



NERC CIP-003-09 - SECTION 6:

Vendor Electronic Remote Access Security Controls

xonasystems.com © 2023 XONA Systems. All rights reserved. +1 866-849-6629 | info@xonasystems.com



The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are the mandatory security standards that apply to entities that own or manage facilities that are part of the U.S. and Canadian electric power grid.

NERC CIP-003-09 (Cyber Security – Security Management Controls) defines "consistent and sustainable security management controls that establish responsibility and accountability to protect Bulk Electric System (BES) Cyber Systems against compromise that could lead to mis operation or instability in the BES."

This document reflects how **XONA** Systems' Critical System Gateway (CSG) addresses **Section 6** of NERC CIP-003-09 – **Vendor Electronic Remote Access Security Controls.**

6. VENDOR ELECTRONIC REMOTE ACCESS SECURITY CONTROLS6.1. DOCUMENTATION SHOWING6.1.1. STEPS TO PREAUTHORIZE ACCESS.

XONA CSG employs a Zero-Trust model that includes both user authentication and authorization.

Authentication is handled either locally, or via 3rd-party identity providers (IdPs). SAML 2.0 is supported, as is multi-factor authentication (MFA) via a variety of tokens or authenticator apps (e.g., Google Authenticator, Microsoft Authenticator, etc.).

Authorization is done using a 'least privilege' approach that limits access to specific operational technology [OT] assets or industrial control systems [ICS]. That access can be tied to a specific time/day. No lateral movement is possible. An additional level of security can be added by delaying user access until entry is authorized by an administrator.

XONS

	4.3 User Access Control – View Users Menu
The XONA CSG platform utilizes an RBAC (Role-Based Access Control) model which allows you to mable access to specific trusted assets for individual users. This allows you to create connection profiles and assign them to individual users without their knowledge of the underlying technical and automatication-based etails. These concention profiles allow you to:	The XONA CSG platform utilizes an RBAC (Role-Based Access Control) model which allows you to enable access to specific trusted assets for individual users. This allows you to create connection profile and assign them to individual users without their knowledge of the underlying technical and authentication-based details. These connection profiles allow you to:
 Assign specific asset access to each user. 	 Assign specific asset access to each user.
 Permit or deny file transfer capabilities to the user. 	 Permit or deny file transfer capabilities to the user.
 Control the direction of file transfers, if enabled for the user 	 Control the direction of file transfers, if enabled for the user
 Provide an additional layer of security by forcing users into a moderated "wait lobby" before being connected to trusted assets, requiring admin approval. 	 Provide an additional layer of security by forcing users into a moderated "wait lobby" before being connected to trusted assets, requiring admin approval.
To assign access controls, begin by going to View Users under "User Administration" in the side navigation bar. Locate the user's entry and click Edit.	To assign access controls, begin by going to View Users under "User Administration" in the side navigation bar. Locate the user's entry and click Edit.
centrated 🖬 Yes ber	essences. Y Text Des
Using 2044	Childred With Darkane Failure Failure Department and Larlinge Latinge Text Constitute Text
aren 201 aren 201 aren 2014/03/2010 2010 2010/2017 2010/201	
	D Add Connection of 10/14/21/n/6 2010/06/31 @
A Van Connections	A Vee Greedone
Monitor Connections Monitor Connections	Mandar Conventions Mandar Conventions Mandar Conventions
oursameneren frat 11 Lat	una substantia da
Wend Laws	We have
Reference	E feb transform
In the user detail window, scroll down and locate the Connections section. This section provides you with a menu to select specific asset profiles for this user to access:	In the user detail window, scroll down and locate the Connections section. This section provides you with a menu to select specific asset profiles for this user to access:
while a need to select specific asses promos for and use to access.	which is many to believe spectrum above promited for any over to decently.
& Connections	& Connections
Connection Name Protocol Access Permissions File Teamfer Direction Moderated Access	Connection Name Protocol Access Permissions Hile Transfer Direction Moderated Access
CSG Setup sh 🛛 🕱	C36 Setup sub 🕱 🕱
	VM VK X X
VMI VIC IIIIIII	ostimi rop VI VI Book To Host From Host
Image: second	
Vol vel x x one en en en en operation operation en en en	

XONA CSG Administrator Manual v4.0 – Page 54

XONA CSG Administrator Manual v4.0 – Page 56

6.1.2. ALERTS GENERATED BY VENDOR LOG ON

Admins can use the 'Moderated Access' feature to be notified, or view user activity.

Connection Name		4334	/iewing lieere
The name assigned to the asset connection profile		4.3.3 V	lewing users
 This is the entry which is visible to users in the Side Navio 	ration Bar under the Systems menu	The View you to out	/ Users menu, located in the lickly and easily locate and m
- Posterol		you to qu	terry and cashy rocate and h
 Protocol Besteval used for the event connection section BDB SSM 	VDIC or Polen	You shou CSG Ada	.ld become familiar with the ninistrator:
 Protocol used for uns asset connection prome: KDP, 35ri, 	vive or relay.	West Game	
Access Permission		Rin Law Raw	
 Checking this box authorizes this user to access this specification 	ic connection profile.	antage:	10% Of Annual Annua
 File Transfer 		•	
 If a user has been granted access to an asset connection, yo authorize the user for File Transfer operations. Select this is 	su may choose to additionally	70 K	Pendoragaman
 If File Transfer is set to ON, you must specify the direction There are three options: 	a the user is allowed to transfer.	ana juanat anang	On decargonation (Includes)
 From Host - The user is only allowed to transfer files t (i.e., download from). 	from the connection profile host	• MFA	
 To Host - The user is only allowed to transfer files to t unload to) 	he connection profile host (i.e.,	• A	.ccounts marked with a lock Name
 Both - The user is permitted bi-directional File Transfe 	rr (i.e., upload/download) to and	• S	hows you the accounts user l
from the connection profile host.		 Full ? 	Name
For additional information on how File Transfer operates from a User	role, please reference the CSG	o P	rovides you the user's profile
User Manual.		• Emai	rovides you the user's profile
 Moderated Access 		Organ	nization
 When this feature is enabled, users will be forced into a "w concernt to this mention trusted event and the CSC will period 	vait lobby" after attempting to	0 P	rovides you the user's profile
connection request.	ty the administrator of the pending	Role	
Diease Stand Ru	(k) =	0 P	rovides you the user's assign
riedse stand by	connections	o P	rovides you the user's last lo
	Access Requests	Last I	Login Time
User	CI Ma (35	• P	rovides you the user's last ac
view	W1000	Last	Connection Platform Data
· · · · · · · · · · · · · · · · · · ·	Admin View	-	Browser
Administrators have been notified of your access request. Open approvel, you will be redivated to your anneation.	Add Connection	-	Operating System
Canad Request	S. Ver Constitutes Munitor Constructions		Device (Desktop/Mobile)

You to o You sh CSG A	ew Users menu, lo quickly and easily ould become fami dministrator:	cated in the Sid- locate and mana liar with the fiel	e Navigation age all CSG	user acco	er the Use unts.	r Administra	ation section,	allows
You sh CSG A	ould become fami dministrator:	liar with the fiel						
You sh CSG A	ould become fami dministrator:	liar with the fiel	all and the second					
an Uant			us or uns m	ain table a	ind what i	ntormation	ney provide j	you as a
-								
	Lal Note	Tend Address	Ogelides		Lef logit to day	Latings fee	Lad Connection Phillips Bala	
oppine	10% 00 Adversaria		1216-5444	-	10120-03	22-0-0-0002	080	
******	dan serie	antiquestances	of series	-	-	2010/01/02	080	
				-	00120-240	10-0-0-032	000	
701		Tendomerson	17.0e	an .	100910	22-2-2-122		
			(Last	-	10000	20010-0-0200	000	
inguma .						PR	ALC: NOT OF THE OWNER.	
	(ins highligh	(none@inseptembre	(Proprieting	reny	114	Pre	new ingestion	
- Lm	Provides you the	user's profile er	nail address	entry.				
 Org 	ganization							
• Org o	<mark>ganization</mark> Provides you the	user's profile or	ganization e	ntry.				
• Org • • Rol	<mark>ganization</mark> Provides you the le	user's profile or	ganization e	ntry.				
• Org • Rol • Rol	<mark>ganization</mark> Provides you the le Provides you the	user's profile or user's assigned	ganization e role (<i>user, p</i>	ntry. ower, adv	nin, file tr	ansfer, ram	or monitor).	
Org O Org Org	ganization Provides you the le Provides you the at Login Location	user's profile or user's assigned	ganization e role (<i>usør, p</i>	ntry. ower, adv	nin, file tr	ransfer, ram	or monitor).	
Org O	ganization Provides you the le Provides you the at Login Location Provides you the	user's profile or user's assigned user's last login	ganization e role (<i>usør, p</i> IP address o	ntry. ower, adi entry (and	nin, file tr l optionall	ransfer, ram ly if enabled	or monitor). their geo-loc	ation).
Org Org Org Org Org Org Ias O Las O	provides you the le Provides you the at Login Location Provides you the at Login Time	user's profile or user's assigned user's last login	ganization e role (<i>usør, p</i> IP address e	ntry. ower, adr entry (and	<i>nin, file tr</i> l optionall	ransfør, rann ly if enabled	or monttor). their geo-loc	ation).
Org Org Org Org Org O Rol O Las O Las O	provides you the le Provides you the at Login Location Provides you the at Login Time Provides you the	user's profile or user's assigned user's last login user's last acces	ganization e role (<i>user, p</i> IP address o s time to the	ntry. ower, add entry (and cSG.	nin, file tr l optionall	ransfer, ram ly if enabled	or monitor). their geo-loc	ation).
Org Org Org Org Org O Rol O Las O Las O Las O	provides you the le Provides you the at Login Location Provides you the at Login Time Provides you the t Connection Plat	user's profile or user's assigned user's last login user's last acces form Data	ganization e role (<i>usør, p</i> IP address e is time to the	ntry. ow <i>er, adı</i> entry (and cSG.	nin, file tr I optionall	ransfer, ram ly if enabled	or monttor). their geo-loc	ation).
Org Org Org Org Nol O Las O Las O Las O Las O	provides you the le Provides you the at Login Location Provides you the at Login Time Provides you the at Connection Plat Provides you the	user's profile or user's assigned user's last login user's last acces form Data user's connectie	ganization e role (<i>user, p</i> IP address e is time to the	ntry. ower, adv entry (and cCSG. including	nin, file tr l optionall	ransfer, ram	or monttor). their geo-loc	ation).
Org Org Rol O Rol O Las O Las O Las O Las O	provides you the le Provides you the at Login Location Provides you the at Login Time Provides you the at Connection Plat Provides you the Browser	user's profile or user's assigned user's last login user's last acces form Data user's connectic	ganization e role (<i>user, p</i> IP address e s time to the on meta data	ntry. <i>ower, adı</i> entry (and e CSG. includinş	ntn, file tr I optionall 3	ransfør, ram ly if enabled	or monitor). their geo-loc	ation).
Org Org Org Org O Ias O Las O Las O	provides you the le Provides you the t Login Location Provides you the t Login Time Provides you the t Connection Plat Provides you the Browser Concretion State	user's profile or user's assigned user's last login user's last acces form Data user's connectio stem	ganization e role (<i>user, p</i> IP address e is time to the on meta data	ntry. <i>ower, adı</i> entry (and e CSG. includinş	nin, file tr l optionall g:	ransfer, ram ly if enabled	or monttor). their geo-loc	ation).

XONA CSG Administrator Manual v4.0 – Page 60

6.1.3. SESSION MONITORING

XODS

User sessions can be monitored by two role types: 'Administrator' and 'Monitor'.



XONA CSG Administrator Manual v4.0 – Page 28





XONA CSG Administrator Manual v4.0 - Page 27

.....

хопа

6.1.4. SECURITY INFORMATION MANAGEMENT LOGGING ALERTS:

XONA CSG captures data regarding activity tied to the XONA CSG and user connection history. This data can be output in a variety of formats including Splunk, RSyslog, and Generic HTTP.

The L	
	ogs section contains the menu items associated with two sets of forensic information:
•	Gateway Logs
	 All actions taken on a CSG platform are logged.
	 The individual log entries include:
	 Login/Logout events
	Connection Start/Stop events
	 File Transfer requests and actions
	 Administrative actions
	Date of event
	Connection History
	 Connection meta-data including:
	 Use of MFA, for both User and MFA-enabled connections
	 Start/Stop time.
	 Connection logs (protocol specific)
	 Screen shot of display.
	 Connection Recording (if configured, see Setup and Configuration section)
The G are ret They o The G	ateway Logis menu displays the most recent log entries generated on the CSG platform. These logs and within the CSG, or they can be forwarded to any syslog type server for analysis and storage. an also be forwarded to a XONA ROAM centralized management platform. ateway log fields include:
	Los Name
	 The User Name (or message system or internally generated events) which created the action
	o The order states (or measure system or meeting) generated events) which created the action.
•	- The senarel esterony of the spart either CATERIAN EVENT or LOCIN' DURANT
	 The general category of the event, entire GATEWAT_EVENT of LOGIN_EVENT
•	Description
	 A detailed description of the event itself. This includes information such as User Name, Connection Name, and a general Event Description of what occurred.
•	Date
	 The date time stamp of when the action occurred
	o The date line stamp of when the action occurred.

XONA CSG Administrator Manual v4.0 – Page 64



XONA CSG Administrator Manual v4.0 – Page 65



XONA CSG Administrator Manual v4.0 - Page 83



6.1.5. TIME OF NEED SESSION INITIATION

User access can be augmented with time and date controls - either specific times and dates, or ranges.

4.0.44 Harry Times	A		
4.2.11 User Time	Access windows		
Additional security provis date-based windows.	led by the CSG platform tailors user access even furth	er by enforcing time	e and
These granular controls a specific dates, and the op	low the CSG Admin to restrict users to specific period ion to setup reoccurring windows of CSG access.	is of times of day,	
Locate the Access Windo Edit.	w section by going to View Users, selecting an individ	lual user and clickir	ıg
Access Window Date	OFF If "Off", user account will be allowed to login at any date.		
O Access Window Time	OFF If "Off", user account will be allowed to login at any time.		
User Time Zone	(UTC-05:00) America/New_York	•	0
Time Zone 4.2.12 Access Wi	ndow Date		
Time Zone 4.2.12 Access Wi Access Window Date con a limited time frame with	ndow Date trol allows you to select a "From" and "To" date inter which an authenticated user is allowed to use their CS	val from which to p G account. Commo	rovide n use
Time Zone Access Window Date con a limited time frame with cases for Access Window Temporary contri	ndow Date trol allows you to select a "From" and "To" date inter which an authenticated user is allowed to use their CS Date include: er workerd	val from which to p G account. Commo	rovide n use
Time Zone Access Window Date con a limited time frame with cases for Access Window Temporary contra 3 rd Party access	ndow Date trol allows you to select a "From" and "To" date inter Valech an authenticated user is allowed to use their CS Date include: ct workers]	val from which to p G account. Commo	rovide m use
Time Zone Access Window Date con a limited time frame with cases for Access Window Temporary contra 3 rd party access Traveling employ	ndow Date trol allows you to select a "Frem" and "To" date inter Which an authenticated user is allowed to use their CS Date include: ct workers ees	val from which to p G account. Commo	rovide n use
 Time Zone 4.2.12 Access Wi Access Window Date con a limited time frame with cases for Access Window Temporary contri 3 ³⁴ Party access Traveling employ 	ndow Date trol allows you to select a "From" and "To" date inter Valch an anthemicated user is allowed to use their CS Date include: et worker] ees	val from which to p G account. Commo	rovide m use
Time Zone Tenne Zone Series Series	ndow Date for allows you to select a "From" and "To" date inter which an authenticated user is allowed to use their CS Date include: ct workers] ees	val from which to p G account. Commo	rovide n use
Time Zone the Xaccess Wildow Access Window Late of the Access Window a cases for Access Window Temporary contra S ⁴⁷ Party access Traveling employ	ndow Date fool allows you to select a "From" and "To" date inter which an authenticated user is allowed to use their CS Date include: et worken] ees	val from which to p	rovide n use

XONA CS	G Administrator	Manual v4.0	– Page 45

Access Window	v Date on it "Off", user	account will be allowed to login at any date.		
	Select Date Ran	ge 02/01/2019 - 03/01/2019		m
Confirm these dates be	efore continuing.	account will be allowed to login at any time.		
User Time Zone	(UTC-05:00) A	merica/New_York	¢	•
Primary Authent	tication Active Director	у	•	•
XONA				
Idap://192.168.1	.10:389			
MFA enabled	0++) if "Off", user	account will only use primary authentication.		
& Connections				_
Connection Nat	me Protocol	Access Permissions File Transfer	Dire	ction
Moxa Relay	relay			
			_	_
New Password	Enter Password			-
Re-Type Passwo	ord Enter Password			*
	6	Change Password		
			-	

XONA CSG Administrator Manual v4.0 – Page 47

Select Date Range 02/01/2019 - 02/0 O Access Window Time Fe 2019 Select the Date Range by clicking the window, calendar will appear r 40 0 10 11 2 13 41 5 0 9 2 2 2 3 0 9 10 11 2 13 44 15 41 7 9 2 2 2 1 10 10 20 2 2 2 1 1 9 2 2 2 1	1/2019 N U Mo Tu 4 25 28	lar 2019 We Th	> Fr Sa	Ö
O Access Window Time Feb 2019 use Frequency Select the Date Range by Clicking Frequency Select the Window, calendar will appear use Select the Date Range by Clicking Frequency Select the Select the Window, calendar will appear use 0 11 12 13 14 15 use 10 11 12 13 14 15 15	Mo Tu 4 25 26	lar 2019 We Th	> Fr Sa	
Select the Date Range by clicking ut this window, calendar will appear 10 11 10 11 10 11 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 10 12 11 12 12 22 13 14 14 15 15 14 16 11 17 19 19 20 21 22 22 22 23 11	4 25 26	we m	ri aa	
10 11 12 13 14 15 16 10 17 18 19 20 21 22 23 11		27 28	1 2	0
10 11 12 13 14 15 16 10 17 18 19 20 21 22 23 11	5 4 5	6 7	8 9	
· · · · · ·	0 11 12 7 18 19	13 14 20 21	15 16 22 23	-
Select the start date and end date 28 27 28 1 2 24	4 25 26	27 28	29 30	
by clicking the days on the calendar 5 6 7 8 9 3	1 1 2	3 4	5 6	
ldap://192.168.1.10:389 02/01/2019	9 - 02/01/2019	Cancel	Apply	
Finally, click Apply to enable the date range.	yin at any date			
Select Date Range 02/01/2019 - 03/0	01/2019			m
The Date Range will update. Confirm				
these dates before containing.				

XONA CSG Administrator Manual v4.0 – Page 46

Jsers can be ass diting an existir ccess. Time slo lates.	igned reoccurring : 1g user, the admini 1s can also be conf	access windows with repeating date/time in strator can select specific days of the week	tervals. When a to permit CSG	dding or Dashboard
diting an existir iccess. Time slot lates.	ig user, the admini is can also be conf	strator can select specific days of the week	to permit CSG	Dashboard
lates.		igured for those specific days. The adminis	trator sets the st	art and end
	Access Window Date	TOP: user account will be allowed to login at any date.		
		Select Date Range 2021/06/30 - 2021/06/30	•	
	O Access Window Time	TOP, user account will be allowed to login at any time.		
	Scheduled Recouring Ar	coess Days on		
	C Select The Desired Days			
	View Even	The caer will only have access on the days of the week that are selected above.		
	a reserve topic			
	User Time Zone	(UTC-05:00) America/New_York	v 0	
Optionally the a When selected,	User Time Zone dmin can set this s the admin will sele	ARC4000 America/New,Yek erries to never expire by clicking on the "N ect a "start" date for this access window.	v 🛛	rameter.
Optionally the a When selected,	User Time Zone dmin can set this s the admin will sele diffecess Window Date	erries to never expire by clicking on the "N et a "start" date for this access window.	v 🛛	rameter.
Optionally the a When selected,	user Terre Zone dmin can set this s the admin will sele Access Window Date	eries to never expire by clicking on the "N exists to server expire by clicking on the "N ext a "start" date for this access window.	ever Expire" par	rameter.
Optionally the a When selected,	user Terre Zone dmin can set this s the admin will sele Access Window Date	eries to never expire by clicking on the "N eries to never expire by clicking on the "N ext a "start" date for this access window.	v e ever Expire" par	rameter.
Optionally the a When selected,	User Time Zone domin Can set this s the admin will sole Access Window Date O Access Window Time	artis to never expire by clicking on the "N tat a "star" due for this access vindow.	ever Expire" par	rameter.
Optionally the a When selected,	User Time Zone domin can set this s the admin will sole discuss Window Tate o Access Window Time dischedded Reccuring	eries to never expire by clicking on the "N exists to answer expire by clicking on the "N exist" and "due this access window.	v e ever Expire" par	rameter.
Optionally the a When selected,	User Time Zone domin can set this s the admin will sold different window Date O Access Window Time different different different C Salect The Desired Day	Collections and the second sec	v e ever Expire" par	rameter.
Optionally the a When selected,	User Time Zone domin can set this s the admin will seld admin will seld admin will seld admin will seld admin will seld admin will seld admin admin admin will seld admin admin admin will seld admin	And the construction of th	v v	rameter.
Optionally the a When selected,	User Time Zone dmin can set this s the admin will sele Access Window Date Access Window Time d Science Swindow Time d Sc	C C C C C C C C C C C C C C C C C C C	v e	rameter.
Optionally the a When selected,	User Time Zone	Collections on every expire by clicking on the "N exist is on every expire by clicking on the "N exist a "start" data for this access violation.	ver Expire" par	rameter.

хопа

Access Window Time co	ntrol allows you to sele	ct a "From" and "To" time interval from wh	ich to
Common use cases for A	ccess Window Time in	clude:	count.
 Limited access to 	critical assets		
 Security controls 	enforcing work schedu	ale access.	
 Location (Time 2 	lone) based access auth	orization.	
To enable Access Windo	w <u>Time</u> click the option	a to the ON position:	
O Access Window Time	ON H=0ff", user acc	 Click Access Window Time to ON position 	n
	Select Time Range	00:00:00 - 23:59:59	0
Range window, clock wil	annear 00) Ame	ri 0 ¢ ; 00 ¢ _23 ¢ ; 59 ¢	0 0
start fine followed by	the End fille		
Click Apply to enat	lethe lime interval.		
O Access Window Time	ON If "Off", user acco	ount will be allowed to login at any time.	
O Access Window Time	ON H "Off", user acco	sunt will be allowed to login at any time. 09:00:00 - 17:00:00	Ø
© Access Window Time The Time Interval will u the time period befor	ON If "Off", user acco Select Time Range pdate. Confirm	sort will be allowed to login at any time.	0
© Access Window Time The Time Interval will u the time period befor	ON If "Off", user according to the second	ourt will be allowed to login at any time.	0
© Access Window Time The Time Interval will ut the time period before	ori II "0ff", user acco Select Time Range pdate. Confirm re continuing.	ourt will be allowed to login at any time.	0

XONA CSG Administrator Manual v4.0 – Page 49

6.1.6. SESSION RECORDING

Sessions connecting to OT/ICS asset can be recorded if they use either the RDP, SSH, or VNC protocols.

Internal before continuing0000) America.New, York Primary Authentication Active Directory Activ		Select '	Time Range	09:00:00 - 17:00	:00		0
Primary Authentication Active Directory B XOHA	ime interval before	continuing.	05:00) Ame	rica/New_York		•	0
Primary Mutantication Active Directory E XONA	-						
XONA Stage://2016.10.389 WTA stabled Image: Connections Connections Connections Image: Connections	Primary Authentica	ition Active	Directory			•	-
Hap: (1992, 19.1.10. 309 WA enabled Image: Constraints Constraints Max Intry Image: Constraints	XONA						
Unit multiply in the second of	Idap://192.168.1.10	-389					
Connection	MPA enabled	000	-Ort", user acc	ount will only use prima	y authentication.		_
Connection team of the framework of the	& Connections						
Vers May New Destination of the Passmond.	Connection Name	Protocol		Access Permissions	File Transfer	Dire	etion
Detex User Cone San charges	New Password Re-Type Password	Enter Passwor	rd rd	hange Pässword			*
					Delete User Clos	e Save cl	hanges

XONA CSG Administrator Manual v4.0 – Page 50

6124 Session	Recording
0.1.2.4 00351011	
The CSG defaults to re-	ord user sessions for the following connection types:
 RDP 	
 VNC 	
 SSH 	
The recording remains a or until the disk space re	stored in RAW format according to the log retention settings (see Log Management) eaches over 90% usage.
If user session recording	g is not required, you may choose to disable it.
Main Server *	Gateway * Services * Security * MFA * File Share * System *
	Appliance Status
	DATEWAY / SESSION RECORDING
	Log Forwarding
	Session Recording
enable-recording	ON Record user session in RDP, VNC and SSH based protocols.
Set "enable-recording" feature by switching to	to ON to start user session recording. At any time, the administrator can disable this OFF.

XONA CSG Administrator Manual v4.0 - Page 91



6.1.7. SYSTEM LOGS

XONA CSG captures data regarding both the XONA CSG and user connection history.



6.1.8. OTHER OPERATIONAL, PROCEDURAL, OR TECHNICAL CONTROLS

The **XONA** CSG supports a variety of controls focused on providing a zero-trust approach to secure user access.

	CSG Version 4.0
5.0 <mark>L(</mark>	OGS
The Log	s section contains the menu items associated with two sets of forensic information:
	Gateway Logs
	 All actions taken on a CSG platform are logged.
	 The individual log entries include:
	 Login/Logout events
	 Connection Start/Stop events.
	 File Transfer requests and actions
	 Administrative actions
	Date of event
	Connection History
	 Connection meta-data including:
	 Use of MFA, for both User and MFA-enabled connections
	 Start/Stop time.
	 Connection logs (protocol specific)
	 Screen shot of display.
	 Connection Recording (if configured, see Setup and Configuration section)
5.1 G	ateway Logs
The Gat are retai They ca The Gat	eway Logs mems displays the most recent log entries generated on the CSG platform. These logs and within the CSG, or they can be forwarded to any syslog type server for analysis and storage. and be forwarded to a XDNA ROAM centralized management platform. eway log fields include:
•	User Name
	 The User Name (or message system or internally generated events) which created the action.
•	Category
	 The general category of the event, either GATEWAY_EVENT or LOGIN_EVENT
•	Description
	 A detailed description of the event itself. This includes information such as User Name, Connection Name, and a general Event Description of what occurred.
•	Date
	 The date time stamp of when the action occurred.

XONA CSG Administrator Manual v4.0 – Page 64

				CSG Version 4.0
O Generate				
-			Terrora .	
04,05764	satisfaction .	the local strap series		10-3.5 MP
Capitre .		de logent agrund antiquemble suid le unique fai and le	that with.	
100715	Latera John	where a party provide what is an other than to an upper		20.44.024
100710	within JAM	the ways of the second state of the second state of the second state		
4875	Lating Adv	Lagrandering and another provide the Article of States		
06,0004	201,001	are report in the solution and the solution.		22-8.8 (216)
1011	201,041	Lage Allerando per Lancing, Allerand Dave P. 12(2) (1)		20-818-0188
1000	64564.367	The second in our particular and an input of		ALC: ALC: STREET
Append .	Latina (AA)	Annual strategy and a light to be a second or super-		10-10-0-10 20-10-0-10
1000		Greater for sense arrange (FT answers, and against		
Lang strongers (tad manage	Antistic and	
he availab	le filters in Filt	er By Log Category 🗸	none	Logs by choosing one of
he availab	le filters in Filt	the lower drop down select er By Log Category	none GATEWAY_EVENT LOGIN_EVENT	Logs by choosing one of
 Fil o o 	Filt Filt Filt Filt Specify e LOGIN_ Suco Suco Suco Faile Sessi Time GATEW. User Conz File t	the lower drop down select er By Log Category Category the LOOKIN SYENT or GG VENT category allows you soful hopin. Soful	house: Tono CATEWAY EVENT CATEWAY EVENT ID GORLEVENT to view: in attempts (usuathercerd). d. d. deleted. d. deleted.	cog ny choosing one of

XONA CSG Administrator Manual v4.0 – Page 65

xona

6.2. DOCUMENTATION SHOWING

6.2.1. DISABLING VENDOR ELECTRONIC REMOTE ACCESS USER OR SYSTEM ACCOUNTS

XONA CSG's 'Lockbox' feature enables administrators to logically disable access for all users to the CSG. In addition, access can be revoked on a user-by-user basis.

The Lockbox feature all	ows the administrator	r or RAM (Remote Access Ma	anager) to:
 Logically disable 	e all users access to t	he CSG.	
 Physically disat 	le Untrusted or Trust	ed Ethernet ports on the CSG.	
 Permit or deny : 	administrative access	from the Untrusted interface.	
During times of mainter operate critical devices t NOT access critical asse	ance or repairs is it c hat could injure local its on the trusted OT i	rucial that remote users are blo plant personnel. This procedu network.	ocked from being able to remotely are ensures that remote users CAN
10	in Server* Gateway* Se	rvices * Security * Milk * File Share *	Bysham *
	Alter user lag	pins - Toppie to enable/disable user access to CSD temporarily.	
	Con Contrusted into	erface status- Topple to enable/disable Unit-solid interface or	C80.
	Trushed Interf	lace status - Toggle to enablicitioable Trusted interface on CSD	
	Untrusted Adv	min Access - Toggle to allow admin access to the CSG while on	
Default settings are disp	layed above. Click ea	ach switch to enable/disable th	e feature:
Allow user login login, authentic: administrators a	ns – When ON, all CS ate and create connec nd RAM users are pe	SG user accounts have access t tions to assets assigned to their mitted to log in to the CSG d	to the CSG dashboard and can r profile. When OFF, only ashboard.
 Untrusted Interf interface is physical 	ace Status – When O sically disabled and E	N, the untrusted interface is en themet link is dropped.	abled. When OFF the untrusted
 Trusted Interfac 	e Status – When ON, abled and Ethernet li	, the trusted interface is enable nk is dropped.	d. When OFF the trusted interface
is physically dis	n Access – When ON	 admin access is available fro Untrusted interface. 	om the Untrusted interface. When
is physically dis Untrusted Admi OFF, admin acc	ess is restricted from		
is physically dis Untrusted Admi OFF, admin acc Be aware of how the dashboard fi	ess is restricted from v you connect to the (rom before using thes	CSG dashboard and know for s e commands. It is possible to l	sure which port you are accessing lock yourself out of the CSG.

XONA CSG Administrator Manual v4.0 – Page 2

4.2.16 Disa	abling Account Acce	ess	
As mentioned i	n the Adding Users section, al	I new user accounts are set to "	'Disabled'' by default. To
 Click o 	n View Users under User Adn	ninistration and look for User ?	Names in RED.
 Hoveria 	ng over the name in RED will	show you a message regarding	their status.
- 03615	win receive a message on logi	in attempts that their account is	disabled.
	📽 View Users		
	MFA User Name	Full Name	Emi
	0		
	csgadmin	XONA Disabled acc	ounts will be in RED
	user	This account is curren	ntly disabled. c
	Your account is our	rently disabled or M	
	expired. Please cor	ntact your	
	organization admin	istrator.	
Users atte with a dis	mpting to login into a CSG abled account will receive		
this messa	ige.		





xona

6.2.2. DISABLING INBOUND AND/ OR OUTBOUND HARDWARE OR SOFTWARE PORTS, SERVICES, OR ACCESS PERMISSIONS ON APPLICATIONS, FIREWALL, IDS/ IPS, ROUTER, SWITCH, VPN, REMOTE DESKTOP, REMOTE CONTROL, OR OTHER HARDWARE OR SOFTWARE USED FOR PROVIDING VENDOR ELECTRONIC REMOTE ACCESS.

The **XONA** CSG is a purpose-built standalone appliance. User sessions can be immediately terminated using the 'Kill Button'. Inbound/outbound ports can be disabled using the 'Lockbox' function or admins.



XONA CSG Administrator Manual v4.0 – Page 27



XONA CSG Administrator Manual v4.0 – Page 96



XONA CSG Configuration Manual – Software v4.0 – Page 29



THE REAL PARTY OF A DESCRIPTION OF A DES	станала и нала и на	re data and provide gener.
Constant and the second s	- D X Sector of Control of Control Sector Sector Sector Sector (Control of Control of Control (Control of Control (Control of Control (C	- 0 X -
TOTAL AND ADDRESS	Destro de desta elos e elos termenos en el el post- to destale?	Tealls of dividie area a CO drug alores vi a col drug alores vi di poti dividie dividie Dr
Transfer and the second	Control t post. # smabled. t to disable? <not< td=""><td>trol t port. nabled. disable7</td></not<>	trol t port. nabled. disable7
	t to disable? <no></no>	diseble? No>
	<no></no>	No>
gildust ENTERIDens Arrownikowe Taka Swisch Kons y		
	switch Menu	itch Menu
		itch Meno
	: Switch Ne	itch Me

XONA CSG Configuration Manual – Software v4.0 – Page 30

6.2.3. DISABLING COMMUNICATIONS PROTOCOLS (SUCH AS IP) USED FOR SYSTEMS.

The **'Edit Connection'** feature can be used to disable communications protocols such as RDP, SSH, etc.

The View Connections menu	i item located under the Manage Connections se	ection of the Side Navigation
Bar allows you to see existin	g conligured connections as well as modify the	ii settings.
814 Balland	Randarilan Nana	
4 55	OSI Desitiva	010
10	Rost Laphap	
104	Windows W Devicing Upunto Devicing	
10.41	Sume 10P Reay	
The menu for the View Conr	sections table contains the following entries:	
 MFA 		
 If the connection 	n is "MFA-enabled" you will see the lock (🚔)	icon.
 Note: For more i Security section 	information on "MFA-enabled" connections see below.	the Additional Connection
 Protocol 		
 The configured ; 	protocol for the connection	
 Connection Name 		
- The name setting	a for the connection	
n l'an a	ior ale connection.	
 Edit Button 	22 2 2 2 2 2	
 Single button to 	modify the connection settings.	
3.3.1 Edit Connecti	on	
Once a connection has been	configured, you have the opportunity at any tim	e to:
 Modify the previous 	connection-specific settings.	
 Enable additional set 	curity settings for a connection.	
To modify a connection, loca dialogue window will enable	ate the profile row in View Connections and clic you to further modify the connection settings.	ek Edit. A protocol specific
For explanations of specific p Connection section.	protocol parameters refer to the individual conn	ection settings section in Add

XONA CSG Administrator Manual v4.0 – Page 24

xona

6.2.4. REMOVING PHYSICAL LAYER CONNECTIVITY (E.G., DISCONNECT AN ETHERNET CABLE, POWER DOWN EQUIPMENT)

XONA CSG's 'Lockbox' feature can be used to 1) logically disable all users access to the CSG, or 2) physically disable untrusted or trusted Ethernet ports on the CSG.

6.2.5. ADMINISTRATIVE CONTROL DOCUMENTATION LISTING THE METHODS, STEPS, OR SYSTEMS USED TO DISABLE VENDOR FLECTRONIC REMOTE ACCESS.

XONA CSG's **'Lockbox'** feature enables administrators to logically disable access for all users to the CSG. In addition, access can be revoked on a user-by-user basis.



XONA CSG Administrator Manual v4.0 - Page 96



XONA CSG Administrator Manual v4.0 - Page 2

хопа

10 46 Dischling Account Access		4.3.1 User Access Control & Role Modification	
4.2.10 Disabiling Account Access		The administrator is free to enable or restrict access to assets as requi	red. The changes made here are
As mentioned in the Adding Users section, all new user accounts are set to "Disabled" identify disabled accounts:	'by default. To	immediately propagated throughout the CSG platform.	
Click on View Users under User Administration and look for User Names in I	RED.	Additionally, the administrator may grant (either temporarily or pern user's CSG role by modifying the entry.	anently) additional privileges to a
 Novering over the name in KED will show you a message regarding their state User's will receive a message on login attempts that their account is disabled. 	25.	Locate the user's account entry under View Users, click Edit and fin	the Role setting:
🗑 View Users		Letit User	
MFA User Name Fuli Name	Emi	User Name poweruser	*
		Full Name Power User	4
csgadmin XONA Disabled accounts will	be in RED	Email poweruser@xonasystems.com	3
user This account is currently disabled	d. c	Organization Xona Systems Modify th	e user's role at any dick "Save Changes"
		Role power	۵ ۵
Uses structure to a SSG		and connection based).	
this message.			

6.2.6. OTHER OPERATIONAL, PROCEDURAL, OR TECHNICAL CONTROLS.

The XONA CSG supports a variety of controls focused on providing a zero-trust approach to secure user access.

XONA CSG	
ADMINISTRATOR MANUAL	
TABLE OF CONTENTS	
TABLE OF CONTENTS	1
1.0 GETTING STARTED	
1.1 XONA Critical System Gateway (CSG) Administration Overview	
1.2 Points of Contact	
1.2.1 Help Desk and Support	
1.3 Did you perform the Initial CSG Setup?	
1.4 Acronyms and Abbreviations	
2.0 ADMINISTRATION USER INTERFACE (UI)	
2.1 Administration UI Overview	
3.0 MANAGE CONNECTIONS	
3.1 Managing Asset Connections	
3.2 Add Connection	
3.2.1 RDP Connection Settings	
3.2.2 VNC Connection Settings	
3.2.3 SSH Connection Settings	
3.2.4 XONA Relay Connection Settings	
3.3 View Connections	
3.3.1 Edit Connection	
3.3.2 Additional Connection Security	
3.4 Monitoring User Connections	
4.0 USER ADMINISTRATION	
4.1 User Administration Overview	••••••
4.2 Adding Users	
4.2.1 User Authentication	
4.2.2 Username + Password (Local Authorization)	••••••
4.2.5 Username + Password (Active Directory)	
4.2.4 Username/Password Authentication Errors	
4.2.5 Username/Password + PIPA	
4.2.0 02P Admenucation Errors	
4.2.9 OTP Authentication Errors	
4.2.9 DSA SecurID Tokan Authantication	
4.2.10 RSA Security Total Automatication Errors	
4 2 11 User Time Access Windows	
4 2 12 Access Window Date	
4.2.13 Access Window Time	
4.2.14 Time Zone	
4.2.15 Session Timeout	
4.2.16 Disabling Account Access	
4.3 User Access Control - View Users Menu	

XONA CSG Administrator Manual v4.0 – Page 2

		000 1010014.0
4.3.1 User Access Control & Role Mo	dification	
4.3.2 Deleting Users		
4.3.3 Viewing Users		
4.4 File Transfer Requests		
5.0 LOGS		
5.1 Gateway Logs		
5.2 Connection History		
6.0 SYSTEM CONFIGURATION		
6.1 Setup Menu		
6.1.1 Server Tab		
6.1.2 Gateway Tab		
6.1.3 Services Tab		
6.1.4 Security Tab		
6.1.5 MFA Tab		
6.1.6 File Share Tab		
6.1.7 System Tab		
7.0 MAINTENANCE		
7.1 Maintenance Procedure		



6.3. DOCUMENTATION SHOWING IMPLEMENTATION OF PROCESSES OR TECHNOLOGIES WHICH CAN DETECT MALICIOUS COMMUNICATIONS SUCH AS:

6.3.1. ANTI MALWARE TECHNOLOGIES

As a purpose-built appliance that protects the data stream between the user and the appliance and translates the OT protocols used between the appliance and the OT/ICS asset, there is no opportunity for malicious software to inject itself into the transaction between the user/OT operator and the OT environment. Any files to be transferred into the OT environment via the XONA CSG should be checked for malware based on organizational policies. The XONA CSG can be configured so that any file transfer requests must be approved by a CSG Administrator.

6.3.2. INTRUSION DETECTION SYSTEM (IDS)/INTRUSION PREVENTION SYSTEM (IPS).

As a purpose-built appliance that protects the data stream between the user and the appliance and translates the OT protocols used between the appliance and the OT/ICS asset, there is no need to integrate IDS/IPS technology.

6.3.3. AUTOMATED OR MANUAL LOG REVIEWS.

XONA CSG can capture both data and video logs. This information can either be reviewed locally or forwarded to another security tool, such as a SIEM.



XONA CSG Administrator Manual v4.0 – Page 24



6.3.4. ALERTING

Through integration with a Moxa relay, we can provide physical alerting using external emergency lighting or sirens at a local plant. This enables the CSG to alert local personnel as to the status of the network as well as connectivity through the CSG to critical assets. This enables the CSG to communicate to personnel in the plant without needing to look at a computer screen.

Alerting can also be achieved by integration with a SIEM or other log aggregation service that supports alerting. There are no alerting capabilities native to the CSG.



XONA CSG Configuration Manual – Software v4.0 – Page 50



XONA CSG Configuration Manual – Software v4.0 – Page 50



6.3.5. OTHER OPERATIONAL, PROCEDURAL, OR TECHNICAL CONTROLS.

The XONA CSG supports a variety of controls focused on providing a zero-trust approach to secure user access.

YONA CEC	
AUNA CSG	
ADMINISTRATOR MANUAL	
TABLE OF CONTENTS	Pa
1.0 GETTING STARTED	
1.1 XONA Critical System Gateway (CSG) Administration Overview	
1.2 Points of Contact	
1.2.1 Help Desk and Support	
1.3 Did you perform the Initial CSG Setup?	
1.4 Acronyms and Abbreviations	
2.0 ADMINISTRATION USER INTERFACE (UI)	
2.1 Administration UI Overview	
3.0 MANAGE CONNECTIONS	
3.1 Managing Asset Connections	
3.2 Add Connection	
3.2.1 RDP Connection Settings	
3.2.2 VNC Connection Settings	
3.2.3 SSH Connection Settings	
3.2.4 XONA Relay Connection Settings	
3.3 View Connections	
3.3.1 Edit Connection	
3.3.2 Additional Connection Security	
3.4 Monitoring User Connections	
4.0 USER ADMINISTRATION	
4.1 User Administration Overview	
4.2 Adding Users	
4.2.1 User Authentication	
4.2.2 Username + Password (Local Authorization)	
4.2.3 Username + Password (Active Directory)	
4.2.4 Username/Password Authentication Errors	
4.2.5 Username/Password + MFA	
4.2.6 U2F Authentication Errors	
4.2.7 OTP Token Enrollment	
4.2.8 OTP Authentication Errors	
4.2.9 RSA SecurID Token Authentication	
4.2.10 RSA SecurID Authentication Errors	
4.2.11 User Time Access Windows	
4.2.12 Access Window Date	
4.2.13 Access Window Time	
4.2.14 Time Zone	
4.2.15 Session Timeout	
4.2.16 Disabling Account Access	
4.3 User Access Control - View Users Menu	

XONA CSG	i Administrator	Manual	v4.0 –	Page 2

4.3.1 User Access Control & Role Mo	dification	
4.3.2 Deleting Users		
4.3.3 Viewing Users		
4.4 File Transfer Requests		
5.0 LOGS		
5.1 Gateway Logs		
5.2 Connection History		
6.0 SYSTEM CONFIGURATION		
6.1 Setup Menu		
6.1.1 Server Tab		
6.1.2 Gateway Tab		
6.1.3 Services Tab		
6.1.4 Security Tab		
6.1.5 MFA Tab		
6.1.6 File Share Tab		
6.1.7 System Tab		
7.0 MAINTENANCE		
7.1 Maintenance Procedure		

XONA CSG Administrator Manual v4.0 - Page 3



ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

