

 \odot

Cybersecurity Hardening Guide

How to prevent or reduce the impact of security risks.

90

F

FO

5C450

907801

A129A29A12

508500

B2AB

FGEE

v.2.0



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

yber Security	4
Meeting cybersecurity risks head on	4
Defending against cyber attacks	4
Membership with CIS (Center for Internet Security)	4
Developing a strong foundation	5
ybersecurity planning	5
ey buildng blocks	5

Plan

Plan	8
Risk and security levels	8
Security mechanisms	9
CIS CONTROL 4: Controlled use of Administrative Privileges	10
Managing passwords and credentials	10
Tools to manage credentials and passwords	10
CIS CONTROL 9: Limitation and Control of Network Ports, Protocols & Services	11

12 Do Install and set up for cybersecurity.....12 Installation and setup of ICX 500 & AlphaCom XE server for cybersecurity......16 Check 20

Act	21
Evaluate and follow up	

Where to learn more

	Our and Oc	~
Download, General Information, CIS, Customer	SupportZz	2

22



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 accounting environment. The CIS

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 <u>https://www. cisecurity.org/controls/</u>

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.





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:





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.

	aroup	menta:):	lion
CIS CONTROL	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 <u>https://</u> <u>strongpasswordgenerator.com</u>. 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 (<u>http://keepass.info</u>). 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:

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 1 - TCP ports and services

Table	2 -	UDP	ports	and	services
	_		P 0		00111000

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







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:

Search I	P addres	srance		Resolve factory IP address								
an IP ad	dress rar	ge for intercom devices		Default static IP address for d	assic IP stations			0.9	art			
m	10	.6.205.9		Default IP 169.254.1.10								
	10	.6.205.16		Resolve to unique IP address	from range			Clean pro-	evious			
Use de	fault crei	lentials		From 169.254.2.1								
				To 169.254.2.25	5]				
								600 -				
nished.	Found 8	station(s)		Note: This PC must have IP ad	dress 169.254	.1.90.		Factor	Reset			
overed i	P station	ø						with DHC	P			
Stations	Alph	aCom servers										
Select	=	MAC	IP	Туре	Mode	Dir.no.		Software	Hardware	Server	Description	Status
	9 1	00-13-CB-28-01-30	10.6.205.16	Zenitel TCIV i.MX8MM board	Alphacom	116	9	vsff8-6.0.2.2	8801	10.6.211.35		ок
	Θ 2	00-13-CB-0D-2C-A7	10.6.205.15	Vingtor-Stentofon Ex-Panels	Alphacom	115	0	5.1.3.2v3	8511	10.6.211.35		ок
	93	00-13-CB-00-2D-39	10.6.205.14	Vingtor-Stentofon Turbine Ext	Alphacom	114	0	5.1.3.2v3	8124	10.6.211.35		ОК
	94	00-13-CB-08-B7-DE	10.6.205.12	Vingtor-Stentofon Turbine Co	Alphacom	112	0	5.1.3.2v3	8121	10.6.211.35		ок
	9 5	00-13-CB-09-01-1D	10.6.205.11	Vingtor-Stentofon Turbine Co	Alphacom	111	٢	5.1.3.2v3	8121	10.6.211.35		ок
	6	00-13-CB-08-FC-7C	10.6.205.13	Vingtor-Stentofon Turbine Co	Alphacom	113	۲	5.1.3.2v3	8121	10.6.211.35		ОК
	9 7	00-13-CB-06-3A-BD	10.6.205.9	Vingtor-Stentofon Turbine Co	Alphacom	109	0	5.0.3.0	8121	10.6.211.35		ок
M		00-13-CB-06-19-4C	10.6.205.10	Vingtor-Stentofon Turbine Co	Alphecom	110	۲	5.0.3.0	8121	10.6.211.35		OK
9 9	 ● 5 ● 6 ● 7 	00-13-CB-09-01-1D 00-13-CB-08-FC-7C 00-13-CB-06-3A-BD 00-13-CB-06-19-4C	10.6.205.11 10.6.205.13 10.6.205.9	Vingtor-Stentofon Turbine Co Vingtor-Stentofon Turbine Co Vingtor-Stentofon Turbine Co Vingtor-Stentofon Turbine Co	Alphacom Alphacom Alphacom	111 113 109	0	5.1.3.2v3 5.1.3.2v3 5.0.3.0 5.0.3.0	8121 8121 8121 8121	10.6.211.35 10.6.211.35 10.6.211.35 10.6.211.35		0

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.

stat	on Wizard														-	
V	S-IMT						STATION W	IZARD								
ngle C	hange															
	Dasic Settings	s			Authentication			🛉 Upload								
	Р	10.6.205.16	Use C	DHCP	Usemane	admin										
	Subnet mask	255.255.255.1	2													
-	Gateway	10.6.205.1														
4	Mode	Alphacom	-		Password											
	Dir.No.	116			Offine Password	d ++++										
	Server	10.6.211.35														
	Site	Default Ste	-													
cave	ed IP stations			✓ APP	UY											
caves #	ed IP stations	AC	IP	✓ APP IP Type	Туре	Mode	Frontboard	Accessory	Dir.no.	Display text	SIP User	SIP Pass	User	Password	Offline pass.	^
cove #	red IP stations M 1 00-13-CB	MAC 8-28-01-30	IP 10.6.205.16	V APP	Type Zenitel TCIV I.MX	Mode Alphacom	Frontboard Video Normal (Accessory No accessory	Dir.no. 116	Display text	SIP User	SIP Pass	User admin	Password	Offline pass.	Di
cove #	red IP stations M 1 00-13-CB 2 00-13-CB	AAC 8-28-01-30	IP 10.6.205.16 10.6.205.15	V APP	Type Zenitel TCIV i.MX Vingtor-Stentofo	Mode Alphacom Alphacom	Frontboard Video Normal (Accessory No accessory No accessory	Dir.no. 116 115	Display text	SIP User	SIP Pass	User admin admin	Password	Offline pass.	Di
cave #	red IP stations M 1 00-13-C8 2 00-13-C8 3 00-13-C8	AAC 8-28-01-30 1-0D-2C-A7 9-0D-2D-39	IP 10.6.205.16 10.6.205.15 10.6.205.14	V APP IP Type STATIC STATIC STATIC	Type Zenitel TCIV i.MX Vingtor-Stentofo Vingtor-Stentofo	Mode Alphacom Alphacom Alphacom	Frontboard Video Normal (Full Keypad TFI	Accessory No accessory No accessory No accessory	Dir.no. 116 115 114	Display text	SIP User 15 14	SIP Pass	User admin admin admin	Password	Offline pass. vvvv	Di Di Di
	red IP stations M 1 00-13-CB 2 00-13-CB 3 00-13-CB 4 00-13-CB	AAC 8-28-01-30 0D-2C-A7 9-0D-2D-39 8-08-87-DE	IP 10.6.205.16 10.6.205.15 10.6.205.14 10.6.205.12	V APP IP Type STATIC STATIC STATIC STATIC	Type Zenitel TCIV i.MX Vingtor-Stantofa Vingtor-Stantofa Vingtor-Stantofa	Mode Alphacom Alphacom Alphacom	Frontboard Video Normal (Full Keypad TFI Video Scrolling	Accessory No accessory No accessory No accessory No accessory	Dic.no. 116 115 114 112	Display text	SIP User 15 14 55	SIP Pass	User admin admin admin admin	Password	Offline pass. vvvv	Dr Dr Dr Dr
	ed IP stations M 1 00-13-CB 2 00-13-CB 3 00-13-CB 4 00-13-CB 5 00-13-CB	AAC 8-28-01-30 I-0D-2C-A7 I-0D-2D-39 8-08-87-08 8-09-01-1D	IP 10.6.205.16 10.6.205.15 10.6.205.14 10.6.205.12 10.6.205.12	V APP IP Type STATIC STATIC STATIC STATIC STATIC	Type Zenitel TCIV &MS Vingtor Stentofe Vingtor-Stentofe Vingtor-Stentofe	Mode Alphacom Alphacom Alphacom Alphacom	Frontboard Video Normal (Full Keypad TFI Video Scrolling Normal (TCIS-1,	Accessory No accessory No accessory No accessory No accessory No accessory	Dic.no. 116 115 114 112 111	Display text	SIP User 15 14 55 11	SIP Pass	User admin admin admin admin	Password	Offline pass. verr ours Atta	Di Di Di Di
	ed IP stations N 1 00-13-CE 2 00-13-CB 3 00-13-CB 4 00-13-CE 5 00-13-CE	AAC 8-28-01-30 1-0D-2C-A7 1-0D-2D-39 8-08-87-08 8-09-01-1D	IP 10.6.205.16 10.6.205.15 10.6.205.14 10.6.205.12 10.6.205.11	V APP IP Type STATIC STATIC STATIC STATIC STATIC	V Zenitel TCIV SMX Vingtor Stentofe Vingtor Stentofe Vingtor Stentofe	Mode Alphacom Alphacom Alphacom Alphacom	Frontboard Video Normal (Full Keypad TFL., Video Scrolling Normal (TCIS-1,	Accessory No accessory No accessory No accessory No accessory No accessory	Dir.no. 116 115 114 112 111	Display text	SIP User 15 14 55 11	SIP Pass	User admin admin admin admin admin	Password	Offline pass. verv user ttes verv	Dr Dr Dr Dr Dr >
icove	ed IP stations M 1 00-13-CB 2 00-13-CB 3 00-13-CB 4 00-13-CB 5 00-13-CB w all password	AAC 8-28-01-30 1-0D-2C-A7 1-0D-2D-39 8-08-B7-08 8-09-01-1D 8-09-01-1D	IP 10.6.205.16 10.6.205.15 10.6.205.14 10.6.205.12 10.6.205.11	V APP	Y Type Zentel TCIV LNX Vingtor Stantofo Vingtor Stantofo Vingtor Stantofo	Mode Alphacom Alphacom Alphacom Alphacom	Frontboard Video Normal (Full Keypad TFL., Video Scrolling Normal (7CIS-1,	Accessory No accessory No accessory No accessory No accessory	Dicno. 116 115 114 112 111	Display text	SIP User 15 14 55 11	SIP Pass	User admin admin admin admin	Password	Offline pass. verr ssar ssar ssar	Di Di Di Di V
scoves # • • • • • • • • • • • • • • • • • •	ed IP stations	AAC 8-28-01-30 1-0D-2C-A7 1-0D-2D-39 8-08-87-0E 8-09-01-1D ds abons	IP 10.6.205.16 10.6.205.15 10.6.205.12 10.6.205.11	V APP	V Type Zentel TCIV LMX Vingtor Stentofo Vingtor Stentofo Vingtor Stentofo	Mode Alphacom Alphacom Alphacom Alphacom	Frontboard Video Normal (Full Keypad Tfl Video Scrolling Nermal (TCIS-1,	Accessory No accessory No accessory No accessory No accessory	Dir.no. 116 115 114 112 111	Display text	SIP User 15 14 55 11	SIP Pass	User admin admin admin admin	Password	Offline pass. verr ssee ssee	Di Di Di Di Di S

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.

VS-IMT Intercom M	anagar	Teol					CONFIGURA	INN .				Stan	ard Project 08-11-2020
B(+5		IP.	Note	Tape	Dir. No.	Display Name/Text	statun mila			station cettings			
P address 🔹		10.5.9.105	Alpheises	Tailine Video	120		Description	Information		Stater Pode	Nohocee		*
		11.4 104 10	Makazar	Total States	114		PAddress	10.6.0.105		Use Papille Values			- 0
lation type		10.0400.10	represent	Tables Views	110		Subnet Mask	255,255,240.0					
DVCA platform IP station	•	13.6.205.15	Alphecom	Ecipo	115		Default Gateway	10.60.1		Mode Setup			*
Dual capity maters	•	13.6.205.14	Alphacere	Turbine IP station	114		DNS Server 1	10.6.0.2		Schwark Settings			+
Rubre Poleten	0	12.6.205.12	Netacen	Turbine IP contion	112		DNIS Server 2			Alphacen Setting	p.		÷
Tartine Video	6	114 114 11	Makes and	Duckey Dansley	111		MAC Address	00:13xb:28:01:78		Call Settings			*
Route		120.00.11	Aprocom	Arcens in tation	10		Software Weslen	1.040.202011051085		Audio Settinge			÷
Exec Analifer/Controller	•	\$2,6,205,13	Alphacom	Burbline IP station	113		Herdon's Type	8801		Tarte Settings			-
lation made	0	10.6.205.9	Alphecere	Ruthing IP station	109		Hardware Version	1					
Abhecen bd 57		12.6.205.10	distance	Balan Palation	110		Software Components Regions			Linke Helwark Lan	e Photocox		
Ruke (Edge							va edgeaudiochere	0.0 4919 g0m1315 e0		HIP Server		Second and	
Thuse Server / Boge Containter							vs-edgepsi	3.1.0		Select Region		CLINDO	
Logo Printers							vi inp	4.0 2613 g01ex107 r0		Select Zone		London	•
Conferent Planets and							us-manp	1.1-+0		T/O Settings			#
of the second seco							Active Partition	8		Sound Detection			
	1						System Model Name	Wagter Stevioles Tarbine Con	mpact -	RISP Softman			
Xz							Herdward Revision	1		Auto lineaners			4
							10.000	4.19.35-1.1.0+g8507afc3a397	11	Contrast of the local			4
tegistered status <u>Check</u>							Kernel Version	SMP PREEMPT New Apr 27 102 UTC 2020	5057	in the second second			
ontari							Devicetree Venion	01		same settings			
9 Configured							Ecol/Creater ment Version	U-Boot 2019.04		MPIP Settings (2)	W 7)		
0 Uncerfacted							Company and the second	8-5.4 y_v2019104-0228843cdt	13	Howard Sectings			*
9 Adhacom							INTERNAL STREET	4103	v	4			
a Pulse/Fáge							SHS Hert updeted	2020-13-13 10:41:05	Spic.				
a Polie Server / Edge Controler													
								O					
ne .							Owception	Open StationWeb Differmation					
a steering) charged							Site	Default Site *	Change				
LIFLOAD DOSCARD		12 2 2 3					Description		(Provide)		SAVE	🙀 DOSCAR	4

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.

VS-INT ING		0.0 million (Revenue Revenue Annual Annua
	Configure	Nanager			10.01	Distant Security of	CONFIDENT	ION	fratio attract	Stancare Project 08-11-2020
Patirect	VLAN Set	p.,	3000	iyye	Los mo.	USJAY Manor loct	Description	information .	C Caston Maria	Heaven r
	BOZ. DK Set	ap.,	- Aprilant	Tarbine meet			19 Address	10.6.8.105	the second second	- 0
Silvetion type 1	Station Re	HUR.	Aphican	TerDine Trées	- 10		Subret Mask	255,255,240,0	Las reserves values	
2 INCA platform (Pistacia	Options	5	Alphicen	Brigo	115		Default Gateway	10.6.0.1	Made Soliep	14
Ous/Dapley states		10.6.205.14	Aphenes	Turbins IP station	114		UNS Server 1	10.6.0.2	Retwork Settings	
Tuble P station		10.6205.12	Apheners	Tables D dation	112		DNS Server 2		Alphacon Setting	é (d
Turbine Video		10.6 205.14	Abstances	Turbine IR station	-		MAC Address	00:13:rh;28:01:78	Call Softings	4
2 Power							Software Version	1.0.0.202011031036	Andia Settings	
Chigo Ampi Nec/Controler		0.626.0	Apsen	Turbine IP station	110		Hardware Type	8801	Time Settings	6
Station wode	•	10.6.205.8	Alphacem	lurbine IP station	109		Flavoluare Version	1	1/0 Schlargs	4
Z hits (The		10.6.255.10	Alphacam	Turbine IP station	118		Venioss		Sound Detection	4
2 take Server / Crime Control in							vo-edgesudocherit	0.0-4979-plas/375-e9	RTSP Sottings	
toop Strees							va olgogul	3.1 10	Auto Messaes	4
Listfured steam							ve-exp	0.0-2643-g94ms107-r0	Failer Fallery	
2 Configured 🖸 Unconfigured							varvaariiniip	3.1-70	Stand Scould	
following vorsion							Active Patition	8	SHITP SCCORE	
N	-						System Model Name	Vingtor-Stemotas Turbine Compact - Video Plus	IN SHE LAND	n Fayeri Debre Quer
Ste.							Hardware Revision	1		
4							Kernel Version	4.19.35-1.1.0-g8507afc3a397.#1		
depaired status (22	22						Devications Version	OI		
B. Collected							Part Include the Include	U 8eet 2019.04		
6 Linesterad							in a second second second	II-3.4.y_v2019.04-9226043cd15		
							Firmware Service	416/5		
C Colorises							Trip last updated	2020-11-18 10-41-05 Same		
D Index Secure / Filter Could	-							Prop 1 Par and 11 Party Party		
0.52								0		
								2	SHIP Settings (7	<i>(10)</i>
									Dervall Settings	
								\smile		
								41		
							0			
	-							Com Statowillab		
B. at death data and	-						Description	3-formation		
C. State of Cargoo	-						Ste	Default Site * Chang	6.) ·	(1997) (1997)

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.

📀 802.1X Setup									?	×
802.1X Batch S	Setup									
MAC	IP	Туре	Mode	Dir. No.	Sta	atus	Choose authentication met	hod		
00-13-CB-08-FC-7C	10.6.205.13	Mini (TMIS-1, TMIS-2)	Alphacom	113	SYNCED		MSCHAPV2			
00-13-CB-06-19-4C	10.6.205.10	Normal (TCIS-1, TCIS-2, TCIS-3)	Alphacom	110	SYNCED		TTLS with PAP			
00-13-CB-08-B7-DE	10.6.205.12	Video Scrolling Station (TCIV-6)	Alphacom	112	SYNCED		O PEAP with MSCHAPV2			
00-13-CB-28-01-30	10.6.205.16	Video Normal (TCIV-2+, TCIV-3+)	Alphacom	116	SYNCED		0 TLS			
00-13-CB-0D-2D-39	10.6.205.14	Full Keypad TFIE-1	Alphacom	114	SYNCED		802.1X Status	DISABLED		-
00-13-CB-09-01-1D	10.6.205.11	Normal (TCIS-1, TCIS-2, TCIS-3)	Alphacom	111	SYNCED		Username	Username		
00-13-CB-06-3A-BD	10.6.205.9	Kit (TKIS-2)	Alphacom	109	SYNCED		Password	•••••		_
00-13-CB-0D-2C-A7	10.6.205.15	Exigo ATEX Station	Alphacom	115	SYNCED		Fast Re-Authentication			
00-13-CB-28-01-78	10.6.8.106	Video Normal (TCIV-2+, TCIV-3+)	Alphacom	120	SYNCED		Get new DHCP on success			
Select stations, configu Colecting 301: X select Colecting 302: X select 502: X colected from 302: X colected from 302: X colected from 502: X colected from 502: X colected from Syndronization complex	re settings and use from 10.6.205,13 from 10.6.205,10 from 10.6.205,16 from 10.6.205,16 from 10.6.205,16 from 10.6.205,17 from 10.6.205,17 from 10.6.205,15 from 10.6.205,15 d.6.205,16 0.6.205,16 0.6.205,14 0.6.205,11 0.6.205,15 0.6.205,12 0.6	"Save" and "Reboot" but	itors for pushing	; setup.		DEPOST	H o get			
				V SAVE	S S	REBOOT	CLOSE CLOSE			

ADV WEB CC	ANCED				VINGTOR 🔶 STENTO	FON	5a. IEEE802.1x at the End device level
Configuration	Station Administration	Advanced SIP	Advanced Network				Log in to the Web
	802.1X Settings						the device.
(Choose authentication method:						Open the Advanced Network
	EAP-MSCHAPV2						
	C EAP-MD5						tab.
	EAP-TTLS with PAP						 Select the desired
	O PEAP with MSCHAPV2						authentication method
	Description		Configuration				
	802.1X Status:		DISABLED V				 Click on Save, then Reboot.
	Username:		Username				
	Password:		•••••				
	Fast Re-Authentication:						
	Get new DHCP on success:						
			SAVE	REBOOT			

Note: Copy paste all of the content in the certificate file(s). The certificates are **not** visible in the text area after they are uploaded. The certificates must be a X509 certificates and be in text format. Uploading a certificate for TTLS/PEAP is not needed if "Verify server with certificate" is off.

evice.

- the Advanced Network
- t the desired entication method.
- on Save, then Reboot.

Main

▹ SNMP

▼ 802.1X Firewall

SI

He fall Frond Joch	tela												
A VS-IMT Intercom M	-	Teel					CONTROLOGY	100				Standard	Project 08-11-2020
11		IP.	Made	Inst	Die No.	Disting Name/Inst.	Sistematio			Color (All the)			
Paddess .	0	116.8.106	Alabarra.	Turbing Video	100		Description	Informatio		Station Hode	Alphacon		
		The second	- Provide State	TOTAL PROPERTY AND A			IF Address	10.6.8.106		The Dealer Volume			
ation type		MAZAIN	Alphacen	Turbene Video	115		Submet Mask	255,255,240.0		COLOR POLA			
INCA platform IP ctation	9	10.6.253.15	Alphacem	Exigo	115		Default Gateway	10.6.0.1		Hode Setup			4
Dual Display station		10.6.205.14	Alphacen	Turbine P station	116		ONS Server 1	10.6.0.2		Network Settings			۲
Turbine IP station		10.6 25 12	Nakaran	Turbine El starion	117		ONS Server 2			Alphenne Setting	14 C		0
Turbine Video	1						MAC Address	00:13:eb;28:01:78		Coll Settings			÷
Perie		052511	Mpsacore.	Turnine IP station			Software Version	1.0.0.202011051036		Andre Settinos			4
Gogo Amplifer/Cantroller		10.62(513	Nekacom	Turking IP station	113		Hardware Type	8801		Tion Ballins			-
tation mode	9	11.6.205.9	Alphacen	Turbine IP station	109		Hardware Version	1		The second			4
Aphacan 🖂 🖘	6	10.5 25 10	****	Technold Red at the	210		Software Components Vaniana			1/0 Semise			50
Puise / Edge		PARA IN	Aprilation	TOTAL P. HIGHT			vt-edecaudic diert	0.0-4179-00037275-02		Sound Detection			
Puice Server / Edge Cariballer							weekeesi	1.1-0		RTSP Settings			49
i Bogo bil Rowine							V5-230	0.0-2543-g\$4ea107-r0		Audio Hessages			*
angurea colu							vorvoorrep	3.1-0		Syslog Settings			÷
Carrigates (c) uncarrigates							Active Partition	8		STREF Scillings			
1							Sentern Model Nerne	Vingtor-Stendorfon Tarbi	ine Compact -	SINNI Settings (Z	AP]		4
	1						Martine Provides	Video Plus		Frewall Settings			-
	7						marzniak kanalen	4.19.35 1.1.0-08507afc	3,397 #1	00000000000			
Acet arete torateige							Kernel Version	SMP PREEMPT Non Apr	27105057	554 10 -22		Altre	•
uniers							Conduction Version	0102020		HTTP 62 80		Altra	-
9 Configured								U-Boot 2019.04-		HTTPS top 440		Altu	•
0 Unconfigured							BOOVENWICEINER WINDO	# 5.4.y_v2019.04+g228	0-Cledf5	500 top 5866		Alten	*
e alphacon							Firmware Version	416/5		5075 Kp 5051		Albu	
0 Pulse / Edge							Info leak updated	2020-11-18 13:40:05	Svec	DEP top 50001		Allow	-
0. Pulse Server (Edge Controlle	9									Demo 12 50010		Altre	•
0 500								0		AudioData uto S	136	Allow	-
										TTTP Server up	60	Alter	-
								•		SHEP with \$51		Alter	*
										100 000		Altra	
								<u> </u>		Defense INC.		1000	
								3					
												AEN	•
										ULP PS/IDCast 33	00001	Abs	
										Discovery utp 2	0.12	Allow	•
								Open Station/Neb		2AP top 50004		Alton	
et.e							Ceargeon	information		Zep/Web top 8080		Albu	-
0 station(s) changed							Ske	Detail Sta	· Owne				
STROAD DISCARD								-			SAIR	E DISCARD	

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.

n Reni								ST/	ATION WIZARD		
b	Complete report NohaCom directory Pulse directory	Errors and w Alpha Com di Duise directs	varnings irectory 277								
overed	and configured IP station	9									
* . 	MAC 00.12 CR 38.01.20	IP 10 6 305 16	IP Туре стотис) C	Mode	Dir.no.	Software	Display text	Description	
,	00-13-CB-0D-2C-47	10.6.205.15	STATIC	÷		Alphacom	115	S112/3			
3	00-13-CB-08-B7-DE	10.6.205.12	STATIC			Alphacom	112	S.1.3.2v3			
) 4	00-13-CB-0D-2D-39	10.6.205.14	STATIC			Alphacom	114	5.1.3.2v3			
5	00-13-CB-09-01-1D	10.6.205.11	STATIC			Alphacom	111	5.1.3.2v3			
6	00-13-C8-08-FC-7C	10.6.205.13	STATIC			Alphacom	113	5.1.3.2v3			
7	00-13-CB-06-3A-BD	10.6.205.9	STATIC	•		Alphacom	109	S.0.3.0			
8 (00-13-CB-06-19-4C	10.6.205.10	STATIC	•		Alphacom	110	5.0.3.0			
al con	igured:		🥝 в	station	(2)				🔒 0 warning(s)	😮 0 error(s)	

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.

ADVANCED WEB CONFIGURATION

Main SIP Configuration Station Administration Advanced SIP Advanced Network

✓ Account / Call	Account Settings		
► Audio	Description	Configuration	
P Huulo	Name:	PEI 2A]
> DAVC	Number (SIP ID):	124]
Direct Access Keys	Server Domain (SIP):	10.9.8.34	
Relays / Outputs	Backup Domain (SIP):	10.9.8.35]
- neidjo y odipalo	Backup Domain 2 (SIP):]
→ Time	Registration Method:	Parallel ~	
→ I/O	Authentication User Name:	124]
Econthoard Manning	Authentication Password:	•••••]
 Promodard mapping 	Register Interval:	100	(min. 60 seconds)
► RTSP	Register Failure Interval:	60	(min. 5 seconds)
▹ Script	Outbound Proxy [optional]:		Port: 5060
Script Events	Outbound Backup Proxy [optional]:		Port: 5060
P Suprema	Outbound Backup Proxy 2 [optional]:		Port: 5060
 Script Upload 	Outbound Transport:	TLS 🗸	
Audio Messages	SIP Scheme:	sip ∨ Using sips forces all	proxies to also use TLS
htellingst Design	RTP Encryption:	srtp_encryption ~	
Multicast Paging	SRTP Crypto Type:	AES_CM_128_HMAC_SHAT	I_80 ∨
Certificates	Use Unencrypted SRTCP:		
	Verify TLS hostname:		
	TLS Private Key:	turbine_server_sha256.key	~

8. Security in SIP mode (Enddevice 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.

VINGTOR 😽 STENTOFON

• 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+.



COMXE

INGTOR STENTOFO

0

ICX-AlphaCom

VINGTOR.STENTOFON

Active _ 1=1=1

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:

VINGTOR 🔶 STENTOFON		AlphaWeb XE	1. Log in to AlphaWeb. You can log in via HTTP or the
	Secure Login (HTTPS)		secure HTTPS protocol.
	Unsecure Login (HTTP)		

Interfaces	Interfaces			
	Interface	npe_eth0		
Routes	IP Address/prefix	len 10.141.208.200	/20 range:	10.141.208.1 - 10.141.223
Filters	Interface	npe_eth1		
Stations/Devices	IP Address/prefix	clen 10.6.211.37/24	range:	10.6.211.1 - 10.6.211.254
Logging				
Licensing	F	Revert		Validate

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.

ystem Monitoring	System Comiguration	System Maintenance	External Systems	Custom Scripts	Help
▶ Interfaces	User Managen	nent			
Routes		Read	User	Read/Write Us	er
 Filters 	Current User Nam	e alpha		admin	
Stations	Current Password	I			
▶ Logging	New User Name				
> Licensing	New Password				
 User Manageme 	Confirm New Pass	sword			
		Up	date User 1	Update Us	ser 2

3. Change the default password.

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

Interfaces	Time and Dat	te			
Routes					
h. Eilhean	Your Region	Local Ti	me	acombor 2020	12:40:24 CET
Filters	Europerosio	Monuay	onui oi De	ecember 2020	12.49.24 CET
Stations/Devices	Select New R	legion			
Logging	New Region	Select	Your Zor	ne	
Licensing		US	~]	
User Management		Subr	nit		
 Time and Date 					
	Set Localtime	e			
		Date		Time	
DNS	New Date/Time	07.12.2020		12:49:24	
Host Names			_		
DHCP server		Set T	ime		
Messaging	Configure No	twork Time Brot	tocol (N		
s tilsk Australiakilik.	configure Ne	WORK TIME FIO		TF) Server	
Fligh Availability			IP Add	iress	
SIP settings	Configured serv	er IP Address			
	New server IP A	ddress	10.5.	2.29	
				Y	

4. Set the NTP server.

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

ystem Monitoring Sy	stem Configuration	System Maintenance	Extern	al Systems	Custom Scripts	Help
▶ Interfaces	Log Configura	tion				
Routes	Destinations	Ctatus		Anting		
▶ Filters	L ocal Filesystem	Configu	red	(Edif)		
L Chalings	Local Serialport	Not con	figured	[Edit]		
Stations	Remote Syslog (UI	OP/TCP) Configu	red	[Edit] / [Add]		
 Logging 	E-Mail	Configu	red	[Edit] / [Add]		
	SNMP Trap	Configu	red	[Edit] / [Add]		
	SNMP System Info	rmation Not con	figured	[Edit]		
Licensing						
User Management						
▶ Time and Date	Destination	type Remo	te Syslo	g (UDP/TCP)		
	IP Address	10.5.	101.134			
▶ DNS	Protocol typ	UDP	`			

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

▶ Interfaces	Firewall Filter Settings					firewall settings.
Routes						
- Filters	Search:					
	Protocol		Port (Lo:Hi)	EthO	Eth1	Make sure all unused por
	<u>*</u>		\$			are disabled.
Stations	TCP					
Lenging	AlphaNet Data		50000			
Logging	AlphaPro		60001			AlphaPro has support for
► Licensing	AlphaVision		55010			LITTPS (port 442)
User Management	DNS server tcp		53			HTTPS (port 443)
	HTTP		80			
Time and Date	HTTPS		443			
DNS	IP Stations		50001			
Host Names	Multimodule Data		50010			
riust Names	OPC Server 1		61112			
DHCP server	OPC Server 2		61113			
Messaging	SSH		22			
	ZAP (Zenitel Applicaton Protocol)		50004			
High Availability	ZAP web		8080			
SIP settings	UDP					
	DHCPv4 client		68			
	DHCPv4 server		67			
	DNS server udp		53			
	NTP server		123			
	SIP		5060			
	VoIP Audio		61000:61150			
		A 4.4 million				



ICX-500

7. For ICX only, Configure 802.1x.

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

IC) WEB	K		1. j.	44
System Monitoring	System Configuration	Syste	m Maintenance	Custom So
▶ Interfaces	High Availability IP			
Routes	Operating interface	e	th0 (169.254.1.5)	~
▶ Filters	Is configuration master]	
▹ Stations/Devices	Peer exchange name			
▶ Logging	Operational IP address			
▶ Licensing	Peer maintainance IP ad	ldress	aloba	
▶ User Management	Password		com	
▶ Time and Date	HTTP (80)			
→ DNS	TLS/HTTPS (443)			
▶ Host Names	Revert		Validate	
► DHCP server	Delete HA config			
► Messaging	Status			
✓ High Availability	Haipd SW version: 1.12.3	3.3		



8. For ICX only, Configure High Availability IP:

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

System Monitoring Sy	stem Configuration Sys	tem Maintenance	External Systems	Custom Scripts	Help	9. Back up configuration data.		
▶ System Upgrade	Backup					Configuration data is stared		
▶ IP Station Upgrade								
▼ Backup	Create Backup	Include tech	Include technical debug information			as to the external PC.		
Use the System Upgrade menu to restore the .apkgs file	Free space: 19644 kB							
▶ System Recovery								

ystem Monitoring	System Confi	guratio	n System M	laintenance	External Systems	Custom Script	is I	lelp			
▹ Node Informatio	n Co	nfiau	red Devices								
 Stations/Devices 	Dov	unload	I dovico list								
Configured Unconfigured	Se	Search: Display 30 V									
	Phy	DirNo O	Display Text	IP Address	MAC Address	Status ©	Туре ≎	SW Ver	HW Rev	Reg Time	Reg Cou
AlphaNet	223	323	SIP InterCom	10.6.211.159	SIP Station	Registered	100		0	24/8-2020 14:29:17	1
- Aprianae	224	324	SIP SIP	10.6.211.159	SIP Station	Registered	100		0	24/8-2020 14:29:17	1
Audio Statistics	4	104	Station 35		DIP free MAC	Not Registered	0		0		0
	5	105	Station 5		DIP free MAC	Not Registered	0		0		0
Logging	6	106	Station 6		DIP free MAC	Not Registered	0		0		0
	7	107	Station 7		DIP free MAC	Not Registered	0		0		0
	8	108	Station 8		DIP free MAC	Not Registered	0		0		0

10. Generate system description report.

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



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 inter- coms 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 <u>wiki.zenitel.</u> <u>com</u> .	
CIS Control 3: Continuous vulnerability management	Check when the log-in password was last changed.	Evaluate the need to change the password, ac- cording 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 un- used services are open.	



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: +1800 654 3140 Email: cs@zenitel.com Email US: info.usa@zenitel.com

www.zenitel.com

sales@zenitel.com

Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Zenitel, Vingtor-Stentofon and Phontech products are developed and marketed by Zenitel. The company's Quality Assurance System is certified to meet the requirements in NS-EN ISO 9001. Zenitel reserves the right to modify designs and alter specifications without notice. ZENITEL PROPRIETARY. This document and its supplementing elements, contain Zenitel or third party information which is proprietary and confidential. Any disclosure, copying, distribution or use is prohibited, if not otherwise explicitly agreed in writing with Zenitel. Any authorized reproduction, in part or in whole, must include this legend. Zenitel – All rights reserved.