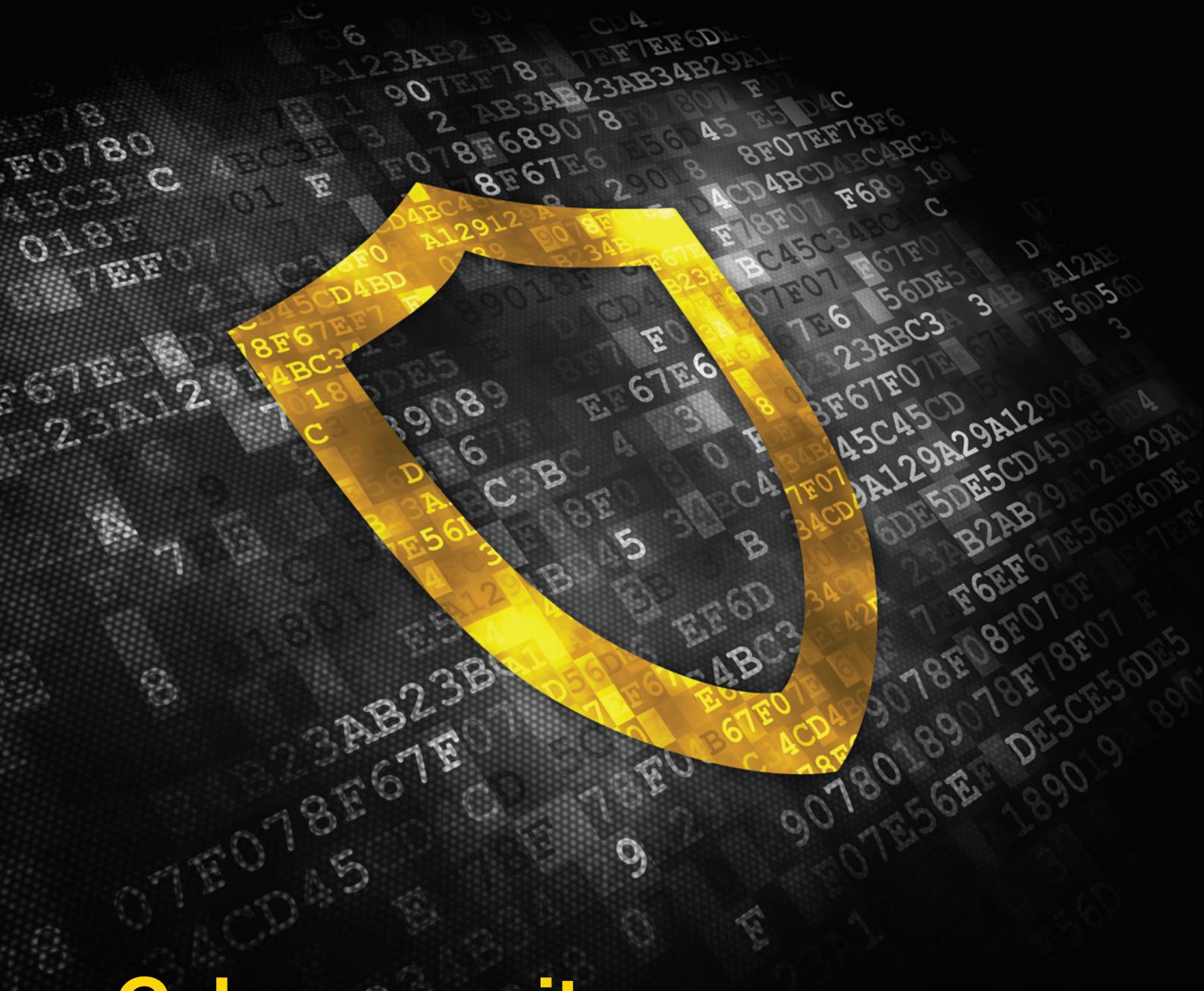
zenitel
because communication is critical



Cybersecurity

Hardening Guide

How to prevent or reduce the impact of security risks.

v.2.0

zenitel

Hear, be heard and be understood – every time, everywhere

Communication is critical in all areas of business. Actionable intelligence is essential to decision making that promotes operational efficiency.

When communication requires voice audio, intelligibility is paramount. You can't afford to get the message wrong — if you do, then you have a business problem.

For over 70 years, Zenitel Group has delivered innovations that solve that business problem, ensuring that people can hear, be heard and be understood – every time, everywhere.

Content

Cybersecurity

Network access gives your staff and company many benefits. However, the more access that you provide, the greater the danger that someone will exploit the increased vulnerabilities. Cybersecurity is the key to ensuring a safe, stable and resilient cyber environment.

Meeting cybersecurity risks head on

Every new system, application or network service added comes with potential security vulnerabilities, making cyber protection increasingly more difficult and complex. By confronting the serious network security risks pragmatically, you can reap the benefits while minimizing those risks. To accomplish this, you need a solid cybersecurity plan and the resources to execute it. Handling cybersecurity risk reduction up front typically takes fewer resources than having to clean up after avoidable cyber attacks.

Defending against cyber attacks

The vast majority of cybersecurity problems that occur can be prevented by proactive actions, technology and practices that are already available. Yet, many organizations are overwhelmed by the "Fog of More": more work, problems, regulatory and compliance requirements, conflicting opinions, marketplace noise, and unclear or daunting recommendations than anyone can manage. Even for the rare enterprise with the information, expertise, resources and time to sort through everything, it is rarely true for all their key business partners, suppliers and clients.

Membership with CIS

(Center for Internet Security) is a forward-thinking nonprofit entity that harnesses the power of the global IT community to safeguard private and public organizations against cyber threats. Its CIS Controls Version 7.1 and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. The CIS Controls align with all the major compliance frameworks, such as NIST Cybersecurity Framework, NIST guidelines and the ISO 27000 series, as well as regulations including PCI, DSS, HIPAA, NERC CIP and FISMA.

A volunteer global community of experienced IT professionals continually refines and verifies these proven guidelines. CIS is home to the Multi-State Information Sharing & Analysis Center (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for state, local, tribal and territorial governments.

Zenitel is proud to be a CIS SecureSuite member, enabling us to further bolster our cybersecurity defenses by leveraging CIS expertise and resources to help protect against today's most pervasive and dangerous cyber attacks.

"The vast majority of cybersecurity problems that occur can be prevented by proactive actions, technology and practices that are already available."

Developing a strong foundation

The CIS Controls are split into what CIS call Basic Foundational and Organizational.

Along with the Basic Controls (1-6), an effective cyber defense system will follow the five critical tenets:
Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups discussed below are a great place for organizations to start identifying relevant Sub-Controls.
Measurements and Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.
Automation: Automate defenses so that organizations can achieve reliable, scalable and continuous measurements of their adherence to the Controls and related metrics.

In CIS's view, it is also vital to make a formal, conscious and top-level decision to integrate the CIS Controls within any organization's standard for cybersecurity. Senior management and the Board of Directors must also be onboard for support and accountability, calling for implementation of the basic CIS Controls in their organizations, as a minimum requirement.

More information about the CIS Critical Security Controls framework can be found at https://www.cisecurity.org/controls/

NOTE:
This guide covers the ICX-500 Gateway and the ICX-AlphaCom and AlphaCom XE server series, plus all Zenitel IP intercom devices, except the ITSV-1 Desktop Video Telephone. Unless explicitly stated, desktop tools such as AlphaPro, AlphaView, VS-Recorder and VS-Intercom Management Tool are not included.

CIS SecureSuite Membership

Cybersecurity planning

You need to consider and understand what is critical for your company and the system and solutions you use. From there, you can plan, implement and manage your cybersecurity defense.

Zenitel has developed this Cybersecurity Hardening Guide to help you approach your planning, based on the CIS Controls. It combines our experience applying best practices developed by CIS to support end users and integrators to build a good cyber defense.

We recommend that organizations follow the CIS Implementation Groups to help prioritize their strategy based on their fit to the following 3 Implementation Groups:

Implementation group 1:

An IG1 organization is usually small-to-medium sized, with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel.
The principal concern of these organizations is to keep the business operational as they have a limited tolerance for downtime. A family-owned business with 10-50 employees could self-classify as IG1.

Implementation group 2:

IG2 organizations tend to be medium-to-large organizations that employ individuals responsible for managing and protecting IT infrastructure, The organizations support multiple departments with differing risk profiles. IG2 organizations often store and process sensitive client or company information and can withstand short interruptions of service. Some small to medium-sized organizations that would normally be seen as IG1 but that are responsible for protecting sensitive data might, therefore, fall into this higher group.

Implementation group 3:

An IG 3 organization will typically be a public body or large corporation with thousands of employees. IG3s employ security experts who specialize in the different facets of cybersecurity, such as risk management, penetration testing and application security. IG3 systems and data tend to contain sensitive information or functions that have regulatory compliance and oversight. Successful attacks can cause significant harm to the public welfare. IG3 focus must therefore be on availability, confidentiality and integrity of data and attack from a sophisticated adversary.

The Key building blocks:

Plan

Risk and Security levels

Risk and security levels vary from organization to organization. The following factors can impact levels:

1.

The number of administrators who will have access to the systems.

A system with many administrators has a higher risk that passwords can fall into the wrong hands or that other things that can go wrong in regards to cybersecurity.

2.

Available resources and expertise levels.

A company with more dedicated IT resources and cybersecurity awareness will be able to implement more controls and make them more effective across the organization as a whole.

3.

The general threat level for your organization.

Companies protecting high-value assets or sensitive data or providing critical infrastructure or public services, face a higher risk that they will have better equipped intruders who will try to break through their cyber defenses.

Security mechanisms

The following table shows the relevant security mechanisms for each level of system, categorized by CIS Control.

CIS CONTROL	Implementation group: IG1	IG2	IG3
Control 1: Inventory of Authorized and Unauthorized Devices			
Own dedicated network for physical security devices.		■	■
Maintain an asset inventory inventory of devices that access the network.	■	■	■
Use asset inventory tools such as DHCP logging, 802.1x with radius accounting, automatic discovery tools, etc. to maintain an up-to-date inventory.		■	■
Deploy Port level authentication via 802.1X to limit and control which devices can access network.		■	■
Use certificates for 802.1X.			■
Resolve unauthorized assets.	■	■	■
Control 2: Inventory of Authorized and Unauthorized Software			
Verify that you have the latest production software for the Zenitel products from your integrator.	■	■	■
Maintain a detailed inventory of authorized software that is required on the network.	■	■	■
Use a software inventory tool to track software running on all devices.		■	■
Resolve unauthorized software.	■	■	■
Control 3: : Continuous Vulnerability Management			
Run automated vulnerability scanning tools.		■	■
Deploy automated SW patch management tools.	■	■	■
Control 4: Controlled use of administrative privileges			
Change default passwords on end devices and servers.	■	■	■
Ensure the use of dedicated administrative accounts for management of the intercom.	■	■	■
Use unique passwords (for more information. (See next page – CIS control 4.)	■	■	■
Maintain a detailed inventory of administrative accounts.		■	■
Control 6: Maintenance, Monitoring and Analysis of Audit Logs			
Activate audit logging.	■	■	■
Enable NTP in the end devices (IP intercom) to ensure all events are logged with the correct time.	■	■	■
Enable SNMP syslog to send event to logging servers.		■	■
Regularly review logs to identify anomalies.		■	■
Control 9: Limitation and Control of Network Ports, Protocols & Services			
Ensure that only ports, protocols and services with validated business needs are applied.		■	■
Apply Host-Based Firewalls or Port-Filtering tools with a default-deny rule to drop traffic from all ports & service other than those specifically allowed.	■	■	■
Review protocols that should be considered to be opened from the dedicated physical network to other corporate networks. (See page 11: CIS Control 9.)	■	■	■
Control 10: Data Recovery Capabilities			
Provide a backup of the configuration on the IP intercom devices.	■	■	■
Control 11: Secure Configuration for Network Devices (Firewalls, Routers & Switches)			
Install the latest stable version of any security-related updates on all devices.	■	■	■

CIS CONTROL 4: Controlled use of Administrative Privileges

Managing passwords and credentials

To manage passwords, you should have a password policy that states how strong the password should be and also how often it needs to be renewed. A strong password is long—the longer the better— and consists of a combination of special characters that is unlikely to for outsiders to guess.

For our IP intercom devices, the ICX 500 gateway, and ICX-AlphaCom / AlphaCom XE servers, Zenitel recommends the use of:

- Strong passwords (up to 20 characters)
- Randomly generated passwords

The log-in credentials for intercom devices and AlphaCom servers are rarely used after the initial configuration. The need to change and renew passwords is therefore not as high as that for passwords used daily. Consider using the same log-in password for the web-config portal on all devices to reduce difficulty with implementation and password management. However to maintain security, only a few administrators should then have and use these credentials.

Tools to manage credentials and passwords

To make credentials for the intercom devices and servers, you should use a password generator. The password should be a minimum of 12 characters, though we recommend 20 characters. You will find a good example of a password generator at https://strongpasswordgenerator.com. Password generators will make credentials that are more difficult to hack.

It is easy to forget strong passwords, and we have seen examples where users have posted their passwords on Post-It notes on their desks. This is obviously not ideal from a security standpoint.

To store passwords, we recommend using a password management program like KeePass, which is open source software, free to use (http://keepass.info). The application stores log-in credentials in an encrypted database. Of course, the password to the database itself needs to be very strong and not something you can remember. But you might need to log in to this database on a daily basis with a password you can remember.

CIS CONTROL 9: Limitation and Control of Network Ports, Protocols & Services

Zenitel's IP communications solutions use the following IP ports, protocols and services:

Table 1 - TCP ports and services

SERVICE	PORT #	DESCRIPTION
AlphaNet Data	50000	Data communication between ICX-AlphaCom servers and external systems
AlphaPro	60001	Used between AlphaPro and AlphaPro PC tool
AlphaVision	55010	Used between AlphaPro and VS Operator PC tool
Demo	50010	Only used for demo applications
DNS server	53	DNS lookup service over TCP
HTTP	80	Used for web and IMT communication
HTTPS	443	Used for web
IP stations	50001	Used between ICX-AlphaCom server and IP intercoms
Multimodule Data	50010	Used between master and slave ICX-AlphaCom server modules
OPC Server 1	61112	Used between ICX-AlphaCom and OPC servers
OPC Server 2	61113	Used between ICX-AlphaCom and OPC servers
SIP	5060	Only supported for SIP intercoms connecting to SIP servers
SIPS	5061	Only supported for SIP intercoms connecting to SIP servers
SSH	22	Used for SSH communication
ZAP	50004	Used for integration between VS devices in SIP/ Edge Mode and external systems
ZAP Web	8080	Used to read ZAP information

Table 2 - UDP ports and services

SERVICE	PORT #	DESCRIPTION
Audio data	5035	Only used for demo
DHCPv4 client	68	Communications with DHCP server
DHCPv4 server	67	Alternative to use ICXAlphaCom as DHCP server
DIP multicast	5001	Group call signaling for ICX-AlphaCom to IP devices
Discovery	5002	Discovery protocol for IP intercom devices
DNS server	53	DNS lookup over UDP
mDNS	5353	
NTP server	123	Synchronize time with NTP servers
SIP	5060	SIP signaling to SIP servers and devices in Edge Mode
Pulse	5062	Additional SIP port used in Edge Mode
SNMP	161	Interface to SNMP servers
TFTP	69	Used for firmware upgrade and auto provisioning
VoIP audio	61000:61250	Transfer of audio and video payload

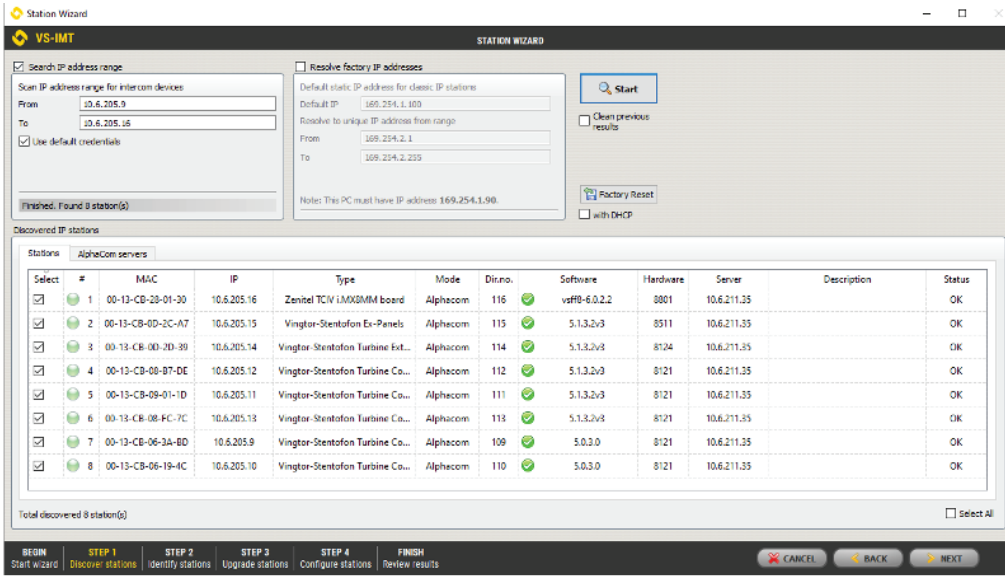
Do

Install and set up for Cybersecurity

Once you have completed the planning phase for ensuring the cybersecurity of your system, it is time to move on to implementation. An important part of this is to configure your device or system correctly. Here, we provide two sets of instructions: one for how to install and configure IP intercom devices and the other for how to install and configure an ICX-AlphaCom / AlphaCom XE server.

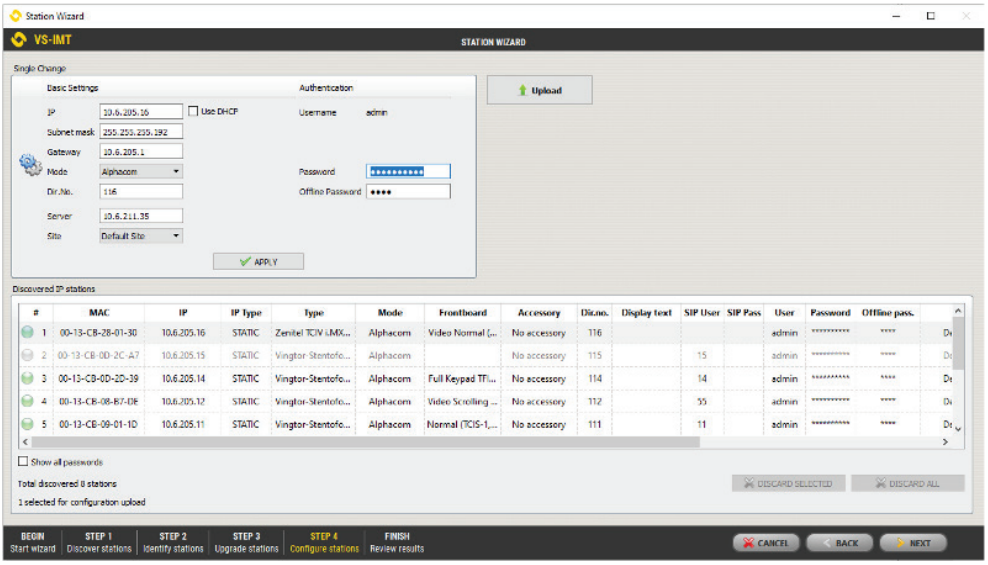
Installation and setup of IP intercom devices for cybersecurity

Here are the basic steps for setting up the system, using IMT for the parameters affecting cybersecurity:



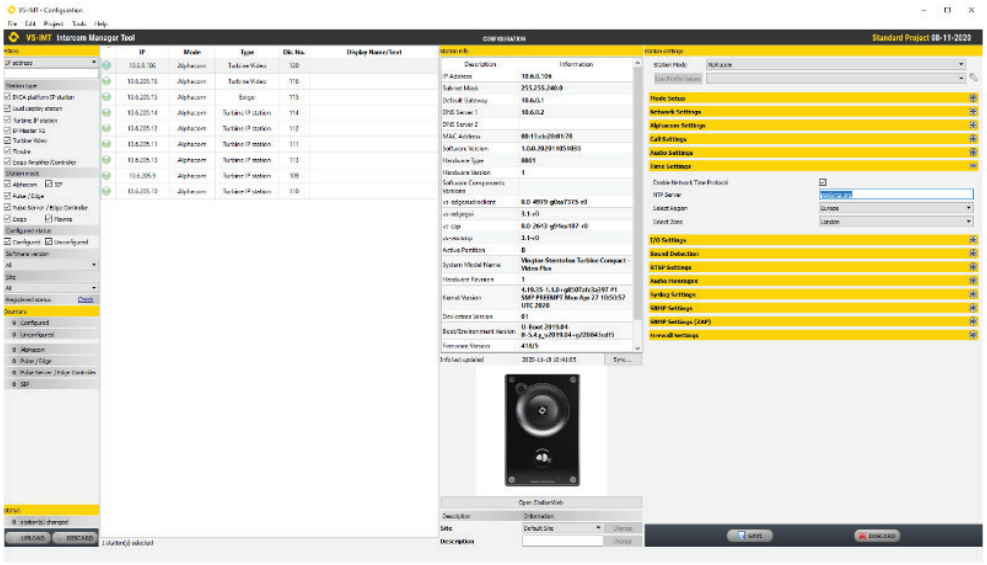
1. Start IMT and discover stations.

- Start the VS-IMT PC tool.
- Open existing project database or press Create to make a new project.
- Press **File > Launch Station Wizard and enter.**
- Select Search, and IMT will find all Zenitel units.



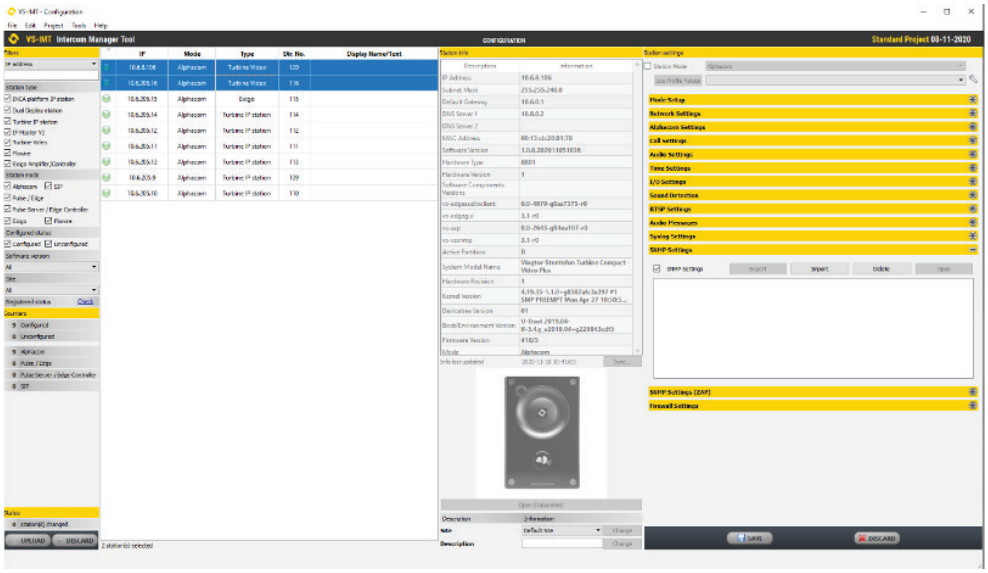
2. Change default password for admin access for all stations.

- Press **Next** until you come to the Configure Stations page.
- Select all stations (Ctrl+ A), Enter the new password, then **Upload.**
- Press **Next** two times to finish the Station Wizard.



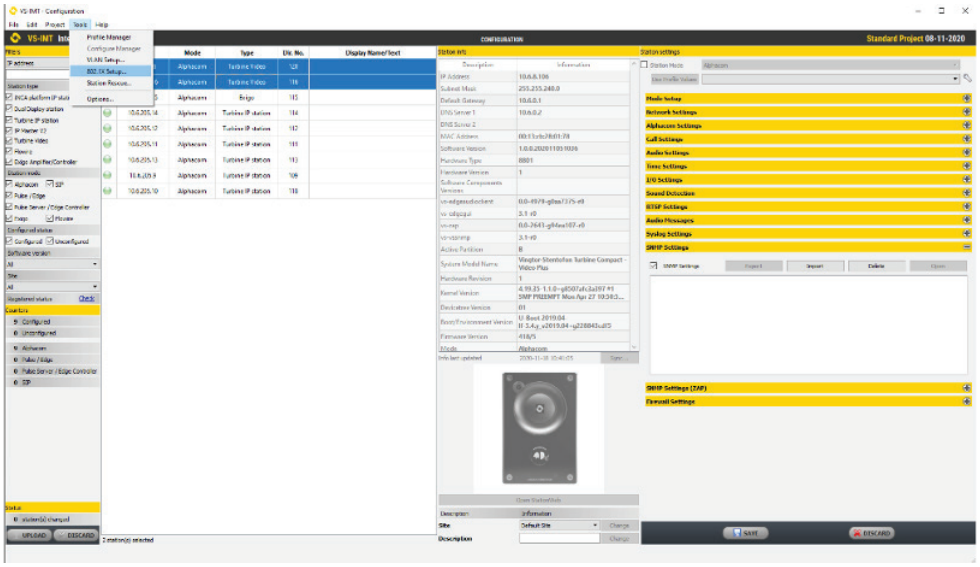
3. Set the NTP server for all stations.

- In the Configuration page, select all stations (Ctrl + A) and open **Time Settings.**
- Enable Network Time Protocol and enter a valid host name or IP Address for the NTP Server.
- Press **Save,** then **Upload.**



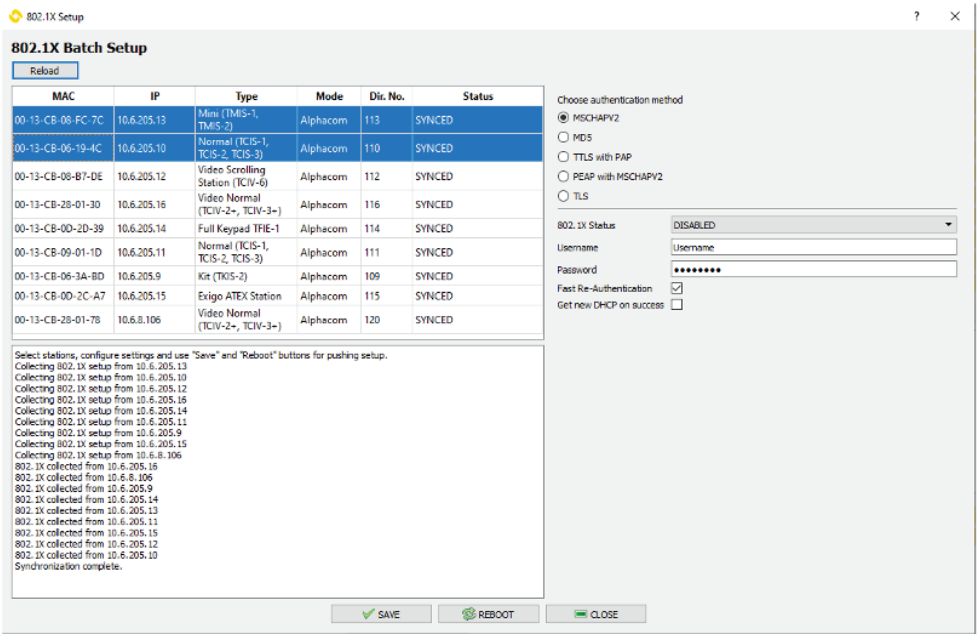
4. Set SNMP parameters

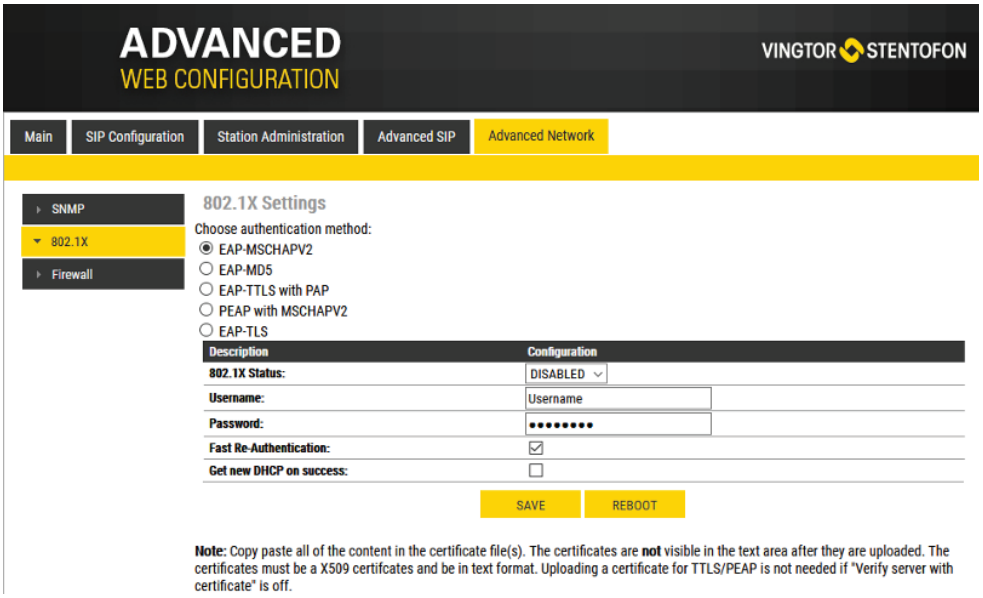
- In the Configuration page, select all stations (Ctrl + A) and open SNMP Settings.
- Enter the relevant SNMP parameters.
- Press **Save,** then **Upload.**



5. Enable IEEE802.1x and set authentication parameters.

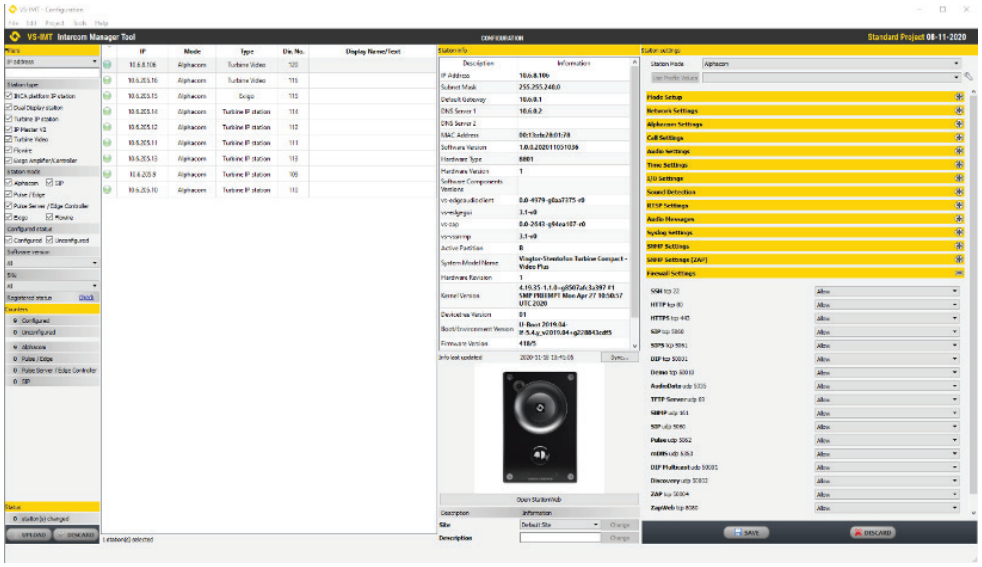
- In the **Configuration page**, from the menu bar, select **Tools > 802.1X Setup.** Select all stations (Ctrl + A).
- Enter the relevant authentication parameters.
- Press **Save,** then **Reboot**.





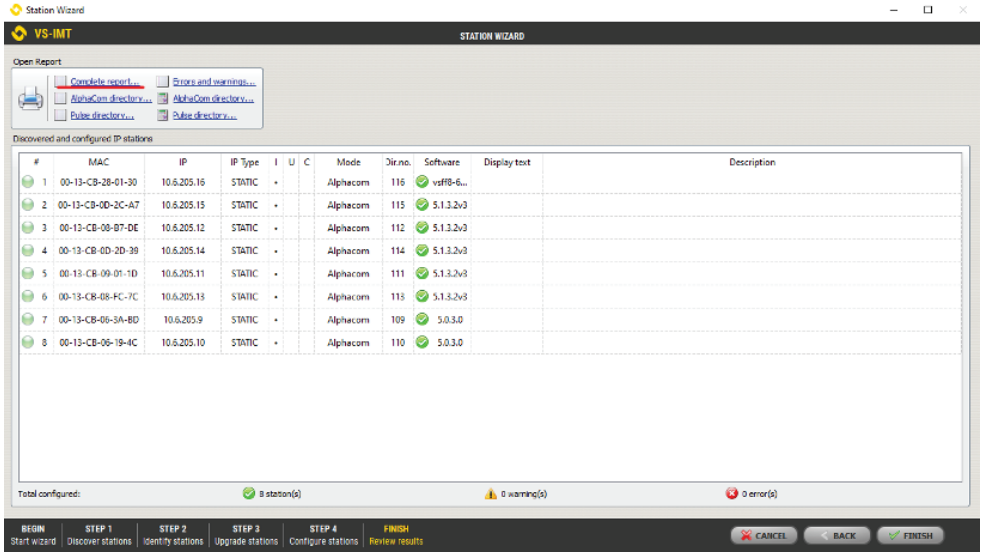
5a. IEEE802.1x at the End device level

- Log in to the Web Configuration page onboard the device.
- Open the **Advanced Network** tab.
- Select the desired authentication method.
- Click on **Save,** then **Reboot.**



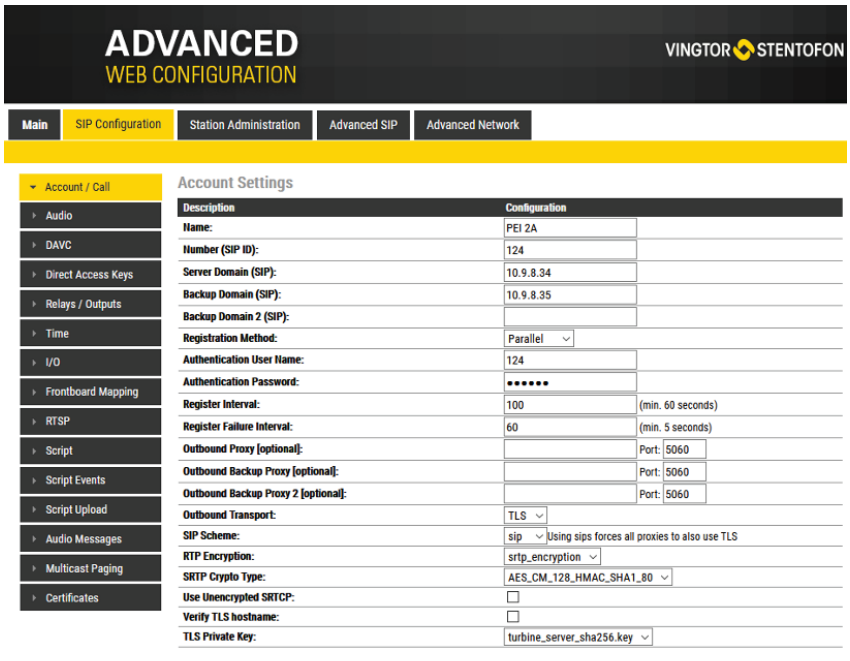
6. Verify IP ports and firewall settings.

- In the **Configuration page**, select one station.
- Open the **Firewall.**
- Check that Allowed/ Blocked services are set according to the needed services.
- Check the Firewall Settings for each station.
- Zenitel products are shipped with the minimum set of IP ports enabled.



7. Generate system description report.

- Launch the Station Wizard. by selecting **File > Launch Station Wizard** and run through the Discover Station process.
- From the last step in the Wizard, use the report generator to create a system report.



8. Security in SIP mode (End-device level)

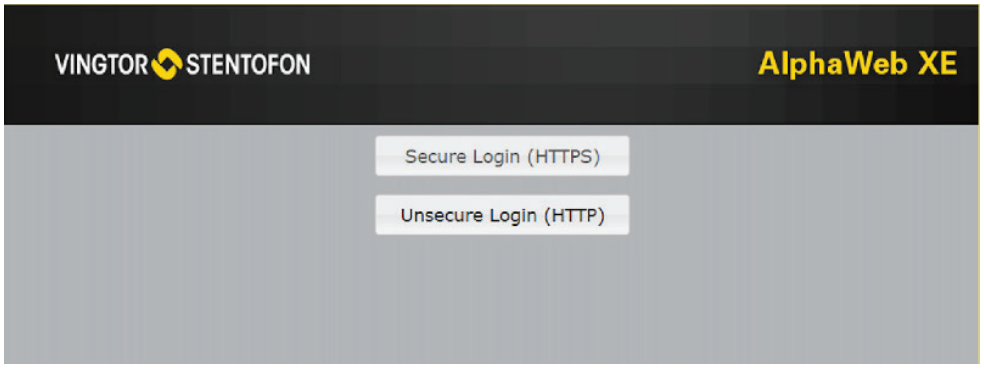
- Log in to the Web Configuration page onboard the device.
- Go to the **SIP configuration** tab, and the **Account/Call** section.
- SIP over TLS encrypts the Transport Layer using the same method as HTTPS.
- TLS 1.2 is supported.
- SRTP encryption is also supported in the following formats:

  AES_CM_128HMAC_SHA1_80

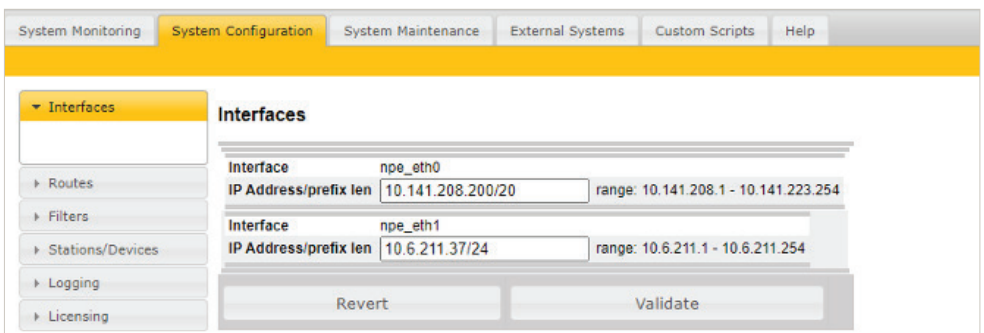
  AES_CM_128HMAC_SHA1_32
- The functions can also be configured in IMT.
- NB: Currently not supported on TCIV+.

Installation and setup of ICX 500 & ICX-AlphaCom / AlphaCom XE server for cybersecurity

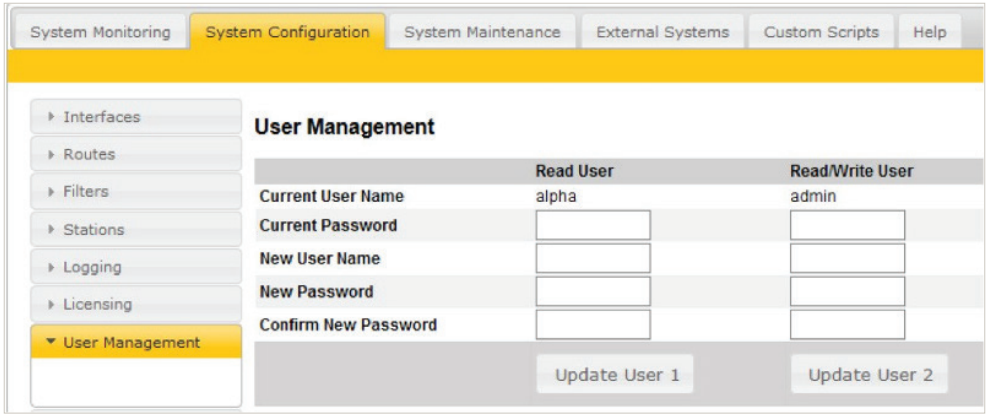
Here are the basic steps for setting up the system using the ICX-AlphaCom / AlphaCom web interface for cybersecurity-related parameters:



1. Log in to AlphaWeb.
You can log in via HTTP or the secure HTTPS protocol.

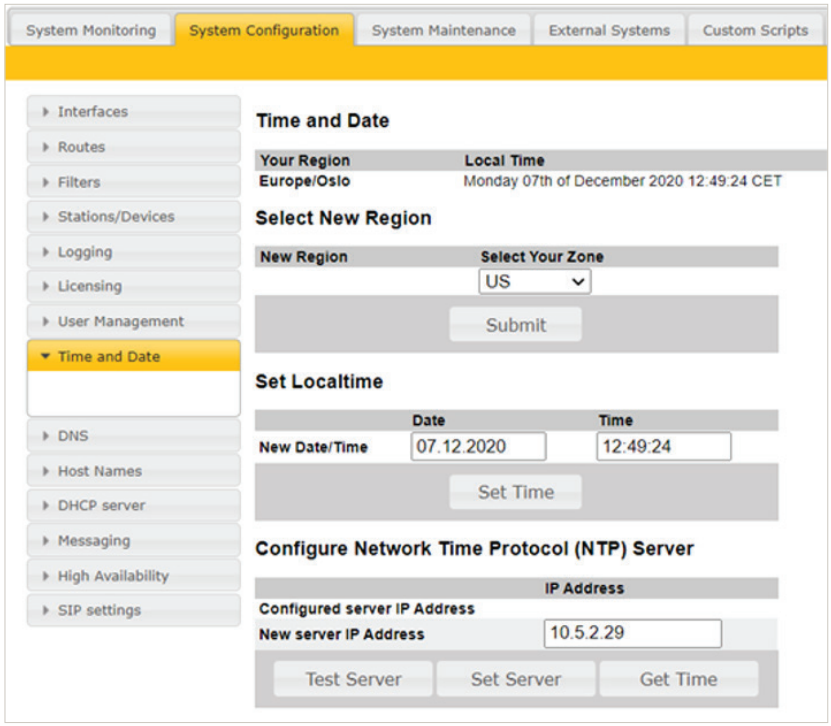


2. Set IP config.
ICX-AlphaCom / AlphaCom has two ethernet interfaces. By default, one port is used for VoIP traffic, the other port for Management.



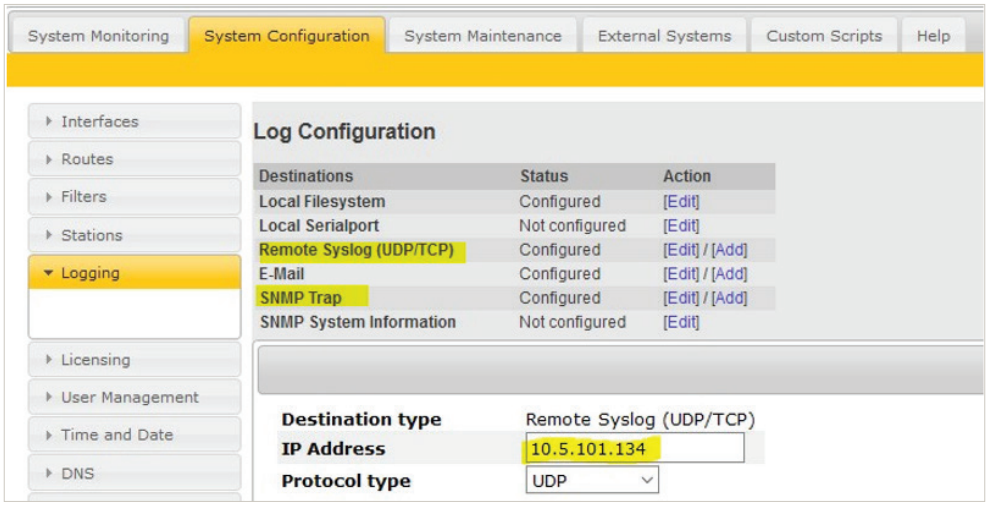
3. Change the default password.

There are two types of passwords: one for read access only and one for read/write access.

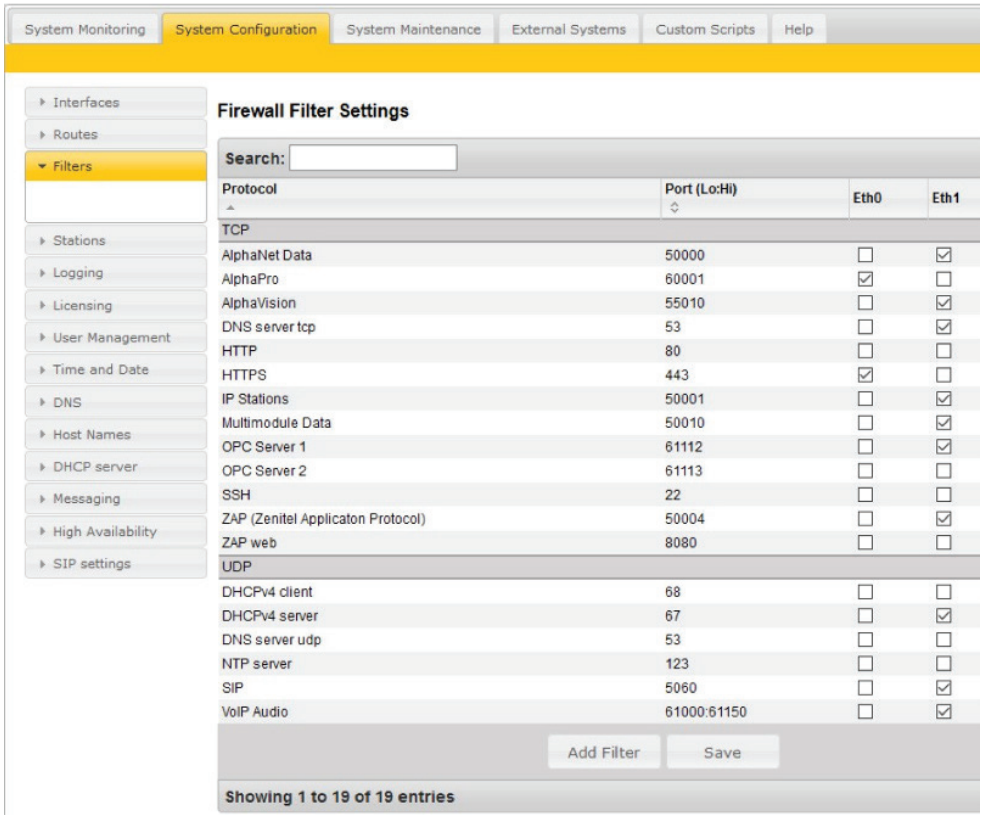


4. Set the NTP server.

ICX-AlphaCom / AlphaCom can synchronize its clock from a NTP server.



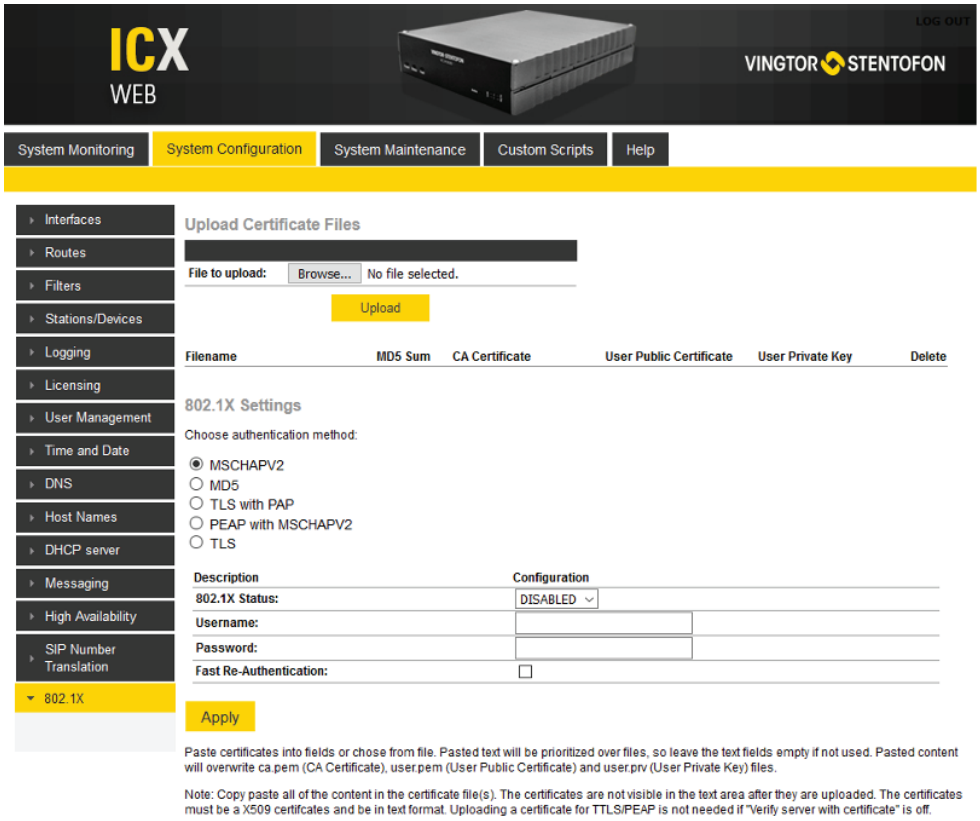
5. Enable SNMP Traps and/or Syslog for monitoring.



6. Verify IP ports and firewall settings.

Make sure all unused ports are disabled.

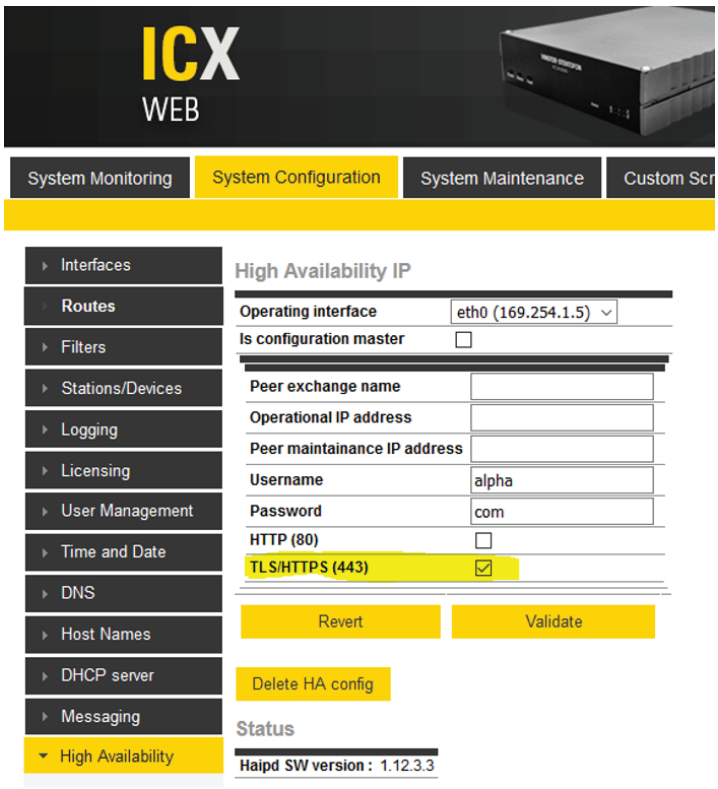
AlphaPro has support for HTTPS (port 443)



ICX-500

7. For ICX only, **Configure 802.1x.**

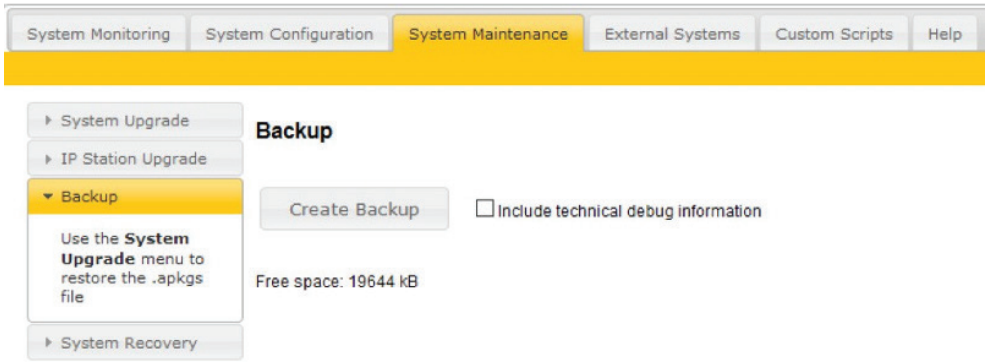
- Configured from System configuration->802.1x.
- Select the desired authentication method.
- Click **Apply.**



ICX-500

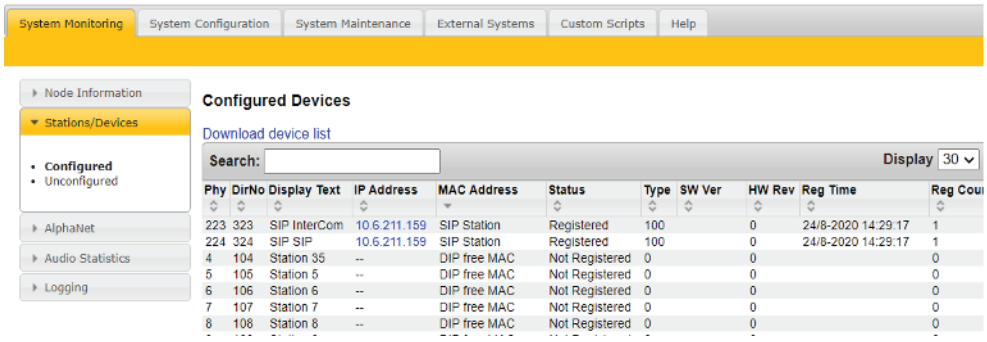
8. For ICX only, **Configure High Availability IP:**

- Configure from **System configuration -> High availability.**
- Check box for TLS/HTTPS (443).
- Click **Validate.**



9. Back up configuration data.

Configuration data is stored on local file on server, as well as to the external PC.



10. Generate system description report.

You can generate a Microsoft Excel report containing all configured devices.

Check

Complete the Cybersecurity checklist

After completing the implementation phase for ensuring the cybersecurity of your system, it is time to check how things are going. To get you started, we've compiled a simple checklist linking the necessary tasks to the relevant CIS Controls.

CIS CONTROL ID	TASK	EXPECTATION	FINDINGS
CIS Control 1: Inventory & control of hardware assets	Review the logs of authorized devices that have accessed the network.	Verify that authorized intercoms have no unplanned network disconnects.	
		Verify that no unknown devices have accessed the network used for physical security.	
CIS Control 2: Inventory and control of software assets	Check the software version of your intercom devices.	Verify that you have the latest production software on Zenitel intercom devices. See release notes at wiki.zenitel.com.	
CIS Control 3: Continuous vulnerability management	Check when the log-in password was last changed.	Evaluate the need to change the password, according to company policy. There should be no critical findings from the vulnerability scan.	
CIS Control 4: Controlled use of administrative privileges	Run a vulnerability scan on the physical security network.	Only current administrators should know the current admin passwords.	
CIS Control 6: Maintenance, monitoring and analysis of audit logs	Review who has access to admin passwords for physical security devices.	Verify that authorized intercoms have no unplanned network/server disconnects.	
CIS Control 9: Limitation and control of network ports, protocols and services	Review SNMP and syslog reports.	Verify that no ports for unused services are open.	

Act

Evaluate and Follow Up

Once you have completed the cybersecurity checklist in the previous stage, you will have a set of findings that will shape your action plan for any necessary follow-up. Review your findings from the checklist and identify the actions needed for each. For example, let's say this is your finding on CIS Control 4:

CIS CONTROL ID	TASK	EXPECTATION	FINDINGS
CIS Control 4: Controlled use of administrative privileges	Review who has access to admin passwords for physical security devices.	Only current administrators know the current admin passwords.	Some former administrators have the current admin passwords.

Naturally, the follow-up action required is to change your admin passwords immediately.

Once you have all the follow-up actions identified, you can more easily prioritize them, evaluate resource needs and work through to completion.

Collecting this information in a structured, consistent way will simplify tracking and make it easier for you to report on your system's cybersecurity health to management on a regular basis.

We hope that this guide will help you to meet your cybersecurity risks head on and ensure that you are maintaining a healthy, robust cyber defense for your systems.

Where to learn more

DOWNLOAD
Our firmware and software is available via our pages:
https://www.zenitel.com/customer-service/wiki-access

GENERAL INFORMATION
We design each of our solutions from the outset with defensibility in mind:
https://www.zenitel.com/cybersecurity/vingtor-stentofon-cybersecurity

CIS (Center for Internet Security) is an independent, non-profit organization with a mission to provide a secure online experience for all:
https://www.cisecurity.org

CUSTOMER SUPPORT
We are available to take your call.
Global: +47 4000 2700
USA: +1 800 654 3140
Email: cs@zenitel.com
Email US: info.usa@zenitel.com

www.zenitel.com

DOC NO.
A100K11771 03/2021

sales@zenitel.com