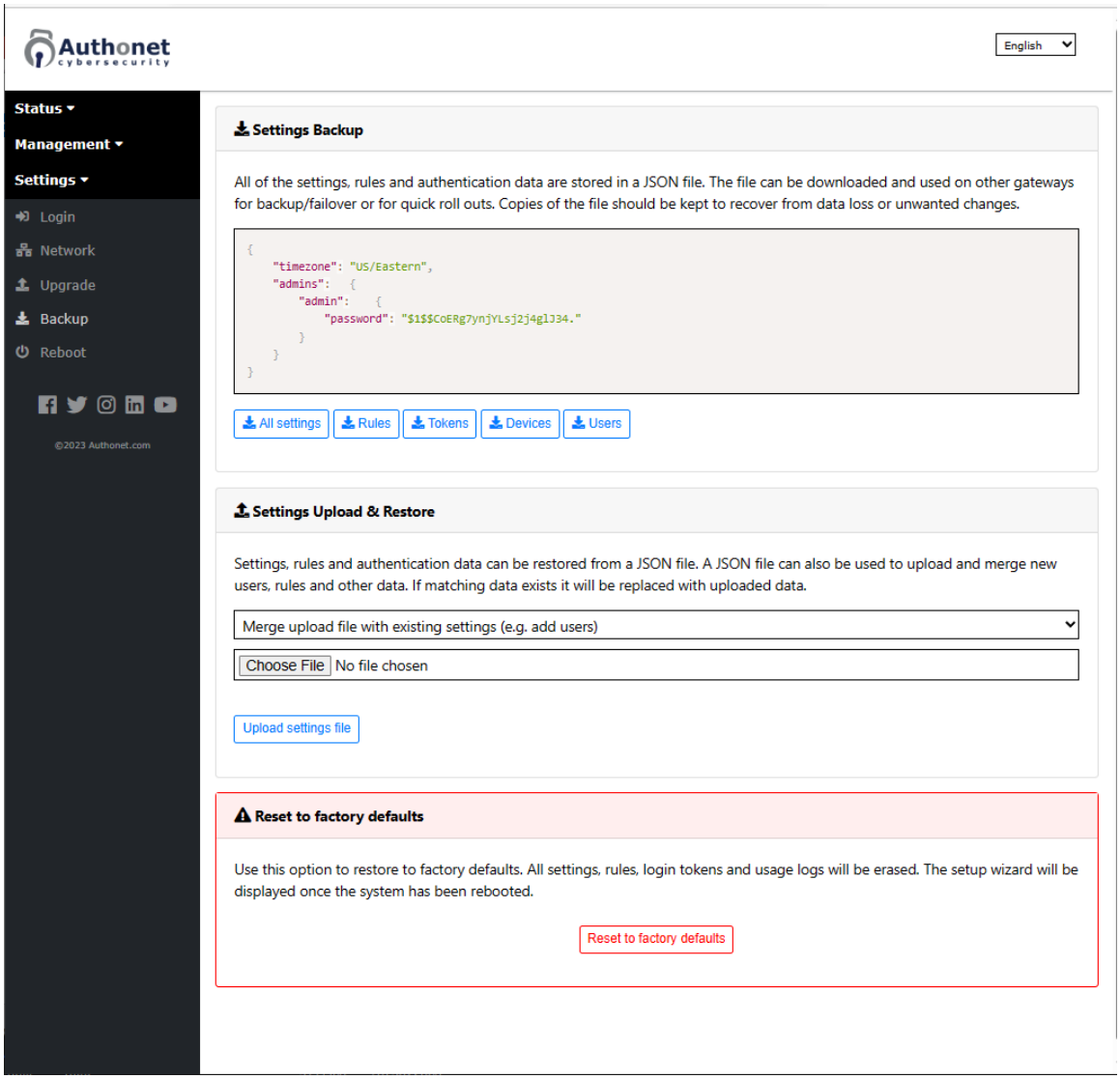
When the administrator has completed the Authonet ZTNA gateway configuration a backup of the configuration must be saved on the administrator's computer. The configuration file uses the JSON format. The backup can be full or partial.

- All settings, Devices, Users or Rules.

If the administrator makes a mistake with subsequent configurations the backup can be restored at any time.

The backup and restore process is a valuable tool for IT service businesses and managed service providers. A basic configuration can be developed which is then installed at each new customer site to speed the configuration process. The specific parameters for each site can then be configured.

The backup and restore screen is shown in the next figure.



Adding Staff and Admins

Several people in an organization or in an IT service provider can manage the Authonet ZTNA gateway. Administration has two roles, 'Admin' and 'Staff'.

The admin role has access to all the features and can manage staff. The admin user can add staff and other admins and change anybody's password.

The staff user has some limitations:

- Staff can't manage other staff and can only change their own password on the staff page.
- Staff can view but can't change rules.
- Staff can't access backups, network settings, login page settings, upgrade the firmware etc.
- Staff can't change default rules or policies.

Staff can carry out some functions as normal:

- Manage activity: Log devices & users in and out.
- Manage devices: Add, remove and change rules for devices.
- Manage users: Add, remove and change passwords and rules for users.

Staff can change rules for users and devices, this means they can allow users to access new services and block others. They can't add new rules (allow a new service that is not set up). Staff such as a 1st or 2nd line support person, can change user's rules because this is part of day-to-day business. Notifications will be sent to admins if rules are added or removed for users or devices and changes are audited.

The staff role is designed for:

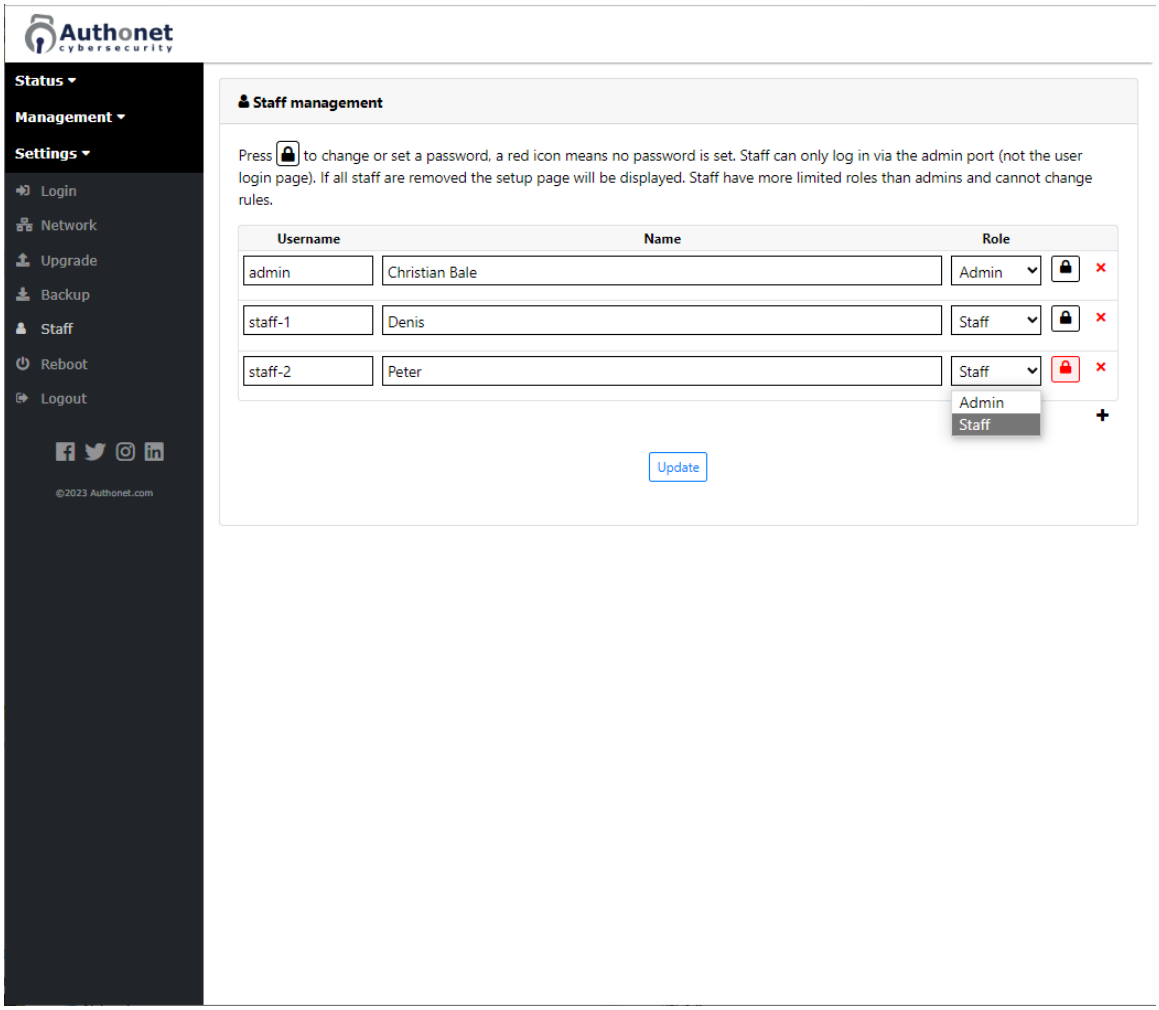
- IT staff who have a limited understanding of networks and security.
- Staff of a business that employs a service company to manage their IT.

The staff role is useful for a IT service company where the service company can set up the system and specify the rules. They have an 'admin' account. They can set up staff accounts for the customer's employees so that the service company does not have to be contacted each time an employee is added or needs access to a service. The IT service company can pass day-to-day management to the customer, and is available for IT management and support.

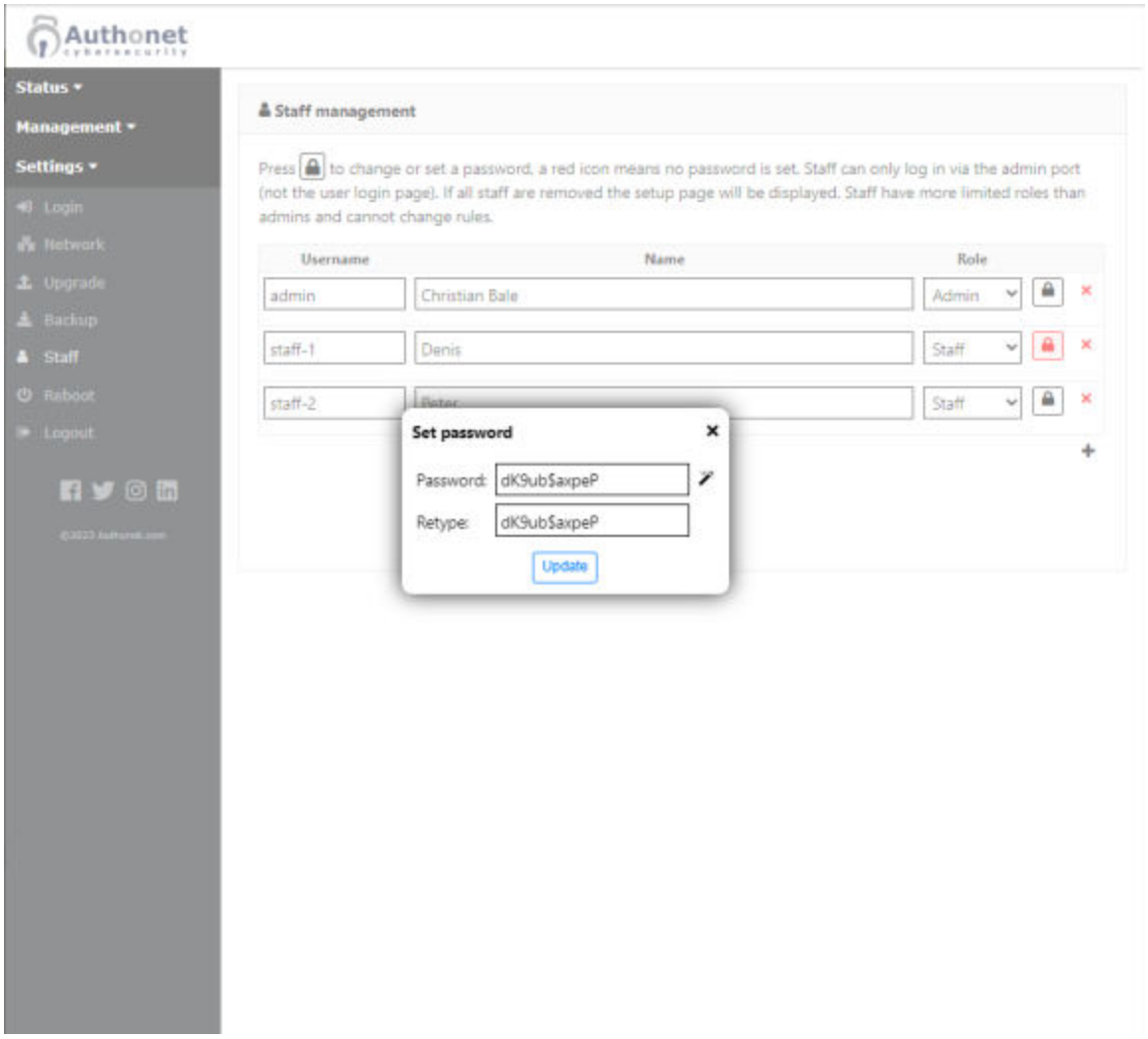
A login can be added for each admin and staff member.

The primary administrator is added during product setup, this is a requirement to begin using the product. Subsequently additional admins and staff can be added using the staff menu. Click the '+' to add a new admin or staff member.

A password has to be set for each admin and staff member. The red lock symbol indicates that a password has not been set. Click on the symbol to set the password for that admin or staff member.



When the lock symbol is clicked a password entry box is opened. Click the pen symbol on the right to auto-generate a password that meets the strength requirements. Click the update button to save the password.

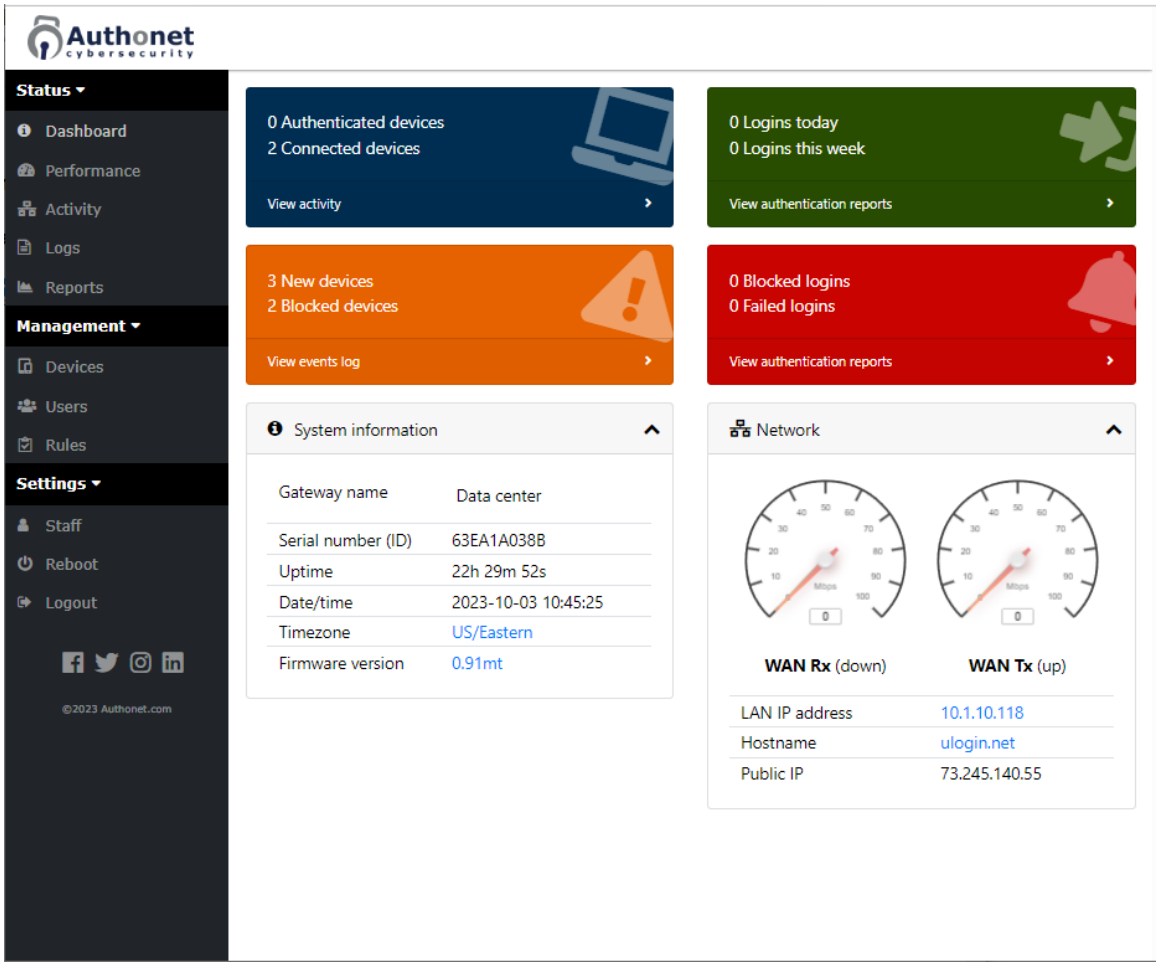


A staff member must login using the LAN4 connection, which is the admin connection. Open a browser and open a new tab. A login box will open.

Enter the staff member username and the password generated for that staff member.

The dashboard page will open. The menu has fewer configuration pages for the staff member than for the admin login as explained previously.

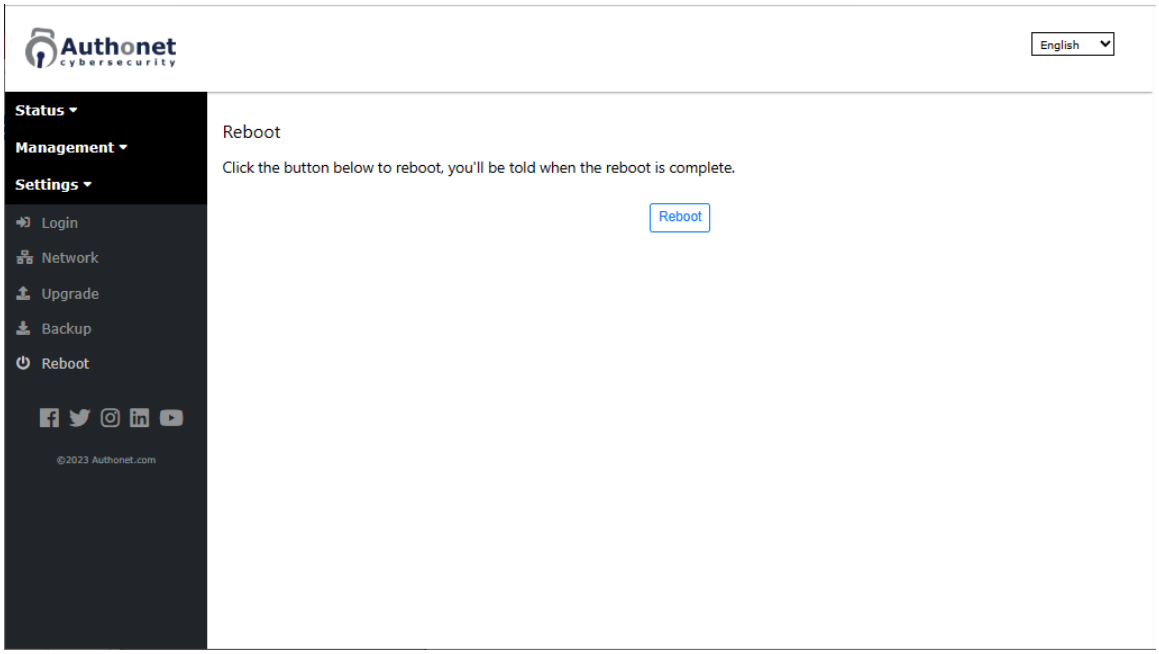
An example of the staff login page is shown in the next figure.



Reboot

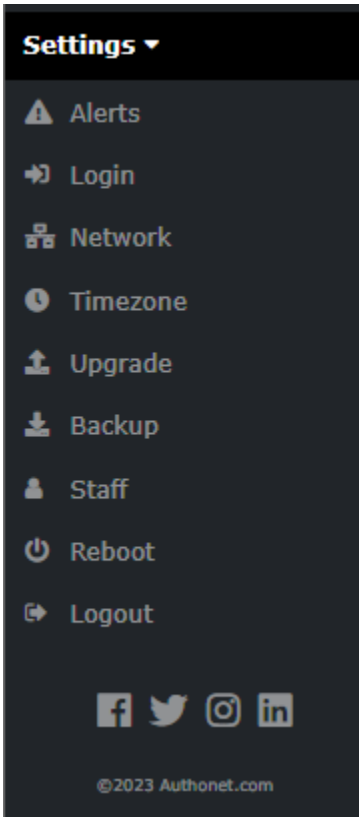
Reboot can be initiated after a configuration change, although most configuration parameters do not require a reboot. Exceptions are the network change from DHCP to static and upon completion of a firmware upgrade.

The reboot screen is shown in the next figure.



Logout

Terminates the administrator session.



PART 6:

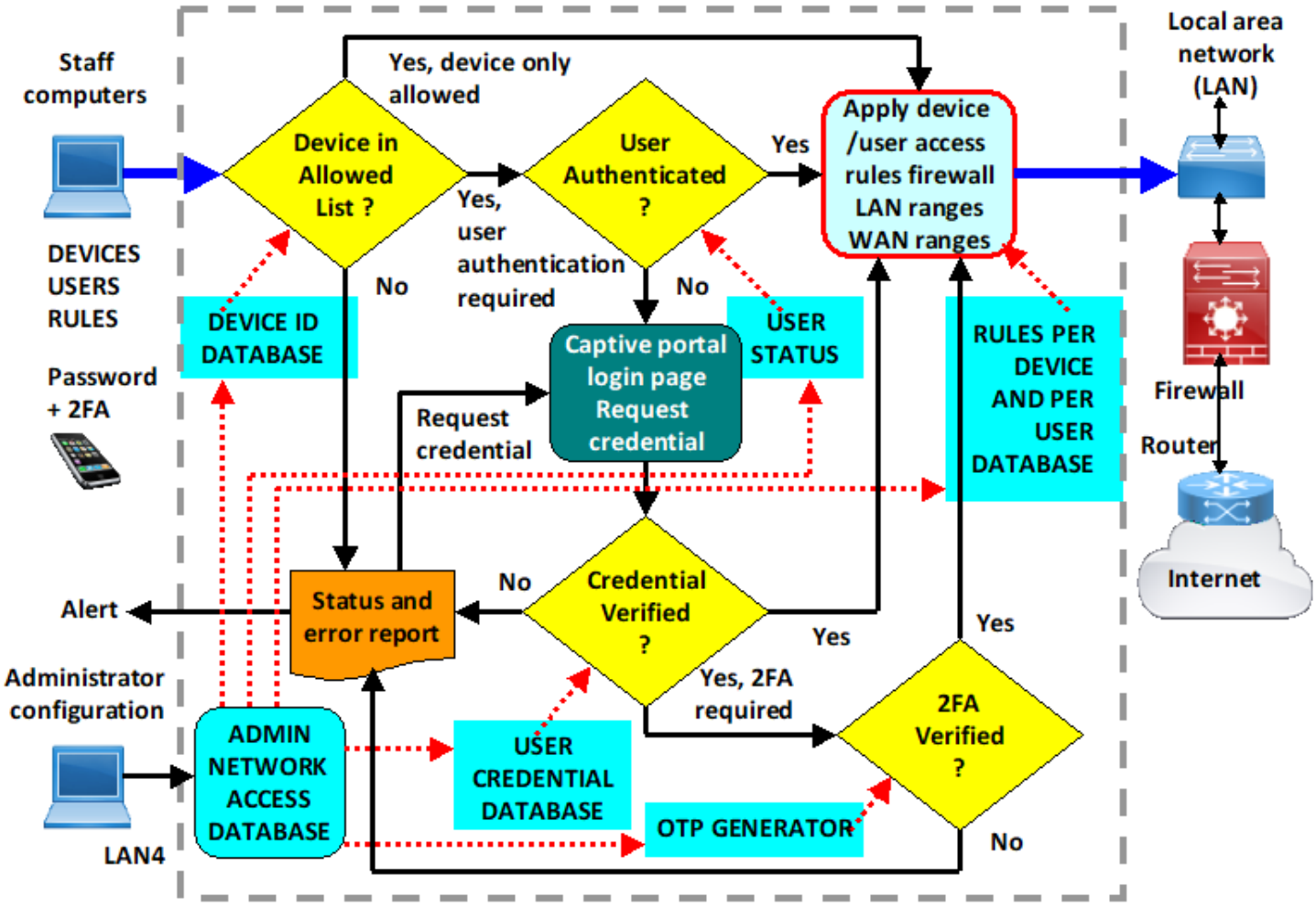
Configuration for Devices, Users and Rules

Authentication and Rule Application

The Authonet Zero Trust Network Access (ZTNA) gateway prevents any device or user accessing the business computer network until that user or device has been authenticated; this is the Zero Trust part of the functionality. The Network Access part of the functionality is controlled by rules applied to each device and each user, that determine what can be accessed in the local area network and what access is blocked. In addition the rules determine what the device or user can access on the Internet. The Network Access rules lock down the network and can be configured to prevent the installation of a Trojan virus via phishing, while permitting staff to proceed with the workflows necessary to complete business transactions.

The next diagram provides a high level view of the Zero Trust Network Access process. The administrator will initially configure the gateway with the device and user authentication information, and will specify the rules that will be applied to each device and user. The configuration is stored in the network access database (NAB) and access to the NAB is made during five stages of the authentication and rule application process.

Authonet ZTNA gateway: device and user authentication and the rule application process



A device may be connected to the network but the device credential may not have been registered during the configuration process. If not registered the network access will be blocked for the device and the device will be logged.

A recognized device may not have a user; the device might be an IoT controller in a manufacturing production environment or a building automation system. The IoT device may connect to the network to provide information for a cloud service or to an external service provider. In this case the device configuration will have an allow access rule and the admin can apply the network access rules. If the IoT device is communicating with an external service provider then all access to the local area network should be blocked by the network access rules. The Internet access will be limited to the external service provider public IP address or domain name. With the IoT device locked down it will be impossible for a cyber criminal to use the device as a portal for access to the network.

With devices configured for login the user will be requested to authenticate via a captive portal screen. If the device is blocked the user will not have access. The user will provide a password and the password will be verified. If the password cannot be verified the user is requested to reenter the password, and a failed authentication is logged. When the user password has been authenticated an optional but essential check will be made for a 2-factor authentication one-time-password (OTP) associated with the password. If there is no 2FA required then the authenticated user connection will pass to the rule application for that user. If there is a 2FA request then the OTP generator will provide the OTP code that is compared with the OTP code provided by the user, obtained from a personal mobile phone. If the OTP code is not authenticated then the user will be requested to enter a new password and the failed authentication will be logged. If the 2FA authentication is successful then the user will have the rules of access applied to all communications with the network.

It is clear that the quality of the security depends on three factors.

- The strength of the password.
- The imposition of 2-factor authentication.
- The robustness of the network access rules applied to each device and user.

The administrator should always use the automatic password generator when configuring a user to ensure a strong password. In addition a policy to change passwords frequently will strengthen the password process.

2-factor authentication is essential for network access to prevent fraudulent network access after password theft. Password theft is the second most frequent criminal access method after phishing.

Robust network rules will prevent a phishing attack if configured correctly. Later sections of this manual deal specifically with protection against password theft and a phishing attack.

Authentication Prioritization

There are two types of network authentication.

- As a device.
    - or
- As a user.

A computer can be logged in as a user or device, not both. A computer may at first be logged in as a device with device rules applied, but when a user logs in, only user rules and policies apply. The original device rules are removed until logout.

A device without a user is an IoT (Internet of Things) or similar device, and can be granted one of two permissions.

- Allow access.
    - or
- Block access.

If the device is granted network access the rules can be applied to the device.

- Determine what can be accessed in the local network.
- Determine what can be accessed in the Internet.

If a device has a user (laptops, desktops, tablets, etc.) then it will be configured for login, however it is the user that logs in to the network, not the device. The device should therefore be configured for:

- Login.

There will be a corresponding user configuration, where the user can be allowed (allow box checked) or blocked (allow box unchecked).

With block the user has no access to the network and will not see a login screen.

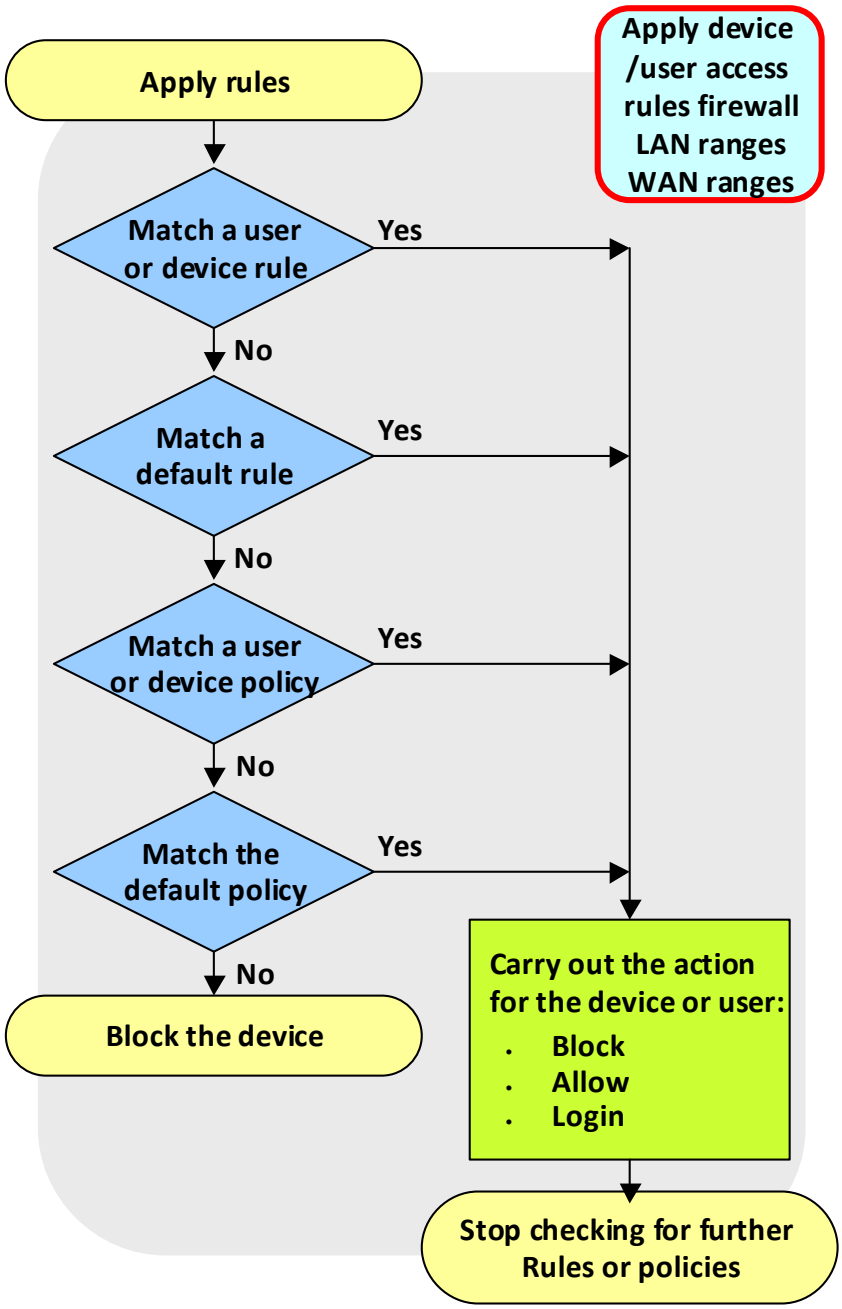
With allow the user will have access to the network, and there may be access rules imposed on the user.

With login the user sees the login screen upon opening a browser window. There are further options for login.

- Set a password: this is a requirement for login. A password only is not secure and not recommended on its own.
- Activate 2-factor authentication by setting a one time password key (OTP-KEY): this is optional but strongly recommended for a security configuration that complies with recognized standards, that include PCI DSS, the HIPAA security rule, and the NIST cybersecurity framework.

The Rules Decision Process

The device and user rules are applied in a sequence of four steps. If a device has a user then the rules set for the user have priority over the device rules. First individual rules are evaluated followed by the default rule. The next rule evaluated in a list has priority over the previous rule. Therefore if two conflicting rules are configured for a user or device, the rule applied is the second in the list. Next individual policies are evaluated for devices of users followed by the default policy. The flowchart below illustrates this process.



Overview of the Cybersecurity Management Configuration

Until the Authonet ZTNA gateway has been configured, devices connected to the Authonet user LAN ports will not have access to the LAN network or Internet. If a browser tab is opened on a user computer then the login page will be displayed, however users have no login credentials until they have been configured.

The Authonet ZTNA cybersecurity defense is configured in three steps.

- Add devices.
- Add users.
- Set rules for devices and users.

Devices and users have three network access configurations.

- Full access.
- Blocked access.
- Login access.

Additional rules specify exemptions to the three basic rules listed above. For example.

- The user has network access blocked with one exception, access is allowed to server 192.168.20.100.
- The device is allowed access with open Internet however access to devices in the local area network is blocked.

There are two approaches to achieve the same desired filtering objective.

- Allow access but specify what is blocked; IP ranges in the LAN and IP or domains in the Internet.
- Block access but specify what is allowed. IP ranges in the LAN and IP or domains in the Internet.

The method chosen depends on the rules that are imposed on devices and users, and is the simplest rule formulation method to impose the rules. Each device and user can be configured independently, some devices or users can be blocked with specified access; some devices or users can be allowed with specified blocking. For most business environments, all user devices will have identical configurations.

When access is allowed then two types of login can be specified additionally.

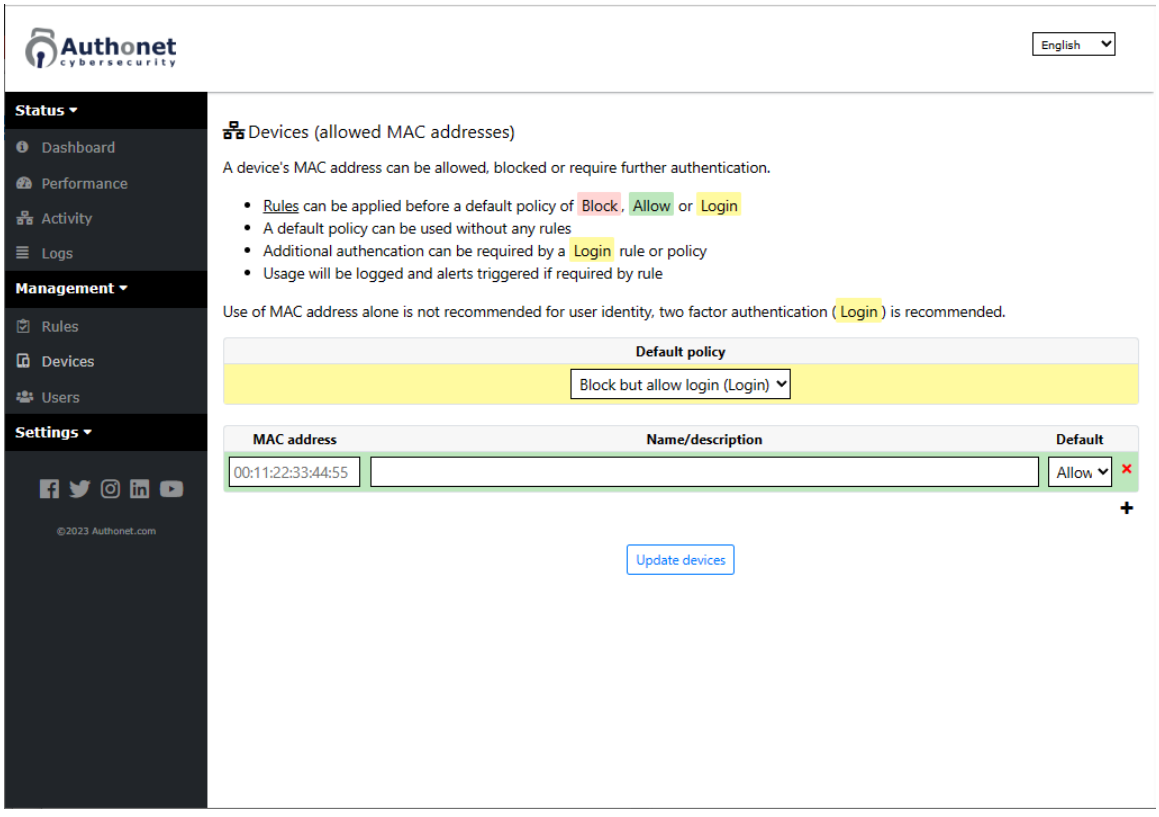
- Password is required to authenticate, admin specified or auto-generated.
- 2-factor authentication, password plus OTP is required to authenticate, where the OTP code is obtained from a phone that the user has.

The administrator computer is connected to LAN4 and has no access to the local network or to the Internet until the administrator adds appropriate authorizations and rules for the device and administrator.

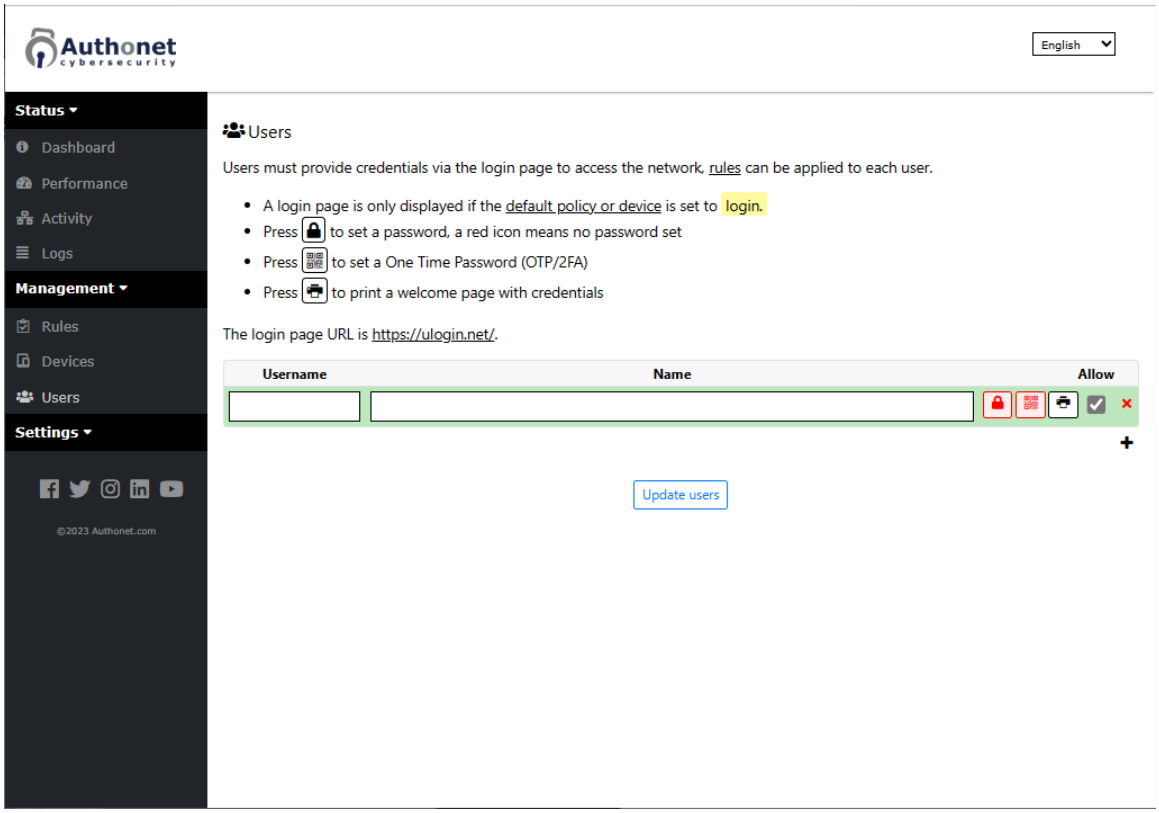
The management menu has three entries.

- Devices: add all devices to the device page that are connected to the user network and set the default rule, allow, block, and login. There is no limit to the number of devices.
- Users: users are added to the user page, with the username for login specified, and the credentials generated for the password and for 2FA. There is no limit to the number of users.
- Rules: formulated to define specific access or blocking requirements in the local area network and the Internet.

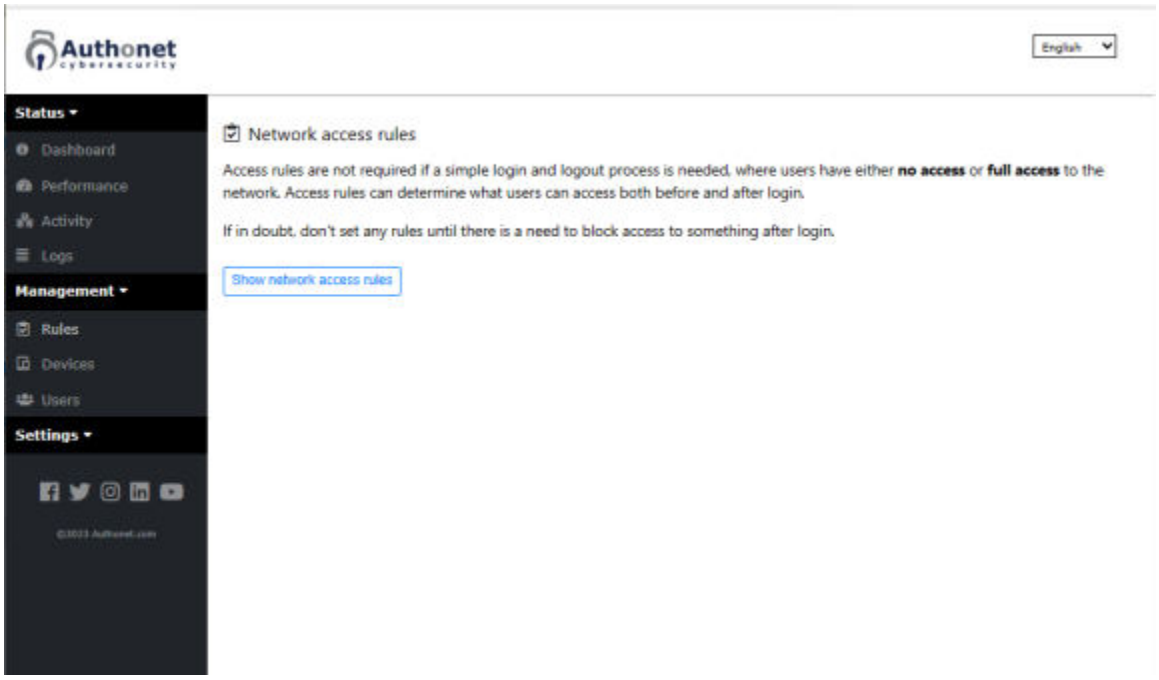
The device menu page is shown in the next figure.



The user menu page is shown in the next figure.



The rules menu page is shown in the next figure.

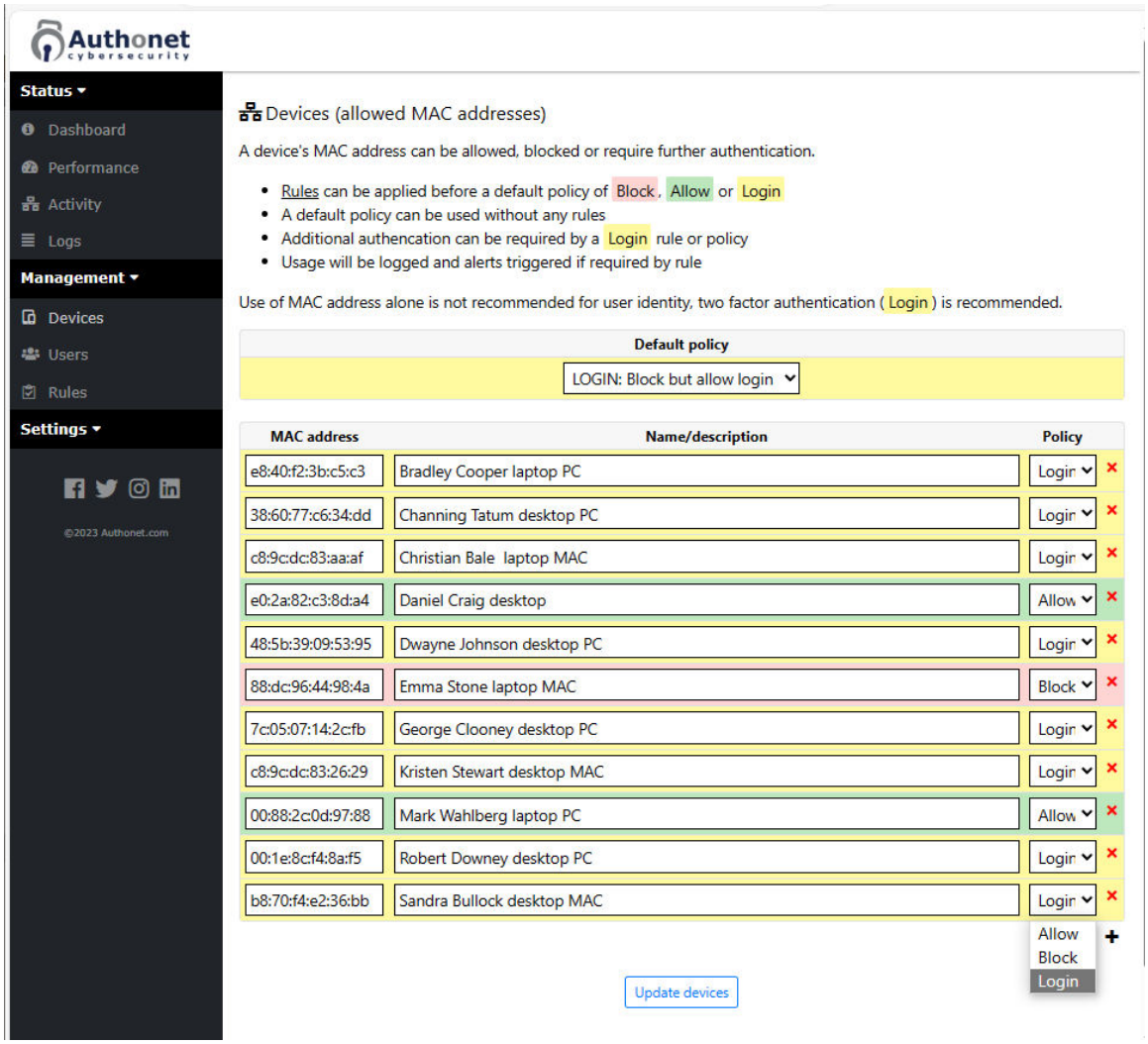


Add Devices to the Device List

All devices that are connected to the user network must be added to the device list. Any device not added to this list is blocked by default. Devices are added to the list by entering the MAC address and a description is added to identify the device. The device has one of three rules selected.

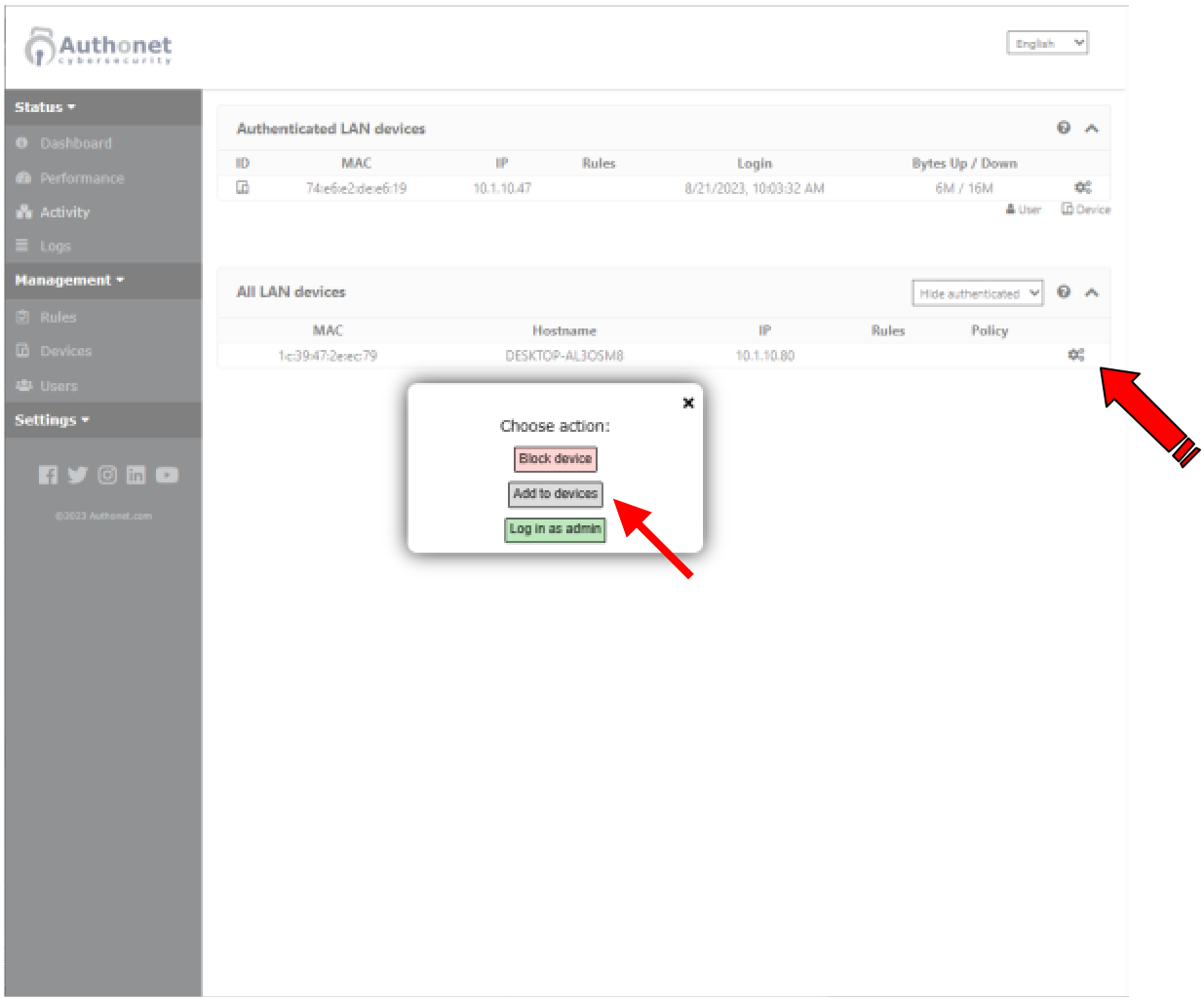
- Block.
- Allow.
- Login.

The device page with several devices already added is shown in the next figure with a policy set for each device. Policies are color coded for easy recognition.



To simplify adding the MAC addresses to the device table, install the Authonet ZTNA gateway in the network with all devices connected. Then open the activity page and add each device to the device table as shown in the next figure.

As each device is added to the device table add a name or description so that the device is easily recognized and then click the update device button to save each device configuration.



When rules are activated (later section) the device page is modified to allow the inclusion of one or more rules for each device. Rule names are added to the corresponding rule box; a comma separates each rule.

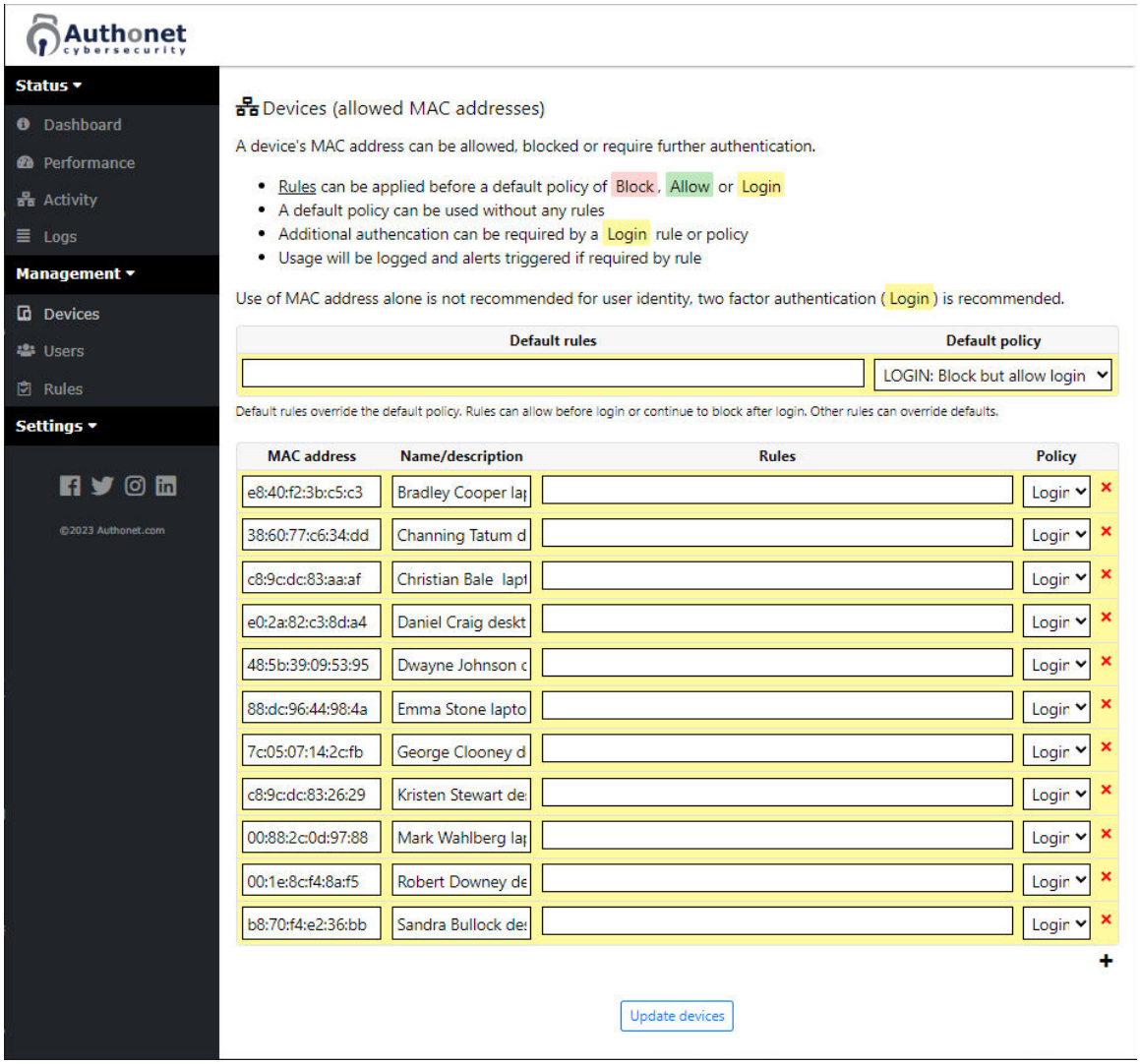
When rules are created using the rules page, one or more rules can be applied to each device in the list by adding the rules to the default rules box, with the corresponding rules policy of, allow, block or login.

There is also a master default rule setting with a corresponding default policy. This is used when one rule configuration has to be applied to all devices.

When a user is associated with a device then the rules set for that user override the rules set for the device.

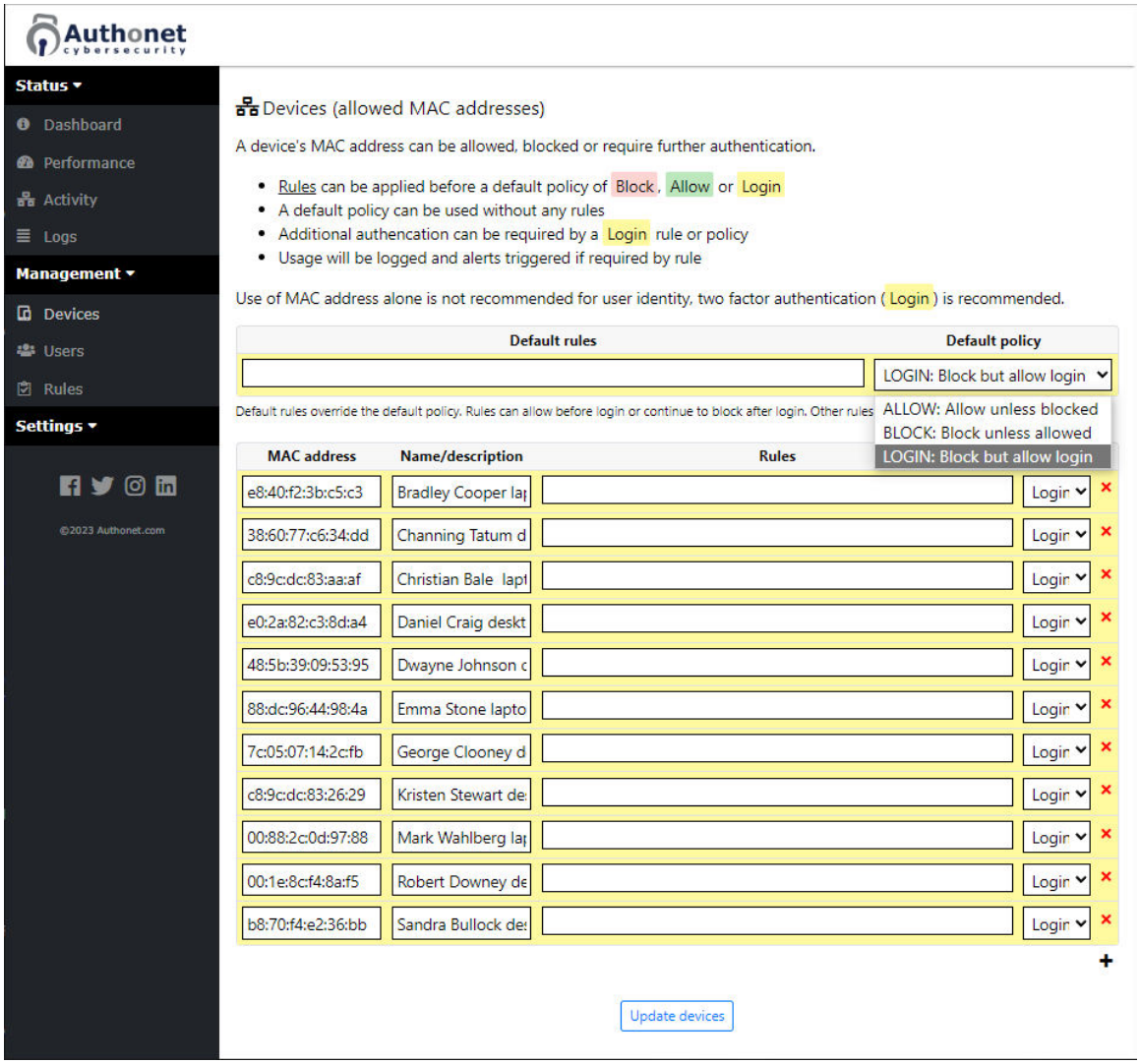
When rules are conflicting, the rule that determines the action is the one later in the list and nulls a previous rule. This is the rule to the right of the rule list.

The next screen shows the devices page with the rule boxes displayed after activation of the rules.



A default policy can apply to all devices in the list. Devices without a user, such as IoT devices will have the device rules and policies applied. Devices with users (computers, mobile devices) will have the user rules and policies take preference over device rules and policies.

Default policy selection is shown in the next figure.



Add Users to the User List

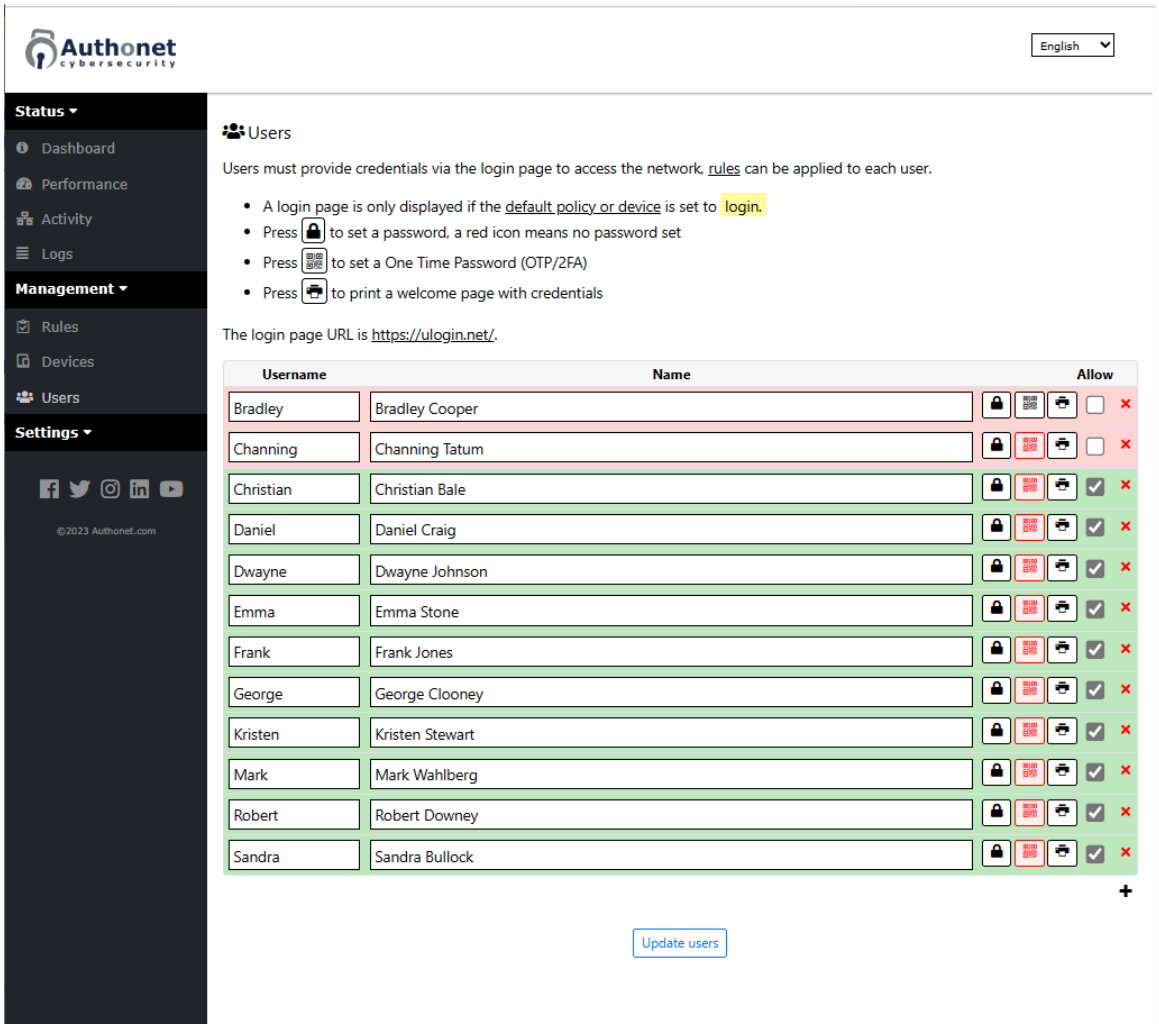
The administrator adds the names of user to the user list. The administrator creates a username, this might be the users first name, or the initial of the users first name followed by the surname.

Users require credentials to access the network, a password plus a one time password (OTP) code is preferred. Credentials are assigned with the user list table.

The allow box can be unchecked to disable the user.

The user list table is shown in the next figure. The rules have not yet been enabled and so the rules boxes are not shown.

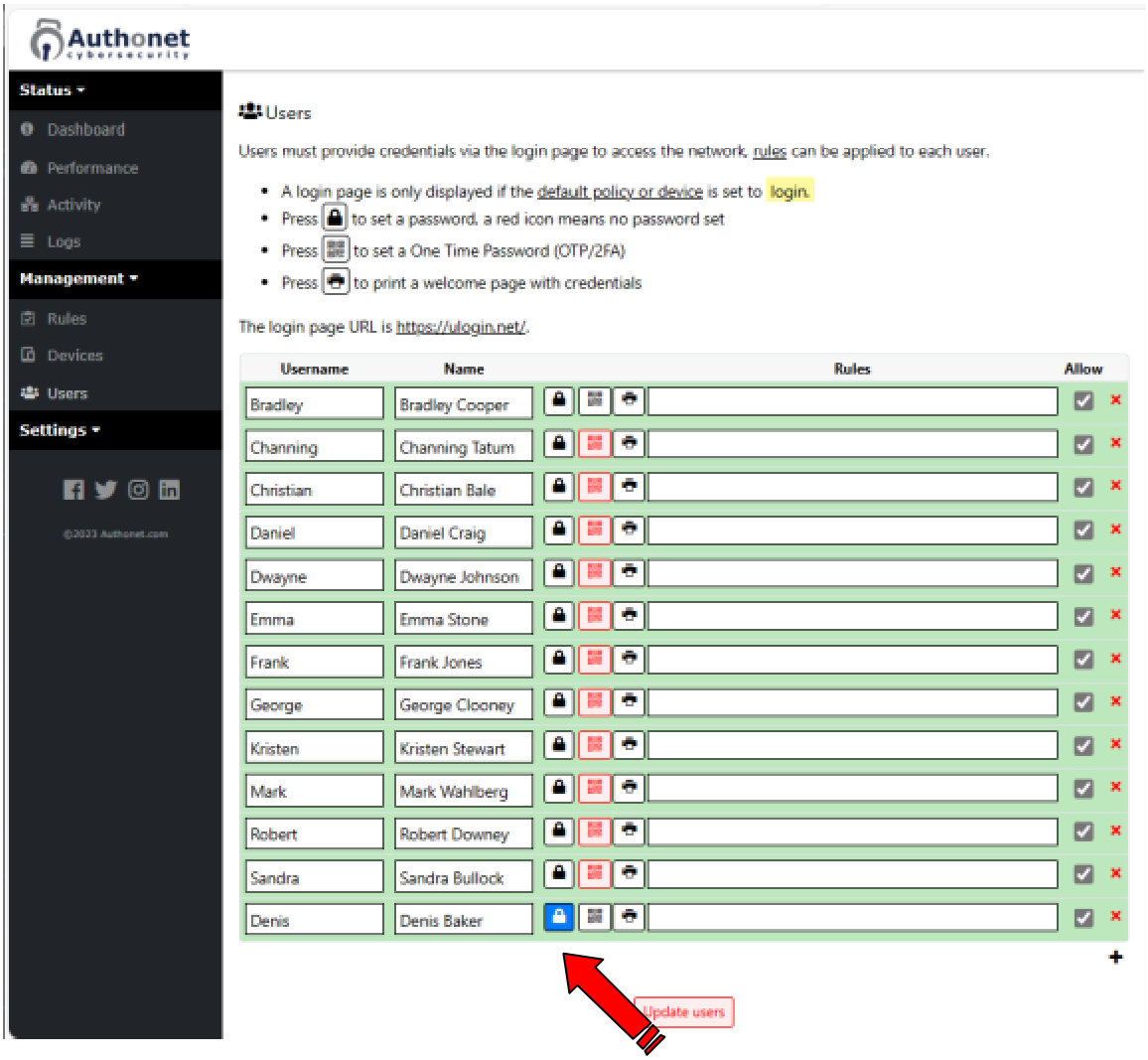
Click the update users button at the bottom of the page after users have been added.



When the rules have been enabled (next section) the rules box is displayed to the right of each user entry. The rule names can be added to this box; where a comma separates each rule. There is no limit to the number of rules that can be added for each entry. When conflicting rules are entered the later rule to the right takes precedence over previous rules to the left.

The next figure shows the user page with the rules enabled.

The button that is highlighted is clicked to set the password for the user. A password has to be set for each user.



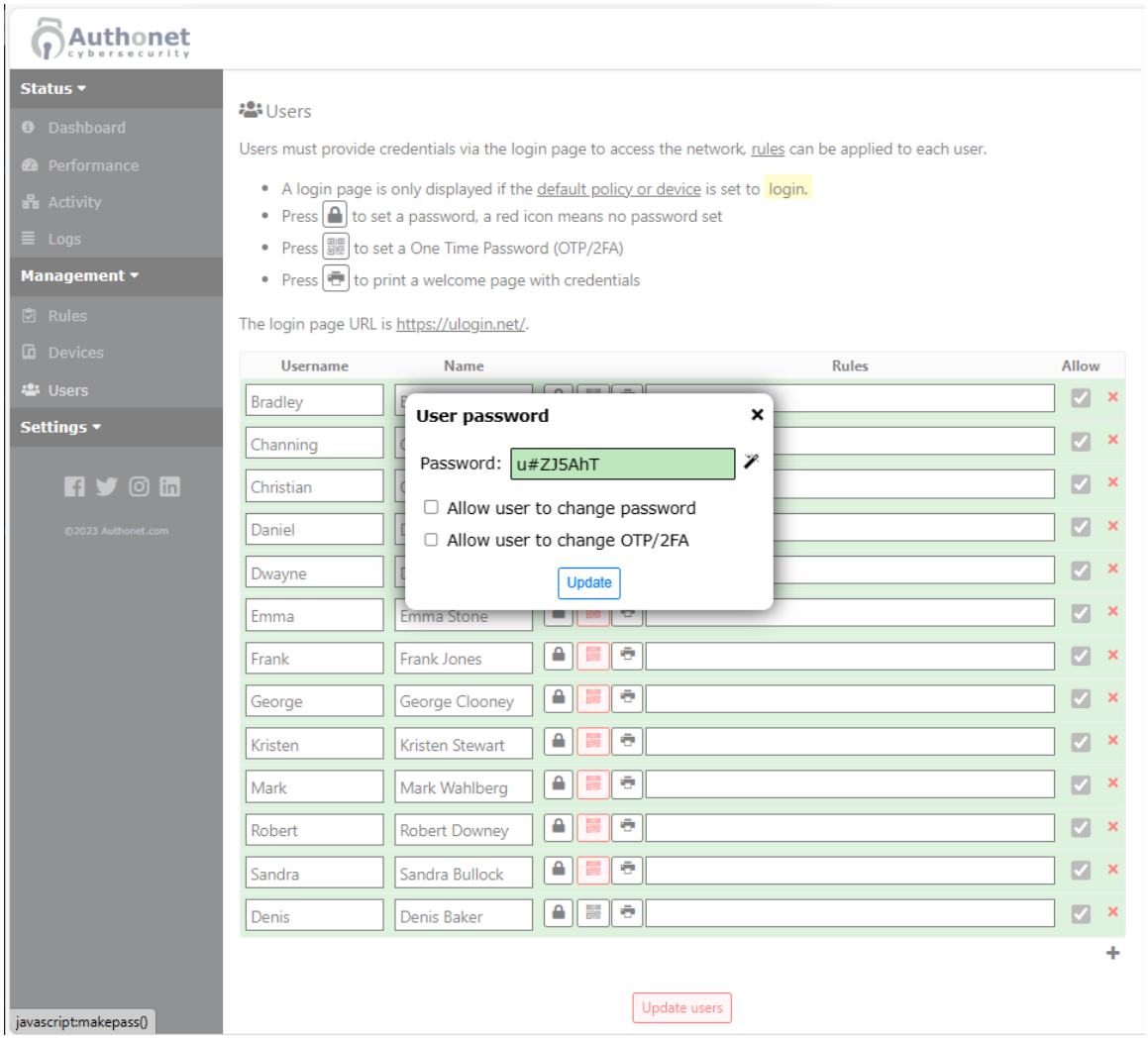
The next step is to assign a password for the user.

Click the lock symbol for each user. Click the pen symbol to the right of the password box to auto-generate a strong password.

Click the button to update the password.

The password can be given to the user.

It is advisable to change the password frequently for added security.

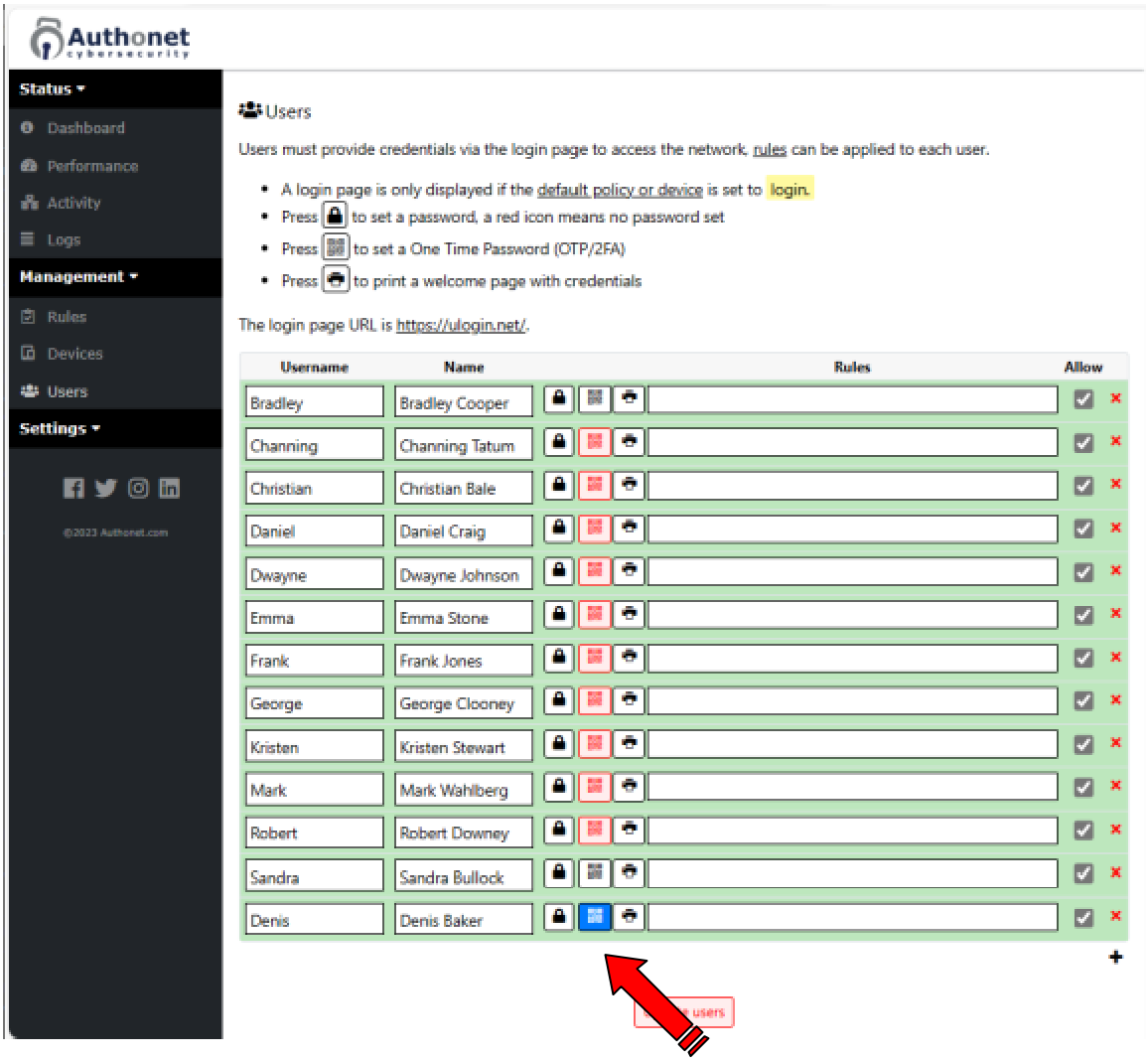


The next step is to generate the QR code for the optional one time password (OTP) for 2-factor authentication.

The user has to install an OTP app on a personal mobile phone. There are many apps available, some free and some providers charge for the app, either a one-time charge or a monthly fee.

FreeOTP is a popular app that is free and available from both the iPhone store and the Android store.

Clicking on the QR code button shown in the next figure generates the 2-factor authentication key.

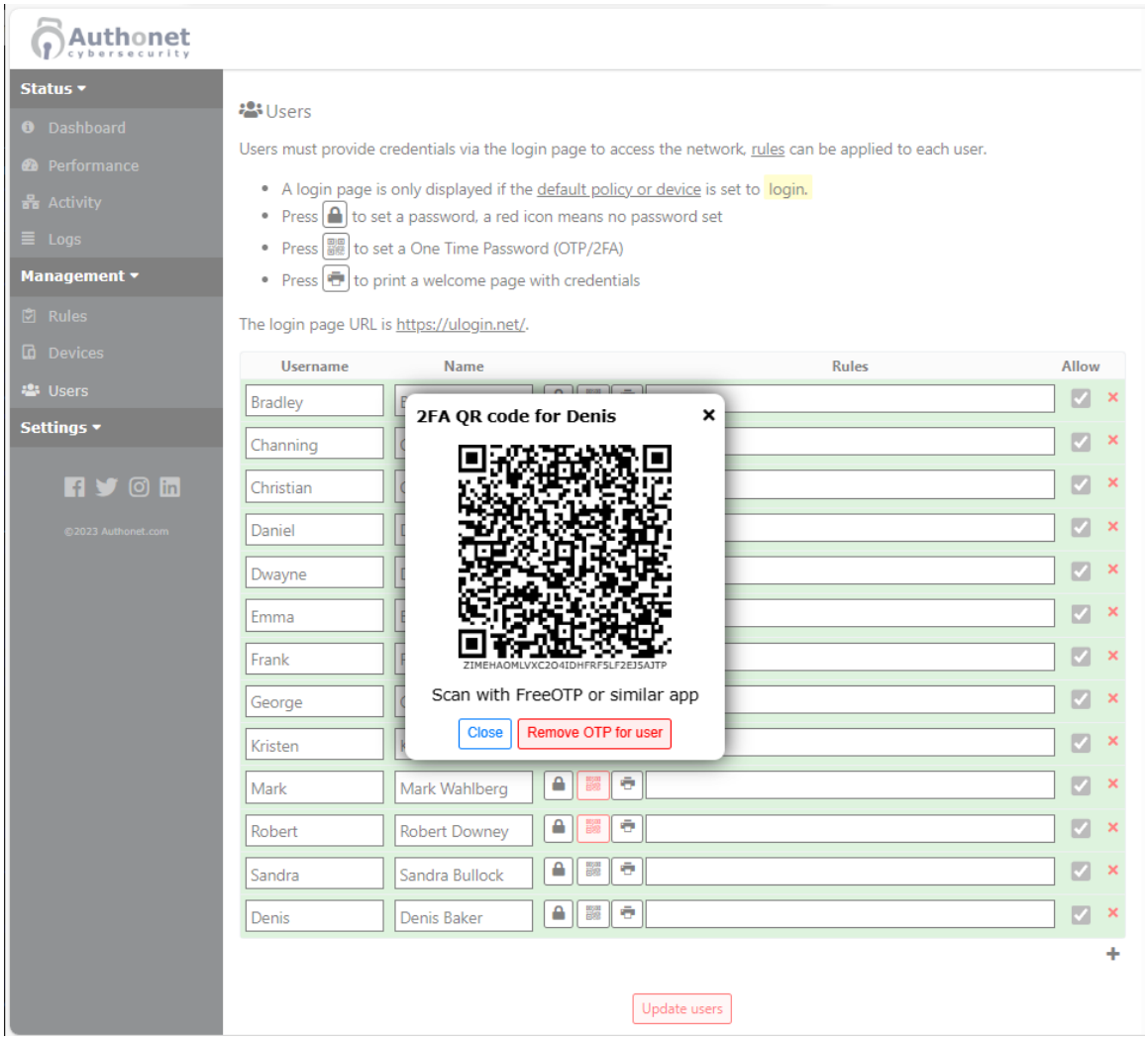


The administrator clicks the QR code symbol for each user and a window will open with a QR code. The app such as FreeOTP is used to read the QR code to initialize the app. Each time that the user logs in the FreeOTP app is opened by the user to get the OTP code requested after entering the password.

2-factor authentication is a very secure method of protecting a business network against a cyber attack and is recommended for all installations. Password theft through social engineering is a common tactic that a cyber criminal will use to gain access to a business network. 2FA prevents the use of a stolen password.

The QR code generated for a user is shown in the next figure.

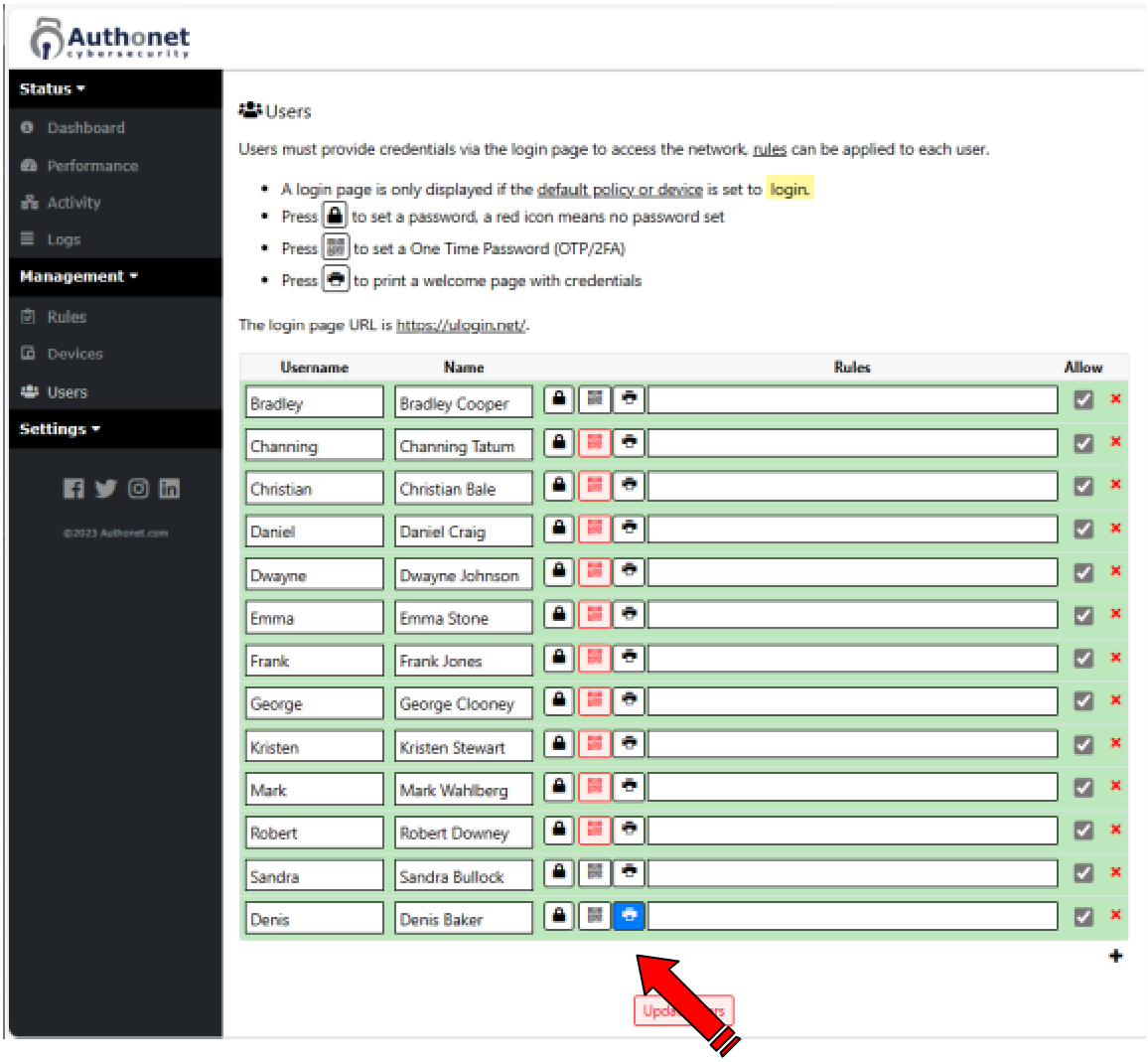
2-factor authentication is removed for a user with the same procedure. Open the QR code box then click the red button, remove OTP for user.



Some of the OTP apps available for mobile phones are listed in the next table.

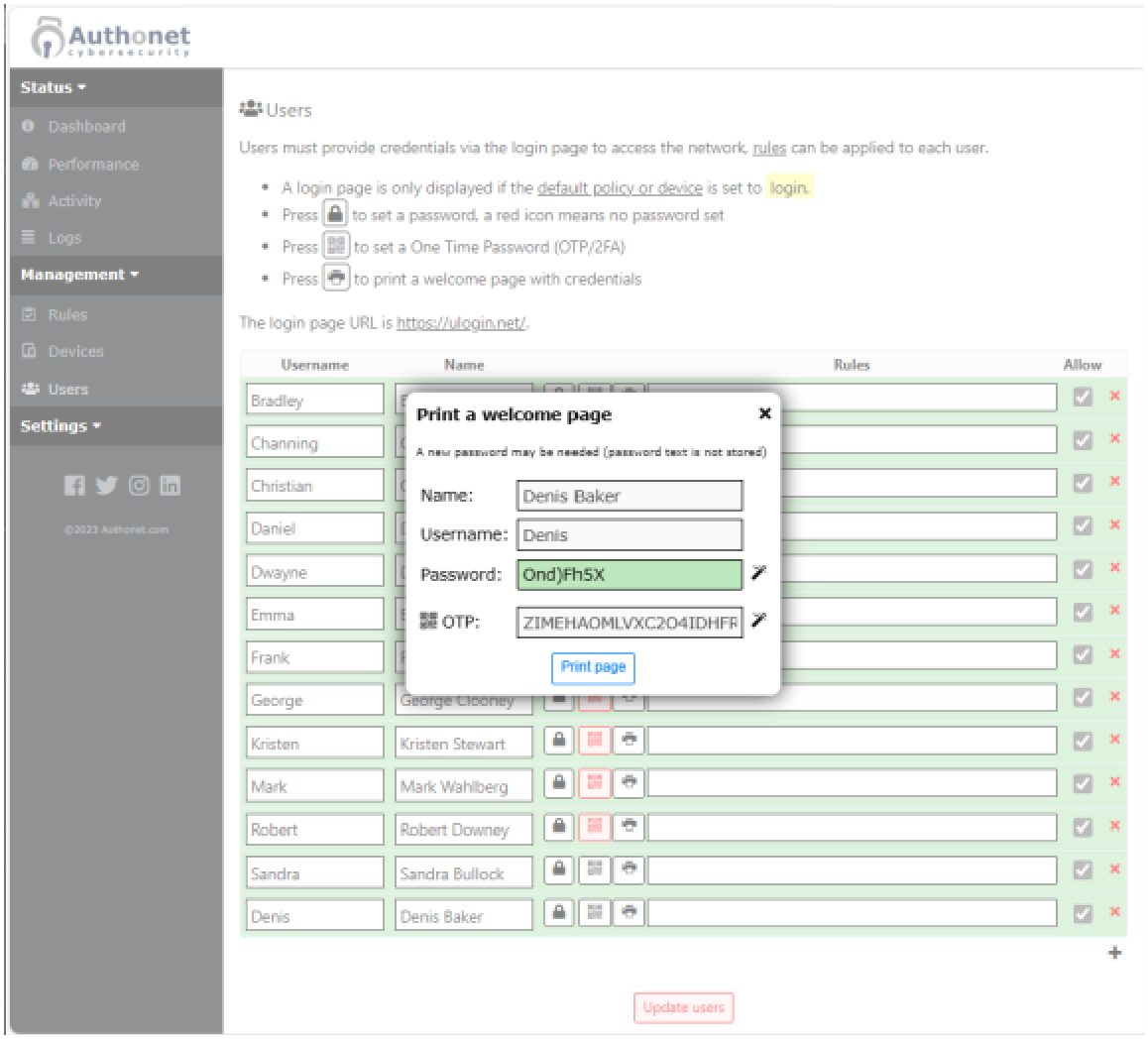
Google Authenticator	Authy
Microsoft Authenticator	LastPass
LastPass Authenticator	FreeOTP
andOTP - OTP Authenticator	TOTP Authenticator – 2FA Cloud
2FA Authenticator (2FAS)	Bitwarden Password Manager
Aegis Authenticator	Aegis

The administrator can print a welcome page for each user, with the password and the QR code for 2FA authentication. The welcome page simplifies the process of adding users to the network. The administrator clicks the printer symbol that is highlighted in the next figure.



When the administrator clicks the printer symbol for each user a box opens showing the password and OTP authentication code to print the welcome page. Using this box the password and OTP authentication code can be changed.

Click the print page button to print the welcome page for each user.



The administrator should plan to meet with all employees for 5 minutes to explain the login process and to hand out the welcome pages.

WARNING

The administrator must request that the welcome pages are returned and the returned pages should be shredded. Do not let the user scan the page and store on the computer under any circumstance.

The 2FA phone app will scan the authentication QR code. Subsequent access to the 2FA phone app will permit the 6-digit OTP code to be read and entered into the login page.

An example of a printed welcome page is shown in the next figure. The user should note the password before returning the sheet to the administrator. The password must not be stored on the users computer.

Authonet cybersecurity

Welcome to the Authonet network

Your credentials to access the network are as follows:

Name: Bradley Cooper

Login page: https://ulogin.net/

Username: Bradley

Password: Da3QY*mW

Two Factor Authentication QR code:

The Two Factor Authentication / One Time Password (2FA/OTP) login adds an extra layer of security to the network, it requires that an extra 6 digit password be provided for each login. The 2FA/OTP password changes at each login. An app needs to be set up on a mobile device such as a phone or tablet to generate the password.

The recommended app to use is **FreeOTP**, this can be downloaded from the Apple App Store or the Google Play/Android store.

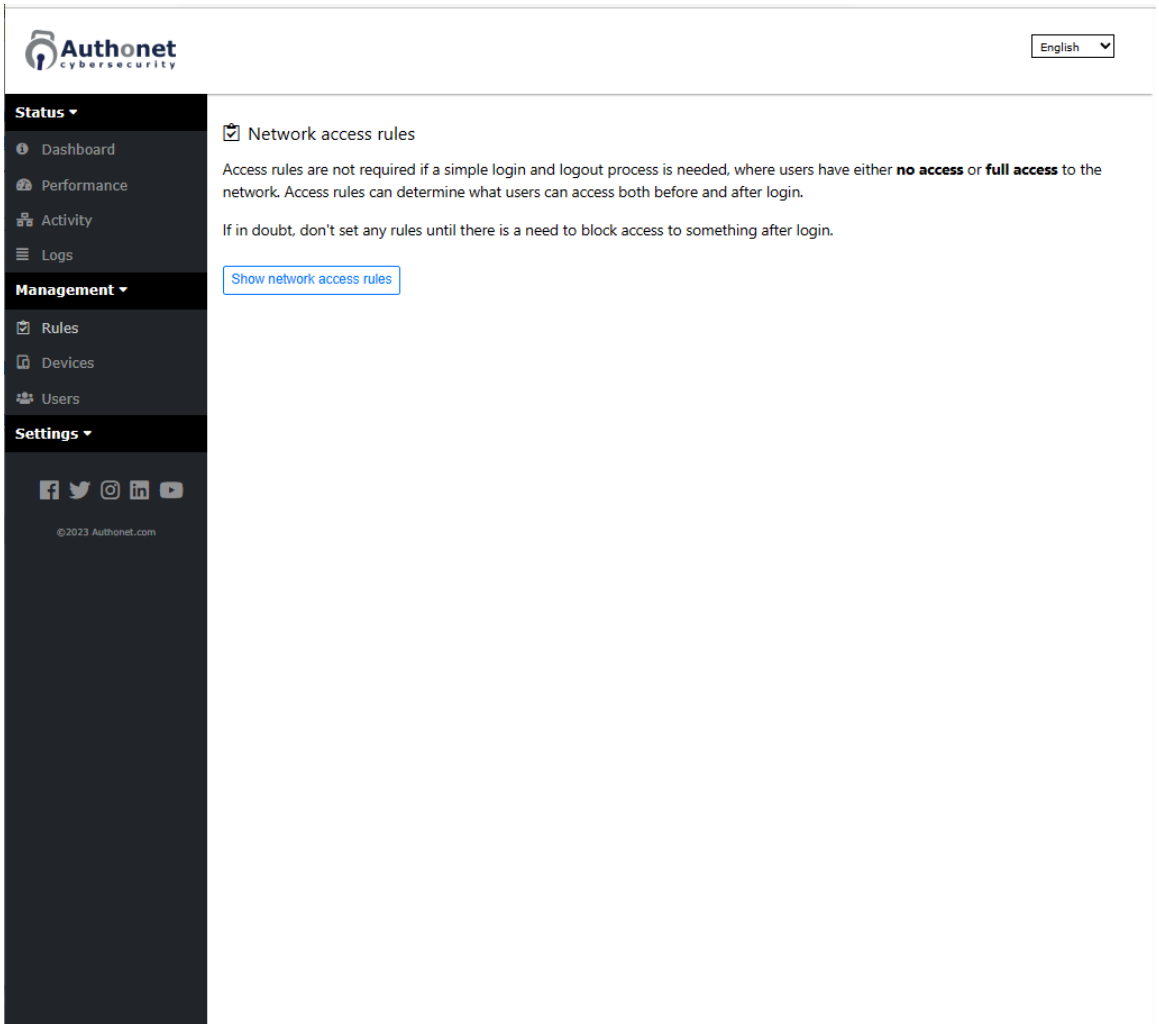
Once the app is installed, click on a **+** sign and/or the QR code icon and scan the QR code above with the camera on the device.

Create Rules using the Rules List

For some applications the simple rules available with the device and user list will be sufficient to protect the business network. For many applications however additional rules must be prepared to provide access control to parts of the local area network and also to the Internet.

When the rules menu entry is first clicked there are no rules. It is necessary to click the button “show network access rules” to begin entering network access rules.

This is shown in the figure below.

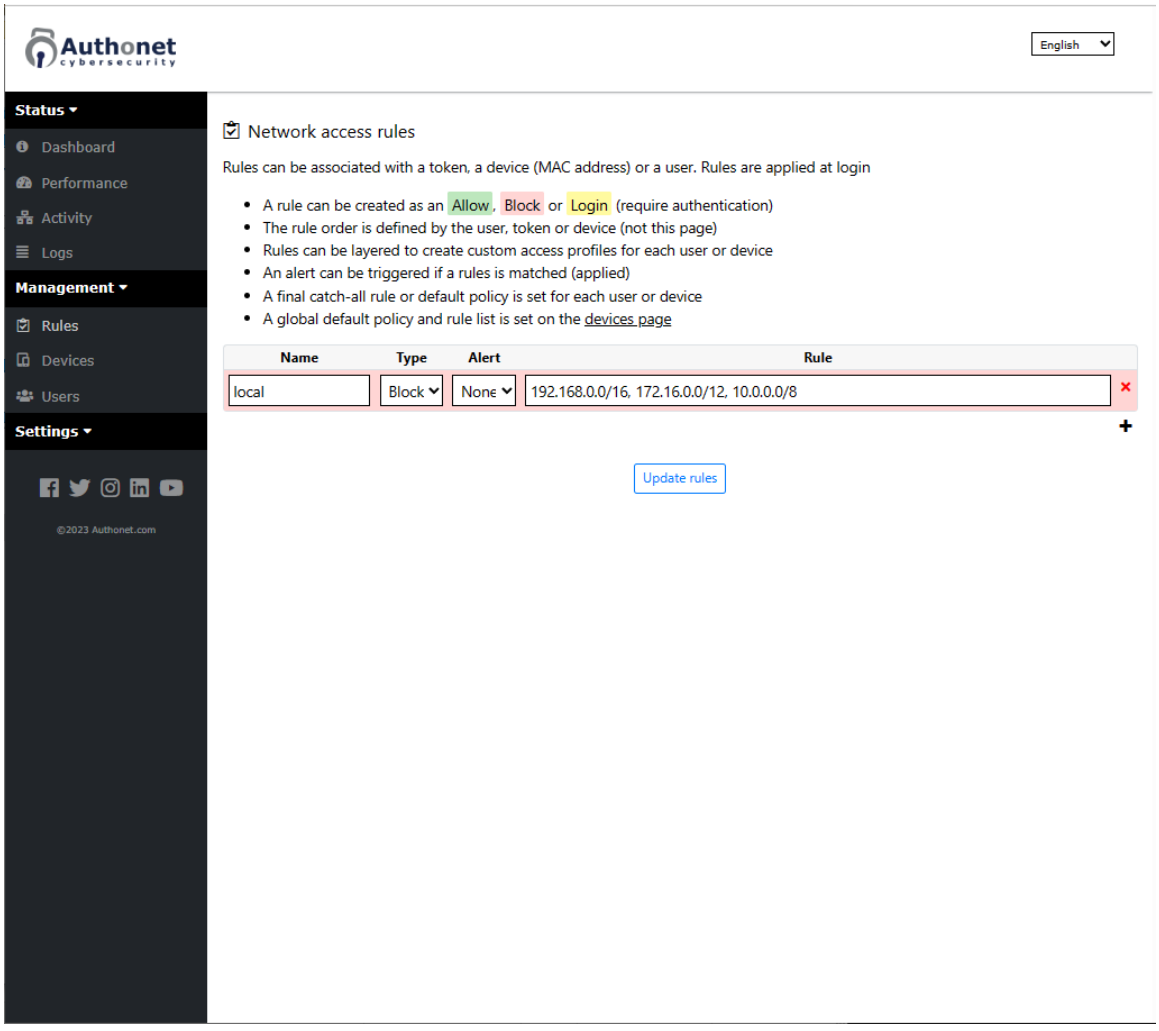


When the “show network rules” button is clicked the page shown below is displayed. The text on the page describes the rules.

Network access rules

Rules can be associated with a device (MAC address) or a user. Rules are applied at login.

- *A rule can be created as an Allow, Block or Login (require authentication)*
- *The rule order is defined by the user or device*
- *Rules can be layered to create custom access profiles for each user or device*
- *An alert can be triggered if a rule is matched*
- *A final catch-all rule or default policy is set for each user or device*
- *A global default policy and rule list is set on the devices page*

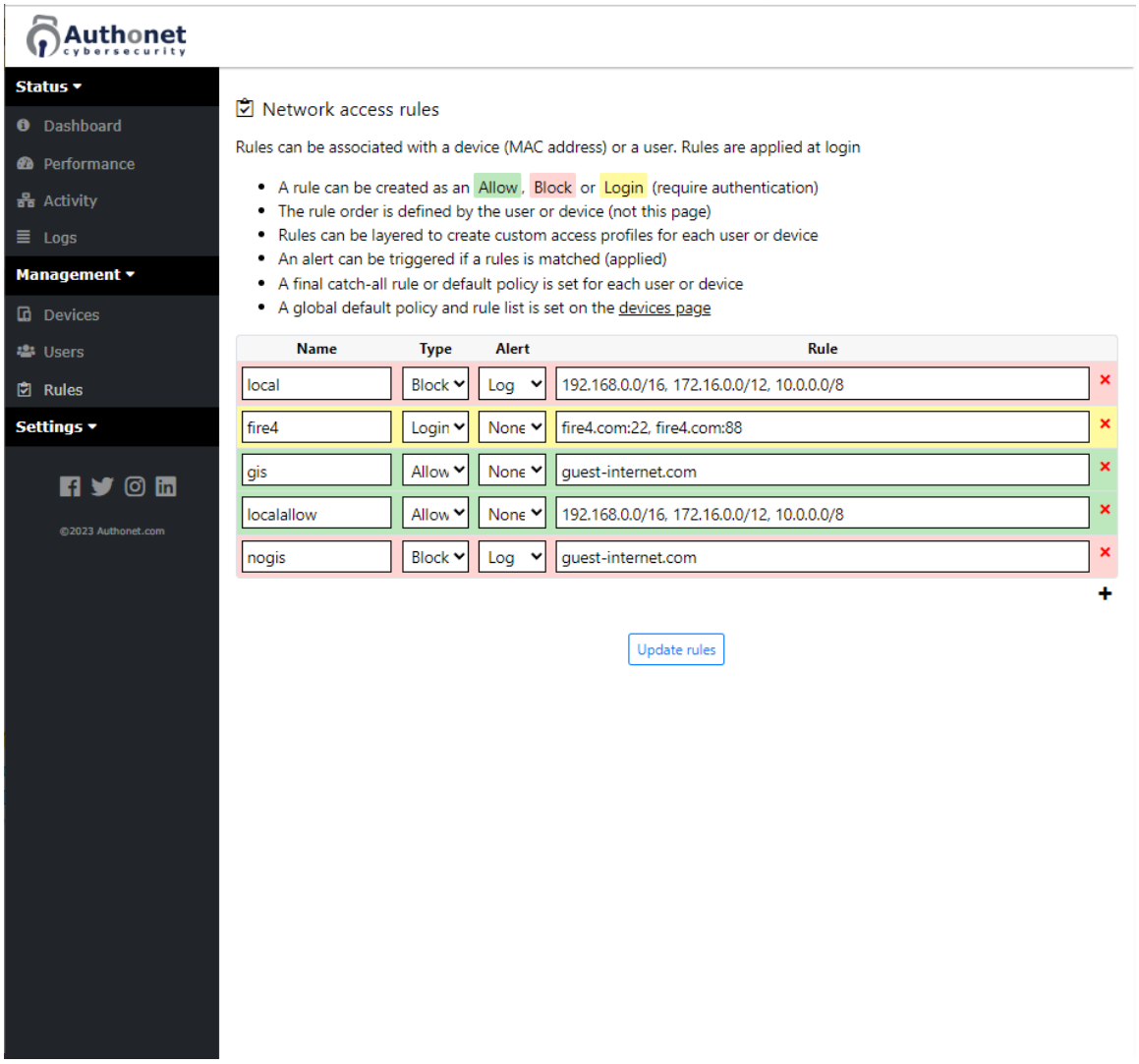


A rule provides an exception to the allow, block or login rules. Examples of rules are:

- Allow access to specific local network IP addresses only or blocks of IP addresses.
- Block access to specific local network IP addresses or blocks of IP addresses.
- Allow access to specific Internet domain names or public IP addresses only.
- Block access to specific Internet domain names or public IP addresses.

The rule is written using both LAN private range and public IP addresses, or using domain names.

The next figure shows five rules added to the rule table. Click the update rules button after each rule is added.

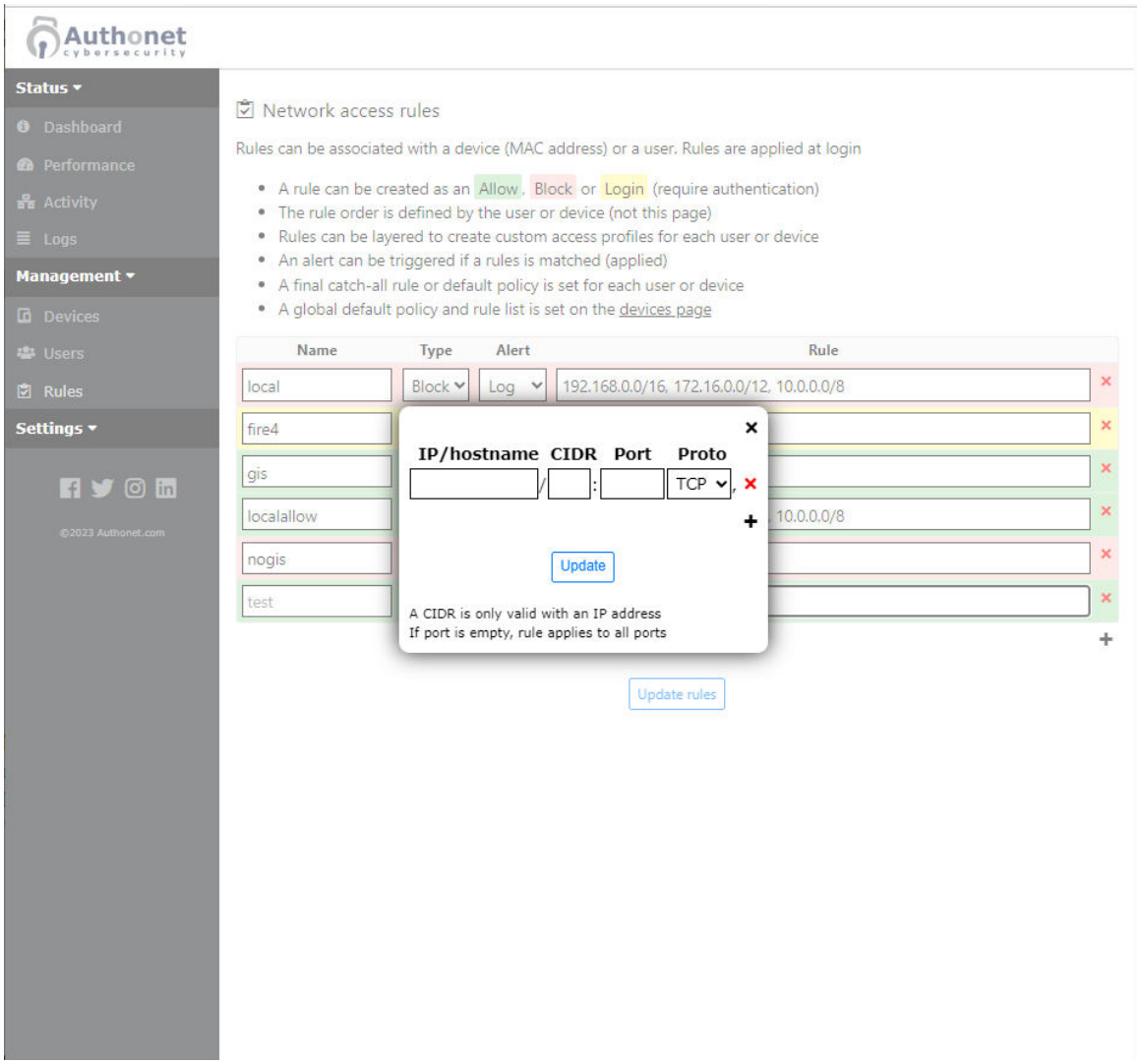


A rule is added by clicking on the rule box, a box will open to enter the rule parameters.

- IP address or domain name.
- CIDR: Classless Inter-Domain Routing specifies the range of IP addresses in a block and is written as /number. For example /28 represents the IP address with a netmask of 255.255.255.240.
- Port number if applicable. This will be port 80 for http access.
- Protocol type, the default is TCP/IP, UDP can also be selected.

Add more rules by clicking the + symbol. There is no limit to the number of rules that can be added. If conflicting rules are added then the later rule to the right of the list is the rule that is applied.

The addition of a rule is shown in the next figure.

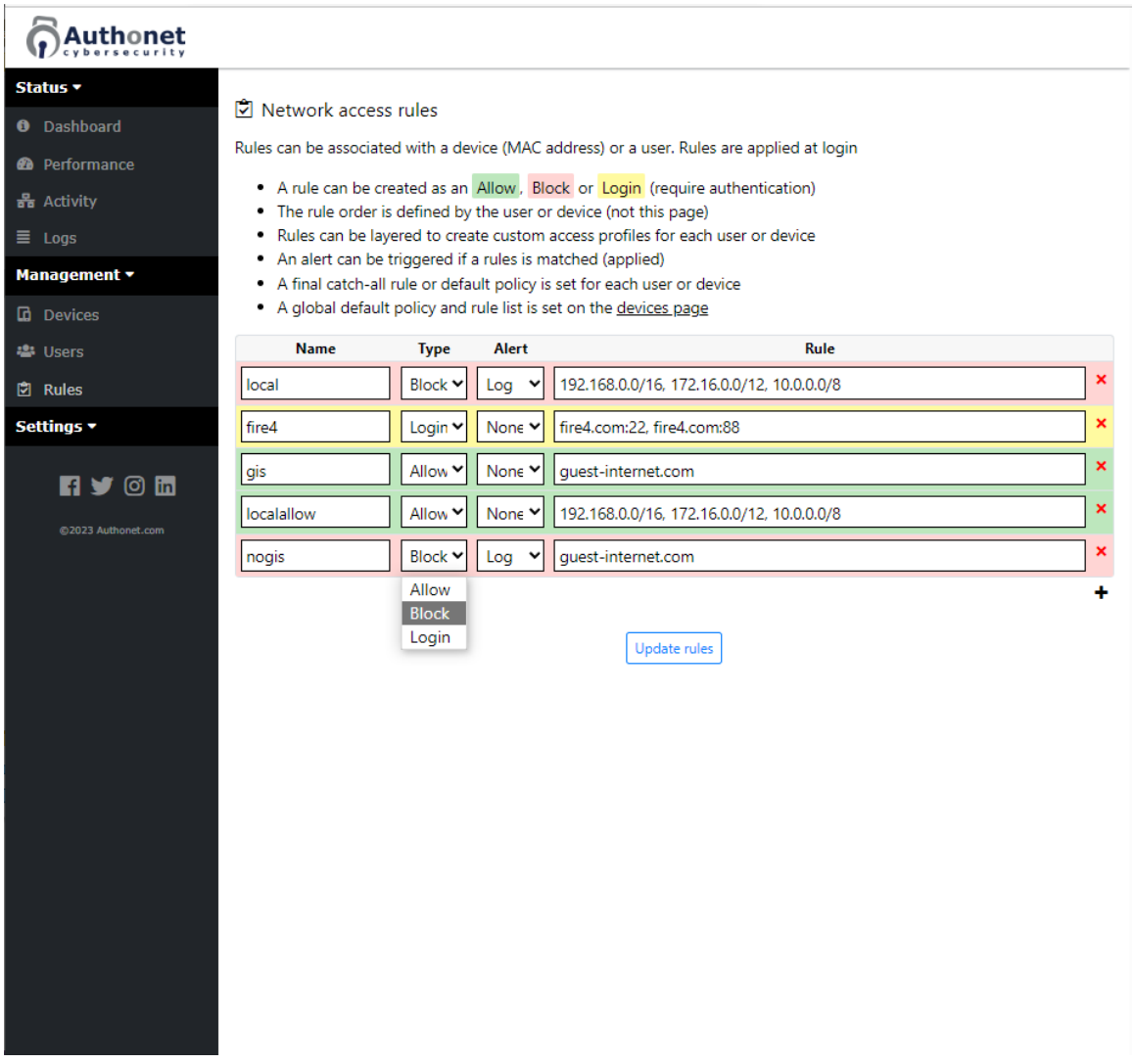


Each rule is given a unique name and the name is added to the device or user list.

Each rule has a type that specifies to allow network access, block network access or require a login, which redirects the user to the login page that requires a password and option OTP.

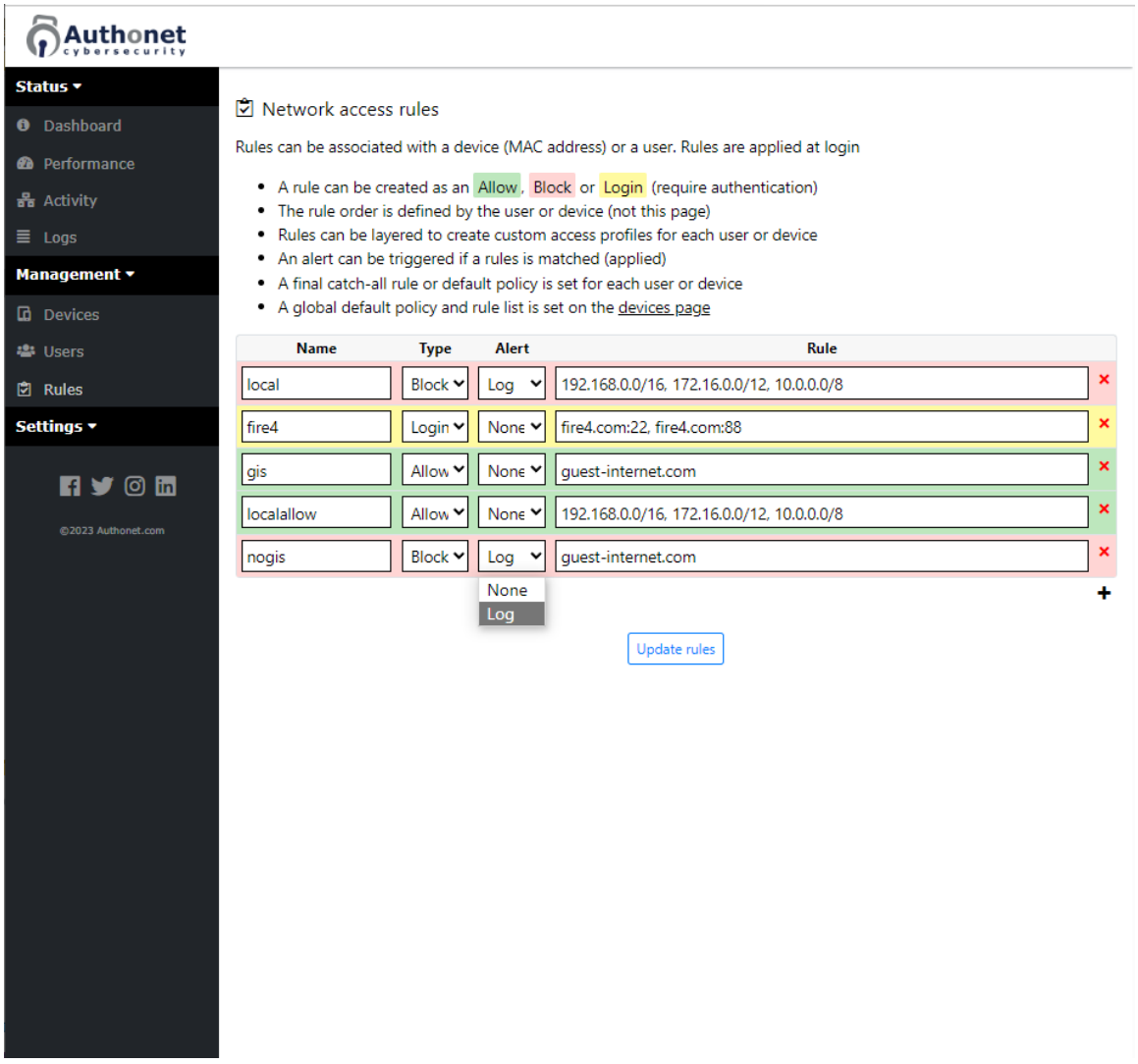
The rule type highlights the line in green, red or yellow based on the access type.

The drop down rule type list is shown in the next figure.



An alert can be selected for the rule; this can be none or log the rule access attempt. With log selected, any attempt to break the rule will be logged and alerted.

The next figure shows the drop down alert menu. Example rules are also shown in the figure.

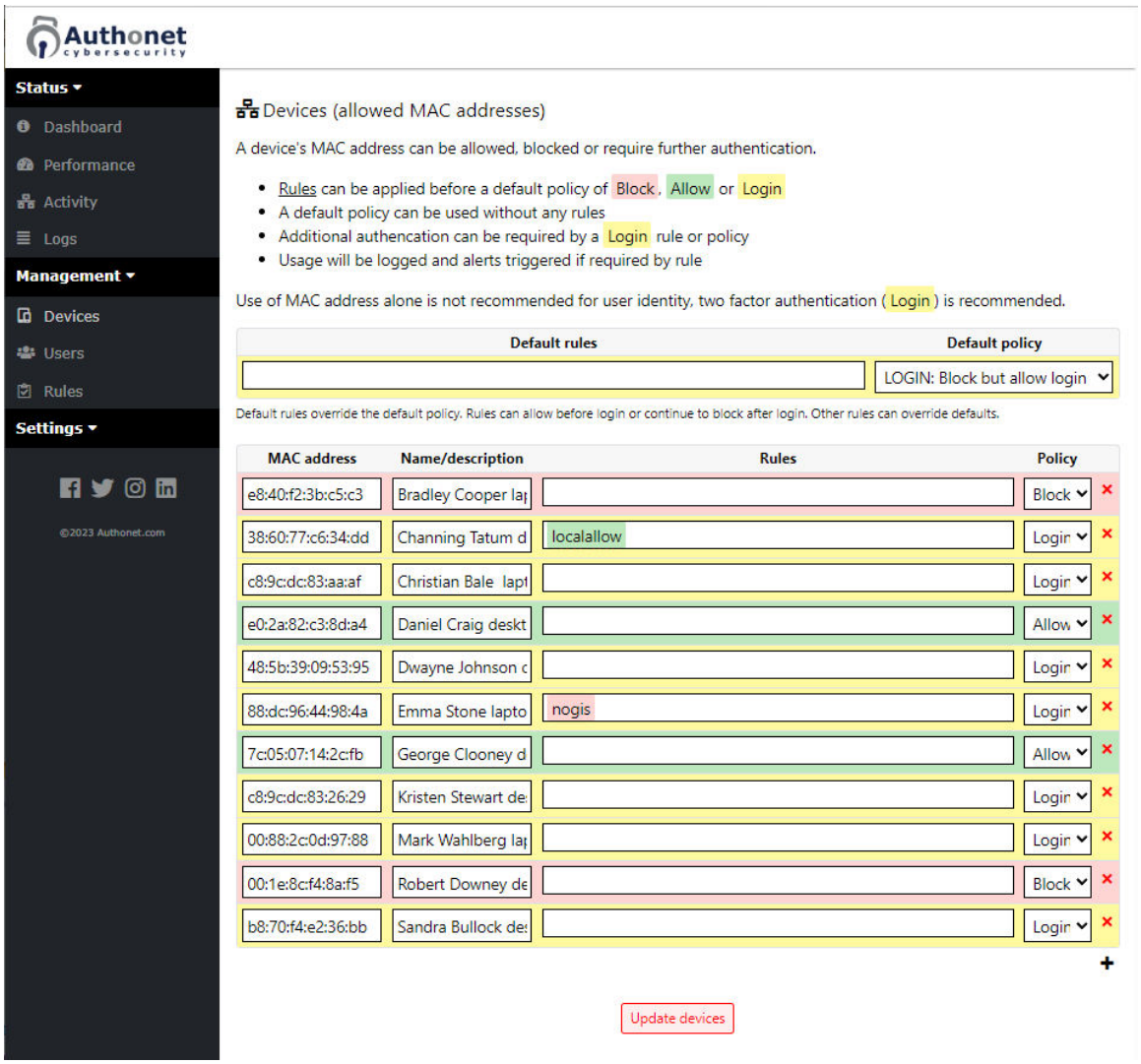


Add Rules to the Device List

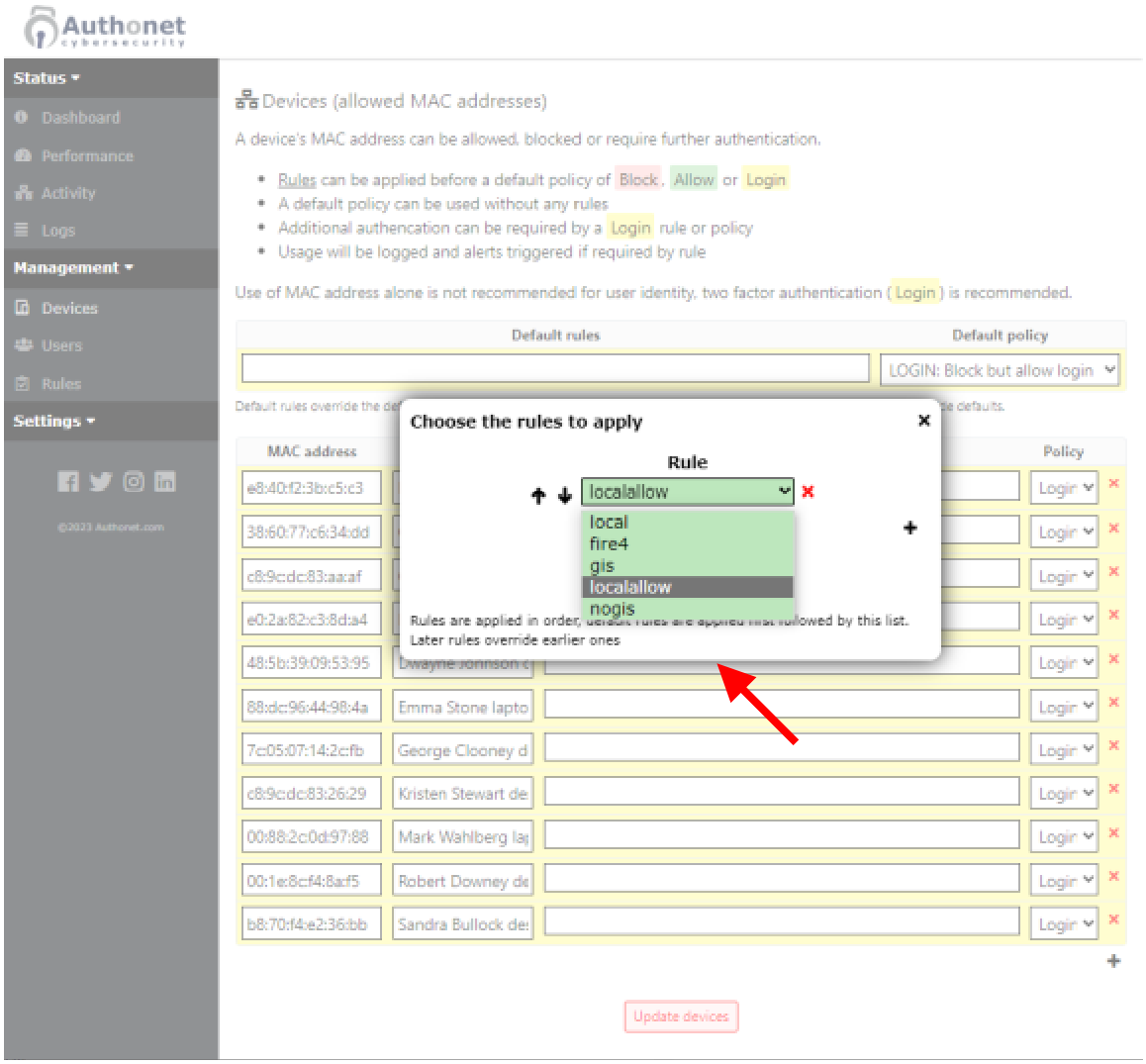
After rules has been enabled and rules have been added to the list, open the device list and prepare the set the rule for each device. First select the policy for each device as shown in the next figure.

- Block.
- Allow.
- Login.

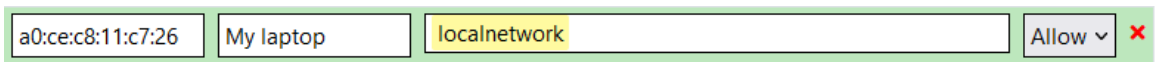
Next click on the rules box for the first device to be configured and the choose rules box will open.



When the choose rules box opens click on the down arrow in the rule box. A drop down list will open with a list of all the rules. Select the required rule from the list. This process can be repeated to add more rules to the device by clicking the + character. Click the set rules button to save the rule when finished. When all devices have been configured click the update devices button at the bottom of the page.



After clicking the set rule button in the box the rule will be added to the device as show in the next figure.

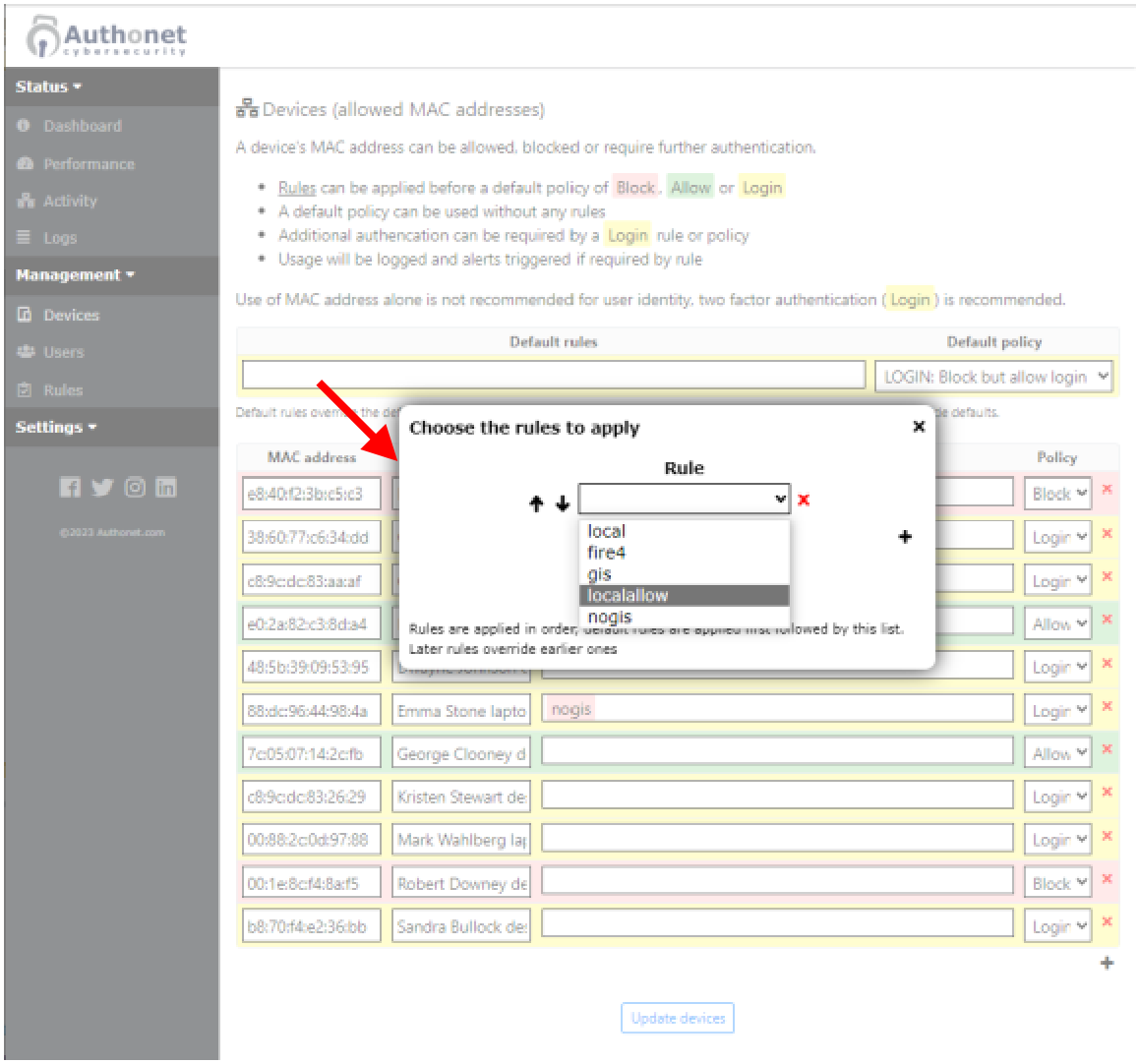


Repeat this procedure for all devices.

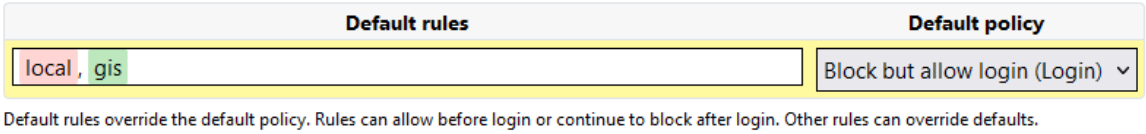
The devices page also has the default policy and default rules list. This is applied to all devices pre login.

When one rule has to be applied to all devices this is added to the default rules box as shown in the next figure. Click the default rules box to open the choose rules box. Click the down arrow in the rule box to see the drop down list of rules. Click a rule in the list to add to the default rules. This process can be repeated for additional rules by clicking the + character. Click the set rules button when finished.

When the default rule has been configured click the update devices button at the bottom of the page.



When the choose rules box is closed the selected rules are shown in the default rules box, as shown in the next figure.



Rule order matters when multiple rules are added. A later rule might override the instruction of a previous rule. For this reason there are up and down arrows in the choose rules box that are used by the admin to change the order of rules.

The default policy in the example shown above is login so the line is yellow (login = yellow). Changing the default policy of allow (unless blocked) or block (unless allow) will change the line to allow=green or blocked=red. If allow or block is selected the login page is not displayed.

The default policy can be changed to block and then each MAC address can be configured for login, which will lock down network access.

An allow rule, eg the green 'gis' rule above is allowed access without the need to log in, all devices get access. In this case the rule allows access to the web site specified by the rule without the need to log in. See the 'gis' line on the previous rules page example.

A red rule, for example the ‘local’ shown above, blocks access even after login.

With a yellow policy of login shown in the example above, the device will have access only to a green rule.

The red rule blocks access permanently unless the user has a green rule that is applied at login, which overrides this red rule. The result is that by default no user has access to the resource blocked by the red rule unless they are specifically given access to the resource by a rule.

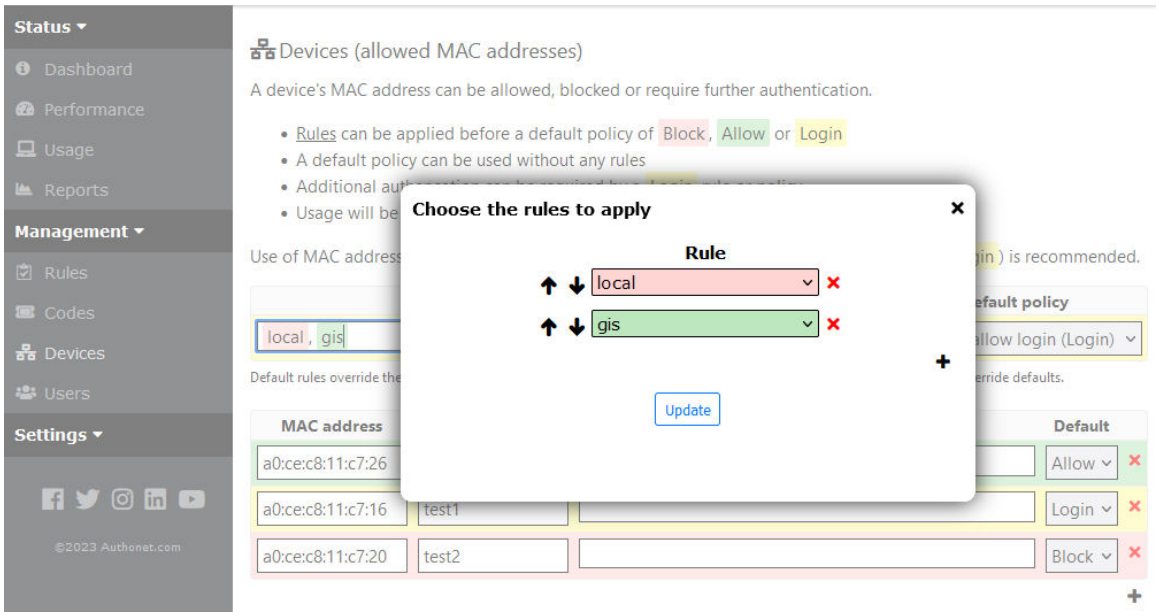
The order of the rules is important. If a resource is blocked by a rule but the rule following allows access to that resource then the user has access.

Alternatively if a rules allows access to a resource but the following rule blocks access to the resource then the resource cannot be accessed.

The default rules are applied first and can be overridden by a login rule.

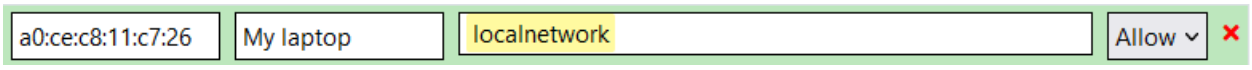
If the device rule box is clicked the choose rule box is opened. This gives an opportunity to change the order of rules, delete rules or add a new rule. When formulating rules take great care with the order that they are added to devices and users.

The next figure shows the choose rule box reopened so that the rule order can be changed using the up and down arrows.



If the admin decides that an additional rule is necessary to achieve the access control objective then a new rule is created and added to the device or user.

Each of the MAC addresses in the list has a policy (allow, block, login) and a list of rules. This is shown in the figure for clarity.



If the policy is set to allow (green), the user gets access to all resources except a resource blocked by a red rule in the default rule box. To negate the default rule block, the user requires a green rule that allows access to the blocked resource. If the admin does not want a resource blocked after login then a red rule should not be added to the default rule list.

If the policy is set to block (red) the MAC is blocked, there is no login page and no access to any resource. A green rule can be added to the rule list that will override the red default policy. Rules always override policies.

If the policy is to set to login (yellow), the MAC user is then shown a login page. A green rule or red rule can be added also.

The example above will allow the MAC address access to the Internet without needing to log in but the user will see a login page when attempting to access the local network: The user will then need to supply credentials. A green 'localnetwork' will override the yellow one.

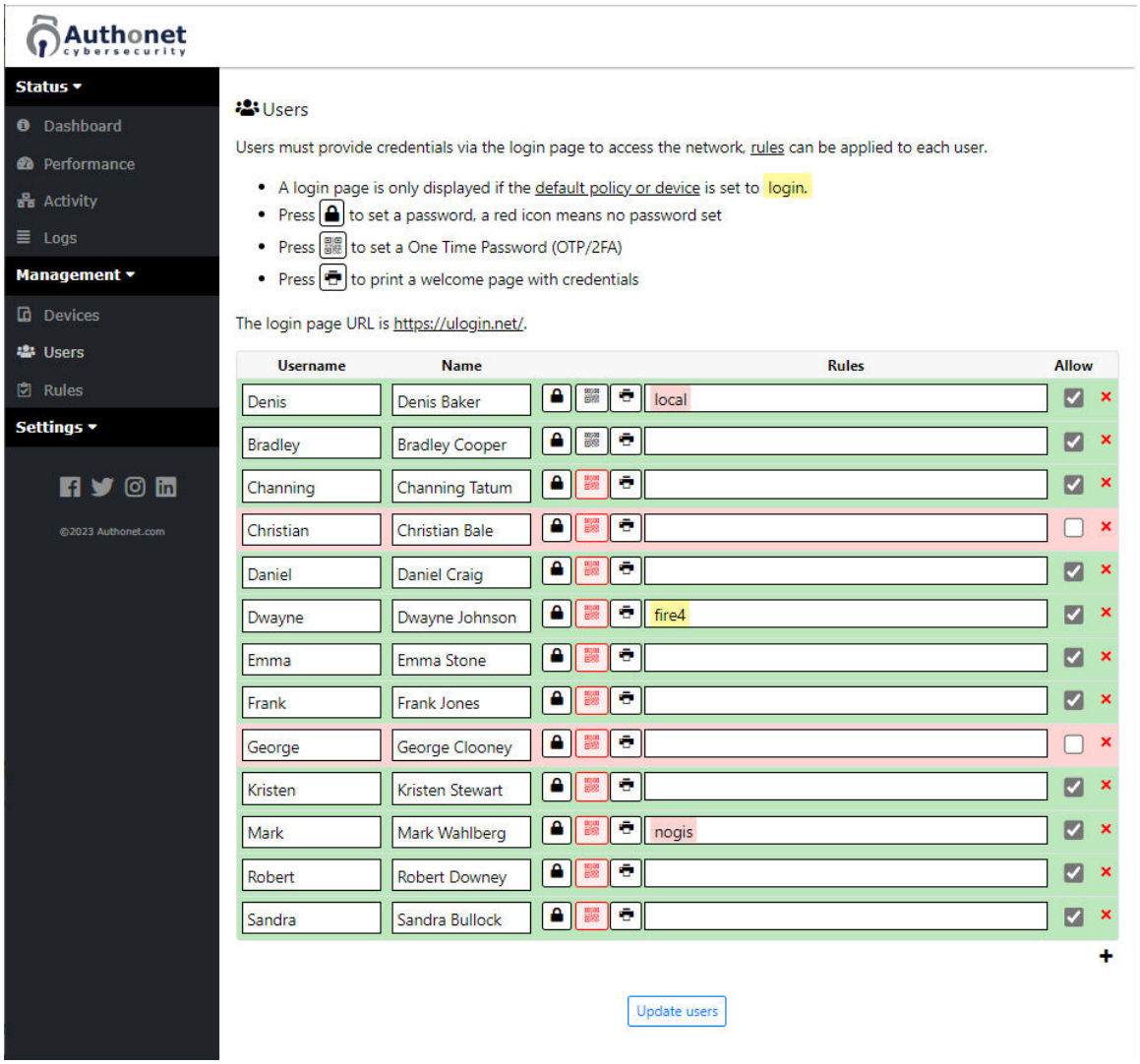
Add Rules to the User List

Next open the user list in preparation to add rules for each user.

Click the first rule box corresponding to a user to open the choose rules box, then select the appropriate rule or rules for the user.

Repeat this process for all users.

When the users have been configured, click the update users button at the bottom of the page.

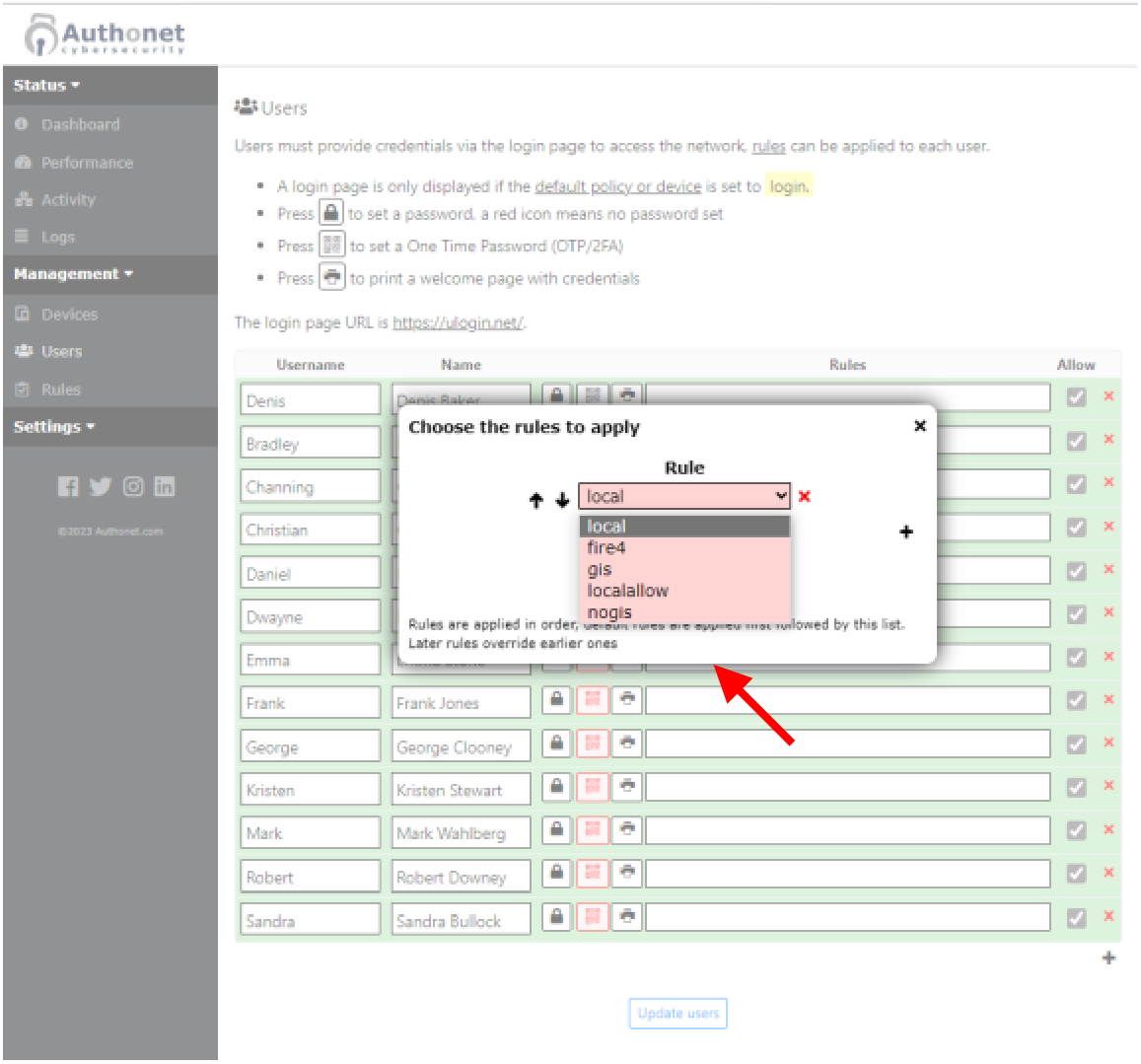


When the user rules box is clicked, the choose rules box opens as shown in the next figure.

Click the down arrow in the rule box to show the drop down list of rules that have been configured. Click a rule from the list to add to the user. More rules can be added by clicking the + character. Continue to add rules from the drop down list.

When all rules have been added click the set rule button on the box.

When the rules have been configured, click the update users button at the bottom of the page.



Rule order matters when multiple rules are added. A later rule might override the instruction of a previous rule. For this reason there are up and down arrows that are used by the admin to change the order of rules.

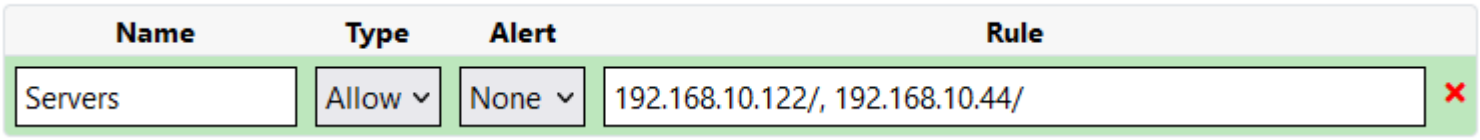
Examples of Rules and their Implementation

Some examples of rules are presented in this section to provide guidance for admins who are creating rules for specific business requirements.

RULE-1: Block access to the LAN but allow access to two servers at the IP's 192.168.10.122 and 192.168.10.44

Is it necessary to require users to log in to access the two servers? If not then set the default to BLOCK with an ALLOW rule. See the example below.

Rules page:



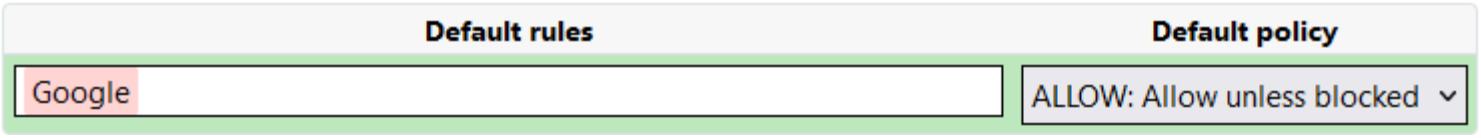
Devices page:

Users will not a see a login page, and will not be able to access the Internet but will be allowed to access the two servers.

RULE-2: allow access to the Internet but block www.google.com

Create a block for Google on the rules page:

Set default on devices page to ALLOW adding the block for Google:

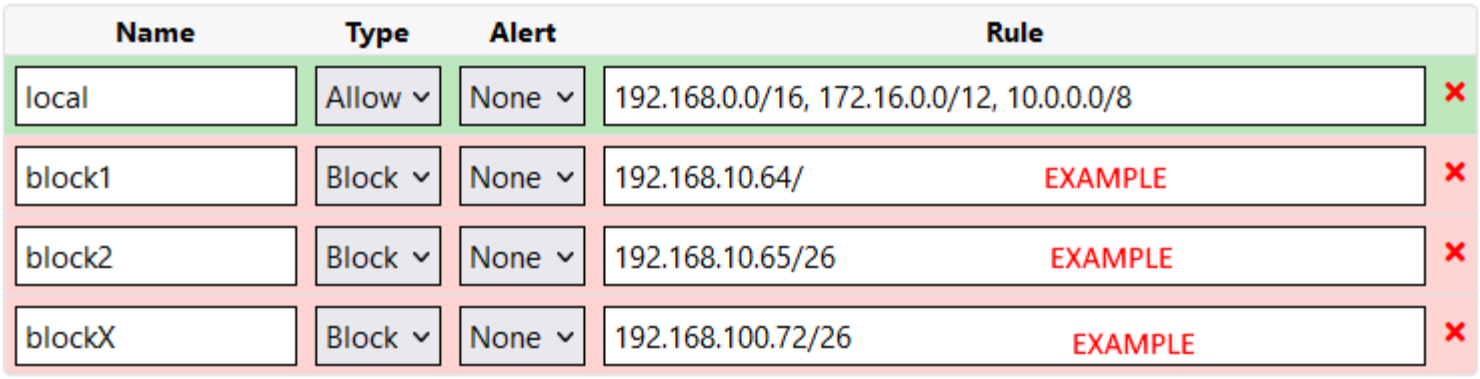


Users will not have to login but will not have access google.com

RULE-3: allow access to the LAN but block a list of servers from IP's 192.168.10.64 to 192.168.100.72

This rule is not straightforward, and not a recommended network configuration starting from an IP address that is mid-block to another IP that is mid-block. It is necessary to use a subnet calculator to work out the subnets to block and create a rule for each one. The last rule allows access to remaining IPs. Set a default of block or allow depending on whether it is required to allow Internet access in addition to the LAN.

Create the rules:

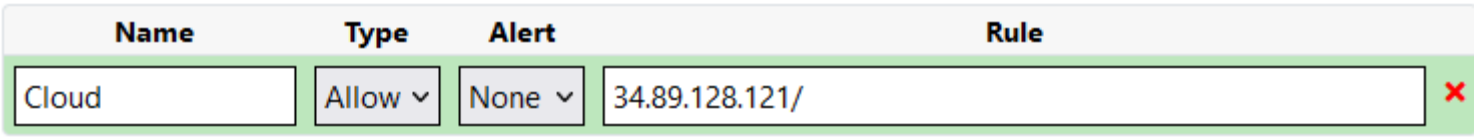


Set the defaults:

In this case, the system would check block1, block2 and blockX to block the server access, then allow the remaining LAN access, and block access to the Internet.

RULE-4: block access to the Internet but allow access to the public cloud server 34.89.128.121

Set the rule on the rules page:



Devices page:

PART 7:

The Users View of Authonet ZTNA Management

Staff Login Preparation

The administrator will add each member of staff to the user database. The administrator will then give each staff member a printed sheet like the one shown below, with the following information.

- Staff member name.
- Browser page to open to login.
- The username to enter.
- The password to enter.
- A QR code that is used for the 2-factor authentication process.

Authonet cybersecurity

Welcome to the Authonet network

Your credentials to access the network are as follows:

Name:	Bradley Cooper
Login page:	https://ulogin.net/
Username:	Bradley
Password:	Da3QY*mW

Two Factor Authentication QR code:

The Two Factor Authentication / One Time Password (2FA/OTP) login adds an extra layer of security to the network, it requires that an extra 6 digit password be provided for each login. The 2FA/OTP password changes at each login. An app needs to be set up on a mobile device such as a phone or tablet to generate the password.

The recommended app to use is **FreeOTP**, this can be downloaded from the Apple App Store or the Google Play/Android store.

Once the app is installed, click on a **+** sign and/or the QR code icon and scan the QR code above with the camera on the device.

The staff member must be instructed to store the login information in a safe place and not share with others. The security of the business information depends on each member of staff maintaining login information in a secure place. The information provided on the printed sheet **must not** be stored on the computer to protect the security of the information.

The administrator must distribute the staff login information on printed sheets, not electronically via email. If a computer becomes infected with a Trojan virus and the login information is stored electronically on the computer then the cyber criminal can use the login information to get access to the network.

The administrator can issue a new sheet periodically to strengthen security; this can be every month or every quarter.

Each staff member must install a 2-factor authentication app on a personal mobile phone. An app called FreeOTP is recommended. FreeOTP is a popular app that is free and available from both the iPhone store and the Android store.

Some of the OTP apps available for mobile phones are listed in the table below.

Google Authenticator	Authy
Microsoft Authenticator	LastPass
LastPass Authenticator	FreeOTP
andOTP - OTP Authenticator	TOTP Authenticator – 2FA Cloud
2FA Authenticator (2FAS)	Bitwarden Password Manager
Aegis Authenticator	Aegis

The app is initialized using the QR code on the password sheet provided by the administrator.

- In the case of FreeOTP, follow the instructions.
- Open the app.
- Bottom right is a ‘+’ sign tap this.
- Above this appears a photo symbol, tap this.
- Hold the phone camera over the QR code on the sheet; the camera will capture the code.

The procedure of capturing the QR code using the FreeOTP app is shown in the next figure.

The app is now ready to provide the one time password (OTP) when required.

If other app’s are used to provide the OTP the administrator should consult the app manufacturers information to scan the QR code and to read the OTP.

Staff Login Procedure

Assume that a member of staff is configured for login with 2FA.

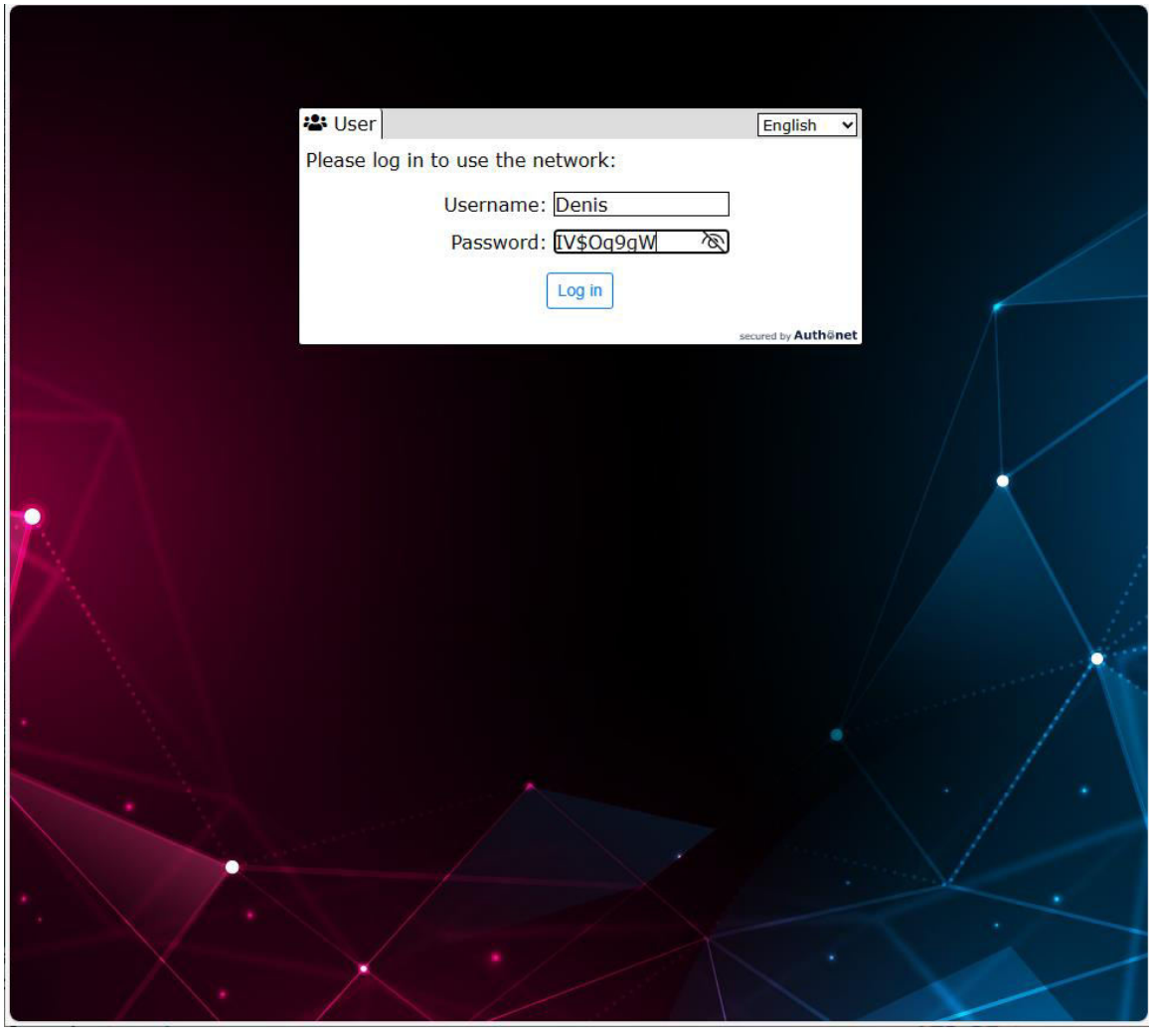
With the staff computer connected to the Authonet ZTNA gateway LAN network, the browser will show the login window when a new tab is opened. Alternatively the user can type the name of the login page, or set the login page as the browser home page.

ulogin.net

or

https://ulogin.net:8080/

The login page will open and the user can enter the username and password and then click the login button. This is shown in the next figure.



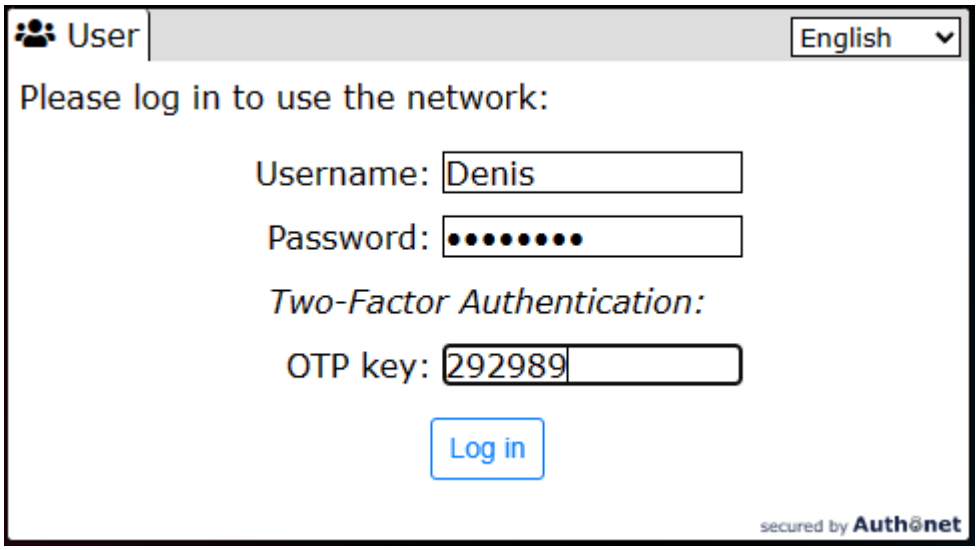
The user then has to use the personal phone to get the one time password (OTP).

- Open FreeOTP.
- Tap the icon with the username.
- The OTP will be displayed, enter this code in the login page.

Using the phone to get the OTP code is shown in the next figure using FreeOTP. The validity of the code is one minute and so has to be entered quickly before it expires. The user may want to wait for the code to change before entering the next code.

After entry of the password the login page displays a box to enter the 6-digit OTP code. The code is typed into the box and then the login button is clicked.

The OTP code entry is shown in the next figure.



PART 8:

Protect Against Password Theft and Phishing Attacks

Protecting a Business Against a Cyber Attack

A cyber attack can originate outside the network via a remote access port or inside the network via a Trojan virus.

An attack outside the network relies on a firewall attack or an attack on a remote access port. A firewall attack is difficult because a properly configured firewall is very difficult to breach. If the business does not have a firewall then a remote attack is made easy.

A criminal may seek to steal a password through social engineering. That can be a password owned by a remote employee of by a third-party supplier to the business. Password theft is remarkably easy. The criminal will research members of staff and can obtain a lot of information through social media. The criminal can then send a message to a staff member as though it was from another staff member that the person knows requesting to “borrow” the password for some invented reason. If the criminal was convincing then the person will provide the password. The criminal then has access to the business network.

Staff training should instruct staff to never share a password. The login screen should have the contact information for the admin to be used if a staff member looses a password. The admin can then speak personally with the staff member.

The Trojan virus attack was explained at the beginning of this manual. The criminal is able to trick a member of staff using phishing messages to install the virus on a computer, which then gives the criminal remote access to that computer, bypassing the firewall. Many business networks use a login method such as Microsoft Active Directory. Unfortunately this does not stop the attacker. With remote access to the computer the criminal has access to the computer network and can attack the server using an operating system exploit. The attacker does not need a login for Microsoft Active Directory. Many smaller businesses do not apply server security patches when available and a lot of businesses have server software versions that are no longer supported by the manufacturer.

Password Theft Protection

Password theft protection can be implemented using an end-point security product with 2-factor authentication. Implementation of 2-factor authentication using the Authonet ZTNA gateway is described in this manual.

With 2-factor authentication, a password alone is not sufficient to access the network. In addition to the password a one-time password (OTP) code must be entered that is obtained from a mobile phone app. While employees might consider 2-factor authentication to be a nuisance, it is in fact the single most effective security tool available. All security providers recommend 2-factor authentication. Microsoft published a security report stating that they consider combining 2-factor authentication with Zero Trust Network Access plus anti-virus

protection and security patch updates will reduce the risk of a cyber attack by 98%. (*Microsoft Digital Defense Report, p.114, The cyber resilience bell curve © copyright Microsoft, 2023*).

Many security standards require the implementation of 2-factor authentication for compliance. The HIPAA (Health Insurance Portability and Accountability Act) security rule requires 2-factor authentication for access to PHI (Protected health information) in order to comply with the rule. More can be read at this link about the HIPAA security rule.

https://www.hhs.gov/hipaa/for-professionals/security/index.html

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

The NIST (National Institute of Standards and Technology) Cybersecurity Framework recommends the use of multi-factor authentication. Read more at this link.

https://www.nist.gov/system/files/documents/noindex/2022/02/17/MFA.pdf

Most banks and large businesses already have multi-factor or 2-factor authentication as part of their cyber attack protection. Many smaller businesses do not have multi-factor authentication. Cyber crime can be reduced by a significant percentage if all businesses adopt 2-factor authentication for staff, customers and suppliers. The technology is economical and easy to implement with Authonet products. Cost is not a barrier to protecting a business from a cyber attack with 2-factor authentication.

Phishing Protection

The process of a phishing attack to install a Trojan virus on a staff computer was explained earlier in this manual. A phishing attack can be blocked with network access management.

The phishing attack relies on a user clicking a link in a phishing message that will then download the Trojan virus and install it on the staff computer. The virus will then give the cyber criminal remote access to the computer.

A phishing attack can be prevented by blocking the message to the criminal's server if a phishing link is clicked.

It is necessary to lock down the network using access control rules. Simple rules are listed below.

- A staff computer has access to all devices in the local area network, however the computer can access only specific Internet web sites that may be cloud application servers or supplier websites. Access to all other websites is blocked.

In practice this requirement is not a great impediment to the daily business operations, and considering that a phishing attack is prevented the implementation is worthwhile. If it is necessary for a member of staff to have full

Internet access then a second computer is provided with the following characteristics.

- The staff Internet computer has full access to the Internet, however all access to the local network is blocked. If a Trojan virus is installed on this computer the criminal has no access to the local network servers.

If it is required that a staff member needs full access to the Internet plus full access to the local network then the staff member is given two computers, each with the configuration described previously. If the staff member needs to transfer information between the two computers then this is done via cloud storage that has virus-checking software. In this scenario the staff members work routine is a little more complicated than would be the case with one computer, however the business is secure from a cyber attack.

Many larger companies such as Google have implemented this method of protection. All banks implement the same method. The majority of smaller businesses do not implement any type of network lock-down and so are susceptible to data theft and ransomware attacks.

It is clear that staff training is essential so that staff members understand the methods of working and the protection that they afford for the business.

Cybersecurity Planning

Protection from a data theft or ransomware attack is accessible to all businesses. The following action items need to be implemented by the business.

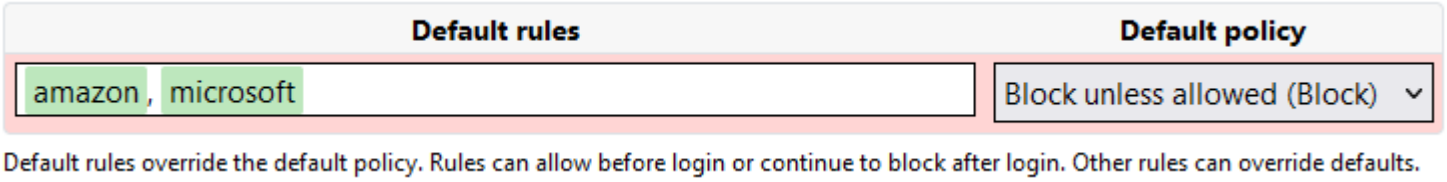
- Ongoing staff training so that staff understands the need to change work routines and the benefits that they bring to the workplace.
- Network infrastructure upgrades to incorporate ZTNA and 2FA, essential tools to protect the business. Ensure that the network Internet interface has a firewall installed.
- Frequent updating of security patches for all applications software, operating systems and firmware in devices such as routers.
- Installation of anti-virus on all computers with automatic updating of the virus signature files.
- If possible switch applications software to cloud versions hosted by the manufacturer for greater security.

Cybersecurity is an ongoing process and all businesses must budget for the cost of cybersecurity. When a business seeks cybersecurity insurance the insurer will request that the business complies with the list of action items above.

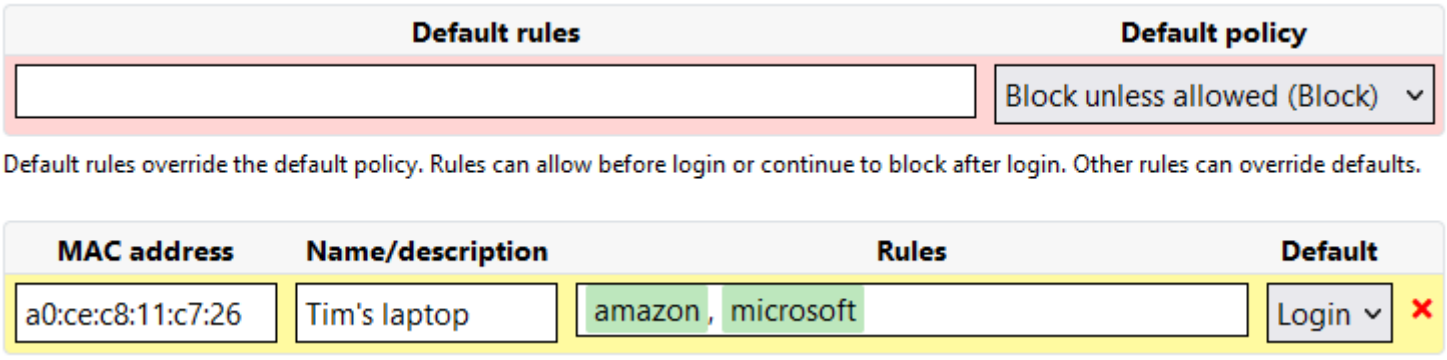
Configuration Example to Block a Phishing Attack

Allow user access to specific Internet domains, block access to all other domains to prevent a phishing attack link installing a Trojan virus after it is clicked.

Create rules for the domains that have access allowed. Set the default to block and then allow specific domains using default rules. Only the specified domains will be accessible, all other domains will be blocked, including the domain that the Trojan virus is trying to access. The devices page will look like this:



An alternative to lock down Internet access is to allow only known MAC's to access the approved domains, in this example amazon.com and microsoft.com. Set the default to block but instead of setting default rules to allow access to domains, configure the MAC's with a default of 'login' and the allow rules for the domains. In this case only the known MAC's will have access, but those MAC's will be forwarded to the login page unless they access the allowed domains. The next example shows this configuration.



Although staff access to the Internet has some restrictions, the benefit of preventing a phishing attack will allow staff to work without concern for a ransomware or similar attack.

PART 9:

Reset the Authonet Gateway to the Factory Default Setting

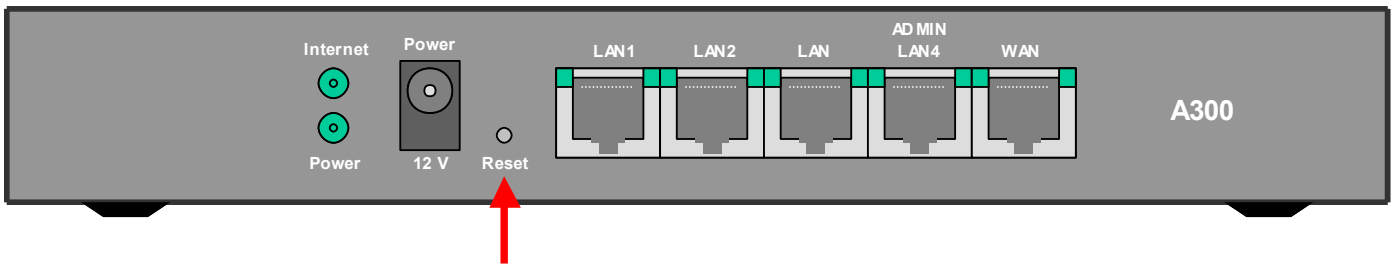
Reset the A300 Gateway to the Factory Default Setting

The A300 gateway has a reset button to the left of the LAN1 port. Follow the steps listed below to reset the gateway to the factory default setting.

1. Power the gateway.
2. Wait 5 minutes for the software to initialize.
3. Using a paperclip, press the button and hold in for 10 seconds, then release the button.
4. The gateway will now reset.
5. Proceed to reconfigure the product using the setup screen as described in an earlier section.

When the gateway is reset to the factory settings all data is erased. If it is wished to keep the settings then they must be backed up and restored after the factory reset.

The reset button is shown in the next diagram.



With the unit powered up hold the reset button in with a paperclip for 10 seconds then release

Reset the A1000 Gateway to the Factory Default Setting

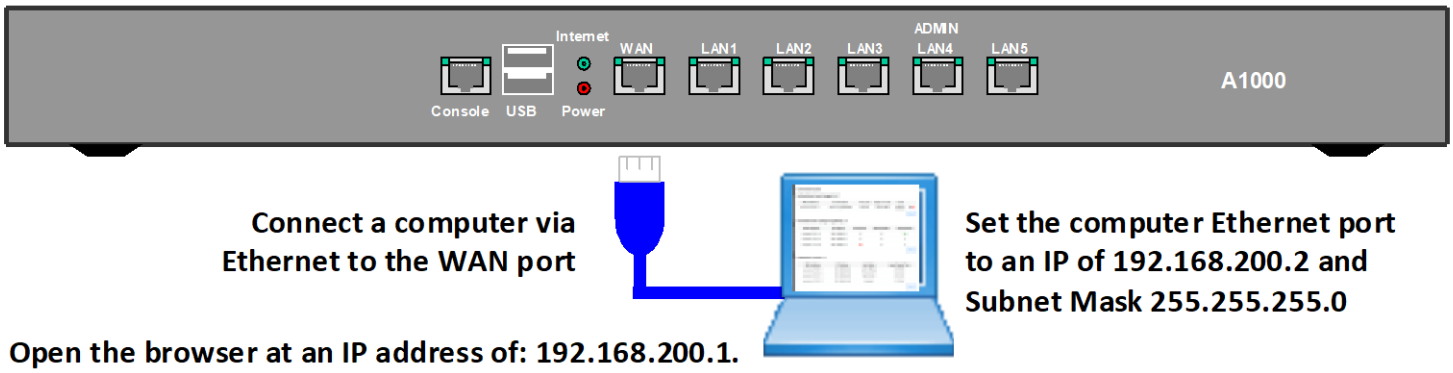
The A1000 gateway does not have a reset button.

To reset to the factory setting follow the configuration listed below:

1. Connect a computer to the WAN port of the gateway.
2. Set the computer Ethernet port to an IP of 192.168.200.2 and Subnet Mask 255.255.255.0.
3. Open the browser at an IP address of: 192.168.200.1.
4. Type the username reset and the password reset.
5. Click on “Enter", another page will appear.
6. Click on the "Reset to defaults" button and then wait two minutes.
7. Switch the product power off then on.
8. Proceed to reconfigure the product using the setup screen as described in an earlier section.

When the gateway is reset to the factory settings all data is erased. If it is wished to keep the settings then they must be backed up and restored after the factory reset.

The reset connection is shown in the next diagram.



Open the browser at an IP address of: 192.168.200.1.
Type the username reset and the password reset.
Click on enter, another page will appear.
Click on the Reset to defaults button and then wait two minutes.
Switch the product power off then on.
Proceed to reconfigure the product as described in an earlier section.

PART 10:

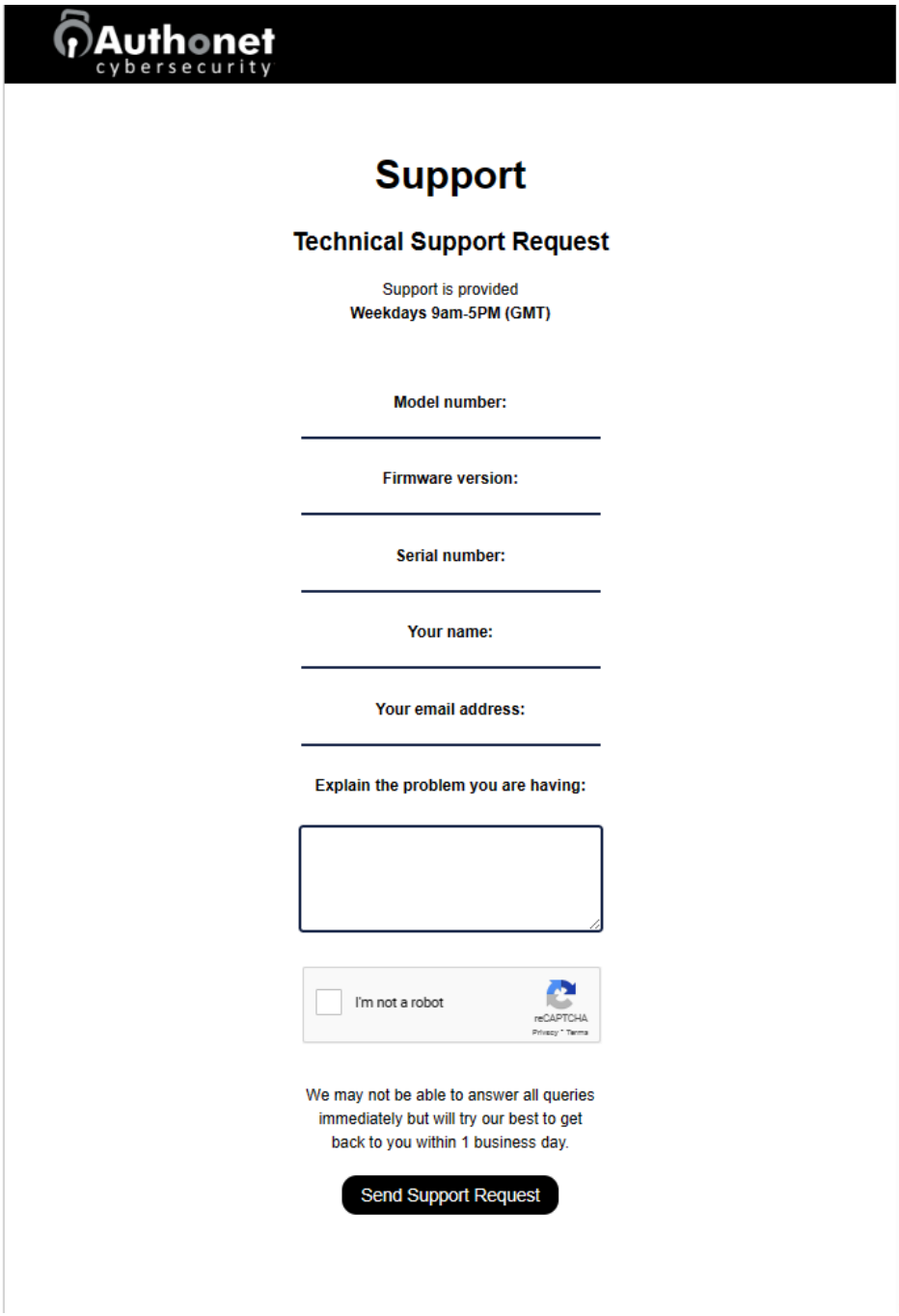
Authonet Product Support and Customer Assistance

Authonet Product Support and Customer Assistance

Authonet provides free on-line installer and customer technical support. Customers and installers should consult this manual and the training videos before contacting technical support. The technical support is available at the Authonet website. Open the following web page.

https://authonet.com/support.html

Provide the information requested on the form shown below.



Provide the following information when requesting technical support.

- Model number:
- Firmware version:
- Serial number:
- Your name:
- Your email address:
- Explain the information that you need, or the problem you are having, with as many details as possible.

Support is provided Weekdays 9am-5PM (GMT). The response time is one to two business days for the free support service.

Authonet Cybersecurity and Product Training

Authonet provides a series of training presentations in a video format for both customers and installers. There are 5-minute introductory videos and 30-minute training videos. The videos are hosted on Youtube and can be accessed through the Authonet website. The videos are free to watch.

The 5-minute videos are as follows.

- Introduction to Cybersecurity for business owners and managers.
- Cybersecurity awareness for business staff.
- Introduction to Authonet cybersecurity for IT service businesses.
- The benefits of Authonet ZTNA cybersecurity gateway products.

The 30-minute videos are as follows.

- Cybersecurity for businesses owners, managers and staff.
- Authonet ZTNA gateway configuration for IT service businesses.

The presentation slides are also available for download from the Authonet website.

Training material is also available for Authonet gateway product distributors and resellers. Please contact Authonet for more information about this training material.

Partner Cybersecurity Training

Authonet has a partnership with Internet Technology Answers Inc to provide training services that are available in modules. All modules in a course can be accessed after the payment of one fee for the course. After purchase the training courses can be viewed multiple times.

The training courses are as follows.

- Cybersecurity protection for business owners and managers: 8-module course, each module is 30 minutes duration.
    - Module 1: Cyber attack risks, methods and attackers.
    - Module 2: Prepare a comprehensive cybersecurity plan.
    - Module 3: Working with service providers to protect the business.
    - Module 4: The importance of staff training to recognize risks.
    - Module 5: Upgrading the network infrastructure for protection.
    - Module 6: Migrating applications to the cloud.
    - Module 7: A ransomware recovery plan.
    - Module 8: Advanced technical infrastructure requirements.
- Cybersecurity awareness for business staff: 8-module course, each module is 30 minutes duration.
    - Module 1: What are cyber threats and cyber attacks?
    - Module 2: What do cyber criminals want?
    - Module 3: How cyber criminals attack.
    - Module 4: How to recognize an attack.
    - Module 5: Escalating to a cybersecurity expert.
    - Module 6: Data theft and ransomware.
    - Module 7: Businesses at risk.
    - Module 8: Methods of protection.

Internet Technology Answers Inc will also plan to host live Q&A sessions, for businesses that purchase the training courses.

Internet Technology Answers Inc will publish a book to advise business owners and managers how to protect their businesses from a cyber attack. The book will be available in print from Amazon and also from Amazon Kindle. Internet Technology Answers Inc publishes a Blog providing many updates about cybersecurity issues.

If you have questions that were not answered in this manual please contact our technical support team.

Free support: https://authonet.com/support.html

Company information

Authonet products protect your business against cyber attacks with a simple and affordable fully-managed Zero Trust Network Access (ZTNA) system that shields the business data from cyber criminal phishing and password theft attacks and provides fast threat alerts.

Authonet products are designed and manufactured in the UK by Fire4 Systems (UK) Ltd.

Phone: 1-800-213-0106 - International: 1-786-358-5406 - Email: info@authonet.com